DO NOT REPRINT
© FORTINET

Brave-dumps.com

FORTINET
CERTIFIED
SOLUTION
SPECIALIST

Secure Access
Service Edge

FortiSASE Administrator Study Guide

FortiSASE 24

FORTINET®
Training Institute

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET

Brave-dumps.com

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

8/13/2024

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET

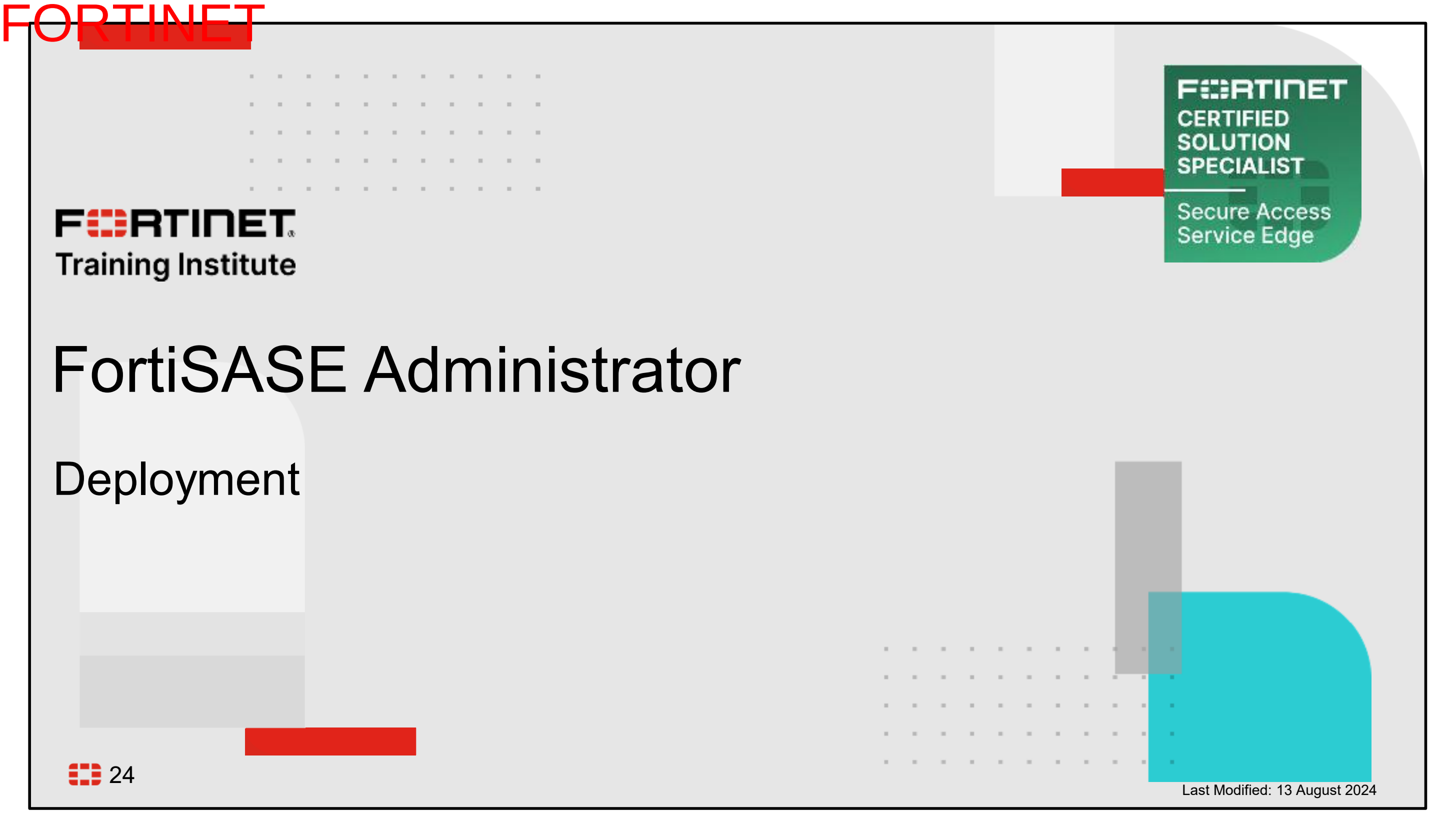
Brave-dumps.com

TABLE OF CONTENTS

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET

Brave-dumps.com



FORTINET
Training Institute

FORTINET
CERTIFIED
SOLUTION
SPECIALIST
Secure Access
Service Edge

FortiSASE Administrator

Deployment

24

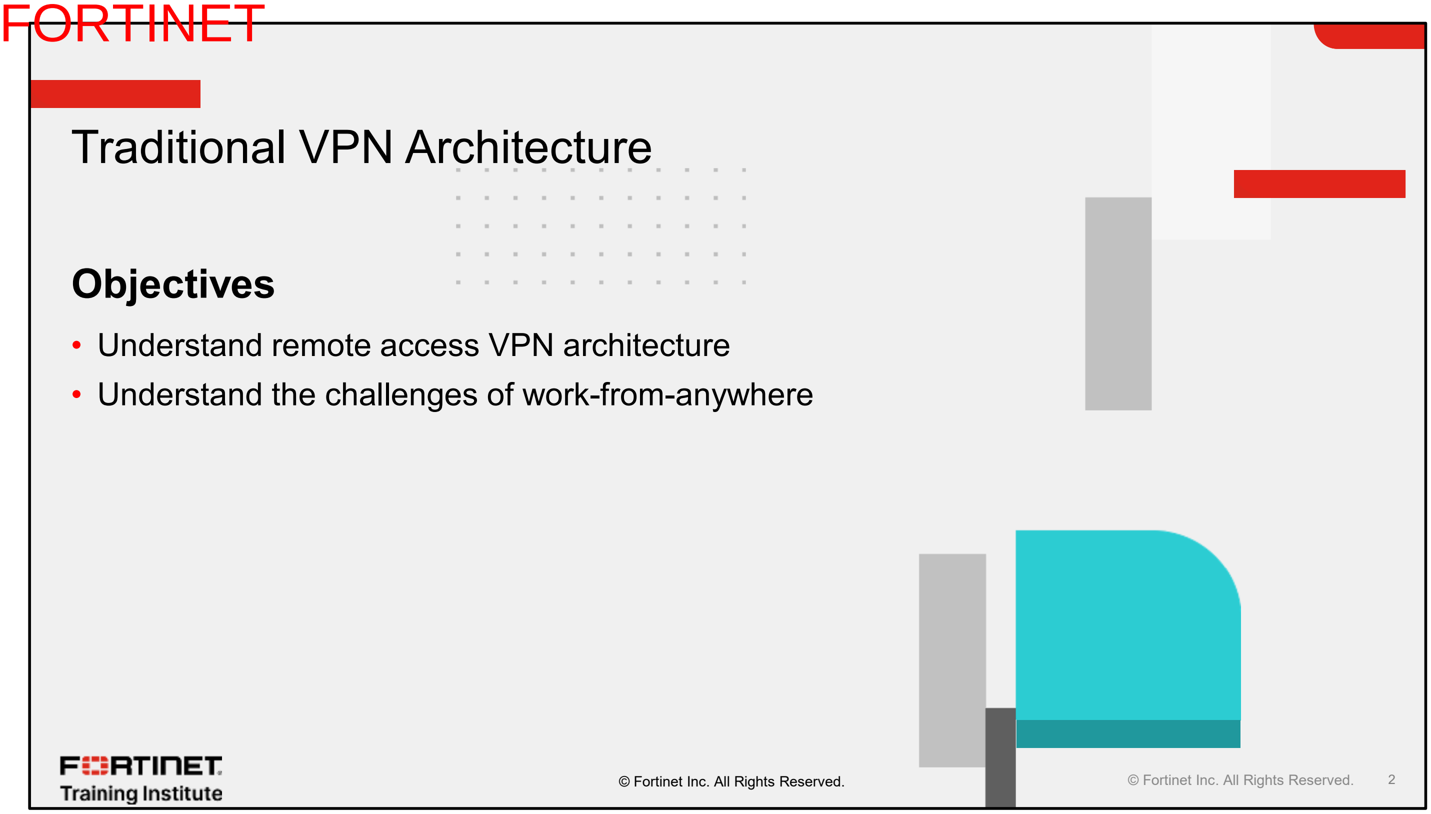
Last Modified: 13 August 2024

In this lesson, you will learn about traditional VPN architecture, secure access service edge (SASE) architecture and components, and the Fortinet SASE solution.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET

Brave-dumps.com



Traditional VPN Architecture

Objectives

- Understand remote access VPN architecture
- Understand the challenges of work-from-anywhere

FERTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved.

2

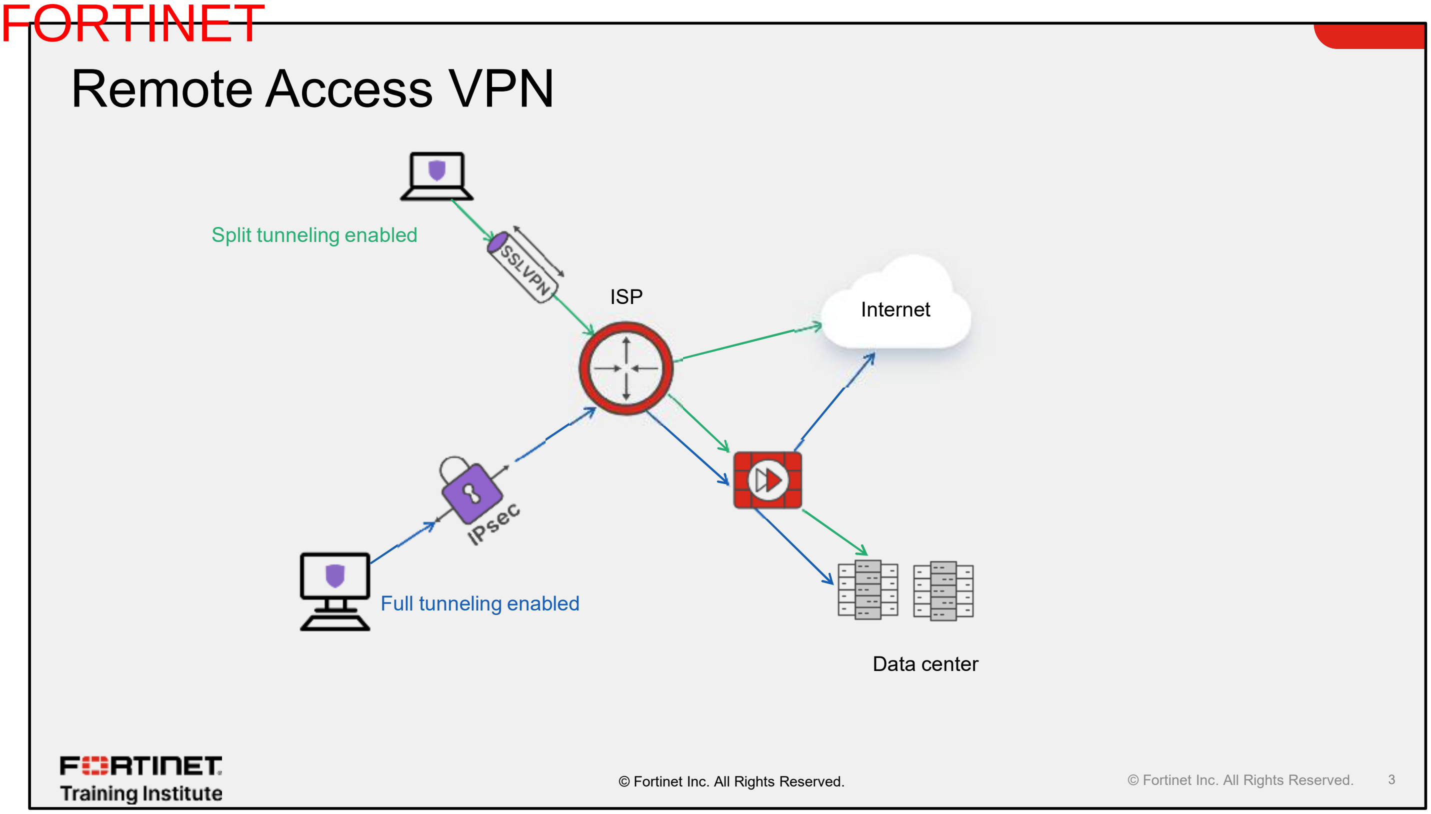
After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating a competent understanding of the standard VPN architecture, and the challenges of work-from-anywhere, you will be able to describe the issues associated with it.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET

Brave-dumps.com



Remote Access VPN

© Fortinet Inc. All Rights Reserved.

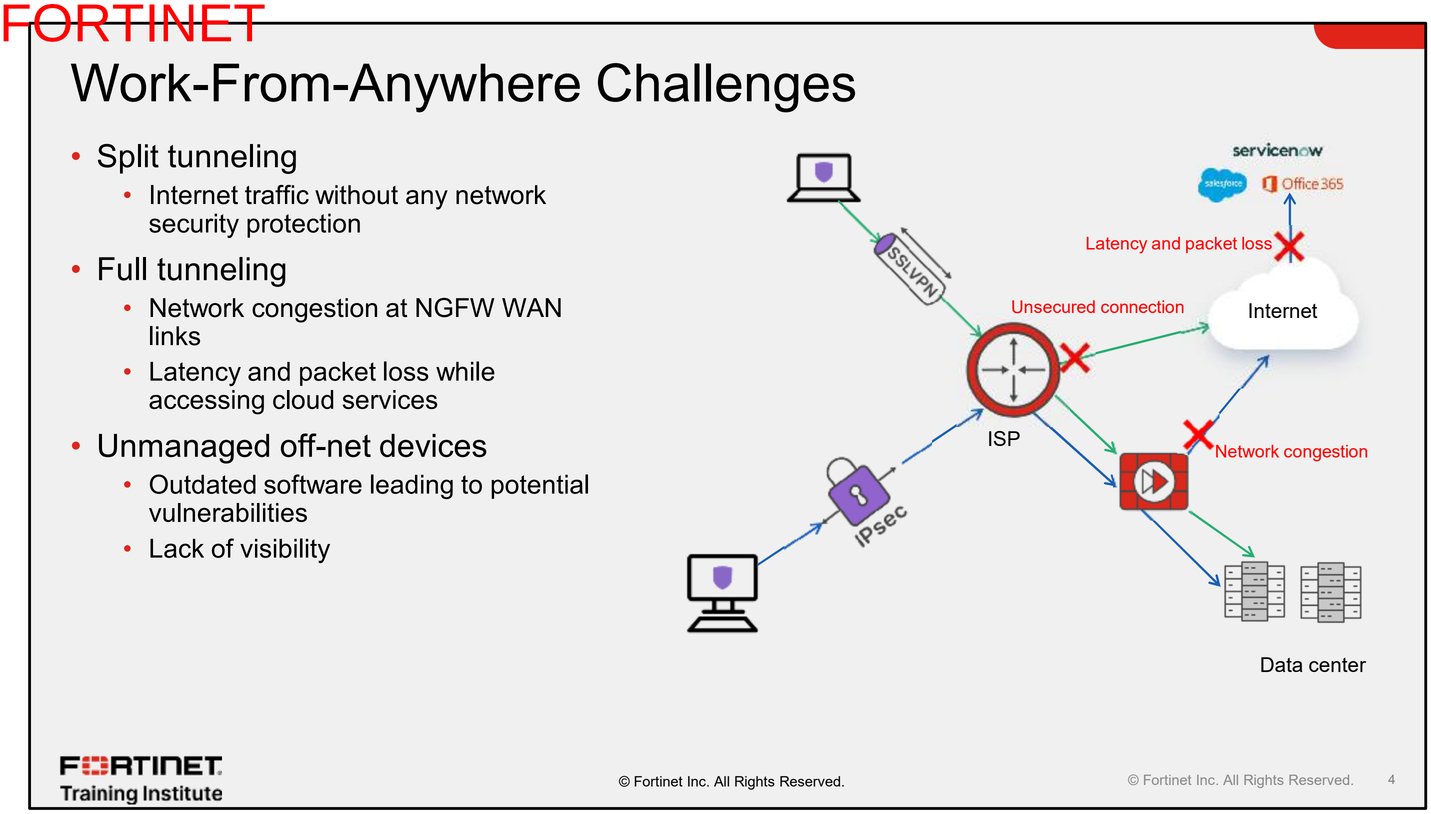
© Fortinet Inc. All Rights Reserved. 3

In a traditional VPN architecture, a next generation firewall (NGFW) is deployed on the edge of an organization's network. Remote access VPNs are intended to extend corporate networks to remote users, in a secure way, using a software client or agent. Remote access VPNs rely on IPsec or SSL-based VPN implementations. Remote access VPNs are deployed with either full tunneling or split tunneling enabled. In full tunneling mode, traffic destined for the organization's internal network and the internet, is sent through the VPN tunnel to the NGFW for threat detection and mitigation. In split tunneling mode, traffic destined for the internal network is sent through the VPN tunnel, and the internet traffic is sent out through their local ISP link.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET

Brave-dumps.com



Work-From-Anywhere Challenges

- Split tunneling
  - Internet traffic without any network security protection
- Full tunneling
  - Network congestion at NGFW WAN links
  - Latency and packet loss while accessing cloud services
- Unmanaged off-net devices
  - Outdated software leading to potential vulnerabilities
  - Lack of visibility

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

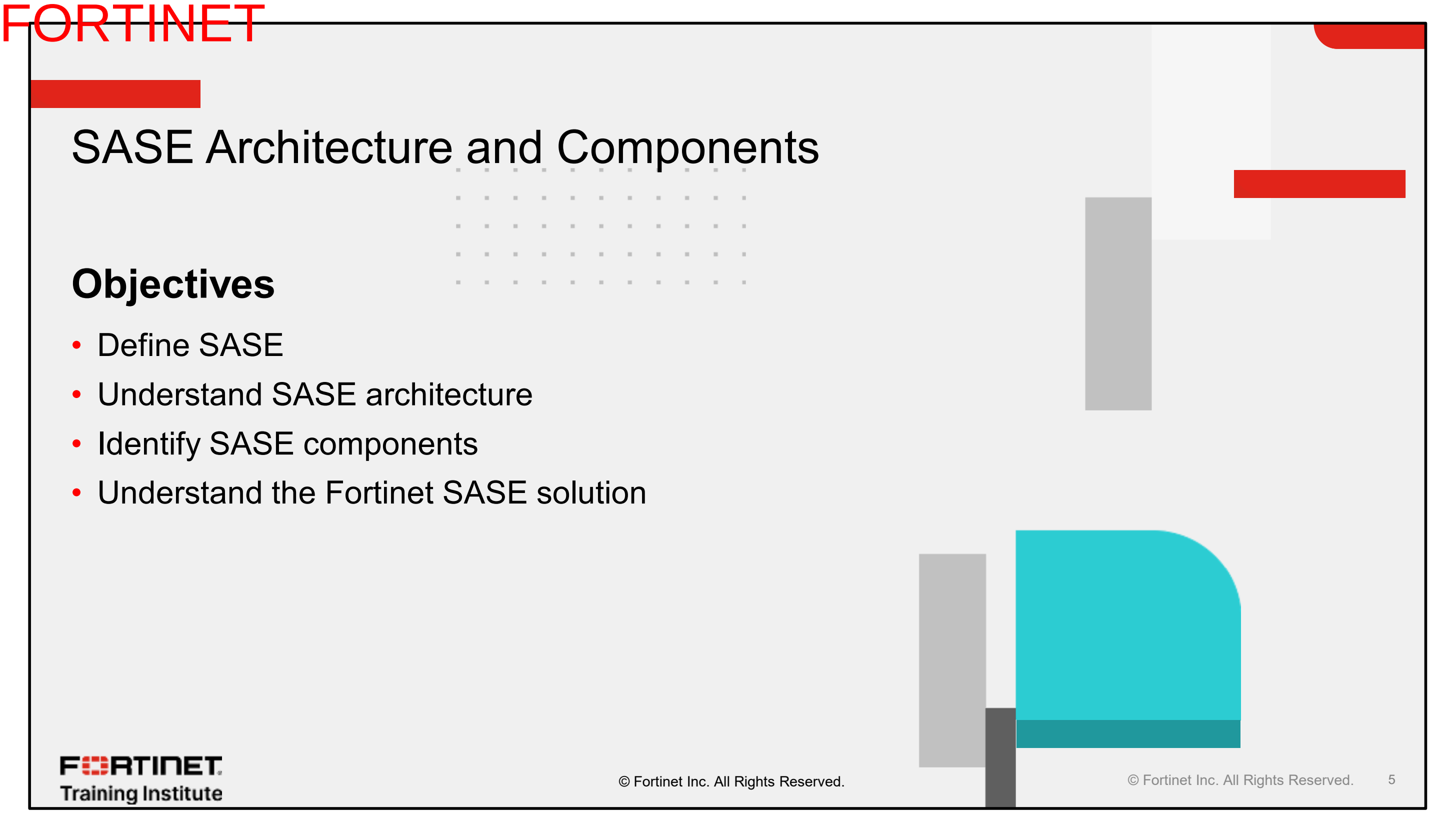
© Fortinet Inc. All Rights Reserved. 4

The standard firewall architecture is well-defined, but it faces significant challenges when dealing with work-from-anywhere practices. Typically, off-net endpoints are unmanaged, meaning the endpoints could fail security postures because of unpatched software and vulnerability updates. These devices cannot be trusted when accessing corporate network resources. When working from anywhere, the majority of the internet traffic is routed through an ISP without any network security protection, which makes it susceptible to malware and other network security threats. To overcome this issue, organizations started deploying full tunneling VPNs to use the NGFW security features at the network edge. An increase in the number of employees working remotely introduced extra load on the NGFW and its WAN links, leading to WAN link network congestion. Today, users are doing a large part of their work using cloud services and not in an on-premises data center. This could introduce latency and packet loss because all the traffic comes to the corporate NGFW first, and then goes back out to the internet. Another challenge that comes with a remote workforce is unmanaged off-net devices with outdated software. These devices can lead to potential vulnerabilities.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET

Brave-dumps.com



SASE Architecture and Components

Objectives

- Define SASE
- Understand SASE architecture
- Identify SASE components
- Understand the Fortinet SASE solution

© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved. 5

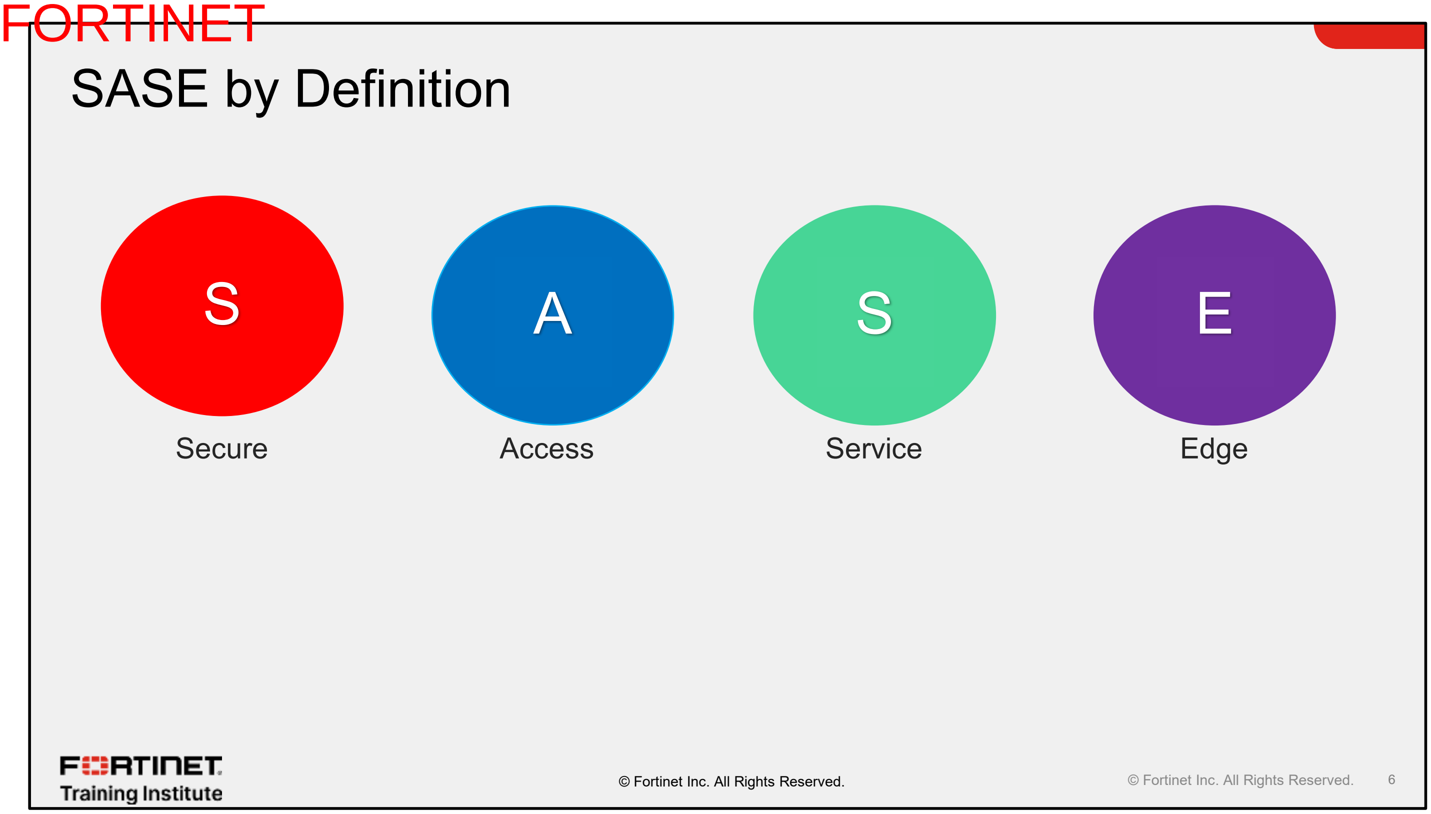
After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating a competent understanding of the SASE architecture, SASE components, and the Fortinet SASE solution, you will understand the purpose and capabilities of a SASE solution.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET

Brave-dumps.com



SASE by Definition

Secure

Access

Service

Edge

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved. 6

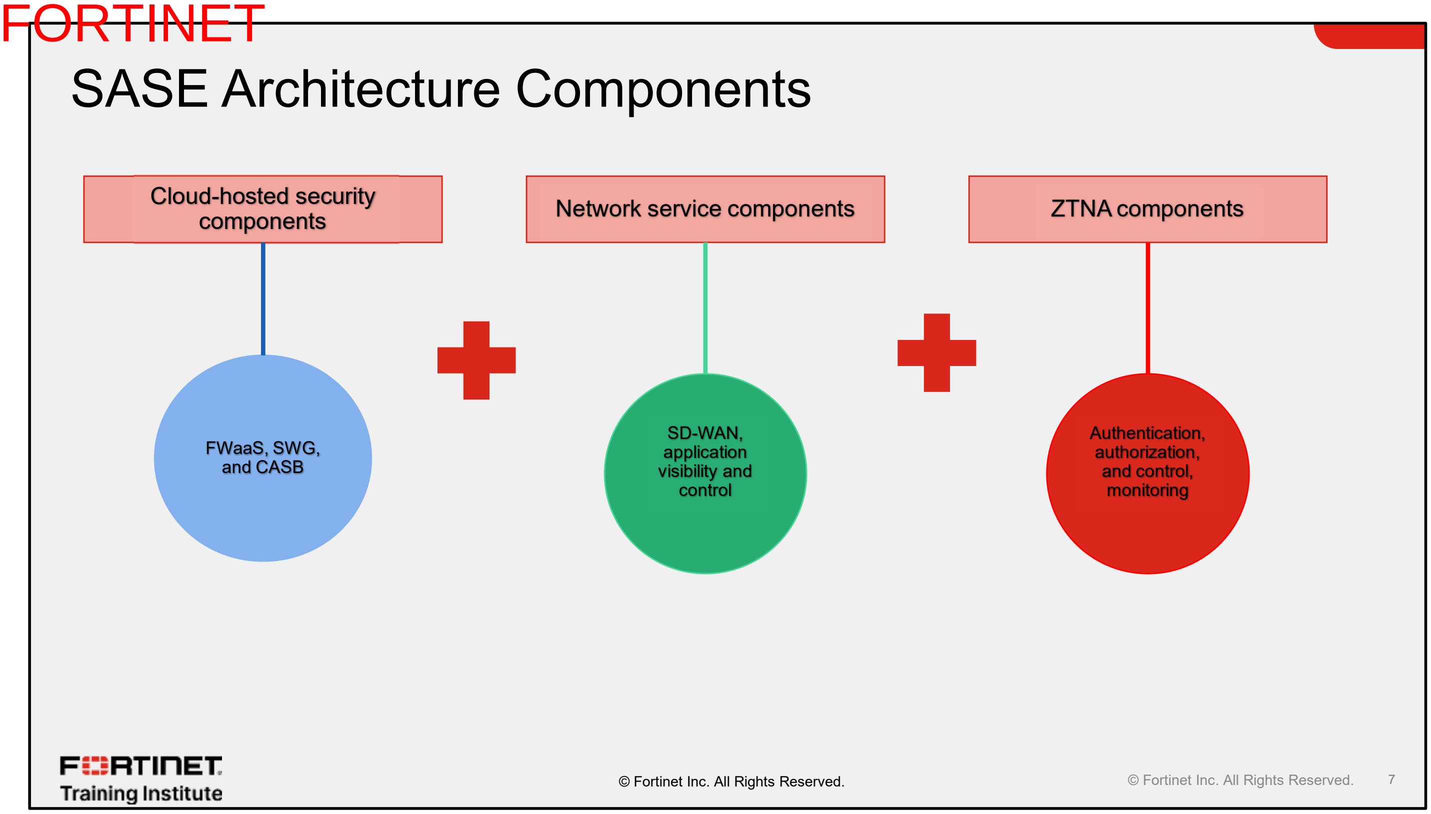
According to Gartner, secure access service edge, or SASE, delivers converged network and Security-as-a-Service (SECaaS) capability, including SD-WAN, secure web gateway (SWG), cloud access security broker (CASB), NGFW, and zero trust network access (ZTNA). SASE supports branch offices, remote workers, and on-premises secure access use cases. SASE is primarily delivered as a service and enables zero-trust access based on the identity of the device or entity, combined with real-time context and security and compliance policies.

The SASE architecture focuses on using a cloud-delivered service that enforces secure access at the farthest edge of the network—namely, at the service edge or user endpoints. The goal of SASE is to offer a secure connection to the user connecting from anywhere.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET

Brave-dumps.com



SASE Architecture Components

Cloud-hosted security components
FWaaS, SWG, and CASB
Network service components
SD-WAN, application visibility and control
ZTNA components
Authentication, authorization, and control, monitoring

© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved. 7

A cloud-hosted security solution frees devices from the need to rely on protection that is hosted at a physical corporate data center. Cloud-host security includes components like Firewall-as-a-Service (FWaaS), SWG, and CASB. FWaaS provides the same security features as a standard hardware firewall, but using software in the cloud. SWG blocks unauthorized traffic from getting into your organization’s network with web filtering, antivirus, file filtering, data loss prevention (DLP), and more for both managed and unmanaged devices. CASB is positioned between the user accessing the cloud and the cloud-based application they are trying to access. It is used to monitor activity and enforce an organization’s security policies.

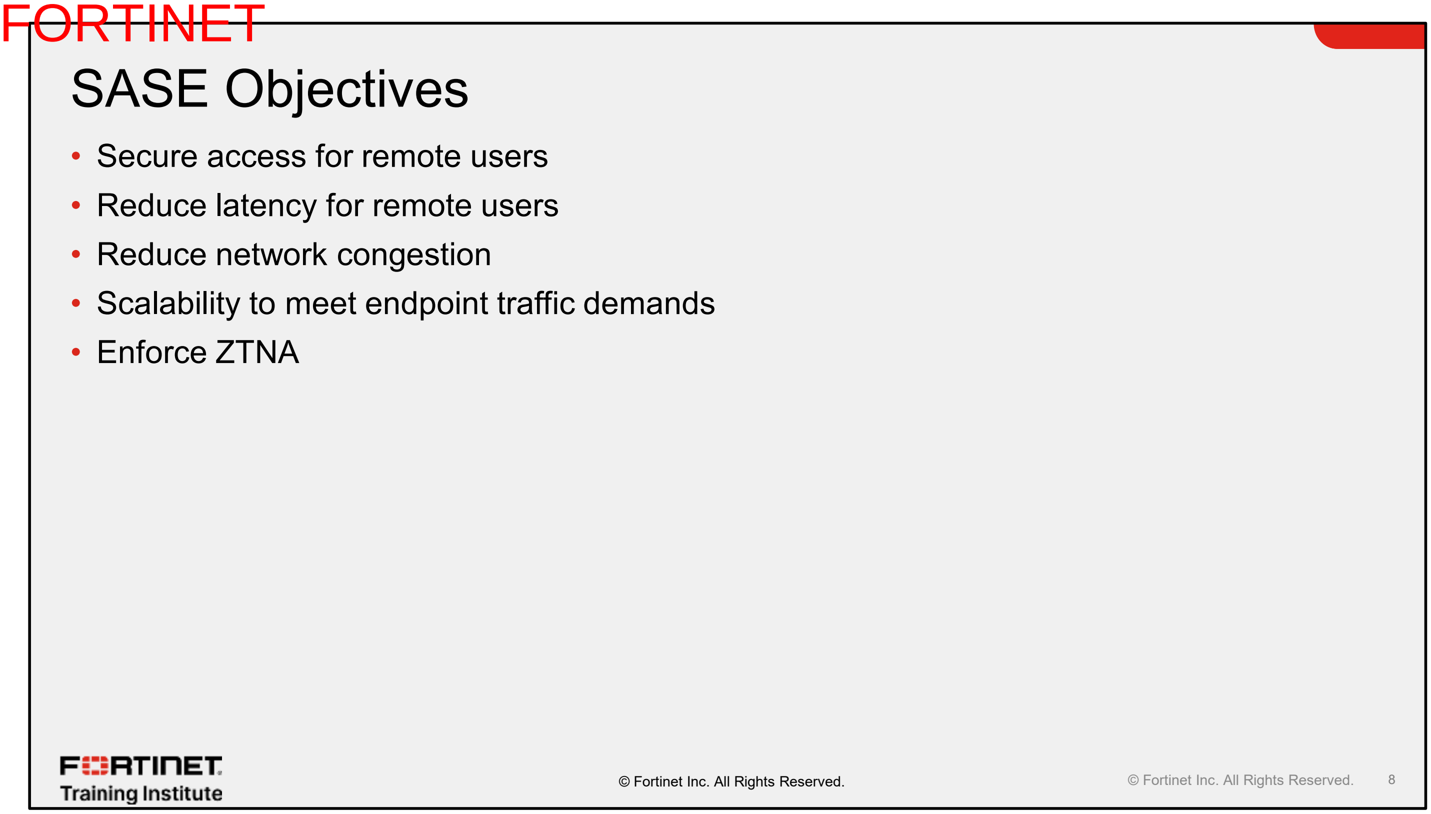
In the context of a SASE architecture, network components are used for optimized path selection and application-based routing. An SD-WAN solution can decide the best path for network traffic, and application-based routing provides access to the user to perform their jobs regardless of their location.

ZTNA is built on the zero-trust access core principle of "never trust, always verify.” All users, devices, and applications are assumed to be threats and, until they prove otherwise, they are not allowed to connect.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET

Brave-dumps.com



SASE Objectives

- Secure access for remote users
- Reduce latency for remote users
- Reduce network congestion
- Scalability to meet endpoint traffic demands
- Enforce ZTNA

Training Institute

© Fortinet Inc. All Rights Reserved.

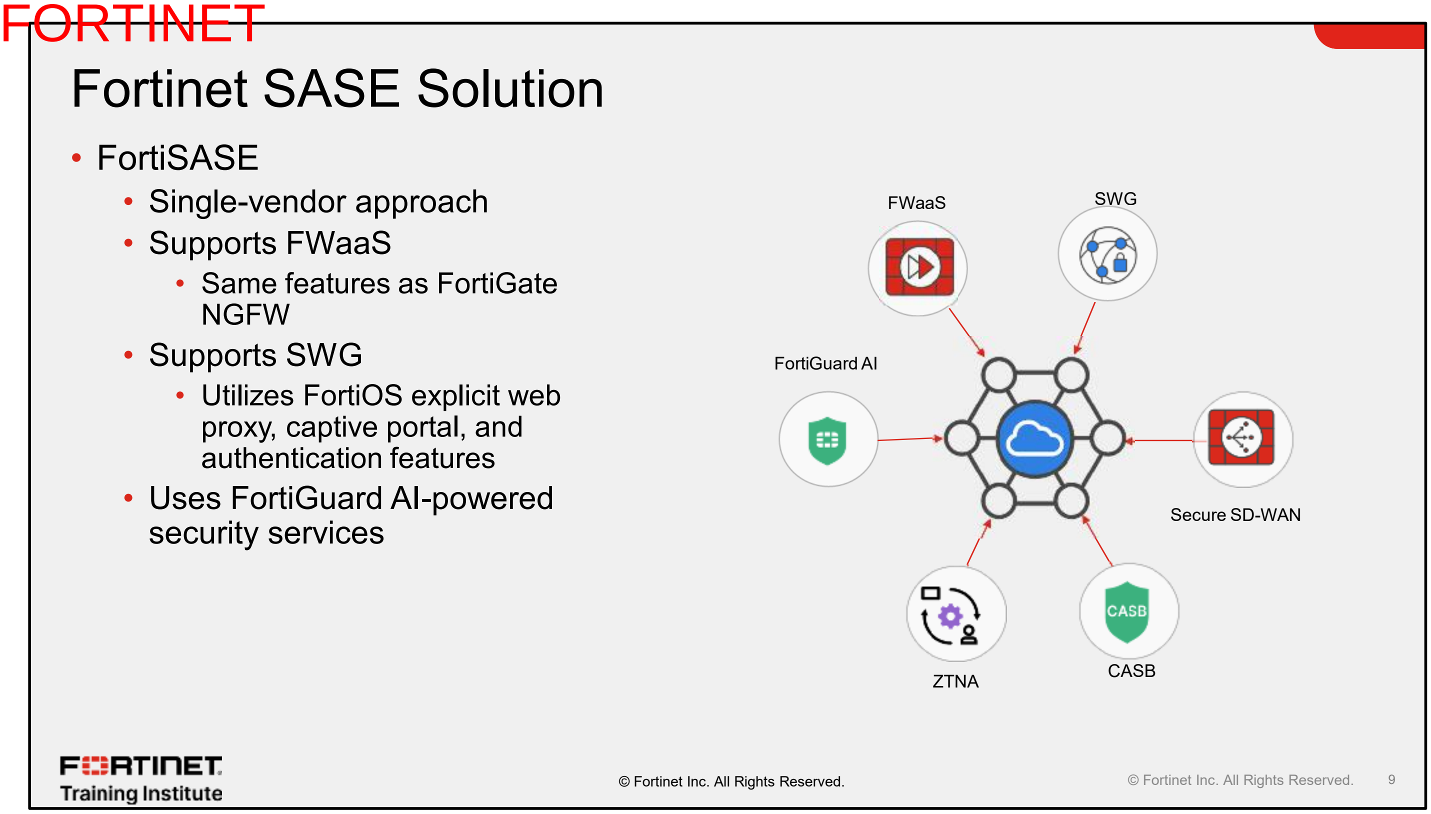
© Fortinet Inc. All Rights Reserved. 8

When remote users connect through VPN and their internet traffic is redirected through the corporate NGFW, they experience high latency. SASE reduces this latency by allowing remote users to connect directly to the closest geographical point of presence (POP) for a cloud-delivered FWaaS, where the internet traffic is subject to advanced threat measures. Also, each POP can scale to meet user demand and reduce the possibility that a single WAN link becomes a congestion point for these remote users. ZTNA allows you to apply zero-trust principles to control which users will access which application over the network. Applications are accessed when needed, directly through an access proxy or broker. With ZTNA, a user can more seamlessly work from the office or remotely, which creates a smoother user experience.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET

Brave-dumps.com



Fortinet SASE Solution

- FortiSASE
  - Single-vendor approach
  - Supports FWaaS
    - Same features as FortiGate NGFW
  - Supports SWG
    - Utilizes FortiOS explicit web proxy, captive portal, and authentication features
  - Uses FortiGuard AI-powered security services

© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved. 9

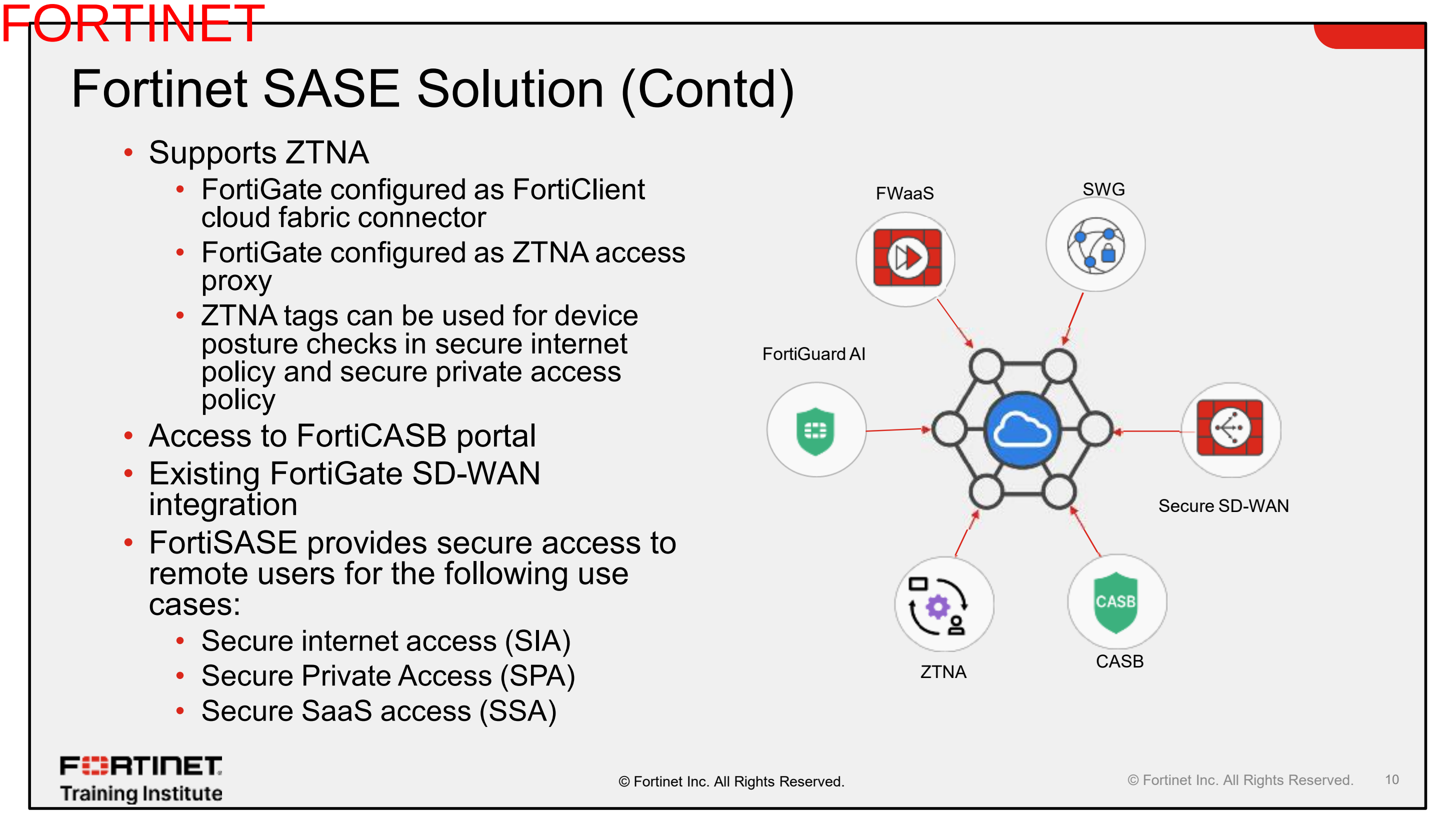
FortiSASE, Fortinet’s single-vendor SASE approach, empowers organizations to consistently apply enterprise-grade security and superior user experience across all edges, converging networking and security across a unified OS and agent. The cloud-delivered security service is located between the remote endpoints and any networks those endpoints access, regardless of the location of the remote endpoints. FortiSASE extends FortiGuard security services across thin edge, secure edge, and remote users, enabling secure access to users both on and off the network. You will learn more about the different deployment methods in another lesson.

FortiSASE supports FWaaS and SWG functionality, both of which rely on threat intelligence that FortiGuard labs provides. The FortiSASE FWaaS has all the same features, security, and reliability that customers depend on the Fortinet FortiGate NGFW physical and virtual appliances. Likewise, FortiSASE SWG relies on FortiOS explicit web proxy, captive portal, and authentication features to secure customers’ web traffic. SSO integration through SAML is supported for SWG and VPN deployments.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET

Brave-dumps.com



Fortinet SASE Solution (Contd)

- Supports ZTNA
  - FortiGate configured as FortiClient cloud fabric connector
  - FortiGate configured as ZTNA access proxy
  - ZTNA tags can be used for device posture checks in secure internet policy and secure private access policy
- Access to FortiCASB portal
- Existing FortiGate SD-WAN integration
- FortiSASE provides secure access to remote users for the following use cases:
  - Secure internet access (SIA)
  - Secure Private Access (SPA)
  - Secure SaaS access (SSA)

Training Institute

© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved.

10

FortiSASE supports ZTNA. In the configuration, the corporate FortiGate device is configured as a FortiClient cloud fabric connector and it acts as a ZTNA access proxy to process ZTNA traffic. FortiSASE synchronizes the ZTNA tags with the corporate FortiGate device. The ZTNA tags are used by FortiGate to allow or deny access to corporate resources. FortiSASE also uses the ZTNA tags to check for device postures in SIA policy and SPA policy.

FortiCASB provides cloud-based and API-based features to enable deep inspection of Software-as-a-Service (SaaS) applications to enable detailed monitoring, analysis, and reporting features. FortiSASE also provides inline-CASB functionality with a web filter and application control security features.

Organizations can integrate FortiSASE with existing FortiGate SD-WAN deployments in order to provide remote users access to private resources. In this configuration, FortiSASE communicates with the FortiGate SD-WAN hub. After completing this configuration, the FortiSASE security POPs act as spokes to this hub.

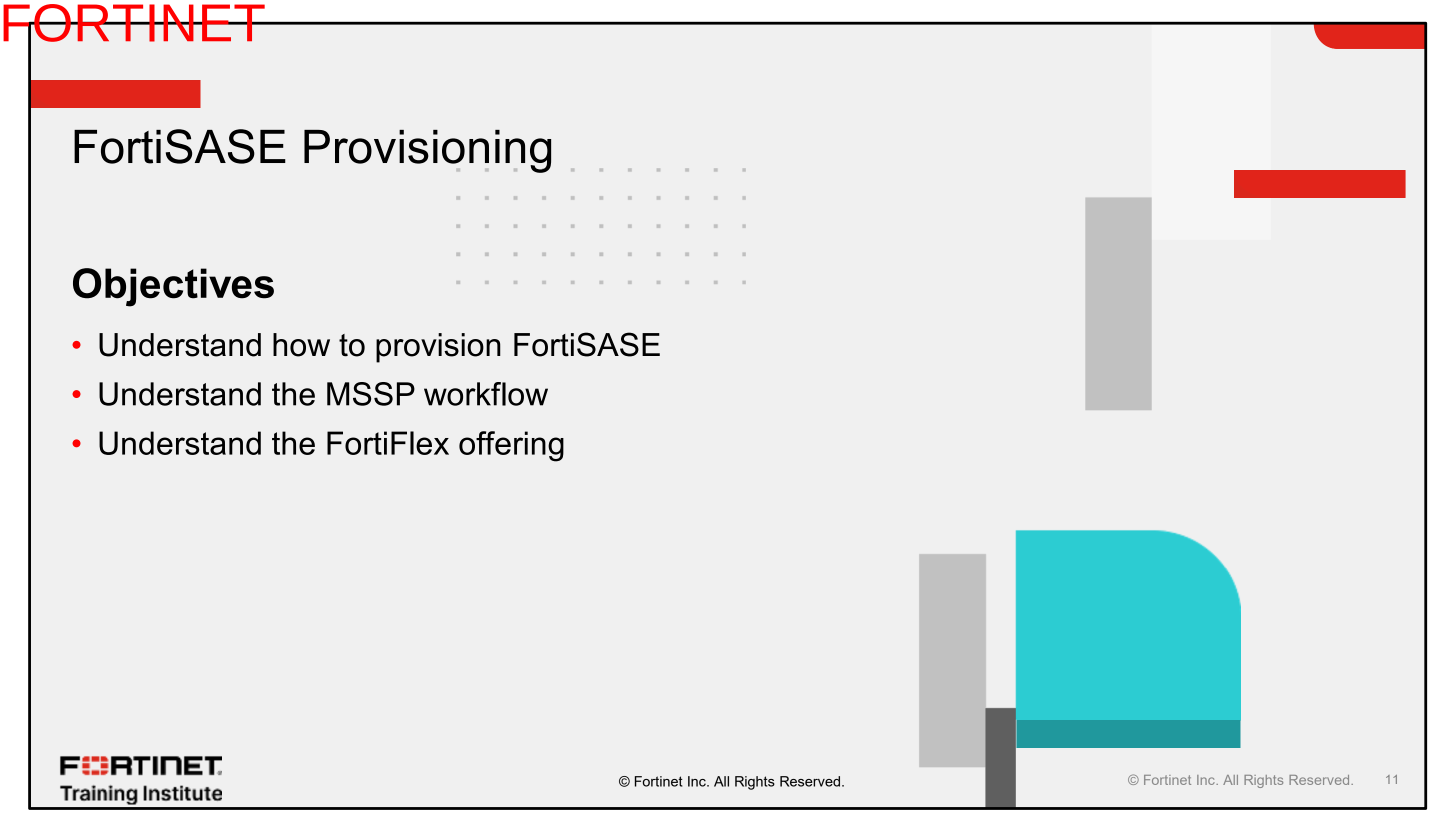
FortiSASE provides secure access to remote users for the following use cases:

- SIA, when remote users access internet and web-based applications
- SPA, when remote users access private company-hosted applications protected by FortiGate
- SSA, when remote users access SaaS applications

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET

Brave-dumps.com



FortiSASE Provisioning

Objectives

- Understand how to provision FortiSASE
- Understand the MSSP workflow
- Understand the FortiFlex offering

© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved. 11

After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating a competent understanding of FortiSASE provisioning, you will be able to provision FortiSASE instances. You will understand the MSSP workflow for FortiSASE deployments. You will also learn about the FortiFlex offerings to deploy FortiSASE.

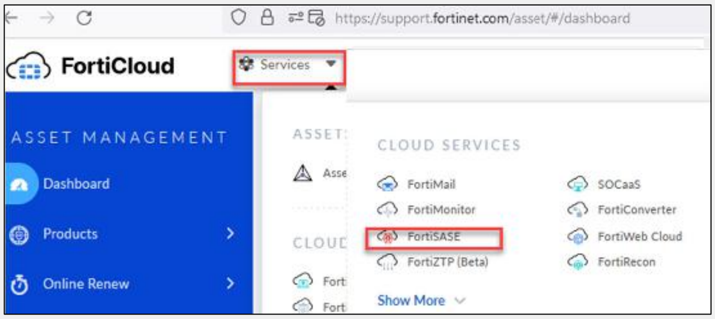
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET

Brave-dumps.com

Provisioning FortiSASE

- FortiCloud account
  - One FortiSASE instance per FortiCloud account
  - Cannot have FortiClient EMS cloud under the same account
- FortiSASE portal access
  - FortiSASE portal can be accessed through `support.fortinet.com` and then click **Services** > **CLOUD SERVICES** > **FortiSASE**



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved.

To provision FortiSASE, you must register the FortiSASE contract on `https://support.fortinet.com` using your FortiCloud account. You can use this FortiCloud account for only one FortiSASE instance and cannot register a FortiClient EMS cloud to this account. To access the FortiSASE portal, visit `https://support.fortinet.com`, and then click **Services** > **CLOUD SERVICES** > **FortiSASE**.

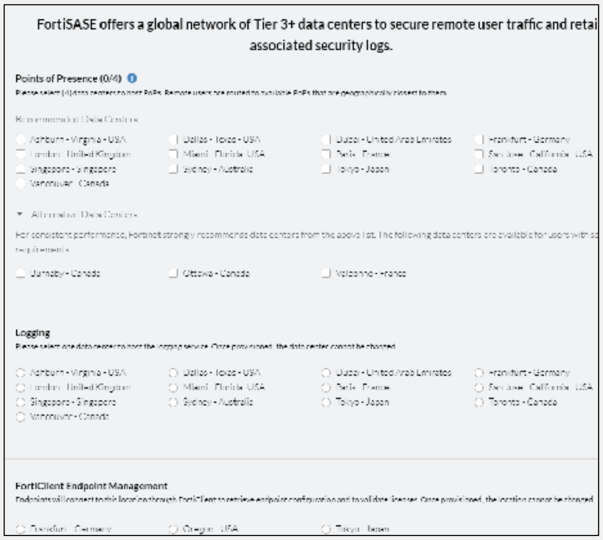
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET

Brave-dumps.com

Provisioning FortiSASE (Contd)

- FortiSASE POPs
  - Remote users are routed to POPs geographically closest to them
  - Additional POPs can be purchased
- Logging
  - Select data center to host the logging service
- FortiClient endpoint management
  - Endpoints connect to this location to retrieve configuration and validate licenses



FortiSASE offers a global network of Tier 3+ data centers to secure remote user traffic and retai
associated security logs.

Points of Presence (0/4)

Please select (4) data centers to host PoPs. Remote users are routed to available PoPs that are geographically closest to them.

Recommended Data Centers

☐ Ashburn - Virginia - USA ☐ Dallas - Texas - USA ☐ Dubai - United Arab Emirates ☐ Frankfurt - Germany
☐ London - United Kingdom ☐ Miami - Florida - USA ☐ Paris - France ☐ San Jose - California - USA
☐ Singapore - Singapore ☐ Sydney - Australia ☐ Tokyo - Japan ☐ Toronto - Canada
☐ Vancouver - Canada

▾ Alternative Data Centers

For consistent performance, Fortinet strongly recommends data centers from the above list. The following data centers are available for users with sp
requirements.

☐ Burnaby - Canada ☐ Ottawa - Canada ☐ Valbonne - France

Logging

Please select one data center to host the logging service. Once provisioned, the data center cannot be changed.

○ Ashburn - Virginia - USA ○ Dallas - Texas - USA ○ Dubai - United Arab Emirates ○ Frankfurt - Germany
○ London - United Kingdom ○ Miami - Florida - USA ○ Paris - France ○ San Jose - California - USA
○ Singapore - Singapore ○ Sydney - Australia ○ Tokyo - Japan ○ Toronto - Canada
○ Vancouver - Canada

FortiClient Endpoint Management

Endpoints will connect to this location through FortiClient to retrieve endpoint configuration and to validate licenses. Once provisioned, the location cannot be changed.

○ Frankfurt - Germany ○ Oregon - USA ○ Tokyo - Japan

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved.

When you access the FortiSASE portal for the first time, you need to select the location of the data centers that suit the requirements of your organization. The FortiSASE POP location is used to route remote users to the POP that is geographically closest to them. The logging data center hosts the logging service. The FortiClient endpoint management retrieves configuration information and validates FortiClient endpoint licenses. You can purchase additional POPs as part of the network add-on licenses. During initial provisioning, you can select fewer security sites than the maximum you are entitled to. In this case, upon each login, the FortiSASE portal prompts you to select up to the maximum number of security sites. For more details about POP locations, see the *FortiSASE Administration Guide*.

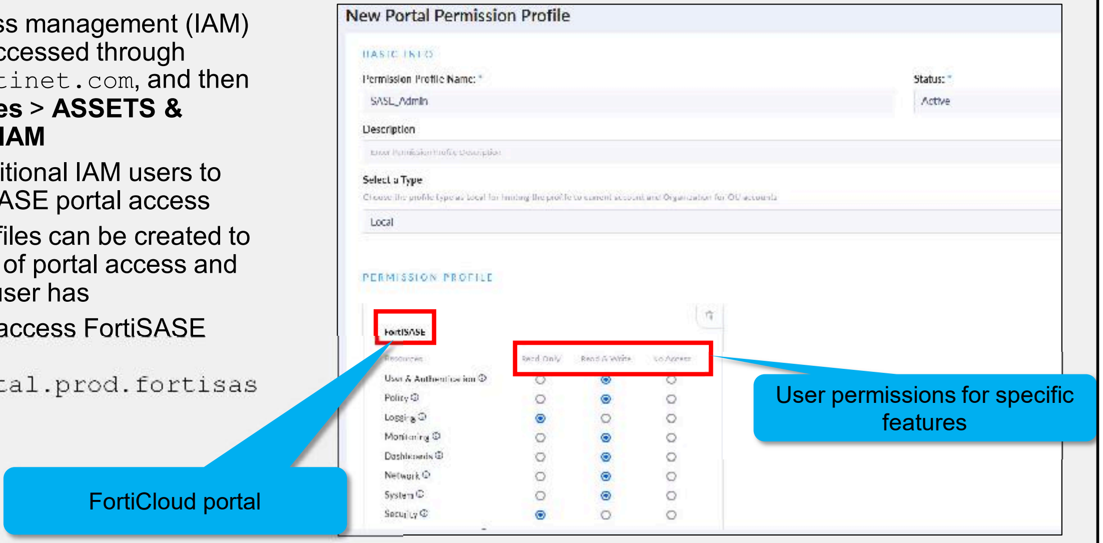
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET

Brave-dumps.com

IAM Users

- Identity & access management (IAM) portal can be accessed through `support.fortinet.com`, and then click on **Services** > **ASSETS & ACCOUNTS** > **IAM**
- Can create additional IAM users to provides FortiSASE portal access
- Permission profiles can be created to define the level of portal access and permissions a user has
- IAM users can access FortiSASE through `https://portal.prod.fortisase.com`



New Portal Permission Profile

BASIC INFO

Permission Profile Name: * SASL_Admin

Status: * Active

Description: Enter Permission Profile Description

Select a Type
Choose the profile type as Local for limiting the profile to current account and Organization for OU accounts

Local

PERMISSION PROFILE

FortiSASE

Resources	Read Only	Read & Write	No Access
User & Authentication	○	●	○
Policy	○	●	○
Logging	●	○	○
Monitoring	○	●	○
Dashboards	○	●	○
Network	○	●	○
System	○	●	○
Security	●	○	○

FortiCloud portal

User permissions for specific features

© Fortinet Inc. All Rights Reserved.

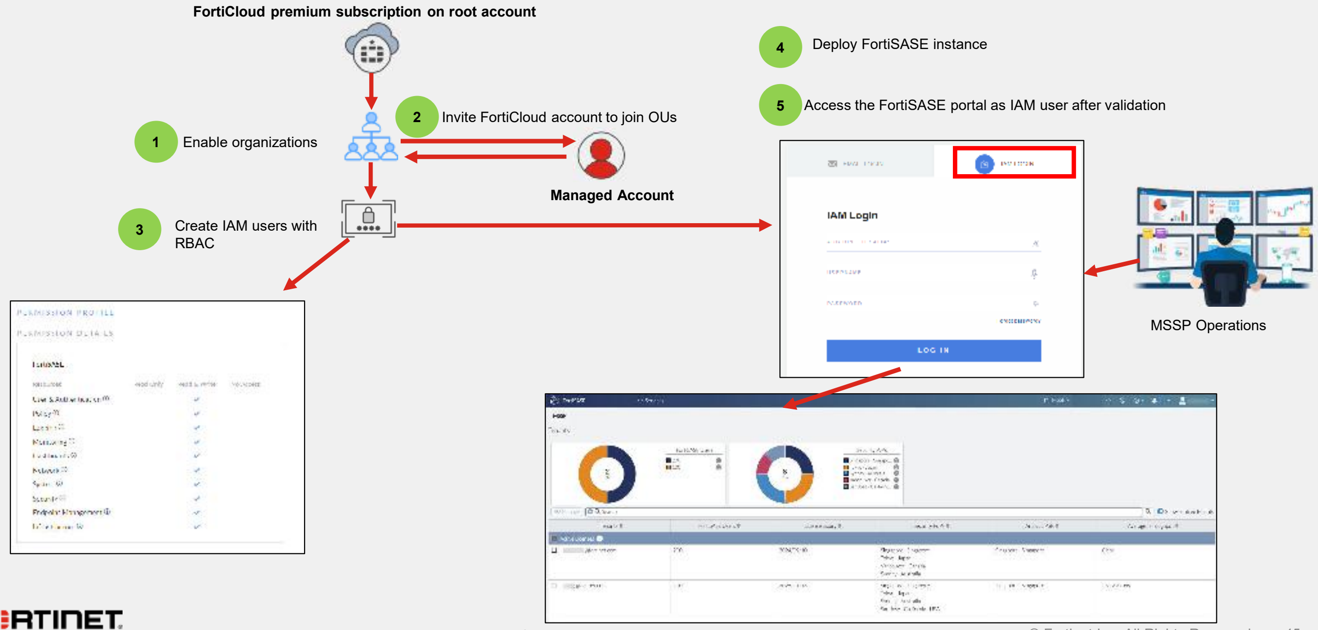
IAM is a service to help you control access to FortiCloud portals and assets. You can use the portal to manage users, authentication credentials, and asset permissions. You can create permission profiles to assign users permissions to specific features, instead off assigning access to the entire portal. To access the IAM portal, visit `https://support.fortinet.com`, and then click **Services** > **ASSETS & ACCOUNTS** > **IAM**. IAM users can access FortiSASE through `https://portal.prod.fortisase.com`, click **SSO Login**, and then click **IAM Login**.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET

Brave-dumps.com

MSSP Workflow


FortiCloud premium subscription on root account
1 Enable organizations
2 Invite FortiCloud account to join OUs
Managed Account
3 Create IAM users with RBAC
4 Deploy FortiSASE instance
5 Access the FortiSASE portal as IAM user after validation
IAM Login
LOG IN
MSSP Operations

Training Institute

© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved. 15

So, the first question is, why multi-tenancy? The primary use case is to manage multiple organizations from a single management console. For example, using multi-tenancy, a managed security service provider (MSSP) requires logins to only one console to manage multiple organizations efficiently and effectively.

The MSSP portal requires configuring an IAM user corresponding to the root account and a FortiCloud premium subscription. A FortiCloud premium subscription to the root account allows the portal to establish an organization and invite other FortiCare accounts to join that organization. FortiSASE includes an MSSP portal that supports centralized management and configuration capabilities, enabling the MSSP to deploy and manage SASE services across their client base.

This slide shows the flow of events to activate the FortiSASE MSSP portal:

1. Enable organizations on FortiCloud using the root account with a FortiCloud premium subscription.
2. Invite FortiCloud accounts to join organizational units (OUs).
3. Use the FortiCloud IAM portal to create and assign role-based access control (RBAC) to IAM users.
4. Deploy a FortiSASE instance.
5. Log in to the FortiSASE portal after validating the IAM user corresponding to the root account. After logging in, the IAM user can monitor and manage a tenant's FortiSASE instance.

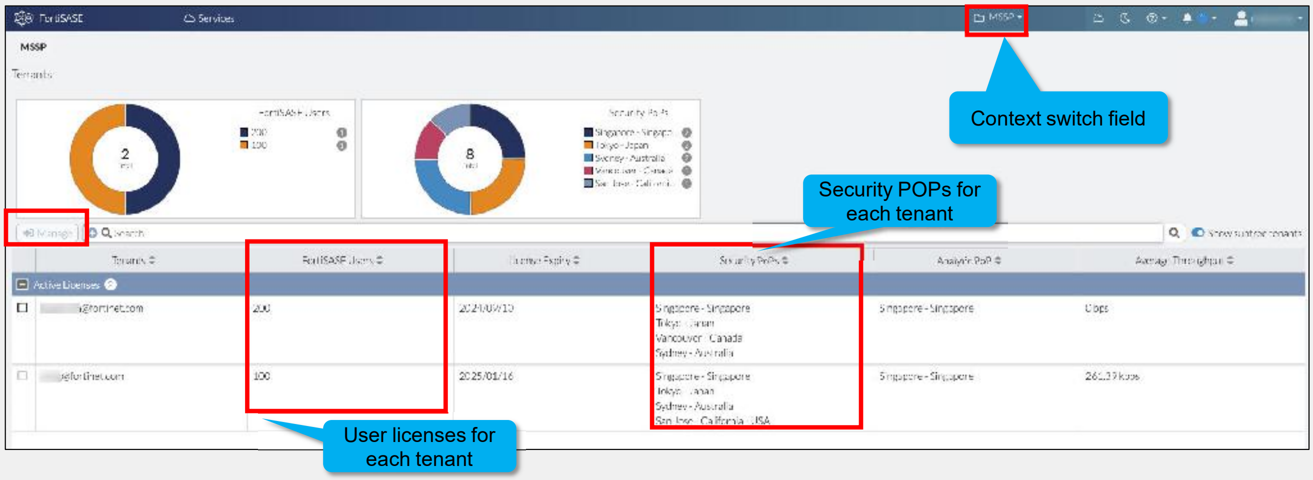
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET

Brave-dumps.com

MSSP Portal

- Two ways to manage customer tenants using FortiSASE
  - In the **Active License** category, select a tenant, and then click **Manage**
  - Select the desired FortiSASE instance from the context switch field



	Tenants	FortiSASE Users	License Expiry	Security PoPs	Analytic PoP	Average Throughput
	Active Licenses					
□	[redacted]@fortinet.com	200	2024/09/13	Singapore - Singapore Tokyo - Japan Vancouver - Canada Sydney - Australia	Singapore - Singapore	0 bps
□	[redacted]@fortinet.com	100	2025/01/16	Singapore - Singapore Tokyo - Japan Sydney - Australia San Jose - California - USA	Singapore - Singapore	261.39 kbps

Context switch field

Security POPs for each tenant

User licenses for each tenant

© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved.

Once logged into the FortiSASE MSSP portal, the MSSP administrator can monitor the tenant data including user licenses, security POPs, and so on.

You can manage the FortiSASE instance in two ways to get access to the primary dashboard of the desired tenant:

1. Select the tenant, and then, in the **Active Licenses** window, click **Manage**.
2. In the upper-right corner, in the context switch field, select the organization or suborganization.

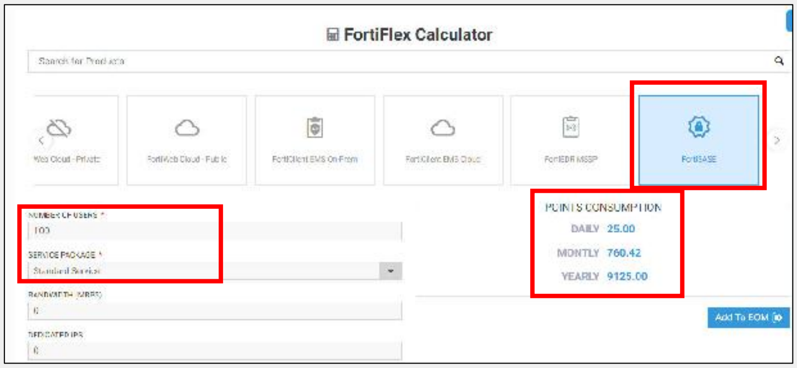
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET

Brave-dumps.com

FortiFlex Offering

- FortiFlex Program
  - Consumption model that offers on-demand use and pay-per-usage charging through BYOL licensing
- FortiSASE can be deployed the following ways:
  - Enterprises subscription: prepaid service
  - MSSP subscription: postpaid service



FortiFlex Calculator

Search for Products

NUMBER OF USERS *
100

SERVICE PACKAGE *
Standard Service

BANDWIDTH (MBPS)
0

DEDICATED IPS
0

POINTS CONSUMPTION

DAILY 25.00

MONTLY 760.42

YEARLY 9125.00

© Fortinet Inc. All Rights Reserved.

The FortiFlex program enable organizations to avoid procurement delays, eliminate legacy license management constraints, and benefit from a predictable OpEx model. It is a new consumption model that brings on-demand use and pay-per-usage charging through bring your own license (BYOL) licensing for virtual security instances, security services, and cloud-based management services.

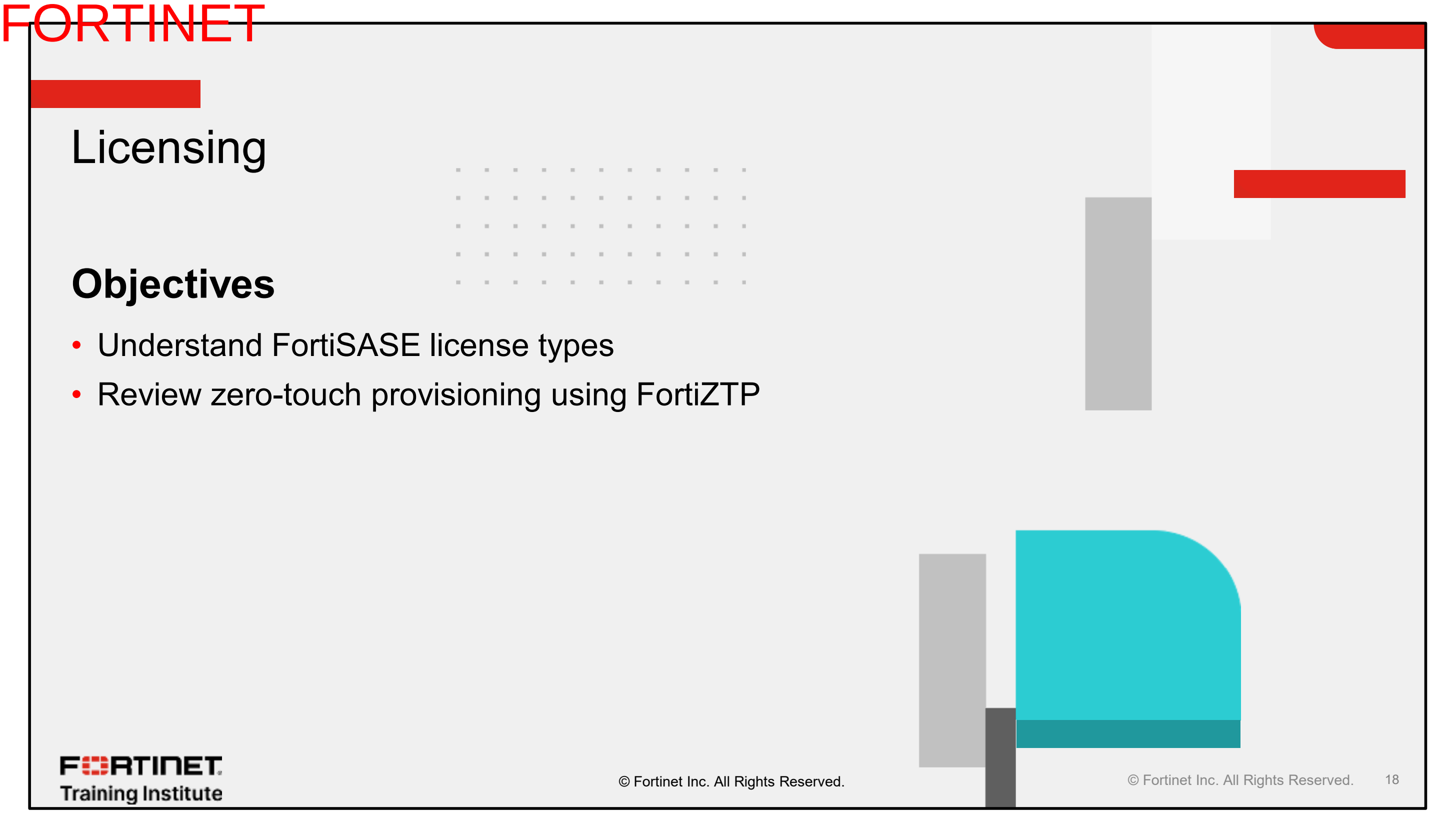
FortiSASE can now also be deployed using the FortiFlex enterprise subscription, a prepaid service using FortiFlex enterprise points or FortiFlex MSSP subscription, a postpaid subscription service that requires monthly payment for usage in consumption credits. A FortiFlex VM sizing calculator is available on `https://fndn.fortinet.net/index.php?/tools/fortiflex/`. This slide shows an example of points consumed while deploying a FortiSASE instance with a standard service package and 100 users using the FortiFlex enterprise subscription.

For more information about the FortiFlex program refer, to the *FortiFlex Ordering Guide*.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET

Brave-dumps.com



Licensing

Objectives

- Understand FortiSASE license types
- Review zero-touch provisioning using FortiZTP

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved.

18

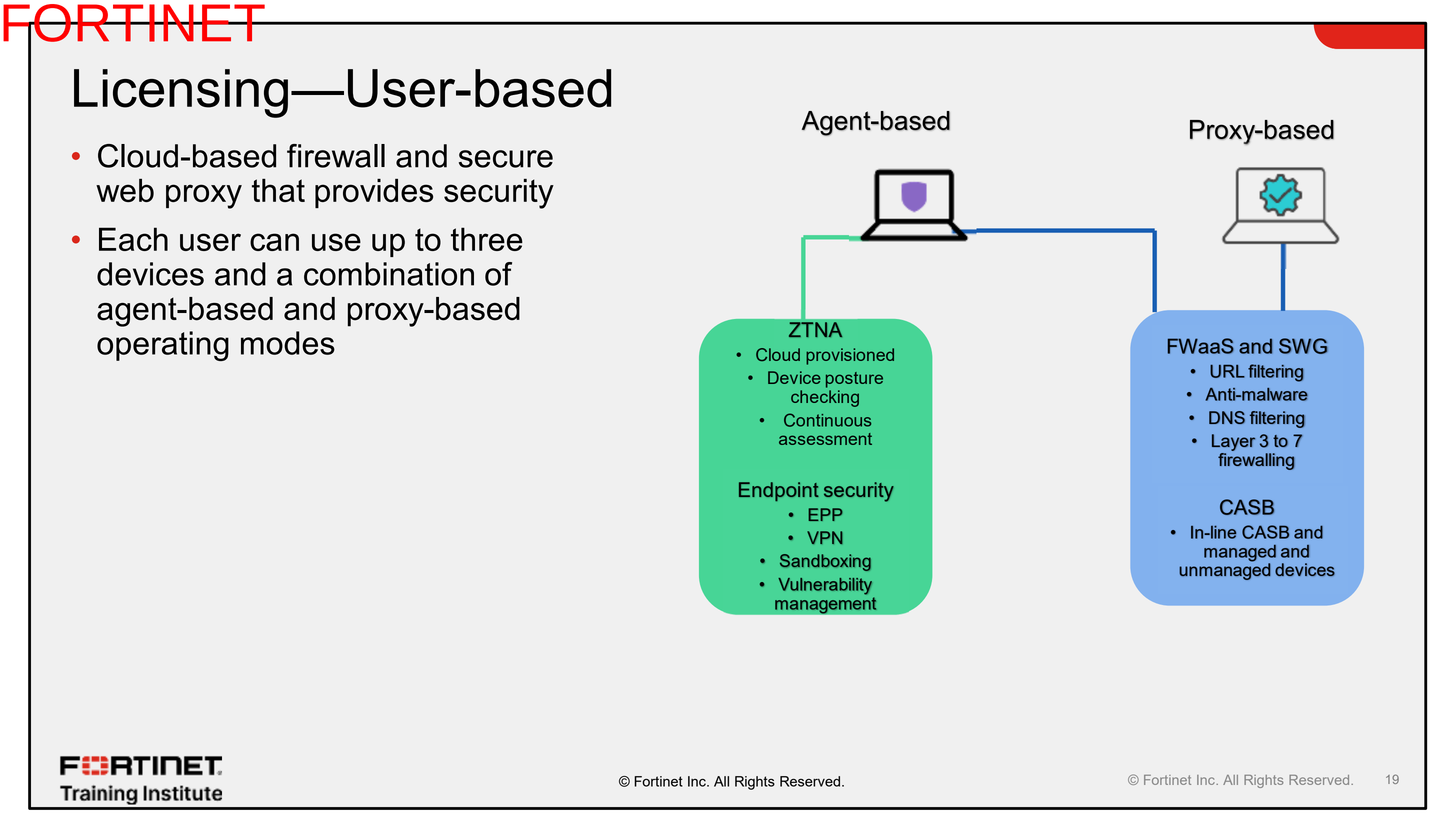
After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating a competent understanding of FortiSASE license types, you will be able to identify the license type that matches your requirements. You will learn how to deploy FortiAP and FortiExtender to FortiSASE using FortiZTP.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET

Brave-dumps.com



Licensing—User-based

- Cloud-based firewall and secure web proxy that provides security
- Each user can use up to three devices and a combination of agent-based and proxy-based operating modes

Agent-based

ZTNA
- Cloud provisioned
- Device posture checking
- Continuous assessment

Endpoint security
- EPP
- VPN
- Sandboxing
- Vulnerability management

Proxy-based

FWaaS and SWG
- URL filtering
- Anti-malware
- DNS filtering
- Layer 3 to 7 firewalling

CASB
- In-line CASB and managed and unmanaged devices

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved. 19

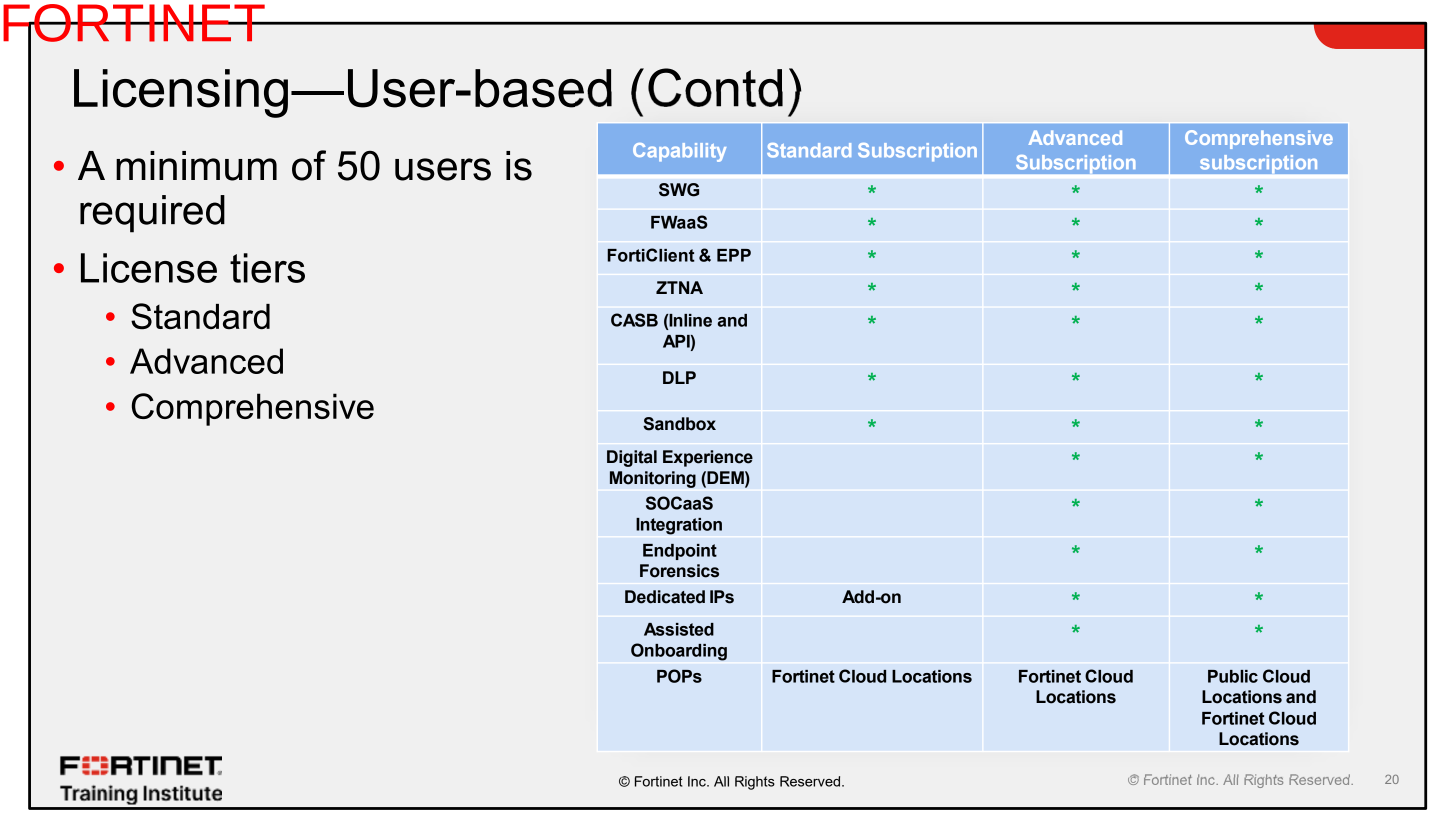
FortiSASE offers user-based licenses and add-on licenses for edge devices, bandwidth add-on, dedicated public IP addresses, and SPA deployments. You can mix and match license types to suit the needs of your organization.

User-based licenses allow users to connect with multiple devices concurrently. You can use user-based licenses in agent-based or proxy-based mode. In proxy-based mode, FortiSASE provides FWaaS and acts as a SWG. The features in proxy-based mode include URL filtering, anti-malware, DNS filtering, layer 3 to 7 firewalling, and an in-line CASB. To use agent-based mode, you must install FortiClient on the endpoint. Agent-based mode offers the same features as proxy-based mode, with the addition of endpoint protection with ZTNA. Each user can use up to three devices and a combination of agent-based and proxy-based modes.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET

Brave-dumps.com



Licensing—User-based (Contd)

- A minimum of 50 users is required
- License tiers
  - Standard
  - Advanced
  - Comprehensive

Capability	Standard Subscription	Advanced Subscription	Comprehensive subscription
SWG	*	*	*
FWaaS	*	*	*
FortiClient & EPP	*	*	*
ZTNA	*	*	*
CASB (Inline and API)	*	*	*
DLP	*	*	*
Sandbox	*	*	*
Digital Experience Monitoring (DEM)		*	*
SOCaaS Integration		*	*
Endpoint Forensics		*	*
Dedicated IPs	Add-on	*	*
Assisted Onboarding		*	*
POPs	Fortinet Cloud Locations	Fortinet Cloud Locations	Public Cloud Locations and Fortinet Cloud Locations

© Fortinet Inc. All Rights Reserved.

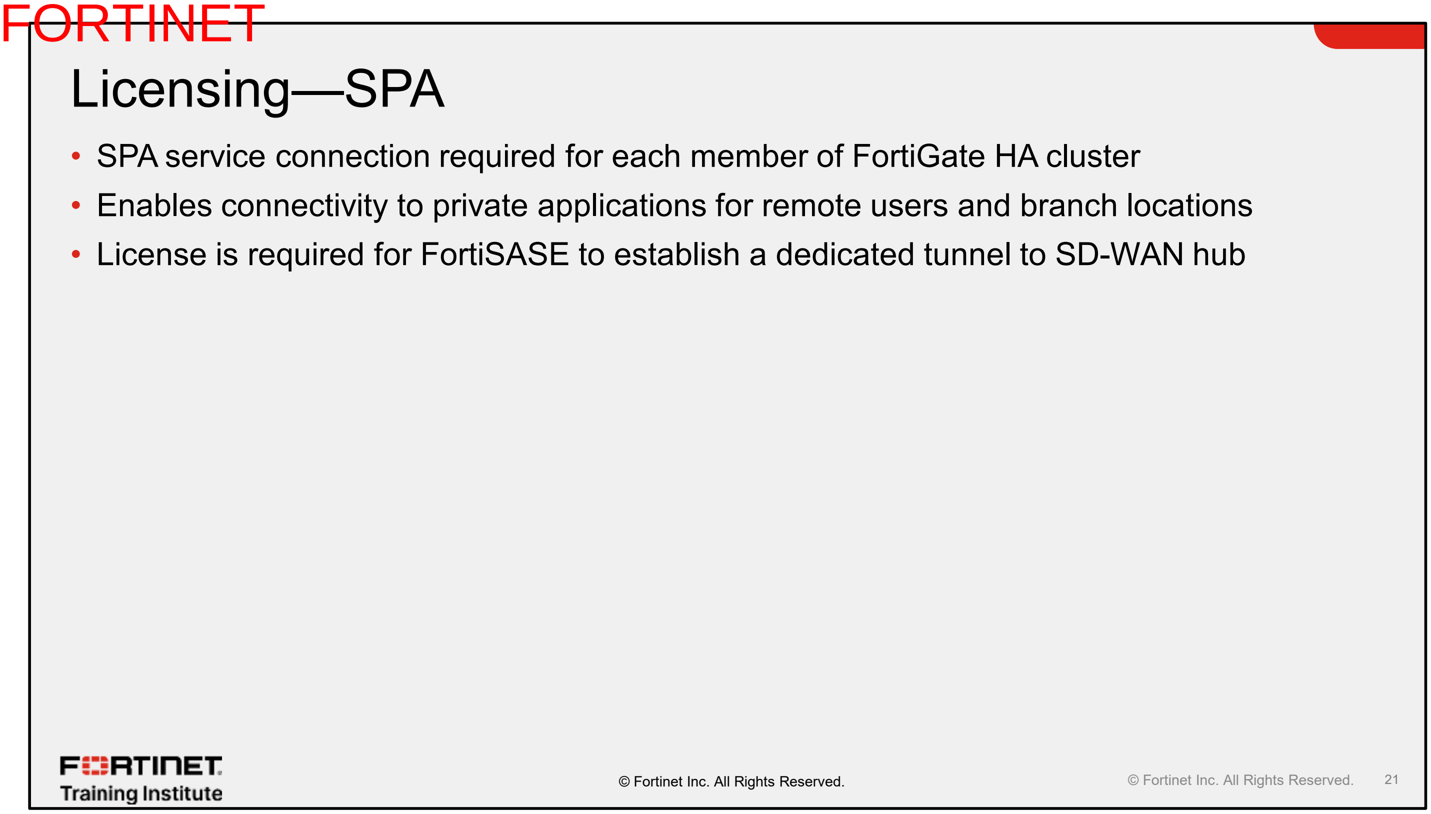
© Fortinet Inc. All Rights Reserved. 20

FortiSASE offers three different license tiers. Standard license includes SIA, SSA, SPA, endpoint protection, SASE cloud management, REST API, SASE cloud logging, and Fortinet cloud-hosted POPs. The advanced license offers the same features as the standard license, as well as DEM, SOC-as-a-Service (SOCaaS) integration, dedicated IP addresses, and FortiGuard forensics service. The comprehensive license offers the same features as the advanced license, but the POPs can be hosted on Fortinet cloud or public cloud locations. All license types have add-on features as well. For more details, contact the Fortinet sales team.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET

Brave-dumps.com



Licensing—SPA

- SPA service connection required for each member of FortiGate HA cluster
- Enables connectivity to private applications for remote users and branch locations
- License is required for FortiSASE to establish a dedicated tunnel to SD-WAN hub

Training Institute

© Fortinet Inc. All Rights Reserved.

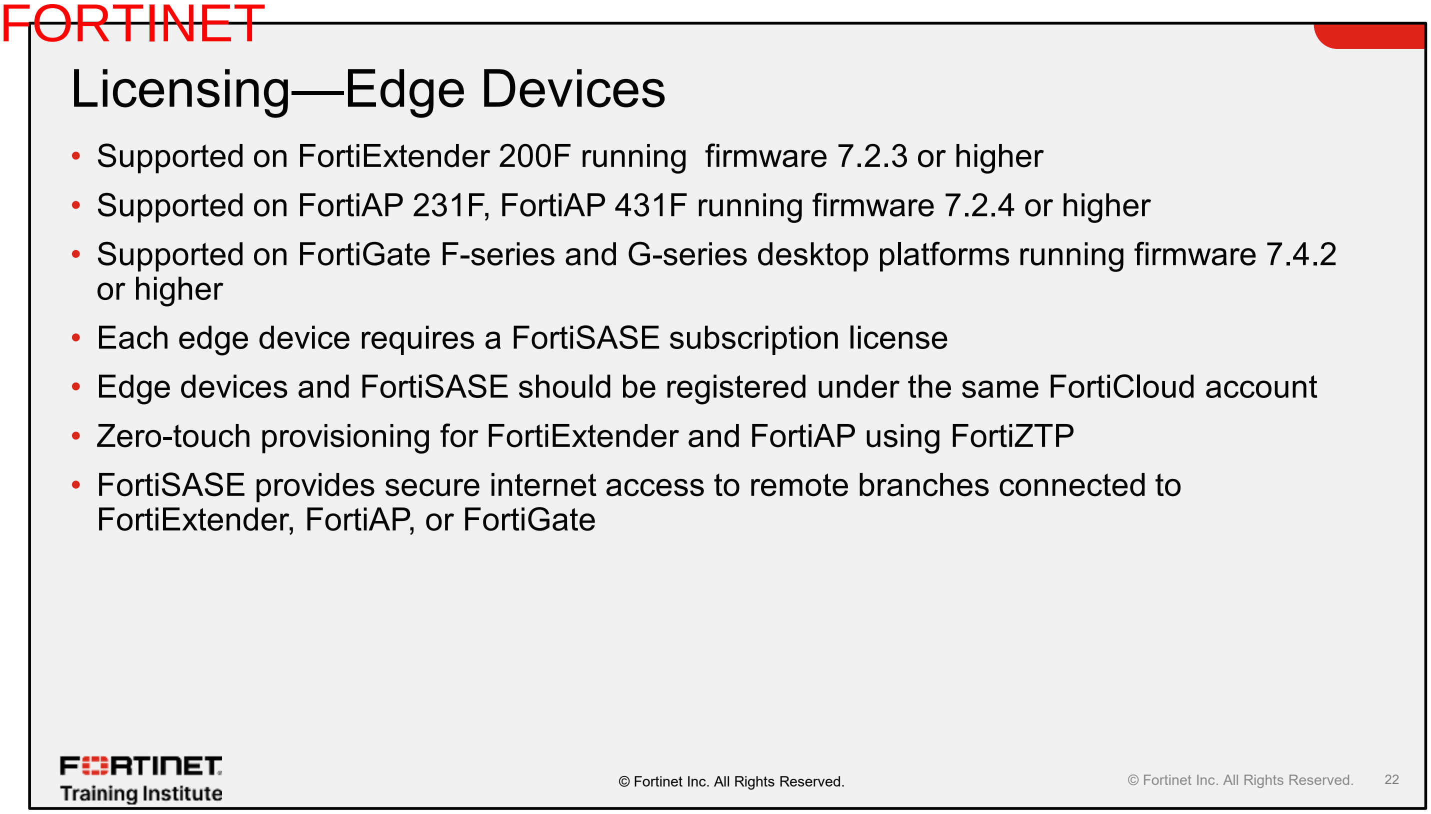
© Fortinet Inc. All Rights Reserved. 21

An SPA license allows remote users and branch locations to connect to private applications. If FortiGate is in a high availability (HA) cluster, you will need a separate license for each HA member. To establish a dedicated tunnel to FortiSASE, the FortiGate SD-WAN hub requires an SPA license. Remote users connected to FortiSASE can access private applications behind the FortiGate using this secure dedicated tunnel.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET

Brave-dumps.com



Licensing—Edge Devices

- Supported on FortiExtender 200F running firmware 7.2.3 or higher
- Supported on FortiAP 231F, FortiAP 431F running firmware 7.2.4 or higher
- Supported on FortiGate F-series and G-series desktop platforms running firmware 7.4.2 or higher
- Each edge device requires a FortiSASE subscription license
- Edge devices and FortiSASE should be registered under the same FortiCloud account
- Zero-touch provisioning for FortiExtender and FortiAP using FortiZTP
- FortiSASE provides secure internet access to remote branches connected to FortiExtender, FortiAP, or FortiGate

© Fortinet Inc. All Rights Reserved.

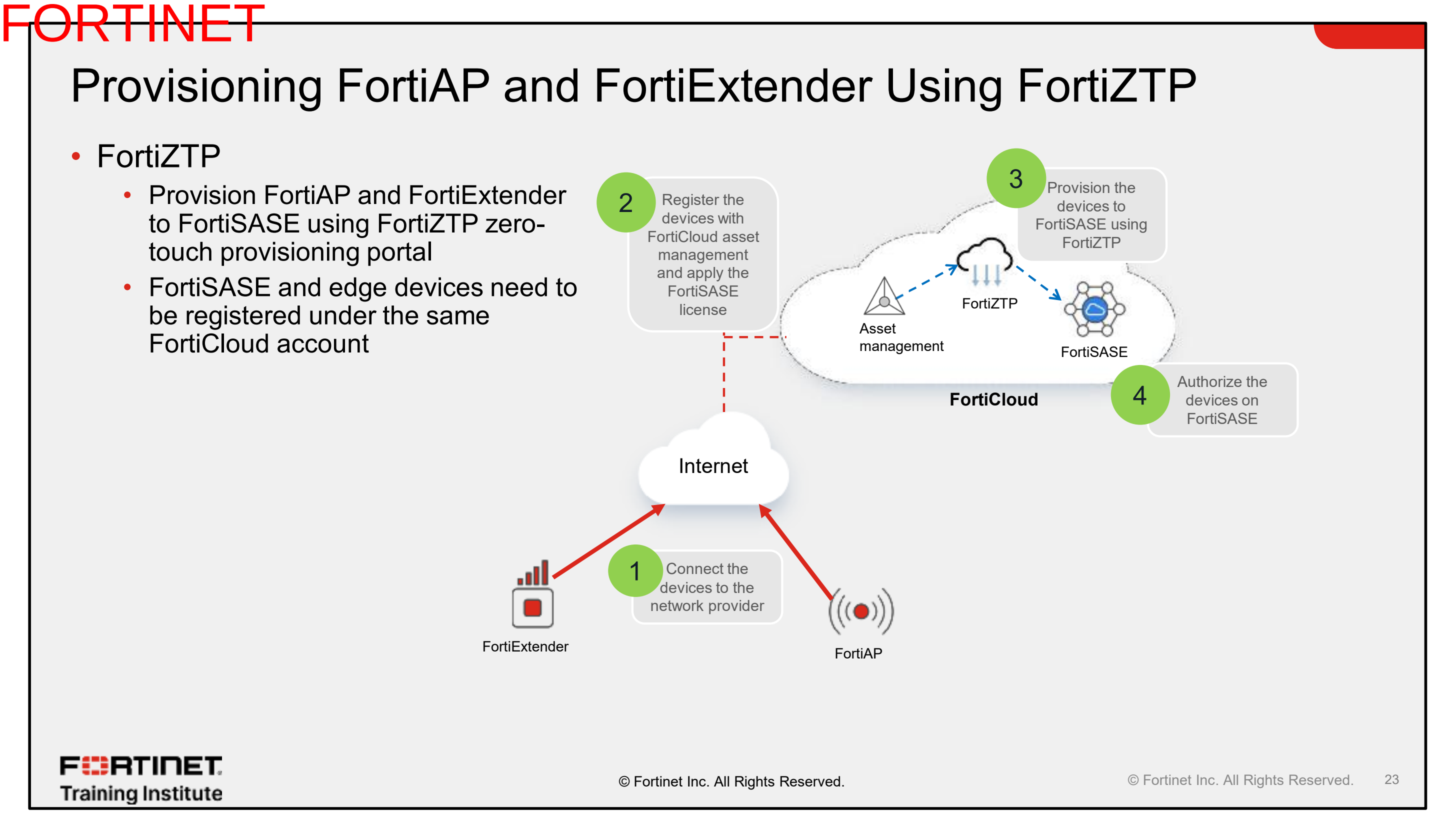
© Fortinet Inc. All Rights Reserved. 22

An edge device license enables customers to connect branch offices to FortiSASE. Edge device licenses are currently supported only on FortiExtender 200F, FortiAP 231F, FortiAP 431F, and all FortiGate F-series and G-series desktop platforms. Edge devices and FortiSASE should be registered under the same FortiCloud account. You can provision a FortiExtender or FortiAP to FortiSASE using FortiZTP.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET

Brave-dumps.com



Provisioning FortiAP and FortiExtender Using FortiZTP

- FortiZTP
  - Provision FortiAP and FortiExtender to FortiSASE using FortiZTP zero-touch provisioning portal
  - FortiSASE and edge devices need to be registered under the same FortiCloud account

1 Connect the devices to the network provider

2 Register the devices with FortiCloud asset management and apply the FortiSASE license

3 Provision the devices to FortiSASE using FortiZTP

4 Authorize the devices on FortiSASE

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved. 23

FortiZTP enables the deployment of Fortinet security, network, and wireless devices at remote locations where on-site provisioning technical expertise is limited. Remote devices can be assigned to a specific Fortinet management device or service. FortiZTP automatically loads devices that are registered to asset management with the same FortiCloud account on `https://support.fortinet.com`.

This slide shows the flow of events to deploy a FortiExtender and FortiAP to your FortiSASE network using FortiZTP:

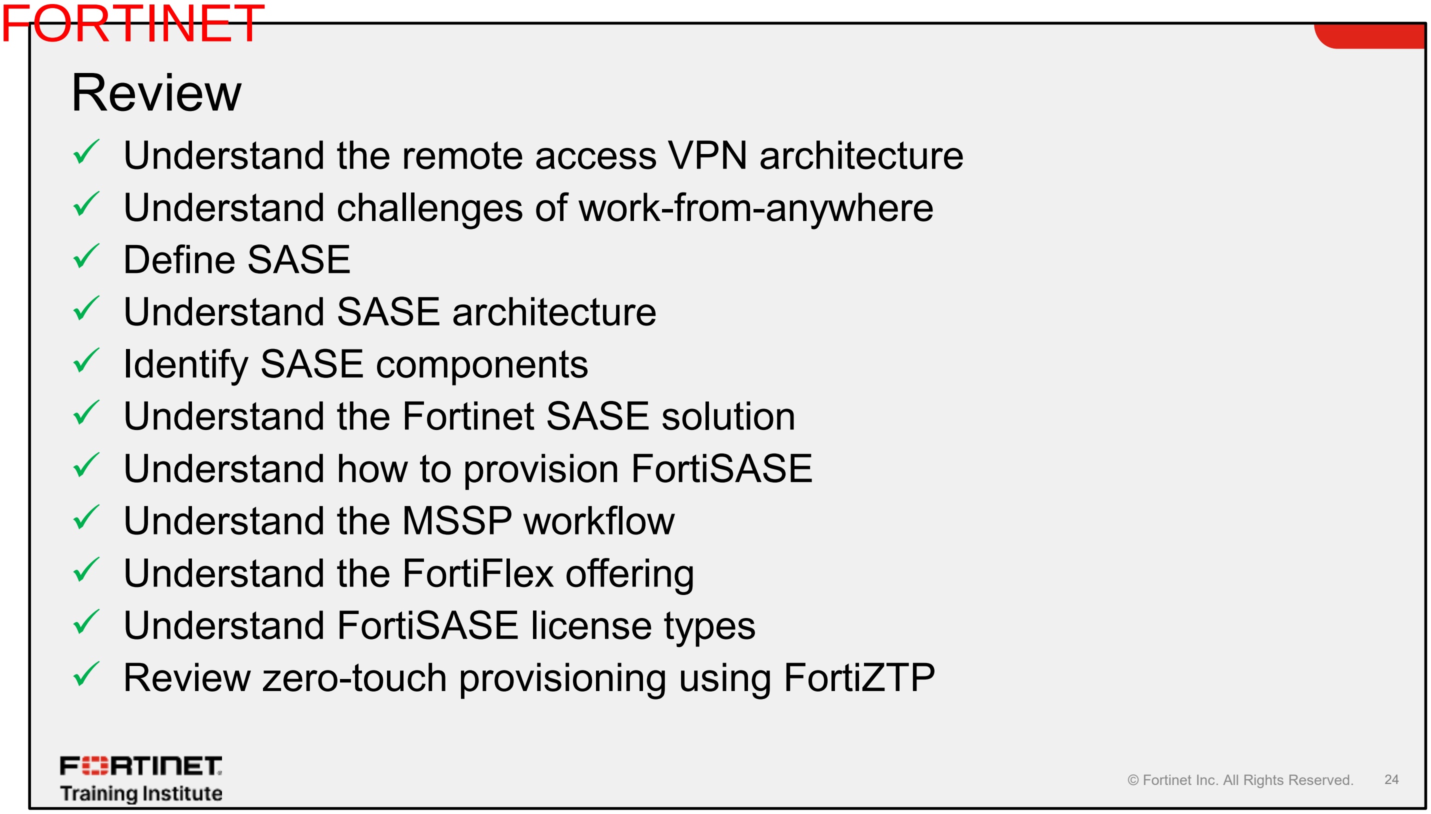
1. Connect the FortiAP and FortiExtender to your network provider.
2. Register the FortiExtender and FortiAP with FortiCloud asset management using your FortiCloud account. Apply the FortiSASE license to the devices.
3. Provision the devices using the FortiZTP portal.
4. Authorize the devices on the FortiSASE portal as edge devices.

You will learn about the configuration of connecting FortiExtender and FortiAP to FortiSASE in another lesson.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET

Brave-dumps.com



Review

- ✓ Understand the remote access VPN architecture
- ✓ Understand challenges of work-from-anywhere
- ✓ Define SASE
- ✓ Understand SASE architecture
- ✓ Identify SASE components
- ✓ Understand the Fortinet SASE solution
- ✓ Understand how to provision FortiSASE
- ✓ Understand the MSSP workflow
- ✓ Understand the FortiFlex offering
- ✓ Understand FortiSASE license types
- ✓ Review zero-touch provisioning using FortiZTP

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 24

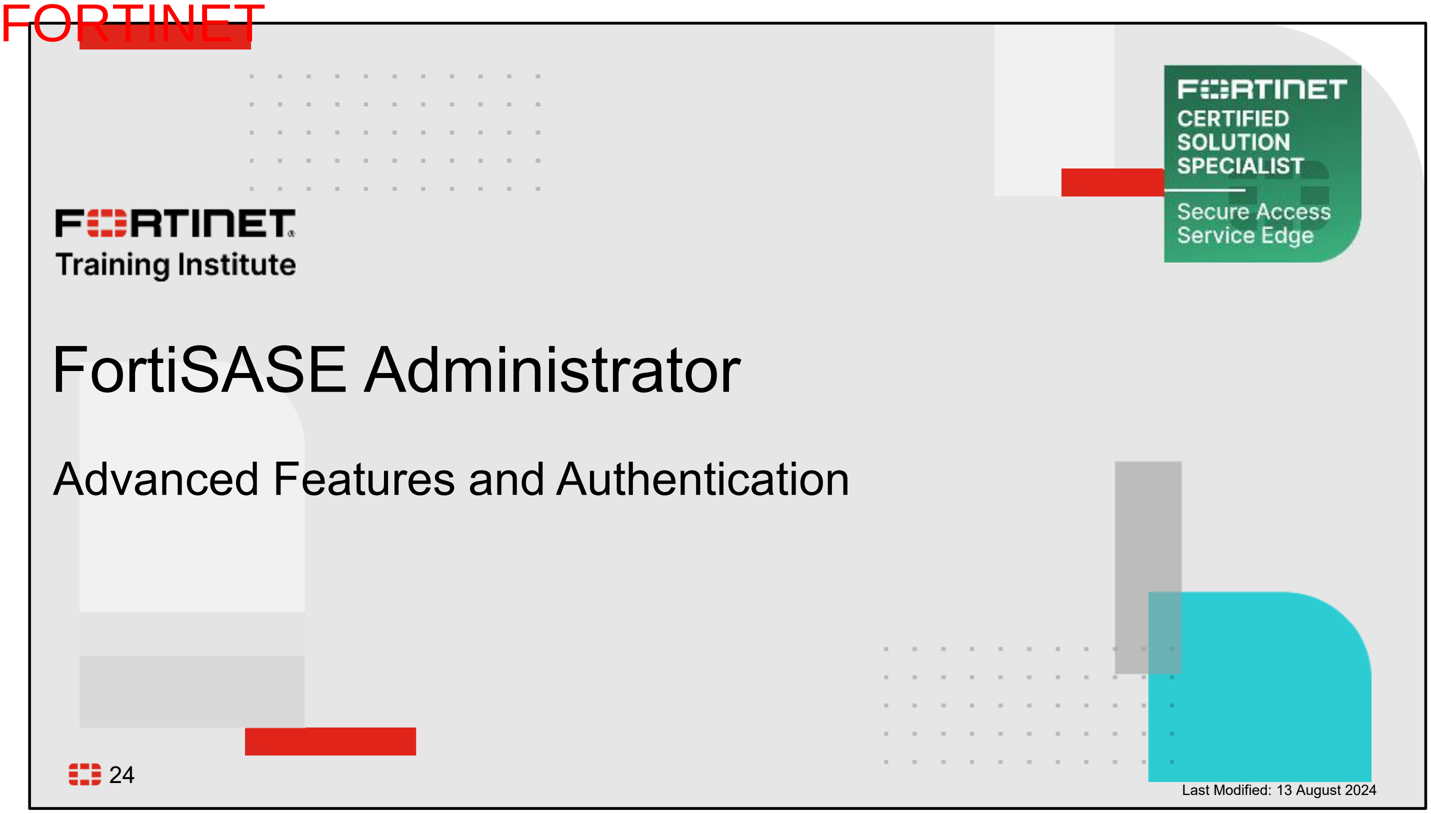
This slide shows the objectives that you covered in this lesson.

By mastering the objectives covered in this lesson, you now know and understand the standard VPN architecture, SASE architecture, SASE components, and the Fortinet SASE solution. You also learned how to provision FortiSASE and the different license types.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET

Brave-dumps.com



FORTINET
Training Institute

FortiSASE Administrator

Advanced Features and Authentication

FORTINET
CERTIFIED
SOLUTION
SPECIALIST
Secure Access
Service Edge

24

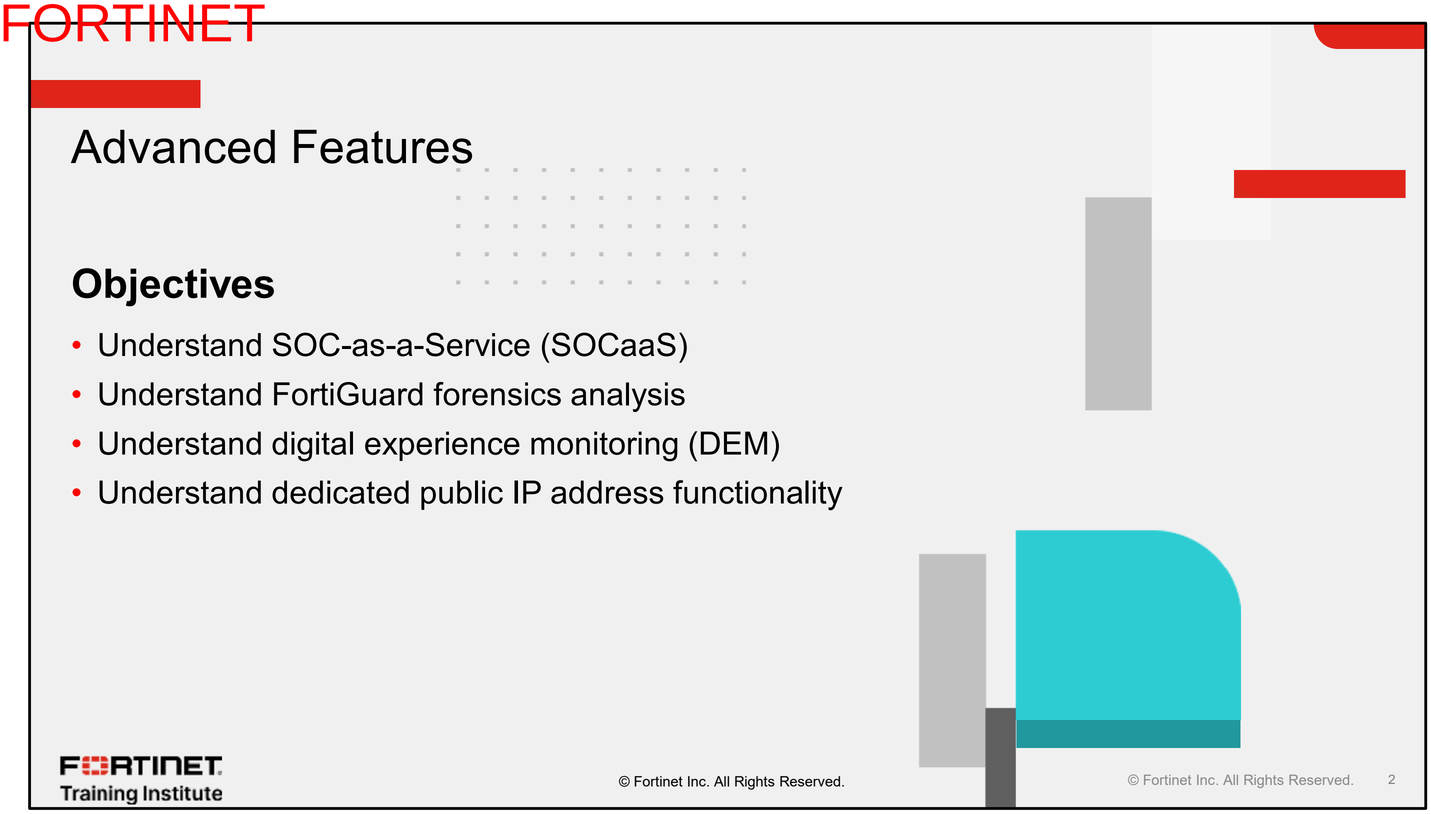
Last Modified: 13 August 2024

In this lesson, you will learn about the advanced features and user authentication on FortiSASE.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET

Brave-dumps.com



Advanced Features

Objectives

- Understand SOC-as-a-Service (SOCaaS)
- Understand FortiGuard forensics analysis
- Understand digital experience monitoring (DEM)
- Understand dedicated public IP address functionality

Training Institute

© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved. 2

After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in understanding advanced features, you will understand when to use the advanced features on FortiSASE.

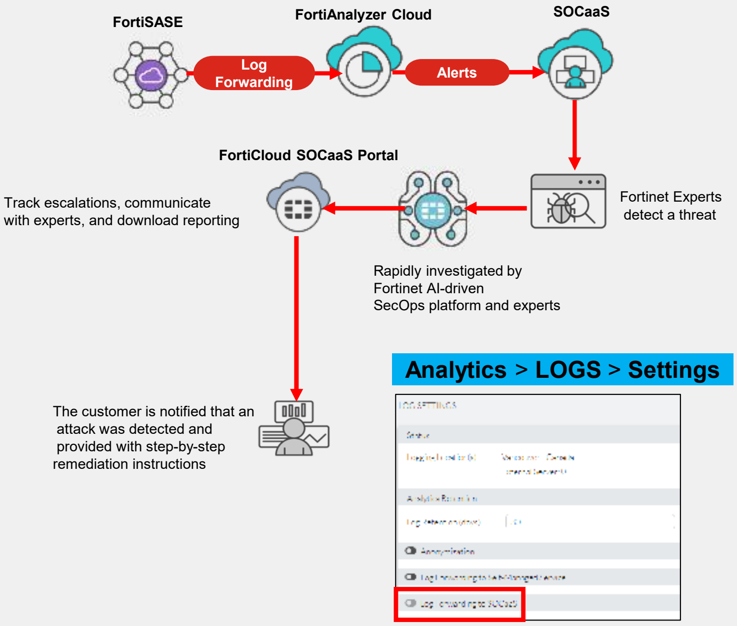
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET

Brave-dumps.com

FortiSASE Integration With SOCaaS

- Included with advanced and comprehensive license
- 24x7x365 monitoring services enabled through global SOC locations
- Powered by FortiGuard threat intelligence and SOAR platform
- Investigations and incident triage led by dedicated Fortinet security experts
- To enable this service on the FortiSASE portal, click **Analytics** > **LOGS** > **Settings**


FortiSASE
FortiAnalyzer Cloud
SOCaaS
Log Forwarding
Alerts
Fortinet Experts detect a threat
FortiCloud SOCaaS Portal
Rapidly investigated by Fortinet AI-driven SecOps platform and experts
Track escalations, communicate with experts, and download reporting
The customer is notified that an attack was detected and provided with step-by-step remediation instructions

Analytics > LOGS > Settings

LOG SETTINGS

Status

Logging Location(s) Vendor ... Console
External Server(s)

Analytics Retention

Log Retention (days)

Anonymization

Log Forwarding to Self-Managed Service

Log Forwarding to SOCaaS

© Fortinet Inc. All Rights Reserved. 3

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

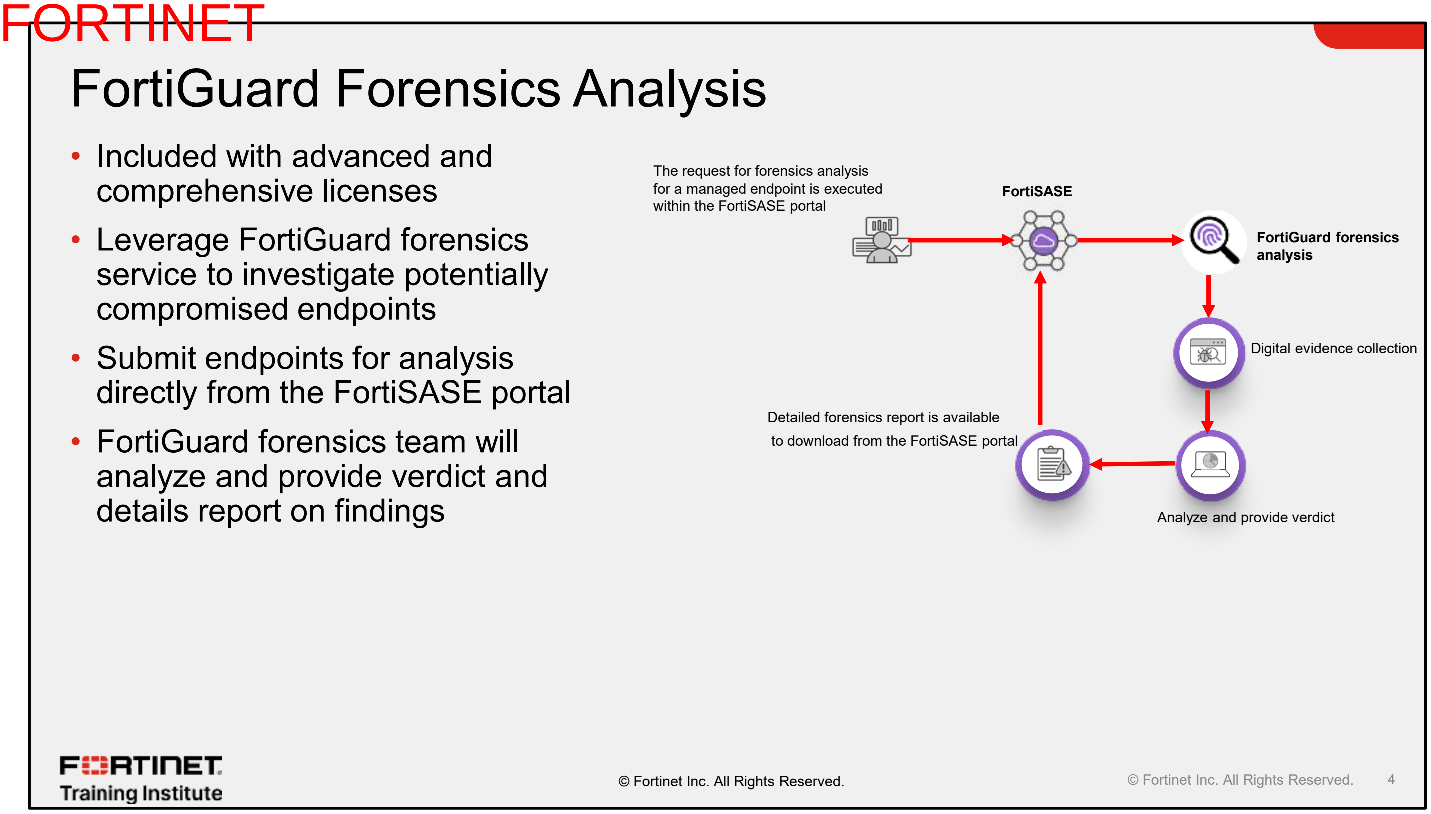
Fortinet SOCaaS is a cloud-based managed security and 24x7x365 monitoring service. The global team of Fortinet experts provides round-the-clock monitoring of your FortiGate and FortiSASE environments, offering vigilance beyond standard business hours. Fortinet leverages artificial intelligence, machine language, and human analysis to sift through alerts, distinguishing real threats from false positives. Upon detecting a threat, the Fortinet SOC team quickly notifies the customer, ensuring rapid response to minimize attacker dwell times. The SOC team guides the customer through resolving these threats, working in real time.

SOCaaS is included with a FortiSASE advanced and comprehensive license. Integrating FortiSASE with SOCaaS helps IT and security teams ensure consistent security monitoring for on-premises and remote users. This integration allows for log forwarding to the SOCaaS portal, enabling effective monitoring and rapid response to detected network anomalies, therefore elevating network defense capabilities. You can enable this service on the FortiSASE portal. The cloud-based SOCaaS portal includes intuitive dashboards, on-demand reports, and quarterly Fortinet expert meetings.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET

Brave-dumps.com



FortiGuard Forensics Analysis

- Included with advanced and comprehensive licenses
- Leverage FortiGuard forensics service to investigate potentially compromised endpoints
- Submit endpoints for analysis directly from the FortiSASE portal
- FortiGuard forensics team will analyze and provide verdict and details report on findings

The request for forensics analysis for a managed endpoint is executed within the FortiSASE portal

FortiSASE

FortiGuard forensics analysis

Digital evidence collection

Analyze and provide verdict

Detailed forensics report is available to download from the FortiSASE portal

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

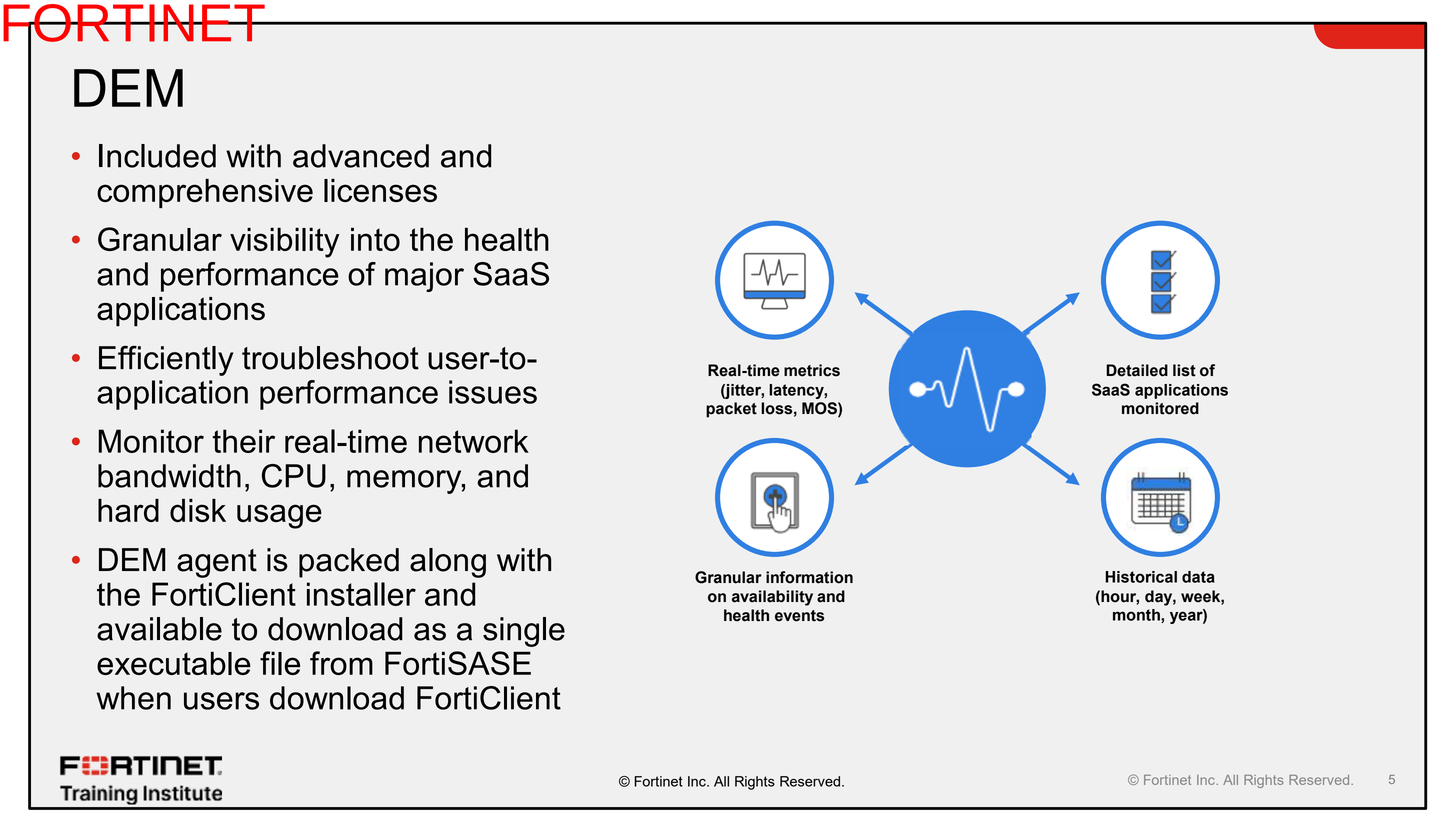
© Fortinet Inc. All Rights Reserved. 4

Like SOCaaS, FortiGuard forensics analysis is included with FortiSASE advanced and comprehensive licenses. The FortiGuard forensics services helps customers identify and mitigate potential risks to their network. The FortiGuard forensics analysis helps endpoint customers respond to and recover from cyber incidents. For each engagement, FortiGuard forensics analysts remotely assists customer in the collection, examination, and presentation of digital evidence, including a final detailed report. A FortiSASE administrator can request a detailed analysis of the endpoint from the FortiGuard forensics team, if they observe a high-risk applications, malware, intrusion attempts, and so on, on that endpoint. FortiSASE subscriptions that include the forensics service, entitle customers to reach out to the forensics experts whenever an event happens. By doing so, they offload the issue from their internal teams, and accelerate the investigation by handing it off to analysts who are deeply familiar with the tools of endpoint security.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET

Brave-dumps.com



DEM

- Included with advanced and comprehensive licenses
- Granular visibility into the health and performance of major SaaS applications
- Efficiently troubleshoot user-to-application performance issues
- Monitor their real-time network bandwidth, CPU, memory, and hard disk usage
- DEM agent is packed along with the FortiClient installer and available to download as a single executable file from FortiSASE when users download FortiClient

Real-time metrics (jitter, latency, packet loss, MOS)

Detailed list of SaaS applications monitored

Granular information on availability and health events

Historical data (hour, day, week, month, year)

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

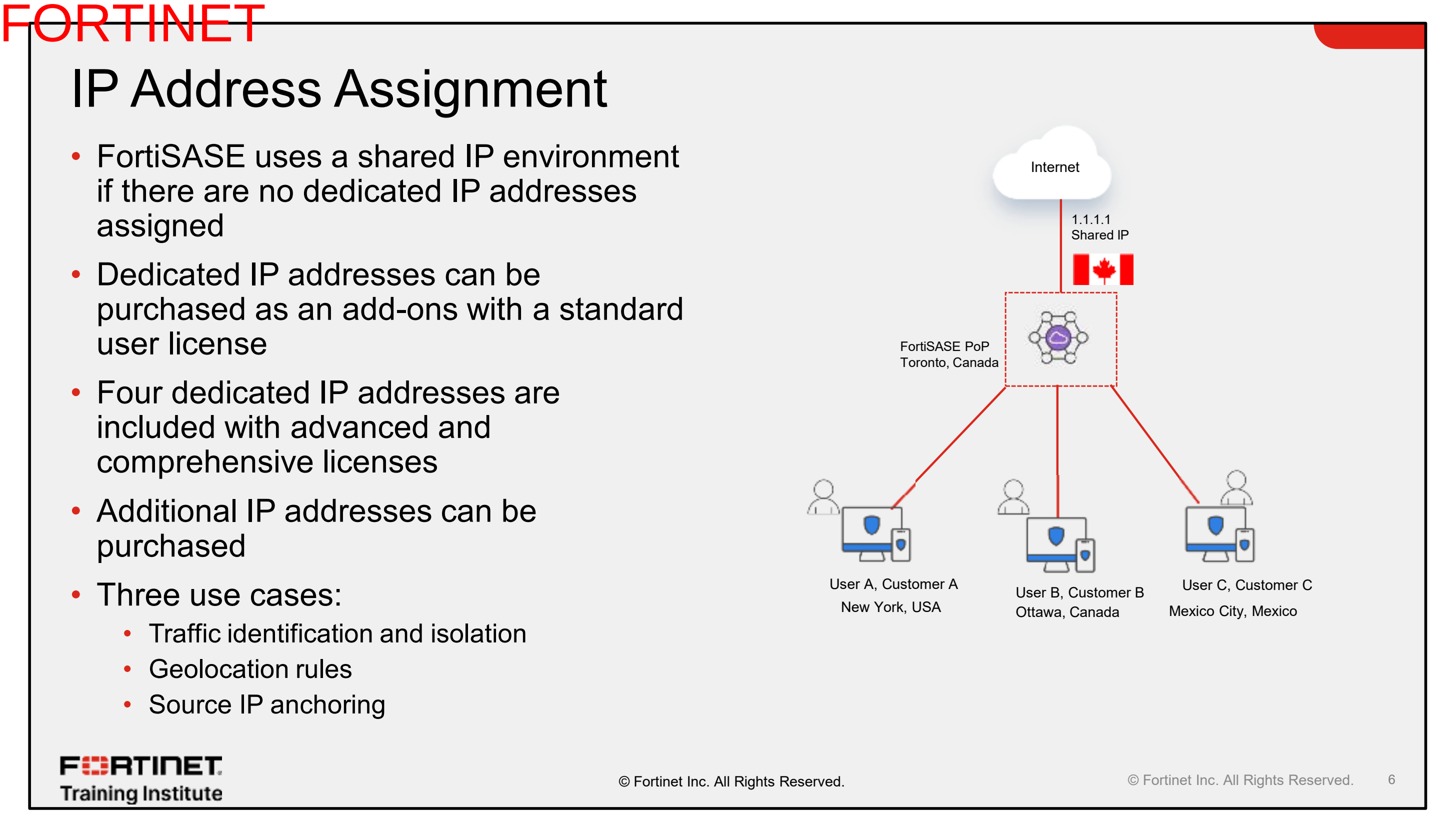
© Fortinet Inc. All Rights Reserved. 5

Remote work presents a challenge when employees are spread out across a large area, use different ISPs, and have different needs. Getting visibility from monitoring nodes located where employees or customers are physically located makes it easier to maintain service delivery for those workers. DEM serves as a valuable tool for network administrators in diagnosing connectivity and network issues for remote users, along with monitoring their real-time network bandwidth, CPU, memory, and hard disk usage. DEM offers quality and experience monitoring between the FortiClient endpoint, FortiSASE POP, and Software-as-a-Service (SaaS) application by tracing end-to-end network performance. DEM functionality is included with FortiSASE advanced and comprehensive user licenses. The DEM agent is packaged along with the FortiClient installer and available to download as a single executable file from FortiSASE when users download. You will learn to run a trace job on an endpoint in a later lesson.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET

Brave-dumps.com



IP Address Assignment

- FortiSASE uses a shared IP environment if there are no dedicated IP addresses assigned
- Dedicated IP addresses can be purchased as an add-ons with a standard user license
- Four dedicated IP addresses are included with advanced and comprehensive licenses
- Additional IP addresses can be purchased
- Three use cases:
  - Traffic identification and isolation
  - Geolocation rules
  - Source IP anchoring

© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved. 6

FortiSASE with a standard user license uses a shared IP environment, meaning remote users from different customers connected to a specific POP use the same public IP address for outgoing traffic. This prevents the identification and isolation of each customer's traffic. Customers can purchase dedicated IP addresses as an add-ons with a standard user license. There are four dedicated IP addresses included with an advanced and comprehensive licenses.

Three common use cases for dedicated public IP address deployments are:

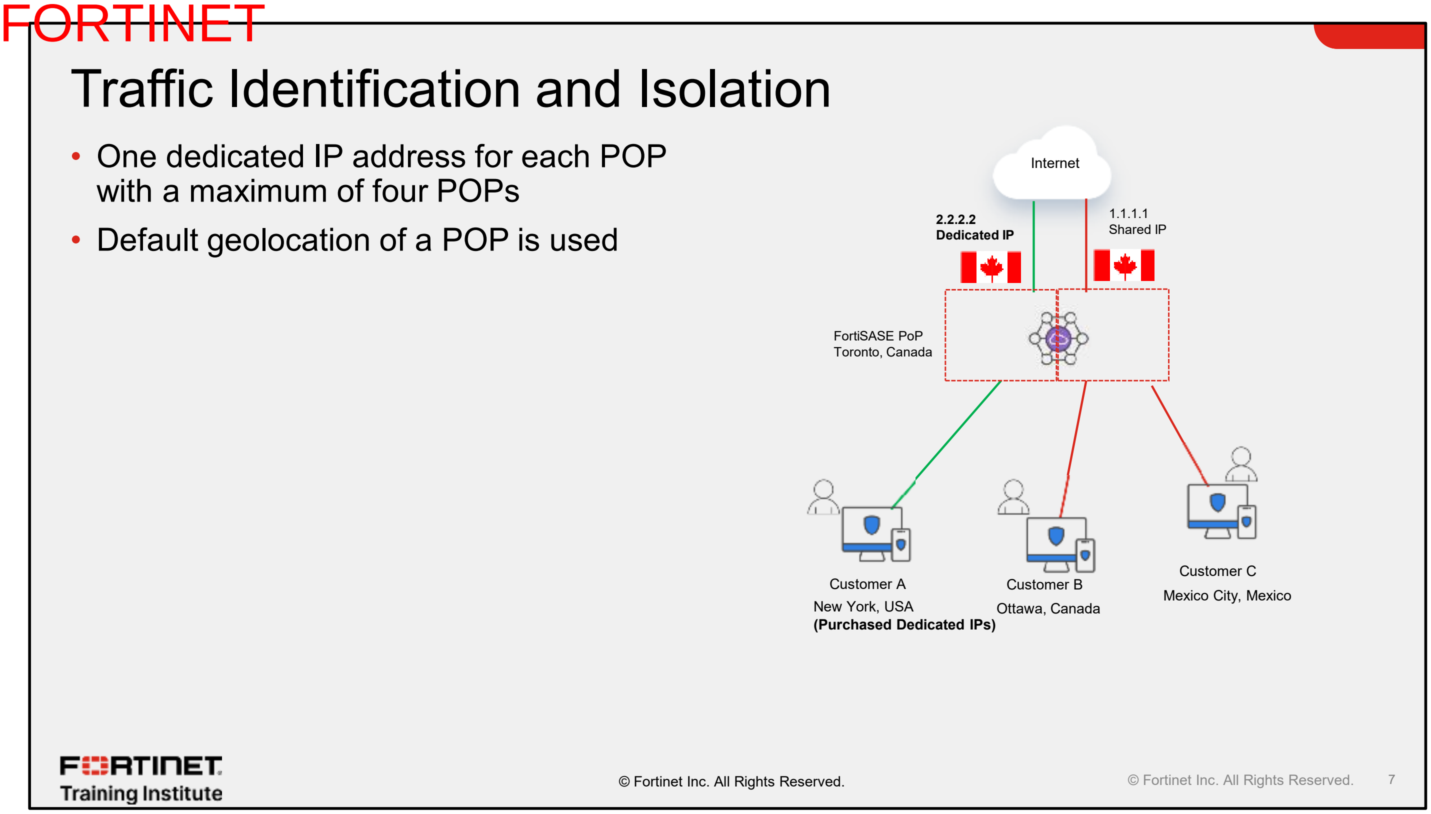
- Traffic identification and isolation
- Geolocation rules
- Source IP anchoring

You must open a support ticket to implement geolocation rules and source IP anchoring use cases. This slide shows an example of a shared IP environment, where remote users from different customers are connected to the same POP location. All of them use the same public IP address to connect to the internet.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET

Brave-dumps.com



Traffic Identification and Isolation

- One dedicated IP address for each POP with a maximum of four POPs
- Default geolocation of a POP is used

Training Institute

© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved. 7

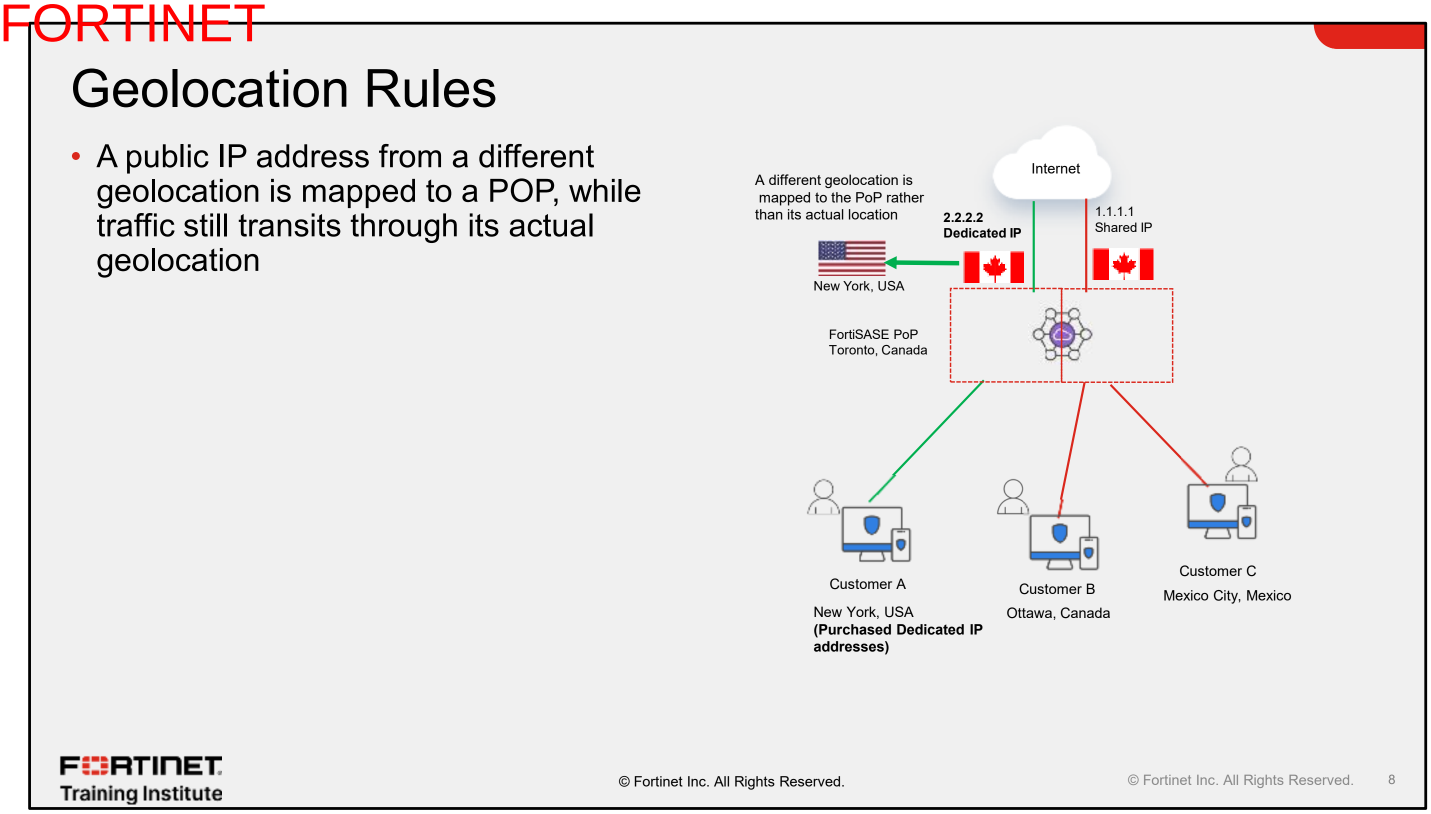
If the customer has purchased an add-on license or has dedicated IP addresses as part of their license, they are entitled to one dedicated IP address per POP, with a maximum of four POPs. The public IP address will be registered to the default geolocation of the POP.

In the example shown on this slide, users of customers A, B, and C are connected to the same FortiSASE POP location. Customer A has a dedicated IP address in their FortiSASE user license. Customer A will get a dedicated public IP address for their user traffic, allowing for traffic isolation and identification.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET

Brave-dumps.com



Geolocation Rules

- A public IP address from a different geolocation is mapped to a POP, while traffic still transits through its actual geolocation

A different geolocation is mapped to the PoP rather than its actual location

Internet

2.2.2.2
Dedicated IP

1.1.1.1
Shared IP

New York, USA

FortiSASE PoP
Toronto, Canada

Customer A

New York, USA
(Purchased Dedicated IP addresses)

Customer B

Ottawa, Canada

Customer C

Mexico City, Mexico

© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved. 8

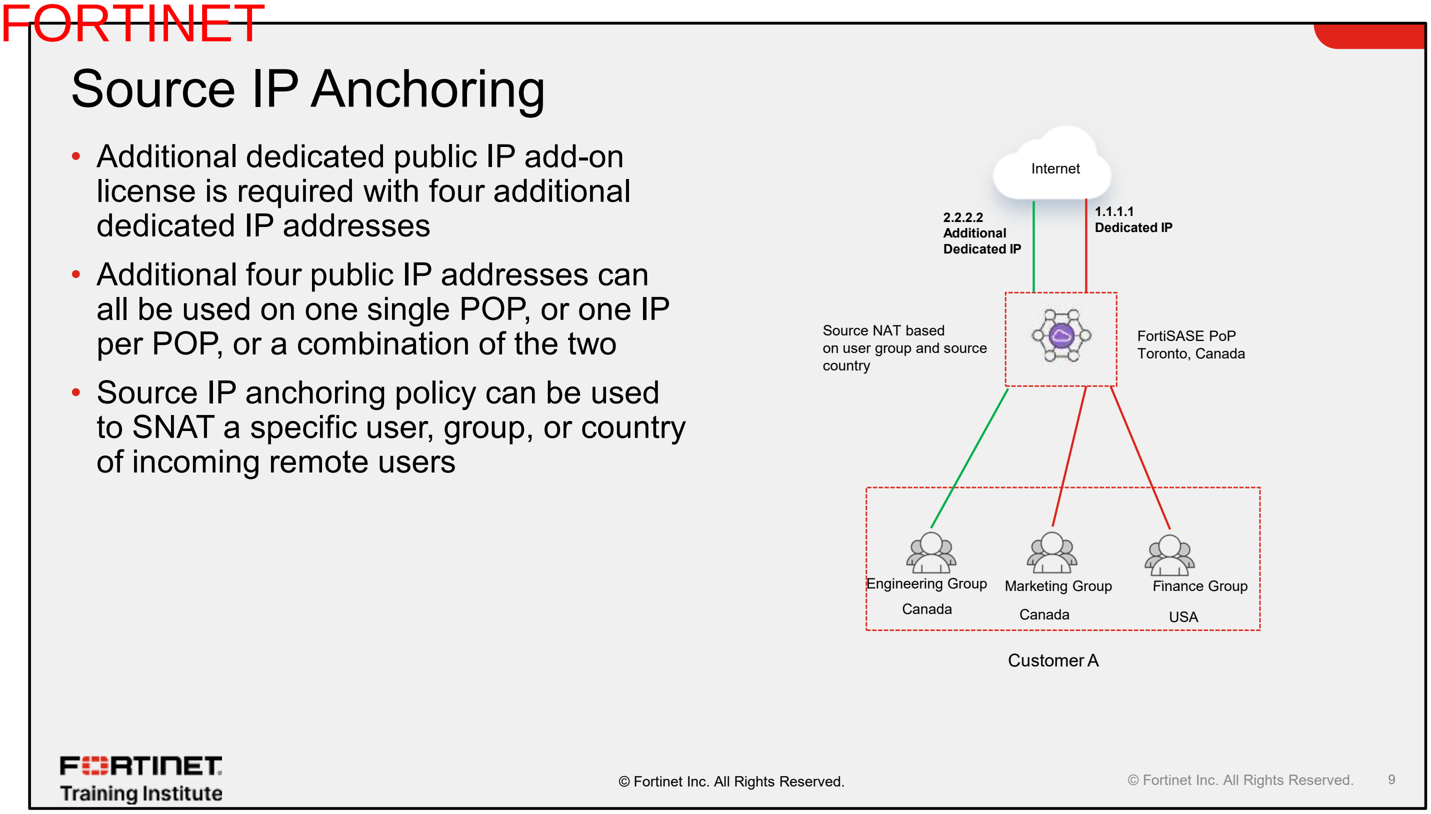
In the geolocation rules use case, the customer can request the dedicated public IP address of a POP to be mapped to a different geolocation, while traffic still transits through its actual geolocation.

In the example shown on this slide, customer A is connected to a POP in Toronto, Canada. The customer can request the dedicated public IP address of the POP to be mapped to New York, USA. This allows for users using a specific security POP to access content that is tailored to or restricted by users’ geolocation. Mapping to a different geolocation is considered the best effort because cloud services use different geolocation providers and not all are consistent.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET

Brave-dumps.com



Source IP Anchoring

- Additional dedicated public IP add-on license is required with four additional dedicated IP addresses
- Additional four public IP addresses can all be used on one single POP, or one IP per POP, or a combination of the two
- Source IP anchoring policy can be used to SNAT a specific user, group, or country of incoming remote users

FERTINET Training Institute

© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved. 9

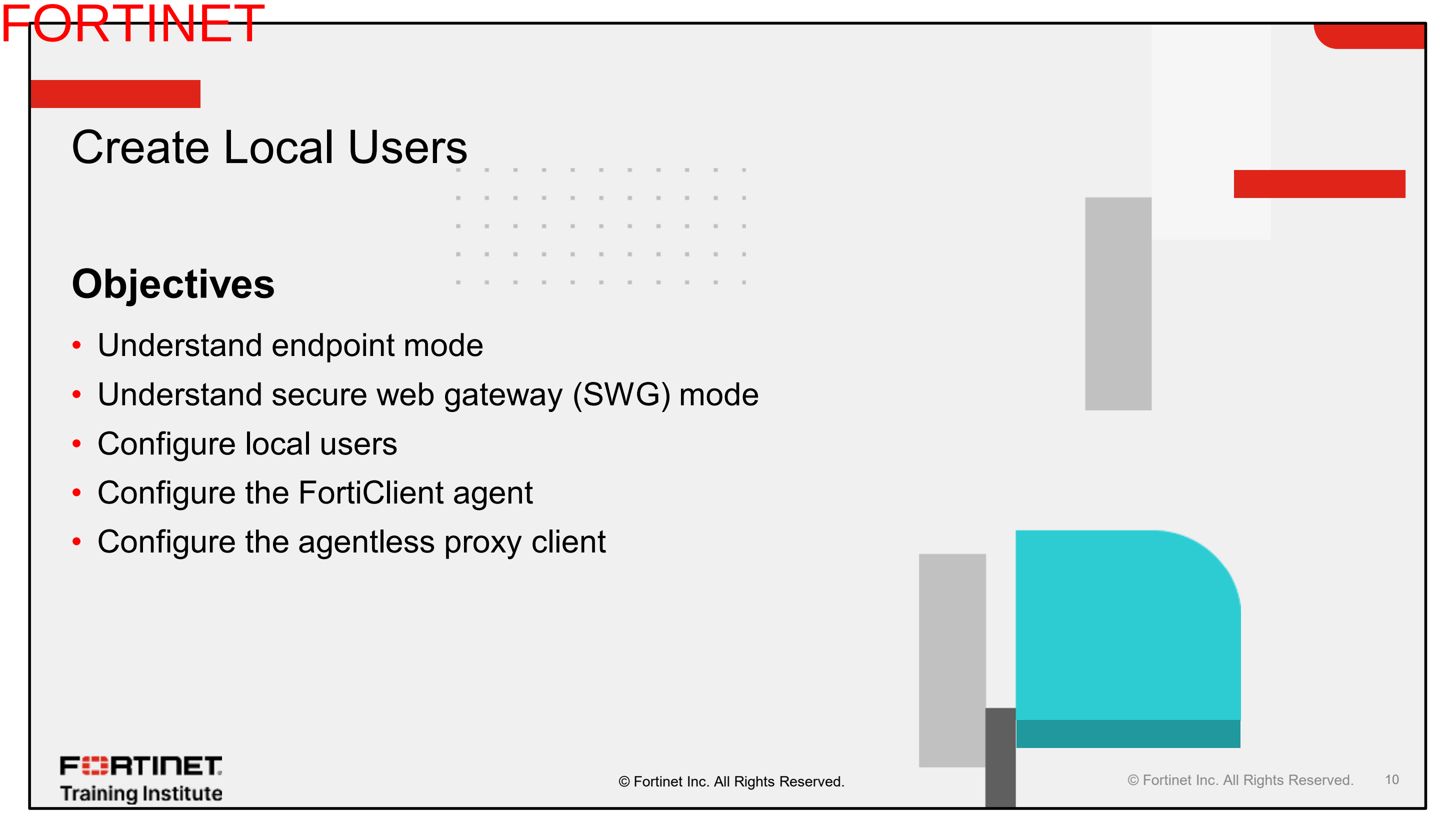
In the source IP anchoring use case, you will need an additional dedicated public IP add-on license with four additional dedicated IP addresses on top of the initial dedicated public IP address license. The additional four public IP addresses can all be used on one single POP, or one IP per POP, or a combination of the two. You can use source network address translation (SNAT) for a specific user, user group, or country of incoming remote users.

In the example shown on this slide, users are part of company A and part of different user groups. Traffic for the engineering group is source-anchored to a different dedicated IP address (`2.2.2.2`) based on the user group and source country, while the marketing group and finance group are using the same dedicated public IP address (`1.1.1.1`).

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET

Brave-dumps.com



Create Local Users

Objectives

- Understand endpoint mode
- Understand secure web gateway (SWG) mode
- Configure local users
- Configure the FortiClient agent
- Configure the agentless proxy client

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved. 10

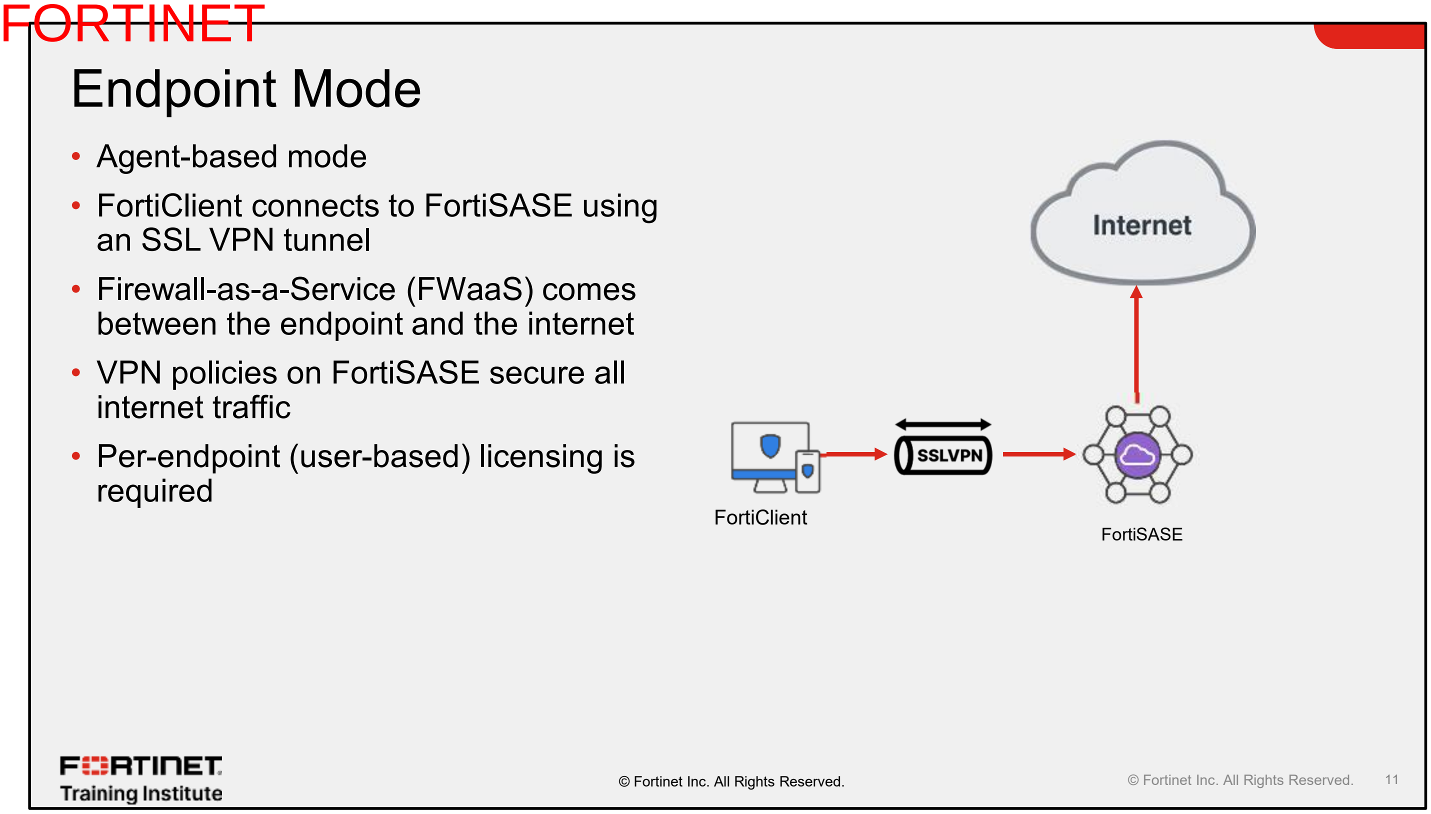
After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in understanding local authentication, you will be able to create and on board local users on FortiSASE.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET

Brave-dumps.com



Endpoint Mode

- Agent-based mode
- FortiClient connects to FortiSASE using an SSL VPN tunnel
- Firewall-as-a-Service (FWaaS) comes between the endpoint and the internet
- VPN policies on FortiSASE secure all internet traffic
- Per-endpoint (user-based) licensing is required

© Fortinet Inc. All Rights Reserved.

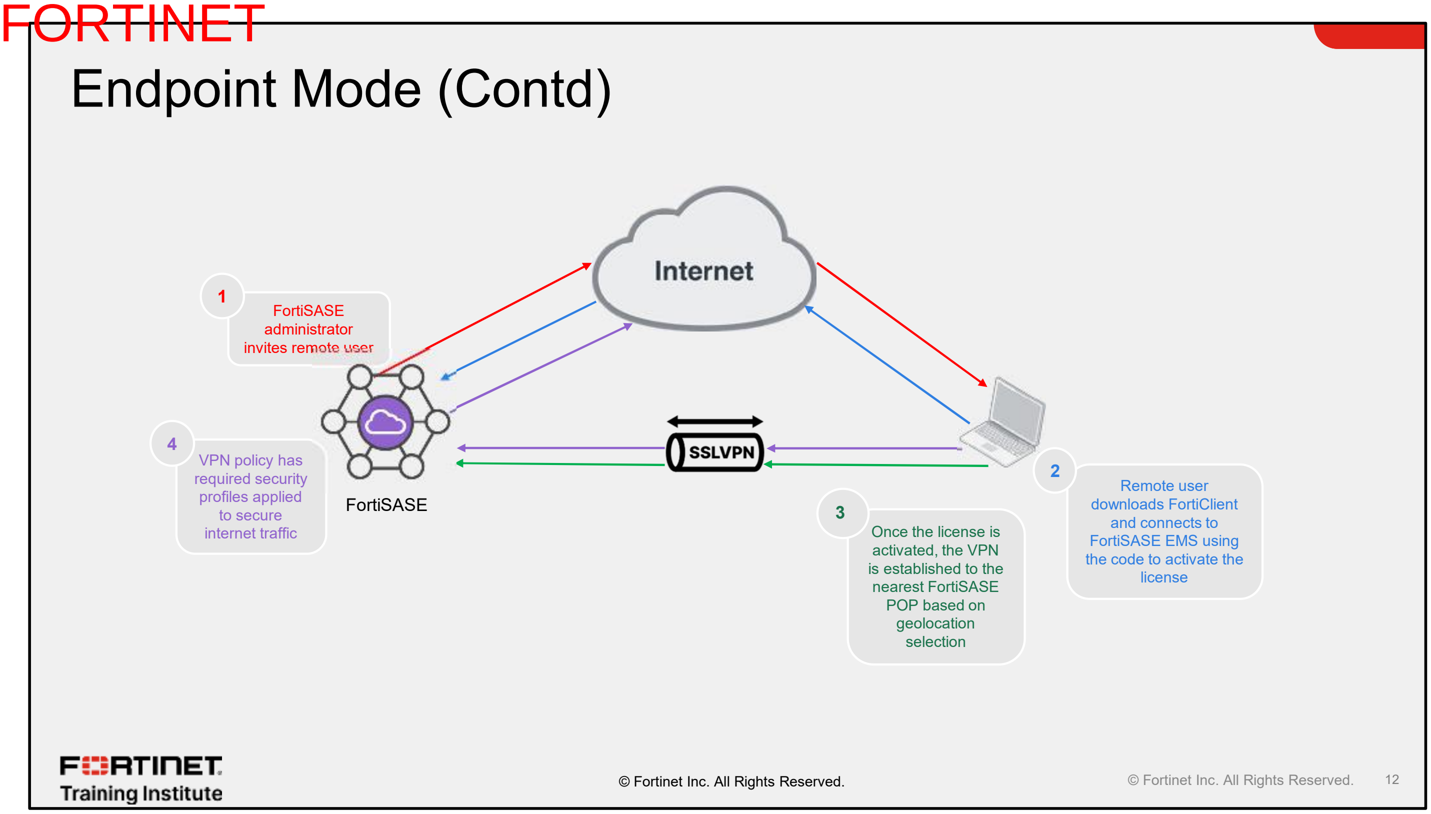
© Fortinet Inc. All Rights Reserved.

In endpoint mode, FortiClient connects to FortiSASE using a secure SSL VPN tunnel. Once the connection is established, FortiSASE acts as a firewall and is placed between the endpoint and the internet. The VPN policy on FortiSASE is configured with the required security components, such as web filter, application control, and so on, to secure the internet traffic. Endpoint mode also supports configuring zero trust network access (ZTNA) for compliance checks.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET

Brave-dumps.com



Endpoint Mode (Contd)

1 FortiSASE administrator invites remote user

2 Remote user downloads FortiClient and connects to FortiSASE EMS using the code to activate the license

3 Once the license is activated, the VPN is established to the nearest FortiSASE POP based on geolocation selection

4 VPN policy has required security profiles applied to secure internet traffic

© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved. 12

This slide shows the flow of events that occurs during endpoint mode manual activation.

1. The FortiSASE administrator sends an invitation email to the remote user, as part of user onboarding.
2. The end user downloads FortiClient and connects to the FortiSASE Endpoint Management System (EMS) to activate the license, using the code in the email.
3. Once the license is activated, a secure SSL VPN is established from FortiClient to the nearest FortiSASE POP, based on geolocation selection.
4. The FortiSASE administrator can apply security profiles on the VPN policies to secure internet traffic.

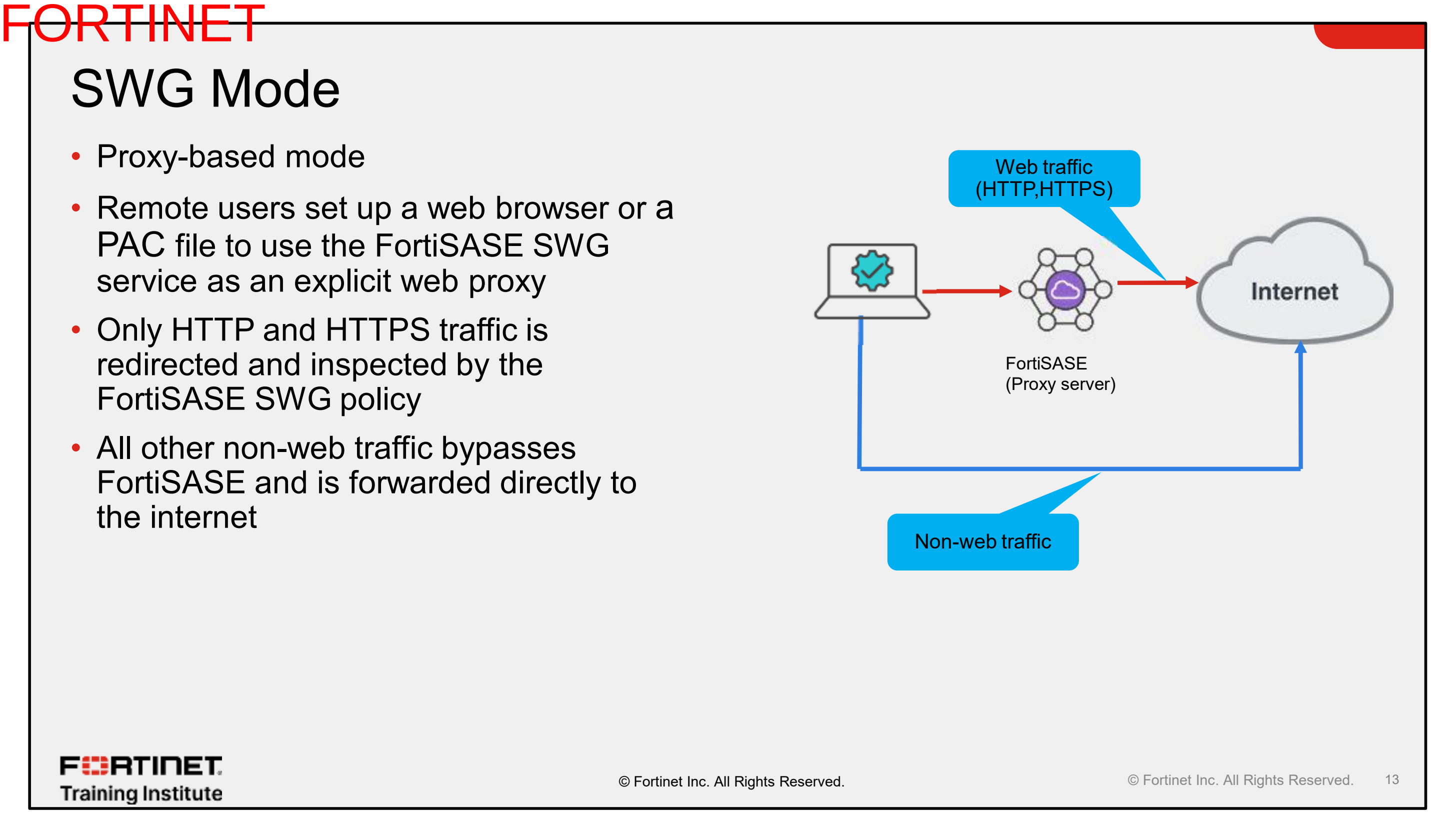
You can also provision using FortiClient installers that you can download from the FortiSASE portal. Click **Configuration**, and then, in the **ACCESS** section, click **Users** > **Onboard Users** > **Download Installer**. You can then provision your endpoints by doing one of the following:

- Use a mobile device management (MDM) software suite using this installer.
- Distribute this installer to end users and have them install it on their endpoints.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET

Brave-dumps.com



SWG Mode

- Proxy-based mode
- Remote users set up a web browser or a PAC file to use the FortiSASE SWG service as an explicit web proxy
- Only HTTP and HTTPS traffic is redirected and inspected by the FortiSASE SWG policy
- All other non-web traffic bypasses FortiSASE and is forwarded directly to the internet

© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved. 13

Secure web gateway mode is an agentless deployment for remote users. Remote users configure FortiSASE as an explicit web proxy through their web browser or by using a proxy autoconfiguration (PAC) file. IT administrators can push a PAC file to the end user by using a group policy object (GPO). FortiSASE supports a Google Chrome extension that allows you to enforce SWG connectivity for selected endpoints with the Google Chrome browser installed, including Chromebooks, based on the endpoint OS and the corresponding extension policy that the Google Workspace administrator configured. The web browser redirects HTTP and HTTPS traffic to FortiSASE, which secures user web traffic by implementing SWG security policies. All other non-web traffic bypasses FortiSASE and is forwarded directly to the internet.

Vouchers & Dumps are Available | WhatsApp +201224560923

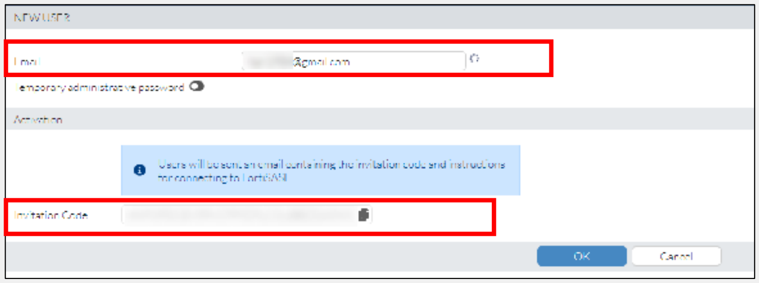
DO NOT REPRINT
© FORTINET

Brave-dumps.com

Configuring Local Users

- User authenticates with FortiSASE directly
- FortiSASE sends instructions and invitation code to the configured email address
- User uses this invitation code to connect FortiClient to FortiSASE
- FortiSASE can import users from a CSV file

Configuration > ACCESS > Users & Groups



NEW USER

Email [redacted]@gmail.com

Temporary administrative password

Activation

Users will be sent an email containing the invitation code and instructions for connecting to FortiSASE

Invitation Code [redacted]

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved. 14

You can configure local users on FortiSASE. These users will directly authenticate with FortiSASE. To do this, click **Configuration** and then, in the **ACCESS** section, click **Users & Groups**.

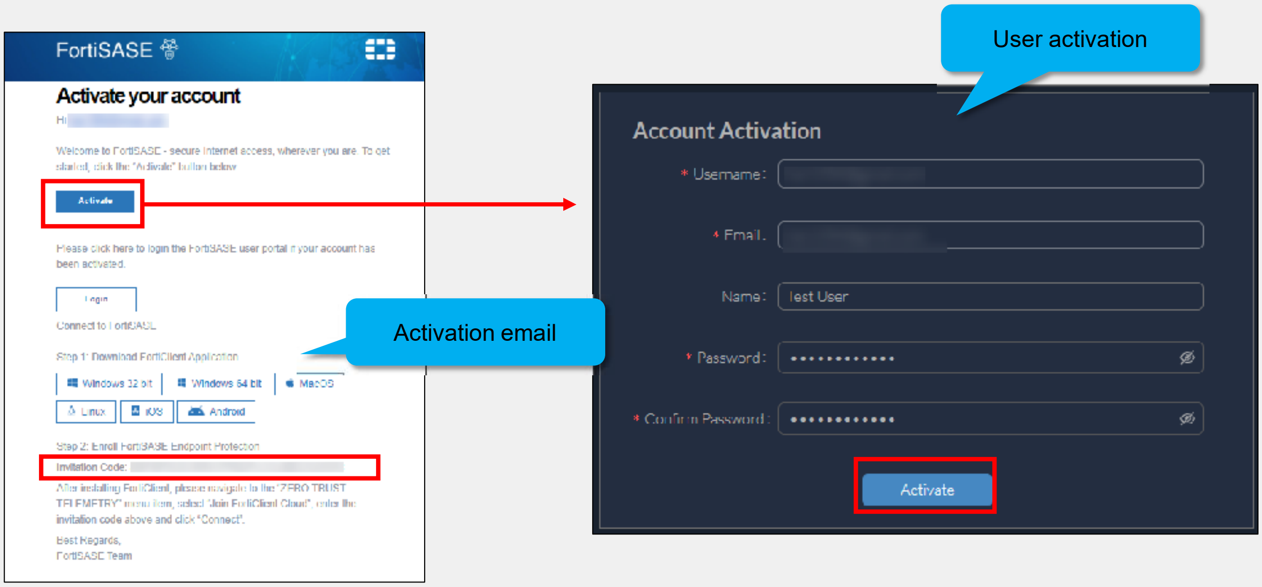
First, type an email address for FortiClient to send the invitation code to. The email address is also the username. The user uses the invitation code to connect FortiClient to FortiSASE. FortiSASE can also import users in bulk from a CSV file. Click **Configuration**, and then in the **ACCESS** section, click **Users** > **Import/Export** > **Import Users**.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET

Brave-dumps.com

Configuring Local Users (Contd)



FortiSASE

Activate your account

Hi [redacted]

Welcome to FortiSASE - secure Internet access, wherever you are. To get started, click the "Activate" button below

Please click here to login the FortiSASE user portal if your account has been activated.

Connect to FortiSASE

Step 1: Download FortiClient Application

Step 2: Enroll FortiSASE Endpoint Protection

Invitation Code: [redacted]

After installing FortiClient, please navigate to the "ZERO TRUST TELEMETRY" menu item, select "Join FortiClient Cloud", enter the invitation code above and click "Connect".

Best Regards,
FortiSASE Team

Account Activation

* Username: [redacted]

* Email: [redacted]

Name: Test User

* Password: ••••••••••••

* Confirm Password: ••••••••••••

© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved. 15

As part of onboarding, FortiSASE sends the user an email instructing the user to activate their account. The user clicks **Activate** and then sets a password.

The activation email also contains links to download FortiClient installers and an invitation code for FortiClient to connect to FortiSASE.

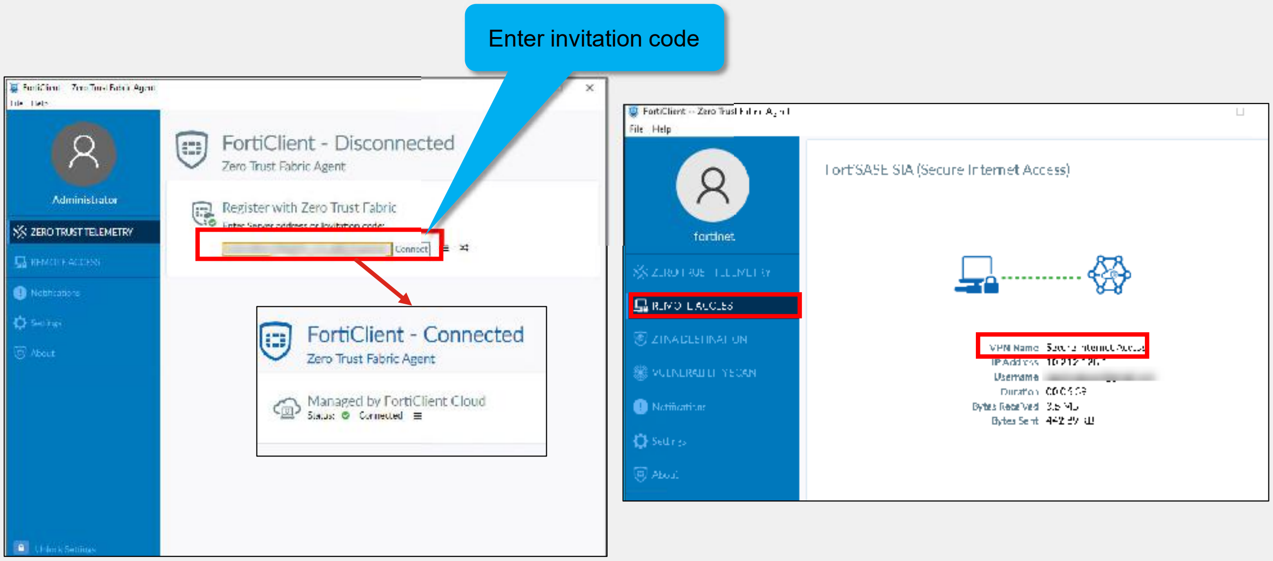
This slide shows an example of an activation email.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET

Brave-dumps.com

Agent Configuration



Enter invitation code

© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved.

To connect FortiClient to FortiSASE, the user types the invitation code from the activation email, in the **ZERO TRUST TELEMETRY**> **Register with Zero Trust Fabric** field, and click **Connect**.

After FortiClient has registered successfully, the **VPN Name** field displays **Secure Internet Access**. Now the FortiSASE EMS manages the endpoint.

The user can connect to the **Secure Internet Access** VPN tunnel by using the credentials set up during user activation or remote authentication, if configured. All user internet traffic is routed using FortiSASE VPN policies.

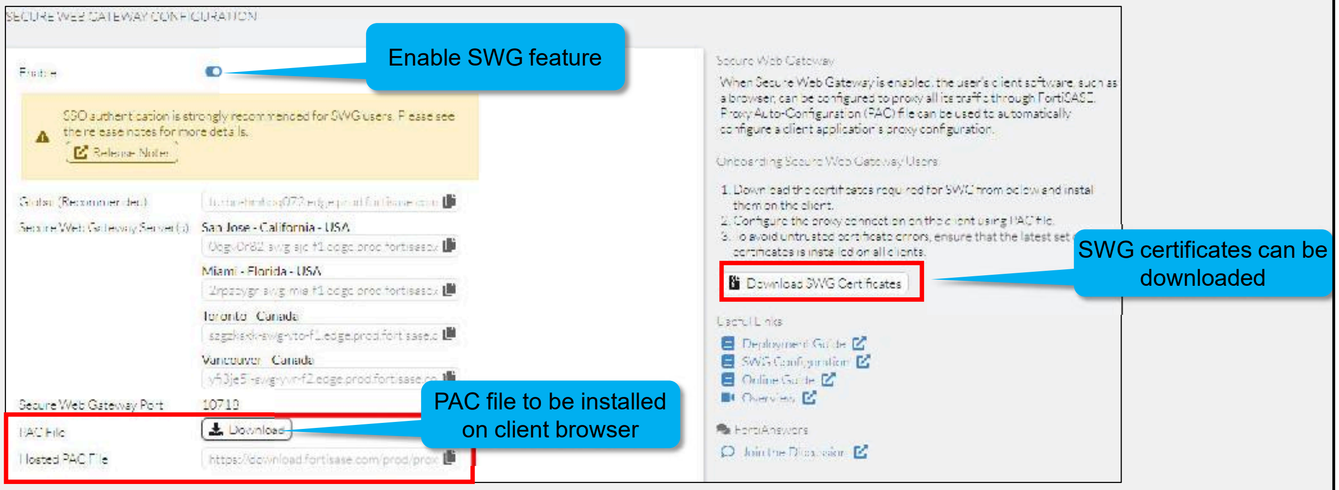
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET

Brave-dumps.com

Agentless Configuration

System > SWG Configuration



SECURE WEB GATEWAY CONFIGURATION

Enable ●

⚠ SSO authentication is strongly recommended for SWG users. Please see the release notes for more details.

Release Notes

Global (Recommended): fortiasehtdxq072.edge.prod.fortisase.com

Secure Web Gateway Server(s):

San Jose - California - USA: 0bgv0r82-swg-sjc-f1.edge.prod.fortisase.c

Miami - Florida - USA: 2rpzzygr-swg-mia-f1.edge.prod.fortisase.c

Toronto - Canada: szgzkexk-swg-yto-f1.edge.prod.fortisase.c

Vancouver - Canada: yh3je5-swg-yvr-f2.edge.prod.fortisase.co

Secure Web Gateway Port: 10710

PAC File: Download

Hosted PAC File: https://download.fortisase.com/prod/prox

Secure Web Gateway

When Secure Web Gateway is enabled, the user's client software, such as a browser, can be configured to proxy all its traffic through FortiSASE. Proxy Auto-Configuration (PAC) file can be used to automatically configure a client application's proxy configuration.

Onboarding Secure Web Gateway Users

1. Download the certificates required for SWG from below and install them on the client.
2. Configure the proxy connection on the client using PAC file.
3. To avoid untrusted certificate errors, ensure that the latest set of certificates is installed on all clients.

Download SWG Certificates

Enable SWG feature

SWG certificates can be downloaded

PAC file to be installed on client browser

© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved.

You can enable SWG on the **SWG Configuration** page.

When you enable SWG, users can configure their browser to proxy all HTTP and HTTPS web traffic for the FortiSASE SWG policies to inspect. While the web traffic is being proxied, FortiSASE replaces and signs the certificates of secure protocols like HTTPS.

You should provide users with the required certificate authority (CA) certificate and PAC file to connect to the FortiSASE gateway. You can download the SWG certificate and the PAC file from the **SWG Configuration** page.

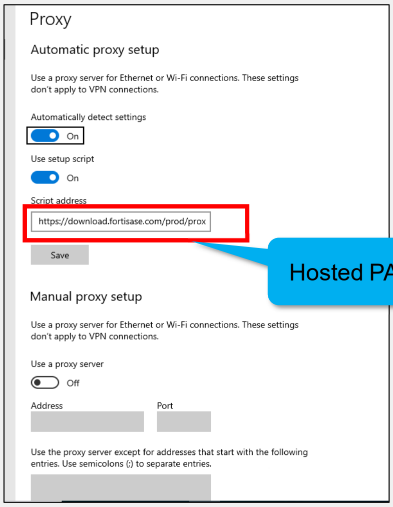
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET

Brave-dumps.com

Agentless Configuration (Contd)

Windows 10: Settings > System > Proxy Settings



Proxy

Automatic proxy setup

Use a proxy server for Ethernet or Wi-Fi connections. These settings don't apply to VPN connections.

Automatically detect settings

On

Use setup script

On

Script address

https://download.fortisase.com/prod/prox

Save

Manual proxy setup

Use a proxy server for Ethernet or Wi-Fi connections. These settings don't apply to VPN connections.

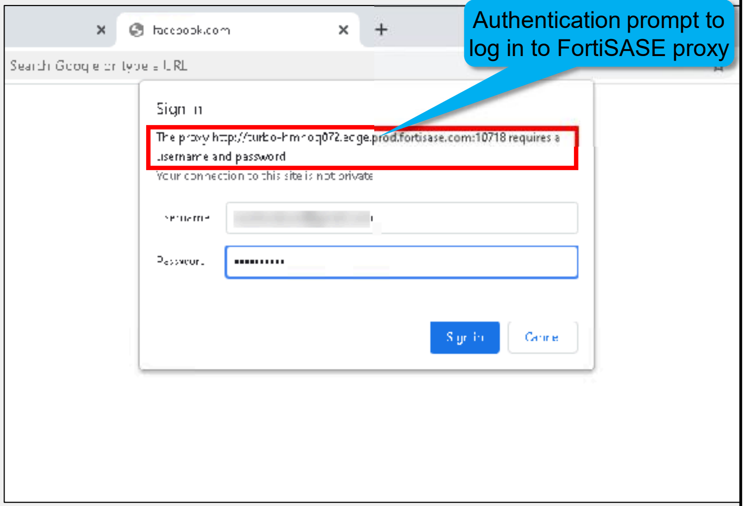
Use a proxy server

Off

Address Port

Use the proxy server except for addresses that start with the following entries. Use semicolons (;) to separate entries.

Hosted PAC file URL



facebook.com

Search Google or type a URL

Sign in

The proxy http://turbo-hmo-oq072.edge.prod.fortisase.com:10718 requires a username and password

Your connection to this site is not private

Username [redacted]

Password ••••••••••

Sign in Cancel

Authentication prompt to log in to FortiSASE proxy

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved. 18

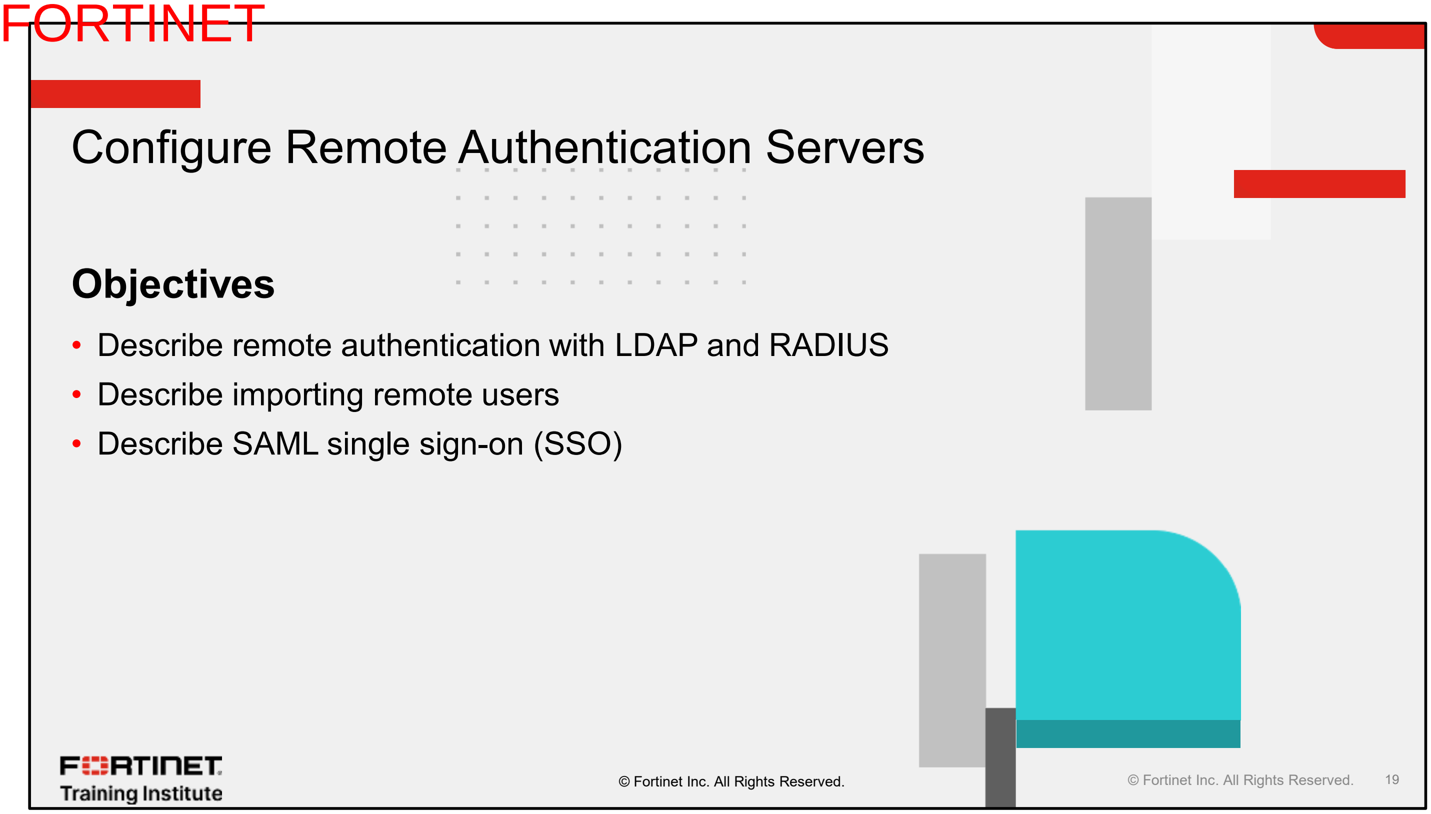
The user can configure the SWG settings at the OS level or in a browser by using a PAC file or by specifying the URL of the hosted PAC file, which is provided by FortiSASE.

When the user starts a new web browser session, they are prompted to log in. The user can log in using the credentials that they set up during activation or any remote authentication, if configured.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET

Brave-dumps.com



Configure Remote Authentication Servers

Objectives

- Describe remote authentication with LDAP and RADIUS
- Describe importing remote users
- Describe SAML single sign-on (SSO)

© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved.

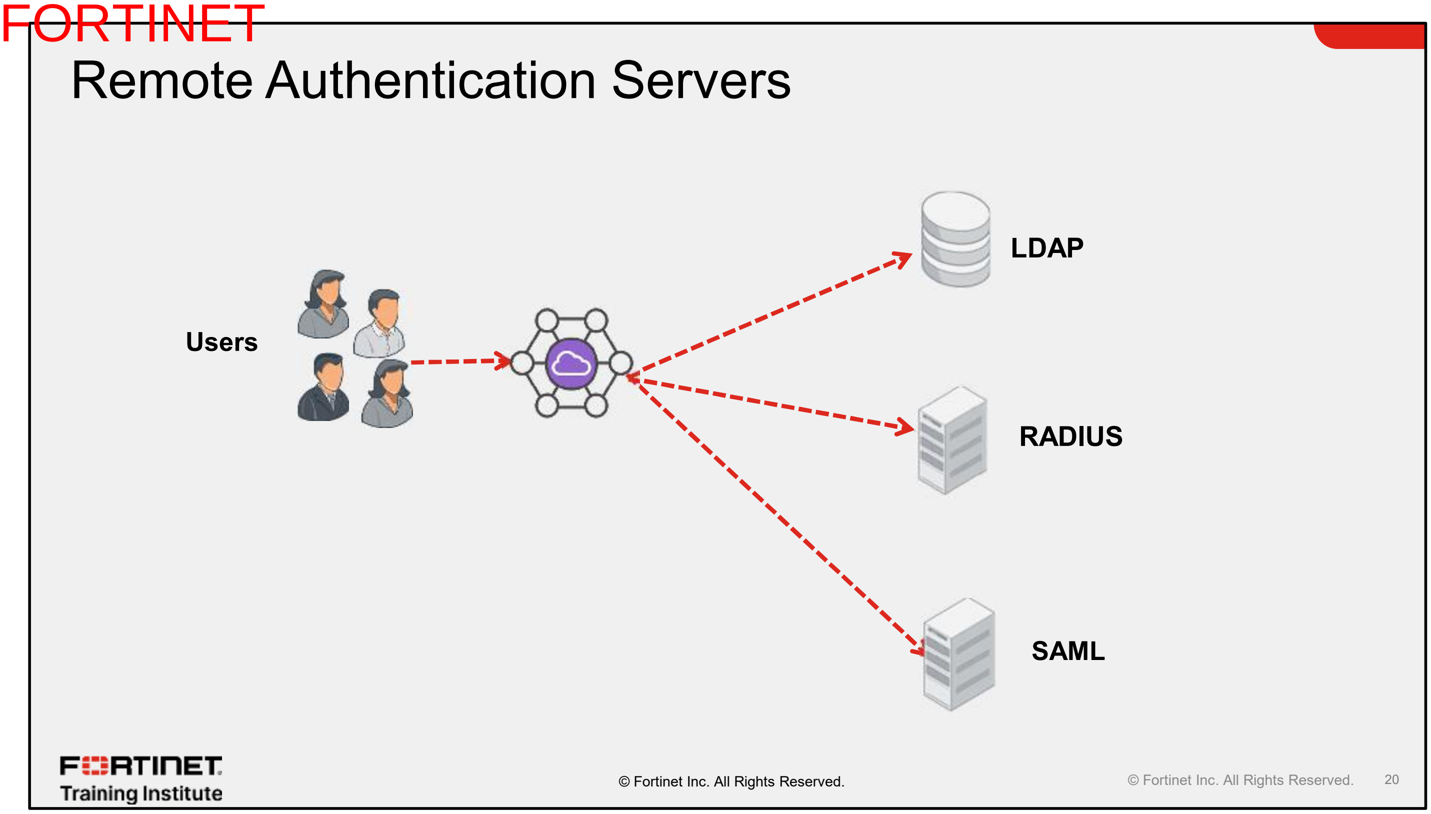
After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in understanding remote authentication, you will be able to configure LDAP, RADIUS, and SSO authentication on FortiSASE.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET

Brave-dumps.com



Remote Authentication Servers

Training Institute

© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved. 20

FortiSASE provides support for many remote authentication servers, including RADIUS, LDAP, and SAML for SSO.

Unlike local user accounts, where FortiSASE knows the credentials, remote authentication servers verify user credentials and provide group membership information to FortiSASE on demand.

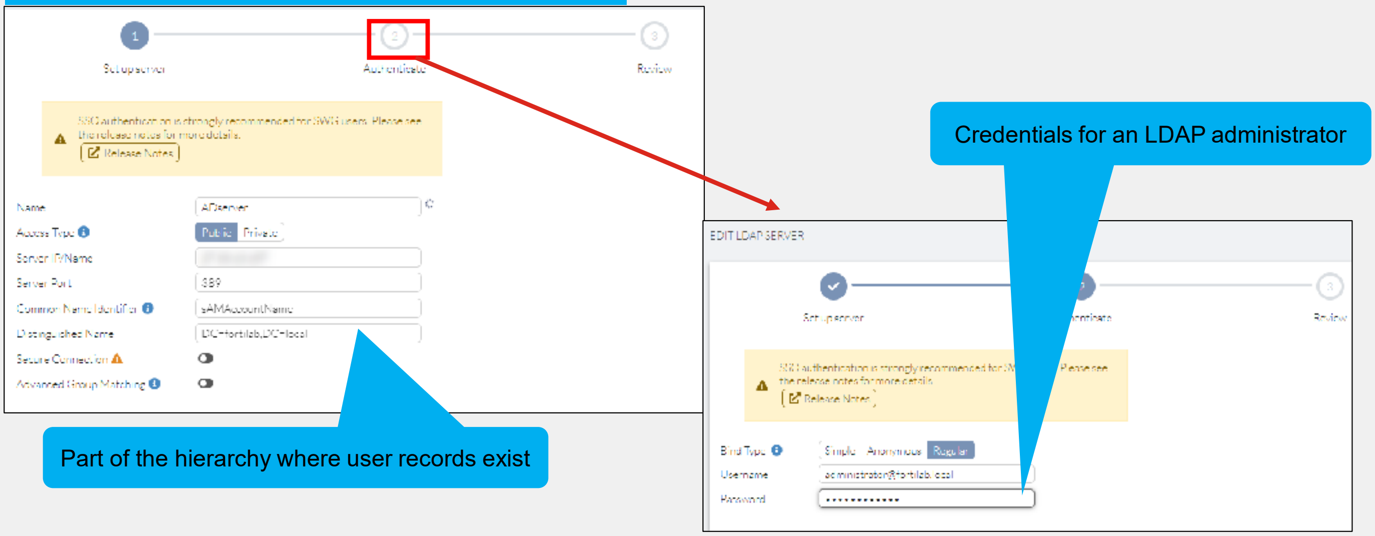
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET

Brave-dumps.com

Remote Authentication Servers—LDAP

Configuration > AUTHENTICATION SOURCES > LDAP



SSO authentication is strongly recommended for SWG users. Please see the release notes for more details.

Name: ADserver
Access Type: Public [✓] Private
Server IP/Name: [redacted]
Server Port: 389
Common Name Identifier: sAMAccountName
Distinguished Name: DC=fortilab,DC=local
Secure Connection: ○
Advanced Group Matching: ○

Part of the hierarchy where user records exist

EDIT LDAP SERVER

Bind Type: Simple Anonymous Regular [✓]
Username: administrator@fortilab.local
Password: ••••••••••••

Credentials for an LDAP administrator

You can configure FortiSASE to connect to a remote LDAP server on the **LDAP** page. You must enter all required information about the remote LDAP server, such as the IP address (or FQDN) as well as the connecting port.

The **Access Type** setting is how the LDAP server can be accessed from FortiSASE.

- **Public** means the LDAP server is directly accessible on the internet.
- **Private** means the LDAP server is accessible through secure private access.

The **Common Name Identifier** setting is the attribute name you use to find the username.

The **Distinguished Name** setting identifies the top of the tree where the users are located, which is generally the domain controller (DC) value; however, it can be a specific container or organizational unit (OU).

The **Bind Type** setting depends on the security settings of the LDAP server. When selecting a bind type, which determines how the authentication information is sent to the server, you can select:

- **Simple**, to bind using the user's password, which is sent to the server in plaintext without a search.
- **Regular**, to bind using the user's distinguished name (DN) and password and then perform a search. Regular bind is required, if searching for a user across multiple domains.
- **Anonymous**, to bind using an anonymous user and search starting from the DN and recurse over the subtrees. Many LDAP servers do not allow this by default.

If you want to have a secure connection between FortiSASE and the remote LDAP server, enable **Secure Connection** and include the LDAP over SSL (LDAPS), as well as any trusted CA certificates.

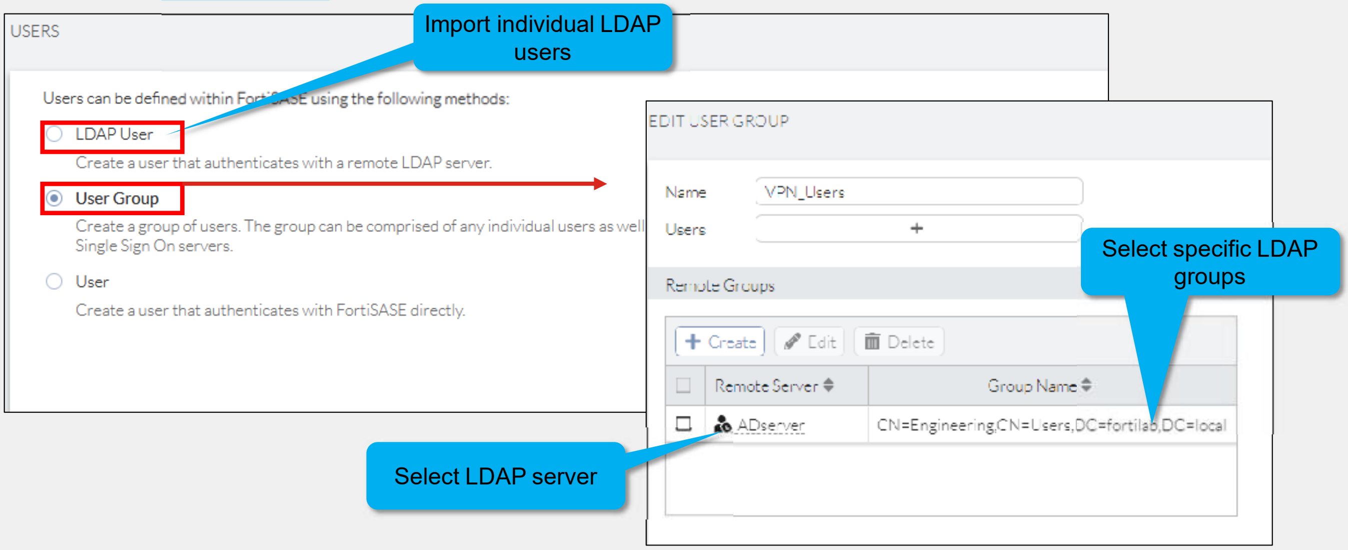
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET

Brave-dumps.com

Importing Remote LDAP Users

Configuration > ACCESS > Users



USERS

Users can be defined within FortiSASE using the following methods:

○ LDAP User
Create a user that authenticates with a remote LDAP server.

● User Group
Create a group of users. The group can be comprised of any individual users as well
Single Sign On servers.

○ User
Create a user that authenticates with FortiSASE directly.

EDIT USER GROUP

Name: VPN_Users

Users: +

Remote Groups

Remote Server	Group Name
ADserver	CN=Engineering,CN=Users,DC=fortilab,DC=local

Import individual LDAP users

Select specific LDAP groups

Select LDAP server

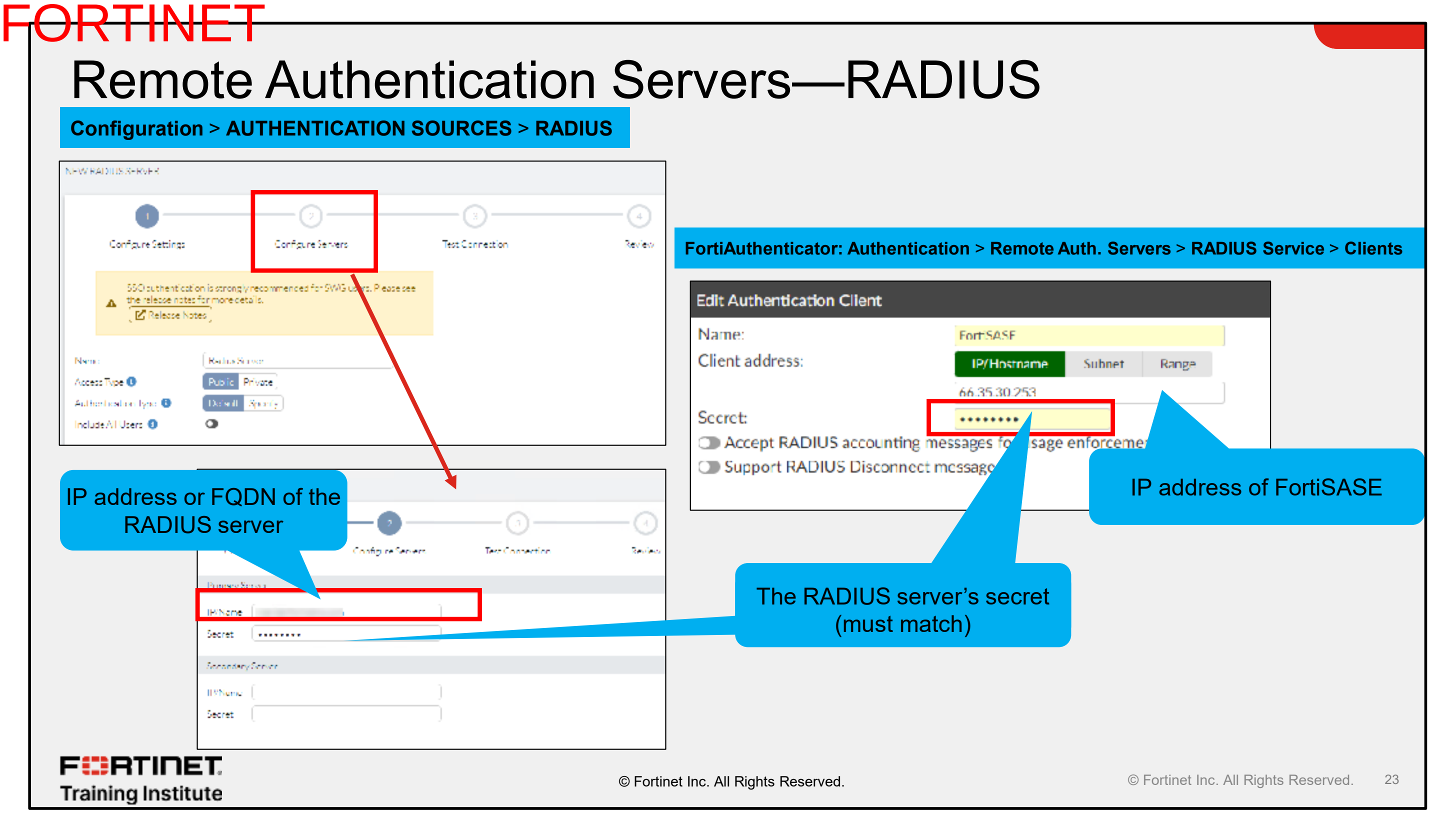
© Fortinet Inc. All Rights Reserved.

You can import remote LDAP users on the **Users** page. You can either import users or import users by group membership. When you are configuring the user group on FortiSASE, select the LDAP server as the remote authentication server and select specific LDAP groups to add to your user group, as defined on the LDAP server. To enter the email addresses of the LDAP users to send the invitation emails to, click **Configuration**, and then in the **ACCESS** section, click **Users** > **Onboard Users**.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET

Brave-dumps.com



Remote Authentication Servers—RADIUS

Configuration > AUTHENTICATION SOURCES > RADIUS

NEW RADIUS SERVER

SSO authentication is strongly recommended for SWG users. Please see the release notes for more details.
Release Notes

Name: Radius Server
Access Type: Public | Private
Authentication Type: Default | Specify
Include All Users

Primary Server
IP/Name
Secret ••••••••

Secondary Server
IP/Name
Secret

IP address or FQDN of the RADIUS server

FortiAuthenticator: Authentication > Remote Auth. Servers > RADIUS Service > Clients

Edit Authentication Client

Name: FortiSASE
Client address: IP/Hostname | Subnet | Range
66.35.30.253
Secret: ••••••••
Accept RADIUS accounting messages fo[r] [mes]sage enforceme[nt]
Support RADIUS Disconnect messag[es]

IP address of FortiSASE

The RADIUS server's secret (must match)

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved. 23

You can configure FortiSASE to connect to a remote RADIUS server on the **RADIUS** page. You must enter all required information about the remote RADIUS server, such as the IP address, port, and shared secret. You also have the option to set up a secondary server for redundancy. You cannot import RADIUS users individually, but you can configure a user group on FortiSASE with RADIUS as the remote authentication server and add user groups based on RADIUS attributes for group membership.

The **Primary Server Secret** setting is the secret that is set up on the RADIUS server in order to allow remote queries from this client. Note that FortiSASE must be listed on the RADIUS server as a client of that RADIUS server, or the server will not reply to FortiSASE queries.

The **Authentication Type** setting refers to the authentication protocol that the RADIUS server supports. Options include Common-Handshake Authentication Protocol (CHAP), Password Authentication Protocol (PAP), Microsoft CHAP (MS-CHAP), and MSCHAP2.

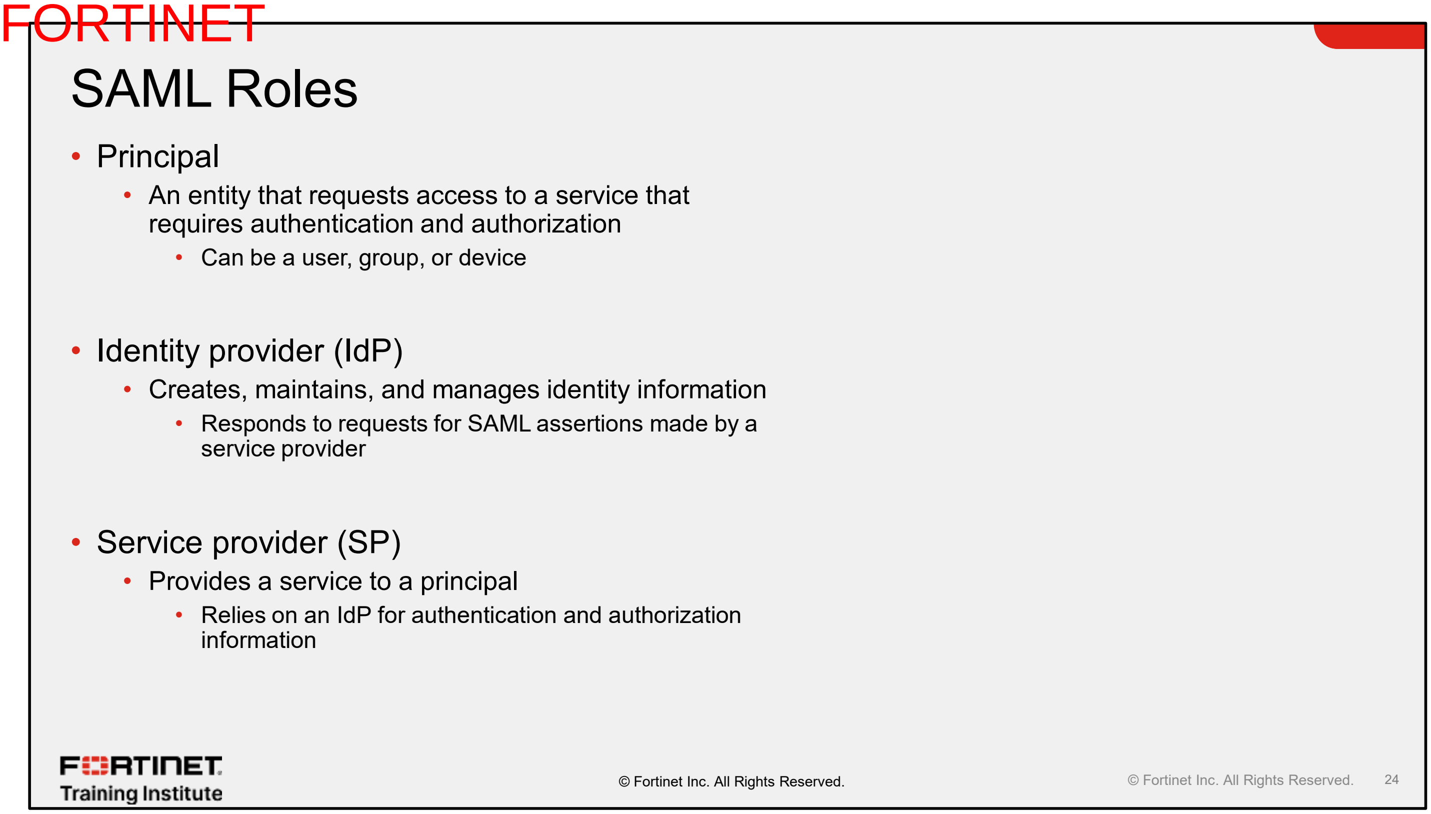
The **Include All Users** option adds the RADIUS server and all users that can authenticate against it, to every user group created on FortiSASE.

This slide shows an example of FortiAuthenticator as the RADIUS server and FortiSASE as the RADIUS client.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET

Brave-dumps.com



SAML Roles

- Principal
  - An entity that requests access to a service that requires authentication and authorization
    - Can be a user, group, or device
- Identity provider (IdP)
  - Creates, maintains, and manages identity information
    - Responds to requests for SAML assertions made by a service provider
- Service provider (SP)
  - Provides a service to a principal
    - Relies on an IdP for authentication and authorization information

© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved. 24

SAML defines a framework for exchanging security assertions between SAML entities. It uses an XML-based framework and browser cookies to exchange security assertions between entities to achieve SSO. One of the main SAML use cases is a multiple-domain web SSO. Online business partners can exchange SAML assertions, to provide user access to multiple web services, without asking the user to log in to each domain.

At a minimum, you need the following SAML entities to perform SSO:

- Principal: requests access to a service that usually requires authentication and authorization using the SAML model. A principal can be a user, group, or machine.
- IdP: responsible for creating, maintaining, and managing identity information for principals. It is responsible for responding to requests for SAML assertions within a federation.
- SP: provides a service to a principal. It relies on an IdP for authentication and authorization information that it can use to provide access to a principal.

Vouchers & Dumps are Available | WhatsApp +201224560923

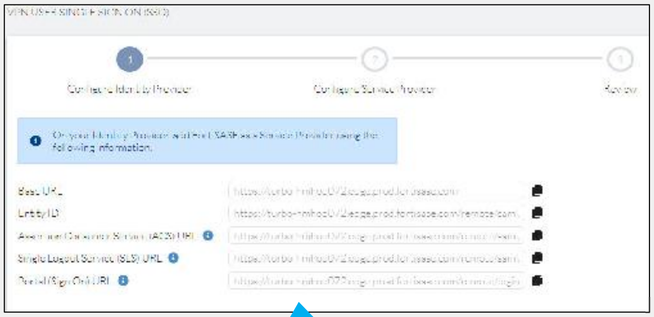
DO NOT REPRINT
© FORTINET

Brave-dumps.com

Configuring SSO

- Enabling SSO authentication overrides any other previously created authentication methods

Configuration > AUTHENTICATION SOURCES > VPN User SSO

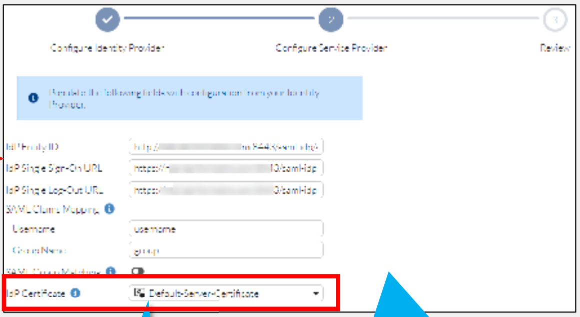


VPN USER SINGLE SIGN ON (SSO)

1 Configure Identity Provider — 2 Configure Service Provider — 3 Review

On your Identity Provider, add FortiSASE as a Service Provider using the following information.

Base URL	https://turbo-rmhodUV2.edge.prod.fortisase.com
Entity ID	https://turbo-rmhodUV2.edge.prod.fortisase.com/remote/saml
Assertion Consumer Service (ACS) URL	https://turbo-[illegible]
Single Logout Service (SLS) URL	https://turbo-[illegible]
Portal (Sign On) URL	https://turbo-[illegible]



Configure Identity Provider — Configure Service Provider — Review

Populate the following fields with configuration from your Identity Provider.

IdP Entity ID	http://[redacted]:9443/saml-idp/
IdP Single Sign-On URL	https://[redacted]0/saml-idp
IdP Single Log-Out URL	https://[redacted]0/saml-idp
SAML Claims Mapping	
Username	username
Group Name	group
SAML Group Matching	
IdP Certificate	Default-Server-Certificate

Preconfigured fields, to be added on the IdP

Select a local service certificate

Add IdP configuration

FURTINET Training Institute

© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved. 25

You can enable SSO authentication for FortiSASE endpoint users by configuring SAML. SSO authentication is supported for both SWG and VPN modes. When configuring FortiSASE as a SAML SP, you do not need to host the user database locally. User authentication is performed by an IdP, and FortiSASE directs principals to the IdP portal for authentication.

You can configure SSO authentication on the **VPN User SSO** page for VPN users or **SWG User SSO** page for SWG users. The service provider fields are preconfigured and should be added to your IdP server. You must enter the IdP configuration into FortiSASE to complete the SSO configuration.

You can upload a certificate for use with SAML SSO authentication on the **Certificates** page under **System**.

Enabling SSO authentication overrides any other previously created authentication methods (local database, LDAP, or RADIUS). Fortinet products, like FortiAuthenticator or FortiTrust Identity, can act as an IdP for this configuration.

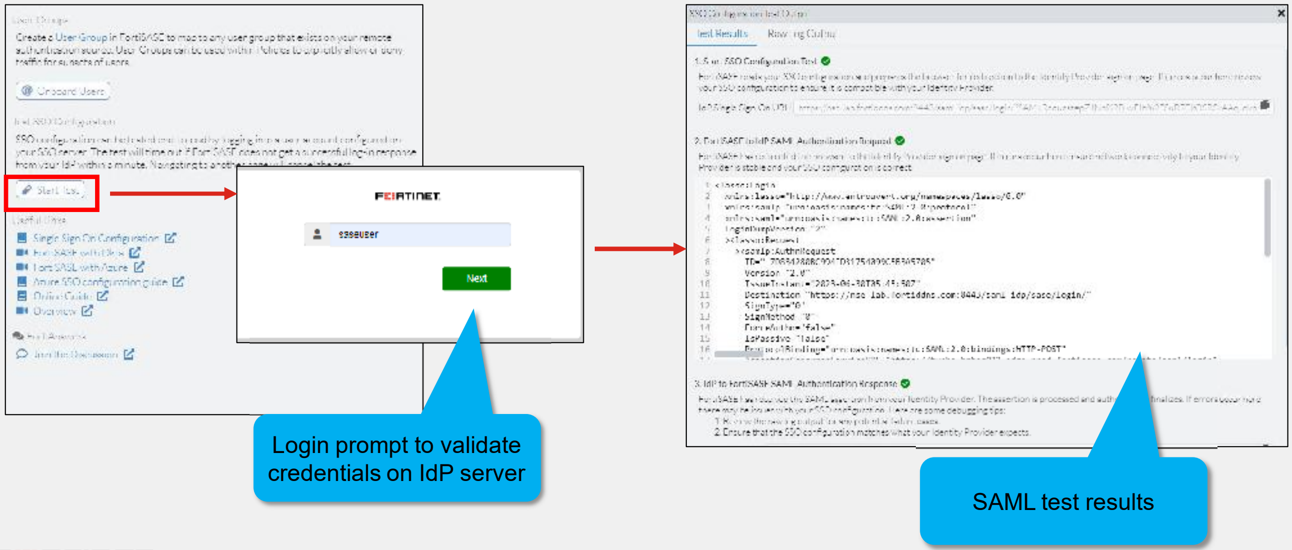
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET

Brave-dumps.com

Testing SSO Configuration

Configuration > AUTHENTICATION SOURCES > VPN User SSO


Create a User Group in FortiSASE to map to any user group that exists on your remote authentication source. User Groups can be used within Policies to explicitly allow or deny traffic for subsets of users.
Onboard Users
Start Test
Single Sign On Configuration
FortiSASE with Azure
Azure SSO configuration guide
Online Guide
Overview
FORTINET
sseuser
Next
Test Results
1. FortiSASE SSO Configuration Test
2. FortiSASE to IdP SAML Authentication Request
3. IdP to FortiSASE SAML Authentication Response
2. Ensure that the SSO configuration matches what your Identity Provider expects.
Login prompt to validate credentials on IdP server
SAML test results

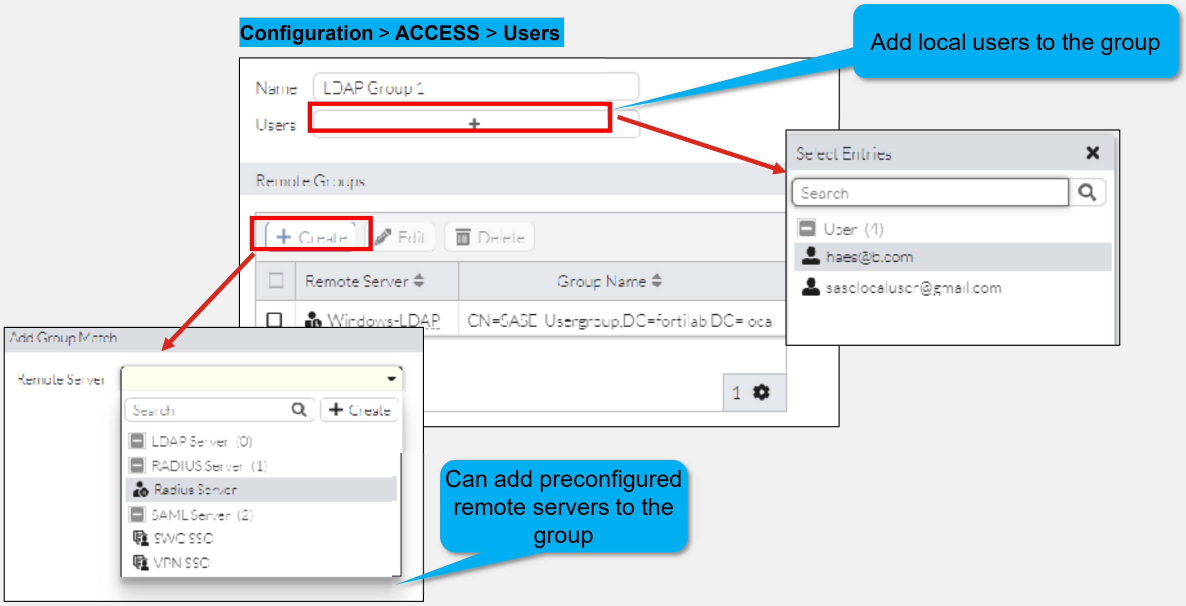
From FortiSASE, you can test the SSO configuration settings end-to-end by logging in to a user account configured on your SSO server. This feature allows you to open a test window that points to the SSO login page. This test provides SSO configuration test results and raw log output of SAML debugs from the security POP. This data can help you troubleshoot issues caused by any misconfigured SSO configuration settings. To perform this test, click **Start Test** on the **VPN User SSO** page. The **Start Test** option is available only after you submit the SSO configuration.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET

Brave-dumps.com

Configuring User Groups



Configuration > ACCESS > Users

Name: LDAP Group 1

Add local users to the group

Can add preconfigured remote servers to the group

© Fortinet Inc. All Rights Reserved.

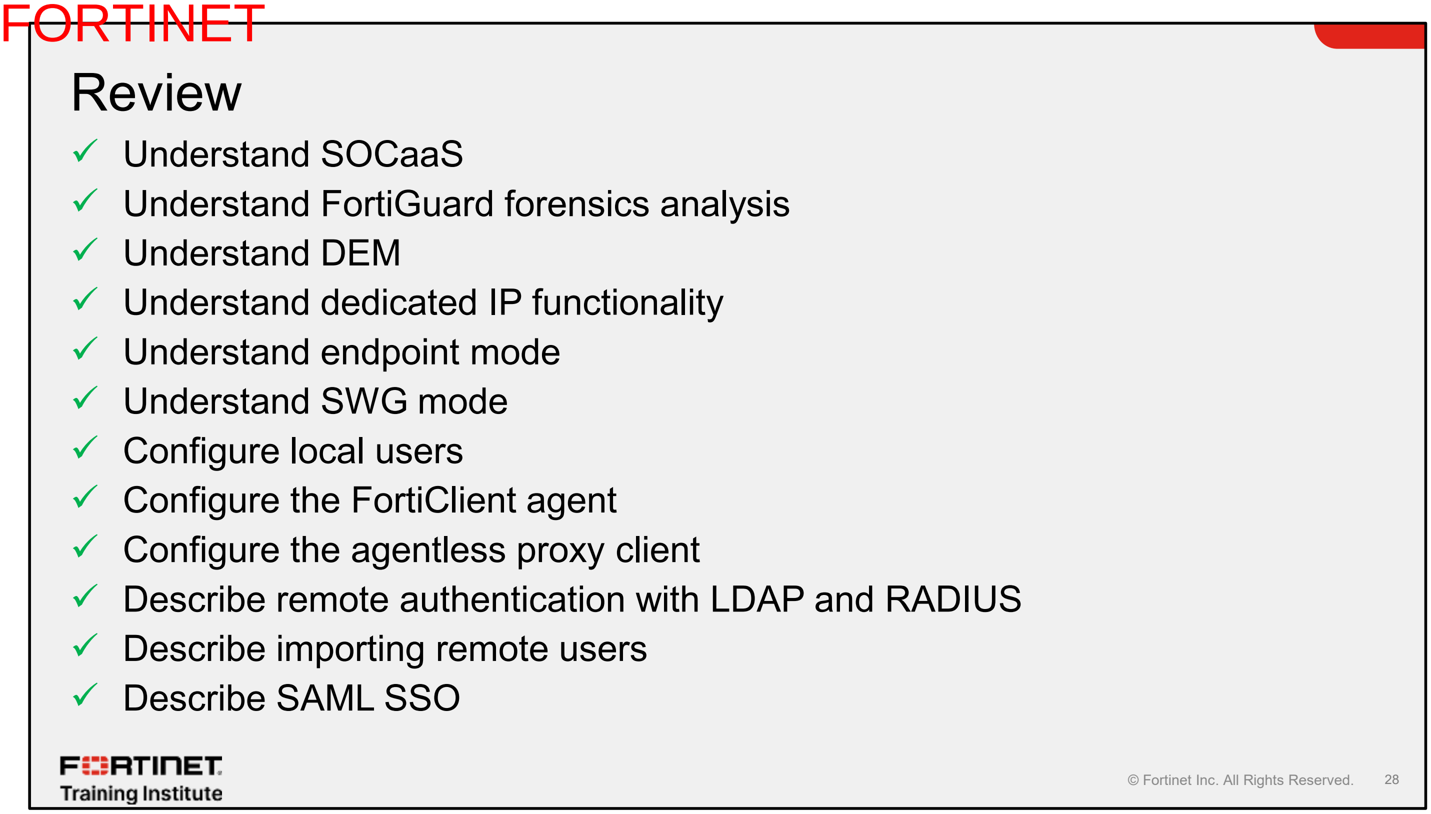
© Fortinet Inc. All Rights Reserved.

You can configure user groups on the **Users** page. You can add local users to the user group, or you can add preconfigured remote servers to the group. User groups simplify your configuration, if you want to treat specific users in the same way.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET

Brave-dumps.com



Review

- ✓ Understand SOCaaS
- ✓ Understand FortiGuard forensics analysis
- ✓ Understand DEM
- ✓ Understand dedicated IP functionality
- ✓ Understand endpoint mode
- ✓ Understand SWG mode
- ✓ Configure local users
- ✓ Configure the FortiClient agent
- ✓ Configure the agentless proxy client
- ✓ Describe remote authentication with LDAP and RADIUS
- ✓ Describe importing remote users
- ✓ Describe SAML SSO

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 28

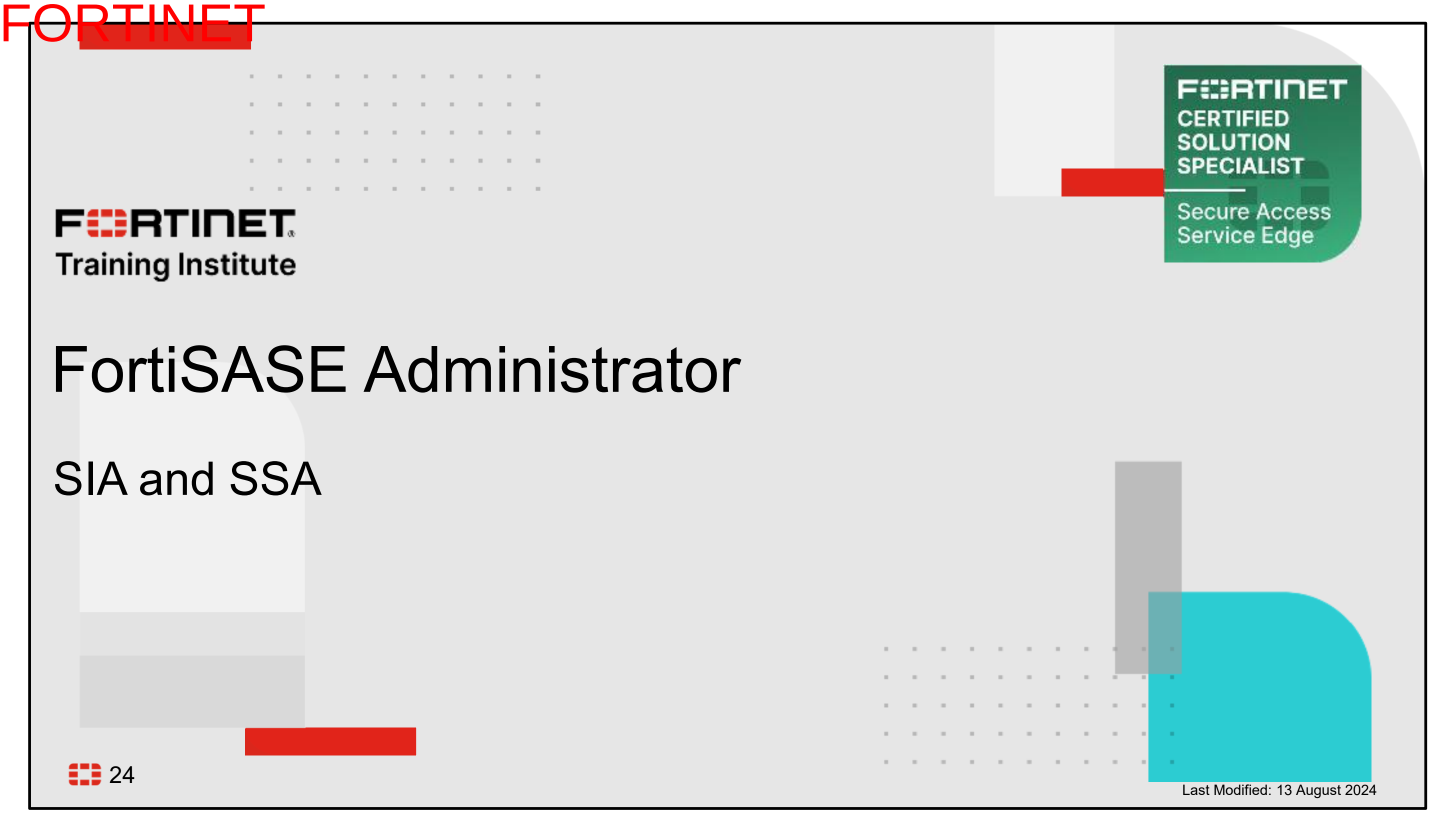
This slide shows the objectives that you covered in this lesson.

By mastering the objectives covered in this lesson, you learned how to use the advanced features and authentication methods on FortiSASE.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET

Brave-dumps.com



FORTINET Training Institute

FORTINET CERTIFIED SOLUTION SPECIALIST

Secure Access Service Edge

FortiSASE Administrator

SIA and SSA

24

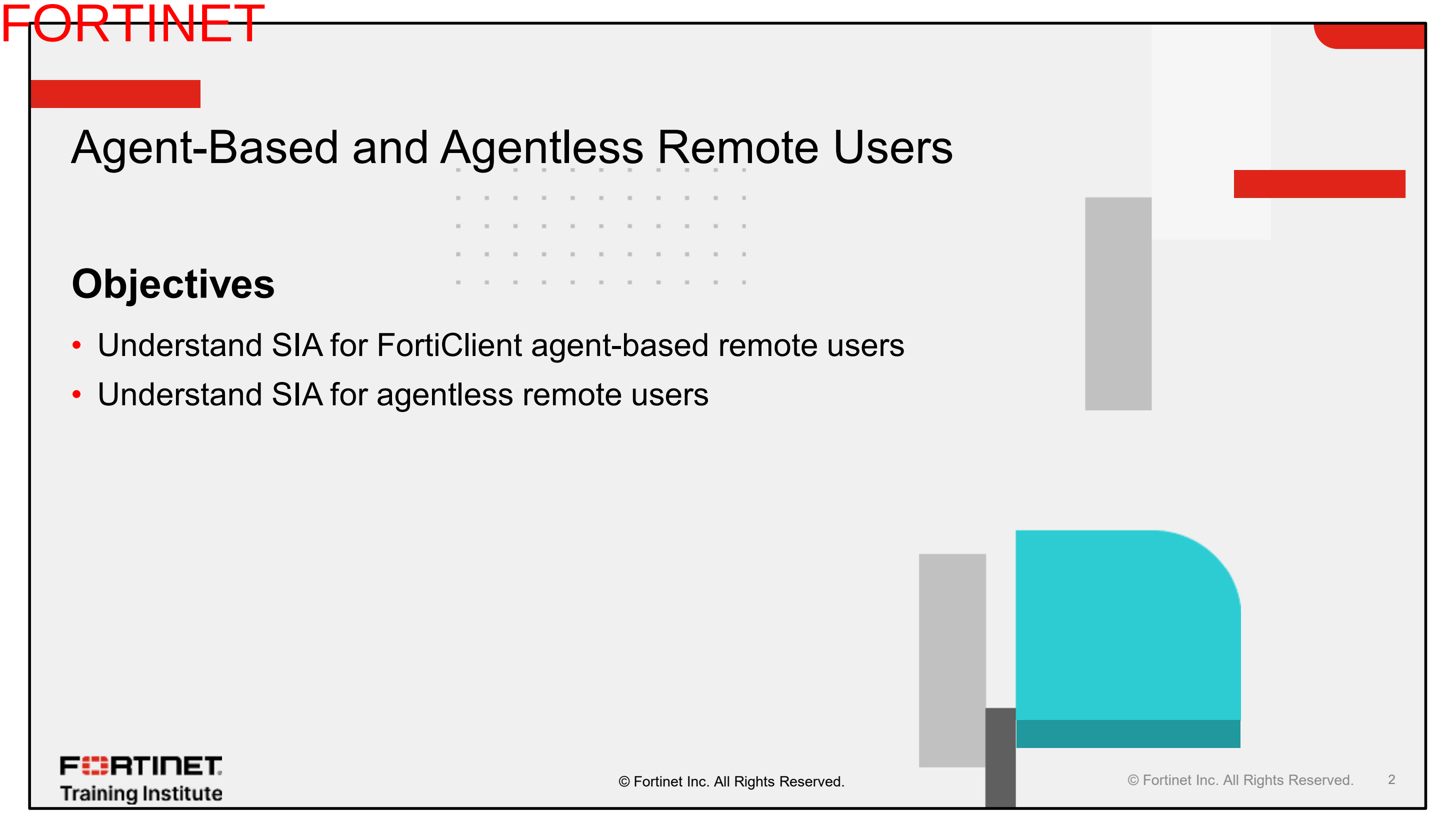
Last Modified: 13 August 2024

In this lesson, you will learn about the common use cases of secure internet access (SIA) and secure SaaS access (SSA) in a FortiSASE deployment.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET

Brave-dumps.com



Agent-Based and Agentless Remote Users

Objectives

- Understand SIA for FortiClient agent-based remote users
- Understand SIA for agentless remote users

© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved. 2

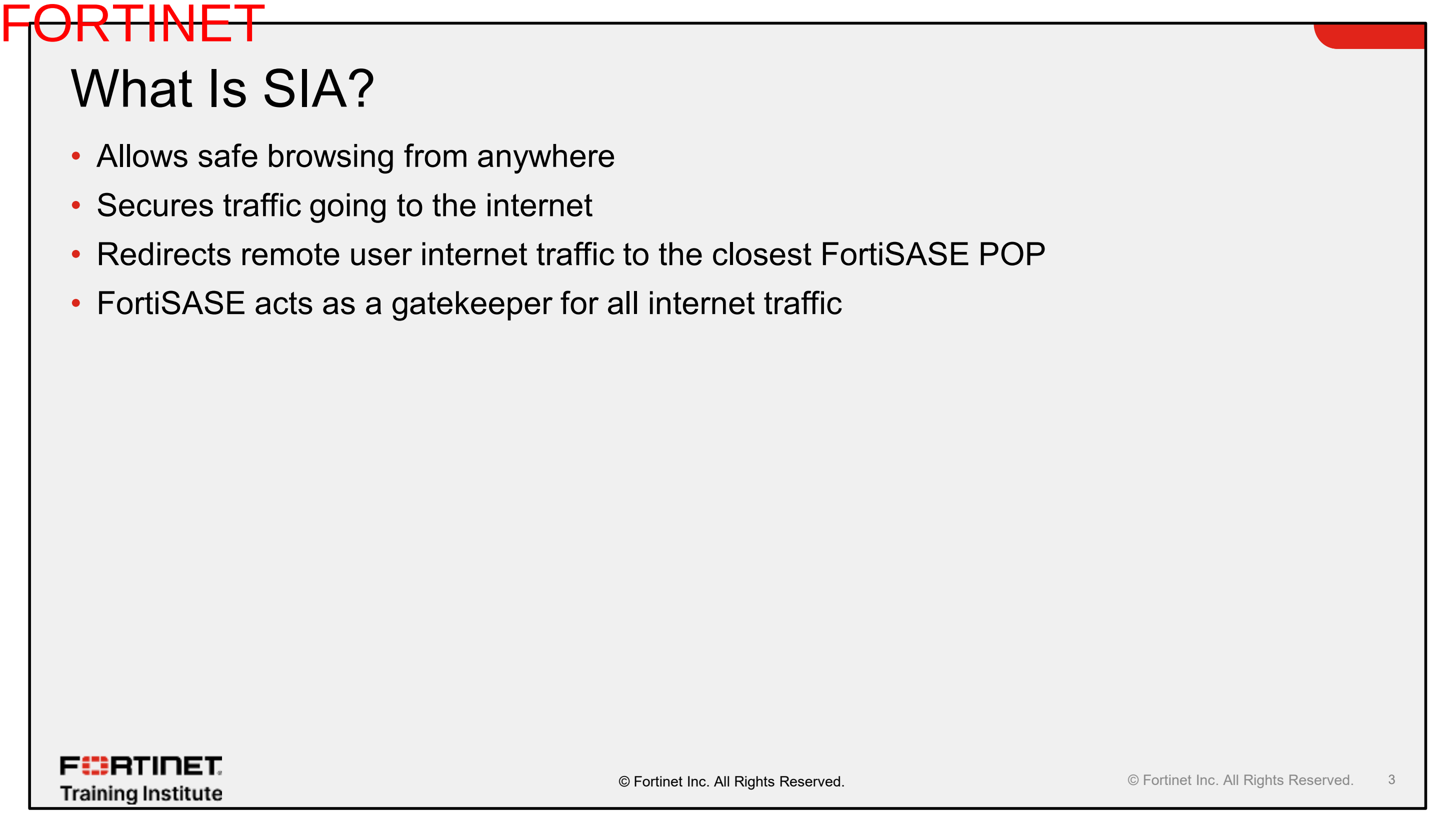
After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating a competent understanding of agent-based and agentless remote users, you will be able to identify use cases for SIA for agent-based and agentless remote users.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET

Brave-dumps.com



What Is SIA?

- Allows safe browsing from anywhere
- Secures traffic going to the internet
- Redirects remote user internet traffic to the closest FortiSASE POP
- FortiSASE acts as a gatekeeper for all internet traffic

© Fortinet Inc. All Rights Reserved.

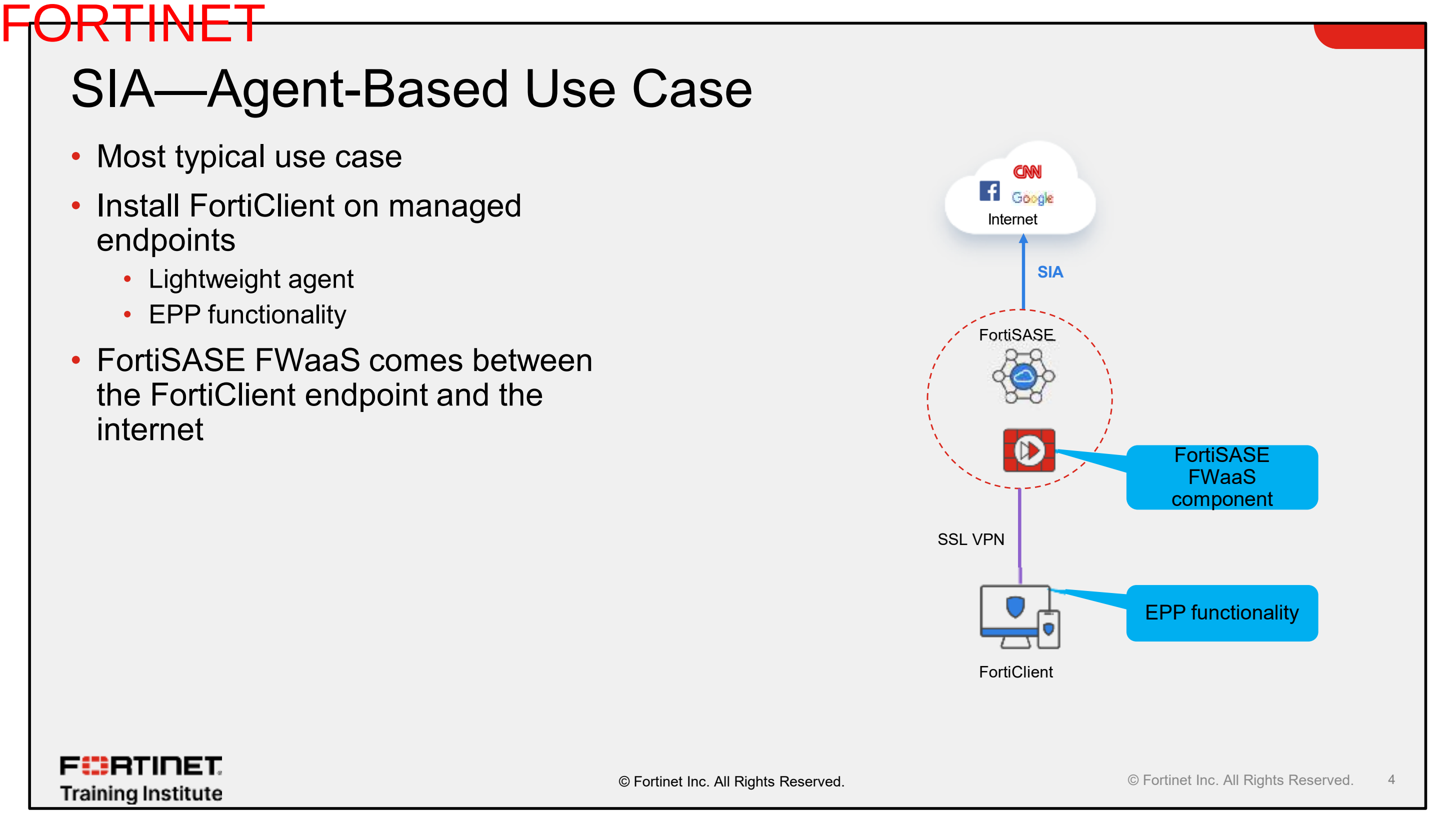
© Fortinet Inc. All Rights Reserved. 3

FortiSASE SIA extends an organization’s security by enforcing a common security policy to remote users for intrusion prevention systems (IPS), application control, web filtering, antimalware, sandboxing, and so on. FortiSASE acts as a gatekeeper to inspect and secure all internet traffic, which allows safe browsing from anywhere for off-net users. FortiSASE redirects the internet traffic of remote users to the closest FortiSASE point of presence (POP) using geolocation selection.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET

Brave-dumps.com



SIA—Agent-Based Use Case

- Most typical use case
- Install FortiClient on managed endpoints
  - Lightweight agent
  - EPP functionality
- FortiSASE FWaaS comes between the FortiClient endpoint and the internet

© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved. 4

Agent-based deployment is the most common use case in FortiSASE deployment. FortiClient is deployed on endpoints and the endpoints connect back to FortiSASE using a secure SSL VPN tunnel. FortiSASE Firewall-as-a-Service (FWaaS) sits between the FortiClient endpoint and the internet to secure the internet. FortiSASE FWaaS uses its security profile component, which includes web filter, application control, SSL deep inspection, and so on, to inspect the internet traffic. FortiClient offers endpoint protection platform (EPP) functionality, which includes features like antivirus, vulnerability scanning, sandbox inspection, and so on. Agent-based deployment also supports zero trust network access (ZTNA) for continuous posture check and enforcement.

Vouchers & Dumps are Available | WhatsApp +201224560923

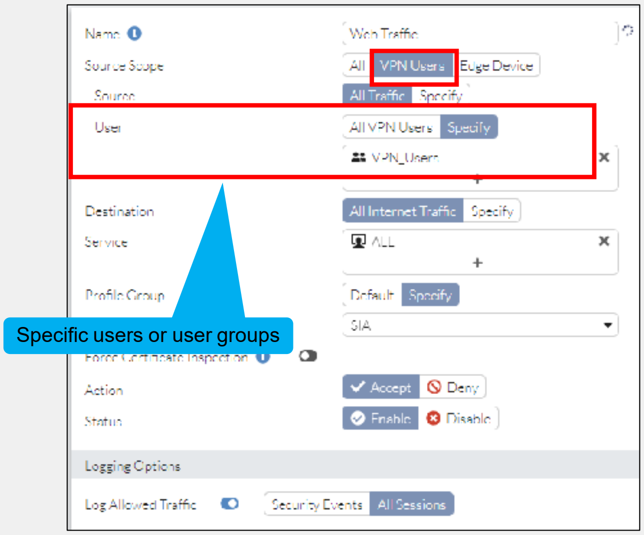
DO NOT REPRINT
© FORTINET

Brave-dumps.com

Configuring Policies—VPN Users

- The **VPN Users** policy controls traffic between the FortiClient endpoint and internet for SIA

Configuration > TRAFFIC > Policies > Internet Access



Name	Web Traffic
Source Scope	All / **VPN Users** / Edge Device
Source	**All Traffic** / Specify
User	All VPN Users / **Specify**
	VPN_Users
Destination	**All Internet Traffic** / Specify
Service	ALL
Profile Group	Default / **Specify**
	SIA
Force Certificate Inspection	○
Action	**✓ Accept** / Deny
Status	**Enable** / Disable
Logging Options	
Log Allowed Traffic ●	Security Events / **All Sessions**

Specific users or user groups

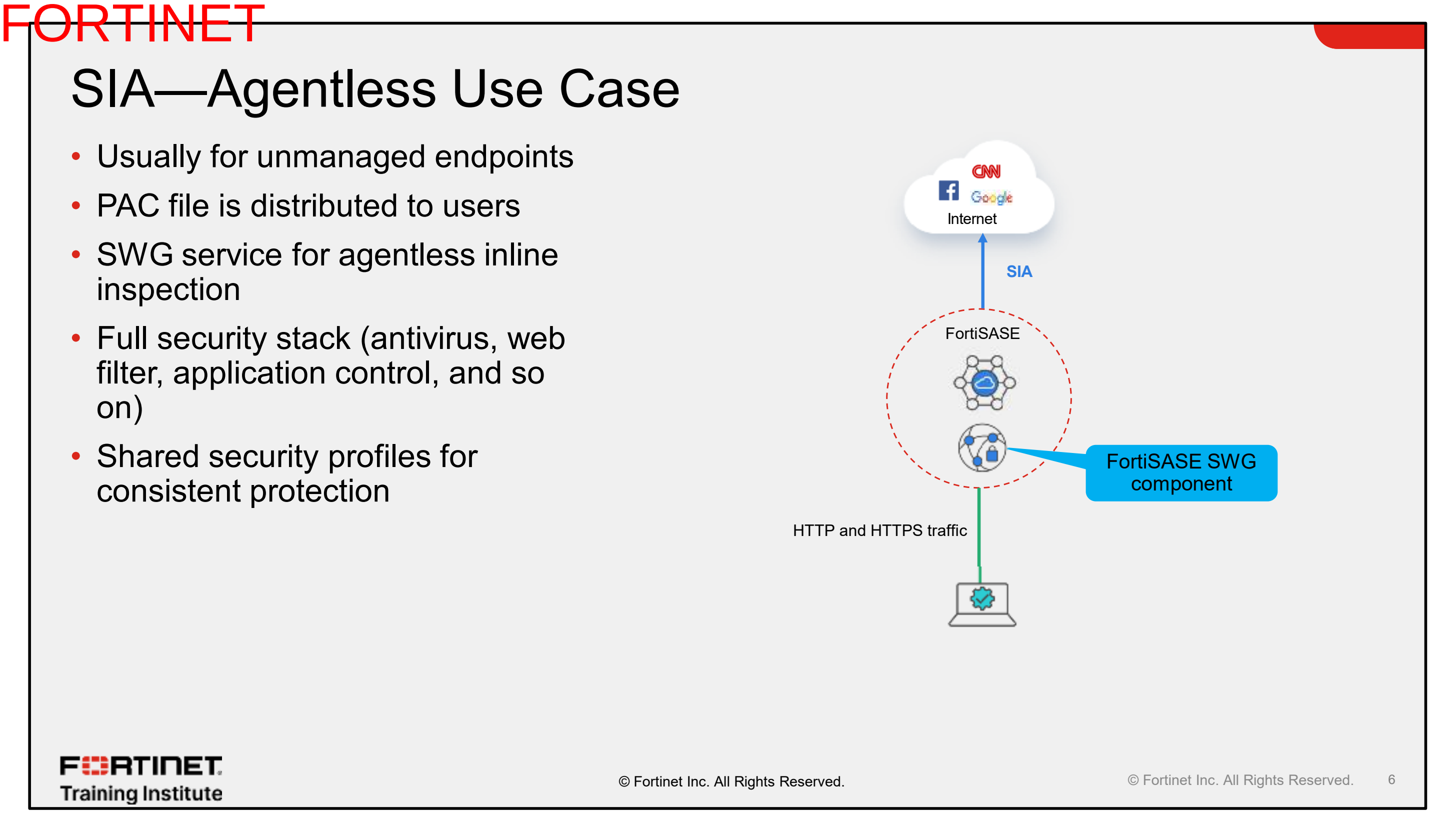
When you create a policy, you configure the following parameters:

- **Name**: The unique policy name is a mandatory parameter, and it helps in analysis for FortiView and logging.
- **Source Scope**: You can select **VPN Users** or **Edge Device**, based on the endpoint traffic requirement.
  - **VPN Users**: Policies that have this scope control the traffic that goes through the SSL VPN tunnel that FortiClient establishes.
- **Source:** You can add ZTNA tags to enforce device posture checks for agent-based (FortiClient) users in an internet access policy or private access policy.
- **User**: This parameter is available only when you select **VPN Users**. It is based on a user identity that can come from several authentication authorities. It is a single user or group you set up in advance and can select from the **User** field.
- **Destination**: You can define policies to connect to specific addresses on the internet.
- **Service**: The services you choose represent the TCP/IP suite port numbers that are most commonly used to transport the named protocols or groups of protocols.
- **Profile Group**: You can create security profile groups, to allow you to group different security profile settings and then apply them to a policy.
- **Force Certificate Inspection**: When enabled, this policy ignores the SSL inspection mode specified in the profile group and user certificate inspection.
- **Action**: If the traffic matches a firewall policy, FortiSASE applies this action. If the **Action** is set to **DENY**, FortiSASE drops the session. If the **Action** is set to **ACCEPT**, FortiSASE allows the session and applies other configured settings for packet processing, such as user authentication, source, antivirus scanning, web filtering, and so on.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET

Brave-dumps.com



SIA—Agentless Use Case

- Usually for unmanaged endpoints
- PAC file is distributed to users
- SWG service for agentless inline inspection
- Full security stack (antivirus, web filter, application control, and so on)
- Shared security profiles for consistent protection

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved. 6

The use case for agentless deployment does not require the installation of FortiClient endpoints, and ZTNA tags are not supported. In this use case, FortiSASE acts as a secure web gateway (SWG) and distributes a proxy auto-configuration file (PAC) file to end users for using the FortiSASE SWG service as an explicit web proxy. SWG deployment secures only web traffic protocols, such as HTTP and HTTPS. The SWG component on FortiSASE offers a full security stack with antivirus, web filter, application control, and so on. The security profiles can be shared between agent and agentless deployment, for consistent protection. This use case is usually recommended for unmanaged endpoints like a contractor or temporary employee.

Vouchers & Dumps are Available | WhatsApp +201224560923

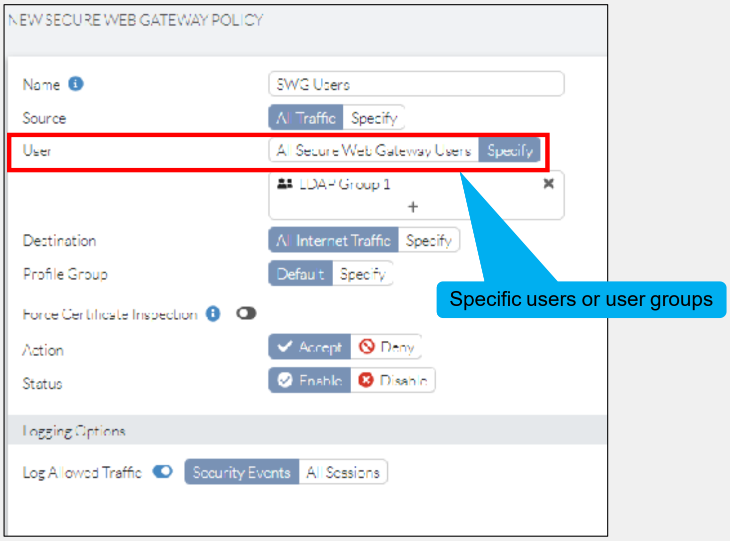
DO NOT REPRINT
© FORTINET

Brave-dumps.com

Configuring Policies—SWG

- An SWG policy controls web traffic between the proxy client endpoint and internet for SIA

Configuration > TRAFFIC > SWG Policies



NEW SECURE WEB GATEWAY POLICY

Name: SWG Users

Source: All Traffic | Specify

User: All Secure Web Gateway Users | Specify

LDAP Group 1

Destination: All Internet Traffic | Specify

Profile Group: Default | Specify

Force Certificate Inspection

Action: ✓ Accept | Deny

Status: Enable | Disable

Logging Options

Log Allowed Traffic: Security Events | All Sessions

Specific users or user groups

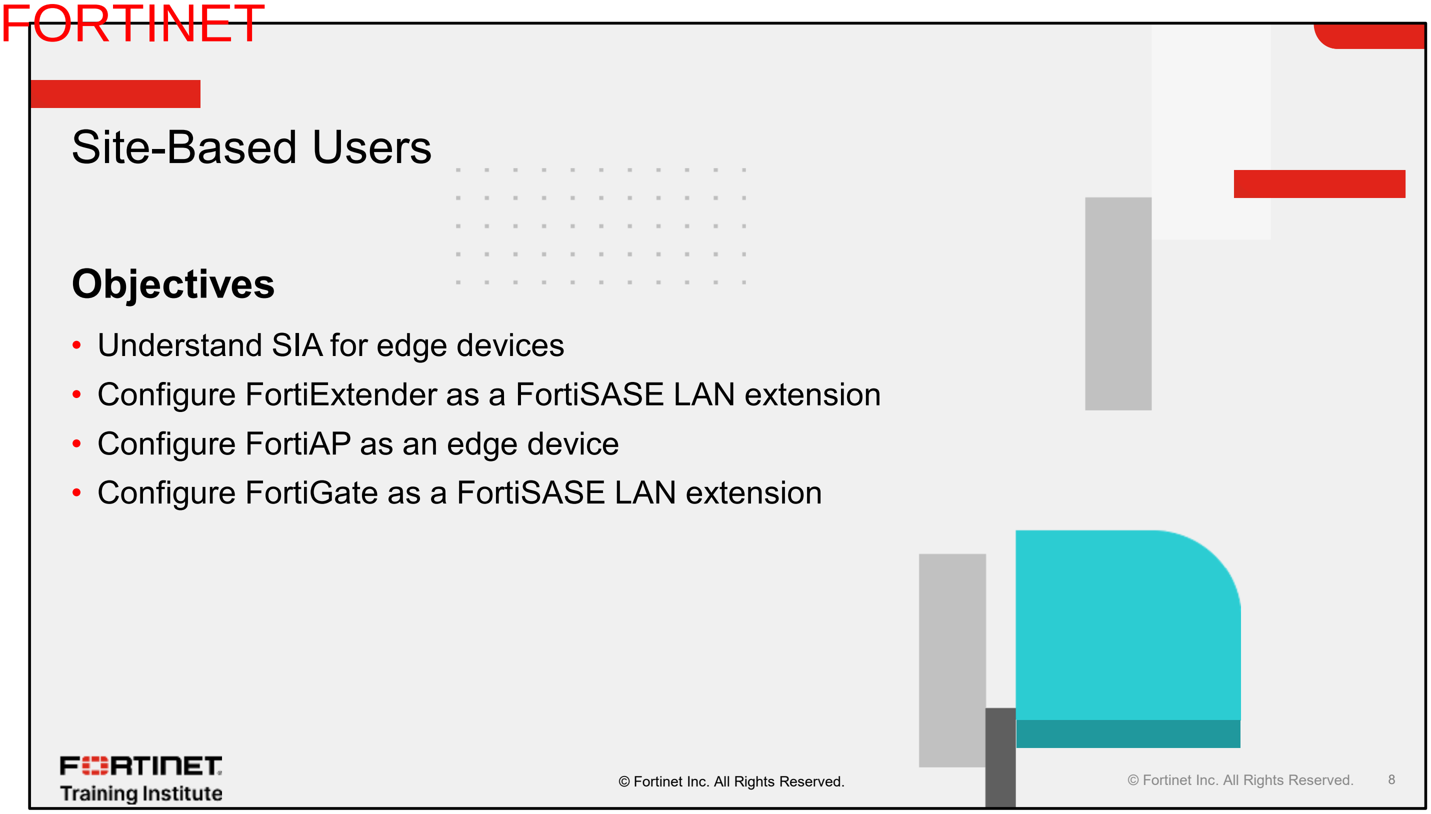
© Fortinet Inc. All Rights Reserved.

SWG policies control the traffic that the user's client software proxies through FortiSASE, such as a web browser. You can configure an SWG policy on the **SWG Policies** page. The parameters used to configure an SWG policy are similar to the **VPN Users** policy.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET

Brave-dumps.com



Site-Based Users

Objectives

- Understand SIA for edge devices
- Configure FortiExtender as a FortiSASE LAN extension
- Configure FortiAP as an edge device
- Configure FortiGate as a FortiSASE LAN extension

© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved. 8

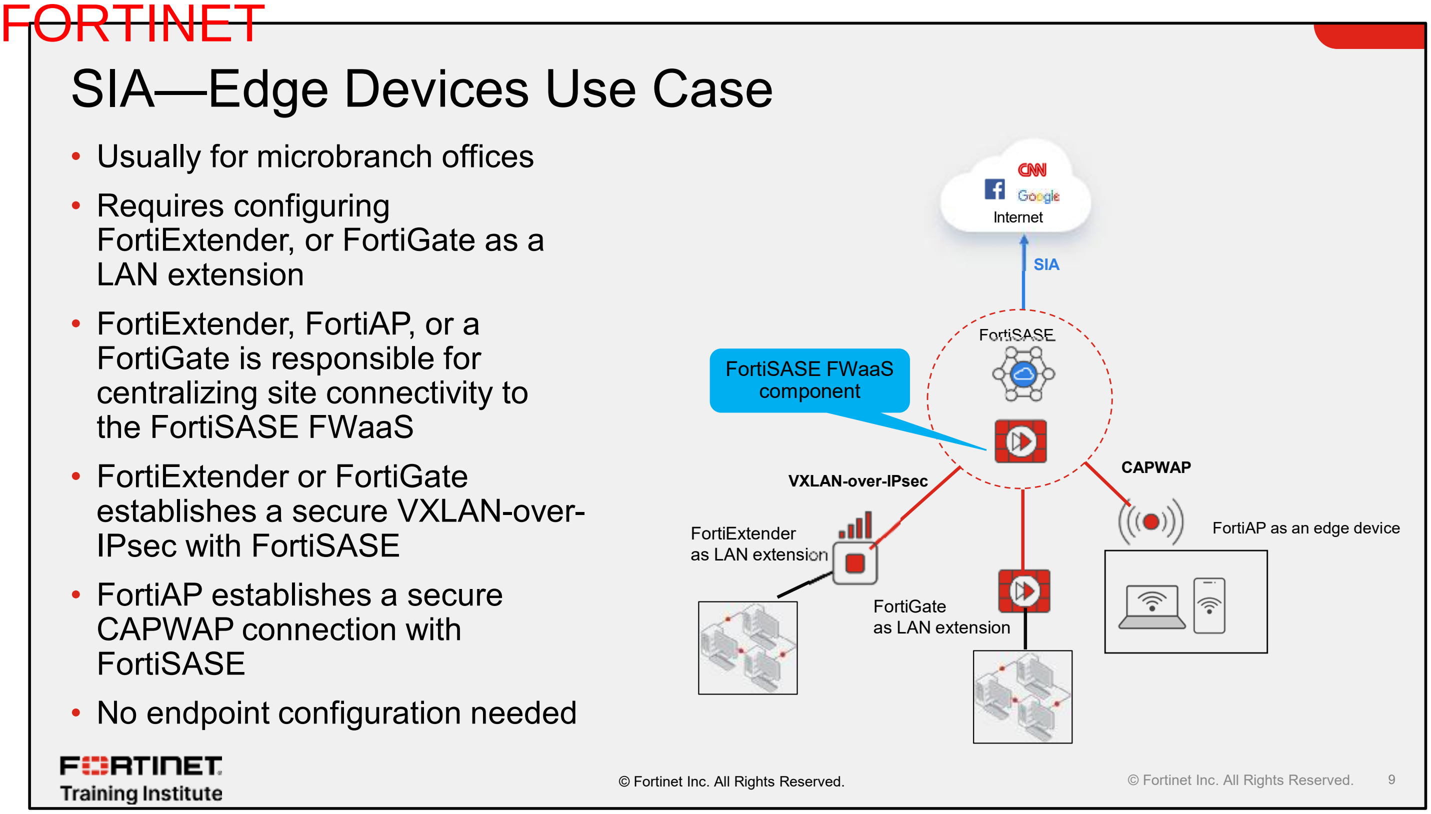
After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating a competent understanding of edge devices, you will be able identify use cases for SIA for edge devices in a FortiSASE deployment.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET

Brave-dumps.com



SIA—Edge Devices Use Case

- Usually for microbranch offices
- Requires configuring FortiExtender, or FortiGate as a LAN extension
- FortiExtender, FortiAP, or a FortiGate is responsible for centralizing site connectivity to the FortiSASE FWaaS
- FortiExtender or FortiGate establishes a secure VXLAN-over-IPsec with FortiSASE
- FortiAP establishes a secure CAPWAP connection with FortiSASE
- No endpoint configuration needed

CNN
Google
Internet
SIA
FortiSASE
FortiSASE FWaaS component
VXLAN-over-IPsec
CAPWAP
FortiExtender as LAN extension
FortiGate as LAN extension
FortiAP as an edge device

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved. 9

LAN extension is a configuration mode on FortiSASE that allows FortiExtender or FortiGate to provide remote thin edge connectivity back to the FortiSASE over a backhaul connection. A FortiExtender or FortiGate deployed at a remote location will discover the FortiSASE access controller (AC) and form an IPsec tunnel back to the FortiSASE. A virtual eXtensible LAN (VXLAN) is established over the IPsec tunnels to create a layer 2 network between the FortiSASE and the network behind the remote FortiExtender or FortiGate.

FortiSASE can manage a FortiAP deployed in a remote location over a backhaul connection to provide SIA to Wi-Fi clients. The FortiAP discovers the FortiSASE AC, and establishes an IPsec VPN tunnel that encrypts the data channel between FortiSASE and FortiAP. The FortiAP carries Control and Provisioning of Wireless Access Points (CAPWAP) data packets and includes the FortiAP serial number within this tunnel.

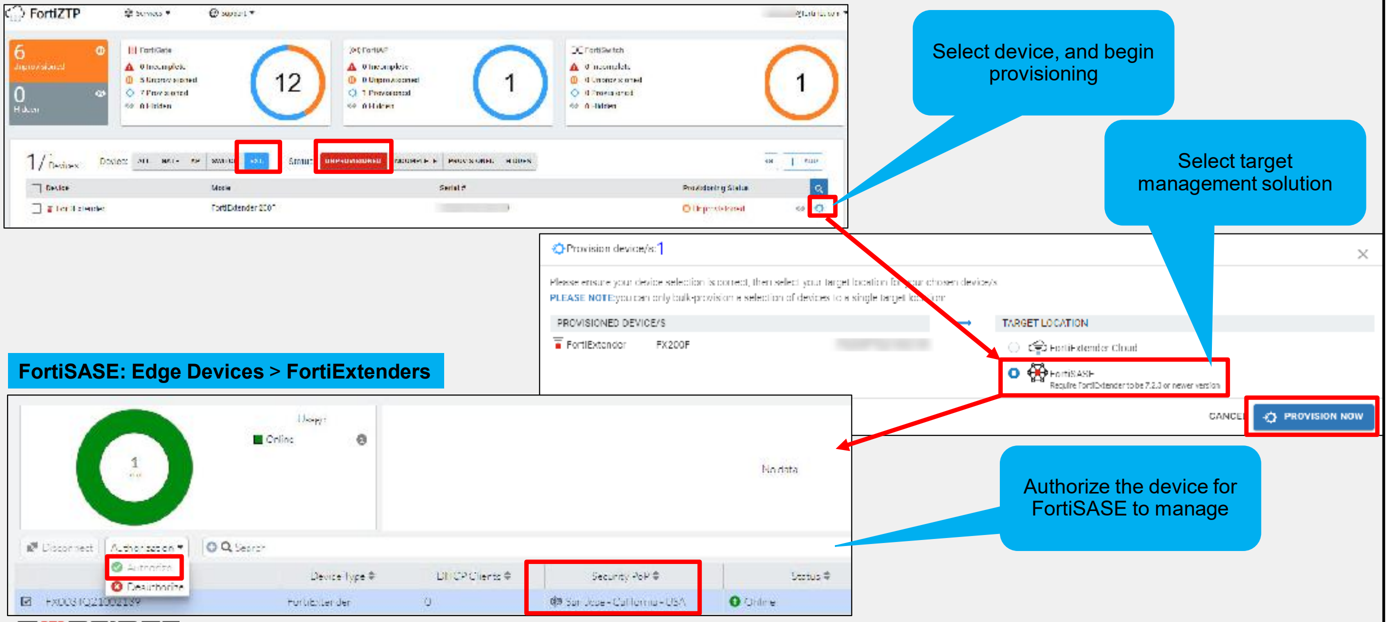
In this SIA use case, FortiExtender, FortiAP, or FortiGate is responsible for centralizing site connectivity to the FortiSASE FWaaS . No configuration is required on endpoints. All endpoint traffic is routed from the FortiExtender, FortiAP, or FortiGate to FortiSASE FWaaS, where security profiles secure it.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET

Brave-dumps.com

Connecting Edge Devices to FortiSASE Using FortiZTP



Select device, and begin provisioning

Select target management solution

FortiSASE: Edge Devices > FortiExtenders

Authorize the device for FortiSASE to manage

© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved. 10

FortiZTP is the recommended configuration method of deploying FortiAP and FortiExtender to FortiSASE. To access the FortiZTP portal, on the FortiSASE portal, click **Services** > **FortiZTP**. After you register the devices on the Fortinet support portal with proper licenses, you can view them on the **UNPROVISIONED** tab on the FortiZTP portal. You can then provision them with the target location **FortiSASE**. After you provision the FortiAP or FortiExtender on the FortiZTP portal, it is automatically listed on the FortiSASE portal as an edge device, and you must **Authorize** it. After you successfully authorize the device on FortiSASE as an edge device, it connects to the POP closest to its physical location.

Vouchers & Dumps are Available | WhatsApp +201224560923

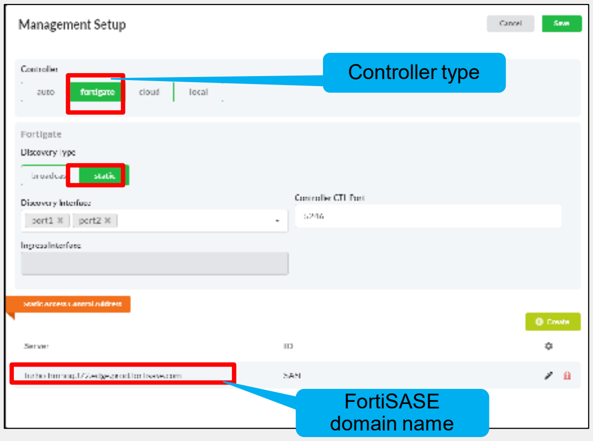
DO NOT REPRINT
© FORTINET

Brave-dumps.com

Alternative Configuration Method

- Obtain FortiSASE domain name from FortiSASE portal

FortiExtender: Settings > Management



Management Setup

Cancel | Save

Controller: ○ auto [✓ fortigate] ○ cloud ○ local

Fortigate

Discovery Type: ○ broadcast [✓ static]

Discovery Interface: port1 ✕ port2 ✕

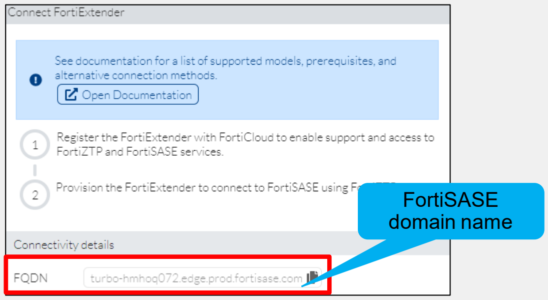
Controller CTL Port: 5246

Ingress Interface

Static Access Control Address

Server	ID
turbo-hmhoq072.edge.prod.fortisase.com	SAN

FortiSASE: Edge Devices > FortiExtenders



Connect FortiExtender

See documentation for a list of supported models, prerequisites, and alternative connection methods.

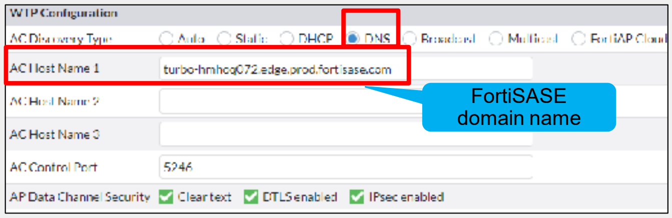
Open Documentation

1. Register the FortiExtender with FortiCloud to enable support and access to FortiZTP and FortiSASE services.
2. Provision the FortiExtender to connect to FortiSASE using Fo

Connectivity details

FQDN: turbo-hmhoq072.edge.prod.fortisase.com

FortiAP: Settings > Local Configuration



WTP Configuration

AC Discovery Type: ○ Auto ○ Static ○ DHCP ● DNS ○ Broadcast ○ Multicast ○ FortiAP Cloud

AC Host Name 1: turbo-hmhoq072.edge.prod.fortisase.com

AC Host Name 2:

AC Host Name 3:

AC Control Port: 5246

AP Data Channel Security: ☑ Clear text ☑ DTLS enabled ☑ IPsec enabled

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

As an alternative configuration method, you can enter the FortiSASE domain name as an access controller in the FortiAP and FortiExtender GUI to connect them as an edge device on FortiSASE. To obtain the FortiSASE domain name from the FortiSASE portal, click **Edge Devices** > **FortiExtenders**, and then click **Connect FEXTs.**

To connect FortiExtender to FortiSASE, on the FortiExtender GUI, click **Settings** > **Management**. Select **fortigate** as the controller type, **static** as the discovery method, and then type the FortiSASE domain name in the **Server** section.

Similarly, you can connect FortiAP to FortiSASE using the FortiAP GUI. On the **Settings** > **Local Configuration** page, in the **WTP Configuration** section, select **DNS** as the **AC Discovery Type**, and then type the FortiSASE domain name in the **AC Host Name 1** field.

Vouchers & Dumps are Available | WhatsApp +201224560923

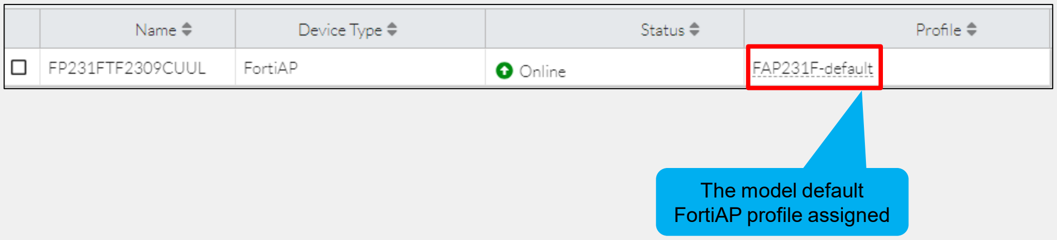
DO NOT REPRINT
© FORTINET

Brave-dumps.com

Access Point Profile

- FortiSASE automatically assigns a default FortiAP profile to newly discovered APs
  - Default profile named is based on the AP model, followed by '-default'
- FortiSASE must authorize the FortiAP device before it pushes any configuration settings to the AP

Edge Devices > FortiAPs > Managed FortiAPs



	Name ⬍	Device Type ⬍	Status ⬍	Profile ⬍
☐	FP231FTF2309CUUL	FortiAP	● Online	FAP231F-default

The model default FortiAP profile assigned

F⁚RTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved. 12

A FortiAP profile defines configuration settings for an access point (AP) including operating band, channels, SSID networks, and so on. The FortiAP profile specifies the type of hardware that a FortiAP device uses. This information is required for FortiSASE when it pushes configuration parameters to the managed AP. By default, when a FortiAP device is connected to FortiSASE, FortiSASE tries to discover the FortiAP device. Upon discovery of the FortiAP device, FortiSASE automatically assigns it a default profile, based on the FortiAP hardware model.

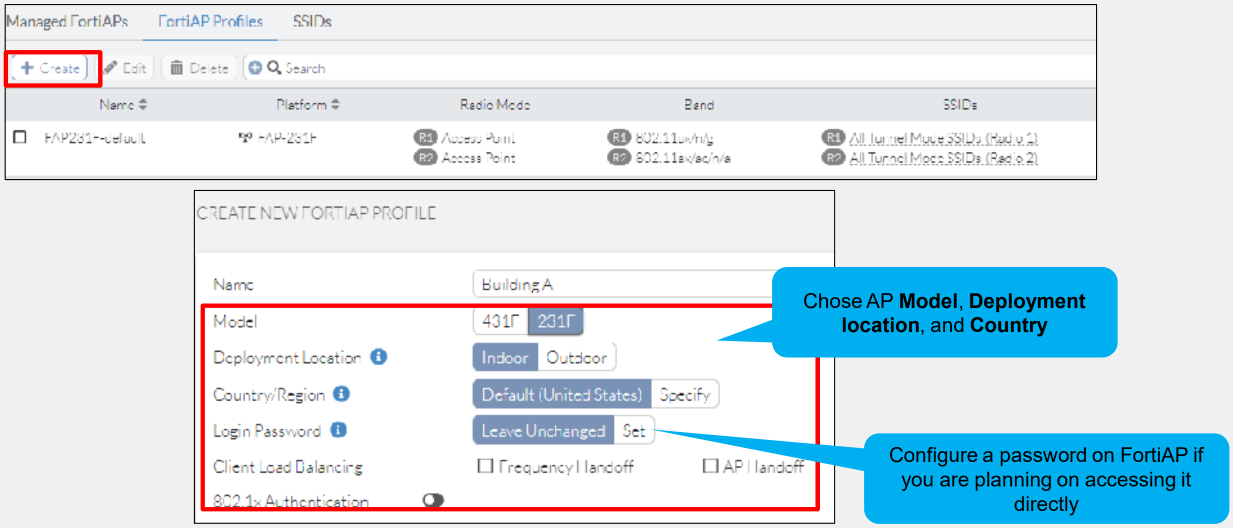
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET

Brave-dumps.com

Custom FortiAP Profile

Edge Devices > FortiAPs > FortiAP Profiles



Managed FortiAPs | FortiAP Profiles | SSIDs

	Name	Platform	Radio Mode	Band	SSIDs
□	FAP231F-default	FAP-231F	R1 Access Point R2 Access Point	R1 802.11ax/n/g R2 802.11ax/ac/n/a	R1 All Tunnel Mode SSIDs (Radio 1) R2 All Tunnel Mode SSIDs (Radio 2)

CREATE NEW FORTIAP PROFILE

Name	Building A
Model	431F [✓ 231F]
Deployment Location	[✓ Indoor] Outdoor
Country/Region	[✓ Default (United States)] Specify
Login Password	[✓ Leave Unchanged] Set
Client Load Balancing	□ Frequency Handoff □ AP Handoff
802.1x Authentication	○

Chose AP **Model**, **Deployment location**, and **Country**

Configure a password on FortiAP if you are planning on accessing it directly

© Fortinet Inc. All Rights Reserved.

FortiSASE allows you to configure a custom AP profile that controls all the settings that it pushes to an AP. You must select the correct model to tell FortiSASE what type of hardware the AP uses.

The **Country/Region** field provides radio frequency (RF) channels available in your area. By default, the country is set to United States. Each country has different radio regulations and, to comply with these regulations, you should select the correct **Country/Region**.

Client Load Balancing can assist with distributing the load across APs, using either **Frequency Handoff** or **AP Handoff**.

FortiAP can act as an 802.1X supplicant to authenticate against the RADIUS server using EAP-FAST, EAP-TLS, or EAP-PEAP. This setting is for FortiAP devices connected to a switch port with 802.1X authentication enabled.

Vouchers & Dumps are Available | WhatsApp +201224560923

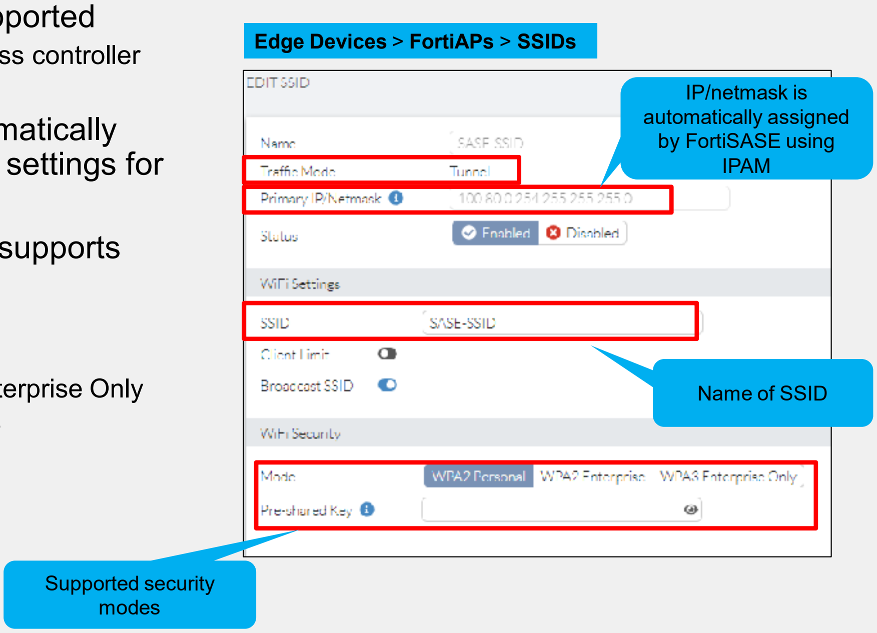
DO NOT REPRINT
© FORTINET

Brave-dumps.com

SSID

- Only traffic mode tunnel is supported
  - Traffic is tunneled back to wireless controller using CAPWAP data channel
- FortiSASE uses IPAM to automatically configure IP address/netmask settings for an SSID
- FortiSASE wireless controller supports the following security modes:
  - WPA2 Personal
    - Pre-shared keys
  - WPA2 Enterprise and WPA3 Enterprise Only
    - RADIUS-based security modes
      - User group
      - Remote RADIUS server

Edge Devices > FortiAPs > SSIDs



EDIT SSID

Name: SASE-SSID

Traffic Mode: Tunnel

Primary IP/Netmask: 100.80.0.254 255.255.255.0

Status: Enabled | Disabled

WiFi Settings

SSID: SASE-SSID

Client Limit

Broadcast SSID

WiFi Security

Mode: WPA2 Personal | WPA2 Enterprise | WPA3 Enterprise Only

Pre-shared Key

IP/netmask is automatically assigned by FortiSASE using IPAM

Name of SSID

Supported security modes

FURTINET Training Institute

© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved. 14

By default, tunnel mode SSID is created when you define an SSID on FortiSASE. In tunnel mode, all the traffic is tunneled back to the FortiSASE wireless controller using a CAPWAP data channel. FortiSASE uses IP address management (IPAM) to automatically configure IP address/netmask settings for an SSID.

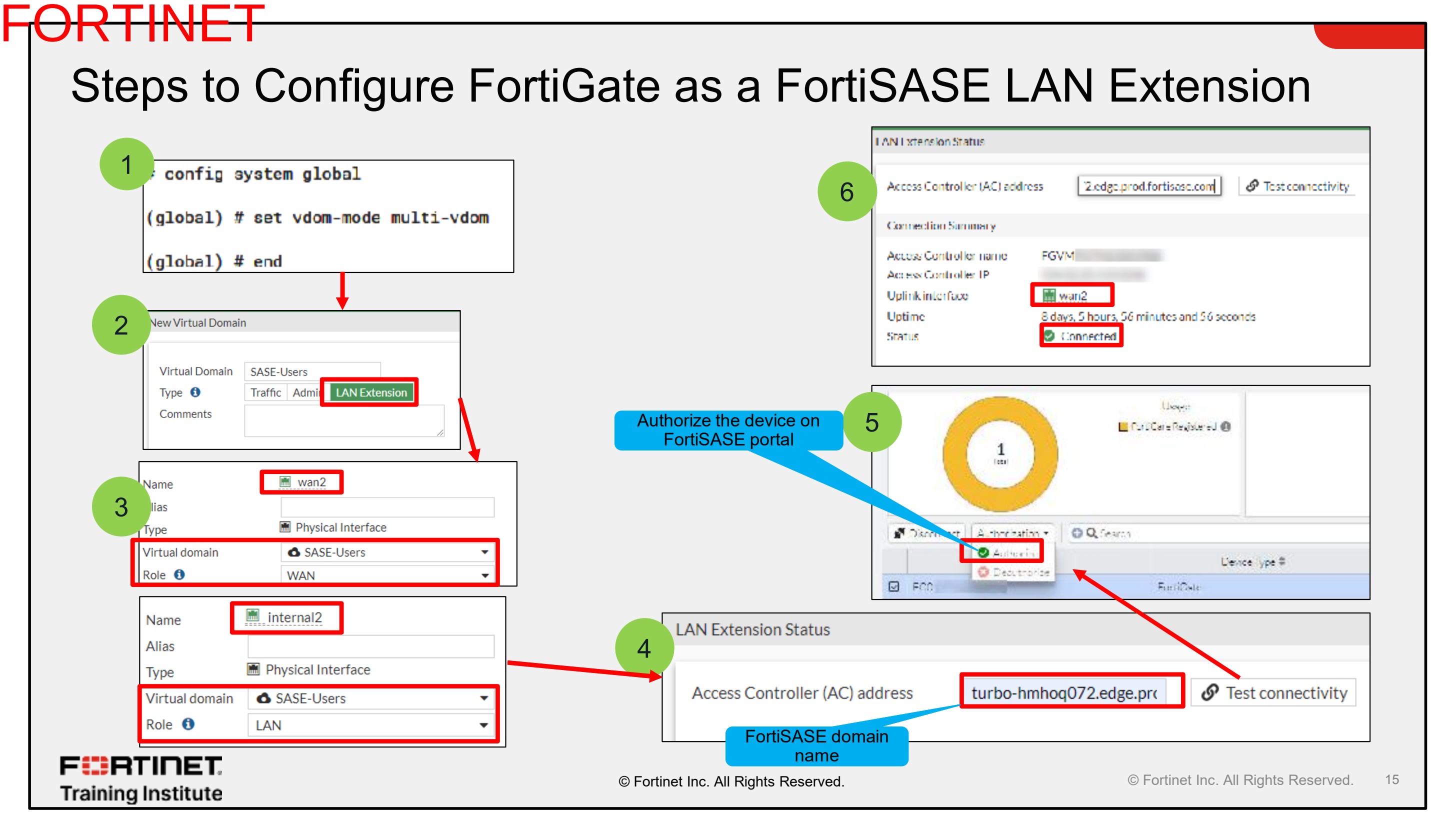
WPA2 security with a pre-shared key for authentication is called **WPA2 Personal**. This mode can work well for one person or a small group of trusted people. But, as the number of users increases, it is difficult to distribute new keys securely and there is increased risk that the key could fall into the wrong hands.

WPA2 Enterprise and **WPA3 Enterprise Only** are RADIUS-based security modes. These are the standards any enterprise class network should be using. If you have a database of users with a RADIUS front end, this is what to use. Encryption and authentication are strongest in an enterprise network. FortiSASE supports two types of RADIUS deployment: user groups and remote RADIUS server.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET

Brave-dumps.com



Steps to Configure FortiGate as a FortiSASE LAN Extension

1

```
# config system global
(global) # set vdom-mode multi-vdom
(global) # end
```

2

New Virtual Domain

Virtual Domain: SASE-Users
Type: Traffic | Admin | LAN Extension
Comments:

3

Name: wan2
Alias:
Type: Physical Interface
Virtual domain: SASE-Users
Role: WAN

Name: internal2
Alias:
Type: Physical Interface
Virtual domain: SASE-Users
Role: LAN

4

LAN Extension Status

Access Controller (AC) address: turbo-hmhoq072.edge.prc
Test connectivity

FortiSASE domain name

5

Authorize the device on FortiSASE portal

6

LAN Extension Status

Access Controller (AC) address: 2.edge.prod.fortisase.com
Test connectivity

Connection Summary

Access Controller name: FGVM[redacted]
Access Controller IP: [redacted]
Uplink interface: wan2
Uptime: 8 days, 5 hours, 56 minutes and 56 seconds
Status: Connected

© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved.

To configure FortiGate as FortiSASE LAN extension, follow these general steps:

1. On the secure edge FortiGate, enable multi-VDOM.
2. Create a new VDOM with type **LAN extension** on the **SYSTEM** > **VDOM** page.
3. Move a minimum of two interfaces from the root VDOM to the newly created LAN extension VDOM. Configure one with the role **WAN** and the other with the role **LAN**. Configure the WAN interface with routing to reach the internet. The interface with the role LAN is where the client PCs connect to for SIA through FortiSASE.
4. To obtain the FortiSASE domain name from the FortiSASE portal, click **Edge Devices** > **FortiGates,** then click **Connect FortiGates,** and then copy the domain name. On the secure edge FortiGate in the newly created LAN extension VDOM, click **Network** > **LAN Extension**, paste the FortiSASE domain name, and then click **Test connectivity.**
5. To authorize the secure edge FortiGate, in the FortiSASE portal, click **Edge Devices** > **FortiGates,** select the FortiGate, and then click **Authorize**.
6. To verify the **Connection Summary** on the secure edge FortiGate, click **Network** > **LAN Extension**.

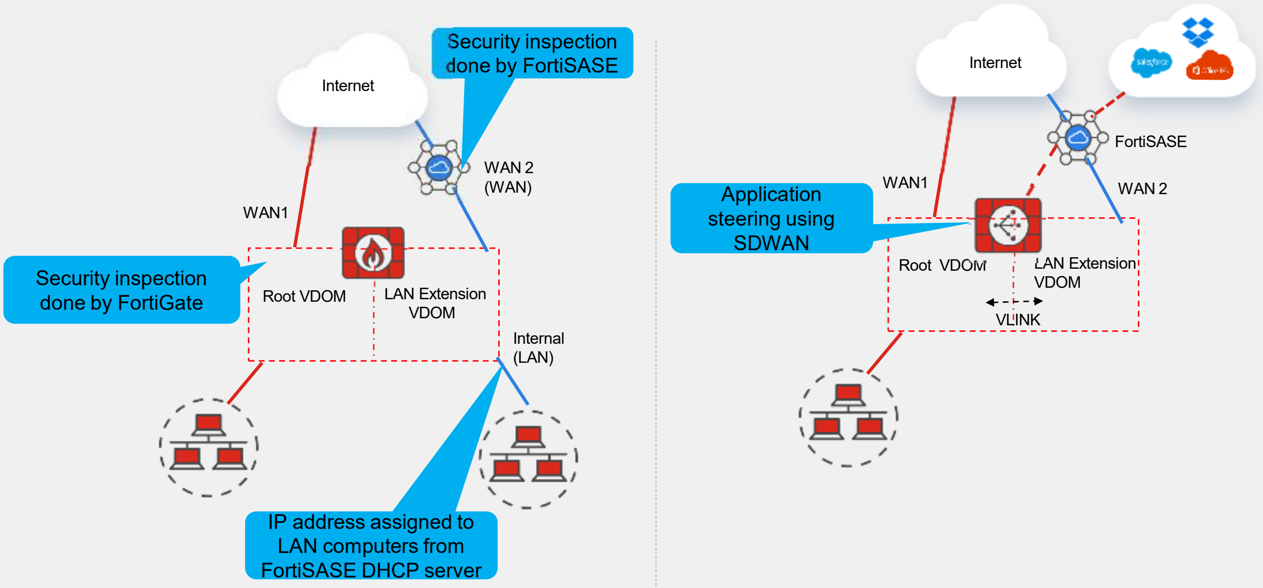
When you configure the LAN extension VDOM on the secure edge FortiGate, FortiOS automatically configures a VDOM link (VLINK) between a traffic VDOM, which is by default the root VDOM, and the LAN extension VDOM.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET

Brave-dumps.com

Secure Edge FortiGate Topologies



Security inspection done by FortiSASE

Security inspection done by FortiGate

IP address assigned to LAN computers from FortiSASE DHCP server

Application steering using SDWAN

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved. 16

When you deploy an edge FortiGate as a FortiSASE LAN extension, FortiSASE can inspect traffic for users connected to the LAN extension VDOM. Edge FortiGate inspects traffic for users connected to the default root VDOM. This can help offload some of the security inspection tasks from the edge FortiGate.

You can also use the SD-WAN functionality on the edge FortiGate to apply application steering to FortiSASE. You can add the local internet interface on the root VDOM and the VLINK interface between the root VDOM and LAN extension VDOM along with the specific applications to the SD-WAN rule.

Vouchers & Dumps are Available | WhatsApp +201224560923

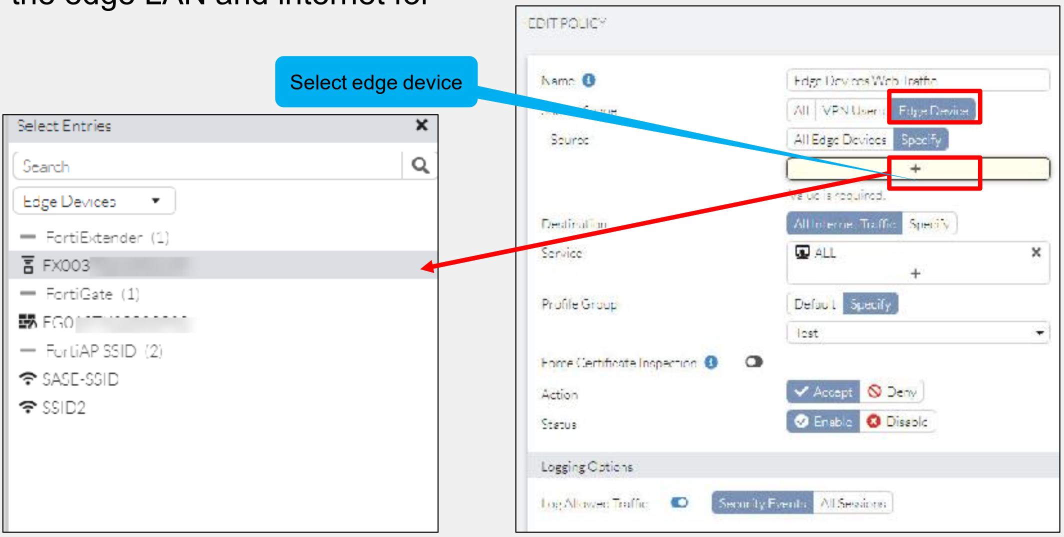
DO NOT REPRINT
© FORTINET

Brave-dumps.com

Configuring Policies—Edge Devices

- An edge device policy controls the traffic between the edge LAN and internet for SIA

Configuration > TRAFFIC > Policies > Internet Access



Select edge device

Select Entries

- FortiExtender (1)
- FX003 [redacted]
- FortiGate (1)
- FG0 [redacted]
- FortiAP SSID (2)
- SASE-SSID
- SSID2

EDIT POLICY

Name: Edge Devices Web Traffic

All | VPN Users | Edge Device

Source: All Edge Devices | Specify

Value is required.

Destination: All Internet Traffic | Specify

Service: ALL

Profile Group: Default | Specify

test

Force Certificate Inspection

Action: Accept | Deny

Status: Enable | Disable

Logging Options

Log Allowed Traffic: Security Events | All Sessions

© Fortinet Inc. All Rights Reserved.

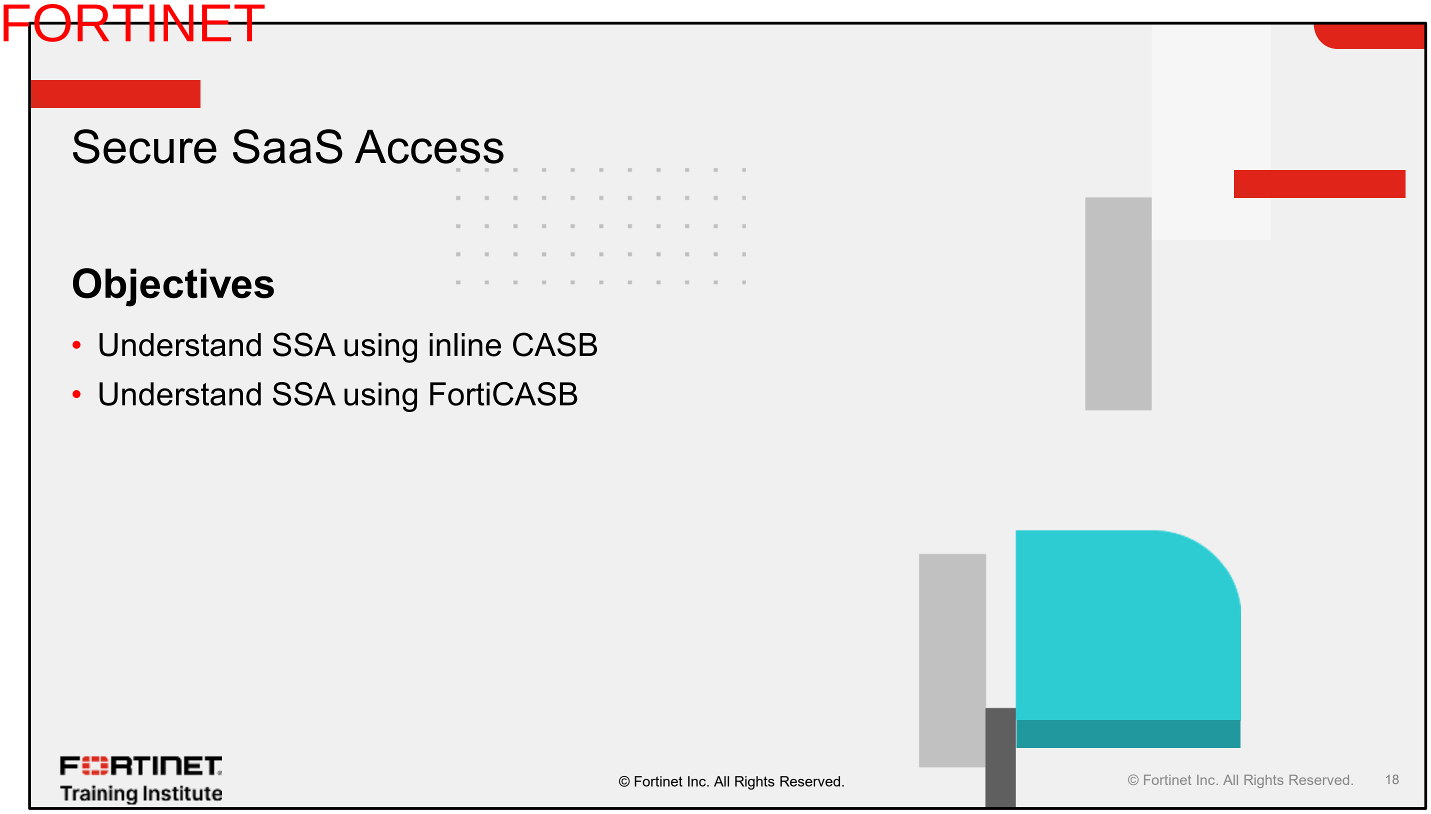
© Fortinet Inc. All Rights Reserved.

Policies with edge scope control the traffic that goes through edge devices, such as FortiExtender, FortiAP, and FortiGate. No FortiClient installation is required in this deployment, therefore it doesn't support ZTNA tags.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET

Brave-dumps.com



Secure SaaS Access

Objectives

- Understand SSA using inline CASB
- Understand SSA using FortiCASB

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved.

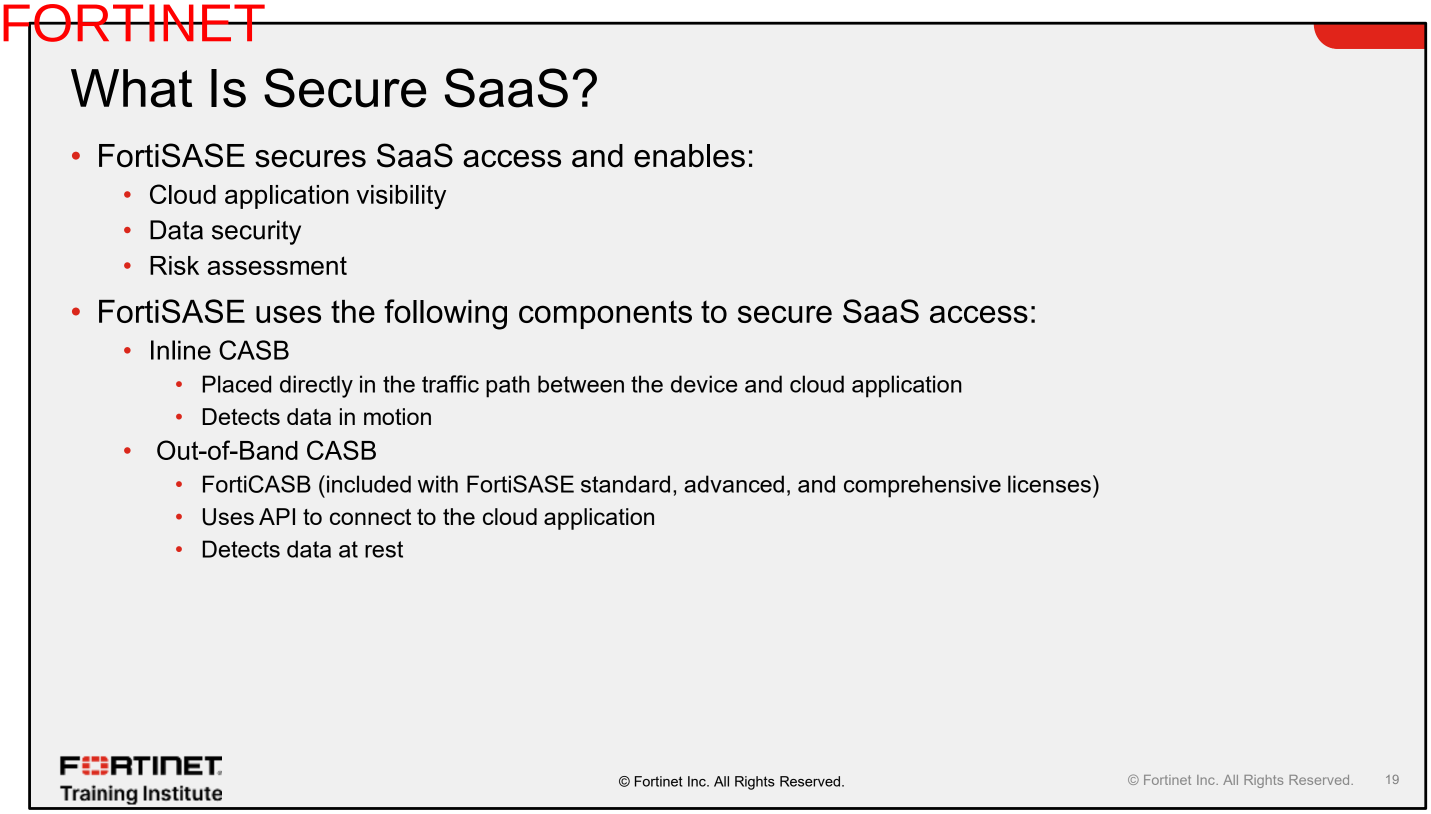
After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating a competent understanding of SSA, you will be able identify use cases for SSA.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET

Brave-dumps.com



What Is Secure SaaS?

- FortiSASE secures SaaS access and enables:
  - Cloud application visibility
  - Data security
  - Risk assessment
- FortiSASE uses the following components to secure SaaS access:
  - Inline CASB
    - Placed directly in the traffic path between the device and cloud application
    - Detects data in motion
  - Out-of-Band CASB
    - FortiCASB (included with FortiSASE standard, advanced, and comprehensive licenses)
    - Uses API to connect to the cloud application
    - Detects data at rest

FURTINET Training Institute

© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved. 19

Given the rapid increase in SaaS adoption, organizations continue to struggle with shadow IT challenges and stopping data exfiltration. FortiSASE is a superior SASE offering that includes SSA with next-generation, dual-mode cloud access security broker (CASB), using both inline and out-of-band support. It provides comprehensive visibility by identifying key SaaS applications and reporting risky applications to overcome shadow IT challenges.

FortiSASE secures SaaS access and enables:

- Cloud application visibility: Discover the usage of cloud applications across all sanctioned and unsanctioned (shadow IT) cloud applications to help enforce policy-based controls.
- Data security: Protect data in motion and at rest within cloud applications. Control productivity, privacy, compliance, and security of corporate and non-corporate tenants.
- Assess risk: Evaluate application usage spikes to determine risk and ensure corporate data is handled safely.

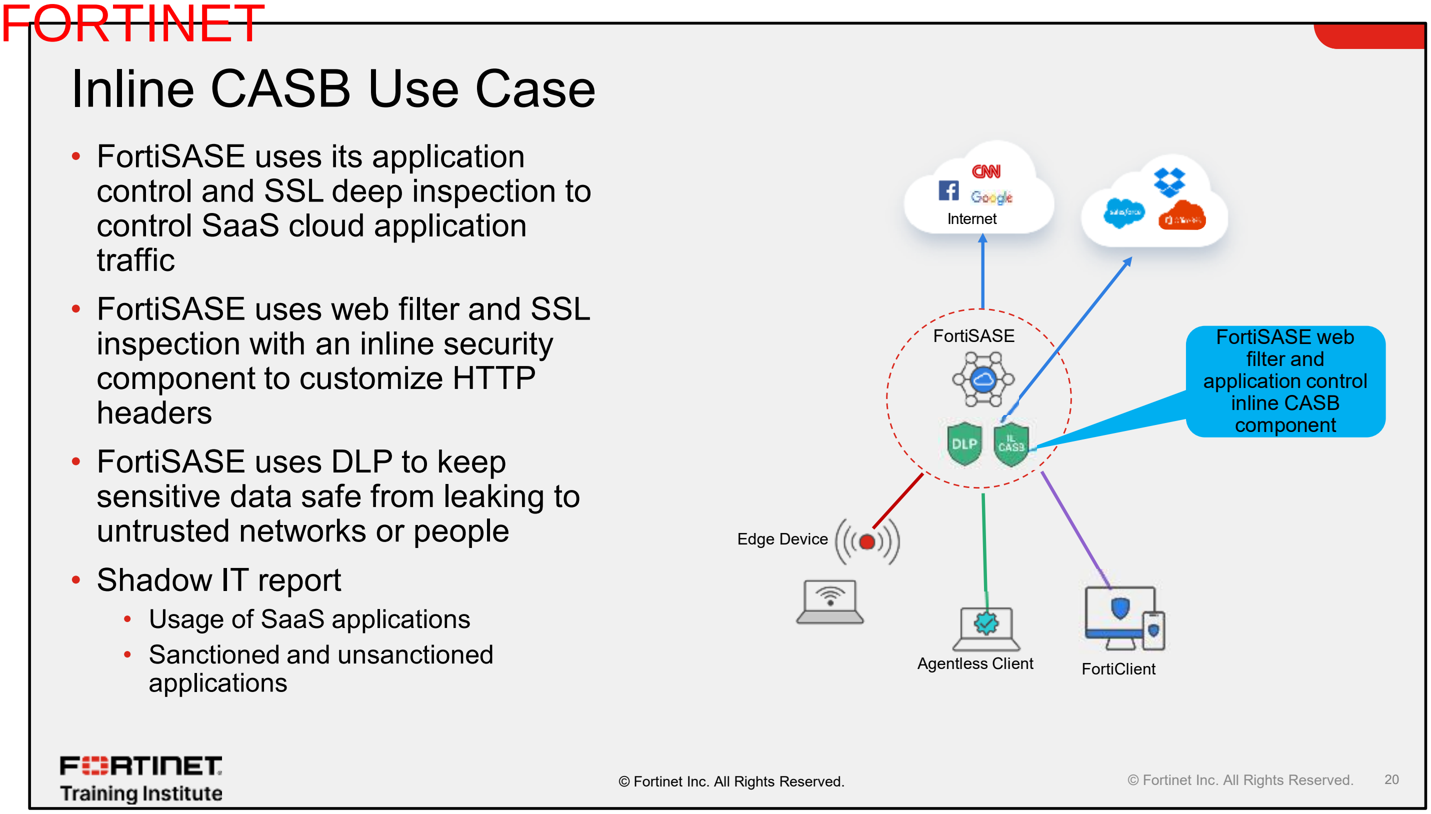
FortiSASE includes an inline CASB component to detect data in motion, meaning it scans the data as it passes through to the cloud application from the endpoint device.

Out-of-band CASB utilizes API to connect to the cloud application. Out-of-band CASB scans the data at rest, meaning the data has already been uploaded to the SaaS application. FortiCASB is included with per-user and per-endpoint FortiSASE licensing.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET

Brave-dumps.com



Inline CASB Use Case

- FortiSASE uses its application control and SSL deep inspection to control SaaS cloud application traffic
- FortiSASE uses web filter and SSL inspection with an inline security component to customize HTTP headers
- FortiSASE uses DLP to keep sensitive data safe from leaking to untrusted networks or people
- Shadow IT report
  - Usage of SaaS applications
  - Sanctioned and unsanctioned applications

FortiSASE web filter and application control inline CASB component

© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved.

Inline CASB recognizes network traffic that many applications generate. Application control with inline CASB using IPS protocol decoders can analyze network traffic to detect application traffic, even if the traffic uses nonstandard ports or protocols. Application control with inline CASB supports traffic detection using HTTP (versions 1.0, 1.1, and 2.0). FortiSASE uses web filter and SSL deep inspection to intercept HTTP headers and can modify them for outgoing traffic. By customizing HTTP headers for FortiSASE outgoing traffic destined for SaaS applications, the web filter with inline CASB can control SaaS application behavior by restricting tenant access.

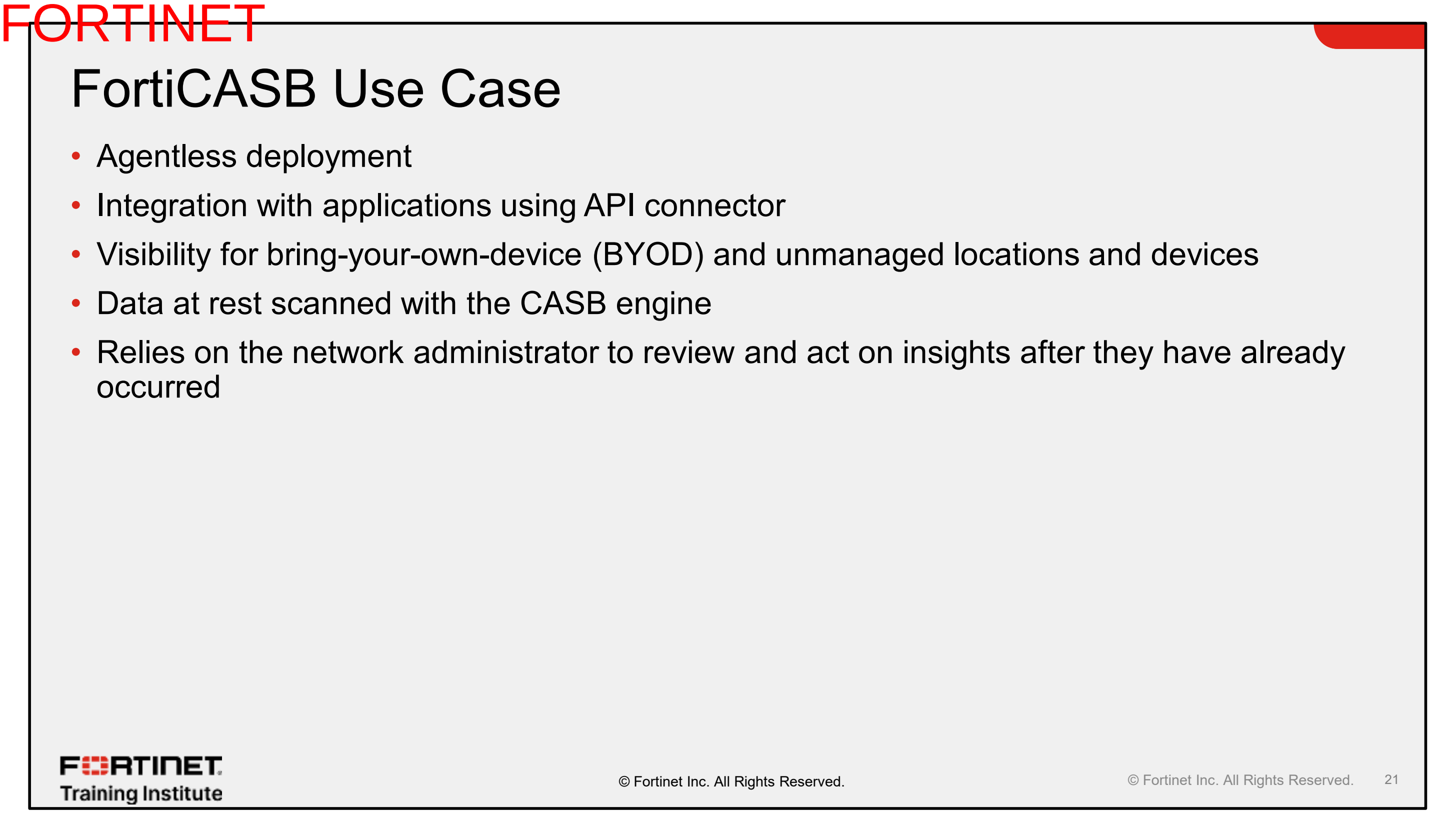
FortiSASE also uses data leak prevention (DLP) to prevent sensitive data from leaving or entering your network by defining various sensitive data patterns, scanning for the patterns while inspecting traffic, and allowing, blocking, or logging only when traffic matches the patterns.

You will learn to configure these features in a later lesson.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET

Brave-dumps.com



FortiCASB Use Case

- Agentless deployment
- Integration with applications using API connector
- Visibility for bring-your-own-device (BYOD) and unmanaged locations and devices
- Data at rest scanned with the CASB engine
- Relies on the network administrator to review and act on insights after they have already occurred

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

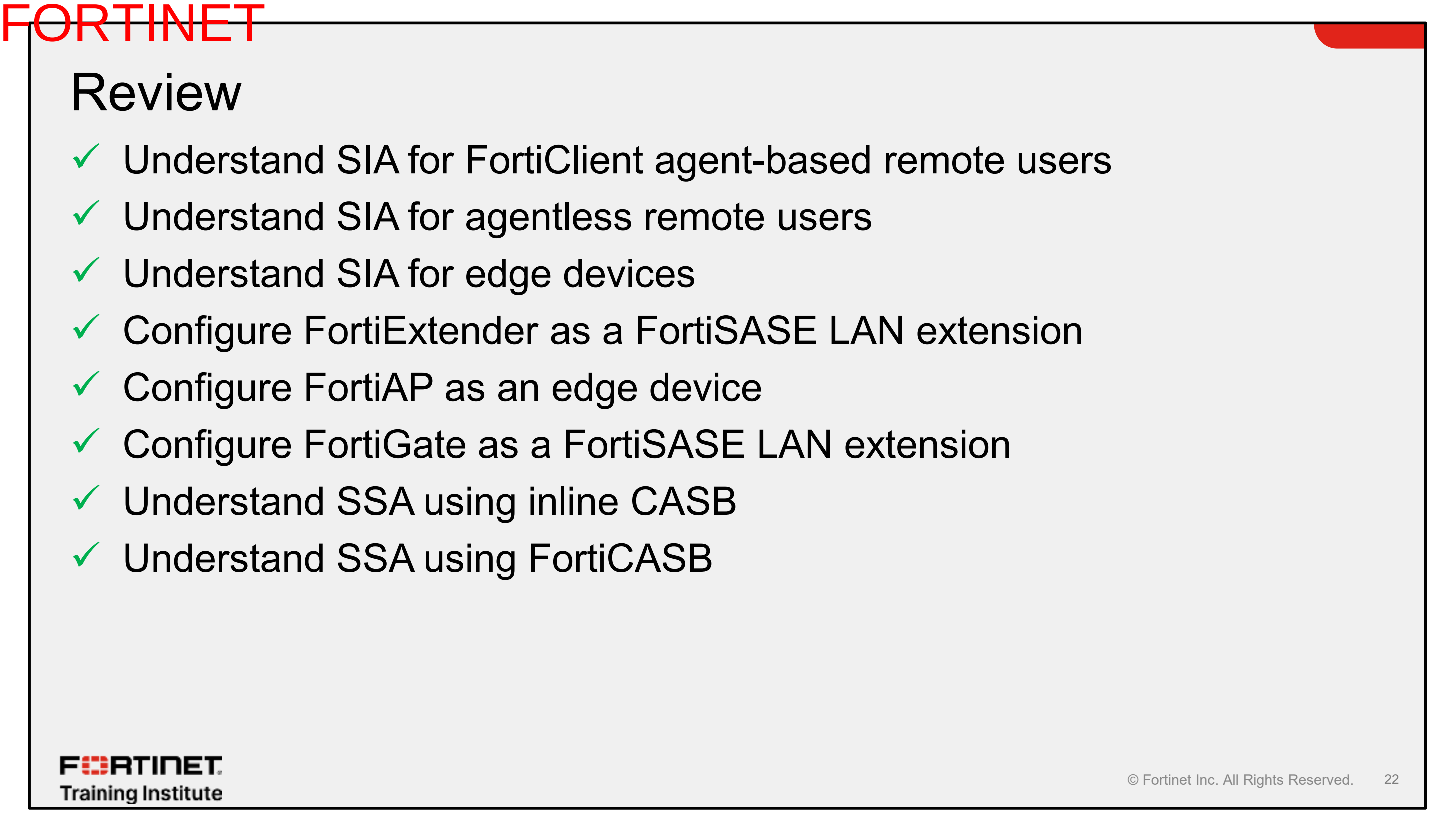
© Fortinet Inc. All Rights Reserved. 21

FortiCASB provides visibility, compliance, data security, and threat protection for cloud applications. Using direct API access, it enables deep inspection and policy management for data stored in SaaS and Infrastructure-as-a-Service (IaaS) applications. It also provides advanced tools that provide detailed user analytics and centralized management to ensure policies are enforced and your organization’s data isn’t getting into the wrong hands. It relies on the network administrator to review and act upon these insights after they have already occurred. Mitigation actions include making configuration changes on FortiSASE to block future suspicious activity, denying or restricting a user’s access on the SaaS application itself for the specific user generating the suspicious activity.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET

Brave-dumps.com



Review

- ✓ Understand SIA for FortiClient agent-based remote users
- ✓ Understand SIA for agentless remote users
- ✓ Understand SIA for edge devices
- ✓ Configure FortiExtender as a FortiSASE LAN extension
- ✓ Configure FortiAP as an edge device
- ✓ Configure FortiGate as a FortiSASE LAN extension
- ✓ Understand SSA using inline CASB
- ✓ Understand SSA using FortiCASB

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 22

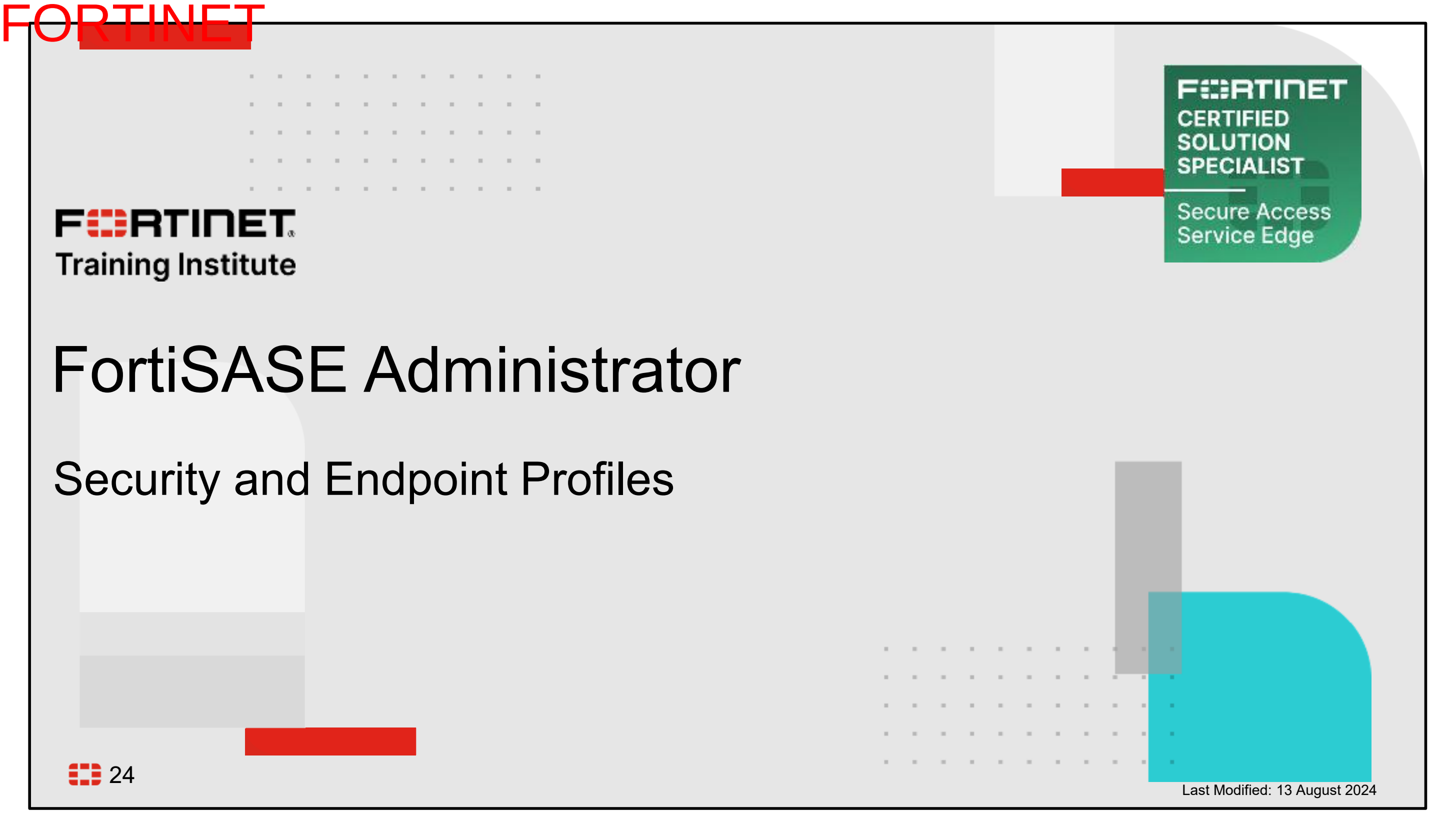
This slide shows the objectives that you covered in this lesson.

By mastering the objectives covered in this lesson, you will be able to describe the common use cases of SIA and SSA in a FortiSASE deployment.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET

Brave-dumps.com



FORTINET
Training Institute

FORTINET CERTIFIED SOLUTION SPECIALIST
Secure Access Service Edge

FortiSASE Administrator

Security and Endpoint Profiles

24

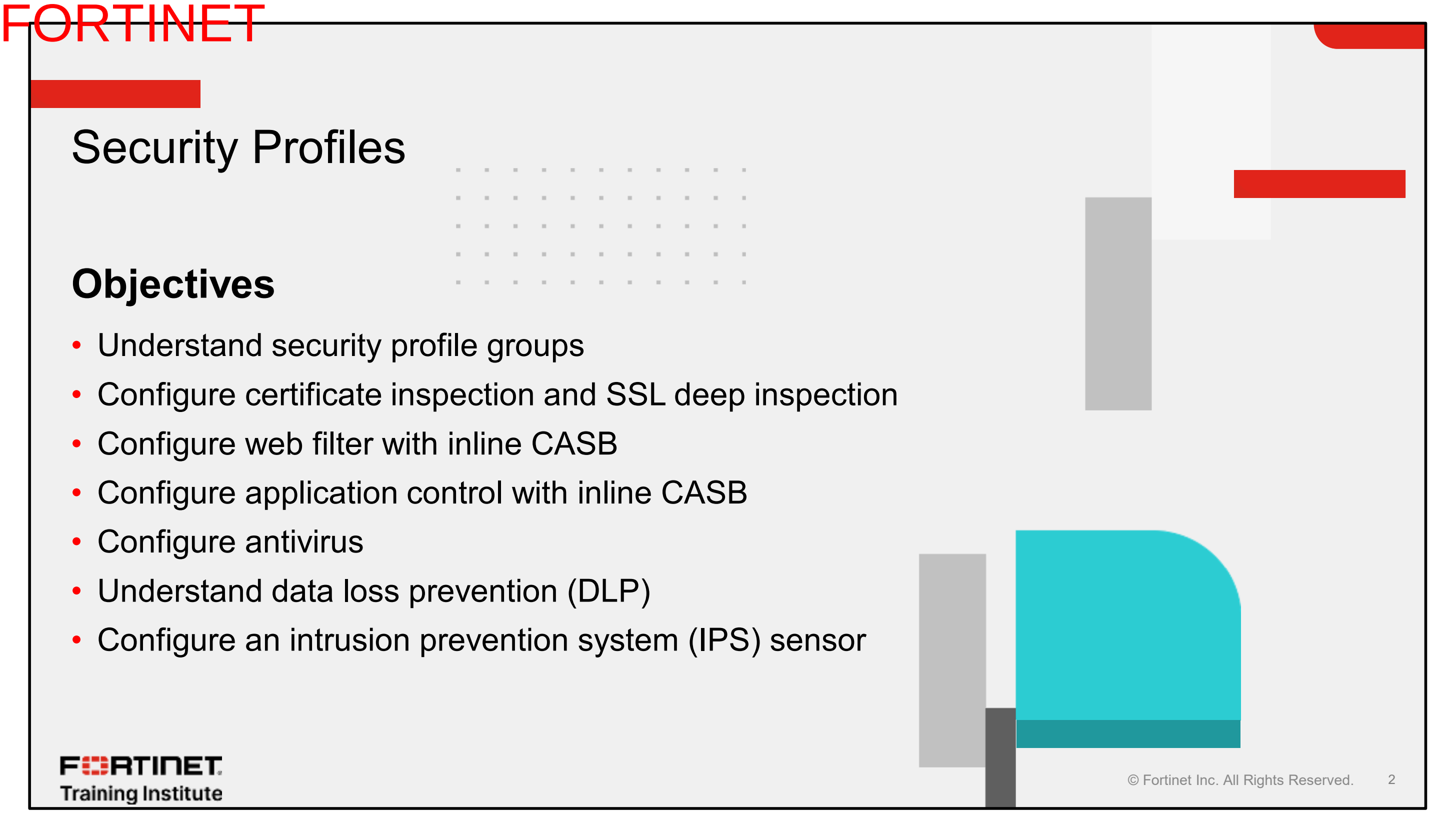
Last Modified: 13 August 2024

In this lesson, you will learn about security and endpoint profiles on FortiSASE.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET

Brave-dumps.com



Security Profiles

Objectives

- Understand security profile groups
- Configure certificate inspection and SSL deep inspection
- Configure web filter with inline CASB
- Configure application control with inline CASB
- Configure antivirus
- Understand data loss prevention (DLP)
- Configure an intrusion prevention system (IPS) sensor

© Fortinet Inc. All Rights Reserved. 2

After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in understanding the basic configuration of security profiles you will be able to apply security profile groups in your FortiSASE policies.

Vouchers & Dumps are Available | WhatsApp +201224560923

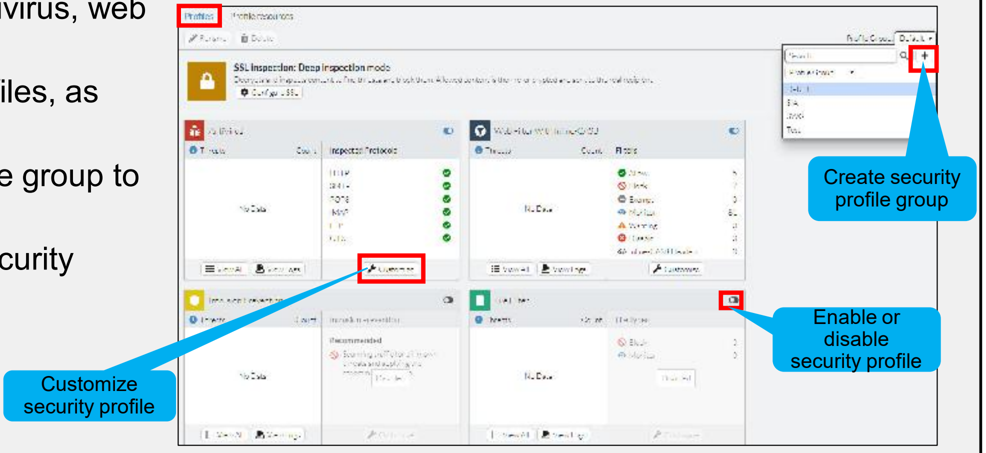
DO NOT REPRINT
© FORTINET

Brave-dumps.com

Security Profile Groups

- Group different security profiles (application control, antivirus, web filter, and so on)
- Customize security profiles, as needed
- Apply the security profile group to a policy
- Can create separate security profile groups

Configuration > TRAFFIC > Security > Profiles



SSL Inspection: Deep Inspection mode

Create security profile group

Enable or disable security profile

Customize security profile

© Fortinet Inc. All Rights Reserved.

You can create security profile groups on the **Security** page. Security profile groups allow you to group different security profile settings. You can then configure the profile group as part of a policy. You can customize and enable or disable security profiles within the security group. You can create separate security profile groups for different policies, depending on the requirements your organization. FortiSASE has a preconfigured default profile that you can’t delete.

The following security profiles are available in a security profile group:

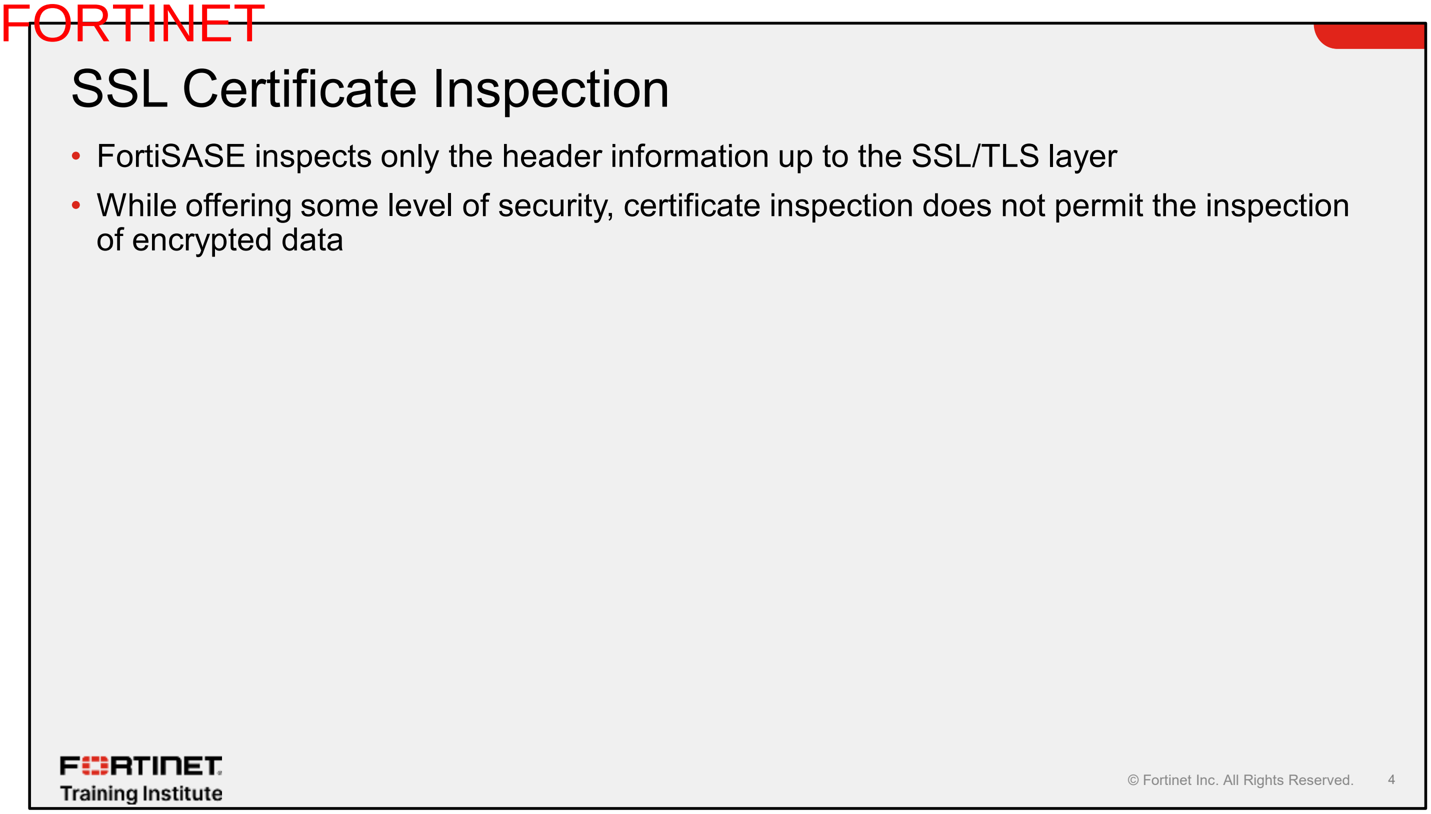
- SSL Inspection
- Antivirus
- Web Filtering With Inline-CASB
- File Filter
- Intrusion Prevention
- Data Loss Prevention
- DNS Filter
- Application Control With Inline-CASB

You will learn about some of the security profiles in this lesson.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET

Brave-dumps.com



SSL Certificate Inspection

- FortiSASE inspects only the header information up to the SSL/TLS layer
- While offering some level of security, certificate inspection does not permit the inspection of encrypted data

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved. 4

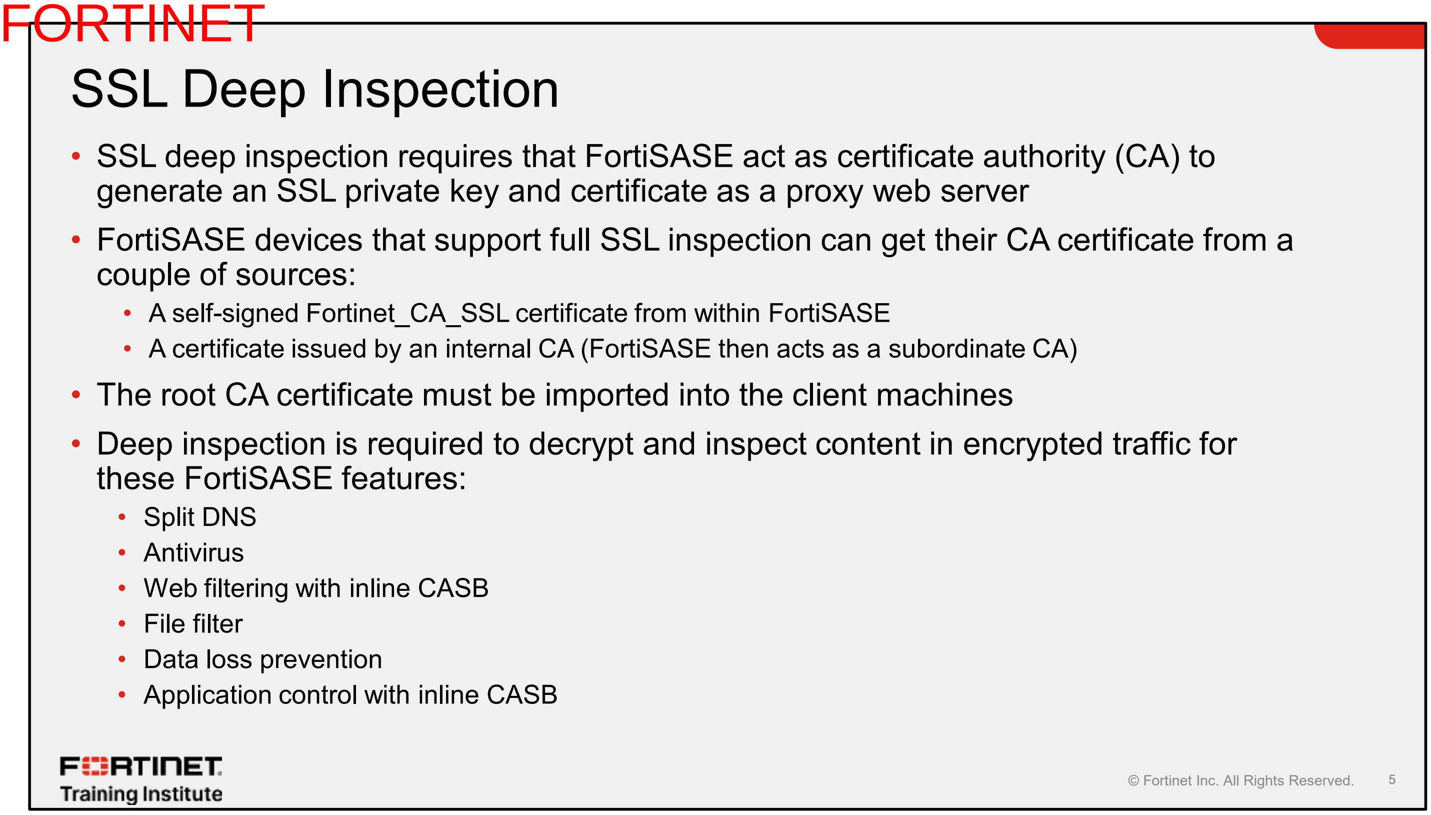
When you use certificate inspection, FortiSASE inspects only the header information of the packets. You use certificate inspection to verify the identity of web servers. You can also use it to make sure that the HTTPS protocol isn't used as a workaround to access sites you have blocked using web filtering.

Certificate inspection offers some level of security, but it does *not* allow FortiSASE to inspect the flow of encrypted data between the outside server and the internal client.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET

Brave-dumps.com



SSL Deep Inspection

- SSL deep inspection requires that FortiSASE act as certificate authority (CA) to generate an SSL private key and certificate as a proxy web server
- FortiSASE devices that support full SSL inspection can get their CA certificate from a couple of sources:
  - A self-signed Fortinet_CA_SSL certificate from within FortiSASE
  - A certificate issued by an internal CA (FortiSASE then acts as a subordinate CA)
- The root CA certificate must be imported into the client machines
- Deep inspection is required to decrypt and inspect content in encrypted traffic for these FortiSASE features:
  - Split DNS
  - Antivirus
  - Web filtering with inline CASB
  - File filter
  - Data loss prevention
  - Application control with inline CASB

Training Institute

© Fortinet Inc. All Rights Reserved. 5

FortiSASE performs web proxy and must act as a CA in order for it to perform SSL deep inspection. The internal CA must generate an SSL private key and certificate each time an internal user connects to an external SSL server. The key pair and certificate are generated *immediately* so the user connection with the web server is not delayed.

Although it appears as though the user browser is connected to the web server, the browser is connected to FortiSASE. FortiSASE is acting as a proxy web server. In order for FortiSASE to act in these roles, its CA certificate must have the basic constraints extension set to **cA=True** and the value of the **keyUsage** extension set to **keyCertSign**.

The **cA=True** value identifies the certificate as a CA certificate. The **keyUsage=keyCertSign** value indicates that the private key corresponding to the certificate is permitted to sign certificates. For more information, see *RFC 5280 Section 4.2.1.9 Basic Constraints*.

All FortiSASE devices that support SSL deep inspection can use the self-signed Fortinet_CA_SSL certificate that is provided with FortiSASE, or an internal CA, to issue FortiSASE a CA certificate. When FortiSASE uses an internal CA, FortiSASE acts as a subordinate CA. Note that your client machines and devices must import the root CA certificate in order to trust FortiSASE and accept an SSL session.

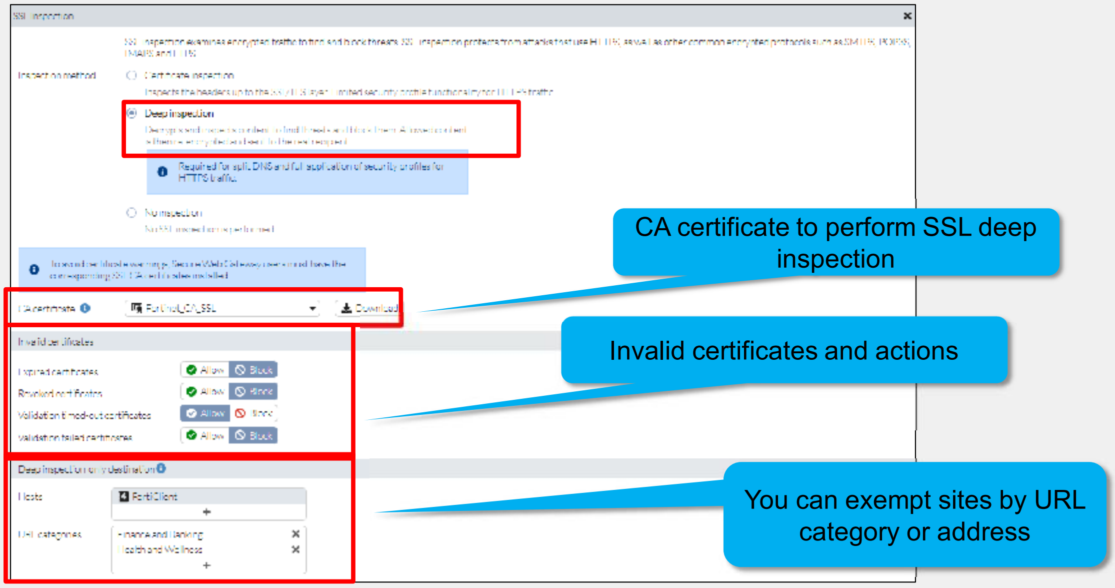
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET

Brave-dumps.com

Configure SSL Inspection

Security > Profiles > SSL Inspection



SSL inspection

SSL inspection examines encrypted traffic to find and block threats. SSL inspection protects from attacks that use HTTPS as well as other common encrypted protocols such as SMTPS, POP3S, IMAPS and FTPS.

Inspection method

○ Certificate inspection
Inspects the headers up to the SSL/TLS layer. Limited security profile functionality for HTTPS traffic.

● Deep inspection
Decrypts and inspects content to find threats and block them. All inspected content is then re-encrypted and sent to the real recipient.

Required for split DNS and full application of security profiles for HTTPS traffic.

○ No inspection
No SSL inspection is performed.

To avoid certificate warnings, Secure Web Gateway users must have the corresponding SSL CA certificates installed.

CA certificate: Fortinet_CA_SSL — Download

Invalid certificates

Expired certificates	Allow [✓ Block]
Revoked certificates	Allow [✓ Block]
Validation timed-out certificates	[✓ Allow] Block
Validation failed certificates	Allow [✓ Block]

Deep inspection only destination

Hosts: FortiClient

URL categories: Finance and Banking, Health and Wellness

CA certificate to perform SSL deep inspection

Invalid certificates and actions

You can exempt sites by URL category or address

Training Institute

© Fortinet Inc. All Rights Reserved. 6

You can configure SSL inspection on the **Security** page by selecting the appropriate security profile group. You can click **Customize** in the SSL inspection profile and then select **Certificate Inspection** to enable certificate inspection. To enable deep inspection, select **Deep Inspection**, and then select the CA certificate to perform SSL deep inspection. You can upload your own CA certificate to use with SSL deep inspection on the **System** > **Certificates** page.

FortiSASE can detect certificates that are invalid for the following reasons:

- Expired: The certificate is expired.
- Revoked: The certificate has been revoked based on CRL or OCSP information.
- Validation timeout: The certificate could not be validated because of a communication timeout.
- Validation failed: The certificate could not be validated because of a communication error.

When a certificate fails for any of the reasons above, you can configure any of the following actions:

- **Allow**: FortiSASE allows the website and takes the certificate as *trusted*.
- **Block**: FortiSASE blocks the content of the site.

Within the deep inspection profile, you can also specify which FortiGuard categories or hosts, if any, you want to exempt from SSL inspection. You may need to exempt traffic from SSL inspection if it is causing problems with traffic, or for legal reasons.

Vouchers & Dumps are Available | WhatsApp +201224560923

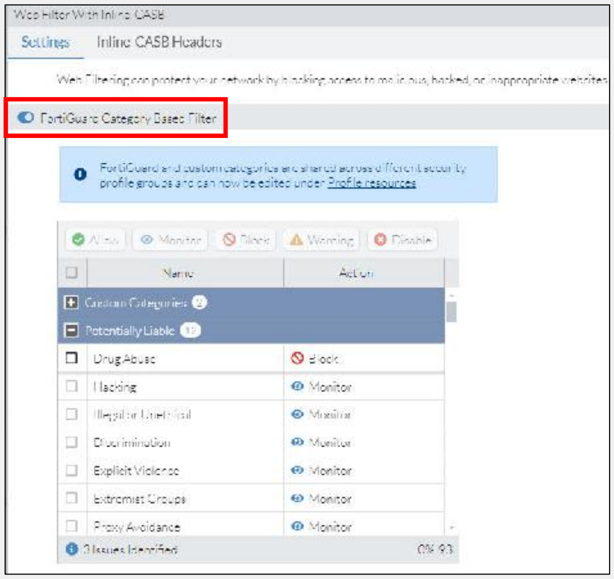
DO NOT REPRINT
© FORTINET

Brave-dumps.com

Web Filter—FortiGuard Category Filter

- FortiGuard category filter
  - Provides categories from the FortiGuard Web Filter service that you can use to filter web traffic
  - Split into multiple categories and subcategories

Security > Profiles > Web Filter With Inline-CASB



Web Filter With Inline-CASB

Web Filtering can protect your network by blocking access to malicious, hacked, or inappropriate websites

FortiGuard Category Based Filter

FortiGuard and custom categories are shared across different security profile groups and can now be edited under Profile resources

□	Name	Action
⊞	Custom Categories 2	
⊟	Potentially Liable 12	
□	Drug Abuse	Block
□	Hacking	Monitor
□	Illegal or Unethical	Monitor
□	Discrimination	Monitor
□	Explicit Violence	Monitor
□	Extremist Groups	Monitor
□	Proxy Avoidance	Monitor

3 Issues Identified 0% 93

© Fortinet Inc. All Rights Reserved. 7

You can configure the **Web Filter With Inline-CASB** profile on the **Security** page by selecting the appropriate security profile group. Rather than blocking or allowing websites individually, FortiGuard category filtering reviews the category that a website has been rated with. Then, FortiSASE takes action based on that category, not based on the URL. In addition, by default, FortiSASE blocks web pages that return a rating error. You can change this behavior by enabling **Allow websites when a rating error occurs**.

You can enable the FortiGuard category filtering on the web filter. Categories and subcategories are listed, and you can customize the actions to perform individually.

The following actions are available:

- **Allow**: passes the traffic to the remaining web filters, antivirus inspection engine, and DLP inspection engine. If the URL does not appear in the URL list, FortiSASE allows the traffic.
- **Monitor**: processes the traffic the same way as the allow action. For the monitor action, FortiSASE generates a log message each time it establishes a matching traffic pattern.
- **Block**: denies or blocks attempts to access any URL that belongs to the category. A replacement message is displayed.
- **Warning**: displays a message to the user allowing them to continue if they choose.

Vouchers & Dumps are Available | WhatsApp +201224560923

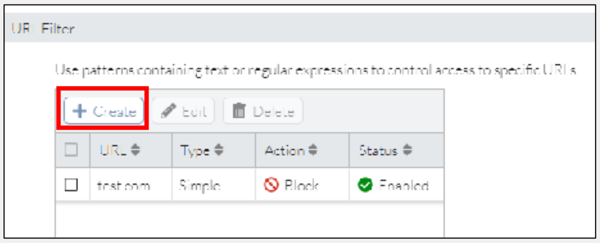
DO NOT REPRINT
© FORTINET

Brave-dumps.com

Web Filter—URL Filtering

- URL filter
  - Check against configured URLs in the URL filter
    - Entries are checked from top to bottom
  - Types of URL patterns:
    - Simple, wildcards, or regular expressions

Security > Profiles > Web Filter With Inline-CASB



URL Filter

Use patterns containing text or regular expressions to control access to specific URLs

□	URL	Type	Action	Status
□	test.com	Simple	Block	✓ Enabled

© Fortinet Inc. All Rights Reserved.

Static URL filtering is another web filter feature. FortiSASE checks configured URLs in the URL filter against the visited websites. If FortiSASE finds a match, it takes the configured action. URL filtering has the following pattern matches: simple, regular expressions, and wildcard.

The following actions are available:

- **Allow**: passes the traffic to the remaining web filters, antivirus inspection engine, and DLP inspection engine. If the URL does not appear in the URL list, FortiSASE allows the traffic.
- **Block**: denies or blocks attempts to access any URL that matches the URL pattern. A replacement message displays.
- **Exempt**: allows the traffic to pass through, bypassing other web filters, the antivirus inspection engine, and the DLP inspection engine.
- **Monitor**: processes the traffic the same way as the allow action. For the monitor action, FortiSASE generates a log message each time it establishes a matching traffic pattern.

Vouchers & Dumps are Available | WhatsApp +201224560923

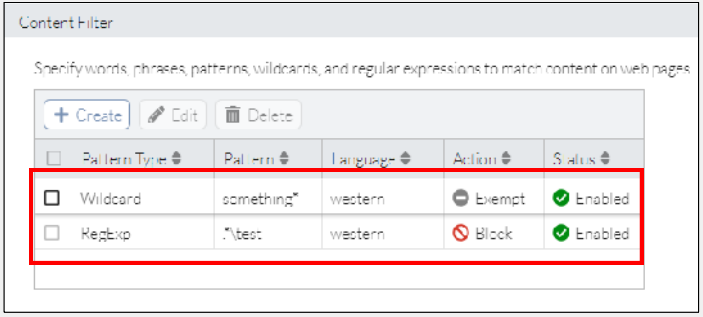
DO NOT REPRINT
© FORTINET

Brave-dumps.com

Web Filter—Content Filtering

- Requires FortiSASE to use SSL deep inspection
- Controls access to web pages containing specific patterns
- Scans the content of every website accepted by security policies
- Matches content from wildcards or Perl regular expressions
- Actions:
  - Exempt
  - Block

Security > **Profiles** > **Web Filter With Inline-CASB**



Content Filter

Specify words, phrases, patterns, wildcards, and regular expressions to match content on web pages

□	Pattern Type	Pattern	Language	Action	Status
□	Wildcard	something*	western	Exempt	✓ Enabled
□	RegExp	.*\test	western	Block	✓ Enabled

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 9

You can also control web content in the web filter profile by blocking access to websites containing specific words or patterns. This helps to prevent access to sites with questionable material.

You can add words, phrases, patterns, wildcards, and Perl regular expressions to match content on websites. You configure this feature at the web filter level, not at the global level. So, it is possible to add multiple web content filter lists and then select the best list for each web filter profile.

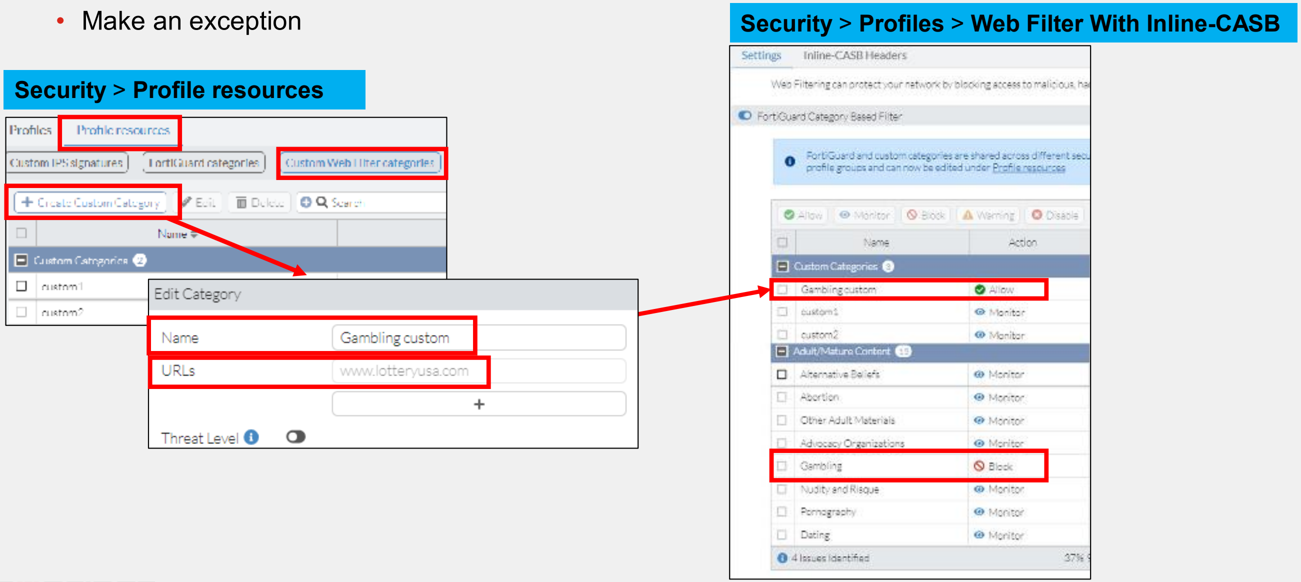
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET

Brave-dumps.com

Web Filter—Custom Category

- Changes a website category, not the category action
  - Make an exception



Security > Profile resources

Profiles | Profile resources

Custom IPS signatures | FortiGuard categories | Custom Web Filter categories

+ Create Custom Category | Edit | Delete | Search

☐	Name
⊟ Custom Categories 2	
☐	custom1
☐	custom2

Edit Category

- Name: Gambling custom
- URLs: www.lotteryusa.com
- Threat Level ○

Security > Profiles > Web Filter With Inline-CASB

Settings | Inline-CASB Headers

Web Filtering can protect your network by blocking access to malicious, ha

FortiGuard Category Based Filter

FortiGuard and custom categories are shared across different secu profile groups and can now be edited under Profile resources

Allow | Monitor | Block | Warning | Disable

☐	Name	Action
⊟	Custom Categories 3	
☐	Gambling custom	✓ Allow
☐	custom1	Monitor
☐	custom2	Monitor
⊟	Adult/Mature Content 13	
☐	Alternative Beliefs	Monitor
☐	Abortion	Monitor
☐	Other Adult Materials	Monitor
☐	Advocacy Organizations	Monitor
☐	Gambling	⊘ Block
☐	Nudity and Risque	Monitor
☐	Pornography	Monitor
☐	Dating	Monitor

4 Issues Identified 37%

© Fortinet Inc. All Rights Reserved.

If you want to make an exception, for example, rather than unblock access to a potentially unwanted category, change the website to an allowed category. You can also do the reverse. You can block a website that belongs to an allowed category.

Remember that changing categories does not automatically result in a different action for the website. This depends on the settings within the web filter profile.

In the example shown on this slide, the URL `www.lotteryusa.com` belongs to the FortiGuard category **Gambling.** The URL `www.lotteryusa.com` is added to the custom category **Gambling custom** to make an exception. The action for the FortiGuard Gambling category in the Web Filter With Inline-CASB profile is **Block**. When a user browses to `www.lotteryusa.com`, the custom category action takes precedence over the FortiGuard category, so access to www.lotteryusa.com is allowed.

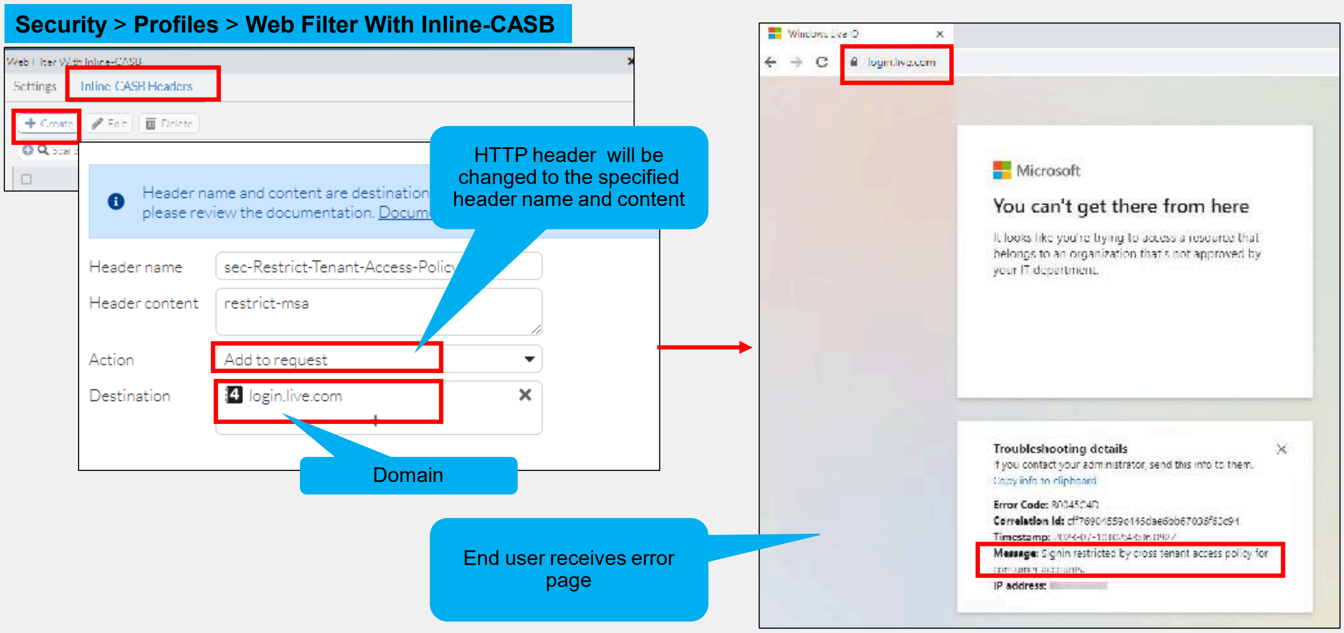
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET

Brave-dumps.com

Web Filter—Inline-CASB Headers

Security > Profiles > Web Filter With Inline-CASB


Web Filter With Inline-CASB
Settings
Inline CASB Headers
+ Create
Edit
Delete
Search
HTTP header will be changed to the specified header name and content
Domain
End user receives error page
Windows Live ID
login.live.com
Microsoft

Header name and content are destination ... please review the documentation. Docum...

Header name: sec-Restrict-Tenant-Access-Policy

Header content: restrict-msa

Action: Add to request

Destination: login.live.com

You can't get there from here

It looks like you're trying to access a resource that belongs to an organization that's not approved by your IT department.

Troubleshooting details

If you contact your administrator, send this info to them.

Copy info to clipboard

Error Code: 90045040

Correlation Id: cf76904559c145dae6bb67036f83c94

Timestamp: [illegible]

Message: Signin restricted by cross tenant access policy for consumer accounts.

IP address: [redacted]

© Fortinet Inc. All Rights Reserved.

The FortiSASE web filter inline cloud access security broker (CASB) component can be used to customize HTTP headers when agentless (proxy) or agent-based (FortiClient) remote users are accessing Software-as-a-Service (SaaS) applications. Customizing HTTP headers requires SSL deep inspection enabled on the security profile group. FortiSASE can intercept HTTP headers to add or remove header requests/responses, as required by the SaaS application. You must know the format and content of vendor-specific headers supported by a SaaS application to use this feature. FortiSASE intercepts HTTP headers and can modify them for outgoing traffic as follows:

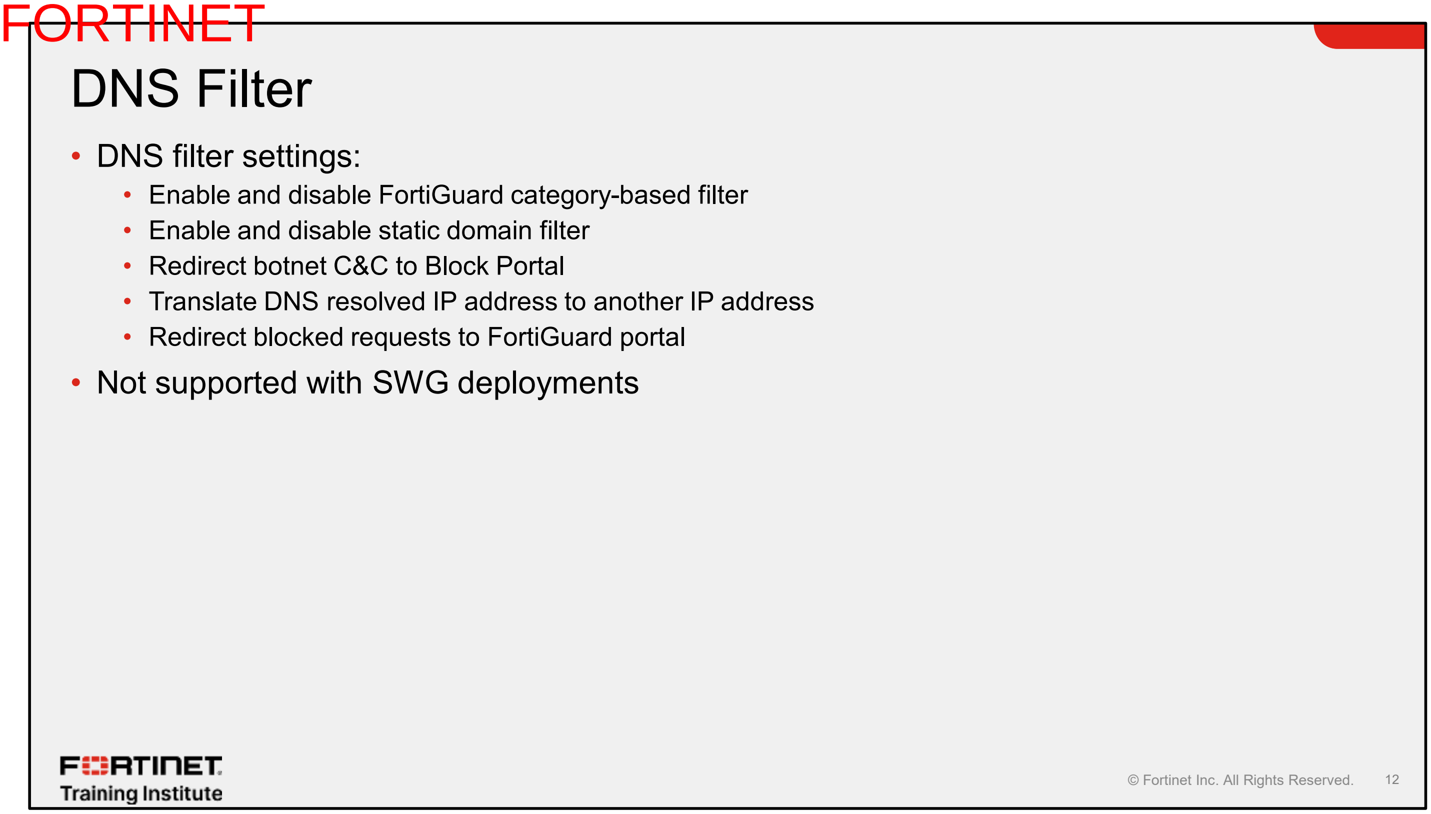
- **Add to request**
- **Add to response**
- **Remove from request**
- **Remove from response**

The example on this slide shows how to restrict access to personal accounts using the `login.live.com` domain. You can restrict access to personal accounts by adding a request to the HTTP header with the vendor header name and header content. You can find the format and content of vendor-specific headers on the vendor's website. You can locate the headers used this in example, at `https://learn.microsoft.com/en-us/azure/active-directory/manage-apps/tenant-restrictions`. You will also need to apply SSL deep inspection to the security profile group, and then apply the security profile group to the applicable policy. When the end user tries to access `login.live.com`, their access will be blocked with a Microsoft error page.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET

Brave-dumps.com



DNS Filter

- DNS filter settings:
  - Enable and disable FortiGuard category-based filter
  - Enable and disable static domain filter
  - Redirect botnet C&C to Block Portal
  - Translate DNS resolved IP address to another IP address
  - Redirect blocked requests to FortiGuard portal
- Not supported with SWG deployments

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 12

The filter includes various configuration settings. You can enable or disable the FortiGuard category-based filter and the static domain filter. You also have the option to:

- Redirect botnet command-and-control requests to block portal
- Allow DNS requests when a rating error occurs from the FortiGuard service
- Redirect blocked requests to FortiGuard portal

Using the **DNS Translation** feature, you can translate a DNS-resolved IP address to another IP address you specify.

DNS filtering supports the following actions:

- Allow
- Monitor
- Redirect to block portal

DNS filtering is not supported in SWG deployments.

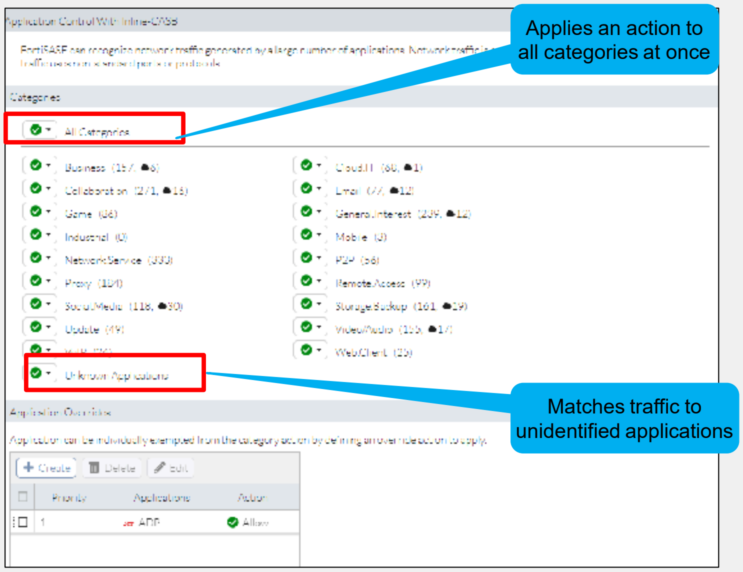
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET

Brave-dumps.com

Configure Application Control With Inline-CASB

Security > **Profiles** > **Application Control With Inline-CASB**



Application Control With Inline-CASB

FortiSASE can recognize network traffic generated by a large number of applications. Network traffic is
traffic uses nonstandard ports or protocols.

Categories

✓ All Categories	
✓ Business (157, ☁6)	✓ Cloud.IT (68, ☁1)
✓ Collaboration (271, ☁15)	✓ Email (77, ☁12)
✓ Game (86)	✓ General.Interest (239, ☁12)
✓ Industrial (0)	✓ Mobile (3)
✓ Network.Service (333)	✓ P2P (56)
✓ Proxy (184)	✓ Remote.Access (99)
✓ Social.Media (118, ☁30)	✓ Storage.Backup (161, ☁19)
✓ Update (49)	✓ Video/Audio (155, ☁17)
✓ VoIP (76)	✓ Web.Client (25)
✓ Unknown Applications	

Application Overrides

Application can be individually exempted from the category action by defining an override action to apply.

☐	Priority	Applications	Action
☐	1	ADP	✓ Allow

Applies an action to all categories at once

Matches traffic to unidentified applications

© Fortinet Inc. All Rights Reserved.

FortiSASE can recognize network traffic generated by a large number of applications. Network traffic is analyzed to detect application traffic, even if the traffic uses nonstandard ports or protocols.

You can configure the Application Control With Inline-CASB profile on the **Security** page, by selecting the appropriate security group. You can configure actions based on categories and application overrides. The **Unknown Applications** setting matches traffic that can't be matched to any application control signature and identifies the traffic as `unknown application` in the logs. The number listed beside the cloud symbol indicates the number of cloud applications in the category.

FortiSASE scans packets for matches, in this order, for the application control profile:

1. Application overrides: If you have configured any application, the application control profile considers those first. It looks for a matching override starting at the top of the list.
2. Categories: Finally, the application control profile applies the action that you've configured for applications in your selected categories.

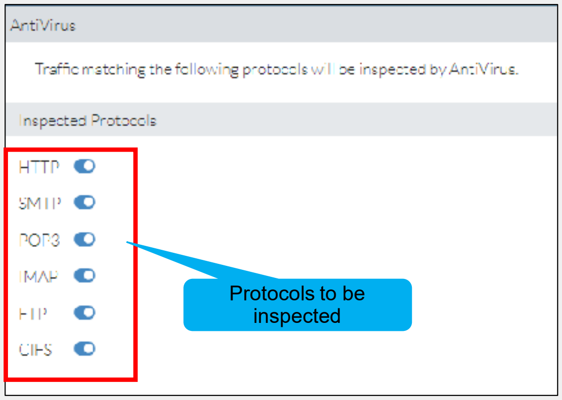
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET

Brave-dumps.com

Configure Antivirus

Security > Profiles > AntiVirus



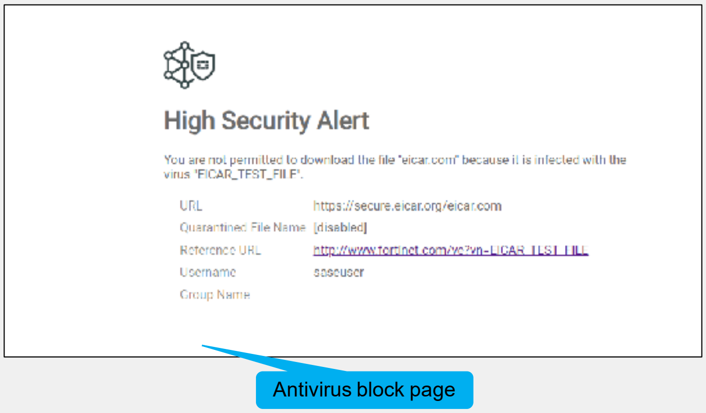
AntiVirus

Traffic matching the following protocols will be inspected by AntiVirus.

Inspected Protocols

- HTTP ●
- SMTP ●
- POP3 ●
- IMAP ●
- FTP ●
- CIFS ●

Protocols to be inspected



High Security Alert

You are not permitted to download the file "eicar.com" because it is infected with the virus "EICAR_TEST_FILE".

URL	https://secure.eicar.org/eicar.com
Quarantined File Name	[disabled]
Reference URL	http://www.fortinet.com/ve?vn=EICAR_TEST_FILE
Username	saseuser
Group Name	

Antivirus block page

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 14

FortiSASE antivirus delivers automated updates that protect against the latest polymorphic attacks, viruses, spyware, and other content-level threats. Based on the patented content pattern recognition language (CPRL), the anti-malware engine is designed to prevent known and previously unknown malware variants. You can customize which protocol needs to be inspected using antivirus for secure internet access. You can configure an antivirus profile on the **Security** page, by selecting the appropriate security profile group. For antivirus scanning, the block replacement page is displayed immediately when a virus is detected.

Vouchers & Dumps are Available | WhatsApp +201224560923

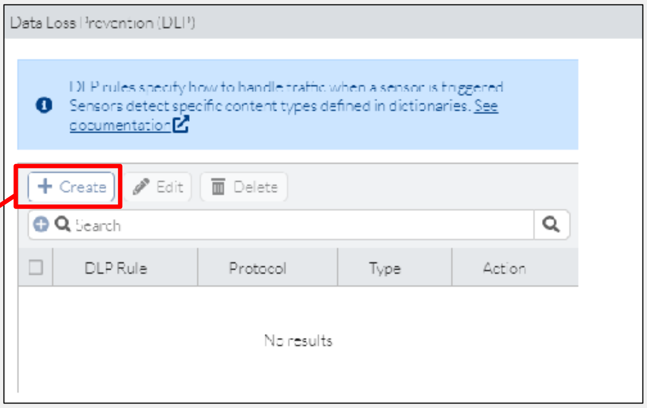
DO NOT REPRINT
© FORTINET

Brave-dumps.com

DLP

- Based on predetermined content patterns or a custom regular expression
- Supports MPIP labels
  - Allows Microsoft documents to be filtered based on their labelling

Security > Profiles > Data Loss Prevention

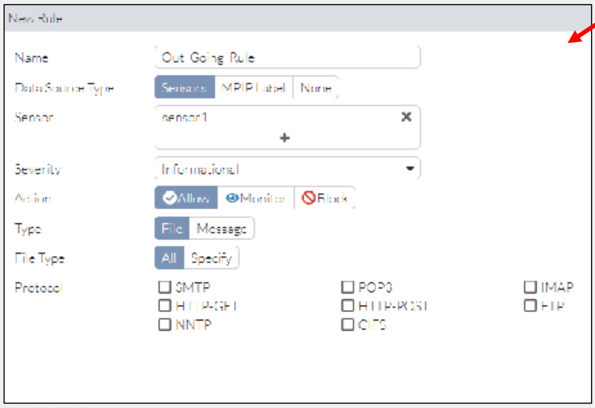


Data Loss Prevention (DLP)

DLP rules specify how to handle traffic when a sensor is triggered. Sensors detect specific content types defined in dictionaries. See documentation

□	DLP Rule	Protocol	Type	Action

No results



New Rule

Name: Out Going Rule
Data Source Type: [✓ Sensors] MPIP Label None
Sensor: sensor1
Severity: Informational
Action: [✓ Allow] Monitor Block
Type: [✓ File] Message
File Type: [✓ All] Specify
Protocol: □ SMTP □ POP3 □ IMAP □ HTTP-GET □ HTTP-POST □ FTP □ NNTP □ CIFS

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

The FortiSASE DLP system allows you to prevent sensitive data from leaving your network. When you define sensitive data patterns, data matching these patterns will be blocked, or logged and allowed, when passing through the FortiSASE. You configure the DLP system by creating individual filters based on file type, file size, a regular expression, an advanced rule, or a compound rule in a DLP sensor.

The DLP system is configured based on the following components:

- **Data Source Type**: DLP supports predefined types such as sensors, Microsoft Purview Information Protection (MPIP) label, or none.
  - **Sensors**: A DLP sensor is a package of filters. Each DLP sensor has one or more filters configured within it. Filters can examine traffic for known files using DLP fingerprints, for files of a particular type or name, for files larger than a specified size, for data matching specified regular expressions, and so on.
  - **MPIP Label**: You can employ labels as markers for sensitive information. Microsoft provides sensitivity labels, which act as identifiers emphasizing the importance of the data that they are associated with, thereby enhancing the security measures in place.
  - **None**: DLP matches using only file or message type and protocol as criteria.

The following actions are available:
Allow: FortiSASE takes no action, even if the patterns specified in the filter are matched.
Monitor: FortiSASE takes no action on network traffic matching a rule with this action. The filter match is logged.
Block: Traffic matching a filter with the block action will not be delivered. The matching message or download is replaced with the data leak prevention replacement message.

Vouchers & Dumps are Available | WhatsApp +201224560923

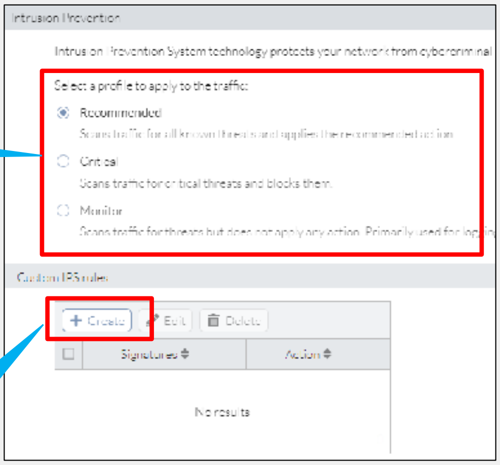
DO NOT REPRINT
© FORTINET

Brave-dumps.com

Configuring IPS Sensors

- Signatures-based defense
- Three profiles available:
  - Recommended
  - Critical
  - Monitor
- Custom IPS signatures are also supported
  - Customer signature syntax:
    - `F-SBID( --<option1> [<value1>]; --<option2> [<value2>];...)`

Security > Profiles > Intrusion Prevention



Intrusion Prevention

Intrusion Prevention System technology protects your network from cybercriminal

Select a profile to apply to the traffic:

● Recommended
Scans traffic for all known threats and applies the recommended action

○ Critical
Scans traffic for critical threats and blocks them.

○ Monitor
Scans traffic for threats but does not apply any action. Primarily used for loggin

Custom IPS rules

□	Signatures ⇕	Action ⇕

No results

Profile type

Create custom IPS signature

© Fortinet Inc. All Rights Reserved. 16

You can configure IPS sensors on the **Security** > **Profiles** page. FortiSASE uses signature-based detection and the FortiGuard extended IPS database to identify malicious activity.

You can select one of the predefined profiles while configuring the IPS sensors:

- **Recommended**: scans traffic for all known threats and applies the recommended action.
- **Critical**: scans traffic for critical threats and blocks them.
- **Monitor**: scans traffic for threats but does not apply any action. Primarily used for logging.

For more information on the IPS profiles refer to the *FortiSASE Administration Guide*.

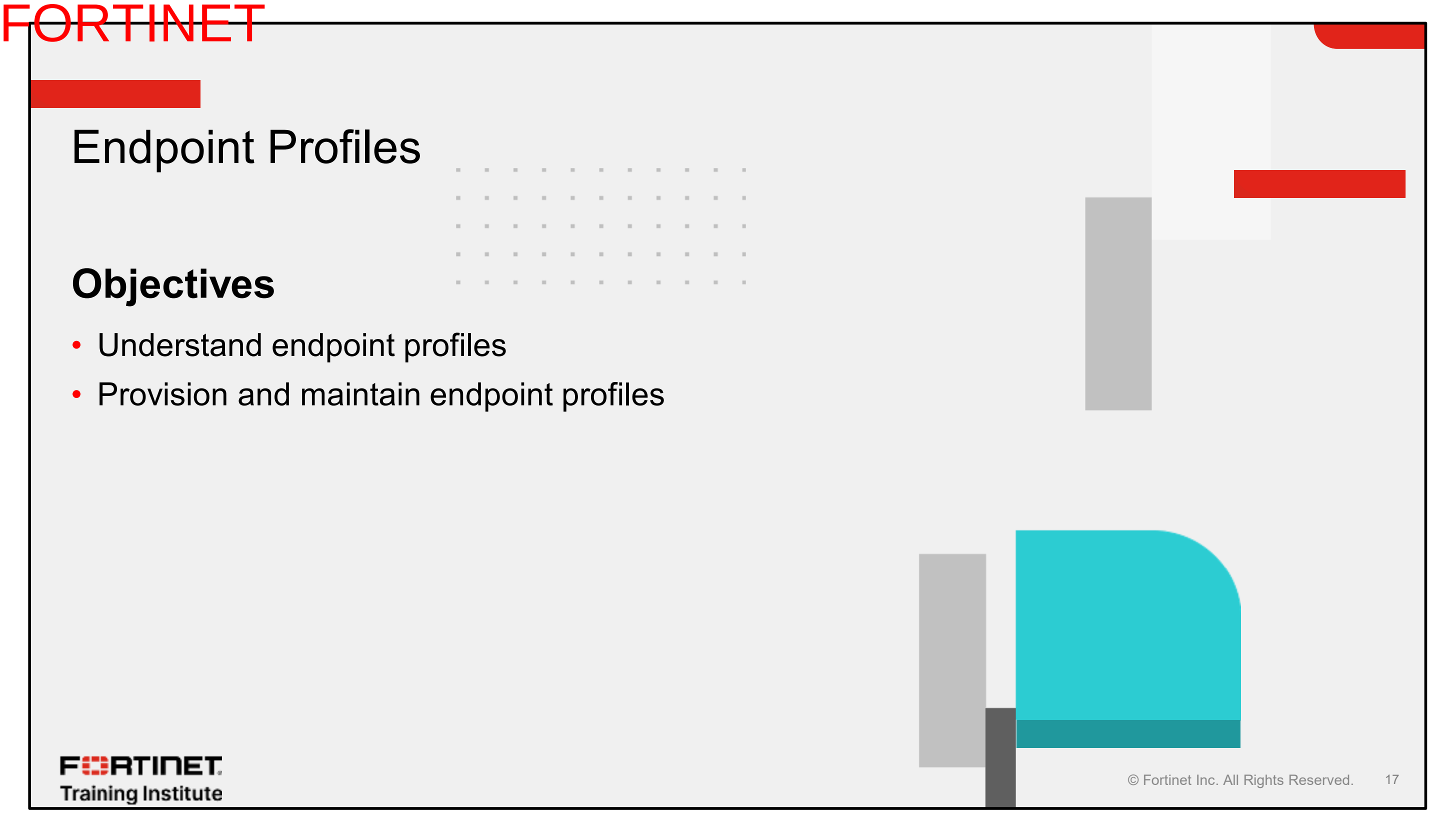
You can create a signature that identifies a certain packet type, and then add the signature to an IPS sensor. All signatures include a type header (F-SBID) and a series of option/value pairs. You use the option/value pairs to uniquely identify a packet. The following options are supported in custom IPS signatures:

- Protocol: options to inspect IP/ICMP/UDP/TCP protocol headers for the value paired with the option.
- Payload: options to inspect the packet payload for the value paired with the option.
- Special: options to inspect other aspects (such as application control) of the packet for the value paired with the option.
- Application options: options to inspect other aspects unique to application control for the value paired with the option.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET

Brave-dumps.com



Endpoint Profiles

Objectives

- Understand endpoint profiles
- Provision and maintain endpoint profiles

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in configuring, editing, assigning, and managing endpoint profiles, you will be able to use endpoint profiles to define the features installed on FortiClient endpoints.

Vouchers & Dumps are Available | WhatsApp +201224560923

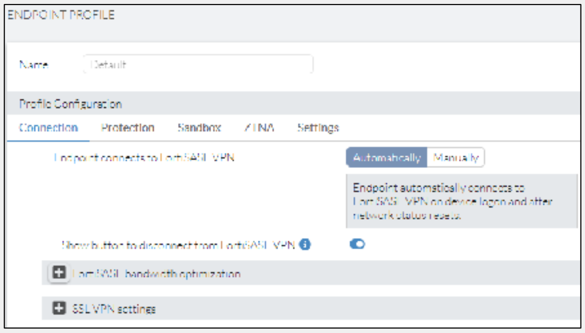
DO NOT REPRINT
© FORTINET

Brave-dumps.com

Endpoint Profiles

- You can configure FortiClient software using endpoint profiles
- Endpoint profiles have the following features:
  - Connection
  - Protection
  - Sandbox
  - ZTNA
  - Settings
- Endpoint profiles do not apply to security web gateway (SWG) mode deployment

Configuration > ENDPOINTS > Profile



ENDPOINT PROFILE

Name: Default

Profile Configuration

Endpoint connects to FortiSASE VPN: Automatically | Manually

Endpoint automatically connects to FortiSASE VPN on device logon and after network status resets.

Show button to disconnect from FortiSASE VPN: ●

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 18

You can configure the endpoint profile on the **Profile** page. Endpoint profiles define the configuration of FortiClient software on endpoints. You can enable features like antivirus, antiransomware, vulnerability scans, sandbox detection, ZTNA connection rules, and so on using this profile. When you provision FortiSASE, a default endpoint profile is created. By default, this profile is applied to the endpoints if there are no additional custom profiles created. The default profile of the feature is designed to provide effective levels of protection. Endpoint profiles have different features, as this slide shows. SWG mode is an agentless solution and endpoint profiles do not apply to SWG deployment.

Vouchers & Dumps are Available | WhatsApp +201224560923

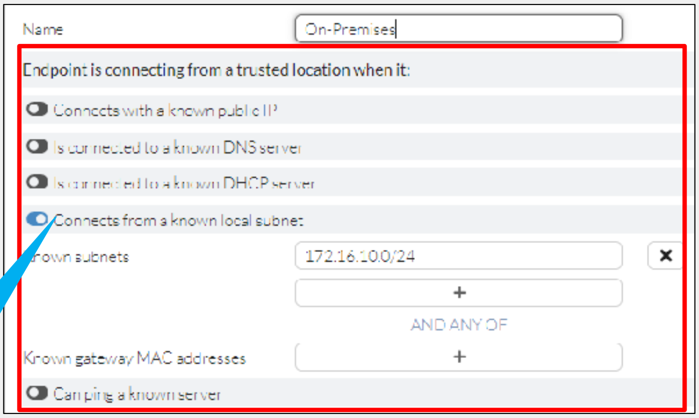
DO NOT REPRINT
© FORTINET

Brave-dumps.com

On-Fabric Rule Sets

- FortiSASE uses rules to determine if the endpoint is on-fabric or off-fabric based on the telemetry data received
- FortiSASE connection can be bypassed based on FortiClient fabric status
- Allows greater control and visibility of endpoints

Configuration > ENDPOINTS > On-fabric rule sets



Name: On-Premises

Endpoint is connecting from a trusted location when it:

○ Connects with a known public IP

○ Is connected to a known DNS server

○ Is connected to a known DHCP server

● Connects from a known local subnet

Known subnets: 172.16.10.0/24 ✕

AND ANY OF

Known gateway MAC addresses: +

○ Can ping a known server

On-fabric detection rule set

FURTINET Training Institute

© Fortinet Inc. All Rights Reserved. 19

You can configure on-fabric detection rules for endpoints. FortiSASE uses the rules to determine if the endpoint is on fabric or off fabric. A rule set is available for on-fabric detection. If you configure rules of multiple detection types for a rule set, the endpoint must satisfy all configured rules to satisfy the entire rule set.

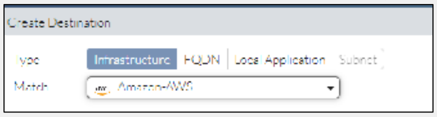
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET

Brave-dumps.com

Connection

- Connect to FortiSASE
  - On-device login
    - Automatically connect to FortiSASE SSL VPN when user logs in to the endpoint
  - Manually
    - Manually connect to the FortiSASE SSL VPN
- Bypass FortiSASE
  - FortiSASE SSL VPN autoconnect can by bypassed based on FortiClient on-fabric status
  - Can specify which application traffic to exclude from the FortiSASE SSL VPN tunnel

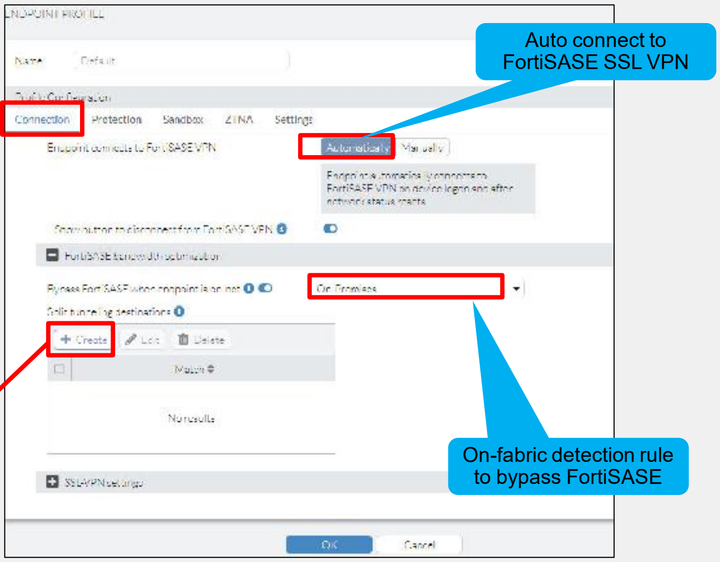


Create Destination

Type: Infrastructure | FQDN | Local Application | Subnet

Match: Amazon-AWS

Configuration > ENDPOINTS > Profile



ENDPOINT PROFILE

Name: Default

Profile Configuration

Connection | Protection | Sandbox | ZTNA | Settings

Endpoint connects to FortiSASE VPN: Automatically | Manually

Endpoint automatically connects to FortiSASE VPN on device login and after network status change

Show button to disconnect from FortiSASE VPN

FortiSASE bandwidth optimization

Bypass FortiSASE when endpoint is on-net: On-Premises

Split tunneling destinations

Auto connect to FortiSASE SSL VPN

On-fabric detection rule to bypass FortiSASE

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

In the endpoint profile, you can configure FortiClient to automatically connect to the FortiSASE SSL VPN when the user logs in to the endpoint, or give the user the ability to connect manually. You can also bypass the FortiSASE autoconnect on FortiClient based on the on-fabric rule set configured. If the endpoint is detected to be on-fabric based on the rule set, then FortiSASE can be bypassed for security inspection because an on-premises firewall like FortiGate protects the internet access.

You can also configure split tunneling, where you can specify which traffic to exclude from the VPN tunnel and redirect to the endpoint physical interface bypassing FortiSASE.

Vouchers & Dumps are Available | WhatsApp +201224560923

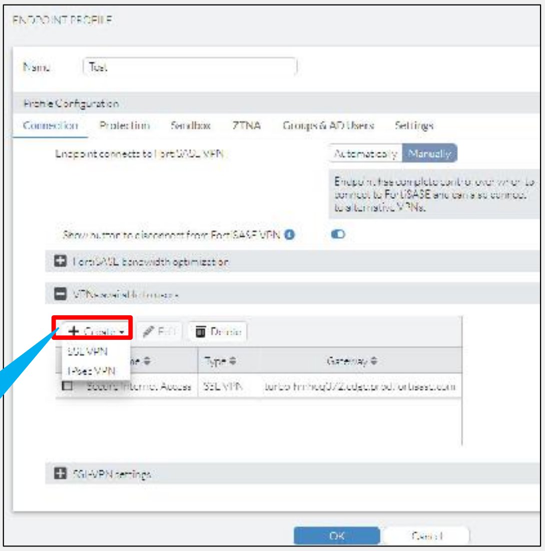
DO NOT REPRINT
© FORTINET

Brave-dumps.com

Connection (Contd)

- Not available in default profile
- Custom VPN tunnels
  - IPsec tunnel
  - SSL VPN tunnel

Configuration > ENDPOINTS > Profile



ENDPOINT PROFILE

Name: Test

Profile Configuration

Endpoint connects to FortiSASE VPN: Automatically [✓ Manually]

Endpoint has complete control over when to connect to FortiSASE and can also connect to alternative VPNs.

Show button to disconnect from FortiSASE VPN ●

Name	Type	Gateway
Secure Internet Access	SSL VPN	turbo fr...edge.prod.fortisase.com

Create additional VPN tunnels

© Fortinet Inc. All Rights Reserved.

You can configure a custom IPsec or SSL VPN configuration. These configurations are typically useful for use cases that require endpoints to connect to an on-premises FortiGate through a VPN.

Vouchers & Dumps are Available | WhatsApp +201224560923

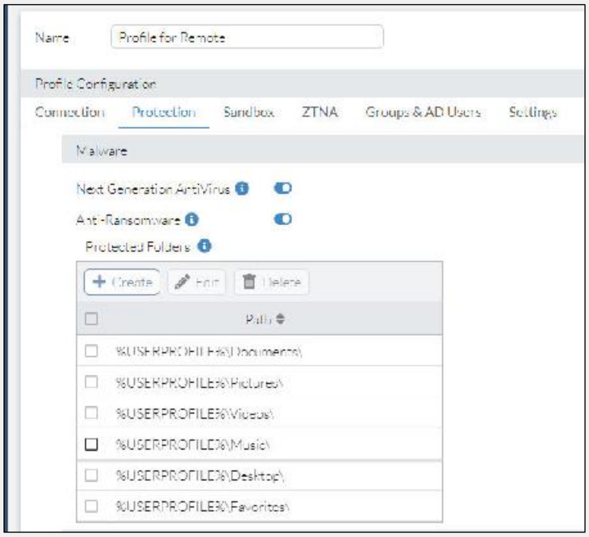
DO NOT REPRINT
© FORTINET

Brave-dumps.com

Protection—Malware

- In the **Malware** section, you can enable **Next Generation AntiVirus and Anti-Ransomware**

Configuration > ENDPOINTS > Profile



Name: Profile for Remote

Profile Configuration

Malware

Next Generation AntiVirus: ●

Anti-Ransomware: ●

Protected Folders

□	Path
□	%USERPROFILE%\Documents\
□	%USERPROFILE%\Pictures\
□	%USERPROFILE%\Videos\
□	%USERPROFILE%\Music\
□	%USERPROFILE%\Desktop\
□	%USERPROFILE%\Favorites\

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved. 22

You can enable **Next Generation AntiVirus** in the **Malware** section. Enabling **Next Generation Antivirus** turns on real-time protection and cloud-based malware detection. Real-time protection scans files as they are downloaded or copied to the endpoint. The cloud-based malware protection feature helps protect endpoints from high-risk file types that come from external sources, such as the internet or network drives, by querying FortiGuard to determine whether files are malicious.

Antiransomware protects specific files, folders, or file types on your endpoints from unauthorized changes. The **Anti-Ransomware** section includes settings for protected folders, file types, and action valid signer. You can select the folders you want in the existing list or create a custom directory to protect. Use the **Create** to add a new folder. FortiClient antiransomware protects all content in the selected folders against unauthorized changes.

Vouchers & Dumps are Available | WhatsApp +201224560923

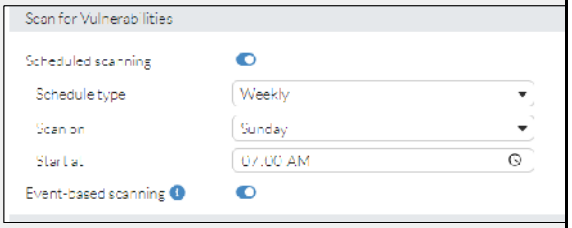
DO NOT REPRINT
© FORTINET

Brave-dumps.com

Protection—Vulnerability Scan

- The **Scan for Vulnerabilities** section enables scanning on endpoints
  - Scan on connecting to FortiSASE
  - Scan for OS and vulnerability signature updates
  - Configure scheduled scans
- Endpoint vulnerabilities can be reviewed on the **Security** dashboard on the FortiSASE portal

Configuration > ENDPOINTS > Profile



Scan for Vulnerabilities

Scheduled scanning	●
Schedule type	Weekly
Scan on	Sunday
Start at	07:00 AM
Event-based scanning	●

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 23

You can enable vulnerability scans to run on endpoints after they connect to FortiSASE and when they update a vulnerability signature. You can enable scanning for endpoint OS updates and then applying the updates. You can also schedule scans. In the **Schedule type** field, you can select **Daily**, **Weekly**, or **Monthly**. You can also specify the time the scan will start.

A vulnerability scan identifies vulnerabilities on the endpoint that should be fixed by installing software patches. You must manually download and install software patches for the vulnerable software. You can view details about endpoint vulnerabilities in the **Security** dashboard on the FortiSASE portal.

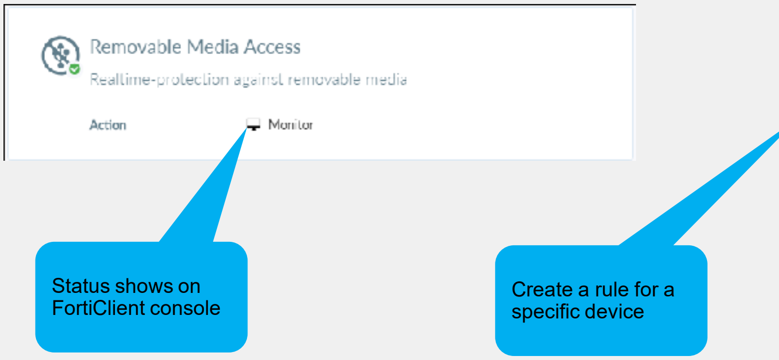
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET

Brave-dumps.com

Protection—Removal Media Access Control

- FortiClient controls access to removable media devices
  - USB drives
  - External hard drives
- FortiClient can allow, block, or monitor devices



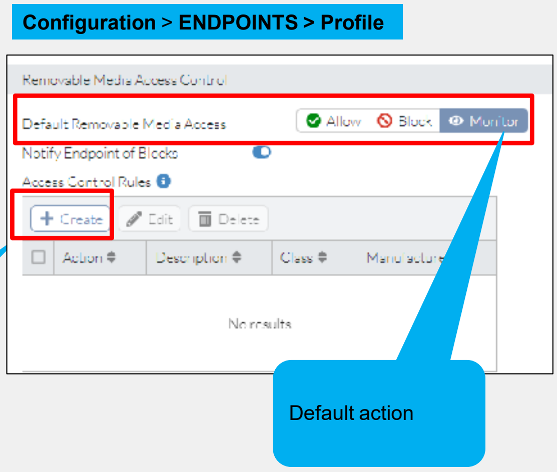
Removable Media Access

Realtime-protection against removable media

Action Monitor

Status shows on FortiClient console

Create a rule for a specific device



Configuration > ENDPOINTS > Profile

Removable Media Access Control

Default Removable Media Access ✓ Allow ⊘ Block Monitor

Notify Endpoint of Blocks

Access Control Rules

Default action

The **Removable Media Access** section controls access to removable media devices, such as USB drives and external hard drives. You can also configure rules to allow or block specific removable devices. Rules for specific devices require the class, manufacturer, vendor ID, product ID, and revision information for the devices. You can find the required values for the devices in one of the following ways:

- Microsoft Windows Device Manager: select the device and view its properties.
- USBDeview

FortiClient can allow, block, or monitor access to removable media devices based on the rules, as configured by the FortiSASE administrator. Access control or action for devices that do not match any configured rules are controlled by the **Default Removable Media Access** setting.

Vouchers & Dumps are Available | WhatsApp +201224560923

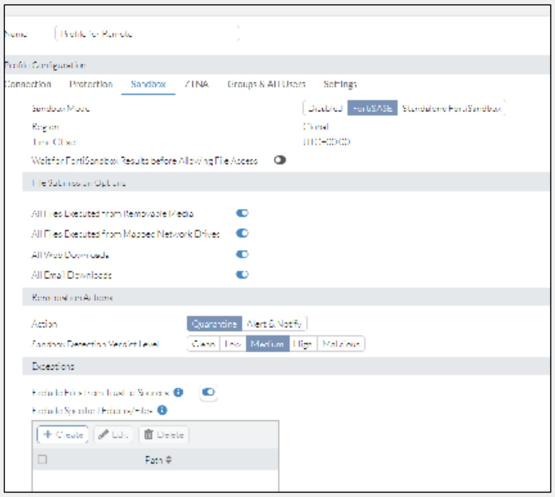
DO NOT REPRINT
© FORTINET

Brave-dumps.com

Configuring Sandbox

- You can enable sandbox detection on the **Sandbox** tab
- Sandbox Mode:
  - FortiSASE
    - FortiSandbox Cloud included with FortiSASE instance
  - Standalone FortiSandbox
    - On-premises standalone FortiSandbox
- Options are:
  - File Submission Options
  - Remediation Actions
  - Exceptions
- FortiClient sends files to FortiSandbox for further analysis if they are not detected locally
- Endpoint users can also manually submit files to FortiSandbox for scanning
- Access to files can be blocked until the FortiSandbox scanning results are returned

Configuration > ENDPOINTS > Profile



Name: Profile for Remote

Profile Configuration

Connection | Protection | Sandbox | ZTNA | Groups & All Users | Settings

Sandbox Mode: Disabled | FortiSASE | Standalone FortiSandbox

Region: Global

Time Offset: UTC+00:00

Wait for FortiSandbox Results before Allowing File Access

File Submission Options

All Files Executed from Removable Media

All Files Executed from Mapped Network Drives

All Web Downloads

All Email Downloads

Remediation Actions

Action: Quarantine | Alert & Notify

Sandbox Detection Verdict Level: Clean | Low | Medium | High | Malicious

Exceptions

Exclude Files from Trusted Sources

Exclude Specified Folders/Files

© Fortinet Inc. All Rights Reserved.

You can enable the sandbox feature on FortiSASE by selecting **FortiSASE** or **Standalone FortiSandbox** as the **Sandbox Mode** on the **Sandbox** tab in the endpoint profile.

When you enable sandbox, the following options are available:

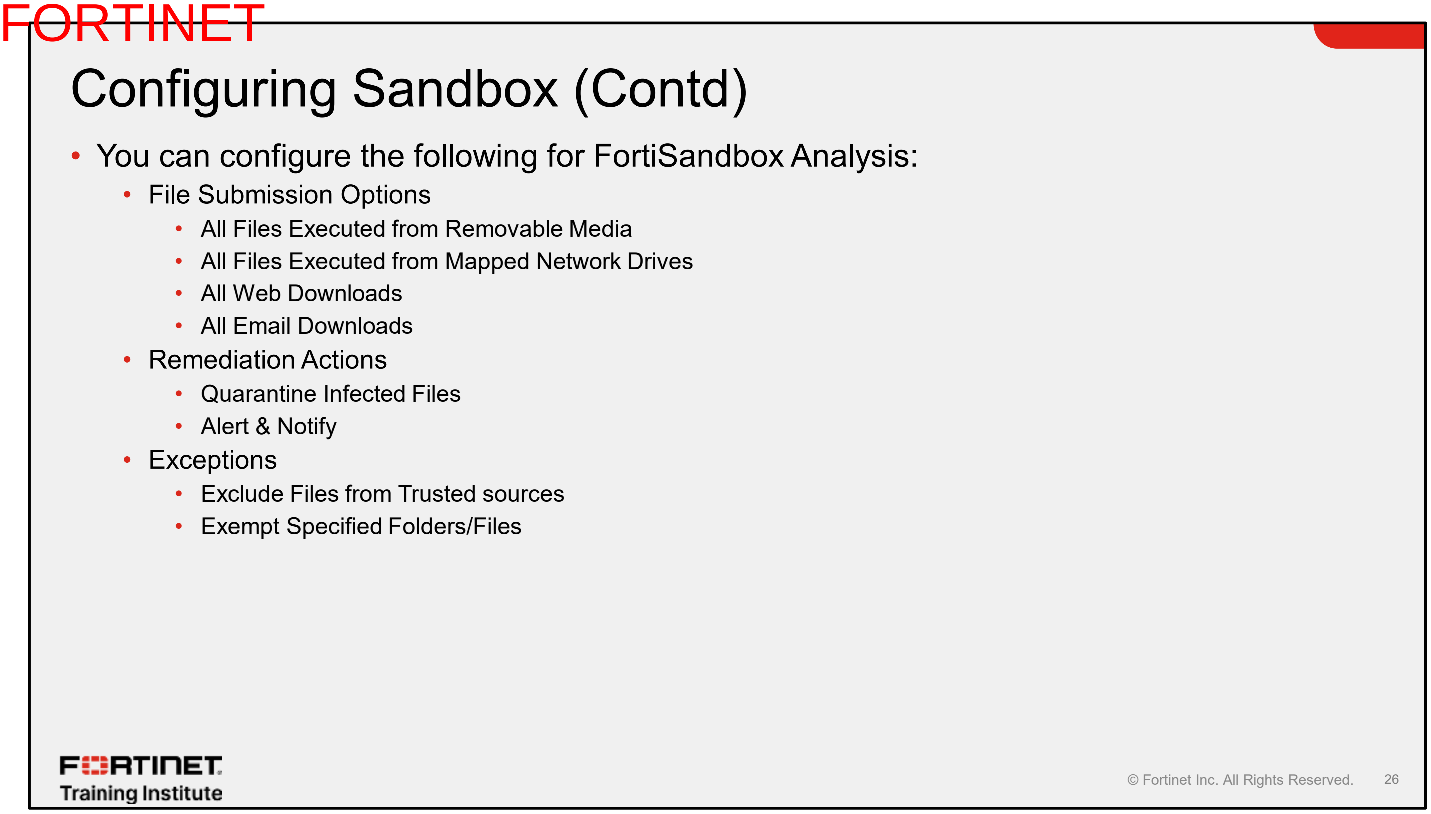
- In the **File Submission Options** section, you can select file resources like removable media, network drives, web downloads, and email downloads.
- **Remediation Actions** allows you to select the **Quarantine** or **Alert & Notify** action for infected files.
- **Exceptions** allows you to exclude files from trusted sources and specific files or folders.

When configured, FortiSandbox automatically scans files that are downloaded on the endpoint, on removable media attached to the endpoint, or on mapped network drives. FortiClient also automatically scans files that are downloaded with an email client on the endpoints, or from the internet. In each case, if the file is not detected locally, and FortiSandbox integration is configured, FortiClient sends the file to FortiSandbox for further analysis. Endpoint users can also manually submit files to FortiSandbox for scanning. FortiClient periodically downloads the latest antivirus signatures from FortiSandbox and applies them locally to all real-time and on-demand antivirus scanning.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET

Brave-dumps.com



Configuring Sandbox (Contd)

- You can configure the following for FortiSandbox Analysis:
  - File Submission Options
    - All Files Executed from Removable Media
    - All Files Executed from Mapped Network Drives
    - All Web Downloads
    - All Email Downloads
  - Remediation Actions
    - Quarantine Infected Files
    - Alert & Notify
  - Exceptions
    - Exclude Files from Trusted sources
    - Exempt Specified Folders/Files

Training Institute

© Fortinet Inc. All Rights Reserved. 26

You can configure the following file submission options:

- **All Files Executed from Removable Media**: Enable this option to send all files executed on removable media, such as USB drives, to FortiSandbox for analysis.
- **All Files Executed from Mapped Network Drives**: Enable this option to submit all files that are executed on mapped network drives to FortiSandbox for analysis.
- **All Web Downloads**: Enable this option to submit all web downloads on the endpoint to FortiSandbox for analysis.
- **All Email Downloads:** Enable this option to submit all email downloads on the endpoint to FortiSandbox for analysis.

You can configure the following remediation options:

- **Quarantine infected files**: Enable this option to quarantine infected files.
- **Alert & Notify**: Enable this option to alert and notify the endpoint user about infected files, but not quarantine infected files.

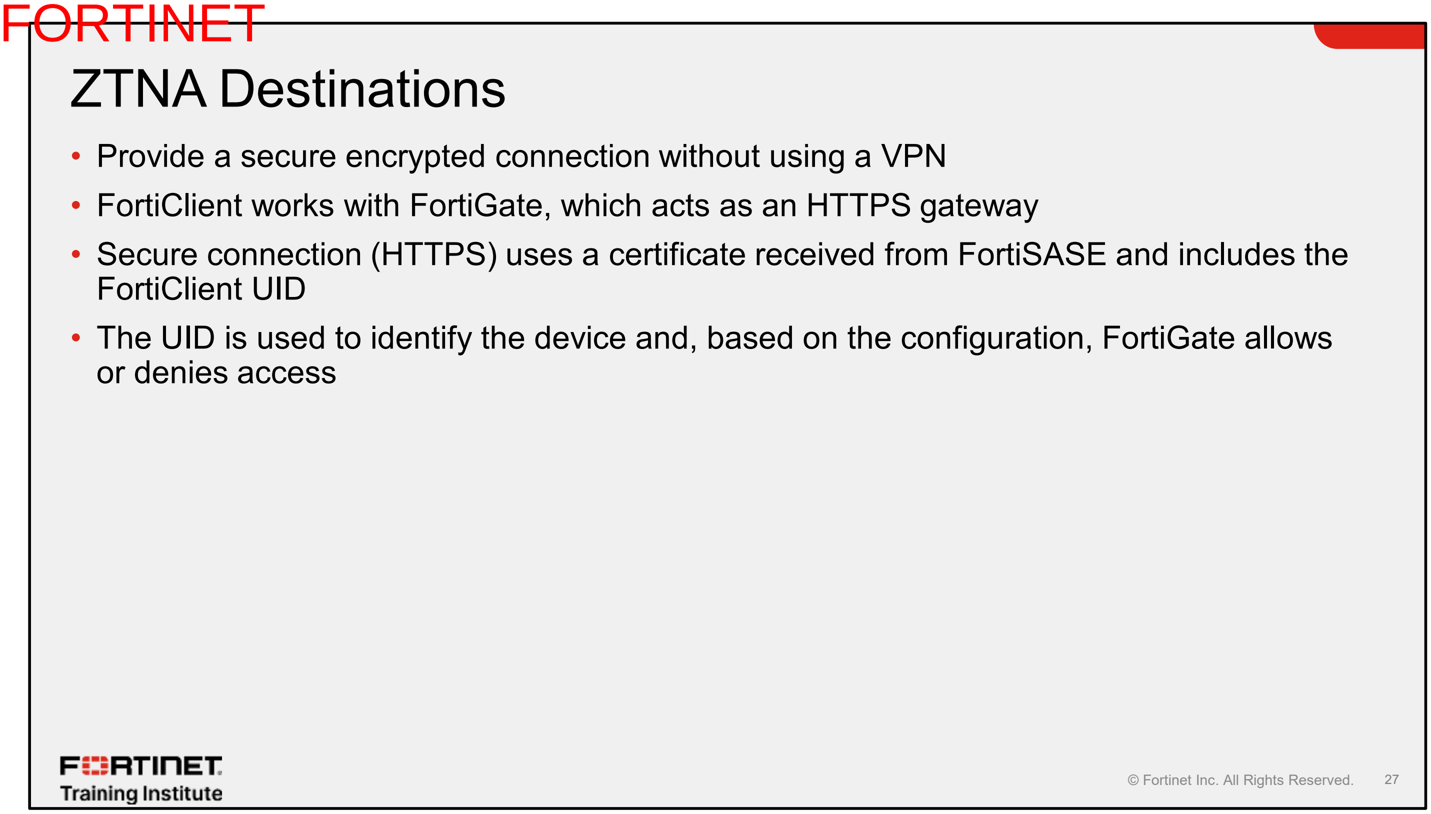
You can configure the following exceptions:

- **Exclude Files from Trusted sources**: Enable this option to exclude files from being sent to FortiSandbox that are signed by trusted sources like Microsoft, Fortinet, Intel, and so on.
- **Exempt Specified Folders/Files**: Create the exclusion list to exempt specified files and/or folders from FortiSandbox analysis.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET

Brave-dumps.com



ZTNA Destinations

- Provide a secure encrypted connection without using a VPN
- FortiClient works with FortiGate, which acts as an HTTPS gateway
- Secure connection (HTTPS) uses a certificate received from FortiSASE and includes the FortiClient UID
- The UID is used to identify the device and, based on the configuration, FortiGate allows or denies access

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

ZTNA destinations on FortiClient create a secure encrypted connection to protected applications without using a VPN. FortiClient uses the FortiGate application proxy feature to create a secure connection through HTTPS, using a certificate received from FortiSASE that includes the FortiClient UID. FortiGate acts as an HTTPS gateway.

FortiGate retrieves the UID to identify the device and check other endpoint information that FortiSASE provides to FortiGate, which can include other identity and posture information. FortiGate allows or denies access, as applicable.

You will learn about this configuration in a later lesson.

Vouchers & Dumps are Available | WhatsApp +201224560923

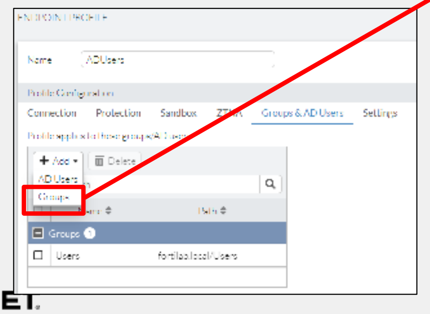
DO NOT REPRINT
© FORTINET

Brave-dumps.com

Groups and Active Directory Users

- Endpoint profiles can be assigned to different users based on:
  - Active Directory (AD) users or group
    - AD server should be integrated with FortiSASE to view the domain users and groups
  - Non-AD users
    - Can create nested non-AD groups and assign endpoints to the group

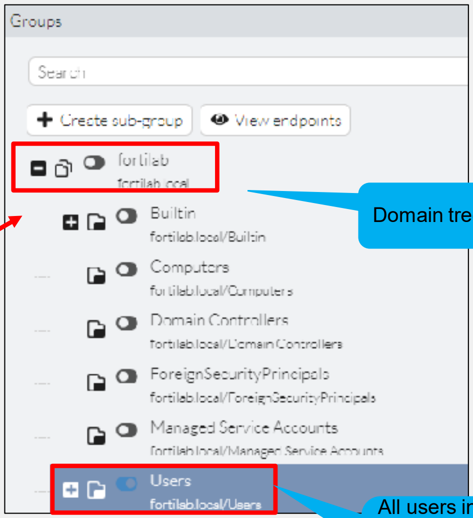
Configuration > ENDPOINTS > Profile



Name: ADUsers

Profile applies to these groups/AD Users

Name	Path
Users	fortilab.local/Users



Domain tree

All users in this AD group will be assigned the ADUsers endpoint profile

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 28

The option to assign profiles to endpoints is only available in newly created profiles and not the default profile. You can assign different endpoint profiles for users based on their AD username or group membership. To view users and groups from the AD server you must integrate your AD server with FortiSASE. The example on this slide shows that the endpoint profile **ADUsers** is assigned to users in the LDAP user group **fortilab.local/Users**.

Another option is to assign endpoint profiles for non-AD groups by creating nested non-AD groups and manually assigning endpoints to the group.

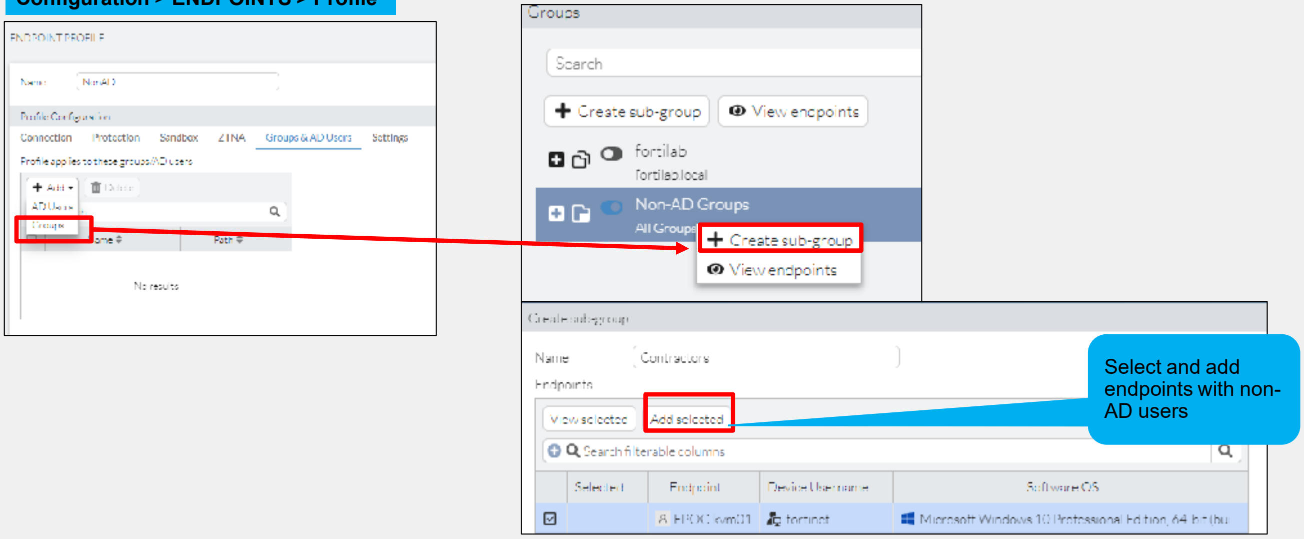
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET

Brave-dumps.com

Groups and Active Directory Users (Contd)

Configuration > ENDPOINTS > Profile



Name: NonAD

Profile applies to these groups/AD users

Name: Contractors

	Selected	Endpoint	Device Username	Software OS
☑		[illegible]-kvm01	fortinet	Microsoft Windows 10 Professional Edition, 64-bit (bu

Select and add endpoints with non-AD users

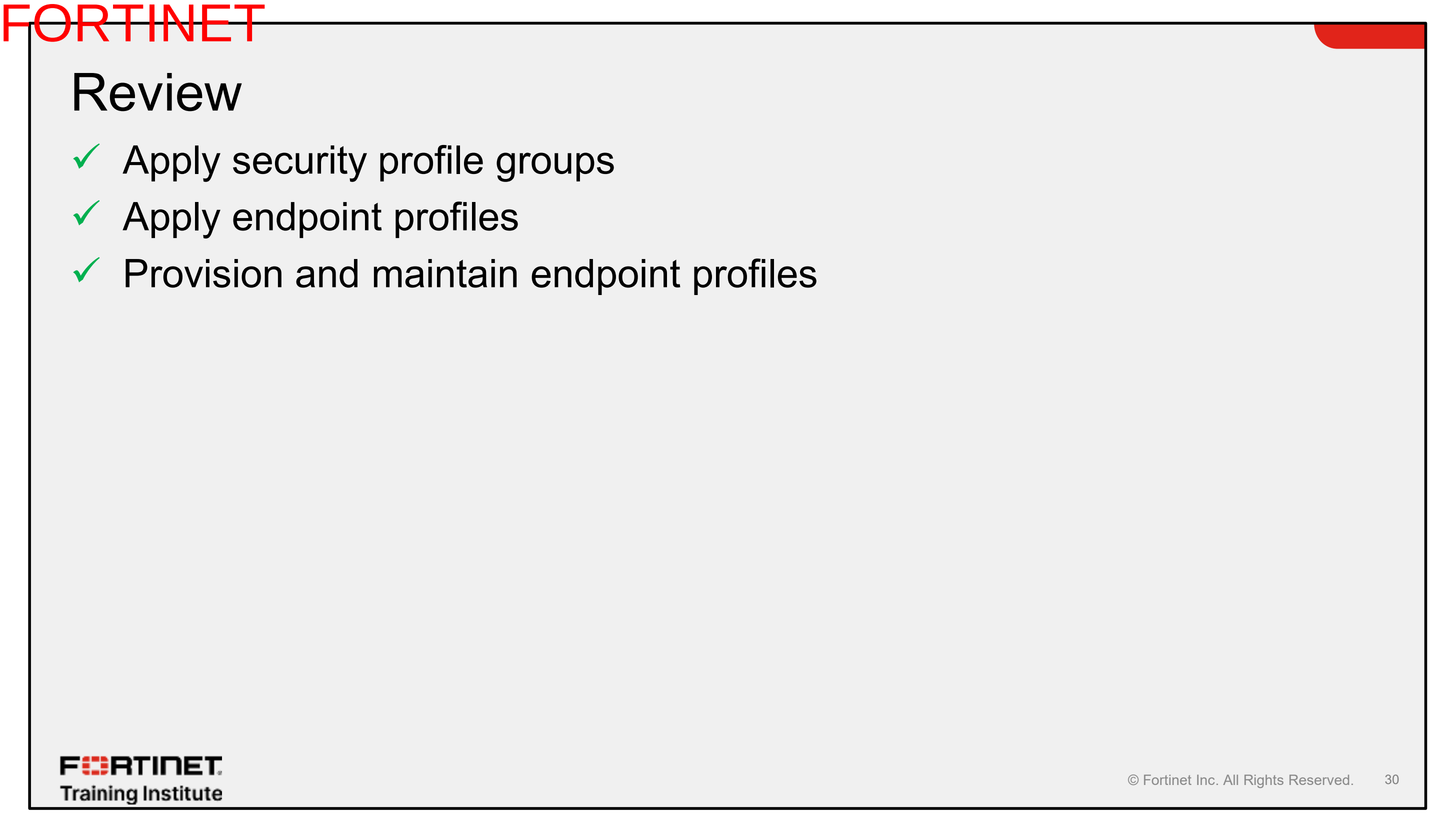
© Fortinet Inc. All Rights Reserved.

The example on this slide shows the process of adding an endpoint with a non-AD user to an endpoint profile.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET

Brave-dumps.com



Review

- ✓ Apply security profile groups
- ✓ Apply endpoint profiles
- ✓ Provision and maintain endpoint profiles

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 30

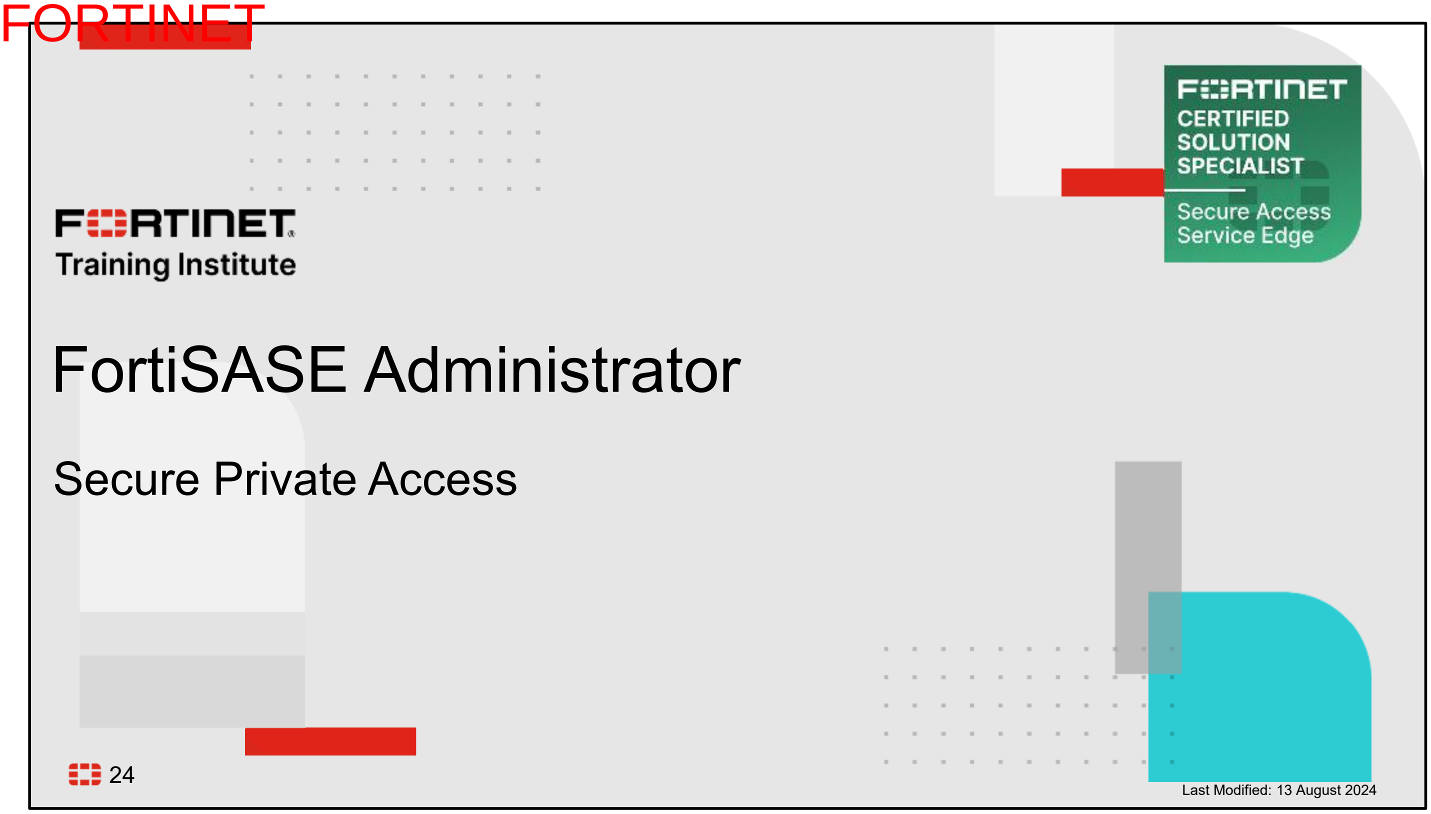
This slide shows the objectives that you covered in this lesson.

By mastering the objectives covered in this lesson, you learned how to configure and use endpoint and security profiles on FortiSASE.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET

Brave-dumps.com



FORTINET CERTIFIED SOLUTION SPECIALIST
Secure Access Service Edge

FORTINET Training Institute

FortiSASE Administrator

Secure Private Access

24

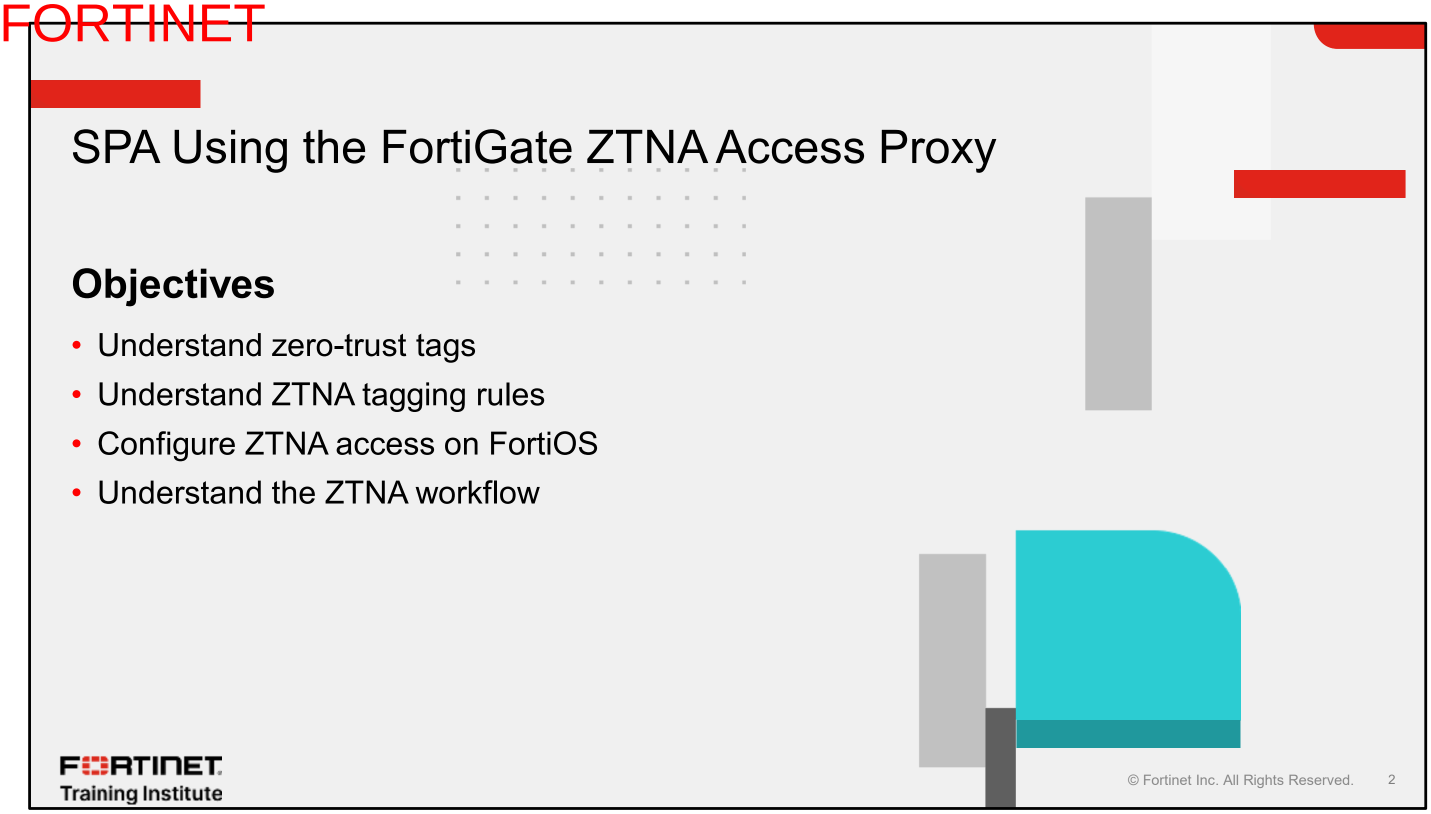
Last Modified: 13 August 2024

In this lesson, you will learn about the common use cases of Secure Private Access (SPA) in a FortiSASE deployment.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET

Brave-dumps.com



SPA Using the FortiGate ZTNA Access Proxy

Objectives

- Understand zero-trust tags
- Understand ZTNA tagging rules
- Configure ZTNA access on FortiOS
- Understand the ZTNA workflow

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

2

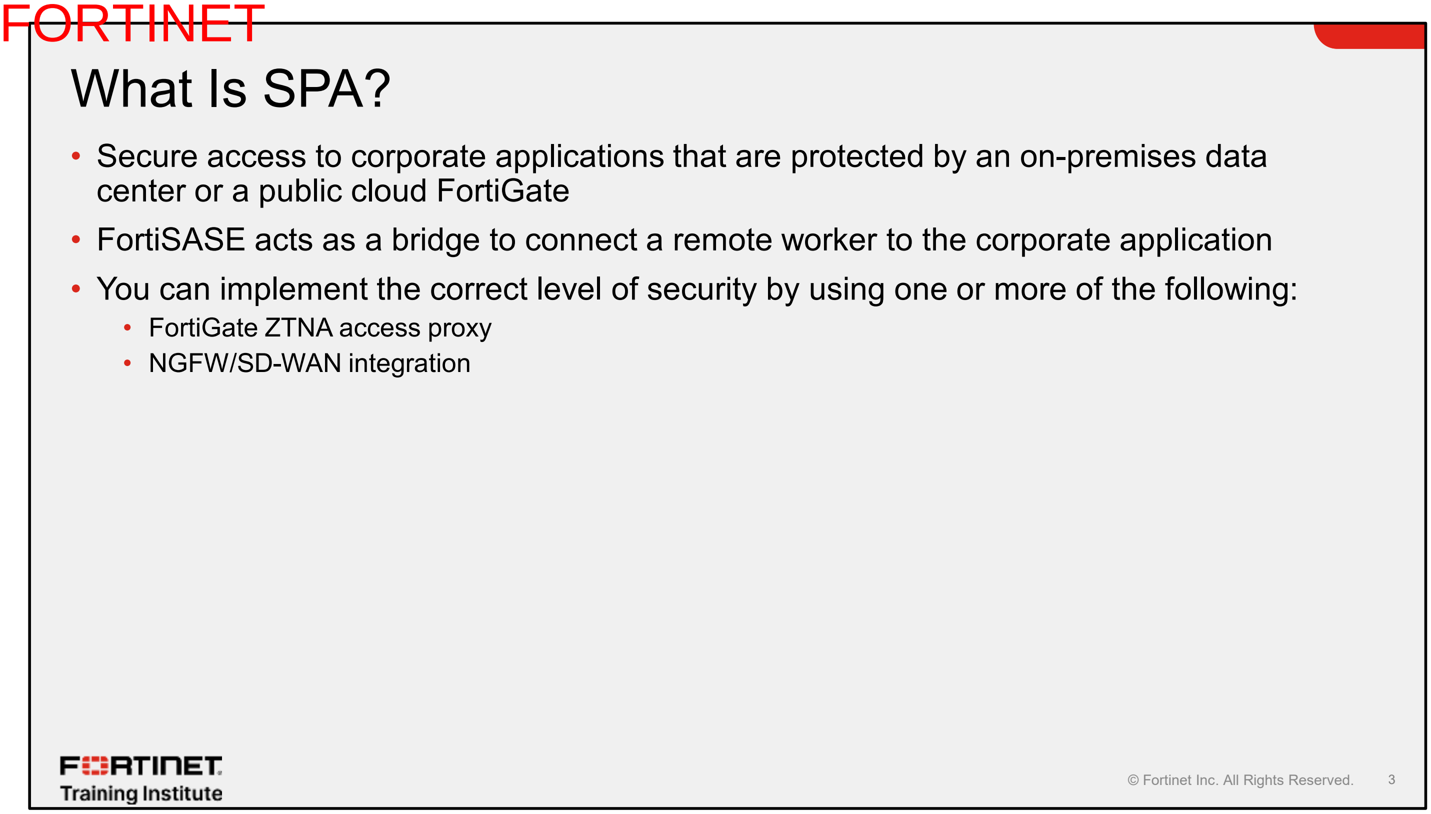
After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in understanding the basic configuration of zero trust network access (ZTNA), you will be able to configure ZTNA in your environment using FortiSASE and FortiGate.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET

Brave-dumps.com



What Is SPA?

- Secure access to corporate applications that are protected by an on-premises data center or a public cloud FortiGate
- FortiSASE acts as a bridge to connect a remote worker to the corporate application
- You can implement the correct level of security by using one or more of the following:
  - FortiGate ZTNA access proxy
  - NGFW/SD-WAN integration

Training Institute

© Fortinet Inc. All Rights Reserved. 3

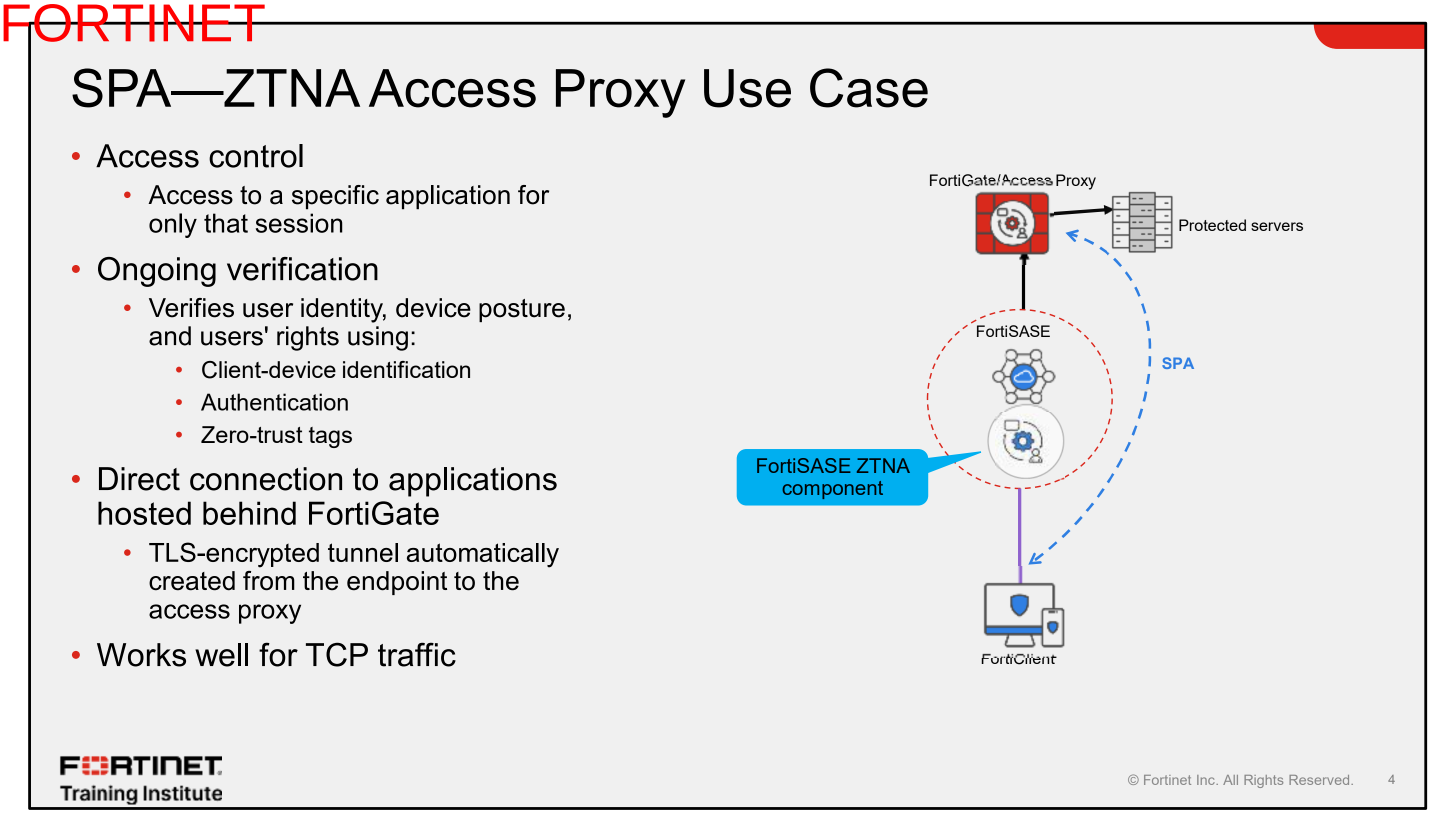
FortiSASE SPA allows access to corporate applications that are protected by an on-premises data center or public cloud FortiGate. FortiSASE acts as a bridge to connect a remote worker to the corporate applications hosted behind your FortiGate device. You can implement the appropriate level of security and access by using one or more of the following:

- ZTNA-FortiSASE integration with a FortiGate ZTNA access proxy
- NGFW/SD-WAN-FortiSASE with a next-generation firewall (NGFW) standalone hub or an existing SD-WAN deployment to form a traditional hub-and-spoke topology

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET

Brave-dumps.com



SPA—ZTNA Access Proxy Use Case

- Access control
  - Access to a specific application for only that session
- Ongoing verification
  - Verifies user identity, device posture, and users' rights using:
    - Client-device identification
    - Authentication
    - Zero-trust tags
- Direct connection to applications hosted behind FortiGate
  - TLS-encrypted tunnel automatically created from the endpoint to the access proxy
- Works well for TCP traffic

Training Institute

© Fortinet Inc. All Rights Reserved. 4

ZTNA is an access control method that uses client device identification, authentication, and zero-trust tags to provide role-based application access. ZTNA grants access to applications only after device verification, authenticating the user's identity, authorizing the user, and then performing context-based posture checks using zero-trust tags. ZTNA functionality offers a direct connection to protected resources, without having to establish a persistent VPN tunnel. ZTNA use cases work well for TCP-based applications.

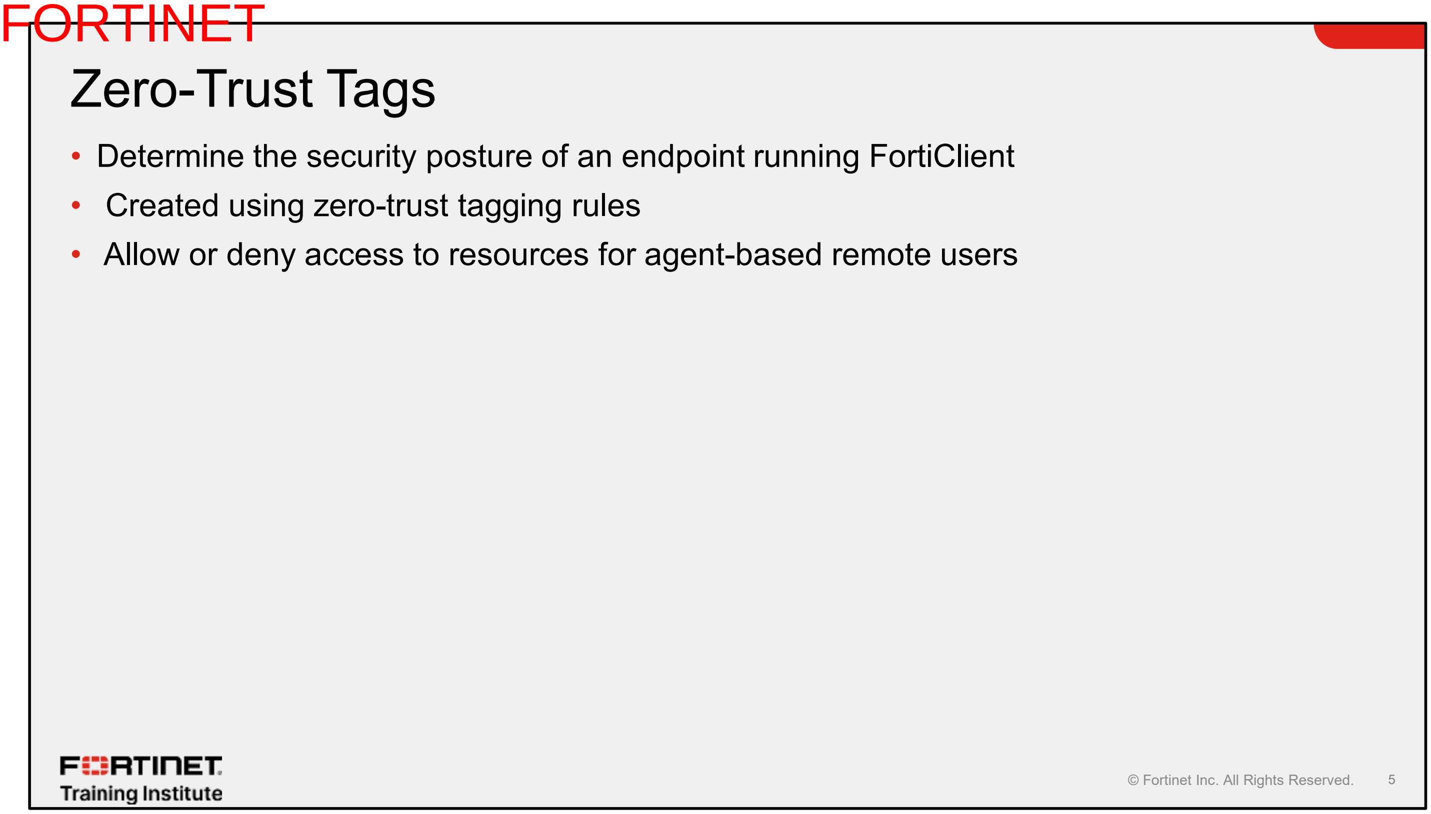
This use case offers a direct (shortest) path to private resources and per-session user authentication, resulting in greater performance and security. ZTNA has the following requirements:

- A FortiGate (on-premises or cloud deployment) configured as a ZTNA access proxy to control access to resources behind FortiGate, using zero-trust tags
- FortiClient installed on remote endpoints

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET

Brave-dumps.com



Zero-Trust Tags

- Determine the security posture of an endpoint running FortiClient
- Created using zero-trust tagging rules
- Allow or deny access to resources for agent-based remote users

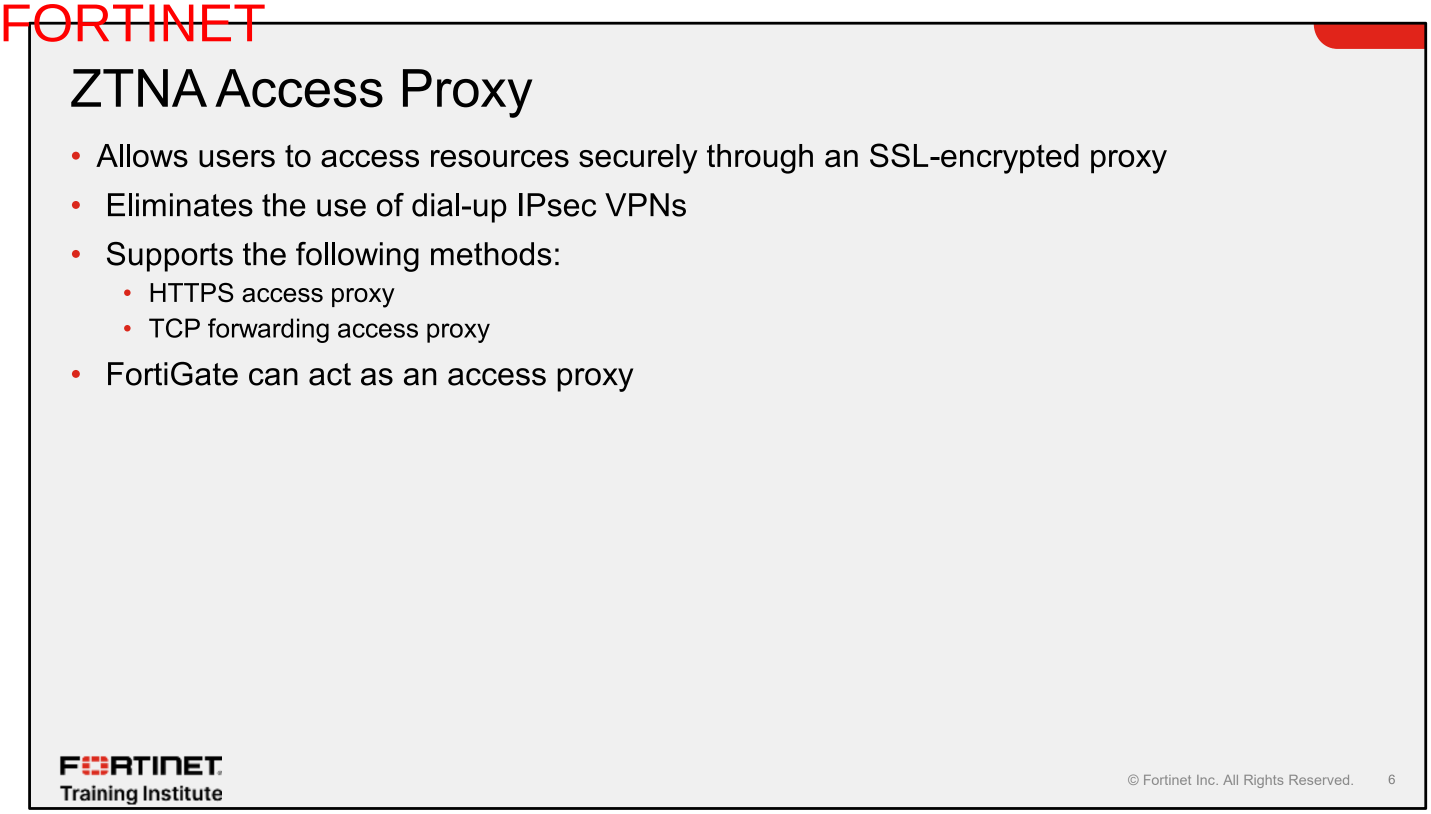
© Fortinet Inc. All Rights Reserved. 5

Zero-trust tags determine the security posture of an endpoint running FortiClient. You can configure zero-trust tags using the zero-trust tagging rules on FortiSASE. You can create zero-trust tagging rules for Windows, macOS, and Linux endpoints based on their OS versions, antivirus software installation, logged-in domains, running processes, and other criteria.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET

Brave-dumps.com



ZTNA Access Proxy

- Allows users to access resources securely through an SSL-encrypted proxy
- Eliminates the use of dial-up IPsec VPNs
- Supports the following methods:
  - HTTPS access proxy
  - TCP forwarding access proxy
- FortiGate can act as an access proxy

© Fortinet Inc. All Rights Reserved. 6

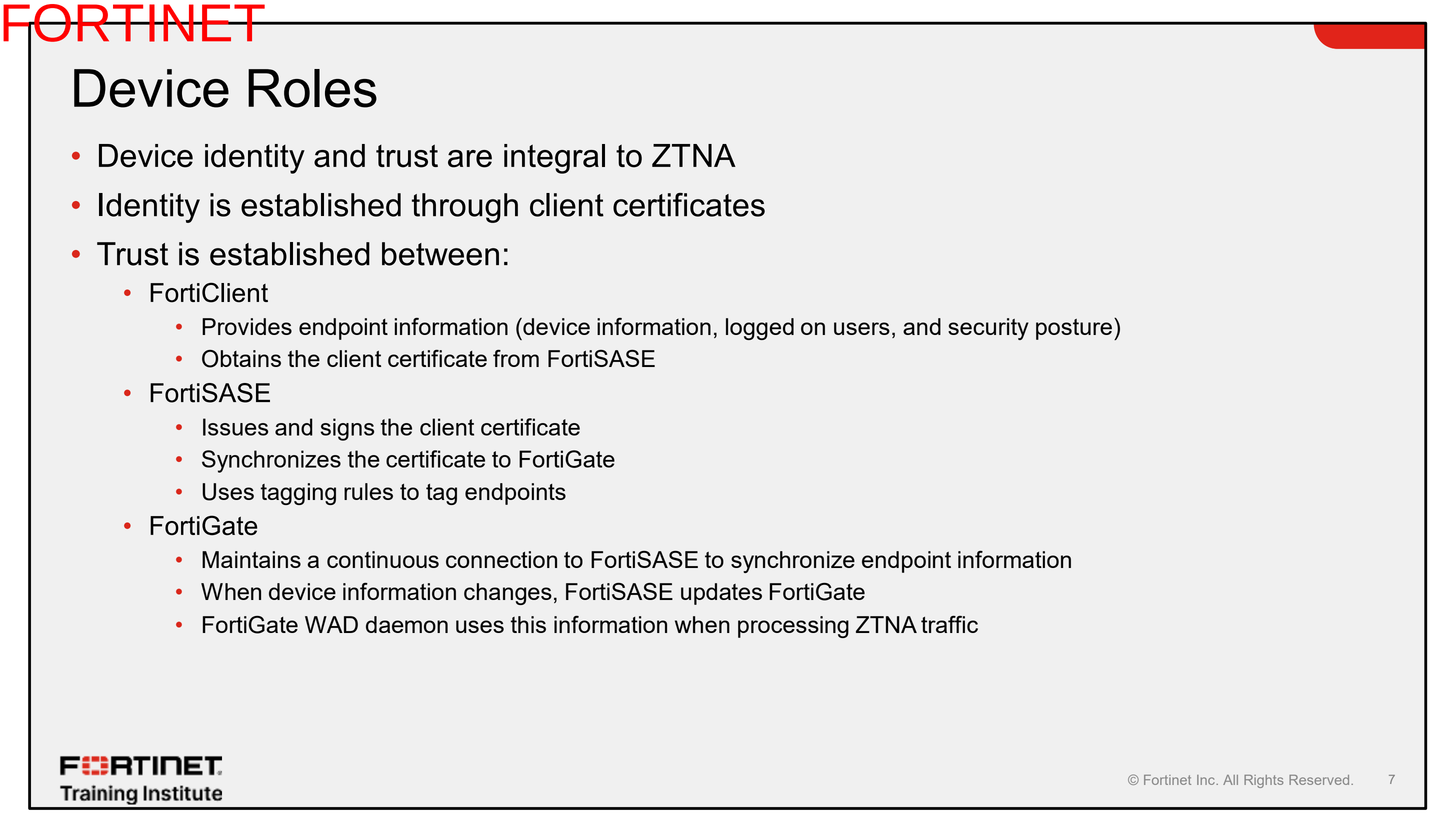
ZTNA access proxy allows users to securely access resources through an SSL-encrypted proxy by eliminating the use of dial-up IPsec VPNs. FortiGate can act as an access proxy and supports the following methods:

- HTTPS access proxy: works as a reverse proxy for the HTTP server. When a client connects to a web page hosted by the protected server, the address resolves to the FortiGate access proxy virtual IP (VIP). FortiGate proxies the connection and takes steps to authenticate the device. It prompts the user for the endpoint certificate on the browser, and verifies this against the ZTNA endpoint record that is synchronized from FortiSASE.
- TCP forwarding access proxy (TFAP): is configured to demonstrate an HTTPS reverse proxy that forwards TCP traffic to the designated resource. The access proxy tunnels TCP traffic between the client and FortiGate over HTTPS, and forwards the TCP traffic to the protected resource. It verifies user identity, device identity, and trust context, before granting access to the protected source.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET

Brave-dumps.com



Device Roles

- Device identity and trust are integral to ZTNA
- Identity is established through client certificates
- Trust is established between:
  - FortiClient
    - Provides endpoint information (device information, logged on users, and security posture)
    - Obtains the client certificate from FortiSASE
  - FortiSASE
    - Issues and signs the client certificate
    - Synchronizes the certificate to FortiGate
    - Uses tagging rules to tag endpoints
  - FortiGate
    - Maintains a continuous connection to FortiSASE to synchronize endpoint information
    - When device information changes, FortiSASE updates FortiGate
    - FortiGate WAD daemon uses this information when processing ZTNA traffic

© Fortinet Inc. All Rights Reserved. 7

Device identity and trust are integral to ZTNA. Device identity is established through client certificates, and trust is established among FortiClient, FortiSASE, and FortiGate devices. In ZTNA, devices perform specific roles.

FortiClient provides the following information to FortiSASE when it registers:

- Device information (network details, operating system, model, and so on)
- Logged-in user information
- Security posture (on-net and off-net, antivirus software, vulnerability status, and so on)

FortiClient also requests and obtains a client-device certificate from the FortiSASE certificate authority (CA) on its first attempt to connect to the access proxy. The client uses this certificate to identify itself to FortiGate.

FortiSASE issues and signs the client certificate with the FortiClient unique identifier (UID), certificate serial number (SN), and FortiSASE Endpoint Management Server (EMS) SN. FortiSASE then synchronizes the certificate with FortiGate. FortiSASE uses zero-trust tagging rules to tag endpoints based on the information that it has on each endpoint. FortiSASE also shares the tags with FortiGate.

FortiGate maintains a continuous connection to FortiSASE to synchronize endpoint device information such as FortiClient UID, client certificate SN, FortiSASE EMS SN, network details (IP and MAC address), and so on. When device information changes, such as when a client moves from on-net to off-net, or their security posture changes, FortiSASE updates the device information, and then updates the FortiGate.

Vouchers & Dumps are Available | WhatsApp +201224560923

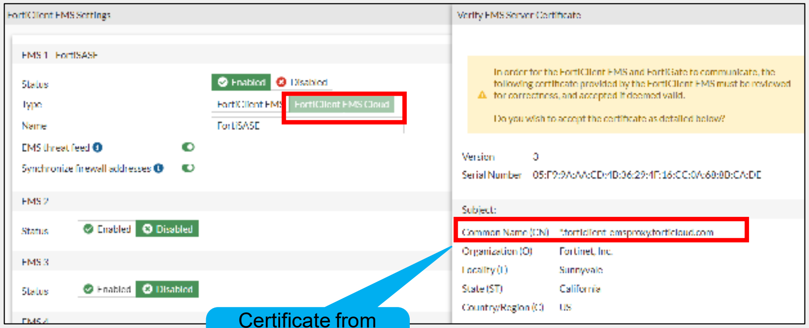
DO NOT REPRINT
© FORTINET

Brave-dumps.com

FortiGate and FortiSASE Connectivity

- FortiGate uses its FortiClient EMS cloud fabric connector to connect to FortiSASE
- You must register FortiGate and FortiSASE under the same FortiCloud account
  - FortiGate must verify the FortiSASE EMS server certificate
  - You must install the CA certificate on FortiGate, otherwise, the certificate is not trusted
- FortiSASE must authorize the FortiGate as a Fabric device

FortiGate: Security Fabric > Fabric Connectors



FortiClient EMS Settings

EMS 1 FortiSASE

Status: Enabled (selected) | Disabled
Type: FortiClient EMS | FortiClient EMS Cloud (selected)
Name: FortiSASE
EMS threat feed: ●
Synchronize firewall addresses: ●

EMS 2

Status: Enabled | Disabled (selected)

EMS 3

Status: Enabled | Disabled (selected)

EMS 4

Verify EMS Server Certificate

⚠ In order for the FortiClient EMS and FortiGate to communicate, the following certificate provided by the FortiClient EMS must be reviewed for correctness, and accepted if deemed valid.

Do you wish to accept the certificate as detailed below?

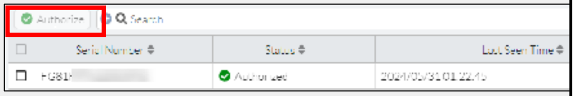
Version	3
Serial Number	05:F9:9A:AA:CD:4D:36:29:4F:16:CC:0A:68:8D:CA:DE

Subject:

Common Name (CN)	*fortliclient.emsproxy.forticloud.com
Organization (O)	Fortinet, Inc.
Locality (L)	Sunnyvale
State (ST)	California
Country/Region (C)	US

Certificate from FortiSASE EMS certificate

FortiSASE: Configuration > Endpoints > ZTNA Application Gateway



□	Serial Number	Status	Last Seen Time
□	FG81[redacted]	✓ Authorized	2024/05/31 01:22:15

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

To configure the FortiClient EMS connector on FortiGate, click **Security Fabric** > **Fabric Connectors**. Select **FortiClient EMS Cloud**, and FortiGate must accept the FortiSASE certificate. You must register FortiGate and FortiSASE under the same FortiCloud account.

Next, you must authorize FortiGate on FortiSASE. On FortiSASE, click **Configuration** > **ENDPOINTS** > **ZTNA Application Gateway**, select the FortiGate device, and then authorize it. Note that the FortiClient EMS connector status appears to be down until you authorize FortiGate on FortiSASE.

FortiGate automatically synchronizes ZTNA tags after it connects to FortiSASE.

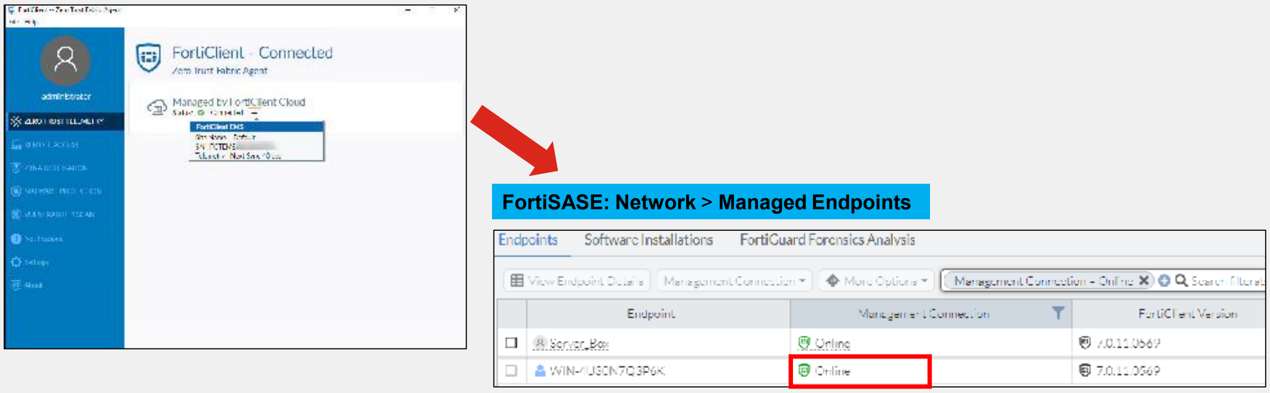
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET

Brave-dumps.com

FortiClient and FortiSASE Connectivity

- You connect FortiClient FortiSASE manually using the invitation code or using the preconfigured FortiClient installer with the included invitation code
- You can check the connection status on the FortiClient **ZERO TRUST TELEMETRY** menu or on the FortiSASE GUI under **Network** > **Managed Endpoints**



FortiClient - Connected
Zero Trust Fabric Agent

Managed by FortiClient Cloud
Status: Connected

FortiClient EMS
Site Name: Default
SN: FCTEMS[redacted]
Tel: Next Sync 70 sec

FortiSASE: Network > Managed Endpoints

	Endpoint	Management Connection	FortiClient Version
□	Server_Box	Online	7.0.11.0569
□	WIN-4U30N7Q3P6K	Online	7.0.11.0569

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved. 9

You must connect FortiClient to FortiSASE using the invitation code you received during user onboarding. Verify the connection status on the FortiClient console from the **ZERO TRUST TELEMETRY** menu, or on the FortiSASE GUI by clicking **Network** > **Managed Endpoints**.

Vouchers & Dumps are Available | WhatsApp +201224560923

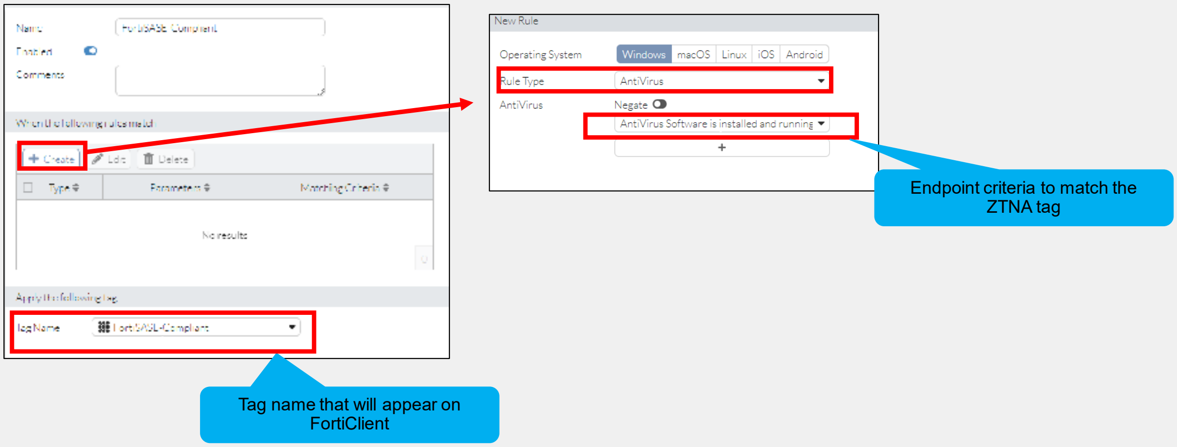
DO NOT REPRINT
© FORTINET

Brave-dumps.com

Zero-Trust Tagging Rules

- The type of zero-trust tagging rule depends on the OS you select

FortiSASE: Configuration > **ENDPOINTS** > **ZTNA Tagging**



Name: FortiSASE-Compliant
Enabled
Comments
When the following rules match

Type	Parameters	Matching Criteria
No results		

Apply the following tag
Tag Name: FortiSASE-Compliant

New Rule
Operating System: Windows | macOS | Linux | iOS | Android
Rule Type: AntiVirus
AntiVirus: Negate
AntiVirus Software is installed and running

Endpoint criteria to match the ZTNA tag

Tag name that will appear on FortiClient

© Fortinet Inc. All Rights Reserved. 10

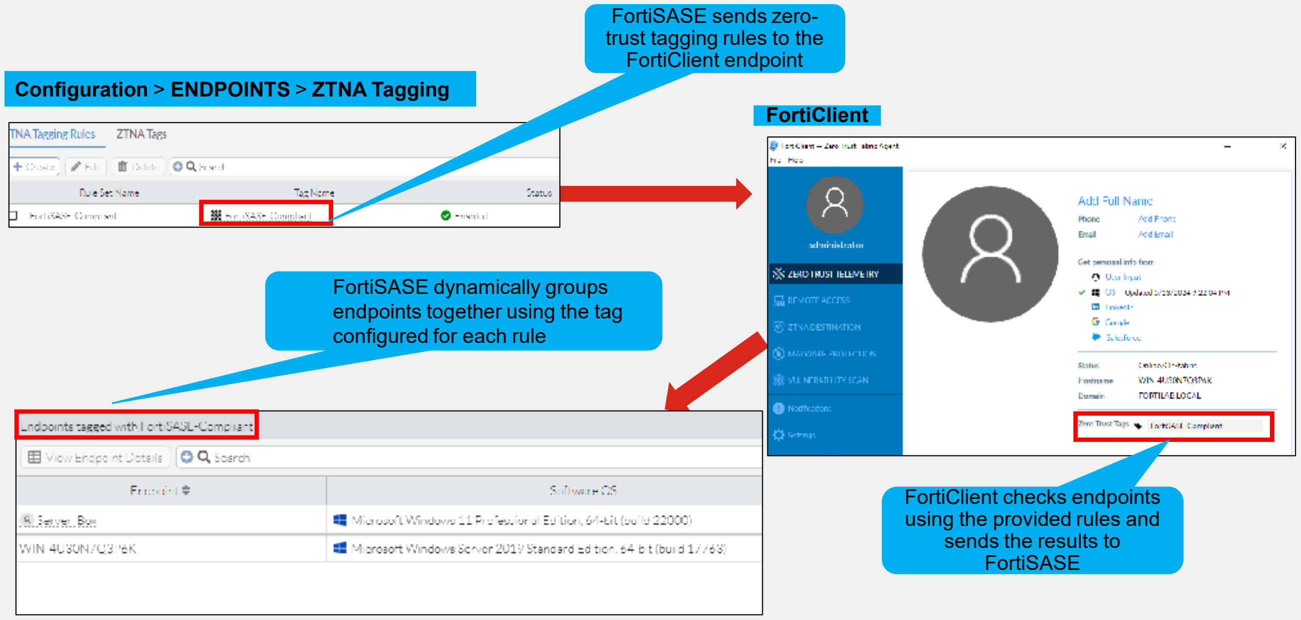
You can create, edit, and delete zero-trust tagging rules for Windows, macOS, Linux, iOS, and Android endpoints.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET

Brave-dumps.com

Zero-Trust Tags Workflow



FortiSASE sends zero-trust tagging rules to the FortiClient endpoint

Configuration > ENDPOINTS > ZTNA Tagging

ZTNA Tagging Rules | ZTNA Tags

+ Create | Edit | Delete | Search

	Rule Set Name	Tag Name	Status
□	FortiSASE-Compliant	FortiSASE-Compliant	✓ Enabled

FortiClient

FortiClient – Zero Trust Fabric Agent

File Help

administrator

ZERO TRUST TELEMETRY

REMOTE ACCESS

ZTNA DESTINATION

MALWARE PROTECTION

VULNERABILITY SCAN

Notifications

Settings

Add Full Name

Phone: Add Phone

Email: Add Email

Get personal info from:

User Input

✓ OS Updated 5/23/2024 7:22:04 PM

LinkedIn

Google

Salesforce

Status: Online/Off-fabric

Hostname: WIN-4U30N7O8PAK

Domain: FORTILAB.LOCAL

Zero Trust Tags: FortiSASE-Compliant

FortiSASE dynamically groups endpoints together using the tag configured for each rule

Endpoints tagged with FortiSASE-Compliant

View Endpoint Details | Search

Endpoint	Software OS
Server_Box	Microsoft Windows 11 Professional Edition, 64-bit (build 22000)
WIN-4U30N7Q3P6K	Microsoft Windows Server 2019 Standard Edition, 64-bit (build 17763)

FortiClient checks endpoints using the provided rules and sends the results to FortiSASE

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 11

This slide shows the zero-trust tags workflow. The following happens when you use zero-trust tagging rules with FortiSASE and FortiClient:

- FortiSASE sends zero-trust tagging rules to endpoints through telemetry communication.
- FortiClient checks endpoints using the provided rules and sends the results to FortiSASE.
- FortiSASE receives the results from FortiClient.
- FortiSASE dynamically groups endpoints together using the tag configured for each rule. To view the dynamic endpoint groups, click **Configuration** > **ENDPOINTS** > **ZTNA Tagging** > **ZTNA Tags**. Select the desired ZTNA tag, and then click **View Tagged Endpoints** to see which endpoint is tagged.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET

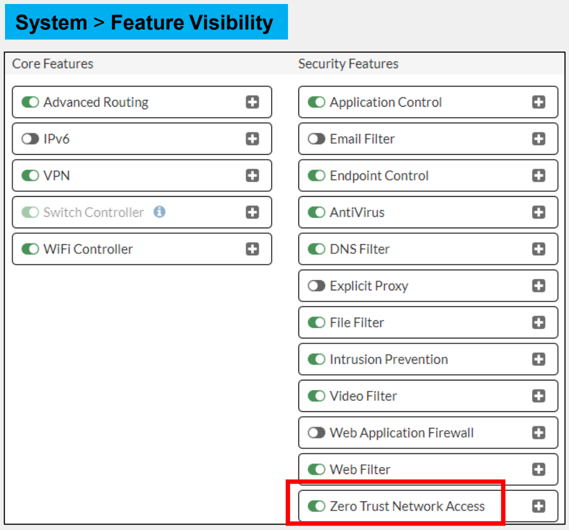
Brave-dumps.com

FortiGate ZTNA Configuration

- To enable ZTNA on the GUI, click **System** > **Feature Visibility**
- To deploy ZTNA on FortiGate, you need the following:
  - FortiClient EMS connector (to connect to FortiSASE)
  - ZTNA server
  - ZTNA tags synced from FortiSASE
  - ZTNA firewall policy
  - Authentication (optional)
- To enable ZTNA on entry-level models (below 100 series), enter the following commands:

```
config system global
set proxy-and-explicit-proxy enable
end
```

System > Feature Visibility



Core Features

- Advanced Routing
- IPv6
- VPN
- Switch Controller
- WiFi Controller

Security Features

- Application Control
- Email Filter
- Endpoint Control
- AntiVirus
- DNS Filter
- Explicit Proxy
- File Filter
- Intrusion Prevention
- Video Filter
- Web Application Firewall
- Web Filter
- Zero Trust Network Access

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 12

To enable ZTNA on the FortiGate GUI, click **System** > **Feature Visibility**, and then enable **Zero Trust Network Access**.

Configure ZTNA configuration on FortiGate as follows:

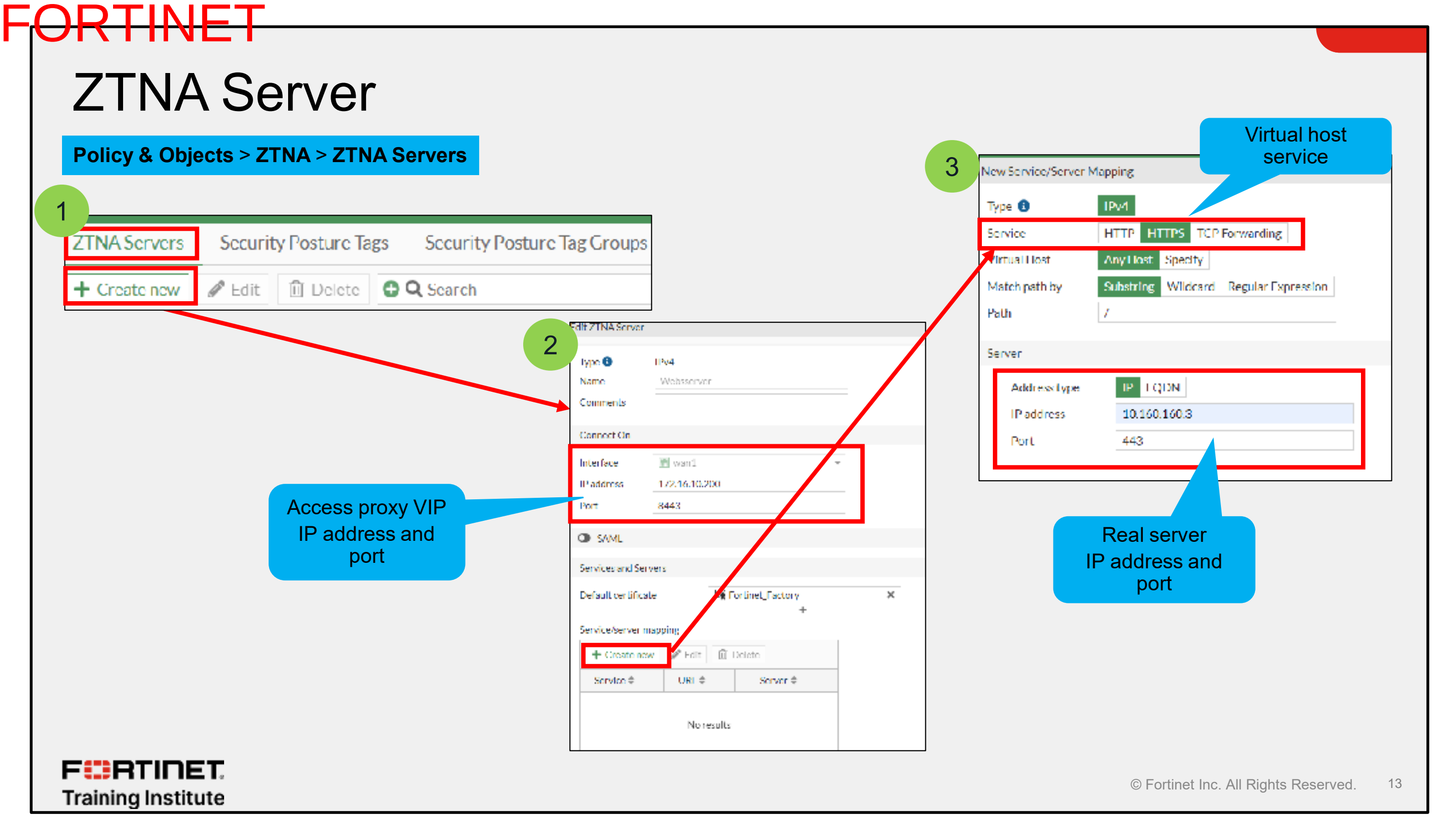
1. Add FortiClient EMS as a Fabric connector in the Security Fabric to connect to FortiSASE. FortiGate maintains a continuous connection to FortiSASE to synchronize endpoint device information, and automatically synchronizes ZTNA tags. You can create groups and add tags to use in the ZTNA policies.
2. On the ZTNA server, define the access proxy VIP and the real servers that clients connect to. Ensure that the firewall policy matches and redirects client requests to the access proxy VIP. You can also enable authentication.
3. Use a ZTNA firewall policy to enforce access control. Define ZTNA tags or tag groups to enforce zero-trust, role-based access. Configure security profiles to protect this traffic.

You can also configure authentication to the access proxy. ZTNA supports basic HTTP and SAML methods.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET

Brave-dumps.com



ZTNA Server

Policy & Objects > ZTNA > ZTNA Servers

1

ZTNA Servers | Security Posture Tags | Security Posture Tag Groups

+ Create new | Edit | Delete | Search

2

Edit ZTNA Server

Type: IPv4
Name: Webserver
Comments

Connect On
Interface: wan1
IP address: 172.16.10.200
Port: 8443

SAML

Services and Servers
Default certificate: Fortinet_Factory

Service/server mapping
+ Create new | Edit | Delete

Service	URL	Server
No results		

Access proxy VIP IP address and port

3

New Service/Server Mapping

Type: IPv4
Service: HTTP [✓ HTTPS] TCP Forwarding
Virtual Host: [✓ Any Host] Specify
Match path by: [✓ Substring] Wildcard Regular Expression
Path: /

Server
Address type: [✓ IP] FQDN
IP address: 10.160.160.3
Port: 443

Virtual host service

Real server IP address and port

© Fortinet Inc. All Rights Reserved.

After you add FortiClient EMS as the Fabric connector and you sync ZTNA tags with FortiGate, you must create a ZTNA server or access proxy. The access proxy VIP is the FortiGate ZTNA gateway that clients make HTTPS connections to. The service and server mappings define the virtual host matching rules and the real server mappings of the HTTPS requests.

The **Servers** table allows you to configure the real server IP address, port number, and status. You can configure multiple servers and server mappings.

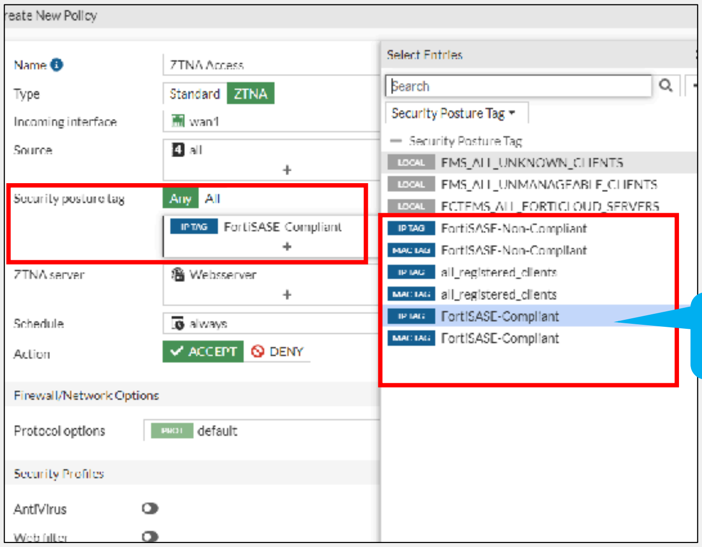
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET

Brave-dumps.com

ZTNA Policy

Policy & Objects > Firewall Policy



reate New Policy

Name: ZTNA Access
Type: Standard | ZTNA
Incoming interface: wan1
Source: all
Security posture tag: Any | All
IP TAG FortiSASE-Compliant
ZTNA server: Webserver
Schedule: always
Action: ✓ ACCEPT | DENY

Firewall/Network Options
Protocol options: PROT default

Security Profiles
AntiVirus ○
Web filter ○

Select Entries
Search
Security Posture Tag
Security Posture Tag
LOCAL FMS_ALL_UNKNOWN_CLIENTS
LOCAL FMS_ALL_UNMANAGEABLE_CLIENTS
LOCAL FCTEMS_ALL_FORTICLOUD_SERVERS
IP TAG FortiSASE-Non-Compliant
MAC TAG FortiSASE-Non-Compliant
IP TAG all_registered_clients
MAC TAG all_registered_clients
IP TAG FortiSASE-Compliant
MAC TAG FortiSASE-Compliant

ZTNA tags synced from FortiSASE

FERTINET Training Institute

© Fortinet Inc. All Rights Reserved. 14

A ZTNA policy is used to enforce access control. You can define security posture (ZTNA) tags or tag groups to enforce zero-trust, role-based access. To create a policy, type a policy name, set the policy type to **ZTNA**, and add IP addresses and ZTNA tags, or tag groups with allowed or blocked access. You can also select the configured ZTNA server and apply security profiles to protect this traffic. If authentication is enabled, you need to add user groups in ZTNA policy in the **Source** field, otherwise no policy match will take place.

Vouchers & Dumps are Available | WhatsApp +201224560923

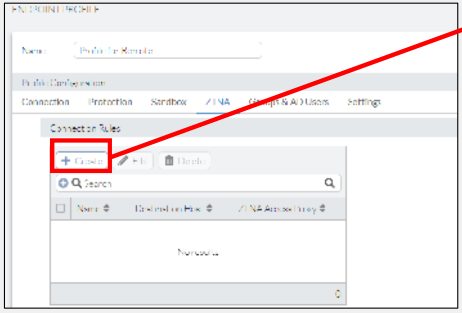
DO NOT REPRINT
© FORTINET

Brave-dumps.com

ZTNA TFAP

- User must create a ZTNA rule on FortiSASE and provision it to FortiClient
- You can also configure a ZTNA TFAP without encryption
  - Improves performance by reducing encryption overhead of an already secure underlying protocol
  - Do not use for insecure protocols

ENDPOINTS > Profiles



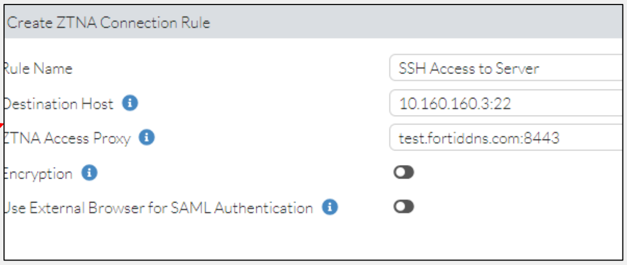
ENDPOINT PROFILE

Name: Profile for Remote

Profile Configuration

☐	Name ⬍	Destination Host ⬍	ZTNA Access Proxy ⬍
		No results	

0



Create ZTNA Connection Rule

Rule Name	SSH Access to Server
Destination Host ℹ	10.160.160.3:22
ZTNA Access Proxy ℹ	test.fortiddns.com:8443
Encryption ℹ	○
Use External Browser for SAML Authentication ℹ	○

© Fortinet Inc. All Rights Reserved.

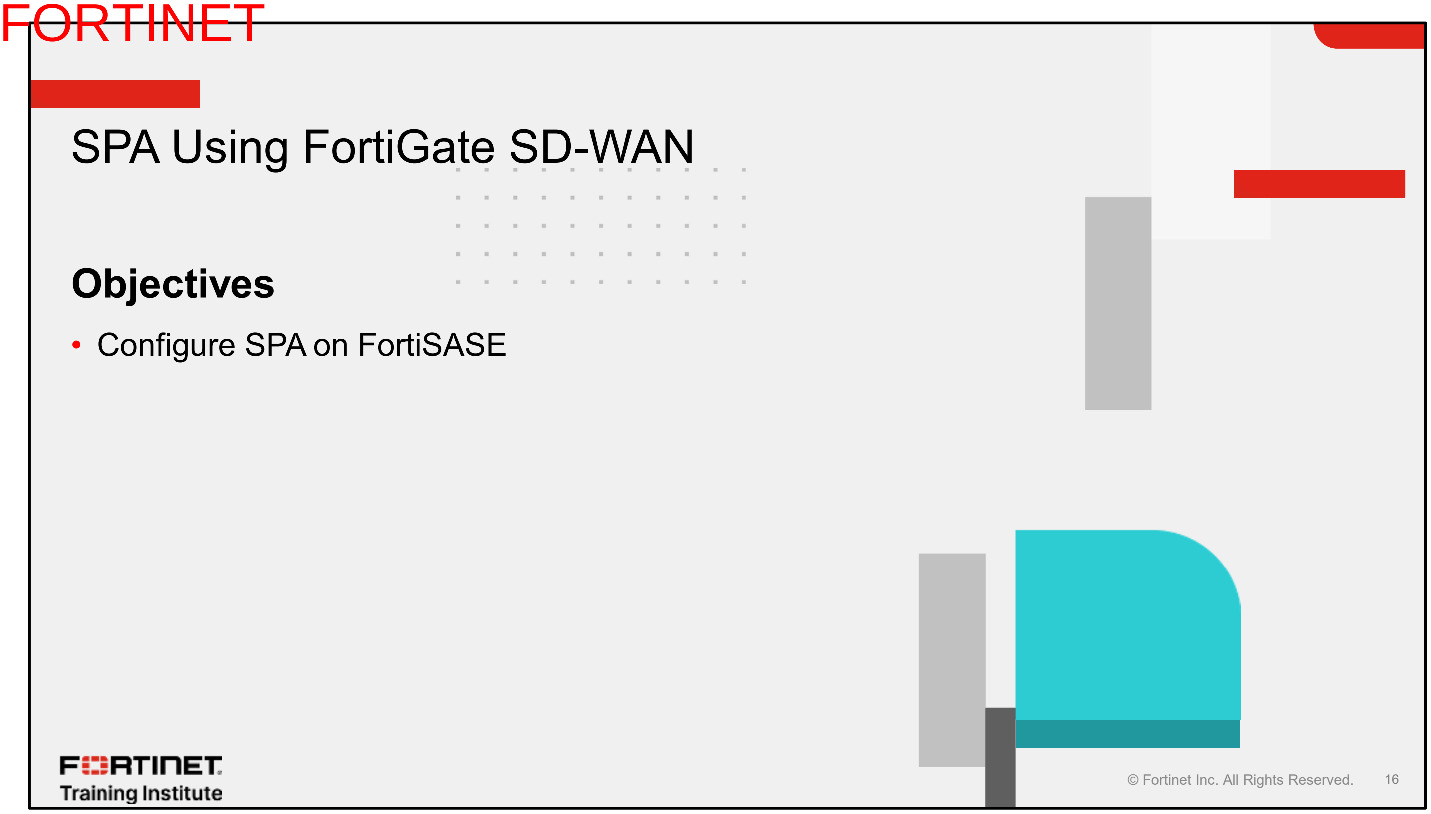
Before connecting, users must create a ZTNA rule on the FortiSASE endpoint profile and provision it to FortiClient. ZTNA connection rules dictate which destination host and ZTNA access proxy traffic is forwarded to. Note that the **Destination Host** field indicates the real internal IP address and port of the server.

You can also configure a ZTNA TFAP without encryption. The connection still begins with a TLS handshake. The client uses the HTTP 101 response to switch protocols and remove the HTTPS stack. Further end-to-end communication between the client and server is encapsulated in the specified TCP port; the access proxy does not encrypt it. This improves performance by reducing the overhead of encrypting an already secured underlying protocol, such as RDP, SSH, or FTPS. Users should still enable the encryption option for end-to-end protocols that are insecure. In a real-life application, you should use the encryption option for an insecure protocol such as Telnet.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET

Brave-dumps.com



SPA Using FortiGate SD-WAN

Objectives

- Configure SPA on FortiSASE

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved. 16

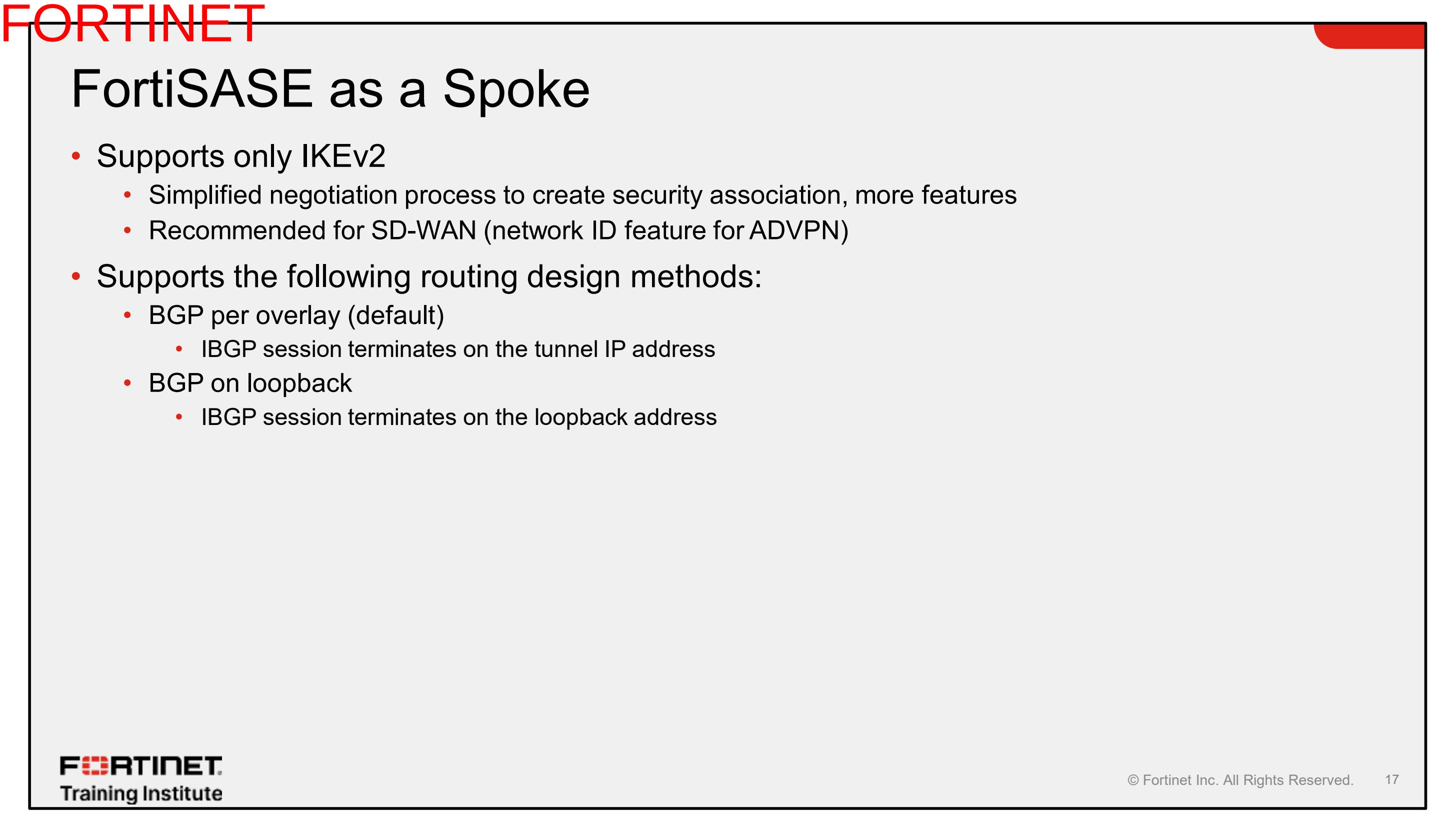
After completing this section, you should be able to achieve the objective shown on this slide.

By demonstrating competence in understanding the configuration of SPA, you will be able to configure SPA on FortiSASE and implement it in your SD-WAN environment.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET

Brave-dumps.com



FortiSASE as a Spoke

- Supports only IKEv2
  - Simplified negotiation process to create security association, more features
  - Recommended for SD-WAN (network ID feature for ADVPN)
- Supports the following routing design methods:
  - BGP per overlay (default)
    - IBGP session terminates on the tunnel IP address
  - BGP on loopback
    - IBGP session terminates on the loopback address

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 17

You can leverage FortiSASE SPA so that a point of presence (POP) connects to a standalone hub using IPsec, or to an existing Fortinet SD-WAN deployment. You can establish the BGP protocol via IPsec links for dynamic route exchange to give access to private resources for FortiSASE remote users.

You should always configure FortiSASE connections toward the hubs. Using the Fortinet proprietary auto-discovery VPN (ADVPN) protocol, FortiSASE dynamically establishes direct IPsec links to the rest of the spokes on the network. If a private resource is behind an organization's spoke device, it can connect directly to that resource through an on-demand tunnel.

FortiSASE spokes support only IKEv2 for IPsec tunnels to the hub. IKEv2 supports the network ID feature, which enables the administrator to establish multiple tunnels between the same local and remote gateways, which can be required during failover scenarios involving SD-WAN and ADVPN.

FortiSASE supports the following routing design methods:

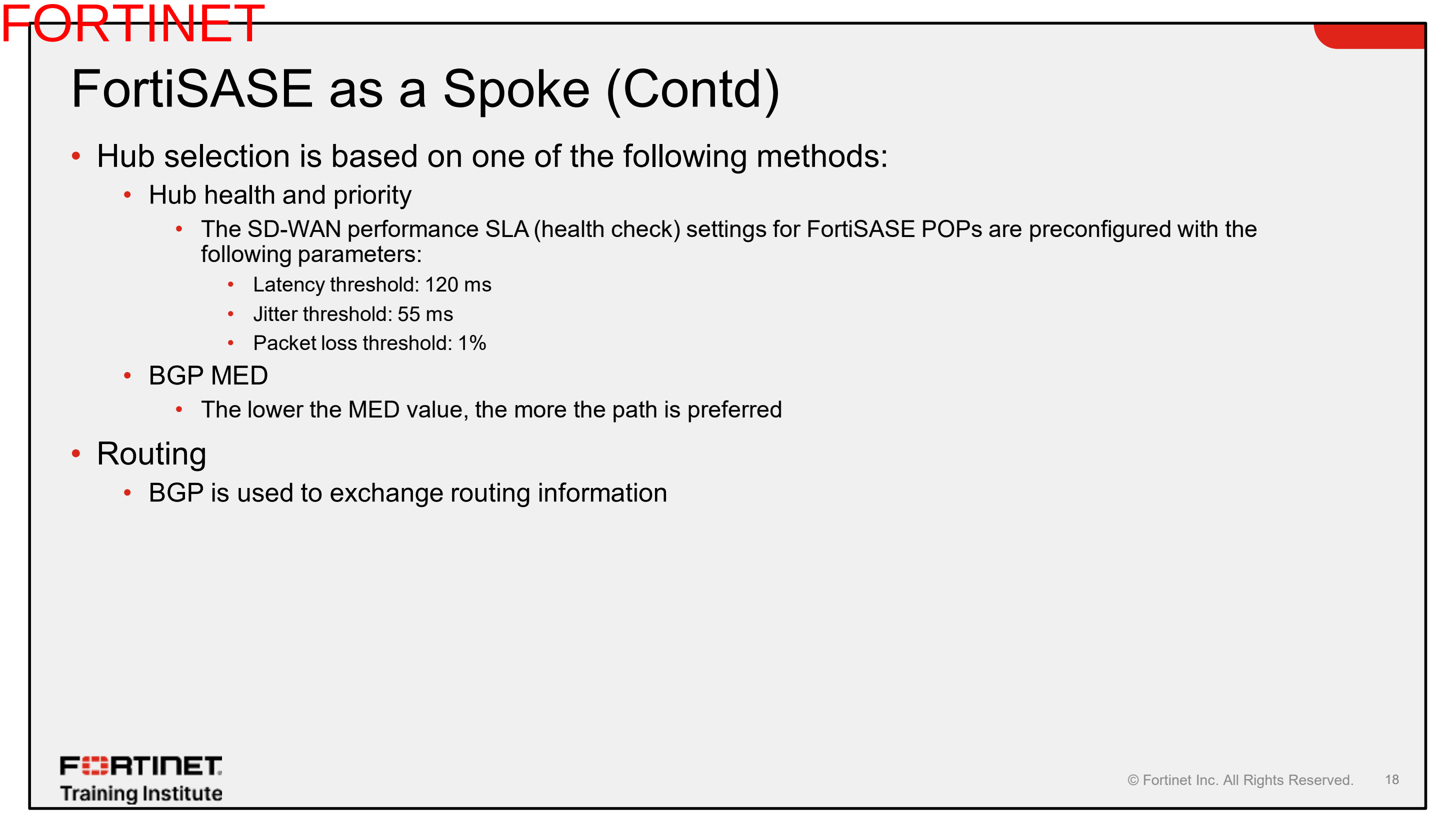
- BGP per overlay: This is the default routing design method on FortiSASE. Each spoke establishes a separate IBGP session toward each hub. Each IBGP session terminates on the tunnel with the corresponding IP address. You must enable mode-cfg on the FortiGate hub to assign an IP address to the FortiSASE spoke tunnel interface.
- BGP on loopback: This method simplifies the configuration on the hub side and reduces the number of routes advertised on the network. Each spoke establishes a single IBGP session to each hub. The IBGP session terminates on the loopback interface, which uniquely defines each SD-WAN node.

You must use the same BGP routing designs for *all* hubs and spokes. You cannot mix them.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET

Brave-dumps.com



FortiSASE as a Spoke (Contd)

- Hub selection is based on one of the following methods:
  - Hub health and priority
    - The SD-WAN performance SLA (health check) settings for FortiSASE POPs are preconfigured with the following parameters:
      - Latency threshold: 120 ms
      - Jitter threshold: 55 ms
      - Packet loss threshold: 1%
  - BGP MED
    - The lower the MED value, the more the path is preferred
- Routing
  - BGP is used to exchange routing information

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 18

FortiSASE supports the following hub selection methods:

- Hub health and priority: FortiSASE has a built-in SD-WAN engine for intelligent routing selection among the established IPsec links. The health check IP address periodically receives jitter, latency, and packet loss for each service connection. FortiSASE selects the highest priority hub within each POP, that meets lowest-cost service-level agreement (SLA) requirements.

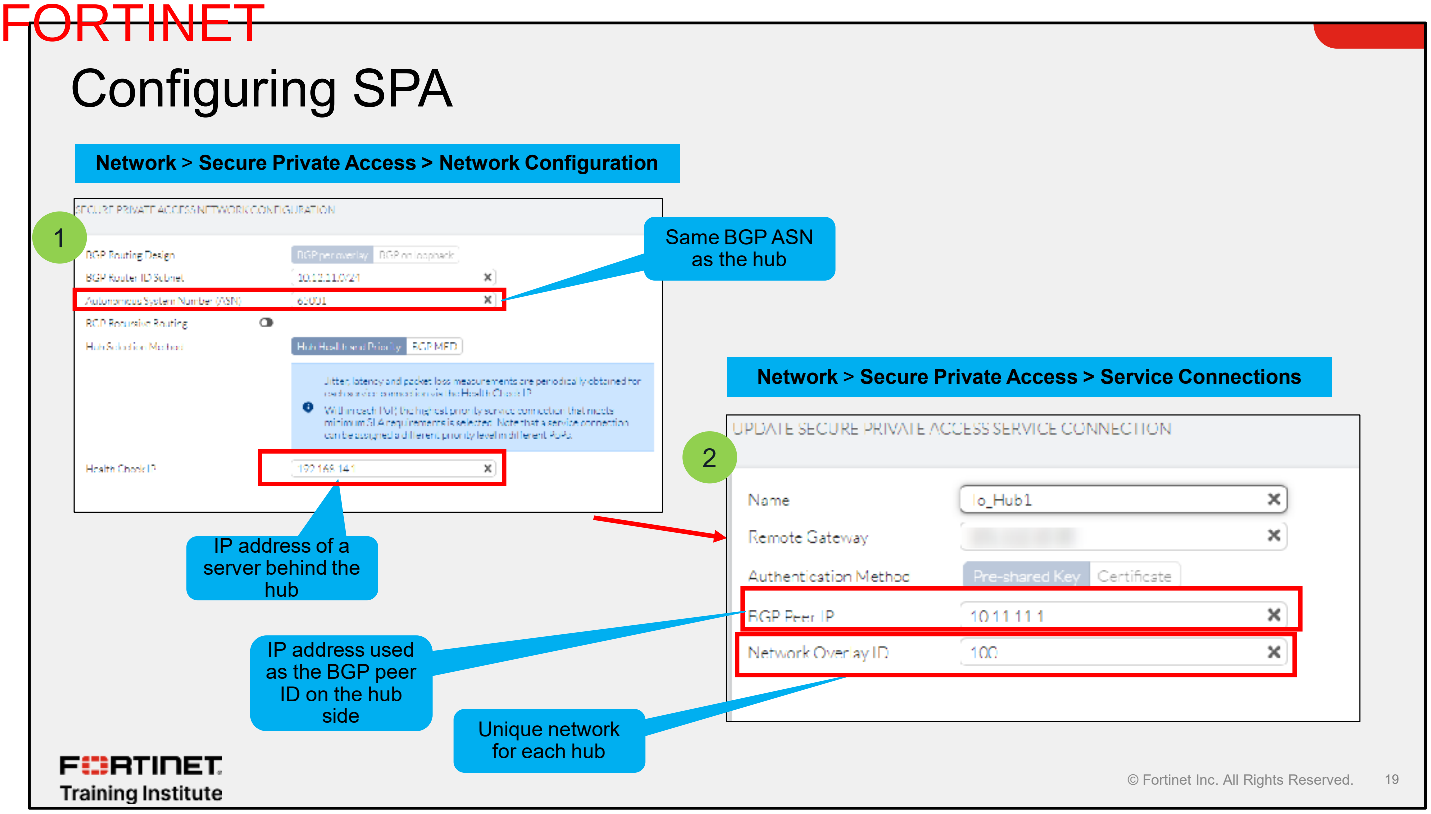
- BGP multi-exit discriminator (MED): a BGP path attribute that discriminates among multiple exit or entry points to the same neighboring AS. The lower the MED value, the more preferred the path is to the receiving router.

The goal of using BGP as the preferred routing protocol is for all the nodes in the SD-WAN network to exchange their prefixes, and to support ADVPN with SD-WAN if needed.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET

Brave-dumps.com



Configuring SPA

Network > Secure Private Access > Network Configuration

1

SECURE PRIVATE ACCESS NETWORK CONFIGURATION

BGP Routing Design: BGP per overlay | BGP on loopback
BGP Router ID Subnet: 10.12.11.0/24
Autonomous System Number (ASN): 65001
BGP Recursive Routing
Hub Selection Method: Hub Health and Priority | BGP MED

Jitter, latency and packet loss measurements are periodically obtained for each service connection via the Health Check IP.
Within each POP, the highest priority service connection that meets minimum SLA requirements is selected. Note that a service connection can be assigned a different priority level in different POPs.

Health Check IP: 192.168.14.1

Same BGP ASN as the hub

IP address of a server behind the hub

Network > Secure Private Access > Service Connections

2

UPDATE SECURE PRIVATE ACCESS SERVICE CONNECTION

Name: lo_Hub1
Remote Gateway: [redacted]
Authentication Method: Pre-shared Key | Certificate
BGP Peer IP: 10.11.11.1
Network Overlay ID: 100

IP address used as the BGP peer ID on the hub side

Unique network for each hub

FURTINET Training Institute

© Fortinet Inc. All Rights Reserved. 19

You can configure SPA on FortiSASE on the **Secure Private Access** page.

Click on the **Network Configuration** tab to enter the BGP-related configuration information. You must configure the following parameters:

- **BGP Routing Design**: Select **BGP per overlay** or **BGP On loopback**.
- **BGP Router ID Subnet**: FortiSASE assigns an address from this subnet to the loopback interface as the BGP router ID. This configuration is beneficial if you select **BGP on loopback**.
- **Autonomous System Number (ASN)**: Select the same BGP ASN as the hub.
- **BGP Recursive Routing**: Enable BGP recursive routing to allow interhub connectivity and redundancy to networks behind the active hub, if each hub has a physical connection to the others, for cases when connectivity between a FortiSASE security POP and the active hub fails.
- **Hub Selection Method:** Select **Hub Health and Priority** or **BGP MED**.
- **Health Check IP**: Select the IP address of a server behind the hub you should use to set up the SD-WAN performance SLA rule.

Save the network configuration, then click on the **Service Connections** tab. You must configure the following parameters:

Name: a name for the service connection.
Remote Gateway: the public IP address of the FortiGate hub
Authentication Method: a pre-shared key or PKI certificate
BGP Peer IP: IP address used as the BGP peer ID on the hub side
Network Overlay ID: unique network ID defined on each hub

Vouchers & Dumps are Available | WhatsApp +201224560923

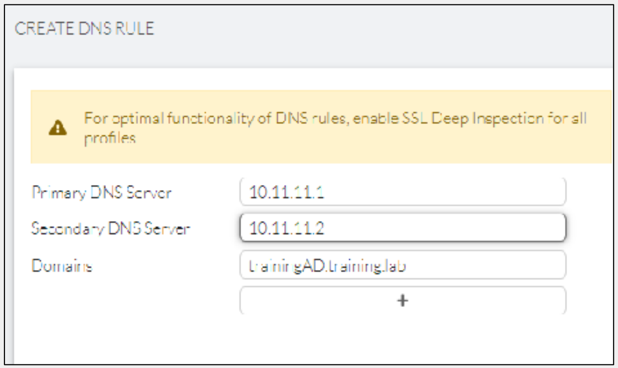
DO NOT REPRINT
© FORTINET

Brave-dumps.com

Configuring DNS Rules

- Required to resolve internal host names
- The endpoint reflects a DNS configuration if the FortiClient connects to FortiSASE after you change it

Configuration > **NETWORK** > **DNS**



CREATE DNS RULE

⚠ For optimal functionality of DNS rules, enable SSL Deep Inspection for all profiles

Primary DNS Server: 10.11.11.1

Secondary DNS Server: 10.11.11.2

Domains: trainingAD.training.lab

+

© Fortinet Inc. All Rights Reserved.

FortiSASE agent-based users often need to resolve internal host names that public DNS servers can’t resolve when connected remotely through FortiClient. Any domains defined in the DNS rules are always resolved using the primary and secondary DNS servers defined in the explicit DNS rule. The endpoint reflects any change you make to the DNS configuration only if the FortiClient VPN connects to FortiSASE after you make the change.

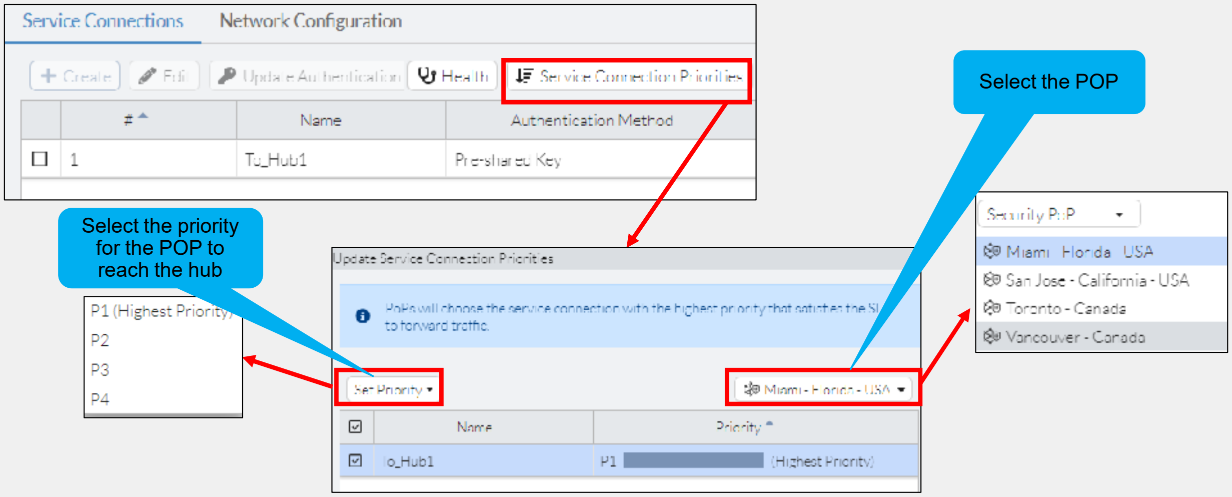
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET

Brave-dumps.com

Service Connection Priority

Network > Secure Private Access



#	Name	Authentication Method
1	To_Hub1	Pre-shared Key

Update Service Connection Priorities

PoPs will choose the service connection with the highest priority that satisfies the SL to forward traffic.

Name	Priority
To_Hub1	P1 (Highest Priority)

Select the POP

Select the priority for the POP to reach the hub

© Fortinet Inc. All Rights Reserved. 21

You can configure service connection priority on the **Secure Private Access** page. This configuration applies when the hub selection method is **Hub Health and Priority**. You can assign a different priority level to a hub in different POPs on the **Service Connection Priorities** page. FortiSASE selects the highest priority hub, if it satisfies the predefined SLA thresholds.

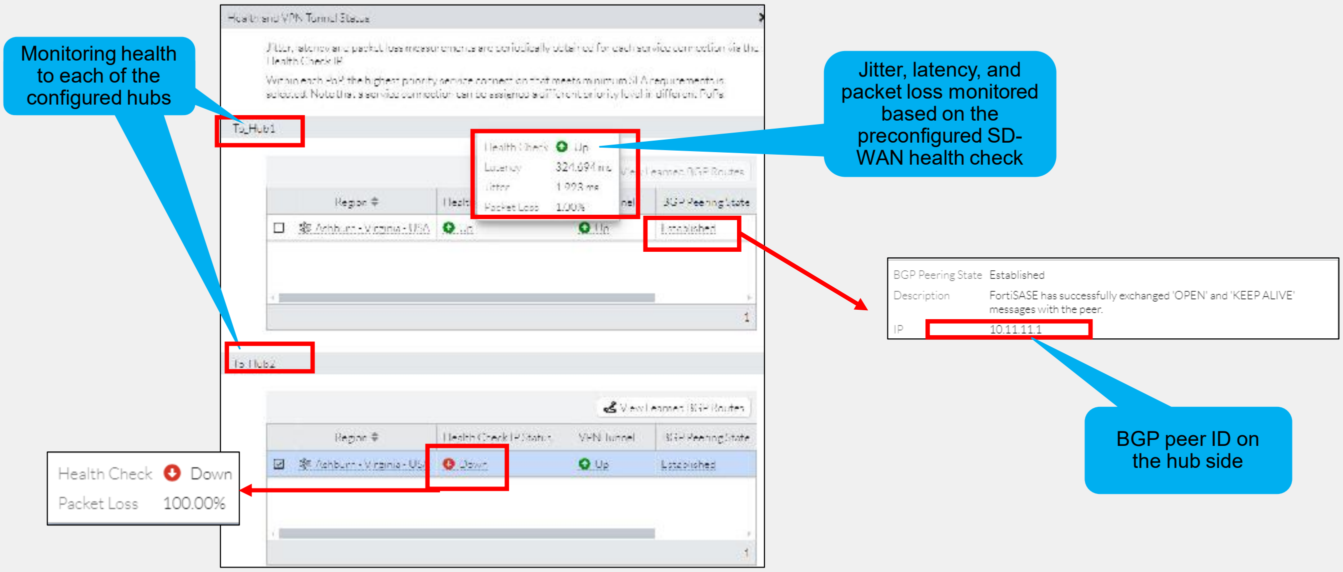
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET

Brave-dumps.com

Monitoring Health

Network > Secure Private Access



Health and VPN Tunnel Status

Jitter, latency and packet loss measurements are periodically obtained for each service connection via the Health Check IP.

Within each PoP the highest priority service connection that meets minimum SLA requirements is selected. Note that a service connection can be assigned a different priority level in different PoPs.

To_Hub1

View Learned BGP Routes

	Region	Health Check IP Status	VPN Tunnel	BGP Peering State
☐	Ashburn - Virginia - USA	Up	Up	Established

Health Check	Up
Latency	324.694 ms
Jitter	1.993 ms
Packet Loss	1.00%

To_Hub2

View Learned BGP Routes

	Region	Health Check IP Status	VPN Tunnel	BGP Peering State
☑	Ashburn - Virginia - USA	Down	Up	Established

Health Check	Down
Packet Loss	100.00%

BGP Peering State	Established
Description	FortiSASE has successfully exchanged 'OPEN' and 'KEEP ALIVE' messages with the peer.
IP	10.11.11.1

Monitoring health to each of the configured hubs

Jitter, latency, and packet loss monitored based on the preconfigured SD-WAN health check

BGP peer ID on the hub side

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

22

To view the health check IP, VPN tunnel status, and BGP peering state for specific hubs, on the **Secure Private Access** page click **Health**. Hover your mouse over a status state to display its statistics.

In the example shown on this slide, the FortiSASE instance has one POP deployed, and it's configured as a spoke to two different hubs. The health check status **To_Hub2** is down because it’s not reachable, and the FortiSASE SD-WAN monitor displays a 100% packet loss. If there are multiple POPs deployed, the connection status to the hub from each POP is shown.

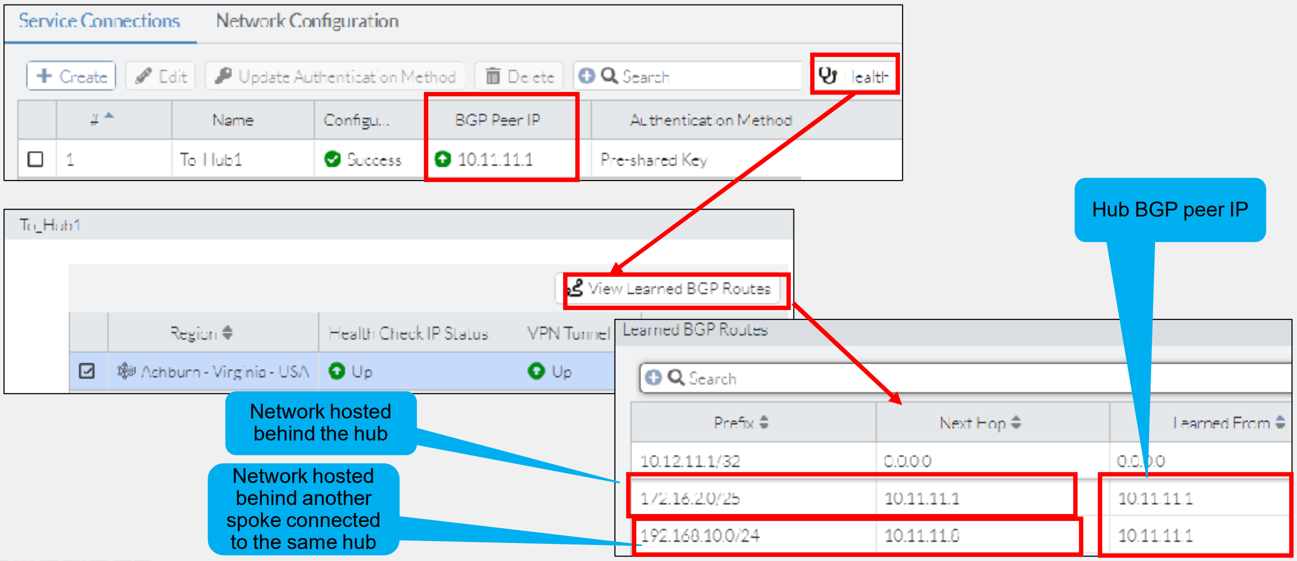
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET

Brave-dumps.com

Routing Table

Network > Secure Private Access



#	Name	Configu...	BGP Peer IP	Authentication Method
□ 1	To Hub1	✓ Success	10.11.11.1	Pre-shared Key

	Region	Health Check IP Status	VPN Tunnel
☑	Ashburn - Virginia - USA	Up	Up

Prefix	Next Hop	Learned From
10.12.11.1/32	0.0.0.0	0.0.0.0
172.16.2.0/25	10.11.11.1	10.11.11.1
192.168.10.0/24	10.11.11.8	10.11.11.1

Network hosted behind the hub

Network hosted behind another spoke connected to the same hub

© Fortinet Inc. All Rights Reserved. 23

To view the routing table, on the **Secure Private Access** page, click **Health**. Select the security POP and then click **View Learned BGP Routes**. The GUI displays the routes that the hub is advertising on the FortiSASE spoke. The routes include networks hosted behind the hub, and networks hosted behind other spokes that are advertised to the same hub.

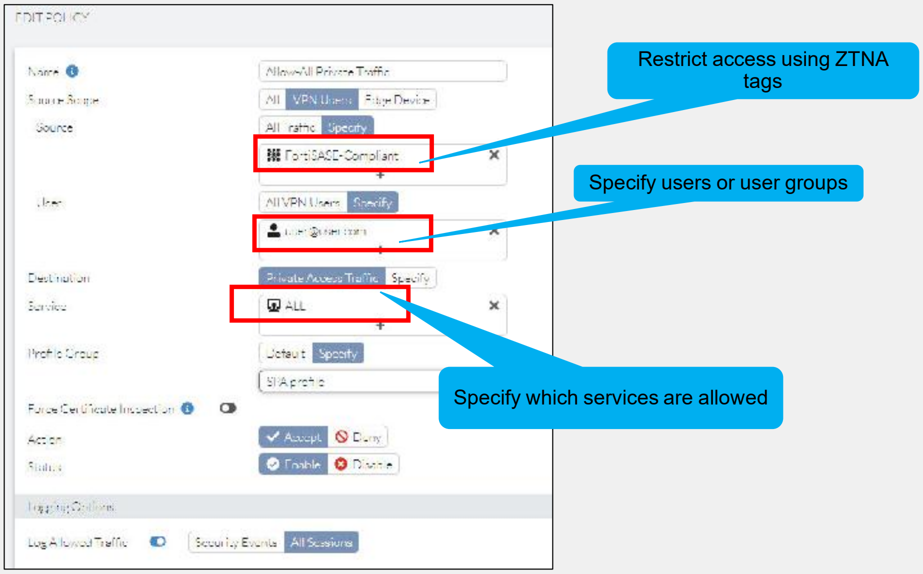
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET

Brave-dumps.com

Configuring Policies—Private Access for VPN Users

Configuration > TRAFFIC > Policies > Private Access



EDIT POLICY

Name: Allow-All Private Traffic

Source Scope: All | VPN Users | Edge Device

Source: All Traffic | Specify

FortiSASE-Compliant

User: All VPN Users | Specify

user@user.com

Destination: Private Access Traffic | Specify

Service: ALL

Profile Group: Default | Specify

SIA profile

Force Certificate Inspection

Action: ✓ Accept | Deny

Status: Enable | Disable

Logging Options

Log Allowed Traffic: Security Events | All Sessions

Restrict access using ZTNA tags

Specify users or user groups

Specify which services are allowed

© Fortinet Inc. All Rights Reserved. 24

You can use the private access policy to restrict access to private applications of any protocol (TCP, UDP, ICMP, and so on) behind a FortiGate hub or spokes connected to that hub. You can also apply ZTNA tags to remote users, based on specified endpoint posture checks.

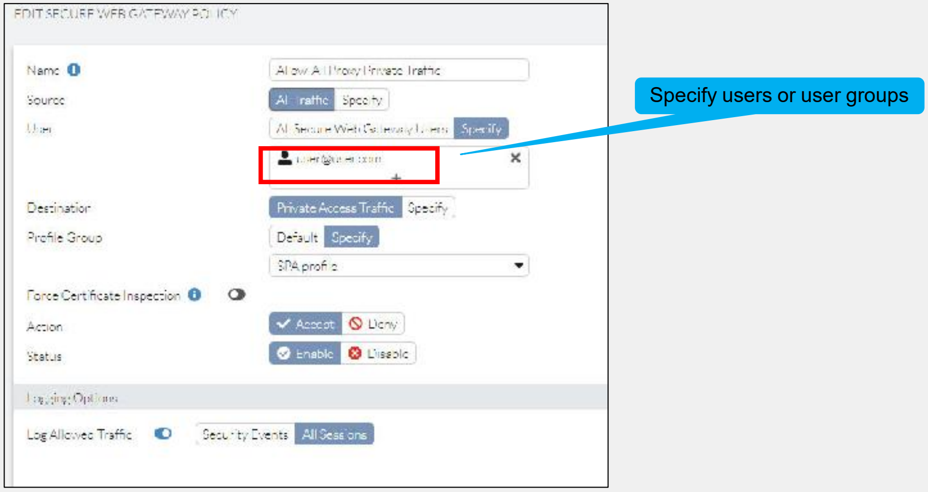
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET

Brave-dumps.com

Configuring Policies—Private Access for SWG Users

Configuration > **TRAFFIC** > **SWG Policies** > **Private Access**



EDIT SECURE WEB GATEWAY POLICY

Name: Allow All Proxy Private Traffic

Source: All Traffic | Specify

User: All Secure Web Gateway Users | Specify

user@[illegible]

Destination: Private Access Traffic | Specify

Profile Group: Default | Specify

SPA profile

Force Certificate Inspection

Action: ✓ Accept | Deny

Status: Enable | Disable

Logging Options

Log Allowed Traffic: Security Events | All Sessions

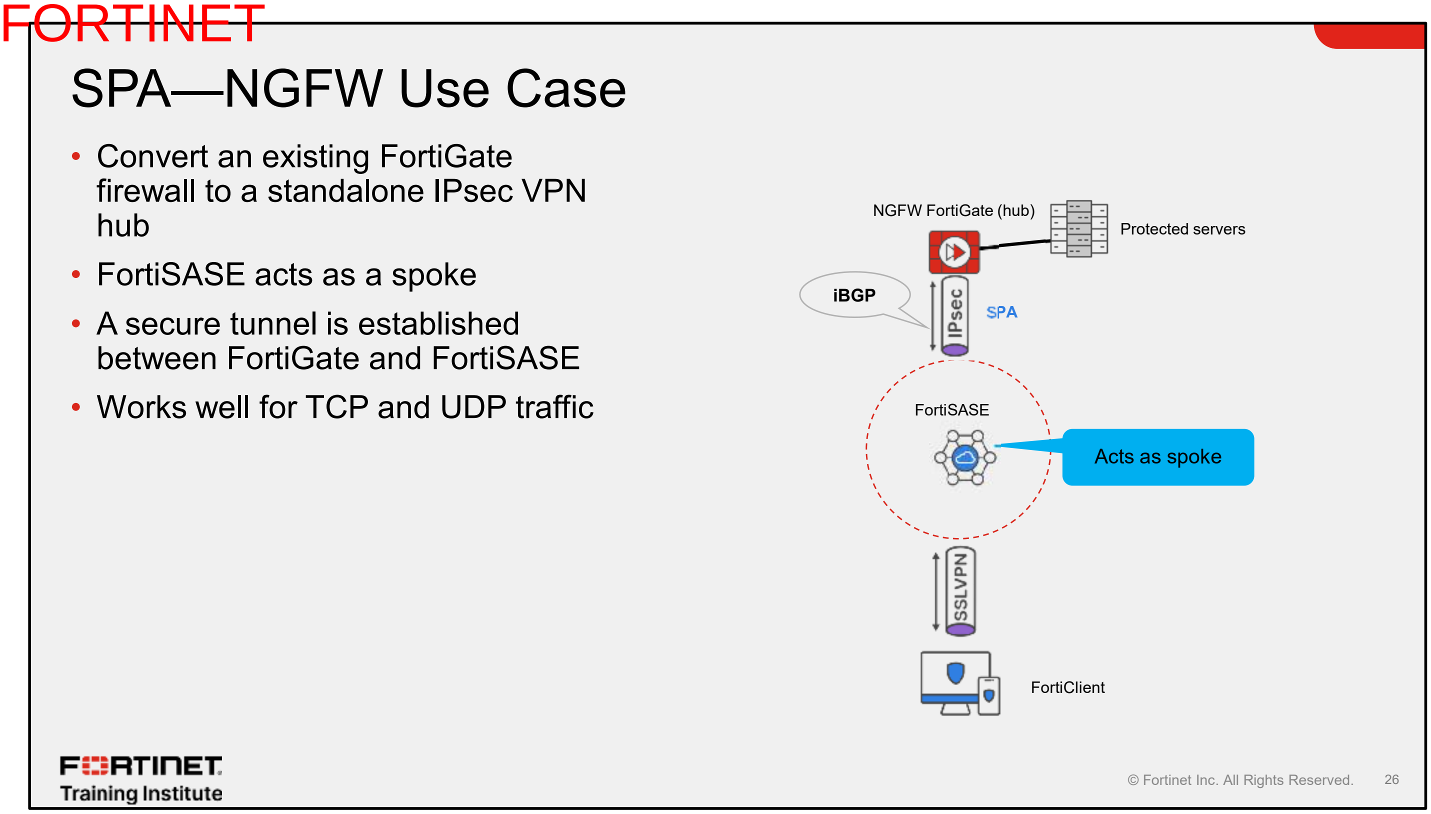
Specify users or user groups

You can use the private access policy for secure web gateway (SWG) users to allow only HTTP and HTTPS access to resources behind the FortiGate hub. Since there is no endpoint deployment for SWG users, ZTNA tags are not supported.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET

Brave-dumps.com



SPA—NGFW Use Case

- Convert an existing FortiGate firewall to a standalone IPsec VPN hub
- FortiSASE acts as a spoke
- A secure tunnel is established between FortiGate and FortiSASE
- Works well for TCP and UDP traffic

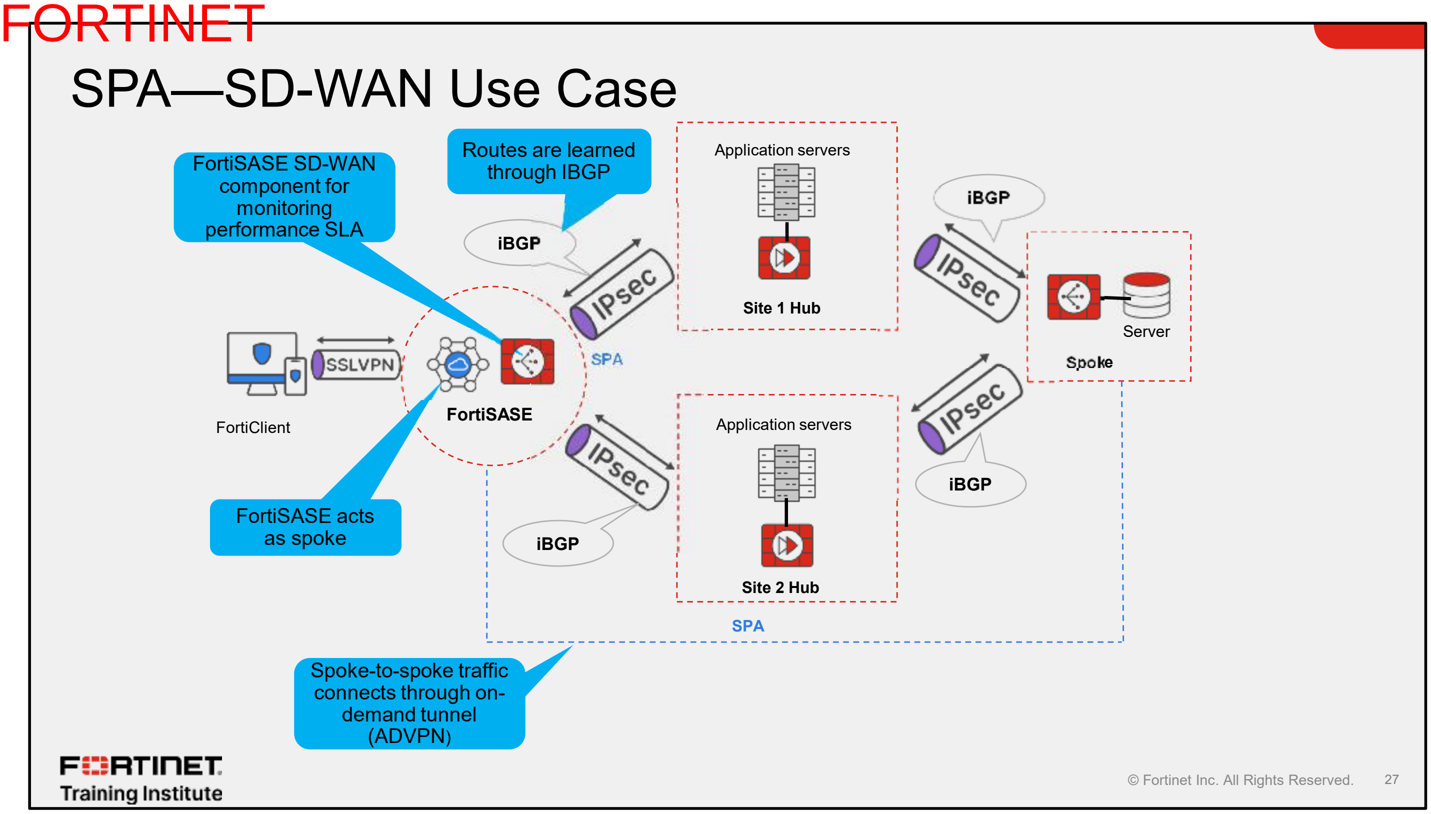
© Fortinet Inc. All Rights Reserved. 26

In the SPA NGFW use case, you must convert your existing FortiGate NGFW to a standalone IPsec VPN hub. The FortiSASE POP acts as a spoke to this FortiGate NGFW hub. A secure tunnel is established between the FortiSASE POPs and FortiGate NGFW, and IBGP is used to route traffic between them. FortiSASE remote users can access private resources behind FortiGate hubs directly through FortiSASE to the IPsec tunnels of the hubs. This use case works well for seamless access for both TCP-based and UDP-based private applications hosted behind FortiGate.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET

Brave-dumps.com



SPA—SD-WAN Use Case

FortiSASE SD-WAN component for monitoring performance SLA

Routes are learned through IBGP

FortiSASE acts as spoke

Spoke-to-spoke traffic connects through on-demand tunnel (ADVPN)

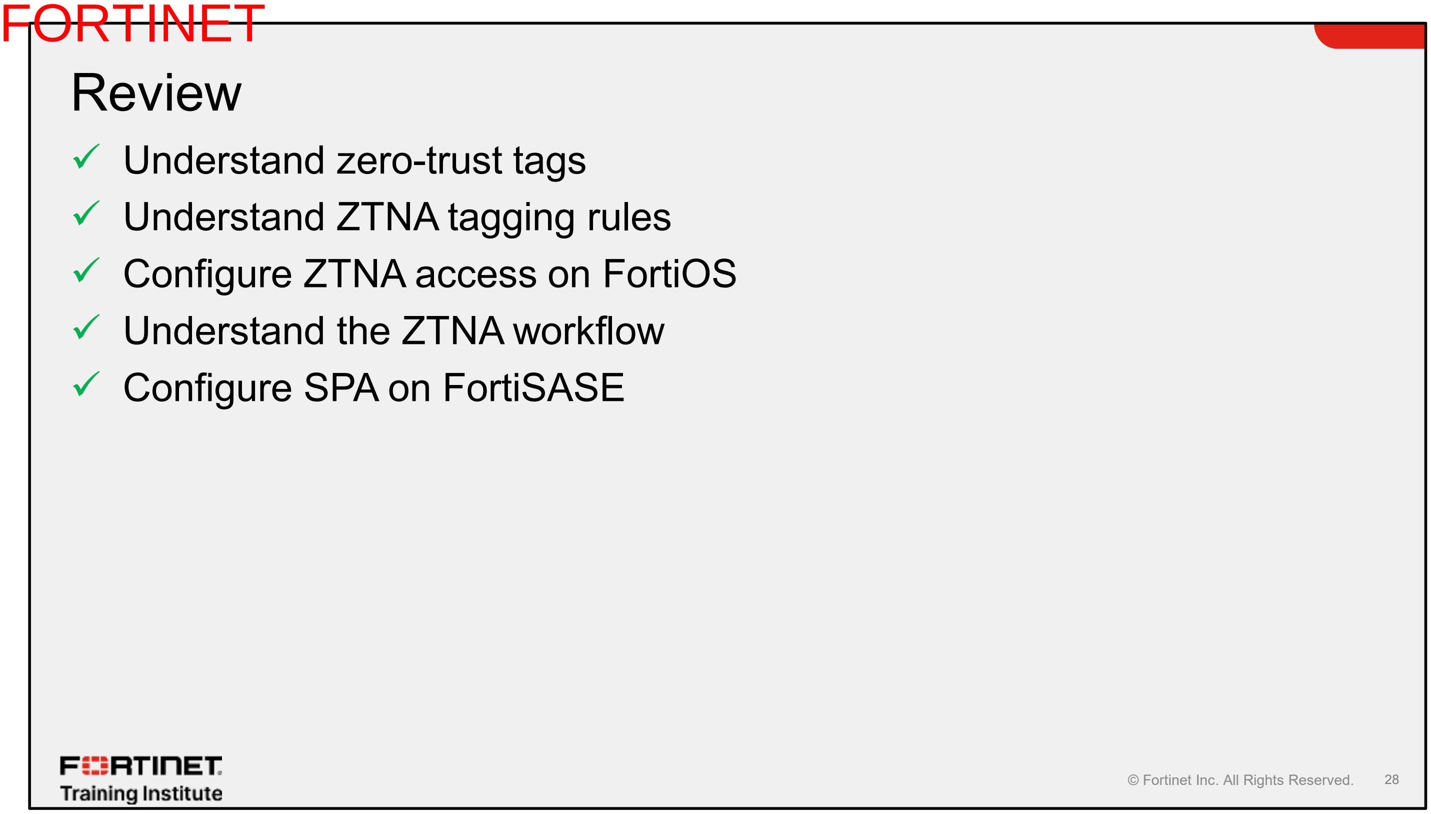
© Fortinet Inc. All Rights Reserved. 27

In the SPA SD-WAN use case, you add FortiSASE as a spoke to an existing FortiGate SD-WAN deployment. The FortiSASE security POPs and the FortiGate SD-WAN hubs form a traditional hub-and-spoke topology that supports the Fortinet ADVPN configuration. If a private resource is behind an organization's spoke device, it can connect directly to that resource through an on-demand tunnel. Like the SPA NGFW use case, the SPA SD-WAN use case also works well for seamless access to TCP-based and UDP-based privately hosted applications.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET

Brave-dumps.com



Review

- ✓ Understand zero-trust tags
- ✓ Understand ZTNA tagging rules
- ✓ Configure ZTNA access on FortiOS
- ✓ Understand the ZTNA workflow
- ✓ Configure SPA on FortiSASE

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 28

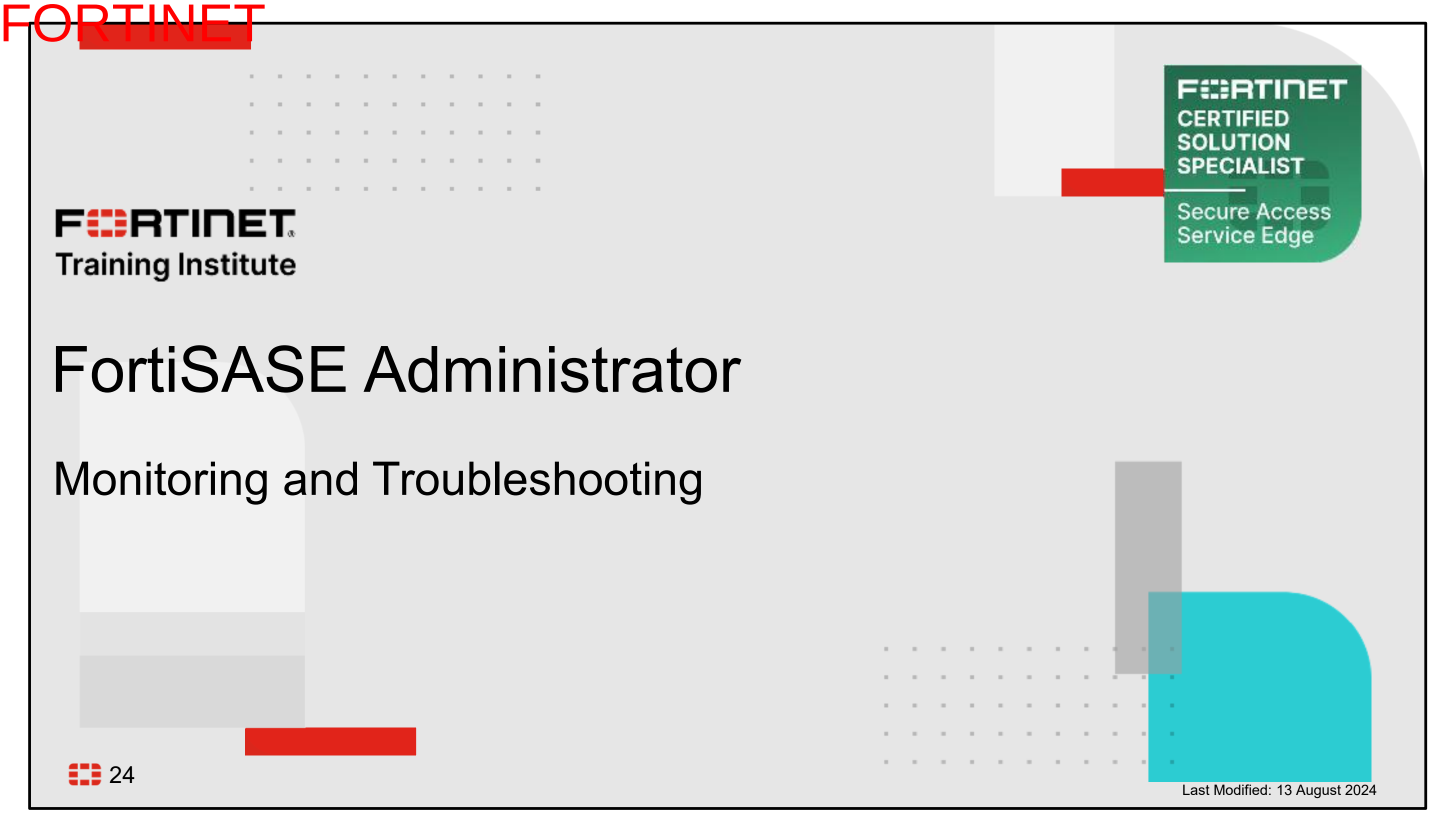
This slide shows the objectives that you covered in this lesson.

By mastering the objectives covered in this lesson, you learned how to configure and implement ZTNA in your environment, and how to configure SPA on FortiSASE and implement it in your SD-WAN environment.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET

Brave-dumps.com



FORTINET
Training Institute

FortiSASE Administrator

Monitoring and Troubleshooting

24

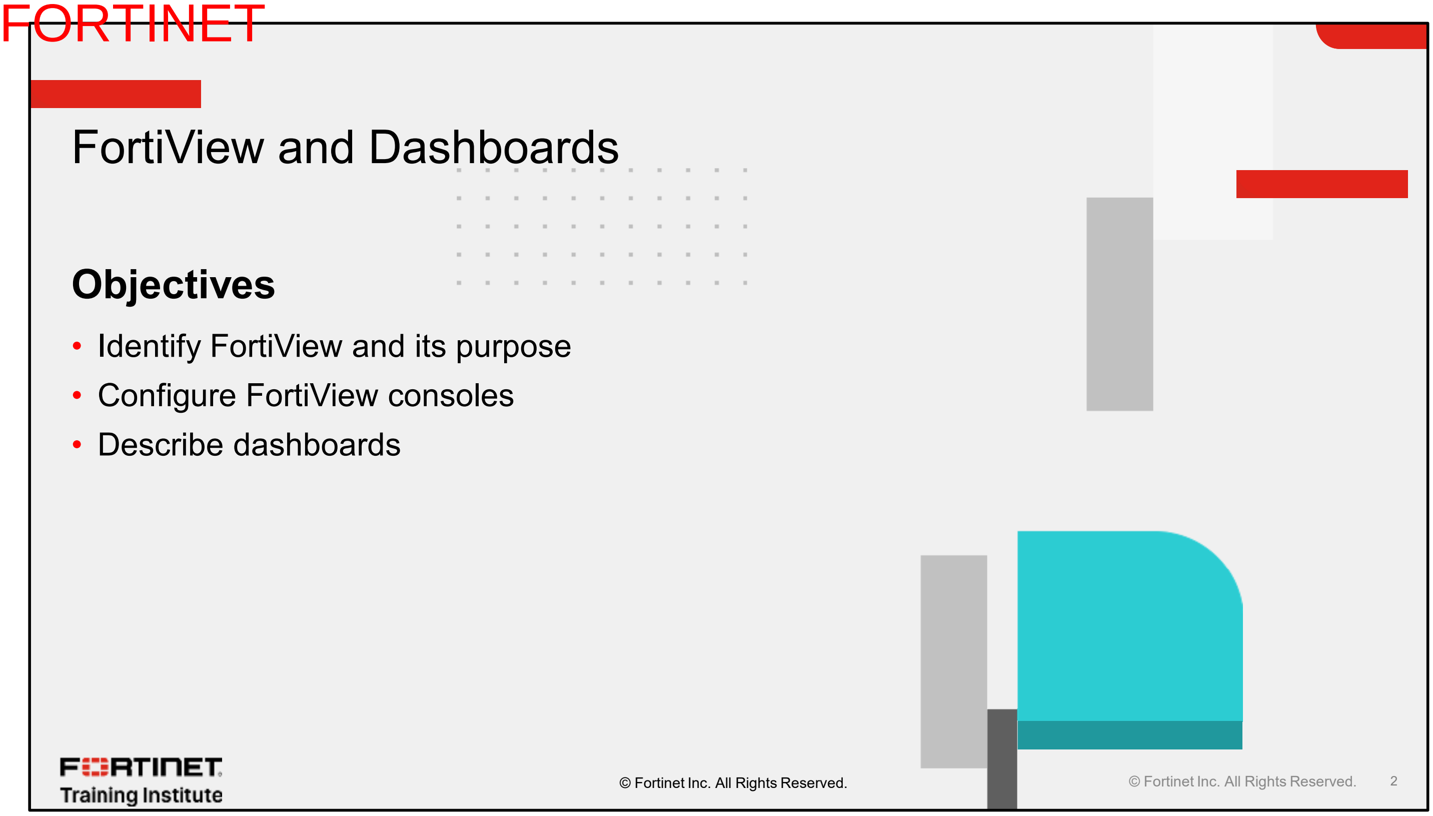
Last Modified: 13 August 2024

In this lesson, you will learn about monitoring and basic troubleshooting on FortiSASE.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET

Brave-dumps.com



FortiView and Dashboards

Objectives

- Identify FortiView and its purpose
- Configure FortiView consoles
- Describe dashboards

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved.

After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in FortiView and dashboards, you will be able to effectively monitor and look up FortiSASE status and security events.

Vouchers & Dumps are Available | WhatsApp +201224560923

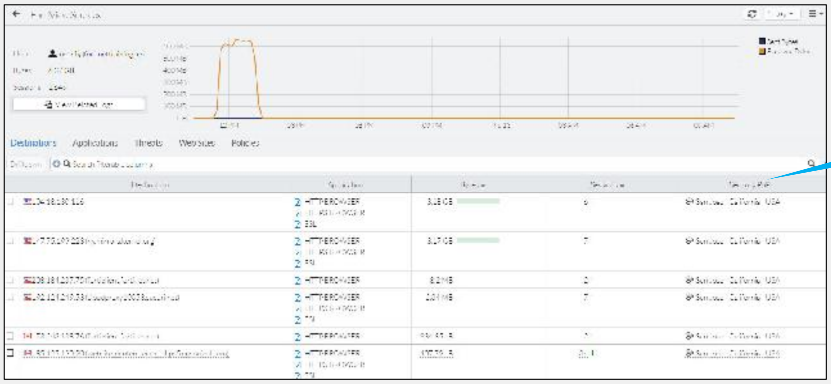
DO NOT REPRINT
© FORTINET

Brave-dumps.com

What Is FortiView?

- Provides alternative ways of viewing various real-time and historical events
- Presents graphical or textual information about security events through aggregation and correlation of logs against a specified sorting criteria and time frame
- Allows easier tracking of activity than is possible through logs alone

Dashboards > MONITOR > FortiView Sources



In FortiView, data is aggregated for easy review

© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved.

What is FortiView?

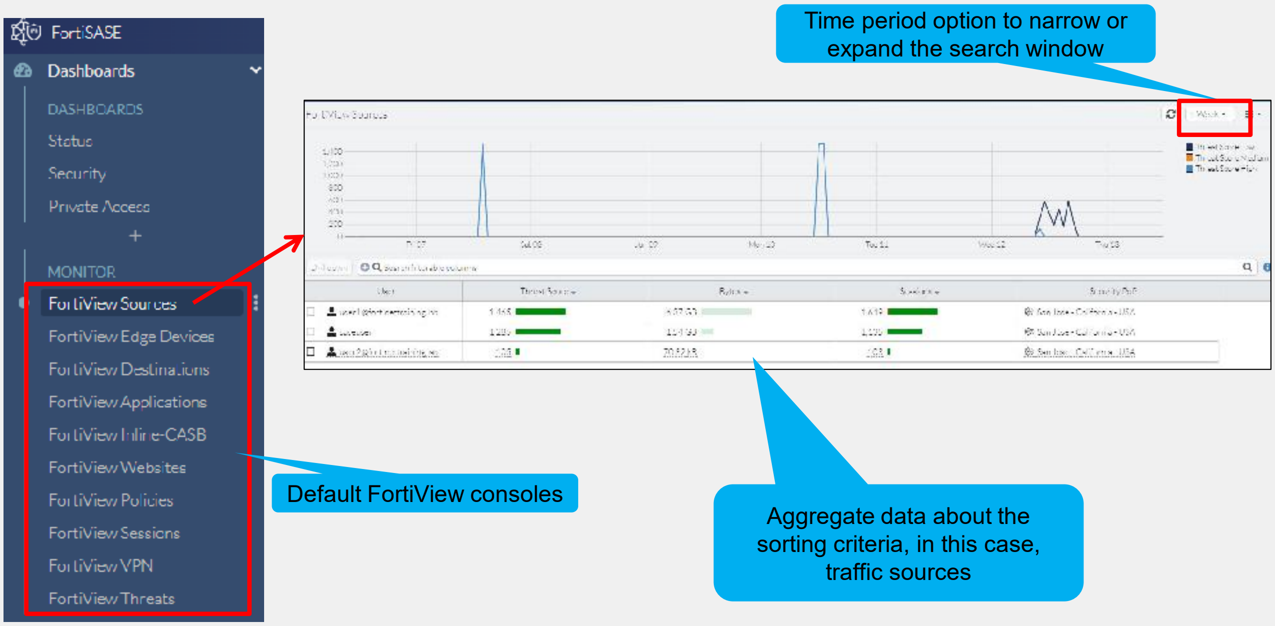
FortiView is another method of inspecting current and previous events in more aggregate views. Simply put, FortiView provides a consolidated series of consoles for administrators to analyze security events, over a period of time, based on a number of different sorting criteria. Information can be presented in various graphical or text-based consoles to simplify the process of locating the data you're searching for. FortiView uses the logs that are available within the GUI, but presents metadata about them, rather than presenting each log individually. This can make searching easier, in some circumstances, compared to log viewing.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET

Brave-dumps.com

FortiView Consoles



Time period option to narrow or expand the search window

Default FortiView consoles

Aggregate data about the sorting criteria, in this case, traffic sources

© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved.

Multiple consoles are available by default.

You can narrow or expand the events to the past hour, day, or week.

In the example shown on this slide, the **FortiView Sources** shows all of the sources that have generated traffic through FortiSASE in the past week. For each entry, a threat score, the total number of bytes uploaded and downloaded, the total number of sessions, and a visual breakdown of blocked and allowed sessions are displayed. The security point of presence (POP) location that the user is connected to is also displayed.

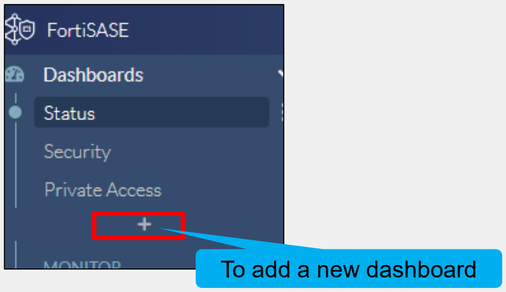
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET

Brave-dumps.com

Dashboards

- Customizable pages within the FortiSASE GUI
- Display a combination of system information, performance, and event widgets, as well as FortiView consoles
- Customizable layout, including widget size and positioning
- New dashboards become a new menu item under the **Dashboards** menu on the GUI
- Three predefined dashboards:
  - **Status**
  - **Security**
  - **Private Access**



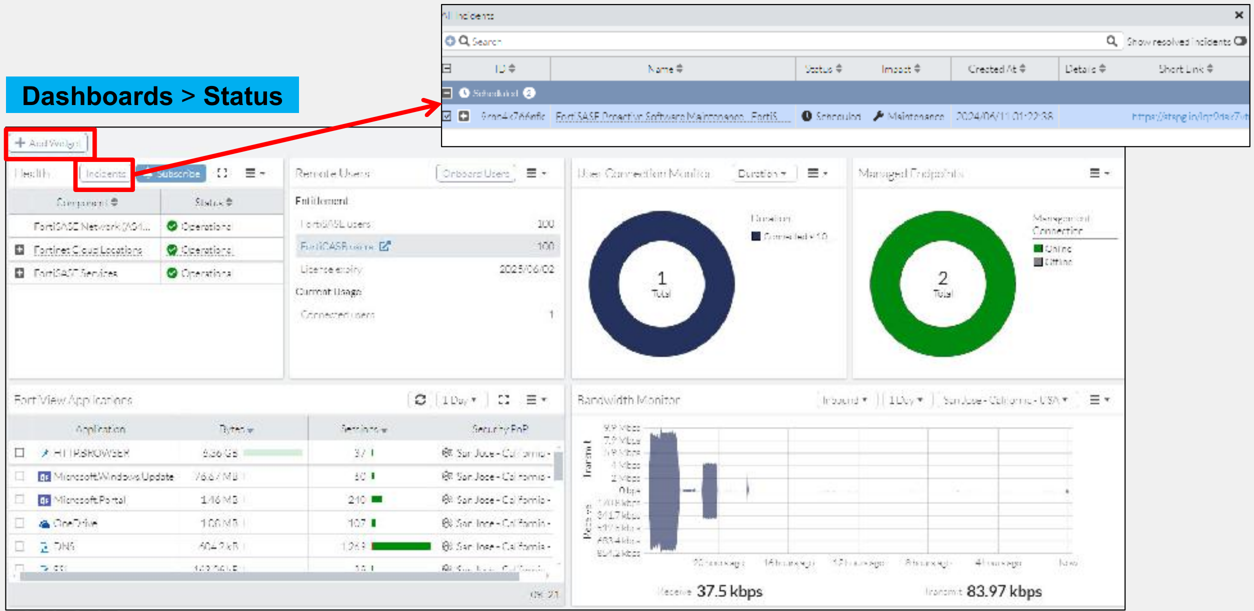
Dashboards are customizable pages within the FortiSASE GUI that display a combination of system information, performance, and event widgets. You can also place FortiView console widgets in your dashboards. You can create dashboards to monitor various system events, security profile inspection events, and so on. You can customize their size, position, and appearance attributes. After you create a new dashboard, it appears as a menu option under the **Dashboards** menu on the GUI.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET

Brave-dumps.com

Status



Dashboards > Status

© Fortinet Inc. All Rights Reserved.

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved. 6

The **Status** dashboard that you see when you first log in contains some of the most common FortiSASE widgets for monitoring the status of the device. As this slide shows, some of these widgets track the health status of FortiSASE components, license entitlement, managed endpoints, user connection monitor, and so on.

In addition to providing real-time details, you can also add FortiView consoles to dashboards as widgets. You can add widgets to any dashboard. Some widgets are interactive, allowing you to drill down into details. You can view any scheduled or ongoing FortiSASE maintenance.

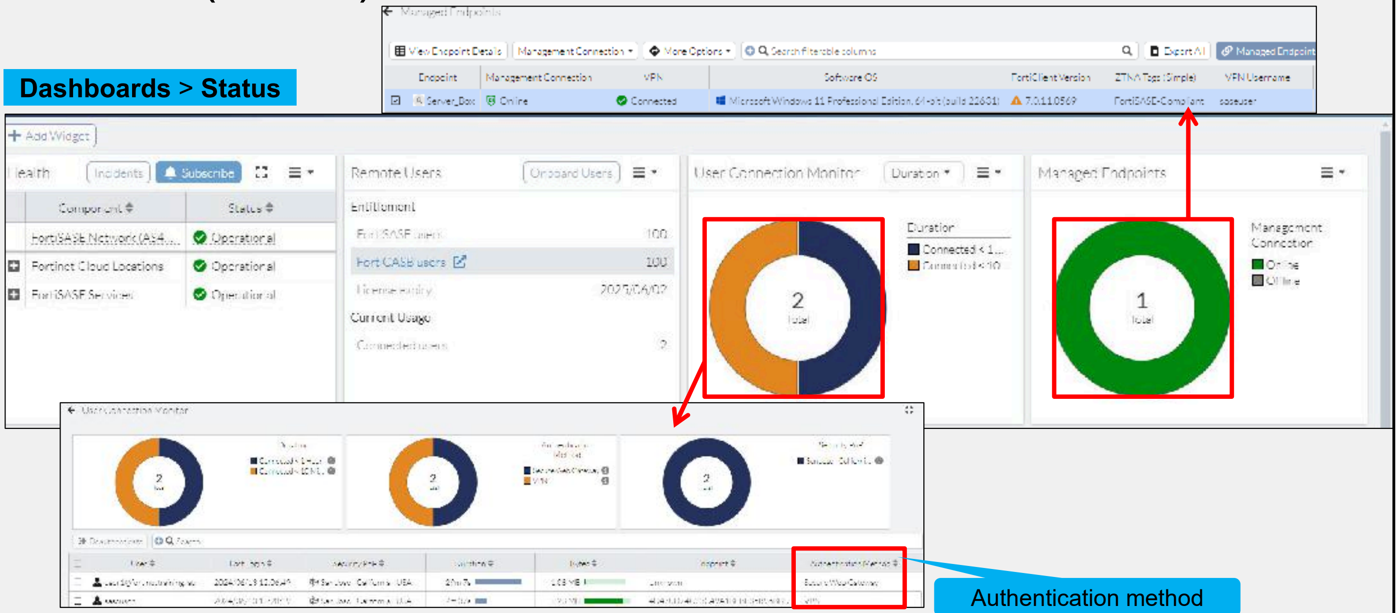
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET

Brave-dumps.com

Status (Contd)

Dashboards > Status



Managed Endpoints

	Endpoint	Management Connection	VPN	Software OS	FortiClient Version	ZTNA Tags (Simple)	VPN Username
☑	Server_Box	Online	✓ Connected	Microsoft Windows 11 Professional Edition, 64-bit (build 22631)	⚠ 7.0.11.0569	FortiSASE-Compliant	saseuser

Health

Component	Status
FortiSASE Network (AS4...	✓ Operational
Fortinet Cloud Locations	✓ Operational
FortiSASE Services	✓ Operational

Remote Users

Entitlement

FortiSASE users	100
FortiCASB users	100
License expiry	2025/04/02

Current Usage

Connected users	2

Authentication method

© Fortinet Inc. All Rights Reserved.

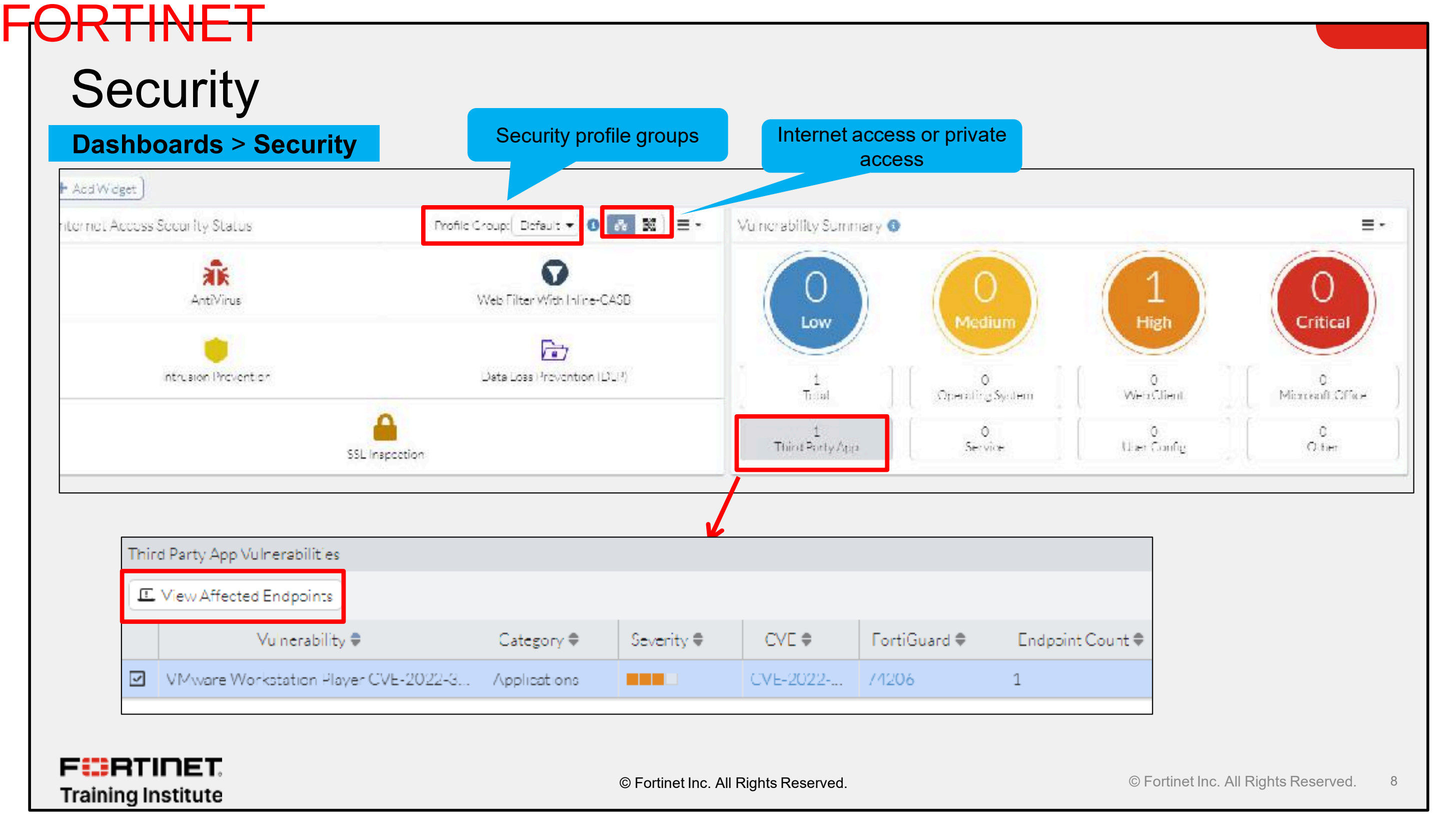
You can use the **User Connection Monitor** widget to view all the remote users connected to FortiSASE for secure internet access and their authentication method.

You can use the **Managed Endpoints** widget to view all FortiClient endpoints connected to FortiSASE. On the **Managed Endpoints** window, you can view endpoint details, such as OS, hardware, zero trust network access (ZTNA) tags, and so on. You can also enable or disable the management connection to FortiClient from FortiSASE.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET

Brave-dumps.com



Security

Dashboards > Security

	Vulnerability	Category	Severity	CVE	FortiGuard	Endpoint Count
☑	VMware Workstation Player CVE-2022-3...	Applications	■■■	CVE-2022-...	71206	1

© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved. 8

The security dashboard contains information about which security features are enabled in each security profile group and a vulnerability summary of all the FortiClient endpoints connected to FortiSASE. You can view details about vulnerabilities by clicking the category you want, such as **Third Party App**. You can click the desired vulnerability, and then click **View Affected Endpoints** to see which endpoint is vulnerable.

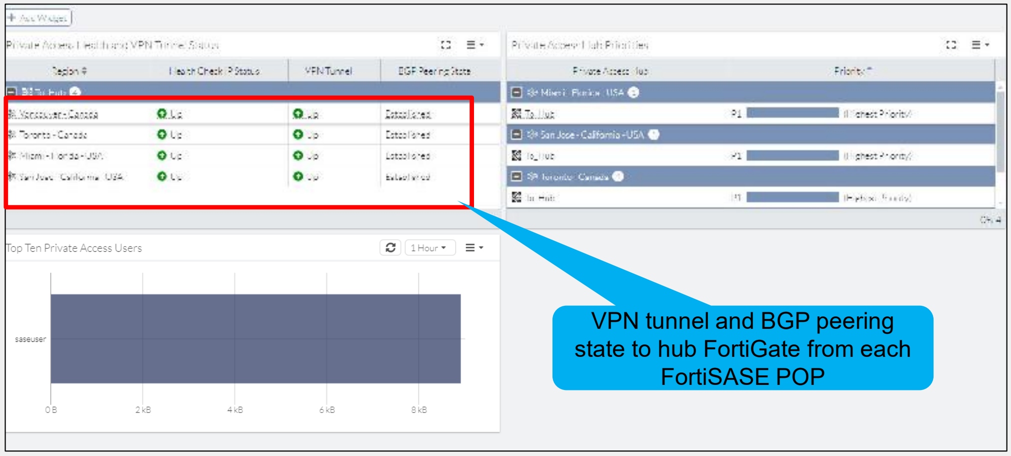
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET

Brave-dumps.com

Private Access

Dashboards > Private Access



Private Access Health and VPN Tunnel Status

Region	Health Check IP Status	VPN Tunnel	BGP Peering State
To_Hub 4			
Vancouver - Canada	Up	Up	Established
Toronto - Canada	Up	Up	Established
Miami - Florida - USA	Up	Up	Established
San Jose - California - USA	Up	Up	Established

Private Access Hub Priorities

Private Access Hub	Priority
Miami - Florida - USA 1	
To_Hub	P1 (Highest Priority)
San Jose - California - USA 1	
To_Hub	P1 (Highest Priority)
Toronto - Canada 1	
To_Hub	P1 (Highest Priority)

VPN tunnel and BGP peering state to hub FortiGate from each FortiSASE POP

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

The private access dashboard contains information about the health status of the VPN tunnel, from each FortiSASE POP to the FortiGate hub, and the top ten users that access the corporate resources hosted behind the FortiGate hub.

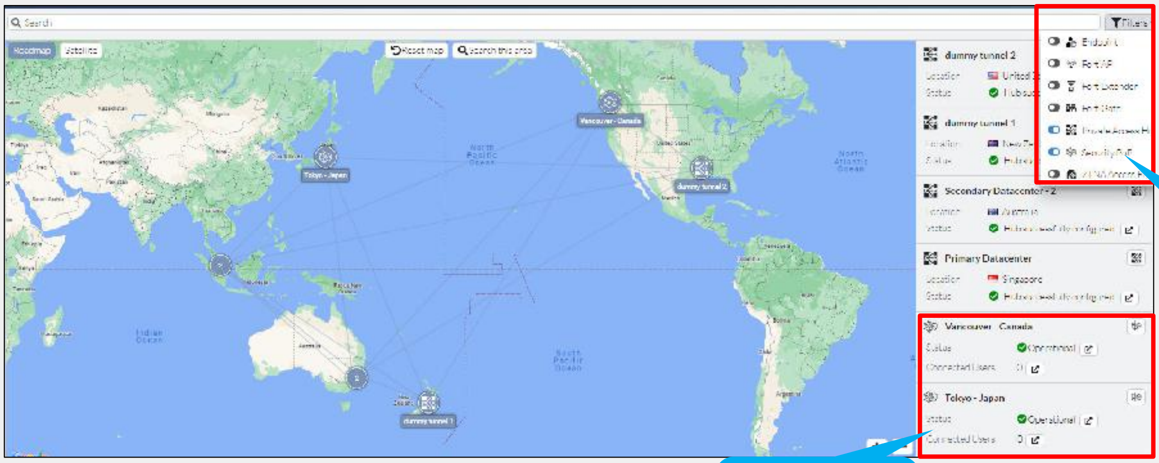
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET

Brave-dumps.com

Asset Map

Network > Asset Map



Toggle to filter out devices from showing on the asset map

Security POP locations

FURTINET Training Institute

© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved. 10

You can verify the private access hub, FortiAP, FortiGate, FortiExtender, security POP, and the endpoint status and location. You can filter out specific devices to prevent them from showing on the asset map.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET

Brave-dumps.com

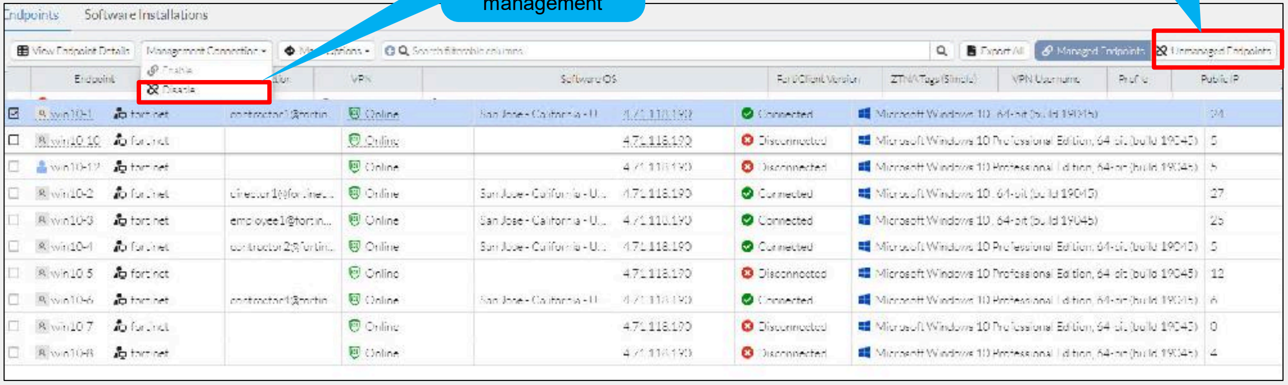
Endpoint Management

- Unmanaged endpoint
  - FortiClient can no longer connect to FortiSASE to be managed
  - FortiSASE removes the endpoint profile and ZTNA tags from the unmanaged endpoint
  - Frees up license seat

Network > Managed Endpoints

To exclude FortiClient from FortiSASE management

To see a list of unmanaged endpoints



☑	win10-1	fortinet	contractor1@fortin	Online	San Jose - California - U	4.71.118.190	Connected	Microsoft Windows 10, 64-bit (build 19045)	24
☐	win10-10	fortinet		Online		4.71.118.190	Disconnected	Microsoft Windows 10 Professional Edition, 64-bit (build 19045)	5
☐	win10-12	fortinet		Online		4.71.118.190	Disconnected	Microsoft Windows 10 Professional Edition, 64-bit (build 19045)	5
☐	win10-2	fortinet	director1@fortinet...	Online	San Jose - California - U...	4.71.118.190	Connected	Microsoft Windows 10, 64-bit (build 19045)	27
☐	win10-3	fortinet	employee1@fortin...	Online	San Jose - California - U...	4.71.110.190	Connected	Microsoft Windows 10, 64-bit (build 19045)	25
☐	win10-4	fortinet	contractor2@fortin...	Online	San Jose - California - U...	4.71.118.190	Connected	Microsoft Windows 10 Professional Edition, 64-bit (build 19045)	5
☐	win10-5	fortinet		Online		4.71.118.190	Disconnected	Microsoft Windows 10 Professional Edition, 64-bit (build 19045)	12
☐	win10-6	fortinet	contractor1@fortin	Online	San Jose - California - U	4.71.118.190	Connected	Microsoft Windows 10 Professional Edition, 64-bit (build 19045)	6
☐	win10-7	fortinet		Online		4.71.118.190	Disconnected	Microsoft Windows 10 Professional Edition, 64-bit (build 19045)	0
☐	win10-8	fortinet		Online		4.71.118.190	Disconnected	Microsoft Windows 10 Professional Edition, 64-bit (build 19045)	4

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved.

On the **Network** > **Managed Endpoints** page, you can see the list of managed and unmanaged endpoints. You can select an endpoint, click **Management Connection**, and then click **Disable** to exclude the endpoint from being managed by FortiSASE. After you disable FortiSASE management, FortiClient can no longer connect to the FortiSASE Zero Trust Telemetry connection, and the license seat is freed up. You can click **Unmanaged Endpoints** to see the list of endpoints that have been excluded from FortiSASE management. To allow an unmanaged endpoint to be managed by and register with FortiSASE, you must select the endpoint and then click **Management Connection** > **Enable**.

Vouchers & Dumps are Available | WhatsApp +201224560923

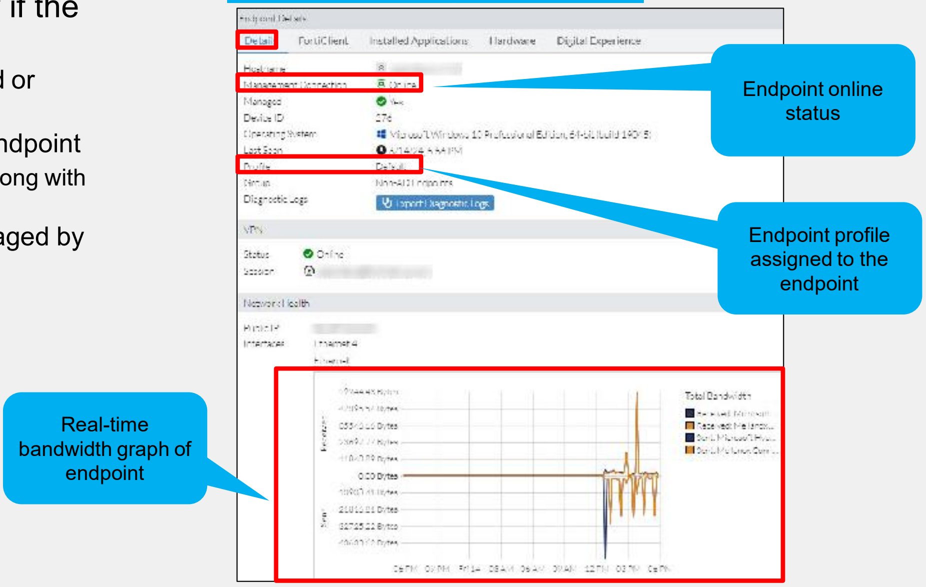
DO NOT REPRINT
© FORTINET

Brave-dumps.com

Endpoint Details—DEM

- DEM data is available only if the following criteria is met:
  - FortiSASE has an advanced or comprehensive license
  - DEM agent is installed on endpoint
    - DEM agent is packaged along with the FortiClient installer
  - Endpoint is online and managed by FortiSASE

Network > Managed Endpoints



Endpoint Details

Detail | FortiClient | Installed Applications | Hardware | Digital Experience

Hostname [redacted]
Management Connection Online
Managed Yes
Device ID 27d
Operating System Microsoft Windows 10 Professional Edition, 64-bit (build 19045)
Last Seen 6/14/24 4:44 PM
Profile Default
Group Non-AD Endpoints
Diagnostic Logs Export Diagnostic Logs

VPN

Status Online
Session [redacted]

Network Health

Public IP [redacted]
Interfaces Ethernet 4
Ethernet

Endpoint online status

Endpoint profile assigned to the endpoint

Real-time bandwidth graph of endpoint

© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved.

You can select an endpoint and then view related details, such as hardware specifics, installed applications, digital experience, and so on. You can see digital experience monitoring (DEM) data if the FortiSASE instance has an advanced or comprehensive license.

You can view information related to all the endpoint’s detected network interfaces and their IP addresses. A real-time graph is also available that shows the total bandwidth used by the endpoint.

Vouchers & Dumps are Available | WhatsApp +201224560923

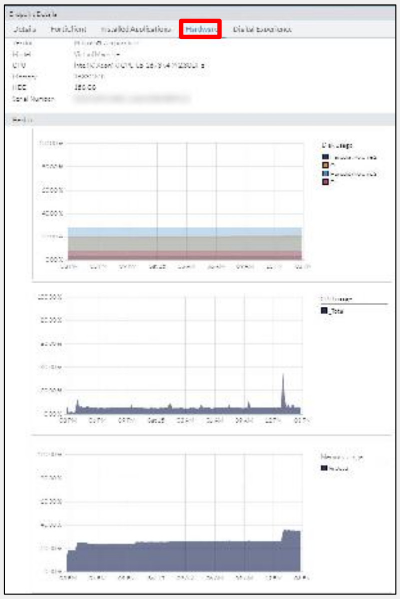
DO NOT REPRINT
© FORTINET

Brave-dumps.com

Endpoint Details—DEM (Contd)

- Real-time data available on the endpoint's resource usage

Network > Managed Endpoints



FURTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved.

You can view endpoint hardware details, such as vendor, model, and CPU. You can also view a real-time graph that shows the endpoint's hard disk, CPU, and memory usage.

Vouchers & Dumps are Available | WhatsApp +201224560923

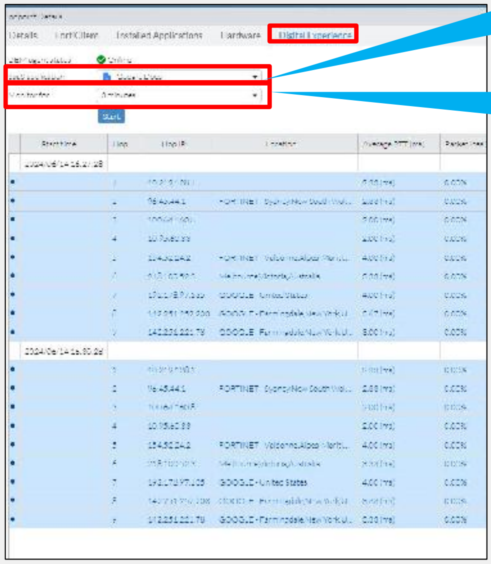
DO NOT REPRINT
© FORTINET

Brave-dumps.com

Endpoint Details—DEM (Contd)

- A trace job provides network visibility from the endpoint to a specific SaaS application

Network > Managed Endpoints



Select the SaaS application to run the trace job against

Duration of the trace job

© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved.

You can run a trace job on the selected endpoint to get end-to-end network visibility from the endpoint to a specific Software-as-a-Service (SaaS) application. The trace output gives information on average round-trip time (RTT) in milliseconds and the percentage of packet loss along each network hop while accessing the SaaS application. The trace can be run while the endpoint is connected to the FortiSASE SSL VPN for secure internet access or when it is disconnected from the FortiSASE SSL VPN and uses its local internet. This helps analyze if the delay is caused by the security POP or some other network hop in the path to reach the SaaS application.

Vouchers & Dumps are Available | WhatsApp +201224560923

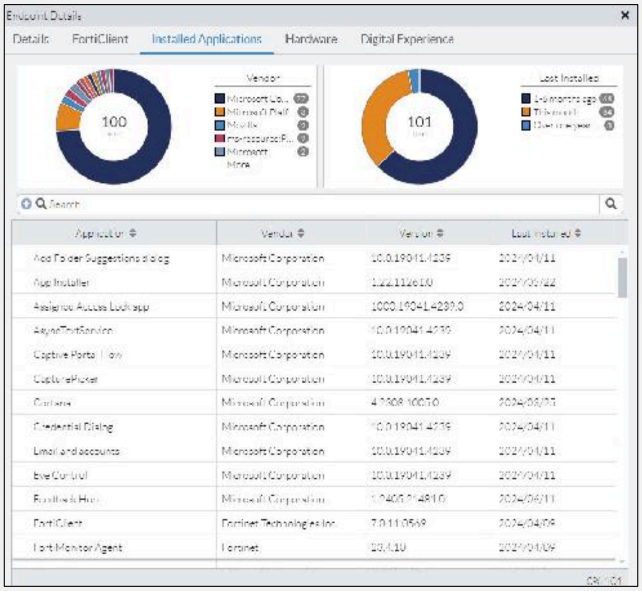
DO NOT REPRINT
© FORTINET

Brave-dumps.com

Applications

- Shows information about installed applications for the selected managed endpoint
- The list includes details for each application, such as vendor and version information

Network > Managed Endpoints



Application	Vendor	Version	Last Installed
Add Folder Suggestions dialog	Microsoft Corporation	10.0.19041.4239	2024/04/11
App Installer	Microsoft Corporation	1.22.11261.0	2024/05/22
Assigned Access Lock app	Microsoft Corporation	1000.19041.4239.0	2024/04/11
AsyncTextService	Microsoft Corporation	10.0.19041.4239	2024/04/11
Captive Portal Flow	Microsoft Corporation	10.0.19041.4239	2024/04/11
CapturePicker	Microsoft Corporation	10.0.19041.4239	2024/04/11
Cortana	Microsoft Corporation	4.2308.10070	2024/05/23
Credential Dialog	Microsoft Corporation	10.0.19041.4239	2024/04/11
Email and accounts	Microsoft Corporation	10.0.19041.4239	2024/04/11
Eye Control	Microsoft Corporation	10.0.19041.4239	2024/04/11
Feedback Hub	Microsoft Corporation	1.2405.21481.0	2024/06/11
FortiClient	Fortinet Technologies Inc.	7.0.11.0569	2024/04/09
FortiMonitor Agent	Fortinet	20.4.10	2024/04/09

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved.

The FortiSASE administrator can view installed applications information for managed endpoints, by host.

You can see the total number of applications installed, vendors, versions, and the installation date. You can view the application names alphabetically or by vendor. You can also apply filters by application name, vendor name, and version number.

Vouchers & Dumps are Available | WhatsApp +201224560923

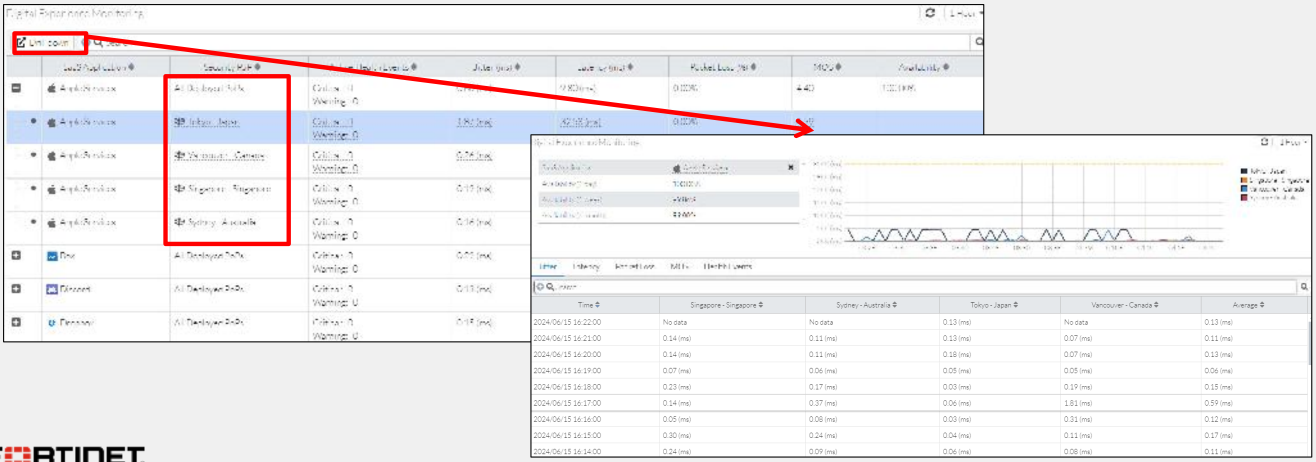
DO NOT REPRINT
© FORTINET

Brave-dumps.com

DEM

- End-to-end network visibility from all the FortiSASE security PoPs to a specific SaaS application
- Jitter, latency, packet loss, and mean opinion score (MOS) are measured

Network > Digital Experience Monitoring



Time	Singapore - Singapore	Sydney - Australia	Tokyo - Japan	Vancouver - Canada	Average
2024/06/15 16:22:00	No data	No data	0.13 (ms)	No data	0.13 (ms)
2024/06/15 16:21:00	0.14 (ms)	0.11 (ms)	0.13 (ms)	0.07 (ms)	0.11 (ms)
2024/06/15 16:20:00	0.14 (ms)	0.11 (ms)	0.18 (ms)	0.07 (ms)	0.13 (ms)
2024/06/15 16:19:00	0.07 (ms)	0.06 (ms)	0.05 (ms)	0.05 (ms)	0.06 (ms)
2024/06/15 16:18:00	0.23 (ms)	0.17 (ms)	0.03 (ms)	0.19 (ms)	0.15 (ms)
2024/06/15 16:17:00	0.14 (ms)	0.37 (ms)	0.06 (ms)	1.81 (ms)	0.59 (ms)
2024/06/15 16:16:00	0.05 (ms)	0.08 (ms)	0.03 (ms)	0.31 (ms)	0.12 (ms)
2024/06/15 16:15:00	0.30 (ms)	0.24 (ms)	0.04 (ms)	0.11 (ms)	0.17 (ms)
2024/06/15 16:14:00	0.24 (ms)	0.09 (ms)	0.06 (ms)	0.08 (ms)	0.11 (ms)

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

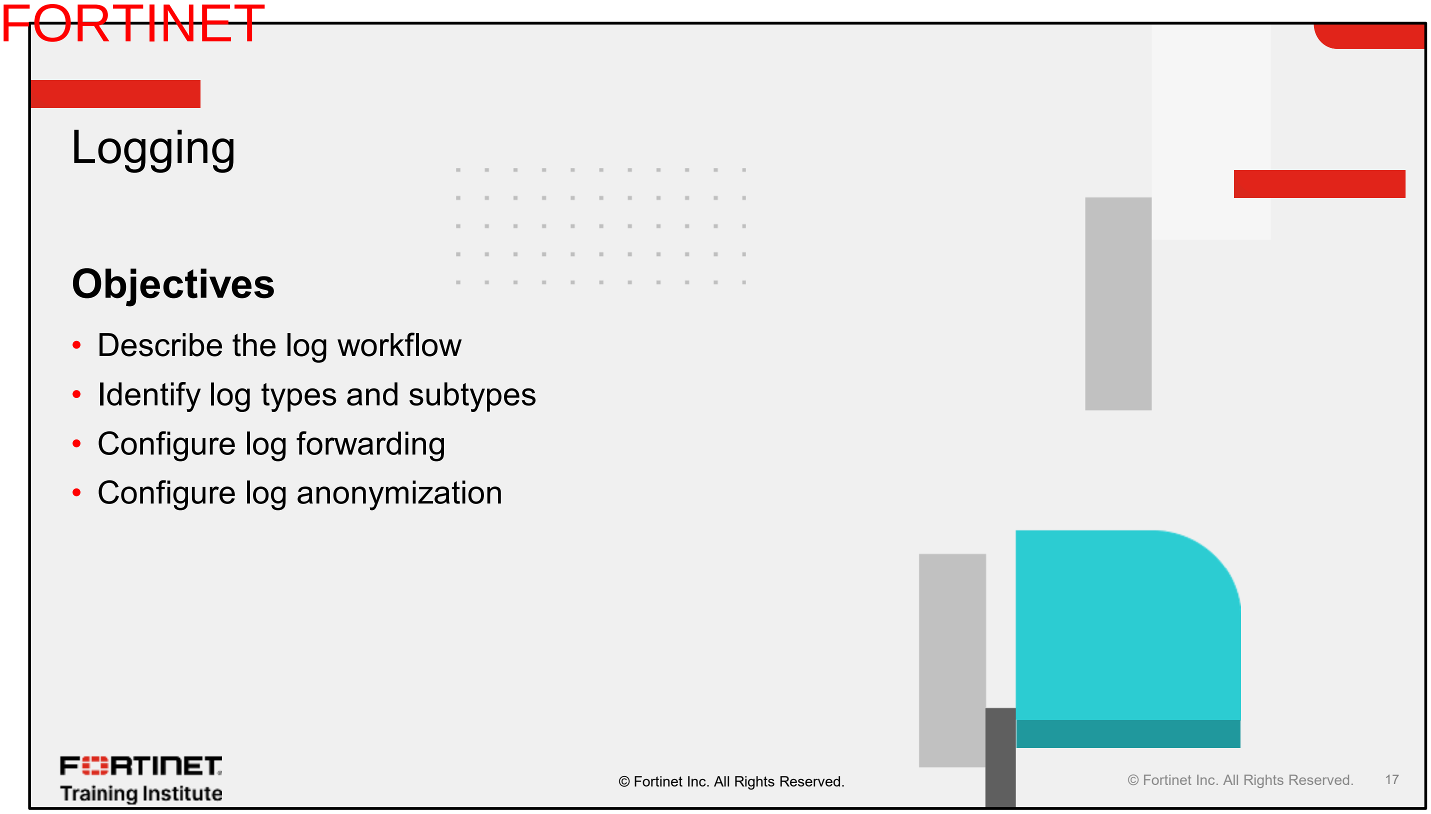
© Fortinet Inc. All Rights Reserved. 16

You can monitor the end-to-end network performance from the FortiSASE security POP to a SaaS application. You can see a list of common SaaS application and health check metrics for first-mile connectivity between your FortiSASE security POPs and these SaaS applications. You can view more details regarding any selected SaaS application. A FortiSASE administrator can use this information to determine if remote user traffic is passing through a POP with ideal connectivity or with some ongoing connectivity issues.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET

Brave-dumps.com



Logging

Objectives

- Describe the log workflow
- Identify log types and subtypes
- Configure log forwarding
- Configure log anonymization

© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved.

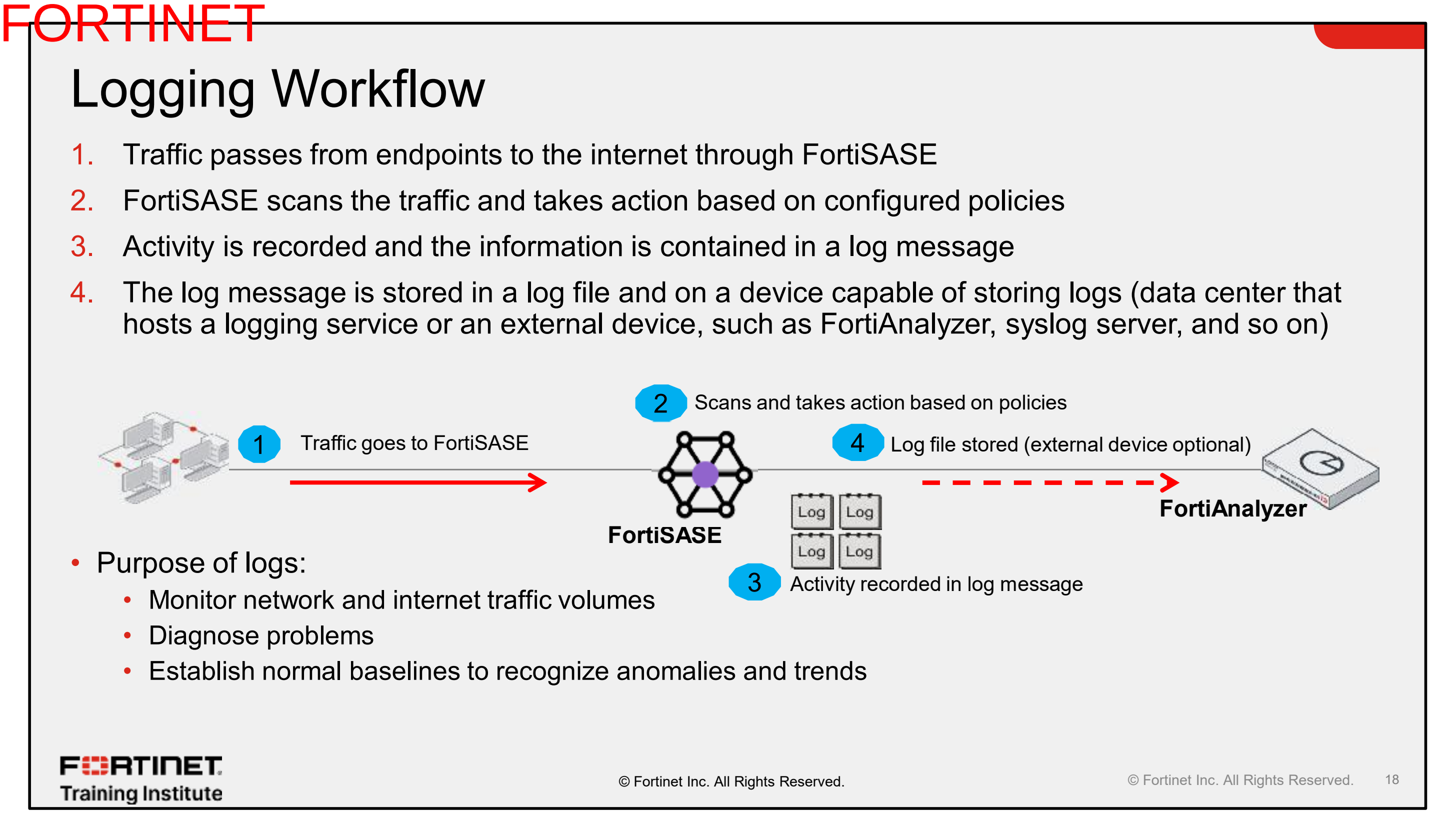
After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in logging, you will be able to more effectively analyze log data on FortiSASE.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET

Brave-dumps.com



Logging Workflow

1. Traffic passes from endpoints to the internet through FortiSASE
2. FortiSASE scans the traffic and takes action based on configured policies
3. Activity is recorded and the information is contained in a log message
4. The log message is stored in a log file and on a device capable of storing logs (data center that hosts a logging service or an external device, such as FortiAnalyzer, syslog server, and so on)

1 Traffic goes to FortiSASE

2 Scans and takes action based on policies

FortiSASE

3 Activity recorded in log message

4 Log file stored (external device optional)

FortiAnalyzer

- Purpose of logs:
  - Monitor network and internet traffic volumes
  - Diagnose problems
  - Establish normal baselines to recognize anomalies and trends

FORTINET Training Institute
© Fortinet Inc. All Rights Reserved.
© Fortinet Inc. All Rights Reserved. 18

When traffic passes from endpoints to the internet through FortiSASE, FortiSASE scans the traffic and then takes action based on the policies in place. This activity is recorded, and the information is contained in a log message. The log message is stored in a log file. The log file is then stored on a logging service that is configured when FortiSASE is deployed. FortiSASE can also send logs to an external storage device, such as FortiAnalyzer, a syslog server, and so on.

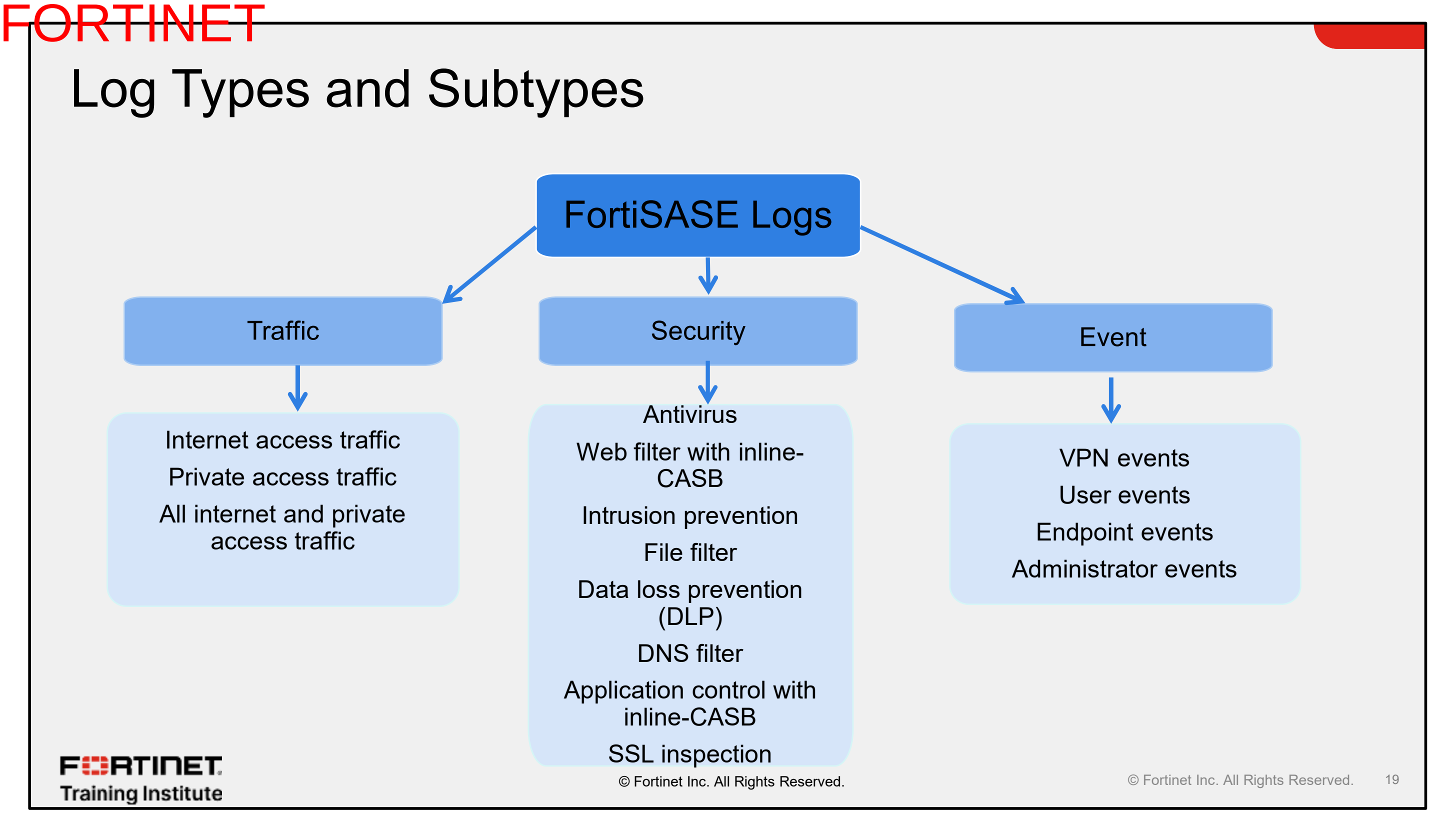
The purpose of logs is to help you monitor your network traffic, locate problems, establish baselines, and more. Logs provide you with a greater perspective of your network, allowing you to adjust your network security settings if necessary.

Some organizations have legal requirements when it comes to logging. When you configure logging, it is important to be aware of your organization's policies.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET

Brave-dumps.com



Log Types and Subtypes

FortiSASE Logs
Traffic
Security
Event
Internet access traffic
Private access traffic
All internet and private access traffic
Antivirus
Web filter with inline-CASB
Intrusion prevention
File filter
Data loss prevention (DLP)
DNS filter
Application control with inline-CASB
SSL inspection
VPN events
User events
Endpoint events
Administrator events
FORTINET Training Institute
© Fortinet Inc. All Rights Reserved.
© Fortinet Inc. All Rights Reserved. 19

There are three different types of logs on FortiSASE: traffic logs, security logs, and event logs. Each type is further divided into subtypes.

Traffic logs record traffic flow information, such as an HTTP/HTTPS request and its response, if any. It contains subtypes named internet access traffic, private access traffic, and all internet and private access traffic.

- Internet access traffic logs contain information about traffic from the endpoints to the internet.
- Private access traffic logs contain information about traffic from the endpoints to the FortiGate private access hubs.
- Internet and private access traffic logs contain information about both the internet traffic and private access hubs from the endpoints.

Security logs record security events, such as virus detection and intrusion attempts. They contain log entries based on the security profile type, including the subtype listed on the slide.

Finally, event logs record events, such as administrator activities, user login information, and VPN negotiations.

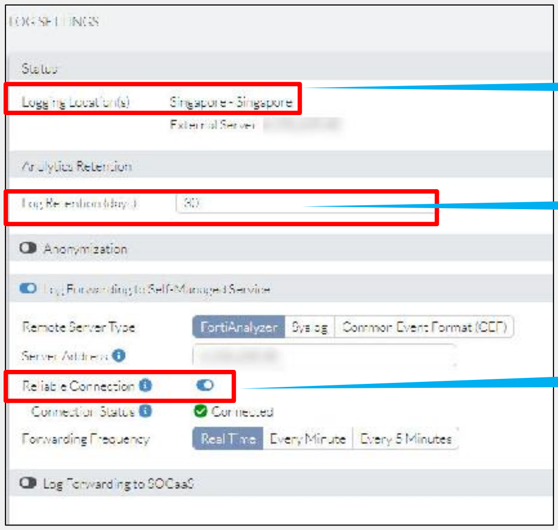
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET

Brave-dumps.com

Log Forwarding

Analytics > LOGS > Settings



LOG SETTINGS

Status

Logging Location(s) Singapore - Singapore

External Server [redacted]

Analytics Retention

Log Retention (days) 30

Anonymization

Log Forwarding to Self-Managed Service

Remote Server Type: FortiAnalyzer | Syslog | Common Event Format (CEF)

Server Address [redacted]

Reliable Connection

Connection Status: Connected

Forwarding Frequency: Real Time | Every Minute | Every 5 Minutes

Log Forwarding to SOCaaS

Data center location where logging is hosted

Maximum log retention is 30 days

Use TCP connection for log forwarding

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved. 20

You can enable log forwarding to an external server. The remote servers supported for log forwarding on FortiSASE are FortiAnalyzer, syslog, or a common event format (CEF) server. You can enable the **Reliable Connection** option to use TCP instead of UDP for log forwarding.

All FortiSASE instances have log retention enabled for a period of 30 days by default. You can configure the log retention policy to be from 2-30 days. The policy applies to traffic, security, and event logs. FortiSASE automatically deletes logs that are older than the specified log retention.

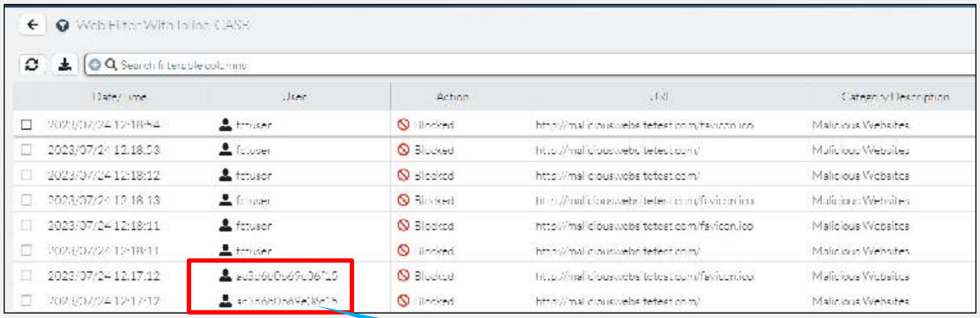
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET

Brave-dumps.com

Log Anonymization

Analytics > LOGS > Security



Web Filter With Inline CASB

Search filterable columns

	Date/Time	User	Action	URL	Category Description
□	2023/07/24 12:18:54	fctuser	Blocked	http://maliciouswebsitetest.com/favicon.ico	Malicious Websites
□	2023/07/24 12:18:53	fctuser	Blocked	http://maliciouswebsitetest.com/	Malicious Websites
□	2023/07/24 12:18:12	fctuser	Blocked	http://maliciouswebsitetest.com/	Malicious Websites
□	2023/07/24 12:18:13	fctuser	Blocked	http://maliciouswebsitetest.com/favicon.ico	Malicious Websites
□	2023/07/24 12:18:11	fctuser	Blocked	http://maliciouswebsitetest.com/favicon.ico	Malicious Websites
□	2023/07/24 12:18:11	fctuser	Blocked	http://maliciouswebsitetest.com/	Malicious Websites
□	2023/07/24 12:17:12	ac3a6b0a69c06f15	Blocked	http://maliciouswebsitetest.com/favicon.ico	Malicious Websites
□	2023/07/24 12:17:12	ac3a6b0a69e06f15	Blocked	http://maliciouswebsitetest.com/	Malicious Websites

Anonymization enabled

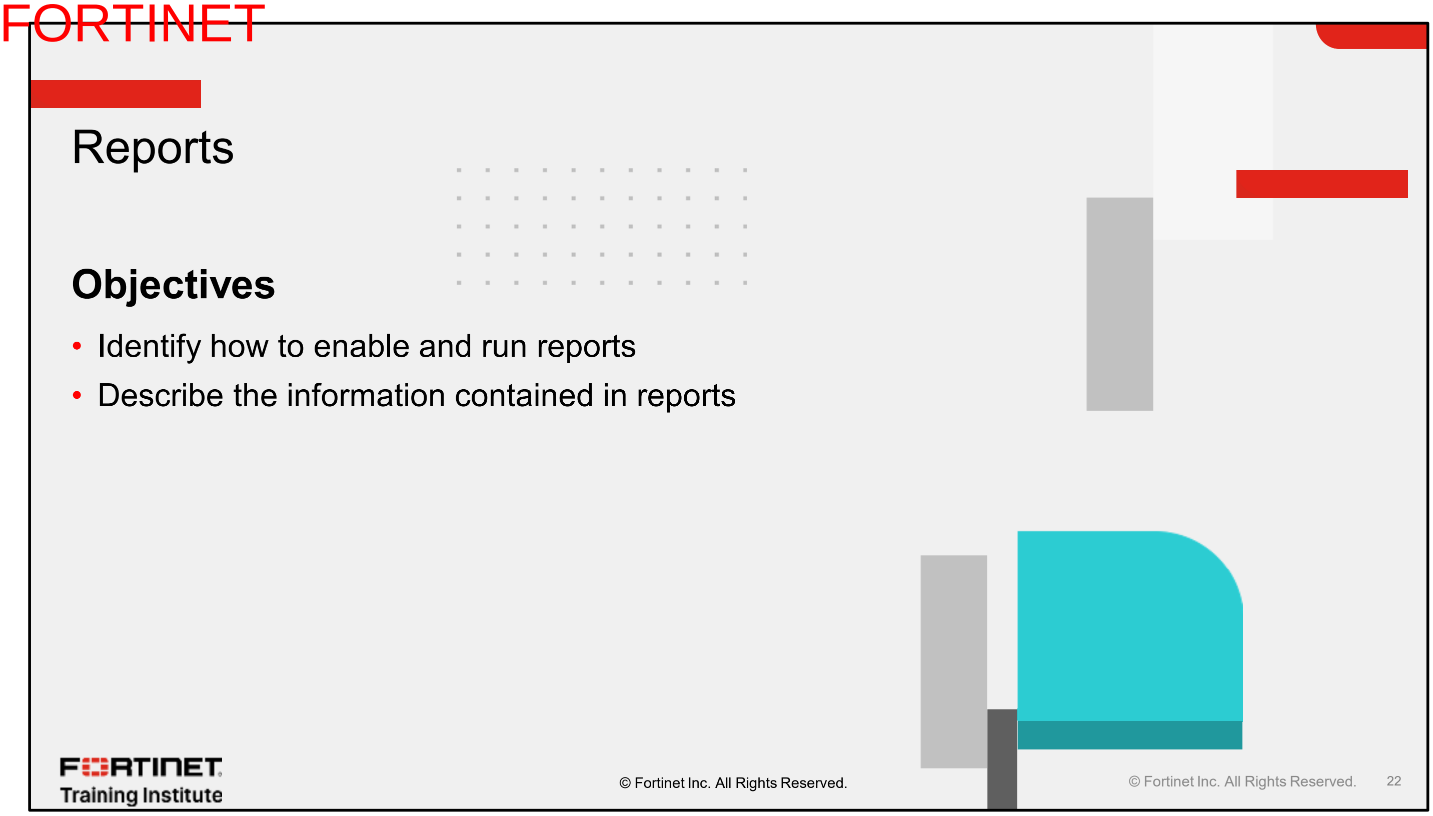
© Fortinet Inc. All Rights Reserved.

Log anonymization allows you to hide personally identifiable user information, such as host name and avatar, in dashboard widgets, logs, and other areas of FortiSASE. The source information is anonymized if anonymization was enabled when the traffic occurred. FortiSASE uses salt encryption to hash the value you entered while enabling anonymization. The hashed value will be shown on dashboard widgets, logs, and other areas of FortiSASE.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET

Brave-dumps.com



Reports

Objectives

- Identify how to enable and run reports
- Describe the information contained in reports

Training Institute

© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved. 22

After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating a competent understanding of reports, you will be able to configure and generate reports on FortiSASE.

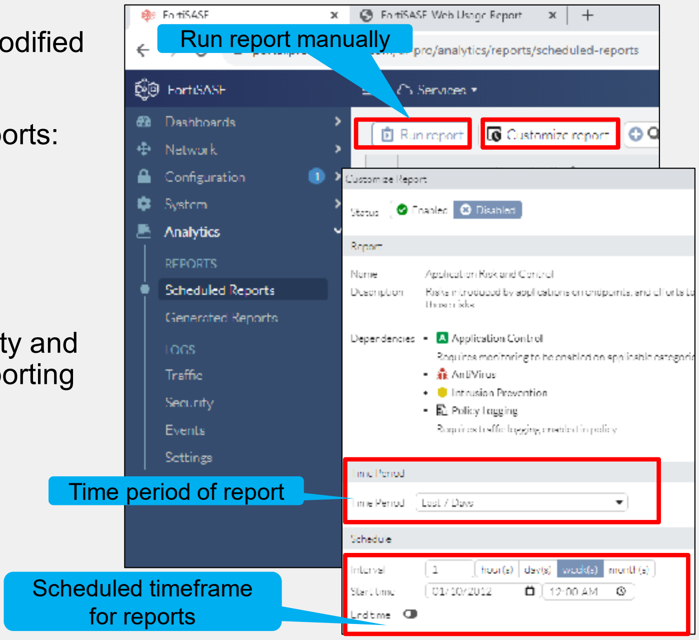
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET

Brave-dumps.com

FortiSASE Reports

- A fixed template report that cannot be modified
- Can run manually or on a schedule
- There are four options for scheduled reports:
  - Hourly
  - Daily
  - Weekly
  - Monthly
- Provides a high-level summary of security and VPN events that occurred during the reporting period



Customize Report

Status: Enabled [✓ Disabled]

Report

Name: Application Risk and Control

Description: Risks introduced by applications on endpoints, and efforts to... these risks

Dependencies:
- Application Control
  Requires monitoring to be enabled on applicable categories
- AntiVirus
- Intrusion Prevention
- Policy logging
  Requires traffic logging enabled in policy

Time Period

Time Period: Last 7 Days

Schedule

Interval: 1 hour(s) day(s) [✓ week(s)] month(s)

Start time: 01/10/2012 12:00 AM

End time: ○

Run report manually

Time period of report

Scheduled timeframe for reports

FERTINET Training Institute

© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved.

FortiSASE can generate a report based on stored logs. You cannot customize this report. It is a fixed report that contains details about security and VPN events that occurred during the reporting period. You can run reports manually or you can configure them to run on a schedule. If you run reports on a schedule, you can set them to run hourly, daily, weekly, or monthly. Reports are stored on FortiSASE and you can view, delete, or download them directly from the GUI.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET

Brave-dumps.com

FortiSASE Report Content

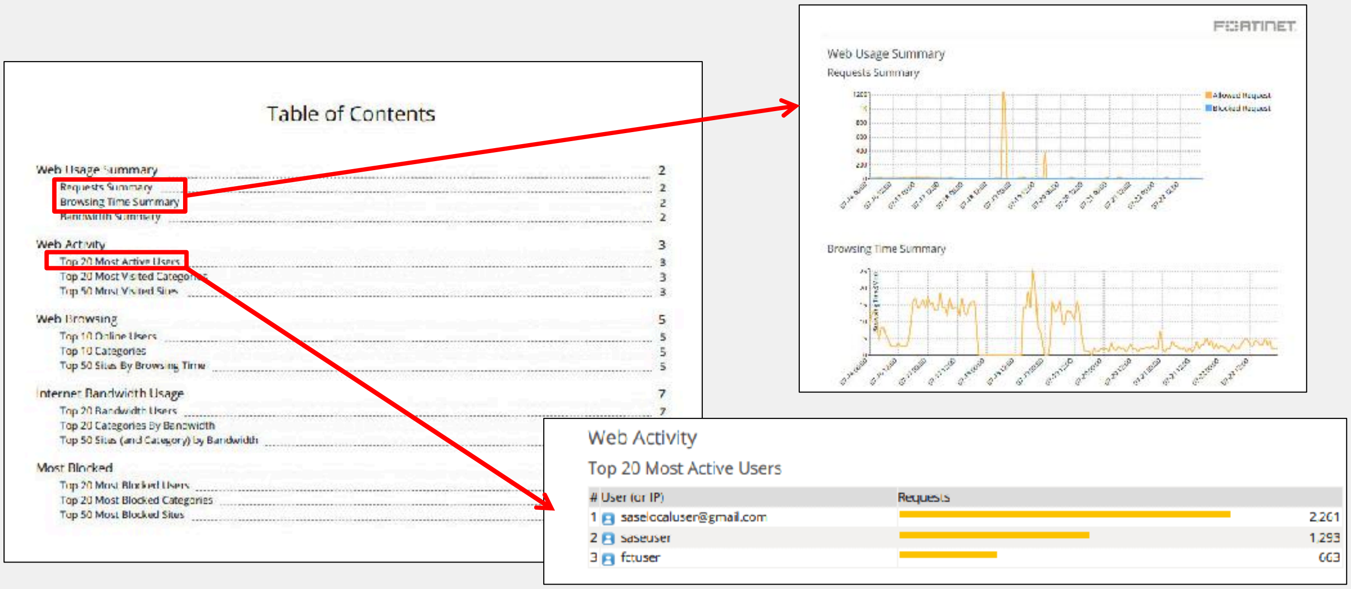


Table of Contents

Web Usage Summary 2
- Requests Summary 2
- Browsing Time Summary 2
- Bandwidth Summary 2

Web Activity 3
- Top 20 Most Active Users 3
- Top 20 Most Visited Categories 3
- Top 50 Most Visited Sites 3

Web Browsing 5
- Top 10 Online Users 5
- Top 10 Categories 5
- Top 50 Sites By Browsing Time 5

Internet Bandwidth Usage 7
- Top 20 Bandwidth Users 7
- Top 20 Categories By Bandwidth
- Top 50 Sites (and Category) by Bandwidth

Most Blocked
- Top 20 Most Blocked Users
- Top 20 Most Blocked Categories
- Top 50 Most Blocked Sites

Web Usage Summary

Requests Summary

Browsing Time Summary

Web Activity

Top 20 Most Active Users

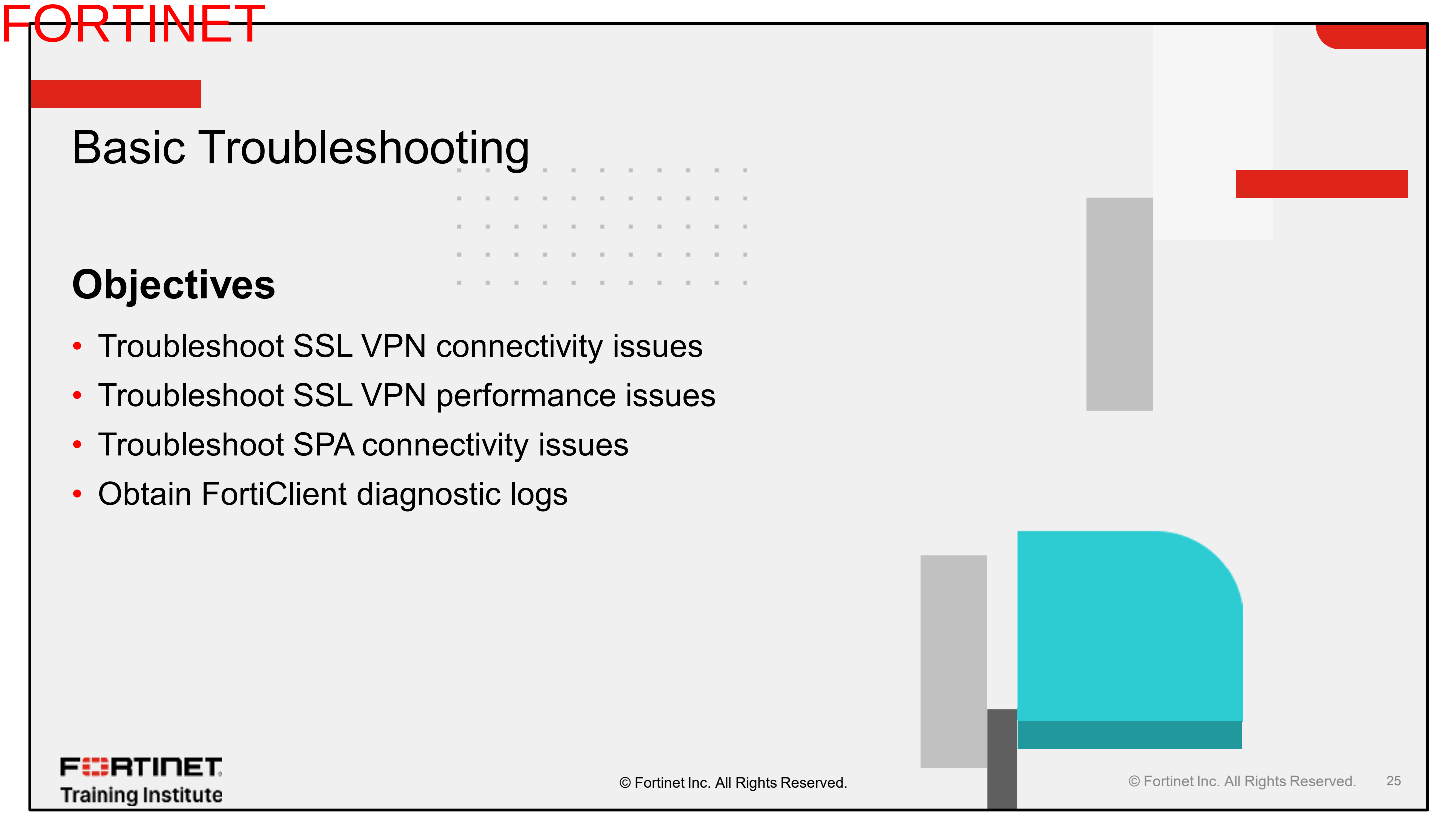
#	User (or IP)	Requests
1	saselocaluser@gmail.com	2,201
2	saseuser	1,293
3	fctuser	663

The example on this slide shows the partial output of the table of contents, and some of the graphs and tables contained within a local report generated on FortiSASE.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET

Brave-dumps.com



Basic Troubleshooting

Objectives

- Troubleshoot SSL VPN connectivity issues
- Troubleshoot SSL VPN performance issues
- Troubleshoot SPA connectivity issues
- Obtain FortiClient diagnostic logs

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved. 25

After completing this section, you should be able to achieve the objectives shown on this slide.

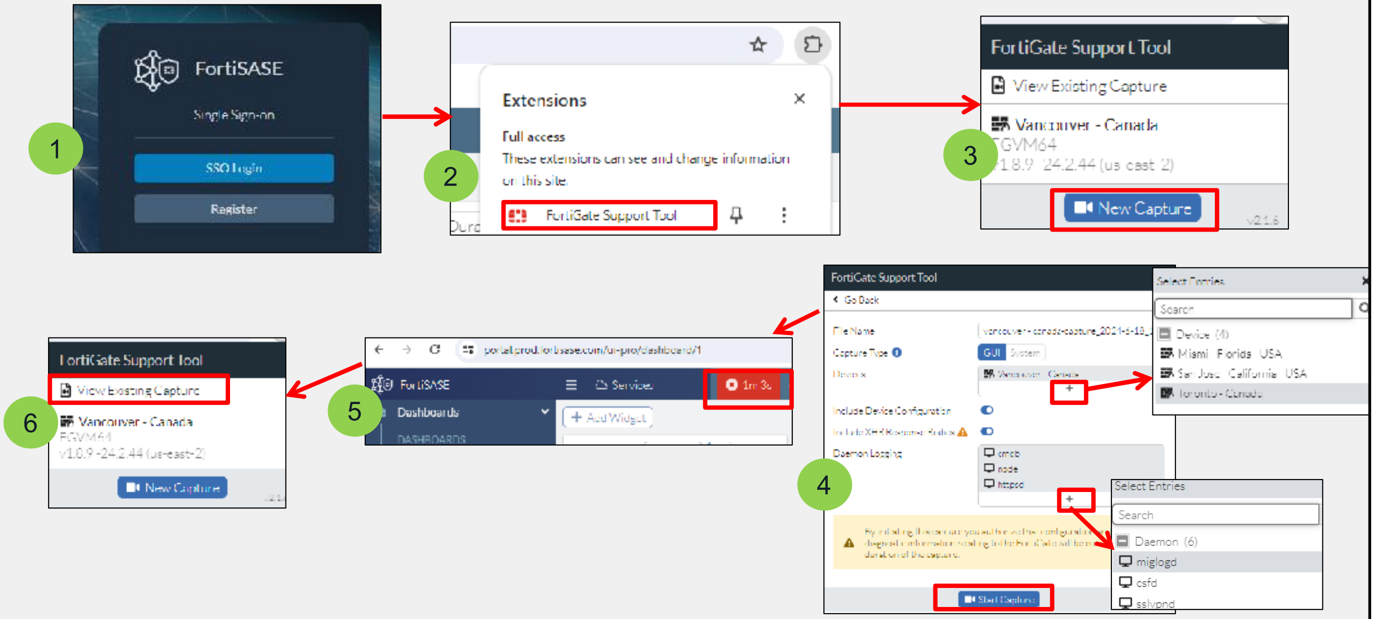
By demonstrating competence in basic troubleshooting, you will be able to gather basic information to troubleshoot FortiSASE issues.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET

Brave-dumps.com

FortiGate Support Tool



F⸬RTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

26

The FortiGate support tool Google chrome extension can be leveraged to collect several pieces of information at once, which may be helpful for troubleshooting. The FortiGate support tool is available from the Google Chrome web store. Add this extension to your Google Chrome browser to capture FortiSASE POP daemon logs, HTTP network logs, CPU and memory usage, and so on.

To create a new capture using the FortiGate support tool, follow these general steps:

1. Log in to FortiSASE using your Google Chrome browser.
2. Locate and click **FortiGate Support Tool**.
3. Click **New Capture** to start a new capture.
4. A new window opens. You can choose options such as **File Name**, **Devices**, and **Daemon Logging** to have to debug enabled. In the **Devices** section, click **+** to add more FortiSASE secure POPs to your capture. In the **Daemon Logging** section, click **+** to add more daemons to the capture. Click **Start Capture** to begin capturing the session.
5. While the capture is running, reproduce the issue and the relevant data will be gathered. Stop the capture by clicking the red button on the FortiSASE portal. After the capture ends, a `.fgtcapture` file will be downloaded.
6. To view the capture, launch the extension again, click **View Existing Capture**, and then select the `.fgtcapture` file that was downloaded in the previous step.

Vouchers & Dumps are Available | WhatsApp +201224560923

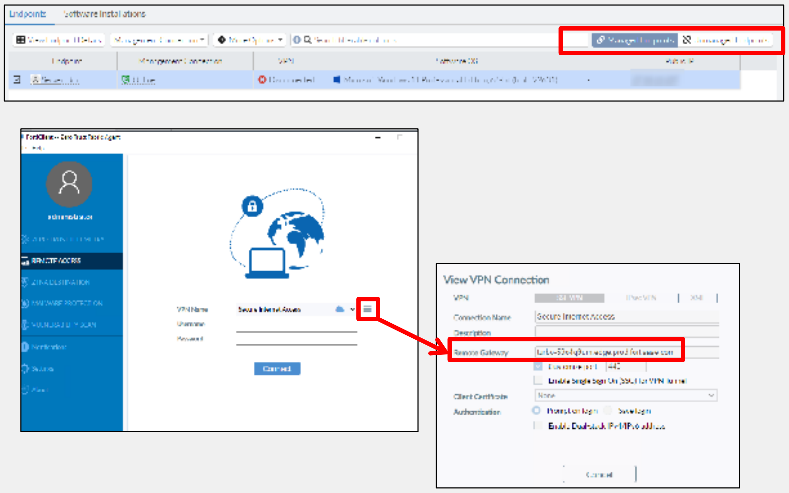
DO NOT REPRINT
© FORTINET

Brave-dumps.com

SSL VPN Connectivity

- Verify that FortiClient is registered and managed by FortiSASE
  - Check if the FortiClient endpoint is managed or unmanaged on the FortiSASE portal
- Verify that the endpoint can resolve the FDQN of the SSL VPN remote gateway
  - Check the connection details of the Secure Internet Access VPN on FortiClient
- Verify that FortiClient is running a supported version
  - Refer to the FortiSASE administrator guide for supported release

Network > Managed Endpoints



© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved.

If you're troubleshooting SSL VPN connectivity issues, the FortiSASE administrator will need to verify that FortiClient is still registered and managed by FortiSASE. You can check the endpoint management status on the **Managed Endpoints** page in the FortiSASE portal. The endpoint should also be able to resolve the fully qualified domain name (FQDN) of the FortiSASE remote gateway. Refer to the *FortiSASE Administrator Guide* to verify that the endpoint is running a supported release of FortiClient.

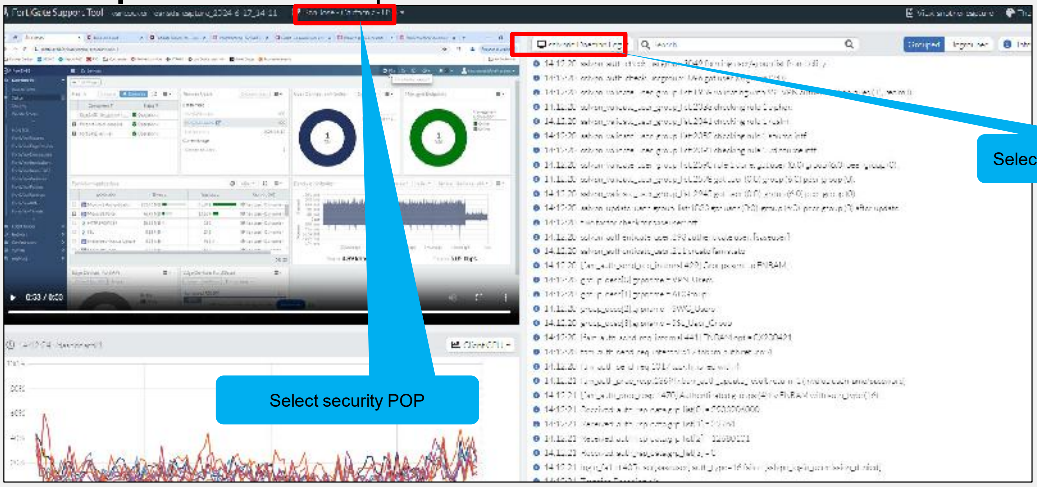
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET

Brave-dumps.com

SSL VPN Connectivity (Contd)

- Enable SSL VPN debug on FortiSASE using the FortiGate support tool
- Select the security POP that the user will connect to, based on their location
- Verify the **sslvpnd** daemon is captured



Select **sslvpn Daeomon Log**

Select security POP

© Fortinet Inc. All Rights Reserved.

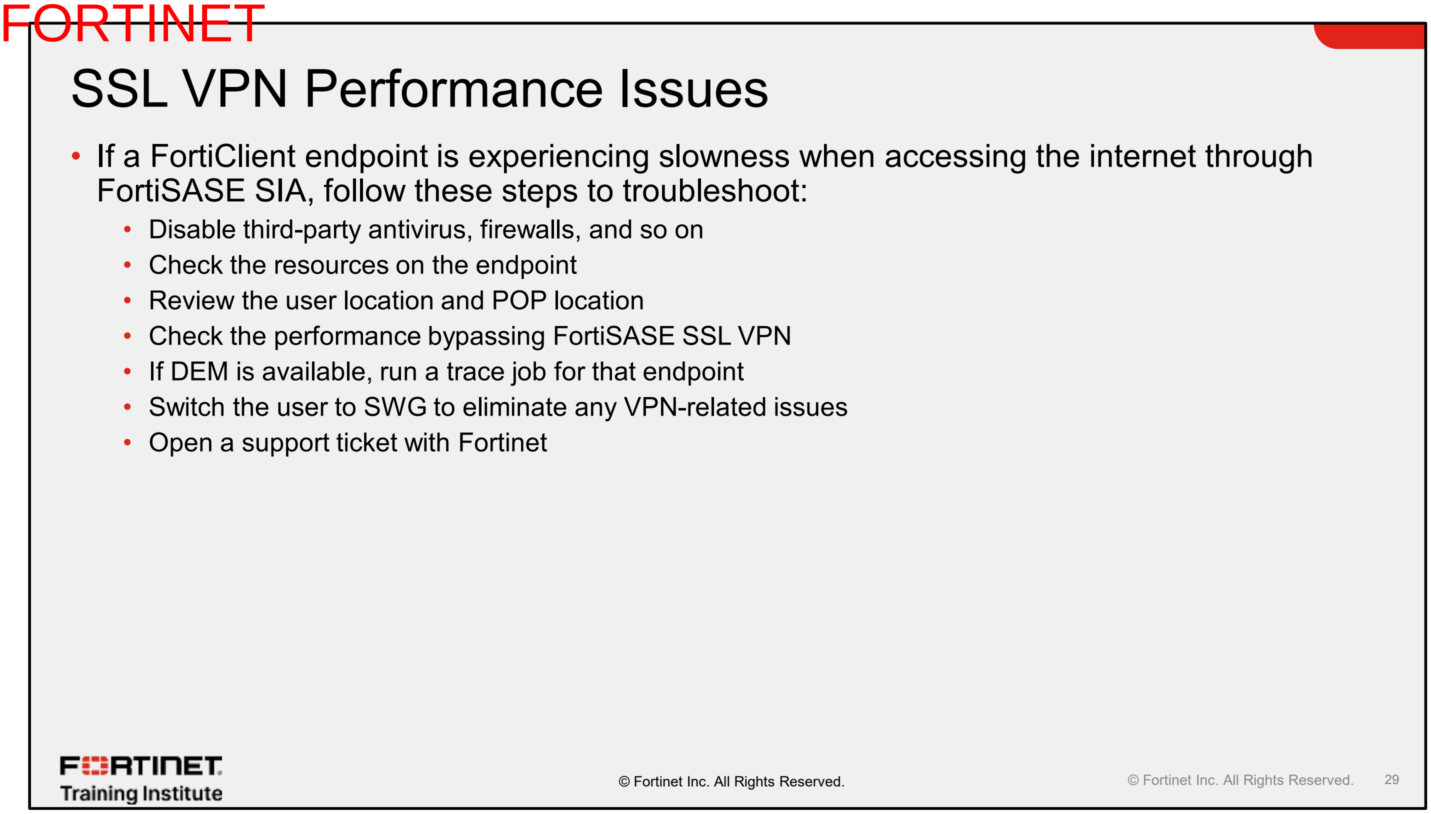
© Fortinet Inc. All Rights Reserved.

You can run real-time SSL VPN debug commands on FortiSASE, using the FortiGate support tool Google Chrome extension. You will need to select the security POP the user is trying to connect to and verify that the **sslvpnd** daemon is logged before starting the capture.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET

Brave-dumps.com



SSL VPN Performance Issues

- If a FortiClient endpoint is experiencing slowness when accessing the internet through FortiSASE SIA, follow these steps to troubleshoot:
  - Disable third-party antivirus, firewalls, and so on
  - Check the resources on the endpoint
  - Review the user location and POP location
  - Check the performance bypassing FortiSASE SSL VPN
  - If DEM is available, run a trace job for that endpoint
  - Switch the user to SWG to eliminate any VPN-related issues
  - Open a support ticket with Fortinet

© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved.

If you’re troubleshooting SSL VPN performance issues on an endpoint, begin by disabling any third-party antivirus, firewalls, and so on. Check the CPU, memory, and network resources on the endpoint.

If the performance issue continues, your next step is to disconnect the FortiSASE SSL VPN and check the performance while the endpoint is accessing the internet using its own default gateway. If the FortiSASE instance is licensed with DEM, run a trace job on the endpoint. To eliminate FortiSASE SSL VPN issues, switch the user to FortiSASE secure web gateway (SWG) and test the internet browsing.

Open a ticket with Fortinet support to do more extensive troubleshooting.

Vouchers & Dumps are Available | WhatsApp +201224560923

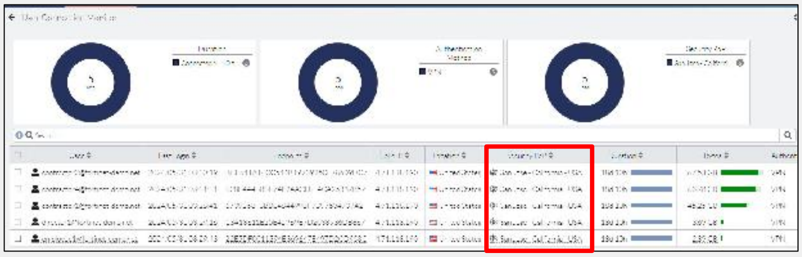
DO NOT REPRINT
© FORTINET

Brave-dumps.com

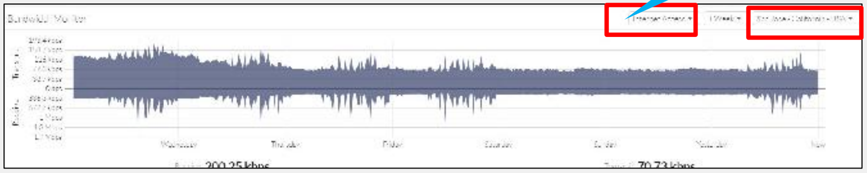
SSL VPN Performance Issues (Contd)

- If multiple FortiClient endpoints are experiencing slowness when accessing the internet through FortiSASE SIA, follow these steps to troubleshoot:
  - Verify that the endpoints are connected to the same security POP
  - Check the bandwidth monitor on FortiSASE for incoming traffic and internet access for that particular POP

Dashboards > Status



Dashboards > Status



Type of traffic

Select POP

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved.

If you’re troubleshooting SSL VPN performance issues on multiple endpoints, begin by verifying that all of the users are connected to the same security POP using the **User Connection Monitor** widget in the FortiSASE portal. You can also check the bandwidth usage on a specific security POP by checking the **Bandwidth Monitor** widget in the FortiSASE portal to see if the POP is overutilized.

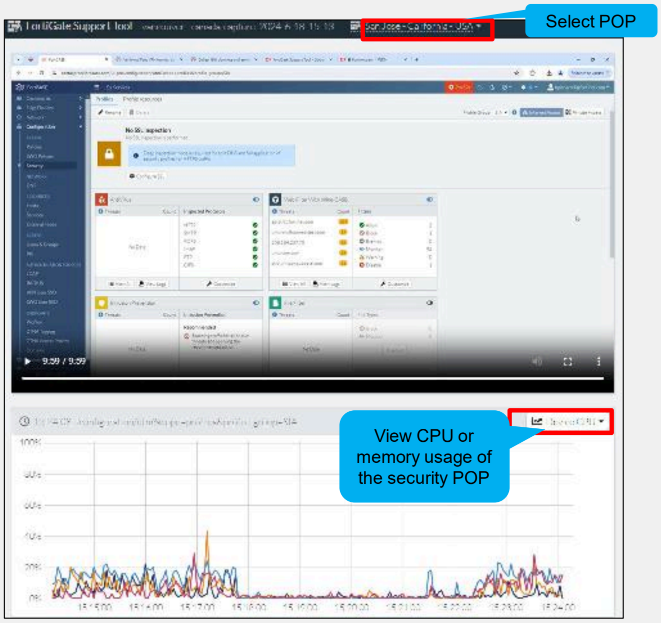
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET

Brave-dumps.com

SSL VPN Performance Issues (Contd)

- Check the CPU and memory of that particular POP for a ten-minute duration using the FortiGate support tool
- Create a new VPN policy and security profile with all security features disabled
- If DEM is available on FortiSASE, check the metrics for that POP
- Open a support ticket with Fortinet



© Fortinet Inc. All Rights Reserved.

You can view the CPU and memory usage of a specific POP using the FortiGate support tool Google chrome extension. You can also create a new VPN policy with a security profile that has no security features enabled. This will help you determine if the security profile is causing any delay or slow internet browsing. Finally, if the FortiSASE instance has a DEM license, you can review the DEM health check metrics for first-mile connectivity between the specified FortiSASE security POPs and the SaaS applications.

Open a ticket with Fortinet support to do more extensive troubleshooting.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET

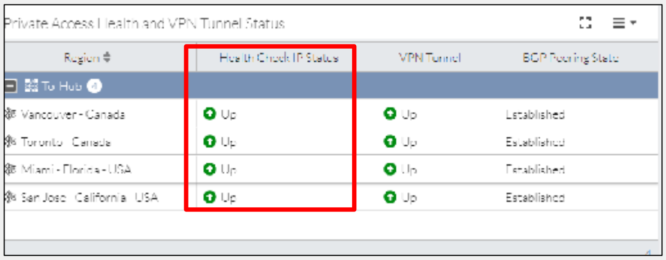
Brave-dumps.com

SPA—IPsec VPN Issues

- On FortiSASE, check the following:
  - The health status of the tunnel from each security POP
  - If the tunnel to the hub FortiGate from any security POP is down, check the FortiSASE portal to see if any maintenance is scheduled
- On the hub FortiGate, run the following debugs to capture the IPsec VPN negotiations:

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

Dashboards > Private Access



Private Access Health and VPN Tunnel Status

Region	Health Check IP Status	VPN Tunnel	BGP Peering State
To Hub 4			
Vancouver - Canada	Up	Up	Established
Toronto - Canada	Up	Up	Established
Miami - Florida - USA	Up	Up	Established
San Jose - California - USA	Up	Up	Established

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved.

You can verify the health of the secure private access (SPA) VPN tunnels on the private access dashboard. On the status dashboard, check if any ongoing maintenance on a specific security POP that is causing the outage.

You can run the debug CLI commands shown on this slide on the hub FortiGate to troubleshoot IPsec VPN connectivity issues.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET

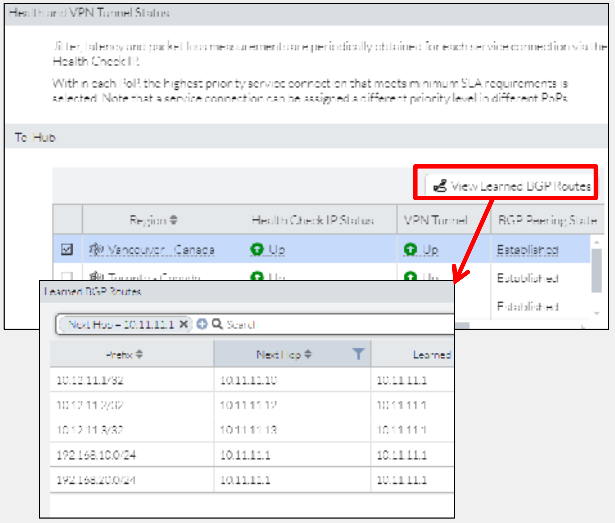
Brave-dumps.com

SPA—BGP Issues

- On FortiSASE, check the following:
  - The BGP peering state from each security POP to the hub FortiGate
  - Review the BGP routes received from the hub FortiGate on the **Secure Private Access** page
- On the hub FortiGate run the following debugs to capture the BGP peering and advertised routes:

```
diagnose ip router bgp all enable
diagnose ip router bgp level info
diagnose debug enable
get router info routing-table bgp
get router info bgp neighbors
<FortiSASE POP IP> advertised-
routes
get router info routing-table bgp
```

Network > Secure Private Access



Health and VPN Tunnel Status

Jitter, latency and packet loss measurements are periodically obtained for each service connection via the Health Check IP.

Within each PoP, the highest priority service connection that meets minimum SLA requirements is selected. Note that a service connection can be assigned a different priority level in different PoPs.

To Hub

	Region	Health Check IP Status	VPN Tunnel	BGP Peering State
☑	Vancouver, Canada	Up	Up	Established
□	Toronto, Canada	Up	Up	Established
				Established

Learned BGP Routes

Prefix	Next Hop	Learned
10.12.11.1/32	10.11.11.10	10.11.11.1
10.12.11.2/32	10.11.11.12	10.11.11.1
10.12.11.3/32	10.11.11.13	10.11.11.1
192.168.10.0/24	10.11.11.1	10.11.11.1
192.168.20.0/24	10.11.11.1	10.11.11.1

© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved.

You can verify the BGP peering state of the SPA VPN tunnels on the private access dashboard. You can also verify the routes advertised by the hub FortiGate on FortiSASE by clicking **Health** on the **Secure Private Access** page. Select the security POP and then click **View Learned BGP Routes**.

You can run the debug CLI commands shown on this slide on the hub FortiGate to troubleshoot BGP peering issues.

Open a ticket with Fortinet support to do more extensive troubleshooting.

Vouchers & Dumps are Available | WhatsApp +201224560923

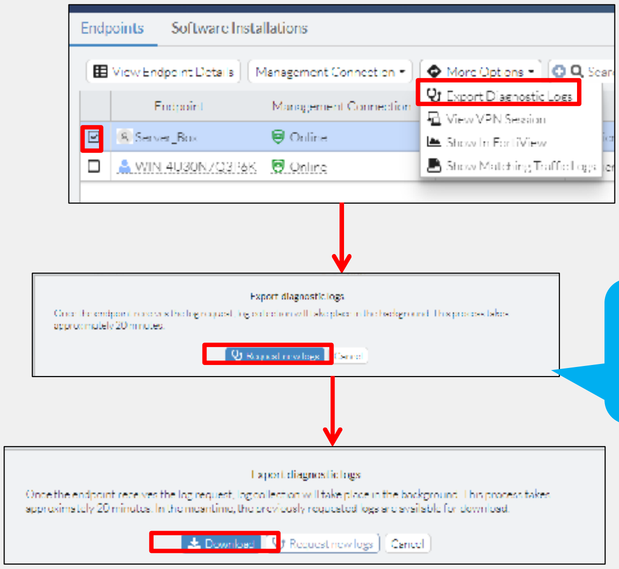
DO NOT REPRINT
© FORTINET

Brave-dumps.com

Diagnostic Logs

- Diagnostic logs can be requested from the FortiSASE portal if the following criteria is met:
  - Endpoint is online and managed by FortiSASE
- Diagnostic logs contain the following information about the endpoint:
  - Windows OS version
  - Windows software updates
  - Names and versions of installed software
  - Names and versions of installed drivers
  - FortiClient configuration
  - FortiClient logs

Network > Managed Endpoints



Export diagnostic logs

Once the endpoint receives the log request, log collection will take place in the background. This process takes approximately 20 minutes.

Export diagnostic logs

Once the endpoint receives the log request, log collection will take place in the background. This process takes approximately 20 minutes. In the meantime, the previously requested logs are available for download.

It will take approximately 20 minutes to gather the diagnostics logs from the FortiClient endpoint

F⁝⁝RTINET
Training Institute

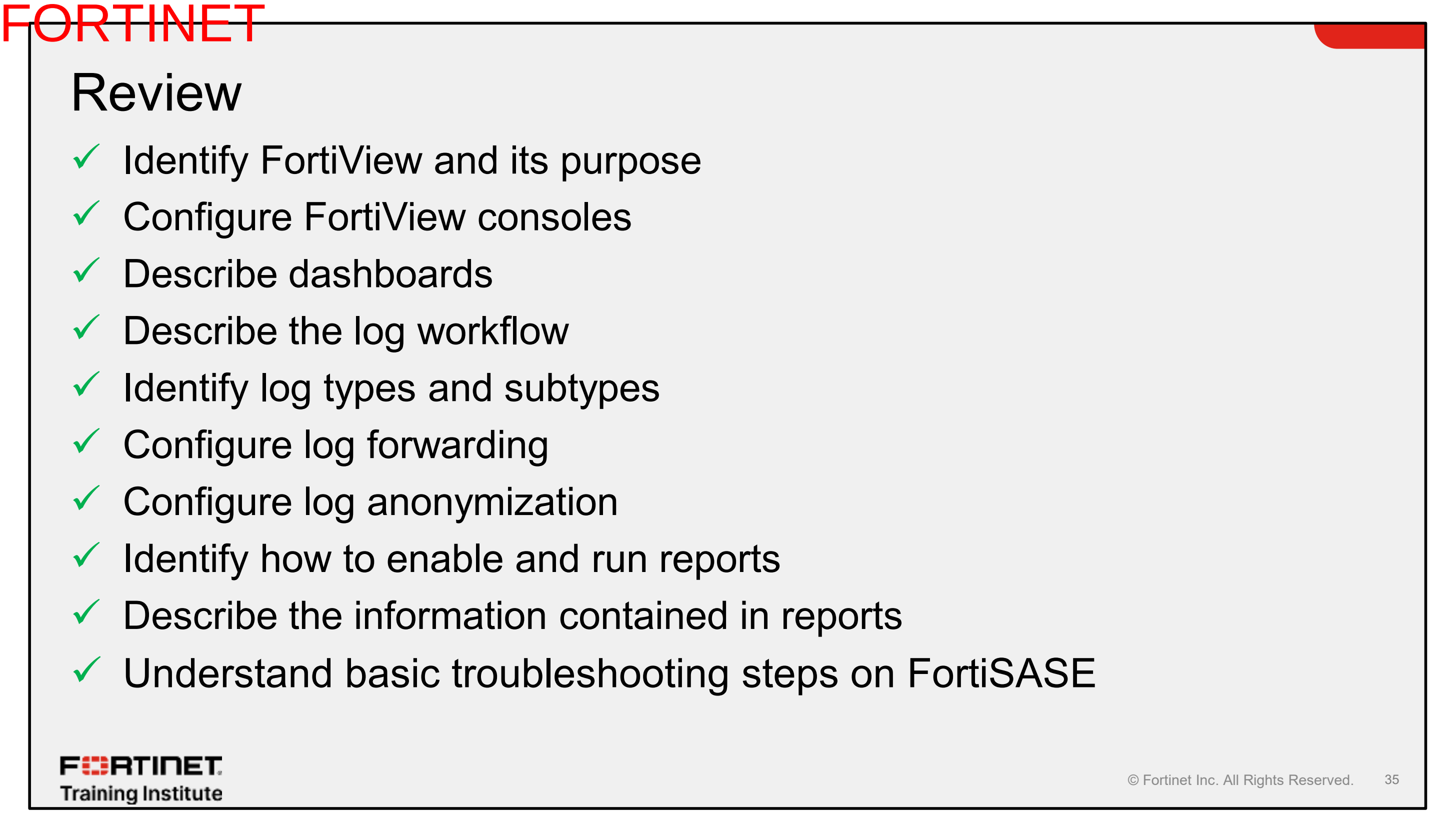
© Fortinet Inc. All Rights Reserved.

You can export diagnostic logs from FortiClient endpoints that are online and managed by FortiSASE, and then provide the debug report to the support team to help with troubleshooting. You can initiate the request to start the diagnostics on the **Managed Endpoints** page. Select the endpoint, then click **More Options** > **Export Diagnostic Logs**. When you request logs from the FortiClient endpoint for the first time, click **Request new logs** to start gathering logs from the endpoint. It will take approximately 20 minutes for this process to complete. Select the endpoint, then click **More Options** > **Export Diagnostic Logs**. This time click, **Download**, to download the available diagnostic logs for the endpoint. When you request new logs for this endpoint, the old ones are overwritten.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET

Brave-dumps.com



Review

- ✓ Identify FortiView and its purpose
- ✓ Configure FortiView consoles
- ✓ Describe dashboards
- ✓ Describe the log workflow
- ✓ Identify log types and subtypes
- ✓ Configure log forwarding
- ✓ Configure log anonymization
- ✓ Identify how to enable and run reports
- ✓ Describe the information contained in reports
- ✓ Understand basic troubleshooting steps on FortiSASE

© Fortinet Inc. All Rights Reserved. 35

This slide shows the objectives that you covered in this lesson.

By mastering the objectives covered in this lesson, you learned how to monitor and perform basic troubleshooting on FortiSASE.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET

Brave-dumps.com

No part of this publication may be reproduced in any form or by any means or used to make any derivative such as translation, transformation, or adaptation without permission from Fortinet Inc., as stipulated by the United States Copyright Act of 1976.

Copyright© 2024 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features, or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations,and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.