JNCIE-SEC Certification Self-Study Bundle

Revision 1.b

Student Workbook and Lab Guide

Juniper Networks | Education Services

1133 Innovation Way
Sunnyvale, CA 94089 USA
408-745-2000
www.juniper.net

Course Number: EDU-JNCIE-SEC-BOOK

Juniper Business Use Only

This document is produced by Juniper Networks, Inc.

This document or any part thereof may not be reproduced or transmitted in any form under penalty of law, without the prior written permission of Juniper Networks Education Services.

Juniper Networks, Junos, Steel-Belted Radius, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. The Juniper Networks Logo, the Junos logo, and JunosE are trademarks of Juniper Networks, Inc. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners.

JNCIE-SEC Certification Self-Study Bundle, Revision 1.b

Copyright © 2020 Juniper Networks, Inc. All rights reserved.

Printed in USA.

Revision History:

Revision 1.a—March 2019
Revision 1.b—March 2020

The information in this document is current as of the date listed above, has been carefully verified, and is believed to be accurate as of this publication date. Juniper Networks assumes no responsibilities for any inaccuracies that may appear in this document. In no event will Juniper Networks be liable for direct, indirect, special, exemplary, incidental, or consequential damages resulting from any defect or omission in this document, even if advised of the possibility of such damages.

Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

YEAR 2000 NOTICE

Juniper Networks hardware and software products do not suffer from Year 2000 problems and hence are Year 2000 compliant. The Junos operating system has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

SOFTWARE LICENSE

The terms and conditions for using Juniper Networks software are described in the software license provided with the software, or to the extent applicable, in an agreement executed between you and Juniper Networks, or Juniper Networks agent. By using Juniper Networks software, you indicate that you understand and agree to be bound by its license terms and conditions. Generally speaking, the software license restricts the manner in which you are permitted to use the Juniper Networks software, may contain prohibitions against certain uses, and may state conditions under which the license is automatically terminated. You should consult the software license for further details.

Contents

Contents 3
About This Publication 10
Education Services Offerings 10
Technical Publications 10
Juniper Networks Support 10
Target Audience 11
Exam strategy 11
Lab Preparation 11
Day Before the Exam 12
Exam Day 12
After the Exam 13
Lab Setup Information 13
Chapter 1: General System Features 16
Task 1: Initial Configuration 16
Task 2: Authentication and Authorization 18
Task 3: Syslog 18
Task 4: NTP 19
Task 5: SNMP 19
Chapter 2: High Availability 20
Task 1: Creating Clusters – Initial Setup 21
Task 2: Configuring Redundancy Groups and Redundant Ethernet Interfaces ... 21

© 2020 Juniper Networks, Inc. All rights reserved.

Chapter 3: Firewall - Security Policies 23
Task 1: Configuring Interfaces and Security Zones 24
Task 2: Local Traffic and Static Routing 25
Task 3: Security Policies 25
Chapter 4: Unified Threat Management 28
Task 1: Web-filtering 29
Task 2: Antivirus 30
Task 3: Content Filtering 31
Task 4: Antispam 32
Chapter 5: IPsec VPNs 33
Task 1: Configuring Policy-based VPN 34
Task 2: Configuring Route-based VPN 36
Task 3: Configuring GRE-tunnel over Route-based VPN 39
Task 4: Configuring ADVPN 41
Chapter 6: NAT 42
Task 1: IPv4 Source NAT 43
Task 2: IPv4 Destination NAT 44
Task 3: IPv4 Static NAT 45
Task 4: NAT Protocol Translation (IPv6/IPv4) 45
Chapter 7: Attack Prevention and Mitigation 46
Task 1: Firewall Filters 47
Task 2: SCREEN 47
Task 3: Intrusion Prevention System 48

© 2020 Juniper Networks, Inc. All rights reserved.

Chapter 8: Extended Implementation Concepts 50
Task 1: Transparent Mode 51
Task 2: Filter Based Forwarding 51
Chapter 9: Advanced Services 52
Task 1: Application Identification 53
Task 2: AppTrack 53
Task 3: AppQoS 53
Task 4: SSL Proxy 54
Task 5: Juniper Identity Management Service (JIMS) 54
Task 6: Security Logging 54
Task 7: Software Defined Secure Network (SDSN) 55
Super Lab 1 56
Task 1: Initial Configuration - Part 1 58
Task 2: Initial Configuration - Part 2 60
Task 3: Interfaces, Zones, Local Traffic, Routing, and Routing Instances 62
Task 4: UTM 64
Task 5: NAT 65
Task 6: IPsec VPN 67
Task 7: Attack Prevention and Mitigation 69
Task 8: Advanced Services – Central Cluster 70
Task 9: Software Defined Secure Network (SDSN) 71
Super Lab 2 72
Task 1: Initial Configuration - Part 1 74

© 2020 Juniper Networks, Inc. All rights reserved.

Task 2: Initial configuration - Part 2 75
Task 3: Control Plane Protection 78
Task 4: Interfaces, Zones, Local Traffic, and Routing 79
Task 5: UTM 81
Task 6: NAT 82
Task 7: IPsec VPN 84
Task 8: Attack Prevention and Mitigation 89
Task 9: Advanced Services – Central cluster 90
Task 10: Software Defined Secure Network (SDSN) 91
Appendices 92
Appendix - Chapter 1: General System Features 93
Task 1: Initial Configuration 94
Task 2: Authentication and Authorization 97
Task 3: Syslog 100
Task 4: NTP 101
Task 5: SNMP 102
Appendix - Chapter 2: High availability 104
Task 1: Creating Clusters – Initial Setup 106
Task 2: Configuring Redundancy Groups and Redundant Ethernet Interfaces. 110
Appendix - Chapter 3: Firewall - Security policies 118
Task 1: Configuring Interfaces and Security Zones 121
Task 2: Local Traffic and Static Routing 124
Task 3: Security Policies 125

© 2020 Juniper Networks, Inc. All rights reserved.

Appendix - Chapter 4: Unified Threat Management 155
Task 1: Web-filtering 159
Task 2: Antivirus 167
Task 3: Content Filtering 171
Task 4: Antispam 173
Task 5: Testing 176
Appendix - Chapter 5: IPsec VPNs 177
Task 1: Configuring Policy-based VPN 180
Task 2: Configuring Route-based VPN 193
Task 3: Configuring GRE-Tunnel Over Route-Based VPN 204
Task 4: Configuring ADVPN 210
Appendix - Chapter 6: NAT 224
Task 1: Source NAT 228
Task 2: Destination NAT 237
Task 3: Static NAT 242
Task 4: NAT Protocol Translation (IPv6/IPv4) 248
Appendix - Chapter 7: Attack Prevention and Mitigation 252
Task 1: Firewall Filters 255
Task 2: SCREEN 258
Task 3: Intrusion Prevention System 262
Task 4: Verification 271
Appendix - Chapter 8: Extended Implementation Concepts 275
Task 1: Transparent Mode 276

© 2020 Juniper Networks, Inc. All rights reserved.

Task 2: Filter Based Forwarding 281
Task 3: Verification 282
Appendix - Chapter 9: Advanced Services 284
Task 1: Application Identification 285
Task 2: AppTrack 286
Task 3: AppQoS 287
Task 4: SSL Proxy 289
Task 5: Juniper Identity Management Service (JIMS) 294
Task 6: Security Logging 297
Task 7: Software Defined Secure Network (SDSN) 300
Appendix - Super Lab 1 361
Task 1: Initial Configuration – Part 1 364
Task 2: Initial Configuration - Part 2 370
Task 3: Interfaces, Zones, Local Traffic, Routing, and Routing Instances 389
Task 4: UTM 401
Task 5: NAT 413
Task 6: IPsec VPN 427
Task 7: Attack Prevention and Mitigation 446
Task 8: Advanced Services – Central cluster 452
Task 9: Software Defined Secure Network (SDSN) 460
Appendix - Super Lab 2 510
Task 1: Initial Configuration – Part1 513
Task 2: Initial Configuration – Part 2 519

© 2020 Juniper Networks, Inc. All rights reserved.

Task 3: Control Plane Protection 522
Task 4: Interfaces, Zones, Local Traffic, and Routing 542
Task 5: UTM 554
Task 6: NAT 566
Task 7: IPsec VPN 590
Task 8: Attack Prevention and Mitigation 643
Task 9: Advanced Security – Central cluster 649
Task 10: Software Defined Secure Network (SDSN) 656

© 2020 Juniper Networks, Inc. All rights reserved.

About This Publication

The JNCIE-SEC lab exam workbook is designed for candidates to practice technologies covered in the JNCIE-SEC lab exam. It also helps candidates practice skills relating to task prioritization, dependencies, and correlations.

This workbook is split into two parts. The first part of the guide outlines the high level tasks for each chapter and practice labs (referred to as Super Labs). The second part is the appendix, which contains the detailed explanations and configuration steps to complete each task.

The JNCIE-SEC Lab exam preparation workbook consists of 9 virtual SRX-series devices running JUNOS version 18.4, a Linux based student-desktop device, a server running JUNOS Space with Security Director, Policy Enforcer and an Active Directory/JIMS server.

Education Services Offerings

You can obtain information on the latest Education Services offerings, course dates, and class locations from the World Wide Web by pointing your Web browser to: http://www.juniper.net/training/education/.

Technical Publications

You can print technical manuals and release notes directly from the Internet in a variety of formats:

- Go to http://www.juniper.net/techpubs/.
- Locate the specific software or hardware release and title you need and choose the format in which you want to view or print the document.

Documentation sets and CDs are available through your local Juniper Networks sales office or account representative.

Juniper Networks Support

For technical support, contact Juniper Networks at http://www.juniper.net/customers/support/, or at 1-888-314-JTAC (within the United States) or 408-745-2121 (outside the United States).

© 2020 Juniper Networks, Inc. All rights reserved.

Target Audience

This workbook is developed for experienced network engineers who are preparing for the JNCIE-SEC lab exam. Although not required, it is highly recommended that you have passed the JNCIA-SEC, JNCIS-SEC, and JNCIP-SEC written exams before you start using this workbook. The *JNCIE-SEC Certification Self-Study Bundle* is a hands-on guide to validate the skills needed to pass the official JNCIE-SEC lab exam. This guide is based on official JNCIE-SEC exam objectives and is targeted at JNCIP-SEC certified engineers who are studying for the expert-level certification and need extra help preparing for the exam. Each chapter covers several technologies with expert-level configuration tasks and detailed answers. In this workbook you will find several technology introductions. However, do not expect a full explanation about OSPF, BGP, IPsec, Junos Space, etc. because there are other resources available to learn the prerequisite knowledge. This guide also contains two practice exams to give you a similar experience to a real JNCIE-SEC exam.

Exam strategy

Lab Preparation

To earn the JNCIE-SEC credential you must first pass the following Juniper Networks written exams: JNCIA-SEC, JNCIS-SEC, and JNCIP-SEC. Finally, you must also pass the very challenging 6 hour JNCIE-SEC lab exam. You must have extensive hands-on experience with the latest Junos Security technologies on vSRX, Junos Space/ Security Director, Sky ATP SDSN, and JIMS. When preparing for the JNCIE-SEC lab exam ensure you fully understand the exam topics and objectives. The latest update for the JNCIE-SEC lab exam topics and objectives can be found on the Juniper Networks certification website.

Use this workbook to verify if you are ready for the JNCIE-SEC lab exam as it covers very challenging tasks specifically written for JNCIE-SEC lab preparation. The workbook tasks are written at the same difficulty level as the JNCIE-SEC lab exam and follows the same structure.

We recommend completing all the workbook's chapter and practice exam tasks at least twice. The first time, work through all the tasks and use the solutions as often as you like. The second time try to solve all the chapter and practice lab tasks without looking at the solutions.

While using this workbook, ensure that you take study notes and record the time spent on each task. Time is of the essence for the JNCIE-SEC lab exam.

© 2020 Juniper Networks, Inc. All rights reserved.

Day Before the Exam

We advise you not to do extensive lab preparation anymore on this day as you should be ready by now, perhaps some review of your study notes, but that's it! On the day before your exam your goal is to stay relaxed and rest.

When travelling multiple hours to the JNCIE lab testing location, please ensure you book a hotel in advance and arrive on the day before of your exam. If possible, visit the JNCIE lab testing center and familiarize yourself with the location. Go to bed early as tomorrow it will be a long day.

Exam Day

When you wake up, ensure you dress comfortable and have a good breakfast. This will be a very long day! Ensure you arrive 30 minutes before the exam start time. Ensure you do not forget to take a valid ID with you, exam registration confirmation and if you prefer your own keyboard and mouse. If you forget your ID, the JNCIE lab exam proctor will not allow you to take the exam. When it's time to enter the exam room, the JNCIE lab exam proctor will direct you to your workstation. Using the SecureCRT or Putty software which provides OOB access to the exam devices. There are Juniper Networks security related PDF documentation files installed on your computer, which you can use to lookup certain commands/features. You do not have Internet access.

When the proctor notifies you that the exams begins, you are allowed to open the exam documents. Before immediately starting with the first task, we would like to advise you to read the entire exam and study the topology first to fully understand all requirements and how tasks might correlate to each other.

Be familiar with the Windows notepad application as it is a real time saver. For example, if you have to apply security policies to multiple devices, with just some small changes then notepad is your friend.

Timing is important! Be quick but pay attention to detail. A simple typo in a firewall filter configuration can cause you to fail a complete task or even the entire exam. Ensure that you meet all requirements as mentioned in the exam documents. You will not be given partial points for tasks.

Be sure there is plenty of time at the end of the day to verify every task for the second time. This is important because you might have broken parts of the network during the exam. In addition to this, you might have missed something in the question when you read it the first time. And finally, after going through the entire exam, you might have a different (or better) understanding of what it is that you are supposed to do.

© 2020 Juniper Networks, Inc. All rights reserved.

If you are struggling with a task for more than 10-15 minutes, check the task and determine whether or not it will have impact on the rest of your exam. If it does not impact any other task on the exam, move to the next task and revisit the question again later on during the exam.

Do not assume any other requirement then then ones mentioned in the tasks. The JNCIE exam is about fulfilling the tasks. It is not about displaying your understanding of the best-practices, scalable network design or anything other than fulfilling the task requirements. So, it might be that your reth interface does not have redundant physical links, the cluster-id is completely random, OSPF timers are not tweaked and the sessions are not authenticated. As long as the tasks do not require any of these things, no one cares!

Sometimes there are multiple ways to complete a task. In that case you can choose your preferred option. If you are unsure about a task requirement then ask the proctor. Do not be shy. While the JNCIE lab exam proctor cannot assist you in solving the tasks, he or she can certainly help you in clarifying the task requirements.

Notify the JNCIE lab exam proctor immediately if you suspect a hardware issue. If it is, the proctor will fix the issue and might extend your time. If not, the proctor will tell you that the issue is caused by your own configuration and that no additional time will be given.

Make sure that you have at least ***one*** task correct in ***each*** section of the exam, if not you will fail the entire exam even if your total score is above the passing requirement!

Be sure to understand that a configuration mistake might result in point loss for multiple sections of the exam. As an example: if you apply a misconfigured firewall filter it might bring your BGP, IGP neighbors and perhaps also other protocols down, which results in point loss for multiple sections.

After the Exam

That's it! There is nothing more you can do for now. It's time to wait and hope you passed the JNCIE lab exam. It usually takes 5 business days before you receive your exam results. If you pass, great! If not, we recommend you retake the exam again as soon as possible as all topics are still fresh in your memory! Some candidates wait a couple of months between attempts. This usually results in losing your configuration speed and it takes more time and energy to relearn/memorize all the topics again.

Lab Setup Information

In the figure below, the management topology is shown that is used throughout this workbook. Together with this workbook you can access the configuration files on each device that you will need while working through the chapters of the course. The workbook

© 2020 Juniper Networks, Inc. All rights reserved.

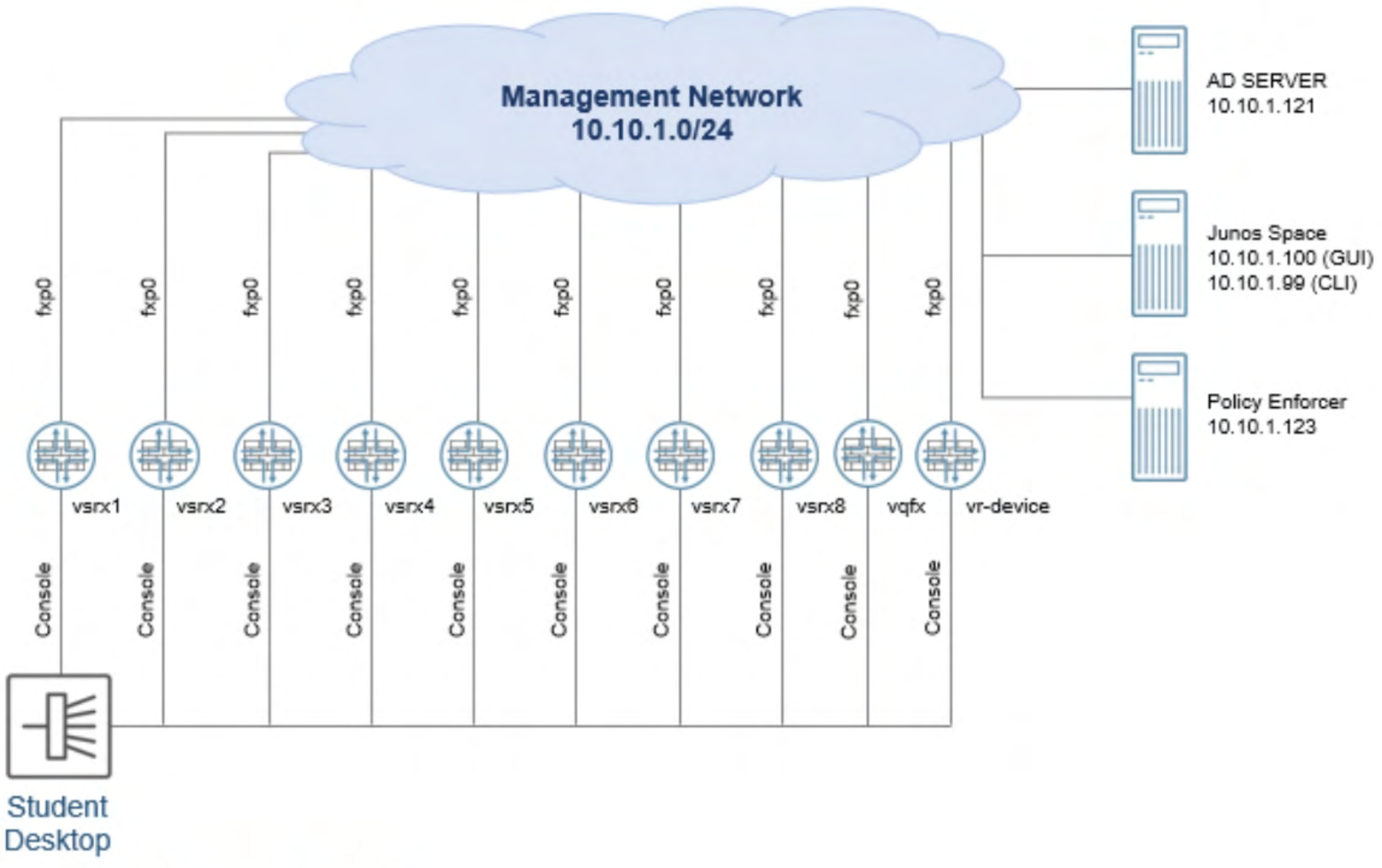
configurations files consist of initial, part, and final configurations for each chapter. These configuration files are stored on the respective device under the /var/home/lab directory.

Note: This workbook has been built to be serial in nature meaning that each chapter builds on previous chapter configurations. You can load the start configuration on **all** devices in the topology to ensure the environment is correct for each chapter and part. For example, if you would like to start with Chapter 4, you must load the ch4-start.config configuration file. In addition to start configurations, end configurations have been provided for each chapter and can be used to verify that all tasks are completed and working properly.

Important: To access the devices in this environment please use the user credentials outlined in the table below:

Device	Username	Password
vSRXs	lab	lab123
Space GUI	super	lab123
Policy Enforcer	root	lab123@Lab
AD Server	jncie	jncie123
Desktop	lab	lab123

© 2020 Juniper Networks, Inc. All rights reserved.



Device and Management Diagram

© 2020 Juniper Networks, Inc. All rights reserved.

Chapter 1: General System Features

This chapter focuses on initial system configuration and general system features. You will configure various features, such as hostnames, access to the management network, authentication and authorization, NTP, SNMP and syslog.

Note: Load the configs on the lab devices. Ensure that you do not forget to load the vr-device configuration for the chapter labs.

Tip: Ensure you read this entire chapter, before starting with the first task.

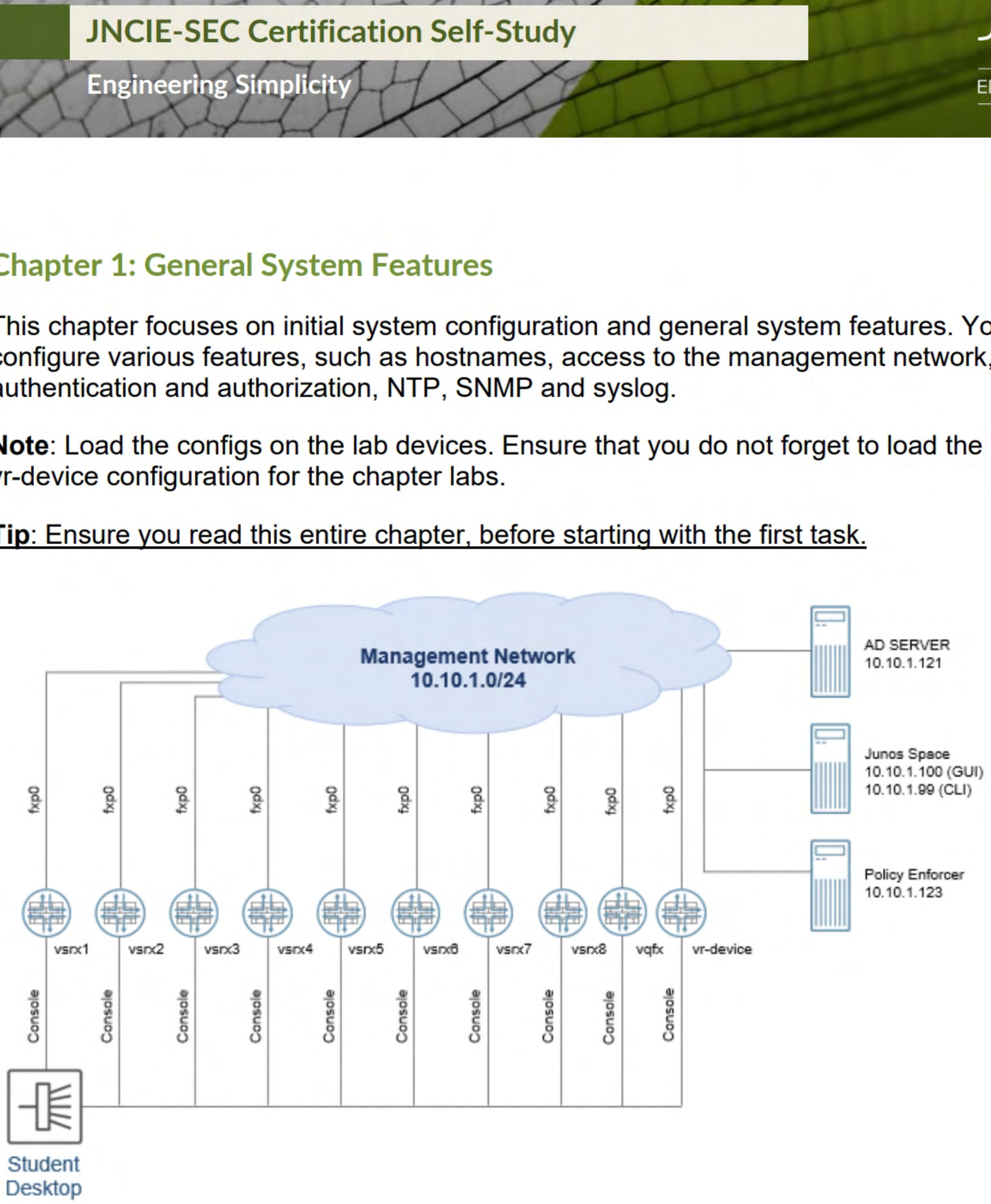


Figure 1: Chapter 1 Topology

Task 1: Initial Configuration

In this part you will configure the device hostnames, the management network interface details including definition of specific services allowed for accessing the device.

1) Configure the hostnames on the devices according the table below:

© 2020 Juniper Networks, Inc. All rights reserved.

Device	Hostname
srx1	srx1
srx2	srx2
srx3	srx3
srx4	srx4
srx5	srx5
srx6	srx6
srx7	srx7
srx8	srx8

2) Based on the topology diagram configure the management and loopback interfaces on each device with the IP address as listed in the table below:

Device	Management IP address	Loopback IP address
srx1	10.10.1.1/24	192.168.1.1/32
srx2	10.10.1.2/24	192.168.1.2/32
srx3	10.10.1.3/24	192.168.1.3/32
srx4	10.10.1.4/24	192.168.1.4/32
srx5	10.10.1.5/24	192.168.1.5/32
srx6	10.10.1.6/24	192.168.1.6/32
srx7	10.10.1.7/24	192.168.1.7/32
srx8	10.10.1.8/24	192.168.1.8/32

3) The management interface on each device needs to be used purely only for management access and won't accept any transit traffic. In addition, this interface will accept only specific services as defined in the table below:

Device	Services
srx1	SSH with allowed root access, telnet, HTTP, HTTPS
srx2	SSH with allowed root access, telnet, HTTP, HTTPS
srx3	SSH with allowed root access, telnet, HTTP, HTTPS
srx4	SSH with allowed root access, telnet, HTTP, HTTPS
srx5	SSH with allowed root access, telnet, HTTP, HTTPS
srx6	SSH with allowed root access, telnet, HTTP, HTTPS
srx7	SSH with allowed root access, telnet, HTTP, HTTPS
srx8	SSH with allowed root access, telnet, HTTP, HTTPS

© 2020 Juniper Networks, Inc. All rights reserved.

Ensure the listed services are enabled.

4) Limit the number of SSH connections to maximum 5 per minute. This limitation is also valid for telnet.

Task 2: Authentication and Authorization

In this part you will configure new users allowed to access the devices and define their privileges and permissions.

1) On every device create a new user lab with the password lab123 that will have super-user privileges.
2) Configure the following additional users on the devices as defined in the table below:

Username	Password	Device	Privileges
ronly	ronly123	All	Has permissions “view” and “view-configuration”. Additionally, can NOT execute the “file delete” command.
admin1	admin123	All	Has permissions “all”. Can access the configuration mode only using “configure private” command.
restricted	restricted123	All	Has permissions “clear” and execute only the “show system uptime”, “show system storage” and “show interfaces terse” commands and nothing else.

Task 3: Syslog

1) Ensure that all devices have following SYSLOG configuration:
   a) All “emergency” messages regardless of the facility are displayed on terminals of all currently logged users.
   b) All messages regardless of the facility with the severity of “critical” and higher are sent to the default syslog file.
   c) A file named “interactive-commands” with command audit trail is maintained, i.e. file with records about the users and commands they execute.
   d) A separate file named “security-policy-logs” is used for security policy log entries. The system should retain 20 archive files each with size of 512 KB (524288 B).

© 2020 Juniper Networks, Inc. All rights reserved.

e) A separate file named “authorization-file” is used for authorization messages with the severity “info” and higher.
f) All “emergency” messages regardless of the facility are sent to the syslog server at 10.10.1.121. Additionally, use a non-physical address as source address for the syslog messages.
g) Ensure the information about the year is included in these messages.

Task 4: NTP

1) Ensure that all devices synchronize their time with the NTP server reachable at 10.10.1.254. Additionally, use a non-physical address as source address.
2) On all devices set the time zone to America/Los_Angeles.
3) Use MD5 authentication with the key number 1 and the password set to “**jncie**”.

Task 5: SNMP

1) Configure all devices to accept read-only SNMP requests from the NMS system located at 10.10.1.254 using the community string “**reading**”.
2) Configure all devices to send the following SNMP traps to the NMS system:
   a) Authentication failures
   b) Hardware and environment
   c) Link transitions
   d) Routing protocol
3) Configure all vSRX devices to accept SNMP requests from Junos Space located at 10.10.1.121 using the community string “JNCIE”

© 2020 Juniper Networks, Inc. All rights reserved.

Chapter 2: High Availability

This chapter focuses on high availability on the SRX devices, i.e. clustering. You will create two SRX clusters and configure them, including control and fabric links, redundancy groups (RG) and their parameters, and redundant Ethernet interfaces (reth).

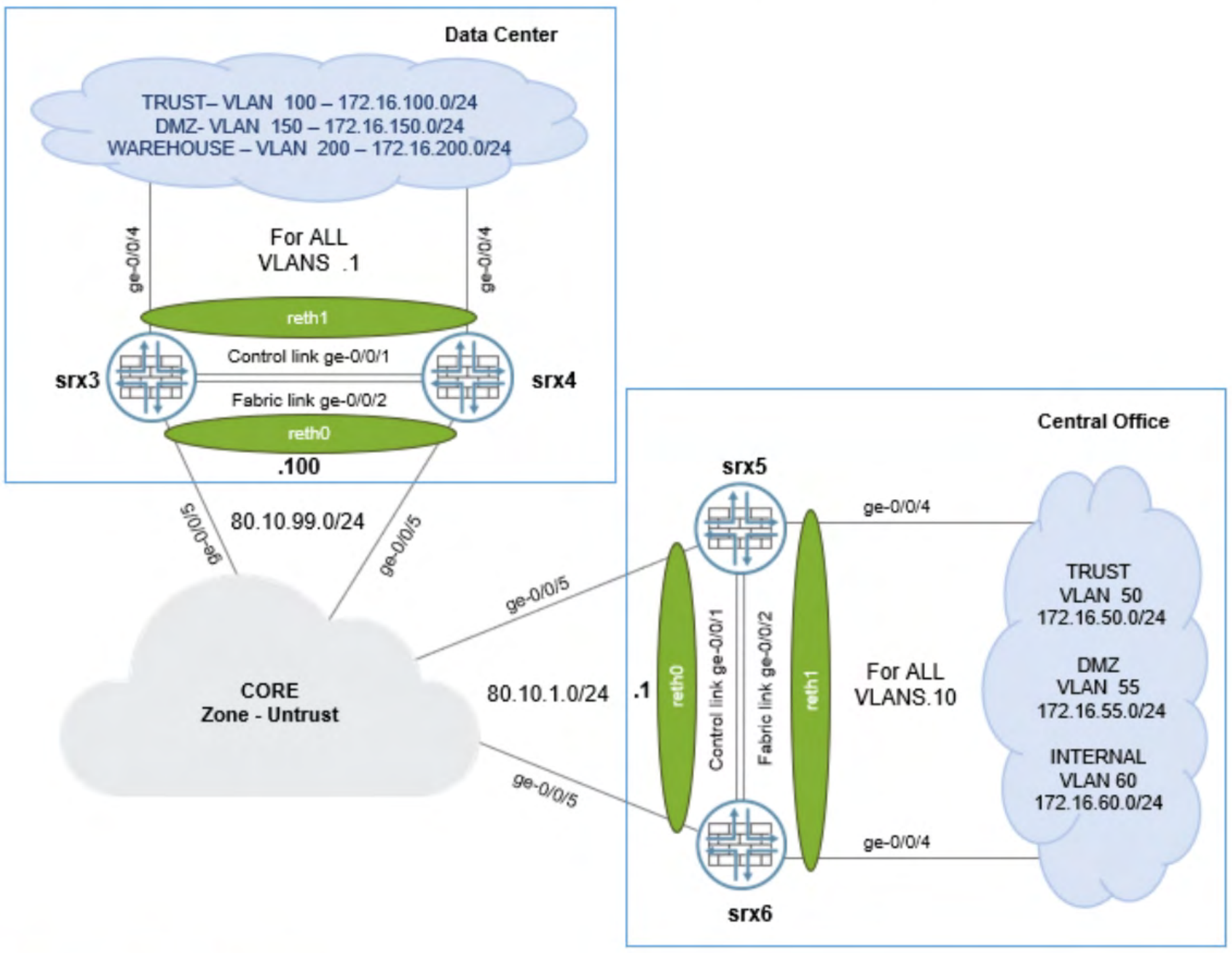


Figure 1: Chapter 2 Topology

You can continue with the configuration in case you have completed tasks from the previous chapter. OR load the latest initial configurations for this chapter.

Note: In case you have already loaded the initial configuration for the vr-device before you don't have to do it again.

Tip: Ensure you read this entire chapter, before starting with the first task.

© 2020 Juniper Networks, Inc. All rights reserved.

Task 1: Creating Clusters – Initial Setup

In this part you will create 2 clusters.

1) Create clusters as defined in the table below:

Device	Node id	Cluster id
srx3	0	1
srx4	1	1
srx5	0	2
srx6	1	2

2) Ensure that both clusters use ge-0/0/2 as the fabric link. Additionally, configure automatic reboot of disabled node after control link failure recovery.
3) Configure each node in both clusters with the hostname and management IP address according to the table below:

Cluster-id/Node-id	Hostname	Management IP address
1/0	srx3	10.10.1.3/24
1/1	srx4	10.10.1.4/24
2/0	srx5	10.10.1.5/24
2/1	srx6	10.10.1.6/24

4) The loopback addresses for the clusters are as follows:

Cluster	IP address
Cluster-id 1	192.168.1.3/32
Cluster-id 2	192.168.1.5/32

Task 2: Configuring Redundancy Groups and Redundant Ethernet Interfaces

Here you will create redundancy groups (RG) and define their parameters, configure redundant ethernet interfaces (reth) and associate them with the redundancy groups.

1) Ensure the node 0 will be the primary for the routing engine RG on both clusters.
2) Configure redundant ethernet interfaces on both clusters as depicted on the topology image.

© 2020 Juniper Networks, Inc. All rights reserved.

3) On cluster-id 1 (cluster 1):
    a) Configure RGs in a manner that allows the defined reths to failover independently of each other.
    b) If multiple RGs are needed to satisfy the previous requirement configure them to be always equally distributed among the nodes, i.e. if both nodes are available each node will have always active half of the RGs.
    c) Ensure each child interface failure triggers RG failover.
4) On cluster-id 2 (cluster 2):
    d) Configure RGs in a manner where all reths will be active always on the same node.
    e) There is no need to RGs failback after failure recovery.
    f) Ensure each child interface failure triggers RG failover.

Note: The following step is **informational** as the redundancy group IP address monitoring functionality is available only on High end SRX devices!

    g) In addition, configure IP monitoring/tracking for every created redundancy group with following aspects:
        i. Track:
            1. Gateway (next-hop) to the CORE network.
            2. IP address of srx7's interface from the INTERNAL zone
        ii. Use appropriate (nearest, not requiring specific security policy) reth interface for tracking.
        iii. The secondary node, e.g. the node having the backup interfaces, should also monitor all these IPs by using different source IP addresses. These IP addresses are incremented IP addresses (by one) of the selected reths.
        iv. Only failure of all tracked IP addresses will trigger redundancy group failover
        v. Failure is represented by 4 successive failed probes/pings and the detection has to be done in 8 seconds.

© 2020 Juniper Networks, Inc. All rights reserved.

Chapter 3: Firewall - Security Policies

This chapter deals with the security policies on the SRX devices. You will configure security policies on the SRX devices to satisfy requirements given in the individual tasks. Within this chapter you will also configure the interfaces, IP addresses and security zones.

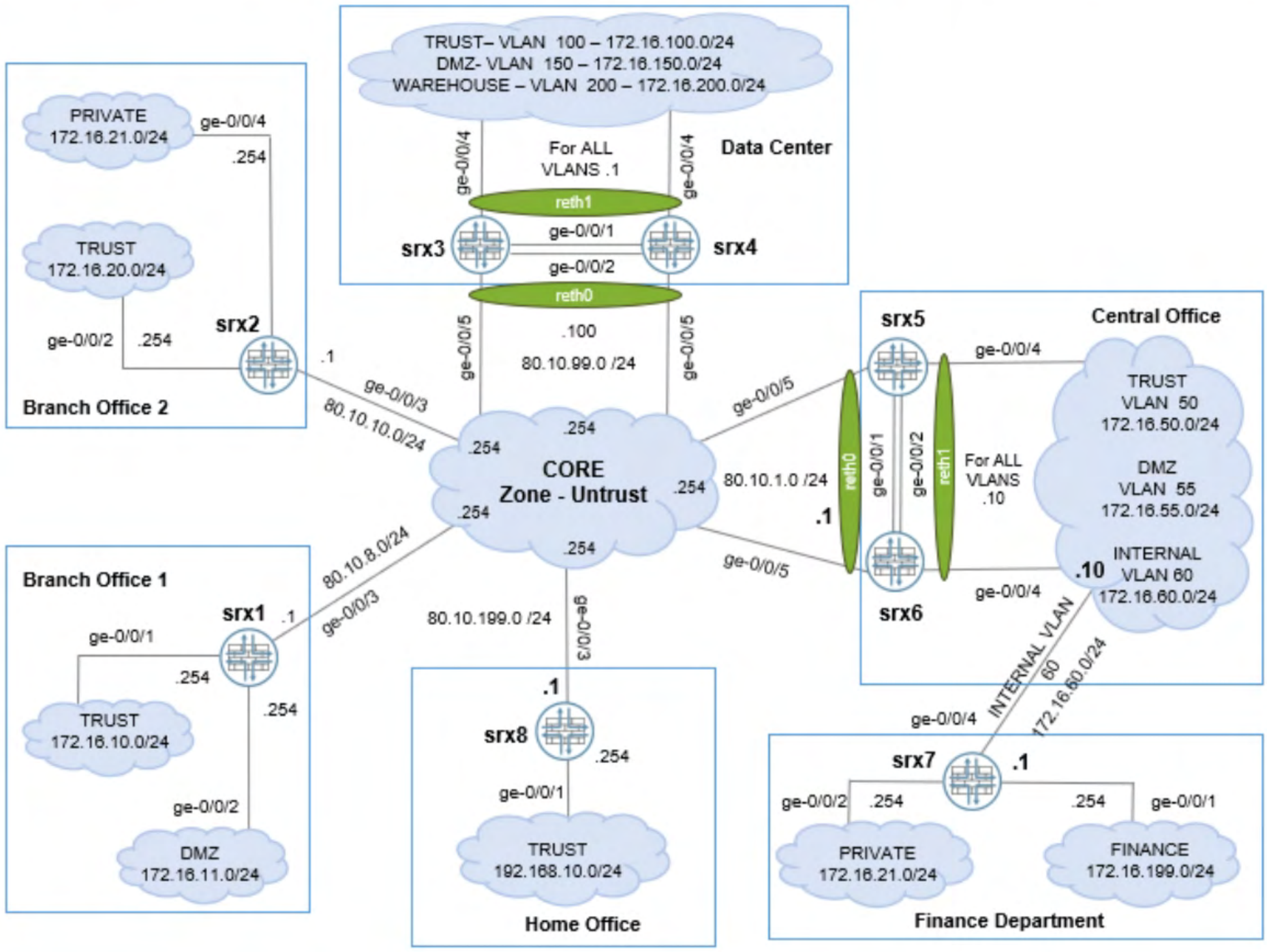


Figure 1: Chapter 3 Topology

You can continue with the configuration if you have completed tasks from the previous chapter. OR load the latest initial configurations for this chapter to the devices. If you have already loaded the chapters configuration for the vr-device previously you don't have to do it again.

Note: The labs starting point requires to have SRX clusters formed between devices srx3 – srx4 and srx5 – srx6 and the respective configuration loaded on them. Please note that a reboot might be required for the devices to be placed into cluster mode.
Tip: Ensure you read this entire chapter, before starting with the first task.

© 2020 Juniper Networks, Inc. All rights reserved.

Task 1: Configuring Interfaces and Security Zones

In this part you will configure the interfaces, zones and assign interfaces to zones.

1) Configure the interfaces on every device according to the table below. The table reflects the topology image.

   The association of loopback interfaces to zones is up to you unless explicitly defined by a given task.

Device	Interface	IP address	VLAN-ID	Zone
srx1	ge-0/0/1.0	172.16.10.254/24	None	TRUST
srx1	ge-0/0/2.0	172.16.11.254/24	None	DMZ
srx1	ge-0/0/3.0	80.10.8.1/24	None	UNTRUST
srx2	ge-0/0/2.0	172.16.20.254/24	None	TRUST
srx2	ge-0/0/3.0	80.10.10.1/24	None	UNTRUST
srx2	ge-0/0/4.0	172.16.21.254/24	None	PRIVATE
Cluster1 (srx3, srx4)	reth0	80.10.99.100/24	101	UNTRUST
Cluster1 (srx3, srx4)	reth1.100	172.16.100.1/24	100	TRUST
Cluster1 (srx3, srx4)	reth1.150	172.16.150.1/24	150	DMZ
Cluster1 (srx3, srx4)	reth1.200	172.16.200.1/24	200	WAREHOUSE
Cluster2 (srx5, srx6)	reth0	80.10.1.1/24	102	UNTRUST
Cluster2 (srx5, srx6)	reth1.50	172.16.50.10/24	50	TRUST
Cluster2 (srx5, srx6)	reth1.55	172.16.55.10/24	55	DMZ
Cluster2 (srx5, srx6)	reth1.60	172.16.60.10/24	60	INTERNAL
srx7	ge-0/0/1.0	172.16.199.254/24	None	FINANCE
srx7	ge-0/0/2.0	172.16.21.254/24	None	PRIVATE
srx7	ge-0/0/4.60	172.16.60.1/24	60	INTERNAL
srx8	ge-0/0/1.0	192.168.10.254/24	None	TRUST
srx8	ge-0/0/3.0	80.10.199.1/24	None	UNTRUST

© 2020 Juniper Networks, Inc. All rights reserved.

Task 2: Local Traffic and Static Routing

This part is focused on handling the traffic destined for the devices themselves.

1. Allow ping on all configured interfaces.
2. Allow OSPF protocol communication on all interfaces connected to the CORE.
3. Allow SSH connections to all interfaces associated with the TRUST zone on every device.
4. Ensure the management interfaces allow following services: SSH, telnet, HTTP, HTTPS, SNMP and NTP. In addition, ensure the srx8 allows for SNMP queries from 2.2.2.0/28 network.
5. Create static default route on each device pointing to the CORE network.
6. Configure the necessary routes using static configuration to provide connectivity for the PRIVATE zone in the Finance department through the cluster 2.
7. Create static route for accessing the NTP, SYSLOG, SNMP servers using the management network. The management network range is 10/8 and the next-hop for the srx devices is 10.10.1.254.

Task 3: Security Policies

Here you will configure security policies to enforce listed restrictions on the transit traffic.

Below are details about networks which are referenced in the tasks:

Name	Network range
Private corporate network	172.16.0.0/16
Internet	0.0.0.0/0

Branch office 1: srx1

1) The hosts from the TRUST zone and its network range can go to the outside network (Internet) with HTTP and HTTPS.
2) Ensure the hosts from the TRUST zone have access to the whole private corporate network (reachable via CORE network) with any application.
3) Devices in the DMZ zone should be accessible from the whole private corporate network including the local TRUST zone with HTTPS.
4) No other connections are allowed to go in or out of the TRUST zone.
5) No connections are allowed to go out from DMZ zone. Log all violations going out to the CORE network.

© 2020 Juniper Networks, Inc. All rights reserved.

Branch office 2: srx2

6) Ensure the hosts from the TRUST zone have access to the whole private corporate network (reachable via CORE network) with any application.
7) No other connections are allowed in or out of the TRUST zone. Log all outgoing violations to the destinations reachable via the CORE network.
8) Hosts from the PRIVATE zone can connect to the DMZ zone in the Central office and Data center using SSH, HTTP, HTTPS, FTP, telnet.

Home office: srx8

9) Hosts connected to the srx8 can access the whole private corporate network regardless of the application and in addition have HTTP and HTTPS permitted to the outside world/Internet.

Finance department: srx7

10) From the FINANCE zone all connections are allowed to the INTERNAL zone and to the WAREHOUSE zone in the Data center only for SQL queries. The database server in Data center listens on ports 5000 – 6000. Ensure the appropriate ALG for SQL is being used.
11) DMZ zones in the Data center and Central office are reachable from the FINANCE zone using HTTP, HTTPS and SSH.

Data center: cluster1

12) The TRUST zone has access to the whole private corporate network (also locally connected networks) with any application.
13) No other connections are allowed in or out of the TRUST zone. Log all outgoing violations, e.g. connections going to CORE network.
14) Full communication between DMZ (local and central office) and WAREHOUSE zone is possible in both directions.
15) Http, HTTPS, SSH, SMTP, FTP and telnet connections from the private corporate network (reachable via CORE network) to DMZ are allowed.
16) Only the specific SQL connections (described previously) from the FINANCE zone in the Finance department are allowed to enter the WAREHOUSE zone. Count this traffic.

© 2020 Juniper Networks, Inc. All rights reserved.

Central office: cluster2

17) Ensure the permitted connections from the Finance department on the srx7 are allowed as well, but focus only network ranges and not applications, i.e. when defining these policies disregard the applications.
18) Hosts located in the INTERNAL zone have full access to the local DMZ resources but only during working days and working hours (8:00 - 18:00).
19) The TRUST zone has access to the whole private corporate network (also locally connected networks) with any application. In addition, only HTTP and HTTPS access is allowed to the Internet from the TRUST zone. Log all outgoing violations.
20) Full communication between DMZ and WAREHOUSE zone is possible in both directions.
21) HTTP, FTP and Telnet requests sourced from the private corporate network arriving on the core network facing interface and destined to the DMZ hosts need to be authenticated in order to be granted. Use the pass-through authentication with following settings
    a. username: testuser, password: testuserpw123
    b. 1 hour of inactivity will result in re-authentication
    c. the passwords are stored locally on the security device
    d. FTP and telnet banners:
        i. initial banner: “Look out firewall authentication!!!”
        ii. in case of successful authentication: “Correct!”
        iii. in case of unsuccessful authentication: “Incorrect!”
22) SSH and HTTPS connections from private corporate network arriving on the core network facing interface and destined to the DMZ hosts the are granted without authentication.
23) Ensure DNS information is not changed when using NAT and ensure that the domain-name length for DNS packets is validated

© 2020 Juniper Networks, Inc. All rights reserved.

Chapter 4: Unified Threat Management

This chapter is dedicated to the Unified Threat Management (UTM) functionality on Junos security devices. The presented tasks will require you to configure web-filtering, content filtering, antivirus and anti-spam features.

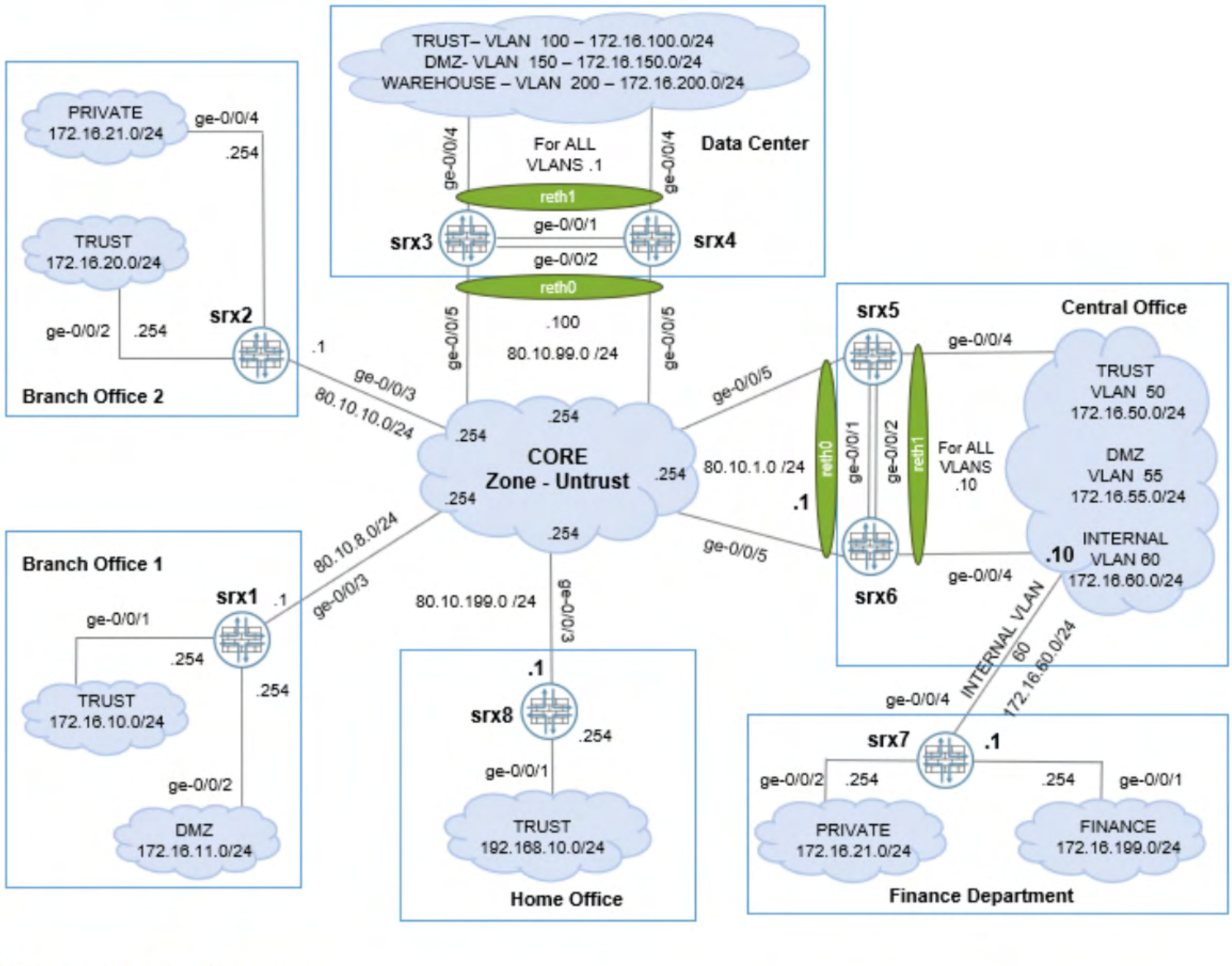


Figure 1: Chapter 4 Topology

You can continue with the configuration if you have completed tasks from the previous chapter. OR load the latest initial configurations for this chapter to the devices. If you have already loaded the chapters configuration for the vr-device previously you don't have to do it again.

Note: The labs starting point requires to have SRX clusters formed between devices srx3 – srx4 and srx5 – srx6 and the respective configuration loaded on them. Please note that a reboot might be required for the devices to be placed into cluster mode.
Tip: Ensure you read this entire chapter, before starting with the first task.

© 2020 Juniper Networks, Inc. All rights reserved.

Task 1: Web-filtering

In this section you will configure the web-filtering on the security devices in branch office, central office and home office.

Try to use existing security policies whenever possible.

Branch office: srx1

1) Protect the HTTP traffic from the TRUST zone to the UNTRUST zone by enabling web-filtering which fulfills following requirements.
2) The Juniper-enhanced type of web-filtering should be used.
3) The device handles the returned categories in following way:
    a. Hacking, Violence, Gambling, Games --> block these categories
    b. News and Media, Computer_Security --> permit these categories
    c. All other URLs --> permit but log the requests
4) In case of a blocked site the clients should receive following message: “Blocked site!”
5) In case the engine has difficulties due various reasons the traffic handling should be:
    a. In case the engine experiences too many requests the subsequent requests are blocked
    b. When problems with server communication (such as reaching the timeout for receiving the responses or server connectivity loss) occur the requests are blocked
    c. For all other causes the requests are permitted but logged
6) The timeout for the server responses is 120 seconds.

Central office: cluster 2

7) The web-filtering in the central office uses other method as the device in the Branch office, namely the WebSense option.
8) The protection happens from the TRUST zone to the UNTRUST zone.
9) The following URLs are excluded from the checking on the WebSense server and are permitted right away (HTTP pages are assumed here):
    a. Sites ending with “bing.com” are permitted
    b. The same applies for google.com sites
    c. The www.juniper.net site is allowed
10) The following URLs should be instantly denied regardless of the WebSense handling:
    a. www.facebook.com/
11) The WebSense server is located at 80.200.200.200 and the communication port is 12345.

© 2020 Juniper Networks, Inc. All rights reserved.

12) In case the security device has communication issues with the WebSense server it should block the requests. If other problems are experienced by the engine the requests are permitted but need to be logged, this includes the too many requests situation.
13) Set the communication timeout with the WebSense server to 180 seconds.
14) The client's notification about dropped requests has to be this custom message: "SRX blocked the request!"
15) The requests forwarded from security device in the central office need to carry information about redirect account to achieve specific treatment and rule enforcement at the WebSense server. The redirect account value is "central office".
16) The number of connections to the WebSense server has to be below 6.

Home office: srx8

17) The srx8 device should enforce the web filtering on the traffic from TRUST zone to the UNTRUST zone.
18) The web-filtering decisions are done entirely by the security device itself without any remote server interactions.
19) The following URLs are denied:
    a. www.facebook.com
    b. www.myspace.com
20) All other URLs are permitted.
21) If a request is blocked the clients will receive following message: "This page is not allowed!"
22) All issues or problems with processing the requests result in blocking behavior.

Task 2: Antivirus

This part contains the tasks related to the antivirus feature that need to take place on the srx8 device.

Home office: srx8

1) The antivirus protection needs operate in comprehensive protection mode, e.g. full file-based scanning utilizing the full database and being capable of applying heuristics methods.
2) Checks for database updates every 2 hours are automatically performed by the device.
3) The antivirus scanning has to be done on HTTP, FTP and SMTP traffic going from the TRUST zone to the Internet (UNTRUST zone). Use the existing policy, if needed modify it.
4) Exclude the www.company.com/ traffic from being scanned.
5) Exclude the video, application and audio mime types from being scanned including their subtypes with the exception of application/javascript and

© 2020 Juniper Networks, Inc. All rights reserved.

application/ecmascript, e.g. application/javascript and application/ecmascript are subject to antivirus scan.

6) Ensure the compressed files are scanned up to the 2nd level of compression.
7) Antivirus scanning has to be performed on all files regardless of their extension.
8) Enable intelligent prescreening.
9) Set the scan engine timeout to 10 minutes.
10) If the antivirus engine detects a virus, the infected message has to be changed by deleting the original content and the notification "AV Engine detected virus!" needs to be included. In case the virus was found in an email message, the sender needs to receive a message having subject "AntiVirus" and body "AV Engine detected virus!".
11) All fallback options are set to block except the default action which permits the traffic and generates a log about it.
12) Fallback notifications generation is according to the requirements below:
    a. Action BLOCK
        i. for non-email protocols message "AV denied the message, because it was not able to scan it!" will be sent to the application (e.g. application/protocol error will be generated)
        ii. for email protocols an email is sent to sender with subject "AntiVirus" and body "AV denied the message, because it was not able to scan it!"
    b. Action NON-BLOCK
        i. for email protocols the engine sends the message to the recipient but tags the subject with "AntiVirus" and body "AV was not able to scan the message!"
13) In case the AV needs longer time for examination, it should send every 25 seconds unchecked small parts of the file to the receiver side to prevent timeout from occurring.

Task 3: Content Filtering

This part lists the requirements for the content filtering performed on the central office security device.

Central office: cluster 2

1) The content filter has to be enforced on the HTTP traffic from TRUST zone to the UNTRUST zone.
2) Ensure the device blocks:
    a. HTTP content types: exe files, cookies and java applets
    b. mime: all video types
    c. files with the extensions bat and sh
    d. HTTP protocol command TRACE

© 2020 Juniper Networks, Inc. All rights reserved.

3) The device should generate protocol errors when blocking with custom message: "Blocked content by SRX!"

Task 4: Antispam

The requirements for the antispam feature are listed here.

Central office: cluster 2

1) One of the company email servers is located in the DMZ zone in the central office. The email server IP address is 172.16.55.100.
2) The SMTP communication from the outside world going to this email server needs to be inspected. If needed create appropriate security policy for this purpose (in the correct context of security zones, using correct address books and application).
3) The SMTP messages received from the 5.5.5.4 address are considered malicious but from the 5.5.5.5 IP address are valid and allowed. The 123.123.123.123 host is considered potentially dangerous too. The company internal policy defines to tag the subject in these email messages with the prefix “SPAM!!!”.
4) Similarly, the domains and email addresses below are considered potentially dangerous and therefore marked accordingly, e.g. tagging the email subject as in the previous case.
    a. Domains: bad.com, spam.com
    b. Email addresses: spam@company.com, adv@company.com
5) The security device performs the decisions internally without consulting any external resources, e.g. external SBLs are not used.

© 2020 Juniper Networks, Inc. All rights reserved.

Chapter 5: IPsec VPNs

This chapter is concentrated on IPsec VPN implementations. You will configure Policy-based IPsec VPN, Route-based IPsec VPN with OSPF, GRE tunnel over Route-based IPsec VPN with OSPF and ADVPN VPN.

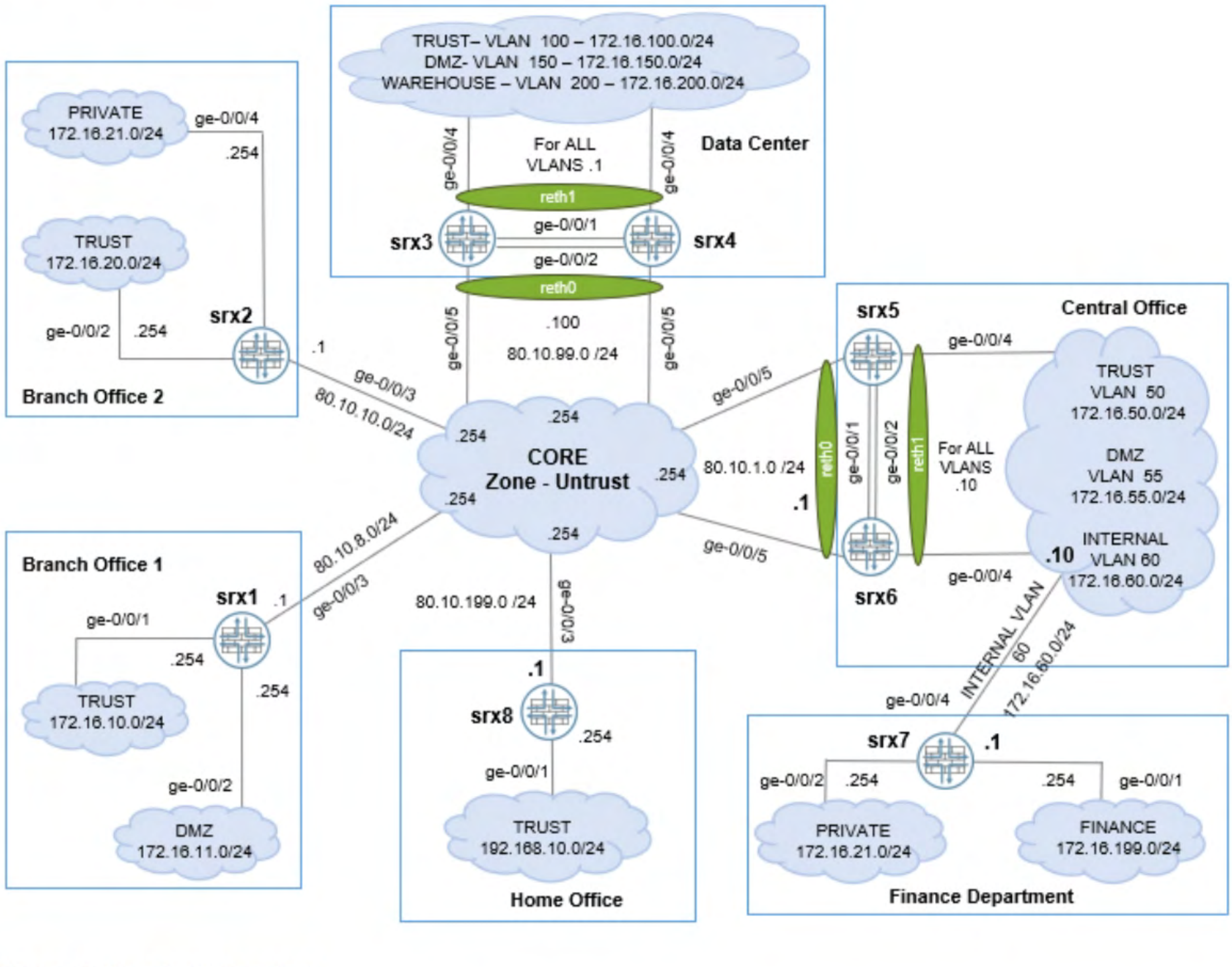


Figure 1: Chapter 5 Topology

You can continue with the configuration if you have completed tasks from the previous chapter. OR load the latest initial configurations for this chapter to the devices. If you have already loaded the chapters configuration for the vr-device previously you don't have to do it again.

Note: The labs starting point requires to have SRX clusters formed between devices srx3 – srx4 and srx5 – srx6 and the respective configuration loaded on them. Please note that a reboot might be required for the devices to be placed into cluster mode.
Tip: Ensure you read this entire chapter, before starting with the first task.

© 2020 Juniper Networks, Inc. All rights reserved.

Task 1: Configuring Policy-based VPN

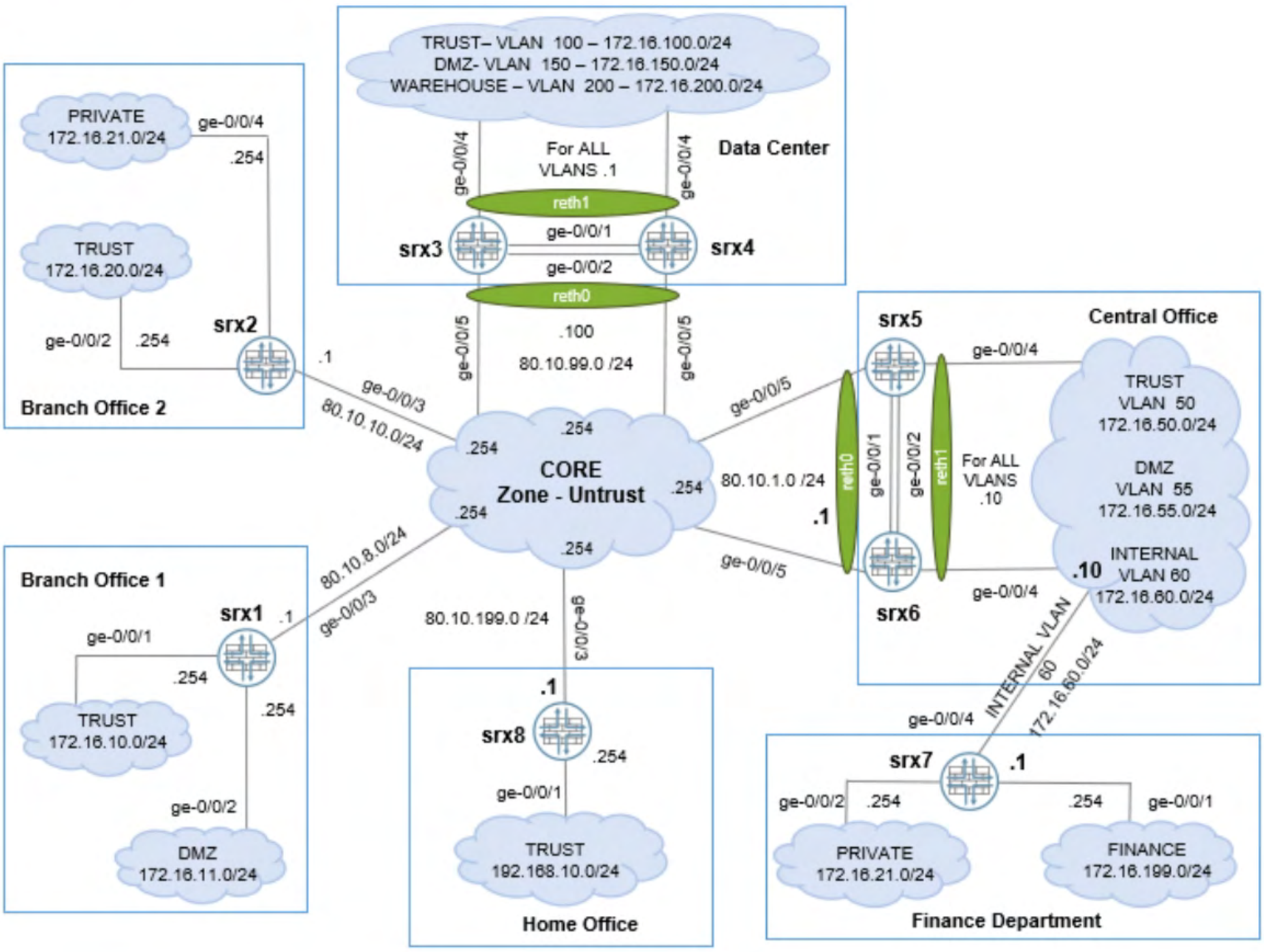


Figure 2: Chapter 5 – Task 1 Topology

In this part you will configure the lab equipment as necessary to build Policy-based VPN between the Data Center, Home Office and Finance department.

1) Configure the IPsec VPN on every device according to the table below, which reflects the topology image.

Local Peer	Interface	Security zone	Remote Peer	Interface	Security zone
srx7	ge-0/0/4.60	Untrust	Cluster1	reth0.0	Untrust
srx8	ge-0/0/3.0	Untrust	Cluster1	reth0.0	Untrust

2) Central Office srx5/srx6 cluster provides only dynamical NAT-SRC service.

© 2020 Juniper Networks, Inc. All rights reserved.

3) The VPN between srx8 and Cluster1 must meet following requirements:
    a. Validate peer reachability with DPD option. The keepalives should be sent to the neighboring peer regardless of traffic patterns every 10 seconds. Consider the peer unreachable if the number of DPD retransmissions exceeds 5 packets.
    b. IKE phase 1 proposal must include: preshared key “juniper”, DES, DH G1, MD5. Rekey Phase1 every 24 hours.
    c. IKE phase 2 proposal must include: AES128, ESP, DH G2, SHA1. Rekey Phase2 every 12 hours.
    d. Ensure that any traffic originated from the Trust zone of the Home Office can only reach the TRUST zone located in the Data Center and vice versa.
    e. Collect the IKE Phase2 security association’s management events in the kmd file on cluster1.
4) The VPN between srx7 and Cluster1 must meet following requirements:
    a. Validate peer reachability with DPD option. The keepalives should be sent to the neighboring peer regardless of traffic patterns every 10 seconds. Consider the peer unreachable if the number of DPD retransmissions exceeds 5 packets.
    b. IKE phase 1 proposal must include: preshared key “juniper”, 3DES, DH G5, SHA1. Rekey Phase1 every 24 hours.
    c. IKE phase 2 proposal must include: AES192, ESP, SHA1. Rekey IPsec tunnel on transmitting 5 MB of traffic.
    d. Ensure that only traffic originated from the FINANCE zone of srx7 can reach the Warehouse zone located in the Data Center and vice versa. This traffic must trigger tunnel establishment.
    e. Collect the IKE Phase2 security association’s management events in the kmd file on the cluster1.

© 2020 Juniper Networks, Inc. All rights reserved.

Task 2: Configuring Route-based VPN

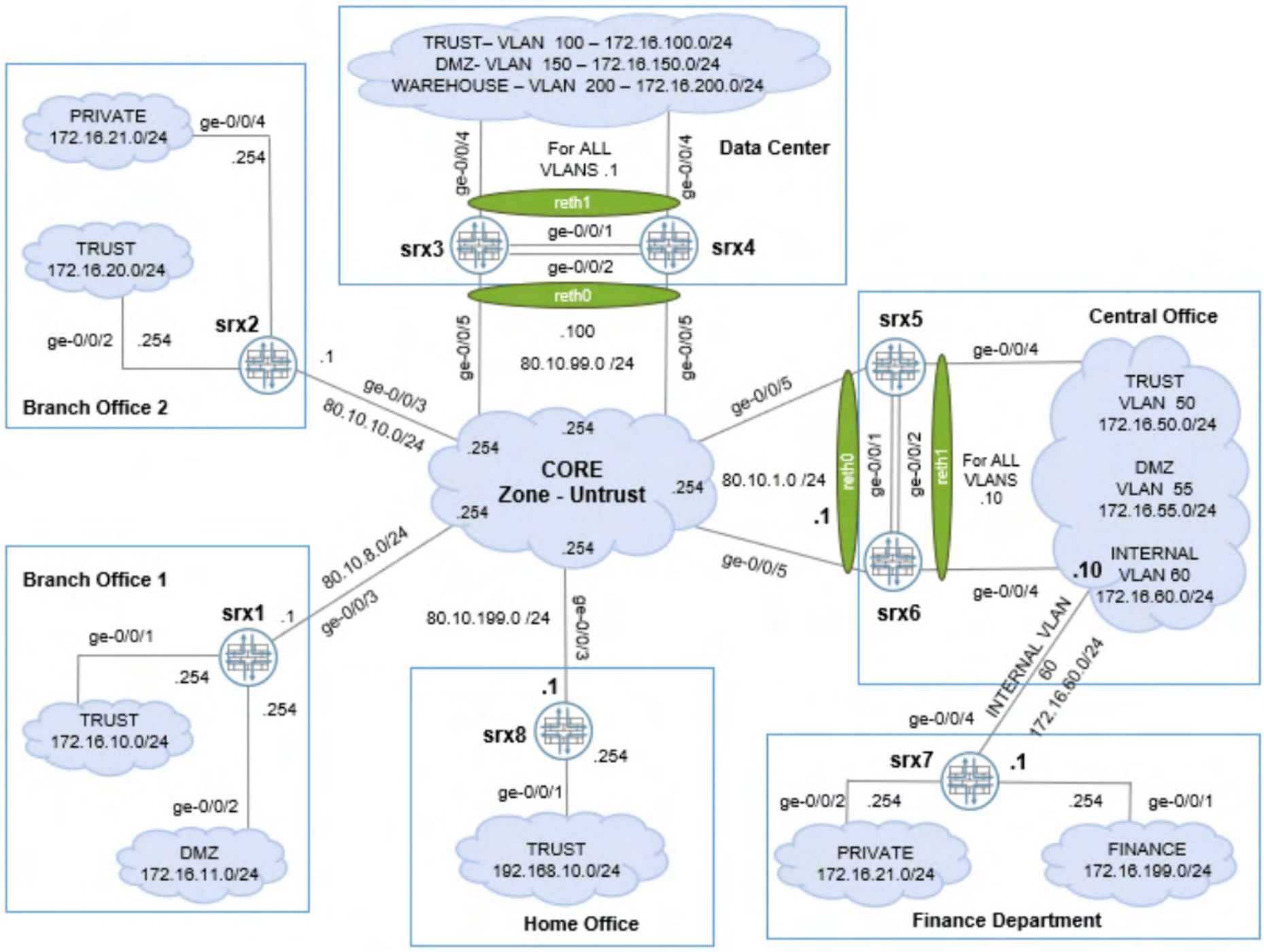


Figure 3: Chapter 5 – Task 2 Topology

In this part you will configure lab equipment as necessary to build full meshed route-based VPN between Central Office, Branch Office 1 and Branch Office 2.

© 2020 Juniper Networks, Inc. All rights reserved.

1) Branch offices have direct tunnel to each other and can communicate either directly or via the Data Center. The forwarding decision is done on the base of tunnel's state. Configure the interfaces on every device according to the table below, which reflects the topology image.

Device	Interface	IP address	VLAN-ID	Zone
srx1	st0.0	11.0.0.2/30	None	Untrust
srx1	st0.1	11.0.0.10/30	None	Untrust
srx2	st0.0	11.0.0.6/30	None	Untrust
srx2	st0.1	11.0.0.9/30	None	Untrust
Cluster2 (srx5, srx6)	st0.0	11.0.0.1/30	None	Untrust
Cluster2 (srx5, srx6)	st0.1	11.0.0.5/30	None	Untrust

Configure the IPsec VPN on every device according to the table below, which reflects the topology image.

Local Peer	Interface	Remote Peer	Interface
Cluster2	reth0.0	srx1	ge-0/0/3.0
Cluster2	reth0.0	srx2	ge-0/0/3.0
srx1	ge-0/0/3.0	srx2	ge-0/0/3.0

2) In this task's topology you will use OSPFv2 as the IGP routing protocol. The subnets located in the TRUST, PRIVATE, INTERNAL or DMZ zones must appear as OSPF internal routes on all devices in OSPF area 0, but no IGP adjacencies may be formed across interfaces located within these security zones. Ensure that traffic originated from any TRUST zone can reach any destination in the TRUST zone.

© 2020 Juniper Networks, Inc. All rights reserved.

Configure the interfaces on every device according to the table below.

Device	Interface	OSPF Area
srx1	st0.0	OSPF Area 0
srx1	st0.1	OSPF Area 0
srx1	ge-0/0/1.0	OSPF Area 0
srx1	ge-0/0/2.0	OSPF Area 0
srx2	st0.0	OSPF Area 0
srx2	st0.1	OSPF Area 0
srx2	ge-0/0/2.0	OSPF Area 0
srx2	ge-0/0/4.0	OSPF Area 0
Cluster2 (srx5, srx6)	st0.0	OSPF Area 0
Cluster2 (srx5, srx6)	st0.1	OSPF Area 0
Cluster2 (srx5, srx6)	reth1.50	OSPF Area 0
Cluster2 (srx5, srx6)	reth1.55	OSPF Area 0
Cluster2 (srx5, srx6)	reth1.60	OSPF Area 0

3) The VPN between srx1 and Cluster2 and between srx2 and Cluster2 must meet the following requirements:
   a. Rekey IPsec tunnel every 8 hours.
   b. Validate data path with VPN monitor option. The keepalives should be sent to the neighboring peer regardless of traffic patterns with 5 sec intervals. It is allowed to miss only three consecutive keepalives after which the tunnel is considered inactive.
   c. IKE phase 1 proposal must include: preshared key “juniper”, AES128, DH G2, SHA.
   d. IKE phase 2 proposal must include: AES256, ESP, SHA1.
   e. Ensure that in case of one tunnel’s failure traffic originated from the TRUST security zone of any site still can reach other site’s protected resources.

4) The VPN between srx1 and srx2 must meet the following requirements:
   a. Rekey IPsec tunnel on transmitting 100 MB of traffic.
   b. Validate data path with VPN monitor option. The keepalives should be sent to the neighboring peer only in absence of traffic patterns.
   c. IKE phase 1 proposal must include: preshared key “juniper”, 3DES, DH G2, MD5.

© 2020 Juniper Networks, Inc. All rights reserved.

d. IKE phase 2 proposal must include: AES256, ESP, SHA1.
e. Ensure that in case of one tunnel's failure traffic originated from the TRUST security zone of any site still can reach other site's protected resources.

Task 3: Configuring GRE-tunnel over Route-based VPN

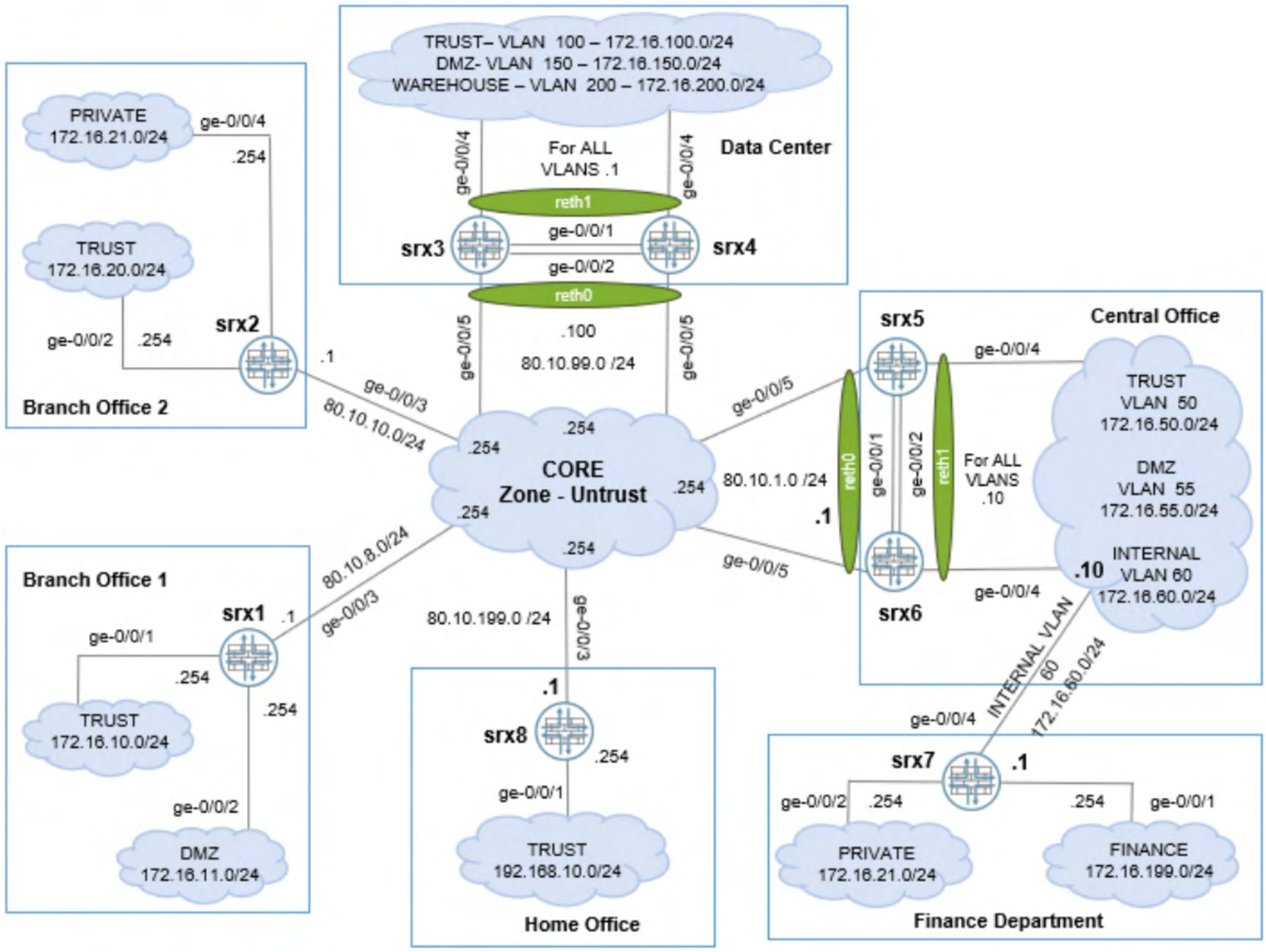


Figure 4: Chapter 5 – Task 3 Topology

In this part you will configure the lab equipment as necessary to build GRE-tunnel over route-based VPN between Branch Office 1 and Branch Office 2.

© 2020 Juniper Networks, Inc. All rights reserved.

1) Configure the interfaces on every device according to the table below.
The GRE tunnel source should be configured as device's local lo0 interface address and the destination should be configured as remote device's lo0 interface address.

Device	Interface	IP address	VLAN-ID	Zone
srx1	gr-0/0/0.0	11.11.11.1/30	None	Untrust
srx1	lo0.0	192.168.1.1/32	None	Untrust
srx2	gr-0/0/0.0	11.11.11.2/30	None	Untrust
srx2	lo0.0	192.168.1.2/32	None	Untrust

2) Configure the interfaces on every device according to the table below.
The GRE tunnel source should be configured as device's local lo0 interface address and the destination should be configured as remote device's lo0 interface address.

Device	Interface	OSPF Area
srx1	gr-0/0/0.0	OSPF Area 0
srx2	gr-0/0/0.0	OSPF Area 0

3) Ensure that any traffic originated from the TRUST zone of Branch Office 1 can reach the TRUST zone of the Branch Office 2 vice versa.

© 2020 Juniper Networks, Inc. All rights reserved.

Task 4: Configuring ADVPN

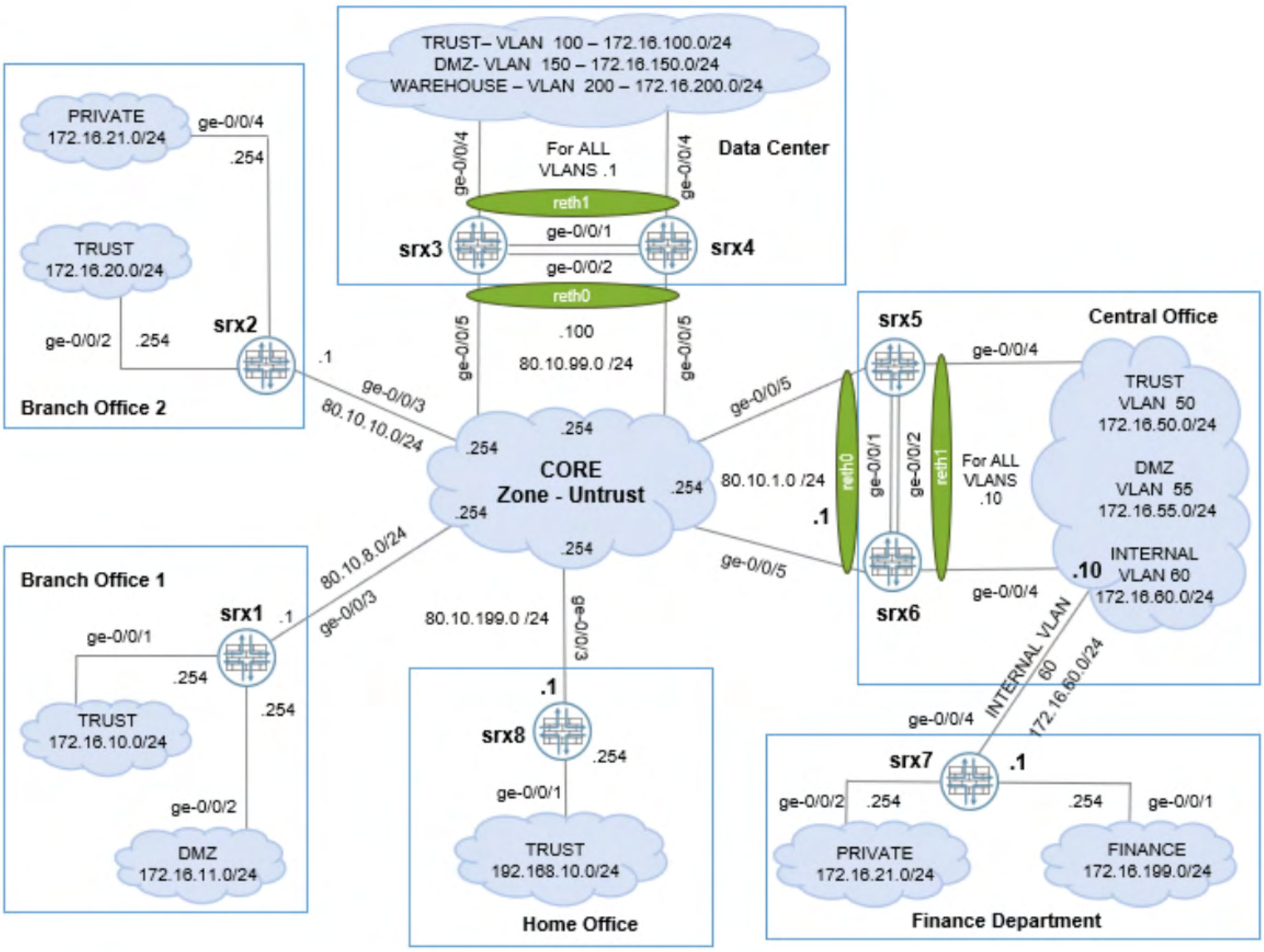


Figure 5: Chapter 5 – Task 4 Topology

Note: Please make sure to load the Chapter 5 initial configurations for SRX1, SRX2, cluster SRX5/6 and the vr-device.

1) Configure an ADVPN between the Central Office, Branch Office 1 and Branch Office 2. Inter-Branch traffic should not have to traverse the Central Office. The certificates are already loaded on the devices.
2) Only allow ping between the TRUST zones of each site.

© 2020 Juniper Networks, Inc. All rights reserved.

Chapter 6: NAT

This chapter is focused on different NAT implementations. You will configure source NAT, destination NAT, static NAT and IPv4/IPv6 protocol translation.

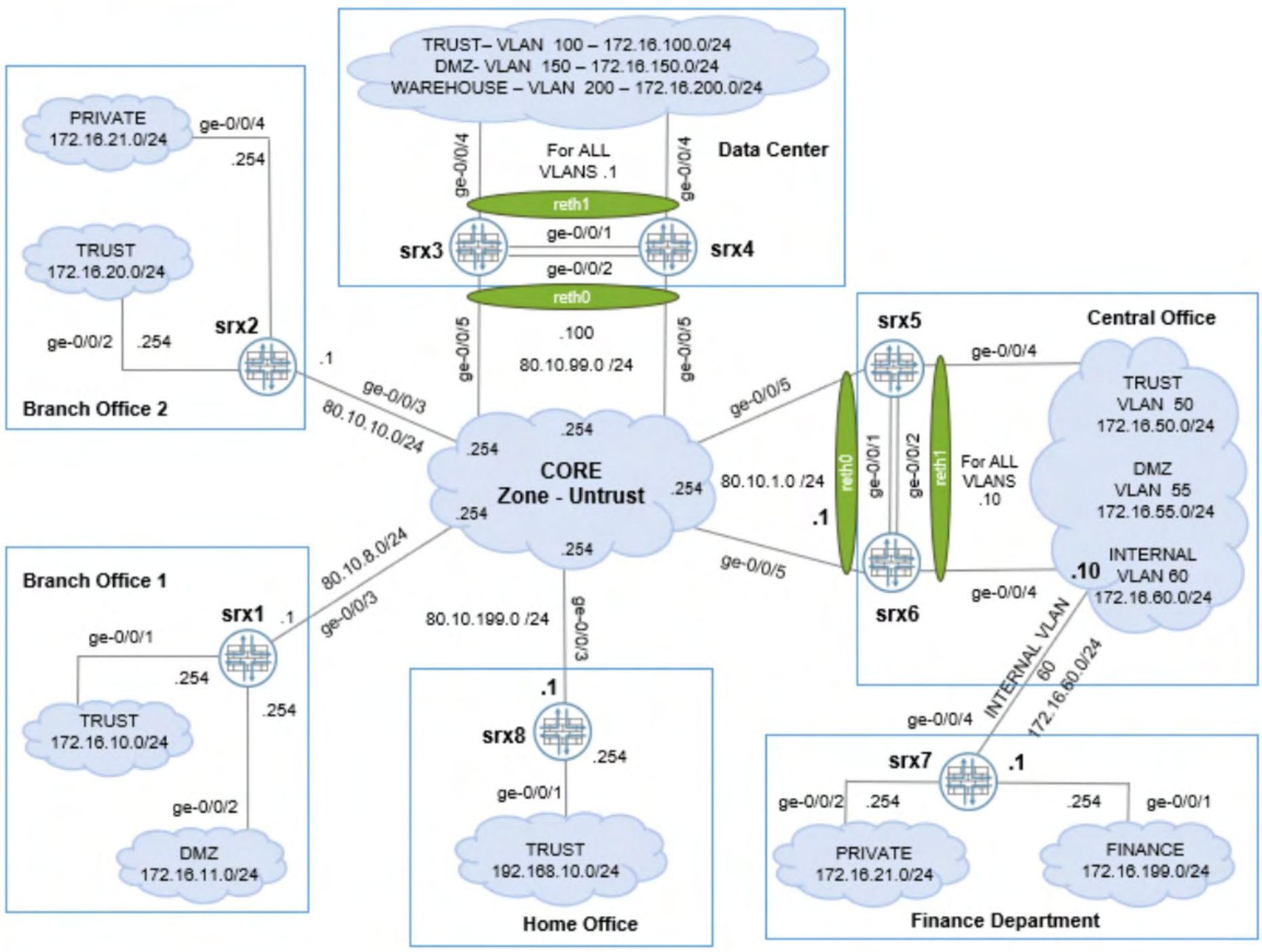


Figure 1: Chapter 6 Topology

You can continue with the configuration if you have completed tasks from the previous chapter. OR load the latest initial configurations for this chapter to the devices. If you have already loaded the chapters configuration for the vr-device previously you don't have to do it again.

Note: The labs starting point requires to have SRX clusters formed between devices srx3 – srx4 and srx5 – srx6 and the respective configuration loaded on them. Please note that a reboot might be required for the devices to be placed into cluster mode.
Tip: Ensure you read this entire chapter, before starting with the first task.

© 2020 Juniper Networks, Inc. All rights reserved.

Task 1: IPv4 Source NAT

In this part you will configure source NAT on srx1, srx2 and srx8 as necessary to enforce listed scenarios between private and public IP addresses.

Home office: srx8

1) The hosts located in Home Office are using IP addresses from the subnet 192.168.10.0/24, which is a non-routable prefix in the Core network. Configure srx8 that any host located in the TRUST zone in the Home office can reach all IP routable prefixes in the Core network.
2) Ensure IP addresses and ports translation mappings are maintained for 1 hour after the sessions are closed. The external hosts can reach the internal hosts by using their reflexive IP address only when they previously have received packet(s) from the internal host.

Branch office 1: srx1

3) Configure srx1 to apply NAT to all sessions originated in the network 172.16.10.0/24 and destined to any routable prefixes in the Core network. Also, to all sessions originated in the network 172.16.11.0/24 and destined to prefixes associated with Data Center and Central office core facing subnets.
4) For sessions originating in the network 172.16.10.0/24 ensure that:
    a. The public range 80.10.8.16/28 is used for address translation if a session is going from TRUST to UNTRUST zone. PAT is not allowed.
    b. If pool of IP addresses is exhausted the egress interface's IP address must be used for translation.
    c. Private IP addresses 172.16.11.201 – 172.16.11.206 are used for address translation if session goes from TRUST to DMZ zone. PAT is allowed.
5) For sessions originated in the network 172.16.11.0/24 ensure that:
    a. The public range 80.10.8.64/27 is used for address translation if a session goes from DMZ to UNTRUST zone. PAT is allowed.
    b. Private IP addresses 172.16.10.97 – 172.16.10.110 are used for address translation if session originates in the DMZ and goes to the TRUST zone. PAT is not allowed.
    c. If the pool of IP addresses is exhausted the egress interface's IP address must be used for translation.
    d. Ensure that multiple concurrent sessions from the same host always use the same IP address.

© 2020 Juniper Networks, Inc. All rights reserved.

Branch Office 2: srx2

6) On srx2 the source NAT should be applied to sessions originated either in the PRIVATE or TRUST zones having the source IP addresses from ranges of 172.16.21.16 – 172.16.21.71 and 172.16.20.200 - 172.16.20.209 and are destined to any addresses from the 80.10.0.0/16 address range. For translation use the IP addresses from the subnet 80.10.10.128/25.
7) Ensure the same internal host from one of the ranges above always uses the same public IP address for outgoing sessions.
8) Ensure that all remaining connections will always be translated to the IP address of the egress interface.

Task 2: IPv4 Destination NAT

In this part you will configure cluster1 as necessary to provide access to resources located in the TRUST, DMZ and WAREHOUSE zones in the Data Center.

Data center: cluster 1

1) There are two public addresses used to provide access to the protected resources in the Data Center network – 80.10.99.101 and 80.10.99.102.
2) The IP address 80.10.99.101 should be mapped to the IP address 172.16.100.1 located in the TRUST zone. PAT is not allowed. Ensure that only sessions initiated from IP addresses associated with Branch and Home Offices 1 and 2 are translated by NAT.
3) The IP address 80.10.99.102 should be mapped to the IP addresses in the DMZ, TRUST and WAREHOUSE zones based on conditions defined in the table below:

Public IP address	Public port number	Private IP address	Private port number
80.10.99.102	21	172.16.100.1	21
80.10.99.102	23	172.16.150.1	23
80.10.99.102	8080	172.16.200.1	80

4) Ensure that all not translated IP packets destined to the 80.10.99.101 and 80.10.99.102 IP addresses are dropped.
5) Ensure that all packets destined to the TRUST zone's resources look as they are originated from the cluster1 itself.

© 2020 Juniper Networks, Inc. All rights reserved.

Task 3: IPv4 Static NAT

This section is dedicated to static NAT configuration. You need to configure cluster2 and srx7 to allow bidirectional NAT translations for some of the protected resources located in the following sites.

Central office: cluster 2

1) Using the cluster 2 ensure the rest of the enterprise network (connecting through the Core network) sees the srx7 loopback address as 80.10.1.11. Srx7 must be able to initiate and accept sessions to/from other security devices in the Core network.
2) The range of IP addresses 80.10.1.128/29 must be mapped to the similar range of IP addresses in the DMZ zone, e.g. to 172.16.55.128/29.

Finance department: srx7

1) On srx7 the 172.16.21.0/26 subnet from the PRIVATE zone and the 172.16.199.0/26 subnet from the FINANCE zone should be hidden from the rest of the corporate network. For access to and from these networks the IP addresses from the range 172.16.60.128/25 have to be used. The mapping should employ shifting and start at 172.16.60.128 <--> 172.16.21.0.
2) Ensure that all IP packets with untranslated destination IP addresses will be dropped.

Task 4: NAT Protocol Translation (IPv6/IPv4)

This section focuses on enabling IPv6 and IPv4 hosts to communicate with each other by using NAT.

Branch 2

1) Ensure that IPv6 users attached to the PRIVATE zone in Branch2 can reach the IPv4 host 80.10.10.100 by sending and receiving traffic from IPv6 address: 2001:a11::253. Modify or change your (existing) policies to allow traffic between the hosts
2) Ensure that IPv4 host 80.10.10.254 can reach IPv6 host 2001:a11::1 by sending and receiving traffic from IPv4 address 80.10.10.2 Modify or change your (existing) policies to allow traffic between the hosts

© 2020 Juniper Networks, Inc. All rights reserved.

Chapter 7: Attack Prevention and Mitigation

This chapter is dedicated to the Attack Prevention and Mitigation functionality on Junos security devices. The presented tasks will require you to configure stateless packet filtering, SCREEN functionality and Intrusion Prevention System features set.

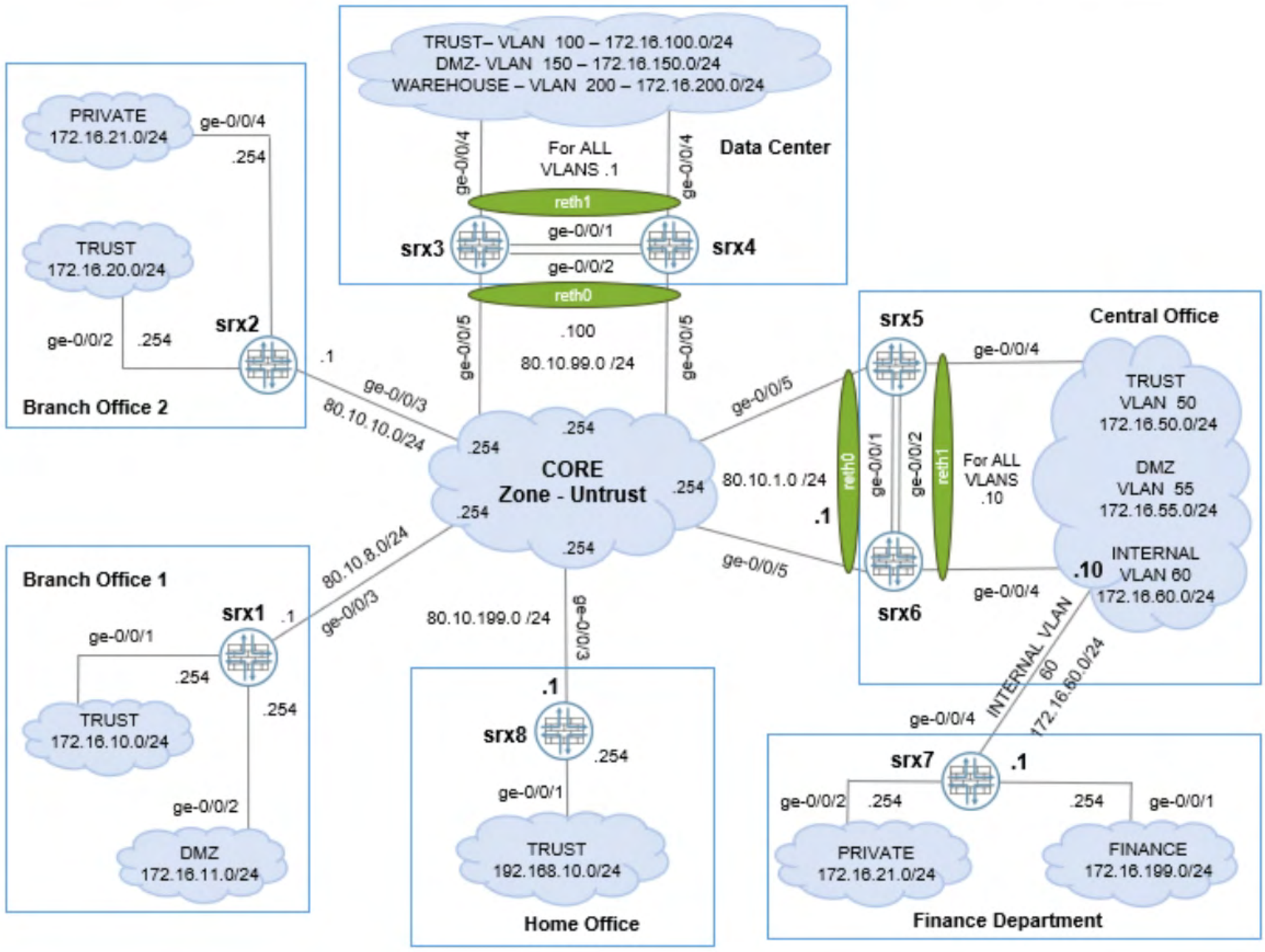


Figure 1: Chapter 7 Topology

You can continue with the configuration if you have completed tasks from the previous chapter. OR load the latest initial configurations for this chapter to the devices. If you have already loaded the chapters configuration for the vr-device previously you don't have to do it again.

Note: The labs starting point requires to have SRX clusters formed between devices srx3 – srx4 and srx5 – srx6 and the respective configuration loaded on them. Please note that a reboot might be required for the devices to be placed into cluster mode.
Tip: Ensure you read this entire chapter, before starting with the first task.

© 2020 Juniper Networks, Inc. All rights reserved.

Task 1: Firewall Filters

1) In this part you will configure stateless packet filters on all security devices in the lab. The goal of this task is to protect every security device's control plane from malicious traffic by applying Firewall Filters to devices loopback interfaces.
2) Ensure that IPsec tunnels can be established for all security devices in the network regardless if they are located in front of or behind NAT devices. All security devices are using ESP as an IPsec protocol.
3) Ensure that OSPF protocol is permitted for of the range of IP addresses allocated for tunnel interfaces.
4) Permit DNS on UDP port 53 and NTP traffic originated from the management network 10/8. Also permit the NTP from the address 10.10.1.254.
5) Permit SNMP, RADIUS, HTTP/HTTPS, telnet, SSH and FTP traffic originated from the out-of-band management network 10/8.
6) Permit ping packets regardless of the source IP address.
7) Ensure that FTP and HTTP traffic is rate limited to 1 Mbps with the allowed traffic burst of 100 KB.
8) Silently drop and syslog all other traffic.

Task 2: SCREEN

In this part you will configure lab equipment as necessary to protect network recourses of Branch offices, Finance department and Home office from different types of reconnaissance and DoS attacks with the SCREEN feature.

Branch office 1, Branch office 2, Home office: srx1, srx2 and srx8

Configure functionality on srx1, srx2 and srx8 to protect sites from malicious traffic arriving from the Core network:

1) Ensure that the SYN Proxy mechanism is enabled.
2) Protect against session table flood with the thresholds of 250 sessions per source and per destination IP addresses.
3) Configure protection against TCP SYN segments flood with the following thresholds and timer values:
    a. The destination thresholds values of 5000 TCP SYN segments per second.
    b. Ensure that security device starts SYN Proxy protection mechanism when TCP SYN segments arrival rate reaches 500 segments per second.
    c. Ensure that security device generates an alarm when TCP SYN segments arrival rate reaches 7000 segments per second.
    d. The maximum time before incomplete sessions are dropped should be 10 seconds.
4) Protect against ICMP flood with the threshold of 500 packets per second.
5) Ensure that security device drops packets with following abnormalities:

© 2020 Juniper Networks, Inc. All rights reserved.

a. Fragmented ICMP packets.
b. Fragmented TCP SYN segments.
c. ICMP packet with size larger than 1024 bytes.

Finance department: srx7

Configure srx7 to protect site from reconnaissance attempts arriving from the INTERNAL zone:

6) Ensure that detection of malicious traffic results in alarm generation instead of dropping the packets belonging to malicious packet flow.
7) Protect against IP addresses sweeps with a detection rate of 10 ICMP packets arrived per 500 ms time interval.
8) Protect against port scans with a detection rate of 10 port scans per 750 ms time interval.
9) Detect IP packets with following values in the Options field:
    a. Time stamp option
    b. Record route option
10) Protect against following operating systems probes:
    a. The TCP segment has both SYN and FIN flags set.
    b. The TCP segment has no flags set.

Task 3: Intrusion Prevention System

In this part you will configure lab equipment as necessary to deploy Intrusion Prevention System features in the Data Center and Central office.

Data Center: cluster1

There are several servers located in different zones in the Data Center network (see the table below). Services that are not mentioned in this table or in the following configuration tasks must be restricted by the security policies.

Security zone name	Services
TRUST	SMTP, POP3, IMAP
DMZ	HTTP, SMTP, POP3, IMAP, FTP
WAREHOUSE	HTTP

1) Configure cluster1 to use the TCP SYN cookie rather TCP SYN proxy mechanism.
2) Protect the Data Center resources with the predefined IDP policy “Recommended”. Ensure that only specified services are monitored for traffic traversing between the Data Center protected resources and Untrust zone.

© 2020 Juniper Networks, Inc. All rights reserved.

3) Ensure that all the Data Center resources are protected against TCP/IP attacks and malware activities from the Untrust zone as well as internal servers can't cause infection or be the source of attacks to any hosts located in the Untrust zone.
4) Allow anonymous access from Untrust zone to the FTP servers 172.16.150.1 and 172.16.150.2 only from the 80.10.1.128/29 range. Restrict access for the rest of the hosts located in the Untrust zone. Silently drop packets from unauthorized hosts, block them for 1 hour and generate log messages with severity level Major and alert flag.

Central office: cluster2

There are two servers located in the DMZ security zone in the Central office network (see table below). Services that are not mentioned in this table or in following configuration tasks must be restricted by security policies.

Server's IP address	Services
172.16.55.100	HTTP
172.16.55.200	FTP

5) Configure Cluster2 to use the TCP SYN cookie rather than the TCP SYN proxy mechanism.
6) Protect the Web and the FTP servers from any kind of HTTP or FTP attacks respectively with the severity level Critical or Major from everywhere. Silently drop session in the case of attack's detection, generate syslog message with the alert flag and block attacker's future connection attempts for two hours.
7) Upload of zip, rar or tgz files to the FTP server is prohibited from anywhere. Each detected attempt results in disconnecting the client from the server by receiving with TCP RST message. The client is blocked for next five minutes. The syslog message with the severity level Major must be generated. Clients located in the TRUST and in the INTERNAL zones are permitted to access servers located both in the UNTRUST zone and in the DMZ zone.
8) Ensure that client's machines located in the TRUST security zone are protected against worms and Trojans types of attacks of all severity levels from anywhere as well as they can't cause infection or be the source of attack for any hosts located in DMZ and INTERNAL security zones.
9) Clients are instantly denied access to the following URLs:
    a. www.instagram.com
    b. www.flickr.com

    The connection must be closed when such attempt is detected.
10) The downloading of pdf files via HTTP is prohibited for users located in the TRUST zone. If such attempt has been detected the connection has to be closed.

© 2020 Juniper Networks, Inc. All rights reserved.

Chapter 8: Extended Implementation Concepts

This chapter is focused on two features of JUNOS Security kit: Transparent mode and Filter Based Forwarding. The presented scenarios require you to reconfigure security devices srx1 and srx7 according to picture below.

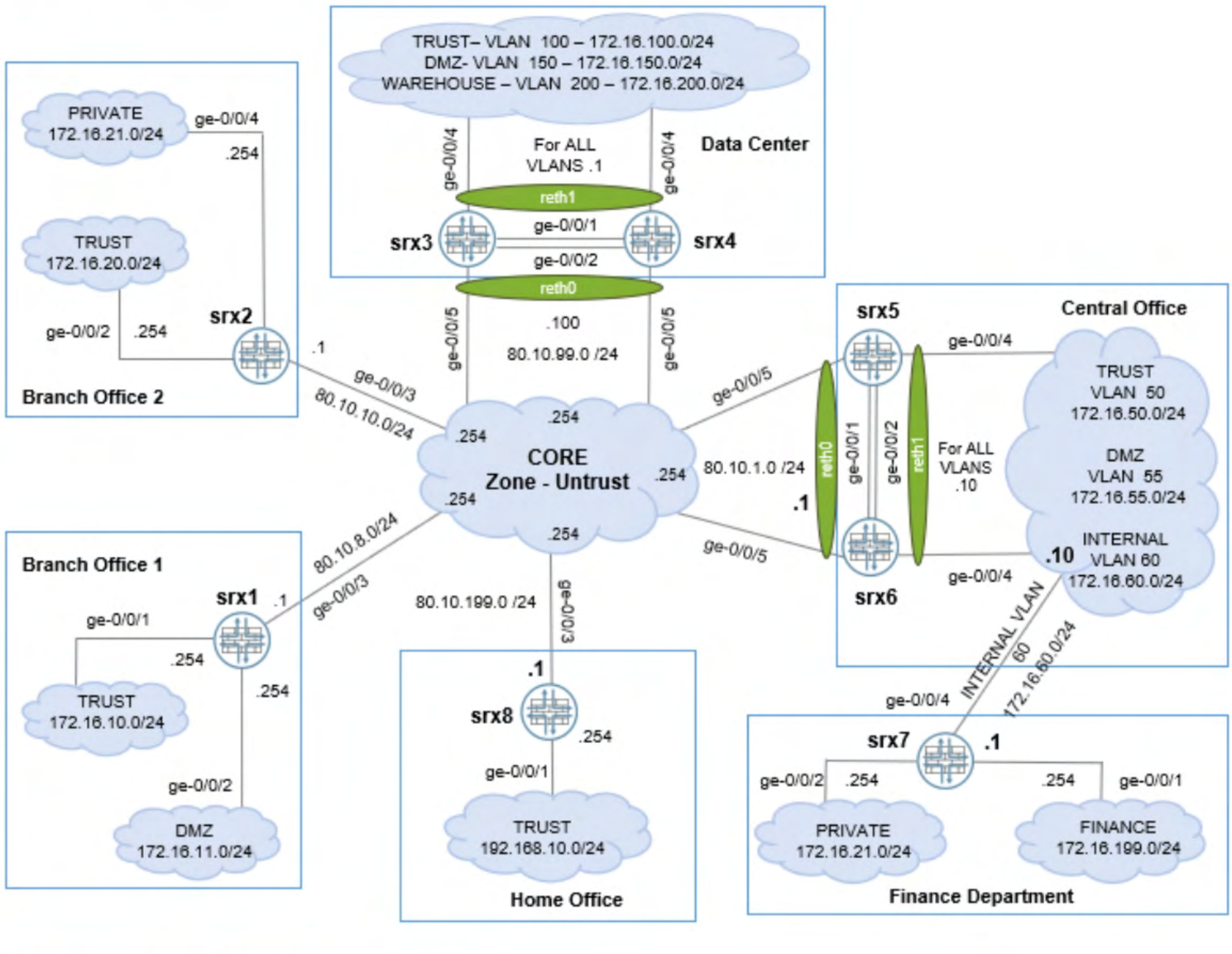


Figure 1: Chapter 8 Topology

Please load the chapter 8 starting configurations on all devices when starting this lab.

Note: In case you have loaded the chapters configuration for the vr-device you don't have to do it again.

Tip: Ensure you read this entire chapter, before starting with the first task.

© 2020 Juniper Networks, Inc. All rights reserved.

Task 1: Transparent Mode

In this section you need to configure Home office's security device in such that srx1 will make forwarding decisions based on MAC address rather than on the base of IP header's information.

1. Configure the interfaces, bridge domain and security zones on the srx1 according to the table below, which reflects the topology image.
   Rewrite vlan-id 81 with the vlan-id 80 on the trunk port ge-0/0/5.0.

Interface	IP address	Interface mode	VLAN-ID	Zone
ge-0/0/4.0	N/A	Access	80	TRUST
ge-0/0/5.0	N/A	Trunk	81	DMZ
ge-0/0/3.0	N/A	Access	80	UNTRUST
Fxp0	80.10.8.5/24			N/A

2. Configure static default route pointing to the IP address 80.10.8.254.
3. The hosts from the TRUST zone and its network range can go to the outside network (Internet) with HTTP and HTTPS.
4. Ensure the hosts from the TRUST zone have access to the whole private corporate network (reachable via CORE network) with any application.
5. Devices in the DMZ zone should be accessible from the whole private corporate network including the local TRUST zone with HTTPS.
6. No other connections are allowed to go in or out of the TRUST zone.
7. No connections are allowed to go out from DMZ zone. Log all violations going out to the CORE network.

Task 2: Filter Based Forwarding

In this section you need to configure Finance department's security device in such that srx7 will forward packets originated from PRIVATE and FINANCE zones on the based-on criteria other than destination IP address.

There are two network paths to the Core network available in the Finance department. One path is direct connection to the Core network via interface ge-0/0/3.0. Another path leads to the Core network via the Central office network and is formed on the base of interface ge-0/0/4.60.

1. Configure srx7 to send HTTPS traffic originated either from the PRIVATE or from the FINANCE zone and destined to the prefix 80.10.99.0/24 is forwarded via interface ge-0/0/3.0. All other traffic should be forwarded via interface ge-0/0/4.60
2. Ensure that asymmetric traffic forwarding is not possible.

© 2020 Juniper Networks, Inc. All rights reserved.

Chapter 9: Advanced Services

This chapter is focused on the configuring advanced security and management features.

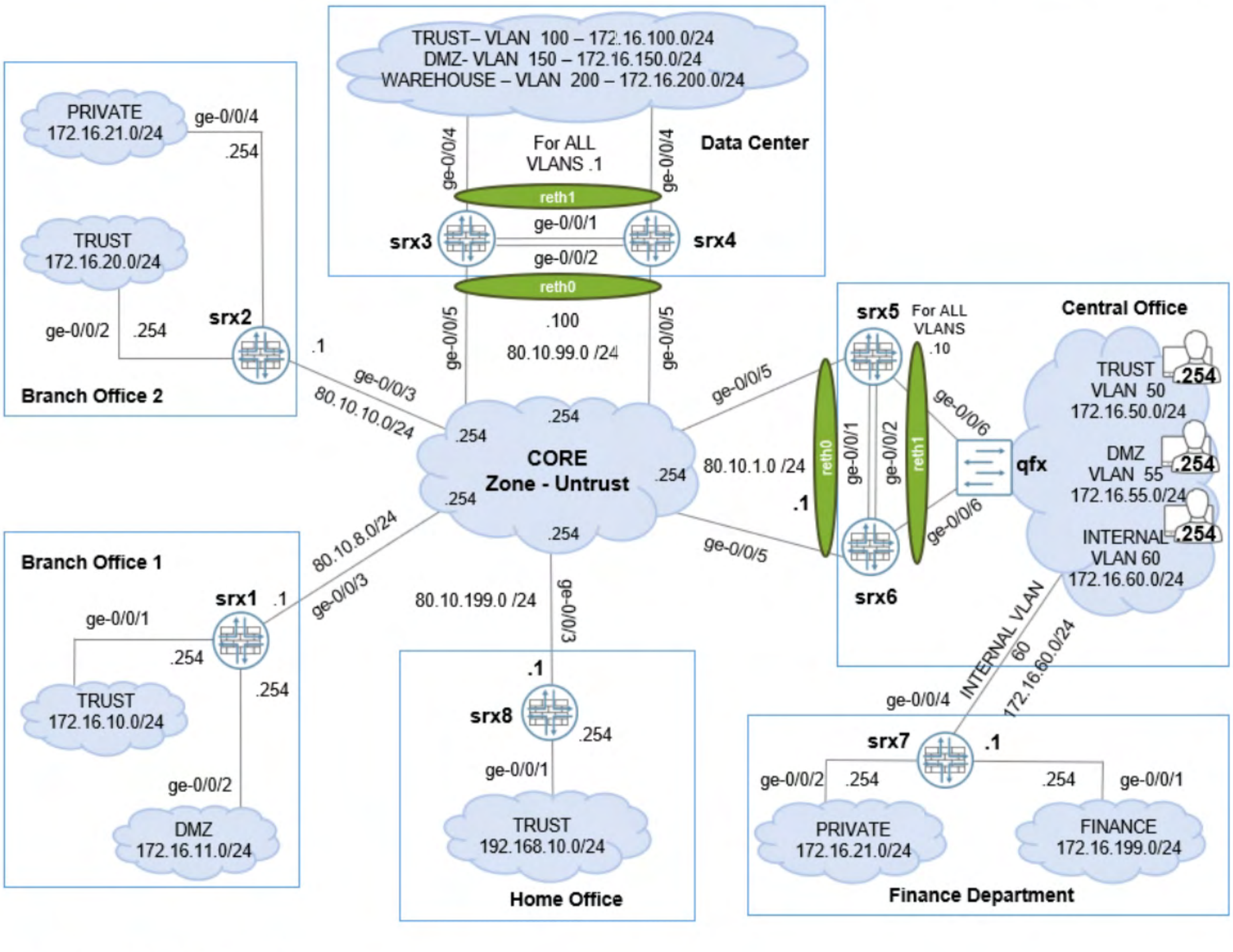


Figure 1: Chapter 9 Topology

Please load the chapter 9 starting configurations on all devices when starting this lab.

Note: In case you have loaded the chapters configuration for the vr-device you don't have to do it again.

Tip: Ensure you read this entire chapter, before starting with the first task.

© 2020 Juniper Networks, Inc. All rights reserved.

Task 1: Application Identification

In this section you will configure application identification on cluster 1.

Data center: cluster 1

1) Ensure the result of application identification is kept for at least 2 hours.
2) The updates have to be downloaded automatically starting from current day at 23:30 with the interval of 24 hours.
3) Allowed encrypted Gmail traffic from the DMZ zone to the UNTRUST zone.
4) Ensure the firewall generates a message when the session has been denied.

Task 2: AppTrack

Here you will configure the cluster 1 to perform application tracking in the required manner.

Data center: cluster 1

1) Deep insight is required into what applications are used by the employees in the TRUST zone. Use AppTrack to satisfy this requirement. Configure it to generate the 1st message immediately when the application is identified and then to send updates every 10 minutes. Have these messages kept together with the security policy logs?

Task 3: AppQoS

This section contains requirements about QoS handling where the device utilizes the knowledge about applications used in the traffic.

Data center: cluster 1

1) Ensure the loss-priority is set to high for the junos:GMAIL application from the DMZ to UNTRUST zone if it crosses 50000kb/s with bursts of 312kB in the server to client direction. In addition, have also the DSCP bit changed for the junos:GMAIL application to value of 101110 (the "ef" dscp code point alias).

© 2020 Juniper Networks, Inc. All rights reserved.

Task 4: SSL Proxy

In here you will configure the cluster 1 to dive deeper and inspect also encrypted sessions.

Data center: cluster 1

1) Ensure the firewall has deep insight into encrypted sessions over the port 443 from users in the TRUST zone to the UNTRUST zone. The certificate for signing the modified server certificates should generated locally on the SRX device with following values:
    a. type: rsa
    b. key size: 1024
    c. domain name: juniper.net
    d. subject: DC=Juniper,CN=Juniper,OU=unit-1,O=Juniper,SN=1234,L=Sunnyvale,ST=US,C=US
    e. email-ID: noreply@juniper.net
2) The connections to www.junosgenius.net, www.juniper.net and www.gmail.com should be excluded from this en/decryption processing.
3) Enable logging for the allowed sessions and have it sent to the "ssl-proxy" file.

Task 5: Juniper Identity Management Service (JIMS)

1) Configure Juniper Identity Management Service to be able to identify network traffic on cluster 1 based on IP address as well as user and device context. Implement your solution for authenticated, unauthenticated and unknown users in the TRUST to UNTRUST zone for traffic destined towards the corporate-networks.

Task 6: Security Logging

1) Cluster1 device should be sending its security logs to the Security Director located at 10.10.1.99 (integrated log collector). Enable logging for at least one policy for the TRUST to UNTRUST zone
2) Ensure a daily report is send to noreply@juniper.net that shows all anomalies for policies that are applied before device specific policies. The SMTP server is located at: 10.10.1.254

© 2020 Juniper Networks, Inc. All rights reserved.

Task 7: Software Defined Secure Network (SDSN)

1) Create a new SkyATP realm. Enroll Policy Enforcer and the central office cluster in the newly created Sky ATP Realm through Security Director

   Use the information below to setup the Sky ATP Realm:

SkyATP Realm	jnciesec-xxx (where xxx is shown in the lab access instructions)
Username	jnciesec-xxx@stu.juniper.net
Password	lab123@Lab
Juniper SSO account	eduservicenow@gmail.com
Juniper SSO password	********

   Use the information for Security Director and Policy Enforcer:

Security Director Username	super
Security Director Password	lab123@Lab
Security Director IP	10.10.1.100
Policy Enforcer Username	root
Policy Enforcer Password	lab123@Lab
Policy Enforcer IP	10.10.1.123

   Note: The password for the Juniper SSO account is auto populated in the Firefox browser on the Student Desktop. For this reason, it is important to use the Firefox browser on the Student Desktop to create the Sky ATP realm

2) Setup for SkyATP with SDSN in Security Director, ensure that HTTP and SMTP traffic is analyzed at cluster 2 (srx5/srx6) for threat levels above 7 for the 172.16.50.100 host. Ensure that connections are silently dropped at access switch vQFX if the 172.16.50.100 host becomes infected with malware. Ensure that only blocked traffic is logged.
3) Ensure that content received by the 172.16.50.100 host from IP address “8.8.8.8” is never classified as Malware, however content from IP address “176.74.246.24” is always blocked.
4) Ensure that (suspicious) emails are sent to SkyATP for inspection for the 172.16.50.100 host. Suspicious emails should always be delivered with the email subject prepended with “SPAM”, however the email header should not be tagged with additional spam identifiers. Ensure that email received from no-reply@juniper.net are excluded from inspection.
5) Block all traffic to and from the Netherlands for the 172.16.50.100 host.

© 2020 Juniper Networks, Inc. All rights reserved.

Super Lab 1

This lab is designed to combine many of the solutions discussed in the previous chapters into a complete practice lab exam. This lab is similar to a real JNCIE-SEC lab exam experience. We recommend attempting this lab if you are able to complete the tasks in the previous chapters without any help.

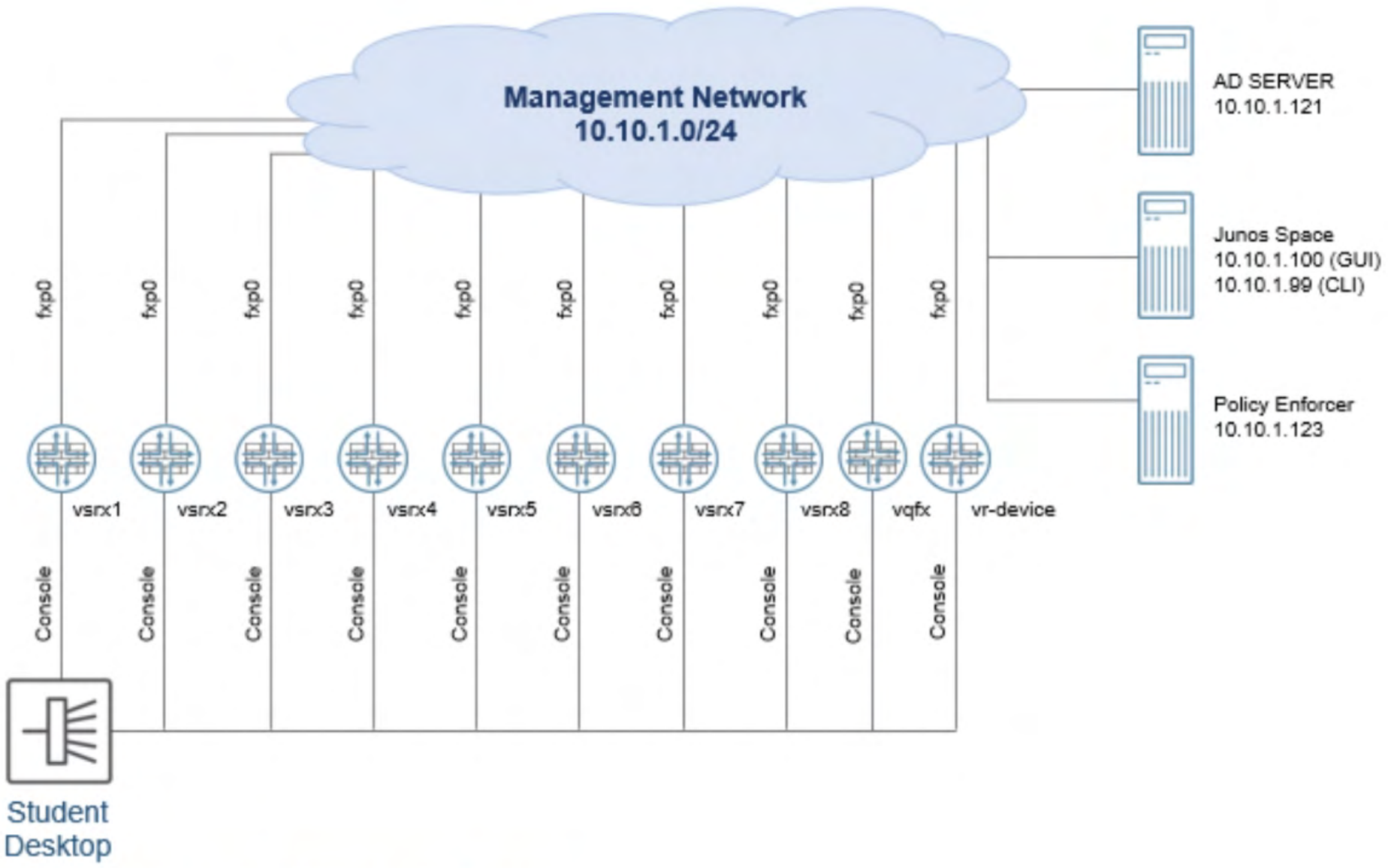


Figure 1: Super Lab 1 – Management Topology

Ensure you load the initial configurations on the devices before you start with this LAB. Ensure that you do not forget to load the initial Super Lab 1 configuration on the vr-device.

Tip: Ensure you read whole tasks before starting them.

© 2020 Juniper Networks, Inc. All rights reserved.

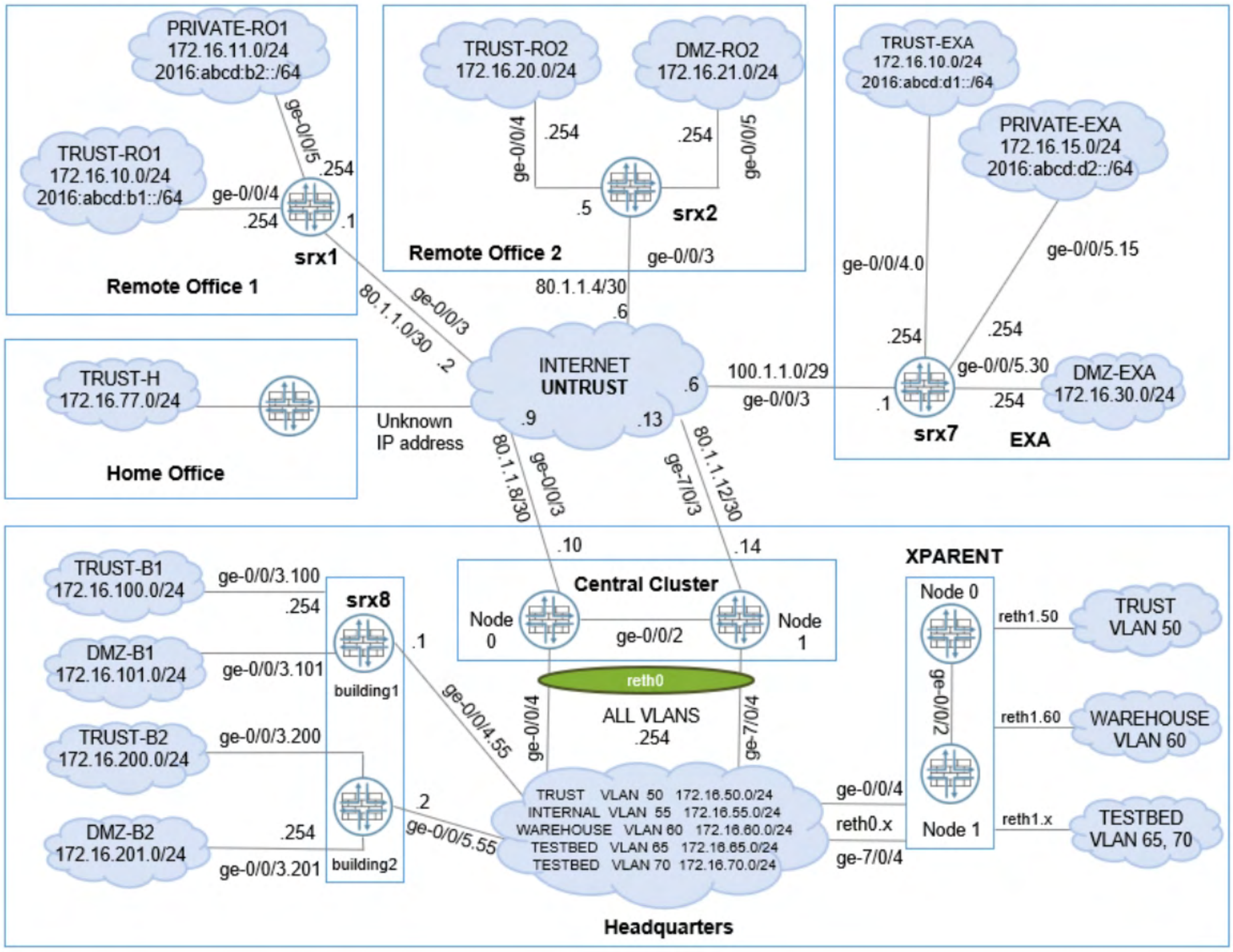


Figure 2: Super Lab 1 Topology

© 2020 Juniper Networks, Inc. All rights reserved.

Task 1: Initial Configuration - Part 1

In this part you will configure the device hostnames, high-availability (cluster) and management interfaces.

1) The table below lists the device hostnames mapping:

Device	Hostname
srx1	roffice1
srx2	roffice2
srx3	central-node0
srx4	central-node1
srx5	xparent-node0
srx6	xparent-node1
srx7	exa-fw
srx8	building

2) Create clusters as defined in the following table:

Device	Node ID	Cluster ID
central-node0	0	1
central-node1	1	1
xparent-node0	0	2
xparent-node1	1	2

3) Ensure ge-0/0/2 is used for the fabric link.
4) The routing engine of xparent cluster needs to be active on node 0.
5) Configure the redundant ethernet interfaces according the figure 2.
6) Clusters should operate in the following manner:
    a. Central cluster redundancy groups mapped to interfaces dependent on physical links, need to be active on node0 whenever node0 is available
        i. Any failure from correspondent child interface triggers the failover
    b. Central cluster redundancy groups (RGs) mapped to interfaces dependent on logical links, need to be active on node1 whenever node1 is available
        i. Uplink interface monitoring triggers the failover
    c. The Central Cluster needs to monitor ICMP reachability to the host address (12.34.56.78) available in the Internet. In case this reachability is

© 2020 Juniper Networks, Inc. All rights reserved.

compromised, the test's uplink interface should be brought down so that the RG fails over.

i. Probe threshold should be between 30 and 60 seconds
ii. Control plane redundancy group needs to follow the same faith of the RG from point 6.b

d. All xparent cluster redundancy groups need to be active on node 0 and should automatically failover in case any of its physical links fail.
   i. No need for automatic recovery of primacy

7) Configure the management interfaces as defined in the table below:

Device	Management IP address
roffice1	10.10.1.1/24
rooffice2	10.10.1.2/24
central-node0	10.10.1.3/24
central-node1	10.10.1.4/24
xparent-node0	10.10.1.5/24
xparent-node1	10.10.1.6/24
exa-fw	10.10.1.7/24
building	10.10.1.8/24

8) Ensure the management interfaces:
   a. Will accept only specific services as defined in the table below.

Device	Services
roffice1	SSH with root access (session limit 3), HTTPS
rooffice2	SSH with root access (session limit 3), HTTPS
central	SSH with root access (session limit 3), HTTPS
xparent	SSH with root access (session limit 3), HTTPS
building	SSH with root access (session limit 3), HTTPS
exa-fw	SSH with root access (session limit 3), HTTPS

© 2020 Juniper Networks, Inc. All rights reserved.

Task 2: Initial Configuration - Part 2

In this part you will configure authentication, authorization, Syslog, SNMP and NTP parameters.

1) Configure users as defined in the table below:

Username	Password	Device	Privileges
ronly	ronly123	All	Has permission “view” and “view-configuration”. Additionally, can NOT execute the “file delete” command and view the [edit system login] configuration hierarchy.
admin1	admin123	All	Has permissions “all”. But is not allowed to reboot the device.
restricted	restricted123	All	Has permissions “clear” and can execute only the “show system users” and “show interface terse” commands and nothing else.
lab	lab123	All	super-user

2) Ensure that all devices have the following SYSLOG configuration:
   a) All “emergency” messages are displayed on terminals of all currently logged users.
   b) Only all “critical” and higher severity messages are sent to the default syslog file.
   c) “interactive-commands” file keeps the audit trail of the users and commands they execute.
   d) File named “security-policy-logs” will contain security policy log entries. The system should retain 20 archive files with size of 512 KB (524288 B).
   e) “authorization-file” stores authorization messages with the severity “info” and higher.
   f) Following messages are sent to the syslog server at 10.10.1.99.
      i. All “emergency” messages
      ii. Authorization messages with severity “info” and higher
3) The syslog messages should contain year and milliseconds information.
4) Ensure that all devices will synchronize their time with the NTP server reachable at 10.10.1.254.
5) The devices have to use this server’s time also during booting.
6) The time zone is set to Europe/Amsterdam.

© 2020 Juniper Networks, Inc. All rights reserved.

7) The NTP communication between the devices and the NTP server needs to be protected using the MD5 authentication – key number 1 and password set to "**jncie**". These devices in turn accept only messages having the same protection.
8) All devices have to accept read-only SNMP requests only from the NMS system located at 10.10.1.20. The community string is "**roaccess**".
9) All devices have to send SNMP traps to the NMS system for following events:
    a) Authentication failures
    b) Hardware and environment
    c) Link transitions
    d) Routing protocol
10) The exa-fw device has to send the authentication failures to a specific monitoring system (10.10.10.50), which runs SNMP version 1 and listens on port 12345.
11) The devices should accept read-write SNMP requests from the network 10.10.199.0/24 except 10.10.199.199. The read-write community string is "snmpRWaccess".
12) All devices need to have defined following locations details:
    a. SNMP contact "**JNCIE admin**"
    b. SNMP description "**JNCIE-SEC device**"
    c. SNMP location "**Rack**"
    d. System location (not in the SNMP configuration): rack number **1**, floor **1**, country-code **NL**.
13) Configure all vSRX devices to accept SNMP requests from Junos Space located at 10.10.1.121 using the community string "JNCIE"
14) Firewall filters must protect all device's control planes in the way described below
    a. Where applicable ensure that any traffic originated from st0 interfaces is accepted.
    b. Permit DNS, NTP, SNMP, HTTPS and SSH traffic originated from subnets 10/8, 172.16/16 and 2016:abcd::/32.
    c. Ensure that ICMPv4 traffic is rate limited to 256kbps with traffic burst of 100k.
    d. Discard and syslog traffic with the protocols from 'step 15.b' for all other networks.
    e. Allow and count any other traffic from exercises where a new term is required.
    f. Silently drop all other traffic.

© 2020 Juniper Networks, Inc. All rights reserved.

Task 3: Interfaces, Zones, Local Traffic, Routing, and Routing Instances

This part is focused on the interfaces, security zones, local traffic handling, routing, routing instance segregation and device operation configurations

1) Configure interfaces and security zones on individual devices as follows (the table is based on figure 2):

Device	Interface	IP address	VLAN-ID	Zone
roffice1	lo0.0	192.168.1.1/32	-	UNTRUST
roffice1	ge-0/0/3	80.1.1.1/30	-	UNTRUST
roffice1	ge-0/0/4	172.16.10.254/24	-	TRUST-RO1
roffice1	ge-0/0/5	172.16.11.254/24	-	PRIVATE-RO1
roffice2	lo0.0	192.168.1.2/32	-	UNTRUST
roffice2	ge-0/0/3	80.1.1.5/30	-	UNTRUST
roffice2	ge-0/0/4	172.16.20.254/24	-	TRUST-RO2
roffice2	ge-0/0/5	172.16.21.254/24	-	DMZ-RO2
central	lo0.0	192.168.1.3/32, 80.1.1.16/32	-	UNTRUST
central	ge-0/0/3	80.1.1.10/30	-	UNTRUST
central	ge-7/0/3	80.1.1.14/30	-	UNTRUST
central	reth0.50	172.16.50.254/24	50	TRUST
central	reth0.55	172.16.55.254/24	55	INTERNAL
central	reth0.60	172.16.60.254/24	60	WAREHOUSE
central	reth0.65	172.16.65.254/24	65	TESTBED
central	reth0.70	172.16.70.254/24	70	TESTBED
xparent	reth0.50	-	50	TRUST
xparent	reth0.60	-	60	WAREHOUSE
xparent	reth0.65	-	65	TESTBED
xparent	reth0.70	-	70	TESTBED
xparent	reth1.50	-	50	TRUST
xparent	reth1.60	-	60	WAREHOUSE
xparent	reth1.65	-	65	TESTBED
xparent	reth1.70	-	70	TESTBED

© 2020 Juniper Networks, Inc. All rights reserved.

Device	Interface	IP address	VLAN-ID	Zone
building1	lo0.1	192.168.1.6/32	-	INTERNAL-B1
building1	ge-0/0/3.100	172.16.100.254/24	100	TRUST-B1
building1	ge-0/0/3.101	172.16.101.254/24	101	DMZ-B1
building1	ge-0/0/4.55	172.16.55.1/24	55	INTERNAL-B1
building2	lo0.2	192.168.1.7/32	-	INTERNAL-B2
building2	ge-0/0/3.200	172.16.200.254/24	200	TRUST-B2
building2	ge-0/0/3.201	172.16.201.254/24	201	DMZ-B2
building2	ge-0/0/5.55	172.16.55.2/24	55	INTERNAL-B2
exa-fw	lo0.0	192.168.1.8/32	-	UNTRUST
exa-fw	ge-0/0/3	100.1.1.1/29	-	UNTRUST
exa-fw	ge-0/0/4	172.16.10.254/24	-	TRUST-EXA
exa-fw	ge-0/0/5.15	172.16.15.254/24	15	PRIVATE-EXA
exa-fw	ge-0/0/5.30	172.16.30.254/24	30	DMZ-EXA

2) Ping to the security devices themselves must be allowed on all interfaces.
3) SSH connections are accepted on all TRUST zone interfaces.
4) On the devices roffice1, roffice2 and exa-fw create a default static route pointing to the UNTRUST network.
5) Use static routes on central cluster to provide connectivity to building's networks
6) On the building device (srx8) create two virtual-router routing-instances named building1 and building2, associate the interfaces of each building accordingly and create a default static route pointing to the correct VLAN interface on the central cluster.
7) Configure VLAN rewriting rules on xparent device:
    a. Interface reth1 – vlan-id 165 to vlan-id 65
    b. Interface reth1 – vlan-id 170 to vlan-id 70
8) Configure BGP between the central device to both external neighboring addresses or the Internet transit provider ASN 4321
    a. Advertise the company owned prefix 80.1.1.0/24 making sure BGP prefixes do not participate in the aggregation process.
    b. Make sure your preferred entry and exit point for general Internet connectivity is node0.

© 2020 Juniper Networks, Inc. All rights reserved.

Task 4: UTM

1) Antivirus scanning has to be done in the Remote office 1 and Remote office 2. Configure the security devices to perform antivirus scanning according to the following requirements:
    a. Only HTTP and FTP traffic from the correspondent TRUST zones to the UNTRUST network will be scanned
    b. The HTTP traffic to www.internalsites.com prefix and audio mime type are excluded from antivirus scan.
    c. The clients have to receive every 40 seconds a small portion of unchecked data to avoid timeout.
    d. The scanning engine timeout is set to 5 minutes.
    e. All fallback options are set to block except default and too-many-requests.
    f. The virus notification message is “Virus detected!”
    g. The fallback notifications are:
        i. BLOCK – “AV blocked the traffic as it was not able to scan it!”
2) The exa-fw device enforces local web-filtering according the requirements below:
    a. The web filtering is done on HTTP connections from the TRUST-EXA zone to the Internet.
    b. The following URLs are denied
        i. www.facebook.com
        ii. www.twitter.com
        iii. www.youtube.com
    c. The clients receive the “This site is not allowed” message in case their request was blocked.
    d. The local engine timeout is set to 10 minutes.
    e. All fallback options except default option block the requests.
3) In headquarters the HTTP and FTP traffic from the TRUST zone to the Internet leaving through the cluster needs to be processed in following manner:
    a. The content handling is:
        i. Cookies and java-applets are blocked
        ii. “bat” and “sh” files are blocked
        iii. The engine generates protocol error “Firewall blocked this content!” once traffic is blocked
4) The company’s email server (172.16.60.199) located in the WAREHOUSE zone behind the XPARENT cluster has to be protected from these outside spammers from the Internet
    a. IP addresses: 4.4.4.4, 5.5.5.5, 45.45.45.45
    b. Domains: spam.com, bad.com
    c. Email senders: spam@gmail.com, spam@yahoo.com

© 2020 Juniper Networks, Inc. All rights reserved.

Task 5: NAT

1) Following NAT translations need to be done on the roffice1 security device:
   a. The egress interface IP address is used to translate connections from the hosts in the TRUST-RO1 zone to the UNTRUST zone.
   b. The host 172.16.11.50 in the PRIVATE-RO1 zone needs to be able to receive connections from and initiate connections to the Internet. The connections from Internet need to be destined to the 80.1.1.64 IP address in order to reach this host.
2) NAT translation details for the roffice2 security device:
   a. Ensure the connections from the TRUST-RO2 zone to the Internet are translated to 80.1.1.96-80.1.1.99 IP addresses. PAT is allowed and concurrent sessions from the same host must be translated using the same IP address.
   b. The web and database servers need to be reachable from the UNTRUST zone as defined in the table below:

Server	Internal address	Internal port	Public address	Public port
Web server	172.16.21.2	80	80.1.1.100	8080
Database server	172.16.21.33	3306	80.1.1.100	3306

   c. Untranslated connections from the UNTRUST zone to these servers are not allowed.
3) The exa-fw device has to provide the following translations:
   a. Traffic from the TRUST-EXA hosts to the Internet has to be translated to the 100.1.1.128-100.1.1.143 range. PAT is not allowed, and the IP address of the egress interface has to be used when the pool is exhausted.
   b. The connections from PRIVATE-EXA hosts to the Internet must be translated in following manner:
      i. 172.16.15.5 --> 100.1.1.192, 172.16.15.6 --> 100.1.1.193, …, up to 172.16.15.10 --> 100.1.1.197
      ii. Ports are not translated
      iii. Connections from other hosts are not translated
   c. The servers in the DMZ-EXA zone need to be reachable from the Internet as specified in the table below:

© 2020 Juniper Networks, Inc. All rights reserved.

Server	Internal address	Internal port	Public address	Public port
Web server	172.16.30.11	80	100.1.1.3	8080
Database server	172.16.30.12	3306	100.1.1.3	3306
SSH server	172.16.30.13	22	100.1.1.4	12345

d. Untranslated connections from the UNTRUST zone to these servers are not allowed.

4) The connections leaving the headquarters through central cluster need to be translated in following way:
   a. All connections arriving on the cluster in the TRUST and INTERNAL zones and destined to the Internet need to be translated using the 80.1.1.128 - 80.1.1.159
   b. Bidirectional translation needs to be provided for the company's email server (172.16.60.199). The public IP address allocated for this purpose is 80.1.1.192. Untranslated traffic from the UNTRUST zone to the email server must be blocked.
   c. From the WAREHOUSE zone only the Websense appliance's (172.16.60.99) initiated connections to the Internet are translated. Use the 80.1.1.160 IP address.
   d. The servers located in the WAREHOUSE zone have to be reachable from the Internet.

Server	Internal address	Internal port	Public address	Public port
Web server	172.16.60.205	80	80.1.1.200	8080
Database server	172.16.60.205	3306	80.1.1.200	3306
SSH server	172.16.60.206	22	80.1.1.201	22
Honeypot	172.16.60.207	All	80.1.1.202	All

e. Untranslated connections from the UNTRUST zone to these servers are not allowed.

© 2020 Juniper Networks, Inc. All rights reserved.

Task 6: IPsec VPN

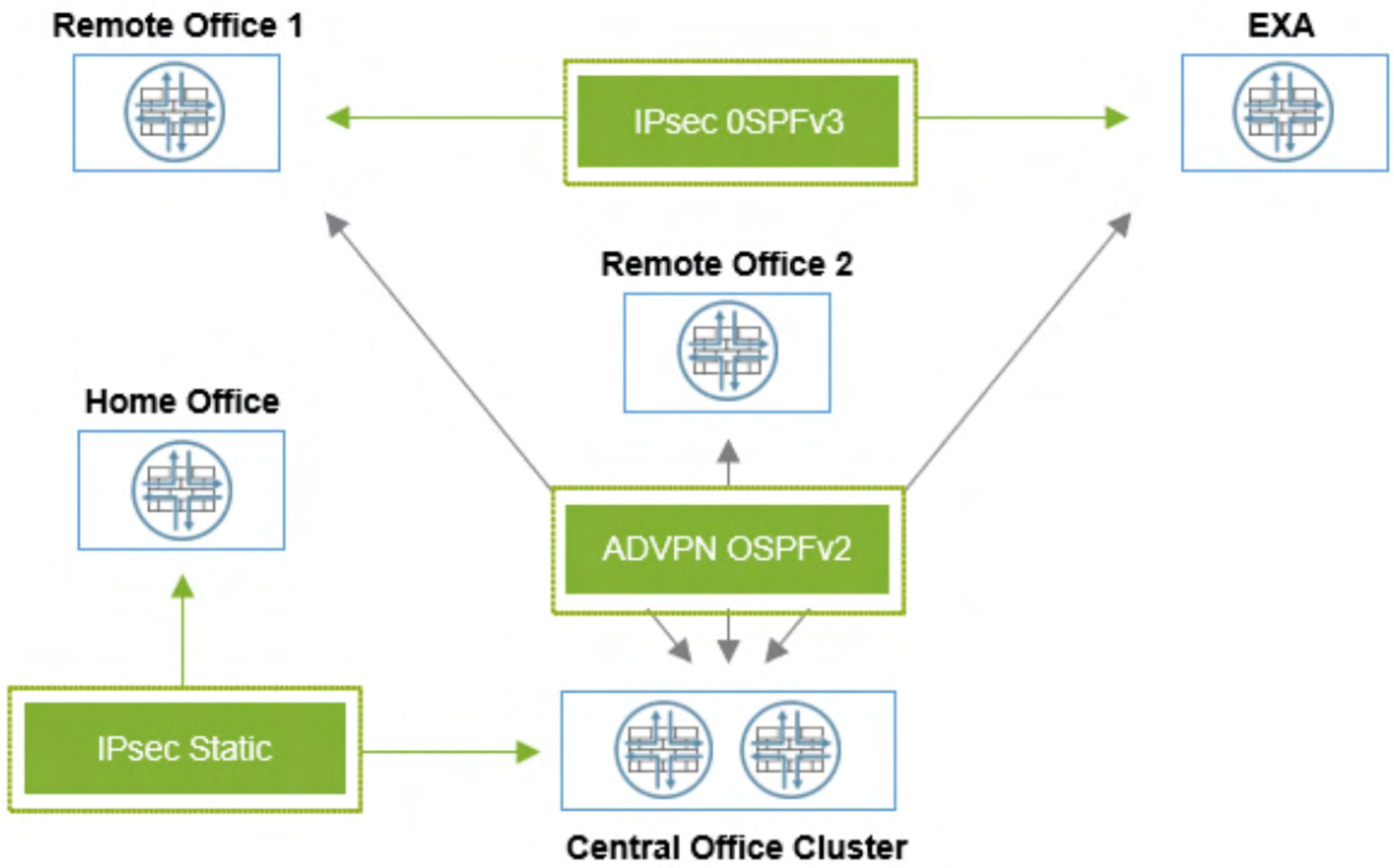


Figure 3: IPsec – VPNv4

1) Create and ADVPN between the central cluster and remote sites: Remote Office1, Remote Office2, and the EXA company. Ensure that traffic between the remote sites and the EXA company do not need to traverse the central cluster.
   a. Configure static NAT on exa-fw and roffice to solve the issue of overlapping subnets in the security zone TRUST-EXA and TRUST-RO1. Use the subnet 172.16.110.0/24 to reach the TRUST-EXA security zone network and 172.16.111.0/24 to reach the TRUST-RO1 security zone network. You can use up to two static routes on the central office cluster.
   b. Ensure all your TRUST networks from any device can communicate with each other.
   c. Ensure the VPN traffic traverses the cluster member that owns priority of the VPN's termination interface
2) You need to configure an IPsec VPN between hoffice and cluster nodes. You do not have access to the hoffice device and can only use CLI for troubleshooting. Here are the VPN parameters that were negotiated with the hoffice administrator:
   a. The home office security device uses statically assigned public IP address. It is always an initiator of the IPsec VPN and is configured in main mode. The IP address of home office gateway is unknown.

© 2020 Juniper Networks, Inc. All rights reserved.

b. IKE phase 1 proposal must include: preshared key “juniper”, DES, DH G1, MD5.
c. IKE phase 2 proposal must include: DES, ESP, MD5.

Device	Interface	IP address	Zone
central	st0.1	-	VPN

d. The IPsec VPN should provide access for all traffic types from the TRUST-H security zone to all TRUST security zones with the least possible number of policies
e. The remote device is prepared to negotiate phase 2 and accept traffic using the 172.16.0.0/16 network
f. The central cluster must forward traffic into the IPsec VPN using the node that bears redundancy group primacy of the tunnel’s endpoint interface.
g. You can add a static route to reach the TRUST zone of the home-office firewall

3) IPv6 networks should have full access between roffice1 and exa-fw devices
   a. Create a new route-based VPN associated with the st0.1 interface as shown in the table below
   b. Create or update existing interfaces with the following IPv6 addresses. Make sure all interfaces respond to ping requests.
   c. Ensure that the ipv6 networks are exchanged between both sites using OSPF.

Device	Interface	IPv6 address	Zone
roffice1	lo0.0	2016:abcd:ffff::2/64	UNTRUST
roffice1	ge-0/0/4.0	2016:abcd:b1::254/64	TRUST-RO1
roffice1	ge-0/0/5.0	2016:abcd:b2::254/64	PRIVATE-RO1
roffice1	st0.1	2002:111::2/64	VPN
exa-fw	lo0.0	2016:abcd:ffff::4/64	UNTRUST
exa-fw	ge-0/0/4.0	2016:abcd:d1::254/64	TRUST-EXA
exa-fw	ge-0/0/5.15	2016:abcd:d2::254/64	PRIVATE-EXA
exa-fw	st0.1	2002:111::1/64	VPN

© 2020 Juniper Networks, Inc. All rights reserved.

Task 7: Attack Prevention and Mitigation

1) Ensure that roffice1 and roffice2 are protected against following attacks arriving from the Internet:
    a. The TCP SYN segments flooding with the following thresholds and timer values:
        i. The destination thresholds values of 10000 TCP SYN segments per second.
        ii. Ensure that security device starts SYN Proxy protection mechanism when TCP SYN segments arrival rate reaches 500 segments per second.
        iii. Ensure that security device generates an alarm when TCP SYN segments arrival rate reaches 2500 segments per second.
        iv. The maximum time before incomplete sessions are dropped should be 10 seconds.
    b. Protect against fragmented TCP SYN segments.
    c. Protect against UDP flooding with the threshold of 500 packets per second.
2) Ensure that building1 and building2 are protected against the following reconnaissance attempts arriving from the INTERNAL security zone:
    a. IP address sweep and port scan both a detection rate of 10 packets arrived per 2 ms time interval.
    b. Detect IP packets with following values in the Options field:
        i. Record-route option.
        ii. Timestamp option.
    c. Protect against following operating systems probes:
        i. The TCP segment has both SYN and FIN flags set.
        ii. The TCP segment has no flags set.
    d. Ensure that detection of malicious traffic results in alarm generation instead of dropping the packets belonging to malicious packet flow.
3) Configure cluster in such a way to protect server 172.16.60.205 and 172.16.60.206:
    a. The uploading of exe or rpm files to the 172.16.60.206 server via FTP is allowed only from the TRUST security zone and prohibited from everywhere else. Each detected attempt results in silently dropping client's sessions.
    b. Allow anonymous access to the FTP service of the 172.16.60.206 server from any TRUST and the TESTBED security zones. Restrict access for the rest of the network. Silently drop packets from unauthorized hosts, block them for 1 hour and generate log messages with severity level Major and alert flag.
    c. Protect servers against scanning and worms from the INTERNAL and TESTBED security zones. Each detected attempt results in silently dropping packets.

© 2020 Juniper Networks, Inc. All rights reserved.

Task 8: Advanced Services – Central Cluster

1) Disable application system cache completely.
2) Enable AppTrack to provide information about applications used in the TRUST zone. The first message for each connection has to be generated 2 minutes after the application has been identified and then an update has to be created every 6 minutes.
3) Block the junos:MSN application over port 80 from the TRUST zone to the UNTRUST zone.
4) Allow only the junos:HTTP application over the default HTTP port from the TESTBED zone into the WAREHOUSE zone.
5) Ensure session deny as well as session close messages are created for exercise 3 and 4.
6) Ensure the junos:MEGAUPLOAD application over the port 80 from the TRUST zone to the UNTRUST zone will have the loss priority of "high" if it crosses 5000 kb/s with bursts of 15000 bytes. This has to be applied in both directions - client to server and server to client.
7) Make sure the SRX knows exactly what is going on in the encrypted sessions on the default HTTPS port from the TESTBED zone to the UNTRUST zone. The certificate for signing the modified server certificates should be locally generated on the SRX device with following values:
   - type: rsa
   - key size: 512
   - domain name: juniper.net
   - subject: DC=JNPR,CN=juniper,OU=unit-1,O=juniper,SN=1234,L=USA,ST=CA,C=US
   - email-ID: noreply@juniper.net

   The SRX will not authenticate any servers. Make sure everything about SSL proxy operations is logged in the “ssl-proxy” file.
8) Configure Juniper Identity Management Service to be able to identify network traffic on cluster 1 based on IP address as well as user and device context. Implement your solution for authenticated, unauthenticated and unknown users in the TRUST to UNTRUST zone.
9) SoundCloud traffic originated in the INTERNAL zone, leaving the Central Office must travers interface ge-7/0/3 and use interface ge-0/0/3 as backup.

© 2020 Juniper Networks, Inc. All rights reserved.

Task 9: Software Defined Secure Network (SDSN)

1) Create a new SkyATP realm. Enroll Policy Enforcer and the central office cluster in the newly created Sky ATP Realm through Security Director

Use the information below to setup the Sky ATP Realm:

SkyATP Realm	jnciesec-xxx (where xxx is shown in the lab access instructions)
Username	jnciesec-xxx@stu.juniper.net
Password	lab123@Lab
Juniper SSO account	eduservicenow@gmail.com
Juniper SSO password	********

Use the information for Security Director and Policy Enforcer:

Security Director Username	super
Security Director Password	lab123@Lab
Security Director IP	10.10.1.100
Policy Enforcer Username	root
Policy Enforcer Password	lab123@Lab
Policy Enforcer IP	10.10.1.123

Note: The password for the Juniper SSO account is auto populated in the Firefox browser on the Student Desktop. For this reason, it is important to use the Firefox browser on the Student Desktop to create the Sky ATP realm

2) Setup for SkyATP with SDSN in Security Director, ensure that HTTP traffic is analyzed at the central cluster (srx3/srx4) for threat levels greater than 8 for the 172.16.50.100 host. Ensure that connections are silently dropped at access switch vQFX if the 172.16.50.100 host becomes infected with malware. Ensure that only blocked traffic is logged. (Note that this includes C&C protection).

© 2020 Juniper Networks, Inc. All rights reserved.

Super Lab 2

This lab is designed to combine many of the solutions discussed in the previous chapters into a complete practice lab exam. This lab is similar to a real JNCIE-SEC lab exam experience. We recommend attempting this lab if you are able to complete the tasks in the previous chapters without any help.

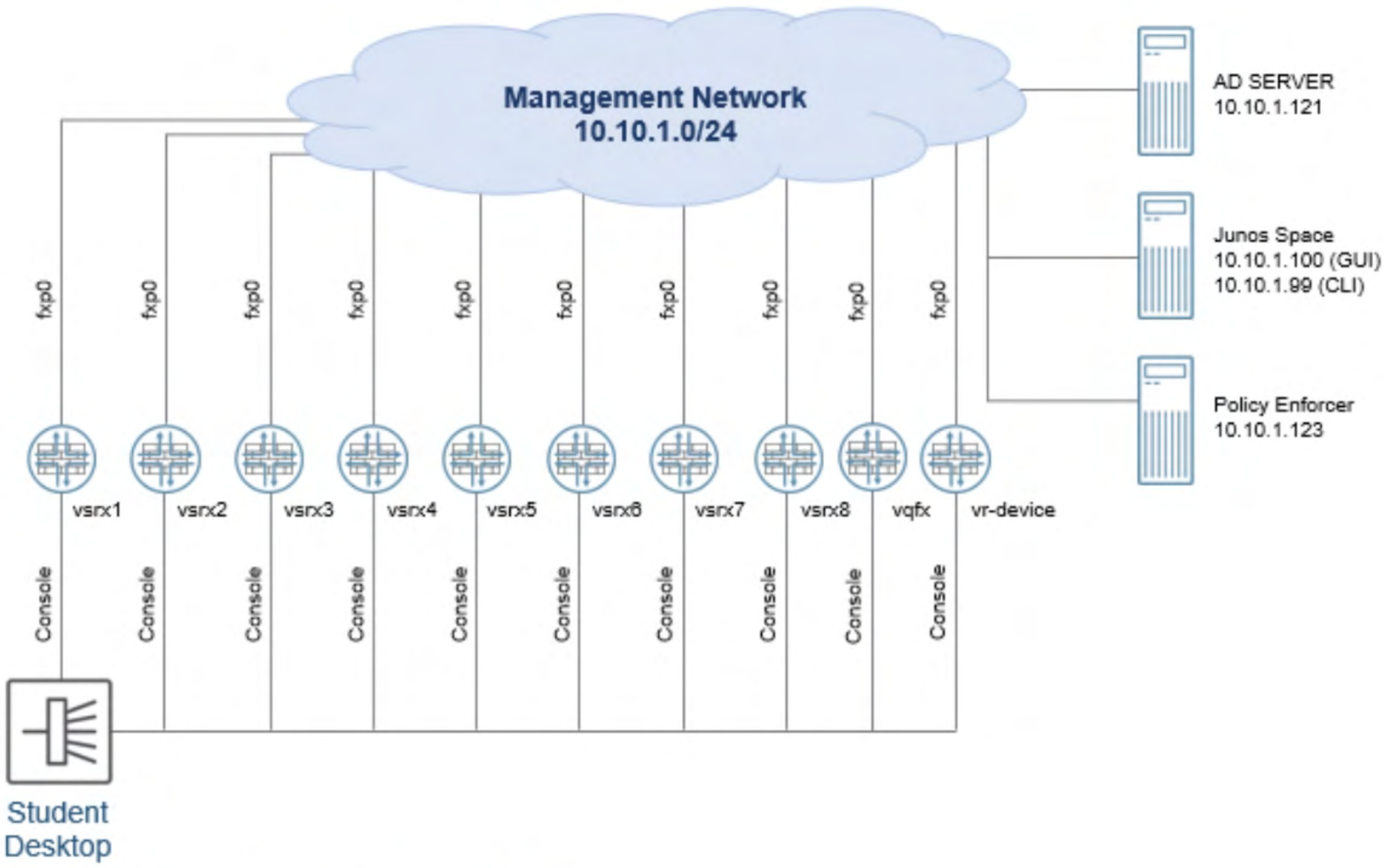


Figure 1: Super Lab 2 – Management Topology

Ensure you load the initial configurations on the devices before you start with this LAB. Ensure that you do not forget to load the initial Super Lab 2 configuration on the vr-device.

Tip: Ensure you read whole tasks before starting them.

© 2020 Juniper Networks, Inc. All rights reserved.

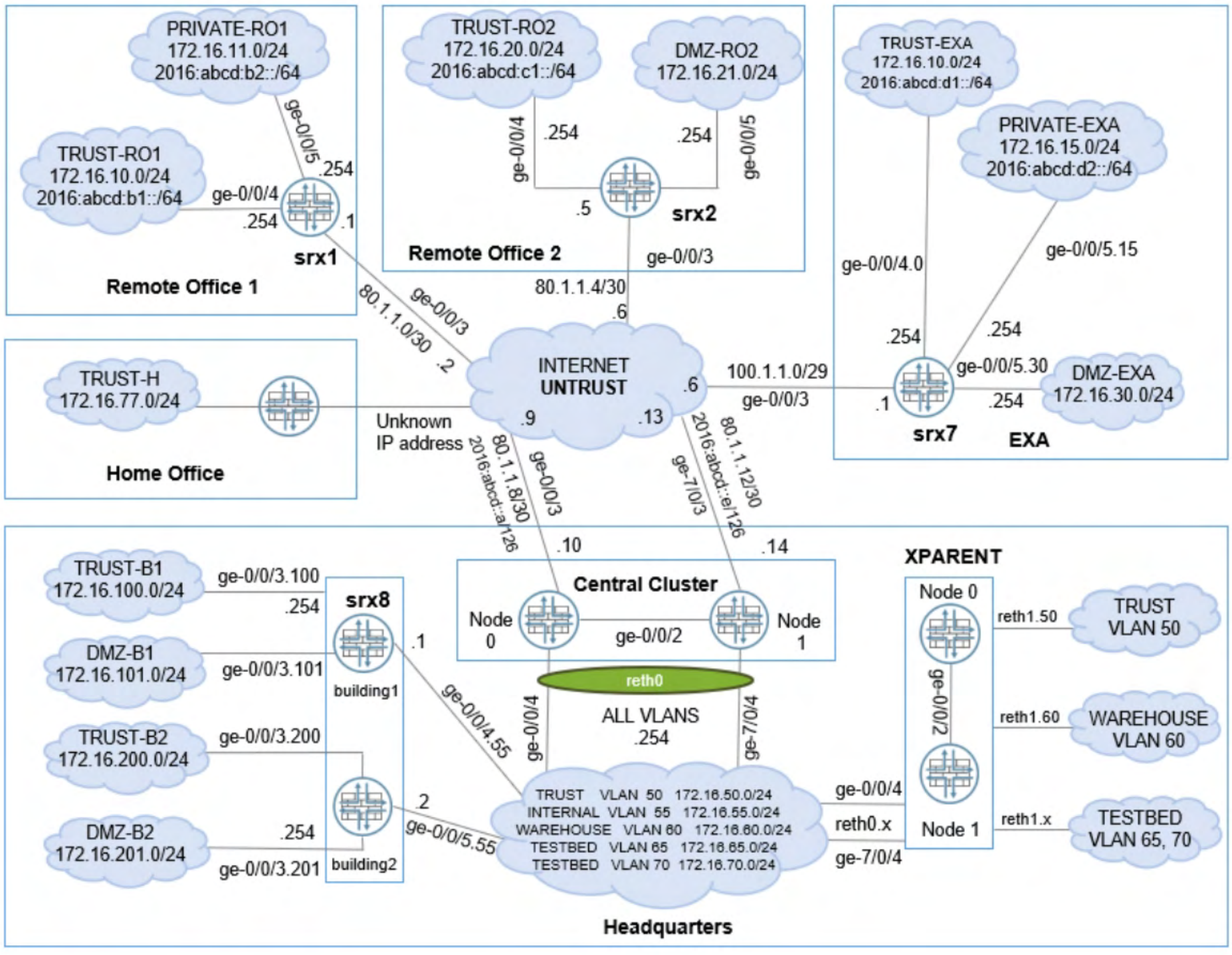


Figure 2: Super Lab 2 Topology

© 2020 Juniper Networks, Inc. All rights reserved.

Task 1: Initial Configuration - Part 1

In this part you will configure the device hostnames, high-availability (cluster) and management interfaces.

1) The table below lists the device hostnames mapping:

Device	Hostname
srx1	roffice1
srx2	roffice2
srx3	central-node0
srx4	central-node1
srx5	xparent-node0
srx6	xparent-node1
srx7	exa-fw
srx8	building

2) Create clusters as defined in the following table:

Device	Node ID	Cluster ID
central-node0	0	1
central-node1	1	1
xparent-node0	0	2
xparent-node1	1	2

3) Ensure ge-0/0/2 is used for the fabric link.
4) The routing engine of xparent cluster needs to be active on node 0
5) Configure the redundant ethernet interfaces according the figure 2.
6) Clusters should operate in the following manner:
    a. Central cluster redundancy groups mapped to interfaces dependent on physical links, need to be active on node0 whenever node0 is available
        i. Any failure from correspondent child interface triggers the failover
    b. Central cluster redundancy groups (RGs) mapped to interfaces dependent on logical links, need to be active on node1 whenever node1 is available
        i. Uplink interface monitoring triggers the failover
    c. The Central Cluster needs to monitor ICMP reachability to the host address (12.34.56.78) available in the Internet. In case this reachability is compromised, the test's uplink interface should be brought down so that the RG fails over.

© 2020 Juniper Networks, Inc. All rights reserved.

i. Probe threshold should be between 30 and 60 seconds
ii. Control plane redundancy group needs to follow the same faith of the RG from point 6.b

d. All xparent cluster redundancy groups need to be active on node 0 and should automatically failover in case any of its physical links fail.
i. No need for automatic recovery of primacy

7) Configure the management interfaces (figure 1) as defined in the table below:

Device	Management IP address
roffice1	10.10.1.1/24
rooffice2	10.10.1.2/24
central-node0	10.10.1.3/24
central-node1	10.10.1.4/24
xparent-node0	10.10.1.5/24
xparent-node1	10.10.1.6/24
exa-fw	10.10.1.7/24
building	10.10.1.8/24

8) Ensure the management interfaces (figure 1):
a. Will accept only specific services as defined in the table below.

Device	Services
roffice1	SSH with root access (session limit 3), HTTPS
rooffice2	SSH with root access (session limit 3), HTTPS
central	SSH with root access (session limit 3), HTTPS
xparent	SSH with root access (session limit 3), HTTPS
building	SSH with root access (session limit 3), HTTPS
exa-fw	SSH with root access (session limit 3), HTTPS

Task 2: Initial configuration - Part 2

In this part you will configure authentication, authorization, Syslog, SNMP and NTP parameters.

1) Configure users as defined in the table below:

© 2020 Juniper Networks, Inc. All rights reserved.

Username	Password	Device	Privileges
ronly	ronly123	All	Has permission “view” and “view-configuration”. Additionally, can NOT execute the “file delete” command and view the [edit system login] configuration hierarchy.
admin1	admin123	All	Has permissions “all”. But is not allowed to reboot the device.
restricted	restricted123	All	Has permissions “clear” and can execute only the “show system users” and “show interface terse” commands and nothing else.
lab	lab123	All	super-user

2) Ensure that all devices have the following SYSLOG configuration:
    a. All “emergency” messages are displayed on terminals of all currently logged users.
    b. Only all “critical” and higher severity messages are sent to the default syslog file.
    c. “interactive-commands” file keeps the audit trail of the users and commands they execute.
    d. File named “security-policy-logs” will contain security policy log entries. The system should retain 20 archive files with size of 512 KB (524288 B).
    e. “authorization-file” stores authorization messages with the severity “info” and higher.
    f. Following messages are sent to the syslog server at 10.10.1.99.
        iii. All “emergency” messages
        iv. Authorization messages with severity “info” and higher
3) The syslog messages should contain year and milliseconds information.
4) Ensure that all devices will synchronize their time with an NTP server reachable at 10.10.1.254.
5) The devices have to use this server’s time also during booting.
6) The time zone is set to Europe/Amsterdam.
7) The NTP communication between the devices and the NTP server needs to be protected using the MD5 authentication – key number 1 and password set to “**jncie**”. These devices in turn accept only messages having the same protection.
8) All devices have to accept read-only SNMP requests only from the NMS system located at 10.10.1.20. The community string is “**roaccess**”.
9) All devices have to send SNMP traps to the NMS system for following events:
    a. Authentication failures
    b. Hardware and environment
    c. Link transitions
    d. Routing protocol

© 2020 Juniper Networks, Inc. All rights reserved.

10) The exa-fw device has to send the authentication failures to a specific monitoring system (10.10.10.50), which runs SNMP version 1 and listens on port 12345.
11) The devices should accept read-write SNMP requests from the network 10.10.199.0/24 except 10.10.199.199. The read-write community string is "snmpRWaccess".
12) All devices need to have defined following locations details:
    a. SNMP contact "**JNCIE admin**"
    b. SNMP description "**JNCIE-SEC device**"
    c. SNMP location "**Rack**"
    d. System location (not in the SNMP configuration): rack number **1**, floor **1**, country-code **NL**.
13) Configure all vSRX devices to accept SNMP requests from Junos Space located at 10.10.1.121 using the community string "JNCIE"
14) Firewall filters must protect all device's control planes in the way described below
    a. Where applicable ensure that any traffic originated from st0 interfaces is accepted.
    b. Permit DNS, NTP, SNMP, HTTPS and SSH traffic originated from subnets 10/8, 172.16/16 and 2016:abcd::/32.
    c. Ensure that ICMPv4 traffic is rate limited to 256kbps with traffic burst of 100k.
    d. Discard and syslog traffic with the protocols from 'step 15.b' for all other networks.
    e. Allow and count any other traffic from exercises where a new term is required.
    f. Silently drop all other traffic.

© 2020 Juniper Networks, Inc. All rights reserved.

Task 3: Control Plane Protection

1) Firewall filters must protect all device's control planes in the way described below
    a. Where applicable ensure that any traffic originated from st0 and gr interfaces is accepted.
    b. Permit DNS, NTP, SNMP, HTTPS and SSH traffic originated from subnets 10/8, 172.16/16, 2016:abcd::/32 and loopback interfaces.
    c. Ensure that ICMPv4 traffic is rate limited to 256kbps with traffic burst of 100k.
    d. Discard and syslog traffic with the protocols from 'step 14.b' from all other networks.
    e. Allow and count any other traffic from exercises where a new term is required.
    f. Silently drop all other traffic.

Note: The firewall filter is a constant point of focus to bear in mind when troubleshooting is involved. Always make sure you update and evaluate your statement along with adding counters to traffic denial rules so that you understand if the firewall filter may be blocking interesting traffic.

© 2020 Juniper Networks, Inc. All rights reserved.

Task 4: Interfaces, Zones, Local Traffic, and Routing

This part is focused on the interfaces, security zones, local traffic handling, routing, routing instance segregation and device operation configurations

1) Configure interfaces and security zones on individual devices as follows:

Device	Interface	IP address	VLAN-ID	Zone
roffice1	lo0.0	192.168.1.1/32	-	UNTRUST
roffice1	ge-0/0/3	80.1.1.1/30	-	UNTRUST
roffice1	ge-0/0/4	172.16.10.254/24	-	TRUST-RO1
roffice1	ge-0/0/5	172.16.11.254/24	-	PRIVATE-RO1
roffice2	lo0.0	192.168.1.2/32	-	UNTRUST
roffice2	ge-0/0/3	80.1.1.5/30	-	UNTRUST
roffice2	ge-0/0/4	172.16.20.254/24	-	TRUST-RO2
roffice2	ge-0/0/5	172.16.21.254/24	-	DMZ-RO2
central	lo0.0	192.168.1.3/32, 80.1.1.16/32	-	UNTRUST
central	ge-0/0/3	80.1.1.10/30	-	UNTRUST
central	ge-7/0/3	80.1.1.14/30	-	UNTRUST
central	reth0.50	172.16.50.254/24	50	TRUST
central	reth0.55	172.16.55.254/24	55	INTERNAL
central	reth0.60	172.16.60.254/24	60	WAREHOUSE
central	reth0.65	172.16.65.254/24	65	TESTBED
central	reth0.70	172.16.70.254/24	70	TESTBED
xparent	reth0.50	-	50	TRUST
xparent	reth0.60	-	60	WAREHOUSE
xparent	reth0.65	-	65	TESTBED
xparent	reth0.70	-	70	TESTBED
xparent	reth1.50	-	50	TRUST
xparent	reth1.60	-	60	WAREHOUSE
xparent	reth1.65	-	65	TESTBED
xparent	reth1.70	-	70	TESTBED

© 2020 Juniper Networks, Inc. All rights reserved.

Device	Interface	IP address	VLAN-ID	Zone
building1	lo0.1	192.168.1.6/32	-	INTERNAL-B1
building1	ge-0/0/3.100	172.16.100.254/24	100	TRUST-B1
building1	ge-0/0/3.101	172.16.101.254/24	101	DMZ-B1
building1	ge-0/0/4.55	172.16.55.1/24	55	INTERNAL-B1
building2	lo0.2	192.168.1.7/32	-	INTERNAL-B2
building2	ge-0/0/3.200	172.16.200.254/24	200	TRUST-B2
building2	ge-0/0/3.201	172.16.201.254/24	201	DMZ-B2
building2	ge-0/0/5.55	172.16.55.2/24	55	INTERNAL-B2
exa-fw	lo0.0	192.168.1.8/32	-	UNTRUST
exa-fw	ge-0/0/3	100.1.1.1/29	-	UNTRUST
exa-fw	ge-0/0/4	172.16.10.254/24	-	TRUST-EXA
exa-fw	ge-0/0/5.15	172.16.15.254/24	15	PRIVATE-EXA
exa-fw	ge-0/0/5.30	172.16.30.254/24	30	DMZ-EXA

2) Ping to the security devices themselves must be allowed on all interfaces.
3) SSH connections are accepted on all TRUST zone interfaces.
4) On the devices roffice1, roffice2 and exa-fw create a default static route pointing to the UNTRUST network.
5) Use static routes on central cluster to provide connectivity to building's networks
6) On the building device (srx8) create two virtual-router routing-instances named building1 and building2, associate the interfaces of each building accordingly and create a default static route pointing to the correct VLAN interface on the central cluster.
7) Configure VLAN rewriting rules on xparent device:
    a. Interface reth1 – vlan-id 165 to vlan-id 65
    b. Interface reth1 – vlan-id 170 to vlan-id 70
8) Configure BGP between the central device to both external neighboring addresses or the Internet transit provider ASN 4321
    a. Advertise the company owned prefix 80.1.1.0/24 making sure BGP prefixes do not participate in the aggregation process.
    b. Make sure your preferred entry and exit point for general Internet connectivity is node0.

© 2020 Juniper Networks, Inc. All rights reserved.

Task 5: UTM

1) Antivirus scanning has to be done in the Remote office 1 and Remote office 2. Configure the security devices to perform antivirus scanning according to the following requirements:
    a. Only HTTP and FTP traffic from the correspondent TRUST zones to the UNTRUST network will be scanned
    b. The HTTP traffic to www.internalsites.com prefix and audio mime type are excluded from antivirus scan.
    c. The clients have to receive every 40 seconds a small portion of unchecked data to avoid timeout.
    d. The scanning engine timeout is set to 5 minutes.
    e. All fallback options are set to block except default and too-many-requests.
    f. The virus notification message is “Virus detected!”
    g. The fallback notifications are:
        i. BLOCK – “AV blocked the traffic as it was not able to scan it!”
2) The exa-fw device enforces local web-filtering according the requirements below:
    a. The web filtering is done on HTTP connections from the TRUST-EXA zone to the Internet.
    b. The following URLs are denied
        i. www.facebook.com
        ii. www.twitter.com
        iii. www.youtube.com
    c. The clients receive the “This site is not allowed” message in case their request was blocked.
    d. The local engine timeout is set to 10 minutes.
    e. All fallback options except default option block the requests.
3) In headquarters the HTTP and FTP traffic from the TRUST zone to the Internet leaving through the cluster needs to be processed in following manner:
    a. The content handling is:
        i. Cookies and java-applets are blocked
        ii. “bat” and “sh” files are blocked
        iii. The engine generates protocol error “Firewall blocked this content!” once traffic is blocked
4) The company’s email server (172.16.60.199) located in the WAREHOUSE zone behind the XPARENT cluster has to be protected from these outside spammers from the Internet
    a. IP addresses: 4.4.4.4, 5.5.5.5, 45.45.45.45
    b. Domains: spam.com, bad.com
    c. Email senders: spam@gmail.com, spam@yahoo.com

© 2020 Juniper Networks, Inc. All rights reserved.

Task 6: NAT

1) Following NAT translations need to be done on the roffice1 security device:
   a. The egress interface IP address is used to translate connections from the hosts in the TRUST-RO1 zone to the UNTRUST zone.
   b. The host 172.16.11.50 in the PRIVATE-RO1 zone needs to be able to receive connections from and initiate connections to the Internet. The connections from Internet need to be destined to the 80.1.1.64 IP address in order to reach this host.
2) NAT translation details for the roffice2 security device:
   a. Ensure the connections from the TRUST-RO2 zone to the Internet are translated to 80.1.1.96-80.1.1.99 IP addresses. PAT is allowed and concurrent sessions from the same host must be translated using the same IP address.
   b. The web and database servers need to be reachable from the UNTRUST zone as defined in the table below:

Server	Internal address	Internal port	Public address	Public port
Web server	172.16.21.2	80	80.1.1.100	8080
Database server	172.16.21.33	3306	80.1.1.100	3306

   c. Untranslated connections from the UNTRUST zone to these servers are not allowed.
3) The exa-fw device has to provide the following translations:
   a. Traffic from the TRUST-EXA hosts to the Internet has to be translated to the 100.1.1.128-100.1.1.143 range. PAT is not allowed, and the IP address of the egress interface has to be used when the pool is exhausted.
   b. The connections from PRIVATE-EXA hosts to the Internet must be translated in following manner:
      i. 172.16.15.5 --> 100.1.1.192, 172.16.15.6 --> 100.1.1.193, …, up to 172.16.15.10 --> 100.1.1.197
      ii. Ports are not translated
      iii. Connections from other hosts are not translated
   c. The servers in the DMZ-EXA zone need to be reachable from the Internet as specified in the table below:

© 2020 Juniper Networks, Inc. All rights reserved.

Server	Internal address	Internal port	Public address	Public port
Web server	172.16.30.11	80	100.1.1.3	8080
Database server	172.16.30.12	3306	100.1.1.3	3306
SSH server	172.16.30.13	22	100.1.1.4	12345

d. Untranslated connections from the UNTRUST zone to these servers are not allowed.

4) The connections leaving the headquarters through central cluster need to be translated in following way:
   a. All connections arriving on the cluster in the TRUST and INTERNAL zones and destined to the Internet need to be translated using the 80.1.1.128 - 80.1.1.159
   b. Bidirectional translation needs to be provided for the company's email server (172.16.60.199). The public IP address allocated for this purpose is 80.1.1.192. Untranslated traffic from the UNTRUST zone to the email server must be blocked.
   c. From the WAREHOUSE zone only the Websense appliance's (172.16.60.99) initiated connections to the Internet are translated. Use the 80.1.1.160 IP address.
   d. The servers located in the WAREHOUSE zone have to be reachable from the Internet.

Server	Internal address	Internal port	Public address	Public port
Web server	172.16.60.205	80	80.1.1.200	8080
Database server	172.16.60.205	3306	80.1.1.200	3306
SSH server	172.16.60.206	22	80.1.1.201	22
Honeypot	172.16.60.207	All	80.1.1.202	All

e. Untranslated connections from the UNTRUST zone to these servers are not allowed.

© 2020 Juniper Networks, Inc. All rights reserved.

Task 7: IPsec VPN

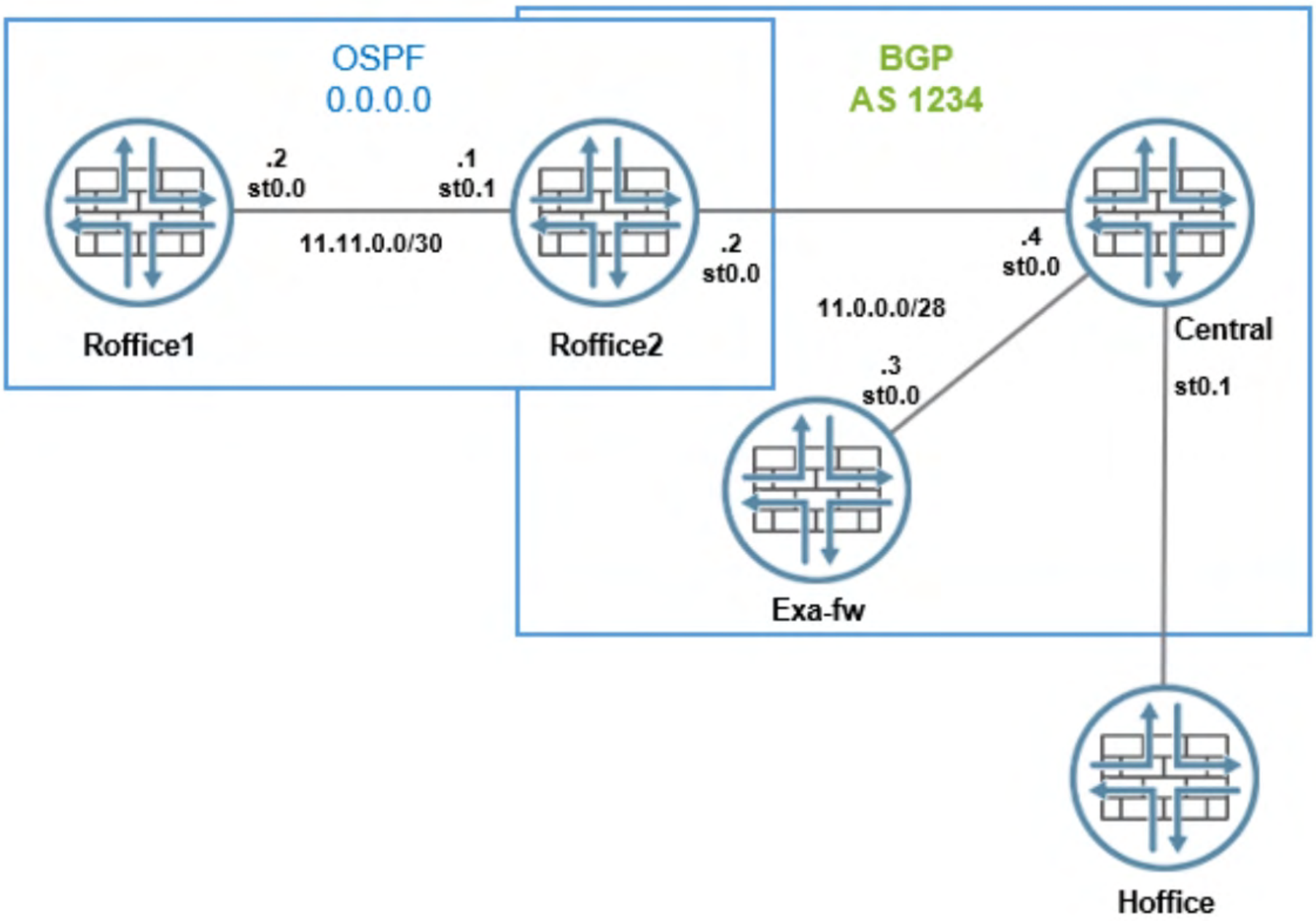


Figure 3: IPsec – VPNv4

1) The VPN design between roffice1 and roffice2 assumes that the OSPFv2 needs to be run on the top of the GRE tunnel. Here are the VPN parameters that were negotiated with the roffice1 administrator:
   a. The roffice1 security device is always an initiator of the IPsec VPN. The local-id is a hostname with the value “roffice1”.
   b. The st0.0 and st0.1 interfaces are used as a termination points for GRE tunnel on roffice1 and roffice2 devices respectively;
   c. The ge-0/0/3.0 interfaces are used as external interfaces for Phase 1 establishment on both sides of the VPN.
   d. IKE phase 1 proposal must include: preshared key “juniper”, 3DES, DH G1, MD5. Rekey Phase1 every 4 hours.
   e. IKE phase 2 proposal must include: AES128, ESP, DH G2, SHA1. Rekey Phase2 every hour.

© 2020 Juniper Networks, Inc. All rights reserved.

f. The interfaces configuration must follow information in the table below. For the GRE tunnel source and destination address use addresses of the interfaces st0.0 on roffice1 and st0.1 on roffice2 from the table below.

Device	Interface	IP address	Zone
roffice1	st0.0	11.11.0.1/30	VPN
roffice1	gr-0/0/0.0	11.11.11.1/30	VPN
roffice2	st0.1	11.11.11.2/30	VPN
roffice2	gr-0/0/0.0	11.11.0.2/30	VPN

g. Ensure that the TRUST zone subnet of both devices appears as OSPF internal route but IGP adjacency must only be attempted across GRE interfaces.
h. Ensure that TRUST networks connected to other hosts appear as OSPF external routes.
i. Ensure that the least possible number of security policies allow the subnets located in roffice's TRUST security zones communicating to each other.

2) You need to configure an IPsec VPN between hoffice and cluster nodes. You do not have access to the hoffice device and can only use CLI for troubleshooting. Here are the VPN parameters that were negotiated with the hoffice administrator:
   a. The hoffice security device uses statically assigned public IP address. It is always an initiator of the IPsec VPN and is configured in main mode. The IP address of hoffice gateway is unknown.
   b. IKE phase 1 proposal must include: preshared key "juniper", DES, DH G1, MD5.
   c. IKE phase 2 proposal must include: DES, ESP, MD5.

Device	Interface	IP address	Zone
central	st0.1	-	VPN

   d. The IPsec VPN should provide access for all traffic types from the TRUST-H security zone to all TRUST security zones with the least possible number of policies
   e. The remote device is prepared to negotiate phase 2 and accept traffic using the 172.16.0.0/16 network
   f. The central cluster must forward traffic into the IPsec VPN using the node that bears redundancy group primacy of the tunnel's endpoint interface.
   g. You can add a static route to reach the TRUST zone of the home-office firewall

© 2020 Juniper Networks, Inc. All rights reserved.

3) The roffice2 and exa-fw security devices need to be connected to the cluster node as spokes of the hub-and-spoke VPN. Here are VPN parameters that must be used for the configuration:
   a. Only one st0 interface per security device can be used for the IPsec tunnel(s) termination.
   b. Configure the interfaces on every device according to the table below:

Device	Interface	IP address	Zone
roffice2	st0.0	11.0.0.2/28	VPN
exa-fw	st0.0	11.0.0.3/28	VPN
central	st0.0	11.0.0.4/28	VPN

   c. Configure static NAT on exa-fw and cluster to solve the issue of overlapping subnets in the security zone TRUST-EXA and TRUST-RO1. Use the subnet 172.16.110.0/24 to reach the TRUST-EXA security zone network and 172.16.111.0/24 to reach the TRUST-RO1 security zone network. You can use up to two static routes.
   d. Validate data path with VPN monitor option. The keepalives should be sent to the neighboring peer regardless of traffic patterns with 5 sec intervals. It is allowed to miss only 3 consecutive keepalives after which the tunnel is considered inactive.
   e. IKE phase 1 proposal must include: preshared key “juniper”, AES128, DH G2, SHA1. Rekey phase 1 every 16 hours.
   f. IKE phase 2 proposal must include: AES192, ESP, SHA1. Rekey phase 2 on transmission of 100 MB of traffic.
   g. Configure internal BGP in the central cluster, roffice2 and exa-fw. Advertise internal network reachability using a single prefix from the central cluster.
   h. Ensure all your TRUST networks from any device can communicate with each other. You must not use static routes.
   i. Ensure the VPN traffic traverses the cluster member that owns priority of the VPN’s termination interface
4) Remote offices and the newly acquired company do not have native IPv6 Internet access so they have to go through the central location in a hub-and-spoke fashion.
   a. Central location uses native IPv6 BGP peering with existing neighbors
      i. Make sure peer #1 is preferred for incoming and outgoing traffic
      ii. Advertise the Enterprise IPv6 public prefix to these peers
   b. Use OSPFv3 between the sites for full reachability between the different IPv6 TRUST zones and HTTP reachability to the Internet.

© 2020 Juniper Networks, Inc. All rights reserved.

5) Create and update existing interfaces with the following IPv6 addresses. Make sure all interfaces respond to ping requests.

Device	Interface	IPv6 address	Zone
roffice1	lo0.0	2016:abcd:ffff::2/64	UNTRUST
roffice1	ge-0/0/4.0	2016:abcd:b1::254/64	TRUST-RO1
roffice1	ge-0/0/5.0	2016:abcd:b2::254/64	PRIVATE-RO1
roffice1	st0.1	2016:abcd:eeee::2/126	VPN
roffice1	st0.2	-	VPN
roffice2	lo0.0	2016:abcd:ffff::3/64	UNTRUST
roffice2	ge-0/0/4.0	2016:abcd:c1::254/64	TRUST-RO2
roffice2	gr-0/0/0.1	2016:abcd:ffff::254/64	VPN
exa-fw	lo0.0	2016:abcd:ffff::4/64	UNTRUST
exa-fw	ge-0/0/4.0	2016:abcd:d1::254/64	TRUST-EXA
exa-fw	ge-0/0/5.15	2016:abcd:d2::254/64	PRIVATE-EXA
exa-fw	gr-0/0/0.0	2016:abcd:eeee::a/126	VPN
exa-fw	st0.1	-	VPN
central	lo0.0	2016:abcd:ffff::1/64	UNTRUST
central	ge-0/0/3.0	2016:abcd:aa01::a/126	UNTRUST
central	ge-5/0/3.0	2016:abcd:aa01::e/126	UNTRUST
central	reth0.50	2016:abcd:a1::254/126	TRUST
central	st0.2	2016:abcd:eeee::1/126	VPN
central	gr-0/0/0.0	2016:abcd:eeee::5/126	VPN
central	gr-0/0/0.1	2016:abcd:eeee::9/126	VPN

6) Configure an IPv6 over IPv4 IPsec VPN between the roffice1 device and the central cluster
   a. Phase1 and Phase 2 should use basic proposals and PSK
   b. Roffice1's external address may change
7) Use existing IPsec VPNs between Roffice2, Exa and Central devices to propagate IPv6 traffic
   a. GRE tunnels have to be used with source and destination mapped to the IPsec interface addresses
8) IPv6 private zones should have total access between roffice1 and exa-fw devices

© 2020 Juniper Networks, Inc. All rights reserved.

a. Create a new route-based VPN associated with the unnumbered tunnel interface from the table above
b. Roffice1's external address may change
c. Use previously created basic proposals and PSK

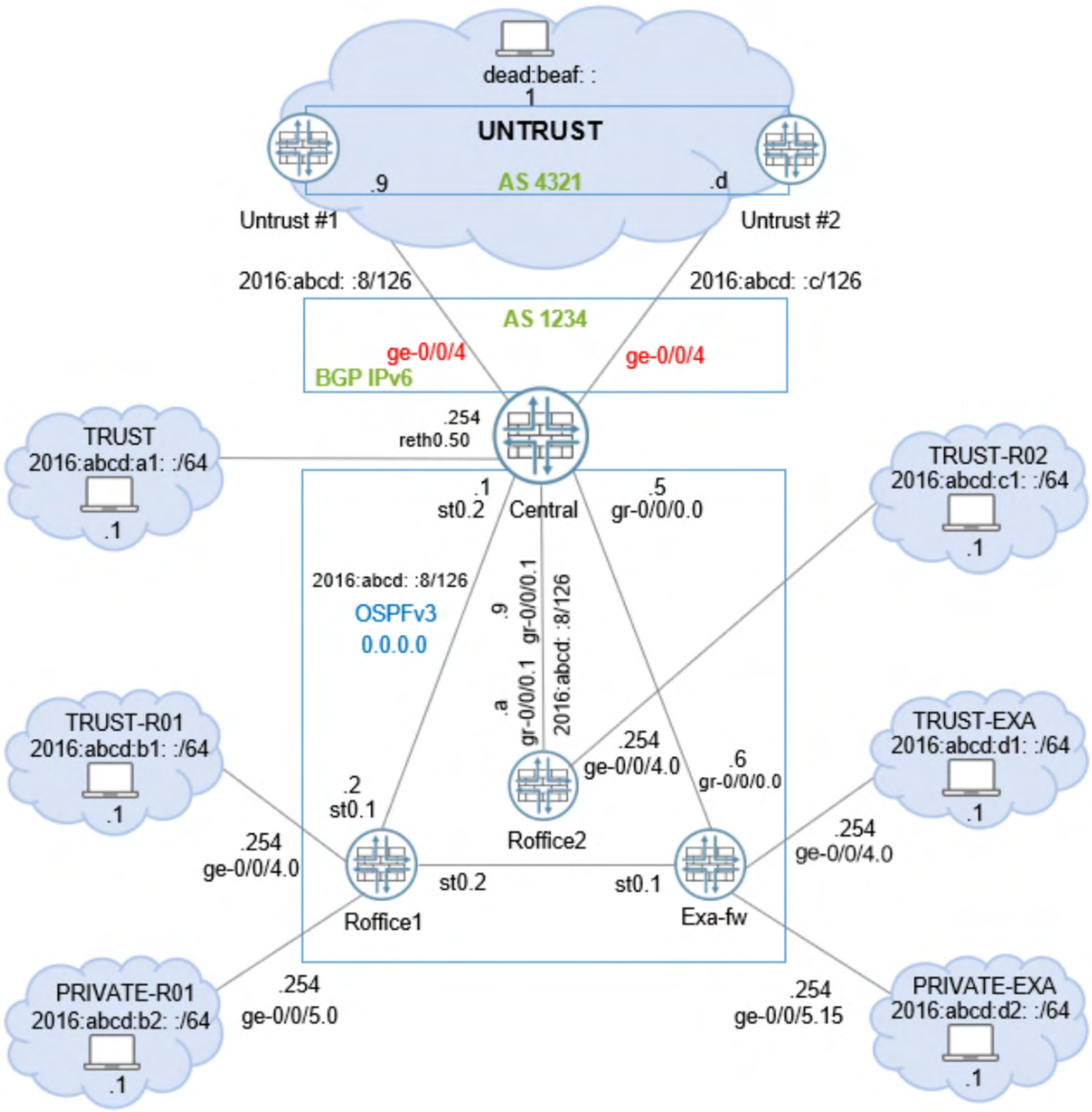


Figure 4: IPsec – VPNv6

© 2020 Juniper Networks, Inc. All rights reserved.

Task 8: Attack Prevention and Mitigation

1) Ensure that roffice1 and roffice2 are protected against following attacks arriving from the Internet:
    a. The TCP SYN segments flooding with the following thresholds and timer values:
        i. The destination thresholds values of 10000 TCP SYN segments per second.
        ii. Ensure that security device starts SYN Proxy protection mechanism when TCP SYN segments arrival rate reaches 500 segments per second.
        iii. Ensure that security device generates an alarm when TCP SYN segments arrival rate reaches 2500 segments per second.
        iv. The maximum time before incomplete sessions are dropped should be 10 seconds.
    b. Protect against fragmented TCP SYN segments.
    c. Protect against UDP flooding with the threshold of 500 packets per second.
2) Ensure that building1 and building2 are protected against the following reconnaissance attempts arriving from the INTERNAL security zone:
    a. IP address sweep and port scan both a detection rate of 10 packets arrived per 2 ms time interval.
    b. Detect IP packets with following values in the Options field:
        i. Record-route option.
        ii. Timestamp option.
    c. Protect against following operating systems probes:
        i. The TCP segment has both SYN and FIN flags set.
        ii. The TCP segment has no flags set.
    d. Ensure that detection of malicious traffic results in alarm generation instead of dropping the packets belonging to malicious packet flow.
3) Configure cluster in such a way to protect server 172.16.60.205 and 172.16.60.206:
    a. The uploading of exe or rpm files to the 172.16.60.206 server via FTP is allowed only from the TRUST security zone and prohibited from everywhere else. Each detected attempt results in silently dropping client's sessions.
    b. Allow anonymous access to the FTP service of the 172.16.60.206 server from any TRUST and the TESTBED security zones. Restrict access for the rest of the network. Silently drop packets from unauthorized hosts, block them for 1 hour and generate log messages with severity level Major and alert flag.
    c. Protect servers against scanning and worms from the INTERNAL and TESTBED security zones. Each detected attempt results in silently dropping packets.

© 2020 Juniper Networks, Inc. All rights reserved.

Task 9: Advanced Services – Central cluster

1) Disable application system cache completely.
2) Enable AppTrack to provide information about applications used in the TRUST zone. The first message for each connection has to be generated 2 minutes after the application has been identified and then an update has to be created every 6 minutes.
3) Ensure the junos:MEGAUPLOAD application over the port 80 from the TRUST zone to the UNTRUST zone will have the loss priority of "high" if it crosses 5000 kb/s with bursts of 15000 bytes. This has to be applied in both directions - client to server and server to client.
4) Make sure the SRX knows exactly what is going on in the encrypted sessions on the default HTTPS port from the TESTBED zone to the UNTRUST zone. The certificate for signing the modified server certificates should be locally generated on the SRX device with following values:
   - type: rsa
   - key size: 512
   - domain name: juniper.net
   - subject: DC=JNPR,CN=juniper,OU=unit-1,O=juniper,SN=1234,L=USA,ST=CA,C=US
   - email-ID: noreply@juniper.net

   The SRX will not authenticate any servers. Make sure everything about SSL proxy operations is logged in the “ssl-proxy” file.

5) Remote Desktop Protocol traffic originated in the INTERNAL zone, leaving the Central Office should always travers interface ge-0/0/3.

© 2020 Juniper Networks, Inc. All rights reserved.

Task 10: Software Defined Secure Network (SDSN)

1) Create a new SkyATP realm. Enroll Policy Enforcer and the central office cluster in the newly created Sky ATP Realm through Security Director

Use the information below to setup the Sky ATP Realm:

SkyATP Realm	jnciesec-xxx (where xxx is shown in the lab access instructions)
Username	jnciesec-xxx@stu.juniper.net
Password	lab123@Lab
Juniper SSO account	eduservicenow@gmail.com
Juniper SSO password	********

Use the information for Security Director and Policy Enforcer:

Security Director Username	super
Security Director Password	lab123@Lab
Security Director IP	10.10.1.100
Policy Enforcer Username	root
Policy Enforcer Password	lab123@Lab
Policy Enforcer IP	10.10.1.123

Note: The password for the Juniper SSO account is auto populated in the Firefox browser on the Student Desktop. For this reason, it is important to use the Firefox browser on the Student Desktop to create the Sky ATP realm

2) Setup for SkyATP with SDSN in Security Director, ensure that HTTP traffic is analyzed at the central cluster (srx3/srx4) for threat levels greater than 6 for the 172.16.50.100 host. Ensure that connections are silently dropped at access switch vQFX if the 172.16.50.100 host becomes infected with malware. Ensure that only blocked traffic is logged. (Note that this includes C&C protection).

© 2020 Juniper Networks, Inc. All rights reserved.

Appendices

The following section provides the detailed explanation of the previous chapters and practice exam tasks. Here you will find details about the configuration and verification steps required to complete each section.

© 2020 Juniper Networks, Inc. All rights reserved.

Appendix - Chapter 1: General System Features

This appendix provides solution details for chapter one which is focused on initial system configuration and general system features.

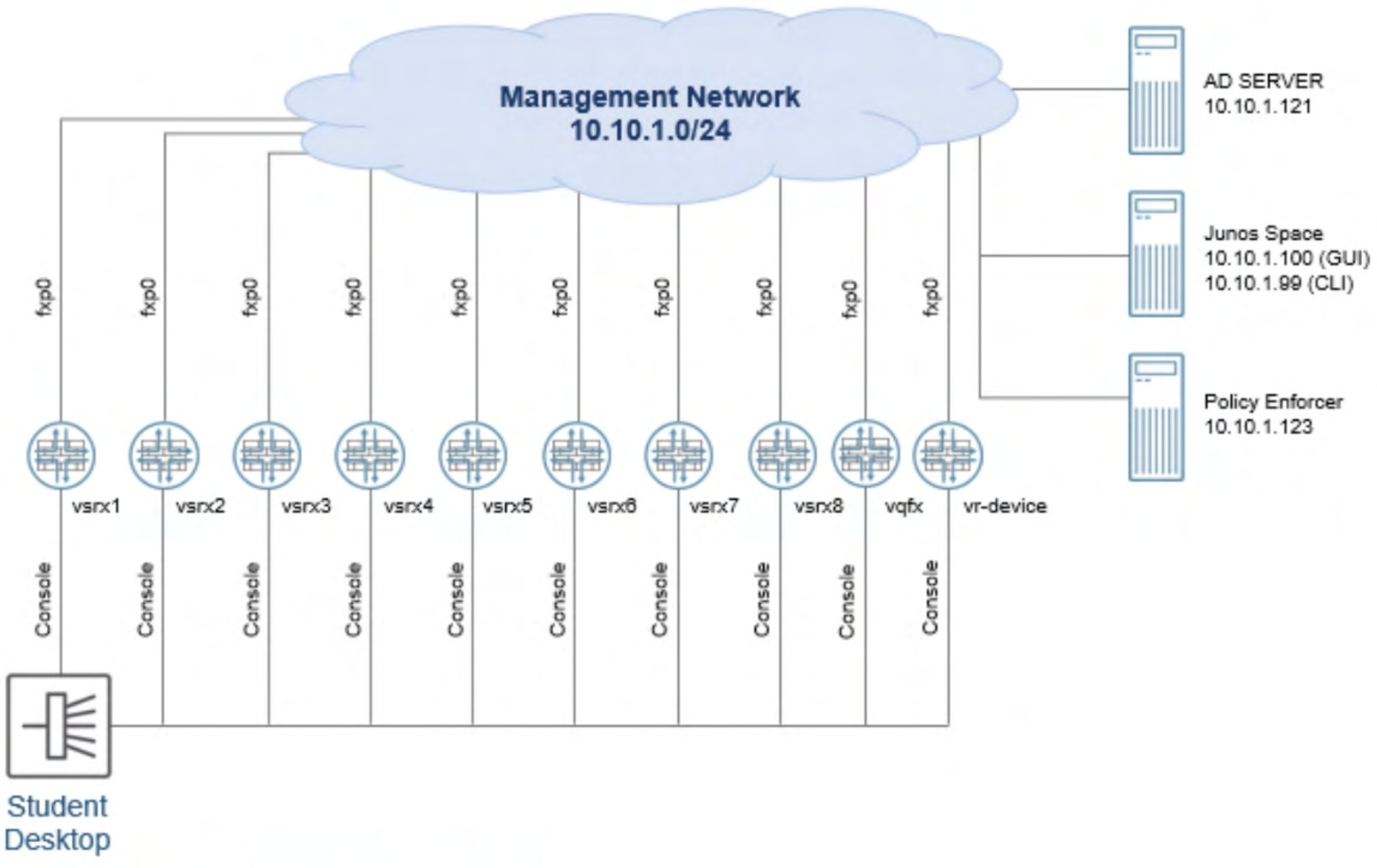


Figure 1: Chapter 1 – Management Topology

© 2020 Juniper Networks, Inc. All rights reserved.

Task 1: Initial Configuration

Note: Because many tasks in this chapter require performing the same or very similar configuration on multiple devices it is suitable to use "copy and paste" approach, e.g. create the configuration on one device copy it to notepad, make changes if needed, copy it to clipboard and then paste it on other device using the "load merge terminal" or "load merge terminal relative" commands. This approach can result in significant time saving which is a huge advantage in the real exam where time is of the essence. Therefore, it is advisable to use this approach whenever possible.

1) Configuring hostname is an easy task performed in the configuration mode using the following commands:

```
[edit]
root@device1# set system host-name srx1

[edit]
root@device1# commit

[edit]
root@srx1#
```

Perform the above procedure on each device and use values according to the defined table.

Device	Hostname
vSRX1	srx1
vSRX2	srx2
vSRX3	srx3
vSRX4	srx4
vSRX5	srx5
vSRX6	srx6
vSRX7	srx7
vSRX8	srx8

© 2020 Juniper Networks, Inc. All rights reserved.

2) As depicted in the topology graphic all SRX devices use the fxp0 interface for the connection to the management network, e.g.it is management interface. The fxp0 and the lo0 interfaces have to be configured according the table below.

Hostname	Management IP address	Loopback IP address
srx1	10.10.1.1/24	192.168.1.1/32
srx2	10.10.1.2/24	192.168.1.2/32
srx3	10.10.1.3/24	192.168.1.3/32
srx4	10.10.1.4/24	192.168.1.4/32
srx5	10.10.1.5/24	192.168.1.5/32
srx6	10.10.1.6/24	192.168.1.6/32
srx7	10.10.1.7/24	192.168.1.7/32
srx8	10.10.1.8/24	192.168.1.8/32

To configure an IP address for the management and for the loopback interfaces following commands need to be used:

```
[edit]
root@srx1# set interfaces fxp0 unit 0 family inet address 10.10.1.1/24

[edit]
root@srx1# set interfaces lo0 unit 0 family inet address 192.168.1.1/32
```

Execute these commands with respective IP addresses on each device.

Enabling the service is done under the “edit system services” stanza. Following commands allow telnet, SSH with allowed root access, HTTP and HTTPS. The HTTPS requires a certificate for operation. Either system generated certificate can be defined or a custom certificate can be loaded on the device and then used.

```
[edit]
root@srx1# edit system services

[edit system services]
root@srx1# set telnet

[edit system services]
root@srx1# set ssh root-login allow
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
[edit system services]
root@srx1# set web-management http

[edit system services]
root@srx1# set web-management https system-generated-certificate
```

Device	Hostname
srx1	SSH with allowed root access, telnet, HTTP, HTTPS
srx2	SSH with allowed root access, telnet, HTTP, HTTPS
srx3	SSH with allowed root access, telnet, HTTP, HTTPS
srx4	SSH with allowed root access, telnet, HTTP, HTTPS
srx5	SSH with allowed root access, telnet, HTTP, HTTPS
srx6	SSH with allowed root access, telnet, HTTP, HTTPS
srx7	SSH with allowed root access, telnet, HTTP, HTTPS
srx8	SSH with allowed root access, telnet, HTTP, HTTPS

3) The maximum connections per minute can be defined under each system service. The following commands set the limit to maximum 5 connections per minute for SSH and telnet.

   Execute these commands on each device.

```
[edit system services]
root@srx1# set telnet rate-limit 5

[edit system services]
root@srx1# set ssh rate-limit 5
```

   In addition to connections per minute, the Junos is capable of limiting the number on simultaneous connections. The configuration statement below defines that maximum 5 parallel FTP connections can be established to the system. It can be defined for SSH and telnet too. This is not required by any of the tasks in this section but could be asked of candidates on the exam.

```
[edit system services]
root@srx1# set ftp connection-limit 5
```


© 2020 Juniper Networks, Inc. All rights reserved.

To check if the system also runs these services you can try to connect to the fxp0.0 interface IP address with telnet, SSH, HTTP or HTTPS from the student desktop or another Junos device.

```
#telnet 10.10.1.1
Trying 10.10.1.1...
Connected to 10.10.1.1.
Escape character is '^]'.

srx1 (ttyp0)

login:
```

```
#ssh root@10.10.1.1
The authenticity of host '10.10.1.1 (10.10.1.1)' can't be established.
ECDSA key fingerprint is 26:a8:73:4e:a7:d9:09:c0:38:b4:f6:d7:bd:1b:e7:42.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.10.1.1' (ECDSA) to the list of known hosts.
root@10.10.1.1's password:
```

Task 2: Authentication and Authorization

Junos uses user accounts as one way for providing access to the device, i.e. authentication. Other options are RADIUS and TACACS+. For each user account you need to define the login name, authentication method/s, access privileges and optionally the identification information for that user. Each user who can log in to the device must belong to exactly one login class. However multiple users can belong to the same login class. The login class is device means to define privileges and permissions for users, namely:

- Access privileges that users have when they are logged in to the router or switch
- Commands and statements that users can and cannot specify
- How long a login session can be idle before it times out and the user is logged out

The system has four predefined login classes with following permissions:

- operator – clear, network, reset, trace, and view
- read-only – view
- superuser or super-user – all
- unauthorized – None

© 2020 Juniper Networks, Inc. All rights reserved.

In this part you will configure new users allowed to access the devices and define their privileges and permissions.

1) Because the new user **lab** should have the super-user privileges it is sufficient to associate it with the predefined login class “super-user” and a password of “lab123”.

```
[edit system services]
root@srx1# top edit system

[edit system]
root@srx1# set login user lab class super-user

[edit system]
root@srx1# set login user lab authentication plain-text-password
New password:
Retype new password:
```

2) Custom login classes need to be created as the definitions in the table below cannot be satisfied with the predefined login classes.

Username	Password	Device	Privileges
ronly	ronly123	All	Has permission “view” and “view-configuration”. Additionally, can NOT execute the “file delete” command.
admin1	admin123	All	Has permissions “all”. Can access the configuration mode only using “configure private” command.
restricted	restricted123	All	Has permissions “clear” and execute only the “show system uptime”, “show system storage” and “show interface terse” commands and nothing else.

The custom login class definition contains multiple parameters:

- permissions – predefined sets of commands allowed to be executed
- allow-commands – string or regular expression. Matching operational mode commands that are allowed to be executed, even if the defined permissions do not contain it
- allow-configuration - string or regular expression. Matching configuration mode commands that are allowed to be executed, even if the defined permissions do not contain it
- deny-commands – string or regular expression. Matching operational mode commands that are denied

© 2020 Juniper Networks, Inc. All rights reserved.

- deny-configuration - string or regular expression. Matching configuration mode commands that are denied

Note: Matching of the “allow-“ statements are done after matching of the “deny-“ statements. If a command matches both “deny-“ and “allow-“ statements it is allowed.

The following configuration excerpt defines the custom login classes, new users and associates them with the appropriate login class as per the table above.

```
[edit system]
root@srx1# edit login

[edit system login]
root@srx1# show
class admin-class {
    permissions all;
    allow-commands "configure private";
    deny-commands configure;
}
class restricted-class {
    permissions clear;
    allow-commands "(show system uptime)|(show system storage)|(show interfaces
terse)";
}
class ronly-users {
    permissions [ view view-configuration ];
    deny-commands "file delete";
}
user admin1 {
    class admin-class;
    authentication {
        encrypted-password "$1$NOYK1.5s$BOx9aqrmXqmYs0lAlSpe.1"; ## SECRET-DATA
  }
}
user restricted {
    class restricted-class;
    authentication {
        encrypted-password "$1$HbJ7opMi$m4u9az/NPVWFWYj89dxcB."; ## SECRET-DATA
    }
}
user ronly {
    class ronly-users;
    authentication {
        encrypted-password "$1$phAybng3$.mzWOja48SjPKWcXOAD2n/"; ## SECRET-DATA
    }
}
```


© 2020 Juniper Networks, Inc. All rights reserved.

Task 3: Syslog

Syslog is a standard for computer data logging, i.e. protocol of passing data, priority, severity and description messages to a server. Syslog messages refer to a facility (auth, kern, syslog, user, local0,local7, …) and are assigned a severity (Emergency, Alert, Critical, Error, Warning, Notice, Info or Debug) by the sender of the message.

1) The syslog configuration in Junos consists of 3 main elements – destination (where the messages will be forwarded), facility (message source, e.g. who generated the message) and severity (message importance). These three elements can be repeated multiple times to achieve the desired behavior in handling the syslog messages. The configuration shown below ensures the following behavior in syslog messages distribution:
   a. All “emergency” messages regardless of the facility are displayed on terminals of all currently logged users.
   b. All messages regardless of the facility with the severity of “critical” and higher are sent to the default syslog file.
   c. A file named “interactive-commands” with command audit trail is maintained, i.e. file with records about the users and commands they execute.
   d. A separate file named “security-policy-logs” is used for security policy log entries. The system retains 20 archive files each with size of 512 KB (524288 B).
   e. A separate file named “authorization-file” is used for authorization messages with the severity “info” and higher.
   f. All “emergency” messages regardless of the facility are sent to the syslog server at 10.10.1.254. A non-physical address is used as source address for the syslog messages.
   g. The information about the year should be included in the messages.

```
[edit system login]
root@srx1# up

[edit system]
root@srx1# show syslog
user * {
    any emergency;
}
host 10.10.1.254 {
    any emergency;
source-address 192.168.1.1;
}
file messages {
    any critical;
}
file interactive-commands {
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
    interactive-commands info;
}
file security-policy-logs {
    user info;
    match RT_FLOW;
    archive size 512k files 20;
}
file authorization-file {
    authorization info;
}
time-format year;
```

Task 4: NTP

Network Time Protocol (NTP) is a networking protocol for clock synchronization between computer systems over packet-switched, variable-latency data networks. It is a client-server protocol, where each device can act as client, server or combination. The Junos default behavior is to slowly step clocks to achieve synchronization with the server in case the difference between local time and server time is more than 128 ms. However, if the difference is greater than 1000 seconds the local device will not synchronize, and a message will be generated about setting the time manually with the “set date” operational mode command. Junos supports following modes: client mode, symmetric active mode, broadcast mode and server mode.

1) The following command sets the time zone for the device.

```
[edit system]
root@srx1# set time-zone America/Los_Angeles
```

2) The following configuration command defines the NTP server reachable at 10.10.1.254.

```
[edit system]
root@srx1# edit ntp

[edit system ntp]
root@srx1# set server 10.10.1.254
```

Alternatively, to configure the device to use another server’s time during booting instead of its own the following configuration has to be done:

```
[edit system ntp]
root@srx1# set boot-server 10.10.1.254
```

The command below tells the device to use specific source address for the NTP packets. Use appropriate IP address, e.g. loopback IP address, for each device:

© 2020 Juniper Networks, Inc. All rights reserved.

```
[edit system ntp]
root@srx1# set source-address 192.168.1.1
```

3) To make the srx1, srx2 and srx8 devices use the MD5 authentication with the key set to “bootcamp” for NTP, issue following commands on each of these three devices:

```
[edit system ntp]
root@srx1# set authentication-key 1 type md5 value jncie

[edit system ntp]
root@srx1# set server 10.10.1.254 key 1
```

To let the devices, accept only updates with the same key is done with following command:

```
[edit system ntp]
root@srx1# set trusted-key 1
```

Task 5: SNMP

Simple Network Management Protocol (SNMP) is an Internet-standard protocol for managing devices on IP networks. Network management information is exchanged between SNMP agent run on a device and network management system. The management system sends request to the agent, such as request for information or actions. The agent in addition to responding to these requests also controls the access the management information base (MIB), which a collection of viewable or changeable objects. The SNMP also allows sending traps or notifications when significant events, (an interface going down, etc.) occur on the device. Junos supports SNMP v1, v2c and v3. The SNMP configuration is located under the [edit snmp] hierarchy.

1) The commands below define to accept read-only SNMP requests only from the NMS system located at 10.10.1.254 using the community string “reading”.

```
[edit system ntp]
root@srx1# top edit snmp

[edit snmp]
root@srx1# set community reading clients 10.10.1.254/32

[edit snmp]
root@srx1# set community reading authorization read-only
```

2) The following configuration excerpt defines to send the SNMP traps listed below to the NMS system:
   a. Authentication failures

© 2020 Juniper Networks, Inc. All rights reserved.

b. Hardware and environment
c. Link transitions
d. Routing protocol

```
[edit snmp]
root@srx1#  show | find trap-group
trap-group test-group {
    categories {
        authentication;
        chassis;
        link;
        routing;
    }
    targets {
        10.10.1.254;
    }
}
```

3) The listed commands define the SNMP contact, description and location with values "Admin user", "JNCIE-SEC device" and "Sunnyvale rack" respectively.

```
[edit snmp]
root@srx1# set contact "Admin user"

[edit snmp]
root@srx1# set description "JNCIE-SEC device"

[edit snmp]
root@srx1# set location "Sunnyvale rack"
```

The system location details, rack number and floor are defined under [edit system location] stanza:

```
[edit system location]
lab@srx1# show
floor 1;
rack 1;
```

4) The following commands ensure that Junos Space and the SRX devices can communicate through SNMP.

```
[edit snmp]
root@srx1# show
community JNCIE;
trap-group space {
    targets {
        10.10.1.121;
    }
}
```


© 2020 Juniper Networks, Inc. All rights reserved.

Appendix - Chapter 2: High availability

This appendix provides details about the solution for the chapter two which is focused on system clustering.

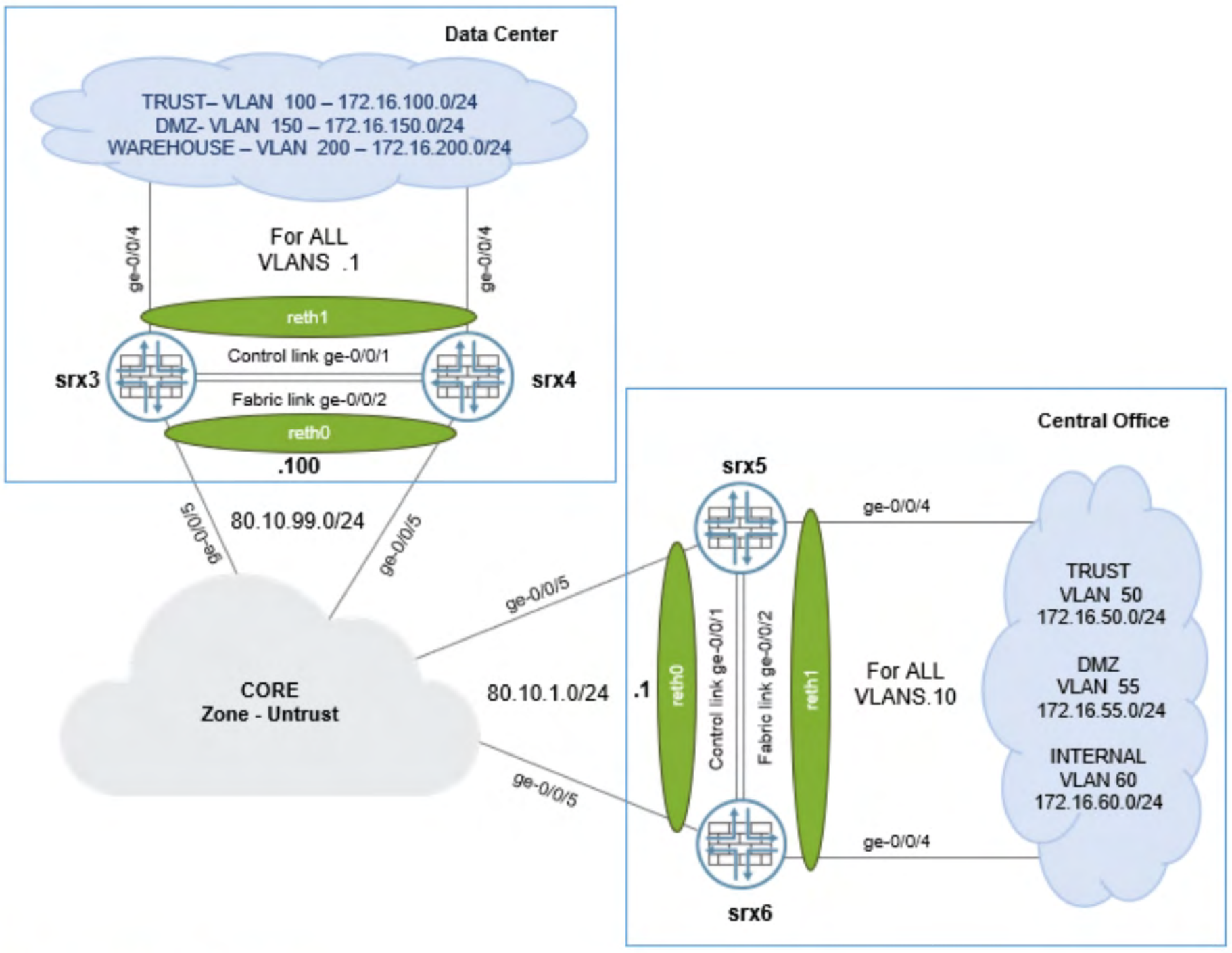


Figure 1: Chapter 2 Topology

Junos security platforms use chassis clustering for providing high-availability. A chassis cluster consists of grouped pair of SRX series connected to each other with control and data links. The control link connection is used to synchronize the configuration and kernel state. The data link uses only revenue ports as fab interfaces on all models and is used to synchronize sessions for redundancy and for transmitting the cross-node data traffic. In chassis cluster both member devices must be the same model having the same hardware revision and cards - SPCs, network processing cards (NPCs), and input/output cards (IOCs) on high-end platforms - placed in the same slots. In this setup the chassis cluster

© 2020 Juniper Networks, Inc. All rights reserved.

provides network node redundancy with stateful failover of processes and services in the event of system or hardware failure.

The control plane operates in active-backup mode whereas the data plane can operate in active/passive or active/active modes depending on the configuration.

The main chassis clusters components are cluster nodes, redundancy groups and redundant ethernet interfaces. Each cluster is identified by an identifier called “cluster-id” from the range 1-15. The cluster members are called nodes. Because each cluster can consist of maximum two devices “node-id” is used for their designation - node 0 or node 1. Each device can belong to only one cluster at any time. When the cluster forms the interface names on the node 1 are changed to reflect the cluster setup. Specifically, the FPC number changes according this formula on node 1: max FPC slots on given device model + standalone FPC slot number.

A redundancy group (RG) is an abstract construct that includes and manages a collection of objects. An RG has objects on both nodes and is primary on one node and secondary on the other at any time. The objects are active on the node where the RG is active to which they belong. RGs are independent units from the failover perspective, i.e. each redundancy group fails over from one node to the other independently from all other redundancy groups. In case of failover all objects belonging to the redundancy group failover together to the other node, i.e. become active. RG0 is reserved and created automatically for routing engines. It manages the primacy of REs, i.e. the routing engine is active on the node where the RG0 is active. All other RGs manage interface redundancy and need to be explicitly defined in the configuration. RG except RG0 can contain up to 15 redundant Ethernet interfaces. The RG primacy is determined by the following things – node priority, node-id and node initialization time. Node with higher priority has the RG is primary. If both nodes have the same priority for the RG it will be primary on the node with lower node-id. If one node boots up and initializes before the other all RGs will be primary on that node unless the preempt option is used. Each RG having the preempt option enabled will be primary on the node with higher priority whenever possible. However, the preempt option is not supported on RG0. Each RG can have defined which interfaces and/or IP addresses to monitor, i.e. checking the interface status – up or down, and the IP address reachability. When a failure is detected – monitored interface or IP address – a failover happens depending whether the weight of failed objects reaches the RG failover threshold of 255.

A reth is a pseudo-interface that includes a physical interface from each node of the cluster. A redundant Ethernet interface must contain, at minimum, a pair of Fast Ethernet interfaces or a pair of Gigabit Ethernet interfaces that are referred to as child interfaces of the redundant Ethernet interface (the redundant parent). If more than two interfaces are assigned to the reth a link aggregation group is created automatically from all children interfaces on the same node. The children interface of reth must be the same kind (fast or gigabit or 10gigabit ethernet) but do not need to be in the same slots on the nodes. The

© 2020 Juniper Networks, Inc. All rights reserved.

association to the reth interface is done in the child interface configuration. The reth configuration contains association to the RG and properties that inherited by the child interfaces. Only child interfaces on the node where the RGs is primary to which the reth belong are active.

The chassis cluster requires both links – control and data – to be up and operational. If one of them fails, the node with RG0 active disables the other node to prevent split brain situation. Once the connection is recovered the disabled node needs to be rebooted to join the cluster. To minimize this situation Junos security allows defining the redundant fabric links on all modes. The redundant control links are available only on the high-end devices, but certain restriction apply, e.g. for SRX5000 series devices each node must be equipped with 2nd RE, on SRX3000 series a SCM module is required on each device.

Few things to remember:

- ***Both nodes must run the same Junos software***
- ***Preempt is not available for RG0***
- ***Each node must have its own license for licensed features, such as UTM, IDP, AppSecure, etc.***

Task 1: Creating Clusters – Initial Setup

Note: Before executing the activities in this part ensure the configuration on all cluster nodes is prepared. The vSRX branch devices in cluster mode use dedicated ports (not configurable) for the management port (fxp0) and control link (em0).

Each cluster is identified by its cluster-id (value 1-15) and consists of 2 nodes, node 0 and node 1. To create the cluster, you must choose cluster-id value for it and then perform following operational mode command on each node, starting usually with node 0.

1) Perform the procedure above to create clusters as the defined in table below.

Device	Node id	Cluster id
srx3	0	1
srx4	1	1
srx5	0	2
srx6	1	2

© 2020 Juniper Networks, Inc. All rights reserved.

Note: Forming the cluster requires that the device's reboot. Therefore, it is suitable to execute the following commands and perform the initial configuration tasks using the console connection.

Node 0:

```
root@srx3>set chassis cluster cluster-id 1 node 0 reboot
```

Node 1:

```
lab@srx4>set chassis cluster cluster-id 1 node 1 reboot
```

To check the status of the cluster after the device's reboot you can use the following command:

```
{primary:node0}
lab@srx3> show chassis cluster status
Cluster ID: 1
Node name         Priority     Status       Preempt Manual failover
Redundancy group: 0 , Failover count: 1
node0       1            primary      no           no
node1       1            secondary    no           no
```

2) As mentioned earlier the branch devices have fixed definition which ports are used for management and the control link (fxp0 and em0). The fabric link on the other hand requires manual configuration. Based on the instructions the ge-0/0/2 ports should be used for fabric link on all clusters and their members.

As the cluster is already formed the configuration needs to be performed only on 1 member, preferably on the primary node.

Note: Keep in mind the interface names/numbers in cluster setup. The FPC number starts from value 7 on node1.

```
{primary:node0}[edit]
lab@srx3# set interfaces fab0 fabric-options member-interfaces ge-0/0/2

{primary:node0}[edit]
lab@srx3# set interfaces fab1 fabric-options member-interfaces ge-7/0/2
```

The automatic reboot of the disabled node after control link failure recovery is done using the following statement.

© 2020 Juniper Networks, Inc. All rights reserved.

```
{primary:node0}[edit]
lab@srx3# set chassis cluster control-link-recovery

{primary:node0}[edit]
lab@srx3# commit
```

3) To configure parameters specific for each node the Junos groups need to be used and applied correctly.

The following configuration excerpt defines and applies the hostname and management IP address for the fxp0 interface on each node. The configuration excerpt is from cluster 1.

Cluster-id/Node-id	Hostname	Management IP address
1/0	srx3	10.10.1.3/24
1/1	srx4	10.10.1.4/24
2/0	srx5	10.10.1.5/24
2/1	srx6	10.10.1.6/24

To keep the configuration clean, delete the hostname configuration and the fxp0 and lo0 interfaces:

```
{primary:node0}[edit]
lab@srx3# delete system host-name

{primary:node0}[edit]
lab@srx3# delete interfaces fxp0

{primary:node0}[edit]
lab@srx3# delete interfaces lo0
```

Use the same approach for defining node specific parameters on cluster 2.

```
{primary:node0}[edit]
lab@srx3# show groups
node0 {
    system {
        host-name srx3;
    }
    interfaces {
        fxp0 {
            unit 0 {
                family inet {
                    address 10.10.1.3/24;
                }
            }
        }
    }
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
}
node1 {
    system {
        host-name srx4;
    }
    interfaces {
        fxp0 {
            unit 0 {
                family inet {
                    address 10.10.1.4/24;
                }
            }
        }
    }
}

{primary:node0}[edit]
lab@srx3# set apply-groups "${node}"
```

Configuring the loopback address is done the same way as in standalone mode (see below). However, in cluster setup only one RE is active at a time and therefore hosts also the loopback interface. In case of RE failover the loopback will be moved to the new active RE.

```
{primary:node0}[edit]
lab@srx3# set interfaces lo0 unit 0 family inet address 192.168.1.3/32

{primary:node0}[edit]
lab@srx3# commit
```

The configuration needs to be done only on one node within the cluster. The cluster takes care of synchronizing the configurations. The following loopback addresses need to be configured on the clusters using the approach above:

Cluster-id	Management IP address
cluster 1	192.168.1.3/32
cluster 2	192.168.1.5/32

© 2020 Juniper Networks, Inc. All rights reserved.

Task 2: Configuring Redundancy Groups and Redundant Ethernet Interfaces

1) The RG0 is reserved for routing engines (this behavior cannot be changed). In SRX cluster every redundancy group can have priorities associated with each node. Normally the RG is active on the node with higher priority and in case of failure the RG becomes active on the other node. Upon failure recovery the failback is dependent whether the RG has the **preempt** parameter defined or not. If defined the RG will be always active on the available node with the highest priority, if not the RG will remain active on the current node. According to the task instructions the node 0 should be normally primary for the RG0 on both clusters. The following configuration excerpt performs that:

```
{primary:node0}[edit chassis cluster]
lab@srx3# show redundancy-group 0
node 0 priority 200;
node 1 priority 100;
```

Note: The preempt parameter cannot be defined for RG0. However manual failover for RG0 is possible.

2) Based on the topology image the following reths need to be created (keep in mind the interface renaming in cluster environment).

Cluster-id	Reth	Reth children
1	reth0	ge-0/0/5, ge-7/0/5
1	reth1	ge-0/0/4, ge-7/0/4
2	reth0	ge-0/0/5, ge-7/0/5
2	reth1	ge-0/0/4, ge-7/0/4

The cluster needs to be explicitly told how many reth interfaces it should create. It might be useful to do it at the beginning of the reth configuration to prevent commit errors.

```
{primary:node0}[edit chassis cluster]
lab@srx3# set reth-count 2
```


© 2020 Juniper Networks, Inc. All rights reserved.

The next step is to associate the children interfaces with their parent reth interface.

```
{primary:node0}[edit interfaces]
lab@srx3# set ge-0/0/5 gigether-options redundant-parent reth0

{primary:node0}[edit interfaces]
lab@srx3# set ge-7/0/5 gigether-options redundant-parent reth0

{primary:node0}[edit interfaces]
lab@srx3# set ge-0/0/4 gigether-options redundant-parent reth1

{primary:node0}[edit interfaces]
lab@srx3# set ge-7/0/4 gigether-options redundant-parent reth1
```

Then the actual reth interface configuration remains. Based on the topology image reth0 is an IP interface without VLAN tagging and the reth1 is VLAN tagged interface (connects to 3 VLANs).

```
{primary:node0}[edit interfaces]
lab@srx3# set reth0 unit 0 family inet address 80.10.99.100/24

{primary:node0}[edit interfaces]
lab@srx3# set reth1 vlan-tagging

{primary:node0}[edit interfaces]
lab@srx3# set reth1 unit 100 vlan-id 100

{primary:node0}[edit interfaces]
lab@srx3# set reth1 unit 100 family inet address 172.16.100.1/24

{primary:node0}[edit interfaces]
lab@srx3# set reth1 unit 150 vlan-id 150

{primary:node0}[edit interfaces]
lab@srx3# set reth1 unit 150 family inet address 172.16.150.1/24

{primary:node0}[edit interfaces]
lab@srx3# set reth1 unit 200 vlan-id 200

{primary:node0}[edit interfaces]
lab@srx3# set reth1 unit 200 family inet address 172.16.200.1/24
```

Perform the same procedure on cluster 2. Please ensure you use to correct VLAN IDs and IP addresses.

© 2020 Juniper Networks, Inc. All rights reserved.

3) Cluster 1:
    a. To allow independent reth interface failover between nodes each reth needs to have its "own" redundancy group, i.e. each redundancy group will have only 1 reth interface associated. This means for current setup 2 RGs are needed – RG1 and RG2, where RG1 will have reth0 associated and RG2 will have reth1 associated.
    b. To equally distribute the two RGs between nodes the node priorities in the redundancy groups have to be correctly specified. For example:
        i. RG1 will have node0 as primary (priority 200) and node1 as secondary (priority 100)
        ii. RG2 will have node0 as secondary (priority 100) and node1 as primary (priority 100)
        In addition, the **preempt** parameter has to be defined, to ensure RG1 will be always active on node0 and RG2 on node1 in case both nodes are available.
    c. According to the setup RGs need to monitor interfaces as listed in the table below:

Redundancy Group	Monitored interfaces
RG1	ge-0/0/5, ge-7/0/5
RG2	ge-0/0/4, ge-7/0/4

As each monitored interface should cause failover their weight needs to be defined as value of 255, which is the failover threshold for redundancy groups.

The following configuration excerpt covers that:

```
{primary:node0}[edit chassis cluster]
lab@srx3# show | find "redundancy-group 1"
redundancy-group 1 {
    node 0 priority 200;
    node 1 priority 100;
    preempt;
    interface-monitor {
        ge-0/0/5 weight 255;
        ge-7/0/5 weight 255;
    }
}
redundancy-group 2 {
    node 0 priority 100;
    node 1 priority 200;
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
    preempt;
    interface-monitor {
        ge-7/0/4 weight 255;
        ge-0/0/4 weight 255;
    }
}
```

The configuration excerpt below lists the reth interfaces configuration that the result of the commands from step 5) plus the association between reth interfaces and the respective redundancy groups:

```
{primary:node0}[edit interfaces]
lab@srx3# show | find "reth0 {"
reth0 {
    redundant-ether-options {
        redundancy-group 1;
    }
    unit 0 {
        family inet {
            address 80.10.99.100/24;
        }
   }
}
reth1 {
vlan-tagging;
redundant-ether-options {
    redundancy-group 2;
    }
    unit 100 {
    vlan-id 100;
        family inet {
            address 172.16.100.1/24;
        }
    }
    unit 150 {
    vlan-id 150;
        family inet {
            address 172.16.150.1/24;
        }
    }
    unit 200 {
    vlan-id 200;
        family inet {
            address 172.16.200.1/24;
        }
    }
}
```


© 2020 Juniper Networks, Inc. All rights reserved.

4) Cluster 2:
    a. Requirements in this case mention that the cluster scenario should be active-passive, where one node will be active and carry traffic and the other node will be standby. Therefore, only one redundancy group is needed and all reth interfaces will be associated with it.
    b. Because there is no need for failback needed after recovery the **preempt** parameter does not have to be defined.
    c. According to the setup the RG needs to monitor all children interfaces of all reths (listed in the table below).

RG	Monitor interfaces
RG1	ge-0/0/5 , ge-7/0/5, ge-0/0/4, ge-7/0/4

As each monitored interface should cause failover their weight needs to be defined as value of 255, which is the failover threshold for redundancy group.

Note: Although not explicitly stated which node should be normally the primary one for the redundancy group it is advisable to define the node priorities anyway.

The following configuration excerpt covers that:

```
{primary:node0}[edit chassis cluster]
lab@srx5# show | find "redundancy-group 1"
redundancy-group 1 {
    node 0 priority 200;
    node 1 priority 100;
    interface-monitor {
        ge-0/0/5 weight 255;
        ge-7/0/5 weight 255;
        ge-7/0/4 weight 255;
        ge-0/0/4 weight 255;
    }
}

{primary:node0}[edit interfaces]
lab@srx5# show | find "reth0 {"
reth0 {
    redundant-ether-options {
        redundancy-group 1;
    }
    unit 0 {
        family inet {
            address 80.10.1.1/24;
        }
    }
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
}
reth1 {
    vlan-tagging;
    redundant-ether-options {
        redundancy-group 1;
    }
    unit 50 {
        vlan-id 150;
        family inet {
            address 172.16.50.10/24;
        }
    }
    unit 55 {
        vlan-id 55;
        family inet {
            address 172.16.55.10/24;
        }
    }
    unit 60 {
        vlan-id 60;
        family inet {
            address 172.16.60.10/24;
        }
    }
}
```

Note: As mentioned in the chapter the following step is informational as the redundancy group IP address monitoring functionality is available only on High-end SRX devices!

a. This step requires configuring the track-ip feature (or otherwise called IP address monitoring or simply IP monitoring). Cluster 2 has only one redundancy group (RG1) created as it should operate in active-passive mode. Therefore, IP monitoring has to be configured for this redundancy group.

Note: If the IP monitoring should be configured for multiple redundancy groups use the same approach as described here.

i. Based on the requirements and on the topology image the following IP addresses should be tracked:
   - gateway (next-hop) to the CORE network --> next-hop for the default route on cluster 2 is: 80.10.1.254
   - IP address of srx7's interface from the INTERNAL zone --> 172.16.60.1

ii. The nearest reths, e.g. the reths which the cluster uses to reach these IPs, are:
   - reth0.0 for 80.10.1.254

© 2020 Juniper Networks, Inc. All rights reserved.

- reth1.60 for 172.16.60.1

iii. Junos security software provides the possibility to check availability of the monitored IP address also from the node where the redundancy group is in secondary state, e.g. the reth's children interfaces serve as backups. This functionality checks if the backup path works before the failover is done (as it makes no sense to do the failover if the backup path is not working too). The actual configuration is very easy, just adding for each monitored IP address the "secondary-ip-address" parameter with the correct value. Here it should be incremented IP address (by one) of the reth interface:
   - for reth0.0 --> 80.10.1.2
   - for reth1.60 --> 172.16.60.11

   However, these IP addresses need to be configured on the reth interfaces as well.

iv. Multiple IP monitoring parameters can be configured in each redundancy group that define the IP monitoring behavior of that redundancy group.
   - weight – value configured for every monitored IP address. In case of IP address failure this weight is deducted from the global-threshold
   - global-weight – one value defined for each redundancy group, defines the amount that is subtracted from the redundancy group failover threshold in case the global-threshold reaches 0 or negative number
   - global-threshold – one value defined for each redundancy group; it is the limit used to determine when the IP monitoring should contribute to the redundancy group failover threshold

Note: This behavior might be bit confusing. It is important to realize that there are 2 different thresholds:

- global-threshold – used ONLY for IP monitoring purposes. It is being defined for each redundancy group separately. Only when the cumulated weights of failed IP addresses reach/cross this value than the IP monitoring for affected redundancy group has failed.
- redundancy group failover threshold – has value 255. The weights of failed interfaces and also the "global-weight" value (but only when the whole IP monitoring for that redundancy group has failed) are deducted from this threshold. In case result is 0 or negative number the RG failover is done.

Based on the given requirements the redundancy group failover should occur only when all monitored IP addresses fail. The following values define that behavior:

© 2020 Juniper Networks, Inc. All rights reserved.

- weights for each monitored IP – 100
- global-threshold – 200 --> since there are 2 monitored IP addresses each having weight of 100
- global-weight – 255 --> as mentioned both failed IP addresses should trigger redundancy group failover

i. To let the redundancy group detect the failure in 8 seconds by using 4 pings, the "retry-interval" needs to be set to 5 (means every 5 seconds a new ping will be sent)

Here is the final configuration related to IP monitoring related for cluster 2 redundancy group 1:

```
{primary:node0}[edit chassis cluster]
lab@srx5# show | find "redundancy-group 1"
redundancy-group 1 {
...
    ip-monitoring {
        global-weight 255;
        global-threshold 200;
        retry-interval 5;
        family {
            inet {
                80.10.1.254 {
                    weight 100;
                    interface reth0.0 secondary-ip-address 80.10.1.2;
                }
                172.16.60.1 {
                    weight 100;
                    interface reth1.60 secondary-ip-address 172.16.60.11;
                }
            }
        }
    }
}
```

Cluster checking: The commands below are very useful when checking the cluster, redundancy group, reth interfaces and IP monitoring status:

```
{primary:node0}
lab@srx3> show chassis cluster status

{primary:node0}
lab@srx3> show interfaces terse | match reth

{primary:node0}
lab@srx3> show chassis cluster interfaces

{primary:node0}
lab@srx3>show chassis cluster ip-monitoring status
```


© 2020 Juniper Networks, Inc. All rights reserved.

Appendix - Chapter 3: Firewall - Security policies

This appendix provides solution details for the security policies chapter. You will configure interfaces, zones and security policies on the SRX devices based on the requirements.

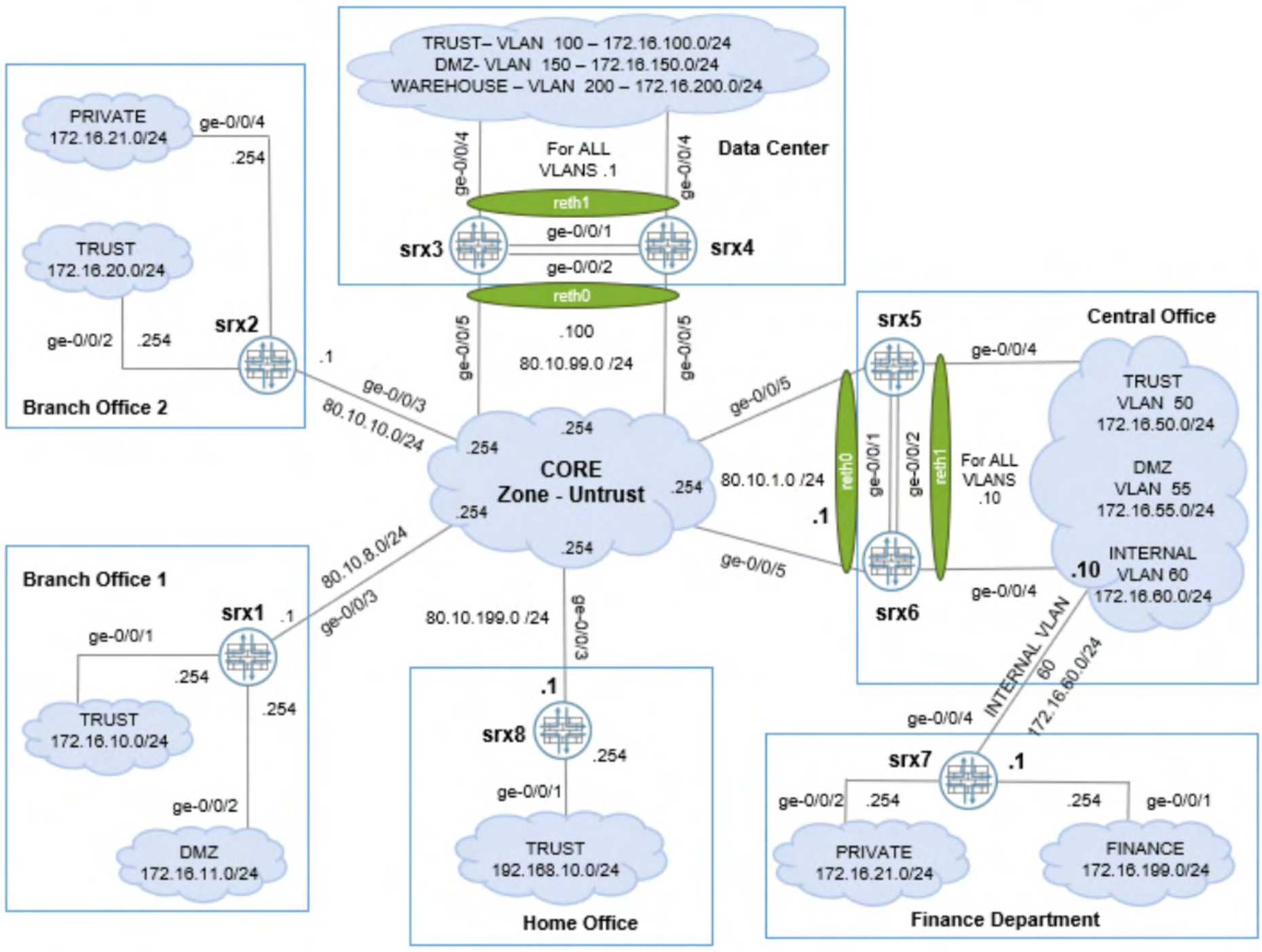


Figure 1: Chapter 3 Topology

Security policies are means that tell the Junos security platforms how to handle traffic. Security policies are unidirectional and are defined within a “from-zone to-zone” context. A security zone is a collection of one or more segments having the same security requirements. Logical unit of interfaces are assigned to zones and each logical unit can be assigned to only zone at a time. However multiple interfaces can be assigned to a single zone. In addition, when using routing-instances on the Junos device all interfaces assigned to a zone must belong to the same routing instance, i.e. whole zone must belong to only one routing-instance. Zones are either system-defined (Null zone and junos-host) and user-defined. Null zone is a default zone and all interfaces not explicitly associated through configuration with any other zone belong to it. All traffic on interfaces from the Null zone is dropped. The junos-host zone is optional and used to apply and enforce security policies

© 2020 Juniper Networks, Inc. All rights reserved.

for the self-traffic, i.e. the traffic destined for the device. In earlier Junos versions the self-traffic was controlled only through host-inbound-traffic configuration. The user-defined zones can be either functional or security. Currently only one functional zone named "management" (other names are not allowed) is available. The functional zone is used for out-of-band management by accepting only traffic destined for the device itself and cannot be used in security policies. All transit traffic received on interfaces from the management zone is dropped. The main use, but not exclusive, of the management zone is on branch devices to isolate transit traffic from management because they lack the dedicated management port fxp0 available on high end platforms. The security zone is a collection of one or more network segments requiring the regulation of inbound and outbound traffic through policies. Security zones are used in the contexts for defining security policies and therefore apply to transit traffic.

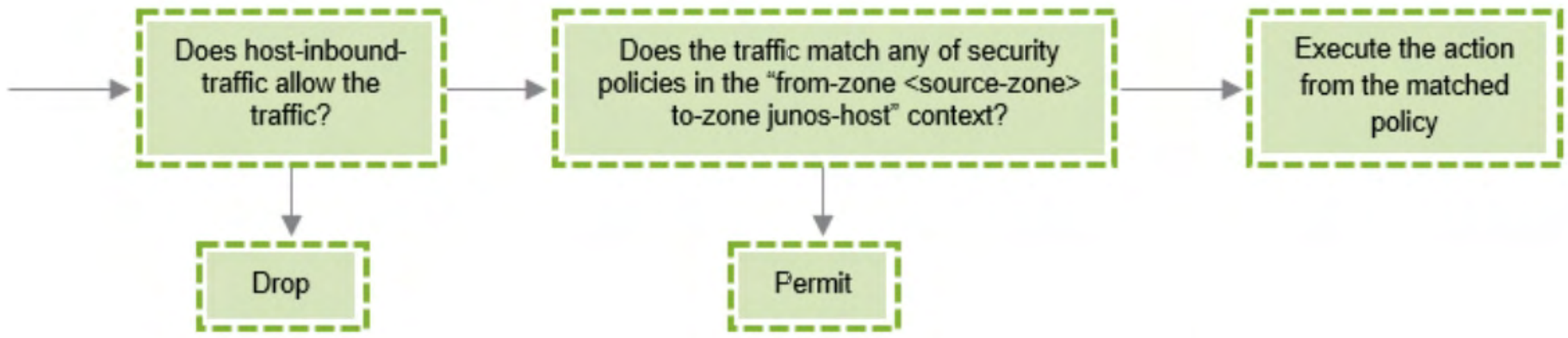
Security policies tell the device how to treat the traffic traversing from one interface to the other. If both interfaces belong to the same zone the traffic is called *intrazone*, otherwise the traffic is called *interzone*. For Junos releases before 11.4 only policies defined in the from-zone to-zone context, called also regular policies, were evaluated. If no match was found the default policy, typically with action deny, was applied. Starting from the Junos release 11.4 a so called global policies are available and the traffic processing has been adjusted. The policies are evaluated in following order until a match is found:

1. Regular policies – Security policies defined in the from-zone to-zone context and are evaluated only against traffic crossing the respective zones.
2. Global policies – Security policies defined under the [edit security policies global] hierarchy which are evaluated against all traffic regardless of the zones involved in case the regular policies processing did not result in a match.
3. Default policy – Security policy applied to all traffic not matching any regular or global policy. This policy does have only action because the condition is an implicit "catch-all" (any, any, any). The action is configured with "set security policies default-policy<permit-all|deny-all>". The default value is "deny-all".

A policy consists of a condition (or criteria) and an action. The condition includes source address, destination address and a service (combination of protocol and ports where applicable) and is matched against the traffic. If the traffic matches the condition the action – permit, deny or reject - of that security policy is executed on the traffic. Also, security policy logging and counting is configured under the action hierarchy. In addition, advanced options can be defined for the permit action, such as firewall authentication, IPsec VPNs, IDP, App identification, UTM, etc. Firewall authentication is described later in this chapter and some of other advanced features will be discussed in later chapters.

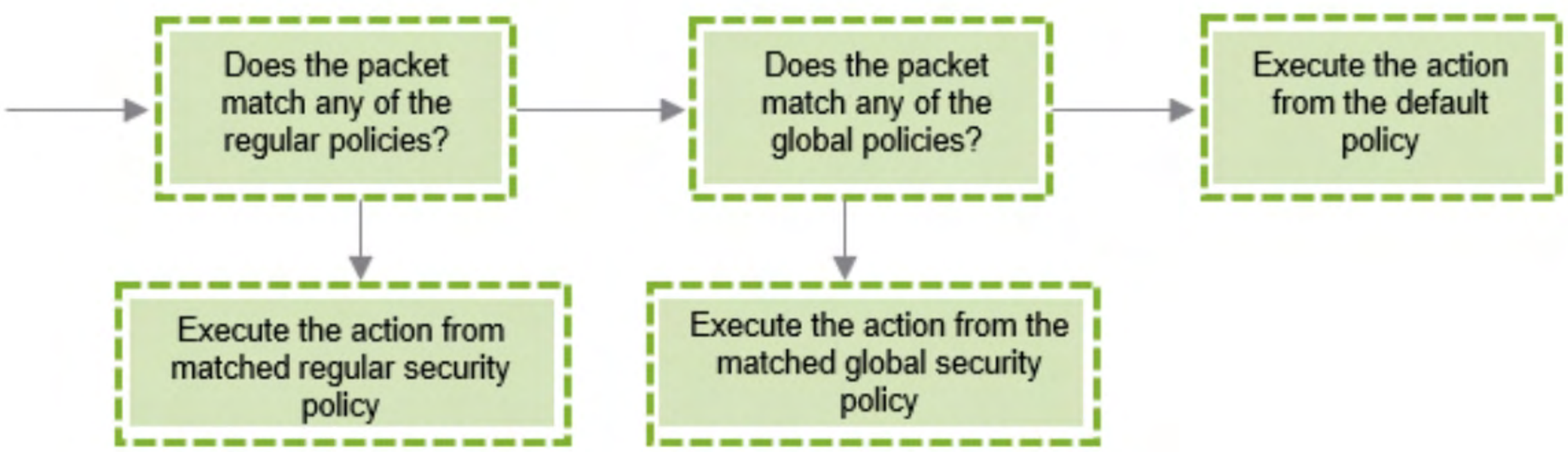
© 2020 Juniper Networks, Inc. All rights reserved.

Processing self traffic:



Self traffic not destined for the incoming interface, i.e. if the packet is destined to an interface IP address on the device but is not received on that interface, must be permitted by respective security policy first.

Processing transit traffic:



Things to remember

- ***Interface not explicitly assigned to a zone belongs to the Null zone and all traffic is being dropped.***
- ***Transit traffic on interfaces from the management zone is dropped.***
- ***Security policies are evaluated sequentially in the order as they appear in the configuration. Typically reordering policies is necessary.***
- ***The action of the default security policy is deny.***
- ***Whereas the default action for the self-traffic, e.g. for policies defined in the "from-zone <zone-name> to-zone junos-host" context, is permit. Of course, the self-traffic must be permitted in the host-inbound-traffic.***

Watch for typos in address entries and custom applications.

© 2020 Juniper Networks, Inc. All rights reserved.

Task 1: Configuring Interfaces and Security Zones

In this part you will configure interfaces, zones and assign interfaces to zones.

1) Interface configuration is pretty straightforward and no different than on any other Junos device. Below are example configuration excerpts for IP interfaces and an interface with VLANs as are outlined on the chapter topology.

```
[edit]
lab@srx7# show interfaces | find ge-0/0/1
ge-0/0/1 {
    unit 0 {
        family inet {
            address 172.16.199.254/24;
        }
    }
}
ge-0/0/2 {
    unit 0 {
        family inet {
            address 172.16.21.254/24;
        }
    }
}
ge-0/0/4 {
    vlan-tagging;
    unit 60 {
        vlan-id 60;
        family inet {
            address 172.16.60.1/24;
        }
    }
}
```

The reth interface configuration including VLANs is similar:

```
[edit]
lab@srx3# show interfaces | find reth1
reth1 {
vlan-tagging;
    unit 100 {
    vlan-id 100;
        family inet {
            address 172.16.100.1/24;
        }
    }
    unit 150 {
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
    vlan-id 150;
        family inet {
            address 172.16.150.1/24;
        }
    }
    unit 200 {
    vlan-id 200;
        family inet {
            address 172.16.200.1/24;
        }
    }
}
```

The SRX device can have two types of custom zones:

- Functional – the name used for this zone must be “management” (no other names are allowed). Interfaces associated with this zone serve solely the management purpose and do not allow any transit traffic to pass. The management zone cannot be used in security policies configuration. Typically, this zone is being used on the branch devices which do not have dedicated management port available.
- Security – user defined names are possible. Security policies are created in contexts of security zones.

The configuration below shows the association on an interface to a security zone.

Note: Do not forget to specify the logical unit number when associating interfaces to security zones. When omitting the logical unit number, the Junos automatically uses unit 0.

```
[edit security zones]
lab@srx7# show | find security-zone
security-zone FINANCE {
    interfaces {
        ge-0/0/1.0;
    }
}
security-zone PRIVATE {
    interfaces {
        ge-0/0/2.0;
    }
}
security-zone INTERNAL {
    interfaces {
        ge-0/0/4.60;
    }
}
```


© 2020 Juniper Networks, Inc. All rights reserved.

Using the approach above configure interfaces, zones and their associations according the table below.

Note: To save time the "copy and paste" approach might be helpful.

Note: The reth0 interfaces have a VLAN applied.

Device	Interface	IP address	VLAN-ID	Zone
srx1	ge-0/0/1.0	172.16.10.254/24	None	TRUST
srx1	ge-0/0/2.0	172.16.11.254/24	None	DMZ
srx1	ge-0/0/3.0	80.10.8.1/24	None	UNTRUST
srx2	ge-0/0/2.0	172.16.20.254/24	None	TRUST
srx2	ge-0/0/3.0	80.10.10.1/24	None	UNTRUST
srx2	ge-0/0/4.0	172.16.21.254/24	None	PRIVATE
Cluster1 (srx3, srx4)	reth0	80.10.99.100/24	101	UNTRUST
Cluster1 (srx3, srx4)	reth1.100	172.16.100.1/24	100	TRUST
Cluster1 (srx3, srx4)	reth1.150	172.16.150.1/24	150	DMZ
Cluster1 (srx3, srx4)	reth1.200	172.16.200.1/24	200	WAREHOUSE
Cluster2 (srx5, srx6)	reth0	80.10.1.1/24	102	UNTRUST
Cluster2 (srx5, srx6)	reth1.50	172.16.50.10/24	50	TRUST
Cluster2 (srx5, srx6)	reth1.55	172.16.55.10/24	55	DMZ
Cluster2 (srx5, srx6)	reth1.60	172.16.60.10/24	60	INTERNAL
srx7	ge-0/0/1.0	172.16.199.254/24	None	FINANCE
srx7	ge-0/0/2.0	172.16.21.254/24	None	PRIVATE
srx7	ge-0/0/4.60	172.16.60.1/24	60	INTERNAL
srx8	ge-0/0/1.0	192.168.10.254/24	None	TRUST
srx8	ge-0/0/3.0	80.10.199.1/24	None	UNTRUST

© 2020 Juniper Networks, Inc. All rights reserved.

Task 2: Local Traffic and Static Routing

The host-inbound-traffic configuration in the security or functional zone is used to control the local traffic, called also “self-traffic”. In chapter one the host-inbound-traffic configuration was done for the management access, i.e. for the functional zone called management. Here the same approach is used for allowing self-traffic on the interfaces associated with security zones. As mentioned in the brief security policy overview at the beginning of this chapter the junos-host zone provides enhanced means of controlling the self-traffic. However, to satisfy the presented tasks the host-inbound-traffic alone is fully sufficient.

The static routing configuration is located under the [edit routing-options static] hierarchy. Because the Junos security devices inherited lot of functionality from Junos routing devices the static routing configuration offers many options, such as bfd, use of rib-groups, etc. However, for the purpose of the given tasks simple static routes with next-hops are enough.

1) As all interfaces should have ping allowed the best way (easy and fast) is to allow ping in each security zone in the host-inbound-traffic statement on each device. The interfaces associated with these zones will then inherit this setting.

```
[edit security zones]
lab@srx7# set security-zone FINANCE host-inbound-traffic system-services ping

[edit security zones]
lab@srx7# set security-zone INTERNAL host-inbound-traffic system-services ping

[edit security zones]
lab@srx7# set security-zone PRIVATE host-inbound-traffic system-services ping
```

2) All interfaces connected to the CORE network are assigned to the UNTUST zone as shown on the topology image. Therefore, allowing the OSPF communication on these interfaces can be done by allowing the OSPF protocol in the UNTRUST zone. The exception is SRX7 which is connected to the cluster 2 and not to the CORE. On this device the OSPF communication is not needed at this time.

```
[edit security zones]
lab@srx1# set security-zone UNTRUST host-inbound-traffic protocols ospf
```

3) Similarly, as in previous step allowing SSH on all interfaces belonging to the zone TRUST can be achieved by allowing the SSH in this zone on every device.

```
[edit security zones]
lab@srx1# set security-zone TRUST host-inbound-traffic system-services ssh
```


© 2020 Juniper Networks, Inc. All rights reserved.

4) The static default route has 0.0.0.0/0 as the destination network and the next hop IP address is different for every device. It depends on the interface facing the CORE network. To configure default static route on each device, execute following command on each device with correct next hop value.

```
[edit]
lab@srx1# set routing-options static route 0.0.0.0/0 next-hop 80.10.8.254
```

In this topology the srx7 device is specific as it is not directly connected to the CORE network. The traffic has to go through the cluster 2. Therefore, the default route on the srx7 has as the next-hop the IP address of the reth1.60 interface on cluster 2.

```
[edit]
lab@srx7# set routing-options static route 0.0.0.0/0 next-hop 172.16.60.10
```

5) To provide connectivity for the FINANCE zone in the Finance department through the cluster 2 the following static route needs to be created on cluster 2.

```
{primary:node0} [edit]
lab@srx5# set routing-options static route 172.16.199.0/24 next-hop 172.16.60.1
```

Task 3: Security Policies

The table below lists the values referenced in the tasks.

Name	Network range
Private corporate network	172.16/16
Internet	0.0.0.0/0

The resulting security policies that need to be created are presented tabular form, containing the device, zone context (incoming zone, outgoing zone), address books values, applications and actions. In addition, for some security policies a brief description/explanation is provided.

The actual configuration (address entries, address-sets, applications, application-sets, security polices and additional needed configuration) for each device is provided at the end of this appendix chapter.

Note: The names for the address entries in the actual configurations can be arbitrary, but it is recommended to keep them meaningful. In addition, it is essential the address entries and address-sets are created in the appropriate zones.

© 2020 Juniper Networks, Inc. All rights reserved.

Note: Another very important thing to keep in mind is the order of security policy execution –the order in which they appear in the configuration defined the sequence of execution. Every time a new security policy is created in a given context of incoming zone to outgoing zone, it is always placed at the end in that context and many times reordering is needed. The command "insert" is used for policy reordering.

Branch office 1: srx 1

1) The hosts from the TRUST zone and its network range can go to the outside network (Internet) with HTTP and HTTPS.
   To avoid creation of multiple policies an application-set can be used to group junos-HTTP and junos-https applications.

Device	Incoming zone	Outgoing zone	Source address entry	Destination address entry	Application	Action
srx1	TRUST	UNTRUST	172.16.10.0/24	Any	junos-http junos-https	permit

2) Ensure the hosts from the TRUST zone have access to the whole private corporate network (reachable via CORE network) with any application.

Device	Incoming zone	Outgoing zone	Source address entry	Destination address entry	Application	Action
srx1	TRUST	UNTRUST	172.16.10.0/24	172.16.0.0/16	any	permit

3) Devices in the DMZ zone should be accessible from the whole private corporate network including the local TRUST zone with HTTPS.

Device	Incoming zone	Outgoing zone	Source address entry	Destination address entry	Application	Action
srx1	UNTRUST	DMZ	172.16.0.0/16	172.16.11.0/24	https	permit
srx1	TRUST	DMZ	172.16.10.0/24	172.16.11.0/24	https	permit

4) No other connections are allowed to go in or out of the TRUST zone.

© 2020 Juniper Networks, Inc. All rights reserved.

Since the devices are firewalls which drop not explicitly allowed traffic by default, no security policy is needed here.

5) No connections are allowed to go out from DMZ zone. Log all violations going out to the CORE network.
As mentioned before the firewalls drop not explicitly allowed traffic by default which means no security policy might be needed here to drop the traffic. But in order to log all violations a security policy has to be defined having the action “log”.

Device	Incoming zone	Outgoing zone	Source address entry	Destination address entry	Application	Action
srx1	DMZ	UNTRUST	Any	Any	any	deny log

Make sure this security policy is last in the context of incoming zone DMZ to outgoing zone UNTUST.

Branch office 2: srx2

6) Ensure the hosts from the TRUST zone have access to the whole private corporate network (reachable via CORE network) with any application.

Device	Incoming zone	Outgoing zone	Source address entry	Destination address entry	Application	Action
srx2	TRUST	UNTRUST	172.16.20.0/24	172.16.0.0/16	any	permit

7) No other connections are allowed in or out of the TRUST zone. Log all outgoing violations to the destinations reachable via the CORE network.
As only the outgoing connections need to be logged one security policy for them has to be created. The incoming connections are dropped by default.

Device	Incoming zone	Outgoing zone	Source address entry	Destination address entry	Application	Action
srx2	TRUST	UNTRUST	172.16.20.0/24	Any	any	deny log

Make sure this security policy is last in the context of incoming zone TRUST to outgoing zone UNTUST.

© 2020 Juniper Networks, Inc. All rights reserved.

8) Hosts from the PRIVATE zone can connect to the DMZ zone in the Central office and Data center using SSH, HTTP, HTTPS, FTP, telnet.
To make connections from the PRIVATE zone to the rest of the network possible NAT needs to be performed. Due the fact the NAT is being performed separately from security policies in Junos firewalls the security polices can be defined also at this moment. Because the source NAT translation is done after the security policies the addresses referenced are the original addresses of the received packets.
In addition to avoid creation of multiple security policies the address-sets and application-sets should be used.

Device	Incoming zone	Outgoing zone	Source address entry	Destination address entry	Application	Action
srx2	PRIVATE	UNTRUST	172.16.21.0/24	172.16.150.0/24 172.16.55.0/24	junos-ssh junos-http junos-https junos-ftp junos-telnet	permit

Home office: srx8

9) Hosts connected to the srx8 can access the whole private corporate network regardless of the application and in addition have HTTP and HTTPS permitted to the outside world/Internet.

Device	Incoming zone	Outgoing zone	Source address entry	Destination address entry	Application	Action
srx8	TRUST	UNTRUST	192.168.10.0/24	172.16.0.0/16	any	permit
srx8	TRUST	UNTRUST	192.168.10.0/24	Any	junos-http junos-https	permit

Finance department: srx7

10) From the FINANCE zone all connections are allowed to the INTERNAL zone and to the WAREHOUSE zone in the Data center only for SQL queries. The database server in Data center listens on ports 5000 – 6000. Ensure the appropriate ALG for SQL is being used.

In this case a custom application needs to be defined:

© 2020 Juniper Networks, Inc. All rights reserved.

```
[edit]
lab@srx7# show applications
application custom-sql {
    application-protocol sqlnet-v2;
    protocol tcp;
    destination-port 5000-6000;
}
```

Device	Incoming zone	Outgoing zone	Source address entry	Destination address entry	Application	Action
srx7	FINANCE	INTERNAL	172.16.199.0/24	172.16.60.0/24	any	permit
srx7	FINANCE	INTERNAL	172.16.199.0/24	172.16.200.0/24	custom-sql	permit

11) DMZ zones in the Data center and Central office are reachable from the FINANCE zone using HTTP, HTTPS and SSH.
The access to the DMZ zones in Data center and Central office is via the INTERNAL zone.
Also, here to avoid creation of multiple security policies the address-sets and application-sets should be used. However, the requirement to allow only specific applications prevents the merging with the defined in the previous step.

Device	Incoming zone	Outgoing zone	Source address entry	Destination address entry	Application	Action
srx7	FINANCE	INTERNAL	172.16.199.0/24	172.16.150.0/24 172.16.55.0/24	junos-http junos-https junos-ssh	permit

Data center: cluster1

12) The TRUST zone has access to the whole private corporate network (also locally connected networks) with any application.

Device	Incoming zone	Outgoing zone	Source address entry	Destination address entry	Application	Action
cluster1	TRUST	UNTUST	172.16.100.0/24	172.16.0.0/16	any	permit
cluster1	TRUST	DMZ	172.16.100.0/24	172.16.150.0/24	any	permit
cluster1	TRUST	WARE HOUSE	172.16.100.0/24	172.16.200.0/24	any	permit

© 2020 Juniper Networks, Inc. All rights reserved.

13)No other connections are allowed in or out of the TRUST zone. Log all outgoing violations, e.g. connections going to CORE network.

Device	Incoming zone	Outgoing zone	Source address entry	Destination address entry	Application	Action
cluster1	TRUST	UNTRUST	172.16.100.0/24	any	any	deny log

Make sure this security policy is last in the context of incoming zone TRUST to outgoing zone UNTUST.

14)Full communication between DMZ (local and central office) and WAREHOUSE zone is possible in both directions.

The full communication here means any application. The access to the DMZ zone in the Central office here goes through the UNTRUST zone.

Device	Incoming zone	Outgoing zone	Source address entry	Destination address entry	Application	Action
cluster1	DMZ	WARE HOUSE	172.16.150.0/24	172.16.200.0/24	any	permit
cluster1	WARE HOUSE	DMZ	172.16.200.0/24	172.16.150.0/24	any	permit
cluster1	WARE HOUSE	UNTRUST	172.16.200.0/24	172.16.55.0/24	any	permit
cluster1	UNTRUST	WARE HOUSE	172.16.55.0/24	172.16.200.0/24	any	permit

15)HTTP, HTTPS, SSH, SMTP, FTP and telnet connections from the private corporate network (reachable via CORE network) to DMZ are allowed.
Also, this security policy should utilize application-set.

© 2020 Juniper Networks, Inc. All rights reserved.

Device	Incoming zone	Outgoing zone	Source address entry	Destination address entry	Application	Action
cluster1	UNTUST	DMZ	172.16.0.0/16	172.16.150.0/24	junos-http junos-https junos-ssh junos-smtp junos-ftp	permit

16) Only the specific SQL connections (described previously) from the FINANCE zone in the Finance department are allowed to enter the WAREHOUSE zone. Count this traffic.
Counting traffic handled by specific policy is achieved using the action “count”. The actual counters can be examined using the “show security policies …. detail” command.
As in case of Finance department also here the custom application needs to be created with the same parameters:

```
applications {
    application custom-sql {
        application-protocol sqlnet-v2;
        protocol tcp;
        destination-port 5000-6000;
    }
}
```

Device	Incoming zone	Outgoing zone	Source address entry	Destination address entry	Application	Action
cluster1	UNTUST	WARE HOUSE	172.16.199.0/24	172.16.200.0/24	custom-sql	permit count

Central office: cluster2

17) Ensure the permitted connections from the Finance department on the srx7 are allowed as well, but focus only network ranges and not applications, i.e. when defining these policies disregard the applications.
Brief recap: in Finance department the following connections are allowed (listing only source zone/device and destination zone/device):
- FINANCE (srx7) --> INTERNAL (srx7)
  - No need for security policy on cluster 2 as this traffic is not traversing the cluster 2.

© 2020 Juniper Networks, Inc. All rights reserved.

- FINANCE (srx7) --> WAREHOUSE (cluster1)
  - Security policy is needed, locally on the cluster 2 this traffic is received in the zone INTERNAL and goes out through the zone UNTRUST.
- FINANCE (srx7) --> DMZ (cluster1)
  - Security policy is needed, locally on the cluster 2 this traffic is received in the zone INTERNAL and goes out through the zone UNTRUST.
  - This security policy can be merged with the previous one.
- FINANCE (srx7) --> DMZ (cluster2)
  - Security policy is needed, locally on the cluster 2 this traffic is received in the zone INTERNAL and goes out through the zone DMZ.

As the applications can be disregarded the security policies will use “any” for the application.

Device	Incoming zone	Outgoing zone	Source address entry	Destination address entry	Application	Action
cluster2	INTERNAL	UNTRUST	172.16.199.0/24	172.16.150.0/24 172.16.200.0/24	any	permit
cluster2	INTERNAL	DMZ	172.16.199.0/24	172.16.55.0/24	any	permit

18) Hosts located in the INTERNAL zone have full access to the local DMZ resources but only during working days and working hours (8:00 - 18:00).
For this purpose, a scheduler active only during working days and defined hours needs to be created and then associated with the security policy.
The scheduler definition is following:

```
schedulers {
    scheduler working-time {
        daily {
            start-time 08:00:00 stop-time 18:00:00;
        }
        sunday exclude;
        saturday exclude;
    }
}
```

The following scheduler definition is correct too:

```
schedulers {
    scheduler working-time {
        monday {
            start-time 08:00:00 stop-time 18:00:00;
        }
        tuesday {
            start-time 08:00:00 stop-time 18:00:00;
        }
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
        wednesday {
            start-time 08:00:00 stop-time 18:00:00;
        }
        thursday {
            start-time 08:00:00 stop-time 18:00:00;
        }
        friday {
            start-time 08:00:00 stop-time 18:00:00;
        }
    }
}
```

Device	Incoming zone	Outgoing zone	Source address entry	Destination address entry	Application	Action
cluster2	INTERNAL	DMZ	172.16.60.0/24	172.16.55.0/24	any	permit scheduler

19) The TRUST zone has access to the whole private corporate network (also locally connected networks) with any application. In addition, only HTTP and HTTPS access is allowed to the Internet from the TRUST zone. Log all outgoing violations, e.g. connections leaving the cluster through the UNTRUST zone.

Device	Incoming zone	Outgoing zone	Source address entry	Destination address entry	Application	Action
cluster2	TRUST	UNTRUST	172.16.50.0/24	172.16.0.0/16	any	permit
cluster2	TRUST	DMZ	172.16.50.0/24	172.16.55.0/24	any	permit
cluster2	TRUST	INTERNAL	172.16.50.0/24	172.16.60.0/24 172.16.199.0/24 172.16.21.0/24 Or use here the corporate network 172.16.0.0/16	any	permit
cluster2	TRUST	UNTRUST	172.16.50.0/24	any	junos-http junos-https	permit
cluster2	TRUST	UNTRUST	172.16.50.0/24	any	any	deny log

Make sure this security policy is last in the context of incoming zone TRUST to outgoing zone UNTUST.

20) Full communication between DMZ and WAREHOUSE zone is possible in both directions.

© 2020 Juniper Networks, Inc. All rights reserved.

Device	Incoming zone	Outgoing zone	Source address entry	Destination address entry	Application	Action
cluster2	DMZ	UNTRUST	172.16.55.0/24	172.16.200.0/24	any	permit
cluster2	UNTRUST	DMZ	172.16.200.0/24	172.16.55.0/24	any	permit

Ensure respective policies are present on the cluster 1 (look for these entries):

Device	Incoming zone	Outgoing zone	Source address entry	Destination address entry	Application	Action
cluster1	WARE HOUSE	UNTRUST	172.16.200.0/24	172.16.55.0/24	any	permit
cluster1	UNTRUST	WARE HOUSE	172.16.55.0/24	172.16.200.0/24	any	permit

21) HTTP, FTP and telnet requests sourced from the private corporate network arriving on the core network facing interface and destined to the DMZ hosts need to be authenticated in order to be granted. Use the pass-through authentication with following settings
    a. username: testuser, password: testuserpw123
    b. 1 hour of inactivity will result in re-authentication
    c. the passwords are stored locally on the security device
    d. FTP and telnet banners:
        i. initial banner: “Look out firewall authentication!!!”
        ii. in case of successful authentication: “Correct!”
        iii. in case of unsuccessful authentication: “Incorrect!”

The pass-through authentication is one of 2 options of the firewall authentication. It is applicable ONLY to clear text protocols: telnet, FTP and HTTP and no others. The firewall here intercepts the communication between the end hosts and asks for authentication inline. The other option is the web-authentication, which can be used also for other protocols and applications. In this case the user needs go to defined IP address on the firewall using browser and authenticate there. Only upon successful authentication the connections to the desired destinations will be granted.

To configure the firewall to perform an authentication in security policy following things are needed:

- an access profile
    - in case of local authentication also the clients and passwords need to be defined locally on the device

© 2020 Juniper Networks, Inc. All rights reserved.

  - idle timeout for enforcing re-authentication after defined inactivity period
- firewall and pass-through authentication settings
  - banners
  - which access profile to use
- configure in the security policy permit action to perform pass-through authentication and specify which clients are allowed to use the policy by defining the "**client-match**" parameter

```
access {
    profile FWauth {
        authentication-order password;
        client testuser {
            firewall-user {
                password "$9$Sm9yMXVb2aGiYgF/tpEhevWXdsYgJkmTJZn/tpB1"; ## SECRET-DATA
            }
        }
        session-options {
            client-idle-timeout 60;
        }
    }
    firewall-authentication {
        pass-through {
            default-profile FWauth;
            ftp {
                banner {
                    login "Look out firewall authentication!!!";
                    success "Correct!";
                    fail "Incorrect!";
                }
            }
            telnet {
                banner {
                    login "Look out firewall authentication!!!";
                    success "Correct!";
                    fail "Incorrect!";
                }
            }
        }
    }
}
```


© 2020 Juniper Networks, Inc. All rights reserved.

Configuration excerpt from the security policy which performs the pass-through authentication:

```
then {
    permit {
        firewall-authentication {
            pass-through {
                client-match testuser;
            }
        }
    }
}
```


© 2020 Juniper Networks, Inc. All rights reserved.

Device	Incoming zone	Outgoing zone	Source address entry	Destination address entry	Application	Action
cluster2	UNTRUST	DMZ	172.16.0.0/16	172.16.55.0/24	junos-http junos-ftp junos-telnet	permit, firewall-authentication

22) SSH and HTTPS connections from private corporate network arriving on the core network facing interface and destined to the DMZ hosts the are granted without authentication.

Device	Incoming zone	Outgoing zone	Source address entry	Destination address entry	Application	Action
cluster2	UNTRUST	DMZ	172.16.0.0/16	172.16.55.0/24	junos-https junos-ssh	permit

Troubleshooting

Testing and especially troubleshooting security policies can be sometimes cumbersome and time consuming process. Here are some tips and possibilities how to perform it and what to look for.

Testing

Typically, the most obvious way to test security policies is to issue traffic and check if it is being handled in the desired way. Following command can be used:

```
lab@srx1> show security flow session
```

The output lists the currently active sessions on the device. In addition, the command offers rich filtering criteria (such as destination address, source address, both ports, protocol, incoming or outgoing interface, etc.) to aid in showing and checking only the desired sessions.

To generate such traffic an external device needs to be available and this might be sometimes hard to accomplish (no device available, security personnel has no access to it, etc.). In such cases the SRX devices offers a capability to test the security policies locally

© 2020 Juniper Networks, Inc. All rights reserved.

by using following command, e.g. the output of this command will show the details about the security policy handling the connection:

```
lab@srx1>show security match-policies ?
Possible completions:
  destination-ip       Match policy for the given destination IP
  destination-port     Match policy for the given destination port) (1..65535)
  from-zone            Match policy for the given source zone
  protocol             Match policy for the given protocol)
  source-ip            Match policy for the given source IP
  source-port          Match policy for the given source port) (1..65535)
  to-zone              Match policy for the given destination zone
```

Note: This command requires that ALL parameters are defined in order to be executed.

Another option for troubleshooting is enabling log action in security policies. The log entries contain information not only about the connection and its statistics but also the name of security policy handling the connection. In production environments with high traffic loads enabling security policies logging needs to be done with great caution as it can generate huge amount of log entries. This not only consumes more system resources but might be harder to analyze due the amount of the log entries.

The tracing (or traceoptions) capability within Junos is intended to aid in troubleshooting in many areas including security policies. It provides detailed information about traffic processing and handling. The configuration is following:

```
[edit security flow]
lab@srx1# set traceoptions ?
Possible completions:
+ apply-groups         Groups from which to inherit configuration data
+ apply-groups-except  Don't inherit configuration data from these groups
> file                 Trace file information
> flag                 Events and other information to include in trace output
  no-remote-trace      Disable remote tracing
> packet-filter        Flow packet debug filters
  rate-limit           Limit the incoming rate of trace messages (0..4294967295)
```

Note: When configuring the FLOW traceoptions always define the "**packet-filter**" with values that identify traffic you want to troubleshoot. This recommendation is crucial again in production environments by saving not only system resources but also speeding up the troubleshooting process as the traceoptions file will contain only entries related to processing of traffic matching the "packet-filter" criteria.

Some examples of common mistakes and causes of problems:

- Incorrect routing
  - the traffic crosses different zones than expected
  - the traffic for which forwarding lookup fails is dropped

© 2020 Juniper Networks, Inc. All rights reserved.

- Security policies
  - wrong order of security policies
  - mistakes/typos in values of addresses (source, destination) and applications

Configurations

Below is the security policies related configuration for all lab devices:

Branch office 1

srx1:

```
applications {
    application-set trust-app-set {
        application junos-http;
        application junos-https;
    }
}

security {
    zones {
        security-zone TRUST {
            address-book {
                address trust-address-range 172.16.10.0/24;
            }
            interfaces {
                ge-0/0/1.0;
            }
        }
        security-zone DMZ {
            address-book {
                address dmz-range 172.16.11.0/24;
            }
            interfaces {
                ge-0/0/2.0;
            }
        }
        security-zone UNTRUST {
            address-book {
                address corp-network 172.16.0.0/16;
            }
            interfaces {
                ge-0/0/3.0;
            }
        }
    }
    policies {
        from-zone TRUST to-zone UNTRUST {
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
policy internet-access {
    match {
        source-address trust-address-range;
        destination-address any;
        application trust-app-set;
    }
    then {
        permit;
    }
}
policy corp-network-access {
    match {
        source-address trust-address-range;
        destination-address corp-network;
        application any;
    }
    then {
        permit;
    }
}
}
from-zone TRUST to-zone DMZ {
    policy trust-to-dmz {
        match {
            source-address trust-address-range;
            destination-address dmz-range;
            application junos-https;
        }
        then {
            permit;
        }
    }
}
from-zone UNTRUST to-zone DMZ {
    policy corp-network-to-dmz {
        match {
            source-address corp-network;
            destination-address dmz-range;
            application junos-https;
        }
        then {
            permit;
        }
    }
}
from-zone DMZ to-zone UNTRUST {
    policy dmz-to-untrust-log {
        match {
            source-address any;
            destination-address any;
            application any;
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
                }
                then {
                    deny;
                    log {
                        session-init;
                    }
                }
            }
        }
    }
}
```

Branch office 2

srx2:

```
applications {
    application-set private-app-set {
        application junos-http;
        application junos-https;
        application junos-ssh;
        application junos-telnet;
        application junos-ftp;
    }
}

security {
    zones {
        security-zone TRUST {
            address-book {
                address trust-address-range 172.16.20.0/24;
            }
            interfaces {
                ge-0/0/2.0;
            }
        }
        security-zone PRIVATE {
            address-book {
                address private-range 172.168.21.0/24;
            }
            interfaces {
                ge-0/0/4.0;
            }
        }
        security-zone UNTRUST {
            address-book {
                address corp-network 172.16.0.0/16;
                address dmz-DC 172.16.150.0/24;
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
            address dmz-CO 172.16.55.0/24;
            address-set dmz-zones {
                address dmz-CO;
                address dmz-DC;
            }
        }
        interfaces {
            ge-0/0/3.0;
        }
    }
}
policies {
    from-zone TRUST to-zone UNTRUST {
        policy corp-network-access {
            match {
                source-address trust-address-range;
                destination-address corp-network;
                application any;
            }
            then {
                permit;
            }
        }
        policy internet-deny-log {
            match {
                source-address any;
                destination-address any;
                application any;
            }
            then {
                deny;
                log {
                    session-init;
                }
            }
        }
    }
    from-zone TRUST to-zone PRIVATE {
        policy trust-to-private {
            match {
                source-address trust-address-range;
                destination-address private-range;
                application junos-https;
            }
            then {
                permit;
            }
        }
    }
    from-zone PRIVATE to-zone UNTRUST {
        policy dmz-access {
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
                match {
                    source-address private-range;
                    destination-address dmz-zones;
                    application private-app-set;
                }
                then {
                    permit;
                }
            }
        }
    }
}
```

Data center

cluster1:

```
applications {
    application custom-sql {
        application-protocol sqlnet-v2;
        protocol tcp;
        destination-port 5000-6000;
    }
    application-set dmz-apps {
        application junos-http;
        application junos-https;
        application junos-ssh;
        application junos-ftp;
        application junos-smtp;
        application junos-telnet;

    }
}
```

```
security {
    zones {
        security-zone TRUST {
            address-book {
                address trust-address-range 172.16.100.0/24;
            }
            interfaces {
                reth1.100;
            }
        }
        security-zone DMZ {
            address-book {
                address dmz-range 172.16.150.0/24;
            }
            interfaces {
                reth1.150;
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
        }
    }
    security-zone UNTRUST {
        address-book {
            address corp-network 172.16.0.0/16;
            address co-dmz-range 172.16.55.0/24;
            address finance-range 172.16.199.0/24;
        }
        interfaces {
            reth0.0;
        }
    }
    security-zone WAREHOUSE {
                address-book {
                    address warehouse-range 172.16.200.0/24;
                }
                interfaces {
                    reth1.200;
                }
            }
        }
    policies {
            from-zone TRUST to-zone UNTRUST {
                policy corp-access {
                    match {
                        source-address trust-address-range;
                        destination-address corp-network;
                        application any;
                    }
                    then {
                        permit;
                    }
                }
                policy internet-denied-log {
                    match {
                        source-address any;
                        destination-address any;
                        application any;
                    }
                    then {
                        deny;
                        log {
                            session-init;
                        }
                    }
                }
            }
        }
        from-zone TRUST to-zone DMZ {
            policy trust-dmz-access {
                match {
                    source-address trust-address-range;
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
            destination-address dmz-range;
            application any;
        }
        then {
            permit;
        }
    }
}
from-zone UNTRUST to-zone DMZ {
    policy access-from-corp {
        match {
            source-address corp-network;
            destination-address dmz-range;
            application dmz-apps;
        }
        then {
            permit;
        }
    }
}
from-zone TRUST to-zone WAREHOUSE {
    policy trust-warehouse-access {
        match {
            source-address trust-address-range;
            destination-address warehouse-range;
            application any;
        }
        then {
            permit;
        }
    }
}
from-zone DMZ to-zone WAREHOUSE {
    policy dmz-warehouse-access {
        match {
            source-address dmz-range;
            destination-address warehouse-range;
            application any;
        }
        then {
            permit;
        }
    }
}
from-zone WAREHOUSE to-zone DMZ {
    policy warehouse-dmz-access {
        match {
            source-address warehouse-range;
            destination-address dmz-range;
            application any;
        }
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
            then {
                permit;
            }
        }
    }
    from-zone WAREHOUSE to-zone UNTRUST {
        policy warehouse-co-dmz-access {
            match {
                source-address warehouse-range;
                destination-address co-dmz-range;
                application any;
            }
            then {
                permit;
            }
        }
    }
    from-zone UNTRUST to-zone WAREHOUSE {
        policy co-dmz-warehouse {
            match {
                source-address co-dmz-range;
                destination-address warehouse-range;
                application any;
            }
            then {
                permit;
            }
        }
        policy finance-warehouse-access {
            match {
                source-address finance-range;
                destination-address warehouse-range;
                application custom-sql;
            }
            then {
                permit;
            }
        }
    }
}
```

Central office

cluster2:

```
applications {
    application-set dmz-apps {
        application junos-http;
        application junos-https;
        application junos-ssh;
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
    }
    application-set dmz-apps-web-auth {
        application junos-ftp;
        application junos-telnet;
        application junos-http;
    }
    application-set internet-apps {
        application junos-http;
        application junos-https;
    }
}
schedulers {
    scheduler working-time {
        daily {
            start-time 08:00:00 stop-time 18:00:00;
        }
        sunday exclude;
        saturday exclude;
    }
}

security {
alg {
    dns {
        doctoring {
            sanity-check;
        }
    }
}
    zones {
        security-zone TRUST {
            address-book {
                address trust-address-range 172.16.50.0/24;
            }
            interfaces {
                reth1.50;
            }
        }
security-zone DMZ {
            address-book {
                address dmz-range 172.16.55.0/24;
            }
            interfaces {
                reth1.55;
            }
        }
        security-zone INTERNAL {
            address-book {
                address internal-range 172.16.60.0/24;
                address finance-range 172.16.199.0/24;
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
            address private-range 172.16.21.0/24;
            address-set internal-finance-private-ranges {
                address internal-range;
                address finance-range;
                address private-range;
            }
        }
        interfaces {
            reth1.60;
        }
    }
    security-zone UNTRUST {
        address-book {
            address corp-network 172.16.0.0/16;
            address dc-warehouse-range 172.16.200.0/24;
            address dc-dmz-range 172.16.150.0/24;
            address-set dc-dmz-warehouse {
                address dc-dmz-range;
                address dc-warehouse-range;
            }
        }
        interfaces {
            reth0.0;
        }
    }
}
policies {
    from-zone INTERNAL to-zone UNTRUST {
        policy finance-dc-dmz-warehouse-access {
            match {
                source-address finance-range;
                destination-address dc-dmz-warehouse;
                application any;
            }
            then {
                permit;
            }
        }
    }
    from-zone INTERNAL to-zone DMZ {
        policy finance-dmz-access {
            match {
                source-address finance-range;
                destination-address dmz-range;
                application any;
            }
            then {
                permit;
            }
        }
        policy internal-dmz-access {
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
            match {
                source-address internal-range;
                destination-address dmz-range;
                application any;
            }
            then {
                permit;
            }
            scheduler-name working-time;
        }
    }
    from-zone TRUST to-zone UNTRUST {
        policy trust-corp-network {
            match {
                source-address trust-address-range;
                destination-address corp-network;
                application any;
            }
            then {
                permit;
            }
        }
        policy internet-access {
            match {
                source-address trust-address-range;
                destination-address any;
                application internet-apps;
            }
            then {
                permit;
            }
        }
        policy internet-denied-log {
            match {
                source-address any;
                destination-address any;
                application any;
            }
            then {
                deny;
                log {
                    session-init;
                }
            }
        }
    }
    from-zone TRUST to-zone DMZ {
        policy trust-dmz-access {
            match {
                source-address trust-address-range;
                destination-address dmz-range;
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
            application any;
        }
        then {
            permit;
        }
    }
}
from-zone TRUST to-zone INTERNAL {
    policy trust-to-int-priv-fin {
        match {
            source-address trust-address-range;
            destination-address internal-finance-private-ranges;
            application any;
        }
        then {
            permit;
        }
    }
}
from-zone DMZ to-zone UNTRUST {
    policy dmz-warehouse-access {
        match {
            source-address dmz-range;
            destination-address dc-warehouse-range;
            application any;
        }
        then {
            permit;
        }
    }
}
from-zone UNTRUST to-zone DMZ {
    policy warehouse-dmz-access {
        match {
            source-address dc-warehouse-range;
            destination-address dmz-range;
            application any;
        }
        then {
            permit;
        }
    }
policy corp-dmz-acces-web-auth {
    match {
        source-address corp-network;
        destination-address dmz-range;
        application dmz-apps-web-auth;
    }
    then {
        permit {
            firewall-authentication {
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
                    pass-through {
                        client-match testuser;
                    }
                }
            }
        }
    }
    policy corp-dmz-acces {
        match {
            source-address corp-network;
            destination-address dmz-range;
            application dmz-apps;
        }
        then {
            permit;
        }
    }
}
access {
    profile FWauth {
        authentication-order password;
        client testuser {
            firewall-user {
                password "$9$Sm9yMXVb2aGiYgF/tpEhevWXdsYgJkmTJZn/tpB1"; ## SECRET-DATA
            }
        }
        session-options {
            client-idle-timeout 60;
        }
    }
    firewall-authentication {
        pass-through {
            default-profile FWauth;
            ftp {
                banner {
                    login "Look out firewall authentication!!!";
                    success "Correct!";
                    fail "Incorrect!";
                }
            }
            telnet {
                banner {
                    login "Look out firewall authentication!!!";
                    success "Correct!";
                    fail "Incorrect!";
                }
            }
        }
    }
}
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
}
```

Finance department

srx7:

```
applications {
    application custom-sql {
        application-protocol sqlnet-v2;
        protocol tcp;
        destination-port 5000-6000;
    }
    application-set dmz-apps {
        application junos-http;
        application junos-https;
        application junos-ssh;
    }
}

security {
    zones {
        security-zone FINANCE {
            address-book {
                address finance-address-range 172.16.199.0/24;
            }
            interfaces {
                ge-0/0/1.0;
            }
        }
        security-zone PRIVATE {
            address-book {
                address private-range 172.168.21.0/24;
            }
            interfaces {
                ge-0/0/2.0;
            }
        }
        security-zone INTERNAL {
            address-book {
                address dmz-DC 172.16.150.0/24;
                address dmz-CO 172.16.55.0/24;
                address warehouse-range 172.16.200.0/24;
                address internal-range 172.16.60.0/24;
                address-set dmz-zones {
                    address dmz-CO;
                    address dmz-DC;
                }
            }
            interfaces {
                ge-0/0/4.60;
            }
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
    }
}
policies {
    from-zone FINANCE to-zone INTERNAL {
        policy finance-internal {
            match {
                source-address finance-address-range;
                destination-address internal-range;
                application any;
            }
            then {
                permit;
            }
        }
        policy warehouse-sql {
            match {
                source-address finance-address-range;
                destination-address warehouse-range;
                application custom-sql;
            }
            then {
                permit;
            }
        }
        policy dmz-zone-access {
            match {
                source-address finance-address-range;
                destination-address dmz-zones;
                application dmz-apps;
            }
            then {
                permit;
            }
        }
    }
}
```

Home office

srx8:

```
applications {
    application-set internet-apps {
        application junos-http;
        application junos-https;
    }
}


security {
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
zones {
    security-zone TRUST {
        address-book {
            address trust-address-range 192.168.10.0/24;
        }
        interfaces {
            ge-0/0/1.0;
        }
    }
    security-zone UNTRUST {
        address-book {
            address corp-network 172.16.0.0/16;
        }
        interfaces {
            ge-0/0/3.0;
        }
    }
}
policies {
    from-zone TRUST to-zone UNTRUST {
        policy corp-network-access {
            match {
                source-address trust-address-range;
                destination-address corp-network;
                application any;
            }
            then {
                permit;
            }
        }
        policy internet-access {
            match {
                source-address trust-address-range;
                destination-address any;
                application internet-apps;
            }
            then {
                permit;
            }
        }
    }
}
```


© 2020 Juniper Networks, Inc. All rights reserved.

Appendix - Chapter 4: Unified Threat Management

This appendix provides the solution details for the Unified Threat Management (UTM) chapter. The configuration involves web and content filtering, anti-spam and antivirus.

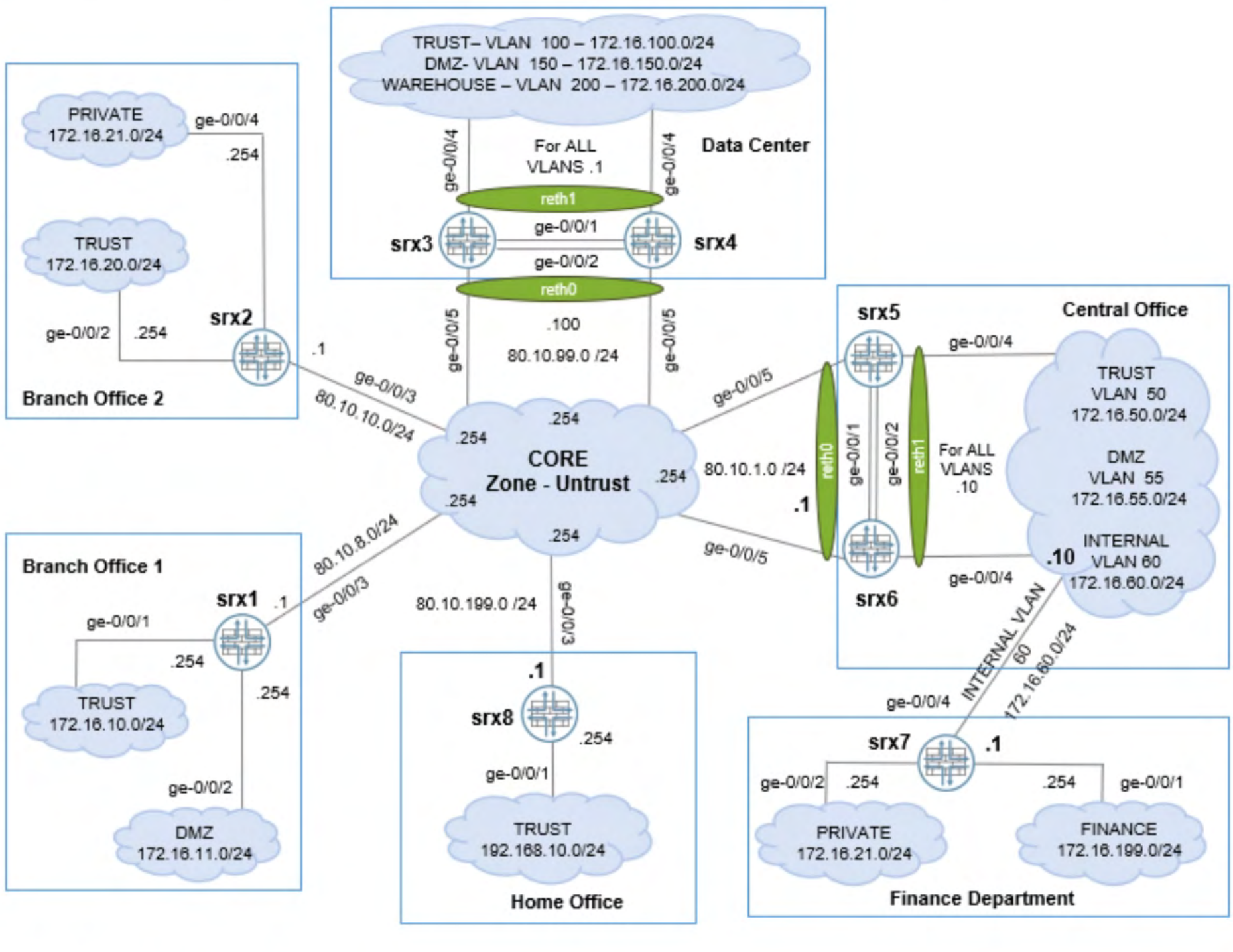


Figure 1: Chapter 4 Topology

UTM consists of a set of security features that provide inspection at the application layer as a protection against multiple threat types. However, the inspection is done only for following protocols – HTTP, FTP, and email protocols such as SMTP, IMAP and POP3.

The UTM features are following:

- *Antispam*: Scans the SMTP traffic going through the security device and blocks or tags unwanted e-mails. The feature supports the use of locally defined white and

© 2020 Juniper Networks, Inc. All rights reserved.

black lists together with an external spam block list (SBL) server. This feature is meant to complement an antispam server and not to replace it.

- *Antivirus*: Inspects traffic for virus-infected files, trojans, worms, spyware, and other malicious codes utilizing a virus database signature and scanning engine. The latest Junos release offers the selection between:
  - Full file-based antivirus scanning uses a scan engine and database provided by Sophos.
  - Express antivirus scanning supports the same protocols as full file-based option but is less CPU intensive because it uses a different scan engine and hardware for pattern matching acceleration. The tradeoff are certain limitations (such as limited support for archive scanning and decompression layers, no support for extension scanning, etc.). The engine does not wait and reassemble the whole file but rather performs the inspection packet by packet.
  - Sophos antivirus scanning also supports the same protocols. It is less CPU intensive as full file-based antivirus feature because it uses the in-the-cloud antivirus solution, where the external servers which contain the virus and malware database are maintained by Sophos. The security device maintains a cache locally with the results to improve the performance.
- *Content Filtering*: Filters traffic based on MIME type, file extension, and protocol commands.
- *Web Filtering*: Allows you to control access to the web content. Following types of web filtering are available:
  - Integrated Web filtering intercepts every HTTP request in a TCP connection and makes the decision (allow or block) based on the category to which the URL belongs. The category is determined either from user-defined categories or from a category server.
  - Redirect Web filtering intercepts HTTP requests and sends them to an external URL filtering server (also provided by Websense) which returns back to the device the decision whether to block the requests or not.
  - Local Web filtering intercepts every HTTP request in a TCP connection. The device determines locally based on the configuration (user-defined categories, white and black lists) whether to block the request or not.
  - Enhanced Web Filtering (EWF) with Websense is an integrated URL filtering solution, which intercepts the HTTP and the HTTPS requests and sends the HTTP URL or the HTTPS source IP to the Websense ThreatSeeker Cloud (TSC) for categorization. The TSC categorizes the URL into one of the 95 or more predefined categories and in addition provides site reputation information. The device uses the returned result to make the decision to permit or block the request.

© 2020 Juniper Networks, Inc. All rights reserved.

Following UTM features require license:

- Antispam SBL option
- Full file based antivirus
- Sophos Antivirus
- Integrated Web filtering
- Enhanced Web Filtering

In case of chassis cluster both nodes must have the UTM licenses available to resume the operation in case of failover. However, the UTM state is not synchronized between the nodes.

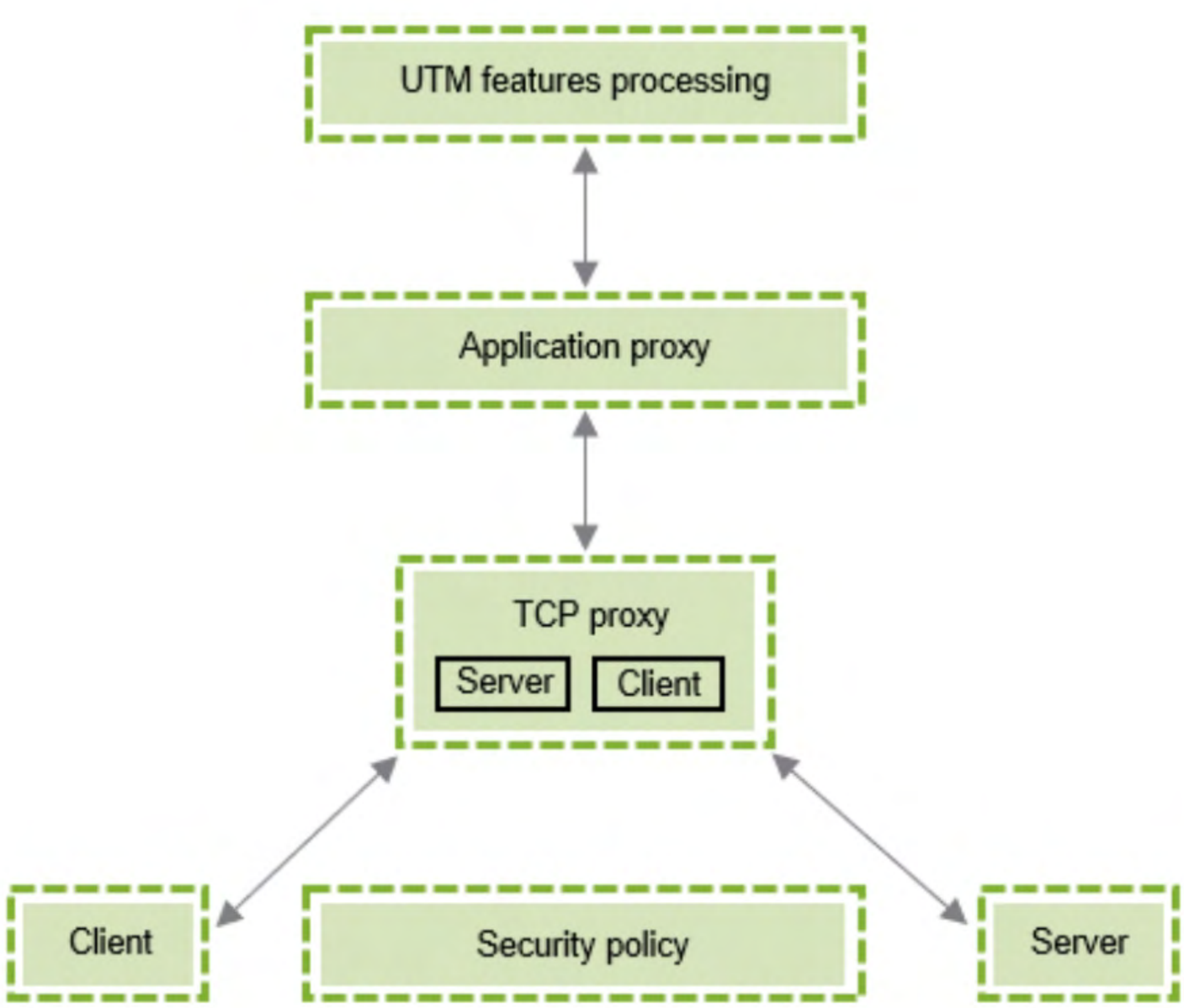
The UTM configuration components are:

- Custom objects – used to define objects that are referenced in the configuration of individual UTM features or feature profiles. For example – file extensions for antivirus scanning, white and black lists for antispam or web-filtering, protocol commands for content filtering, etc. The configuration hierarchy for custom object is [edit security utm custom-objects]
- Feature profile – are used to configure individual UTM features (antispam, antivirus, content and web filtering) and their operation. The features profiles for individual UTM features are configured separately and depending on the requirements reference the created custom objects. The configuration hierarchy is [edit security utm feature-profile]
- UTM policy – references the appropriate feature profiles. The resulting combination UTM features are then executed on the traffic. Multiple UTM policies can exist on a single security device and can be referenced by different security policies. However, each security policy can list only one UTM policy. The achieved behavior is enforcing different UTM features on different traffic depending on the requirement and needs. The UTM policies are configured under the [edit security utm utm-policy] are referenced within the permit action in the security policy with “permit application-services utm-policy <utm-policy-name>” parameter.

Because the UTM policy is referenced in a security policy the UTM features are enforced only on traffic permitted by a security policy. The actual UTM processing happens within the service processing stage.

© 2020 Juniper Networks, Inc. All rights reserved.

To enforce UTM features correctly additional processing is needed. The security device intercepts all TCP connections, because all supported UTM protocols are TCP based. In the next step TCP proxy is used where security device acts as the server to the originating client and as the client to the desired server. This allows the security device to request the needed data for UTM processing from either side independently. The data is then supplied to the application proxy which decodes and extracts the application protocol (HTTP, FTP, IMAP, POP3, SMTP) information and sends it to the appropriate UTM feature for further processing.



Things to remember

- ***Only high memory branch devices support UTM***
- ***UTM is enforced only on following protocols: HTTP, FTP, IMAP, POP3 and SMTP.***
- ***Certain UTM features require a license***
- ***In chassis cluster environments the UTM license must be present on both nodes***

© 2020 Juniper Networks, Inc. All rights reserved.

Note: The device requires Internet access and correct DNS configuration ("system name-server" configuration parameter) for UTM features those utilize communication with external server or need to download information (such as databases, etc.) from external sources to operate correctly.

Because the lab environment is isolated the communication to these external sources is not possible and the verification commands for will not display success for the affected features.

Task 1: Web-filtering

This part is dedicated to the web filtering.

The instructions define the existing policies should be reused whenever possible, e.g. associating the newly created utm-policy with already existing security policies.

The UTM configuration is located under the [edit security utm] stanza, but the associations of utm-policies and security policies are done in the security policies configuration under the "then permit" stanza.

Branch office: srx1

1) The following security policy created in the previous chapter can be used to enforce the web-filtering on the traffic from zone TRUST to UNTRUST.

Device	Incoming zone	Outgoing zone	Source address entry	Destination address entry	Application	Action
srx1	TRUST	UNTRUST	172.16.10.0/24	any	junos-http junos-https	permit

2) The web-filtering offers 3 options:
   i. Juniper-enhanced
   ii. Websense-redirect
   iii. juniper-local

   Following command defines that the juniper-enhanced type will be used for web-filtering.

```
[edit security utm]
lab@srx1# set security utm feature-profile web-filtering type juniper-enhanced
```


© 2020 Juniper Networks, Inc. All rights reserved.

In the config examples the BranchOffice-Web was defined as the web-filtering feature profile name.

3) The security device makes the decision based on the URL's category. The configuration below assures the appropriate handling of requests according the requirements:
   i. Categories: Hacking, Violence, Gambling, Games --> blocked
   ii. Categories: News and Media, Computer_Security --> permitted
   iii. All other URL's --> permitted and logged
      i. The default action for URLs not matching any of the defined categories should be permit and log.

```
[edit]
lab@srx1# show security
utm {
    feature-profile {
        web-filtering {
            type juniper-enhanced;
            juniper-enhanced {
                profile BranchOffice-Web {
                    category {
                        Enhanced_Hacking {
                            action block;
                        }
                        Enhanced_Violence {
                            action block;
                        }
                        Enhanced_Gambling {
                            action block;
                        }
                        Enhanced_Games {
                            action block;
                        }
                        Enhanced_News_and_Media {
                            action permit;
                        }
                        Enhanced_Computer_Security {
                            action permit;
                        }
                    }
                    default log-and-permit;
```

Note: The custom categories and URL's belonging to them are defined using custom objects under [edit security utm] stanza. The evaluation for custom categories precedes the predefined (SurfControl) ones.

© 2020 Juniper Networks, Inc. All rights reserved.

4) Execute this command to define the custom message (“Blocked site!”) clients will receive in case their request is blocked.

```
[edit]
lab@srx1# set security utm feature-profile web-filtering juniper-enhanced profile
BranchOffice-Web custom-block-message "Blocked site!"
```

5) The fallback options specify the engine behavior when experiencing various issues when processing requests. The given instructions require following handling:
   i. For “too many requests” situation the action is drop/block

```
[edit]
lab@srx1# set security utm feature-profile web-filtering juniper-enhanced profile
BranchOffice-Web fallback-settings too-many-requests block
```

   ii. Server communication problems (response timeout reached and lost connectivity) result in blocking the requests

```
[edit]
lab@srx1# set security utm feature-profile web-filtering juniper-enhanced profile
BranchOffice-Web fallback-settings server-connectivity block

[edit]
lab@srx1# set security utm feature-profile web-filtering juniper-enhanced profile
BranchOffice-Web fallback-settings timeout block
```

   iii. For all other causes (default) the action is permit and log

```
[edit]
lab@srx1# set security utm feature-profile web-filtering juniper-enhanced profile
BranchOffice-Web fallback-settings default log-and-permit
```

6) The following command defines 120 seconds as server communication timeout limit.

```
[edit]
lab@srx1# set security utm feature-profile web-filtering juniper-enhanced profile
BranchOffice-Web timeout 120
```

The remaining part is to define the utm policy (chosen name is “Branch-web-filter”) referencing this created BranchOffice-Web web-filtering profile and then associate this utm policy with the correct security policy listed in the step 1.

```
[edit security utm]
lab@srx1# show | find utm-policy
utm-policy Branch-web-filter {
    web-filtering {
        http-profile BranchOffice-Web;
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
    }
}

[edit security policies from-zone TRUST to-zone UNTRUST]
lab@srx1# show
policy internet-access {
    match {
        source-address trust-address-range;
        destination-address any;
        application trust-app-set;
    }
    then {
        permit {
            application-services {
                utm-policy Branch-web-filter;
            }
        }
    }
}
```

Central office: cluster 2

7) The other available type (WebSense) of web-filtering has to be used on this device.

```
{primary:node0}[edit security utm]
lab@srx5# set feature-profile web-filtering type websense-redirect
```

8) It will be enabled on the following existing security policy between TRUST and UNTRUST zones.

Device	Incoming zone	Outgoing zone	Source address entry	Destination address entry	Application	Action
cluster2	TRUST	UNTRUST	172.16.50.0/24	any	junos-http junos-https	permit

9) The URLs listed in the white-list are excluded from web-filtering. To satisfy the given requirements the use of wildcards is needed.

Note: Although the SRX allows using wildcards when defining URLs there are some limitations. The following wildcard rule applies: *\.[]\?* and you must precede all wildcard URLs with http://. You can only use "*" if it is at the beginning of the URL and is followed by a ".". You can only use "?" at the end of the URL. The following wildcard syntax is supported: http://*.juniper.net, http://www.juniper.ne?,

© 2020 Juniper Networks, Inc. All rights reserved.

http://www.juniper.n??. The following wildcard syntax is NOT supported: *.juniper.net , www.juniper.ne?, http://*juniper.net, http://*.

a. Bing.com site with the pages listing the search results should be permitted
   i. http://*.bing.com
b. The same applies for google.com
   i. http://*.google.com
c. The juniper.net site is allowed
   i. http://www.juniper.net

10)For denying defined URLs the black-list has to be used

d. Anything that start with www.facebook.com
   i. http://www.facebook.com

```
{primary:node0}[edit security utm]
lab@srx5# show
custom-objects {
    url-pattern {
        Allowed-sites {
            value [ http://*.bing.com http://*.google.com http://www.juniper.net ];
        }
        Blocked-sites {
            value http://www.facebook.com;
        }
    }
    custom-url-category {
        Allowed-sites-category {
            value Allowed-sites;
        }
        Blocked-sites-category {
            value Blocked-sites;
        }
    }
}
feature-profile {
    web-filtering {
        url-whitelist Allowed-sites-category;
        url-blacklist Blocked-sites-category;
    }
}
```

11) The configuration below shows the defined server details - IP address and port.

```
{primary:node0}[edit security utm feature-profile web-filtering websense-redirect]
lab@srx5# show
profile central-Office-web-filtering {
    server {
        host 80.200.200.200;
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
        port 12345;
    }
}
```

12) The fallback settings define the request's handling when problems or issues arise, specifically the behavior can be defined for following situations:
    a. When the device cannot connect to the server
    b. When the defined timeout for server responses elapses
    c. When the engine received too many request
    d. All other problems

    Based on the instructions the actions for a. and b. are "block", and for c. and d. options are "permit and log".

```
{primary:node0}[edit security utm feature-profile web-filtering websense-redirect
profile central-Office-web-filtering]
lab@srx5# show | find fall
fallback-settings {
    default log-and-permit;
    server-connectivity block;
    timeout block;
    too-many-requests log-and-permit;
}
```

13) The command below sets the timeout for WebSense server responses to 180 seconds.

```
{primary:node0}[edit security utm feature-profile web-filtering websense-redirect
profile central-Office-web-filtering]
lab@srx5# set timeout 180
```

14) Definition of message the clients will receive in case of blocked request is:

```
{primary:node0}[edit security utm feature-profile web-filtering websense-redirect
profile central-Office-web-filtering]
lab@srx5# set custom-block-message "SRX blocked the request!"
```

15) The engine will include the string defined in the "account" parameter into the requests sent to WebSense to achieve specific treatment.

```
{primary:node0}[edit security utm feature-profile web-filtering websense-redirect
profile central-Office-web-filtering]
lab@srx5# set account centraloffice
```

16) The "sockets" parameter defines the limit for parallel connections to the WebSense server. It has to be set to 5 for the number of parallel connections to stay below 6.

© 2020 Juniper Networks, Inc. All rights reserved.

```
{primary:node0} [edit security utm feature-profile web-filtering websense-redirect
profile central-Office-web-filtering]
lab@srx5# set sockets 5
```

Similarly, as on the srx1 device the utm-policy needs to be created and associated with appropriate security policy:

```
{primary:node0}[edit security utm]
lab@srx5# show | find utm-policy
utm-policy central-office-utm {
    web-filtering {
        http-profile central-Office-web-filtering;
    }
}

{primary:node0}[edit security policies from-zone TRUST to-zone UNTRUST policy
internet-access]
lab@srx5# show
match {
    source-address trust-address-range;
    destination-address any;
    application internet-apps;
}
then {
    permit {
        application-services {
            utm-policy central-office-utm;
        }
    }
}
```

Home office: srx8

17) The following security policy will be used to enforce the web-filtering:

Device	Incoming zone	Outgoing zone	Source address entry	Destination address entry	Application	Action
srx8	TRUST	UNTRUST	192.168.10.0/24	any	junos-http junos-https	permit

18) The “juniper-local” option tells the device to make the web-filtering decisions purely on its own using white, black lists and default action.

```
[edit security utm feature-profile web-filtering]
lab@srx8# set type juniper-local
```


© 2020 Juniper Networks, Inc. All rights reserved.

19)The same approach for configuring white and black lists as on the cluster 2 is used.

```
[edit security utm]
lab@srx8# set custom-objects url-pattern denied-sites value http://www.facebook.com

[edit security utm]
lab@srx8# set custom-objects url-pattern denied-sites value http://www.myspace.com

[edit security utm]
lab@srx8# set custom-objects custom-url-category denied-sites-category value denied-
sites
```

To deny these sites the created custom category has to be defined as blacklist.

```
[edit security utm feature-profile web-filtering]
lab@srx8# show
url-blacklist denied-sites-category;
```

20)The “default” action instructs the engine how it should handle all requests where the URL did not match the black or white list.

```
[edit security utm feature-profile web-filtering juniper-local profile HomeOffice-web-
filtering]
lab@srx8# set default permit
```

21)Following command defines the message the clients receive in case their request was blocked:

```
[edit security utm feature-profile web-filtering juniper-local profile HomeOffice-web-
filtering]
lab@srx8# set custom-block-message "This page is not allowed!"
```

22)This step requires all the fallback options to be set to block.

```
[edit security utm feature-profile web-filtering juniper-local profile HomeOffice-web-
filtering]
lab@srx8# show | find fallback
fallback-settings {
    default block;
    timeout block;
    too-many-requests block;
}
```

The remaining step is to create the utm-policy referencing the web-filtering profile and then associate the utm-policy with the appropriate security policy.

```
[edit security utm]
lab@srx8# show | find utm-policy
utm-policy home-office-utm {
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
    web-filtering {
        http-profile HomeOffice-web-filtering;
    }
}
```

```
[edit security policies from-zone TRUST to-zone UNTRUST policy internet-access]
lab@srx8# show
match {
    source-address trust-address-range;
    destination-address any;
    application internet-apps;
}
then {
    permit {
        application-services {
            utm-policy home-office-utm;
        }
    }
}
```

Task 2: Antivirus

The information listed here is about the antivirus feature and its configuration based on the given requirements.

Home office: srx8

1) The full file-based scanning mode of operation for the antivirus engine is defined under “Sophos-engine” stanza in the anti-virus feature profile.
2) The following existing security policy will be used, but in order to cope with the task the application-set needs to be adjusted by adding FTP and SMTP applications to it. Because srx8 device already has the web-filtering enabled on this security policy, the existing utm-policy can be reused, and only antivirus feature profile will be added to it – the procedure is shown at the end of this task.

Device	Incoming zone	Outgoing zone	Source address entry	Destination address entry	Application	Action
srx8	TRUST	UNTRUST	192.168.10.0/24	any	junos-http junos-https	permit

```
[edit applications]
lab@srx8# show
application-set internet-apps {
    application junos-http;
    application junos-https;
    application junos-mail;
    application junos-ftp;
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
}

[edit security policies from-zone TRUST to-zone UNTRUST]
lab@srx8# show policy internet-access
match {
    source-address trust-address-range;
    destination-address any;
    application internet-apps;
}
then {
    permit {
        application-services {
            utm-policy home-office-utm;
        }
    }
}
```

3) Custom objects (url-pattern, custom-url-category) and “url-whitelist” parameter are used to exclude the prefix www.company.com from being scanned.

   Note: The url-whitelist is defined for the whole anti-virus feature profile regardless of the engine mode of operation (full file-based, Juniper-Express, etc.)

```
[edit security utm]
lab@srx8# show custom-objects
url-pattern {
    denied-sites {
        value [ http://www.facebook.com http://www.myspace.com ];
    }
    company-site {
        value http://www.company.com;
    }
}
custom-url-category {
    denied-sites-category {
        value denied-sites;
    }
    AV-excluded-sites {
        value company-site;
    }
}

[edit security utm feature-profile anti-virus]
lab@srx8# show | match whitelist
url-whitelist AV-excluded-sites;
```

4) Similar approach is also valid for mime types - custom objects (mime-pattern) and “mime-whitelist” stanza. Prefixes need to be used for matching all video, application

© 2020 Juniper Networks, Inc. All rights reserved.

and audio mime types. The string used as prefix must have the "/" character placed at the end (for example "video/", "audio/", etc.)

Two mime patterns stanzas (list and exception) are available, one for excluding and one for including defined mime types from scanning respectively.

Note: The mime types are defined for the whole anti-virus feature profile regardless of the engine mode of operation (full file-based, Juniper-Express, etc.)

```
[edit security utm custom-objects]
lab@srx8# show mime-pattern
AV-excluded-mime {
    value [ audio/ video/ application/ ];
}
AV-included-mime {
    value [ application/javascript application/ecmascript ];
}

[edit security utm feature-profile anti-virus]
lab@srx8# show mime-whitelist
list AV-excluded-mime;
exception AV-included-mime;
```

5) Scanning timeout set to 10 minutes (600 seconds)

```
lab@srx8# set security utm feature-profile anti-virus sophos-engine profile AV-full-
file-scan scan-options timeout 600
```

6) The notifications details are configured under the "notification-options ", such as custom message text, notification type (message or protocol level error), if emails should be sent for email protocols (IMAP, POP3, SMTP). These parameters are defined separately for various situations:
   a. when virus is detected (step 34)
   b. when a problem occurs during processing the traffic and the engine blocks or permits the message (step 36)

```
[edit security utm feature-profile anti-virus sophos-engine profile AV-full-file-scan
notification-options]
lab@srx8# show
virus-detection {
    type message;
    custom-message "AV Engine detected virus!";
    custom-message-subject AntiVirus;
}
```

7) The "fallback-options" stanza contains parameters that define handling of packets for various cases, such as when the engine is out of resources, the scanning took too long, the engine is not ready, etc.

© 2020 Juniper Networks, Inc. All rights reserved.

```
[edit security utm feature-profile anti-virus sophos-engine profile AV-full-file-scan]
lab@srx8# show
fallback-options {
    default log-and-permit;
    content-size block;
    engine-not-ready block;
    timeout block;
    out-of-resources block;
    too-many-requests block;
}
```

8) SRX allows defining notifications/messages for fallback situations. Messages and the notifications behavior are defined separately for cases when the action executed on the traffic is “block” and separately for the action “log-and-permit” (non-block). The configuration shown below defines the behavior as requested in this task.

Note: For NON-BLOCK cases the defined custom message is used only for email protocols. The other scanned protocols don’t generate anything because the data is transmitted.

```
[edit security utm feature-profile anti-virus sophos-engine profile AV-full-file-scan
notification-options]
lab@srx8# show
virus-detection {
    type message;
    custom-message "AV Engine detected virus!";
    custom-message-subject AntiVirus;
}
fallback-block {
    type protocol-only;
    notify-mail-sender;
    custom-message "AV denied the message, because it was not able to scan it!";
    custom-message-subject AntiVirus;
}
fallback-non-block {
    notify-mail-recipient;
    custom-message "AV was not able to scan the message! ";
    custom-message-subject Antivirus;
}
```

9) The antivirus scanning process takes time and sometimes can cause timeout on the clients receiving the data. The “trickling” feature can be used to prevent this situation. The engine sends periodically, in defined intervals, only small portions of the data to the recipient, even if the data has not been scanned yet.

```
[edit security utm feature-profile anti-virus sophos-engine profile AV-full-file-scan]
lab@srx8# show
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
trickling timeout 25;
```

As mentioned earlier the srx8 device has already utm-policy associated with appropriate security policy. Therefore, the remaining task here is to modify the utm-policy and associate the created antivirus feature profile with the appropriate protocols (step 27 defines the HTTP, FTP and SMTP traffic is subject to scanning):

```
[edit security utm]
lab@srx8# show | find utm-policy
utm-policy home-office-utm {
    anti-virus {
        http-profile AV-full-file-scan;
        ftp {
            upload-profile AV-full-file-scan;
            download-profile AV-full-file-scan;
        }
        smtp-profile AV-full-file-scan;
    }
    web-filtering {
        http-profile HomeOffice-web-filtering;
    }
}
```

Task 3: Content Filtering

This section provides details about the solution for the defined content filtering requirements.

Central office: cluster 2

1) Because the content filtering takes place on the traffic from zone TRUST to zone UNTRUST on the cluster 2, it is suitable to reuse the existing utm-policy (created in task 1).
2) New feature profile for content filtering covering following aspects needs to be defined:
    a. HTTP content types: exe files, cookies and java applets
        i. The “block-content-type” stanza defines which content types in HTTP messages are blocked

```
{primary:node0} [edit security utm feature-profile content-filtering profile central-
office-content-filter]
lab@srx5# show
block-content-type {
    java-applet;
    exe;
    http-cookie;
}
```


© 2020 Juniper Networks, Inc. All rights reserved.

b. mime: video prefix
    i. Similar as before the mime types have to be defined as custom objects and then referenced in the “block-mime” stanza. The use of prefixes is needed here to achieve matching all video mime types.

```
{primary:node0} [edit security utm]
lab@srx5# show custom-objects mime-pattern
mime-video-prefix {
    value video/;
}

{primary:node0} [edit security utm feature-profile content-filtering profile central-
office-content-filter]
lab@srx5# show
block-mime {
    list mime-video-prefix;
}
```

c. bat and sh file extensions
    i. Also, file extensions are defined as custom object and then referenced in the “block-extension” parameter.

```
{primary:node0} [edit security utm]
lab@srx5# show custom-objects filename-extension
blocked-file-ext {
    value [ bat sh ];
}

{primary:node0} [edit security utm feature-profile content-filtering profile central-
office-content-filter]
lab@srx5# show | match extension
block-extension blocked-file-ext;
```

d. HTTP protocol TRACE
    i. Here created custom object containing HTTP command is referenced in the “protocol-command” statement.

```
{primary:node0} [edit security utm]
lab@srx5# show custom-objects protocol-command
http-TRACE {
    value trace;
}

{primary:node0} [edit security utm feature-profile content-filtering profile central-
office-content-filter]
lab@srx5# show | match block-command
block-command http-TRACE;
```


© 2020 Juniper Networks, Inc. All rights reserved.

3) Below are the custom message definition clients receive when the data is blocked.

```
{primary:node0} [edit security utm feature-profile content-filtering profile central-
office-content-filter]
lab@srx5# set notification-options custom-message "Blocked content by SRX!"
```

Following parameter needs to be configured to tell the device to generate protocol error when blocking the data.

```
{primary:node0} [edit security utm feature-profile content-filtering profile central-
office-content-filter]
lab@srx5# set notification-options type protocol-only
```

```
[edit security utm utm-policy central-office-utm]
lab@srx5# show
content-filtering {
    http-profile central-office-content-filter;
}
web-filtering {
    http-profile central-Office-web-filtering;
}
```

Task 4: Antispam

The instructions to fulfill the antispam tasks are presented here.

Central office: cluster 2

1) The email server location is in DMZ zone and the IP address is 172.16.55.100.
2) Because the SMTP communication going to this server needs to be checked a new security policy has to be defined:
    a. zone context: UNTRUST --> to DMZ
    b. addresses: any --> 172.16.55.100
    c. application: junos-mail
    d. this policy needs to be placed before the existing ones to provide correct treatment for the SMTP traffic going only to the mail server

```
[edit security]
lab@srx5# set zones security-zone DMZ address-book address smtp-server
172.16.55.100/32
```

```
[edit security policies from-zone UNTRUST to-zone DMZ]
lab@srx5# show
policy SMTP-server {
    match {
        source-address any;
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
        destination-address smtp-server;
        application junos-mail;
    }
    then {
        permit;
    }
}
policy warehouse-dmz-access {
    match {
        source-address dc-warehouse-range;
        destination-address dmz-range;
        application any;
    }
    then {
        permit;
    }
}
…
```

3) The antispam feature is configured under the “edit security utm feature-profile anti-spam“ stanza. The white and black lists define in the antispam configuration allowed and denied sources (IP addresses, domains or email addresses) for email communication.
The checking starts with evaluating the senders (or relay agents) IP address against the white list, and if no match is found the black list is examined for the IP address. If neither block nor white list resulted in a match the SBL (spam block list) server will be consulted, but only if it is explicitly configured. If the IP address did not result in any matches the domain is checked against the white list. Again, if no match is found the domain is verified against the black list. At last the email address of the sender is checked in similar manner as domain. If no match is found at all the email is normally transmitted.

Note: The antispam black and white list reference “url-pattern” custom object and NOT the “custom-url-category”!

The requirements define:

- 5.5.5.4 IP address is considered malicious --> blacklist
- 5.5.5.5 IP address is allowed --> whitelist
- 123.123.123.123 host is considered dangerous --> blacklist
- subject of the identified spam messages has to be tagged with the prefix “SPAM!!!”

4) The custom objects listed above needs to be modified to cover the requirements from this step.

© 2020 Juniper Networks, Inc. All rights reserved.

a. bad.com, spam.com --> blacklist
b. spam@company.com, adv@company.com --> blacklist

```
[edit security utm custom-objects]
lab@srx5# show
url-pattern {
    allowed-mail-sources {
        value 5.5.5.5;
    }
    denied-mail-sources {
        value [ 5.5.5.4 123.123.123.123 bad.com spam.com "spam@company.com"
"adv@company.com" ];
    }
}

[edit security utm feature-profile anti-spam]
lab@srx5# show
address-whitelist allowed-mail-sources;
address-blacklist denied-mail-sources;
sbl {
    profile SMTP-server-antispam-prof {
        spam-action tag-subject;
        custom-tag-string "SPAM!!!";
    }
}
```

5) To tell the device to perform the decisions internally without consulting the SBL server following statement has to be executed:

```
[edit security utm]
lab@srx5# set default-configuration anti-spam type sbl

[edit security utm]
lab@srx5# set feature-profile anti-spam sbl profile SMTP-server-antispam-prof no-sbl-
default-server
```

Again, as in the previous tasks the utm-policy needs to be created and associated with appropriate security policy.

```
[edit security utm utm-policy SMTP-server-utm-policy]
lab@srx5# show
anti-spam {
    smtp-profile SMTP-server-antispam-prof;
}

[edit security policies from-zone UNTRUST to-zone DMZ policy SMTP-server]
lab@srx5# show
match {
    source-address any;
    destination-address smtp-server;
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
    application junos-mail;
}
then {
    permit {
        application-services {
            utm-policy SMTP-server-utm-policy;
        }
    }
}
```

Task 5: Testing

The SRX device provides a simple tool (operational mode command) for checking the utm configuration (anti-spam, anti-virus, web-filtering).

```
lab@srx5> test security utm ?
Possible completions:
  anti-spam            Test anti-spam profile
  anti-virus           Test anti-virus profile
  web-filtering        Test web-filtering profile
```

Example:

Note: These commands are not currently available in the vSRX

```
lab@srx5> test security utm anti-spam profile SMTP-server-antispam-prof test-string
123.123.123.123
Anti-spam test result:
Return SPAM, action Tag email subject, reason Match local blacklist

lab@srx5> test security utm anti-spam profile SMTP-server-antispam-prof test-string
5.5.5.5
Anti-spam test result:
Return NON SPAM, action Pass, reason Match local whitelist
```


© 2020 Juniper Networks, Inc. All rights reserved.

Appendix - Chapter 5: IPsec VPNs

The purpose of this appendix is to guide you through the milestones of Chapter 5. You will find here configuration excerpts, tips and recommendations for successful completion of IPsec VPN tasks.

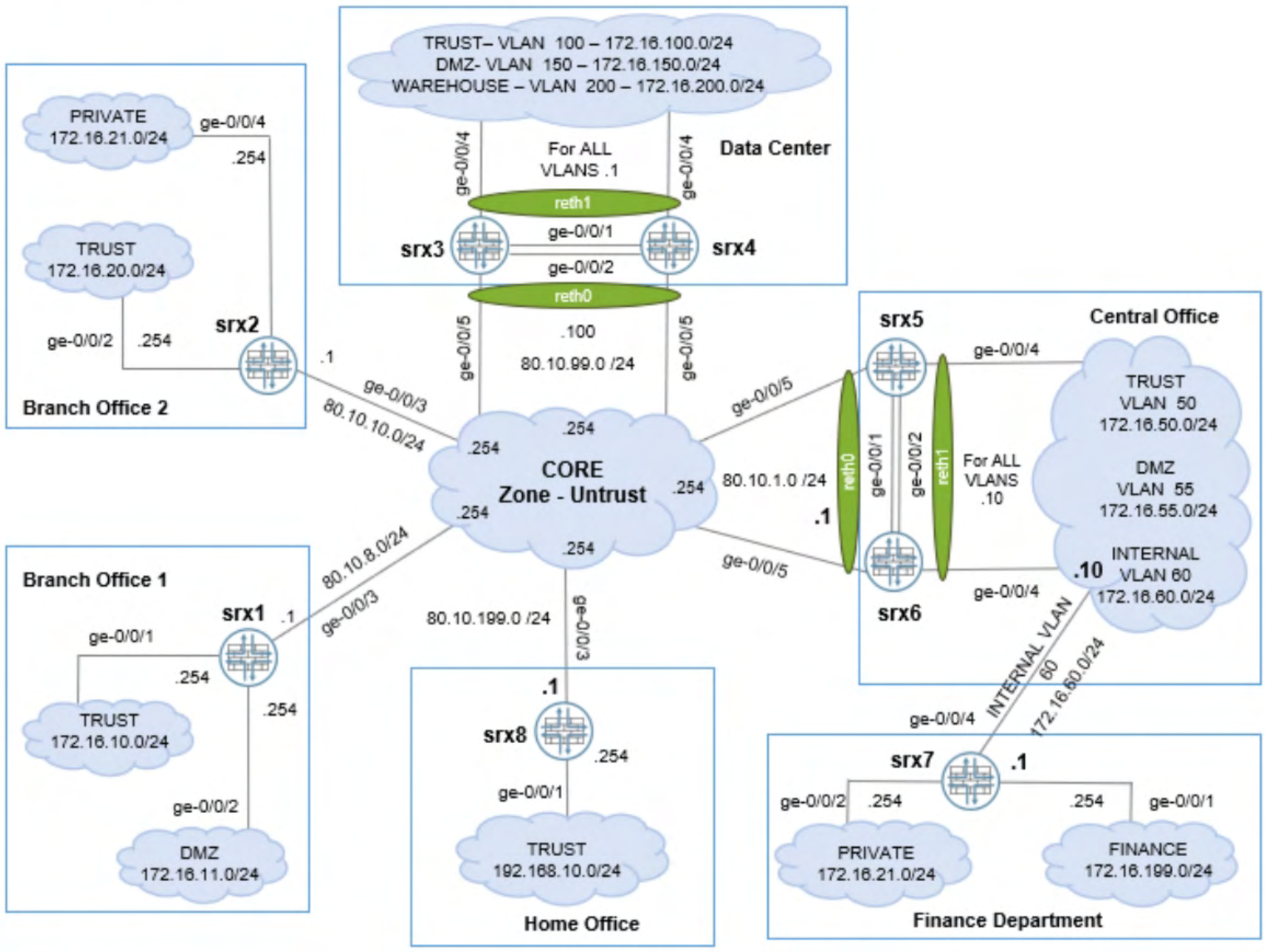


Figure 1: Chapter 5 Topology

IPsec VPN overview

Internet Protocol Security (IPsec) is a protocol suite of open standards for securing IP communications over networks. It operates over the IP protocol and supports both unicast and multicast traffic.

© 2020 Juniper Networks, Inc. All rights reserved.

Three major concerns – data confidentiality, data integrity and data authentication – are addressed by the IPsec. Data confidentiality is achieved using cryptographic techniques by encrypting the original packet to make the information value extraction very difficult for not involved parties. Data Encryption Standard (DES), triple Data Encryption Standard (3DES), or Advanced encryption standard (AES) are used cryptographic algorithms. Data integrity is provided through application of hashing algorithms, such as Message digest 5 (MD5) or Secure hash algorithm 1 or 2 (SHA1 or SHA2). They help recognize if even slightest modification has been done to the data as it traversed through the network. And authentication is based on secret keys or certificates to assure the data origin is known and trusted. IPsec defines how the encryption, validation, and authentication methods are actually implemented in networks.

IPsec protocols are Encapsulated security payload (ESP) and Authentication header (AH). Both of these protocols provide data integrity, authentication, and antireplay services. ESP in addition provides also data confidentiality, i.e. the ESP protocol encrypts the data whereas the AH does not. Antireplay helps to detect repeated packets which are then discarded. This saves processing resources which otherwise would be wasted for processing such packets. IPsec operates either in tunnel or transparent mode. In tunnel the whole original packet is encapsulated into IPsec packet (with new IP and IPsec headers). Typically, the tunnel mode is implemented between IPsec gateways or remote clients and gateways. The whole IPsec processing might be totally transparent to the end communicating devices, because the gateways handle and perform it. In the transport mode on the other hand the communicating end stations are aware of the IPsec because they create the IPsec packets right away and no packet encapsulation takes place. Most of the IPsec deployments utilize the tunnel mode.

In Junos two methods of IPsec implementation are provided.

- Policy-based VPNs – the IPsec VPN tunnel is specified as the parameter under the permit action within security policy. Traffic matching the security policy is transmitted within the tunnel. Typical use for policy-based VPNs is to provide secure access for remote users.
- Route-based VPNs – the decision whether a traffic will traverse the VPN is made based on the routing information. Each route-based IPsec VPN is bound to a secure tunnel interface st0.x and if the next-hop from the routing lookup is the st0.x interface or a secure tunnel interface IP address of the peer the traffic will be placed into the tunnel. Typically, with route-based VPNs only one VPN exists between two peers. This aspect allows to create more complex architectures with route-based VPNs such as hub-and-spoke, full-mesh or hybrid multipoint VPNs.

© 2020 Juniper Networks, Inc. All rights reserved.

Depending the environment, number of devices and requirements for the IPsec VPNs the applied architectures vary from simple ones, e.g. site-to-site or remote access, to very complex ones, e.g. hub-and-spoke or full-mesh.

Both endpoints, initiator (start the communication) and responder, require knowledge of certain information (used algorithms, keys, protocol, etc.) for establishing an IPsec VPN. These details can be provided to both tunnel end points either manually or dynamically through Internet key exchange protocol (IKE). Manually option is used very rarely because various reasons, e.g. lack of flexibility, prone to typos and configuration errors, etc. IKE protocol is used to setup security associations for IPsec VPNs, i.e. set of attributes and details to support secure communication such as the algorithms, keys, etc. The IKE communication happens over UDP protocol with port 500 and is performed in two phases. IKE phase 1 negotiates most importantly the encryption algorithm, hashing algorithm and authentication method between peers and result in establishing secure bidirectional tunnel between them. This tunnel then serves for securing the IKE phase 2 control communication which negotiates the encryption algorithm, hashing algorithm and IPsec protocol. As a result, are two unidirectional secured tunnels used for transmitting the actual data. Diffie-Hellman key exchanges serves to determine the symmetric encryption key on both peers without exchanging any sensitive information and is mandatory for phase 1 and optional for phase 2. Performing Diffie-Hellman in phase 2 is called perfect forwarding secrecy (PFS). If both peers have statically defined IP addresses the IKE phase 1 communication is done in main mode. However, if one of the endpoints has dynamically assigned IP address (for example through DHCP) the IKE phase 1 mode must be aggressive. In aggressive mode fewer messages are exchanged comparing to main mode. The IKE phase 2 is generally called quick mode.

The IPsec monitoring can be done in either IKE phase. Dead peer detection method (DPD) performs phase 1 monitoring and is supported by other vendors. However, the VPN monitor is supported only on Juniper platforms and monitors the phase 2 tunnels by utilizing ICMP echo request and response messages. They are sent over the phase 2 tunnels and use IP addresses of the gateways.

© 2020 Juniper Networks, Inc. All rights reserved.

Task 1: Configuring Policy-based VPN

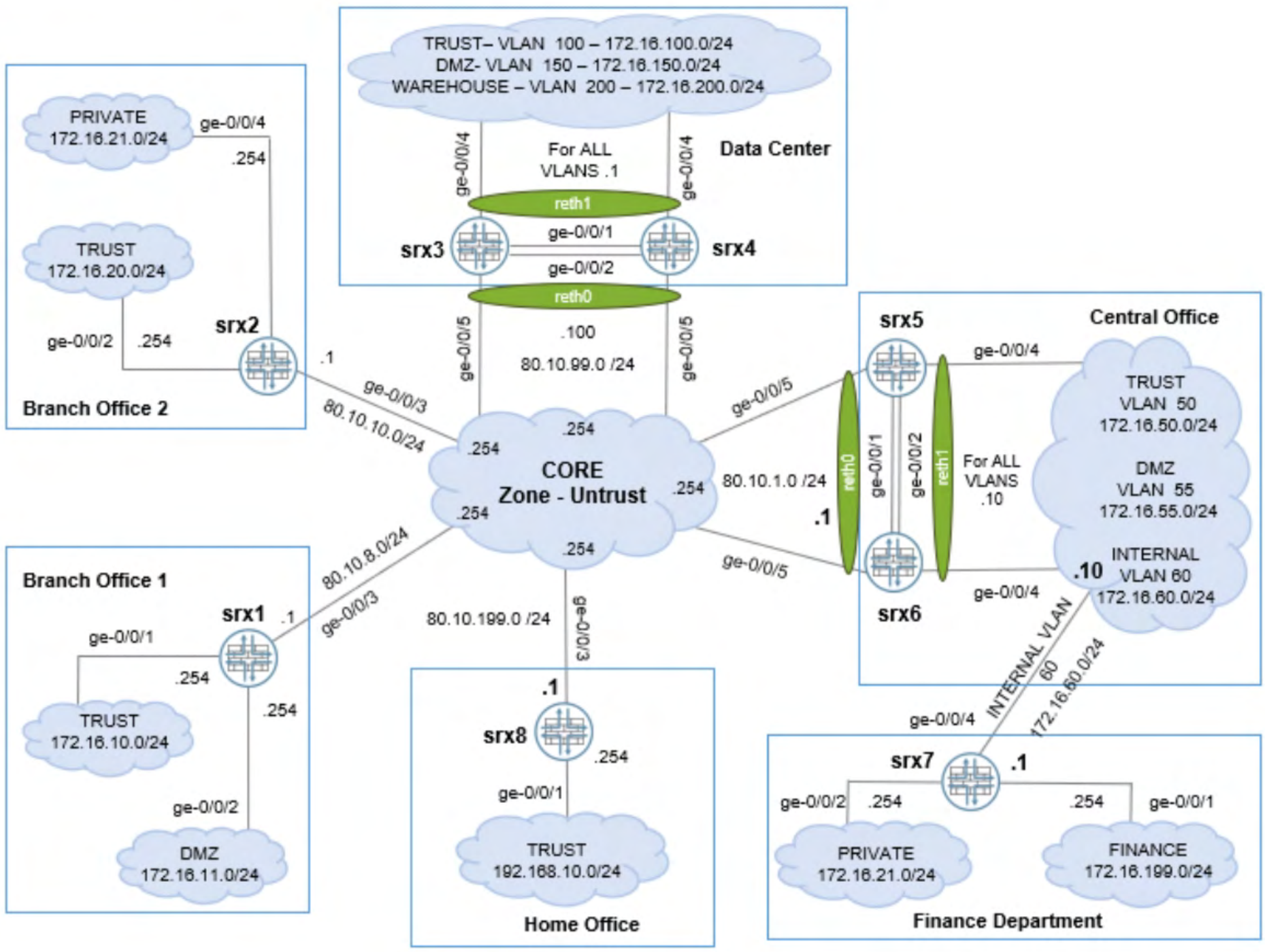


Figure 2: Chapter 5 – Task 1 Topology

In this task you will configure lab equipment as necessary to build Policy-based VPN between Data Center, Home Office and Finance department.

1) Configure the IPsec VPN on every device according to the table below, which reflects the topology image.

Local Peer	Interface	Security zone	Remote Peer	Interface	Security zone
srx7	ge-0/0/4.60	Untrust	Cluster1	reth0.0	Untrust
srx8	ge-0/0/3.0	Untrust	Cluster1	reth0.0	Untrust

SRX7

© 2020 Juniper Networks, Inc. All rights reserved.

```
lab@srx7# show security ike
proposal ike-proposal {
    authentication-method pre-shared-keys;
    dh-group group5;
    authentication-algorithm sha1;
    encryption-algorithm 3des-cbc;
    lifetime-seconds 86400;
}
policy ike-policy {
    mode aggressive;
    proposals ike-proposal;
    pre-shared-key ascii-text "$9$zj5Y3/tleWN-wM8qfTzCAvWLNb2"; ## SECRET-DATA
}
gateway ike-gateway {
    ike-policy ike-policy;
    address 80.10.99.100;
    dead-peer-detection {
        always-send;
        interval 10;
        threshold 5;
    }
    local-identity hostname srx7;
    external-interface ge-0/0/4.60;
}

lab@srx7# show security ipsec
proposal ipsec-proposal {
    protocol esp;
    authentication-algorithm hmac-sha1-96;
    encryption-algorithm aes-192-cbc;
    lifetime-kilobytes 5000;
}
policy ipsec-policy {
    proposals ipsec-proposal;
}
vpn to-cluster1 {
    ike {
        gateway ike-gateway;
        ipsec-policy ipsec-policy;
    }
    establish-tunnels on-traffic;
}
```

SRX8

```
lab@srx8# show security ike
proposal ike-proposal {
    authentication-method pre-shared-keys;
    dh-group group1;
    authentication-algorithm md5;
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
    encryption-algorithm des-cbc;
    lifetime-seconds 86400;
}
policy ike-policy {
    mode main;
    proposals ike-proposal;
    pre-shared-key ascii-text "$9$5znCO1hKMXtuMX7-2gTz3"; ## SECRET-DATA
}
gateway ike-gateway {
    ike-policy ike-policy;
    address 80.10.99.100;
    dead-peer-detection {
        always-send;
        interval 10;
        threshold 5;
    }
    external-interface ge-0/0/3.0;
}

lab@srx8# show security ipsec
proposal ipsec-proposal {
    protocol esp;
    authentication-algorithm hmac-sha1-96;
    encryption-algorithm aes-128-cbc;
    lifetime-seconds 43200;
}
policy ipsec-policy {
    perfect-forward-secrecy {
        keys group2;
    }
    proposals ipsec-proposal;
}
vpn to-cluster1 {
    ike {
        gateway ike-gateway;
        ipsec-policy ipsec-policy;
    }
    establish-tunnels immediately;
}
```

2) Central Office srx5/srx6 cluster provides only dynamical NAT-src service.

```
[edit security nat]
lab@srx5# show
source {
   rule-set int-nat {
        from zone INTERNAL;
        to zone UNTRUST;
        rule for-finance-dep {
            match {
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
                source-address 172.16.60.0/24;
            }
             then {
                source-nat interface;
            }
        }
    }
}
```

3) VPN between srx8 and Cluster1 must meet the following requirements:

   Configuration for the steps a) and b) below can be done from the `[edit security ike]` level of CLI hierarchy. There are three configuration elements that need to be defined there: Phase1 IKE proposal, Phase1 IKE policy and Phase1 IKE gateway.

   a. Validate peer reachability with DPD option. The keepalives should be sent to the neighboring peer regardless of traffic patterns every 10 seconds. Consider peer unreachable if the number of DPD retransmissions exceeds 5 packets.
   b. IKE phase 1 proposal must include: preshared key “juniper”, DES, DH G1, MD5. Rekey Phase1 every 24 hours.

Cluster1

```
lab@srx3# show security ike
proposal ike-proposal-1 {
    authentication-method pre-shared-keys;
    dh-group group1;
    authentication-algorithm md5;
    encryption-algorithm des-cbc;
    lifetime-seconds 86400;
}
proposal ike-proposal-2 {
    authentication-method pre-shared-keys;
    dh-group group5;
    authentication-algorithm sha1;
    encryption-algorithm 3des-cbc;
    lifetime-seconds 86400;
}
policy ike-policy-1 {
    mode main;
    proposals ike-proposal-1;
    pre-shared-key ascii-text "$9$5znCO1hKMXtuMX7-2gTz3"; ## SECRET-DATA
}
policy ike-policy-2 {
    mode aggressive;
    proposals ike-proposal-2;
    pre-shared-key ascii-text "$9$zj5Y3/tleWN-wM8qfTzCAvWLNb2"; ## SECRET-DATA
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
}
gateway ike-gateway-1 {
    ike-policy ike-policy-1;
    address 80.10.199.1;
    dead-peer-detection {
        always-send;
        interval 10;
        threshold 5;
    }
    external-interface reth0.0;
}
gateway ike-gateway-2 {
    ike-policy ike-policy-2;
    dynamic hostname srx7;
    dead-peer-detection {
        always-send;
        interval 10;
        threshold 5;
    }
    external-interface reth0.0;
}


lab@srx3# show security ipsec
traceoptions {
    flag security-associations;
}
proposal ipsec-proposal-1 {
    protocol esp;
    authentication-algorithm hmac-sha1-96;
    encryption-algorithm aes-128-cbc;
    lifetime-seconds 43200;
}
proposal ipsec-proposal-2 {
    protocol esp;
    authentication-algorithm hmac-sha1-96;
    encryption-algorithm aes-192-cbc;
    lifetime-kilobytes 5000;
}
policy ipsec-policy-1 {
    perfect-forward-secrecy {
        keys group2;
    }
    proposals ipsec-proposal-1;
}
policy ipsec-policy-2 {
    proposals ipsec-proposal-2;
}
vpn to-srx8 {
    ike {
        gateway ike-gateway-1;
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
        ipsec-policy ipsec-policy-1;
    }
    establish-tunnels immediately;
}
vpn to-srx7 {
    ike {
        gateway ike-gateway-2;
        ipsec-policy ipsec-policy-2;
    }
}
```

SRX8

```
lab@srx8# show security ike
proposal ike-proposal {
    authentication-method pre-shared-keys;
    dh-group group1;
    authentication-algorithm md5;
    encryption-algorithm des-cbc;
    lifetime-seconds 86400;
}
policy ike-policy {
    mode main;
    proposals ike-proposal;
    pre-shared-key ascii-text "$9$5znCO1hKMXtuMX7-2gTz3"; ## SECRET-DATA
}
gateway ike-gateway {
    ike-policy ike-policy;
    address 80.10.99.100;
    dead-peer-detection {
        always-send;
        interval 10;
        threshold 5;
    }
    external-interface ge-0/0/3.0;
}

lab@srx8# show security ipsec
proposal ipsec-proposal {
    protocol esp;
    authentication-algorithm hmac-sha1-96;
    encryption-algorithm aes-128-cbc;
    lifetime-seconds 43200;
}
policy ipsec-policy {
    perfect-forward-secrecy {
        keys group2;
    }
    proposals ipsec-proposal;
}
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
vpn to-cluster1 {
    ike {
        gateway ike-gateway;
        ipsec-policy ipsec-policy;
    }
    establish-tunnels immediately;
}
```

Note: The proposal must be the same for both peers that are participating in Phase1 establishment. The mistake at this configuration step will lead to the failure of Phase1 establishment with the possible cause code "`No proposal chosen`" in the kmd log on the responder's side.

The preshared key's value together with the tunnel's mode is defined in the Phase1 IKE Policy. The previously defined Phase1 proposal also referenced in the Phase1 policy:

Note: The other possible issue during Phase1 configuration is a mismatch of preshared key's value. The mistake at this configuration step will lead to the failure of Phase1 establishment with the possible cause code "`Invalid payload type`" in the kmd log on the responder's side.

Note: One more possible issue during Phase1 configuration is a mismatch of peers' logical interfaces that are specified with the "`address`" and "`external-interface`" keywords. The mistake at this configuration step will lead to the failure of Phase1 establishment with the possible cause code "`Remote peer is not recognized`" in the kmd log on the responder's side.

Note: The proposal must be the same for both peers that are participating in IPsec tunnel establishment. The mistake at this configuration step will lead to the failure of Phase2 establishment with the possible cause code "`No proposal chosen`" in the kmd log on the responder's side.

The Perfect Forward Secrecy must be configured according to conditions of task c). You can accomplish it by specifying DH group at appropriate part of IPsec policy's configuration.

Next step is to bind together previously configured IKE gateway and IPsec policy, so Phase1 and Phase2 parameters will be combined together and associated with the IPsec VPN's name. One more thing to do is to specify conditions for tunnel establishment with the key word "`establish-tunnels`", which can be either immediately upon commit (value "immediately") or when traffic for the VPN arrives (value "on-traffic"). Because the task does not explicitly define the value, configure the value "immediately" to test whether the VPN configuration is correct.

© 2020 Juniper Networks, Inc. All rights reserved.

c. Ensure that any traffic originated from TRUST zone of Home Office can reach only TRUST zone located in the Data Center and vice versa.

There are two ways to direct traffic into the IPsec tunnel:

1) The security policies define which traffic must forwarded via the tunnel.
2) The routing table directs traffic destined to the particular prefixes via the tunnel.

This task is dedicated for policy-based VPNs and you need to create security policies that will allow you to accomplish step d) conditions.

The configuration excerpts below is representing srx8 settings, although cluster1 configuration is similar.

There are two paired policies that describe traffic between TRUST zones of the Home office and the Data Center. Since this configuration is added to the existing one, you should make sure that the old policies in the same zone context do not shade new policies. Use command "`insert`" to move the new policy above the old one if it is necessary.

```
lab@srx8# show security zones security-zone UNTRUST
address-book {
    address dc-trust-address-range 172.16.100.0/24;
}

lab@srx8# show security policies
from-zone TRUST to-zone UNTRUST {
    policy ipsec-out {
        match {
            source-address trust-address-range;
            destination-address dc-trust-address-range;
            application any;
        }
        then {
            permit {
                tunnel {
                    ipsec-vpn to-cluster1;
                    pair-policy ipsec-in;
                }
            }
        }
    }
}
from-zone UNTRUST to-zone TRUST {
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
policy ipsec-in {
    match {
        source-address dc-trust-address-range;
        destination-address trust-address-range;
        application any;
    }
    then {
        permit {
            tunnel {
                ipsec-vpn to-cluster1;
                pair-policy ipsec-out;
            }
        }
    }
}
```

Note: Keep in mind that ProxyID values for Phase2 negotiation are derived from the security policies. If address book entries referenced as the source-address on one end of the tunnel and the destination-address on the other end of the tunnel are not match it will lead to the failure of Phase2 establishment with the possible cause code "`Failed to match the peer proxy ids`".

d. Collect the IKE Phase2 security association's management events in the kmd file on the cluster1.

```
lab@srx3# show security ipsec
traceoptions {
    flag security-associations;
}
```

If you were careful enough, you noticed that the proposed sequence of configuration actions for steps c) – d) is not optimal. You configured IPsec parameters, after that you switched to the security policies configuration and, finally, you returned back to the IPsec traceoptions.

This implies a simple conclusion that preliminary study of all the tasks can help you making more efficient use of your time.

4) VPN between srx7 and Cluster1 must meet following requirements:
   a. Validate peer reachability with DPD option. The keepalives should be sent to the neighboring peer regardless of traffic patterns every 10 seconds. Consider peer unreachable if the number of DPD retransmissions exceeds 5 packets.

© 2020 Juniper Networks, Inc. All rights reserved.

b. IKE phase 1 proposal must include: preshared key “jncie”, 3DES, DH G5, SHA1. Rekey Phase1 every 24 hours.

The main difference between this step and step 4) is the Phase1 configuration.

The connection between srx8 and cluster1 is established using statically assigned IP addresses. So, the Phase1 mode configured for srx8 and cluster1 is Main mode.

The connection between srx7 and cluster1 is established using dynamically assigned IP address on the srx7 side. That is why the Phase1 mode must be configured as Aggressive mode in IKE policy.

```
[edit security ike policy ike-policy]
lab@srx7# show
mode aggressive;
```

One more setting that need to be done on the initiator’s side is the local-identity value. Example below uses local-identity’s type “hostname” and value “srx7”.

```
[edit security ike gateway ike-gateway]
lab@srx7# show
local-identity hostname srx7;
```

Same string “srx7” must be configured on the responder’s side as dynamic hostname’s value.

```
[edit security ike gateway ike-gateway-2]
lab@cluster1# show
dynamic hostname srx7;
```

c. IKE phase 2 proposal must include: AES-192, ESP, and SHA1. Rekey IPsec tunnel on transmitting 5 MB of traffic.

The IPsec tunnel’s lifetime can be described either as period of time or amount of traffic forward through the tunnel. The example below shows how to accomplish conditions of step c).

```
[edit]
lab@srx7# set security ipsec proposal ipsec-proposal lifetime-kilobytes 5000;
```

d. Ensure that only traffic originated from the FINANCE zone of srx7 can reach Warehouse zone located in the Data Center and vice versa. This traffic must trigger the tunnel establishment.

As mentioned before the “`establish-tunnels`” parameter controls that. Here the task explicitly requires the “on-traffic” value. To test if the configuration is correct

© 2020 Juniper Networks, Inc. All rights reserved.

and such IPsec VPN tunnel established a traffic needs to be received on the firewall that matches the security policy referencing the VPN, i.e. when generating traffic to start the VPN make sure the source and destination IP addresses match the security policy that has the VPN name defined in the action.

Another option is to define the “immediately” value for the “`establish-tunnels`” parameter to make the IPsec VPN to start upon commit. If the configuration is validated by the IPsec VPN coming up correctly change the “`establish-tunnels`” parameter value back to “on-traffic” to comply with the task. See the configuration example below:

```
lab@srx7# show security policies
from-zone FINANCE to-zone INTERNAL {
    policy ipsec-out {
        match {
            source-address finance-address-range;
            destination-address warehouse-range;
            application any;
        }
        then {
            permit {
                tunnel {
                    ipsec-vpn to-cluster1;
                    pair-policy ipsec-in;
                }
            }
        }
    }
}
from-zone INTERNAL to-zone FINANCE {
    policy ipsec-in {
        match {
            source-address warehouse-range;
            destination-address finance-address-range;
            application any;
        }
        then {
            permit {
                tunnel {
                    ipsec-vpn to-cluster1;
                    pair-policy ipsec-out;
                }
            }
        }
    }
}

lab@srx7# show security ipsec
proposal ipsec-proposal {
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
    protocol esp;
    authentication-algorithm hmac-sha1-96;
    encryption-algorithm aes-192-cbc;
    lifetime-kilobytes 5000;
}
policy ipsec-policy {
    proposals ipsec-proposal;
}
vpn to-cluster1 {
    ike {
        gateway ike-gateway;
        ipsec-policy ipsec-policy;
    }
    establish-tunnels on-traffic;
}
```

Finally, the policies have to be created on the Data Center cluster. Note that the *ipsec-out-1* policy needs to be inserted before the other policies using the "`insert`" command.

```
{primary:node0}[edit]
lab@srx3# show security policies
from-zone TRUST to-zone UNTRUST {
    policy ipsec-out-1 {
        match {
            source-address trust-address-range;
            destination-address home-trust;
            application any;
        }
        then {
            permit {
                tunnel {
                    ipsec-vpn to-srx8;
                    pair-policy ipsec-in-1;
                }
            }
        }
    }
}
from-zone WAREHOUSE to-zone UNTRUST {
    policy ipsec-out-2 {
        match {
            source-address warehouse-range;
            destination-address finance-range;
            application any;
        }
        then {
            permit {
                tunnel {
                    ipsec-vpn to-srx7;
                    pair-policy ipsec-in-2;
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
                }
            }
        }
    }
}
from-zone UNTRUST to-zone WAREHOUSE {
    policy ipsec-in-2 {
        match {
            source-address finance-range;
            destination-address warehouse-range;
            application any;
        }
        then {
            permit {
                tunnel {
                    ipsec-vpn to-srx7;
                    pair-policy ipsec-out-2;
                }
            }
        }
    }
}
from-zone UNTRUST to-zone TRUST {
    policy ipsec-in-1 {
        match {
            source-address home-trust;
            destination-address trust-address-range;
            application any;
        }
        then {
            permit {
                tunnel {
                    ipsec-vpn to-srx8;
                    pair-policy ipsec-out-1;
                }
            }
        }
    }
}
```


© 2020 Juniper Networks, Inc. All rights reserved.

Task 2: Configuring Route-based VPN

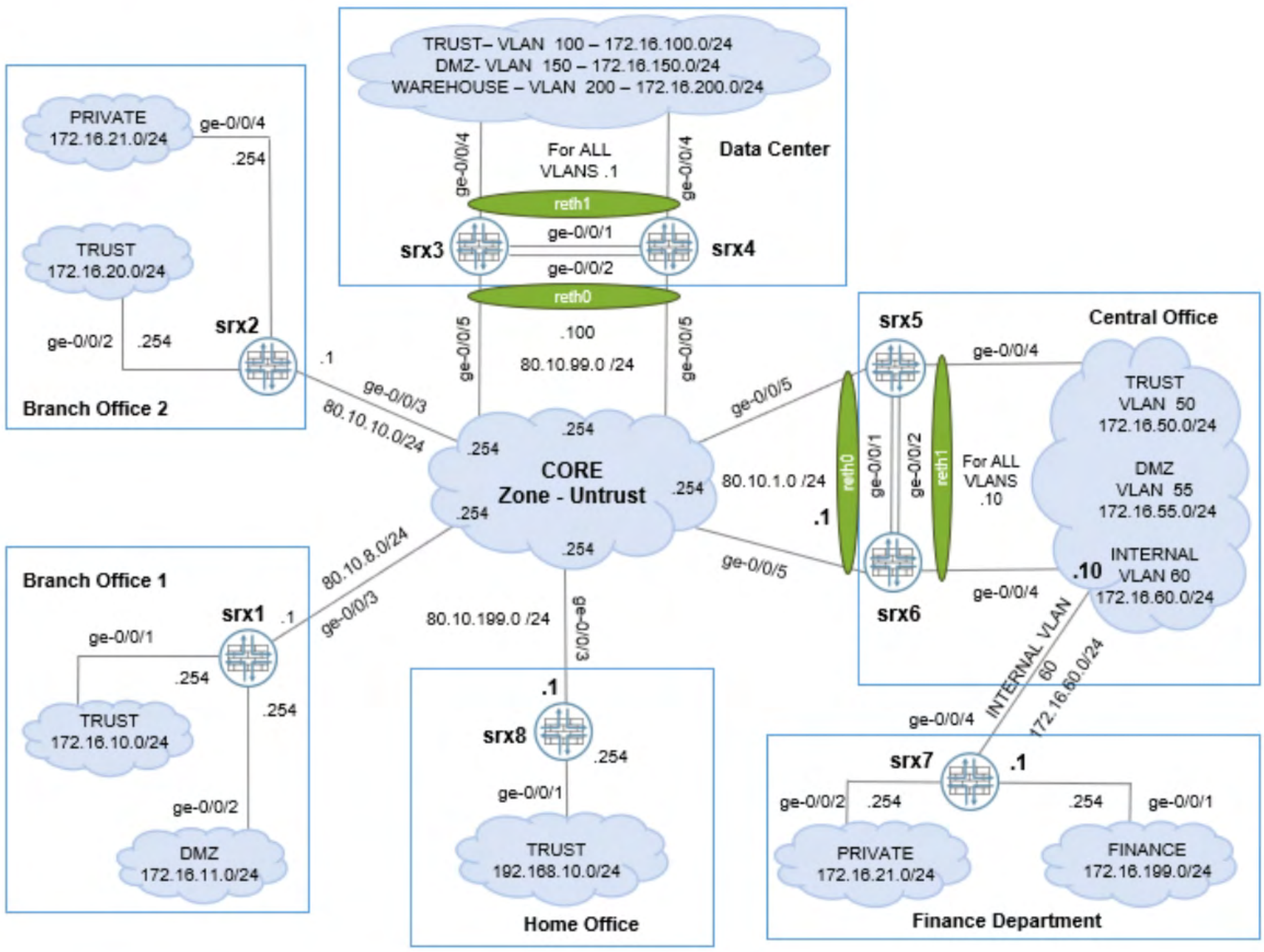


Figure 3: Chapter 5 – Task 2 Topology

In this part you will configure lab equipment as necessary to build full meshed Route-based VPN between Central Office, Branch office 1 and Branch office 2.

1) Branch offices have direct tunnel to each other and can communicate either directly or via Data Center. The forwarding decision is done on the base of tunnel's state.

   a) Configure the interfaces on every device according to the table below, which reflects the topology image.

Device	Interface	IP address	VLAN-ID	Zone
srx1	st0.0	11.0.0.2/30	None	Untrust
srx1	st0.1	11.0.0.10/30	None	Untrust

© 2020 Juniper Networks, Inc. All rights reserved.

srx2	st0.0	11.0.0.6/30	None	Untrust
srx2	st0.1	11.0.0.9/30	None	Untrust

Cluster2 (srx5, srx6)	st0.0	11.0.0.1/30	None	Untrust
Cluster2 (srx5, srx6)	st0.1	11.0.0.5/30	None	Untrust

The configuration that you need to create at this step is similar to task 1 of chapter 3 “Firewall – Security Policies”.

Below is the configuration excerpt for tunnel interfaces of srx1.

```
[edit interfaces]
lab@srx1# show
...
st0 {
    unit 0 {
        family inet {
            address 11.0.0.2/30;
        }
    }
    unit 1 {
        family inet {
            address 11.0.0.10/30;
        }
    }
}
```

b) At this step you also need to add st0 interfaces to the UNTRUST zone and verify that OSPF is the protocol permitted by host-inbound-traffic.

```
[edit security zones security-zone UNTRUST]
lab@srx1# show
host-inbound-traffic {
    protocols {
        ospf;
    }
}
interfaces {
    ge-0/0/3.0;
    lo0.0;
    st0.0;
    st0.1;
}
```

c) Configure static routes using the st interfaces as the next hop.

```
[edit routing-options]
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
lab@srx1# show
static {
    route 0.0.0.0/0 next-hop 80.10.8.254;
    route 192.168.1.5/32 next-hop st0.0;
    route 192.168.1.2/32 next-hop st0.1;
}
```

d) Configure the IPsec VPN on every device according to the table below, which reflects the topology image.

Local Peer	Interface	Remote Peer	Interface
cluster2	reth0.0	srx2	ge-0/0/3.0
srx1	ge-0/0/3.0	srx2	ge-0/0/3.0

Branch Office 1 (SRX1)

```
[edit]
lab@srx1# show interfaces st0
unit 0 {
    family inet {
        address 11.0.0.2/30;
    }
}
unit 1 {
    family inet {
        address 11.0.0.10/30;
    }
}

[edit]
lab@srx1# show security ike
traceoptions {
    flag all;
}
proposal ike-proposal {
    authentication-method pre-shared-keys;
    dh-group group2;
    authentication-algorithm sha1;
    encryption-algorithm aes-128-cbc;
}
proposal ike-proposal-1 {
    authentication-method pre-shared-keys;
    dh-group group2;
    authentication-algorithm md5;
    encryption-algorithm 3des-cbc;
}
policy ike-policy {
    mode main;
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
    proposals ike-proposal;
    pre-shared-key ascii-text "$9$Q-UPF6ArlM7NbvWkP5Q9CKM87VY"; ## SECRET-DATA
}
policy ike-policy-1 {
    mode main;
    proposal-set basic;
    pre-shared-key ascii-text "$9$cVySvLdVYoZjs2"; ## SECRET-DATA
}
gateway ike-gateway {
    ike-policy ike-policy;
    address 80.10.1.1;
    external-interface ge-0/0/3.0;
}
gateway ike-gateway-1 {
    ike-policy ike-policy-1;
    address 80.10.10.1;
    external-interface ge-0/0/3.0;
}

[edit]
lab@srx1# show security ipsec
traceoptions {
    flag all;
}
vpn-monitor-options {
    interval 5;
    threshold 3;
}
proposal ipsec-proposal {
    protocol esp;
    authentication-algorithm hmac-sha1-96;
    encryption-algorithm aes-256-cbc;
    lifetime-seconds 28800;
}
proposal ipsec-proposal-1 {
    protocol esp;
    authentication-algorithm hmac-sha1-96;
    encryption-algorithm aes-256-cbc;
    lifetime-kilobytes 100000;
}
policy ipsec-policy {
    proposals ipsec-proposal;
}
policy ipsec-policy-1 {
    proposals ipsec-proposal-1;
}
vpn to-cluster2 {
    bind-interface st0.0;
    vpn-monitor {
        optimized;
        source-interface lo0.0;
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
        destination-ip 192.168.1.5;
    }
    ike {
        gateway ike-gateway;
        ipsec-policy ipsec-policy;
    }
    establish-tunnels immediately;
}
vpn to-srx2 {
    bind-interface st0.1;
    vpn-monitor {
        optimized;
        source-interface lo0.0;
        destination-ip 192.168.1.2;
    }
    ike {
        gateway ike-gateway-1;
        ipsec-policy ipsec-policy-1;
    }
    establish-tunnels immediately;
}
```

Branch Office 2 (SRX2)

```
[edit]
lab@srx2# show interfaces st0
unit 0 {
    family inet {
        address 11.0.0.6/30;
    }
}
unit 1 {
    family inet {
        address 11.0.0.9/30;
    }
}

[edit]
lab@srx2# show security ike
traceoptions {
    flag all;
}
proposal ike-proposal {
    authentication-method pre-shared-keys;
    dh-group group2;
    authentication-algorithm sha1;
    encryption-algorithm aes-128-cbc;
}
proposal ike-proposal-1 {
    authentication-method pre-shared-keys;
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
    dh-group group2;
    authentication-algorithm md5;
    encryption-algorithm 3des-cbc;
}
policy ike-policy {
    mode main;
    proposals ike-proposal;
    pre-shared-key ascii-text "$9$Q-UPF6ArlM7NbvWkP5Q9CKM87VY"; ## SECRET-DATA
}
policy ike-policy-1 {
    mode main;
    proposal-set basic;
    pre-shared-key ascii-text "$9$TQ/t1IclvLhS"; ## SECRET-DATA
}
gateway ike-gateway {
    ike-policy ike-policy;
    address 80.10.1.1;
    external-interface ge-0/0/3.0;
}
gateway ike-gateway-1 {
    ike-policy ike-policy-1;
    address 80.10.8.1;
    external-interface ge-0/0/3.0;
}

[edit]
lab@srx2# show security ipsec
vpn-monitor-options {
    interval 5;
    threshold 3;
}
proposal ipsec-proposal {
    protocol esp;
    authentication-algorithm hmac-sha1-96;
    encryption-algorithm aes-256-cbc;
    lifetime-seconds 28800;
}
proposal ipsec-proposal-1 {
    protocol esp;
    authentication-algorithm hmac-sha1-96;
    encryption-algorithm aes-256-cbc;
    lifetime-kilobytes 100000;
}
policy ipsec-policy {
    proposals ipsec-proposal;
}
policy ipsec-policy-1 {
    proposals ipsec-proposal-1;
}
vpn to-cluster2 {
    bind-interface st0.0;
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
    vpn-monitor {
        optimized;
        source-interface lo0.0;
        destination-ip 192.168.1.5;
    }
    ike {
        gateway ike-gateway;
        ipsec-policy ipsec-policy;
    }
    establish-tunnels immediately;
}
vpn to-srx-1 {
    bind-interface st0.1;
    vpn-monitor {
        optimized;
        source-interface lo0.0;
        destination-ip 192.168.1.1;
    }
    ike {
        gateway ike-gateway-1;
        ipsec-policy ipsec-policy-1;
    }
    establish-tunnels immediately;
}
```

Central Office (SRX5/6)

```
{primary:node0}[edit]
lab@srx5# show interfaces st0
unit 0 {
    family inet {
        address 11.0.0.1/30;
    }
}
unit 1 {
    family inet {
        address 11.0.0.5/30;
    }
}

{primary:node0}[edit]
lab@srx5# show security ike
proposal ike-proposal {
    authentication-method pre-shared-keys;
    dh-group group2;
    authentication-algorithm sha1;
    encryption-algorithm aes-128-cbc;
}
policy ike-policy {
    mode main;
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
        proposals ike-proposal;
        pre-shared-key ascii-text "$9$Q-UPF6ArlM7NbvWkP5Q9CKM87VY"; ## SECRET-DATA
    }
    gateway ike-gateway-1 {
        ike-policy ike-policy;
        address 80.10.8.1;
        external-interface reth0.0;
    }
    gateway ike-gateway-2 {
        ike-policy ike-policy;
        address 80.10.10.1;
        external-interface reth0.0;
    }

    {primary:node0}[edit]
    lab@srx5# show security ipsec
    traceoptions {
        flag all;
    }
    vpn-monitor-options {
        interval 5;
        threshold 3;
    }
    proposal ipsec-proposal {
        protocol esp;
        authentication-algorithm hmac-sha1-96;
        encryption-algorithm aes-256-cbc;
        lifetime-seconds 28800;
    }
    policy ipsec-policy {
        proposals ipsec-proposal;
    }
    vpn to-srx2 {
        bind-interface st0.1;
        vpn-monitor {
            optimized;
            source-interface lo0.0;
            destination-ip 192.168.1.2;
        }
        ike {
            gateway ike-gateway-2;
            ipsec-policy ipsec-policy;
        }
        establish-tunnels immediately;
    }
    vpn to-srx1 {
        bind-interface st0.0;
        vpn-monitor {
            optimized;
            source-interface lo0.0;
            destination-ip 192.168.1.1;
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
    }
    ike {
        gateway ike-gateway-1;
        ipsec-policy ipsec-policy;
    }
}
```

2) In this task's topology you will use OSPF as a dynamic routing protocol. The subnets located in TRUST, PRIVATE, INTERNAL or DMZ zones must appear as OSPF internal routes on all devices in OSPF area 0, but no IGP adjacencies may be formed across interfaces located within these security zones.

Ensure that traffic originated from any TRUST zone can reach any other TRUST zone.

To accomplish this requirement, you should create two security policies that describe traffic between TRUST zones of the Branch office 1, Branch office 2 and the Central office. Since this configuration is added to the existing one, you should make sure that the old policies in the same zone context do not shade new policies. Use command "`insert`" to move the new policy above the old one if it is necessary.

© 2020 Juniper Networks, Inc. All rights reserved.

Configure the interfaces on every device according to the table below, which reflects the topology image.

Device	Interface	OSPF Area
srx1	st0.0	OSPF Area 0
srx1	st0.1	OSPF Area 0
srx1	ge-0/0/1.0	OSPF Area 0
srx1	ge-0/0/2.0	OSPF Area 0
srx2	st0.0	OSPF Area 0
srx2	st0.1	OSPF Area 0
srx2	ge-0/0/2.0	OSPF Area 0
srx2	ge-0/0/4.0	OSPF Area 0
Cluster2 (srx5, srx6)	st0.0	OSPF Area 0
Cluster2 (srx5, srx6)	st0.1	OSPF Area 0
Cluster2 (srx5, srx6)	reth1.50	OSPF Area 0
Cluster2 (srx5, srx6)	reth1.55	OSPF Area 0
Cluster2 (srx5, srx6)	reth1.60	OSPF Area 0

To accomplish the whole task, you need to create OSPF area 0.0.0.0 and place all appropriate interfaces in this area. The interfaces that are associated with TRUST, PRIVATE, INTERNAL or DMZ zones should be configured as passive. Below is the configuration excerpt for OSPF protocol configuration.

```
[edit protocols ospf area 0.0.0.0]
lab@srx1#show
interface st0.0;
interface st0.1;
interface ge-0/0/1.0 {
    passive;
}
interface ge-0/0/2.0 {
    passive;
}
```

3) VPN between srx1 and Cluster2 and between srx2 and Cluster2 must meet following requirements:
    a. Rekey IPsec tunnel every 8 hours.

© 2020 Juniper Networks, Inc. All rights reserved.

b. Validate data path with VPN monitor option. The keepalives should be sent to the neighboring peer regardless of traffic patterns with 5 sec intervals. It is allowed to miss only three consecutive keepalives after which the tunnel is considered inactive.
c. IKE phase 1 proposal must include: preshared key “jncie”, AES128, DH G2, SHA.
d. IKE phase 2 proposal must include: AES256, ESP, SHA.
e. Ensure that in case of one tunnel’s failure traffic originated from the TRUST security zone of any site still can reach other site’s protected recourses.

4) VPN between srx1 and srx2 must meet following requirements:
   a. Rekey IPsec tunnel on transmitting 100 MB of traffic.
   b. Validate data path with VPN monitor option. The keepalives should be sent to the neighboring peer only in absence of traffic patterns.
   c. IKE phase 1 proposal must include: preshared key “jncie”, 3DES, DH G2, MD5.
   d. IKE phase 2 proposal must include: AES256, ESP, SHA.
   e. Ensure that in case of one tunnel’s failure traffic originated from the TRUST security zone of any site still can reach other site’s protected recourses.

The main differences between IKE / IPsec configurations for Task 1 and Task 2 are:

1) The way traffic is forwarded into the IPsec tunnel. Task 2 assumes that security devices use routing tables’ information instead of security policies.
   This is accomplished by enabling dynamic routing protocol on srx1, srx2 and cluster2. The OSPF learns prefixes reachability and maintain routing information into the inet.0 routing table.
   The one more mandatory configuration step that you need to do is the binding of tunnel interfaces to the IPsec VPN. Below is the command you can use for this task.

```
[edit]
lab@srx1# set security ipsec vpn to-cluster2 bind-interface st0.0
```

2) The replacement of DPD feature with the VPN monitor.
   This task requires you to monitor IPsec tunnel state with the VPN monitor feature that is available at the `[edit security ipsec]` level of configuration hierarchy.
   The “`optimized`” keyword allows using traffic patterns as an evidence of peer’s aliveness.

```
[edit security ipsec]
lab@srx1# show vpn to-cluster2
vpn-monitor {
    optimized;
    source-interface lo0.0;
    destination-ip 192.168.1.5;
}
```


© 2020 Juniper Networks, Inc. All rights reserved.

...

The interval and threshold for VPN monitor keepalives can be configured at `[edit security ipsec vpn-monitor-options]` the level of configuration hierarchy.

```
[edit security ipsec vpn-monitor-options]
lab@srx1# show
interval 5;
threshold 3;
```

Task 3: Configuring GRE-Tunnel Over Route-Based VPN

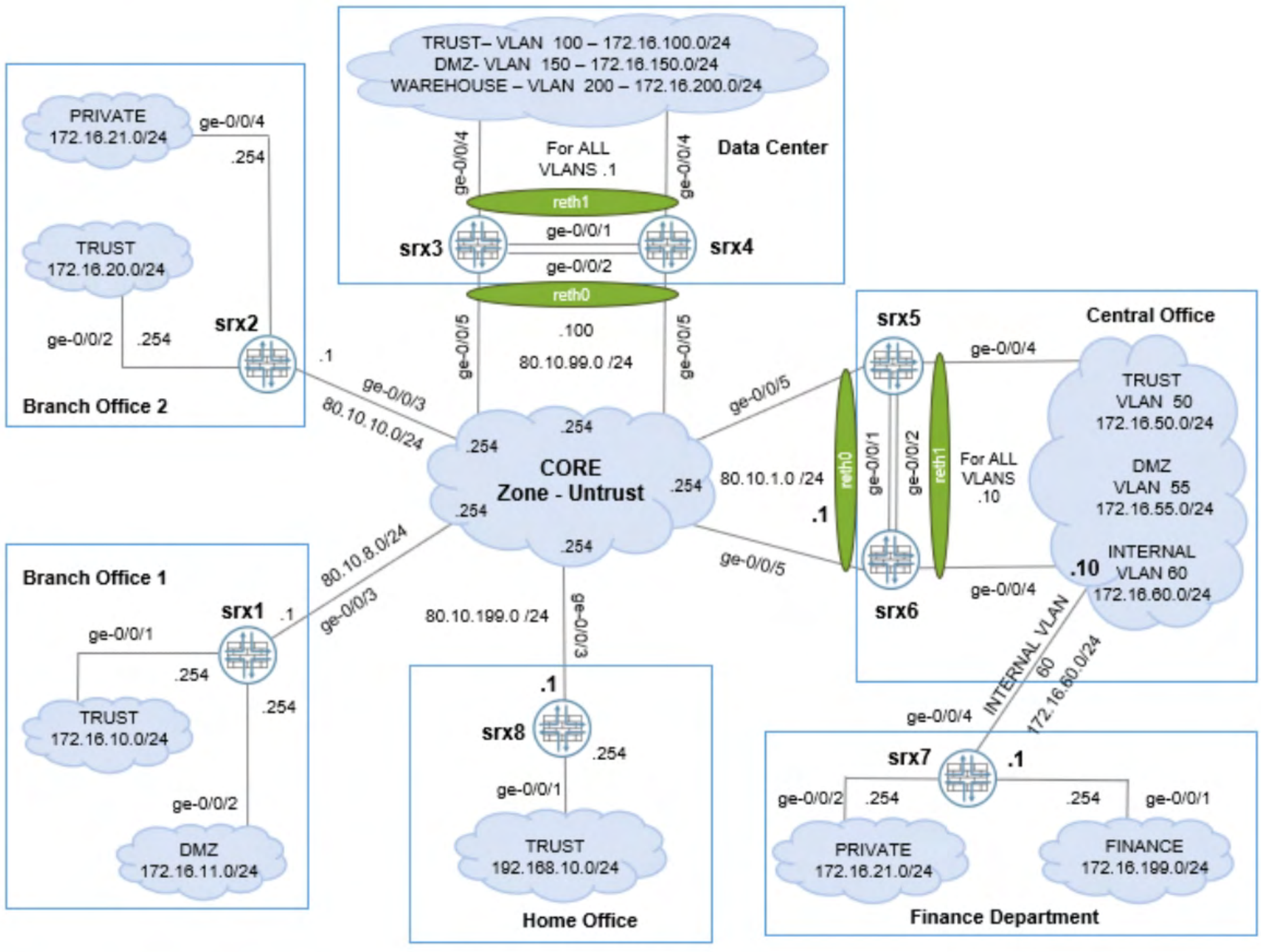


Figure 4: Chapter 5 – Task 3 Topology

In this part you will configure lab equipment as necessary to build GRE-tunnel over Route-based VPN between Branch Office 1 and Branch Office 2.

© 2020 Juniper Networks, Inc. All rights reserved.

1) Configure the interfaces on every device according to the table below.
The GRE tunnel source should be configured as device's local lo0 interface address and the destination should be configured as remote device's lo0 interface address.

Device	Interface	IP address	VLAN-ID	Zone
srx1	gr-0/0/0.0	11.11.11.1/30	None	Untrust
srx1	lo0.0	192.168.1.1/32	None	Untrust
srx2	gr-0/0/0.0	11.11.11.2/30	None	Untrust
srx2	lo0.0	192.168.1.2/32	None	Untrust

Tip: Ensure that GRE tunnel's termination points are reachable via the IPsec tunnel

The configuration that you need to create at this step is similar to task 1 of chapter 3 "Firewall – Security Policies". Below is the configuration excerpt for GRE interfaces of srx1.

Branch Office 1 (SRX1)

```
[edit]
lab@srx1# show interfaces gr-0/0/0
unit 0 {
    tunnel {
        source 192.168.1.1;
        destination 192.168.1.2;
    }
    family inet {
        address 11.11.11.1/30;
    }
}
```

Branch Office 2 (SRX2)

```
[edit]
lab@srx2# show interfaces gr-0/0/0
unit 0 {
    tunnel {
        source 192.168.1.2;
        destination 192.168.1.1;
    }
    family inet {
        address 11.11.11.2/30;
    }
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
}
```

2) You need to configure OSPF as a dynamic routing protocol running between Branch Office 1 and Branch Office 2.

Branch Office 1 (SRX1)

```
lab@srx1# show protocols ospf
area 0.0.0.0 {
    interface st0.0;
    interface st0.1;
    interface ge-0/0/2.0 {
        passive;
    }
    interface ge-0/0/1.0 {
        passive;
    }
    interface lo0.0;
    interface gr-0/0/0.0;
}
```

Branch Office 2 (SRX2)

```
lab@srx2# show protocols ospf
area 0.0.0.0 {
    interface lo0.0;
    interface st0.0;
    interface ge-0/0/2.0 {
        passive;
    }
    interface ge-0/0/4.0 {
        passive;
    }
    interface st0.1;
    interface gr-0/0/0.0;
}
```

Configure the interfaces on every device according to the table below, which reflects the topology image.

Device	Interface	OSPF Area
srx1	gr-0/0/0.0	OSPF Area 0
srx2	gr-0/0/0.0	OSPF Area 0

© 2020 Juniper Networks, Inc. All rights reserved.

3) Ensure that any traffic originated from TRUST zone of Branch Office 1 can reach TRUST zone of the Branch Office 2 and vice versa.

Branch Office 1 (SRX1)

```
[edit]
lab@srx1# show security zones security-zone TRUST address-book
address trust-address-range 172.16.10.0/24;

[edit]
lab@srx1# show security zones security-zone UNTRUST
address-book {
    address corp-network 172.16.0.0/16;
    address core-loopbacks 192.168.1.0/24;
    address gre-int 11.11.11.0/30;
    address TRUST-BO2 172.16.20.0/24;
}


[edit]
lab@srx1# show security policies
from-zone TRUST to-zone UNTRUST {
    policy internet-access {
        match {
            source-address trust-address-range;
            destination-address any;
            application trust-app-set;
        }
        then {
            permit {
                application-services {
                    utm-policy Branch-web-filter;
                }
            }
        }
    }
}
from-zone UNTRUST to-zone UNTRUST {
    policy UNTRUST-intra {
        match {
            source-address [ core-loopbacks gre-int ];
            destination-address [ core-loopbacks gre-int ];
            application [ junos-gre junos-icmp-all ];
        }
        then {
            permit;
        }
    }
}
from-zone UNTRUST to-zone TRUST {
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
    policy TRUST-BO2-to-TRUST-BO1 {
        match {
            source-address TRUST-BO2;
            destination-address trust-address-range;
            application any;
        }
        then {
            permit;
        }
    }
}
```

Branch Office 2 (SRX2)

```
[edit]
lab@srx2# show security zones security-zone TRUST address-book
address trust-address-range 172.16.20.0/24;

[edit]
lab@srx2# show security zones security-zone UNTRUST address-book
address corp-network 172.16.0.0/16;
address dmz-DC 172.16.150.0/24;
address dmz-CO 172.16.55.0/24;
address core-loopbacks 192.168.1.0/24;
address gre-int 11.11.11.0/30;
address TRUST-BO1 172.16.10.0/24;
address-set dmz-zones {
    address dmz-CO;
    address dmz-DC;
}

[edit]
lab@srx2# show security policies
from-zone TRUST to-zone UNTRUST {
    policy corp-network-access {
        match {
            source-address trust-address-range;
            destination-address corp-network;
            application any;
        }
        then {
            permit;
        }
    }

}
from-zone UNTRUST to-zone UNTRUST {
    policy UNTRUST-intra {
        match {
            source-address [ core-loopbacks gre-int ];
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
            destination-address [ core-loopbacks gre-int ];
            application [ junos-icmp-all junos-gre ];
        }
        then {
            permit;
        }
    }
}
from-zone UNTRUST to-zone TRUST {
    policy TRUST-BO1-to-TRUST-BO2 {
        match {
            source-address TRUST-BO1;
            destination-address trust-address-range;
            application any;
        }
        then {
            permit;
        }
    }
}
```


© 2020 Juniper Networks, Inc. All rights reserved.

Task 4: Configuring ADVPN

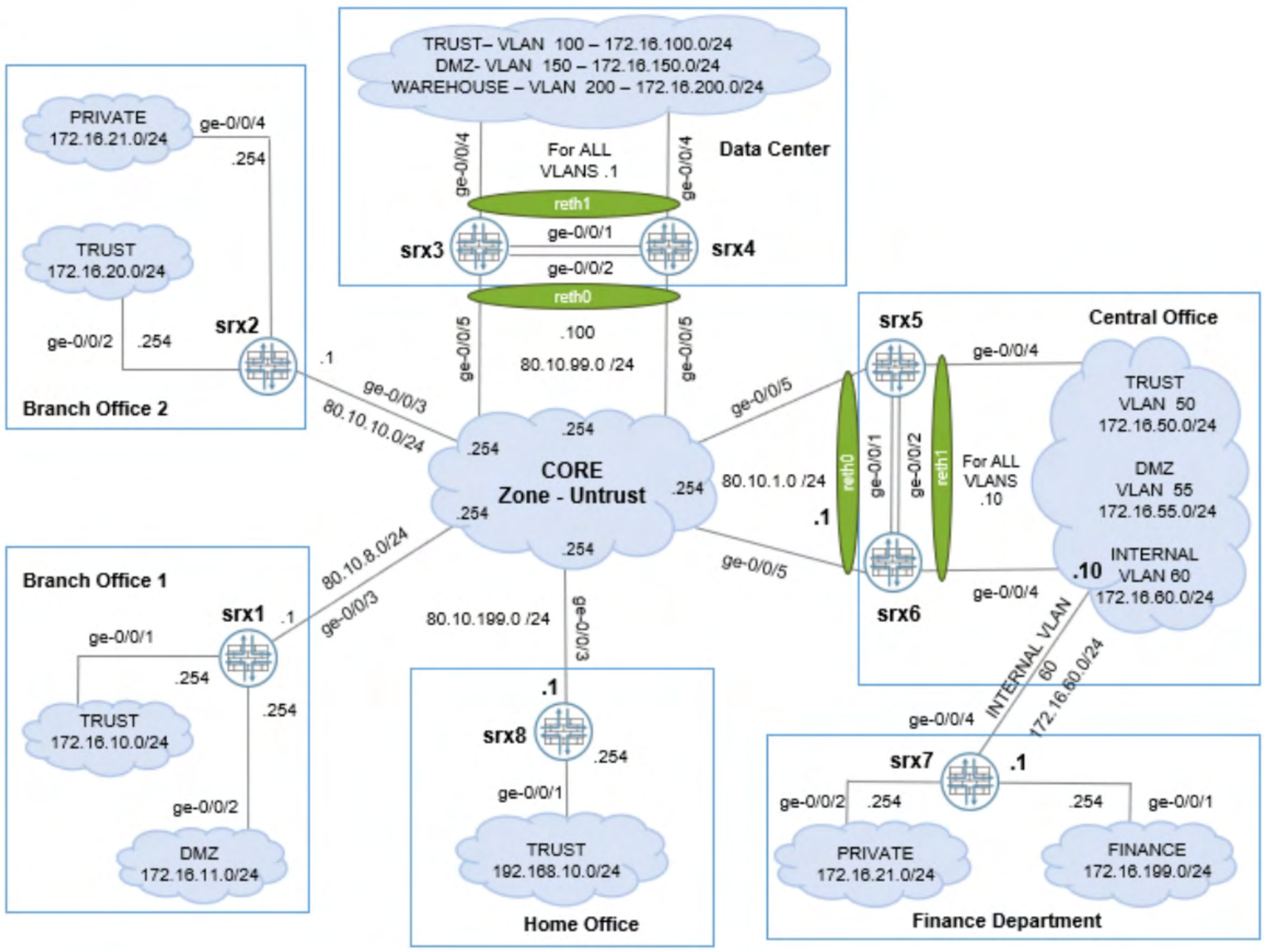


Figure 5: Chapter 5 – Task 4 Topology

Auto Discovery VPN (ADVPN) is a technology that allows the central HUB to dynamically inform spokes about a better path for traffic between two spokes. When both spokes acknowledge the information from the HUB, they establish a shortcut tunnel and change the routing topology for the host to reach the other side without sending traffic through the HUB.

ADVPN use an extension of IKEv2 protocol to exchange messages between two peers, which allows the spokes to establish a shortcut tunnel between each other. Devices that support the ADVPN extension send an ADVPN_SUPPORTED notification in the IKEv2 Notify payload including its capability information and the ADVPN version number during the initial IKE exchange. A device that supports ADVPN can act as either a shortcut suggester or a shortcut partner, but not both.

Establishing a Shortcut

© 2020 Juniper Networks, Inc. All rights reserved.

An IPsec VPN gateway can act as a shortcut suggester when it notices that traffic is exiting a tunnel with one of its peers and entering a tunnel with another peer. Figure 1 shows traffic from Spoke 1 to Spoke 3 passing through the hub.

Figure 1: Spoke-to-Spoke Traffic Passing Through Hub

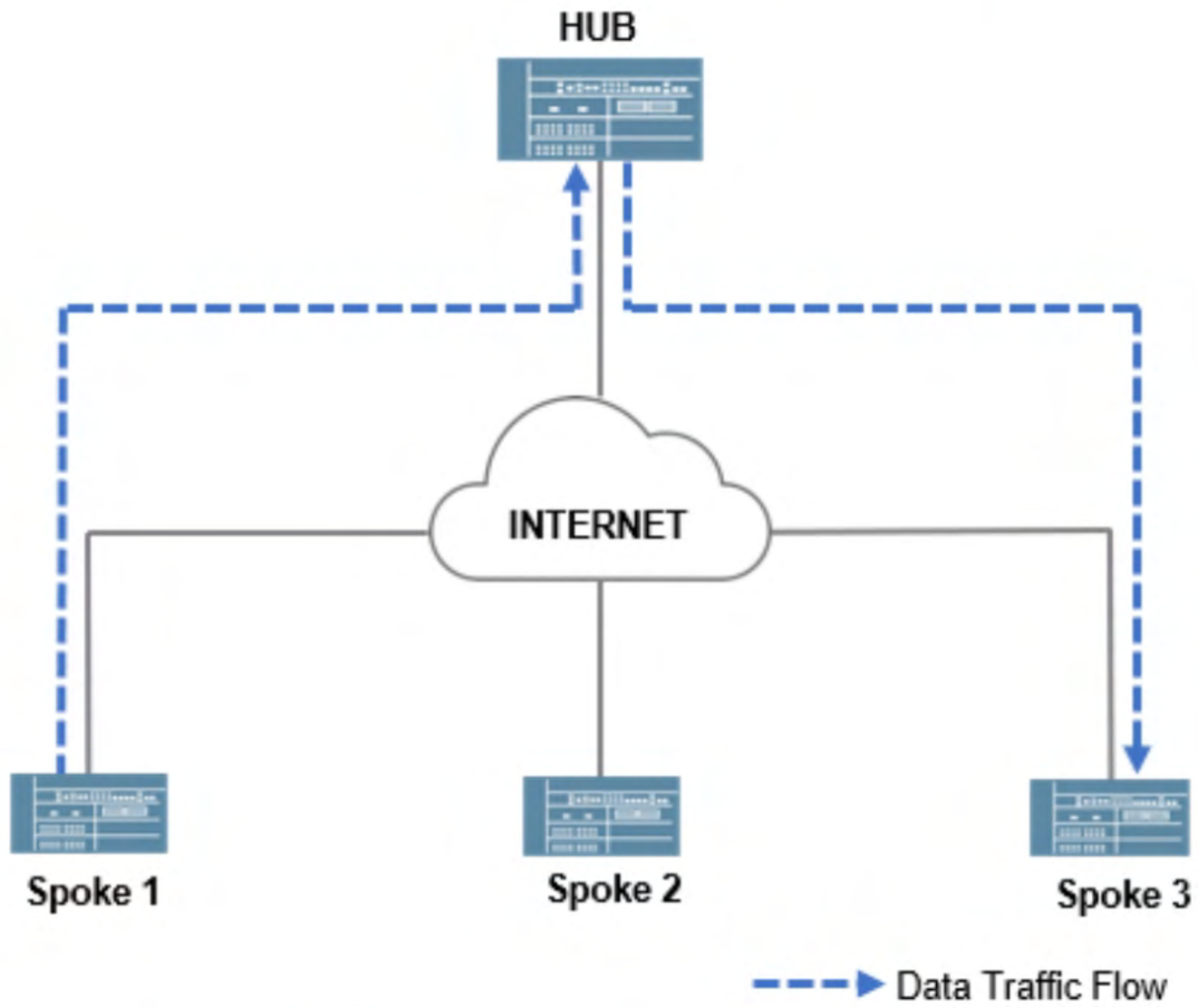


Figure 6: Spoke-to-Spoke Traffic Passing Through Hub

When ADVPN is configured on the devices, ADVPN shortcut capability information is exchanged between the hub and the spokes. As long as Spokes 1 and 3 have previously advertised ADVPN shortcut partner capability to the hub, the hub can suggest that Spokes 1 and 3 establish a shortcut between each other.

The shortcut suggester uses its already established IKEv2 SAs with the peers to begin a shortcut exchange with one of the two peers. If the peer accepts the shortcut exchange, then the shortcut suggester begins a shortcut exchange with the other peer. The shortcut exchange includes information to allow the peers (referred to as shortcut partners) to establish IKE and IPsec SAs with each other. The creation of the shortcut between the shortcut partners starts only after both peers accept the shortcut exchange.

Figure 2 shows traffic passing through a shortcut between Spokes 1 and 3. Traffic from Spoke 1 to Spoke 3 does not need to traverse the hub.

© 2020 Juniper Networks, Inc. All rights reserved.

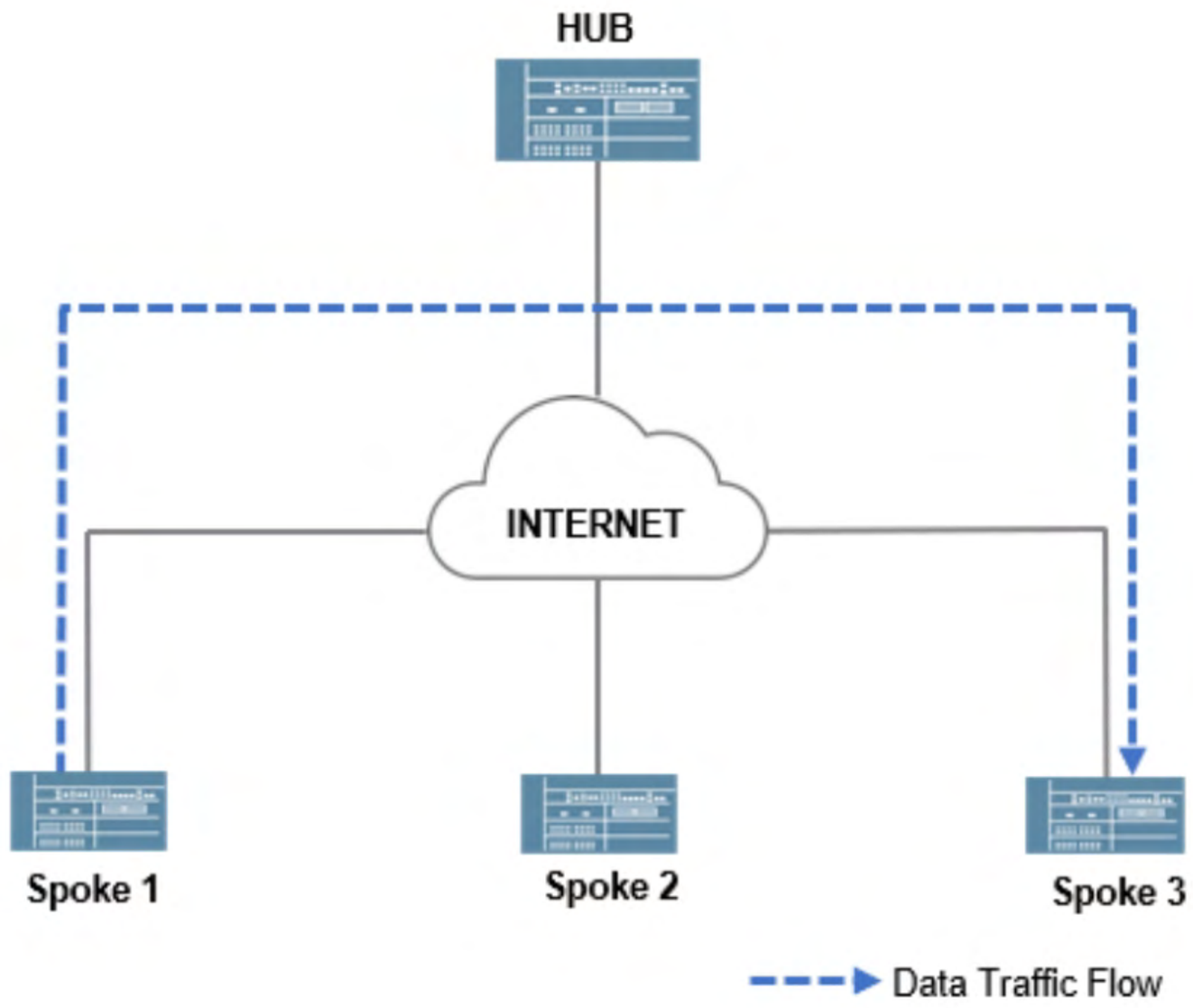


Figure 6: Spoke-to-Spoke Traffic Passing Through Shortcut

Shortcut Initiator and Responder Roles

The shortcut suggester chooses one of the shortcut partners to act as the initiator for the shortcut, the other partner acts as the responder. If one of the partners is behind a NAT device, then the partner behind the NAT device is chosen as the initiator. If none of the partners is behind a NAT device, then the suggester randomly chooses one of the partners as the initiator, the other partner acts as the responder. If both partners are behind NAT devices, then a shortcut cannot be created between them; the suggester does not send a shortcut exchange to any of the peers.

The shortcut suggester begins the shortcut exchange with the responder first. If the responder accepts the shortcut suggestion, then the suggester notifies the initiator.

Using information contained in the shortcut suggester's notification, the shortcut initiator establishes an IKEv2 exchange with the responder, and a new IPsec SA is established between the two partners. On each partner, the route to the network behind its partner now points to the shortcut instead of to the tunnel between the partner and the suggester. Traffic originating behind one of the partners that is destined to a network behind the other shortcut partner flows over the shortcut.

© 2020 Juniper Networks, Inc. All rights reserved.

If the partners decline the shortcut suggestion, then the partners notify the suggester with the reason for the rejection. In this case, traffic between the partners continues to flow through the shortcut suggester.

Note: Please make sure to load the Chapter 5 task 4 (`ch5-task4-start.config`) initial configuration for SRX1, SRX2, and cluster SRX5/6.

1) Configure an ADVPN between the Central Office, Branch Office 1 and Branch Office 2. Inter-Branch traffic should not have to traverse the Central Office. The certificates are already loaded on the devices.

First, we need to find out what kind of certificates are used on the devices

```
lab@srx5# run show security pki local-certificate
node0:
--------------------------------------------------------------------------

Certificate identifier: srx5
  Issued to: srx5.juniper.net, Issued by: C = US, ST = California, L = Sunnyvale, O = Juniper,
CN = student, emailAddress = student@juniper.net
  Validity:
    Not before: 01- 9-2019 20:17 UTC
    Not after: 01- 6-2029 20:17 UTC
  Public key algorithm: rsaEncryption(1024 bits)


lab@srx1# run show security pki local-certificate
Certificate identifier: srx1
  Issued to: srx1.juniper.net, Issued by: C = US, ST = California, L = Sunnyvale, O = Juniper,
CN = student, emailAddress = student@juniper.net
  Validity:
    Not before: 01- 9-2019 18:16 UTC
    Not after: 01- 6-2029 18:16 UTC
  Public key algorithm: rsaEncryption(1024 bits)

lab@srx2# run show security pki local-certificate
Certificate identifier: srx2
  Issued to: srx2.juniper.net, Issued by: C = US, ST = California, L = Sunnyvale, O = Juniper,
CN = student, emailAddress = student@juniper.net
  Validity:
    Not before: 01- 9-2019 18:17 UTC
    Not after: 01- 6-2029 18:17 UTC
  Public key algorithm: rsaEncryption(1024 bits)
```

It seems that RSA certificates are installed on the vSRX devices . Now we can create the appropriate ADVPN configurations and reference the RSA certificates.

© 2020 Juniper Networks, Inc. All rights reserved.

On Central Office (Suggester) disable partner mode.

```
{primary:node0}[edit security]
lab@srx5# show
pki {
    ca-profile advpn {
        ca-identity advpn;
        revocation-check {
            disable;
        }
    }
}
ike {
    traceoptions {
        file ike-advpn.log;
        flag all;
    }
    proposal advpn-ike-prop {
        authentication-method rsa-signatures;
    }
    policy advpn-pol1 {
        mode main;
        proposals advpn-ike-prop;
        certificate {
            local-certificate srx5;
        }
    }
    gateway advpn-gw1 {
        ike-policy advpn-pol1;
        dynamic {
            distinguished-name {
                wildcard O=Juniper;
            }
            ike-user-type group-ike-id;
        }
        local-identity distinguished-name;
        external-interface reth0.0;
        local-address 80.10.1.1;
        advpn {
            partner {
                disable;
            }
        }
        version v2-only;
    }
}
ipsec {
    proposal ipsecprop {
        protocol esp;
        authentication-algorithm hmac-sha-256-128;
        encryption-algorithm aes-256-cbc;
        lifetime-seconds 3600;
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
    }
    policy ipsecpol {
        proposals ipsecprop;
    }
    vpn advpn-vpn {
        bind-interface st0.0;
        ike {
            gateway advpn-gw1;
            ipsec-policy ipsecpol;
        }
    }
}
```

On the Branch Offices (Partner) disable suggester mode.

```
[edit security]
lab@srx1# show
pki {
    ca-profile advpn {
        ca-identity advpn;
        revocation-check {
            disable;
        }
    }
}
ike {
    proposal advpn-ike-prop {
        authentication-method rsa-signatures;
    }
    policy advpn-pol1 {
        proposals advpn-ike-prop;
        certificate {
            local-certificate srx1;
        }
    }
    gateway advpn-gw1 {
        ike-policy advpn-pol1;
        address 80.10.1.1;
        local-identity distinguished-name;
        remote-identity distinguished-name container O=Juniper;
        external-interface ge-0/0/3.0;
        local-address 80.10.8.1;
        advpn {
            suggester {
                disable;
            }
        }
        version v2-only;
    }
}
ipsec {
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
proposal ipsecprop {
    protocol esp;
    authentication-algorithm hmac-sha-256-128;
    encryption-algorithm aes-256-cbc;
    lifetime-seconds 3600;
}
policy ipsecpol {
    proposals ipsecprop;
}
vpn advpn-vpn {
    bind-interface st0.0;
    ike {
        gateway advpn-gw1;
        ipsec-policy ipsecpol;
    }
    establish-tunnels immediately;
}
```

```
[edit security]
lab@srx2# show
pki {
    ca-profile advpn {
        ca-identity advpn;
        revocation-check {
            disable;
        }
    }
}
ike {
    traceoptions {
        file ike-advpn.log;
        flag all;
    }
proposal advpn-ike-prop {
    authentication-method rsa-signatures;
}
policy advpn-pol1 {
    proposals advpn-ike-prop;
    certificate {
        local-certificate srx2;
    }
}
gateway advpn-gw1 {
    ike-policy advpn-pol1;
    address 80.10.1.1;
    local-identity distinguished-name;
    remote-identity distinguished-name container O=Juniper;
    external-interface ge-0/0/3.0;
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
        local-address 80.10.10.1;
        advpn {
            suggester {
                disable;
            }
        }
        version v2-only;
    }
}
ipsec {
    proposal ipsecprop {
        protocol esp;
        authentication-algorithm hmac-sha-256-128;
        encryption-algorithm aes-256-cbc;
        lifetime-seconds 3600;
    }
    policy ipsecpol {
        proposals ipsecprop;
    }
    vpn advpn-vpn {
        bind-interface st0.0;
        ike {
            gateway advpn-gw1;
            ipsec-policy ipsecpol;
        }
        establish-tunnels immediately;
    }
}
```

```
[edit]
lab@srx1, srx2 and srx5# show security-zone VPN
interfaces {
    st0.0 {
        host-inbound-traffic {
            system-services {
                ping;
            }
            protocols {
                ospf;
            }
        }
    }
}
```

Issue the following command on srx1, srx2, and srx5:

```
[edit]
lab@srx1# show security zones security-zone UNTRUST
host-inbound-traffic {
    system-services {
        ping;
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
        ike;
    }
}
```

Next step is to create the st tunnel interface and enable OSPF for dynamic routing

```
[edit]
lab@srx5# show interfaces st0
unit 0 {
    multipoint;
    family inet {
        address 192.168.250.254/24;
    }
}

[edit]
lab@srx5# show protocols ospf
area 0.0.0.0 {
    interface st0.0 {
        interface-type p2mp;
        retransmit-interval 1;
        dead-interval 40;
        demand-circuit;
        dynamic-neighbors;
    }
}

lab@srx2# show interfaces st0
unit 0 {
    multipoint;
    family inet {
        address 192.168.250.2/24;
    }
}

[edit]
lab@srx2# show protocols ospf
area 0.0.0.0 {
    interface st0.0 {
        interface-type p2mp;
        retransmit-interval 1;
        dead-interval 40;
        demand-circuit;
        dynamic-neighbors;
    }
}

lab@srx1# show interfaces st0
unit 0 {
    multipoint;
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
    family inet {
        address 192.168.250.1/24;
    }
}


[edit]
lab@srx1# show protocols ospf
area 0.0.0.0 {
    interface st0.0 {
        interface-type p2mp;
        retransmit-interval 1;
        dead-interval 40;
        demand-circuit;
        dynamic-neighbors;
    }
}
```

2) Only allow ping between the TRUST zones of each site.

Advertise the TRUST subnets in OSPF

```
[edit]
lab@srx5# show policy-options
policy-statement 2ospf {
    term 1 {
        from {
            route-filter 172.16.50.0/24 exact;
        }
        then accept;
    }
}

[edit]
lab@srx5# show protocols ospf
export 2ospf;
}


[edit]
lab@srx1# show policy-options
policy-statement 2ospf {
    term 1 {
        from {
            route-filter 172.16.10.0/24 exact;
        }
        then accept;
    }
}
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
[edit]
lab@srx1# show protocols ospf
export 2ospf;
}

[edit]
lab@srx2# show policy-options
policy-statement 2ospf {
    term 1 {
        from {
            route-filter 172.16.20.0/24 exact;
        }
        then accept;
    }
}

[edit]
lab@srx1# show protocols ospf
export 2ospf;
}
```

Make sure to allow junos-ping between the TRUST zones of each ADVPN site.

```
{primary:node0}[edit security]
lab@srx5# show policies
from-zone VPN to-zone VPN {
    policy ADVPN {
        match {
            source-address any;
            destination-address any;
            application junos-ping;
        }
        then {
            permit;
        }
    }
}
from-zone TRUST to-zone VPN {
    policy ADVPN {
        match {
            source-address any;
            destination-address any;
            application junos-ping;
        }
        then {
            permit;
        }
    }
}
from-zone VPN to-zone TRUST {
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
    policy ADVPN {
        match {
            source-address any;
            destination-address any;
            application junos-ping;
        }
        then {
            permit;
        }
    }
}
```

Create policies to allow traffic between the TRUST and VPN zones on srx1 and srx2.

```
[edit security]
lab@srx1# show policies
from-zone TRUST to-zone VPN {
    policy ADVPN {
        match {
            source-address any;
            destination-address any;
            application junos-ping;
        }
        then {
            permit;
        }
    }
}
from-zone VPN to-zone TRUST {
    policy ADVPN {
        match {
            source-address any;
            destination-address any;
            application junos-ping;
        }
        then {
            permit;
        }
    }
}
```

Verify ADVPN IKE and IPSEC SA's. Please note that you need to generate traffic between the branch networks to establish the shortcut tunnels.

```
{primary:node0}[edit security]
lab@srx5# run show security ike sa
node0:
--------------------------------------------------------------------------
Index   State  Initiator cookie  Responder cookie  Mode           Remote Address
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
3765519 UP     7b3db94e89a3cad6  3aab52127f240357  IKEv2          80.10.8.1
3765520 UP     6ea9424b9d3f11e4  d9638f955b657541  IKEv2          80.10.10.1

{primary:node0}[edit security]
lab@srx5# run show security ipsec sa
node0:
--------------------------------------------------------------------------
  Total active tunnels: 2     Total Ipsec sas: 2
  ID    Algorithm       SPI      Life:sec/kb  Mon lsys Port  Gateway
  <67108865 ESP:aes-cbc-256/sha256 1f60e72b 2553/ unlim - root 500 80.10.8.1
  >67108865 ESP:aes-cbc-256/sha256 ea99b9b7 2553/ unlim - root 500 80.10.8.1
  <67108866 ESP:aes-cbc-256/sha256 472b4dc1 2686/ unlim - root 500 80.10.10.1
  >67108866 ESP:aes-cbc-256/sha256 4f061089 2686/ unlim - root 500 80.10.10.1

{primary:node0}[edit security]
lab@srx5#


lab@srx1# run show security ike sa
Index   State  Initiator cookie  Responder cookie  Mode           Remote Address
6861269 UP     7b3db94e89a3cad6  3aab52127f240357  IKEv2          80.10.1.1
6861270 UP     90889bade4527a70  30cfccd635590555  IKEv2          80.10.10.1

[edit]
lab@srx1# run show security ipsec sa
  Total active tunnels: 2     Total Ipsec sas: 2
  ID    Algorithm       SPI      Life:sec/kb  Mon lsys Port  Gateway
  <67108871 ESP:aes-cbc-256/sha256 ea99b9b7 2479/ unlim - root 500 80.10.1.1
  >67108871 ESP:aes-cbc-256/sha256 1f60e72b 2479/ unlim - root 500 80.10.1.1
  <67108873 ESP:aes-cbc-256/sha256 804396b1 3569/ unlim - root 500 80.10.10.1
  >67108873 ESP:aes-cbc-256/sha256 d5b0cbe8 3569/ unlim - root 500 80.10.10.1

[edit]

lab@srx2# run show security ike sa
Index   State  Initiator cookie  Responder cookie  Mode           Remote Address
2341321 UP     6ea9424b9d3f11e4  d9638f955b657541  IKEv2          80.10.1.1
2341322 UP     90889bade4527a70  30cfccd635590555  IKEv2          80.10.8.1

[edit]
lab@srx2# run show security ipsec sa
  Total active tunnels: 2     Total Ipsec sas: 2
  ID    Algorithm       SPI      Life:sec/kb  Mon lsys Port  Gateway
  <67108871 ESP:aes-cbc-256/sha256 4f061089 2577/ unlim - root 500 80.10.1.1
  >67108871 ESP:aes-cbc-256/sha256 472b4dc1 2577/ unlim - root 500 80.10.1.1
  <67108873 ESP:aes-cbc-256/sha256 d5b0cbe8 3534/ unlim - root 500 80.10.8.1
  >67108873 ESP:aes-cbc-256/sha256 804396b1 3534/ unlim - root 500 80.10.8.1
```

Verify the next-hop for inter branch traffic. Please note that you need to generate traffic between the branch networks to establish the shortcut tunnels.

© 2020 Juniper Networks, Inc. All rights reserved.

```
[edit]
lab@srx2# run show route 172.16.10.0

inet.0: 18 destinations, 18 routes (18 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

172.16.10.0/24     *[OSPF/150] 00:00:53, metric 0, tag 0
                    > to 192.168.250.254 via st0.0

[edit]
lab@srx2# run ping 172.16.10.254
PING 172.16.10.254 (172.16.10.254): 56 data bytes
64 bytes from 172.16.10.254: icmp_seq=0 ttl=63 time=13.965 ms
64 bytes from 172.16.10.254: icmp_seq=1 ttl=63 time=3.967 ms
^C
--- 172.16.10.254 ping statistics ---
2 packets transmitted, 2 packets received, 0% packet loss
round-trip min/avg/max/stddev = 3.967/8.966/13.965/4.999 ms



[edit]
lab@srx2# run show route 172.16.10.0

inet.0: 18 destinations, 18 routes (18 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

172.16.10.0/24     *[OSPF/150] 00:00:07, metric 0, tag 0
                    > to 192.168.250.1 via st0.0
```


© 2020 Juniper Networks, Inc. All rights reserved.

Appendix - Chapter 6: NAT

This appendix provides the solution details for the Network address translation (NAT) chapter. The configuration contains source NAT, destination NAT and static NAT.

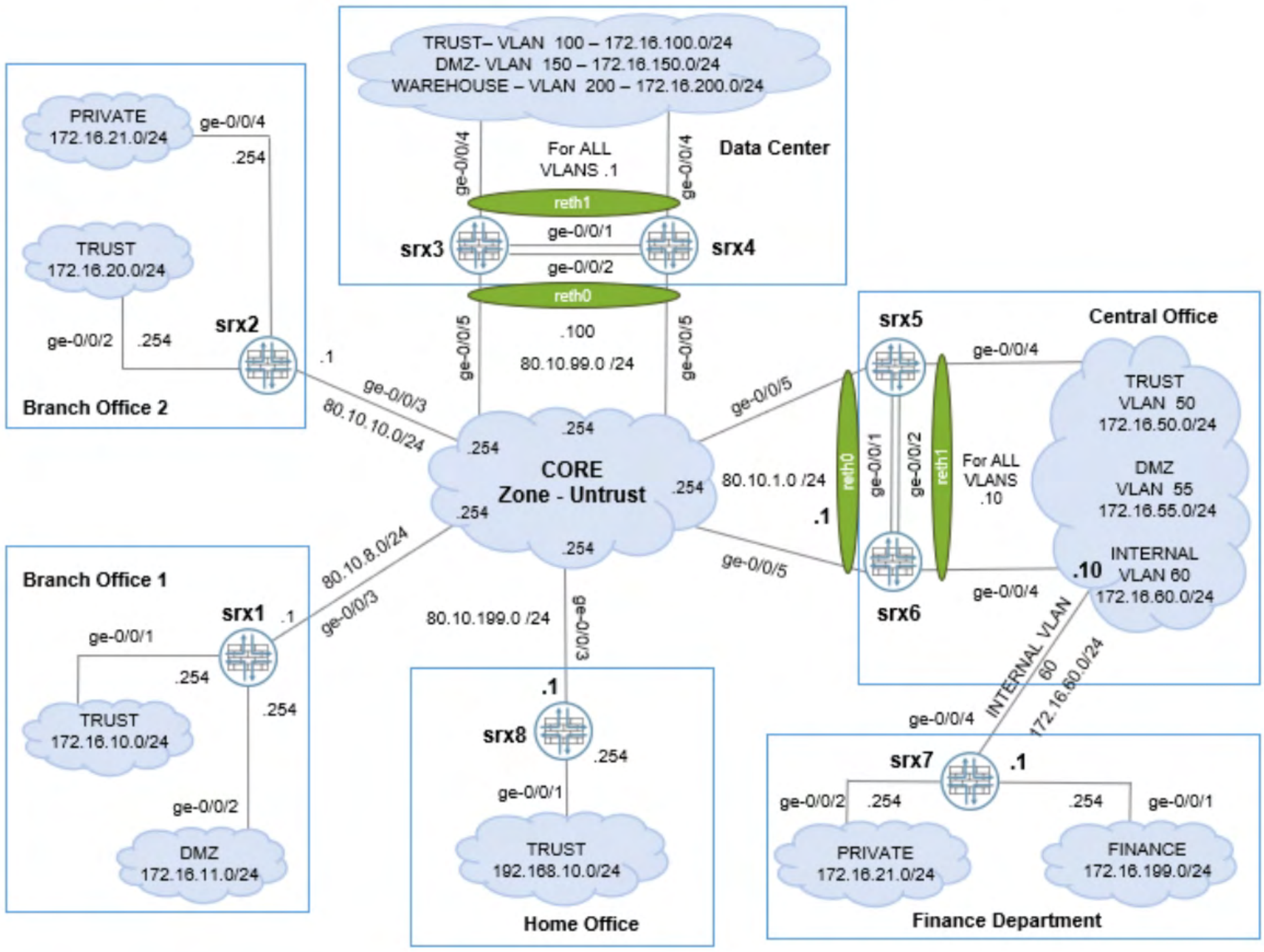


Figure 1: Chapter 6 Topology

Network Address Translation overview

Network address translation in general modifies the IP packet header by changing IP addresses, either source or destination or both, and optionally ports, either source or destination or both. Sometimes the IP address and port are translation is designated as network address and port translation (NAPT) or PAT port address translation. Typically, the NAT performs translation from private IP address range (10/8, 172.16.0/12 or

© 2020 Juniper Networks, Inc. All rights reserved.

192.168/16) to public IP address and vice versa. This helps to conserve and save public IP addresses and helped to postpone the IPv4 address space depletion. However, in general NAT supports translation between any IP addresses.

NAT type designation is done based on which IP addresses are translated in the initial flow. Two high-level NAT types exists

- Source NAT – the source IP address is translated in initial flow. Optionally the source port can be translated. Source NAT is typically used in situations where connectivity for private hosts to the public environment. The security side effect here is the connections initiated from the public environment to the private hosts do not succeed unless specific configuration is done (persistent NAT).
- Destination NAT – the destination IP address is translated in the initial flow. Optionally the destination port can be translated too. Destination NAT is typically done to provide connectivity from the public environment to the private hosts, for example servers.

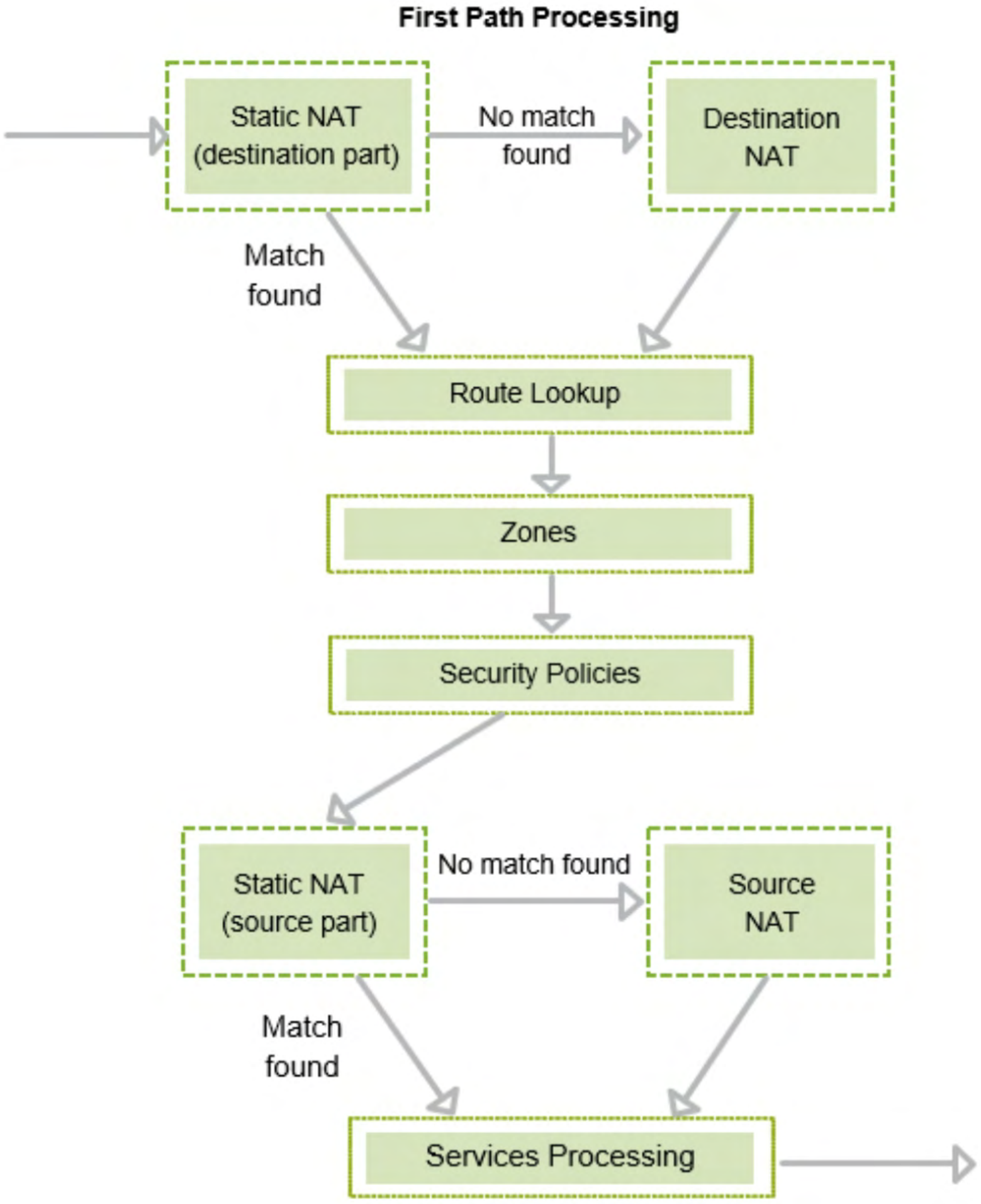
Junos security device supports both of these translations. In addition, it allows configuration of so called “static NAT” which is a combination of source and destination NAT. In static NAT the type of used translation depends on the initiator of the communication. Typically, if the connection is initiated from outside the destination NAT is done and if the connection is initiated from within the internal network the source NAT is performed.

The whole NAT configuration, e.g. source, destination and static NAT, is located under the [edit security nat] hierarchy. Wide area of translation options are available, such as one-to-one, many-to-one or many-to-many mappings, using the IP address of the outgoing interface or an IP address from the defined pool for translation, enabling or disabling the port translation, etc.

Junos uses rule-sets and rules for the NAT configuration, where the rules are subordinate objects to the rule-sets. Criteria defined in rule-sets are evaluated first. Destination and static NAT rule-sets contain only “from” statement and source NAT rules contain “from” and “to” statements. All these statements can reference routing-instance, zone or interface for matching. If traffic matches criteria from multiple rule-sets the rule-set with most specific criteria is selected, where interface is more specific than zone which is more specific than routing-instance. Next the criteria in the rules within the selected rule-set are evaluated. Here the evaluation is done sequentially in the order the rules appear in the configuration. The rule criteria can use IP addresses and ports for matching. The static NAT rules are evaluated before the destination and source NAT rules. Proxy arp needs to be configured if addresses from directly attached networks different than the IP addresses on the interfaces are used for translation. Destination part of the static NAT and the destination NAT are executed before the route lookup and the security policies evaluation in the first path traffic processing sequence. The source part of the static NAT and the source NAT on

© 2020 Juniper Networks, Inc. All rights reserved.

the other hand are performed after the security policies evaluation. This has a very important effect: the routing lookup and the security policies match criteria need to reflect the changed destination address if destination NAT was done. However, the security policies match criteria need to reflect the original source address before, i.e. the source IP address directly from the received packet.



© 2020 Juniper Networks, Inc. All rights reserved.

Things to remember

- ***Static NAT has precedence over source and destination NAT***
- ***NAT is performed independently from the security policies***
- ***Destination NAT is performed before the routing lookup and security policies lookup, i.e. the translated/changed destination IP address is used in routing lookup and for matching the security policies.***
- ***Source NAT is performed after the security policies matching, i.e. the security policies match criteria have to use the original IP address***
- ***Define proxy arp if addresses used for translation are from the same subnet as the interface on the security device. This tells the security device to respond to the ARP requests even if the address is not configured on the interface.***
- ***If the traffic matches multiple rule-sets the one with the most specific condition (interface -> zone -> routing-instance) is selected.***

© 2020 Juniper Networks, Inc. All rights reserved.

Task 1: Source NAT

This section contains the details about the source NAT configuration on devices srx1, srx2 and srx8.

The solutions listed in this chapter rely on the existing security policy configuration present on the devices. If any additional security policy configuration is needed it will be shown in the respective step.

Home office: srx8

1) As instructed by task the connections from hosts in the 192.168.10.0/24 subnet (TRUST zone) have to be translated when connecting to the prefixes in the Core network (80.10.0.0/16).
   As it is not given which IP address to use the easiest and simplest option would be the IP address of the outgoing interface. Another alternative could be source NAT translation using an address pool.
   Here the source NAT rule-set condition will be “from zone TRUST to zone UNTRUST” and the subnet ranges above will be used in the rule match condition.
2) This indicates persistent NAT (formerly cone NAT) is meant. The persistent NAT requires the port translation to be disabled even if the egress interface’s IP address is being used for translation. The type of persistent NAT here is the “target-host” option as the external hosts can contact the internal ones only after they have received any packet from them. In addition, this task tells to set the inactivity-timeout to 1 hour (3600 seconds).

   Note: During the time when the persistent sessions are maintained the connections initiated in the reverse direction (e.g. from the external hosts to the internal host’s reflexive address) are allowed. No explicit security policy configuration is needed as the security policy search is bypassed and the sessions will match the same security policy as the connections from the internal zone to the external one.

```
[edit security nat source]
lab@srx8# show
interface {
    port-overloading off;
}
rule-set src-persistent-NAT {
    from zone TRUST;
    to zone UNTRUST;
    rule persistent-to-trust {
        match {
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
    source-address 192.168.10.0/24;
    destination-address 80.10.0.0/16;
}
then {
    source-nat {
        interface {
            persistent-nat {
                permit target-host;
                inactivity-timeout 3600;
            }
        }
    }
}
```

Branch office 1: srx1

3) The connections from the TRUST zone (subnet 172.16.10.0/24) to the Core networks (zone UNTRUST and subnet 80.10.0.0/16) have to be translated.

   The connections from the DMZ zone (subnet 172.16.11.0/24) to the Data center and Central office networks (zone UNTRUST and subnets 80.10.99.0/24 and 80.10.1.0/24) have to be translated as well.

   The source NAT rule-sets conditions will be “from zone TRUST to zone UNTRUST” and “from zone DMZ to zone UNTRUST”.

   Additional translation specifics are listed in the next steps.

4) For sessions from the TRUST zone (subnet 172.16.10.0/24):
   a. Address pool 80.10.8.16/28 has to be used for translation and the PAT (port translation) has to be disabled (the “port no-translation” configuration within the address pool does that).
   b. Junos allows defining so called “overflow-pool” (also egress interface IP address can be used) to aid in situation when the used pool is exhausted. The instructions in this step define to use the egress interface IP address.

   Note: The linked pools or egress interface must have port translation enabled.

```
[edit security nat source]
lab@srx1# show
pool src-NAT-trust {
    address {
        80.10.8.16/28;
    }
    port no-translation;
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
    overflow-pool interface;
}
…
rule-set src-NAT-trust-untrust {
    from zone TRUST;
    to zone UNTRUST;
    rule trust-to-untrust {
        match {
            source-address 172.16.10.0/24;
            destination-address 80.10.0.0/16;
        }
        then {
            source-nat {
                pool {
                    src-NAT-trust;
                }
            }
        }
    }
}
```

c. The 172.16.11.201 – 172.16.11.206 address pool has to be used for connections from the TRUST zone to the DMZ zone. Port translation is allowed here. Another rule-set needs to be created for this purpose with the condition “from zone TRUST to zone DMZ”.

```
[edit security nat source]
lab@srx1# show pool trust-to-dmz
address {
    172.16.11.201/32 to 172.16.11.206/32;
}

[edit security nat source]
lab@srx1# show rule-set src-NAT-trust-to-dmz
from zone TRUST;
to zone DMZ;
rule trust-to-dmz {
    match {
        source-address 172.16.10.0/24;
    }
    then {
        source-nat {
            pool {
                trust-to-dmz;
            }
        }
    }
}
```

5) For sessions from the DMZ zone (subnet 172.16.11.0/24):

© 2020 Juniper Networks, Inc. All rights reserved.

a. 80.10.8.64/27 address pool with allowed port translation is used for connections destined to the Data center and Central office public addresses.

```
[edit security nat source]
lab@srx1# show pool src-NAT-dmz
address {
    80.10.8.64/27;
}

[edit security nat source]
lab@srx1# show rule-set src-NAT-dmz-untrust
from zone DMZ;
to zone UNTRUST;
rule dmz-to-dc-and-co {
    match {
        source-address 172.16.11.0/24;
        destination-address [ 80.10.99.0/24 80.10.1.0/24 ];
    }
    then {
        source-nat {
            pool {
                src-NAT-dmz;
            }
        }
    }
}
```

b. Sessions from DMZ zone to TRUST zone are translated using the 172.16.10.97 – 172.16.10.110 address range with disabled PAT. To perform this translation another rule-set needs to be configured (the condition will be “from zone DMZ to zone TRUST”)
c. If pool of IP addresses is exhausted the egress interface’s IP address must be used for translation.

```
[edit security nat source]
lab@srx1# show pool dmz-to-trust
address {
    172.16.10.97/32 to 172.16.10.110/32;
}
port no-translation;
overflow-pool interface;

[edit security nat source]
lab@srx1# show rule-set srx-NAT-dmz-to-trust
from zone DMZ;
to zone TRUST;
rule dmz-to-trust {
    match {
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
        source-address 172.16.11.0/24;
    }
    then {
        source-nat {
            pool {
                dmz-to-trust;
            }
        }
    }
}
```

The current security policy configuration does not allow traffic to pass from DMZ zone to TRUST zone. Therefore, new security policy needs to be defined. Below is a configuration example using the existing address entries and defining any application.

```
[edit security policies from-zone DMZ to-zone TRUST]
lab@srx1# show
policy dmz-to-trust {
    match {
        source-address dmz-range;
        destination-address trust-address-range;
        application any;
    }
    then {
        permit;
    }
}
```

d. To ensure that connections initiated from the same host will be translated to the same IP address the “address-persistent” parameter has to be defined.

Note: The “address-persistent” parameter is configured globally for the whole source NAT configuration and therefore affects all source NAT translations.

```
[edit security nat source]
lab@srx1# set address-persistent
```

Note: In some cases, such as the next device does not automatically build the ARP entries the proxy-arp needs to be configured with the IP addresses of the source pools .

© 2020 Juniper Networks, Inc. All rights reserved.

Branch office 2: srx2

6) Below is the appropriate address pool configuration.

```
[edit security nat source]
lab@srx2# show
pool src-NAT-pool {
    address {
        80.10.10.128/25;
    }
}
```

One way to accomplish this task is to define two source NAT rule-sets defined with following conditions:

Rule-set “src-NAT-trust-to-untrust” --> from zone TRUST to zone UNTRUST
Rule-set “src-NAT-private-to-untrust” --> from zone PRIVATE to zone UNTRUST

Because the match criteria can contain only subnet definitions (IP addresses and masks) multiple subnet definitions are required to cover the given ranges 172.16.20.200 - 172.16.20.209 and 172.16.21.16 – 172.16.21.71.
172.16.20.200 - 172.16.20.209
- 172.16.20.200 - 172.16.20.207 --> 172.16.20.200/29
- 172.16.20.208 --> 172.16.20.208/32
- 172.16.20.209 --> 172.16.20.209/32

172.16.21.16 – 172.16.21.71
- 172.16.21.16 – 172.16.21.31 --> 172.16.21.16/28
- 172.16.21.32 – 172.16.21.63 --> 172.16.21.32/27
- 172.16.21.64 – 172.16.21.71 --> 172.16.21.64/29

```
[edit security nat source]
lab@srx2# show
pool src-NAT-pool {
    address {
        80.10.10.128/25;
    }
}
rule-set src-NAT-trust-to-untrust {
    from zone TRUST;
    to zone UNTRUST;
    rule IPs-200-207 {
        match {
            source-address [ 172.16.20.200/29 172.16.20.208/32 172.16.20.209/32 ];
            destination-address 80.10.0.0/16;
        }
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
        then {
            source-nat {
                pool {
                    src-NAT-pool;
                }
            }
        }
    }
}
rule-set src-NAT-private-to-untrust {
    from zone PRIVATE;
    to zone UNTRUST;
    rule IPs-16-71 {
        match {
            source-address [ 172.16.21.16/28 172.16.21.32/27 172.16.21.64/29 ];
            destination-address 80.10.0.0/16;
        }
        then {
            source-nat {
                pool {
                    src-NAT-pool;
                }
            }
        }
    }
}
```

7) Defining the “address-persistent” parameter assures all parallel connections from one internal host will be translated to the same IP address.

```
[edit security nat source]
lab@srx2# set address-persistent
```

8) As instructed all remaining connections should be translated using the IP address of the egress interface. This can be achieved by adding one rule with appropriate match condition and action to each of the existing rule-sets. The new rules need to be placed at the end within each rule-set to be evaluated as last.

```
[edit security nat source]
lab@srx2# show
address-persistent;
pool src-NAT-pool {
    address {
        80.10.10.128/25;
    }
}
rule-set src-NAT-trust-to-untrust {
    from zone TRUST;
    to zone UNTRUST;
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
rule IPs-200-207 {
    match {
        source-address [ 172.16.20.200/29 172.16.20.208/32 172.16.20.209/32 ];
        destination-address 80.10.0.0/16;
    }
    then {
        source-nat {
            pool {
                src-NAT-pool;
            }
        }
    }
}
    rule all-other-trust {
        match {
            source-address 0.0.0.0/0;
        }
        then {
            source-nat {
                interface;
            }
        }
    }
}
rule-set src-NAT-private-to-untrust {
    from zone PRIVATE;
    to zone UNTRUST;
    rule IPs-16-71 {
        match {
            source-address [ 172.16.21.16/28 172.16.21.32/27 172.16.21.64/28 ];
            destination-address 80.10.0.0/16;
        }
        then {
            source-nat {
                pool {
                    src-NAT-pool;
                }
            }
        }
    }
    rule all-other-private {
        match {
            source-address 0.0.0.0/0;
        }
        then {
            source-nat {
                interface;
            }
        }
    }
}
```


© 2020 Juniper Networks, Inc. All rights reserved.

The current security policies do allow connections from the TRUST and PRIVATE zones only to specific corporate networks. In order to allow connections also to other destinations new security policies need to be created.
For simplicity the security policies will allow any any any connections from these zones as the focus in this chapter is on NAT and not security policies. To achieve this, the current security policies can be deleted in the following contexts:

from-zone TRUST to-zone UNTRUST
from-zone PRIVATE to-zone UNTRUST

And new security policies should be created as follows:

```
[edit security policies from-zone TRUST to-zone UNTRUST]
lab@srx2# show
policy allow-all {
    match {
        source-address any;
        destination-address any;
        application any;
    }
    then {
        permit;
    }
}

[edit security policies from-zone PRIVATE to-zone UNTRUST]
lab@srx2# show
policy allow-everything {
    match {
        source-address any;
        destination-address any;
        application any;
    }
    then {
        permit;
    }
}
```


© 2020 Juniper Networks, Inc. All rights reserved.

Task 2: Destination NAT

This part contains details about the destination NAT configuration on the cluster 1 located in the Data center.

The initial security policy configuration is assumed. If any additional security policy is needed the configuration will be presented in the respective step.

Data center: cluster 1

1) 80.10.99.101 and 80.10.99.102 public addresses are used by the external devices for accessing the protected resources. As the connections come from the Core network the destination NAT rule-set condition will be “from zone UNTRUST”.
   The subsequent steps provide more details about the required NAT destination behavior.
   The 80.10.99.101 IP address has to be translated to the 172.16.100.1 IP address. The destination ports have to remain the same, e.g. PAT will not be performed. The destination NAT address pool will contain only one IP address (172.16.100.1) without any port reference. The destination IP address in the rule match criteria will be 80.10.99.101.

```
{primary:node0}[edit security nat destination]
lab@srx3# show
pool ip-172-16-100-1 {
    address 172.16.100.1/32;
}
```

2) In addition, only hosts from the Home office and Branch office 1 and 2 have to be translated. The matching criterion here needs to reflect the correct source IP addresses of the connections from the Home and Branch offices, as their security devices perform source NAT.
   a. Connections from Home office have the following source address: 80.10.199.1 (the IP address of the egress interface is used – see step 1)
   b. Connections from Branch office 1 use 80.10.8.16/28, 80.10.8.64/27 or 80.10.8.1 (egress interface is defined as overflow-pool in step 4.b.) IP addresses.
   c. Connections from Branch office 2 use 80.10.10.128/25 or 80.10.10.1 IP addresses.

```
{primary:node0}[edit security nat destination]
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
lab@srx3# show rule-set public-access
from zone UNTRUST;
rule ip-80-10-99-101 {
    match {
        source-address [ 80.10.199.1/32 80.10.8.16/28 80.10.8.64/27 80.10.8.1/32
80.10.10.128/25 80.10.10.1/32 ];
        destination-address 80.10.99.101/32;
    }
    then {
        destination-nat pool ip-172-16-100-1;
    }
}
```

3) The table below lists the required mappings of the 80.10.99.102 IP address:

Public IP address	Public port number	Private IP address	Private port number
80.10.99.102	21	172.16.100.1	21
80.10.99.102	23	172.16.150.1	23
80.10.99.102	8080	172.16.200.1	80

As it can be seen from the table the port translation needs to be done. The destination NAT will contain 3 address pools, each referencing 1 IP address and port combination from the table.

```
{primary:node0}[edit security nat destination]
lab@srx3# show
…
pool ip-172-16-100-1-port-21 {
    address 172.16.100.1/32 port 21;
}
pool ip-172-16-150-1-port-23 {
    address 172.16.150.1/32 port 23;
}
pool ip-172-16-200-1-port-80 {
    address 172.16.200.1/32 port 80;
}
```

The destination NAT rule-set from the previous step can be reused, just new rules will be added to it. The match criteria in the new rules will contain only destination address and port combination as no restrictions were given for the source address. The reordering here is not necessary as the criteria do not overlap.

```
{primary:node0}[edit security nat destination rule-set public-access]
lab@srx3# show
from zone UNTRUST;
rule ip-80-10-99-101 {
    match {
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
        source-address [ 80.10.199.1/32 80.10.8.16/28 80.10.8.64/27 80.10.8.1/32
80.10.10.128/25 80.10.10.1/32 ];
        destination-address 80.10.99.101/32;
    }
    then {
        destination-nat pool ip-172-16-100-1;
    }
}
rule ip-80-10-99-102-port-21 {
    match {
        destination-address 80.10.99.102/32;
        destination-port 21;
    }
    then {
        destination-nat pool ip-172-16-100-1-port-21;
    }
}
rule ip-80-10-99-103-port-23 {
    match {
        destination-address 80.10.99.102/32;
        destination-port 23;
    }
    then {
        destination-nat pool ip-172-16-150-1-port-23;
    }
}
rule ip-80-10-99-102-port-8080 {
    match {
        destination-address 80.10.99.102/32;
        destination-port 8080;
    }
    then {
        destination-nat pool ip-172-16-200-1-port-80;
    }
}
```

4) Junos can check within security policies whether a NAT translation was performed on the packet or not and based on the result handle the packet as desired (permit, deny, etc.). Additional security policies are needed because the existing ones on the cluster 1 do not handle traffic destined to the 80.10.99.101 and 80.10.99.102 addresses.
   The criteria in the security policies can contain specific source, destination IP addresses as well as specific set of applications. However, in this case it is sufficient to base the criteria only on the destination IP addresses (172.16.100.1, 172.16.150.1, 172.16.200.1) and the checking whether the packet was translated or not.

© 2020 Juniper Networks, Inc. All rights reserved.

Note: Because the destination NAT is executed before security policies the security policies criteria need to consider the changed packets, e.g. use translated addresses.

Appropriate address book entries need to be created in respective zones. Below are shown all address-book entries for the affected zones not just the new ones.

```
{primary:node0}[edit security]
lab@srx3# show zones security-zone TRUST address-book
address trust-address-range 172.16.100.0/24;
address ip-172.16.100.1 172.16.100.1/32;
```

```
{primary:node0}[edit security]
lab@srx3# show zones security-zone DMZ address-book
address dmz-range 172.16.150.0/24;
address ip-172.16.150.1 172.16.150.1/32;

{primary:node0}[edit security]
lab@srx3# show zones security-zone WAREHOUSE address-book
address warehouse-range 172.16.200.0/24;
address ip-172.16.200.1 172.16.200.1/32;
```

The next step is to create the security policies. As these security policies have very specific criteria (host destination IP address) they should be placed on top of the security policies list in each context of zones to be evaluated first:

- from UNTUST to TRUST
- from UNTUST to DMZ
- from UNTUST to WAREHOUSE

The reordering of security policies is achieved using the “insert” command.

The permit action allows defining whether translated or untranslated packets should be dropped.

```
{primary:node0}[edit security policies from-zone UNTRUST to-zone TRUST]
lab@srx3# show
policy public-TRUST {
    match {
        source-address any;
        destination-address ip-172.16.100.1;
        application any;
    }
    then {
        permit {
            destination-address {
                drop-untranslated;
            }
        }
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
    }
}

{primary:node0}[edit security policies from-zone UNTRUST to-zone DMZ]
lab@srx3# show
policy public-DMZ {
    match {
        source-address any;
        destination-address ip-172.16.150.1;
        application any;
    }
    then {
        permit {
            destination-address {
                drop-untranslated;
            }
        }
    }
}
policy access-from-corp{
…


{primary:node0}[edit security policies from-zone UNTRUST to-zone WAREHOUSE]
lab@srx3# show
policy public-WAREHOUSE {
    match {
        source-address any;
        destination-address ip-172.16.200.1;
        application any;
    }
    then {
        permit {
            destination-address {
                drop-untranslated;
            }
        }
    }
}
policy co-dmz-warehouse {
…
```

5) Interface based source NAT has to be defined in order for the hosts within the TRUST zone to think the traffic was sent from cluster 1 itself. The rule-set condition will be “from routing instance default to zone TRUST” to cover all traffic going to TRUST zone. The rule match criteria will list the destination address range 172.16.100.0/24 and the then statement will reference the interface.

```
{primary:node0}[edit security nat source]
lab@srx3# show
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
rule-set traffic-to-TRUST {
    from routing-instance default;
    to zone TRUST;
    rule traffic-to-trust-zone {
        match {
            destination-address 172.16.100.0/24;
        }
        then {
            source-nat {
                interface;
            }
        }
    }
}
```

Note: Because the used IP addresses for destination NAT are from the same range as the IP address on the incoming interface the proxy-ARP needs to be configured.

```
{primary:node0}[edit security nat proxy-arp]
lab@srx3# show
interface reth0.0 {
    address {
        80.10.99.101/32 to 80.10.99.102/32;
    }
}
```

Task 3: Static NAT

This section presents the static NAT configuration details on the cluster 2 and srx7.

Central office: cluster 2

1) Static NAT provides bidirectional address translation, e.g. combination of source and destination NAT. Based on the given requirements this type of translation should be provided for the srx7 loopback IP address. The mapping here is 80.10.1.11/32 <--> 192.168.1.7/32 and the rule-set condition is “from zone UNTRUST”. Below is the static NAT configuration from cluster

```
{primary:node0}[edit security nat static]
lab@srx5# show
rule-set srx7-loopback {
    from zone UNTRUST;
    rule srx7-loopback-IP {
        match {
            destination-address 80.10.1.11/32;
        }
        then {
            static-nat prefix 192.168.1.7/32;
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
        }
    }
}
```

Two appropriate security policies have to be created to allow srx7 to initiate and accept connections to and from its loopback interface. First security policy will be from UNTRUST zone to INTERNAL zone with the following criteria: source address any, destination address 192.168.1.7/32 and application any. The second policy will be for the sessions in reverse direction, e.g. from INTERNAL zone to UNTRUST zone with the following criteria: source address 192.168.1.7/32, destination address any and application any. In this particular case no policy reordering is needed as the existing policies do not overlap with the new ones.

```
{primary:node0}[edit security zones security-zone INTERNAL]
lab@srx5# set address-book address srx7-loopback 192.168.1.7/32

{primary:node0}[edit security policies from-zone UNTRUST to-zone INTERNAL]
lab@srx5# show
policy srx-loopback-access {
    match {
        source-address any;
        destination-address srx7-loopback;
        application any;
    }
    then {
        permit;
    }
}

{primary:node0}[edit security policies from-zone INTERNAL to-zone UNTRUST]
lab@srx5# show
policy srx7-loopack-initiated {
   match {
       source-address srx7-loopback;
       destination-address any;
       application any;
   }
   then {
       permit;
   }
}
```

2) Similarly, as in the previous step static NAT will be used for mapping the following ranges 80.10.1.128/29 <--> 172.16.55.128/29. Here the rule-set condition can be “from routing-instance default” to allow hosts from any network to connect to the protected resources using the 80.10.1.128/29 IP addresses. The exiting security policies define in more details who will have access to which protected resources.

© 2020 Juniper Networks, Inc. All rights reserved.

```
{primary:node0}[edit security nat static]
lab@srx5# show rule-set dmz-access
from routing-instance default;
rule dmz-access-172-16-55-128 {
    match {
        destination-address 80.10.1.128/29;
    }
    then {
        static-nat prefix 172.16.55.128/29;
    }
}
```

Note: The proxy-arp needs to be configured for the static NAT as well.

```
{primary:node0}[edit security nat proxy-arp]
lab@srx5# show
interface reth0.0 {
    address {
        80.10.1.128/29;
        80.10.1.11/32;
    }
}
```

Note: A static route needs to be defined to provide connectivity to the srx7's lo0 IP address:

```
{primary:node0}[edit]
lab@srx5# set routing-options static route 192.168.1.7/32 next-hop 172.16.60.1
```

Finance department: srx7

3) Hiding the given address can be done using again static NAT translation. The static NAT allows defining one-to-one mappings between subnets (or networks). This mapping is based on address shifting, e.g. 1st IP address of public range is mapped to the 1st IP address of the private range,2nd IP address of public range is mapped to the 2nd IP address of the private range, etc.
   The address range for translation needs to be split because the address ranges to be hidden are smaller. The instructions tell the mappings have to start with these IP addresses: 172.16.60.128 <--> 172.16.21.0. Based on this information the subnets will be mapped as follows:
   172.16.60.128/26 <--> 172.16.21.0/26
   172.16.60.192/26 <--> 172.16.199.0/26
   One static NAT rule-set will be sufficient to provide both mapping and will have the condition "from zone INTERNAL".

```
[edit security nat static]
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
lab@srx7# show
rule-set PRIVATE-FINANCE-static-NAT {
    from zone INTERNAL;
    rule PRIVATE-static-NAT {
        match {
            destination-address 172.16.60.128/26;
        }
        then {
            static-nat prefix 172.16.21.0/26;
        }
    }
    rule FINANCE-static-NAT {
        match {
            destination-address 172.16.60.192/26;
        }
        then {
            static-nat prefix 172.16.199.0/26;
        }
    }
}
```

In this case the proxy-arp configuration is needed too.

```
[edit security nat proxy-arp]
lab@srx7# show
interface ge-0/0/4.60 {
    address {
        172.16.60.128/25;
    }
}
```

4) Due the processing sequence, checking if the packets were or weren't translated can be done only for sessions where destination NAT was performed. (Destination NAT is done before while source NAT is done after security policies.). Because the existing policies on the srx7 device do not allow any traffic going from the INTERNAL zone to the FINANCE (or PRIVATE) zone new security policies that will allow only translated traffic to pass need to be created. Below are the security policies details.
    a. First policy:
        i. From zone INTERNAL to zone FINANCE
            - Criteria: source address any, destination address 172.16.199.0/26, application any

        The existing policies will be used to determine whether to allow or deny the connections in opposite the direction.

```
[edit security zones security-zone FINANCE]
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
lab@srx7# set address-book address FINANCE-static-NAT 172.16.199.0/26

[edit security policies from-zone INTERNAL to-zone FINANCE]
lab@srx7# show
policy FINANCE-access {
    match {
        source-address any;
        destination-address FINANCE-static-NAT;
        application any;
    }
    then {
        permit {
            destination-address {
                drop-untranslated;
            }
        }
    }
}
```

b. Second policy:
    ii. From zone INTERNAL to zone PRIVATE
    - Criteria: source address any, destination address 172.16.21.0/26, application any
    iii. A security policy that allows connections in the reverse direction from PRIVATE to INTERNAL zone.
        - Criteria: source address 172.16.21.0/26, destination address any, application any

```
[edit security zones security-zone PRIVATE]
lab@srx7# set address-book address PRIVATE-static-NAT 172.16.21.0/26

[edit security policies from-zone INTERNAL to-zone PRIVATE]
lab@srx7# show
policy PRIVATE-access {
    match {
        source-address any;
        destination-address PRIVATE-static-NAT;
        application any;
    }
    then {
        permit {
            destination-address {
                drop-untranslated;
            }
        }
    }
}
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
[edit security policies from-zone PRIVATE to-zone INTERNAL]
lab@srx7# show
policy access-from-PRIVATE-static-NAT {
    match {
        source-address PRIVATE-static-NAT;
        destination-address any;
        application any;
    }
    then {
        permit;
    }
}
```

Note: The configuration on the cluster2 allows connections to the srx7 loopback IP address, but the current srx7 configuration does not. The following tasks need to be done to provide that:

- Assign lo0 to a security zone
- Create appropriate security policies

For simplicity sake the lo0 interface will be assigned to the INTERNAL zone and a new security policy that allows intrazone traffic within the INTERNAL zone will be created.

```
[edit security zones security-zone INTERNAL]
lab@srx7# set interfaces lo0.0 host-inbound-traffic system-services all

[edit security zones security-zone INTERNAL]
lab@srx7# set interfaces lo0.0 host-inbound-traffic protocols all

[edit security policies from-zone INTERNAL to-zone INTERNAL]
lab@srx7# show
policy intrazone-INTERNAL-traffic {
    match {
        source-address any;
        destination-address any;
        application any;
    }
    then {
        permit;
    }
}
```


© 2020 Juniper Networks, Inc. All rights reserved.

Task 4: NAT Protocol Translation (IPv6/IPv4)

This section focuses on enabling IPv6 and IPv4 hosts to communicate with each other by using NAT.

Branch 2

1) Configure the following IPv6 network for the PRIVATE zone: 2001:a11::254/64. Ensure the Branch2 device can reach IPv6 host 2001:a11::1/128 on interface ge-0/0/4.

```
[edit]
lab@srx2# show interfaces ge-0/0/4
unit 0 {
    ...
    family inet6 {
        address 2001:a11::254/64;
    }
}

[edit]
lab@srx2# show security forwarding-options
family {
    inet6 {
        mode flow-based;
    }
}
```

Ensure that you reboot the Branch2 device.

2) Ensure that IPv6 host 2001:a11::1/128 attached to the PRIVATE zone in Branch2 can reach the IPv4 host 80.10.10.100 by sending and receiving traffic to and from IPv6 address: 2001:a11::253. Modify or change your (existing) policies to allow traffic between the hosts

3) Ensure that IPv4 host 80.10.10.254 attached in the UNTRUST zone can reach IPv6 host 2001:a11::1 by sending and receiving traffic to and from IPv4 address 80.10.10.2 Modify or change your (existing) policies to allow traffic between the hosts

© 2020 Juniper Networks, Inc. All rights reserved.

```
[edit]
lab@srx2# show
security {
    nat {
        source {
            pool v4v6 {
                address {
                    2001:a11::253/128;
                }
            }
            pool v6v4 {
                address {
                    80.10.10.2/32;
                }
            }
        }
        rule-set src-NAT-private-to-untrust {
            from zone PRIVATE;
            to zone UNTRUST;
            rule 64nat {
                match {
                    source-address 2001:a11::1/128;
                    destination-address 80.10.10.100/32;
                }
                then {
                    source-nat {
                        pool {
                            v6v4;
                        }
                    }
                }
            }
        rule-set src-NAT-untrust-to-private {
            from zone UNTRUST;
            to zone PRIVATE;
            rule 46nat {
                match {
                    source-address 80.10.10.254/32;
                    destination-address 2001:a11::1/128;
                }
                then {
                    source-nat {
                        pool {
                            v4v6;
                        }
                    }
                }
            }
        }
    }
    static {
        rule-set v4-2-v6 {
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
from zone UNTRUST;
rule natpt-1 {
    match {
        destination-address 80.10.10.2/32;
    }
    then {
        static-nat {
            prefix {
                2001:a11::1/128;
            }
        }
    }
}
    }
    rule-set v6-2-v4 {
        from zone PRIVATE;
        rule natpt-2 {
            match {
                destination-address 2001:a11::253/128;
            }
            then {
                static-nat {
                    prefix {
                        80.10.10.100/32;
                    }
                }
            }
        }
    }
}
proxy-arp {
    interface ge-0/0/3.0 {
        address {
            80.10.10.2/32;
        }
    }
    proxy-ndp {
        interface ge-0/0/4.0 {
            address {
                2001:a11::253/128;
            }
        }
    }
}
```

Allow the traffic

```
lab@srx2# show security policies
from-zone PRIVATE to-zone UNTRUST {
    policy allow-everything {
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
        match {
            source-address any;
            destination-address any;
            application any;
        }
        then {
            permit;
        }
    }
}
from-zone UNTRUST to-zone PRIVATE {
    policy allow-everything {
        match {
            source-address any;
            destination-address any;
            application any;
        }
        then {
            permit;
        }
    }
}
```


© 2020 Juniper Networks, Inc. All rights reserved.

Appendix - Chapter 7: Attack Prevention and Mitigation

This chapter is dedicated to the Attack Prevention and Mitigation functionality on Junos security devices. The presented tasks will require you to configure stateless packet filtering, SCREEN functionality and Intrusion Prevention System features set.

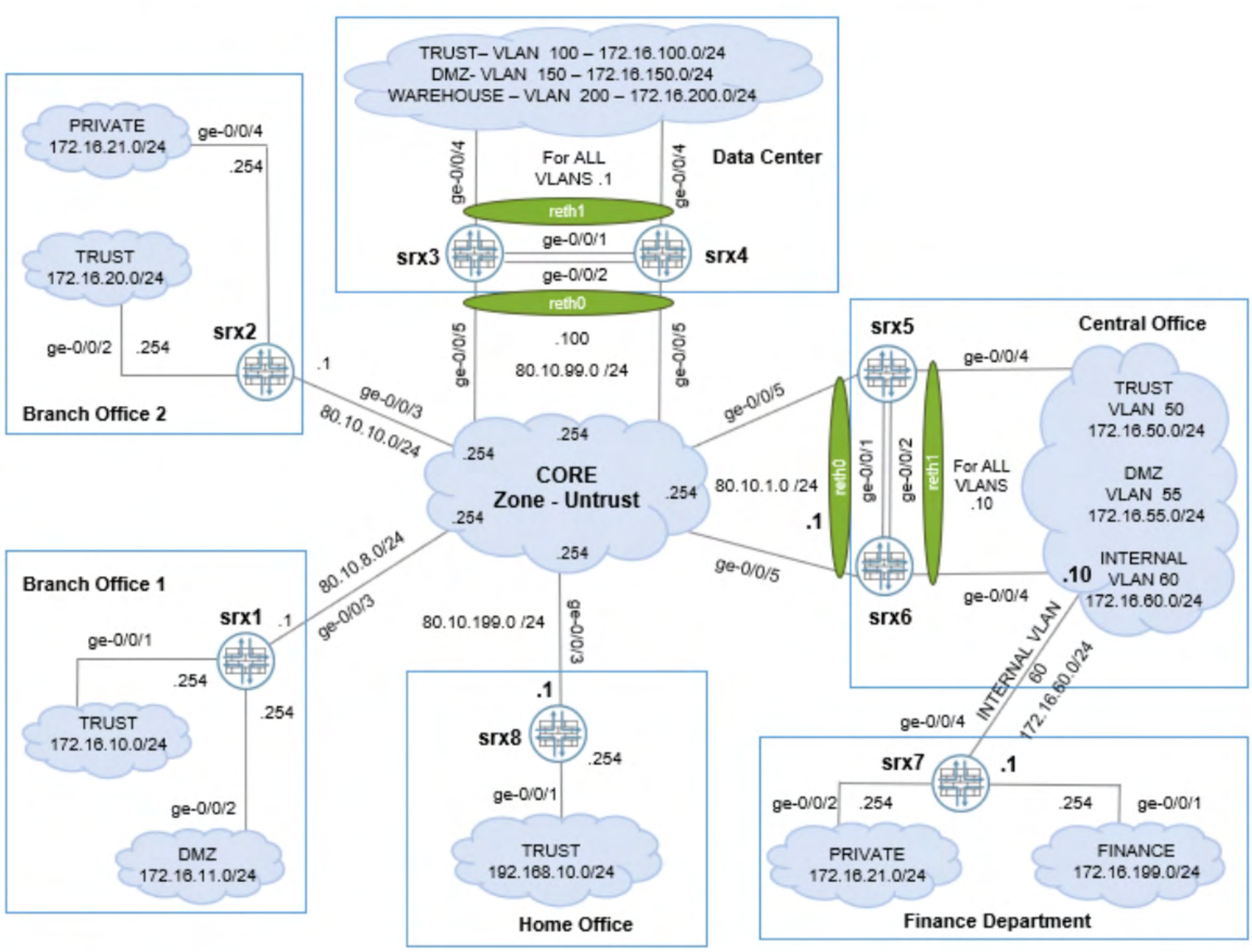


Figure 1: Chapter 7 Topology

© 2020 Juniper Networks, Inc. All rights reserved.

Firewall Filters Overview

Junos uses firewall filters to control packets passing through or destined to the device. Similarly, as security policies the traffic is matched against their defined criteria and when a match is found the respective action is executed. The firewall filters are stateless in nature which means they process each packet individually.

Firewall filters support a wide variety of match criteria, such as source and destination IP addresses and ports, priority bits, packet length, TCP flags, IP options, etc. Typically, the used actions define whether the packet is allowed or denied. However, the available actions within firewall filters offer a lot more , for example logging, assigning packets to forwarding classes, policing traffic, sampling, packet forwarding (e.g. filter based forwarding), etc. This makes the use of firewall filters very versatile.

Firewall filters consist of one or multiple blocks called terms. Each term has a condition (or criteria) and an action. The firewall filter evaluation is performed term by term in the order they appear in the configuration until a match with the criteria in the term is found and the respective action is executed. This means the term order is very important (specific terms should precede generic terms). If the packet does not match any criteria in the configured terms within the firewall filter the packet is dropped because it matches an implicit deny that is located at the end of each firewall filter. In other words, all traffic not explicitly allowed by the firewall filter is dropped.

Firewall filters associations are done in the input, output direction or both on interface logical units, physical interfaces, VLANs, routing instances. However, the supported association points depend on the Junos platform. Junos security device input firewall filters are executed the whole security processing and output firewall filters are enforced after the whole security processing.

A very common firewall filter application is to control traffic to the device control plane. It is achieved through associating a firewall filter to the loopback interface typically in the input direction. The firewall filter will be then enforced on all traffic destined to the device itself and not just on the traffic destined to the loopback interface. Therefore, pay extra attention to the firewall filter for the loopback interface and make sure all required traffic is permitted, e.g. routing protocol, remote access services, etc.

© 2020 Juniper Networks, Inc. All rights reserved.

You can use following approach for simplify the task. Highlight main traffic types and try to group them in a way that allows you to define simple criteria.

Things to remember

- ***Firewall filters are stateless.***
- ***When a firewall filter is applied to an interface all traffic not explicitly allowed in the filter is dropped.***
- ***When working with firewall filters applied to the interface used for connection apply the changes with the "commit confirmed" command.***
- ***A firewall filter associated with the loopback interface will be enforced on ALL traffic destined to the device and not just on traffic destined to the loopback interface.***

Terms are evaluated in the order they appear in the firewall filter. Try to avoid terms with generic criteria at the top.

© 2020 Juniper Networks, Inc. All rights reserved.

Task 1: Firewall Filters

In this part you will configure stateless packet filters on all security devices in the lab. The goal of this task is to protect every security device's control plane from malicious traffic by applying Firewall Filters to devices loopback interfaces.

Firewall filter works similarly to security policies in way of matching traffic patterns and applying actions. The main difference is it works in the stateless manner and needs to be applied to ingress or egress interfaces.

In case of this task firewall filter is managing traffic destined to the control plane and need to be applied as an input filter to the loopback interface.

You could find that task is quite complicated until you follow simple approach. Highlight main traffic types and group them in such a way that the key elements can be described by simple conditional clauses. That will allow you creating building blocks of your desired firewall filter.

As soon as all bricks are ready you just need to place them in correct order. Term's order does a crucial matter because matching criteria look up is going from the top to the bottom till first match! You must avoid having terms with general matching criteria on the top of you firewall filter.

1) Ensure that IPsec tunnels can be established for all security devices in the network regardless if they are located in front of or behind NAT devices. All security devices are using ESP as an IPsec protocol. **Complete this on all devices**.

In our labs we use only ESP as an IPsec protocol so it must be matched in the "`from`" statement. The UDP port 500 needs to be opened for the IKE communications in normal circumstance and UDP port 4500 in case if VPN gateway is located behind NAT device.

```
[edit firewall family inet filter protect-lo0 term ipsec]
lab@srx8# show
from {
    source-address {
        80.10.0.0/16;
    }
    protocol [ esp udp ];
    port [ 500 4500 ];
}
then accept;
```

2) Ensure that OSPF protocol is permitted for of the range of IP addresses allocated for tunnel interfaces;

© 2020 Juniper Networks, Inc. All rights reserved.

The configuration excerpt below allows OSPF traffic coming from st0 interfaces configured in other security devices.

```
[edit firewall family inet filter protect-lo0 term ospf]
lab@srx8# show
from {
    source-address {
        11.0.0.0/24;
    }
    protocol ospf;
}
then accept;
```

3) Permit DNS on UDP port 53 and NTP traffic originated from the IP address 10.10.1.0/24;

```
[edit firewall family inet filter protect-lo0 term dns-ntp]
lab@srx8# show
from {
    source-address {
        10.10.1.0/24;
    }
    protocol udp;
    destination-port [ 53 123 ];
}
```

4) Permit SNMP, RADIUS, HTTP/HTTPS, telnet and FTP traffic originated from the out-of-band management network 10/8;

```
[edit firewall family inet filter protect-lo0 term radius-snmp]
lab@srx8# show
from {
    source-address {
        10.0.0.0/8;
    }
    protocol udp;
    destination-port [ snmp radius ];
}
then accept;
```

The configuration of this task is looking straightforward until you start to do step 6. The FTP and HTTP traffic are mentioned in both steps. You can create single term that would describe SNMP, RADIUS, HTTP, HTTPS and FTP. But, in such a case, this term will shade the term that you will create later, during step 6.

The work around for this issue is to describe HTTP and FTP traffic in separate term. See configuration excerpt for step 6.

© 2020 Juniper Networks, Inc. All rights reserved.

```
[edit firewall family inet filter protect-lo0 term telnet-https-ssh]
lab@srx8# show
from {
    source-address {
        10.0.0.0/8;
    }
    protocol tcp;
    destination-port [ https telnet ssh ];
}
```

5) Permit ping packets regardless of the source IP address.

```
[edit firewall family inet filter protect-lo0 term ping]
lab@srx8# show
from {
    protocol icmp;
}
then accept;
```

6) Ensure that FTP and HTTP traffic is rate limited to 1 Mbps with the allowed traffic burst of 100 KB.

The configuration element that allows you to rate limit particular types of traffic is a policer. Its configuration is available under the `[edit firewall]` level of hierarchy. As soon as you described the way in which traffic must be limited you need to apply policer to the particular term as an action.

```
[edit firewall family inet filter protect-lo0 term rate-limit-ftp-http]
lab@srx8# show
from {
    source-address {
        10.0.0.0/8;
    }
    protocol tcp;
    port [ ftp ftp-data http ];
}
then policer rate-limit-ftp-http;
```

When you deal with the policer configuration keep in mind that "`bandwidth-limit`" is measured in bits per second and "`burst-size-limit`" is measured in bytes!

```
[edit firewall policer rate-limit-ftp-http]
lab@srx8# show
if-exceeding {
    bandwidth-limit 1m;
    burst-size-limit 100k;
}
then discard;
```


© 2020 Juniper Networks, Inc. All rights reserved.

7) Silently drop and syslog all other traffic.

The configuration example below combines "`syslog`" and "`discard`" actions together. In case if you do not need to syslog dropped traffic you can simply use implicit deny which is available by default for every firewall filter.

```
[edit firewall family inet filter protect-lo0 term deny-any-other]
lab@srx8# show
then {
    syslog;
    discard;
}
```

As soon as you completed the firewall filter's configuration it is a time applying it to the lo0 interface.

```
[edit interfaces lo0 unit 0]
lab@srx8# show
family inet {
    filter {
        input protect-lo0;
    }
    address 192.168.1.8/32;
}
```

Task 2: SCREEN

In this part you will configure lab equipment as necessary to protect network recourses of Branch offices, Finance department and Home office from different types of reconnaissance and DoS attacks with the SCREEN feature.

SCREENs are a security feature available on Junos security device helpful as an additional network protection against various types of attacks, such as flood attacks (SYN, ICMP, UDP), IP sweeps, port scans, suspicious packets, etc.

Specifying the list of attacks to look for and protect using SCREENs is done using so called "ids-options" which are located under [edit security screen] hierarchy. The attack selection is done from a fixed predefined set of options where some options can be only enabled but for some options the configuration allows to define custom threshold values. The ids-options are then associated to the zone or zones where the attack detection and protection should be performed. Multiple ids-options can be created on a single system and referenced by different zones to provide increased flexibility. However, each security zone can reference only one ids-option.

SCREEN execution is performed in the stateful processing right after the session lookup, i.e. SCREENs are the first step in the security processing before NAT translations, route

© 2020 Juniper Networks, Inc. All rights reserved.

and policy lookup. Therefore, appropriate SCREEN configuration results not only in increased network protection but also saves system resources which otherwise would be wasted with further processing.

Things to remember

- ***SCREENs are defined using ids-options.***
- ***SCREENs are association with security zones.***
- ***The system allows definition of multiple ids-options, but each security zone can reference only one ids-option at a time***
- ***SCREENs are performed right after session lookup before NAT translations, route and policy lookup.***

Branch office 1, Branch office 2, Home office: srx1, srx2 and srx8

Configure functionality on srx1, srx2 and srx8 to protect sites from malicious traffic arriving from the Core network:

1) Ensure that the SYN Proxy mechanism is enabled.

Your firewall can operate either in the syn-proxy or in the syn-cookie mode. Here is the example of syn-proxy configuration, which is enabled by default.

```
[edit security flow]
lab@srx8# show
syn-flood-protection-mode syn-proxy;
```

2) Protect against session table flood with the thresholds of 250 sessions per source and per destination IP addresses.

The SCREEN configuration is straightforward and can be done and verified on one security device. The "`load merge`" command will help you to complete configuration for the rest of the network sites.

The configuration excerpt below shows the how to configure session's limit.

```
[edit security screen ids-option from-core]
lab@srx8# show
limit-session {
    source-ip-based 250;
    destination-ip-based 250;
}
```

3) Configure protection against TCP SYN segments flood with the following thresholds and timer values:

© 2020 Juniper Networks, Inc. All rights reserved.

a. The destination thresholds values of 5000 TCP SYN segments per second.
b. Ensure that security device starts SYN Proxy protection mechanism when TCP SYN segments arrival rate reaches 500 segments per second.
c. Ensure that security device generates an alarm when TCP SYN segments arrival rate reaches 7500 segments per second.
d. The maximum time before incomplete sessions are dropped should be 10 seconds.

The configuration excerpt below shows the how to enable protection against SYN flooding.

```
[edit security screen ids-option from-core tcp]
lab@srx8# show
syn-flood {
    alarm-threshold 7500;
    attack-threshold 500;
    destination-threshold 5000;
    timeout 10;
}
```

4) Protect against ICMP flood with the threshold of 500 packets per second.

```
[edit]
lab@srx8# show security screen
ids-option from-core {
    icmp {
        fragment;
        large;
        flood threshold 500;
    }

}
```

5) Ensure that security device drops packets with following abnormalities:
    a. Fragmented ICMP packets.
    b. Fragmented TCP SYN segments.
    c. ICMP packet with size larger than 1024 bytes.

```
[edit]
lab@srx8# show security screen
ids-option from-core {
    icmp {
        fragment;
        large;
        flood threshold 500;
    }
    tcp {
        syn-frag;
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
        syn-flood {
            alarm-threshold 7500;
            attack-threshold 500;
            destination-threshold 5000;
            timeout 10;
        }
    }
}
```

As soon as all requested protection mechanisms are enabled in the ids profile you need to apply it to the security zone from which you are expecting malicious traffic arrival.

```
lab@srx8#set security zones security-zone UNTRUST screen from-core
```

Finance department: srx7

Configure srx7 to protect site from reconnaissance attempts arriving from the INTERNAL zone:

6) Ensure that detection of malicious traffic results in alarm generation instead of dropping the packets belonging to malicious packet flow.

The configuration approach for srx7 is very similar to previously discussed settings. The main difference is the alarm flag that you need to set up in the ids option for srx7 INTERNAL zone.

```
[edit security screen ids-option protect-from-internal]
lab@srx7# show
alarm-without-drop;
```

7) Protect against IP addresses sweeps with a detection rate of 10 ICMP packets arrived per 500 ms time interval.

```
[edit]
lab@srx7# show security screen
ids-option protect-from-internal {
    alarm-without-drop;
    icmp {
        ip-sweep threshold 500000;
    }
}
```

8) Protect against port scans with a detection rate of 10 port scans per 750 ms time interval.

```
[edit]
lab@srx7# show security screen
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
ids-option protect-from-internal {
    tcp {
        syn-fin;
        tcp-no-flag;
        port-scan threshold 750000;
    }
}
```

9) Detect IP packets with following values in the Options field:
    a. Time stamp option
    b. Record route option

```
[edit]
lab@srx7# show security screen
ids-option protect-from-internal {
    ip {
        record-route-option;
        timestamp-option;
    }
}
```

10) Protect against following operating systems probes:
    a. The TCP segment has both SYN and FIN flags set.
    b. The TCP segment has no flags set.

```
[edit]
lab@srx7# show security screen
ids-option protect-from-internal {
    tcp {
        syn-fin;
        tcp-no-flag;
        port-scan threshold 750000;
    }
}
```

Task 3: Intrusion Prevention System

In this part you will configure lab equipment as necessary to deploy Intrusion Prevention System features in the Data Center and Central office.

Intrusion Prevention System (IPS) represents additional security processing available on the Junos security platforms that allows the traffic inspection up to the layer 7. The IPS processing is based on attack database used for pattern matching against the traffic payload. This happens after the security policies enforcement during services processing stage. At first the data stream is being reassembled and then the application identification is performed. Next based on the identified application the message is chopped into

© 2020 Juniper Networks, Inc. All rights reserved.

contexts which are checked for anomalies (invalid values) and matched against the attack signatures from the attack database.

The IPS requires license for retrieving application identification and attack signature updates from Juniper. The database retrieval and installation on the device are separate tasks executed after one another (installation follows the retrieval) but both are performed in the background.

The IPS configuration is based on the IDP (Intrusion Detection and Prevention) policy. Initially the IDP was used as designation for the feature and later has been replaced with IPS. The replacement however did not happen completely and currently both acronyms are used and mean the same. The IDP policy consists of rulebases - IPS and Exempt. The rulebases consist of rules that have a condition and an action. The condition includes in addition to similar criteria as the security policies have – source and destination address and application – also the zones and attack objects or groups. The zone context in the IPS rule match criteria is bidirectional, i.e. the from-zone A1 to-zone A2 automatically matches also connections from-zone A2 to-zone A1. When enabling the IPS on the security device an active IDP policy needs to be configured. Remember only one IDP policy can be active on a single device at any given time. The determination whether IDP inspection should be done is defined in the security policy permit action. This means the IDP is executed only on traffic that is being handled by a security policy that has IDP enabled, i.e. the selection which traffic is subject to IDP processing is done on per security policy basis. The IDP policy evaluation differs from security policies processing. When a match is found for a rule within the IPS rulebase the matching continues until either a match is found with a terminal rule or the end of the rulebase is reached. At the end the actions from all matching rules are compared and most severe action is executed. For example, if rule with action drop packet is matched together with a rule with action close connection, the close connection action is executed on the traffic. The exempt rulebases purpose is to reduce false positives and exclude certain traffic from IPS inspection. Specifically, before the action is performed on the traffic the device tries to match the traffic against the condition in the exempt rulebase and if a match is found the traffic is forwarded. Be careful and as specific as possible when defining the exempt rules to exclude only trusted traffic and not generate false negatives.

An option exists to punish the attackers or violators with the help of so-called IP actions. When an attack is detected the IP action defines how should the subsequent connections from the attacker (or the whole network) be handled (close connection, block packets or notify) and how long. Juniper provides also IDP policy configuration templates which can be used and tweaked as needed.

The IPS can operate in three different modes:

- Integrated mode: The same process performs security policies and IPS. Only this mode is supported on the branch Junos security platforms support.

© 2020 Juniper Networks, Inc. All rights reserved.

- Dedicated mode: Separate processes perform security policies and IPS. The traffic subject to IPS processing is sent to IPS only after being permitted by the security policy. The packet is forwarded only when allowed by the IPS. This mode allows defining how much of the SPU resources are dedicated to the firewall versus the IPS processing:
  - Equal - half security policies and half IPS
  - Firewall - two-thirds security policies and one-third IPS
  - IPS - one-third security policies and two-thirds IPS
- Inline tap mode: Separate processes perform security policies and IPS. However, the packet permitted by security policy is forwarded right away and a copy is sent to IPS. Obviously, this mode is not capable of blocking single packet attacks.

Things to remember

- ***A license is required to retrieve signature updates from Juniper.***
- ***Only one IDP policy can be active on the device at any given time.***
- ***Exempt rulebase is used to reduce false positives.***
- ***The selection which traffic should be processed by the IPS is done within the security policy permit action.***
- ***The IPS zone contexts are bidirectional***

Data Center: cluster1

There are several servers located in different zones in the Data Center network (see the table below). Services that are not mentioned in this table or in the following configuration tasks must be restricted by the security policies.

Security zone name	Services
TRUST	SMTP, POP3, IMAP
DMZ	HTTP, SMTP, POP3, IMAP, FTP
WAREHOUSE	HTTP

1) Configure cluster1 to use the TCP SYN cookie rather TCP SYN proxy mechanism.

Your firewall can operate either in the syn-proxy or in the syn-cookie mode. Here is the example of syn-cookie configuration.

```
[edit security flow]
lab@srx3# show
syn-flood-protection-mode syn-cookie;
```


© 2020 Juniper Networks, Inc. All rights reserved.

2) Protect the Data Center resources with the predefined IDP policy “Recommended”. Ensure that only specified services are monitored for traffic traversing between the Data Center protected resources and Untrust zone.

You can configure only one active IDP policy per the branch SRX and this policy must describe all traffic types that you intend to monitor regardless of security zone context. The IDP policy can be modified in such a way that matching criteria would describe very specific traffic types.

The configuration excerpt below is activating Recommended idp policy.

There are few predefined policies that were installed during the initial IDP setup. You need to activate Recommended IDP policy. Use command “`show configuration security idp idp-policy Recommended`” to see all types of traffic that is analyzed by this policy. The policy consists of 9 predefined rules and some of them are excessive for the conditions of this task. You need to leave rules that monitor HTTP, SMTP, POP3, IMAP and FTP traffic.

```
[edit security idp]
lab@srx3# set default-policy Recommended
```

3) Ensure that all the Data Center resources are protected against TCP/IP attacks and malware activities from the Untrust zone as well as internal servers can’t cause infection or be the source of attacks to any hosts located in the Untrust zone.

The rulebase-ips contains two more rules that are necessary for this step’s conditions. These rules are:

```
Rule 1 /* This rule is designed to protect your networks against important TCP/IP attacks. */
Rule 9 /* This rule is designed to protect your network against common internet malware. */
```

4) Allow anonymous access from Untrust zone to the FTP servers 172.16.150.1 and 172.16.150.2 only from the 80.10.1.128/29 range. Restrict access for the rest of the hosts located in the Untrust zone. Silently drop packets from unauthorized hosts, block them for 1 hour and generate log messages with severity level Major and alert flag.

The first step assumes creation of custom attack object that describes anonymous access to FTP server.

```
[edit security idp custom-attack deny-ftp-anonymous]
lab@srx3# show
recommended-action drop;
severity major;
attack-type {
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
    signature {
        context ftp-username;
        pattern "^anonymous$";
        direction client-to-server;
    }
}
```

The representation of pattern's value as the string "^anonymous$" means that we're looking for exact matching of the FTP username starting (^) with "a" and ended ($) with "s".

As soon as attack object is created you can use it in the IDP policy. In example below we created one more rule in the rulebase-ips. This rule describes traffic that must be dropped.

Note that action can be specified either explicitly in the "then" statement of the rule or can be borrowed from the "recommended-action" of attack object.

```
[edit security idp idp-policy Recommended rulebase-ips rule deny-anonymous-ftp]
lab@srx3# show
match {
    from-zone UNTRUST;
    source-address any;
    to-zone DMZ;
    destination-address [ 172.16.150.1 172.16.150.2 ];
    application junos-ftp;
    attacks {
        custom-attacks deny-ftp-anonymous;
    }
}
then {
    action {
        recommended;
    }
    ip-action {
        ip-block;
        target source-address;
        timeout 3600;
    }
    notification {
        log-attacks {
            alert;
        }
    }
}
```

The conditions of this step define that only particular traffic sourced from the IP subnet 80.10.1.128/29 and destined to IP addresses 172.16.150.1 and 172.16.150.2 is permitted.

```
[edit security idp idp-policy Recommended rulebase-exempt rule allow-anonymous-ftp]
lab@srx3# show
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
match {
    from-zone UNTRUST;
    source-address 80.10.1.128/29 ;
    to-zone DMZ;
    destination-address [ 172.16.150.1 172.16.150.2 ];
    attacks {
        custom-attacks deny-ftp-anonymous;
    }
}
```

If the configuration of your IDP policy is complete, it is time to apply it as an action to the security policy. You do not need to specify IDP policy's name at this configuration step because only active IDP policy is used.

```
[edit security policies from-zone UNTRUST to-zone DMZ]
lab@cluster1# show
policy idp-inspection {
    match {
        source-address any;
        destination-address any;
        application [ junos-http junos-smtp junos-pop3 junos-imap junos-ftp ];
    }
    then {
        permit {
            application-services {
                idp;
            }
        }
    }
}
```

Central office: cluster2

There are two servers located in the DMZ security zone in the Central office network (see table below). Services that are not mentioned in this table or in following configuration tasks must be restricted by security policies.

Server's IP address	Services
172.16.55.100	HTTP
172.16.55.200	FTP

5) Configure cluster2 to use the TCP SYN cookie rather than the TCP SYN proxy mechanism.
6) Protect the Web and the FTP servers from any kind of HTTP or FTP attacks respectively with the severity level Critical or Major from everywhere. Silently drop

© 2020 Juniper Networks, Inc. All rights reserved.

session in the case of attack's detection, generate syslog message with the alert flag and block attacker's future connection attempts for two hours.

At this step you need to use predefined attack groups for HTTP and FTP with appropriate severity levels. In example below we created one more rule in the rulebase-ips.

```
rule rule-protect-http-ftp-servers {
    match {
        from-zone any;
        source-address any;
        to-zone DMZ;
        destination-address [ 172.16.55.100/32 172.16.55.200/32 ];
        attacks {
            predefined-attack-groups [ "FTP - Critical" "FTP - Major" "HTTP - Critical" "HTTP
- Major" ];
        }
    }
    then {
        action {
            drop-connection;
        }
        ip-action {
            ip-block;
            target source-address;
            timeout 7200;
        }
        notification {
            log-attacks {
                alert;
            }
        }
    }
}
```

7) Upload of zip, rar or tgz files to the FTP server is prohibited from anywhere. Each detected attempt results in disconnecting the client from the server by receiving with TCP RST message. The client is blocked for next five minutes. The syslog message with the severity level Major must be generated. Clients located in the TRUST and in the INTERNAL zones are permitted to access servers located both in the UNTRUST zone and in the DMZ zone.

This example's goal is to show you how to configure compound attack object and describe traffic patterns with simple regular expressions.

The main difference between the configuration excerpt below and configuration for step 21 is the "`attack-type`" that is specified now as a "`chain`" and allows combining together few sub objects.

© 2020 Juniper Networks, Inc. All rights reserved.

```
[edit security idp custom-attack upload-to-ftp]
lab@cluster2# show
severity major;
attack-type {
    chain {
        expression "zip or rar or tgz";
        member zip {
            attack-type {
                signature {
                    context ftp-put-filename;
                    pattern ".*\.\[zip\]";
                    direction client-to-server;
                }
            }
        }
```

The pattern `".*\.\[zip\]"` describes all files with .zip extension. The ".*" is used as a wildcard. The "\" is used to match character ".". The `\[zip\]"` describes case-insensitive match.

```
        member rar {
            attack-type {
                signature {
                    context ftp-put-filename;
                    pattern ".*\.\[rar\]";
                    direction client-to-server;
                }
            }
        }
        member tgz {
            attack-type {
                signature {
                    context ftp-put-filename;
                    pattern ".*\.\[tgz\]";
                    direction client-to-server;
                }
            }
        }
    }
}
```

8) Ensure that client's machines located in the TRUST security zone are protected against worms and Trojans types of attacks of all severity levels from anywhere as well as they can't cause infection or be the source of attack for any hosts located in DMZ and INTERNAL security zones.

```
rule rule-protect-clients {
    match {
        from-zone any;
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
        source-address any;
        to-zone TRUST;
        destination-address any;
        attacks {
predefined-attack-groups [ "TROJAN - All" "WORM - All" ];
        }
    }
    then {
        action {
            drop-connection;
        }
        notification {
            log-attacks {
                alert;
            }
        }
    }
}
```

Ensure that security policies between TRUST zone and DMZ and INTERNAL zones use action “application service idp” as in example below:

```
from-zone TRUST to-zone INTERNAL {
    policy trust-to-int-priv-fin {
        match {
            source-address trust-address-range;
            destination-address internal-finance-private-ranges;
            application any;
        }
        then {
            permit;
 application-services {
                    idp;
                }
            }
        }
    }
```

9) Clients are instantly denied access to the following URLs:
    a. www.instagram.com
    b. www.flickr.com

   The connection must be closed when such attempt is detected.

```
[edit security idp custom-attack prohibited-web-sites]
lab@cluster2# show
recommended-action close;
severity major;
attack-type {
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
chain {
    member instagram {
        attack-type {
            signature {
                context http-header-host;
                pattern ".*\.\[instagram\.com\]";
                direction client-to-server;
            }
        }
    }
    member flickr {
        attack-type {
            signature {
                context http-header-host;
                pattern ".*\.\[flickr\.com\]";
                direction client-to-server;
            }
        }
    }
}
```

10) The downloading of PDF files via HTTP is prohibited for users located in the TRUST zone. If such attempt has been detected the connection has to be closed.

```
[edit security idp custom-attack download-to-clients]
lab@cluster2# show
recommended-action close;
severity major;
attack-type {
    signature {
        context http-header-content-type;
        pattern ".*\[pdf\].*";
        direction server-to-client;
    }
}
```

As soon as all attack objects and groups are defined you can combine them together into the IDP policy. You will create and activate your own policy rather than will use any of predefined IDP policies, and, as a final step, enable IDP action for the necessary security policies.

Task 4: Verification

Firewall Filters

The way that you can verify firewall filter's operations is to launch different types of traffic destined to the Routing Engine and observe the fact of the success or the failure.

© 2020 Juniper Networks, Inc. All rights reserved.

You can temporary enable action count for some particular terms as a work around.

```
[edit firewall family inet filter protect-lo0 term public-services]
lab@srx8# show
from {
    source-address {
        172.31.10.1/32;
    }
    protocol udp;
    port [ ntp 53 ];
}
then {
    count public-services;
    accept;
}
```

If any traffic matches the "from" statement you will be able to see counter incremented in the output below:

```
lab@srx8> show firewall filter protect-lo0 counter public-services
Filter: protect-lo0
Counters:
   Name                    Bytes                  Packets
   public-services         0                      0
```

SCREEN

You can verify your SCREEN configuration by launching command below.

```
lab@srx8> show security screen ids-option from-core-net
Screen object status:

Name                                        Value
ICMP flood threshold                        500
TCP SYN flood attack threshold              500
TCP SYN flood alarm threshold               7500
TCP SYN flood source threshold              4000
TCP SYN flood destination threshold         5000
TCP SYN flood timeout                       10
Session source limit threshold              250
Session destination limit threshold         250
```

If you are looking for real statistic use command "show security screen statistics". This command allows you deriving statistics on per interface or on per security zone base.

```
lab@srx8> show security screen statistics zone UNTRUST
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
Screen statistics:

IDS attack type                          Statistics
  ICMP flood                             0
  UDP flood                              0
  TCP winnuke                            0
  TCP port scan                          0
  ICMP address sweep                     0
  TCP sweep                              0
  UDP sweep                              0
  IP tear drop                           0
  TCP SYN flood                          0
  IP spoofing                            0
  ICMP ping of death                     0
  IP source route option                 0
  TCP land attack                        0
  TCP SYN fragment                       0
  TCP no flag                            0
  IP unknown protocol                    0
  IP bad options                         0
  IP record route option                 0
  IP timestamp option                    0
  IP security option                     0
  IP loose source route option           0
  IP strict source route option          0
  IP stream option                       0
  ICMP fragment                          0
  ICMP large packet                      0
  TCP SYN FIN                            0
  TCP FIN no ACK                         0
  Source session limit                   0
  TCP SYN-ACK-ACK proxy                  0
  IP block fragment                      0
  Destination session limit              0
```

Intrusion Prevention System

There are few commands below that can be used for IDP troubleshooting and monitoring.

```
lab@srx5> show security idp status

lab@ srx5> show security idp attack table

lab@ srx5> show security flow ip-action all
```

You can verify that IDP configuration is operational or not by analyzing local file "messages". The best way to sift through the contents of this file is to filter syslog messages with the text string "RT_IDP".

© 2020 Juniper Networks, Inc. All rights reserved.

```
lab@ srx3>show log messages | match RT_IDP | match severity
```

Another option for verification is traceoptions. The only flag available at the moment is "all".

```
[edit security idp traceoptions]
lab@ srx5# show
file idp_ts;
flag all;
```


© 2020 Juniper Networks, Inc. All rights reserved.

Appendix - Chapter 8: Extended Implementation Concepts

This chapter is focused on two features of JUNOS Security: Transparent mode and Filter Based Forwarding. The presented scenarios require you to reconfigure security devices srx1 and srx7 according to picture below.

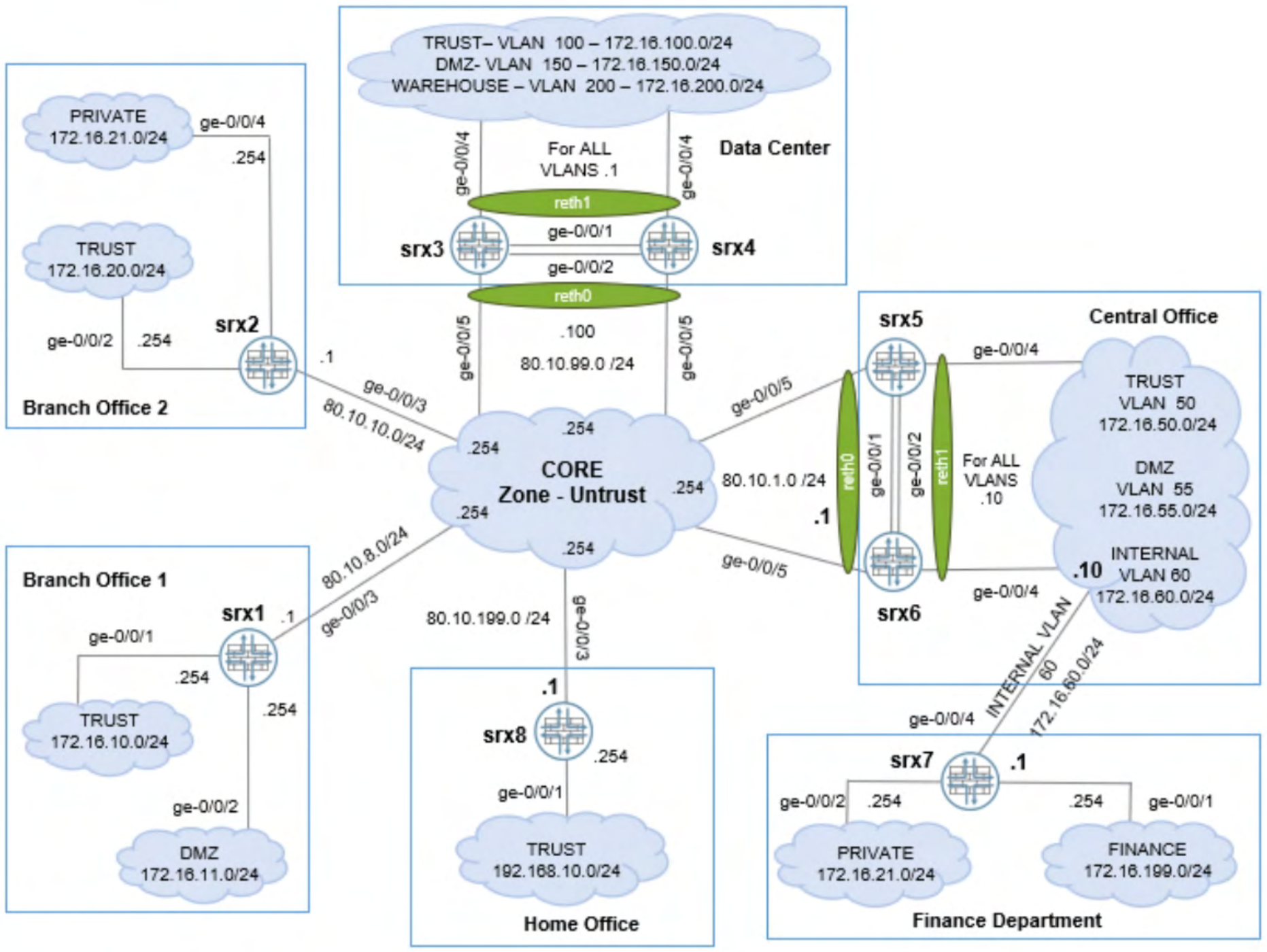


Figure 1: Chapter 6 Topology

Typically, Junos security device represents a layer 3 device in the networks that performs routing. However, situations exist where deploying firewall as layer 3 device cannot be done, for example when the environment would have to be readdresses which might not be is not possible or when the readdressing is not ready, and the firewall services are needed immediately, etc. The transparent mode is suitable for these cases because it essentially lets the firewall behave like a layer 2 switch, i.e. the firewall does the forwarding decisions based on the MAC addresses rather than on the IP addresses. It does segment the layer 2 domain from the security perspective, but it does not create layer 2 domain

© 2020 Juniper Networks, Inc. All rights reserved.

boundaries from the network perspective, i.e. it is transparent to the RM OSI model layer 3. Even when in transparent mode the device still provides and supports the security functionality – stateful firewalling using zones and security policies, IPS, SCREENs, etc. Transparent mode is supported in chassis cluster deployments, but certain features are not supported, such as NAT or IPsec VPN, also some protocol support, such as STP protocols, IGMP snooping, Q-in-Q, etc. is currently not available. For detailed list refer to the respective Junos release documentation. The Junos security device can run either in routing mode or in transparent mode. Both modes simultaneously on single device are not supported. When configuring the device to run in transparent mode a reboot is required. In transparent mode so "vlans" are configured on the device and the interfaces are layer 2 and have family "ethernet-switching" defined and operating either as access or trunk ports.

Things to remember

- ***Junos security device can operate either in routing or transparent mode. Running both modes simultaneously on a single device is not supported.***
- ***In transparent mode the firewall makes the forwarding decisions based on MAC addresses.***
- ***To run device in transparent mode requires device reboot.***
- ***Chassis cluster is also supported for transparent mode.***

Task 1: Transparent Mode

In this section you need to configure Home office's security device in such that srx1 will make forwarding decisions based on MAC address rather than on the base of IP header's information.

1) Configure the interfaces, bridge domain and security zones on the srx1 according to the table below, which reflects the topology image.
   Rewrite vlan-id 81 with the vlan-id 80 on the trunk port ge-0/0/5.0.

Interface	IP address	Interface mode	VLAN-ID	Zone
ge-0/0/4.0	n/a	Access	80	TRUST
ge-0/0/5.0	n/a	Trunk	81	DMZ
ge-0/0/3.0	n/a	Access	80	UNTRUST
irb.0	80.10.8.5/24		80	N/a

The main difference between configuring transparent mode instead of Layer 3 mode is the configuration of logical interfaces. You do not need to specify "`family inet`" and IP addresses anymore. Instead of this "`family ethernet-switching`" must be associated

© 2020 Juniper Networks, Inc. All rights reserved.

with the logical units as well as interface mode (access or trunk) and "`vlan members`" value regardless if Ethernet port is in the trunk or in the access mode.

The code excerpt below provides you with the example how interface configuration can be accomplished. Note that for trunk interface ge-0/0/5.0 vlan tagging rewriting is applied.

```
[edit interfaces]
lab@srx1# show
ge-0/0/3 {
    unit 0 {
        family ethernet-switching {
            interface-mode access;
            vlan {
                members vlan80;
            }
        }
    }
}
ge-0/0/4 {
    unit 0 {
        family ethernet-switching {
            interface-mode access;
            vlan {
                members vlan80;
            }
        }
    }
}
ge-0/0/5 {
    vlan-tagging;
    unit 80 {
        family ethernet-switching {
            interface-mode trunk;
            vlan {
                members vlan80;
            }
            vlan-rewrite {
                translate 81 80;
            }
        }
    }
}
fxp0 {
    unit 0 {
        family inet {
            address 10.10.1.1/24;
        }
    }
}
irb {
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
    unit 0 {
        family inet {
            address 80.10.8.5/24;
        }
    }
}
lo0 {
    unit 0 {
        family inet {
            address 192.168.1.1/32;
        }
    }
}
```

```
[edit vlans]
lab@srx1# show
vlan80 {
    vlan-id 80;
    l3-interface irb.0;
}
vlan81 {
    vlan-id 81;
}
```

The security device will be converted into the transparent mode only after the system's reboot:

```
lab@srx1# commit and-quit
warning: Interfaces are changed from route mode to transparent mode. Please reboot the device
or all nodes in the HA cluster!
commit complete
Exiting configuration mode

lab@srx1> request system reboot
```

The rest of configuration is similar to steps that are discussed in Chapter 3 "Firewall. Security policies".

1) Configure static default route pointing to the IP address 80.10.8.5/24.
2) The hosts from the TRUST zone and its network range can go to the outside network (Internet) with HTTP and HTTPS.
3) Ensure the hosts from the TRUST zone have access to the whole private corporate network (reachable via CORE network) with any application.
4) Devices in the DMZ zone should be accessible from the whole private corporate network including the local TRUST zone with HTTPS.
5) No other connections are allowed to go in or out of the TRUST zone.

© 2020 Juniper Networks, Inc. All rights reserved.

6) No connections are allowed to go out from DMZ zone. Log all violations going out to the CORE network.
7) Ensure that irb.0 interface with IP address 80.10.8.5 is accessible with ping, telnet and HTTP only from the TRUST zone.

Configure the security zones

```
[edit]
lab@srx1# show security zones
security-zone UNTRUST {
    address-book {
        address corp-network 172.16.0.0/16;
    }
    interfaces {
        ge-0/0/3.0;
    }
}
security-zone TRUST {
    host-inbound-traffic {
        system-services {
            ping;
            http;
            telnet;
        }
    }
    interfaces {
        ge-0/0/4.0;
    }
}
security-zone DMZ {
    address-book {
        address dmz-server 80.10.8.101/32;
    }
    interfaces {
        ge-0/0/5.80;
    }
}
```

Configure the security policies

```
[edit]
lab@srx1# show security policies
from-zone TRUST to-zone UNTRUST {
    policy internet-access {
        match {
            source-address any;
            destination-address any;
            application [ junos-http junos-https ];
        }
        then {
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
            permit;
        }
    }
    policy corp-network-access {
        match {
            source-address any;
            destination-address corp-network;
            application any;
        }
        then {
            permit;
        }
    }
    from-zone TRUST to-zone DMZ {
        policy trust-to-dmz {
            match {
                source-address any;
                destination-address dmz-server;
                application junos-https;
            }
            then {
                permit;
            }
        }
    }
    from-zone UNTRUST to-zone DMZ {
        policy corp-network-to-dmz {
            match {
                source-address corp-network;
                destination-address dmz-server;
                application junos-https;
            }
            then {
                permit;
            }
        }
    }
    from-zone DMZ to-zone UNTRUST {
        policy dmz-to-untrust-log {
            match {
                source-address any;
                destination-address any;
                application any;
            }
            then {
                deny;
                log {
                    session-init;
                }
            }
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
    }
}
```

Task 2: Filter Based Forwarding

In this section you need to configure Finance department's security device in such that srx7 will forward packets originated from the PRIVATE and FINANCE zones on other criteria then the destination IP address.

There are two network paths to the Core network available in the Finance department. One path is direct connection to the Core network via interface ge-0/0/3.0. Another path leads to the Core network via the Central office network and is formed on the base of interface ge-0/0/4.60.

1) Configure srx7 in such that HTTPS traffic originated either from the PRIVATE or from the FINANCE zone and destined to the prefix 80.10.99.0/24 is forwarded via interface ge-0/0/3.0. All other traffic should be forwarded via interface ge-0/0/4.60
2) Ensure that asymmetric traffic forwarding is not possible.

The main goals of this task can be accomplished in three steps.

I. The first step assumes that ingress traffic needs to be classified according to the forwarding criteria. You will create firewall filters that should be applied as input filters to interfaces ge-0/0/1.0 and ge-0/0/2.0. The purpose of this firewall filters is to identify HTTP traffic and redirect it to the special routing instance which forwards packets differently from the muster routing instance.

```
[edit firewall family inet filter fbf term match-https]
lab@srx7# show
from {
    protocol tcp;
    port https
}
then {
    routing-instance fbf-instance;
}
```

As soon as firewall filter is created apply it to the interfaces ge-0/0/1.0 and ge-0/0/2.0 in input direction using commands below:

```
lab@srx7# set interface ge-0/0/1.0 family inet filter input fbf
lab@srx7# set interface ge-0/0/2.0 family inet filter input fbf
```


© 2020 Juniper Networks, Inc. All rights reserved.

II. The goal of second step is to create such a routing instance which forwarding behavior will be different from the master routing instance inet.0. In simple words, we want to define different default gateway for HTTPS traffic.

```
[edit routing-instances fbf-instance]
lab@srx7# show
instance-type forwarding;
routing-options {
    static {
        route 0.0.0.0/0 next-hop 80.10.2.254;
    }
}
```

III. All interfaces direct routes are located in the master routing instance `inet.0`. It means that routing instance `fbf-instance` cannot resolve next-hop's IP address for the default route. Configuring rib-group element can solve this issue. The idea is to describe which routes must be copied from the `inet.0` into the `fbf-instance`. Here you are going:

```
[edit routing-options]
lab@srx7# show
interface-routes {
    rib-group inet int-routes;
}
rib-groups {
    int-routes {
        import-rib [ inet.0 fbf-instance.inet.0 ];
    }
}
```

The goal of this can be accomplished by ensuring that source NAT is applied to traffic originated from the PRIVATE and FINANCE security zones.

Task 3: Verification

Transparent Mode

All commands that you learned in appendix for chapter 3 are applicable here as well.

It also can be useful to verify the status of security device's interfaces, in which mode they operate, to which bridge domains they belong.

```
lab@srx1> show ethernet-switching interface
lab@srx1> show ethernet-switching global-information
```

If you are satisfied with the interfaces and VLAN configuration it is time to check the content of the bridge table with the command below.

© 2020 Juniper Networks, Inc. All rights reserved.

```
lab@srx1> show ethernet-switching table
```

Filter based forwarding.

First of all, initiate HTTPS session from either the PRIVATE or the FINANCE security zone. It can be done with the command below:

```
lab@srx7> telnet 172.31.10.1 port 443
```

Check session table of srx7 to ensure that HTTPS connection is established via the outgoing interface ge-0/0/2.0. Here is the command for this action:

```
lab@srx7> show security flow session protocol tcp port 443
```

NOTE: If you failed to observe expected entries in the session table ensure that security policies from the PRIVATE and from the FINANCE zones to the UNTRUST zone exist and permit HTTP traffic.

© 2020 Juniper Networks, Inc. All rights reserved.

Appendix - Chapter 9: Advanced Services

In this appendix section you will find the solutions for tasks from the Advanced Services chapter.

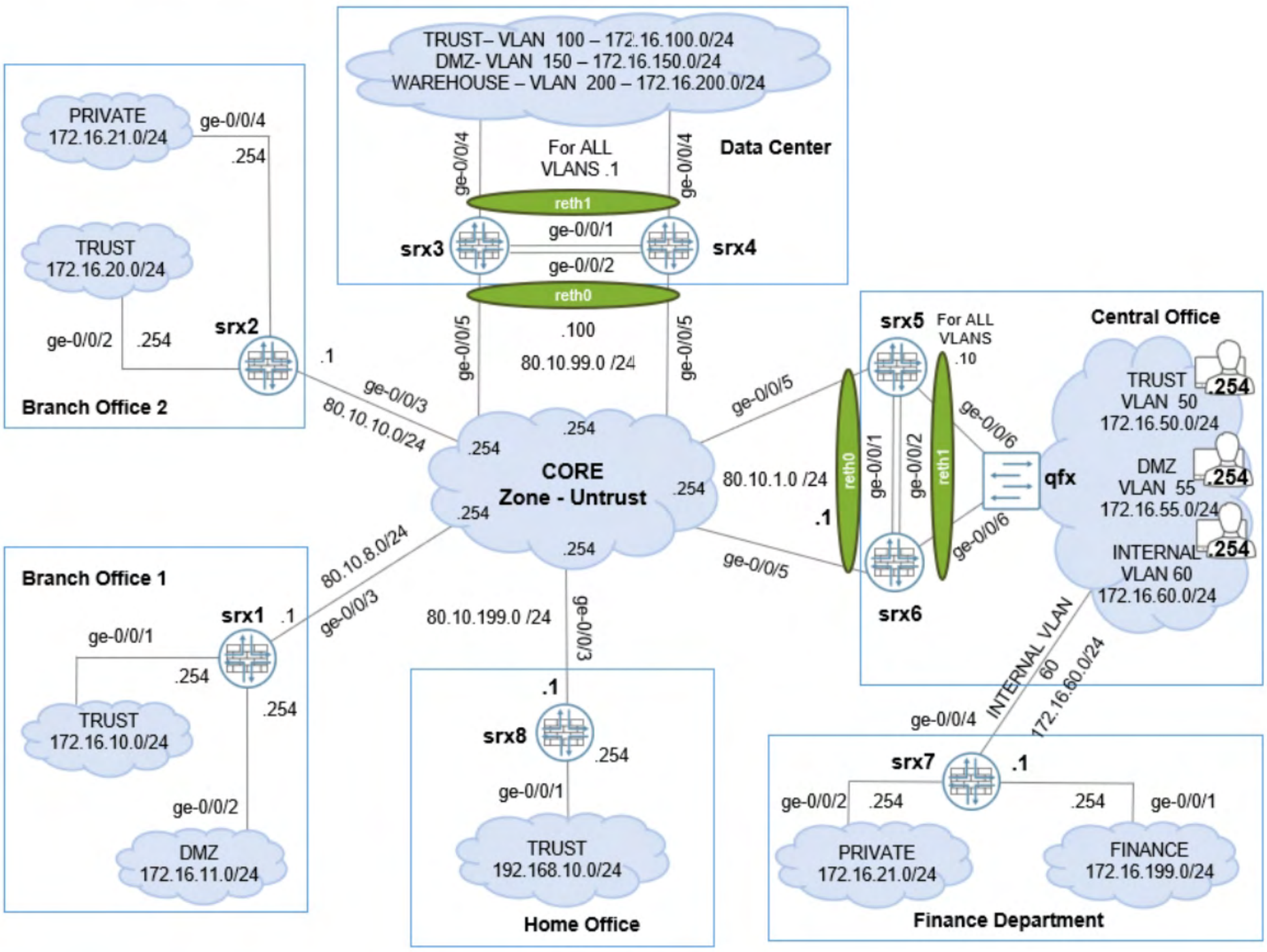


Figure 1: Chapter 9 Topology

© 2020 Juniper Networks, Inc. All rights reserved.

Task 1: Application Identification

Data center: cluster 1

1) The application system cache (ASC) configuration is located under [edit services application-identification] stanza. The cache timeout is defined with the command below. The parameter takes values in seconds: 2 hours = 7200 seconds.

```
{primary:node0}[edit services application-identification]
lab@srx3# set application-system-cache-timeout 7200
```

2) The following configuration excerpt enables the automatic AppID updates that start from 30th of March at 23:30 with the update interval of 24 hours. To fulfill the task requirement just define the date that represents the day on which you are completing the task.

```
{primary:node0}[edit services application-identification]
lab@srx3# show
download {
    automatic {
        start-time 03-30.23:30;
        interval 24;
    }
}
```

1) Allow encrypted Gmail traffic from the DMZ zone to the UNTRUST zone.
2) Ensure the firewall generates a message when the session has been denied.

```
[edit security policies from-zone DMZ to-zone UNTRUST]
lab@srx3# show
policy allow-specific-APPs {
    match {
        source-address dmz-range;
        destination-address any;
        application junos-https;
        dynamic-application junos:GMAIL;
    }
    then {
        permit
        log {
            session-init;
        }
    }
}
```


© 2020 Juniper Networks, Inc. All rights reserved.

Task 2: AppTrack

The following information is about how to configure the application tracking on the cluster 1 to meet the given requirements.

Data center: cluster 1

1) The AppTrack feature is enabled on per security zone basis. Once defined for a zone the firewall will generate session tracking messages for connections in that zone. Junos allows adjusting the message creation settings such as when the 1st for a session is created – either directly when the application is identifier or after the defined interval elapses, and interval for periodic updates.
   Execute the following commands to have the firewall create the initial tracking message right when the application identification concludes and then send an update every 10 minutes.

```
{primary:node0}[edit]
lab@srx3# set security application-tracking first-update

{primary:node0}[edit]
lab@srx3# set security application-tracking session-update-interval 10
```

   The AppTrack messages are syslog messages that are generated by the RT_FLOW (same as security policy logs). For specific identification the "APPTRACK" string can be used. The task demands the logs being kept together with the security policy logs. Check the current syslog configuration.

```
{primary:node0}[edit]
lab@srx3# show system syslog
user * {
    any emergency;
}
host 10.10.1.254 {
    any emergency;
    source-address 192.168.1.3;
}
file messages {
    any critical;
}
file interactive-commands {
    interactive-commands info;
}
file security-policy-logs {
    user info;
    match RT_FLOW;
    archive size 512k files 20;
}
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
file authorization-file {
    authorization info;
}
time-format year;
```

From the syslog configuration above (currently present on cluster 1) the security-policy-logs file will store the AppTrack messages right away.

Enable the AppTrack for the TRUST zone.

```
{primary:node0}[edit]
lab@srx3# set security zones security-zone TRUST application-tracking
```

Task 3: AppQoS

In here the AppQoS configuration is listed that fulfills the given requirements.

Data center: cluster 1

1) The location of the AppQoS configuration is under the [edit class-of-service application-traffic-control] stanza. The main part is based on rule-sets (similar as AppFW) where the defined information tells what applications to look for and then how to handle them from the class of service perspective (e.g. apply rate limiters, change the priority bits and forwarding class). The last step – referencing the rule-set within the security policy permit action – might now come as no surprise.

   The AppQoS can use rate-limiters that are defined under the same hierarchy ([edit class-of-service application-traffic-control]) as the rule-sets.

   The task instructs to limit the junos:GMAIL application to the limit of 50000kb/s with burst of 312kB. Below is the rate-limiter configuration that reflects these values.

```
{primary:node0}[edit class-of-service]
lab@srx3# show
application-traffic-control {
    rate-limiters gmail-rl {
        bandwidth-limit 50000;
        burst-size-limit 312000;
    }
}
```


© 2020 Juniper Networks, Inc. All rights reserved.

NOTE: Please keep in mind the bandwidth is defined in kilobits per second whereas the burst-size-limit is defined in bytes.

The rule-set accommodating the requirements (rate-limiting the junos:GMAIL application in the “from server” direction, setting the loss priority to high once the rate-limiter threshold is crossed and changing the dscp priority bits) follows:

```
{primary:node0}[edit class-of-service application-traffic-control]
lab@srx3# show rule-sets gmail-rs
rule-sets gmail-rs {
    rule gmail {
        match {
            application junos:GMAIL;
        }
        then {
            dscp-code-point ef;
            rate-limit {
                server-to-client gmail-rl;
loss-priority-high;
            }
        }
    }
}
```

Traffic where this specific CoS behavior has to be enforced is from the DMZ to the UNTRUST zone. A security policy in the DMZ to UNTRUST zone context already exists (from task 3 AppFW). Only the reference to the AppQoS rule-set has to be added under the permit action.

```
{primary:node0}[edit]
lab@srx3# set security policies from-zone DMZ to-zone UNTRUST policy allow-specific-APPs then
permit application-services application-traffic-control rule-set gmail-rs
```

The security policy then looks like this:

```
lab@srx3# show security policies from-zone DMZ to-zone UNTRUST
policy allow-specific-APPs {
    match {
        source-address dmz-range;
        destination-address any;
        application junos-https;
        dynamic-application junos:GMAIL;
    }
    then {
        permit {
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
            application-services {
                application-traffic-control {
                    rule-set gmail-rs;
                }
            }
        }
        log {
            session-init;
        }
    }
}
```

Task 4: SSL Proxy

This part handles the SSL Proxy configuration based on the given tasks.

Data center: cluster 1

1) First step is to locally generate the certificate for signing the modified server certificates that will be presented to the end user. The task contains details which the signing certificate must fulfill. The certificate creation requires a key to be present. So, the starting point is the key generation with the given specifics:

```
{primary:node0}
lab@srx3> request security pki generate-key-pair certificate-id MY-CERT size 1024 type rsa
```

Then the certificate generation follows:

```
request security pki local-certificate generate-self-signed certificate-id
MY-CERT domain-name juniper.net subject "DC=JNPR,CN=Juniper,OU=unit-
1,O=Juniper,SN=1234,L=,ST=US,C=US" email noreply@juniper.net add-ca-
constraint
```

Note: Please keep in mind the “add-ca-constraint“ parameter is crucial here. It tells the device to generate a certificate for signing other certificates.

Note: In case the key pair is already generated you will receive the following error message

```
lab@srx3> request security pki generate-key-pair certificate-id MY-CERT size
1024 type rsa
node0:
--------------------------------------------------------------------------
error: Command aborted as key pair already exists. Retry after clearing the
existing key pair
```

2) Due the nature of the SSL proxy feature, the end user gets a modified server certificate instead of the original one. That means he is not able to do the

© 2020 Juniper Networks, Inc. All rights reserved.

verification himself. This task is performed on the SRX by default (but can be disabled through configuration – the "ignore-server-auth" action in the SSL proxy profile). However, the SRX needs to know which CA certificates to use for the server certificate validation. A CA-profile-group is used for that. Below is the command that loads the CA certificate for validation from the file listed in the task.

Note: Please keep in mind in case the "ignore-server-auth" action is used this step is not needed and can be skipped. This has already been done in the lab environment.

```
{primary:node0}
lab@srx3> request security pki ca-certificate ca-profile-group load ca-group-name MY-CA-GROUP
filename /etc/certs/EngineeringCA.pem
```

3) The configuration allows defining URLs that should bypass the SSL proxy processing – a whitelist. The whitelist references addresses or address-sets from the global address book.

   Note: Please keep in mind that two ways are supported on SRXs for defining the addresses and address-sets:
   - "Old" style – the addresses and address-sets are defined in address-book under the security zone
   - "New" style – the address-books are defined right under [edit security] stanza and zones are attached to them. One address-book called "global" can be used by each security zone by default without any explicit association or attachment.

   However, the configuration allows the use of only one of the styles at a time, i.e. they cannot be used together in the same configuration.

   As mentioned above the SSL proxy whitelist uses the addresses/address-sets from the global address book. This means the "new" style has to be used in the configuration! If the configuration is using the "old" style it must be converted.

   The task whitelist definition is below. Again, two options exist – group the addresses in an address-set or define multiple addresses directly in the whitelist parameter. The following sample configuration uses the address-set approach to illustrate the components needed:

© 2020 Juniper Networks, Inc. All rights reserved.

```
{primary:node0}[edit]
lab@srx3# show security address-book
global {
    address JNPR {
        dns-name www.juniper.net;
    }
    address JunosGenius {
        dns-name www.junosgenius.net;
    }
    address GMAIL {
        dns-name www.gmail.com;
    }
    address-set SSL-WHITELIST {
        address JNPR;
        address JunosGenius;
        address GMAIL;
    }
}
```

Note: Please keep in mind the DNS server has to be configured (set system name-server A.B.C.D) when using domain names for the address entries. Otherwise the system will not be able to resolve them to IP addresses. For this lab, please use 8.8.8.8 for your DNS definition.

```
{primary:node0}[edit]
lab@srx3# set system name-server 8.8.8.8
```

4) Now the SSL proxy profile needs to be configured (the configuration hierarchy is [edit services ssl proxy]). The SSL proxy profile contains details about the certificate to be used for signing the modified server certificates, which CA certificates to use for server authentication or disables the authentication, what to log and the whitelist.
The SSL proxy profile configuration below meets the task requirements.

```
{primary:node0}[edit]
lab@srx3# show services ssl
proxy {
    profile MY-SSL-PROFILE {
        trusted-ca MY-CA-GROUP;
        root-ca MY-CERT;
        whitelist SSL-WHITELIST;
        actions {
            log {
                sessions-allowed;
            }
        }
    }
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
}
```

In addition, the task asks for sending the SSL proxy logs into the “ssl-proxy” file. The SSL proxy generates the log messages with the facility of PFE. The “match SSL” statement ensures that only SSL proxy generated messages go into the file and no other. Below is the syslog configuration excerpt.

```
{primary:node0}[edit]
lab@srx3# show system syslog file ssl-proxy
pfe any;
match SSL;
```

Finally, the SSL proxy profile has to be referenced from the security policy permit action. Currently no suitable security policy exists from TRUST to UNTRUST zone that could be used for referencing the SSL proxy profile. Therefore, a new one has to be created. The configuration is shown below:

```
{primary:node0}[edit security policies from-zone TRUST to-zone UNTRUST]
lab@srx3# show
...
policy https-traffic {
    match {
        source-address trust-address-range;
        destination-address any;
        application junos-https;
    }
    then {
        permit {
            application-services {
                ssl-proxy {
                    profile-name MY-SSL-PROFILE;
                }
            }
        }
    }
}
```

This new policy is placed at the end in the TRUST to UNTRUST zone context. To achieve correct operation, it has to be moved in front of the “internet-denied-log” policy. The following command does just that:

```
{primary:node0}[edit security policies from-zone TRUST to-zone UNTRUST]
lab@srx3# insert policy https-traffic before policy internet-denied-log
```

The resulting security policies sequence in the TRUST to UNTRUST zone context:

```
{primary:node0}[edit security policies from-zone TRUST to-zone UNTRUST]
lab@srx3# show | no-more
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
policy corp-access {
    match {
        source-address trust-address-range;
        destination-address corp-network;
        application any;
    }
    then {
        permit;
    }
}
policy http-access {
    match {
        source-address trust-address-range;
        destination-address any;
        application junos-http;
    }
    then {
        permit {
            application-services {
                application-firewall {
                    rule-set deny-spec-APPS;
                }
            }
        }
        log {
            session-init;
        }
    }
}
policy https-traffic {
    match {
        source-address trust-address-range;
        destination-address any;
        application junos-https;
    }
    then {
        permit {
            application-services {
                ssl-proxy {
                    profile-name MY-SSL-PROFILE;
                }
            }
        }
    }
}
policy internet-denied-log {
    match {
        source-address any;
        destination-address any;
        application any;
    }
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
        then {
            deny;
            log {
                session-init;
            }
        }
}
```

Task 5: Juniper Identity Management Service (JIMS)

Juniper Identity Management Service (JIMS) provides a robust and scalable user identification and IP address mapping implementation that includes endpoint context and machine ID. JIMS collects user identity information from different authentication sources, for SRX Series devices.

JIMS collects user identity information from a configured Active Directory and makes it available to SRX Series devices or vSRX instances. You can download and install Juniper Identity Management Service (JIMS), configure the CSO client on JIMS to obtain user identity information from the configured Active Directory, and use CSO and JIMS to manage user-based firewall policy intents on SRX Series devices and vSRX instances.

The SRX Series devices communicate with JIMS through HTTP or HTTPS connection. Use HTTP connection for debugging and HTTPS for deployments. SRX Series devices consist of primary and secondary JIMS configurations. These devices must always query the primary JIMS. The secondary JIMS is available as a fall back option with limited resources. The secondary JIMS must be used when the HTTP GET query or a number of queries to the primary JIMS fails. SRX Series devices constantly scrutinize the failed primary JIMS and revert to the primary JIMS, once it is up and running.

When you request a JIMS report, the SRX Series device specifies the timestamp. JIMS forms an HTTPS response from the earliest known report since the requested timestamp. SRX Series devices request for the maximum number of reports to include in the response from JIMS. Along with the requested reports, JIMS always returns a cookie. In the subsequent requests to JIMs, SRX Series devices include cookies instead of timestamp to indicate the same context, same beginning timestamp, and to resume the same response from where it has stopped the previous time.

© 2020 Juniper Networks, Inc. All rights reserved.

Note:

- IP and user mapping information might be inaccurate, if the user identities in JIMS are cleared, delayed, or missing.
- SRX firewall authentication can also push the authentication entries to JIMS.

The SRX Series device communicates with JIMS through HTTP or HTTPS messages to obtain the access token and query for user identities. The following different query modes are available, and all queries can happen simultaneously.

Access Token Query

JIMS requires OAuth 2.0 protocol to authenticate or authorize. The SRX Series device user query function requires an access token to query the JIMS server. The SRX Series device uses the client credentials such as client ID and client secret to obtain an access token. These parameters must be consistent with the API client configured on JIMS.

Batch or Periodic Query

At the beginning, SRX Series device sends the batch queries to JIMS sequentially to obtain all the expected user identities. When there are no more entries in JIMS, SRX Series device periodically queries for the newly generated reports with the configured interval.

The timestamp is mentioned in the query to restart the response. The timestamp is expected in the query under the following circumstances:

- SRX Series device queries the JIMS server for the first time
- SRX Series device switches over to the secondary JIMS
- SRX Series device does the error recovery because of an internal error or upon receiving error response from JIMS

For all the other cases, SRX Series device provides the received cookie information in the query instead of a timestamp.

IP Address Query

SRX Series device can provide another query to JIMS specifying the IP address, if it has missed the data for the existing IP address flow. If there are many IP address queries in the queue, SRX Series device can keep multiple concurrent HTTP or HTTPS connections with JIMS to increase the throughput. However, the number of

© 2020 Juniper Networks, Inc. All rights reserved.

concurrent connections is restricted to less than or equal to 20 connections to reduce the load on JIMS.

User Mapping Query

SRX Series device can engage Captive Portal to obtain the user ID to authenticate the user. Once the user is authenticated, SRX Series device can issue another query to JIMS specifying the user ID and IP address to obtain user information. The firewall authentication uses the *https://<JIMS>/<query-api>/user/ip=<ip>&id=<id>&domain=<domain>* API to push an authentication success entry to JIMS with the user IP, user ID, and the domain. JIMS responds with the user information.

The difference between the IP address query and user query is that the IP address query does not have the user ID. Both these queries insert the user information to the internal cache of JIMS , and all SRX devices are updated with user information.

This part provides insight into the solution for the Juniper identification task that involves active directory.

Data center: cluster 1

1) Configure Juniper Identity Management Service to be able to identify network traffic on cluster 1 based on IP address as well as user and device context. Implement your solution for authenticated, unauthenticated and unknown users in the TRUST to UNTRUST zone for traffic destined towards the corporate-networks.

```
{primary:node0}[edit services user-identification]
lab@srx3# show
identity-management {
    authentication-entry-timeout 60;
    connection {
        connect-method https;
        port 443;
        primary {
            address 10.10.1.121;
            client-id jncie;
            client-secret "$9$TF6ArlMXxdBIyKMWx7jHkPz3"; ## SECRET-DATA
        }
        token-api oauth_token/oauth;
        query-api user_query/v2;
    }
}
```

The final step is to include the “user-identity” parameter in the matching criteria of the appropriate security policy. The task defines to use the “jncie-

© 2020 Juniper Networks, Inc. All rights reserved.

sec-exam" value for this parameter in the security policy that handles the access from the TRUST zone to the corporate network (zone UNTRUST). By examining the current policies in this context (TRUST to UNTRUST) the policy "corp-access" looks like to perfect candidate because of its criteria – source address matches the TRUST subnet and destination address matches the corporate subnet. The resulting policy configuration is displayed below:

```
{primary:node0}[edit security policies from-zone TRUST to-zone UNTRUST]
lab@srx3# show policy corp-access
match {
    source-address trust-address-range;
    destination-address corp-network;
    application any;
    source-identity any;
}
then {
    permit;
}
```

Verify is the AD server is reachable and the HTTPS connection is up and running.

```
{primary:node0}[edit services user-identification]
lab@srx3# run show services user-identification identity-management status
node0:
--------------------------------------------------------------------------
Primary server :
    Address                       : 10.10.1.121
    Port                          : 443
    Connection method             : HTTPS
    Connection status             : Online
    Last received status message : OK (200)
    Access token                  : j1gwTLfcgDBf7CMtbneFTP1P6WyJq8VyGCzNUsm
    Token expire time             : 2019-01-11 11:24:28
Secondary server :
    Address                       : Not configured
```

Task 6: Security Logging

3) Cluster1 device should be sending its security logs to the Security Director located at 10.10.1.99 (integrated log collector). Enable logging for at least one policy for the TRUST to UNTRUST zone

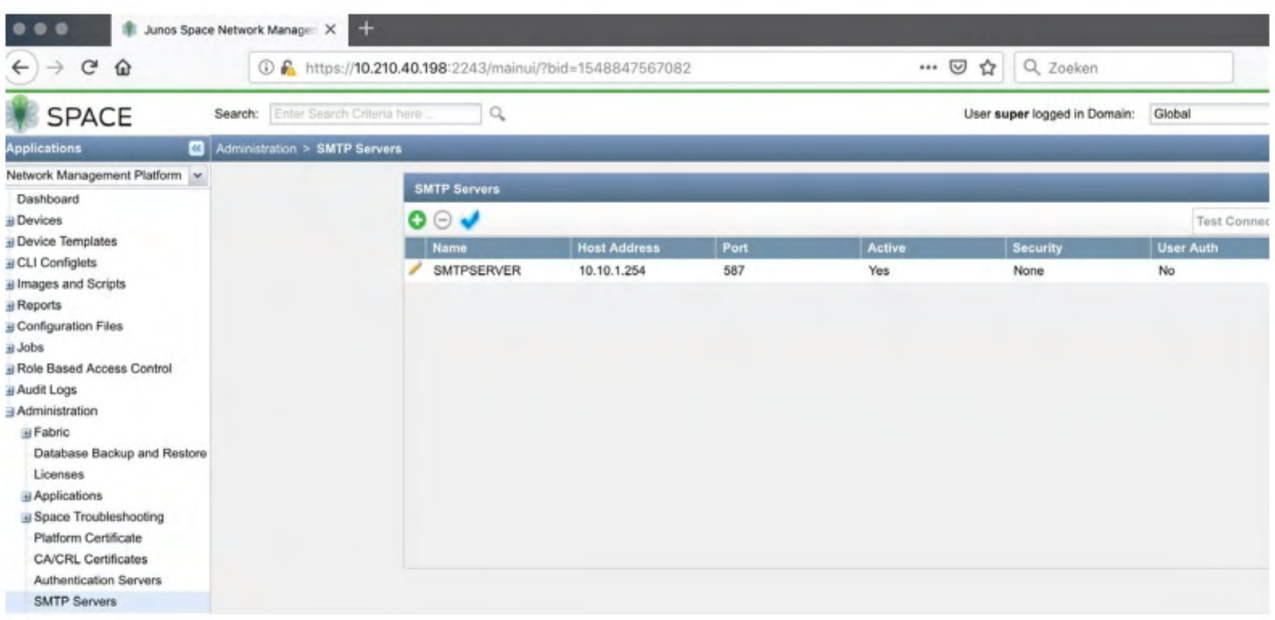
```
{primary:node0}[edit]
lab@srx3# show security log
mode stream;
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
format sd-syslog;
source-address 10.10.1.3;
stream my-stream {
    severity info;
    format sd-syslog;
    category all;
    host {
        10.10.1.99;
    }
}

from-zone TRUST to-zone UNTRUST {
    policy corp-access {
        match {
            source-address trust-address-range;
            destination-address corp-network;
            application any;
            source-identity any;
        }
        then {
            permit;
            log {
                session-init;
                session-close;
            }
        }
    }
}
```

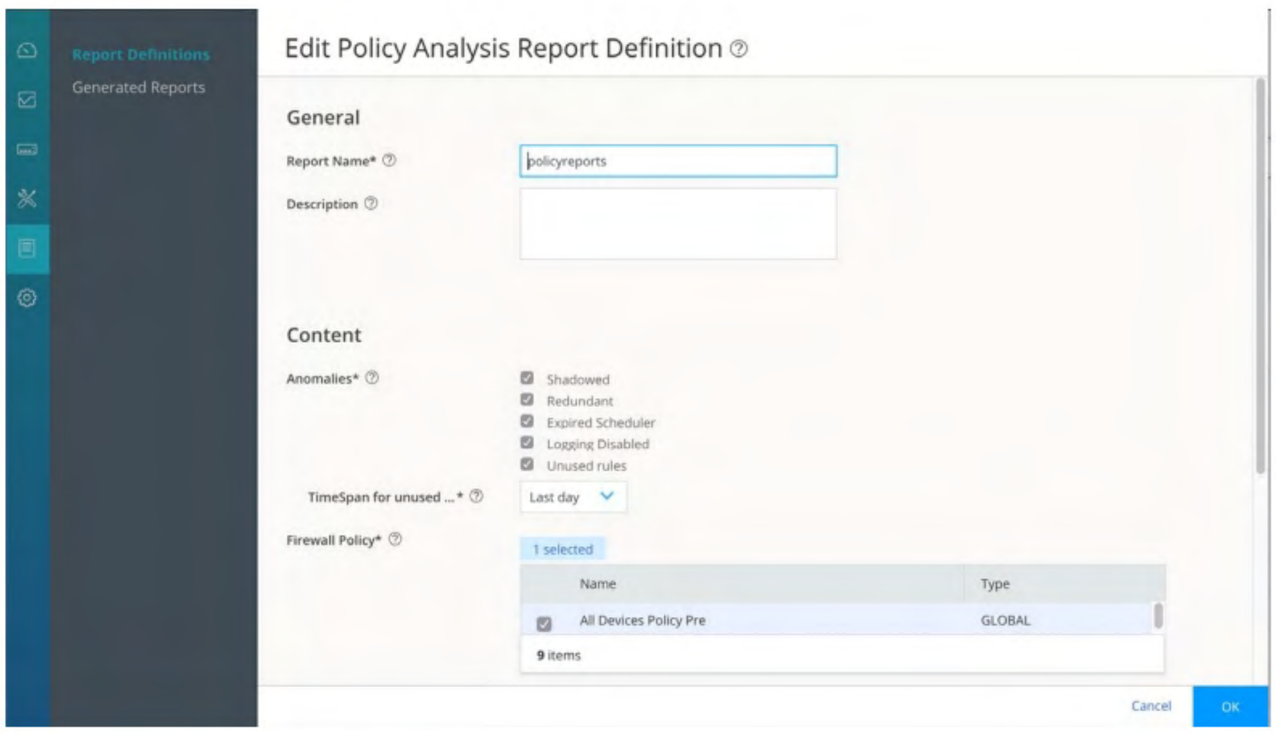
4) Ensure a daily report is send to noreply@juniper.net that shows all anomalies for policies that are applied before device specific policies. The SMTP server is located at: 10.10.1.254

Configure the SMTP server in SD under the administration/ smtp server section

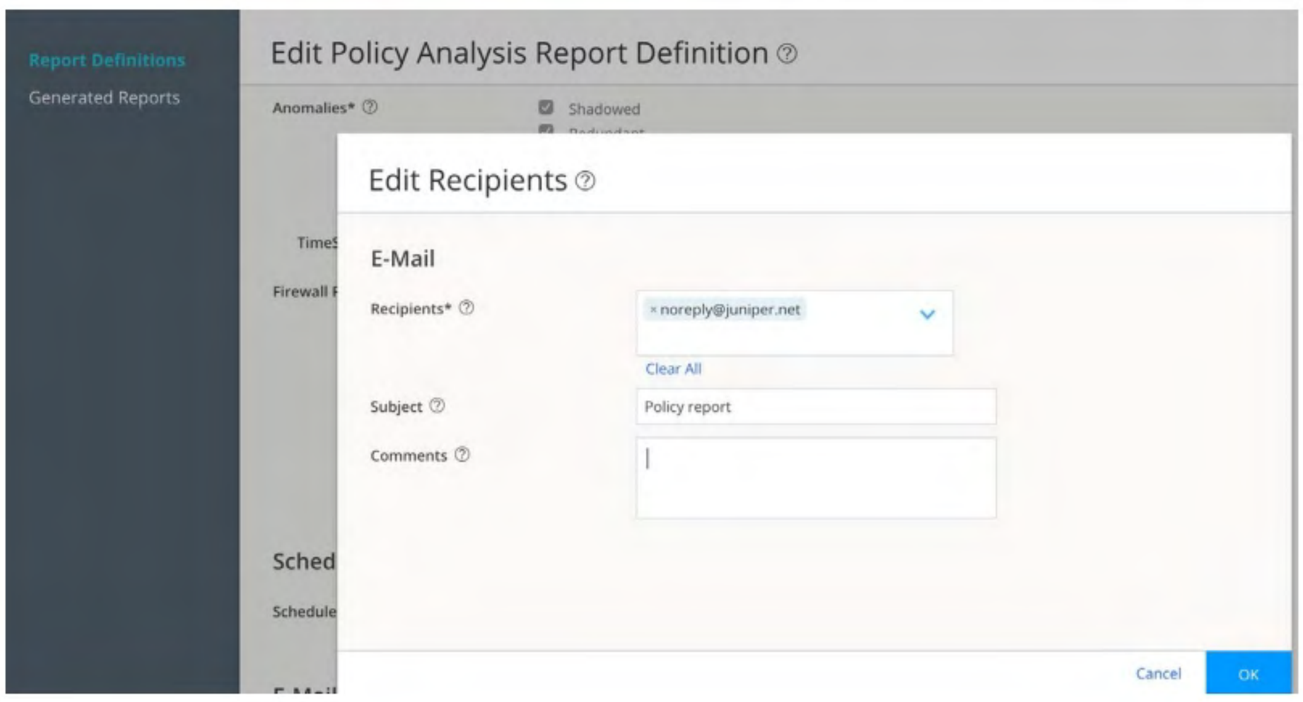


© 2020 Juniper Networks, Inc. All rights reserved.

Next create a Policy Analysis Report Definition. Make sure to select all anomalies. The timespan should be set to “daily” and enable the report for “All Devices Policy Pre” group policies



Specify noreply@juniper.net as the email recipient to meet the task requirement



© 2020 Juniper Networks, Inc. All rights reserved.

Task 7: Software Defined Secure Network (SDSN)

Juniper Sky Advanced Threat Prevention (Juniper Sky ATP) is a security framework that protects all hosts in your network against evolving security threats by employing cloud-based threat detection software with a next-generation firewall system.

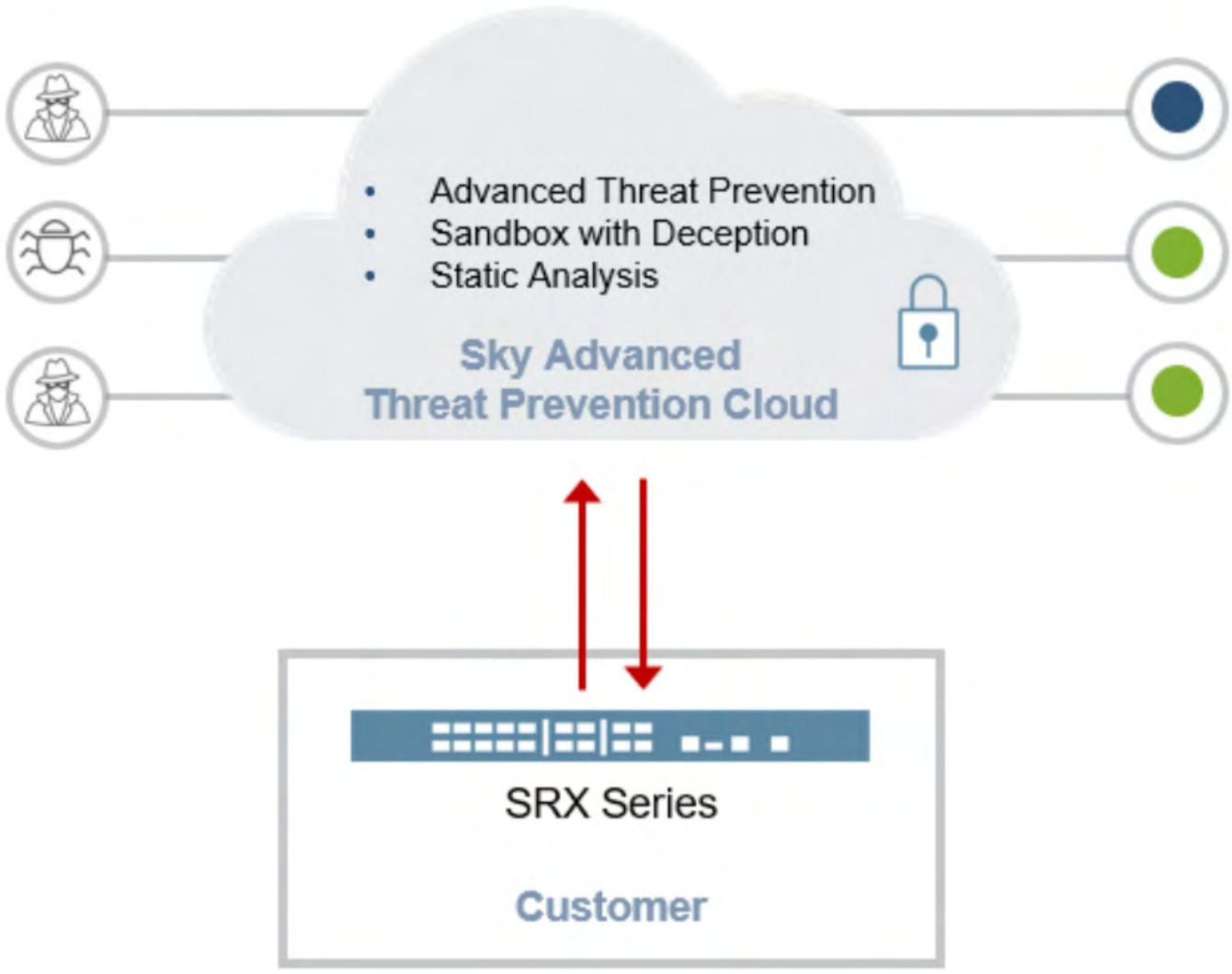


Figure 2: Juniper Sky ATP Components

Juniper Sky ATP protects your network by performing the following tasks:

- The SRX Series device extracts potentially malicious objects and files and sends them to the cloud for analysis.
- Known malicious files are quickly identified and dropped before they can infect a host.
- Multiple techniques identify new malware, adding it to the known list of malware.
- Correlation between newly identified malware and known Command and Control (C&C) sites aids analysis.

© 2020 Juniper Networks, Inc. All rights reserved.

- The SRX Series device blocks known malicious file downloads and outbound C&C traffic.

Juniper Sky ATP supports the following modes:

- Layer 3 mode
- Tap mode
- Transparent mode using MAC address
- Secure wire mode (high-level transparent mode using the interface to directly pass traffic, not by MAC address.)

Juniper Sky ATP Features

Juniper Sky ATP is a cloud-based solution. Cloud environments are flexible and scalable, and a shared environment ensures that everyone benefits from new threat intelligence in near real-time. Your sensitive data is secured even though it is in a cloud shared environment. Security analysts can update their defense when new attack techniques are discovered and distribute the threat intelligence with very little delay.

In addition, Juniper Sky ATP offers the following features:

- Integrated with the SRX Series device to simplify deployment and enhance the anti-threat capabilities of the firewall.
- Delivers protection against “zero-day” threats using a combination of tools to provide robust coverage against sophisticated, evasive threats.
- Checks inbound and outbound traffic with policy enhancements that allow users to stop malware, quarantine infected systems, prevent data exfiltration, and disrupt lateral movement.
- High availability to provide uninterrupted service.
- Scalable to handle increasing loads that require more computing resources, increased network bandwidth to receive more customer submissions, and a large storage for malware.
- Provides deep inspection, actionable reporting, and inline malware blocking.
- APIs for C&C feeds, whitelist and blacklist operations, and file submission.

© 2020 Juniper Networks, Inc. All rights reserved.

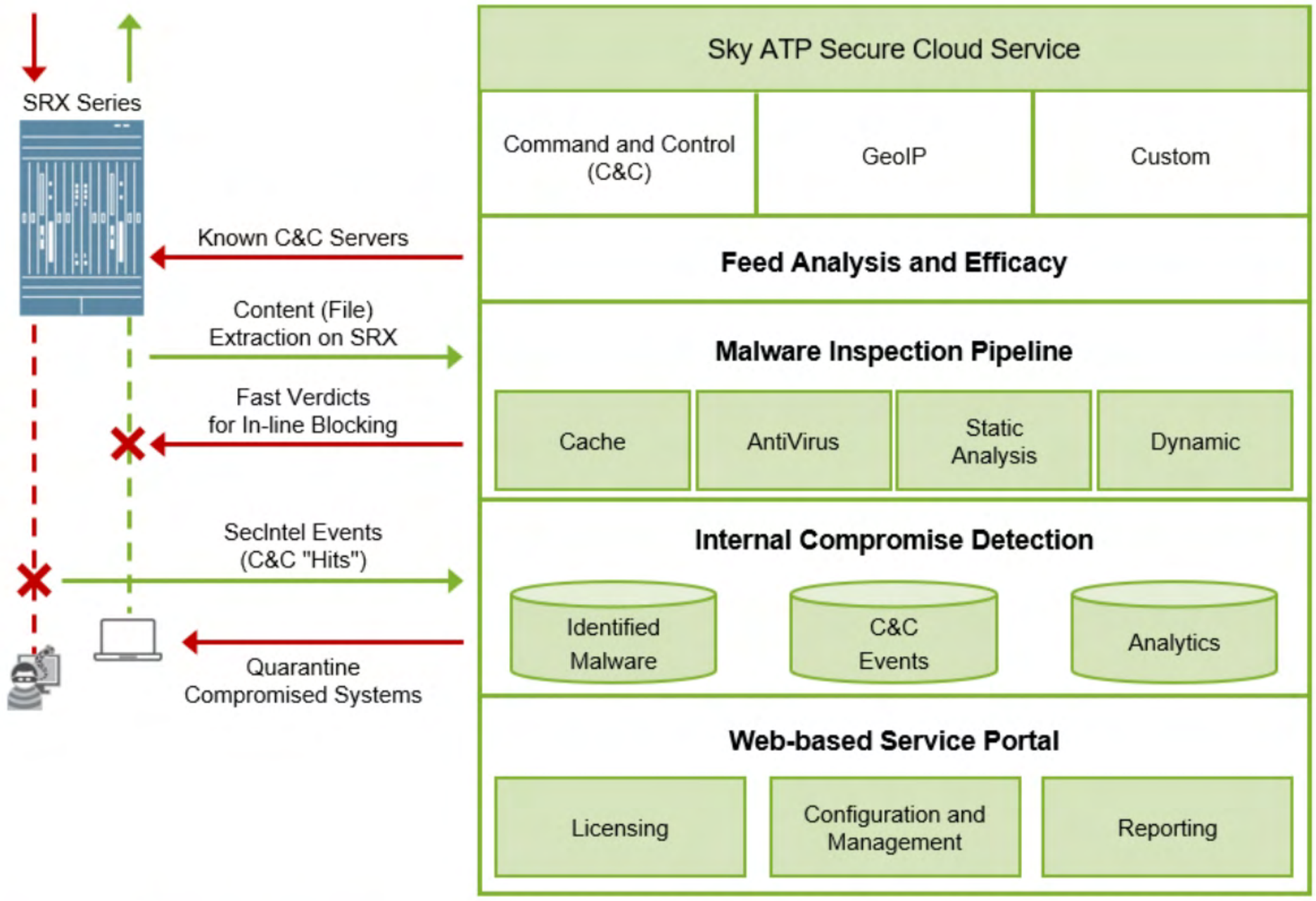


Figure 3: Juniper Sky ATP Components

How the SRX Series Device Remediates Traffic

The SRX Series devices use intelligence provided by Juniper Sky ATP to remediate malicious content through the use of security policies. If configured, security policies block that content before it is delivered to the destination address.

For inbound traffic, security policies on the SRX Series device look for specific types of files, like .exe files, to inspect. When one is encountered, the security policy sends the file to the Juniper Sky ATP cloud for inspection. The SRX Series device holds the last few KB of the file from the destination client while Juniper Sky ATP checks if this file has already been analyzed. If so, a verdict is returned, and the file is either sent to the client or blocked depending on the file's threat level and the user-defined policy in place. If the cloud has not inspected this file before, the file is sent to the client while Juniper Sky ATP performs an exhaustive analysis. If the file's threat level indicates malware (and depending on the user-defined configurations) the client system is marked as an infected host and blocked from outbound traffic.

© 2020 Juniper Networks, Inc. All rights reserved.

1) Create a new SkyATP realm. Enroll Policy Enforcer and the central office cluster in the newly created Sky ATP Realm through Security Director

Use the information below to setup the Sky ATP Realm:

SkyATP Realm	jnciesec-xxx (where xxx is your lab username)
Username	jnciesec-xxx@stu.juniper.net
Password	lab123@Lab
Juniper SSO account	eduservicenow@gmail.com
Juniper SSO password	********

Use the information for Security Director and Policy Enforcer:

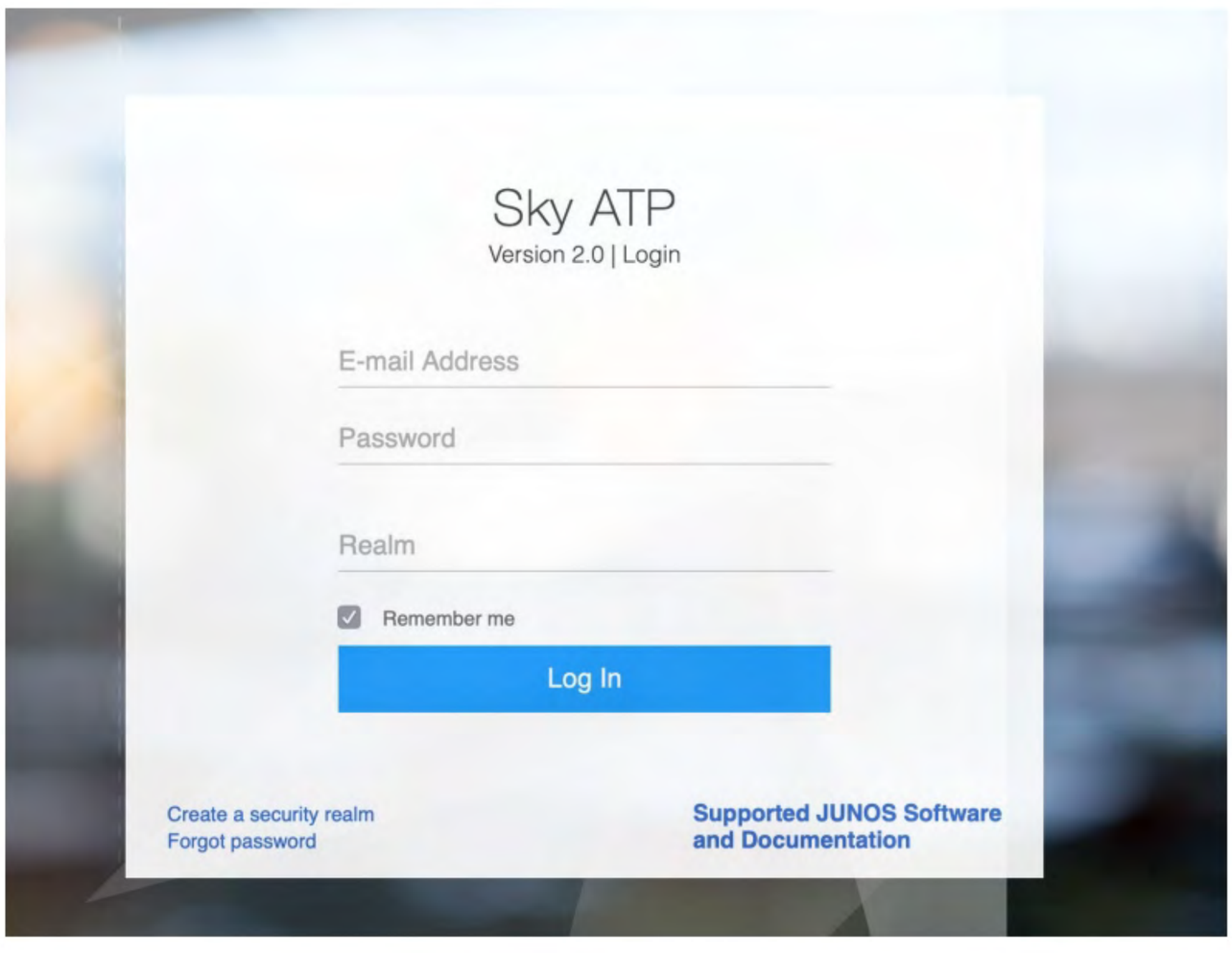
Security Director Username	super
Security Director Password	lab123@Lab
Security Director IP	10.10.1.100
Policy Enforcer Username	root
Policy Enforcer Password	lab123@Lab
Policy Enforcer IP	10.10.1.123

Note: The password for the Juniper SSO account is auto populated in the Firefox browser on the Student Desktop. For this reason, it is important to use the Firefox browser on the Student Desktop to create the Sky ATP realm.

© 2020 Juniper Networks, Inc. All rights reserved.

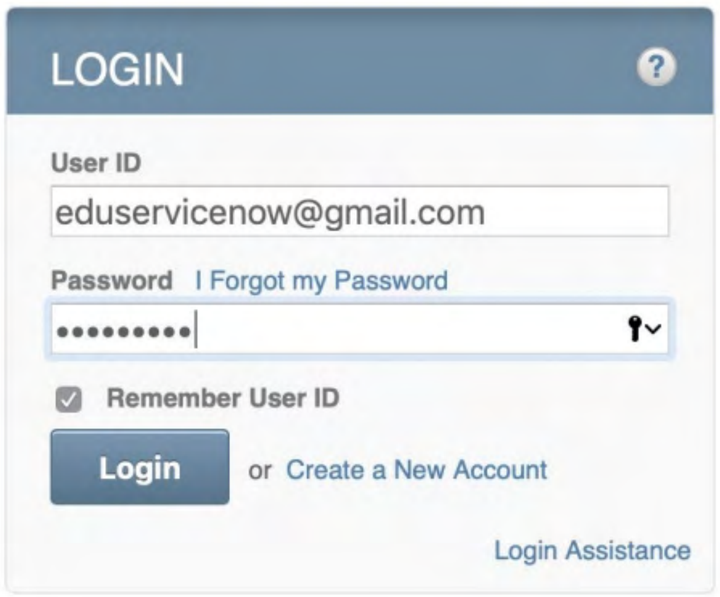
a) The first step is to create a new SkyATP realm. To do this you have to navigate to the following URL: http://amer.sky.junipersecurity.net using the Firefox browser of the Student Desktop.

Click on "**Create a security realm**" in the lower left corner of the Sky ATP login screen.



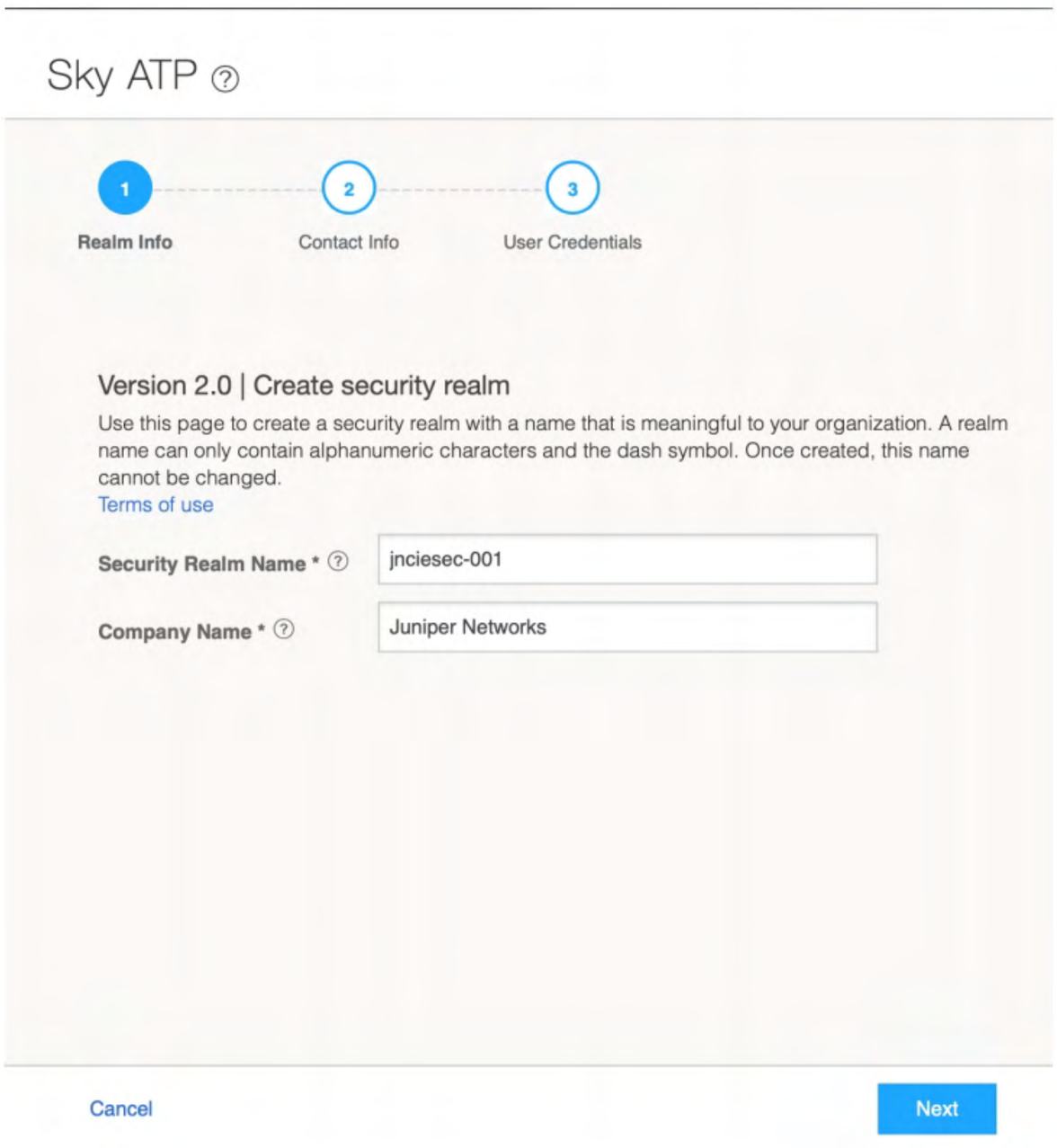
© 2020 Juniper Networks, Inc. All rights reserved.

b) To create a new SkyATP realm you are redirected to Juniper Network Single Sign On (SSO) and you must login with a valid account. As mentioned in the instructions it is important to use the Firefox browser installed on the student desktop as the password for userID: eduservicenow@gmail.com is auto populated. Click on the login button to proceed.



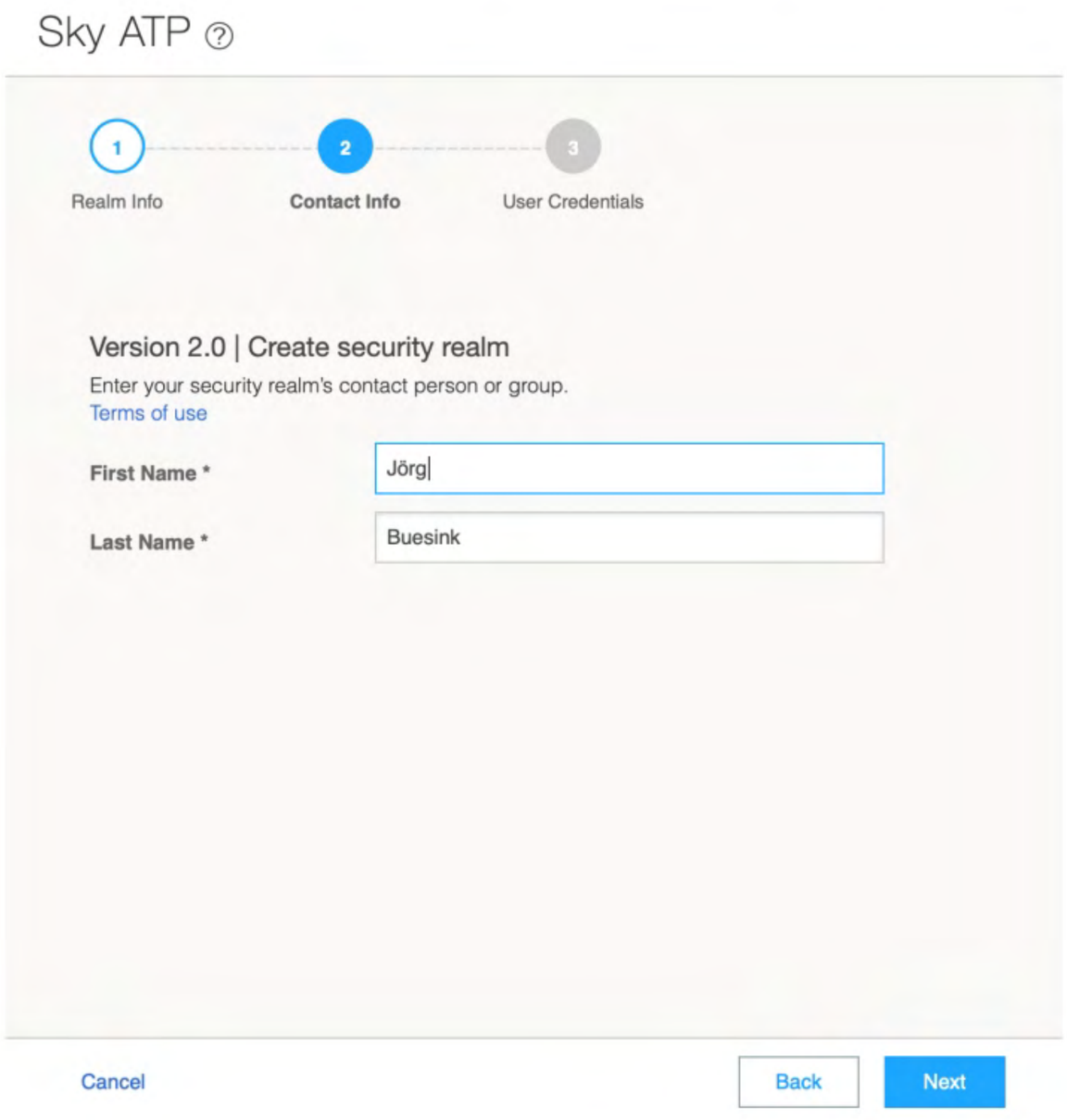
© 2020 Juniper Networks, Inc. All rights reserved.

c) Enter the Security Realm Name as provided with your lab access instructions. In this case the Security Realm Name: jnciesec-001 is used. Also specify the company name and click the “Next” button.



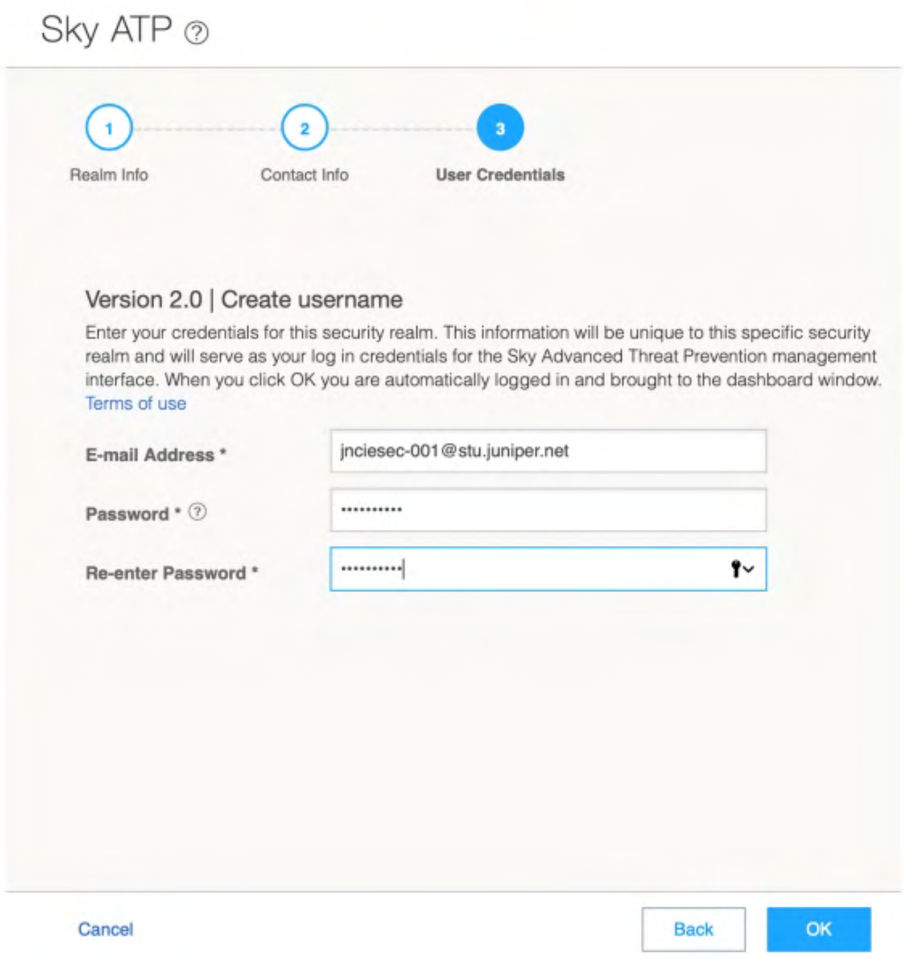
© 2020 Juniper Networks, Inc. All rights reserved.

d) Enter your first and last name and click the “Next” button.

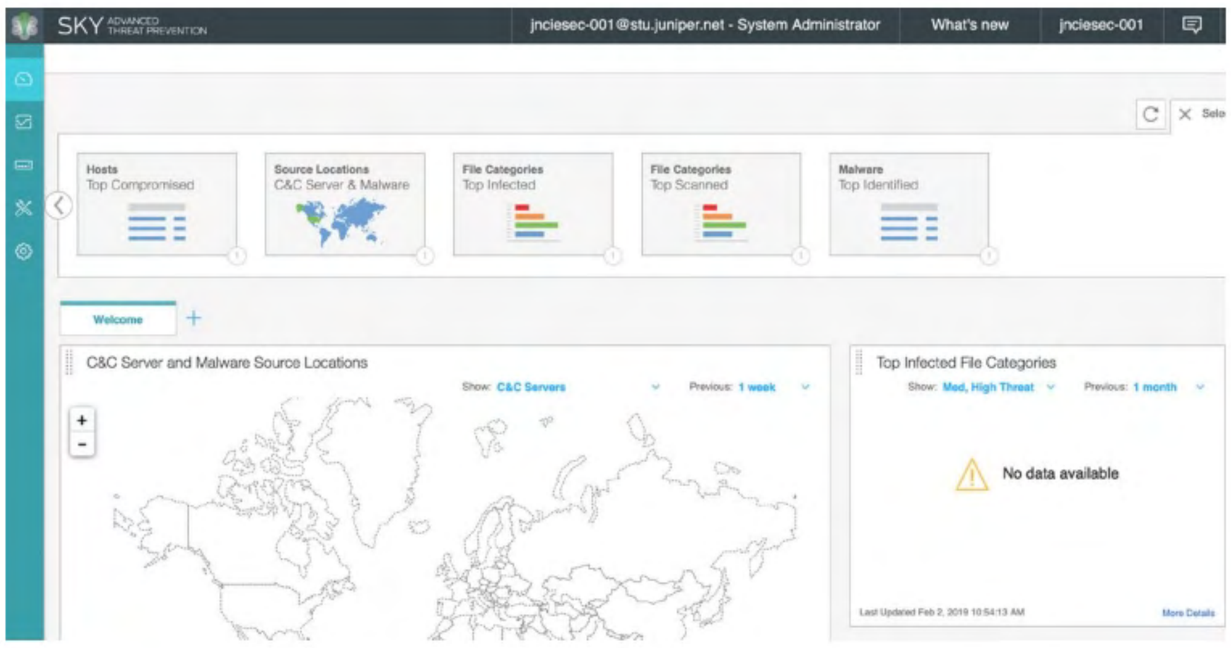


© 2020 Juniper Networks, Inc. All rights reserved.

e) Specify the user credentials to be used to login to the Sky ATP realm. In this case the email address: jnciesec-001@stu.juniper.net is used with password lab123@Lab. Make sure you use the credentials provided as mentioned in the lab access instructions. Press the “Ok” button.

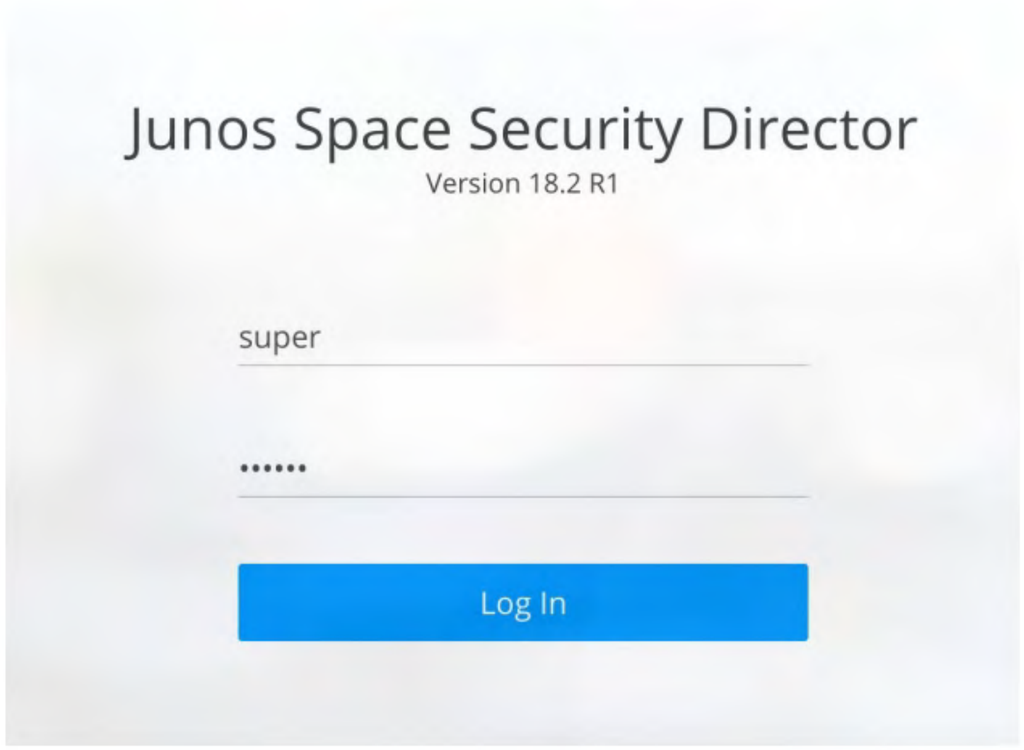


f) If you completed all steps correctly the SkyATP realm is created and you will auto login to the Sky ATP realm. At the top of the screen you should see your Sky ATP email address and the Sky ATP realm name. You can now close the Firefox browser as we will use Security Director to enroll the required devices.



© 2020 Juniper Networks, Inc. All rights reserved.

g) Access Security Director using the GUI interface and enter the login credentials as provided in your lab access instructions.



h) Navigate to the Devices / Device Discovery workspace. Create a new discovery job to discover the SRX devices and vQFX device (10.10.1.1 – 10.10.1.10) as the following screenshots show. Note that vQFX is located between cluster 2 (srx5/srx6) and its internal hosts. Note that if the discovery job fails for any reason, run it again until all the devices are in the managed state.
    a) Job Name: jncie-sec
    b) IP Address Range: 10.10.1.1 – 10.10.1.10
    c) Probes:
        i. Use NAT: unchecked
        ii. Use Ping: checked
        iii. Use SNMP: unchecked
    d) Credentials
        i. Username: lab
        ii. Password: lab123
    e) Schedule Discovery Job
        i. Type: Run now
        ii. Import and Publish Policies: unchecked

© 2020 Juniper Networks, Inc. All rights reserved.

Create Device Discovery Profile

Add Device Discovery Target — Specify Probes — Specify Credentials — Specify Device Fingerprint — Schedule Discovery Job

Add Device Discovery Target

Discovery Profile Name* : jncie-sec

Discovery Parameters : Add Manually / Import From CSV File — Sample CSV File

Target Type* : IP Address / IP Range / IP Subnet / Hostname

Target Details

Start IP Address* : 10.10.1.1

End IP Address* : 10.10.1.10

Cancel — Next

Create Device Discovery Profile

Add Device Discovery Target — Specify Probes — Specify Credentials — Specify Device Fingerprint — Schedule Discovery Job

Specify Probes

Use NAT : Enable

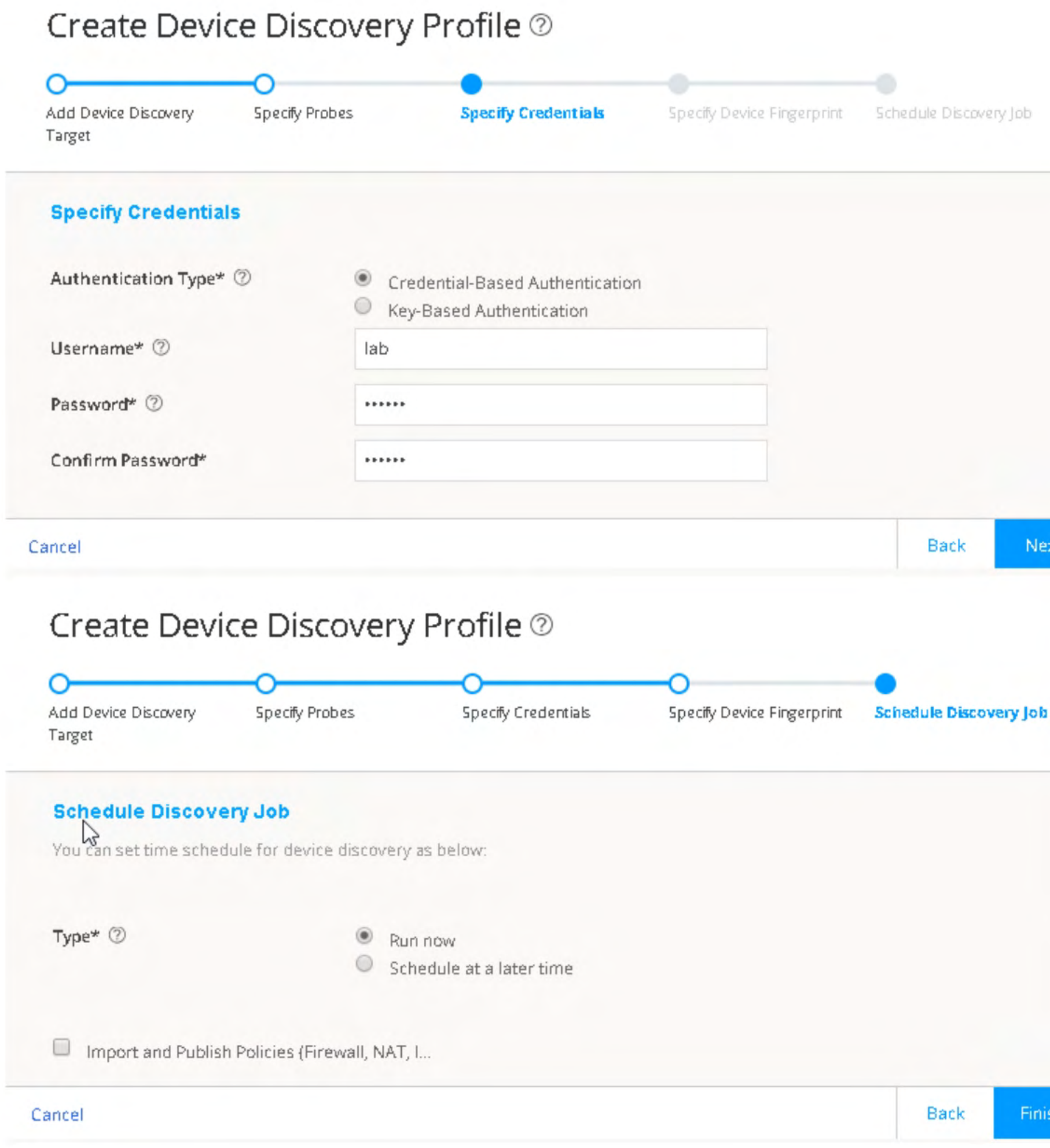
Use Ping : Enable

Use SNMP : Enable

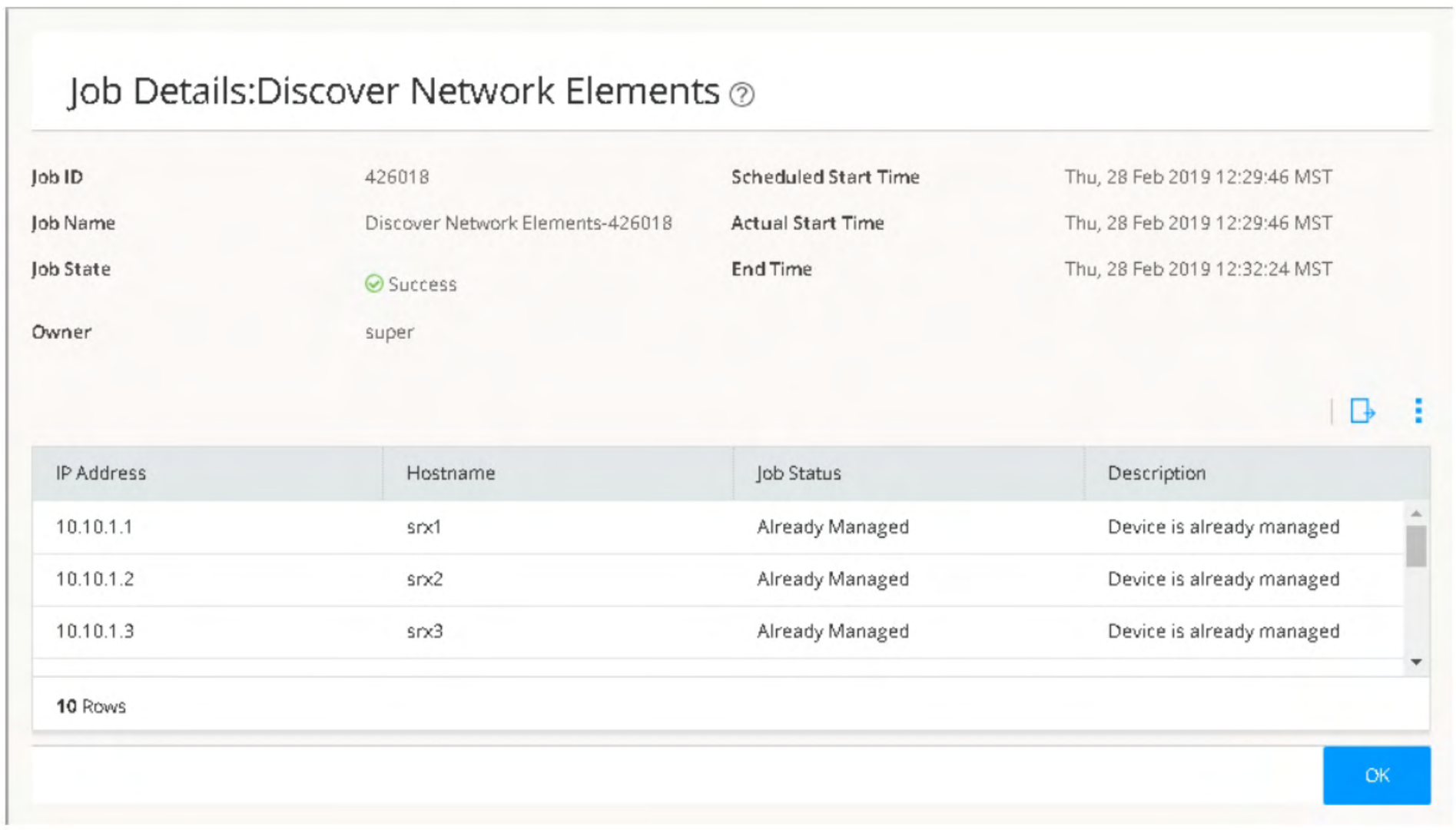
Warning: If SNMP is disabled, the Network Monitoring functionality will be limited. To enable SNMP settings later, you must go to the Network Monitoring workspace in Junos Space Network Management Platform.

Cancel — Back — Next

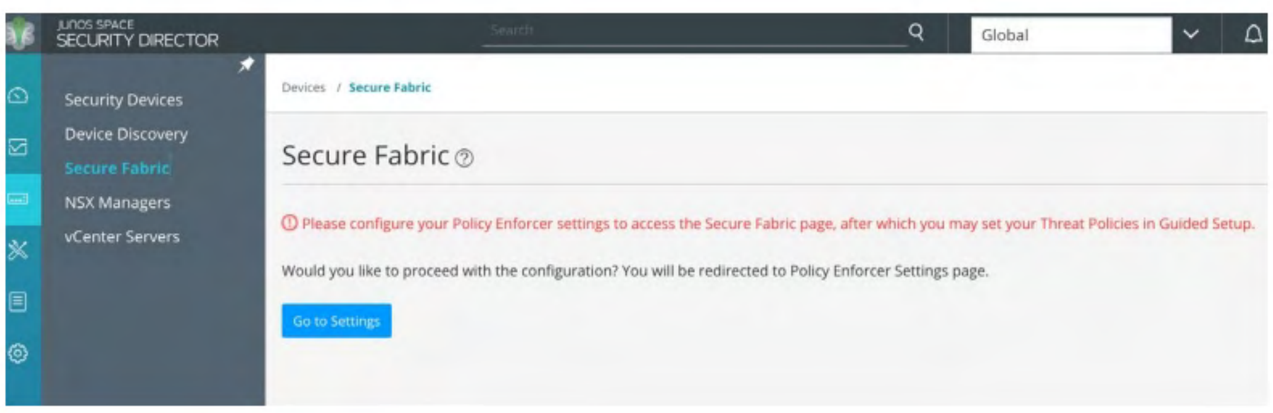
© 2020 Juniper Networks, Inc. All rights reserved.



© 2020 Juniper Networks, Inc. All rights reserved.



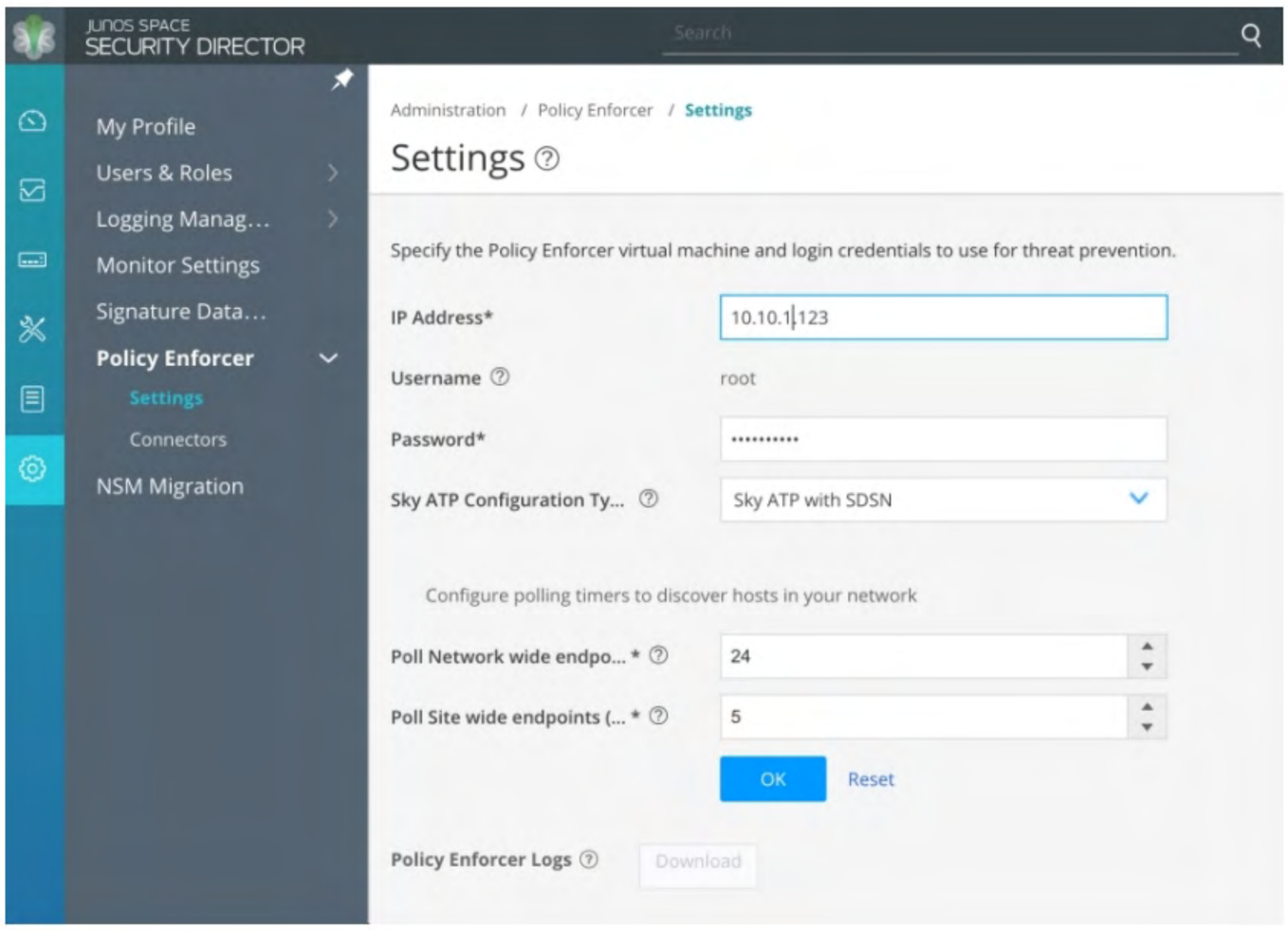
i) Navigate to Devices / Secure Fabric. Security Director gives a notification that we first need to configure Policy Enforcer to access the Secure Fabric Page.



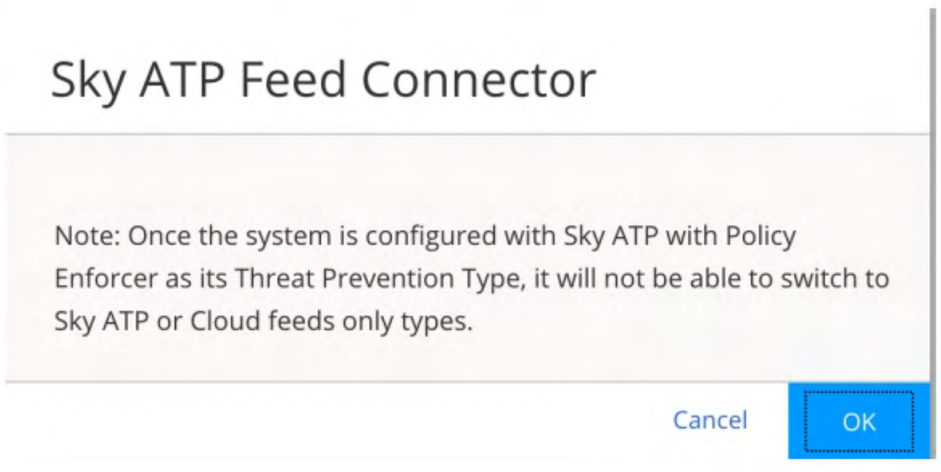
© 2020 Juniper Networks, Inc. All rights reserved.

j) Navigate to Administration / Policy Enforcer / Settings. Enter the IP address, username and password of Policy Enforcer as mentioned in your lab access instructions.

Make sure to select “Sky ATP with SDSN” as the Sky ATP configuration type and click the “OK” button.

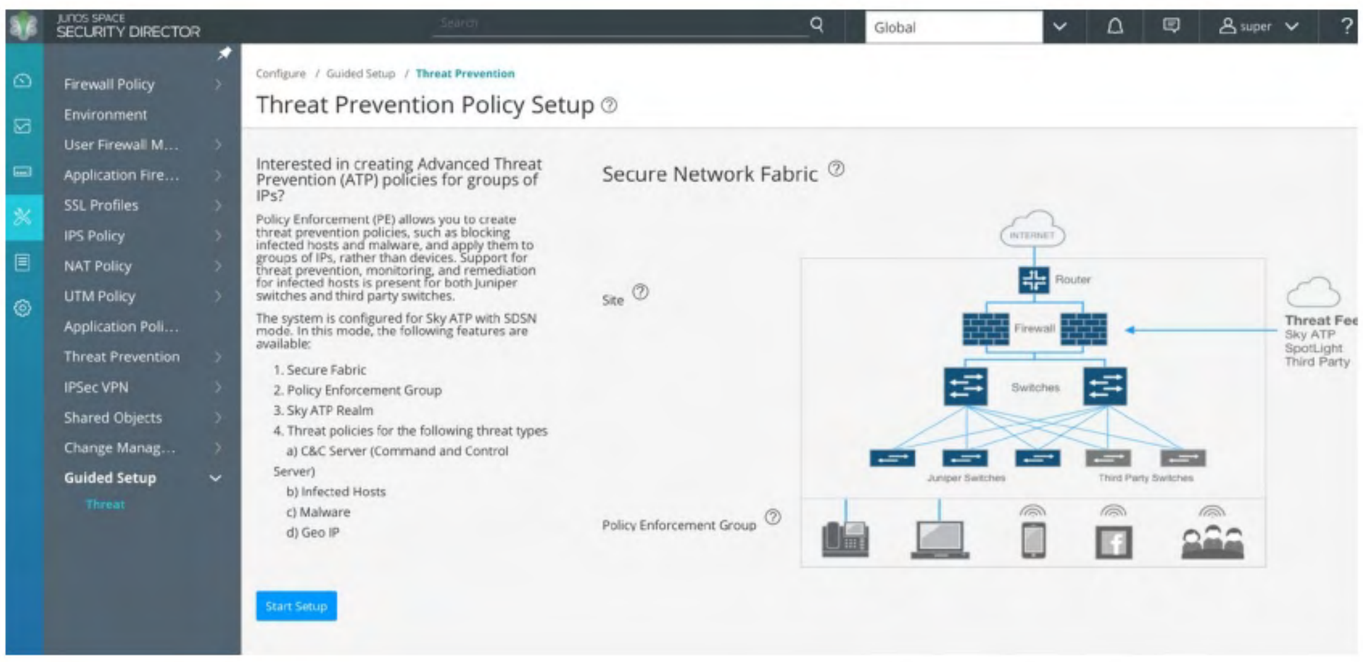


k) You should receive the following notification. Click the “ok” button to proceed.

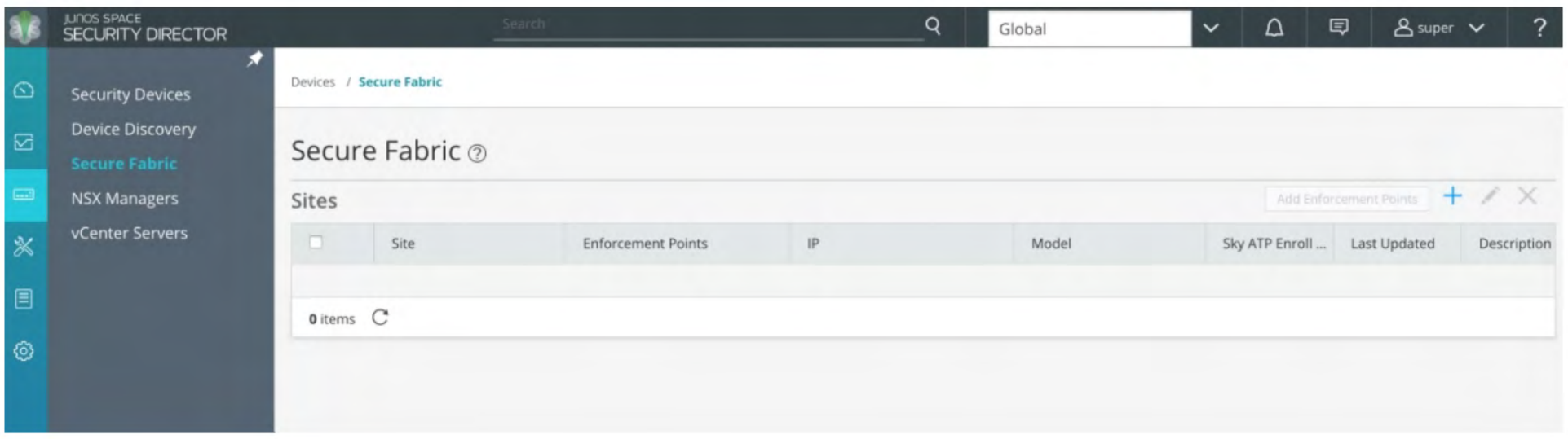


© 2020 Juniper Networks, Inc. All rights reserved.

l) Once Policy Enforcer is registered you are redirected to the “Threat Prevention Policy Setup” guided setup. At this stage we are not creating a Threat Prevention Policy yet as the task requirement is to enroll Policy Enforcer and the required security devices.

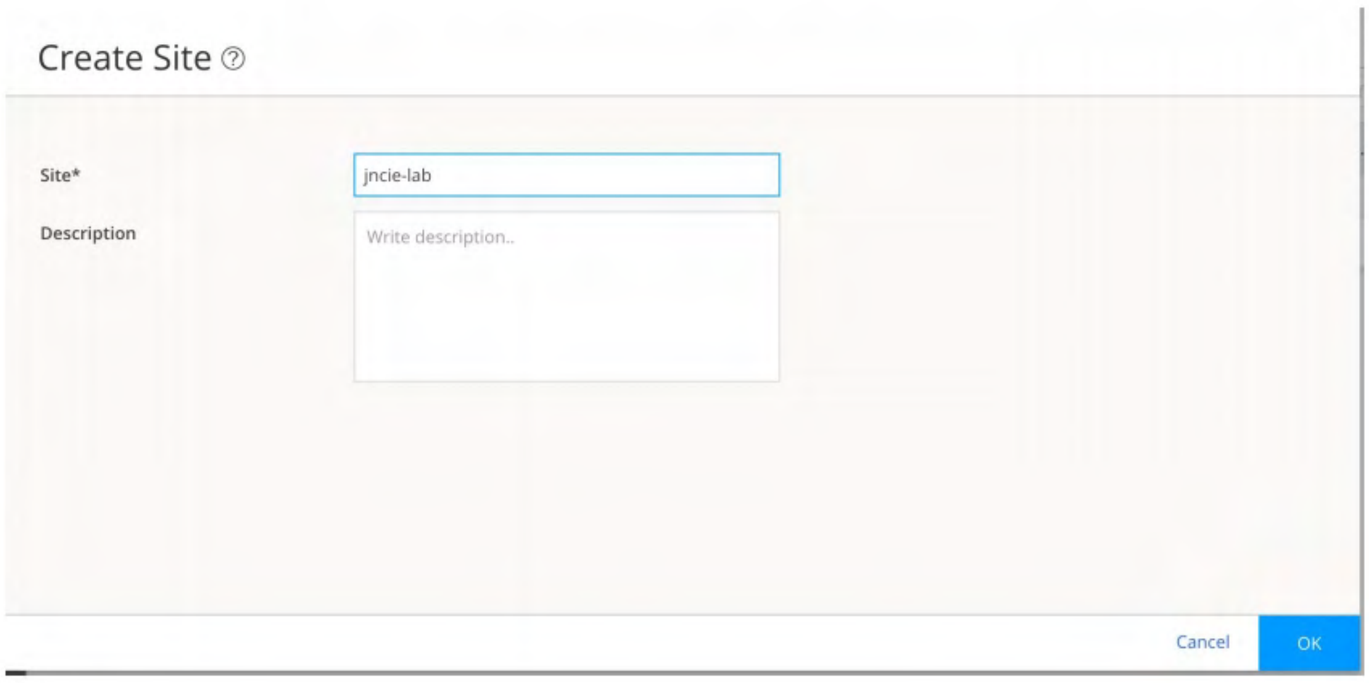


m) Navigate in the left vertical menu to “Devices” and select “Secure Fabric”. You need to define a “Site” and add “Enforcement points” to the site.

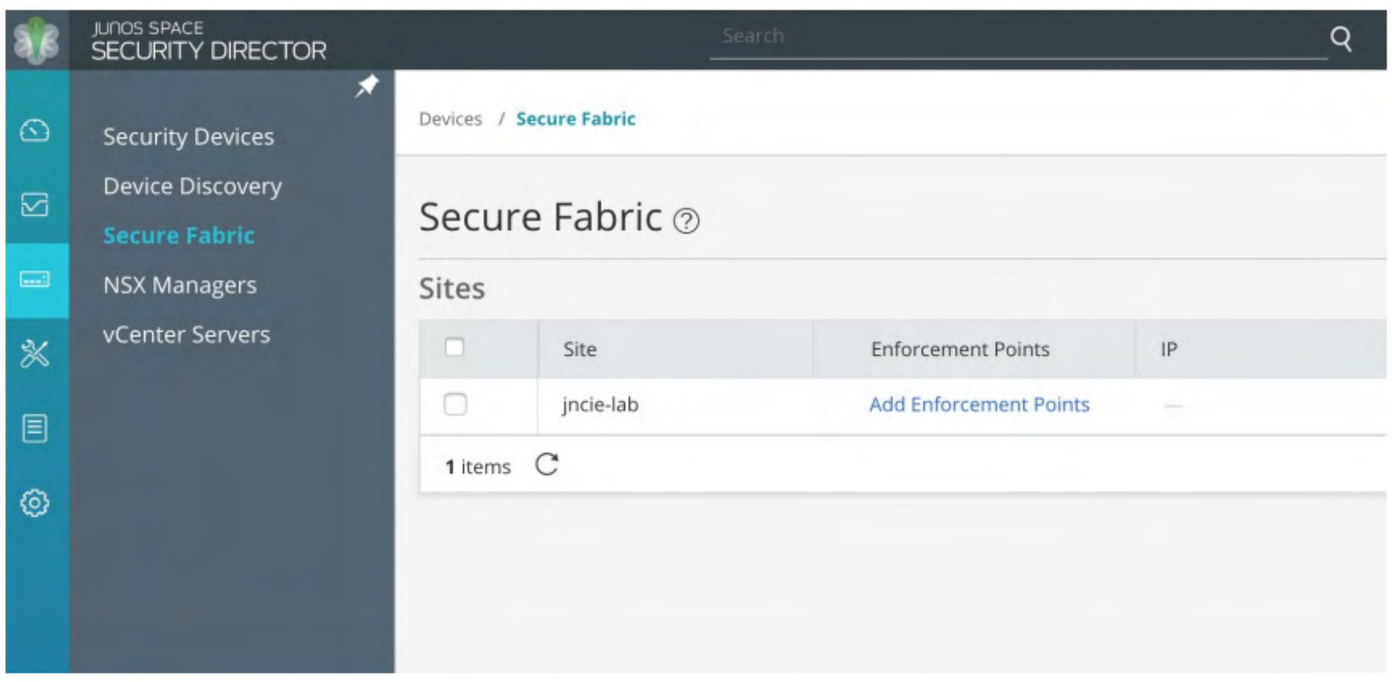


© 2020 Juniper Networks, Inc. All rights reserved.

n) Create a site and specific a Site name. In this case we call the Site “jncie-lab”. Click on the “Ok” button to proceed.

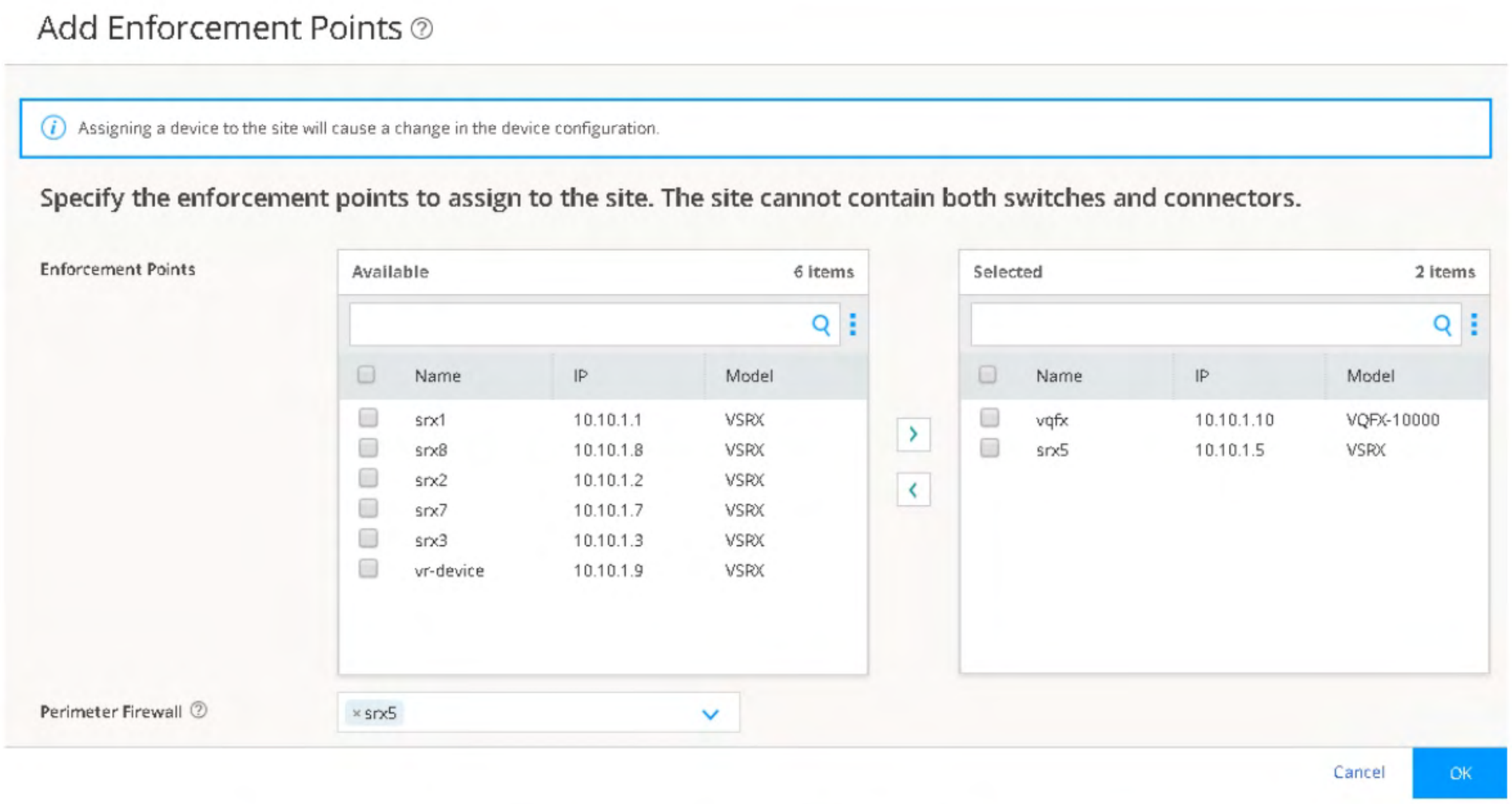


o) Now select “Add Enforcement Points” to add the cluster 2 node and the vQFX device to the Secure Fabric.

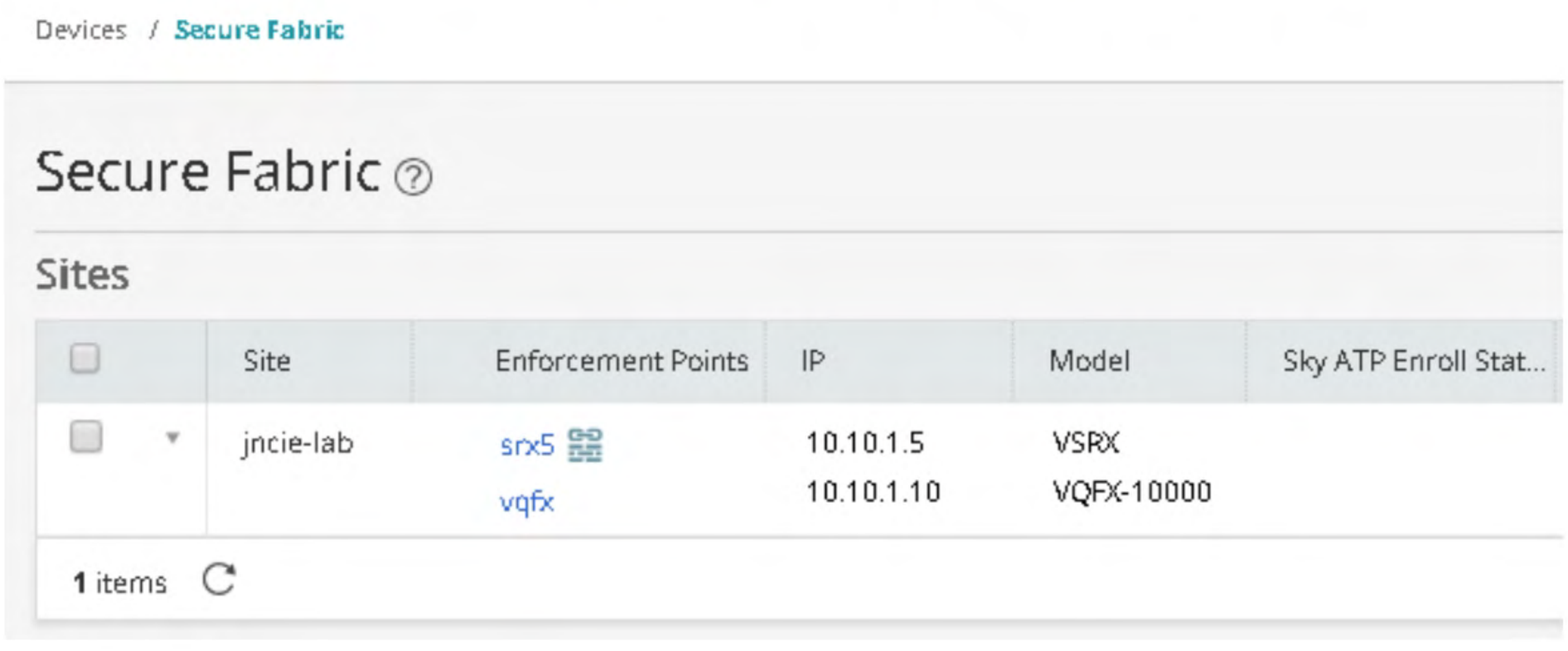


© 2020 Juniper Networks, Inc. All rights reserved.

p) Select the cluster 2 primary (srx5) and the vQFX device as an enforcement point and click the “ok” button.



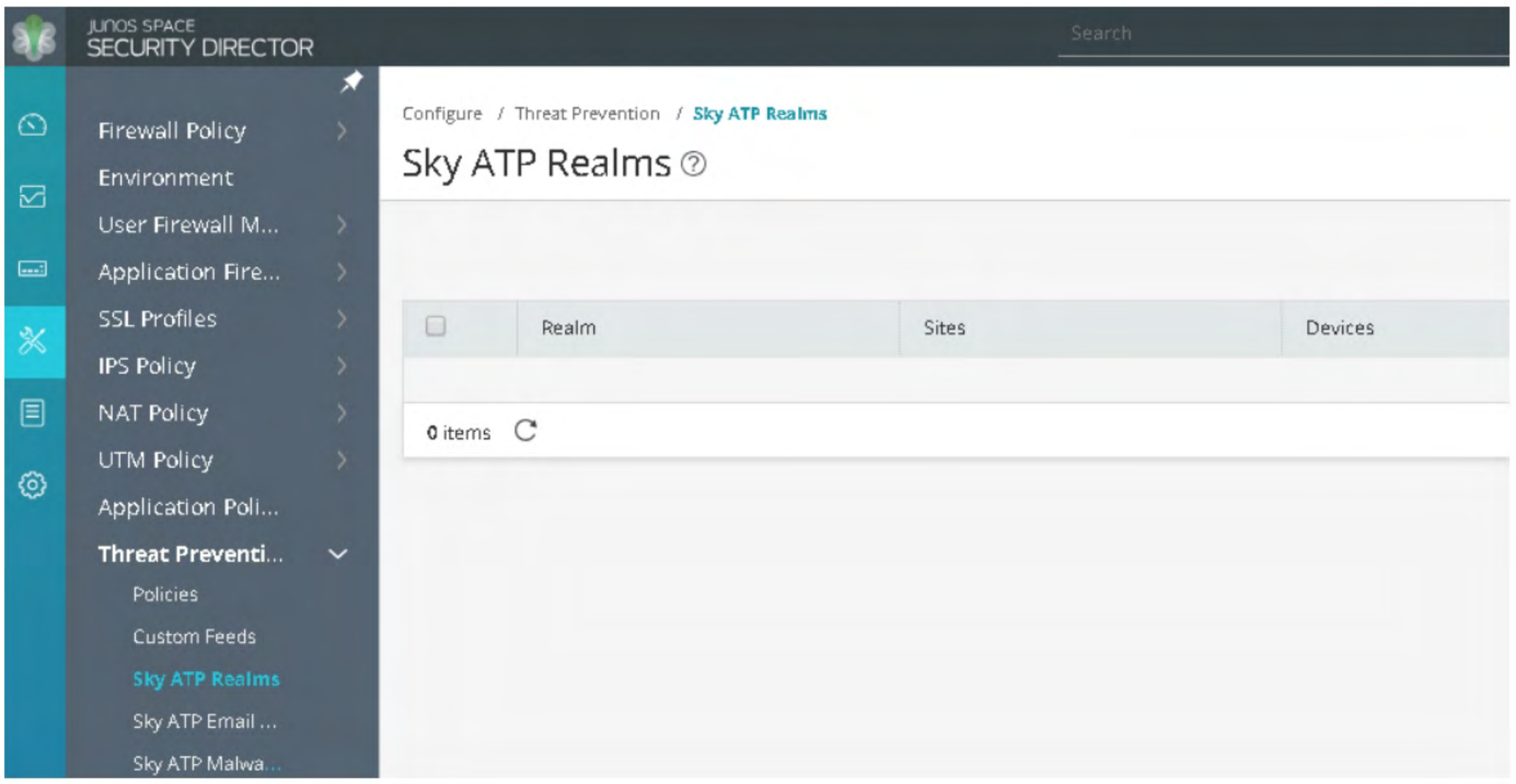
q) Now the cluster 2 device (srx5/srx6) and the vQFX device should be added as an enforcement point to the Secure Fabric for Site “jncie-lab”.



© 2020 Juniper Networks, Inc. All rights reserved.

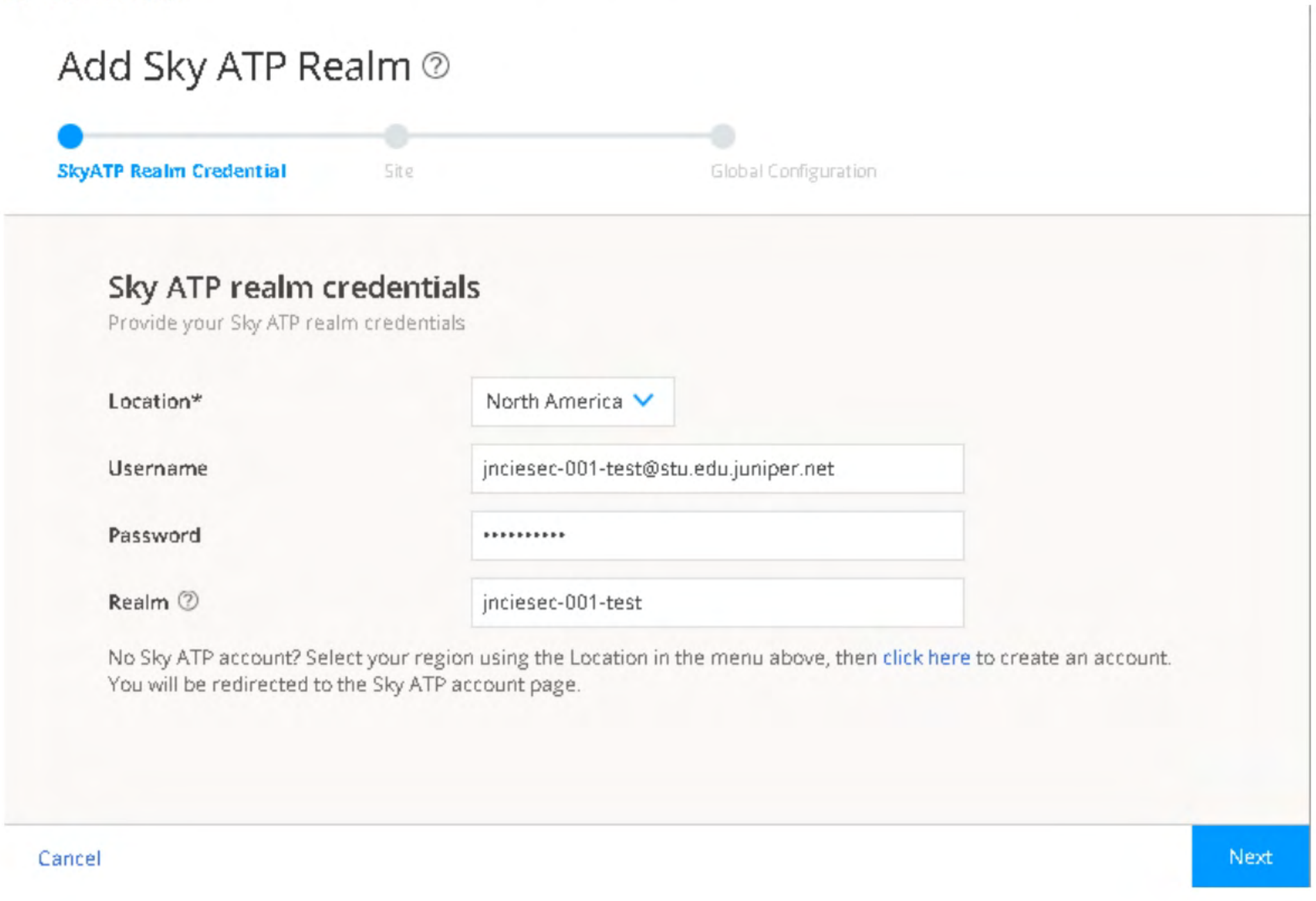
2) Setup for SkyATP with SDSN in Security Director, ensure that HTTP and SMTP traffic is analyzed at cluster 2 (srx5/srx6) for threat levels 7 or above for the 172.16.50.100 host. Ensure that connections are silently dropped at access switch vQFX if the 172.16.50.100 host becomes infected with malware. Ensure that only blocked traffic is logged.

   a. Navigate to the Configure / Threat Prevention / Sky ATP Realms workspace.



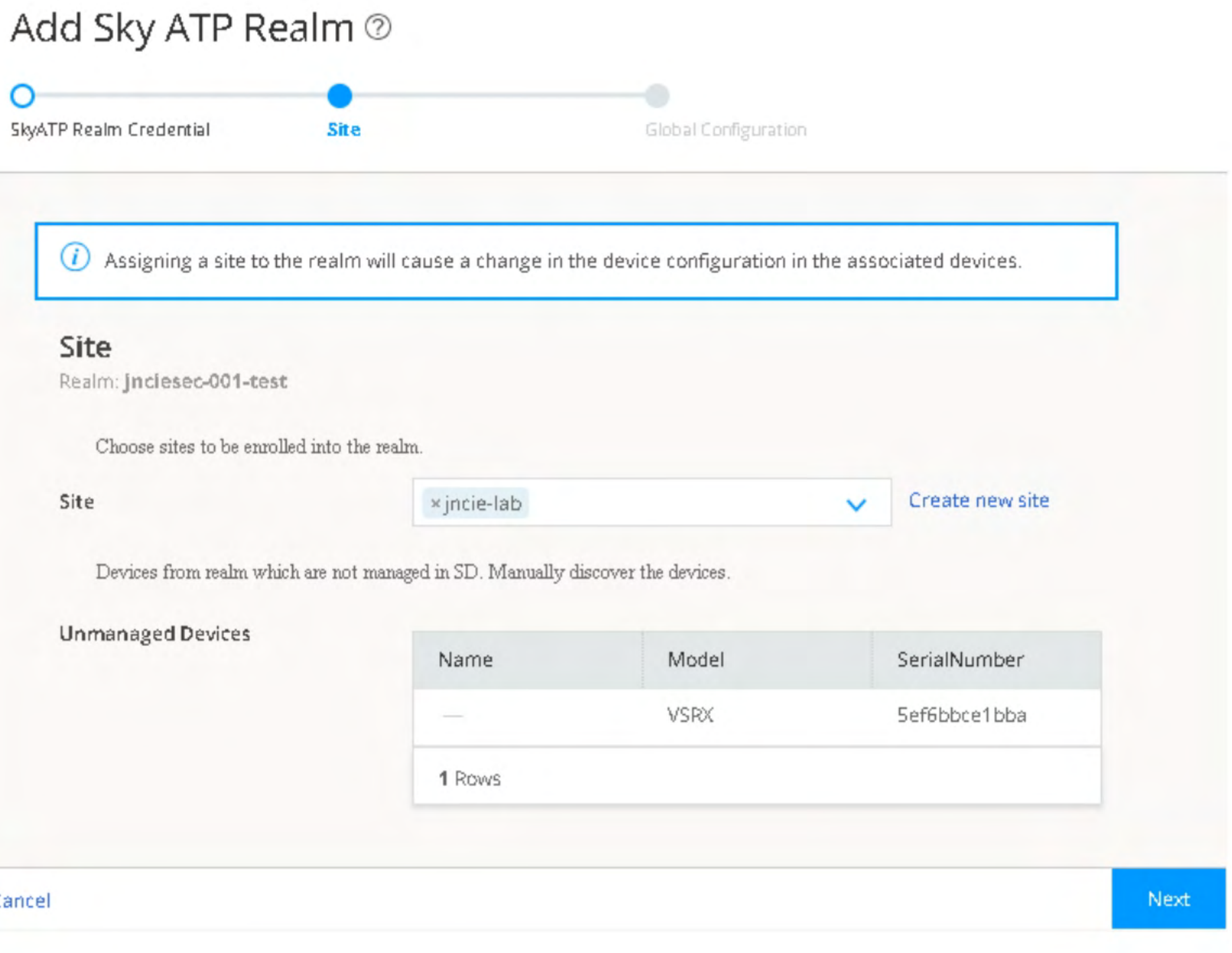
© 2020 Juniper Networks, Inc. All rights reserved.

b. Click the create button and enter your Sky ATP realm credentials. Click Next to continue.



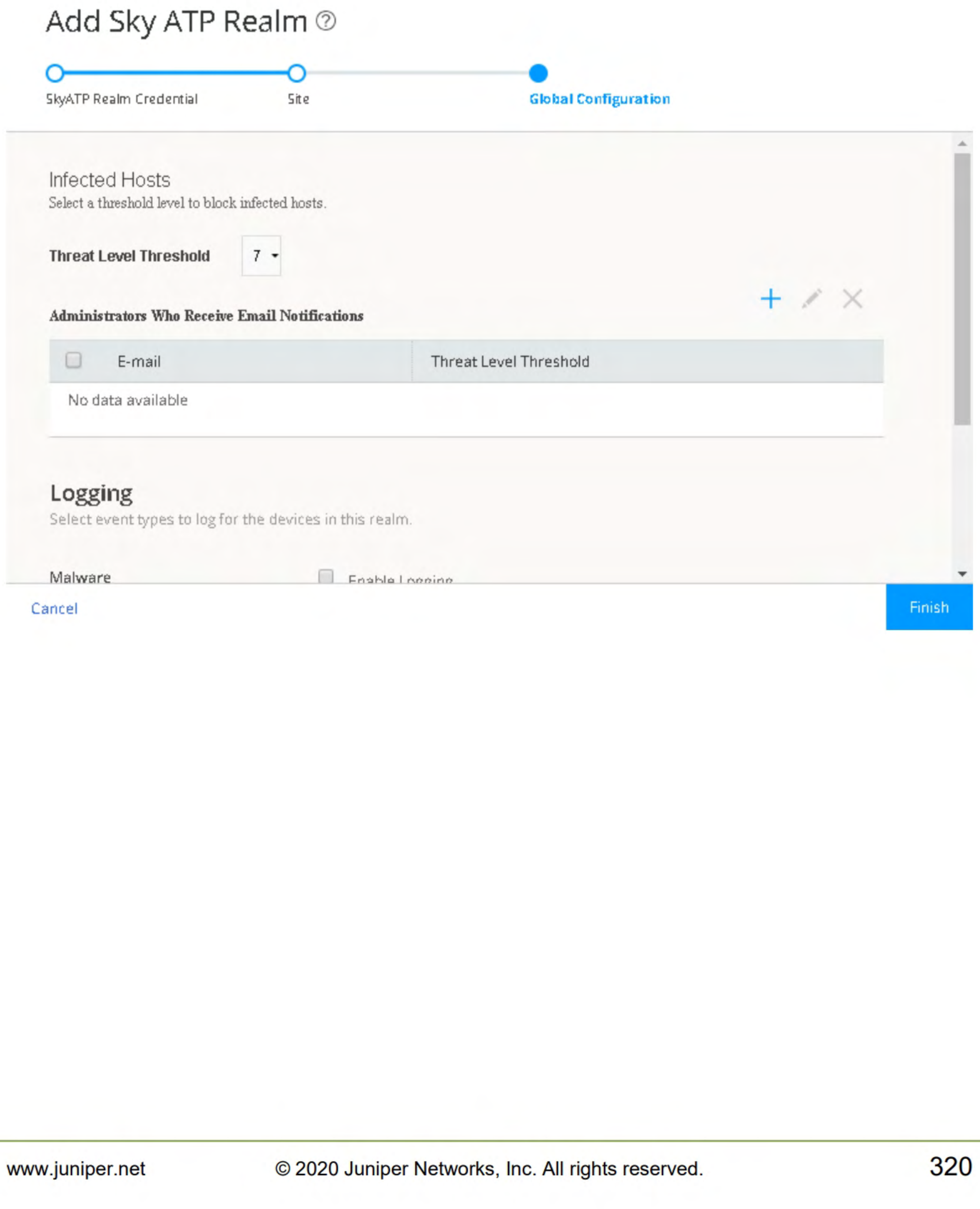
© 2020 Juniper Networks, Inc. All rights reserved.

c. Select your SDSN site and click next.



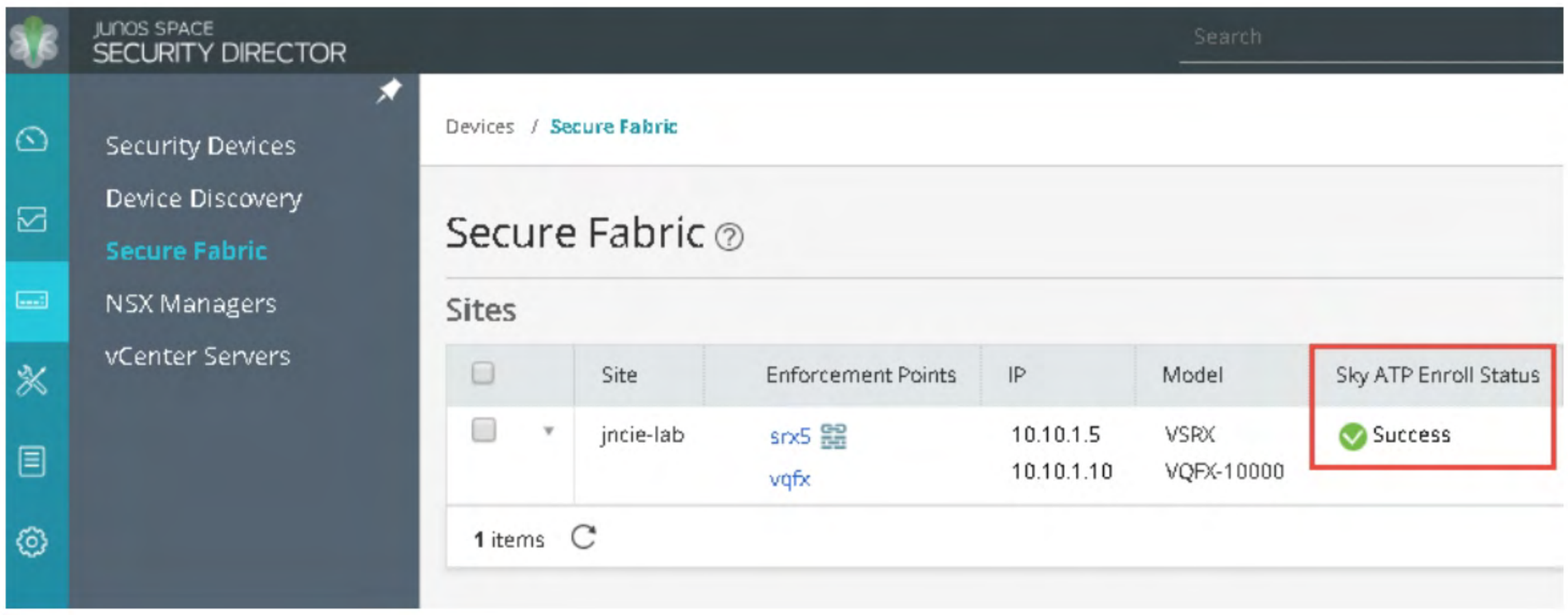
© 2020 Juniper Networks, Inc. All rights reserved.

d. Leave everything at the defaults for the Global Configuration page and click Finish.



© 2020 Juniper Networks, Inc. All rights reserved.

e. Navigate to the Devices / Secure Fabric workspace. Ensure that the srx5 device Sky ATP enrolment status is successful. Note if the status shows Pending then you should wait 5 minutes and refresh the page.



f. Create a policy enforcement group for the 172.16.50.100 host. Ensure that connections are silently dropped if the threat is identified. Ensure that only blocked traffic is logged.

   i. Navigate to the Configure / Shared Objects / Policy Enforcement Groups workspace. Create a new PEG and add the new 172.16.50.100 IP address

© 2020 Juniper Networks, Inc. All rights reserved.

Policy Enforcement Group

Name* JNCIE-PEG

Description

Group Type IP Address / Subnet

Connector IPs/subnets

Available 4 items

Subnets	Source	Model
80.10.1.1/24	srx5	space
172.16.60.10/24	srx5	space
172.16.55.10/24	srx5	space
172.16.50.10/24	srx5	space

Selected 0 items

Subnets	Source	Model

Refresh Available subnets

Additional IP 172.16.50.100 Space Add

Cancel OK

Policy Enforcement Group

Name* JNCIE-PEG

Description

Group Type IP Address / Subnet

Connector IPs/subnets

Available 4 items

Subnets	Source	Model
80.10.1.1/24	srx5	space
172.16.60.10/24	srx5	space
172.16.55.10/24	srx5	space
172.16.50.10/24	srx5	space

Selected 1 items

Subnets	Source	Model
172.16.50.100	space	space

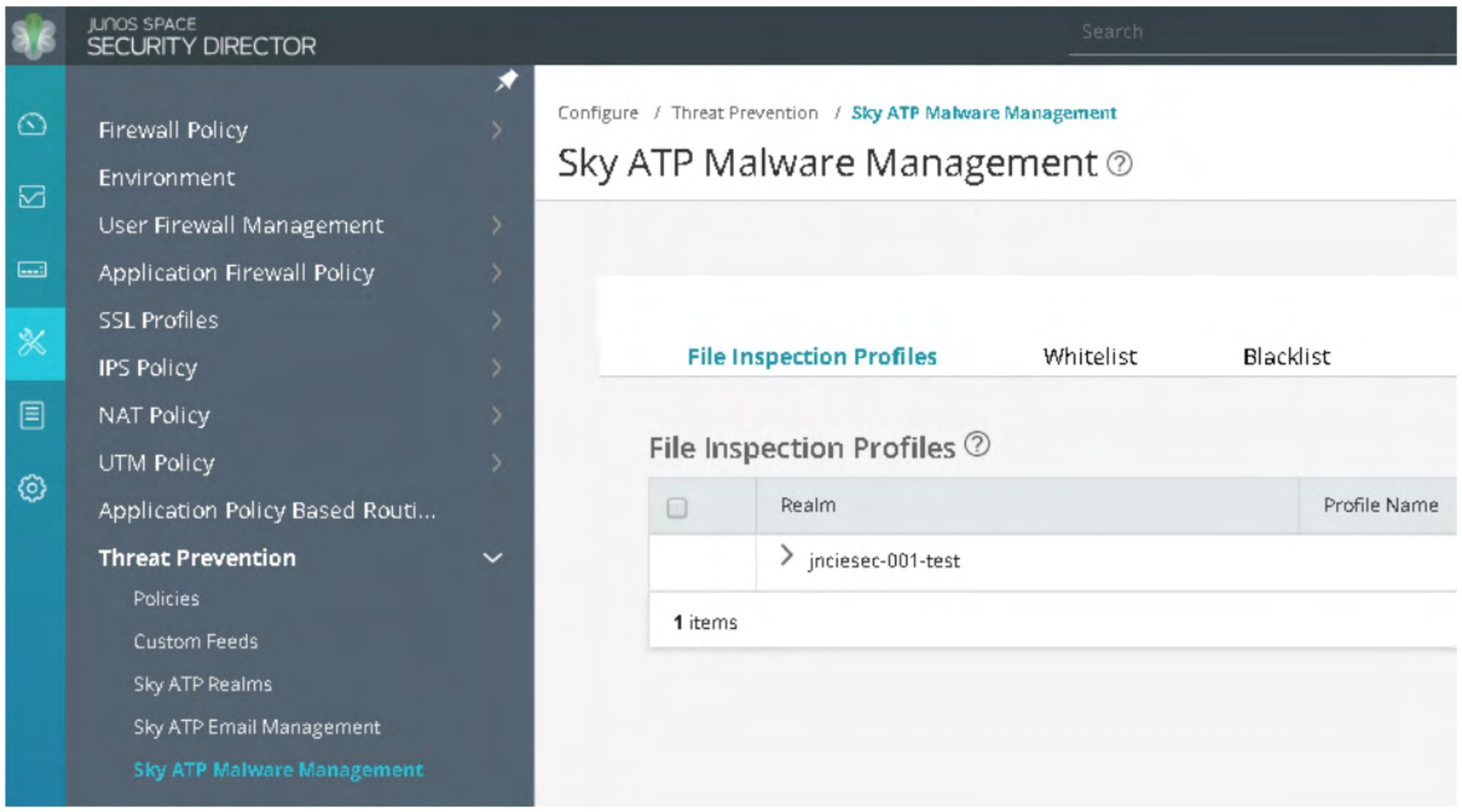
Refresh Available subnets

Additional IP Space Add

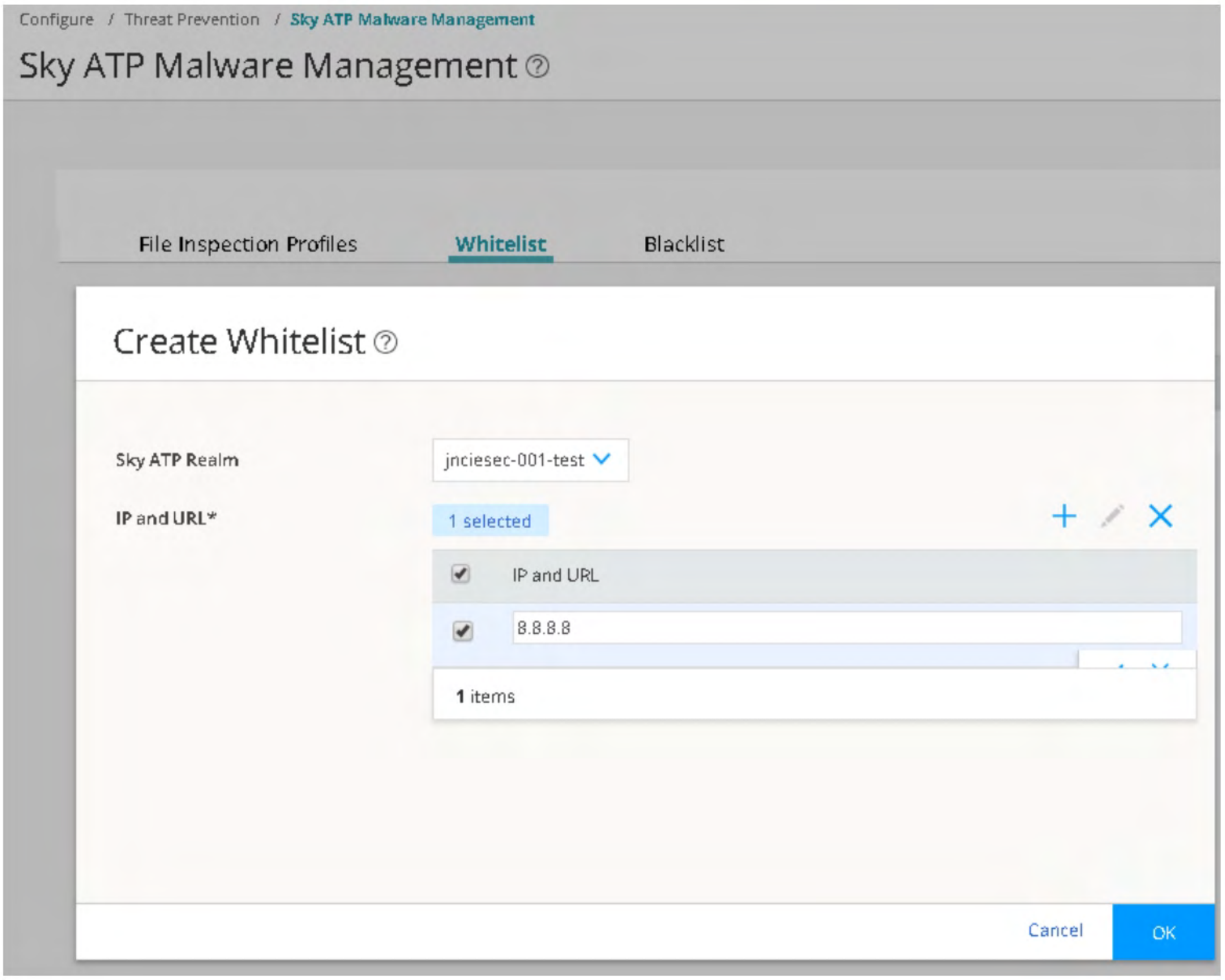
Cancel OK

© 2020 Juniper Networks, Inc. All rights reserved.

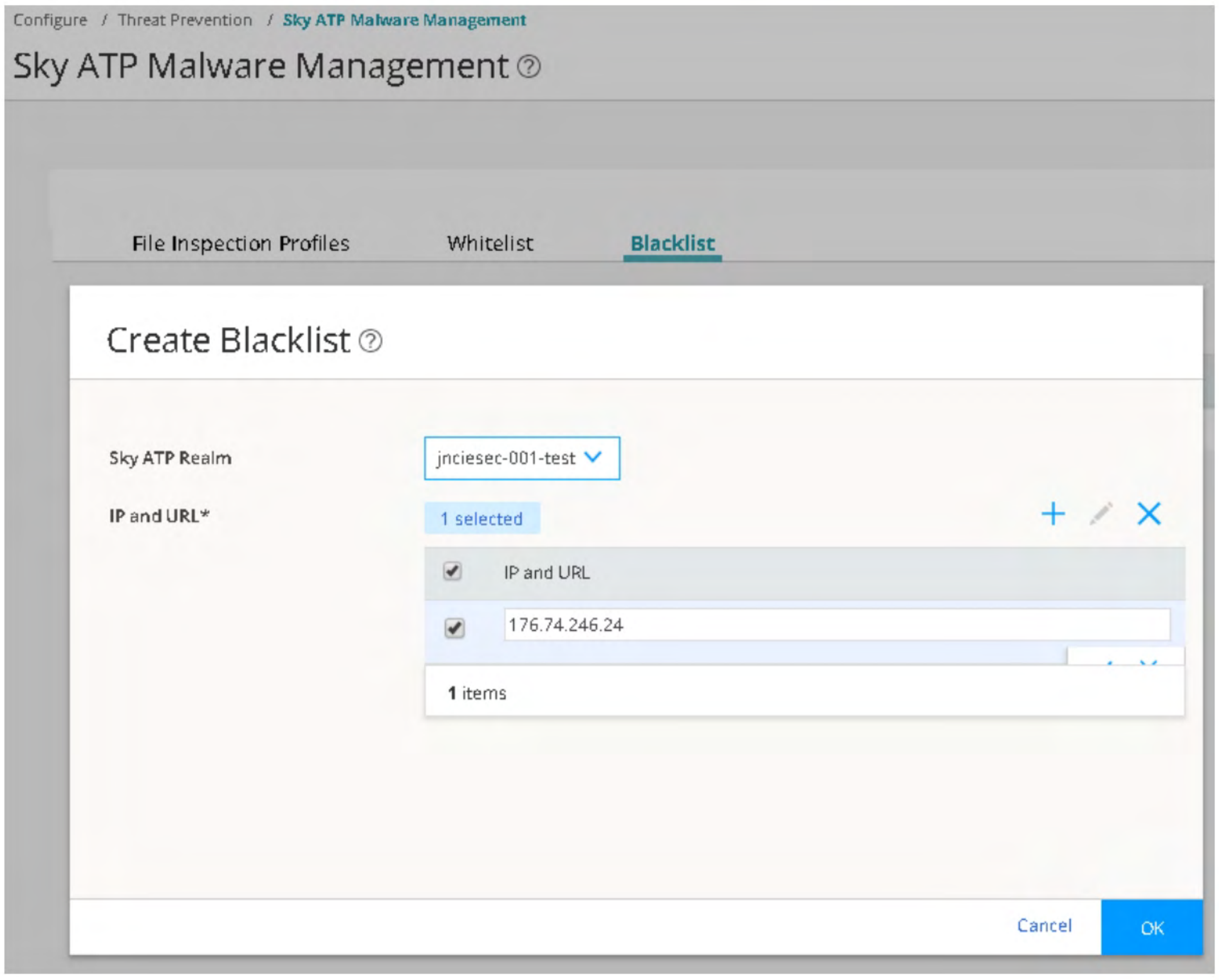
3) Ensure that content received from IP address “8.8.8.8” is never classified as Malware, however content from IP address “176.74.246.24” is always blocked.



© 2020 Juniper Networks, Inc. All rights reserved.

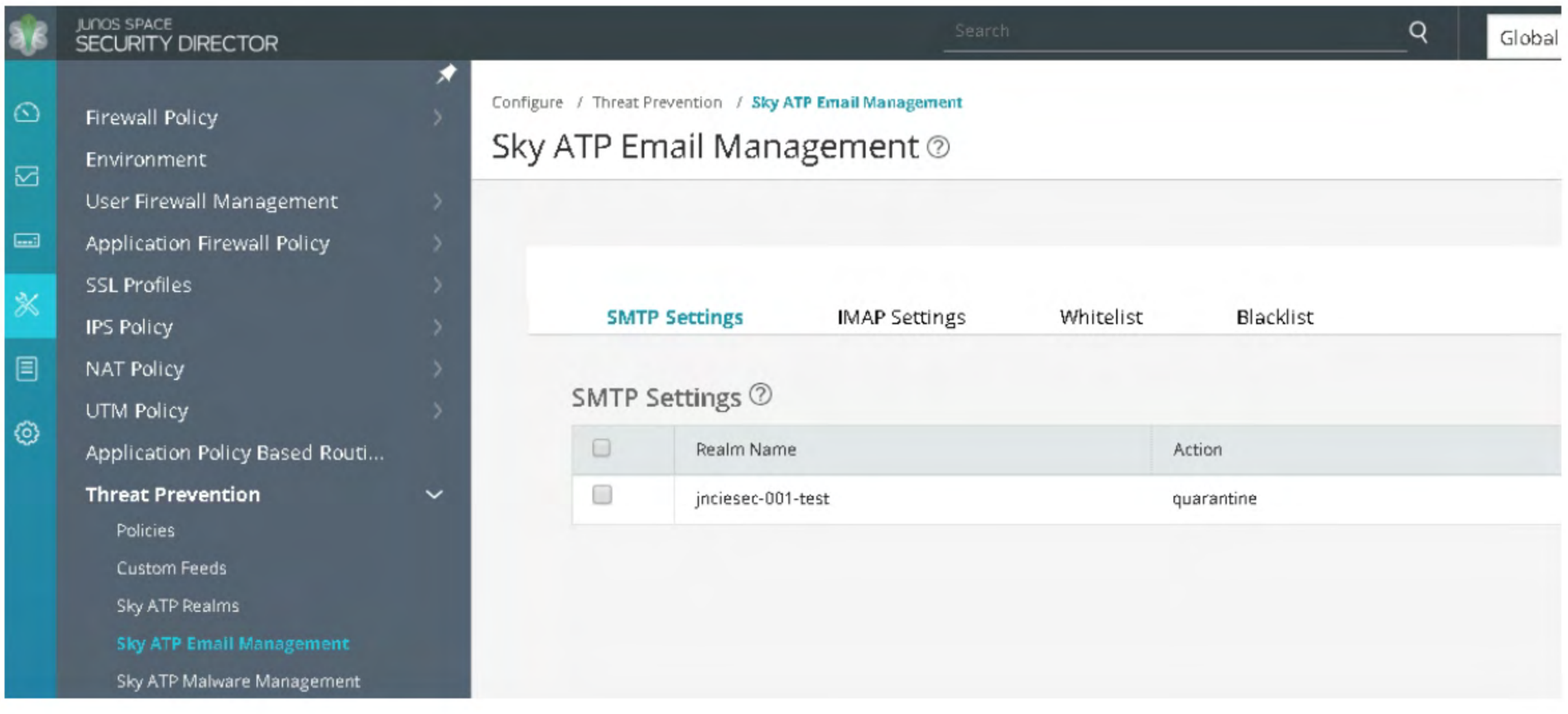


© 2020 Juniper Networks, Inc. All rights reserved.



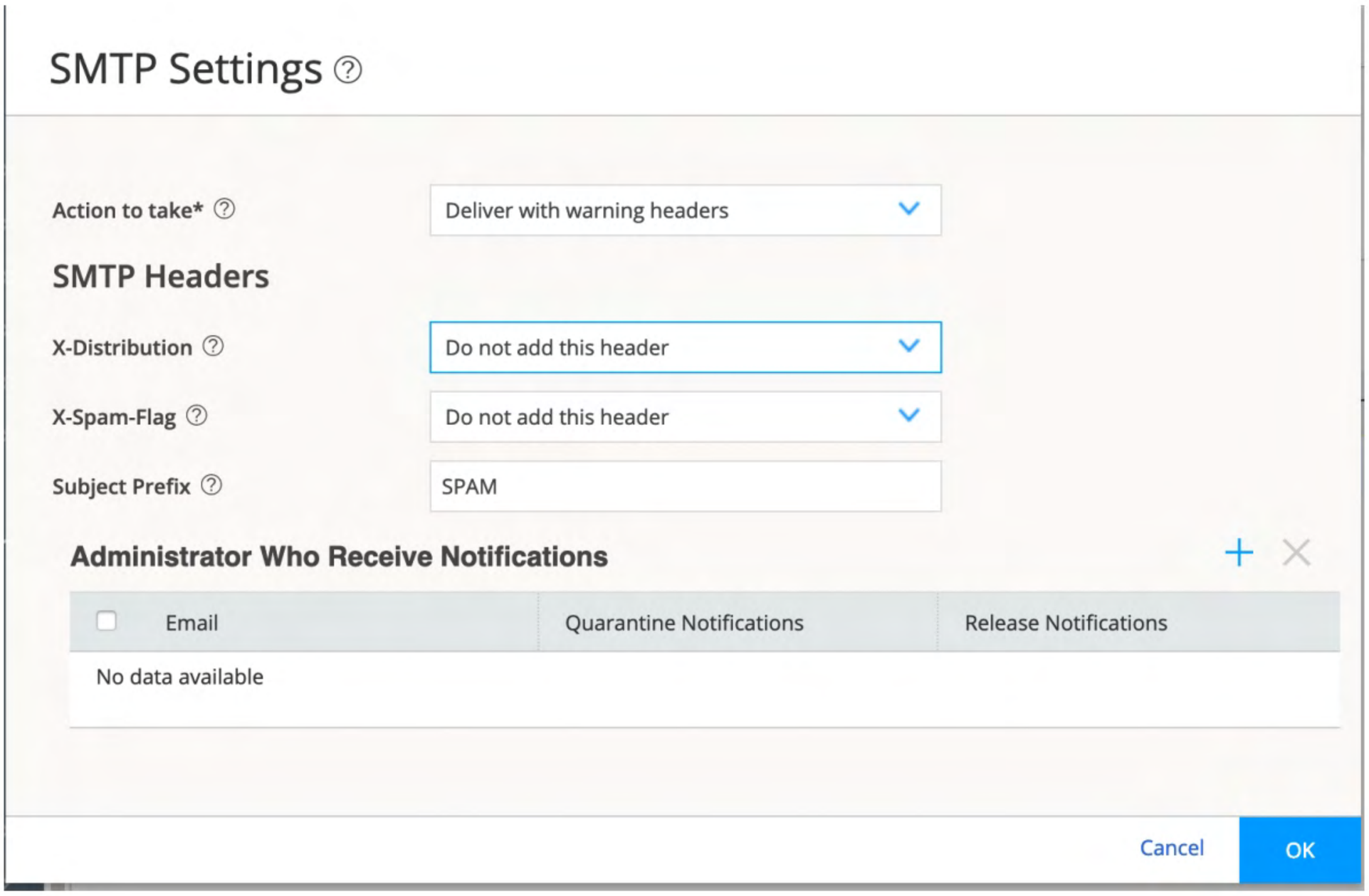
© 2020 Juniper Networks, Inc. All rights reserved.

4) Ensure that (suspicious) emails are sent to SkyATP for inspection. Suspicious emails should always be delivered with the email subject prepended with “SPAM”, however the email header should not be tagged with additional spam identifiers. Ensure that email received from no-reply@juniper.net are excluded from inspection.
    a) Navigate to “Threat Prevention” and select “Sky ATP Email Management”. Ensure that the SkyATP realm is activated for the SMTP settings tab. Note that by default the SMTP “action” is set to “quarantine”.



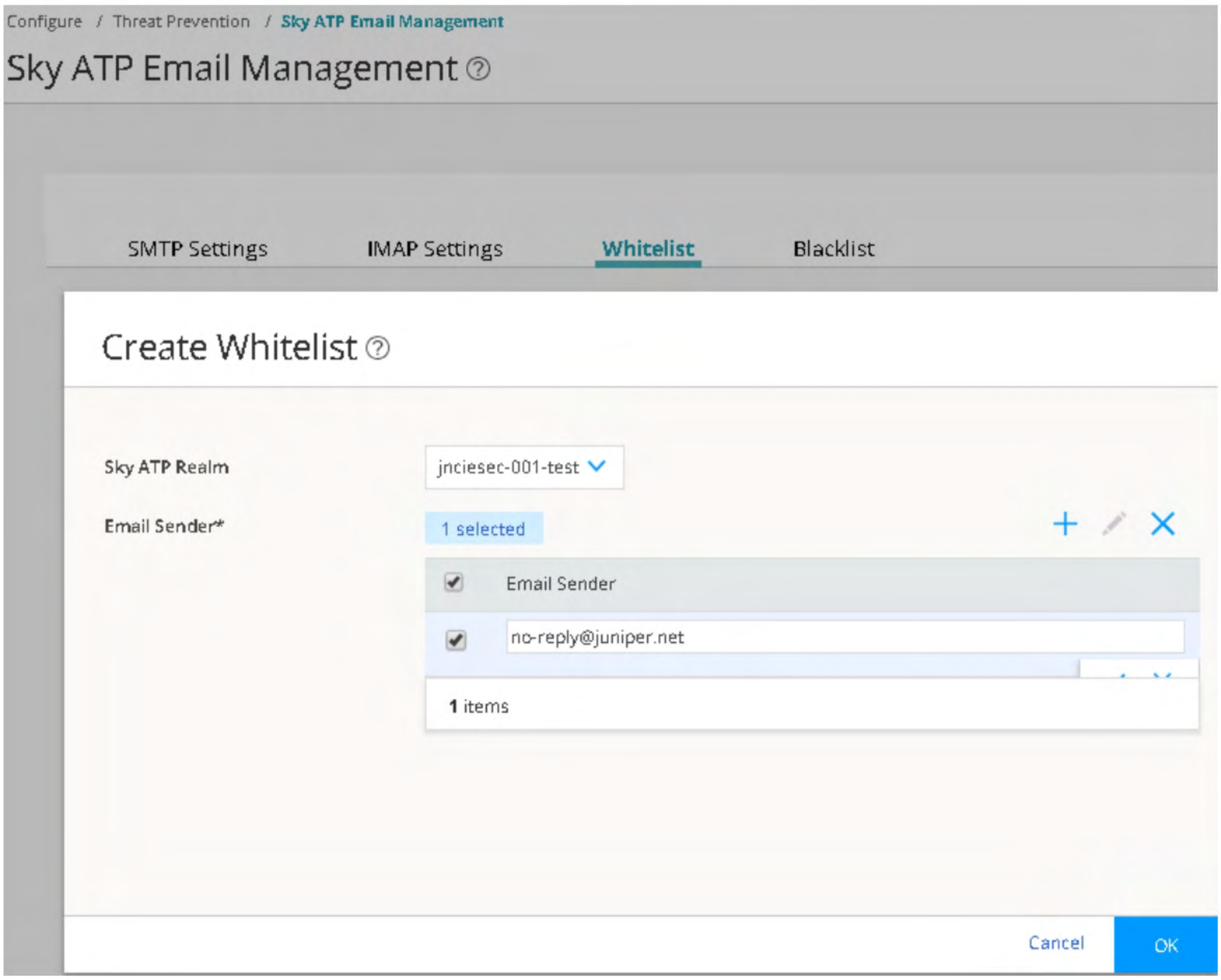
© 2020 Juniper Networks, Inc. All rights reserved.

b) Change the SMTP settings to meet the task requirements. The “action to take” must be set to Deliver with warning headers”. Make sure to disable “X-Distribution and X-Spam-Flag” to meet the task requirements that email headers should not be tagged with additional spam notifications. The email subject must be prepended with the word “SPAM” only.



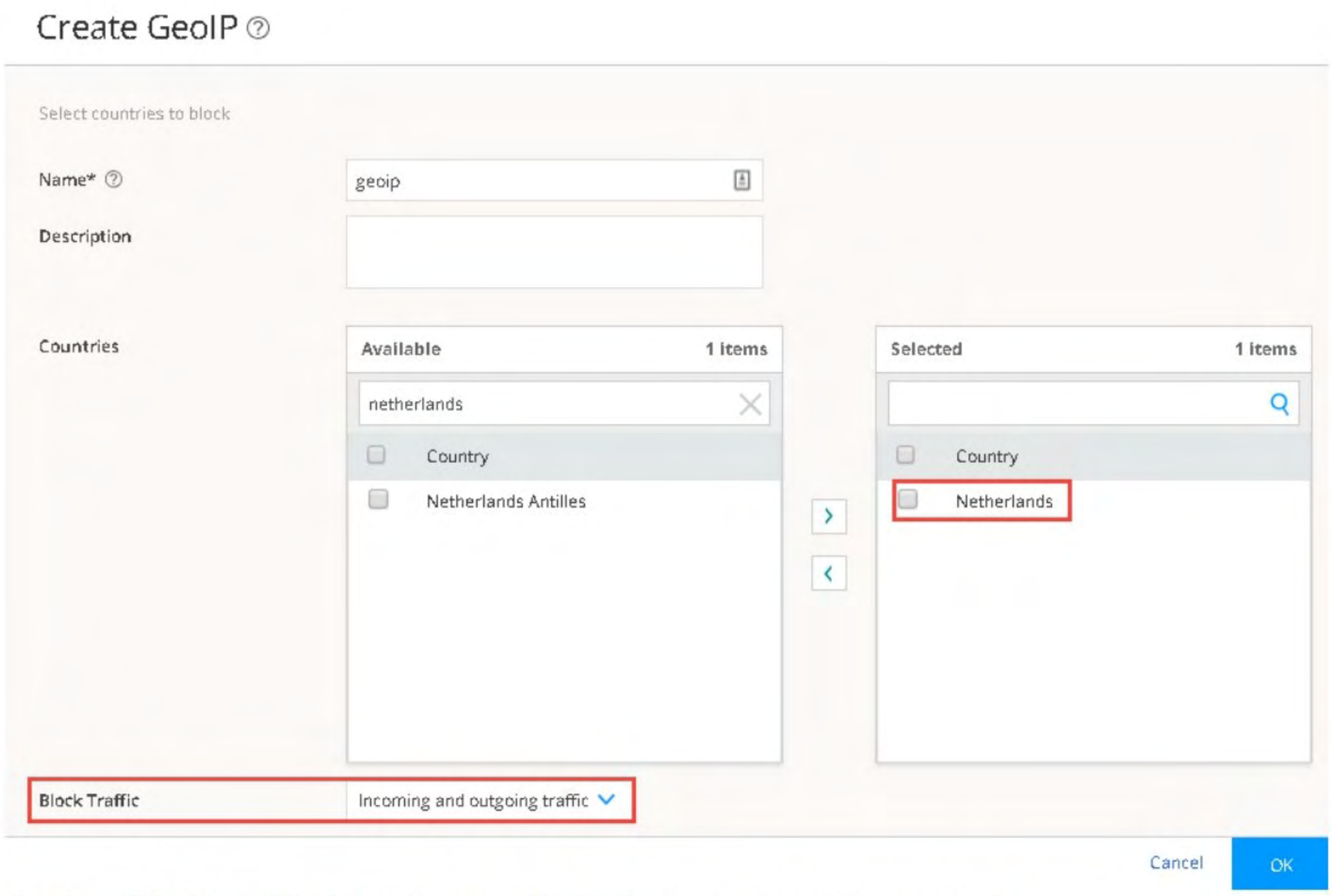
© 2020 Juniper Networks, Inc. All rights reserved.

c) Navigate to “Whitelist” and add no-reply@juniper.net to the whitelist. This ensures that emails received from no-reply@juniper.net are excluded for inspection.

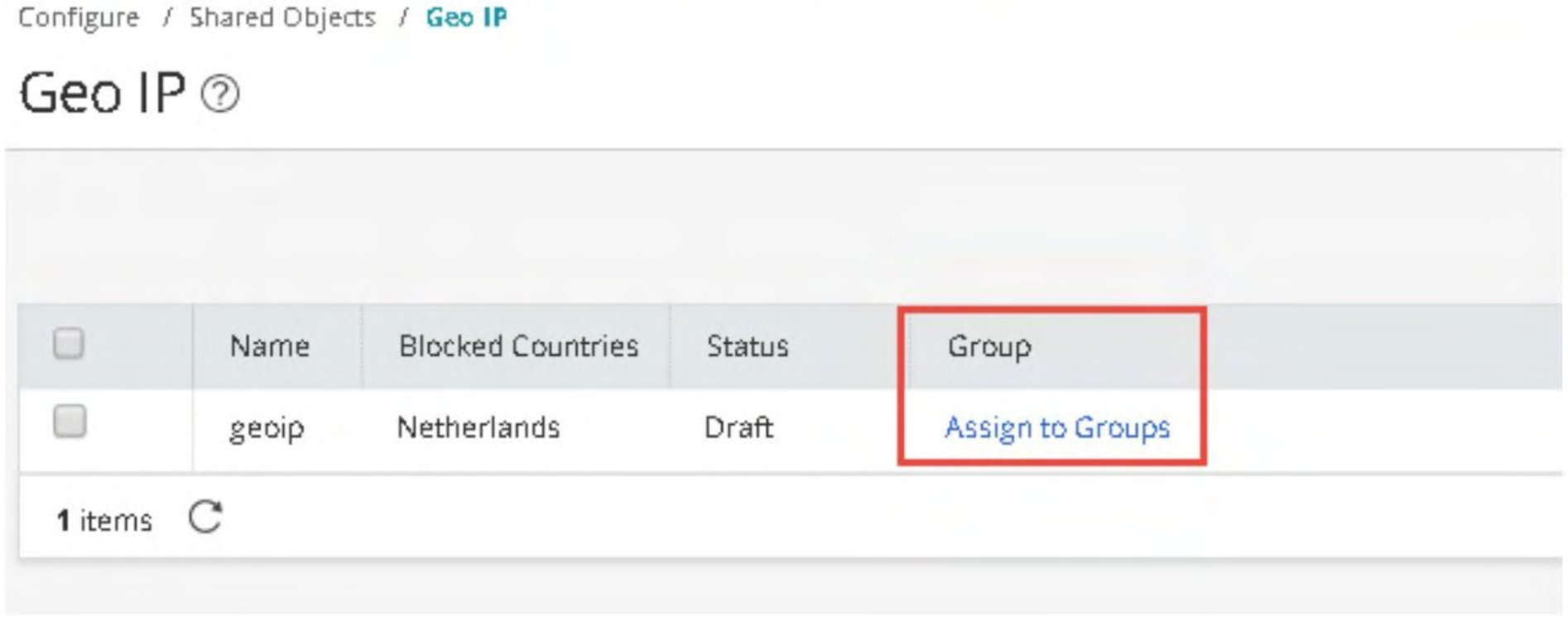


© 2020 Juniper Networks, Inc. All rights reserved.

5) Block all traffic to and from the Netherlands.
    a) Navigate to Configure / Shared Objects / Geo IP. Specify a name for the Geo IP object and "Netherlands" should be selected.

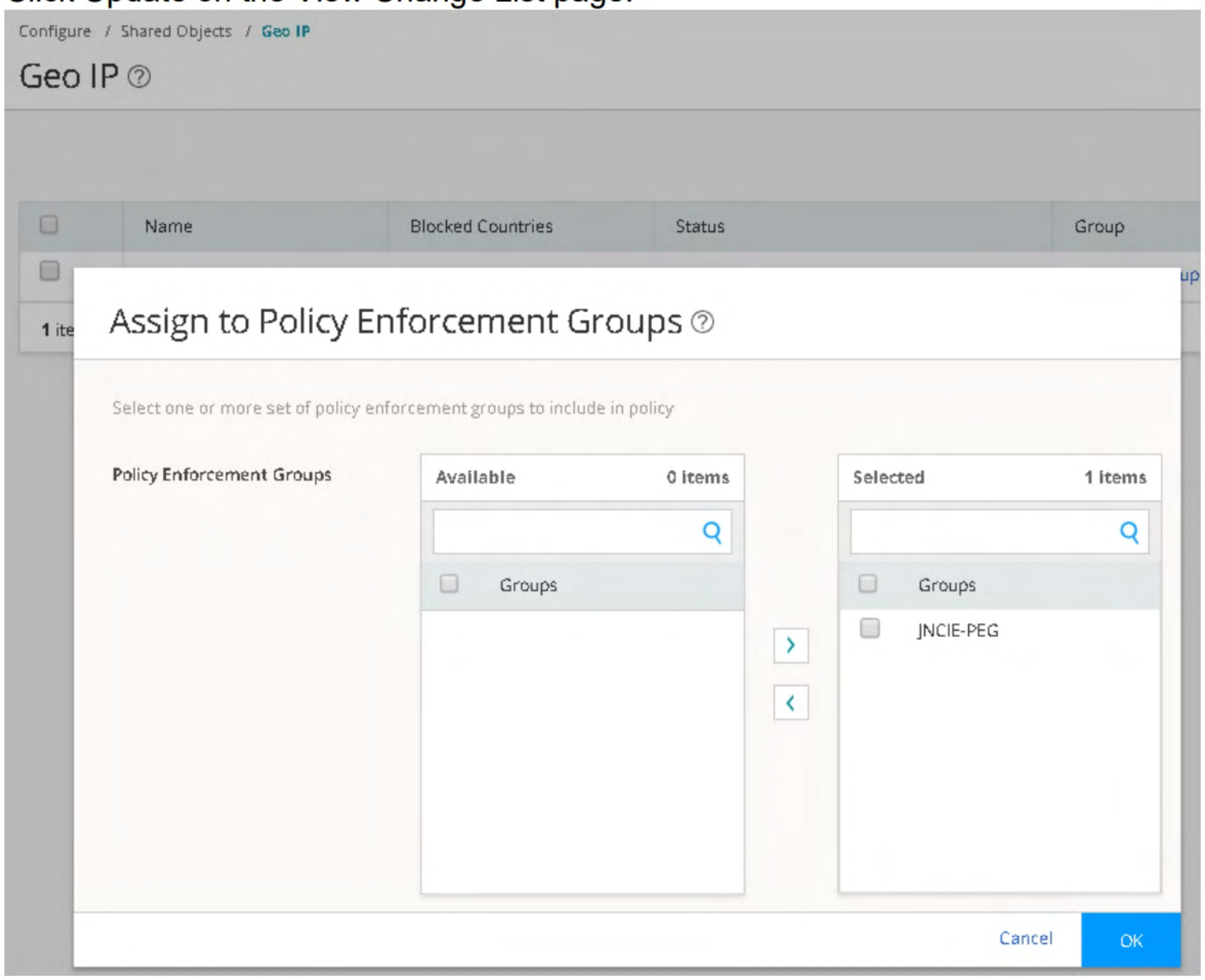


Assign this Geo IP object to your PEG that you recently created.

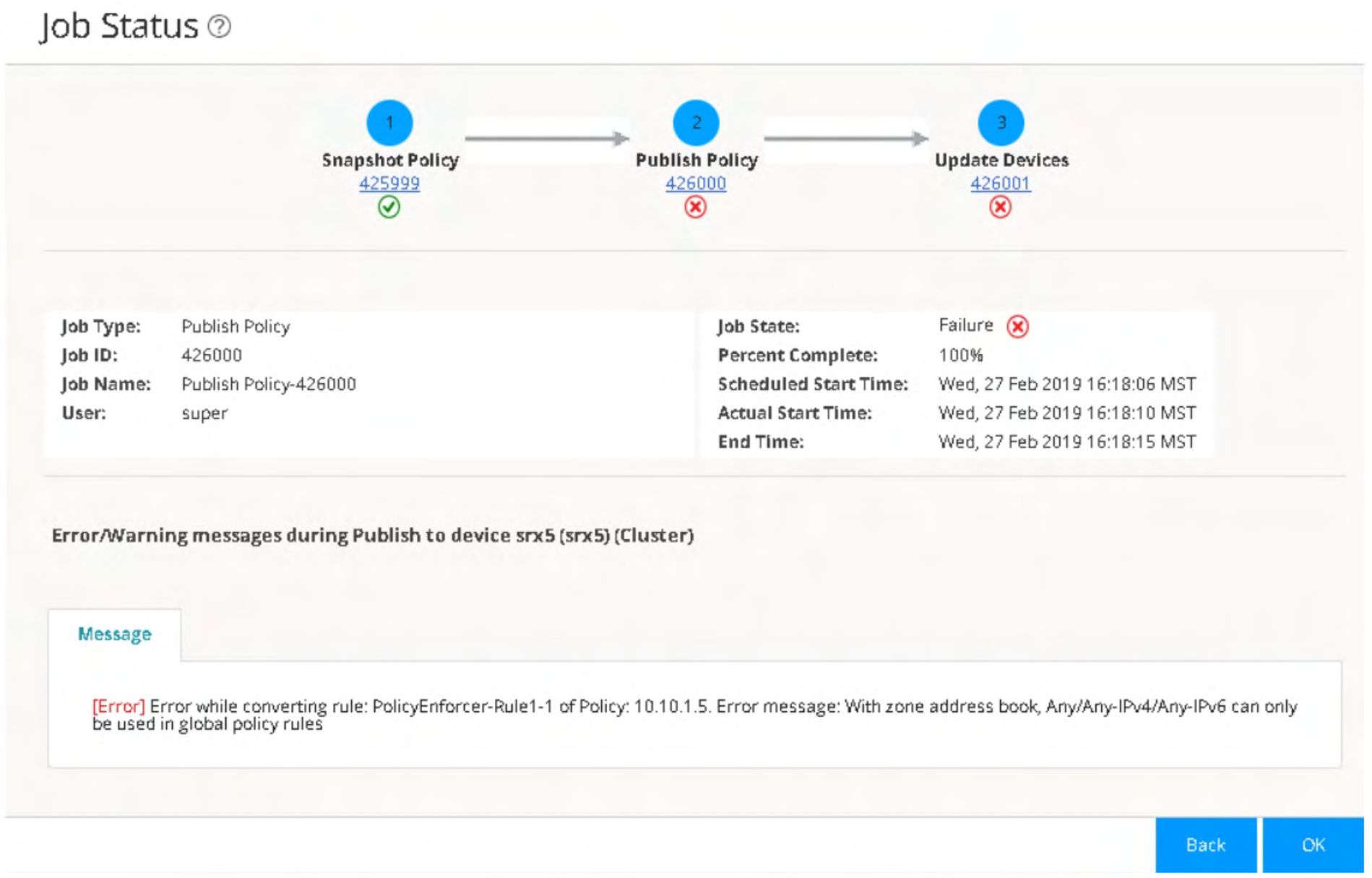


© 2020 Juniper Networks, Inc. All rights reserved.

Click Update on the View Change List page.



© 2020 Juniper Networks, Inc. All rights reserved.



b) The Publish Policy failed because there are zonal address books. We need to remove those zonal address books and put them back in as part of the global address book. Log into cluster 2 (srx5/srx6) CLI and remove all zonal address book entries. Commit and exit the configuration when you are done.

```
{primary:node0}[edit]
lab@srx5# edit security zones

{primary:node0}[edit security zones]
lab@srx5# delete security-zone TRUST address-book

{primary:node0}[edit security zones]
lab@srx5# delete security-zone DMZ address-book

{primary:node0}[edit security zones]
lab@srx5# delete security-zone INTERNAL address-book

{primary:node0}[edit security zones]
lab@srx5# delete security-zone UNTRUST address-book

{primary:node0}[edit security zones]
lab@srx5# up 1 edit address-book global
```

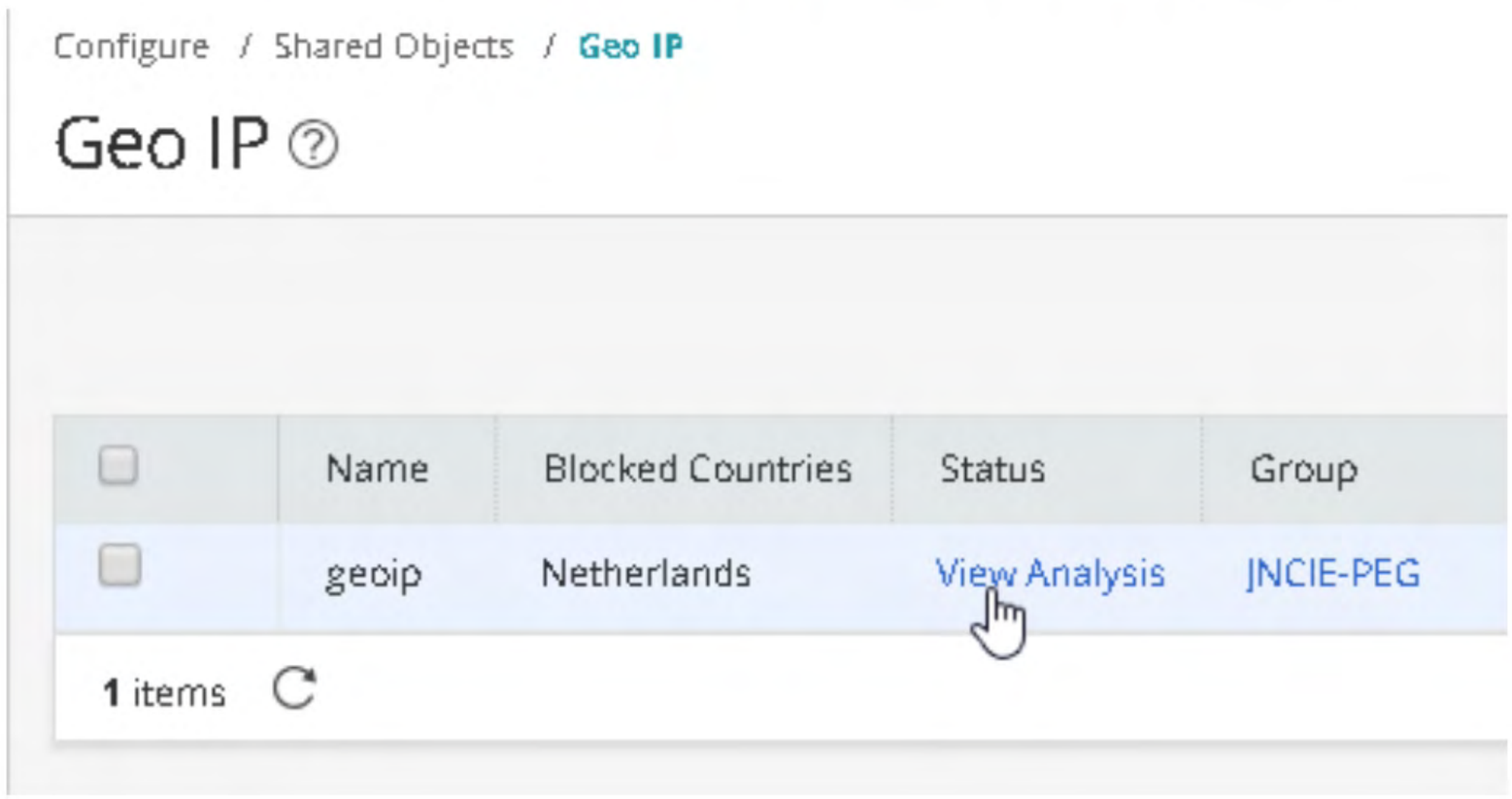

© 2020 Juniper Networks, Inc. All rights reserved.

```
{primary:node0}[edit security address-book global]
lab@srx5# set address trust-address-range 172.16.50.0/24

{primary:node0}[edit security address-book global]
lab@srx5# set address dmz-range 172.16.55.0/24

{primary:node0}[edit security address-book global]
lab@srx5# set address internal-range 172.16.60.0/24

{primary:node0}[edit security address-book global]
lab@srx5# set address finance-range 172.16.199.0/24

{primary:node0}[edit security address-book global]
lab@srx5# set address private-range 172.16.21.0/24

{primary:node0}[edit security address-book global]
lab@srx5# set address-set internal-finance-private-ranges address internal-range

{primary:node0}[edit security address-book global]
lab@srx5# set address-set internal-finance-private-ranges address finance-range

{primary:node0}[edit security address-book global]
lab@srx5# set address-set internal-finance-private-ranges address private-range

{primary:node0}[edit security address-book global]
lab@srx5# set address corp-network 172.16.0.0/16

{primary:node0}[edit security address-book global]
lab@srx5# set address dc-warehouse-range 172.16.200.0/24

{primary:node0}[edit security address-book global]
lab@srx5# set address dc-dmz-range 172.16.150.0/24

{primary:node0}[edit security address-book global]
lab@srx5# set address-set dc-dmz-warehouse address dc-dmz-range

{primary:node0}[edit security address-book global]
lab@srx5# set address-set dc-dmz-warehouse address dc-warehouse-range

{primary:node0}[edit security address-book global]
lab@srx5# show
address trust-address-range 172.16.50.0/24;
address dmz-range 172.16.55.0/24;
address internal-range 172.16.60.0/24;
address finance-range 172.16.199.0/24;
address private-range 172.16.21.0/24;
address corp-network 172.16.0.0/16;
address dc-warehouse-range 172.16.200.0/24;
address dc-dmz-range 172.16.150.0/24;
address-set internal-finance-private-ranges {
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
    address internal-range;
    address finance-range;
    address private-range;
}
address-set dc-dmz-warehouse {
    address dc-dmz-range;
    address dc-warehouse-range;
}

{primary:node0}[edit security address-book global]
lab@srx5# top

{primary:node0}[edit]
lab@srx5# commit and-quit
node0:
configuration check succeeds
node1:
commit complete
node0:
commit complete
Exiting configuration mode

{primary:node0}
lab@srx5>
```

c) Dismiss the fail job status window and click the “View Analysis” link in the Configure / Shared Objects / Geo IP workspace.



© 2020 Juniper Networks, Inc. All rights reserved.

d) Click Update again in the View Change List page.

View Change List

The following policies will be edited after analysis. Click on the policy to view these changes.

	Seq.	Name	Changed Rules Summary	Devices	Domain
>	**POLICIES APPLIED BEFORE 'DEVICE SPECIFIC POLICIES' (0 policy)**				
v	**DEVICE SPECIFIC POLICIES (1 policy)**				
		10.10.1.5	2 Rules Added, 2 Rules Deleted	srx5	Global
>	**POLICIES APPLIED AFTER 'DEVICE SPECIFIC POLICIES' (0 policy)**				

1 Rows

Cancel Update

Job Status

1 Snapshot Policy 426003 ✓ → 2 Publish Policy 426004 ✓ → 3 Update Devices 426005 ✓

Job Type:	Update Devices	**Job State:**	Success ✓
Job ID:	426005	**Percent Complete:**	100%
Job Name:	Update Devices-426005	**Scheduled Start Time:**	Wed, 27 Feb 2019 16:35:25 MST
User:	super	**Actual Start Time:**	Wed, 27 Feb 2019 16:35:25 MST
		End Time:	Wed, 27 Feb 2019 16:35:40 MST

Export to CSV

	Name	Status	Services	Message	Configuration	Commit time
	srx5 (srx5) (Cluster)	Success	10.10.1.5 [FWPolicy]	**View**	**View**	Wed, 27 Feb 2019 16:35:38 MST

1 Rows

OK

© 2020 Juniper Networks, Inc. All rights reserved.

e) Click the "View" link under the "Configuration" section.

i. ***WARNING:*** As the security device configuration for the central office node was not imported during the device discovery process the existing security configuration on the central device is unknown to Security Director. For this reason, Security Director will remove (most) of the existing security configuration and applies the newly created Threat prevention policy to the central office.

ii. The following output shows that most of the security device configuration is removed and that the Threat prevention policies is applied.

View configuration for srx5 (srx5) (Cluster)

CLI XML

Added Deleted Modified Comments

```
##Global address book configurations##
set security address-book global address JNCIE-PEG_172.16.50.100 172.16.50.100/32
delete security address-book global address corp-network
delete security address-book global address dc-dmz-range
delete security address-book global address dc-warehouse-range
delete security address-book global address dmz-range
delete security address-book global address finance-range
delete security address-book global address internal-range
delete security address-book global address private-range
delete security address-book global address trust-address-range
delete security address-book global address-set dc-dmz-warehouse
delete security address-book global address-set internal-finance-private-ranges
##Applications##
delete applications application-set dmz-apps
delete applications application-set dmz-apps-web-auth
delete applications application-set internet-apps
##Security Firewall Policy : INTERNAL - UNTRUST##
delete security policies from-zone INTERNAL to-zone UNTRUST
##Security Firewall Policy : INTERNAL - DMZ##
delete security policies from-zone INTERNAL to-zone DMZ
##Security Firewall Policy : TRUST - UNTRUST##
delete security policies from-zone TRUST to-zone UNTRUST
##Security Firewall Policy : TRUST - DMZ##
delete security policies from-zone TRUST to-zone DMZ
##Security Firewall Policy : TRUST - INTERNAL##
delete security policies from-zone TRUST to-zone INTERNAL
##Security Firewall Policy : DMZ - UNTRUST##
delete security policies from-zone DMZ to-zone UNTRUST
##Security Firewall Policy : UNTRUST - DMZ##
delete security policies from-zone UNTRUST to-zone DMZ
##Security Firewall Policy : INTERNAL - UNTRUST##
delete security policies from-zone INTERNAL to-zone UNTRUST
##Security Firewall Policy : INTERNAL - DMZ##
delete security policies from-zone INTERNAL to-zone DMZ
##Security Firewall Policy : TRUST - UNTRUST##
delete security policies from-zone TRUST to-zone UNTRUST
##Security Firewall Policy : TRUST - DMZ##
delete security policies from-zone TRUST to-zone DMZ
##Security Firewall Policy : TRUST - INTERNAL##
delete security policies from-zone TRUST to-zone INTERNAL
##Security Firewall Policy : DMZ - UNTRUST##
delete security policies from-zone DMZ to-zone UNTRUST
##Security Firewall Policy : UNTRUST - DMZ##
delete security policies from-zone UNTRUST to-zone DMZ
##Security Firewall Policy : global ##
set security policies global policy PolicyEnforcer-Rule1-1 match application any
set security policies global policy PolicyEnforcer-Rule1-1 match destination-address JNCIE-PEG_172.16.50.100
set security policies global policy PolicyEnforcer-Rule1-1 match source-address geoip
set security policies global policy PolicyEnforcer-Rule1-1 then deny
set security policies global policy PolicyEnforcer-Rule2-1 match application any
set security policies global policy PolicyEnforcer-Rule2-1 match destination-address geoip
set security policies global policy PolicyEnforcer-Rule2-1 match source-address JNCIE-PEG_172.16.50.100
set security policies global policy PolicyEnforcer-Rule2-1 then deny
##Dynamic Address Configurations##
set security dynamic-address address-name geoip profile category GeoIP property country string NL
##schedulers##
delete schedulers
```

OK

© 2020 Juniper Networks, Inc. All rights reserved.

f) Return to the CLI with cluster 2 (srx5/srx6) and enter configuration mode. Examine the differences between the current and previous configurations.

```
{primary:node0}
lab@srx5>

{primary:node0}[edit]
lab@srx5# show | compare rollback 1
[edit security address-book global]
+    address JNCIE-PEG_172.16.50.10/24 172.16.50.0/24;
+    address JNCIE-PEG_172.16.55.10/24 172.16.55.0/24;
+    address JNCIE-PEG_172.16.60.10/24 172.16.60.0/24;
-    address trust-address-range 172.16.50.0/24;
-    address dmz-range 172.16.55.0/24;
-    address internal-range 172.16.60.0/24;
-    address finance-range 172.16.199.0/24;
-    address private-range 172.16.21.0/24;
-    address corp-network 172.16.0.0/16;
-    address dc-warehouse-range 172.16.200.0/24;
-    address dc-dmz-range 172.16.150.0/24;
[edit security address-book global]
-    address-set internal-finance-private-ranges {
-        address internal-range;
-        address private-range;
-        address finance-range;
-    }
-    address-set dc-dmz-warehouse {
-        address dc-warehouse-range;
-        address dc-dmz-range;
-    }
[edit security]
+   dynamic-address {
+       address-name geoip {
+           profile {
+               category GeoIP {
+                   property country {
+                       string NL;
+                   }
+               }
+           }
+       }
+   }
[edit security policies]
-    from-zone INTERNAL to-zone UNTRUST {
-        policy finance-dc-dmz-warehouse-access {
-            match {
-                source-address finance-range;
-                destination-address dc-dmz-warehouse;
-                application any;
-            }
-            then {
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
-                 permit;
-             }
-         }
-     }
-     from-zone INTERNAL to-zone DMZ {
-         policy finance-dmz-access {
-             match {
-                 source-address finance-range;
-                 destination-address dmz-range;
-                 application any;
-             }
-             then {
-                 permit;
-             }
-         }
-         policy internal-dmz-access {
-             match {
-                 source-address internal-range;
-                 destination-address dmz-range;
-                 application any;
-             }
-             then {
-                 permit;
-             }
-             scheduler-name working-time;
-         }
-     }
-     from-zone TRUST to-zone UNTRUST {
-         policy trust-corp-network {
-             match {
-                 source-address trust-address-range;
-                 destination-address corp-network;
-                 application any;
-             }
-             then {
-                 permit;
-             }
-         }
-         policy internet-access {
-             match {
-                 source-address trust-address-range;
-                 destination-address any;
-                 application internet-apps;
-             }
-             then {
-                 permit;
-             }
-         }
-         policy internet-denied-log {
-             match {
-                 source-address any;
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
-                 destination-address any;
-                 application any;
-             }
-             then {
-                 deny;
-                 log {
-                     session-init;
-                 }
-             }
-         }
-     }
-     from-zone TRUST to-zone DMZ {
-         policy trust-dmz-access {
-             match {
-                 source-address trust-address-range;
-                 destination-address dmz-range;
-                 application any;
-             }
-             then {
-                 permit;
-             }
-         }
-     }
-     from-zone TRUST to-zone INTERNAL {
-         policy trust-to-int-priv-fin {
-             match {
-                 source-address trust-address-range;
-                 destination-address internal-finance-private-ranges;
-                 application any;
-             }
-             then {
-                 permit;
-             }
-         }
-     }
-     from-zone DMZ to-zone UNTRUST {
-         policy dmz-warehouse-access {
-             match {
-                 source-address dmz-range;
-                 destination-address dc-warehouse-range;
-                 application any;
-             }
-             then {
-                 permit;
-             }
-         }
-     }
-     from-zone UNTRUST to-zone DMZ {
-         policy warehouse-dmz-access {
-             match {
-                 source-address dc-warehouse-range;
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
-                 destination-address dmz-range;
-                 application any;
-             }
-             then {
-                 permit;
-             }
-         }
-         policy corp-dmz-acces-web-auth {
-             match {
-                 source-address corp-network;
-                 destination-address dmz-range;
-                 application dmz-apps-web-auth;
-             }
-             then {
-                 permit {
-                     firewall-authentication {
-                         pass-through {
-                             client-match testuser;
-                         }
-                     }
-                 }
-             }
-         }
-         policy corp-dmz-acces {
-             match {
-                 source-address corp-network;
-                 destination-address dmz-range;
-                 application dmz-apps;
-             }
-             then {
-                 permit;
-             }
-         }
-     }
[edit security policies]
+     global {
+         policy PolicyEnforcer-Rule1-1 {
+             match {
+                 source-address geoip;
+                 destination-address [ JNCIE-PEG_172.16.55.10/24 JNCIE-PEG_172.16.50.10/24
JNCIE-PEG_172.16.60.10/24 ];
+                 application any;
+             }
+             then {
+                 deny;
+             }
+         }
+         policy PolicyEnforcer-Rule2-1 {
+             match {
+                 source-address [ JNCIE-PEG_172.16.55.10/24 JNCIE-PEG_172.16.50.10/24 JNCIE-
PEG_172.16.60.10/24 ];
```


© 2020 Juniper Networks, Inc. All rights reserved.

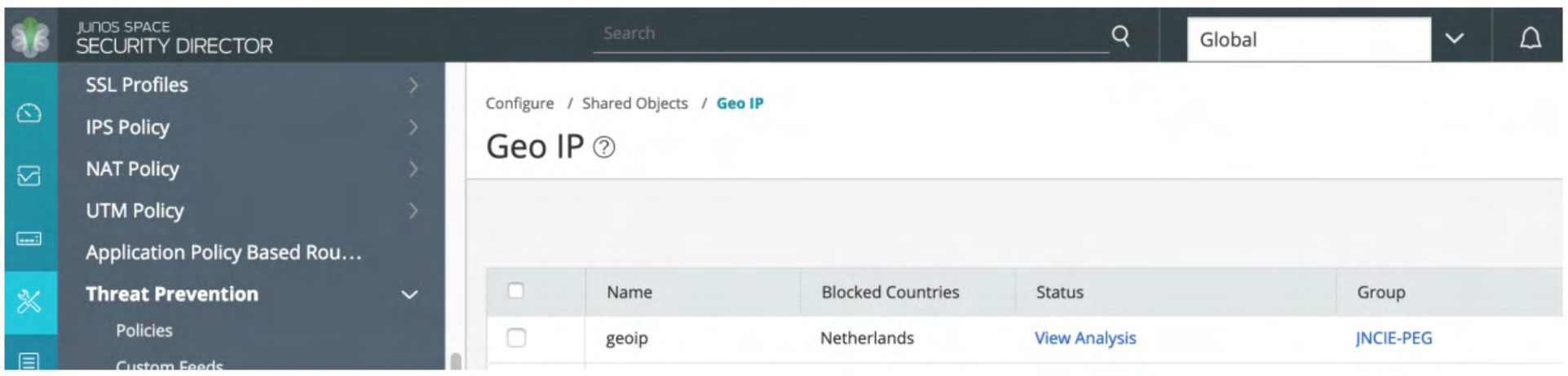
```
+                destination-address geoip;
+                application any;
+            }
+            then {
+                deny;
+            }
+        }
+    }
[edit]
-  applications {
-      application-set dmz-apps {
-          application junos-http;
-          application junos-https;
-          application junos-ssh;
-      }
-      application-set dmz-apps-web-auth {
-          application junos-ftp;
-          application junos-telnet;
-          application junos-http;
-      }
-      application-set internet-apps {
-          application junos-http;
-          application junos-https;
-      }
-  }
-  schedulers {
-      scheduler working-time {
-          daily {
-              start-time 08:00:00 stop-time 18:00:00;
-          }
-          sunday exclude;
-          saturday exclude;
-      }
-  }
```

g) Merge the current configuration with the previous configuration. Note that the new global polices conflict with some zonal policies. The conflict means the zonal policies are honored before global based polices, this idea means that the traffic from the 172.16.50.100 host is not subject to SDSN. We will fix this issue in a later step.

```
{primary:node0}[edit]
lab@srx5# rollback 1
load complete

{primary:node0}[edit]
lab@srx5# save ch9-task7-sdsn.config
Wrote 642 lines of configuration to 'ch9-task7-sdsn.config'

{primary:node0}[edit]
```

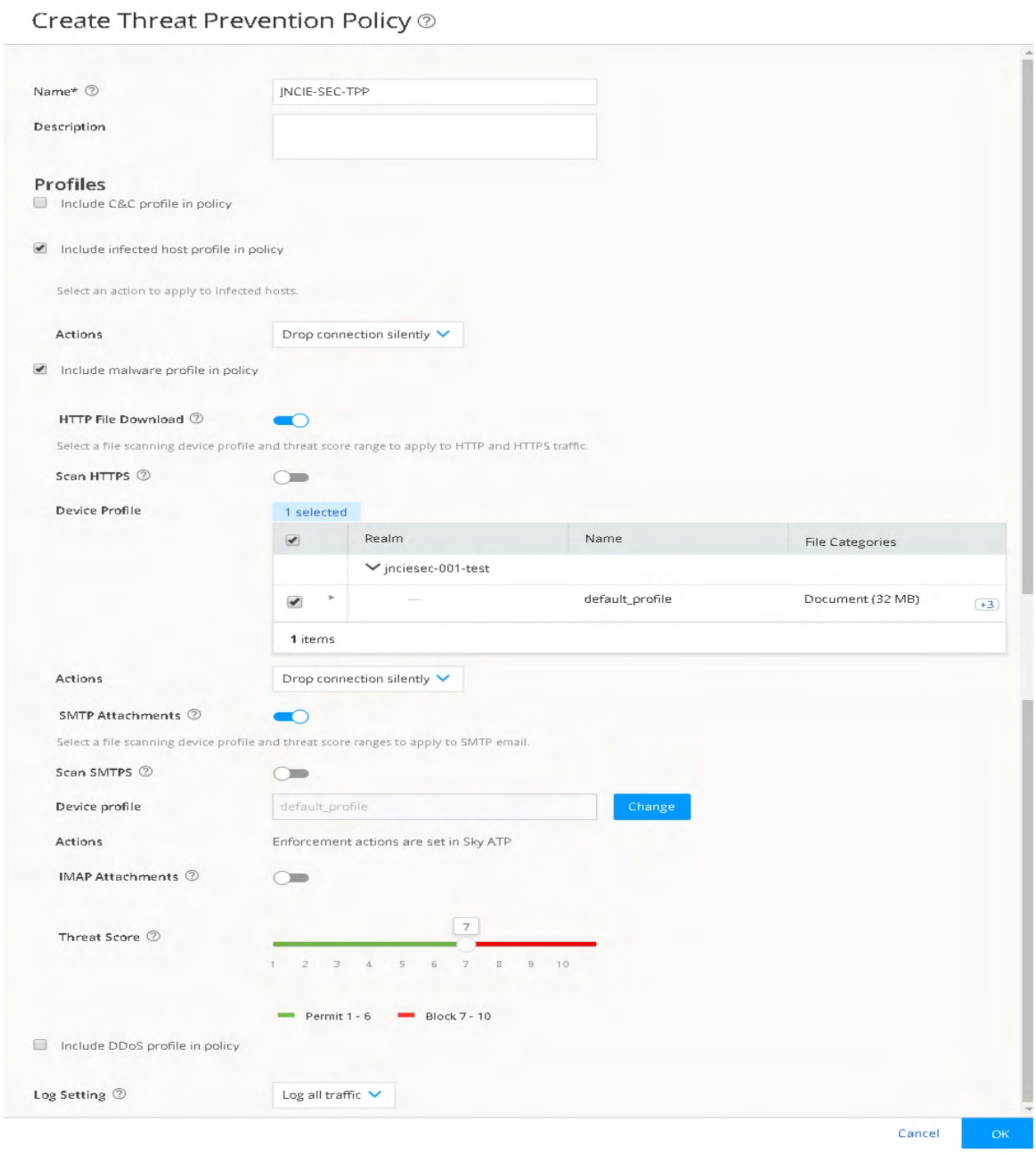

© 2020 Juniper Networks, Inc. All rights reserved.

```
lab@srx5# rollback

{primary:node0}[edit]
lab@srx5# load merge ch9-task7-sdsn.config
load complete

{primary:node0}[edit]
lab@srx5# commit and-quit
node0:
configuration check succeeds
node1:
commit complete
node0:
commit complete

{primary:node0}[edit]
lab@srx5>
```



© 2020 Juniper Networks, Inc. All rights reserved.

h) Return to the Security Directory GUI and navigate to the Configure / Threat Prevention / Policies workspace to setup a threat prevention policy. Make sure that you include the infected host profile and the malware profile in the policy. Scan HTTP and SMTP files downloads using the default profile associated with your realm. Set the Threat score to block threats rated at a value of 7 or above.



© 2020 Juniper Networks, Inc. All rights reserved.

i) Assign your PEG to the policy.

Configure / Threat Prevention / Policies

Threat Prevention Policies

	Name	C&C Server	Infected Host	Malware HTTP	DDoS	Malware SM...	Malware IMAP	Status	Policy Enforcement Groups	Log
	JNCIE-SEC-TPP	—	Block Drop	default_profile	—	default_profile		Draft	Assign to Groups	Log all traffic

1 items

Configure / Threat Prevention / Policies

Threat Prevention Policies

	Name	C&C Server	Infected Host	Malware H...	DDoS	Malware S...	Malware IM...	Status	Policy Enforcement ...
	JNCIE-SEC-T...	—	Block Drop	default_profi...	—	default_profi...		Draft	Assign to Groups

1 items

Assign to Policy Enforcement Groups

Select one or more set of policy enforcement groups to include in policy

Policy Enforcement Groups

Available 0 items

Groups

Selected 1 items

Groups

JNCIE-PEG

Cancel OK

© 2020 Juniper Networks, Inc. All rights reserved.

j) Click Update on the View Change List page.

View Change List

The following policies will be edited after analysis. Click on the policy to view these changes.

	Seq.	Name	Changed Rules Summary	Devices	Domain
>	POLICIES APPLIED BEFORE 'DEVICE SPECIFIC POLICIES' (0 policy)				
⌄	DEVICE SPECIFIC POLICIES (1 policy)				
	10.10.1.5		1 Rule Added	srx5	Global
>	POLICIES APPLIED AFTER 'DEVICE SPECIFIC POLICIES' (0 policy)				

1 Rows

Cancel Update

Job Status

1 Snapshot Policy 426009 ✓ → 2 Publish Policy 426010 ✓ → 3 Update Devices 426011 ✓

Job Type:	Update Devices	**Job State:**	Success ✓
Job ID:	426011	**Percent Complete:**	100%
Job Name:	Update Devices-426011	**Scheduled Start Time:**	Wed, 27 Feb 2019 16:41:35 MST
User:	super	**Actual Start Time:**	Wed, 27 Feb 2019 16:41:35 MST
		End Time:	Wed, 27 Feb 2019 16:41:50 MST

Export to CSV

	Name	Status	Services	Message	Configuration	Commit time
	srx5 (srx5) (Cluster)	Success	10.10.1.5 [FWPolicy]	**View**	**View**	Wed, 27 Feb 2019 16:41:46 MST

1 Rows

OK

© 2020 Juniper Networks, Inc. All rights reserved.

k) Merge the current configuration with the previously saved configuration file.

```
{primary:node0}[edit]
lab@srx5# load merge ch9-task7-sdsn.config
load complete

{primary:node0}[edit]
lab@srx5# commit and-quit
node0:
configuration check succeeds
node1:
commit complete
node0:
commit complete
Exiting configuration mode

{primary:node0}
lab@srx5>
```

l) There is still a conflict between the global policies and the zone policies that will not let traffic from the 172.16.10.100 host hit the global policies with the SDSN content. Enter configuration mode and convert the zonal policies to global policies. Remember to maintain the zone to zone context for these policies.
   i. Examine the zonal policies.

```
{primary:node0}[edit]
lab@srx5# edit security policies

{primary:node0}[edit security policies]
lab@srx5# show
from-zone INTERNAL to-zone UNTRUST {
    policy finance-dc-dmz-warehouse-access {
        match {
            source-address finance-range;
            destination-address dc-dmz-warehouse;
            application any;
        }
        then {
            permit;
        }
    }
}
from-zone INTERNAL to-zone DMZ {
    policy finance-dmz-access {
        match {
            source-address finance-range;
            destination-address dmz-range;
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
        application any;
    }
    then {
        permit;
    }
}
policy internal-dmz-access {
    match {
        source-address internal-range;
        destination-address dmz-range;
        application any;
    }
    then {
        permit;
    }
    scheduler-name working-time;
}
}
from-zone TRUST to-zone UNTRUST {
    policy trust-corp-network {
        match {
            source-address trust-address-range;
            destination-address corp-network;
            application any;
        }
        then {
            permit;
        }
    }
    policy internet-access {
        match {
            source-address trust-address-range;
            destination-address any;
            application internet-apps;
        }
        then {
            permit;
        }
}
policy internet-denied-log {
    match {
        source-address any;
        destination-address any;
        application any;
    }
    then {
        deny;
        log {
            session-init;
        }
    }
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
    }
}
from-zone TRUST to-zone DMZ {
    policy trust-dmz-access {
        match {
            source-address trust-address-range;
            destination-address dmz-range;
            application any;
        }
        then {
            permit;
        }
    }
}
from-zone TRUST to-zone INTERNAL {
    policy trust-to-int-priv-fin {
        match {
            source-address trust-address-range;
            destination-address internal-finance-private-ranges;
            application any;
        }
        then {
            permit;
        }
    }
}
from-zone DMZ to-zone UNTRUST {
    policy dmz-warehouse-access {
        match {
            source-address dmz-range;
            destination-address dc-warehouse-range;
            application any;
        }
        then {
            permit;
        }
    }
}
from-zone UNTRUST to-zone DMZ {
    policy warehouse-dmz-access {
        match {
            source-address dc-warehouse-range;
            destination-address dmz-range;
            application any;
        }
        then {
            permit;
        }
    }
    policy corp-dmz-acces-web-auth {
        match {
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
        source-address corp-network;
        destination-address dmz-range;
        application dmz-apps-web-auth;
    }
    then {
        permit {
            firewall-authentication {
                pass-through {
                    client-match testuser;
                }
            }
        }
    }
    policy corp-dmz-acces {
        match {
            source-address corp-network;
            destination-address dmz-range;
            application dmz-apps;
        }
        then {
            permit;
        }
    }
}
global {
    policy PolicyEnforcer-Rule1-1 {
        match {
            source-address geoip;
            destination-address JNCIE-PEG_172.16.50.100;
            application any;
        }
        then {
            deny;
        }
    }
    policy PolicyEnforcer-Rule2-1 {
        match {
            source-address JNCIE-PEG_172.16.50.100;
            destination-address geoip;
            application any;
        }
        then {
            deny;
        }
    }
    policy PolicyEnforcer-Rule1-2 {
        match {
            source-address JNCIE-PEG_172.16.50.100;
            destination-address any;
            application any;
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
        }
        then {
            permit {
                application-services {
                    security-intelligence-policy JNCIE-SEC-TPP;
                    advanced-anti-malware-policy JNCIE-SEC-TPP;
                }
            }
        }
    }
}
```

ii. Copy and paste the zonal policies into the [edit security policies global] configuration hierarchy.

```
{primary:node0}[edit security policies]
lab@srx5# edit global

{primary:node0}[edit security policies global]lab@srx5# load merge terminal relative
[Type ^D at a new line to end input]
    policy finance-dc-dmz-warehouse-access {
        match {
            source-address finance-range;
            destination-address dc-dmz-warehouse;
            application any;
        }
        then {
            permit;
        }
    }load complete

{primary:node0}[edit security policies global]
lab@srx5# load merge terminal relative
[Type ^D at a new line to end input]
    policy finance-dmz-access {
        match {
            source-address finance-range;
            destination-address dmz-range;
            application any;
        }
        then {
            permit;
        }
    }
    policy internal-dmz-access {
        match {
            source-address internal-range;
            destination-address dmz-range;
            application any;
        }
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
        then {
            permit;
        }
        scheduler-name working-time;
    }load complete

{primary:node0}[edit security policies global]
lab@srx5# load merge terminal relative
[Type ^D at a new line to end input]
    policy trust-corp-network {
        match {
            source-address trust-address-range;
            destination-address corp-network;
            application any;
        }
        then {
            permit;
        }
    }
    policy internet-access {
        match {
            source-address trust-address-range;
            destination-address any;
            application internet-apps;
        }
        then {
            permit;
        }
    }
    policy internet-denied-log {
        match {
            source-address any;
            destination-address any;
            application any;
        }
        then {
            deny;
            log {
                session-init;
            }
        }
    }load complete

{primary:node0}[edit security policies global]
lab@srx5# load merge terminal relative
[Type ^D at a new line to end input]
    policy trust-dmz-access {
        match {
            source-address trust-address-range;
            destination-address dmz-range;
            application any;
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
        }
        then {
            permit;
        }
    }load complete

{primary:node0}[edit security policies global]
lab@srx5# load merge terminal relative
[Type ^D at a new line to end input]
    policy trust-to-int-priv-fin {
        match {
            source-address trust-address-range;
            destination-address internal-finance-private-ranges;
            application any;
        }
        then {
            permit;
        }
    }load complete

{primary:node0}[edit security policies global]
lab@srx5# load merge terminal relative
[Type ^D at a new line to end input]
    policy dmz-warehouse-access {
        match {
            source-address dmz-range;
            destination-address dc-warehouse-range;
            application any;
        }
        then {
            permit;
        }
    }load complete

{primary:node0}[edit security policies global]
lab@srx5# load merge terminal relative
[Type ^D at a new line to end input]
    policy warehouse-dmz-access {
        match {
            source-address dc-warehouse-range;
            destination-address dmz-range;
            application any;
        }
        then {
            permit;
        }
    }
    policy corp-dmz-acces-web-auth {
        match {
            source-address corp-network;
            destination-address dmz-range;
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
        application dmz-apps-web-auth;
    }
    then {
        permit {
            firewall-authentication {
                pass-through {
                    client-match testuser;
                }
            }
        }
    }
}
policy corp-dmz-acces {
        match {
            source-address corp-network;
            destination-address dmz-range;
            application dmz-apps;
        }
        then {
            permit;
        }
    }load complete
```

iii. Delete the zonal policies.

```
{primary:node0}[edit security policies global]
lab@srx5# up 1

{primary:node0}[edit security policies]
lab@srx5# show | match from-zone
from-zone INTERNAL to-zone UNTRUST {
from-zone INTERNAL to-zone DMZ {
from-zone TRUST to-zone UNTRUST {
from-zone TRUST to-zone DMZ {
from-zone TRUST to-zone INTERNAL {
from-zone DMZ to-zone UNTRUST {
from-zone UNTRUST to-zone DMZ {

{primary:node0}[edit security policies]
lab@srx5# delete from-zone INTERNAL to-zone UNTRUST

{primary:node0}[edit security policies]
lab@srx5# delete from-zone INTERNAL to-zone DMZ

{primary:node0}[edit security policies]
lab@srx5# delete from-zone TRUST to-zone UNTRUST

{primary:node0}[edit security policies]
lab@srx5# delete from-zone TRUST to-zone DMZ
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
{primary:node0}[edit security policies]
lab@srx5# delete from-zone TRUST to-zone INTERNAL

{primary:node0}[edit security policies]
lab@srx5# delete from-zone DMZ to-zone UNTRUST

{primary:node0}[edit security policies]
lab@srx5# delete from-zone UNTRUST to-zone DMZ
```

iv. Configure the new global policies to have the same zone to zone context as when they were zonal policies.

```
{primary:node0}[edit security policies]
lab@srx5# edit global

{primary:node0}[edit security policies global]
lab@srx5# set policy finance-dc-dmz-warehouse-access match from-zone INTERNAL to-zone UNTRUST

{primary:node0}[edit security policies global]
lab@srx5# set policy finance-dmz-access match from-zone INTERNAL to-zone DMZ

{primary:node0}[edit security policies global]
lab@srx5# set policy internal-dmz-access match from-zone INTERNAL to-zone DMZ

{primary:node0}[edit security policies global]
lab@srx5# set policy trust-corp-network match from-zone TRUST to-zone UNTRUST

{primary:node0}[edit security policies global]
lab@srx5# set policy internet-access match from-zone TRUST to-zone UNTRUST

{primary:node0}[edit security policies global]
lab@srx5# set policy internet-denied-log match from-zone TRUST to-zone UNTRUST

{primary:node0}[edit security policies global]
lab@srx5# set policy trust-dmz-access match from-zone TRUST to-zone DMZ

{primary:node0}[edit security policies global]
lab@srx5# set policy trust-to-int-priv-fin match from-zone TRUST to-zone INTERNAL

{primary:node0}[edit security policies global]
lab@srx5# set policy dmz-warehouse-access match from-zone DMZ to-zone UNTRUST

{primary:node0}[edit security policies global]
lab@srx5# set policy warehouse-dmz-access match from-zone UNTRUST to-zone DMZ

{primary:node0}[edit security policies global]
lab@srx5# set policy corp-dmz-acces-web-auth match from-zone UNTRUST to-zone DMZ

{primary:node0}[edit security policies global]
lab@srx5# set policy corp-dmz-acces match from-zone UNTRUST to-zone DMZ
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
{primary:node0}[edit security policies global]
lab@srx5# show
policy PolicyEnforcer-Rule1-1 {
    match {
        source-address geoip;
        destination-address JNCIE-PEG_172.16.50.100;
        application any;
    }
    then {
        deny;
    }
}
policy PolicyEnforcer-Rule2-1 {
    match {
        source-address JNCIE-PEG_172.16.50.100;
        destination-address geoip;
        application any;
    }
    then {
        deny;
    }
}
policy PolicyEnforcer-Rule1-2 {
    match {
        source-address JNCIE-PEG_172.16.50.100;
        destination-address any;
        application any;
    }
    then {
        permit {
            application-services {
                security-intelligence-policy JNCIE-SEC-TPP;
                advanced-anti-malware-policy JNCIE-SEC-TPP;
            }
        }
    }
}
policy finance-dc-dmz-warehouse-access {
    match {
        source-address finance-range;
        destination-address dc-dmz-warehouse;
        application any;
        from-zone INTERNAL;
        to-zone UNTRUST;
    }
    then {
        permit;
    }
}
policy finance-dmz-access {
    match {
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
        source-address finance-range;
        destination-address dmz-range;
        application any;
        from-zone INTERNAL;
        to-zone DMZ;
    }
    then {
        permit;
    }
}
policy internal-dmz-access {
    match {
        source-address internal-range;
        destination-address dmz-range;
        application any;
        from-zone INTERNAL;
        to-zone DMZ;
    }
    then {
        permit;
    }
    scheduler-name working-time;
}
policy trust-corp-network {
    match {
        source-address trust-address-range;
        destination-address corp-network;
        application any;
        from-zone TRUST;
        to-zone UNTRUST;
    }
    then {
        permit;
    }
}
policy internet-access {
    match {
        source-address trust-address-range;
        destination-address any;
        application internet-apps;
        from-zone TRUST;
        to-zone UNTRUST;
    }
    then {
        permit;
    }
}
policy internet-denied-log {
    match {
        source-address any;
        destination-address any;
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
        application any;
        from-zone TRUST;
        to-zone UNTRUST;
    }
    then {
        deny;
        log {
            session-init;
        }
    }
}
policy trust-dmz-access {
    match {
        source-address trust-address-range;
        destination-address dmz-range;
        application any;
        from-zone TRUST;
        to-zone DMZ;
    }
    then {
        permit;
    }
}
policy trust-to-int-priv-fin {
    match {
        source-address trust-address-range;
        destination-address internal-finance-private-ranges;
        application any;
        from-zone TRUST;
        to-zone INTERNAL;
    }
    then {
        permit;
    }
}
policy dmz-warehouse-access {
    match {
        source-address dmz-range;
        destination-address dc-warehouse-range;
        application any;
        from-zone DMZ;
        to-zone UNTRUST;
    }
    then {
        permit;
    }
}
policy warehouse-dmz-access {
    match {
        source-address dc-warehouse-range;
        destination-address dmz-range;
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
        application any;
        from-zone UNTRUST;
        to-zone DMZ;
    }
    then {
        permit;
    }
}
policy corp-dmz-acces-web-auth {
    match {
        source-address corp-network;
        destination-address dmz-range;
        application dmz-apps-web-auth;
        from-zone UNTRUST;
        to-zone DMZ;
    }
    then {
        permit {
            firewall-authentication {
                pass-through {
                    client-match testuser;
                }
            }
        }
    }
}
policy corp-dmz-acces {
    match {
        source-address corp-network;
        destination-address dmz-range;
        application dmz-apps;
        from-zone UNTRUST;
        to-zone DMZ;
    }
    then {
        permit;
    }
}
{primary:node0}[edit security policies global]
lab@srx5# top

{primary:node0}[edit]
lab@srx5# commit
node0:
configuration check succeeds
node1:
commit complete
node0:
commit complete
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
{primary:node0}
lab@srx5>
```

m) You can verify the SDSN policies on in the CLI of srx5.

```
{primary:node0}
lab@srx5> show configuration services
ssl {
    initiation {
        profile aamw-ssl {
            trusted-ca [ aamw-secintel-ca aamw-cloud-ca ];
            client-certificate aamw-srx-cert;
            actions {
                crl {
                    disable;
                }
            }
        }
    }
}
security-intelligence {
    url https://10.10.1.123:443/api/v1/manifest.xml;
    authentication {
        auth-token PKY8AM0SYQ492TPA00IGI82YG9BJ4RWZ;
    }
    profile JNCIE-SEC-TPP_Infected-Hosts {
        category Infected-Hosts;
        rule Rule-1 {
            match {
                threat-level [ 1 2 3 4 5 6 ];
            }
            then {
                action {
                    permit;
                }
                log;
            }
        }
        rule Rule-2 {
            match {
                threat-level [ 7 8 9 10 ];
            }
            then {
                action {
                    block {
                        drop;
                    }
                }
                log;
            }
        }
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
    }
    policy JNCIE-SEC-TPP {
        Infected-Hosts {
            JNCIE-SEC-TPP_Infected-Hosts;
        }
    }
}
advanced-anti-malware {
    connection {
        url https://srxapi.us-west-2.sky.junipersecurity.net;
        authentication {
            tls-profile aamw-ssl;
        }
    }
    policy JNCIE-SEC-TPP {
        http {
            inspection-profile default_profile;
            action block;
            notification {
                log;
            }
        }
        smtp {
            inspection-profile default_profile;
            notification {
                log;
            }
        }
        verdict-threshold 7;
        fallback-options {
            action permit;
            notification {
                log;
            }
        }
        default-notification {
            log;
        }
        whitelist-notification {
            log;
        }
        blacklist-notification {
            log;
        }
    }
}

{primary:node0}
lab@srx5> show configuration security policies
global {
    policy PolicyEnforcer-Rule1-1 {
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
        match {
            source-address geoip;
            destination-address [ JNCIE-PEG_172.16.60.10/24 JNCIE-PEG_172.16.55.10/24 JNCIE-
PEG_172.16.50.10/24 ];
            application any;
        }
        then {
            deny;
        }
    }
    policy PolicyEnforcer-Rule2-1 {
        match {
            source-address [ JNCIE-PEG_172.16.60.10/24 JNCIE-PEG_172.16.55.10/24 JNCIE-
PEG_172.16.50.10/24 ];
            destination-address geoip;
            application any;
        }
        then {
            deny;
        }
    }
    policy PolicyEnforcer-Rule1-2 {
        match {
            source-address [ JNCIE-PEG_172.16.60.10/24 JNCIE-PEG_172.16.55.10/24 JNCIE-
PEG_172.16.50.10/24 ];
            destination-address any;
            application any;
        }
        then {
            permit {
                application-services {
                    security-intelligence-policy JNCIE-SEC-TPP;
                    advanced-anti-malware-policy JNCIE-SEC-TPP;
                }
            }
        }
    }
}
```


© 2020 Juniper Networks, Inc. All rights reserved.

Appendix - Super Lab 1

This lab is designed to combine many of the solutions discussed in the previous chapters into a complete practice lab exam. This lab is similar to a real JNCIE-SEC lab exam experience. We recommend attempting this lab if you are able to complete the tasks in the previous chapters without any help.

This walkthrough provides details about the solution for the “Super Lab 1” section of the workbook. Assumption is that the walkthrough of the workbook is completed and understood. The focus of this solution targets on thought strategy and quick perception on how to address prompted tasks.

Structure of document

The construct of this lab tasks focuses on strategy for the real JNCIE exam. It is never enough to emphasize how important it is to read the whole chapter and even the whole exam before starting the configuration of the devices. Here again we can see that several tasks depend on subsequent steps in order to achieve full functionality.

Do not forget that previous tasks may be impacted by configurations performed at later stages. A full revision of the Lab should take place in the end to confirm all tasks are performing according to requirement.

The input commands are sensitive to the prompt tag. Please be aware of the **#** and the **>** signs when checking the snippet. Also consider the device you are inputting the commands; the interpretation section will identify a single or multiple devices and the prompt will either be absent of node identification or explicitly identify where the configuration is being input. In the case of absence, it is the main device the majority of the commands are being input or it is part of multiple devices.

Hierarchical moves are not shown and commit operation is assumed implicit for configuration to become active. Although several tasks show the verification result please bear in mind that such commit and verification may be dependent on other tasks.

The outputs from the devices may been trimmed for the sake of simplicity.

Functionality:

- **You will be able to test functionality of tasks to make sure that your network is operational.**
- **The VR device bears necessary routing instances to emulate all end devices**

© 2020 Juniper Networks, Inc. All rights reserved.

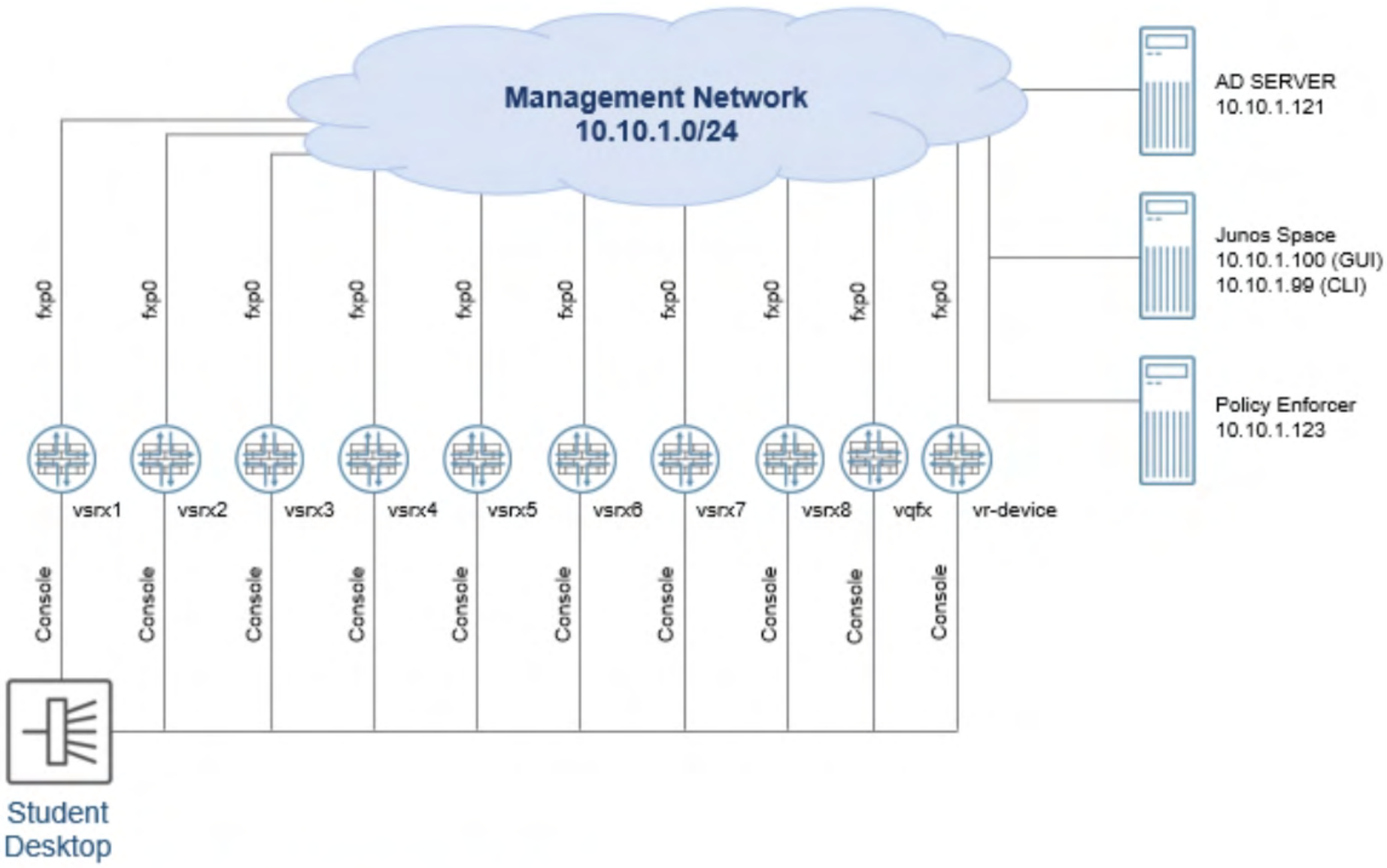


Figure 1: Super Lab 1 – Management Topology

Ensure you load the initial configurations on the devices before you start with this LAB. Ensure that you do not forget to load the initial Super Lab 1 configuration on the vr-device.

Tip: Ensure you read whole tasks before starting them.

© 2020 Juniper Networks, Inc. All rights reserved.

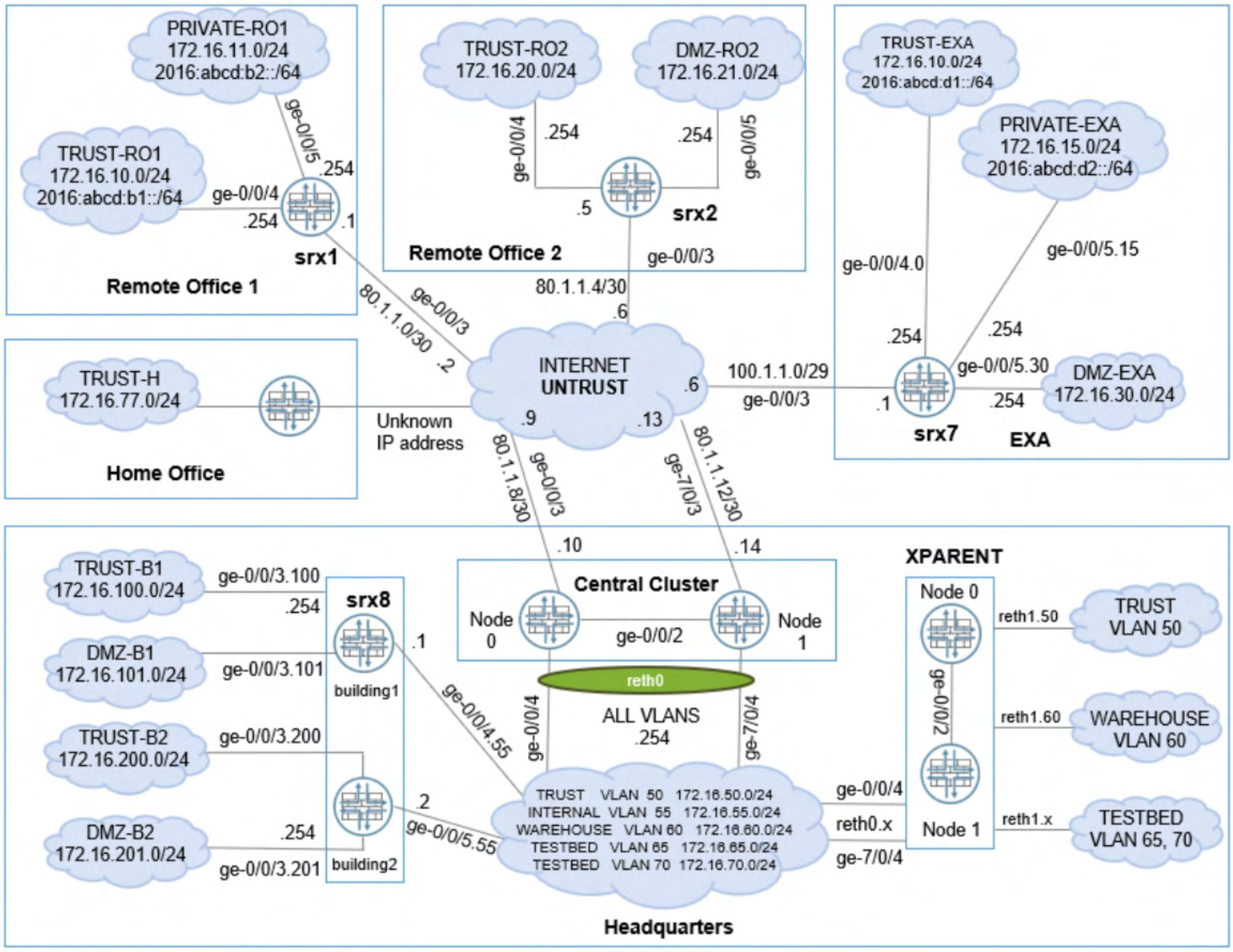


Figure 2: Super Lab 1 Topology

© 2020 Juniper Networks, Inc. All rights reserved.

Task 1: Initial Configuration – Part 1

In this part you will configure the device hostnames, high-availability (cluster) and management interfaces.

1) The table below lists the device hostnames mapping:

Device	Hostname
srx1	roffice1
srx2	roffice2
srx3	central-node0
srx4	central-node1
srx5	xparent-node0
srx6	xparent-node1
srx7	exa-fw
srx8	Building

```
lab@srx1# set system host-name roffice1
commit
[edit]
lab@roffice1#
```

2) Create clusters as defined in the following table:

Device	Node ID	Cluster ID
central-node0	0	1
central-node1	1	1
xparent-node0	0	2
xparent-node1	1	2

3) Ensure ge-0/0/2 is used for the fabric link.

Central nodes:

```
lab@central-node0# run set chassis cluster cluster-id 1 node 0 reboot
Successfully enabled chassis cluster. Going to reboot now.

lab@central-node1# run set chassis cluster cluster-id 1 node 1 reboot
Successfully enabled chassis cluster. Going to reboot now.
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
{primary:node0}
lab@central-node0>
delete system hostname
delete interfaces fxp0
set groups node0 system host-name central-node0
set groups node0 interfaces fxp0 unit 0 family inet address 10.10.1.3/24
set groups node1 system host-name central-node1
set groups node1 interfaces fxp0 unit 0 family inet address 10.10.1.4/24
set apply-groups "${node}"
set interfaces fab0 fabric-options member-interfaces ge-0/0/2
set interfaces fab1 fabric-options member-interfaces ge-7/0/2
```

xparent nodes:

```
lab@xparent-node0# run set chassis cluster cluster-id 2 node 0 reboot
Successfully enabled chassis cluster. Going to reboot now.

lab@xparent-node1# run set chassis cluster cluster-id 2 node 1 reboot
Successfully enabled chassis cluster. Going to reboot now.
```

After the reboot configure the fab links and management

```
{primary:node0}[edit]
lab@xparent-node0#
delete system hostname
delete interfaces fxp0
set groups node0 system host-name xparent-node0
set groups node0 interfaces fxp0 unit 0 family inet address 10.10.1.5/24
set groups node1 system host-name xparent-node1
set groups node1 interfaces fxp0 unit 0 family inet address 10.10.1.6/24
set apply-groups "${node}"
set interfaces fab0 fabric-options member-interfaces ge-0/0/2
set interfaces fab1 fabric-options member-interfaces ge-7/0/2
```

- Verification

```
> show chassis cluster interfaces | match "(Fabric)|(Control)|(fab)" | except
interfaces
Control link status: Up

Fabric link status: Up
    fab0    ge-0/0/2            Up   / Up
    fab0
    fab1    ge-7/0/2            Up   / Up
    fab1
```


© 2020 Juniper Networks, Inc. All rights reserved.

4) The routing engine of xparent cluster needs to be active on node 0
5) Configure the redundant ethernet interfaces according the figure 2.
6) Clusters should operate in the following manner:
    a. Central cluster redundancy groups mapped to interfaces dependent on physical links, need to be active on node0 whenever node0 is available
        i. Any failure from correspondent child interface triggers the failover
    b. Central cluster redundancy groups (RGs) mapped to interfaces dependent on logical links, need to be active on node1 whenever node1 is available
        i. Uplink interface monitoring triggers the failover
    c. The Central Cluster needs to monitor ICMP reachability to the host address (12.34.56.78) available in the Internet. In case this reachability is compromised, the test's uplink interface should be brought down so that the RG fails over.
        i. Probe threshold should be between 30 and 60 seconds
        ii. Control plane redundancy group needs to follow the same faith of the RG from point 6.b
    d. All xparent cluster redundancy groups need to be active on node 0 and should automatically failover in case any of its physical links fail.
        i. No need for automatic recovery of primacy

Note: Where the SRX cluster is the end point, all services need to be directed to a interface that depends on Redundant Groups. Since this setup has two physical interfaces connecting to the service provider environment, we need to terminate all services that may be arriving from those interfaces in such a logical interface.

Note: The task differentiates redundancy groups mapped to redundant interfaces which bear physical links or logical interfaces that may have redundancy group dependency. In the SRX cluster the loopback interface is such logical interface which by default is part of RG0.

```
>show chassis cluster interfaces | find Redundant-pseudo
Redundant-pseudo-interface Information:
```

Central-node:

```
set interfaces reth0 vlan-tagging
set interfaces reth0 redundant-ether-options redundancy-group 1
set interfaces reth0 unit 50 vlan-id 50
set interfaces reth0 unit 50 family inet address 172.16.50.254/24
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
set interfaces reth0 unit 50 family inet6 address 2016:abcd:a1::254/64
set interfaces reth0 unit 55 vlan-id 55
set interfaces reth0 unit 55 family inet address 172.16.55.254/24
set interfaces reth0 unit 60 vlan-id 60
set interfaces reth0 unit 60 family inet address 172.16.60.254/24
set interfaces reth0 unit 65 vlan-id 65
set interfaces reth0 unit 65 family inet address 172.16.65.254/24
set interfaces reth0 unit 70 vlan-id 70
set interfaces reth0 unit 70 family inet address 172.16.70.254/24
set interfaces ge-0/0/4 gigether-options redundant-parent reth0
set chassis cluster reth-count 4
set chassis cluster redundancy-group 0 node 0 priority 1
set chassis cluster redundancy-group 0 node 1 priority 100
set chassis cluster redundancy-group 1 node 0 priority 100
set chassis cluster redundancy-group 1 node 1 priority 1
set chassis cluster redundancy-group 1 preempt
set chassis cluster redundancy-group 1 interface-monitor ge-0/0/4 weight 255
set chassis cluster redundancy-group 1 interface-monitor ge-7/0/4 weight 255
set chassis cluster redundancy-group 2 node 0 priority 1
set chassis cluster redundancy-group 2 node 1 priority 100
set chassis cluster redundancy-group 2 preempt
```

Configure the RPM probe and the ip-monitoring policy:

```
set services rpm probe ping-9 test icmp probe-type icmp-ping
set services rpm probe ping-9 test icmp target address 12.34.56.78
set services rpm probe ping-9 test icmp probe-count 3
set services rpm probe ping-9 test icmp probe-interval 5
set services rpm probe ping-9 test icmp test-interval 15
set services rpm probe ping-9 test icmp thresholds successive-loss 3
set services rpm probe ping-9 test icmp thresholds total-loss 3
set services rpm probe ping-9 test icmp next-hop 80.1.1.9
set services rpm probe ping-13 test icmp probe-type icmp-ping
set services rpm probe ping-13 test icmp target address 12.34.56.78
set services rpm probe ping-13 test icmp probe-count 3
set services rpm probe ping-13 test icmp probe-interval 5
set services rpm probe ping-13 test icmp test-interval 15
set services rpm probe ping-13 test icmp thresholds successive-loss 3
set services rpm probe ping-13 test icmp thresholds total-loss 3
set services rpm probe ping-13 test icmp next-hop 80.1.1.13
set services ip-monitoring policy ping-9 match rpm-probe ping-9
set services ip-monitoring policy ping-9 then interface ge-0/0/3 disable
set services ip-monitoring policy ping-13 match rpm-probe ping-13
set services ip-monitoring policy ping-13 then interface ge-7/0/3 disable
```

Note: You cannot verify this step until the uplink interfaces towards the UNTRUST/ INTERNET are configured and the EBGP sessions are established.

© 2020 Juniper Networks, Inc. All rights reserved.

Xparent node:

Note: By adding the following configuration the XPARENT cluster is going to change from route to transparent mode. For this reason, a reboot is required.

```
set interfaces reth0 vlan-tagging
set interfaces reth0 redundant-ether-options redundancy-group 1
set interfaces reth0 unit 50 family ethernet-switching interface-mode trunk
set interfaces reth0 unit 50 family ethernet-switching vlan members vlan50
set interfaces reth0 unit 60 family ethernet-switching interface-mode trunk
set interfaces reth0 unit 60 family ethernet-switching vlan members vlan60
set interfaces reth0 unit 65 family ethernet-switching interface-mode trunk
set interfaces reth0 unit 65 family ethernet-switching vlan members vlan65
set interfaces reth0 unit 70 family ethernet-switching interface-mode trunk
set interfaces reth0 unit 70 family ethernet-switching vlan members vlan70
set interfaces reth1 vlan-tagging
set interfaces reth1 redundant-ether-options redundancy-group 1
set interfaces reth1 unit 50 family ethernet-switching interface-mode trunk
set interfaces reth1 unit 50 family ethernet-switching vlan members vlan50
set interfaces reth1 unit 60 family ethernet-switching interface-mode trunk
set interfaces reth1 unit 60 family ethernet-switching vlan members vlan60
set interfaces reth1 unit 65 family ethernet-switching interface-mode trunk
set interfaces reth1 unit 65 family ethernet-switching vlan members vlan65
set interfaces reth1 unit 65 family ethernet-switching vlan-rewrite translate 165 65
set interfaces reth1 unit 70 family ethernet-switching interface-mode trunk
set interfaces reth1 unit 70 family ethernet-switching vlan members vlan70
set interfaces reth1 unit 70 family ethernet-switching vlan-rewrite translate 170 70

set interfaces ge-0/0/3 gigether-options redundant-parent reth1
set interfaces ge-0/0/4 gigether-options redundant-parent reth0

set chassis cluster reth-count 2
set chassis cluster redundancy-group 0 node 0 priority 100
set chassis cluster redundancy-group 0 node 1 priority 1
set chassis cluster redundancy-group 1 node 0 priority 100
set chassis cluster redundancy-group 1 node 1 priority 1
set chassis cluster redundancy-group 1 interface-monitor ge-7/0/4 weight 255
set chassis cluster redundancy-group 1 interface-monitor ge-0/0/4 weight 255
set interfaces ge-7/0/4 gigether-options redundant-parent reth0
set vlans vlan50 vlan-id 50
set vlans vlan60 vlan-id 60
set vlans vlan65 vlan-id 65
set vlans vlan70 vlan-id 70

lab@xparent-node0# commit warning: Interfaces are changed from route mode to transparent mode.
Please reboot the device or all nodes in the HA cluster!

node0:
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
configuration check succeeds
node1:
warning: Interfaces are changed from route mode to transparent mode. Please reboot the device
or all nodes in the HA cluster!
commit complete
node0:
commit complete

lab@ xparent-node0# run request system reboot
Reboot the system ? [yes,no] (no) yes
```

7) Configure the management interfaces (figure 1) as defined in the table below:

Device	Management IP address
roffice1	10.10.1.1/24
roffice2	10.10.1.2/24
central-node0	10.10.1.3/24
central-node1	10.10.1.4/24
xparent-node0	10.10.1.5/24
xparent-node1	10.10.1.6/24
exa-fw	10.10.1.7/24
building	10.10.1.8/24

This task should not require any configuration for non-cluster devices as the management addresses are preconfigured in the initial configurations. This task is to ensure all management addresses are correctly configured.

8) Configure the management interfaces (Figure 1) as defined in the table below:

a. Will accept only specific services as defined in the table below.

Device	Services
roffice1	SSH with root access (session limit 3), HTTPS
roffice2	SSH with root access (session limit 3), HTTPS
central	SSH with root access (session limit 3), HTTPS
xparent	SSH with root access (session limit 3), HTTPS
building	SSH with root access (session limit 3), HTTPS
exa-fw	SSH with root access (session limit 3), HTTPS

© 2020 Juniper Networks, Inc. All rights reserved.

All devices:

```
set system services ssh root-login allow
set system services ssh connection-limit 3
set system services web-management https system-generated-certificate
```

Verification

```
roffice1> telnet 10.10.1.2 port 22
Trying 10.10.1.2...
Connected to 10.10.1.2.
Escape character is '^]'.
SSH-2.0-OpenSSH_6.6

roffice1> telnet 10.10.1.2 port 443
Trying 10.10.1.2...
Connected to 10.10.1.2.
Escape character is '^]'.
```

Task 2: Initial Configuration - Part 2

In this part you will configure authentication, authorization, Syslog, SNMP and NTP parameters.

1) Configure users as defined in the table below:

Username	Password	Device	Privileges
ronly	ronly123	All	Has permission “view” and “view-configuration”. Additionally, can NOT execute the “file delete” command and view the [edit system login] configuration hierarchy.
admin1	admin123	All	Has permissions “all”. But is not allowed to reboot the device.
restricted	restricted123	All	Has permissions “clear” and can execute only the “show system users” and “show interface terse” commands and nothing else.
lab	lab123	All	super-user

© 2020 Juniper Networks, Inc. All rights reserved.

All devices:

```
set system login class admin permissions all
set system login class admin deny-commands "request system reboot"
set system login class restricted permissions clear
set system login class restricted allow-commands "(show system users)|(show interfaces terse)"
set system login class ronly permissions view
set system login class ronly permissions view-configuration
set system login class ronly deny-commands "file delete"
set system login class ronly deny-configuration "system login"
set system login user admin1 uid 2007
set system login user admin1 class admin
set system login user admin1 authentication encrypted-password
"$1$2Ufc.UpI$s/SmYOgJSv33V5HlhwOqO1"
set system login user lab uid 2009
set system login user lab class super-user
set system login user lab authentication encrypted-password
"$1$hfW4uwbb$C5GrqK6JMX/y2o54.1jWz0"
set system login user restricted uid 2010
set system login user restricted class restricted
set system login user restricted authentication encrypted-password
"$1$XuzfeAyb$PVeSVjo2Y5Jgc6WFh6Hhm."
set system login user ronly uid 2015
set system login user ronly class ronly
set system login user ronly authentication encrypted-password
"$1$JsllqvQw$a/vER20W/pfwUPGHAfdtT1"
```

2) Ensure that all devices have the following SYSLOG configuration.
    h. All “emergency” messages are displayed on terminals of all currently logged users.
    i. Only all “critical” and higher severity messages are sent to the default syslog file.
    j. “interactive-commands” file keeps the audit trail of the users and commands they execute.
    k. File named “security-policy-logs” will contain security policy log entries. The system should retain 20 archive files with size of 512 KB (524288 B).
    l. “authorization-file” stores authorization messages with the severity “info” and higher.
    m. Following messages are sent to the syslog server at 10.10.1.99.
        v. All “emergency” messages
        vi. Authorization messages with severity “info” and higher
3) The syslog messages should contain year and milliseconds information.

All devices:

```
set system syslog user * any emergency
set system syslog host 10.10.1.99 any emergency
set system syslog host 10.10.1.99 authorization info
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
set system syslog file messages any critical
set system syslog file interactive-commands interactive-commands any
set system syslog file security-policy-logs user info
set system syslog file security-policy-logs match RT_FLOW
set system syslog file security-policy-logs archive size 512k
set system syslog file security-policy-logs archive files 20
set system syslog file authorization-file authorization any
set system syslog file ssl-proxy any any
set system syslog file ssl-proxy match SSL
set system syslog time-format year
set system syslog time-format millisecond
```

4) Ensure that all devices will synchronize their time with the NTP server reachable at 10.10.1.254.
5) The devices have to use this server's time also during booting.
6) The time zone is set to America/Los_Angeles.

```
set system ntp boot-server 10.10.1.254
set system ntp server 10.10.1.254
set system ntp trusted-key 1
set system time-zone America/Los_Angeles
```

7) All devices have to accept read-only SNMP requests only from the NMS system located at 10.10.1.20. The community string is "**roaccess**".
8) All devices have to send SNMP traps to the NMS system for following events:
    e. Authentication failures
    f. Hardware and environment
    g. Link transitions
    h. Routing protocol
9) The exa-fw device has to send the authentication failures to a specific monitoring system (10.10.10.50), which runs SNMP version 1 and listens on port 12345.
10) The devices should accept read-write SNMP requests from the network 10.10.199.0/24 except 10.10.199.199. The read-write community string is "snmpRWaccess".
11) All devices need to have defined following locations details:
    a. SNMP contact "**JNCIE admin**"
    b. SNMP description "**JNCIE-SEC device**"
    c. SNMP location "**Rack**"
    d. System location (not in the SNMP configuration): rack number **1**, floor **1**, country-code **NL**.
12) Configure all vSRX devices to accept SNMP requests from Junos Space located at 10.10.1.121 using the community string "JNCIE"

All devices:

```
set system location country-code UK
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
set system location floor 1
set system location rack 1
set snmp description "JNCIE-SEC device"
set snmp location Rack
set snmp contact "JNCIE admin"
set snmp view all oid .1
set snmp community roaccess view all
set snmp community roaccess authorization read-only
set snmp community roaccess clients 10.10.1.20/32
set snmp community snmpRWaccess clients 10.10.199.0/24
set snmp community snmpRWaccess clients 10.10.199.199/32 restrict
set snmp community JNCIE
set snmp trap-group sl categories authentication
set snmp trap-group sl categories chassis
set snmp trap-group sl categories link
set snmp trap-group sl categories routing
set snmp trap-group sl categories chassis-cluster
set snmp trap-group sl targets 10.10.1.20
set snmp trap-group space targets 10.10.1.121
```

13) Firewall filters must protect all device's control planes in the way described below
    a. Where applicable ensure that any traffic originated from st0 interfaces is accepted.
    b. Permit DNS, NTP, SNMP, HTTPS and SSH traffic originated from subnets 10/8, 172.16/16, 2016:abcd::/32 and loopback interfaces.
    c. Ensure that ICMPv4 traffic is rate limited to 256kbps with traffic burst of 100k.
    d. Discard and syslog traffic with the protocols from 'step 14.b' from all other networks.
    e. Allow and count any other traffic from exercises where a new term is required.
    f. Silently drop all other traffic.

Note: The firewall filter is a constant point of focus to bear in mind when troubleshooting is involved. Always make sure you update and evaluate your statement along with adding counters to traffic denial rules so that you understand if the firewall filter may be blocking interesting traffic.

As Roffice 1 and EXA both perform IPv6 routing you must also enable IPv6 control plane protection on these devices.

Roffice1:

```
[edit]
lab@roffice1# show policy-options prefix-list mgmt
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
10.0.0.0/8;
172.16.0.0/16;
192.168.1.1/32;
[edit]
lab@roffice1# show firewall
family inet {
    filter RE-PROTECT-v4 {
        term IFD {
            from {
                interface st0;
            }
            then accept;
        }
        term PORT-UDP {
            from {
                source-prefix-list {
                    mgmt;
                }
                protocol udp;
                port [ domain ntp ];
            }
            then accept;
        }
        term LOG-UDP {
            from {
                protocol udp;
                port [ domain ntp ];
            }
            then {
                count LOG-UDP;
                discard;
            }
        }
        term PORT-TCP {
            from {
                source-prefix-list {
                    mgmt;
                }
                protocol tcp;
                destination-port [ https ssh ];
            }
            then accept;
        }
        term LOG-TCP {
            from {
                protocol tcp;
                destination-port [ https ssh ];
            }
            then {
                count LOG-TCP;
                discard;
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
        }
    }
    term ICMP {
        from {
            protocol icmp;
        }
        then {
            policer ICMP-POLICER;
            accept;
        }
    }
    term SNMP {
        from {
            source-prefix-list {
                mgmt;
            }
            port [ snmp snmptrap ];
        }
        then {
            count SNMP;
            accept;
        }
    }
    term IKE {
        from {
            port 500;
        }
        then {
            count IKE;
            accept;
        }
    }
}
family inet6 {
    filter RE-PROTECT-v6 {
        term IFD {
            from {
                interface st0;
            }
            then accept;
        }
        term SRC-ALLOW {
            from {
                source-address {
                    2016:abcd::/32;
                }
                source-port [ domain ntp ];
            }
            then accept;
        }
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
term SRC-DENY {
    from {
        source-port [ domain ntp ];
    }
    then count SRC-DENY;
}
term DST-ALLOW {
    from {
        source-address {
            2016:abcd::/32;
        }
        destination-port [ https ssh ];
    }
        then accept;
    }
    term DST-DENY {
        from {
            destination-port [ https ssh ];
        }
        then count DST-DENY;
    }
    term ICMP {
        from {
            icmp-type [ echo-reply echo-request destination-unreachable neighbor-
advertisement neighbor-solicit time-exceeded ];
        }
        then accept;
    }
}
policer ICMP-POLICER {
    if-exceeding {
        bandwidth-limit 256k;
        burst-size-limit 100k;
    }
    then discard;
}

[edit]
lab@roffice1# show interfaces lo0
unit 0 {
    family inet {
        filter {
            input RE-PROTECT-v4;
        }
        address 192.168.1.1/32;
    }
    family inet6 {
        filter {
            input RE-PROTECT-v6;
        }
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
        address 2016:abcd:ffff::2/128;
    }
}
```

ROFFICE2:

```
[edit]
lab@roffice2# show policy-options prefix-list mgmt
10.0.0.0/8;
172.16.0.0/16;
192.168.1.2/32;
```

```
[edit]
lab@roffice2# show firewall | no-more
family inet {
    filter RE-PROTECT-v4 {
        term IFD {
            from {
                interface st0;
            }
            then accept;
        }
        term PORT-UDP {
            from {
                source-prefix-list {
                    mgmt;
                }
                protocol udp;
                port [ domain ntp ];
            }
            then accept;
        }
        term LOG-UDP {
            from {
                protocol udp;
                port [ domain ntp ];
            }
            then {
                count LOG-UDP;
                discard;
            }
        }
    term PORT-TCP {
        from {
            source-prefix-list {
                mgmt;
            }
            protocol tcp;
            destination-port [ https ssh ];
        }
        then accept;
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
}
term LOG-TCP {
    from {
        protocol tcp;
        destination-port [ https ssh ];
    }
    then {
        count LOG-TCP;
        discard;
    }
}
term ICMP {
    from {
        protocol icmp;
    }
    then {
        policer ICMP-POLICER;
        accept;
    }
}
term SNMP {
    from {
        source-prefix-list {
            mgmt;
        }
        port [ snmp snmptrap ];
    }
    then {
        count SNMP;
        accept;
    }
}
term IKE {
    from {
        port 500;
        }
        then {
            count IKE;
            accept;
        }
    }
}
policer ICMP-POLICER {
    if-exceeding {
        bandwidth-limit 256k;
        burst-size-limit 100k;
    }
    then discard;
}
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
[edit]
lab@roffice2# show interfaces lo0
unit 0 {
    family inet {
        filter {
            input RE-PROTECT-v4;
        }
        address 192.168.1.2/32;
    }
}
```

Central-node:

```
{primary:node0}[edit]
lab@srx3# show policy-options
prefix-list mgmt {
    10.0.0.0/8;
    80.1.1.16/32;
    172.16.0.0/16;
    192.168.1.3/32;
}
prefix-list bgp {
    apply-path "protocols bgp group <*> neighbor <*>";
}
```

```
{primary:node0}[edit]
lab@central-node0# show firewall | no-more
family inet {
    filter RE-PROTECT-v4 {
        term IFD {
            from {
                interface st0;
            }
            then accept;
        }
        term PORT-UDP {
            from {
                source-prefix-list {
                    mgmt;
                }
                protocol udp;
                port [ domain ntp ];
            }
            then accept;
        }
        term LOG-UDP {
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
        from {
            protocol udp;
            port [ domain ntp ];
        }
        then {
            count LOG-UDP;
            discard;
        }
    }
    term PORT-TCP {
        from {
            source-prefix-list {
                mgmt;
            }
            protocol tcp;
            destination-port [ https ssh ];
        }
        then accept;
    }
    term LOG-TCP {
        from {
            protocol tcp;
            destination-port [ https ssh ];
        }
        then {
            count LOG-TCP;
            discard;
        }
    }
    term ICMP {
        from {
            protocol icmp;
        }
        then {
            policer ICMP-POLICER;
            accept;
        }
    }
    term SNMP {
        from {
            source-prefix-list {
                mgmt;
            }
            port [ snmp snmptrap ];
        }
        then {
            count SNMP;
            accept;
        }
    }
    term BGP {
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
        from {
            prefix-list {
                bgp;
            }
            protocol tcp;
            port bgp;
        }
        then {
            count BGP;
            accept;
        }
    }
    term OSPF {
        from {
            protocol ospf;
        }
        then {
            count OSPF;
            accept;
        }
    }
    term IKE {
        from {
            port 500;
        }
        then {
            count IKE;
            accept;
        }
    }
  }
}
policer ICMP-POLICER {
    if-exceeding {
        bandwidth-limit 256k;
        burst-size-limit 100k;
    }
    then discard;
}

{primary:node0}[edit]
lab@central-node0# show interfaces lo0
unit 0 {
    family inet {
        filter {
            input RE-PROTECT-v4;
        }
        address 80.1.1.16/32 {
            primary;
        }
        address 192.168.1.3/32;
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
    }
}
redundant-pseudo-interface-options {
    redundancy-group 2;
}
```

EXA:

```
[edit]
lab@exa-fw# show policy-options
prefix-list mgmt {
    10.0.0.0/8;
    172.16.0.0/16;
    192.168.1.5/32;
}
prefix-list vpn {
    80.1.1.5/32;
    80.1.1.16/32;
    100.1.1.1/32;
    200.1.1.100/32;
}

[edit]
lab@exa-fw# show firewall | no-more
family inet {
    filter RE-PROTECT-v4 {
        term IFD {
            from {
                interface st0;
            }
            then accept;
        }
        term PORT-UDP {
            from {
                source-prefix-list {
                    mgmt;
                }
                protocol udp;
                port [ domain ntp ];
            }

            then accept;
        }
        term LOG-UDP {
            from {
                protocol udp;
                port [ domain ntp ];
            }
            then {
                count LOG-UDP;
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
        discard;
    }
}
term PORT-TCP {
    from {
        source-prefix-list {
            mgmt;
        }
        protocol tcp;
        destination-port [ https ssh ];
    }
    then accept;
}
term LOG-TCP {
    from {
        protocol tcp;
        destination-port [ https ssh ];
    }
    then {
        count LOG-TCP;
        discard;
    }
}
term ICMP {
    from {
        protocol icmp;
    }
    then {
        policer ICMP-POLICER;
        accept;
    }
}
term SNMP {
    from {
        source-prefix-list {
            mgmt;
        }
        port [ snmp snmptrap ];
    }
    then {
        count SNMP;
        accept;
    }
}
term IKE {
    from {
        port 500;
    }
    then {
        count IKE;
        accept;
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
            }
        }
    }
}
family inet6 {
    filter RE-PROTECT-v6 {
        term IFD {
            from {
                interface st0;
                interface st0.1;
            }
            then accept;
        }
        term SRC-ALLOW {
            from {
                source-address {
                    2016:abcd::/32;
                }
                source-port [ domain ntp ];
            }
            then accept;
        }
        term SRC-DENY {
            from {
                source-port [ domain ntp ];
            }
            then count SRC-DENY;
        }
        term DST-ALLOW {
            from {
                source-address {
                    2016:abcd::/32;
                }
                destination-port [ https ssh ];
            }
            then accept;
        }
        term DST-DENY {
            from {
                destination-port [ https ssh ];
            }
            then count DST-DENY;
        }
        term ICMP {
            from {
                icmp-type [ echo-reply echo-request destination-unreachable neighbor-
advertisement neighbor-solicit time-exceeded ];
            }
            then accept;
        }
    }
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
}
policer ICMP-POLICER {
    if-exceeding {
        bandwidth-limit 256k;
        burst-size-limit 100k;
    }
    then discard;
}

[edit]
lab@exa-fw# show interfaces lo0
unit 0 {
    family inet {
        filter {
            input RE-PROTECT-v4;
        }
        address 192.168.1.5/32;
    }
    family inet6 {
        filter {
            input RE-PROTECT-v6;
        }
        address 2016:abcd:ffff::4/128;
    }
}
```

XPARENT

```
{primary:node0}[edit]
lab@xparent-node0# show policy-options prefix-list mgmt
10.0.0.0/8;
172.16.0.0/16;

{primary:node0}[edit]
lab@xparent-node0# show firewall | no-more
family inet {
    filter RE-PROTECT-v4 {
        term IFD {
            from {
                interface st0;
            }
            then accept;
        }
        term PORT-UDP {
            from {
                source-prefix-list {
                    mgmt;
                }
                protocol udp;
                port [ domain ntp ];
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
        }
        then accept;
    }
    term LOG-UDP {
        from {
            protocol udp;
            port [ domain ntp ];
        }
        then {
            count LOG-UDP;
            discard;
        }
    }
    term PORT-TCP {
        from {
            source-prefix-list {
                mgmt;
            }
            protocol tcp;
            destination-port [ https ssh ];
        }
        then accept;
    }
    term LOG-TCP {
        from {
            protocol tcp;
            destination-port [ https ssh ];
        }
        then {
            count LOG-TCP;
            discard;
        }
    }
    term ICMP {
        from {
            protocol icmp;
        }
        then {
            policer ICMP-POLICER;
            accept;
        }
    }
    term SNMP {
        from {
            source-prefix-list {
                mgmt;
            }
            port [ snmp snmptrap ];
        }
        then {
            count SNMP;
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
                accept;
            }
        }
    }
}
policer ICMP-POLICER {
    if-exceeding {
        bandwidth-limit 256k;
        burst-size-limit 100k;
    }
    then discard;
}
```

```
{primary:node0}[edit]
lab@xparent-node0# show interfaces lo0
unit 0 {
    family inet {
        filter {
            input RE-PROTECT-v4;
        }
    }
}
```

Building

```
[edit]
lab@building# show policy-options prefix-list mgmt
10.0.0.0/8;
172.16.0.0/16;
```

```
[edit]
lab@building# show firewall | no-more
family inet {
    filter RE-PROTECT-v4 {
        term IFD {
            from {
                interface st0;
            }
            then accept;
        }
        term PORT-UDP {
            from {
                source-prefix-list {
                    mgmt;
                }
                protocol udp;
                port [ domain ntp ];
            }
            then accept;
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
}
term LOG-UDP {
    from {
        protocol udp;
        port [ domain ntp ];
    }
    then {
        count LOG-UDP;
        discard;
    }
}
term PORT-TCP {
    from {
        source-prefix-list {
            mgmt;
        }
        protocol tcp;
        destination-port [ https ssh ];
    }
    then accept;
}
term LOG-TCP {
    from {
        protocol tcp;
        destination-port [ https ssh ];
    }
    then {
        count LOG-TCP;
        discard;
    }
}
term ICMP {
    from {
        protocol icmp;
    }
    then {

        policer ICMP-POLICER;
        accept;
    }
}
term SNMP {
    from {
        source-prefix-list {
            mgmt;
        }
        port [ snmp snmptrap ];
    }
    then {
        count SNMP;
        accept;
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
            }
        }
    }
}
policer ICMP-POLICER {
    if-exceeding {
        bandwidth-limit 256k;
        burst-size-limit 100k;
    }
    then discard;
}

[edit]
lab@building# show interfaces lo0
unit 0 {
    family inet {
        filter {
            input RE-PROTECT-v4;
        }
    }
}
unit 1 {
    family inet {
        address 192.168.1.6/32;
    }
}
unit 2 {
    family inet {
        address 192.168.1.7/32;
    }
}
```

Task 3: Interfaces, Zones, Local Traffic, Routing, and Routing Instances

This part is focused on the interfaces, security zones, local traffic handling, routing, routing instance segregation and device operation configurations

1) Configure interfaces and security zones on individual devices as follows:

Device	Interface	IP address	VLAN-D	Zone
roffice1	lo0.0	192.168.1.1/32	-	UNTRUST
roffice1	ge-0/0/3	80.1.1.1/30	-	UNTRUST
roffice1	ge-0/0/4	172.16.10.254/24	-	TRUST-RO1
roffice1	ge-0/0/5	172.16.11.254/24	-	PRIVATE-RO1
roffice2	lo0.0	192.168.1.2/32	-	UNTRUST

© 2020 Juniper Networks, Inc. All rights reserved.

roffice2	ge-0/0/3	80.1.1.5/30	-	UNTRUST
roffice2	ge-0/0/4	172.16.20.254/24	-	TRUST-RO2
roffice2	ge-0/0/5	172.16.21.254/24	-	DMZ-RO2
central	lo0.0	192.168.1.3/32, 80.1.1.16/32	-	UNTRUST
central	ge-0/0/3	80.1.1.10/30	-	UNTRUST
central	ge-7/0/3	80.1.1.14/30	-	UNTRUST
central	reth0.50	172.16.50.254/24	50	TRUST
central	reth0.55	172.16.55.254/24	55	INTERNAL
central	reth0.60	172.16.60.254/24	60	WAREHOUSE
central	reth0.65	172.16.65.254/24	65	TESTBED
central	reth0.70	172.16.70.254/24	70	TESTBED
xparent	reth0.50	-	50	TRUST
xparent	reth0.60	-	60	WAREHOUSE
xparent	reth0.65	-	65	TESTBED
xparent	reth0.70	-	70	TESTBED
xparent	reth1.50	-	50	TRUST
xparent	reth1.60	-	60	WAREHOUSE
xparent	reth1.65	-	65	TESTBED
xparent	reth1.70	-	70	TESTBED
building1	lo0.1	192.168.1.6/32	-	INTERNAL-B1
building1	ge-0/0/3.100	172.16.100.254/24	100	TRUST-B1
building1	ge-0/0/3.101	172.16.101.254/24	101	DMZ-B1
building1	ge-0/0/4.55	172.16.55.1/24	55	INTERNAL-B1
building2	lo0.2	192.168.1.7/32	-	INTERNAL-B2
building2	ge-0/0/3.200	172.16.200.254/24	200	TRUST-B2
building2	ge-0/0/3.201	172.16.201.254/24	201	DMZ-B2
building2	ge-0/0/5.55	172.16.55.2/24	55	INTERNAL-B2
exa-fw	lo0.0	192.168.1.8/32	-	UNTRUST
exa-fw	ge-0/0/3	100.1.1.1/29	-	UNTRUST
exa-fw	ge-0/0/4	172.16.10.254/24	-	TRUST-EXA
exa-fw	ge-0/0/5.15	172.16.15.254/24	15	PRIVATE-EXA

© 2020 Juniper Networks, Inc. All rights reserved.

exa-fw	ge-0/0/5.30	172.16.30.254/24	30	DMZ-EXA

2) Ping to the security devices themselves must be allowed on all interfaces.
3) SSH connections are accepted on all TRUST zone interfaces.
4) On the devices roffice1, roffice2 and exa-fw create a default static route pointing to the UNTRUST network.
5) Use static routes on central cluster to provide connectivity to building's networks
6) On the building device (srx8) create two virtual-router routing-instances named building1 and building2, associate the interfaces of each building accordingly and create a default static route pointing to the correct VLAN interface on the central cluster.
7) Configure VLAN rewriting rules on xparent device:
    a. Interface reth1 – vlan-id 165 to vlan-id 65
    b. Interface reth1 – vlan-id 170 to vlan-id 70

Roffice1:

```
set interfaces ge-0/0/3 unit 0 family inet address 80.1.1.1/30
set interfaces ge-0/0/4 vlan-tagging
set interfaces ge-0/0/4 unit 0 vlan-id 110
set interfaces ge-0/0/4 unit 0 family inet address 172.16.10.254/24
set interfaces ge-0/0/4 unit 0 family inet6 address 2016:abcd:b1::254/64
set interfaces ge-0/0/5 vlan-tagging
set interfaces ge-0/0/5 unit 0 vlan-id 111
set interfaces ge-0/0/5 unit 0 family inet address 172.16.11.254/24
set interfaces ge-0/0/5 unit 0 family inet6 address 2016:abcd:b2::254/64
set interfaces fxp0 unit 0 family inet address 10.10.1.1/24
set interfaces lo0 unit 0 family inet filter input RE-PROTECT-v4
set interfaces lo0 unit 0 family inet address 192.168.1.1/32
set interfaces lo0 unit 0 family inet6 filter input RE-PROTECT-v6
set interfaces lo0 unit 0 family inet6 address 2016:abcd:ffff::2/128
set security zones security-zone UNTRUST host-inbound-traffic system-services ping
set security zones security-zone UNTRUST interfaces ge-0/0/3.0
set security zones security-zone UNTRUST interfaces lo0.0
set security zones security-zone TRUST-RO1 host-inbound-traffic system-services ping
set security zones security-zone TRUST-RO1 host-inbound-traffic system-services ssh
set security zones security-zone TRUST-RO1 interfaces ge-0/0/4.0
set security zones security-zone PRIVATE-RO1 host-inbound-traffic system-services ping
set security zones security-zone PRIVATE-RO1 interfaces ge-0/0/5.0
```

Roffice2:

```
set security zones security-zone UNTRUST host-inbound-traffic system-services ping
set security zones security-zone UNTRUST host-inbound-traffic system-services ike
set security zones security-zone UNTRUST interfaces lo0.0
set security zones security-zone UNTRUST interfaces ge-0/0/3.0
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
set security zones security-zone TRUST-RO2 host-inbound-traffic system-services ping
set security zones security-zone TRUST-RO2 host-inbound-traffic system-services ssh
set security zones security-zone TRUST-RO2 interfaces ge-0/0/4.0
set security zones security-zone DMZ-RO2 host-inbound-traffic system-services ping
set security zones security-zone DMZ-RO2 interfaces ge-0/0/5.0
set interfaces ge-0/0/3 unit 0 family inet address 80.1.1.5/30
set interfaces ge-0/0/4 vlan-tagging
set interfaces ge-0/0/4 unit 0 vlan-id 210
set interfaces ge-0/0/4 unit 0 family inet address 172.16.20.254/24
set interfaces ge-0/0/5 vlan-tagging
set interfaces ge-0/0/5 unit 0 vlan-id 211
set interfaces ge-0/0/5 unit 0 family inet address 172.16.21.254/24
set interfaces fxp0 unit 0 family inet address 10.10.1.2/24
set interfaces lo0 unit 0 family inet filter input RE-PROTECT-v4
set interfaces lo0 unit 0 family inet address 192.168.1.2/32
```

Central-node:

```
set interfaces ge-0/0/3 unit 0 family inet address 80.1.1.10/30
set interfaces ge-0/0/3 unit 0 family inet6 address 2016:abcd::a/126
set interfaces ge-0/0/4 gigether-options redundant-parent reth0
set interfaces ge-7/0/3 unit 0 family inet address 80.1.1.14/30
set interfaces ge-7/0/3 unit 0 family inet6 address 2016:abcd::e/126
set interfaces ge-7/0/4 gigether-options redundant-parent reth0
set interfaces fab0 fabric-options member-interfaces ge-0/0/2
set interfaces fab1 fabric-options member-interfaces ge-7/0/2
set interfaces lo0 unit 0 family inet filter input RE-PROTECT-v4
set interfaces lo0 unit 0 family inet address 80.1.1.16/32 primary
set interfaces lo0 unit 0 family inet address 192.168.1.3/32
set interfaces lo0 redundant-pseudo-interface-options redundancy-group 2
set interfaces reth0 vlan-tagging
set interfaces reth0 redundant-ether-options redundancy-group 1
set interfaces reth0 unit 50 vlan-id 50
set interfaces reth0 unit 50 family inet address 172.16.50.254/24
set interfaces reth0 unit 50 family inet6 address 2016:abcd:a1::254/64
set interfaces reth0 unit 55 vlan-id 55
set interfaces reth0 unit 55 family inet address 172.16.55.254/24
set interfaces reth0 unit 60 vlan-id 60
set interfaces reth0 unit 60 family inet address 172.16.60.254/24
set interfaces reth0 unit 65 vlan-id 65
set interfaces reth0 unit 65 family inet address 172.16.65.254/24
set interfaces reth0 unit 70 vlan-id 70
set interfaces reth0 unit 70 family inet address 172.16.70.254/24

set security zones security-zone UNTRUST host-inbound-traffic system-services ping
set security zones security-zone UNTRUST host-inbound-traffic protocols bgp
set security zones security-zone UNTRUST interfaces lo0.0 host-inbound-traffic system-services
ike
set security zones security-zone UNTRUST interfaces lo0.0 host-inbound-traffic system-services
ping
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
set security zones security-zone UNTRUST interfaces lo0.0 host-inbound-traffic protocols ldp
set security zones security-zone UNTRUST interfaces lo0.0 host-inbound-traffic protocols bgp
set security zones security-zone UNTRUST interfaces ge-0/0/3.0
set security zones security-zone UNTRUST interfaces ge-7/0/3.0
set security zones security-zone TRUST host-inbound-traffic system-services ping
set security zones security-zone TRUST host-inbound-traffic system-services ssh
set security zones security-zone TRUST interfaces reth0.50
set security zones security-zone INTERNAL host-inbound-traffic system-services ping
set security zones security-zone INTERNAL interfaces reth0.55
set security zones security-zone WAREHOUSE host-inbound-traffic system-services ping
set security zones security-zone WAREHOUSE interfaces reth0.60
set security zones security-zone TESTBED host-inbound-traffic system-services ping
set security zones security-zone TESTBED interfaces reth0.65
set security zones security-zone TESTBED interfaces reth0.70

set interfaces lo0 redundant-pseudo-interface-options redundancy-group 2
set chassis cluster redundancy-group 2 node 0 priority 1
set chassis cluster redundancy-group 2 node 1 priority 100
set chassis cluster redundancy-group 2 preempt
```

Note: As per previous task requirements adding logical interface lo0 interface also requires adding an additional redundancy-group.

XPARENT:

```
set security zones security-zone WAREHOUSE interfaces reth1.60
set security zones security-zone WAREHOUSE interfaces reth0.60
set security zones security-zone TRUST interfaces reth0.50
set security zones security-zone TRUST interfaces reth1.50
set security zones security-zone TESTBED interfaces reth1.65
set security zones security-zone TESTBED interfaces reth1.70
set security zones security-zone TESTBED interfaces reth0.65
set security zones security-zone TESTBED interfaces reth0.70
```

EXA:

```
set security zones security-zone UNTRUST host-inbound-traffic system-services ping
set security zones security-zone UNTRUST interfaces lo0.0
set security zones security-zone UNTRUST interfaces ge-0/0/3.0
set security zones security-zone TRUST-EXA host-inbound-traffic system-services ping
set security zones security-zone TRUST-EXA host-inbound-traffic system-services ssh
set security zones security-zone TRUST-EXA interfaces ge-0/0/4.0
set security zones security-zone PRIVATE-EXA host-inbound-traffic system-services ping
set security zones security-zone PRIVATE-EXA interfaces ge-0/0/5.15
set security zones security-zone DMZ-EXA host-inbound-traffic system-services ping
set security zones security-zone DMZ-EXA interfaces ge-0/0/5.30
set interfaces ge-0/0/3 unit 0 family inet address 100.1.1.1/29
set interfaces ge-0/0/4 unit 0 family inet address 172.16.10.254/24
set interfaces ge-0/0/4 unit 0 family inet6 address 2016:abcd:d1::254/64
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
set interfaces ge-0/0/5 vlan-tagging
set interfaces ge-0/0/5 unit 15 vlan-id 15
set interfaces ge-0/0/5 unit 15 family inet address 172.16.15.254/24
set interfaces ge-0/0/5 unit 15 family inet6 address 2016:abcd:d2::254/64
set interfaces ge-0/0/5 unit 30 vlan-id 30
set interfaces ge-0/0/5 unit 30 family inet address 172.16.30.254/24
set interfaces fxp0 unit 0 family inet address 10.10.1.7/24
set interfaces lo0 unit 0 family inet filter input RE-PROTECT-v4
set interfaces lo0 unit 0 family inet address 192.168.1.5/32
```

BUILDING:

```
set interfaces ge-0/0/3 vlan-tagging
set interfaces ge-0/0/3 unit 100 vlan-id 100
set interfaces ge-0/0/3 unit 100 family inet address 172.16.100.254/24
set interfaces ge-0/0/3 unit 101 vlan-id 101
set interfaces ge-0/0/3 unit 101 family inet address 172.16.101.254/24
set interfaces ge-0/0/3 unit 200 vlan-id 200
set interfaces ge-0/0/3 unit 200 family inet address 172.16.200.254/24
set interfaces ge-0/0/3 unit 201 vlan-id 201
set interfaces ge-0/0/3 unit 201 family inet address 172.16.201.254/24
set interfaces ge-0/0/4 vlan-tagging
set interfaces ge-0/0/4 unit 55 vlan-id 55
set interfaces ge-0/0/4 unit 55 family inet address 172.16.55.1/24
set interfaces ge-0/0/5 vlan-tagging
set interfaces ge-0/0/5 unit 55 vlan-id 55
set interfaces ge-0/0/5 unit 55 family inet address 172.16.55.2/24
set interfaces lo0 unit 1 family inet address 192.168.1.6/32
set interfaces lo0 unit 2 family inet address 192.168.1.7/32
set interfaces lo0 unit 0 family inet filter input RE-PROTECT-v4

set security zones security-zone INTERNAL-B1 host-inbound-traffic system-services ping
set security zones security-zone INTERNAL-B1 interfaces ge-0/0/4.55
set security zones security-zone INTERNAL-B1 interfaces lo0.1
set security zones security-zone TRUST-B1 host-inbound-traffic system-services ping
set security zones security-zone TRUST-B1 host-inbound-traffic system-services ssh
set security zones security-zone TRUST-B1 interfaces ge-0/0/3.100
set security zones security-zone DMZ-B1 host-inbound-traffic system-services ping
set security zones security-zone DMZ-B1 interfaces ge-0/0/3.101
set security zones security-zone INTERNAL-B2 host-inbound-traffic system-services ping
set security zones security-zone INTERNAL-B2 interfaces lo0.2
set security zones security-zone INTERNAL-B2 interfaces ge-0/0/5.55
set security zones security-zone TRUST-B2 host-inbound-traffic system-services ping
set security zones security-zone TRUST-B2 host-inbound-traffic system-services ssh
set security zones security-zone TRUST-B2 interfaces ge-0/0/3.200
set security zones security-zone DMZ-B2 host-inbound-traffic system-services ping
set security zones security-zone DMZ-B2 interfaces ge-0/0/3.201

set routing-instances building1 instance-type virtual-router
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
set routing-instances building1 interface ge-0/0/3.100
set routing-instances building1 interface ge-0/0/3.101
set routing-instances building1 interface ge-0/0/4.55
set routing-instances building1 interface lo0.1
set routing-instances building1 routing-options static route 0.0.0.0/0 next-hop 172.16.55.254
set routing-instances building2 instance-type virtual-router
set routing-instances building2 interface ge-0/0/3.200
set routing-instances building2 interface ge-0/0/3.201
set routing-instances building2 interface ge-0/0/5.55
set routing-instances building2 interface lo0.2
set routing-instances building2 routing-options static route 0.0.0.0/0 next-hop 172.16.55.254
```

BGP Overview:

Border Gateway Protocol version 4 (BGP-4) is a path vector protocol as defined in RFC4271. Routing loops are detected and avoided by a device checking its own path number (Autonomous System Number - ASN) in the message received from a neighbor. Although in-depth understand of BGP is out of scope of the syllabus, you should understand key elements to successfully configure the devices and how to best steer network traffic using BGP.

BGP uses TCP for session establishment and reserved port number 179.
The following table identifies the states of BGP peering and their meaning:

State	Description
Idle	Initial state when all incoming BGP connections are refused. A start event is required for the local system to initialize BGP resources and prepare for a transport connection with the other BGP peer.
Connect	BGP is waiting for the transport protocol connection to be completed. If the transport protocol connection succeeds, the local system sends an OPEN message and transitions to the OpenSent state. If the transport protocol connection fails, the local system restarts the ConnectRetryTimer, listens for a connection initiated by the remote BGP peer, and changes its state to Active.
Active	BGP is trying to acquire a peer by initiating a transport protocol connection. If the transport protocol connection succeeds, the local system sends an OPEN message to its peer and transitions to the OpenSent state. If the local system's BGP state remains in the Active state, you should check physical connectivity as well as the configuration on both peers.
OpenSent	BGP waits for an OPEN message from its peer. When an OPEN

© 2020 Juniper Networks, Inc. All rights reserved.

	message is received, it is checked and verified to ensure that no errors exist. If an error is detected, the system transitions back to the Idle state. If no errors are detected, BGP sends a Keepalive message
OpenConfirm	BGP waits for a KEEPALIVE or NOTIFICATION message. If no KEEPALIVE message is received before the negotiated hold timer expires, the local system sends a NOTIFICATION message stating that the hold timer has expired and changes its state to Idle. Likewise, if the local system receives a NOTIFICATION message, it changes its state to Idle. If the local system receives a KEEPALIVE message, it changes its state to Established.
Established	BGP can exchange UPDATE, NOTIFICATION, and KEEPALIVE messages with its peer. When the local system receives an UPDATE or KEEPALIVE message and when the negotiated holdtimer value is nonzero, it restarts its hold timer. If the negotiated hold timer reaches zero, the local system sends out a KEEPALIVE message and restarts the hold timer.

BGP works with the concept of attributes. The following table identifies their types:

Type	Description
Well-known mandatory	Must be supported by all BGP implementations and must be included in every BGP update
Well-known discretionary	Must be supported in all BGP implementations, but do not have to be included in every BGP update
Optional transitive	Not required to be supported by all BGP implementations but, if they are, they should be passed along, unchanged, to other BGP peers
Optional non-transitive	Not required to be supported by all BGP implementations. If an optional nontransitive attribute is not recognized, it is ignored and not passed to other peers

Well known mandatory attributes include AS_PATH which means that we must identify our local autonomous system number, the NEXT-HOP which identifies the peer to send the

© 2020 Juniper Networks, Inc. All rights reserved.

destination traffic and the ORIGIN that identifies if it is coming from an EBGP peer (E), the IGP (I) or unknown source also known as incomplete (?).

Well known discretionary attributes include LOCAL-PREFERENCE and this allows us to select a specific neighbor over two equal cost prefixes whenever such option exists.

A few rules to bear in mind about BGP are how information advertisement works. This is fundamental to prevents routing loops.

1. IBGP peers advertise routes received from EBGP peers to other IBGP peers
2. EBGP peers advertise routes learned from IBGP or EBGP peers to other EBGP peers
3. IBGP peers do not advertise routes received from IBGP peers to other IBGP peers

BGP stores its information in internal routing tables. These are called Routing Information Base (RIB) and there are 3 types of RIBs:

Type	Description
RIB-In	BGP routing information as it was received from the specified BGP neighbor and before any import policy processing occurs.
RIB-local	Only active routes are installed in this table and are used by the device. These are the prefixes after the import policy processing occurs.
RIB-Out	The information reflects the routes that the routing table exported into the routing protocol, along with any attributes that have been attached. This is after the export policy processing occurs.

Another key element of BGP is its path selection algorithm. Verify that the next hop can be resolved

1. For BGP, prefer the path with higher local preference
2. For BGP, prefer the path with the shortest autonomous system (AS) path value
3. Prefer strictly external BGP (EBGP) paths over external paths learned through internal BGP (IBGP) sessions, over incomplete E > I > ?
4. A path is considered a BGP equal-cost path (and will be used for forwarding) when paths are learned by a multipath-enabled BGP neighbor within the same neighboring AS

© 2020 Juniper Networks, Inc. All rights reserved.

Note: The central cluster supports multi-homing from two distinct addresses in the local device to neighboring peers. Equal cost multi path (ECMP) exists for received prefixes so we need local preference manipulation to select the next hop we desire to send traffic to and AS path manipulation for the peer to understand which is the least preferred neighbor to send traffic to.

BGP does not advertise any prefix by default so we need to advertise the company's owned prefix 80.1.1.0/24 which does not exist and needs to be created as an aggregate route.

8) Configure BGP between the central device to both external neighboring addresses or the Internet transit provider ASN 4321
    a. Advertise the company owned prefix 80.1.1.0/24 making sure BGP prefixes do not participate in the aggregation process.
    b. Make sure your preferred entry and exit point for general Internet connectivity is node0.

```
{primary:node0}[edit]
lab@central-node0# show policy-options
policy-statement from-bgp13 {
    term default {
        from {
            protocol bgp;
            route-filter 0.0.0.0/0 exact;
        }
        then accept;
    }
    term specific {
        from {
            protocol bgp;
            route-filter 0.0.0.0/0 longer;
        }
        then {
            local-preference 200;
            accept;
        }
    }
}
policy-statement from-bgp9 {
    term default {
        from {
            protocol bgp;
            route-filter 0.0.0.0/0 exact;
        }
        then {
            local-preference 200;
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
            accept;
        }
    }
    term specific {
        from {
            protocol bgp;
            route-filter 0.0.0.0/0 longer;
        }
        then accept;
    }
}
policy-statement no-bgp {
    term bgp {
        from protocol bgp;
        then reject;
    }
    term else {
        then accept;
    }
}
policy-statement to-bgp13 {
    term company {
        from {
            protocol aggregate;
            route-filter 80.1.1.0/24 exact;
        }
        then {
            as-path-prepend "1234 1234";
            accept;
        }
    }
    term lo0 {
        from {
            interface lo0.0;
            route-filter 80.1.1.16/32 exact;
        }
        then accept;
    }
}
policy-statement to-bgp9 {
    term company {
        from {
            protocol aggregate;
            route-filter 80.1.1.0/24 exact;
        }
        then accept;
    }
    term lo0 {
        from {
            interface lo0.0;
            route-filter 80.1.1.16/32 exact;
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
        }
        then {
            as-path-prepend "1234 1234";
            accept;
        }
    }
}

{primary:node0}[edit]
lab@central-node0# show routing-options
aggregate {
    route 80.1.1.0/24 policy no-bgp;
}
autonomous-system 1234;


{primary:node0}[edit]
lab@central-node0# show protocols bgp
group untrust-v4 {
    type external;
    peer-as 4321;
    neighbor 80.1.1.9 {
        import from-bgp9;
        export to-bgp9;
    }
    neighbor 80.1.1.13 {
        import from-bgp13;
        export to-bgp13;
    }
}

{primary:node0}[edit]
lab@central-node0# run show bgp summary
Groups: 2 Peers: 2 Down peers: 0
Table          Tot Paths  Act Paths Suppressed    History Damp State    Pending
inet.0
                      10          5          0          0          0          0
Peer                     AS      InPkt     OutPkt    OutQ   Flaps Last Up/Dwn
State|#Active/Received/Accepted/Damped...
80.1.1.9                4321          6          4       0       0           3 1/5/5/0
0/0/0/0
80.1.1.13               4321          5          4       0       0           6 4/5/5/0
0/0/0/0

{primary:node0}[edit]
lab@central-node0# run show route advertising-protocol bgp 80.1.1.9

inet.0: 25 destinations, 30 routes (25 active, 0 holddown, 0 hidden)
  Prefix                  Nexthop              MED     Lclpref    AS path
* 80.1.1.0/24             Self                                    I
* 80.1.1.16/32            Self                                    1234 1234 [1234] I
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
{primary:node0}[edit]
lab@central-node0# run show route advertising-protocol bgp 80.1.1.13

inet.0: 25 destinations, 30 routes (25 active, 0 holddown, 0 hidden)
  Prefix                  Nexthop              MED     Lclpref    AS path
* 80.1.1.0/24             Self                                    1234 1234 [1234] I
* 80.1.1.16/32            Self                                    I

lab@central-node0# run show route receive-protocol bgp 80.1.1.9

inet.0: 25 destinations, 30 routes (25 active, 0 holddown, 0 hidden)
  Prefix                  Nexthop              MED     Lclpref    AS path
* 0.0.0.0/0               80.1.1.9                                4321 I
  80.1.1.0/30             80.1.1.9                                4321 I
  80.1.1.4/30             80.1.1.9                                4321 I
  100.0.0.0/8             80.1.1.9                                4321 I
  200.0.0.0/8             80.1.1.9                                4321 I

inet6.0: 10 destinations, 10 routes (10 active, 0 holddown, 0 hidden)

{primary:node0}[edit]
lab@central-node0# run show route receive-protocol bgp 80.1.1.13

inet.0: 25 destinations, 30 routes (25 active, 0 holddown, 0 hidden)
  Prefix                  Nexthop              MED     Lclpref    AS path
  0.0.0.0/0               80.1.1.13                               4321 I
* 80.1.1.0/30             80.1.1.13                               4321 I
* 80.1.1.4/30             80.1.1.13                               4321 I
* 100.0.0.0/8             80.1.1.13                               4321 I
* 200.0.0.0/8             80.1.1.13                               4321 I
```

Task 4: UTM

1) Antivirus scanning has to be done in the Remote office 1 and Remote office 2. Configure the security devices to perform antivirus scanning according to the following requirements:
   a. Only HTTP and FTP traffic from the correspondent TRUST zones to the UNTRUST network will be scanned
   b. The HTTP traffic to www.internalsites.com prefix and audio mime type are excluded from antivirus scan.
   c. The clients have to receive every 40 seconds a small portion of unchecked data to avoid timeout.
   d. The scanning engine timeout is set to 5 minutes.
   e. All fallback options are set to block except default and too-many-requests.
   f. The virus notification message is “Virus detected!”
   g. The fallback notifications are:
      i. BLOCK – “AV blocked the traffic as it was not able to scan it!”

© 2020 Juniper Networks, Inc. All rights reserved.

Roffice1 & Roffice2:

```
lab@roffice2# show security utm
custom-objects {
    mime-pattern {
        AV-excluded-mime {
            value audio/;
        }
    }
    url-pattern {
        company-site {
            value www.internalsites.com;
        }
    }
    custom-url-category {
        AV-excluded-sites {
            value company-site;
        }
    }
}
feature-profile {
    anti-virus {
        mime-whitelist {
            list AV-excluded-mime;
        }
        url-whitelist AV-excluded-sites;
        sophos-engine {
            profile AV-full-file-scan {
                fallback-options {
                    default block;
                    content-size block;
                    engine-not-ready block;
                    timeout block;
                    out-of-resources block;
                    too-many-requests log-and-permit;
                }
                scan-options {
                    timeout 300;
                }
                trickling timeout 40;
                notification-options {
                    virus-detection {
                        type message;
                        custom-message "Virus detected!";
                    }
                    fallback-block {
                        type message;
                        custom-message "AV blocked the traffic as it was not able to scan
it!";
                    }
                }
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
            }
        }
    }
}
utm-policy RO-AV {
    anti-virus {
        http-profile AV-full-file-scan;
        ftp {
            upload-profile AV-full-file-scan;
            download-profile AV-full-file-scan;
        }
    }
}
```

Roffice1:

```
lab@roffice1# show security policies
from-zone TRUST-RO1 to-zone UNTRUST {
    policy HTTP-FTP {
        match {
            source-address RO1-TRUST;
            destination-address any;
            application [ junos-http junos-ftp ];
        }
        then {
            permit {
                application-services {
                    utm-policy RO-AV;
                }
            }
        }
    }
```

Roffice2:

```
lab@roffice2# show security policies
from-zone UNTRUST to-zone DMZ-RO2 {
    policy SERVERS {
        match {
            source-address any;
            destination-address [ RO2-SRV-WEB RO2-SRV-DB ];
            application [ junos-http RO2-SQL ];
        }
        then {
            permit {
                destination-address {
                    drop-untranslated;
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
                }
            }
        }
    }
}
from-zone TRUST-RO2 to-zone UNTRUST {
    policy HTTP-FTP {
        match {
            source-address RO2-TRUST;
            destination-address any;
            application [ junos-http junos-ftp ];
        }
        then {
            permit {
                application-services {
                    utm-policy RO-AV;
                }
            }
        }
    }
}
```

2) The exa-fw device enforces local web-filtering according the requirements below:
    a. The web filtering is done on HTTP connections from the TRUST-EXA zone to the Internet.
    b. The following URLs are denied
        i. www.facebook.com
        ii. www.twitter.com
        iii. www.youtube.com
c. The clients receive the “This site is not allowed” message in case their request was blocked.
d. The local engine timeout is set to 10 minutes.
e. All fallback options except default option block the requests.

```
[edit]
lab@exa-fw# show security utm
custom-objects {
    url-pattern {
        denied-sites {
            value [ http://www.facebook.com http://www.twitter.com http://www.www.youtube.com
];
        }
    }
    custom-url-category {
        denied-sites-category {
            value denied-sites;
        }
    }
}
feature-profile {
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
web-filtering {
    url-blacklist denied-sites-category;
    type juniper-local;
    juniper-local {
        profile Web-filtering {
            default permit;
            custom-block-message "This site is not allowed!";
            fallback-settings {
                default block;
                timeout block;
                too-many-requests block;
            }
            timeout 600;
        }
    }
}
utm-policy EXA-WebFilter {
    web-filtering {
        http-profile Web-filtering;
    }
}

[edit]
lab@exa-fw# show security policies
from-zone TRUST-EXA to-zone UNTRUST {
    policy HTTP {
        match {
            source-address EXA-TRUST;
            destination-address any;
            application junos-http;
        }
        then {
            permit {
                application-services {
                    utm-policy EXA-WebFilter;
                }
            }
        }
    }
}
```

3) In headquarters the HTTP and FTP traffic from the TRUST zone to the Internet leaving through the cluster needs to be processed in following manner:
    a. The content handling is:
        i. Cookies and java-applets are blocked
        ii. “bat” and “sh” files are blocked
        iii. The engine generates protocol error “Firewall blocked this content!” once traffic is blocked

© 2020 Juniper Networks, Inc. All rights reserved.

4) The company's email server (172.16.60.199) located in the WAREHOUSE zone behind the XPARENT cluster has to be protected from these outside spammers from the Internet

   a. IP addresses: 4.4.4.4, 5.5.5.5, 45.45.45.45
   b. Domains: spam.com, bad.com
   c. Email senders: spam@gmail.com, spam@yahoo.com

Central-Node0:

```
{primary:node0}[edit]
lab@central-node0# show security utm
custom-objects {
    filename-extension {
        bat-sh {
            value [ bat sh ];
        }
    }
    url-pattern {
        spam-sources {
            value [ 4.4.4.4 5.5.5.5 45.45.45.45 spam.com bad.com "spam@gmail.com"
"spam@yahoo.com" ];
        }
    }
}
default-configuration {
    anti-spam {
        type sbl;
    }
}
feature-profile {
    anti-spam {
        address-blacklist spam-sources;
        sbl {
            profile smtp-protect {
                no-sbl-default-server;
                spam-action block;
            }
        }
    }
    content-filtering {
        profile CENTRAL-content-filter {
            block-extension bat-sh;
            block-content-type {
                java-applet;
                http-cookie;
            }
            notification-options {
                type protocol-only;
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
                custom-message "Firewall blocked this content!";
            }
        }
    }
}
utm-policy CENTRAL-Content {
    content-filtering {
        http-profile CENTRAL-content-filter;
        ftp {
            upload-profile CENTRAL-content-filter;
            download-profile CENTRAL-content-filter;
        }
    }
}
utm-policy CENTRAL-SPAM {
    anti-spam {
        smtp-profile smtp-protect;
    }
}

{primary:node0}[edit]
lab@central-node0# show security policies from-zone TRUST to-zone UNTRUST
policy HTTP-FTP {
    match {
        source-address CENTRAL-TRUST;
        destination-address any;
        application [ junos-http junos-ftp ];
        dynamic-application junos:MSN;
    }
    then {
        permit {
            application-services {
                utm-policy CENTRAL-Content;
            }
        }
        log {
            session-init;
            session-close;
        }
    }
}

{primary:node0}[edit]
lab@central-node0# show services ssl
proxy {
    profile CENTRAL-SSL {
        root-ca MY-CERT;
        actions {
            ignore-server-auth-failure;
            log {
                all;
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
            }
        }
    }
}

{primary:node0}[edit]
lab@central-node0# show security policies
from-zone UNTRUST to-zone WAREHOUSE {
    policy SRV-MAIL {
        match {
            source-address any;
            destination-address SRV-MAIL;
            application junos-smtp;
        }
        then {
            permit {
                destination-address {
                    drop-untranslated;
                }
                application-services {
                    utm-policy CENTRAL-SPAM;
                }
            }
        }
    }
    policy SERVERS {
        match {
            source-address any;
            destination-address [ WAREHOUSE-SRV-205 WAREHOUSE-SRV-206 WAREHOUSE-HONEYPOT ];
            application any;
        }
        then {
            permit {
                destination-address {
                    drop-untranslated;
                }
                application-services {
                    idp;
                }
            }
        }
    }
}
from-zone TRUST to-zone UNTRUST {
    policy HTTP-FTP {
        match {
            source-address CENTRAL-TRUST;
            destination-address any;
            application [ junos-http junos-ftp ];
            dynamic-application junos:MSN;
        }
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
then {
    permit {
        application-services {
            utm-policy CENTRAL-Content;
            application-traffic-control {
                rule-set MEGA;
            }
        }
    }
    log {
        session-init;
        session-close;
    }
    }
    policy INTERNET {
        match {
            source-address CENTRAL-TRUST;
            destination-address any;
            application any;
        }
        then {
            permit;
        }
    }
}
from-zone INTERNAL to-zone WAREHOUSE {
    policy WEBSENSE {
        match {
            source-address CENTRAL-INTERNAL;
            destination-address any;
            application junos-http;
        }
        then {
            permit;
        }
    }
}
from-zone TESTBED to-zone WAREHOUSE {
    policy WEBSENSE {
        match {
            source-address CENTRAL-TESTBED;
            destination-address any;
            application junos-http;
            dynamic-application junos:HTTP;
        }
        then {
            permit;
            log {
                session-init;
                session-close;
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
            }
        }
    }
}
from-zone WAREHOUSE to-zone UNTRUST {
    policy WEBSENSE {
        match {
            source-address WEBSENSE;
            destination-address any;
            application junos-http;
        }
        then {
            permit;
        }
    }
    policy SRV-MAIL {
        match {
            source-address SRV-MAIL;
            destination-address any;
            application any;
        }
        then {
            permit;
        }
    }
}
from-zone INTERNAL to-zone UNTRUST {
    policy INTERNET {
        match {
            source-address CENTRAL-INTERNAL;
            destination-address any;
            application any;
        }
        then {
            permit;
        }
    }
}
from-zone UNTRUST to-zone UNTRUST {
    policy UNTRUST {
        match {
            source-address any;
            destination-address any;
            application any;
        }
        then {
            permit;
        }
    }
}
from-zone TESTBED to-zone UNTRUST {
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
policy HTTPS {
    match {
        source-address CENTRAL-TESTBED;
        destination-address any;
        application junos-https;
    }
    then {
        permit {
            application-services {
                ssl-proxy {
                    profile-name CENTRAL-SSL;
                }
            }
        }
    }
}
from-zone WAREHOUSE to-zone WAREHOUSE {
    policy WAREHOUSE {
        match {
            source-address any;
            destination-address any;
            application any;
        }
        then {
            permit;
        }
    }
}
```

Xparent-node0:

```
{primary:node0}[edit]
lab@xparent-node0# show security policies
from-zone WAREHOUSE to-zone WAREHOUSE {
    policy WAREHOUSE {
        match {
            source-address CENTRAL-WAREHOUSE;
            destination-address CENTRAL-WAREHOUSE;
            application any;
        }
        then {
            permit;
        }
    }
    policy WEBSENSE {
        match {
            source-address [ CENTRAL-INTERNAL CENTRAL-TESTBED WEBSENSE ];
            destination-address any;
            application junos-http;
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
        }
        then {
            permit;
        }
    }
    policy SRV-MAIL-IN {
        match {
            source-address any;
            destination-address SRV-MAIL;
            application junos-smtp;
        }
        then {
            permit;
        }
    }
    policy SRV-MAIL-OUT {
        match {
            source-address SRV-MAIL;
            destination-address any;
            application any;
        }
        then {
            permit;
        }
    }
    policy SERVERS {
        match {
            source-address any;
            destination-address [ WAREHOUSE-SRV-205 WAREHOUSE-SRV-206 ];
            application [ junos-http SQL junos-ssh junos-ftp ];
        }
        then {
            permit;
        }
    }
}
from-zone TRUST to-zone TRUST {
    policy TRUST {
        match {
            source-address TRUST-NETWORKS;
            destination-address TRUST-NETWORKS;
            application any;
        }
        then {
            permit;
        }
    }
}
from-zone TESTBED to-zone TESTBED {
    policy TESTBED {
        match {
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
            source-address [ CENTRAL-TESTBED6 CENTRAL-TESTBED7 ];
            destination-address [ CENTRAL-TESTBED6 CENTRAL-TESTBED7 ];
            application junos-ping;
        }
        then {
            permit;
        }
    }
}
```

Task 5: NAT

1) Following NAT translations need to be done on the roffice1 security device:
    a. The egress interface IP address is used to translate connections from the hosts in the TRUST-RO1 zone to the UNTRUST zone.
    b. The host 172.16.11.50 in the PRIVATE-RO1 zone needs to be able to receive connections from and initiate connections to the Internet. The connections from Internet need to be destined to the 80.1.1.64 IP address in order to reach this host.

```
[edit]
lab@roffice1# show security nat
source {
    rule-set TRUST-RO1 {
        from zone TRUST-RO1;
        to zone UNTRUST;
        rule INTERNET {
            match {
                destination-address 0.0.0.0/0;
            }
            then {
                source-nat {
                    interface;
                }
            }
        }
    }
}
static {
    rule-set RO1-HOST-PRIVATE {
        from zone UNTRUST;
        rule RO1-HOST-PRIVATE {
            match {
                destination-address 80.1.1.64/32;
            }
            then {
                static-nat {
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
                    prefix {
                        172.16.11.50/32;
                    }
                }
            }
        }
    }
}


[edit]
lab@roffice1# show security policies from-zone TRUST-RO1 to-zone UNTRUST policy INTERNET
match {
    source-address RO1-TRUST;
    destination-address any;
    application any;
}
then {
    permit;
}


[edit]
lab@roffice1# show security policies from-zone PRIVATE-RO1 to-zone UNTRUST policy INTERNET
match {
    source-address RO1-HOST-PRIVATE;
    destination-address any;
    application any;
}
then {
    permit;
}
```

Verification

© 2020 Juniper Networks, Inc. All rights reserved.

```
VR-DEVICE> telnet routing-instance roffice1-trust 12.34.56.78 port 80
Trying 12.34.56.78...
Connected to 12.34.56.78.
Escape character is '^]'.

roffice1> show security flow session destination-port 80
Session ID: 3513, Policy name: HTTP-FTP/8, Timeout: 298, Valid
  In: 172.16.10.1/62321 --> 12.34.56.78/80;tcp, If: ge-0/0/4.0, Pkts: 2,
Bytes: 116
  Out: 12.34.56.78/80 --> 80.1.1.1/14569;tcp, If: ge-0/0/3.0, Pkts: 1, Bytes:
64
Total sessions: 1

VR-DEVICE> ping routing-instance roffice1-trust 12.34.56.78 count 1
PING 12.34.56.78 (12.34.56.78): 56 data bytes
64 bytes from 12.34.56.78: icmp_seq=0 ttl=63 time=2.581 ms

roffice1> show security flow session protocol icmp
Session ID: 3520, Policy name: INTERNET/6, Timeout: 4, Valid
  In: 172.16.10.1/1 --> 12.34.56.78/3852;icmp, If: ge-0/0/4.0, Pkts: 1,
Bytes: 84
  Out: 12.34.56.78/3852 --> 80.1.1.1/28867;icmp, If: ge-0/0/3.0, Pkts: 1,
Bytes: 84
```

```
VR-DEVICE> ping routing-instance roffice1-private 12.34.56.78 source
172.16.11.50 count 1
PING 12.34.56.78 (12.34.56.78): 56 data bytes
64 bytes from 12.34.56.78: icmp_seq=0 ttl=63 time=2.806 ms

roffice1> show security flow session protocol icmp
Session ID: 3537, Policy name: INTERNET/9, Timeout: 2, Valid
  In: 172.16.11.50/0 --> 12.34.56.78/3863;icmp, If: ge-0/0/5.0, Pkts: 1,
Bytes: 84
  Out: 12.34.56.78/3863 --> 80.1.1.64/0;icmp, If: ge-0/0/3.0, Pkts: 1, Bytes:
84
Total sessions: 1

VR-DEVICE> ping routing-instance untrust 80.1.1.64 count 1
PING 80.1.1.64 (80.1.1.64): 56 data bytes
64 bytes from 80.1.1.64: icmp_seq=0 ttl=63 time=2.686 ms

roffice1> show security flow session protocol icmp
Session ID: 3548, Policy name: RO1-HOST-PRIVATE/4, Timeout: 2, Valid
  In: 80.1.1.2/0 --> 80.1.1.64/3877;icmp, If: ge-0/0/3.0, Pkts: 1, Bytes: 84
  Out: 172.16.11.50/3877 --> 80.1.1.2/0;icmp, If: ge-0/0/5.0, Pkts: 1, Bytes:
84
Total sessions: 1
```


© 2020 Juniper Networks, Inc. All rights reserved.

2) NAT translation details for the roffice2 security device:
   a. Ensure the connections from the TRUST-RO2 zone to the Internet are translated to 80.1.1.96-80.1.1.99 IP addresses. PAT is allowed and concurrent sessions from the same host must be translated using the same IP address.
   b. The web and database servers need to be reachable from the UNTRUST zone as defined in the table below:

Server	Internal address	Internal port	Public address	Public port
Web server	172.16.21.2	80	80.1.1.100	8080
Database server	172.16.21.33	3306	80.1.1.100	3306

   c. Untranslated connections from the UNTRUST zone to these servers are not allowed.

```
[edit]
lab@roffice2# show security nat
source {
    pool INTERNET {
        address {
            80.1.1.96/32 to 80.1.1.99/32;
        }
    }
    address-persistent;
    rule-set TRUST-RO2 {
        from zone TRUST-RO2;
        to zone UNTRUST;
        rule INTERNET {
            match {
                destination-address 0.0.0.0/0;
            }
            then {
                source-nat {
                    pool {
                        INTERNET;
                    }
                }
            }
        }
    }
}
destination {
    pool RO2-SRV-WEB {
        address 172.16.21.2/32 port 80;
    }
    pool RO2-SRV-DB {
        address 172.16.21.33/32;
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
}
rule-set RO2-SERVERS {
    from zone UNTRUST;
    rule RO2-SRV-WEB {
        match {
            destination-address 80.1.1.100/32;
            destination-port {
                8080;
            }
        }
        then {
            destination-nat {
                pool {
                    RO2-SRV-WEB;
                }
            }
        }
    }
    rule RO2-SRV-DB {
        match {
            destination-address 80.1.1.100/32;
            destination-port {
                3306;
            }
        }
        then {
            destination-nat {
                pool {
                    RO2-SRV-DB;
                }
            }
        }
    }
}
```

```
[edit]
lab@roffice2# show security policies from-zone TRUST-RO2 to-zone UNTRUST policy INTERNET
match {
    source-address RO2-TRUST;
    destination-address any;
    application any;
}
then {
    permit;
}
```


© 2020 Juniper Networks, Inc. All rights reserved.

Verification

```
vr-device> telnet routing-instance untrust 80.1.1.100 port 3306
Trying 80.1.1.100...
Connected to 80.1.1.100.
Escape character is '^]'.

roffice2> show security flow session destination-port 3306
Session ID: 478, Policy name: SERVERS/5, Timeout: 1768, Valid
  In: 80.1.1.6/59544 --> 80.1.1.100/3306;tcp, If: ge-0/0/3.0, Pkts: 2, Bytes:
116
  Out: 172.16.21.33/3306 --> 80.1.1.6/59544;tcp, If: ge-0/0/5.0, Pkts: 1,
Bytes: 64
Total sessions: 1
```

```
vr-device> telnet routing-instance roffice2-trust 12.34.56.78 port 80
Trying 12.34.56.78...
Connected to 12.34.56.78.
Escape character is '^]'.

roffice2> show security flow session destination-port 3306
Session ID: 392, Policy name: INTERNET/6, Timeout: 1788, Valid
  In: 172.16.20.1/56866 --> 12.34.56.78/3306;tcp, If: ge-0/0/4.0, Pkts: 2,
Bytes: 116
  Out: 12.34.56.78/3306 --> 80.1.1.97/30461;tcp, If: ge-0/0/3.0, Pkts: 1,
Bytes: 64
Total sessions: 1

vr-device> ping routing-instance roffice2-trust 12.34.56.78 count 1
PING 12.34.56.78 (12.34.56.78): 56 data bytes
64 bytes from 12.34.56.78: icmp_seq=0 ttl=63 time=2.581 ms

roffice2> show security flow session protocol icmp
Session ID: 399, Policy name: INTERNET/6, Timeout: 2, Valid
  In: 172.16.20.1/0 --> 12.34.56.78/8661;icmp, If: ge-0/0/4.0, Pkts: 1,
Bytes: 84
  Out: 12.34.56.78/8661 --> 80.1.1.97/27985;icmp, If: ge-0/0/3.0, Pkts: 1,
Bytes: 84
```

3) The exa-fw device has to provide the following translations:
   a. Traffic from the TRUST-EXA hosts to the Internet has to be translated to the 100.1.1.128-100.1.1.143 range. PAT is not allowed, and the IP address of the egress interface has to be used when the pool is exhausted.
   b. The connections from PRIVATE-EXA hosts to the Internet must be translated in following manner:

© 2020 Juniper Networks, Inc. All rights reserved.

i. 172.16.15.5 --> 100.1.1.192, 172.16.15.6 --> 100.1.1.193, …, up to 172.16.15.10 --> 100.1.1.197
ii. Ports are not translated
iii. Connections from other hosts are not translated

c. The servers in the DMZ-EXA zone need to be reachable from the Internet as specified in the table below:

Server	Internal address	Internal port	Public address	Public port
Web server	172.16.30.11	80	100.1.1.3	8080
Database server	172.16.30.12	3306	100.1.1.3	3306
SSH server	172.16.30.13	22	100.1.1.4	12345

d. Untranslated connections from the UNTRUST zone to these servers are not allowed.

```
[edit]
lab@exa-fw# show security nat
source {
    pool TRUST {
        address {
            100.1.1.128/32 to 100.1.1.143/32;
        }
        port {
            no-translation;
        }
        overflow-pool interface;
    }
    pool PRIVATE {
        address {
            100.1.1.192/32 to 100.1.1.197/32;
        }
        host-address-base 172.16.15.5/32;
        port {
            no-translation;
        }
    }
rule-set INTERNET {
    from zone [ PRIVATE-EXA TRUST-EXA ];
    to zone UNTRUST;
    rule TRUST {
        match {
            source-address 172.16.10.0/24;
            destination-address 0.0.0.0/0;
        }
        then {
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
            source-nat {
                pool {
                    TRUST;
                }
            }
        }
    }
    rule PRIVATE {
        match {
            source-address 172.16.15.0/24;
            destination-address 0.0.0.0/0;
        }
        then {
            source-nat {
                pool {
                    PRIVATE;
                }
            }
        }
    }
    destination {
        pool EXA-SRV-WEB {
            address 172.16.30.11/32 port 80;
        }
        pool EXA-SRV-DB {
            address 172.16.30.12/32;
        }
        pool EXA-SRV-SSH {
            address 172.16.30.13/32 port 22;
        }
        rule-set SERVERS {
            from zone UNTRUST;
            rule EXA-SRV-WEB {
                match {
                    destination-address 100.1.1.3/32;
                    destination-port {
                        8080;
                    }
                }
                then {
                    destination-nat {
                        pool {
                            EXA-SRV-WEB;
                        }
                    }
                }
            }
            rule EXA-SRV-DB {
                match {
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
            destination-address 100.1.1.3/32;
            destination-port {
                3306;
            }
        }
        then {
            destination-nat {
                pool {
                    EXA-SRV-DB;
                }
            }
        }
    }
}
            rule EXA-SRV-SSH {
                match {
                    destination-address 100.1.1.4/32;
                    destination-port {
                        12345;
                    }
                }
                then {
                    destination-nat {
                        pool {
                            EXA-SRV-SSH;
                        }
                    }
                }
            }
        }
    }
}
```

```
VR-DEVICE> telnet routing-instance exa-trust 12.34.56.78 port 80
Trying 12.34.56.78...
Connected to 12.34.56.78.
Escape character is '^]'.

exa-fw> show security flow session destination-port 80
Session ID: 9572, Policy name: HTTP/16, Timeout: 292, Valid
  In: 172.16.10.1/56121 --> 12.34.56.78/80;tcp, If: ge-0/0/4.0, Pkts: 2,
Bytes: 116
  Out: 12.34.56.78/80 --> 100.1.1.133/56121;tcp, If: ge-0/0/3.0, Pkts: 1,
Bytes: 64
Total sessions: 1
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
VR-DEVICE> telnet routing-instance exa-private 12.34.56.78 port 80 source
172.16.15.10
Trying 12.34.56.78...
Connected to 12.34.56.78.
Escape character is '^]'.

exa-fw> show security flow session destination-port 80
Session ID: 9582, Policy name: INTERNET/5, Timeout: 220, Valid
  In: 172.16.15.10/54716 --> 12.34.56.78/80;tcp, If: ge-0/0/5.15, Pkts: 2,
Bytes: 116
  Out: 12.34.56.78/80 --> 100.1.1.197/54716;tcp, If: ge-0/0/3.0, Pkts: 1,
Bytes: 64
Total sessions: 1
```

```
VR-DEVICE> telnet routing-instance untrust 100.1.1.3 port 8080
Trying 100.1.1.3...
Connected to 100.1.1.3.
Escape character is '^]'.

exa-fw> show security flow session destination-port 80
Session ID: 9625, Policy name: EXA-SRV-WEB/6, Timeout: 250, Valid
  In: 100.1.1.6/52344 --> 100.1.1.3/8080;tcp, If: ge-0/0/3.0, Pkts: 3, Bytes:
170
  Out: 172.16.30.11/80 --> 100.1.1.6/52344;tcp, If: ge-0/0/5.30, Pkts: 2,
Bytes: 116
Total sessions: 1
```

```
VR-DEVICE> telnet routing-instance untrust 100.1.1.3 port 3306
Trying 100.1.1.3...
Connected to 100.1.1.3.
Escape character is '^]'.

exa-fw> show security flow session destination-port 3306
Session ID: 9635, Policy name: EXA-SRV-DB/17, Timeout: 1796, Valid
  In: 100.1.1.6/54543 --> 100.1.1.3/3306;tcp, If: ge-0/0/3.0, Pkts: 2, Bytes:
116
  Out: 172.16.30.12/3306 --> 100.1.1.6/54543;tcp, If: ge-0/0/5.30, Pkts: 1,
Bytes: 64
Total sessions: 1
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
VR-DEVICE> telnet routing-instance exa-private 12.34.56.78 port 80 source
172.16.15.10
Trying 12.34.56.78...
Connected to 12.34.56.78.
Escape character is '^]'.

exa-fw> show security flow session destination-port 80
Session ID: 9582, Policy name: INTERNET/5, Timeout: 220, Valid
  In: 172.16.15.10/54716 --> 12.34.56.78/80;tcp, If: ge-0/0/5.15, Pkts: 2,
Bytes: 116
  Out: 12.34.56.78/80 --> 100.1.1.197/54716;tcp, If: ge-0/0/3.0, Pkts: 1,
Bytes: 64
Total sessions: 1
```

```
VR-DEVICE> telnet routing-instance untrust 100.1.1.4 port 12345
Trying 100.1.1.4...
Connected to 100.1.1.4.
Escape character is '^]'.
SSH-2.0-OpenSSH_6.6

exa-fw> show security flow session destination-port 22
Session ID: 9656, Policy name: EXA-SRV-SSH/18, Timeout: 1748, Valid
  In: 100.1.1.6/51872 --> 100.1.1.4/12345;tcp, If: ge-0/0/3.0, Pkts: 3, Bytes:
168
  Out: 172.16.30.13/22 --> 100.1.1.6/51872;tcp, If: ge-0/0/5.30, Pkts: 2,
Bytes: 137
Total sessions: 1
```

4) The connections leaving the headquarters through central cluster need to be translated in following way:
   a. All connections arriving on the cluster in the TRUST and INTERNAL zones and destined to the Internet need to be translated using the 80.1.1.128 - 80.1.1.159
   b. Bidirectional translation needs to be provided for the company's email server (172.16.60.199). The public IP address allocated for this purpose is 80.1.1.192. Untranslated traffic from the UNTRUST zone to the email server must be blocked.
   c. From the WAREHOUSE zone only the Websense appliance's (172.16.60.99) initiated connections to the Internet are translated. Use the 80.1.1.160 IP address.
   d. The servers located in the WAREHOUSE zone have to be reachable from the Internet.

© 2020 Juniper Networks, Inc. All rights reserved.

Server	Internal address	Internal port	Public address	Public port
Web server	172.16.60.205	80	80.1.1.200	8080
Database server	172.16.60.205	3306	80.1.1.200	3306
SSH server	172.16.60.206	22	80.1.1.201	22
Honeypot	172.16.60.207	All	80.1.1.202	All

e. Untranslated connections from the UNTRUST zone to these servers are not allowed.

```
{primary:node0}[edit]
lab@central-node0# show security nat
source {
    pool INTERNET {
        address {
            80.1.1.128/32 to 80.1.1.159/32;
        }
    }
    pool WEBSENSE {
        address {
            80.1.1.160/32;
        }
    }
    rule-set UNTRUST {
        from zone [ INTERNAL TRUST WAREHOUSE ];
        to zone UNTRUST;
        rule WEBSENSE {
            match {
                source-address 172.16.60.99/32;
                destination-address 0.0.0.0/0;
            }
        then {
            source-nat {
                pool {
                    WEBSENSE;
                }
            }
        }
    }
    rule INTERNET {
        match {
            source-address [ 172.16.50.0/24 172.16.55.0/24 ];
            destination-address 0.0.0.0/0;
        }
        then {
            source-nat {
                pool {
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
                        INTERNET;
                    }
                }
            }
        }
    }
}
destination {
    pool WAREHOUSE-SRV-WEB {
        address 172.16.60.205/32 port 80;
    }
    pool WAREHOUSE-SRV-DB {
        address 172.16.60.205/32;
    }
    pool WAREHOUSE-SRV-SSH {
        address 172.16.60.206/32;
    }
    pool WAREHOUSE-HONEYPOT {
        address 172.16.60.207/32;
    }
    rule-set SERVERS {
        from zone UNTRUST;
        rule WAREHOUSE-SRV-WEB {
            match {
                destination-address 80.1.1.200/32;
                destination-port {
                    8080;
                }
            }
            then {
                destination-nat {
                    pool {
                        WAREHOUSE-SRV-WEB;
                    }
                }
            }
        }
        rule WAREHOUSE-SRV-DB {
            match {
                destination-address 80.1.1.200/32;
                destination-port {
                    3306;
                }
            }
            then {
                destination-nat {
                    pool {
                        WAREHOUSE-SRV-DB;
                    }
                }
            }
        }
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
}
rule WAREHOUSE-SRV-SSH {
    match {
        destination-address 80.1.1.201/32;
        destination-port {
            22;
        }
    }
    then {
        destination-nat {
            pool {
                WAREHOUSE-SRV-SSH;
            }
        }
    }
    rule WAREHOUSE-HONEYPOT {
        match {
            destination-address 80.1.1.202/32;
        }
        then {
            destination-nat {
                pool {
                    WAREHOUSE-HONEYPOT;
                }
            }
        }
    }
}
static {
    rule-set SRV-MAIL {
        from zone UNTRUST;
        rule mail {
            match {
                destination-address 80.1.1.192/32;
            }
            then {
                static-nat {
                    prefix {
                        172.16.60.199/32;
                    }
                }
            }
        }
    }
}
```


© 2020 Juniper Networks, Inc. All rights reserved.

Task 6: IPsec VPN

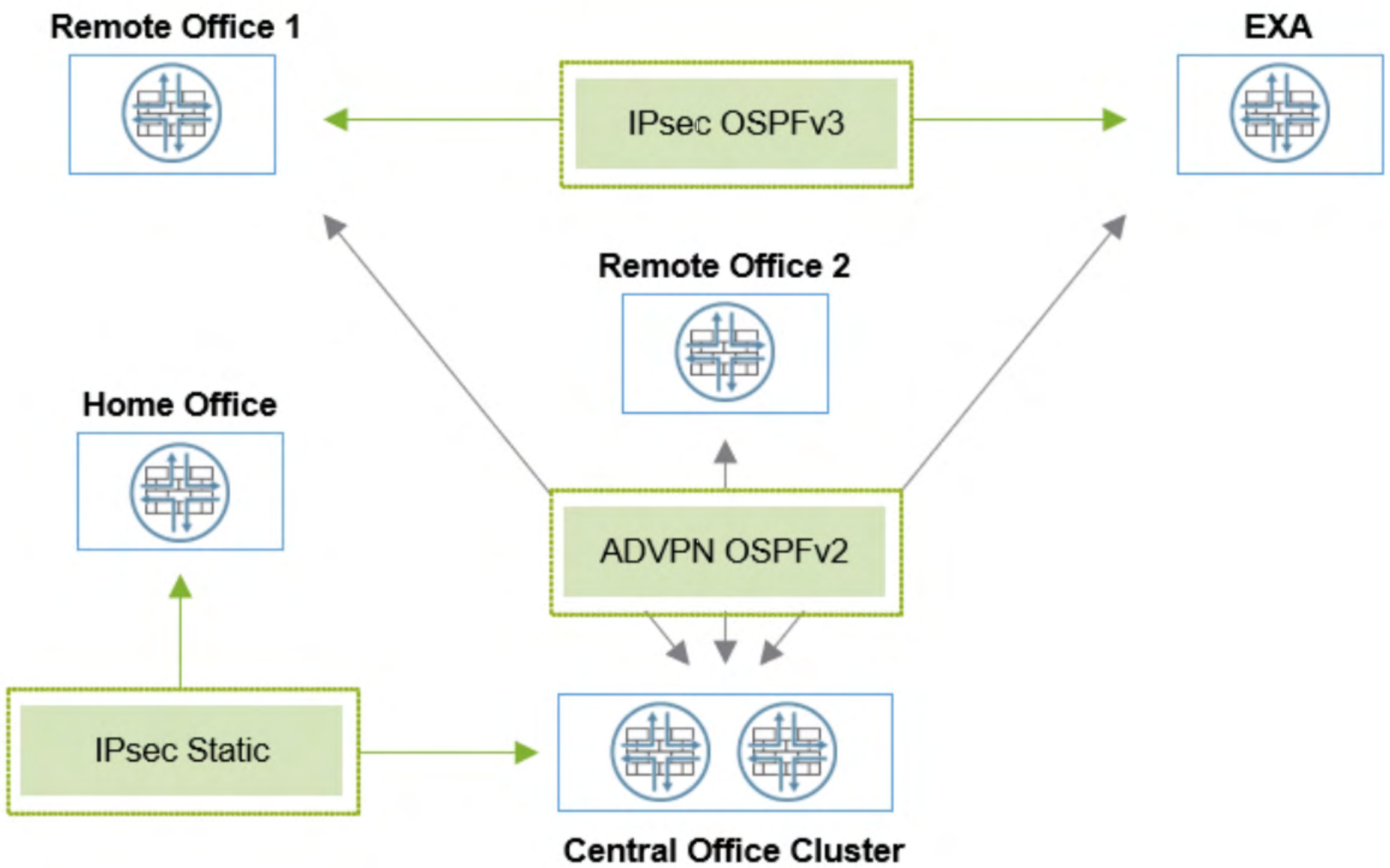


Figure 3: IPsec – VPNv4

1) Create and ADVPN between the central cluster and remote sites: Remote Office1 , Remote Office2 and the EXA company. Ensure that traffic between the remote sites and the EXA company do not need to traverse the central cluster.
   a. Configure static NAT on exa-fw and roffice to solve the issue of overlapping subnets in the security zone TRUST-EXA and TRUST-RO1. Use the subnet 172.16.110.0/24 to reach the TRUST-EXA security zone network and 172.16.111.0/24 to reach the TRUST-RO1 security zone network. You can use up to two static routes on the central office cluster.
   b. Ensure all your TRUST networks from any device can communicate with each other.
   c. Ensure the VPN traffic traverses the cluster member that owns priority of the VPN's termination interface

Roffice1:

As the certificates are preinstalled on the devices, you first need to verify the certificate name, distinguished-name and certificate type to be able to configure the IKE authentication method and reference the local-certificate name.

© 2020 Juniper Networks, Inc. All rights reserved.

```
[edit]
lab@roffice1# run show security pki local-certificate
Certificate identifier: srx1
  Issued to: srx1.juniper.net, Issued by: C = US, ST = California, L = Sunnyvale, O = Juniper,
OU = Base, emailAddress = student@juniper.net
  Validity:
    Not before: 01-30-2019 18:02 UTC
    Not after: 01-27-2029 18:02 UTC
  Public key algorithm: rsaEncryption(1024 bits)

[edit]
lab@roffice1# show interfaces st0.0
multipoint;
family inet {
    address 11.0.0.1/24;
}

[edit]
lab@roffice1# show security ike
proposal advpn-ike-prop {
    authentication-method rsa-signatures;
}
policy advpn-pol1 {
    proposals advpn-ike-prop;
    certificate {
        local-certificate srx1;
    }
}
gateway advpn-gw1 {
    ike-policy advpn-pol1;
    address 80.1.1.16;
    local-identity distinguished-name;
    remote-identity distinguished-name container O=Juniper;
    external-interface ge-0/0/3.0;
    local-address 80.1.1.1;
    advpn {
        suggester {
            disable;
        }
    }
    version v2-only;
}

[edit]
lab@roffice1# show security ipsec
proposal ipsecprop {
    protocol esp;
    authentication-algorithm hmac-sha-256-128;
    encryption-algorithm aes-256-cbc;
    lifetime-seconds 3600;
}
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
policy ipsecpol {
    proposals ipsecprop;
}
vpn advpn-vpn {
    bind-interface st0.0;
    ike {
        gateway advpn-gw1;
        ipsec-policy ipsecpol;
    }
    establish-tunnels immediately;
}

[edit]
lab@roffice1# show security pki
ca-profile advpn {
    ca-identity advpn;
    revocation-check {
        disable;
        crl {
            disable on-download-failure;
        }
    }
}

[edit]
lab@roffice1# show protocols ospf
area 0.0.0.0 {
    interface st0.0 {
        interface-type p2mp;
        retransmit-interval 1;
        dead-interval 40;
        demand-circuit;
        dynamic-neighbors;
    }
    interface ge-0/0/5.0 {
        passive;
    }
}

[edit]
lab@roffice1# show routing-options
static {
    route 172.16.110.0/24 next-hop 11.0.0.3;
}

[edit]
lab@roffice1# show security nat static rule-set OVERLAP
from interface st0.0;
rule OVERLAP-TRUST {
    match {
        destination-address 172.16.111.0/24;
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
    }
    then {
        static-nat {
            prefix {
                172.16.10.0/24;
            }
        }
    }
}

[edit]
lab@roffice1# show security zones security-zone VPN
host-inbound-traffic {
    system-services {
        ping;
    }
}
interfaces {
    st0.0 {
        host-inbound-traffic {
            system-services {
                ping;
            }
            protocols {
                ospf;
            }
        }
    }
}
```

Roffice2:

```
[edit]
lab@roffice2# run show security pki local-certificate
Certificate identifier: srx2
  Issued to: srx2.juniper.net, Issued by: C = US, ST = California, L = Sunnyvale, O = Juniper,
OU = Base, emailAddress = student@juniper.net
  Validity:
    Not before: 01-30-2019 18:02 UTC
    Not after: 01-27-2029 18:02 UTC
  Public key algorithm: rsaEncryption(1024 bits)

[edit]
lab@roffice2# show interfaces st0.0
multipoint;
family inet {
    address 11.0.0.2/24;
}

[edit]
lab@roffice2# show security ike
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
proposal advpn-ike-prop {
    authentication-method rsa-signatures;
}
policy advpn-pol1 {
    proposals advpn-ike-prop;
    certificate {
        local-certificate srx2;
    }
}
gateway advpn-gw1 {
    ike-policy advpn-pol1;
    address 80.1.1.16;
    local-identity distinguished-name;
    remote-identity distinguished-name container O=Juniper;
    external-interface ge-0/0/3.0;
    local-address 80.1.1.5;
    advpn {
        suggester {
            disable;
        }
    }
    version v2-only;
}

[edit]
lab@roffice2# show security ipsec
proposal ipsecprop {
    protocol esp;
    authentication-algorithm hmac-sha-256-128;
    encryption-algorithm aes-256-cbc;
    lifetime-seconds 3600;
}
policy ipsecpol {
    proposals ipsecprop;
}

vpn advpn-vpn {
    bind-interface st0.0;
    ike {
        gateway advpn-gw1;
        ipsec-policy ipsecpol;
    }
    establish-tunnels immediately;
}

[edit]
lab@roffice2# show protocols ospf
export to-ospf;
area 0.0.0.0 {
    interface ge-0/0/4.0 {
        passive;
    }
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
    interface st0.0 {
        interface-type p2mp;
        retransmit-interval 1;
        dead-interval 40;
        demand-circuit;
        dynamic-neighbors;
    }
    interface ge-0/0/5.0 {
        passive;
    }
}

[edit]
lab@roffice2# show security pki
ca-profile advpn {
    ca-identity advpn;
    revocation-check {
        disable;
        crl {
            disable on-download-failure;
        }
    }
}

[edit]
lab@roffice2# show routing-options
static {
    route 172.16.110.0/24 next-hop 11.0.0.3;
}

[edit]
lab@roffice2# show security zones security-zone VPN
host-inbound-traffic {
    system-services {
        ping;
    }
}
interfaces {
    st0.0 {
        host-inbound-traffic {
            system-services {
                ping;
            }
            protocols {
                bgp;
                ospf;
            }
        }
    }
}
```


© 2020 Juniper Networks, Inc. All rights reserved.

EXA:

```
[edit]
lab@exa-fw# run show security pki local-certificate
Certificate identifier: srx7
  Issued to: srx7.juniper.net, Issued by: C = US, ST = California, L = Sunnyvale, O = Juniper,
OU = Base, emailAddress = student@juniper.net
  Validity:
    Not before: 01-30-2019 18:02 UTC
    Not after: 01-27-2029 18:02 UTC
  Public key algorithm: rsaEncryption(1024 bits)
```

```
[edit]
lab@exa-fw# show security ike
proposal advpn-ike-prop {
    authentication-method rsa-signatures;
}
policy advpn-pol1 {
    proposals advpn-ike-prop;
    certificate {
        local-certificate srx7;
    }
}
gateway advpn-gw1 {
    ike-policy advpn-pol1;
    address 80.1.1.16;
    local-identity distinguished-name;
    remote-identity distinguished-name container O=Juniper;
    external-interface ge-0/0/3.0;
    local-address 100.1.1.1;
    advpn {
        suggester {
            disable;
        }
    }
    version v2-only;
}
```

```
[edit]
lab@exa-fw# show security ipsec
proposal ipsecprop {
    protocol esp;
    authentication-algorithm hmac-sha-256-128;
    encryption-algorithm aes-256-cbc;
    lifetime-seconds 3600;
}
policy ipsecpol {
    proposals ipsecprop;
}
vpn advpn-vpn {
    bind-interface st0.0;
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
    ike {
        gateway advpn-gw1;
        ipsec-policy ipsecpol;
    }
    establish-tunnels immediately;
}

[edit]
lab@exa-fw# show interfaces st0
unit 0 {
    multipoint;
    family inet {
        address 11.0.0.3/24;
    }
}

[edit]
lab@exa-fw# show protocols ospf
area 0.0.0.0 {
    interface st0.0 {
        interface-type p2mp;
        retransmit-interval 1;
        dead-interval 40;
        demand-circuit;
        dynamic-neighbors;
    }
    interface ge-0/0/5.15 {
        passive;
    }
    interface ge-0/0/5.30 {
        passive;
    }
}

[edit]
lab@exa-fw# show security nat static
rule-set OVERLAP {
    from interface st0.0;
    rule EXA-TRUST {
        match {
            destination-address 172.16.110.0/24;
        }
        then {
            static-nat {
                prefix {
                    172.16.10.0/24;
                }
            }
        }
    }
}
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
[edit]
lab@exa-fw# show security pki
ca-profile advpn {
    ca-identity advpn;
    revocation-check {
        disable;
        crl {
            disable on-download-failure;
        }
    }
}
```

```
[edit]
lab@exa-fw# show routing-options
static {
    route 172.16.111.0/24 next-hop 11.0.0.1;
}

[edit]
lab@exa-fw# show security zones security-zone VPN
host-inbound-traffic {
    system-services {
        ping;
    }
}
interfaces {
    st0.0 {
        host-inbound-traffic {
            protocols {
                bgp;
                ospf;
            }
        }
    }
}
```

Central-node:

```
{primary:node0}[edit]
lab@central-node0# run show security pki local-certificate
node0:
--------------------------------------------------------------------------
Certificate identifier: srx3
  Issued to: srx3.juniper.net, Issued by: C = US, ST = California, L = Sunnyvale, O = Juniper,
OU = Base, emailAddress = student@juniper.net
  Validity:
    Not before: 01-30-2019 18:02 UTC
    Not after: 01-27-2029 18:02 UTC
  Public key algorithm: rsaEncryption(1024 bits)
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
{primary:node0}[edit]
lab@central-node0# show interfaces st0.0
multipoint;
family inet {
    address 11.0.0.4/24;
}

{primary:node0}[edit]
lab@central-node0# show security pki
ca-profile advpn {
    ca-identity advpn;
    revocation-check {
        disable;
        crl {
            disable on-download-failure;
        }
    }
}

{primary:node0}[edit]
lab@central-node0# show security ike
proposal advpn-ike-prop {
    authentication-method rsa-signatures;
}
policy advpn-pol1 {
    mode main;
    proposals advpn-ike-prop;
    certificate {
        local-certificate srx3;
    }
}
gateway advpn-gw1 {
    ike-policy advpn-pol1;
    dynamic {
        distinguished-name {
            wildcard O=Juniper;
        }
        ike-user-type group-ike-id;
    }
    local-identity distinguished-name;
    external-interface lo0;
    local-address 80.1.1.16;
    advpn {
        partner {
            disable;
        }
    }
    version v2-only;
}
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
{primary:node0}[edit]
lab@central-node0# show security ipsec
proposal ipsecprop {
    protocol esp;
    authentication-algorithm hmac-sha-256-128;
    encryption-algorithm aes-256-cbc;
    lifetime-seconds 3600;
}
policy ipsecpol {
    proposals ipsecprop;
}
vpn advpn-vpn {
    bind-interface st0.0;
    ike {
        gateway advpn-gw1;
        ipsec-policy ipsecpol;
    }
}

{primary:node0}[edit]
lab@central-node0# show protocols ospf
export to-ospf;
area 0.0.0.0 {
    interface lo0.0 {
        passive;
    }
    interface st0.0 {
        interface-type p2mp;
        retransmit-interval 1;
        dead-interval 40;
        demand-circuit;
        dynamic-neighbors;
    }
}

{primary:node0}[edit]
lab@central-node0# show routing-options static
route 172.16.110.0/24 next-hop 11.0.0.3;
route 172.16.111.0/24 next-hop 11.0.0.1;

{primary:node0}[edit]
lab@central-node0# show routing-options aggregate
route 172.16.0.0/16;

{primary:node0}[edit]
lab@central-node0# show policy-options policy-statement to-ospf
term 1 {
    from {
        protocol aggregate;
        route-filter 172.16.0.0/16 exact;
    }
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
    then accept;
}

{primary:node0}[edit]
lab@central-node0# show security zones security-zone VPN
host-inbound-traffic {
    system-services {
        ping;
    }
}
interfaces {
    st0.0 {
        host-inbound-traffic {
            protocols {
                bgp;
                ospf;
            }
        }
    }
}
```

Verification:

```
{primary:node0}[edit]
lab@central-node0# run show security ike sa
node0:
--------------------------------------------------------------------------
Index   State  Initiator cookie  Responder cookie  Mode           Remote Address
7593736 UP     275130ec7ae68508  47aa2674f89301b7  IKEv2          80.1.1.1
7593737 UP     e6174f64327420be  5e740996e8ec0776  IKEv2          80.1.1.5

{primary:node0}[edit]
lab@central-node0# run show security ipsec sa
node0:
--------------------------------------------------------------------------
  Total active tunnels: 4     Total Ipsec sas: 4
  ID    Algorithm       SPI      Life:sec/kb  Mon lsys Port  Gateway
  <67108865 ESP:aes-cbc-256/sha256 9af2ca28 1577/ unlim - root 500 100.1.1.1
  >67108865 ESP:aes-cbc-256/sha256 20f60f09 1577/ unlim - root 500 100.1.1.1
  <67108866 ESP:aes-cbc-256/sha256 eb5c2326 1578/ unlim - root 500 80.1.1.1
  >67108866 ESP:aes-cbc-256/sha256 6efa00c6 1578/ unlim - root 500 80.1.1.1
  <67108867 ESP:aes-cbc-256/sha256 e9e127a 1591/ unlim - root 500 80.1.1.5
  >67108867 ESP:aes-cbc-256/sha256 b5ed476a 1591/ unlim - root 500 80.1.1.5

{primary:node0}[edit]
lab@central-node0# run show route protocol ospf brief

inet.0: 44 destinations, 49 routes (44 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

11.0.0.1/32        *[OSPF/10] 00:41:59, metric 1
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
                    > to 11.0.0.1 via st0.0
11.0.0.2/32         *[OSPF/10] 00:41:49, metric 1
                    > to 11.0.0.2 via st0.0
11.0.0.3/32         *[OSPF/10] 00:41:49, metric 1
                    > to 11.0.0.3 via st0.0
172.16.10.0/24      *[OSPF/10] 00:41:49, metric 2
                    > to 11.0.0.1 via st0.0
                      to 11.0.0.3 via st0.0
172.16.11.0/24      *[OSPF/10] 00:41:59, metric 2
                    > to 11.0.0.1 via st0.0
172.16.15.0/24      *[OSPF/10] 00:41:49, metric 2
                    > to 11.0.0.3 via st0.0
172.16.20.0/24      *[OSPF/10] 00:41:49, metric 2
                    > to 11.0.0.2 via st0.0
172.16.21.0/24      *[OSPF/10] 00:41:49, metric 2
                    > to 11.0.0.2 via st0.0
172.16.30.0/24      *[OSPF/10] 00:41:49, metric 2
                    > to 11.0.0.3 via st0.0
```

2) You need to configure an IPsec VPN between home office and central office node. You do not have access to the home office device and can only use CLI for troubleshooting. Here are the VPN parameters that were negotiated with the home office administrator:
   a. The home office security device uses statically assigned public IP address. It is always an initiator of the IPsec VPN and is configured in main mode. The IP address of home office gateway is unknown.
   b. IKE phase 1 proposal must include: preshared key “juniper”, DES, DH G1, MD5.
   c. IKE phase 2 proposal must include: DES, ESP, MD5.

Device	Interface	IP address	Zone
central	st0.1	-	VPN

   d. The IPsec VPN should provide access for all traffic types from the TRUST-H security zone to all TRUST security zones with the least possible number of policies
   e. The remote device is prepared to negotiate phase 2 and accept traffic using the 172.16.0.0/16 network
   f. The central cluster must forward traffic into the IPsec VPN using the node that bears redundancy group primacy of the tunnel’s endpoint interface.
   g. You can add a static route to reach the TRUST zone of the home office firewall

© 2020 Juniper Networks, Inc. All rights reserved.

Troubleshooting: The output of 'show security ike sa' should provide visibility of an attempt to initiate a connection. This only displays the remote address and not the local address to which the remote device is trying to connect to.

```
Index   State  Initiator cookie  Responder cookie  Mode
Remote Address

14435863 DOWN  2a75d20ad716b8db  0000000000000000 Any
200.1.1.100
```

Troubleshooting IKE: Traceoptions for IKE will display a result similar to the below. This output identifies that the remote IP address is 200.1.1.100 which is trying to establish a connection to our ip address 80.1.1.16 that represents the loopback address.

Bear in mind that traceoptions for debugging purpose should immediately be deactivated after the required troubleshooting is performed to alleviate the burden on the control plane.

```
# set security ike traceoptions file ike.log
# set security ike traceoptions flag ike

80.1.1.16:500 (Responder) <-> 200.1.1.100:500 { 8daa6f31 37560e0e - 7d7cc373
0818b5b0 [-1] / 0x00000000 } IP; Error = No proposal chosen (14)
```

Troubleshooting Flow: Traceoptions for Security Flow will observe an incoming packet and its path through flowd module. This allows to obtain the same information as abov as an alternative approach. The packet filter is essential to trim the mounf of information you wil gather from this procedure.

Bear in mind that traceoptions for debugging purpose should immediately be deactivated after the required troubleshooting is performed to alleviate the burden on the control plane.

```
# set security flow traceoptions file hoffice
# set security flow traceoptions flag basic-datapath
#  setsecurity  flow  traceoptions  packet-filter  hoffice  source-prefix
200.1.1.100/32
```

```
{primary:node0}[edit]
lab@central-node0# show security ike
proposal IKE-PROP-HOFFICE {
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
    authentication-method pre-shared-keys;
    dh-group group1;
    authentication-algorithm md5;
    encryption-algorithm des-cbc;
}
policy IKE-POL-HOFFICE {
    mode main;
    proposals IKE-PROP-HOFFICE;
    pre-shared-key ascii-text "$9$qPT3ApBSrv69rvWLVb.P5"; ## SECRET-DATA
}

gateway TO-HOFFICE {
    ike-policy IKE-POL-HOFFICE;
    address 200.1.1.100;
    external-interface lo0.0;
}

{primary:node0}[edit]
lab@central-node0# show security ipsec
proposal IPSEC-PROP-HOFFICE {
    protocol esp;
    authentication-algorithm hmac-md5-96;
    encryption-algorithm des-cbc;
}
policy IPSEC-POL-HOFFICE {
    proposals IPSEC-PROP-HOFFICE;
}
vpn TO-HOFFICE {
    bind-interface st0.1;
    ike {
        gateway TO-HOFFICE;
        proxy-identity {
            local 172.16.0.0/16;
            remote 172.16.77.0/24;
            service any;
        }
        ipsec-policy IPSEC-POL-HOFFICE;
    }
    establish-tunnels immediately;
}

{primary:node0}[edit]
lab@central-node0# show interfaces st0.1
family inet;

{primary:node0}[edit]
lab@central-node0# show routing-options static
route 172.16.77.0/24 next-hop st0.1;

{primary:node0}[edit]
lab@central-node0# show security zones security-zone VPN
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
host-inbound-traffic {
    system-services {
        ping;
    }
}
interfaces {
    st0.1;
    st0.0 {
        host-inbound-traffic {
            protocols {
                bgp;
                ospf;
            }
        }
    }
}
```

3) IPv6 networks should have full access between roffice1 and exa-fw devices
   a. Create a new route-based VPN associated with the st0.1 interface as shown in the table below
   b. Create or update existing interfaces with the following IPv6 addresses. Make sure all interfaces respond to ping requests.
   c. Ensure that the ipv6 networks are exchanged between both sites using OSPF.

Device	Interface	IPv6 address	Zone
roffice1	lo0.0	2016:abcd:ffff::2/64	UNTRUST
roffice1	ge-0/0/4.0	2016:abcd:b1::254/64	TRUST-RO1
roffice1	ge-0/0/5.0	2016:abcd:b2::254/64	PRIVATE-RO1
roffice1	st0.1	2002:111::2/64	VPN
exa-fw	lo0.0	2016:abcd:ffff::4/64	UNTRUST
exa-fw	ge-0/0/4.0	2016:abcd:d1::254/64	TRUST-EXA
exa-fw	ge-0/0/5.15	2016:abcd:d2::254/64	PRIVATE-EXA
exa-fw	st0.1	2002:111::1/64	VPN

Roffice1:

```
set interfaces ge-0/0/4 unit 0 family inet6 address 2016:abcd:b1::254/64
set interfaces ge-0/0/5 unit 0 family inet6 address 2016:abcd:b2::254/64
set interfaces st0 unit 1 family inet6 address 2016:111::2/126

[edit]
lab@roffice1# show security ike
policy IKE-POL-BASIC {
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
    mode aggressive;
    proposal-set basic;
    pre-shared-key ascii-text "$9$pTmG01h7Nb4oGVw39ApREdbs4Zj"; ## SECRET-DATA
}

gateway TO-EXA {
    ike-policy IKE-POL-BASIC;
    address 100.1.1.1;
    external-interface ge-0/0/3.0;
}

[edit]
lab@roffice1# show security ipsec
policy IPSEC-POL-BASIC {
    proposal-set basic;
}

vpn TO-EXA {
    bind-interface st0.1;
    ike {
        gateway TO-EXA;
        ipsec-policy IPSEC-POL-BASIC;
    }
    establish-tunnels immediately;
}

[edit]
lab@roffice1# show protocols ospf3
area 0.0.0.0 {
    interface st0.1 {
        interface-type p2p;
    }
    interface lo0.0 {
        passive;
    }
    interface ge-0/0/4.0 {
        passive;
    }
    interface ge-0/0/5.0;
}

[edit]
lab@roffice1# show security zones security-zone VPN
host-inbound-traffic {
    system-services {
        ping;
    }
}
interfaces {
    st0.0 {
        host-inbound-traffic {
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
        system-services {
            ping;
        }
        protocols {
            ospf;
        }
    }
}
st0.1 {
    host-inbound-traffic {
        protocols {
            ospf3;
        }
    }
}
```

Exa-fw:

```
set interfaces st0 unit 1 family inet6 address 2002:111::1/64

[edit]
lab@exa-fw# show security ike
policy IKE-POL-BASIC {
    mode aggressive;
    proposal-set basic;
    pre-shared-key ascii-text "$9$pTmG01h7Nb4oGVw39ApREdbs4Zj"; ## SECRET-DATA
}
gateway TO-ROFFICE1 {
    ike-policy IKE-POL-BASIC;
    address 80.1.1.1;
    external-interface ge-0/0/3.0;
}
```

```
[edit]
lab@exa-fw# show security ipsec
policy IPSEC-POl-BASIC {
    proposal-set basic;
}
vpn TO-ROFFICE1 {
    bind-interface st0.1;
    ike {
        gateway TO-ROFFICE1;
        ipsec-policy IPSEC-POl-BASIC;
    }
}

[edit]
lab@exa-fw# show protocols ospf3
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
area 0.0.0.0 {
    interface ge-0/0/4.0 {
        passive;
    }
    interface ge-0/0/5.15 {
        passive;
    }
    interface lo0.0 {
        passive;
    }
    interface st0.1 {
        interface-type p2p;
    }
}

[edit]
lab@exa-fw# show security zones security-zone VPN
host-inbound-traffic {
    system-services {
        ping;
    }
}
interfaces {
    st0.0 {
        host-inbound-traffic {
            protocols {
                bgp;
                ospf;
            }
        }
    }
    st0.1 {
        host-inbound-traffic {
            protocols {
                ospf3;
            }
        }
    }
}
```

Verification:

```
[edit]
lab@exa-fw# run show ospf3 neighbor
ID              Interface             State     Pri   Dead
192.168.1.1     st0.1                 Full      128     32
  Neighbor-address fe80::5254:10:fc18:28e6

[edit]
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
lab@exa-fw# run show route protocol ospf3
inet.0: 23 destinations, 23 routes (23 active, 0 holddown, 0 hidden)

inet6.0: 17 destinations, 18 routes (17 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

2002:111::/64       [OSPF3/10] 01:25:44, metric 1
                    > via st0.1
2016:abcd::/126    *[OSPF3/10] 01:25:21, metric 2
                    > via st0.1
2016:abcd:b1::/64  *[OSPF3/10] 01:25:21, metric 2
                    > via st0.1
2016:abcd:b2::/64  *[OSPF3/10] 01:25:21, metric 2
                    > via st0.1
2016:abcd:ffff::2/128
                   *[OSPF3/10] 01:25:21, metric 1
                    > via st0.1
ff02::5/128        *[OSPF3/10] 01:25:49, metric 1
                      MultiRecv
```

Task 7: Attack Prevention and Mitigation

1) Ensure that roffice1 and roffice2 are protected against following attacks arriving from the Internet:
    a. The TCP SYN segments flooding with the following thresholds and timer values:
        i. The destination thresholds values of 10000 TCP SYN segments per second.
        ii. Ensure that security device starts SYN Proxy protection mechanism when TCP SYN segments arrival rate reaches 500 segments per second.
        iii. Ensure that security device generates an alarm when TCP SYN segments arrival rate reaches 2500 segments per second.
        iv. The maximum time before incomplete sessions are dropped should be 10 seconds.
    b. Protect against fragmented TCP SYN segments.
    c. Protect against UDP flooding with the threshold of 500 packets per second.

© 2020 Juniper Networks, Inc. All rights reserved.

Roffice1:

```
[edit]
lab@roffice1# show security screen
ids-option SCREEN-UNTRUST {
    tcp {
        syn-frag;
        syn-flood {
            alarm-threshold 2500;
            attack-threshold 500;
            destination-threshold 10000;
            timeout 10;
        }
    }
    udp {
        flood {
            threshold 500;
        }
    }
}

[edit]
lab@roffice1# set security zones security-zone UNTRUST screen SCREEN-UNTRUST
```

Roffice2:

```
[edit]
lab@roffice2# show security screen
ids-option SCREEN-UNTRUST {
    tcp {
        syn-frag;
        syn-flood {
            alarm-threshold 2500;
            attack-threshold 500;
            destination-threshold 10000;
            timeout 10;
        }
    }
    udp {
        flood {
            threshold 500;
        }
    }
}

[edit]
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
lab@roffice2# set security zones security-zone UNTRUST screen SCREEN-UNTRUST
```

2) Ensure that building1 and building2 are protected against the following reconnaissance attempts arriving from the INTERNAL security zone:
   a. IP address sweep and port scan both a detection rate of 10 packets arrived per 2 ms time interval.
   b. Detect IP packets with following values in the Options field:
      iii. Record-route option.
      iv. Timestamp option.
   c. Protect against following operating systems probes:
      iii. The TCP segment has both SYN and FIN flags set.
      iv. The TCP segment has no flags set.
   d. Ensure that detection of malicious traffic results in alarm generation instead of dropping the packets belonging to malicious packet flow.

```
[edit]
lab@building# show security screen
ids-option SCREEN-INTERNAL {
    alarm-without-drop;
    icmp {
        ip-sweep threshold 2000;
    }
    ip {
        record-route-option;
        timestamp-option;
    }
    tcp {
        syn-fin;
        tcp-no-flag;
        port-scan threshold 2000;
    }
}
```

```
[edit]
lab@building# set security zones security-zone INTERNAL-B1 screen SCREEN-INTERNAL

[edit]
lab@building# set security zones security-zone INTERNAL-B2 screen SCREEN-INTERNAL
```

3) Configure cluster in such a way to protect server 172.16.60.205 and 172.16.60.206:
   a. The uploading of exe or rpm files to the 172.16.60.206 server via FTP is allowed only from the TRUST security zone and prohibited from everywhere else. Each detected attempt results in silently dropping client's sessions.
   b. Allow anonymous access to the FTP service of the 172.16.60.206 server from any TRUST and the TESTBED security zones. Restrict access for the rest of the network. Silently drop packets from unauthorized hosts, block

© 2020 Juniper Networks, Inc. All rights reserved.

them for 1 hour and generate log messages with severity level Major and alert flag.

c. Protect servers against scanning and worms from the INTERNAL and TESTBED security zones. Each detected attempt results in silently dropping packets.

```
{primary:node0}[edit security idp]
lab@central-node0#show
 idp {
    idp-policy CENTRAL-IDP {
        rulebase-ips {
            rule FILE-ATTACK {
    match {
        from-zone any;
        source-address any;
        to-zone WAREHOUSE;
        destination-address WAREHOUSE-SRV-206;
        application junos-ftp;
        attacks {
            custom-attacks FILE-ATTACK;
        }
    }
    then {
        action {
            drop-connection;
        }
    }
}
rule ANONYMOUS-ATTACK {
    match {
        from-zone any;
        source-address any;
        to-zone WAREHOUSE;
        destination-address WAREHOUSE-SRV-206;
        application junos-ftp;
        attacks {
            custom-attacks ANONYMOUS-ATTACK;
        }
}
then {
    action {
        drop-packet;
    }
    ip-action {
        ip-block;
        target source-address;
        timeout 3600;
    }
    notification {
        log-attacks {
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
                    alert;
                }
            }
        }
    }
}
rulebase-exempt {
    rule FILE-ATTACK {
        match {
            from-zone TRUST;
            source-address any;
            to-zone WAREHOUSE;
            destination-address WAREHOUSE-SRV-206;
            attacks {
                custom-attacks FILE-ATTACK;
            }
        }
    }
    rule ANONYMOUS-TRUST {
        match {
            from-zone TRUST;
            source-address any;
            to-zone WAREHOUSE;
            destination-address WAREHOUSE-SRV-206;
            attacks {
                custom-attacks ANONYMOUS-ATTACK;
            }
        }
    }
    rule ANONYMOUS-TESTBED {
        match {
            from-zone TESTBED;
            source-address any;
            to-zone WAREHOUSE;
            destination-address WAREHOUSE-SRV-206;
            attacks {
                custom-attacks ANONYMOUS-ATTACK;
            }
        }
    }
}
custom-attack FILE-ATTACK {
    severity major;
    attack-type {
        chain {
            expression "exe or rpm";
            member exe {
                attack-type {
                    signature {
                        context ftp-put-filename;
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
                pattern ".*\.\[exe\]";
                direction client-to-server;
            }
        }
    }
    member rpm {
        attack-type {
            signature {
                context ftp-put-filename;
                pattern ".*\.\[rpm\]";
                direction client-to-server;
            }
        }
    }
    custom-attack ANONYMOUS-ATTACK {
        severity major;
        attack-type {
            signature {
                context ftp-username;
                pattern "^anonymous$";
                direction client-to-server;
            }
        }
    }
}

{primary:node0}[edit]
lab@central-node0# show security policies global policy WAREHOUSE
match {
    source-address any;
    destination-address CENTRAL-WAREHOUSE;
    application junos-ftp;
    to-zone WAREHOUSE;
}
then {
    permit {
        application-services {
            idp;
        }
    }
}
```


© 2020 Juniper Networks, Inc. All rights reserved.

Task 8: Advanced Services – Central cluster

1) Disable application system cache completely.

```
{primary:node0}[edit]
lab@central-node0# show services application-identification
no-application-system-cache;
```

Verification

```
{primary:node0}[edit]
lab@central-node0# run show services application-identification application-system-cache
node0:
--------------------------------------------------------------------------
Application System Cache Configurations:
  application-cache: off
    Cache lookup for security-services: off
    Cache lookup for miscellaneous-services: on
  cache-entry-timeout: 3600 seconds

node1:
--------------------------------------------------------------------------
Application System Cache Configurations:
  application-cache: off
    Cache lookup for security-services: off
    Cache lookup for miscellaneous-services: on
  cache-entry-timeout: 3600 seconds    cache-entry-timeout: 3600 seconds
```

2) Enable AppTrack to provide information about applications used in the TRUST zone. The first message for each connection has to be generated 2 minutes after the application has been identified and then an update has to be created every 6 minutes.

```
{primary:node0}[edit]
lab@central-node0# show security application-tracking
first-update-interval 2;
session-update-interval 6;

{primary:node0}[edit]
lab@central-node0# show security zones security-zone TRUST
host-inbound-traffic {
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
    system-services {
        ping;
        ssh;
    }
}
interfaces {
    reth0.50;
}
application-tracking;
```

3) Block the junos:MSN application over port 80 from the TRUST zone to the UNTRUST zone.

```
{primary:node0}[edit security policies from-zone TRUST to-zone UNTRUST policy HTTP-FTP]
lab@central-node0# show
match {
    source-address CENTRAL-TRUST;
    destination-address any;
    application [ junos-http junos-ftp ];
    dynamic-application junos:MSN;
}
then {
    permit {
        application-services {
            utm-policy CENTRAL-Content;
        }
    }
    log {
        session-init;
        session-close;
    }
}
```


© 2020 Juniper Networks, Inc. All rights reserved.

Verification

```
> show security policies from-zone TRUST to-zone UNTRUST policy-name HTTP-FTP
detail | match session
  Session log: at-create, at-close
```

4) Ensure the junos:MEGAUPLOAD application over the port 80 from the TRUST zone to the UNTRUST zone will have the loss priority of "high" if it crosses 5000 kb/s with bursts of 15000 bytes. This has to be applied in both directions - client to server and server to client.

```
{primary:node0}[edit]
lab@central-node0# show class-of-service
application-traffic-control {
    rate-limiters MEGA {
        bandwidth-limit 5000;
        burst-size-limit 15000;
    }
    rule-sets MEGA {
        rule rate {
            match {
                application junos:MEGAUPLOAD;
            }
            then {
                rate-limit {
                    client-to-server MEGA;
                    server-to-client MEGA;
                    loss-priority-high;
                }
            }
        }
    }
}

{primary:node0}[edit security policies from-zone TRUST to-zone UNTRUST policy HTTP-FTP]
lab@central-node0# show
match {
    source-address CENTRAL-TRUST;
    destination-address any;
    application [ junos-http junos-ftp ];
    dynamic-application junos:MSN;
}
then {
    permit {
        application-services {
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
            utm-policy CENTRAL-Content;
            application-traffic-control {
                rule-set MEGA;
            }
        }
    }
    log {
        session-init;
        session-close;
    }
}
```

5) Make sure the SRX knows exactly what is going on in the encrypted sessions on the default HTTPS port from the TESTBED zone to the UNTRUST zone. The certificate for signing the modified server certificates should be locally generated on the SRX device with following values:
   - type: rsa
   - key size: 512
   - domain name: juniper.net
   - subject: DC=JNPR,CN=juniper,OU=unit-1,O=juniper,SN=1234,L=USA,ST=CA,C=US
   - email-ID: noreply@juniper.net

   The SRX will not authenticate any servers. Make sure everything about SSL proxy operations is logged in the “ssl-proxy” file.

```
{primary:node0}[edit]
lab@central-node0# run request security pki generate-key-pair certificate-id MY-CERT size 1024
type rsa
      node0:
--------------------------------------------------------------------------
Generated key pair MY-CERT, key size 1024 bits

run request security pki local-certificate generate-self-signed certificate-id MY-CERT domain-
name juniper.net subject "DC=JNPR,CN=Juniper,OU=unit-1,O=Juniper,SN=1234,L=USA,ST=CA,C=US"
email noreply@juniper.net add-ca-constraint

node1:
--------------------------------------------------------------------------
Self-signed certificate generated and loaded successfully


{primary:node0}[edit]
lab@central-node0# show services ssl
proxy {
    profile CENTRAL-SSL {
        root-ca MY-CERT;
        actions {
            ignore-server-auth-failure;
            log {
                all;
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
            }
        }
    }
}

{primary:node0}[edit]
lab@central-node0# show security policies from-zone TESTBED to-zone UNTRUST
policy HTTPS {
    match {
        source-address CENTRAL-TESTBED;
        destination-address any;
        application junos-https;
    }
    then {
        permit {
            application-services {
                ssl-proxy {
                    profile-name CENTRAL-SSL;
                }
            }
        }
    }
}

{primary:node0}[edit]
lab@central-node0# show system syslog file ssl-proxy
any any;
match SSL;
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
lab@central-node0# run show security policies from-zone TESTBED to-zone
UNTRUST policy-name HTTPS detail
node0:
--------------------------------------------------------------------------
Policy: HTTPS, action-type: permit, State: enabled, Index: 17, Scope Policy:
0
  Policy Type: Configured
  Sequence number: 1
  From zone: TESTBED, To zone: UNTRUST
  Source addresses:
    CENTRAL-TESTBED7(global): 172.16.70.0/24
    CENTRAL-TESTBED6(global): 172.16.65.0/24
  Destination addresses:
    any-ipv4(global): 0.0.0.0/0
    any-ipv6(global): ::/0
  Application: junos-https
    IP protocol: tcp, ALG: 0, Inactivity timeout: 1800
      Source port range: [0-0]
      Destination port range: [443-443]
  Per policy TCP Options: SYN check: No, SEQ check: No, Window scale: No
  Intrusion Detection and Prevention: disabled
  Unified Access Control: disabled
  SSL Proxy Profile Name: CENTRAL-SSL
```

6) Configure Juniper Identity Management Service to be able to identify network traffic on cluster 1 based on IP address as well as user and device context. Implement your solution for authenticated, unauthenticated and unknown users in the TRUST to UNTRUST zone

```
{primary:node0}[edit services user-identification]
lab@central-node0# show
identity-management {
    authentication-entry-timeout 60;
    connection {
        connect-method https;
        port 443;
        primary {
            address 10.10.1.121;
            client-id jncie;
            client-secret "$9$TF6ArlMXxdBIyKMWx7jHkPz3"; ## SECRET-DATA
        }
        token-api oauth_token/oauth;
        query-api user_query/v2;
    }
}
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
{primary:node0}[edit]
lab@central-node0# show security policies global
policy TRUST {
    match {
        source-address TRUST-NETWORKS;
        destination-address TRUST-NETWORKS;
        application any;
        source-identity any;
    }
    then {
        permit;
    }
}
```

Verify is the AD server is reachable and the HTTPS connection is up and running.

```
{primary:node0}[edit]
lab@srx3# run show services user-identification identity-management status
node0:
--------------------------------------------------------------------------
Primary server :
    Address                       : 10.10.1.121
    Port                          : 443
    Connection method             : HTTPS
    Connection status             : Online
    Last received status message : OK (200)
    Access token                  : j1gwTLfcgDBf7CMtbneFTP1P6WyJq8VyGCzNUsm
    Token expire time             : 2019-01-11 11:24:28
Secondary server :
    Address                       : Not configured
```

7) SoundCloud traffic originated in the INTERNAL zone, leaving the Central Office must travers interface ge-7/0/3 and use interface ge-0/0/3 as backup.

```
{primary:node0}[edit]
lab@central-node0# show routing-options
interface-routes {
    rib-group inet apbr;
}
rib-groups {
    apbr {
        import-rib [ inet.0 apbr.inet.0 ];
        import-policy apbr;
    }
}
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
{primary:node0}[edit]
lab@central-node0# show policy-options policy-statement apbr
term 1 {
    from interface ge-0/0/3.0;
    from interface ge-7/0/3.0;
    to rib apbr.inet.0;
    then accept;
}
term 2 {
    then reject;
}

{primary:node0}[edit]
lab@central-node0# show security zones security-zone INTERNAL
...
advance-policy-based-routing-profile {
    apbr;
}

{primary:node0}[edit]
lab@central-node0# show security advance-policy-based-routing
profile apbr {
    rule 1 {
        match {
            dynamic-application junos:SOUNDCLOUD;
        }
        then {
            routing-instance apbr;
        }
    }
}

{primary:node0}[edit]
lab@central-node0# show routing-instances apbr
instance-type forwarding;
routing-options {
    static {
        route 0.0.0.0/0 {
            next-hop 80.1.1.13;
            qualified-next-hop 80.1.1.9 {
                preference 7;
            }
        }
    }
}

{primary:node0}[edit]
lab@central-node0# run show route table apbr
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
apbr.inet.0: 3 destinations, 4 routes (3 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

0.0.0.0/0          *[Static/5] 02:06:26
                    > to 80.1.1.13 via ge-7/0/3.0
                    [Static/7] 02:06:26
                    > to 80.1.1.9 via ge-0/0/3.0
80.1.1.8/30        *[Direct/0] 02:06:26
                    > via ge-0/0/3.0
80.1.1.12/30       *[Direct/0] 02:06:26
                    > via ge-7/0/3.0
```

Task 9: Software Defined Secure Network (SDSN)

1) Create a new SkyATP realm. Enroll Policy Enforcer and the central office cluster in the newly created Sky ATP Realm through Security Director

   Use the information below to setup the Sky ATP Realm:

SkyATP Realm	jnciesec-xxx (where xxx is your lab username)
Username	jnciesec-xxx@stu.juniper.net
Password	lab123@Lab
Juniper SSO account	eduservicenow@gmail.com
Juniper SSO password	********

   Use the information for Security Director and Policy Enforcer:

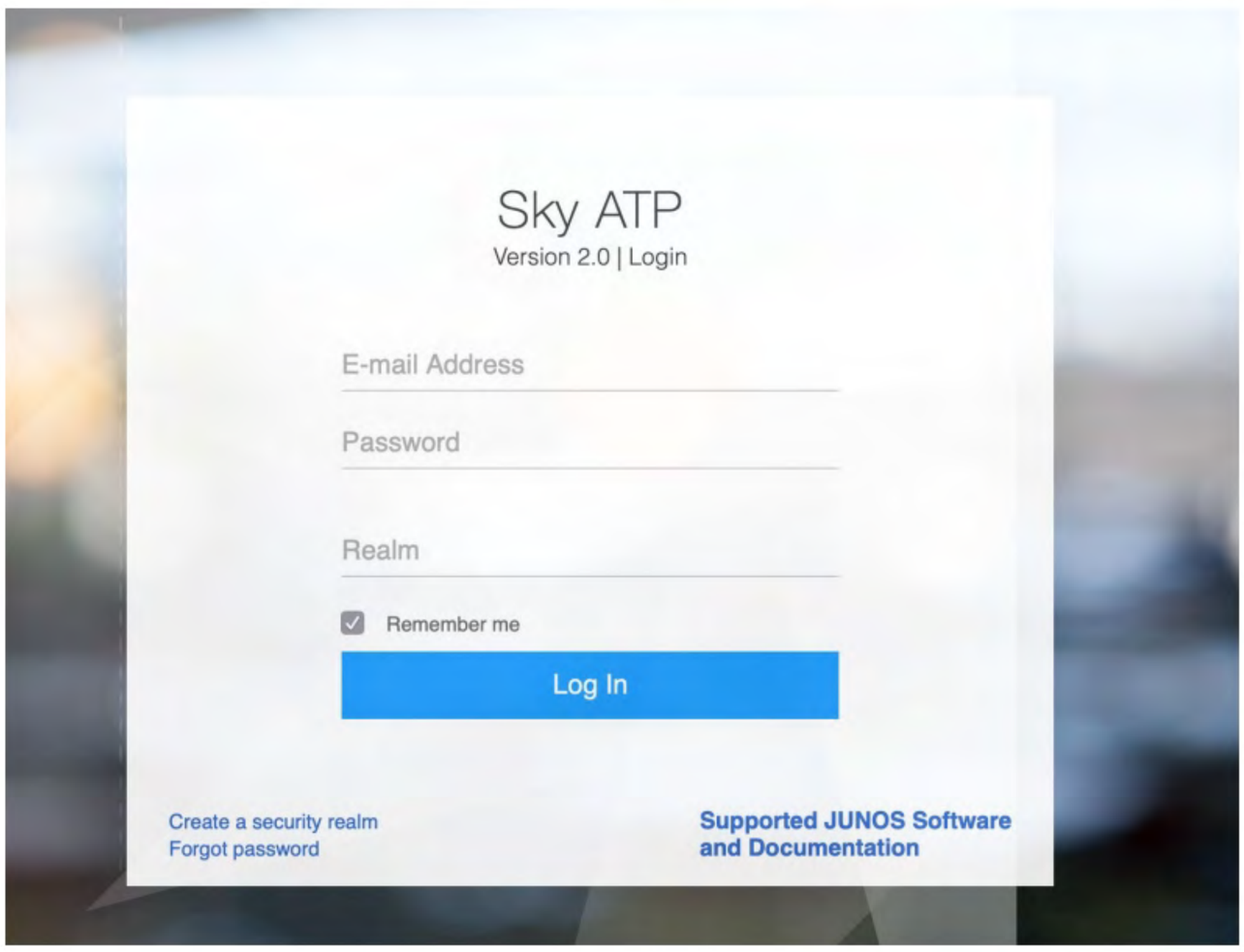
Security Director Username	super
Security Director Password	lab123@Lab
Security Director IP	10.10.1.100
Policy Enforcer Username	root
Policy Enforcer Password	lab123@Lab
Policy Enforcer IP	10.10.1.123

   Note: The password for the Juniper SSO account is auto populated in the Firefox browser on the Student Desktop. For this reason, it is important to use the Firefox browser on the Student Desktop to create the Sky ATP realm.

© 2020 Juniper Networks, Inc. All rights reserved.

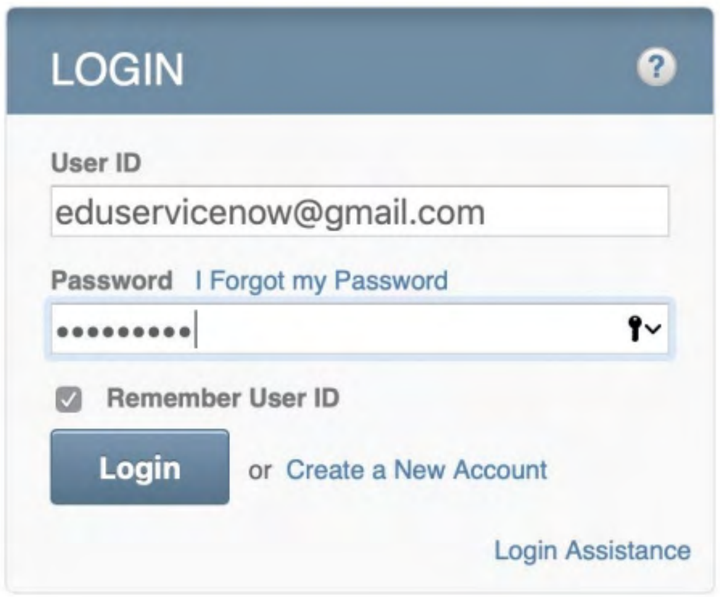
a) The first step is to create a new SkyATP realm. To do this you have to navigate to the following URL: http://amer.sky.junipersecurity.net using the Firefox browser of the Student Desktop.

Click on "**Create a security realm**" in the lower left corner of the Sky ATP login screen.



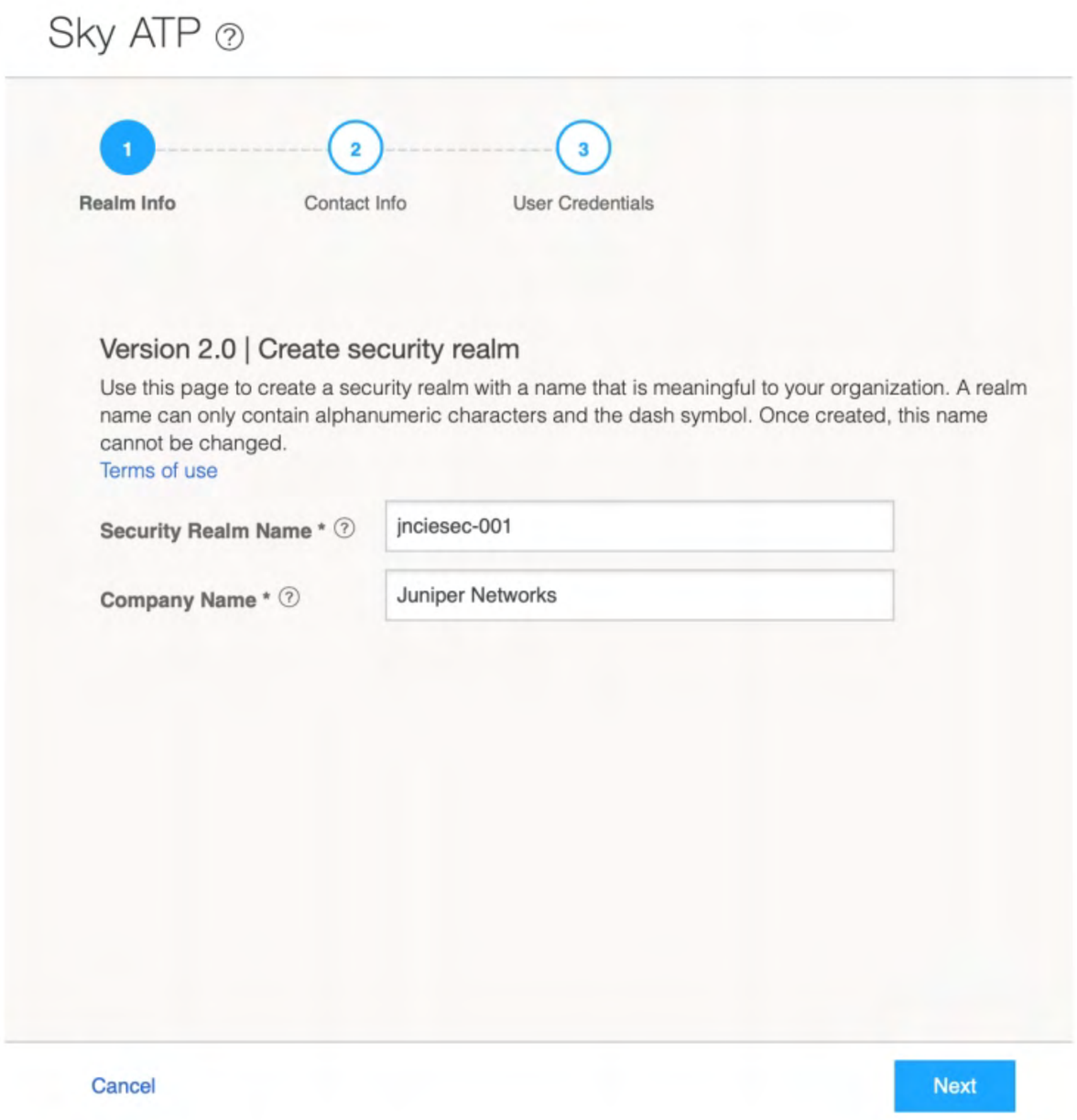
© 2020 Juniper Networks, Inc. All rights reserved.

b) To create a new SkyATP realm you are redirected to Juniper Network Single Sign On (SSO) and you must login with a valid account. As mentioned in the instructions it is important to use the Firefox browser installed on the student desktop as the password for userID: eduservicenow@gmail.com is auto populated. Click on the login button to proceed.



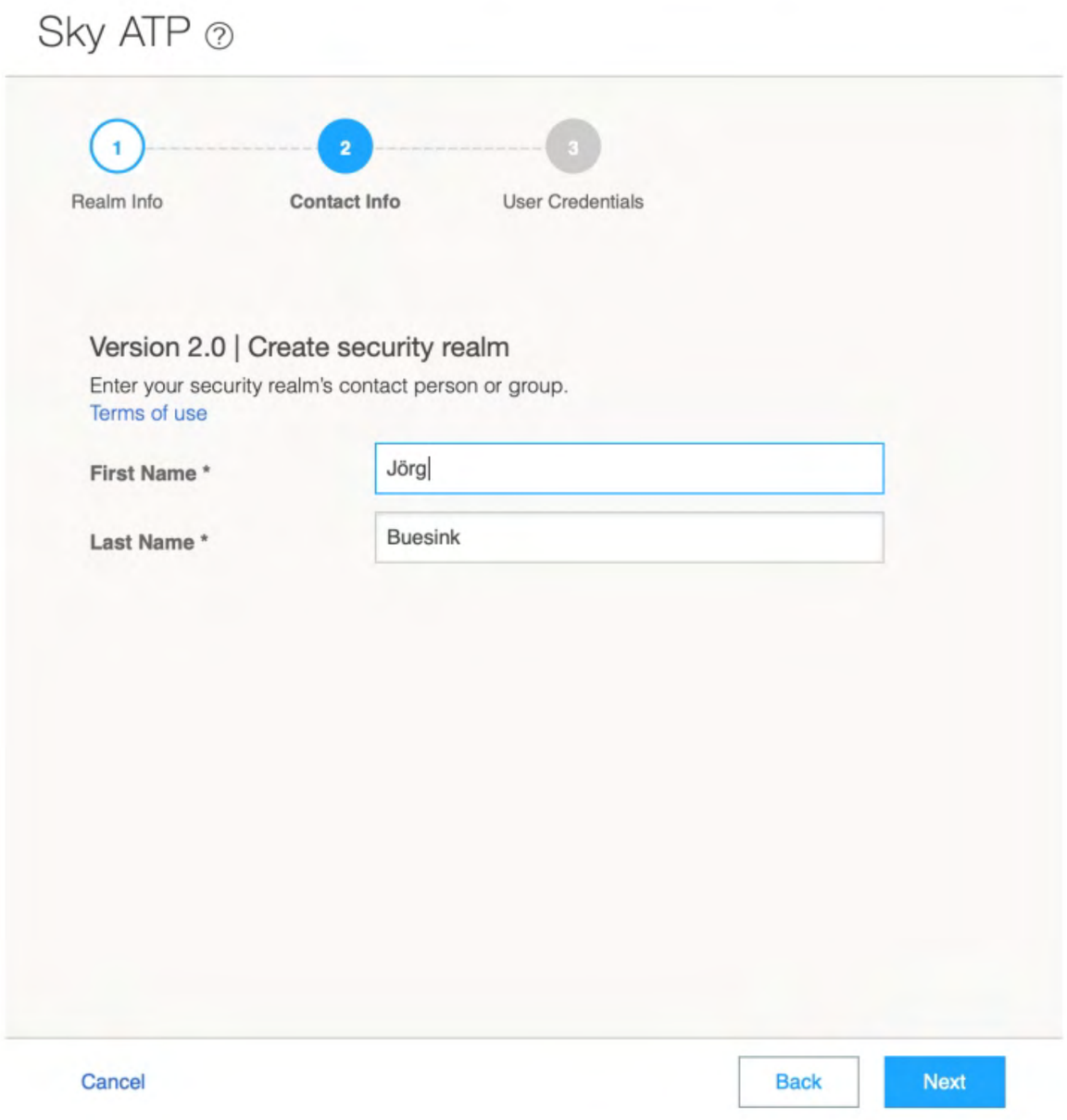
© 2020 Juniper Networks, Inc. All rights reserved.

c) Enter the Security Realm Name as provided with your lab access instructions. In this case the Security Realm Name: jnciesec-001 is used. Also specify the company name and click the “Next” button.



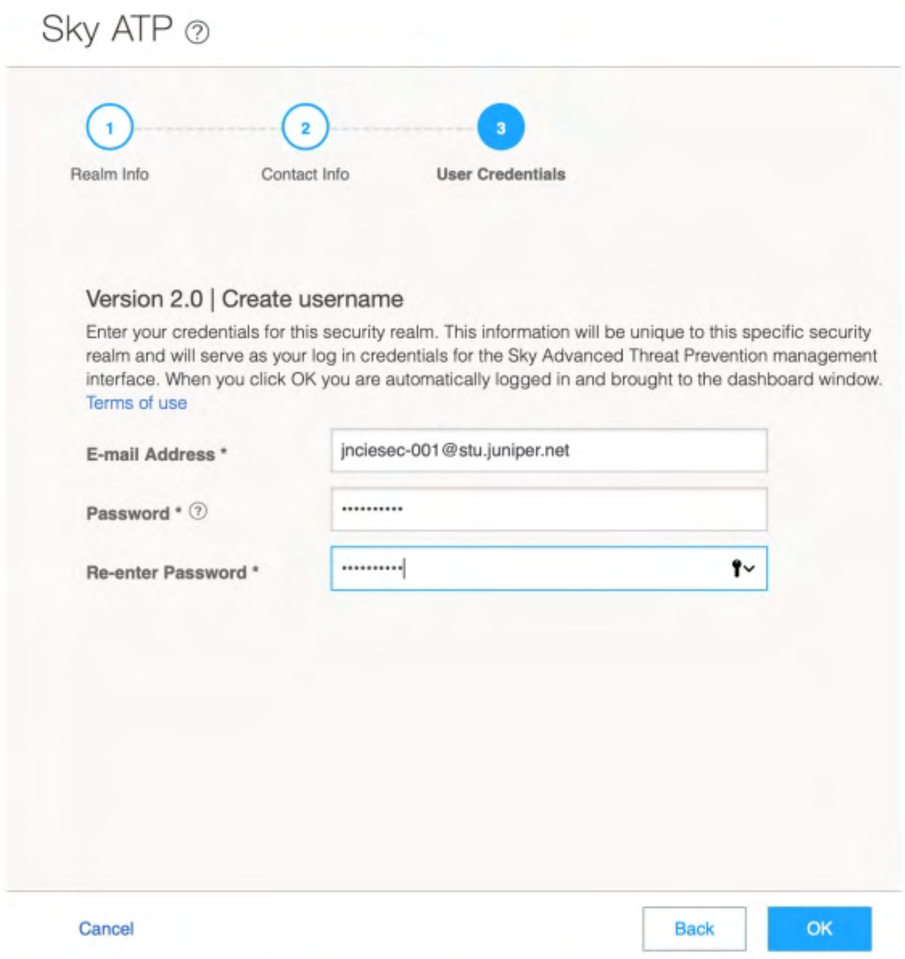
© 2020 Juniper Networks, Inc. All rights reserved.

d) Enter your first and last name and click the “Next” button.

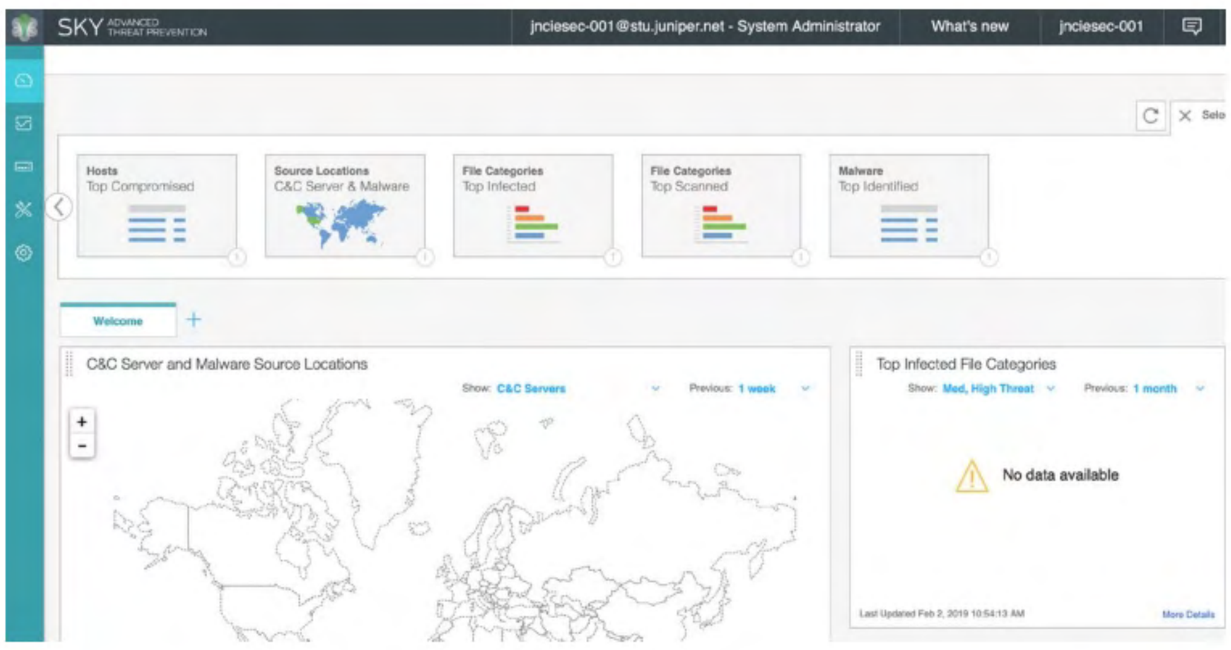


© 2020 Juniper Networks, Inc. All rights reserved.

e) Specify the user credentials to be used to login to the Sky ATP realm. In this case the email address: jnciesec-001@stu.juniper.net is used with password lab123@Lab. Make sure you use the credentials provided as mentioned in the lab access instructions. Press the “Ok” button.

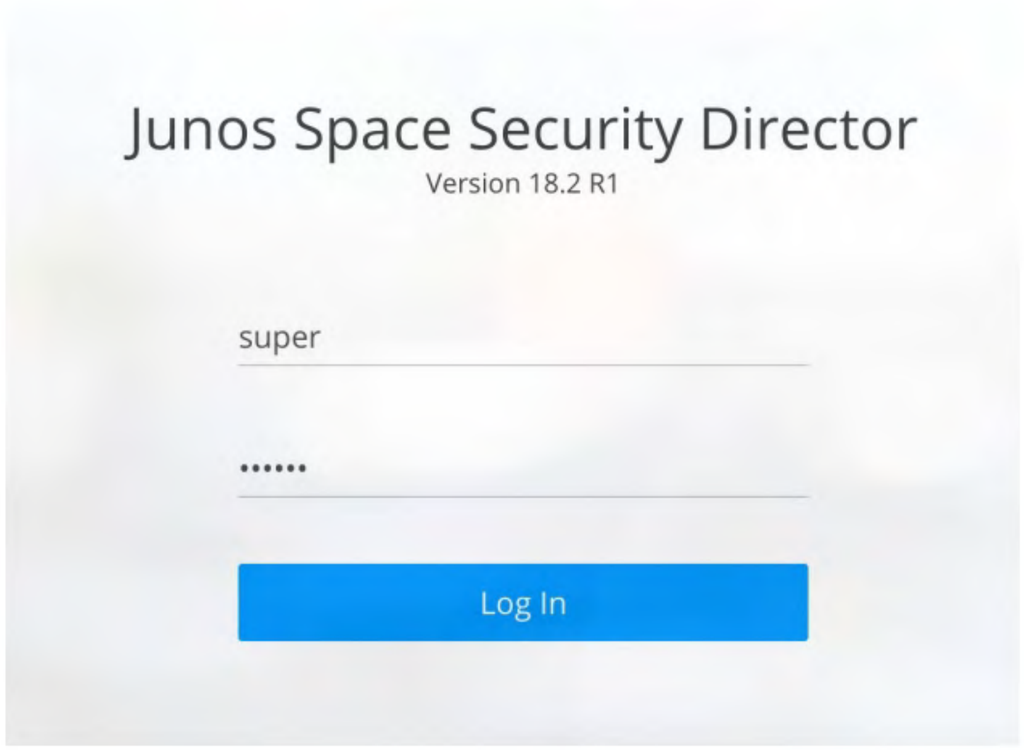


f) If you completed all steps correctly the SkyATP realm is created and you will auto login to the Sky ATP realm. At the top of the screen you should see your Sky ATP email address and the Sky ATP realm name. You can now close the Firefox browser as we will use Security Director to enroll the required devices.



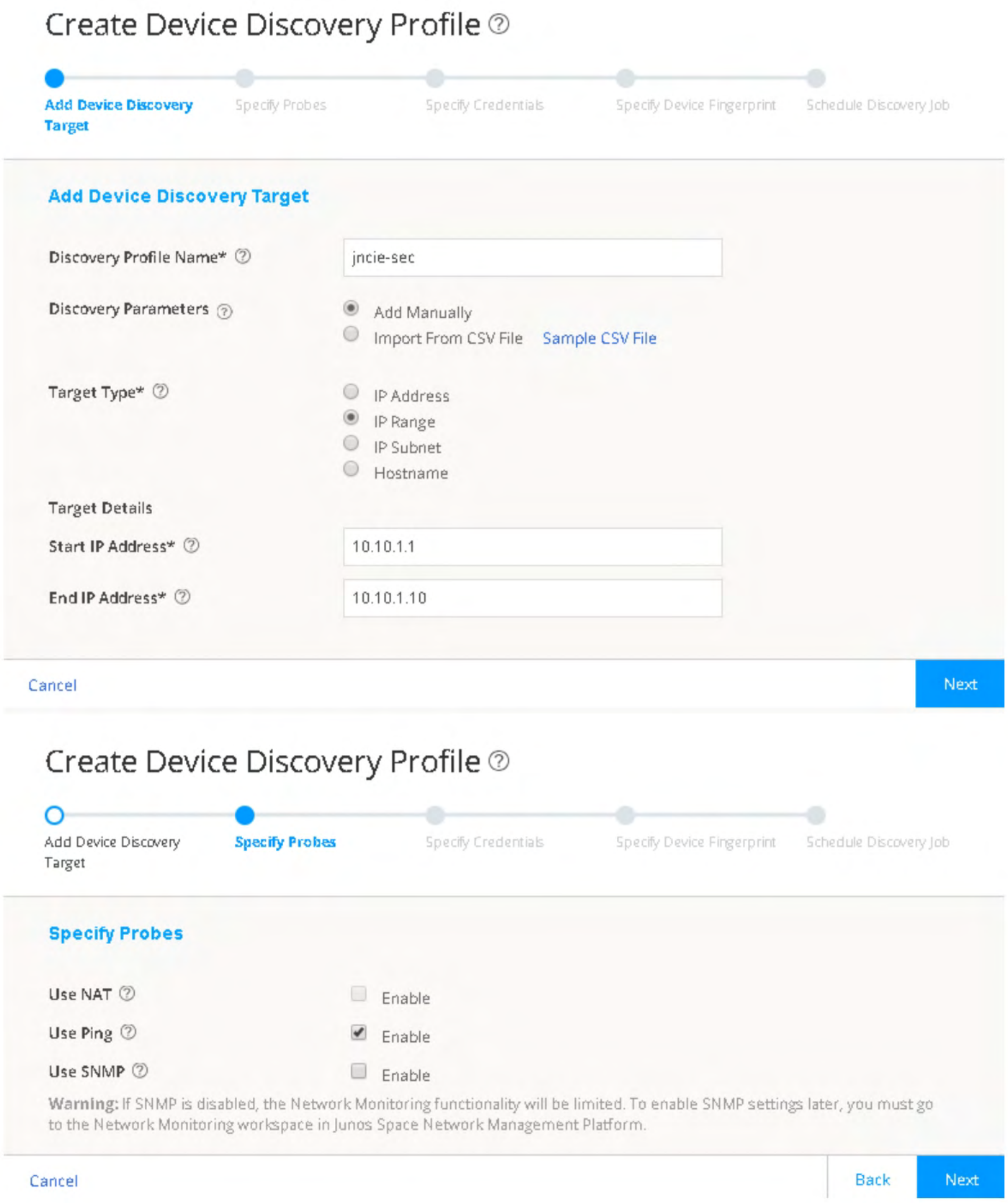
© 2020 Juniper Networks, Inc. All rights reserved.

g) Access Security Director using the GUI interface and enter the login credentials as provided in your lab access instructions.

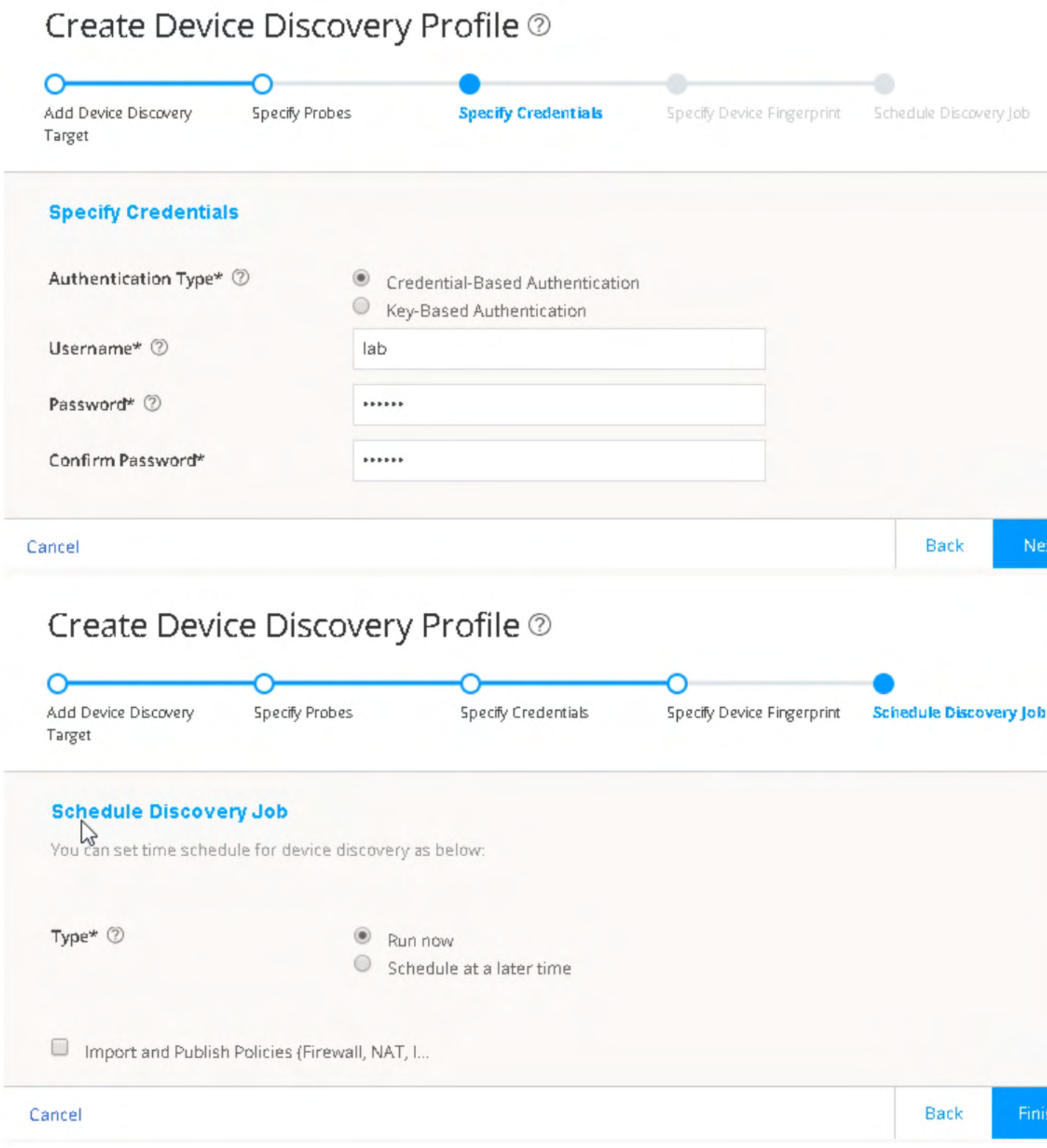


h) Navigate to the Devices / Device Discovery workspace. Create a new discovery job to discover the SRX devices and vQFX device (10.10.1.1 – 10.10.1.10) as the following screenshots show. Note that vQFX is located between cluster 2 (srx5/srx6) and its internal hosts. Note that if the discovery job fails for any reason, run it again until all the devices are in the managed state.
    a) Job Name: jncie-sec
    b) IP Address Range: 10.10.1.1 – 10.10.1.10
    c) Probes:
        i. Use NAT: unchecked
        ii. Use Ping: checked
        iii. Use SNMP: unchecked
    d) Credentials
        i. Username: lab
        ii. Password: lab123
    e) Schedule Discovery Job
        i. Type: Run now
        ii. Import and Publish Policies: unchecked

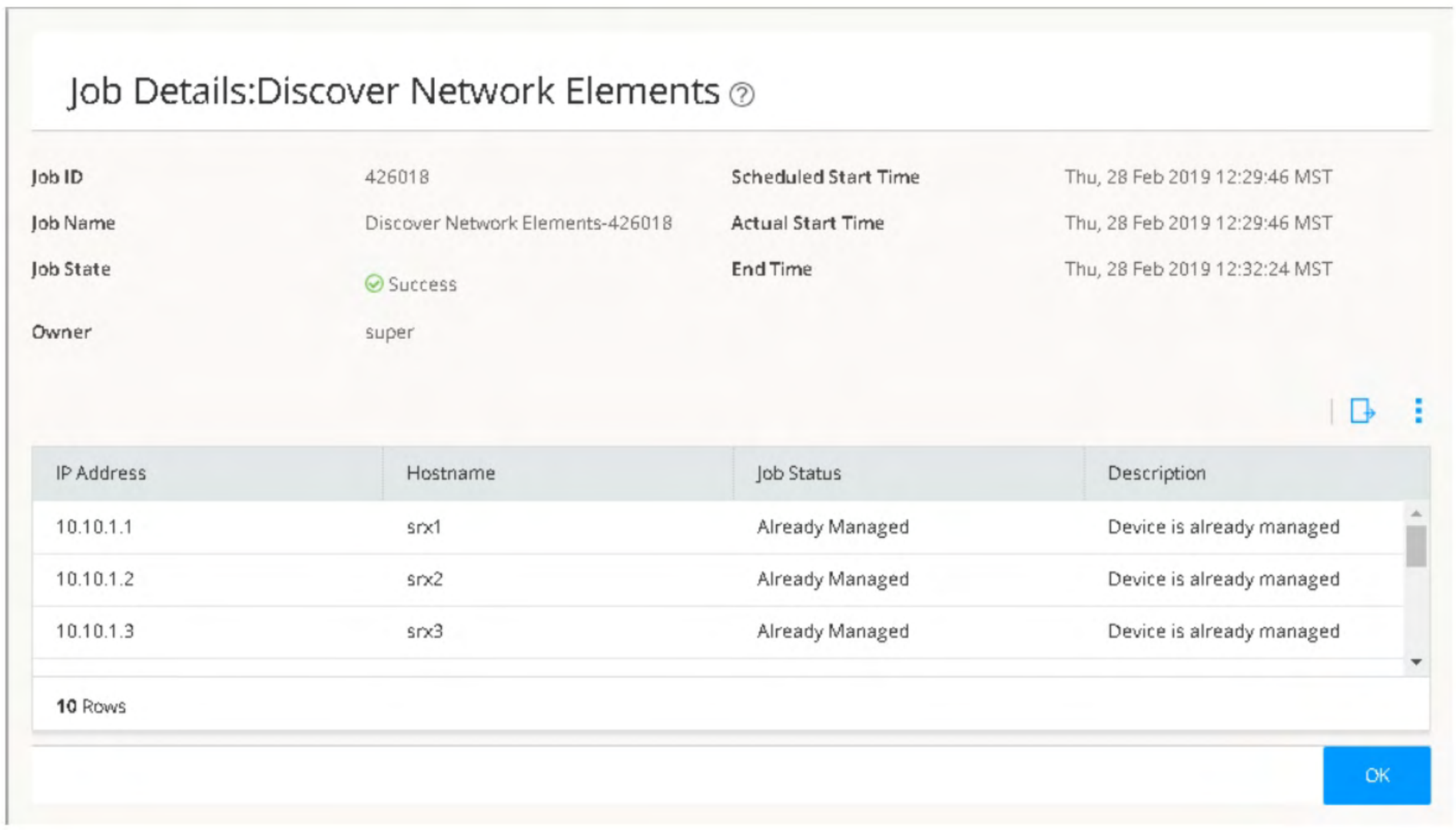
© 2020 Juniper Networks, Inc. All rights reserved.



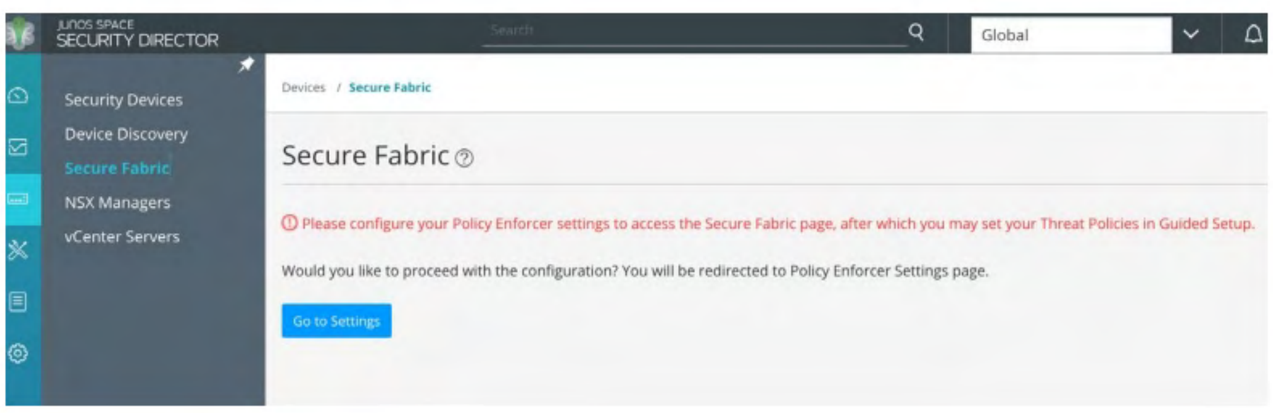
© 2020 Juniper Networks, Inc. All rights reserved.



© 2020 Juniper Networks, Inc. All rights reserved.



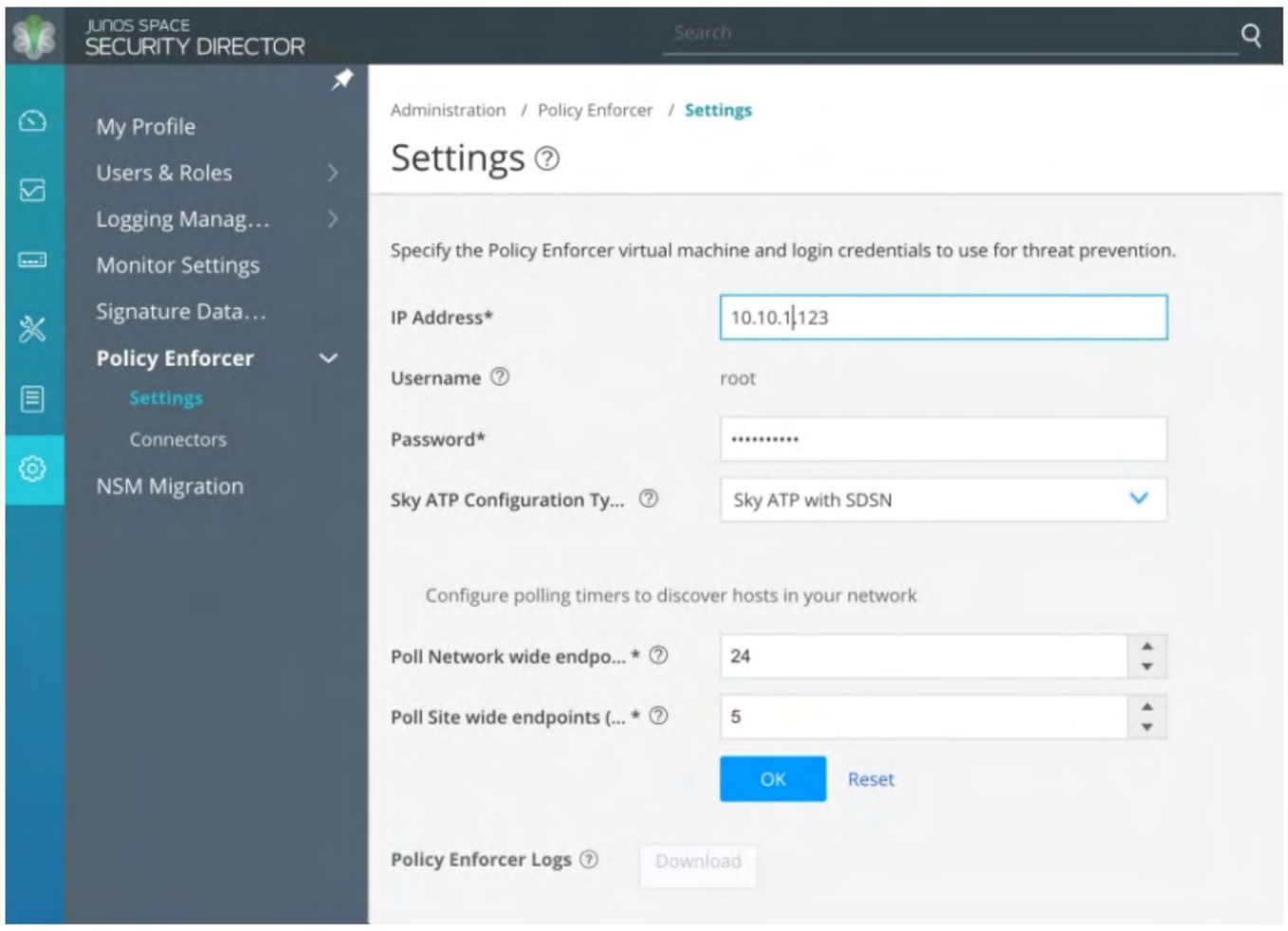
i) Navigate to Devices / Secure Fabric. Security Director gives a notification that we first need to configure Policy Enforcer to access the Secure Fabric Page.



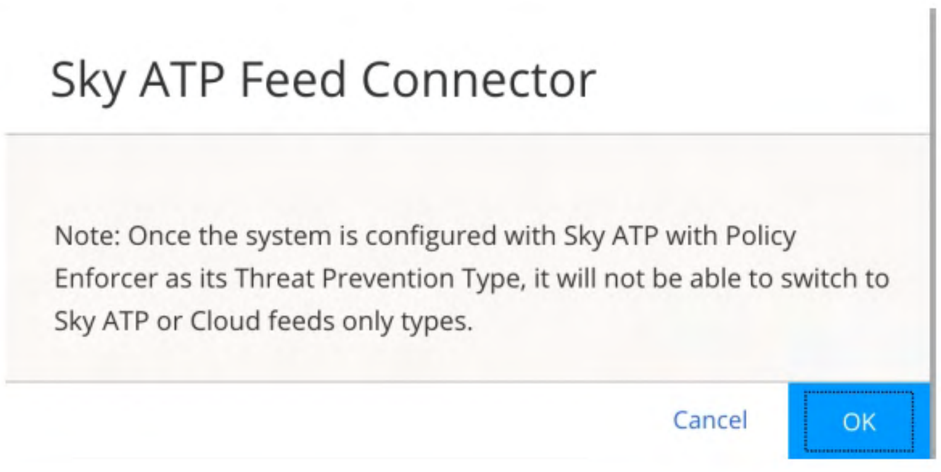
© 2020 Juniper Networks, Inc. All rights reserved.

j) Navigate to Administration / Policy Enforcer / Settings. Enter the IP address, username and password of Policy Enforcer as mentioned in your lab access instructions.

Make sure to select “Sky ATP with SDSN” as the Sky ATP configuration type and click the “OK” button.

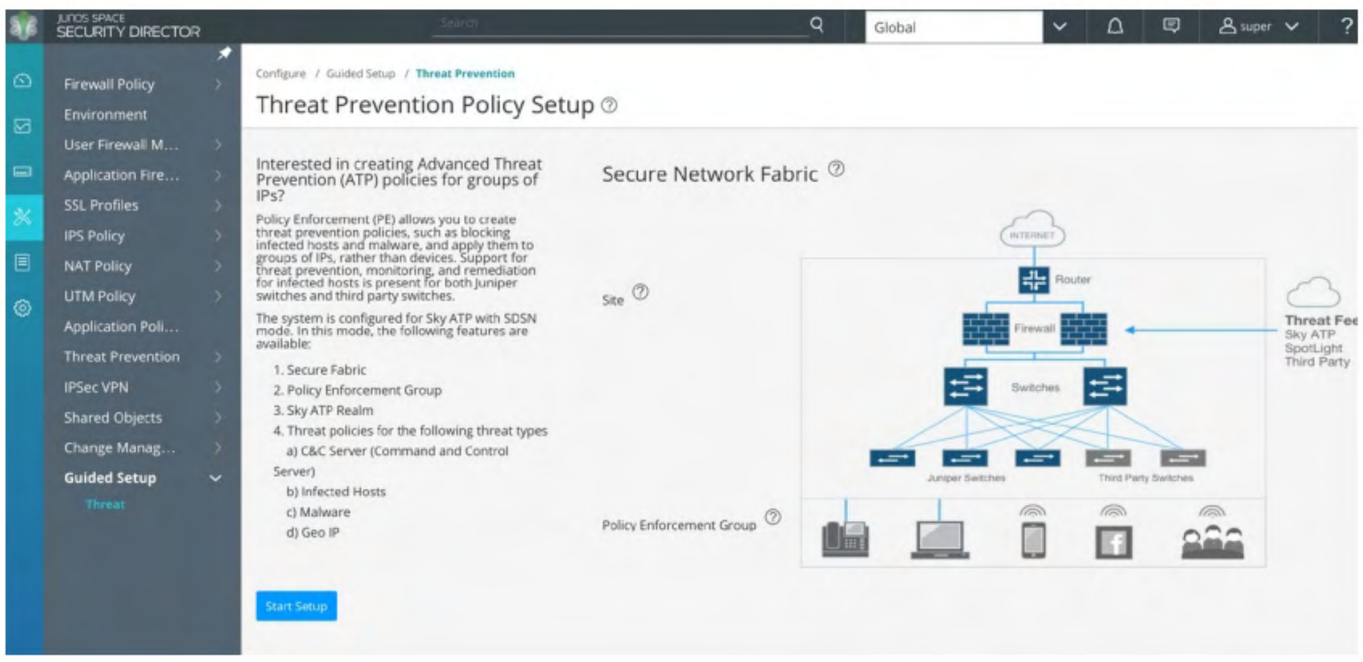


k) You should receive the following notification. Click the “ok” button to proceed.

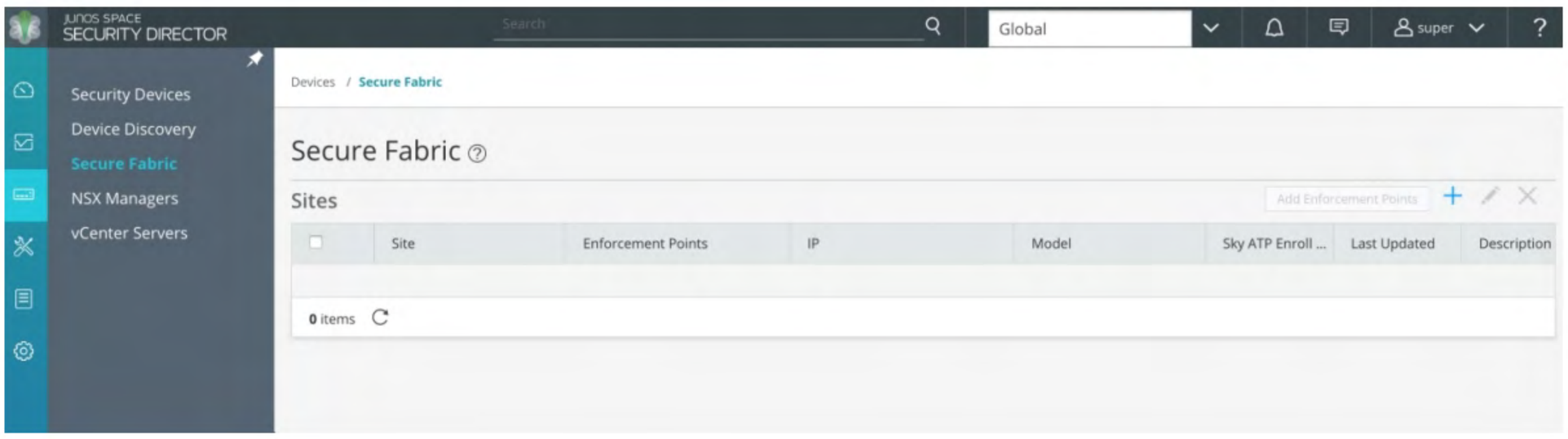


© 2020 Juniper Networks, Inc. All rights reserved.

l) Once Policy Enforcer is registered you are redirected to the “Threat Prevention Policy Setup” guided setup. At this stage we are not creating a Threat Prevention Policy yet as the task requirement is to enroll Policy Enforcer and the required security devices.

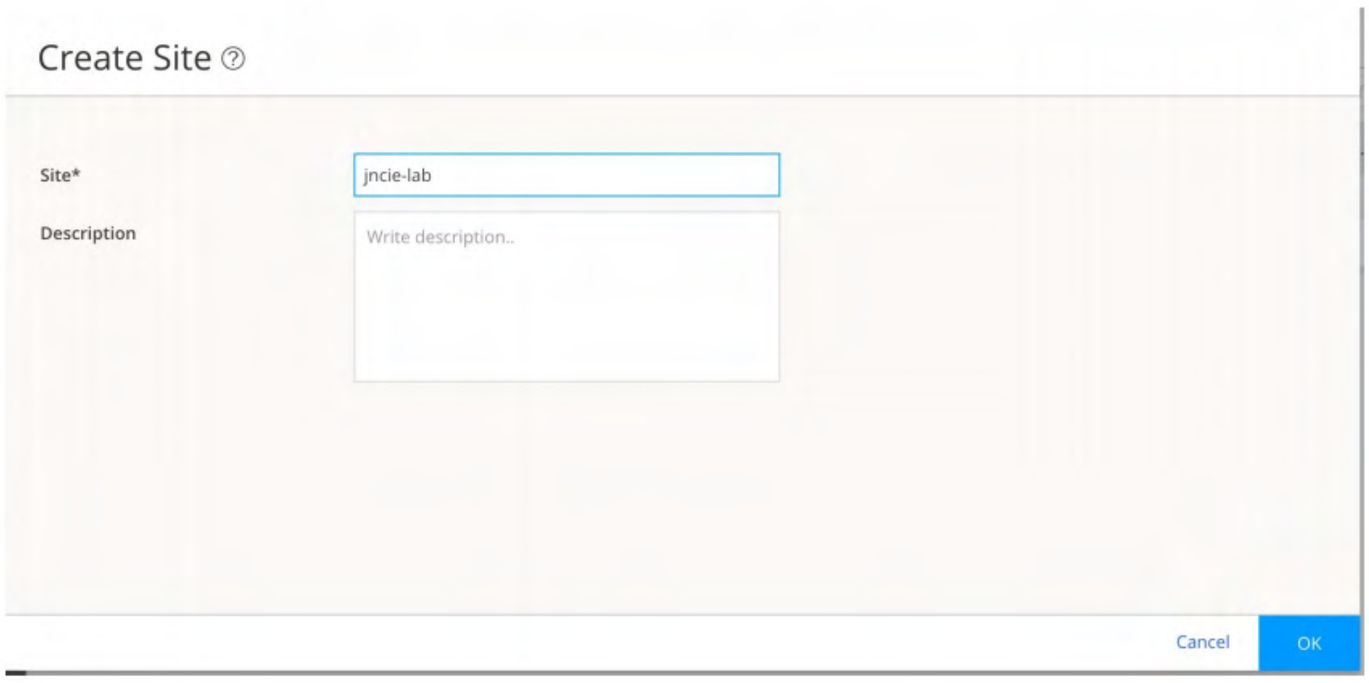


m) Navigate in the left vertical menu to “Devices” and select “Secure Fabric”. You need to define a “Site” and add “Enforcement points” to the site.

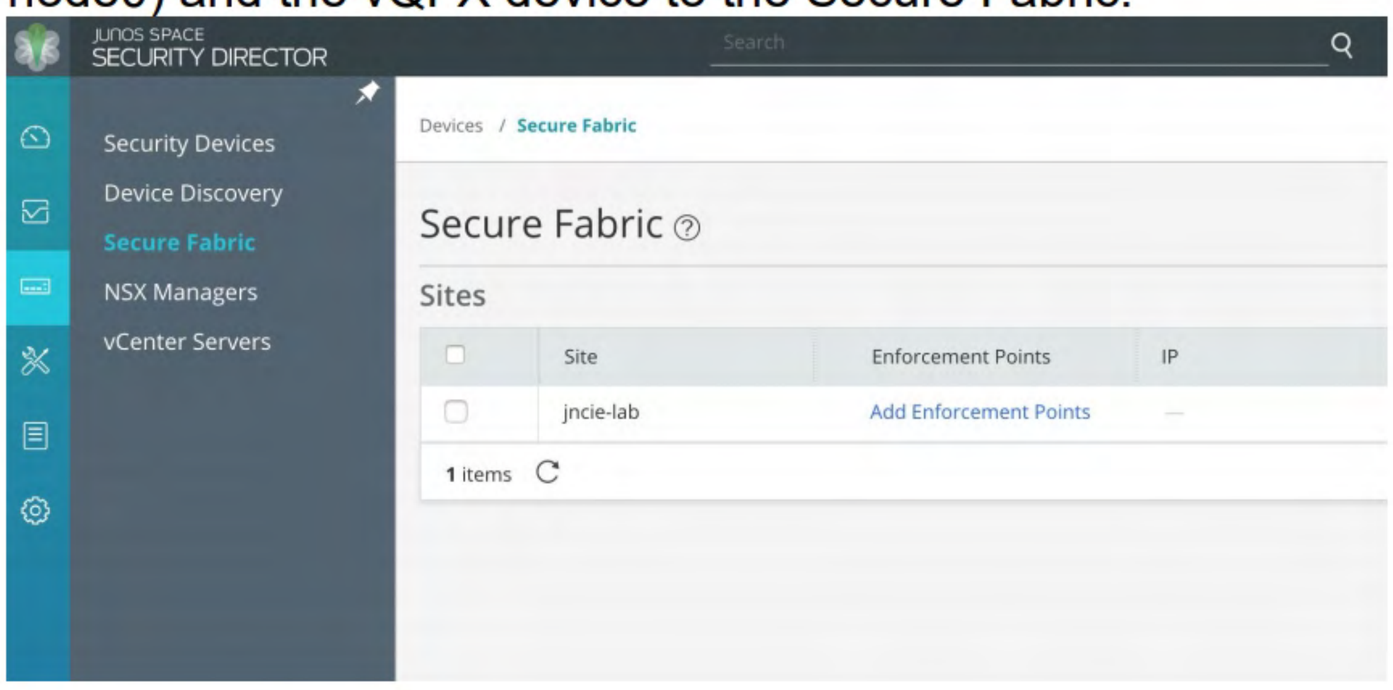


© 2020 Juniper Networks, Inc. All rights reserved.

n) Create a site and specific a Site name. In this case we call the Site “jncie-lab”. Click on the “Ok” button to proceed.

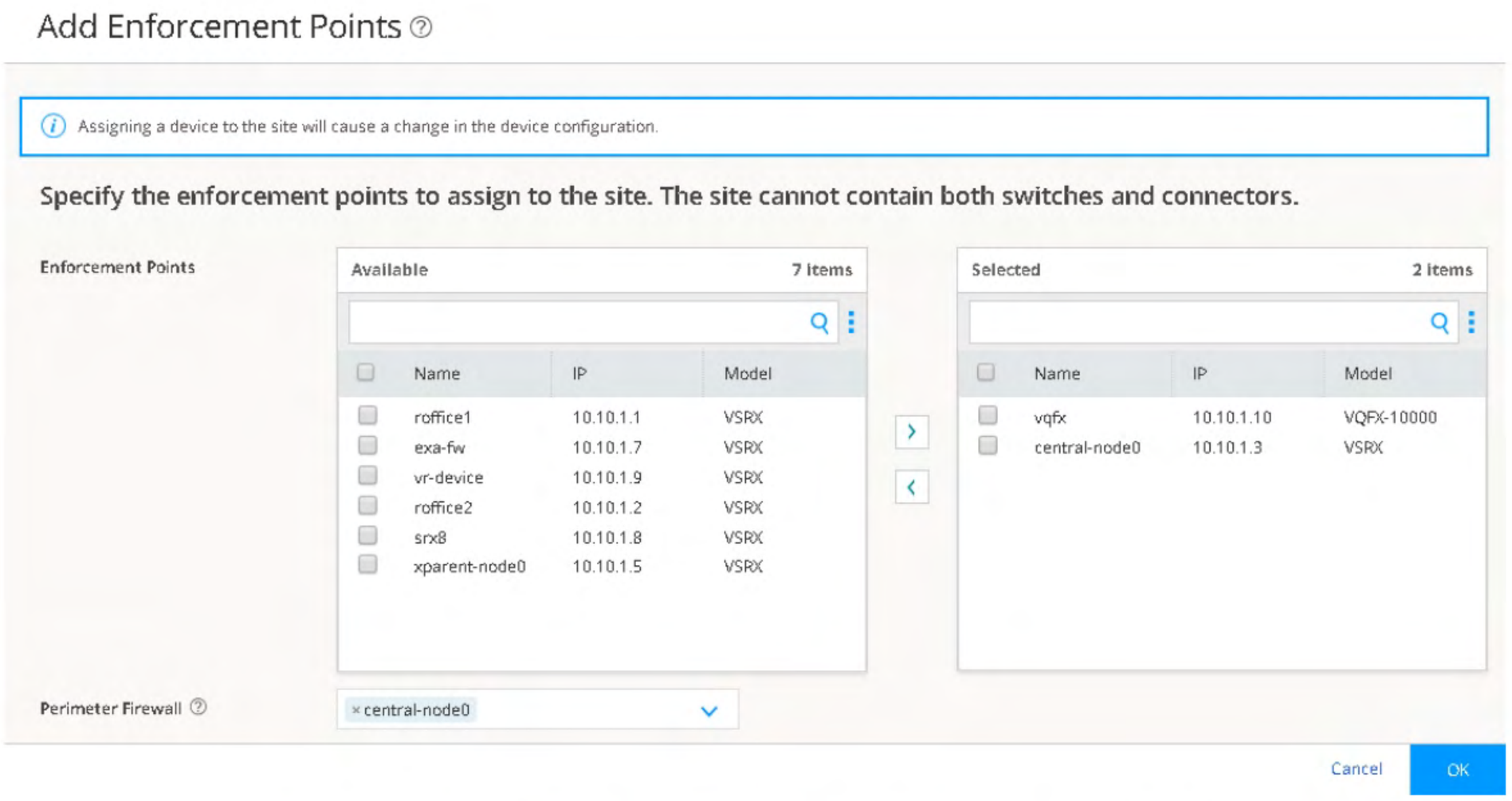


o) Now select “Add Enforcement Points” to add the central cluster (central-node0) and the vQFX device to the Secure Fabric.

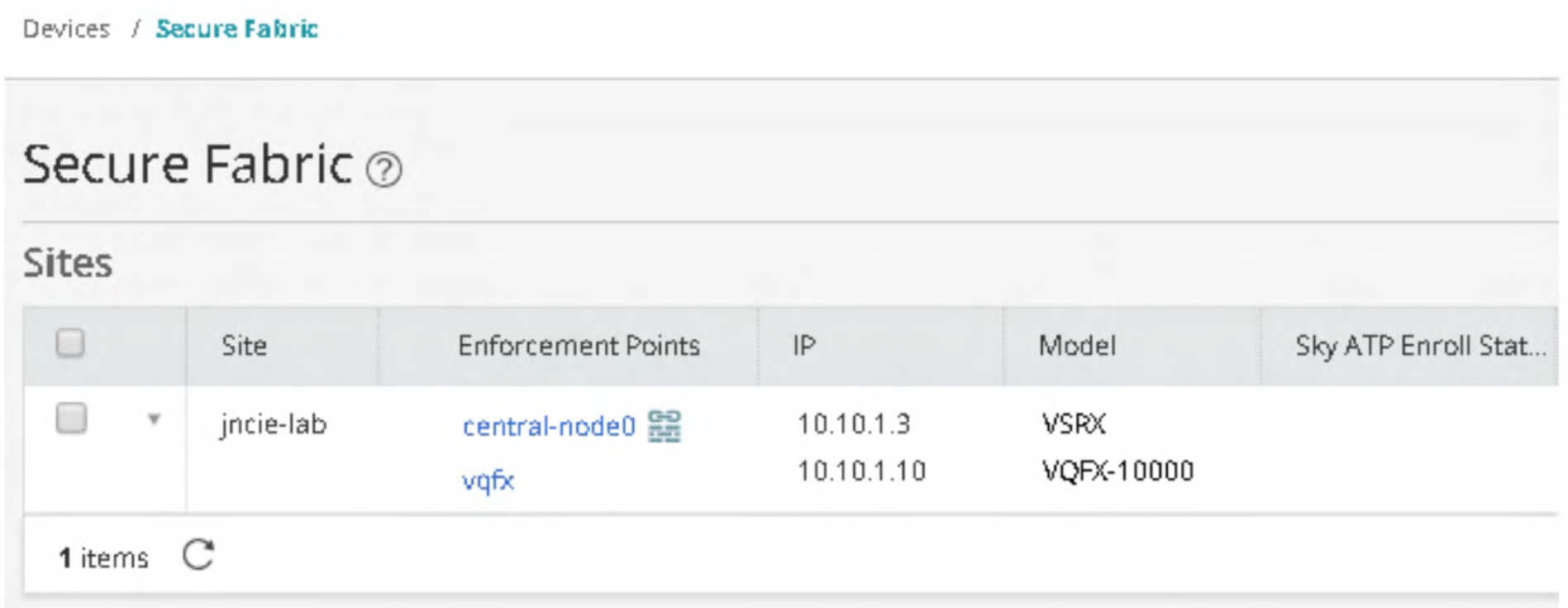


© 2020 Juniper Networks, Inc. All rights reserved.

p) Select the xparent-node0 device and the vQFX device as an enforcement points and click the “ok” button.



q) Now the central cluster and the vQFX device should be added as an enforcement point to the Secure Fabric for Site “jncie-lab”.



© 2020 Juniper Networks, Inc. All rights reserved.

2) Setup for SkyATP with SDSN in Security Director, ensure that HTTP and SMTP traffic is analyzed at the central cluster (srx3/srx4) for threat levels greater than 6 for the 172.16.50.100 host. Ensure that connections are silently dropped at access switch vQFX if the 172.16.50.100 host becomes infected with malware. Ensure that only blocked traffic is logged. (Note that this includes C&C protection).

   a) Return to the open CLI session with the central-node0 device and add a term to the loopback filter (RE-PROTECT-v4) to allow DNS replies from the 8.8.8.8 DNS server. Note that hostname resolution is necessary for Sky ATP realm enrollment to work. You must also adjust the loopback filter to all for communication with the Sky ATP servers (TCP ports 443, 80, 8080)

```
{primary:node0}
lab@central-node0> configure
warning: Clustering enabled; using private edit
warning: uncommitted changes will be discarded on exit
Entering configuration mode

{primary:node0}[edit]
lab@central-node0# edit firewall family inet filter RE-PROTECT-v4

{primary:node0}[edit firewall family inet filter RE-PROTECT-v4]
lab@central-node0# set term DNS from source-address 8.8.8.8

{primary:node0}[edit firewall family inet filter RE-PROTECT-v4]
lab@central-node0# set term DNS then accept

{primary:node0}[edit firewall family inet filter RE-PROTECT-v4]
lab@central-node0# insert term DNS before term IFD

{primary:node0}[edit firewall family inet filter RE-PROTECT-v4]
lab@central-node0# set term sdsn from protocol tcp port https

{primary:node0}[edit firewall family inet filter RE-PROTECT-v4]
lab@central-node0# set term sdsn from port http

{primary:node0}[edit firewall family inet filter RE-PROTECT-v4]
lab@central-node0# set term sdsn from port 8080

{primary:node0}[edit firewall family inet filter RE-PROTECT-v4]
lab@central-node0# set term sdsn then accept

{primary:node0}[edit firewall family inet filter RE-PROTECT-v4]
lab@central-node0# insert term sdsn before term IFD

{primary:node0}[edit firewall family inet filter RE-PROTECT-v4]
lab@central-node0# show
term DNS {
    from {
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
        source-address {
            8.8.8.8/32;
        }
        port domain;
    }
    then accept;
}
term sdsn {
    from {
        protocol tcp;
        port [ https http 8080 ];
    }
    then accept;
}
term IFD {
    from {
        interface st0;
    }
    then accept;
}
term PORT-UDP {
    from {
        source-prefix-list {
            mgmt;
        }
        protocol udp;
        port [ domain ntp ];
    }
    then accept;
}
term LOG-UDP {
    from {
        protocol udp;
        port [ domain ntp ];
    }
    then {
        count LOG-UDP;
        discard;
    }
}
term PORT-TCP {
    from {
        source-prefix-list {
            mgmt;
        }
        protocol tcp;
        destination-port [ https ssh ];
    }
    then accept;
}
term LOG-TCP {
```

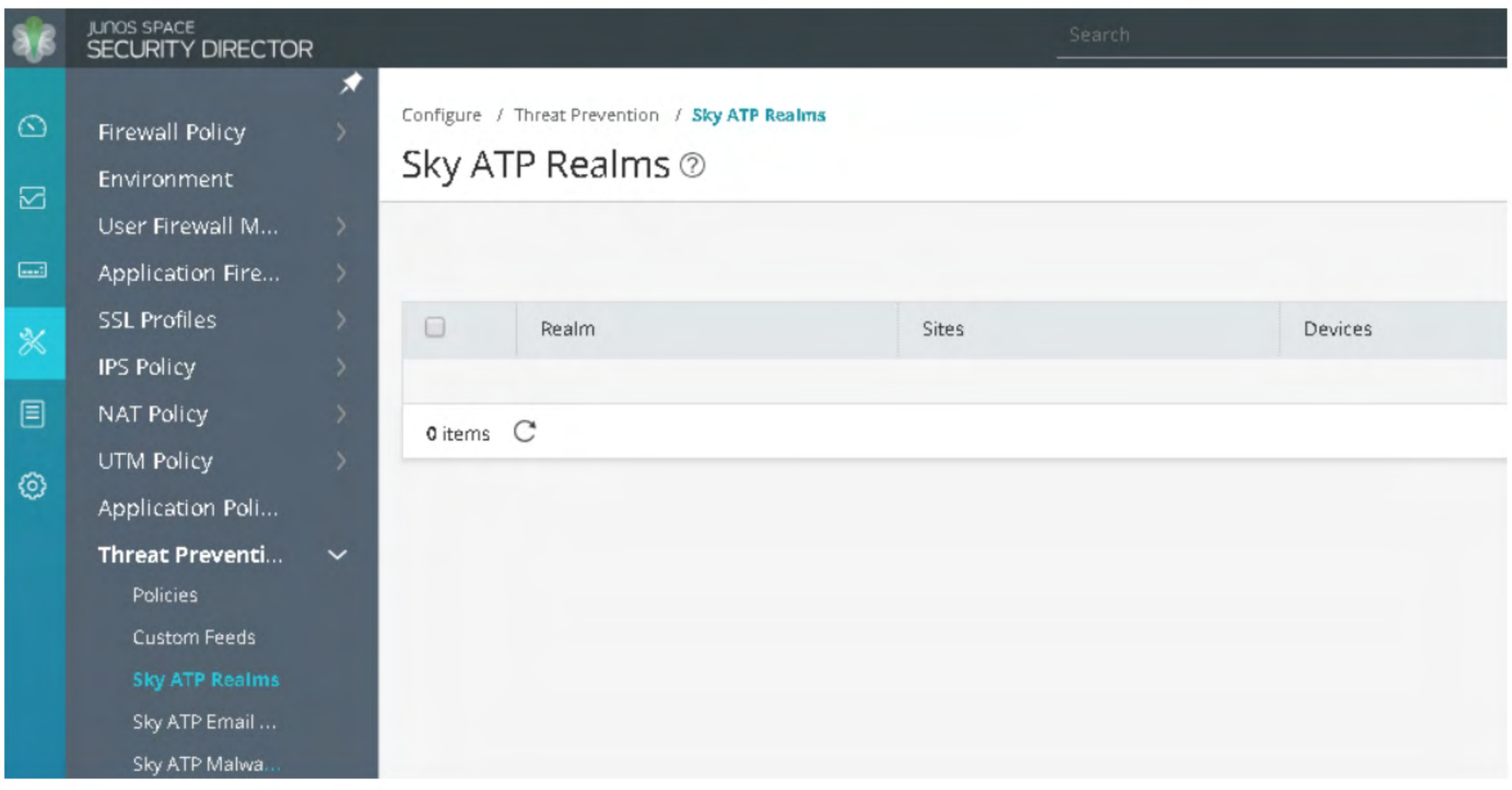

© 2020 Juniper Networks, Inc. All rights reserved.

```
        from {
            protocol tcp;
            destination-port [ https ssh ];
        }
        then {
            count LOG-TCP;
            discard;
        }
    }
    term ICMP {
        from {
            protocol icmp;
        }
        then {
            policer ICMP-POLICER;
            accept;
        }
    }
    term SNMP {
        from {
            source-prefix-list {
                mgmt;
            }
            port [ snmp snmptrap ];
        }
        then {
            count SNMP;
            accept;
        }
    }
    term BGP {
        from {
            prefix-list {
                bgp;
            }
            protocol tcp;
            port bgp;
        }
        then {
            count BGP;
            accept;
        }
    }
    term OSPF {
        from {
            protocol ospf;
        }
        then {
            count OSPF;
            accept;
        }
```


© 2020 Juniper Networks, Inc. All rights reserved.

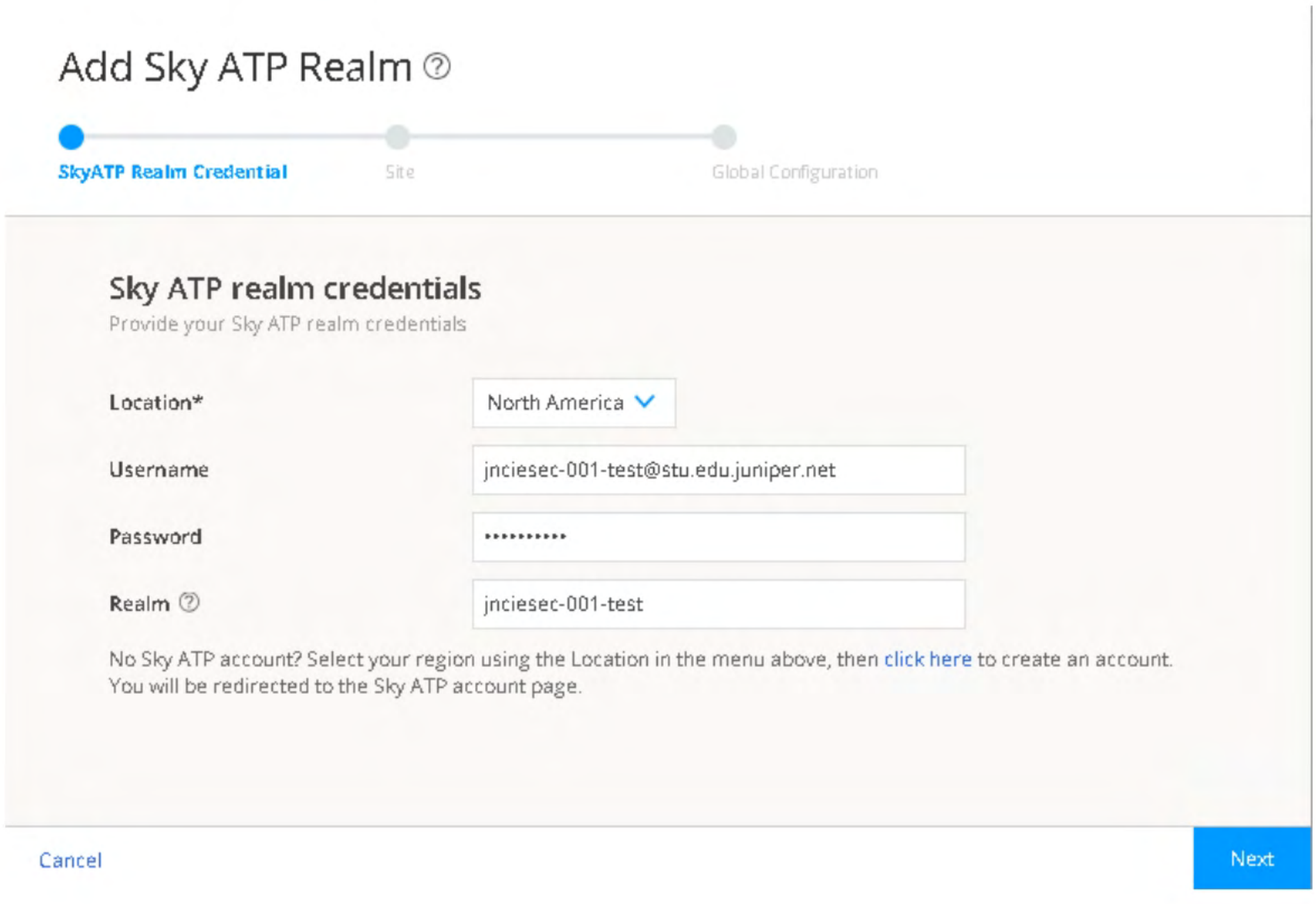
```
}
term IKE {
    from {
        port 500;
    }
    then {
        count IKE;
        accept;
    }
}

{primary:node0}[edit firewall family inet filter RE-PROTECT-v4]
lab@central-node0# top

{primary:node0}[edit]
lab@central-node0# commit and-quit
node0:
configuration check succeeds
node1:
commit complete
node0:
commit complete
Exiting configuration mode

{primary:node0}
lab@central-node0>
```

b) Navigate to the Configure / Threat Prevention / Sky ATP Realms workspace.



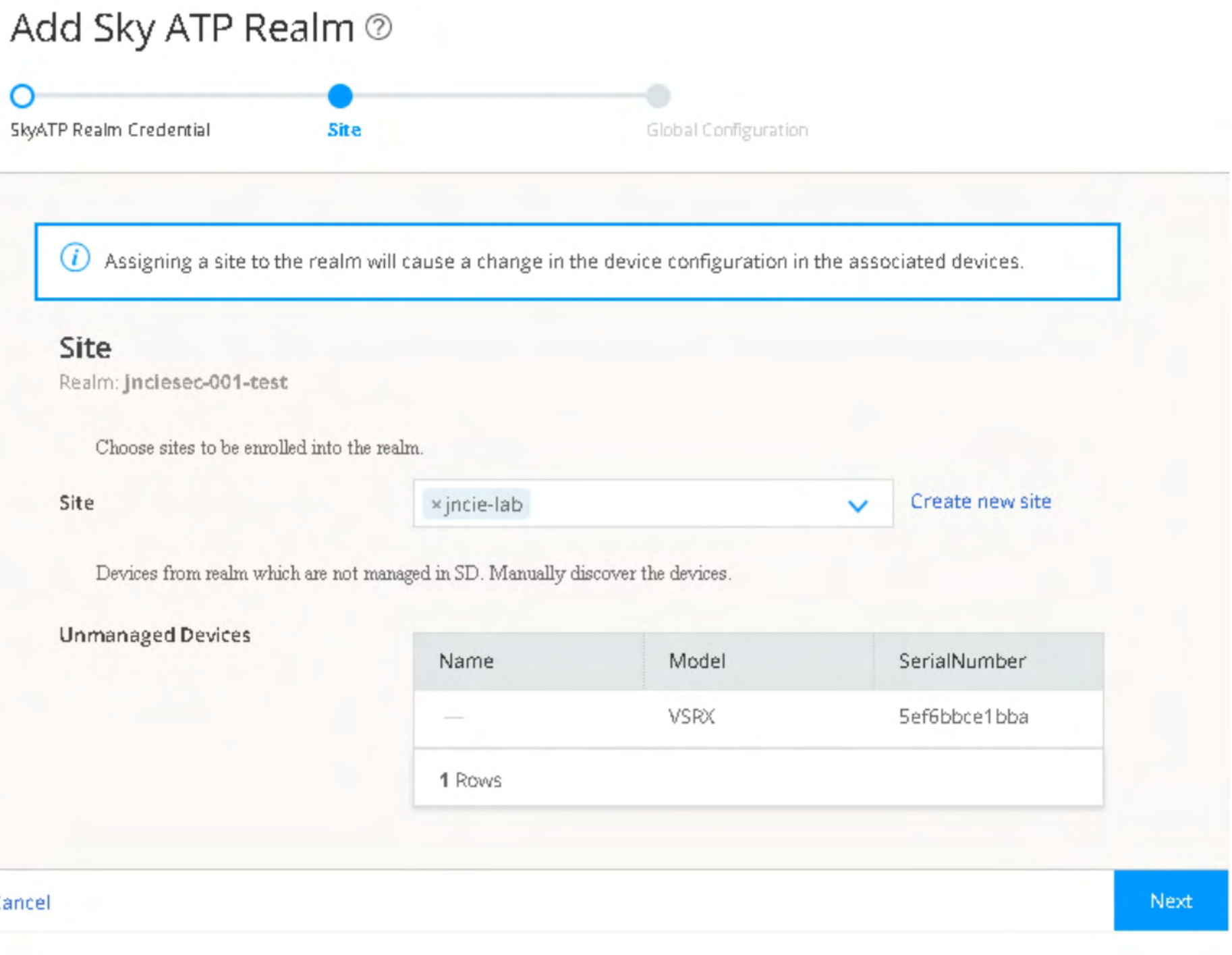
© 2020 Juniper Networks, Inc. All rights reserved.

c) Click the create button and enter your Sky ATP realm credentials. Click Next to continue.



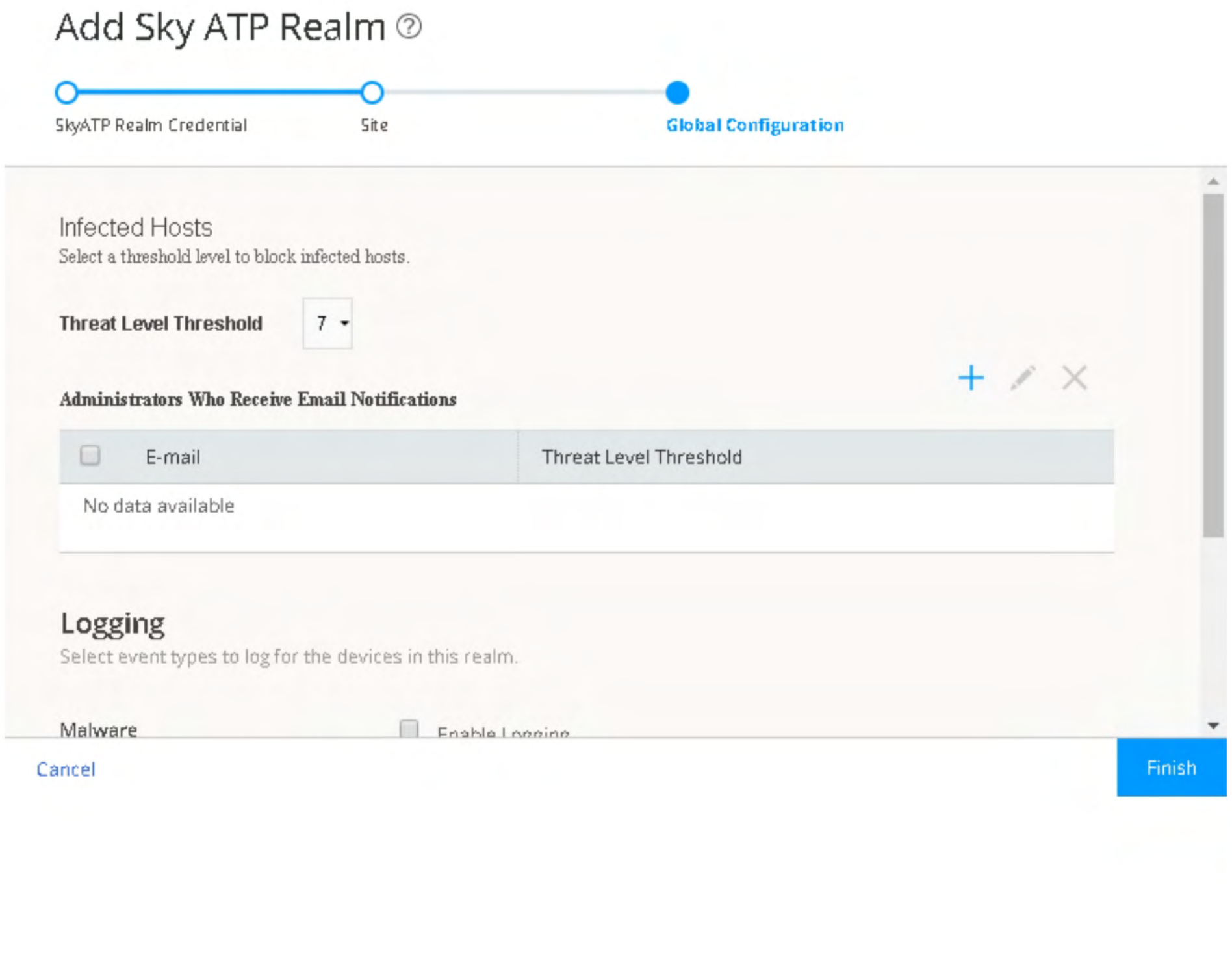
© 2020 Juniper Networks, Inc. All rights reserved.

d) Select your SDSN site and click next.



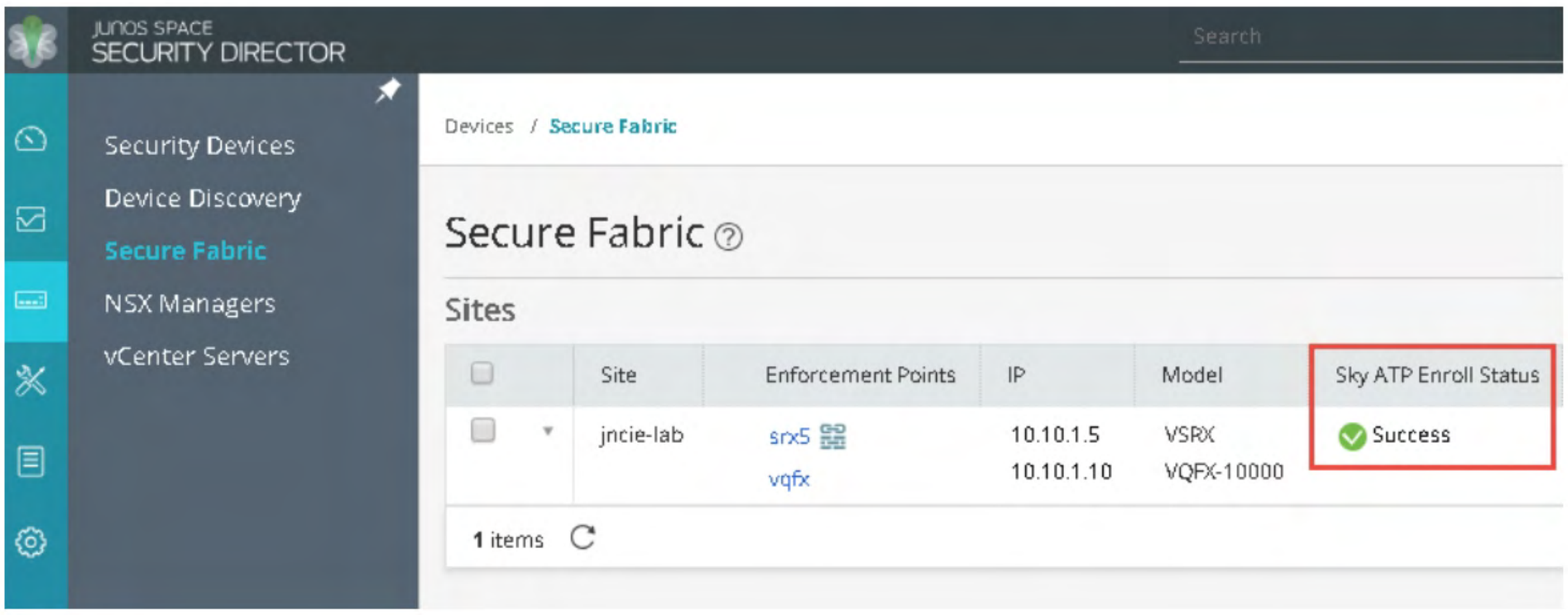
© 2020 Juniper Networks, Inc. All rights reserved.

e) Leave everything at the defaults for the Global Configuration page and click Finish.



© 2020 Juniper Networks, Inc. All rights reserved.

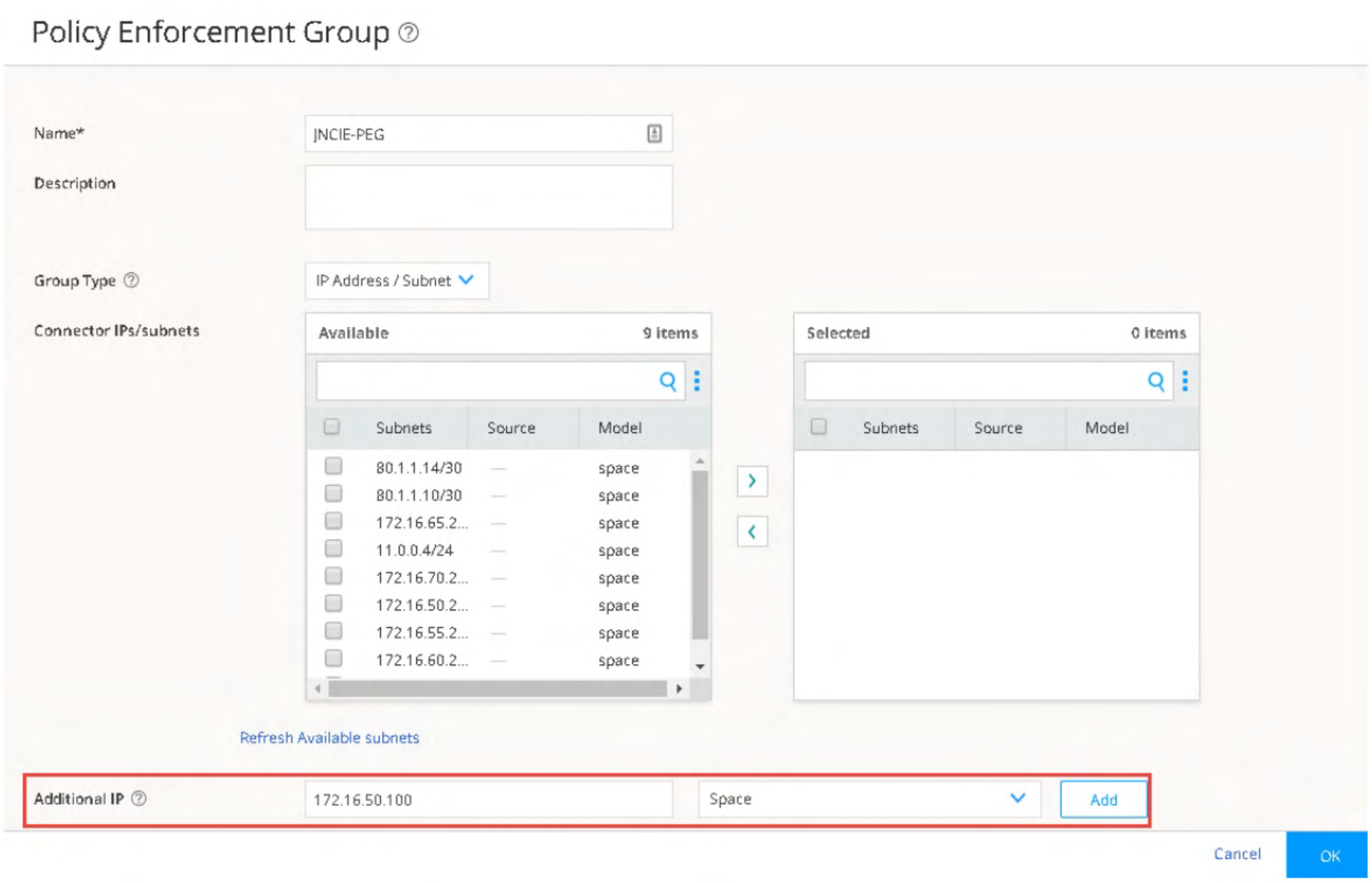
f) Navigate to the Devices / Secure Fabric workspace. Ensure that the central-node0 device Sky ATP enrolment status is successful. Note if the status shows Pending then you should wait 5 minutes and refresh the page.



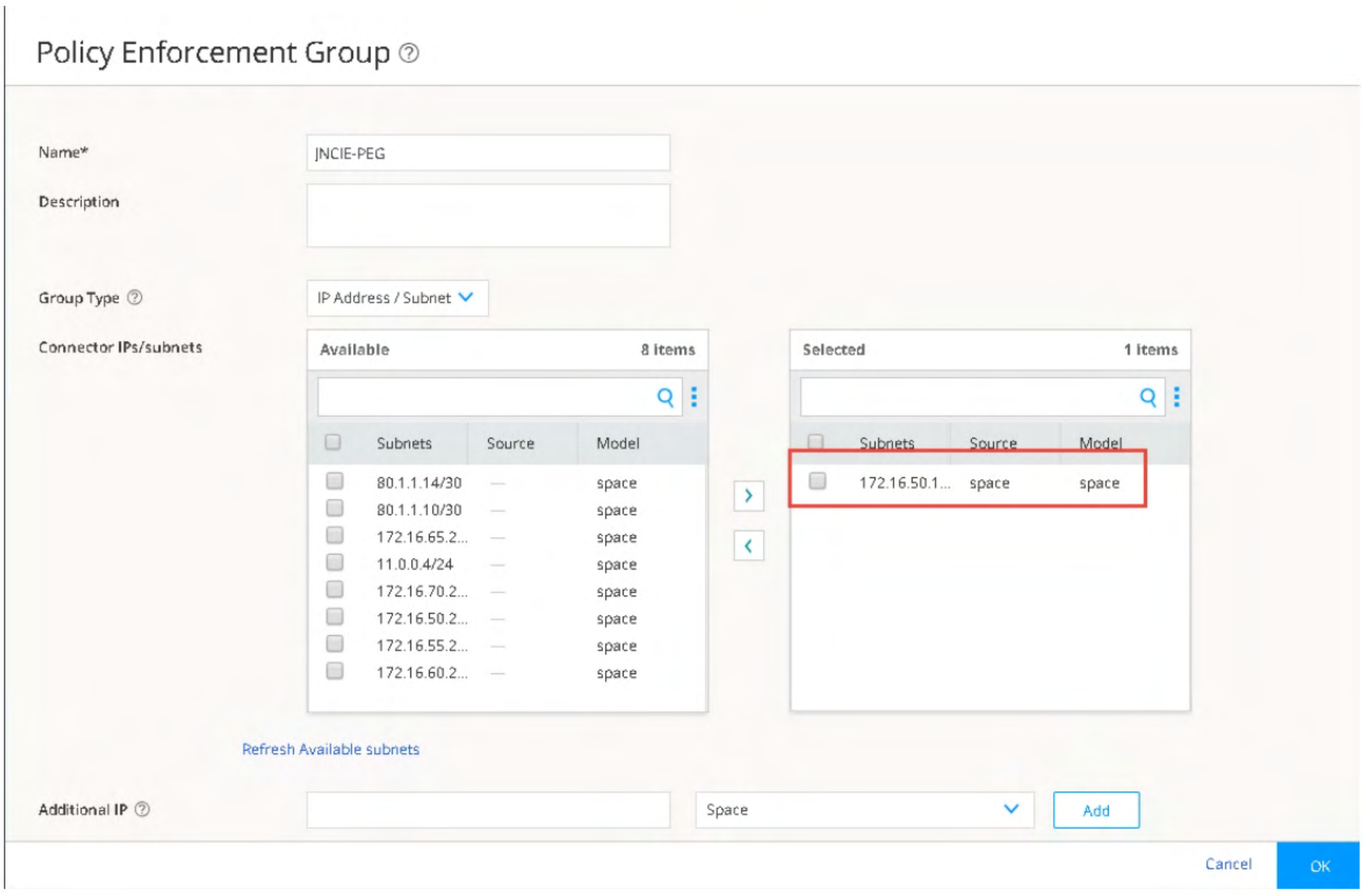
© 2020 Juniper Networks, Inc. All rights reserved.

g) Create a policy enforcement group for the 172.16.50.100 host. Ensure that connections are silently dropped if the threat is identified. Ensure that only blocked traffic is logged.

i. Navigate to the Configure / Shared Objects / Policy Enforcement Groups workspace. Create a new PEG and add the new 172.16.50.100 IP address

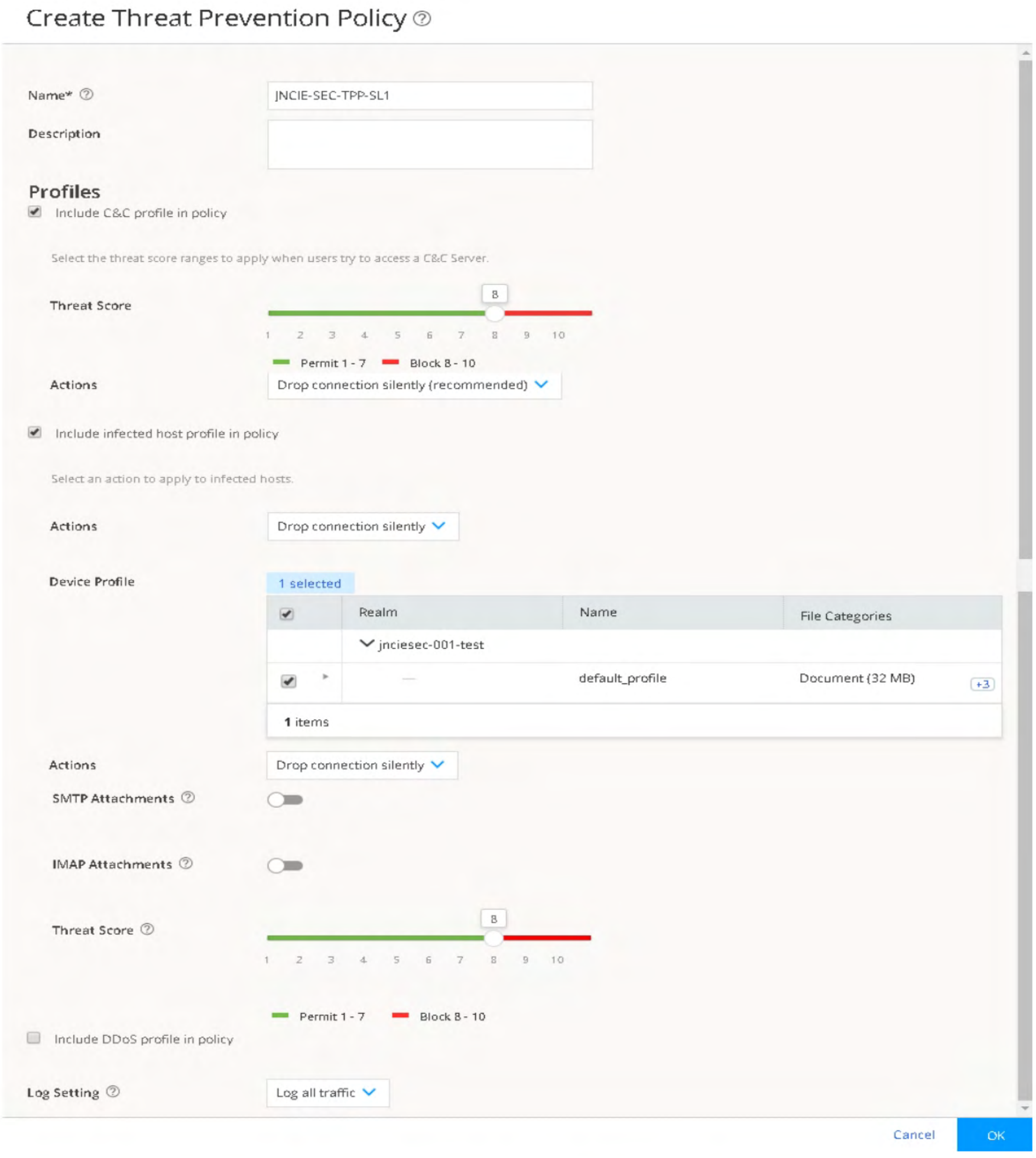


© 2020 Juniper Networks, Inc. All rights reserved.



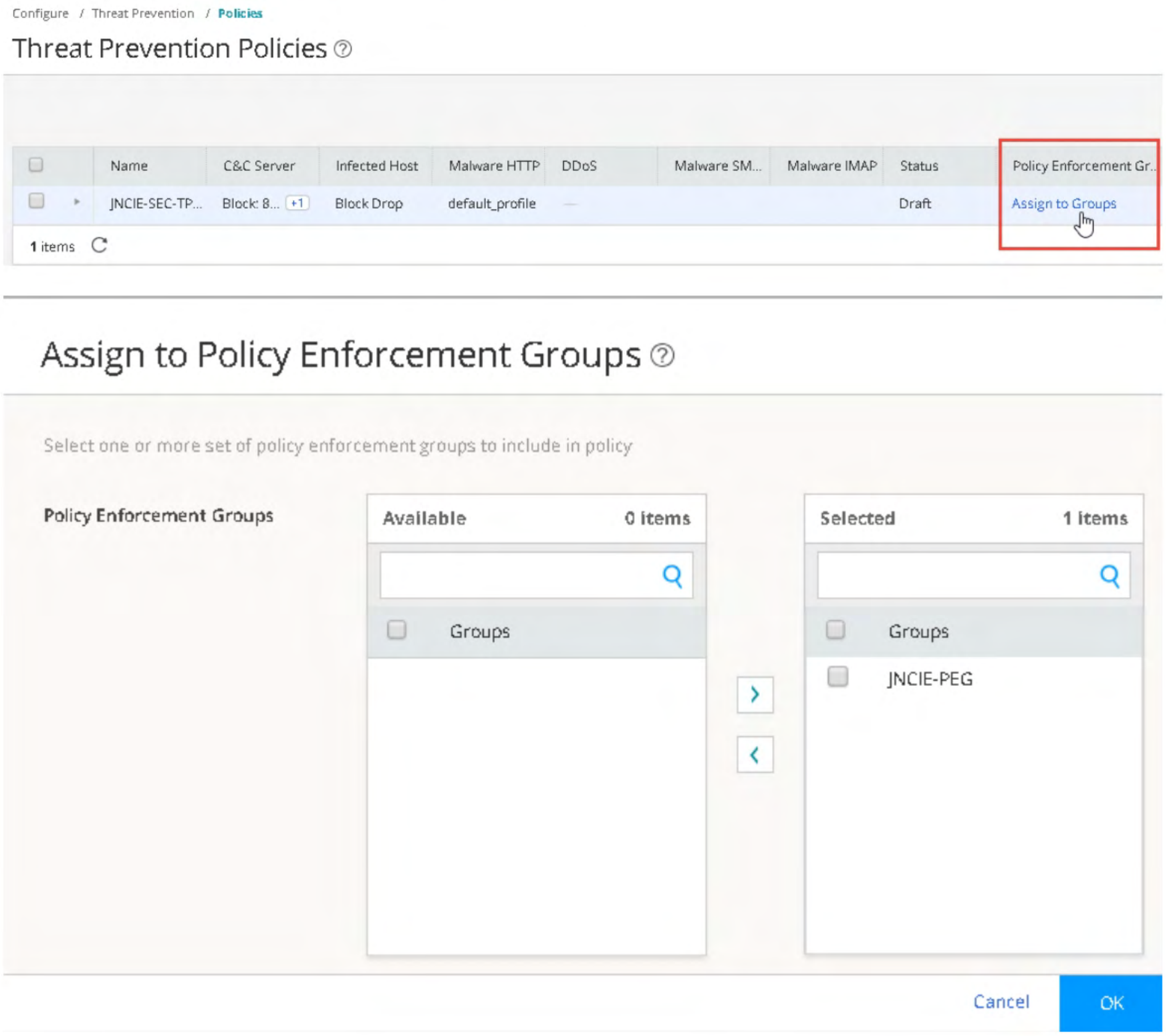
© 2020 Juniper Networks, Inc. All rights reserved.

h) Navigate to the Configure / Threat Prevention / Policies workspace to setup a threat prevention policy. Make sure that you include the infected host profile and the malware profile in the policy. Scan HTTP files downloads using the default profile associated with your realm. Set the Threat score to block threats rated at a value that is greater than 8. (Note that this includes C&C protection).



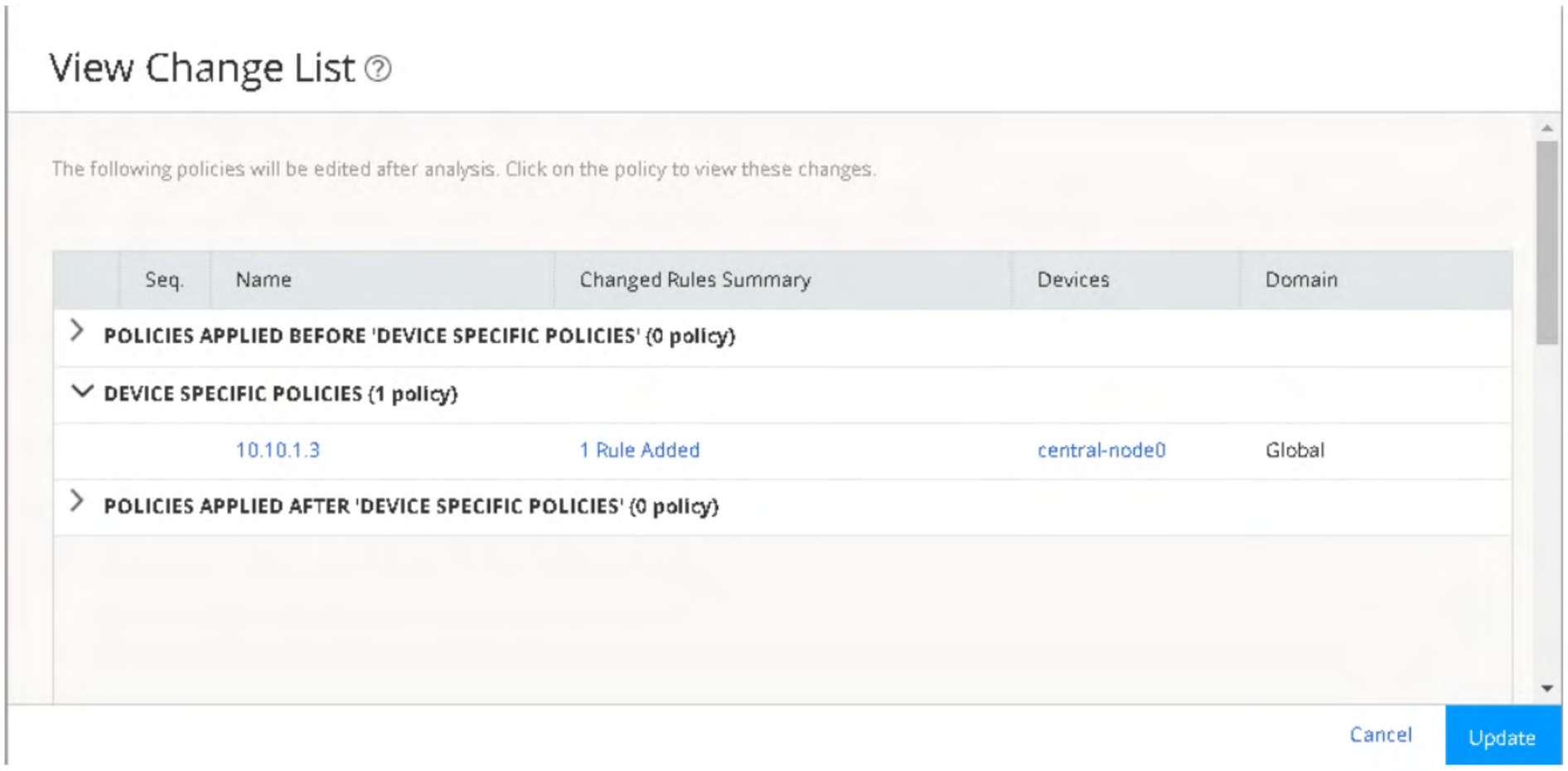
© 2020 Juniper Networks, Inc. All rights reserved.

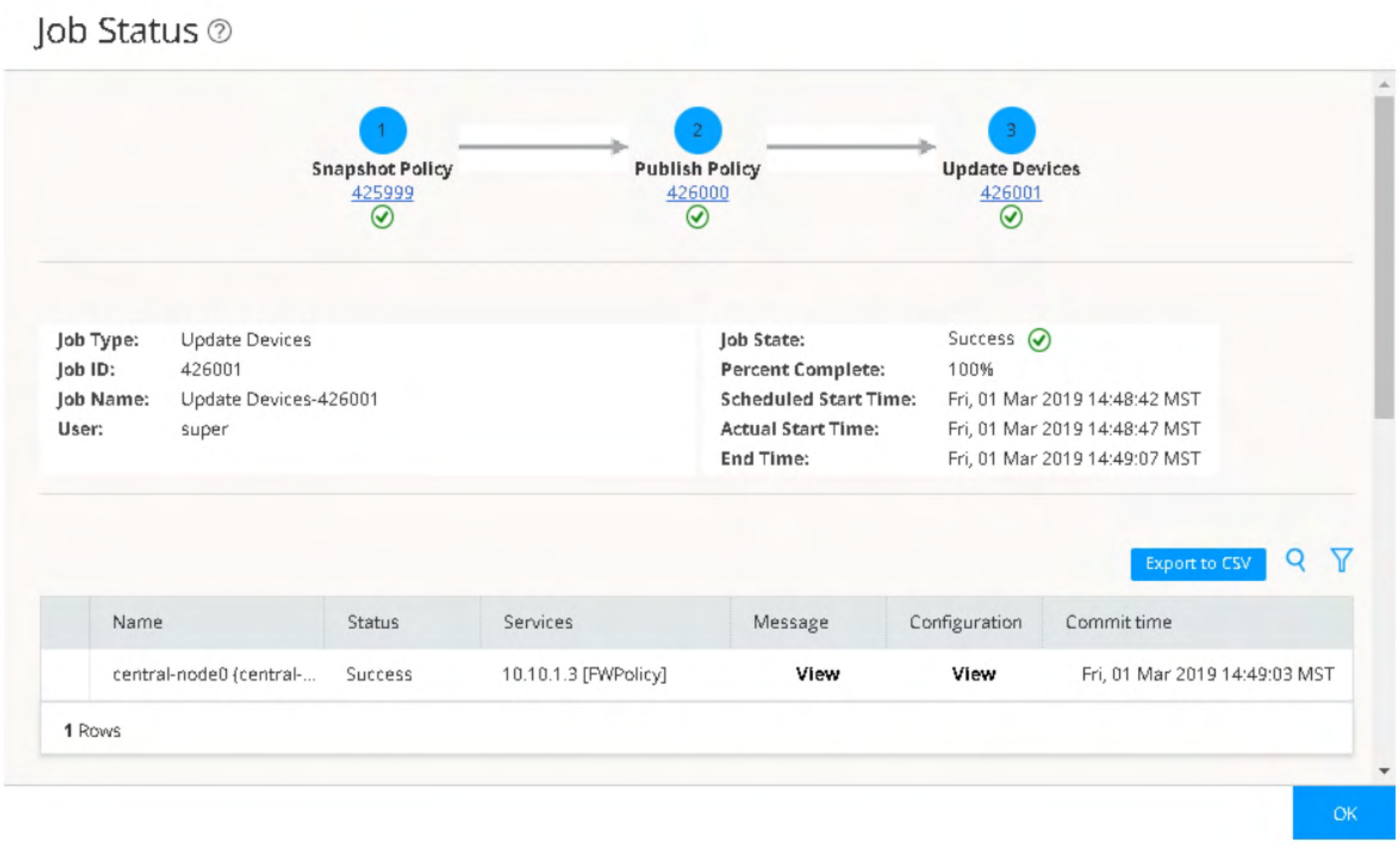
i) Assign your PEG to the policy.



© 2020 Juniper Networks, Inc. All rights reserved.

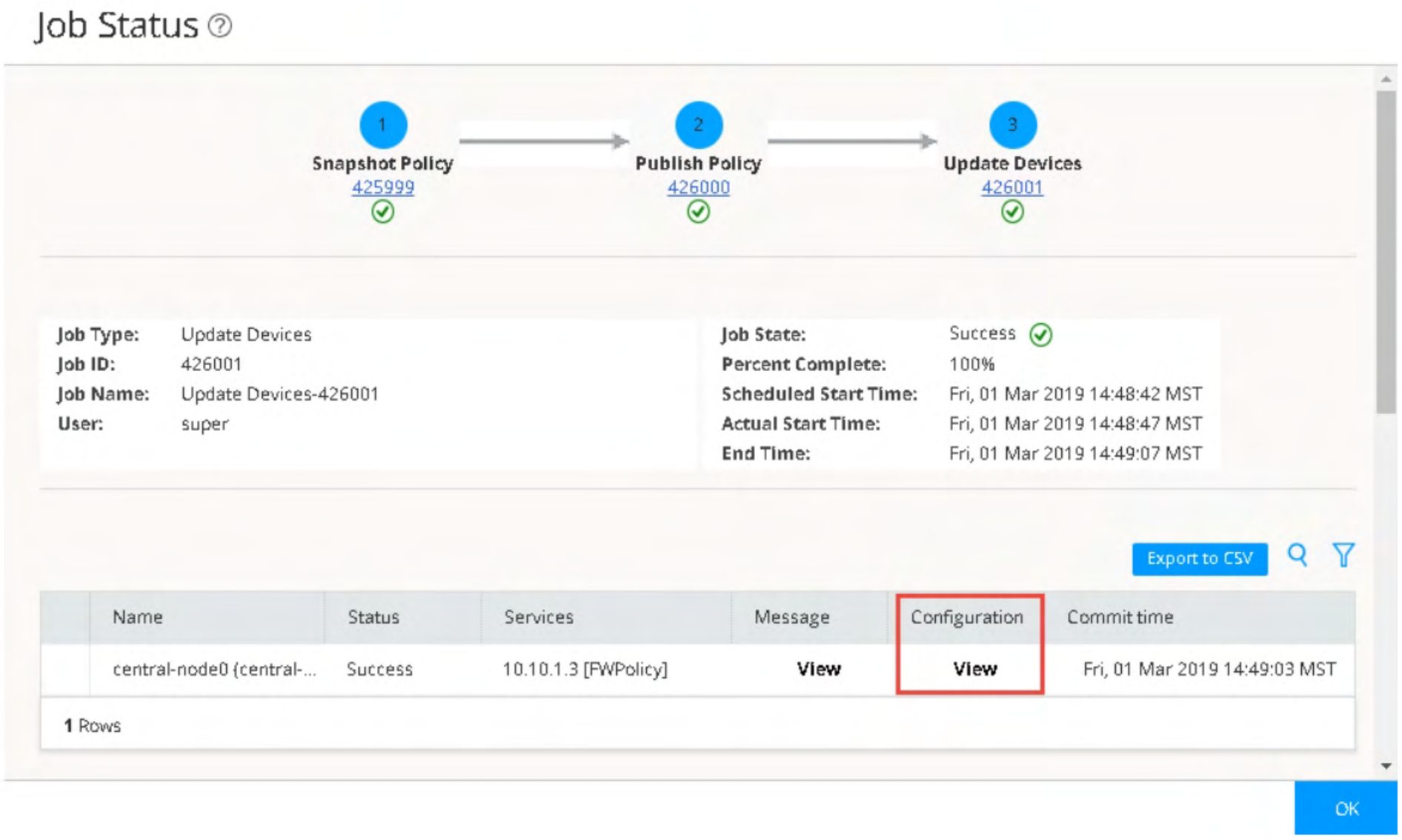
j) Click Update on the View Change List page.





© 2020 Juniper Networks, Inc. All rights reserved.

k) Click the View link for the Configuration section.



© 2020 Juniper Networks, Inc. All rights reserved.

View configuration for central-node0 (central-node0) (Cluster)

CLI XML

Added Deleted Modified Comments

```
##Global address book configurations##
delete security address-book global address BUILDING-DMZ-B1
delete security address-book global address BUILDING-DMZ-B2
delete security address-book global address BUILDING-TRUST-B1
delete security address-book global address BUILDING-TRUST-B2
delete security address-book global address CENTRAL-INTERNAL
delete security address-book global address CENTRAL-TESTBED6
delete security address-book global address CENTRAL-TESTBED7
delete security address-book global address CENTRAL-TRUST
delete security address-book global address CENTRAL-WAREHOUSE
delete security address-book global address EXA-PRIVATE
delete security address-book global address EXA-SRV-DB
delete security address-book global address EXA-SRV-SSH
delete security address-book global address EXA-SRV-WEB
delete security address-book global address EXA-TRUST
delete security address-book global address EXA-TRUST-OVERLAP
delete security address-book global address HOFFICE-TRUST
set security address-book global address JNCIE-PEG_172.16.50.100 172.16.50.100/32
delete security address-book global address RO1-HOST-PRIVATE
delete security address-book global address RO1-TRUST
delete security address-book global address RO1-TRUST-OVERLAP
delete security address-book global address RO2-SRV-DB
delete security address-book global address RO2-SRV-WEB
delete security address-book global address RO2-TRUST
delete security address-book global address SRV-MAIL
delete security address-book global address WAREHOUSE-HONEYPOT
delete security address-book global address WAREHOUSE-SRV-205
delete security address-book global address WAREHOUSE-SRV-206
delete security address-book global address WEBSENSE
delete security address-book global address-set CENTRAL-TESTBED
delete security address-book global address-set TRUST-NETWORKS
##Security Firewall Policy : UNTRUST - WAREHOUSE##
delete security policies from-zone UNTRUST to-zone WAREHOUSE
##Security Firewall Policy : TRUST - UNTRUST##
delete security policies from-zone TRUST to-zone UNTRUST
##Security Firewall Policy : INTERNAL - WAREHOUSE##
delete security policies from-zone INTERNAL to-zone WAREHOUSE
##Security Firewall Policy : TESTBED - WAREHOUSE##
delete security policies from-zone TESTBED to-zone WAREHOUSE
##Security Firewall Policy : WAREHOUSE - UNTRUST##
delete security policies from-zone WAREHOUSE to-zone UNTRUST
##Security Firewall Policy : INTERNAL - UNTRUST##
delete security policies from-zone INTERNAL to-zone UNTRUST
##Security Firewall Policy : UNTRUST - UNTRUST##
delete security policies from-zone UNTRUST to-zone UNTRUST
##Security Firewall Policy : TESTBED - UNTRUST##
delete security policies from-zone TESTBED to-zone UNTRUST
##Security Firewall Policy : WAREHOUSE - WAREHOUSE##
delete security policies from-zone WAREHOUSE to-zone WAREHOUSE
##Security Firewall Policy : UNTRUST - WAREHOUSE##
delete security policies from-zone UNTRUST to-zone WAREHOUSE
##Security Firewall Policy : TRUST - UNTRUST##
delete security policies from-zone TRUST to-zone UNTRUST
##Security Firewall Policy : INTERNAL - WAREHOUSE##
delete security policies from-zone INTERNAL to-zone WAREHOUSE
##Security Firewall Policy : TESTBED - WAREHOUSE##
delete security policies from-zone TESTBED to-zone WAREHOUSE
##Security Firewall Policy : WAREHOUSE - UNTRUST##
delete security policies from-zone WAREHOUSE to-zone UNTRUST
##Security Firewall Policy : INTERNAL - UNTRUST##
delete security policies from-zone INTERNAL to-zone UNTRUST
##Security Firewall Policy : UNTRUST - UNTRUST##
delete security policies from-zone UNTRUST to-zone UNTRUST
##Security Firewall Policy : TESTBED - UNTRUST##
delete security policies from-zone TESTBED to-zone UNTRUST
##Security Firewall Policy : WAREHOUSE - WAREHOUSE##
delete security policies from-zone WAREHOUSE to-zone WAREHOUSE
##Security Firewall Policy : global ##
delete security policies global policy TRUST
delete security policies global policy WAREHOUSE
set security policies global policy PolicyEnforcer-Rule1-1 match application any
set security policies global policy PolicyEnforcer-Rule1-1 match destination-address any
set security policies global policy PolicyEnforcer-Rule1-1 match source-address JNCIE-PEG_172.16.50.100
set security policies global policy PolicyEnforcer-Rule1-1 then permit application-services advanced-anti-malware-policy JNCIE-SEC-TPP-SL1
set security policies global policy PolicyEnforcer-Rule1-1 then permit application-services security-intelligence-policy JNCIE-SEC-TPP-SL1
##Security Intelligence Policy Configurations##
set services security-intelligence policy JNCIE-SEC-TPP-SL1 CC JNCIE-SEC-TPP-SL1_CC
set services security-intelligence policy JNCIE-SEC-TPP-SL1 Infected-Hosts JNCIE-SEC-TPP-SL1_Infected-Hosts
##Security Intelligence Profile Configurations##
set services security-intelligence profile JNCIE-SEC-TPP-SL1_CC category CC
set services security-intelligence profile JNCIE-SEC-TPP-SL1_CC rule Rule-1 match threat-level 1
set services security-intelligence profile JNCIE-SEC-TPP-SL1_CC rule Rule-1 match threat-level 2
set services security-intelligence profile JNCIE-SEC-TPP-SL1_CC rule Rule-1 match threat-level 3
set services security-intelligence profile JNCIE-SEC-TPP-SL1_CC rule Rule-1 match threat-level 4
set services security-intelligence profile JNCIE-SEC-TPP-SL1_CC rule Rule-1 match threat-level 5
set services security-intelligence profile JNCIE-SEC-TPP-SL1_CC rule Rule-1 match threat-level 6
set services security-intelligence profile JNCIE-SEC-TPP-SL1_CC rule Rule-1 match threat-level 7
set services security-intelligence profile JNCIE-SEC-TPP-SL1_CC rule Rule-1 then action permit
set services security-intelligence profile JNCIE-SEC-TPP-SL1_CC rule Rule-1 then log
set services security-intelligence profile JNCIE-SEC-TPP-SL1_CC rule Rule-2 match threat-level 8
set services security-intelligence profile JNCIE-SEC-TPP-SL1_CC rule Rule-2 match threat-level 9
set services security-intelligence profile JNCIE-SEC-TPP-SL1_CC rule Rule-2 match threat-level 10
set services security-intelligence profile JNCIE-SEC-TPP-SL1_CC rule Rule-2 then action block drop
set services security-intelligence profile JNCIE-SEC-TPP-SL1_CC rule Rule-2 then log
set services security-intelligence profile JNCIE-SEC-TPP-SL1_Infected-Hosts category Infected-Hosts
set services security-intelligence profile JNCIE-SEC-TPP-SL1_Infected-Hosts rule Rule-1 match threat-level 1
set services security-intelligence profile JNCIE-SEC-TPP-SL1_Infected-Hosts rule Rule-1 match threat-level 2
set services security-intelligence profile JNCIE-SEC-TPP-SL1_Infected-Hosts rule Rule-1 match threat-level 3
set services security-intelligence profile JNCIE-SEC-TPP-SL1_Infected-Hosts rule Rule-1 match threat-level 4
set services security-intelligence profile JNCIE-SEC-TPP-SL1_Infected-Hosts rule Rule-1 match threat-level 5
set services security-intelligence profile JNCIE-SEC-TPP-SL1_Infected-Hosts rule Rule-1 match threat-level 6
set services security-intelligence profile JNCIE-SEC-TPP-SL1_Infected-Hosts rule Rule-1 then action permit
set services security-intelligence profile JNCIE-SEC-TPP-SL1_Infected-Hosts rule Rule-1 then log
set services security-intelligence profile JNCIE-SEC-TPP-SL1_Infected-Hosts rule Rule-2 match threat-level 7
set services security-intelligence profile JNCIE-SEC-TPP-SL1_Infected-Hosts rule Rule-2 match threat-level 8
set services security-intelligence profile JNCIE-SEC-TPP-SL1_Infected-Hosts rule Rule-2 match threat-level 9
set services security-intelligence profile JNCIE-SEC-TPP-SL1_Infected-Hosts rule Rule-2 match threat-level 10
set services security-intelligence profile JNCIE-SEC-TPP-SL1_Infected-Hosts rule Rule-2 then action block drop
set services security-intelligence profile JNCIE-SEC-TPP-SL1_Infected-Hosts rule Rule-2 then log
##Advanced AntiMalware Policy Configurations##
set services advanced-anti-malware policy JNCIE-SEC-TPP-SL1 blacklist-notification log
set services advanced-anti-malware policy JNCIE-SEC-TPP-SL1 default-notification log
set services advanced-anti-malware policy JNCIE-SEC-TPP-SL1 fallback-options action permit
set services advanced-anti-malware policy JNCIE-SEC-TPP-SL1 fallback-options notification log
set services advanced-anti-malware policy JNCIE-SEC-TPP-SL1 http action block
set services advanced-anti-malware policy JNCIE-SEC-TPP-SL1 http inspection-profile default_profile
set services advanced-anti-malware policy JNCIE-SEC-TPP-SL1 http notification log
set services advanced-anti-malware policy JNCIE-SEC-TPP-SL1 verdict-threshold 8
set services advanced-anti-malware policy JNCIE-SEC-TPP-SL1 whitelist-notification log
##SSL Forward proxy Profile Configurations##
delete services ssl proxy profile CENTRAL-SSL
##UTM Configurations##
delete security utm
```

OK

© 2020 Juniper Networks, Inc. All rights reserved.

l) Return to the CLI with the central cluster (srx3/srx4) and enter configuration mode. Examine the differences between the current and previous configurations.

```
{primary:node0}
lab@central-node0> configure
warning: Clustering enabled; using private edit
warning: uncommitted changes will be discarded on exit
Entering configuration mode

{primary:node0}[edit]
lab@central-node0# show | compare rollback 1
[edit services ssl]
-    proxy {
-        profile CENTRAL-SSL {
-            root-ca MY-CERT;
-            actions {
-                ignore-server-auth-failure;
-                log {
-                    all;
-                }
-            }
-        }
-    }
[edit services security-intelligence]
+    profile JNCIE-SEC-TPP-SL1_CC {
+        category CC;
+        rule Rule-1 {
+            match {
+                threat-level [ 1 2 3 4 5 6 7 ];
+            }
+            then {
+                action {
+                    permit;
+                }
+                log;
+            }
+        }
+        rule Rule-2 {
+            match {
+                threat-level [ 8 9 10 ];
+            }
+            then {
+                action {
+                    block {
+                        drop;
+                    }
+                }
+                log;
+            }
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
+         }
+     }
+     profile JNCIE-SEC-TPP-SL1_Infected-Hosts {
+         category Infected-Hosts;
+         rule Rule-1 {
+             match {
+                 threat-level [ 1 2 3 4 5 6 ];
+             }
+             then {
+                 action {
+                     permit;
+                 }
+                 log;
+             }
+         }
+         rule Rule-2 {
+             match {
+                 threat-level [ 7 8 9 10 ];
+             }
+             then {
+                 action {
+                     block {
+                         drop;
+                     }
+                 }
+                 log;
+             }
+         }
+     }
+     policy JNCIE-SEC-TPP-SL1 {
+         CC {
+             JNCIE-SEC-TPP-SL1_CC;
+         }
+         Infected-Hosts {
+             JNCIE-SEC-TPP-SL1_Infected-Hosts;
+         }
+     }
[edit services advanced-anti-malware]
+     policy JNCIE-SEC-TPP-SL1 {
+         http {
+             inspection-profile default_profile;
+             action block;
+             notification {
+                 log;
+             }
+         }
+         verdict-threshold 8;
+         fallback-options {
+             action permit;
+             notification {
+                 log;
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
+            }
+        }
+        default-notification {
+            log;
+        }
+        whitelist-notification {
+            log;
+        }
+        blacklist-notification {
+            log;
+        }
+    }
[edit security address-book global]
+    address JNCIE-PEG_172.16.50.100 172.16.50.100/32;
-    address CENTRAL-TRUST 172.16.50.0/24;
-    address CENTRAL-INTERNAL 172.16.55.0/24;
-    address CENTRAL-WAREHOUSE 172.16.60.0/24;
-    address CENTRAL-TESTBED6 172.16.65.0/24;
-    address CENTRAL-TESTBED7 172.16.70.0/24;
-    address SRV-MAIL 172.16.60.199/32;
-    address WAREHOUSE-SRV-205 172.16.60.205/32;
-    address WAREHOUSE-SRV-206 172.16.60.206/32;
-    address WAREHOUSE-HONEYPOT 172.16.60.207/32;
-    address RO1-TRUST 172.16.10.0/24;
-    address RO2-TRUST 172.16.20.0/24;
-    address EXA-TRUST 172.16.10.0/24;
-    address WEBSENSE 172.16.60.99/32;
-    address RO1-HOST-PRIVATE 172.16.11.50/32;
-    address RO2-SRV-WEB 172.16.21.2/32;
-    address RO2-SRV-DB 172.16.21.33/32;
-    address EXA-SRV-WEB 172.16.30.11/32;
-    address EXA-SRV-DB 172.16.30.12/32;
-    address EXA-SRV-SSH 172.16.30.13/32;
-    address EXA-PRIVATE 172.16.15.0/24;
-    address HOFFICE-TRUST 172.16.77.0/24;
-    address EXA-TRUST-OVERLAP 172.16.110.0/24;
-    address RO1-TRUST-OVERLAP 172.16.111.0/24;
-    address BUILDING-TRUST-B1 172.16.100.0/24;
-    address BUILDING-TRUST-B2 172.16.200.0/24;
-    address BUILDING-DMZ-B2 172.16.201.0/24;
-    address BUILDING-DMZ-B1 172.16.101.0/24;
[edit security address-book global]
-    address-set CENTRAL-TESTBED {
-        address CENTRAL-TESTBED6;
-        address CENTRAL-TESTBED7;
-    }
-    address-set TRUST-NETWORKS {
-        address RO1-TRUST;
-        address RO2-TRUST;
-        address CENTRAL-TRUST;
-        address HOFFICE-TRUST;
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
-         address EXA-TRUST-OVERLAP;
-         address RO1-TRUST-OVERLAP;
-         address BUILDING-TRUST-B1;
-         address BUILDING-TRUST-B2;
-     }
[edit security]
-    utm {
-        custom-objects {
-            filename-extension {
-                bat-sh {
-                    value [ bat sh ];
-                }
-            }
-            url-pattern {
-                spam-sources {
-                    value [ 4.4.4.4 5.5.5.5 45.45.45.45. spam.com bad.com "spam@gmail.com"
"spam@yahoo.com" ];
-                }
-            }
-        }
-        default-configuration {
-            anti-spam {
-                type sbl;
-            }
-        }
-        feature-profile {
-            anti-spam {
-                address-blacklist spam-sources;
-                sbl {
-                    profile smtp-protect {
-                        no-sbl-default-server;
-                        spam-action block;
-                    }
-                }
-            }
-            content-filtering {
-                profile CENTRAL-content-filter {
-                    block-extension bat-sh;
-                    block-content-type {
-                        java-applet;
-                        http-cookie;
-                    }
-                    notification-options {
-                        type protocol-only;
-                        custom-message "Firewall blocked this content!";
-                    }
-                }
-            }
-        }
-        utm-policy CENTRAL-Content {
-            content-filtering {
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
-                 http-profile CENTRAL-content-filter;
-                 ftp {
-                     upload-profile CENTRAL-content-filter;
-                     download-profile CENTRAL-content-filter;
-                 }
-             }
-         }
-         utm-policy CENTRAL-SPAM {
-             anti-spam {
-                 smtp-profile smtp-protect;
-             }
-         }
-     }
[edit security policies]
-     from-zone UNTRUST to-zone WAREHOUSE {
-         policy SRV-MAIL {
-             match {
-                 source-address any;
-                 destination-address SRV-MAIL;
-                 application junos-smtp;
-             }
-             then {
-                 permit {
-                     destination-address {
-                         drop-untranslated;
-                     }
-                     application-services {
-                         utm-policy CENTRAL-SPAM;
-                     }
-                 }
-             }
-         }
-         policy SERVERS {
-             match {
-                 source-address any;
-                 destination-address [ WAREHOUSE-SRV-205 WAREHOUSE-SRV-206 WAREHOUSE-HONEYPOT
];
-                 application any;
-             }
-             then {
-                 permit {
-                     destination-address {
-                         drop-untranslated;
-                     }
-                     application-services {
-                         idp;
-                     }
-                 }
-             }
-         }
-     }
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
-    from-zone TRUST to-zone UNTRUST {
-        policy HTTP-FTP {
-            match {
-                source-address CENTRAL-TRUST;
-                destination-address any;
-                application [ junos-http junos-ftp ];
-                dynamic-application junos:MSN;
-            }
-            then {
-                permit {
-                    application-services {
-                        utm-policy CENTRAL-Content;
-                        application-traffic-control {
-                            rule-set MEGA;
-                        }
-                    }
-                }
-                log {
-                    session-init;
-                    session-close;
-                }
-            }
-        }
-        policy INTERNET {
-            match {
-                source-address CENTRAL-TRUST;
-                destination-address any;
-                application any;
-            }
-            then {
-                permit;
-            }
-        }
-    }
-    from-zone INTERNAL to-zone WAREHOUSE {
-        policy WEBSENSE {
-            match {
-                source-address CENTRAL-INTERNAL;
-                destination-address any;
-                application junos-http;
-            }
-            then {
-                permit;
-            }
-        }
-    }
-    from-zone TESTBED to-zone WAREHOUSE {
-        policy WEBSENSE {
-            match {
-                source-address CENTRAL-TESTBED;
-                destination-address any;
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
-                 application junos-http;
-                 dynamic-application junos:HTTP;
-             }
-             then {
-                 permit;
-                 log {
-                     session-init;
-                     session-close;
-                 }
-             }
-         }
-     }
-     from-zone WAREHOUSE to-zone UNTRUST {
-         policy WEBSENSE {
-             match {
-                 source-address WEBSENSE;
-                 destination-address any;
-                 application junos-http;
-             }
-             then {
-                 permit;
-             }
-         }
-         policy SRV-MAIL {
-             match {
-                 source-address SRV-MAIL;
-                 destination-address any;
-                 application any;
-             }
-             then {
-                 permit;
-             }
-         }
-     }
-     from-zone INTERNAL to-zone UNTRUST {
-         policy INTERNET {
-             match {
-                 source-address CENTRAL-INTERNAL;
-                 destination-address any;
-                 application any;
-             }
-             then {
-                 permit;
-             }
-         }
-     }
-     from-zone UNTRUST to-zone UNTRUST {
-         policy UNTRUST {
-             match {
-                 source-address any;
-                 destination-address any;
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
-                 application any;
-             }
-             then {
-                 permit;
-             }
-         }
-     }
-     from-zone TESTBED to-zone UNTRUST {
-         policy HTTPS {
-             match {
-                 source-address CENTRAL-TESTBED;
-                 destination-address any;
-                 application junos-https;
-             }
-             then {
-                 permit {
-                     application-services {
-                         ssl-proxy {
-                             profile-name CENTRAL-SSL;
-                         }
-                     }
-                 }
-             }
-         }
-     }
-     from-zone WAREHOUSE to-zone WAREHOUSE {
-         policy WAREHOUSE {
-             match {
-                 source-address any;
-                 destination-address any;
-                 application any;
-             }
-             then {
-                 permit;
-             }
-         }
-     }
[edit security policies global]
+     policy PolicyEnforcer-Rule1-1 {
+         match {
+             source-address JNCIE-PEG_172.16.50.100;
+             destination-address any;
+             application any;
+         }
+         then {
+             permit {
+                 application-services {
+                     security-intelligence-policy JNCIE-SEC-TPP-SL1;
+                     advanced-anti-malware-policy JNCIE-SEC-TPP-SL1;
+                 }
+             }
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
+         }
+     }
-     policy TRUST {
-         match {
-             source-address TRUST-NETWORKS;
-             destination-address TRUST-NETWORKS;
-             application any;
-             source-identity any;
-         }
-         then {
-             permit;
-         }
-     }
-     policy WAREHOUSE {
-         match {
-             source-address any;
-             destination-address CENTRAL-WAREHOUSE;
-             application junos-ftp;
-             to-zone WAREHOUSE;
-         }
-         then {
-             permit {
-                 application-services {
-                     idp;
-                 }
-             }
-         }
-     }

{primary:node0}[edit]
lab@central-node0#
```

m) Merge the current configuration with the previous configuration. Note that the new global polices conflict with some zonal policies. The conflict means the zonal policies are honored before global based polices, this idea means that the traffic from the 172.16.50.100 host is not subject to SDSN. We will fix this issue in a later step.

```
{primary:node0}[edit]
lab@srx5# rollback 1
load complete

{primary:node0}[edit]
lab@srx5# save sl1-task9-sdsn.config
Wrote 1744 lines of configuration to 'sl1-task9-sdsn.config'

{primary:node0}[edit]
lab@srx5# rollback

{primary:node0}[edit]
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
lab@srx5# load merge sl1-task9-sdsn.config
load complete

{primary:node0}[edit]
lab@srx5# commit and-quit
node0:
configuration check succeeds
node1:
commit complete
node0:
commit complete

{primary:node0}[edit]
lab@srx5>
```

n) There still is a conflict between the global policies and the zone policies that will not let traffic from the 172.16.10.100 host hit the global policies with the SDSN content. Enter configuration mode and convert the zonal policies to global policies. Remember to maintain the zone to zone context for these policies.

i. Examine the security policies

```
{primary:node0}
lab@central-node0> show configuration security policies
from-zone UNTRUST to-zone WAREHOUSE {
    policy SRV-MAIL {
        match {
            source-address any;
            destination-address SRV-MAIL;
            application junos-smtp;
        }
        then {
            permit {
                destination-address {
                    drop-untranslated;
                }
                application-services {
                    utm-policy CENTRAL-SPAM;
                }
            }
        }
    }
    policy SERVERS {
        match {
            source-address any;
            destination-address [ WAREHOUSE-SRV-205 WAREHOUSE-SRV-206 WAREHOUSE-HONEYPOT ];
            application any;
        }
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
        then {
            permit {
                destination-address {
                    drop-untranslated;
                }
                application-services {
                    idp;
                }
            }
        }
    }
}
from-zone TRUST to-zone UNTRUST {
    policy HTTP-FTP {
        match {
            source-address CENTRAL-TRUST;
            destination-address any;
            application [ junos-http junos-ftp ];
            dynamic-application junos:MSN;
        }
        then {
            permit {
                application-services {
                    utm-policy CENTRAL-Content;
                    application-traffic-control {
                        rule-set MEGA;
                    }
                }
            }
            log {
                session-init;
                session-close;
            }
        }
    }
    policy INTERNET {
        match {
            source-address CENTRAL-TRUST;
            destination-address any;
            application any;
        }
        then {
            permit;
        }
    }
}
from-zone INTERNAL to-zone WAREHOUSE {
    policy WEBSENSE {
        match {
            source-address CENTRAL-INTERNAL;
            destination-address any;
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
            application junos-http;
        }
        then {
            permit;
        }
    }
}
from-zone TESTBED to-zone WAREHOUSE {
    policy WEBSENSE {
        match {
            source-address CENTRAL-TESTBED;
            destination-address any;
            application junos-http;
            dynamic-application junos:HTTP;
        }
        then {
            permit;
            log {
                session-init;
                session-close;
            }
        }
    }
}
from-zone WAREHOUSE to-zone UNTRUST {
    policy WEBSENSE {
        match {
            source-address WEBSENSE;
            destination-address any;
            application junos-http;
        }
        then {
            permit;
        }
    }
    policy SRV-MAIL {
        match {
            source-address SRV-MAIL;
            destination-address any;
            application any;
        }
        then {
            permit;
        }
    }
}
from-zone INTERNAL to-zone UNTRUST {
    policy INTERNET {
        match {
            source-address CENTRAL-INTERNAL;
            destination-address any;
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
            application any;
        }
        then {
            permit;
        }
    }
}
from-zone UNTRUST to-zone UNTRUST {
    policy UNTRUST {
        match {
            source-address any;
            destination-address any;
            application any;
        }
        then {
            permit;
        }
    }
}
from-zone TESTBED to-zone UNTRUST {
    policy HTTPS {
        match {
            source-address CENTRAL-TESTBED;
            destination-address any;
            application junos-https;
        }
        then {
            permit {
                application-services {
                    ssl-proxy {
                        profile-name CENTRAL-SSL;
                    }
                }
            }
        }
    }
}
from-zone WAREHOUSE to-zone WAREHOUSE {
    policy WAREHOUSE {
        match {
            source-address any;
            destination-address any;
            application any;
        }
        then {
            permit;
        }
    }
}
global {
    policy PolicyEnforcer-Rule1-1 {
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
match {
    source-address JNCIE-PEG_172.16.50.100;
    destination-address any;
    application any;
}
then {
    permit {
        application-services {
            security-intelligence-policy JNCIE-SEC-TPP-SL1;
            advanced-anti-malware-policy JNCIE-SEC-TPP-SL1;
        }
    }
}
policy TRUST {
    match {
        source-address TRUST-NETWORKS;
        destination-address TRUST-NETWORKS;
        application any;
        source-identity any;
    }
    then {
        permit;
    }
}
policy WAREHOUSE {
    match {
        source-address any;
        destination-address CENTRAL-WAREHOUSE;
        application junos-ftp;
        to-zone WAREHOUSE;
    }
    then {
        permit {
            application-services {
                idp;
            }
        }
    }
}
```

ii. Enter configuration mode and copy and paste the PolicyEnforcer-Rule1-1 global policy into the [edit security policies from-zone TRUST to-zone UNTRUST] configuration hierarchy.

```
{primary:node0}
lab@central-node0> configure
warning: Clustering enabled; using private edit
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
warning: uncommitted changes will be discarded on exit
Entering configuration mode

{primary:node0}[edit]
lab@central-node0# edit security policies from-zone TRUST to-zone UNTRUST

{primary:node0}[edit]
lab@central-node0# edit security policies from-zone TRUST to-zone UNTRUST

{primary:node0}[edit security policies from-zone TRUST to-zone UNTRUST]
lab@central-node0# load merge terminal relative
[Type ^D at a new line to end input]
    policy PolicyEnforcer-Rule1-1 {
        match {
            source-address JNCIE-PEG_172.16.50.100;
            destination-address any;
            application any;
        }
        then {
            permit {
                application-services {
                    security-intelligence-policy JNCIE-SEC-TPP-SL1;
                    advanced-anti-malware-policy JNCIE-SEC-TPP-SL1;
                }
            }
        }
    }
load complete

{primary:node0}[edit security policies from-zone TRUST to-zone UNTRUST]
lab@central-node0# up 1 delete global policy PolicyEnforcer-Rule1-1

{primary:node0}[edit security policies from-zone TRUST to-zone UNTRUST]
lab@central-node0#
```

iii. Configure the PolicyEnforcer-Rule1-1 to match on all dynamic applications

```
{primary:node0}[edit security policies from-zone TRUST to-zone UNTRUST]
lab@central-node0# set policy PolicyEnforcer-Rule1-1 match dynamic-application any
```

iv. Place the PolicyEnforcer-Rule1-1 before all the other policies in the TRUST to UNTRUST zone context.

```
{primary:node0}[edit security policies from-zone TRUST to-zone UNTRUST]
lab@central-node0# insert policy PolicyEnforcer-Rule1-1 before policy HTTP-FTP

{primary:node0}[edit security policies from-zone TRUST to-zone UNTRUST]
lab@central-node0# top
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
{primary:node0}[edit]
lab@central-node0# commit and-quit
node0:
configuration check succeeds
node1:
commit complete
node0:
commit complete
Exiting configuration mode

{primary:node0}
lab@central-node0>
```

o) You can verify the SDSN policies on in the CLI of the central cluster (srx3/4).

```
{primary:node0}
lab@central-node0> show configuration services
rpm {
    probe ping-9 {
        test icmp {
            probe-type icmp-ping;
            target address 12.34.56.78;
            probe-count 3;
            probe-interval 5;
            test-interval 15;
            thresholds {
                successive-loss 3;
                total-loss 3;
            }
            next-hop 80.1.1.9;
        }
    }
    probe ping-13 {
        test icmp {
            probe-type icmp-ping;
            target address 12.34.56.78;
            probe-count 3;
            probe-interval 5;
            test-interval 15;
            thresholds {
                successive-loss 3;
                total-loss 3;
            }
            next-hop 80.1.1.13;
        }
    }
}
application-identification {
    no-application-system-cache;
}
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
ssl {
    initiation {
        profile aamw-ssl {
            trusted-ca [ aamw-secintel-ca aamw-cloud-ca ];
            client-certificate aamw-srx-cert;
            actions {
                crl {
                    disable;
                }
            }
        }
    }
    proxy {
        profile CENTRAL-SSL {
            root-ca MY-CERT;
            actions {
                ignore-server-auth-failure;
                log {
                    all;
                }
            }
        }
    }
}
security-intelligence {
    url https://10.10.1.123:443/api/v1/manifest.xml;
    authentication {
        auth-token PKY8AM0SYQ492TPA00IGI82YG9BJ4RWZ;
    }
    profile JNCIE-SEC-TPP-SL1_CC {
        category CC;
        rule Rule-1 {
            match {
                threat-level [ 1 2 3 4 5 6 7 ];
            }
            then {
                action {
                    permit;
                }
                log;
            }
        }
        rule Rule-2 {
            match {
                threat-level [ 8 9 10 ];
            }
            then {
                action {
                    block {
                        drop;
                    }
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
                }
                log;
            }
        }
    }
    profile JNCIE-SEC-TPP-SL1_Infected-Hosts {
        category Infected-Hosts;
        rule Rule-1 {
            match {
                threat-level [ 1 2 3 4 5 6 ];
            }
            then {
                action {
                    permit;
                }
                log;
            }
        }
        rule Rule-2 {
            match {
                threat-level [ 7 8 9 10 ];
            }
            then {
                action {
                    block {
                        drop;
                    }
                }
                log;
            }
        }
    }
    policy JNCIE-SEC-TPP-SL1 {
        CC {
            JNCIE-SEC-TPP-SL1_CC;
            }
            Infected-Hosts {
                JNCIE-SEC-TPP-SL1_Infected-Hosts;
            }
        }
    }
    advanced-anti-malware {
        connection {
            url https://srxapi.us-west-2.sky.junipersecurity.net;
            authentication {
                tls-profile aamw-ssl;
            }
        }
        policy JNCIE-SEC-TPP-SL1 {
            http {
                inspection-profile default_profile;
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
        action block;
        notification {
            log;
        }
    }
    verdict-threshold 8;
    fallback-options {
        action permit;
        notification {
            log;
        }
    }
    default-notification {
            log;
        }
        whitelist-notification {
            log;
        }
        blacklist-notification {
            log;
        }
    }
}
user-identification {
    identity-management {
        connection {
            connect-method https;
            port 443;
            primary {
                address 10.10.1.121;
                client-id jncie;
                client-secret "$9$wv2oGzF/tpBk.Qn/9pu8XxdYg"; ## SECRET-DATA
            }
            token-api oauth_token/oauth;
            query-api user_query/v2;
        }
    }
}
ip-monitoring {
    policy ping-9 {
        match {
            rpm-probe ping-9;
        }
        then {
            interface ge-0/0/3 {
                disable;
            }
        }
    }
    policy ping-13 {
        match {
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
            rpm-probe ping-13;
        }
        then {
            interface ge-7/0/3 {
                disable;
            }
        }
    }
}

{primary:node0}
lab@central-node0> show configuration security policies from-zone TRUST to-zone UNTRUST
policy PolicyEnforcer-Rule1-1 {
    match {
        source-address JNCIE-PEG_172.16.50.100;
        destination-address any;
        application any;
        dynamic-application any;
    }
    then {
        permit {
            application-services {
                security-intelligence-policy JNCIE-SEC-TPP-SL1;
                advanced-anti-malware-policy JNCIE-SEC-TPP-SL1;
            }
        }
    }
}
policy HTTP-FTP {
    match {
        source-address CENTRAL-TRUST;
        destination-address any;
        application [ junos-http junos-ftp ];
        dynamic-application junos:MSN;
    }
    then {
        permit {
            application-services {
                utm-policy CENTRAL-Content;
                application-traffic-control {
                    rule-set MEGA;
                }
            }
        }
        log {
            session-init;
            session-close;
        }
    }
}
policy INTERNET {
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
        match {
            source-address CENTRAL-TRUST;
            destination-address any;
            application any;
        }
        then {
            permit;
        }
    }
```

END SUPER LAB 1

© 2020 Juniper Networks, Inc. All rights reserved.

Appendix - Super Lab 2

This lab is designed to combine many of the solutions discussed in the previous chapters into a complete practice lab exam. This lab is similar to a real JNCIE-SEC lab exam experience. We recommend attempting this lab if you are able to complete the tasks in the previous chapters without any help.

This walkthrough provides details about the solution for the “Super Lab 2” section of the workbook. Assumption is that the walkthrough of the workbook is completed and understood. The focus of this solution targets on thought strategy and quick perception on how to address prompted tasks.

Structure of document

The construct of this lab tasks focuses on strategy for the real JNCIE exam. It is never enough to emphasize how important it is to read the whole chapter and even the whole exam before starting the configuration of the devices. Here again we can see that several tasks depend on subsequent steps in order to achieve full functionality.

Do not forget that previous tasks may be impacted by configurations performed at later stages. A full revision of the Lab should take place in the end to confirm all tasks are performing according to requirement.

The input commands are sensitive to the prompt tag. Please be aware of the **#** and the **>** signs when checking the snippet. Also consider the device you are inputting the commands; the interpretation section will identify a single or multiple devices and the prompt will either be absent of node identification or explicitly identify where the configuration is being input. In the case of absence, it is the main device the majority of the commands are being input or it is part of multiple devices.

Hierarchical moves are not shown and commit operation is assumed implicit for configuration to become active. Although several tasks show the verification result please bear in mind that such commit and verification may be dependent on other tasks.
The outputs from the devices may been trimmed for the sake of simplicity.

Functionality:

- **You will be able to test functionality of tasks to make sure that your network is operational.**
- **The VR device bears necessary routing instances to emulate all end devices**

© 2020 Juniper Networks, Inc. All rights reserved.

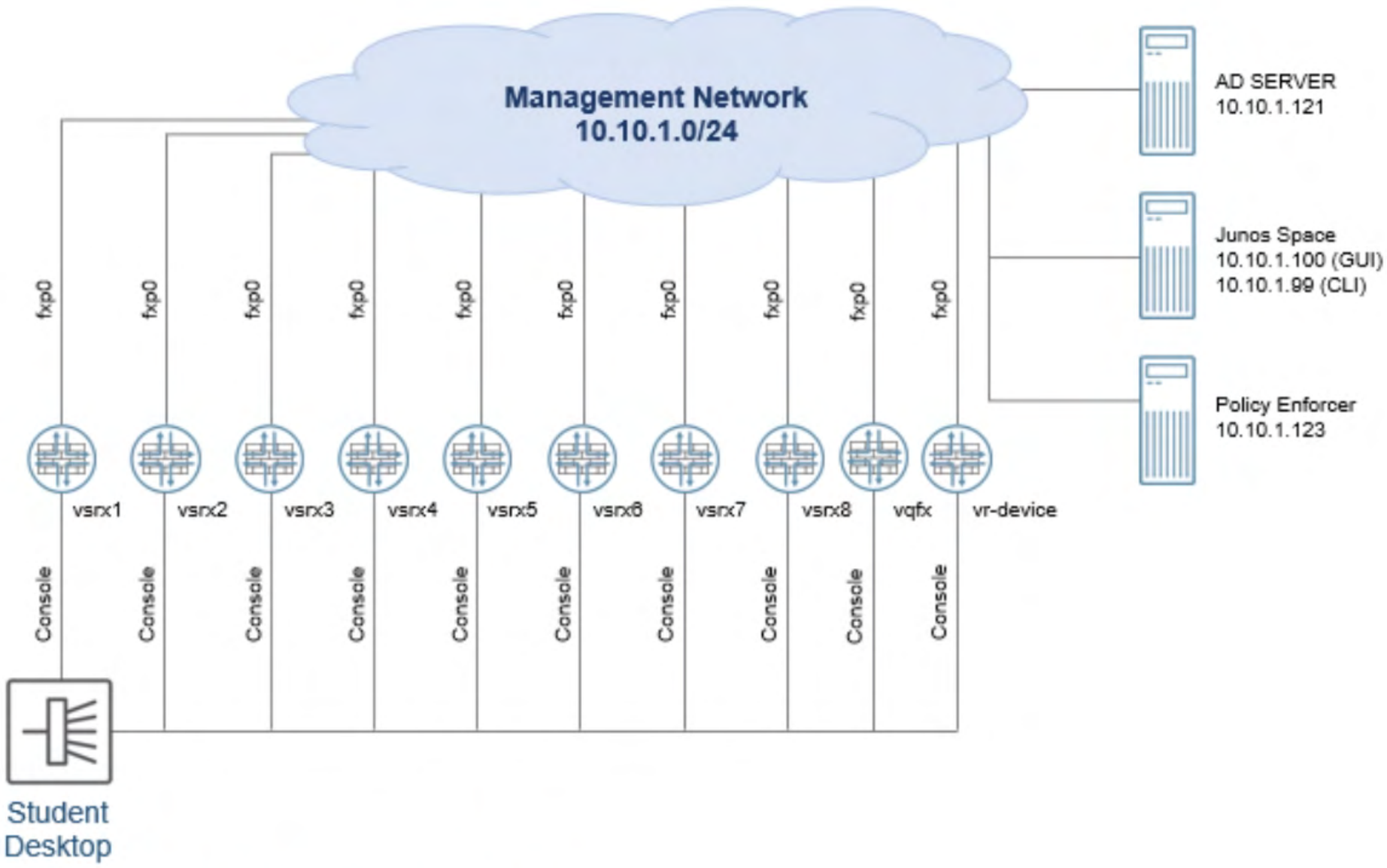


Figure 1: Super Lab 2 – Management Topology

Ensure you load the initial configurations on the devices before you start with this LAB. Ensure that you do not forget to load the initial Super Lab 2 configuration on the vr-device.

Tip: Ensure you read whole tasks before starting them.

© 2020 Juniper Networks, Inc. All rights reserved.

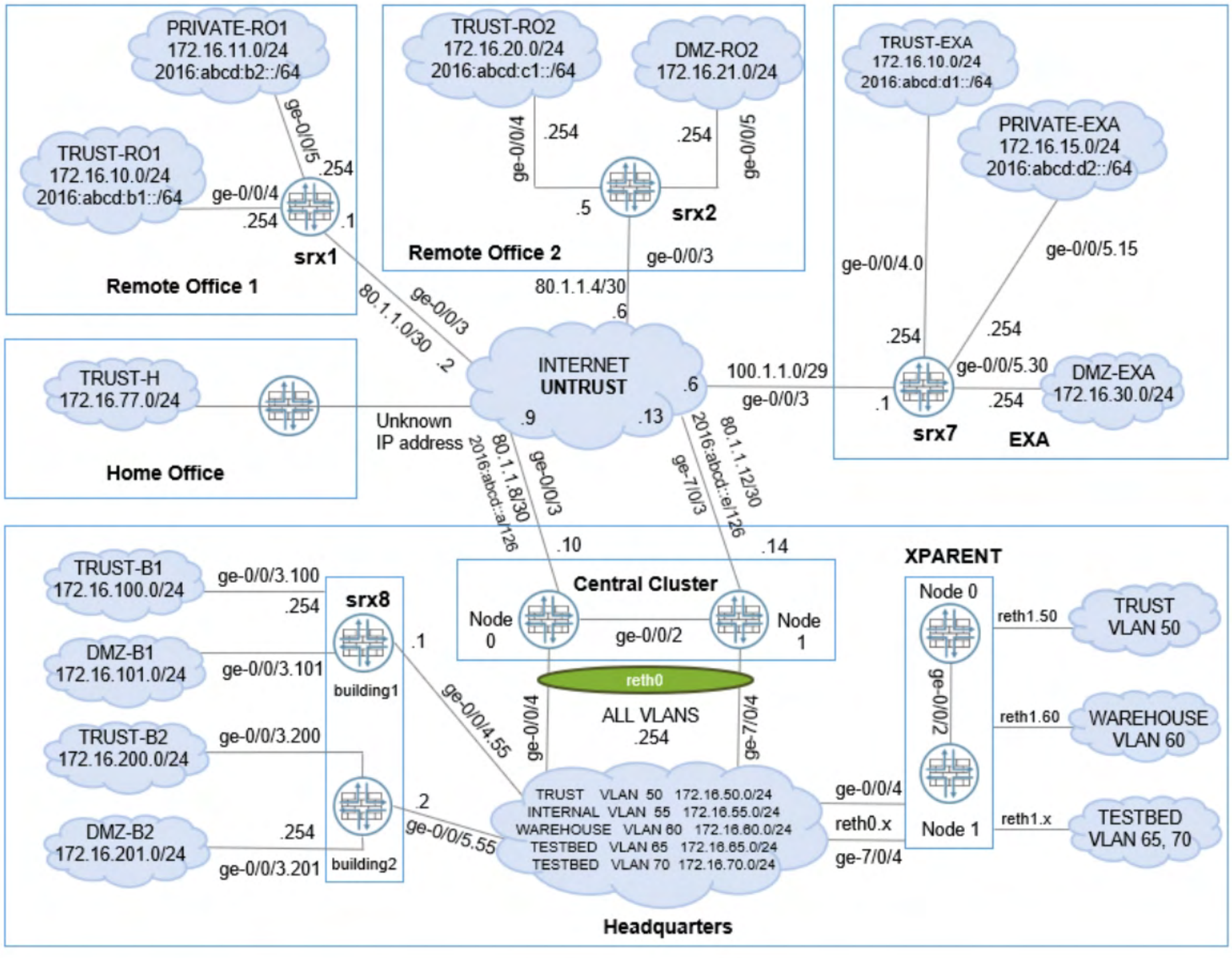


Figure 2: Super Lab 2 Topology

© 2020 Juniper Networks, Inc. All rights reserved.

Task 1: Initial Configuration – Part1

1) The table below lists the device hostnames mapping:

Device	Hostname
srx1	roffice1
srx2	roffice2
srx3	central-node0
srx4	central-node1
srx5	xparent-node0
srx6	xparent-node1
srx7	exa-fw
srx8	building

```
lab@roffice1# show system host-name
host-name roffice1;
```

2) Create clusters as defined in the following table:

Device	Node ID	Cluster ID
central-node0	0	1
central-node1	1	1
xparent-node0	0	2
xparent-node1	1	2

3) Ensure the ge-0/0/2 interfaces are used fabric link respectively.

Central nodes:

```
lab@srx3# run set chassis cluster cluster-id 1 node 0 reboot
lab@srx4# run set chassis cluster cluster-id 1 node 1 reboot
Successfully enabled chassis cluster. Going to reboot now.

{primary:node0}
lab@central-node0>

delete system hostname
delete interfaces fxp0
set groups node0 system host-name central-node0
set groups node0 interfaces fxp0 unit 0 family inet address 10.10.1.3/24
set groups node1 system host-name central-node1
set groups node1 interfaces fxp0 unit 0 family inet address 10.10.1.4/24
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
set apply-groups "${node}"
set interfaces fab0 fabric-options member-interfaces ge-0/0/2
set interfaces fab1 fabric-options member-interfaces ge-7/0/2
```

xparent nodes:

```
lab@srx5# run set chassis cluster cluster-id 2 node 0 reboot
lab@srx6# run set chassis cluster cluster-id 2 node 1 reboot
Successfully enabled chassis cluster. Going to reboot now.
```

After the reboot configure the fab links and management

```
{primary:node0}[edit]
lab@xparent-node0#
delete system hostname
delete interfaces fxp0
set groups node0 system host-name xparent-node0
set groups node0 interfaces fxp0 unit 0 family inet address 10.10.1.5/24
set groups node1 system host-name xparent-node1
set groups node1 interfaces fxp0 unit 0 family inet address 10.10.1.6/24
set apply-groups "${node}"
set interfaces fab0 fabric-options member-interfaces ge-0/0/2
set interfaces fab1 fabric-options member-interfaces ge-7/0/2
```

Verification

```
> show chassis cluster interfaces | match "(Fabric)|(Control)|(fab)" | except
interfaces
Control link status: Up

Fabric link status: Up
    fab0    ge-0/0/2            Up   / Up
    fab0
    fab1    ge-7/0/2            Up   / Up
    fab1
```

4) The routing engine of xparent cluster needs to be active on node 0
5) Configure the redundant ethernet interfaces according the figure 2.
6) Clusters should operate in the following manner:
    a. Central cluster redundancy groups mapped to interfaces dependent on physical links, need to be active on node0 whenever node0 is available
        i. Any failure from correspondent child interface triggers the failover
    b. Central cluster redundancy groups (RGs) mapped to interfaces dependent on logical links, need to be active on node1 whenever node1 is available
        i. Uplink interface monitoring triggers the failover

© 2020 Juniper Networks, Inc. All rights reserved.

c. The Central Cluster needs to monitor ICMP reachability to the host address available in the Internet. In case this reachability is compromised, the test's uplink interface should be brought down so that the RG fails over.
    i. Probe threshold should be between 30 and 60 seconds
    ii. Control plane redundancy group needs to follow the same faith of the RG from step 6.b
d. All xparent cluster redundancy groups need to be active on node 0 and should automatically failover in case any of its physical links fail.
    i. No need for automatic recovery of primacy

Note: Where the SRX cluster is the end point, all services need to be directed to a interface that depends on Redundant Groups. Since this setup has two physical interfaces connecting to the service provider environment, we need to terminate all services that may be arriving from those interfaces in such a logical interface.

Note: The task differentiates redundancy groups mapped to redundant interfaces which bear physical links or logical interfaces that may have redundancy group dependency. In the SRX cluster the loopback interface is such logical interface which by default is part of RG0.

```
>show chassis cluster interfaces | find Redundant-pseudo
Redundant-pseudo-interface Information:
    Name         Status      Redundancy-group
    lo0          Up          0
```

Note: IP-monitoring for redundant groups is only valid when the probe is sent through a reth interface for reachability test. The setup depends on two distinct physical links, so it is not possible to use this feature. The RPM service probes for host reachability and the IP Monitoring acts upon probe's result. In case the probe fails, the interface is brought down.

Central-node:

```
set interfaces reth0 vlan-tagging
set interfaces reth0 redundant-ether-options redundancy-group 1
set interfaces reth0 unit 50 vlan-id 50
set interfaces reth0 unit 50 family inet address 172.16.50.254/24
set interfaces reth0 unit 50 family inet6 address 2016:abcd:a1::254/64
set interfaces reth0 unit 55 vlan-id 55
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
set interfaces reth0 unit 55 family inet address 172.16.55.254/24
set interfaces reth0 unit 60 vlan-id 60
set interfaces reth0 unit 60 family inet address 172.16.60.254/24
set interfaces reth0 unit 65 vlan-id 65
set interfaces reth0 unit 65 family inet address 172.16.65.254/24
set interfaces reth0 unit 70 vlan-id 70
set interfaces reth0 unit 70 family inet address 172.16.70.254/24
set interfaces ge-0/0/4 gigether-options redundant-parent reth0
set interfaces ge-7/0/4 gigether-options redundant-parent reth0

set chassis cluster reth-count 4
set chassis cluster redundancy-group 0 node 0 priority 1
set chassis cluster redundancy-group 0 node 1 priority 100
set chassis cluster redundancy-group 1 node 0 priority 100
set chassis cluster redundancy-group 1 node 1 priority 1
set chassis cluster redundancy-group 1 preempt
set chassis cluster redundancy-group 1 interface-monitor ge-0/0/4 weight 255
set chassis cluster redundancy-group 1 interface-monitor ge-7/0/4 weight 255
set chassis cluster redundancy-group 2 node 0 priority 1
set chassis cluster redundancy-group 2 node 1 priority 100
set chassis cluster redundancy-group 2 preempt
set chassis cluster redundancy-group 3 node 0 priority 1
set chassis cluster redundancy-group 3 node 1 priority 100
set chassis cluster redundancy-group 3 preempt
```

Configure the RPM probe and the ip-monitoring policy:

```
set services rpm probe ping-9 test icmp probe-type icmp-ping
set services rpm probe ping-9 test icmp target address 12.34.56.78
set services rpm probe ping-9 test icmp probe-count 3
set services rpm probe ping-9 test icmp probe-interval 5
set services rpm probe ping-9 test icmp test-interval 15
set services rpm probe ping-9 test icmp thresholds successive-loss 3
set services rpm probe ping-9 test icmp thresholds total-loss 3
set services rpm probe ping-9 test icmp next-hop 80.1.1.9
set services rpm probe ping-13 test icmp probe-type icmp-ping
set services rpm probe ping-13 test icmp target address 12.34.56.78
set services rpm probe ping-13 test icmp probe-count 3
set services rpm probe ping-13 test icmp probe-interval 5
set services rpm probe ping-13 test icmp test-interval 15
set services rpm probe ping-13 test icmp thresholds successive-loss 3
set services rpm probe ping-13 test icmp thresholds total-loss 3
set services rpm probe ping-13 test icmp next-hop 80.1.1.13

set services ip-monitoring policy ping-9 match rpm-probe ping-9
set services ip-monitoring policy ping-9 then interface ge-0/0/3 disable
set services ip-monitoring policy ping-13 match rpm-probe ping-13
set services ip-monitoring policy ping-13 then interface ge-7/0/3 disable
```

Note: You cannot verify this step until the uplink interfaces towards the UNTRUST/ INTERNET are configured and the EBGP sessions are established.

© 2020 Juniper Networks, Inc. All rights reserved.

Xparent node:

Note: By adding the following configuration the XPARENT cluster is going to change from route to transparent mode. For this reason, a reboot is required.

```
set interfaces reth0 vlan-tagging
set interfaces reth0 redundant-ether-options redundancy-group 1
set interfaces reth0 unit 50 family ethernet-switching interface-mode trunk
set interfaces reth0 unit 50 family ethernet-switching vlan members vlan50
set interfaces reth0 unit 60 family ethernet-switching interface-mode trunk
set interfaces reth0 unit 60 family ethernet-switching vlan members vlan60
set interfaces reth0 unit 65 family ethernet-switching interface-mode trunk
set interfaces reth0 unit 65 family ethernet-switching vlan members vlan65
set interfaces reth0 unit 70 family ethernet-switching interface-mode trunk
set interfaces reth0 unit 70 family ethernet-switching vlan members vlan70
set interfaces reth1 vlan-tagging
set interfaces reth1 redundant-ether-options redundancy-group 1
set interfaces reth1 unit 50 family ethernet-switching interface-mode trunk
set interfaces reth1 unit 50 family ethernet-switching vlan members vlan50
set interfaces reth1 unit 60 family ethernet-switching interface-mode trunk
set interfaces reth1 unit 60 family ethernet-switching vlan members vlan60
set interfaces reth1 unit 65 family ethernet-switching interface-mode trunk
set interfaces reth1 unit 65 family ethernet-switching vlan members vlan65
set interfaces reth1 unit 65 family ethernet-switching vlan-rewrite translate 165 65
set interfaces reth1 unit 70 family ethernet-switching interface-mode trunk
set interfaces reth1 unit 70 family ethernet-switching vlan members vlan70
set interfaces reth1 unit 70 family ethernet-switching vlan-rewrite translate 170 70

set interfaces ge-0/0/3 gigether-options redundant-parent reth1
set interfaces ge-0/0/4 gigether-options redundant-parent reth0
set chassis cluster reth-count 2
set chassis cluster redundancy-group 0 node 0 priority 100
set chassis cluster redundancy-group 0 node 1 priority 1
set chassis cluster redundancy-group 1 node 0 priority 100
set chassis cluster redundancy-group 1 node 1 priority 1
set chassis cluster redundancy-group 1 interface-monitor ge-7/0/4 weight 255
set chassis cluster redundancy-group 1 interface-monitor ge-0/0/4 weight 255
set interfaces ge-7/0/4 gigether-options redundant-parent reth0
set vlans vlan50 vlan-id 50
set vlans vlan60 vlan-id 60
set vlans vlan65 vlan-id 65
set vlans vlan70 vlan-id 70

lab@srx5# commit
warning: Interfaces are changed from route mode to transparent mode. Please reboot the device
or all nodes in the HA cluster!
node0:
configuration check succeeds
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
node1:
warning: Interfaces are changed from route mode to transparent mode. Please reboot the device
or all nodes in the HA cluster!
commit complete
node0:
commit complete

lab@srx5# run request system reboot
Reboot the system ? [yes,no] (no) yes
```

7) Configure the management interfaces (figure 1) as defined in the table below:

Device	Management IP address
roffice1	10.10.1.1/24
roffice2	10.10.1.2/24
central-node0	10.10.1.3/24
central-node1	10.10.1.4/24
xparent-node0	10.10.1.5/24
xparent-node1	10.10.1.6/24
exa-fw	10.10.1.7/24
building	10.10.1.8/24

This task should not require any configuration for non-cluster devices as the management addresses are preconfigured in the initial configurations. This task is to ensure all management addresses are correctly configured.

8) Ensure the management interfaces (figure 1):
   a. Will accept only specific services as defined in the table below.

Device	Services
roffice1	SSH with root access (session limit 3), HTTPS
roffice2	SSH with root access (session limit 3), HTTPS
central	SSH with root access (session limit 3), HTTPS
xparent	SSH with root access (session limit 3), HTTPS
building	SSH with root access (session limit 3), HTTPS
exa-fw	SSH with root access (session limit 3), HTTPS

© 2020 Juniper Networks, Inc. All rights reserved.

All devices:

```
set system services ssh root-login allow
set system services ssh connection-limit 3
set system services web-management https system-generated-certificate
```

Verification

```
roffice1> telnet 10.10.1.2 port 22
Trying 10.10.1.2...
Connected to 10.10.1.2.
Escape character is '^]'.
SSH-2.0-OpenSSH_6.6

roffice1> telnet 10.10.1.2 port 443
Trying 10.10.1.2...
Connected to 10.10.1.2.
Escape character is '^]'.
```

Task 2: Initial Configuration – Part 2

In this part you will configure authentication, authorization, Syslog, SNMP and NTP parameters.

1) Configure users as defined in the table below:

Username	Password	Device	Privileges
ronly	ronly123	All	Has permission “view” and “view-configuration”. Additionally, can NOT execute the “file delete” command and view the [edit system login] configuration hierarchy.
admin1	admin123	All	Has permissions “all”. But is not allowed to reboot the device.
restricted	restricted123	All	Has permissions “clear” and can execute only the “show system users” and “show interface terse” commands and nothing else.
lab	lab123	All	super-user

© 2020 Juniper Networks, Inc. All rights reserved.

All devices:

```
set system login class admin permissions all
set system login class admin deny-commands "request system reboot"
set system login class restricted permissions clear
set system login class restricted allow-commands "(show system users)|(show interfaces terse)"
set system login class ronly permissions view
set system login class ronly permissions view-configuration
set system login class ronly deny-commands "file delete"
set system login class ronly deny-configuration "system login"
set system login user admin1 uid 2007
set system login user admin1 class admin
set system login user admin1 authentication encrypted-password
"$1$2Ufc.UpI$s/SmYOgJSv33V5HlhwOqO1"
set system login user lab uid 2009
set system login user lab class super-user
set system login user lab authentication encrypted-password
"$1$hfW4uwbb$C5GrqK6JMX/y2o54.1jWz0"
set system login user restricted uid 2010
set system login user restricted class restricted
set system login user restricted authentication encrypted-password
"$1$XuzfeAyb$PVeSVjo2Y5Jgc6WFh6Hhm."
set system login user ronly uid 2015
set system login user ronly class ronly
set system login user ronly authentication encrypted-password
"$1$JsllqvQw$a/vER20W/pfwUPGHAfdtT1"
```

2) Ensure that all devices have the following SYSLOG configuration:
    n. All “emergency” messages are displayed on terminals of all currently logged users.
    o. Only all “critical” and higher severity messages are sent to the default syslog file.
    p. “interactive-commands” file keeps the audit trail of the users and commands they execute.
    q. File named “security-policy-logs” will contain security policy log entries. The system should retain 20 archive files with size of 512 KB (524288 B).
    r. “authorization-file” stores authorization messages with the severity “info” and higher.
    s. Following messages are sent to the syslog server at 10.10.1.99.
        vii. All “emergency” messages
        viii. Authorization messages with severity “info” and higher

3) The syslog messages should contain year and milliseconds information.

All devices:

```
set system syslog user * any emergency
set system syslog host 10.10.1.99 any emergency
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
set system syslog host 10.10.1.99 authorization info
set system syslog file messages any critical
set system syslog file interactive-commands interactive-commands any
set system syslog file security-policy-logs user info
set system syslog file security-policy-logs match RT_FLOW
set system syslog file security-policy-logs archive size 512k
set system syslog file security-policy-logs archive files 20
set system syslog file authorization-file authorization any
set system syslog file ssl-proxy any any
set system syslog file ssl-proxy match SSL
set system syslog time-format year
set system syslog time-format millisecond
```

4) Ensure that all devices will synchronize their time with the NTP server reachable at 10.10.1.254.
5) The devices have to use this server's time also during booting.
6) The time zone is set to America/Los_Angeles.

```
set system ntp boot-server 10.10.1.254
set system ntp server 10.10.1.254
set system ntp trusted-key 1
set system time-zone America/Los_Angeles
```

7) All devices have to accept read-only SNMP requests only from the NMS system located at 10.10.1.20. The community string is "**roaccess**".
8) All devices have to send SNMP traps to the NMS system for following events:
    i. Authentication failures
    j. Hardware and environment
    k. Link transitions
    l. Routing protocol
9) The exa-fw device has to send the authentication failures to a specific monitoring system (10.10.10.50), which runs SNMP version 1 and listens on port 12345.
10) The devices should accept read-write SNMP requests from the network 10.10.199.0/24 except 10.10.199.199. The read-write community string is "snmpRWaccess".
11) All devices need to have defined following locations details:
    a. SNMP contact "**JNCIE admin**"
    b. SNMP description "**JNCIE-SEC device**"
    c. SNMP location "**Rack**"
    d. System location (not in the SNMP configuration): rack number **1**, floor **1**, country-code **US**.
12) Configure all vSRX devices to accept SNMP requests from Junos Space located at 10.10.1.121 using the community string "JNCIE"

© 2020 Juniper Networks, Inc. All rights reserved.

All devices:

```
set system location country-code US
set system location floor 1
set system location rack 1
set snmp description "JNCIE-SEC device"
set snmp location Rack
set snmp contact "JNCIE admin"
set snmp view all oid .1
set snmp community roaccess view all
set snmp community roaccess authorization read-only
set snmp community roaccess clients 10.10.1.20/32
set snmp community snmpRWaccess clients 10.10.199.0/24
set snmp community snmpRWaccess clients 10.10.199.199/32 restrict
set snmp community JNCIE
set snmp trap-group sl categories authentication
set snmp trap-group sl categories chassis
set snmp trap-group sl categories link
set snmp trap-group sl categories routing
set snmp trap-group sl categories chassis-cluster
set snmp trap-group sl targets 10.10.1.20
set snmp trap-group space targets 10.10.1.121
```

Task 3: Control Plane Protection

2) Firewall filters must protect all device's control planes in the way described below
    a. Where applicable ensure that any traffic originated from st0 and gr interfaces is accepted.
    b. Permit DNS, NTP, SNMP, HTTPS and SSH traffic originated from subnets 10/8, 172.16/16, 2016:abcd::/32 and loopback interfaces.
    c. Ensure that ICMPv4 traffic is rate limited to 256kbps with traffic burst of 100k.
    d. Discard and syslog traffic with the protocols from 'step 14.b' from all other networks.
    e. Allow and count any other traffic from exercises where a new term is required.

    f. Silently drop all other traffic.

Note: The firewall filter is a constant point of focus to bear in mind when troubleshooting is involved. Always make sure you update and evaluate your statement along with adding counters to traffic denial rules so that you understand if the firewall filter may be blocking interesting traffic.

© 2020 Juniper Networks, Inc. All rights reserved.

ROFFICE1:

```
[edit]
lab@roffice1# show policy-options prefix-list mgmt | no-more
10.0.0.0/8;
172.16.0.0/16;
192.168.1.1/32;

[edit]
lab@roffice1# show firewall | no-more
family inet {
    filter RE-PROTECT-v4 {
        term IFD {
            from {
                interface gr-0/0/0;
                interface st0;
            }
            then accept;
        }
        term PORT-TCP {
            from {
                source-prefix-list {
                    mgmt;
                }
                protocol tcp;
                destination-port [ https ssh ];
            }
            then accept;
        }
        term LOG-TCP {
            from {
                protocol tcp;
                destination-port [ https ssh ];
            }
            then {
                count LOG-TCP;
                discard;
            }
        }
        term ICMP {
            from {
                protocol icmp;
            }
            then {
                policer ICMP-POLICER;
                accept;
            }
        }
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
term SNMP {
    from {
        source-prefix-list {
            mgmt;
        }
        port [ snmp snmptrap ];
    }
    then {
        count SNMP;
        accept;
    }
}
term IKE {
    from {
        port 500;
    }
    then {
        count IKE;
        accept;
    }
}
term PORT-UDP {
    from {
        source-prefix-list {
            mgmt;
        }
        protocol udp;
        port [ domain ntp ];
    }
    then accept;
}
term LOG-UDP {
    from {
        protocol udp;
        port [ domain ntp ];
            }
            then {
                count LOG-UDP;
                discard;
            }
        }
    }
}
family inet6 {
    filter RE-PROTECT-v6 {
        term IFD {
            from {
                interface gr-0/0/0;
                interface st0;
            }
            then accept;
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
}
term SRC-ALLOW {
    from {
        source-address {
            2016:abcd::/32;
        }
        source-port [ domain ntp ];
    }
    then accept;
}
term SRC-DENY {
    from {
        source-port [ domain ntp ];
    }
    then count SRC-DENY;
}
term DST-ALLOW {
    from {
        source-address {
            2016:abcd::/32;
        }
        destination-port [ https ssh ];
    }
    then accept;
}
term DST-DENY {
    from {
        destination-port [ https ssh ];
    }
    then count DST-DENY;
}
term ICMP {
    from {
        icmp-type [ echo-reply echo-request destination-unreachable neighbor-
advertisement neighbor-solicit time-exceeded ];
    }
    then accept;
}
}
}
policer ICMP-POLICER {
    if-exceeding {
        bandwidth-limit 256k;
        burst-size-limit 100k;
    }
    then discard;
}

[edit]
lab@roffice1# show interfaces lo0 | no-more
unit 0 {
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
        family inet {
            filter {
                input RE-PROTECT-v4;
            }
            address 192.168.1.1/32;
        }
        family inet6 {
            filter {
                input RE-PROTECT-v6;
            }
            address 2016:abcd:ffff::2/128;
        }
    }
```

ROFFICE2:

```
[edit]
lab@roffice2# show policy-options prefix-list mgmt | no-more
10.0.0.0/8;
172.16.0.0/16;
192.168.1.2/32;

[edit]
lab@roffice2# show firewall | no-more
family inet {
    filter RE-PROTECT-v4 {
        term IFD {
            from {
                interface gr-0/0/0;
                interface st0;
            }
            then accept;
        }
        term PORT-TCP {
            from {
                source-prefix-list {
                    mgmt;
                }
                protocol tcp;
                destination-port [ https ssh ];
            }
            then accept;

        }
        term LOG-TCP {
            from {
                protocol tcp;
                destination-port [ https ssh ];
            }
            then {
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
            count LOG-TCP;
            discard;
        }
    }
    term ICMP {
        from {
            protocol icmp;
        }
        then {
            policer ICMP-POLICER;
            accept;
        }
    }
    term SNMP {
        from {
            source-prefix-list {
                mgmt;
            }
            port [ snmp snmptrap ];
        }
        then {
            count SNMP;
            accept;
        }
    }
    term IKE {
        from {
            port 500;
        }
        then {
            count IKE;
            accept;
        }
    }
    term PORT-UDP {
        from {
            source-prefix-list {
                mgmt;
            }
            protocol udp;
            port [ domain ntp ];
        }
        then accept;
    }
    term LOG-UDP {
        from {
            protocol udp;
            port [ domain ntp ];
        }
        then {
            count LOG-UDP;
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
                discard;
            }
        }
    }
}
family inet6 {
    filter RE-PROTECT-v6 {

        term IFD {
            from {
                interface gr-0/0/0;
                interface st0;
            }
            then accept;
        }
        term SRC-ALLOW {
            from {
                source-address {
                    2016:abcd::/32;
                }
                source-port [ domain ntp ];
            }
            then accept;
        }
        term SRC-DENY {
            from {
                source-port [ domain ntp ];
            }
            then count SRC-DENY;
        }
        term DST-ALLOW {
            from {
                source-address {
                    2016:abcd::/32;
                }
                destination-port [ https ssh ];
            }
            then accept;
        }
        term DST-DENY {
            from {
                destination-port [ https ssh ];
            }
            then count DST-DENY;
        }
        term ICMP {
            from {
                icmp-type [ echo-reply echo-request destination-unreachable neighbor-
advertisement neighbor-solicit time-exceeded ];
            }
            then accept;
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
        }
    }
}
policer ICMP-POLICER {
    if-exceeding {
        bandwidth-limit 256k;
        burst-size-limit 100k;
    }
    then discard;
}

[edit]
lab@roffice2# show interfaces lo0 | no-more
unit 0 {
    family inet {
        filter {
            input RE-PROTECT-v4;
        }
        address 192.168.1.2/32;
    }
    family inet6 {
        filter {
            input RE-PROTECT-v6;
        }
        address 2016:abcd:ffff::3/128;
    }
}
```

EXA:

```
[edit]
lab@exa-fw# show policy-options prefix-list mgmt | no-more
10.0.0.0/8;
172.16.0.0/16;
192.168.1.5/32;

[edit]
lab@exa-fw# show firewall | no-more
family inet {
    filter RE-PROTECT-v4 {
        term IFD {
            from {
                interface gr-0/0/0;
                interface st0;
            }
            then accept;
        }
        term PORT-TCP {
            from {
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
            source-prefix-list {
                mgmt;
            }
            protocol tcp;
            destination-port [ https ssh ];
        }
        then accept;
    }
    term LOG-TCP {
        from {
            protocol tcp;
            destination-port [ https ssh ];
        }
        then {
            count LOG-TCP;
            discard;
        }
    }
    term ICMP {
        from {
            protocol icmp;
        }
        then {
            policer ICMP-POLICER;
            accept;
        }
    }
    term SNMP {
        from {
            source-prefix-list {
                mgmt;
            }
            port [ snmp snmptrap ];
        }
        then {
            count SNMP;
            accept;
        }
    }
    term IKE {
        from {
            port 500;
        }
        then {
            count IKE;
            accept;
        }
    }
    term PORT-UDP {
        from {
            source-prefix-list {
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
            mgmt;
        }
        protocol udp;
        port [ domain ntp ];
    }
    then accept;
}
term LOG-UDP {
    from {
        protocol udp;
        port [ domain ntp ];
    }
    then {
        count LOG-UDP;
        discard;
    }
}
}
family inet6 {
    filter RE-PROTECT-v6 {
        term IFD {
            from {
                interface gr-0/0/0;
                interface st0;
            }
            then accept;
        }
        term SRC-ALLOW {
            from {
                source-address {
                    2016:abcd::/32;
                }
                source-port [ domain ntp ];
            }
            then accept;
        }
        term SRC-DENY {
            from {
                source-port [ domain ntp ];
            }
            then count SRC-DENY;
        }
        term DST-ALLOW {
            from {
                source-address {
                    2016:abcd::/32;
                }
                destination-port [ https ssh ];
            }
            then accept;
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
        }
        term DST-DENY {
            from {
                destination-port [ https ssh ];
            }
            then count DST-DENY;
        }
        term ICMP {
            from {
                icmp-type [ echo-reply echo-request destination-unreachable neighbor-
advertisement neighbor-solicit time-exceeded ];
            }
            then accept;
        }
    }
}
policer ICMP-POLICER {
    if-exceeding {
        bandwidth-limit 256k;
        burst-size-limit 100k;
    }
    then discard;
}

[edit]
lab@exa-fw# show interfaces lo0 | no-more
unit 0 {
    family inet {
        filter {
            input RE-PROTECT-v4;
        }
        address 192.168.1.5/32;
    }
    family inet6 {
        filter {
            input RE-PROTECT-v6;
        }
        address 2016:abcd:ffff::4/128;
    }
}
```

CENTRAL OFFICE:

```
{primary:node0}[edit]
lab@central-node0# show policy-options
prefix-list mgmt {
    10.0.0.0/8;
    80.1.1.16/32;
    172.16.0.0/16;
    192.168.1.3/32;
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
}
prefix-list bgp {
    apply-path "protocols bgp group <*> neighbor <*>";
}

{primary:node0}[edit]
lab@central-node0# show firewall | no-more
family inet {
    filter RE-PROTECT-v4 {
        term IFD {
            from {
                interface gr-0/0/0;
                interface st0;
            }
            then accept;
        }
        term PORT-TCP {
            from {
                source-prefix-list {
                    mgmt;
                }
                protocol tcp;
                destination-port [ https ssh ];
            }
            then accept;
        }
        term LOG-TCP {
            from {
                protocol tcp;
                destination-port [ https ssh ];
            }
            then {
                count LOG-TCP;
                discard;
            }
        }
        term ICMP {
            from {
                protocol icmp;
            }
            then {
                policer ICMP-POLICER;
                accept;
            }
        }
        term SNMP {
            from {
                source-prefix-list {
                    mgmt;
                }
                port [ snmp snmptrap ];
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
        }
        then {
            count SNMP;
            accept;
        }
    }
    term BGP {
        from {
            prefix-list {

                bgp;
            }
            protocol tcp;
            port bgp;
        }
        then {
            count BGP;
            accept;
        }
    }
    term OSPF {
        from {
            protocol ospf;
        }
        then {
            count OSPF;
            accept;
        }
    }
    term LDP {
        from {
            port ldp;
        }
        then {
            count LDP;
            accept;
        }
    }
    term IKE {
        from {
            port 500;
        }
        then {
            count IKE;
            accept;
        }
    }
    term PORT-UDP {
        from {
            source-prefix-list {
                mgmt;
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
            }
            protocol udp;
            port [ domain ntp ];
        }
        then accept;
    }
    term LOG-UDP {
        from {
            protocol udp;
            port [ domain ntp ];
        }
        then {
            count LOG-UDP;
            discard;
        }
    }
}
filter FBF-WEBSENSE {
    term http {
        from {
            protocol tcp;
            destination-port http;
        }
        then {
            routing-instance websense;
        }
    }
    term else {
        then accept;
    }
}
family inet6 {
    filter RE-PROTECT-v6 {
        term IFD {
            from {
                interface gr-0/0/0;
                interface st0;
            }
            then accept;
        }
        term SRC-ALLOW {
            from {
                source-address {
                    2016:abcd::/32;
                }
                source-port [ domain ntp ];
            }
            then accept;
        }
        term SRC-DENY {
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
        from {
            source-port [ domain ntp ];
        }
        then count SRC-DENY;
    }
    term DST-ALLOW {
        from {
            source-address {
                2016:abcd::/32;
            }
            destination-port [ https ssh ];
        }
        then accept;
    }
    term DST-DENY {
        from {
            destination-port [ https ssh ];
        }
        then count DST-DENY;
    }
    term BGP {
        from {
            prefix-list {
                bgp;
            }
            port bgp;
        }
        then {
            count BGP;
            accept;
        }
    }
    term ICMP {
        from {
            icmp-type [ echo-reply echo-request neighbor-advertisement neighbor-solicit ];
            }
            then {
                count ICMP;
                accept;
            }
        }
    }
}
policer ICMP-POLICER {
    if-exceeding {
        bandwidth-limit 256k;
        burst-size-limit 100k;
    }
    then discard;
}
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
{primary:node0}[edit]
lab@central-node0# show interfaces lo0 | no-more
unit 0 {
    family inet {
        inactive: filter {
            input RE-PROTECT-v4;
        }
        address 80.1.1.16/32 {
            primary;
        }
        address 192.168.1.3/32;
    }
    family inet6 {
        filter {
            input RE-PROTECT-v6;
        }
        address 2016:abcd:ffff::1/128;
    }
}
redundant-pseudo-interface-options {
    redundancy-group 3;
}
```

XPARENT:

```
{primary:node0}[edit]
lab@xparent-node0# show policy-options prefix-list mgmt | no-more
10.0.0.0/8;
172.16.0.0/16;

{primary:node0}[edit]
lab@xparent-node0# show firewall | no-more
family inet {
    filter RE-PROTECT-v4 {
        term IFD {
            from {
                interface gr-0/0/0;
                interface st0;
            }
            then accept;
        }
        term PORT-TCP {
            from {
                source-prefix-list {
                    mgmt;
                }
                protocol tcp;
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
        destination-port [ https ssh ];
    }
    then accept;
}
term LOG-TCP {
    from {
        protocol tcp;
        destination-port [ https ssh ];
    }
    then {
        count LOG-TCP;
        discard;
    }
}
term ICMP {
    from {
        protocol icmp;
    }
    then {
        policer ICMP-POLICER;
        accept;
    }
}
term SNMP {
    from {
        source-prefix-list {
            mgmt;
        }
        port [ snmp snmptrap ];
    }
    then {
        count SNMP;
        accept;
    }
}
term PORT-UDP {
    from {
        source-prefix-list {
            mgmt;
        }
        protocol udp;
        port [ domain ntp ];
    }
    then accept;
}
term LOG-UDP {
    from {
        protocol udp;
        port [ domain ntp ];
    }
    then {
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
                count LOG-UDP;
                discard;
            }
        }
    }
}
family inet6 {
    filter RE-PROTECT-v6 {
        term IFD {
            from {
                interface gr-0/0/0;
                interface st0;
            }
            then accept;
        }
        term SRC-ALLOW {
            from {
                source-address {
                    2016:abcd::/32;
                }
                source-port [ domain ntp ];
            }
            then accept;
        }
        term SRC-DENY {
            from {
                source-port [ domain ntp ];
            }
            then count SRC-DENY;
        }
        term DST-ALLOW {
            from {
                source-address {
                    2016:abcd::/32;
                }
                destination-port [ https ssh ];
            }
            then accept;
        }
        term DST-DENY {
            from {
                destination-port [ https ssh ];
            }
            then count DST-DENY;
        }
    }
}
policer ICMP-POLICER {
    if-exceeding {
        bandwidth-limit 256k;
        burst-size-limit 100k;
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
    }
    then discard;
}

{primary:node0}[edit]
lab@xparent-node0# show interfaces lo0 | no-more
unit 0 {
    family inet {
        filter {
            input RE-PROTECT-v4;
        }
    }
    family inet6 {
        filter {
            input RE-PROTECT-v6;
        }
    }
}
```

BUILDING:

```
[edit]
lab@building# show policy-options prefix-list mgmt | no-more
10.0.0.0/8;
172.16.0.0/16;

[edit]
lab@building# show firewall | no-more
show interfaces lo0 | no-more
family inet {
    filter RE-PROTECT-v4 {
        term IFD {
            from {
                interface st0;
            }
            then accept;
        }
        term PORT-TCP {
            from {
                source-prefix-list {
                    mgmt;
                }
                protocol tcp;
                destination-port [ https ssh ];
            }
            then accept;
        }
        term LOG-TCP {
            from {
                protocol tcp;
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
            destination-port [ https ssh ];
        }
        then {
            count LOG-TCP;
            discard;
        }
    }
    term ICMP {
        from {
            protocol icmp;
        }
        then {
            policer ICMP-POLICER;
            accept;
        }
    }
    term SNMP {
        from {
            source-prefix-list {
                mgmt;
            }
            port [ snmp snmptrap ];
        }
        then {
            count SNMP;
            accept;
        }
    }
    term PORT-UDP {
        from {
            source-prefix-list {
                mgmt;
            }
            protocol udp;
            port [ domain ntp ];
            }
            then accept;
        }
        term LOG-UDP {
            from {
                protocol udp;
                port [ domain ntp ];
            }
            then {
                count LOG-UDP;
                discard;
            }
        }
    }
}
policer ICMP-POLICER {
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
    if-exceeding {
        bandwidth-limit 256k;
        burst-size-limit 100k;
    }
    then discard;
}

[edit]
lab@building# show interfaces lo0 | no-more
unit 0 {
    family inet {
        filter {
            input RE-PROTECT-v4;
        }
    }
}
unit 1 {
    family inet {
        address 192.168.1.6/32;
    }
}
unit 2 {
    family inet {
        address 192.168.1.7/32;
    }
}
```

Task 4: Interfaces, Zones, Local Traffic, and Routing

This part is focused on the interfaces, security zones, local traffic handling, routing, routing instance segregation and device operation configurations

1) Configure interfaces and security zones on individual devices as follows (the table is based on the figure 2):

Device	Interface	IP address	VLAN-ID	Zone
roffice1	lo0.0	192.168.1.1/32	-	UNTRUST
roffice1	ge-0/0/3	80.1.1.1/30	-	UNTRUST
roffice1	ge-0/0/4	172.16.10.254/24	-	TRUST-RO1
roffice1	ge-0/0/5	172.16.11.254/24	-	PRIVATE-RO1
roffice2	lo0.0	192.168.1.2/32	-	UNTRUST
roffice2	ge-0/0/3	80.1.1.5/30	-	UNTRUST
roffice2	ge-0/0/4	172.16.20.254/24	-	TRUST-RO2

© 2020 Juniper Networks, Inc. All rights reserved.

roffice2	ge-0/0/5	172.16.21.254/24	-	DMZ-RO2
central	lo0.0	192.168.1.3/32, 80.1.1.16/32	-	UNTRUST
central	ge-0/0/3	80.1.1.10/30	-	UNTRUST
central	ge-7/0/3	80.1.1.14/30	-	UNTRUST
central	reth0.50	172.16.50.254/24	50	TRUST
central	reth0.55	172.16.55.254/24	55	INTERNAL
central	reth0.60	172.16.60.254/24	60	WAREHOUSE
central	reth0.65	172.16.65.254/24	65	TESTBED
central	reth0.70	172.16.70.254/24	70	TESTBED
xparent	reth0.50	-	50	TRUST
xparent	reth0.60	-	60	WAREHOUSE
xparent	reth0.65	-	65	TESTBED
xparent	reth0.70	-	70	TESTBED
xparent	reth1.50	-	50	TRUST
xparent	reth1.60	-	60	WAREHOUSE
xparent	reth1.65	-	65	TESTBED
xparent	reth1.70	-	70	TESTBED
building1	lo0.1	192.168.1.6/32	-	INTERNAL-B1
building1	ge-0/0/3.100	172.16.100.254/24	100	TRUST-B1
building1	ge-0/0/3.101	172.16.101.254/24	101	DMZ-B1
building1	ge-0/0/4.55	172.16.55.1/24	55	INTERNAL-B1
building2	lo0.2	192.168.1.7/32	-	INTERNAL-B2
building2	ge-0/0/3.200	172.16.200.254/24	200	TRUST-B2
building2	ge-0/0/3.201	172.16.201.254/24	201	DMZ-B2
building2	ge-0/0/5.55	172.16.55.2/24	55	INTERNAL-B2
exa-fw	lo0.0	192.168.1.8/32	-	UNTRUST
exa-fw	ge-0/0/3	100.1.1.1/29	-	UNTRUST
exa-fw	ge-0/0/4	172.16.10.254/24	-	TRUST-EXA
exa-fw	ge-0/0/5.15	172.16.15.254/24	15	PRIVATE-EXA
exa-fw	ge-0/0/5.30	172.16.30.254/24	30	DMZ-EXA

© 2020 Juniper Networks, Inc. All rights reserved.

2) Ping to the security devices themselves must be allowed on all interfaces.
3) SSH connections are accepted on all TRUST zone interfaces.
4) On the devices roffice1, roffice2 and exa-fw create a default static route pointing to the UNTRUST network.
5) Use static routes on central cluster to provide connectivity to building's networks
6) On the building device (srx8) create two virtual-router routing-instances named building1 and building2, associate the interfaces of each building accordingly and create a default static route pointing to the correct VLAN interface on the central cluster.
7) Configure VLAN rewriting rules on xparent device:
    a. Interface reth1 – vlan-id 165 to vlan-id 65
    b. Interface reth1 – vlan-id 170 to vlan-id 70

Roffice1:

```
set interfaces ge-0/0/3 unit 0 family inet address 80.1.1.1/30
set interfaces ge-0/0/4 vlan-tagging
set interfaces ge-0/0/4 unit 0 vlan-id 110
set interfaces ge-0/0/4 unit 0 family inet address 172.16.10.254/24
set interfaces ge-0/0/4 unit 0 family inet6 address 2016:abcd:b1::254/64
set interfaces ge-0/0/5 vlan-tagging
set interfaces ge-0/0/5 unit 0 vlan-id 111
set interfaces ge-0/0/5 unit 0 family inet address 172.16.11.254/24
set interfaces ge-0/0/5 unit 0 family inet6 address 2016:abcd:b2::254/64
set interfaces fxp0 unit 0 family inet address 10.10.1.1/24
set interfaces lo0 unit 0 family inet filter input RE-PROTECT-v4
set interfaces lo0 unit 0 family inet address 192.168.1.1/32
set interfaces lo0 unit 0 family inet6 filter input RE-PROTECT-v6
set interfaces lo0 unit 0 family inet6 address 2016:abcd:ffff::2/128
```

```
set security zones security-zone UNTRUST host-inbound-traffic system-services ping
set security zones security-zone UNTRUST interfaces ge-0/0/3.0
set security zones security-zone UNTRUST interfaces lo0.0
set security zones security-zone TRUST-RO1 host-inbound-traffic system-services ping
set security zones security-zone TRUST-RO1 host-inbound-traffic system-services ssh
set security zones security-zone TRUST-RO1 interfaces ge-0/0/4.0
set security zones security-zone PRIVATE-RO1 host-inbound-traffic system-services ping
set security zones security-zone PRIVATE-RO1 interfaces ge-0/0/5.0
```

Roffice2:

```
set security zones security-zone UNTRUST host-inbound-traffic system-services ping
set security zones security-zone UNTRUST host-inbound-traffic system-services ike
set security zones security-zone UNTRUST interfaces lo0.0
set security zones security-zone UNTRUST interfaces ge-0/0/3.0
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
set security zones security-zone TRUST-RO2 host-inbound-traffic system-services ping
set security zones security-zone TRUST-RO2 host-inbound-traffic system-services ssh
set security zones security-zone TRUST-RO2 interfaces ge-0/0/4.0
set security zones security-zone DMZ-RO2 host-inbound-traffic system-services ping
set security zones security-zone DMZ-RO2 interfaces ge-0/0/5.0
set interfaces ge-0/0/3 unit 0 family inet address 80.1.1.5/30
set interfaces ge-0/0/4 vlan-tagging
set interfaces ge-0/0/4 unit 0 vlan-id 210
set interfaces ge-0/0/4 unit 0 family inet address 172.16.20.254/24
set interfaces ge-0/0/5 vlan-tagging
set interfaces ge-0/0/5 unit 0 vlan-id 211
set interfaces ge-0/0/5 unit 0 family inet address 172.16.21.254/24
set interfaces fxp0 unit 0 family inet address 10.10.1.2/24
set interfaces lo0 unit 0 family inet filter input RE-PROTECT-v4
set interfaces lo0 unit 0 family inet address 192.168.1.2/32
```

Central-node:

```
set interfaces ge-0/0/3 unit 0 family inet address 80.1.1.10/30
set interfaces ge-7/0/3 unit 0 family inet address 80.1.1.14/30
set interfaces reth2 redundant-ether-options redundancy-group 2
set interfaces reth2 unit 0 family inet address 172.16.255.0/31
set interfaces reth3 redundant-ether-options redundancy-group 2
set interfaces reth3 unit 0 family inet address 172.16.255.1/31
set security zones security-zone UNTRUST host-inbound-traffic system-services ping
set security zones security-zone UNTRUST host-inbound-traffic protocols bgp
set security zones security-zone UNTRUST interfaces lo0.0 host-inbound-traffic system-services
ike
set security zones security-zone UNTRUST interfaces lo0.0 host-inbound-traffic protocols ldp
set security zones security-zone UNTRUST interfaces lo0.0 host-inbound-traffic protocols bgp
set security zones security-zone UNTRUST interfaces ge-0/0/3.0
set security zones security-zone UNTRUST interfaces ge-7/0/3.0
set security zones security-zone TRUST host-inbound-traffic system-services ping
set security zones security-zone TRUST host-inbound-traffic system-services ssh
set security zones security-zone TRUST interfaces reth0.50
set security zones security-zone TRUST application-tracking
set security zones security-zone INTERNAL host-inbound-traffic system-services ping
set security zones security-zone INTERNAL interfaces reth0.55
set security zones security-zone WAREHOUSE host-inbound-traffic system-services ping
set security zones security-zone WAREHOUSE interfaces reth0.60
set security zones security-zone WAREHOUSE interfaces reth3.0
set security zones security-zone TESTBED host-inbound-traffic system-services ping
set security zones security-zone TESTBED interfaces reth0.65
set security zones security-zone TESTBED interfaces reth0.70
```

XPARENT:

```
set security zones security-zone WAREHOUSE interfaces reth1.60
set security zones security-zone WAREHOUSE interfaces reth0.60
set security zones security-zone TRUST interfaces reth0.50
set security zones security-zone TRUST interfaces reth1.50
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
set security zones security-zone TESTBED interfaces reth1.65
set security zones security-zone TESTBED interfaces reth1.70
set security zones security-zone TESTBED interfaces reth0.65
set security zones security-zone TESTBED interfaces reth0.70
```

EXA:

```
set security zones security-zone UNTRUST host-inbound-traffic system-services ping
set security zones security-zone UNTRUST interfaces lo0.0
set security zones security-zone UNTRUST interfaces ge-0/0/3.0
set security zones security-zone TRUST-EXA host-inbound-traffic system-services ping
set security zones security-zone TRUST-EXA host-inbound-traffic system-services ssh
set security zones security-zone TRUST-EXA interfaces ge-0/0/4.0
set security zones security-zone PRIVATE-EXA host-inbound-traffic system-services ping
set security zones security-zone PRIVATE-EXA interfaces ge-0/0/5.15
set security zones security-zone DMZ-EXA host-inbound-traffic system-services ping
set security zones security-zone DMZ-EXA interfaces ge-0/0/5.30
set interfaces ge-0/0/3 unit 0 family inet address 100.1.1.1/29
set interfaces ge-0/0/4 unit 0 family inet address 172.16.10.254/24
set interfaces ge-0/0/4 unit 0 family inet6 address 2016:abcd:d1::254/64
set interfaces ge-0/0/5 vlan-tagging
set interfaces ge-0/0/5 unit 15 vlan-id 15
set interfaces ge-0/0/5 unit 15 family inet address 172.16.15.254/24
set interfaces ge-0/0/5 unit 15 family inet6 address 2016:abcd:d2::254/64
set interfaces ge-0/0/5 unit 30 vlan-id 30
set interfaces ge-0/0/5 unit 30 family inet address 172.16.30.254/24
set interfaces fxp0 unit 0 family inet address 10.10.1.7/24
set interfaces lo0 unit 0 family inet filter input RE-PROTECT-v4
set interfaces lo0 unit 0 family inet address 192.168.1.5/32
```

BUILDING:

```
set interfaces ge-0/0/3 vlan-tagging
set interfaces ge-0/0/3 unit 100 vlan-id 100
set interfaces ge-0/0/3 unit 100 family inet address 172.16.100.254/24
set interfaces ge-0/0/3 unit 101 vlan-id 101
set interfaces ge-0/0/3 unit 101 family inet address 172.16.101.254/24
set interfaces ge-0/0/3 unit 200 vlan-id 200
set interfaces ge-0/0/3 unit 200 family inet address 172.16.200.254/24
set interfaces ge-0/0/3 unit 201 vlan-id 201
set interfaces ge-0/0/3 unit 201 family inet address 172.16.201.254/24
set interfaces ge-0/0/4 vlan-tagging
set interfaces ge-0/0/4 unit 55 vlan-id 55
set interfaces ge-0/0/4 unit 55 family inet address 172.16.55.1/24
set interfaces ge-0/0/5 vlan-tagging
set interfaces ge-0/0/5 unit 55 vlan-id 55
set interfaces ge-0/0/5 unit 55 family inet address 172.16.55.2/24
set interfaces lo0 unit 1 family inet address 192.168.1.6/32
set interfaces lo0 unit 2 family inet address 192.168.1.7/32
set interfaces lo0 unit 0 family inet filter input RE-PROTECT-v4
set security zones security-zone INTERNAL-B1 host-inbound-traffic system-services ping
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
set security zones security-zone INTERNAL-B1 interfaces ge-0/0/4.55
set security zones security-zone INTERNAL-B1 interfaces lo0.1
set security zones security-zone TRUST-B1 host-inbound-traffic system-services ping
set security zones security-zone TRUST-B1 host-inbound-traffic system-services ssh
set security zones security-zone TRUST-B1 interfaces ge-0/0/3.100
set security zones security-zone DMZ-B1 host-inbound-traffic system-services ping
set security zones security-zone DMZ-B1 interfaces ge-0/0/3.101
set security zones security-zone INTERNAL-B2 host-inbound-traffic system-services ping
set security zones security-zone INTERNAL-B2 interfaces lo0.2
set security zones security-zone INTERNAL-B2 interfaces ge-0/0/5.55
set security zones security-zone TRUST-B2 host-inbound-traffic system-services ping
set security zones security-zone TRUST-B2 host-inbound-traffic system-services ssh
set security zones security-zone TRUST-B2 interfaces ge-0/0/3.200
set security zones security-zone DMZ-B2 host-inbound-traffic system-services ping
set security zones security-zone DMZ-B2 interfaces ge-0/0/3.201
set routing-instances building1 instance-type virtual-router
set routing-instances building1 interface ge-0/0/3.100
set routing-instances building1 interface ge-0/0/3.101
set routing-instances building1 interface ge-0/0/4.55
set routing-instances building1 interface lo0.1
set routing-instances building1 routing-options static route 0.0.0.0/0 next-hop 172.16.55.254
set routing-instances building2 instance-type virtual-router
set routing-instances building2 interface ge-0/0/3.200
set routing-instances building2 interface ge-0/0/3.201
set routing-instances building2 interface ge-0/0/5.55
set routing-instances building2 interface lo0.2
set routing-instances building2 routing-options static route 0.0.0.0/0 next-hop 172.16.55.254
```

BGP Overview:

Border Gateway Protocol version 4 (BGP-4) is a path vector protocol as defined in RFC4271 . Routing loops are detected and avoided by a device checking its own path number (Autonomous System Number - ASN) in the message received from a neighbor. Although in-depth understand of BGP is out of scope of the syllabus, you should understand key elements to successfully configure the devices and how to best steer network traffic using BGP.

BGP uses TCP for session establishment and reserved port number 179.

The following table identifies the states of BGP peering and their meaning:

State	Description
Idle	Initial state when all incoming BGP connections are refused. A start event is required for the local system to initialize BGP resources and prepare for a transport connection with the other BGP peer.
Connect	BGP is waiting for the transport protocol connection to be completed. If the transport protocol connection succeeds, the local system sends

© 2020 Juniper Networks, Inc. All rights reserved.

	an OPEN message and transitions to the OpenSent state. If the transport protocol connection fails, the local system restarts the ConnectRetryTimer, listens for a connection initiated by the remote BGP peer, and changes its state to Active.
Active	BGP is trying to acquire a peer by initiating a transport protocol connection. If the transport protocol connection succeeds, the local system sends an OPEN message to its peer and transitions to the OpenSent state. If the local system's BGP state remains in the Active state, you should check physical connectivity as well as the configuration on both peers.
OpenSent	BGP waits for an OPEN message from its peer. When an OPEN message is received, it is checked and verified to ensure that no errors exist. If an error is detected, the system transitions back to the Idle state. If no errors are detected, BGP sends a Keepalive message
OpenConfirm	BGP waits for a KEEPALIVE or NOTIFICATION message. If no KEEPALIVE message is received before the negotiated hold timer expires, the local system sends a NOTIFICATION message stating that the hold timer has expired and changes its state to Idle. Likewise, if the local system receives a NOTIFICATION message, it changes its state to Idle. If the local system receives a KEEPALIVE message, it changes its state to Established.
Established	BGP can exchange UPDATE, NOTIFICATION, and KEEPALIVE messages with its peer. When the local system receives an UPDATE or KEEPALIVE message and when the negotiated holdtimer value is nonzero, it restarts its hold timer. If the negotiated hold timer reaches zero, the local system sends out a KEEPALIVE message and restarts the hold timer.

BGP works with the concept of attributes. The following table identifies their types:

Type	Description
Well-known mandatory	Must be supported by all BGP implementations and must be included in every BGP update
Well-known discretionary	Must be supported in all BGP implementations, but do not have to be included in every BGP update
Optional transitive	Not required to be supported by all BGP

© 2020 Juniper Networks, Inc. All rights reserved.

	implementations but, if they are, they should be passed along, unchanged, to other BGP peers
Optional non-transitive	Not required to be supported by all BGP implementations. If an optional nontransitive attribute is not recognized, it is ignored and not passed to other peers

Well known mandatory attributes include AS_PATH which means that we must identify our local autonomous system number, the NEXT-HOP which identifies the peer to send the destination traffic and the ORIGIN that identifies if it is coming from an EBGP peer (E), the IGP (I) or unknown source also known as incomplete (?).

Well known discretionary attributes include LOCAL-PREFERENCE and this allows us to select a specific neighbor over two equal cost prefixes whenever such option exists.

A few rules to bear in mind about BGP are how information advertisement works. This is fundamental to prevents routing loops.

4. IBGP peers advertise routes received from EBGP peers to other IBGP peers
5. EBGP peers advertise routes learned from IBGP or EBGP peers to other EBGP peers
6. IBGP peers do not advertise routes received from IBGP peers to other IBGP peers

© 2020 Juniper Networks, Inc. All rights reserved.

BGP stores its information in internal routing tables. These are called Routing Information Base (RIB) and there are 3 types of RIBs:

Type	Description
RIB-In	BGP routing information as it was received from the specified BGP neighbor and before any import policy processing occurs.
RIB-local	Only active routes are installed in this table and are used by the device. These are the prefixes after the import policy processing occurs.
RIB-Out	The information reflects the routes that the routing table exported into the routing protocol, along with any attributes that have been attached. This is after the export policy processing occurs.

Another key element of BGP is its path selection algorithm. Verify that the next hop can be resolved

5. For BGP, prefer the path with higher local preference
6. For BGP, prefer the path with the shortest autonomous system (AS) path value
7. Prefer strictly external BGP (EBGP) paths over external paths learned through internal BGP (IBGP) sessions, over incomplete E > I > ?
8. A path is considered a BGP equal-cost path (and will be used for forwarding) when paths are learned by a multipath-enabled BGP neighbor within the same neighboring AS

© 2020 Juniper Networks, Inc. All rights reserved.

Note: The central cluster supports multi-homing from two distinct addresses in the local device to neighboring peers. Equal cost multi path (ECMP) exists for received prefixes so we need local preference manipulation to select the next hop we desire to send traffic to and AS path manipulation for the peer to understand which is the least preferred neighbor to send traffic to.

BGP does not advertise any prefix by default so we need to advertise the company's owned prefix 80.1.1.0/24 which does not exist and needs to be created as an aggregate route

8) Configure ipv4 BGP sessions between the central device to both external neighboring addresses or the Internet transit provider ASN 4321
    a. Advertise the company owned prefix 80.1.1.0/24 making sure BGP prefixes do not participate in the aggregation process.
    b. Make sure your preferred entry and exit point for general Internet connectivity is node0.

```
{primary:node0}[edit]
lab@central-node0# show policy-options
policy-statement from-bgp13 {
    term default {
        from {
            protocol bgp;
            route-filter 0.0.0.0/0 exact;
        }
        then accept;
    }
    term specific {
        from {
            protocol bgp;
            route-filter 0.0.0.0/0 longer;
        }
        then {
            local-preference 200;
            accept;
        }
    }
}
policy-statement from-bgp9 {
    term default {
        from {
            protocol bgp;
            route-filter 0.0.0.0/0 exact;
        }
        then {
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
            local-preference 200;
            accept;
        }
    }
    term specific {
        from {
            protocol bgp;
            route-filter 0.0.0.0/0 longer;
        }
        then accept;
    }
}
policy-statement no-bgp {
    term bgp {
        from protocol bgp;
        then reject;
    }
    term else {
        then accept;
    }
}
policy-statement to-bgp13 {
    term company {
        from {
            protocol aggregate;
            route-filter 80.1.1.0/24 exact;
        }
        then {
            as-path-prepend "1234 1234";
            accept;
        }
    }
    term lo0 {
        from {
            interface lo0.0;
            route-filter 80.1.1.16/32 exact;
        }
        then accept;
    }
}
policy-statement to-bgp9 {
    term company {
        from {
            protocol aggregate;
            route-filter 80.1.1.0/24 exact;
        }
        then accept;
    }
    term lo0 {
        from {
            interface lo0.0;
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
            route-filter 80.1.1.16/32 exact;
        }
        then {
            as-path-prepend "1234 1234";
            accept;
        }
    }
}

{primary:node0}[edit]
lab@central-node0# show routing-options
aggregate {
    route 80.1.1.0/24 policy no-bgp;
}
autonomous-system 1234;


{primary:node0}[edit]
lab@central-node0# show protocols bgp
group untrust-v4 {
    type external;
    peer-as 4321;
    neighbor 80.1.1.9 {
        import from-bgp9;
        export to-bgp9;
    }
    neighbor 80.1.1.13 {
        import from-bgp13;
        export to-bgp13;
    }
}

{primary:node0}[edit]
lab@central-node0# run show bgp summary
Groups: 2 Peers: 2 Down peers: 0
Table            Tot Paths  Act Paths Suppressed    History Damp State    Pending
inet.0
                        10          5          0          0          0          0
Peer                     AS      InPkt     OutPkt    OutQ   Flaps Last Up/Dwn
State|#Active/Received/Accepted/Damped...
80.1.1.9               4321          6          4       0       0           3 1/5/5/0
0/0/0/0
80.1.1.13              4321          5          4       0       0           6 4/5/5/0
0/0/0/0

{primary:node0}[edit]
lab@central-node0# run show route advertising-protocol bgp 80.1.1.9
inet.0: 25 destinations, 30 routes (25 active, 0 holddown, 0 hidden)
  Prefix                  Nexthop              MED     Lclpref    AS path
* 80.1.1.0/24             Self                                    I
* 80.1.1.16/32            Self                                    1234 1234 [1234] I
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
{primary:node0}[edit]
lab@central-node0# run show route advertising-protocol bgp 80.1.1.13
inet.0: 25 destinations, 30 routes (25 active, 0 holddown, 0 hidden)
  Prefix                  Nexthop              MED     Lclpref    AS path
* 80.1.1.0/24             Self                                    1234 1234 [1234] I
* 80.1.1.16/32            Self                                    I

{primary:node0}[edit]
lab@central-node0# run show route receive-protocol bgp 80.1.1.9
inet.0: 25 destinations, 30 routes (25 active, 0 holddown, 0 hidden)
  Prefix                  Nexthop              MED     Lclpref    AS path
* 0.0.0.0/0               80.1.1.9                                4321 I
  80.1.1.0/30             80.1.1.9                                4321 I
  80.1.1.4/30             80.1.1.9                                4321 I
  100.0.0.0/8             80.1.1.9                                4321 I
  200.0.0.0/8             80.1.1.9                                4321 I
inet6.0: 10 destinations, 10 routes (10 active, 0 holddown, 0 hidden)

{primary:node0}[edit]
lab@central-node0# run show route receive-protocol bgp 80.1.1.13
inet.0: 25 destinations, 30 routes (25 active, 0 holddown, 0 hidden)
  Prefix                  Nexthop              MED     Lclpref    AS path
  0.0.0.0/0               80.1.1.13                               4321 I
* 80.1.1.0/30             80.1.1.13                               4321 I
* 80.1.1.4/30             80.1.1.13                               4321 I
* 100.0.0.0/8             80.1.1.13                               4321 I
* 200.0.0.0/8             80.1.1.13                               4321 I
```

Task 5: UTM

1) Antivirus scanning has to be done in the Remote office 1 and Remote office 2. Configure the security devices to perform antivirus scanning according to the following requirements:

   a. Only HTTP and FTP traffic from the correspondent TRUST zones to the UNTRUST network will be scanned
   b. Full-file based scanning is done and all files and file extensions are scanned
   c. The device checks every 90 minutes for antivirus database updates
   d. The HTTP traffic to www.internalsites.com prefix and audio mime type are excluded from antivirus scan.
   e. Compressed files are scanned up to the 3rd compression level. Files having more compression levels are dropped.
   f. Intelligent prescreening has to be enabled.
   g. The clients have to receive every 40 seconds a small portion of unchecked data to avoid timeout.

© 2020 Juniper Networks, Inc. All rights reserved.

h. The scanning engine timeout is set to 5 minutes.
i. All fallback options are set to block except default and too-many-requests.
j. The virus notification message is “Virus detected!”
k. The fallback notifications are:
    i. BLOCK – “AV blocked the traffic as it was not able to scan it!”

Roffice1:

```
[edit]
lab@roffice1# show security utm
custom-objects {
    mime-pattern {
        AV-excluded-mime {
            value audio/;
        }
    }
    url-pattern {
        company-site {
            value www.internalsites.com;
        }
    }
    custom-url-category {
        AV-excluded-sites {
            value company-site;
        }
    }
}
feature-profile {
    anti-virus {
        mime-whitelist {
            list AV-excluded-mime;
        }
        url-whitelist AV-excluded-sites;
        type sophos-engine;
        sophos-engine {
            profile AV-full-file-scan {
                notification-options {
                    virus-detection {
                        type message;
                    }
                }
            }
        }
    }
}
utm-policy RO-AV {
    anti-virus {
        http-profile AV-full-file-scan;
        ftp {
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
            upload-profile AV-full-file-scan;
            download-profile AV-full-file-scan;
        }
    }
}

[edit]
lab@roffice1# show security policies
from-zone TRUST-RO1 to-zone UNTRUST {
    policy HTTP-FTP {
        match {
            source-address RO1-TRUST;
            destination-address any;
            application [ junos-http junos-ftp ];
        }
        then {
            permit {
                application-services {
                    utm-policy RO-AV;
                }
            }
        }
    }
}
```

Roffice2:

```
[edit]
lab@roffice2# show security utm
custom-objects {
    mime-pattern {
        AV-excluded-mime {
            value audio/;
        }
    }
    url-pattern {
        company-site {
            value www.internalsites.com;
        }
    }
    custom-url-category {
        AV-excluded-sites {
            value company-site;
        }
    }
}
feature-profile {
    anti-virus {
        mime-whitelist {
            list AV-excluded-mime;
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
}
url-whitelist AV-excluded-sites;
sophos-engine {
    profile AV-full-file-scan {
        fallback-options {
            default block;
            content-size block;
            engine-not-ready block;
            timeout block;
            out-of-resources block;
            too-many-requests log-and-permit;
        }
        scan-options {
            timeout 300;
        }
        trickling timeout 40;
        notification-options {
            virus-detection {
                type message;
                custom-message "Virus detected!";
            }
            fallback-block {
                type message;
                custom-message "AV blocked the traffic as it was not able to scan
it!";
            }
        }
    }
}
utm-policy RO-AV {
    anti-virus {
        http-profile AV-full-file-scan;
        ftp {
            upload-profile AV-full-file-scan;
            download-profile AV-full-file-scan;
        }
    }
}

[edit]
lab@roffice2# show security policies
from-zone TRUST-RO2 to-zone UNTRUST {
    policy HTTP-FTP {
        match {
            source-address RO2-TRUST;
            destination-address any;
            application [ junos-http junos-ftp ];
        }
        then {
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
            permit {
                application-services {
                    utm-policy RO-AV;
                }
            }
        }
    }
}
```

2) The exa-fw device enforces local web-filtering according the requirements below:
    a. The web filtering is done on HTTP connections from the TRUST-EXA zone to the Internet.
    b. The following URLs are denied
        i. www.facebook.com
        ii. www.twitter.com
        iii. www.youtube.com
    c. The clients receive the “This site is not allowed” message in case their request was blocked.
    d. The local engine timeout is set to 10 minutes.
    e. All fallback options except default option block the requests.

```
[edit]
lab@exa-fw# show security utm
custom-objects {
    url-pattern {
        denied-sites {
            value [ http://www.facebook.com http://www.twitter.com http://www.www.youtube.com
];
        }
    }
    custom-url-category {
        denied-sites-category {
            value denied-sites;
        }
    }
}
feature-profile {
    web-filtering {
        url-blacklist denied-sites-category;
        type juniper-local;
        juniper-local {
            profile Web-filtering {
                default permit;
                custom-block-message "This site is not allowed!";
                fallback-settings {
                    default block;
                    timeout block;
                    too-many-requests block;
                }
                timeout 600;
            }
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
        }
    }
}
utm-policy EXA-WebFilter {
    web-filtering {
        http-profile Web-filtering;
    }
}

[edit]
lab@exa-fw# show security policies
from-zone TRUST-EXA to-zone UNTRUST {
    policy HTTP {
        match {
            source-address EXA-TRUST;
            destination-address any;
            application junos-http;
        }
        then {
            permit {
                application-services {
                    utm-policy EXA-WebFilter;
                }
            }
        }
    }
}
```

3) In the central office the HTTP and FTP traffic from the TRUST zone to the Internet leaving through the cluster needs to be processed in following manner:
    a. The content handling is:
        i. Cookies and java-applets are blocked
        ii. “bat” and “sh” files are blocked
        iii. The engine generates protocol error “Firewall blocked this content!” once traffic is blocked
4) The company’s email server (172.16.60.199) located in the WAREHOUSE zone behind the XPARENT cluster has to be protected from these outside spammers from the Internet
    a. IP addresses: 4.4.4.4, 5.5.5.5, 45.45.45.45
    b. Domains: spam.com, bad.com
    c. Email senders: spam@gmail.com, spam@yahoo.com

```
{primary:node0}[edit]
lab@central-node0# show security utm
custom-objects {
    filename-extension {
        bat-sh {
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
            value [ bat sh ];
        }
    }
    url-pattern {
        spam-sources {
            value [ 4.4.4.4 5.5.5.5 45.45.45.45 spam.com bad.com "spam@gmail.com"
"spam@yahoo.com" ];
        }
    }
}
default-configuration {
    anti-spam {
        type sbl;
    }
}
feature-profile {
    anti-spam {
        address-blacklist spam-sources;
        sbl {
            profile smtp-protect {
                no-sbl-default-server;
                spam-action block;
            }
        }
    }
    content-filtering {
        profile CENTRAL-content-filter {
            block-extension bat-sh;
            block-content-type {
                java-applet;
                http-cookie;
            }
            notification-options {
                type protocol-only;
                custom-message "Firewall blocked this content!";
            }
        }
    }
}
utm-policy CENTRAL-Content {
    content-filtering {
        http-profile CENTRAL-content-filter;
        ftp {
            upload-profile CENTRAL-content-filter;
            download-profile CENTRAL-content-filter;
        }
    }
}
utm-policy CENTRAL-SPAM {
    anti-spam {
        smtp-profile smtp-protect;
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
    }
}

{primary:node0}[edit]
lab@central-node0# show security policies from-zone TRUST to-zone UNTRUST
policy HTTP-FTP {
    match {
        source-address CENTRAL-TRUST;
        destination-address any;
        application [ junos-http junos-ftp ];
    }
    then {
        permit;
        log {
            session-init;
            session-close;
        }
    }
}

{primary:node0}[edit]
lab@central-node0# show security policies from-zone UNTRUST to-zone WAREHOUSE
policy SRV-MAIL {
    match {
        source-address any;
        destination-address SRV-MAIL;
        application junos-smtp;
    }
    then {
        permit {
            destination-address {
                drop-untranslated;
            }
            application-services {
                utm-policy CENTRAL-SPAM;
            }
        }
    }
}

{primary:node0}[edit]
lab@central-node0# show security policies from-zone WAREHOUSE to-zone WAREHOUSE
policy WAREHOUSE {
    match {
        source-address any;
        destination-address any;
        application any;
    }
    then {
        permit;
    }
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
}

{primary:node0}[edit]
lab@central-node0# show security nat static rule-set SRV-MAIL
from zone UNTRUST;
rule mail {
    match {
        destination-address 80.1.1.192/32;
    }
    then {
        static-nat {
            prefix {
                172.16.60.199/32;
            }
        }
    }
}
```

5) In headquarters all HTTP requests from the INTERNAL and TESTBED zones have to be redirected to the Websense V10000 appliance (172.16.60.99) located in the WAREHOUSE zone behind the XPARENT cluster firewall
    a. The Websense appliance performs proxy operation and changes the source address of the request to its own

```
{primary:node0}[edit]
lab@central-node0# show routing-instances
websense {
    instance-type forwarding;
    routing-options {
        static {
            route 0.0.0.0/0 next-hop 172.16.60.99;
        }
    }
}
```

```
{primary:node0}[edit]
lab@central-node0# show policy-options policy-statement WAREHOUSE
term NETWORK {
    from {
        protocol direct;
        route-filter 172.16.60.0/24 exact;
    }
    then accept;
}
term else {
    then reject;
}
lab@central-node0# show routing-options
interface-routes {
    rib-group inet TO-WEBSENSE;
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
}
rib-groups {
    TO-WEBSENSE {
        import-rib [ inet.0 websense.inet.0 ];
        import-policy WAREHOUSE;
    }
}

{primary:node0}[edit]
lab@central-node0# show interfaces reth0
vlan-tagging;
redundant-ether-options {
    redundancy-group 1;
}
unit 50 {
    vlan-id 50;
    family inet {
        address 172.16.50.254/24;
    }
    family inet6 {
        address 2016:abcd:a1::254/64;
    }
}
unit 55 {
    vlan-id 55;
    family inet {
        filter {
            input FBF-WEBSENSE;
        }
        address 172.16.55.254/24;
    }
}
unit 60 {
    vlan-id 60;
    family inet {
        address 172.16.60.254/24;
    }
}
unit 65 {
    vlan-id 65;
    family inet {
        filter {
            input FBF-WEBSENSE;
        }
        address 172.16.65.254/24;
    }
}
unit 70 {
    vlan-id 70;
    family inet {
        filter {
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
            input FBF-WEBSENSE;
        }
        address 172.16.70.254/24;
    }
}

{primary:node0}[edit]
lab@central-node0# show security policies from-zone INTERNAL to-zone WAREHOUSE policy WEBSENSE
match {
    source-address CENTRAL-INTERNAL;
    destination-address any;
    application junos-http;
}
then {
    permit;
}

primary:node0}[edit]
lab@central-node0# show security policies from-zone TESTBED to-zone WAREHOUSE policy WEBSENSE
match {
    source-address CENTRAL-TESTBED;
    destination-address any;
    application junos-http;
    dynamic-application junos:HTTP;
}
then {
    permit;
    log {
        session-init;
        session-close;
    }
}

{primary:node0}[edit]
lab@central-node0# show security policies from-zone WAREHOUSE to-zone UNTRUST policy WEBSENSE
match {
    source-address WEBSENSE;
    destination-address any;
    application junos-http;
}
then {
    permit;
}

{primary:node0}[edit]
lab@central-node0# show security nat source
pool WEBSENSE {
    address {
        80.1.1.160/32;
    }
}
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
{primary:node0}[edit]
lab@central-node0# show security nat source rule-set UNTRUST
from zone [ INTERNAL TRUST WAREHOUSE ];
to zone UNTRUST;
rule WEBSENSE {
    match {
        source-address 172.16.60.99/32;
        destination-address 0.0.0.0/0;
    }
    then {
        source-nat {
            pool {
                WEBSENSE;
            }
        }
    }
}

primary:node0}[edit]
lab@central-node0# show security policies from-zone WAREHOUSE to-zone UNTRUST
policy WEBSENSE {
    match {
        source-address WEBSENSE;
        destination-address any;
        application junos-http;
    }
    then {
        permit;
    }
}

primary:node0}[edit]
lab@central-node0# show policy-options policy-statement WAREHOUSE
term NETWORK {
    from {
        protocol direct;
        route-filter 172.16.60.0/24 exact;
    }
    then accept;
}
term else {
    then reject;
}

primary:node0}[edit]
lab@central-node0# show routing-options rib-groups
TO-WEBSENSE {
    import-rib [ inet.0 websense.inet.0 ];
    import-policy WAREHOUSE;
}
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
primary:node0}[edit]
lab@central-node0# show firewall family inet filter FBF-WEBSENSE
term http {
    from {
        protocol tcp;
        destination-port http;
    }
    then {
        routing-instance websense;
    }
}
term else {
    then accept;
}
```

Task 6: NAT

1) Following NAT translations need to be done on the roffice1 security device:
    a. The egress interface IP address is used to translate connections from the hosts in the TRUST-RO1 zone to the UNTRUST zone.
    b. The host 172.16.11.50 in the PRIVATE-RO1 zone needs to be able to receive connections from and initiate connections to the Internet. The connections from Internet need to be destined to the 80.1.1.64 IP address in order to reach this host.

Roffice1:

```
[edit]
lab@roffice1# show security nat
source {
    rule-set TRUST-RO1 {
        from zone TRUST-RO1;
        to zone UNTRUST;
        rule INTERNET {
            match {
                destination-address 0.0.0.0/0;
            }
            then {
                source-nat {
                    interface;
                }
            }
        }
    }
}
static {
    rule-set RO1-HOST-PRIVATE {
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
from zone UNTRUST;
rule RO1-HOST-PRIVATE {
    match {
        destination-address 80.1.1.64/32;
    }
    then {
        static-nat {
            prefix {
                172.16.11.50/32;
            }
        }
    }
}

[edit]
lab@roffice1#show security policies
from-zone TRUST-RO1 to-zone UNTRUST {
    policy HTTP-FTP {
        match {
            source-address RO1-TRUST;
            destination-address any;
            application [ junos-http junos-ftp ];
        }
        then {
            permit {
                application-services {
                    utm-policy RO-AV;
                }
            }
        }
    }
    policy INTERNET {
        match {
            source-address RO1-TRUST;
            destination-address any;
            application any;
        }
        then {
            permit;
        }
    }
}
from-zone UNTRUST to-zone PRIVATE-RO1 {
    policy RO1-HOST-PRIVATE {
        match {
            source-address any;
            destination-address RO1-HOST-PRIVATE;
            application any;
        }
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
        then {
            permit;
        }
    }
}
from-zone PRIVATE-RO1 to-zone UNTRUST {
    policy INTERNET {
        match {
            source-address RO1-HOST-PRIVATE;
            destination-address any;
            application any;
        }
        then {
            permit;
        }
    }
}
```

```
VR-DEVICE> telnet routing-instance roffice1-trust 12.34.56.78 port 80
Trying 12.34.56.78...
Connected to 12.34.56.78.
Escape character is '^]'.

roffice1> show security flow session destination-port 80
Session ID: 3513, Policy name: HTTP-FTP/8, Timeout: 298, Valid
  In: 172.16.10.1/62321 --> 12.34.56.78/80;tcp, If: ge-0/0/4.0, Pkts: 2,
Bytes: 116
  Out: 12.34.56.78/80 --> 80.1.1.1/14569;tcp, If: ge-0/0/3.0, Pkts: 1, Bytes:
64
Total sessions: 1

VR-DEVICE> ping routing-instance roffice1-trust 12.34.56.78 count 1
PING 12.34.56.78 (12.34.56.78): 56 data bytes
64 bytes from 12.34.56.78: icmp_seq=0 ttl=63 time=2.581 ms

roffice1> show security flow session protocol icmp
Session ID: 3520, Policy name: INTERNET/6, Timeout: 4, Valid
  In: 172.16.10.1/1 --> 12.34.56.78/3852;icmp, If: ge-0/0/4.0, Pkts: 1,
Bytes: 84
  Out: 12.34.56.78/3852 --> 80.1.1.1/28867;icmp, If: ge-0/0/3.0, Pkts: 1,
Bytes: 84
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
VR-DEVICE> ping routing-instance roffice1-private 12.34.56.78 source
172.16.11.50 count 1
PING 12.34.56.78 (12.34.56.78): 56 data bytes
64 bytes from 12.34.56.78: icmp_seq=0 ttl=63 time=2.806 ms

roffice1> show security flow session protocol icmp
Session ID: 3537, Policy name: INTERNET/9, Timeout: 2, Valid
  In: 172.16.11.50/0 --> 12.34.56.78/3863;icmp, If: ge-0/0/5.0, Pkts: 1,
Bytes: 84
  Out: 12.34.56.78/3863 --> 80.1.1.64/0;icmp, If: ge-0/0/3.0, Pkts: 1, Bytes:
84
Total sessions: 1

VR-DEVICE> ping routing-instance untrust 80.1.1.64 count 1
PING 80.1.1.64 (80.1.1.64): 56 data bytes
64 bytes from 80.1.1.64: icmp_seq=0 ttl=63 time=2.686 ms

roffice1> show security flow session protocol icmp
Session ID: 3548, Policy name: RO1-HOST-PRIVATE/4, Timeout: 2, Valid
  In: 80.1.1.2/0 --> 80.1.1.64/3877;icmp, If: ge-0/0/3.0, Pkts: 1, Bytes: 84
  Out: 172.16.11.50/3877 --> 80.1.1.2/0;icmp, If: ge-0/0/5.0, Pkts: 1, Bytes:
84
Total sessions: 1
```

2) NAT translation details for the roffice2 security device:
   a. Ensure the connections from the TRUST-RO2 zone to the Internet are translated to 80.1.1.96-80.1.1.99 IP addresses. PAT is allowed and concurrent sessions from the same host must be translated using the same IP address.
   b. The web and database servers need to be reachable from the UNTRUST zone as defined in the table below:
   c. Untranslated connections from the UNTRUST zone to these servers are not allowed

Server	Internal address	Internal port	Public address	Public port
Web server	172.16.21.2	80	80.1.1.100	8080
Database server	172.16.21.33	3306	80.1.1.100	3306

Roffice2:

```
[edit]
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
lab@roffice2# show security nat | no-more
source {
    pool INTERNET {
        address {
            80.1.1.96/32 to 80.1.1.99/32;
        }
    }
    address-persistent;
    rule-set TRUST-RO2 {
        from zone TRUST-RO2;
        to zone UNTRUST;
        rule INTERNET {
            match {
                destination-address 0.0.0.0/0;
            }
            then {
                source-nat {
                    pool {
                        INTERNET;
                    }
                }
            }
        }
    }
}
destination {
    pool RO2-SRV-WEB {
        address 172.16.21.2/32 port 80;
    }
    pool RO2-SRV-DB {
        address 172.16.21.33/32;
    }
    rule-set RO2-SERVERS {
        from zone UNTRUST;
        rule RO2-SRV-WEB {
            match {
                destination-address 80.1.1.100/32;
                destination-port 8080;
            }
            then {
                destination-nat {
                    pool {
                        RO2-SRV-WEB;
                    }
                }
            }
        }
    rule RO2-SRV-DB {
        match {
            destination-address 80.1.1.100/32;
            destination-port 3306;
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
                }
                then {
                    destination-nat {
                        pool {
                            RO2-SRV-DB;
                        }
                    }
                }
            }
        }
    }

[edit]
lab@roffice2# show security policies | no-more
from-zone UNTRUST to-zone TRUST-RO2 {
    policy trust {
        match {
            source-address any;
            destination-address RO2-TRUST;
            application any;
        }
        then {
            permit;
        }
    }
}
from-zone UNTRUST to-zone DMZ-RO2 {
    policy SERVERS {
        match {
            source-address any;
            destination-address [ RO2-SRV-WEB RO2-SRV-DB ];
            application [ junos-http RO2-SQL ];
        }
        then {
            permit {
                destination-address {
                    drop-untranslated;
                }
            }
        }
    }
}
from-zone TRUST-RO2 to-zone UNTRUST {
    policy HTTP-FTP {
        match {
            source-address RO2-TRUST;
            destination-address any;
            application [ junos-http junos-ftp ];
        }
        then {
            permit {
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
            application-services {
                utm-policy RO-AV;
            }
        }
    }
}
policy INTERNET {
    match {
        source-address RO2-TRUST;
        destination-address any;
        application any;
    }
    then {
        permit;
    }
}
```

```
[edit]
lab@roffice2# show applications
application RO2-SQL {
    protocol tcp;
    destination-port 3306;
}
```

- Verification (example)

```
vr-device> telnet routing-instance untrust 80.1.1.100 port 3306
Trying 80.1.1.100...
Connected to 80.1.1.100.
Escape character is '^]'.

roffice2> show security flow session destination-port 3306
Session ID: 478, Policy name: SERVERS/5, Timeout: 1768, Valid
  In: 80.1.1.6/59544 --> 80.1.1.100/3306;tcp, If: ge-0/0/3.0, Pkts: 2, Bytes:
116
  Out: 172.16.21.33/3306 --> 80.1.1.6/59544;tcp, If: ge-0/0/5.0, Pkts: 1,
Bytes: 64
Total sessions: 1
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
vr-device> telnet routing-instance roffice2-trust 12.34.56.78 port 80
Trying 12.34.56.78...
Connected to 12.34.56.78.
Escape character is '^]'.

roffice2> show security flow session destination-port 3306
Session ID: 392, Policy name: INTERNET/6, Timeout: 1788, Valid
  In: 172.16.20.1/56866 --> 12.34.56.78/3306;tcp, If: ge-0/0/4.0, Pkts: 2,
Bytes: 116
  Out: 12.34.56.78/3306 --> 80.1.1.97/30461;tcp, If: ge-0/0/3.0, Pkts: 1,
Bytes: 64
Total sessions: 1

vr-device> ping routing-instance roffice2-trust 12.34.56.78 count 1
PING 12.34.56.78 (12.34.56.78): 56 data bytes
64 bytes from 12.34.56.78: icmp_seq=0 ttl=63 time=2.581 ms

roffice2> show security flow session protocol icmp
Session ID: 399, Policy name: INTERNET/6, Timeout: 2, Valid
  In: 172.16.20.1/0 --> 12.34.56.78/8661;icmp, If: ge-0/0/4.0, Pkts: 1,
Bytes: 84
  Out: 12.34.56.78/8661 --> 80.1.1.97/27985;icmp, If: ge-0/0/3.0, Pkts: 1,
Bytes: 84
```

3) The exa-fw device has to provide the following translations:
   a. Traffic from the TRUST-EXA hosts to the Internet has to be translated to the 100.1.1.128-100.1.1.143 range. PAT is not allowed, and the IP address of the egress interface has to be used when the pool is exhausted.
   b. The connections from PRIVATE-EXA hosts to the Internet must be translated in following manner:
      i. 172.16.15.5 --> 100.1.1.192, 172.16.15.6 --> 100.1.1.193, …, up to 172.16.15.10 --> 100.1.1.197
      ii. Ports are not translated
      iii. Connections from other hosts are not translated
   c. The servers in the DMZ-EXA zone need to be reachable from the Internet as specified in the table below:

Server	Internal address	Internal port	Public address	Public port
Web server	172.16.30.11	80	100.1.1.3	8080
Database server	172.16.30.12	3306	100.1.1.3	3306
SSH server	172.16.30.13	22	100.1.1.4	12345

   d. Untranslated connections from the UNTRUST zone to these servers are not allowed.

© 2020 Juniper Networks, Inc. All rights reserved.

Exa-fw:

```
[edit]
lab@exa-fw# show security nat | no-more
source {
    pool TRUST {
        address {
            100.1.1.128/32 to 100.1.1.143/32;
        }
        port no-translation;
        overflow-pool interface;
    }
pool PRIVATE {
    address {
        100.1.1.192/32 to 100.1.1.197/32;
    }
    host-address-base 172.16.15.5/32;
    port no-translation;
}
rule-set INTERNET {
    from zone [ PRIVATE-EXA TRUST-EXA ];
    to zone UNTRUST;
    rule TRUST {
        match {
            source-address 172.16.10.0/24;
            destination-address 0.0.0.0/0;
        }
        then {
            source-nat {
                pool {
                    TRUST;
                }
            }
        }
    }
        rule PRIVATE {
            match {
                source-address 172.16.15.0/24;
                destination-address 0.0.0.0/0;
            }
            then {
                source-nat {
                    pool {
                        PRIVATE;
                    }
                }
            }
        }
    }
}
destination {
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
pool EXA-SRV-WEB {
    address 172.16.30.11/32 port 80;
}
pool EXA-SRV-DB {
    address 172.16.30.12/32;
}
pool EXA-SRV-SSH {
    address 172.16.30.13/32 port 22;
}
rule-set SERVERS {
    from zone UNTRUST;
    rule EXA-SRV-WEB {
        match {
            destination-address 100.1.1.3/32;
            destination-port 8080;
        }
        then {
            destination-nat {
                pool {
                    EXA-SRV-WEB;
                }
            }
        }
    }
    rule EXA-SRV-DB {
        match {
            destination-address 100.1.1.3/32;
            destination-port 3306;
        }
        then {
            destination-nat {
                pool {
                    EXA-SRV-DB;
                }
            }
        }
    }
    rule EXA-SRV-SSH {
        match {
            destination-address 100.1.1.4/32;
            destination-port 12345;
        }
        then {
            destination-nat {
                pool {
                    EXA-SRV-SSH;
                }
            }
        }
    }
}
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
}

[edit]
lab@exa-fw# show security policies | no-more
from-zone TRUST-EXA to-zone UNTRUST {
    policy HTTP {
        match {
            source-address EXA-TRUST;
            destination-address any;
            application junos-http;
        }
        then {
            permit {
                application-services {
                    utm-policy EXA-WebFilter;
                }
            }
        }
    }
    policy INTERNET {
        match {
            source-address EXA-TRUST;
            destination-address any;
            application any;
        }
        then {
            permit;
        }
    }
}
from-zone PRIVATE-EXA to-zone UNTRUST {
    policy INTERNET {
        match {
            source-address EXA-PRIVATE;
            destination-address any;
            application any;
        }
        then {
            permit
            }
        }
    }
}
from-zone UNTRUST to-zone DMZ-EXA {
    policy EXA-SRV-WEB {
        match {
            source-address any;
            destination-address EXA-SRV-WEB;
            application junos-http;
        }
        then {
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
        permit;
    }
}
policy EXA-SRV-DB {
    match {
        source-address any;
        destination-address EXA-SRV-DB;
        application EXA-SQL;
    }
    then {
        permit;
    }
}
    policy EXA-SRV-SSH {
        match {
            source-address any;
            destination-address EXA-SRV-SSH;
            application junos-ssh;
        }
        then {
            permit;
        }
    }
}

[edit]
lab@exa-fw# show applications
application EXA-SQL {
    protocol tcp;
    destination-port 3306;
}
```

```
VR-DEVICE> telnet routing-instance exa-trust 12.34.56.78 port 80
Trying 12.34.56.78...
Connected to 12.34.56.78.
Escape character is '^]'.

exa-fw> show security flow session destination-port 80
Session ID: 9572, Policy name: HTTP/16, Timeout: 292, Valid
  In: 172.16.10.1/56121 --> 12.34.56.78/80;tcp, If: ge-0/0/4.0, Pkts: 2,
Bytes: 116
  Out: 12.34.56.78/80 --> 100.1.1.133/56121;tcp, If: ge-0/0/3.0, Pkts: 1,
Bytes: 64
Total sessions: 1
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
VR-DEVICE> telnet routing-instance exa-private 12.34.56.78 port 80 source
172.16.15.10
Trying 12.34.56.78...
Connected to 12.34.56.78.
Escape character is '^]'.

exa-fw> show security flow session destination-port 80
Session ID: 9582, Policy name: INTERNET/5, Timeout: 220, Valid
  In: 172.16.15.10/54716 --> 12.34.56.78/80;tcp, If: ge-0/0/5.15, Pkts: 2,
Bytes: 116
  Out: 12.34.56.78/80 --> 100.1.1.197/54716;tcp, If: ge-0/0/3.0, Pkts: 1,
Bytes: 64
Total sessions: 1
```


```
VR-DEVICE> telnet routing-instance exa-private 12.34.56.78 port 80 source
172.16.15.10
Trying 12.34.56.78...
Connected to 12.34.56.78.
Escape character is '^]'.

exa-fw> show security flow session destination-port 80
Session ID: 9582, Policy name: INTERNET/5, Timeout: 220, Valid
  In: 172.16.15.10/54716 --> 12.34.56.78/80;tcp, If: ge-0/0/5.15, Pkts: 2,
Bytes: 116
  Out: 12.34.56.78/80 --> 100.1.1.197/54716;tcp, If: ge-0/0/3.0, Pkts: 1,
Bytes: 64
Total sessions: 1
```


```
VR-DEVICE> telnet routing-instance untrust 100.1.1.3 port 8080
Trying 100.1.1.3...
Connected to 100.1.1.3.
Escape character is '^]'.

exa-fw> show security flow session destination-port 80
Session ID: 9625, Policy name: EXA-SRV-WEB/6, Timeout: 250, Valid
  In: 100.1.1.6/52344 --> 100.1.1.3/8080;tcp, If: ge-0/0/3.0, Pkts: 3, Bytes:
170
  Out: 172.16.30.11/80 --> 100.1.1.6/52344;tcp, If: ge-0/0/5.30, Pkts: 2,
Bytes: 116
Total sessions: 1
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
VR-DEVICE> telnet routing-instance untrust 100.1.1.3 port 3306
Trying 100.1.1.3...
Connected to 100.1.1.3.
Escape character is '^]'.

exa-fw> show security flow session destination-port 3306
Session ID: 9635, Policy name: EXA-SRV-DB/17, Timeout: 1796, Valid
  In: 100.1.1.6/54543 --> 100.1.1.3/3306;tcp, If: ge-0/0/3.0, Pkts: 2, Bytes:
116
  Out: 172.16.30.12/3306 --> 100.1.1.6/54543;tcp, If: ge-0/0/5.30, Pkts: 1,
Bytes: 64
Total sessions: 1
```

```
VR-DEVICE> telnet routing-instance untrust 100.1.1.4 port 12345
Trying 100.1.1.4...
Connected to 100.1.1.4.
Escape character is '^]'.
SSH-2.0-OpenSSH_6.6

exa-fw> show security flow session destination-port 22
Session ID: 9656, Policy name: EXA-SRV-SSH/18, Timeout: 1748, Valid
  In: 100.1.1.6/51872 --> 100.1.1.4/12345;tcp, If: ge-0/0/3.0, Pkts: 3, Bytes:
168
  Out: 172.16.30.13/22 --> 100.1.1.6/51872;tcp, If: ge-0/0/5.30, Pkts: 2,
Bytes: 137
Total sessions: 1
```

4) The connections leaving the headquarters through central cluster need to be translated in following way:
   a. All connections arriving on the cluster in the TRUST and INTERNAL zones and destined to the Internet need to be translated using the 80.1.1.128 - 80.1.1.159
   b. Bidirectional translation needs to be provided for the company's email server (172.16.60.199). The public IP address allocated for this purpose is 80.1.1.192. Untranslated traffic from the UNTRUST zone to the email server must be blocked.
   c. From the WAREHOUSE zone only the Websense V10000 appliance's (172.16.60.99) initiated connections to the Internet are translated. Use the 80.1.1.160 IP address.
   d. The servers located in the WAREHOUSE zone have to be reachable from the Internet.

© 2020 Juniper Networks, Inc. All rights reserved.

Server	Internal address	Internal port	Public address	Public port
Web server	172.16.60.205	80	80.1.1.200	8080
Database server	172.16.60.205	3306	80.1.1.200	3306
SSH server	172.16.60.206	22	80.1.1.201	22
Honeypot	172.16.60.207	All	80.1.1.202	All

e. Untranslated connections from the UNTRUST zone to these servers are not allowed.

Central-node0:

```
{primary:node0}[edit]
lab@central-node0# show security nat
source {
    pool INTERNET {
        address {
            80.1.1.128/32 to 80.1.1.159/32;
        }
    }
    pool WEBSENSE {
        address {
            80.1.1.160/32;
        }
    }
    rule-set UNTRUST {
        from zone [ INTERNAL TRUST WAREHOUSE ];
        to zone UNTRUST;
        rule WEBSENSE {
            match {
                source-address 172.16.60.99/32;
                destination-address 0.0.0.0/0;
            }
            then {
                source-nat {
                    pool {
                        WEBSENSE;
                    }
                }
            }
        }
    }
    rule INTERNET {
        match {
            source-address [ 172.16.50.0/24 172.16.55.0/24 ];
            destination-address 0.0.0.0/0;
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
            }
            then {
                source-nat {
                    pool {
                        INTERNET;
                    }
                }
            }
        }
    }
}
destination {
    pool WAREHOUSE-SRV-WEB {
        address 172.16.60.205/32 port 80;
    }
    pool WAREHOUSE-SRV-DB {
        address 172.16.60.205/32;
    }
    pool WAREHOUSE-SRV-SSH {
        address 172.16.60.206/32;
    }
    pool WAREHOUSE-HONEYPOT {
        address 172.16.60.207/32;
    }
    rule-set SERVERS {
        from zone UNTRUST;
        rule WAREHOUSE-SRV-WEB {
            match {
                destination-address 80.1.1.200/32;
                destination-port {
                    8080;
                }
            }
            then {
                destination-nat {
                    pool {
                        WAREHOUSE-SRV-WEB;
                    }
                }
            }
        }
    }
    rule WAREHOUSE-SRV-DB {
        match {
            destination-address 80.1.1.200/32;
            destination-port {
                3306;
            }
        }
        then {
            destination-nat {
                pool {
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
                    WAREHOUSE-SRV-DB;
                }
            }
        }
    }
    rule WAREHOUSE-SRV-SSH {
        match {
            destination-address 80.1.1.201/32;
            destination-port {
                22;
            }
        }
        then {
            destination-nat {
                pool {
                    WAREHOUSE-SRV-SSH;
                }
            }
        }
    }
    rule WAREHOUSE-HONEYPOT {
        match {
            destination-address 80.1.1.202/32;
        }
        then {
            destination-nat {
                pool {
                    WAREHOUSE-HONEYPOT;
                }
            }
        }
    }
}
static {
    rule-set SRV-MAIL {
        from zone UNTRUST;
        rule mail {
            match {
                destination-address 80.1.1.192/32;
            }
            then {
                static-nat {
                    prefix {
                        172.16.60.199/32;
                    }
                }
            }
        }
    }
}
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
{primary:node0}[edit]
lab@central-node0# show security address-book global | match warehouse
    address CENTRAL-WAREHOUSE 172.16.60.0/24;
    address WAREHOUSE-SRV-205 172.16.60.205/32;
    address WAREHOUSE-SRV-206 172.16.60.206/32;
    address WAREHOUSE-HONEYPOT 172.16.60.207/32;


{primary:node0}[edit]
lab@central-node0# show security policies from-zone TRUST to-zone UNTRUST
policy HTTP-FTP {
    match {
        source-address CENTRAL-TRUST;
        destination-address any;
        application [ junos-http junos-ftp ];
    }
    then {
        permit {
            application-services {
                utm-policy CENTRAL-Content;
            }
        }
    }
}
policy INTERNET {
    match {
        source-address CENTRAL-TRUST;
        destination-address any;
        application any;
    }
    then {
        permit;
    }
}

{primary:node0}[edit]
lab@central-node0# show security policies from-zone INTERNAL to-zone UNTRUST
policy INTERNET {
    match {
        source-address CENTRAL-INTERNAL;
        destination-address any;
        application any;
    }
    then {
        permit;
    }
}

{primary:node0}[edit]
lab@central-node0# show security policies from-zone WAREHOUSE to-zone UNTRUST
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
policy WEBSENSE {
    match {
        source-address WEBSENSE;
        destination-address any;
        application junos-http;
    }
    then {
        permit;
    }
}
policy SRV-MAIL {
    match {
        source-address SRV-MAIL;
        destination-address any;
        application any;
    }
    then {
        permit;
    }
}

{primary:node0}[edit]
lab@central-node0# show security policies from-zone UNTRUST to-zone WAREHOUSE
policy SRV-MAIL {
    match {
        source-address any;
        destination-address SRV-MAIL;
        application junos-smtp;
    }
    then {
        permit {
            destination-address {
                drop-untranslated;
            }
            application-services {
                utm-policy CENTRAL-SPAM;
            }
        }
    }
}
policy SERVERS {
    match {
        source-address any;
        destination-address [ WAREHOUSE-SRV-205 WAREHOUSE-SRV-206 WAREHOUSE-HONEYPOT ];
        application any;
    }
    then {
        permit {
            destination-address {
                drop-untranslated;
            }
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
        }
    }
}
```

Xparent-node0:

```
{primary:node0}[edit]
lab@xparent-node0# show security address-book global | match warehouse
    address CENTRAL-WAREHOUSE 172.16.60.0/24;
    address WAREHOUSE-SRV-205 172.16.60.205/32;
    address WAREHOUSE-SRV-206 172.16.60.206/32;

{primary:node0}[edit]
lab@xparent-node0# show security policies from-zone WAREHOUSE to-zone WAREHOUSE
policy WAREHOUSE {
    match {
        source-address CENTRAL-WAREHOUSE;
        destination-address CENTRAL-WAREHOUSE;
        application any;
    }
    then {
        permit;
    }
}
policy WEBSENSE {
    match {
        source-address [ CENTRAL-INTERNAL CENTRAL-TESTBED WEBSENSE ];
        destination-address any;
        application junos-http;
    }
    then {
        permit;
    }
}
policy SRV-MAIL-in {
    match {
        source-address any;
        destination-address SRV-MAIL;
        application junos-smtp;
    }
    then {
        permit;
    }
}
policy SRV-MAIL-out {
    match {
        source-address SRV-MAIL;
        destination-address any;
        application any;
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
    }
    then {
        permit;
    }
}
policy SERVERS {
    match {
        source-address any;
        destination-address [ WAREHOUSE-SRV-205 WAREHOUSE-SRV-206 ];
        application [ junos-http SQL junos-ssh ];
    }
    then {
        permit;
    }
}
```

Verification

```
VR-DEVICE> ping 12.34.56.78 routing-instance central-trust count 1
PING 12.34.56.78 (12.34.56.78): 56 data bytes
64 bytes from 12.34.56.78: icmp_seq=0 ttl=63 time=3.210 ms

central-node0> show security flow session protocol icmp
Session ID: 81635, Policy name: INTERNET/10, State: Active, Timeout: 2, Valid
  In: 172.16.50.100/0 --> 12.34.56.78/20931;icmp, If: reth0.50, Pkts: 1,
Bytes: 84
  Out: 12.34.56.78/20931 --> 80.1.1.131/52830;icmp, If: ge-0/0/3.0, Pkts: 1,
Bytes: 84
Total sessions: 1
```

```
VR-DEVICE> ping 12.34.56.78 routing-instance central-internal count 1
PING 12.34.56.78 (12.34.56.78): 56 data bytes
64 bytes from 12.34.56.78: icmp_seq=0 ttl=63 time=3.231 ms

central-node0> show security flow session protocol icmp
Session ID: 81697, Policy name: INTERNET/13, State: Active, Timeout: 2, Valid
  In: 172.16.55.100/0 --> 12.34.56.78/20940;icmp, If: reth0.55, Pkts: 1,
Bytes: 84
  Out: 12.34.56.78/20940 --> 80.1.1.133/32880;icmp, If: ge-0/0/3.0, Pkts: 1,
Bytes: 84
Total sessions: 1
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
VR-DEVICE> ping 12.34.56.78 routing-instance xparent-warehouse source
172.16.60.199 count 1
PING 12.34.56.78 (12.34.56.78): 56 data bytes
64 bytes from 12.34.56.78: icmp_seq=0 ttl=63 time=3.795 ms

central-node0> show security flow session protocol icmp
Session ID: 81772, Policy name: SRV-MAIL/8, State: Active, Timeout: 2, Valid
  In: 172.16.60.199/0 --> 12.34.56.78/20984;icmp, If: reth0.60, Pkts: 1,
Bytes: 84
  Out: 12.34.56.78/20984 --> 80.1.1.192/0;icmp, If: ge-0/0/3.0, Pkts: 1,
Bytes: 84
Total sessions: 1
```

```
VR-DEVICE> telnet 80.1.1.192 routing-instance untrust port 25
Trying 80.1.1.192...

central-node0> show security flow session destination-port 25
Session ID: 81795, Policy name: SRV-MAIL/9, State: Active, Timeout: 14, Valid
  In: 80.1.1.9/63922 --> 80.1.1.192/25;tcp, If: ge-0/0/3.0, Pkts: 2, Bytes:
128
  Out: 172.16.60.199/25 --> 80.1.1.9/63922;tcp, If: reth0.60, Pkts: 0, Bytes:
0
Total sessions: 1
```

```
VR-DEVICE> telnet 12.34.56.78 routing-instance xparent-warehouse source
172.16.60.99 port 80
Trying 12.34.56.78...
Connected to 12.34.56.78.
Escape character is '^]'.

central-node0> show security flow session destination-port 80
Session ID: 82247, Policy name: WEBSENSE/6, State: Active, Timeout: 294, Valid
  In: 172.16.60.99/59580 --> 12.34.56.78/80;tcp, If: reth0.60, Pkts: 2, Bytes:
116
  Out: 12.34.56.78/80 --> 80.1.1.160/40247;tcp, If: ge-0/0/3.0, Pkts: 1,
Bytes: 64
Total sessions: 1
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
VR-DEVICE> telnet routing-instance untrust 80.1.1.200 port 8080
Trying 80.1.1.200...
Connected to 80.1.1.200.
Escape character is '^]'.

central-node0> show security flow session destination-port 80
Session ID: 82293, Policy name: SERVERS/7, State: Active, Timeout: 294, Valid
  In: 80.1.1.9/64292 --> 80.1.1.200/8080;tcp, If: ge-0/0/3.0, Pkts: 2, Bytes:
116
  Out: 172.16.60.205/80 --> 80.1.1.9/64292;tcp, If: reth0.60, Pkts: 1, Bytes:
64
Total sessions: 1

xparent-node0> show security flow session destination-port 80
Session ID: 184311, Policy name: SERVERS/10, State: Active, Timeout: 296,
Valid
  In: 80.1.1.9/53993 --> 172.16.60.205/80;tcp, If: reth0.60, Pkts: 2, Bytes:
152
  Out: 172.16.60.205/80 --> 80.1.1.9/53993;tcp, If: reth1.60, Pkts: 1, Bytes:
82
Total sessions: 1
```

```
VR-DEVICE> telnet routing-instance untrust 80.1.1.200 port 3306
Trying 80.1.1.200...
Connected to 80.1.1.200.
Escape character is '^]'.

central-node0> show security flow session destination-port 3306
Session ID: 82322, Policy name: SERVERS/7, State: Active, Timeout: 1794,
Valid
  In: 80.1.1.9/55128 --> 80.1.1.200/3306;tcp, If: ge-0/0/3.0, Pkts: 2, Bytes:
116
  Out: 172.16.60.205/3306 --> 80.1.1.9/55128;tcp, If: reth0.60, Pkts: 1,
Bytes: 64
Total sessions: 1

xparent-node0> show security flow session destination-port 3306
Session ID: 184310, Policy name: SERVERS/10, State: Active, Timeout: 1794,
Valid
  In: 80.1.1.9/59530 --> 172.16.60.205/3306;tcp, If: reth0.60, Pkts: 2,
Bytes: 152
  Out: 172.16.60.205/3306 --> 80.1.1.9/59530;tcp, If: reth1.60, Pkts: 1,
Bytes: 82
Total sessions: 1
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
VR-DEVICE> ssh routing-instance untrust 80.1.1.201
Password:

central-node0> show security flow session destination-port 22
Session ID: 82710, Policy name: SERVERS/7, State: Active, Timeout: 1716,
Valid
  In: 80.1.1.9/54859 --> 80.1.1.201/22;tcp, If: ge-0/0/3.0, Pkts: 14, Bytes:
2917
  Out: 172.16.60.206/22 --> 80.1.1.9/54859;tcp, If: reth0.60, Pkts: 12,
Bytes: 2793
Total sessions: 1

xparent-node0> show security flow session destination-port 22
Session ID: 184309, Policy name: SERVERS/10, State: Active, Timeout: 1784,
Valid
  In: 80.1.1.9/54859 --> 172.16.60.206/22;tcp, If: reth0.60, Pkts: 13, Bytes:
3099
  Out: 172.16.60.206/22 --> 80.1.1.9/54859;tcp, If: reth1.60, Pkts: 11,
Bytes: 2939
Total sessions: 1
```

```
VR-DEVICE> telnet routing-instance untrust 80.1.1.202 no-resolve
Trying 80.1.1.202...
Connected to 80.1.1.202.
Escape character is '^]'.
VR-DEVICE (ttyp1)

login:

central-node0> show security flow session destination-port 23
Session ID: 82382, Policy name: SERVERS/7, State: Active, Timeout: 1754, Valid
  In: 80.1.1.9/64605 --> 80.1.1.202/23;tcp, If: ge-0/0/3.0, Pkts: 9, Bytes:
621
  Out: 172.16.60.207/23 --> 80.1.1.9/64605;tcp, If: reth0.60, Pkts: 7, Bytes:
597
Total sessions: 1
```


© 2020 Juniper Networks, Inc. All rights reserved.

Task 7: IPsec VPN

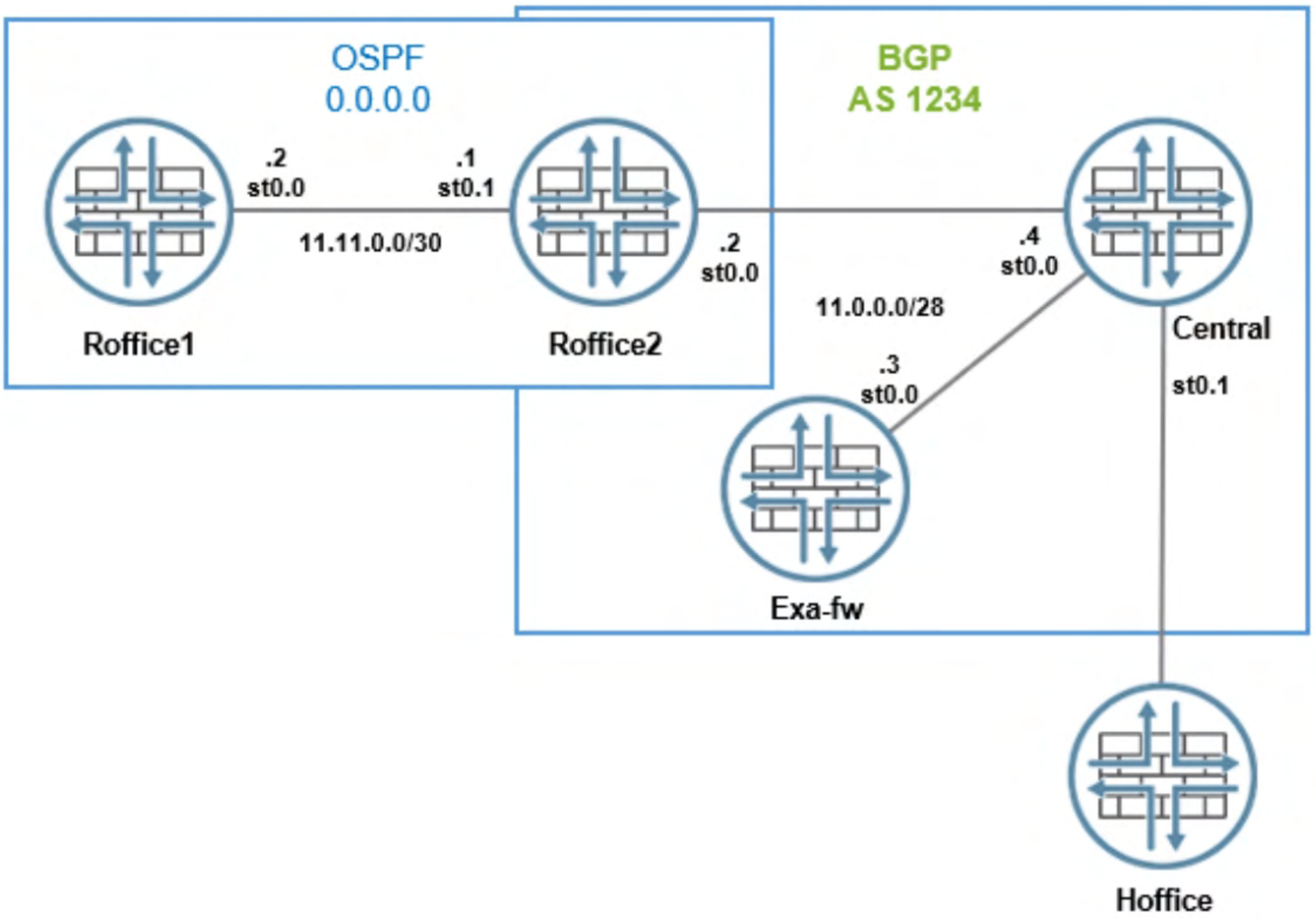


Figure 3: IPsec – VPNv4

1) The VPN design between roffice1 and roffice2 assumes that the OSPFv2 needs to be run on the top of the GRE tunnel. Here are the VPN parameters that were negotiated with the roffice1 administrator:
    a. The roffice1 security device is always an initiator of the IPsec VPN. The local-id is a hostname with the value “roffice1”.
    b. The st0.0 and st0.1 interfaces are used as a termination points for GRE tunnel on roffice1 and roffice2 devices respectively;
    c. The ge-0/0/3.0 interfaces are used as external interfaces for Phase 1 establishment on both sides of the VPN.
    d. IKE phase 1 proposal must include: preshared key “juniper”, 3DES, DH G1, MD5. Rekey Phase1 every 4 hours.
    e. IKE phase 2 proposal must include: AES128, ESP, DH G2, SHA1. Rekey Phase2 every hour.

© 2020 Juniper Networks, Inc. All rights reserved.

f. The interfaces configuration must follow information in the table below. For the GRE tunnel source and destination address use addresses of the interfaces st0.0 on roffice1 and st0.1 on roffice2 from the table below.

Device	Interface	IP address	Zone
roffice1	st0.0	11.11.0.1/30	VPN
roffice1	gr-0/0/0.0	11.11.11.1/30	VPN
roffice2	st0.1	11.11.11.2/30	VPN
roffice2	gr-0/0/0.0	11.11.0.2/30	VPN

g. Ensure that the TRUST zone subnet of both devices appears as OSPF internal route but IGP adjacency must only be attempted across GRE interfaces.
h. Ensure that TRUST networks connected to other hosts appear as OSPF external routes.
i. Ensure that the least possible number of security policies allow the subnets located in roffice's TRUST security zones communicating to each other.

Roffice1 & Roffice2

```
[edit]
lab@roffice1# show firewall family inet filter RE-PROTECT-v4 term IKE
from {
    port 500;
}
then {
    count IKE;
    accept;
}
```

```
[edit]
lab@roffice1# show security zones security-zone UNTRUST host-inbound-traffic
system-services {
    ping;
    ike;
}

[edit]
lab@roffice1# show protocols ospf
area 0.0.0.0 {
    interface gr-0/0/0.0 {
        interface-type p2p;
    }
    interface ge-0/0/4.0 {
        passive;
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
    }
}
```

Roffice1

```
[edit]
lab@roffice1# show security address-book global | match trust
        address CENTRAL-TRUST 172.16.50.0/24;
          address RO1-TRUST 172.16.10.0/24;
          address RO2-TRUST 172.16.20.0/24;
          address EXA-TRUST 172.16.10.0/24;
address HOFFICE-TRUST 172.16.77.0/24;
address EXA-TRUST-OVERLAP 172.16.110.0/24;
address RO1-TRUST-OVERLAP 172.16.111.0/24;
address BUILDING-TRUST-B1 172.16.100.0/24;
address BUILDING-TRUST-B2 172.16.200.0/24;
address CENTRAL-TRUST-V6 2016:abcd:a1::/64;
address RO1-TRUST-V6 2016:abcd:b1::/64;
address RO2-TRUST-V6 2016:abcd:c1::/64;
address EXA-TRUST-V6 2016:abcd:d1::/64;
address-set TRUST-NETWORKS {
    address RO1-TRUST;
    address RO2-TRUST;
    address CENTRAL-TRUST;
    address HOFFICE-TRUST;
    address EXA-TRUST-OVERLAP;
    address RO1-TRUST-OVERLAP;
    address BUILDING-TRUST-B1;
    address BUILDING-TRUST-B2;
address-set TRUST-NETWORKS-V6 {
    address CENTRAL-TRUST-V6;
    address RO1-TRUST-V6;
    address RO2-TRUST-V6;
    address EXA-TRUST-V6;
```

```
[edit]
lab@roffice1# show security ike
proposal IKE-PROP-ROFFICE {
    authentication-method pre-shared-keys;
    dh-group group1;
    authentication-algorithm md5;
    encryption-algorithm 3des-cbc;
    lifetime-seconds 14400;
}
policy IKE-POL-ROFFICE {
    mode aggressive;
    proposals IKE-PROP-ROFFICE;
    pre-shared-key ascii-text "$9$xkZNVYq.5n6AfTeWLxwsP5QnCu"; ## SECRET-DATA
}
gateway TO-RO2 {
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
    ike-policy IKE-POL-ROFFICE;
    address 80.1.1.5;
    local-identity hostname roffice1;
    external-interface ge-0/0/3;
}

[edit]
lab@roffice1# show interfaces st0
unit 0 {
    family inet {
        address 11.11.0.1/30;
    }
}
unit 1 {
    family inet6 {
        address 2016:abcd::2/126;
    }
}
unit 2 {
    family inet6;
}

[edit]
lab@roffice1# show security ipsec
proposal IPSEC-PROP-ROFFICE {
    protocol esp;
    authentication-algorithm hmac-sha1-96;
    encryption-algorithm aes-128-cbc;
    lifetime-seconds 3600;
}
policy IPSEC-POL-ROFFICE {
    perfect-forward-secrecy {
        keys group2;
    }
    proposals IPSEC-PROP-ROFFICE;
}
vpn TO-RO2 {
    bind-interface st0.0;
    ike {
        gateway TO-RO2;
        ipsec-policy IPSEC-POL-ROFFICE;
    }
    establish-tunnels immediately;
}

[edit]
lab@roffice1# show interfaces gr-0/0/0
unit 0 {
    tunnel {
        source 11.11.0.1;
        destination 11.11.0.2;
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
    }
    family inet {
        address 11.11.11.1/30;
    }
}

[edit]
lab@roffice1# show security zones security-zone VPN
host-inbound-traffic {
    system-services {
        ping;
    }
}
interfaces {
    st0.0;
    gr-0/0/0.0 {
        host-inbound-traffic {
            protocols {
                ospf;
            }
        }
    }
}
```

Roffice2

```
[edit]
lab@roffice2# show security ike
proposal IKE-PROP-ROFFICE {
    authentication-method pre-shared-keys;
    dh-group group1;
    authentication-algorithm md5;
    encryption-algorithm 3des-cbc;
    lifetime-seconds 14400;
}
policy IKE-POL-ROFFICE {
    mode aggressive;
    proposals IKE-PROP-ROFFICE;
    pre-shared-key ascii-text "$9$xkZNVYq.5n6AfTeWLxwsP5QnCu"; ## SECRET-DATA
}
gateway TO-RO1 {
    ike-policy IKE-POL-ROFFICE;
    dynamic hostname roffice1;
    external-interface ge-0/0/3;
}

[edit]
lab@roffice2# show interfaces st0
unit 0 {
    family inet {
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
        address 11.0.0.2/28;
    }
}
unit 1 {
    family inet {
        address 11.11.0.2/30;
    }
}


[edit]
lab@roffice2# show security ipsec
proposal IPSEC-PROP-ROFFICE {
    protocol esp;
    authentication-algorithm hmac-sha1-96;
    encryption-algorithm aes-128-cbc;
    lifetime-seconds 3600;
}
policy IPSEC-POL-ROFFICE {
    perfect-forward-secrecy {
        keys group2;
    }
    proposals IPSEC-PROP-ROFFICE;
}
vpn TO-RO1 {
    bind-interface st0.1;
    ike {
        gateway TO-RO1;
        ipsec-policy IPSEC-POL-ROFFICE;
    }
}

[edit]
lab@roffice2# show interfaces gr-0/0/0
unit 0 {
    tunnel {
        source 11.11.0.2;
        destination 11.11.0.1;
    }
    family inet {
        address 11.11.11.2/30;
    }
}

[edit]
lab@roffice2# show security zones security-zone VPN
host-inbound-traffic {
    system-services {
        ping;
    }
}
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
interfaces {
    st0.1;
    gr-0/0/0.0 {
        host-inbound-traffic {
            protocols {
                ospf;
            }
        }
    }
}
```

```
roffice1> show security ike sa detail
IKE peer 80.1.1.5, Index 5459983, Gateway Name: TO-RO2
  Role: Initiator, State: UP
  Initiator cookie: 1cc49f63198baa23, Responder cookie: 08aa87b2677aadda
  Exchange type: Aggressive, Authentication method: Pre-shared-keys
  Local: 80.1.1.1:500, Remote: 80.1.1.5:500
  Lifetime: Expires in 1239 seconds
  Peer ike-id: 80.1.1.5
  Xauth assigned IP: 0.0.0.0
  Algorithms:
   Authentication        : hmac-md5-96
   Encryption            : 3des-cbc
   Pseudo random function: hmac-md5
   Diffie-Hellman group  : DH-group-1
  Traffic statistics:
   Input  bytes  :                1928
   Output bytes  :                2692
   Input  packets:                   6
   Output packets:                  17
  Flags: IKE SA is created
  IPsec security associations: 5 created, 0 deleted
  Phase 2 negotiations in progress: 0

    Negotiation type: Quick mode, Role: Initiator, Message ID:0
    Local: 80.1.1.1:500, Remote: 80.1.1.5:500
    Local identity: roffice1
    Remote identity: 80.1.1.5
    Flags: IKE SA is created
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
roffice1> show security ipsec sa detail
  ID: 131076 Virtual-system: root, VPN Name: TO-RO2
  Local Gateway: 80.1.1.1, Remote Gateway: 80.1.1.5
  Local Identity: ipv4_subnet(any:0,[0..7]=0.0.0.0/0)
  Remote Identity: ipv4_subnet(any:0,[0..7]=0.0.0.0/0)
  Version: IKEv1
    DF-bit: clear
    Bind-interface: st0.0

  Port: 500, Nego#: 20, Fail#: 0, Def-Del#: 0 Flag: 0x600a29
  Last Tunnel Down Reason: Lifetime expired
    Direction: inbound, SPI: 2e4dae4, AUX-SPI: 0
                                , VPN Monitoring: -
    Hard lifetime: Expires in 2342 seconds
    Lifesize Remaining:  Unlimited
    Soft lifetime: Expires in 1703 seconds
    Mode: Tunnel(0 0), Type: dynamic, State: installed
    Protocol: ESP, Authentication: hmac-sha1-96, Encryption: aes-cbc (128
bits)
    Anti-replay service: counter-based enabled, Replay window size: 64

    Direction: outbound, SPI: a6cfeadd, AUX-SPI: 0
                                , VPN Monitoring: -
    Hard lifetime: Expires in 2342 seconds
    Lifesize Remaining:  Unlimited
    Soft lifetime: Expires in 1703 seconds
    Mode: Tunnel(0 0), Type: dynamic, State: installed
    Protocol: ESP, Authentication: hmac-sha1-96, Encryption: aes-cbc (128
bits)
    Anti-replay service: counter-based enabled, Replay window size: 64
```

```
roffice1> ping 11.11.11.2 count 1
PING 11.11.11.2 (11.11.11.2): 56 data bytes
64 bytes from 11.11.11.2: icmp_seq=0 ttl=64 time=7.160 ms

roffice1> show ospf neighbor
Address          Interface              State     ID               Pri  Dead
11.11.11.2       gr-0/0/0.0             Full      192.168.1.2      128    36
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
VR-DEVICE> ping routing-instance roffice1-trust 172.16.20.1 count 1
PING 172.16.20.1 (172.16.20.1): 56 data bytes
64 bytes from 172.16.20.1: icmp_seq=0 ttl=62 time=3.963 ms

roffice1> show security flow session protocol icmp
Session ID: 3586, Policy name: TRUST/5, Timeout: 2, Valid
  In: 172.16.10.1/0 --> 172.16.20.1/28262;icmp, If: ge-0/0/4.0, Pkts: 1,
Bytes: 84
  Out: 172.16.20.1/28262 --> 172.16.10.1/0;icmp, If: gr-0/0/0.0, Pkts: 1,
Bytes: 84
Total sessions: 1

roffice2> show security flow session protocol icmp
Session ID: 19360, Policy name: TRUST/7, Timeout: 2, Valid
  In: 172.16.10.1/1 --> 172.16.20.1/28263;icmp, If: gr-0/0/0.0, Pkts: 1,
Bytes: 84
  Out: 172.16.20.1/28263 --> 172.16.10.1/1;icmp, If: ge-0/0/4.0, Pkts: 1,
Bytes: 84
```

```
VR-DEVICE> ping routing-instance roffice2-trust 172.16.10.1
PING 172.16.10.1 (172.16.10.1): 56 data bytes
64 bytes from 172.16.10.1: icmp_seq=0 ttl=62 time=3.785 ms

roffice2> show security flow session protocol icmp
Session ID: 19386, Policy name: TRUST/7, Timeout: 4, Valid
  In: 172.16.20.1/14 --> 172.16.10.1/28274;icmp, If: ge-0/0/4.0, Pkts: 1,
Bytes: 84
  Out: 172.16.10.1/28274 --> 172.16.20.1/14;icmp, If: gr-0/0/0.0, Pkts: 1,
Bytes: 84

roffice1> show security flow session protocol icmp
Session ID: 3618, Policy name: TRUST/5, Timeout: 2, Valid
  In: 172.16.20.1/37 --> 172.16.10.1/28274;icmp, If: gr-0/0/0.0, Pkts: 1,
Bytes: 84
  Out: 172.16.10.1/28274 --> 172.16.20.1/37;icmp, If: ge-0/0/4.0, Pkts: 1,
Bytes: 84
```

2) You need to configure an IPsec VPN between hoffice and cluster nodes. You do not have access to the hoffice device and can only use CLI for troubleshooting. Here are the VPN parameters that were negotiated with the hoffice administrator:
    a. The hoffice security device uses statically assigned public IP address. It is always an initiator of the IPsec VPN and is configured in main mode. The IP address of hoffice gateway is unknown.
    b. IKE phase 1 proposal must include: preshared key “juniper”, DES, DH G1, MD5.
    c. IKE phase 2 proposal must include: DES, ESP, MD5.

© 2020 Juniper Networks, Inc. All rights reserved.

Device	Interface	IP address	Zone
central	st0.1	-	VPN

d. The IPsec VPN should provide access for all traffic types from the TRUST-H security zone to all TRUST security zones with the least possible number of policies
e. The remote device is prepared to negotiate Phase 2 and accept traffic using the 172.16.0.0/16 network
f. The central cluster must forward traffic into the IPsec VPN using the node that bears redundancy group primacy of the tunnel's endpoint interface.
g. You can add a static route to reach the TRUST zone of the home-office firewall

Note: For this task a single phase 2 SA is required so that the CENTRAL cluster device is able to forward and receive traffic between the local TRUST zones and the remote TRUST-HOME zone's networks.

Troubleshooting: The output of the 'show security ike sa' command should provide visibility of an attempt to initiate a connection. This only displays the remote address and not the local address to which the remote device is trying to connect to.

```
Index    State   Initiator cookie   Responder cookie   Mode              Remote
Address
```


© 2020 Juniper Networks, Inc. All rights reserved.

TROUBLESHOOTING IKE: Traceoptions for IKE will display a result similar to the below. This output identifies that the remote IP address is 200.1.1.100 which is trying to establish a connection to our IP address 80.1.1.16 that represents the loopback address.

Bear in mind that traceoptions for debugging purpose should immediately be deactivated after the required troubleshooting is performed to alleviate the burden on the control plane.

```
set security ike traceoptions file ike.log
set security ike traceoptions flag ike

80.1.1.16:500 (Responder) <-> 200.1.1.100:500 { 8daa6f31 37560e0e - 7d7cc373
0818b5b0 [-1] / 0x00000000 } IP; Error = No proposal chosen (14)
```

TROUBLESHOOTING FLOW: Traceoptions for Security Flow will observe an incoming packet and its path through flowd module. This allows to obtain the same information as above as an alternative approach. The packet filter is essential to trim the amount of information you will gather from this procedure.

Bear in mind that traceoptions for debugging purpose should immediately be deactivated after the required troubleshooting is performed to alleviate the burden on the control plane.

```
set security flow traceoptions file hoffice

set security flow traceoptions flag basic-datapath

set security flow traceoptions packet-filter hoffice source-prefix
200.1.1.100/32
```

IPsec tunnel and security policies:

```
{primary:node0}[edit]
lab@central-node0# show firewall family inet filter RE-PROTECT-v4 term IKE
from {
    port 500;
}
then {
    count IKE;
    accept;
}
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
{primary:node0}[edit]
lab@central-node0# show security zones security-zone UNTRUST interfaces lo0.0
host-inbound-traffic {
    system-services {
        ike;
    }
    protocols {
        bgp;
    }
}

{primary:node0}[edit]
lab@central-node0# show security ike
traceoptions {
    file ike.log;
    flag ike;
}
proposal IKE-PROP-HOFFICE {
    authentication-method pre-shared-keys;
    dh-group group1;
    authentication-algorithm md5;
    encryption-algorithm des-cbc;
}
policy IKE-POL-HOFFICE {
    mode main;
    proposals IKE-PROP-HOFFICE;
    pre-shared-key ascii-text "$9$IUwhyKX7V4aUM8aUjH5TRhS"; ## SECRET-DATA
}
gateway TO-HOFFICE {
    ike-policy IKE-POL-HOFFICE;
    address 200.1.1.100;
    external-interface lo0.0;
}

{primary:node0}[edit]
lab@central-node0# show security ipsec
proposal IPSEC-PROP-HOFFICE {
    protocol esp;
    authentication-algorithm hmac-md5-96;
    encryption-algorithm des-cbc;
}
policy IPSEC-POL-HOFFICE {
    proposals IPSEC-PROP-HOFFICE;
}
vpn TO-HOFFICE {
    bind-interface st0.1;
    ike {
        gateway TO-HOFFICE;
        proxy-identity {
            local 172.16.0.0/16;
            remote 172.16.77.0/24;
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
            service any;
        }
        ipsec-policy IPSEC-POL-HOFFICE;
    }
    establish-tunnels immediately;
}

{primary:node0}[edit]
lab@central-node0# show security address-book global | match trust
    address CENTRAL-TRUST 172.16.50.0/24;
    address RO1-TRUST 172.16.10.0/24;
    address RO2-TRUST 172.16.20.0/24;
    address EXA-TRUST 172.16.10.0/24;
    address HOFFICE-TRUST 172.16.77.0/24;
    address EXA-TRUST-OVERLAP 172.16.110.0/24;
    address RO1-TRUST-OVERLAP 172.16.111.0/24;
    address BUILDING-TRUST-B1 172.16.100.0/24;
    address BUILDING-TRUST-B2 172.16.200.0/24;
    address CENTRAL-TRUST-V6 2016:abcd:a1::/64;
    address RO1-TRUST-V6 2016:abcd:b1::/64;
    address RO2-TRUST-V6 2016:abcd:c1::/64;
    address EXA-TRUST-V6 2016:abcd:d1::/64;
    address-set TRUST-NETWORKS {
        address RO1-TRUST;
        address RO2-TRUST;
        address CENTRAL-TRUST;
        address HOFFICE-TRUST;
        address EXA-TRUST-OVERLAP;
        address RO1-TRUST-OVERLAP;
        address BUILDING-TRUST-B1;
        address BUILDING-TRUST-B2;
    address-set TRUST-NETWORKS-V6 {
        address CENTRAL-TRUST-V6;
        address RO1-TRUST-V6;
        address RO2-TRUST-V6;
        address EXA-TRUST-V6;

{primary:node0}[edit]
lab@central-node0# show security policies global
policy TRUST {
    match {
        source-address TRUST-NETWORKS;
        destination-address TRUST-NETWORKS;
        application any;
    }
    then {
        permit;
    }
}
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
{primary:node0}[edit]
lab@central-node0# show interfaces st0
unit 1 {
    family inet;
}

{primary:node0}[edit]
lab@central-node0# show routing-options static route 172.16.77.0/24
next-hop st0.1;

{primary:node0}[edit]
lab@central-node0# show security zones security-zone VPN
host-inbound-traffic {
    system-services {
        ping;
    }
}
interfaces {
    st0.1;
}
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
central-node1> show security ike sa index 10676259 detail
node1:
--------------------------------------------------------------------------
IKE peer 200.1.1.100, Index 10676259, Gateway Name: TO-HOME
  Role: Initiator, State: UP
  Initiator cookie: 464f583f76f1c912, Responder cookie: 8d05bc0bc7c0b4af
  Exchange type: Main, Authentication method: Pre-shared-keys
  Local: 80.1.1.16:500, Remote: 200.1.1.100:500
  Lifetime: Expires in 28781 seconds
  Peer ike-id: 200.1.1.100
  Xauth assigned IP: 0.0.0.0
  Algorithms:
   Authentication        : hmac-md5-96
   Encryption            : des-cbc
   Pseudo random function: hmac-md5
   Diffie-Hellman group  : DH-group-1
  Traffic statistics:
   Input  bytes  :                  560
   Output bytes  :                  772
   Input  packets:                    4
   Output packets:                    5
  Flags: IKE SA is created
  IPsec security associations: 1 created, 0 deleted
  Phase 2 negotiations in progress: 0

    Negotiation type: Quick mode, Role: Initiator, Message ID: 0
    Local: 80.1.1.16:500, Remote: 200.1.1.100:500
    Local identity: 80.1.1.16
    Remote identity: 200.1.1.100
    Flags: IKE SA is created
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
central-node1> show security ipsec sa detail index 268173316
node1:
--------------------------------------------------------------------------
  ID: 268173316 Virtual-system: root, VPN Name: TO-HOME
  Local Gateway: 80.1.1.16, Remote Gateway: 200.1.1.100
  Traffic Selector Name: trust-central
  Local Identity: ipv4(172.16.50.0-172.16.50.255)
  Remote Identity: ipv4(172.16.77.0-172.16.77.255)
  Version: IKEv1
    DF-bit: clear
    Bind-interface: st0.1

  Port: 500, Nego#: 0, Fail#: 0, Def-Del#: 0 Flag: 0x2c608b29
  Last Tunnel Down Reason: Peer Entry cleanup
    Direction: inbound, SPI: 57d3f0e6, AUX-SPI: 0
                               , VPN Monitoring: -
    Hard lifetime: Expires in 3573 seconds
    Lifesize Remaining:  Unlimited
    Soft lifetime: Expires in 2962 seconds
    Mode: Tunnel(0 0), Type: dynamic, State: installed
    Protocol: ESP, Authentication: hmac-md5-96, Encryption: des-cbc
    Anti-replay service: counter-based enabled, Replay window size: 64

    Direction: outbound, SPI: 7d5080e9, AUX-SPI: 0
                               , VPN Monitoring: -
    Hard lifetime: Expires in 3573 seconds
    Lifesize Remaining:  Unlimited
    Soft lifetime: Expires in 2962 seconds
    Mode: Tunnel(0 0), Type: dynamic, State: installed
    Protocol: ESP, Authentication: hmac-md5-96, Encryption: des-cbc
    Anti-replay service: counter-based enabled, Replay window size: 64
```

```
VR-DEVICE> ping routing-instance central-trust 172.16.77.1 count 1
PING 172.16.77.1 (172.16.77.1): 56 data bytes
64 bytes from 172.16.77.1: icmp_seq=1 ttl=63 time=3.182 ms

central-node1# run show security flow session protocol icmp
node0:
Session ID: 15294, Policy name: TRUST/22, State: Active, Timeout: 2, Valid
  In: 172.16.50.100/8 --> 172.16.77.1/29609;icmp, If: reth0.50, Pkts: 1,
Bytes: 84
  Out: 172.16.77.1/29609 --> 172.16.50.100/8;icmp, If: st0.1, Pkts: 1, Bytes:
84
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
VR-DEVICE> ping routing-instance home-office 172.16.50.10 count 1
PING 172.16.50.100 (172.16.50.100): 56 data bytes
64 bytes from 172.16.50.100: icmp_seq=17 ttl=63 time=3.871 ms

central-node1# run show security flow session protocol icmp
node0:
Session ID: 16541, Policy name: TRUST/22, State: Active, Timeout: 2, Valid
  In: 172.16.77.1/20 --> 172.16.50.100/29719;icmp, If: st0.1, Pkts: 0, Bytes:
84
  Out: 172.16.50.100/29719 --> 172.16.77.1/20;icmp, If: reth0.50, Pkts: 1,
Bytes: 84

xparent-node0# run show security flow session protocol icmp
node0:
Session ID: 184328, Policy name: TRUST/5, State: Active, Timeout: 2, Valid
  In: 172.16.77.1/10 --> 172.16.50.10/32870;icmp, If: reth0.50, Pkts: 1,
Bytes: 102
  Out: 172.16.50.10/32870 --> 172.16.77.1/10;icmp, If: reth1.50, Pkts: 1,
Bytes: 102
```

Traffic steering:

Notes: Looking at the existing policy and BGP revision notes, it is only required to add new terms to the existing policies already applied to the BGP group configuration. The BGP peers are advertising more prefixes that are significant to task 6.3 and require the same manipulation. The implementation should bear in mind the future requirements in order to avoid redundant work.

```
{primary:node0}[edit]
lab@central-node0# show policy-options policy-statement from-bgp9
term default {
    from {
        protocol bgp;
        route-filter 0.0.0.0/0 exact;
    }
    then {
        local-preference 200;
        accept;
    }
}
term specific {
    from {
        protocol bgp;
        route-filter 0.0.0.0/0 longer;
    }
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
    then accept;
}

{primary:node0}[edit]
lab@central-node0# show policy-options policy-statement from-bgp13
term default {
    from {
        protocol bgp;
        route-filter 0.0.0.0/0 exact;
    }
    then accept;
}
term specific {
    from {
        protocol bgp;
        route-filter 0.0.0.0/0 longer;
    }
    then {
        local-preference 200;
        accept;
    }
}

{primary:node0}[edit]
lab@central-node0# show policy-options policy-statement to-bgp9
term company {
    from {
        protocol aggregate;
        route-filter 80.1.1.0/24 exact;
    }
    then accept;
}
term lo0 {
    from {
        interface lo0.0;
        route-filter 80.1.1.16/32 exact;
    }
    then {
        as-path-prepend "1234 1234";
        accept;
    }
}

{primary:node0}[edit]
lab@central-node0# show policy-options policy-statement to-bgp13
term company {
    from {
        protocol aggregate;
        route-filter 80.1.1.0/24 exact;
    }
    then {
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
        as-path-prepend "1234 1234";
        accept;
    }
}
term lo0 {
    from {
        interface lo0.0;
        route-filter 80.1.1.16/32 exact;
    }
    then accept;
}
```

Verification

```
VR-DEVICE> ping 12.34.56.78 routing-instance central-trust count 1
PING 12.34.56.78 (12.34.56.78): 56 data bytes
64 bytes from 12.34.56.78: icmp_seq=0 ttl=63 time=3.210 ms

central-node0> show security flow session protocol icmp
node0:
--------------------------------------------------------------------------
Session ID: 16712, Policy name: TRUST/22, State: Active, Timeout: 2, Valid
  In: 172.16.77.1/3 --> 172.16.50.100/29735;icmp, If: st0.1, Pkts: 0, Bytes:
0
  Out: 172.16.50.100/29735 --> 172.16.77.1/3;icmp, If: reth0.50, Pkts: 1,
Bytes: 84

node1:
--------------------------------------------------------------------------
Session ID: 5460, Policy name: TRUST/22, State: Forward, Timeout: 4, Valid
  In: 172.16.77.1/0 --> 172.16.50.100/29735;icmp, If: st0.1, Pkts: 1, Bytes:
84
  Out: 172.16.50.100/29735 --> 172.16.77.1/0;icmp, If: reth0.50, Pkts: 0,
Bytes: 0
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
central-node0> show bgp summary | find 80.1.1.9
80.1.1.9                4321        397        395       0       1     2:45:58
Establ
  inet.0: 1/5/5/0
80.1.1.13               4321        543        538       0       0     4:00:29
Establ
  inet.0: 4/5/5/0
80.1.1.17               8765        532        532       0       0     3:59:58
Establ
  bgp.l3vpn.0: 0/1/1/0
  l3vpn.inet.0: 0/1/1/0

central-node0> show route advertising-protocol bgp 80.1.1.9
inet.0: 47 destinations, 55 routes (47 active, 0 holddown, 0 hidden)
  Prefix                  Nexthop              MED     Lclpref    AS path
* 80.1.1.0/24             Self                                    I
* 80.1.1.16/32            Self                                    1234 1234
[1234] I

central-node0> show route advertising-protocol bgp 80.1.1.13
inet.0: 47 destinations, 55 routes (47 active, 0 holddown, 0 hidden)
  Prefix                  Nexthop              MED     Lclpref    AS path
* 80.1.1.0/24             Self                                    1234 1234
[1234] I
* 80.1.1.16/32            Self                                    I
```

```
central-node0> show interfaces fab0 | match rate
  Input rate     : 2896 bps (2 pps)
  Output rate    : 2800 bps (2 pps)

VR-DEVICE> ping routing-instance home-office 172.16.50.100 rapid count 10000
PING 172.16.50.100 (172.16.50.100): 56 data bytes
!!!!!!!!!!!!!!!!!!! ^C

central-node0> show interfaces fab0 | match rate
  Input rate     : 278224 bps (200 pps)
  Output rate    : 134320 bps (198 pps)
```

3) The roffice2 and exa-fw security devices need to be connected to the cluster node as spokes of the hub-and-spoke VPN. Here are VPN parameters that must be used for the configuration:
    a. Only one st0 interface per security device can be used for the IPsec tunnel(s) termination.

© 2020 Juniper Networks, Inc. All rights reserved.

b. Configure the interfaces on every device according to the table below:

Device	Interface	IP address	Zone
roffice2	st0.0	11.0.0.2/28	VPN
exa-fw	st0.0	11.0.0.3/28	VPN
central	st0.0	11.0.0.4/28	VPN

c. Configure static NAT on exa-fw and cluster to solve the issue of overlapping subnets in the security zone TRUST-EXA and TRUST-RO1. Use the subnet 172.16.110.0/24 to reach the TRUST-EXA security zone network and 172.16.111.0/24 to reach the TRUST-RO1 security zone network. You can use up to two static routes.
d. Validate data path with VPN monitor option. The keepalives should be sent to the neighboring peer regardless of traffic patterns with 5 sec intervals. It is allowed to miss only 3 consecutive keepalives after which the tunnel is considered inactive.
e. IKE phase 1 proposal must include: preshared key “juniper”, AES128, DH G2, SHA1. Rekey phase 1 every 16 hours.
f. IKE phase 2 proposal must include: AES192, ESP, SHA1. Rekey phase 2 on transmission of 100 MB of traffic.
g. Configure internal BGP in the central cluster, roffice2 and exa-fw. Advertise internal network reachability using a single prefix from the central cluster.
h. Ensure all your TRUST networks from any device can communicate with each other. You must not use static routes.
i. Ensure the VPN traffic traverses the cluster member that owns priority of the VPN’s termination interface

IPSEC Note: All host-based services such as IPsec VPN should terminate in an logical interface associated with a redundancy group when in cluster mode. Although it is possible to terminate tunnels in physical interfaces this is not supported, not recommended nor a best practice.

IPsec tunnels:

Central-node0:

```
{primary:node0}[edit]
lab@central-node0# show security ike | no-more
proposal IKE-PROP-HUB-SPOKE {
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
    authentication-method pre-shared-keys;
    dh-group group2;
    authentication-algorithm sha1;
    encryption-algorithm aes-128-cbc;
    lifetime-seconds 57600;
}
proposal IKE-PROP-HOFFICE {
    authentication-method pre-shared-keys;
    dh-group group1;
    authentication-algorithm md5;
    encryption-algorithm des-cbc;
}
policy IKE-POL-HUB-SPOKE {
    mode main;
    proposals IKE-PROP-HUB-SPOKE;
    pre-shared-key ascii-text "$9$sY2oGzF/u0I69xdbsJZn/Cu1h"; ## SECRET-DATA
}
policy IKE-POL-HOFFICE {
    mode main;
    proposals IKE-PROP-HOFFICE;
    pre-shared-key ascii-text "$9$rW-eMXaJD.mTUj1hSr8LGDi.5F"; ## SECRET-DATA
}
gateway TO-ROFFICE2 {
    ike-policy IKE-POL-HUB-SPOKE;
    address 80.1.1.5;
    external-interface lo0.0;
}
gateway TO-EXA {
    ike-policy IKE-POL-HUB-SPOKE;
    address 100.1.1.1;
    external-interface lo0.0;
}
gateway TO-HOFFICE {
    ike-policy IKE-POL-HOFFICE;
    address 200.1.1.100;
    external-interface lo0.0;
}

{primary:node0}[edit]
lab@central-node0# show security ipsec | no-more
vpn-monitor-options {
    interval 5;
    threshold 3;
}
proposal IPSEC-PROP-HUB-SPOKE {
    protocol esp;
    authentication-algorithm hmac-sha1-96;
    encryption-algorithm aes-192-cbc;
    lifetime-kilobytes 100000;
}
proposal IPSEC-PROP-HOFFICE {
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
    protocol esp;
    authentication-algorithm hmac-md5-96;
    encryption-algorithm des-cbc;
}
policy IPSEC-POL-HUB-SPOKE {
    proposals IPSEC-PROP-HUB-SPOKE;
}
policy IPSEC-POL-HOFFICE {
    proposals IPSEC-PROP-HOFFICE;
}
vpn TO-ROFFICE2 {
    bind-interface st0.0;
    vpn-monitor;
    ike {
        gateway TO-ROFFICE2;
        ipsec-policy IPSEC-POL-HUB-SPOKE;
    }
    establish-tunnels immediately;
}
vpn TO-EXA {
    bind-interface st0.0;
    vpn-monitor;
    ike {
        gateway TO-EXA;
        ipsec-policy IPSEC-POL-HUB-SPOKE;
    }
    establish-tunnels immediately;
}
vpn TO-HOFFICE {
    bind-interface st0.1;
    ike {
        gateway TO-HOFFICE;
        proxy-identity {
            local 172.16.0.0/16;
            remote 172.16.77.0/24;
            service any;
        }
        ipsec-policy IPSEC-POL-HOFFICE;
    }
    establish-tunnels immediately;}

{primary:node0}[edit]
lab@central-node0# show interfaces st0
unit 0 {
    multipoint;
    family inet {
        address 11.0.0.4/28;
    }
}
unit 1 {
    family inet;
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
}
{primary:node0}[edit]
lab@central-node0# show security zones security-zone VPN
host-inbound-traffic {
    system-services {
        ping;
    }
}
interfaces {
    st0.1;
    st0.0
    }
}
```

Roffice2

```
[edit]
lab@roffice2# show security ike | no-more
proposal IKE-PROP-ROFFICE {
    authentication-method pre-shared-keys;
    dh-group group1;
    authentication-algorithm md5;
    encryption-algorithm 3des-cbc;
    lifetime-seconds 14400;
}
proposal IKE-PROP-HUB-SPOKE {
    authentication-method pre-shared-keys;
    dh-group group2;
    authentication-algorithm sha1;
    encryption-algorithm aes-128-cbc;
    lifetime-seconds 57600;
}
policy IKE-POL-ROFFICE {
    mode aggressive;
    proposals IKE-PROP-ROFFICE;
    pre-shared-key ascii-text "$9$xkZNVYq.5n6AfTeWLxwsP5QnCu"; ## SECRET-DATA
}
policy IKE-POL-HUB-SPOKE {
    mode main;
    proposals IKE-PROP-HUB-SPOKE;
    pre-shared-key ascii-text "$9$sY2oGzF/u0I69xdbsJZn/Cu1h"; ## SECRET-DATA
}
gateway TO-RO1 {
    ike-policy IKE-POL-ROFFICE;
    dynamic hostname roffice1;
    external-interface ge-0/0/3;
}
gateway TO-CENTRAL {
    ike-policy IKE-POL-HUB-SPOKE;
    address 80.1.1.16;
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
    external-interface ge-0/0/3;
}

[edit]
lab@roffice2# show security ipsec | no-more
vpn-monitor-options {
    interval 5;
    threshold 3;
}
proposal IPSEC-PROP-ROFFICE {
    protocol esp;
    authentication-algorithm hmac-sha1-96;
    encryption-algorithm aes-128-cbc;
    lifetime-seconds 3600;
}
proposal IPSEC-PROP-HUB-SPOKE {
    protocol esp;
    authentication-algorithm hmac-sha1-96;
    encryption-algorithm aes-192-cbc;
    lifetime-kilobytes 100000;
}
policy IPSEC-POL-ROFFICE {
    perfect-forward-secrecy {
        keys group2;
    }
    proposals IPSEC-PROP-ROFFICE;
}
policy IPSEC-POL-HUB-SPOKE {
    proposals IPSEC-PROP-HUB-SPOKE;
}
vpn TO-RO1 {
    bind-interface st0.1;
    ike {
        gateway TO-RO1;
        ipsec-policy IPSEC-POL-ROFFICE;
    }
}
vpn TO-CENTRAL {
    bind-interface st0.0;
    vpn-monitor;
    ike {
        gateway TO-CENTRAL;
        ipsec-policy IPSEC-POL-HUB-SPOKE;
    }
    establish-tunnels immediately;
}

[edit]
lab@roffice2# show interfaces st0
unit 0 {
    family inet {
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
        address 11.0.0.2/28;
    }
}
unit 1 {
    family inet {
        address 11.11.0.2/30;
    }
}

[edit]
lab@roffice2# show security zones security-zone VPN
host-inbound-traffic {
    system-services {
        ping;
    }
}
interfaces {
    st0.1;
    st0.0;
    gr-0/0/0.0 {
        host-inbound-traffic {
            protocols {
                ospf;
            }
        }
    }
}
```

Exa-fw

```
[edit]
lab@exa-fw# show security ike | no-more
proposal IKE-PROP-HUB-SPOKE {
    authentication-method pre-shared-keys;
    dh-group group2;
    authentication-algorithm sha1;
    encryption-algorithm aes-128-cbc;
    lifetime-seconds 57600;
}
policy IKE-POL-HUB-SPOKE {
    mode main;
    proposals IKE-PROP-HUB-SPOKE;
    pre-shared-key ascii-text "$9$sY2oGzF/u0I69xdbsJZn/Cu1h"; ## SECRET-DATA
}
gateway TO-CENTRAL {
    ike-policy IKE-POL-HUB-SPOKE;
    address 80.1.1.16;
    external-interface ge-0/0/3;
}
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
[edit]
lab@exa-fw# show security ipsec | no-more
vpn-monitor-options {
    interval 5;
    threshold 3;
}
proposal IPSEC-PROP-HUB-SPOKE {
    protocol esp;
    authentication-algorithm hmac-sha1-96;
    encryption-algorithm aes-192-cbc;
    lifetime-kilobytes 100000;
}
policy IPSEC-POL-HUB-SPOKE {
    proposals IPSEC-PROP-HUB-SPOKE;
}
vpn TO-CENTRAL {
    bind-interface st0.0;
    vpn-monitor;
    ike {
        gateway TO-CENTRAL;
        ipsec-policy IPSEC-POL-HUB-SPOKE;
    }
    establish-tunnels immediately;
}

[edit]
lab@exa-fw# show interfaces st0
unit 0 {
    family inet {
        address 11.0.0.3/28;
    }
}

[edit]
lab@exa-fw# show security zones security-zone VPN
interfaces {
    st0.0;
}
```

Static NAT:

Central

```
{primary:node0}[edit]
lab@central-node0# show security nat static rule-set OVERLAP
from interface st0.0;
rule trust-ro1 {
    match {
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
        destination-address 172.16.111.0/24;
    }
    then {
        static-nat {
            prefix {
                172.16.10.0/24;
            }
        }
    }
}
```

EXA-FW

```
[edit]
lab@exa-fw# show security nat static
rule-set OVERLAP {
    from interface st0.0;
    rule EXA-TRUST {
        match {
            destination-address 172.16.110.0/24;
        }
        then {
            static-nat {
                prefix {
                    172.16.10.0/24;
                }
            }
        }
    }
}
```

Internal BGP:

Central-node0:

```
{primary:node0}[edit]
lab@central-node0# show security zones security-zone VPN interfaces st0.0
host-inbound-traffic {
    protocols {
        bgp;
    }
}

{primary:node0}[edit]
lab@central-node0# show protocols bgp group internal
type internal;
export to-bgp-internal;
neighbor 11.0.0.3;
neighbor 11.0.0.2;
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
{primary:node0}[edit]
lab@central-node0# show routing-options aggregate
route 80.1.1.0/24 policy no-bgp;
route 172.16.0.0/16;

{primary:node0}[edit]
lab@central-node0# show policy-options policy-statement to-bgp-internal
term aggregate {
    from {
        protocol aggregate;
        route-filter 172.16.0.0/16 exact;
    }
    then accept;
}
```

Roffice2

```
[edit]
lab@roffice2# show security zones security-zone VPN interfaces st0.0
host-inbound-traffic {
    protocols {
        bgp;
    }
}

[edit]
lab@roffice2# show routing-options
static {
    route 0.0.0.0/0 next-hop 80.1.1.6;
    route 10.0.0.0/8 next-hop 10.10.1.254;
}
autonomous-system 1234;

[edit]
lab@roffice2# show protocols bgp group internal
type internal;
export to-bgp;
neighbor 11.0.0.4;

[edit]
lab@roffice2# show policy-options policy-statement to-bgp
term direct {
    from {
        protocol direct;
        route-filter 172.16.20.0/24 exact;
    }
    then accept;
}
term ospf {
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
    from {
        protocol ospf;
        route-filter 172.16.10.0/24 exact;
    }
    then accept;
}

[edit]
lab@roffice2# show policy-options policy-statement to-ospf
term bgp {
    from {
        protocol bgp;
        route-filter 172.16.0.0/16 exact;
    }
    then accept;
}

[edit]
lab@roffice2# show protocols ospf
export to-ospf;
area 0.0.0.0 {
    interface gr-0/0/0.0 {
        interface-type p2p;
    }
    interface ge-0/0/4.0 {
        passive;
    }
}
```

EXA-FW

```
[edit]
lab@exa-fw# show security zones security-zone VPN interfaces st0.0
host-inbound-traffic {
    protocols {
        bgp;
    }
}

[edit]
lab@exa-fw# show routing-options autonomous-system
1234;

[edit]
lab@exa-fw# show protocols bgp
group internal {
    type internal;
    neighbor 11.0.0.4;
}
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
central-node0> show bgp summary | mat "(11.0.0.2)|(11.0.0.3)"
11.0.0.2               1234        582        576       0       0     4:20:12
Establ
11.0.0.3               1234        574        570       0       1     4:17:27
Establ

VR-DEVICE> ping routing-instance building-trust-b1 172.16.77.1 count 1
PING 172.16.77.1 (172.16.77.1): 56 data bytes
64 bytes from 172.16.77.1: icmp_seq=0 ttl=62 time=6.207 ms

VR-DEVICE> ping routing-instance roffice1-trust 172.16.110.1 count 1
PING 172.16.110.1 (172.16.110.1): 56 data bytes
64 bytes from 172.16.110.1: icmp_seq=0 ttl=60 time=6.009 ms

VR-DEVICE> ping routing-instance exa-trust 172.16.50.10 count 1
PING 172.16.50.10 (172.16.50.10): 56 data bytes
64 bytes from 172.16.50.10: icmp_seq=0 ttl=62 time=6.243 ms

VR-DEVICE> ping routing-instance home-office 172.16.200.1 count 1
PING 172.16.200.1 (172.16.200.1): 56 data bytes
64 bytes from 172.16.200.1: icmp_seq=0 ttl=62 time=6.117 ms
```

4) Remote offices and the newly acquired company do not have native IPv6 Internet access so they have to go through the central location in a hub-and-spoke fashion.
    a. Central location uses native IPv6 BGP peering with existing neighbors
        i. Make sure peer #1 is preferred for incoming and outgoing traffic
        ii. Advertise the Enterprise IPv6 public prefix to these peers
    b. Use OSPFv3 between the sites for full reachability between the different IPv6 TRUST zones and HTTP reachability to the Internet.

© 2020 Juniper Networks, Inc. All rights reserved.

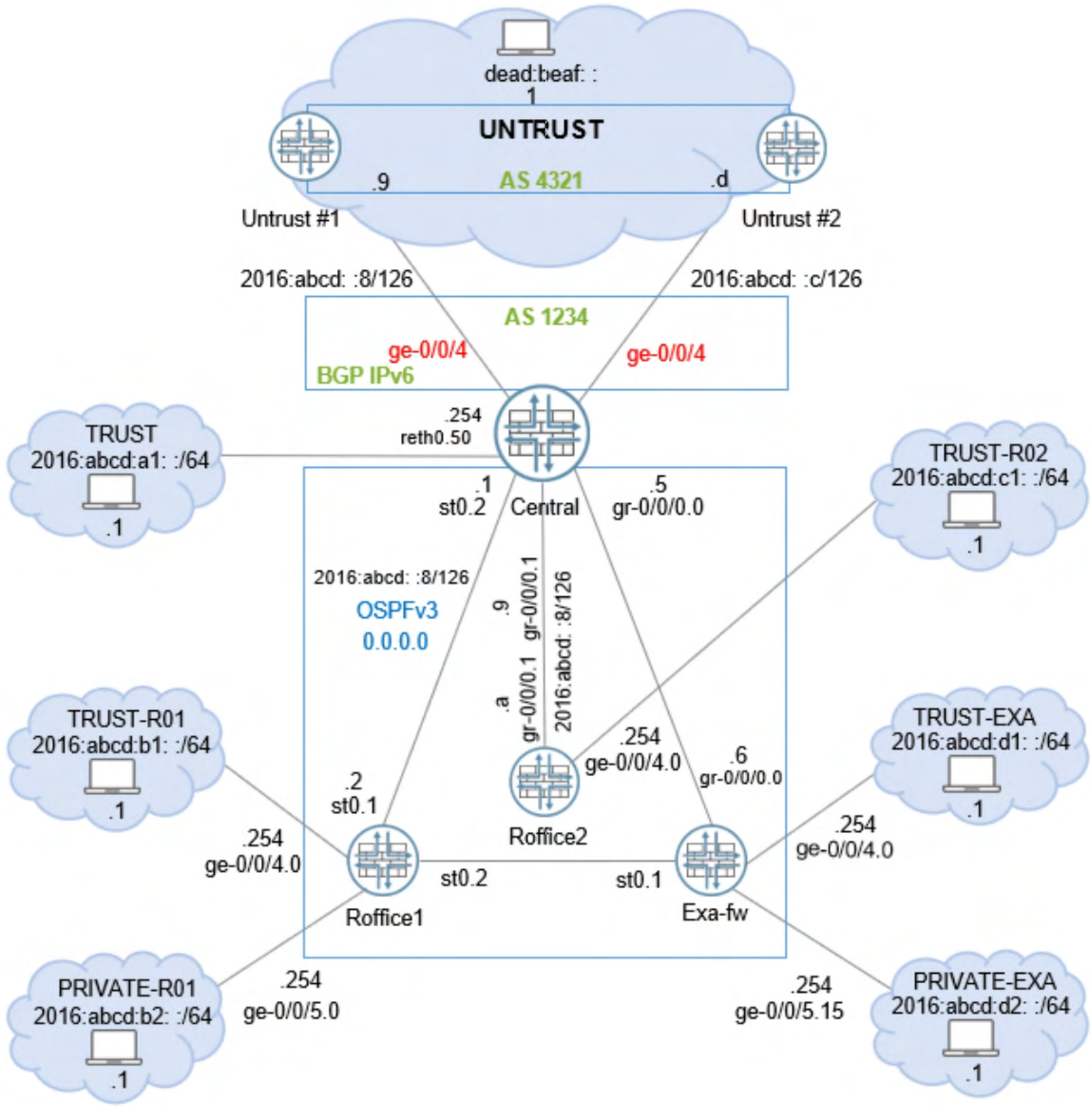


Figure 4: IPsec – VPNv6

Central Cluster:

```
{primary:node0}[edit]
lab@central-node0# show firewall family inet6 filter RE-PROTECT-v6 term BGP
from {
    prefix-list {
        bgp;
    }
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
    port bgp;
}
then {
    count BGP;
    accept;
}

{primary:node0}[edit]
lab@central-node0# show policy-options policy-statement from-bgp::d
term preference {
    then {
        local-preference 50;
        accept;
    }
}

{primary:node0}[edit]
lab@central-node0# show policy-options policy-statement to-bgp::9
term aggregate {
    from {
        protocol aggregate;
        route-filter 2016:abcd::/32 exact;
    }
    then accept;
}

{primary:node0}[edit]
lab@central-node0# show policy-options policy-statement to-bgp::d
term aggregate {
    from {
        protocol aggregate;
        route-filter 2016:abcd::/32 exact;
    }
    then {
        as-path-prepend "1234 1234 1234";
        accept;
    }
}

{primary:node0}[edit]
lab@central-node0# show policy-options policy-statement to-ospf3
term bgp {
    from {
        protocol bgp;
        route-filter ::/0 exact;
        route-type external;
    }
    then accept;
}
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
{primary:node0}[edit]
lab@central-node0# show protocols bgp group untrust-v6
type external;
peer-as 4321;
neighbor 2016:abcd::9 {
    export to-bgp::9;
}
neighbor 2016:abcd::d {
    import from-bgp::d;
    export to-bgp::d;
}
```

```
{primary:node0}[edit]
lab@central-node0# show protocols ospf3
export to-ospf3;
area 0.0.0.0 {
    interface st0.2 {
        interface-type p2p;
    }
    interface lo0.0 {
        passive;
    }
    interface gr-0/0/0.1 {
        interface-type p2p;
    }
    interface gr-0/0/0.0 {
        interface-type p2p;
    }
    interface reth0.50 {
        passive;
    }
}
```

```
{primary:node0}[edit]
lab@central-node0# show security address-book global | match V6
address CENTRAL-TRUST-V6 2016:abcd:a1::/64;
address RO1-TRUST-V6 2016:abcd:b1::/64;
address RO2-TRUST-V6 2016:abcd:c1::/64;
address EXA-TRUST-V6 2016:abcd:d1::/64;
address EXA-PRIVATE-V6 2016:abcd:d2::/64;
address ROFFICE1-PRIVATE-V6 2016:abcd:b2::/64;
address-set TRUST-NETWORKS-V6 {
    address CENTRAL-TRUST-V6;
    address RO1-TRUST-V6;
    address RO2-TRUST-V6;
    address EXA-TRUST-V6;
address-set PRIVATE-NETWORKS-V6 {
    address ROFFICE1-PRIVATE-V6;
    address EXA-PRIVATE-V6;
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
{primary:node0}[edit]
lab@central-node0# show security policies global | find INTERNET-V6
policy INTERNET-V6 {
    match {
        source-address TRUST-NETWORKS-V6;
        destination-address any;
        application junos-http;
    }
    then {
        permit;
    }
}
policy TRUST-V6 {
    match {
        source-address TRUST-NETWORKS-V6;
        destination-address TRUST-NETWORKS-V6;
        application any;
    }
    then {
        permit;
    }
}
```

Roffice1:

```
[edit]
lab@roffice1# show security policies global policy TRUST
match {
    source-address [ TRUST-NETWORKS TRUST-NETWORKS-V6 ];
    destination-address [ TRUST-NETWORKS TRUST-NETWORKS-V6 ];
    application any;
}
then {
    permit;
}

[edit]
lab@roffice1# show security policies from-zone TRUST-RO1 to-zone VPN policy INTERNET-V6
match {
    source-address RO1-TRUST-V6;
    destination-address any;
    application junos-http;
}
then {
    permit;
}

[edit]
lab@roffice1# show security address-book global | match V6
address RO1-TRUST-V6 2016:abcd:b1::/64;
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
address RO2-TRUST-V6 2016:abcd:c1::/64;
address EXA-TRUST-V6 2016:abcd:d1::/64;
address EXA-PRIVATE-V6 2016:abcd:d2::/64;
address ROFFICE1-PRIVATE-V6 2016:abcd:b2::/64;
address-set TRUST-NETWORKS-V6 {
    address RO1-TRUST-V6;
    address RO2-TRUST-V6;
    address EXA-TRUST-V6;
address-set PRIVATE-NETWORKS-V6 {
    address ROFFICE1-PRIVATE-V6;
    address EXA-PRIVATE-V6;

[edit]
lab@roffice1# show protocols ospf3
area 0.0.0.0 {
    interface st0.1 {
        interface-type p2p;
    }
    interface lo0.0 {
        passive;
    }
    interface ge-0/0/4.0 {
        passive;
    }
}
```

Roffice2:

```
[edit]
lab@roffice2# show security policies global policy TRUST
match {
    source-address [ TRUST-NETWORKS TRUST-NETWORKS-V6 ];
    destination-address [ TRUST-NETWORKS TRUST-NETWORKS-V6 ];
    application any;
}
then {
    permit;
}

[edit]
lab@roffice2# show security policies from-zone TRUST-RO2 to-zone VPN
policy INTERNET-V6 {
    match {
        source-address RO2-TRUST-V6;
        destination-address any;
        application junos-http;
    }
    then {
        permit;
    }
}
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
[edit]
lab@roffice2# show security address-book global | match V6
address RO1-TRUST-V6 2016:abcd:b1::/64;
address RO2-TRUST-V6 2016:abcd:c1::/64;
address EXA-TRUST-V6 2016:abcd:d1::/64;
address EXA-PRIVATE-V6 2016:abcd:d2::/64;
address ROFFICE1-PRIVATE-V6 2016:abcd:b2::/64;
address-set TRUST-NETWORKS-V6 {
    address RO1-TRUST-V6;
    address RO2-TRUST-V6;
    address EXA-TRUST-V6;
address-set PRIVATE-NETWORKS-V6 {
    address ROFFICE1-PRIVATE-V6;
    address EXA-PRIVATE-V6;

[edit]
lab@roffice2# show protocols ospf3
area 0.0.0.0 {
    interface gr-0/0/0.1 {
        interface-type p2p;
    }
    interface lo0.0 {
        passive;
    }
    interface ge-0/0/4.0 {
        passive;
    }
}
```

exa-fw:

```
[edit]
lab@exa-fw# show security policies global policy TRUST
match {
    source-address [ TRUST-NETWORKS TRUST-NETWORKS-V6 ];
    destination-address [ TRUST-NETWORKS TRUST-NETWORKS-V6 ];
    application any;
}
then {
    permit;
}

[edit]
lab@exa-fw# show security policies from-zone TRUST-EXA to-zone VPN
policy INTERNET-V6 {
    match {
        source-address EXA-TRUST-V6;
        destination-address any;
        application junos-http;
    }
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
    then {
        permit;
    }
}

[edit]
lab@exa-fw# show security address-book global | match V6
address RO1-TRUST-V6 2016:abcd:b1::/64;
address RO2-TRUST-V6 2016:abcd:c1::/64;
address EXA-TRUST-V6 2016:abcd:d1::/64;
address EXA-PRIVATE-V6 2016:abcd:d2::/64;
address ROFFICE1-PRIVATE-V6 2016:abcd:b2::/64;
address-set TRUST-NETWORKS-V6 {
    address RO1-TRUST-V6;
    address RO2-TRUST-V6;
    address EXA-TRUST-V6;
address-set PRIVATE-NETWORKS-V6 {
    address EXA-PRIVATE-V6;
    address ROFFICE1-PRIVATE-V6;

[edit]
lab@exa-fw# show protocols ospf3
area 0.0.0.0 {
    interface gr-0/0/0.0 {
        interface-type p2p;
    }
    interface lo0.0 {
        passive;
    }
    interface ge-0/0/4.0 {
        passive;
    }
}
```


© 2020 Juniper Networks, Inc. All rights reserved.

5) Create and update existing interfaces with the following IPv6 addresses. Make sure all interfaces respond to ping requests.

Device	Interface	IPv6 address	Zone
roffice1	lo0.0	2016:abcd:ffff::2/64	UNTRUST
roffice1	ge-0/0/4.0	2016:abcd:b1::254/64	TRUST-RO1
roffice1	ge-0/0/5.0	2016:abcd:b2::254/64	PRIVATE-RO1
roffice1	st0.1	2016:abcd:eeee::2/126	VPN
roffice1	st0.2	-	VPN
roffice2	lo0.0	2016:abcd:ffff::3/64	UNTRUST
roffice2	ge-0/0/4.0	2016:abcd:c1::254/64	TRUST-RO2
roffice2	gr-0/0/0.1	2016:abcd:ffff::254/64	VPN
exa-fw	lo0.0	2016:abcd:ffff::4/64	UNTRUST
exa-fw	ge-0/0/4.0	2016:abcd:d1::254/64	TRUST-EXA
exa-fw	ge-0/0/5.15	2016:abcd:d2::254/64	PRIVATE-EXA
exa-fw	gr-0/0/0.0	2016:abcd:eeee::a/126	VPN
exa-fw	st0.1	-	VPN
central	lo0.0	2016:abcd:ffff::1/64	UNTRUST
central	ge-0/0/3.0	2016:abcd:aa01::a/126	UNTRUST
central	ge-7/0/3.0	2016:abcd:aa01::e/126	UNTRUST
central	reth0.50	2016:abcd:a1::254/126	TRUST
central	st0.2	2016:abcd:eeee::1/126	VPN
central	gr-0/0/0.0	2016:abcd:eeee::5/126	VPN
central	gr-0/0/0.1	2016:abcd:eeee::9/126	VPN

Central Cluster

```
{primary:node0}[edit]
lab@central-node0# show interfaces gr-0/0/0
unit 0 {
    family inet6 {
        address 2016:abcd:eeee::9/126;
    }
}
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
unit 1 {
    family inet6 {
        address 2016:abcd:eeee::5/126;
    }
}

{primary:node0}[edit]
lab@central-node0# show interfaces ge-0/0/3
unit 0 {
    family inet {
        address 80.1.1.10/30;
    }
    family inet6 {
        address 2016:abcd::a/126;
    }
}

{primary:node0}[edit]
lab@central-node0# show interfaces ge-7/0/3
unit 0 {
    family inet {
        address 80.1.1.14/30;
    }
    family inet6 {
        address 2016:abcd::e/126;
    }
}

{primary:node0}[edit]
lab@central-node0# show interfaces reth0.50
vlan-id 50;
family inet {
    address 172.16.50.254/24;
}
family inet6 {
    address 2016:abcd:a1::254/64;
}

{primary:node0}[edit]
lab@central-node0# show interfaces lo0.0
family inet {
    filter {
        input RE-PROTECT-v4;
    }
    address 80.1.1.16/32 {
        primary;
    }
    address 192.168.1.3/32;
}
family inet6 {
    filter {
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
        input RE-PROTECT-v6;
    }
    address 2016:abcd:ffff::1/128;
}

{primary:node0}[edit]
lab@central-node0# show interfaces st0.2
family inet6 {
    address 2016:abcd::1/126;
}

{primary:node0}[edit]
lab@central-node0# show security zones security-zone VPN interfaces | find st0.2
st0.2 {
    host-inbound-traffic {
        protocols {
            ospf3;
        }
    }
}
gr-0/0/0.1 {
    host-inbound-traffic {
        protocols {
            ospf3;
        }
    }
}
gr-0/0/0.0 {
    host-inbound-traffic {
        protocols {
            ospf3;
        }
    }
}

{primary:node0}[edit]
lab@central-node0# show firewall family inet6 filter RE-PROTECT-v6 term ICMP
from {
    icmp-type [ echo-reply echo-request neighbor-advertisement neighbor-solicit ];
}
then {
    count ICMP;
    accept;
}
```

Roffice1:

```
[edit]
lab@roffice1# show interfaces ge-0/0/4
unit 0 {
    family inet {
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
        address 172.16.10.254/24;
    }
    family inet6 {
        address 2016:abcd:b1::254/64;
    }
}

[edit]
lab@roffice1# show interfaces ge-0/0/5
vlan-tagging;
unit 0 {
    vlan-id 111;
    family inet {
        address 172.16.11.254/24;
    }
    family inet6 {
        address 2016:abcd:b2::254/64;
    }
}

[edit]
lab@roffice1# show interfaces lo0
unit 0 {
    family inet {
        filter {
            input RE-PROTECT-v4;
        }
        address 192.168.1.1/32;
    }
    family inet6 {
        filter {
            input RE-PROTECT-v6;
        }
        address 2016:abcd:ffff::2/128;
    }
}

[edit]
lab@roffice1# show interfaces st0 | find "unit 1"
unit 1 {
    family inet6 {
        address 2016:abcd::2/126;
    }
}
unit 2 {
    family inet6;
}

[edit]
lab@roffice1# show security zones security-zone VPN interfaces | find st0.1
st0.1 {
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
    host-inbound-traffic {
        protocols {
            ospf3;
        }
    }
}
st0.2;

[edit]
lab@roffice1# show firewall family inet6 filter RE-PROTECT-v6 term ICMP
from {
    icmp-type [ echo-reply echo-request neighbor-advertisement neighbor-solicit ];
}
then {
    count ICMP;
    accept;
}
```

Roffice2:

```
[edit]
lab@roffice2# show interfaces ge-0/0/4
vlan-tagging;
unit 0 {
    vlan-id 210;
    family inet {
        address 172.16.20.254/24;
    }
    family inet6 {
        address 2016:abcd:c1::254/64;
    }
}

[edit]
lab@roffice2# show interfaces lo0
unit 0 {
    family inet {
        filter {
            input RE-PROTECT-v4;
        }
        address 192.168.1.2/32;
    }
    family inet6 {
        filter {
            input RE-PROTECT-v6;
        }
        address 2016:abcd:ffff::3/128;
    }
}
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
[edit]
lab@roffice2# show interfaces gr-0/0/0.1
family inet6 {
    address 2016:abcd::6/126;
}

[edit]
lab@roffice2# show security zones security-zone VPN interfaces | find gr-0/0/0.1
gr-0/0/0.1 {
    host-inbound-traffic {
        protocols {
            ospf3;
        }
    }
}

[edit]
lab@roffice2# show firewall family inet6 filter RE-PROTECT-v6 term ICMP
from {
    icmp-type [ echo-reply echo-request neighbor-advertisement neighbor-solicit ];
}
then {
    count ICMP;
    accept;
}
```

Exa-fw:

```
[edit]
lab@exa-fw# show interfaces gr-0/0/0
unit 0 {
    tunnel {
        source 11.0.0.3;
        destination 11.0.0.4;
    }
    family inet6 {
        address 2016:abcd::a/126;
    }
}

[edit]
lab@exa-fw# show interfaces ge-0/0/4
unit 0 {
    family inet {
        address 172.16.10.254/24;
    }
    family inet6 {
        address 2016:abcd:d1::254/64;
    }
}
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
[edit]
lab@exa-fw# show interfaces ge-0/0/5.15
vlan-id 15;
family inet {
    address 172.16.15.254/24;
}
family inet6 {
    address 2016:abcd:d2::254/64;
}

[edit]
lab@exa-fw# show interfaces lo0
unit 0 {
    family inet {
        filter {
            input RE-PROTECT-v4;
        }
        address 192.168.1.5/32;
    }
    family inet6 {
        filter {
            input RE-PROTECT-v6;
        }
        address 2016:abcd:ffff::4/128;
    }
}

[edit]
lab@exa-fw# show interfaces st0.1
family inet6;

[edit]
lab@exa-fw# show security zones security-zone VPN interfaces | find gr-0/0/0.0
gr-0/0/0.0 {
    host-inbound-traffic {
        protocols {
            ospf3;
        }
    }
}

[edit]
lab@exa-fw# show firewall family inet6 filter RE-PROTECT-v6 term ICMP
from {
    icmp-type [ echo-reply echo-request neighbor-advertisement neighbor-solicit ];
}
then {
    count ICMP;
    accept;
}
```


© 2020 Juniper Networks, Inc. All rights reserved.

Verification

```
central-node1# run ping count 1 2016:abcd:a1::1
PING6(56=40+8+8 bytes) 2016:abcd:a1::254 --> 2016:abcd:a1::1
16 bytes from 2016:abcd:a1::1, icmp_seq=0 hlim=64 time=18.855 ms

roffice1> ping count 1 2016:abcd:b2::1
PING6(56=40+8+8 bytes) 2016:abcd:b2::254 --> 2016:abcd:b2::1
16 bytes from 2016:abcd:b2::1, icmp_seq=0 hlim=64 time=9.006 ms

roffice2> ping count 1 2016:abcd:c1::1
PING6(56=40+8+8 bytes) 2016:abcd:c1::254 --> 2016:abcd:c1::1
16 bytes from 2016:abcd:c1::1, icmp_seq=0 hlim=64 time=6.875 ms

exa-fw> ping count 1 2016:abcd:d2::1
PING6(56=40+8+8 bytes) 2016:abcd:d2::254 --> 2016:abcd:d2::1
16 bytes from 2016:abcd:d2::1, icmp_seq=0 hlim=64 time=10.402 ms
```

6) Configure an IPv6 over IPv4 IPsec VPN between the roffice1 device and the central cluster
    a. Phase1 and Phase 2 should use basic proposals and PSK
    b. Roffice1's external address may change

Roffice1

```
[edit]
lab@roffice1# show security ike policy IKE-POL-BASIC
mode aggressive;
proposal-set basic;
pre-shared-key ascii-text "$9$pTmG01h7Nb4oGVw39ApREdbs4Zj"; ## SECRET-DATA

[edit]
lab@roffice1# show security ike gateway TO-CENTRAL
ike-policy IKE-POL-BASIC;
address 80.1.1.16;
local-identity hostname roffice1;
external-interface ge-0/0/3;

[edit]
lab@roffice1# show security ipsec policy IPSEC-POL-BASIC
proposal-set basic;
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
[edit]
lab@roffice1# show security ipsec vpn TO-CENTRAL
bind-interface st0.1;
ike {
    gateway TO-CENTRAL;
    ipsec-policy IPSEC-POL-BASIC;
}
establish-tunnels immediately;
```

Central Cluster

```
{primary:node0}[edit]
lab@central-node0# show security ike policy IKE-POL-BASIC
mode aggressive;
proposal-set basic;
pre-shared-key ascii-text "$9$pTmG01h7Nb4oGVw39ApREdbs4Zj"; ## SECRET-DATA

{primary:node0}[edit]
lab@central-node0# show security ike gateway TO-ROFFICE1
ike-policy IKE-POL-BASIC;
dynamic hostname roffice1;
external-interface lo0.0;

{primary:node0}[edit]
lab@central-node0# show security ipsec policy IPSEC-POL-BASIC
proposal-set basic;

{primary:node0}[edit]
lab@central-node0# show security ipsec vpn TO-ROFFICE1
bind-interface st0.2;
ike {
    gateway TO-ROFFICE1;
    ipsec-policy IPSEC-POL-BASIC;
}
```

7) Use existing IPsec VPNs between Roffice2, Exa and Central devices to propagate IPv6 traffic
    a. GRE tunnels have to be used with source and destination mapped to the IPsec interface addresses

Central Cluster

```
{primary:node0}[edit]
lab@central-node0# show interfaces gr-0/0/0
unit 0 {
    tunnel {
        source 11.0.0.4;
        destination 11.0.0.3;
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
    }
    family inet6 {
        address 2016:abcd:eeee::9/126;
    }
}
unit 1 {
    tunnel {
        source 11.0.0.4;
        destination 11.0.0.2;
    }
    family inet6 {
        address 2016:abcd:eeee::5/126;
    }
}

{primary:node0}[edit]
lab@central-node0# show routing-options
rib inet6.0 {
    aggregate {
        route 2016:abcd::/32;
    }
}
```

Roffice2

```
[edit]
lab@roffice2# show interfaces gr-0/0/0.1
tunnel {
    source 11.0.0.2;
    destination 11.0.0.4;
}
family inet6 {
    address 2016:abcd::6/126;
}
```

EXA-FW

```
[edit]
lab@exa-fw# show interfaces gr-0/0/0
unit 0 {
    tunnel {
        source 11.0.0.3;
        destination 11.0.0.4;
    }
    family inet6 {
        address 2016:abcd::a/126;
    }
}
```


© 2020 Juniper Networks, Inc. All rights reserved.

Verification

```
central-node0> show ospf3 neighbor
ID              Interface              State     Pri   Dead
192.168.1.5     gr-0/0/0.0             Full      128     32
  Neighbor-address fe80::42b4:f000:53:1080
192.168.1.2     gr-0/0/0.1             Full      128     37
  Neighbor-address fe80::42b4:f000:53:3e00
192.168.1.1     st0.2                  Full      128     38
  Neighbor-address fe80::42b4:f00f:fc53:1740
```

8) IPv6 private zones should have total access between roffice1 and exa-fw devices
    a. Create a new route-based VPN associated with the unnumbered tunnel interface from the table above
    b. Roffice1's external address may change
    c. Use previously created basic proposals and PSK

Roffice1

```
[edit]
lab@roffice1# show security ike gateway TO-EXA
ike-policy IKE-POL-BASIC;
address 100.1.1.1;
local-identity hostname roffice1;
external-interface ge-0/0/3.0;

[edit]
lab@roffice1# show security ipsec vpn TO-EXA
bind-interface st0.2;
ike {
    gateway TO-EXA;
    ipsec-policy IPSEC-POL-BASIC;
}
traffic-selector exa-private {
    local-ip 2016:abcd:b2::/64;
    remote-ip 2016:abcd:d2::/64;
}
establish-tunnels immediately;

[edit]
lab@roffice1# show security policies global policy PRIVATE-V6
match {
    source-address PRIVATE-NETWORKS-V6;
    destination-address PRIVATE-NETWORKS-V6;
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
    application any;
}
then {
    permit;
}
```

EXA-FW

```
[edit]
lab@exa-fw# show security ike policy IKE-POL-BASIC
mode aggressive;
proposal-set basic;
pre-shared-key ascii-text "$9$pTmG01h7Nb4oGVw39ApREdbs4Zj"; ## SECRET-DATA

[edit]
lab@exa-fw# show security ike gateway TO-ROFFICE1
ike-policy IKE-POL-BASIC;
dynamic hostname roffice1;
external-interface ge-0/0/3.0;

[edit]
lab@exa-fw# show security ipsec policy IPSEC-POl-BASIC
proposal-set basic;

[edit]
lab@exa-fw# show security ipsec vpn TO-ROFFICE1
bind-interface st0.1;
ike {
    gateway TO-ROFFICE1;
    ipsec-policy IPSEC-POl-BASIC;
}
traffic-selector roffice1-private {
    local-ip 2016:abcd:d2::/64;
    remote-ip 2016:abcd:b2::/64;
}

[edit]
lab@exa-fw# show security policies global policy PRIVATE-V6
match {
    source-address PRIVATE-NETWORKS-V6;
    destination-address PRIVATE-NETWORKS-V6;
    application any;
}
then {
    permit;
}
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
[edit]
lab@exa-fw# show security zones security-zone VPN
host-inbound-traffic {
    system-services {
        ping;
    }
}
interfaces {
    st0.0 {
        host-inbound-traffic {
            protocols {
                bgp;
            }
        }
    }
    gr-0/0/0.0 {
        host-inbound-traffic {
            protocols {
                ospf3;
            }
        }
    }
    st0.1 {
        host-inbound-traffic {
            protocols {
                ospf3;
            }
        }
    }
}
```

Verification

```
VR-DEVICE> ping count 1 routing-instance roffice1-private 2016:abcd:d2::1
PING6(56=40+8+8 bytes) 2016:abcd:b2::1 --> 2016:abcd:d2::1
16 bytes from 2016:abcd:d2::1, icmp_seq=0 hlim=62 time=15.713 ms

VR-DEVICE> ping count 1 routing-instance exa-private 2016:abcd:b2::1
PING6(56=40+8+8 bytes) 2016:abcd:d2::1 --> 2016:abcd:b2::1
16 bytes from 2016:abcd:b2::1, icmp_seq=0 hlim=62 time=6.273 ms
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
exa-fw> show security ike sa index 4789681 detail
IKE peer 80.1.1.1, Index 4789681, Gateway Name: TO-ROFFICE1
  Role: Responder, State: UP
  Initiator cookie: 6dc1ac552bdb1597, Responder cookie: 9eca3b65f57a2430
  Exchange type: Aggressive, Authentication method: Pre-shared-keys
  Local: 100.1.1.1:500, Remote: 80.1.1.1:500
  Lifetime: Expires in 17665 seconds
  Peer ike-id: roffice1
  Xauth assigned IP: 0.0.0.0
  Algorithms:
   Authentication        : hmac-sha1-96
   Encryption            : des-cbc
   Pseudo random function: hmac-sha1
   Diffie-Hellman group  : DH-group-1
Traffic statistics:
   Input  bytes  :                 2308
   Output bytes  :                 1380
   Input  packets:                   16
   Output packets:                    6
Flags: IKE SA is created
IPsec security associations: 5 created, 4 deleted
Phase 2 negotiations in progress: 0

Negotiation type: Quick mode, Role: Responder, Message ID: 0
   Local: 100.1.1.1:500, Remote: 80.1.1.1:500
   Local identity: 100.1.1.1
   Remote identity: roffice1
   Flags: IKE SA is created
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
exa-fw> show security ipsec sa index 268173313 detail
  ID: 268173313 Virtual-system: root, VPN Name: TO-ROFFICE1
  Local Gateway: 100.1.1.1, Remote Gateway: 80.1.1.1
  Traffic Selector Name: roffice1-private
  Local Identity: ipv6(2016:abcd:d2::-2016:abcd:d2:0:ffff:ffff:ffff:ffff)36
  Remote Identity: ipv6(2016:abcd:b2::-2016:abcd:b2:0:ffff:ffff:ffff:ffff)
  Version: IKEv1
    DF-bit: clear
    Bind-interface: st0.1

  Port: 500, Nego#: 6, Fail#: 0, Def-Del#: 0 Flag: 0x24608b29
  Last Tunnel Down Reason: Delete payload received
    Direction: inbound, SPI: 27e9c8a2, AUX-SPI: 0
                               , VPN Monitoring: -
    Hard lifetime: Expires in 1380 seconds
    Lifesize Remaining:  Unlimited
    Soft lifetime: Expires in 807 seconds
    Mode: Tunnel(0 0), Type: dynamic, State: installed
    Protocol: ESP, Authentication: hmac-sha1-96, Encryption: des-cbc
    Anti-replay service: counter-based enabled, Replay window size: 64

    Direction: outbound, SPI: ddfd465d, AUX-SPI: 0
                               , VPN Monitoring: -
    Hard lifetime: Expires in 1380 seconds
    Lifesize Remaining:  Unlimited
    Soft lifetime: Expires in 807 seconds
    Mode: Tunnel(0 0), Type: dynamic, State: installed
    Protocol: ESP, Authentication: hmac-sha1-96, Encryption: des-cbc
    Anti-replay service: counter-based enabled, Replay window size: 64
```


© 2020 Juniper Networks, Inc. All rights reserved.

Task 8: Attack Prevention and Mitigation

1) Ensure that roffice1 and roffice2 are protected against following attacks arriving from the Internet:
    a. The TCP SYN segments flooding with the following thresholds and timer values:
        i. The destination thresholds values of 10000 TCP SYN segments per second.
        ii. Ensure that security device starts SYN Proxy protection mechanism when TCP SYN segments arrival rate reaches 500 segments per second.
        iii. Ensure that security device generates an alarm when TCP SYN segments arrival rate reaches 2500 segments per second.
        iv. The maximum time before incomplete sessions are dropped should be 10 seconds.
    b. Protect against fragmented TCP SYN segments.
    c. Protect against UDP flooding with the threshold of 500 packets per second.

Roffice1 & Roffice2

```
[edit]
lab@roffice1# show security screen
ids-option SCREEN-UNTRUST {
    tcp {
        syn-frag;
        syn-flood {
            alarm-threshold 2500;
            attack-threshold 500;
            destination-threshold 10000;
            timeout 10;
        }
    }
    udp {
        flood threshold 500;
    }
}

[edit]
lab@roffice1# show security zones security-zone UNTRUST screen
screen SCREEN-UNTRUST;
```

2) Ensure that building1 and building2 are protected against the following reconnaissance attempts arriving from the INTERNAL security zone:

© 2020 Juniper Networks, Inc. All rights reserved.

a. IP address sweep and port scan both a detection rate of 10 packets arrived per 2 ms time interval.
b. Detect IP packets with following values in the Options field:
    v. Record-route option.
    vi. Timestamp option.
c. Protect against following operating systems probes:
    v. The TCP segment has both SYN and FIN flags set.
    vi. The TCP segment has no flags set.
d. Ensure that detection of malicious traffic results in alarm generation instead of dropping the packets belonging to malicious packet flow.

Building

```
[edit]
lab@building1# show security screen
ids-option SCREEN-INTERNAL {
    alarm-without-drop;
    icmp {
        ip-sweep threshold 2000;
    }
    ip {
        record-route-option;
        timestamp-option;
    }
    tcp {
        syn-fin;
        tcp-no-flag;
        port-scan threshold 2000;
    }
}

[edit]
lab@building1# show security zones | match "(internal)|(screen)"
security-zone INTERNAL-B1 {
    screen SCREEN-INTERNAL;
security-zone INTERNAL-B2 {
    screen SCREEN-INTERNAL;
```

3) Configure central cluster in such a way to protect server 172.16.60.205 and 172.16.60.206:
    a. The uploading of exe or rpm files to the 172.16.60.206 server via FTP is allowed only from the TRUST security zone and prohibited from everywhere else. Each detected attempt results in silently dropping client's sessions.
    b. Allow anonymous access to the FTP service of the 172.16.60.206 server from any TRUST and the TESTBED security zones. Restrict access for the rest of the network. Silently drop packets from unauthorized hosts, block

© 2020 Juniper Networks, Inc. All rights reserved.

them for 1 hour and generate log messages with severity level Major and alert flag.

c. Protect servers against scanning and worms from the INTERNAL and TESTBED security zones. Each detected attempt results in silently dropping packets.

```
{primary:node0}[edit]
lab@central-node0# show security idp
idp-policy CENTRAL-IDP {
    rulebase-ips {
        rule FILE-ATTACK {
            match {
            from-zone any;
            source-address any;
            to-zone WAREHOUSE;
            destination-address WAREHOUSE-SRV-206;
            application junos-ftp;
            attacks {
                custom-attacks FILE-ATTACK;
            }
        }
        then {
            action {
                drop-connection;
            }
        }
    }
    rule ANONYMOUS-ATTACK {
        match {
            from-zone any;
            source-address any;
            to-zone WAREHOUSE;
            destination-address WAREHOUSE-SRV-206;
            application junos-ftp;
            attacks {
                custom-attacks ANONYMOUS-ATTACK;
            }
        }
        then {
            action {
                drop-packet;
            }
            ip-action {
                ip-block;
                target source-address;
                timeout 3600;
            }
            notification {
                log-attacks {
                    alert;
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
            }
        }
    }
}
rule INTERNAL-SCAN-WORM-ATTACK {
    match {
        from-zone INTERNAL;
        source-address any;
        to-zone WAREHOUSE;
        destination-address [ WAREHOUSE-SRV-205 WAREHOUSE-SRV-206 ];
        attacks {
            dynamic-attack-groups SCAN-WORM;
        }
    }
    then {
        action {
            drop-packet;
        }
    }
}
rule TESTBED-SCAN-WORM-ATTACK {
    match {
        from-zone TESTBED;
        source-address any;
        to-zone WAREHOUSE;
        destination-address [ WAREHOUSE-SRV-205 WAREHOUSE-SRV-206 ];
        attacks {
            dynamic-attack-groups SCAN-WORM;
        }
    }
    then {
        action {
            drop-packet;
        }
    }
}
rulebase-exempt {
    rule FILE-ATTACK {
        match {
            from-zone TRUST;
            source-address any;
            to-zone WAREHOUSE;
            destination-address WAREHOUSE-SRV-206;
            attacks {
                custom-attacks FILE-ATTACK;
            }
        }
    }
    rule ANONYMOUS-TRUST {
        match {
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
        from-zone TRUST;
        source-address any;
        to-zone WAREHOUSE;
        destination-address WAREHOUSE-SRV-206;
        attacks {
            custom-attacks ANONYMOUS-ATTACK;
        }
    }
}
rule ANONYMOUS-TESTBED {
    match {
        from-zone TESTBED;
        source-address any;
        to-zone WAREHOUSE;
        destination-address WAREHOUSE-SRV-206;
        attacks {
            custom-attacks ANONYMOUS-ATTACK;
        }
    }
  }
}
active-policy CENTRAL-IDP;
custom-attack FILE-ATTACK {
    severity major;
    attack-type {
        chain {
            expression "exe or rpm";
            member exe {
                attack-type {
                    signature {
                        context ftp-put-filename;
                        pattern ".*\.\[exe\]";
                        direction client-to-server;
                    }
                }
            }
            member rpm {
                attack-type {
                    signature {
                        context ftp-put-filename;
                        pattern ".*\.\[rpm\]";
                        direction client-to-server;
                    }
                }
            }
        }
    }
}
custom-attack ANONYMOUS-ATTACK {
    severity major;
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
    attack-type {
        signature {
            context ftp-username;
            pattern "^anonymous$";
            direction client-to-server;
        }
    }
}
dynamic-attack-group SCAN-WORM {
    filters {
        category {
            values [ SCAN WORM ];
        }
    }
}

{primary:node0}[edit]
lab@central-node0# show security policies from-zone UNTRUST to-zone WAREHOUSE policy SERVERS
then
permit {
    destination-address {
        drop-untranslated;
    }
    application-services {
        idp;
    }
}

{primary:node0}[edit]
lab@central-node0# show security policies global policy WAREHOUSE
match {
    source-address any;
    destination-address CENTRAL-WAREHOUSE;
    application junos-ftp;
    to-zone WAREHOUSE;
}
then {
    permit {
        application-services {
            idp;
        }
    }
}

{primary:node0}[edit]
lab@central-node0# show security policies from-zone WAREHOUSE to-zone WAREHOUSE policy SERVERS
match {
    source-address any;
    destination-address [ WAREHOUSE-SRV-205 WAREHOUSE-SRV-206 ];
    application [ junos-http SQL junos-ssh junos-ftp ];
}
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
then {
    permit;
}
```

Verification

```
lab@central-node0> show security policies global policy-name WAREHOUSE detail
| match intrusion
  Intrusion Detection and Prevention: enabled

lab@vr-device> telnet routing-instance central-trust 172.16.60.205 port 21
Trying 172.16.60.205...
Connected to 172.16.60.205.
Escape character is '^]'.
220 vr-device FTP server (Version 6.00LS) ready.

lab@central-node0> show security flow session destination-port 21 | find
session
Session ID: 11164, Policy name: WAREHOUSE/7, State: Active, Timeout: 1734,
Valid
  In: 172.16.50.100/51698 --> 172.16.60.205/21;tcp, If: reth0.50, Pkts: 3,
Bytes: 124
  Out: 172.16.60.205/21 --> 172.16.50.100/51698;tcp, If: reth0.60, Pkts: 2,
Bytes: 131
Total sessions: 1
```

Task 9: Advanced Security – Central cluster

1) Disable application system cache completely.

```
{primary:node0}[edit]
lab@central-node0# show services application-identification
no-application-system-cache;
```


© 2020 Juniper Networks, Inc. All rights reserved.

Verification

```
{primary:node0}[edit]
lab@central-node0# run show services application-identification application-
system-cache
node0:
--------------------------------------------------------------------------
Application System Cache Configurations:
  application-cache: off
    Cache lookup for security-services: off
    Cache lookup for miscellaneous-services: on
  cache-entry-timeout: 3600 seconds
pic: 0/0
Logical system name: 0
IP address: 172.16.60.205                              Port: 21     Protocol:
TCP
Application: FTP                                       Encrypted: No
Classification Path: IP:TCP:FTP


node1:
--------------------------------------------------------------------------
Application System Cache Configurations:
  application-cache: off
    Cache lookup for security-services: off
    Cache lookup for miscellaneous-services: on
  cache-entry-timeout: 3600 seconds
```

2) Enable AppTrack to provide information about applications used in the TRUST zone. The first message for each connection has to be generated 2 minutes after the application has been identified and then an update has to be created every 6 minutes.

```
{primary:node0}[edit]
lab@central-node0# show security application-tracking
first-update-interval 2;
session-update-interval 6;

{primary:node0}[edit]
lab@central-node0# show security zones security-zone TRUST |find app
application-tracking;
```


© 2020 Juniper Networks, Inc. All rights reserved.

Verification

```
lab@central-node0> show services application-identification status | match
"(application)|(status)"
Application Identification
 Status                              Enabled
Application System Cache
 Status                              Disabled
 Negative cache status               Disabled
 Application package version         2648
 Status                              Active
 Status                              Not Applicable
```

3) Ensure the junos:MEGAUPLOAD application over the port 80 from the TRUST zone to the UNTRUST zone will have the loss priority of "high" if it crosses 5000 kb/s with bursts of 15000 bytes. This has to be applied in both directions - client to server and server to client.

```
{primary:node0}[edit]
lab@central-node0# show class-of-service
application-traffic-control {
    rate-limiters MEGA {
        bandwidth-limit 5000;
        burst-size-limit 15000;
    }
    rule-sets MEGA {
        rule rate {
            match {
                application junos:MEGAUPLOAD;
            }
            then {
                rate-limit {
                    client-to-server MEGA;
                    server-to-client MEGA;
                    loss-priority-high;
                }
            }
        }
    }
}

{primary:node0}[edit]
lab@central-node0# show security policies from-zone TRUST to-zone UNTRUST policy HTTP-FTP
match {
    source-address CENTRAL-TRUST;
    destination-address any;
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
    application [ junos-http junos-ftp ];
    dynamic-application junos:MSN;
}
then {
    permit {
        application-services {
            utm-policy CENTRAL-Content;
            application-traffic-control {
                rule-set MEGA;
            }
        }
    }
    log {
        session-init;
        session-close;
    }
}
```

Verification

```
lab@central-node0> show security policies from-zone TRUST to-zone UNTRUST
policy-name HTTP-FTP detail | match traffic
  Application traffic control: MEGA
```

4) Make sure the SRX knows exactly what is going on in the encrypted sessions on the default HTTPS port from the TESTBED zone to the UNTRUST zone. The certificate for signing the modified server certificates should be locally generated on the SRX device with following values:
   - type: rsa
   - key size: 512
   - domain name: juniper.net
   - subject: DC=JNPR,CN=juniper,OU=unit-1,O=juniper,SN=1234,L=USA,ST=CA,C=US
   - email-ID: noreply@juniper.net

   The SRX will not authenticate any servers. Make sure everything about SSL proxy operations is logged in the “ssl-proxy” file.

```
run request security pki generate-key-pair certificate-id MY-CERT
size 1024 type rsa

node0:
--------------------------------------------------------------------------
-----
Generated key pair MY-CERT, key size 1024 bits
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
run request security pki local-certificate generate-self-signed
certificate-id MY-CERT domain-name juniper.net subject
"DC=JNPR,CN=Juniper,OU=unit-1,O=Juniper,SN=1234,L=USA,ST=CA,C=US"
email noreply@juniper.net add-ca-constraint

node1:
--------------------------------------------------------------------
Self-signed certificate generated and loaded successfully
```

```
{primary:node0}[edit]
lab@central-node0# show services ssl
proxy {
    profile CENTRAL-SSL {
        root-ca MY-CERT;
        actions {
            ignore-server-auth-failure;
            log {
                all;
            }
        }
    }
}

{primary:node0}[edit]
lab@central-node0# show system syslog file ssl-proxy
any any;
match SSL;

{primary:node0}[edit]
lab@central-node0# show security policies from-zone TESTBED to-zone UNTRUST policy HTTPS
match {
    source-address CENTRAL-TESTBED;
    destination-address any;
    application junos-https;
}
then {
    permit {
        application-services {
            ssl-proxy {
                profile-name CENTRAL-SSL;
            }
        }
    }
}
```


© 2020 Juniper Networks, Inc. All rights reserved.

Verification

```
lab@central-node0> show security policies from-zone TESTBED to-zone UNTRUST
policy-name HTTPS detail | match ssl
  SSL Proxy Profile Name: CENTRAL-SSL

lab@central-node0> show services ssl proxy statistics
node0:
--------------------------------------------------------------------------
PIC:fwdd1 fpc[0] pic[0] ------
        sessions matched                          0
        sessions whitelisted                      0
        sessions bypassed:non-ssl                 0
        sessions bypassed:mem overflow            0
        sessions created                          0
        sessions ignored                          0
        sessions active                           0
        sessions dropped                          0
```

5) Remote Desktop Protocol traffic originated in the INTERNAL zone, leaving the Central Office should always travers interface ge-0/0/3.

```
{primary:node0}[edit]
lab@central-node0# show routing-options
interface-routes {
    rib-group inet apbr;
}
rib-groups {
    apbr {
        import-rib [ inet.0 apbr.inet.0 ];
        import-policy apbr;
    }
}

lab@central-node0# show policy-options policy-statement apbr
term 1 {
    from interface ge-0/0/3.0;
    to rib apbr.inet.0;
    then accept;
}
term 2 {
    then reject;
}
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
{primary:node0}[edit security zones security-zone INTERNAL]
lab@central-node0# show
...
advance-policy-based-routing-profile {
apbr;
}

lab@central-node0# show security advance-policy-based-routing
profile apbr {
    rule 1 {
        match {
            dynamic-application junos:RDP;
        }
        then {
            routing-instance apbr;
        }
    }
}

{primary:node0}[edit routing-instances apbr]
lab@central-node0# show
instance-type forwarding;
routing-options {
    static {
        route 0.0.0.0/0 {
            next-hop 80.1.1.9;
        }
    }
}

lab@central-node0# run show route table apbr
apbr.inet.0: 3 destinations, 4 routes (3 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

0.0.0.0/0          *[Static/5] 02:06:26
                    > to 80.1.1.13 via ge-7/0/3.0
                    [Static/7] 02:06:26
                    > to 80.1.1.9 via ge-0/0/3.0
80.1.1.8/30        *[Direct/0] 02:06:26
                    > via ge-0/0/3.0
```


© 2020 Juniper Networks, Inc. All rights reserved.

Task 10: Software Defined Secure Network (SDSN)

1) Create a new SkyATP realm. Enroll Policy Enforcer and the central office cluster in the newly created Sky ATP Realm through Security Director.

Use the information below to setup the Sky ATP Realm:

SkyATP Realm	jnciesec-xxx (where xxx is your lab username)
Username	jnciesec-xxx@stu.juniper.net
Password	lab123@Lab
Juniper SSO account	eduservicenow@gmail.com
Juniper SSO password	********

Use the information for Security Director and Policy Enforcer:

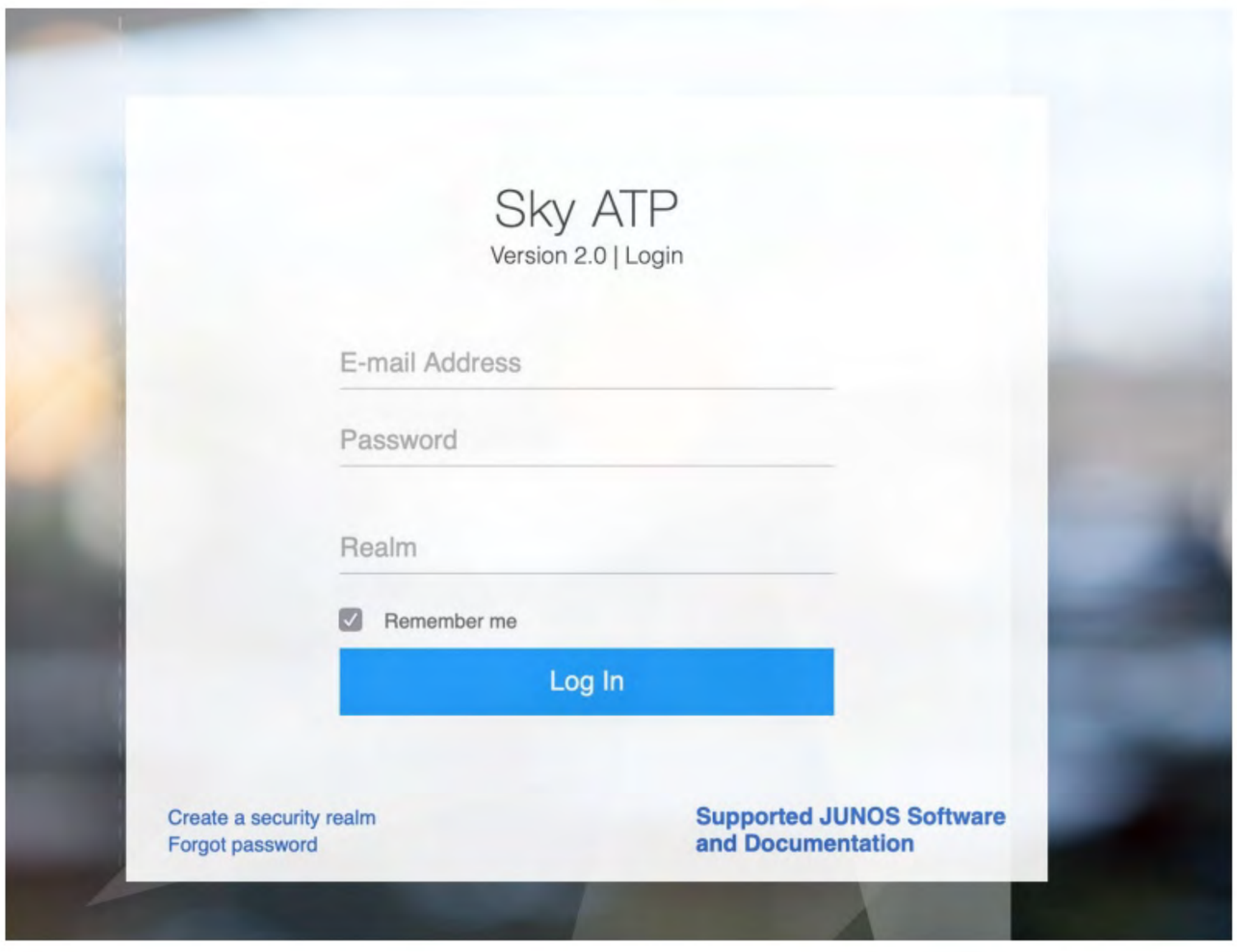
Security Director Username	super
Security Director Password	lab123@Lab
Security Director IP	10.10.1.100
Policy Enforcer Username	root
Policy Enforcer Password	lab123@Lab
Policy Enforcer IP	10.10.1.123

Note: The password for the Juniper SSO account is auto populated in the Firefox browser on the Student Desktop. For this reason, it is important to use the Firefox browser on the Student Desktop to create the Sky ATP realm.

© 2020 Juniper Networks, Inc. All rights reserved.

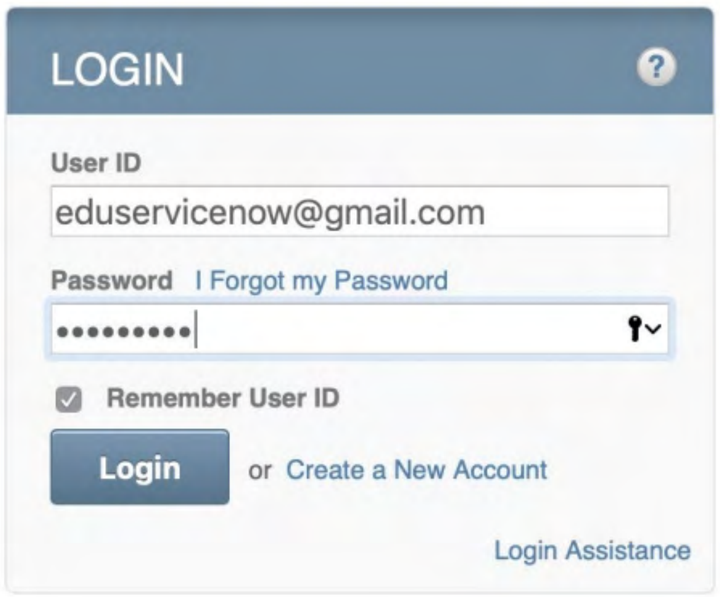
a) The first step is to create a new SkyATP realm. To do this you have to navigate to the following URL: http://amer.sky.junipersecurity.net using the Firefox browser of the Student Desktop.

Click on "**Create a security realm**" in the lower left corner of the Sky ATP login screen.



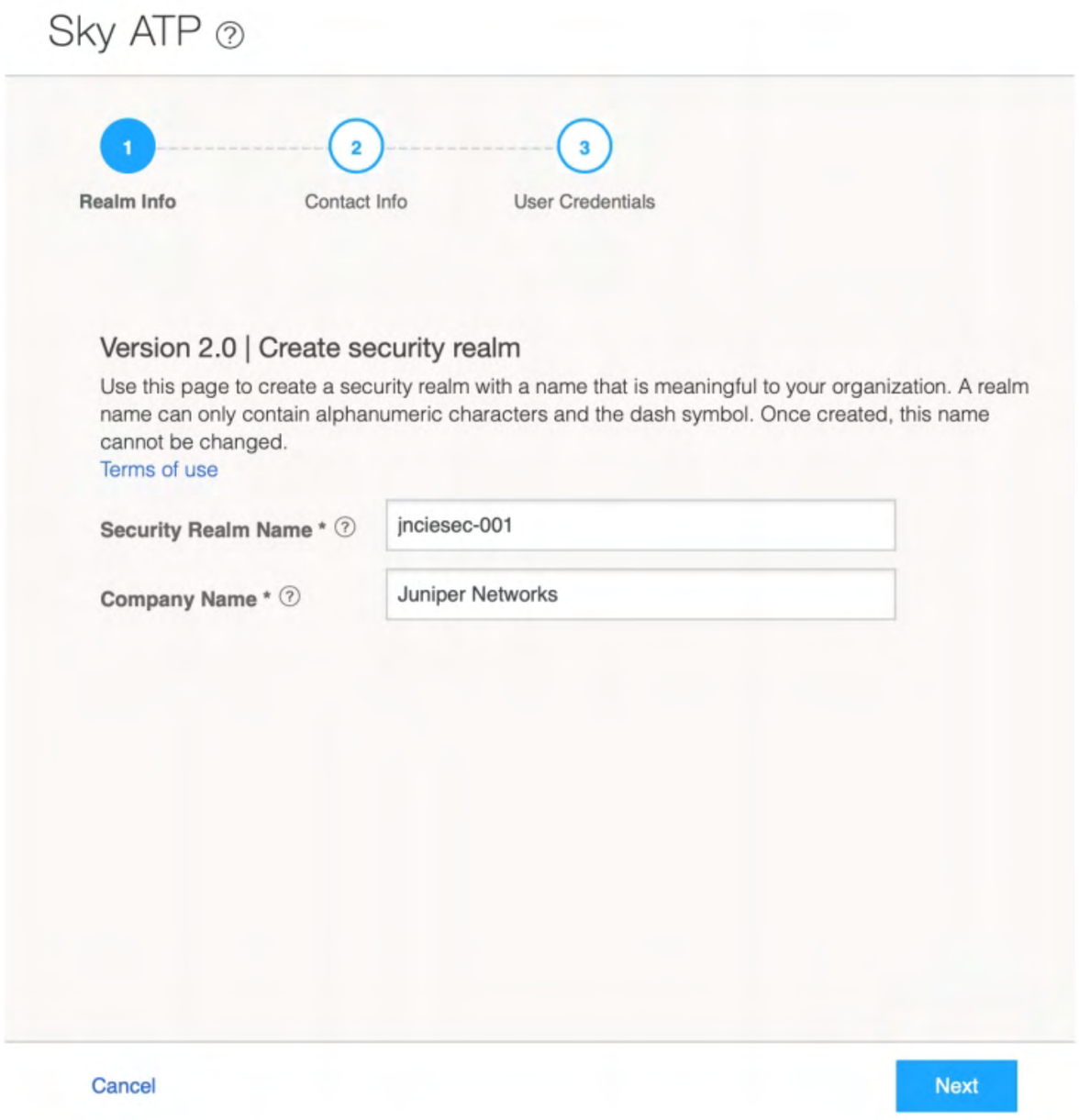
© 2020 Juniper Networks, Inc. All rights reserved.

b) To create a new SkyATP realm you are redirected to Juniper Network Single Sign On (SSO) and you must login with a valid account. As mentioned in the instructions it is important to use the Firefox browser installed on the student desktop as the password for userID: eduservicenow@gmail.com is auto populated. Click on the login button to proceed.



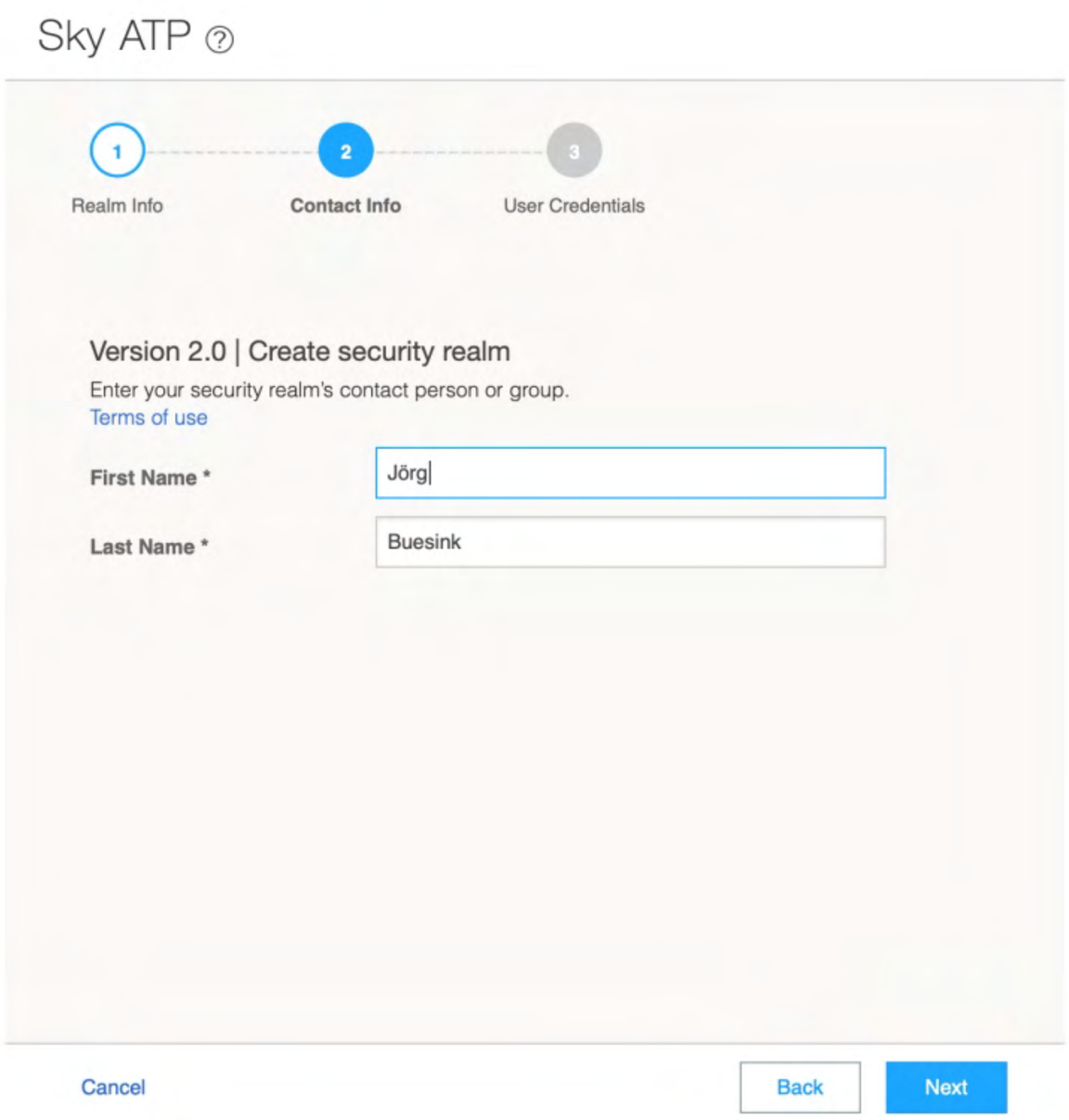
© 2020 Juniper Networks, Inc. All rights reserved.

c) Enter the Security Realm Name as provided with your lab access instructions. In this case the Security Realm Name: jnciesec-001 is used. Also specify the company name and click the “Next” button.



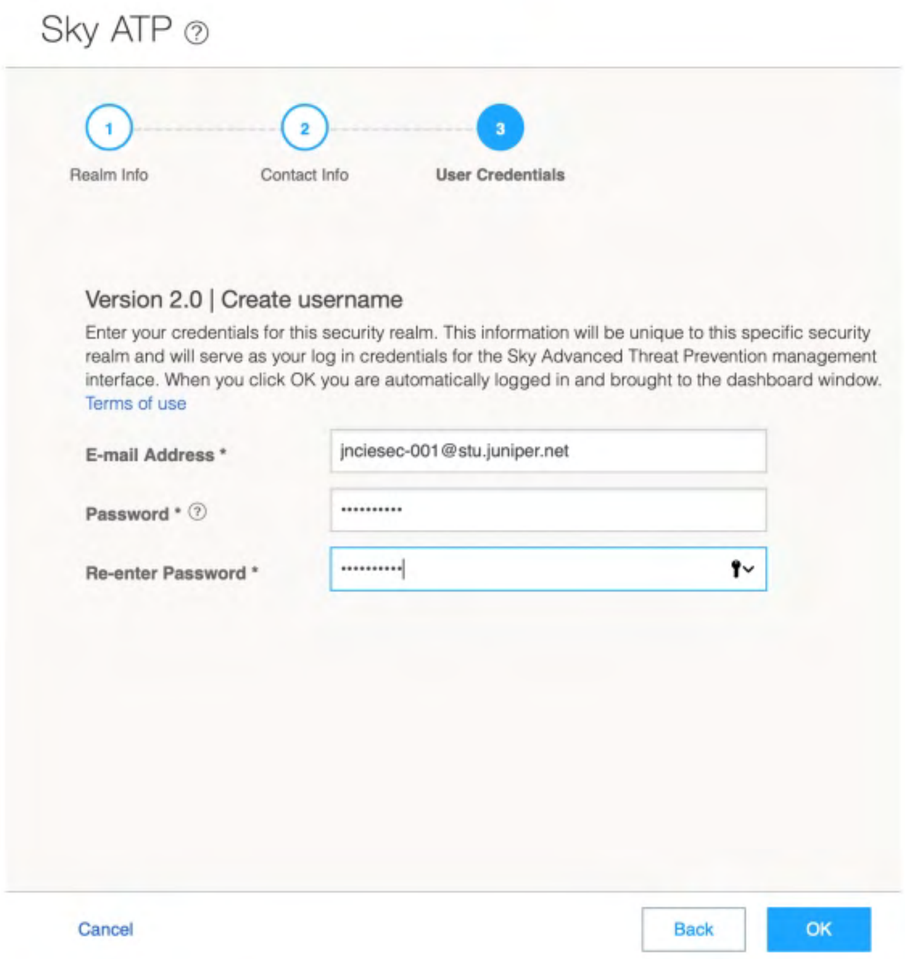
© 2020 Juniper Networks, Inc. All rights reserved.

d) Enter your first and last name and click the “Next” button.

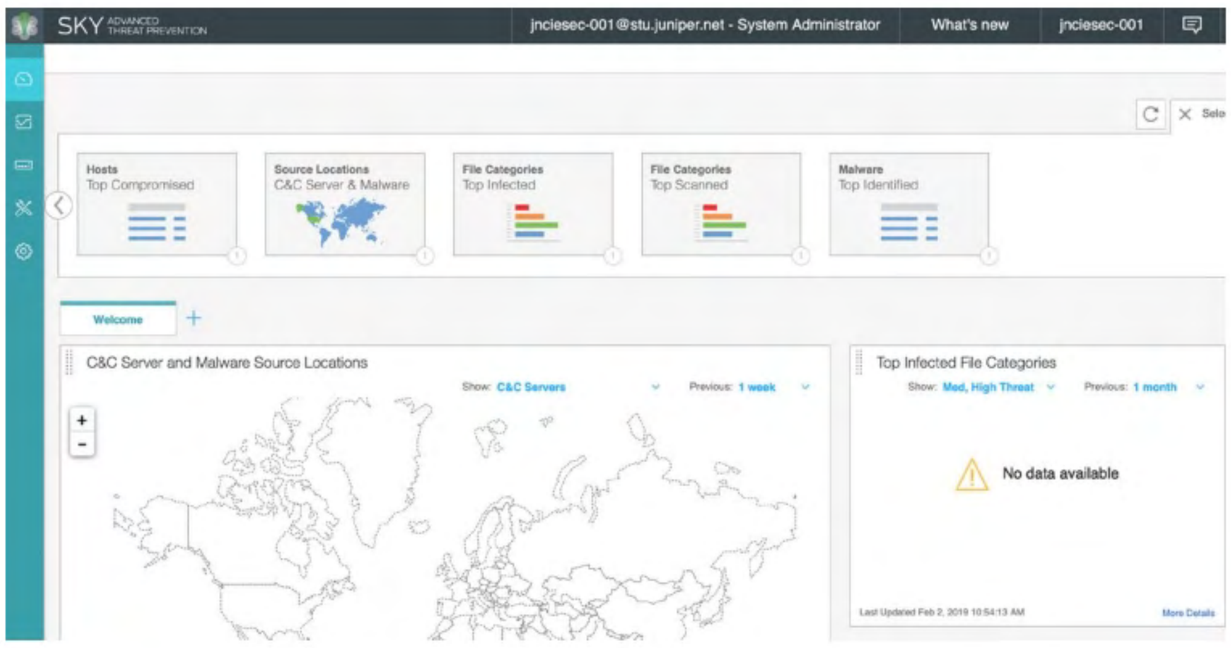


© 2020 Juniper Networks, Inc. All rights reserved.

e) Specify the user credentials to be used to login to the Sky ATP realm. In this case the email address: jnciesec-001@stu.juniper.net is used with password lab123@Lab. Make sure you use the credentials provided as mentioned in the lab access instructions. Press the “Ok” button.

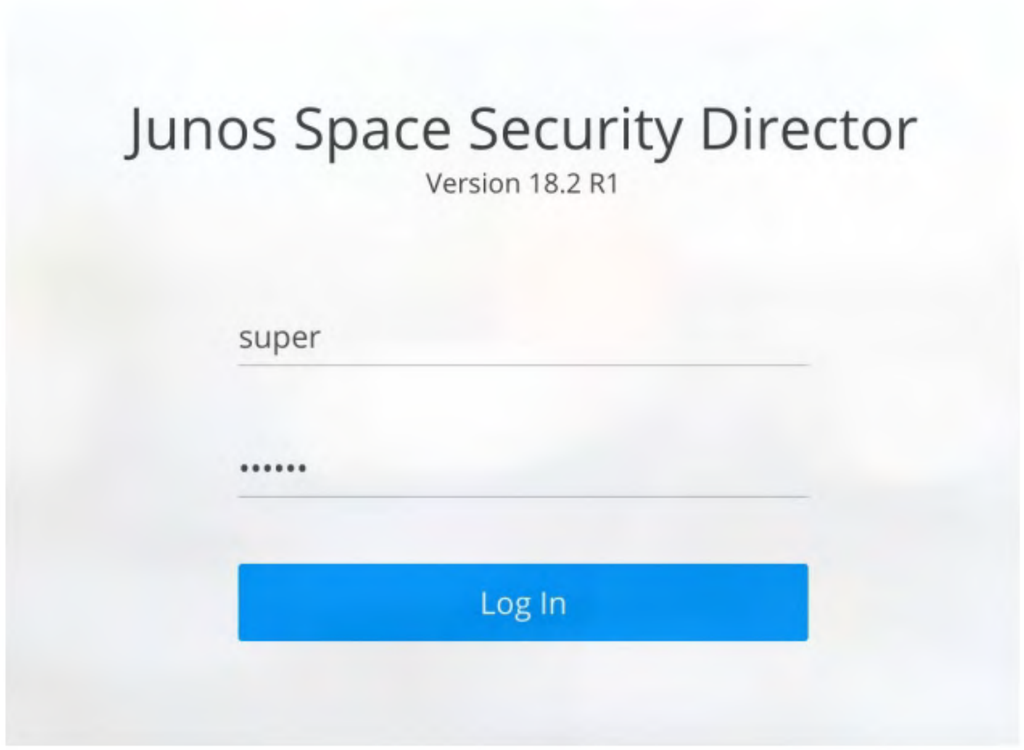


f) If you completed all steps correctly the SkyATP realm is created and you will auto login to the Sky ATP realm. At the top of the screen you should see your Sky ATP email address and the Sky ATP realm name. You can now close the Firefox browser as we will use Security Director to enroll the required devices.



© 2020 Juniper Networks, Inc. All rights reserved.

g) Access Security Director using the GUI interface and enter the login credentials as provided in your lab access instructions.



h) Navigate to the Devices / Device Discovery workspace. Create a new discovery job to discover the SRX devices and vQFX device (10.10.1.1 – 10.10.1.10) as the following screenshots show. Note that vQFX is is located between cluster 2 (srx5/srx6) and its internal hosts. Note that if the discovery job fails for any reason, run it again until all the devices are in the managed state.
    a. Job Name: jncie-sec
    b. IP Address Range: 10.10.1.1 – 10.10.1.10
    c. Probes:
        i. Use NAT: unchecked
        ii. Use Ping: checked
        iii. Use SNMP: unchecked
    d. Credentials
        i. Username: lab
        ii. Password: lab123
    e. Schedule Discovery Job
        i. Type: Run now
        ii. Import and Publish Policies: unchecked

© 2020 Juniper Networks, Inc. All rights reserved.

Create Device Discovery Profile

Add Device Discovery Target — Specify Probes — Specify Credentials — Specify Device Fingerprint — Schedule Discovery Job

Add Device Discovery Target

Discovery Profile Name* jncie-sec

Discovery Parameters
- (•) Add Manually
- ( ) Import From CSV File Sample CSV File

Target Type*
- ( ) IP Address
- (•) IP Range
- ( ) IP Subnet
- ( ) Hostname

Target Details

Start IP Address* 10.10.1.1

End IP Address* 10.10.1.10

Cancel Next

Create Device Discovery Profile

Add Device Discovery Target — Specify Probes — Specify Credentials — Specify Device Fingerprint — Schedule Discovery Job

Specify Probes

Use NAT [ ] Enable

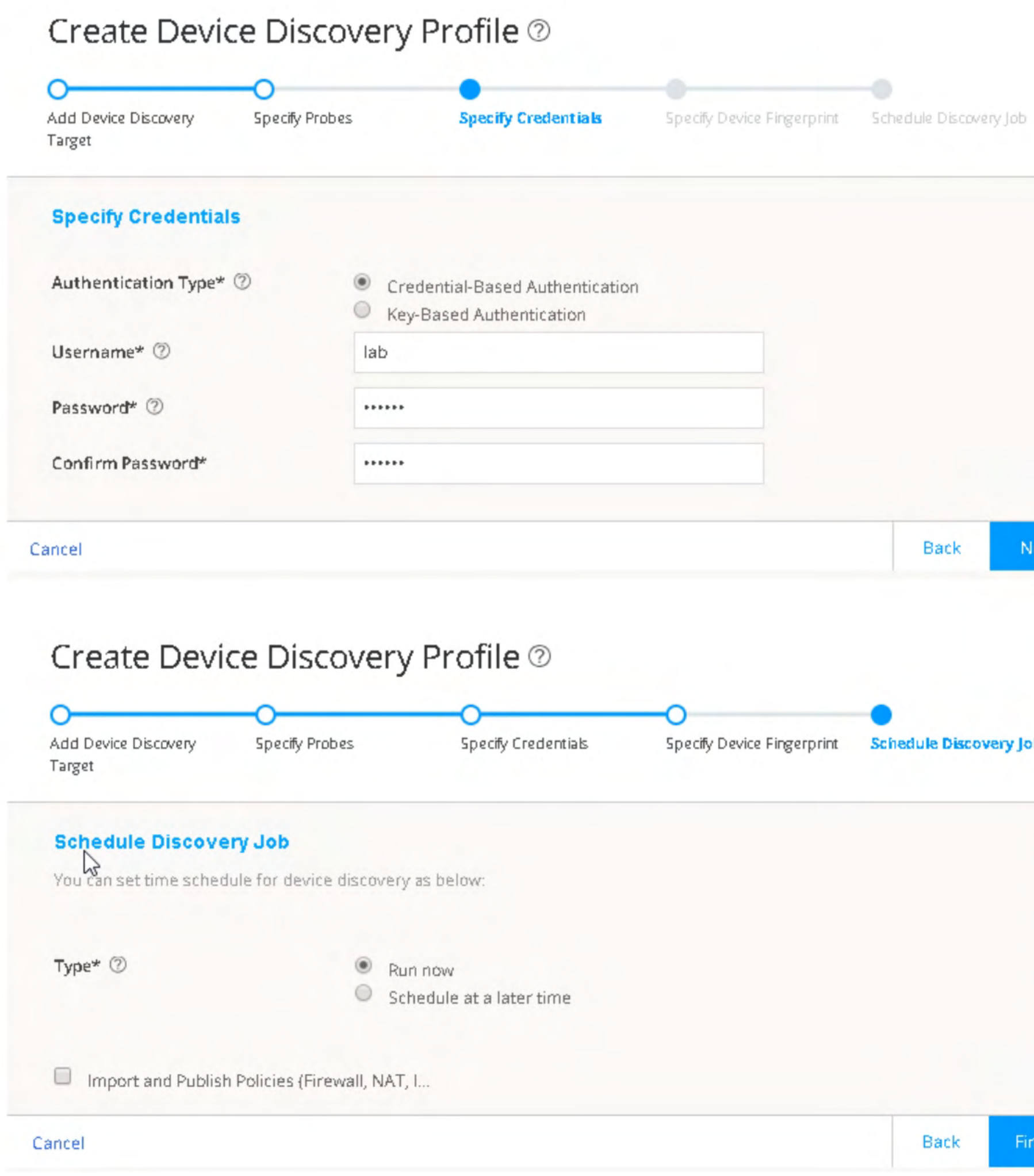
Use Ping [✓] Enable

Use SNMP [ ] Enable

Warning: If SNMP is disabled, the Network Monitoring functionality will be limited. To enable SNMP settings later, you must go to the Network Monitoring workspace in Junos Space Network Management Platform.

Cancel Back Next

© 2020 Juniper Networks, Inc. All rights reserved.



© 2020 Juniper Networks, Inc. All rights reserved.

Job Details:Discover Network Elements

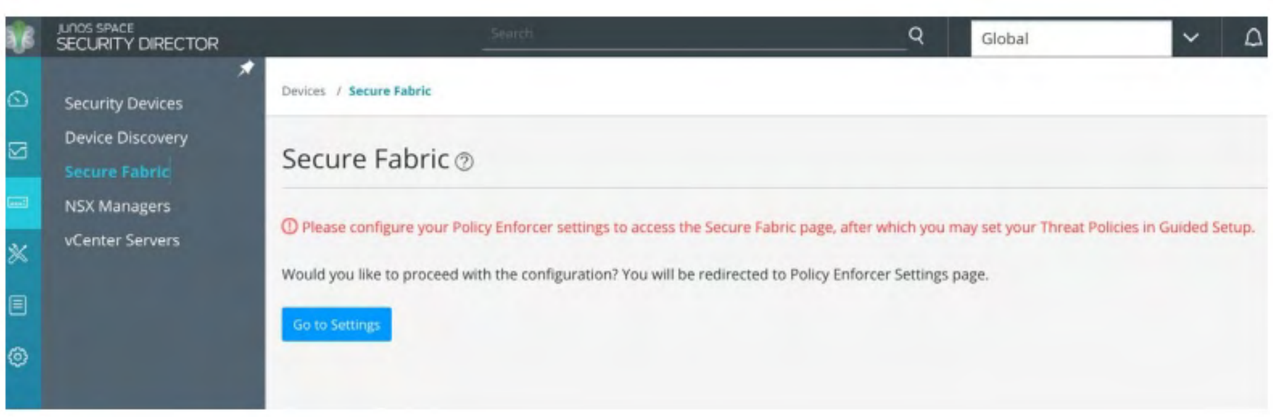
Job ID	426018	**Scheduled Start Time**	Thu, 28 Feb 2019 12:29:46 MST
Job Name	Discover Network Elements-426018	**Actual Start Time**	Thu, 28 Feb 2019 12:29:46 MST
Job State	Success	**End Time**	Thu, 28 Feb 2019 12:32:24 MST
Owner	super		

IP Address	Hostname	Job Status	Description
10.10.1.1	srx1	Already Managed	Device is already managed
10.10.1.2	srx2	Already Managed	Device is already managed
10.10.1.3	srx3	Already Managed	Device is already managed

10 Rows

OK

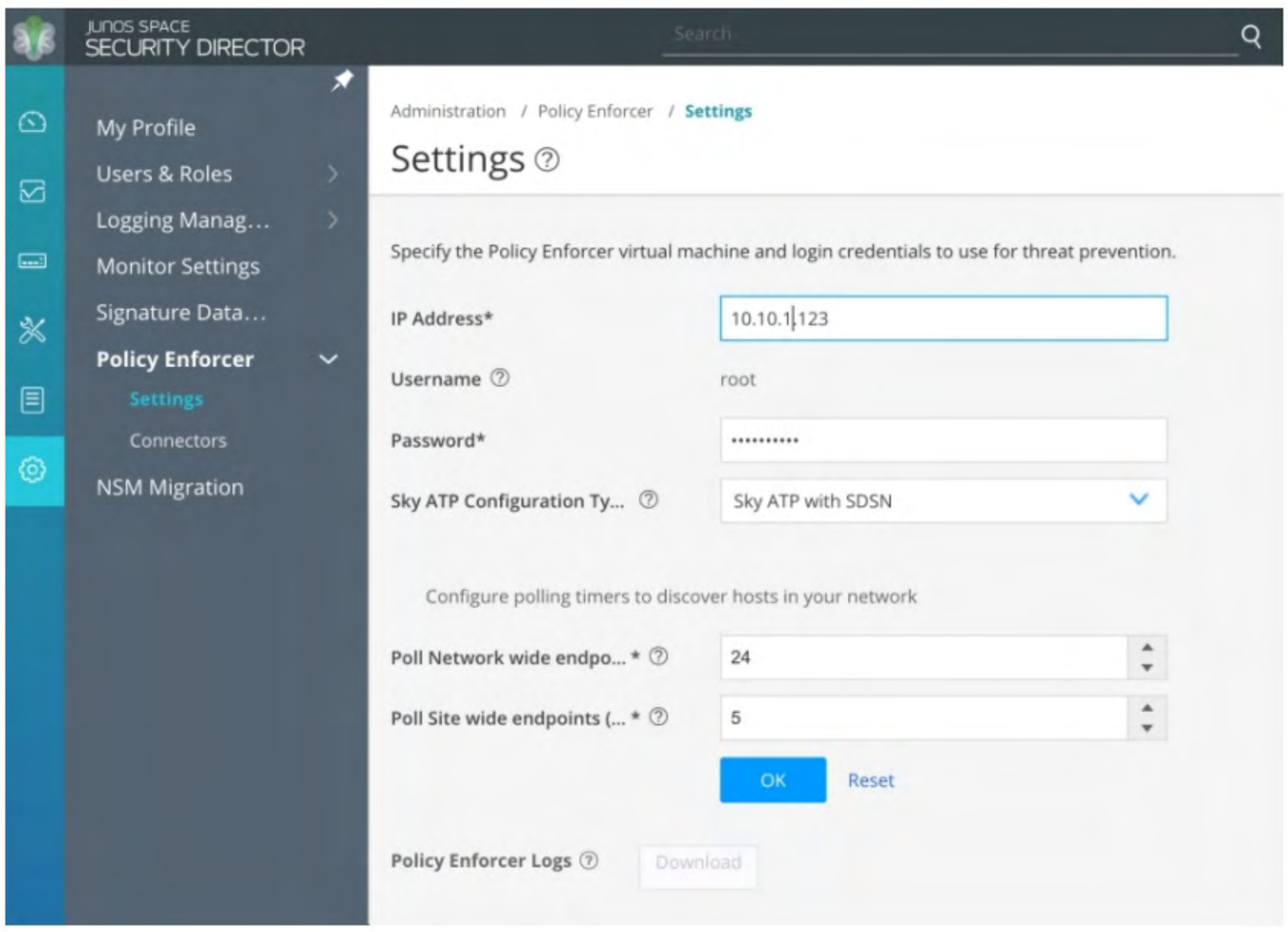
i) Navigate to Devices / Secure Fabric. Security Director gives a notification that we first need to configure Policy Enforcer to access the Secure Fabric Page.



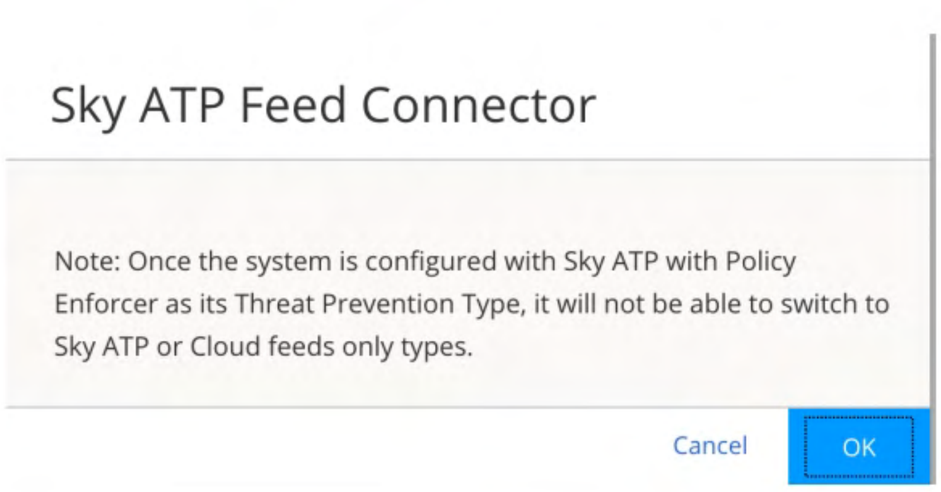
© 2020 Juniper Networks, Inc. All rights reserved.

j) Navigate to Administration / Policy Enforcer / Settings. Enter the IP address (10.10.1.123), username and password (lab123@Lab) of Policy Enforcer as mentioned in your lab access instructions.

Make sure to select “Sky ATP with SDSN” as the Sky ATP configuration type and click the “OK” button.

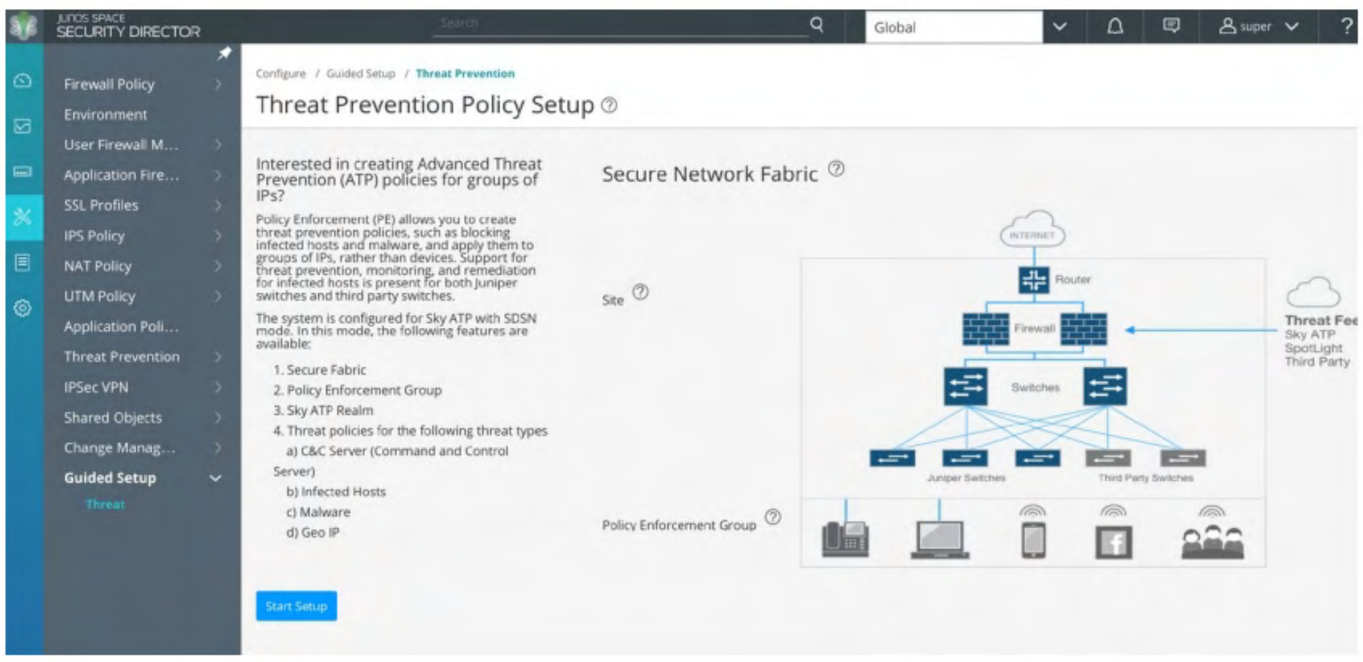


k) You should receive the following notification. Click the “ok” button to proceed.

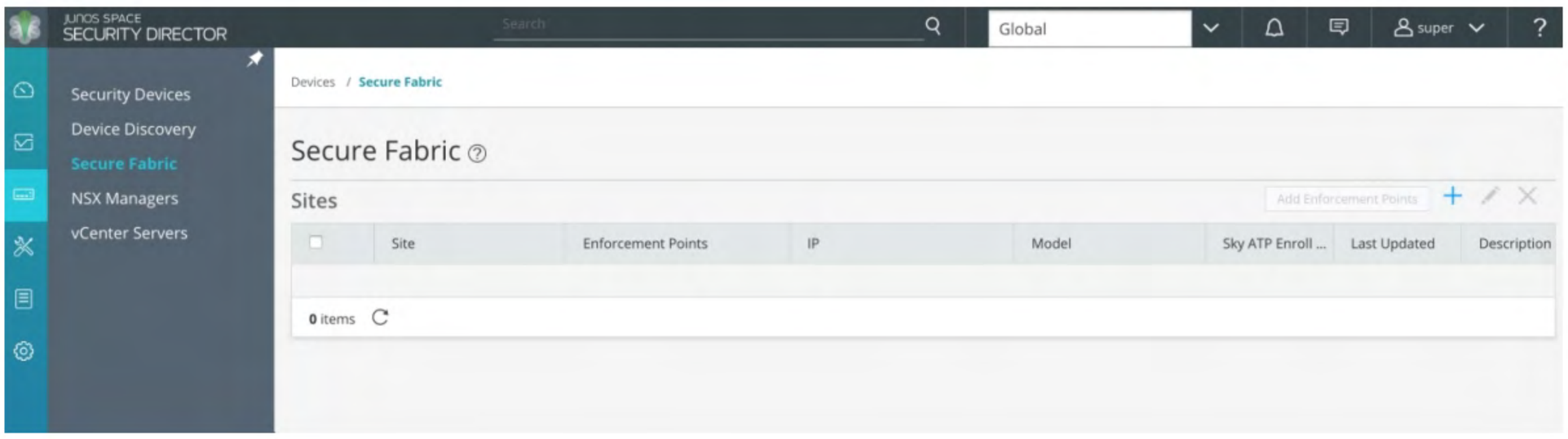


© 2020 Juniper Networks, Inc. All rights reserved.

l) Once Policy Enforcer is registered you are redirected to the “Threat Prevention Policy Setup” guided setup. At this stage we are not creating a Threat Prevention Policy yet as the task requirement is to enroll Policy Enforcer and the required security devices.

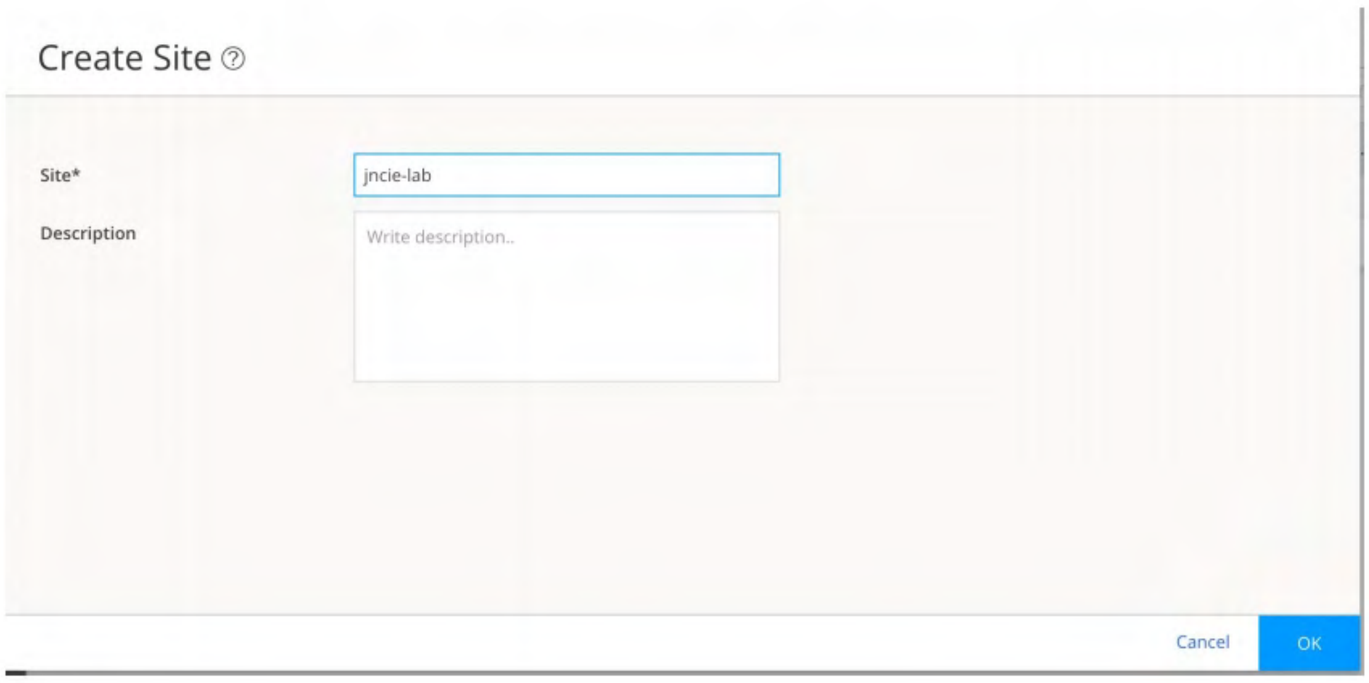


m) Navigate in the left vertical menu to “Devices” and select “Secure Fabric”. You need to define a “Site” and add “Enforcement points” to the site.

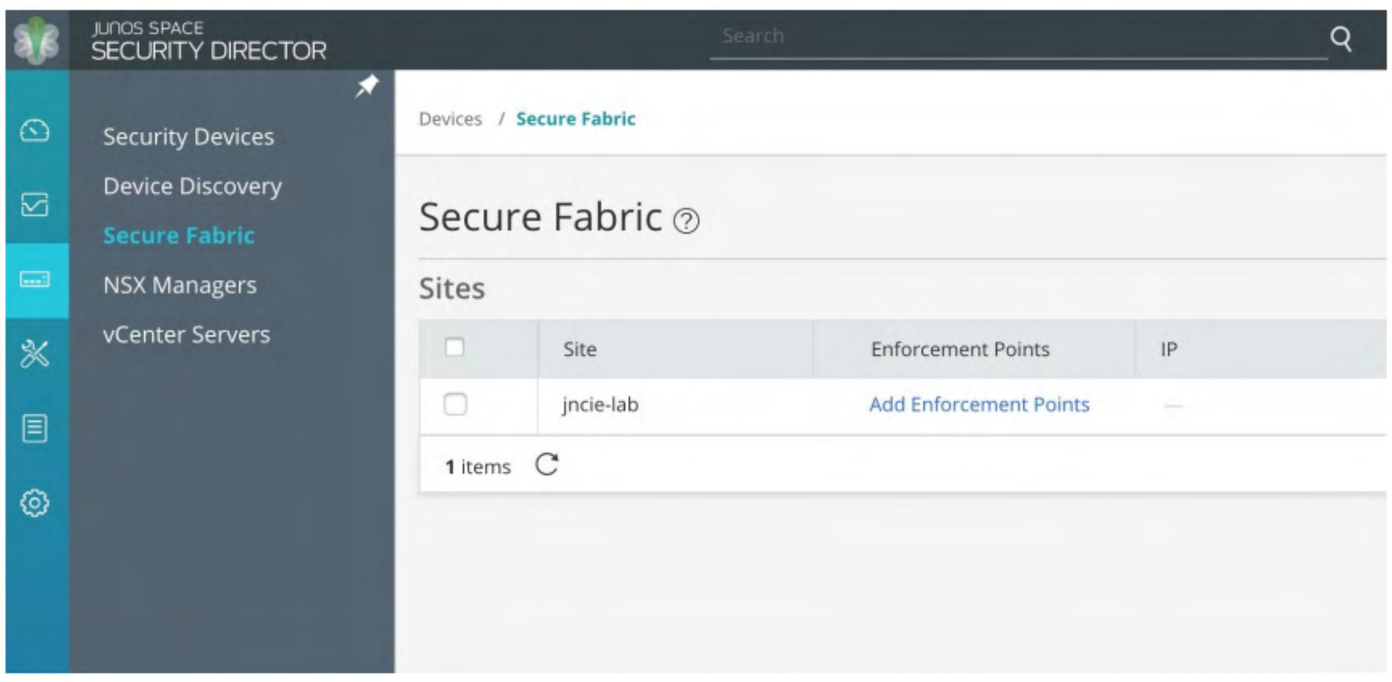


© 2020 Juniper Networks, Inc. All rights reserved.

n) Create a site and specific a Site name. In this case we call the Site “jncie-lab”. Click on the “Ok” button to proceed.

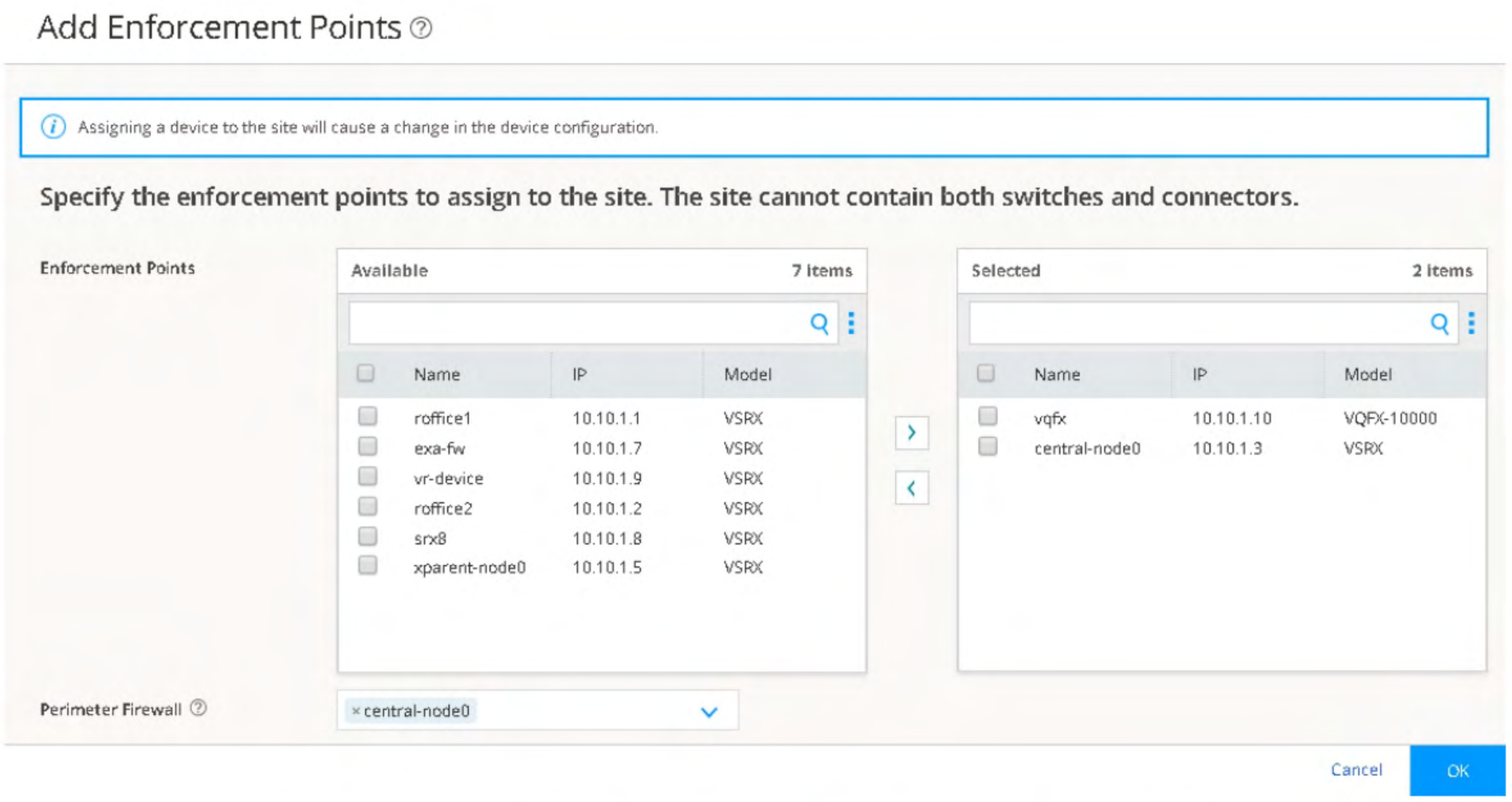


o) Now select “Add Enforcement Points” to add the central cluster (central-node0) and the vQFX device to the Secure Fabric.

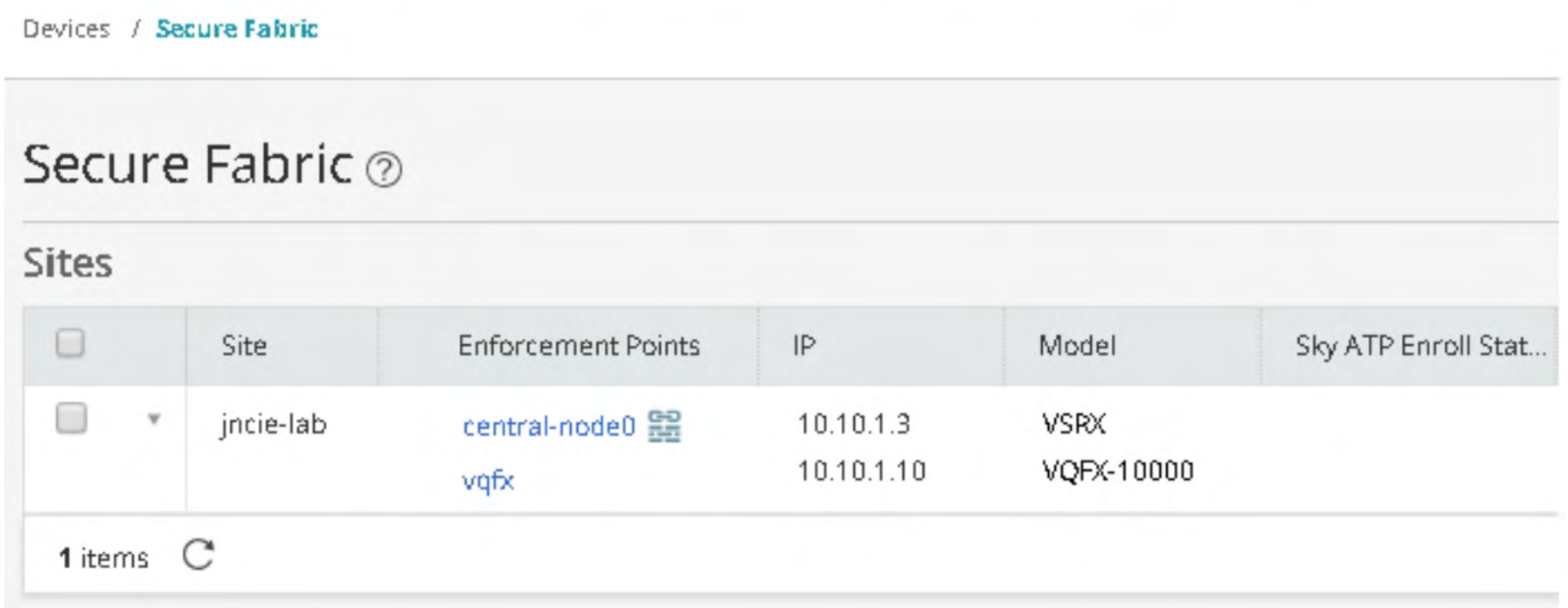


© 2020 Juniper Networks, Inc. All rights reserved.

p) Select the central-node0 (10.10.1.3) device and the vQFX device as an enforcement points and click the “ok” button.



q) Now the central cluster and the vQFX device should be added as an enforcement point to the Secure Fabric for Site “jncie-lab”.



© 2020 Juniper Networks, Inc. All rights reserved.

2) Setup for SkyATP with SDSN in Security Director, ensure that HTTP and SMTP traffic is analyzed at the central cluster (srx3/srx4) for threat levels greater than 6 for the 172.16.50.100 host. Ensure that connections are silently dropped at access switch vQFX if the 172.16.50.100 host becomes infected with malware. Ensure that only blocked traffic is logged. (Note that this includes C&C protection).

    a) Return to the open CLI session with the central-node0 device and add a term to the loopback filter (RE-PROTECT-v4) to allow DNS replies from the 8.8.8.8 DNS server. Note that hostname resultion is necessary for Sky ATP realm enrollment to work. You must also adjust the loopback filter to all for communication with the Sky ATP servers (TCP ports 443, 80, 8080)

```
{primary:node0}
lab@central-node0> configure
warning: Clustering enabled; using private edit
warning: uncommitted changes will be discarded on exit
Entering configuration mode

{primary:node0}[edit]
lab@central-node0# edit firewall family inet filter RE-PROTECT-v4

{primary:node0}[edit firewall family inet filter RE-PROTECT-v4]
lab@central-node0# set term DNS from source-address 8.8.8.8

{primary:node0}[edit firewall family inet filter RE-PROTECT-v4]
lab@central-node0# set term DNS then accept

{primary:node0}[edit firewall family inet filter RE-PROTECT-v4]
lab@central-node0# insert term DNS before term IFD

{primary:node0}[edit firewall family inet filter RE-PROTECT-v4]
lab@central-node0# set term sdsn from protocol tcp port https

{primary:node0}[edit firewall family inet filter RE-PROTECT-v4]
lab@central-node0# set term sdsn from port http

{primary:node0}[edit firewall family inet filter RE-PROTECT-v4]
lab@central-node0# set term sdsn from port 8080

{primary:node0}[edit firewall family inet filter RE-PROTECT-v4]
lab@central-node0# set term sdsn then accept

{primary:node0}[edit firewall family inet filter RE-PROTECT-v4]
lab@central-node0# insert term sdsn before term IFD

{primary:node0}[edit firewall family inet filter RE-PROTECT-v4]
lab@central-node0# show
term DNS {
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
        from {
            source-address {
                8.8.8.8/32;
            }
            port domain;
        }
        then accept;
    }
    term sdsn {
        from {
            protocol tcp;
            port [ https http 8080 ];
        }
        then accept;
    }
    term IFD {
        from {
            interface gr-0/0/0;
            interface st0;
        }
        then accept;
    }
    term PORT-TCP {
        from {
            source-prefix-list {
                mgmt;
            }
            protocol tcp;
            destination-port [ https ssh ];
        }
        then accept;
    }
    term LOG-TCP {
        from {
            protocol tcp;
            destination-port [ https ssh ];
        }
        then {
            count LOG-TCP;
            discard;
        }
    }
    term ICMP {
        from {
            protocol icmp;
        }
        then {
            policer ICMP-POLICER;
            accept;
        }
    }
```


© 2020 Juniper Networks, Inc. All rights reserved.

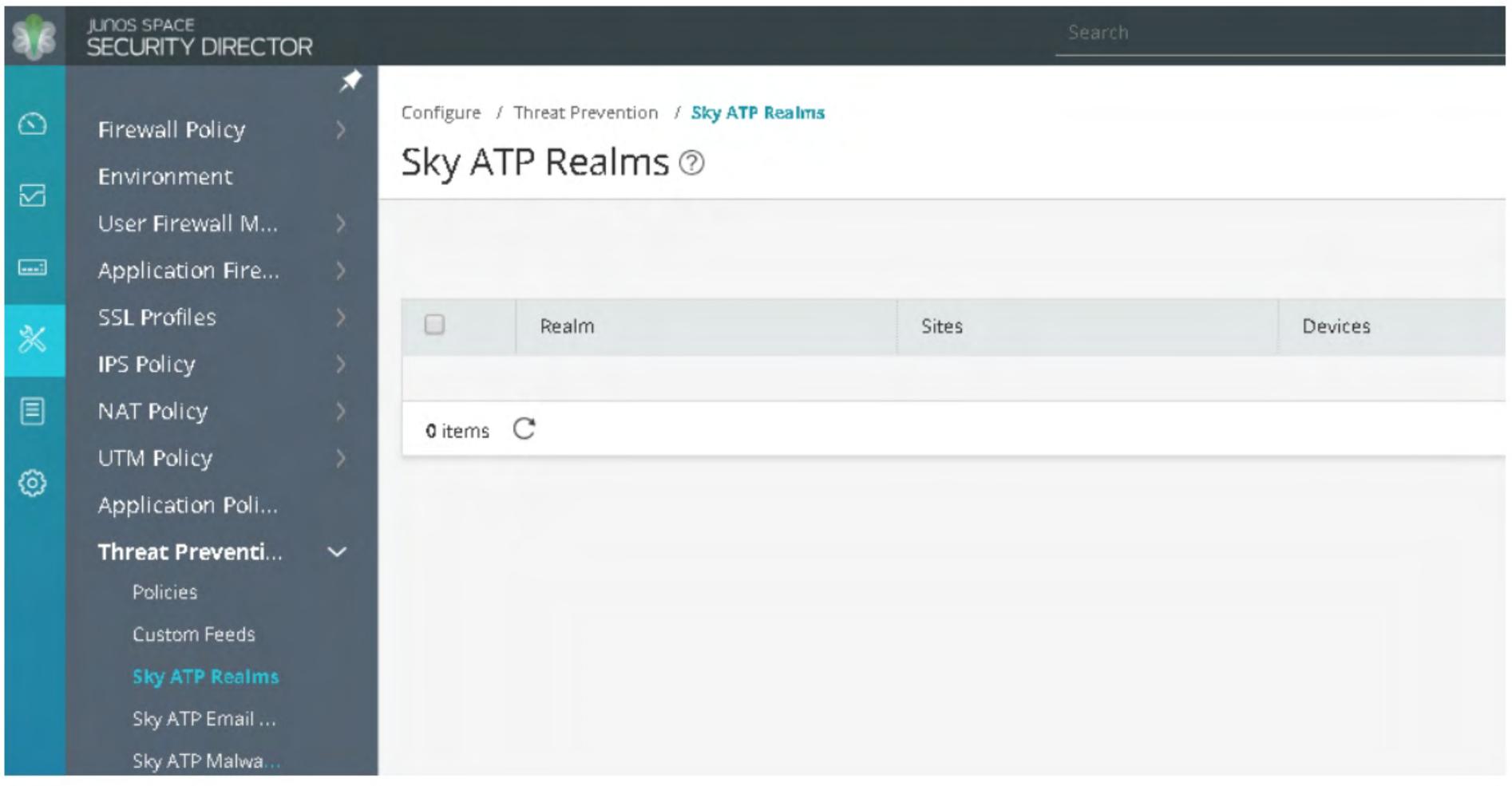
```
term SNMP {
    from {
        source-prefix-list {
            mgmt;
        }
        port [ snmp snmptrap ];
    }
    then {
        count SNMP;
        accept;
    }
}
term BGP {
    from {
        prefix-list {
            bgp;
        }
        protocol tcp;
        port bgp;
    }
    then {
        count BGP;
        accept;
    }
}
term OSPF {
    from {
        protocol ospf;
    }
    then {
        count OSPF;
        accept;
    }
}
term LDP {
    from {
        port ldp;
    }
    then {
        count LDP;
        accept;
    }
}
term IKE {
    from {
        port 500;
    }
    then {
        count IKE;
        accept;
    }
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
}
term PORT-UDP {
    from {
        source-prefix-list {
            mgmt;
        }
        protocol udp;
        port [ domain ntp ];
    }
    then accept;
}
term LOG-UDP {
    from {
        protocol udp;
        port [ domain ntp ];
    }
    then {
        count LOG-UDP;
        discard;
    }
}

{primary:node0}[edit firewall family inet filter RE-PROTECT-v4]
lab@central-node0# top

{primary:node0}[edit]
lab@central-node0# commit and-quit
node0:
configuration check succeeds
node1:
commit complete
node0:
commit complete
Exiting configuration mode

{primary:node0}
lab@central-node0>
```

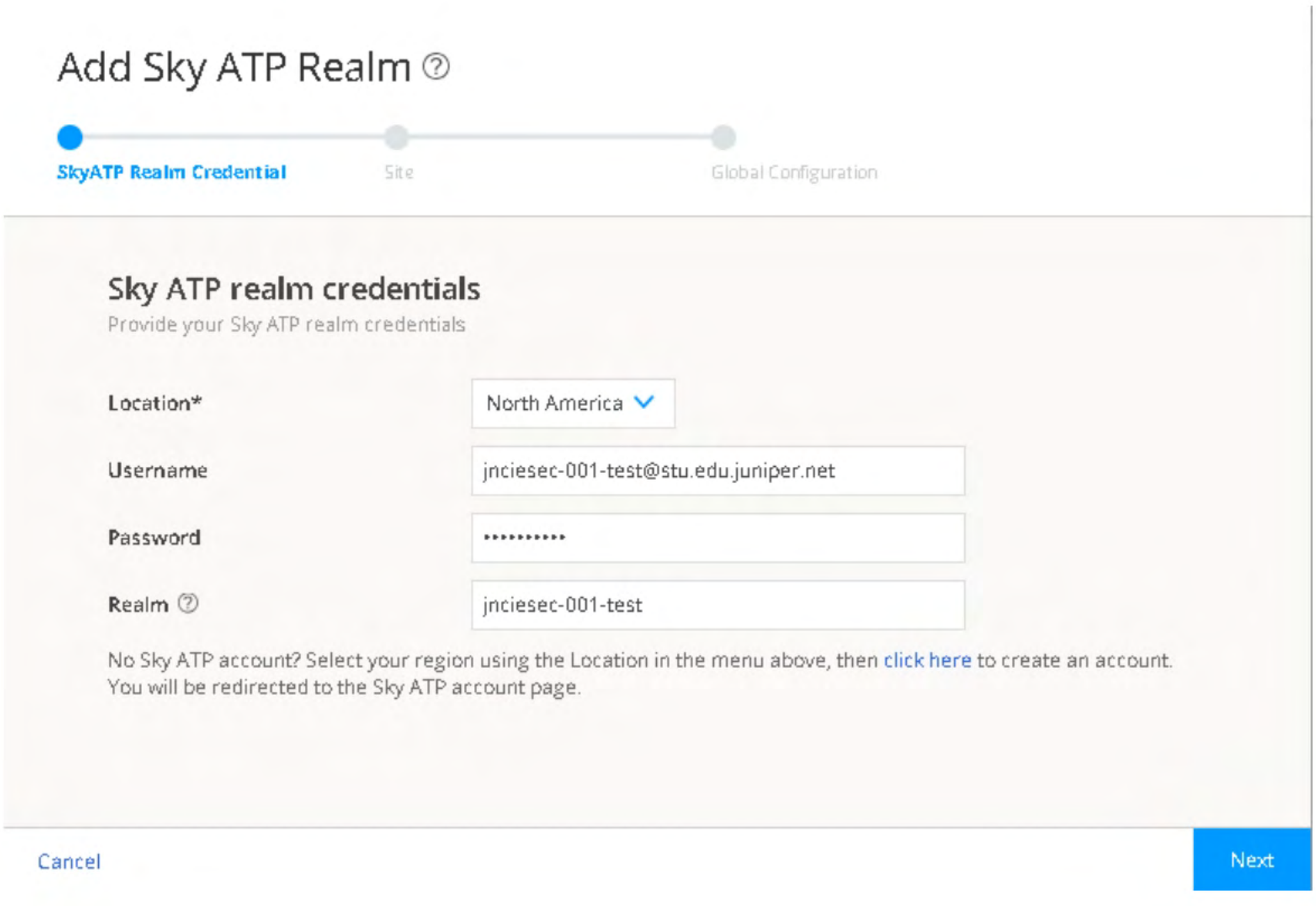

© 2020 Juniper Networks, Inc. All rights reserved.

b) Return to the Security Director GUI and navigate to the Configure / Threat Prevention / Sky ATP Realms workspace.



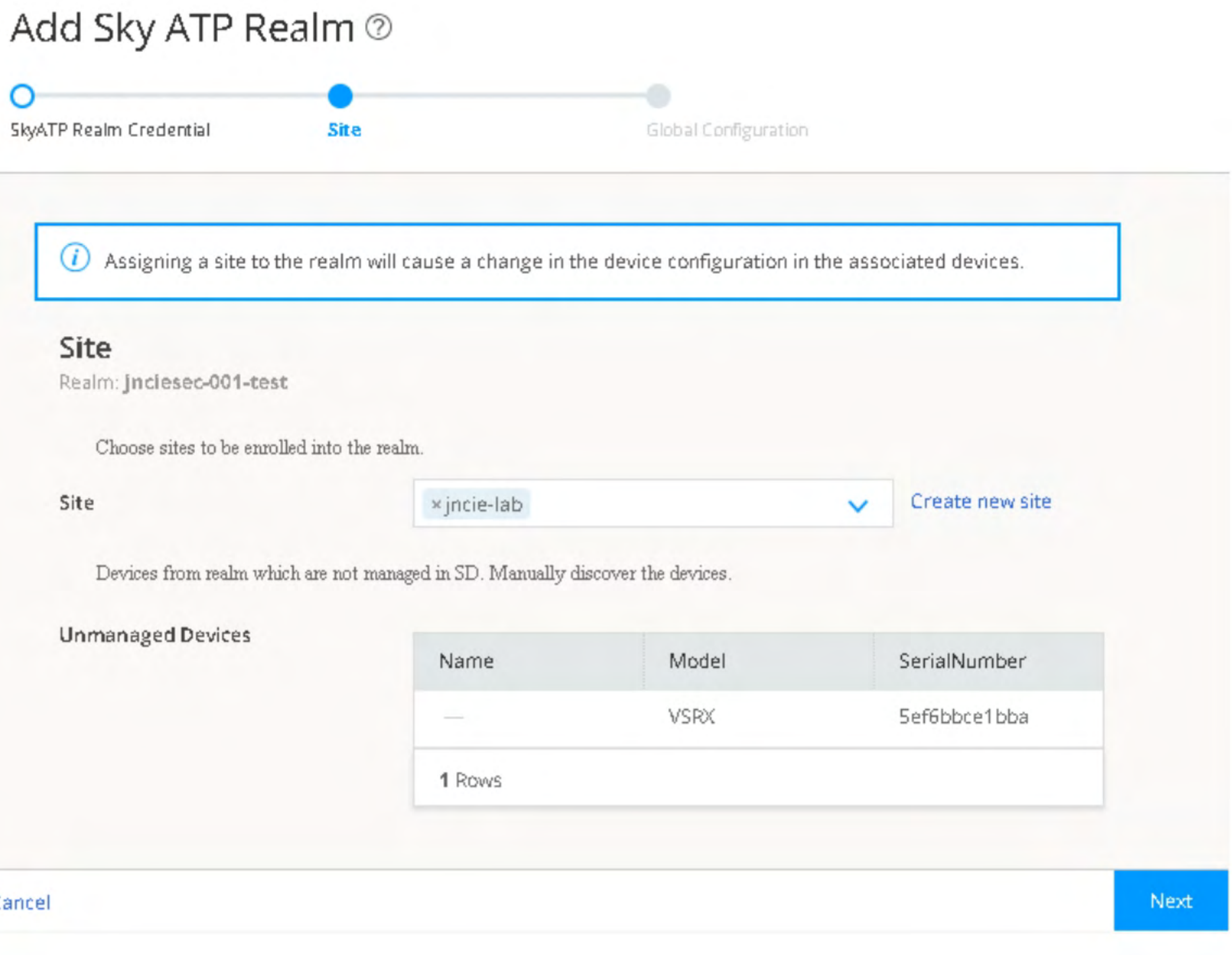
© 2020 Juniper Networks, Inc. All rights reserved.

c) Click the create button and enter your Sky ATP realm credentials. Click Next to continue.



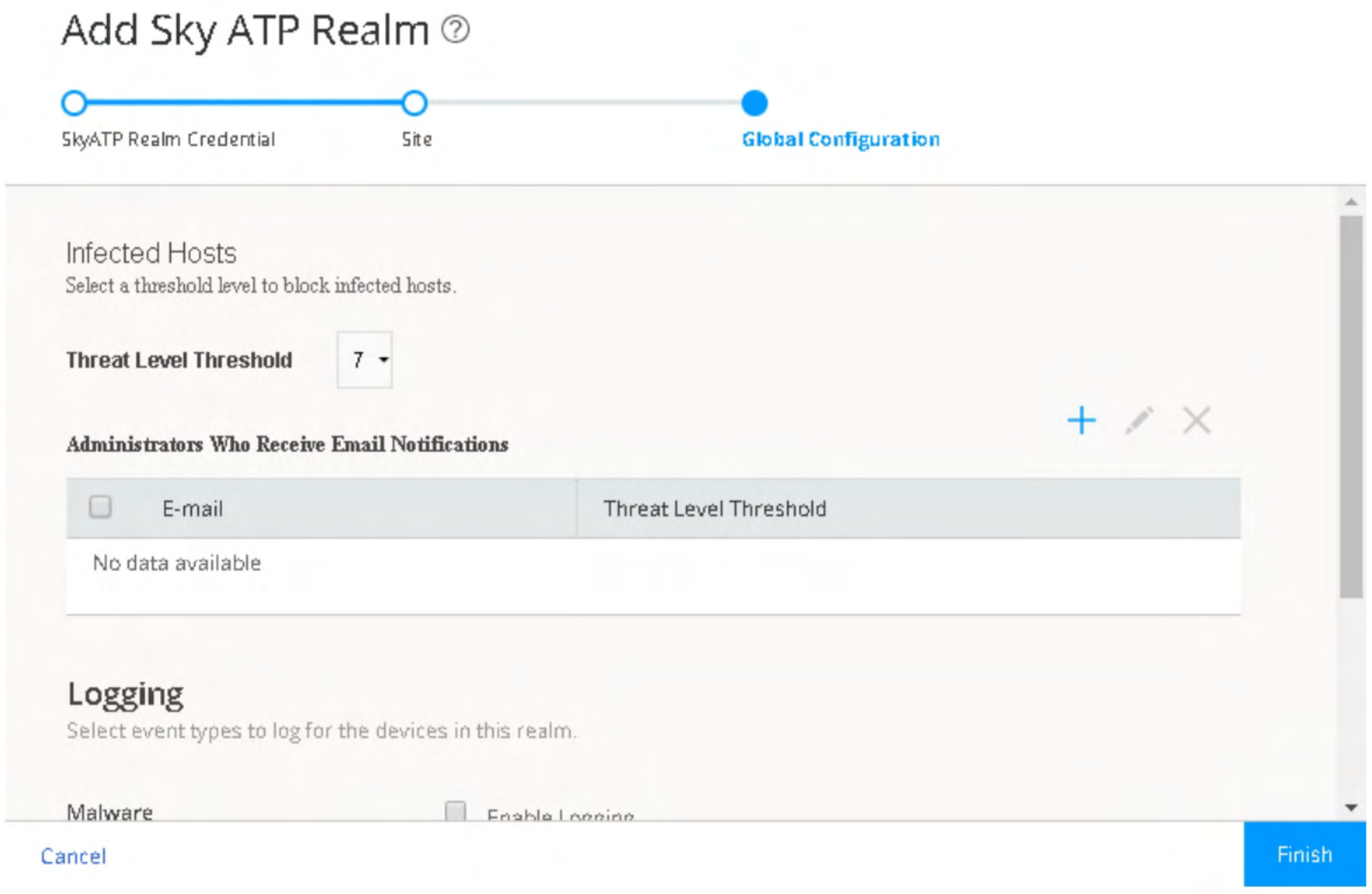
© 2020 Juniper Networks, Inc. All rights reserved.

d) Select your SDSN site and click next.



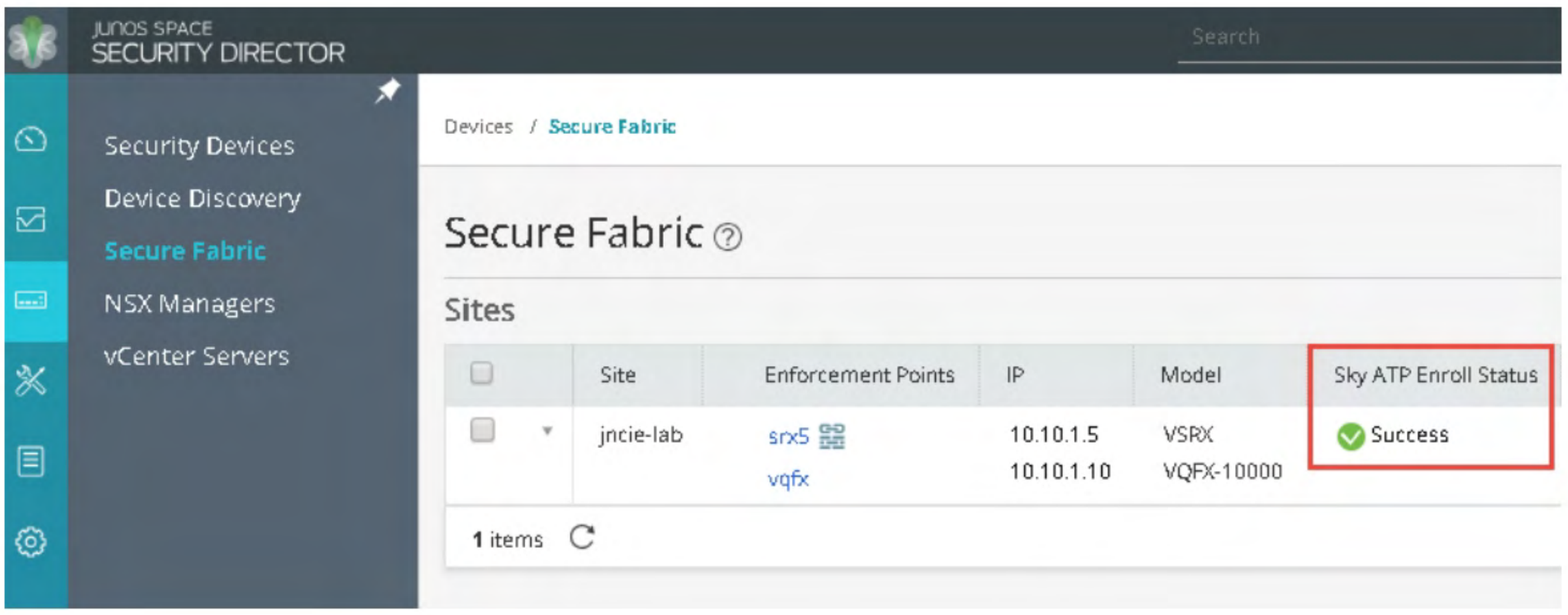
© 2020 Juniper Networks, Inc. All rights reserved.

e) Leave everything at the defaults for the Global Configuration page and click Finish.



© 2020 Juniper Networks, Inc. All rights reserved.

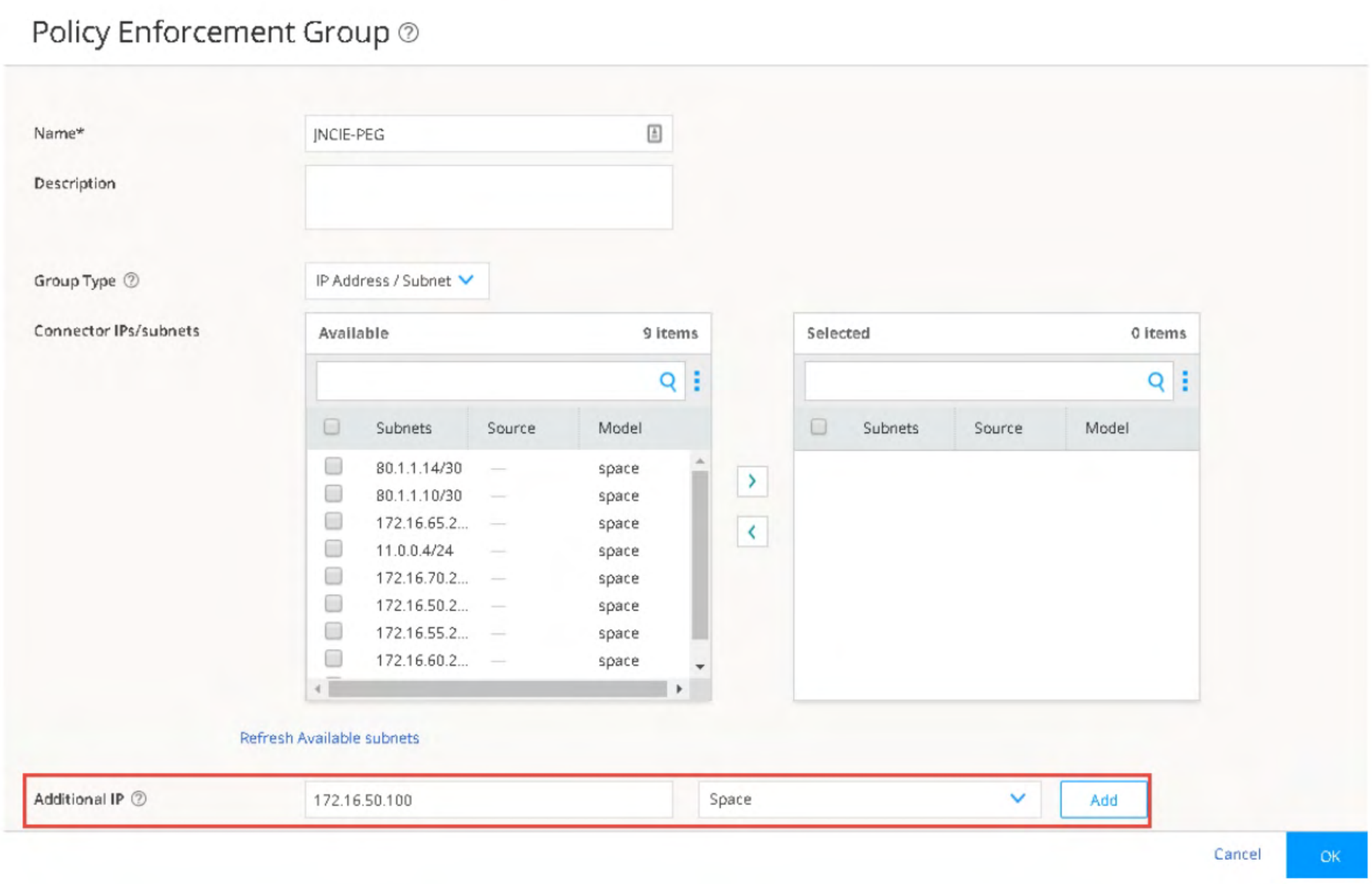
f) Navigate to the Devices / Secure Fabric workspace. Ensure that the central-node0 device Sky ATP enrolment status is successful. Note if the status shows Pending then you should wait 5 minutes and refresh the page.



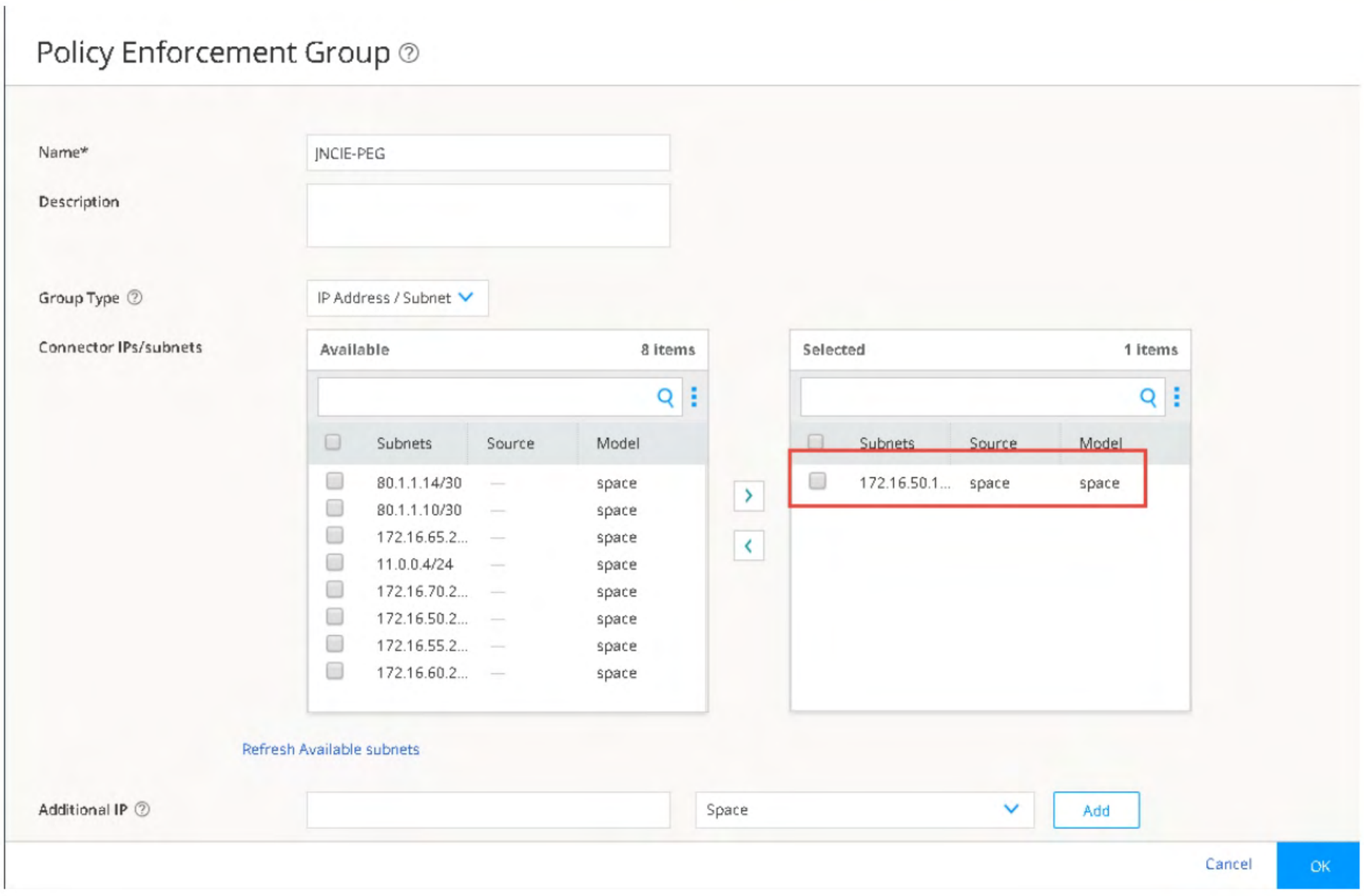
© 2020 Juniper Networks, Inc. All rights reserved.

g) Create a policy enforcement group for the 172.16.50.100 host. Ensure that connections are silently dropped if the threat is identified. Ensure that only blocked traffic is logged.

   i. Navigate to the Configure / Shared Objects / Policy Enforcement Groups workspace. Create a new PEG and add the new 172.16.50.100 IP address

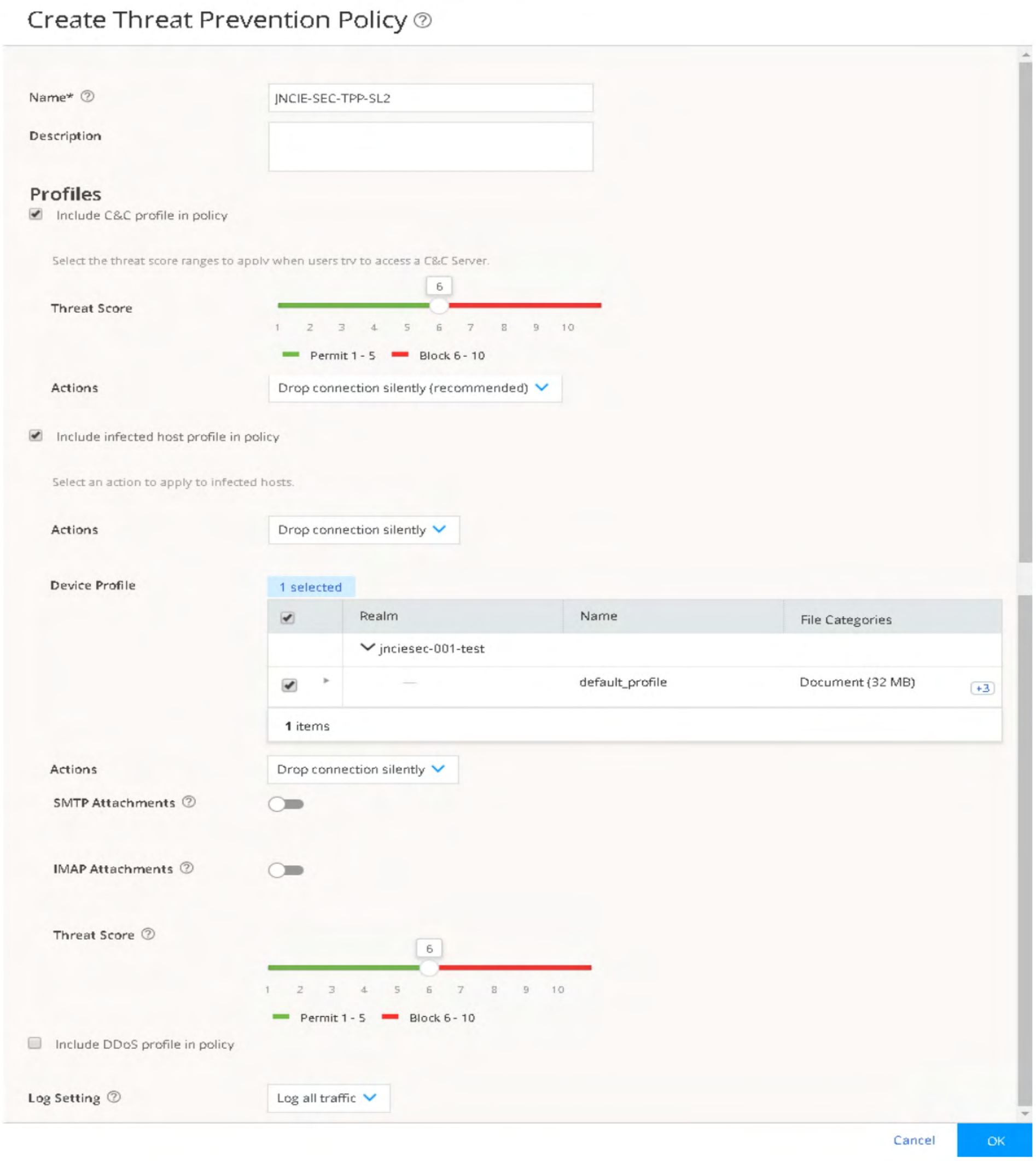


© 2020 Juniper Networks, Inc. All rights reserved.



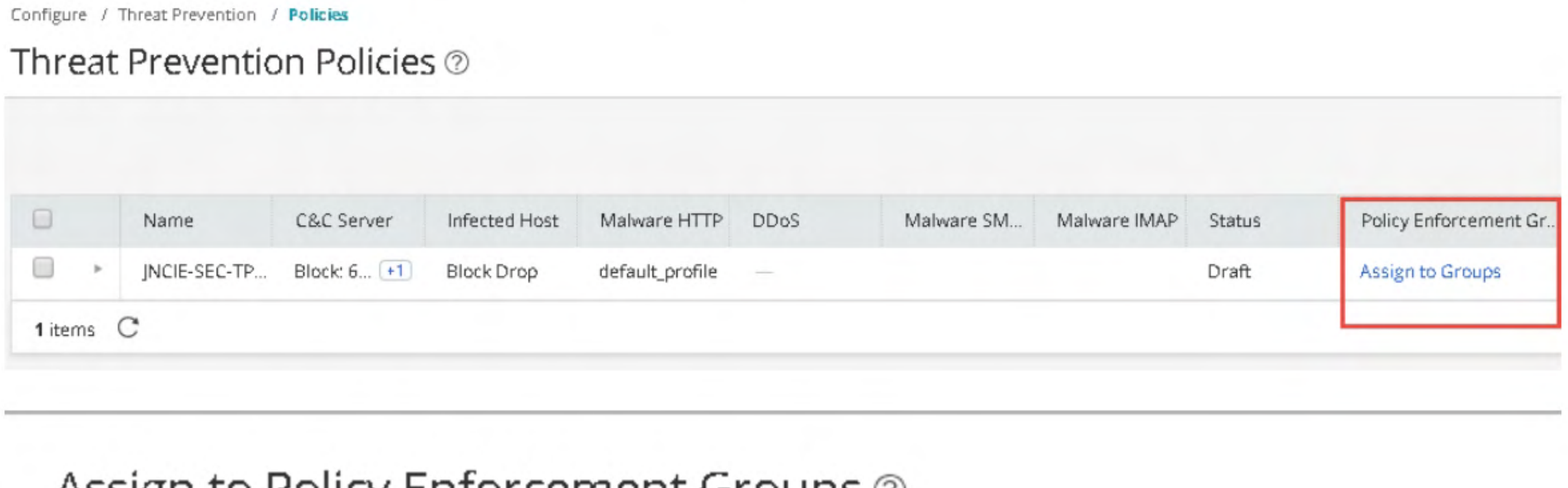
© 2020 Juniper Networks, Inc. All rights reserved.

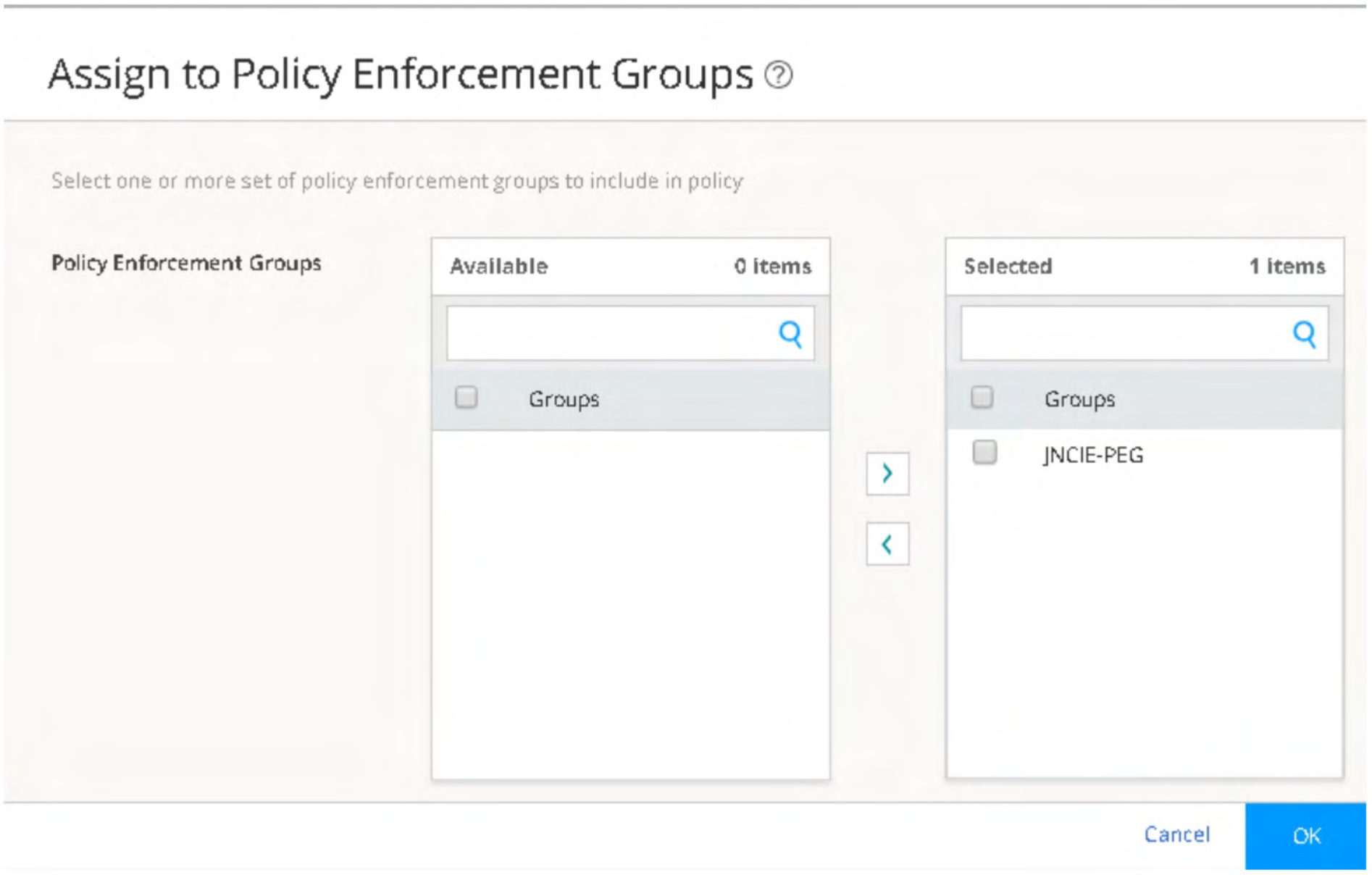
h) Navigate to the Configure / Threat Prevention / Policies workspace to setup a threat prevention policy. Make sure that you include the infected host profile and the malware profile in the policy. Scan HTTP files downloads using the default profile associated with your realm. Set the Threat score to block threats rated at a value that is greater than 6. (Note that this includes C&C protection).



© 2020 Juniper Networks, Inc. All rights reserved.

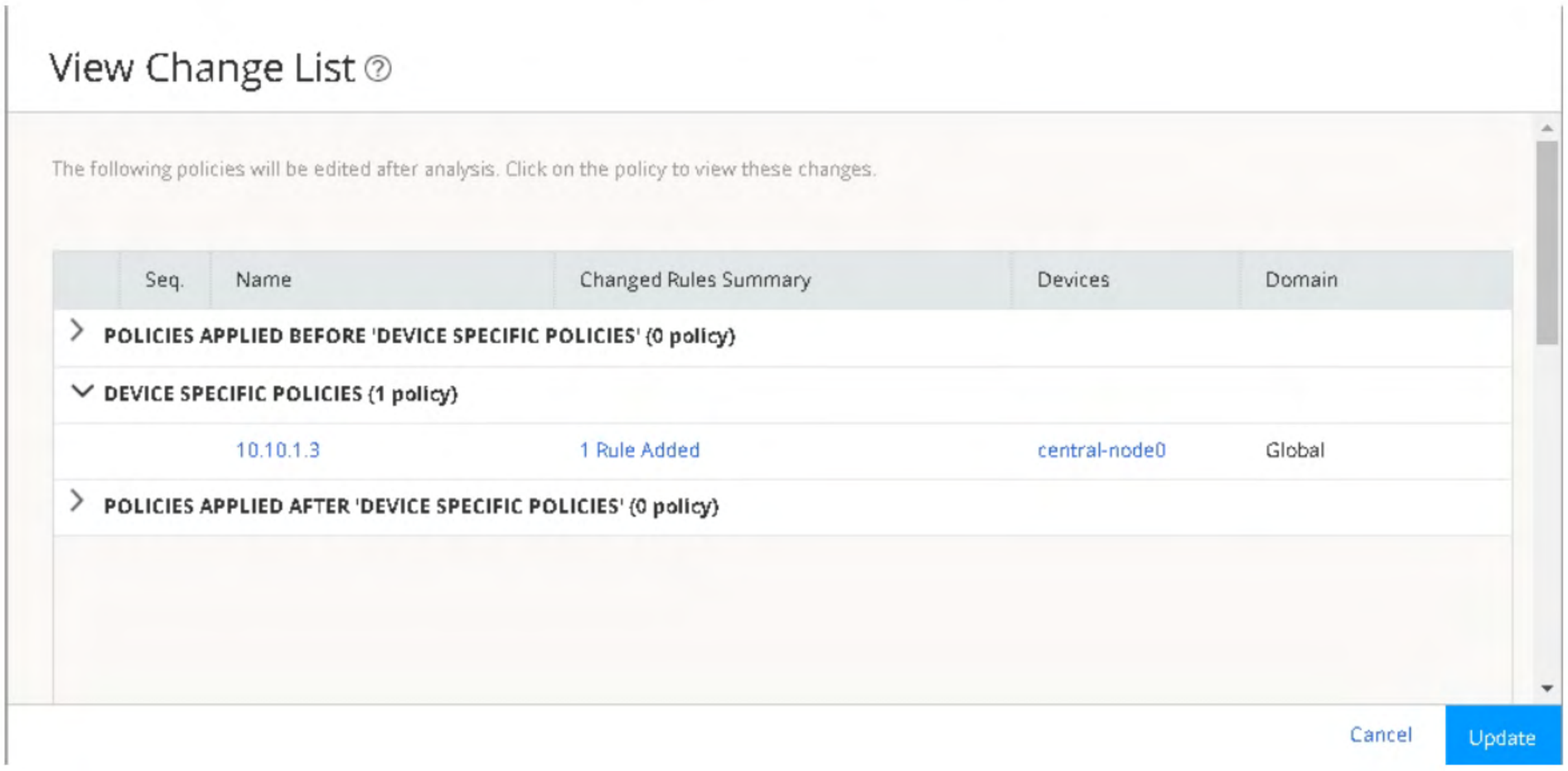
i) Assign your PEG to the policy.

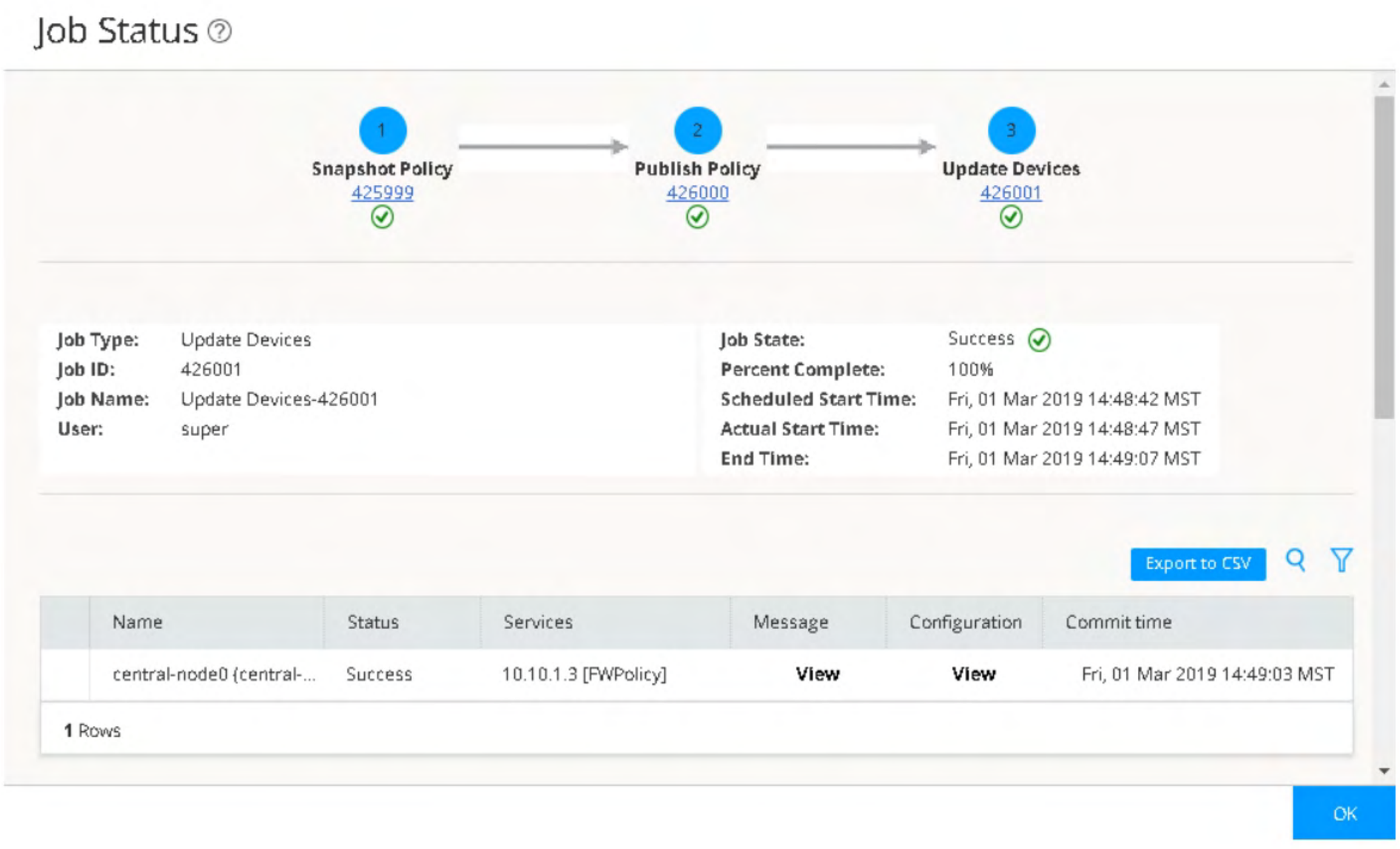




© 2020 Juniper Networks, Inc. All rights reserved.

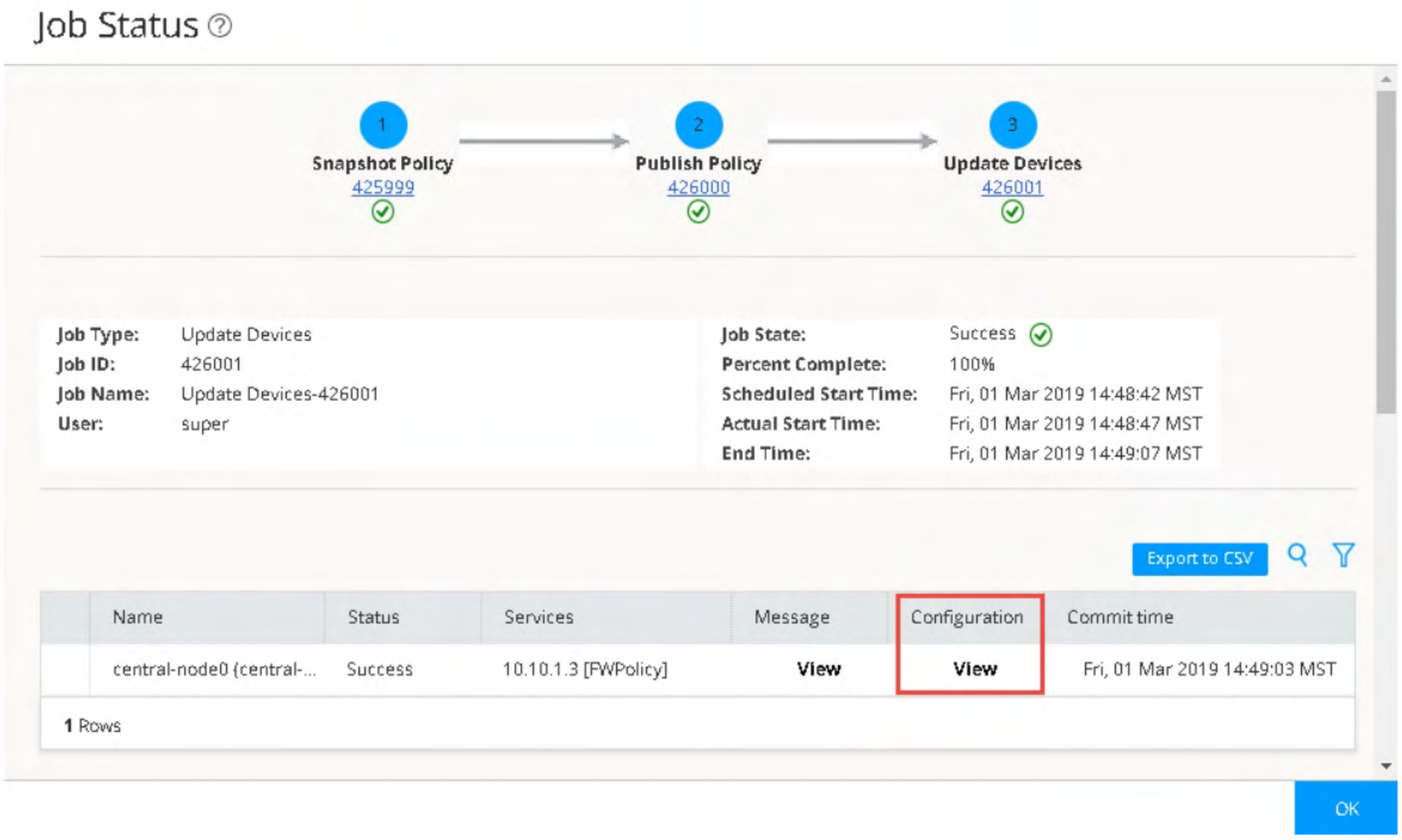
j) Click Update on the View Change List page.





© 2020 Juniper Networks, Inc. All rights reserved.

k) Click the View link for the Configuration section.



© 2020 Juniper Networks, Inc. All rights reserved.

View configuration for central-node0 (central-node0) (Cluster)

CLI | XML

Added Deleted Modified Comments

```
##Global address book configurations##
delete security address-book global address BUILDING-DMZ-B1
delete security address-book global address BUILDING-DMZ-B2
delete security address-book global address BUILDING-TRUST-B1
delete security address-book global address BUILDING-TRUST-B2
delete security address-book global address CENTRAL-INTERNAL
delete security address-book global address CENTRAL-TESTBED6
delete security address-book global address CENTRAL-TESTBED7
delete security address-book global address CENTRAL-TRUST
delete security address-book global address CENTRAL-TRUST-V6
delete security address-book global address CENTRAL-WAREHOUSE
delete security address-book global address EXA-PRIVATE
delete security address-book global address EXA-PRIVATE-V6
delete security address-book global address EXA-SRV-DB
delete security address-book global address EXA-SRV-SSH
delete security address-book global address EXA-SRV-WEB
delete security address-book global address EXA-TRUST
delete security address-book global address EXA-TRUST-OVERLAP
delete security address-book global address EXA-TRUST-V6
delete security address-book global address HOFFICE-TRUST
set security address-book global address JNCIE-PEG_172.16.50.100 172.16.50.100/32
delete security address-book global address RO1-HOST-PRIVATE
delete security address-book global address RO1-TRUST
delete security address-book global address RO1-TRUST-OVERLAP
delete security address-book global address RO1-TRUST-V6
delete security address-book global address RO2-SRV-DB
delete security address-book global address RO2-SRV-WEB
delete security address-book global address RO2-TRUST
delete security address-book global address RO2-TRUST-V6
delete security address-book global address ROFFICE1-PRIVATE-V6
delete security address-book global address SRV-MAIL
delete security address-book global address WAREHOUSE-HONEYPOT
delete security address-book global address WAREHOUSE-SRV-205
delete security address-book global address WAREHOUSE-SRV-206
delete security address-book global address WEBSENSE
delete security address-book global address-set CENTRAL-TESTBED
delete security address-book global address-set PRIVATE-NETWORKS-V6
delete security address-book global address-set TRUST-NETWORKS
delete security address-book global address-set TRUST-NETWORKS-V6
##Security Firewall Policy : UNTRUST - WAREHOUSE##
delete security policies from-zone UNTRUST to-zone WAREHOUSE
##Security Firewall Policy : TRUST - UNTRUST##
delete security policies from-zone TRUST to-zone UNTRUST
##Security Firewall Policy : INTERNAL - WAREHOUSE##
delete security policies from-zone INTERNAL to-zone WAREHOUSE
##Security Firewall Policy : TESTBED - WAREHOUSE##
delete security policies from-zone TESTBED to-zone WAREHOUSE
##Security Firewall Policy : WAREHOUSE - UNTRUST##
delete security policies from-zone WAREHOUSE to-zone UNTRUST
##Security Firewall Policy : INTERNAL - UNTRUST##
delete security policies from-zone INTERNAL to-zone UNTRUST
##Security Firewall Policy : UNTRUST - UNTRUST##
delete security policies from-zone UNTRUST to-zone UNTRUST
##Security Firewall Policy : TESTBED - UNTRUST##
delete security policies from-zone TESTBED to-zone UNTRUST
##Security Firewall Policy : WAREHOUSE - WAREHOUSE##
delete security policies from-zone WAREHOUSE to-zone WAREHOUSE
##Security Firewall Policy : UNTRUST - WAREHOUSE##
delete security policies from-zone UNTRUST to-zone WAREHOUSE
##Security Firewall Policy : TRUST - UNTRUST##
delete security policies from-zone TRUST to-zone UNTRUST
##Security Firewall Policy : INTERNAL - WAREHOUSE##
delete security policies from-zone INTERNAL to-zone WAREHOUSE
##Security Firewall Policy : TESTBED - WAREHOUSE##
delete security policies from-zone TESTBED to-zone WAREHOUSE
##Security Firewall Policy : WAREHOUSE - UNTRUST##
delete security policies from-zone WAREHOUSE to-zone UNTRUST
##Security Firewall Policy : INTERNAL - UNTRUST##
delete security policies from-zone INTERNAL to-zone UNTRUST
##Security Firewall Policy : UNTRUST - UNTRUST##
delete security policies from-zone UNTRUST to-zone UNTRUST
##Security Firewall Policy : TESTBED - UNTRUST##
delete security policies from-zone TESTBED to-zone UNTRUST
##Security Firewall Policy : WAREHOUSE - WAREHOUSE##
delete security policies from-zone WAREHOUSE to-zone WAREHOUSE
##Security Firewall Policy : global ##
delete security policies global policy TRUST
delete security policies global policy WAREHOUSE
delete security policies global policy INTERNET-V6
delete security policies global policy TRUST-V6
set security policies global policy PolicyEnforcer-Rule1-1 match application any
set security policies global policy PolicyEnforcer-Rule1-1 match destination-address any
set security policies global policy PolicyEnforcer-Rule1-1 match source-address JNCIE-PEG_172.16.50.100
set security policies global policy PolicyEnforcer-Rule1-1 then permit application-services advanced-anti-malware-policy JNCIE-SEC-TPP-SL2
set security policies global policy PolicyEnforcer-Rule1-1 then permit application-services security-intelligence-policy JNCIE-SEC-TPP-SL2
##Security Intelligence Policy Configurations##
set services security-intelligence policy JNCIE-SEC-TPP-SL2 CC JNCIE-SEC-TPP-SL2_CC
set services security-intelligence policy JNCIE-SEC-TPP-SL2 Infected-Hosts JNCIE-SEC-TPP-SL2_Infected-Hosts
##Security Intelligence Profile Configurations##
set services security-intelligence profile JNCIE-SEC-TPP-SL2_CC category CC
set services security-intelligence profile JNCIE-SEC-TPP-SL2_CC rule Rule-1 match threat-level 1
set services security-intelligence profile JNCIE-SEC-TPP-SL2_CC rule Rule-1 match threat-level 2
set services security-intelligence profile JNCIE-SEC-TPP-SL2_CC rule Rule-1 match threat-level 3
set services security-intelligence profile JNCIE-SEC-TPP-SL2_CC rule Rule-1 match threat-level 4
set services security-intelligence profile JNCIE-SEC-TPP-SL2_CC rule Rule-1 match threat-level 5
set services security-intelligence profile JNCIE-SEC-TPP-SL2_CC rule Rule-1 then action permit
set services security-intelligence profile JNCIE-SEC-TPP-SL2_CC rule Rule-1 then log
set services security-intelligence profile JNCIE-SEC-TPP-SL2_CC rule Rule-2 match threat-level 6
set services security-intelligence profile JNCIE-SEC-TPP-SL2_CC rule Rule-2 match threat-level 7
set services security-intelligence profile JNCIE-SEC-TPP-SL2_CC rule Rule-2 match threat-level 8
set services security-intelligence profile JNCIE-SEC-TPP-SL2_CC rule Rule-2 match threat-level 9
set services security-intelligence profile JNCIE-SEC-TPP-SL2_CC rule Rule-2 match threat-level 10
set services security-intelligence profile JNCIE-SEC-TPP-SL2_CC rule Rule-2 then action block drop
set services security-intelligence profile JNCIE-SEC-TPP-SL2_CC rule Rule-2 then log
set services security-intelligence profile JNCIE-SEC-TPP-SL2_Infected-Hosts category Infected-Hosts
set services security-intelligence profile JNCIE-SEC-TPP-SL2_Infected-Hosts rule Rule-1 match threat-level 1
set services security-intelligence profile JNCIE-SEC-TPP-SL2_Infected-Hosts rule Rule-1 match threat-level 2
set services security-intelligence profile JNCIE-SEC-TPP-SL2_Infected-Hosts rule Rule-1 match threat-level 3
set services security-intelligence profile JNCIE-SEC-TPP-SL2_Infected-Hosts rule Rule-1 match threat-level 4
set services security-intelligence profile JNCIE-SEC-TPP-SL2_Infected-Hosts rule Rule-1 match threat-level 5
set services security-intelligence profile JNCIE-SEC-TPP-SL2_Infected-Hosts rule Rule-1 match threat-level 6
set services security-intelligence profile JNCIE-SEC-TPP-SL2_Infected-Hosts rule Rule-1 then action permit
set services security-intelligence profile JNCIE-SEC-TPP-SL2_Infected-Hosts rule Rule-1 then log
set services security-intelligence profile JNCIE-SEC-TPP-SL2_Infected-Hosts rule Rule-2 match threat-level 7
set services security-intelligence profile JNCIE-SEC-TPP-SL2_Infected-Hosts rule Rule-2 match threat-level 8
set services security-intelligence profile JNCIE-SEC-TPP-SL2_Infected-Hosts rule Rule-2 match threat-level 9
set services security-intelligence profile JNCIE-SEC-TPP-SL2_Infected-Hosts rule Rule-2 match threat-level 10
set services security-intelligence profile JNCIE-SEC-TPP-SL2_Infected-Hosts rule Rule-2 then action block drop
set services security-intelligence profile JNCIE-SEC-TPP-SL2_Infected-Hosts rule Rule-2 then log
##Advanced AntiMalware Policy Configurations##
set services advanced-anti-malware policy JNCIE-SEC-TPP-SL2 blacklist-notification log
set services advanced-anti-malware policy JNCIE-SEC-TPP-SL2 default-notification log
set services advanced-anti-malware policy JNCIE-SEC-TPP-SL2 fallback-options action permit
set services advanced-anti-malware policy JNCIE-SEC-TPP-SL2 fallback-options notification log
set services advanced-anti-malware policy JNCIE-SEC-TPP-SL2 http action block
set services advanced-anti-malware policy JNCIE-SEC-TPP-SL2 http inspection-profile default_profile
set services advanced-anti-malware policy JNCIE-SEC-TPP-SL2 http notification log
set services advanced-anti-malware policy JNCIE-SEC-TPP-SL2 verdict-threshold 6
set services advanced-anti-malware policy JNCIE-SEC-TPP-SL2 whitelist-notification log
##SSL Forward proxy Profile Configurations##
delete services ssl proxy profile CENTRAL-SSL
##UTM Configurations##
delete security utm
```

OK

© 2020 Juniper Networks, Inc. All rights reserved.

l) Return to the CLI with the central cluster (srx3/srx4) and enter configuration mode. Examine the differences between the current and previous configurations.

```
{primary:node0}
lab@central-node0> configure
warning: Clustering enabled; using private edit
warning: uncommitted changes will be discarded on exit
Entering configuration mode

{primary:node0}[edit]
lab@central-node0# show | compare rollback 1
-    proxy {
-        profile CENTRAL-SSL {
-            root-ca MY-CERT;
-            actions {
-                ignore-server-auth-failure;
-                log {
-                    all;
-                }
-            }
-        }
-    }
[edit services security-intelligence]
+    profile JNCIE-SEC-TPP-SL2_CC {
+        category CC;
+        rule Rule-1 {
+            match {
+                threat-level [ 1 2 3 4 5 ];
+            }
+            then {
+                action {
+                    permit;
+                }
+                log;
+            }
+        }
+        rule Rule-2 {
+            match {
+                threat-level [ 6 7 8 9 10 ];
+            }
+            then {
+                action {
+                    block {
+                        drop;
+                    }
+                }
+                log;
+            }
+        }
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
+    }
+    profile JNCIE-SEC-TPP-SL2_Infected-Hosts {
+        category Infected-Hosts;
+        rule Rule-1 {
+            match {
+                threat-level [ 1 2 3 4 5 6 ];
+            }
+            then {
+                action {
+                    permit;
+                }
+                log;
+            }
+        }
+        rule Rule-2 {
+            match {
+                threat-level [ 7 8 9 10 ];
+            }
+            then {
+                action {
+                    block {
+                        drop;
+                    }
+                }
+                log;
+            }
+        }
+    }
+    policy JNCIE-SEC-TPP-SL2 {
+        CC {
+            JNCIE-SEC-TPP-SL2_CC;
+        }
+        Infected-Hosts {
+            JNCIE-SEC-TPP-SL2_Infected-Hosts;
+        }
+    }
[edit services advanced-anti-malware]
+    policy JNCIE-SEC-TPP-SL2 {
+        http {
+            inspection-profile default_profile;
+            action block;
+            notification {
+                log;
+            }
+        }
+        verdict-threshold 6;
+        fallback-options {
+            action permit;
+            notification {
+                log;
+            }
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
+         }
+         default-notification {
+             log;
+         }
+         whitelist-notification {
+             log;
+         }
+         blacklist-notification {
+             log;
+         }
+     }
[edit security address-book global]
+     address JNCIE-PEG_172.16.50.100 172.16.50.100/32;
-     address CENTRAL-TRUST 172.16.50.0/24;
-     address CENTRAL-INTERNAL 172.16.55.0/24;
-     address CENTRAL-WAREHOUSE 172.16.60.0/24;
-     address CENTRAL-TESTBED6 172.16.65.0/24;
-     address CENTRAL-TESTBED7 172.16.70.0/24;
-     address SRV-MAIL 172.16.60.199/32;
-     address WAREHOUSE-SRV-205 172.16.60.205/32;
-     address WAREHOUSE-SRV-206 172.16.60.206/32;
-     address WAREHOUSE-HONEYPOT 172.16.60.207/32;
-     address RO1-TRUST 172.16.10.0/24;
-     address RO2-TRUST 172.16.20.0/24;
-     address EXA-TRUST 172.16.10.0/24;
-     address WEBSENSE 172.16.60.99/32;
-     address RO1-HOST-PRIVATE 172.16.11.50/32;
-     address RO2-SRV-WEB 172.16.21.2/32;
-     address RO2-SRV-DB 172.16.21.33/32;
-     address EXA-SRV-WEB 172.16.30.11/32;
-     address EXA-SRV-DB 172.16.30.12/32;
-     address EXA-SRV-SSH 172.16.30.13/32;
-     address EXA-PRIVATE 172.16.15.0/24;
-     address HOFFICE-TRUST 172.16.77.0/24;
-     address EXA-TRUST-OVERLAP 172.16.110.0/24;
-     address RO1-TRUST-OVERLAP 172.16.111.0/24;
-     address BUILDING-TRUST-B1 172.16.100.0/24;
-     address BUILDING-TRUST-B2 172.16.200.0/24;
-     address BUILDING-DMZ-B2 172.16.201.0/24;
-     address BUILDING-DMZ-B1 172.16.101.0/24;
-     address CENTRAL-TRUST-V6 2016:abcd:a1::/64;
-     address RO1-TRUST-V6 2016:abcd:b1::/64;
-     address RO2-TRUST-V6 2016:abcd:c1::/64;
-     address EXA-TRUST-V6 2016:abcd:d1::/64;
-     address EXA-PRIVATE-V6 2016:abcd:d2::/64;
-     address ROFFICE1-PRIVATE-V6 2016:abcd:b2::/64;
[edit security address-book global]
-     address-set CENTRAL-TESTBED {
-         address CENTRAL-TESTBED6;
-         address CENTRAL-TESTBED7;
-     }
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
-     address-set TRUST-NETWORKS {
-         address RO1-TRUST;
-         address RO2-TRUST;
-         address CENTRAL-TRUST;
-         address HOFFICE-TRUST;
-         address EXA-TRUST-OVERLAP;
-         address RO1-TRUST-OVERLAP;
-         address BUILDING-TRUST-B1;
-         address BUILDING-TRUST-B2;
-     }
-     address-set TRUST-NETWORKS-V6 {
-         address CENTRAL-TRUST-V6;
-         address RO1-TRUST-V6;
-         address RO2-TRUST-V6;
-         address EXA-TRUST-V6;
-     }
-     address-set PRIVATE-NETWORKS-V6 {
-         address ROFFICE1-PRIVATE-V6;
-         address EXA-PRIVATE-V6;
-     }
[edit security]
-    utm {
-        custom-objects {
-            filename-extension {
-                bat-sh {
-                    value [ bat sh ];
-                }
-            }
-            url-pattern {
-                spam-sources {
-                    value [ 4.4.4.4 5.5.5.5 45.45.45.45. spam.com bad.com "spam@gmail.com"
"spam@yahoo.com" ];
-                }
-            }
-        }
-        default-configuration {
-            anti-spam {
-                type sbl;
-            }
-        }
-        feature-profile {
-            anti-spam {
-                address-blacklist spam-sources;
-                sbl {
-                    profile smtp-protect {
-                        no-sbl-default-server;
-                        spam-action block;
-                    }
-                }
-            }
-            content-filtering {
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
-                profile CENTRAL-content-filter {
-                    block-extension bat-sh;
-                    block-content-type {
-                        java-applet;
-                        http-cookie;
-                    }
-                    notification-options {
-                        type protocol-only;
-                        custom-message "Firewall blocked this content!";
-                    }
-                }
-            }
-        }
-        utm-policy CENTRAL-Content {
-            content-filtering {
-                http-profile CENTRAL-content-filter;
-                ftp {
-                    upload-profile CENTRAL-content-filter;
-                    download-profile CENTRAL-content-filter;
-                }
-            }
-        }
-        utm-policy CENTRAL-SPAM {
-            anti-spam {
-                smtp-profile smtp-protect;
-            }
-        }
-    }
[edit security policies]
-     from-zone UNTRUST to-zone WAREHOUSE {
-         policy SRV-MAIL {
-             match {
-                 source-address any;
-                 destination-address SRV-MAIL;
-                 application junos-smtp;
-             }
-             then {
-                 permit {
-                     destination-address {
-                         drop-untranslated;
-                     }
-                     application-services {
-                         utm-policy CENTRAL-SPAM;
-                     }
-                 }
-             }
-         }
-         policy SERVERS {
-             match {
-                 source-address any;
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
-                 destination-address [ WAREHOUSE-SRV-205 WAREHOUSE-SRV-206 WAREHOUSE-HONEYPOT
];
-                 application any;
-             }
-             then {
-                 permit {
-                     destination-address {
-                         drop-untranslated;
-                     }
-                     application-services {
-                         idp;
-                     }
-                 }
-             }
-         }
-         from-zone TRUST to-zone UNTRUST {
-             policy HTTP-FTP {
-                 match {
-                     source-address CENTRAL-TRUST;
-                     destination-address any;
-                     application [ junos-http junos-ftp ];
-                     dynamic-application junos:MSN;
-                 }
-                 then {
-                     permit {
-                         application-services {
-                             utm-policy CENTRAL-Content;
-                             application-traffic-control {
-                                 rule-set MEGA;
-                             }
-                         }
-                     }
-                     log {
-                         session-init;
-                         session-close;
-                     }
-                 }
-             }
-             policy INTERNET {
-                 match {
-                     source-address CENTRAL-TRUST;
-                     destination-address any;
-                     application any;
-                 }
-                 then {
-                     permit;
-                 }
-             }
-         }
-         from-zone INTERNAL to-zone WAREHOUSE {
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
-         policy WEBSENSE {
-             match {
-                 source-address CENTRAL-INTERNAL;
-                 destination-address any;
-                 application junos-http;
-             }
-             then {
-                 permit;
-             }
-         }
-     }
-     from-zone TESTBED to-zone WAREHOUSE {
-         policy WEBSENSE {
-             match {
-                 source-address CENTRAL-TESTBED;
-                 destination-address any;
-                 application junos-http;
-                 dynamic-application junos:HTTP;
-             }
-             then {
-                 permit;
-                 log {
-                     session-init;
-                     session-close;
-                 }
-             }
-         }
-     }
-     from-zone WAREHOUSE to-zone UNTRUST {
-         policy WEBSENSE {
-             match {
-                 source-address WEBSENSE;
-                 destination-address any;
-                 application junos-http;
-             }
-             then {
-                 permit;
-             }
-         }
-         policy SRV-MAIL {
-             match {
-                 source-address SRV-MAIL;
-                 destination-address any;
-                 application any;
-             }
-             then {
-                 permit;
-             }
-         }
-     }
-     from-zone INTERNAL to-zone UNTRUST {
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
-         policy INTERNET {
-             match {
-                 source-address CENTRAL-INTERNAL;
-                 destination-address any;
-                 application any;
-             }
-             then {
-                 permit;
-             }
-         }
-     }
-     from-zone UNTRUST to-zone UNTRUST {
-         policy UNTRUST {
-             match {
-                 source-address any;
-                 destination-address any;
-                 application any;
-             }
-             then {
-                 permit;
-             }
-         }
-     }
-     from-zone TESTBED to-zone UNTRUST {
-         policy HTTPS {
-             match {
-                 source-address CENTRAL-TESTBED;
-                 destination-address any;
-                 application junos-https;
-             }
-             then {
-                 permit {
-                     application-services {
-                         ssl-proxy {
-                             profile-name CENTRAL-SSL;
-                         }
-                     }
-                 }
-             }
-         }
-     }
-     from-zone WAREHOUSE to-zone WAREHOUSE {
-         policy WAREHOUSE {
-             match {
-                 source-address any;
-                 destination-address any;
-                 application any;
-             }
-             then {
-                 permit;
-             }
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
-         }
-     }
[edit security policies global]
+     policy PolicyEnforcer-Rule1-1 {
+         match {
+             source-address JNCIE-PEG_172.16.50.100;
+             destination-address any;
+             application any;
+         }
+         then {
+             permit {
+                 application-services {
+                     security-intelligence-policy JNCIE-SEC-TPP-SL2;
+                     advanced-anti-malware-policy JNCIE-SEC-TPP-SL2;
+                 }
+             }
+         }
+     }
-     policy TRUST {
-         match {
-             source-address TRUST-NETWORKS;
-             destination-address TRUST-NETWORKS;
-             application any;
-             source-identity any;
-         }
-         then {
-             permit;
-         }
-     }
-     policy WAREHOUSE {
-         match {
-             source-address any;
-             destination-address CENTRAL-WAREHOUSE;
-             application junos-ftp;
-             to-zone WAREHOUSE;
-         }
-         then {
-             permit {
-                 application-services {
-                     idp;
-                 }
-             }
-         }
-     }
-     policy INTERNET-V6 {
-         match {
-             source-address TRUST-NETWORKS-V6;
-             destination-address any;
-             application junos-http;
-         }
-         then {
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
-             permit;
-         }
-     }
-     policy TRUST-V6 {
-         match {
-             source-address TRUST-NETWORKS-V6;
-             destination-address TRUST-NETWORKS-V6;
-             application any;
-         }
-         then {
-             permit;
-         }
-     }

{primary:node0}[edit]
lab@central-node0#
```

m) Merge the current configuration with the previous configuration. Note that the new global polices conflict with some zonal policies. The conflict means the zonal policies are honored before global based polices, this idea means that the traffic from the 172.16.50.100 host is not subject to SDSN. We will fix this issue in a later step.

```
{primary:node0}[edit]
lab@srx5# rollback 1
load complete

{primary:node0}[edit]
lab@srx5# save sl2-task10-sdsn.config
Wrote 1912 lines of configuration to 'sl2-task10-sdsn.config'

{primary:node0}[edit]
lab@srx5# rollback

{primary:node0}[edit]
lab@srx5# load merge sl2-task10-sdsn.config
load complete

{primary:node0}[edit]
lab@srx5# commit and-quit
node0:
configuration check succeeds
node1:
commit complete
node0:
commit complete

{primary:node0}[edit]
lab@srx5>
```


© 2020 Juniper Networks, Inc. All rights reserved.

n) There still is a conflict between the global policies and the zone policies that will not let traffic from the 172.16.10.100 host hit the global policies with the SDSN content. Enter configuration mode and convert the zonal policies to global policies. Remember to maintain the zone to zone context for these policies.
   i. Examine the security policies

```
{primary:node0}
lab@central-node0> show configuration security policies
from-zone UNTRUST to-zone WAREHOUSE {
    policy SRV-MAIL {
        match {
            source-address any;
            destination-address SRV-MAIL;
            application junos-smtp;
        }
        then {
            permit {
                destination-address {
                    drop-untranslated;
                }
                application-services {
                    utm-policy CENTRAL-SPAM;
                }
            }
        }
    }
policy SERVERS {
    match {
        source-address any;
        destination-address [ WAREHOUSE-SRV-205 WAREHOUSE-SRV-206 WAREHOUSE-HONEYPOT ];
        application any;
    }
    then {
        permit {
            destination-address {
                drop-untranslated;
            }
            application-services {
                idp;
            }
        }
    }
}
from-zone TRUST to-zone UNTRUST {
    policy HTTP-FTP {
        match {
            source-address CENTRAL-TRUST;
            destination-address any;
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
        application [ junos-http junos-ftp ];
        dynamic-application junos:MSN;
    }
    then {
        permit {
            application-services {
                utm-policy CENTRAL-Content;
                application-traffic-control {
                    rule-set MEGA;
                }
            }
        }
        log {
            session-init;
            session-close;
        }
    }
    policy INTERNET {
        match {
            source-address CENTRAL-TRUST;
            destination-address any;
            application any;
        }
        then {
            permit;
        }
    }
}
from-zone INTERNAL to-zone WAREHOUSE {
    policy WEBSENSE {
        match {
            source-address CENTRAL-INTERNAL;
            destination-address any;
            application junos-http;
        }
        then {
            permit;
        }
    }
}
from-zone TESTBED to-zone WAREHOUSE {
    policy WEBSENSE {
        match {
            source-address CENTRAL-TESTBED;
            destination-address any;
            application junos-http;
            dynamic-application junos:HTTP;
        }
        then {
            permit;
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
            log {
                session-init;
                session-close;
            }
        }
    }
}
from-zone WAREHOUSE to-zone UNTRUST {
    policy WEBSENSE {
        match {
            source-address WEBSENSE;
            destination-address any;
            application junos-http;
        }
        then {
            permit;
        }
    }
    policy SRV-MAIL {
        match {
            source-address SRV-MAIL;
            destination-address any;
            application any;
        }
        then {
            permit;
        }
    }
}
from-zone INTERNAL to-zone UNTRUST {
    policy INTERNET {
        match {
            source-address CENTRAL-INTERNAL;
            destination-address any;
            application any;
        }
        then {
            permit;
        }
    }
}
from-zone UNTRUST to-zone UNTRUST {
    policy UNTRUST {
        match {
            source-address any;
            destination-address any;
            application any;
        }
        then {
            permit;
        }
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
    }
}
from-zone TESTBED to-zone UNTRUST {
    policy HTTPS {
        match {
            source-address CENTRAL-TESTBED;
            destination-address any;
            application junos-https;
        }
        then {
            permit {
                application-services {
                    ssl-proxy {
                        profile-name CENTRAL-SSL;
                    }
                }
            }
        }
    }
}
from-zone WAREHOUSE to-zone WAREHOUSE {
    policy WAREHOUSE {
        match {
            source-address any;
            destination-address any;
            application any;
        }
        then {
            permit;
        }
    }
}
global {
    policy PolicyEnforcer-Rule1-1 {
        match {
            source-address JNCIE-PEG_172.16.50.100;
            destination-address any;
            application any;
        }
        then {
            permit {
                application-services {
                    security-intelligence-policy JNCIE-SEC-TPP-SL2;
                    advanced-anti-malware-policy JNCIE-SEC-TPP-SL2;
                }
            }
        }
    }
}
policy TRUST {
    match {
        source-address TRUST-NETWORKS;
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
        destination-address TRUST-NETWORKS;
        application any;
        source-identity any;
    }
    then {
        permit;
    }
}
policy WAREHOUSE {
    match {
        source-address any;
        destination-address CENTRAL-WAREHOUSE;
        application junos-ftp;
        to-zone WAREHOUSE;
    }
    then {
        permit {
            application-services {
                idp;
            }
        }
    }
}
policy INTERNET-V6 {
    match {
        source-address TRUST-NETWORKS-V6;
        destination-address any;
        application junos-http;
    }
    then {
        permit;
    }
}
policy TRUST-V6 {
    match {
        source-address TRUST-NETWORKS-V6;
        destination-address TRUST-NETWORKS-V6;
        application any;
    }
    then {
        permit;
    }
}
}}
```

ii. Enter configuration mode and copy and paste the PolicyEnforcer-Rule1-1 global policy into the [edit security policies from-zone TRUST to-zone UNTRUST] configuration hierarchy.

© 2020 Juniper Networks, Inc. All rights reserved.

```
{primary:node0}
lab@central-node0> configure
warning: Clustering enabled; using private edit
warning: uncommitted changes will be discarded on exit
Entering configuration mode

{primary:node0}[edit]
lab@central-node0# edit security policies from-zone TRUST to-zone UNTRUST

{primary:node0}[edit]
lab@central-node0# edit security policies from-zone TRUST to-zone UNTRUST

{primary:node0}[edit security policies from-zone TRUST to-zone UNTRUST]
lab@central-node0# load merge terminal relative
[Type ^D at a new line to end input]
    policy PolicyEnforcer-Rule1-1 {
        match {
            source-address JNCIE-PEG_172.16.50.100;
            destination-address any;
            application any;
        }
        then {
            permit {
                application-services {
                    security-intelligence-policy JNCIE-SEC-TPP-SL1;
                    advanced-anti-malware-policy JNCIE-SEC-TPP-SL1;
                }
            }
        }
    }load complete

{primary:node0}[edit security policies from-zone TRUST to-zone UNTRUST]
lab@central-node0# up 1 delete global policy PolicyEnforcer-Rule1-1

{primary:node0}[edit security policies from-zone TRUST to-zone UNTRUST]
lab@central-node0#
```

iii. Configure the PolicyEnforcer-Rule1-1 to match on all dynamic applications

```
{primary:node0}[edit security policies from-zone TRUST to-zone UNTRUST]
lab@central-node0# set policy PolicyEnforcer-Rule1-1 match dynamic-application any
```

iv. Place the PolicyEnforcer-Rule1-1 before all the other policies in the TRUST to UNTRUST zone context.

```
{primary:node0}[edit security policies from-zone TRUST to-zone UNTRUST]
lab@central-node0# insert policy PolicyEnforcer-Rule1-1 before policy HTTP-FTP

{primary:node0}[edit security policies from-zone TRUST to-zone UNTRUST]
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
lab@central-node0# top

{primary:node0}[edit]
lab@central-node0# commit and-quit
node0:
configuration check succeeds
node1:
commit complete
node0:
commit complete
Exiting configuration mode

{primary:node0}
lab@central-node0>
```

o) You can verify the SDSN policies on in the CLI of the central cluster (srx3/4).

```
{primary:node0}
lab@central-node0> show configuration services
inactive: rpm {
    probe ping-9 {
        test icmp {
            probe-type icmp-ping;
            target address 12.34.56.78;
            probe-count 3;
            probe-interval 5;
            test-interval 15;
            thresholds {
                successive-loss 3;
                total-loss 3;
            }
            next-hop 80.1.1.9;
        }
    }
    probe ping-13 {
        test icmp {
            probe-type icmp-ping;
            target address 12.34.56.78;
            probe-count 3;
            probe-interval 5;
            test-interval 15;
            thresholds {
                successive-loss 3;
                total-loss 3;
            }
            next-hop 80.1.1.13;
        }
    }
}
application-identification {
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
    no-application-system-cache;
}
ssl {
    initiation {
        profile aamw-ssl {
            trusted-ca [ aamw-secintel-ca aamw-cloud-ca ];
            client-certificate aamw-srx-cert;
            actions {
                crl {
                    disable;
                }
            }
        }
    }
    proxy {
        profile CENTRAL-SSL {
            root-ca MY-CERT;
            actions {
                ignore-server-auth-failure;
                log {
                    all;
                }
            }
        }
    }
}
security-intelligence {
    url https://10.10.1.123:443/api/v1/manifest.xml;
    authentication {
        auth-token PKY8AM0SYQ492TPA00IGI82YG9BJ4RWZ;
    }
    profile JNCIE-SEC-TPP-SL2_CC {
        category CC;
        rule Rule-1 {
            match {
                threat-level [ 1 2 3 4 5 ];
            }
            then {
                action {
                    permit;
                }
                log;
            }
        }
        rule Rule-2 {
            match {
                threat-level [ 6 7 8 9 10 ];
            }
            then {
                action {
                    block {
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
                    drop;
                }
            }
            log;
        }
    }
}
profile JNCIE-SEC-TPP-SL2_Infected-Hosts {
    category Infected-Hosts;
    rule Rule-1 {
        match {
            threat-level [ 1 2 3 4 5 6 ];
        }
        then {
            action {
                permit;
            }
            log;
        }
    }
    rule Rule-2 {
        match {
            threat-level [ 7 8 9 10 ];
        }
        then {
            action {
                block {
                    drop;
                }
            }
            log;
        }
    }
}
policy JNCIE-SEC-TPP-SL2 {
    CC {
        JNCIE-SEC-TPP-SL2_CC;
    }
    Infected-Hosts {
        JNCIE-SEC-TPP-SL2_Infected-Hosts;
    }
}
advanced-anti-malware {
    connection {
        url https://srxapi.us-west-2.sky.junipersecurity.net;
        authentication {
            tls-profile aamw-ssl;
        }
    }
    policy JNCIE-SEC-TPP-SL2 {
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
http {
    inspection-profile default_profile;
    action block;
    notification {
        log;
    }
}
verdict-threshold 6;
fallback-options {
    action permit;
    notification {
        log;
    }
    default-notification {
        log;
    }
    whitelist-notification {
        log;
    }
    blacklist-notification {
        log;
    }
}
user-identification {
    active-directory-access {
        domain jnciesec.inetzero.com {
            user {
                administrator;
                password "$9$6uSOCpOMWxdVYhSvLx7Vb.Pfz/C"; ## SECRET-DATA
            }
            domain-controller SRV-AD {
                address 10.10.10.10;
            }
            user-group-mapping {
                ldap {
                    base DC=jnciesec,DC=inetzero,DC=com;
                }
            }
        }
    }
}
ip-monitoring {
    policy ping-9 {
        match {
            rpm-probe ping-9;
        }
        then {
            interface ge-0/0/3 {
                disable;
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
        }
    }
}
policy ping-13 {
    match {
        rpm-probe ping-13;
    }
    then {
        interface ge-7/0/3 {
            disable;
        }
    }
}
```

```
{primary:node0}
lab@central-node0> show configuration security policies from-zone TRUST to-zone UNTRUST
policy PolicyEnforcer-Rule1-1 {
    match {
        source-address JNCIE-PEG_172.16.50.100;
        destination-address any;
        application any;
        dynamic-application any;
    }
    then {
        permit {
            application-services {
                security-intelligence-policy JNCIE-SEC-TPP-SL2;
                advanced-anti-malware-policy JNCIE-SEC-TPP-SL2;
            }
        }
    }
}
policy HTTP-FTP {
    match {
```

```
    source-address CENTRAL-TRUST;
    destination-address any;
    application [ junos-http junos-ftp ];
    dynamic-application junos:MSN;
}
then {
    permit {
        application-services {
            utm-policy CENTRAL-Content;
            application-traffic-control {
                rule-set MEGA;
            }
        }
    }
    log {
        session-init;
```


© 2020 Juniper Networks, Inc. All rights reserved.

```
            session-close;
        }
    }
}
policy INTERNET {
    match {
        source-address CENTRAL-TRUST;
        destination-address any;
        application any;
    }
    then {
        permit;
    }
}
```

END SUPER LAB 2

© 2020 Juniper Networks, Inc. All rights reserved.