FORTINET NSE 7 ARCHITECT

Network Security Support Engineer

Lab Guide

for FortiOS 7.2

FORTINET Training Institute

Fortinet Training Institute - Library

https://training.fortinet.com

Fortinet Product Documentation

https://docs.fortinet.com

Fortinet Knowledge Base

https://kb.fortinet.com

Fortinet Fuse User Community

https://fusecommunity.fortinet.com/home

Fortinet Forums

https://forum.fortinet.com

Fortinet Product Support

https://support.fortinet.com

FortiGuard Labs

https://www.fortiguard.com

Fortinet Training Program Information

https://www.fortinet.com/nse-training

Fortinet | Pearson VUE

https://home.pearsonvue.com/fortinet

Fortinet Training Institute Helpdesk (training questions, comments, feedback)

https://helpdesk.training.fortinet.com/support/home

FORTINET

6/2/2023

TABLE OF CONTENTS

Firmware Version 6
Network Topology 7
Lab 1: Troubleshooting Concepts 8
Exercise 1: Using the Debug Flow to Filter Traffic 9
Analyze the Debug Flow Output on ISFW 9
Modify the Debug Flow Filter 10
Disable and Reset the Debug Flow 12
Lab 2: System Resources 13
Exercise 1: Analyzing System Information 14
Check Resource Usage 14
Exercise 2: Analyzing a Crash Log 15
Display the Processes 15
Generate a Crash Log Entry 15
Check the Crash Log 16
Lab 3: Sessions, Traffic Flow, and Networking 17
Exercise 1: Exploring the Session Table 19
Analyze the Session Table 19
Create a Dirty Session 20
Exercise 2: Troubleshooting Connectivity Issues 22
Network Topology 22
Problem Description 22
Objective 23
Tips for Troubleshooting 23
Lab 4: Security Fabric 25
Exercise 1: Troubleshooting Downstream Communication 29
Network Topology 29
Problem Description 29
Objective 29
Tips for Troubleshooting 29
Lab 5: Authentication 31
Exercise 1: Troubleshooting LDAP Authentication 33
Network Topology 33
Problem Description 33

Objectives 34
Tips for Troubleshooting 34
Lab 6: FSSO 36
Exercise 1: Troubleshooting FSSO 38
Network Topology 38
Problem Description 38
Review the FSSO Configuration on FortiGate 38
Tips for Troubleshooting 40
Lab 7: Web Filtering and Antivirus 41
Exercise 1: Troubleshooting Web Filtering 43
Network Topology 43
Problem Description 43
Objective 44
Tips for Troubleshooting 44
Exercise 2: Troubleshooting Antivirus 45
Network Topology 45
Problem Description 45
Objective 46
Tips for Troubleshooting 46
Lab 8: High Availability 47
Exercise 1: Troubleshooting High Availability 49
Network Topology 49
Problem Description 49
Objective 49
Tips for Troubleshooting 49
Disconnect NGFW-2 From the Cluster 50
Lab 9: IPsec 51
Exercise 1: Troubleshooting IPsec 53
Network Topology 53
Problem Description 53
Objective 53
Tips for Troubleshooting 53
Lab 10: IPsec—IKEv2 55
Exercise 1: Troubleshooting IPsec Using IKEv2 57
Network Topology 57
Problem Description 57
Objective 57
Change the Firewall Rules on Linux Router 57
Tips for Troubleshooting 58
Lab 11: Routing 59
Exercise 1: Testing the Failover of Existing Sessions 62

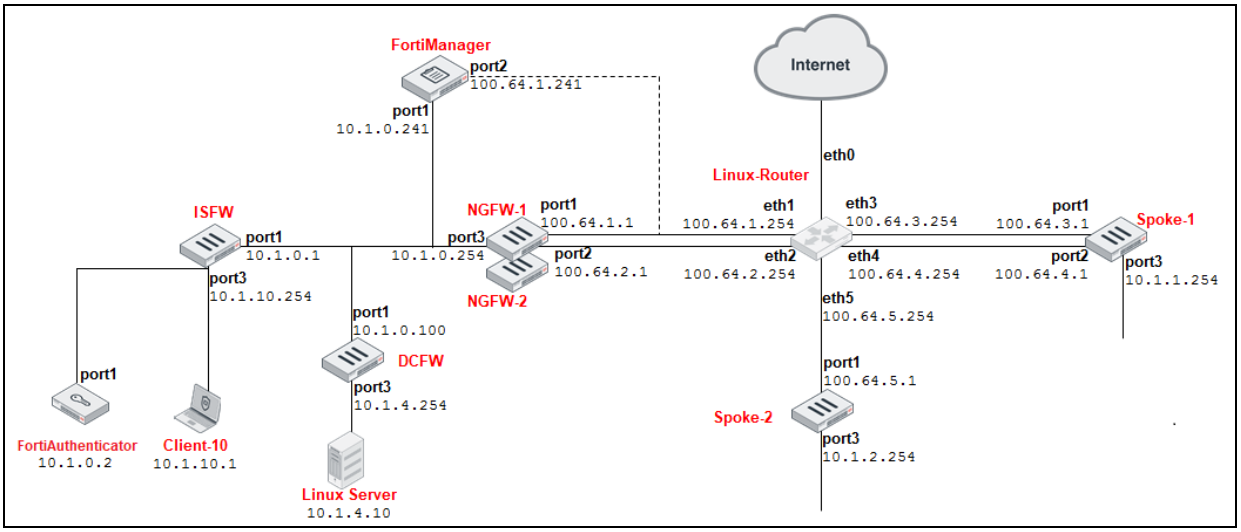
Check the Routing Table 62
Test the Primary Default Route 63
Test the Failover 63
Test the Failback 64
Exercise 2: Troubleshooting Routing 65
Prerequisites 65
Network Topology 66
Problem Description 66
Objectives 66
Tips for Troubleshooting 66
Lab 12: BGP Troubleshooting 68
Exercise 1: Troubleshooting the BGP Neighbors 70
Problem Description 70
Objective 70
Tips for Troubleshooting 71
Exercise 2: Troubleshooting BGP Routing 72
Network Topology 72
Problem Description 72
Objective 72
Tips for Troubleshooting 73
Lab 13: OSPF 74
Exercise 1: Monitoring OSPF 78
Check the Status of OSPF on NGFW-1 78
Check the Status of OSPF on DCFW and ISFW 79
Check Connectivity 79
Exercise 2: Troubleshooting OSPF 80
Network Topology 80
Problem Description 80
Objective 80
Tips for Troubleshooting 80

Firmware Version

The Network Security Support Engineer course content is based on the following products and firmware versions:

Product	Firmware Version
FortiGate	7.2.4

Network Topology



Lab 1: Troubleshooting Concepts

In this lab, you will learn how to use the debug flow command to collect debug data on a FortiGate.

Objectives

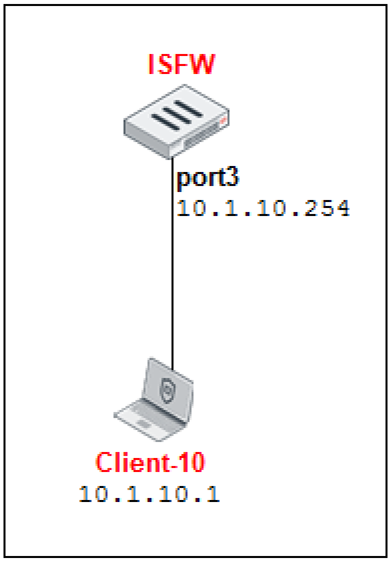
- Use filtering to make the debugging process easier by narrowing traffic down to the traffic you want to examine

Time to Complete

Estimated: 25 minutes

Which Network Segment Will You Work On?

In this lab, you will configure the ISFW FortiGate.



VM Usernames and Passwords

VM	Username	Password
Client-10	student	password
ISFW	admin	password

Exercise 1: Using the Debug Flow to Filter Traffic

In this exercise, you will configure the debug filter to analyze specific traffic.

Analyze the Debug Flow Output on ISFW

You will use the debug flow filter to make the debugging process easier by narrowing traffic down to the traffic you want to examine.

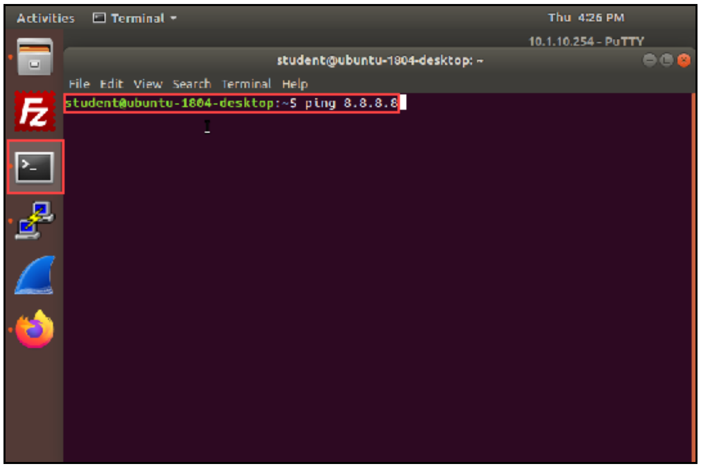
To configure the debug flow on ISFW

1. Log in to Client-10 with the username `student` and password `password`.
2. Connect over SSH to ISFW using PuTTY.
3. Log in with the username `admin` and password `password`.
4. Enter the following commands to enable and configure the debug flow filter:

```
diagnose debug disable
diagnose debug flow trace stop
diagnose debug flow filter clear
diagnose debug reset
diagnose debug flow filter addr 10.1.10.1
diagnose debug flow filter proto 1
diagnose debug flow show iprope enable
diagnose debug flow show function-name enable
diagnose debug console timestamp enable
diagnose debug flow trace start 10
diagnose debug enable
```

It is recommended that you disable the debug command and filters before you configure new filter values.

5. On Client-10, access a terminal, and then enter the `ping 8.8.8.8` command.


Activities
Terminal
Thu 4:26 PM
10.1.10.254 - PuTTY
student@ubuntu-1804-desktop: ~
File Edit View Search Terminal Help

```
student@ubuntu-1804-desktop:~$ ping 8.8.8.8
```

To monitor debug flow output

1. Return to the ISFW SSH session, and then review the debug output.

   The debug flow output should contain entries similar to the following example:

```
ISFW # id=65308 trace_id=45 func=print_pkt_detail line=5892 msg="vd-root:0
received a packet(proto=1, 10.1.10.1:19148->8.8.8.8:2048) tun_id=0.0.0.0 from
port3. type=8, code=0, id=19148, seq=1."

 id=65308 trace_id=45 func=init_ip_session_common line=6073 msg="allocate a new
session-00004097, tun_id=0.0.0.0"

 id=65308 trace_id=45 func=vf_ip_route_input_common line=2605 msg="find a route:
flag=04000000 gw-10.1.0.254 via port1"

 id=65308 trace_id=45 func=fw_forward_handler line=918 msg="Allowed by Policy-
1:"

 id=65308 trace_id=46 func=print_pkt_detail line=5892 msg="vd-root:0 received a
packet(proto=1, 8.8.8.8:19148->10.1.10.1:0) tun_id=0.0.0.0 from port1. type=0,
code=0, id=19148, seq=1."

 id=65308 trace_id=46 func=resolve_ip_tuple_fast line=5980 msg="Find an existing
session, id-00004097, reply direction "2023-01-22 19:09:51 id=65308 trace_id=46
func=vf_ip_route_input_common line=2605 msg="find a

route: flag=00000000 gw-10.1.10.1 via port3"

 id=65308 trace_id=46 func=npu_handle_session44 line=1194 msg="Trying to
offloading session from port1 to port3, skb.npu_flag=00000000
ses.state=00000204 ses.npu_state=0x00000100"

 id=65308 trace_id=46 func=fw_forward_dirty_handler line=414
msg="state=00000204, state2=00000001, npu_state=00000100"

 id=65308 trace_id=47 func=print_pkt_detail line=5892 msg="vd-root:0 received a
packet(proto=1, 10.1.10.1:19148->8.8.8.8:2048) tun_id=0.0.0.0 from port3.
type=8, code=0, id=19148, seq=2."

...
```

2. Analyze the debug output, and then answer the following questions:

   What interface is receiving the inbound packets from IP `10.1.10.1`?

   What firewall policy number is the ping traffic using?

   What interface is the gateway for this ping traffic?

Modify the Debug Flow Filter

You will modify the debug flow filter to monitor web traffic on port 443.

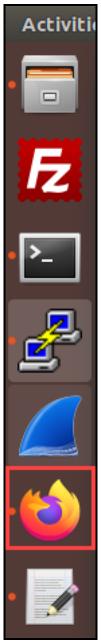
To modify the debug flow filter

1. Continuing on the SSH session, enter the following commands:

```
    diagnose debug flow filter proto 6
```

```
diagnose debug flow filter port 443
diagnose debug flow trace start 10
```

2. Under **Activities**, open FireFox.



3. Access `www.fortinet.com`.

4. Continuing on the SSH session, from the debug flow output, analyze the messages that `iprope` generated:

```
id=65308 trace_id=409 func=__iprope_check_one_policy line=2047 msg="checked
gnum-100004 policy-1, ret-matched, act-accept"

id=65308 trace_id=409 func=__iprope_user_identity_check line=1822 msg="ret-
matched"

id=65308 trace_id=409 func=__iprope_check line=2295 msg="gnum-4e20, check-
ffffffffa002c457"

id=65308 trace_id=409 func=__iprope_check_one_policy line=2047 msg="checked
gnum-4e20 policy-6, ret-no-match, act-accept"

id=65308 trace_id=409 func=__iprope_check_one_policy line=2047 msg="checked
gnum-4e20 policy-6, ret-no-match, act-accept"

id=65308 trace_id=409 func=__iprope_check_one_policy line=2047 msg="checked
gnum-4e20 policy-6, ret-no-match, act-accept"

id=65308 trace_id=409 func=__iprope_check line=2312 msg="gnum-4e20 check
result: ret-no-match, act-accept, flag-00000000, flag2-00000000"

id=65308 trace_id=409 func=__iprope_check_one_policy line=2265 msg="policy-1 is
matched, act-accept"
```

Stop and think!

When you troubleshoot why specific traffic is not matching a specific firewall policy, it is often helpful to enable the tracking of policy checking in the debug flow output. This helps you understand exactly which firewall policies are checked and eventually matched or not matched.

Disable and Reset the Debug Flow

1. Return to the ISFW SSH session.
2. Enter the following commands:

```
diagnose debug disable
diagnose debug flow trace stop
diagnose debug flow filter clear
diagnose debug reset
```

Lab 2: System Resources

In this lab, you will use system and memory debug commands to verify the status of a device. You will also manually stop a process on the device, and then view the corresponding crash log.

Objectives

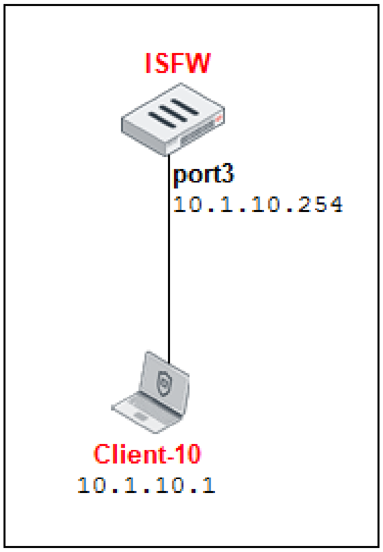
- Use debug commands to diagnose system problems
- Generate a crash log, and then analyze the output on ISFW

Time to Complete

Estimated: 25 minutes

Which Network Segment Will You Work On?

In this lab, you will access ISFW.



Exercise 1: Analyzing System Information

You will run debug commands to get information about resource usage on ISFW.

Check Resource Usage

You will use commands to get information about memory and CPU usage.

To check resource usage

1. Log in to the ISFW GUI with the username `admin` and password `password`.
2. Click **Dashboard** > **Status**.
3. Analyze the information displayed in the **System Information**, **CPU**, **Memory**, and **Sessions** widgets.
4. Connect over SSH to ISFW.
5. Log in with the username `admin` and password `password`.
6. Enter the following commands, and then analyze the output:
```
get system status
get system performance status
```
7. Enter the following commands to get more details about memory usage:
```
diagnose hardware sysinfo memory
diagnose hardware sysinfo shm
diagnose hardware sysinfo slab
diagnose hardware sysinfo conserve
```

   Using the output above, can you answer the following questions?

   - Does ISFW have a hard disk for logging?
   - How much memory is available?
   - Is ISFW in conserve mode?

8. Close the SSH session.

Exercise 2: Analyzing a Crash Log

In this exercise, you will stop a process manually on a device, and then analyze the entry generated in the crash log.

Display the Processes

You will use a diagnostics command to display the list of processes running on ISFW.

To display the processes

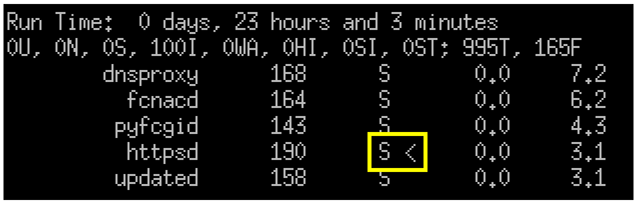
1. Connect over SSH to ISFW.
2. Log in with the username `admin` and password `password`.
3. Enter the following command to display CPU and memory usage by process:

   ```
   diagnose sys top
   ```

   What process is using the most CPU? (View the fourth column from the left.)

   What process is using the most memory? (View the second last column from the left.)
4. Can you identify which processes on ISFW are running with a high priority?

The processes that are running with a high priority are indicated with a `<`.



```
Run Time:  0 days, 23 hours and 3 minutes
0U, 0N, 0S, 100I, 0WA, 0HI, 0SI, 0ST; 995T, 165F
        dnsproxy      168      S        0.0     7.2
          fcnacd      164      S        0.0     6.2
         pyfcgid      143      S        0.0     4.3
          httpsd      190      S <      0.0     3.1
         updated      158      S        0.0     3.1
```

Don't stop the `diagnose sys top` output yet. Keep it running for the next procedure.

Generate a Crash Log Entry

You will manually stop a process to generate a crash log entry.

To generate a crash log entry

1. Continuing on the ISFW CLI, in the output of the `diagnose sys top` command, find one of the following two processes: `miglogd` or `ipshelper`.

   Do you see them running?
2. Choose one of the processes and write down its process ID (the number in the second column from the left).
3. Press `Ctrl+C` to stop the `diagnose sys top` command.
4. Use the following command to stop the process that you chose:

```
diagnose sys kill 11 <process_id>
```

You use the `kill` command in this exercise to reproduce a process failure. `11` is the kill signal that stops the process by sending a segmentation fault (number 11) signal.

5. Run the following command one more time:

   ```
   diagnose sys top
   ```

   Observe that the stopped process is running again, but this time it is using a higher ID number. Each time a process starts, it uses the next available process ID number.

6. Press `Ctrl`+`C` to stop the `diagnose sys top` output.

Check the Crash Log

You will review the entry in the crash log for the process that you stopped in the previous procedure.

To check the crash log

1. Continuing on the ISFW CLI, enter the following command:

   ```
   diagnose debug crashlog read
   ```

   The output should contain entries similar to the following example (line number and timestamp is omitted):

   ```
   <02587> firmware FortiGate-VM64 v7.2.4,build1396b1396,230131 (GA.F) (Release)
   <02587> application miglogd
   <02587> *** signal 11 (Segmentation fault) received ***
   <02587> Register dump:
   <02587> RAX: 0000000000000001 RBX: 00000000011d0ef0
   ...
   <02587> stack: 0x7ffcfaaf2a38 - 0x7ffcfaaf2e30
   <02587> Backtrace:
   <02587> [0x7fdd3336b016] => /usr/lib/x86_64-linux-gnu/libc.so.6
   ...
   (__libc_start_main+0x000000eb) liboffset 00023deb
   <02587> [0x00444f1a] => /bin/miglogd
   <02587> fortidev 6.0.1.0005
   Signal <11> was sent to process <02587> by user <admin>
   ```

2. Check the first three lines of the output.

   They contain the FortiOS build number, the name of the process that failed (or was stopped), and the kill signal number.

Lab 3: Sessions, Traffic Flow, and Networking

In this lab, you will examine how to use debug commands to troubleshoot connectivity problems. You will also analyze the information in the FortiGate session table, run the built-in sniffer, and use the debug flow to understand how FortiGate is processing each IP packet.

Objectives

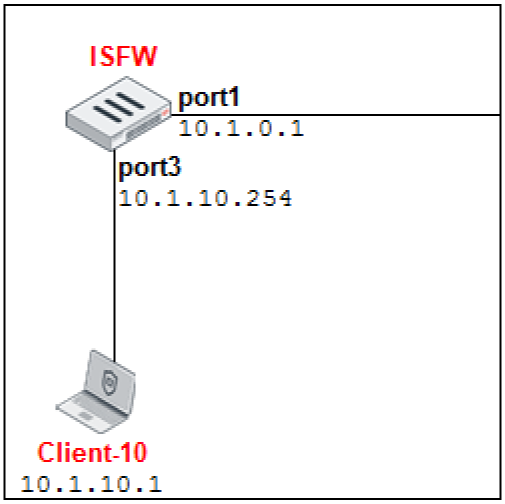
- Analyze the information in the session table
- Capture traffic using the built-in sniffer tool
- Troubleshoot IP connectivity problems

Time to Complete

Estimated: 50 minutes

Which Network Segment Will You Work On?

In this lab, you will work on Client-10 and ISFW.

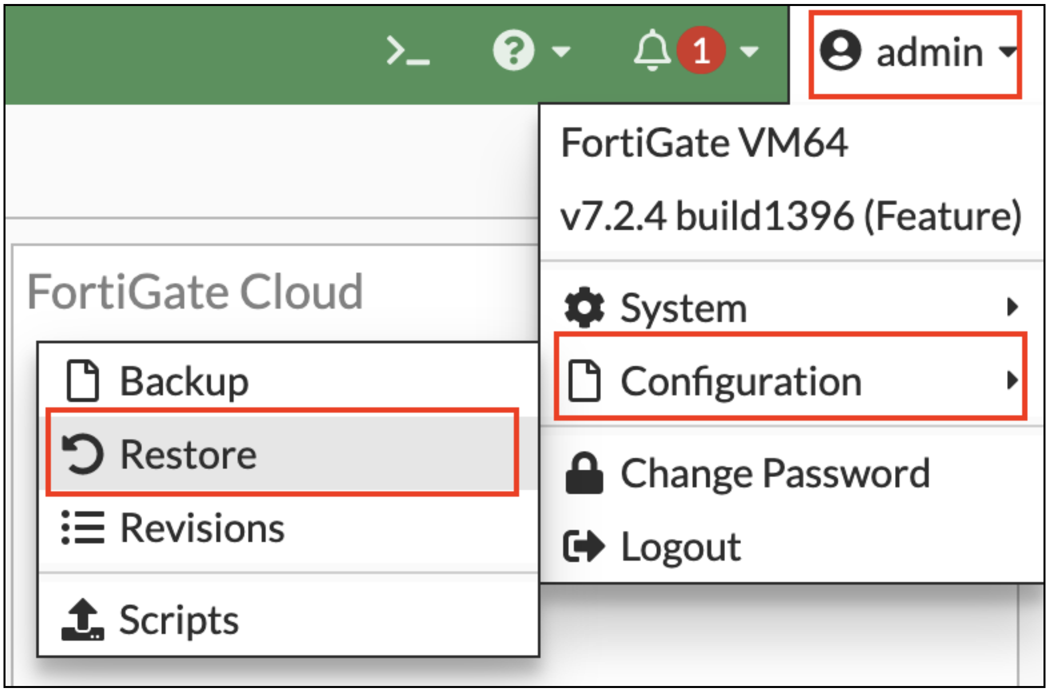


Prerequisites

Before you begin this lab, you must restore the initial configuration files to the FortiGate devices. The configuration files are located on the desktop of the Client-10 VM.

To restore the ISFW configuration file

1. Open a browser, and then log in to the ISFW GUI with the username `admin` and password `password`.
2. In the upper-right corner of the screen, click **admin**, and then click **Configuration** > **Restore**.



3. Click **Local PC**, and then click **Upload**.
4. Click **Desktop** > **Resources** > **NST** > **Session_Monitoring**, select `ISFW_Session_Monitoring.conf`, and then click **Open**.
5. Click **OK**.
6. Click **OK** to reboot.

Exercise 1: Exploring the Session Table

In this exercise, you will analyze the information displayed in the FortiGate session table.

Analyze the Session Table

You will generate SSH traffic on Client-10. Then, you will analyze the entry for this traffic created in the ISFW session table.

To analyze the session table

1. Connect to the Client-10 VM.
2. On the Client-10 VM, open a terminal session, and then enter the following command to connect over SSH to NGFW-1:

   ```
   ssh admin@10.1.0.254
   ```

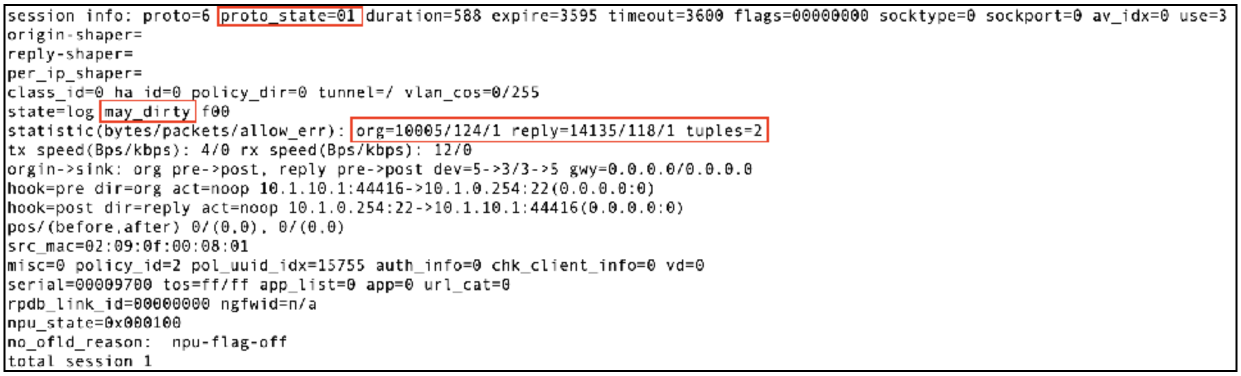
3. Enter the password `password`.

Don't close the SSH session—keep it connected.

4. Connect to the ISFW CLI using SSH.
5. Log in with the username `admin` and password `password`.
6. Enter the following debug commands:

   ```
   diagnose sys session filter clear
   diagnose sys session filter dport 22
   diagnose sys session filter dst 10.1.0.254
   diagnose sys session list
   ```

7. Analyze the information related to the SSH session created for the test traffic.



```
session info: proto=6 proto_state=01 duration=588 expire=3595 timeout=3600 flags=00000000 socktype=0 sockport=0 av_idx=0 use=3
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
state=log may_dirty f00
statistic(bytes/packets/allow_err): org=10005/124/1 reply=14135/118/1 tuples=2
tx speed(Bps/kbps): 4/0 rx speed(Bps/kbps): 12/0
orgin->sink: org pre->post, reply pre->post dev=5->3/3->5 gwy=0.0.0.0/0.0.0.0
hook=pre dir=org act=noop 10.1.10.1:44416->10.1.0.254:22(0.0.0.0:0)
hook=post dir=reply act=noop 10.1.0.254:22->10.1.10.1:44416(0.0.0.0:0)
pos/(before,after) 0/(0,0), 0/(0,0)
src_mac=02:09:0f:00:08:01
misc=0 policy_id=2 pol_uuid_idx=15755 auth_info=0 chk_client_info=0 vd=0
serial=00009700 tos=ff/ff app_list=0 app=0 url_cat=0
rpdb_link_id=00000000 ngfwid=n/a
npu_state=0x000100
no_ofld_reason:  npu-flag-off
total session 1
```

8. View the following information in the session table entry:

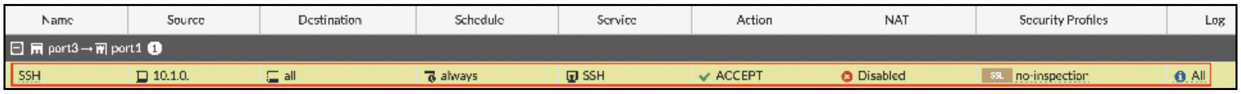
- The `may_dirty` flag
- The line containing statistics, which displays the number of SSH packets sent and received
- The protocol state, which has a value of `01`, indicating that the TCP session is established

Create a Dirty Session

You will change the configuration in the firewall policies to deny the SSH traffic coming from Client-10. Then, you will see that the `dirty` flag is added to the existing SSH session.

To change the firewall policy

1. Log in to the ISFW GUI with the username `admin` and password `password`.
2. Click **Policy & Objects** > **Firewall Policy**.
3. Edit the **SSH** firewall policy.



Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log
⊟ port3 → port1 ❶								
SSH	10.1.0.	all	always	SSH	✓ ACCEPT	Disabled	SSL no-inspection	All

4. Change the **Action** to **DENY**.
5. Click **OK**.

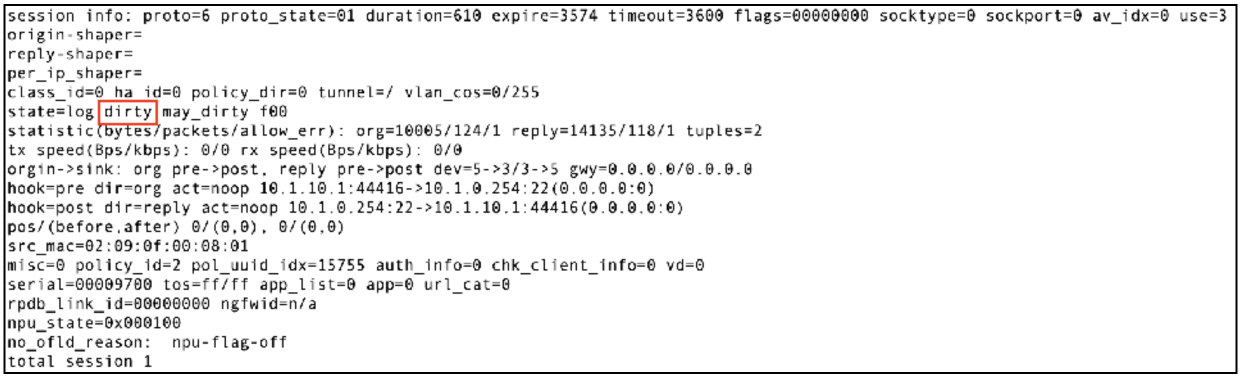
   After a firewall policy configuration change, FortiGate adds the `dirty` flag to all sessions with the `may_dirty` flag. The next time there is traffic that matches any of those sessions, FortiGate re-evaluates the action to take.

To check the dirty flag

1. Return to the ISFW CLI, and then enter the following command again:

   ```
   diagnose sys session list
   ```

   You should see the dirty flag in the output.



```
session info: proto=6 proto_state=01 duration=610 expire=3574 timeout=3600 flags=00000000 socktype=0 sockport=0 av_idx=0 use=3
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
state=log dirty may_dirty f00
statistic(bytes/packets/allow_err): org=10005/124/1 reply=14135/118/1 tuples=2
tx speed(Bps/kbps): 0/0 rx speed(Bps/kbps): 0/0
orgin->sink: org pre->post, reply pre->post dev=5->3/3->5 gwy=0.0.0.0/0.0.0.0
hook=pre dir=org act=noop 10.1.10.1:44416->10.1.0.254:22(0.0.0.0:0)
hook=post dir=reply act=noop 10.1.0.254:22->10.1.10.1:44416(0.0.0.0:0)
pos/(before,after) 0/(0,0), 0/(0,0)
src_mac=02:09:0f:00:08:01
misc=0 policy_id=2 pol_uuid_idx=15755 auth_info=0 chk_client_info=0 vd=0
serial=00009700 tos=ff/ff app_list=0 app=0 url_cat=0
rpdb_link_id=00000000 ngfwid=n/a
npu_state=0x000100
no_ofld_reason:  npu-flag-off
total session 1
```

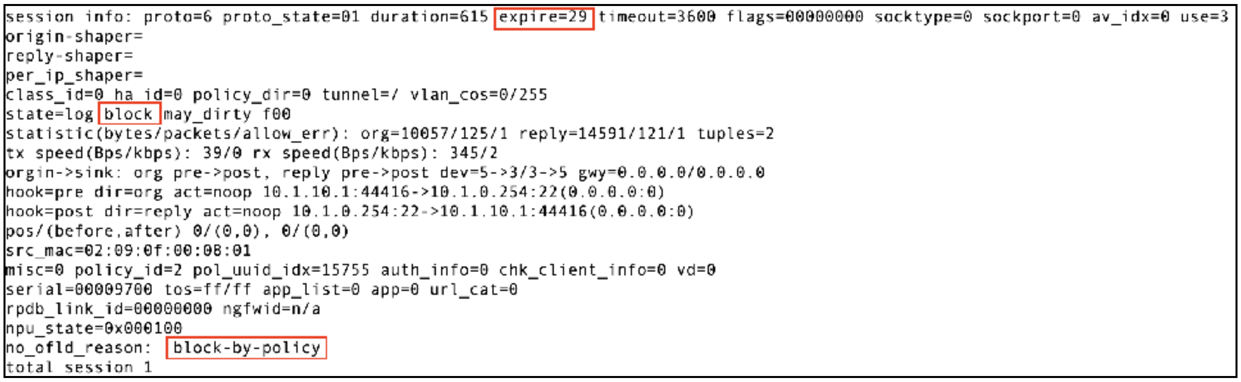
2. Return to the terminal window connected to NGFW-1, and then press some keys to generate more SSH traffic.

   There won't be any output because FortiGate is now blocking SSH, but the connection is still active.

3. Quickly return to the ISFW CLI, and then check the session information one more time, using the following command:

   ```
   diagnose sys session list
   ```

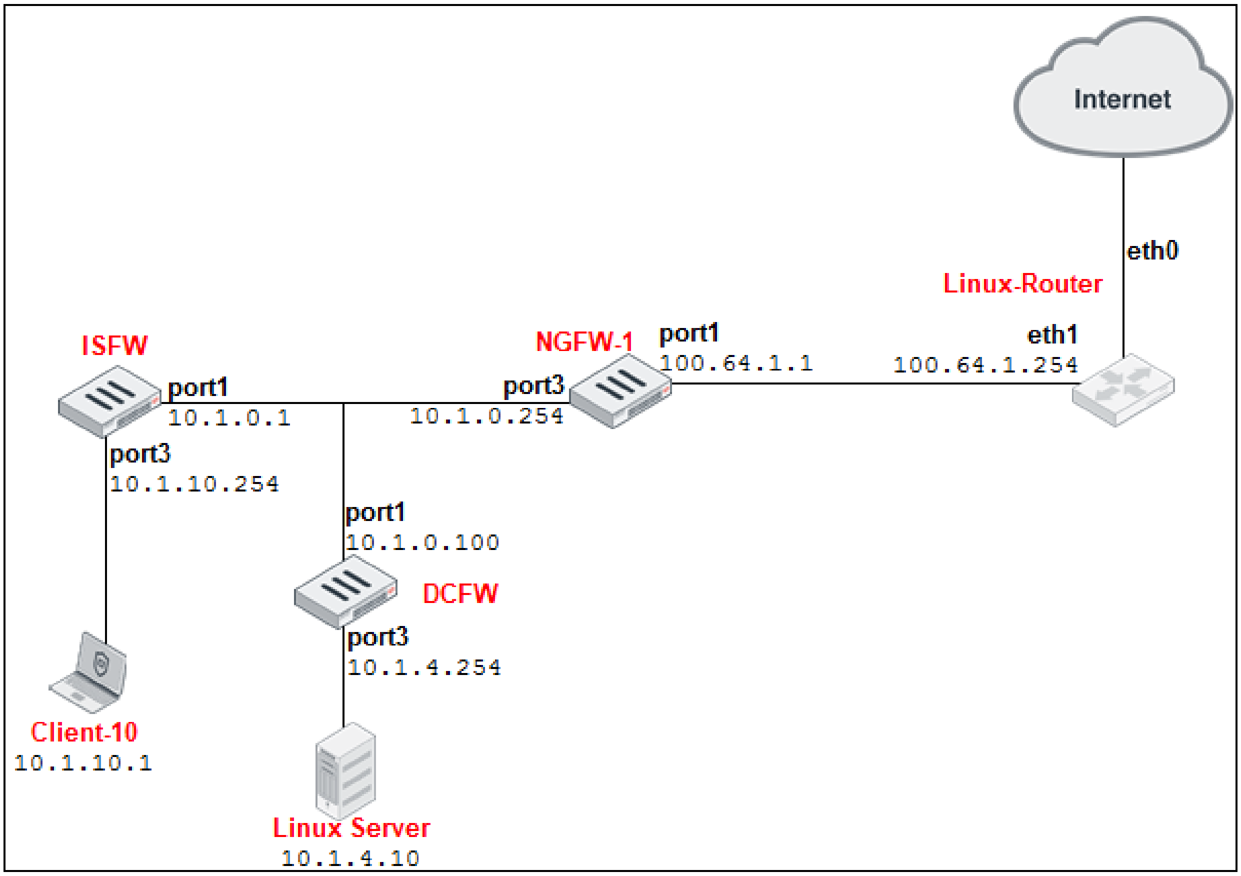
If you perform all of these steps quickly enough, you will notice that the session is still there but the `block` flag is added. FortiGate denies all traffic that matches a session with that flag. Also, the session expiration time is much smaller now. The session remains in FortiGate memory until this timer expires (30 seconds).



```
session info: proto=6 proto_state=01 duration=615 expire=29 timeout=3600 flags=00000000 socktype=0 sockport=0 av_idx=0 use=3
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
state=log block may_dirty f00
statistic(bytes/packets/allow_err): org=10057/125/1 reply=14591/121/1 tuples=2
tx speed(Bps/kbps): 39/0 rx speed(Bps/kbps): 345/2
orgin->sink: org pre->post, reply pre->post dev=5->3/3->5 gwy=0.0.0.0/0.0.0.0
hook=pre dir=org act=noop 10.1.10.1:44416->10.1.0.254:22(0.0.0.0:0)
hook=post dir=reply act=noop 10.1.0.254:22->10.1.10.1:44416(0.0.0.0:0)
pos/(before,after) 0/(0,0), 0/(0,0)
src_mac=02:09:0f:00:08:01
misc=0 policy_id=2 pol_uuid_idx=15755 auth_info=0 chk_client_info=0 vd=0
serial=00009700 tos=ff/ff app_list=0 app=0 url_cat=0
rpdb_link_id=00000000 ngfwid=n/a
npu_state=0x000100
no_ofld_reason:  block-by-policy
total session 1
```

Exercise 2: Troubleshooting Connectivity Issues

Network Topology



Problem Description

In this part of the lab, you will troubleshoot various connectivity issues on ISFW. Don't make changes on any other devices in the network.

There are three problems:

1. Although the Telnet protocol is enabled for administrative access on ISFW port3 (`10.1.10.254`), you can't access the device CLI using Telnet from Client-10 to `10.1.10.254`.
2. You can't access any public websites from Client-10.
3. You can't connect over Telnet to the Linux-Router (`100.64.1.254`) from Client-10.

To test the Telnet connections, on the Client-10 desktop, use PuTTY.

Objective

Find the causes of these problems by using debug commands first, before you look for configuration errors.

You can change only the ISFW configuration. Don’t make configuration changes on any other devices.

Tips for Troubleshooting

- Can you ping the destination IP address from Client-10?
- Use the sniffer tool to verify that the traffic is actually arriving on the port3 interface on ISFW. Use verbosity 4 and a filter that can capture the traffic in both directions.

  Examples:

  ```
  diagnose sniffer packet any "port 23 and host 10.1.10.1" 4
  diagnose sniffer packet any "port 80 and host 10.1.10.1" 4
  diagnose sniffer packet any "icmp and host 10.1.10.1" 4
  ```

- If the traffic isn't intended to terminate on FortiGate, use the sniffer again to check that the traffic is being forwarded to the next-hop IP address (use the network diagram provided). Again, use a filter in the sniffer that can capture the traffic in both directions.
- Check the session table. Is ISFW creating the session? Check the session protocol state. Do you see anything wrong there?

  ```
  diagnose sys session filter clear
  diagnose sys session filter src 10.1.10.1
  diagnose sys session filter dport <port_number>
  diagnose sys session list
  ```

- Clear the related session (if any) from the session table, enable the debug flow, and generate more test traffic. Do you see any debug flow errors?

  ```
  diagnose debug flow filter clear
  diagnose debug flow filter dport <port_number>
  diagnose debug flow filter addr 10.1.10.1
  diagnose debug flow trace start 10
  diagnose debug enable
  ```

- As a reference, the following table contains the most common debug flow error messages and possible causes:

Error	Possible cause
Denied by forward policy check (policy 0)	No firewall policy allows the traffic. A firewall policy allows the traffic but a disclaimer is enabled. You must accept the disclaimer first.
Denied by quota check	The packet was dropped because of traffic shaping.
Reverse path check fail, drop	The packet was dropped because of the reverse path forwarding check.
Iprope_in_check() check failed, drop	The packet is destined for a FortiGate IP address (management traffic) but: • The service isn't enabled. • Or, the service is using a different TCP port. • Or, the source IP address isn’t included in the trusted host list. • Or, the packet matches a local-in policy with the action deny. The packet isn't destined for a FortiGate IP address, but there is a virtual IP or IP pool configuration using the destination IP address.

Lab 4: Security Fabric

In this lab, you will use troubleshooting methodologies and commands that you learned in the Security Fabric lesson.

Objectives

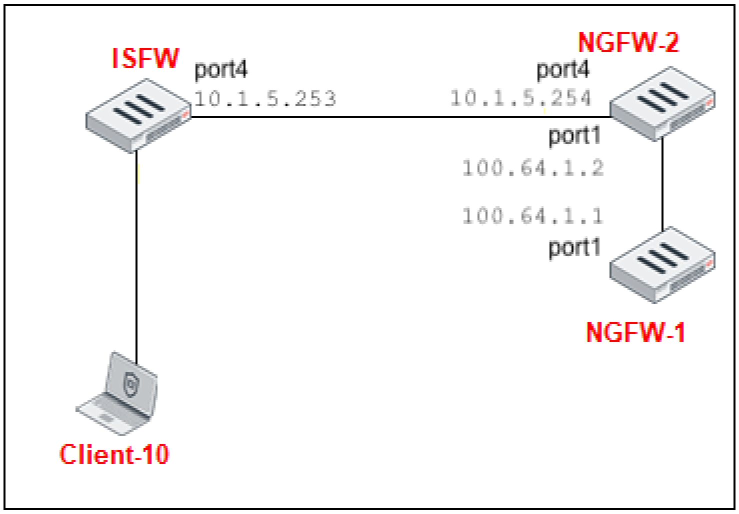
- Troubleshoot downstream communication issues
- Monitor the Security Fabric communications and status

Time to Complete

Estimated: 30 minutes

Which Network Segment Will You Work On?

In this lab, you will work on the ISFW, NGFW-2, and NGFW-1 FortiGate devices.



VM Usernames and Passwords

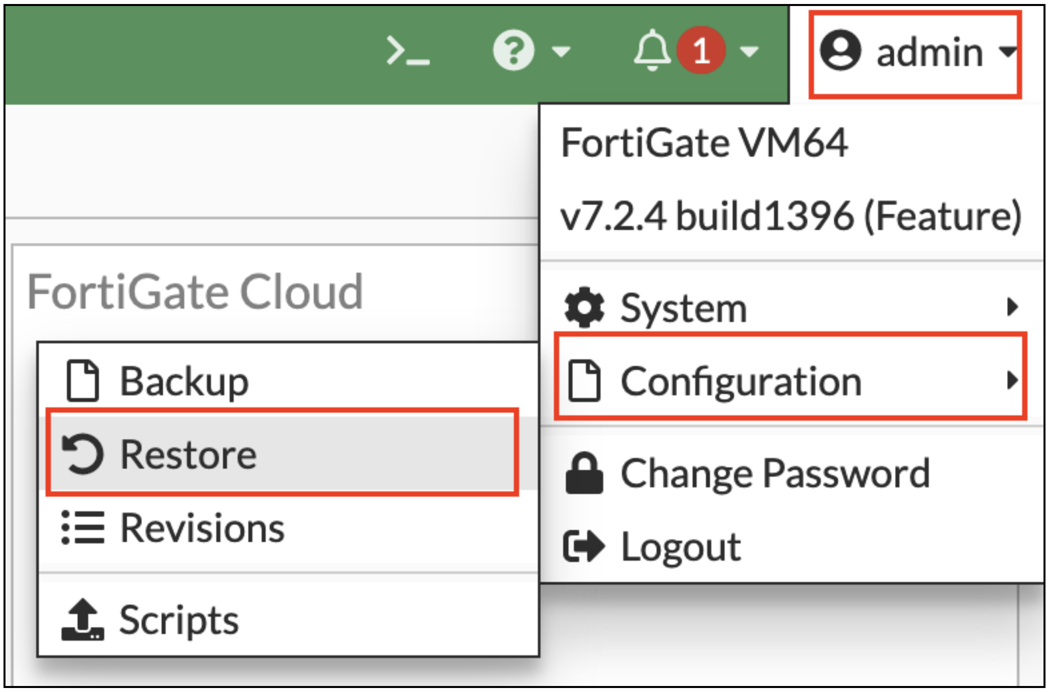
VM	Username	Password
ISFW	admin	password
NGFW-1	admin	password
NGFW-2	admin	password

Prerequisites

Before you begin this lab, you must restore the initial configuration files to the FortiGate devices. The configuration files are located on the desktop of the Client-10 VM.

To restore the NGFW-1 configuration file

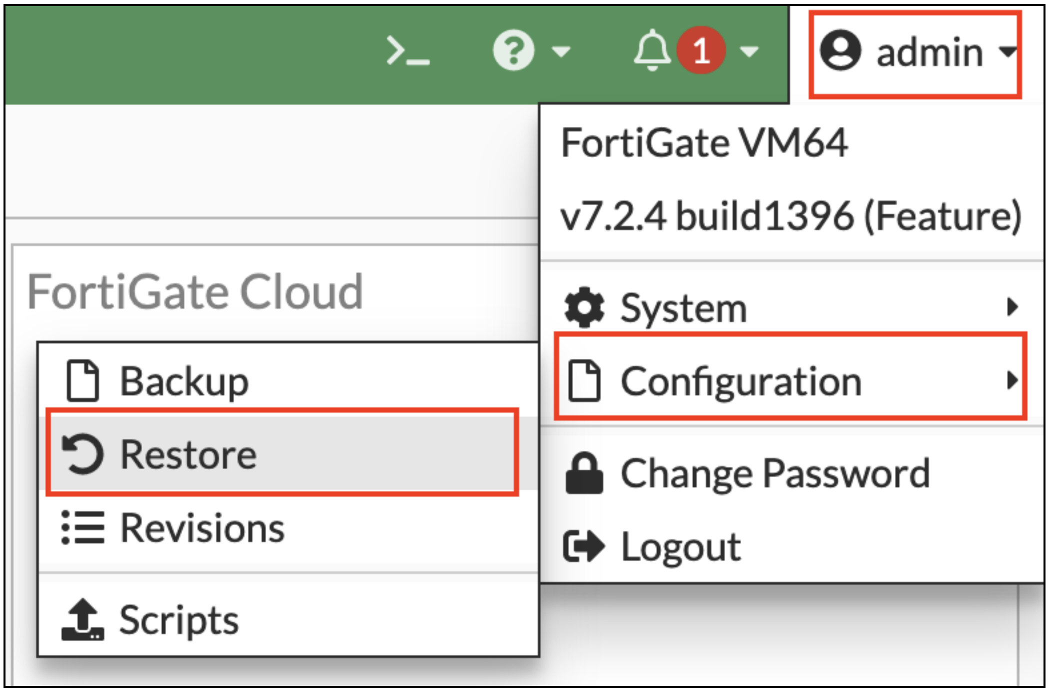
1. On the Client-10 VM, open a browser, and then log in to the NGFW-1 - GUI with the username `admin` and password `password`.
2. In the upper-right corner of the screen, click **admin**, and then click **Configuration** > **Restore**.



3. Click **Local PC**, and then click **Upload**.
4. Click **Desktop** > **Resources** > **NST** > **SecurityFabric**, select `NGFW-1_SecFab.conf`, and then click **Open**.
5. Click **OK**.
6. Click **OK** to reboot.

To restore the NGFW-2 configuration file

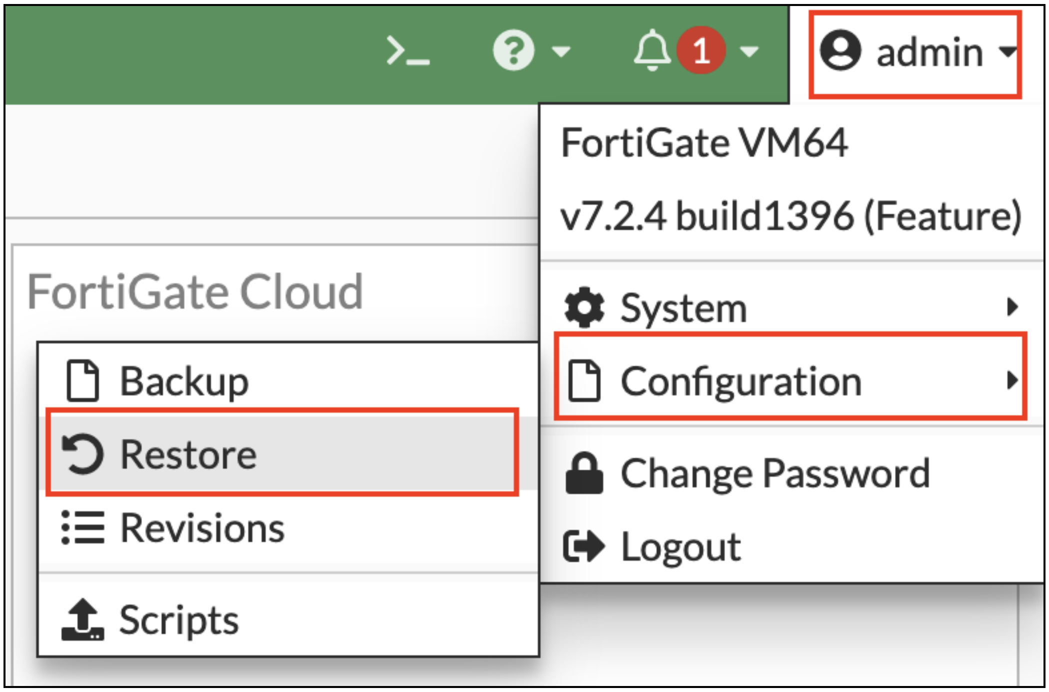
1. On the Client-10 VM, open a browser, and then log in to the NGFW-2 GUI with the username `admin` and password `password`.
2. In the upper-right corner of the screen, click **admin**, and then click **Configuration** > **Restore**.



3. Click **Local PC**, and then click **Upload**.
4. Click **Desktop** > **Resources** > **NST** > **SecurityFabric**, select `NGFW-2_SecFab.conf`, and then click **Open**.
5. Click **OK**.
6. Click **OK** to reboot.

To restore the ISFW configuration file

1. On the Client-10 VM, open a browser, and then log in to the ISFW- GUI with the username `admin` and password `password`.
2. In the upper-right corner of the screen, click **admin**, and then click **Configuration** > **Restore**.

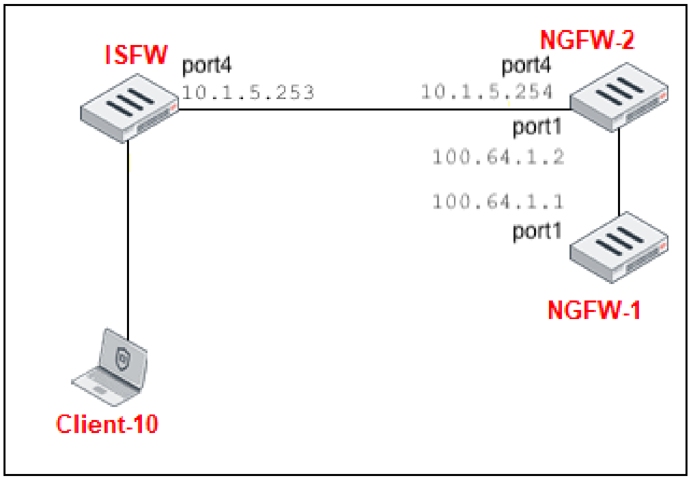


3. Click **Local PC**, and then click **Upload**.
4. Click **Desktop** > **Resources** > **NST** > **SecurityFabric**, select `ISFW_SecFab.conf`, and then click **Open**.
5. Click **OK**.
6. Click **OK** to reboot.

Exercise 1: Troubleshooting Downstream Communication

In this exercise, you will troubleshoot Security Fabric communication issues between NGFW-1 and ISFW.

Network Topology



Problem Description

NGFW-1 is supposed to join the Security Fabric where ISFW is the root. NGFW-2 is located between NGFW-1 and ISFW. NGFW-1 is unable to join the Security Fabric.

Objective

Use the knowledge you gained in the lesson, as well as Security Fabric diagnostic commands, to troubleshoot and fix the communication problems. You should also use the sniffer and flow tools. You will achieve the objective when NGFW-1 successfully joins the Security Fabric.

Tips for Troubleshooting

- Do not log in to the GUI and perform configuration changes right away.
- Remember the potential issues that can cause communication issues.
- Use the Security Fabric debug commands.

```
diagnose test application csfd 1
diagnose sys csf upstream
diagnose sys csf downstream
```

- Use the sniffer and flow tools to analyze Security Fabric traffic.
- What configuration changes can you make on NGFW-2 to fix the problems?
- Before you authorize NGFW-1 on ISFW, enable the real-time debug on both ISFW and NGFW-1, and then observe the output.

```
diagnose debug application csfd -1
diagnose debug enable
```

- After you finish analyzing the output, remember to disable the real- time debug:

```
diagnose debug reset
```

Lab 5: Authentication

In this lab, you will learn to use the authentication and LDAP debug commands to troubleshoot an authentication issue.

Objectives

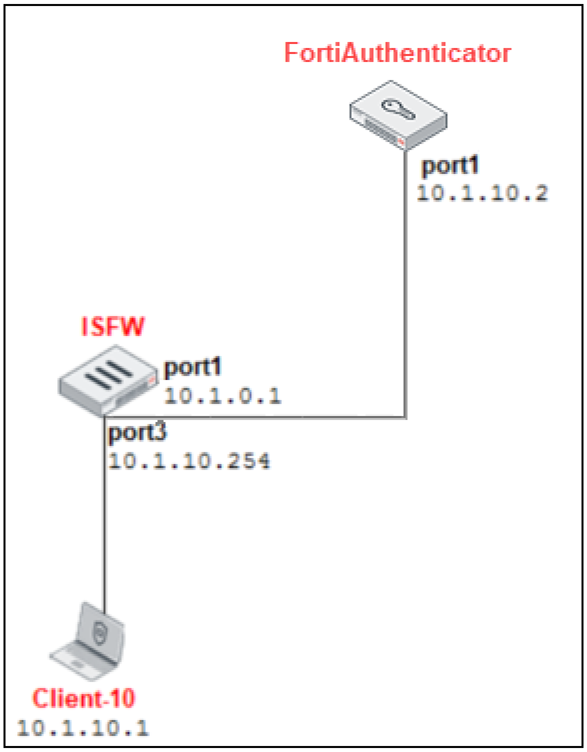
- Monitor the status of authenticated users
- Troubleshoot problems related to LDAP authentication

Time to Complete

Estimated: 40 minutes

Which Network Segment Will You Work On?

In this lab, you will work on ISFW and FortiAuthenticator.

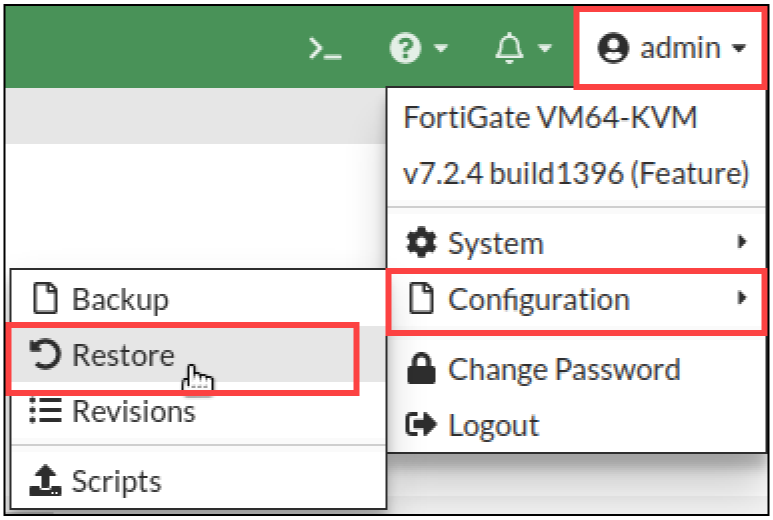


Prerequisites

Before you begin this lab, you must restore the initial configuration files to the FortiGate devices. The configuration files are located on the desktop of the Client-10 VM.

To restore the ISFW-1 configuration file

1. On the Client-10 VM, open a browser, and then log in to the ISFW GUI with the username `admin` and password `password`.
2. In the upper-right corner, click **admin**, and then click **Configuration** > **Restore**.

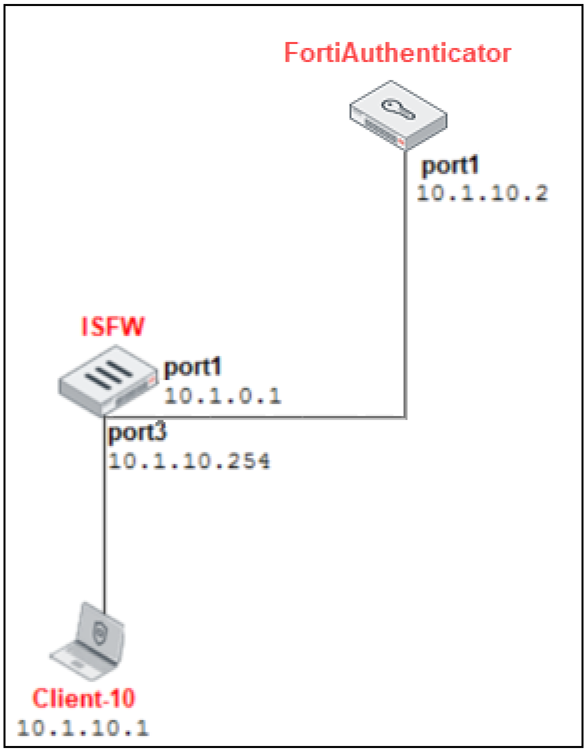


3. Click **Local PC**, and then click **Upload**.
4. Click **Desktop** > **Resources** > **NST** > **Authentication**, select `ISFW_Authentication.conf`, and then click **Open**.
5. Click **OK**.
6. Click **OK** to reboot.

Exercise 1: Troubleshooting LDAP Authentication

In this exercise, you will diagnose the authentication negotiation between FortiGate and an LDAP server.

Network Topology



Problem Description

An administrator has configured ISFW to perform LDAP authentication against a FortiAuthenticator located at `10.1.10.2`. However, the captive portal is failing.

Two LDAP users have been created on the LDAP server:

- Username: student, password: Fort1net
  - Must not have access to information technology sites like www.fortinet.com
  - Belongs to the following LDAP group:

    `CN= Users,OU=Training,DC=trainingAD,DC=training,DC=lab`
- Username: aduser1, password: password
  - No internet access restrictions
  - Belongs to the following LDAP group:

    `CN= AD_users,OU=Training,DC=trainingAD,DC=training,DC=lab`

Objectives

- Use the authentication and LDAP debug commands you learned to isolate and fix the problem
- Explain why FortiGate is not challenging users to authenticate
- Change the FortiGate configuration to fix the problem
- Verify that when a user browses the internet, ForitGate sends the authentication request to the LDAP server

Tips for Troubleshooting

- Test LDAP authentication, on the CLI, after you enable the real-time debug.

```
diagnose debug application fnbamd -1
diagnose debug enable
diagnose test authserver ldap External-LDAP aduser1 password
diagnose test authserver ldap External-LDAP student Fort1net
```

- Once the LDAP CLI test works, check the firewall authentication by browsing the internet from Client-10. Look at the session table or run the debug flow to determine which firewall policy is matching the traffic.

  Access www.fortinet.com—is user authentication requested?

  - Monitor authenticated users.

```
diagnose firewall auth list
```

  - Analyze the session table, and verify if there is user authentication information in the session that was created. If it is not populated, what is the reason? The following is a session information example:

```
diagnose sys session filter dport 80
diagnose sys session filter policy 1
diagnose sys session list

session info: proto=6 proto_state=11 duration=8 expire=3593 timeout=3600
    flags=00000000 socktype=0 sockp
ort=80 av_idx=1 use=5
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
user=student auth_server=External-LDAP state=redir log local may_dirty authed f00
    acct-ext
statistic(bytes/packets/allow_err): org=1742/9/1 reply=2545/5/1 tuples=3
tx speed(Bps/kbps): 206/1 rx speed(Bps/kbps): 301/2
orgin->sink: org pre->post, reply pre->post dev=5->3/3->5 gwy=10.1.0.254/0.0.0.0
hook=post dir=org act=snat 10.1.10.1:35024->72.21.91.29:80(10.1.0.1:35024)
hook=pre dir=reply act=dnat 72.21.91.29:80->10.1.0.1:35024(10.1.10.1:35024)
hook=post dir=reply act=noop 72.21.91.29:80->10.1.10.1:35024(0.0.0.0:0)
pos/(before,after) 0/(0,0), 0/(0,0)
misc=0 policy_id=1 pol_uuid_idx=15749 auth_info=3 chk_client_info=0 vd=0
serial=00010454 tos=40/40 app_list=0 app=0 url_cat=0
rpdb_link_id=00000000 ngfwid=n/a
npu_state=0x000100
no_ofld_reason: redir-to-av
```

- After any configuration change, deauthenticate the users from the FortiGate and clear the browser cache. It is also recommended that you clear the related entries in the session table.

```
diagnose sys session filter dport 80
diagnose sys session filter policy <policy ID>
diagnose sys session clear
```

- To deauthenticate users, use the following command:

```
diagnose firewall auth clear
```

Lab 6: FSSO

In this lab, you will test user authentication using FSSO. The lab uses a demo environment to emulate the behavior of an active FSSO DC agent from the Local-Client VM using a Python script. Therefore, you will not configure a DC agent to send logon events from the Local-Client VM.

Objectives

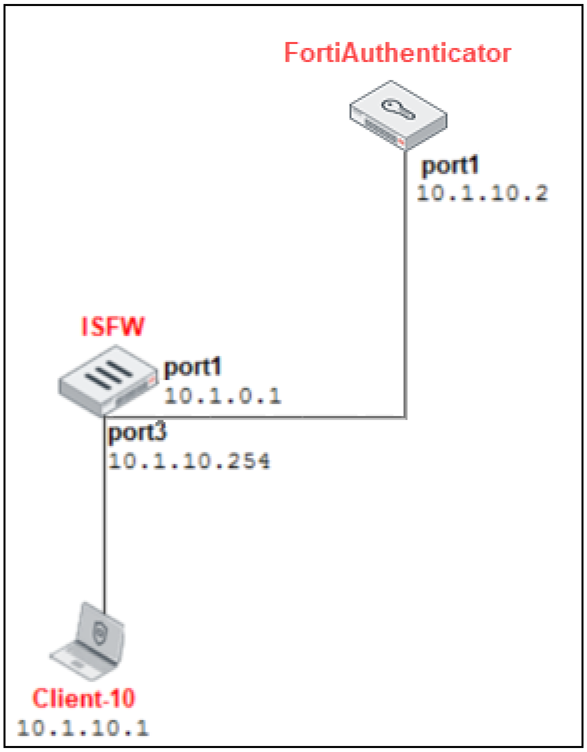
- Use the authentication and FSSO debug commands you learned to isolate and fix the problem
- Explain why FortiGate is allowing internet access to the current user on Client-10
- Change the FortiGate configuration to fix the problem

Time to Complete

Estimated: 35 minutes

Which Network Segment Will You Work On?

In this lab, you will work on ISFW and FortiAuthenticator.

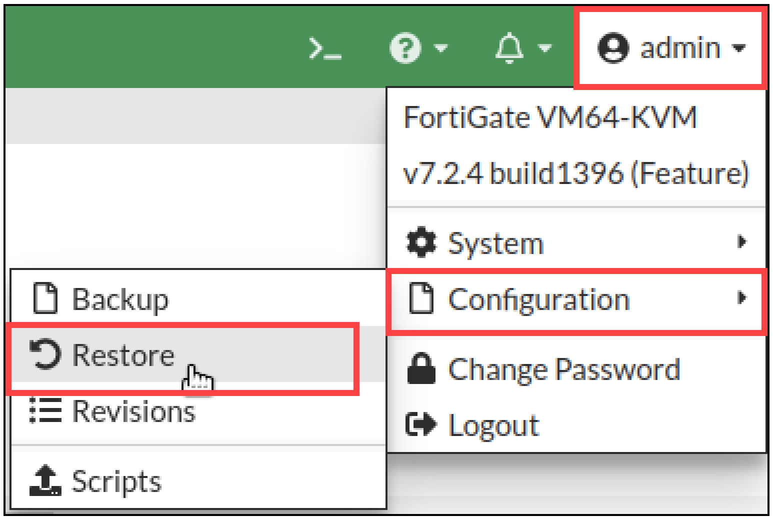


Prerequisites

Before you begin this lab, you must restore the initial configuration files to the FortiGate devices. The configuration files are located on the desktop of the Client-10 VM.

To restore the ISFW configuration file

1. On the Client-10 VM, open a browser, and then log in to the ISFW- GUI with the username `admin` and password `password`.
2. In the upper-right corner, click **admin**, and then click **Configuration** > **Restore**.

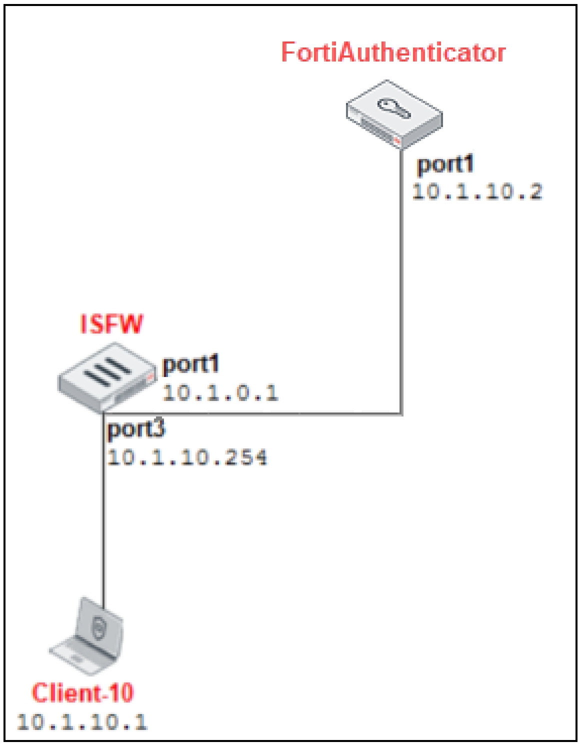


3. Click **Local PC**, and then click **Upload**.
4. Click **Desktop** > **Resources** > **NST** > **FSSO**, select `ISFW_FSSO.conf`, and then click **Open**.
5. Click **OK**.
6. Click **OK** to reboot

Exercise 1: Troubleshooting FSSO

In this exercise, you will monitor and troubleshoot FSSO authentication to grant internet access.

Network Topology



Problem Description

In this exercise, an administrator has configured the ISFW FortiGate to allow internet access only to active FSSO users. However, it is not working—active FSSO users do not have internet access.

Use the authentication and FSSO debug commands that you learned to isolate and fix the problem.

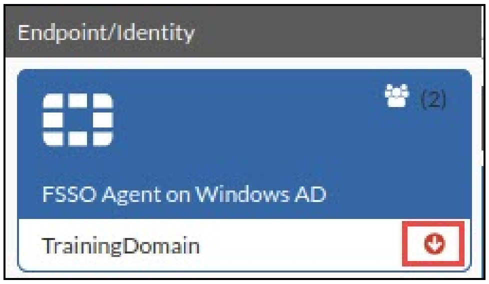
Review the FSSO Configuration on FortiGate

You will review the FSSO configuration and FSSO user groups on FortiGate. FSSO allows FortiGate to automatically identify the users who connect using SSO.

To review the FSSO server and FSSO user group configuration on FortiGate

1. On the ISFW GUI, log in with the username `admin` and password `password`.
2. Click **Security Fabric** > **External Connectors**.

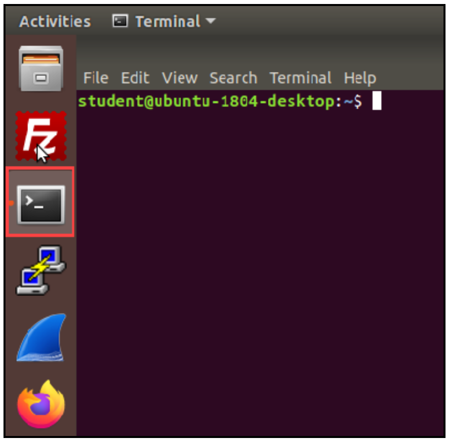
3. Select **TrainingDomain**, and then click **Edit**.



4. In the upper-right corner, review the **Endpoint/Identity** status, and notice that the status is **Disconnected**.
5. Leave the window open.

To run a script to simulate a user logon event

1. On the Client-10 VM, open a terminal window.



```
student@ubuntu-1804-desktop:~$
```

2. Enter the following commands to simulate a user logon event:

```
cd Desktop/FSSO/
python2 fssoreplay.py -l 8000 -f sample.log
```

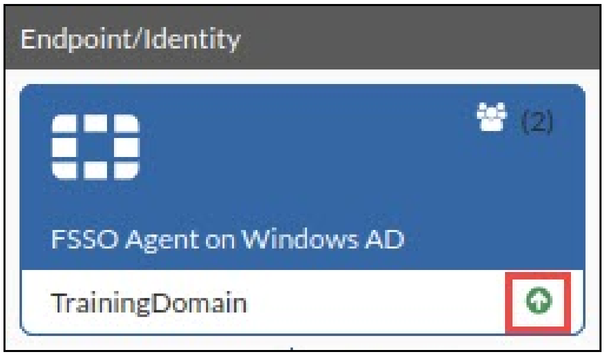
3. Keep the terminal window open.

   The script continues to run in the background.

To review the FSSO connection and FSSO user groups

1. Return to the ISFW GUI, and then in the **TrainingDomain** window, click **Apply & Refresh**.
2. Select **TrainingDomain**, and then click **Edit**.
3. In the **Users/Groups** field, click **View**.
4. Click **X** to close the **Collector Agent Group Filters** window.
5. Click **OK**.

   A green up arrow confirms that communication with the FSSO collector agent is up.



Tips for Troubleshooting

- Use the following command to check the active FSSO users on FortiGate:

```
diagnose debug authd fsso list
```

- Use the FortiGate real-time debug commands for FSSO:

```
diagnose debug application authd 8256
diagnose debug enable
```

- Use the following commands to reset the debug command:

```
diagnose debug disable
diagnose debug reset
```

Lab 7: Web Filtering and Antivirus

In this lab, you will test the configuration by generating traffic from Client-10. Additionally, you will troubleshoot a web filtering problem and an antivirus event.

Objectives

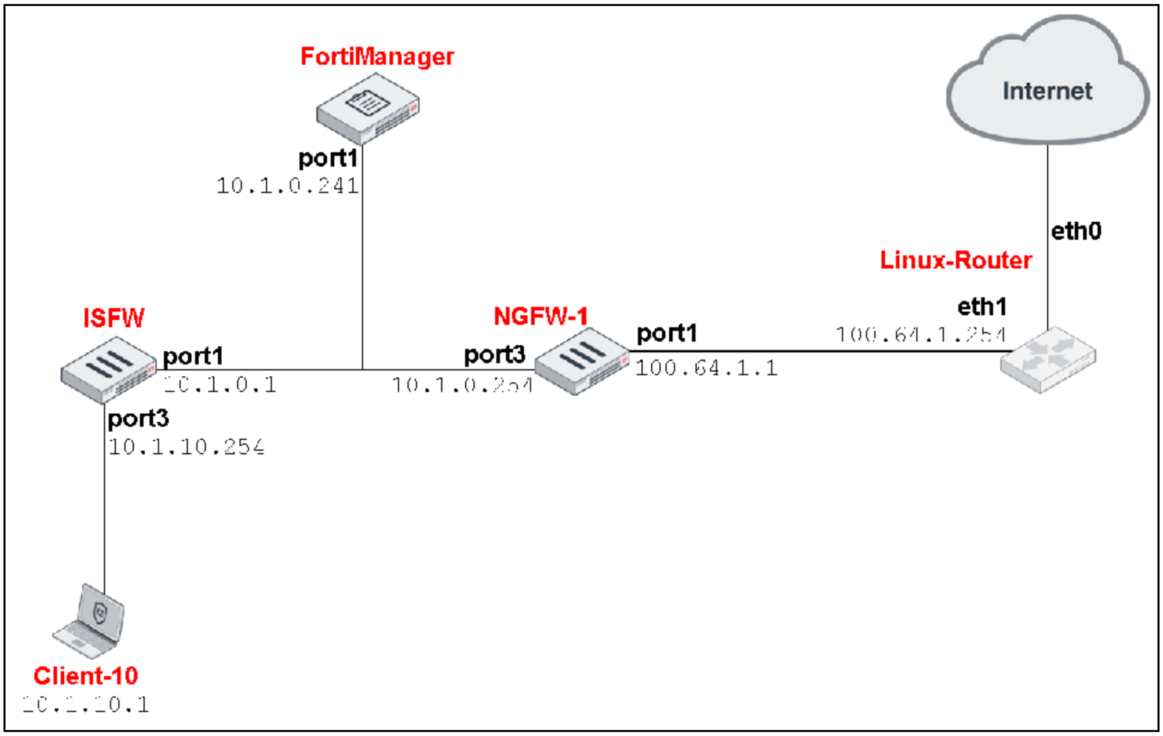
- Troubleshoot a web filtering problem
- Troubleshoot an antivirus event

Time to Complete

Estimated: 45 minutes

Which Network Segment Will You Work On?

You will configure web filtering and antivirus on ISFW. Then, you will generate test traffic from Client-10.

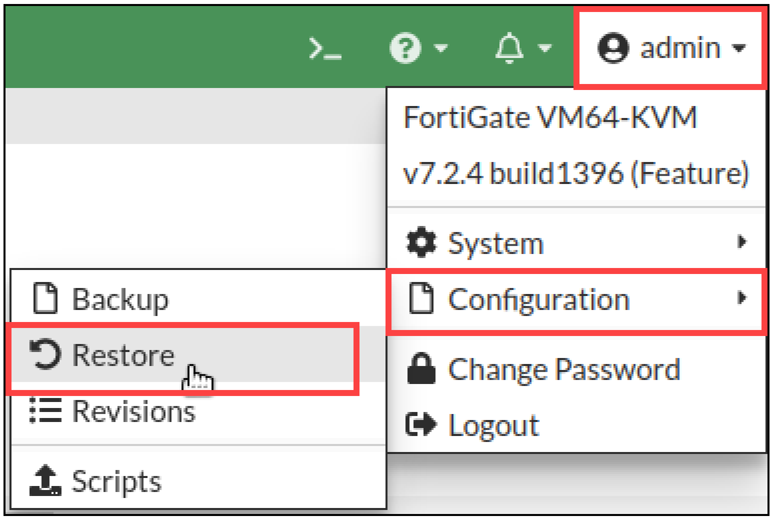


Prerequisites

Before you begin this lab, you must restore the initial configuration file to the FortiGate. The configuration files are located on the desktop of the Client-10 VM.

To restore the ISFW configuration file

1. On the Client-10 VM, open a browser, and then log in to the ISFW GUI with the username `admin` and password `password`.
2. In the upper-right corner of the screen, click **admin**, and then click **Configuration** > **Restore**.

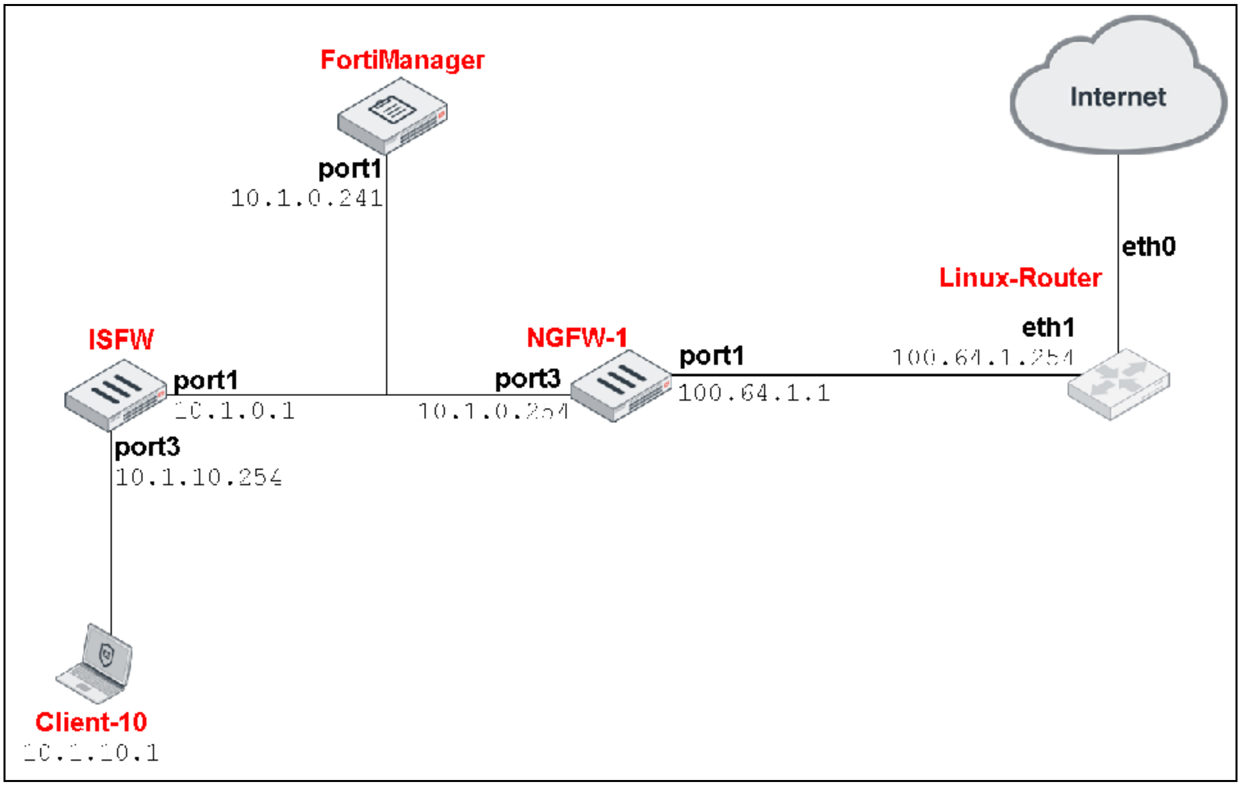


3. Click **Local PC**, and then click **Upload**.
4. Click **Desktop** > **Resources** > **NST** > **WF_&_AV**, select `ISFW_WF_AV.conf`, and then click **Open**.
5. Click **OK**.
6. Click **OK** to reboot.

Exercise 1: Troubleshooting Web Filtering

In this exercise, you will learn how to identify FortiGuard categories.

Network Topology



Problem Description

ISFW has a web filter configured for the internet traffic coming from Client-10. The applied web filter blocks the following FortiGuard categories:

- Bandwidth Consuming
- Adult/Mature Content
- Security Risk

Many restricted sites seem to be correctly blocked, such as:

- www.youtube.com
- www.tunein.com

However, the following site is not blocked. According to users, it should be blocked because it belongs to the **Security Risk** category.

- www.eicar.org

Objective

Use the web filtering debug commands available on ISFW to find out why the website is not being blocked.

Tips for Troubleshooting

- Clear the browser cache before each test. Also, clear the FortiGate web filtering cache, using the following command:

```
diagnose test application urlfilter 2
```

- Enable the following real-time debug while browsing the website:

```
diagnose debug application urlfilter -1
diagnose debug enable
```

Can you spot how FortiGuard is categorizing the website?

The output can be verbose, so save it from the SSH session to a local file.

If you want to verify the category codes, use the following CLI command:

```
get webfilter categories
```

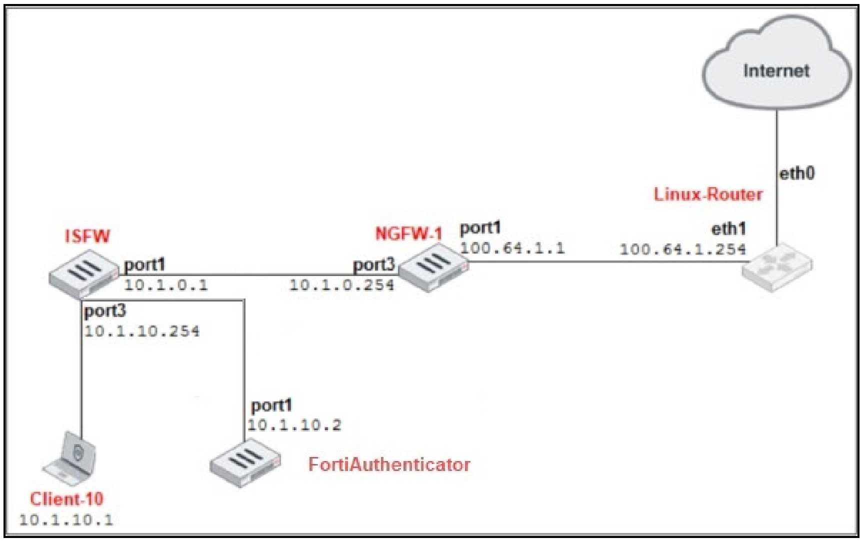
- After you finish troubleshooting, disable the real-time debug, using the following commands:

```
diagnose debug application urlfilter 0
diagnose debug disable
```

Exercise 2: Troubleshooting Antivirus

In this exercise, you will diagnose and troubleshoot the accurate antivirus detection of an infected file.

Network Topology

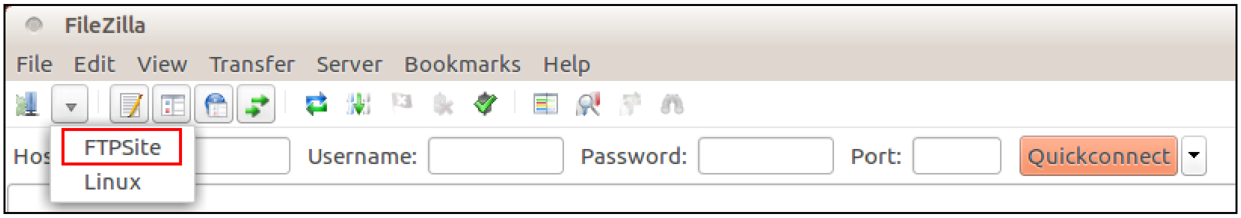


Problem Description

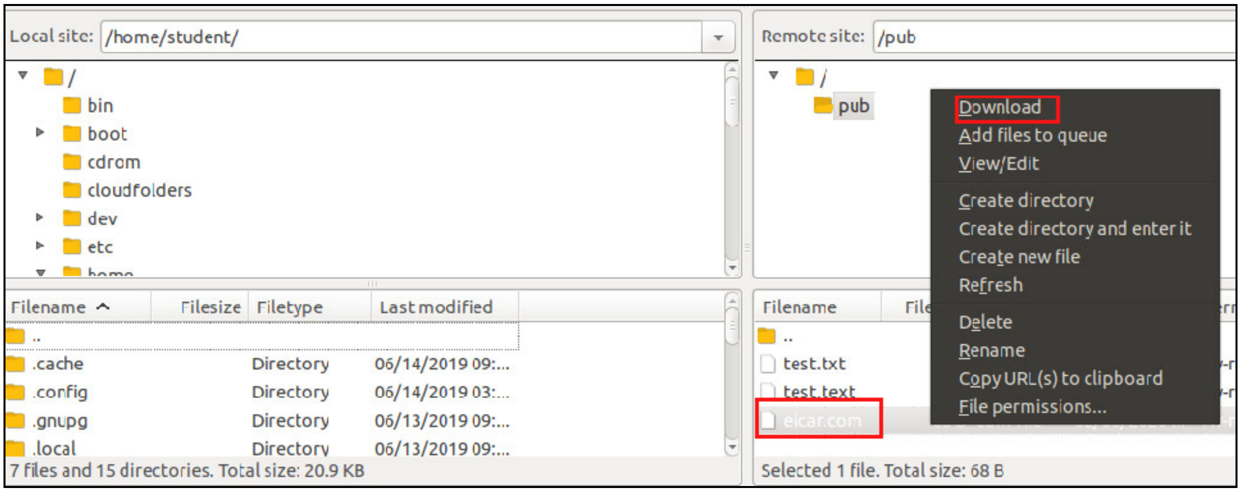
Even though you enabled antivirus on ISFW, a user connecting from Client-10 complains that it's still possible to download the virus sample `eicar.com` located at the FTP server `100.64.3.254`.

To test antivirus

1. On the Client-10 VM, open FileZilla.
2. In the **Site Manager** drop-down list, select **FTPSite**.



3. Select **Desktop** as the local site folder, and **pub** as the remote site folder.
4. Right-click the `eicar.com` file, and then select **Download**.



Filename	Filesize	Filetype	Last modified
..			
.cache		Directory	06/14/2019 09:...
.config		Directory	06/14/2019 03:...
.gnupg		Directory	06/13/2019 09:...
.local		Directory	06/13/2019 09:...

7 files and 15 directories. Total size: 20.9 KB

Filename
..
test.txt
test.text
eicar.com

Selected 1 file. Total size: 68 B

Why isn't ISFW detecting the EICAR virus?

Objective

Use the debug commands available on ISFW to find out why FortiGate isn’t blocking the FTP file transfer.

Tips for Troubleshooting

- Sniff the FTP traffic, using the following command:

```
diagnose sniffer packet any "host 100.64.3.254" 4
```

- Analyze the output of the debug flow, using the following commands:

```
diagnose debug flow filter addr 100.64.3.254
diagnose debug flow trace start
diagnose debug enable
```

Can you confirm from the output that FortiGate is inspecting the traffic? If it isn’t, can you explain why?

Delete the `eicar.com` file from the desktop.

Lab 8: High Availability

In this lab, you will troubleshoot an HA cluster between two FortiGate devices.

Objectives

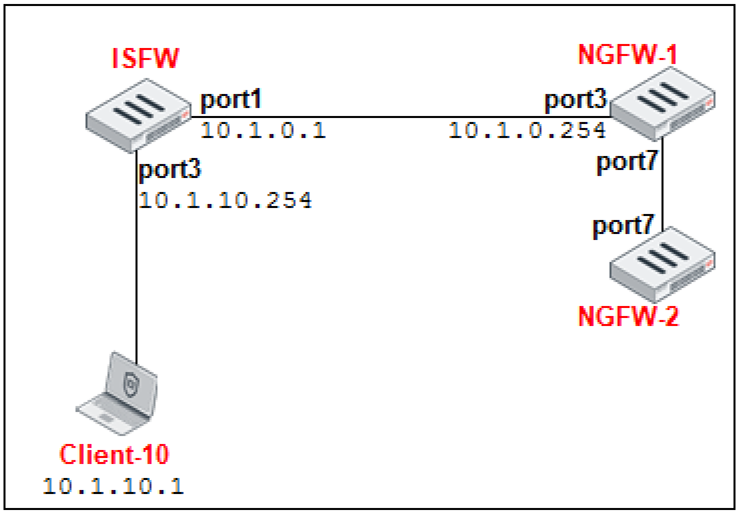
- Troubleshoot the formation of an HA cluster
- Check the status of the HA configuration
- Monitor the HA cluster

Time to Complete

Estimated: 45 minutes

Which Network Segment Will You Work On?

During this lab, you will review the configuration of ISFW and troubleshoot the HA issue on NGFW-1 and NGFW-2.

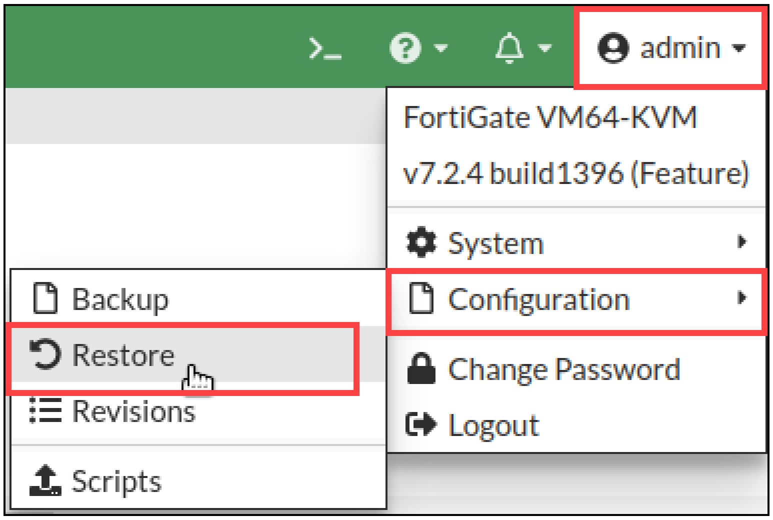


Prerequisites

Before you begin this lab, you must restore the initial configuration files to the FortiGate devices. The configuration files are located on the desktop of the Client-10 VM.

To restore the NGFW-1 configuration file

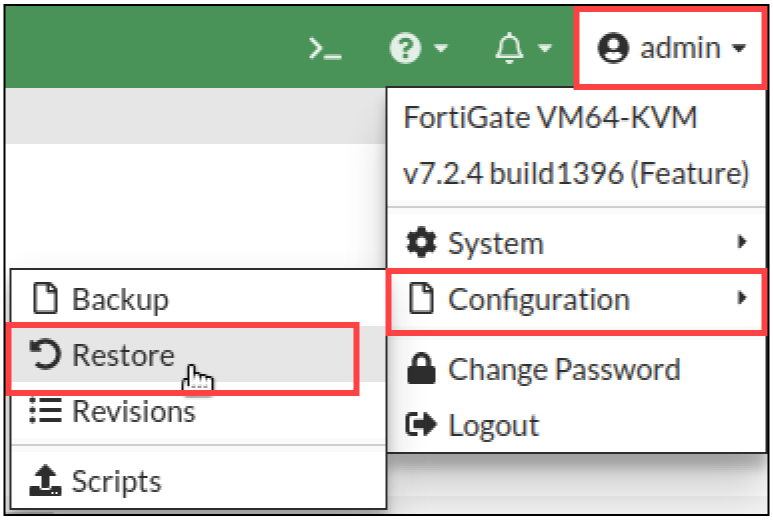
1. On the Client-10 VM, open a browser, and then log in to the NGFW-1 GUI with the username `admin` and password `password`.
2. In the upper-right corner, click **admin**, and then click **Configuration** > **Restore**.



3. Click **Local PC**, and then click **Upload**.
4. Click **Desktop** > **Resources** > **NST** > **HA**, select `NGFW-1_HA_Initial.conf`, and then click **Open**.
5. Click **OK**.
6. Click **OK** to reboot.

To restore the NGFW-2 configuration file

1. On the Client-10 VM, open a browser, and then log in to the NGFW-2 GUI with the username `admin` and password `password`.
2. In the upper-right corner, click **admin**, and then click **Configuration** > **Restore**.

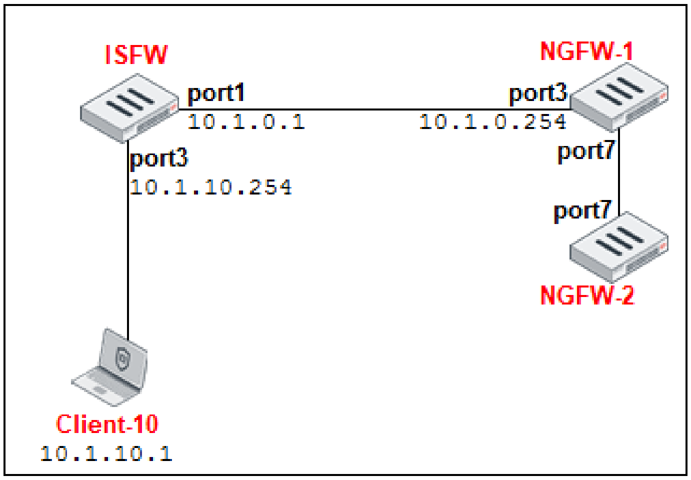


3. Click **Local PC**, and then click **Upload**.
4. Click **Desktop** > **Resources** > **NST** > **HA**, select `NGFW-2_HA_Initial.conf`, and then click **Open**.
5. Click **OK**.
6. Click **OK** to reboot.

Exercise 1: Troubleshooting High Availability

In this exercise, you will diagnose and troubleshoot two FortiGate devices that are not forming an HA cluster.

Network Topology



Problem Description

NGFW-1 and NGFW-2 are not forming an HA cluster.

Objective

Use HA diagnostic commands to troubleshoot and fix the HA problems. You will achieve the objective when NGFW-2 joins the HA cluster.

Tips for Troubleshooting

- Don’t change the HA priorities on any of the FortiGate devices. Configuring incorrect priorities might delete the existing configuration on NGFW-1.
- Since the HA cluster is broken, you might not be able to connect HTTPS or connect over SSH to the FortiGate devices. Use the console port instead, and then enter the following HA debug commands:

```
diagnose sys ha status
get sys ha status
diagnose sys ha checksum cluster
```

- Run the HA real-time debug and sniffer on both FortiGate devices.

```
diagnose sniffer packet any 'ether proto 0x8890' 4
diagnose debug application hatalk -1
diagnose debug application hasync -1
diagnose debug enable
```

- What configuration changes can you make on NGFW-1 to fix the problems?
- After you finish troubleshooting, remember to disable the real-time debug.

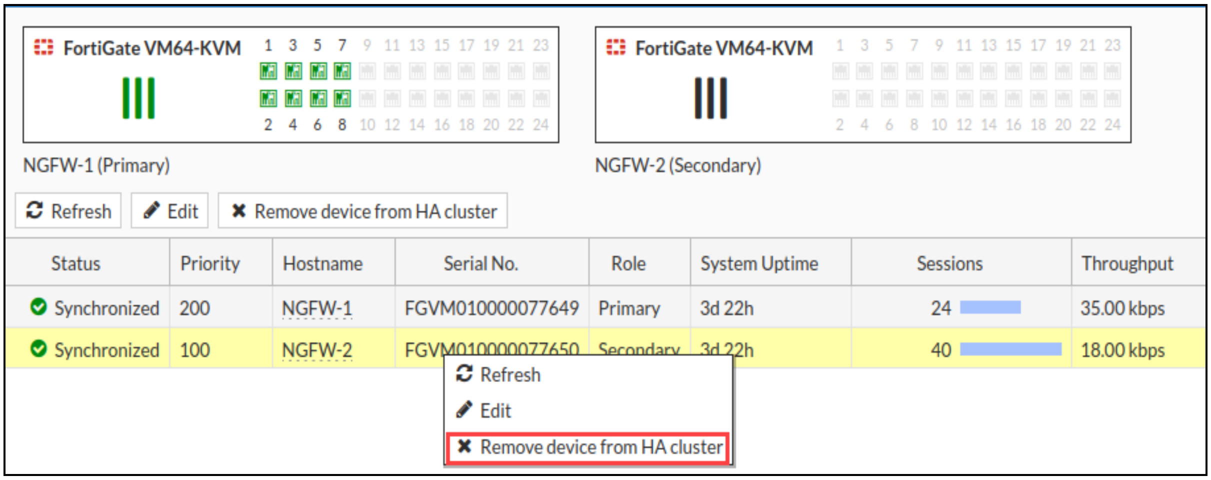
```
diagnose debug reset
```

Disconnect NGFW-2 From the Cluster

You will disconnect NGFW-2 from the cluster. The HA cluster will prompt you to configure an IP address on port3 on NGFW-2 so that you can access it after the disconnection.

To disconnect NGFW-2 from the cluster

1. On the Client-10 VM, open a browser, and then access the NGFW HA cluster GUI at 10.1.0.254.
2. Log in with the username `admin` and password `password`.
3. Click `System` > `HA`.
4. Right-click `NGFW-2`, and then click `Remove device from HA cluster`.



Status	Priority	Hostname	Serial No.	Role	System Uptime	Sessions	Throughput
Synchronized	200	NGFW-1	FGVM010000077649	Primary	3d 22h	24	35.00 kbps
Synchronized	100	NGFW-2	FGVM010000077650	Secondary	3d 22h	40	18.00 kbps

5. When prompted, configure the following settings:

Field	Value
Interface	port3
IP/Netmask	10.1.0.253/24

6. Click **OK**.
   This removes the FortiGate from the HA cluster.

Lab 9: IPsec

In this lab, you will troubleshoot an IPsec problem between Spoke-1 and Spoke-2.

Objectives

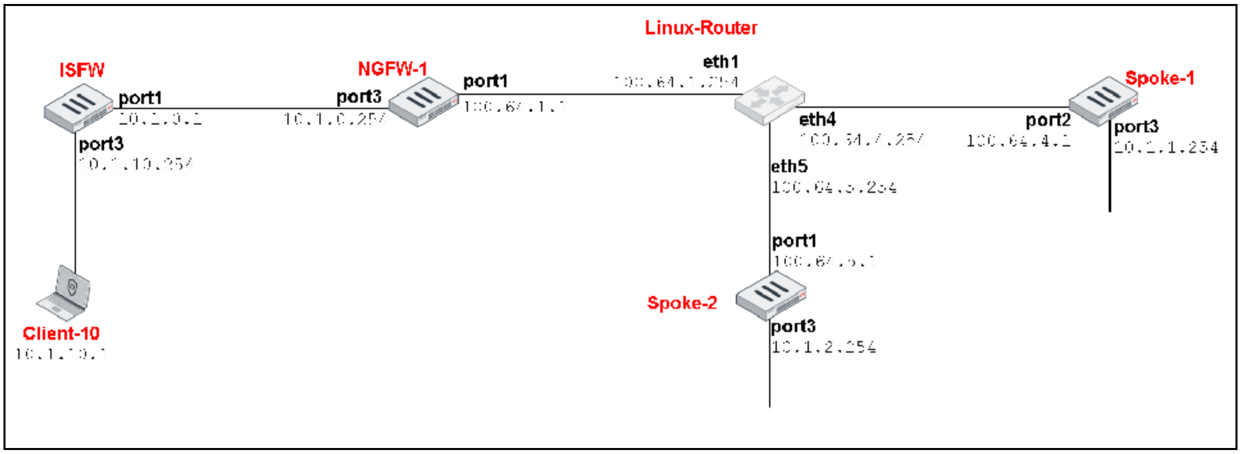
- Troubleshoot IPsec problems
- Run CLI commands to gather the IPsec status and statistics

Time to Complete

Estimated: 30 minutes

Which Network Segment Will You Work On?

You will work on NGFW-1, Spoke-1, and Spoke-2.



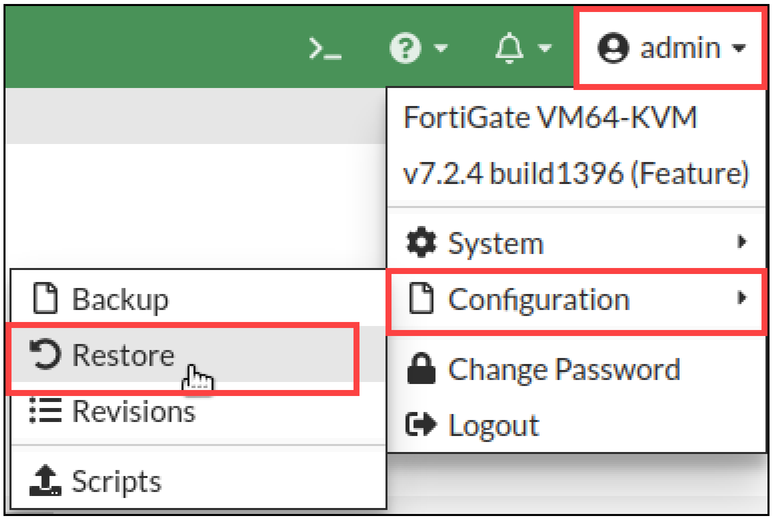
Prerequisites

Before you begin this lab, you must restore the initial configuration files to the FortiGate devices. The configuration files are located on the desktop of the Client-10 VM.

Additionally, you must have completed the previous lab. Notify your instructor if this is not the case.

To restore the Spoke-1 configuration file

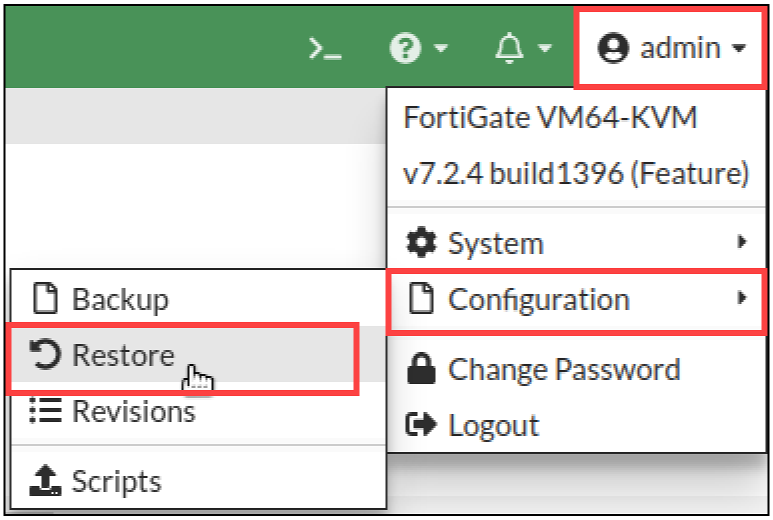
1. On the Client-10 VM, open a browser, and then log in to the Spoke-1 GUI with the username `admin` and password `password`.
2. In the upper-right corner of the screen, click **admin**, and then click **Configuration** > **Restore**.



3. Select **Local PC**, and then click **Upload**.
4. Click **Desktop** > **Resources** > **NST** > **IPsec**, select `Spoke-1_IPSec.conf`, and then click **Open**.
5. Click **OK**.
6. Click **OK** to reboot.

To restore the Spoke-2 configuration file

1. On the Client-10 VM, open a browser, and then log in to the Spoke-2 GUI with the username `admin` and password `password`.
2. In the upper-right corner of the screen, click **admin**, and then click **Configuration** > **Restore**.

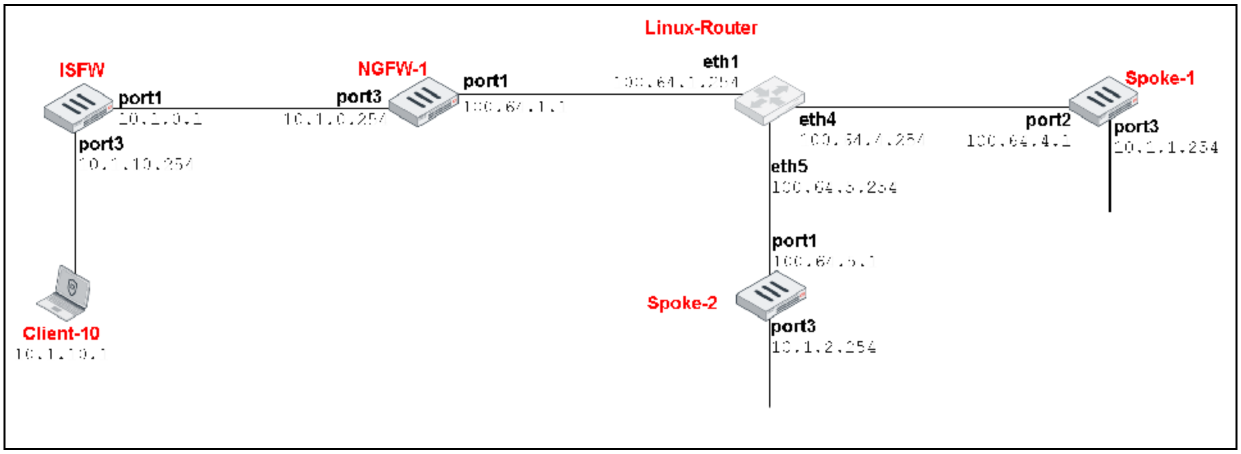


3. Select **Local PC**, and then click **Upload**.
4. Click **Desktop** > **Resources** > **NST** > **IPsec**, select `Spoke-2_IPSec.conf`, and then click **Open**.
5. Click **OK**.
6. Click **OK** to reboot.

Exercise 1: Troubleshooting IPsec

In this exercise, you will perform troubleshooting steps to bring up an IPsec VPN tunnel between two FortiGate devices.

Network Topology



Problem Description

An administrator has configured an IPsec connection between port2 (`100.64.4.1`) on Spoke-1 and port1 (`100.64.5.1`) on Spoke-2. However, the tunnel fails to establish.

Objective

Use IPsec diagnostic commands on the spokes to find out why the tunnel isn't establishing. Make all changes in the VPN configurations to fix the problems and connect the tunnel.

After the tunnel is established, you will notice that traffic isn't crossing the tunnel. Use the debug flow and sniffer tools to find out why. You don't need to fix this traffic flow problem, but you need to explain why it's happening.

Tips for Troubleshooting

- Use the IKE real-time debug to view the negotiations for phases 1 and 2, using the following commands:

```
diagnose debug application ike -1
diagnose debug enable
```

Do you see any error messages that could point out where the problems are?

Could you fix the problems by changing the VPN configurations?

Use the following command to monitor the VPN status:

```
diagnose vpn tunnel list
```

- After the tunnel connects, ping from Spoke-2 to Spoke-1, using the following commands:

  ```
  execute ping-options source 10.1.2.254
  execute ping 10.1.1.254
  ```

  Also, test the ping from Spoke-1 to Spoke-2, using the following commands:

  ```
  execute ping-options source 10.1.1.254
  execute ping 10.1.2.254
  ```

Why isn't it working? Use the sniffer and debug flow tools to explain why. Sniff not only the ICMP traffic, but also the ESP traffic between the FortiGate devices.

Lab 10: IPsec—IKEv2

In this lab, you will troubleshoot an IPsec problem between Spoke-1 and Spoke-2 using IKEv2.

Objectives

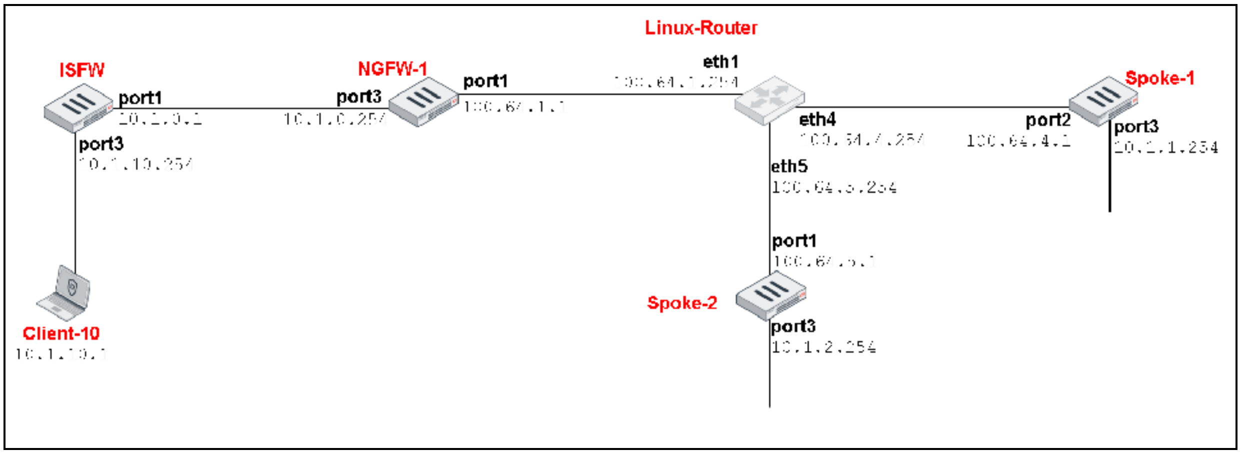
- Troubleshoot IPsec problems
- Run CLI commands to gather the IPsec status

Time to Complete

Estimated: 30 minutes

Which Network Segment Will You Work On?

You will work on NGFW-1, Spoke-1, and Spoke-2.

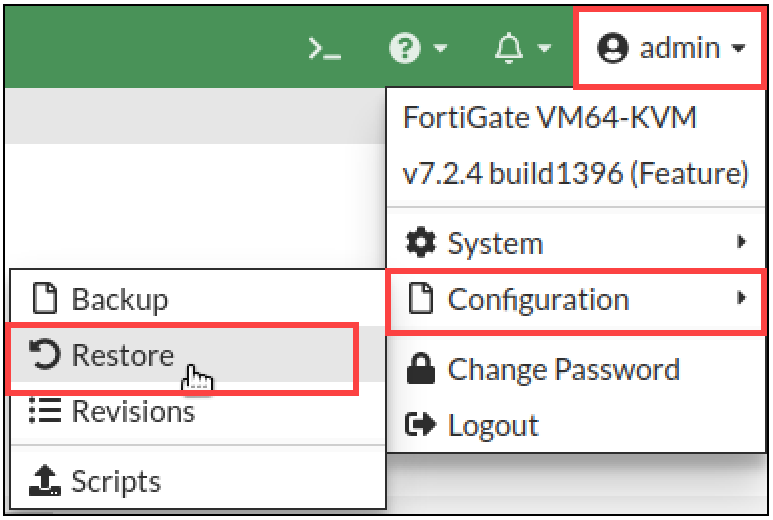


Prerequisites

Before you begin this lab, you must restore the initial IPsec IKEv2 configuration files to the FortiGate devices. The configuration files are located on the desktop of the Client-10 VM.

To restore the Spoke-1 configuration file

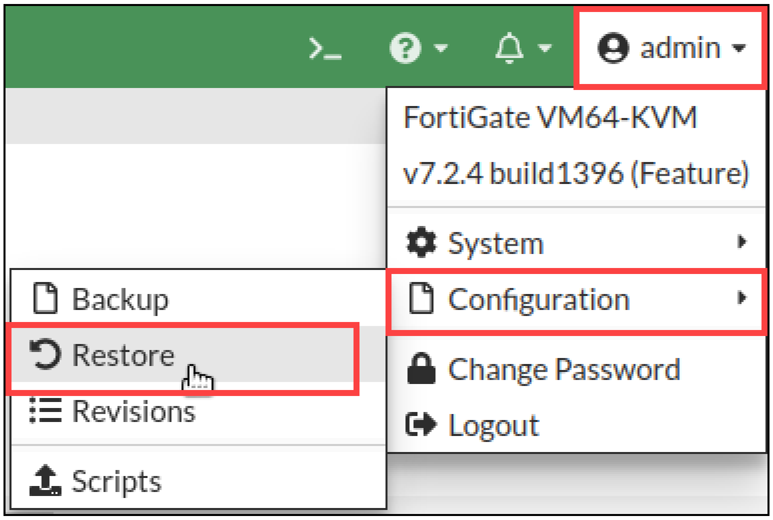
1. On the Client-10 VM, open a browser, and then log in to the Spoke-1 GUI with the username `admin` and password `password`.
2. In the upper-right corner, click **admin**, and then click **Configuration** > **Restore**.



3. Select **Local PC**, and then click **Upload**.
4. Click **Desktop** > **Resources** > **NST** > **IPsec_IKEv2**, select `Spoke-1_IPSec_IKEv2.conf`, and then click **Open**.
5. Click **OK**.
6. Click **OK** to reboot.

To restore the Spoke-2 configuration file

1. Open a browser, and then log in to the Spoke-2 GUI with the username `admin` and password `password`.
2. Click **Login Read-Write**.
3. In the upper-right corner, click **admin**, and then click **Configuration** > **Restore**.

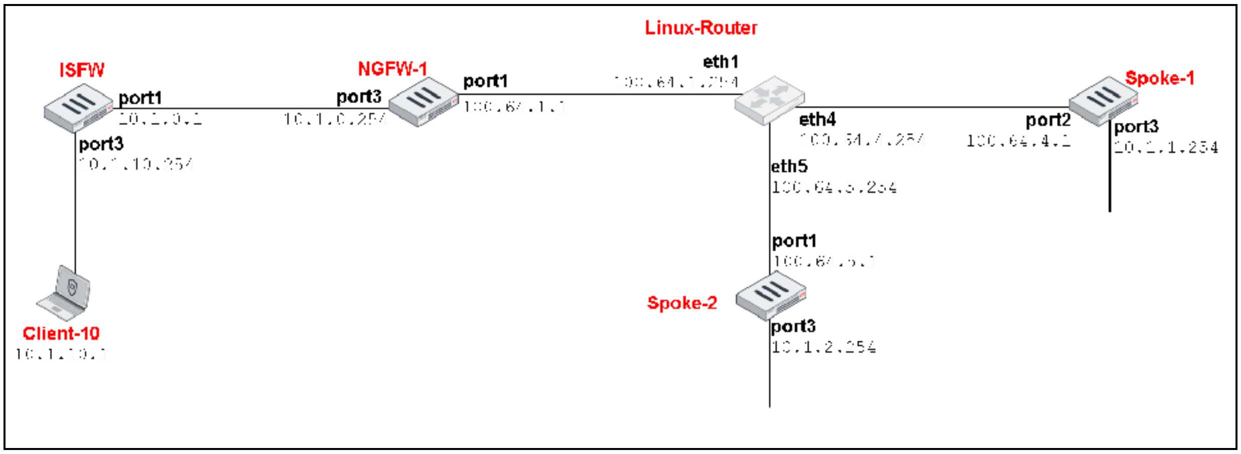


4. Select **Local PC**, and then click **Upload**.
5. Click **Desktop** > **Resources** > **NST** > **IPsec_IKEv2**, select `Spoke-2_IPSec_IKEv2.conf`, and then click **Open**.
6. Click **OK**.
7. Click **OK** to reboot.

Exercise 1: Troubleshooting IPsec Using IKEv2

In this exercise, you will perform troubleshooting steps to bring up an IPsec VPN tunnel between two FortiGate devices.

Network Topology



Problem Description

Configure a successful gateway-to-gateway IPsec VPN connection using IKEv2 between port2 (`100.64.4.1`) on Spoke-1 and port1 (`100.64.5.1`) on Spoke-2.

Objective

Use IPsec diagnostic commands on the spokes to find out why the tunnel isn't establishing. Make all changes in the VPN configurations to fix the problems and connect the tunnel.

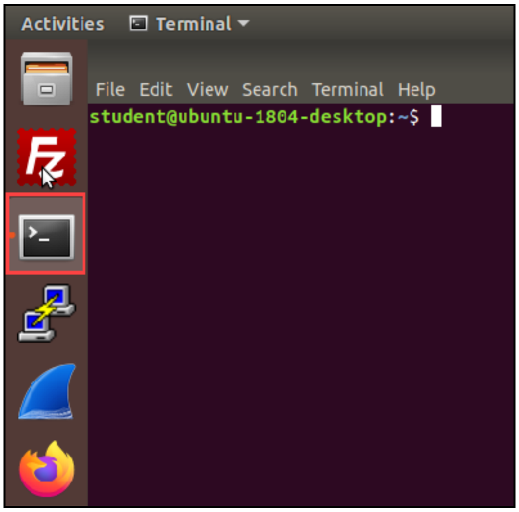
After the tunnel is established and traffic flows successfully through the tunnel, you will notice that after approximately 5 minutes, the tunnel is down again. Use the debug flow and sniffer tools to find out why.

Change the Firewall Rules on Linux Router

You must run a script on the Client-10 VM to change the firewall rules on Linux-Router.

To run a script to change firewall rules on Linux-Router

1. On the Client-10 VM, open a terminal window.



```
student@ubuntu-1804-desktop:~$
```

2. Enter the following commands to run a script:

```
cd Desktop/Resources/NST/IPsec_IKEv2/
sh ikescript.sh
```

3. Once the script is executed, close the terminal window.

Tips for Troubleshooting

- Use the IKE real-time debug to view the negotiations, using the following commands:

  ```
  diagnose debug application ike -1
  diagnose debug enable
  ```

  Do you see any error messages that could point out where the problems are?

  Could you fix the problems by changing the VPN configurations?

- After the tunnel connects, ping from Spoke-2 to Spoke-1, using the following commands:

  ```
  execute ping-options source 10.1.2.254
  execute ping 10.1.1.254
  ```

  Also, test the ping from Spoke-1 to Spoke-2, using the following commands:

  ```
  execute ping-options source 10.1.1.254
  execute ping 10.1.2.254
  ```

- After approximately 5 minutes, the tunnel is down again. What triggered this behavior?

  To trigger a VPN renegotiation, enter the following command on either FortiGate:

  ```
  diagnose vpn ike gateway flush
  ```

Lab 11: Routing

In this lab, you will troubleshoot routing problems. You will test how FortiGate handles a routing failover scenario.

Objectives

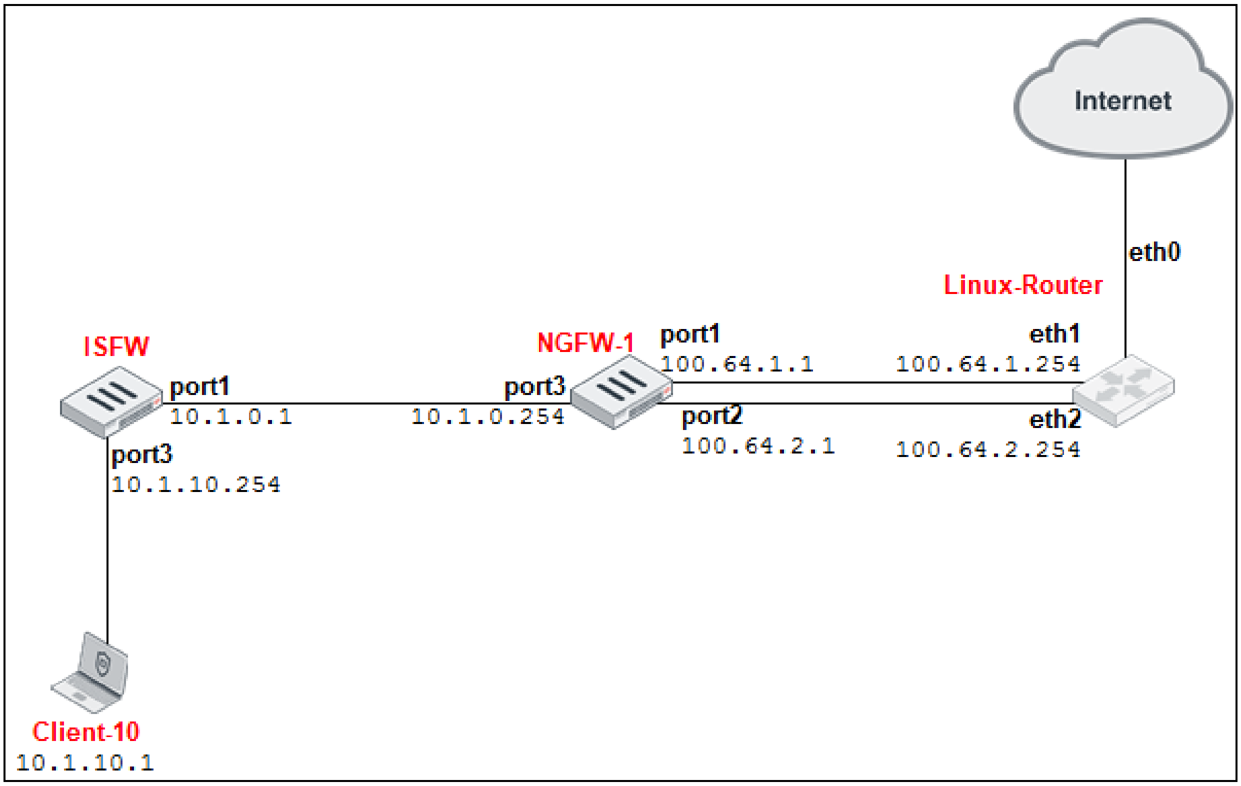
- Analyze the information in the routing table
- Troubleshoot routing problems

Time to Complete

Estimated: 45 minutes

Which Network Segment Will You Work On?

In this lab, you will work on Client-10 and NGFW-1.

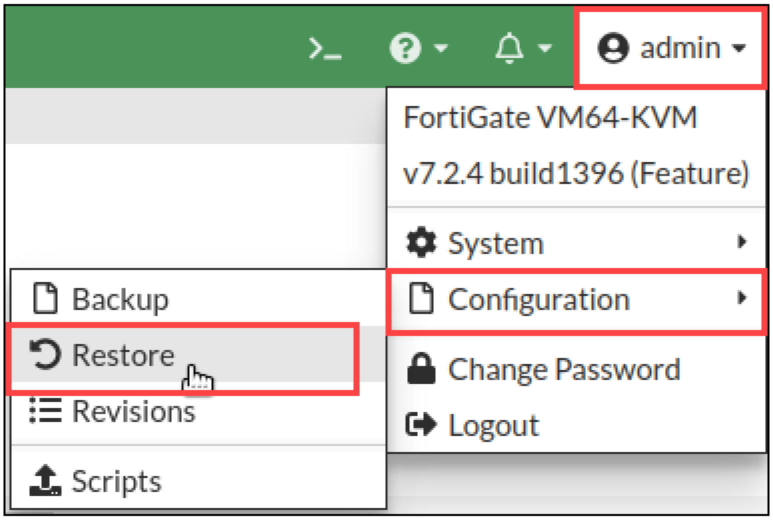


Prerequisites

Before you begin this lab, you must restore the initial configuration files to the FortiGate devices. The configuration files are located on the desktop of the Client-10 VM.

To restore the NGFW-1 configuration file

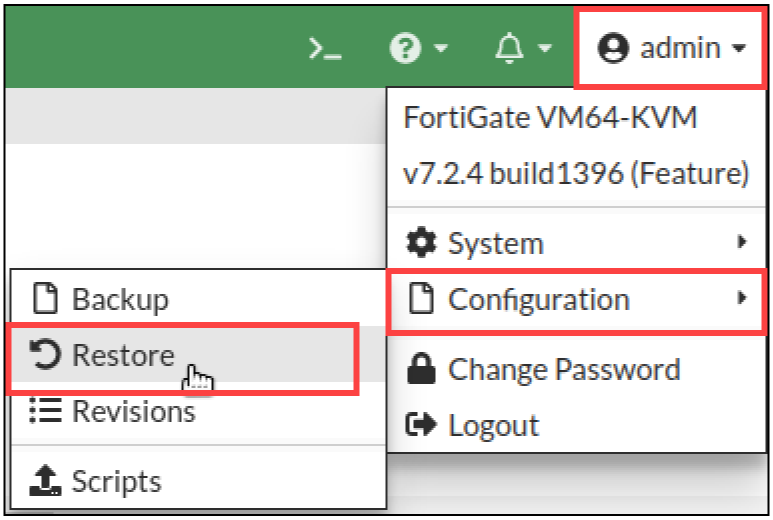
1. On the Client-10 VM, open a browser, and then log in to the NGFW-1 GUI with the username `admin` and password `password`.
2. In the upper-right corner of the screen, click **admin**, and then click **Configuration** > **Restore**.



3. Click **Local PC**, and then click **Upload**.
4. Click **Desktop** > **Resources** > **NST** > **Routing**, select `NGFW-1_Routing_inital.conf`, and then click **Open**.
5. Click **OK**.
6. Click **OK** to reboot.

To restore the ISFW configuration file

1. On the Client-10 VM, open a browser, and then log in to the ISFW GUI with the username `admin` and password `password`.
2. In the upper-right corner of the screen, click **admin**, and then click **Configuration** > **Restore**.



3. Click **Local PC**, and then click **Upload**.
4. Click **Desktop** > **Resources** > **NST** > **Routing**, select `ISFW_Routing_initial.conf`, and then click **Open**.

5. Click **OK**.
6. Click **OK** to reboot.

Exercise 1: Testing the Failover of Existing Sessions

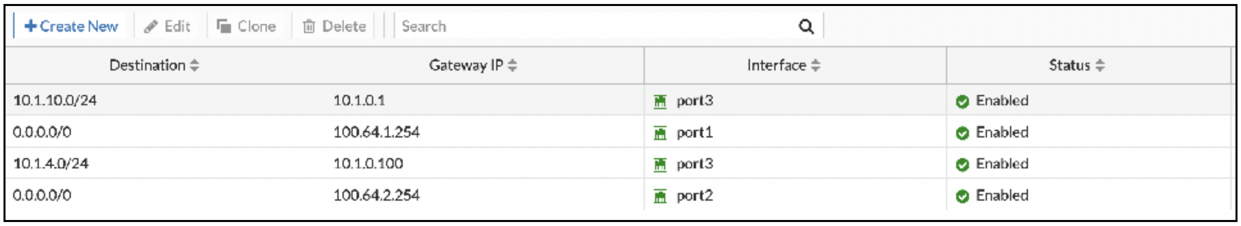
In this exercise, you will test routing failover when FortiGate has two static routes with the same distance, but different priorities. You will also learn how the route failback works when FortiGate is doing source NAT of the traffic.

Check the Routing Table

Before you test the route failover, you will check the current NGFW-1 routing configuration.

To check the routing table

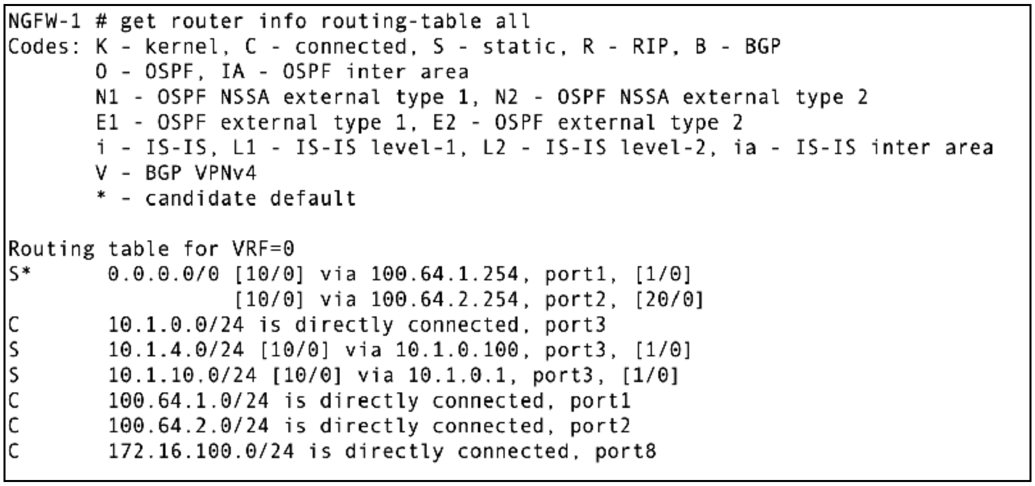
1. Open a browser, and then log in to the NGFW-1 GUI with the username `admin` and password `password`.
2. Click **Network** > **Static Routes**, and then analyze the information displayed.



Destination	Gateway IP	Interface	Status
10.1.10.0/24	10.1.0.1	port3	✓ Enabled
0.0.0.0/0	100.64.1.254	port1	✓ Enabled
10.1.4.0/24	10.1.0.100	port3	✓ Enabled
0.0.0.0/0	100.64.2.254	port2	✓ Enabled

3. Connect over SSH to NGFW-1.
4. Log in with the username `admin` and password `password`.
5. Enter the following command to view the NGFW-1 routing table, and then analyze the routing table output:

```
get router info routing-table all
```



```
NGFW-1 # get router info routing-table all
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       V - BGP VPNv4
       * - candidate default

Routing table for VRF=0
S*      0.0.0.0/0 [10/0] via 100.64.1.254, port1, [1/0]
                  [10/0] via 100.64.2.254, port2, [20/0]
C       10.1.0.0/24 is directly connected, port3
S       10.1.4.0/24 [10/0] via 10.1.0.100, port3, [1/0]
S       10.1.10.0/24 [10/0] via 10.1.0.1, port3, [1/0]
C       100.64.1.0/24 is directly connected, port1
C       100.64.2.0/24 is directly connected, port2
C       172.16.100.0/24 is directly connected, port8
```

There are two default routes—one using port1 and another using port2. The route using port1 is the primary route because it has a lower priority than the route using port2.

Test the Primary Default Route

You will generate internet traffic from Client-10, and then confirm that NGFW-1 is using the port1 default route.

To test the primary default route

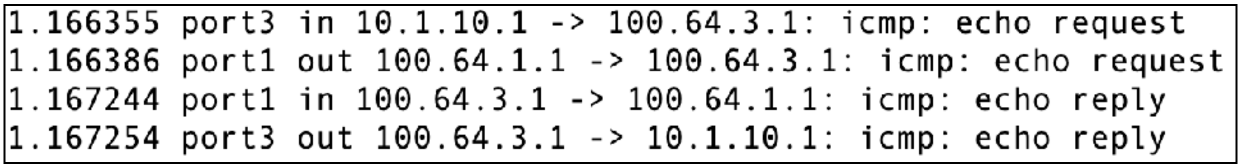
1. On the Client-10 VM, open a terminal session, and then start a continuous ping to Spoke-1.

```
ping 100.64.3.1
```

2. Leave the ping running.
3. Return to the NGFW-1 CLI, and then enter the following command to start a sniffer:

```
diagnose sniffer packet any "icmp and host 100.64.3.1" 4
```

You should see the echo requests coming in to port3 and going out on port1. You should also see the echo replies coming in to port1 and going out on port3.



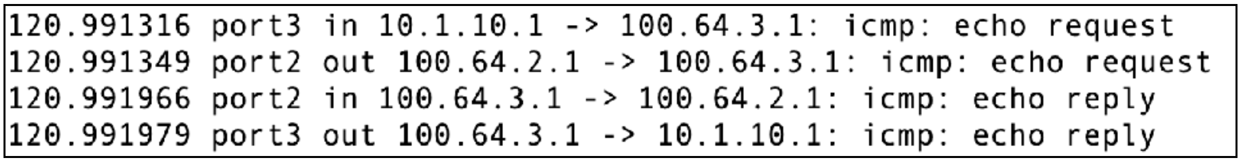
```
1.166355 port3 in 10.1.10.1 -> 100.64.3.1: icmp: echo request
1.166386 port1 out 100.64.1.1 -> 100.64.3.1: icmp: echo request
1.167244 port1 in 100.64.3.1 -> 100.64.1.1: icmp: echo reply
1.167254 port3 out 100.64.3.1 -> 10.1.10.1: icmp: echo reply
```

Test the Failover

You will simulate a failure in the primary route by disabling port1. Then, you will confirm that NGFW-1 is routing traffic through the secondary default route using port2.

To test the failover

1. Verify that both the ping from the Client-10 VM and the sniffer on the NGFW-1 CLI are still running.
2. Return to the NGFW-1 GUI, and then click **Network** > **Interfaces**.
3. Click **port1** to select it, and then click **Edit**.
4. Change the **Status** to **Disabled**.
5. Click **OK**.
6. Return to the NGFW-1 CLI, and then observe the sniffer output.



```
120.991316 port3 in 10.1.10.1 -> 100.64.3.1: icmp: echo request
120.991349 port2 out 100.64.2.1 -> 100.64.3.1: icmp: echo request
120.991966 port2 in 100.64.3.1 -> 100.64.2.1: icmp: echo reply
120.991979 port3 out 100.64.3.1 -> 10.1.10.1: icmp: echo reply
```

The default route using port2 takes over, and the ping traffic is automatically routed through port2. This confirms that the default route failover works.

Test the Failback

You will re-enable port1, and then check how NGFW-1 is routing the continuous ping traffic from Client-10.

To test the failback

1. Return to the NGFW-1 GUI, and then click **Network** > **Interfaces**.
2. Click **port1** to select it, and then click **Edit**.
3. Change the **Status** to **Enabled**.
4. Click **OK**.

   The **port1** physical state changes to up.

5. Return to the NGFW-1 CLI, and then observe the sniffer output.

   You will notice that the ICMP traffic is still using port2 even after you re-enabled port1.

   Why is FortiGate still routing the ping traffic through port2 (and not through port1)?

   What can be done to prevent this problem?

Exercise 2: Troubleshooting Routing

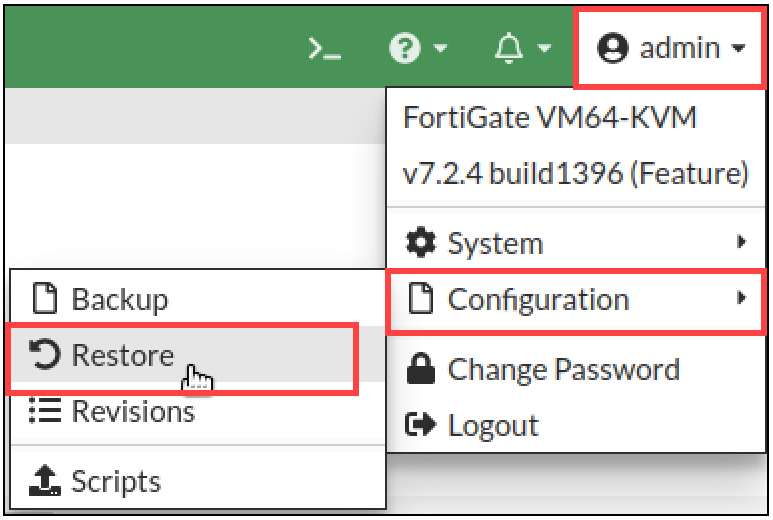
You will use routing debug commands, the built-in sniffer, and debug flow to troubleshoot routing problems.

Prerequisites

Before you begin this lab, you must restore the initial configuration file to FortiGate. The configuration files are located on the desktop of the Client-10 VM.

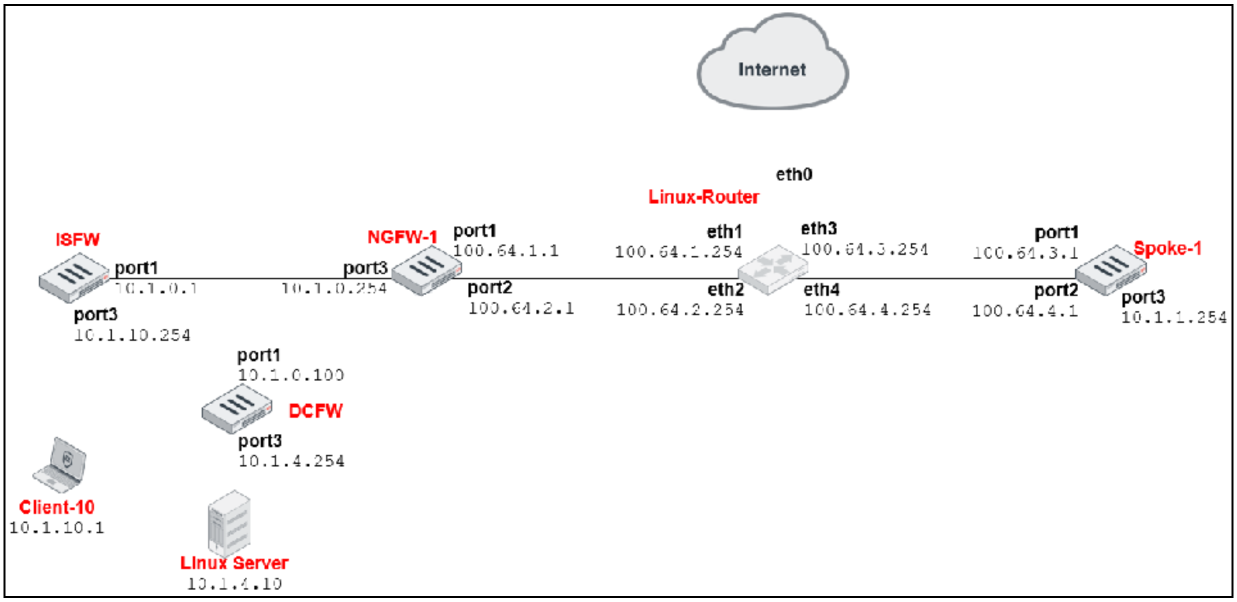
To restore the NGFW-1 configuration file

1. On the Client-10 VM, open a browser, and then log in to the NGFW-1 GUI with the username `admin` and password `password`.
2. In the upper-right corner of the screen, click **admin**, and then click **Configuration** > **Restore**.



3. Click **Local PC**, and then click **Upload**.
4. Click **Desktop** > **Resources** > **NST** > **Routing**, select `NGFW-1_Routing_troubleshooting.conf`, and then click **Open**.
5. Click **OK**.
6. Click **OK** to reboot.

Network Topology



Problem Description

NGFW-1 configuration includes two default routes—one using port1 and another using port2. Both routes should be active in the routing table. However, only one of them is active.

Objectives

The following requirements are necessary to complete this lab:

1. Both default routes (`port1` and `port2`) must be active in the routing table. This means the output of the following command must display both default routes:
```
get router info routing-table all
```
2. The route using port1 must be the primary route.
3. The traffic from Client-10 to the IP address `100.64.3.1` must use the port1 route.

Tips for Troubleshooting

- Try to accomplish objectives 1 and 2 first. Use the following commands to check the routing table:
```
get router info routing-table all
get router info routing-table database
```
- Remember the following requirements for a route to be active in the routing table:

- The outgoing interface is up.
- There is no other matching route with a lower distance.
- If configured, the link health monitor is successful.

- After both default routes are active, and the port1 route is the primary route, generate a continuous ping from Client-10 to `100.64.3.1`, and then sniff the traffic.

```
diagnose sniffer packet any "host 100.64.3.1 and icmp" 4
```

Why is NGFW-1 routing this ICMP traffic through port2 instead of port1?

- Stop the ping, and then clear the existing ICMP session.

```
diagnose sys session filter proto 1
diagnose sys session clear
```

Then, enable the debug flow, and restart the ping to `100.64.3.1`.

```
diagnose debug flow filter clear
diagnose debug flow filter proto 1
diagnose debug flow filter addr 100.64.3.1
diagnose debug enable
diagnose debug flow trace start 10
```

Lab 12: BGP Troubleshooting

In this lab, you will troubleshoot BGP routing issues between NGFW-1 and Linux-Router.

Objectives

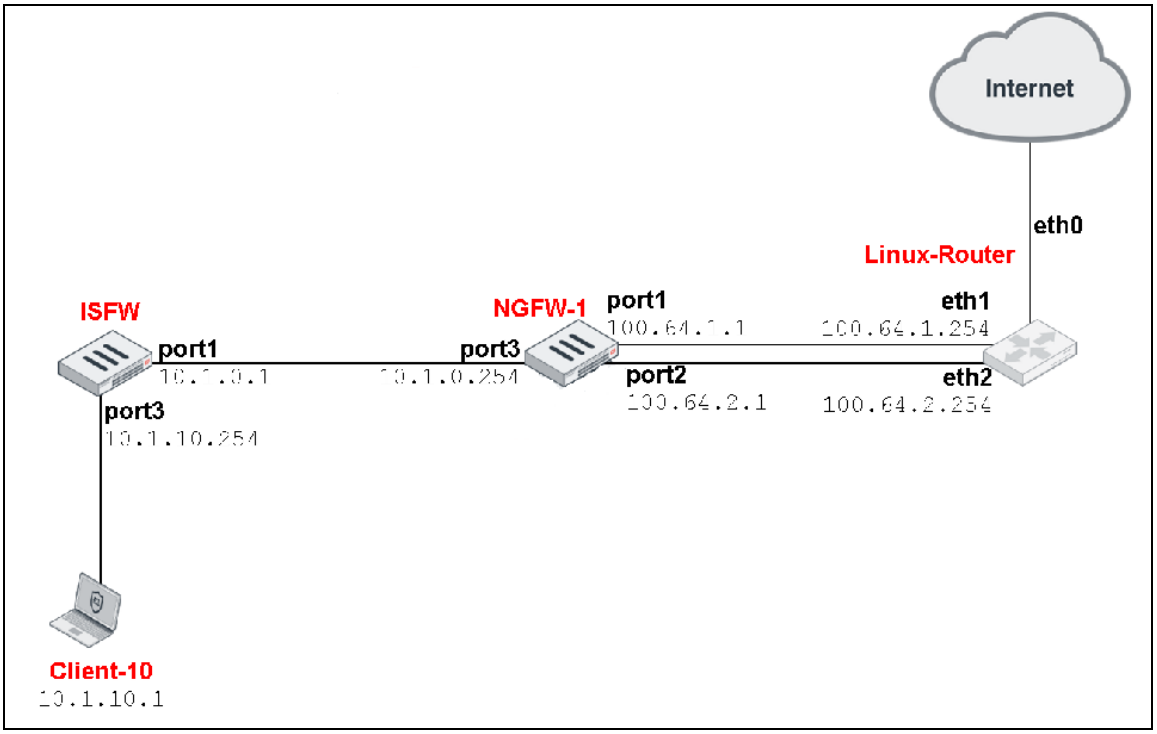
- Diagnose the status of a BGP network
- Troubleshoot BGP problems

Time to Complete

Estimated: 35 minutes

Which Network Segment Will You Work On?

In this lab, you will troubleshoot BGP on NGFW-1. Then, you will make the necessary configuration changes on NGFW-1.

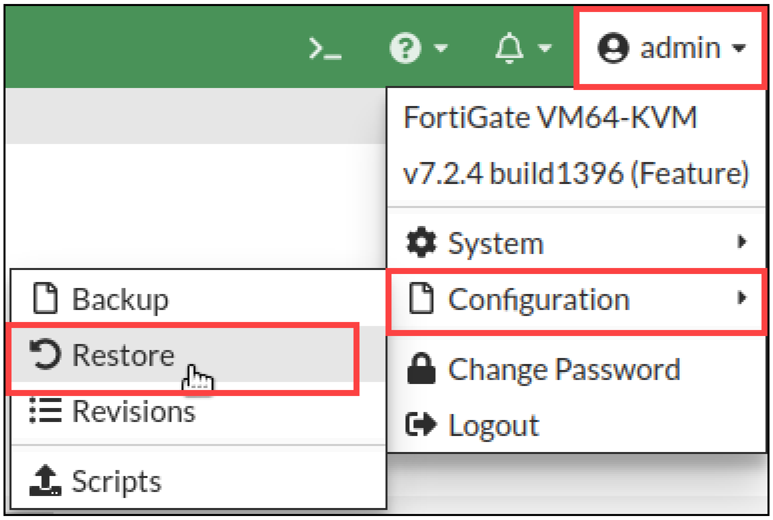


Prerequisites

Before you begin this lab, you must restore the initial configuration file to FortiGate. The configuration files are located on the desktop of the Client-10 VM.

To restore the NGFW-1 configuration file

1. On the Client-10 VM, open a browser, and then log in to the NGFW-1 GUI with the username `admin` and password `password`.
2. In the upper-right corner of the screen, click **admin**, and then click **Configuration** > **Restore**.

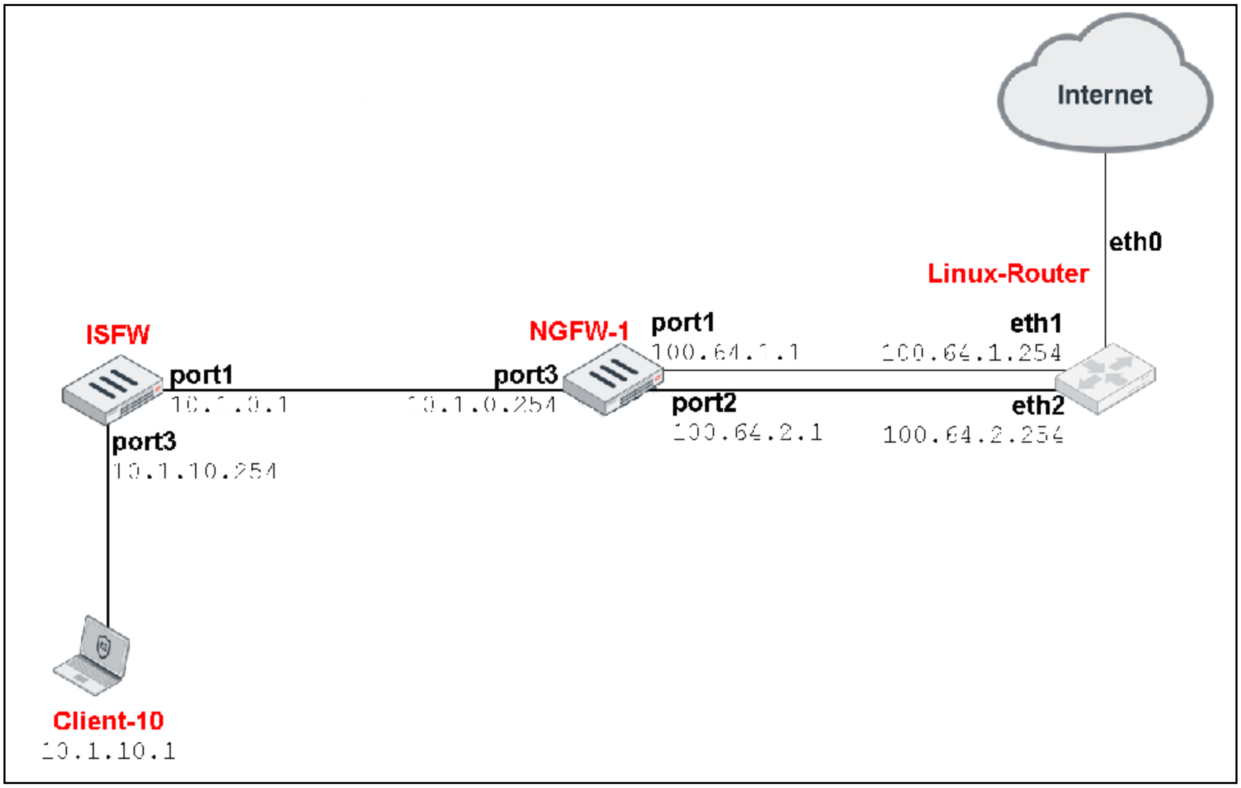


3. Click **Local PC**, and then click **Upload**.
4. Click **Desktop** > **Resources** > **NST** > **BGP**, select `NGFW-1_BGP_initial.conf`, and then click **Open**.
5. Click **OK**.
6. Click **OK** to reboot.

Exercise 1: Troubleshooting the BGP Neighbors

In this exercise, you will use the BGP debug commands to determine why the BGP neighbors are down.

Network Topology



Problem Description

BGP has been configured on NGFW-1 to peer with Linux-Router. NGFW-1 has two connections to the internet through Linux-Router, one using port1 and the other using port2. Linux-Router is the ISP router and is advertising default routes using BGP. However, the BGP neighbors (Linux-Router) aren't coming up. The output of the following command doesn't show any established BGP neighbors:

```
get router info bgp summary
```

Objective

You don't have access to the Linux-Router configuration. Use the BGP debug commands available on NGFW-1 to find out why the BGP neighbors are down. Change the BGP configuration on NGFW-1 to fix the problem.

Don’t make any changes on Linux-Router. To fix the problem, you must make all changes on NGFW-1.

Tips for Troubleshooting

- Check the BGP status on NGFW-1 using the following commands before and after fixing the issue:

```
get router info bgp summary
get router info bgp neighbors
get router info bgp network
```

- Run the BGP real-time debug using the following commands:

```
diagnose ip router bgp all enable
diagnose ip router bgp level info
diagnose debug enable
```

Do you see any errors in the real-time debug that can explain why the BGP neighbors are not peering?

- After you make the necessary BGP configuration changes on NGFW-1, use the following command to restart the BGP connections:

```
execute router clear bgp all
```

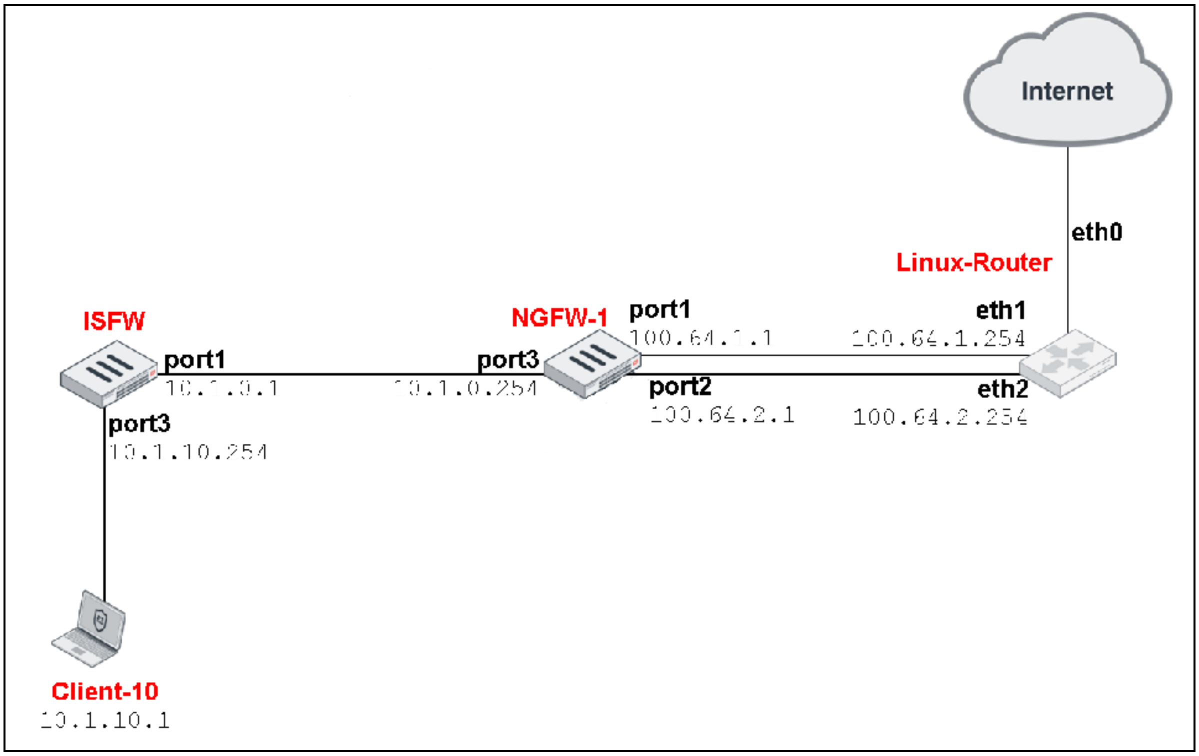
- After you troubleshoot the problem, use the following commands to disable the real-time debug:

```
diagnose debug disable
diagnose ip router bgp all disable
```

Exercise 2: Troubleshooting BGP Routing

In this exercise, you will use the routing and BGP diagnostic commands on NGFW-1 to determine why traffic destined for the IP address `8.8.8.8` is using port2 instead of port1.

Network Topology



Problem Description

After the BGP adjacency is established, the administrator reports a problem with the current configuration. The default BGP route using port1 is the primary link for internet traffic. However, all traffic destined for the IP address `8.8.8.8` is using port2 instead.

Objective

Use the routing and BGP diagnostic commands on NGFW-1 to find out why this is happening.

You don’t have to fix this issue. What are two methods that can be applied to ensure traffic for 8.8.8.8/32 will use port1?

Tips for Troubleshooting

- On NGFW-1, use the built-in sniffer on a ping from Client-10 to `8.8.8.8`.
- Use the following commands to check the routing table:

```
get router info routing-table all
get router info routing-table database
```

Lab 13: OSPF

In this lab, OSPF has already been configured. You will use OSPF troubleshooting commands to monitor OSPF routing operations, and then you will fix any issues that you discover.

Objectives

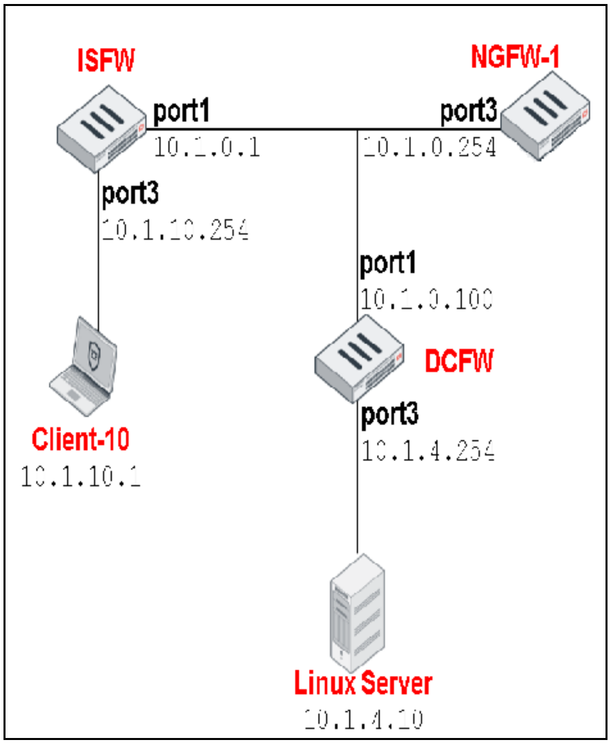
- Diagnose the status of an OSPF network
- Troubleshoot OSPF problems

Time to Complete

Estimated: 30 minutes

Which Network Segment Will You Work On?

You will monitor the status and operations of OSPF on NGFW-1, DCFW, and ISFW. You will also troubleshoot adjacency and routing issues between the Linux server and DCFW.

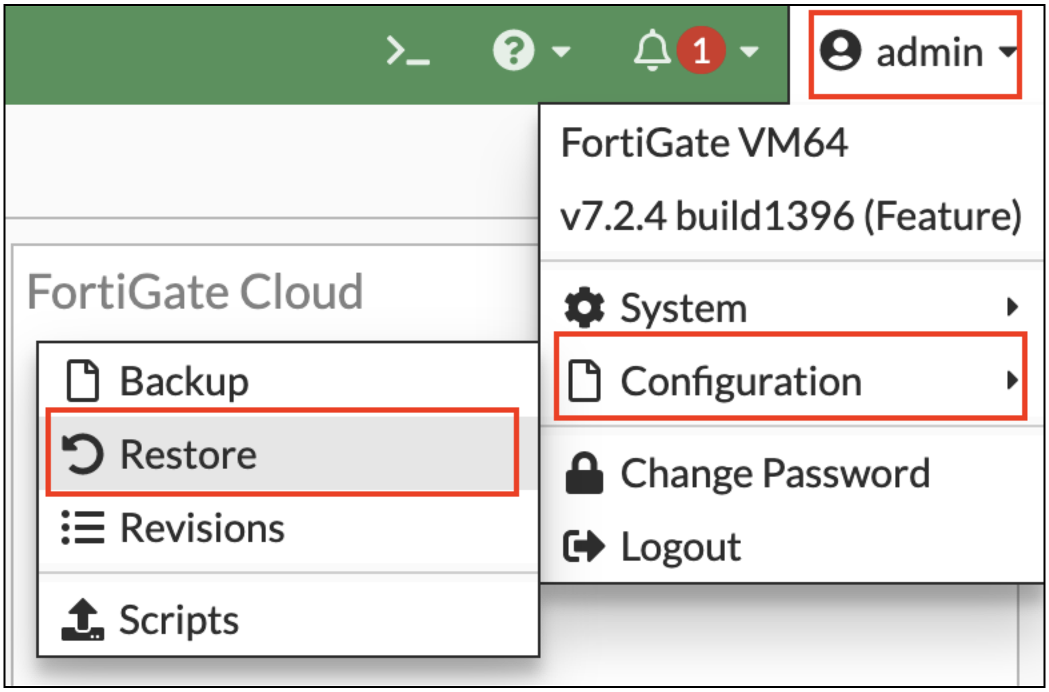


Prerequisites

Before you begin this lab, you must restore the initial configuration files to the FortiGate devices. The configuration files are located on the desktop of the Client-10 VM.

To restore the ISFW configuration file

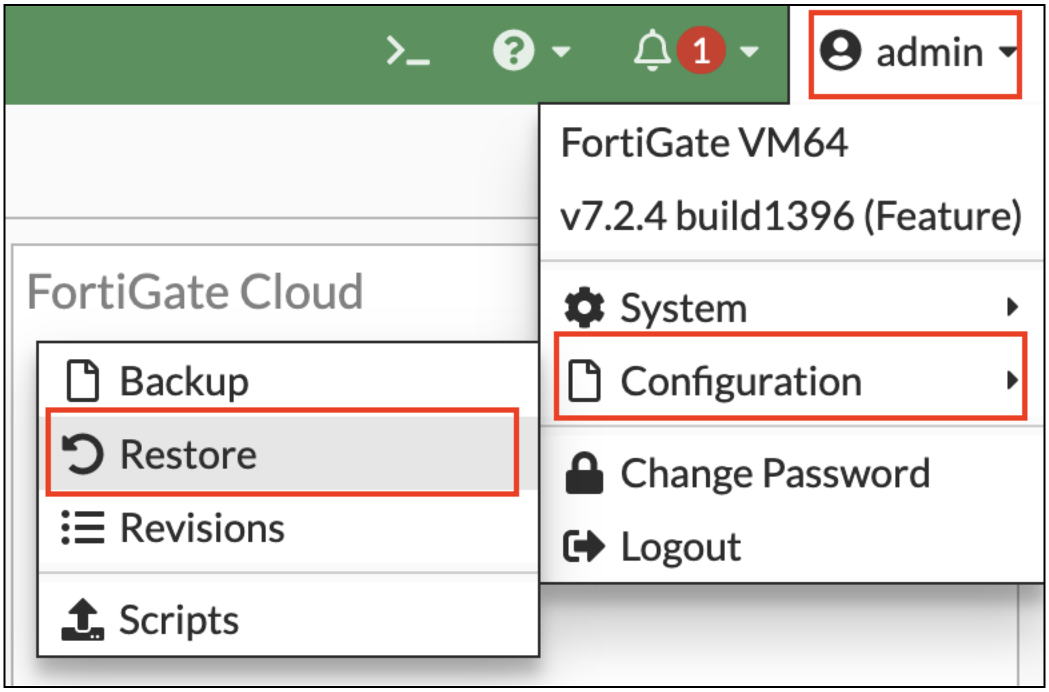
1. On the Client-10 VM, open a browser, and then log in to the ISFW- GUI with the username `admin` and password `password`.
2. In the upper-right corner of the screen, click **admin**, and then click **Configuration** > **Restore**.



3. Click **Local PC**, and then click **Upload**.
4. Click **Desktop** > **Resources** > **NST** > **OSPF**, select `ISFW_OSPF.conf`, and then click **Open**.
5. Click **OK**.
6. Click **OK** to reboot.

To restore the NGFW-1 configuration file

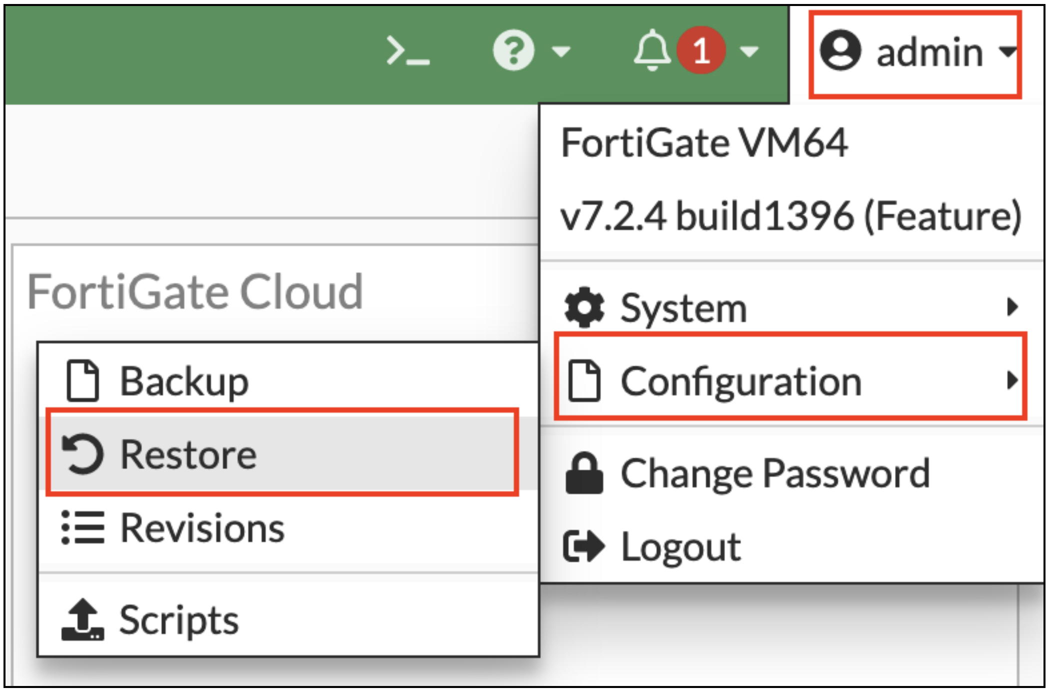
1. On the Client-10 VM, open a browser, and then log in to the NGFW-1 GUI with the username `admin` and password `password`.
2. In the upper-right corner of the screen, click **admin**, and then click **Configuration** > **Restore**.



3. Click **Local PC**, and then click **Upload**.
4. Click **Desktop** > **Resources** > **NST** > **OSPF**, select `NGFW-1_OSPF.conf`, and then click **Open**.
5. Click **OK**.
6. Click **OK** to reboot.

To restore the DCFW configuration file

1. On the Client-10 VM, open a browser, and then log in to the DCFW- GUI with the username `admin` and password `password`.
2. In the upper-right corner of the screen, click **admin**, and then click **Configuration** > **Restore**.



3. Click **Local PC**, and then click **Upload**.
4. Click **Desktop** > **Resources** > **NST** > **OSPF**, select `DCFW_OSPF.conf`, and then click **Open**.
5. Click **OK**.
6. Click **OK** to reboot.

Exercise 1: Monitoring OSPF

Basic OSPF has already been configured on the three FortiGate devices that are part of the hub network: ISFW, DCFW, and NGFW-1. In this exercise, you will use OSPF monitoring commands that you learned in the lesson to ensure OSPF is operating correctly.

Check the Status of OSPF on NGFW-1

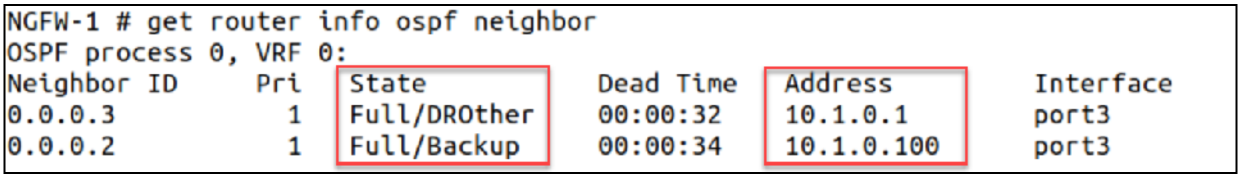
You will run OSPF diagnostic commands on NGFW-1 to verify OSPF operation.

To check the status of OSPF on NGFW-1

1. Connect over SSH to NGFW-1.
2. Log in with the username `admin` and password `password`.
3. Enter the following command:

   ```
   get router info ospf neighbor
   ```

   You should see that NGFW-1 has two neighbors: DCFW and ISFW. The `State` column should display `Full`.



```
NGFW-1 # get router info ospf neighbor
OSPF process 0, VRF 0:
Neighbor ID      Pri   State           Dead Time   Address         Interface
0.0.0.3            1   Full/DROther    00:00:32    10.1.0.1        port3
0.0.0.2            1   Full/Backup     00:00:34    10.1.0.100      port3
```

Stop and think!

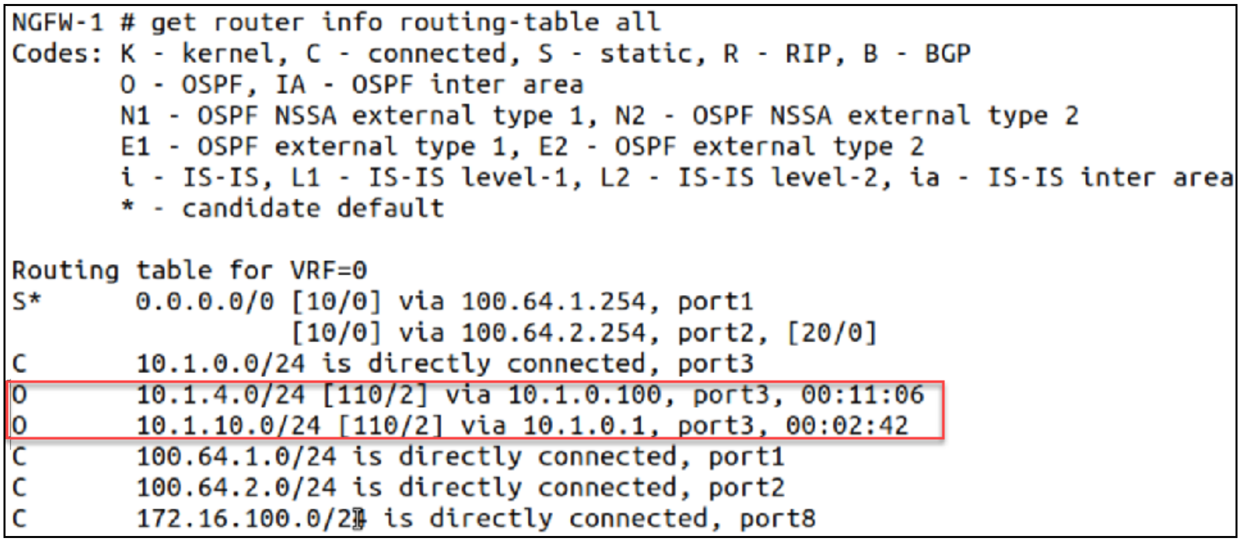
The three FortiGate devices are connected to the same broadcast network (`10.1.0.0/24`). Can you identify from this output what the designated router (DR) is?

The `State` of the designated router is displayed as `Full/DROther`. If neither of the two routers display this state, it means that the designated router is the local FortiGate which, in this case, is NGFW-1. Check the local state using the `get router info ospf interface` command.

4. Enter the following command:

   ```
   get router info routing-table all
   ```

   You should see that NGFW has learned the routes to the `10.1.4.0/24` and `10.1.10.0/24` subnets through OSPF.



```
NGFW-1 # get router info routing-table all
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

Routing table for VRF=0
S*      0.0.0.0/0 [10/0] via 100.64.1.254, port1
                  [10/0] via 100.64.2.254, port2, [20/0]
C       10.1.0.0/24 is directly connected, port3
O       10.1.4.0/24 [110/2] via 10.1.0.100, port3, 00:11:06
O       10.1.10.0/24 [110/2] via 10.1.0.1, port3, 00:02:42
C       100.64.1.0/24 is directly connected, port1
C       100.64.2.0/24 is directly connected, port2
C       172.16.100.0/24 is directly connected, port8
```

Check the Status of OSPF on DCFW and ISFW

You will run OSPF diagnostic commands on DCFW and ISFW to verify OSPF operation.

To check the status of OSPF on DCFW and ISFW

1. Connect over SSH to DCFW.
2. Enter the following commands to verify OSPF operation on DCFW:

   ```
   get router info ospf neighbor
   get router info routing-table all
   ```

3. Connect over SSH to ISFW.
4. Enter the following commands to verify OSPF operation on ISFW:

   ```
   get router info ospf neighbor
   get router info routing-table all
   ```

Check Connectivity

You will confirm that the FortiGate devices are routing traffic correctly by running a ping from Client-10 to the Linux server.

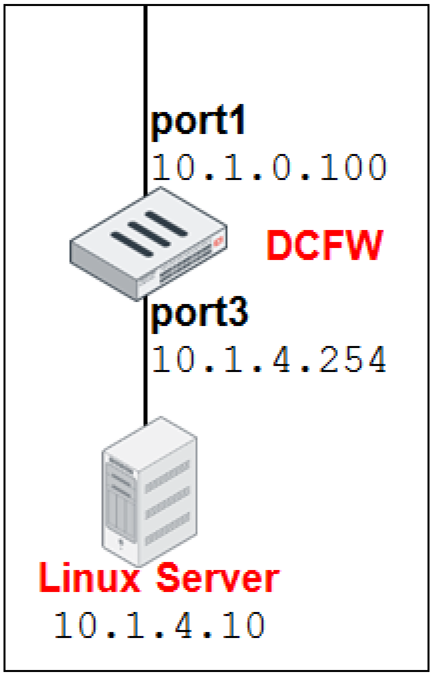
To check connectivity

1. On the Client-10 VM, open a terminal window.
2. Run a ping to the Linux server (`10.1.4.10`).

   The ping should succeed, confirming that the FortiGate devices are correctly routing the traffic between the `10.1.10.0/24` and `10.1.4.0/24` subnets.

Exercise 2: Troubleshooting OSPF

Network Topology



Problem Description

The Linux server is running OSPF. It's configured to form an OSPF adjacency with DCFW. However, it's not coming up. The DCFW doesn't show the Linux server as an OSPF neighbor.

Objective

You don't have access to the Linux server. Use the available OSPF debug commands on DCFW to find out why the OSPF adjacency between the Linux server and DCFW is down. After that, change the configuration on DCFW to fix the problem.

Tips for Troubleshooting

- Check the OSPF neighbor status on DCFW, using the following commands:

```
get router info ospf status
get router info ospf neighbor
```

Initially, you will see that DCFW has only two neighbors: `10.1.0.1` and `10.1.0.254`. Why is the Linux server (`10.1.4.10`) not showing up as a neighbor?

- Run the real-time debug, using the following commands:

```
diagnose ip router ospf all enable
diagnose ip router ospf level info
diagnose debug enable
```

Do you see any errors in the real-time debug that explain why the adjacency establishment is failing? There might be more than one issue.

- After you troubleshoot the problem, use the following commands to disable the real-time debug:

```
diagnose debug disable
diagnose ip router ospf all disable
```