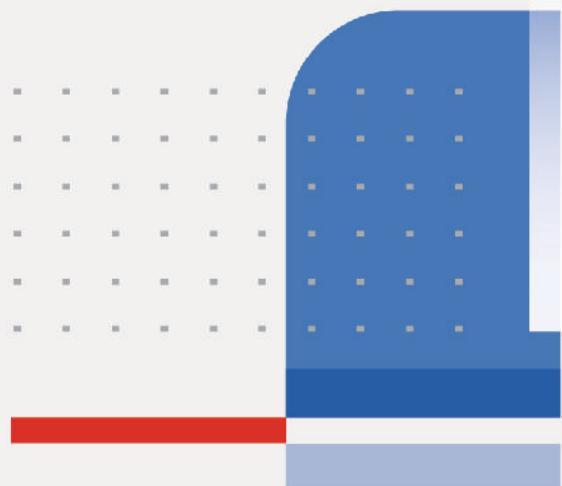


DO NOT REPRINT
© FORTINET

FortiOS Administrator Study Guide

FortiOS 7.6

FORTINET®
Training Institute



DO NOT REPRINT

© FORTINET

Fortinet Training Institute - Library

<https://training.fortinet.com>

Fortinet Product Documentation

<https://docs.fortinet.com>

Fortinet Knowledge Base

<https://community.fortinet.com/t5/Knowledge-Base/ct-p/knowledgebase>

Fortinet Fuse User Community

<https://community.fortinet.com/>

Fortinet Forums

<https://community.fortinet.com/t5/Support-Forum/bd-p/fortinet-discussion>

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>



TABLE OF CONTENTS

01 System and Network Settings.....	4
02 Logging and Monitoring.....	31
03 Firewall Policies and NAT.....	68
04 Routing.....	111
05 Firewall Authentication.....	142
06 Fortinet Single Sign-On (FSSO).....	174
07 Certificate Operations.....	216
08 Antivirus.....	250
09 Web Filtering.....	279
10 Intrusion Prevention and Application Control.....	309
11 IPsec VPN.....	346
12 SD-WAN Configuration and Monitoring.....	402
13 High Availability.....	445
14 Diagnostics and Troubleshooting.....	476
15 FortiGate in the Cloud.....	507
16 FortiSASE.....	535

DO NOT REPRINT

© FORTINET

FORTINET
Training Institute

FortiOS Administrator

System and Network Settings

FortiOS 7.6

Last Modified: 6 October 2025

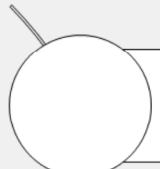
© Fortinet Inc. All Rights Reserved. 1

In this lesson, you will learn about system and network settings on FortiGate.

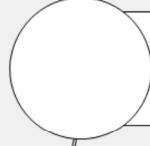
DO NOT REPRINT

© FORTINET

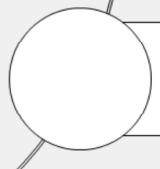
Lesson Overview



Initial Setup



Basic Administration



FortiGuard Subscription



© Fortinet Inc. All Rights Reserved.

2

In this lesson, you will learn about the topics shown on this slide.

DO NOT REPRINT**© FORTINET**

Initial Setup

Objectives

- Configure FortiGate using the factory default settings
- Configure FortiGate as the DHCP server

 © Fortinet Inc. All Rights Reserved. 3

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

By demonstrating competence in basic system and network administration, you will be able to perform the initial setup of FortiGate and configure basic networking settings.

DO NOT REPRINT**© FORTINET**

The Modern Context of Network Security

- Firewalls are more than gatekeepers on the network perimeter
- Today's firewalls are designed in response to multifaceted and multidevice environments with no identifiable perimeter:
 - Mobile workforce
 - Partners accessing your network services
 - Public and private clouds
 - Internet of Things (IoT)
 - Operation technology (OT)
 - Bring your own device (BYOD)
- Firewalls are expected to perform different functions within a network
 - Different deployment modes:
 - Distributed enterprise firewall
 - Next-generation firewall (NGFW)
 - Internal segmentation firewall (ISFW)
 - Data-center firewall
 - DNS, DHCP, web filter, intrusion prevention system (IPS), and so on



In the past, the most common method of protecting a network was securing the perimeter and installing a firewall at the entry point. Network administrators trusted everything and everyone inside the perimeter.

Now, malware can easily bypass any entry-point firewall and get inside the network. This could happen through an infected USB stick or a compromised device being connected to the corporate network. Additionally, because attacks can come from inside a network, network administrators can no longer inherently trust internal all users and devices.

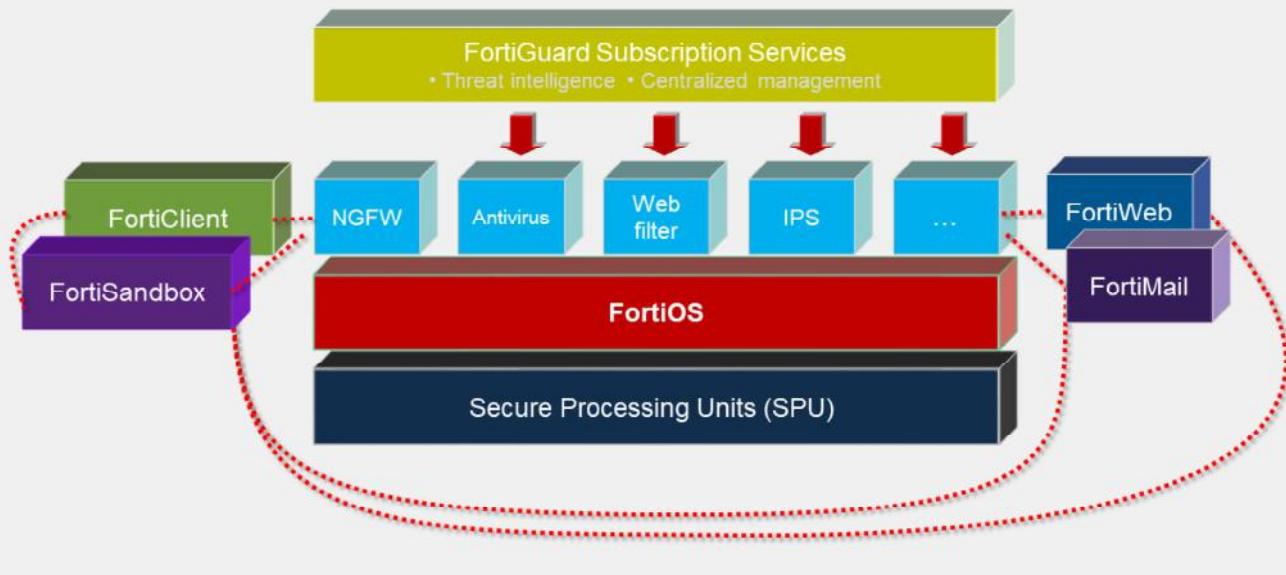
What's more, today's networks are highly complex environments whose borders are constantly changing. Networks run vertically from the LAN to the internet, and horizontally from the physical network to the private virtual network and to the cloud. A mobile and diverse workforce (employees, partners, and customers) accessing network resources; public and private clouds; and IoT, OT, and BYOD programs all conspire to increase the number of attack vectors faced by your network.

In response to this highly complex environment, firewalls have become robust, multifunctional devices that counter an array of threats to your network. FortiGate can act in different modes or roles to address different requirements. For example, FortiGate can be deployed as a data-center firewall whose function is to monitor inbound requests to servers and to protect them without increasing latency for the requester. Alternatively, FortiGate can be deployed as an ISFW as a way to contain a network breach.

FortiGate can also function as DNS and DHCP servers and be configured to provide web filter, antivirus, and IPS services.

DO NOT REPRINT
© FORTINET

Platform Design



© Fortinet Inc. All Rights Reserved.

5

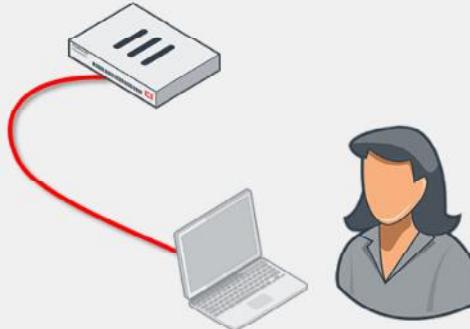
In the architecture diagram shown on this slide, you can see how FortiGate platforms add strength, without compromising flexibility. Like separate, dedicated security devices, FortiGate is still *internally* modular. Plus:

- Devices add duplication. Sometimes, dedication *doesn't* mean efficiency. If it's overloaded, can one device borrow free RAM from nine others? Do you want to configure policies, logging, and routing on 10 separate devices? Does 10 times the duplication bring you 10 times the benefit, or is it a hassle? For small and midsize businesses (SMB) or enterprise branch offices, unified threat management (UTM) is often a superior solution compared to separate, dedicated appliances.
- FortiGate hardware isn't just off-the-shelf. It's carrier grade. Most FortiGate models have one or more specialized circuits, called application-specific integrated circuits (ASIC), that are engineered by Fortinet. For example, a content processor (CP) or network processor (NP) chip handles cryptography and packet forwarding more efficiently. Compared to a single-purpose device with only a CPU, FortiGate can have dramatically better performance. This is especially critical for data centers and carriers where throughput is business critical.
 (The exception? Virtualization platforms—VMware, Citrix Xen, Microsoft, or Oracle Virtual Box—have general-purpose virtual CPUs (vCPUs). But, virtualization might be worthwhile because of other benefits, such as distributed computing and cloud-based security.)
- FortiGate is flexible. If all you need is fast firewalling and antivirus, FortiGate will not cause you to waste CPU, RAM, and electricity on other features. In each firewall policy, you can enable or disable UTM and NGFW modules. Also, you won't pay more to add VPN seat licenses later.
- FortiGate cooperates. A preference for open standards instead of proprietary protocols means less vendor lock-in and more choice for system integrators. And, as your network grows, FortiGate can leverage other Fortinet products, such as FortiSandbox and FortiWeb, to distribute processing for deeper security and optimal performance—a total Security Fabric approach.

DO NOT REPRINT**© FORTINET**

Factory Default Settings

- IP: 192.168.1.99/24
 - Management interface on high-end and mid-range models
 - Port1 or internal interface on entry-level models
 - PING, HTTPS, and SSH protocol management enabled
 - Built-in DHCP server is enabled on port1 or internal interface
 - Only on entry-level models that support DHCP server
 - Default login
- User: admin
- Password: (blank)
- Both are case sensitive
 - Modify the default (blank) password
- Can access FortiGate on the CLI
 - Console: without network
 - CLI console widget and terminal emulator, such as PuTTY or Tera Term



© Fortinet Inc. All Rights Reserved.

6

Network address translation (NAT) mode is the default operation mode. What are the other factory default settings? After you have removed FortiGate from its box, what do you do next?

Attach your computer network cable to port1 or the internal switch ports (on the entry-level model). For high-end and mid-range models, connect to the management interface. In most entry-level models, there is a DHCP server on that interface. So, if your computer's network settings have DHCP enabled, your computer should automatically get an IP address, and you can begin to set up.

To access the GUI on FortiGate or FortiWiFi, open a web browser and visit <https://192.168.1.99>.

The default login information is public knowledge. Never leave the default password blank. Your network is only as secure as your FortiGate admin account. Once you log in with default login details, you'll see a message instructing you to the default admin user password. Before you connect FortiGate to your network, you should set a complex password. You will also be asked to apply additional configuration information such as host name, dashboard setup, FortiCare registration, and so on.

All FortiGate models have a console port, or USB management port, or both. The port provides CLI access, without a network. You can access the CLI using the CLI console widget on the GUI or from a terminal emulator, such as PuTTY or Tera Term.

DO NOT REPRINT**© FORTINET**

Modes of Operation

NAT mode (default operation mode)

- FortiGate is an OSI layer 3 *router*
- Interfaces have IP addresses
- Packets are routed by IP address



Transparent mode

- FortiGate is an OSI layer 2 *switch* or *bridge*
- Interfaces do *not* have IP addresses
- Cannot route packets, only forward or block



When you deploy FortiGate, you can choose between two operating modes: NAT mode or transparent mode.

- In NAT mode, FortiGate routes packets based on layer 3, like a router. Each of its logical network interfaces has an IP address, and FortiGate determines the outgoing or egress interface based on the destination IP address and entries in its routing tables.
- In transparent mode, FortiGate forwards packets at layer 2, like a switch. Its interfaces have no IP addresses, and FortiGate identifies the outgoing or egress interface based on the destination MAC address. The device in transparent mode has an IP address used for management traffic.

NAT mode is the default operation mode. In this course, you will learn about only the NAT mode operation of FortiGate.

DO NOT REPRINT

© FORTINET

Interface IP Addresses

- In NAT mode, you can't use interfaces until they have an IP address:
 - Manually assigned
 - Automatic
 - DHCP
 - PPPoE

Network > Interfaces

Edit Interface

Name	port5
Alias	
Type	Physical Interface
VRF ID	0
Role	Undefined
<input type="checkbox"/> Dedicated Management Port	
Address	
Addressing mode	Manual
IP/Netmask	0.0.0.0/0.0.0.0
Secondary IP address	<input type="checkbox"/>

Network > Interfaces

Edit Interface

Name	port5
Alias	
Type	Physical Interface
VRF ID	0
Role	Undefined
<input type="checkbox"/> Dedicated Management Port	
Address	
Addressing mode	DHCP
Retrieve default gateway from server	<input checked="" type="checkbox"/>
Distance	5
Override internal DNS	<input type="checkbox"/>

© Fortinet Inc. All Rights Reserved. 8

When FortiGate is operating in NAT mode, every interface that handles traffic must have an IP address. When in NAT mode, FortiGate can use the IP address to source the traffic, if it needs to start or reply to a session, and as a destination address for devices trying to contact FortiGate or route traffic through it. There are multiple ways to get an IP address:

- Manually
- Automatically, using either DHCP or Point-to-Point Protocol over Ethernet (PPPoE) (available on the CLI)

DO NOT REPRINT
© FORTINET

Interface Role Compared to Alias

- Role defines interface settings typically grouped together:
 - Prevents accidental misconfiguration
 - Four types:
 - LAN
 - WAN
 - DMZ
 - Undefined (show all settings)
 - Not in a list of policies
- Alias is a friendly descriptor for the interface:
 - Used in a list of policies to label interfaces by purpose

The screenshot shows two parts of the FortiGate management interface. The top part, titled 'Network > Interfaces', displays the configuration for 'port5'. It includes fields for Name (port5), Alias (Internal_Network, highlighted with a red box), Type (Physical Interface), VRF ID (0), Role (set to LAN, also highlighted with a red box), and Addressing mode (Manual). The bottom part, titled 'Policy & Objects > Firewall Policy', shows a policy rule named 'Full_Access (1)' with 'Internal_Network (port5)' listed under the 'From' field, also highlighted with a red box.



© Fortinet Inc. All Rights Reserved.

9

How many times have you seen network issues caused by a DHCP server—not client—enabled on the WAN interface?

You can configure the interface role. The roles shown on the GUI are the usual interface settings for that part of a topology. Settings that do not apply to the current role are hidden on the GUI. (All settings are always available on the CLI, regardless of the role.) This prevents accidental misconfiguration.

For example, when the role is configured as **WAN**, there is no DHCP server and device detection configuration available. Device detection is usually used to detect devices internally on your LAN.

If there is an unusual case, and you need to use an option that's hidden by the current role, you can always switch the role to **Undefined**. This displays all options.

To help you remember the purpose of each interface, you can give them aliases. For example, you could call port3 `internal_network`. This can make your list of policies easier to comprehend.

Administrative access options are also limited depending on the role that is set for the interface. For an example, setting the interface role to **WAN** would not display the **Ping** option mitigating the risk of responding to a DoS ICMP attack from the WAN.

DO NOT REPRINT
© FORTINET

FortiGate as a DHCP Server

Network > Interfaces

The screenshot shows the FortiGate interface for managing network interfaces. On the left, under 'Edit Interface' for port3, the 'Address' section is highlighted with a red box around the IP/Netmask field, which contains '10.0.1.254/255.255.255.0'. On the right, the 'Administrative Access' section is shown with various checkboxes for protocols like HTTPS, HTTP, PING, etc. A large red box highlights the 'DHCP Server' section, which includes fields for 'Address range' (10.0.1.1-10.0.1.253), 'Netmask' (255.255.255.0), 'Default gateway' (Same as Interface IP), 'DNS server' (Same as System DNS), and 'Lease time' (604800 seconds).

For an interface (such as port3), select **Manual**, enter a static IP address, and then enable **DHCP Server**. Options for the built-in DHCP server appear, including provisioning features, such as DHCP options and IP address assignment rules.

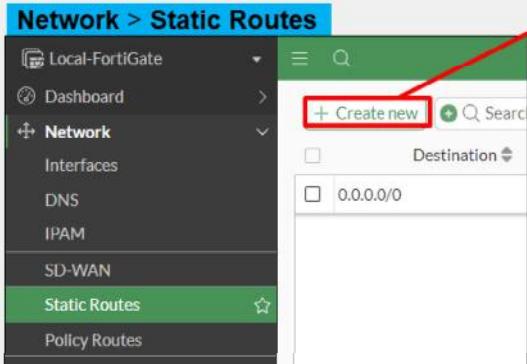
Advanced DHCP options allow you to automatically configure clients with additional network settings, such as DNS servers or NTP configurations. You can also enable DHCP relay to forward requests to an external server which is useful when managing IP addresses across multiple subnets. Additionally, custom IP address assignment rules provide precise control by mapping specific IP addresses to MAC addresses, or allocating address ranges, preventing conflicts, and ensuring consistency across the network.

DO NOT REPRINT

© FORTINET

Static Gateway

- Set a default route or configure a static one
- If the interface is DHCP or PPPoE, the gateway can be set dynamically



New Static Route

Destination	Subnet Internet Service 0.0.0.0/0.0.0.0
Gateway Address	0.0.0.0
Interface	port1
Administrative Distance	10
Comments	Write a comment... /255
Status	Enabled
Advanced Options	
Priority	1



Before you integrate FortiGate into your network, you should configure a default gateway.

If FortiGate gets its IP address through a dynamic method, such as DHCP or PPPoE, then it should also retrieve the default gateway.

Otherwise, you must configure a static route. Without this, FortiGate will not be able to respond to packets outside the subnets directly attached to its own interfaces. It likely will not be able to connect to FortiGuard—which is crucial for FortiGate updates—and may fail to route traffic correctly.

Make sure that FortiGate has a default route (matching all packets with the destination 0.0.0.0/0) configured to forward traffic through the network interface connected to the internet, directing it to the IP address of the next router.

You must configure routing to establish essential network settings before you can configure firewall policies.

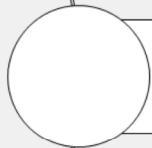
DO NOT REPRINT

© FORTINET

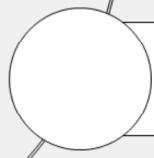
Lesson Progress



Initial Setup



Basic Administration



FortiGuard Subscription



© Fortinet Inc. All Rights Reserved.

12

Good job! You now understand how to perform the initial setup of FortiGate.

Now, you will learn about basic administration.

DO NOT REPRINT**© FORTINET**

Basic Administration

Objectives

- Configure and control administrator access to FortiGate

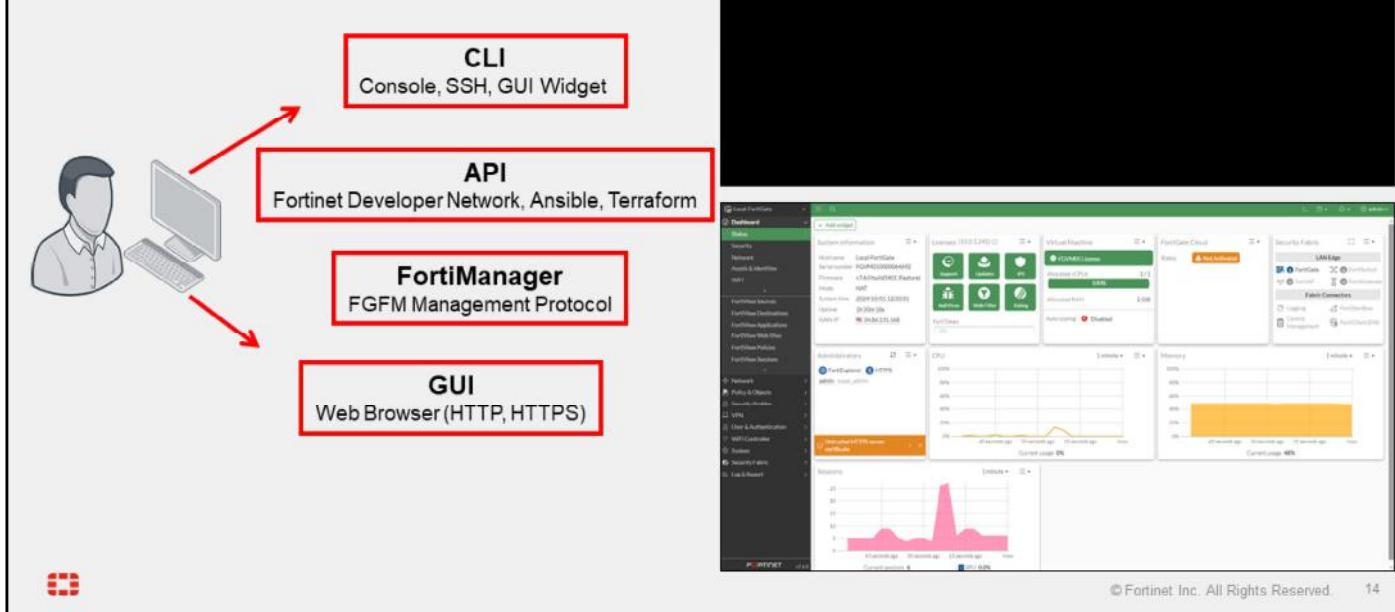


After completing this section, you should be able to achieve the objective shown on this slide.

By demonstrating competence in basic administration, you will be able to better manage administrative users and implement stronger security practices for administrative access.

DO NOT REPRINT
© FORTINET

Administration Methods



Most features are available on both the GUI and CLI, but there are a few exceptions. You can't view reports on the CLI. Also, advanced settings and diagnostic commands for super users are usually not available on the GUI.

As you become more familiar with FortiGate, and especially if you want to script its configuration, you might want to use the CLI, API or FortiManager in addition to the GUI. You can access the CLI through either the JavaScript widget on the GUI named **CLI Console**, or through a terminal emulator such as Tera Term or PuTTY. Your terminal emulator can connect through the network—SSH—or the local console port.

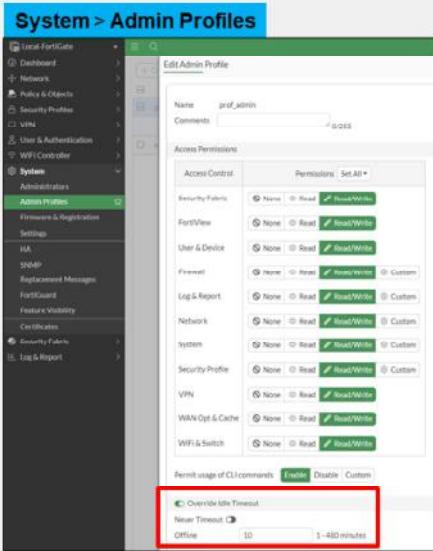
SNMP and some other administrative protocols are also supported, but they are read-only. You can't use them for basic setup.

DO NOT REPRINT

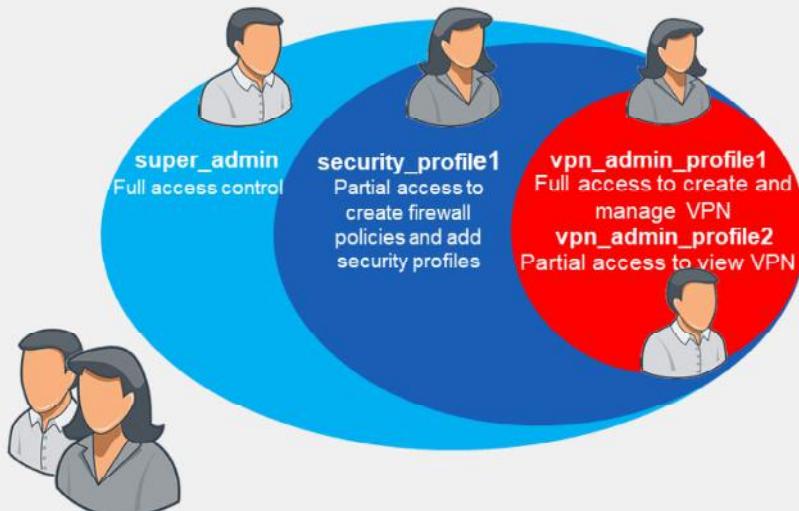
© FORTINET

Administrator Profiles

- Permissions



- Hierarchy



© Fortinet Inc. All Rights Reserved.

15

When assigning permissions to an administrator profile, you can specify read-and-write, read-only, or none to each area.

By default, there is a special profile named `super_admin`, which is used by the account named `admin`. You can't change it. It provides full access to everything, making the `admin` account similar to a root superuser account.

You aren't required to use a default profile. You could create a profile named `auditor_access` with read-only permissions. Restricting a person's permissions to those necessary for his or her job is a best practice, because even if that account is compromised, the compromise to your FortiGate device (or network) is not total. To do this, create administrator profiles and then select the appropriate profile when configuring an account.

The **Override Idle Timeout** option allows the `admintimeout` value, under `config system accprofile`, to be overridden for each access profile. You can configure administrator profiles to increase inactivity timeout and facilitate use of the GUI for central monitoring. Note that you can do this on a per-profile basis, to prevent the option from being unintentionally set globally. So, what are the effects of administrator profiles?

It's actually more than just read or write access. Depending on the type of administrator profile that you assign, an administrator may not be able to access the entire FortiGate device. For example, you could configure an account that can view only `vpn` settings and configure another profile to create firewall policies and security profiles.

DO NOT REPRINT
© FORTINET

Administrative Access—Trusted Sources

The screenshot shows the FortiOS interface for managing administrators. On the left, under 'System > Administrators', there is a configuration section for 'Trusted Hosts'. A red arrow points from the 'Trusted Host 1' field, which contains '10.0.1.10/32', to the right-hand list of administrators. The list shows a single entry: 'System Administrator' (admin) with IP '10.0.1.10/32', type 'super_admin', and status 'Local'. Below this, a note says: 'You can restrict an admin user to manage guest users with a guest group in place to provision users'. Another blue callout notes: 'If the admin user attempts to log in to the FortiGate GUI from any IP address other than 10.0.1.10, they receive this message'. To the right, a separate window shows a login screen with a red error message: 'Authentication failure'. The Fortinet logo and copyright information are at the bottom.

Another way to secure FortiGate is to define the hosts or subnets that are trusted sources from which to log in.

In this example, 10.0.1.10 is configured as the only trusted IP address for sources that the administrator logs in from. If the administrator attempts to log in from a machine with any other IP address, they will receive an authentication failure message.

Note that if trusted hosts are configured on all administrators and an administrator is trying to log in from an IP address that is not set on any of the trusted hosts for any administrators, then the administrator will not get the login page.

If you leave any IPv4 address as 0.0.0.0/0, it means that connections from any source IP address will be allowed. By default, 0.0.0.0/0 is the configuration for the administrator, although you may want to change this.

Note that each account can define its management host or subnet differently. Be aware of any NAT that occurs between the specified device and FortiGate. You can easily prevent an administrator from logging in from the specified IP address if it is later NATed to another address before reaching FortiGate, thus defeating the purpose of the trusted hosts.

You can also configure an administrator account that is restricted to provisioning guest accounts only. This option requires you to configure a guest user group.

DO NOT REPRINT
© FORTINET

Administrative Access—Ports and Password

- Port numbers are customizable
- Fortinet recommends using only secure access (SSH, HTTPS)
- Default **Idle timeout** value is 5 minutes

The screenshot shows the 'System > Settings' interface. The 'Administration Settings' section includes fields for HTTP port (80), Redirect to HTTPS (disabled), HTTPS port (443), HTTPS server certificate (self-sign), SSH port (22), Telnet port (23), and Idle timeout (5 minutes). The 'Password Policy' section includes fields for Password scope (Admin selected), Minimum length (8), Minimum number of new characters (0), Character requirements (disabled), Allow password reuse (disabled), and Password expiration (disabled).



© Fortinet Inc. All Rights Reserved. 17

You may also want to customize the administrative protocols port numbers.

You can choose whether to allow concurrent sessions. You can disallow concurrent sessions to avoid accidentally overwriting settings. Allowing concurrent settings lets an administrator open multiple browser tabs and CLI sessions at the same time. This may be more convenient for some situations, but it may also result in an administrator accidentally editing the same settings in conflicting ways over different connections.

For better security, use only secure protocols, and enforce password complexity and changes.

The **Idle timeout** setting specifies the number of minutes before an inactive administrator session times out (the default is 5 minutes). A shorter idle timeout is more secure, but increasing the timer can reduce the chance of administrators being logged out while testing changes.

You can override the idle timeout setting for each administrator profile using the **Override Idle Timeout** setting.

DO NOT REPRINT
© FORTINET

Administrative Access—Protocols

- Enable acceptable management protocols on each interface independently:
 - Separate IPv4 and IPv6
 - IPv6 options hidden by default
- Other protocols for which FortiGate is the destination IP address:
 - Security Fabric connection:
 - CAPWAP
 - FortiTelemetry
 - FMG-Access
 - FTM
 - RADIUS Accounting
- LLDP support
 - Detecting an upstream Security Fabric FortiGate through LLDP

The screenshot shows the 'Edit Interface' screen for 'port4'. The 'Administrative Access' section is highlighted with a red box. It contains checkboxes for various protocols:

Protocol	Status
SCIM	<input type="checkbox"/>
PING	<input checked="" type="checkbox"/>
SNMP	<input type="checkbox"/>
Security Fabric Connection	<input checked="" type="checkbox"/>
HTTPS	<input checked="" type="checkbox"/>
FMG-Access	<input type="checkbox"/>
FTM	<input type="checkbox"/>
Speed Test	<input type="checkbox"/>
HTTP	<input checked="" type="checkbox"/>
SSH	<input checked="" type="checkbox"/>
RADIUS Accounting	<input type="checkbox"/>



You've defined the management subnet—that is, the trusted hosts—for each administrator account. How do you enable or disable management protocols?

This is specific to each interface. For example, if your administrators connect to FortiGate only from port3, then you should disable administrative access on all other ports. This prevents brute force attempts and also insecure access. Your management protocols are HTTPS, HTTP, PING, and SSH. By default, the HTTP option is not visible on the GUI.

Consider the location of the interface on your network. Enabling PING on an internal interface is useful for troubleshooting. However, if it's an external interface (in other words, exposed to the internet), then the PING protocol could expose FortiGate to a denial of service (DoS) attack. You should disable protocols that do not encrypt data flow, such as HTTP. IPv4 and IPv6 protocols are separate. It's possible to have both IPv4 and IPv6 addresses on an interface, but only respond to pings on IPv6.

Security Fabric connection includes CAPWAP and FortiTelemetry. Protocols like FortiTelemetry are *not* for administrative access, but, like GUI and CLI access, they are protocols where the packets have FortiGate as a destination IP. Use the FortiTelemetry protocol specifically for managing FortiClient and the Security Fabric. Use the CAPWAP protocol for FortiAP, FortiSwitch, and FortiExtender when they are managed by FortiGate. Use the FMG-Access protocol specifically for communicating with FortiManager when that server is managing multiple FortiGate devices. Use the RADIUS accounting protocol when FortiGate needs to listen for and process RADIUS accounting packets for single sign-on (SSO) authentication. FTM, or FortiToken Mobile push, supports second-factor authentication requests from a FortiToken mobile app.

When you assign the interface roles LAN or WAN to the appropriate interfaces, your FortiGate uses the Link Layer Discovery Protocol (LLDP) to detect if there's an upstream FortiGate in your network. If FortiGate discovers an upstream FortiGate, you're prompted to configure the upstream FortiGate device to join the Security Fabric.

DO NOT REPRINT

© FORTINET

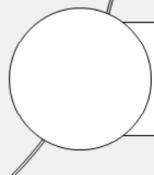
Lesson Progress



Initial Setup



Basic Administration



FortiGuard Subscription



© Fortinet Inc. All Rights Reserved.

19

Good job! You now understand basic administration.

Now, you will learn about FortiGuard subscription.

DO NOT REPRINT

© FORTINET

FortiGuard Subscription

Objectives

- Check and verify FortiGuard licenses
- Describe session packets on FortiGate

© Fortinet Inc. All Rights Reserved. 20

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

By demonstrating competence in FortiGuard subscription, you will be able to ensure that FortiGate remains reliably in service throughout its life cycle.

DO NOT REPRINT**© FORTINET**

FortiGuard Subscription Services

- Internet connection and contract required
- Provided by FortiGuard Distribution Network (FDN)
 - Major data centers in North America, Asia, and Europe
 - Or, from FDN through your FortiManager
 - FortiGate prefers the data center in nearest time zone, but will adjust by server load
- Package updates: FortiGuard antivirus and IPS
 - update.fortiguard.net
 - TCP port 443 (SSL)
- Live queries: FortiGuard web filtering, DNS filtering, and antispam
 - service.fortiguard.net for proprietary protocol on UDP port 53 or 8888
 - securewf.fortiguard.net for HTTPS over port 443, 53 or, 8888
- FortiOS uses FortiGuard server for DNS request
 - By default, uses DNS over TLS (DoT) to secure DNS traffic



© Fortinet Inc. All Rights Reserved. 21

Some FortiGate services connect to other servers, such as FortiGuard, in order to work. FortiGuard Subscription Services provide FortiGate with up-to-date threat intelligence. FortiGate uses FortiGuard by:

- Periodically requesting packages that contain a new engine and signatures
- Querying the FDN on an individual URL or host name

By default, the FortiGuard server location is set to anywhere FortiGate selects a server based on server load, from any part of the world. However, you have the option to change the FortiGuard server location to USA. In this case, FortiGate selects a USA-based FortiGuard server.

Queries are real-time; that is, FortiGate asks the FDN every time it scans for spam or filtered websites. FortiGate queries, instead of downloading the database, because of the size and frequency of changes that occur to the database. Also, you can select queries to use UDP or HTTPs for transport; the protocols are not designed for fault tolerance, but for speed. So, queries require that your FortiGate device has a reliable internet connection.

Packages, like antivirus and intrusion prevention system (IPS), are smaller and don't change as frequently, so they are downloaded (in many cases), only once a day. They are downloaded using TCP for reliable transport. After the database is downloaded, their associated FortiGate features continue to function, even if FortiGate does not have reliable internet connectivity. However, you should still try to avoid interruptions during downloads—if your FortiGate device must try repeatedly to download updates, it can't detect new threats during that time.

When using FortiGuard servers for DNS, FortiOS uses DNS over TLS (DoT) by default to secure the DNS traffic. New FortiGuard DNS servers have been added as primary and secondary servers.

DO NOT REPRINT**© FORTINET**

FortiGuard Licenses

The screenshot shows the 'System > FortiGuard' page. On the left, there's a table titled 'FortiGuard Distribution Network' under 'License Information'. It lists various service entitlements with their status (e.g., Licensed, Not Licensed) and expiration dates. Actions like 'Purchase', 'Activate', or 'Upgrade' are available for some items. A note says 'FortiCare support contracts can be activated here and applied directly to this FortiGate.' Below the table is a section for 'FortiGuard Updates' with a 'Next Update' timestamp and options to 'Update Licenses & Definitions Now' or 'Manual Update' via 'Upload License File'. To the right, there's a table for 'FortiGuard Updates' showing service names and traffic volume over the last 24 hours. At the bottom, there's an 'Additional Information' section with links to 'API Preview', 'Edit In CLI', and 'Online Guides' (including 'Relevant Documentation', 'Video Tutorials', and 'How to Purchase/Renew Fortinet Service Subscriptions').

You can check the status of FortiGuard licenses and the communication to FortiGuard on the FortiGate GUI. You can also check the versions of the locally installed databases for each of the FortiGuard services.

DO NOT REPRINT**© FORTINET**

FortiGuard Licenses (Contd)

```
Local-FortiGate # diagnose autoupdate versions
AV Engine
-----
Version: 7.00030 signed
Contract Expiry Date: Mon Jan 19 2026
Last Updated using manual update on Thu Jul 13 02:54:00 2024
Last Update Attempt: Mon Aug 25 13:52:18 2024
Result: No Updates

Virus Definitions
-----
Version: 90.01635 signed
Contract Expiry Date: Mon Jan 19 2026
Last Updated using manual update on Mon Jul 25 13:52:18 2024
Last Update Attempt: Mon Aug 25 13:52:18 2024
Result: Updates Installed
```

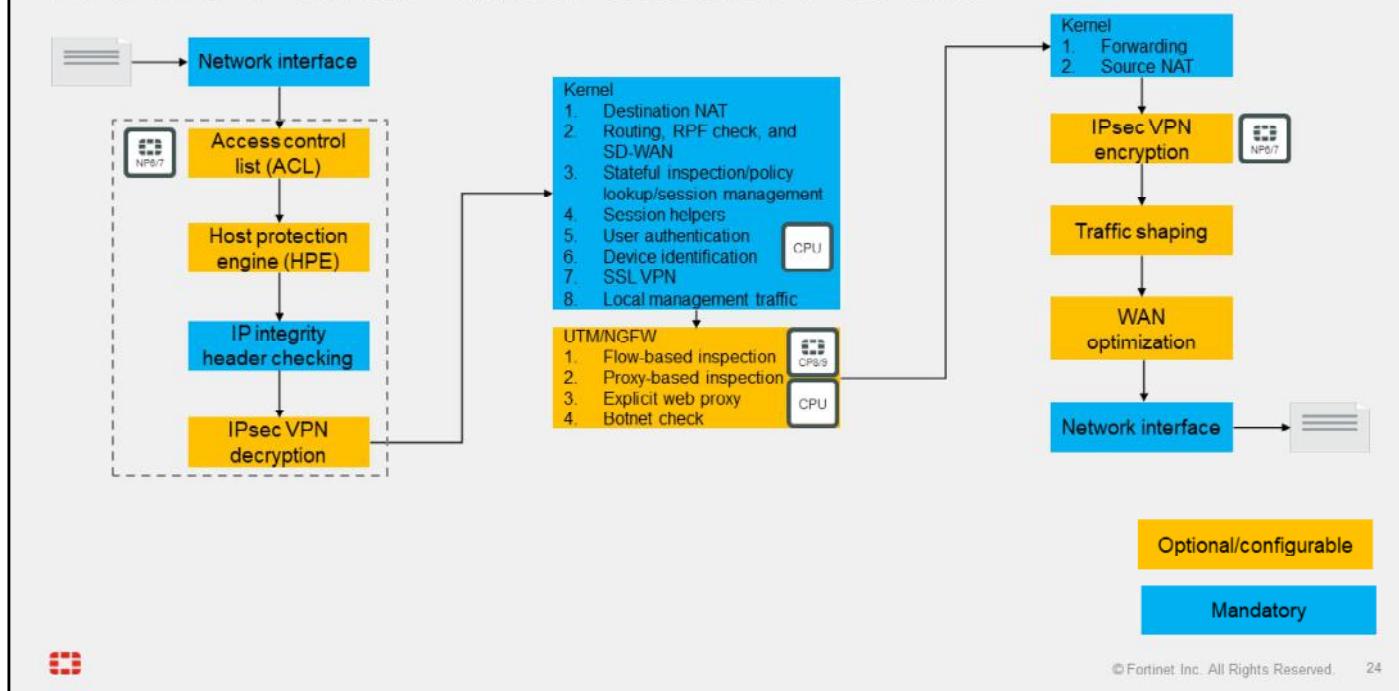


The command shown on this slide lists all the FortiGuard databases and engines installed. The information includes the version, contract expiration date, time it was updated, and what happened during the last update.

The list includes but is not limited to antivirus, IPS, application, mobile malware definitions, and other security services. FortiGate is licensed and updated using FortiGuard services.

DO NOT REPRINT
© FORTINET

Life of a Packet—Initial Session Packets



The flowchart on this slide shows the sequence of operations that the first packets of a new session go through as they enter, pass through, and exit FortiGate.

It also shows which processes can be offloaded to the network processor (NP) and content processor (CP), which are specially designed integrated circuits that improve performance and increase processing speeds on FortiGate. These processors are collectively known as secure processing units (SPU).

Many of the topics you covered in this lesson are included in this flow chart. You can use it as reference material.

DO NOT REPRINT**© FORTINET**

Knowledge Check

1. How do you restrict logins to FortiGate from specific IP addresses?
 - A. Change the FortiGate management interface IP address.
 - B. Configure a trusted host.

2. Which protocol option should you enable to give FortiManager access on FortiGate?
 A. FMG-Access protocol
 B. FTM protocol



DO NOT REPRINT

© FORTINET

Lesson Progress



Initial Setup



Basic Administration



FortiGuard Subscription



© Fortinet Inc. All Rights Reserved.

26

Congratulations! You have completed this lesson.

Now, you will review the objectives covered in this lesson.

DO NOT REPRINT**© FORTINET**

Review

- ✓ Configure FortiGate using the factory default settings
- ✓ Configure FortiGate as the DHCP server
- ✓ Configure and control administrator access to FortiGate
- ✓ Check and verify FortiGuard licenses
- ✓ Describe session packets on FortiGate



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

By mastering the objectives covered in this lesson, you learned how and where FortiGate fits into your network and how to perform basic FortiGate administration.

DO NOT REPRINT

© FORTINET

FORTINET
Training Institute

FortiOS Administrator

Logging and Monitoring

FortiOS 7.6

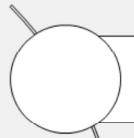
Last Modified: 6 October 2025

© Fortinet Inc. All Rights Reserved. 1

In this lesson, you will learn about FortiAnalyzer logging and monitoring.

DO NOT REPRINT**© FORTINET**

Lesson Overview



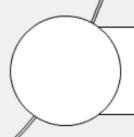
Describe the Log Workflow



Identify Log Storage Options



Register FortiGate with FortiAnalyzer



View and Search for Log Messages



© Fortinet Inc. All Rights Reserved.

2

In this lesson, you will learn about the topics shown on this slide.

DO NOT REPRINT**© FORTINET**

Describe the Log Workflow

Objectives

- Describe how traffic passes through FortiGate
- Identify various log types and subtypes
- Describe log severity levels



© Fortinet Inc. All Rights Reserved. 3

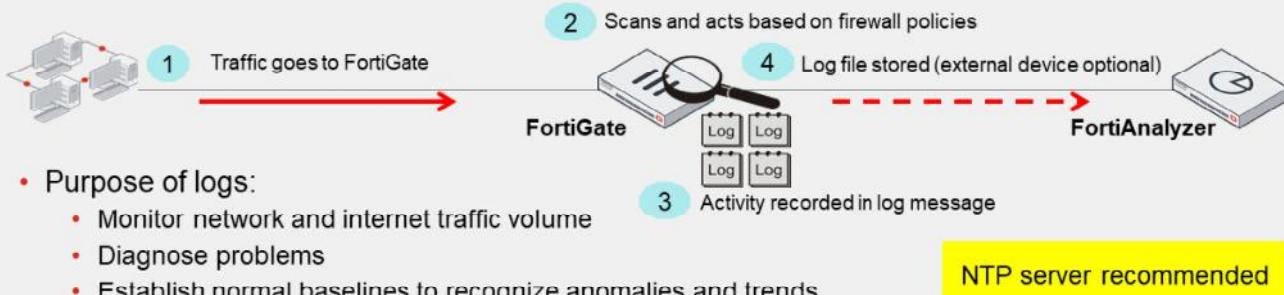
After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in the FortiGate log workflow, you will be able to record logs effectively in your network.

DO NOT REPRINT**© FORTINET**

Logging Workflow

1. Traffic passes through FortiGate to your network
2. FortiGate scans the traffic and acts based on configured firewall policies
3. FortiGate records the activity and stores the information in a log message
4. FortiGate adds the log message to a log file on a device capable of storing logs (local FortiGate device or an external device, such as FortiAnalyzer)



When traffic passes through FortiGate to your network, FortiGate scans the traffic and then acts based on the firewall policies in place. FortiGate records this activity and stores the information in a log message. The log message is stored in a log file, which is then stored on a device capable of storing logs. FortiGate can store logs locally or send them to an external storage device, such as FortiAnalyzer.

Logs help you monitor your network traffic, locate problems, establish baselines, and more. Logs give you valuable insight into your network, enabling you to adjust your network security as needed.

Some organizations have legal requirements regarding logging, so it is important to be aware of your organization's policies during configuration.

For effective logging, your FortiGate system date and time should be accurate. You can either manually set the system date and time or configure FortiGate to keep its time correct automatically by synchronizing with a Network Time Protocol (NTP) server. Fortinet recommends using an NTP server. FortiGate is used as NTP server by default.

DO NOT REPRINT**© FORTINET**

Log Types and Subtypes

- *Traffic* logs record traffic flow information, such as an HTTP/HTTPS request and its response (if any)
- *Event* logs record system and administrative events, such as adding or modifying a setting, or daemon activities
- *Security* logs record security events, such as virus attacks and intrusion attempts, based on the security profile type (log type = utm)
 - If no security logs exist, the menu item does not appear in the GUI

Traffic	Event	Security
Forward	Endpoint control	Application control
Local	High availability	Antivirus
Sniffer	System	Data loss prevention (DLP)
	User	Antispam
	Router	Web filter
	VPN	Intrusion prevention system (IPS)
	WAD	Anomaly (DoS policy)
	Wireless	Web application firewall (WAF)

WAN optimization logs are found within traffic logs

GPRS Tunneling Protocol (GTP) logs are handled separately from default event logs



FortiGate has three types of logs: traffic, event, and security. Each type is divided into subtypes.

Traffic logs record traffic flow information, such as an HTTP/HTTPS request and its response. It contains the subtypes forward, local, and sniffer:

- Forward traffic logs contain information about traffic that FortiGate either accepted or rejected according to a firewall policy.
- Local traffic logs contain information about traffic sent directly to and from the FortiGate management IP addresses. They also include connections to the GUI and FortiGuard queries.
- Sniffer logs contain information related to traffic seen by the one-arm sniffer.

Event logs record system and administrative events, such as adding or modifying a setting, or daemon activities. Event logs contain subtypes named endpoint control, high availability (HA), system, user, router, VPN, WAD, and wireless:

- System event logs contain information related to operations, such as automatic FortiGuard updates and GUI logins.
- User logs contain login and logoff events for firewall policies with user authentication.
- Router, VPN, WAD, and wireless subtypes include logs for those features. For example, VPN contains IPsec and SSL VPN log entries.

Security logs record security events, such as virus attacks and intrusion attempts. They contain log entries based on the security profile type (log type = utm), including application control, antivirus, data loss prevention (DLP), antispam (email filter), web filter, intrusion protection, anomaly (DoS policy), and web application firewall (WAF). Security logs and subtypes are visible in the GUI only if logs are created within it—if no security logs exist, the menu item does not appear.

DO NOT REPRINT**© FORTINET**

Log Severity Levels

- Each log entry includes a log level (also known as priority level) that ranges in order of importance
 - 0 = high importance / 6 = low importance

Levels	Description
0 – Emergency	System unstable
1 – Alert	Immediate action required
2 – Critical	Functionality effected
3 – Error	Error exists that can affect functionality
4 – Warning	Functionality could be affected
5 – Notification	Information about normal events
6 – Information	General system information
7 – Debug	Diagnostic information for investigating issues

Rarely used, unless actively investigating an issue with Fortinet Support



Each log entry includes a log level (or priority level) that ranges in order of importance from emergency to information.

There is also a debug level, which adds diagnostic information to an event log. The debug level is rarely used, unless you are actively investigating an issue with Fortinet Support.

Generally, the lowest log level you should use is information, but even this level generates many logs and can cause premature hard disk failure. Depending on the type of log and your organization's needs, you may want to use only notification logs or higher.

DO NOT REPRINT

© FORTINET

Log Message Layout

- Log header (similar in all logs)

- Type and subtype = Name of log file
- Level = Severity level

```
date=2025-08-07 time=07:29:09 eventtime=1754576949412373904 tz="-0700" logid="0316013056"
type="utm" subtype="webfilter" eventtype="ftgd blk" level="warning" vd="root"
```

- Log body (varies by log type)

- policyid = Firewall policy applied to session
- hostname = URL or IP of host

- srcip and dstip = Source and destination IP address
- action = Action taken by FortiGate
- msg = Reason for the action

```
policyid=1 poluid="5476b1d8-8be7-51ef-d3c8-3e0539bb2ec0" policytype="policy" sessionid=35060
srcip=10.0.11.50 srcport=46830 srccountry="Reserved" srcintf="port4" srcintfrole="undefined"
srcuuid="7bc87d34-7916-51e7-3d5b-71812a61b98e" dstip=151.101.67.5 dstport=80 dstcountry="United States"
dstintf="port2" dstintfrole="undefined" dstuuid="7bc87d34-7916-51e7-3d5b-71812a61b98e" proto=6
httpmethod="GET" services="HTTP" hostname="cnn.com" agent="Mozilla/5.0 (X11; Ubuntu; Linux x86_64;
rv:139.0) Gecko/20100101" profile="default" action="blocked" reqtype="direct" url="http://cnn.com/"
sentbyte=501 rcvbyte=0 direction="outgoing" msg="URL belongs to a denied category in policy"
ratemethod="domain" cat=36 catdesc="News and Media"
```



Every log message has a standard layout comprising two sections: a header and a body.

The header contains fields that are common to all log types, such as originating date and time, log identifier, log category, severity level, and VDOM. The value of each field is specific to the log message. In the raw log entry example shown on this slide, the log type is `utm`, the subtype is `webfilter`, and the level is `warning`. The type and subtype of logs determine which fields appear in the log body.

The body, therefore, describes the reason the log was created and the actions that FortiGate took. These fields vary by log type. In the example shown on this slide, the fields are as follows:

- The `policyid` field indicates which firewall rule matched the traffic.
- The `srcip` field indicates the source IP address.
- The `dstip` field indicates the destination IP address.
- The `hostname` field indicates the URL or IP of the host.
- The `action` field indicates what FortiGate did when it found a policy that matched the traffic.
- The `msg` field indicates the reason for the action taken. In this example, the action is `blocked`, which means that FortiGate prevented this IP packet from passing, and the reason is that it belongs to a denied category in the firewall policy.

If you log onto a third-party device, such as a syslog server, knowing the log structure is crucial to integration. For information about log structures and associated meanings, visit <http://docs.fortinet.com>.

DO NOT REPRINT

© FORTINET

Lesson Progress



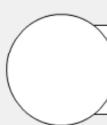
Describe the Log Workflow



Identify Log Storage Options



Register FortiGate with FortiAnalyzer



View and Search for Log Messages



© Fortinet Inc. All Rights Reserved.

8

Good job! You now understand log workflow.

Now, you will learn how to identify log storage options.

DO NOT REPRINT**© FORTINET**

Identify Log Storage Options

Objectives

- Differentiate between local logs and remote logs
- Describe FortiAnalyzer log repository
- Describe FortiAnalyzer operating modes



© Fortinet Inc. All Rights Reserved.

9

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

By demonstrating competence in the log storage options, you will be able to efficiently manage how and where to store FortiGate logs.

DO NOT REPRINT

© FORTINET

Log Storage—Local

- To store logs locally on FortiGate, you must enable disk logging

```
# config log disk setting
    set status enable
```

- If disk logging is enabled, the report daemon collects statistics used for historical FortiView from disk
 - If disk logging is disabled, FortiView logs are only available in real time
- By default, logs older than seven days are deleted from disk (configurable)

```
# config log disk setting
    set maximum-log-age <integer>
```



- FortiGate devices that have a hard drive store logs in a SQL database
- Data is extracted from the SQL database for reports



Hard drive

Performance may be impacted under heavy strain

© Fortinet Inc. All Rights Reserved. 10

Typically, mid-level to high-end FortiGate models have a hard drive. FortiGate can store logs on its hard drive, which is known as local logging or disk logging. Depending on the model series, disk logging may be enabled by default.

FortiGate can store all log types, including log archives and traffic logs, locally. Traffic logs and log archives are larger files that require a lot of room when logged by FortiGate.

Under heavy log usage, disk logging will result in a performance impact.

If you are using the local hard disk on a device for WAN optimization, you cannot also log to disk, unless your device has two separate disks. If your device has two separate disks, you can use one for WAN optimization and the other for logging. If you are using the local hard disk for WAN optimization, and only one disk is available, you can log to remote FortiAnalyzer devices or syslog servers.

If you want to store logs locally on FortiGate, you must enable disk logging on the **Log Settings** page. Only some FortiGate models support disk logging. If your FortiGate does not support disk logging, you can log to an external device instead.

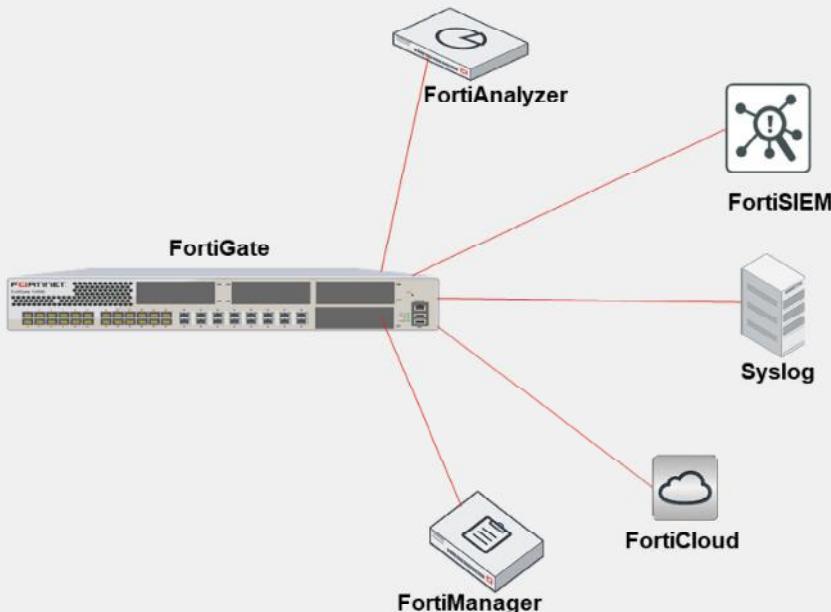
You must enable disk logging in order for information to appear on the FortiView dashboards. If disabled, logs display in real time only. You can also enable this setting using the CLI `config log disk setting` command.

By default, logs older than seven days are deleted from the disk. This value is configurable.

DO NOT REPRINT
© FORTINET

Log Storage—Remote

- Various options available for remote logging:
 - FortiAnalyzer
 - FortiSIEM
 - Syslog server
 - FortiCloud
 - FortiManager



© Fortinet Inc. All Rights Reserved. 11

You can configure FortiGate to store logs on syslog servers, FortiCloud, FortiSIEM, FortiAnalyzer, or FortiManager. These logging devices can also be used as a backup solution. Whenever possible, it is preferred to store logs externally.

Syslog is a logging server that is used as a central repository for networked devices.

FortiCloud is a Fortinet subscription-based, hosted security management and log retention service that offers long-term storage of logs with reporting. If you have a smaller network, FortiCloud is usually more feasible than buying a dedicated logging device. Note that every FortiGate offers a free tier and will keep logs for seven days. You must upgrade to the paid service to retain logs for one year.

FortiSIEM provides unified event correlation and risk management that can collect, parse, normalize, index, and store security logs.

FortiAnalyzer and FortiManager are external logging devices with which FortiGate can communicate. You can place FortiAnalyzer or FortiManager on the same network as FortiGate, or outside of it. While FortiAnalyzer and FortiManager share a common hardware and software platform and can both take log entries, FortiAnalyzer and FortiManager have different capabilities that are worth noting. The primary purpose of FortiManager is to centrally manage multiple FortiGate devices. As such, log volumes are limited to a fixed amount per day, which is less than the equivalent size of FortiAnalyzer. On the other hand, the primary purpose of FortiAnalyzer is to store and analyze logs, so the log limit is much higher (though the limit is model dependent). Note that local logging is not required for you to configure logging to FortiAnalyzer or FortiManager.

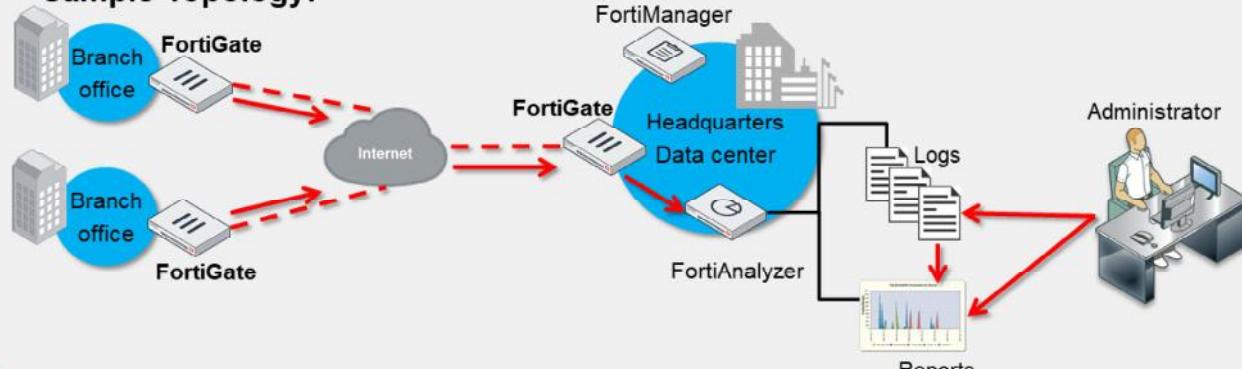
DO NOT REPRINT
© FORTINET

FortiAnalyzer Centralized Log Repository

Workflow:

1. Registered devices send logs to FortiAnalyzer
2. FortiAnalyzer buffers, reorganizes, and stores the logs
3. Administrators:
 - View and search the logs
 - Configure, request, and view reports (based on log data)

- **Sample Topology:**



© Fortinet Inc. All Rights Reserved.

12

The logging and reporting workflow operates as follows:

1. Registered devices send logs to FortiAnalyzer.
2. FortiAnalyzer collates and stores those logs in a way that makes it easy to search and run reports.
3. Administrators can connect to FortiAnalyzer using the GUI to view the logs manually or generate reports to analyze the data. You can also use the CLI to perform administrative tasks.

FortiAnalyzer can be easily integrated into a network, even with multiple sites. A sample topology can include various branches and headquarters. The firewall for each location is added to FortiAnalyzer, and the administrator can view logs and generate reports for the entire network on one interface.

DO NOT REPRINT**© FORTINET**

Storage of Incoming Logs

- FortiAnalyzer stores incoming logs in the following manner:

1. Raw format

- For long-term archive purposes
- You cannot view them in FortiView or Log View



Raw logs

2. Inserted into the database

- FortiAnalyzer inserts logs into the SQL database
- You can view the logs and run reports



FortiAnalyzer adds logs to the database



FortiAnalyzer first stores incoming logs in raw format. These are for archive purposes, and you can't view them using FortiView or Log View. Next, FortiAnalyzer inserts the logs into the SQL database. You can view these logs and run reports on them.

DO NOT REPRINT
© FORTINET

FortiAnalyzer Operating Modes—Analyzer

Dashboard > System Information

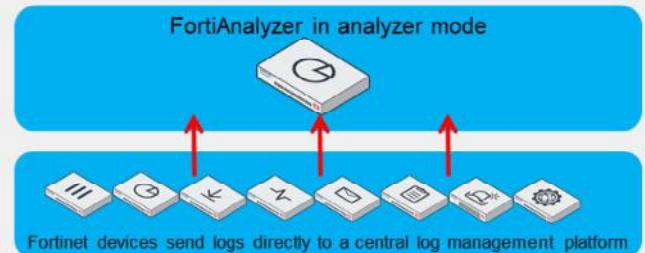
Operation Mode

Analyzer

Collector

Analyzer is the default mode

- Central log aggregator for one or more logging devices, or FortiAnalyzer in collector mode
 - Can still forward logs to another FortiAnalyzer (or syslog/CEF server)



© Fortinet Inc. All Rights Reserved.

14

FortiAnalyzer has two modes of operation: analyzer and collector. The mode of operation you choose depends on your network topology and individual requirements.

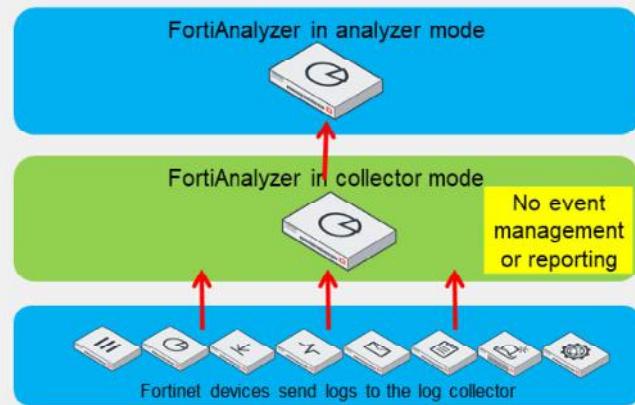
You can change the operating mode in the **System Information** widget on the dashboard.

In analyzer mode, FortiAnalyzer acts as a central log aggregator for one or more log collectors, such as a FortiAnalyzer operating in collector mode or any other supported device sending logs. Analyzer mode is the default operating mode.

DO NOT REPRINT
© FORTINET

FortiAnalyzer Operating Modes—Collector

- Collects logs from multiple devices and forwards them to FortiAnalyzer in analyzer mode
 - Can aggregate logs to another FortiAnalyzer
 - Can forward to syslog/CEF server in real-time forwarding mode only
- Not used for analytics—archiving only



When operating in collector mode, FortiAnalyzer collects logs from multiple devices. Then it forwards those logs, in their original binary format, to another device, such as a FortiAnalyzer operating in analyzer mode. Depending on the forwarding mode, it can also send them to a syslog server or a common event format (CEF) server.

A collector does not have the same feature-rich options as an analyzer because its only purpose is to collect and forward logs. It does not allow event management or reporting.

DO NOT REPRINT

© FORTINET

Lesson Progress



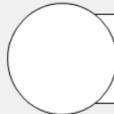
Describe the Log Workflow



Identify Log Storage Options



Register FortiGate with FortiAnalyzer



View and Search for Log Messages



© Fortinet Inc. All Rights Reserved.

16

Good job! You now understand log storage options.

Now, you will learn how to register a device on FortiAnalyzer.

DO NOT REPRINT**© FORTINET**

Register FortiGate with FortiAnalyzer

Objectives

- Describe methods of device registration
- Describe how FortiGate encrypts and transmits logs
- Identify rolling logs and auto-deleting logs



© Fortinet Inc. All Rights Reserved.

17

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

By demonstrating competence in FortiGate registration with FortiAnalyzer, you will be able to manage log devices.

DO NOT REPRINT**© FORTINET**

Methods of Device Registration

- Two device registration states:
 - Registered: authorized to store logs on FortiAnalyzer
 - Unregistered: requesting to store logs on FortiAnalyzer
- Various ways to register a device with FortiAnalyzer:
 - Initiate registration from FortiAnalyzer or from the remote device
 - Stage devices on FortiAnalyzer by prepopulating information



For FortiAnalyzer to start collecting logs from a device, that device must become a registered device on FortiAnalyzer. To FortiAnalyzer, there are only two types of devices: those that are registered and those that are unregistered. A registered device has been *authorized* to store logs on FortiAnalyzer, whereas an unregistered device is *requesting* to store logs on FortiAnalyzer.

There are various ways you can register a device with FortiAnalyzer. A supported device can send a registration request, which the FortiAnalyzer administrator can accept or deny. You can also add devices to FortiAnalyzer using the **Add Device** wizard. You can add a device based on its serial number or a pre-shared key. If the device is supported and all its details are correct, FortiAnalyzer registers the device.

DO NOT REPRINT

© FORTINET

Request From a Supported Device

1. The FortiGate administrator enables remote logging to FortiAnalyzer

2. The FortiAnalyzer administrator accepts (or rejects) the registration request
 - You can assign a new name to the device (not shown in the image)

Security Fabric > Fabric Connectors > Logging & Analytics

FortiAnalyzer		Cloud Logging
Status	<input checked="" type="radio"/> Enabled	<input type="radio"/> Disabled
Server	10.0.13.125	
Connection status	Connected	
Upload option	<input type="radio"/> Refresh <input checked="" type="radio"/> RealTime Every Minute Every 5 Minutes	
Allow access to FortiGate REST API	<input checked="" type="checkbox"/>	
Verify FortiAnalyzer certificate	<input checked="" type="checkbox"/> FAZ-VMTM24012176	

The screenshot shows the FortiAnalyzer Device Manager. At the top, there's a toolbar with buttons for 'Add Device', 'Device Group', 'Search...', 'Authorize' (which is highlighted with a red box), 'Hide', 'Delete', 'Display Hidden Devices', and 'Full Screen'. Below the toolbar is a table header with columns: 'All Logging Devices (0)', 'Unauthorized Devices (1)', 'Device Name', 'Platform', 'Serial Number', 'IP Address', 'Firmware Version', and 'Management Mode'. In the 'Unauthorized Devices' row, there's a checkbox, a link to 'HQ-NGFW...', and details: 'FortiGate-VM64...', 'FGVM02TM2401342', '10.0.13.254', 'FortiGate 7.6.build3401', and 'Logging Only'. A red box also highlights the status message '1 unauthorized device.' at the top right of the table area.

© Fortinet Inc. All Rights Reserved.

19

There are two ways to initiate a request from a FortiGate device.

In the first method, you must configure the FortiAnalyzer IP address and enable logging on FortiGate. After you click **Apply**, and if the request reaches FortiAnalyzer successfully, you must confirm the serial number of the FortiAnalyzer device if the **Verify FortiAnalyzer certificate** setting is enabled.

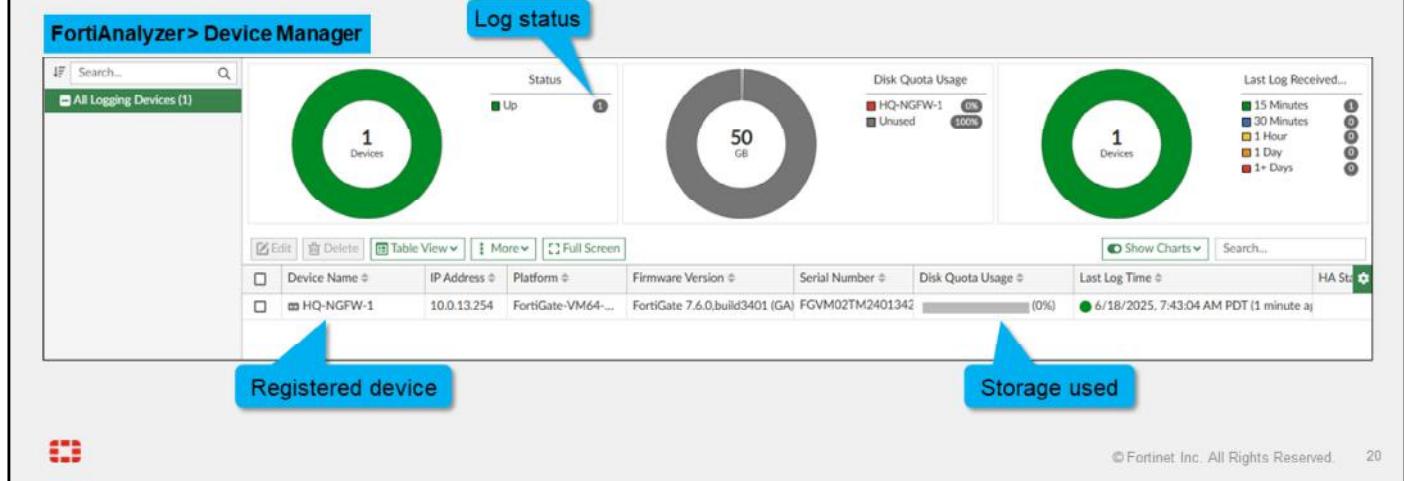
After the supported device makes the request, it automatically appears under the root ADOM in **Device Manager**. The FortiAnalyzer administrator should review the details of the unauthorized device and, if satisfied, authorize the device. Upon acceptance of the registration request. You can also assign a device name.

DO NOT REPRINT

© FORTINET

Viewing Device Status

- **Device Manager** displays:
 - All registered devices
 - Log status (up or down)
 - Storage used



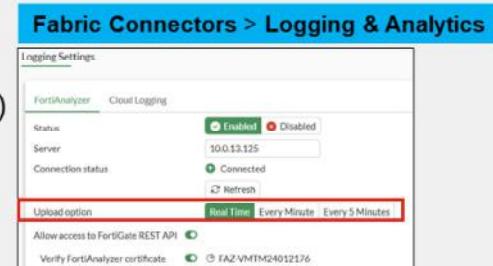
After registering a Fortinet device, you can access it on the **Device Manager** tab. Additionally, you can review details regarding log status and storage utilization.

DO NOT REPRINT

© FORTINET

Upload Option

- Near real-time uploading and consistent high-speed compression and analysis
- Configure logging options:
 - store-and-upload (CLI configuration only)
 - **Real Time**
 - **Every Minute**
 - **Every 5 Minutes** (default)



```
# configure log fortianalyzer setting
  set upload-option [store-and-upload |realtime/1-minute/5-minute]
```

store-and-upload available only on FortiGate devices that have an internal hard drive

- By default, if the FortiAnalyzer disk is full, the oldest logs are overwritten; however, you can configure FortiAnalyzer to stop logging



FortiGate allows near real-time uploading and consistent high-speed compression and analysis to FortiAnalyzer and FortiManager.

If your FortiGate model includes an internal hard drive, the `store-and-upload` option is available. This allows you to store logs on the disk and then upload them to FortiAnalyzer or FortiManager at a scheduled time (usually a low-bandwidth time). You can configure the `store-and-upload` option and a schedule on the CLI only.

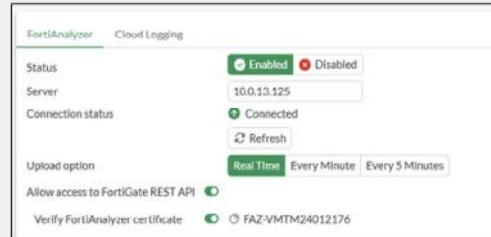
DO NOT REPRINT

© FORTINET

Log Transmission

- FortiGate uses UDP 514 for log transmission by default

```
config log fortianalyzer setting
  set status enable
  set server "10.0.13.125"
  set serial "FAZ-VMTM24012176"
  set enc-algorithm high-medium
  set upload-option realtime
end
```



- FortiGate is sending UDP 514 traffic to FortiAnalyzer

```
HQ-NGFW-1 # diagnose sniffer packet any "host 10.0.13.125" 4
Using Original Sniffing Mode
interfaces=[any]
filters=[host 10.0.13.125]
2.173071 port6 out 10.0.13.254.14974 -> 10.0.13.125.514: udp 347
3.334638 port6 out 10.0.13.254.23054 -> 10.0.13.125.514: psh 4017477514 ack 2638032500
3.335098 port6 in 10.0.13.125.514 -> 10.0.13.254.23054: psh 2638032500 ack 4017477548
3.335129 port6 out 10.0.13.254.23054 -> 10.0.13.125.514: ack 2638032543
```

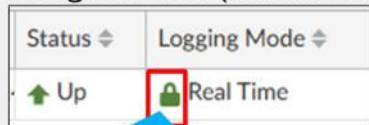


FortiGate uses UDP port 514 for log transmission by default . As shown on this slide, sniffer output on the FortiGate shows that traffic is sent to FortiAnalyzer IP address 10.0.13.125 through UDP port 514.

DO NOT REPRINT
© FORTINET

Reliable Logging and OFTPS

- Changes the log transport delivery method from UDP to TCP
- TCP provides reliable data transfer
- If you enable logging to FortiAnalyzer using the FortiAnalyzer GUI, reliable logging is autoenabled
 - If you enable logging to FortiAnalyzer using the CLI, reliable logging is not autoenabled—you must manually enable it using the CLI command shown in the screenshot below
- If using reliable logging, you can encrypt communications using SSL-secured OFTP (OFTPS)
- FortiCloud uses TCP, and you can set the encryption algorithm using the CLI (default setting is high)



Device manager shows reliable logging is enabled

```
# config log fortianalyzer setting
  set status enable
  set enc-algorithm [high-medium | high | low]
  set reliable enable
end
```

Reliable logging must be enabled to use OFTPS

Controls encryption algorithm

© Fortinet Inc. All Rights Reserved. 23

When you enable reliable logging on FortiGate, the log transport delivery method changes from UDP to TCP. TCP provides reliable data transfer, guaranteeing that the transferred data remains intact and arrives in the same order in which it was sent.

If you enable logging to FortiAnalyzer using the FortiAnalyzer GUI, reliable logging is automatically enabled. If you enable logging using the CLI, you must use the CLI command shown on this slide to enable reliable logging. If you use the FortiGate Fabric Connector to enable FortiAnalyzer logging, reliable logging is not autoenabled.

Logging to FortiCloud uses TCP, and you can set the encryption algorithm using the CLI. The default encryption setting is high.

Optionally, if using reliable logging, you can encrypt communications using SSL-encrypted OFTP traffic, so when a log message is generated, it is safely transmitted across an unsecured network. You can choose the level of SSL protection used by configuring the `enc-algorithm` setting on the CLI.

When both FortiGate and FortiAnalyzer are running version 7.2 or later, and reliable logging is configured, FortiGate keeps logs in a *confirm queue* until it verifies that FortiAnalyzer received them. This is achieved by using sequence numbers (`seq_no`) to track the logs received. FortiOS periodically queries FortiAnalyzer for the latest `seq_no` of the last log received, and clears logs from the *confirm queue* up to the `seq_no`.

DO NOT REPRINT**© FORTINET**

Logging Scope

- Depending on the size of your organization, the amount of data can vary significantly
- Balance between reducing security risks and assigning resources while adhering to regulations
 - If logging is optional for certain flows, decide whether to spend resources on it
 - Too much data can be as bad as too little
- Prioritize analysis based on
 - Source and destination
 - Type of traffic
 - Type of security event (for example, web filter or intrusion prevention)
 - Frequency
 - Time



Depending on your organization's size, the amount of log data generated can become overwhelming. Logs are usually generated continuously, and one workstation can generate a large volume of logs in a short time. As an analyst, it is not practical to review every log entry. Most logs are normal: Using resources to analyze them yields no benefits.

Not everything in the network needs to be logged. For example, if your infrastructure team plans to conduct tests on an isolated network, you can work with them to disable logging beforehand. Guest devices on a restricted network also may not need to be logged.

In your analysis, prioritize factors such as the traffic type or types, the traffic sources and destinations, and any security events associated with the traffic. In addition, if traffic is being sent at an unexpected frequency, whether you are seeing traffic more or less frequently than expected, further investigation is warranted. Knowing when your network is expected to produce traffic can also help you identify anomalous behavior, such as excessive traffic during off-hours.

You can access the latest best practices from the Fortinet document library.

DO NOT REPRINT
© FORTINET

Rolling Logs and Automatically Deleting Old Logs

- How can you better manage your logs on disk?

The screenshot shows the 'System Settings > Advanced > Device Log Settings' page. It is divided into two main sections: 'Registered Device Logs' and 'Automatically Delete'.

Registered Device Logs:

- 'Roll log file when size exceeds' is set to 200 MB (10-1000).
- 'Roll log files at scheduled time' is enabled, with a schedule set for 'Every Sunday 00:00'.
- 'Upload logs using a standard file transfer protocol' and 'Upload logs to cloud storage' are both disabled.

Automatically Delete:

- 'Device log files older than' is set to 365 days, scheduled daily at 00:00.
- 'Reports older than', 'Content archive files older than', and 'Quarantined files older than' are all set to 365 days, also scheduled daily at 00:00.

A blue callout box points to the 'Roll log file when size exceeds a set threshold' setting with the text: 'Roll log files when the size exceeds a set threshold'. Another blue callout box points to the 'Device log files older than' section with the text: 'Automatically delete logs of a specified age'.

© Fortinet Inc. All Rights Reserved. 25

Aside from changing your disk log quota, you can enforce global settings to help manage your logs.

You can:

- Specify a global log roll policy to roll or upload logs when the size exceeds a set threshold.
- Specify a global automatic deletion policy for all log files, quarantined files, reports, and content archive files on FortiAnalyzer.

All deletion policies are always active on FortiAnalyzer. Therefore, you should carefully configure each policy. For example, suppose the disk utilization policy reaches its threshold before the global automatic file deletion policy for the FortiAnalyzer device. In that case, FortiAnalyzer automatically deletes the archive logs for the affected device. Conversely, if the global automatic file deletion policy reaches its threshold first, FortiAnalyzer deletes the oldest archive logs regardless of the log storage settings associated with the device.

DO NOT REPRINT**© FORTINET**

Lesson Progress



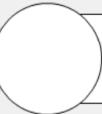
Describe the Log Workflow



Identify Log Storage Options



Register FortiGate with FortiAnalyzer



View and Search for Log Messages



© Fortinet Inc. All Rights Reserved. 26

Good job! You now understand device registration.

Now, you will learn how to view and search for log messages.

DO NOT REPRINT**© FORTINET**

View and Search for Log Messages

Objectives

- View and search for logs on FortiGate
- View and search for logs on FortiAnalyzer
- Differentiate between real-time views and historical views



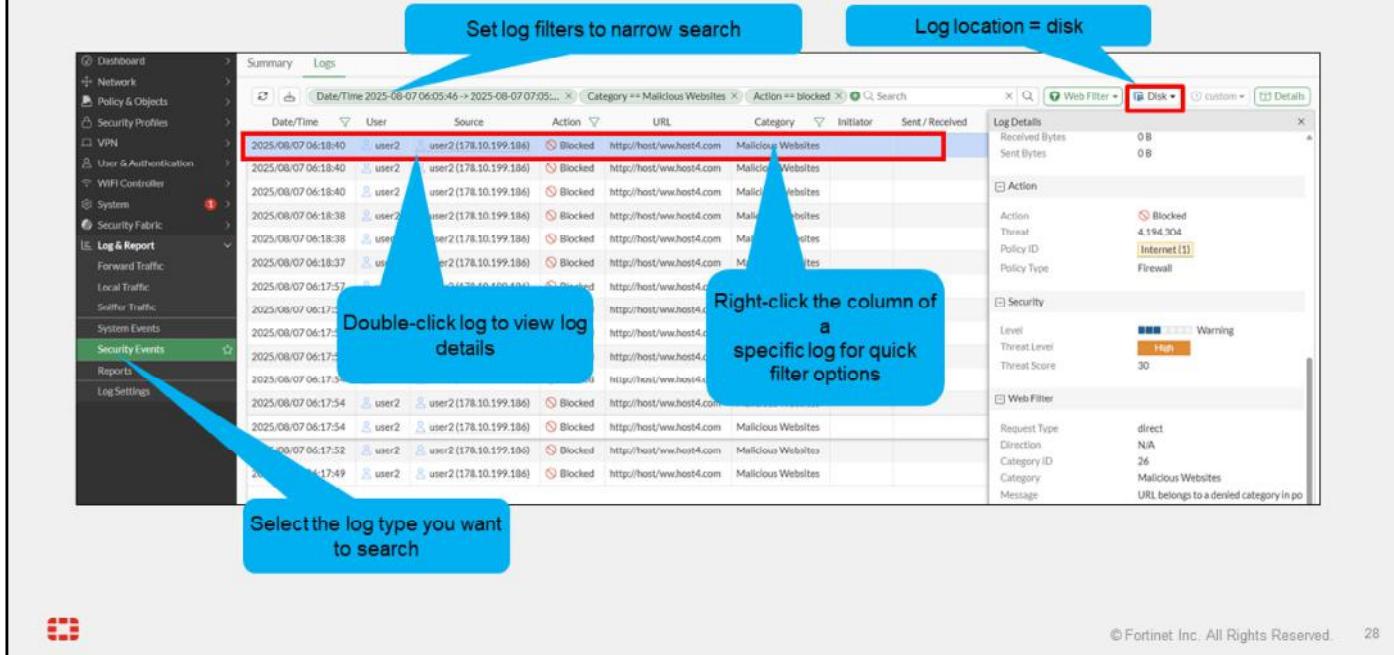
© Fortinet Inc. All Rights Reserved. 27

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

By demonstrating competence in the log view, you will be able to search logs on FortiGate and FortiAnalyzer.

DO NOT REPRINT
© FORTINET

FortiGate: Viewing and Searching Log Messages—GUI



You can access your logs on the GUI in the **Log & Report** menu.

Select the type of log you want to view, such as **Security Events**. Logs on the GUI appear in a formatted table view. The formatted view is easier to read than the raw view, and it enables you to filter information when viewing log messages. To view the log details, select the log in the table. The log details then appear in the **Log Details** section on the right side of the window.

If archiving is enabled on security profiles that support it (such as DLP), archived information appears in the **Log Details** section in the **Archived Data** section. Archived logs are also recorded when using FortiAnalyzer or FortiCloud.

If you configure FortiGate to log to multiple locations, you can change the log display location in this section. In the example shown on this slide, the log location is set to **Disk**. If you are logging to a FortiAnalyzer, you can toggle the disk location to FortiAnalyzer instead.

To navigate the logs more efficiently, you can set up log filters. The more information you specify in the filter, the easier it is to find the precise log entry. Filters are configurable for each column of log data on the display. Click the plus icon to select the filter in the drop-down list that appears. If you see data that you want to filter on in a log that is already in the table, you can right-click that data to select the quick filter option. For example, if you see a webfilter log in the table with a specific category name, right-click the name in the table, and a quick filter option opens, allowing you to filter on all logs with that category name.

By default, the most common columns are shown, and the less common columns are hidden. To add columns, right-click any column field and, in the pop-up menu that opens, select the column in the section.

DO NOT REPRINT

© FORTINET

FortiGate: Viewing Logs Associated With a Firewall Policy

- Access log messages generated by individual policies

The screenshot shows the FortiGate management interface under 'Policy & Objects > Firewall Policy'. A policy named 'port4 -> port2' is selected. A context menu is open over this policy, with the 'Show matching logs' option highlighted and a red arrow pointing to it.

Policy List:

Policy	Source	Destination	Schedule	Action	IP Pool	NAT	Type	Security Profiles	Log	Bytes
port4 -> port2	Internet (1)	all	always	ALL	✓ ACCEPT	NAT	Standard	certificate-inspection WEB default	All	1.09 GB
								no-inspection	UTM	0 B

Log Viewer:

Policy UUID == 5476b3c8-8be7-51ef-d3cb-3e05399602... | Search | Date/Time | Source | Device | Destination | Application Name | Result | Policy ID

Date/Time	Source	Device	Destination	Application Name	Result	Policy ID
2025/08/07 07:24:54	10.0.11.50		185.125.190.58 (http://ubuntu.com)	N/A	✓ Accept (76 B / 76 B)	Internet (1)
2025/08/07 07:24:42	10.0.11.53		96.45.45.45 (dns1.fortiguard.net)	DNS	✓ Accept (649 B / 2.09 kB)	Internet (1)
2025/08/07 07:24:41	10.0.11.50		142.251.33.170 (youtube.googleapis.com)	HTTPS	✓ Accept (4.42 kB / 6.07 kB)	Internet (1)
2025/08/07 07:24:30	10.0.11.53		96.45.45.45 (dns1.fortiguard.net)	DNS	✓ Accept (2.96 kB / 25.31 kB)	Internet (1)

You can also access log messages generated by individual policies. Right-click the policy for which you want to view all associated logs and, in the pop-up menu, select **Show Matching Logs**. FortiGate takes you to the **Forward Traffic** page where a filter is automatically set based on the policy universally unique identifier (UUID).

DO NOT REPRINT
© FORTINET

Viewing and Searching Log Message—CLI

Configures which log messages you will see, how many log messages you can view at one time (a maximum of 1000 lines of log messages), and the type of log messages you can view

execute log filter ← Allows you to see specific log messages that you already configured within the execute log filter command

```
HQ-NGFW-1 # execute log filter category 3
```

```
HQ-NGFW-1 # execute log display
```

```
45 logs found.  
10 logs returned.  
93.8% of logs has been searched.
```

```
1: date=2025-08-07 time=07:29:09 eventtime=1754576949412373904 tz="-0700" logid="0316013056" type="utm"  
subtype="webfilter" eventtype="ftgd_blk" level="warning" vd="root" policyid=1 poluid="5476b1d8-8be7-51ef-d3c8-  
3e0539bb2ec0" policytype="policy" sessionid=35060 srcip=10.0.11.50 srcport=46830 srccountry="Reserved"  
srcintf="port4" srcintfrole="undefined" srcuaid="7bc87d34-7916-51e7-3d5b-71812a61b98e" dstip=151.101.67.5 dstport=80  
dstcountry="United States" dstintf="port2" dstintfrole="undefined" dstuaid="7bc87d34-7916-51e7-3d5b-71812a61b98e"  
proto=httpmethod="GET" service="HTTP" hostname="cnn.com" agent="Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:139.0)  
Gecko/20100101" profile="default" action="blocked" reqtype="direct" url="http://cnn.com/" sentbyte=501 rcvbyte=0  
direction="outgoing" msg="URL belongs to a denied category in policy" ratemethod="domain" cat=36 catdesc="News and  
Media"
```



You are not restricted to the GUI for viewing log messages. You can also view log messages on the CLI, using the execute log display command. This command allows you to see specific log messages that you already configured within the execute log filter command. The execute log filter command configures which log messages you will see, how many log messages you can view at one time (a maximum of 1000 lines of log messages), and the type of log messages you can view.

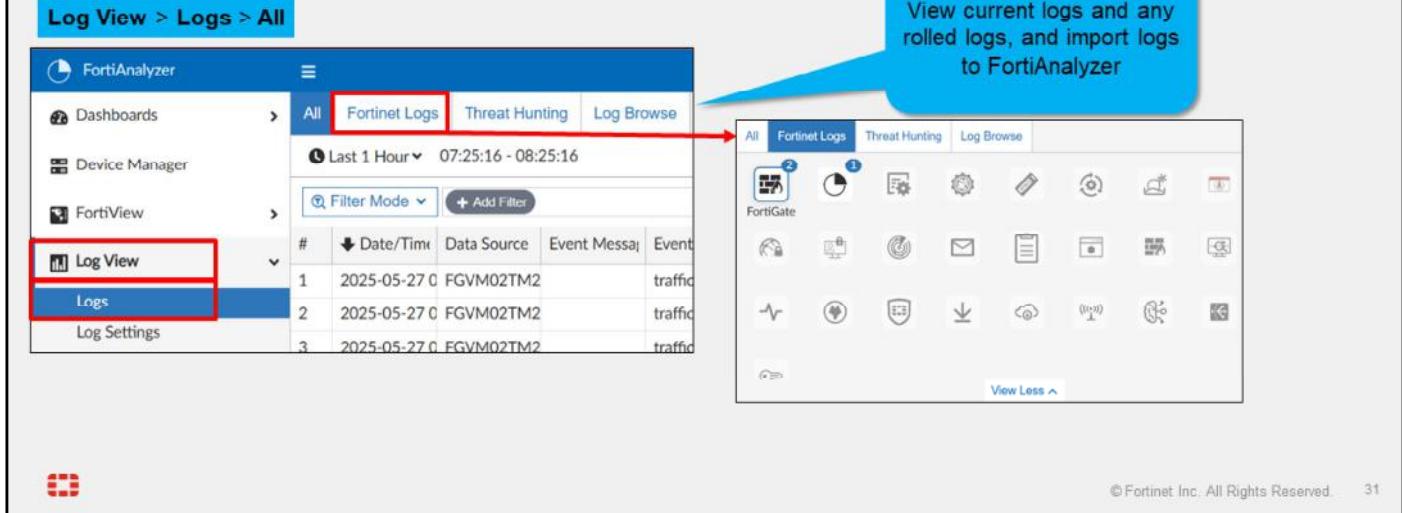
Logs appear in the raw format view, which displays them as they appear within the log file.

Like the GUI, if you have configured either a syslog or security information and event management (SIEM) server, you will not be able to view log messages on the CLI.

DO NOT REPRINT
© FORTINET

Log View—FortiAnalyzer

- View all logs received for each FortiGate
- You can choose to view only specific devices, Fortinet logs, log browse, log groups



The screenshot shows the FortiAnalyzer interface with the following details:

- Top Navigation:** Log View > Logs > All
- Sidebar:** Dashboards, Device Manager, FortiView, Log View (highlighted with a red box), and Logs (highlighted with a blue box).
- Main Content:**
 - Log Types:** All, Fortinet Logs, Threat Hunting, Log Browse (highlighted with a red box).
 - Time Range:** Last 1 Hour (07:25:16 - 08:25:16).
 - Filter Mode:** Filter Mode (dropdown) and Add Filter (button).
 - Table Headers:** #, Date/Time, Data Source, Event Message, Event Type.
 - Table Data:**

#	Date/Time	Data Source	Event Message	Event Type
1	2025-05-27 07:25:16	FGVM02TM2	traffic	traffic
2	2025-05-27 07:25:16	FGVM02TM2	traffic	traffic
3	2025-05-27 07:25:16	FGVM02TM2	traffic	traffic
- Bottom Right:** A callout bubble states: "View current logs and any rolled logs, and import logs to FortiAnalyzer".
- Bottom Left:** A small red icon.
- Bottom Right:** © Fortinet Inc. All Rights Reserved. 31

The log view allows you to view all log types, in normalized logs format, being received by FortiAnalyzer.

You can choose to view logs from specific devices, Fabric groups, or log groups. A log group is a group of devices placed together in a single logical object. Log groups are virtual, so they don't have SQL databases or occupy additional disk space. You can view logs generated by FortiAnalyzer, the current log files, and any rolled log files. You can also import logs from other FortiAnalyzer devices.

DO NOT REPRINT
© FORTINET

Viewing FortiGate Logs on FortiAnalyzer

- View three different types of FortiGate logs: traffic, security, and event
- Security and event logs offer a summary dashboard

#	Date/Time	Device ID	Action	Source	Destination IP	Service	Application	Sent/Received	Security Event List
1	2025-05-27 1	FGVM02TM2401: ✓		10.0.11.253	96.45.45.45	DNS	DNS	649.0 B/2.2 KB	
2	2025-05-27 1	FGVM02TM2401: ✓		10.0.11.253	96.45.45.45	DNS	DNS	649.0 B/2.2 KB	
3	2025-05-27 1	FGVM02TM2401: ✓		168.10.199.186	224.141.85.77	other	other	0 B/0 B	
4	2025-05-27 1	FGVM02TM2401: ⚡ Deny:UTM		178.10.199.186	224.141.85.77	HTTP	HTTP	900.0 B/2.8 KB	
5	2025-05-27 1	FGVM02TM2401: ⚡ Deny:UTM		178.10.199.186	224.141.85.77	HTTP	HTTP	3.2 KB/1.3 KB	HTTP 1
8	2025-05-27 1	FGVM02TM2401: ⚡ Deny:UTM		178.10.199.186	224.141.85.77	HTTP	HTTP	1.8 KB/7.5 KB	EMAIL 1
9	2025-05-27 1	FGVM02TM2401: ✓		177.10.199.186	224.141.85.77	HTTP	Vimeo_Video.Play	1.4 KB/11.6 KB	APP 1
10	2025-05-27 1	FGVM02TM2401: ✓		175.10.199.186	224.141.85.77	HTTP	Dropbox_File.Upload	2.7 KB/3.4 KB	APP 1

© Fortinet Inc. All Rights Reserved. 32

Traffic logs allow you to view the traffic traversing the firewalls, including details such as source, destination, service, action (whether the traffic is allowed), and more. Security logs allow you to view logs related to unified threat management (UTM) inspection. Event logs are generally related to firewall system operations.

You can select the security or event log subtype you want to see or access a summary dashboard for an overview.

DO NOT REPRINT
© FORTINET

Viewing FortiGate Logs on FortiAnalyzer (Contd)

- View a summary of security logs or event logs to investigate

The screenshot displays two side-by-side summary dashboards on the FortiAnalyzer interface:

- Left Dashboard (Security: Summary):**
 - Widgets: AntiVirus and SSL.
 - AntiVirus Widget Data:

Top Virus/Botnet	Action	Count
9238	monitored	17933
8448	passthrough	8967
virus_test3	passthrough	8967
 - SSL Widget Data:

Top Category	Action	Count
SSL connection is blocked due to	blocked	8966
Logid_62305	blocked	4
Logid_62307	info	3
- Right Dashboard (Event: Summary):**
 - Widgets: Total Events, System Events, and User Events.
 - Total Events Chart (Y-axis 0-5000, X-axis 2025/02/26-2025/05/22):
 - System Events Table:

Event Name	Level	Count
System performance statistics	notice	3344
GUI FortiGuard resource prefetch	information	861
FortiGate update succeeded	notice	552
Test	warning	394
 - User Events Table:

Event Name	Level	Count
FSSO authentication successful	notice	788
FSSO authentication failed	notice	788
Authentication lockout	warning	394
FSSO log off authentication status	notice	394

A blue callout bubble points to the left dashboard with the text: "Click any entry to drill down for more details".

© Fortinet Inc. All Rights Reserved. 33

You can monitor all enabled security and event log types from their respective summary dashboards. Summary dashboards use multiple widgets to display the top logs for each subtype. You can add or remove widgets as needed.

The time filter set at the dashboard level affects the information included on all widgets simultaneously, so you must ensure that it is set correctly.

You can click the links in provided in summary dashboards to go to specific logs. Doing so takes you to the specific log subtype section with the appropriate filters applied to search for the specific log entries.

DO NOT REPRINT

© FORTINET

Real Time vs. Historical Log Views

- View historical logs with the option to specify a time period
- By default, historical logs are displayed
- When viewing logs in real time, you can pause the view to get a more detailed view of the logs

Log View > Logs > Fortinet Logs							
Traffic	Security	Event	FortiSwitch				
All Devices							
#	Date/Time	Device ID	Action	Source	Destination IP	Service	Application
24	2025-05-28 0 FGVM02TM2401:	✓	user2(177.10.199.1	224.141.85.77	HTTP	Vimeo_Video	
25	2025-05-28 0 FGVM02TM2401:	✓	175.10.199.186	224.141.85.77	HTTP	Dropbox_File	
26	2025-05-28 0 FGVM02TM2401:	✓	user3(175.10.199.1	224.141.85.77	HTTP	Dropbox_File_Upload	0 B/0 B
27	2025-05-28 0 FGVM02TM2401:	✓	173.10.199.186	224.141.85.77	HTTP	Dropbox_File_Download	1.5 KB/6.3 KB
28	2025-05-28 0 FGVM02TM2401:	✓	user2(173.10.199.1	224.141.85.77	HTTP	Dropbox_File_Download	0 B/0 B
29	2025-05-28 0 FGVM02TM2401:	✓	171.10.199.186	224.141.85.77	HTTP	Dropbox_File_Download	281.0 B/9.2 KB
30	2025-05-28 0 FGVM02TM2401:	✓	user5(171.10.199.1	224.141.85.77	HTTP	Dropbox_File_Download	0 B/0 B
31	2025-05-28 0 FGVM02TM2401:	✓	169.10.199.186	224.141.85.77	HTTP	Dropbox_File_Download	158.0 B/4.3 KB
32	2025-05-28 0 FGVM02TM2401:	✓	user2(169.10.199.1	224.141.85.77	HTTP	Dropbox_File_Download	0 B/0 B
33	2025-05-28 0 FGVM02TM2401:	✓	10.0.13.130	208.91.112.63	NTP		141.0 KB/141.0...
34	2025-05-28 0 FGVM02TM2401:	✓	178.10.199.186	224.141.85.77	HTTP		2.7 KB/13.2 KB
35	2025-05-28 0 FGVM02TM2401:	✓	user5(178.10.199.1	224.141.85.77			0 B/0 B



© Fortinet Inc. All Rights Reserved. 34

You can view historical logs with the option to specify a time period. By default, historical logs are displayed. You must be using the historical log view to use the custom view or chart builder features.

You can switch from viewing historical logs to viewing logs in real time. When viewing logs in real time, you can pause the view to get a more detailed view of the logs.

DO NOT REPRINT**© FORTINET**

Knowledge Check

1. In which operating mode does FortiAnalyzer use analytics logs?
 A. Analyzer
 B. Collector

2. Which protocol does FortiGate use to send encrypted logs to FortiAnalyzer?
 A. OFTPS
 B. SSL

3. If you enable reliable logging, which transport protocol will FortiGate use?
 A. UDP
 B. TCP



DO NOT REPRINT**© FORTINET**

Lesson Progress

**Describe the Log Workflow****Identify Log Storage Options****Register FortiGate with FortiAnalyzer****View and Search for Log Messages**

Congratulations! You have completed this lesson.

Now, you will review the objectives that you covered in this lesson.

DO NOT REPRINT**© FORTINET**

Review

- ✓ Describe how traffic passes through FortiGate
- ✓ Identify various log types and subtypes
- ✓ Describe log severity levels
- ✓ Differentiate between local logs and remote logs
- ✓ Describe FortiAnalyzer log repository
- ✓ Describe FortiAnalyzer operating modes
- ✓ View and search for logs on FortiGate and FortiAnalyzer



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

By mastering the objectives covered in this lesson, you learned how to manage logs on both FortiGate and FortiAnalyzer.

DO NOT REPRINT**© FORTINET**

FortiOS Administrator

Firewall Policies and NAT

The logo for FortiOS 7.6, consisting of a small red square icon followed by the text "FortiOS 7.6".

Last Modified: 6 October 2025

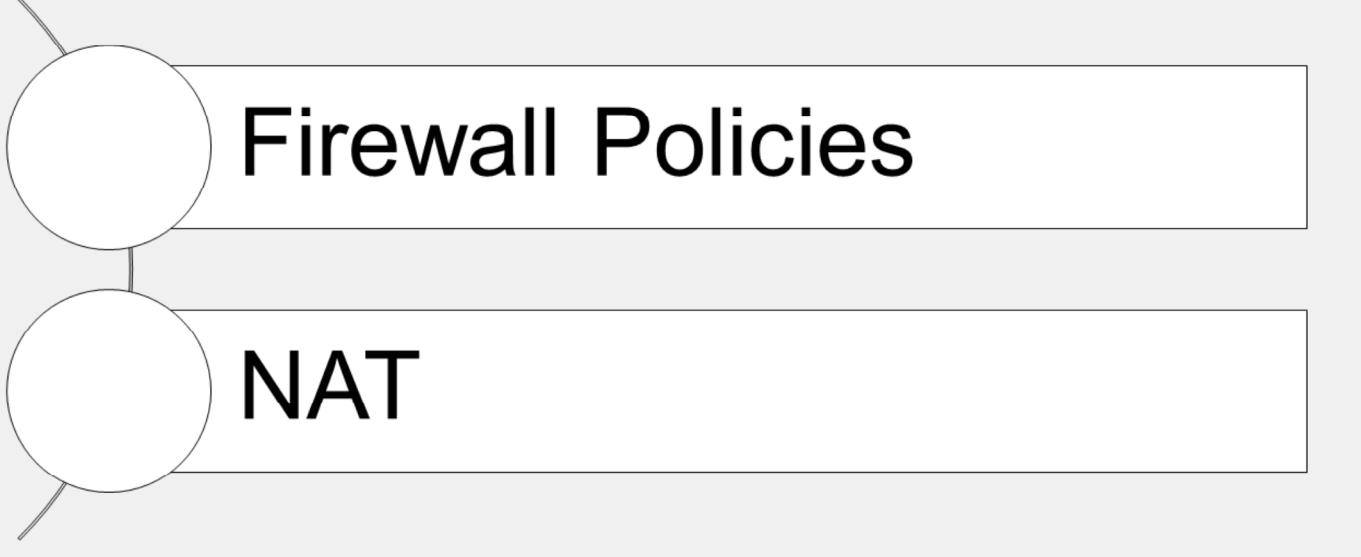
© Fortinet Inc. All Rights Reserved. 1

In this lesson, you will learn about firewall policies and how to apply them to allow and deny traffic passing through FortiGate. At its core, FortiGate is a firewall, so almost everything that it does to your traffic is linked to your firewall policies. You will also learn how to configure network address translation (NAT) and use it to implement source NAT (SNAT) and destination NAT (DNAT) for traffic passing through FortiGate.

DO NOT REPRINT

© FORTINET

Lesson Overview



Firewall Policies



NAT

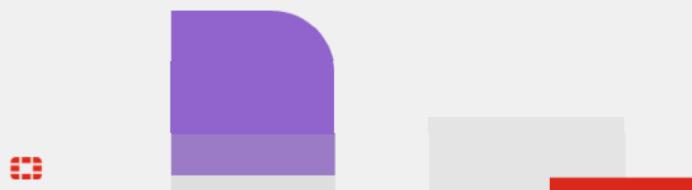
In this lesson, you will learn about the topics shown on this slide.

DO NOT REPRINT**© FORTINET**

Firewall Policies

Objectives

- Configure IPv4 firewall policies
- Monitor traffic logs from firewall policies
- Choose inspection modes for firewall policies

A decorative graphic in the bottom right corner of the slide features a purple rounded square shape above a smaller grey rectangle, which is itself above a small red horizontal bar.

© Fortinet Inc. All Rights Reserved. 3

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

By demonstrating competence in identifying the different components of firewall policies, and recognizing how FortiGate matches traffic with firewall policies and takes appropriate action, you will have a better understanding of how firewall policies interact with network traffic.

DO NOT REPRINT

© FORTINET

What Are Firewall Policies?

- Policies define:
 - Which traffic matches them
 - How to process matching traffic
- When a new IP session packet arrives, FortiGate:
 - Starts at the top of the list to look for a policy match
 - Applies the first matching policy
- Implicit Deny**
 - No matching policy? FortiGate drops packet

Policy	ID	Source	Destination	Schedule	Service	Action	NAT	Type	Security Profiles	Log
LAN (port1) → port1	1	all	all	always	ALL	✓ ACCEPT	NAT	Standard	deep-inspection AV default WIB default	UTM
LAN (port3) → port2	2	all	all	always	ALL	✓ ACCEPT	NAT	Standard	deep-inspection AV default WIB default	UTM
Implicit	0	all	all	always	ALL	✗ DENY				Disabled

Implicit Deny

© Fortinet Inc. All Rights Reserved. 4

To begin, you will learn what firewall policies are.

Any traffic passing through a FortiGate must be associated with a firewall policy. A policy is a set of instructions that controls traffic flow through the FortiGate. These instructions determine where the traffic goes, how it's handled, and whether it's allowed to pass through the FortiGate. In summary, firewall policies are sets of rules that specify which traffic is allowed through the FortiGate and what FortiGate should do when traffic matches a policy.

Should the traffic be allowed? FortiGate bases this decision on simple criteria. FortiGate analyzes the source of the traffic, the destination IP address, and the service. If the policy does not block the traffic, FortiGate begins a more computationally expensive security profile inspection—often known as unified threat management (utm)—such as antivirus, application control, and web filtering, if you've chosen it in the policy. These inspections block the traffic if there is a security risk, for example, if the traffic contains a virus. Otherwise, the traffic is allowed.

Will NAT be applied? Is authentication required? Firewall policies also determine the answers to these questions. After processing is finished, FortiGate forwards the packet toward its destination.

FortiGate looks for the matching firewall policy from *top-to-bottom* and, if a match is found, the traffic is processed based on the firewall policy. If no match is found, the traffic is dropped by the default implicit deny firewall policy.

DO NOT REPRINT
© FORTINET

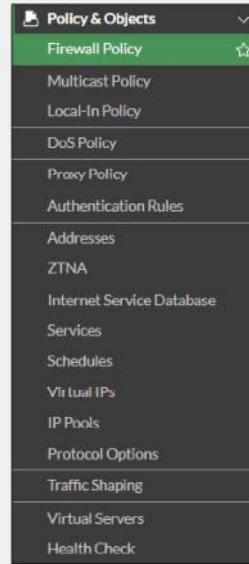
Components and Policy Types

Objects used by policies

- Interface and zone
- Address, user, and internet service objects
- Service definitions
- Schedules
- NAT rules
- Security profiles

Policy types

- Firewall Policy (IPv4, IPv6)
- Firewall Virtual Wire Pair Policy (IPv4, IPv6)
- Proxy Policy
- Multicast Policy (IPv4, IPv6)
- Local-in Policy
- DoS Policy (IPv4, IPv6)
- Traffic Shaping



© Fortinet Inc. All Rights Reserved.

5

Each policy matches traffic and applies security by referring to the objects that you've defined, such as addresses and profiles.

Common policy types are:

- Firewall policy: A firewall policy consists of set of rules that control traffic flow through FortiGate.
- Firewall virtual wire pair policy: A virtual wire pair policy is used to control the traffic between the interfaces in a virtual wire pair.
- Multicast Policy: A multicast policy allows multicast packets to pass from one interface to another.
- Local-In Policy: A local-in policy controls the traffic to a FortiGate interface and can be used to restrict administrative access.
- DoS Policy: A denial-of-service (DoS) policy checks for the anomalous patterns in the network traffic that arrives at a FortiGate interface.

By default, only **Firewall Policy** is visible under **Policy and Object**. Other policies are available based on the interface configurations and advanced features enabled through **Feature Visibility**.

In this lesson, you will learn about IPv4 firewall policies, because they are the most commonly used policies.

DO NOT REPRINT

© FORTINET

Configuring Firewall Policies

- Mandatory policy name when creating on GUI
 - Can relax the requirement by enabling **Allow Unnamed Policies**



- Flat GUI view allows:
 - Select by clicking
 - Drag-and-drop

```
config firewall policy
edit 1
set name "Training"
set uid 2204966e-47f7-51..
```

Universally unique identifier (UUID)

The screenshot shows the 'Firewall > Policy' configuration screen. The 'Name' field is highlighted with a red box and a callout 'Enabled by default Must specify unique name'. The 'Source' field contains 'HQ_SUBNET', also highlighted with a red box. A callout 'Highlights selected entry' points to the 'HQ_SUBNET' entry in the 'Select Entries' dropdown list, which is also highlighted with a red box.

© Fortinet Inc. All Rights Reserved.

6

By default, when you configure a new firewall policy using the GUI, you must specify a unique name for the policy. You will not be able to save the policy without entering something in the **Name** field. This is a best practice to help the administrators quickly identify the purposes of the policies.

By contrast, if you configure a new firewall policy using the CLI, the `name` field is optional and you are allowed to save the new policy without giving it a name. However, if you then edit that policy, the GUI requires you to add a name before you can save your changes.

You can turn off this GUI enforcement by enabling **Allow Unnamed Policies** on the **Feature Visibility** page. Enabling this feature makes the **Name** field optional on the GUI.

You can select an **Internet Service** as the source. **Internet Service** is a combination of one or more addresses and one or more services associated with a service found on the internet, such as an update service for software.

You can configure many other options in the firewall policy, such as firewall and network options, security profiles, logging options, and enabling or disabling a policy.

When creating firewall objects or policies, a UUID attribute is added so that logs can record these UUIDs and improve functionality when integrating with FortiManager or FortiAnalyzer.

When creating firewall policies, remember that FortiGate is a stateful firewall. As a result, you must create only one firewall policy that matches the direction of the traffic that initiates the session. FortiGate automatically remembers the source-destination pair and allows replies.

DO NOT REPRINT
© FORTINET

How Are Policy Matches Determined?

Incoming and outgoing interfaces	✓
Source: IP address, user, internet services	✓
Destination: IP address or internet services	✓
Services	✓
Schedules	✓

Policy & Objects > Firewall Policy

Name: Full Access
 Schedule: always
 Action: ✓ ACCEPT (DENY)
 Incoming interface: port2
 Outgoing interface: port4
 Source & Destination: Hide logic

Source: HQ-PC-1, BR1-PC-1
 User/group: guest, user1
 Destination: REMOTE_ETH2, REMOTE_BR1_SUBNET
 Service: HTTP, HTTPS, DNS

Action = **ACCEPT** or **DENY**

The diagram illustrates the flow of traffic from a cloud source through a FortiGate device. The device applies a security profile, which includes authentication, logging, and a shield icon representing a firewall policy. The shield icon indicates that the device is evaluating the traffic against a configured policy to determine if it should be accepted or denied.

© Fortinet Inc. All Rights Reserved.

7

When a packet arrives, how does FortiGate find a matching policy? Each policy has match criteria, which you can define using the following objects:

- **Incoming Interface**
- **Outgoing Interface**
- **Source**: IP address, user, internet services
- **Destination**: IP address or internet services
- **Schedule**: specific times to apply policy
- **Service**: IP protocol and port number

If the traffic matches a firewall policy, FortiGate applies the action configured in the firewall policy:

- If the **Action** is set to **DENY**, FortiGate drops the session.
- If the **Action** is set to **ACCEPT**, FortiGate allows the session and applies other configured settings for packet processing, such as user authentication, SNAT, antivirus scanning, web filtering, and so on.

When FortiGate receives traffic, it evaluates the packet source IP address, destination IP address, and the requested service (protocol and port number). It also checks the incoming interface and the outgoing interface it needs to use. Based on this information, FortiGate identifies the firewall policy and evaluates the traffic. If the traffic matches the policy, then FortiGate applies the action (accept/deny) defined in the policy.

For example, to block incoming FTP traffic to all but a few FTP servers, define the addresses of the FTP servers as the destination, and select FTP as the service. You probably *wouldn't* specify a source (often any location on the internet is allowed) or schedule (FTP servers are usually always available, day or night). Finally, set the **Action** setting to **ACCEPT**.

FortiOS 7.6 Administrator Study Guide

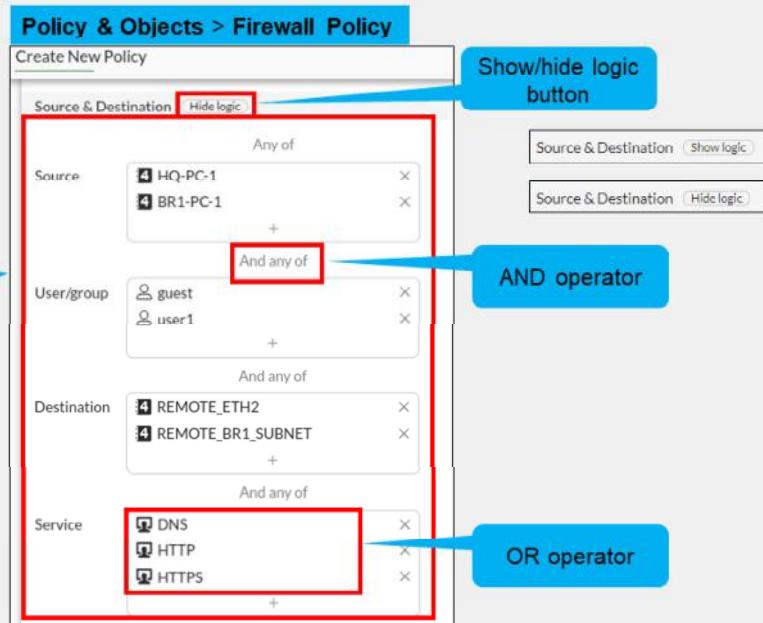
74

DO NOT REPRINT
© FORTINET

Example—Logical Operations for Firewall Policies

- Source and destination logic

Traffic must match all criteria to apply the policy



© Fortinet Inc. All Rights Reserved.

8

In the example shown on this slide, you can see the option to apply logical AND operations among various policy objects within the GUI.

The **Show Logic** button is available. Click **Show Logic** to display the labels **Any of** and **And any of** to clarify how the objects are used to match traffic. The **And any of** label indicates a logical AND relationship between the objects.

In the **Source & Destination** section, you will see how mandatory and optional fields interact based on the following configurations:

- Source:** Windows-Client or Mac-Clients
- User/group:** LDAP-Administrator, LDAP-Finance, or LDAP-Sales
- Destination:** Webserver1 or Webserver2
- Service:** DNS, HTTP, or HTTPS

Traffic must match all criteria above to apply the policy.

DO NOT REPRINT
© FORTINET

Selecting Multiple Interfaces or Any Interface

- Disabled by default
 - Cannot select multiple interfaces or any interface in firewall policy on the GUI
- Can be made visible in the GUI

The screenshot illustrates the configuration of a firewall policy across three panels:

- Top Panel (System > Feature Visibility):** Shows the "Multiple Interface Policies" checkbox being checked. A red arrow points down to the "Policy & Objects > Firewall Policy" screen.
- Middle Panel (Policy & Objects > Firewall Policy):** Shows a policy named "Single_interface" with "port4" selected for both incoming and outgoing interfaces. A blue callout bubble says "Multiple interface policies disabled".
- Bottom Panel (Policy & Objects > Firewall Policy):** Shows a policy named "Multiple_interfaces" with "port7" and "port8" selected for incoming interfaces, and "any" selected for the outgoing interface. A blue callout bubble says "Multiple interface policies enabled".

By default, you can select only a single interface as the incoming interface and a single interface as the outgoing interface. This is because the option to select multiple interfaces, or **any** interface in a firewall policy, is disabled on the GUI. However, you can enable the **Multiple Interface Policies** option on the **Feature Visibility** page to disable the single interface restriction.

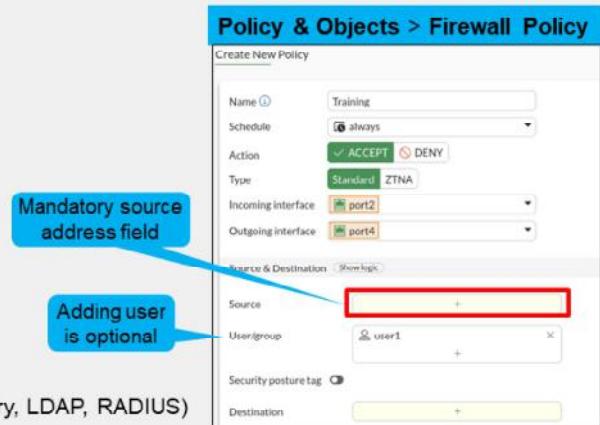
You can also specify multiple interfaces, or use the **any** option, if you configure a firewall policy on the CLI, regardless of the default GUI setting.

It is also worth mentioning that when you choose the **any** interface option, you cannot select multiple interfaces for that interface. In the example shown on this slide, because **any** is selected as the outgoing interface, you cannot add any additional interfaces, because **any** interface implies that all interfaces have already been selected.

DO NOT REPRINT
© FORTINET

Matching by Source

- Must specify at least one source (ISDB)
 - IP address or range
 - Subnet (IP/netmask)
 - FQDN
 - Geography
 - Dynamic
 - Fabric connector address
 - MAC address range
- May specify:
 - Source user—individual user or user group
 - This may refer to:
 - Local firewall accounts
 - Accounts on a remote server (for example, Active Directory, LDAP, RADIUS)
 - FSSO
 - Personal certificate (PKI-authenticated) users
- ISDB and geography are valid with a valid support contract



© Fortinet Inc. All Rights Reserved. 10

The next match criteria that FortiGate considers is the packet's source.

In each firewall policy, you *must* select a source address object. Optionally, you can refine your definition of the source address by *also* selecting a user, or a user group, which provides a much more granular match, for increased security. You can also select ISDB objects as the source in the firewall policy, which you will learn about later in this lesson.

When selecting a FQDN as the source address, it must be resolved by DNS and cached in FortiGate. Make sure FortiGate is configured properly for DNS settings. If FortiGate is not able to resolve an FQDN address, it will present a warning message, and a firewall policy configured with that FQDN may not function properly.

FortiGate devices with valid FortiCare support contract receive up-to-date information to use the internet services database (ISDB) and geography database and use them as firewall objects.

DO NOT REPRINT**© FORTINET**

Geographic-Based ISDB

- By default, ISDB updates are enabled
- Allows users to define ISDB objects based on a country, region, and city
- Objects can be used in firewall policies for more granular control over the location of the parent ISDB object

The screenshot shows the 'Edit Internet Service' configuration page. On the left, there's a form with fields: Name (Training-Location-ISDB), Type (Predefined, Geographic Based selected), Primary Internet Service (Google-Other), Country/Region (United States), Region (California), and City (Sunnyvale). On the right, details for the primary service are shown: Primary Internet Service Name (Google-Other), Primary Internet Service ID (65536), Direction (Both), and Entries (with a 'View/Edit Entries' button).



Geographic-based internet service database (ISDB) objects allow users to define a country, region, and city. These objects can be used in firewall policies for more granular control over the location of the parent ISDB object.

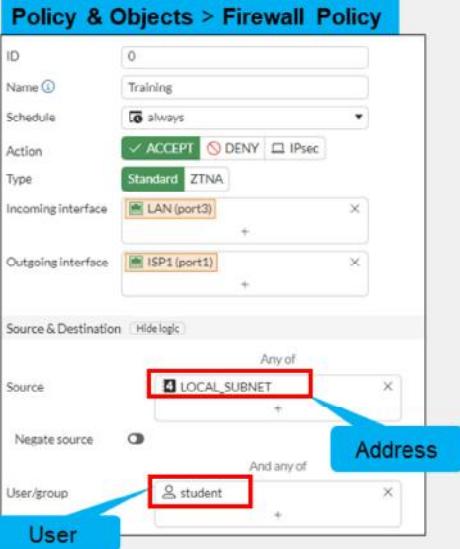
ISDB objects are referenced in policies by name, instead of by ID.

DO NOT REPRINT

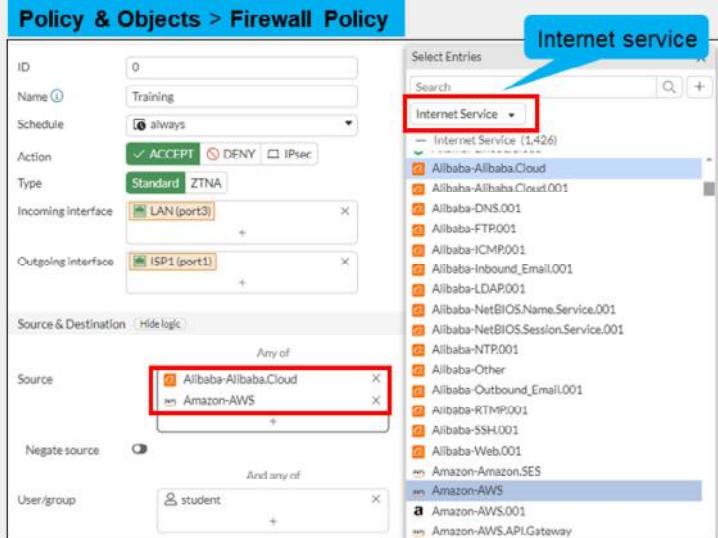
© FORTINET

Example—Matching Policy by Source

- Matches by source address, user



- Source as ISDB objects



In the example shown on this slide, source selectors identify the specific subnet and user group. Remember, user is an optional object. The user object is used here to make the policy more specific. If you wanted the policy to match more traffic, you would leave the user object undefined.

You can also use ISDB objects as a source in the firewall policy. There is an either/or relationship between ISDB objects and source address objects in firewall policies. This means that you can select either a source address or an internet service, but not both.

DO NOT REPRINT**© FORTINET**

Matching by Destination

Like source, destination criteria can use:

- Address objects:
 - Subnet (IP or netmask)
 - IP address or address range
 - FQDN
 - DNS query used to resolve FQDN
 - Geography
 - Country defines addresses by ISP geographical location
 - Database updated periodically through FortiGuard
 - Dynamic
 - Fabric connector address
- ISDB objects



Like the packet's source, FortiGate also checks the destination address for a match.

You can use address objects or ISDB objects as destinations in the firewall policy. The address object may be a host name, IP subnet, or range. If you enter an FQDN as the address object, make sure that you've configured your FortiGate device with DNS servers. FortiGate uses DNS to resolve those FQDN host names to IP addresses, that appear in the IP header.

You can also choose geographic addresses, which are groups or ranges of addresses that are assigned to a country. FortiGuard is used to update these objects.

Why is there is no option to select a user? The user identification is determined at the ingress interface, and packets are forwarded only to the egress interface after the user is successfully authenticated.

DO NOT REPRINT
© FORTINET

Security Profiles

- Firewall policies limit access to configured networks
- Security profiles configured in firewall policies protect your network by:
 - Blocking threats
 - Controlling access to certain applications and URLs
 - Preventing specific data from leaving your network

Profile Type	Status	Default Profile
AntiVirus	AV	default
Web filter	WFR	default
DNS filter	DNS	default
Application control	ADD	default
IPS	IPS	default
File filter	FILE	default
SSL inspection	SSL	no-inspection



One of the most important features that a firewall policy can apply is security profiles, such as IPS and antivirus. A security profile inspects each packet in the traffic flow, where the session has already been conditionally accepted by the firewall policy.

When inspecting traffic, FortiGate can use one of two methods: flow-based inspection or proxy-based inspection. Different security features are supported by each inspection type.

Note that by default, the **Video Filter**, **VOIP**, **Web Application Firewall**, **Virtual Patching** and **Inline-CASB** security profile options are not visible on the policy page on the GUI. You need to enable them on the **Feature Visibility** page.

DO NOT REPRINT

© FORTINET

Policy ID

- Firewall policies are ordered primarily on a top-down basis
- Policy IDs are identifiers:
 - The system assigns a policy ID when the rule is created
 - The ID number never changes as rules move higher or lower in the sequence

```
config firewall policy
  edit <policy_id>
end
```

The screenshot shows the 'Policy & Objects > Firewall Policy' interface. A table lists several firewall policies. The first two rows are highlighted with yellow boxes. The first row has a policy named 'LAN (port3) → DMZ (port2)' with ID 1, and the second row has a policy named 'LAN (port3) → ISP (port1)' with ID 2. A callout bubble points to these rows with the text 'Unified policy name and ID column'. The third row has a policy named 'Block FTP (1)' with ID 1, and the fourth row has a policy named 'Full_Access (3)' with ID 3. A red box highlights the 'ID' column header. Another red box highlights the 'Policy' column header. To the right of the table, a code snippet shows how a policy rule is configured in the CLI:

```
config firewall policy
  edit 2
    set name "DMZ"
  ...
  next
  edit 1
    set name "Block FTP"
```

© Fortinet Inc. All Rights Reserved. 15

An important concept to grasp about firewall policies is their reliance on order of precedence—essentially, a "first come, first served" approach.

Policy IDs are identifiers. You can add or remove the policy ID column using the **Configure Table** settings icon.

FortiGate automatically assigns a policy ID when you create a new firewall policy using the GUI. The policy ID never changes, even if you move the rule higher or lower in the sequence.

The **Policy** column on the **Policy & Objects, Firewall Policy** page combines the policy name and ID.

When you enable **Policy Advanced Options** in **Feature Visibility**, additional configuration options appear in the policy rules, including the ability to manually assign a policy ID. If you try to create a policy rule with a policy ID that already exists, the system generates an error and allows you to choose a different ID.

Assigning policy ID 0 automatically assigns the next available policy ID number, just as if you hadn't manually set it. This is useful to know when creating policy rules using the CLI, where you're required to set the policy ID and may not know the next available number.

DO NOT REPRINT

© FORTINET

Policy List—Interface Pair View and By Sequence

- **Interface Pair View**

- Lists policies by ingress and egress interfaces (or zone) pairings

The screenshot shows two views of the Firewall Policy list:

- Interface Pair View:** Shows policies grouped by interface pairs. A blue callout points to the first policy "LAN (port1) --> DMZ (port2)" which has "all" selected for both source and destination. Another blue callout labeled "Interface policy pairs" points to the second policy "LAN (port2) --> ISP1 (port1)" which also has "all" selected.
- Sequence Grouping View:** A red box highlights the "By Sequence" option in the top right corner of the interface pair view table. A blue callout points to this area with the text: "Sequence Grouping View groups firewall policies based on the sequence order of the policies".
- By Sequence View:** Shows policies listed sequentially. A blue callout points to the first policy "Block_FTP (1)" with "all" selected for both source and destination. A red box highlights the "DENY" action. Another blue callout labeled "Multiple interfaces" points to the second policy "DMZ (2)" which also has "all" selected. A blue callout labeled "any interface" points to the fourth policy "Block_ICMP (4)" where both source and destination are set to "any".

Firewall policies appear in an organized list. The list is organized as one of **Interface Pair View**, **Sequence Grouping View**, or **By Sequence**.

By default, the policy list appears in **Interface Pair View**. Each section contains policies in the order that they are evaluated for matching traffic and are arranged by ingress-egress interface pair. Alternatively, you can view your policies as a single, comprehensive list by selecting **Sequence Grouping View** or **By Sequence** at the top of the page. In these two views, the policies are also listed in the order in which they are evaluated for traffic matching—they are grouped as uncategorized in **Sequence Grouping View** layout. You can create new labels to group firewall policies as necessary to organize the firewall policies with the sequence order in mind.

To help you remember the use of each interface, you add aliases by editing the interface on the **Network** page. For example, you could call port1 **/ISP1**. This can help to make your list of policies easier to understand.

DO NOT REPRINT
© FORTINET

Policy List—By Sequence and Interface Pair View

Policy	From	To	Source	Destination
Full_Access - ISP1 (1)	port3	port1	HQ_SUBNET	all
Full_Access - ISP2 (2)	port3	port2	HQ_SUBNET	all
Internal_to_WebServer (5)	port3	port4	HQ_SUBNET	all
Inbound_Web_ISP1 (3)	port1	port4	all	VIP_WebServer
Inbound_Web_ISP2 (4)	port2	port4	all	VIP_Webserver2
Internal_to_FTPServer (6)	port3	port4	HQ_SUBNET	FTPServer
Inbound_FTP_ISP1 (8)	port1	port4	all	VIP_FTPServer
Inbound_FTP_ISP2 (9)	port2	port4	all	VIP_FTPServer2
Internal_to_SSHServer (7)	port3	port4	HQ_SUBNET	SSHServer
Inbound_SSH_ISP1 (10)	port1	port4	all	VIP_SSHServer
Inbound_SSH_ISP2 (11)	port2	port4	all	VIP_SSHServer2
Implicit Deny (0)	any	any	all	all

Policy	Source	Destination
port1 → port4 (3)	all	VIP_WebServer
Inbound_FTP_ISP1 (8)	all	VIP_FTPServer
Inbound_SSH_ISP1 (10)	all	VIP_SSHServer
port2 → port4 (4)	all	VIP_Webserver2
Inbound_Web_ISP2 (4)	all	VIP_FTPServer2
Inbound_SSH_ISP2 (11)	all	VIP_SSHServer2
port3 → port1 (1)	HQ_SUBNET	all
Full_Access - ISP1 (1)	HQ_SUBNET	all
port3 → port2 (2)	HQ_SUBNET	all
port3 → port4 (3)	HQ_SUBNET	all
Internal_to_WebServer (5)	HQ_SUBNET	WebServer
Internal_to_FTPServer (6)	HQ_SUBNET	FTPServer
Internal_to_SSHServer (7)	HQ_SUBNET	SSHServer
Implicit (1)	all	all
Implicit Deny (0)	all	all



© Fortinet Inc. All Rights Reserved.

17

While the default view for the policy list is **Interface Pair View**, it is essential to approach firewall policies as a complete list. Place specific policies at the top, followed by more general policies. This concept applies in both **Interface Pair View** and **By Sequence**, emphasizing the importance of viewing it as a single, ordered list. The firewall begins evaluating policies from the top of the list, so organize them with the most specific and more heavily used rules at the top.

DO NOT REPRINT

© FORTINET

Adjusting Policy Order

- On the GUI, drag and drop

Before policy move

Policy	ID	From	To
Full_Access (1)	1	LAN (port3)	ISP1 (port1)
		DMZ (port2)	
Block_FTP (2)	2	LAN (port3)	ISP1 (port1)
		DMZ (port2)	
DMZ (3)	3	LAN (port3)	DMZ (port2)

```
config firewall policy
edit 1
  set name "Full_Access"
...
next
edit 2
  set name "Block_FTP"
```

After policy move

Policy	ID	From	To
Block_FTP (2)	2	LAN (port3)	ISP1 (port1)
		DMZ (port2)	
Full_Access (1)	1	LAN (port3)	ISP1 (port1)
		DMZ (port2)	
DMZ (3)	3	LAN (port3)	DMZ (port2)

ID remains same

```
config firewall policy
edit 2
  set name "Block_FTP"
...
next
edit 1
  set name "Full_Access"
```



Remember you learned that only the first matching policy applies? Arranging your policies in the *correct position* is important. It affects which traffic is blocked or allowed. In the section of the applicable interface pair, FortiGate looks for a matching policy, beginning at the top. So, you should put more specific policies at the top; otherwise, more general policies will match the traffic first, and more granular policies will never be applied.

In the example shown on this slide, you're moving the **Block_FTP** policy (ID 2) that matches only FTP traffic, to a position above a more general **Full_Access** (accept everything from everywhere) policy. Otherwise, FortiGate would always apply the first matching policy in the applicable interface pairs—**Full_Access**—and never reach the **Block_FTP** policy.

When moving the policies across the policy list, policy IDs remain unchanged.

DO NOT REPRINT

© FORTINET

Moving Policies by ID

- On the GUI, move by ID

The screenshot shows the 'Firewall Policy' page in the FortiGate GUI. It displays a list of policies with columns for Policy, ID, From, To, and Source. A policy named 'Full_Access (1)' is selected and highlighted with a red border. A context menu is open over this policy, with the 'Move by ID' option highlighted. A callout bubble points to this option with the text 'Move by ID'. Above the table, there is a dropdown menu with options: 'Export', 'By Sequence', 'Interface Pair View', 'Sequence Grouping View', and 'By Sequence'. The 'By Sequence' option is highlighted with a green box. The table has a header row: Policy, ID, From, To, and Source. Below the header, the policies listed are:

Policy	ID	From	To	Source
Full_Access (1)	1	LAN (port3)	ISP1 (port1)	all
Deny (4)	4	ISP1 (port1)	LAN (port3)	Deny_IP
Allow_Access (3)	3	ISP1 (port1)	LAN (port3)	all
Allow_Access (3)	3	ISP1 (port1)	LAN (port3)	all
Implicit Deny (0)	0	any	any	all

Below the table, there is a 'Move by ID' dialog box. It shows the selected policy 'Allow_Access (3)', the 'Move' button, and a dropdown for 'Destination policy ID' with the value '4' highlighted with a red box. A callout bubble points to this dropdown with the text 'Move the policy above or below the specified policy ID'. At the bottom right of the dialog, there is a checkbox for 'Jump to policy after move'.

You can move policies by their ID, placing them before or after a specified policy ID.

Using **Move by ID** is especially useful when you have hundreds of policies, because dragging and dropping would take too much time. Moving by ID allows you to quickly organize policies without manually dragging them.

If you do not want to automatically view the new location of the policy, disable **Jump to policy after move**. This feature is enabled by default.

You can only move policies by ID when viewing the **Firewall Policy** page in **By Sequence** or **Sequence Grouping View**.

DO NOT REPRINT
© FORTINET

Combining Firewall Policies

- Check the settings before combining firewall policies
 - Source and destination interfaces
 - Source and destination addresses
 - Services
 - Schedules
 - Security profiles
 - Logging
 - NAT rules

Can combine Policy ID 1 and 2 by combining services

Make decisions for logging settings when combining Policy ID 1 and 2

Policy	ID	Source	Destination	Schedule	Action	NAT	Type	Security Profiles	Log	Bytes
LAN (port3) → ISP1 (port1)	1	all	all	always	✓ ACCEPT	✓ NAT	Standard	SQL deep-Inspection AV default WEB default	UTM	298.24 kB
Full_Access (1)	1	all	all	always	✓ ACCEPT	✓ NAT	Standard	SQL deep-Inspection AV default WEB default	UTM	298.24 kB
ICMP (2)	2	all	all	always	✓ ACCEPT	✓ NAT	Standard	SQL no-inspection	All	74.92 kB
Implicit	1	all	all	always	ALL	DENY			Disabled	917.89 kB
Implicit Deny (0)	0	all	all	always	ALL	DENY				
		all	all							



© Fortinet Inc. All Rights Reserved. 20

In order to optimize and consolidate firewall policies, always check all configured settings. In the example shown on this slide, the two firewall policies have differences in terms of services, security profiles, and logging settings. You can consolidate these two firewall policies by combining services and choosing appropriate logging settings.

If you select **Security Events** (UTM) for the logging settings, traffic logs will not be generated for **ALL_ICMP** traffic.

Note that the **ALL_ICMP** service is not subject to web filter and antivirus scans, which means that applying these security profiles to the ICMP traffic will result in the traffic passing through without being inspected.

DO NOT REPRINT**© FORTINET**

Best Practices

- Test policies in a maintenance window before deploying in production
 - Test policy for a few IP addresses, users, and so on
- Be careful when editing, disabling, or deleting firewall policies and objects
 - Changes are saved and activated immediately
 - Reevaluate active sessions
- Create firewall policies to match as specifically as possible
 - Example: Restrict firewall policies based on source, destination, service
 - Use proper subnetting for address objects
- Analyze and enable appropriate settings on a per-policy basis
 - Security profiles
 - Logging settings



Always plan a maintenance window and create a test case for a few IP addresses and users, before implementing configuration changes in the production network. Any configuration changes made using the GUI or CLI take effect immediately, and can interrupt service.

As a best practice, try to configure firewall policies as specifically as possible. This helps to restrict access to only those resources. For example, use correct subnets when configuring address objects.

Another setting worth mentioning is security profiles. Security profiles help to provide appropriate security for your network. Proper logging configuration can also help you to analyze, diagnose, and resolve common network issues.

DO NOT REPRINT
© FORTINET

Inspection Modes on Firewall Policies

- Enabling security profiles has an impact on firewall throughput
- FortiGate kernel inspect sessions to enforce filtering (for example, web filter)
- Selecting the FortiGate inspection modes on firewall policies:
 - Flow-based
 - Default mode
 - Optimizes performance
 - Proxy-based
 - Processed by CPU
 - Provides thorough inspection



Enabling the security profiles on FortiGate impacts firewall resources and throughput. Packets are sent to the kernel or main CPU to enforce filtering. FortiOS supports flow-based and proxy-based inspection in firewall policies and security profiles.

Depending on your requirements, you can select inspection mode, but it is useful to know some differences and how it can impact the firewall performance. Flow-based inspection identifies and blocks threats in real time as FortiOS identifies them. This requires lower processing resources than proxy-based inspection. It is recommended to apply flow-based inspection to policies that prioritize traffic throughput.

Proxy-based inspection involves buffering traffic and examining it as a whole, before determining an action. Having all the data to analyze allows for the examination of more data points than flow-based inspection. Some advanced features like usage quota and web-profile override are also supported in proxy-based inspection.

DO NOT REPRINT**© FORTINET**

Inspection Modes—Proxy-Based Visibility

- Proxy-based inspection mode is available on most FortiGate devices
- Some security profiles are available only in proxy-based inspection mode, such as:
 - Video Filter
 - Inline CASB
 - ICAP
 - Web Application Firewall
 - Data Leak Prevention (available on the CLI)
- Proxy-based inspection is not available on low-end platforms with 2 GB of RAM or less



By default, low-end FortiGate platforms with 2 GB or less of RAM do not show proxy-based settings on the GUI for firewall policies and security profiles. This is to reduce memory usage on these platforms because the RAM is designed to serve the purpose of the low-end FortiGate and also maximize security using flow-based security inspection across FortiGate.

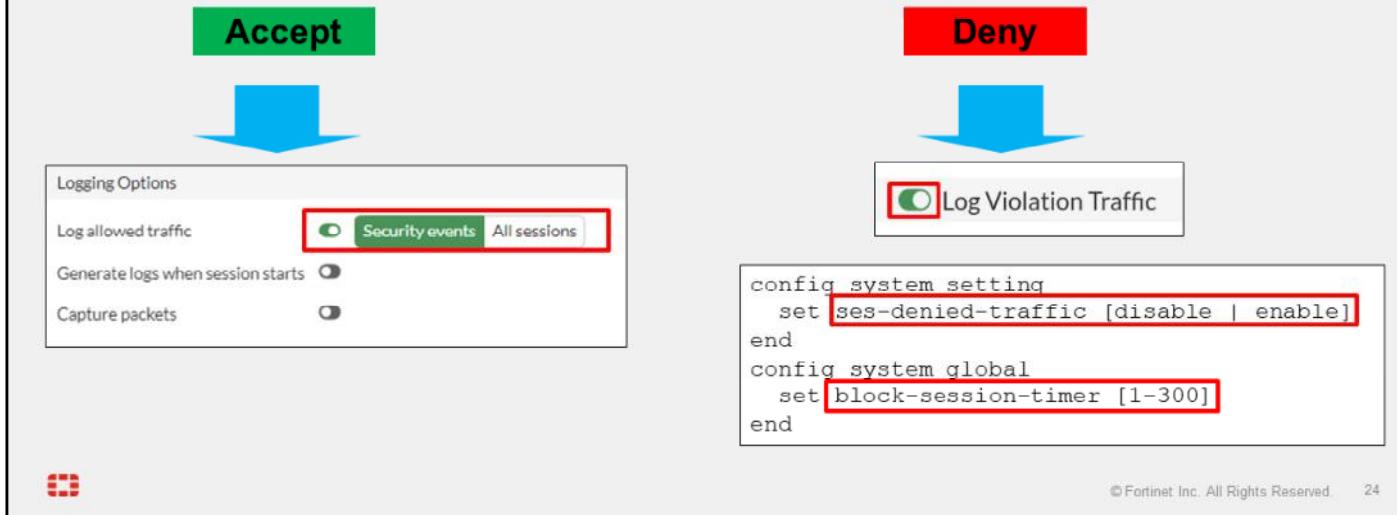
To confirm whether your FortiGate supports proxy inspection, enter `diagnose hardware sysinfo conserve` on the CLI. If the total RAM value is less than 2 GB, then your device has 2 GB RAM or less.

DO NOT REPRINT

© FORTINET

Logging

- By default, set to **Security events**
 - Generates logs based on the applied security profile only
- Can change to **All sessions**



If you enable logging in the policy, FortiGate generates traffic logs after a firewall policy closes an IP session.

By default, **Log allowed traffic** is enabled and set to **Security events** and generates logs only for the applied security profiles in the firewall policy. However, you can change the setting to **All sessions**, which generates logs for all sessions.

If you enable **Generate logs when session starts**, FortiGate creates a traffic log when the session begins. FortiGate also generates a second log for the same session when it is closed. Remember that increasing logging decreases performance, so use it only when necessary.

During the session, if a security profile detects a violation, FortiGate records the attack log immediately. To reduce the number of log messages generated and improve performance, you can enable a session table entry of dropped traffic. This creates the denied session in the session table and, if the session is denied, all packets for that session are also denied. This ensures that FortiGate does not have to perform a policy lookup for each new packet matching the denied session, which reduces CPU usage and log generation.

The CLI command is `ses-denied-traffic`. You can also set the duration for block sessions. This determines how long a session will be kept in the session table by setting `block-session-timer` in the CLI. By default, it is set to 30 seconds.

If the GUI option **Generate Logs when Session Starts** is not displayed, this means that your FortiGate device does not have internal storage. Regardless of internal storage, the CLI command is `set logtraffic-start enable`.

DO NOT REPRINT

© FORTINET

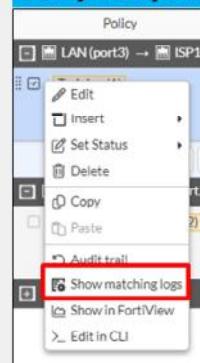
Monitor Traffic Logs

- FortiGate supports storing all types of logs in several log devices
 - FortiGate local and cloud
 - FortiAnalyzer local and cloud
 - Syslog
- View traffic logs in **Log & Report > Forward Traffic**
 - Apply filter to display relevant logs
 - Select the source of logs
 - Specify the historical time frame
- Right-click firewall policy and view matching traffic logs

Log & Report > Forward Traffic

Data/Time	#	Source	Device	Destination	Application Name	Result	Policy ID
2024/10/01 13:14:34	303.119	32099999000001	ME 5.0.8.8	DNS		✓ Accept (142.81 / 1048)	Training [1]
2024/10/01 13:14:26	303.119	32099999000001	ME 5.0.8.8	DNS		✓ Accept (244.0 / 2048)	Training [1]
2024/10/01 13:14:26	303.119	32099999000001	ME 74.32.190.33	tcp/8080		✓ Accept (117.15 kB / 29.63 MB)	Training [1]
2024/10/01 13:14:26	303.119	32099999000001	ME 74.32.190.33	tcp/8080		✓ Accept (105.51 kB / 29.19 MB)	Training [1]
2024/10/01 13:14:26	303.119	32099999000001	ME 44.79.50.48	tcp/8080		✓ Accept (127.92 kB / 30.39 MB)	Training [1]
2024/10/01 13:14:26	303.119	32099999000001	ME 44.79.50.48	tcp/8080		✓ Accept (132.20 kB / 28.45 MB)	Training [1]
2024/10/01 13:14:26	303.119	32099999000001	ME 44.79.50.48	tcp/8080		✓ Accept (114.13 kB / 25.52 MB)	Training [1]

Policy & Objects > Firewall Policy



Apply the desired filter to reduce irrelevant log entries

Only logs matching the firewall policy are displayed on the forward traffic logs page

© Fortinet Inc. All Rights Reserved.

25

Logging on FortiGate records the traffic that passes through, starts from, or ends on FortiGate. It records the actions during the traffic scanning process. FortiGate supports sending all log types to several log devices including its local storage, which is subject to the disk available on different FortiGate models.

You can view traffic logs in **Log & Report > Forward Traffic**. Apply the filter needed to display the logs and then enter the policy UUID in the filter field to display records that match the firewall policy. Select the source of the logs and specify the historical time frame to reduce irrelevant log entries.

You can also view the logs by right-clicking the firewall policy, and then clicking **Show matching logs**.

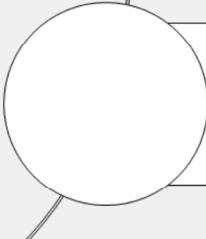
DO NOT REPRINT

© FORTINET

Lesson Progress



Firewall Policies



NAT



© Fortinet Inc. All Rights Reserved. 26

Good job! You now understand firewall policies.

Now, you will learn about NAT.

DO NOT REPRINT**© FORTINET****NAT****Objectives**

- Configure SNAT
- Configure a firewall policy to perform DNAT using VIP



© Fortinet Inc. All Rights Reserved. 27

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

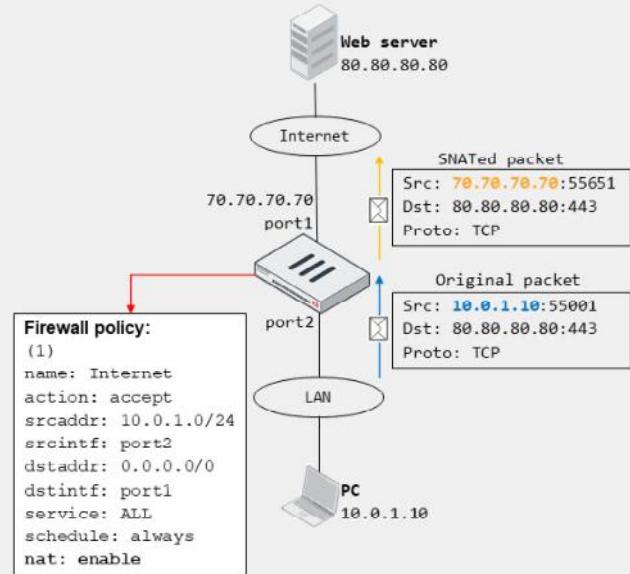
By demonstrating competence in NAT firewall policies, you will be able to configure firewall policies, invoke SNAT and DNAT on the policies, and understand how the policies are applied to traffic traversing FortiGate.

DO NOT REPRINT

© FORTINET

NAT

- Method of translating IP addresses in a packet
 - If ports are also translated, it is called PAT
- Benefits:
 - Real address is hidden from external networks
 - Prevents depletion of public IP address space
 - Private address space flexibility
- Types:
 - SNAT
 - Translates source IP address and source port
 - Enabled on firewall policy
 - DNAT
 - Translates destination IP address and destination port
 - Requires VIP object on firewall policy



© Fortinet Inc. All Rights Reserved. 28

NAT is a method that enables a NAT device such as a firewall or router, to translate (or map) the IP address in a packet to another IP address, usually for connectivity purposes. If the port information in the packet is also translated, then the translation method is called PAT. NAT provides the following benefits:

- Security: The real address of a device is hidden from external networks.
- Public address depletion prevention: Hundreds of computers can share the same public IPv4 address.
- Private address flexibility: The addresses can stay the same, even if ISPs change. You can reuse private addresses in multiple networks.

There are two types of NAT: SNAT and DNAT. In SNAT, a NAT device translates the source IP address and source port in a packet. In DNAT, a NAT device translates the destination IP address and destination port. You can configure FortiGate to perform SNAT and DNAT as follows:

- For SNAT, you enable NAT on the matching firewall policy.
- For DNAT, you configure virtual IPs (VIPs) and then reference them on the matching firewall policy.

The example on this slide shows the most common use case for NAT: SNAT. FortiGate, acting as a NAT device, translates the private IP address assigned to the PC to the public address assigned by your ISP. The private-to-public source address translation is needed for the PC to access the internet web server.

DO NOT REPRINT
© FORTINET

Firewall Policy SNAT

- There are two ways to SNAT traffic:
 - Using the outgoing interface address
 - Using a dynamic IP pool



The screenshot shows the 'Policy & Objects > Firewall Policy' configuration window. The policy is named 'Training' and has an 'ACCEPT' action. It is set to 'always' schedule and 'Standard' type. The incoming interface is 'LAN (port3)' and the outgoing interface is 'ISP1 (port1)'. In the 'Source & Destination' section, the source is 'LOCAL_SURNFT' and the destination is 'all'. Under 'Service', 'ALL' is selected. In the 'Firewall/Network Options' section, 'Flow-based' inspection mode is chosen. The 'NAT' tab is selected, showing 'NAT' as the mode. Under 'IP pool configuration', 'Use Outgoing Interface Address' is checked. The bottom section shows 'Protocol options' set to 'HTTP default'.

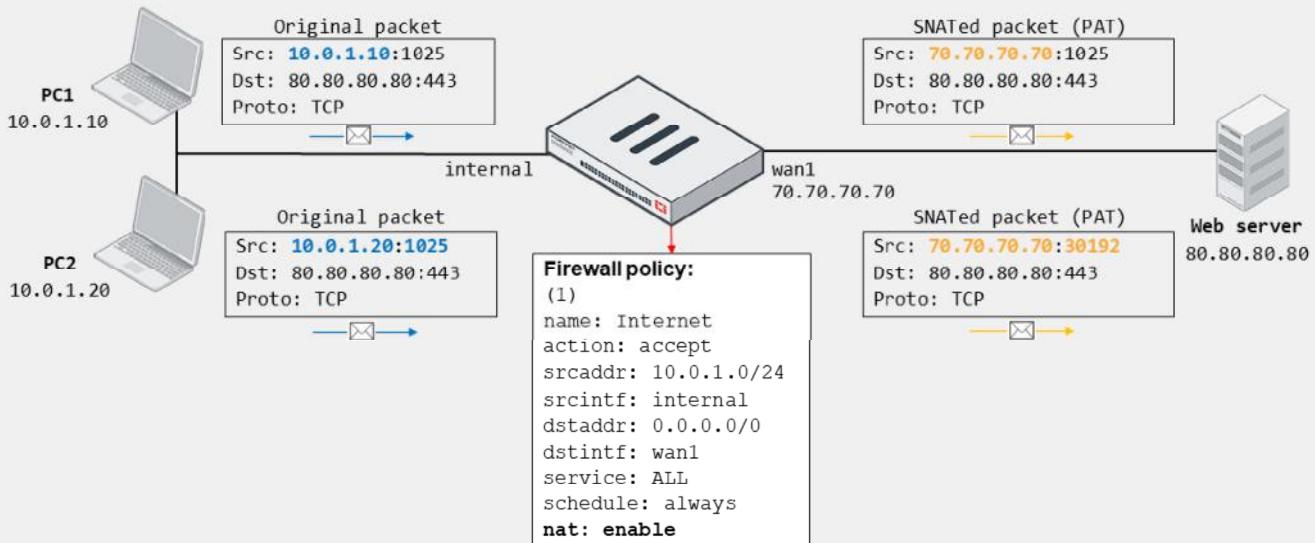
© Fortinet Inc. All Rights Reserved. 29

To configure a firewall policy, you can enable SNAT in the firewall and network options section. There are two options to select and choose how SNAT should work:

1. To use the outgoing interface IP address: Packets matching the firewall policy translate the IP address in a packet to another IP address, usually for connectivity purposes.
2. To use a dynamic IP pool: This is dynamic SNAT which allows FortiGate to map private IP addresses to the first available public address from a pool of addresses.

DO NOT REPRINT
© FORTINET

Firewall Policy SNAT Using the Outgoing Interface



© Fortinet Inc. All Rights Reserved. 30

When you select **Use Outgoing Interface Address** on the matching firewall policy, FortiGate uses the egress interface address as the NAT IP for performing SNAT.

If there are multiple devices behind FortiGate, FortiGate performs many-to-one NAT. This is also known as PAT. FortiGate assigns to each connection sharing the egress interface address a port number from a pool of available ports. The assignment of a port enables FortiGate to identify packets associated with the connection and then perform the corresponding translation. This is the same behavior as the overload IP pool type, which you will also learn about.

Optionally, you may select a fixed port, in which case the source port translation is disabled. With a fixed port, if two or more connections require the same source port for a single IP address, only one connection is established.

The example on this slide shows two PCs behind FortiGate that share the same public IP address (70.70.70.70) to access the internet web server 80.80.80.80. Because **Use Outgoing Interface Address** is enabled on the firewall policy—set `nat enable` on the CLI—the source IP address of the PCs is translated to the egress interface address. The source port, however, is not always translated. It depends on the available ports and the connection 5-tuple. In the example shown on this slide, FortiGate translates the source port of the connection from PC2 only. Otherwise, the two connections would have the same information on the session table for the reply traffic, which would result in a session clash.

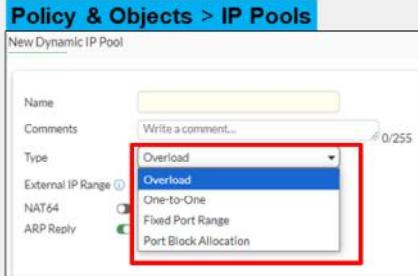
DO NOT REPRINT

© FORTINET

IP Pools

- IP pools define a single IP address or a range of IP addresses to be used as the source address for the duration of the session
- IP pools are usually configured in the same range as the interface IP address
- There are four types of IP pools:
 - Overload (default)
 - One-to-one
 - Fixed port range
 - Port block allocation

Useful for CGN



Policy & Objects > Firewall Policy

The screenshot shows the 'Policy & Objects > Firewall Policy' configuration. The 'Name' is set to 'Training', 'Schedule' is 'always', 'Action' is 'ACCEPT', 'Type' is 'Standard ZTNA', 'Incoming Interface' is 'LAN (port3)', and 'Outgoing Interface' is 'ISP1 (port1)'. Under 'Firewall/Network Options', 'Inspection mode' is 'Flow-based', 'NAT' is selected, and 'NAT46' and 'NAT64' are available. In the 'IP pool configuration' section, 'Use Outgoing Interface Address' is checked, and 'Use Dynamic IP Pool' is selected, with 'INTERNAL-HOST-EXT-IP' listed.

© Fortinet Inc. All Rights Reserved. 31

IP pools allow sessions leaving the FortiGate firewall to use NAT. An IP pool defines a single IP address or a range of IP addresses to be used as the source address for the duration of the session. These assigned addresses are used instead of the IP address assigned to that FortiGate interface.

IP pools are usually configured in the same range as the interface IP address.

When you configure the IP pools that will be used for NAT, there is a limitation that you must take into account. If the IP addresses in the IP pool are different from the IP addresses that are assigned to the interfaces, communications based on those IP addresses *may fail if the routing is not properly configured*. For example, if the IP address assigned to an interface is 172.16.100.1/24, you cannot choose 10.10.10.1 to 10.10.10.50 for the IP pool unless you configure appropriate routing.

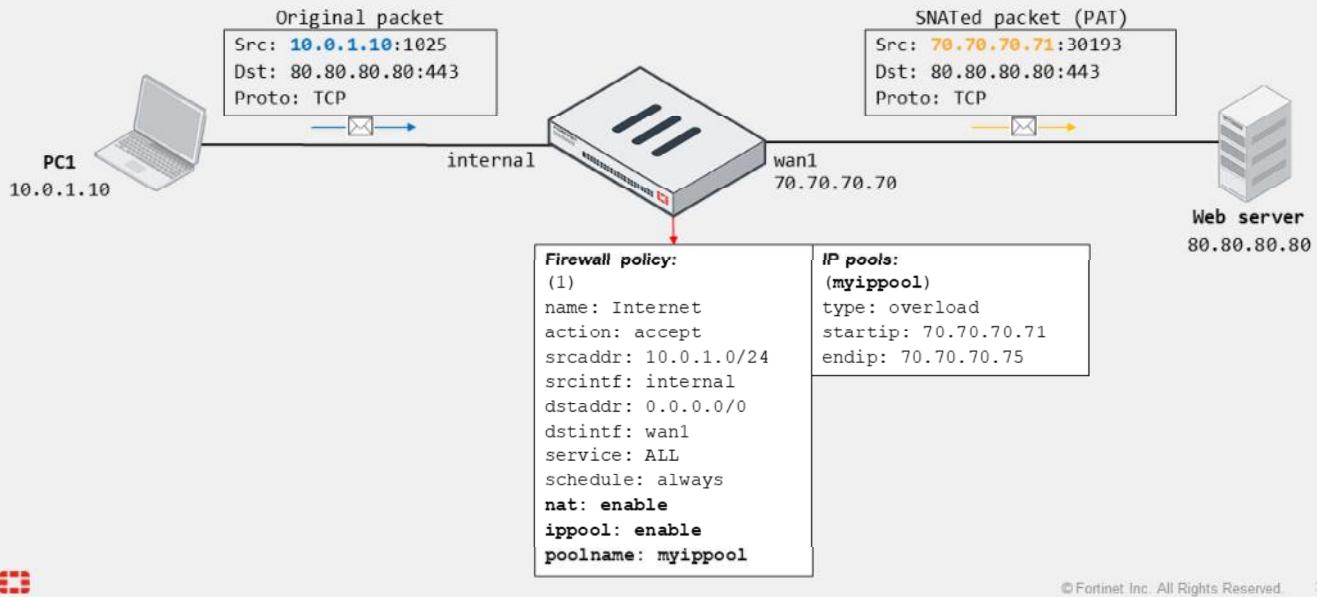
There are four types of IP pools that you can configure on the FortiGate firewall:

- Overload
- One-to-one
- Fixed port range
- Port block allocation

The fixed port range and port block allocation types are more common carrier-grade NAT (CGN) deployments.

DO NOT REPRINT
© FORTINET

IP Pool Type—Overload



If you use an IP pool, the source address is translated to an address from that pool, rather than the egress interface address. The larger the number of addresses in the pool, the greater the number of connections that the pool can support.

The default IP pool type is overload. In the overload IP pool type, a many-to-one or many-to-few relationship and port translation is used.

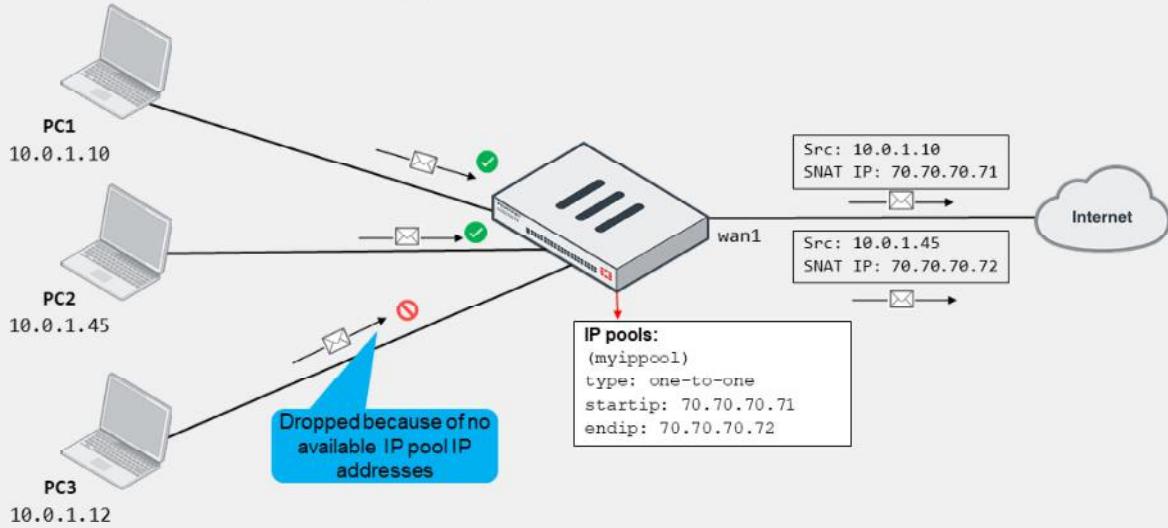
In the example shown on this slide, source IP 10.0.1.10 is translated to the address 70.70.70.71, which is one of the addresses defined in the IP pool (70.70.70.71 – 70.70.70.75).

DO NOT REPRINT

© FORTINET

IP Pool Type—One-to-One

- Assigns an IP pool address to an internal host on a first-come, first-served basis
 - Packets from unserved hosts are dropped if there are no available addresses in the IP pool



© Fortinet Inc. All Rights Reserved. 33

In the one-to-one pool type, FortiGate assigns an IP pool address to an internal host on a first-come, first-served basis.

There is a single mapping of an internal address to an external address. That is, an IP pool address is not shared with any other internal host, thus the name one-to-one. If there are no more addresses available in the IP pool, FortiGate drops packets from unserved hosts.

The example on this slide shows three internal hosts accessing the internet. PC1 and PC2 packets are received first by FortiGate and, therefore, assigned addresses 70.70.70.71 and 70.70.70.72, respectively. However, FortiGate drops packets sourced from PC3 because they arrived last, which is when there are no more available addresses in the IP pool to choose from.

DO NOT REPRINT

© FORTINET

VIPs

- DNAT objects
- Default type is **Static NAT**
 - One-to-one mapping, applies to both:
 - Ingress traffic (DNAT; use internal IP as NAT IP)
 - Egress traffic (SNAT; use external IP as NAT IP)
 - Reference IP addresses or FQDN objects (set **Type** to **FQDN**)
- Enable **Port Forwarding** to:
 - Redirect traffic destined to external IP and port to mapped internal address and port
 - Reuse external IP on multiple VIPs

The screenshot shows the FortiGate management interface with two windows open:

- Policy & Objects > Virtual IPs**: Shows a list of VIPs. One entry, "VIP-INTERNAL-HOST", is highlighted.
- Policy & Objects > Firewall Policy**: Shows a list of firewall policies. The second policy, "Web Server Access", has its "Destination" field set to "VIP-INTERNAL-HOST".

A red arrow points from the "VIP-INTERNAL-HOST" entry in the Virtual IPs list to the "Destination" field in the Firewall Policy's "Source & Destination" section. A blue callout box highlights this connection with the text "VIP used as destination in firewall policy".



© Fortinet Inc. All Rights Reserved.

34

VIPs are DNAT objects. For sessions matching a VIP, the destination address is translated; usually a public internet address is translated to the private network address of a server. VIPs are selected in the firewall policy **Destination** field.

The default VIP type is **Static NAT**. This is a one-to-one mapping. This means that:

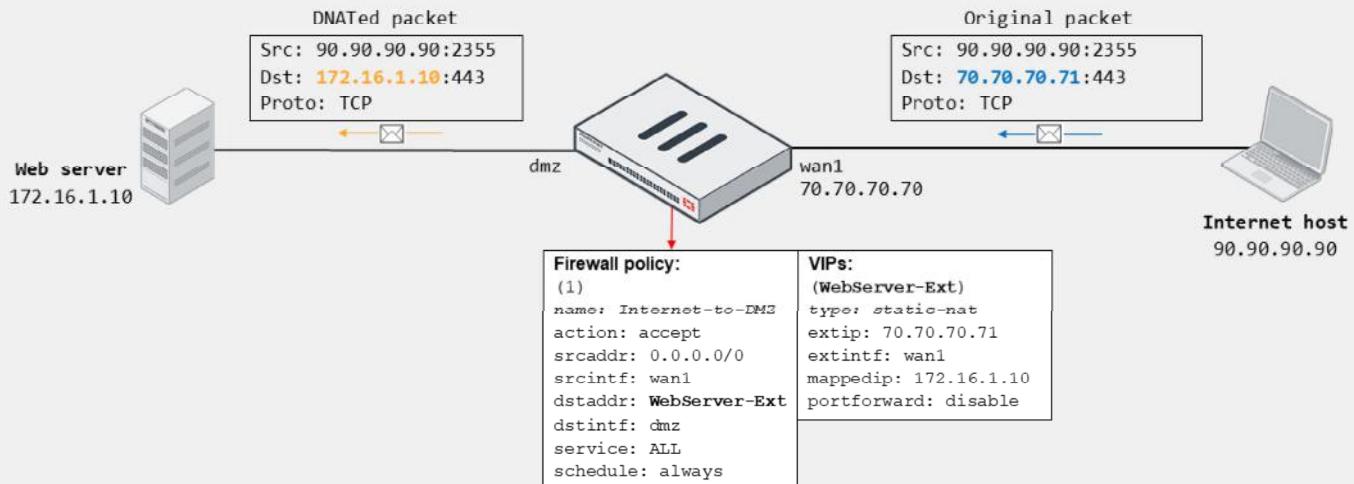
1. FortiGate performs DNAT on ingress traffic destined to the external IP address defined in the VIP, regardless of the protocol and port of the connection, provided the matching firewall policy references the VIP as **Destination**.
2. FortiGate uses the external IP address defined in the VIP as the NAT IP address when performing SNAT on all egress traffic sourced from the mapped address in the VIP, provided the matching firewall policy has NAT enabled. That is, FortiGate doesn't use the egress interface address as NAT IP.

Note that you can override the behavior described in step 2 by using an IP pool. You can also select **FQDN** as the VIP type. When you select **FQDN**, you can configure FQDN address objects as external and internal IP addresses. This enables FortiGate to automatically update the external and internal IP addresses used by the VIP in case the FQDN resolved address changes.

Optionally, you can enable **Port Forwarding** on the VIP to instruct FortiGate to redirect the traffic matching the external address and port in the VIP to the mapped internal address and port. When you enable port forwarding, FortiGate no longer performs one-to-one mapping. This means that you can reuse the same external address and map it to different internal addresses and ports provided the external port is unique. For example, you can configure a VIP so connections to the external IP address 70.70.70.70 on port 8080 map to the internal IP address 192.168.0.70 on port 80. You can then configure another VIP so connections to the external IP address 70.70.70.70 on port 8081 map to the internal IP 192.168.0.71 on port 80.

DO NOT REPRINT
© FORTINET

VIP Example—Static NAT—Incoming Connection

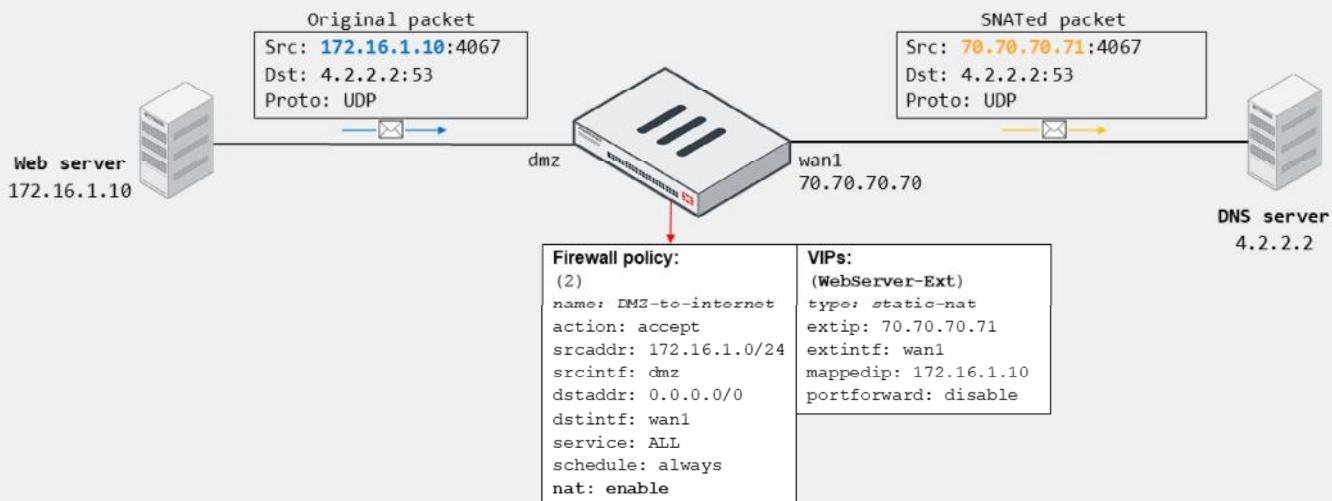


In the example shown on this slide, the internet host initiates a connection to 70.70.70.71 on TCP port 443. On FortiGate, the traffic matches the firewall policy ID 1, which references the WebServer-Ext VIP as destination. Because the VIP is configured as static NAT and has port forwarding disabled, then FortiGate translates the destination address of the packet to 172.16.1.10 from 70.70.70.71. Note that the destination port doesn't change because port forwarding is disabled.

Also note that the external interface address is different from the external address configured in the VIP. This is not a problem as long as the upstream network has its routing properly set. You can also enable ARP reply on the VIP (enabled by default) to facilitate routing on the upstream network. You will learn more about ARP reply in this lesson.

DO NOT REPRINT
© FORTINET

VIP Example—Static NAT—Outgoing Connection

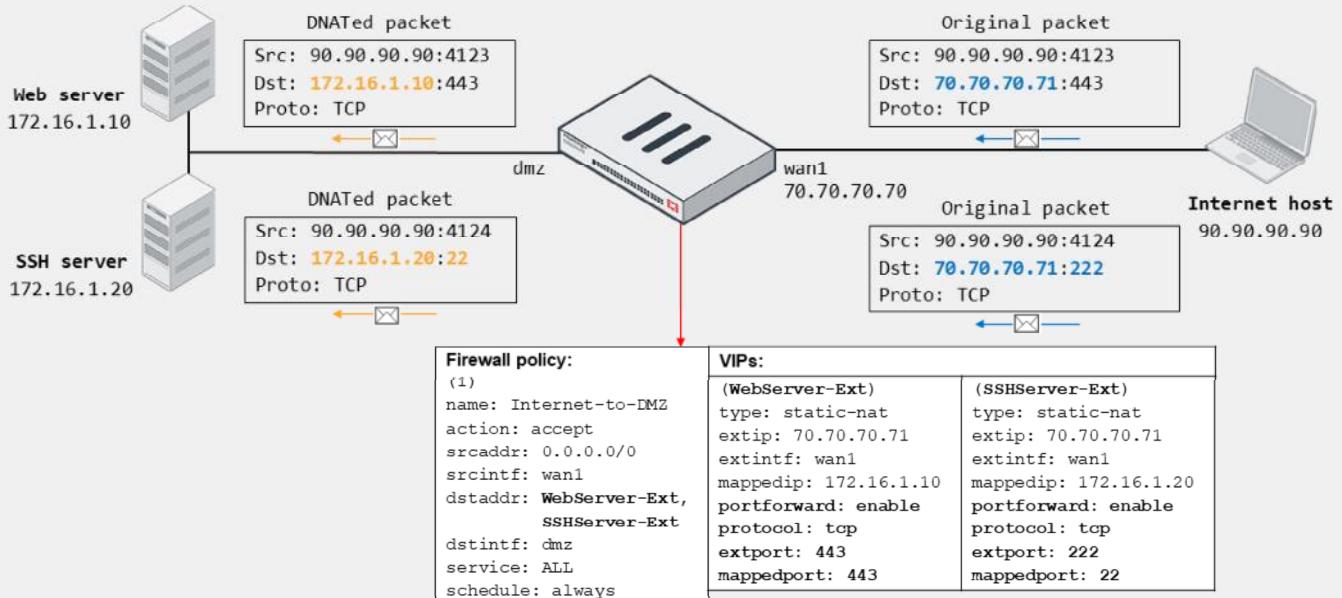


Now, suppose that the internal web server (172.16.1.10) initiates a DNS connection to the internet DNS server (4.2.2.2). On FortiGate, the traffic matches the firewall policy ID 2, which has `nat` enabled. Because the source address matches the internal address of the VIP, and because the VIP is configured as static NAT with port forwarding disabled, FortiGate translates the source address of the packet to 70.70.70.71 from 172.16.1.10. Note that FortiGate doesn't have to perform PAT because the static NAT VIP equals one-to-one mapping. That is, the external IP is used by the web server only for SNAT.

Also note that FortiGate uses the VIP external address for SNAT if the VIP is referenced in an incoming firewall policy. That is, if you don't configure firewall policy ID 1, which is shown on the previous slide, or if you disable the firewall policy, then FortiGate doesn't automatically use the external IP for translating the source address of the web server. Instead, FortiGate uses the egress interface address (70.70.70.70).

DO NOT REPRINT
© FORTINET

VIP Example—Port Forwarding—Incoming Connection



© Fortinet Inc. All Rights Reserved. 37

The example on this slide shows how FortiGate handles two incoming connections to the same external address, but on different ports. FortiGate forwards each connection to a different internal host based on the VIP mapping settings. This is possible because port forwarding is enabled on the VIPs, which enables FortiGate to redirect the external traffic to the corresponding internal address and port, while using the same external address.

Both connections match the firewall policy ID, which references two VIPs as destination. The HTTPS connection matches the WebServer-Ext VIP, and the SSH connection matches the SSHServer-Ext VIP. Note that for the SSH connection, FortiGate also translates the destination port to 22 from 222.

Although not shown on this slide, outgoing connections sourced from the web and SSH server would result in FortiGate using as NAT IP the egress interface address for SNAT, providing there is a matching firewall policy with `nat` enabled.

DO NOT REPRINT

© FORTINET

VIP—Matching Policies

- Default behavior: Firewall address objects match VIPs
 - Blocks an egress-to-ingress connection, when the deny policy precedes the allow policy with the VIP
 - The CLI command `match-vip` is available only for firewall policies with the action set to **DENY**
- VIP policy (WAN to LAN)

Policy	ID	Source	Destination	Schedule	Service	Action
ISP1 (port1) → LAN (port3) 2						
<input type="checkbox"/> Deny (4)	4	Deny_IP	all	always	All	 DENY
<input type="checkbox"/> Allow_Access (3)	3	all	Web_Server	always	HTTP HTTPS	 ACCEPT

- CLI configuration:

```
config firewall policy
  edit <deny policy ID>
    set match-vip enable
  next
end
```

VIP access falls through to this policy and the connection is blocked

By default, `match-vip` is enable in the deny policy



In FortiOS, VIPs and firewall address objects are completely different. They are stored separately with no overlap. Starting in version 7.2.4, the parameter `match-vip` is `enable` by default and allows the firewall address objects to match VIPs.

In the example shown on this slide, the destination of the first firewall policy is set to **all**. This means all destination addresses (`0.0.0.0/0`), by default, including the external addresses defined on the VIPs. The result is that traffic destined to the external address defined on the **Web_Server** VIP matches the first policy.

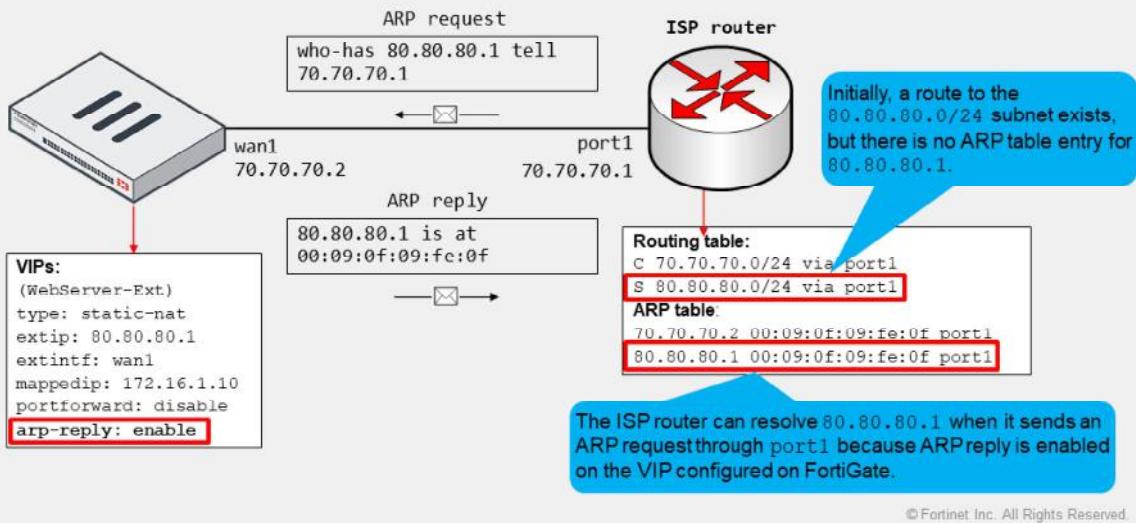
But what if you want the first policy to block all incoming traffic to all destinations, except the traffic destined to any VIPs? You can do this by disabling `match-vip` on the first firewall policy. Disabling `match-vip` instructs FortiGate not to also check for VIPs during policy evaluation. Note that the `match-vip` setting is available only when the firewall policy action is set to **DENY**.

DO NOT REPRINT

© FORTINET

ARP Reply Option in VIPs and IP Pools

- Enabled by default; instructs FortiGate to reply to ARP requests for external address
- Sometimes required to overcome routing misconfigurations
 - Example:



© Fortinet Inc. All Rights Reserved.

39

When you configure a VIP or an IP pool, ARP reply is enabled by default. When ARP reply is enabled, FortiGate replies to incoming ARP requests for the external address configured in the VIP and IP pools.

Enabling ARP reply is usually not required in most networks because the routing tables on the adjacent devices contain the correct next-hop information, so the networks are reachable. However, sometimes the routing configuration is not fully correct, and having ARP reply enabled can solve the issue for you. For this reason, it's a best practice to keep ARP reply enabled.

Consider the example shown on this slide, which shows an internet connection between FortiGate and an ISP router. The example also shows a simplified version of the ISP router routing table and ARP table.

The ISP assigns the FortiGate administrator the public subnet 80.80.80.0/24 to deploy internet-facing services. The administrator configured the VIP shown on this slide to provide internet users with access to the company web server. While testing, the administrator confirms that internet users can reach the web server at 80.80.80.1.

However, the administrator is likely unaware that having ARP reply enabled was key for a successful connectivity. The reason is that the ISP router doesn't have a route in its routing table to access the 80.80.80.0/24 subnet through the 70.70.70.2 gateway. Instead, the routing table contains a static route for the subnet through port1. The result is that the ISP router generates ARP requests out of port1 to resolve the MAC address of any of the addresses in the 80.80.80.0/24 subnet. Nonetheless, because FortiGate responds to ARP requests for the external address in the VIP, the ISP router is able to resolve the MAC address successfully.

DO NOT REPRINT**© FORTINET**

NAT Implementation Best Practices

- Avoid misconfiguring an IP pool range:
 - Double-check the start and end IP addresses of each IP pool
 - Ensure that the IP pool address range does not overlap with addresses assigned to FortiGate and hosts
 - If internal and external users are accessing the same servers, configure your DNS service so internal users resolve to the destination internal address
- Don't configure a NAT rule for inbound traffic unless it is required by an application
- Schedule a maintenance window to make changes on NAT configuration



Use the following best practices when implementing NAT:

- Avoid misconfiguring an IP pool range:
 - Double-check the start and end IP addresses of each IP pool.
 - Ensure that the IP pool address range does not overlap with addresses assigned to FortiGate interfaces or to any hosts on directly connected networks.
 - If you have internal and external users accessing the same servers, configure your DNS services so internal users resolve to use the destination internal address instead of its external address defined in the VIP.
- Don't configure a NAT rule for inbound traffic unless it is required by an application.
 - For example, if there is a matching NAT rule for inbound SMTP traffic, the SMTP server might act as an open relay.
- You must schedule a maintenance window when making changes to NAT settings configuration, since making changes could create a network outage.

DO NOT REPRINT**© FORTINET**

Knowledge Check

1. Which criteria does FortiGate use to match traffic to a firewall policy?

- A. Source and destination interfaces
- B. Security profiles

2. What is the purpose of applying security profiles to a firewall policy?

- A. To allow access to specific subnets
- B. To protect your network from threats, and control access to specific applications and URL

3. What is the default IP pool type?

- A. One-to-one
- B. Overload

4. Which is the default VIP type?

- A. static-nat
- B. load-balance



DO NOT REPRINT

© FORTINET

Lesson Progress



Firewall Policies



NAT



© Fortinet Inc. All Rights Reserved.

42

Congratulations! You have completed this lesson.

Now, you will review the objectives covered in this lesson.

DO NOT REPRINT**© FORTINET**

Review

- ✓ Configure IPv4 firewall policies
- ✓ Monitor traffic logs from firewall policies
- ✓ Choose inspection modes for firewall policies
- ✓ Configure SNAT
- ✓ Configure a firewall policy to perform DNAT using VIP



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

By mastering the objectives covered in this lesson, you learned how to configure, use, and manage firewall policies and NAT on FortiGate.

DO NOT REPRINT

© FORTINET

FORTINET
Training Institute

FortiOS Administrator

Routing

 FortiOS 7.6

Last Modified: 6 October 2025

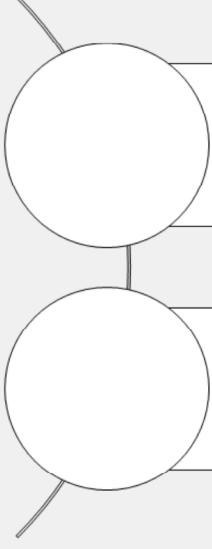
© Fortinet Inc. All Rights Reserved. 1

In this lesson, you will learn about the routing capabilities and features available on FortiGate.

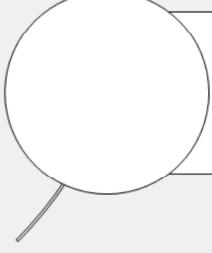
DO NOT REPRINT

© FORTINET

Lesson Overview



Routing on FortiGate



ECMP Routing

In this lesson, you will learn about the topics shown on this slide.

© Fortinet Inc. All Rights Reserved.

2

DO NOT REPRINT

© FORTINET

Routing on FortiGate

Objectives

- Configure static routing
- Interpret the routing table on FortiGate



© Fortinet Inc. All Rights Reserved. 3

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

By demonstrating competence in routing on FortiGate, you should be able to implement static routing and understand the routing table.

DO NOT REPRINT**© FORTINET**

What Is IP Routing?

- FortiGate acts as an IP router in network address translation (NAT) mode
 - Forwards packets between IP networks
 - Supports IPv4 and IPv6 routing
- IP routing:
 - Performed for firewall traffic and local-out traffic
 - Determines next hop (outgoing interface and gateway) for packet destination address
 - Next hop can be the destination router or another router along the path



When FortiGate operates in NAT mode—the default operation mode—FortiGate behaves as an IP router. An IP router is a device that forwards packets between IP networks. For that, a router performs IP routing, which is the process of determining the next hop to forward a packet to based on the packet destination IP address. FortiGate supports both IPv4 and IPv6 routing.

FortiGate performs routing for both firewall traffic (also known as user traffic) and local-out traffic. Firewall traffic is the traffic that travels through FortiGate. Local-out traffic is the traffic generated by FortiGate, usually for management purposes. For example, when you ping a device from FortiGate, that's local-out traffic. When FortiGate connects to FortiGuard to download the latest definitions, that's also local-out traffic.

DO NOT REPRINT**© FORTINET**

What Is IP Routing? (Contd)

- **Routing table:**
 - Contains routes with next-hop information for a destination
 - Entries are checked during route lookup (best route selection)
 - *Best route*: most specific route to the destination
 - *Duplicate routes*: multiple routes to the same destination
 - Route attributes are used as tiebreakers for best route selection
- **Routing precedes most security actions**
 - Configure your security policies based on routing settings, not the opposite



Routers maintain a routing table. A routing table contains a series of entries, also known as routes. Each route in the routing table indicates the *next hop* for a particular destination. The next hop refers to the outgoing interface and gateway to use for forwarding the packet. The next hop can be the destination of the packet or another router along the path to the destination. If the next hop isn't the destination, the next router in the path routes the packet to the next hop. The routing process is repeated on each router along the path until the packet reaches its destination.

To route packets, FortiGate performs a route lookup to identify the best route to the destination. The best route is the most specific route to the destination. If FortiGate finds duplicate routes—multiple routes to the same destination—it uses various route attributes as a tiebreaker to determine the best route.

Routing takes place before most security features. For example, routing precedes firewall policy evaluation, content inspection, traffic shaping, and source NAT (SNAT). This means that the security actions that FortiGate performs depend on the outgoing interface determined by the routing process. This also means that your security policy configuration must follow your routing configuration, and not the opposite.

DO NOT REPRINT**© FORTINET**

Route Lookup

- For any session, FortiGate performs a route lookup twice:
 - For the first packet sent by the originator
 - For the first reply packet coming from the responder
- Routing information is written to the session table
- All other packets for that session will use the same path
- No more route lookups done unless the session is impacted by a routing change
 - Route information on the session is flushed and new route lookups are performed



For each session, FortiGate performs two route lookups:

- For the first packet sent by the originator
- For the first reply packet coming from the responder

After completing these two lookups, FortiGate writes the routing information to its session table. Subsequent packets are routed according to the *session table*, not the routing table. So, all packets that belong to the same session follow the same path. However, there is an exception to this rule: if there is a change in the routing table that impacts the session, then FortiGate removes the route information for the session table, and then performs additional route lookups to rebuild this information.

DO NOT REPRINT

© FORTINET

RIB and FIB

- FortiGate maintains two tables containing routing information: RIB and FIB
- RIB
 - Standard routing table containing active (or best) connected, static, and dynamic routes
 - Visible from the GUI and CLI
- FIB
 - Routing table from a kernel perspective
 - Composed mostly of RIB entries, plus some system-specific entries
 - Used for route lookups
 - Visible from the CLI with the command `get router info kernel`



FortiGate maintains its routing information in two tables: RIB and FIB. The routing table, also known as the routing information base (RIB), is a standard routing table containing active (or the best) connected, static, and dynamic routes. The forwarding information base (FIB) can be described as the routing table from the kernel point of view, and contains mostly RIB entries plus some system-specific entries required by FortiOS.

When FortiGate performs a route lookup, it checks the FIB and not the RIB. However, because the FIB is composed mostly of RIB entries, a route lookup mainly involves checking routes from the RIB. For this reason, the route lookup is often referred to as the routing table lookup process. Nonetheless, it is more accurate to refer to a route lookup as a FIB lookup process.

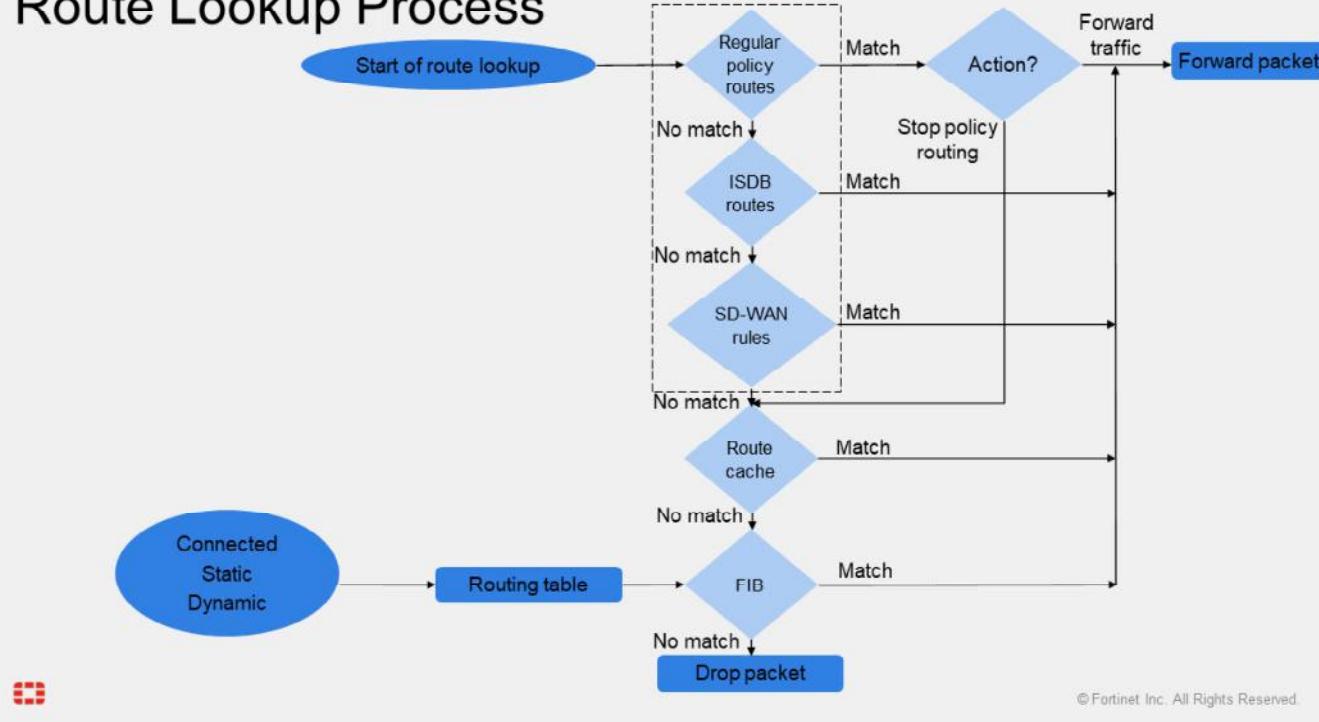
You can display the RIB entries on the FortiGate GUI and CLI. You can display FIB entries on the FortiGate CLI only.

This lesson focuses on the RIB (or routing table) only. You will learn more about it, including how to monitor its entries, in this lesson.

DO NOT REPRINT

© FORTINET

Route Lookup Process



© Fortinet Inc. All Rights Reserved.

8

The flowchart on this slide describes the route lookup process in FortiOS.

First, FortiGate checks the policy routes. If there is a match, and the selected action is **Forward Traffic**, FortiGate routes the packet accordingly, as long as the policy route passes the forwarding information base (FIB) validation process. If the selected action is **Stop Policy Routing**, FortiGate moves on to check its route cache, if applicable.

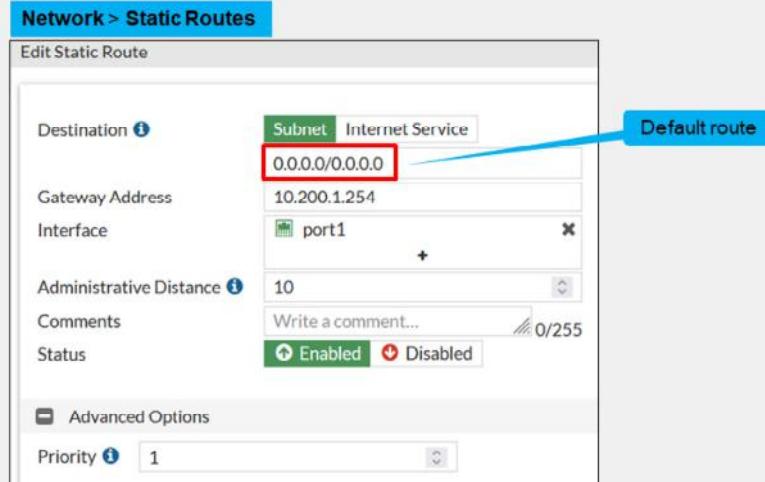
If the packet doesn't match any of the policy routes, FortiGate moves on to check the ISDB routes first, and then the SD-WAN rules.

Next, FortiGate checks the FIB, which is the table that is used to perform standard routing. If the packet doesn't match any of the routes in the FIB, FortiGate drops the packet and sends an ICMP destination network unreachable message to the sender.

DO NOT REPRINT
© FORTINET

Static Routes

- Configured *manually*, by an administrator
- Simple matching of packets to a route, based on the packet destination IP address



© Fortinet Inc. All Rights Reserved. 9

One type of manually configured route is called a static route. When you configure a static route, you are telling FortiGate, “When you see a packet whose destination is within a specific range, send it through a specific network interface, towards a specific router.” You can also configure the distance and priority so that FortiGate can identify the best route to any destination matching multiple routes. You will learn about distance and priority in this lesson.

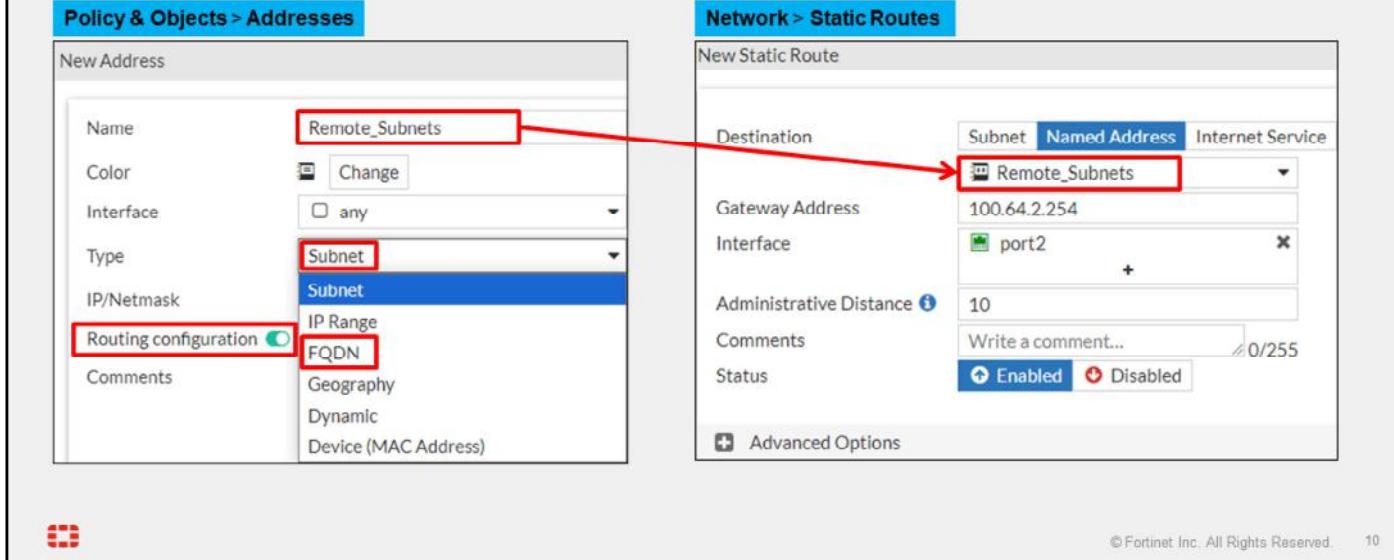
For example, in simple home networks, DHCP automatically retrieves and configures a route. Your modem then sends all outgoing traffic through your ISP internet router, which can relay packets to their destination. This is typically referred to as a default route, because all traffic not matching any other routes will, by default, be routed using this route. The example shown on this slide is a default route. The destination subnet value of $0.0.0.0/0.0.0.0$ matches all addresses within any subnet. Most FortiGate devices deployed at the edge of the network have at least one of these default routes to ensure internet traffic is forwarded to the ISP network.

Static routes are not needed for subnets to which FortiGate has direct Layer 2 connectivity.

DO NOT REPRINT
© FORTINET

Static Routes With Named Addresses

- Firewall addresses set to type **Subnet** or **FQDN** can be used as destinations for static routes



The screenshot displays two configuration screens from the FortiGate management interface:

- Policy & Objects > Addresses**: A "New Address" dialog. The "Name" field is set to "Remote_Subnets". The "Type" dropdown is set to "Subnet", which is highlighted in blue. The "Routing configuration" checkbox is checked and highlighted with a red box. The "Comments" section includes options like IP Range, FQDN, Geography, Dynamic, and Device (MAC Address).
- Network > Static Routes**: A "New Static Route" dialog. The "Destination" dropdown is set to "Named Address", which is highlighted in blue. The value "Remote_Subnets" is selected from the dropdown. Other fields include "Gateway Address" (100.64.2.254), "Interface" (port2), "Administrative Distance" (10), and "Status" (Enabled).

A red arrow points from the "Named Address" dropdown in the static route dialog to the "Named Address" entry in the address list dialog, indicating the relationship between the two configurations.

If you create a firewall address object with the type **Subnet** or **FQDN**, you can use that firewall address as the destination of one or more static routes. First, enable **Routing configuration** in the firewall address configuration. After you enable it, the firewall address object becomes available for use in the **Destination** drop-down list for static routes with named addresses.

DO NOT REPRINT
© FORTINET

Internet Services Routing

- Route well-known internet services through specific interfaces

The screenshot shows two windows from the FortiOS interface:

- Policy & Objects > Internet Service Database**: A table listing various internet services with their names, directions, entry counts, and references. One row for "Amazon-AWS" is highlighted with a red border.
- Network > Static Routes**: A configuration window for creating a new static route. It includes fields for Destination (set to "aws Amazon-AWS"), Gateway Address ("10.200.1.254"), Interface ("port1"), and Status (set to "Enabled").

A blue callout box points to the ISDB table, stating: "Database containing IP addresses, protocols, and port numbers used by most common Internet services". A red arrow points from the highlighted "Amazon-AWS" row in the ISDB table to the "Destination" field in the static route configuration window.

What happens if you need to route traffic to a public internet service (such as Amazon-AWS or Apple Store) through a specific WAN link? Say you have two ISPs and you want to route Netflix traffic through one ISP and all your other internet traffic through the other ISP. To achieve this goal, you need to know the Netflix IP addresses and configure the static route. After that, you must frequently check that none of the IP addresses have changed. The internet service database (ISDB) helps make this type of routing easier and simpler. ISDB entries are applied to static routes to selectively route traffic through specific WAN interfaces.

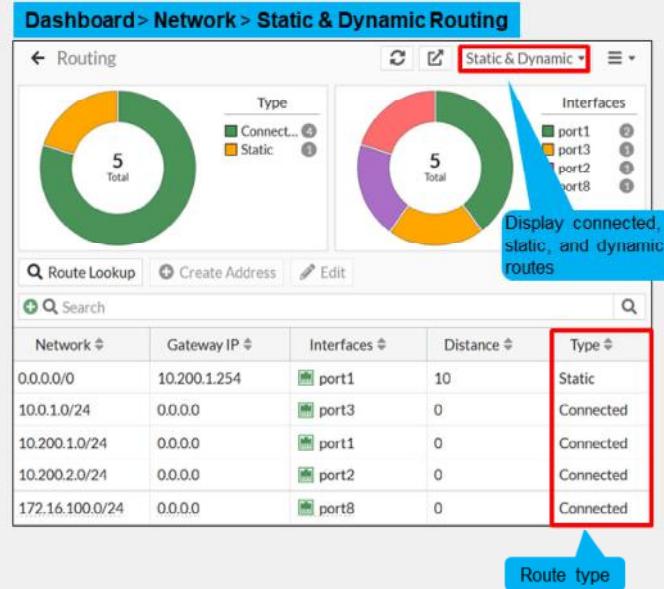
Even though they are configured as static routes, ISDB routes are actually policy routes and take precedence over any other routes in the routing table. As such, ISDB routes are added to the policy routing table.

DO NOT REPRINT

© FORTINET

Routing Monitor

- Routing table (**Static & Dynamic**) view
 - Contains best routes (active routes):
 - Connected, static, and dynamic routes
 - Doesn't contain:
 - Inactive, standby, and policy routes



© Fortinet Inc. All Rights Reserved.

12

The routing monitor widget on the dashboard page enables you to view the routing table and policy route table entries. The routing table contains *the best routes* (or active routes) of the following types:

- Static: manual routes that are configured by the administrator.
- Connected: automatic routes added by FortiOS after an interface is assigned an IP address. A connected route references the interface IP address subnet.
- Dynamic: routes learned using a dynamic routing protocol such as BGP or OSPF. FortiGate installs these routes automatically in the routing table and indicates the dynamic routing protocol used.

To view the routing table entries, select **Static & Dynamic**, as shown on this slide. However, keep in mind that the routing table doesn't contain the following routes:

- Inactive routes: These are static and connected routes with interfaces that are administratively down or with links that are down. Static routes are marked inactive when the link health monitor detects that their gateway is dead.
- Standby routes: These are active routes that are removed from the routing table because they are duplicate and have higher distances. Some examples of standby routes are:
 - A second static default route with a higher distance than another static default route
 - A dynamic route such as BGP or OSPF, to the same destination as another static route. However, the dynamic route is not displayed in the routing table because the static route has a lower distance.
- Policy routes: These include regular policy routes, ISDB routes, and SD-WAN rules. Policy routes are viewed in a separate table—the policy route table. You will learn more about policy routes in another lesson.

DO NOT REPRINT

© FORTINET

Route Attributes

- Each route in the routing table has the following attributes:

- Network
- Gateway IP
- Interfaces
- Distance
- Metric
- Priority

The screenshot shows the FortiGate GUI interface. On the left, there's a navigation bar with 'Dashboard > Network > Static & Dynamic Routing'. Below it is a table titled 'Static & Dynamic Routing' with columns: Network, Gateway IP, Interfaces, Distance, Type, and Metric. A red box highlights the 'Metric' column header. To the right of the table is a 'Select Columns' dialog box with a list of checkboxes. The 'Metric' checkbox is checked and highlighted with a red box. A blue callout bubble points to this checkbox with the text 'Enable the Metric column (disabled by default)'. Below the table, a command-line interface (CLI) window displays the output of the command '# get router info routing-table all'. The CLI output lists several routes with their details like network, gateway, interfaces, and metrics.

Network	Gateway IP	Interfaces	Distance	Type	Metric
0.0.0.0/0	10.0.11.254	port2	10	Static	0
10.0.3.0/24	10.0.11.254	port2	120	RIP	2
10.0.4.0/24	10.0.11.254	port2	110	OSPF	2
10.0.5.0/24	10.0.11.254	port2	20	BGP	0
10.0.11.0/24	0.0.0.0	port2	0	Connected	0
192.168.0.0/16	0.0.0.0	port1	0	Connected	0

```
# get router info routing-table all
Codes: K - kernel, C - connected, S - stat
...output omitted...
Routing table for VRF=0
S* 0.0.0.0/0 [10/0] via 10.0.11.254, port2, [1/0]
R 10.0.3.0/24 [120/2] via 10.0.11.254, port2, 00:00:03, [1/0]
O 10.0.4.0/24 [110/2] via 10.0.11.254, port2, 00:11:29, [1/0]
B 10.0.5.0/24 [20/0] via 10.0.11.254 (recursive is directly connected, port2), 01:04:00, [1/0]
C 10.0.11.0/24 is directly connected, port2
C 192.168.0.0/24 is directly connected, port1
```

Each of the routes listed in the routing table includes several attributes with associated values.

The **Network** column lists the destination IP address and subnet mask to match. The **Interfaces** column lists the interface to use to deliver the packet.

The **Distance**, **Metric**, and **Priority** attributes are used by FortiGate to make various route selection decisions. You will learn about each of these in this lesson.

This slide also shows the command you can run to display the routing table on the FortiGate CLI. The `get router info routing-table all` command displays the same route entries as the routing monitor widget on the FortiGate GUI.

DO NOT REPRINT**© FORTINET**

Distance

- First tiebreaker for duplicate routes (best route selection)
 - The lower the distance, the higher the preference
 - Set by the administrator (except connected routes)
- Best route selection
 - Route with lowest distance is installed in the RIB
 - Standby routes (higher distance) are not installed in the RIB
 - They are installed in the routing table database
- Avoid multiple equal-distance duplicate routes but different protocol
 - FortiGate keeps the route that was learned last



Distance, or administrative distance, is the first tiebreaker that routers use to determine the best route for a particular destination. If there are two or more routes to the same destination (duplicate routes), the lowest-distance route is considered the best route and, as a result, is installed in the routing table. Other lower-distance routes to the same destination are standby routes and, as a result, are not installed in the routing table. Instead, they are installed in the routing table database.

DO NOT REPRINT

© FORTINET

Distance (Contd)

- Default distance per route type:

Connected	Static (SD-WAN zone)	Static (DHCP)	Static (Manual)	Static (IKE)	EBGP	OSPF	IS-IS	RIP	IBGP
0	1	5	10	15	20	110	115	120	200

Dashboard > Network > Static & Dynamic Routing

Network	Gateway IP	Interface	Distance	Type	Metric
0.0.0.0/0	10.200.1.254	port1	10	Static	0
10.0.1.0/24	0.0.0.0	port3	0	Connected	0
10.0.3.0/24	10.0.1.200	port3	200	BGP	0
10.0.4.0/24	10.0.1.200	port3	110	OSPF	2
10.0.5.0/24	10.0.1.200	port3	120	RIP	2
10.200.1.0/24	0.0.0.0	port1	0	Connected	0
10.200.2.0/24	0.0.0.0	port2	0	Connected	0
172.16.100.0/24	0.0.0.0	port8	0	Connected	0



You can set the distance for all route types except connected and IS-IS routes—both are hardcoded and their distance value cannot change. This slide shows the default values per type of route.

In case FortiGate learns two equal-distance routes to the same destination but that are sourced from different protocols, then FortiGate installs in the routing table the route that was learned *last*. For example, if you set the distance of BGP routes to 110, and there is another OSPF route to the same destination using the default administrative distance (110), then FortiGate keeps whichever route was learned last in the routing table. Because this behavior can lead to different results based on the timing of events, then it's not recommended to configure different-protocol routes with the same distance.

DO NOT REPRINT

© FORTINET

Metric

- Tiebreaker for same-protocol duplicate dynamic routes
 - The lower the metric, the higher the preference
- Best route is installed in the routing table and other duplicate routes in the routing table database
- The calculation method differs among routing protocols

Dashboard > Network > Static & Dynamic Routing

Network	Gateway IP	Interface	Distance	Type	Metric
0.0.0.0/0	10.200.1.254	port1	10	Static	0
10.0.1.0/24	0.0.0.0	port3	0	Connected	0
10.0.3.0/24	10.0.1.200	port3	200	BGP	0
10.0.4.0/24	10.0.1.200	port3	110	OSPF	2
10.0.5.0/24	10.0.1.200	port3	120	RIP	2
10.200.1.0/24	0.0.0.0	port1	0	Connected	0
10.200.2.0/24	0.0.0.0	port2	0	Connected	0
172.16.100.0/24	0.0.0.0	port8	0	Connected	0



© Fortinet Inc. All Rights Reserved.

16

When a dynamic route protocol learns two or more routes to the same destination, it uses the metric as a tiebreaker to identify the best route. The lower the metric, the higher the preference. The dynamic routing protocol then installs the best route in the routing table and the higher-metric routes in the routing table database. Note that the metric is used as tiebreaker for same-protocol dynamic routes, and *not* between different-protocol dynamic routes.

The metric calculation differs among routing protocols, and the details are not covered in this course. For example, RIP uses the hop count, which is the number of routers the packet must pass through to reach the destination. OSPF uses cost, which is determined by the link bandwidth.

DO NOT REPRINT

© FORTINET

Priority

- Tiebreaker for static routes with same distance
 - All static routes with equal distance are installed in the routing table, even if they have different priorities
 - Routes with lower priorities are preferred routes
 - Default value: 1
- Best route is used during route lookup

Dashboard > Network > Static & Dynamic

Network	Gateway IP	Distance	Type	Metric	Priority
0.0.0.0/0	10.1.254	10	Static	0	1
0.0.0.0/0	10.1.254	10	Static	0	10
10.1.0.0/24	0.0.0.0	0	Connected	0	0
10.1.4.0/24	10.1.0.100	110	OSPF	2	1
10.1.5.0/24	0.0.0.0	0	Connected	0	0
100.0.0.0/8	10.1.254	120	RIP	2	1
100.64.1.0/24	10.1.0.254	20	BGP	0	1
100.75.5.1/32	10.1.5.254	120	RIP	2	1

Network > Static Routes

Edit Static Route

Destination	Subnet Internet Service
0.0.0.0/0.0.0.0	
Gateway Address	10.1.0.254
Interface	port1
Administrative Distance	10
Comments	Write a comment... /255
Status	Enabled
Advanced Options	
Priority	10

Priority set to 10
(default value is 1)



When there are two or more duplicate static routes that have the same distance, FortiGate installs all of them in the routing table.

The priority setting enables administrators to break the tie among *static* routes. During the route lookup process, FortiGate selects the best route—that is, the static route with the lowest priority among all the equal-distance, duplicate static routes. The lower the priority value, the higher the preference.

The priority attribute applies to all routes except connected routes and is set to 1 by default.

For dynamic routes, you can change the priority of BGP routes only. The priority of other dynamic routes is hardcoded to 1. In dynamic routes, the priority value is useful for advanced routing deployments involving SD-WAN and multiple virtual routing and forwarding (VRF) IDs. A detailed explanation of how the priority attribute is beneficial for such cases is outside the scope of this course.

For static routes, you can configure the priority settings in the **Advanced Options** section, as shown on this slide.

To view the priority in the routing monitor widget, you must enable the **Priority** column (disabled by default). You can also view the priority in the routing table on the FortiGate CLI.

DO NOT REPRINT**© FORTINET**

Routing Table—CLI

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

Routing table for VRF=0
S* 0.0.0.0/0 [10/0] via 10.200.1.254, port1, [1/0]
C 10.0.1.0/24 is directly connected, port3
C 10.200.1.0/24 is directly connected, port1
C 10.200.2.0/24 is directly connected, port2
C 172.16.100.0/24 is directly connected, port8
```

Source

Distance/Metric

Priority/Weight



The CLI command shown on this slide displays all entries in the routing table. The routing table displays the routes that make it the best active routes to a destination.

The left-most column indicates the route source. Route attributes are shown inside square brackets. The first number, in the first pair of attributes, is distance, which applies to both dynamic and static routes. The second number is metric, which applies to dynamic routes only.

Static routes and dynamic routes also have priority and weight attributes, which are shown as the last pair of attributes for the respective route. In the case of dynamic routes, the weight is always zero.

This command doesn't show standby or inactive routes, which are present in the routing table database only. For example, when two static routes to the same destination subnet have different distances, the one with the lower distance is installed in the routing table, and the one with the higher distance in the routing table database.

DO NOT REPRINT

© FORTINET

GUI Route Lookup Tool

- Look up route by:
 - Destination address (required)
 - Destination port, source address, source port, protocol, and source interface (optional)
- If all criteria are provided:
 - FortiGate checks both routing table and policy route table entries
 - Otherwise, FortiGate checks routing table entries only
- Matching route is highlighted

The screenshot illustrates the FortiGate GUI interface for route lookup. At the top, a navigation bar shows 'Dashboard > Network > Static & Dynamic Routing'. Below it, a 'Route Lookup' dialog box is open, with its title bar also reading 'Route Lookup'. The dialog contains fields for Destination (8.8.8.8), Destination port (1-65535), Source (IP or FQDN), Source port (1-65535), Protocol (TCP), and Source Interface. A red box highlights the 'Destination' field. A blue callout bubble points to this field with the text 'You are redirected to the policy page if you enter all attributes'. An arrow points from the 'Route Lookup' dialog to a table below. The table has columns: Network, Gateway IP, Interfaces, Distance, and Type. It lists three routes: 0.0.0.0/0 (Gateway IP 10.200.1.254, Interface port1, Distance 10, Type Static), 10.0.1.0/24 (Gateway IP 0.0.0.0, Interface port3, Distance 0, Type Connected), and 10.200.1.0/24 (Gateway IP 0.0.0.0, Interface port1, Distance 0, Type Connected). The first row (the static default route) is highlighted with a red box and a blue callout bubble pointing to it with the text 'Matching route'.

You can perform a route lookup on the routing monitor widget by clicking **Route Lookup**. Then, you must indicate at least the destination address to look up for, and optionally, the destination port, source address, source port, protocol, and source interface.

The way the route lookup works is as follows:

- If you don't provide all lookup criteria, FortiGate considers only the routing table entries. FortiGate then highlights the matching route, if any.
- If you provide all lookup criteria, FortiGate considers both routing table and policy table entries. If the lookup matches a policy route, the GUI redirects you to the policy route page, and then highlights the corresponding matching policy route.

The example on this slide shows a route lookup tool for 8.8.8.8 and TCP as destination address and protocol, respectively. Because the administrator doesn't provide all criteria, FortiGate considers the routing table entries only. Then, the route lookup highlights the static default route as the matching route.

DO NOT REPRINT**© FORTINET**

Reverse Path Forwarding

- IP anti-spoofing protection
- Source IP is checked for a return path
- RPF check is only carried out on:
 - The first packet in the session, not on a reply
- Two modes:
 - Feasible path (default; formerly loose)
 - Return path doesn't have to be the best route
 - Strict
 - Return path must be the best route
- If RPF check fails, debug flow shows:
 - reverse path check fail, drop

- Set RPF mode (default = disable):

```
config system settings
  set strict-src-check [disable | enable]
end
```

Strict mode

- Disable RPF (default = enable):

```
config system interface
  edit <interface>
    set src-check disable
  next
end
```



The RPF check is a mechanism that protects FortiGate and your network from IP spoofing attacks by checking for a return path to the source in the routing table.

The premise behind the RPF check is that if FortiGate receives a packet on an interface, and FortiGate doesn't have a route to the packet source address through the incoming interface, then the source address of the packet could have been forged, or the packet was routed incorrectly. In either case, you want to drop that unexpected packet, so it doesn't enter your network.

FortiGate performs an RPF check only on the first packet of a new session. That is, after the first packet passes the RPF check and FortiGate accepts the session, FortiGate doesn't perform any additional RPF checks on that session.

There are two RPF check modes:

- Feasible path: Formerly known as loose, it's the default mode. In this mode, FortiGate verifies that the routing table contains a route that matches the source address of the packet and the incoming interface. The matching route doesn't have to be the best route in the routing table for that source address. It just has to match the source address and the incoming interface of the packet.
- Strict: In this mode, FortiGate also verifies that the matching route is the best route in the routing table. That is, if the routing table contains a matching route for the source address and incoming interface, but there is a better route for the source address through another interface, then, the RPF check fails.

This slide also shows how to change the RPF check mode on the FortiGate CLI, as well as how to disable the RPF check on the interface level.

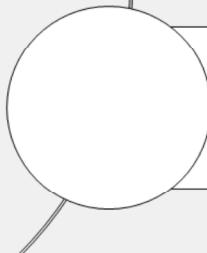
DO NOT REPRINT

© FORTINET

Lesson Progress



Routing on FortiGate



ECMP Routing



© Fortinet Inc. All Rights Reserved. 21

Good job! You now understand routing on FortiGate.

Now, you will learn about equal cost multipath (ECMP) routing.

DO NOT REPRINT

© FORTINET

ECMP Routing

Objectives

- Implement route redundancy and load balancing



© Fortinet Inc. All Rights Reserved. 22

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

By demonstrating competence in ECMP routing, you will be able to implement routing load balancing.

DO NOT REPRINT

© FORTINET

ECMP

- Same-protocol routes with equal:
 - Destination subnet
 - Distance
 - Metric
 - Priority
- ECMP routes are installed in the RIB
 - Traffic is load balanced among routes



So far, you've learned about the different route attributes that FortiGate looks at to identify the best route to a destination.

But what happens when two or more routes of the same type have the same destination, distance, metric, and priority? These routes are called equal cost multipath (ECMP) routes, and FortiGate installs all of them in the routing table. FortiGate also load balances the traffic among the ECMP routes.

DO NOT REPRINT
© FORTINET

ECMP (Contd)

Two ECMP static routes

Two ECMP BGP routes

Two ECMP OSPF routes

Dashboard > Network > Static & Dynamic

Network	Gateway IP	Interfaces	Distance	Type	Metric	Priority
0.0.0.0/0	10.200.1.254	port1	10	Static	0	5
0.0.0.0/0	10.200.2.254	port2	10	Static	0	5
10.0.1.0/24	0.0.0.0	port3	0	Connected	0	0
10.0.2.0/24	0.0.0.0	port4	0	Connected	0	0
10.0.3.0/24	10.0.1.200	port3	200	BGP	0	1
10.0.3.0/24	10.0.2.200	port4	200	BGP	0	1
10.0.4.0/24	10.0.1.200	port3	110	OSPF	2	1
10.0.4.0/24	10.0.2.200	port4	110	OSPF	2	1
10.200.1.0/24	0.0.0.0	port1	0	Connected	0	0
10.200.2.0/24	0.0.0.0	port2	0	Connected	0	0

```
# get router info routing-table all
...output omitted...
Routing table for VRF=0
S*   0.0.0.0/0 [10/0] via 10.200.1.254, port1, [5/0]
      [10/0] via 10.200.2.254, port2, [5/0]
C    10.0.1.0/24 is directly connected, port3
C    10.0.2.0/24 is directly connected, port4
B    10.0.3.0/24 [200/0] via 10.0.1.200 (recursive is directly connected, port3), 00:07:04, [1/0]
      [200/0] via 10.0.2.200 (recursive is directly connected, port4), 00:07:04, [1/0]
O    10.0.4.0/24 [110/2] via 10.0.1.200, port3, 00:15:12, [1/0]
      [110/2] via 10.0.2.200, port4, 00:15:12, [1/0]
C    10.200.1.0/24 is directly connected, port1
C    10.200.2.0/24 is directly connected, port2
```



© Fortinet Inc. All Rights Reserved.

24

The example on this slide shows two ECMP static routes, two ECMP BGP routes, and two ECMP OSPF routes. For each ECMP group, the destination subnet, distance, metric, and priority are the same.

The result is that FortiGate installs both routes of each ECMP group in the routing table. This lesson, however, focuses on ECMP static routes only.

DO NOT REPRINT**© FORTINET**

ECMP Load Balancing Algorithms

- Source IP (default)
 - Sessions sourced from the same address use the same route
- Source-destination IP
 - Sessions with the same source *and* destination address pair use the same route
- Weighted
 - Applies to static routes only
 - Sessions are distributed based on route, or interface weights
 - The higher the weight, the more sessions are routed through the selected route
- Usage (spillover)
 - One route is used until the bandwidth threshold is reached, then the next route is used



ECMP can load balance sessions using one of the following four algorithms:

- Source IP: This is the default algorithm. FortiGate uses the same ECMP route to route sessions sourced from the same address.
- Source-destination IP: FortiGate uses the same ECMP route to route sessions with the same source-destination IP address pair.
- Weighted: Applies to static routes only. FortiGate load balances sessions based on the route weight or the respective interface weight. The higher the weight, the more sessions FortiGate routes through the selected route.
- Usage (spillover): FortiGate sends sessions to the interface of the first ECMP route until the bandwidth of the interface reaches the configured spillover limit. After the spillover limit is reached, FortiGate uses the interface of the next ECMP route.

DO NOT REPRINT**© FORTINET**

Configuring ECMP

- If SD-WAN is disabled, the ECMP algorithm is set on the CLI:

```
config system settings
  set v4-ecmp-mode [source-ip-based | weight-based | usage-based | source-dest-ip-based]
end
```

- Configure weight values on the CLI on the interface level (left) and route level (right):

```
config system interface
  edit <interface name>
    set weight <0-255>
  next
end
```

Interface weight has precedence over the weight of a static route using the interface

```
config router static
  edit <id>
    set weight <0-255>
  next
end
```

- Configure spillover thresholds on the CLI (kbps):

```
config system interface
  edit <interface name>
    set spillover-threshold <0-16776000>
    set ingress-spillover-threshold <0-16776000>
  next
end
```



If SD-WAN is disabled, you can change the ECMP load balancing algorithm on the FortiGate CLI using the commands shown on this slide.

When SD-WAN is enabled, FortiOS hides the `v4-ecmp-mode` setting and replaces it with the `load-balance-mode` setting under `config system sdwan`. That is, when you enable SD-WAN, you control the ECMP algorithm with the `load-balance-mode` setting.

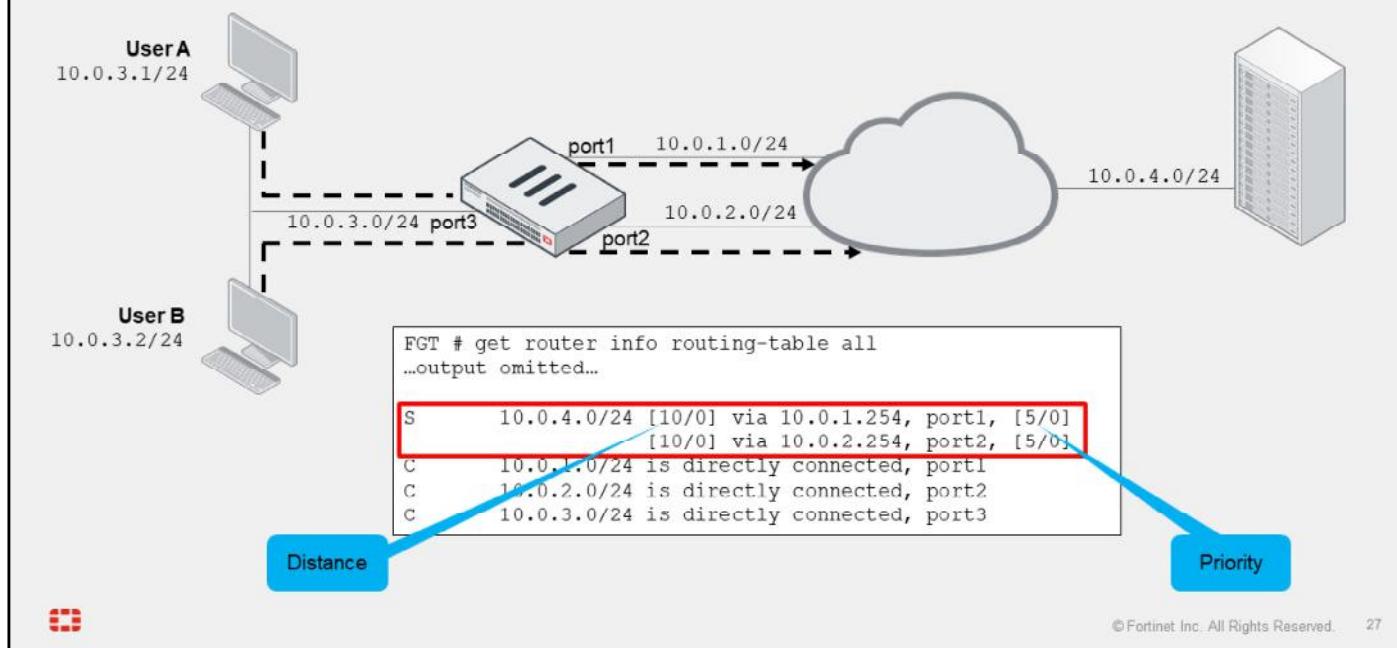
For spillover to work, you must also configure the egress and ingress spillover thresholds, as shown on this slide. If you disable SD-WAN, FortiGate selects the lowest numbered interface first. The thresholds are set to 0 by default, which disables spillover check.

For a weighted algorithm, you must configure the weights at the interface level or route level, as shown on this slide. If two or more routes are added to the routing table, and you set `v4-ecmp-mode` to `weight-based`, FortiGate routes sessions based on the weight value of each route.

DO NOT REPRINT

© FORTINET

ECMP Example



In the scenario shown on this slide, FortiGate has ECMP routes for the 10.0.4.0/24 subnet on port1 and port2. Using the default ECMP algorithm (source IP based), FortiGate may use any of the two routes to route traffic from user A and user B.

In the example shown on this slide, FortiGate selects the route over port1 for user A, and the route over port2 for user B. FortiGate continues to use the same selected routes for the same traffic. If the route over port1 is removed from the routing table, FortiGate automatically starts to forward the traffic sourced from both users and destined to 10.0.4.0/24 through port2.

ECMP enables you to use multiple paths for the same destination, as well as provide built-in failover. Usually, you want to use ECMP for mission-critical services that require high availability. Another reason to use ECMP is for bandwidth aggregation. That is, you can leverage the bandwidth of multiple links by load balancing sessions across them.

While ECMP enables you to leverage multiple WAN links on FortiGate, you may want to use SD-WAN because of the additional benefits.

DO NOT REPRINT

© FORTINET

Default ECMP Algorithm vs. SD-WAN ECMP Algorithm

ECMP (v4-ecmp-mode)	SD-WAN (load-balance-mode)
Both control ECMP algorithms	
Not available when SD-WAN is enabled	Not available when SD-WAN is disabled
Doesn't support volume algorithm	Support volume algorithm
Uses the weight defined in the static route	Uses the SD-WAN member weight
Uses the interface spillover thresholds	Uses the SD-WAN member spillover thresholds

- **Volume algorithm:**
 - FortiGate tracks the cumulative number of bytes of the member
 - The higher the member weight, the higher the target volume, the more traffic is sent to it



When you enable SD-WAN, FortiOS hides the v4-ecmp-mode setting and replaces it with the load-balance-mode setting under config system sdwan. That is, after you enable SD-WAN, you now control the ECMP algorithm with the load-balance-mode setting.

There are some differences between the two settings. The main difference is that load-balance-mode supports the volume algorithm, and v4-ecmp-mode does not. In addition, the related settings such as weight and spillover thresholds are configured differently. That is, when you enable SD-WAN, the weight and spillover thresholds are defined on the SD-WAN member configuration. When you disable SD-WAN, the weight and spillover thresholds are defined on the static route and interface settings, respectively.

When you set the ECMP algorithm to volume—this is when SD-WAN is enabled, FortiGate load balances sessions across members based on the measured interface volume and the member weight. That is, the volume algorithm instructs FortiGate to track the cumulative number of bytes of each member and to distribute sessions based on the weight. The higher the weight, the higher the target volume of the interface and, as a result, the more traffic FortiGate sends to it.

DO NOT REPRINT

© FORTINET

Knowledge Check

1. The priority attribute is a tiebreaker for which type of routes?
 A. Static
 B. Connected

2. Which attribute does FortiGate use to determine the *best* route for same-protocol, duplicate dynamic routes?
 A. Priority
 B. Metric

3. What is the default ECMP algorithm on FortiGate?
 A. Weighted
 B. Source IP



DO NOT REPRINT

© FORTINET

Lesson Progress



Routing on FortiGate



ECMP Routing



© Fortinet Inc. All Rights Reserved. 30

Congratulations! You have completed this lesson.

Now, you will review the objectives covered in this lesson.

DO NOT REPRINT

© FORTINET

Review

- ✓ Configure static routing
- ✓ Interpret the routing table on FortiGate
- ✓ Implement route redundancy and load balancing



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

By mastering the objectives covered in this lesson, you learned how to configure, monitor, and load balance routes on FortiGate.

DO NOT REPRINT

© FORTINET

FORTINET
Training Institute

FortiOS Administrator

Firewall Authentication

FortiOS 7.6

Last Modified: 6 October 2025

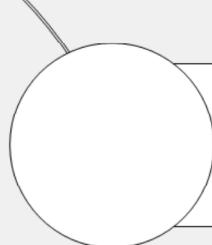
© Fortinet Inc. All Rights Reserved. 1

In this lesson, you will learn about using authentication on the firewall policies of FortiGate.

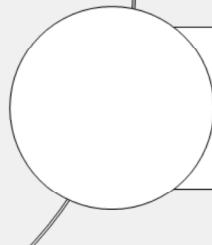
DO NOT REPRINT

© FORTINET

Lesson Overview



Remote Authentication



Methods of Authentication



© Fortinet Inc. All Rights Reserved.

2

In this lesson, you will learn about the topics shown on this slide.

DO NOT REPRINT**© FORTINET**

Remote Authentication

Objectives

- Configure a remote LDAP authentication server on FortiGate
- Configure a remote RADIUS authentication server on FortiGate



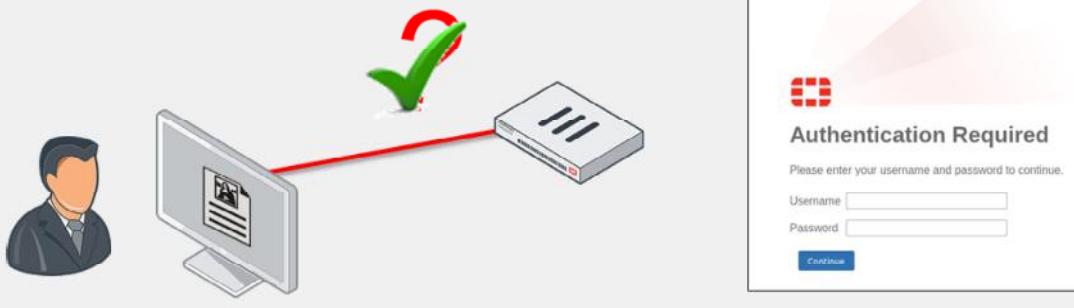
After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating a competent understanding of remote authentication, you will be able to enforce authentication on specific users and user groups.

DO NOT REPRINT
© FORTINET

Firewall Authentication

- Includes the authentication of users and user groups
 - It is more reliable than just IP address and device-type authentication
 - Users must authenticate by entering valid credentials
- After FortiGate identifies the user or device, FortiGate applies firewall policies and profiles to allow or deny access to each specific network resource



© Fortinet Inc. All Rights Reserved.

4

Traditional firewalls grant network access by verifying the source IP address and device. This is inadequate and can pose a security risk because the firewall cannot determine who is using the device to which it is granting access.

FortiGate includes authentication of users and user groups. As a result, you can follow individuals across multiple devices.

Where access is controlled by a user or user group, users must authenticate by entering valid credentials (such as username and password). After FortiGate validates the user, FortiGate applies firewall policies and profiles to allow or deny access to specific network resources.

DO NOT REPRINT**© FORTINET**

FortiGate Methods of Firewall Authentication

- Local password authentication
 - Username and password stored on FortiGate
- Server-based password authentication (also called remote password authentication)
 - Password stored on a POP3, RADIUS, LDAP, or TACACS+ server
- Two-factor authentication
 - Enabled on top of an existing method
 - Requires something you know and something you have (token or certificate)



FortiGate supports multiple methods of firewall authentication:

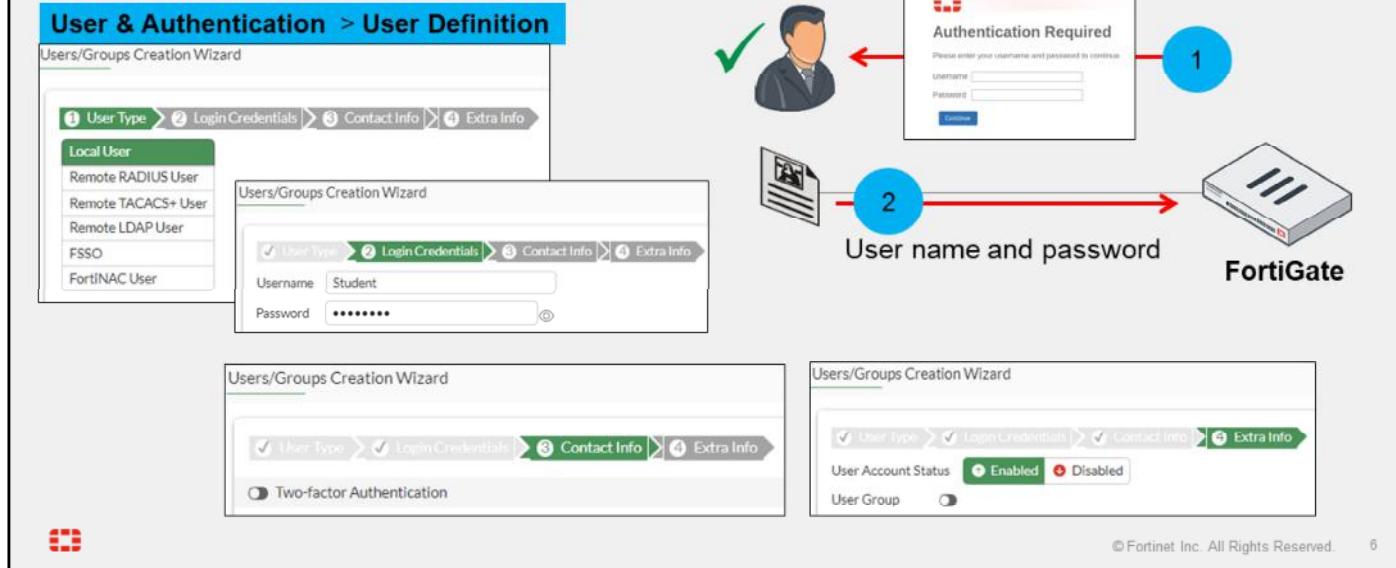
- Local password authentication
- Server-based password authentication (also called remote password authentication)
- Two-factor authentication
This is a system of authentication that is enabled on top of an existing method—it cannot be enabled without first configuring one of the other methods. It requires something you know, such as a password, and something you have, such as a token or certificate.

During this lesson, you will learn about each method of firewall authentication in detail.

DO NOT REPRINT
© FORTINET

Local Password Authentication

- User accounts stored locally on FortiGate
 - Works well for single FortiGate installations



The simplest method of authentication is local password authentication. User account information (username and password) is stored locally on the FortiGate device. This method works well for a single FortiGate installation.

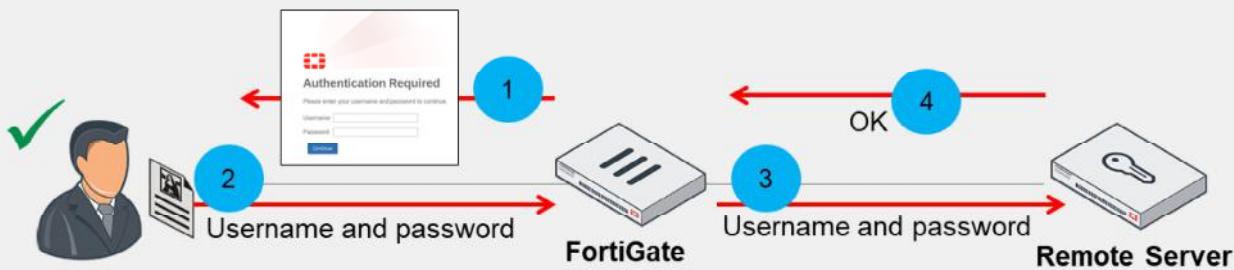
Local accounts are created on the **User Definition** page where a wizard takes you through the process. For local password authentication, select **Local User** as the user type and create a username and password. If desired, you can also add email and SMS information to the account, enable two-factor authentication, and add the user to a preconfigured user group.

After you create the user, you can add the user—or any preconfigured user group in which the user is a member—to a firewall policy, in order to authenticate. You will learn about user groups and firewall policies in this lesson.

DO NOT REPRINT
© FORTINET

Server-Based Password Authentication

- Accounts are stored on a remote authentication server
- Administrators can do one of the following:
 - Create an account for the user locally and specify the server to verify the password
 - Add the authentication server to a user group
 - All users in that server become members of the group



© Fortinet Inc. All Rights Reserved.

7

When server-based password authentication is used, a remote authentication server authenticates users. This method is desirable when multiple FortiGate devices need to authenticate the same users or user groups, or when adding FortiGate to a network that already contains an authentication server.

When you use a remote authentication server to authenticate users, FortiGate sends the user's entered credentials to the remote authentication server. The remote authentication server responds by indicating whether the credentials are valid or not. If valid, FortiGate consults its configuration to deal with the traffic. Note that it is the remote authentication server—not FortiGate—that evaluates the user credentials.

When the server-based password authentication method is used, FortiGate does not store all (or some configurations, any) of the user information locally.

DO NOT REPRINT
© FORTINET

Server-Based Password Authentication—Users

- Create user accounts on FortiGate
 - Select remote server type and point to preconfigured remote server
 - Add user to a group
- Add the remote authentication server to user groups

The screenshot shows the 'User & Authentication > User Definition' section of the FortiGate interface. It displays two separate windows: 'Edit User Group' and 'User & Authentication > User Definition'.

Edit User Group: This window shows a user group named 'Remote-users' assigned to the 'Firewall' type. A blue callout labeled 'Option 2' points to the 'Remote Groups' section, which contains a table with columns 'Remote Server' and 'Group Name'. The table shows an entry for 'FortiAuth-RADIUS' under 'Remote Server' and 'Remote-users' under 'Group Name'. A blue box highlights this table with the text 'Must be preconfigured on FortiGate'.

User & Authentication > User Definition: This window shows the 'User Type' step of a 'Users/Groups Creation Wizard'. It lists several options: 'Local User', 'Remote RADIUS User' (highlighted with a red box), 'Remote TACACS+ User', 'Remote LDAP User', 'FSSO', and 'FortiNAC User'. A blue callout labeled 'Option 1' points to the 'Remote RADIUS User' option. Another blue callout points to the 'Username' field with the text 'Must specify username'. A third blue callout points to the 'RADIUS Server' dropdown with the text 'Must be preconfigured on FortiGate'.



© Fortinet Inc. All Rights Reserved.

8

You can configure FortiGate to use external authentication servers in the following two options:

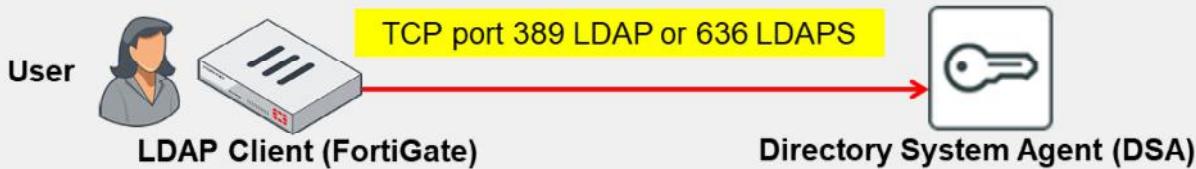
- Option 1: Create user accounts on FortiGate. With this method, you must select the remote authentication server type (RADIUS, TACACS+, or LDAP), point FortiGate to your preconfigured remote authentication server, and add the user to an appropriate group. The username needs to match an existing user account on the Radius server. This is usually done when you want to add two-factor authentication to your remote users. Remember, POP3 is only configurable through the CLI.
- Option 2: Add the remote authentication server to user groups. With this method, you must create a user group and add the preconfigured remote server to the group. This setup allows you to select one or more pre-existing groups from the Radius server, enabling any user within those groups to be authenticated. Accordingly, any user who has an account on the remote authentication server can authenticate. If you are using other types of remote servers, such as an LDAP server, as the remote authentication server, you can control access to specific LDAP groups, as defined on the LDAP server.

Similar to local password authentication, you must then add the preconfigured user group (in which the user is a member) to a firewall policy in order to authenticate. You will learn about user groups and firewall policies later in this lesson.

DO NOT REPRINT**© FORTINET**

LDAP Overview

- LDAP is an application protocol for accessing and maintaining distributed directory information services



- LDAP maintains authentication data, including:
 - Departments, people (and groups of people), passwords, email addresses, and printers
- LDAP consists of a data-representation scheme, a set of defined operations, and a request-and-response network
- Binding is the operation in which the LDAP server authenticates the user



Lightweight Directory Access Protocol (LDAP) is an application protocol used for accessing and maintaining distributed directory information services.

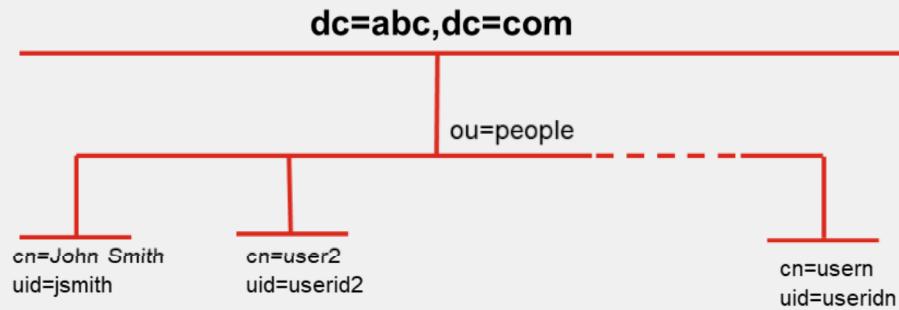
The LDAP protocol is used to maintain authentication data that may include departments, people, groups of people, passwords, email addresses, and printers. LDAP consists of a data-representation scheme, a set of defined operations, and a request-and-response network.

The LDAP protocol includes a number of operations that a client can request, such as search, compare, and add or delete an entry. Binding is the operation in which the LDAP server authenticates the user. If the user is successfully authenticated, binding allows the user access to the LDAP server, based on that user's permissions.

Note that it is important to understand that LDAP on port 389 is not secure because it sends the password in clear text. It is highly recommended to use LDAPS which is more secure.

DO NOT REPRINT**© FORTINET**

LDAP Structure



The LDAP structure is similar to a tree that contains entries (objects) in each branch. An LDAP server hierarchy often reflects the hierarchy of the organization it serves. The root represents the organization itself, usually defined as domain component (DC), and a DNS domain, such as abc.com (because the name contains a dot, it is written as two parts separated by a comma: `dc=abc,dc=com`). You can add additional levels of hierarchy as needed, such as organizational unit (ou), user group (cn), user (uid) and so on.

The example shown on this slide is an LDAP hierarchy in which all user account entries reside at the organization unit (OU) level, just below DC.

When requesting authentication, an LDAP client, such as a FortiGate device, must specify the part of the hierarchy where the user account record can be found. This is called the distinguished name (DN). In the example on this slide, DN is `ou=people,dc=abc,dc=com`.

The authentication request must also specify the particular user account entry. Although this is often called the common name (CN), the identifier you use is not necessarily CN. On a computer network, it is appropriate to use UID, the person's user ID, because that is the information that they will provide when they log in.

DO NOT REPRINT
© FORTINET

Configuring an LDAP Server on FortiGate

Directory tree attribute that identifies users

Part of the hierarchy where user records exist

Credentials for an LDAP administrator

User & Authentication > LDAP Servers	
Name	External_Server
Server IP/Name	10.0.1.150
Server Port	389
Common Name Identifier	uid
Distinguished Name	ou=Training,dc=trainingAD,dc=training
Exchange server	<input checked="" type="checkbox"/>
Bind Type	Simple <input type="radio"/> Anonymous <input checked="" type="radio"/> Regular
Username	uid=admin,dc=trainingAD,dc=training
Password	*****
Secure Connection	<input checked="" type="checkbox"/>
Connection status	Successful
<input type="button" value="Test Connectivity"/>	
<input type="button" value="Test User Credentials"/>	



On the **LDAP Servers** page, you can configure FortiGate to point to an LDAP server for server-based password authentication. The configuration depends heavily on the server's schema and security settings. Windows Active Directory (AD) is very common.

The **Common Name Identifier** setting is the attribute name you use to find the user name. Some schemas allow you to use the attribute `userid`. AD most commonly uses `sAMAccountName` or `cn`, but can use others as well.

The **Distinguished Name** setting identifies the top of the tree where the users are located, which is generally the `dc` value; however, it can be a specific container or OU. You must use the correct X.500 or LDAP format.

The **Bind Type** setting depends on the security settings of the LDAP server. You must use the setting **Regular** (to specify a regular bind) if you are searching across multiple domains and require the credentials of a user that is authorized to perform LDAP queries (for example, an LDAP administrator).

If you want a secure connection between FortiGate and the remote LDAP server, enable **Secure Connection** and include the LDAP server protocol (LDAPS or STARTTLS) as well as the CA certificate that verifies the server certificate. LDAPS uses port 636 for communication.

Test Connectivity tests only whether the connection to the LDAP server is successful or not. To test whether a user's credentials can successfully authenticate, you can use **Test User Credentials** or the CLI.

DO NOT REPRINT**© FORTINET**

RADIUS Overview

- RADIUS is a standard protocol that provides AAA services



© Fortinet Inc. All Rights Reserved.

12

RADIUS is much different from LDAP, because there is no directory tree structure to consider. RADIUS is a standard protocol that provides authentication, authorization, and accounting (AAA) services.

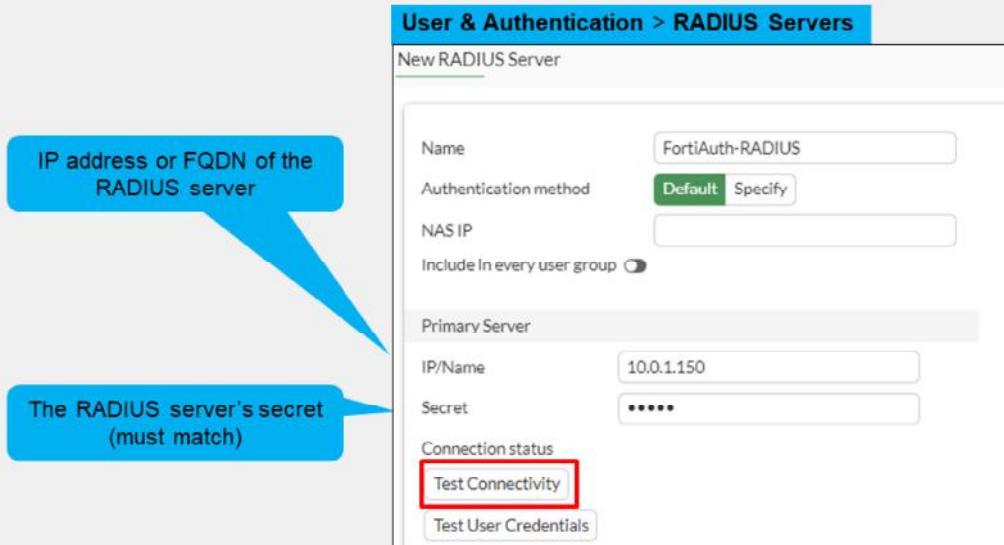
When a user is authenticating, the client (FortiGate) sends an ACCESS-REQUEST packet to the RADIUS server. The reply from the server is one of the following:

- ACCESS-ACCEPT, which means that the user credentials are correct
- ACCESS-REJECT, which means that the credentials are wrong
- ACCESS-CHALLENGE, which means that the server is requesting a secondary password ID, token, or certificate. This is typically the reply from the server when using two-factor authentication.

Not all RADIUS clients support the RADIUS challenge method.

DO NOT REPRINT
© FORTINET

Configuring a RADIUS Server on FortiGate



© Fortinet Inc. All Rights Reserved.

13

You can configure FortiGate to point to a RADIUS server for server-based password authentication through the **RADIUS Servers** page.

The **Primary Server IP/Name** setting is the IP address or FQDN of the RADIUS server.

The **Primary Server Secret** setting is the secret that was set up on the RADIUS server in order to allow remote queries from this client. Backup servers (with separate secrets) can be defined in case the primary server fails. Note that FortiGate must be listed on the RADIUS server as a client of that RADIUS server or else the server will not reply to queries done by FortiGate.

The **Authentication Method** setting refers to the authentication protocol that the RADIUS server supports. Options include chap, pap, mschap, and mschap2. If you select **Default**, FortiGate will use pap, mschap2, and chap (in that order).

The **Test Connectivity** button tests only whether the connection to the RADIUS server is successful or not. To test whether a user's credentials can successfully authenticate, you can use the **Test User Credentials** button or the CLI.

The **Include in every User Group** option adds the RADIUS server and all users who can authenticate against it, to every user group created on FortiGate. So, you should enable this option only in very specific scenarios (for example, when only administrators can authenticate against the RADIUS server and policies are ordered from least restrictive to most restrictive).

DO NOT REPRINT
© FORTINET

Testing the LDAP and RADIUS Query on the CLI

- diagnose test authserver ldap <server_name> <username> <password>
- Example:

```
# diagnose test authserver ldap External_Server aduser1 Training!
authenticate 'aduser1' against 'External_Server' succeeded!
Group membership(s) - CN=AD-users,OU=Training,DC=trainingAD,DC=training,DC=lab
```

- diagnose test authserver radius <server_name> <scheme> <user> <password>
- Example:

```
# diagnose test authserver radius FortiAuth-RADIUS pap student fortinet
authenticate 'student' against 'pap' succeeded, server=primary
assigned_rad_session_id=810153440 session timeout=0 secs!
Group membership(s) - remote-RADIUS-admins
```

Group memberships are provided by vendor-specific attributes configured on the RADIUS server



14

Use the `diagnose test authserver` command on the CLI to test whether a user's credentials can successfully authenticate. You want to ensure that authentication is successful, before implementing it on any of your firewall policies.

The response from the server reports success, failure, and group membership details.

Testing RADIUS is much the same as testing LDAP. Use the `diagnose test authserver` command on the CLI to test whether a user's credentials can successfully authenticate. Again, you should do this to ensure authentication is successful before implementing it on any of your firewall policies.

Like LDAP, it reports success, failure, and group membership details, depending on the server's response. Deeper troubleshooting usually requires RADIUS server access.

Note that Fortinet has a vendor-specific attributes (VSA) dictionary to identify the Fortinet-proprietary RADIUS attributes. This capability allows you to extend the basic functionality of RADIUS.

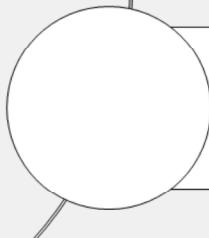
DO NOT REPRINT

© FORTINET

Lesson Progress



Remote Authentication



Methods of Authentication



© Fortinet Inc. All Rights Reserved.

15

Good job! You now understand how to configure remote authentication.

Now, you will learn about methods of authentication.

DO NOT REPRINT**© FORTINET**

Methods of Authentication

Objectives

- Deploy active and passive authentication
- Monitor firewall users using the FortiGate GUI



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

By demonstrating a competent understanding of firewall authentication methods, you will be able to describe and identify the supported methods of firewall authentication available on FortiGate.

DO NOT REPRINT**© FORTINET**

Two-Factor Authentication

- Strong authentication that improves security by preventing attacks associated with the use of static passwords alone
- Requires two independent methods of identifying a user:
 - Something you know, such as a password or PIN
 - Something you have, such as a token or certificate



Traditional user authentication requires your user name plus something you know, such as a password. The weakness in this traditional method of authentication is that if someone obtains your username, they need only your password to compromise your account. Furthermore, since people tend to use the same password across multiple accounts (some sites having more security vulnerabilities than others), accounts are vulnerable to attack, regardless of password strength.

Two-factor authentication, on the other hand, requires something you know, such as a password, and something you have, such as a token or certificate. Because this method places less importance on often vulnerable passwords, it makes compromising the account more complex for an attacker. You can use two-factor authentication on FortiGate with both user and administrator accounts. The user (or user group to which the user belongs) is added to a firewall policy in order to authenticate. Note that you cannot use two-factor authentication with explicit proxies.

DO NOT REPRINT**© FORTINET**

Two-Factor Authentication (Contd)

- A one-time password (OTP) can be used one time only
 - OTPs are more secure than static passwords
- Available on both user and administrator accounts
 - The user or user group is added to a firewall policy in order to authenticate
- Methods of OTP delivery include:
 - FortiToken 200 or FortiToken Mobile
 - Generates a six-digit code every 60 seconds based on a unique seed and GMT time
 - Email or SMS
 - An OTP is sent to the user's email or SMS
 - Email or SMS must be configured on the user's account
 - FortiToken mobile push
 - Supports two-factor authentication without requiring user to enter code
- NTP server recommended!



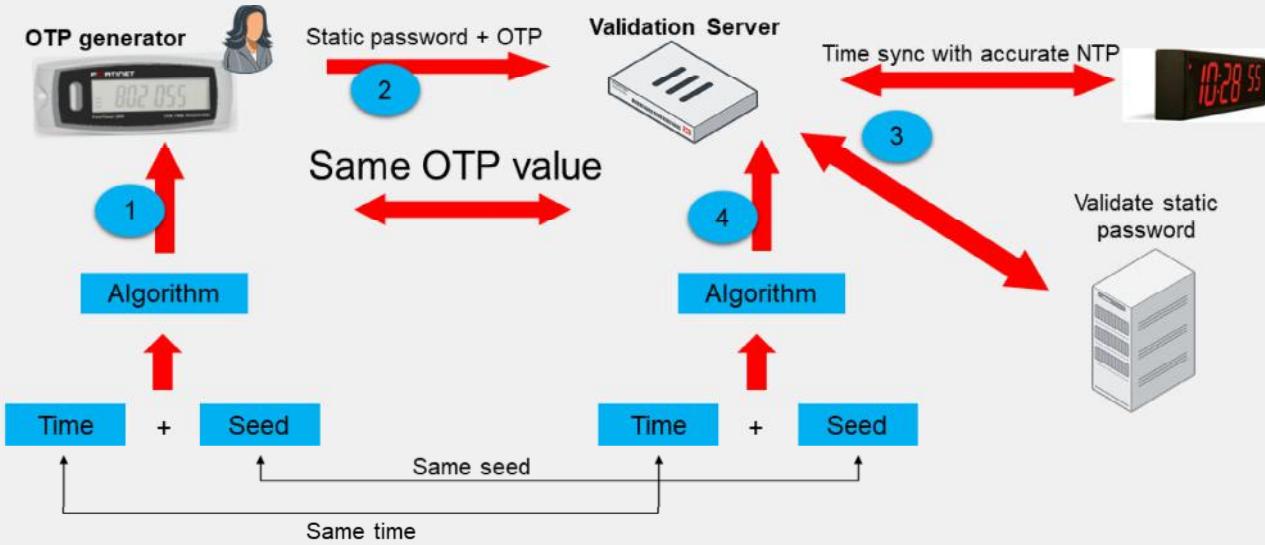
You can use OTPs as your second factor. OTPs are more secure than static passwords because the passcode changes at regular intervals and is valid for only a short amount of time. After you use the OTP, you can't use it again. So, even if it is intercepted, it is useless. FortiGate can deliver OTPs through tokens such as FortiToken 200 (hardware token) and FortiToken Mobile (software token), as well as through email or SMS. To deliver an OTP over email or SMS, the user account must contain user contact information.

FortiTokens and OTPs delivered through email and SMS are time based. FortiTokens, for example, generate a new, six-digit password every 60 seconds (by default). An NTP server is highly recommended to ensure the OTPs remain in sync. FortiToken Mobile Push allows users to accept the authorization request from their FortiToken mobile app, without the need to enter an additional code.

DO NOT REPRINT

© FORTINET

FortiTokens



© Fortinet Inc. All Rights Reserved. 19

Tokens use a specific algorithm to generate an OTP. The algorithm consists of:

- A seed: a unique, randomly-generated number that does not change over time
- The time: obtained from an accurate internal clock

Both seed and time use an algorithm that generates an OTP (or passcode) on the token. The passcode has a short life span, usually measured in seconds (60 seconds for FortiToken 200, possibly more or less for other RSA key generators). Once the life span ends, the algorithm generates a new passcode.

When using two-factor authentication with a token, the user must first log in with a static password followed by the passcode that the token generates. A validation server (FortiGate) receives the user's credentials and validates the static password. Next, the validation server validates the passcode. It does so by regenerating the same passcode using the seed and system time (which is synchronized with the one on the token) and comparing it with the passcode received from the user. If the static password is valid, and the OTP matches, the user is successfully authenticated. Again, both the token and the validation server must use the same seed and have synchronized system clocks. As such, it is crucial that you configure the date and time correctly on FortiGate, or link it to an NTP server (which is recommended).

DO NOT REPRINT
© FORTINET

Assigning a FortiToken to a User

The screenshot shows the FortiGate User & Authentication interface. On the left, the 'FortiTokens' page lists two tokens: 'FTKMOB6B91B33BE5' and 'FTKMOB6BCB3CCB31', both marked as 'Available'. A blue callout points to the second token with the text 'Two free FortiToken Mobile activations'. In the center, two 'New FortiToken' creation forms are shown, one for 'Hard Token' and one for 'Mobile Token'. On the right, a user profile for 'student' is being edited. The 'Two-factor Authentication' section is highlighted with a red box. It shows 'Authentication Type' set to 'FortiToken Cloud' and 'FortiToken' selected in the 'Token' dropdown, which contains 'FTKMOB6B91B33BE5'. A blue callout points to this section with the text 'Can add a user to a group and create a firewall policy based on the user group'. At the bottom right, there's a copyright notice: '© Fortinet Inc. All Rights Reserved. 20'.

- Enable **Two-factor Authentication** and select the registered FortiToken

You can add a FortiToken 200 or FortiToken Mobile to FortiGate on the **FortiTokens** page.

A hard token has a serial number that provides FortiGate with details on the initial seed value. If you have several hard tokens to add, you can import a text file, where one serial number is listed per line.

A soft token requires an activation code. Note that each FortiGate (and FortiGate VM) provides two free FortiToken Mobile activations. You must purchase any additional tokens from Fortinet.

You cannot register the same FortiToken on more than one FortiGate. If you want to use the same FortiToken for authentication on multiple FortiGate devices, you must use a central validation server, such as FortiAuthenticator. In that case, FortiTokens are registered and assigned to users on FortiAuthenticator, and FortiGate uses FortiAuthenticator as its validation server.

After you have registered the FortiToken devices with FortiGate, you can assign them to users to use as their second-factor authentication method. To assign a token, edit (or create) the user account and select **Enable Two-factor Authentication**. In the **Token** field, select the registered token you want to assign.

DO NOT REPRINT**© FORTINET**

Authentication Methods

- Active
 - User receives a login prompt
 - User manually enters credentials to authenticate
 - POP3, LDAP, RADIUS, Local, and TACACS+
- Passive
 - User does not receive a login prompt from FortiGate
 - Credentials are determined automatically
 - Method varies depending on type of authentication used
 - FSSO, RSSO, and NTLM



All the authentication methods you've learned about—local password authentication, server-based authentication, and two-factor authentication—use active authentication. Active authentication means that users are prompted to manually enter their login credentials before being granted access.

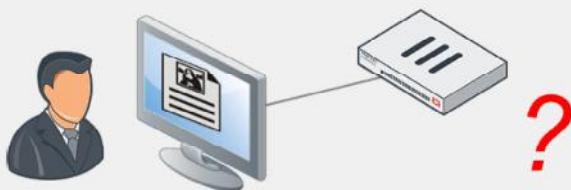
But not all users authenticate in the same way. Some users can be granted access transparently, because user information is determined without asking the user to enter their login credentials. This is known as passive authentication. Passive authentication occurs with the single sign-on method for server-based password authentication: FSSO, RSSO, and NTLM.

DO NOT REPRINT

© FORTINET

Firewall Policy—Source

- Firewall policies can use user and user group objects to define the source. The objects include:
 - Local firewall accounts
 - External (remote) server accounts
 - PKI (certificate) users
 - FSSO users
- Anyone who belongs to the group and provides correct information will have a successful authentication



© Fortinet Inc. All Rights Reserved.

22

Policies & Objects > Firewall Policy

Edit Policy

ID	1
Name	Full_Access
Schedule	always
Action	<input checked="" type="checkbox"/> ACCEPT <input type="checkbox"/> DENY <input type="checkbox"/> IPsec
Type	Standard ZTNA
Incoming Interface	LAN (port1)
Outgoing Interface	ISP1 (port1)
Source & Destination Show logic	
Source	LOCAL_SUBNET
User/group	External-Server-Users
Security profile tag	
Destination	all
Negate destination	
Service	Web Access FTP
Select Entries	
Search	User
— User (3) guest student Student	
— User Group (3) External-Server-Users Guest-group SSO_Guest_Users	

A firewall policy consists of access and inspection rules (compartmentalized sets of instructions) that tell FortiGate how to handle traffic on the interface whose traffic they filter. After the user makes an initial connection attempt, FortiGate checks the firewall policies to determine whether to accept or deny the communication session. However, a firewall policy also includes a number of other instructions, such as those dealing with authentication. You can use the source of a firewall policy for this purpose. The source of a firewall policy must include the source address (IP address), but you can also include the user and user group. In this way, any user, or user group that is included in the source definition for the firewall policy can successfully authenticate.

User and user group objects can consist of local firewall accounts, external server accounts, PKI users, and FSSO users.

DO NOT REPRINT
© FORTINET

Protocols

- A firewall policy must allow a protocol in order to show the authentication dialog that is used in active authentication:
 - HTTP
 - HTTPS
 - FTP
 - Telnet
- All other services are not allowed until the user has authenticated successfully through one of the protocols listed above



As well as the DNS service, the firewall policy must specify the allowed protocols, such as HTTP, HTTPS, FTP, and Telnet. If the firewall policy that has authentication enabled does not allow at least one of the supported protocols used for obtaining user credentials, the user will not be able to authenticate.

Protocols are required for all authentication methods that use active authentication (local password authentication, server-based password authentication, and two-factor authentication). Active authentication prompts the user for user credentials based on the following:

- The protocol of the traffic
- The firewall policy

Passive authentication, on the other hand, determines the user identity behind the scenes, and does not require any specific services to be allowed within the policy.

DO NOT REPRINT**© FORTINET**

Firewall Policy—Service

- DNS traffic can be allowed if user has not authenticated yet**
 - Hostname resolution is often required by the application layer protocol (HTTP/HTTPS/FTP/Telnet) that is used to authenticate
 - DNS service must be explicitly listed as a service in the policy

Policies & Objects > Firewall Policy								
Policy	ID	Source	Destination	Schedule	Service	Action	NAT	
<input type="checkbox"/> Full_Access (1)	1	External-Server-Users LOCAL_SUBNET	all	always	<input checked="" type="checkbox"/> HTTP <input checked="" type="checkbox"/> DNS	✓ ACCEPT	<input checked="" type="checkbox"/> NAT	



A firewall policy also checks the service in order to transport the named protocols or group of protocols. No service (with the exception of DNS) is allowed through the firewall policy before successful user authentication. DNS is usually used by HTTP so that people can use domain names for websites, instead of their IP address. DNS is allowed because it is a base protocol and will most likely be required to initially see proper authentication protocol traffic. Hostname resolution is almost always a requirement for any protocol. However, the DNS service must still be defined in the policy as allowed, in order for it to pass.

In the example shown on this slide, policy ID 1 (Full_Access) allows users to use external DNS servers in order to resolve host names, before successful authentication. DNS is also allowed if authentication is unsuccessful because users need to be able to try to authenticate again. Any service that includes DNS would function the same way, like the default ALL service.

HTTP service is TCP port 80 and does not include DNS (UDP port 53).

DO NOT REPRINT

© FORTINET

Mixing Policies

- Enabling authentication in policies doesn't always mean users must actively authenticate. An open policy at the end of the list can allow passive or no-prompt authentication.

Policy	ID	Source	Destination	Security Profiles	Schedule	Service	Action	Status
<input type="checkbox"/> Guest (17)	17	<input checked="" type="checkbox"/> Guest-group <input checked="" type="checkbox"/> LOCAL_SUBNET	all	<input checked="" type="checkbox"/> SSL certificate-inspection <input checked="" type="checkbox"/> AV Guest_AV	always	ALL	✓ ACCEPT	Enabled
<input type="checkbox"/> Contractor (18)	18	<input checked="" type="checkbox"/> Contractor <input checked="" type="checkbox"/> LOCAL_SUBNET	all	<input checked="" type="checkbox"/> SSL certificate-inspection <input checked="" type="checkbox"/> AV Contractor_AV	always	ALL	✓ ACCEPT	Enabled
<input type="checkbox"/> Other (19)	19	<input checked="" type="checkbox"/> LOCAL_SUBNET	all	<input checked="" type="checkbox"/> SSL certificate-inspection <input checked="" type="checkbox"/> AV default	always	ALL	✓ ACCEPT	Enabled

- Three options:
 - Enable authentication on every policy that could match the traffic
 - Enable the authentication on demand option (CLI only)
 - Enable a captive portal on the ingress interface for the traffic
- If login cannot be determined passively, then FortiGate uses active authentication
 - FortiGate does not prompt the user for login credentials when it can identify the user passively
 - By default, active authentication is intended to be used as a backup when passive authentication fails



In the example shown on this slide, assuming active authentication is used, any initial traffic from LOCAL_SUBNET will not match policy ID 17 (Guest). Policy ID 17 looks for both IP address and user, and user group information (LOCAL_SUBNET and Guest-group respectively). Because the user has not yet authenticated, the user group aspect of the traffic does not match. Since the policy match is not complete, FortiGate continues its search down the ID list, to see if there is a complete match.

Next, FortiGate evaluates policy ID 18 to see if the traffic matches. It will not for the same reason it did not match 17.

Finally, FortiGate evaluates policy ID 19 to see if the traffic matches. It matches all criteria, so the traffic is allowed with no need to authenticate.

When you use only active authentication, if all possible policies that could match the source IP address have authentication enabled, then the user will receive a login prompt (assuming they use an acceptable login protocol). In other words, if policy ID 19 also had authentication enabled, the users would receive login prompts.

If you use passive authentication and it can successfully obtain user details, then traffic from LOCAL_SUBNET with users that belong to Guest-group will apply to policy ID 17, even though policy ID 19 does not have authentication enabled.

If you use both active and passive authentication, and FortiGate can identify a user's credentials through passive authentication, the user never receives a login prompt, regardless of the order of any firewall policies. This is because there is no need for FortiGate to prompt the user for login credentials when it can identify who the user is, passively. When you combine active and passive authentication methods, active authentication is intended to be used as a backup, to be used only when passive authentication fails.

DO NOT REPRINT**© FORTINET**

Active Authentication Behavior

- **Option 1:** Enable authentication on every policy that could match the traffic:
 - All firewall policies must have authentication enabled (active or passive)

- **Option 2:** Enforce authentication on-demand option:

- CLI option only

```
# config user setting  
(setting) # set auth-on-demand <always|implicitly>
```

- Provides more granular control
- Authentication is enabled at a firewall policy level
- You must place passive authentication policies on top of active authentication policies



As mentioned earlier, there are three different ways you can alter active authentication behavior. If you have an active authentication firewall policy followed by a fall-through policy that does not have authentication enabled on it, then all traffic will use the fall-through policy. This means that users are not asked to authenticate. By default, all traffic passes through the catch-all policy without being authenticated. You can alter this behavior by enabling authentication on all firewall policies. When you enable authentication, all the systems must authenticate before traffic is placed on the egress interface.

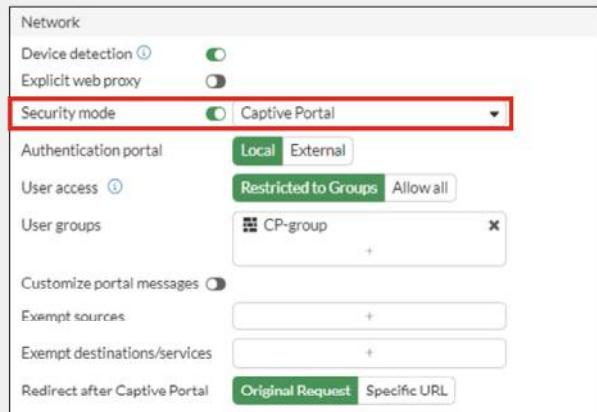
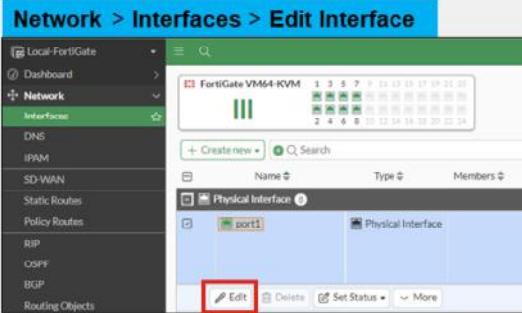
Alternatively, only on the CLI, you can change the auth-on-demand options. There are two options:

- **Implicitly** – The default option. It will not trigger authentication if there is a fall through policy.
- **Always** – Triggers an authentication prompt for policies that have active authentication enabled regardless of a fall-through policy. In this case, the traffic is not allowed until authentication is successful.

DO NOT REPRINT
© FORTINET

Active Authentication Behavior (Contd)

- **Option 3:** Enable a captive portal on the ingress interface for the traffic:
 - Authentication happens at an interface level
 - Traffic is not allowed without valid authentication unless it matches an exemption
 - All users are prompted for authentication before they can access any resource



© Fortinet Inc. All Rights Reserved. 27

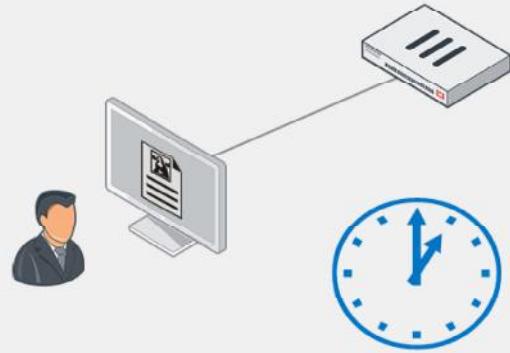
If you want to have all users connect to a specific interface, then it is better to enable captive portal authentication at the interface level. This way, all devices must authenticate before they are allowed to access any resources.

DO NOT REPRINT**© FORTINET**

Authentication Timeout

```
#config user setting  
    set auth-timeout-type [idle-timeout|hard-timeout|new-session]  
end
```

- Timeout specifies how long a user can remain idle before the user must authenticate again
 - Default is 5 minutes
- Three options for behavior:
 - Idle (default): no traffic for that amount of time
 - Hard: authentication expires after that amount of time, regardless of activity
 - New session: authentication expires if no new session is created in that amount of time



© Fortinet Inc. All Rights Reserved. 28

An authentication timeout is useful for security purposes. It minimizes the risk of someone using the IP of the legitimate authenticated user. It also ensures users do not authenticate and then stay in memory indefinitely. If users stayed in memory forever, it would eventually lead to memory exhaustion.

There are three options for timeout behavior:

- **Idle:** This looks at the packets from the host IP. If there are no packets generated by the host device in the configured timeframe, then the user is logged out.
- **Hard:** Time is an absolute value. Regardless of the user's behavior, the timer starts as soon as the user authenticates and expires after the configured value.
- **New session:** Even if traffic is being generated on existing communications channels, the authentication expires if no new sessions are created through the firewall from the host device within the configured timeout value.

Choose the type of timeout that best suits the authentication needs of your environment.

DO NOT REPRINT
© FORTINET

Monitoring Users

Dashboard > Assets & Identities > Firewall Users

The screenshot shows the 'Firewall Users' page. It features two large green circular dashboards: one for 'Total' users (1) and one for 'User Group' (1, Remote-users). Below these are search filters for 'User Name', 'IP Address', 'User Group', 'Duration', 'Traffic Volume', and 'Method'. A table lists a single user: 'aduser1' (User Name), '10.0.1.10' (IP Address), 'Remote-users' (User Group), '48s' (Duration), '167.29 KIB' (Traffic Volume), and 'Firewall' (Method). A red arrow points from the 'Deauthenticate' button in the table to a modal dialog titled 'Confirm' with the message 'Are you sure you want to deauthenticate the selected user(s)?' with 'OK' and 'Cancel' buttons.

- Also used to terminate authenticated sessions

© Fortinet Inc. All Rights Reserved. 29

You can monitor users who authenticate through your firewall policies using the **Dashboard > Assets & Identities > Firewall Users** page. It displays the user, user group, duration, IP address, traffic volume, and authentication method.

It does not include administrators, because they are not authenticating through firewall policies that allow traffic. They are logging in directly on FortiGate.

This page also allows you to disconnect a user, or multiple users, at the same time.

DO NOT REPRINT**© FORTINET**

Knowledge Check

1. A remote LDAP user is trying to authenticate with a username and password. How does FortiGate verify the login credentials?
 - A. FortiGate queries its own database for user credentials.
 - B. FortiGate sends the user-entered credentials to the remote server for verification.

2. When FortiGate uses a RADIUS server for remote authentication, which statement about RADIUS is true?
 - A. FortiGate must query the remote RADIUS server using the distinguished name (dn).
 - B. RADIUS group memberships are provided by vendor-specific attributes (VSAs) configured on the RADIUS server.

3. Which statement about active authentication is true?
 - A. Active authentication is always used before passive authentication.
 - B. The firewall policy must allow the HTTP, HTTPS, FTP, or Telnet protocols in order for the user to be prompted for credentials.



DO NOT REPRINT

© FORTINET

Lesson Progress



Remote Authentication



Methods of Authentication



© Fortinet Inc. All Rights Reserved. 31

Congratulations! You have completed this lesson.

Now, you will review the objectives covered in this lesson.

DO NOT REPRINT**© FORTINET**

Review

- ✓ Configure a remote LDAP authentication server on FortiGate
- ✓ Configure a remote RADIUS authentication server on FortiGate
- ✓ Deploy active and passive authentication
- ✓ Monitor firewall users using the FortiGate GUI



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

By mastering the objectives covered in this lesson, you learned how to use authentication on the firewall policies of FortiGate.

DO NOT REPRINT**© FORTINET**

FortiOS Administrator

Fortinet Single Sign-On (FSSO)

FortiOS 7.6

Last Modified: 6 October 2025

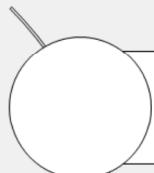
© Fortinet Inc. All Rights Reserved. 1

In this lesson, you will learn about Fortinet single sign-on (FSSO). Using this feature allows your users to access different network resources without needing to log in each time.

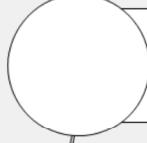
DO NOT REPRINT

© FORTINET

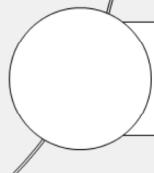
Lesson Overview



FSSO Deployment



FSSO Settings



Troubleshooting



© Fortinet Inc. All Rights Reserved.

2

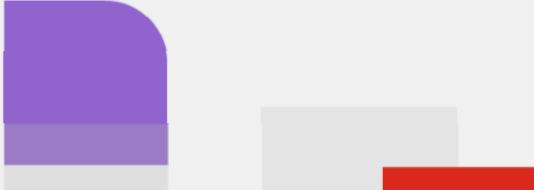
In this lesson, you will learn about the topics shown on this slide.

DO NOT REPRINT**© FORTINET**

FSSO Deployment

Objectives

- Identify FSSO modes for Windows AD
- Deploy FSSO in DC agent mode
- Deploy FSSO in polling mode



© Fortinet Inc. All Rights Reserved. 3

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

By demonstrating competence in understanding SSO concepts, you will be able to more effectively understand FSSO methods.

DO NOT REPRINT**© FORTINET**

SSO and FSSO

- SSO is a process that allows identified users access to multiple applications without having to reauthenticate
- Users who are already identified can access applications without being prompted to provide credentials
 - FSSO software identifies a user's user ID, IP address, and group membership
 - FortiGate allows access based on membership in FSSO groups configured on FortiGate
 - FSSO groups can be mapped to individual users, user groups, organizational units (OUs), or a combination
- FSSO is typically used with directory services, such as Windows Active Directory or Novell eDirectory



SSO is a process that allows users to be automatically logged in to every application after being identified, regardless of platform, technology, and domain.

FSSO is a software agent that enables FortiGate to identify network users for security policies or for VPN access, without asking for their username and password. When a user logs in to a directory service, the FSSO agent sends FortiGate the username, the IP address, and the list of groups that the user belongs to. FortiGate uses this information to maintain a local database of usernames, IP addresses, and group mappings.

Because the domain controller authenticates users, FortiGate does not perform authentication. When the user tries to access network resources, FortiGate selects the appropriate security policy for the destination. If the user belongs to one of the permitted user groups, the connection is allowed.

FSSO is typically used with directory service networks, such as Windows Active Directory or Novell eDirectory.

DO NOT REPRINT**© FORTINET**

FSSO Deployment and Configuration

Microsoft Active Directory (AD)

- Domain controller (DC) agent mode
- Polling mode:
 - Collector agent-based
 - Agentless
- Terminal server (TS) agent
 - Enhances login capabilities of a collector agent or FortiAuthenticator
 - Gathers logins for Citrix and terminal servers where multiple users share the same IP address



Novell eDirectory

- eDirectory agent mode
- Uses Novell API or LDAP setting



© Fortinet Inc. All Rights Reserved.

5

How you deploy and configure FSSO depends on the server that provides your directory services.

FSSO for Windows Active Directory (AD) uses a collector agent. Domain controller (DC) agents may also be required, depending on the collector agent working mode. There are two working modes that monitor user sign-on activities in Windows: DC agent mode and polling mode. FortiGate also offers a polling mode that does not require a collector agent, which is intended for simple networks with a minimal number of users.

There is another kind of DC agent that is used exclusively for Citrix and terminal services environments: terminal server (TS) agents. TS agents require the Windows Active Directory collector agent or FortiAuthenticator to collect and send the login events to FortiGate.

The eDirectory agent is installed on a Novell network to monitor user sign-ons and send the required information to FortiGate. It functions much like the collector agent on a Windows AD domain controller. The agent can obtain information from the Novell eDirectory using either the Novell API or LDAP.

DO NOT REPRINT**© FORTINET**

DC Agent Mode

- DC agent mode is the most scalable mode and is, in most environments, the recommended mode for FSSO
- Requires one DC agent (`dcagent.dll`) installed on each Windows DC in the `Windows\system32` directory. The DC agent is responsible for:
 - Monitoring user login events and forwarding them to the collector agents
 - Handling DNS lookups (by default)
- Requires one or more collector agents installed on Windows servers. The collector agent is responsible for:
 - Group verification
 - Workstation checks
 - Updates of login records on FortiGate
 - Sending domain local security group, organizational units (OUs), and global security group information to FortiGate



DC agent mode is considered the recommended mode for FSSO.

DC agent mode requires:

- One DC agent installed on each Windows DC
If you have multiple DCs, you need multiple DC agents. DC agents monitor and forward user login events to the collector agents.
- A collector agent, which is another FSSO component
The collector agent is installed on a Windows server that is a member of the domain you are trying to monitor. It consolidates events received from the DC agents, then forwards them to FortiGate. The collector agent is responsible for group verification, workstation checks, and FortiGate updates of login records. The FSSO collector agent can send domain local security group information, organizational units (OUs), and global security group information to FortiGate devices. It can also be customized for DNS lookups.

When the user logs on, the DC agent intercepts the login event on the domain controller and sends the client's NetBIOS or DNS name to the collector agent. The collector agent then sends a request to a DNS server to resolve the name and verify whether the user's IP address has changed.

In some configurations, double DNS resolution is a problem. In this case, you may configure a registry key on the domain controller that hosts the DC agent to not resolve the DNS:

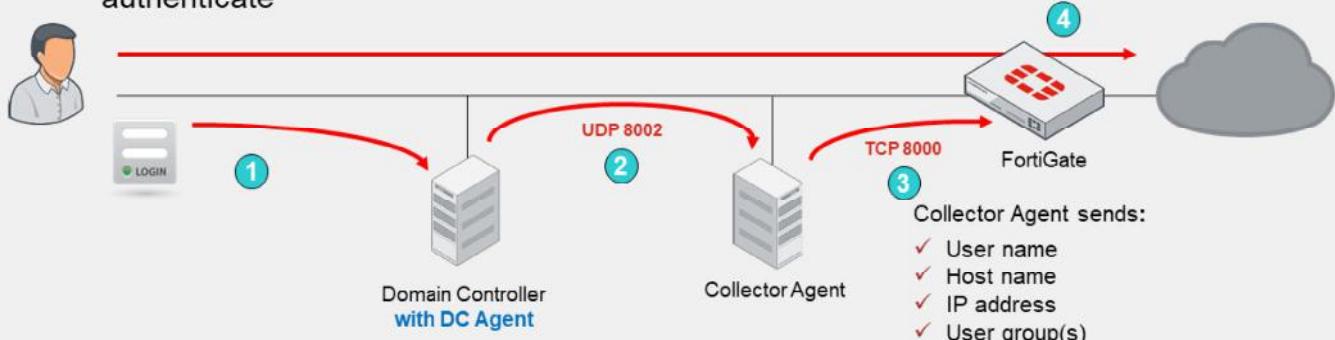
```
donot_resolve = (DWORD) 1 at HKLM\Software\Fortinet\FSAE/dcagent
```

DO NOT REPRINT

© FORTINET

DC Agent Mode Process

1. The user authenticates against the Windows DC
2. The DC agent sees the login event and forwards it to the collector agent
3. The collector agent receives the event from the DC agent and forwards it to FortiGate
4. FortiGate knows the user based on their IP address, so the user does not need to authenticate



© Fortinet Inc. All Rights Reserved. 7

This slide shows the process of information passing between DC agents, the collector agent, and a FortiGate configured for FSSO authentication.

1. When users authenticate with the DC, they provide their credentials.
2. The DC agent sees the login event, and forwards it to the collector agent.
3. The collector agent aggregates all login events and forwards that information to FortiGate. The information sent by the collector agent contains the user name, host name, IP address, and user group(s). The collector agent communicates with FortiGate over TCP port 8000 (default) and it listens on UDP port 8002 (default), for updates from the DC agents. The ports are customizable.
4. FortiGate learns from the collector agent who the user is, their IP address, and some of the AD groups that the user is a member of. When a user tries to access the internet, FortiGate compares the source IP address to its list of active FSSO users. Because the user in this case has already logged in to the domain, and FortiGate already has their information, FortiGate doesn't prompt the user to authenticate again. Rather it allows or denies the traffic based on the matching firewall policy.

DO NOT REPRINT**© FORTINET**

Collector Agent-Based Polling Mode

- A collector agent must be installed on a Windows server
 - No FSSO DC agent is required
- Every few seconds, the collector agent polls each DC for user login events. The collector agent uses:
 - SMB (TCP 445) protocol, by default, to request the event logs
 - TCP 135, TCP 139, and UDP 137 as fallbacks
- This mode requires a less complex installation, which reduces ongoing maintenance
- Three methods:
 - NetAPI
 - WinSecLog
 - WMI
- Event logging must be enabled on the DCs (except in NetAPI)



Polling mode can be collector agent-based or agentless.

First, you'll look at the collector agent-based polling mode. Like DC agent mode, collector agent-based mode requires a collector agent to be installed on a Windows server, but it *doesn't* require DC agents to be installed on each DC. In collector agent-based polling mode, the collector agent must be more powerful than the collector agent in DC agent mode, and it also generates unnecessary traffic when there have been no login events.

In Windows Event Log Polling, the most commonly deployed polling mode, the collector agent uses the SMB (TCP port 445) protocol to periodically request event logs from the domain controllers. Other methods may gather information differently, but after the login is received by the collector agent, the collector agent parses the data and builds the user login database, which consists of usernames, workstation names/IP addresses, and user group memberships. This information is then ready to be sent to FortiGate.

DO NOT REPRINT
© FORTINET

Collector Agent-Based Polling Mode Options

WMI	WinSecLog	NetAPI
<ul style="list-style-type: none"> DC returns all requested login events every 3 seconds* <ul style="list-style-type: none"> Reads selected event logs Improves WinSec bandwidth usage <ul style="list-style-type: none"> Reduces network load between collector agent and DC 	<ul style="list-style-type: none"> Polls all security events on DC every 10 seconds, or more* <ul style="list-style-type: none"> Log latency if network is large or system is slow Requires fast network links Slower, but... <ul style="list-style-type: none"> Sees all login events Only parses known event IDs by collector agent 	<ul style="list-style-type: none"> Polls the NetSessionEnum function on Windows every 9 seconds, or less* <ul style="list-style-type: none"> Authentication session table in RAM Retrieves login sessions, including DC login events Faster, but... <ul style="list-style-type: none"> If DC has heavy system load, can miss some login events

Most recommended → Least recommended

* The poll interval times are estimates. The interval times depend on the number of servers and network latency.



© Fortinet Inc. All Rights Reserved.

9

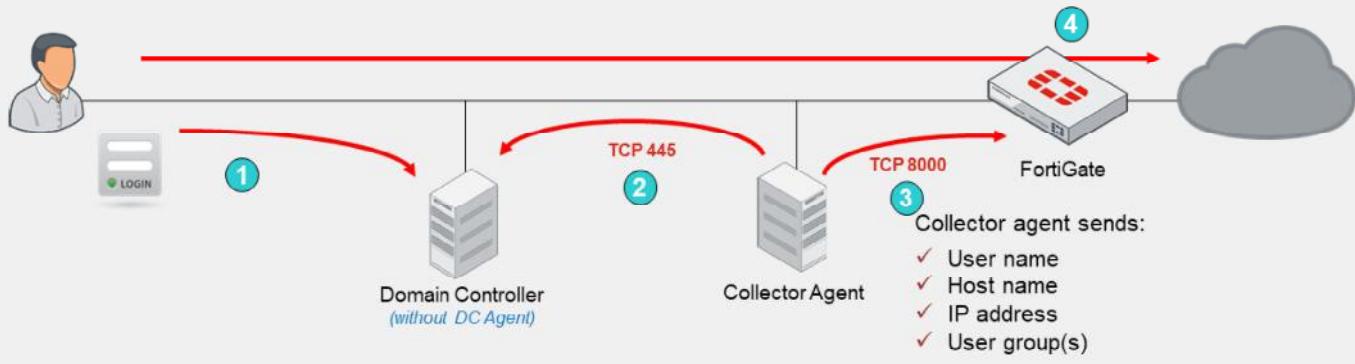
As previously stated, collector agent-based polling mode has three methods (or options) for collecting login information. The order on the slide from left to right shows most recommend to least recommended:

- WMI:** is a Windows API that gets system information from a Windows server. The DC returns all requested login events. The collector agent is a WMI client and sends WMI queries for user login events to the DC, which, in this case, is a WMI server. The collector agent doesn't need to search security event logs on the DC for user login events; instead, the DC returns all requested login events. This reduces network load between the collector agent and DC.
- WinSecLog:** polls all the security event logs from the DC. It doesn't miss any login events that have been recorded by the DC because events are not normally deleted from the logs. There can be some delay in FortiGate receiving events if the network is large and, therefore, writing to the logs is slow. It also requires that the audit success of specific event IDs is recorded in the Windows security logs.
- NetAPI:** polls temporary sessions created on the DC when a user logs in or logs out and calls the NetSessionEnum function on Windows. It's faster than the WinSec and WMI methods; however, it can miss some login events if a DC is under heavy system load. This is because sessions can be quickly created and purged from RAM, before the agent has a chance to poll and notify FortiGate.

DO NOT REPRINT
© FORTINET

Collector Agent-Based Polling Mode Process

1. The user authenticates with the DC
2. The collector agent frequently polls the DCs to collect user login events
3. The collector agent forwards logins to FortiGate
4. The user does not need to authenticate



© Fortinet Inc. All Rights Reserved. 10

This slide shows an example of FSSO using the collector agent-based polling mode. This example includes a DC, a collector agent, and FortiGate, but the DC doesn't have the dcagent installed.

1. The user authenticates with the DC, providing their credentials.
2. The collector agent periodically (every few seconds) polls TCP port 445 of each DC directly, to ask if anyone has logged in.
3. The collector agent sends login information to FortiGate over TCP port 8000. This is the same information that is sent in DC agent mode.
4. When user traffic arrives at FortiGate, FortiGate already knows which users are at which IP addresses, and no repeated authentication is required.

DO NOT REPRINT**© FORTINET**

Agentless Polling Mode

- Similar to agent-based polling, but FortiGate polls instead
- Doesn't require an external DC agent or collector agent
 - FortiGate collects the data directly
- Event logging must be enabled on the DCs
- More CPU and RAM required by FortiGate
- Support for polling option WinSecLog only
 - FortiGate uses the SMB protocol to read the event viewer logs
- Fewer available features than collector agent-based polling mode
- FortiGate doesn't poll workstation
 - Workstation verification is not available in agentless polling mode



You can deploy FSSO without installing an agent. FortiGate polls the DCs directly, instead of receiving login information indirectly from a collector agent.

Because FortiGate collects all of the data itself, agentless polling mode requires greater system resources, and it doesn't scale as easily.

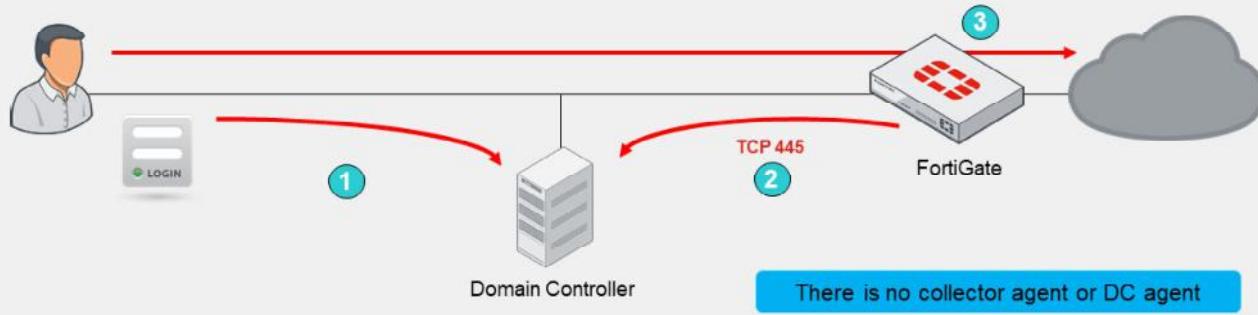
Agentless polling mode operates in a similar way to WinSecLog, but with only two event IDs: 4768 and 4769. Because there's no collector agent, FortiGate uses the SMB protocol to read the event viewer logs from the DCs.

In agentless polling mode, FortiGate acts as a collector. It is responsible for polling on top of its normal FSSO tasks but does not have all the extra features, such as workstation checks, that are available with the external collector agent.

DO NOT REPRINT
© FORTINET

Agentless Polling Mode Process

1. The user authenticates with the DC
2. FortiGate frequently polls DCs to collect user login events
 - o FortiGate discovers the login event
3. The user does not need to authenticate
 - o FortiGate already knows whose traffic it is receiving



© Fortinet Inc. All Rights Reserved. 12

This slide shows how communication is processed without agents. (There is no collector agent or DC agent.)

1. User authenticates with the DC.
2. FortiGate polls the DC TCP port 445 to collect user login events. FortiGate registers a login event, obtaining the user name, the host name, and the IP address. FortiGate then queries for the user's user group or groups.
3. When the user sends traffic, FortiGate already knows whose traffic it is receiving; therefore, the user does not need to authenticate.

DO NOT REPRINT**© FORTINET**

Comparing Modes

	DC agent mode	Polling mode (agentless and collector agent-based)
Installation	Complex—multiple installations (one per DC). Requires reboot.	Easy—one or no installations. No reboot required.
DC agent required	Yes	No
Resources	Shares with DC agents	Has own resources
Scalability	Higher	Lower
Redundancy	Yes	Yes
Level of confidence	Captures all logins	Might miss a login (NetAPI), or have a delay (WinSecLog)



This table summarizes the main differences between DC agent mode and polling mode.

DC agent mode is more complex. It requires not only a collector agent, but also a DC agent for each monitored domain controller. However, it is also more scalable because the DC agents capture logins and then pass the information directly to the collector.

In polling mode, the collector needs to query every domain controller, every few seconds. So, with each DC that is added, the number of queries grows. If you want to add a second collector agent for redundancy in polling mode, both collector agents need to query every DC individually.

In DC agent mode, the DC agent just has to collect the log once, and send a copy of the necessary information to all the collector agents. In comparison, if you use polling mode, some login events might be missed or delayed, depending on the polling option used.

You do not have to install a collector agent on the DC; you can install it on any Windows computer on the network.

DO NOT REPRINT**© FORTINET**

Additional FSSO AD Requirements

- The DNS server must be able to resolve all workstation names
 - Microsoft login events contain workstation names, but not IP addresses
 - The collector agent uses a DNS server to resolve the workstation name to an IP address
- For full feature functionality, the collector agent must be able to poll workstations
 - This informs the collector agents whether or not the user is still logged in
 - TCP ports 445 (default) and 139 (backup) must be open between collector agents or FortiGate and all hosts
 - Collector agent uses Windows Management Instrumentation (WMI) to verify whether a user is still logged in on remote workstations



Regardless of the collector method you choose, some FSSO requirements for your AD network are the same:

- Microsoft Windows login events have the workstation name and username, but not the workstation IP address. When the collector agent receives a login event, it queries a DNS server to resolve the IP address of the workstation. So, FSSO requires that you have your own DNS server. If a workstation IP address changes, DNS records must be updated immediately in order for the collector agent to be aware of the change and report it to FortiGate.
- For full feature functionality, collector agents need connectivity with all workstations. Since a monitored event log is not generated on logout, the collector agent (depending on the FSSO mode) must use a different method to verify whether users are still logged in. So, each user workstation is polled to see if users are still there. By default, all currently supported versions of FSSO collector agent use WMI to verify whether a user is still logged in on remote workstations.
- The DC agent, when the user logs in, intercepts the login event on the domain controller. It then resolves the DNS of the client, and sends it to the collector agent.

The collector agent receives the DNS and then performs a DNS resolution in order to check whether the IP address of the user has changed.

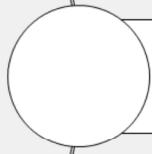
DO NOT REPRINT

© FORTINET

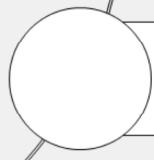
Lesson Progress



FSSO Deployment



FSSO Settings



Troubleshooting



© Fortinet Inc. All Rights Reserved.

15

Good job! You now understand basic concepts about the function of FSSO and how it is deployed.

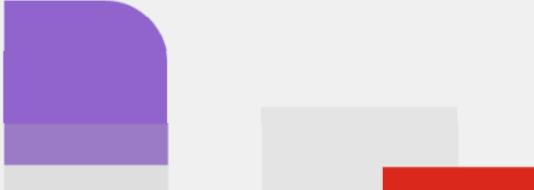
Now, you will learn how to configure FSSO settings.

DO NOT REPRINT**© FORTINET**

FSSO Settings

Objectives

- Configure FSSO settings on FortiGate
- Configure a collector agent

A decorative graphic in the bottom right corner of the slide. It consists of several overlapping geometric shapes: a large purple square at the top, a smaller grey rectangle below it, and a red rectangle at the bottom right. To the left of the purple square is a small red icon.

© Fortinet Inc. All Rights Reserved. 16

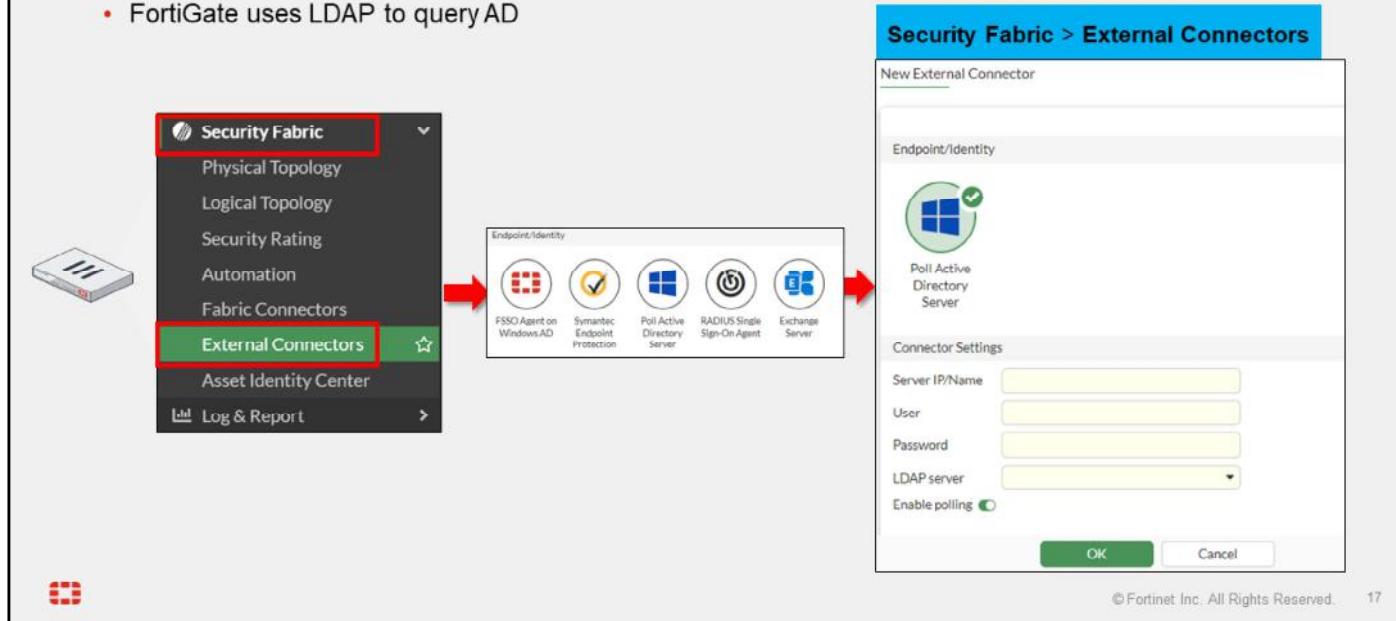
After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in configuring the FSSO agents and settings on FortiGate, you will be able to implement FSSO within your network.

DO NOT REPRINT
© FORTINET

FSSO Configuration—Agentless Polling Mode

- Agentless polling mode:
 - FortiGate uses LDAP to query AD



FortiGate FSSO configuration is straightforward.

If FortiGate is acting as a collector for agentless polling mode, you must select **Poll Active Directory Server** and configure the IP addresses and AD administrator credentials for each DC.

FortiGate uses LDAP to query AD to retrieve user group information. For this to happen, you must add the LDAP server to the **Poll Active Directory Server** configuration.

DO NOT REPRINT

© FORTINET

FSSO Configuration—Collector Agent-Based Polling or DC Agent Mode

- Collector agent-based polling or DC agent mode:
 - The FSSO agent can monitor users' login information from AD, Exchange, Terminal, Citrix, and eDirectory servers



If you have collector agents, using either the DC agent mode or the collector agent-based polling mode, you must select **Fortinet Single-Sign-On Agent** and configure the IP address and password for each collector agent.

The FSSO collector agent can access Windows AD in one of two modes:

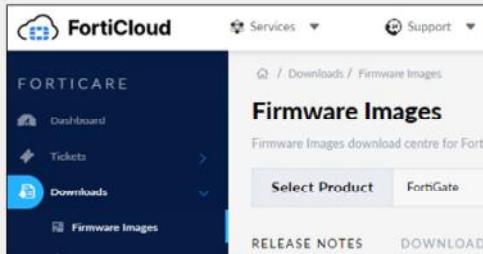
- **Collector Agent:** You create group filters on the collector agent. You can set FortiGate to **Collector Agent** mode, and the collector agent can still use **Advanced** mode to access nested groups.
- **Local:** You create group filters on FortiGate, using the LDAP server. If you set FortiGate to **Local** mode, you must set the collector agent to **Advanced** mode, otherwise the collector agent does not recognize the group filter sent by FortiGate and does not pass down any user logins.

DO NOT REPRINT
© FORTINET

FSSO Agent Installation

1. Visit the Fortinet support website:
 - <https://support.fortinet.com>

2. Click **Support > Firmware Download**



Available agents:

- DC agent: DCAgent_Setup
- CA for Microsoft servers: FSSO_Setup
- CA for Novell: FSSO_Setup_edirectory
- TS Agent: TAgent_Setup

3. Select **FortiGate**, then click **Download**.

4. Click **v7.00 > 7.6 > 7.6.0 > FSSO**

Example image below:

 A screenshot of the 'Firmware Images' download center for FortiGate. The page title is 'Firmware Images' with a sub-header 'Firmware Images download centre for Fortinet's extensive line of security solutions.' There are tabs for 'Select Product' and 'FortiGate'. The 'FortiGate' tab is selected. Below the tabs are buttons for 'RELEASE NOTES', 'DOWNLOAD' (which is underlined), 'UPGRADE PATHS', and 'FORTIGATE SUPPORT TOOL'. The main content is a table listing files for 'v7.00 > 7.6 > 7.6.0 > FSSO'. The table has columns: NAME, SIZE (KB), DATE CREATED, DATE MODIFIED, and HTTPS Checksum. The table lists several files including DCAgent_Setup_5.0.0316.exe, DCAgent_Setup_5.0.0316.msi, DCAgent_Setup_5.0.0316_x64.exe, DCAgent_Setup_5.0.0316_x64.msi, FSSO_Setup_5.0.0316.exe, FSSO_Setup_5.0.0316_x64.exe, FSSO_Setup_edirectory_5.0.0316.exe, md5sum.txt, TAgent_Setup_5.0.0316.exe, and TAgent_Setup_5.0.0316.msi. All files were created on 2024-07-25 and modified on 2024-07-25. The HTTPS Checksum column shows 'HTTPS Checksum' for all files.

NAME	SIZE (KB)	DATE CREATED	DATE MODIFIED	HTTPS Checksum
DCAgent_Setup_5.0.0316.exe	4,400	2024-07-25	2024-07-25	HTTPS Checksum
DCAgent_Setup_5.0.0316.msi	4,064	2024-07-25	2024-07-25	HTTPS Checksum
DCAgent_Setup_5.0.0316_x64.exe	5,272	2024-07-25	2024-07-25	HTTPS Checksum
DCAgent_Setup_5.0.0316_x64.msi	4,936	2024-07-25	2024-07-25	HTTPS Checksum
FSSO_Setup_5.0.0316.exe	12,376	2024-07-25	2024-07-25	HTTPS Checksum
FSSO_Setup_5.0.0316_x64.exe	12,740	2024-07-25	2024-07-25	HTTPS Checksum
FSSO_Setup_edirectory_5.0.0316.exe	5,608	2024-07-25	2024-07-25	HTTPS Checksum
md5sum.txt	1	2024-07-25	2024-07-25	HTTPS Checksum
TAgent_Setup_5.0.0316.exe	4,640	2024-07-25	2024-07-25	HTTPS Checksum
TAgent_Setup_5.0.0316.msi	4,304	2024-07-25	2024-07-25	HTTPS Checksum

© Fortinet Inc. All Rights Reserved.

19

The FSSO agents are available on the Fortinet Support website. There you will find the following:

- The DC agent
- The collector agent for Microsoft servers: FSSO_Setup
- The collector agent for Novell directories: FSSO_Setup_edirectory
- The terminal server agent (TAgent) installer for Citrix and terminal servers: TAgent_Setup

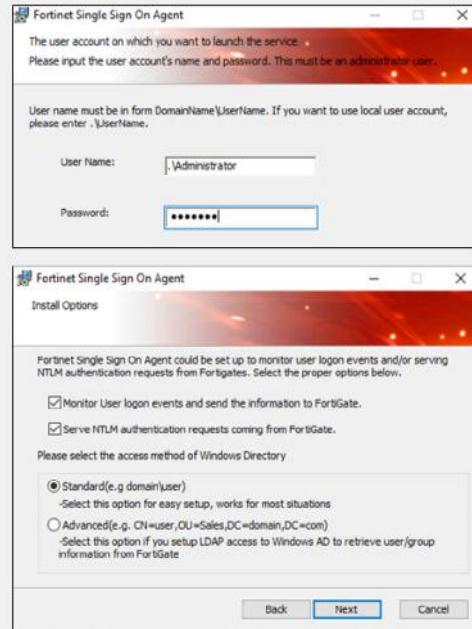
Also, for each agent, there are two versions: the executable (.exe) and Microsoft Installer (.msi).

Notice that you do not need to match the FSSO version with your exact FortiGate firmware version. When installing FSSO, grab the latest collector agent for your major release. You do however, need to match the DC agent version to the collector agent version.

DO NOT REPRINT
© FORTINET

FSSO Collector Agent Installation Process

1. Run the installation process as Administrator
2. Enter the user name in the following format:
 - DomainName\UserName
3. Configure the collector agent for:
 - Monitoring logins
 - NTLM authentication
 - Directory access
4. Optionally, launch the DC agent installation wizard before exiting the collector agent installation wizard



© Fortinet Inc. All Rights Reserved. 20

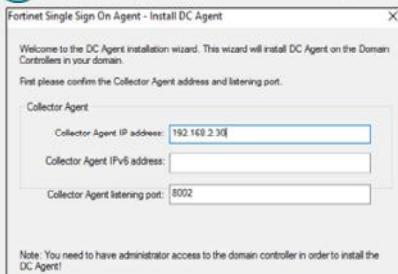
After you've downloaded the collector agent, run the installation process as Administrator and follow these steps in the installation wizard:

1. Read and accept the license agreement.
2. Optionally, change the installation location. The default folder is named **FSAE** (Fortinet Server Authentication Extension).
3. Enter the username. By default, the agent uses the name of the currently running account; however, you can change it using the format: **DomainName\UserName**.
4. Alternatively, configure your collector agent for monitoring, NTLM authentication, and directory access. These options are also customizable after installation. Although the default is **Standard** mode, when doing new FSSO setups it is always a best practice to install in **Advanced** mode. You will look at some of the advantages in this lesson.
5. If you want to use DC agent mode, make sure that **Launch DC Agent Install Wizard** is selected. This automatically starts the DC agent installation.

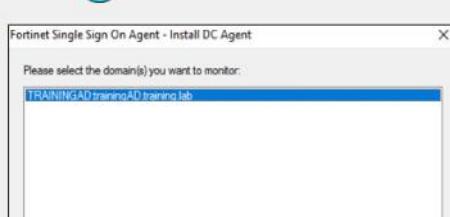
DO NOT REPRINT
© FORTINET

DC Agent Installation Process

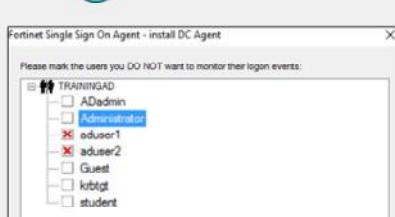
1 IP and port for collector agent



2 Domains to monitor



3 Remove users



4 Select domain controllers to install the DC agent

5 **DC Agent Mode** – to install DC agent on selected DC
Polling Mode – DC agent will not be installed



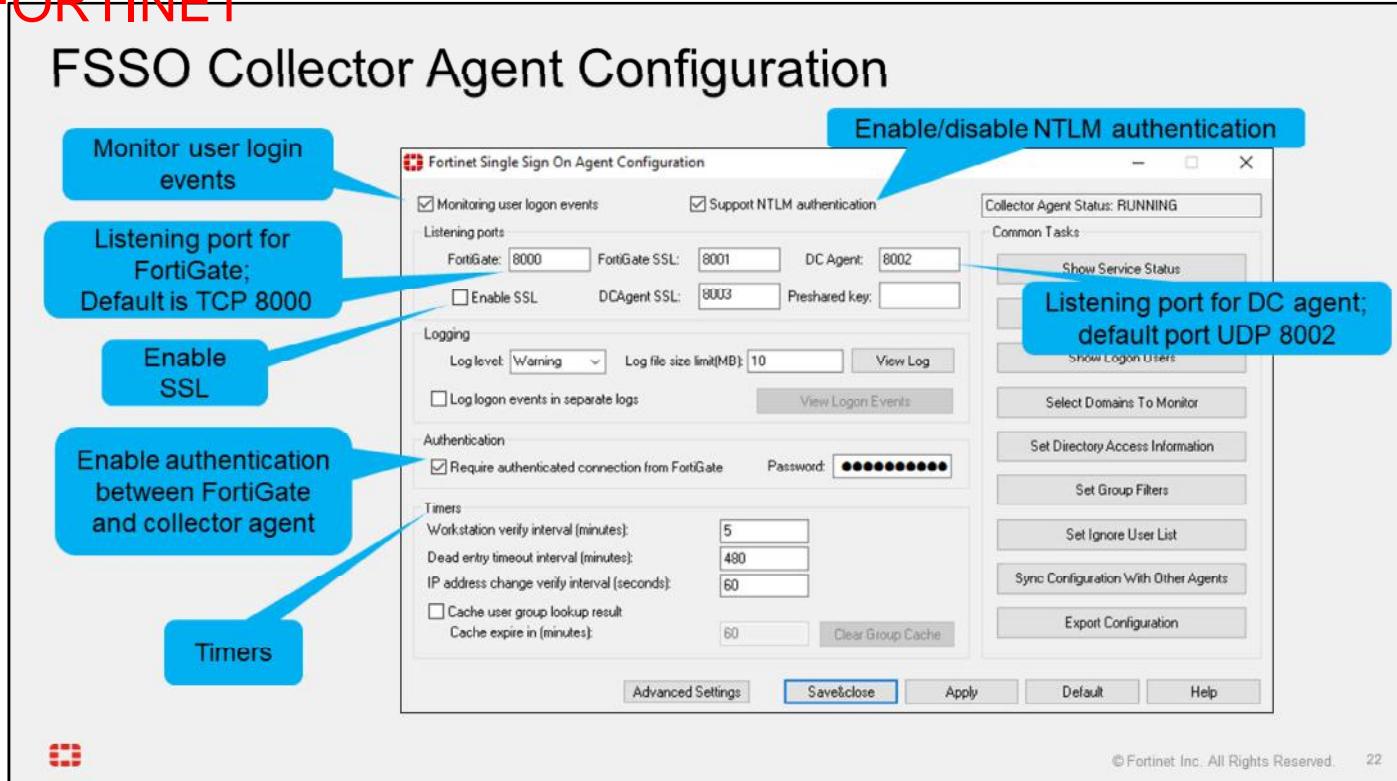
If you have just installed the collector agent and you selected **Launch DC Agent Install Wizard**, the installation process for domain controller agent automatically starts.

1. Enter the IP address for the collector agent. Optionally, you can customize the listening port, if the default value is already used by another service.
2. Select the domains to monitor. If any of your required domains are not listed, cancel the wizard and set up the correct trusted relationship with the domain controller. Then, run the wizard again. Note that this could also be a result of using an account without all the necessary permissions.
3. Optionally, select users that you do not want to monitor; these users' login events are not recorded by the collector and therefore are not passed to FortiGate. While these users are still able to generate login events to the domain, when they are detected by the collector agent, they are discarded so as to not interfere with the logged in user. This is especially useful in environments with a centrally managed antivirus solution, or a scheduled backup service that uses an AD account to start. These accounts can create login events for the collector agent that overwrite existing user logins. This may result in FortiGate applying the incorrect policies and profiles based on the overriding account. You can also customize the option to ignore users after installation is complete.
4. Optionally, clear the checkboxes of domain controllers that you don't want to install the DC agent on. Remember, for DC agent mode FSSO, at least one domain controller must have the DC agent installed. Also remember that installing the DC agent requires a reboot of the DC before it will start gathering login events. You can add or remove the DC agent to DCs at any time after the installation is complete.
5. Select **DC Agent Mode** as the working mode. If you select **Polling Mode**, the DC agent will not be installed.

Finally, the wizard requests a system reboot.

DO NOT REPRINT
© FORTINET

FSSO Collector Agent Configuration



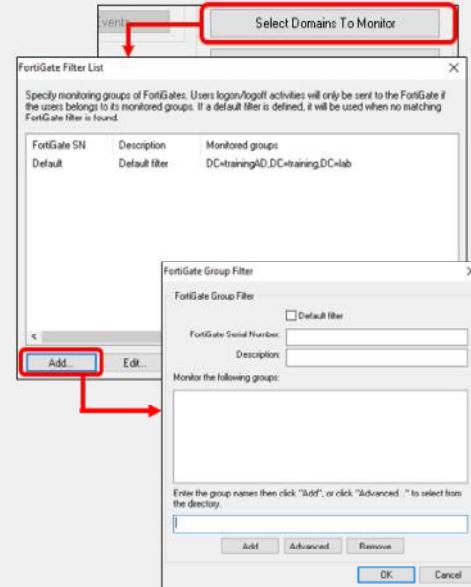
On the FSSO agent configuration GUI, you can configure settings such as:

- The listening port for communication with DC agents (UDP)
- The listening port for communication with FortiGate (TCP)
- NTLM authentication support
- Enable SSL
- Password authentication between the collector agent and FortiGate
- Timers

DO NOT REPRINT
© FORTINET

Group Filter

- The FSSO collector agent manages FortiGate group filters
- FortiGate group filters control which user's login information is sent to that FortiGate device
 - Filters are tied to the FortiGate serial number
- You can set filters for groups, OUs, users, or a combination



The FSSO collector agent allows you to configure a FortiGate group filter, which actively controls what user login information is sent to each FortiGate device. So, you can define which groups the collector agent passes to individual FortiGate devices.

Monitoring the entire group list in a large AD structure is highly inefficient, and a waste of resources. Most FSSO deployments need group segmentation (at least four or five groups), with the intention of assigning varying levels of security profile configurations to the different groups, using identity-based policies.

Group filters also help to limit the traffic sent to FortiGate. The maximum number of Windows AD user groups allowed on FortiGate depends on the model. Low-end FortiGate models support 256 Windows AD user groups. Mid-range and high-end models can support more groups. This is per VDOM, if VDOMs are enabled on FortiGate.

You can filter on FortiGate instead of the collector agent, but only if the collector agent is operating in advanced mode. In this case, the collector agent uses the list of groups you selected on FortiGate as its group filter for that device.

The filter list is initially empty. At a minimum, you should create a default filter that applies to all FortiGate devices without a defined filter. The default filter applies to any FortiGate device that does not have a specific filter defined in the list.

Note that if you change the AD access mode from **Standard** to **Advanced** or **Advanced** to **Standard**, you must recreate the filters because they vary depending on the mode.

DO NOT REPRINT**© FORTINET**

Ignored User List

- The collector agent ignores any login events that match the **Ignore User List** entries
 - Example: network service accounts
- User logins are not reported to FortiGate
- This helps to ensure users get the correct policies and profiles on FortiGate



The FSSO collector agent ignores any login events that match the **Ignore User List** entries. Therefore, these login events are not recorded by the collector agent, nor are they reported to FortiGate.

It is a good practice to add all network service accounts to the **Ignore User List**. Service accounts tend to overwrite user login events, and create issues with identity-based policy matching.

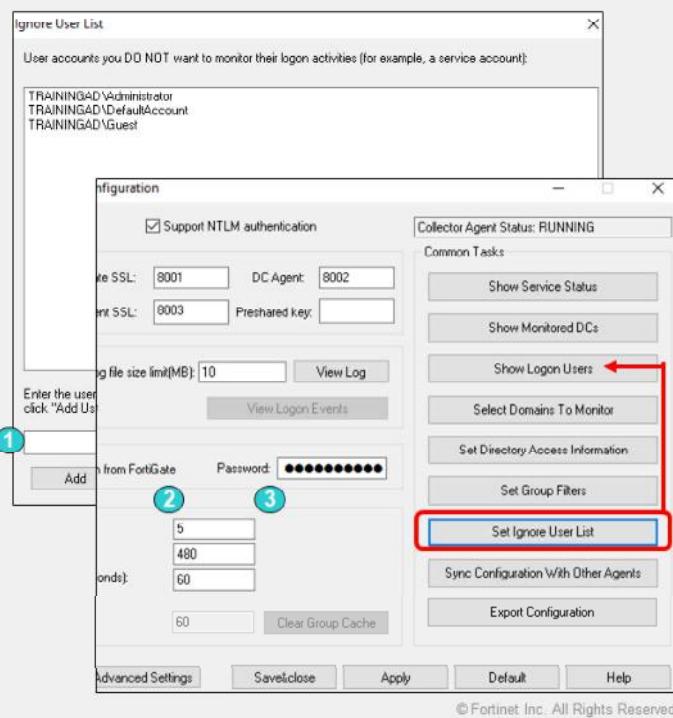
DO NOT REPRINT

© FORTINET

Ignored User List (Contd)

To add users to the ignore list:

1. Manual entry
2. **Add Users:** Select users you do not want to monitor
3. **Add by OU:** Select an OU from the directory tree



25

You can add users to the **Ignore Users List** in the following ways:

- Manually enter the username.
- Click **Add Users**, and then choose the users you do not want to monitor.
- Click **Add by OU**, and then select an OU from the directory tree. Be aware that, All users under the selected OU are added to the **Ignore User List**.

DO NOT REPRINT**© FORTINET**

Collector Agent Timers

Workstation verify interval

- Verifies if a user is still logged on
- Uses remote registry service to verify
- Default: 5 minutes
- Disable: Set value to 0

Dead entry timeout interval

- Applies to unverified entries only
 - Used to purge login information
 - Default: 480 minutes (8h)
 - Disable: Set value to 0
- Under the workstation verify interval

Timers	
Workstation verify interval [minutes]:	5
Dead entry timeout interval [minutes]:	480
IP address change verify interval [seconds]:	60
<input type="checkbox"/> Cache user group lookup result	
Cache expire in [minutes]:	60

IP address change verify interval

- Important on DHCP or dynamic environments
- Default – 60 seconds

Cache user group lookup result

- Collector agent remembers user group membership



© Fortinet Inc. All Rights Reserved. 26

The FSSO collector agent timers play an important role in ensuring the correct operation of FSSO.

Now, you'll take a look at each one and how they work.

- **Workstation verify interval.** This setting controls when the collector agent connects to individual workstations on port 139 (or port 445), and uses the remote registry service to verify if a user is still logged in to the same station. It changes the status of the user under **Show login User**, to **not verified** when it cannot connect to the workstation. If it does connect, it verifies the user and the status remains **OK**. To facilitate this verification process, you should set the remote registry service to auto start on all domain member PCs.
- **Dead entry timeout interval.** This setting applies only to entries with an unverified status. When an entry is not verified, the collector starts this timer. It's used to age out the entry. When the timer expires, the login is removed from the collector. From the perspective of FortiGate, there is no difference between entries that are **OK** and entries that are **not verified**. Both are considered valid.
- **IP address change verify interval.** This setting checks the IP addresses of logged in users and updates FortiGate when a user's IP address changes. This timer is especially important in DHCP or dynamic environments to prevent users from being locked out if they change IP address. The domain DNS server should be accurate; if the DNS server does not update the affected records promptly, the collector agent's IP information is inaccurate.
- **Cache user group lookup result.** This setting caches the user group membership for a defined period of time. It is not updated, even if the user changes group membership in AD.

DO NOT REPRINT
© FORTINET

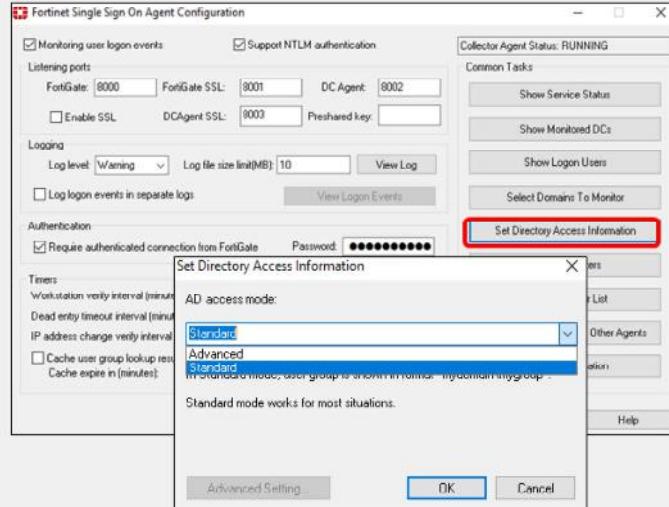
AD Access Mode Configuration

Standard access mode

- Windows convention:
 - Domain\groups
- Firewall policy authentication can apply to AD groups only (no individual users)
 - Nested group is not supported
- Group filters at collector agent

Advanced access mode

- LDAP convention user names:
 - CN=User, OU=Name, DC=Domain
- Firewall policy authentication can apply to AD users, groups, and OUs
 - Supports nested or inherited groups
- Group filtering:
 - FortiGate as an LDAP client, or group filter on collector agent
 - Filter groups defined on FortiGate



Another important FSSO setting is **AD access mode**. To set the AD access mode, click **Set Directory Access Information**. The AD access mode specifies how the collector agent accesses and collects the user and user group information. There are two modes that you can use to access AD user information: **Standard** and **Advanced**.

The main difference between modes is the naming convention used:

- **Standard** mode uses the Windows convention, NetBios: Domain\groups
- **Advanced** mode uses the LDAP convention: CN=User, OU=Name, DC=Domain

Advanced mode supports nested or inherited groups; that is, users can be members of subgroups that belong to monitored *parent* groups. Additionally, in advanced mode, FortiGate firewall policy authentication can be applied to individual users, user groups, and OUs.

In comparison, in standard mode, you can have a firewall policy authentication which can apply to user groups but not to individual users or OUs.

In advanced mode, you can configure FortiGate as an LDAP client and configure the group filters on FortiGate. You can also configure group filters on the collector agent.

If the LDAP on the collector agent fails, it doesn't matter what the LDAP on FortiGate indicates, FSSO won't work. If FortiGate LDAP fails, but the LDAP on the collector agent is still running, FortiGate may not be able to collect logs, but the collector agent still collects logs. Therefore it is recommended that you create filters from the collector agent.

DO NOT REPRINT
© FORTINET

FortiGate FSSO Group Object Configuration

User & Authentication > User Groups > Create new > Fortinet Single Sign-On (FSSO)

Collector Agent Group Filters

- Delete
- Search
- AD Group
- User Groups

- TRAININGAD/ACCESS CONTROL ASSISTANCE OPERATORS
- TRAININGAD/ACCOUNT OPERATORS
- TRAININGAD/AD-USERS
- TRAININGAD/ADMINISTRATORS
- TRAININGAD/ALLOWED RODC PASSWORD REPLICATION
- TRAININGAD/BACKUP OPERATORS
- TRAININGAD/CERT PUBLISHERS

Standard access mode

Users/Groups

Show subtree

- dc=trainingad,dc=training,dc=lab
 - CN=Users
 - CN=Computers
 - OU=Domain Controllers
 - CN=System
 - CN=ForeignSecurityPrincipals
 - CN=Program Data
 - CN=Managed Service Accounts
 - CN=Keys

ID	Name
Administrator	Administrator
DefaultAccount	DefaultAccount
Guest	Guest
krbtgt	krbtgt
user1	user1
user2	user2
user3	user3

Advanced access mode



In standard access mode, when you configure an FSSO group object on FortiGate, you will be able to select only AD groups as members.

In Advanced access mode, you can select any combination of users, groups, and OUs.

DO NOT REPRINT**© FORTINET**

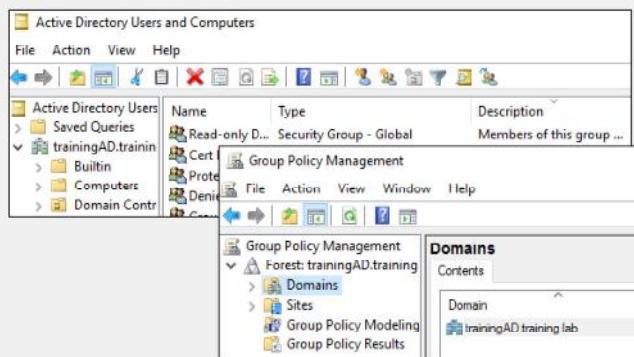
AD Group Support

Group type supported:

- Security groups
- Universal groups
- Groups inside OUs
- Local or universal groups that contain universal groups from child domains (only with Global Catalog)

If the user is not part of an FSSO group:

- For passive FSSO authentication:
 - User is part of **SSO_Guest_Users**
- For passive and active FSSO authentication:
 - User is prompted to log in



© Fortinet Inc. All Rights Reserved. 29

In AD settings, not all group types are supported. AD settings supports filtering groups only from:

- Security groups
- Universal groups
- Groups inside OUs
- Local or universal groups that contain universal groups from child domains (only with Global Catalog)

All FortiGate configurations include a user group called **SSO_Guest_Users**. When only passive authentication is used, all the users that do not belong to any FSSO group are automatically included in this guest group.

This allows an administrator to configure limited network access to guest users that do not belong to the Windows AD domain.

However, if both passive and active authentication are enabled for specific traffic, you cannot use **SSO_Guest_Users**, because traffic from IP addresses not on the FSSO user list must be prompted to enter their credentials.

DO NOT REPRINT**© FORTINET**

Advanced Settings

Citrix/Terminal Server

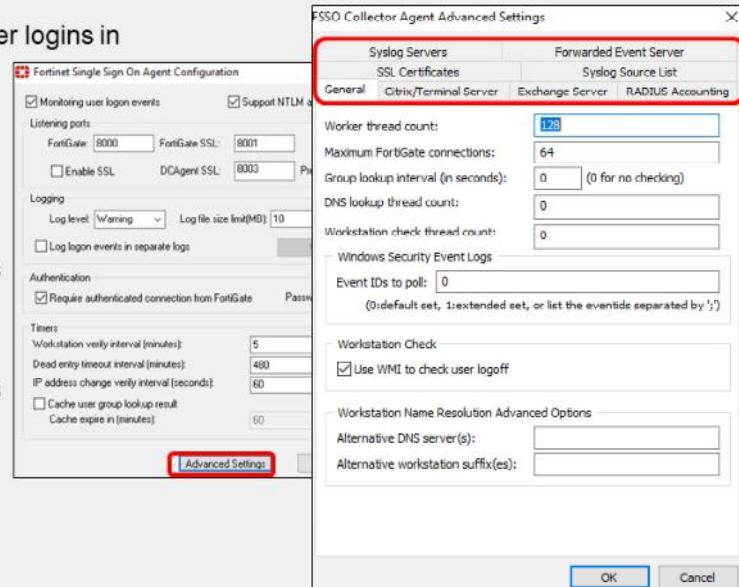
- Terminal server (TS) agent mode: monitors user logins in real time
- Requires a collector agent
 - No polling support from FortiGate

RADIUS Accounting

- Notify the firewall upon login and logout events

Syslog Servers

- Notify the firewall upon login and logout events



Depending on your network, you might need to configure advanced settings on your FSSO collector agent.

Citrix servers support FSSO. TS agent mode allows the server to monitor user logins in real time. The TS agent is like a DC agent, it also needs the collector agent to collect and send the login events to FortiGate. It then uses the same ports to report the logins back to the collector agent.

The collector agent on its own can get accurate login events from Citrix servers only if each user has their own IP address. If multiple users share the same IP address, the TS agent is required to report the user, the IP address, and the source port range assigned to that user to the collector agent. The TS agent cannot forward logs directly to FortiGate; the logs first have to be gathered by a collector. This does not work with polling from FortiGate.

A RADIUS server configured as a RADIUS-based accounting system can interact in your network by sending accounting messages to the collector agent. The FSSO collector agent also supports integration with syslog servers, for the same purpose.

You can configure which event IDs are polled for Windows security event logs in the **Event IDs to poll** field.

DO NOT REPRINT

© FORTINET

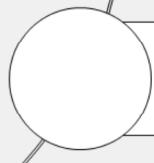
Lesson Progress



FSSO Deployment



FSSO Settings



Troubleshooting



© Fortinet Inc. All Rights Reserved.

31

Good job! You now understand how to configure the FSSO settings on FortiGate and the FSSO collector agent.

Now, you will learn about some basic troubleshooting options.

DO NOT REPRINT**© FORTINET**

Troubleshooting

Objectives

- Recognize and monitor FSSO-related log messages
- Troubleshoot FSSO login issues



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

By demonstrating competence in FSSO monitoring and troubleshooting, you will be able to prevent, identify, and solve common issues related to FSSO.

DO NOT REPRINT**© FORTINET**

Troubleshooting Tips for FSSO

- Ensure all firewalls allow the ports that FSSO requires
- Guarantee at least 64 Kbps bandwidth for each domain controller
- Configure the timeout timer to flush inactive sessions after a shorter time
- Ensure DNS is configured and updating IP addresses if the host IP address changes
- Never set the timer workstation verify interval to 0
- Include all FSSO groups in the firewall policies when using passive authentication



Begin with the following tips, which are useful in many FSSO troubleshooting situations:

- FSSO has a number of required ports that you must allow through all firewalls, or connections will fail. These include ports 139 (workstation verification), 445 (workstation verification and event log polling), 389 (LDAP), and 445 and 636 (LDAPS).
- Configure traffic shaping to have a minimum guaranteed bandwidth of 64 Kbps for each domain controller. If there is insufficient bandwidth, some FSSO information might not reach FortiGate.
- In an all-Windows environment, flush inactive sessions. Otherwise, a session for a non-authenticated machine may be sent as an authenticated user. This can occur if the DHCP lease expires for the authenticated user with the collector agent being able to verify that the user has logged out.
- Ensure DNS is configured correctly and is updating IP addresses, if workstation IP addresses change.
- Never set the workstation verify interval to 0. This prevents the collector agent from deleting stale entries, which means that they can be removed only by a new event overwriting them. This can be especially dangerous in environments where FSSO and non-FSSO users share the same DHCP pool.
- When using passive authentication only, include the group of guest users in a policy and give them access. Associate their group with a security policy. If you use active authentication as a backup, ensure you do not add SSO_Guest_User to any policies. SSO_Guest_User and active authentication are mutually exclusive.

DO NOT REPRINT
© FORTINET

FSSO Log Messages on FortiGate

- FSSO logs are generated from authentication events, such as user login and logout events and NTLM authentication events
 - To log all events, set the minimum log level to **Notification** or **Information**

The screenshot shows the FortiGate Log & Report interface. A red arrow points from the 'Log ID' field in the 'Details' section of a selected log entry to the 'Log ID' column in a table of log messages.

Log & Report > System Events > User Events

User	Action	Message
ADUSER1	authentication	User ADUSER1 succeeded in logout
ADUSER1	FSSO-logoff	FSSO-logoff event from TrainingDomain: user ADUSER1 logged off 10.0.1.10
ADUSER1	FSSO-logon	FSSO-logon event from TrainingDomain: user ADUSER1 logged on 10.0.1.10

Details

Event
 Message FSSO-logon event from TrainingDomain: user ADUSER1 logged on 10.0.1.10

Other
 Destination TrainingDomain
 Log ID **43014**
 Sub Type user
 roll 65533

Message ID	Severity	Description
43008	Notification	Authentication was successful
43009	Notification	Authentication session failed
43010	Warning	Authentication locked out
43011	Notification	Authentication timed out
43012	Notification	FSSO authentication successful
43013	Notification	FSSO authentication failed
43014	Notification	FSSO user logged on
43015	Notification	FSSO user logged off
43016	Notification	NTLM authentication successful
43017	Notification	NTLM authentication failed

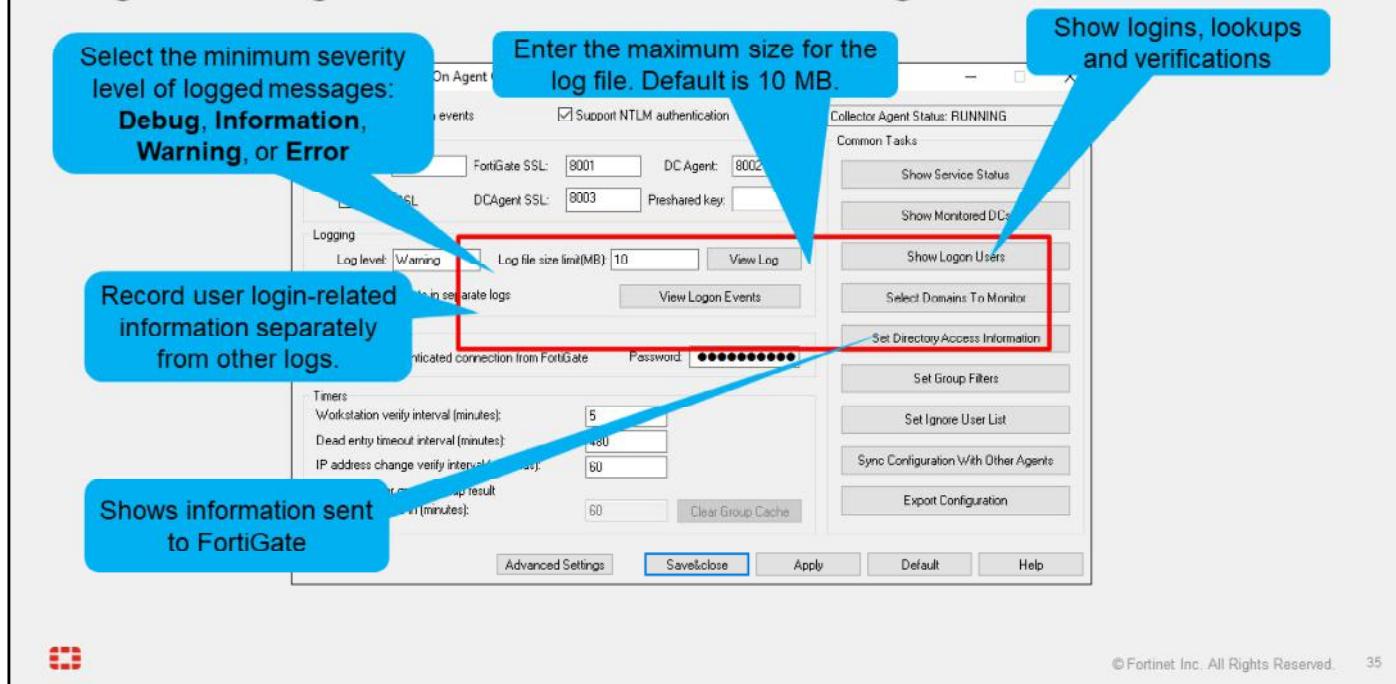
© Fortinet Inc. All Rights Reserved. 34

FSSO-related log messages are generated from authentication events. These include user login and logout events, and NTLM authentication events. These log messages are central to network accounting policies, and can also be useful in troubleshooting issues.

To ensure you log all the events needed, set the minimum log level to **Notification** or **Information**. Firewall logging requires **Notification** as a minimum log level. The closer the log level is to **Debug** level, the more information is logged.

DO NOT REPRINT
© FORTINET

Log Messages on FSSO Collector Agent



When troubleshooting FSSO agent-based deployments, you might want to look at the log messages generated directly on the FSSO collector agent.

The **Logging** section of the FSSO collector agent allows the following configurations:

- **Log level:** Select the minimum severity level of logged messages. Includes these levels:
 - **Debug:** the most detailed log level. Use it when actively troubleshooting issues.
 - **Information:** includes details about login events and workstation checks. This is the recommended level for most troubleshooting.
 - **Warning:** the default level. It provides information about failures.
 - **Error:** lists only the most severe events.
- **Log file size limit (MB):** Enter the maximum size for the log file in MB. The default is 10.
- **View Log:** View all FSSO agent logs.
- **Log login events in separate logs:** Record user login-related information separately from other logs. The information in this log includes: data received from DC agents, user login/logout information, workstation IP change information, and data sent to FortiGate devices. When selected, a summary of events sent and removed from FortiGate is listed under **View login Events**, while all other information remains under **View Log**.
- **View login Events:** If **Log login events in separate logs** is enabled, you will can view user login-related information.

DO NOT REPRINT

© FORTINET

Currently Logged-In Users

The screenshot illustrates the integration of Fortinet Single Sign-On (FSSO) with FortiGate. It shows both command-line interface (CLI) output and a graphical user interface (GUI) dashboard.

CLI Output:

```
# diagnose debug authd fssso list
----FSSO logins----
IP: 10.0.1.10 User: ADUSER1 Groups: TRAININGAD/AD-USERS
Workstation: WIN-INTERNAL MemberOf: Training
IP: 192.168.131.5 User: ADUSER1 Groups: TRAININGAD/AD-USERS
Workstation: WIN-INTERNAL MemberOf: Training

Total number of logins listed: 2, filtered: 0
----end of FSSO logins----
```

Annotations for the CLI output:

- IP address:** Points to the IP address 10.0.1.10.
- User name:** Points to the user name ADUSER1.
- User group:** Points to the user group TRAININGAD/AD-USERS.
- Workstation name:** Points to the workstation name WIN-INTERNAL.
- Group created on FortiGate:** Points to the entry "MemberOf: Training".

Dashboard > Assets & Identities > Firewall Users:

The dashboard provides a summary of FSSO logins. It includes two donut charts: one for the total number of users (1) and another for the total number of logins (2). A callout box points to the "Show all FSSO Logons" button.

User Group	Count
Training	1
TRAININGAD/AD-USERS	1

Annotations for the GUI:

- To view FSSO users:** Points to the "Show all FSSO Logons" button.
- User FSSO Group:** Points to the "User FSSO Group" section, which lists TRAININGAD/AD-USERS.
- Connector References:** Points to the "Connector References" section, which shows 1 reference.
- Show in list:** Points to the "Show in list" checkbox.

If applying the tips from the previous slide didn't solve your FSSO issues, you may need to apply some `debug` commands.

To display the list of FSSO users that are currently logged in, use the CLI command `diagnose debug authd fssso list`.

For each user, the user name, user group, IP address, and the name of the workstation from which they logged in shows. The `MemberOf` section shows the group that was created on the firewall, to which you mapped the AD group. The same group should show in the **User group** screen on the GUI.

Also, use `execute fssso refresh` to manually refresh user group information from any directory service servers connected to FortiGate, using the collector agent.

DO NOT REPRINT**© FORTINET**

Connection to FortiGate

- Check connectivity between collector agent and FortiGate

```
# diagnose debug authd fssso server-status
```

Server Name	Connection Status	Version	Address
TrainingDomain	connected	FSAE server 1.1	10.0.1.10



To show the status of communication between FortiGate and each collector agent, you can use the CLI command `diagnose debug authd fssso server-status`.

DO NOT REPRINT**© FORTINET**

Additional Commands

```
# diagnose debug authd fss0 <...>

    filter  - Filters used for list or clear logins
    list    - Show currently logged on users
    refresh-groups - Refresh group mapping
    summary   - Summary of currently logged on users
    clear-logons - Delete cached login status
    refresh-logons - Resynchronize login database
    show-address - Show FSAE dynamic addresses
    server-status - Show FSSO agent connection status

# diagnose firewall auth clear - Clears all filtered users
# diagnose firewall auth filter- Filter specific group, id, and so on
# diagnose firewall auth list  - List authenticated users
# diagnose firewall auth mac   - Authenticated MAC users
# diagnose firewall auth ipv6 - Authenticated IPv6 users
```



Also, available under `diagnose debug authd fss0` are commands for clearing the FortiGate cache of all currently logged in users, filtering the display of the list of logged in users, and refreshing the login and user group information.

DO NOT REPRINT

© FORTINET

Polling Mode

```
diagnose debug fssso-polling detail
AD Server Status:
ID=1, name(10.0.1.10),ip=10.0.1.10,source(security),users(0)
port=auto username=administrator
read log offset=251636, latest login timestamp: Wed Sep 20 09:47:31 2023
polling frequency: every 10 second(s) success(246), fail(0)
LDAP query: success(0), fail(0)
LDAP max group query period(seconds): 0
most recent connection status: connected
```

Status of polls by FortiGate to DC


```
diagnose debug fssso-polling refresh-user
refresh completes. All login users are obsolete. Please re-login to make them available.
```

Active FSSO users


```
diagnose sniffer packet any 'host ip address and tcp port 445'
```

Sniff polls


```
diagnose debug application fssod -1
```



The command `diagnose debug fssso-polling detail` displays status information and some statistics related to the polls done by FortiGate on each DC in agentless polling. If the `read log offset` is incrementing, FortiGate is connecting to and reading the logs on the domain controller. If the `read log offset` is incrementing but you are not getting any login events, check that the group filter is correct and that the domain controller is creating the correct event IDs.

The command `diagnose debug fssso-polling refresh-user` flushes information about all the active FSSO users.

In agentless polling mode, FortiGate frequently polls the event viewer to get the login events. You can sniff this traffic on port 445.

Also, there is a specific FortiGate daemon that handles polling mode. It is the `fssod` daemon. To enable agentless polling mode real-time debug, use the `diagnose debug application fssod -1` command.

DO NOT REPRINT**© FORTINET**

Knowledge Check

1. Which mode is recommended for FSSO deployments?
 A. DC agent mode
 B. Polling mode: Agentless

2. Which naming conventions does the FSSO collector agent use to access the Windows AD in standard access mode?
 A. Windows convention—NetBios: Domain\groups
 B. LDAP convention: CN=User, OU=Name, DC=Domain

3. Which FSSO mode requires more FortiGate system resources (CPU and RAM)?
 A. Collector agent-based polling mode
 B. Agentless polling mode



DO NOT REPRINT

© FORTINET

Lesson Progress



FSSO Deployment



FSSO Settings



Troubleshooting



© Fortinet Inc. All Rights Reserved.

41

Congratulations! You have completed this lesson.

Now, you will review the objectives covered in this lesson.

DO NOT REPRINT**© FORTINET**

Review

- ✓ Install FSSO in DC agent mode
- ✓ Install a collector agent
- ✓ Troubleshoot FSSO login issues



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

By mastering the objectives covered in this lesson, you learned how to use FSSO so that your users don't need to log in each time they access a different network resource.

DO NOT REPRINT**© FORTINET**

FortiOS Administrator

Certificate Operations

A small red square icon containing a white square with a diagonal line, followed by the text "FortiOS 7.6".

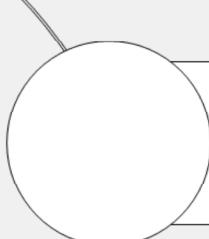
Last Modified: 6 October 2025

© Fortinet Inc. All Rights Reserved. 1

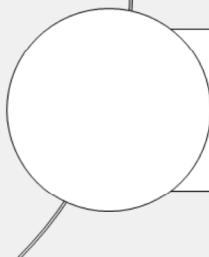
In this lesson, you will learn why FortiGate uses digital certificates, and how to configure FortiGate to use certificates for SSL and SSH traffic inspection.

DO NOT REPRINT**© FORTINET**

Lesson Overview



Authenticate and Secure Data Using Certificates



Inspect Encrypted Data



© Fortinet Inc. All Rights Reserved.

2

In this lesson, you will learn about the topics shown on this slide.

DO NOT REPRINT**© FORTINET**

Authenticate and Secure Data Using Certificates

Objectives

- Describe why FortiGate uses digital certificates
- Describe how FortiGate uses certificates to authenticate users and devices
- Describe how FortiGate uses certificates to ensure the privacy of data



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

By demonstrating a competent understanding of how FortiGate uses certificates, you will be better able to judge how and when certificates could be used in your own networks.

DO NOT REPRINT

© FORTINET

Digital Certificate

- What is a digital certificate?
 - A digital identity produced and signed by a certificate authority (CA)
 - Analogy: passport or driver's license
- Primary purposes
 - Authentication
 - Encryption and decryption
 - Integrity
- How does FortiGate use certificates to identify devices and people?
 - The **Subject** and **Subject Alternative Name** fields in the certificate identify the device or person associated with the certificate
- FortiGate uses the X.509v3 certificate standard

Field	Value
Version	V3
Serial number	0cacbf0403e86fc4ba3da5f26b...
Signature algorithm	sha256RSA
Signature hash algorithm	sha256
Issuer	Amazon RSA 2048 M02, Amaz...
Valid from	Sunday, 26 February 2023 02...
Valid to	Thursday, 28 March 2024 01:...
Subject	training.fortinet.com
Public key	RSA (2048 Bits)
Public key parameters	05 00
Authority Key Identifier	KeyID=c03152cd5a50c3827c7...
Subject Key Identifier	54c8bdc749bd966ac110f515d...
Subject Alternative Name	DNS Name=training.fortinet.c...
Enhanced Key Usage	Server Authentication (1.3.6....
CRL Distribution Points	[1]CRL Distribution Point: Distr...
Certificate Policies	[1]Certificate Policy:Policy Ide...
Authority Information Access	[1]Authority Info Access: Acc...
SCT List	v1, eecdd064d5db1acec55cb7...
Key Usage	Digital Signature, Key Encipher...
Basic Constraints	Subject Type=End Entity, Pat...
Thumbprint	5a09781b2bc9d911f18c2d285...



© Fortinet Inc. All Rights Reserved.

4

A digital certificate is a file or password used to authenticate a device, server, or user through cryptography and public key infrastructure (PKI). It is a digital document produced and signed by a CA.

It ensures that only trusted devices and users gain access to a network. It identifies an end entity, such as a person (for example, Joe Bloggings), a device (for example, webserver.acme.com), or thing (for example, a certificate revocation list). Another common use of digital certificates is to verify a website's legitimacy to a browser, known as an SSL certificate.

Certificates serve three primary purposes:

- Authentication: The common name (CN) or subject alternative name (SAN) field, or both are used to identify the device that the certificate is representing.
- Encryption and decryption: Private and public key pairs are used to encrypt and decrypt traffic.
- Integrity: Messages are hashed using a secret key known to both the sender and the receiver. The receiver uses the key to check the hash value and confirm the integrity and authenticity of the message data.

FortiGate identifies the device or person by reading the CN value in the **Subject** field, which is expressed as a distinguished name (DN). FortiGate could also use alternate identifiers, shown in the **Subject Alternative Name** field, whose values could be a network ID or an email address, for example. FortiGate can use the **Subject Key Identifier** and **Authority Key Identifier** values to determine the relationship between the issuer of the certificate (identified in the **Issuer** field), and the certificate.

FortiGate supports the X.509v3 certificate standard, which is the most common standard for certificates.

DO NOT REPRINT**© FORTINET**

Why Does FortiGate Use Digital Certificates?

- Inspection
 - SSL/SSH and HTTPS traffic inspection
 - Inbound or outbound traffic through FortiGate
 - Traffic to and from FortiGate
- Privacy
 - Ensure privacy for exchanges with other devices, such as FortiGuard
- Authentication
 - User authentication for network access
 - User authentication for VPN connection
 - As second-factor authentication for FortiGate administrator



FortiGate uses digital certificates to enhance security in multiple areas.

FortiGate uses digital certificates for inspection, mainly outbound or inbound traffic inspection. If FortiGate trusts the certificate, it permits the connection. But if FortiGate does not trust the certificate, it can prevent the connection. How you configure FortiGate determines the behavior; however, other policies that are being used may also affect whether FortiGate accepts or rejects connection attempts. FortiGate can also inspect certificates to identify people and devices (in the network and on the internet), before it permits a person or device to make a full connection to the entity that it is protecting.

FortiGate uses digital certificates to enforce privacy. Certificates, and their associated private keys, ensure that FortiGate can establish a private SSL connection to another service, such as FortiGuard, or a web browser or web server.

FortiGate also uses certificates for authentication. Users who have certificates issued by a known and trusted CA can authenticate on FortiGate to access the network or establish a VPN connection. Administrator users can use certificates as a second-factor authentication credential to log in to FortiGate.

DO NOT REPRINT
© FORTINET

How Does FortiGate Trust Certificates?

- FortiGate does the following checks against a certificate before trusting it and using it:
 - Revocation check
 - CA certificate possession
 - FortiGate uses the **Issuer** value to determine if FortiGate possesses the corresponding CA certificate
 - Without the corresponding CA certificate, FortiGate cannot trust the certificate
 - Validity dates
 - Digital signature validation
 - The verification of the digital signature on the certificate must pass

Field	Value
Version	V3
Serial number	0cacbf0403e86fc4ba3da5f26b...
Signature algorithm	sha256RSA
Signature hash algorithm	sha256
Issuer	Amazon RSA 2048 M02, Amaz...
Valid from	Sunday, 26 February 2023 02...
Valid to	Thursday, 28 March 2024 01:...
Subject	training.fortinet.com
Public key	RSA (2048 Bits)
Public key parameters	05 00
Authority Key Identifier	KeyID=c03152cd5a50c3827c7...
Subject Key Identifier	54c8bdc749bd966ac110f515d...
Subject Alternative Name	DNS Name=training.fortinet.c...
Enhanced Key Usage	Server Authentication (1.3.6....
CRL Distribution Points	[1]CRL Distribution Point: Distr...
Certificate Policies	[1]Certificate Policy:Policy Ide...
Authority Information Access	[1]Authority Info Access: Acc...
SCT List	v1, eecdd064d5db1acec55cb7...
Key Usage	Digital Signature, Key Encipher...
Basic Constraints	Subject Type=End Entity, Pat...
Thumbprint	5a09781b2bc9d911f18c2d285...



© Fortinet Inc. All Rights Reserved.

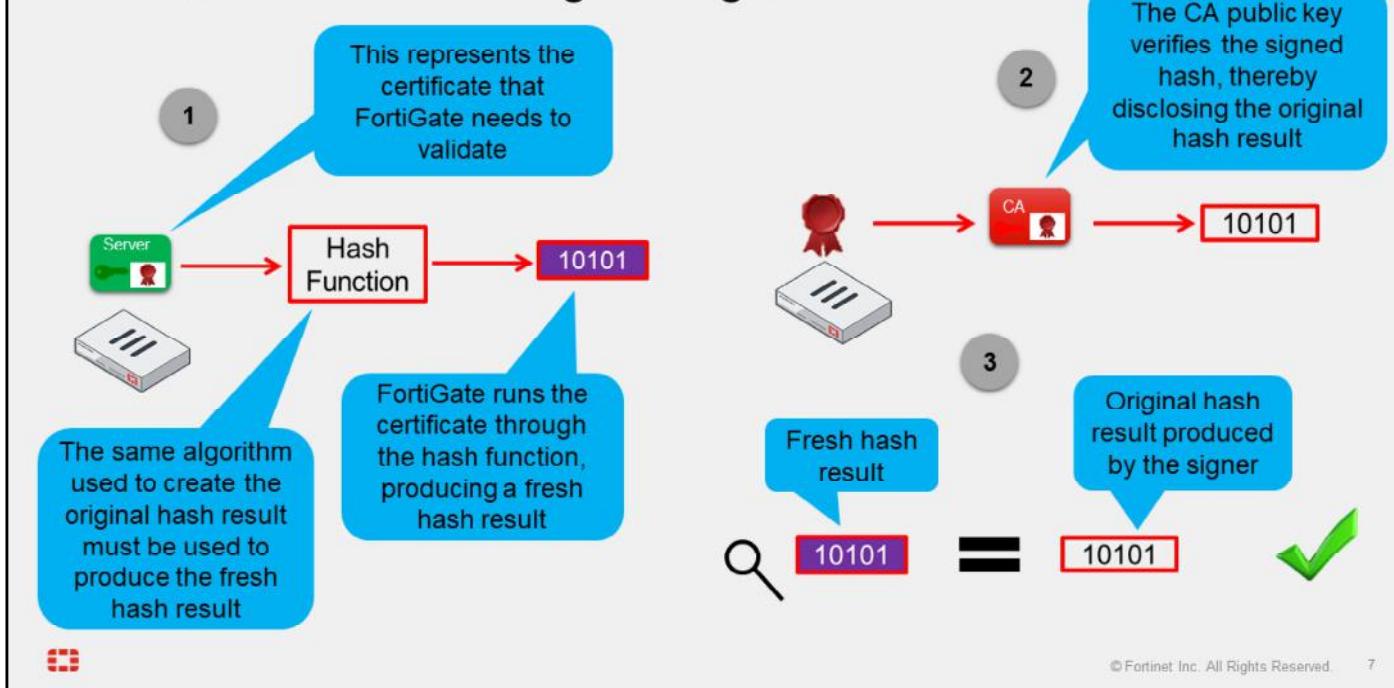
6

FortiGate runs the following checks before it trusts the certificate:

- Checks the certificate revocation lists (CRL) locally on FortiGate to verify if the certificate has been revoked by the CA.
 - FortiGate can download the relevant CRL, and check if the serial number of the certificate is listed on the CRL. If the certificate is listed, it means that it has been revoked, and it is no longer trusted.
- Reads the value in the **Issuer** field to determine if it has the corresponding CA certificate. Without the CA certificate, FortiGate does not trust the certificate.
- Verifies that the current date is between the **Valid From** and **Valid To** values. If it is not, the certificate is rendered invalid.
- Validates the signature on the certificate. The signature must be successfully validated.

DO NOT REPRINT
© FORTINET

FortiGate Verifies a Digital Signature



When the CA generates a digital signature, it runs the content of the certificate through a hash function, producing a hash result, which is a mathematical representation of the data. This hash result is referred to as the *original hash result*. The CA signs the original hash result using its *private key*. The signed hash result is the digital signature. To validate a certificate, or any signed data, the digital signature and the hash result must be verified.

When validating a certificate, FortiGate runs the certificate through a hash function, producing a *fresh hash result*. FortiGate must use the same hash function, or hashing algorithm, that the CA used to create the digital signature. The hashing algorithm is identified in the certificate. Then, FortiGate verifies the digital signature using the CA *public key* and the same asymmetric algorithm that the CA used to sign the hash result. This process verifies the signature. If the key cannot restore the signed hash result, then the signature verification fails. If the verification succeeds, then it proves that the CA's private key signed the certificate. In the third, and final, part of the verification process, FortiGate compares the fresh hash result to the original hash result. If the two values are identical, then the integrity of the certificate is confirmed. If the two hash results are different, then the version of the certificate that FortiGate has is not the same as the one that the CA signed, and data integrity fails.

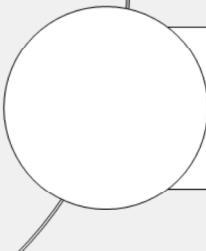
Sometimes the terms *encrypt* and *decrypt* are used to describe the digital signature process, but actually the language is more nuanced. The terms *sign* and *verify* more accurately describe digital signature processes because the purpose of digital signatures differs from the purpose of encryption. While the purpose of encryption is to obfuscate the input data so that it's unreadable, the purpose of digital signatures is to identify the signer, verify the integrity of the data, and sometimes to inextricably bind the data to the signer.

DO NOT REPRINT**© FORTINET**

Lesson Progress



**Authenticate and Secure Data
Using Certificates**



Inspect Encrypted Data



© Fortinet Inc. All Rights Reserved.

8

Good job! You now understand why and how FortiGate uses certificates to authenticate devices and people. You also understand how FortiGate uses certificates to ensure the privacy of data as it flows from FortiGate to another device, or from another device to FortiGate.

Now, you will learn how to inspect encrypted data.

DO NOT REPRINT**© FORTINET**

Inspect Encrypted Data

Objectives

- Describe SSL inspection on FortiGate
- Identify invalid certificates
- Describe import certificates on FortiGate

 © Fortinet Inc. All Rights Reserved. 9

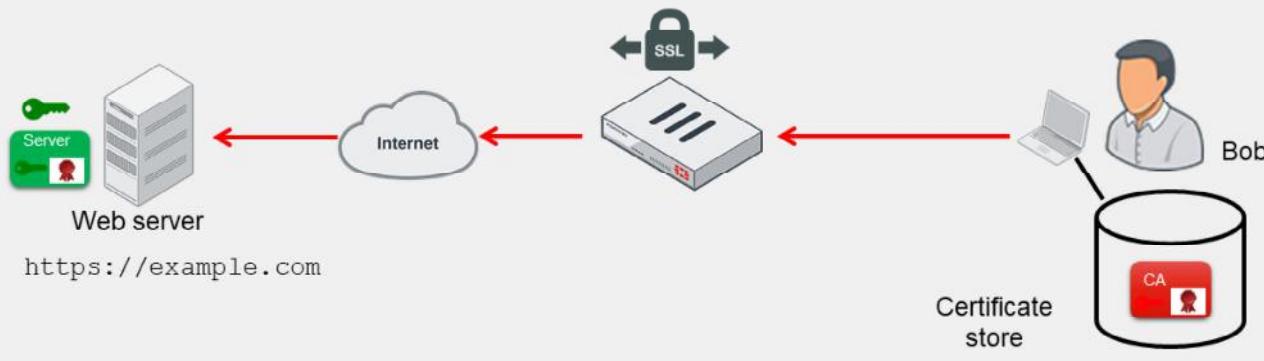
After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in understanding and configuring full SSL inspection and certificate inspection, you will be able to implement one of these SSL inspection solutions in your network.

DO NOT REPRINT
© FORTINET

Encrypted Traffic With No SSL Inspection

- Cloaked by encryption, viruses can pass through network defenses unless you enable full SSL inspection



© Fortinet Inc. All Rights Reserved. 10

While there are benefits to using HTTPS, there are risks associated with its use as well, because encrypted traffic can be used to get around normal defenses. For example, if a session is encrypted when you download a file containing a virus, the virus might get past your network security measures.

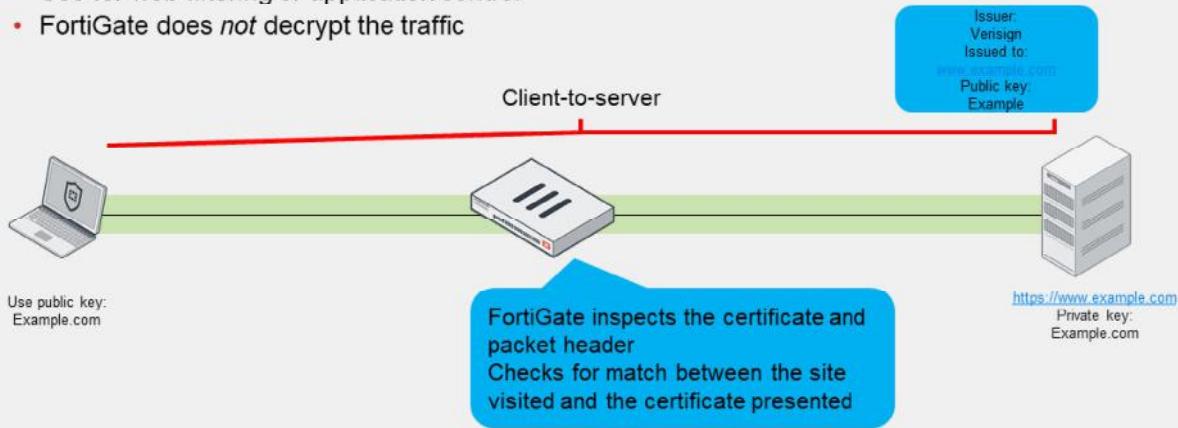
In the example shown on this slide, Bob connects to a site with a certificate issued by a legitimate CA. Because the CA is an approved CA, the CA verification certificate is in Bob's certificate store, and Bob's browser is able to establish an SSL session with the example.com site. However, unknown to Bob, the example.com site has been infected with a virus. The virus, cloaked by encryption, passes through FortiGate undetected, and enters Bob's computer. The virus is able to breach security because full SSL inspection is not enabled.

You can use full SSL inspection, also known as deep inspection, to inspect encrypted sessions.

DO NOT REPRINT**© FORTINET**

SSL Inspection Modes

- SSL certificate inspection
 - Relies on extracting the FQDN of the URL from either
 - TLS extension server name indication (SNI)
 - SSL certificate **Subject** or **SAN** fields
 - Use for web filtering or application control
 - FortiGate does *not* decrypt the traffic



There are two SSL inspection modes: SSL certificate inspection and full SSL inspection.

When using SSL certificate inspection, FortiGate is not decrypting the traffic. During the exchange of hello messages at the beginning of an SSL handshake, FortiGate parses the server name indication (SNI) from the client Hello, which is an extension of the TLS protocol. The SNI tells FortiGate the hostname of the SSL server, which is validated against the **CN** or **SAN** field in the returned server certificate. If there is no SNI exchanged, then FortiGate identifies the server by the value in the **Subject** field or **SAN** field in the server certificate.

First, FortiGate tries to get the URL from the SNI field. The SNI field is a TLS extension that contains the complete URL that the user is connecting to. It is supported by most modern browsers.

If the SNI field is not present (because the web client may not support it), FortiGate proceeds to inspect the server digital certificate to get information about the URL or the domain.

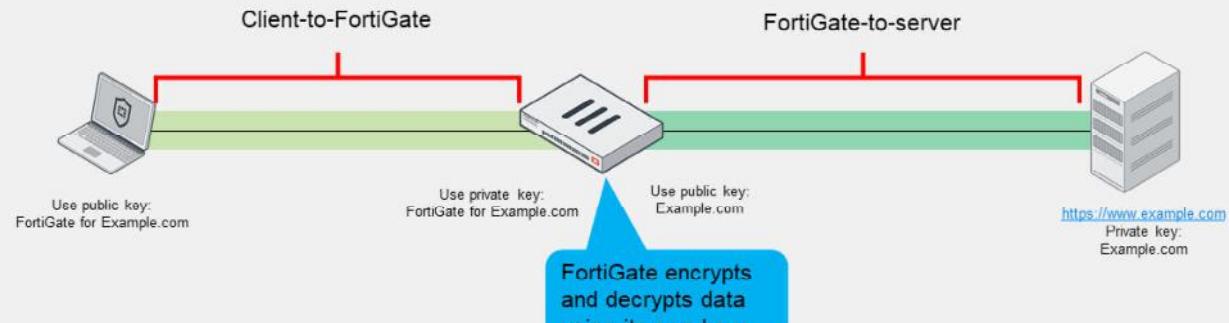
The only security features you can apply using SSL certificate inspection mode are web filtering and application control. SSL certificate inspection allows FortiGate to identify the website visited or the application in use, and categorize it. You can, therefore, use it to make sure that the HTTPS protocol isn't used as a workaround to access sites you have blocked using web filtering.

Note that while offering some level of security, certificate inspection does not allow FortiGate to inspect the flow of encrypted data.

DO NOT REPRINT
© FORTINET

SSL Inspection Modes (Contd)

- Full SSL inspection
 - FortiGate acts as a man-in-the-middle proxy
 - Maintains two separate SSL sessions—client-to-FortiGate and FortiGate-to-server
 - FortiGate encrypts and decrypts packets using its own keys
 - FortiGate can inspect the traffic



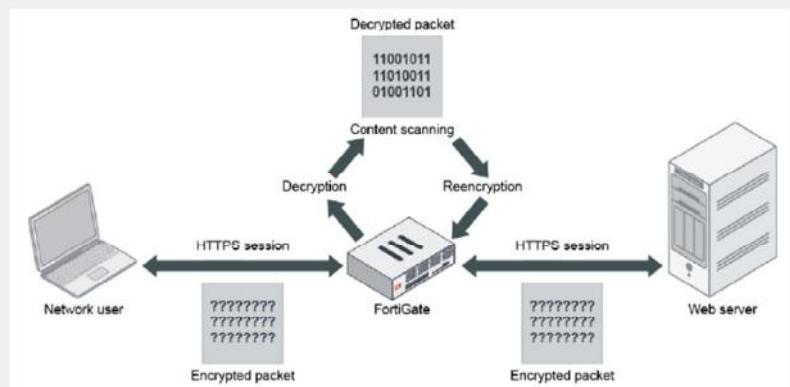
© Fortinet Inc. All Rights Reserved. 12

You can configure full SSL inspection to inspect all of the packet contents, including the payload. FortiGate performs this inspection by proxying the SSL connection. Two SSL sessions are established—client-to-FortiGate and FortiGate-to-server. The two established sessions allow FortiGate to encrypt and decrypt packets using its own keys, which allows FortiGate to fully inspect all data inside the encrypted packets.

DO NOT REPRINT**© FORTINET**

Full SSL Inspection (SSL Deep Inspection)

- Protect from attacks that use commonly used SSL-encrypted protocols
 - HTTPS
 - SMTPS
 - POP3S
 - IMAPS
 - FTPS
- FortiGate impersonates the recipient of the originating SSL session
 - Impersonates – decrypts
 - Inspects – blocks threats
 - Re-encrypts and sends to real recipient



Why we have to use deep inspection?

During an e-commerce session, you could download a file that contains a virus, or you might get a phishing email with an apparently harmless download that, when clicked, opens an encrypted session to a command and control (C&C) server and installs malware on your machine. These attacks may be able to bypass the safety measures on your network because the sessions are encrypted.

When you use deep inspection, FortiGate impersonates the recipient of the originating SSL session, and then decrypts and inspects the content to find threats and block them. It then re-encrypts the content and sends it to the real recipient. Deep inspection protects from attacks that use HTTPS and other commonly used SSL-encrypted protocols, such as SMTPS, POP3S, IMAPS, and FTPS.

DO NOT REPRINT
© FORTINET

SSL Inspection Profile Configuration

- Customized SSL/SSH inspection profile
 - Based on deep inspection profile
 - User defined

The screenshot shows the 'Edit SSL/SSH Inspection Profile' screen. Key elements include:

- Name:** custom-deep-inspection
- Comments:** Customizable deep Inspection profile.
- SSL Inspection Options:**
 - Enable SSL inspection of:** Multiple Clients Connecting to Multiple Servers (Protecting SSL Server)
 - Inspection method:** Full SSL Inspection (selected)
 - CA certificate:** Fortinet_CA_SSL (selected)
 - Blocked certificates:** Allow, Block, Ignore
 - Untrusted SSL certificates:** Allow, Block, Ignore
 - Server certificate SNI check:** Enable, Strict, Disable
 - Enforce SSL cipher compliance:** Off
 - Enforce SSL negotiation compliance:** Off
 - RPC over HTTPS:** Off



© Fortinet Inc. All Rights Reserved.

14

On FortiGate, you can select the inspection mode applied at the firewall policy level. Three predefined SSL/SSH inspection profiles are available and correspond to the most common use cases.

The profile applied by default when you create a new firewall policy is the self-explanatory no-inspection profile. Other predefined profiles available are certificate-inspection and deep-inspection, which applies full SSL inspection to outbound traffic.

The predefined certificate-inspection and deep-inspection profiles are read-only. If you want to adjust the profile parameters, you can use the predefined custom-deep-inspection profile or create a new, user-defined profile.

When you define a custom SSL/SSH profile, you can enable SSL inspection for outbound traffic with the parameter **Multiple Clients Connecting to Multiple Servers**, or for inbound traffic with the parameter **Protecting SSL Server**.

You can select the CA certificate used for traffic reencryption between FortiGate and the destination. By default, FortiGate uses the preloaded `Fortinet_CA_SSL` certificate.

You can also specify the action that FortiGate takes according to some certificate parameters or status. For instance, you can define whether you want to allow or block the traffic for untrusted or blocked certificates.

DO NOT REPRINT
© FORTINET

Exempting Sites From SSL Inspection

- Why exempt?
 - Problems with traffic
 - Legal issues

Allowlist exemption as rated by
FortiGuard web filtering as "reputable"

Exempt per web category

Exempt per address
(FQDN, IP address, address range)

Security Profiles > SSL/SSH Inspection

Exempt from SSL Inspection

Reputable websites

Web categories

Finance and Banking	<input type="button" value="X"/>
Health and Wellness	<input type="button" value="X"/>
+	

Addresses

adobe	<input type="button" value="X"/>
android	<input type="button" value="X"/>
dropbox.com	<input type="button" value="X"/>
fortinet	<input type="button" value="X"/>
google-drive	<input type="button" value="X"/>
google-play	<input type="button" value="X"/>
microsoft	<input type="button" value="X"/>
softwareupdate.vmware.com	<input type="button" value="X"/>
verisign	<input type="button" value="X"/>
+	

Log SSL exemptions

© Fortinet Inc. All Rights Reserved.

15



Within the full SSL inspection profile, you can also specify which SSL sites, 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.

Performing SSL inspection on a site that is enabled with HTTP Strict Transport Security(HSTS), for example, can cause problems with traffic. Remember, the only way for FortiGate to inspect encrypted traffic is to intercept the certificate coming from the server and generate a temporary one. After FortiGate presents the temporary SSL certificate, browsers that use HSTS refuse to proceed.

Laws protecting privacy might be another reason to bypass SSL inspection. For example, in some countries, it is illegal to inspect SSL bank-related traffic. Configuring an exemption for sites is simpler than setting up firewall policies for each individual bank. You can exempt sites based on their web category, such as **Finance and Banking**, or you can exempt them based on their address. Alternatively, you can enable **Reputable websites**, which excludes an allowlist of reputable domain names maintained by FortiGuard from full SSL inspection. This list is periodically updated and downloaded to FortiGate devices through FortiGuard.

The predefined **deep-inspection** and **custom-deep-inspection** profiles exclude some web categories—**Finance and Banking**, and **Heath and Wellness**—and some FQDN addresses such as google-play, skype, or verisign. When using the **custom-deep-inspection** profile, you can add or remove sites from this list.

DO NOT REPRINT**© FORTINET**

Invalid Certificates

- FortiGate can detect invalid certificates for a variety of reasons
 - Invalid certificates produce security warnings due to problems with the certificate details
- FortiGate can **Keep Untrusted & Allow**, **Block**, or **Trust & Allow** invalid certificates
- Selecting **Custom** allows the user to select the action for each reason

Security Profiles > SSL/SSH Inspection

Common Options	
Invalid SSL certificates	Allow Block Custom
Expired certificates	Keep Untrusted & Allow Block Trust & Allow
Revoked certificates	Keep Untrusted & Allow Block Trust & Allow
Validation timed-out certificates	Keep Untrusted & Allow Block Trust & Allow
Validation failed certificates	Keep Untrusted & Allow Block Trust & Allow
Log SSL anomalies	<input type="checkbox"/> <input checked="" type="checkbox"/>



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

- Expired: The certificate is expired.
- Revoked: The certificate has been revoked based on CRL information.
- Validation timeout: The certificate could not be validated because of a communication timeout.
- Validation failed: FortiGate could not validate the certificate, or it is not yet valid.

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

- **Keep Untrusted & Allow:** FortiGate allows the website and lets the browser decide the action to take. FortiGate takes the certificate as *untrusted*.
- **Block:** FortiGate blocks the content of the site.
- **Trust & Allow:** FortiGate allows the website and takes the certificate as *trusted*.

The certificate check feature can be broken down into two major checks, which are done in parallel:

- FortiGate checks if the certificate is invalid due to any of the four reasons described on this slide.
- FortiGate performs certificate chain validation based on the CA certificates installed locally and the certificates presented by the SSL server.

Based on the actions configured and the check results, FortiGate presents the certificate as either trusted (signed by `Fortinet_CA_SSL`) or untrusted (signed by `Fortinet_CA_Untrusted`), and either allows the content or blocks it. You can also track certificate anomalies by enabling the **Log SSL anomalies** option.

DO NOT REPRINT

© FORTINET

Untrusted SSL Certificates Setting

- Allow, block, or ignore untrusted certificates (only available if **Multiple Clients Connecting to Multiple Servers** is selected)
 - Allow:** sends the browser an untrusted temporary certificate when the server certificate is untrusted
 - Block:** blocks the connection when an untrusted server certificate is detected
 - Ignore:** uses a trusted FortiGate certificate to replace the server certificate always, even when the server certificate is untrusted



© Fortinet Inc. All Rights Reserved.

17

The browser presents a certificate warning when you attempt to access an HTTPS site that uses an untrusted certificate. Untrusted certificates include self-signed SSL certificates, unless the certificate is imported into the browser-trusted certificate store. FortiGate has its own configuration setting on the **SSL/SSH Inspection** profile, which includes options to **Allow**, **Block**, or **Ignore** untrusted SSL certificates.

When you set the **Untrusted SSL certificates** setting to **Allow**, and FortiGate detects an untrusted SSL certificate, FortiGate generates a temporary certificate signed by the built-in `Fortinet_CA_Untrusted` certificate. FortiGate then sends the temporary certificate to the browser, which presents a warning to the user indicating that the site is untrusted.

If FortiGate receives a trusted SSL certificate, then it generates a temporary certificate signed by the built-in `Fortinet_CA_SSL` certificate and sends it to the browser. If the browser trusts the `Fortinet_CA_SSL` certificate, the browser completes the SSL handshake. Otherwise, the browser also presents a warning message informing the user that the site is untrusted. In other words, for this function to work as intended, you must import the `Fortinet_CA_SSL` certificate into the trusted root CA certificate store of your browser. The `Fortinet_CA_Untrusted` certificate must *not* be imported.

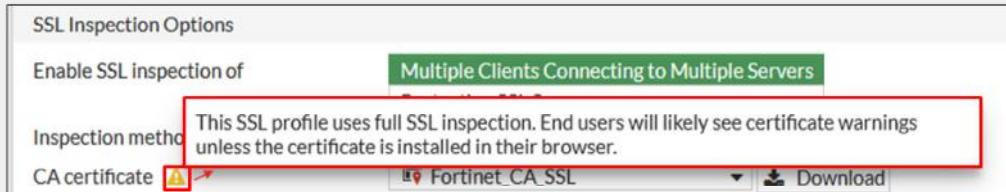
When the setting is set to **Block**, and FortiGate receives an untrusted SSL certificate, FortiGate blocks the connection outright, and the user cannot proceed.

When the setting is set to **Ignore**, FortiGate sends the browser a temporary certificate signed by the `Fortinet_CA_SSL` certificate, regardless of the SSL certificate status—trusted or untrusted. FortiGate then proceeds to establish SSL sessions.

DO NOT REPRINT**© FORTINET**

FortiGate Self-Signed CA Certificates

- By default, FortiGate uses a self-signed encrypting SSL CA certificate
 - Fortinet_CA_SSL
 - Not listed with an approved CA, therefore, by default, not trusted



- To avoid warnings on user devices
 - Install CA certificate `Fortinet_CA_SSL` as a trusted CA on user devices
 - Install a company CA certificate on FortiGate for SSL full inspection



By default, FortiGate uses a self-signed CA certificate for the reencryption required by the SSL full inspection. Because the corresponding CA is not prepopulated in client device certificate stores, users will likely see certificate warnings for traffic flows protected by the full SSL inspection.

To avoid the warning, you can install the `Fortinet_CA_SSL` certificate as a trusted CA on the user devices. You can install it as part of the deployment process for all your company computers. Alternatively on FortiGate, you can install a CA certificate, used for traffic reencryption, that is signed by your company CA. This certificate will already be recognized as valid by your company devices.

The certificate used to re-encrypt the traffic after the SSL full inspection must follow some specific requirements, which you will learn about in this lesson.

DO NOT REPRINT**© FORTINET**

Full SSL Inspection—Certificate Requirements

- Full SSL inspection requires that FortiGate act as a CA to generate an SSL private key and certificate
 - The CA certificate requires these two extensions to issue certificates:
 - cA=True
 - keyUsage=keyCertSign
- FortiGate can use:
 - The preloaded, self-signed `Fortinet_CA_SSL` certificate
 - A subordinate certificate issued by an internal CA
- The root CA certificate must be imported into the client machines



To perform full SSL inspection, FortiGate acts as a web proxy, and must act as a CA to reencrypt the traffic. The FortiGate internal CA must generate an SSL private key and certificate each time it needs to reencrypt a new traffic flow. The key pair and certificate are generated *immediately*, so the user connection with the web server is not delayed.

Although, from the user point of view, it appears as though the user browser is connected to the web server, the browser is in fact connected to FortiGate. To perform this proxy role and generate a certificate that corresponds to the server visited, the CA certificate must allow the generation of new certificates. To achieve this, it must have the following extensions: `cA` set to `True` and `keyUsage` set to `keyCertSign`.

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

All FortiGate devices come with the self-signed `Fortinet_CA_SSL` certificate that you can use for full SSL inspection. If your company has an internal CA, you can ask the CA administrator to issue a certificate for your FortiGate device. Your FortiGate device then acts as a subordinate CA. A subordinate (or intermediate) certificate is a certificate issued by the root CA that allows another device to create an endpoint (server or user) certificate on its behalf, as if it were issued directly from the CA itself.

If you use the `Fortinet_CA_SSL` certificate, or a certificate issued by your company CA to trust FortiGate and accept reencrypted SSL sessions without warning, you must import the root CA certificate to your client devices.

DO NOT REPRINT
© FORTINET

Full SSL Inspection on Inbound Traffic

- A user from the internet attempts to connect to a protected server
- The SSL connection is split into two, both terminating at FortiGate
 - FortiGate proxies the SSL traffic
 - The server certificate, private key, and chain of certificates must be installed on FortiGate
 - FortiGate presents the signed certificate to the user on behalf of the server

Security Profiles > SSL/SSH Inspection

SSL Inspection Options

Enable SSL inspection of **Multiple Clients Connecting to Multiple Servers Protecting SSL Server**

Server certificate: Cert_Webserver

Protocol Port Mapping

Inspect all ports: HTTPS port 443

https://www.example.com

© Fortinet Inc. All Rights Reserved. 20

In the example shown on this slide, FortiGate is protecting a web server. This is the second configuration option for full SSL inspection. When configuring the SSL inspection profile for this server, you must select **Protecting SSL Server**, import the server key pair to FortiGate, and then select the certificate in the **Server Certificate** field.

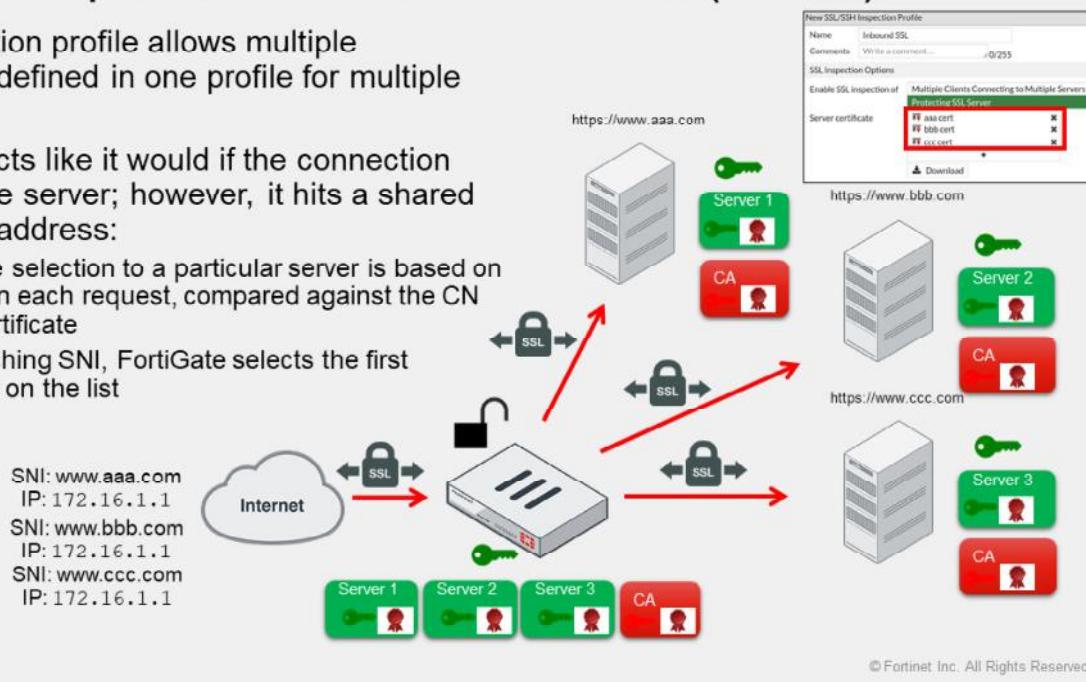
When Alice attempts to connect to the protected server, FortiGate becomes a surrogate web server by establishing a secure connection with the client using the server key pair. FortiGate also establishes a secure connection with the server but acting as a client. This configuration allows FortiGate to decrypt the data from either direction, scan it, and if it is clean, reencrypt it and send it to the intended recipient.

You must install the server certificate and private key, plus the chain of certificates required to build the chain of trust. FortiGate sends the chain of certificates to the browser for this purpose.

DO NOT REPRINT
© FORTINET

Full SSL Inspection on Inbound Traffic (Contd)

- The inspection profile allows multiple certificates defined in one profile for multiple servers
- FortiGate acts like it would if the connection targeted one server; however, it hits a shared external IP address:
 - Certificate selection to a particular server is based on the SNI on each request, compared against the CN on the certificate
 - If no matching SNI, FortiGate selects the first certificate on the list



© Fortinet Inc. All Rights Reserved. 21

By creating a full SSL inspection profile on inbound traffic, you can configure the profile to use multiple websites if they are accessible by the same external IP address. When FortiGate receives client and server hello messages, it selects the certificate to perform the full SSL inspection based on the server name indication (SNI) value compared to the common name (CN) on the certificate part of the inspection profile. If a certificate CN matches the SNI on the request, FortiGate then selects this certificate to replace the original certificate and uses it to inspect the traffic.

If the SNI does not match the CN in the certificate list in the SSL profile, FortiGate selects the first server certificate in the list.

DO NOT REPRINT

© FORTINET

Applications and SSL Inspection

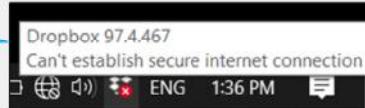
- Any SSL application might be impacted by SSL inspection (not just the browser)
 - The solution depends on the application security design
 - Consider other SSL-based protocols such as FTPS, SMTPS, and STARTTLS (not just HTTPS)
- Microsoft Outlook 365 for Windows error after enabling full SSL inspection:

Solution: Import the CA certificate into the Windows certificate store (FortiGate keeps inspecting SSL traffic)



- Dropbox for Windows error after enabling full SSL inspection:

Solution: Exempt Dropbox domains from SSL inspection (FortiGate no longer inspects SSL traffic)



More and more applications are using SSL to securely exchange data over the internet. While most of the content in this lesson centers around the operation and impact of SSL inspection on browsers, the same applies to other applications using SSL as well. After all, the browser is just another application using SSL on your device.

For this reason, when you enable SSL inspection on FortiGate, you need to consider the potential impact on your SSL-based applications. For example, Microsoft Outlook 365 for Windows reports a certificate error when you enable full SSL inspection because the CA certificate used by FortiGate is not trusted. To solve this issue, you can import the CA certificate into your Windows certificate store as a trusted root certificate authority. Because Microsoft Outlook 365 trusts the certificates in the Windows certificate store, the application won't report the certificate error anymore. Another option is to exempt your Microsoft Exchange server addresses from SSL inspection. While this prevents the certificate error, you are no longer performing SSL inspection on email traffic.

There are other applications that have built-in extra security checks that prevent man-in-the-middle attacks, such as HSTS. For example, Dropbox uses certificate pinning to ensure that no SSL inspection is possible on user traffic. As a result, when you enable full SSL inspection on FortiGate, your Dropbox client stops working and reports that it can't establish a secure connection. In the case of Dropbox, the only way to solve the connection error is by exempting the domains that Dropbox connects to from SSL inspection.

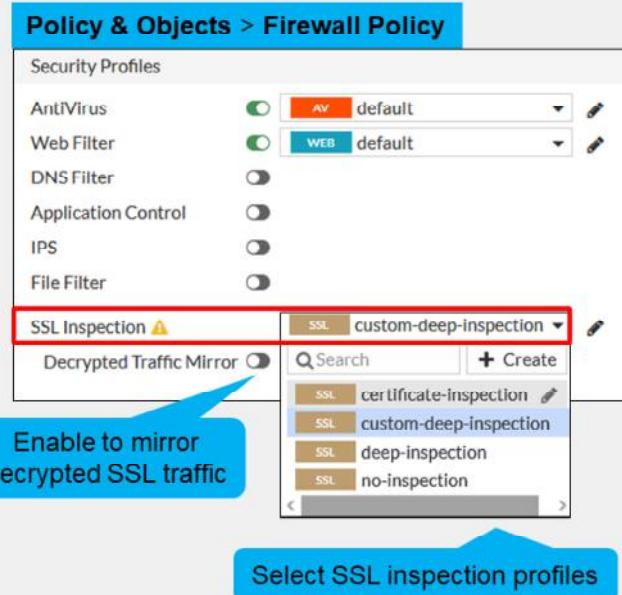
In addition, remember that SSL is leveraged by different protocols, not just HTTP. For example, there are other SSL-based protocols such as FTPS, POP3S, SMTPS, STARTTLS, LDAPS, and SIP TLS. If you have an application using any of these SSL-based protocols, and you have turned on SSL inspection along with a security profile that inspects those protocols, then the applications may report an SSL or certificate error. The solution depends on the security measures adopted by the application.

DO NOT REPRINT

© FORTINET

Applying an SSL Inspection Profile to a Firewall Policy

- For SSL inspection
 - Define SSL inspection profile
 - Allow the traffic with a firewall policy
 - Apply security profiles
 - Apply SSL inspection
- Combine SSL inspection with security profiles
- With the **no-inspection** SSL profile there is no SSL or SSH traffic inspection
 - No web filtering
 - No application control



To perform SSL inspection on traffic flowing through the FortiGate device, you must allow the traffic with a firewall policy and apply an SSL inspection profile to the policy. Note than an SSL inspection profile alone will not trigger a security inspection. You must combine it with other security profiles like **Antivirus**, **Web Filter**, **Application Control**, or **IPS**.

By default, firewall policies are set with the **no-inspection** SSL profile. Therefore, any encrypted traffic flows through uninspected. For instance, with the **no-inspection** profile, FortiGate cannot perform any web filtering for HTTPS traffic. To allow web filtering, DNS filtering, or application control for HTTPS traffic, you *must* select an SSL inspection profile with certificate inspection or a deep inspection enabled. For antivirus or IPS control, you should use a deep-inspection profile.

You can see a warning sign near the SSL inspection profile selection menu on the GUI. You will see this warning each time you select an SSL inspection profile with deep inspection. It is there to alert you to the certificate warning that can appear on the user browser when traffic is allowed with this policy. If you hover over the warning sign you can read this message: "This SSL profile uses full SSL inspection. End users will likely see certificate warnings unless the certificate is installed in their browser."

If you select a profile with full SSL inspection enabled, the option **Decrypted Traffic Mirror** appears. Enable this option if you want FortiGate to send a copy of the decrypted SSL traffic to an interface. It works with both flow-based and proxy-based inspection. When you enable **Decrypted Traffic Mirror**, FortiGate displays a window with the terms of use for this feature. The users must agree to the terms before they can use the feature. You will apply an SSL profile to a firewall policy the same way for inbound or outbound traffic flow inspection. It is the SSL profile applied that specifies the certificate in use when the FortiGate device reencrypts the traffic.

DO NOT REPRINT
© FORTINET

Certificate Warnings During Full SSL Inspection

- During full SSL inspection, browsers might display a warning because they do not trust the CA



Software is Preventing Firefox From Safely Connecting to This Site

www.goto.com is most likely a safe site, but a secure connection could not be established. This issue is caused by FGVM which is either software on your computer or your network.

- To enable a smooth user experience and prevent certificate warnings, do one of the following:
 - Use the Fortinet_CA_SSL certificate
 - And import the FortiGate CA root certificate into all the browsers
 - Use an SSL certificate issued by a private CA
 - This CA may already be available in the device browsers
- This is not a FortiGate limitation, but a consequence of how SSL and digital certificates work



© Fortinet Inc. All Rights Reserved.

24

When doing full SSL inspection using the FortiGate self-signed CA, your browser might display a certificate warning each time you connect to an HTTPS site. This is because the browser is receiving certificates signed by FortiGate, which is a CA it does not know and trust. This is not a limitation of FortiGate, but a consequence of how digital certificates are designed to work.

There are two ways to avoid those warnings:

- The first option is to download the default FortiGate certificate for SSL proxy inspection and install it on all the workstations as a trusted root authority.
- The second option is to generate a new SSL proxy certificate from a private CA. In this case, the private CA certificate must still be imported into all the browsers.

If you use an SSL certificate signed by a subordinate CA, you must ensure that the entire chain of certificates—from the SSL certificate to the root CA certificate—is installed on FortiGate. Verify also that the root CA is installed on all client browsers. This is required for trust purposes. Because FortiGate sends the chain of certificates to the browser during the SSL handshake, you do not have to import the intermediate CA certificates into the browsers.

DO NOT REPRINT
© FORTINET

Certificate Warnings on the FortiGate GUI

- By default, FortiGate uses a self-signed SSL certificate
 - Not listed with an approved CA, therefore, by default, not trusted
 - Used for HTTPS GUI access
- Available options to avoid those warnings:
 - Accept the warning at first connection
 - Use the `Fortinet_GUI_Server` certificate and import the `Fortinet_CA_SSL` certificate
 - Use a certificate signed by a recognized CA



© Fortinet Inc. All Rights Reserved. 25

By default, FortiGate uses a self-signed certificate to authenticate itself to HTTPS clients. Because the corresponding CA certificate is not prepopulated in the certificate stores of client devices, the first HTTPS connection to a FortiGate device triggers a security warning.

If you trust the FortiGate device and want to keep the self-signed certificate to establish SSL sessions, you can accept the warning and establish the connection. When you accept the warning, your browser imports the FortiGate self-signed certificate into its certificate store. So, the next time you connect to this FortiGate device, your browser already trusts the certificate presented.

Alternatively, you can configure FortiGate to use the `Fortinet_GUI_Server` certificate and add the FortiGate self-signed CA certificate—`Fortinet_CA_SSL`—to the local certificate store of any computer that needs to connect to the FortiGate device. For subsequent connections to the FortiGate GUI interface, those devices trust the certificate and allow connections without warning.

Another option for companies who manage their own CA is to generate a certificate for each of their FortiGate devices and use them to secure HTTPS connections.

DO NOT REPRINT
© FORTINET

Download Private CA Certificates From FortiGate

- Download `Fortinet_CA_SSL` private CA certificate

The screenshot shows the 'System > Certificates' page. At the top, there are buttons for 'Create/Import', 'Edit', 'Delete', 'View Details', and a red-bordered 'Download' button. Below the buttons is a table with columns for 'Name', 'Subject', and 'Comments'. There are two entries:

Name	Subject	Comments
Fortinet_CA_SSL	C = US, ST = California, L = Sunnyvale, O...	This is the default CA ce
Fortinet_CA_Untrusted	C = US, ST = California, L = Sunnyvale, O...	This is the default CA ce

- Generate a file `Fortinet_CA_SSL.cer`
- Transfer to any computer that requires it



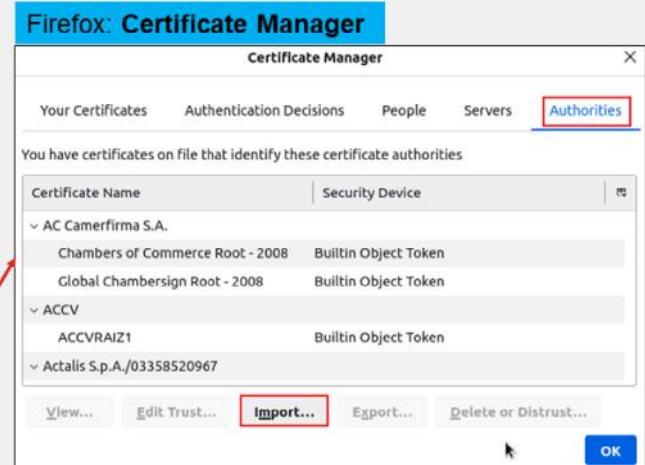
Before you can import the default CA certificate—`Fortinet_CA_SSL`—into the user devices, you must download it from FortiGate.

You can get it from the FortiGate certificate store available under the **System** menu. Upon download, FortiGate generates a `CER` file that you can import into any device, as required.

DO NOT REPRINT
© FORTINET

Import Private CA Certificates Into Endpoints

- Import Fortinet_CA_SSL private CA certificate into the user device
 - Exact process depends on the OS
 - Example for Linux and Firefox
 - Open the browser setting menu
 - Open the certificate store
 - Import the certificate as a CA



© Fortinet Inc. All Rights Reserved. 27

After you download the CA certificate from FortiGate, you can import it into any web browser or operating system. Not all browsers use the same certificate repository. For example, Firefox uses its own repository, while Internet Explorer and Chrome store certificates in a system-wide repository. In order to prevent certificate warnings, you must import the SSL certificate as a trusted root CA.

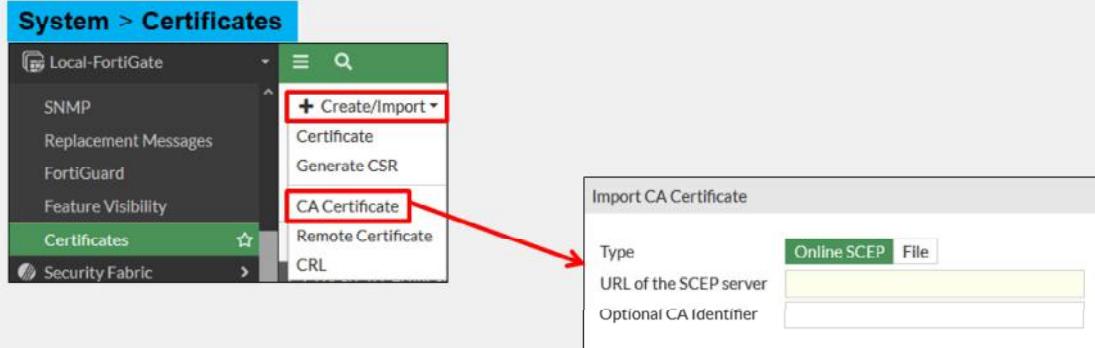
When you import the certificate, make sure that you save it to the certificate store for root authorities.

The example on this slide shows the menu you use to import a certificate into the Firefox browser.

DO NOT REPRINT
© FORTINET

Import a CA Certificate on FortiGate

- Import company-owned private CA or CA signed by a certificate authority



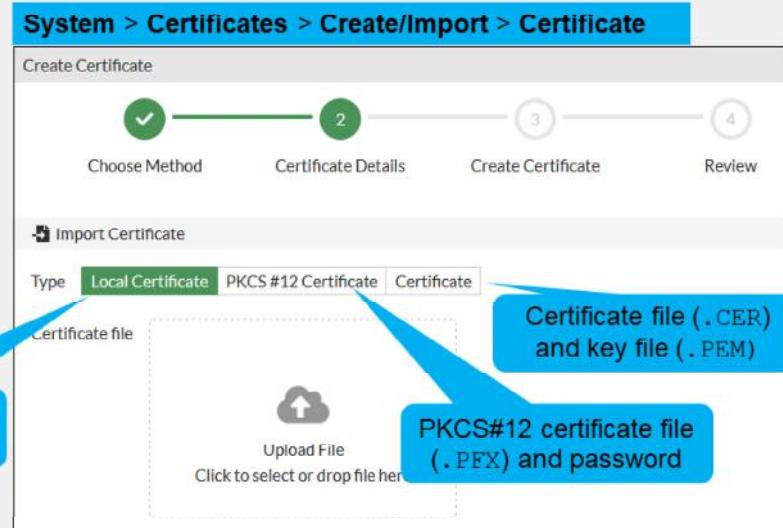
If your company has a private signing CA or a signing CA signed by a certificate authority, you can import the corresponding certificate onto the FortiGate device as shown on this slide. Note that you can import the certificate by connecting to the SCEP server or as a file. SCEP stands for Simple Certificate Enrollment Protocol, and it is a popular and widely available certificate enrollment protocol.

DO NOT REPRINT
© FORTINET

Import a Certificate on FortiGate

- Import private certificates
- Used for:
 - FortiGate GUI
- Import options:
 - Certificate after a CSR request
 - Certificate and associated key file
 - PKCS#12 certificate

Certificate file (.CER)
after a CSR request



© Fortinet Inc. All Rights Reserved. 29

If your company manages its own CA, you can generate certificates for FortiGate GUI access.

FortiGate offers three options to import private certificates:

- You can first generate a certificate signing request (CSR) and submit it to the CA for certificate generation. With this process, the key file is automatically generated and stored on FortiGate when it generates the CSR. Later, you import only the certificate file (CER file) provided by the CA.
- Another option is to import the certificate file and the associated key into the FortiGate certificate store.
- Alternatively, you can load a PKCS#12 certificate file, which is identified as a PFX file. It contains the certificate and associated private key.

DO NOT REPRINT
© FORTINET

Import CRLs on FortiGate

- CRLs are lists of revoked certificates
- Published by CA administrator and updated periodically
- Import on FortiGate
 - Online updating
 - HTTP
 - LDAP
 - SCEP
 - File import

Name	Subject	Comments	Issuer	Expires	Status	Source
CRL_1			DigiCert Inc		Valid	User
Local CA Certificate						
Fortinet_CA_SSL	C = US, ST = Califor...	This is the default...	Fortinet	2030/04/25 13:37:28	Valid	Factory
Fortinet_CA_Untrus...	C = US, ST = Califor...	This is the default...	Fortinet	2030/04/25 12:21:58	Valid	Factory



© Fortinet Inc. All Rights Reserved. 30

Because it is not possible to recall a certificate, the certificate revocation list (CRL) details certificates signed by valid CAs that should no longer be trusted. Certificates may be revoked for many reasons, such as if the certificate was issued erroneously, or if the private key of a valid certificate has been compromised.

CA administrators publish CRLs and periodically update them. You can load CRLs into the FortiGate device as files provided by CA administrators, or direct FortiGate to connect to the CRL repositories and load the corresponding list.

The recommended method to keep the list of revoked certificates up to date is to load them through one of the following available protocols: HTTP, LDAP, or SCEP. Alternatively, you can load the CRL list into the FortiGate certificate store by importing CRL files.

You can get the CRL distribution point associated with a certificate by editing it and navigating to the CRL endpoints information part.

Note that the CRL section on the FortiGate GUI **Certificates** menu is visible only after you have loaded at least one CRL.

DO NOT REPRINT

© FORTINET

FortiGate Certificate Store

- Central location for CA, certificates, and CRL on FortiGate

The screenshot shows the 'System > Certificates' page in the FortiGate interface. On the left, there are several blue callout boxes with labels pointing to specific sections in the table:

- Loaded CRLs**: Points to the 'CRL' section.
- Deep inspection signing CAs certificates**: Points to the 'Local CA Certificate' section.
- Pending CSR**: Points to the 'Local Certificate' section.
- User certificate**: Points to the 'User certificate' row.
- Company cert. for FortiGate**: Points to the 'Company cert.' row.
- CA certificates**: Points to the 'Remote CA Certificate' section.
- Imported CA certificates**: Points to the 'Imported CA certificates' section.

The table lists various certificates and CRLs:

Name	Subject	Comments	Issuer	Expires	Status	Source
CRL 1			DigiCert Inc	2024/09/27 06:21:00	Valid	User
CRL_1						
Local CA Certificate 3						
ACME-SSL-Cert	C = CA, O = ACME, OU = ACME-IIT, CN = ACME-SSL...	Company signing CA	ACME	2024/09/27 06:21:00	Valid	User
Fortinet_CA_SSL	C = US, ST = California, L = Sunnyvale, O = Fortinet, O...	This is the default CA certificate ...	Fortinet	2030/04/25 13:37:28	Valid	Factory
Fortinet_CA_Untrusted	C = US, ST = California, L = Sunnyvale, O = Fortinet, O...	This is the default CA certificate ...	Fortinet	2030/04/25 12:21:58	Valid	Factory
Local Certificate 18						
FortiGate_ACME					Pending	User
Ana	C = CA, O = ACME, OU = ACME-Finance, CN = Ana, e...		ACME	2024/09/27 06:21:00	Valid	User
Local-FortiGate	C = CA, O = ACME, OU = ACME IT, CN = ACME-FGT, ...		ACME	2024/09/27 06:04:00	Valid	User
Fortinet_Wifi	C = US, ST = California, L = Sunnyvale, O = "Fortinet, I..."	This certificate is embedded in t...	DigiCert Inc	2024/06/06 16:59:59	Valid	Factory
Fortinet_GUI_Server	C = US, ST = California, L = Sunnyvale, O = Fortinet Lt...	This is the default CA certificate ...	Fortinet	2025/08/28 10:57:01	Valid	Factory
Remote CA Certificate 5						
CA_Cert_1	C = CA, O = ACME, OU = ACME-IIT, CN = ACME-SSL...		ACME	2024/09/27 06:21:00	Valid	User
Fortinet_Wifi_CA	C = US, O = DigiCert Inc, CN = DigiCert TLS RSA SHA...		DigiCert Inc	2030/09/23 16:59:59	Valid	Factory
Fortinet_CA	C = US, ST = California, L = Sunnyvale, O = Fortinet, O...		Fortinet	2056/05/27 13:27:39	Valid	Factory

© Fortinet Inc. All Rights Reserved. 31

The central location to review the certificates imported into a FortiGate device is the certificate list available in the **Certificates** section of the **System** menu.

In this table you can view:

- The **CRL** section, which contains all loaded CRLs.
- The **Local CA Certificate** section, which contains the FortiGate signing CA certificate. By default, it contains the `Fortinet_CA_SSL` and `Fortinet_CA_untrusted` certificates. If you import a signing CA certificate from your company, it will appear in this section.
- The **Local Certificate** section, which contains device and user certificates. In the example shown on this slide you can see a user certificate, `Ana`, and a device certificate, `Local-FortiGate`. For both, the issuer is ACME, which is the company private CA in this example.
- The **Remote CA** certificate section, which is section where FortiGate displays all imported CA certificates that are not signing CA certificates.

Note that:

- The **CRL** section is visible only after you have loaded at least one CRL.
- FortiGate displays CRLs only if the corresponding CA certificate is imported into the certificate store.
- FortiGate shows the certificate signing requests (CSR) in the **Local Certificate** section with the status **Pending**.
- The **Source** column indicates the origin of the certificate, either **Factory** for certificates always present or **User** for certificates imported by an administrator user.

DO NOT REPRINT**© FORTINET**

Knowledge Check

1. What is the most common reason for a certificate error if full SSL inspection is enabled on a Windows application?
 A. The FortiGate CA certificate is not trusted.
 B. The certificate is listed in the CRL.

2. Which SSL inspection profile must be used if FortiGate is used for antivirus or IPS control?
 A. Certificate inspection
 B. Deep inspection



DO NOT REPRINT

© FORTINET

Lesson Progress



**Authenticate and Secure Data
Using Certificates**



Inspect Encrypted Data



© Fortinet Inc. All Rights Reserved. 33

Congratulations! You have completed this lesson.

Now, you will review the objectives covered in this lesson.

DO NOT REPRINT**© FORTINET**

Review

- ✓ Describe why FortiGate uses digital certificates
- ✓ Describe how FortiGate uses certificates to authenticate users and devices
- ✓ Describe how FortiGate uses certificates to ensure the privacy of data
- ✓ Describe SSL inspection on FortiGate
- ✓ Identify invalid certificates
- ✓ Describe import certificates on FortiGate



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

By mastering the objectives covered in this lesson, you learned how FortiGate uses certificates and how to manage and work with certificates in your network.

DO NOT REPRINT

© FORTINET

FORTINET
Training Institute

FortiOS Administrator

Antivirus

 FortiOS 7.6

Last Modified: 6 October 2025

© Fortinet Inc. All Rights Reserved. 1

In this lesson, you will learn how to use FortiGate to protect your network against malware.

DO NOT REPRINT

© FORTINET

Lesson Overview

Antivirus Scanning Modes

Troubleshooting



© Fortinet Inc. All Rights Reserved.

2

In this lesson, you will learn about the topics shown on this slide.

DO NOT REPRINT

© FORTINET

Antivirus Scanning Modes

Objectives

- Configure the antivirus profile in flow-based inspection mode
- Configure the antivirus profile in proxy-based inspection mode
- Configure protocol options

© Fortinet Inc. All Rights Reserved. 3

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

By demonstrating competence in antivirus basics, you will be able to understand and apply antivirus on FortiGate.

DO NOT REPRINT

© FORTINET

Antivirus Techniques



- Antivirus scanning engine uses antivirus signature databases to identify malicious codes
- Signature databases are updated in real time by FortiGuard antivirus service
- Antivirus scanning techniques:
 - Antivirus scan
 - Grayware scan
 - AI scan



A primary function of an antivirus scan is to detect and stop viruses that could cause harm to your system or compromise the security of your connected devices. It can be installed on individual endpoints (FortiClient), or it can operate as an antivirus engine to perform traffic inspection inside a next generation firewall (NGFW). The FortiGate antivirus engine operates by leveraging the information stored in signature databases that are updated by the FortiGuard antivirus service in real time. These signature databases are essentially vast repositories that contain detailed profiles of known and previously unknown viruses.

FortiGate uses many techniques to detect viruses. These detection techniques include:

- Antivirus scan: This scan is the first, fastest, simplest way to detect malware. It detects viruses that are an exact match for a signature in the antivirus database.
- Grayware scan: This scan detects unsolicited programs, known as grayware, that have been installed without the user's knowledge or consent. Often, grayware can be detected with a simple FortiGuard grayware signature.
- Artificial intelligence (AI) scan: The AI-based scan engine integrates with the regular antivirus scanning to detect zero-day malware in Windows portable executable (PE) files. Zero-day malware are new, unknown malware that have not been investigated by antimalware vendors and therefore have no existing associated signature that can detect them. FortiGuard Labs uses many malware samples to train the AI scanner to identify file features that comprise zero-day malware. Files detected by the AI scanner are identified with the W32/AI.Pallas.Suspicious virus signature.

If all antivirus features are enabled, FortiGate applies the following scanning order: antivirus scan, followed by grayware scan, followed by AI scan.

DO NOT REPRINT

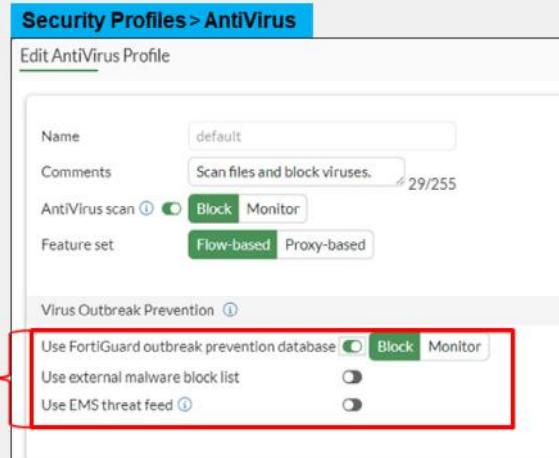
© FORTINET

Antivirus Techniques (Contd)

- FortiGate uses several industry-standard techniques for antivirus protection

- Signature-based detection
- Virus outbreak prevention
- External malware block list
- EMS threat feed

Select the techniques for antivirus protection



FortiGate uses a variety of industry-standard techniques for antivirus protection. You can configure these techniques on the GUI and CLI. The most common techniques are:

- Signature-based detection: Antivirus scan detects and compares the malicious file against virus signatures database. The FortiGuard antivirus service uses content pattern recognition language (CPRL), which is more efficient and accurate than traditional signature-based detection methods.
- Virus outbreak prevention: FortiGuard Virus Outbreak Protection Service (VOS) allows the FortiGate antivirus database to be subsidized with third-party malware hash signatures curated by FortiGuard. The hash signatures are obtained from FortiGuard's Global Threat Intelligence database. The antivirus database queries FortiGuard with the hash of a scanned file. If FortiGuard returns a match, the scanned file is deemed to be malicious. You do not have to enable the antivirus engine scan to use this feature, but you must register FortiGate with a valid FortiGuard outbreak prevention license.
- External malware block list: FortiGate can enhance the antivirus database by linking dynamic external malware block lists to FortiGate. The lists are hosted on web servers and are available through HTTP/HTTPS URLs. To use this feature, you must create a new malware hash external connection under the Security Fabric. Then, you must select the external connector in the antivirus security profile. The hash lists hosted on these web servers can be MD5, SHA1, and SHA256 hashes, and are written on separate lines in a plaintext file.
- EMS threat feed: FortiGate receives malware feeds from FortiClient EMS, which itself gathers detected malware hashes from FortiClients. If an external malware blocklist and the FortiGuard outbreak prevention database are also enabled in the antivirus profile, the checking order is: antivirus local database, EMS threat feed, external malware blocklist, and FortiGuard outbreak prevention database. If the EMS threat feed and external malware blocklist contain the same hash value, then the EMS infection will be reported if both of them are blocked.

DO NOT REPRINT

© FORTINET

Antivirus Techniques (Contd)

- Content disarm and reconstruction (CDR)
- Behavior-based detection
- CIFS scanning
- AI/ML, behavioral, and human analysis

Enabling CDR antivirus technique

Security Profiles > AntiVirus

Edit AntiVirus Profile

AntiVirus scan (Block) Monitor

Feature set: Flow-based **Proxy-based**

APT Protection Options

Content Disarm and Reconstruction (Available with proxy-based feature sets)

- Apply CDR to office files (Enabled)
- Apply CDR to PDF files (Enabled)
- Retain original file after CDR (Disabled)
- Allow transmission if a CDR error occurs (Enabled)
- Insert cover page to processed documents (Enabled)

Treat Windows executables in email attachments as viruses (Enabled)

Send files to FortiSandbox for Inspection (Disabled)

Send files to FortiNDR for Inspection (Enabled)

Include mobile malware protection (Enabled)

Quarantine (Disabled)

Virus Outbreak Prevention (Enabled)

© Fortinet Inc. All Rights Reserved.

6

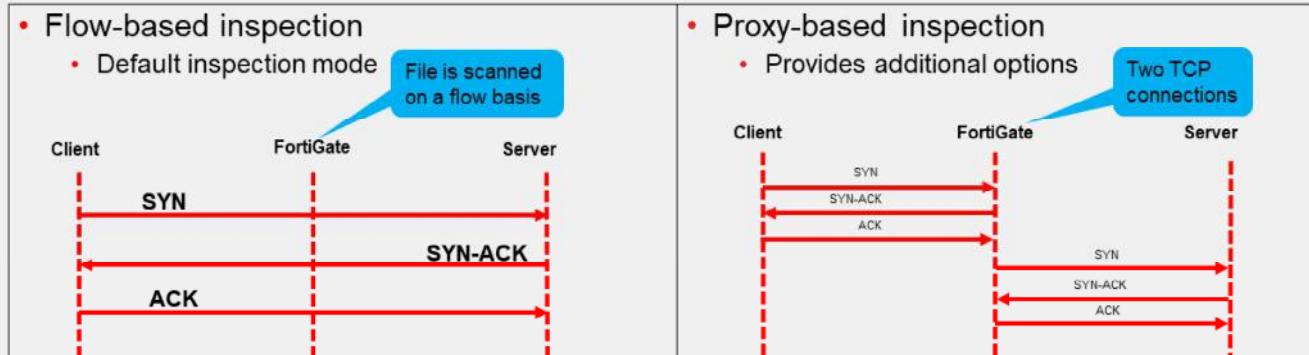
- CDR allows FortiGate to sanitize Microsoft Office documents and PDF files (including those that are in ZIP archives) by removing active content, such as hyperlinks, embedded media, JavaScript, macros, and so on from the files without affecting the integrity of the textual content. When the client tries to download the file, FortiGate removes all exploitable content in real time and sends the disarmed file to the client. CDR is supported on HTTP, SMTP, POP3, and IMAP. CDR does not support flow-based inspection modes.
- Behavior-based detection: Submit suspected malicious files to FortiSandbox for inspection.
- CIFS scanning: File filtering and antivirus scanning on common internet file system (CIFS) traffic is supported.
- AI/ML, behavioral, and human analysis: These types of analysis help you identify, classify, and respond to threats. The antivirus engine AI malware detection model integrates into regular antivirus scanning to help detect potentially malicious files, such as malicious Windows PE or executable and linkable format (ELF) files, in order to mitigate zero-day attacks. Previously, this type of detection was handled by heuristics that analyzed file behavior. The antivirus engine AI package can be downloaded by FortiOS through FortiGuard, on devices with an active antivirus subscription. The ML detection setting is enabled by default at a per-VDOM level. Files detected by the antivirus engine AI are identified with the W32/AI.Pallas.Suspicious virus signature.

DO NOT REPRINT

© FORTINET

Inspection Modes

- Available inspection modes



© Fortinet Inc. All Rights Reserved.

7

FortiGate uses different inspection modes for performance improvement and granularity.

Antivirus can operate in flow-based or proxy-based inspection mode.

Flow-based inspection takes a snapshot of content packets and uses pattern matching to identify security threats in the content. Proxy-based inspection reconstructs content that passes through FortiGate and inspects the content for security threats.

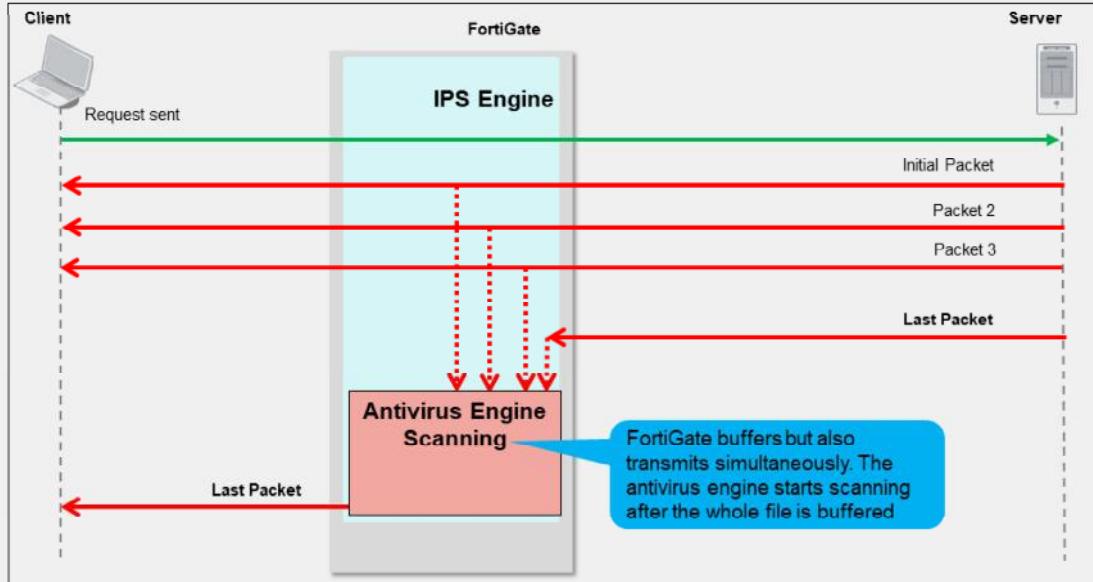
While both modes offer significant security, proxy-based mode provides more feature configuration options, while flow-based mode is designed to optimize performance.

Regardless of which mode you use, both use the full antivirus database (extended or extreme—depending on the CLI command `use-extreme-db` and the FortiGate model) and the scan techniques give similar detection rates. How can you choose which inspection mode to use?

If security is your priority, proxy-based inspection mode—with client comforting disabled—is more appropriate. If performance is your top priority, then flow-based inspection mode is more appropriate. Depending on the FortiGate model, flow-based pattern matching can be offloaded to CP8 or CP9 processors, and FortiGate models that support NTurbo can accelerate antivirus processing to enhance performance. NTurbo creates a special data path to redirect traffic from the ingress interface to the IPS engine, and from the IPS engine to the egress interface. This acceleration does not apply to proxy-based inspection.

DO NOT REPRINT
© FORTINET

Flow-Based Inspection Mode Packet Flow



© Fortinet Inc. All Rights Reserved.

8

Flow-based inspection is the default inspection mode for all new antivirus profiles.

Flow-based inspection mode uses a hybrid of two scanning modes: the default scanning mode and the legacy scanning mode. The scan method is determined by the intrusion prevention system (IPS) engine algorithm that is based on the type of file being scanned. The default antivirus scan automatically uses stream-based scanning in flow mode for HTML and JavaScript files. It triggers the legacy scan for unsupported configurations and file types.

This slide shows that the client sends a request and starts receiving packets immediately, but FortiGate also caches those packets at the same time. When the last packet arrives, FortiGate caches it and puts it on hold. Then, the IPS engine extracts the payload of the last packet, assembles the whole file, and sends it to the antivirus engine for scanning. If the antivirus scan does not detect any viruses, and the result comes back clean, the last cached packet is regenerated and delivered to the client. However, if the engine does find a virus, FortiGate resets the connection and does not send the last piece of the file. Although the receiver gets most of the file content, the file is truncated and therefore, can't be opened. The IPS engine also caches the URL of the infected file, so that if a second attempt to transmit the file is made, the IPS engine sends a block replacement message to the client instead of scanning the file again.

Because the file is transmitted at the same time, flow-based mode consumes more CPU cycles than proxy-based mode. However, depending on the FortiGate model, some operations can be offloaded to secure processing units (SPU) to improve performance.

DO NOT REPRINT
© FORTINET

Flow-Based Inspection Mode

- Default mode

The screenshot displays two main configuration panels:

Security Profiles > AntiVirus

Edit AntiVirus Profile

- Name:** default
- Comments:** Scan files and block viruses.
- AntiVirus scan:** Block (selected)
- Feature set:** Flow-based (selected)
- Inspected Protocols:** HTTP, SMTP, POP3, IMAP, FTP, CIFS (all selected)

Policy & Objects > Firewall Policy

Create New Policy

- Name:** (empty)
- Incoming Interface:** (empty)
- Outgoing Interface:** (empty)
- Source:** (empty)
- Destination:** (empty)
- Schedule:** always
- Action:** ✓ ACCEPT (selected)
- Inspection Mode:** Flow-based (selected)
- Firewall/Network Options:** NAT (disabled), IP Pool Configuration (disabled), Preserve Source Port (disabled), Protocol Options (disabled)
- Security Profiles:** AntiVirus (selected)

Annotations provide additional context:

- Action applied to the infected files:** Points to the 'Action' field in the Firewall Policy panel.
- Only display profile with flow-based feature sets:** Points to the 'Feature set' dropdown in the AntiVirus profile panel.
- Enable AntiVirus profile in the firewall policy:** Points to the 'AntiVirus' selection in the 'Security Profiles' dropdown of the Firewall Policy panel.
- Default Inspection mode is Flow-based:** Points to the 'Inspection Mode' dropdown in the Firewall Policy panel.
- Select the antivirus profile:** Points to the 'AntiVirus' selection in the 'Security Profiles' dropdown of the Firewall Policy panel.

Flow-based inspection mode is the default mode, and its configuration consists of two steps:

- Creating an antivirus profile that includes the inspected protocols and the action FortiGate will take when detects a virus-infected file.
- Applying the flow-based antivirus profile to a firewall policy.

DO NOT REPRINT

© FORTINET

Stream-Based Antivirus Scanning In Flow-Based Inspection

- Scanning for HTML and JavaScript files with antivirus engine 7.0
- Eliminates the need to cache entire file
- Improves memory usage

FortiGate will not use stream-based scanning if any of the following antivirus scanning configurations or features are enabled:

- ML-based malware detection
- Extreme antivirus database
- Greyware scan
- Mobile malware database
- External block list
- EMS threat feed
- FortiGuard outbreak prevention
- DLP
- File filter

- **Flow-based inspection mode**
 - Pattern matching can be offloaded to CP8 or CP9
 - Priority on traffic throughput



With antivirus engine 7.0, FortiGate uses stream-based antivirus scanning as the default scanning method for HTML or Javascript files. The antivirus engine determines the necessary amount of the file payload to buffer. Using the flow-based signatures, the antivirus engine scans the partial buffer in certain instances, eliminating the need to cache the entire file, which improves the memory usage.

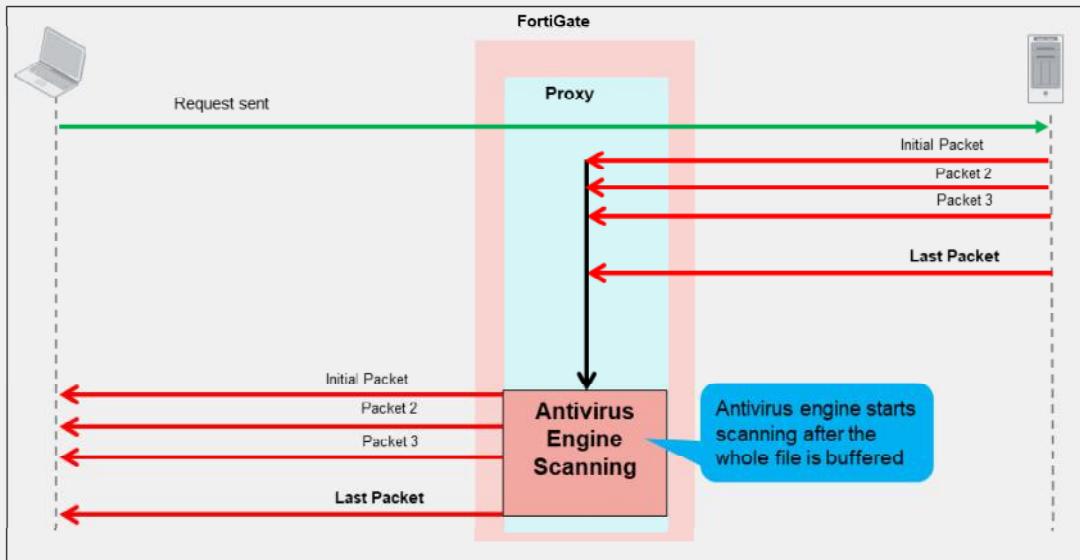
FortiGate uses legacy antivirus scan for all file types that are not supported by the default antivirus scanning. The legacy antivirus scan is also used automatically when any of the following antivirus scanning features or configurations are enabled:

- ML-based malware detection (set machine-learning-detection) (enabled by default)
- Extreme antivirus database (set use-extreme-db)
- Antivirus potentially unwanted programs (PUP) and potentially unwanted applications (PUA) grayware checks
- Mobile malware database (set mobile-malware-db)
- External block list (set external-blocklist)
- EMS threat feed
- FortiGuard outbreak prevention
- DLP
- File filter

DO NOT REPRINT

© FORTINET

Proxy Inspection Mode Packet Flow



Proxy inspection packet flow steps:

1. The client sends a request to the server, for example, a file download.
2. FortiGate receives the packet and identifies it for proxy inspection. Then, the connection is split into two parts—client-to-FortiGate and FortiGate-to-server.
3. FortiGate receives and buffers the data from the server and starts the antivirus scan once the entire file is buffered. The FortiGate antivirus engine scans for malware in files, using its signature database.
4. If the engine does not detect a threat, the file is forwarded to the client. If the engine finds a virus, no packets are delivered to the end client and the proxy sends the replacement block message to the end client.

You can configure client comforting for HTTP and FTP from the `config firewall profile-protocol-options` command tree. This allows the proxy to slowly transmit data until it can complete the buffer and finish the scan. This prevents a connection or session timeout. No block replacement message appears in the first attempt because FortiGate is transmitting the packets to the end client.

DO NOT REPRINT

© FORTINET

Proxy Inspection Mode Enabled

- Configure the antivirus profile
 - Feature set is proxy based**
- Provides additional antivirus support
 - MAPI and SSH protocol inspection
 - CDR
 - FortiNDR inspection
- Requires more than 2 GB RAM

Display profiles with flow-based or proxy-based feature sets

Available only in proxy-based inspection mode

The screenshot shows the 'Edit AntiVirus Profile' screen with the following configuration:

- Name:** default
- Comments:** Scan files and block viruses. 29/255
- AntiVirus scan:** Block, Monitor
- Feature set:** Proxy-based (highlighted)
- Inspected Protocols:**
 - HTTP (green)
 - SMTP (green)
 - POP3 (green)
 - IMAP (green)
 - FTP (green)
 - CIFS (green)
 - MAPI (red)** (highlighted)
 - SSH (red)** (highlighted)
- APT Protection Options:**
 - Content Disarm and Reconstruction (red)** (highlighted)
 - Treat Windows executables in email attachments as viruses (green)
 - Send files to FortiSandbox for Inspection (green)
 - Send files to FortiNDR for Inspection (red)** (highlighted)
 - Include mobile malware protection (green)
 - Quarantine (green)



Proxy-based inspection mode is applied when you set **Feature set** to **Proxy-based**.

Unlike flow-based inspection mode, proxy-based inspection mode allows the profile to inspect the MAPI and SSH protocols traffic, as well as sanitize Microsoft documents and PDF files using the CDR feature.

FortiNDR can be used with antivirus profiles in proxy inspection mode (flow mode is currently not supported). FortiNDR inspects high-risk files and issues a verdict to the firewall based on how close the file features match those of malware.

To enhance performance and optimize memory usage, FortiOS no longer supports proxy-related features on FortiGate models with 2 GB RAM or less. Before you upgrade from a firmware version that supports proxy-related features to FortiOS 7.4.4 or a later version that no longer supports proxy-related features on FortiGate 2 GB RAM models, it is crucial that you carefully review the upgrade scenarios.

DO NOT REPRINT
© FORTINET

Firewall Policy With Proxy Inspection Mode

The screenshot shows the 'Policy & Objects > Firewall Policy' screen. A callout bubble points to the 'Inspection Mode' field, which is set to 'Proxy-based'. Another callout bubble points to the 'AntiVirus' section under 'Security Profiles', where profiles like 'default', 'QSearch', and 'with-default' are listed. A third callout bubble points to the 'Available only in proxy-based inspection mode' note.

Set Inspection Mode to Proxy-based

Available only in proxy-based inspection mode

Proxy-based and flow-based antivirus profiles available

© Fortinet Inc. All Rights Reserved. 13

The next step is to apply the proxy-based antivirus profile to a firewall policy.
You must set the **Inspection Mode** to **Proxy-based** to be able to see proxy-based security profiles.

You can also view and select flow-based security profiles in a proxy-based policy rule. This is because other security features configured on the same policy rule may require the proxy, even if antivirus does not.

DO NOT REPRINT

© FORTINET

Stream-Based Antivirus Scanning In Proxy-Based Inspection

- Default scan mode in proxy mode
- Supports ZIP, GZIP, BZIP2, TAR, and ISO (ISO 9660) archive file types
- Supports HTTP(S), FTP(S), and SCP/SFTP protocols
- Inspects the contents of large archive files without buffering the entire file
- Decompresses and scans large archive files
- Identifies file types quickly
- Detects viruses effectively
- Can be disabled through the CLI

```
#config antivirus profile
  edit <string>
    set feature-set proxy
    set scan-mode {default* | legacy}
  next
end
```

- Proxy-based inspection mode
 - Required for its additional options
 - Priority on network security



Protecting emails
received by mail servers
through SMTP or MAPI

legacy settings
disables stream-based
scanning



© Fortinet Inc. All Rights Reserved. 14

Using proxy inspection antivirus allows you to use stream-based scanning, which is enabled by default. Stream-based scanning scans large archive files by decompressing the files and then scanning and extracting them at the same time. This process optimizes memory use to conserve resources on FortiGate. Viruses are detected even if they are in the middle or toward the end of these large files.

Stream-based scanning supports ZIP, GZIP, BZIP2, TAR, and ISO (ISO 9660) archive files types and HTTP(S), FTP(S), and SCP/SFTP protocols. It does not support HTTP POST.

Stream-based scanning is not supported if the following features are enabled:

- DLP
- Quarantine
- FortiGuard outbreak prevention, external block list, and EMS threat feed
- Content disarm

DO NOT REPRINT

© FORTINET

Antivirus Block Page

- Information available on the antivirus block page

The image shows two screenshots side-by-side. On the left is the 'Antivirus Block Page' from Fortinet, featuring a 'High Security Alert' message stating that a file is infected with the 'EICAR TEST FILE'. It includes fields for 'File name', 'Virus name', 'Website host or URL', and 'Reference URL'. A red arrow points from the 'Link to FortiGuard Encyclopedia' button to the right screenshot. On the right is the 'Threat Encyclopedia' page from FortiGuard Labs, showing details for the 'EICAR_TEST_FILE' including its release date (Oct 15, 1996) and analysis status.

Antivirus Block Page Labels:

- File name
- Virus name
- Website host or URL
- Reference URL
- Link to FortiGuard Encyclopedia

© Fortinet Inc. All Rights Reserved. 15

For antivirus scanning in proxy-based inspection mode (with client comforting disabled), the block replacement page is displayed *immediately* when a virus is detected.

For flow-based inspection mode scanning, if a virus is detected at the start of the stream, the block replacement page is displayed at the *first attempt*. If a virus is detected after a few packets have been transmitted, the block replacement page is *not* displayed. However, FortiGate caches the URL and can display the replacement page immediately, on the second attempt.

Note that if deep inspection is enabled, all HTTPS-based applications also display the block replacement message.

The block page includes the following:

- File name
- Virus name
- Website host and URL
- Username and group (if authentication is enabled)
- Link to FortiGuard Encyclopedia—which provides analysis, recommended actions (if any), and detection availability

You can go directly to the FortiGuard website to view information about other malware, and scan, submit, or do both, with a sample of suspected malware.

DO NOT REPRINT
© FORTINET

Configuring Protocol Options

- Available for both proxy-based and flow-based firewall policies

The screenshot shows two windows side-by-side. On the left is the 'Policy & Objects > Firewall Policy' window, where a new policy is being created. In the 'Protocol Options' dropdown, the 'proto default' profile is selected. A red arrow points from this dropdown to the 'Protocol Port Mapping' section of the 'Policy & Objects > Protocol Options' window on the right. This mapping section lists various protocols (HTTP, SMTP, POP3, IMAP, FTP, NNTP, MAPI, DNS, CIFS) with their original ports and mapped ports. A blue callout box highlights the 'Specify' field for the FTP port, which contains '21,22,23'. Another blue callout box notes that multiple ports can be specified separated by commas. On the right side of the interface, there are other options like 'Comfort Clients' and 'Web Options'.

Port mapping works only in proxy-based inspection

Name of the protocol options profile to apply in a firewall policy

You can specify more than one port number (separated by commas)

Prevents transmission failures

Protocol options provide more granular control than antivirus profiles. You can configure protocol port mappings, common options, web options, email options, and more. Some options, like **Protocol Port Mapping**, apply only to proxy-based inspection.

When proxy-based antivirus scanning is enabled, FortiGate buffers files as they are downloaded. Once the entire file is captured, FortiGate begins scanning the file. The user must wait during the buffering and scanning procedure. After the scan is completed and if no infection is found, the file is sent to the next step in the process flow. If the file is large, this part of the process can take some time. In some cases, enough time that some users may get impatient and cancel the download.

The **Comfort Clients** option mitigates this potential issue by feeding a trickle of data while waiting for the scan to complete. The user is aware that processing is taking place and that there has not been a failure in the transmission. The slow transfer rate continues until the antivirus scan is complete. The transfer will proceed at full speed once the file is scanned successfully and does not contain any viruses.

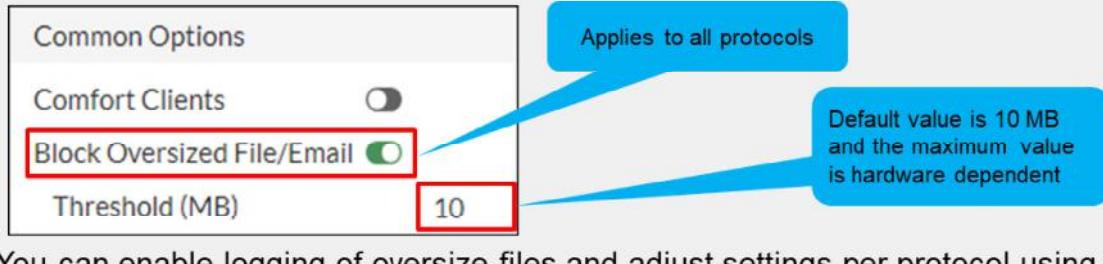
Antivirus and other security profiles, such as web filtering, DNS filtering, and data loss prevention (DLP), use protocol options.

After configuring the protocol options, you should apply them to the firewall policy.

DO NOT REPRINT
© FORTINET

Protocol Options—Large Files

- By default, files that are bigger than the oversize limit are bypassed from scanning
- You can modify this behavior for all protocols



- You can enable logging of oversize files and adjust settings per protocol using the CLI

```
config firewall profile-protocol-options
  edit <profile name>
    set oversize-log {enable|disable}
    config <protocol Name>
      set options oversize
      set oversize-limit <integer>
    end
  end
end
```

Oversize file logging setting

Name of the specific protocol

© Fortinet Inc. All Rights Reserved. 17

So, what does the additional granularity provided by protocol options include? It allows you to block large files. You can also adjust the threshold for optimal performance in your network. The buffer limit varies by model. A smaller buffer minimizes proxy latency (for both scanning modes) and RAM usage, but that may allow viruses to pass through undetected. When a buffer is too large, clients may notice transmission timeouts. You must balance the two.

You can also disable the oversize option and adjust the oversize-limit per protocol from the config firewall profile-protocol-options command tree.

If you aren't sure about the value to set the oversize-limit to, you can temporarily enable the oversize-log to see if FortiGate is scanning large files frequently. You can then adjust the value accordingly.

DO NOT REPRINT
© FORTINET

Protocol Options—Compressed Files

- Archives are unpacked and files and archives within are scanned separately
- Password-protected archives cannot be decompressed
- Increasing the limits impacts memory usage

```
config firewall profile-protocol-options
  edit <profile_name>
    config <protocol_name>
      set uncompressed-oversize-limit [1-<model_limit>]
      set uncompressed-nest-limit [1-<model_limit>]
    end
  end
```

Oversize limit specific to decompressed files

Nested archive limit



Large files are often compressed. When compressed files go through scanning, the compression acts like encryption: the signatures won't match. So, FortiGate must decompress the file in order to scan it.

Before decompressing a file, FortiGate must first identify the compression algorithm. Some archive types can be correctly identified using only the header. Also, FortiGate must check whether the file is password protected. If the archive is protected with a password, FortiGate can't decompress it and, therefore, can't scan it.

FortiGate decompresses files into RAM. Just like other large files, the RAM buffer has a maximum size. Increasing this limit may decrease performance, but it allows you to scan larger compressed files.

If an archive is nested—for example, if an attacker is trying to circumvent your scans by putting a ZIP file inside a ZIP file—FortiGate will try to undo all layers of compression. By default, FortiGate will attempt to decompress and scan up to 12-layers deep, but you can configure it to scan up to the maximum number supported by your device (usually 100). Increase this setting is not recommended because it increases RAM usage.

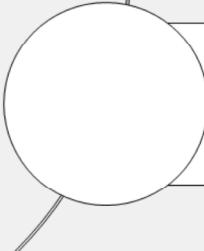
DO NOT REPRINT

© FORTINET

Lesson Progress



Antivirus Scanning Modes



Troubleshooting



© Fortinet Inc. All Rights Reserved.

19

Good job! You now understand antivirus scanning modes.

Now, you will learn about antivirus troubleshooting.

DO NOT REPRINT

© FORTINET

Troubleshooting

Objectives

- Monitor antivirus events
- Troubleshoot common antivirus issues

© Fortinet Inc. All Rights Reserved. 20

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

By demonstrating competence in troubleshooting common antivirus issues, you will be able to configure and maintain an effective antivirus solution.

DO NOT REPRINT

© FORTINET

Antivirus Logs

The screenshot shows the FortiGuard antivirus interface. At the top, a summary table shows 12 events, with the first entry for 'AntiVirus' highlighted. A red box highlights the 'AntiVirus' icon in the summary table. Below this is a detailed log table with three entries. The second entry, dated 2024/10/30 14:09:58, is highlighted with a red box and has a blue callout pointing to it with the text 'Log entry when a virus is detected'. To the right of the log table is a detailed view of the second log entry, which includes fields like Protocol (FTP), Service (eicar.com), File Name (EICAR_TEST_FILE), and Action (Blocked). A red box highlights the 'Details' button in this panel. Another blue callout points to this button with the text 'Details on the virus with FortiGuard reference'. The bottom right corner of the interface shows '© Fortinet Inc. All Rights Reserved. 21'.

Date/Time	Service	Source	File Name	Virus/Botnet	User	Details	Action	Infection Type
2024/10/30 14:09:58	FTP	10.0.1.10	eicar.com	EICAR_TEST_FILE		Host: 10.200.1.254	Blocked	Malicious
2024/10/30 14:09:58	FTP	10.0.1.10	eicar.com	EICAR_TEST_FILE		Host: 10.200.1.254	Blocked	Malicious
2024/10/30 14:09:58	FTP	10.0.1.10	eicar.com	EICAR_TEST_FILE		Host: 10.200.1.254	Blocked	Malicious

Logging is an important part of managing a secure network. When you enable unified threat management (UTM) logging in a firewall policy, you can find details on the **AntiVirus** log page under **Security Events**.

When the antivirus scan detects a virus, by default, it creates a log about which virus was detected, as well as the action, policy ID, antivirus profile name, and detection type. It also provides a link to more information on the FortiGuard website.

When you enable oversized file logging, a log entry is also created with the details that include the message, "Size limit is exceeded".

DO NOT REPRINT
© FORTINET

Forward Traffic Logs

The screenshot shows two windows from a FortiGate interface. The left window, titled 'Log & Report > Forward Traffic', displays a table of log entries. One specific entry is highlighted with a red box and a blue arrow pointing to it, labeled 'Forward traffic log entry'. The right window, titled 'Log Details', shows detailed information for a selected log entry. It has tabs for 'Details' and 'Security', with 'Security' selected. A red box highlights the 'Security' tab, and a red arrow points from the 'Forward traffic log entry' to this tab. Another blue arrow points from the 'Forward traffic log entry' to the detailed log information in the right window.

Date/Time	Source	Device	Destination	Application Name	Result	Policy ID
2024/10/30 14:26:53	10.0.1.10	34.107.221.62 (detectportal.firefox.com)	HTTP	✓ Accept (926 B / 1.17 kB)	Full_Access [1]	
2024/10/30 14:26:06	10.0.1.10	10.200.1.254	HTTP	✗ Deny (Deny: UTM Blocked)	Full_Access [1]	
2024/10/30 14:25:56	10.0.1.10	10.200.1.254	HTTP	✗ Deny (Deny: UTM Blocked)	Full_Access [1]	
2024/10/30 14:25:23	10.0.1.10	10.200.1.254	HTTP	✗ Deny (Deny: UTM Blocked)	Full_Access [1]	
2024/10/30 14:23:09	10.0.1.200	96.45.43.43 (dns1.fortiguard.net)	tcp/853	✓ Accept (16.75 kB / 17.25 kB)	Full_Access [1]	

Forward traffic log entry

Security log details

Log Details

Security

AntiVirus

Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:109.0) Gecko/201001 Firefox/117.0

Submitted to FortiSandbox: false

Direction: incoming

Destination UUID: 7bc87d34-7916-51e7-3d5b-71812a61b98e

Detection Type: av-engine

Event original timestamp: 1730.312.755.004.399.400

Event type: infected

File Name: eicar.com

HTTP request method: GET

Infection Type: Malicious

Level: Warning

Profile: default

Quarantine Skip: Quarantine-disabled

Reference: https://fortiguard.com/virusinfo/eicar/av-test/2172

Referrer URI: http://10.200.1.254/test_av.html

Source UUID: 703e6ff6-791a-51e7-daa0-9859ce6c1d02

Sub Type: virus

Transaction ID: 1

Type: utm

Timezone: -0700

URL: http://10.200.1.254/eicar.com

Virus/Botnet: EICAR_TEST_FILE

Virus Category: Virus

Virus ID: 2.172

Details: URL: http://10.200.1.254/eicar.com

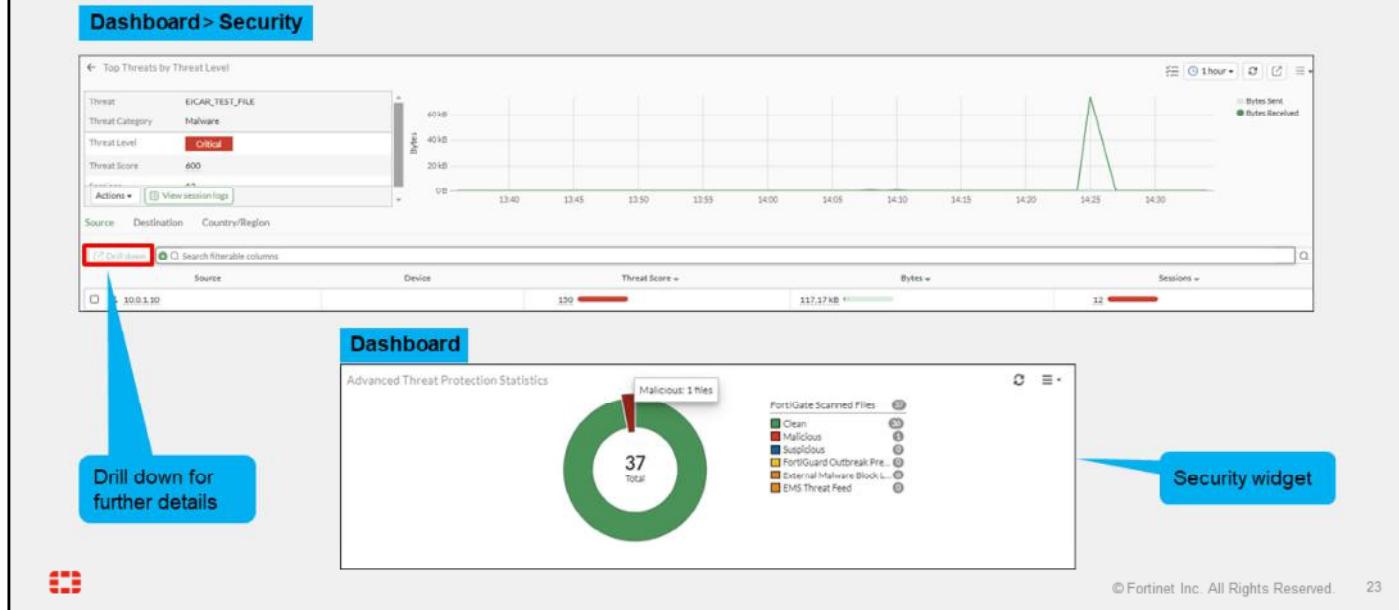


You can also view log details on the **Forward Traffic** page, where firewall policies record traffic activity. You can find a summary of the traffic on which FortiGate applied an antivirus action in the corresponding security details.

DO NOT REPRINT
© FORTINET

Security Dashboard

- Security widget and dashboard allow you to monitor your network



You can also use the **Security** dashboard to view relevant information regarding threats to your network. The security dashboard organizes information into source and destination, and allows you to drill down to see session logs details.

You can add the **Advanced Threat Protection Statistics** widget to the dashboard for monitoring purposes.

DO NOT REPRINT
© FORTINET

Troubleshooting Common Antivirus Issues

- Verify FortiGuard antivirus license

The screenshot shows the 'FortiGuard Distribution Network' interface under 'System > FortiGuard'. In the 'License Information' section, there is a table with columns for 'Entitlement' and 'Status'. Under 'Entitlement', 'Advanced Malware Protection' is listed. In the 'Status' column, it says 'Licensed (Expiration Date: 2026/01/17)' with a red box around it. To the right of the table, a blue callout bubble contains the text 'Valid license'.

Entitlement	Status
Advanced Malware Protection	Licensed (Expiration Date: 2026/01/17) <input checked="" type="radio"/> Version 2.05360 <input type="radio"/> Version 90.01635 <input type="radio"/> Version 7.00030 <input type="radio"/> Version 90.01635 <input checked="" type="radio"/> Licensed (Expiration Date: 2026/01/17)

- Force FortiGate to check for new antivirus updates

```
# execute update-av
```

- Run the real-time update debug to isolate update-related issues

```
# diagnose debug application update -l
# diagnose debug enable
# execute update-av
```



Viruses are constantly evolving and you must have the latest antivirus definitions version to ensure correct protection. With a valid license, FortiGate checks regularly for updates. If an antivirus profile is applied on at least one firewall policy, you can also force an update of the antivirus definitions database with the CLI command `execute update-av`.

If you are having issues with the antivirus license or FortiGuard updates, start troubleshooting with basic connectivity tests. Most of the time, issues related to updates are caused by connectivity problems with FortiGuard servers. You can do the following to handle common antivirus issues:

- Make sure that FortiGate has a stable internet connection and can resolve DNS (`update.fortinet.net`).
- If there is another firewall between FortiGate and the internet, make sure TCP port 443 is open and traffic is allowed from and to FortiGate.
- If you continue to see issues with the update, run the real-time debug command to identify the problem.

DO NOT REPRINT
© FORTINET

Troubleshooting Common Antivirus Issues (Contd)

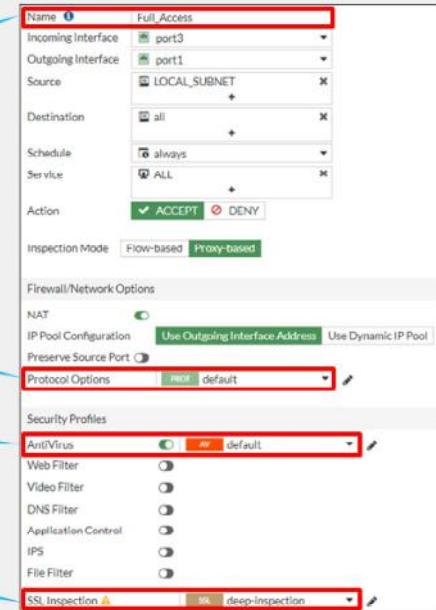
- Unable to detect viruses even with a valid contract?

Check firewall policy configuration

In proxy-based inspection mode,
verify the protocol port mapping

Verify the antivirus profile applied

For encrypted protocols,
you must select deep inspection



What if you have a valid contract and updated database, but you are still having issues catching viruses? Start troubleshooting for basic configuration errors. Most of the time, issues are caused by misconfiguration on the device. You can do the following to verify:

- Make sure that the correct antivirus profile is applied on the correct firewall policy.
- Make sure that the correct protocol port is configured when proxy-based inspection mode is used.
- Make sure that you are using the correct antivirus profile and SSL/SSH inspection on all firewall policies.

DO NOT REPRINT
© FORTINET

Troubleshooting Common Antivirus Issues (Contd)

- Check useful antivirus commands

```
# get system performance status
```

Virus caught: 100 total in 1 minute

Displays virus statistics for the last one minute

```
# diagnose antivirus database-info
```

version: 90.01635(04/22/0022 13:26)

atdb found 1 loaded 1

virus ID count 29630

grayware ID count 140

signature ID count 49988

etdb found 1 loaded 1

virus ID count 60712

grayware ID count 4429

signature ID count 806735

exdb found 1 loaded 0

virus ID count 0

grayware ID count 0

signature ID count 0

Displays current antivirus database information

Displays version information

```
# diagnose autoupdate versions  
Virus Definitions
```

Version: 90.01635 signed

Contract Expiry Date: Mon Jan 19 2026

Last Updated using manual update on Mon

Apr 25 13:52:18 2022

Last Update Attempt: Wed Sep 13 06:27:50
2023

Result: No Updates

```
# diagnose antivirus test "get scantime"  
antivirus test (manager)
```

0~5s: 0

5~10s: 0

10~15s: 0

15~20s: 0

20~25s: 0

25~30s: 0

>30s: 0

Displays scan times for infected files



To troubleshoot further common antivirus issues, you can check the information provided by the following commands:

- get system performance status: Displays statistics for the last one minute.
- diagnose antivirus database-info: Displays current antivirus database information.
- diagnose autoupdate versions: Displays current antivirus engine and signature versions.
- diagnose antivirus test "get scantime": Displays scan times for infected files.

DO NOT REPRINT**© FORTINET**

Knowledge Check

1. Which additional features of an antivirus profile are available in proxy-based inspection mode?
 A. MAPI, SSH, CDR, and FortiNDR
 B. Full and quick

2. What does the oversize files logging setting do?
 A. Enables logging of all files that exceed the oversize limit
 B. Logs all files that are over 5 MB

3. Which feature does not support stream-based scanning?
 A. Data loss prevention (DLP)
 B. Signature-based detection



DO NOT REPRINT

© FORTINET

Lesson Progress



Antivirus Scanning Modes



Troubleshooting



© Fortinet Inc. All Rights Reserved. 28

Congratulations! You have completed this lesson.

Now, you will review the objectives covered in this lesson.

DO NOT REPRINT

© FORTINET

Review

- ✓ Apply the antivirus profile in flow-based inspection modes
- ✓ Apply the antivirus profile in proxy-based inspection modes
- ✓ Compare inspection modes
- ✓ Configure protocol options
- ✓ Monitor antivirus events
- ✓ Troubleshoot common antivirus issues



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

By mastering the objectives covered in this lesson, you learned how to use FortiGate features and functions to protect your network against viruses.

DO NOT REPRINT

© FORTINET

FORTINET
Training Institute

FortiOS Administrator

Web Filtering

 FortiOS 7.6

Last Modified: 6 October 2025

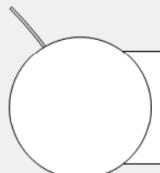
© Fortinet Inc. All Rights Reserved. 1

In this lesson, you will learn how to configure web filtering on FortiGate to control web traffic in your network.

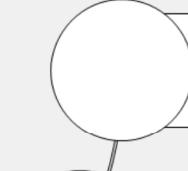
DO NOT REPRINT

© FORTINET

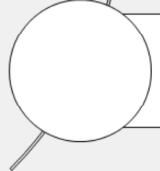
Lesson Overview



Inspection Modes



Web Filtering Basics



Troubleshooting



© Fortinet Inc. All Rights Reserved.

2

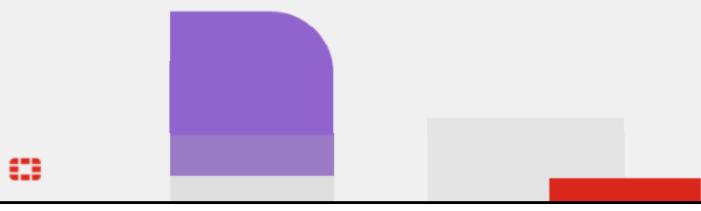
In this lesson, you will learn about the topics shown on this slide.

DO NOT REPRINT**© FORTINET**

Inspection Modes

Objectives

- Select the correct inspection mode flow or proxy based on security needs

A decorative graphic in the bottom left corner consists of several overlapping squares. A large purple square is at the top, followed by a smaller grey square, and a red square at the bottom right.

© Fortinet Inc. All Rights Reserved. 3

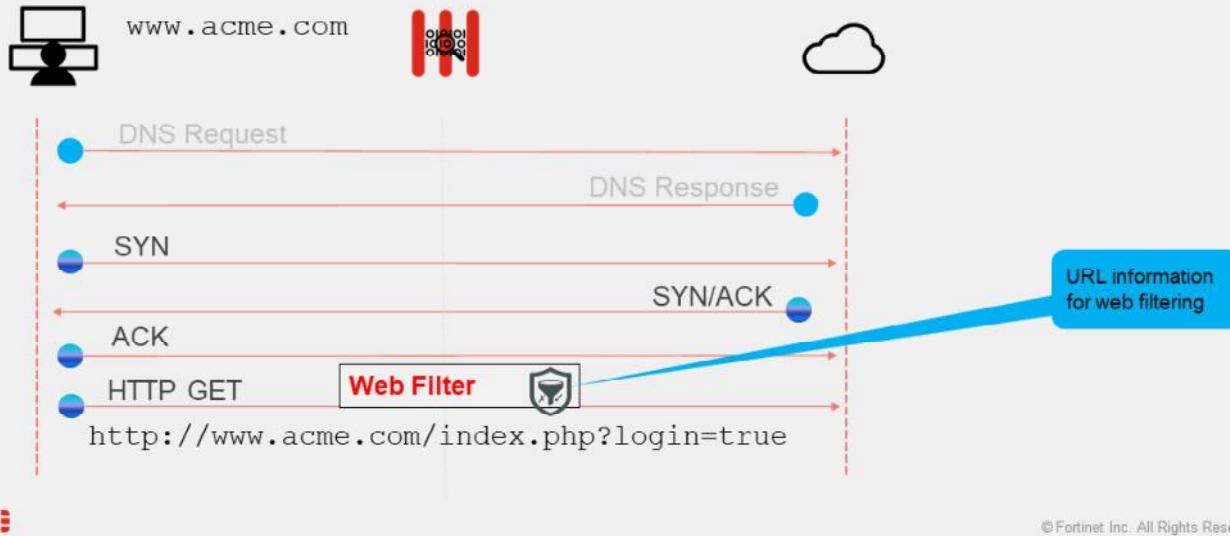
After completing this lesson, you should be able to achieve the objective shown on this slide.

By demonstrating competence in understanding inspection modes, you will be able to implement the appropriate inspection modes to support the desired security profiles.

DO NOT REPRINT

© FORTINET

When Does Web Filtering Activate With Initial Unencrypted HTTP Traffic?



© Fortinet Inc. All Rights Reserved.

4

FortiGate web filtering helps stop infections from malware sites and prevent communication if an infection occurs.

After a TCP connection is established, the user requests the content of a specific web site (for example, www.acme.com) using an HTTP GET request.

FortiGate checks the HTTP GET request to collect the information shown in the slide and sends a real-time request to the FortiGuard servers to determine the category of the website. Based on the category information from the FortiGuard Distribution Network (FDN), FortiGate performs the specific action based on the profile applied to the policy.

In FortiOS, there are three main components of web filtering:

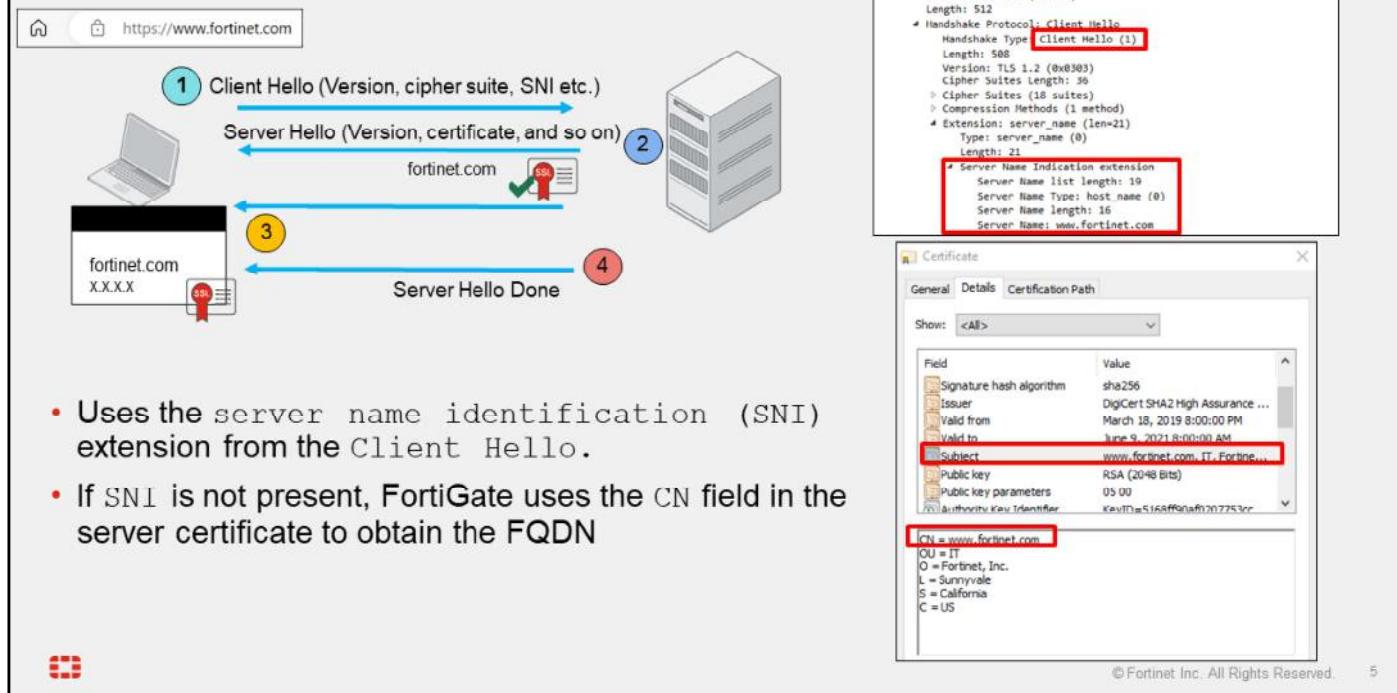
- Web content filtering: blocks web pages containing words or patterns that you specify.
- URL filtering: uses URLs and URL patterns to block or exempt web pages from specific sources, or block malicious URLs discovered by FortiSandbox.
- FortiGuard Web Filtering service: provides many additional categories you can use to filter web traffic.

If you filter by domain, sometimes the filter blocks too much. For example, each blog on tumblr.com is viewed as a separate piece of content because they have different authors. So, when filtering blogs, you might want to be more specific and block blogs based on specific parts of the URL, for example, tumblr.com/hacking.

DO NOT REPRINT

© FORTINET

SSL Certificate Inspection



The stages of the TLS handshake process are as follows:

1. The "Client Hello" message, which includes SNI, is sent to the server.
2. The server receives the packet from the client and replies with the "Server Hello" message, which may initially include empty information in the SNI response.
3. The server sends the authentication details required by the SNI request.
4. Finally, the server sends a "Server Hello Done" message.

For encrypted protocols, FortiGate requires additional inspection. When using SSL certificate inspection, FortiGate inspects the headers up to only the SSL/TLS layer. FortiGate doesn't decrypt or inspect any encrypted traffic. Using this method, FortiGate inspects only the initial unencrypted SSL handshake.

If the SNI field exists, FortiGate uses it to obtain the FQDN to rate the site. If the SNI isn't present, FortiGate retrieves the FQDN from the CN field of the server certificate.

In some cases, the CN server name might not match the requested FQDN. For example, the value in the common name (CN) field in the digital certificate of youtube.com is google.com. So, if you connect to youtube.com from a browser that doesn't support SNI, and FortiGate uses the SSL certificate inspection method, FortiGate assumes, incorrectly, that you are connecting to google.com, and uses the google.com category instead of the category for youtube.com.

SSL certificate inspection works correctly with web filtering, because the full payload does not need to be inspected.

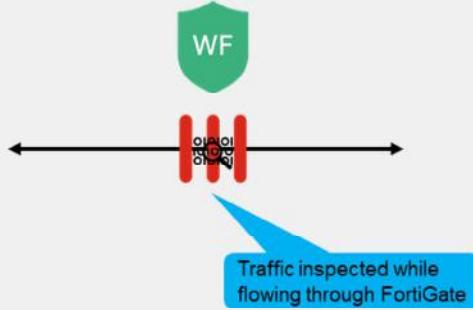
DO NOT REPRINT

© FORTINET

Web Filtering Inspection Modes

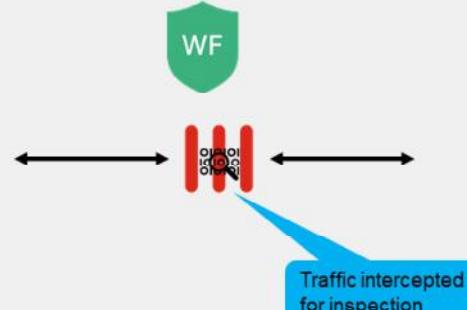
- Flow-based inspection

- Default inspection mode
- Requires fewer processing resources
- Faster scanning



- Proxy-based inspection

- More thorough inspection
- Provides additional options
- More resource intensive



- Firewall policy must include an SSL inspection profile and a web filter profile



© Fortinet Inc. All Rights Reserved.

6

You can configure web filtering in flow-based or proxy-based inspection mode.

The flow-based inspection method examines the file as it passes through FortiGate, without buffering it.

Packets are analyzed and forwarded as they are received, without waiting for the complete file or web page.

The advantages of flow-based inspection mode are:

- The user sees a faster response time for HTTP requests compared to proxy-based inspection mode.
- There is less chance of a time-out error caused by the server at the other end responding slowly.
- From FortiOS 7.4.4 and later flow-based web filter profiling supports safe search and restrictions on YouTube and Vimeo access.

The disadvantages of flow-based inspection mode are:

- A number of security features that are available in proxy-based inspection mode are not available in flow-based inspection mode.
- Fewer actions are available based on the categorization of the website by FortiGuard services.

On the other hand, proxy-based scanning refers to transparent proxy. It's called transparent because, at the IP layer, FortiGate is not the destination address, but FortiGate *does* intercept the traffic. When proxy-based inspection is enabled, FortiGate buffers traffic and examines it *as a whole*, before determining an action.

Because FortiGate examines the data as a whole, it can examine more points of data than it does when using flow-based inspection.

The proxy analyzes the headers and may change the headers, such as HTTP host and URL, for web filtering. If a security profile decides to block the connection, the proxy can send a replacement message to the client. This adds latency to the overall transmission speed.

Make sure that both an SSL inspection profile (such as the certificate-inspection profile) and a web filter profile are selected in the associated firewall policy.

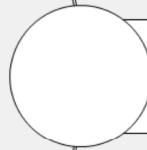
DO NOT REPRINT

© FORTINET

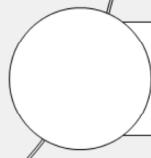
Lesson Progress



Inspection Modes



Web Filtering Basics



Troubleshooting



© Fortinet Inc. All Rights Reserved.

7

Good job! You now understand inspection modes.

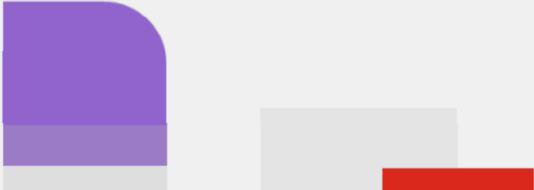
Now, you will learn about web filtering basics.

DO NOT REPRINT**© FORTINET**

Web Filtering Basics

Objectives

- Configure certificate inspection for web filtering
- Configure a web filter profile in flow-based inspection mode
- Configure a web filter profile in proxy-based inspection mode
- Configure FortiGuard categories
- Configure a URL filter



© Fortinet Inc. All Rights Reserved. 8

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

By demonstrating competence in web filtering configuration, you will be able to implement the web filter profile in an effective manner.

DO NOT REPRINT
© FORTINET

Configure SSL Certificate Inspection

Security Profiles > SSL/SSH Inspection

Name: test

Comments: Write a comment... 0/255

SSL Inspection Options

Enable SSL inspection of: **Multiple Clients Connecting to Multiple Servers**

Inspection method: **SSL Certificate Inspection** Full SSL Inspection

CA certificate: Fortinet_CA_SSL

Blocked certificates: Allow

Untrusted SSL certificates: Allow

Server certificate SNI check: **Enable**

Protocol Port Mapping

HTTPS: 443,10443

© Fortinet Inc. All Rights Reserved. 9

FortiGate has a read-only preconfigured profile for SSL certificate inspection named **certificate-inspection**. If you want to enable SSL certificate inspection, select this profile when configuring a firewall policy.

Alternatively, you can create your own profile for SSL certificate inspection by following these steps:

1. On the FortiGate GUI, click **Security Profiles**, and then click **SSL/SSH Inspection**.
2. Click **Create New** to create a new SSL/SSH inspection profile.
3. Select **Multiple Clients Connecting to Multiple Servers**, and then click **SSL Certificate Inspection**.
4. Select the action for **Server certificate SNI check**.

When the **Server certificate SNI check** configuration is **Enable**, FortiGate uses the domain in the CN field instead of the domain in the SNI field if the domain in the SNI field does not match any of the domains listed in the CN and SAN fields. With **Strict**, FortiGate closes the client connection if there is a mismatch. When **SNI check is Disable**, FortiGate always rates URLs based on the FQDN.

DO NOT REPRINT
© FORTINET

Configure Web Filter Profiles—Flow Based

- Apply web filter profile to a flow-based firewall policy

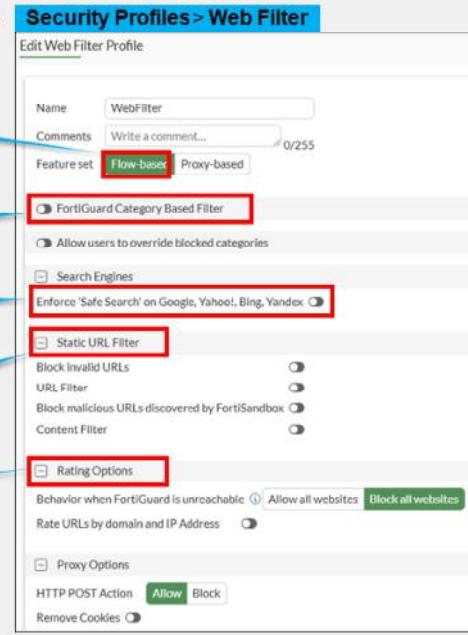
Select Flow-based

Enable FortiGuard Category Based Filter and configure each category

Enable Safe Search if needed

Enable and configure Static URL Filter if needed

Enable and configure Rating Options if needed



© Fortinet Inc. All Rights Reserved. 10

Now, you will learn more about configuring the web filter profile. You can configure this security profile to use a feature set for proxy-based or flow-based inspection modes. However, depending on the mode you select, the available settings are different. Flow-based inspection has fewer available options.

Selecting rating options allows you to enable two advanced filter features:

- Allow websites when a rating error occurs:** If you have activated services that require a FortiGuard license (such as FortiGuard filter), but do not have a license, then you will get a rating error message. Use this setting to allow access to websites that return a rating error from the FortiGuard Web Filter service.
- Rate URLs by domain and IP address:** If you enable this option, in addition to sending only the domain information, FortiGate will always send the URL domain name and the IP address of the TCP/IP packet (except private IP addresses) to FortiGuard for rating. If a different IP address and URL domain category has been returned by the FortiGuard server, then FortiGate uses the rating weight of the IP address or domain name to determine the rating result and decision. This rating weight is hard coded in FortiOS.

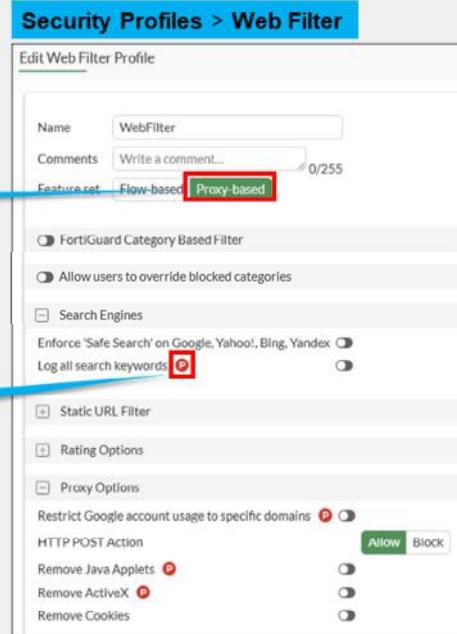
DO NOT REPRINT
© FORTINET

Configure Web Filter Profiles—Proxy Based

- Apply a web filter profile to a proxy-based firewall policy
- Supported on only FortiGate models with more than 2 GB RAM

Select Proxy-based

Feature available only in proxy based



In the example shown on this slide, the security profile is configured to use a proxy-based feature set. It provides features specific to proxy-based configuration.

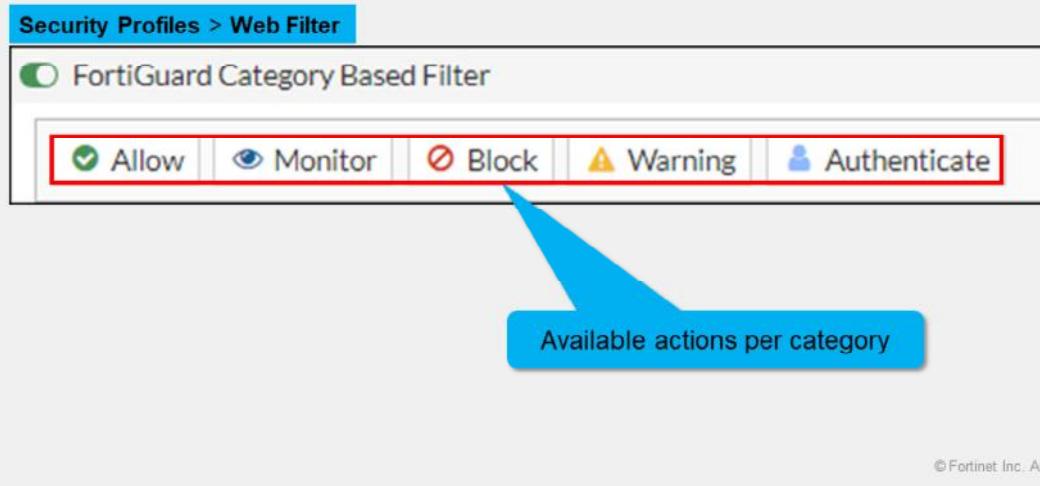
After you configure your web filter profile, you can apply this profile to the firewall policy configured to use proxy-based inspection mode, so the filtering is applied to your web traffic.

To enhance performance and optimize memory usage, FortiOS no longer supports proxy-related features on FortiGate models with 2 GB of RAM or less.

DO NOT REPRINT**© FORTINET**

FortiGuard Category Filter

- Websites split into multiple categories
- Live connection to FortiGuard with active contract required
- Can use FortiManager instead of FortiGuard



In the web filter profile, FortiGuard category filtering enhances the web filter features. Rather than block or allow websites individually, it looks at the category that a website has been rated with. Then, FortiGate takes action based on that category, not based on the URL.

FortiGuard category filtering is a live service that requires an active contract. The contract validates connections to the FortiGuard network. If the contract expires, there is a two-day grace period during which you can renew the contract before the service ends. If you do not renew, after the two-day grace period, FortiGate reports a rating error for every rating request made. In addition, by default, FortiGate blocks web pages that return a rating error. You can change this behavior by enabling the **Allow websites when a rating error occurs** setting.

You can configure FortiManager to act as a local FortiGuard server. To do this, you must download the databases to FortiManager, and configure FortiGate to validate the categories against FortiManager, instead of FortiGuard.

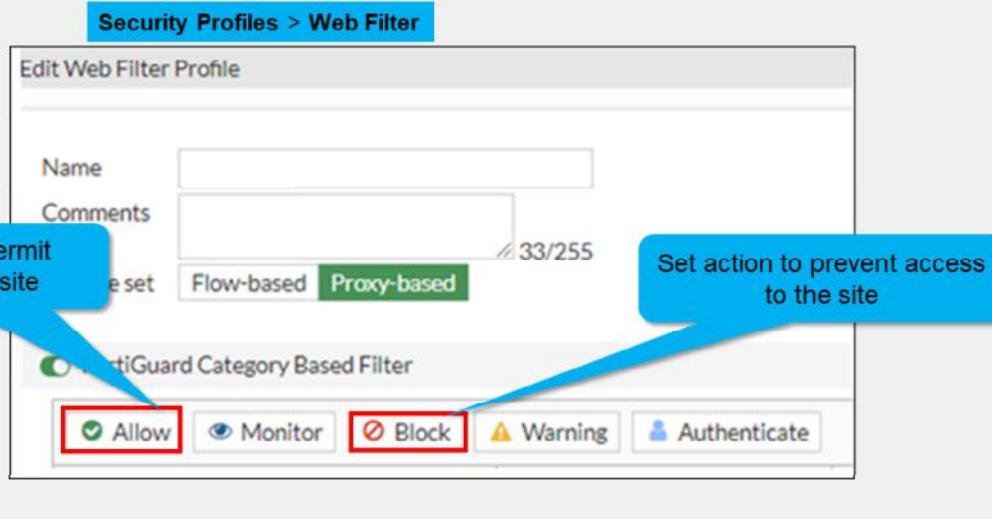
You can enable the FortiGuard category filtering on the web filter profile. Categories are listed, and you can customize the actions to perform individually. The actions available are **Allow**, **Monitor**, **Block**, **Warning**, and **Authenticate**.

To review the complete list of categories, visit the FortiGuard web filter website.

DO NOT REPRINT
© FORTINET

Web Filter FortiGuard Category Action—Allow or Block

- Allow or block access web sites



The **Allow** action permits access to the sites in the category but does not create a web filter security log. The **Block** action prevents access to the sites in the category and creates a web filter security log as well. Users trying to access a blocked site will get a message indicating the site is blocked.

DO NOT REPRINT
© FORTINET

Web Filter FortiGuard Category Action—Monitor

- Monitor action allows and logs web sites accesses

Set action to Monitor

The screenshot shows the 'Edit Web Filter Profile' screen under 'Security Profiles > Web Filter'. The profile is named 'Monitor' with the comment 'Monitor and log all visited URLs.' A 'FortiGuard Category Based Filter' is enabled. In the action selection row, the 'Monitor' button is highlighted with a red border. Below it, a table lists a single category rule: 'Education' with 'Action' set to 'Monitor'. A progress bar at the bottom indicates 27% completion.

Name	Action
Education	Monitor

© Fortinet Inc. All Rights Reserved. 14

The **Monitor** action allows access to the sites in the category and creates a security log for analysis purposes.

DO NOT REPRINT

© FORTINET

Web Filter FortiGuard Category Action—Warning

- Informs the user before proceeding
- Displays a customizable warning message

The screenshot shows the FortiGate Web Filter configuration interface. On the left, under 'Security Profiles > Web Filter', a new profile named 'Warning' is being created. It is set to 'Proxy-based' and includes a 'FortiGuard Category Based Filter'. A row for 'Internet Telephony' is selected, and the 'Action' column for it is set to 'Warning'. A red box highlights the 'Warning' button. Another red box highlights the 'Warning Interval' field in the 'Edit Filter' section below, which contains fields for hour(s), minute(s), and second(s). Three callout bubbles provide additional information: one points to the 'Warning' button with the text 'Set action to Warning'; another points to the 'Warning' link in the 'Action' column with the text 'Click to view the website'; and a third points to the 'Warning Interval' field with the text 'Customizable warning interval'.

© Fortinet Inc. All Rights Reserved. 15

FortiGuard Intrusion Prevention - Access Blocked

Web Page Blocked

You have tried to access a web page which is in violation of your Internet usage policy.

Category Internet Telephony
URL http://www.skype.com/
To have the rating of this web page re-evaluated [please click here](#)

Proceed Go Back

The **Warning** action informs users that the requested website is not allowed by the internet policies. However, the action gives the user the option to proceed to the requested website or return to the previous website.

You can customize the warning interval. When the timer expires, FortiGate displays the warning message again, if you access other websites in the same category.

You can customize the warning replacement message. By default, it provides information about the URL and its corresponding category. With this information, the user can click **Proceed** to override the internet usage policy.

The user's first attempt to connect will be blocked, and a corresponding web filter security log will be generated accordingly with action **blocked** and, if the user clicks **Proceed**, another web filter security log will be generated with the action **passthrough** and the message "URL belongs to a category with warnings enabled".

DO NOT REPRINT

© FORTINET

Web Filter FortiGuard Category Action—Authenticate

- To configure the **Authenticate** action:
 - Define users and a group
 - Set action to **Authenticate**
 - Select a user group

The screenshot shows the 'Security Profiles > Web Filter' interface. A specific profile named 'Streaming Media and Download' is selected. The 'Action' column for this profile is set to 'Authenticate'. A callout bubble points to this selection with the text 'Set action to Authenticate'.

Below the main table, there is an 'Edit Filter' dialog box. It contains a 'Warning Interval' field with values 0 hour(s), 5 minute(s), and 0 second(s). Another callout bubble points to this field with the text 'Customizable authenticate interval'.

Underneath the warning interval, there is a 'Selected User Groups' section. A callout bubble points to this section with the text 'User groups allowed to authenticate'.

At the bottom right of the interface, there is a copyright notice: © Fortinet Inc. All Rights Reserved. 16.

The **Authenticate** action blocks the requested websites, unless the user enters a successful username and password. FortiGate supports local and remote authentication using LDAP, RADIUS, and so on, for web filtering authentication. Choosing this action prompts you to define user groups that are allowed to override the block.

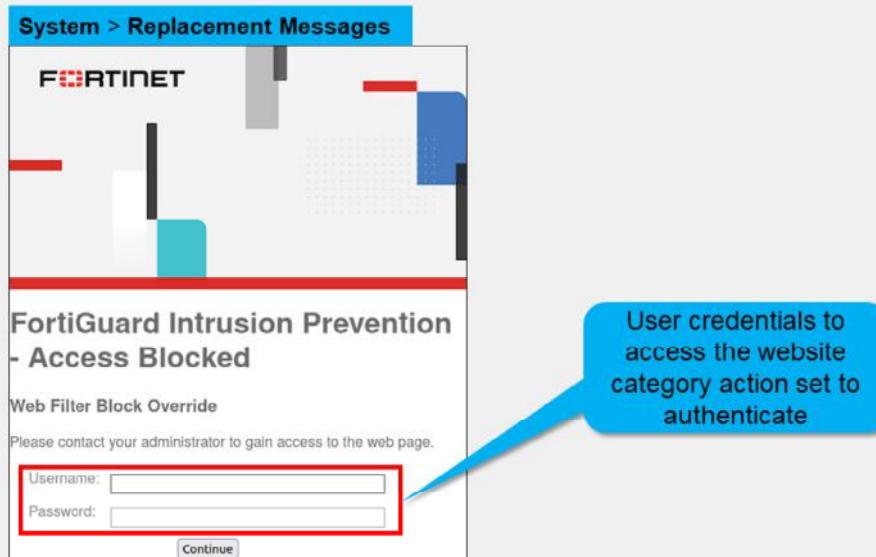
You can also customize the interval of time to allow access. Users are not prompted to authenticate again if they access other websites in the same category until the timer expires.

The user's first attempt to connect will be blocked, and a corresponding web filter security log will be generated. If the user proceeds and successfully authenticates, then another web filter security log will be generated with the action `passthrough` and the message "URL belongs to a category with warnings enabled".

DO NOT REPRINT
© FORTINET

Web Filter FortiGuard Category Action—Authenticate (Contd)

- User credentials requested in message



Like the **Warning** action, FortiGate displays a replacement message to proceed and a second one asks for user credentials. You can customize these replacement messages in **System > Replacement Messages**.

DO NOT REPRINT

© FORTINET

Web Filter FortiGuard Category Action—Quotas

- Applies to **Monitor**, **Warning** and **Authenticate** actions
- Quotas available only in proxy-based mode

The screenshot shows the FortiGate management interface for 'Edit Web Filter Profile' under 'Security Profiles > Web Filter'. A blue callout box points to the 'New/Edit Quota' dialog window, which is titled 'New/Edit Quota' and shows 'Category: Education'. It has tabs for 'Time' (selected) and 'Traffic'. Under 'Time', 'Total quota' is set to 0 hours, 5 minutes, and 0 seconds. Under 'Traffic', 'Total quota' is set to 1024 MB. A red callout box points to the 'Create New' button in the 'Category Usage Quota' section of the main profile configuration page. Another red callout box points to the 'Traffic' tab in the 'New/Edit Quota' dialog.

Quota configuration available in proxy-based mode

Daily quotas based on time or traffic amount

© Fortinet Inc. All Rights Reserved. 18

Quotas allow daily access for a specific length of time or bandwidth.

At midnight, quotas reset. Once the daily quota is reached for a category, FortiGate blocks the traffic and displays a replacement message page. You can apply quotas to **Monitor**, **Warning** and **Authenticate** actions.

DO NOT REPRINT
© FORTINET

Web Rating Override

- Changes a website category, not the category action

The screenshot illustrates the Fortinet FortiGate Web Rating Overrides feature. The main interface shows a list of overrides for 'Malicious Websites'. One entry for 'www.bing.com' is selected, showing its original category as 'Search Engines and Portals' (under 'General Interest - Business' and 'Search Engines and Portals'). A red arrow points from the 'Create New' button in the top-left of the main window to the 'Edit Web Rating Override' dialog. This dialog provides detailed configuration for the selected URL. It includes fields for 'URL' (www.bing.com), 'Category' (General Interest - Business), 'Sub-Category' (Search Engines and Portals), and 'Comments' (Write a comment...). The 'Override to' section is highlighted with a red box, showing 'Category' set to 'Security Risk' and 'Sub-Category' set to 'Malicious Websites'. Three callout boxes provide additional context: one points to the 'Original Category' column in the main table, another points to the 'Show original categories' checkbox at the top of the main window, and a third points to the 'Override to' configuration in the dialog.

If you consider that a particular URL does not have the correct category, you can ask to re-evaluate the rating in the Fortinet URL Rating Submission website. You can also override a web rating for an exceptional URL in the FortiGate configuration.

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.

DO NOT REPRINT

© FORTINET

Configure a URL Filter

- Check against configured URLs in URL filter from top to bottom

Enable URL Filter

Three pattern types

Four available actions

URL	Type	Action	Status
^\something\.(org biz)	Regular Express...	Exempt	Enable
somewhere."	Wildcard	Monitor	Enable
www.somesite.com/s...	Simple	Block	Enable



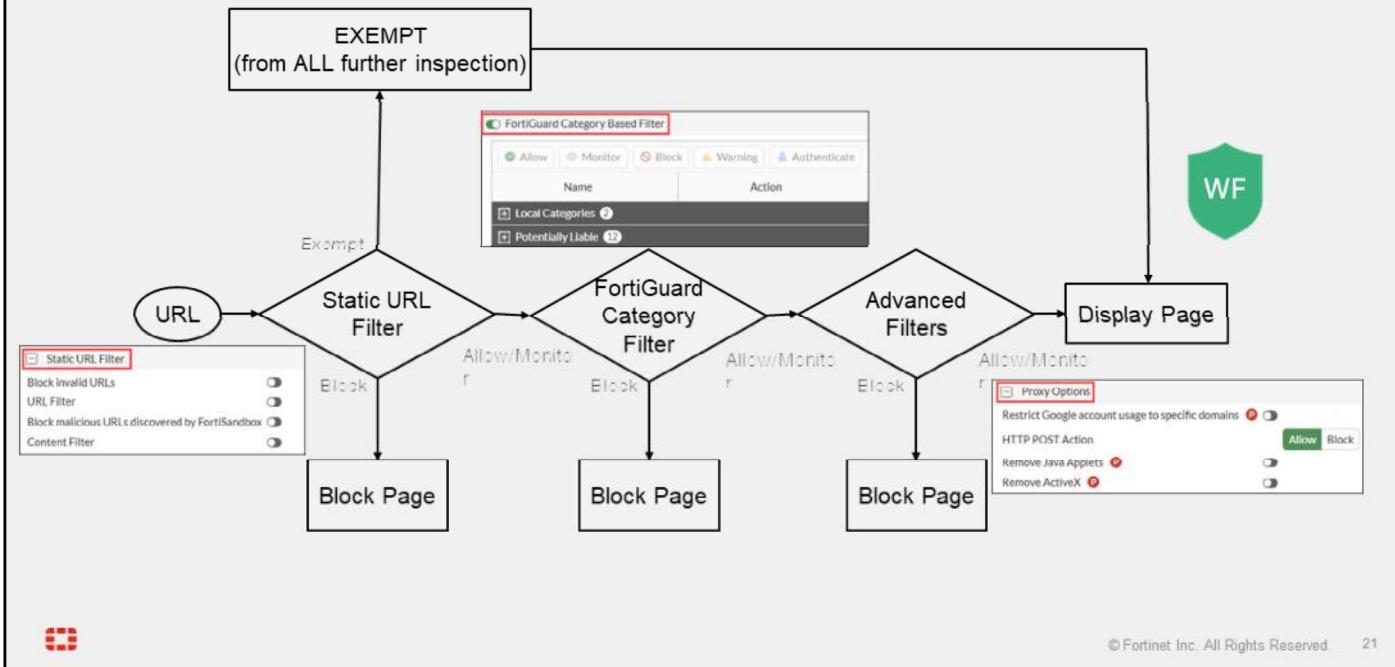
Static URL filtering is another web filter feature, which provides more granularity. Configured URLs in the URL filter are checked from top to bottom against the visited websites. If FortiGate finds a match, it applies the configured action. You can configure one of four actions:

- Exempt** allows the traffic from trusted sources to bypass all security inspections.
- Block** denies the attempt and the user receives a replacement message.
- Allow** permits access. The traffic is passed to the remaining operations, including FortiGuard web filter, web content filter, web script filters, and antivirus scanning.
- Monitor** allows the traffic while creating log entries. The traffic is still subject to all the other security profile inspections.

To find the exact match, URL filtering has three pattern types: **Simple**, **Regular Expressions**, and **Wildcard**.

DO NOT REPRINT
© FORTINET

HTTPS Inspection Order



So, with these different features, what is the inspection order? If you have enabled many of them, the inspection order flows as follows:

1. The local static URL filter
2. FortiGuard category filtering (to determine a rating)
3. Advanced filters (such as safe search or removing Active X components)

For each step, if there is no match, FortiGate moves on to the next check enabled.

DO NOT REPRINT

© FORTINET

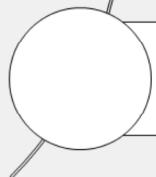
Lesson Progress



Inspection Modes



Web Filtering Basics



Troubleshooting



© Fortinet Inc. All Rights Reserved. 22

Good job! You now understand the basics of web filtering.

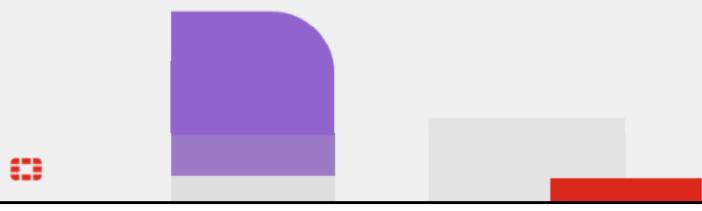
Now, you will learn about troubleshooting.

DO NOT REPRINT**© FORTINET**

Troubleshooting

Objectives

- Troubleshoot web filtering issues
- Monitor logs for web filtering events

A decorative graphic in the bottom left corner features a purple rounded rectangle overlapping a smaller grey rectangle. To the right of this is a small red horizontal bar.

© Fortinet Inc. All Rights Reserved. 23

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

By demonstrating competence in troubleshooting, you will be able to apply troubleshooting techniques to avoid and investigate common issues.

DO NOT REPRINT
© FORTINET

Troubleshooting the FortiGuard Connection

- FortiGuard category filtering requires a live connection

```

FortiGate # diagnose debug rating
Locale      : english

Service     : Web-filter
Status      : Enable
License     : Contract
 \
Num. of servers : 1
Protocol    : https
Port        : 8888
Anycast     : Disable
Default servers : Not included

-- Server List (Wed Sep 20 09:22:42 2023) --
IP          Weight   RTT Flags   TZ   FortiGuard-requests Curr Lost Total Lost          Updated Time
10.0.1.241    -244     2 I       0      122      0      0 Wed Sep 20 09:21:55 2023

```

Weight decreases with successful packets



Category-based filtering requires a live connection to FortiGuard.

You can verify the connection to FortiGuard servers by running the `diagnose debug rating` CLI command. This command displays a list of FortiGuard servers you can connect to, as well as the following information:

- **Weight:** It is based on the difference in time zones between FortiGate and this server to reduce the possibility of using a remote server.
- **RTT:** Return trip time
- **Flags:** D (IP returned from DNS), I (Contract server contacted), T (being timed), F (failed)
- **TZ:** Server time zone
- **FortiGuard-requests:** The number of requests sent by FortiGate to FortiGuard
- **Curr Lost:** Current number of consecutive lost FortiGuard requests (in a row, it resets to 0 when one packet succeeds)
- **Total Lost:** Total number of lost FortiGuard requests

The list is of variable length depending on the FortiGuard Distribution Network and the FortiGate configuration.

DO NOT REPRINT

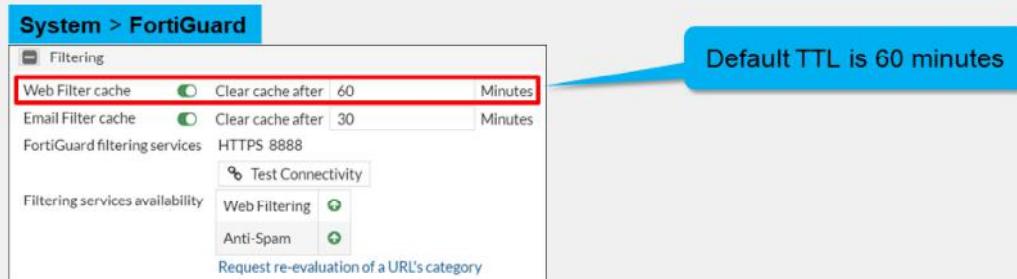
© FORTINET

Troubleshooting the FortiGuard Connection (Contd)

- Change default FortiGuard or FortiManager communications from HTTPS port 443:
 - Disable FortiGuard anycast setting on CLI to use UDP ports 443, 53, or 8888

```
config system fortiguard
  set fortiguard-anycast {enable|disable}
  set protocol {udp|https}
  set port {8888|53|443}
end
```

- Enable **Web Filter cache** to reduce requests to FortiGuard



© Fortinet Inc. All Rights Reserved. 25

By default, FortiGate is configured to enforce the use of HTTPS port 443 to perform live filtering with FortiGuard or FortiManager. When the `fortiguard-anycast` command is `enable`, the FortiGuard domain name resolves to a single anycast IP address, which is the only entry in the list of FortiGuard servers. By disabling the FortiGuard anycast setting on the CLI, other ports and protocols are available. These ports and protocols query the servers (FortiGuard or FortiManager) on HTTPS port 53 and port 8888, UDP port 443, port 53, and port 8888. If you are using UDP port 53, any kind of inspection reveals that this traffic is not DNS and prevents the service from working. In this case, you can switch to the alternate UDP port 443 or port 8888, or change the protocol to HTTPS, but these ports are not guaranteed to be open in all networks, so you must check beforehand.

If the number of FortiGuard requests is too high, you can also enable **Web Filter cache**. Once enabled, FortiGate maintains a list of recent website rating responses in memory. So, if the URL is already known, FortiGate doesn't send back a rating request. Caching responses reduces the amount of time it takes to establish a rating for a website since the memory lookup is much quicker than packets travelling on the internet.

DO NOT REPRINT
© FORTINET

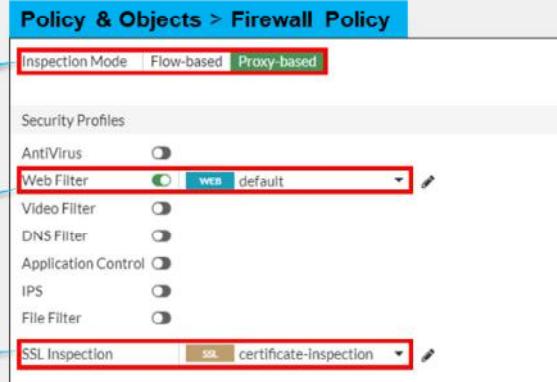
Troubleshooting Web Filtering Issues

- Web filtering not working even with a valid FortiGuard live connection?

Compare inspection mode setting with feature set in web filter profile

Verify the web filter profile applied

For encrypted protocols, certificate-inspection must be at least selected



What if you have a live connection to FortiGuard and configured your security profiles, but they are not performing web inspection?

Most of the time, issues are caused by misconfiguration on the device. You can verify them as follows:

- Make sure that the **SSL Inspection** field includes at least one profile with an SSL certification inspection method.
- Make sure that the correct web filter profile is applied on the firewall policy.
- Verify the inspection mode setting with the feature set in the corresponding web filter profile.

DO NOT REPRINT

© FORTINET

Web Filter Log

- Record HTTP traffic activity including action, profile used, category, URL and quota info

Log & Report > Security Events > Web Filter

Date/Time	User	Source	Action	URL	Category	Initiator	Sent / Received
2023/09/20 07:43:02	10.0.1.10		Blocked	https://www.google.com/	Search Engines and Portals		517 B / 0 B

Click to download the raw log data

Information on action and policy ID

Name of web filter profile

Name of web filter profile and replacement message used

Log Details

Action

- Action: Blocked
- Policy ID: 1 (Full_Access)

Web Filter

- Profile: default
- Request Type: direct
- Direction: outgoing
- Category ID: 41
- Category: Search Engines and Portals
- Message: URL belongs to a category with warnings enabled

© Fortinet Inc. All Rights Reserved. 27

To confirm the correct configuration and web filtering behavior, you can view the web filter logs.

This slide shows an example of a log message. Access details include information about the FortiGuard quota and category (if those are enabled), which web filter profile was used to inspect the traffic, the URL, and more details about the event.

You can also view the raw log data by clicking the download icon. The file downloaded is a plaintext file in a syslog format.

DO NOT REPRINT

© FORTINET

Knowledge Check

1. Which action in the FortiGuard category filter supports the category usage quota?
 A. Warning
 B. Allow

2. Which configuration change is required to use UDP ports 443, 53, or 8888 for the FortiGuard connection?
 A. Use the `set fortiguard-anycast disable` command on the CLI.
 B. Enable the **Override FortiGuard Servers** setting on the GUI.



DO NOT REPRINT

© FORTINET

Lesson Progress



Inspection Modes



Web Filtering Basics



Troubleshooting



© Fortinet Inc. All Rights Reserved.

29

Congratulations! You have completed this lesson.

Now, you will review the objectives covered in this lesson.

DO NOT REPRINT

© FORTINET

Review

- ✓ Describe FortiOS inspection modes
- ✓ Implement a web filter profile in flow-based and proxy-based inspection modes
- ✓ Work with web filter categories
- ✓ Configure a URL filter for further granularity
- ✓ Troubleshoot common web filtering issues
- ✓ Monitor logs for web filtering events



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

By mastering the objectives covered in this lesson, you learned how to configure web filtering on FortiGate to control web traffic in your network.

DO NOT REPRINT**© FORTINET**

FortiOS Administrator

Intrusion Prevention and Application Control

A small red square icon containing a white square with a diagonal line, followed by the text "FortiOS 7.6".

Last Modified: 6 October 2025

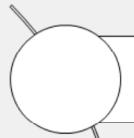
© Fortinet Inc. All Rights Reserved. 1

In this lesson, you will learn how to use FortiGate to protect your network against intrusions and monitor and control network applications that may use standard or nonstandard protocols and ports—beyond simply blocking or allowing a protocol, port number, or IP address.

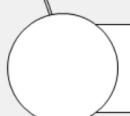
DO NOT REPRINT

© FORTINET

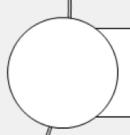
Lesson Overview



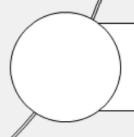
IPS Configuration



IPS Monitoring



Application Control Basics



Application Control Configuration



© Fortinet Inc. All Rights Reserved.

2

In this lesson, you will learn about the topics shown on this slide.

DO NOT REPRINT**© FORTINET**

IPS Configuration

Objectives

- Identify the different components of an intrusion prevention system (IPS) package
- Configure an IPS sensor



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

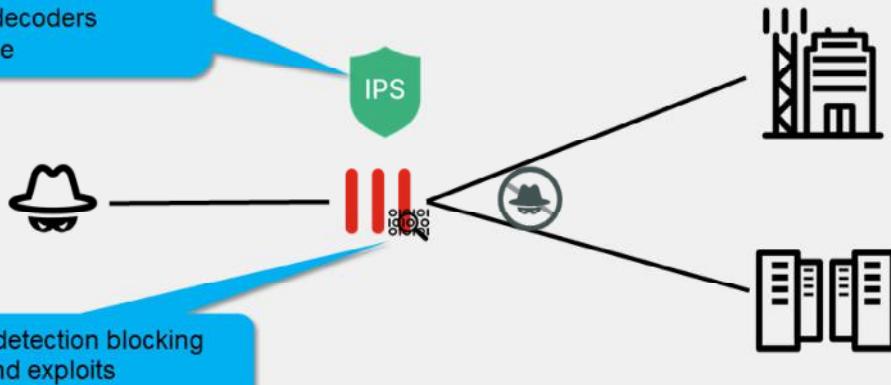
By demonstrating competence in IPS configuration, you will be able to implement an effective IPS solution.

DO NOT REPRINT

© FORTINET

IPS

- IPS components include:
- IPS signature databases
 - Protocol decoders
 - IPS engine



Intrusion Prevention System (IPS) detects network attacks and prevents threats from compromising the network, including protected devices. IPS utilizes signatures, protocol decoders, heuristics (or behavioral monitoring), threat intelligence (such as FortiGuard Labs), and advanced threat detection can prevent exploit of known and unknown zero-day threats. FortiGate IPS can perform deep packet inspection to scan encrypted payloads to detect and prevent threats from attackers.

IPS components include the following:

1. **IPS Signatures:** IPS on FortiGate uses signature databases to detect known attacks, like exploits. Rate-based IPS signatures also allows you to detect anomalies, which are unusual behaviors in the network, such as higher-than-usual CPU use or network traffic. Rate-based IPS signatures are part of behavioral analysis, like DoS policies and protocol constraints inspection, which detect and monitor (and, in some cases, block or mitigate) anomalies, because they reveal the symptoms of a new, never-previous-seen attack.
2. **Protocol decoders:** Protocol decoders can detect network errors and protocol anomalies. Protocol decoders parse each packet according to the protocol specifications. By understanding the protocol, the IPS can identify anomalies or malicious activities even if they are encapsulated in legitimate protocol behaviors. If the traffic doesn't conform to the specification—if, for example, it sends malformed or invalid commands to your servers—then the protocol decoder detects the error.
3. **IP Engine:** The IPS engine is responsible for IPS and protocol decoders, in addition to application control, flow-based antivirus protection, web filtering, and email filtering.

DO NOT REPRINT

© FORTINET

List of IPS Signatures

- Create new IPS sensors and view a list of predefined sensors

Name	Severity	Target	OS	Action	CVE-ID
3Com.3CDaemon.FTP.Server.Buffer.Overflow	Medium	Server	Windows	Block	CVE-2005-0277
3Com.3CDaemon.FTP.Server.Information.Disclosure	Information	Client	Windows	Pass	CVE-2005-0278
3Com.OfficeConnect. ADSL.Wireless.Firewall.Router.DoS	Medium	Server	Linux	Block	
427BB.Cookie-Based.Authentication.Bypass	Medium	Server	Other	Block	CVE-2006-0153
A325.Botnet	Medium	Server	All	Block	
		Client		Reset	

FortiGate IPS sensor is a collection of IPS signatures and filters that define the scope of what the IPS engine will scan when the IPS sensor is applied. Multiple sets of signatures, filters, or both may be present in an IPS sensor. A set of IPS signatures consists of manually selected signatures, while a set of IPS filters consists of filters based on signature attributes like target, severity, protocol, OS, and application. Each signature has predefined attributes and an action, such as block, allow, monitor (pass), quarantine, and reset. It is also possible to create custom IPS signatures to apply to an IPS sensor.

FortiOS includes predefined IPS sensors with associated predefined signatures. Examples are default, all_default, protect_client, protect_http_server, and so on.

FortiGate downloads a FortiGuard IPS package and new signatures will appear in the signature list. When configuring FortiGate, you can change the **Action** setting for each sensor that uses a signature.

The default action setting is often correct, except in the following cases:

- Your software vendor releases a security patch. Continuing to scan for exploits wastes FortiGate resources.
- Your network has a custom application with traffic that inadvertently triggers an IPS signature. You can change the action setting until you notify Fortinet so that the FortiGuard team can modify the signature to avoid false positives.

DO NOT REPRINT
© FORTINET

Configuring IPS Sensors

- Add individual signatures
- Add groups of signatures using filters

The screenshot shows the FortiGate UI for configuring an IPS sensor. On the left, the 'New IPS Sensor' configuration page is displayed, featuring fields for Name (set to 'IPS profile'), Comments (with placeholder 'Write a comment'), and Block malicious URLs (disabled). Below these are tabs for Details, Exempt IPs, Action, and Packet Logging, all showing 'No results'. A red box highlights the '+ Create New' button under the 'IPS Signatures and Filters' section. On the right, two overlapping windows show how to add signatures. The top window, titled 'Add Signatures', has its 'Type' dropdown set to 'Signature' (highlighted by a red box) and lists several pre-defined signatures like '3Com.3CDaemon.FTP.Server.Buffer.Overflow' and '3Com.3CDaemon.FTP.Server.InformationDisclosure'. The bottom window, also titled 'Add Signatures', has its 'Type' dropdown set to 'Filter' (highlighted by a red box) and shows a 'Filter' table with columns for Type (Server, Client), OS (All, Windows, Mac OS, Linux, HTTP), and Status (Enabled, Disabled). Both windows include a search bar and a table at the bottom showing specific signatures with their details.

There are two ways to add predefined signatures to an IPS sensor. One way is to select the signatures individually. After selecting a signature in the list, the signature is added to the sensor with its default action.

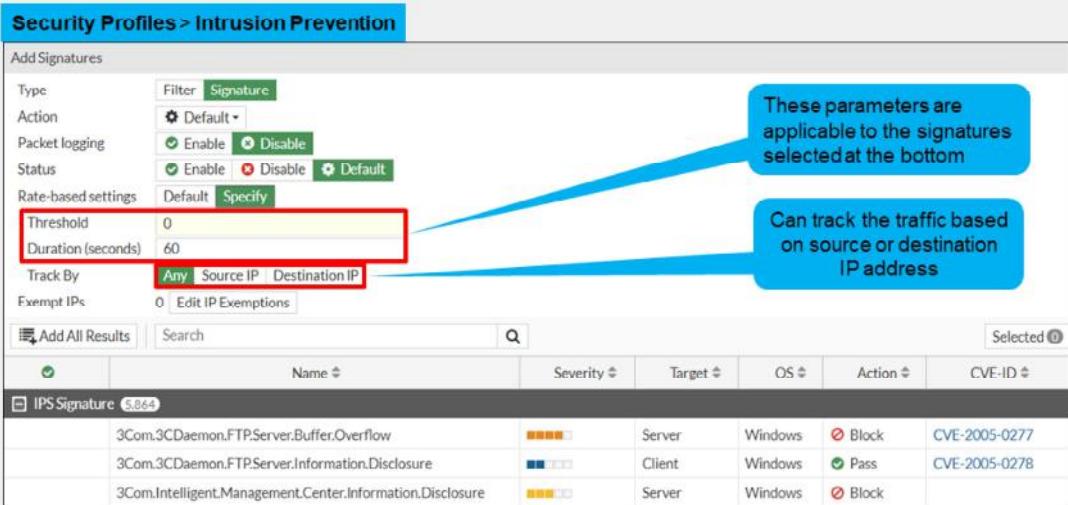
The second way to add a signature to a sensor is using filters. FortiGate adds all the signatures that match the filters.

The purpose of the IPS feature is to protect the inside of the network from outside threats.

DO NOT REPRINT
© FORTINET

Configuring IPS Sensors—Rate-Based Signatures

- Add rate-based signatures to block traffic when the threshold is exceeded during a time period



The screenshot shows the 'Security Profiles > Intrusion Prevention' page. In the 'Add Signatures' section, the 'Type' is set to 'Signature'. Under 'Rate-based settings', the 'Threshold' is set to 0 and 'Duration (seconds)' is set to 60. A callout bubble points to these fields with the text: 'These parameters are applicable to the signatures selected at the bottom'. Below this, another callout bubble points to the 'Track By' dropdown which has 'Any' selected, with the text: 'Can track the traffic based on source or destination IP address'. At the bottom of the page, there is a table titled 'IPS Signature (5,864)' listing three entries:

Name	Severity	Target	OS	Action	CVE-ID
3Com.3CDaemon.FTP.Server.Buffer.Overflow	■■■■■	Server	Windows	Block	CVE-2005-0277
3Com.3CDaemon.FTP.Server.Information.Disclosure	■■■■■	Client	Windows	Pass	CVE-2005-0278
3Com.Intelligent.Management.Center.Information.Disclosure	■■■■■	Server	Windows	Block	

Selected 0

You can also add rate-based signatures to block specific traffic when the threshold is exceeded. On the CLI, if you set the command `rate-mode` to `periodical`, FortiGate triggers the action when the threshold is reached during the configured **Duration** time period. You should apply rate-based signatures only to protocols you use. This saves system resources and can discourage a repeat attack. FortiGate does not track statistics for that client while it is temporarily blocklisted.

DO NOT REPRINT
© FORTINET

IPS Sensor Inspection Sequence

New entries are placed at the bottom of the list

IPS signatures and filters are processed in sequence

Details	Exempt IPs	Action	Packet Logging
Apache.Tomcat.Integer.Overflow.Information.Disclosure	0	<input checked="" type="checkbox"/> Monitor <input type="radio"/> Default	<input checked="" type="checkbox"/> Disabled <input type="radio"/> Enabled
TGT Server			
SEV			
SEV			
OS Windows			

When the IPS engine compares traffic with the signatures in each filter, order matters. The rules are similar to firewall policy matching; the engine evaluates the filters and signatures at the top of the list first, and applies the first match. The engine skips subsequent filters.

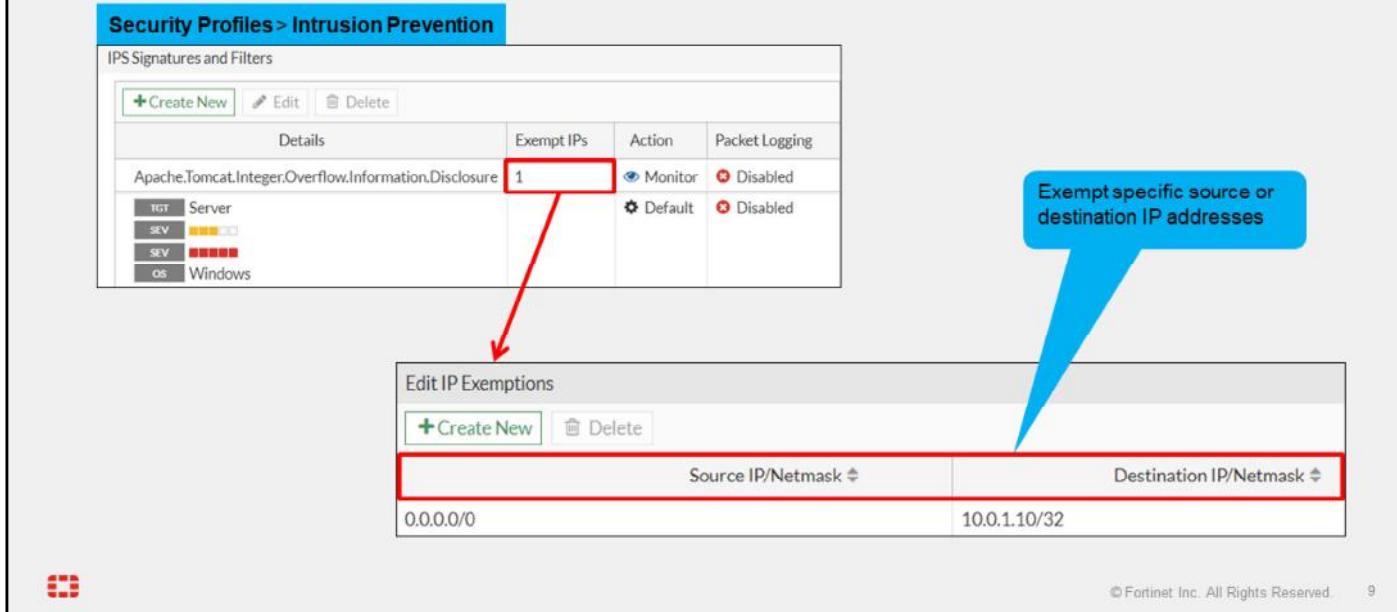
So, position the most likely matching filters, or signatures, at the top of the list. Avoid making too many filters, because this increases evaluations and CPU usage. Also, avoid making very large signature groups in each filter, which increase RAM use.

In the event of a false-positive outbreak, you can add the triggered signature as an individual signature, and then set the action to **Monitor**. This allows you to monitor the signature events using IPS logs, while investigating the false-positive issue.

DO NOT REPRINT
© FORTINET

Configuring IP Exemptions

- Only configurable under individual IPS signatures



The screenshot shows the FortiGate management interface. At the top, a blue header bar reads "Security Profiles > Intrusion Prevention". Below it is a table titled "IPS Signatures and Filters". A row in the table is selected, highlighted with a red border. This row corresponds to the signature "Apache.Tomcat.Integer.Overflow.Information.Disclosure". The "Exempt IPs" column contains the value "1", which is also highlighted with a red border. A red arrow points from this value down to the "Edit IP Exemptions" dialog box below.

Details	Exempt IPs	Action	Packet Logging
Apache.Tomcat.Integer.Overflow.Information.Disclosure	1	<input checked="" type="radio"/> Monitor <input type="radio"/> Default	<input checked="" type="radio"/> Disabled <input type="radio"/> Disabled
TGT Server SEV ■■■■■ SEV ■■■■■ OS Windows			

Edit IP Exemptions

Source IP/Netmask	Destination IP/Netmask
0.0.0.0/0	10.0.1.10/32

A blue callout bubble with the text "Exempt specific source or destination IP addresses" is positioned to the right of the "Exempt IPs" cell in the table.

Sometimes, it is necessary to exempt specific source or destination IP addresses from specific signatures. This feature is useful during false-positive outbreaks. You can temporarily bypass affected endpoints until you investigate and correct the false-positive issue.

You can configure IP exemptions on individual signatures only. Each signature can have multiple exemptions.

DO NOT REPRINT

© FORTINET

IPS Actions

Action to take when a signature is triggered

Copies the packets for later analysis

	Sev...	Target	OS	Action	CVE-ID
HP.Database.Archiving.Software.GIOP.Parsing.Buffer....	██████	Server	Windows Solaris	Block	CVE-2011-4164
Symantec.Gateway.Products.DNS.Cache.Poisoning	██████	Client	Windows Solaris	Block	CVE-2005-0817
Oracle.Outside.In.OOXML.Tag.Parsing.Stack.Buffer.O...	██████	Client	Windows Solaris	Block	
Oracle.Outside.In.Lotus123.Heap.Buffer.Overflow	██████	Client	Windows Solaris	Block	CVE-2012-0110

© Fortinet Inc. All Rights Reserved. 10

When you create a new entry to add signatures or filters, you can select the action by clicking **Action**.

Select **Allow** to allow traffic to continue to its destination. Select **Monitor** to allow traffic to continue to its destination and log the activity. Select **Block** to silently drop traffic matching any of the signatures included in the entry. Select **Reset** to generate a TCP RST packet whenever the signature is triggered. Select **Default** to use the default action of the signatures.

Quarantine allows you to quarantine the attacker's IP address for a set duration. You can set the quarantine duration to any number of days, hours, or minutes.

When you enable **Packet logging**, FortiGate stores a local copy of the packet that matches the signature. This enhances the view of erroneous or suspicious packets. FortiGate's IPS packet logging helps to provide robust security operations by providing accurate information into network traffic, which are crucial for detecting, investigating, and mitigating cyber threats. Even though enabling packet logging consume significant storage, memory, and processing resources, you can enable packet logging for different use case scenarios such as detection and prevention of zero-day attacks, troubleshooting, behavioral analysis, threat hunting etc.

You can set these actions on hold for new FortiGuard IPS signature by enabling the `override-signature-hold-by-id` CLI command. During the time defined by the CLI command `signature-hold-time`, the action is then set to **Monitor** to avoid false positives, with a log created including the message 'signature is on hold'.

DO NOT REPRINT
© FORTINET

Enabling Botnet Protection

The screenshot shows the FortiOS Security Profiles > Intrusion Prevention interface. It displays an IPS Signature named "Apache.Tomcat.Integer.Overflow.Information.Disclosure" with the following details:

Details	Exempt IPs	Action	Packet Logging
Apache.Tomcat.Integer.Overflow.Information.Disclosure	0	<input checked="" type="radio"/> Monitor	<input checked="" type="radio"/> Disabled
TGT Server SEV SEV OS Windows		<input checked="" type="radio"/> Default	<input checked="" type="radio"/> Disabled

Below this, under "Botnet C&C", there is a section titled "Scan Outgoing Connections to Botnet Sites" with three buttons: "Disable" (disabled), "Block" (selected), and "Monitor". A tooltip indicates "3100 IP Addresses in botnet package." A callout bubble points to the "Block" button with the text "Set action to Block or Monitor". Another callout bubble points to the "Block" button with the text "Botnet database from FortiGuard (included with a valid IPS license)".

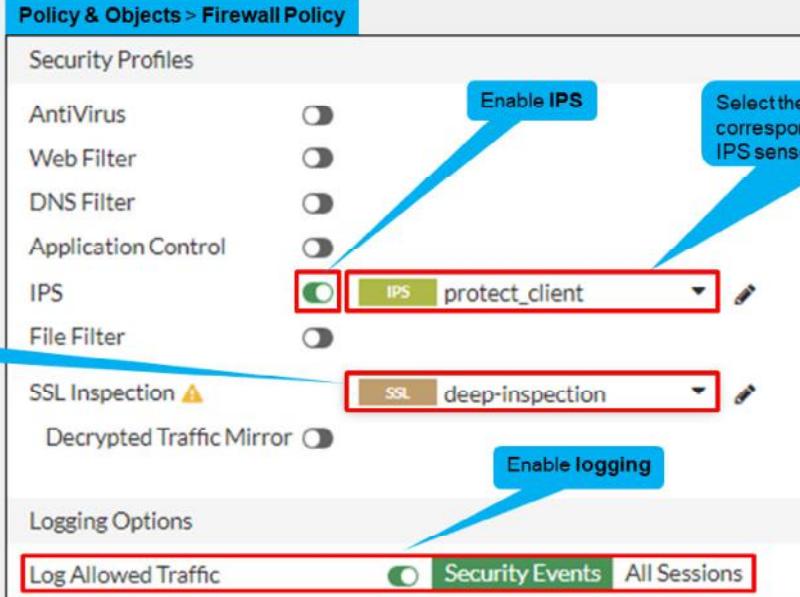
For consolidated botnet protection, you can enable botnet scanning on the IPS profile that you apply the firewall policy on.

There are three possible actions for **Botnet and C&C**:

- **Disable**: Do not scan connections to botnet servers
- **Block**: Block connections to botnet servers
- **Monitor**: Log connections to botnet servers

DO NOT REPRINT
© FORTINET

Applying IPS Inspection



The screenshot shows the 'Policy & Objects > Firewall Policy' interface. In the 'Security Profiles' section, the 'IPS' profile is selected and enabled. A callout points to the 'Enable IPS' switch with the text 'Set deep-inspection for encrypted protocols'. Another callout points to the dropdown menu next to the 'IPS' profile with the text 'Select the IPS security profile corresponding to the configured IPS sensors', showing 'protect_client' is selected. In the 'SSL Inspection' section, the 'deep-inspection' profile is selected. A callout points to this dropdown with the text 'Enable logging'. In the 'Logging Options' section, the 'Security Events' method is selected. A callout points to this dropdown with the text 'Log Allowed Traffic'.

© Fortinet Inc. All Rights Reserved. 12

To apply an IPS sensor, you must enable **IPS** and then select the sensor in a firewall policy.

Certain vulnerabilities apply only to encrypted connections and FortiGate can't identify the threat reliably if it can't parse the payload. For this reason, you must use an SSL inspection profile, usually **deep-inspection**, if you want to get the maximum benefit from your IPS features.

By default, FortiGate logs all security events. This means you can see any traffic that is being blocked or monitored by IPS.

If you think some traffic should be blocked but is passing through the policy, you should change the **Log Allowed Traffic** method to **All Sessions**. This logs all traffic processed by that firewall policy, and not just the traffic that is blocked or monitored by the security profiles. This can help you in identifying false negative events.

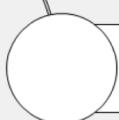
DO NOT REPRINT

© FORTINET

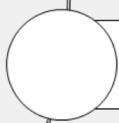
Lesson Progress



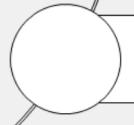
IPS Configuration



IPS Monitoring



Application Control Basics



Application Control Configuration



© Fortinet Inc. All Rights Reserved.

13

Good job! You now understand IPS on FortiGate.

Now, you will learn about IPS monitoring.

DO NOT REPRINT**© FORTINET**

IPS Monitoring

Objectives

- Troubleshoot IPS high CPU usage
- Manage IPS fail open

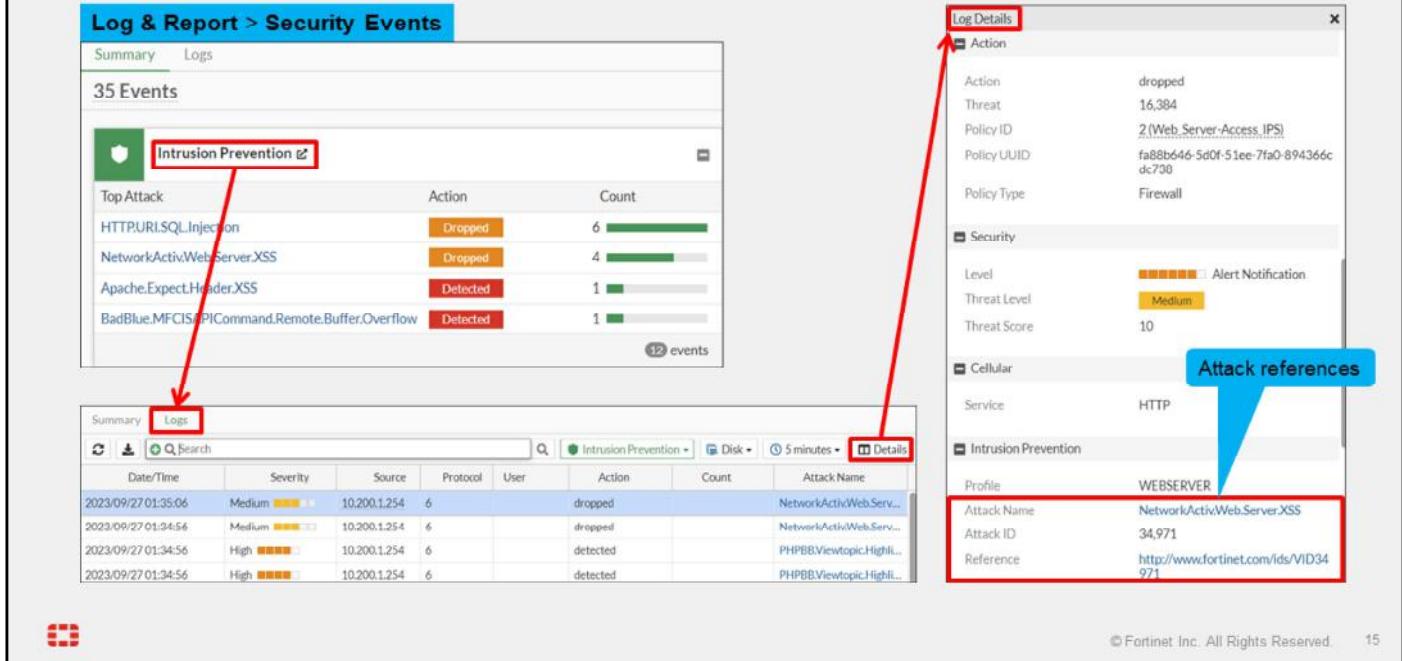
 © Fortinet Inc. All Rights Reserved. 14

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

By demonstrating competence in troubleshooting, you should be able to identify, investigate, and manage some common issues with IPS deployments on FortiGate.

DO NOT REPRINT
© FORTINET

IPS Logging



The screenshot shows the FortiGate Log & Report interface. In the top left, there's a summary of 35 events, with a bar chart showing the count of actions (Dropped or Detected) for various attack types like Top Attack, HTTP.URL.SQL.Injection, NetworkActiv.WebServer.XSS, Apache.Expect.Header.XSS, and BadBlue.MFCISAPICommand.Remote.Buffer.Overflow. A red arrow points from the 'Intrusion Prevention' link in the summary to the 'Logs' tab in the main pane below.

The main pane displays a table of logs. The columns include Date/Time, Severity, Source, Protocol, User, Action, Count, and Attack Name. The table shows four entries:

Date/Time	Severity	Source	Protocol	User	Action	Count	Attack Name
2023/09/27 01:35:06	Medium	10.200.1.254	6		dropped		NetworkActiv/Web.Serv...
2023/09/27 01:34:56	Medium	10.200.1.254	6		dropped		NetworkActiv/Web.Serv...
2023/09/27 01:34:56	High	10.200.1.254	6		detected		PHPBB.Viewtopic.Highl...
2023/09/27 01:34:56	High	10.200.1.254	6		detected		PHPBB.Viewtopic.Highl...

A red arrow points from the 'Details' button in the log table to a detailed log entry on the right. This entry includes fields like Action (dropped), Threat (16,384), Policy ID (2 (Web_Server-Access_IPS)), and Policy Type (Firewall). It also shows security details (Level: Alert Notification, Threat Level: Medium, Threat Score: 10), cellular information (Service: HTTP), and intrusion prevention profile (Profile: WEBSERVER, Attack Name: NetworkActiv/Web.Server.XSS, Attack ID: 34,971, Reference: http://www.fortinet.com/ids/VID34971).

If you enabled security events logging in the firewall policies that apply IPS, the logs are available on the **Security Events** pane on the **Log & Report** page. You can view the logs by clicking on **Intrusion Prevention**.

You should review IPS logs frequently. The logs are an important source of information about the kinds of attacks that are being targeted at your network. This helps you develop action plans and focus on specific events, for example, patching a critical vulnerability.

DO NOT REPRINT
© FORTINET

Troubleshoot IPS High-CPU Usage

- CLI command to troubleshoot continuous high CPU use by IPS engines

```
# diag test application ipsmonitor <Integer>

IPS Engine Test Usage:

1: Display IPS engine information
2: Toggle IPS engine enable/disable status
5: Toggle bypass status
99: Restart all IPS engines and monitor

IPS engine remains active,
but does not inspect traffic
```

```
# diag test application ipsmonitor 1
pid = 2011, engine count = 1 (+1)
0 - pid:2058:2058 cfg:1 master:0 run:1
1 - pid:2832:2832 cfg:0 master:1 run:1

pid:          2832 index:1 master
version:      07006000FLEN07600-00007.00006
up time:      0 days 0 hours 5 minutes
init time:    0 seconds
socket size: 256(MB)
database:     ipsetdb isdb
bypass:       disable
```



While using IPS, short spikes in CPU usage by IPS processes can be caused by firewall policy or profile changes. These spikes are usually normal. Spikes might happen when FortiGate has hundreds of policies and profiles, or many virtual domains. Continuous high CPU use by the IPS engines is not normal, and you should investigate it. You can use the command shown on this slide, along with displayed options, to troubleshoot these issues.

If there are high CPU use problems caused by the IPS engine, you can use the `diagnose test application ipsmonitor` command with option 5 to isolate where the problem might be. Option 5 enables IPS bypass mode. In this mode, the IPS engine is still running, but it is not inspecting traffic. If the CPU use decreases after that, it usually indicates that the volume of traffic being inspected is too high for that FortiGate model.

If the CPU use remains high after you enable IPS bypass mode, it usually indicates a problem in the IPS engine, which you must report to Fortinet support. You can disable the IPS engine completely using option 2. If you want to restore IPS inspection of traffic after you finish troubleshooting, use option 2 again. At any time, you can check the status of the IPS engines using option 1.

Another recommendation to keep in mind is that if you need to restart the IPS, use option 99, as the slide shows. This guarantees that all the IPS-related processes restart correctly.

DO NOT REPRINT

© FORTINET

IPS Fail Open

- Fail open is triggered when the IPS socket buffer is full and new packets can't be added for inspection

```
config ips global
  set fail-open <enable|disable>
  ...
end
```

Enable – bypass the packet without inspection
Disable – drop the new packet (default)

- IPS fail open entry log :

```
date=2024-11-4 time=09:07:59 logid=0100022700 type=event subtype=system
level=critical vd="root" logdesc="IPS session scan paused" action="drop"
msg="IPS session scan, enter fail open mode"
```

- When troubleshooting IPS fail-open events, try to identify a pattern
 - Has the traffic volume increased recently?
 - Does fail open trigger at specific times during the day?
- Create IPS profiles specifically for the traffic type
 - An IPS sensor configured to protect Windows servers doesn't need Linux signatures
 - Disable IPS on internal-to-internal policies

Default disable and packets are dropped!



IPS goes into fail-open mode when IPS socket buffer is full for new packets. IPS engine has no space in memory to create more sessions and needs to decide whether to drop the sessions or bypass the sessions without inspection. What happens during this state depends on the IPS configuration. If the `fail-open` setting is enabled, some new packets (depending on the system load) will pass through without being inspected. By default, it is disabled, new packets are dropped.

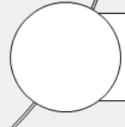
IPS fail-open is recommended only in situations where network availability takes precedence over network security—such as in a datacenter.

What to identify in fail-open scenarios? Frequent IPS fail open events usually indicate that IPS can't keep up with the traffic demands. So, try to identify patterns. Has the traffic volume increased recently? Have throughput demands increased? Does fail open trigger at specific times during the day?

Once you identified the resource constraints try to tune and optimize your IPS configuration. Create IPS profiles specific to the type of traffic being inspected, and disable IPS profiles on policies that don't need them.

DO NOT REPRINT**© FORTINET**

Lesson Progress

**IPS Configuration****IPS Monitoring****Application Control Basics****Application Control Configuration**

© Fortinet Inc. All Rights Reserved.

18

Good job! You now understand IPS monitoring on FortiGate.

Now, you will learn about application control basics.

DO NOT REPRINT**© FORTINET**

Application Control Basics

Objectives

- Understand application control
- Use application control signatures



© Fortinet Inc. All Rights Reserved. 19

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

By demonstrating competence in application control basics, you will be able to understand how application control works on FortiGate.

DO NOT REPRINT**© FORTINET**

Application Control

- Uses the IPS engine in flow-based scan
- Detects and acts on network application traffic
- Appropriate for detecting peer-to-peer (P2P) applications



As previously mentioned, the IPS engine is also responsible for application control. You can configure application control in proxy-based and flow-based firewall policies. However, because application control uses the IPS engine, which uses flow-based inspection, the inspection is always flow-based.

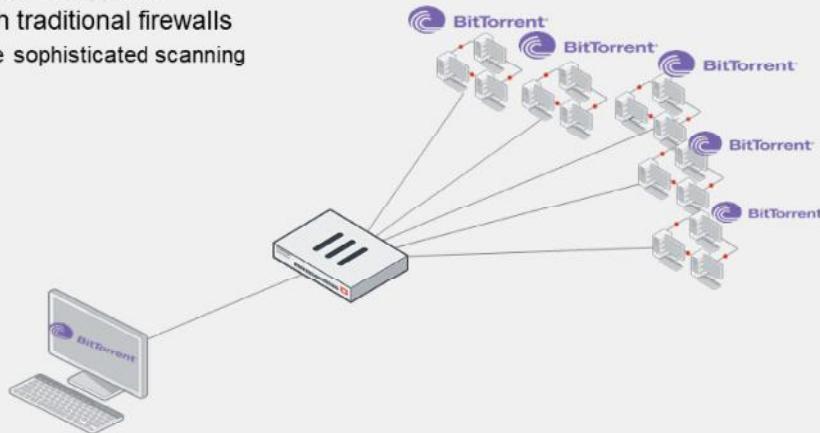
Application control identifies applications, such as Google Talk, by matching known patterns to the application transmission patterns. Therefore, an application can be accurately identified, only if its transmission pattern is unique. However, not every application behaves in a unique way. Many applications reuse pre-existing, standard protocols and communication methods. For example, many video games, such as *World of Warcraft*, use the BitTorrent protocol to distribute game patches. Still, with the help of the IPS engine, application control analyzes network traffic and detects application traffic, even if the application is using standard or non-standard protocols and ports. It doesn't operate using built-in protocol states. As a consequence, application control is better suited for detecting P2P protocols, because they use port randomization, pinholes, and changing encryption pattern techniques.

DO NOT REPRINT

© FORTINET

Peer-to-Peer Architecture

- Peer-to-peer (P2P) download
 - One client
 - Many servers
 - Dynamic port numbers
 - Optionally, dynamic encryption
 - *Hard to block* with traditional firewalls
 - Requires more sophisticated scanning



© Fortinet Inc. All Rights Reserved.

Peer-to-peer (P2P) downloads divide each file among multiple (theoretically unlimited) peers. Each peer delivers part of the file. While having many clients is a disadvantage in client-server architectures, it is an advantage for P2P architecture because, as the number of peers increases to n , the file is delivered n times faster.

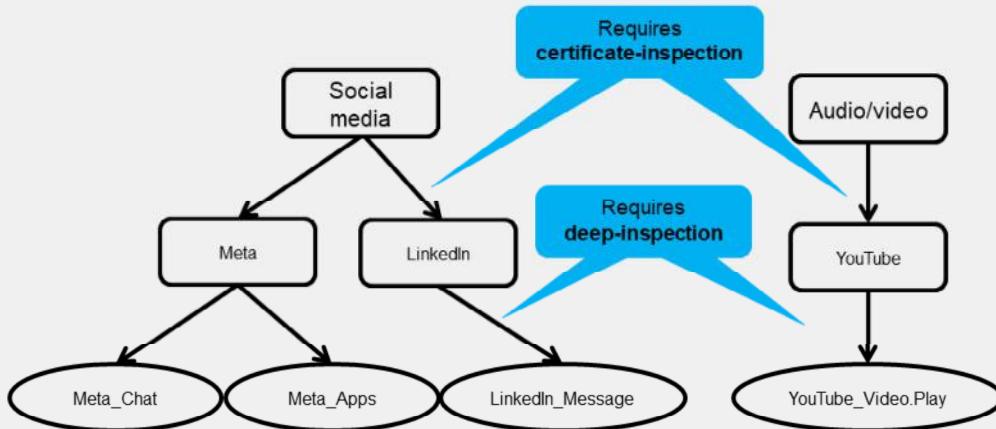
Because popularity increases the speed of delivery—unlike traditional client-server architecture where popularity could effectively cause a denial of service (DoS) attack on the server—some software, such as BitTorrent distributions of Linux, and games distributing new patches, leverage this advantage. Even if each client has little bandwidth, together they can offer more bandwidth for the download than many powerful servers.

Consequently, in order to download the file, the requesting peer can consume much more bandwidth per second than it would from only a single server. Even if there is only one peer in your network, it can consume unusually large amounts of bandwidth. Because the protocols are usually evasive, and there will be many sessions to many peers, they are difficult to completely block.

DO NOT REPRINT
© FORTINET

Application Control—Hierarchical Structure

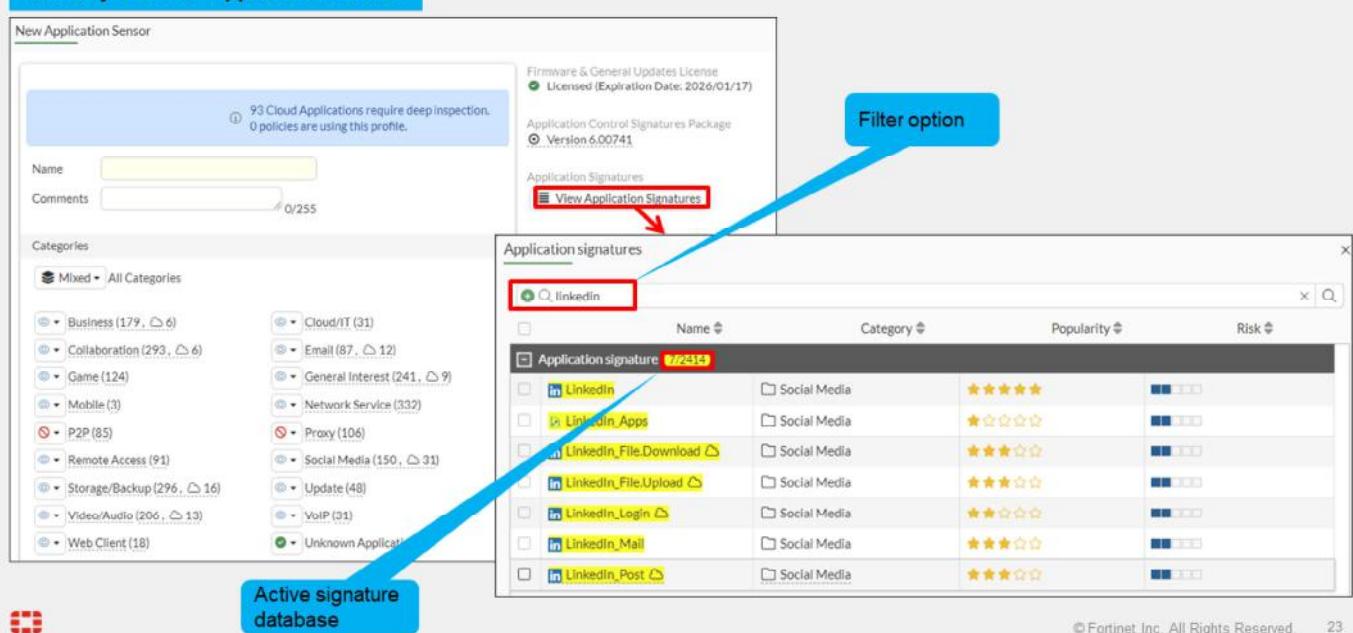
- Application control signatures are organized in a hierarchical structure
 - The parent signature takes precedence over the child signature



Many web applications offer functionality that can be embedded in third-party websites or applications. For example, you can embed a Meta **Like** button at the end of an article, or reference a YouTube video on an educational website. FortiOS gives administrators all the tools they need to inspect subapplication traffic. The FortiGuard application control signature database is organized in a hierarchical structure. This gives you the ability to inspect the traffic with more granularity. You can block Meta applications while allowing users to collaborate using Meta chat.

DO NOT REPRINT
© FORTINET

List of Application Signatures



The screenshot shows the FortiGuard Application Control Signature package interface. At the top, it displays a message about 93 Cloud Applications requiring deep inspection. Below this, there are fields for Name and Comments, and a Categories section with a dropdown set to 'Mixed - All Categories'.

On the right, there's a 'Firmware & General Updates License' section indicating it is licensed until 2026/01/17. Below that is the 'Application Control of Signatures Package' section, showing Version 6.00741. A red box highlights the 'View Application Signatures' button.

A blue callout labeled 'Filter option' points to the 'View Application Signatures' button. Another blue callout labeled 'Active signature database' points to the search bar in the 'Application signatures' list.

The 'Application signatures' list table has columns for Name, Category, Popularity, and Risk. It shows several LinkedIn-related signatures:

Name	Category	Popularity	Risk
LinkedIn	Social Media	★★★★★	███ ███
LinkedIn_Apps	Social Media	★★★★★	███ ███
LinkedIn_File.Download	Social Media	★★★★★	███ ███
LinkedIn_File.Upload	Social Media	★★★★★	███ ███
LinkedIn_Login	Social Media	★★★★★	███ ███
LinkedIn_Mail	Social Media	★★★★★	███ ███
LinkedIn_Post	Social Media	★★★★★	███ ███

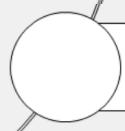
At the bottom right, there are copyright notices: © Fortinet Inc. All Rights Reserved. and 23.

After FortiGate downloads a FortiGuard Application Control Signature package, new signatures appear in the signature list.

In the example shown on this slide, the signatures are filtered with LinkedIn, showing its category and the corresponding hierarchical structure.

DO NOT REPRINT**© FORTINET**

Lesson Progress

**IPS Configuration****IPS Monitoring****Application Control Basics****Application Control Configuration**

© Fortinet Inc. All Rights Reserved. 24

Good job! You now understand basic application control functionality.

Now, you will learn about application control configuration.

DO NOT REPRINT**© FORTINET**

Application Control Configuration

Objectives

- Configure and apply application control profile
- Monitor application control events
- Troubleshoot traffic matching with application control profile issues



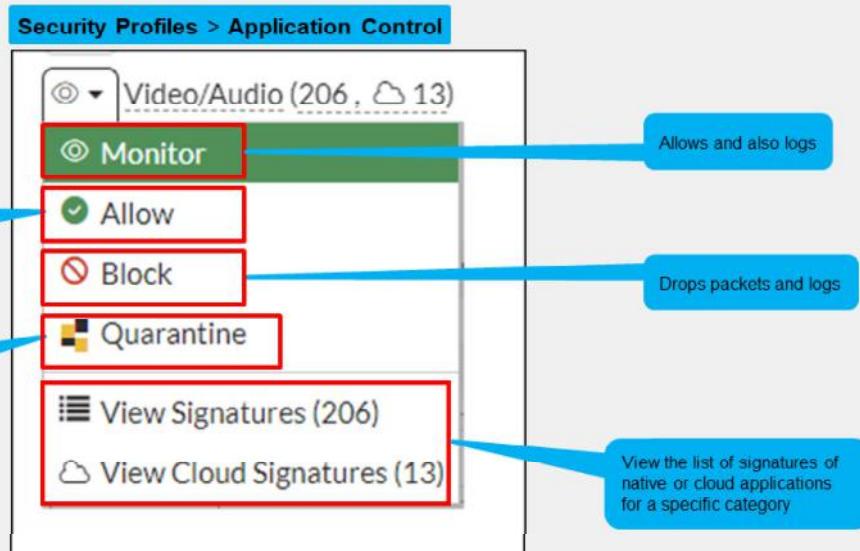
After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in application control feature configuration and monitoring, you will be able to use and maintain application control in profile mode.

DO NOT REPRINT

© FORTINET

Filters Actions



For each filter in the application control profile, you must indicate an action—what FortiGate does when traffic matches. Actions include the following:

- **Allow**: Passes the traffic and does not generate a log
- **Monitor**: Passes the traffic, but also generates a log message
- **Block**: Drops the detected traffic and generates a log message
- **Quarantine**: Blocks the traffic from the suspected source until the expiration time is reached, and generates a log message

The **View Signature** action allows you to view signatures from a particular category only and is *not* a configurable action. The **View Cloud Signatures** action allows you to view application signatures for cloud applications from a particular category.

Which is the correct action to choose?

If you're not sure which action to choose, **Monitor** can be useful initially, while you study your network. Later, after you have studied your network traffic, you can fine-tune your filter selection by choosing the most appropriate action. The action you choose also depends on the application. If an application requires feedback to prevent instability or other unwanted behavior, then you might choose **Quarantine** instead of **Block**. Otherwise, the most efficient use of FortiGate resources is to block.

DO NOT REPRINT

© FORTINET

Configuring Additional Options

The screenshot shows the FortiOS Security Profiles > Application Control interface. A red box highlights the "Network Protocol Enforcement" checkbox. Below it, a blue callout box states: "Allows blocking or monitoring of known services on unknown ports". An arrow points from this box to a sub-menu window titled "New Default Network Service". This window lists "Enforce protocols" (PROT HTTP) and "Violation action" (Monitor, Block). A red box highlights the "Block" button. Another red box highlights the "PROT HTTP" entry in the protocol list. A blue callout box labeled "List of known services" points to a sidebar containing a list of services: DNS, FTP, PROT HTTP (highlighted), HTTPS, IMAP, NNTP, POP3, SMTP, SNMP, SSH, and TELNET.

Options

- Block applications detected on non-default ports (checkbox)
- Allow and Log DNS Traffic (checkbox)
- Replacement Messages for HTTP-based Applications (checkbox)

Forces applications to run on its default port

Applies only to HTTP/HTTPS applications

© Fortinet Inc. All Rights Reserved. 27

The **application sensor** provides also additional options.

Enabling the **Network Protocol enforcement** option allows you to configure network services (for example, FTP, HTTP, and HTTPS) on known ports (for example, 21, 80, and 443), while blocking those services on other ports.

This feature takes action in the following scenarios:

- When one protocol dissector confirms the service of network traffic, **Network Protocol Enforcement** can check whether the confirmed service is allowlisted under the server port. If it is not, then the traffic is considered a violation and IPS can take the action (for example, block) specified in the configuration.
- When there is no confirmed service for network traffic. It would be considered a service violation if IPS dissectors rule out all the services enforced under its server port, for example, if port 21 is configured for FTP and the protocol dissector could not decide on the exact service but is sure it is not FTP. If the port of the non-FTP traffic is 21, it will be a violation.

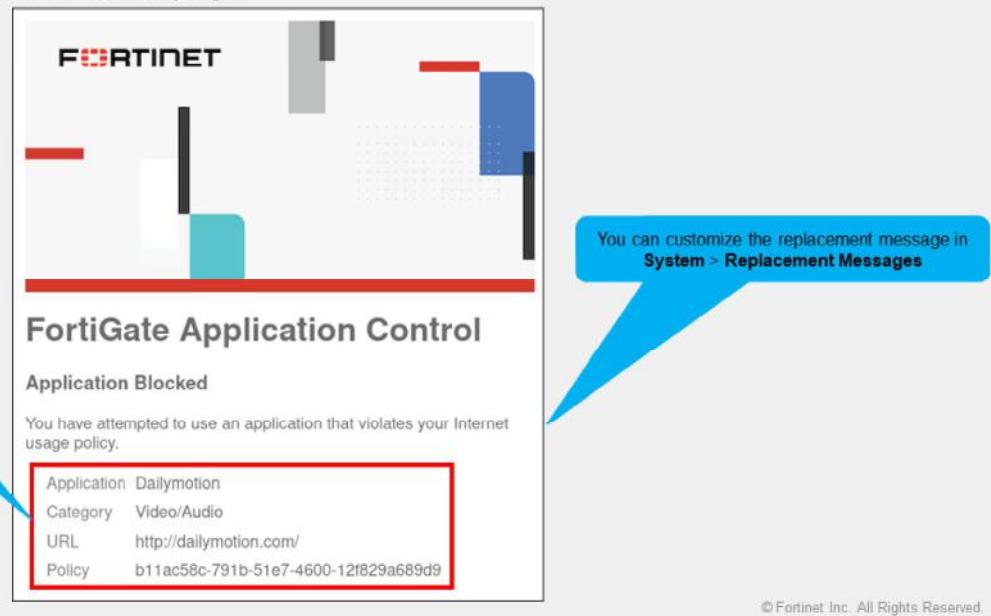
When the **Block applications detected on non-default ports** option enabled, FortiGate compares the ports used by the application with the ones defined in FortiGuard application signatures. The traffic is blocked if it does not match.

The **Replacement Messages for HTTP-based Applications** setting allows you to replace blocked content from HTTP/HTTPS applications with an explanation for the user's benefit. For non-HTTP/HTTPS applications, FortiGate only drops the packets or resets the TCP connection.

DO NOT REPRINT**© FORTINET**

HTTP Block Page

- Application control HTTP block page



© Fortinet Inc. All Rights Reserved. 28

For HTTP-based applications, application control can provide feedback to the user about why their application was blocked. This is called a block page, and it is similar to the one you can configure for URLs that you block using FortiGuard web filtering.

It is also worth mentioning that, if deep inspection is enabled in the firewall policy, all HTTPS-based applications provide this block page.

The block page contains the following information:

- Signature that detected the application (in this case, Dailymotion)
- Signature category (in this case, Video/Audio)
- URL that was specifically blocked (in this case, the index page of www.dailymotion.com), since a web page can be assembled from multiple URLs
- User name (if authentication is enabled)
- Group name (if authentication is enabled)
- Universal unique identifier (UUID) of the policy governing the traffic

The last item in this list can help you to identify which policy on FortiGate blocked the page, even if you have a large number of policies with many FortiGate devices securing different segments.

DO NOT REPRINT

© FORTINET

Scanning Order

- The IPS engine identifies the application
- The application control profile scans for matches in this order:
 - Application and filter overrides
 - Categories

The screenshot shows the 'Edit Application Sensor' configuration page. At the top, there are fields for 'Name' (set to 'default') and 'Comments' (set to 'Monitor all applications, 25/255'). Below these are two sections: 'Categories' and 'Application and Filter Overrides'. The 'Categories' section is highlighted with a red box and a green number 2. It contains a list of application categories with their counts: Business (179), Collaboration (293), Game (124), Mobile (3), P2P (85), Remote Access (91), Storage/Backup (296), Video/Audio (206), Web Client (18), Cloud/IT (31), Email (87), General Interest (241), Network Service (332), Proxy (106), Social Media (150), Update (48), VoIP (31), and Unknown Applications. The 'Application and Filter Overrides' section is highlighted with a red box and a green number 1. It has a table with columns: Priority, Details, Type, and Action. The table displays the message 'No results'.



With these multiple filters, which one has the priority?

After the IPS engine examines the traffic stream for a signature match, FortiGate scans packets for matches, in this order, for the application control profile:

- Application and filter overrides: If you have configured any application overrides or filter overrides, the application control profile considers those first. It looks for a matching override starting at the top of the list, like firewall policies.
- Categories: Finally, the application control profile applies the action that you have configured for applications in your selected categories.

DO NOT REPRINT

© FORTINET

Order of Scan and Blocking Behavior (Scenario 1)

The screenshot shows the 'Security Profiles > Application Control' page. At the top, there's a search bar with 'Name: default' and 'Comments: Monitor all applications.' Below it, under 'Categories', there's a tree view of application categories. Three categories are highlighted with red boxes and circled numbers: 'Game (124)' (circled 3), 'Video/Audio (206, △ 13)' (circled 3), and 'Excessive-Bandwidth' (circled 2). A callout bubble for 'Game' and 'Video/Audio' states: 'The Game and Video/Audio categories are set to Block and all other categories are set to Monitor'. Another callout bubble for 'Excessive-Bandwidth' states: 'Application overrides set for Battle Net and Dailymotion applications' and 'Filter overrides set for applications that consume excessive bandwidth'. In the 'Application and Filter Overrides' section, there are two entries: entry 1 for 'Battle.Net' (Application, Monitor) and entry 2 for 'Excessive-Bandwidth' (Filter, Block). A small '© Fortinet Inc. All Rights Reserved.' and '30' are at the bottom right.

In the example profile shown on this slide, the application control profile blocks the **Game** and **Video/Audio** categories. All other categories are set to **Monitor**, except **Unknown Applications**, which is set to **Allow**.

In the **Application and Filter Overrides** section, you can see that some exceptions are specified. Instead of being set to **Block**, **Battle.Net (Game)**, and **Dailymotion (Video/Audio)** are set to **Monitor**. Because application overrides are applied first in the scan, these two applications are allowed and generate logs.

Next, the scan checks for **application and filter overrides**. Because a filter override is configured to block applications that use excessive bandwidth, it blocks all applications using excessive bandwidth, regardless of other categories that allow these applications.

This slide shows an example of how several security profile features could work together, overlap, or work as substitutes, on the same traffic.

After FortiGate completes the application control profile scan, it begins other scans, such as web filtering. The web filtering scan could block Battle.Net and Dailymotion, but it would use its own block message. Also, web filtering doesn't check the list of application control overrides. So, even if an application control override allows an application, web filtering could still block it.

Similarly, static URL filtering has its own exempt action, which bypasses all subsequent security checks. However, application control occurs before web filtering, so that the web filtering exemption *cannot* bypass application control.

DO NOT REPRINT

© FORTINET

Order of Scan and Blocking Behavior (Scenario 2)

The screenshot shows the 'Security Profiles > Application Control' interface. At the top, there is a 'Categories' section with a 'Mixed - All Categories' dropdown. Below it is a list of application categories: Business (179), Collaboration (293), Game (124) (highlighted with a red box and circled with a green '3'), Mobile (3), P2P (85), Remote Access (91), Storage/Backup (296), Video/Audio (206), and Web Client (18). In the 'Application and Filter Overrides' section, there is a table with two entries:

Priority	Details	Type	Action
1	Excessive-Bandwidth Filter	Block	
2	Battle.Net Dailymotion	Application Monitor	

A blue callout bubble points to the 'Game (124)' category with the text: 'The filter override entry is moved above the application override entry'. A green circle labeled '1' highlights the first row in the overrides table, and a green circle labeled '2' highlights the second row. A green circle labeled '3' highlights the 'Game (124)' category in the categories list.

© Fortinet Inc. All Rights Reserved. 31

In the example profile shown on this slide, the filter override has been moved above the application override. In this scenario, the filter override (**Excessive-Bandwidth**) is blocked and, since Dailymotion falls under the excessive bandwidth category, Dailymotion is blocked even though it is set to **Monitor** in the **Application and Filter Overrides** section.

The priority in which application and filter overrides are placed takes precedence.

DO NOT REPRINT

© FORTINET

Applying an Application Control Profile

- You must apply the **application control** profile on a firewall policy to scan the passing traffic
- Enable logging for security events or all sessions to log application control events.

The screenshot shows the 'Policy & Objects > Firewall Policy' section of the FortiGate management interface. It displays various security profiles: AntiVirus, Web Filter, DNS Filter, Application Control, IPS, File Filter, and SSL Inspection. The 'Application Control' and 'SSL Inspection' profiles are highlighted with red boxes and have edit icons next to them. Below these profiles are 'Decrypted Traffic Mirror' and 'Logging Options'. The 'Logging Options' section has a red box around the 'Log Allowed Traffic' switch, which is set to 'Security Events' and 'All Sessions'. A blue callout bubble points to the 'Application Control' profile with the text 'Enable Application Control and select the profile'. Another blue callout bubble points to the 'SSL Inspection' profile with the text 'Use deep-inspection profile to scan encrypted traffic'. A third blue callout bubble points to the 'Log Allowed Traffic' switch with the text 'Enable logging'.

Policy & Objects > Firewall Policy

Security Profiles

- AntiVirus
- Web Filter
- DNS Filter
- Application Control**
- IPS
- File Filter
- SSL Inspection**
- Decrypted Traffic Mirror

Logging Options

Log Allowed Traffic **Security Events** **All Sessions**

© Fortinet Inc. All Rights Reserved. 32

After you configure an application control profile, you must apply it to a firewall policy. This instructs FortiGate to start scanning application traffic that is subject to the firewall policy.

When you enable the logging of security events or all sessions on a firewall policy, application control events are also logged. It allows you to monitor the application control use.

DO NOT REPRINT

© FORTINET

Monitoring Application Control Logging

The screenshot shows the FortiGate Log & Report interface. In the top navigation bar, 'Log & Report > Security Events' is selected. Below it, there are two tabs: 'Summary' and 'Logs'. The 'Logs' tab is active, showing a table of security events. A red box highlights the 'Logs' tab. A red arrow points from the 'Logs' tab to a red box labeled 'Application Control' in the summary section. Another red arrow points from the 'Logs' tab to a red box labeled 'Details' in the log table. A blue speech bubble labeled 'Application control information' points to the 'Details' box.

Top Category	Action	Count
Web.Client	Pass	70
General Interest	Pass	25
Video/Audio	Block	8
Network.Service	Pass	5

Logs

Date/Time	Source	Destination	Application Name	Action
2024/10/07 16:22:04	10.0.1.10	3.134.235.187	Dailymotion	Block
2024/10/07 16:22:04	10.0.1.10	3.134.235.187	HTTPS.BROWSER	Pass
2024/10/07 16:22:04	10.0.1.10	3.134.235.187	Dailymotion	Block
2024/10/07 16:22:04	10.0.1.10	3.134.235.187	HTTPS.BROWSER	Pass
2024/10/07 16:22:00	10.0.1.10	3.134.235.187	HTTPS.BROWSER	Pass
2024/10/07 16:21:58	10.0.1.10	142.251.111.94	Google.Accounts	Pass

Log Details

Sensor	default
Application Name	Dailymotion
Application ID	16072
Category	Video/Audio
Application Risk	Low
Protocol	HTTP
Service	Video/Audio
Message	Video/Audio: Dailymotion
Action	Block
Action	Block
Policy ID	Application_Control (1)
Policy UUID	b11ac58c-791b-51e7-4600-12f829a689d9
Policy Type	Firewall

© Fortinet Inc. All Rights Reserved. 33

FortiGate logs all application control events on the **Log & Report > Security Events** page. You can view the logs by clicking **Application Control**.

In the example shown on this slide, the default application control profile blocks access to Dailymotion. You can view this information in the **Log Details** section, as well as information about the log source, destination, application, and action.

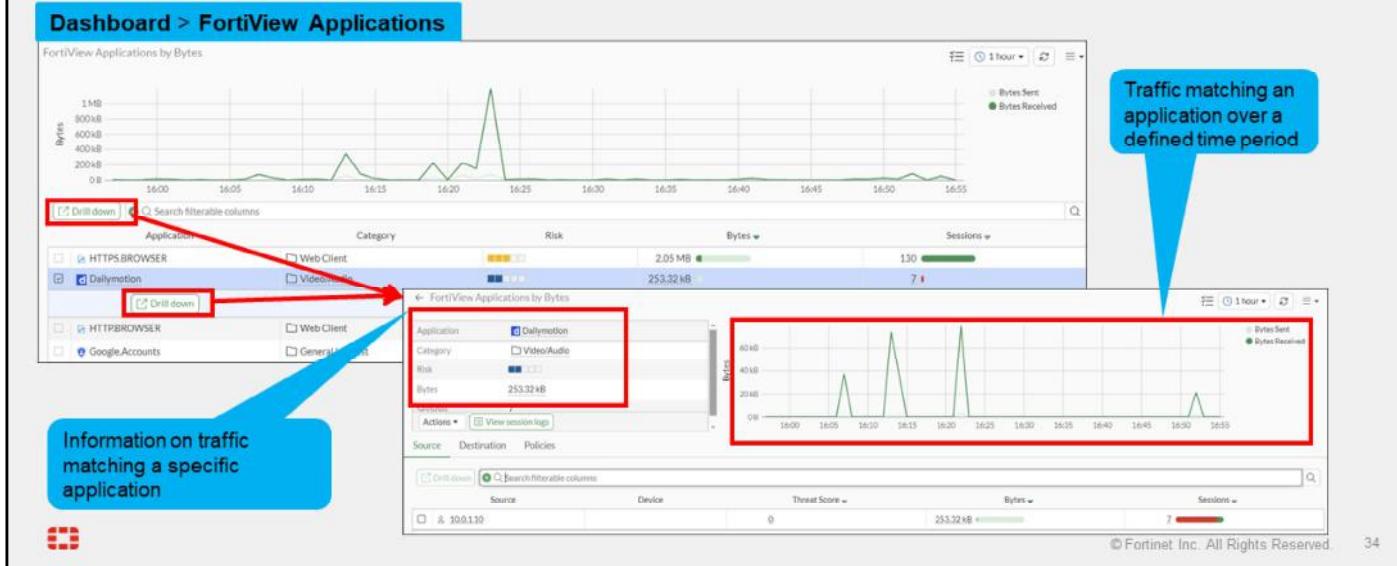
You can also view the details on the **Forward Traffic** logs page, where firewall policies record activity. You can also find a summary of the traffic to which FortiGate applied application control. Again, this is because application control is applied by a firewall policy. To find out which policy applied application control, you can review either the **Policy ID** or the **Policy UUID** fields of the log message.

DO NOT REPRINT

© FORTINET

Troubleshoot Traffic Matching Application Control Profile

- Apply application control only to the traffic that requires it, and enable logging
- Review the logs and modify the configuration according to observations



Because not all traffic requires an application control scan, you must monitor the security event logs. If a traffic match is incorrect, you must then modify your configuration by first finding the firewall policy involved. This firewall policy reference is available in the **security events** logs and **forward traffic** logs.

You can also check the traffic matching with application control profiles on the **Dashboard > FortiView Applications** page. You can then select a specific application and drill down to view the sessions and bytes information for the traffic matching that application.

DO NOT REPRINT**© FORTINET**

Knowledge Check

1. Which IPS component is responsible for application control?
 A. Protocol decoders
 B. IPS engine

2. Which statement about the HTTP block page for application control is true?
 A. It can be used only for web applications.
 B. It works for all types of applications.



DO NOT REPRINT

© FORTINET

Lesson Progress



IPS Configuration



IPS Monitoring



Application Control Basics



Application Control Configuration



© Fortinet Inc. All Rights Reserved. 36

Congratulations! You have completed this lesson.

Now, you will review the objectives covered in this lesson.

DO NOT REPRINT**© FORTINET**

Review

- ✓ Configure an IPS sensor
- ✓ Troubleshoot IPS high CPU usage and IPS fail open
- ✓ Configure and apply an application control profile
- ✓ Monitor application control events
- ✓ Troubleshoot traffic matching with application control profile issues



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

By mastering the objectives covered in this lesson, you learned how to configure, maintain, and troubleshoot the FortiGate IPS solution. You also learned how to use methods beyond simply blocking protocols, port numbers, or IP addresses, to monitor and control both standard and non-standard network applications.

DO NOT REPRINT

© FORTINET

FORTINET
Training Institute

FortiOS Administrator

IPsec VPN

 FortiOS 7.6

Last Modified: 6 October 2025

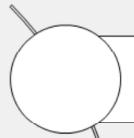
© Fortinet Inc. All Rights Reserved. 1

In this lesson, you will learn about the architectural components of IPsec VPN and how to configure them.

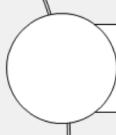
DO NOT REPRINT

© FORTINET

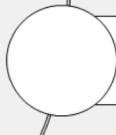
Lesson Overview



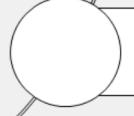
IPsec Basics



IPsec Configuration



Routing and Firewall Policies



Monitoring



© Fortinet Inc. All Rights Reserved.

2

In this lesson, you will learn about the topics shown on this slide.

DO NOT REPRINT

© FORTINET

IPsec Basics

Objectives

- Describe the benefits of IPsec VPN
- Be familiar with the IPsec protocol
- Understand how IPsec works
- Select an appropriate VPN topology



© Fortinet Inc. All Rights Reserved. 3

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

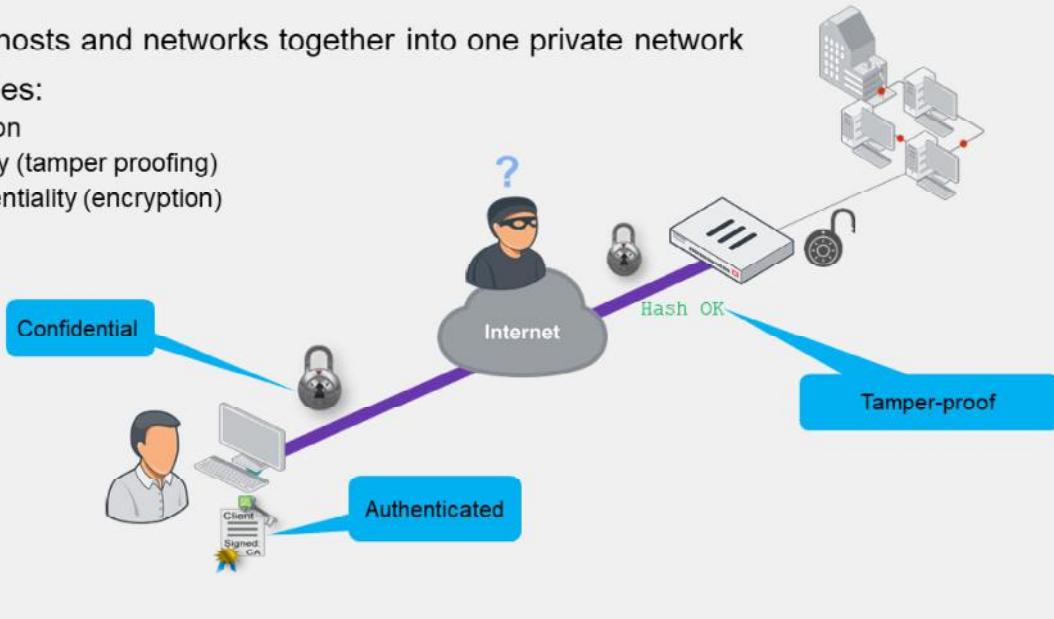
By demonstrating competence in IPsec basics, you will be able to understand IPsec concepts and benefits.

DO NOT REPRINT

© FORTINET

What Is IPsec?

- Joins remote hosts and networks together into one private network
- Usually provides:
 - Authentication
 - Data integrity (tamper proofing)
 - Data confidentiality (encryption)



© Fortinet Inc. All Rights Reserved.

4

What is IPsec? When should you use it?

IPsec is a vendor-neutral set of standard protocols that is used to join two physically distinct LANs. The LANs are joined as if they were a single logical network, despite being separated by the internet.

In theory, IPsec *does* support null encryption—that is, you can make VPNs that don't encrypt traffic. IPsec also supports null data integrity. But does that provide any advantages over plain traffic? No. No one can trust traffic that may have had an attack injected by an attacker. Rarely do people want data sent by an unknown source. Most people also want private network data, such as credit card transactions and medical records, to remain private.

Regardless of the vendor, IPsec VPNs almost always have settings that allow them to provide three important benefits:

- Authentication: to verify the identity of both ends
- Data integrity (or HMAC): to prove that encapsulated data has not been tampered with as it crosses a potentially hostile network
- Confidentiality (or encryption): to make sure that only the intended recipient can read the message

DO NOT REPRINT

© FORTINET

What Is the IPsec Protocol?

- Multiple protocols that work together
 - Authentication Header (AH) provides integrity but not encryption
 - AH is defined in the RFC, but FortiGate does not use it
- Port numbers and encapsulation vary by network address translation (NAT)

Protocol	NAT Traversal (NAT-T)	No NAT
IKE	IP protocol 17:	IP protocol 17:
RFC 2409 (IKEv1)	UDP port 500	UDP port 500
RFC 4306 (IKEv2)	(UDP 4500 for rekey, quick mode, mode-cfg)	
ESP	IP protocol 17:	IP protocol 50
RFC 4303	UDP port 4500 (encapsulated)	

- If required, set a custom port for both IKE and IKE NAT-T (initiator and responder)*:

```
config system settings
  set ike-port <port>
end
```

* Custom port range: 1024–65535. FortiGate always listens on UDP port 4500 (responder only)



If you're passing your VPN through firewalls, it helps to know which protocols to allow.

IPsec is a suite of separate protocols, which includes:

- Internet Key Exchange (IKE): used to authenticate peers, exchange keys, and negotiate the encryption and checksums that are used—essentially, it is the *control channel*
- AH: contains the authentication header—the checksums that verify the integrity of the data
- Encapsulating Security Payload (ESP): the encapsulated security payload—the encrypted payload, which is essentially the *data channel*

So, if you must pass IPsec traffic through a firewall, remember that allowing only one protocol or port number is usually not enough.

Note that the IPsec RFC mentions AH, however, AH does not offer encryption, which is an important benefit. Therefore, FortiGate does not use AH. As a result, you don't need to allow the AH IP protocol (51).

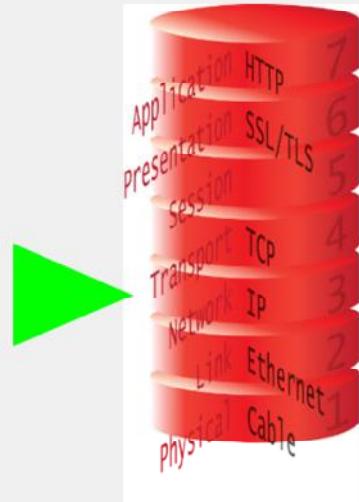
To set up a VPN, you must configure matching settings on both ends of the VPN—whether the VPN is between two FortiGate devices, FortiGate and FortiClient, or a third-party device and FortiGate. If the settings don't match, the tunnel setup fails.

The default ports for standard IKE traffic and IKE NAT-T traffic are UDP 500 and UDP 4500, respectively. You can use the CLI command shown on this slide to configure a custom port for both IKE and IKE NAT-T. The custom port is used to initiate and respond to tunnel requests. If NAT is detected, then the custom port can be used for both IKE and UDP-encapsulated ESP traffic. Note that FortiGate always listens for port UDP 4500 regardless of the custom port settings. This enables FortiGate to negotiate NAT-T tunnels on custom and standard ports.

DO NOT REPRINT**© FORTINET**

How Does IPsec Work?

- Encapsulation
 - Other protocols wrapped inside IPsec
 - What's inside? Varies by mode:
 - Transport mode—TCP/UDP
 - Tunnel mode—additional IP layer, then TCP/UDP
- Negotiation
 - Authentication
 - Handshake to exchange keys, settings

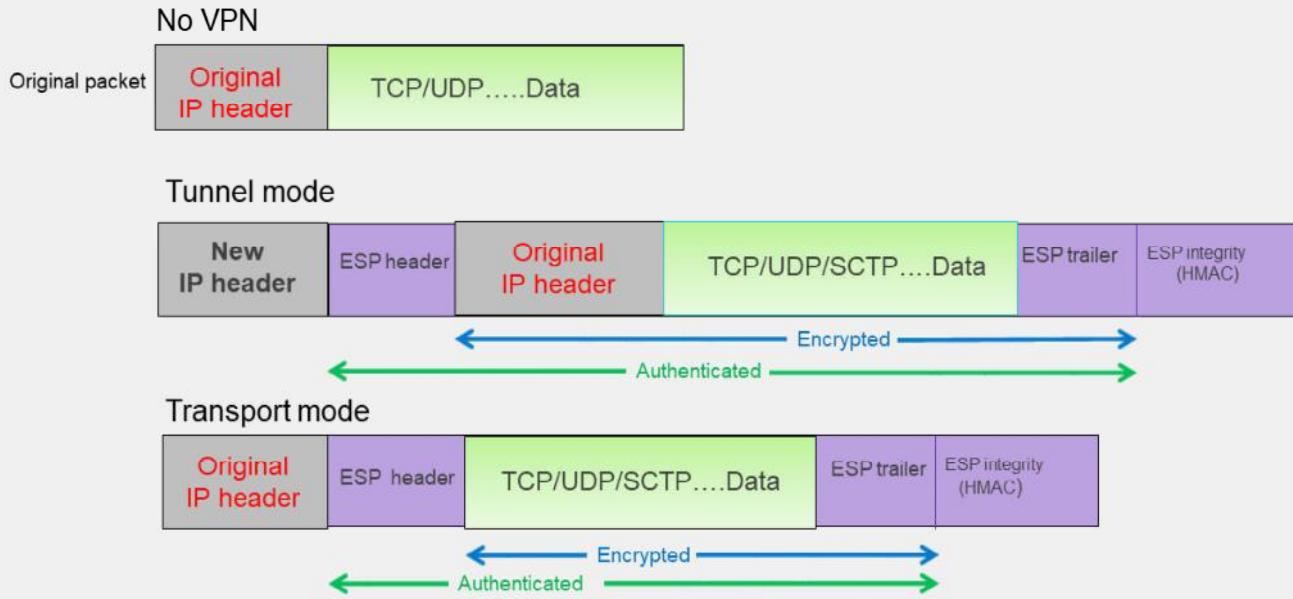


IPsec provides services at the IP (network) layer. During tunnel establishment, both ends negotiate the encryption and authentication algorithms to use.

After the tunnel has been negotiated and is up, data is encrypted and encapsulated into ESP packets.

DO NOT REPRINT
© FORTINET

ESP Encapsulation—Tunnel or Transport Mode



© Fortinet Inc. All Rights Reserved. 7

What's encapsulated? It depends on the encapsulation mode IPsec uses. IPsec can operate in two modes: transport mode and tunnel mode.

- Transport mode directly encapsulates and protects the fourth layer (transport) and above. It does not protect the original IP header and does not add an additional IP header.
- Tunnel mode is a true tunnel. It encapsulates the whole IP packet and adds a new IP header at the beginning. After the IPsec packet reaches the remote LAN and is unwrapped, the original packet can continue on its journey.

Note that after you remove the VPN-related headers, a transport mode packet can't be transmitted any further; it has no second IP header inside, so it's not routable. For that reason, this mode is usually used only for end-to-end (or client-to-client) VPNs.

DO NOT REPRINT

© FORTINET

What Is IKE?

- Default ports: UDP port 500 (and UDP port 4500 when crossing NAT)
- Negotiates a tunnel's private keys, authentication, and encryption
- Phases:
 - Phase 1
 - Phase 2
- Versions
 - IKEv1 (legacy, wider adoption)
 - IKEv2 (new, simpler operation)



IKE uses UDP port 500. If NAT-T is enabled in a NAT scenario, IKE uses UDP port 4500.

IKE establishes an IPsec VPN tunnel. FortiGate uses IKE to negotiate with the peer and determine the IPsec security association (SA). The IPsec SA defines the authentication, keys, and settings that FortiGate uses to encrypt and decrypt that peer's packets. It is based on the Internet Security Association and Key Management Protocol (ISAKMP).

IKE defines two phases: phase 1 and phase 2.

There are two IKE versions: IKEv1 and IKEv2. Even though IKEv2 is a newer version and features a simpler protocol operation, this lesson focuses on IKEv1 only, because of its much wider adoption.

DO NOT REPRINT

© FORTINET

IKEv1 vs. IKEv2

Feature	IKEv1	IKEv2
Exchange modes	<ul style="list-style-type: none"> Main <ul style="list-style-type: none"> Total messages: 9 (6 for phase 1, 3 for phase 2) Aggressive <ul style="list-style-type: none"> Total messages: 6 (3 for phase 1, 3 for phase 2) 	<ul style="list-style-type: none"> One exchange procedure only Total messages: 4 (one child SA only)
Authentication methods	Symmetric: <ul style="list-style-type: none"> Pre-shared key (PSK) Certificate signature Extended authentication (XAuth) 	Asymmetric: <ul style="list-style-type: none"> PSK Certificate signature EAP (pass-through—no client support)
NAT-T	Supported as extension	Native support
Reliability	Unreliable—messages are not acknowledged	Reliable—messages are acknowledged
Dial-up phase 1 matching by ID	<ul style="list-style-type: none"> Peer ID + aggressive mode + PSK Peer ID + main mode + certificate signature 	<ul style="list-style-type: none"> Peer ID Network ID
Traffic selector narrowing	Not supported	Supported



This slide shows a table comparing some of the IKEv1 and IKEv2 features that FortiOS supports. IKEv2 provides a simpler operation, which is the result of using a single exchange mode and requiring less messages to bring up the tunnel.

Authentication-wise, both versions support PSK and certificate signature. Although only IKEv1 supports XAuth, IKEv2 supports EAP, which is equivalent to XAuth. However, the FortiOS IKEv2 EAP implementation is pass-through only. That is, FortiOS doesn't support EAP as a client, which means that you cannot revoke access to peers using IKEv2 unless you use a certificate signature. With IKEv1, you can deny access to VPN peers without having to use a certificate signature by using XAuth. IKEv2 also supports asymmetric authentication, which enables you to configure each peer to use a different authentication method.

Both IKE versions support NAT-T. However, IKEv2 supports NAT-T natively, while IKEv1 supports NAT-T as an extension. Also, IKEv2 is a more reliable protocol than IKEv1 because, like TCP, peers must acknowledge the messages exchanged between them. IKEv1 doesn't support such a mechanism.

When you configure multiple dial-up IPsec VPNs, IKEv2 makes it simpler to match the intended gateway by peer ID. With IKEv2, you can either use the standard peer ID attribute or the Fortinet proprietary network ID attribute to indicate the phase 1 gateway to match on the dial-up server, regardless of the authentication mode in use. However, with IKEv1, you can use the peer ID only, and then combine it with aggressive mode and pre-shared key authentication, or with main mode and certificate signature authentication.

Finally, IKEv2 allows the responder to choose a subset of the traffic the initiator proposes. This is called traffic selector narrowing and enables you to have more flexible phase 2 selector configurations. Traffic selector narrowing enables a peer to automatically narrow down its traffic selector addresses, so it agrees with the traffic selector the remote peer proposes.

DO NOT REPRINT**© FORTINET**

Negotiation—Security Association (SA)

- IKE allows the parties involved in a transaction to set up their Security Associations (SAs)
 - SAs are the basis for building security functions into IPsec
 - In normal two-way traffic, the exchange is secured by a pair of SAs
 - IPsec administrators decide the encryption and authentication algorithms that can be used in the exchange
- IKE uses two distinct phases:
 - Phase 1 → Outcome: IKE SA
 - Phase 2 → Outcome: IPsec SA



In order to create an IPsec tunnel, both devices must establish their SAs and secret keys, which are facilitated by the IKE protocol.

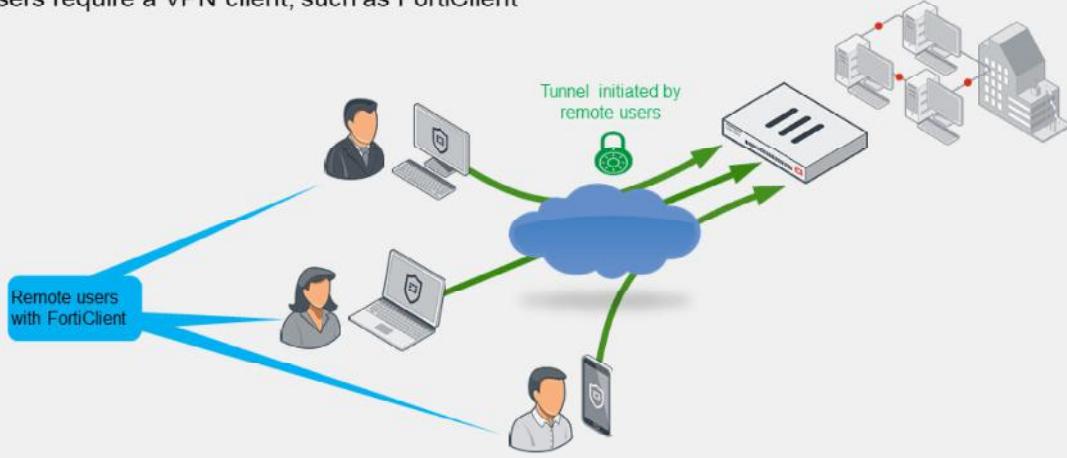
The IPsec architecture uses SAs as the basis for building security functions into IPsec. An SA is the bundle of algorithms and parameters being used to encrypt and authenticate data travelling through the tunnel. In normal two-way traffic, this exchange is secured by a pair of SAs, one for each traffic direction. Essentially, both sides of the tunnel must agree on the security rules. If both sides cannot agree on the rules for sending data and verifying each other's identity, then the tunnel is not established. SAs expire and need to be renegotiated by the peers after they have reached their lifetime.

IKE uses two distinct phases: phase 1 and phase 2. Each phase negotiates different SA types. The SA negotiated during phase 1 is called IKE SA, and the SA negotiated during phase 2 is called IPsec SA. FortiGate uses IKE SAs for setting up a secure channel to negotiate IPsec SAs. FortiGate uses IPsec SAs for encrypting and decrypting the data sent and received, respectively, through the tunnel.

DO NOT REPRINT
© FORTINET

VPN Topologies—Remote Access

- Remote users connect to corporate resources
 - FortiGate is configured as dial-up server—only clients can initiate the VPN
 - Users require a VPN client, such as FortiClient



Use remote access VPNs when remote internet users need to securely connect to the office to access corporate resources. The remote user connects to a VPN server located on the corporate premises, such as FortiGate, to establish a secure tunnel. After the user is authenticated, FortiGate provides access to network resources, based on the permissions granted to that user.

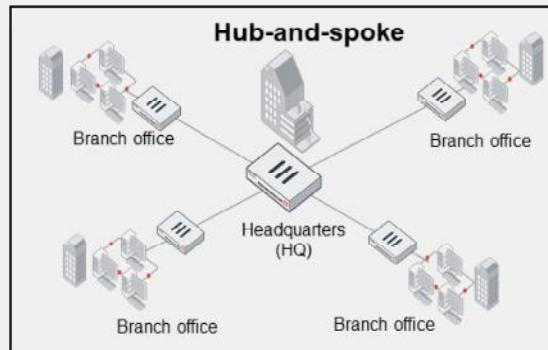
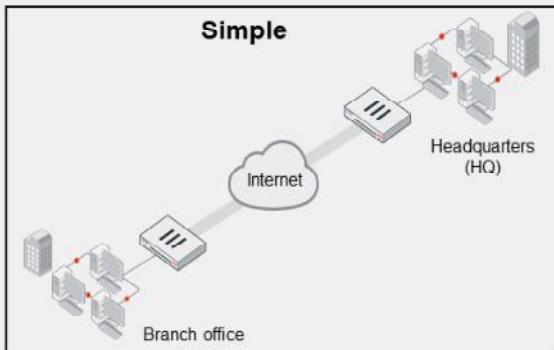
In a remote access VPN, FortiGate is usually configured as a dial-up server. You will learn more about dial-up VPNs in this lesson. The IP address of the remote internet user is usually dynamic. Because FortiGate does not know the IP address of the remote user, only the remote user can initiate a VPN connection request.

The remote user side needs a VPN client, such as FortiClient. You must configure FortiClient to match the VPN server settings. FortiClient takes care of establishing the tunnel, as well as routing the traffic destined to the remote site through the tunnel.

In addition, you can use one remote access VPN configuration on your FortiGate device for many remote users. FortiGate establishes a separate tunnel for each of them.

DO NOT REPRINT**© FORTINET**

VPN Topologies—Site-to-Site



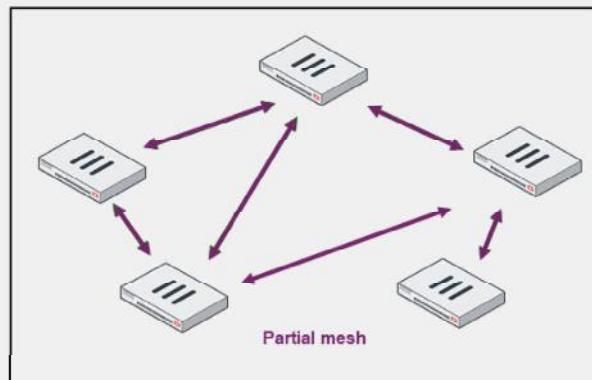
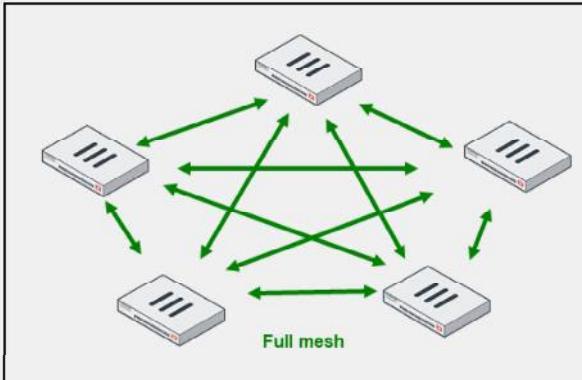
Site-to-site VPN is also known as LAN-to-LAN VPN. A simple site-to-site deployment involves two peers communicating directly to connect two networks located at different offices.

When you need to connect more than two locations, you can use a hub-and-spoke topology. In hub-and-spoke, all clients connect through a central hub. In the example shown on this slide, the clients—spokes—are branch office FortiGate devices. For any branch office to reach another branch office, its traffic must pass through the hub. One advantage of this topology is that the configuration needed is easy to manage. Another advantage is that only the FortiGate at HQ must be very powerful because it handles all tunnels simultaneously, while the branch office FortiGate devices require much fewer resources because they maintain only one tunnel. One disadvantage is that communication between branch offices through HQ is slower than in a direct connection, especially if your HQ is physically distant. Also, if the FortiGate device at HQ fails, VPN failure is company-wide.

DO NOT REPRINT
© FORTINET

VPN Topologies—Site-to-Site (Contd)

Full mesh and partial mesh



© Fortinet Inc. All Rights Reserved.

13

In a mesh topology, you can connect FortiGate devices directly and therefore bypass HQ. Two variations of mesh topology exist: full mesh and partial mesh. Full mesh connects every location to every other location. The higher the number of FortiGate devices, the higher the number of tunnels to configure on each FortiGate device. For example, in a topology with five FortiGate devices, you would need to configure four tunnels on each device, for a total of 20 tunnels. This topology causes less latency and requires much less HQ bandwidth than hub-and-spoke, but requires each FortiGate device to be more powerful. Partial mesh attempts to compromise, minimizing required resources but also latency. Partial mesh can be appropriate if communication is not required between every location. However, the configuration of each FortiGate device is more complex than in hub-and-spoke. Routing, especially, may require extensive planning.

Generally, the more locations you have, hub-and-spoke will be cheaper, but slower, than a mesh topology. Mesh places less strain on the central location. It's more fault-tolerant, but also more expensive.

DO NOT REPRINT
© FORTINET

VPN Topologies—Comparison

Hub-and-Spoke	Partial Mesh	Full Mesh
Easy configuration	Moderate configuration	Complex configuration
Few tunnels	Medium number of tunnels	Many tunnels
High central bandwidth	Medium bandwidth in hub sites	Low bandwidth
Not fault tolerant	Some fault tolerance	Fault tolerant
Low system requirements on average, but high for center	Medium system requirements	High system requirements
Scalable	Somewhat scalable	Difficult to scale
No direct communication between spokes	Direct communication between some sites	Direct communication between all sites



To review, this slide shows a high-level comparison of VPN topologies. You should choose the topology that is most appropriate to your situation.

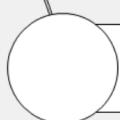
DO NOT REPRINT

© FORTINET

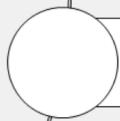
Lesson Progress



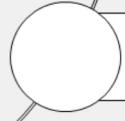
IPsec Basics



IPsec Configuration



Routing and Firewall Policies



Monitoring



© Fortinet Inc. All Rights Reserved.

15

Good job! You have now been introduced to IPsec.

Now, you will learn about IPsec configuration.

DO NOT REPRINT

© FORTINET

IPsec Configuration

Objectives

- Configure IPsec VPN using the IPsec wizard
- Configure IPsec VPN manually



© Fortinet Inc. All Rights Reserved.

16

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

By demonstrating competence in IPsec configuration, you will also be able to successfully determine the settings required for your IPsec VPN deployment.

DO NOT REPRINT

© FORTINET

IPsec Wizard

VPN > IPsec Wizard

Network diagram describing deployment type

Summary of objects created by the IPsec wizard

In this lesson, you will learn only about IKEv1 configuration

© Fortinet Inc. All Rights Reserved. 17

When you create an IPsec tunnel on the GUI, FortiGate redirects you to the **IPsec Wizard**. The wizard simplifies the creation of the new VPN by walking you through a four to five-step process. The first step is to select a template type. If you want to manually configure your VPN, you can select **Custom as Template type**, upon which FortiGate takes you directly to the phase 1 and phase 2 settings of the new VPN.

If you want the wizard to configure the VPN for you, then select the template type (**Site to Site, Hub-and-Spoke, or Remote Access**) that best matches your VPN. After that, the wizard asks you for key information, such as the remote gateway information, authentication method, interfaces involved, and subnets. Based on the input you provide, the wizard applies one of the preconfigured IPsec tunnel templates comprising IPsec phase 1 and 2 settings and other related firewall address objects, routing settings, and firewall policies needed for the new tunnel to work.

In addition, the wizard shows a network diagram that changes based on the input you provide. The purpose of the diagram is for the administrator to have a visual understanding of the IPsec VPN deployment that the wizard configures based on the input it receives.

At the end of the wizard, the wizard provides a summary of the configuration changes made in the system, and that the administrator can review if needed.

If you are new to FortiGate, or don't have much experience with IPsec VPNs, using the IPsec wizard is recommended. You can later adjust the configuration applied by the wizard to match your specific needs.

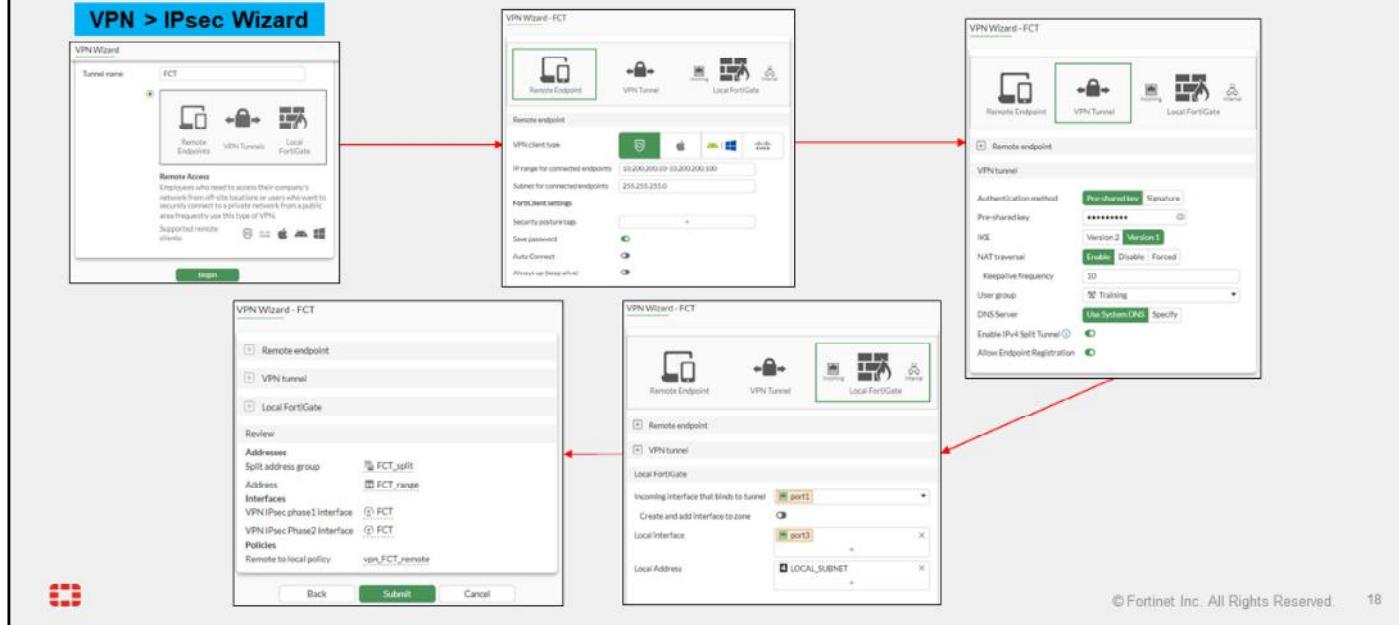
Note that, in this lesson, you will learn only about IKEv1 configuration.

DO NOT REPRINT

© FORTINET

Using the IPsec Wizard for a FortiClient VPN

- Simplifies IPsec configuration for a FortiClient VPN



A common use of the IPsec wizard is for configuring a remote access VPN for FortiClient users. The wizard enables IKE mode config, XAuth, and other appropriate settings for FortiClient users. You will learn more about IKE mode config and XAuth in this lesson.

The images on this slide show the four-step process used by the IPsec wizard for assisting the administrator on the FortiClient VPN configuration.

DO NOT REPRINT**© FORTINET**

Phase 1—Overview

- Each peer of the tunnel—the initiator and the responder—connects and begins to set up the VPN
- On the first connection, the channel is not secure
 - Unencrypted keys can be intercepted
- To exchange sensitive private keys, both peers create a secure channel
 - Both peers negotiate the real keys for the tunnel later



Phase 1 takes place when each peer of the tunnel—the initiator and the responder—connects and begins to set up the VPN. The initiator is the peer that starts the phase 1 negotiation, while the responder is the peer that responds to the initiator request.

When the peers first connect, the channel is not secure. An attacker in the middle could intercept unencrypted keys. Neither peer has a strong guarantee of the other peer's identity, so how can they exchange sensitive private keys? They can't. First, both peers create a secure tunnel. Then, they use this secure tunnel to negotiate the real keys for the tunnel later.

DO NOT REPRINT**© FORTINET**

Phase 1—How it Works

1. Authenticate peers
 - PSK or digital signature
 - XAuth
2. Negotiate one bidirectional SA (called IKE SA)
 - In IKE v1, two possible ways:
 - Main mode
 - Aggressive mode
 - Not the same as IPsec SA
 - Encrypted tunnel for Diffie-Hellman (DH)

Bidirectional SA: same key to encrypt the outgoing traffic and decrypt the incoming traffic



3. DH exchange for secret keys



Now you'll examine how phase 1 works.

The purpose of phase 1 is to authenticate peers and set up a secure channel for negotiating the phase 2 SAs (or IPsec SAs) that are later used to encrypt and decrypt traffic between the peers. To establish this secure channel, the peers negotiate a phase 1 SA. This SA is called the IKE SA and is bidirectional because it uses the same session key for both inbound and outbound.

To authenticate each other, the peers use two methods: pre-shared key or digital signature. You can also enable an additional authentication method, XAuth, to enhance authentication.

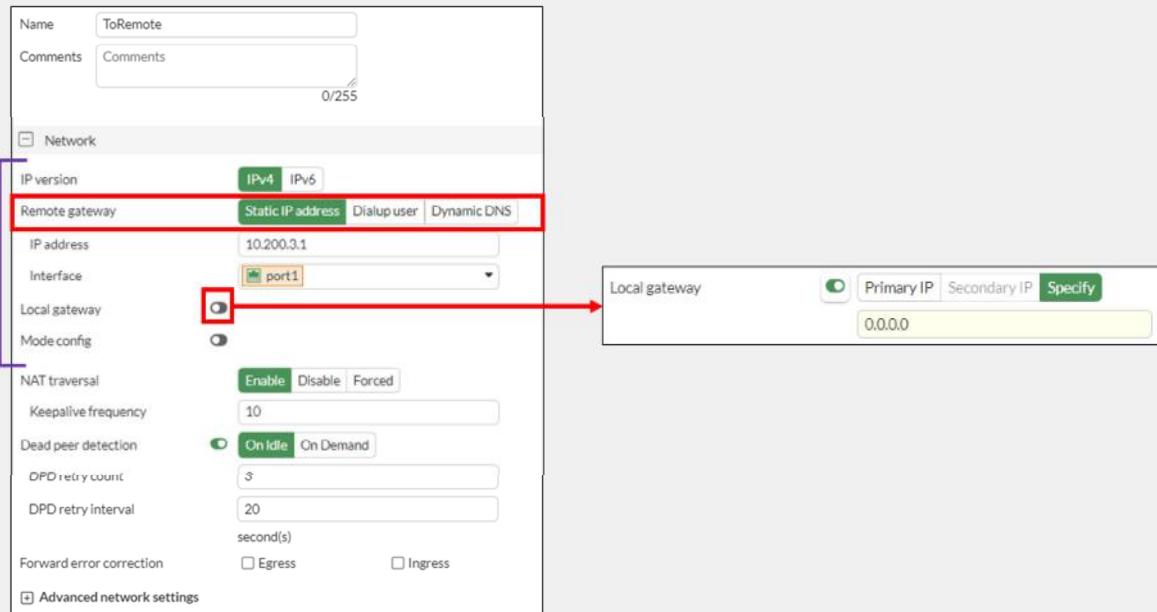
In IKEv1, there are two possible modes in which the IKE SA negotiation can take place: main, and aggressive mode. Settings on both ends must agree; otherwise, phase 1 negotiation fails and both IPsec peers are not able to establish a secure channel.

At the end of phase 1, the negotiated IKE SA is used to negotiate the DH keys that are used in phase 2. DH uses the public key (that both ends know) plus a mathematical factor called a nonce, in order to generate a common private key. With DH, even if an attacker can listen to the messages containing the public keys, they cannot determine the secret key.

DO NOT REPRINT

© FORTINET

Phase 1—Network



© Fortinet Inc. All Rights Reserved. 21

Phase 1 configuration is broken down on the GUI into four sections: **Network**, **Authentication**, **Phase 1 Proposal**, and **XAUTH**. You will learn about the settings available on each section. You will learn about some of these settings in more detail on separate slides.

The section shown on this slide corresponds to the **Network** settings. The section includes the settings related to the connectivity of the IPsec tunnel:

- **IP Version:** select the IP version to use for the IPsec tunnel. Note that this defines only the IP version of the outer layer of the tunnel (after encapsulation). The packets being encapsulated (protected traffic) can be IPv4 or IPv6, and their IP version is defined in the phase 2 selectors.
- **Remote Gateway:** defines the type of the remote gateway. There are three types: **Static IP Address**, **Dialup User**, and **Dynamic DNS**. You will learn more about these types later in this lesson.
- **IP Address:** the IP address of the remote gateway. This field appears only when you select **Static IP Address** as **Remote Gateway**.
- **Interface:** refers to the interface where the IPsec tunnel terminates on the local FortiGate. Usually, this is the interface connected to the internet or the WAN. You need to make sure there is an active route to the remote gateway through this interface, otherwise the tunnel won't come up.
- **Local Gateway:** enable this setting when the interface where the tunnel terminates has multiple addresses assigned, and you want to specify which address to use for the tunnel. When you enable this setting, you see three options: **Primary IP**, **Secondary IP**, and **Specify**. Select **Specify** if you want to use an IP address different from the primary or secondary IP address.
- **Mode Config:** Enables automatic configuration through IKE. FortiGate acts as an *IKE mode config client* when you enable **Mode Config** and you set **Remote Gateway** to either **Static IP address** or **Dynamic DNS**. If you set **Remote Gateway** to **Dialup User**, FortiGate acts as an *IKE mode config server*, and more configuration options appear on the GUI. You will learn more about **Mode Config** in this lesson.

DO NOT REPRINT

© FORTINET

Phase 1—Network (Contd)

The screenshot shows the 'Network' configuration page for a tunnel named 'ToRemote'. The 'Advanced network settings' section is highlighted with a purple box and a red arrow points from it to a detailed view of those settings on the right.

Network Configuration Fields:

- Name: ToRemote
- Comments: Comments
0/255
- IP version: IPv4 (selected)
- Remote gateway: Static IP address: 10.200.3.1; Interface: port1
- Local gateway: (disabled)
- Mode config: (disabled)
- NAT traversal: (disabled)
- Keepalive frequency: 10
- Dead peer detection: On Idle (selected)
- DPD retry count: 3
- DPD retry interval: 20 second(s)
- Forward error correction: Egress (unchecked), Ingress (unchecked)

Advanced network settings (highlighted):

- Add route: Enable (checked)
- Auto discovery sender: Enable (checked)
- Auto discovery receiver: Enable (checked)
- Auto discovery forwarder: Enable (checked)
- Exchange interface IP: Enable (checked)
- Device creation: Enable (checked)
- Aggregate member: Enable (checked)

Fortinet Inc. All Rights Reserved. 22

The following are the other options available on the GUI in the **Network** section:

- **NAT Traversal:** The option controls the behavior for NAT traversal. You will learn more about NAT traversal later in this lesson.
- **Keepalive Frequency:** When you enable NAT traversal, FortiGate sends keepalive probes at the configured frequency.
- **Dead Peer Detection:** Use dead peer detection (DPD) to detect dead tunnels. There are three DPD modes. **On Demand** is the default mode. You will learn more about DPD later in this lesson.
- **Forward Error Correction:** Forward error correction (FEC) is a technique that you can use to reduce the number of retransmissions in IPsec tunnels established over noisy links, at the expense of using more bandwidth. You can enable FEC on egress and ingress, and it is only supported when you disable IPsec hardware offloading. You will learn more about IPsec hardware offloading later in this lesson.
- **Advanced:**
 - **Add route:** Disable this setting if you are using a dynamic routing protocol over IPsec and do not want FortiGate to automatically add static routes.
 - **Auto discovery sender:** Enable this setting on a hub if you want the hub to facilitate ADVPN shortcut negotiation for spokes. When enabled, the hub sends a shortcut offer to the spoke to indicate that it can establish a shortcut to the remote spoke.
 - **Auto discovery receiver:** Enable this setting on a spoke if you want the spoke to negotiate an ADVPN shortcut.
 - **Exchange interface IP:** Enable this setting to allow the exchange of IPsec interface IP addresses. This allows a point-to-multipoint connection between the hub and spokes..
 - **Device creation:** Enable this setting to instruct FortiOS to create an interface for every dial-up client. To increase performance, disable this setting in dial-up servers with many dial-up clients.
 - **Aggregate member:** FortiGate allows you to aggregate multiple IPsec tunnels into a single interface. Enable this option if you want the tunnel to become an aggregate member.

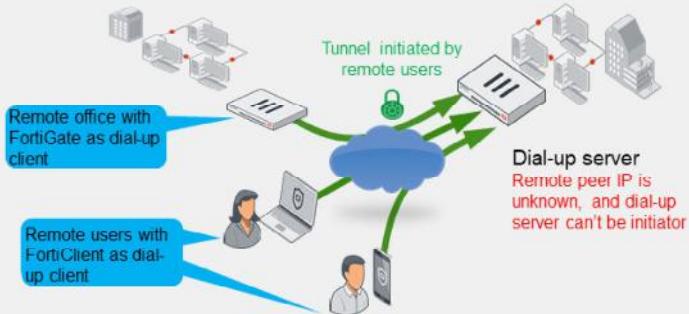
DO NOT REPRINT

© FORTINET

Phase 1—Network—Remote Gateway

Dial-up user

- Two roles: dial-up server and client
- Dial-up server doesn't know client address
 - Dial-up client is always the initiator
- VPN peers:
 - FortiGate to FortiClient (or third-party client)
 - FortiGate to FortiGate (or third-party gateway)



© Fortinet Inc. All Rights Reserved. 23

You have three options when configuring the remote gateway type of your VPN: **Dialup User**, **Static IP Address**, and **Dynamic DNS**.

Use **Dialup User** when the remote peer IP address is unknown. The remote peer whose IP address is unknown acts as the dial-up client, and this is often the case for branch offices and mobile VPN clients that use dynamic IP addresses, and no dynamic DNS. The dial-up client must know the IP address or FQDN of the remote gateway, which acts as the dial-up server. Because the dial-up server doesn't know the remote peer address, only the dial-up client can initiate the VPN tunnel.

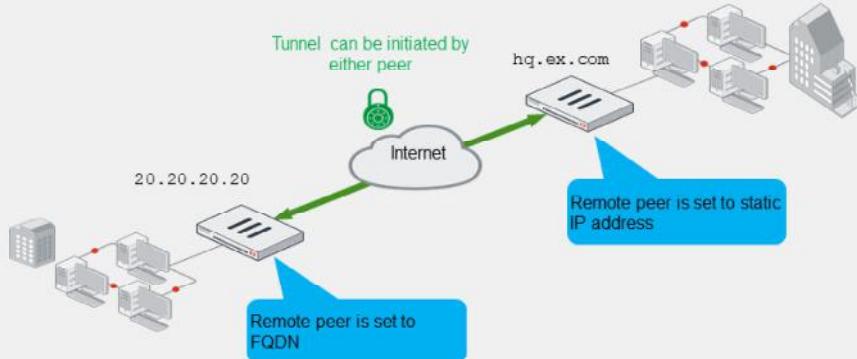
Usually, dial-up clients are remote and mobile employees with FortiClient on their computer or handheld devices. You can also have a FortiGate device acting as a dial-up client for a remote office. You can use one dial-up server configuration on FortiGate for multiple IPsec tunnels from many remote offices or users.

DO NOT REPRINT
© FORTINET

Phase 1—Network—Remote Gateway (Contd)

Static IP address/dynamic DNS

- Dynamic DNS uses FQDN
- The address of the remote peer is known
 - Local peer can be initiator or responder
- VPN peers:
 - FortiGate to FortiGate (or third-party gateway)



Use **Static IP Address** or **Dynamic DNS** when you know the remote peer address. If you select **Static IP Address**, then you must provide an IP address. If you select **Dynamic DNS**, then you must provide a fully qualified domain name (FQDN), and make sure FortiGate can resolve that FQDN. When both peers know the remote peer address, that is, the remote gateway on both peers is set to **Static IP Address** or **Dynamic DNS**, then any peer can initiate the VPN tunnel.

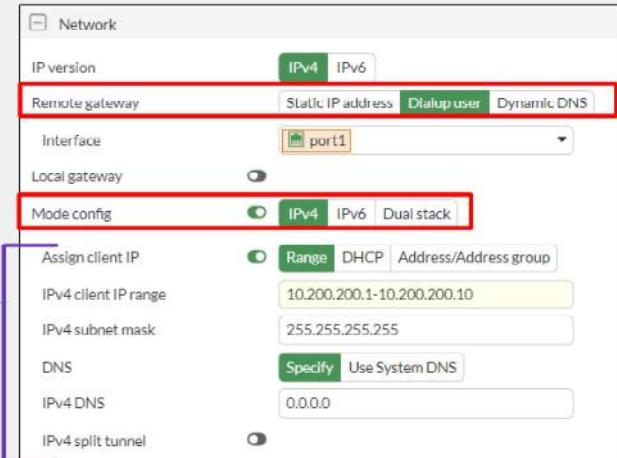
Note that in a dial-up setup, the dial-up client is just a VPN peer with the remote gateway set to **static IP address** or **dynamic DNS**. When setting your VPN, you can combine different types of remote gateways. For obvious reasons, a tunnel in which both peers have the remote gateway set to **Dialup user** won't work.

DO NOT REPRINT
© FORTINET

Phase 1—Network—IKE Mode Config

- Like DHCP, automatically configures VPN clients' virtual network settings
- By default, FortiClient VPNs use it to retrieve their VPN IP address settings from FortiGate
- You must enable **Mode Config** on both peers

IKE mode config settings are only displayed if Remote Gateway is set to Dialup User



IKE Mode Config is similar to DHCP because a server assigns network settings such as IP address, netmask, and DNS servers, to clients. This assignment takes place over IKE messages.

When you enable **Mode Config** on a FortiGate device acting as dial-up server, it pushes network settings to dial-up clients. The dial-up clients are usually FortiClient peers, but they can also be FortiGate peers.

For IKE mode config to work, you must enable the feature on both peers. On FortiClient, **Mode Config** is enabled by default, but on FortiGate, you must manually enable it.

Note that the IKE **Mode Config** settings, are displayed on the GUI only when you set **Remote Gateway** to **Dialup User**. On the FortiGate device acting as dial-up client, you can select **Mode Config** on the GUI, but the additional settings are not displayed.

DO NOT REPRINT
© FORTINET

Phase 1—Network—NAT Traversal (NAT-T)

- ESP can't support NAT because it has no port numbers
- If **NAT Traversal** is set to **Enable**, it detects whether NAT devices exist on the path
 - If yes, both ESP and IKE use UDP port 4500
 - Recommended if the initiator or responder is behind NAT
- If **NAT Traversal** is set to **Forced**:
 - ESP and IKE always use UDP port 4500, even when there are no NAT devices on the path
- Keepalive probes are sent frequently to keep the connection across the routers active



The ESP protocol usually has problems crossing devices that are performing NAT. One of the reasons is that ESP does not use port numbers, like TCP and UDP do, to differentiate one tunnel from another.

To solve this, NAT transversal (NAT-T) was added to the IPsec specifications. When NAT-T is enabled on both ends, peers can detect any NAT device along the path. If NAT is found, then the following occurs on both peers:

- IKE negotiation switches to using UDP port 4500.
- ESP packets are encapsulated in UDP port 4500.

So, if you have two FortiGate devices that are behind, for example, an ISP modem that performs NAT, you will probably need to enable this setting.

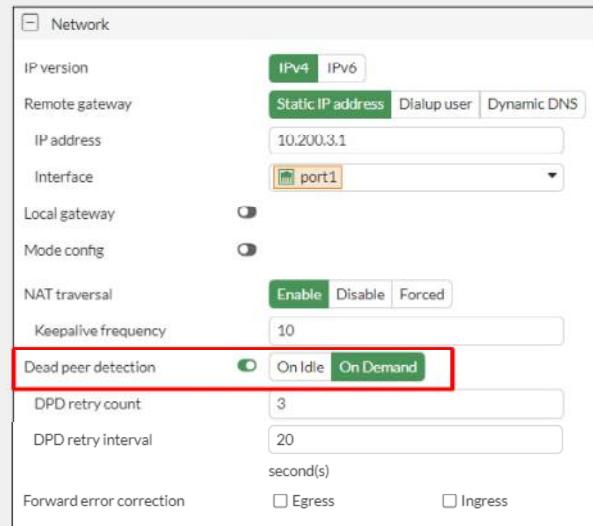
When you set the **NAT Traversal** setting to **Forced**, UDP port 4500 is always used, even when there is no NAT device along the path.

When you enable NAT-T, the **Keepalive Frequency** option shows the interval (in seconds) at which FortiGate sends keepalive probes. You need NAT-T when there is one or more routers along the path performing NAT. The purpose of the keepalive probes is to keep the IPsec connection active across those routers along the path.

DO NOT REPRINT
© FORTINET

Phase 1—Network—Dead Peer Detection (DPD)

- Mechanism to detect a dead tunnel
- Useful in redundant VPNs, where multiple paths are available
- Three modes:
 - **On Demand:** DPD probes are sent when there is no inbound traffic
 - **On Idle:** DPD probes are sent when there is no traffic
 - **Disabled:** only reply to DPD probes—don't send probes



The screenshot shows the 'Network' configuration page in FortiOS. Under the 'Dead peer detection' section, two radio buttons are present: 'On Idle' and 'On Demand'. The 'On Demand' button is highlighted with a red border, indicating it is the selected mode.

Setting	Value
IP version	IPv4
Remote gateway	Static IP address
IP address	10.200.3.1
Interface	port1
Local gateway	(checkbox)
Mode config	(checkbox)
NAT traversal	Enable
Keepalive frequency	10
Dead peer detection	<input checked="" type="radio"/> On Idle <input type="radio"/> On Demand
DPD retry count	3
DPD retry interval	20 second(s)
Forward error correction	<input type="checkbox"/> Egress <input type="checkbox"/> Ingress



After the peers negotiate the IPsec SAs of a tunnel and, therefore, the tunnel is considered up, the peers usually don't negotiate another IPsec SA until it expires. In most cases, the IPsec SA expires every few hours. This means that if there is a network disruption along the path of the tunnel before the IPsec SA expires, the peers will continue to send traffic through the tunnel even though the communication between the sites is disrupted.

When you enable DPD, DPD probes are sent to detect a failed (or dead) tunnel and bring it down before its IPsec SAs expire. This failure detection mechanism is very useful when you have redundant paths to the same destination, and you want to fail over to a backup connection when the primary connection fails to keep the connectivity between the sites up.

FortiGate supports three DPD modes:

- **On Demand:** FortiGate sends DPD probes if there is only outbound traffic through the tunnel, but no inbound. Because network applications are usually bidirectional, observing only traffic on the outbound direction could be an indication of a network failure.
- **On Idle:** FortiGate sends DPD probes when no traffic is observed in the tunnel. An idle tunnel does not necessarily mean the tunnel is dead. Avoid this mode if you have many tunnels, because the overhead introduced by DPD can be very resource intensive.
- **Disabled:** FortiGate replies only to DPD probes received. FortiGate never sends DPD probes to the remote peer and therefore cannot detect a dead tunnel.

The default DPD mode is **On Demand**. In terms of scalability, **On Demand** is a better option than **On Idle**.

DO NOT REPRINT
© FORTINET

Phase 1—Authentication

The screenshot shows the FortiOS 7.6 interface for configuring Phase 1 authentication. The main window displays the following settings:

- Method:** Pre-shared Key (selected)
- Pre-shared key:** A masked password entry field.
- IKE:** Version 1 (selected)
- Mode:** Aggressive (selected)

A red arrow points from the 'Accepted peer ID' dropdown in the main configuration window to the 'Any peer ID' option in the expanded dropdown menu. The expanded menu also includes 'Main (ID protection)' and 'Specific peer ID'.

Now, you will learn about the **Authentication** section in phase 1 configuration:

- Method:** FortiGate supports two authentication methods: **Pre-shared Key** and **Signature**. When you select **Pre-shared Key**, you must configure both peers with the same pre-shared key. When you select **Signature**, phase 1 authentication is based on digital certificate signatures. Under this method, the digital signature on one peer is validated by the presence of the CA certificate installed on the other peer. That is, on the local peer, you need to install both the local peer's certificate and the CA certificate that issued the remote peer certificate.
- Version:** allows you to select the IKE version to use. When selecting version **2**, aggressive and main modes disappear because they don't apply to IKEv2.
- Mode:** refers to the IKEv1 mode. Two options are available: **Aggressive** and **Main (ID protection)**. You will learn more about these modes in this lesson.

DO NOT REPRINT**© FORTINET**

Phase 1—Authentication—Modes

Aggressive

- Not as secure as main mode
- Faster negotiation (three packets exchanged)
- Required when peer ID check is needed

Main

- More secure
- Slower negotiation (six packets exchanged)
- Often used when peer ID check is not needed



IKE supports two different negotiation modes: main and aggressive. Which one should you use?

To answer that question, we can analyze three categories: security, performance, and deployment.

Security wise, main mode is considered more secure because the pre-shared key hash is exchanged encrypted, whereas in aggressive mode, the hash is exchanged unencrypted. Although the attacker would still have to guess the cleartext pre-shared key for the attack to be successful, the fact that the pre-shared key hash has been encrypted in main mode reduces considerably the chances of a successful attack.

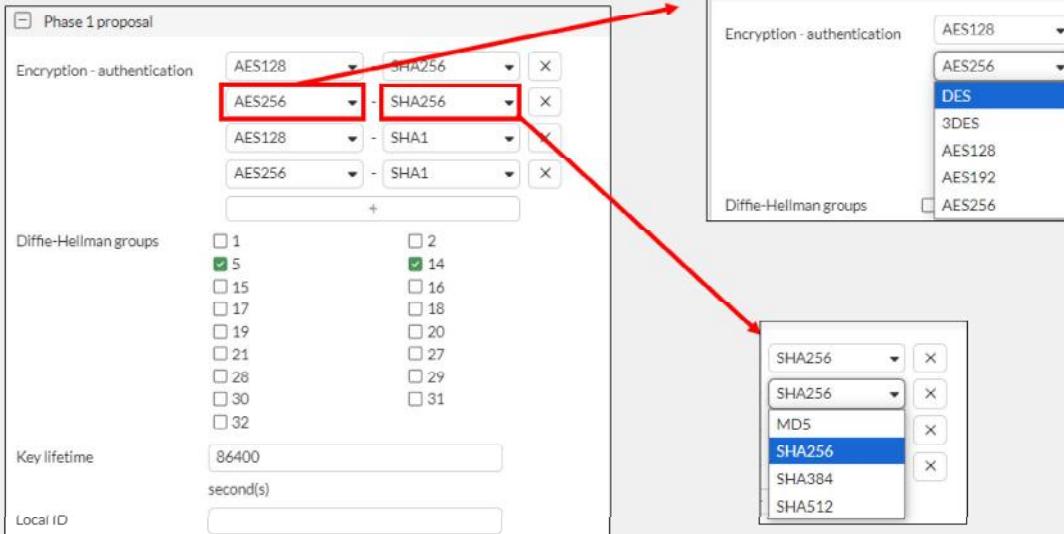
In terms of performance, aggressive mode may be a better option. This is because the negotiation is completed after only three packets are exchanged, whereas in main mode, six packets are exchanged. For this reason, you may want to use aggressive mode when a great number of tunnels terminate on the same FortiGate device, and performance is a concern.

Another use case for aggressive mode, is when there is more than one dial-up tunnel terminating on the same FortiGate IP address, and the remote peer is authenticated using a peer ID because its IP address is dynamic. Because peer ID information is sent in the first packet in an aggressive mode negotiation, then FortiGate can match the remote peer with the correct dial-up tunnel. The latter is not possible in main mode because the peer ID information is sent in the last packet, and after the tunnel has been identified.

When both peers know each other's IP address or FQDN, you may want to use main mode to take advantage of its more secure negotiation. In this case, FortiGate can identify the remote peer by its IP address and, as a result, associate it with the correct IPsec tunnel.

DO NOT REPRINT
© FORTINET

Phase 1—Phase 1 Proposal



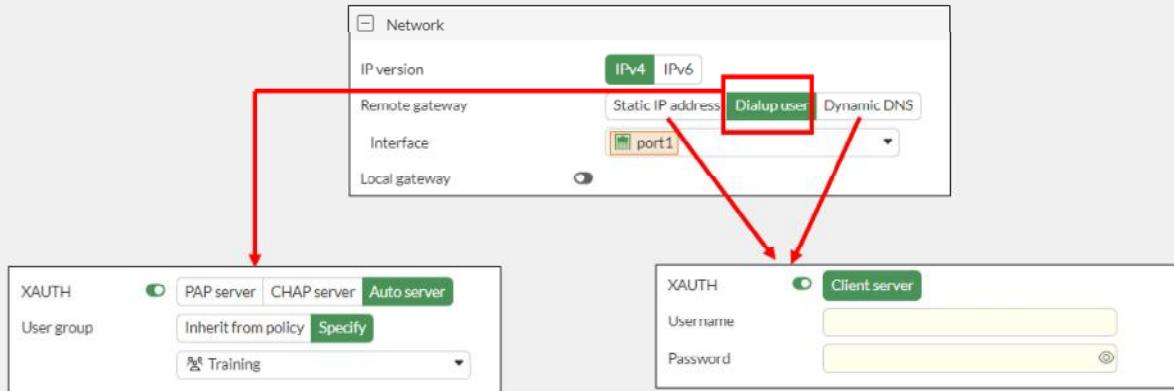
Now, you will learn about the **Phase 1 Proposal** section of phase 1 configuration. This section allows you to enable the different proposals that FortiGate supports when negotiating the IKE SA (or phase 1 SA). You can combine different parameters to suit your security needs. You must at least configure one combination of encryption and authentication algorithms, or several.

- **Encryption:** select the algorithm to use for encrypting and decrypting the data.
- **Authentication:** select the authentication algorithm to use for verifying the integrity and authenticity of the data.
- **Diffie-Hellman Groups:** The Diffie-Hellman (DH) algorithm is used during IKE SA negotiation. The use of DH in phase 1 is mandatory and can't be disabled. You must select at least one DH group. The higher the DH group number, the more secure the phase 1 negotiation is. However, a higher DH group number also results in a longer compute time.
- **Key Lifetime:** defines the lifetime of the IKE SA. At the end of the lifetime, a new IKE SA is negotiated.
- **Local ID:** if the peer accepts a specific peer ID, type that same peer ID in this field.

DO NOT REPRINT
© FORTINET

Phase 1—Extended Authentication (XAuth)

- XAuth adds stronger authentication: username + password
- You can authorize all users who belong to a specific user group or inherit it from the matching policy



Phase 1 supports two types of authentication: pre-shared keys and digital signatures. The XAuth extension, sometimes called phase 1.5, forces remote users to authenticate additionally with their credentials (username and password). So, additional authentication packets are exchanged if you enable it. What is the benefit? Stronger authentication.

When you set **Remote Gateway** to **Dialup User**, FortiGate acts as the authentication server. The **XAUTH** section shows the authentication server type options: **PAP Server**, **CHAP Server**, and **Auto Server**. In the example shown on this slide, **Auto Server** is selected, which means that FortiGate automatically detects the authentication protocol used by the client.

After you select the authentication server type, you configure how user group matching is performed. There are two options: **Inherit from policy** and **Choose**. The latter is used in the example on this slide, and allows you to select one of the user groups available on FortiGate. Note that, when you select **Choose**, you must configure a separate dial-up VPN for every group of users that require a different network access policy.

The other way to authenticate VPN users with XAuth is by selecting **Inherit from policy**. When you select this option, FortiGate authenticates users based on their matching IPsec policy and, as a result, the configuration for controlling network access is simpler. That is, you control network access by configuring multiple policies for different user groups, instead of configuring multiple tunnels for different user groups. The **Inherit from policy** option follows a similar authentication approach used for SSL VPN remote users that you learned in the SSL VPN lesson.

When **Remote Gateway** is set to **Static IP Address** or **Dynamic DNS**, FortiGate acts as the client, and the **XAUTH** section shows the **Client** option as **Type**. You can then set the credentials that FortiGate uses to authenticate against the remote peer through XAuth.

DO NOT REPRINT**© FORTINET**

Phase 2—How it Works

- Negotiates two unidirectional IPsec SAs for ESP
 - Protected by phase 1 IKE SA

Two unidirectional SAs: one key to encrypt the outgoing traffic and another one to decrypt the incoming traffic



- When IPsec SAs are about to expire, it renegotiates
 - Optionally, if **Perfect Forward Secrecy** is enabled, FortiGate uses DH to generate new keys each time phase 2 expires
- Each phase 1 can have multiple phase 2s
 - High security subnets can have stronger ESP



After phase 1 has established a secure channel to exchange data, phase 2 begins.

Phase 2 negotiates security parameters for two IPsec SAs over the secure channel established during phase 1. ESP uses IPsec SAs to encrypt and decrypt traffic exchanged between sites, with one outbound SA and one inbound SA. Additionally, authentication header (AH) uses two integrity keys to authenticate the source of the packets and verify data integrity. AH does not provide encryption.

Phase 2 does not end when ESP begins. Phase 2 periodically renegotiates IPsec SAs to maintain security. If you enable **Perfect Forward Secrecy**, each time phase 2 expires, FortiGate uses DH to recalculate new secret keys. In this way, new keys are not derived from older keys, making it much harder for an attacker to crack the tunnel.

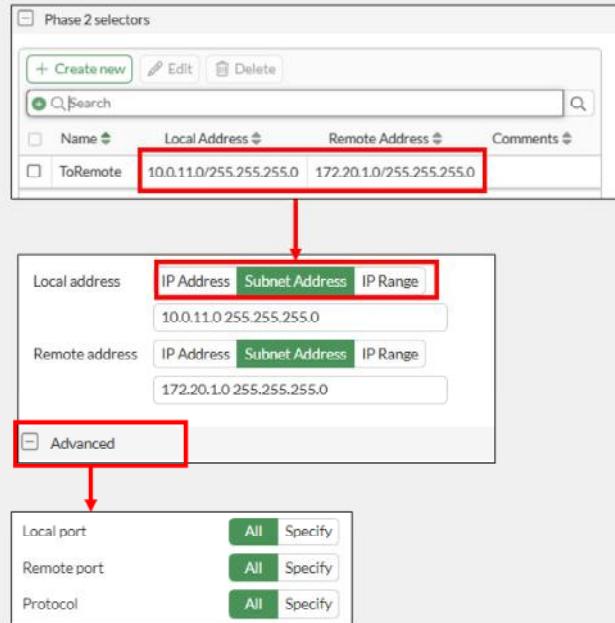
Each phase 1 can have multiple phase 2s. When would this happen? For example, you may want to use different encryption keys for each subnet whose traffic is crossing the tunnel. How does FortiGate select which phase 2 to use? By checking which phase 2 selector (or quick mode selector) matches the traffic.

DO NOT REPRINT

© FORTINET

Phase 2—Phase 2 Selectors

- Determines the encryption domain
 - You can configure multiple selectors for granular control
 - If traffic does not match a selector, it is dropped
 - In point-to-point VPNs, selectors must match
 - The source on one FortiGate is the destination setting on the other
- Select which selector to use using:
 - Local Address** and **Remote Address**
 - Protocol** number
 - Local Port** and **Remote Port**



© Fortinet Inc. All Rights Reserved. 33

In phase 2, you must define the encryption domain (or interesting traffic) of your IPsec tunnel. The encryption domain refers to the traffic that you want to protect with IPsec, and it is determined by your phase 2 selector configuration.

You can configure multiple selectors to have more granular control over traffic. When you configure a phase 2 selector, you specify the encryption domain by indicating the following network parameters:

- Local Address** and **Remote Address**: as seen in the example shown on this slide, you can define IPv4 or IPv6 addresses using different address scopes. When selecting **Named Address** or **Named IPv6 Address**, FortiGate allows you to select an IPv4 or IPv6 firewall address object, respectively, configured in the system.
- Protocol**: is in the **Advanced** section, and is set to **All** by default.
- Local Port** and **Remote Port**: are also shown in the **Advanced** section, and are set to **All** by default. This applies only to port-based traffic such as TCP or UDP. You will learn more about the **Advanced** section later in this lesson.

Note that after the traffic is accepted by a firewall policy, traffic is dropped before entering the IPsec tunnel if the traffic does not match any of the phase 2 selectors configured. For this reason, usually, it's more intuitive to filter traffic with firewall policies. So, if you don't want to use phase 2 selector filtering, you can just create one phase 2 selector with both the local and remote addresses set to any subnet, like in the example shown on this slide, and then use firewall policies to control which traffic is accepted on the IPsec tunnel.

In addition, the phase 2 selector network parameters on both peers must match if the tunnel is point-to-point, that is, when the remote gateway is *not* set to dial-up user.

DO NOT REPRINT
© FORTINET

Phase 2—Phase 2 Proposal

- Determines the encryption algorithms
 - You can configure multiple proposals for added flexibility
 - Impacts performance and hardware offloading
- You can enable replay detection to protect against ESP replay attacks
 - Local setting

Encryption and authentication algorithms for IPsec encryption

The screenshot shows the 'Encryption - authentication' section of the configuration. The 'Advanced' checkbox is checked. The 'Encryption - authentication' dropdown is open, showing options: AES128, NULL, DES, 3DES, AES192, AES256, and CHACHA20POLY1305. The 'AES128' option is selected. Below the dropdown are checkboxes for 'Replay detection' (Enable) and 'Perfect forward secrecy (PFS)' (Enable). There is also a list of Diffie-Hellman groups (1, 14, 15, 16, 17, 18, 19, 20, 21, 22, 27, 28, 29, 30, 31, 32), with group 14 selected. The 'Protocol' section includes 'Local port' (All, Specify), 'Remote port' (All, Specify), and 'Protocol' (All, Specify). 'Auto-negotiate' is enabled. 'Autokey keep alive' is enabled. 'Key lifetime' is set to 'Seconds Kilobytes Both' with a value of 43200.

© Fortinet Inc. All Rights Reserved. 34

For every phase 2 selector, you need to configure one or more phase 2 proposals. A phase 2 proposal defines the algorithms supported by the peer for encrypting and decrypting the data over the tunnel. You can configure multiple proposals to offer more options to the remote peer when negotiating the IPsec SAs.

Like in phase 1, you need to select a combination of encryption and authentication algorithms. Some algorithms are considered more secure than others, so make sure to select the algorithms that conform with your security policy. However, note that the selection of the algorithms has a direct impact on FortiGate IPsec performance. For example, **3DES** is known to be a much more resource-intensive encryption algorithm than **DES** and **AES**, which means that your IPsec throughput could be negatively impacted if you select **3DES** as the encryption algorithm. Also, note that if you select **NULL** as the encryption algorithm, traffic is not encrypted.

In addition, some encryption algorithms, such as **CHACHA20POLY1305**, are not supported for hardware offload. That is, if you have a FortiGate device that contains network processor (NP) units, you can achieve higher IPsec performance if you select an algorithm that is supported for IPsec offload by your NP unit model, such as AES or DES. For a list of supported encryption algorithms for IPsec hardware offloading, refer to <https://docs.fortinet.com>.

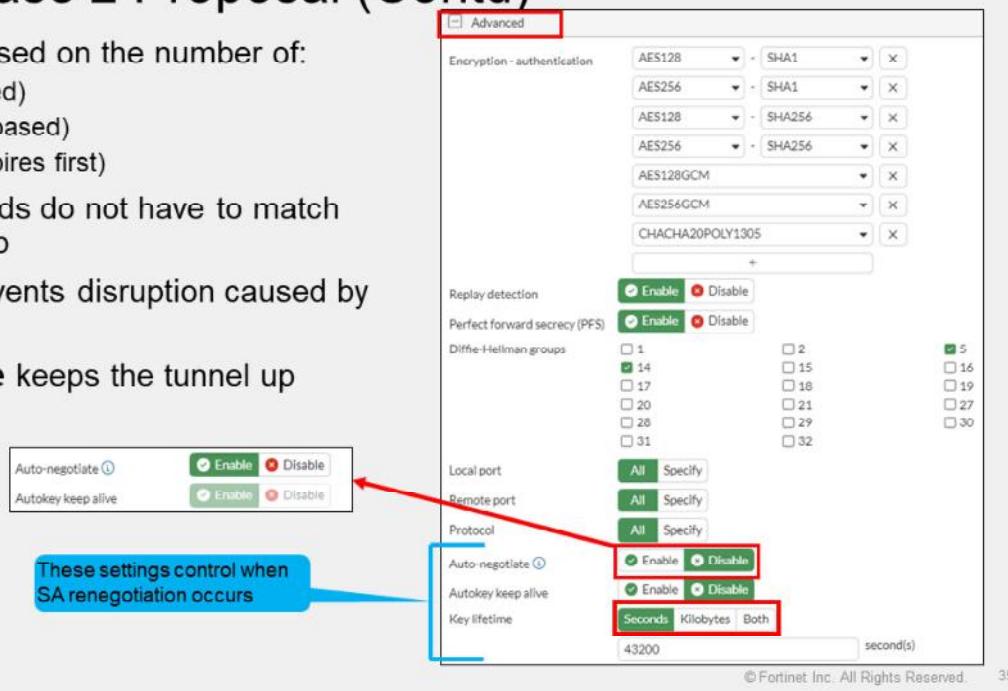
When configuring the phase 2 proposal, you can select **Enable Replay Detection** to detect antireplay attacks on ESP packets. Note that this is a local setting and, therefore, it is not included as part of the proposals presented by the peer during phase 2 negotiation.

Also, if you enable **Perfect Forward Secrecy**, FortiGate uses DH to enhance security during the negotiation of IPsec SAs.

DO NOT REPRINT
© FORTINET

Phase 2—Phase 2 Proposal (Contd)

- IPsec SA expires based on the number of:
 - **Seconds** (time-based)
 - **Kilobytes** (volume-based)
 - **Both** (whichever expires first)
- Key lifetime thresholds do not have to match for tunnel to come up
- **Auto-negotiate** prevents disruption caused by SA renegotiation
- **Autokey Keep Alive** keeps the tunnel up



IPsec SAs are periodically renegotiated to improve security, but when does that happen? It depends on the key lifetime settings configured on the phase 2 proposal.

The expiration of an IPsec SA is determined by the lifetime type and threshold configured. By default, **Key Lifetime** is set to **Seconds** (time-based). This means that when the SA duration reaches the number of seconds set as **Seconds**, the SA is considered expired. You can also set the key lifetime to **Kilobytes** (volume-based), upon which the SA expires after the amount of traffic encrypted and decrypted using that SA reaches the threshold set. Alternatively, you can select **Both** as the key lifetime type, upon which FortiGate tracks both the duration of the SA and the amount of traffic. Then, when any of the two thresholds is reached, the SA is considered expired. Note that the key lifetime thresholds do not have to match for the tunnel to come up. When thresholds are different, the peers agree on using the lowest threshold value offered between the two.

When IPsec SAs expire, FortiGate needs to negotiate new SAs to continue sending and receiving traffic over the IPsec tunnel. Technically, FortiGate deletes the expired SAs from the respective phase 2 selectors, and installs new ones. If IPsec SA renegotiation takes too much time, then FortiGate might drop interesting traffic because of the absence of active SAs. To prevent this, you can enable **Auto-negotiate**. When you do this, FortiGate not only negotiates new SAs before the current SAs expire, but it also starts using the new SAs right away. The latter prevents traffic disruption by IPsec SA renegotiation.

Another benefit of enabling **Auto-negotiate** is that the tunnel comes up and stays up automatically, even when there is no interesting traffic. When you enable **Autokey Keep Alive** and keep **Auto-negotiate** disabled, the tunnel does not come up automatically unless there is interesting traffic. However, after the tunnel is up, it stays that way because FortiGate periodically sends keep alive packets over the tunnel. Note that when you enable **Auto-negotiate**, **Autokey Keep Alive** is implicitly enabled.

DO NOT REPRINT

© FORTINET

IPsec Hardware Offloading

- On some FortiGate models, you can offload IPsec encryption and decryption to hardware
- Hardware offloading capabilities and supported algorithms vary by processor type and model
- By default, offloading is enabled for supported algorithms
 - You can manually disable offloading:

```
config vpn ipsec phasel-interface
    edit ToRemote
        set npu-offload disable
    next
end
```



On some FortiGate models, you can offload the encryption and decryption of IPsec traffic to hardware. The algorithms that are supported depend on the NP unit model present on FortiGate. For a list of supported encryption algorithms for IPsec hardware offloading, refer to <https://docs.fortinet.com>.

By default, hardware offloading is enabled for the supported algorithms. This slide shows the commands you can use to disable hardware offloading per tunnel, if necessary.

DO NOT REPRINT

© FORTINET

Lesson Progress



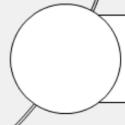
IPsec Basics



IPsec Configuration



Routing and Firewall Policies



Monitoring



© Fortinet Inc. All Rights Reserved. 37

Good job! You now understand IPsec configuration.

Now, you will learn about routing and firewall policies for IPsec traffic.

DO NOT REPRINT

© FORTINET

Routing and Firewall Policies

Objectives

- Understand route-based IPsec VPNs
- Configure firewall policies for IPsec traffic
- Configure a redundant VPN between two FortiGate devices



© Fortinet Inc. All Rights Reserved. 38

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

By demonstrating competence in routing and firewall policies for IPsec VPNs, you will be able to set up appropriate routing and firewall policies on FortiGate, and add redundancy to your IPsec VPN deployment.

DO NOT REPRINT**© FORTINET**

Route-Based IPsec VPNs

- Types of IPsec VPNs:
 - Route-based
 - Virtual interface for each VPN: VPN matching based on routing
 - Policy-based
 - Legacy: VPN matching based on policy. Not recommended.
- Route-based VPNs benefits:
 - Simpler operation and configuration
 - Redundancy
 - Support for:
 - L2TP-over-IPsec
 - GRE-over-IPsec
 - Dynamic routing protocols



FortiGate supports two types of IPsec VPNs: route-based and policy-based. Policy-based is a legacy IPsec VPN that is supported only for backward compatibility reasons, and its use *is not recommended* for new deployments. Unless otherwise stated, all IPsec VPN references in this lesson are for route-based IPsec VPNs.

In a route-based IPsec VPN, FortiGate automatically adds a virtual interface with the VPN name. This means that not only can you configure routing and firewall policies for IPsec traffic in the same way you do for non-IPsec traffic, but you also can leverage the presence of multiple connections to the same destination to achieve redundancy.

Another benefit of route-based IPsec VPNs is that you can deploy variations of IPsec VPNs such as L2TP-over-IPsec and GRE-over-IPsec. In addition, you can also enable dynamic routing protocols for scalability purposes and best path selection.

DO NOT REPRINT

© FORTINET

Routes for IPsec VPNs

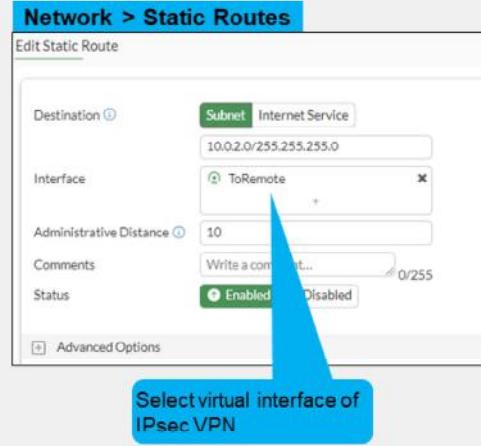
Dial-up user

```
config vpn ipsec phasel-interface
    edit "Dialup"
        set add-route enable | disable
    next
end
```

- **add-route is enabled (default)**
 - No need to configure static routes
 - Static routes are added after phase 2 is up
 - The destination is the local network presented by the dial-up client during phase 2 negotiation
 - The default route distance is 15
 - Static routes are deleted after phase 2 is down
- **add-route is disabled**
 - Useful when dynamic routing protocol is used
 - Dynamic routing protocol takes care of routing updates

Static IP address / dynamic DNS

- Static routes are needed



Although you can use dynamic routing protocols for IPsec VPNs, this lesson covers only the use of static routes.

The routing configuration needed for your IPsec VPN depends on the type of remote gateway configured. When you set the remote gateway to **Dialup User** and enable `add-route`, FortiGate automatically adds a static route for the local network presented by the remote peer during phase 2 negotiation. In addition, the route is added to the routing table only after phase 2 is up. If phase 2 goes down, the static route is removed from the routing table.

When you set the remote gateway to **Dialup User** and disable `add-route`, FortiGate does not add static routes automatically. In this case, a dynamic routing protocol is used between the remote peers to exchange routing information.

When the remote gateway is set to **Static IP Address** or **Dynamic DNS**, you must configure static routes. When you configure a static route, you select the virtual interface of the IPsec tunnel as the outgoing interface.

DO NOT REPRINT

© FORTINET

Firewall Policies for IPsec VPNs

- At least one firewall policy is needed for a tunnel to come up
- Usually two firewall policies are configured for every tunnel

The screenshot shows two side-by-side 'Policy & Objects > Firewall Policy' configuration windows.

Left Window (Remote_out):

- Name: Remote_out
- Schedule: always
- Action: ACCEPT DENY
- Incoming Interface: port3
- Outgoing Interface: ToRemote
- Source & Destination (Show logic):
 - Source: LOCAL_SUBNET
 - Destination: REMOTE_SUBNET
 - Service: ALL
- Firewall/Network Options: NAT (disabled)

Right Window (Remote_in):

- Name: Remote_in
- Schedule: always
- Action: ACCEPT DENY
- Incoming Interface: ToRemote
- Outgoing Interface: port3
- Source & Destination (Show logic):
 - Source: REMOTE_SUBNET
 - Destination: LOCAL_SUBNET
 - Service: ALL
- Firewall/Network Options: NAT (disabled)

Annotations on the interface:

- A callout points to the 'Incoming Interface' field in both windows with the text: "Virtual interface matches phase 1 name".
- A large callout at the bottom points to the 'Source & Destination' section with the text: "Allow and inspect the traffic coming from/going to the IPsec virtual interface".

© Fortinet Inc. All Rights Reserved. 41

You must configure at least one firewall policy that accepts traffic on your IPsec tunnel. Otherwise, the tunnel will not come up.

When you configure firewall policies for non-IPsec traffic, the policy determines the direction of the traffic that initiates sessions. The same applies to IPsec traffic. For this reason, you usually want to configure at least two firewall policies for your IPsec VPN: one incoming policy and one outgoing policy. The incoming policy allows traffic initiated from the remote site, while the outgoing policy allows traffic to be initiated from the local network.

Note that the policies are configured with the virtual tunnel interface (or phase 1 name) as the incoming or outgoing interface.

DO NOT REPRINT

© FORTINET

Redundant VPNs

- If the primary VPN tunnel fails, FortiGate then routes traffic through the backup VPN
- *Partially redundant*: one peer has two connections



- *Fully redundant*: both peers have two connections



How can you make your IPsec VPN deployment more resilient? Provide a second ISP connection to your site and configure two IPsec VPNs. If the primary IPsec VPN fails, another tunnel can be used instead.

There are two types of redundant VPNs:

- Partially redundant: on one peer (usually the hub, where a backup ISP is available if the main ISP is down), each VPN terminates on *different* physical ports. That way, FortiGate can use an alternative VPN. On the other peer, each VPN terminates on the *same* physical port—so the spoke is not fault tolerant.
- Fully-redundant: both peers terminate their VPNs on different physical ports, so they are both fault tolerant.

DO NOT REPRINT

© FORTINET

Redundant VPN Configuration

- Add one phase 1 configuration for each tunnel. You should enable DPD on both ends.
- Add at least one phase 2 definition for each phase 1
- Add one static route for each path
 - Use distance or priority to select primary routes over backup routes
 - Alternatively, use dynamic routing
- Configure firewall policies for each IPsec interface



So, how do you configure a partially or fully redundant VPN?

First, create one phase 1 for each path—one phase 1 for the primary VPN and one for the backup VPN. You should also enable DPD on both ends.

Second, create at least one phase 2 definition for each phase 1.

Third, you must add at least one static route for each VPN. Routes for the primary VPN must have a lower distance (or lower priority) than the backup. This causes FortiGate to use the primary VPN while it's available. If the primary VPN fails, then FortiGate automatically uses the backup route. Alternatively, you could use a dynamic routing protocol, such as OSPF or BGP.

Finally, configure firewall policies to allow traffic through both the primary and backup VPNs.

DO NOT REPRINT

© FORTINET

Lesson Progress



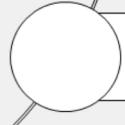
IPsec Basics



IPsec Configuration



Routing and Firewall Policies



Monitoring



© Fortinet Inc. All Rights Reserved.

44

Good job! You now understand routing and firewall policies for IPsec traffic.

Now, you will learn about monitoring IPsec VPNs and reviewing their logs.

DO NOT REPRINT

© FORTINET

Monitoring

Objectives

- Monitor IPsec VPNs and review logs
- Troubleshoot IPsec VPN issues

© Fortinet Inc. All Rights Reserved. 45

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

By demonstrating competence in monitoring and logs, you will be able to monitor IPsec VPN and investigate common issues.

DO NOT REPRINT

© FORTINET

IPsec VPN Status—IPsec Monitor Widget

- Monitor IPsec VPN tunnels
 - Display status and statistics
 - Bring up or bring down VPNs

Dashboard > Network > IPsec

Comments
Created
Phase 2 Protocols
Proxy Destination Ports
Proxy ID Destination
Proxy ID Source
Proxy Source Ports
Remote Port
Status
Timeout
Two-factor Authentication
XAUTH User

Apply Cancel

© Fortinet Inc. All Rights Reserved. 46

On the GUI dashboard, you can use the IPsec widget to monitor the status of your IPsec VPNs. The widget shows the phase 1 and phase 2 status of an IPsec VPN.

You can also bring up or bring down individual VPNs, and get additional details. When you bring up an IPsec VPN using the IPsec widget, you can choose between bringing up a particular phase 2 selector or all phase 2 selectors in that VPN. Because bringing up a phase 2 selector requires bringing up its phase 1 first, then bringing up a phase 2 selector results in its phase 1 also coming up.

To bring down the VPN, you can choose between bringing down a particular phase 2 selector, all selectors, or the entire tunnel. When you bring down the entire tunnel, you bring down all phase 2 selectors as well as the phase 1.

The **Name** column indicates the VPN status. The VPN is up when at least one of its phase 2 selectors is up. If all phase 2 selectors are down, the VPN status is also down. The **Phase 1** and **Phase 2 Selectors** columns indicate the status of phase 1 and phase 2 selectors, respectively.

The IPsec widget also displays the amount of data sent and received through the tunnel. When you right-click any of the columns, a menu opens with a list of all the columns available. You can enable additional columns to get further details about the IPsec tunnels.

In the example shown on this slide, the **ToRemote** VPN is up because at least one of its phase 2 selectors (**ToRemote**) is up.

DO NOT REPRINT

© FORTINET

Monitor IPsec Routes

- IPsec routes appear in the routing table after:
 - Phase 1 comes up, if the remote gateway is set to static IP address or dynamic DNS

Dashboard > Network > IPsec

Phase 1	Phase 2 Selectors
ToRemote	ToRemote ToRemote2

Phase 1 is up

Dashboard > Network > Static & Dynamic Routing

Network	Gateway IP	Interfaces	Distance
0.0.0.0/0	10.200.1.254	port1	10
10.0.1.0/24	0.0.0.0	port3	0
10.0.2.0/24		ToRemote	10

- Phase 2 comes up, if the remote gateway is set to dial-up user

Dashboard > Network > IPsec

Name	Remote Gateway	Peer ID
Dialup_0	10.9.15.30	

Phase 2 is up

Dashboard > Network > Static & Dynamic Routing

Network	Gateway IP	Interfaces	Distance
0.0.0.0/0	10.9.15.254	port1	10
10.0.2.0/24	10.9.15.30	Dialup	15

© Fortinet Inc. All Rights Reserved. 47

If you set the remote gateway to **Static IP Address** or **Dynamic DNS**, the static routes for these tunnels become active in the routing table after phase 1 comes up. Phase 1 negotiation is started automatically because automatic negotiation is enabled on phase 1 by default. This behavior allows FortiGate to match interesting traffic to the right tunnel. Moreover, if phase 2 is not up, traffic matching the static route triggers a phase 2 negotiation, which eventually results in the tunnel (or phase 2) to come up.

When you set the remote gateway to **Dialup User**, by default, a static route for the destination network is added after phase 2 comes up. The distance set for the static route is 15. If phase 2 goes down, the route is removed from the routing table.

DO NOT REPRINT

© FORTINET

IPsec Logs

The screenshot shows the FortiGate IPsec Log Details window. At the top, a message says "Phase 2 is up (tunnel is up)". A callout points to the log entry for "phase2-up". Another callout points to the "Log Details" pane, which shows "Phase 1 is DONE (up)" under the "Action" section.

Log & Report > System Events > VPN Events

Phase 2 is up (tunnel is up)

Double-click any log to get more details

Date/Time	Level	Action	Status	Message	VPN Tunnel
2024/09/13 06:24:16	Notice	negotiate	success	progress IPsec phase 2	ToRemote
2024/09/13 06:24:16	Notice	negotiate	success	negotiate IPsec phase 2	ToRemote
2024/09/13 06:24:16	Notice	negotiate	success	progress IPsec phase 2	ToRemote
2023/09/13 06:24:16	Notice	tunnel-up		IPsec connection status change	ToRemote
2024/09/13 06:24:16	Notice	phase2-up		IPsec phase 2 status change	ToRemote
2024/09/13 06:24:16	Notice	install_sa		install IPsec SA	ToRemote
2024/09/13 06:24:16	Notice	negotiate	success	progress IPsec phase 2	ToRemote
2024/09/13 06:24:08	Notice	negotiate	success	progress IPsec phase 1	ToRemote
2024/09/13 06:24:08	Notice	negotiate	success	progress IPsec phase 1	ToRemote
2024/09/13 06:24:07	Notice	delete_phase1_sa		delete IPsec phase 1 SA	ToRemote
2024/09/13 06:24:07	Notice	phase2-down		IPsec phase 2 status change	ToRemote
2024/09/13 06:24:07	Notice	tunnel-down		IPsec connection status change	ToRemote

Log Details

General

- Absolute Date/Time: 2024-09-13 06:24:08
- Last Access Time: 06:24:08
- VDOM: root
- Log Description: Progress IPsec phase 1

source

- Local IP: 10.200.1.1
- Source Country/Region: Reserved
- FortiClient ID: N/A
- User: Remote-FortiGate
- Group: N/A
- XAUTH User: N/A
- XAUTH Group: N/A

Action

- Action: negotiate
- Status: success
- Result: DONE

© Fortinet Inc. All Rights Reserved. 48

FortiGate logs IPsec VPN events by default. To view IPsec VPN event logs, click **Log & Report > System Events > VPN Events**.

The logs track the progress of phase 1 and phase 2 negotiations, and report on tunnel up and down events and DPD failures, among other events. For more information about IPsec logs, visit <https://docs.fortinet.com>.

DO NOT REPRINT**© FORTINET**

IPsec SA Management

```
# diagnose vpn tunnel ?  
down      Shut down tunnel  
up       Activate tunnel  
list     list all tunnel  
flush    Flush tunnel SAs.  
...
```



© Fortinet Inc. All Rights Reserved. 49

The same command `diagnose vpn tunnel` offers options for listing, shutting down, activating, or flushing a VPN tunnel.

DO NOT REPRINT

© FORTINET

IPsec SA

```
# diagnose vpn tunnel list name Hub2Spoke1
list IPsec tunnel by names in vd 0
-----
name=Hub2Spoke1 ver=1 serial=2 10.10.1.1:0->10.10.2.2:0
bound_if=6 lgwy=static/1 tun=intf/0 mode=auto/1 encap=none/8 options[0008]=npu
proxyid_num=1 child_num=0 refcnt=8 ilast=11 olast=3 auto-discovery=0
stat: rxp=513 txp=129 rxb=459050 txb=93
dpd: mode=on-demand on=1 idle=20000ms retry=3 count=0 segno=36
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=Hub2Spoke1 proto=0 sa=1 ref=2 serial=1
src: 0:192.168.1.0/255.255.255.0:0
dst: 0:10.10.20.0/255.255.255.0:0
SA: ref=7 options=2e type=00 soft=0 mtu=1438 expire=41195/0B replaywin=1024 seqno=9d esn=0
replaywin lastseq=00000200
life: type=01 bytes=0/0 timeout=43150/43200
dec: spi=01e54b14 esp=aes key=16 914dc5d092667ed436ea7f6efb867976
    ah=sha1 key=20 a81b019d4cdfda32ce51e6b01d0b1ea42a74adce
enc: spi=3dd3545f esp=aes key=16 017b8ff6c4ba21eac99b22380b7de74d
    ah=sha1 key=20 edd8141f4956140eef703d9042621d3dbf5cd961
dec:pkts/bytes=513/458986, enc:pkts/bytes=250/26848
npu_flag=03 npu_rgwy=10.10.2.2 npu_lgwy=10.10.1.1 npu_selid=1
```

Lists specified tunnel information only

DPD information

Anti-replay is enabled

SA information

Hardware offload information



The command `diagnose vpn tunnel list` displays the current IPsec SA information for all active tunnels.

The command `diagnose vpn tunnel list name <tunnel name>` provides SA information about a specific tunnel.

DO NOT REPRINT

© FORTINET

IPsec Tunnel Details

```

Hub # get vpn ipsec tunnel details
gateway
  name: 'Hub2Spoke1'
  type: route-based
  local-gateway: 10.10.1.1:0 (static)
  remote-gateway: 10.10.2.2:0 (static)
  mode: ike-v1
  interface: 'wan2' (6)
  rx packets: 1025 bytes: 524402 errors: 0
  tx packets: 641 bytes: 93 errors: 0
  dpd: on-demand/negotiated idle: 20000ms retry: 3 count: 0
  selectors
    name: 'Hub2Spoke1'
    auto-negotiate: disable
    mode: tunnel
    src: 0:192.168.1.0/0.0.0.0:0
    dst: 0:10.10.20.0/0.0.0.0:0
  SA
    lifetime/rekey: 43200/32137
    mtu: 1438
    tx-esp-seq: 2ce
    replay: enabled
    inbound
      spi: 01e54b14
      enc: aes-cb 914dc5d092667ed436ea7f6efb867976
      auth: sha1 a81b019d4cfd32ce51efb01d0b1ea42a74adce
    outbound
      spi: 3dd3545f
      enc: aes-cb 017b0ff6c4ba21eac99b22300b7de74d
      auth: sha1 edd80141f4956140ee703d9042621d3dbf5cd961
    NPU acceleration: encryption(outbound) decryption(inbound)

```

Phase 1 details

Quick mode selectors

Tunnel MTU

Phase 2 SAs for each direction

Hardware acceleration

© Fortinet Inc. All Rights Reserved. 51

The command `get vpn ipsec tunnel details` provides information for the active IPsec tunnels.

The output shows traffic counters, negotiated quick mode selectors, and negotiated encryption, authentication, and keys.

DO NOT REPRINT

© FORTINET

IKE Gateway List

```
Hub # diagnose vpn ike gateway list name Hub2Spoke1
vd: root/0
name: Hub2Spoke1
version: 1
interface: wan2 6
addr: 10.10.1.1:500 -> 10.10.2.2:500
created: 3196s ago When phase 1 was created
auto-discovery: 0
IKE SA: created 1/1 established 1/1 time 6020/6020/6020 ms
IPsec SA: created 1/1 established 1/1 time 40/40/40 ms
```

```
id/spi: 87 16b474clae9de3ca/67e428c8c7118617
direction: initiator Is this gateway an initiator or responder?
status: established 3196-3190s ago = 6020ms
proposal: aes128-sha256
key: 34641b135ceeb2cd-c44a41d15dec439c
lifetime/rekey: 86400/82909
DPD sent/recv: 00000040/0000002e
```

```
Hub # diagnose vpn ike gateway clear <name>
```

Clear phase 1



The command `diagnose vpn ike gateway list` also provides some details about a tunnel.

The command `diagnose vpn ike gateway clear` closes a phase 1. Be careful when using this command because it has a global effect. This means that running it without specifying the phase 1 name results in all phase 1s of all VDOMs being cleared.

DO NOT REPRINT**© FORTINET**

Common IPsec Problems

Problem	Output of IKE debug	Common causes	Common solutions
Tunnel is not coming up	Error: negotiation failure	IPsec configuration mismatch	Verify phase 1 and phase 2 configurations between both peers
	Error: no SA proposal chosen	IPsec configuration mismatch	Verify phase 1 and phase 2 configurations between both peers Enable NAT-Traversal
Tunnel is unstable	DPD packet lost	ISP issue	Check internet connection Enable NAT-Traversal
Tunnel is up but traffic doesn't pass through it	Error in debug flow: no matching IPsec selector, drop	Traffic not matching quick mode selector	Verify quick mode selectors are correct
	Routing issue	NAT is enabled	Disable NAT on the VPN firewall policy
		Route missing or pointing to wrong device	Verify route is correctly defined Enable NAT-Traversal



This slide shows a summary of the most common IPsec problems and solutions.

If the tunnel doesn't come up, use the IKE real-time debug. In such cases, an error message usually appears.

When the tunnel is unstable, you usually see that DPD packets are being lost, which indicates that the problem might be on the ISP side.

If the tunnel is up but traffic isn't passing through it, use the debug flow. One of the peers might be dropping packets or routing traffic incorrectly. Another possibility is that the packets don't match the quick mode selectors, so FortiGate drops the packets.

DO NOT REPRINT

© FORTINET

Knowledge Check

1. What is a configuration requirement for an IPsec tunnel to come up?
 A. A firewall policy accepting traffic on the IPsec tunnel
 B. A route for IPsec traffic

2. Which setting determines whether a tunnel is used as primary or backup without ECMP?
 A. Routing
 B. Firewall policies

3. When the remote gateway is set to dial-up user, a static route to the remote network is added to the routing table after _____.
 A. Phase 1 comes up
 B. Phase 2 comes up



DO NOT REPRINT

© FORTINET

Lesson Progress



IPsec Basics



IPsec Configuration



Routing and Firewall Policies



Monitoring



© Fortinet Inc. All Rights Reserved. 55

Congratulations! You have completed this lesson.

Now, you will review the objectives covered in this lesson.

DO NOT REPRINT

© FORTINET

Review

- ✓ Configure IPsec VPN manually
- ✓ Configure IPsec VPN using the IPsec wizard
- ✓ Configure a redundant VPN between two FortiGate devices
- ✓ Monitor IPsec VPNs and review logs
- ✓ Troubleshoot IPsec VPN issues



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

By mastering the objectives covered in this lesson, you learned how the IPsec protocol works, and how to configure and monitor IPsec VPNs on FortiGate.

DO NOT REPRINT

© FORTINET

FORTINET
Training Institute

FortiOS Administrator

SD-WAN Configuration and Monitoring

 FortiOS 7.6

Last Modified: 6 October 2025

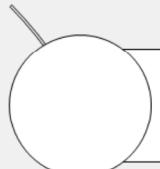
© Fortinet Inc. All Rights Reserved. 1

In this lesson, you will learn about the SD-WAN feature available on FortiGate.

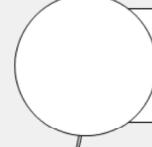
DO NOT REPRINT

© FORTINET

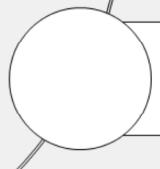
Lesson Overview



SD-WAN Basics



SD-WAN Fundamentals



SD-WAN Basic Monitoring



© Fortinet Inc. All Rights Reserved.

2

In this lesson, you will learn about the topics shown on this slide.

DO NOT REPRINT**© FORTINET**

SD-WAN Basics

Objectives

- Describe SD-WAN
- Identify the main use cases for SD-WAN



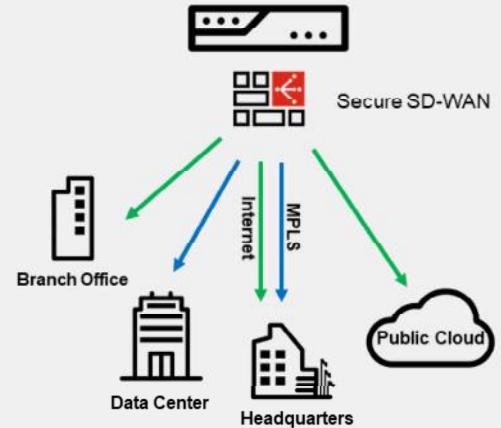
After completing this section, you should be able to achieve the objectives shown on this slide.

By understanding an SD-WAN solution and its use cases, you should be able to identify the most common scenarios where SD-WAN can be deployed to distribute traffic across your WAN links effectively and securely.

DO NOT REPRINT**© FORTINET**

What Is SD-WAN?

- Software-defined approach to steer WAN traffic using:
 - Flexible user-defined rules
 - Protocol and service-based traffic matching
 - Application-awareness
 - Dynamic link selection
 - Controls egress traffic
- Secure SD-WAN
 - Fortinet SD-WAN implementation (built-in security)
- Benefits:
 - Effective WAN use
 - Improved application performance
 - Cost reduction



According to Gartner, software-defined WAN (SD-WAN) provides dynamic, policy-based, application path selection across multiple WAN connections, and supports service chaining for additional services, such as WAN optimization and firewalls. The Fortinet implementation of SD-WAN is called secure SD-WAN because it also provides security by leveraging the built-in security features available on FortiOS.

Secure SD-WAN relies on well-known FortiOS features, such as IPsec, link monitoring, advanced routing, internet services database (ISDB), traffic shaping, UTM inspection, and load balancing. The administrator can then combine these features and set rules that define how FortiGate steers traffic across the WAN based on multiple factors, such as the protocol, service, or application identified for the traffic, and the quality of the links. Note that SD-WAN controls *egress* traffic, *not ingress* traffic. This means that the return traffic may use a different link from the one SD-WAN chose for egress.

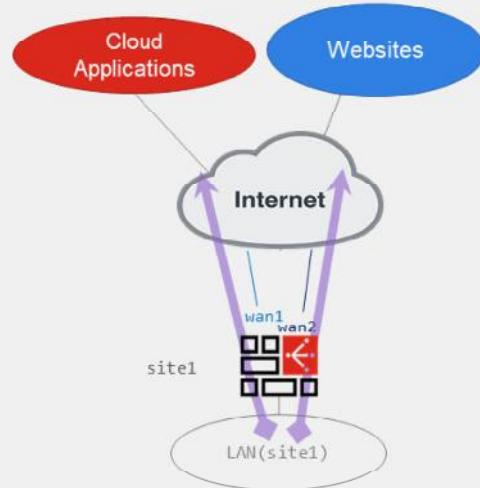
One benefit of SD-WAN is effective WAN use. That is, you can use public (for example, broadband or LTE) and private (for example, MPLS) links to securely steer traffic to different destinations: internet, public cloud, private cloud, and the corporate network. This approach of using different types of links to connect sites to private and public networks is known as hybrid WAN. Using a hybrid WAN reduces costs mainly because administrators usually steer traffic over low-cost fast internet links more than over high-cost slow private links. The result is that private links, such as MPLS links, are often used to steer critical traffic only, or as failover links for high availability.

Another benefit of SD-WAN is improved application performance because you can steer traffic through the best link that meets the application requirements. During congestion, you can leverage traffic shaping to prioritize sensitive and critical applications over less important ones.

DO NOT REPRINT
© FORTINET

SD-WAN Use Cases—Direct Internet Access

- Traffic steered across multiple physical internet links
- Typical operation:
 - Critical/sensitive traffic expedited and steered over best performing links
 - Costly links used for critical traffic or failover
 - Static default routing
- Example:
 - Two internet links (wan1 and wan2)
 - Both steer traffic from the LAN
 - Use best-performing link for critical applications
 - Use low-cost link for web surfing



Direct internet access (DIA), also known as local breakout, is arguably the most common use case for SD-WAN. A site has multiple internet links (also known as underlay links), and the administrator wants FortiGate to steer internet traffic across the links. The links are connected to FortiGate using different types of physical interfaces: physical port, VLAN, link aggregation (LAG), USB modem, or through FortiExtender.

Usually, the administrator chooses to send sensitive traffic over the best-performing links, while distributing non-critical traffic across one or more links using a best-effort approach. Costly internet links are commonly used as backup links, or to steer critical traffic only.

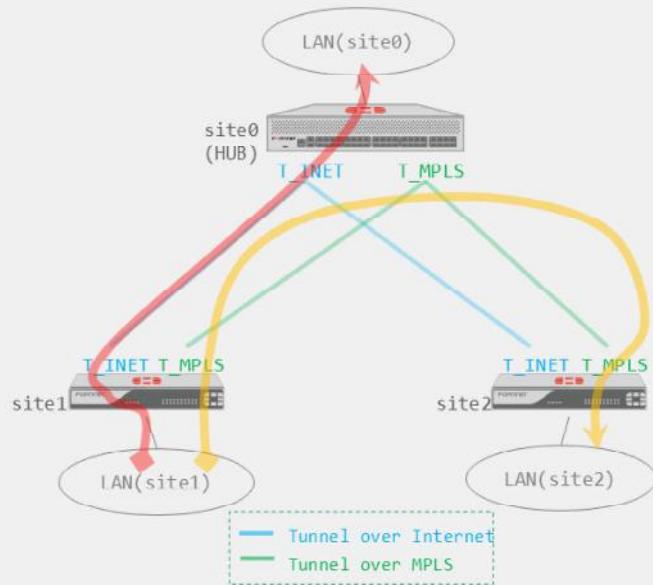
Because the internet traffic leaves the organization boundaries directly on the local site, administrators usually enforce strict security policies on the internet traffic. For routing, a typical configuration makes use of static default routes. However, in some cases, BGP is used between the ISP and FortiGate, especially if the site must advertise a public IP prefix.

Administrators can also manually define the upstream and downstream speeds of each link to prevent saturation during traffic distribution. Alternatively, they can configure FortiGate to use the SD-WAN bandwidth monitoring service to run speed tests against FortiGuard, and then automatically adjust the upstream and downstream speeds of the links based on the test results.

DO NOT REPRINT
© FORTINET

SD-WAN Use Cases—Site-to-Site Traffic

- Use overlay links to steer site-to-site corporate traffic
 - Overlay: tunnels
 - Underlay: physical links
- Typical operation:
 - Hub-and-spoke topologies
 - Dynamic IPsec tunnels used for overlay
 - Dynamic routing



You can use SD-WAN to steer corporate site-to-site traffic. Usually, companies follow a hub-and-spoke topology, and use VPN tunnels—typically dynamic IPsec tunnels—to transport the traffic between the sites. The tunnels (also known as overlay links) are established over internet or MPLS links (also known as underlay links). Tunnels can also carry internet traffic from a spoke to a hub where it then exits to the internet.

SD-WAN can monitor the link quality of the tunnels and select the best performing link for sensitive and critical traffic

For routing, static routing is possible, but a dynamic routing protocol, such as BGP, is often used to exchange routing information through the tunnels. Dynamic routing scales more easily when adding new sites.

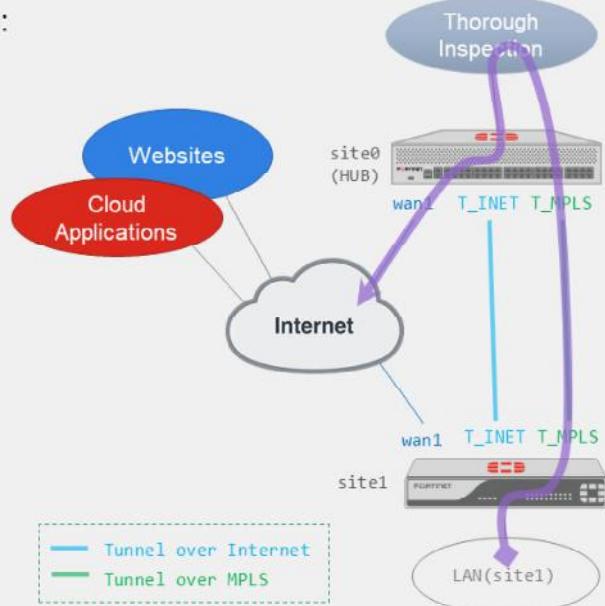
Similar to DIA, the hub FortiGate can run speed tests against the spokes to determine the upstream speed of tunnels. The hub FortiGate can then apply the speed test result as the upstream speed on the tunnel for traffic shaping purposes.

In the example shown on this slide, each site has two overlays configured, one using the internet underlay and the other the MPLS underlay. SD-WAN steers spoke-to-hub traffic.

DO NOT REPRINT
© FORTINET

SD-WAN Use Cases—Remote Internet Access

- Internet traffic steered across overlay links to:
 - Centralize inspection on hub
 - Improve performance if DIA performance is poor
 - Provide internet access if DIA is unavailable
- Typical operation:
 - Limited inspection on spokes
 - Hub performs thorough inspection
 - Backup direct internet access



© Fortinet Inc. All Rights Reserved. 7

Remote Internet Access (RIA), also known as remote breakout, is another use case for SD-WAN. Internet traffic from the spokes is backhauled through the WAN using overlay links. When the traffic arrives at the hub, it breaks out to the internet.

The most common reason to use RIA is to centralize security inspection and internet access on the hub. For example, you can have a central high-end FortiGate device that inspects all the internet traffic that leaves the organization and conforms with the company policy, instead of having each low-end spoke FortiGate device to inspect traffic, thus reducing costs and administrative overhead.

Another reason to use RIA is for DIA backup. For example, you could configure FortiGate to steer internet traffic through an MPLS link if the performance measured for internet applications on internet links is worse than on MPLS links, or simply if the internet links become unavailable.

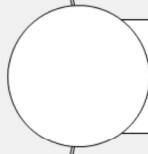
DO NOT REPRINT

© FORTINET

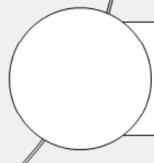
Lesson Progress



SD-WAN Basics



SD-WAN Fundamentals



SD-WAN Basic Monitoring



© Fortinet Inc. All Rights Reserved.

8

Good job! You now understand the basics of SD-WAN.

Now, you will learn about SD-WAN fundamentals.

DO NOT REPRINT**© FORTINET**

SD-WAN Fundamentals

Objectives

- Introduce SD-WAN basic components
- Configure SD-WAN on FortiGate
- Describe and analyze routing behavior in an SD-WAN context



© Fortinet Inc. All Rights Reserved.

9

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

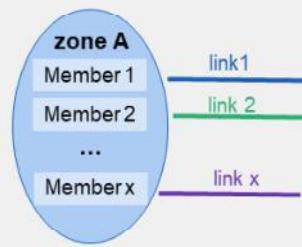
By demonstrating competence in SD-WAN fundamentals, you should be able to configure a basic SD-WAN setup.

DO NOT REPRINT**© FORTINET**

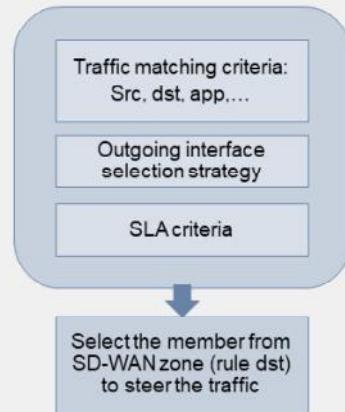
SD-WAN Components

- Members
 - Interfaces used to steer traffic
 - Logical or physical interfaces
- Zones
 - Logical grouping of members
 - Optimize configuration
- Performance SLAs
 - Performs member health check
 - State: alive or dead
 - Performance: packet loss, latency, jitter
- SD-WAN rules
 - Define where to steer the traffic
 - Traffic matching criteria (src, dst, app,...)
 - Outgoing interface selection strategy
 - Performances or members

SD-WAN zone



SD-WAN rule



Select the member from SD-WAN zone (rule dst) to steer the traffic



© Fortinet Inc. All Rights Reserved. 10

On FortiGate, an SD-WAN configuration is built on SD-WAN rules. SD-WAN rules combine traffic matching criteria and traffic steering preferences. They describe the administrator choices related to the SD-WAN solution.

To define SD-WAN rules use:

- Members: These are the logical or physical interfaces used to steer the traffic.
- Zones: Zones are groups of members used to optimize the configuration.
- Performances SLA rules: With the performance SLA rules you can define how you want to monitor the status of members and the performance criteria that you want to monitor. It can be packet loss, jitter, latency, or a weighted mix of a few criteria.

You first define the criteria of the application or traffic to match. Then, you indicate the forward policy to follow for steering traffic across one or more members and zones, including the strategy to apply and the performance metrics to determine the preferred members.

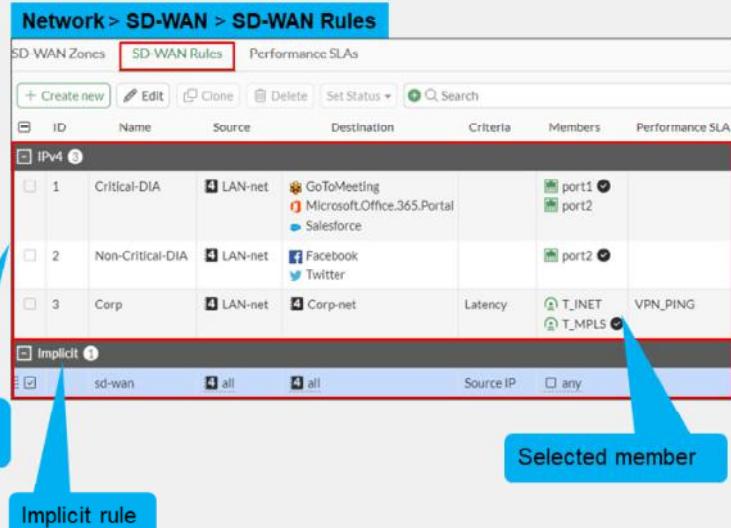
In the next few slides, you will learn more about each element that composes an SD-WAN rule.

DO NOT REPRINT

© FORTINET

SD-WAN Rules

- Describe administrator SD-WAN choices
- Define steering rules based on:
 - Matching traffic criteria
 - Member preference
 - Define zones to steer traffic to a list of preferred members
 - Member performance
 - Define criteria SLA members must meet
 - Strategy and quality criteria:
 - Manual, best quality, lowest cost
 - Latency, jitter, packet loss



SD-WAN rules combine traffic-matching criteria and traffic-steering preferences. They describe the administrator choices related to the SD-WAN solution and its software-defined components.

You first define the criteria of the application or traffic to match. Then, you indicate the forward policy to follow for steering traffic across one or more members and zones, including the strategy to apply and the performance metrics to determine the preferred members.

Preferred members are the best alive members in a zone based on the strategy in use. FortiGate then uses the preferred members—provided they are acceptable—to steer traffic. For all strategies, if you don't activate a load balancing mode, FortiGate chooses a single member to steer traffic. You will discover the strategies available later in this lesson.

If none of the user-defined SD-WAN rules are matched, then FortiGate uses the implicit rule.

The example on this slide shows three user-defined rules. A rule named **Corp** which is used to steer critical traffic from the branch office to the headquarters. The rule steers traffic from LAN-net to the Corp-net through the overlay links (T_INET and T_MPLS). The member selection is done using latency criteria and T_MPLS is the selected member. The rules **Critical-DIA** and **Non-Critical-DIA**, which FortiGate uses to steer traffic for DIA through the underlay zone (port1 and port2), differentiate the link selection according to the application in use. Note that only the most significant parts of rule configuration are shown in the output.

DO NOT REPRINT**© FORTINET**

SD-WAN Rules (Contd)

- Evaluated in descending order:
 - First match applies
 - SD-WAN rules are used to steer traffic
 - Firewall policy required to allow the traffic
- Implicit rule
 - Always present
 - Used if user-defined rules are not matched
 - Follow standard routing table
 - Traffic is load balanced (default: per source IP)

ID	Name	Source	Destination	Criteria	Members	Hit Count	Last Used
1	Critical-DIA	LAN-net	GoToMeeting Microsoft.Office.365.Portal Salesforce		port1 port2	0	47 minutes ago
2	Corp	LAN-net	Corp-net	Latency	T_INET T_MPLS	8	28 seconds ago
	Implicit	sd-wan	all	Source IP	any		

© Fortinet Inc. All Rights Reserved. 12

FortiGate evaluates SD-WAN rules in the same way as firewall policies: from top to bottom, using the first match. However, unlike firewall policies, they are used to steer traffic, *not* to allow traffic. When you use SD-WAN rules, you *must* configure corresponding firewall policies to allow SD-WAN traffic.

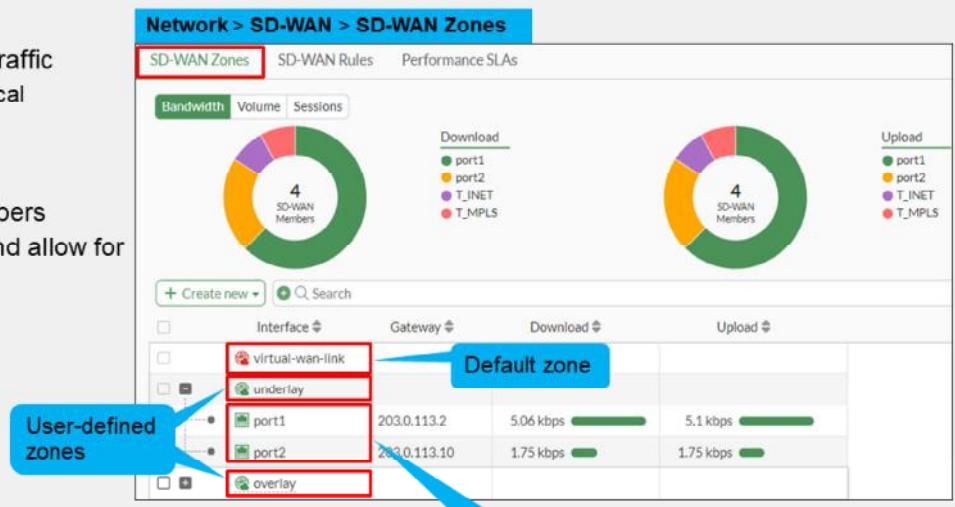
There is an implicit SD-WAN rule created by default. It is always present at the bottom of the SD-WAN rule list. If none of the user-defined SD-WAN rules are matched, then the implicit rule is used. This means that FortiGate routes the traffic according to the regular process. By default, the implicit rule load balances the traffic across all available SD-WAN members. In the example above, the implicit rule can steer the traffic through overlay (T_INET, T_MPLS) or underlay (port1, port2) members, according to the best match in the routing table.

You can double-click the implicit rule to display the load balancing options. By default, the implicit rule load balances the traffic according to **Source IP**. You can decide to load balance according to **Source-Destination IP**, **Sessions**, **Volume**, or **Spillover**.

DO NOT REPRINT
© FORTINET

SD-WAN Members and Zones

- Members
 - Interfaces used to steer traffic
 - Can be physical or logical
 - Organized in zones
- Zones
 - Logical grouping of members
 - Optimize configuration and allow for segmentation
 - Predefined default zone:
 - **virtual-wan-link**



The first step to configure SD-WAN is to define the members and assign them to zones. This configuration is done on the **SD-WAN Zones** page.

Members (also known as links) are existing physical or logical FortiOS interfaces that you select to be part of SD-WAN. FortiGate then uses the interfaces to steer traffic based on the SD-WAN rules configured.

When you configure a member in SD-WAN, you must assign it to a zone and, optionally, set a gateway. Zones are logical groupings of interfaces. The interfaces in a zone have similar configuration requirements. Like FortiGate interface zones, the goal with SD-WAN zones is to reference them in the configuration instead of individual members to optimize the configuration by avoiding duplicate settings. When set, FortiGate uses the **Gateway** setting as the next hop to forward traffic through the member.

FortiGate creates one zone by default, called **virtual-wan-link** zone. It is where FortiGate places any new member if you don't assign them to a user-defined zone.

The example on this slide shows the default SD-WAN zone—**virtual-wan-link**—and two user-defined zones: **underlay** and **overlay**. The **underlay** zone contains **port1** and **port2** as members, which are used for a basic DIA setup. Note that although the zone is named **underlay** because it contains this type of members, you can assign any name you like.

DO NOT REPRINT
© FORTINET

SD-WAN Members—Underlay and Overlay Links

- Underlay:
 - Physical links provided by ISP
 - Cable, DSL, fiber, MPLS, 3G/4G/5G/LTE, ATM
 - Restricted routing
 - No added security
- Overlay:
 - Virtual links built on top of underlay links
 - IPsec, GRE, IP-in-IP
 - Flexible routing
 - Enhanced security

Supported SD-WAN Members*	
Interface	Type
Physical	
VLAN	
LAG	Underlay
3G/4G/5G/LTE USB modems	
FortiExtender	
IPsec (including ADVPN)	
GRE	Overlay
IP-in-IP	



In an SD-WAN environment, the terms *underlay* and *overlay* are commonly used to describe the link type of an SD-WAN member.

Underlays refer to the physical links that you can rent or buy from an ISP, such as cable, DSL, fiber, MPLS, 3G/4G/5G/LTE, and ATM links. These links are part of the ISP physical infrastructure that is responsible for delivering packets across networks. The traffic that travels through underlays is restricted to the routing policies deployed by the ISP and, therefore, the packet source and destination IP addresses must be routable within the ISP network. This restriction leaves you with limited options to define your network addressing plan. In addition, traffic transmitted through underlays is usually not encrypted by the ISP network, which means that unauthorized parties can access sensitive data if the sender does not encrypt the data.

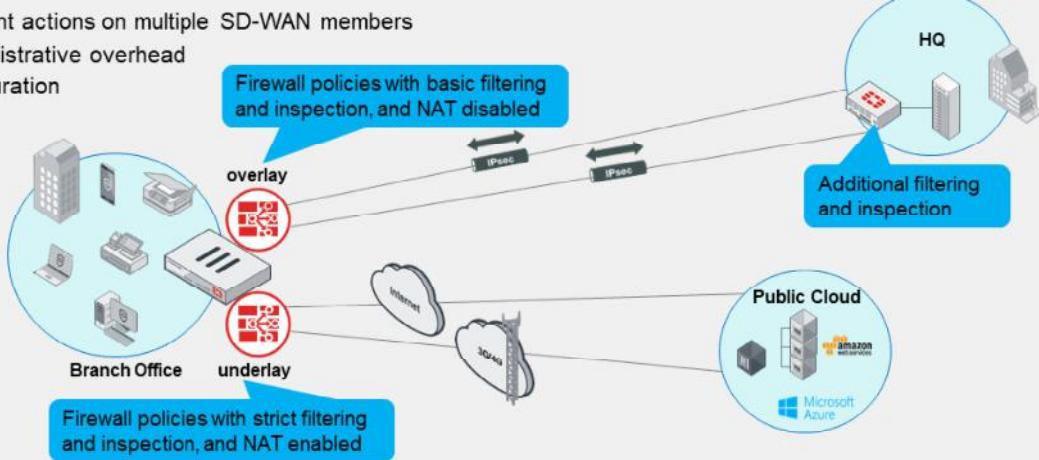
Overlays are virtual links that you build on top of underlays. A common example of an overlay is an IPsec tunnel. Because original packets are often encapsulated in ESP packets, the networks that communicate through the IPsec tunnel are no longer restricted to the routing policies of the ISP. In addition, the privacy and authentication features provided by IPsec protect your traffic from unauthorized access.

This slide shows the different underlay and overlay links supported by FortiGate as SD-WAN members.

DO NOT REPRINT
© FORTINET

SD-WAN Zones

- Divides SD-WAN members into groups
 - Default zone: **virtual-wan-link**
 - Can't be deleted
 - An interface can belong to one zone only
- Apply firewall policies on SD-WAN zones
 - Perform different actions on multiple SD-WAN members
 - Reduces administrative overhead
 - Cleaner configuration



© Fortinet Inc. All Rights Reserved. 15

Usually, you should apply a different set of policies based on the link type of your SD-WAN members. For example, you may want to enable NAT and apply strict security policies to internet traffic sent through underlay links, because the traffic directly leaves the site boundaries. Conversely, you may want to disable NAT and apply basic filtering and inspection to traffic sent through overlay links, because the remote site is fully routable and performs additional filtering and inspection on the traffic.

SD-WAN zones allow administrators to group members that require a similar set of firewall policies. Usually, this means grouping underlays and overlays into different SD-WAN zones.

FortiGate creates the **virtual-wan-link** SD-WAN zone by default, which you can't delete. It contains any SD-WAN member not explicitly assigned to a user-defined SD-WAN zone. Firewall policies defined for your SD-WAN traffic, must reference the SD-WAN zones, and cannot reference individual SD-WAN members.

The topology shown on this slide shows a branch office with two SD-WAN zones configured: overlay and underlay. The overlay SD-WAN zone is composed of IPsec tunnels and the underlay SD-WAN zone is composed of an internet link and a 3G/4G link. The branch office uses the overlays to access the headquarter networks, and the underlays to access services in the public cloud. By dividing SD-WAN members into zones, you can apply the same set of firewall policies to a zone instead of having to apply them to their individual members, thus reducing the administrative overhead and building a cleaner configuration.

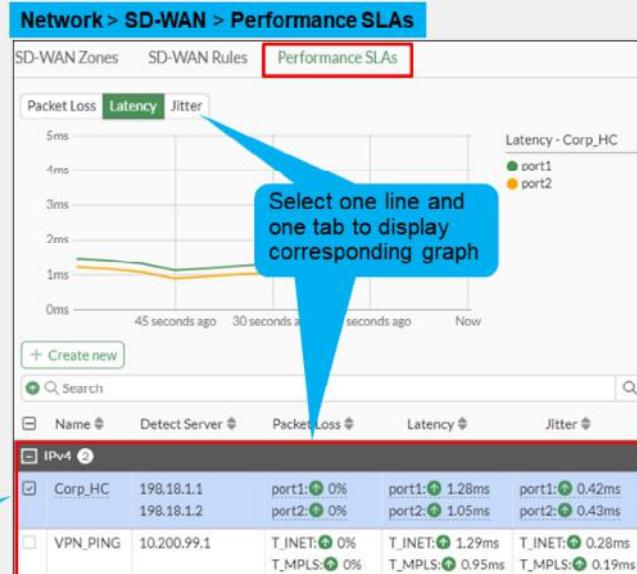
DO NOT REPRINT

© FORTINET

Performance SLAs

- Monitor member health
 - State
 - Alive or dead
 - Performance
 - Packet loss, latency, and jitter
 - SLA targets
 - Minimum performance requirements
- Health can be measured
 - Actively
 - Based on periodic probes sent to configured servers
 - Passively
 - Based on member traffic
- Use for strategy application

User-defined performance SLAs



© Fortinet Inc. All Rights Reserved. 16

After you define your SD-WAN members and assign them to zones, you can monitor the health of your SD-WAN members on the **Performance SLAs** page. Although configuring performance SLAs is optional, you should configure them to ensure members meet the health and performance requirements for steering traffic, which is critical for effective WAN use with SD-WAN.

FortiGate performance SLAs monitor the state of each member—whether it is alive or dead—and measures the member packet loss, latency, and jitter. SD-WAN then uses the member health information to make traffic steering decisions based on the configured SD-WAN rules. For example, you can instruct FortiGate to steer internet traffic to a member, provided the member is alive and its latency doesn't exceed a given threshold. Performance SLAs also detect situations where the interface is physically up, but FortiGate is unable to reach the desired destination and flags the corresponding link as dead.

When you configure a performance SLA, you can decide whether you want to monitor the link health actively or passively. In active monitoring, the performance SLA checks the health of the member periodically—by default every 500ms— sending probes from the member to one or two servers that act as a beacon. In passive monitoring, the performance SLA determines the health of a member based on the traffic passing through the member. Note that only active monitoring can detect if a link is alive or dead.

The example on this slide shows an entry named **Corp_HC**. The entry contains two servers, both of which are used to monitor the health of **port1** and **port2**. The performance SLA **VPN_PING** monitors the health of the two overlay tunnels, **T_INET** and **T_MPLS**. The results show that the members are alive (green arrow), report no packet loss, and have average values for latency. (Jitter is also measured but not visible in this example.)

DO NOT REPRINT
© FORTINET

Performance SLA Configuration

The screenshot shows the 'Edit Performance SLA' configuration page. Key fields include:

- Name:** Corp_HC
- Probe mode:** Active (selected)
- Protocol:** Ping
- Servers:** 198.18.1.1, 198.18.1.2
- Participants:** All SD-WAN Members (Specify: port1, port2)
- SLA Target:**
 - Latency threshold: 5 ms
 - Jitter threshold: 5 ms
 - Packet Loss threshold: 0 %
- Link Status:**
 - Check interval: 500 ms
 - Failures before inactive: 5
 - Restore link after: 5 check(s)
- Actions when Inactive:** Update static route



© Fortinet Inc. All Rights Reserved. 17

When you configure a performance SLA rule, you first define the link health monitor parameters.

In this section you will define the detection mode that FortiGate uses to monitor the link quality:

- **Active:** FortiGate sends active probes to the configured server to monitor the link health.
- **Passive:** FortiGate uses traffic through the link to evaluate the link health. It uses session information from traffic on selected firewall policies (firewall policies with the parameter `passive-wan-health-measurement` enabled).
- **Prefer Passive:** FortiGate uses passive monitoring and, only if there is no traffic through the link, sends probes.

You can specify up to two servers to act as your beacons. This guards against the server being at fault, and not the link.

The SLA target section is optional. It's where you define the performance requirements of alive members (latency, jitter, and packet loss thresholds). The performance SLA uses SLA targets with some SD-WAN rule strategies, like **Lowest Cost (SLA)**, to decide if the link is eligible for traffic steering or not.

The link status section is available for **Active** and **Prefer Passive** probe mode. It is where you define how often FortiGate sends probes through each monitored link, and how many failed probes you accept before declaring a link as dead.

The example on this slide shows the configuration of a performance SLA named **Corp_HC**. It is defined with **Active** probe mode, and default values for SLA target and probe configuration. It monitors the status and performances of two underlay interfaces, port1 and port2.

DO NOT REPRINT
© FORTINET

SD-WAN Rules Strategies

- Define
 - Requirements for preferred members
 - Single or multiple member traffic distribution
- Preferred members
 - Best candidates to steer traffic
 - Are used only if they have a valid route to the destination
- Member selection
 - **Manual**
 - Configuration order preference
 - **Best Quality**
 - Best performing member based on quality criteria
 - **Lowest Cost (SLA)**
 - Member that meets SLA target (tiebreakers: cost and priority)



The strategy in a rule defines the requirements for preferred members. The preferred members are the best members from the outgoing interface (`oif`) list—based on the strategy in use—that meet the SLA requirements (if applicable). The `oif` list sorts the configured members by preference. That is, although the members are the same, their order in the `oif` list and the **Interface preference** list, can be different. There are three strategies you can chose from:

- **Manual:** FortiGate prefers members according to configuration order. Member metrics are not considered for member preference.
- **Best quality:** FortiGate prefers the best-performing member based on the configured quality criteria.
- **Lowest cost (SLA):** FortiGate prefers the member that meets the configured SLA target. If multiple members meet the SLA target, member cost, followed by the configuration order, are used as tiebreakers.

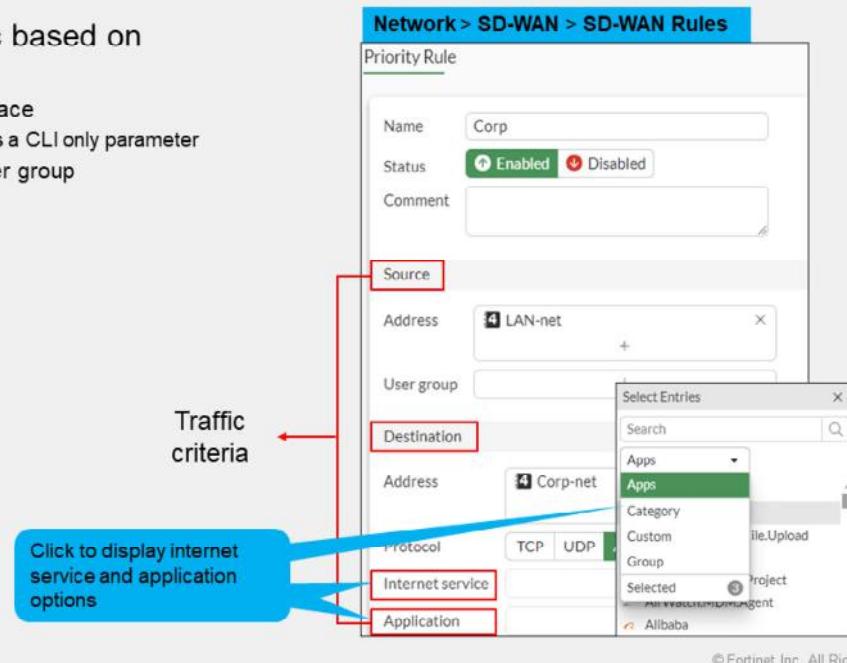
You can combine the strategy **Manual** and **Lowest cost (SLA)** with the load balancing option to instruct FortiGate to steer the traffic through multiple members. When you combine **Manual** with load balancing, FortiGate distributes the traffic through all members that are up. When you combine load balancing with the **Lowest cost (SLA)** strategy, FortiGate distributes the traffic through all members that meet the SLA target.

Note that for all strategies, by default, FortiGate must check that the preferred member has a valid route to the destination. If the member doesn't have a valid route, then FortiGate checks the next member in the `oif` list, and so on, until it finds an acceptable member. Moreover, all strategies, except **Manual**, consider the member metrics for member preference.

DO NOT REPRINT
© FORTINET

SD-WAN Rule Traffic Match Criteria

- Rules can match traffic based on
 - Source
 - IP address and interface
 - Source interface is a CLI only parameter
 - Firewall user and user group
 - Destination
 - IP address
 - IP protocol number
 - Port range
 - Internet service
 - Application
 - Single application
 - Application category
 - Group of application
 - ToS



© Fortinet Inc. All Rights Reserved. 19

You can configure rules to match traffic based on the following criteria:

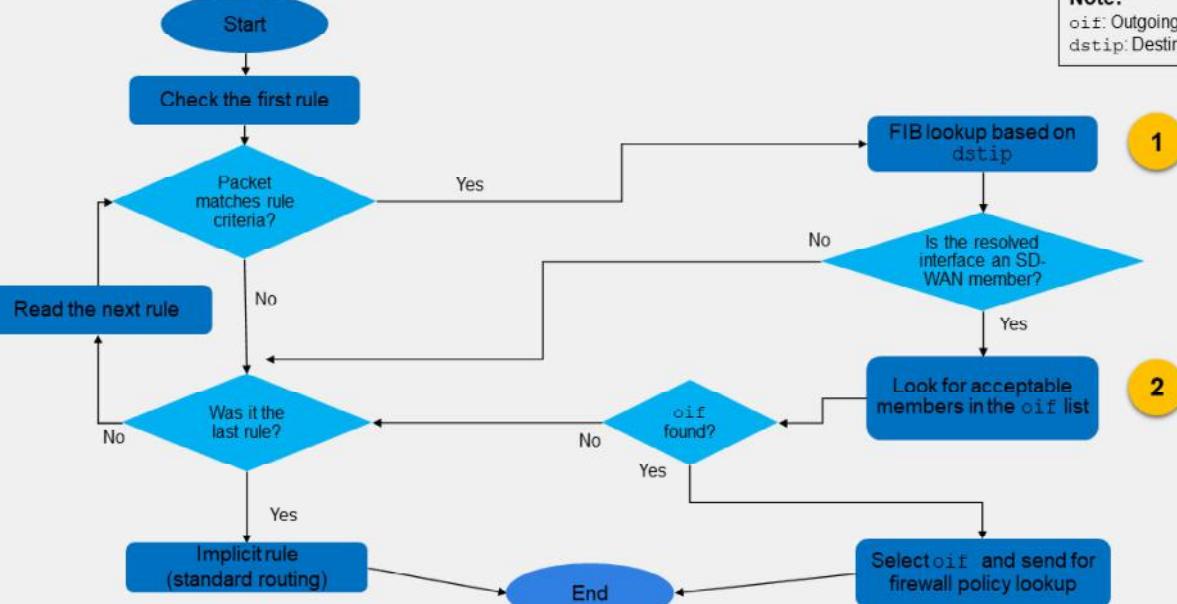
- Source IP address, source interface, firewall user, and firewall user group. If you want to specify the source interface, you should use the CLI commands `input-device` and `input-device-negate`.
- Destination IP address, IP protocol, destination port number
- Internet service
- Application: single application, application category, or group of applications
- Type of Service (ToS)

SD-WAN rules offer great flexibility for traffic matching. For example, you can match Netflix traffic sourced from specific authenticated users, or match the ICMP traffic—IP protocol 1—destined to a particular address.

Note that, by default, the GUI rule configuration menu does not display the application criteria field. If you want to use this feature, you should enable the criteria visibility from the CLI under `config system global`.

DO NOT REPRINT**© FORTINET**

Rule Lookup Process



© Fortinet Inc. All Rights Reserved. 20

This slide shows the SD-WAN rule lookup process. SD-WAN rules are essentially policy routes. Like regular policy routes, SD-WAN rules are checked from top to bottom (first match). For each rule, FortiGate maintains an outgoing interface (`oif`) list. The `oif` list sorts the configured members by preference based on the strategy in use. The members that are placed first in the list have higher preference for steering traffic. FortiGate starts the lookup process by comparing the packet against the rule matching criteria. If the packet doesn't match the criteria, FortiGate moves on to the next rule, and so on, until it finds a match. Then, FortiGate proceeds as follows:

1. FortiGate performs a forwarding information base (FIB) lookup for the packet destination IP (`dstip`). If the resolved interface for the `fib-best-match` isn't an SD-WAN member, then FortiGate moves on to the next rule. This behavior follows the key routing principle: *SD-WAN rules are skipped if the best route to the destination isn't an SD-WAN member*.
2. If the resolved interface is an SD-WAN member, then FortiGate looks for one or more acceptable members in the `oif` list, starting with the first member in the list. An acceptable member is an alive member that has a route to the destination. This behavior follows the key routing principle: *SD-WAN rules are skipped if none of the configured members in the rule have a valid route to the destination*.

If FortiGate finds an acceptable member, it forwards the packet to that member—then the firewall policy check occurs—and the rule lookup process ends. Otherwise, FortiGate moves on to the next rule. If all rules are skipped, then FortiGate routes the packet using standard routing, hence the key routing principle: *The implicit SD-WAN rule equals standard FIB lookup*.

DO NOT REPRINT**© FORTINET**

Firewall Policies With SD-WAN

- Steered traffic *must* be allowed by a firewall policy
- Reference SD-WAN zones only
 - Simplified configuration
- Can't reference a member directly

Policy & Objects > Firewall Policy

Policy	From	To	Source	Destination	Schedule	Service	Action	NAT	ID
To-Hub-Overlay (3)	port3	overlay	LOCAL_SUBNET	REMOTE_SUBNET	always	ALL	✓ ACCEPT	Disabled	3
From-Hub-Overlay (4)	overlay	port3	REMOTE_SUBNET	LOCAL_SUBNET	always	FTP HTTP HTTPS	✓ ACCEPT	Disabled	4
DIA (2)	port3	underlay	LOCAL_SUBNET	all	always	ALL	✓ ACCEPT	NAT	2
Implicit Deny (0)	any	any	any	all	always	ALL	✗ DENY		0

Individual port, which is not a member of an SD-WAN zone

SD-WAN zones

© Fortinet Inc. All Rights Reserved. 21

To be allowed by FortiGate, the traffic steered by an SD-WAN rule *must* also be allowed by a firewall policy.

You configure SD-WAN firewall policies in the same way as regular firewall policies except that, when selecting an outgoing or incoming interface, you must reference an interface that refers to an SD-WAN zone. When you reference a zone, you simplify the configuration by avoiding duplicate firewall policies. You can't use individual members of an SD-WAN zone in firewall policies.

The example on this slide shows firewall policies that reference the **underlay** and **overlay** SD-WAN zones. The **underlay** zone contains port1 and port2 as members, and the **overlay** zone contains T_INET and T_MPLS. Those policies also contain, as source or destination, the interface for the individual port port3. This interface is *not* part of an SD-WAN zone.

DO NOT REPRINT

© FORTINET

Policy Routes

- Provide more granular matching than static routes
 - Protocol
 - Source address
 - Source ports
 - Destination ports
 - ToS marking
 - Destination internet service
- Have precedence over SD-WAN rules and entries in the FIB
- Best practice
 - Narrow down matching criteria
- SD-WAN rules are essentially policy routes with additional software-defined criteria



Network > Policy Routes

New Routing Policy

If incoming traffic matches:

Incoming Interface	port5
Source Address	10.0.1.0/24
Addresses	
Destination Address	10.10.10.0/32
IP/Netmask	
Addresses	
Internet service	
Protocol	TCP
Source ports	0 - 65535
Destination ports	10444 - 10444
Type of service	0x00 Bit Mask: 0x00

Then:

Action	Forward Traffic
Outgoing Interface	port1
Gateway address	192.2.0.2
Comments	Write a comment... 0/255
Status	Enabled

Matching criteria
Action

© Fortinet Inc. All Rights Reserved. 22

When you configure an SD-WAN rule, FortiGate essentially applies a policy route on FortiOS. For this reason, before learning how routing in SD-WAN works, it is useful to first understand policy routes.

Static routes are simple and are often used in small networks. Policy routes, however, are more flexible because they can match more than just the destination IP address. For example, you can configure as matching criteria the incoming interface, the source and destination subnets, protocol, and port number. *Because regular policy routes have precedence over any other routes*, it is a best practice to narrow down the matching criteria as much as possible. Otherwise, traffic that is expected to be routed by SD-WAN rules or other routes in the forwarding information base (FIB) could be handled by regular policy routes instead.

This slide shows an example of a policy route configured using the FortiGate GUI. The policy route instructs FortiGate to match traffic received at **port5**, sourced from **10.0.1.0/24** and destined to the host **10.10.10.10**. The traffic must also be destined to TCP port **10444** for the policy route to match. FortiGate then forwards the traffic—the **Forward Traffic** action—to **port1** through the gateway **192.2.0.2**.

DO NOT REPRINT**© FORTINET**

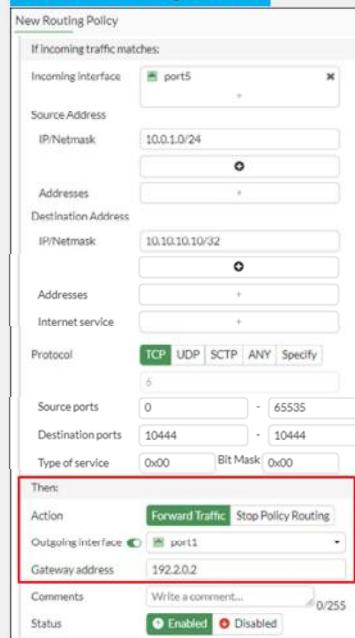
Policy Route—Actions

- **Stop Policy Routing**

- Skips all policy routes, uses the FIB

- **Forward Traffic**

- Forwards traffic using the set outgoing interface and gateway
- FIB must have a matching route; otherwise, policy route is considered invalid and skipped



Network > Policy Routes

New Routing Policy

If incoming traffic matches:

- Incoming interface: port5
- Source Address: 10.0.1.0/24
- Destination Address: 10.10.10.10/32
- Protocol: TCP
- Source ports: 0 - 65535
- Destination ports: 10444 - 10444
- Type of service: 0x00 Bit Mask: 0x00

Then:

Action: **Forward Traffic** (highlighted)

Outgoing interface: port1

Gateway address: 192.2.0.2

Comments: Write a comment... 0/255

Status: Enabled

Action

© Fortinet Inc. All Rights Reserved. 23



When a packet matches a policy route, FortiGate takes one of two actions. Either it routes the packet to the configured outgoing interface and gateway—the **Forward Traffic** action—or it stops checking the policy routes—the **Stop Policy Routing** action—so the packet is routed based on the FIB.

Note that when you configure **Forward Traffic** as the action, the **Destination Address**, **Outgoing interface**, and the **Gateway address** settings must match a route in the FIB. Otherwise, the policy route is considered invalid and, as a result, skipped.

Also note that policy routes have precedence over SD-WAN rules, and over any routes in the FIB. That is, if a packet matches a policy route and the policy route has a matching route in the FIB, then FortiGate doesn't check any of the configured SD-WAN rules or the routes in the FIB.

DO NOT REPRINT

© FORTINET

Routing

- Valid route required for steering traffic to members
- Static and dynamic routes supported
- Static routes
 - Reference a zone
 - Common case, simplified configuration
 - Individual ECMP routes installed for each member in the zone
 - Gateway obtained from member configuration
 - Reference a member
 - More granular control

Network > Static Routes				
	Destination	Gateway IP	Interface	Status
	0.0.0.0/0		underlay	Enabled

A zone can be referenced

```
# get router info routing-table all
...omitted output...
S*      0.0.0.0/0 [1/0] via 10.200.1.254, port1
[1/0] via 10.200.2.254, port2
...
```

Individual ECMP routes for each member in the zone



SD-WAN rules define the traffic steering policies in SD-WAN. However, traffic won't be forwarded to an SD-WAN member unless there is a valid route that matches the destination address of the traffic through the SD-WAN member.

Because the goal is to have SD-WAN pick the best member to forward the traffic to, based on the SD-WAN rule criteria, it's a best practice to configure your routing setup so your SD-WAN sites know all possible routes to all possible destinations that are intended for handling by SD-WAN. Otherwise, SD-WAN may fail to choose the best member, not because it doesn't meet the application requirements, but because FortiGate doesn't have a route for the destination and member.

You can use static and dynamic routing in SD-WAN. This slide shows an example of a static default route configured for the **underlay** zone, which is used to route traffic in a basic DIA setup.

DO NOT REPRINT
© FORTINET

Static Routes Configuration

- Static route per SD-WAN zone
 - Simplified configuration
 - Gateway is retrieved from member settings
- Static route per SD-WAN member
 - More granularity
 - Gateway not retrieved from member settings

The screenshot shows two parts of the FortiOS interface: 'Network > Static Routes' and a terminal window displaying the routing table.

Network > Static Routes:

- Left Panel (Zone Configuration):**
 - Destination: Subnet Internet Service (8.0.0.0/0.0.0.0)
 - Interface: underlay (highlighted with a red box)
 - Status: Enabled
- Right Panel (Member Configuration):**
 - Destination: Subnet Internet Service (8.8.8.8/255.255.255.255)
 - Gateway Address: Dynamic Specify (10.200.1.199) (highlighted with a red box)
 - Interface: port1 (highlighted with a red box)
 - Status: Enabled

Terminal Output:

```
# get router info routing-table all
...
S* 0.0.0.0/0 [1/0] via 10.200.1.254, port1, [1/0]
    [1/0] via 10.200.2.254, port2, [1/0]
S 8.8.8.8/32 [10/0] via 10.200.1.199, port1, [1/0]
...
```

Annotations explain the output:

- Individual ECMP routes for each member in the zone:** Points to the first route entry in the terminal output.
- Part of SD-WAN zone:** Points to the 'port1' entry in the member configuration panel.
- As individual interface:** Points to the 'port1' entry in the terminal output.
- Specific member from an SD-WAN zone:** Points to the 'Specify' button in the member configuration panel.
- Gateway:** Points to the 'Specify' button in the member configuration panel.

© Fortinet Inc. All Rights Reserved. 25

When you configure a static route, you can reference one or more zones as the outgoing interface. As a result, FortiOS installs a static route in the routing table for every member configured in the zone. Because the static routes share the same distance, they become ECMP routes. FortiOS uses the gateway defined for each zone member.

Alternatively, you can configure per-member static routes for more granular control over traffic. However, unlike static routes for zones, which retrieve the member gateway from the member configuration, with per-member static routes, you must specify a gateway if the interface type requires it.

When you create a static route for a zone, FortiOS assigns the routes with a distance of 1 by default. FortiOS assigns such a low distance by default because administrators usually want their SD-WAN routes to have preference over other routes in the FIB. However, you can change the distance to a different value if required. Static routes for individual members have default distance of 10.

In the example shown on this slide, `port1` and `port2` are members of the `underlay` zone. The administrator created a default static route that references this zone. The result is that the routing table displays ECMP routes for each member of the zone. In addition, the administrator created a per-member static route for `8.8.8.8` through `port1`. All three routes can then be used by SD-WAN rules to route traffic, or by the FIB to route traffic when no rule is matched.

DO NOT REPRINT

© FORTINET

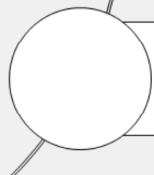
Lesson Progress



SD-WAN Basics



SD-WAN Fundamentals



SD-WAN Basic Monitoring



© Fortinet Inc. All Rights Reserved.

26

Good job! You now understand the fundamentals of SD-WAN.

Now, you will learn about SD-WAN basic monitoring.

DO NOT REPRINT**© FORTINET**

SD-WAN Basic Monitoring

Objectives

- Identify SD-WAN traffic logs and events
- Monitor SD-WAN behavior, link usage, and quality status



© Fortinet Inc. All Rights Reserved. 27

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

By understanding basic monitoring of SD-WAN, you should be able to identify the tools available on the FortiGate GUI to check SD-WAN traffic distribution, health, and events.

DO NOT REPRINT
© FORTINET

Verify SD-WAN Traffic Routing

- Use the **Forward Traffic** logs or the packet capture tool to verify traffic routing

Log & Report > Forward Traffic

Date/Time	Source	Destination	Destination Interface	Application Name	Result	Policy ID	SD-WAN Rule Name
2024/09/10 05:36:13	10.0.2.101	8.8.8.8 (dns.google)	port1	Ping	✓ Accept (UTM Allowed)	DIA (1)	
2024/09/10 05:35:57	10.0.2.101	128.66.0.1	port1	Ping	✓ Accept (UTM Allowed)	DIA (1)	
2024/09/10 05:35:42	10.0.2.101	10.2.0.7	T_MPLS	PING	✓ Accept (252 B / 0 B)	To Hub0-Overlay (2)	Corp
2024/09/10 05:35:31	10.0.2.101	10.1.0.7	T_MPLS	PING	✓ Accept (252 B / 252 B)	To Hub0-Overlay (2)	Corp
2024/09/10 05:33:56	10.0.2.101	217.180.209.214	port1	NTP	✓ Accept (UTM Allowed)	DIA (1)	

SD-WAN rule match Empty for Implicit rule

```
# diagnose sniffer packet any 'tcp[13]&2==2 and port 443' 4
5.455914 port1 out 192.168.1.254.59785 -> 192.168.1.11.443: syn 457459
5.455930 port2 out 192.168.1.11.443 -> 192.168.1.254.59785: syn 163440 ack 457460
5.455979 port2 out 192.168.1.32.49573 -> 192.168.1.25.443 : syn 927943
5.456043 port1 out 192.168.1.21.54711 -> 192.168.1.114.443: syn 930863
```

Use verbosity level 4 to 6 to see egress interface



To verify SD-WAN traffic routing, for logged flows, you can use the forward traffic logs. You can use the **Destination Interface** column in the **Forward Traffic** logs to verify that traffic is egressing the SD-WAN member interfaces. The column **SD-WAN Rule Name** indicates the name of the SD-WAN rule that applies. No name in this column means that the flow was routed according to the default **Implicit** SD-WAN rule.

Alternatively, you can use verbosity levels 4 to 6 to view the egress interface using the CLI packet capture tool.

The example on this slide shows a capture with a filter that matches any packets with the SYN flag on and port 443. So, the sniffer output shows all SYN packets to port 443 (HTTPS).

DO NOT REPRINT**© FORTINET**

Policy Route Lookup

- SD-WAN fields in proute list

```
# diagnose firewall proute list
list route policy info(vf=root):
  SD-WAN rule ID and rule name
  SD-WAN members by order of preference
  SD-WAN members by order of preference

id=2131034113(0x7f050001) vwl_service=1(Critical-DIA) vwl_mbr_seq=1 2 dscp_tag=0xfc despite flags=0x0 tos=0x00
tos_mask=0x00 protocol=0 sport=0-65535 iif=(any) dport=1-65535 path(2) oif=3(port1) oif=4(port2)
source(1): 10.0.1.0-10.0.1.255
destination wildcard(1): 0.0.0.0/0.0.0.0
internet service(3): GoToMeeting(4294836842,0,0,0, 16354) Microsoft.Office.365.Portal(4294837313,0,0,0,0,
41468) Salesforce(4294837785,0,0,0, 16920)
hit_count=34219 last_used=2024-09-11 07:37:43

id=2131034115(0x7f050003) vwl_service=3(Corp) vwl_mbr_seq=3 4 dscp_tag=0xfc last used flags=0x0 tos=0x00
tos_mask=0x00 protocol=0 sport=0-65535 iif=(any) dport=1-65535 path(3) oif=19(T_INET) oif=20(T_MPLS)
source(1): 10.0.1.0-10.0.1.255
destination(1): 10.0.0.0-10.255.255.255
hit_count=13 last_used=2024-09-11 07:38:27
```

Outgoing interface by order of preference



This slide shows an example of a policy route list output.

Note the fields `vwl_service` and `vwl_mbr`, which indicate the SD-WAN rule that allowed the route creation and the SD-WAN member used to steer the traffic.

The ID displayed in the `diagnose firewall proute list` command output corresponds to the ID displayed in the debug flow output when a packet matches a rule. The output also includes the outgoing interface list, with the interface preference sorted from left to right.

For troubleshooting purposes, the output of the `diagnose firewall proute list` command also displays the rule hit count and the last time the rule was hit.

DO NOT REPRINT
© FORTINET

SD-WAN Fields in Session List

- CLI commands
 - diag sys session filter
 - diag sys session list
 - diag sys session6 list
- SD-WAN information for the session
 - sdwan_mbr_seq
 - sdwan_service_id
 - None if traffic matches default SD-WAN rule
 - None if not an SD-WAN session

```
# diagnose sys session list
session info: proto=6 proto_state=11 duration=5
expire=3596 timeout=3600 flags=00000000 socktype=0

... output omitted ...

misc=0 policy_id=3 auth_info=0 chk_client_info=0 vd=0
serial=000b2f2d tos=ff/ff app_list=2002 app=16060
url_cat=0
sdwan_mbr_seq=4 sdwan_service_id=2
rpdb_link_id=ff000002 ngfwid=n/a
npu_state=0x001008
```



The CLI command `diagnose sys session filter` allows you to filter the sessions to display. Then, use the command `diagnose sys session list` to display the session detail.

You can use `diagnose sys session filter ?` to view available filters, `diagnose sys session filter` to see active filters, and `diagnose sys session filter clear` to reset the filters settings. Use the command `diagnose sys session list` for IPv4 traffic, and `diagnose sys session6 list` for IPv6 traffic.

The right part of this slide shows an example output with detailed information about the session table entry.

Only information related to SD-WAN is highlighted. From left to right, and from top to bottom:

- The ID of the matching policy
- The application ID (used for SD-WAN rules with application criteria)
- The SD-WAN-specific session information. `sdwan_mbr_seq` and `sdwan_service_id` indicate the SD-WAN member ID and the SD-WAN rule ID in use, respectively. If the session matched the SD-WAN implicit rule, and therefore was handled using standard FIB routing, those SD-WAN fields do not appear.

DO NOT REPRINT**© FORTINET**

SD-WAN Monitoring

- SD-WAN requires regular, or event triggered monitoring
- SD-WAN specific monitoring tools
 - Dashboard widget
 - Graphical view on SD-WAN configuration menus
 - Traffic distribution
 - Rule overview
 - Performance graphs of members
 - System event log messages for SD-WAN
 - Traffic logs with SD-WAN columns
- Other FortiGate tools
 - IPsec monitoring for overlay tunnels
 - Routing table and Proute list
 - Session table
 - Sniffer traces



Because of the dynamic nature of SD-WAN routing, you should periodically check the link health, routing behavior, and traffic distribution of your SD-WAN devices. You might want to check that traffic distribution corresponds to expectations with, for instance, only critical traffic steered through the costliest links. On the other hand, when you detect an unexpected event on your network, you want to be able to easily understand the impact on SD-WAN traffic steering and routing decisions.

For those activities, you can count on some general FortiGate monitoring tools you already know, like the routing table, the session table or the embedded packet capture tool. You can also benefit from dedicated SD-WAN monitoring tools provided by the FortiGate GUI interface. Through the next few slides, you will discover the SD-WAN monitoring tools provided by the FortiGate GUI.

DO NOT REPRINT
© FORTINET

Dashboard—Network

- Network dashboard pane with SD-WAN, routing, and IPsec widgets

The screenshot displays the Network dashboard with three main sections:

- Static & Dynamic Routing:** A donut chart showing 12 total routes, with 8 Static and 4 Connected.
- IPsec:** A table listing three tunnels: T_INET_1 (Remote Gateway 100.64.1.9, Peer ID 100.64.1.9), T_INET (Remote Gateway 100.64.1.1, Peer ID 100.64.1.1), and T_MPLS (Remote Gateway 172.16.1.5, Peer ID 172.16.1.5).
- SD-WAN:** A summary card showing 4 Total SD-WAN links, all in green (Latency < 150ms). A red arrow points from this card to a detailed SD-WAN interface table below.

A blue button at the bottom of the SD-WAN card says "Click to expand".

Interface	Status	Scalars	Upload	Download
port1	Up	7	4.96 kbps	4.99 kbps
port2	Up	2	1.75 kbps	1.75 kbps
T_INET	Up	1	640 kbps	640 kbps
T_MPLS	Up	2	1.21 kbps	1.21 kbps

© Fortinet Inc. All Rights Reserved. 32

By default, the **Network** dashboard includes three widgets useful for SD-WAN monitoring. It should be the first place you look when you want to check the SD-WAN behavior on a FortiGate device.

From this page you can view:

- Static and dynamic routing
- IPsec tunnels status
- SD-WAN interfaces performances

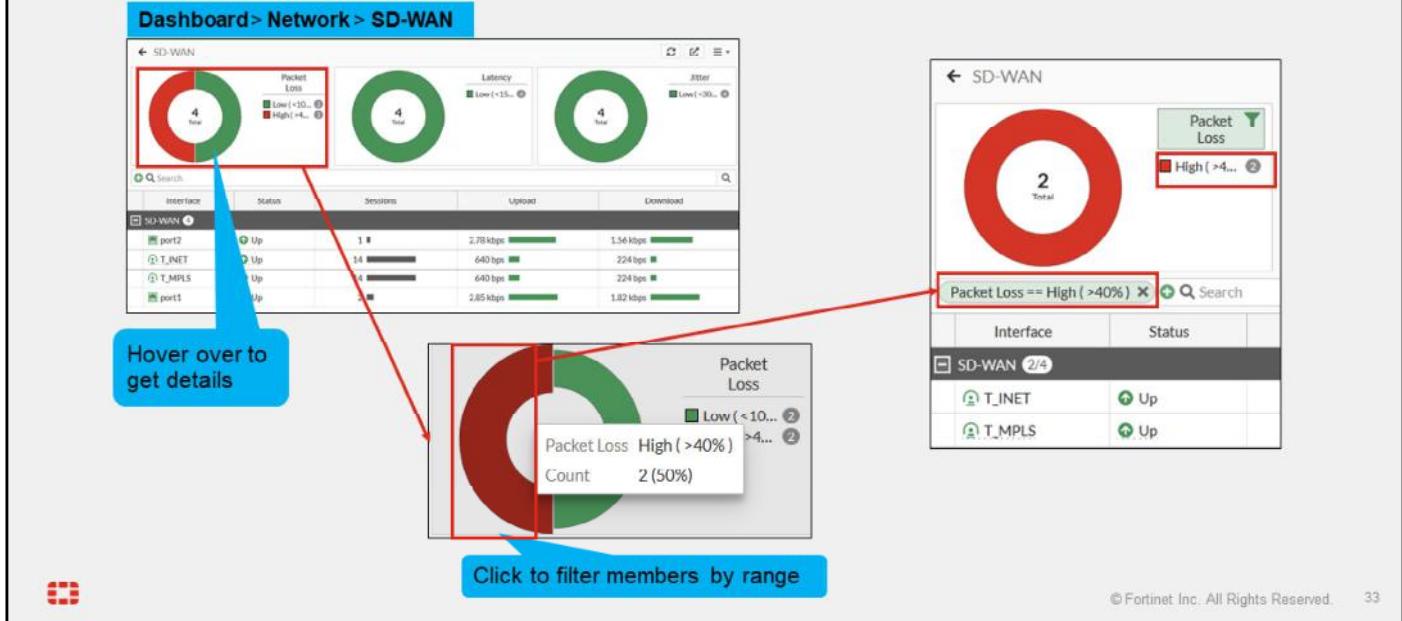
Click any widget to expand and get additional details per topic. The SD-WAN widget provides an overview of the status of each monitored SD-WAN link.

The example on this slide shows the details you can view by clicking the SD-WAN widget.

DO NOT REPRINT
© FORTINET

Dashboard—SD-WAN Widget Details

- Consolidated view of member health and utilization



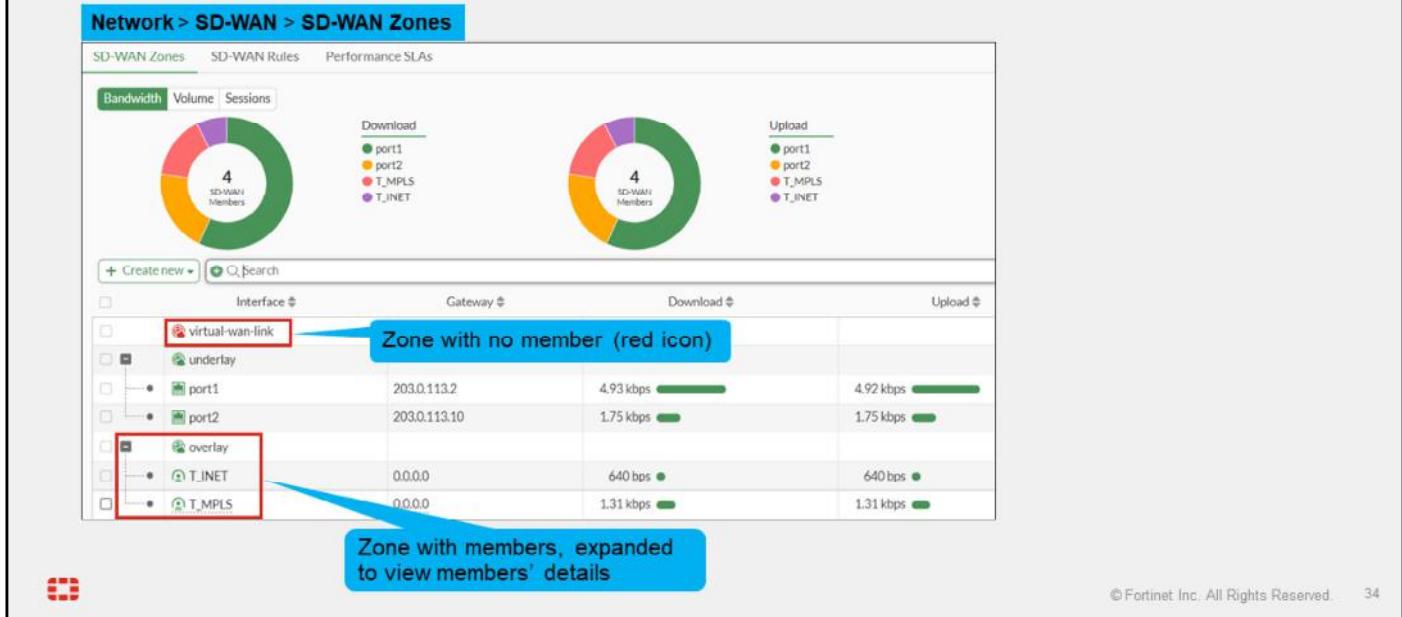
From the SD-WAN widget detailed view, you can hover over the graph to view details. You can also click a graph part to filter the member list and display only the members that match the selected criteria.

In the example shown on this slide, two members have a high rate of packet loss—above 40%. This is displayed on the diagram as the red part of the circle. When you click this red part of the circle, FortiGate filters the member list to display only members with a high rate of packet loss—for this example, T_INET and T_MPLS.

DO NOT REPRINT
© FORTINET

SD-WAN Interfaces and Zones Summary

- Synthetic view of zones and members configuration and status



The **SD-WAN Zones** page in the menu **Network > SD-WAN**, provides a synthetic view of the SD-WAN zones and members configuration. Note that zones with no member appear with a red icon. Next to zones with members is a + sign that you can click to display the members.

The diagram at the top of the page displays traffic allocation per interface, evaluated by bandwidth use, volume, or number of sessions.

From this menu, you can double-click zone or interface lines to adjust their configurations.

DO NOT REPRINT**© FORTINET**

Traffic Distribution

- View traffic distribution on the **SD-WAN Zones** page:



© Fortinet Inc. All Rights Reserved. 35

From the SD-WAN zone page presented on the previous slide, you can monitor the traffic distribution over the SD-WAN members. The page contains graphs that display traffic distribution based on bandwidth, volume, or sessions. Note that bandwidth refers to the data rate, while volume refers to the amount of data.

You can also hover over a member or the graph to get a specific amount of bandwidth, volume, or sessions.

DO NOT REPRINT
© FORTINET

SD-WAN Rules Overview

- Summary view of SD-WAN rules

	Name	Source	Destination	Criteria	Members	Hit Count	Last Used	Performance SLA
IPv4 2	1 Critical-DIA LAN-net	GoToMeeting Microsoft.Office.365.Portal Salesforce	port1 ✓ port2	0	Yesterday			
Implicit 1	2 Corp LAN-net	Corp-net	Latency	T_INET ✓ T MPLS ✓	63	32 minutes ago	VPN_PING	
	sd-wan all	all	Source IP	any	0	58 minutes ago		

© Fortinet Inc. All Rights Reserved. 36

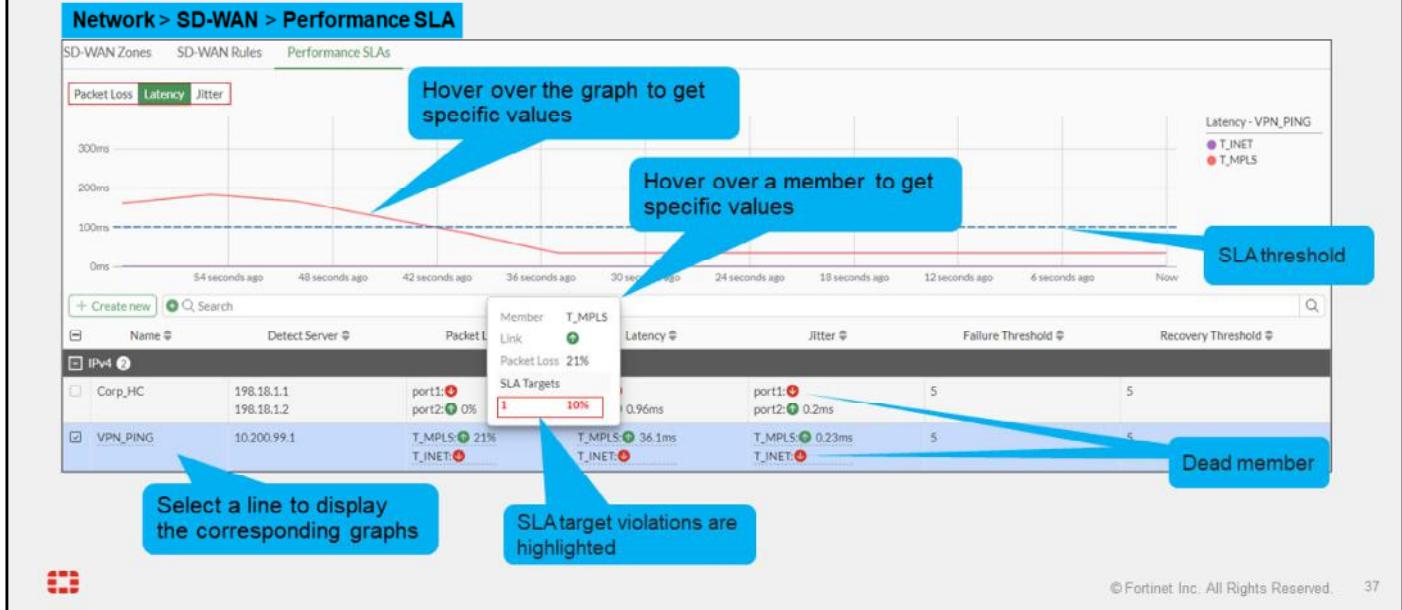
The **SD-WAN Rules** page in the menu **Network > SD-WAN**, provides a summary view of SD-WAN rules configuration. From this list you can quickly view the main configuration parameters of a rule, members in use, and the last time the rule was used to steer traffic. With drag-and-drop you can re-order the rules. You can also double-click any user-defined rule to adjust its configuration.

If you want to adjust the view, you can reorder the column with drag-and-drop, add or remove columns with the parameter menu on the left side of the top bar. You can also filter on any column to adjust the display to what you are looking for. Hover over the columns corner to view the filter configuration icon.

DO NOT REPRINT
© FORTINET

Member State and Performance

- Graphical view of performance SLA measurement over the past 10 minutes



You can browse to the **Performance SLAs** page to monitor the health of your members. You first select the performance SLA you want to check (VPN_PING in the example). The graphs on the page then display the packet loss, latency, and jitter of each member using the selected performance SLA. Note that the information shown on the graphs is limited to the last minute.

If you configured an SLA target, it appears on the graph as a horizontal dotted line. You can quickly detect the member status. The FortiGate GUI shows alive members with a green up arrow icon, and dead members with a red down arrow icon. For a missed SLA target, FortiGate highlights the impacted metric in red. It is important to note that the green up arrows indicate only that the server is responding to the health check, regardless of the packet loss, latency, and jitter values. It is not an indication that any of the SLAs are being met.

You can display graphs for **Packet Loss**, **Latency**, or **Jitter** by selecting the upper tabs. You can also hover over the graph to get a specific amount of packet loss, latency, or jitter. Because link quality plays an important role in link selection when using SD-WAN, monitoring the link quality status of the SD-WAN member interfaces is a good practice. You should investigate any prolonged issues with packet loss, latency, or jitter to ensure your network traffic does not experience outages or degraded performance.

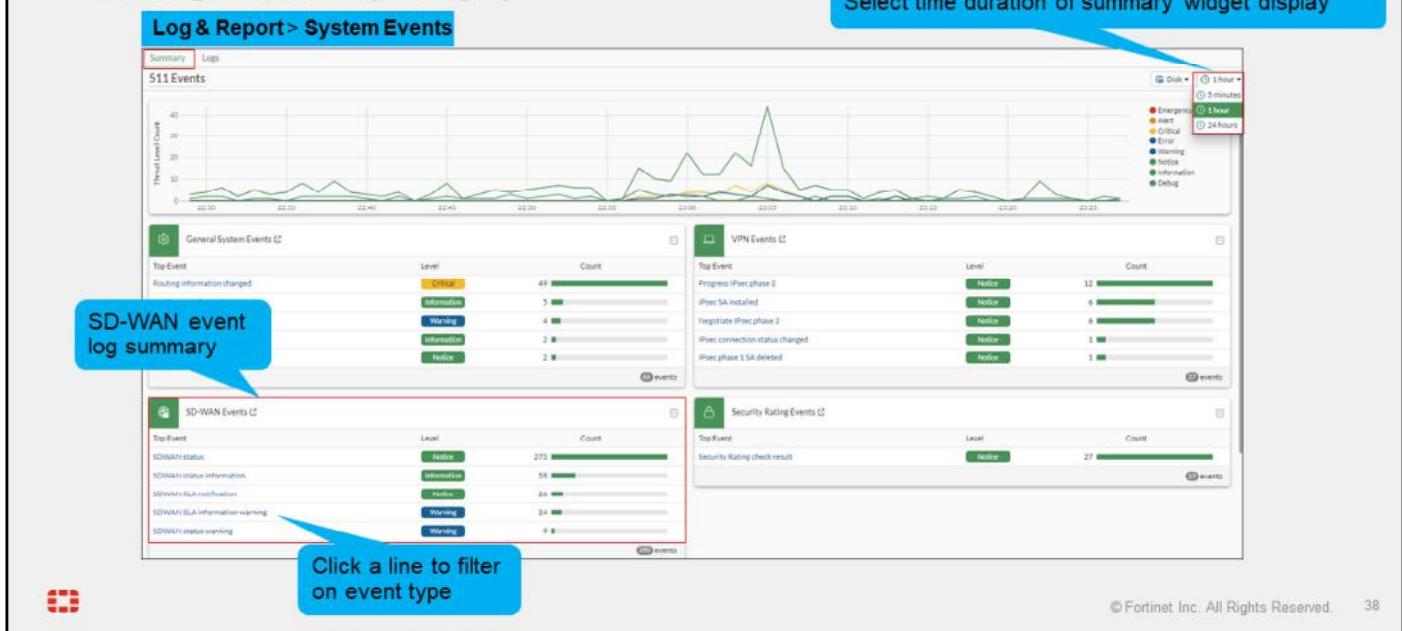
In the example shown on this slide, the **VPN_PING** performance SLA is selected and reports that **T_MPLS** is alive and **T_INET** is dead. The graph shows latency for both monitored interfaces over the past minute.

From this page you can also update a performance SLA configuration, or create a new one.

DO NOT REPRINT**© FORTINET**

System Event Logs

- Event log overview by category



From the **System Events** log summary menu, you get an overview of recent events ordered by category and message type. By default, the summary page considers logs received over the past 5 minutes. You can adjust to get a summary over the past 1 hour or past 24 hours. In the **SD-WAN Events** summary widget, you will log events about SLA status changes, priority member order changes, and so on. The **VPN Events** widget provides useful information to understand overlay links behavior.

Click the widget title to view the corresponding logs in detail. Click an event name to view the logs filtered by event name.

DO NOT REPRINT

© FORTINET

SD-WAN Events

- View SD-WAN member state changes

The screenshot shows the SD-WAN Events log and its detailed view for a specific log entry.

Log & Report > System Events > SD-WAN Events

Date/Time	Level	Message	Log Description
2024/09/11 23:42:58	Notice	Service will be redirected in sequence order.	SDWAN status
2024/09/11 23:42:58	Notice	Member link is available. Start forwarding traffic.	SDWAN status
2024/09/11 23:42:57	Notice	SD-WAN health-check member changed state.	SDWAN SLA notification
2024/09/11 23:42:43	Notice	Service will be redirected in sequence order.	SDWAN status
2024/09/11 23:42:43	Notice	Member link is unreachable or miss threshold. Stop forwarding traffic.	SDWAN status
2024/09/11 23:42:43	Warning	SD-WAN health-check member changed state.	SDWAN SLA information warning
2024/09/11 23:42:37	Notice	Number of pass member changed.	SDWAN status
2024/09/11 23:42:37	Notice	Member status changed. Member out-of-sla.	SDWAN status
2024/09/11 23:42:28	Notice	Number of pass member changed.	SDWAN status
2024/09/11 23:42:28	Information	Member status changed. Member in sla.	SDWAN status information

Warning: port2 is detected dead and stopped forwarding traffic

port2 removed from the member preference list

Log details:
Member state changed from alive to dead for port2

Log Details

General	port2
Source	FGVh01TH12000078
Data	SD-WAN health-check member changed state.
Security	Warning
Other	7413643397241503749
ID	2024-09-11 23:42:44
Time	3
guid	3
epid	3
deviceid	3
deviceip	3
Log ID	0113022931
Type	event
Sub Type	adwan
Probe Protocol	ping
Log event original timestamp	17544122042944691200
Timestamp	-0700
Event Type	Health Check
Health Check	Corp_HC
Old Value	alive
New Value	dead
D-Time	2024-09-11 23:42:43
I-Time	1728323364
Device Name	branch2_fg



© Fortinet Inc. All Rights Reserved. 39

The **SD-WAN Events** subsection on the **Events** page displays logs that report the state changes of the SD-WAN members.

In most cases, you want to click a log to fully understand the event. For example, the warning log message highlighted in the table indicates that the state of **port2** changed from **alive** to **dead**. Although the details below this one are not shown, the logs report that port2 stopped forwarding traffic, and that the member preference in the rule that uses port2 was updated to remove port2.

DO NOT REPRINT

© FORTINET

Traffic Logs

- Enable SD-WAN columns to view SD-WAN-related information

The screenshot shows the 'Log & Report > Forward Traffic' interface. A red box highlights the 'SD-WAN Rule Name' and 'SD-WAN Quality' columns in the table. Below the table, a 'Select Columns' dialog is open, also with a red box highlighting the 'SD-WAN Rule Name' and 'SD-WAN Quality' options. Callouts point from these highlighted areas to blue boxes labeled 'Available columns regarding SD-WAN', 'Rule name', and 'Selected member and reason'.

Date/Time	Source	Destination	Application Name	Result	Policy ID	SD-WAN Rule Name	SD-WAN Quality
2024/09/12 00:00:59	10.0.2.101	35.183.176.123 (www.fortinet.com)	HTTPBROWSER	✓ Accept (UTM Allowed)	DIA (1)		
2024/09/12 00:00:24	10.0.2.101	10.1.0.7	HTTP	✓ Accept (392 B / 1.07 kB)	To Hub0-Overlay (2)	Corp	Seq_num(3 T_INET overlay), alive, latency: 1.260, selected
2024/09/12 00:00:24	10.0.2.101	8.8.8.8 (dns.google)	DNS	✓ Accept (73 B / 140 B)	DIA (1)		
2024/09/12 00:00:24	10.0.2.101	8.8.8.8 (dns.google)	DNS	✓ Accept (124 B / 366 B)	DIA (1)		
2024/09/12 00:00:03	10.0.2.101	217.180.209.214 (ntp1.versadns.com)	NTP	✓ Accept (UTM Allowed)	DIA (1)		

© Fortinet Inc. All Rights Reserved. 40

The **Forward Traffic** logs page is useful to identify how sessions are distributed in SD-WAN and the reason. Make sure to enable the **SD-WAN Rule Name** and **SD-WAN Quality** columns, which are disabled by default. The former specifies the matched SD-WAN rule for a session, while the latter identifies the member to which the session was steered and the reason.

Note that the **Implicit** SD-WAN rule name does not appear in the **SD-WAN Rule Name** column. When the traffic is steered according to this rule, the field remains empty.

The table on this slide shows multiple sessions. The second session in the table was identified as an **HTTP** application, matched the **Corp** rule, and was sent to **T_INET**. The reason that **T_INET** was selected is because it had the lowest latency.

DO NOT REPRINT**© FORTINET**

Knowledge Check

1. What item is defined in an SD-WAN rule?
 A. SLA criteria
 B. Security profile
 C. Logging options

2. What is the routing behavior in an SD-WAN context?
 A. Static routes apply first.
 B. Regular policy routes apply first.
 C. SD-WAN policy routes apply first.

3. Where can you review SD-WAN event history?
 A. Forward Traffic in Log & Report
 B. SD-WAN widget on the dashboard
 C. SD-WAN widget in System Events



DO NOT REPRINT

© FORTINET

Lesson Progress



SD-WAN Basics



SD-WAN Fundamentals



SD-WAN Basic Monitoring



© Fortinet Inc. All Rights Reserved.

42

Congratulations! You have completed this lesson.

Now, you will review the objectives covered in this lesson.

DO NOT REPRINT

© FORTINET

Review

- ✓ Describe SD-WAN
- ✓ Identify the main use cases for SD-WAN
- ✓ Configure SD-WAN on FortiGate
- ✓ Describe and analyze routing behavior in an SD-WAN context
- ✓ Monitor SD-WAN behavior, link usage, and quality status



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

By mastering the objectives covered in this lesson, you learned how to configure, maintain, and monitor a FortiGate SD-WAN solution.

DO NOT REPRINT

© FORTINET

FORTINET
Training Institute

FortiOS Administrator

High Availability

 FortiOS 7.6

Last Modified: 6 October 2025

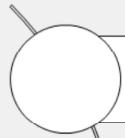
© Fortinet Inc. All Rights Reserved. 1

In this lesson, you will learn about the fundamentals of FortiGate high availability (HA) and how to configure it. FortiGate HA provides a solution for enhanced reliability and increased performance.

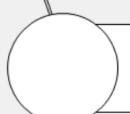
DO NOT REPRINT

© FORTINET

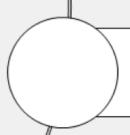
Lesson Overview



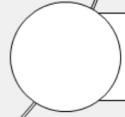
HA Operation Modes



HA Cluster Synchronization



HA Failover



Monitoring



© Fortinet Inc. All Rights Reserved.

2

In this lesson, you will learn about the topics shown on this slide.

DO NOT REPRINT**© FORTINET**

HA Operation Modes

Objectives

- Identify the different operation modes for HA with the FortiGate Clustering Protocol (FGCP)
- Explain the primary FortiGate election in an HA cluster



© Fortinet Inc. All Rights Reserved.

3

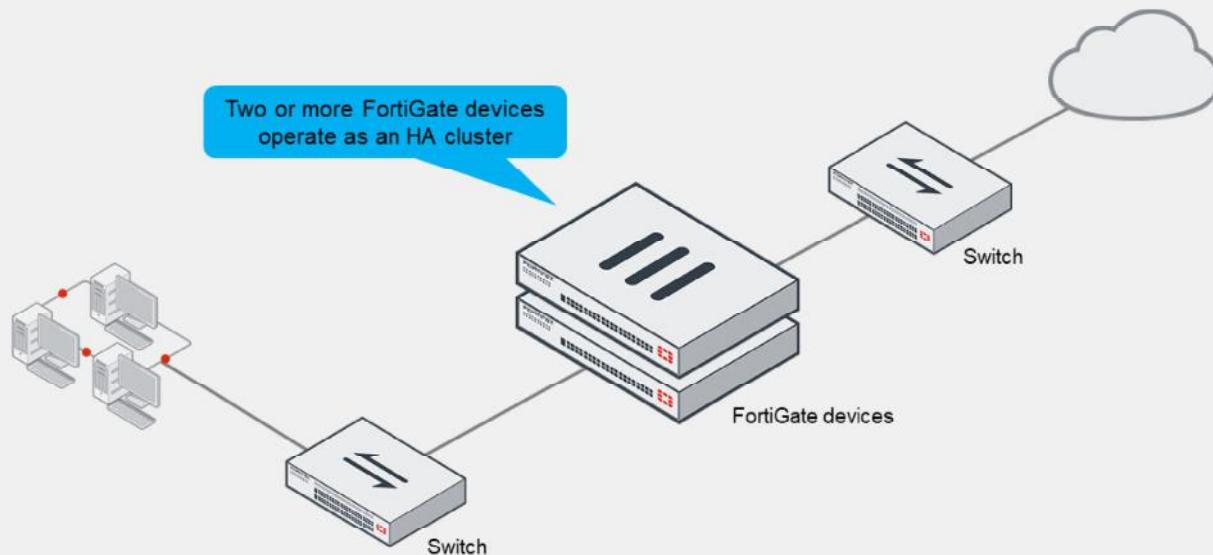
After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in HA operation modes and primary FortiGate election, you will be able to choose and implement the right HA operation mode in your network based on your requirements.

DO NOT REPRINT

© FORTINET

What Is FortiGate HA?



© Fortinet Inc. All Rights Reserved.

4

FortiGate HA uses FGCP to discover members, elect the primary FortiGate, synchronize data among members, and monitor the health of members. FortiGate HA links and synchronizes two or more FortiGate devices to form a cluster for redundancy and performance purposes.

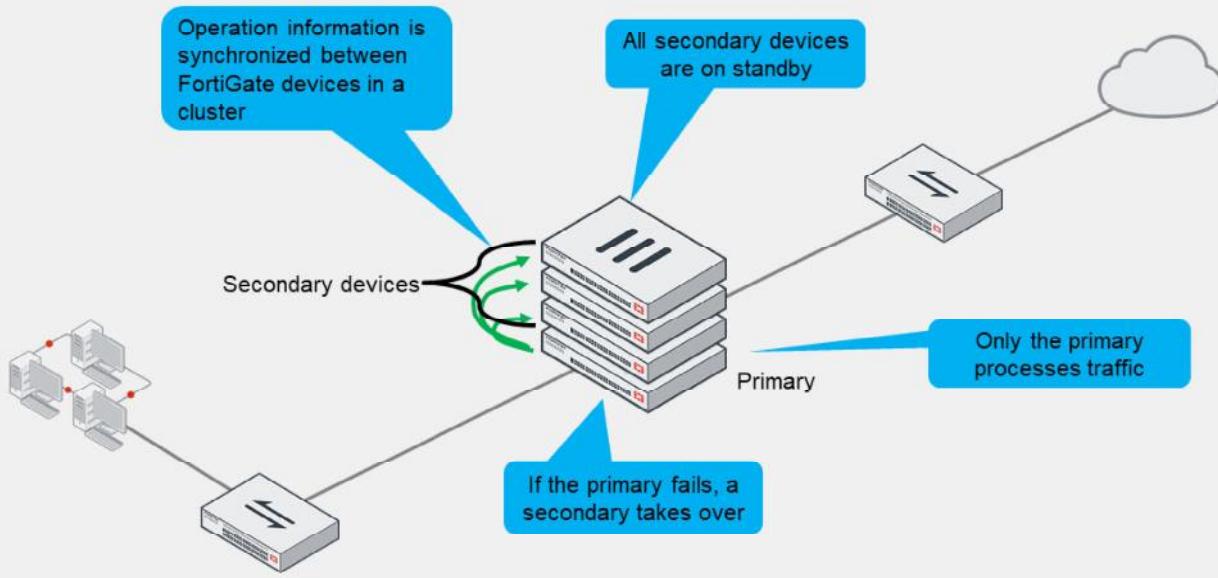
A cluster includes one device that acts as the primary FortiGate. The primary sends its complete configuration to other members that join the cluster, overwriting their configuration (except for a few settings). It also synchronizes session information, forwarding information base (FIB) entries, FortiGuard definitions, and other operation-related information to the secondary devices, which are also known as standby devices.

The cluster shares one or more heartbeat interfaces among all devices—also known as members—for synchronizing data and monitoring the health of each member.

There are two HA operation modes available: active-active and active-passive. Now, you will learn about the differences.

DO NOT REPRINT**© FORTINET**

Active-Passive HA



© Fortinet Inc. All Rights Reserved.

5

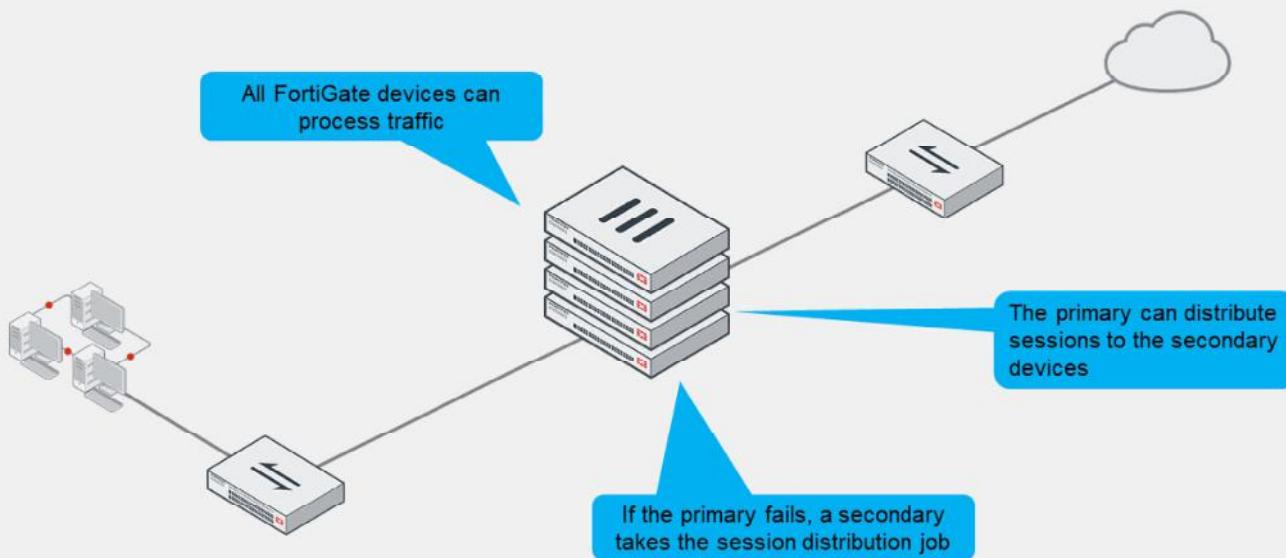
In active-passive mode, the primary FortiGate is the only FortiGate that actively processes traffic. Secondary FortiGate devices remain in passive mode, monitoring the status of the primary device.

In either of the two HA operation modes, the operation information (sessions, FIB entries, and so on) of the primary FortiGate is synchronized with secondary devices. If a problem is detected on the primary FortiGate, one of the secondary devices takes over the primary role. This event is called an *HA failover*.

If a secondary FortiGate device fails, the primary updates its list of available secondary FortiGate devices. It also starts monitoring for the failed secondary, waiting for it to come online again.

DO NOT REPRINT**© FORTINET**

Active-Active HA



© Fortinet Inc. All Rights Reserved.

6

The other HA mode is active-active.

Like active-passive HA, in active-active HA, the operation-related data is synchronized between devices in the cluster. Also, if a problem is detected on the primary device, one of the secondary devices takes over the role of the primary to process the traffic.

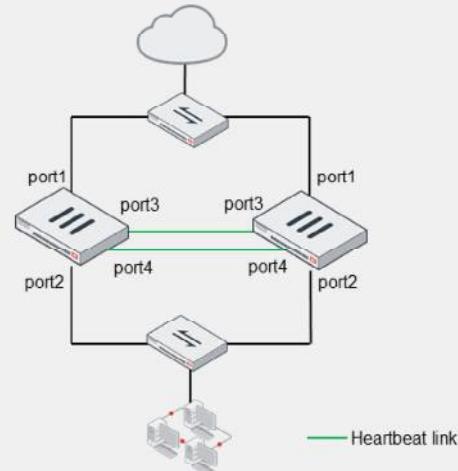
However, one of the main differences from active-passive mode is that in active-active mode, all cluster members can process traffic. That is, based on the HA settings and traffic type, the primary FortiGate can distribute supported sessions to the secondary devices. If one of the secondary devices fails, the primary also reassigns sessions to a different secondary FortiGate.

DO NOT REPRINT

© FORTINET

HA Requirements

- All members must have the same:
 - Model
 - Firmware version
 - Licensing
 - If different, the cluster uses the lowest-level license
 - Hard drive configuration
 - Operating mode (management VDOM)
- Setup:
 - Same HA group ID, group name, password, and heartbeat interface settings
 - Identical interfaces on each member must be connected to the same layer 2 network
- Best practice:
 - Use at least two heartbeat interfaces
 - Initially, switch DHCP and PPPoE interfaces to static configuration



Example:

```
config system ha
  set mode a-p
  set group-id 10
  set group-name "Training"
  set password <password>
  set hbdev "port3" 10 "port4" 20
end
```

© Fortinet Inc. All Rights Reserved.

7

To successfully form an HA cluster, you must ensure that the members have the same:

- Model: hardware model or VM model
- Firmware version
- Licensing: includes the FortiGuard license, virtual domain (VDOM) license, FortiClient license, and so on
- Hard drive configuration: the same number and size of drives and partitions
- Operating mode: the operating mode—NAT mode or transparent mode—of the management VDOM. VDOMs divide a FortiGate device into two or more virtual units, essentially dividing one physical firewall into additional logical devices.

If the licensing level among members isn't the same, the cluster resolves to use the lowest licensing level among all members. For example, if you purchase FortiGuard Web Filtering for only one of the members in a cluster, none of the members will support FortiGuard Web Filtering when they form the cluster.

From a configuration and setup point of view, you must ensure that the HA settings on each member have the same group ID, group name, password, and heartbeat interface settings. Try to place all heartbeat interfaces in the same broadcast domain, or for two-member clusters, connect them directly. It's also a best practice to configure at least two heartbeat interfaces for redundancy purposes. This way, if one heartbeat link fails, the cluster uses the next one, as indicated by the priority and position in the heartbeat interface list. In the example shown, port3 would have a priority of 10 and port4 would have a priority of 20, making port4 the preferred interface.

If you are using DHCP or Point-to-Point Protocol over Ethernet (PPPoE) interfaces, use static configuration during the cluster initial setup to prevent incorrect address assignment. After the cluster is formed, you can revert to the original interface settings.

**DO NOT REPRINT
© FORTINET**

Primary FortiGate Election—Override Disabled

- Override disabled (default)
 - Force a failover

```
# diagnose sys ha reset-uptime
```

 - Check the HA uptime difference:

```
# diagnose sys ha reset-uptime
```

Digitized by srujanika@gmail.com

- Check the HA uptime difference:

- Check the HA uptime difference

* diagnose sys. ha dump by valuator

• diagnose by na dumpt by verlaat

ECU/Mxx92; uptime/reset cnt=7814/0

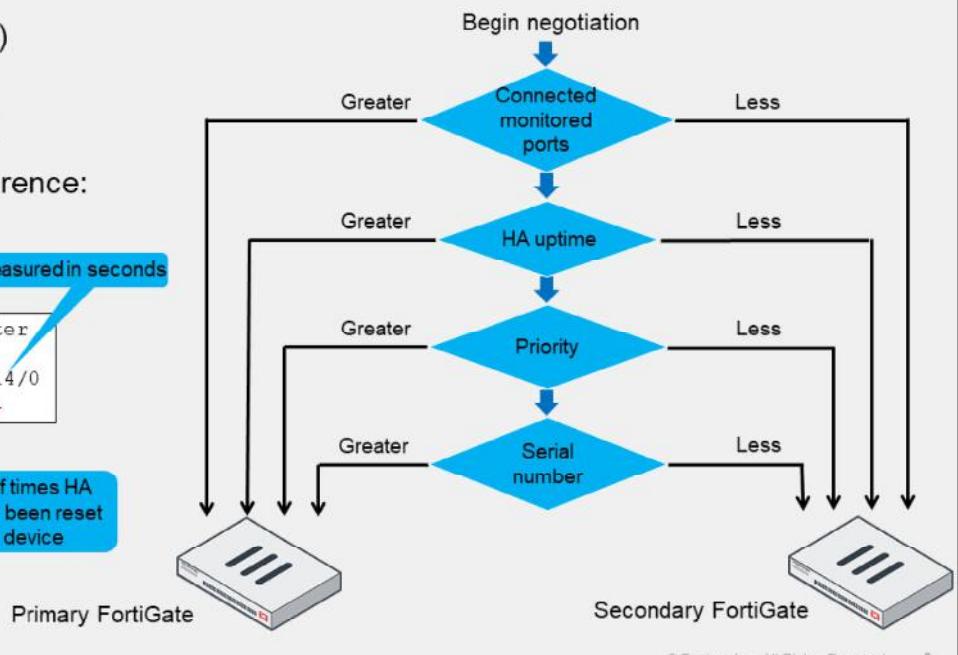
FGVMXX92....uptime/reset_cnt=7814/0
FGVMXX92....uptime/reset_cnt=0/1

FGVMXX93:...uptime/reset_cnt=0/1

www.ijerpi.org | 10

0 is for the device with the lowest HA uptime

Number of times HA
uptime has been reset
for this device



© Fortinet Inc. All Rights Reserved.

This slide shows the different criteria that a cluster considers during the primary FortiGate election process. The criteria order evaluation depends on the HA override setting. This slide shows the order when the HA override setting is disabled, which is the default behavior. Note that the election process stops at the first matching criteria that successfully selects a primary FortiGate in a cluster.

1. The cluster compares the number of monitored interfaces that have a status of up. The member with the most available monitored interfaces becomes the primary.
 2. The cluster compares the HA uptime of each member. The member with the highest HA uptime, by at least five minutes, becomes the primary.
 3. The member with the highest priority becomes the primary.
 4. The member with the highest serial number becomes the primary.

When HA override is disabled, the HA uptime has precedence over the priority setting. This means that if you must manually fail over to a secondary device, you can do so by reducing the HA uptime of the primary FortiGate. You can do this by running the `diagnose sys ha reset-uptime` command on the primary FortiGate, which resets its HA uptime to 0.

Note that the `diagnose sys ha reset-uptime` command resets the HA uptime and not the system uptime. Also, note that if a monitoring interface fails or a member reboots, the HA uptime for that member is reset to 0.

This slide also shows how to identify the HA uptime difference between members. The member with 0 in the uptime column indicates the device with the lowest uptime. The example shows that the device with the serial number ending in 92 has an HA uptime that is 7814 seconds higher than the other device in the HA cluster. The `reset cnt` column indicates the number of times the HA uptime has been reset for that device.

DO NOT REPRINT
© FORTINET

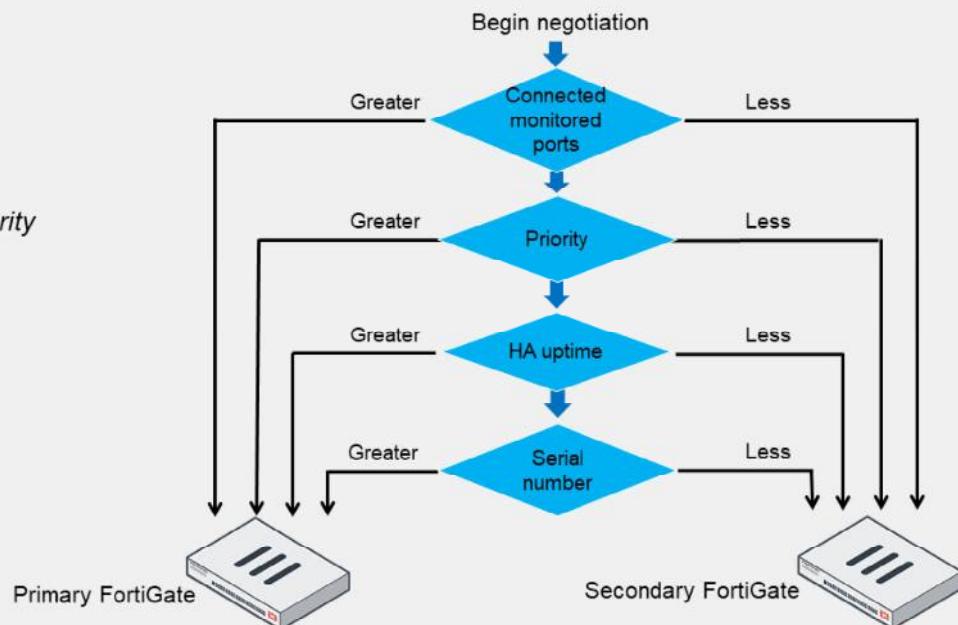
Primary FortiGate Election—Override Enabled

- Override enabled

```
config system ha
  set override enable
end
```

- Force a failover

- Change the HA priority



© Fortinet Inc. All Rights Reserved.

9

If the HA override setting is enabled, the priority is considered before the HA uptime.

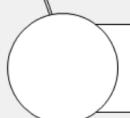
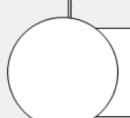
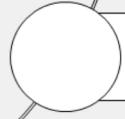
The advantage of this method is that you can specify which device is the preferred primary every time (as long as it is up and running) by configuring it with the highest HA priority value. The disadvantage is that a failover event is triggered not only when the primary fails, but also when the primary is available again. That is, when the primary becomes available again, it takes its primary role back from the secondary FortiGate that temporarily replaced it.

When override is enabled, the easiest way of triggering a failover is to change the HA priorities. For example, you can either increase the priority of one of the secondary devices, or decrease the priority of the primary.

The override setting and device priority values are not synchronized to cluster members. You must manually enable override and adjust the priority on each member.

DO NOT REPRINT**© FORTINET**

Lesson Progress

**HA Operation Modes****HA Cluster Synchronization****HA Failover****Monitoring**

© Fortinet Inc. All Rights Reserved.

10

Good job! You now understand HA operation modes and the election of the primary FortiGate in an HA cluster.

Now, you will learn about HA cluster synchronization.

DO NOT REPRINT**© FORTINET**

HA Cluster Synchronization

Objectives

- Identify the primary and secondary device tasks in an HA cluster
- Identify what is synchronized between HA cluster members



© Fortinet Inc. All Rights Reserved.

11

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

By demonstrating competence in cluster synchronization, you will be able to identify the tasks assigned to members based on their roles, as well as what information is synchronized between members.

DO NOT REPRINT**© FORTINET**

Primary FortiGate Tasks

- Broadcasts hello packets for member discovery and monitoring
- Synchronizes operation-related data such as:
 - Configuration (some settings are not synchronized)
 - FIB entries
 - DHCP leases
 - ARP table
 - FortiGuard definitions
 - IPsec tunnel SAs
 - Sessions (must be enabled)
- In active-active mode only:
 - Distributes sessions to secondary members



So, what are the tasks of a primary FortiGate device?

It monitors the cluster by broadcasting hello packets and listening for hello packets from other members. The members use the hello packets to identify whether other FortiGate devices are alive and available.

The primary FortiGate also synchronizes its operation-related data to the secondary members. Some of the data synchronized includes its configuration, FIB entries, DHCP leases, ARP table, FortiGuard definitions, and IPsec tunnel security associations (SAs). Note that some parts of the configuration are not synchronized because they are device-specific. For example, the host name, HA priority, and HA override settings are not synchronized.

Optionally, you can configure the primary FortiGate to synchronize qualifying sessions to all the secondary devices. When you enable session synchronization, the new primary can resume communication for sessions after a failover event. The goal is for existing sessions to continue flowing through the new primary FortiGate with minimal or no interruption.

In active-active mode only, a primary FortiGate is also responsible for distributing sessions to secondary members.

DO NOT REPRINT**© FORTINET**

Secondary FortiGate Tasks

- Broadcasts hello packets for member discovery and monitoring
- Synchronizes data from the primary
 - Changes made on secondary devices, however, are synced with other members if the cluster is in sync
- Monitors the health of the primary
 - If the primary fails, the secondary devices elect a new primary
- In active-active mode only
 - Processes traffic distributed by the primary



Now, take a look at the tasks of secondary FortiGate devices.

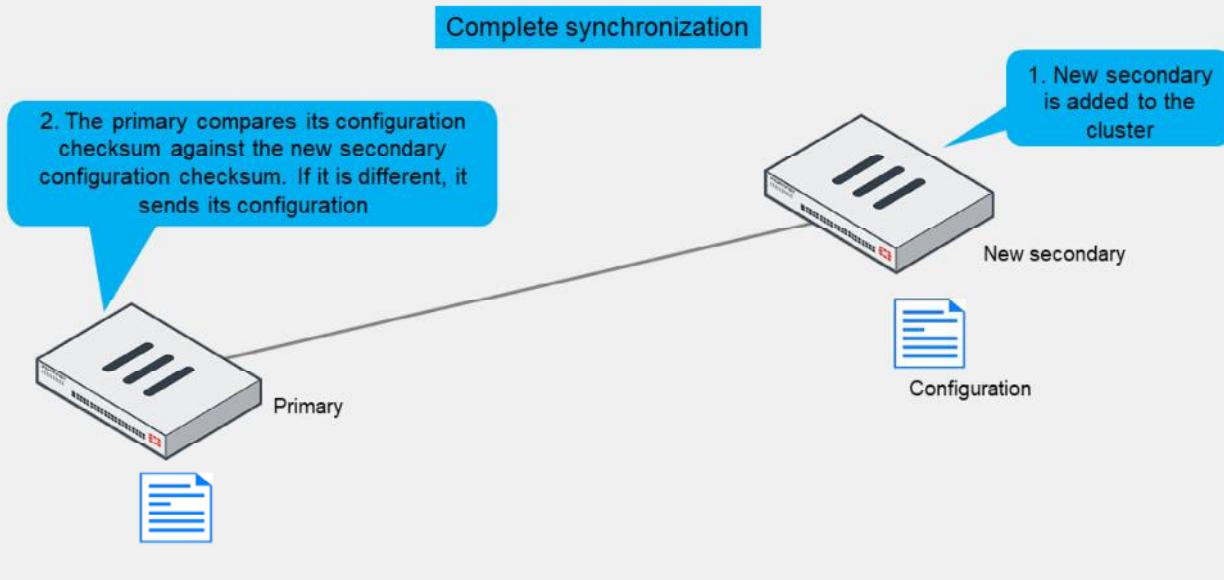
Like the primary, secondary members also broadcast hello packets for discovery and monitoring purposes.

In addition, in active-passive mode, the secondary devices act as a standby device, receiving synchronization data but not actually processing any traffic. If the primary FortiGate fails, the secondary devices elect a new primary. Once a cluster is in sync, configuration changes made on a secondary device are propagated to other members. In other words, with a cluster that is in sync, you can make changes on any of its members—not just the primary device only—and all changes are synchronized among the cluster members. However, it is recommended that you make configuration changes on the primary device because this prevents the loss of configuration changes if there are synchronization issues between cluster members.

In active-active mode, the secondary devices don't wait passively. They process all traffic assigned to them by the primary device.

DO NOT REPRINT
© FORTINET

HA Complete Configuration Synchronization



© Fortinet Inc. All Rights Reserved. 14

To prepare for a failover, an HA cluster keeps its configurations in sync.

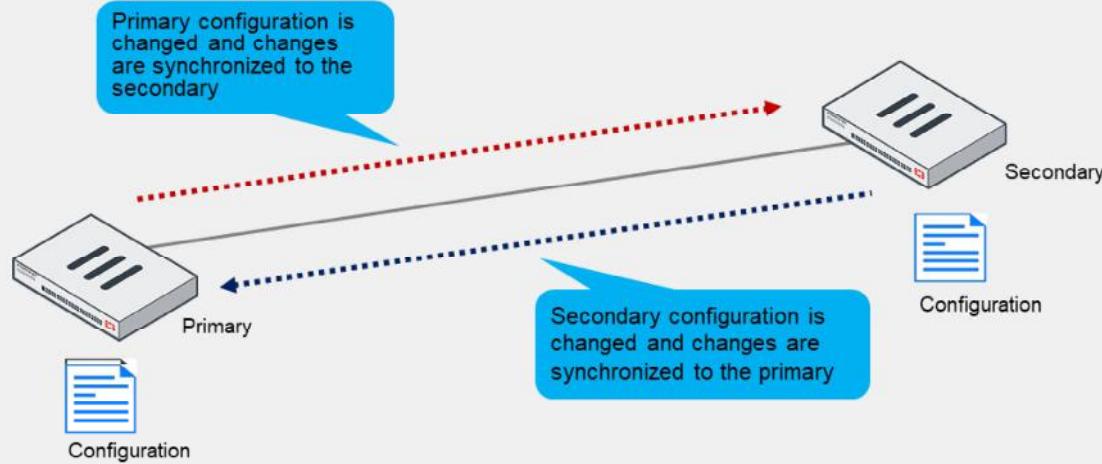
FortiGate HA uses a combination of both incremental and complete synchronizations.

When you add a new FortiGate to the cluster, the primary FortiGate compares its configuration checksum with the new secondary FortiGate configuration checksum. If the checksums don't match, the primary FortiGate uploads its complete configuration to the secondary FortiGate.

DO NOT REPRINT
© FORTINET

HA Incremental Configuration Synchronization

Incremental synchronization



After the initial synchronization is complete, whenever a change is made to the configuration of an HA cluster device (primary or secondary), incremental synchronization sends the same configuration change to all other cluster devices over the HA heartbeat link. An HA synchronization process running on each cluster device receives the configuration change and applies it to the cluster device. For example, if you create a firewall address object, the primary doesn't resend its complete configuration—it sends only the new object.

What Is Not Synchronized?

- These configuration settings are *not* synchronized between cluster members:
 - HA management interface settings
 - Default route for the reserved management interface
 - In-band HA management interface
 - HA override
 - HA device priority
 - HA virtual cluster priority
 - FortiGate host name
 - Ping server HA priorities
 - The HA priority (`ha-priority`) setting for a ping server or dead gateway detection configuration
 - Licenses
 - FortiGuard, FortiCloud activation, and FortiClient licensing
 - Cache
 - FortiGuard Web Filtering and email filter, web cache, and so on
 - GUI dashboard widgets



HA propagates more than just configuration details. Some runtime data, such as DHCP leases and FIB entries, are also synchronized.

By default, the cluster checks every 60 seconds to ensure that all devices are synchronized. If a secondary device is out of sync, its checksum is checked every 15 seconds. If the checksum of the out-of-sync secondary device doesn't match for five consecutive checks, FortiGate performs a complete resynchronization of that secondary device.

Not all the configuration settings are synchronized in HA. There are a few that are not, such as:

- System interface settings of the HA reserved management interface and the HA default route for the reserved management interface
- In-band HA management interface
- HA override
- HA device priority
- Virtual cluster priority
- FortiGate host name
- HA priority setting for a ping server (or dead gateway detection) configuration
- All licenses except FortiToken licenses (serial numbers)
- Cache
- GUI dashboard widgets

DO NOT REPRINT

© FORTINET

Lesson Progress



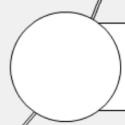
HA Operation Modes



HA Cluster Synchronization



HA Failover



Monitoring



© Fortinet Inc. All Rights Reserved.

17

Good job! You now understand HA cluster synchronization.

Now, you will learn about HA cluster failover protection types.

DO NOT REPRINT

© FORTINET

HA Failover



Objectives

- Identify the HA failover types



© Fortinet Inc. All Rights Reserved.

18

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

By demonstrating competence in failover types, you will be able to identify how enhanced reliability is achieved through HA failover protection.

DO NOT REPRINT

© FORTINET

Failover Protection

- Types:
 - Device failover
 - The secondary devices stop receiving hello packets from the primary
 - Link failover
 - The link of one or more monitored interfaces goes down
 - Remote link failover
 - One or more interfaces are monitored using the link health monitor
 - The primary fails if the accumulated penalty of all failed interfaces reaches the configured threshold
 - Memory-based failover
 - Memory utilization on the primary exceeds the configured threshold and monitoring period
 - SSD failover
 - FortiOS detects extended filesystem (Ext-fs) errors in an SSD
- Identify failover protection type by looking at:
 - Event logs, SNMP traps, and alert email record failover events
- Enable session synchronization for seamless session failover



The most common types of failovers are device failovers and link failovers. A device failover occurs when the secondary devices stop receiving hello packets from the primary. A link failover occurs when the link status of a monitored interface on the primary FortiGate goes down. You can configure an HA cluster to monitor one or more interfaces. If a monitored interface on the primary FortiGate is unplugged, or its link status goes down, a new primary FortiGate is elected.

When you configure remote link failover, FortiGate uses the link health monitor feature to monitor the health of one or more interfaces against one or more servers that act as beacons. The primary FortiGate fails if the accumulated penalty of all failed interfaces reaches the configured threshold.

If you enable memory-based failover, an HA failover is triggered when the memory utilization on the primary FortiGate reaches the configured threshold for the configured monitoring period. You can also enable SSD failover, which triggers a failover if FortiOS detects Ext-fs errors on an SSD on the primary FortiGate.

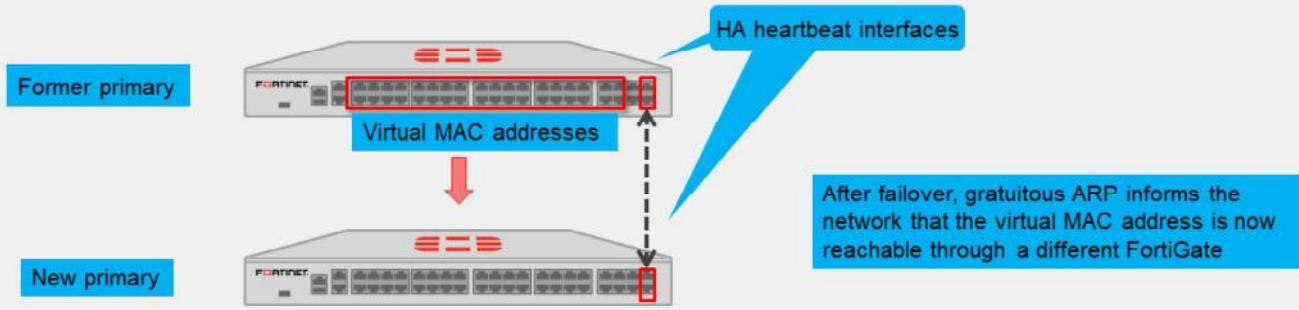
There are multiple events that might trigger an HA failover, such as a hardware or software failure on the primary FortiGate, an issue on one of the interfaces on the primary, or an administrator-triggered failover. When a failover occurs, an event log is generated. Optionally, you can configure the device to also generate SNMP traps and alert emails.

Enabling session pickup allows active sessions to be seamlessly handed picked up by the new primary in the event of an HA failover. In other words, users' sessions will continue uninterrupted, and they will not even know that a failover occurred. Note that there are some limitations to this – for example, any sessions that terminate at the FortiGate itself (e.g. SSL VPN, proxy sessions) cannot be handed off to another FortiGate and must be restarted on the new primary.

DO NOT REPRINT
© FORTINET

Virtual MAC Addresses and Failover

- On the primary, each interface is assigned a virtual MAC address
 - HA heartbeat interfaces are not assigned a virtual MAC address
- Upon failover, the newly elected primary adopts the same virtual MAC addresses as the former primary



© Fortinet Inc. All Rights Reserved. 20

To forward traffic correctly, a FortiGate HA solution uses virtual MAC addresses. When a primary joins an HA cluster, each interface is assigned a virtual MAC address. The HA group ID, virtual cluster ID (if enabled), and interface index number are used in the creation of virtual MAC addresses assigned to each interface. So, if you have two or more HA clusters in the same broadcast domain, and using the same HA group ID, you might get MAC address conflicts. For those cases, it is strongly recommended that you assign different HA group IDs to each cluster.

Through the heartbeats, the primary informs all secondary devices about the assigned virtual MAC address. Upon failover, a secondary adopts the same virtual MAC addresses for the equivalent interfaces.

The new primary broadcasts gratuitous ARP packets, notifying the network that each virtual MAC address is now reachable through a different switch port.

Note that the MAC address of a reserved HA management interface is not changed to a virtual MAC address. Instead, the reserved management interface keeps its original MAC address.

DO NOT REPRINT

© FORTINET

Lesson Progress



HA Operation Modes



HA Cluster Synchronization



HA Failover



Monitoring



© Fortinet Inc. All Rights Reserved.

21

Good job! You now understand HA failover.

Now, you will learn about monitoring an HA cluster.

DO NOT REPRINT**© FORTINET**

Monitoring

Objectives

- Verify the normal operation of an HA cluster
- Configure the HA management interface



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

By demonstrating competence in monitoring FortiGate HA, you will be able to verify its operational status, and make changes to suit your business and security requirements.

DO NOT REPRINT

© FORTINET

Checking the HA Status on the GUI

The screenshot shows two main sections of the FortiGate GUI:

- System > HA**: A table listing cluster members. The first row shows NGFW-1 (Primary) with a priority of 50, serial number FGVM010000077649, and a red box around its "Role" column which says "Primary". The second row shows NGFW-2 (Secondary) with a priority of 25, serial number FGVM010000077650, and a red box around its "Role" column which says "Secondary". Other columns include Status, Priority, Hostname, Serial No., System Uptime, Sessions, and Throughput.
- Dashboard > Status**: A summary of HA status. It shows Mode: Active-Passive, Group: fortinet, Primary: NGFW-1, Secondary: NGFW-2, Uptime: -8h-26m-4s, and State Changed: -8h-37m-32s. A blue callout bubble points to the "More columns available" link in the sidebar.

Sidebar (Select Columns):

- Best Fit All Columns
- Reset Table
- Select Columns
- Serial No. (checked)
- Role (checked)
- System Uptime (checked)
- Sessions (checked)
- Throughput (checked)
- AV Events
- Bytes
- Checksum
- Cluster Uptime
- CPU
- Down Ports
- IPS Events
- IPv6 Sessions
- Packets
- RAM
- Virtual Domains

© Fortinet Inc. All Rights Reserved. 23

The **HA** page on the FortiGate GUI shows important information about the health of your HA cluster. For each cluster member, the page shows whether the member is synchronized or not, and its status, host name, serial number, role, priority, uptime, active sessions, and more.

On the **HA** page, you can remove a device from a cluster. When you remove a device from HA, the device operation mode is set to standalone. You can also enable more columns that display other important information about each member, such as the checksum, CPU, and memory.

You can also add the **HA Status** widget on the **Dashboard** page. The widget provides a summary of the HA status on the device.

DO NOT REPRINT

© FORTINET

Checking the HA Status on the CLI

```
# get system ha status
HA Health Status: OK
Model: FortiGate-VM64-KVM
Mode: HA A-P
Group Name: Training
Group ID: 0
Debug: 0
Cluster Uptime: 0 days 2h:5m:42s
Cluster state change time: 2024-09-16 09:17:51
Primary selected using:
<2024/09/16 09:17:51> vcluster-1: FGVM010000077649 is selected as the primary because its override priority is
larger than peer member FGVM010000077650.
ses_pickup: disable
override: disable
Configuration Status:
FGVM010000077649 (updated 4 seconds ago): in-sync
FGVM010000077649 cksum dump: 31 4e 3e b6 07 3d 5d 90 10 80 c4 c3 0d 86 64 99
FGVM010000077650 (updated 2 seconds ago): in-sync
FGVM010000077650 cksum dump: 31 4e 3e b6 07 3d 5d 90 10 80 c4 c3 0d 86 64 99
System Usage stats:
FGVM010000077649 (updated 4 seconds ago):
    sessions=8, average-cpu-user/nice/system/idle=1%/0%/0%/98%, memory=38%
FGVM010000077650 (updated 2 seconds ago):
    sessions=0, average-cpu-user/nice/system/idle=0%/0%/0%/100%, memory=36%
...
...
```

Cluster status, member model, HA mode, and cluster uptime

Latest primary election results and the reason

Configuration sync status

Performance stats of each member



You can get more information about the HA status on the FortiGate CLI by using the `get system ha status` command.

The command displays comprehensive HA status information in a user-friendly output and is usually executed as the first step when troubleshooting HA. This slide shows the first part of an example output that the command provides.

At the beginning of the output, you can see the cluster status, the member model, the HA mode in use, and the cluster uptime. The example output shows that the cluster status is good, the member model is FortiGate-VM64-KVM, and the HA mode is active-passive.

Next, you can see the latest primary election events, the result, and the reason.

The configuration status information is displayed next. It indicates the configuration sync status for each member. For both members, the configuration is in sync.

Following the configuration status information, you can see the system usage statistics, which report on performance statistics for each member. They indicate the number of sessions that each member handles, as well as the average CPU and memory usage. Note that the `sessions` field accounts for any sessions that the member handles, and not only the sessions that are distributed when the HA mode is active-active.

DO NOT REPRINT
© FORTINET

Checking the HA Status on the CLI (Contd)

```
HBDEV stats:
    FGVM010000077649(updated 3 seconds ago):
        port7: physical/10000full, up, rx-bytes/packets/dropped/errors=4029545/11074/0/0, tx=5360086/11576/0/0
    FGVM010000077650(updated 1 seconds ago):
        port2: physical/10000full, up, rx-bytes/packets/dropped/errors=5377151/11684/0/0, tx=4023101/10991/0/0
MONDEV stats:
    FGVM010000077649(updated 3 seconds ago):
        port1: physical/10000full, up, rx-bytes/packets/dropped/errors=42166263/29629/0/0, tx=570354/5486/0/0
    FGVM010000077650(updated 1 seconds ago):
        port1: physical/10000full, up, rx-bytes/packets/dropped/errors=14470/141/0/0, tx=0/0/0/0
PINGSVR stats:
    FGVM010000077649(updated 3 seconds ago):
        port1: physical/10000full, up, rx-bytes/packets/dropped/errors=42166263/29629/0/0, tx=570354/5486/0/0
        pingsvr: state=up(since 2024/09/16 09:22:06), server=8.8.8.8, ha_prio=5
    FGVM010000077650(updated 1 seconds ago):
        port1: physical/10000full, up, rx-bytes/packets/dropped/errors=14470/141/0/0, tx=0/0/0/0
        pingsvr: state=N/A(since 2024/09/22 09:22:03), server=8.8.8.8, ha_prio=5
Primary   : NGFW-1      , FGVM010000077649, HA cluster index = 1
Secondary : NGFW-2      , FGVM010000077650, HA cluster index = 0
number of vcluster: 1
vcluster 1: work 169.254.0.2
Primary: FGVM010000077649, HA operating index = 0
Secondary: FGVM010000077650, HA operating index = 1
```

Heartbeat, monitored, and remote link interfaces status

Member role, host name, serial number, and ID



This slide shows the second part of the example output that the `get system ha status` command provides.

The output begins with the status information for the configured heartbeat, monitored, and remote link interfaces. These interfaces enable the cluster to perform device failover, link failover, and remote link failover protection, respectively.

Next, the output shows the role, host name, serial number, and ID information for each member of the cluster. The output indicates that the NGFW-1 and NGFW-2 devices are primary and secondary members, respectively.

DO NOT REPRINT

© FORTINET

Checking the Configuration Synchronization

- Display the member checksum:

```
# diagnose sys ha checksum show

is_manage_primary()=1, is_root_primary()=1
debugzone
global: 87 cd b6 19 5a 94 21 a0 ab 1f af 56 58 94 e4 ac
root: 63 3d 55 72 97 90 a4 cb f2 78 be 02 55 47 2c 05
all: e3 92 b7 90 5b ca e7 b5 a6 7d e7 5b ee 2d 9c 54

checksum
global: 87 cd b6 19 5a 94 21 a0 ab 1f af 56 58 94 e4 ac
root: 63 3d 55 72 97 90 a4 cb f2 78 be 02 55 47 2c 05
all: e3 92 b7 90 5b ca e7 b5 a6 7d e7 5b ee 2d 9c 54
```

Configuration is in sync when all hash values on each member match

- If the checksums don't match, try running:

```
diagnose sys ha checksum recalculate
```



- Display the checksum for all members:

```
# diagnose sys ha checksum cluster
=====
FGVM010000077649 =====

is_manage_primary()=1, is_root_primary()=1
debugzone
global: 87 cd b6 19 5a 94 21 a0 ab 1f af 56 58 94 e4 ac
root: 63 3d 55 72 97 90 a4 cb f2 78 be 02 55 47 2c 05
all: e3 92 b7 90 5b ca e7 b5 a6 7d e7 5b ee 2d 9c 54

checksum
global: 87 cd b6 19 5a 94 21 a0 ab 1f af 56 58 94 e4 ac
root: 63 3d 55 72 97 90 a4 cb f2 78 be 02 55 47 2c 05
all: e3 92 b7 90 5b ca e7 b5 a6 7d e7 5b ee 2d 9c 54
===== FGVM010000077650 =====

is_manage_primary()=0, is_root_primary()=0
debugzone
global: 07 cd b6 19 5a 94 21 a0 ab 1f af 56 50 94 e4 ac
root: 63 3d 55 72 97 90 a4 cb f2 78 be 02 55 47 2c 05
all: e3 92 b7 90 5b ca e7 b5 a6 7d e7 5b ee 2d 9c 54

checksum
global: 87 cd b6 19 5a 94 21 a0 ab 1f af 56 58 94 e4 ac
root: 63 3d 55 72 97 90 a4 cb f2 78 be 02 55 47 2c 05
all: e3 92 b7 90 5b ca e7 b5 a6 7d e7 5b ee 2d 9c 54
```

© Fortinet Inc. All Rights Reserved.

26

The `diagnose sys ha checksum` command tree enables you to check the cluster configuration sync status. In most cases, you should use the `diagnose sys ha checksum cluster` command to view the cluster checksum. The output includes the checksum of each member in the cluster.

When you run the `diagnose sys ha checksum cluster` command, the checksum is polled from each member using the heartbeat interface. If HA is not working correctly, or if there are heartbeat communication issues, then the command may not show the checksum for members other than the one on which you run the command. An alternative is to connect to each member individually and run the `diagnose sys ha checksum show` command instead, which shows the checksum of that member.

After you obtain each member's checksums, you can identify the configuration sync status by comparing them. If all members show the exact same hash values for each configuration scope, then the configuration of all members is in sync.

To calculate checksums, FortiGate computes a hash value for each of the following configuration scopes:

- `global`: global configuration, such as global settings, FortiGuard settings, and so on
- `root`: settings and objects specific to the root VDOM—if you configure multiple VDOMs, FortiGate computes hash values for each VDOM
- `all`: global configuration plus the configuration of all VDOMs

In some cases, the configuration of members is in sync even though the checksums are different. For these cases, try running the `diagnose sys ha checksum recalculate` command to recalculate the HA checksums.

DO NOT REPRINT
© FORTINET

Switching to the CLI of Another Member

- Using the FortiGate CLI, you can connect to the CLI of any member:

```
# execute ha manage <member_id> <admin_username>
```

- To list the ID of each member, use a question mark:

```
# execute ha manage
<id>    please input peer box index.
<0>      Subsidiary unit FGVM010000077650
```



When FortiGate devices form an HA cluster, the primary device synchronizes most of its configuration to the secondary device, including the interface settings. From that point, each cluster member will have the same IP addresses configured on each interface, but only the primary member will respond on the network. As a result, the secondary devices will not be reachable over the network for administrative access (SSH/HTTPS), SNMP monitoring, or any other purposes.

If you cannot access the secondary cluster member, how can you configure the dedicated IP on it, or anything else for that matter? You can accomplish this by first connecting to the primary FortiGate CLI via SSH and then running the `execute ha manage` command as shown on this slide to tunnel into the secondary device's CLI via the primary device.

This command requires you to indicate the secondary device's member ID, which can be obtained by typing a question mark at that point in the command (see screenshot). You will also need to provide the username of an administrator account in the command. If the connection is successful, you will be prompted for the administrator password.

Once you are connected to the secondary device's CLI, you can enter CLI commands normally to configure or view whatever you wish. Type `exit` to close the connection to the secondary member and return to the primary member's CLI prompt.

DO NOT REPRINT**© FORTINET**

Connect to Any Member Directly

- Reserved HA management interface
 - Out-of-band
 - Up to four dedicated interfaces
 - For local-in traffic and *some* local-out traffic
 - Separate routing table
 - Configuration example (not synchronized):

```
config system ha
  set ha-mgmt-status enable
  config ha-mgmt-interfaces
    edit 1
      set interface "port10"
      set gateway 192.168.100.254
    next
  end
config system interface
  edit "port10"
    set ip 192.168.100.1 255.255.255.0
    set allowaccess ping https ssh snmp
  next
end
```

- In-band HA management interface

- In-band
- Use any user-traffic interface
- For local-in and local-out traffic
- Shared routing table
- Configuration example (not synchronized):

```
config system interface
  edit "port1"
    set management-ip 10.0.10.1 255.0.0.0
    set allowaccess ping https ssh snmp
  next
end
```



When you connect to a cluster using any of its virtual IP addresses, you always connect to the primary. You can then switch to the CLI of any member in the cluster by using the `execute ha manage` command. But what if you want to access the GUI of a secondary member or maybe poll data from it using SNMP? For this, you need a way to access each member directly regardless of its role in the cluster.

FortiGate provides two ways for the administrator to connect to a member directly no matter what the member role is. The reserved HA management interface is the out-of-band option. You configure up to four dedicated management interfaces, and you assign them a unique address on each member. You can then use the unique address assigned to each member to connect to them directly. You can also instruct FortiGate to use the dedicated management interface for some outbound management services such as SNMP traps, logs, and authentication requests.

Alternatively, you can configure in-band HA management, which enables you to assign a unique management address to a member without having to set aside an interface for that purpose. You assign the management address to any user-traffic that the member uses, and then connect to the member using that unique management address.

If you have unused interfaces, then it's generally more convenient to use a reserved HA management interface because the user and management traffic don't have to compete. Many FortiGate models come with a management interface that you can use for this purpose. Also, the routing information for a reserved HA management interface is placed in a separate routing table, which means that you don't see the interface routes in the FortiGate routing table. This allows for segmentation between data and management traffic.

This slide also shows configuration examples for both management options. For both options, the configuration you apply on a member is not synchronized to other members in the cluster.

DO NOT REPRINT**© FORTINET**

Knowledge Check

1. What is the default order criteria (override disabled) for selecting the primary device in an HA cluster?
 A. Connected monitored ports > HA uptime > priority > serial number
 B. Priority > HA uptime > connected monitored ports > serial number

2. Which HA setting must be identical in active-passive HA cluster members?
 A. Hostname
 B. Group name

3. Which statement about the two HA clusters in the same broadcast domain and using the same HA group ID is true?
 A. You may experience MAC address conflicts.
 B. You may experience IP address conflicts.



DO NOT REPRINT

© FORTINET

Lesson Progress



HA Operation Modes



HA Cluster Synchronization



HA Failover



Monitoring



© Fortinet Inc. All Rights Reserved. 30

Congratulations! You have completed this lesson.

Now, you will review the objectives covered in this lesson.

DO NOT REPRINT

© FORTINET

Review

- ✓ Configure HA to use FGCP
- ✓ Identify the primary and secondary device tasks in an HA cluster
- ✓ Identify what is synchronized between HA cluster members
- ✓ Identify the HA failover types
- ✓ Verify the normal operation of an HA cluster
- ✓ Configure the HA management interface



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

By mastering the objectives covered in this lesson, you learned about the fundamentals of FortiGate HA and how to configure it.

DO NOT REPRINT**© FORTINET**

FortiOS Administrator

Diagnostics and Troubleshooting

A small red square icon containing a white graphic of a network device or server, followed by the text "FortiOS 7.6".

Last Modified: 6 October 2025

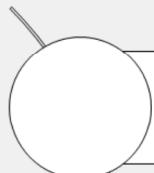
© Fortinet Inc. All Rights Reserved. 1

In this lesson, you will learn about using diagnostic commands and tools.

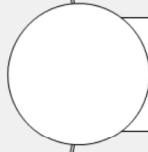
DO NOT REPRINT

© FORTINET

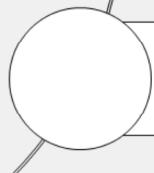
Lesson Overview



General Diagnosis



Packet Sniffer and Debug Flow



CPU and Memory



© Fortinet Inc. All Rights Reserved.

2

In this lesson, you will learn about the topics shown on this slide.

DO NOT REPRINT**© FORTINET**

General Diagnosis

Objectives

- Monitor for abnormal behavior, such as traffic spikes
- Diagnose problems at the physical and network layers



© Fortinet Inc. All Rights Reserved. 3

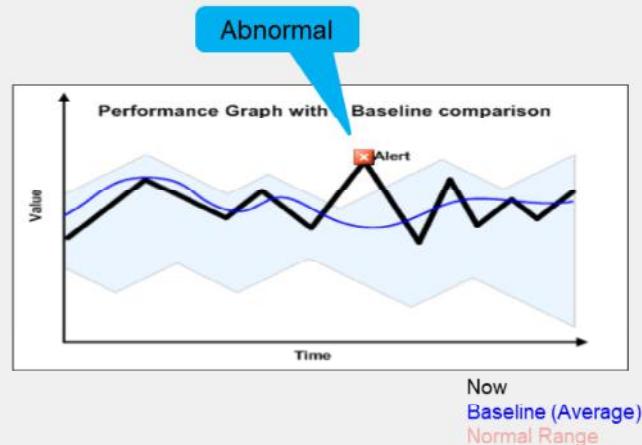
After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in overall diagnosis, you will be able to discover general information about the status of FortiGate.

DO NOT REPRINT
© FORTINET

Before a Problem Occurs

- Know what normal is (baseline):
 - CPU usage
 - Memory usage
 - Traffic volume
 - Traffic directions
 - Protocols and port numbers
 - Traffic pattern and distribution
- Why?
 - Abnormal behavior is difficult to identify, *unless* you know, relatively, what normal is



Diagnosis is the process of finding the underlying cause of a problem.

In order to define any problem, first you must know what your network's *normal* behavior is.

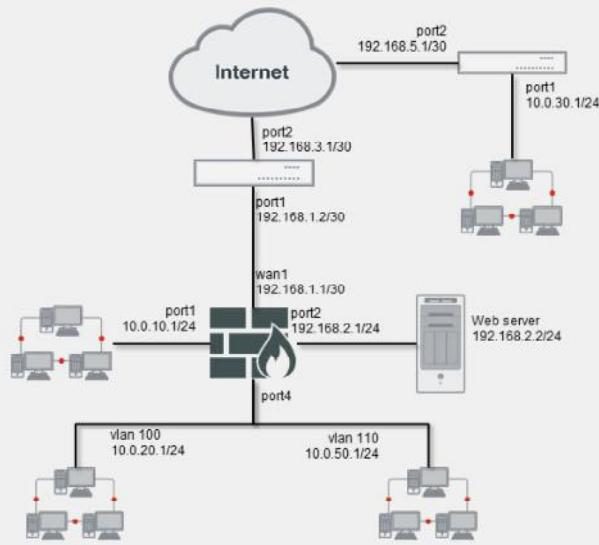
In the graph shown on this slide, the range that indicates *normal* is shown in blue. What exactly is this blue line? It indicates the averages—our baseline. What is the thick black line? It's the current behavior. When the current behavior (black line) leaves the normal range, an abnormal event is happening.

Normal is measured and defined in many ways. It can be performance: the expected CPU and memory utilization, bandwidth, and traffic volumes. But, it can also be your network topology: which devices are normally connected at each node. It is also behavior: traffic flow directions, which protocols are blocked or proxied, and the distribution of protocols and applications used during specific times of the day, week, or year.

DO NOT REPRINT**© FORTINET**

Network Diagrams

- Why?
 - Explaining or analyzing complex networks is difficult and time consuming without them
- Physical diagrams:
 - Include cables, ports, and physical network devices
 - Show relationships at layer 1 and layer 2
- Logical diagrams:
 - Include subnets, routers, logical devices
 - Show relationships at layer 3



© Fortinet Inc. All Rights Reserved.

5

What is the first way to define what is *normal* for your network?

Flows and other specifications of *normal* behaviour are derived from the topology. So, during troubleshooting, a network diagram is essential. If you create a ticket with Fortinet Technical Support, a network diagram should be the first thing you attach.

Network diagrams sometimes combine the two types of diagrams:

- Physical
- Logical

A physical diagram shows how cables, ports, and devices are connected between buildings and cabinets. A logical diagram shows relationships (usually at OSI layer 3) between virtual LANs, IP subnets, and routers. It can also show application protocols such as HTTP or DHCP.

When you configure the devices and add them to the Security Fabric, these physical and logical topologies are available in the **Security Fabric** section of the FortiGate device.

DO NOT REPRINT
© FORTINET

Monitoring Traffic Flows and Resource Usage

- Get normal data before problems or complaints
- Tools:
 - Security Fabric
 - Dashboard with widgets
 - SNMP
 - Alert email
 - Logging/syslog/FortiAnalyzer
 - CLI debug commands



© Fortinet Inc. All Rights Reserved.

6

Another way to define normal is to know the average performance range. On an ongoing basis, collect data that shows normal use.

For example, if traffic processing is suddenly slow, and the FortiGate CPU use is 75%, what does that indicate? If CPU use is usually 60–69%, then 75% is probably still normal. But if normal is 12–15%, there may be a problem.

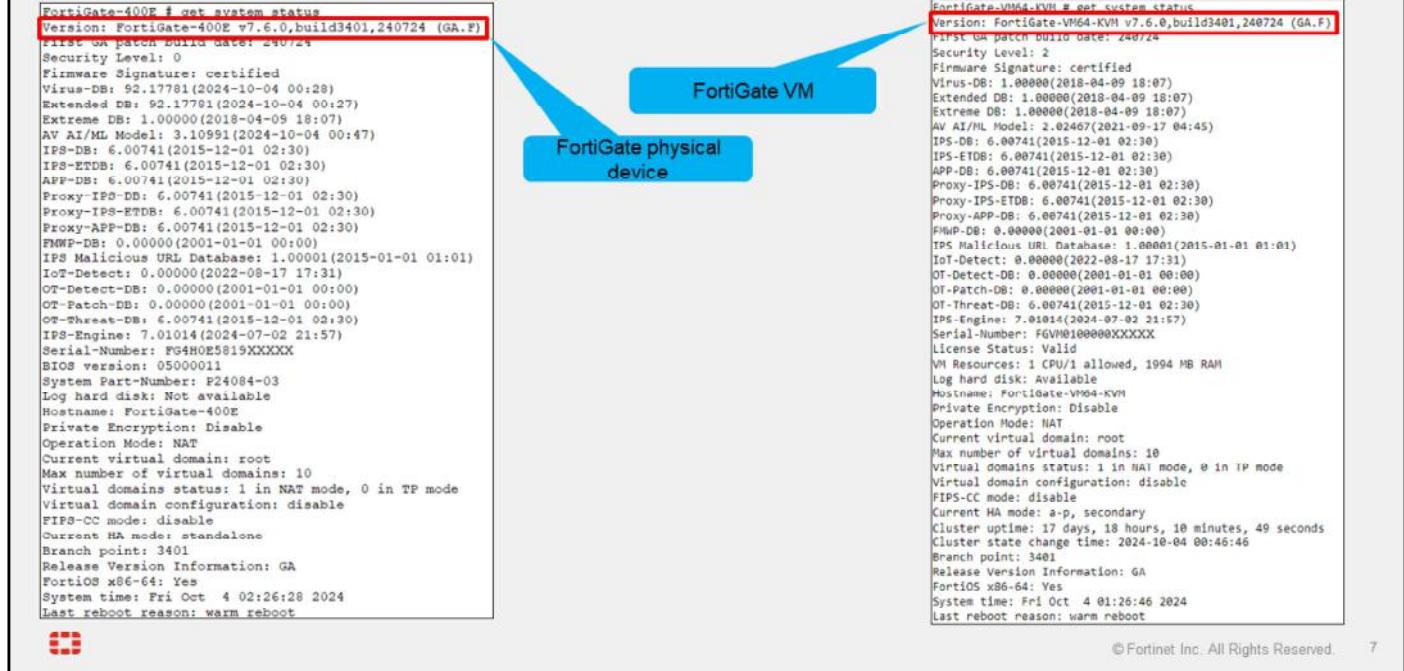
Get data on both the typical maximum and minimum for the time and date. That is, on a workday or holiday, how many bits per second should ingress or egress each interface in your network diagrams?

FortiGate provides a range of tools to monitor the traffic flows and resource usage, including FortiView monitors and dashboard widgets. For example, you can monitor an interface bandwidth and adjust the time frame to one hour, one day, or one week.

DO NOT REPRINT

© FORTINET

System Information



How can we get information about the current status? First, look at CLI commands; you can use them through a local console, even if network issues make GUI access slow or impossible.

A few commands provide system statuses. The `get system status` command provides mostly general-purpose information. The output shows:

- Model
- Serial number
- Firmware version
- Host name
- FortiGuard license status
- System time
- Version of the FortiGuard antivirus, IPS, and IP reputation databases, and others

DO NOT REPRINT**© FORTINET**

Network Layer Troubleshooting

```
# execute ping-options
adaptive-ping      Adaptive ping <enable|disable>.
data-size          Integer value to specify datagram size in bytes.
df-bit             Set DF bit in IP header <yes | no>.
interface          Auto | <outgoing interface>.
interval           Integer value to specify seconds between two pings.
pattern            Hex format of pattern, e.g. 00ffaabb.
repeat-count       Integer value to specify how many times to repeat PING.
...
# execute ping <x.x.x.x> "IP address or domain name"
# execute traceroute <x.x.x.x> "Destination IP address or hostname"
```



Say that FortiGate can contact some hosts through port1, but not others. Is the problem in the physical layer or the link layer? Neither. Connectivity has been proven with at least part of the network. Instead, you should check the network layer. To test this, as usual, start with ping and traceroute.

The same commands exist for IPv6: execute ping becomes execute ping6, for example.

Remember: Location matters. Tests are accurate only if you use the same path as the traffic that you are troubleshooting. To test from FortiGate (to FortiAnalyzer or FortiGuard, for example), use the FortiGate execute ping and execute traceroute CLI commands. But, to test the path through FortiGate, also use ping and tracert or traceroute from the endpoint—from the Windows, Linux, or Mac OS X computer—not only from the FortiGate CLI.

Because of NAT and routing, you might need to specify a different ping source IP address—the default address is the IP of the outgoing interface. If there is no response, verify that the target is configured to reply to ICMP echo requests.

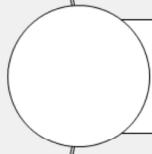
DO NOT REPRINT

© FORTINET

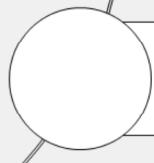
Lesson Progress



General Diagnosis



Packet Sniffer and Debug Flow



CPU and Memory



© Fortinet Inc. All Rights Reserved.

9

Good job! You now understand general diagnostics.

Now, you will learn about packet sniffer and debug flow.

DO NOT REPRINT**© FORTINET**

Packet Sniffer and Debug Flow

Objectives

- Diagnose connectivity problems using sniffer and debug flow



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

By demonstrating competence in the packet sniffer and debug flow, you will be able to diagnose connectivity problems.

DO NOT REPRINT**© FORTINET**

Packet Sniffer

- Packet sniffer command:

- `#diagnose sniffer packet <interface> <filter> <verbose> <count> <tsformat>`
- `<count>` stops packet capture after this many packets
- `<tsformat>` changes the time stamp format
- a – Absolute UTC time
- l – Local time

Level	IP headers	IP payload	Ethernet headers	Port names
1	✓			
2	✓	✓		
3	✓	✓	✓	
4	✓			✓
5	✓	✓		✓
6	✓	✓	✓	✓



FortiGate includes the sniffer command, which is a useful tool when troubleshooting requires you to dig further to diagnose the source of the issue.

The sniffer command can sniff packets on physical or virtual interfaces. If the sniffer command is set to `any`, it can sniff all available interfaces simultaneously.

You can use a filter to customize and narrow down the packets that you want to capture. The sniffer filter uses Berkeley Packet Filter (BPF) syntax.

The verbose setting has six verbosity levels:

- 1: print header of packets
- 2: print header and data from the IP header of the packets
- 3: print header and data from the Ethernet header of the packets
- 4: print header of packets with interface name
- 5: print header and data from IP of packets with interface name
- 6: print header and data from Ethernet of packets with interface name

DO NOT REPRINT
© FORTINET

Packet Sniffer Example

```
Local-FortiGate # diagnose sniffer packet any 'host 8.8.8.8 and icmp' 4
interfaces=[any]
filters=[host 8.8.8.8 and icmp]
11.208116 lan in 10.1.10.1 -> 8.8.8.8: icmp: echo request
11.208370 wan1 out 172.20.121.11 -> 8.8.8.8: icmp: echo request
11.216576 wan1 in 8.8.8.8 -> 172.20.121.11: icmp: echo reply
11.216680 lan out 8.8.8.8 -> 10.1.10.1: icmp: echo reply
4 packets received by filter
0 packets dropped by kernel
```

any to capture all interfaces

Number of packets matching the filter that could not be captured by the sniffer; therefore, you must use a more specific filter

```
Local-FortiGate # diagnose sniffer packet any 'icmp' 4 3 a
interfaces=[any]
filters=[host 8.8.8.8 and icmp]
2019-05-15 18:04:48.722396 port3 in 10.1.10.1 -> 8.8.8.8: icmp: echo request
2019-05-15 18:04:48.722549 port1 out 172.20.121.11 -> 8.8.8.8: icmp: echo request
2019-05-15 18:04:48.730349 port1 in 8.8.8.8 -> 172.20.121.11: icmp: echo reply
```

Timestamp



To sniffer traffic in all interfaces, use the keyword `any` as the interface name.

Stop the sniffer by pressing `Ctrl+C`, and check for dropped packets. If there were dropped packets during the sniffer, it means that not all the traffic that matched the sniffer filter could be captured. So, you might need to capture the traffic again using a stricter filter.

If you do not specify an option for the timestamp, the debug shows the time, in seconds, since it started running. You can prepend the local system time to easily correlate a packet with another recorded event.

DO NOT REPRINT**© FORTINET**

Packet Capture—GUI

- From the GUI:

The screenshot shows the Network > Diagnostics > Packet Capture interface. A red box highlights the 'Packet capture' tab. A green box highlights the '+ New packet capture' button, which has a red arrow pointing to the 'New Capture' dialog window. The 'New Capture' window displays captured packets with columns for Time, Packet Type, Source IP, Destination IP, Source Port, Destination Port, and Protocol. The first three packets are shown: 1.31158s IP from 208.91.112.62 to 100.65.1.111 on port 123 to 123 UDP; 0.03896s IP from 192.168.1.111 to 192.168.0.1 on port 443 to 50170 TCP; and 1.05835s IP from 192.168.1.111 to 192.168.0.1 on port 443 to 50170 TCP. A blue callout box points to the 'Save as .pcap' button at the bottom right of the 'New Capture' window, with the text 'You can download the packet capture'.

Time	Packet Type	Source IP	Destination IP	Source Port	Destination Port	Protocol
1.31158s	IP	208.91.112.62	100.65.1.111	123	123	UDP
0.03896s	IP	192.168.1.111	192.168.0.1	443	50170	TCP
1.05835s	IP	192.168.1.111	192.168.0.1	443	50170	TCP

The Packet Capture tool allows you to view packet capture output on the GUI in real time until you stop the capture process.

This tool helps you to examine the packet capture details directly on the GUI.

When you set up the packet capture, you can enable **Filters** to filter using basic criteria such as host address, port number, and protocol name.

After you stop the packet capture, you can export the output as a pcap file.

DO NOT REPRINT**© FORTINET**

Debug Flow

- Shows what the CPU is doing, step-by-step, with the packets
 - If a packet is dropped, it shows the reason
- Multi-step command
 1. Define a filter: diagnose debug flow filter <filter>
 2. Enable debug output: diagnose debug enable
 3. Start the trace: diagnose debug flow trace start <xxx> Repeat number
 4. Stop the trace: diagnose debug flow trace stop



If FortiGate is dropping packets, can a packet capture (sniffer) be used to identify the reason? To find the cause, you should use the debug (packet) flow.

The debug flow shows, step-by-step, how the CPU is handling each packet.

To use the debug flow, follow these steps:

1. Define a filter.
2. Enable debug output.
3. Start the trace.
4. Stop the trace when it's finished.

DO NOT REPRINT

© FORTINET

Debug Flow Example—SYN

```
#diagnose debug flow filter addr 66.171.121.44
#diagnose debug flow filter port 80
#diagnose debug flow trace start 20
#diagnose debug enable
```

IP addresses, port numbers,
and incoming interface

Create a new session

```
trace id=1 func=print_pkt detail line=5839 msg="vd-rod :0 received a
packet(proto=6, 10.0.1.11:5128->66.171.121.44:80) tun_id=0.0.0.0 from internal
flag [S], seq 3647447081, ack 0, win 65535"
```

```
trace id=1 func=init_ip_session_common line=6017 msg="allocate a new session-
00002410, tun_id=0.0.0.0"
```

```
trace id=1 func=vf_ip_route_input_common line=2612 msg="find a route:
flag=04000000 qw-192.168.1.1 via wan1"
```

Found a matching route. Shows next-
hop IP address and outgoing interface

```
func=fw_forward_handler line=1003 msg="Allowed by Policy-1: SNAT"
```

Matching firewall
policy

```
trace id=1 func= ip_session_run_tuple line=3421 msg="SNAT 10.0.1.111-
>192.168.1.102:5128"
```

Source NAT



This slide shows an example of a debug flow output of the above `diagnose debug flow` commands, which captures the first packet of a TCP three-way handshake, the SYN packet. It shows:

- The packet arriving at FortiGate, indicating the source and destination IP addresses, port numbers, and incoming interface
- FortiGate creating a session, indicating the session ID
- The route to the destination, indicating the next-hop IP address and outgoing interface
- The ID of the policy that matches and allows this traffic
- How the source NAT is applied

DO NOT REPRINT
© FORTINET

Debug Flow Example—SYN/ACK

```
trace_id=2 func=print_pkt_detail line=5839 msg="vd-root:0 received a
packet(proto=6, 66.171.121.44:80->192.168.1.102:5128) tun_id=0.0.0.0 from wan1.
flag [S.], seq 2200164917, ack 3647447082, win 65535"
```

IP addresses, port numbers,
and incoming interface

```
trace id=2 func=resolve_ip_tuple_fast line=5922 msg="Find an existing session. id-
00002410, reply direction"
```

Using an existing session

```
trace id=2 func=_ip_session_run_tuple line=3435 msg="DNAT 192.168.1.102:5128-
>10.0.1.111:5128"
```

Destination NAT

```
trace id=2 func=vf_ip_route_input_common line=2612 msg="find a route:
flag=00000000 gw=10.0.1.111 via internal"
```

Found a matching route.
Shows next-hop IP address
and outgoing interface



© Fortinet Inc. All Rights Reserved.

16

This slide shows the output for the SYN/ACK packet, which is from the same `diagnose debug` command shown on the previous slide. It shows:

- The packet arrival, indicating again the source and destination IP addresses, port numbers, and incoming interface
- The ID of the existing session for this traffic. This number matches the ID of the session created during the SYN packet. The ID is unique for each session, and useful to trace the request/reply packets of the session.
- How the destination NAT is applied
- The route to the destination, indicating again the next-hop IP address and outgoing interface.

If the packet is dropped by FortiGate, this debug shows the reason for that action.

This tool is useful for many other troubleshooting cases, including when you need to understand why a packet is taking a specific route, or why a specific NAT IP address is being applied.

DO NOT REPRINT

© FORTINET

Debug Flow—GUI

- From the GUI:

The screenshot shows the 'Network > Diagnostics > Debug Flow' page. It has two main sections: 'Basic' and 'Advanced' filter types.

Basic Filter Configuration:

- Number of packets: 100
- IP type: IPv4
- IP address: 8.8.8.8
- Protocol dropdown menu open, showing options: ICMP, Any, Specify, TCP, UDP, SCTP, ICMP.

A blue callout bubble points to the 'Protocol' dropdown with the text: "Select a protocol or Any".

Advanced Filter Configuration:

- Number of packets: 100
- IP type: IPv4
- Source IP: 10.0.1.10
- Source port: 8.8.8.8
- Destination IP: 8.8.8.8
- Destination port: 8.8.8.8
- Protocol: ICMP

A blue callout bubble points to the 'Advanced' filter section with the text: "Select source IP address, source port, destination IP address, destination port, and protocol".

At the bottom right of the interface, there is a copyright notice: © Fortinet Inc. All Rights Reserved. 17.

The Debug Flow tool allows you to view debug flow output on the GUI in real time until you stop the debug process.

This tool helps you to examine the packet flow details directly on the GUI.

After you stop the debug flow, you can view the completed output, and filter it by time, message, or function. You can also export the output as a CSV file.

You can set up the Debug Flow tool to use either Basic or Advanced filter options. **Basic** allows you to filter using basic criteria such as host address, port number, and protocol name. **Advanced** allows you to filter by source IP address, source port, destination IP address, destination port, and protocol.

DO NOT REPRINT

© FORTINET

Debug Flow—GUI (Contd)

- Real-time analysis
 - Embedded real-time analysis page
 - Save and download the packet trace output as a CSV file

Real-time flow output

```

Packet Capture Debug Flow
Capturing Packets
07:08:02 165 vd-root0 received a packet(proto>1, 10.0.1.10:2480->8.8.8.8:2048) tun_id=0.0.0.0 from port3, type=8, code=0, id=2480, seq=7.
07:08:02 165 allocate a new session-0000513b, tun_id=0.0.0.0
07:08:02 165 in:[port3],out:[]
07:08:02 165 len=0
07:08:02 163 result(skb,flags=0x20000000,vid=0,ret-no-match,act=accept,flag=0x00000000)
07:08:02 165 find a route; flag=0x4000000 gw=10.200.1.254 via port1
07:08:02 165 in:[port3],out:[port1],skb,flags=0x20000000,vid=0,app_id=0,url_cat_id=0
07:08:02 165 grum-100004, use add/intf hash, len=2
07:08:02 165 checked grum-100004 policy-1, ret-no-match, act=accept
07:08:02 165 checked grum-100004 policy-0, ret-matched, act=accept
07:08:02 165 ret-matched
07:08:02 165 policy-0 is matched, act=drop
07:08:02 165 after lsoope_captive_check(); is_captive=0, ret-matched,act=drop, id=0
07:08:02 165 after lsoope_captive_check(); is_captive=0, ret-matched,act=drop, id=0
07:08:02 165 Denied by forward policy check [policy 0]

```

Packet Trace output

Time	Message
07:08:02	v6 root0 received a packet(proto>1, 10.0.1.10:2480->8.8.8.8:2048) tun_id=0.0.0.0 from port3, type=8, code=0, id=2480, seq=7.
07:08:02	allocate a new session-0000513b, tun_id=0.0.0.0
07:08:02	in:[port3],out:[]
07:08:02	len=0
07:08:02	result(skb,flags=0x20000000,vid=0,ret-no-match,act=accept,flag=0x00000000)
07:08:02	find a route; flag=0x4000000 gw=10.200.1.254 via port1
07:08:02	in:[port3],out:[port1],skb,flags=0x20000000,vid=0,app_id=0,url_cat_id=0
07:08:02	grum-100004, use add/intf hash, len=2
07:08:02	checked grum-100004 policy 1, ret-no-match, act=accept
07:08:02	checked grum-100004 policy 0, ret-matched, act=accept
07:08:02	ret-matched
07:08:02	policy-0 is matched, act=drop
07:08:02	after lsoope_captive_check(); is_captive=0, ret=0
07:08:02	after lsoope_captive_check(); is_captive=0, ret-matched,act=drop
07:08:02	Denied by forward policy check [policy 0]



After you start the debug flow, the GUI starts displaying the captured packets based on the filter.

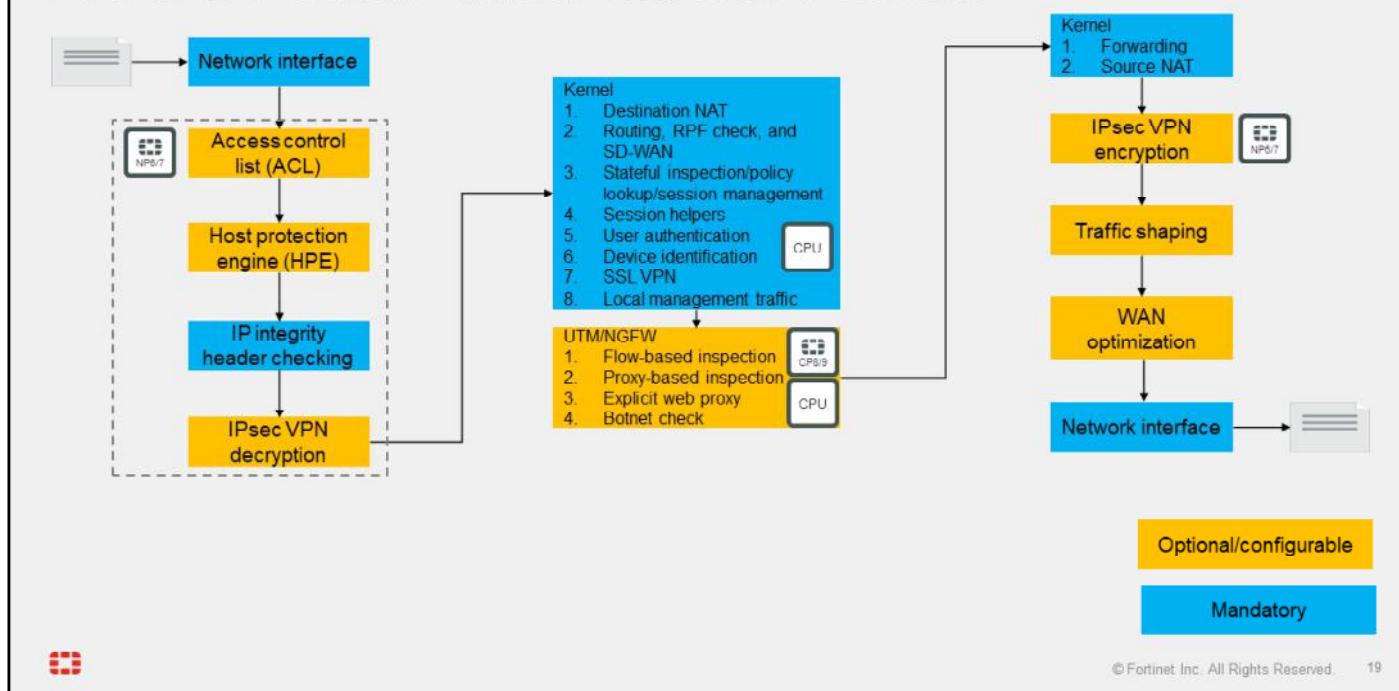
When you stop the debug flow, FortiGate displays a packet trace output that you can download and save as a CSV file.

The main difference between these two outputs is that real-time messages are displayed for real-time analysis, but you can save the packet trace outputs and download them for future reference.

DO NOT REPRINT

© FORTINET

Life of a Packet—Initial Session Packets



The debug flow tool shows the processing of the packets, and this slide summarizes the steps that the first packets of a session go through as they enter, pass through, and exit FortiGate.

FortiGate first performs some security inspections, such as ACL, HPE, and IP integrity header checking, to make sure the packets are within acceptable parameters before allowing them to move through the rest of the processes. These inspections are handled by the network processor (NP) to minimize impact on the FortiGate CPU.

Each version of the NP has criteria that define which traffic can be offloaded. The NP enhances overall performance by allowing offloaded sessions to bypass the FortiGate CPU after the session is established and the session key is installed in the NP. The NP can also handle IPsec VPN encryption and decryption operations, where the configured encryption and hashing algorithms are supported in the hardware.

The content processor (CP) functions like a coprocessor for the FortiGate CPU to improve overall system performance by offloading certain tasks, such as pattern matching for flow-based UTM inspection with the intrusion prevention system (IPS) engine, SSL/TLS decryption and encryption for deep SSL inspection, and IPsec encryption and decryption operations for supported algorithms.

Note that the packet processing for virtual FortiGate devices is identical with the only difference being that the CPU handles all processes instead of being able to offload some of them to NPs and CPs.

DO NOT REPRINT**© FORTINET**

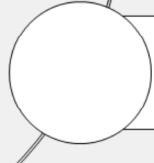
Lesson Progress



General Diagnosis



Packet Sniffer and Debug Flow



CPU and Memory



© Fortinet Inc. All Rights Reserved. 20

Good job! You now understand packet sniffer and debug flow.

Now, you will learn about FortiGate CPU and memory diagnosis.

DO NOT REPRINT**© FORTINET**

CPU and Memory

Objectives

- Diagnose resource problems, such as high CPU or memory usage
- Diagnose memory conserve mode

 © Fortinet Inc. All Rights Reserved. 21

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

By demonstrating a competent understanding of CPU and memory usage, you will be able to diagnose the most common CPU and memory problems.

DO NOT REPRINT**© FORTINET**

Slowness

- High CPU usage
- High memory usage
- What was the last feature you enabled?
 - Enable one at a time
- How high is the CPU usage? Why?
 - # get system performance status
 - # diagnose sys top



Not all problems are network connectivity failures. Sometimes, there are resource problems in the devices.

What else could cause latency? After you have eliminated problems with the physical media and bandwidth usage, you should check the FortiGate resources usage: CPU and memory.

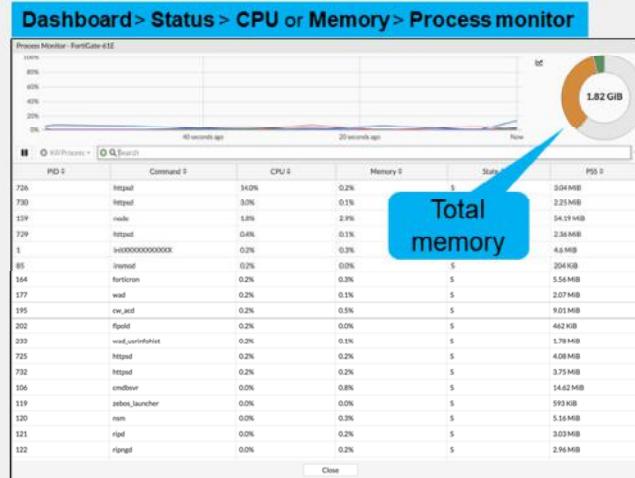
If usage is high, there are tools that can identify which feature is consuming the most CPU. Additionally, you can troubleshoot faster if you know precisely which change (if any) corresponds with the time the problem began.

DO NOT REPRINT

© FORTINET

High CPU and Memory Troubleshooting—Process Monitor

- Processing monitor displays running processes
- Each process shows CPU and memory usage
- Can apply filters and sorting to fine-tune results
- Allow terminating processes



You can use the process to view the running processes and their CPU and memory usage levels. You can apply filters, sort, and terminate processes in the process monitor.

DO NOT REPRINT**© FORTINET**

High CPU and Memory Troubleshooting—CLI

```
# diagnose sys top
Run Time: 0 days, 0 hours and 18 minutes
1U, 4N, 0S, 95I, 0WA, 0HI, 0SI, 0ST; 994T, 421F
    forticron      248      S      2.9      3.8
    newcli         251      R      0.1      1.0
    merged_daemons 185      S      0.1      0.7
    miglogd        177      S      0.0      6.8
    wad             249      S      0.0      3.0
    wad             246      S      0.0      2.8
    miglogd        197      S      0.0      2.7
    cmdbsvr        113      S      0.0      2.4
```

Process name

Memory usage (%)

Sort by CPU: Shift + P
Sort by RAM: Shift + M

Process ID

Process state

CPU usage (%)



Next, examine the output for `diagnose sys top`. It lists processes that use the most CPU or memory. Some common processes include:

- ipsengine, scanunitd, and other inspection processes
- fgfmd for FortiGuard and FortiManager connections
- forticron for scheduling
- Management processes (newcli, miglogd, cmdb, sshd, and httpsd)

To sort the list by highest CPU usage, press Shift+P. To sort by highest RAM usage, press Shift+M.

DO NOT REPRINT**© FORTINET**

Memory Conserve Mode

- FortiOS protects itself when memory usage is high
 - It prevents using so much memory that FortiGate becomes unresponsive
- Three configurable thresholds:

Threshold	Definition	Default (% of total RAM)
Green	Threshold at which FortiGate exits conserve mode	82%
Red	Threshold at which FortiGate enters conserve mode	88%
Extreme	Threshold at which new sessions are dropped	95%

```
config system global
  set memory-use-threshold-green <percentage>
  set memory-use-threshold-red <percentage>
  set memory-use-threshold-extreme <percentage>
end
```



If memory usage becomes too high, FortiGate may enter into memory conserve mode. While FortiGate is in memory conserve mode, it must take action to prevent memory usage from increasing, which could cause the system to become unstable and inaccessible.

Memory conserve mode is never a desirable state because it impacts the user traffic.

Three different configurable thresholds define when FortiGate enters and exits conserve mode. If memory usage goes above the percentage of total RAM defined as the red threshold, FortiGate enters conserve mode. The actions that the device takes depend on the device configuration.

If memory usage keeps increasing, it might exceed the extreme threshold. While memory usage is above this highest threshold, all new sessions are dropped.

The third configuration setting is the green threshold. If memory usage goes below this threshold, FortiGate exits conserve mode.

DO NOT REPRINT**© FORTINET**

What Happens During Conserve Mode?

- System configuration cannot be changed
- FortiGate skips quarantine actions (including FortiSandbox analysis)
- For packets that require any flow-based inspection by the IPS engine:

```
config ips global
    set fail-open {enable|disable}
end
    • enable: Packets can still be transmitted without IPS scanning while in conserve mode
    • Disable (default): Packets are dropped for new incoming sessions.
```



What actions does FortiGate take to preserve memory while in conserve mode?

- FortiGate does not accept configuration changes, because they might increase memory usage.
- FortiGate does not run any quarantine action, including forwarding suspicious files to FortiSandbox.
- You can configure the `fail-open` setting under `config ips global` to control how the IPS engine behaves when the IPS socket buffer is full.

If the IPS engine does not have enough memory to build more sessions, the `fail-open` setting determines whether the FortiGate should drop the sessions or bypass the sessions without inspection.

It is important to understand that the IPS `fail-open` setting is not just for conserve mode—it kicks in whenever IPS fails. Most failures are due to a high CPU issue or a high memory (conserve mode) issue. Enable the setting so that packets can still be transmitted while in conserve mode (or during any other IPS failure) but are not inspected by IPS. Disable the setting so that packets are dropped for new, incoming sessions.

Remember that the IPS engine is used for all types of flow-based inspections. The IPS engine is also used when FortiGate must identify the network application, regardless of the destination TCP/UDP port (for example, for application control). Note that NTurbo doesn't support the `fail-open` setting. If `fail-open` is triggered, new sessions that would typically be accelerated with NTurbo are dropped, even if the `fail-open` setting is enabled.

DO NOT REPRINT**© FORTINET**

What Happens During Conserve Mode? (Contd)

- For traffic that requires any proxy-based inspection (and if memory usage has not exceeded the extreme threshold yet):

```
config system global
    set av-failopen [off | pass | one-shot]
end


- off: All new sessions with content scanning enabled are not passed
- pass (default): All new sessions pass without inspection
- one-shot: Similar to pass in that traffic is not inspected. However, it will keep bypassing the antivirus proxy even after leaving conserve mode. Administrators must either change this setting, or restart the device, to restart the antivirus scanning

```

- The `av-failopen` setting also applies to flow-based antivirus inspection
- If memory usage exceeds the extreme threshold, all new sessions that require inspection (flow-based or proxy-based) are blocked



The `av-failopen` setting defines the action that is applied to any proxy-based inspected traffic, while the unit is in conserve mode (and as long as the memory usage does not exceed the extreme threshold). This setting also applies to flow-based antivirus inspection. Three different actions can be configured:

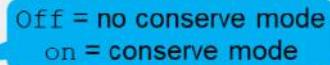
- off:** All new sessions with content scanning enabled are not passed but FortiGate processes the current active sessions.
- pass (default):** All new sessions pass without inspection until FortiGate switches back to non-conserve mode.
- one-shot:** Similar to `pass` in that traffic passes without inspection. However, it will keep bypassing the antivirus proxy even after it leaves conserve mode. Administrators must either change this setting, or restart the unit to restart the antivirus scanning

However, if the memory usage exceeds the extreme threshold, new sessions are always dropped, regardless of the FortiGate configuration.

DO NOT REPRINT**© FORTINET**

System Memory Conserve Mode Diagnostics

```
# diagnose hardware sysinfo conserve  
memory conserve mode:  
total RAM: 3040 MB  
memory used: 2706 MB 89% of total RAM  
memory freeable: 334 MB 11% of total RAM  
memory used + freeable threshold extreme: 2887 MB 95% of total RAM  
memory used threshold red: 2675 MB 88% of total RAM  
memory used threshold green: 2492 MB 82% of total RAM
```

on  Off = no conserve mode
on = conserve mode



© Fortinet Inc. All Rights Reserved. 28

The `diagnose hardware sysinfo conserve` command is used to identify if a FortiGate device is currently in memory conserve mode.

DO NOT REPRINT**© FORTINET**

Knowledge Check

1. Which information is displayed in the output of a debug flow?
 A. Incoming interface and matching firewall policy
 B. Matching security profile and traffic log

2. When is a new TCP session allocated?
 A. When a SYN packet is received
 B. When a SYN/ACK packet is received

3. Which action does FortiGate take during memory conserve mode?
 A. Configuration changes are not allowed.
 B. Administrative access is denied.



DO NOT REPRINT**© FORTINET**

Lesson Progress



General Diagnosis



Packet Sniffer and Debug Flow



CPU and Memory



© Fortinet Inc. All Rights Reserved. 30

Congratulations! You have completed this lesson.

Now, you will review the objectives covered in this lesson.

DO NOT REPRINT**© FORTINET**

Review

- ✓ Monitor for abnormal behavior, such as traffic spikes
- ✓ Diagnose problems at the physical and network layers
- ✓ Diagnose connectivity problems using sniffer and debug flow
- ✓ Diagnose resource problems, such as high CPU or memory usage
- ✓ Diagnose memory conserve mode



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

By mastering the objectives covered in this lesson, you learned how to use diagnostic commands and tools, and learned more about FortiGate status and operation.

DO NOT REPRINT

© FORTINET

FORTINET
Training Institute

FortiOS Administrator

FortiGate in the Cloud

 FortiOS 7.6

Last Modified: 6 October 2025

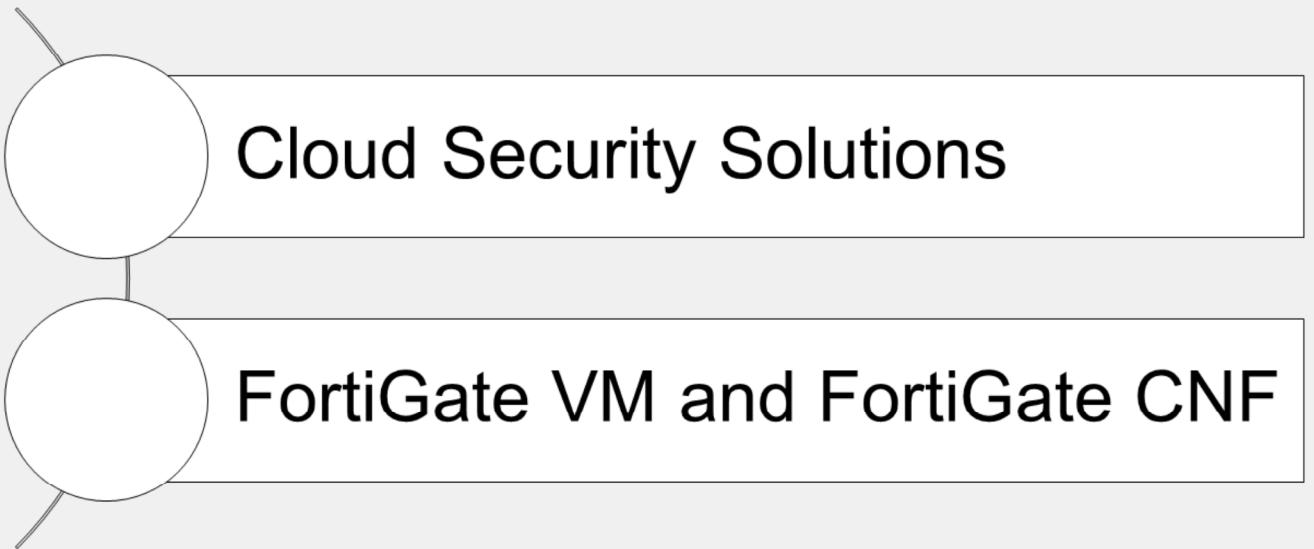
© Fortinet Inc. All Rights Reserved. 1

In this lesson, you will learn about public cloud security solutions.

DO NOT REPRINT

© FORTINET

Lesson Overview



Cloud Security Solutions

FortiGate VM and FortiGate CNF



© Fortinet Inc. All Rights Reserved.

2

In this lesson, you will learn about the topics shown on this slide.

DO NOT REPRINT**© FORTINET**

Cloud Security Solutions

Objectives

- Identify threats and challenges in the public cloud
- Identify Fortinet public cloud solutions



© Fortinet Inc. All Rights Reserved. 3

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

By demonstrating competence in understanding cloud security solutions, you will understand the challenges in the public cloud and implement Fortinet public cloud solutions.

DO NOT REPRINT**© FORTINET**

Threats and Challenges of the Public Cloud

- Threats:
 - Cloud misconfigurations
 - Malware
 - Insecure interfaces/APIs
 - Exfiltration of sensitive data
 - Unauthorized access
 - All the regular threats for any other environment where a next-generation firewall (NGFW) is applied
- Challenges:
 - Who is responsible for security?
 - Which cloud architecture should be implemented?
 - Achieving regulatory compliance



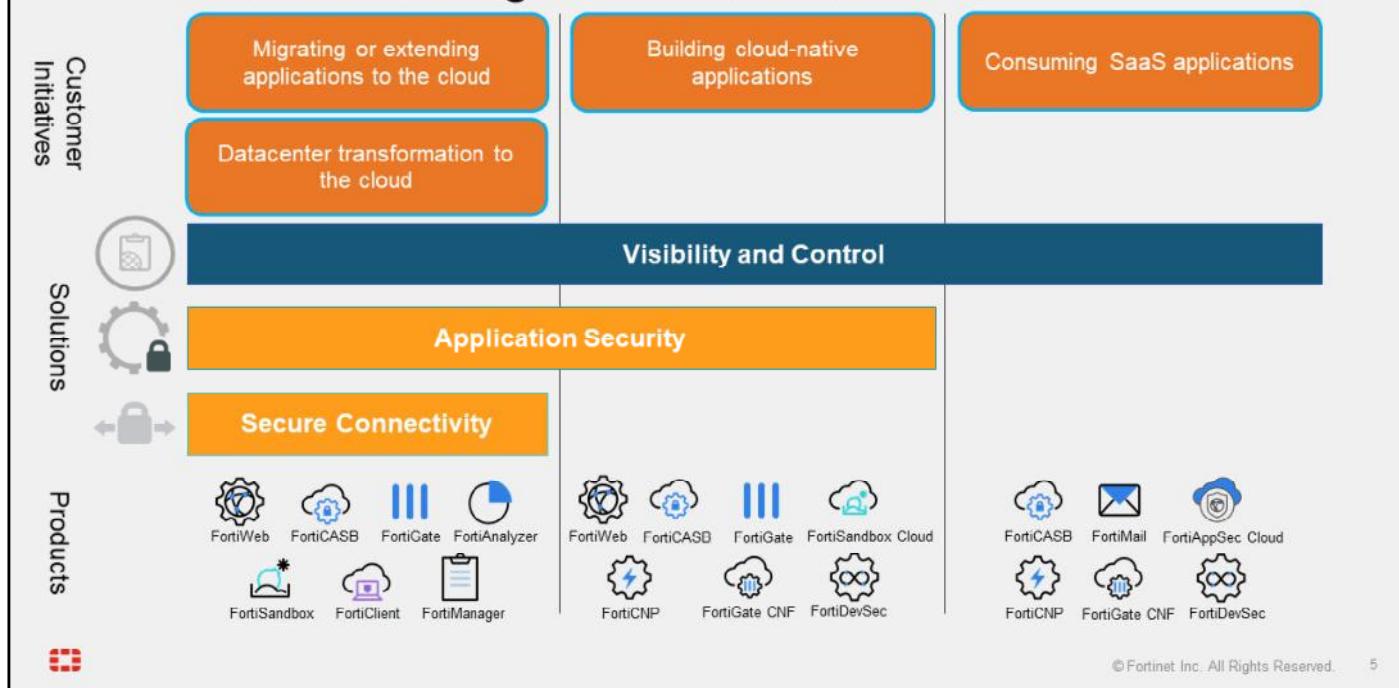
According to the 2023 Cloud Security Report conducted by Cybersecurity Insiders and sponsored by Fortinet, more than 51% of surveyed cybersecurity professionals deem misconfigurations of the public cloud the number one threat. Malware, insecure interfaces and APIs, and exfiltration of sensitive data were also commonly reported as threats. Also, all the regular threats for any other environment where an NGFW is applied.

The top challenges of the public cloud are security responsibility, the type of cloud architecture that should be implemented, and achieving regulatory compliance.

DO NOT REPRINT

© FORTINET

What Does Securing the Cloud Mean?



As the leader in multicloud security, Fortinet gives you the confidence to deploy any application in any cloud. Fortinet solutions provide broad protection across the entire digital attack surface, both on-premises and in public clouds, such as AWS, Azure, and Google Cloud. Native integration with each of the major cloud providers enables automated, centralized management across all clouds uniformly and seamlessly. This gives you unified visibility, control, and policy management that supports risk management and compliance requirements.

There are three Fortinet solutions for securing the cloud: the secure connectivity solution, which belongs to the category Infrastructure-as-a-Service (IaaS); application security; and visibility and control. Fortinet provides solutions for each of these categories. For example, Fortinet can provide secure connectivity for IaaS but cannot provide the same solution for Software-as-a-Service (SaaS) applications. So, for SaaS, Fortinet can provide only visibility and control. In other words, you cannot create an IPsec tunnel or web application firewall (WAF) to a drop box (SaaS).

DO NOT REPRINT**© FORTINET**

Fortinet Cloud Security Solution

- Extends to physical, virtual, and cloud devices with advanced security orchestration and unified threat protection
- Enhances control and visibility by identifying and setting policy for user applications, device specifications, IP addresses, and network interfaces
- Delivers a highly optimized solution that protects application workloads beyond native cloud vendor security options



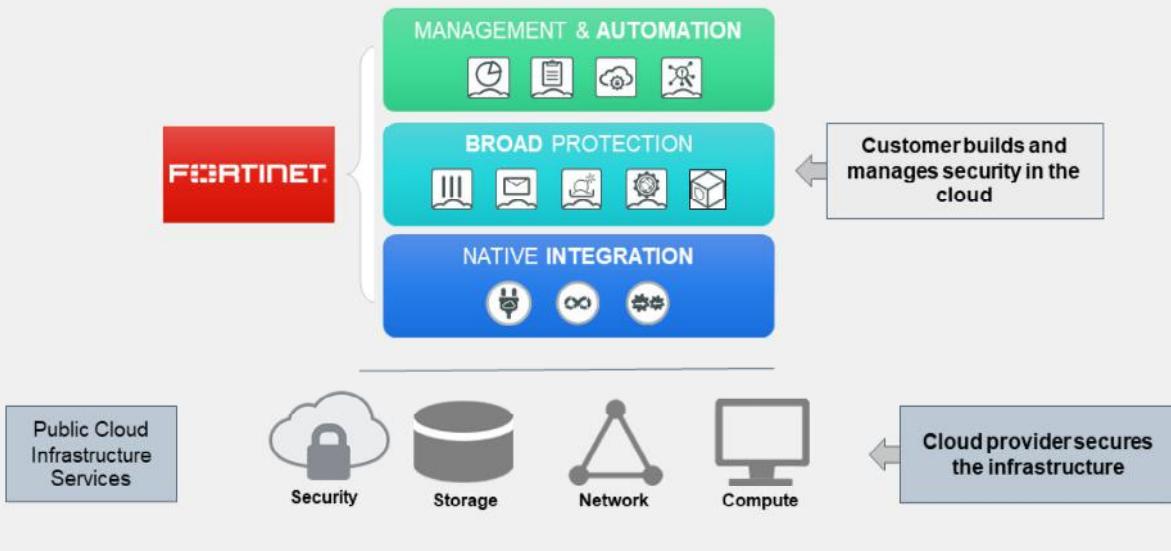
© Fortinet Inc. All Rights Reserved.

6

The Fortinet cloud security solution is not a replacement for existing cloud vendor security but an added layer that provides greater control, visibility, and optimized protection beyond native options.

DO NOT REPRINT
© FORTINET

Fortinet Can Help You Secure the Cloud



© Fortinet Inc. All Rights Reserved. 7

As this slide shows, Fortinet can provide different products to secure the cloud.

Management and automation: To help optimize limited security resources, Fortinet offers a single-pane-of-glass solution that enables consistent management of the broad set of protection services natively integrated into the cloud infrastructure. This approach also automates management through standard web-based APIs and supports the use of predefined automation recipes. By extending this automation framework across multiple cloud environments, customers can embed security services into DevOps-driven application lifecycles while supporting more agile application and business operations.

Broad protection: By offering the broadest set of security products both in and out of the cloud, Fortinet enables customers to consistently build highly secure infrastructures, regardless of deployment mode, workflow complexity, or degree of scale. Native integration with the cloud infrastructure allows Fortinet to deliver multiple security products across and between the cloud environments offered by every major cloud service provider, helping customers create automation-ready, consumable security services to protect their cloud applications wherever they are deployed.

Native integration: Integration seamlessly extends consistent security across every major cloud platform, enabling organizations to define security uniformly across their multicloud and on-premises deployments. Likewise, native integration allows security products to consume cloud services natively, delivering faster, more seamless protection and response while extending the web service-based APIs of products running in the cloud.

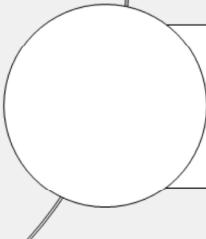
DO NOT REPRINT

© FORTINET

Lesson Progress



Cloud Security Solutions



FortiGate VM and FortiGate CNF



© Fortinet Inc. All Rights Reserved.

8

Good job! You now know about public cloud fundamentals.

Now, you will learn about FortiGate VM and FortiGate Cloud-Native Firewall (CNF).

DO NOT REPRINT**© FORTINET**

FortiGate VM and FortiGate CNF

Objectives

- Identify FortiGate VM in the cloud
- Describe FortiGate CNF
- Identify the differences between FortiGate CNF and FortiGate VM



© Fortinet Inc. All Rights Reserved.

9

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

By demonstrating competence in understanding FortiGate VM and FortiGate CNF, you will be able to select the best solutions for your cloud deployment.

DO NOT REPRINT
© FORTINET

FortiGate VM in the Cloud

- Available to deploy from AWS, Azure, or other cloud vendor marketplaces or templates
- Superior performance compared to cloud vendor native services
- Available with BYOL, PAYG, or FortiFlex licensing
- Advanced features
 - VPN
 - SD-WAN
 - Dynamic routing



Search solution by name

Marketplace

Showing results for 'Fortinet FortiGate Next-Generation Firewall'

Showing 1 to 5 of 5 results.

Offer	Description	Actions
Fortinet FortiGate Next-Generation Firewall	Fortinet	Create
Fortigate Next-Generation Firewall for Azure Stack	Fortinet	Create

Single VM

Active-Passive HA with Forticloud Connector Failover

Active-Active LoadBalanced with ELB/LB

Active-Passive HA with ELB/LB

© Fortinet Inc. All Rights Reserved. 10



FortiGate VM is a powerful virtual instance offering advanced security, VPN, SD-WAN, and routing features. Its capabilities enable complex configurations and granular control.

For example, FortiGate for AWS delivers critical features that are not included by default in AWS native services, such as VPN, SD-WAN, and dynamic routing.

The main licensing models are pay-as-you-go (PAYG), bring your own license (BYOL), and FortiFlex. These models provide flexibility and scalability based on the organization's specific requirements. FortiFlex is a prepaid enterprise license for Fortinet VM use, trackable through the FortiCloud portal. Resource consumption is calculated using a point-based system.

For example, FortiGate supports additional IPsec topologies, such as full mesh and partial mesh, which are not available in AWS native services. It also enables SD-WAN, a feature AWS does not natively provide.

FortiGate also extends dynamic routing capabilities.

DO NOT REPRINT**© FORTINET**

Public Cloud FortiGate Options (Use Cases)

- Network security
- Protection against known exploits and malware
- Protection against unknown threats (sandboxing)
- Content inspection
- Data protection
- VPN gateway



FortiGate VM for public cloud environments delivers complete content and network protection by combining stateful inspection with NGFW features.

- Application control identifies thousands of applications, including cloud applications, for deep inspection of network traffic.
- Continuous threat intelligence provided by FortiGuard Labs security services protects against known exploits and malware.
- Intrusion prevention system (IPS) technology protects against current and emerging network-level threats. In addition to signature-based threat detection, IPS performs anomaly-based detection, which alerts users to any traffic that matches attack behavior profiles.
- Sandboxing integration protects against unknown attacks using dynamic analysis and provides automated mitigation to stop targeted attacks.

FortiGate VM has APIs for automation and orchestration with cloud and software-defined network (SDN) extensions. For example, it can be integrated with AWS GuardDuty threat intelligence feeds for automated incident response.

DO NOT REPRINT**© FORTINET**

Public Cloud Components

- Amazon EC2
- Amazon Virtual Private Cloud (VPC)
- Azure Virtual Machine (VM)
- Azure Virtual Network (VNet)
- AWS Internet Gateway (IGW)
- Azure NAT Gateway



Amazon EC2



Amazon VPC



Azure VM



Azure VNet

AWS Internet
GatewayAzure NAT
Gateway

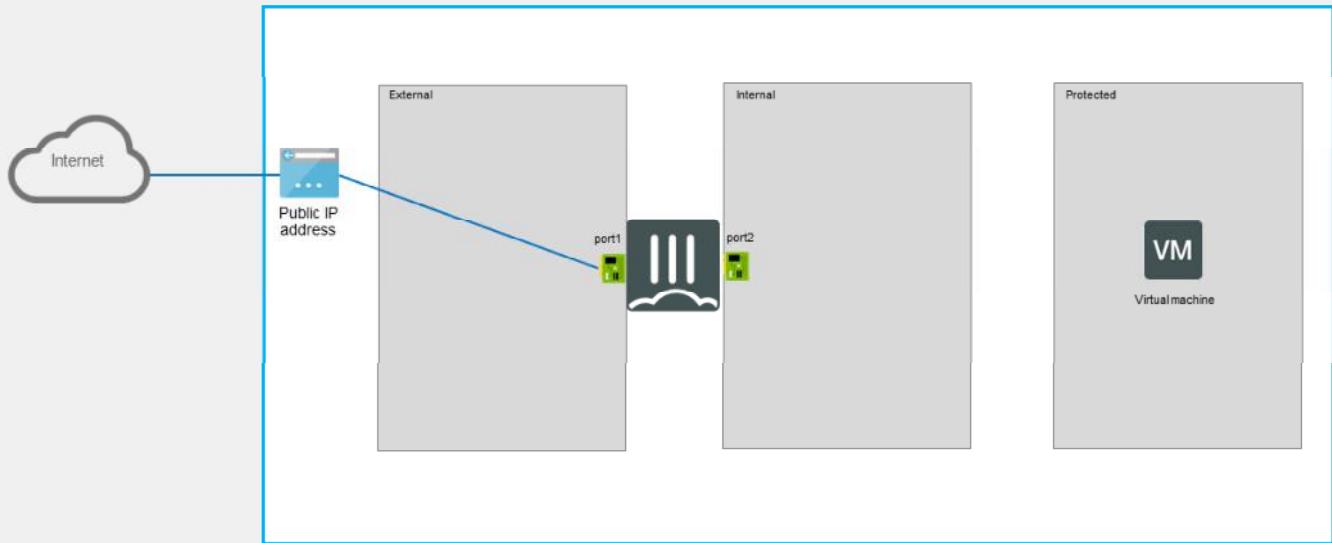
© Fortinet Inc. All Rights Reserved. 12

This lesson covers these key Amazon Web Services (AWS) and Microsoft Azure components:

- Amazon EC2 is a scalable cloud computing service that provides resizable VMs (instances) for running applications and services on the AWS cloud infrastructure.
- Amazon Virtual Private Cloud (VPC) is a customizable and isolated network environment within AWS. It allows users to launch AWS resources like EC2 instances in a virtual network they fully control.
- Azure Virtual Network (VNet) is the fundamental building block of Azure networking. It is a fundamental component of the Azure networking infrastructure. The VNet service securely connects Azure resources to each other, like the Amazon VPC.
- AWS Internet Gateway (IGW) is a VPC component that facilitates communication between instances in your VPC and the internet.
- Azure NAT Gateway is a managed network address translation (NAT) service. You can use Azure NAT Gateway to let all instances in a private subnet connect to the internet.

DO NOT REPRINT
© FORTINET

Example Deployment of a Single FortiGate Instance



The slide shows the topology of a simple FortiGate deployment in the cloud. The VM resides in the protected subnet, which has two internal and external subnets on port 2 and port 1, respectively. The internet traffic coming from the VM gets inspected through FortiGate. This is a simple solution, but more advanced solutions, such as high availability (HA), SD-WAN, and load-balancing options, are also available to deploy.

DO NOT REPRINT**© FORTINET**

What Is FortiGate CNF?

- High-performing, auto-scaling next-generation firewall (NGFW) solution to control and inspect north-south and east-west network traffic
- AWS: supports north-south and east-west network traffic
- Azure: supports only north-south traffic
- Firewall-as-a-Service (FWaaS)

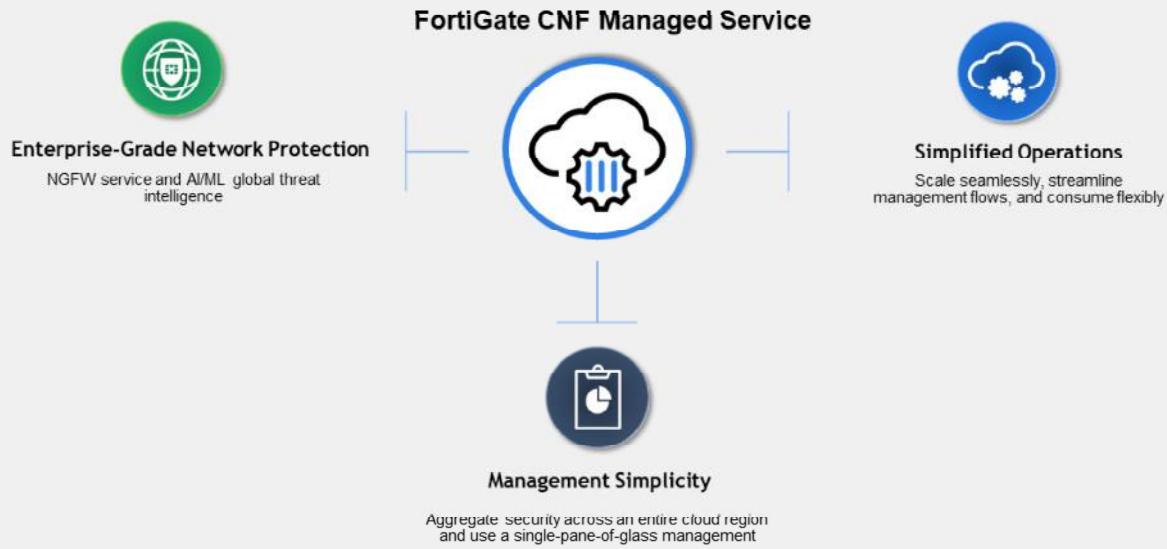


Manually deploying and managing FortiGate devices can be complex and time-consuming. Fortinet addresses this with FortiGate CNF, a FWaaS that reduces network security operations workloads. Enterprises no longer need to configure, provision, or maintain firewall software infrastructure. FortiGate CNF leverages FortiOS software to provide consistent availability, scalability, and ease-of-use, focusing on automation and securing specific cloud network security use cases, such as:

- Protecting cloud workloads from threats associated with outbound communication by blocking malicious IP communication and enforcing geographical fences
- Securing lateral traffic within cloud networks and between cloud workloads using dynamic objects
- Protecting assets hosted in the cloud

DO NOT REPRINT
© FORTINET

What Is FortiGate CNF? (Contd)



In addition, enterprises enjoy the following benefits:

- **Enterprise-grade protection:** FortiGate CNF supports the security inspection capabilities of an NGFW, providing deep visibility into the application layer along with advanced detection and comprehensive protection. It includes geo-IP blocking, advanced filtering, and threat protection. With this level of traffic inspection, customers can reduce the risk of unauthorized events on AWS workloads caused by web-based threats, vulnerability exploits, and other external and internal threat vectors.
- **Zero operations overhead:** FortiGate CNF simplifies security delivery by using a single FortiGate CNF instance to secure an entire AWS or Azure region. It can protect multiple accounts, subnets, VPCs, and availability zones, consolidating security in a region. Cloud-native integration with AWS Gateway Load Balancer (GWLB) helps network security teams move at the speed and scale of application teams. It eliminates do-it-yourself automation and helps easily secure Amazon VPC environments with built-in HA and scaling.
- **Simplified management:** Cloud-native organizations can use the lightweight user interface and intuitive wizards on the FortiGate CNF console to easily create, deploy, and manage security policies for their AWS environment. For hybrid cloud deployments, you can use a centralized management tool like FortiManager to define, deploy, and manage advanced security policies, backed by the FortiGuard Global Threat Intelligence service, which operates consistently across hybrid environments. You can use integration with AWS Firewall Manager to streamline security workflows and automate security rollout, saving time and increasing efficiency.
- **Lower costs:** Because there is no security software infrastructure to build, deploy, and operate, operational costs are reduced. Organizations also can save on the training and resourcing costs that would be necessary to deliver do-it-yourself security on AWS. Aggregating security across a region into a single CNF instance avoids the extra costs accrued by solutions that charge by cloud network or availability zone. In addition, the FortiGate CNF service uses AWS Graviton instances to deliver better price performance.

DO NOT REPRINT**© FORTINET**

Benefits of FortiGate CNF

- Scalable, flexible, and security capabilities
 - CNF can scale up or down based on the network demands
 - Works seamlessly in a cloud environment and is easy to deploy
 - Advanced security capabilities
- Easy Integration and automation
 - Integrate with other security solutions and cloud platforms
 - Can be easily automated
- High performance with cost-effectiveness
 - Optimized for cloud environments
 - More cost-effective than traditional firewalls



CNF is delivered as a service that scales to demand and doesn't require customer maintenance. For example, customers can define and assign policies to protect networks without configuring, provisioning, or maintaining any firewall software infrastructure.

FortiGate CNF offers several key benefits, including:

Scalability: Scales quickly to accommodate changing workload demands.

Flexibility: Works seamlessly in cloud environments, providing flexibility in deployment and management.

Security: Provides advanced security capabilities, protecting workloads against a wide range of threats and vulnerabilities.

Integration: Integrates with other security solutions and cloud platforms, enabling organizations to create a comprehensive security ecosystem.

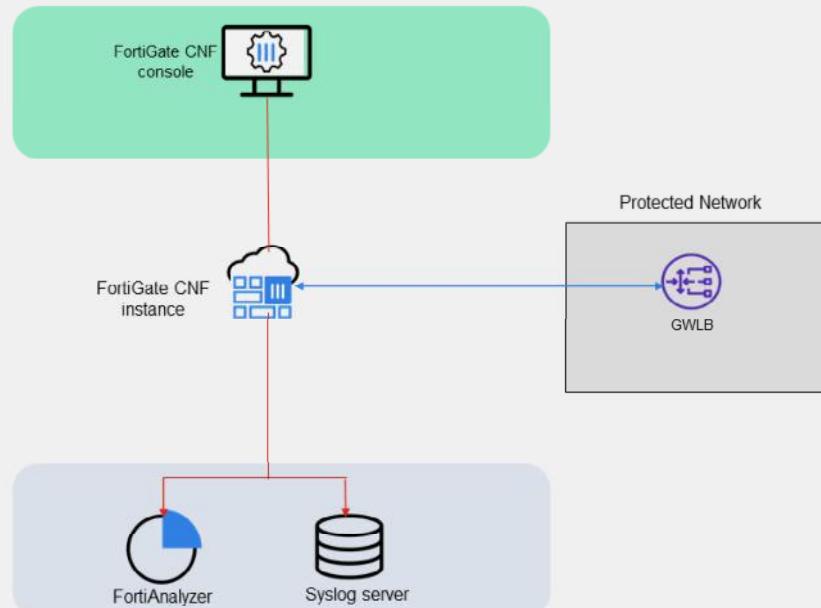
Automation: Is easily automated, allowing organizations to streamline their security operations and reduce the risk of human error.

Performance: Is optimized for cloud environments, providing high-performance security and networking capabilities that are essential for modern cloud workloads.

Cost-effectiveness: Can be more cost-effective than traditional firewalls because they are designed to work seamlessly in cloud environments and can be scaled as needed, reducing the need for expensive hardware or software licenses.

DO NOT REPRINT
© FORTINET

Components of FortiGate CNF



© Fortinet Inc. All Rights Reserved. 17

This slide shows the FortiGate CNF console, your primary management interface for creating FortiGate CNFs, defining and deploying policies, and onboarding cloud accounts for protection. You can also use FortiGate CNF to create a load balancer and distribute logs from CNF instances to a customer syslog server or FortiAnalyzer.

DO NOT REPRINT
© FORTINET

What Is Gateway Load Balancer?

- Scalable and highly available entry point for network traffic
- Centralized entry point
- Distributes traffic across multiple availability zones
- Gateway load balancer (GWLB) uses GWLB endpoint (GWLBe)



AWS GWLB



Azure GWLB



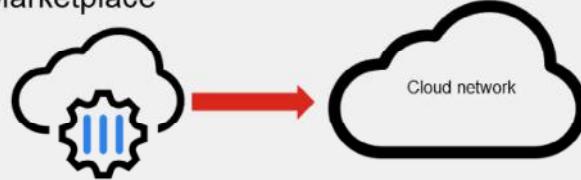
The GWLB simplifies deployment and management of virtual instances by providing a scalable and highly available entry point for network traffic. It serves as a centralized entry point for incoming and outgoing network traffic, allowing you to route traffic to and from multiple virtual instances in your network. It is typically designed for HA, allowing you to distribute traffic across multiple availability zones.

The GWLB deploys a GWLBe, which is referenced in AWS route tables to forward traffic. Instead of routing traffic directly out to the internet gateway, you can use the GWLBe to forward traffic to a FortiGate or FortiGate CNF first and then to the internet.

DO NOT REPRINT**© FORTINET**

FortiGate CNF Cloud Vendor Integration

- Seamless and transparent integration into existing cloud network
- Ability to associate with cloud vendor accounts
- Available on AWS Marketplace and Azure Marketplace



FortiGate CNF integrates seamlessly with your existing cloud vendor infrastructure. The service is in a separate subnet from your existing cloud network. When the instance is deployed to this subnet, a cloud load balancer is deployed with it, which is then used to forward all traffic requiring inspection to FortiGate CNF.

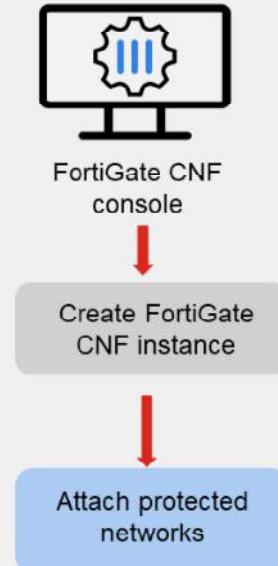
A FortiGate CNF instance is dedicated to one customer; however, it can connect to multiple VPCs, accounts, and availability zones. FortiGate CNF is available on the cloud vendor marketplace.

DO NOT REPRINT

© FORTINET

FortiGate CNF Setup

- Subscribe to FortiGate CNF service using the AWS Marketplace or Azure Marketplace
- Add the AWS or Azure cloud accounts with the FortiGate CNF console
- Create FortiGate CNF instance using the FortiGate CNF console
 - Define the instance name and select the cloud vendor region
- Protecting workload with FortiGate CNF
 - Deploy a load balancer endpoint in your cloud account
 - Route traffic to and from the FortiGate CNF



Setting up FortiGate CNF requires several steps, all of which you can perform on the FortiGate CNF console. The console is accessible through your FortiCloud account once you have subscribed to the service using the cloud vendor marketplace.

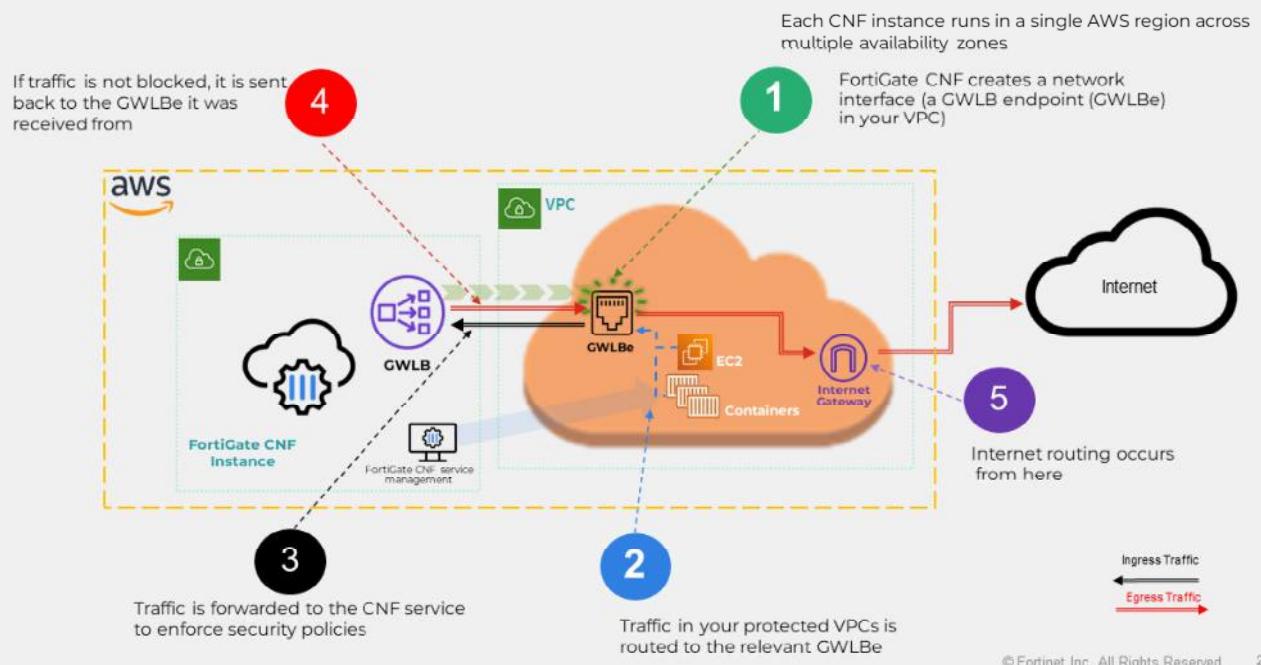
First, you must associate your AWS or Azure cloud account with FortiGate CNF. Then, you will be prompted to launch a template that allows FortiGate CNF read-only access to your cloud-protected networks.

Second, you must create a CNF instance using the FortiGate CNF console. You must define an instance name and select the cloud region in which to deploy the instance. This process can take up to ten minutes. When the process is complete, the instance will have been created.

Finally, to protect workloads with FortiGate CNF, deploy a load balancer endpoint in your AWS or Azure cloud accounts.

DO NOT REPRINT
© FORTINET

How FortiGate CNF for AWS Works

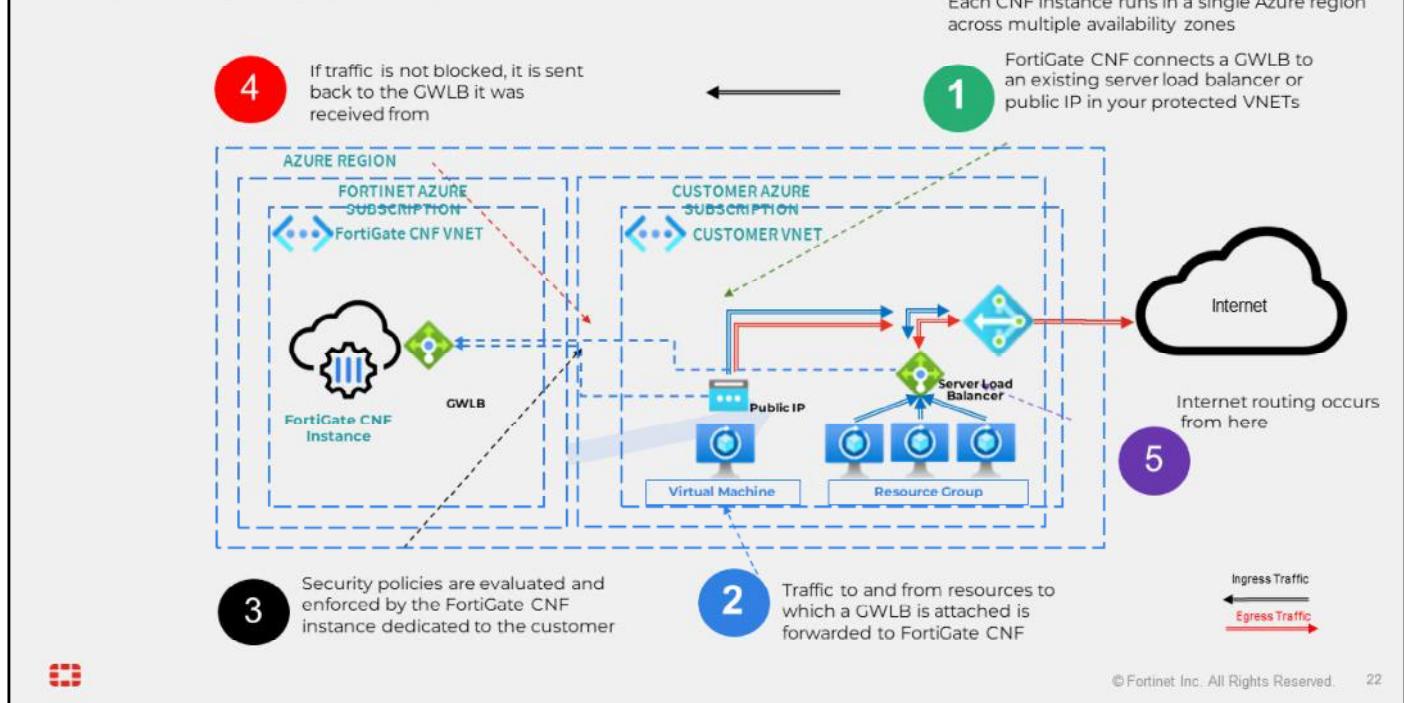


The following steps outline how FortiGate CNF works with AWS:

1. FortiGate CNF creates a network interface (a GWLB endpoint or a GWLBe in your VPC) in your protected networks.
2. Traffic in your protected VPCs is routed to the relevant GWLBe.
3. Traffic is forwarded to the CNF service to enforce security policies.
4. If traffic is not blocked, it is sent back to the GWLBe it was received from.
5. Traffic passes out through the internet gateway.

DO NOT REPRINT
© FORTINET

How FortiGate CNF for Azure Works



The following steps outline how FortiGate CNF works with Azure:

1. FortiGate CNF connects a GWLB to an existing server load balancer or public IP address in your protected VNets.
2. Traffic to and from resources to which a GWLB is attached is forwarded to FortiGate CNF.
3. Security policies are evaluated and enforced by the FortiGate CNF instance dedicated to the customer.
4. If traffic is not blocked, it is sent back to the GWLB it was received from.
5. Traffic then passes out through the Azure NAT Gateway.

DO NOT REPRINT
© FORTINET

Which Solution to Choose?



FortiGate VM



FortiGate CNF

Deployment Model	VM (IaaS)	Cloud-native (SaaS)
Network Operations	Granular control, but some experience required	Limited, but simple and easy to manage
Scalability	Requires configuration and planning	Automated
Use Cases	Hybrid and multi-cloud NGFW N/S and E/W within and between platforms Advanced functions: zero trust and SD-WAN Public and private cloud	AWS and Azure clouds Cloud-native apps requiring easy scaling Resource and staffing constraints
Security	State-of-the-art: Powered by FortiGuard Labs AI- and ML-based threat intelligence	



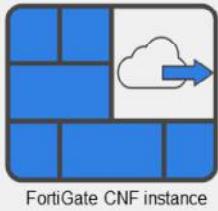
This slide shows a comparison of FortiGate CNF and FortiGate VM. FortiGate CNF is the preferred choice if your primary requirement is NGFW functionality. It is also the better choice if ease of management and scalability are important factors. If you require FortiGate to have additional features such as VPN, SD-WAN, or NAT functionality, choose FortiGate VM.

DO NOT REPRINT
© FORTINET

Use Cases—Outbound Traffic Inspection

- FortiGate CNF inspects outbound traffic

Secures against threats that include:



FortiGate CNF instance



Malware

Prevent unintentional downloads from intentional traffic



Data Exfiltration

Inspect cloud traffic to prevent exfiltration of sensitive information



Compliance Violations

Stop unauthorized communications with restricted entities and regions



Botnets

Block communications to botnet command and control servers



Cryptomining

Prevent connections that exploit cloud resources for cryptomining



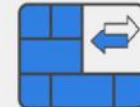
A primary use case for FortiGate CNF is outbound traffic inspection. It protects against common threats arising from unsecured outbound traffic, such as:

- Malware: connections to compromised servers resulting in unintentional malware downloads
- Data exfiltration: compromised systems communicating out and sending data to unauthorized systems
- Command and control (C&C) server communication: compromised workloads communicating with C&C servers to receive commands for malicious actions
- Cryptomining: connections to IP addresses that exploit cloud resources for cryptomining purposes
- Compliance violations: unauthorized communications with restricted or prohibited countries, systems, or other entities not in accordance with published guidelines

DO NOT REPRINT
© FORTINET

Use Cases—East-West and Inbound Protection

- East-west traffic security
 - FortiGate CNF stops the lateral spread of threats between workloads in different trust zones
- Inbound traffic protection
 - FortiGate CNF uses deep visibility and advanced security to prevent intrusion and other cyberthreats from compromising your workloads



FortiGate CNF instance

East-West Traffic Security



FortiGate CNF instance

Inbound Traffic Protection



FortiGate CNF is capable of handling east-west traffic security between workloads and zones, as well as inbound traffic protection. FortiGate CNF enforces compliance using geo-location policies to prevent communication with restricted or prohibited regions.

DO NOT REPRINT

© FORTINET

Knowledge Check

1. Who is responsible for building security in the public cloud?
 A. Customer
 B. Cloud provider

2. Which product is the best solution for SD-WAN deployment in the public cloud?
 A. FortiGate CNF
 B. FortiGate VM



DO NOT REPRINT

© FORTINET

Lesson Overview



Cloud Security Solutions



FortiGate VM and FortiGate CNF



© Fortinet Inc. All Rights Reserved. 27

Congratulations! You have completed this lesson.

Now, you will review the objectives that you covered in this lesson.

DO NOT REPRINT

© FORTINET

Review

- ✓ Identify threats and challenges in the public cloud
- ✓ Identify Fortinet public cloud solutions
- ✓ Identify FortiGate VM in the cloud
- ✓ Describe FortiGate CNF
- ✓ Identify the differences between FortiGate CNF and FortiGate VM



© 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 about Fortinet cloud security solutions and which solutions to choose.

DO NOT REPRINT

© FORTINET

FORTINET
Training Institute

FortiOS Administrator

FortiSASE

 FortiOS 7.6

Last Modified: 6 October 2025

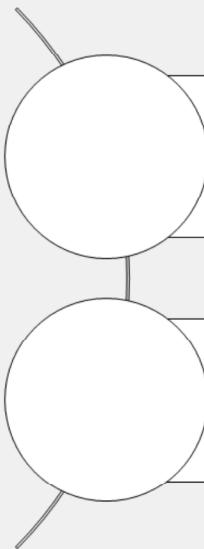
© Fortinet Inc. All Rights Reserved. 1

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

DO NOT REPRINT

© FORTINET

Lesson Overview



FortiSASE Solution Overview

FortiSASE Use Cases



© Fortinet Inc. All Rights Reserved.

2

In this lesson, you will learn about the topics shown on this slide.

DO NOT REPRINT

© FORTINET

FortiSASE Solution Overview

Objectives

- Describe the challenges with remote work
- Describe SASE architecture
- Identify FortiSASE components
- Describe security features



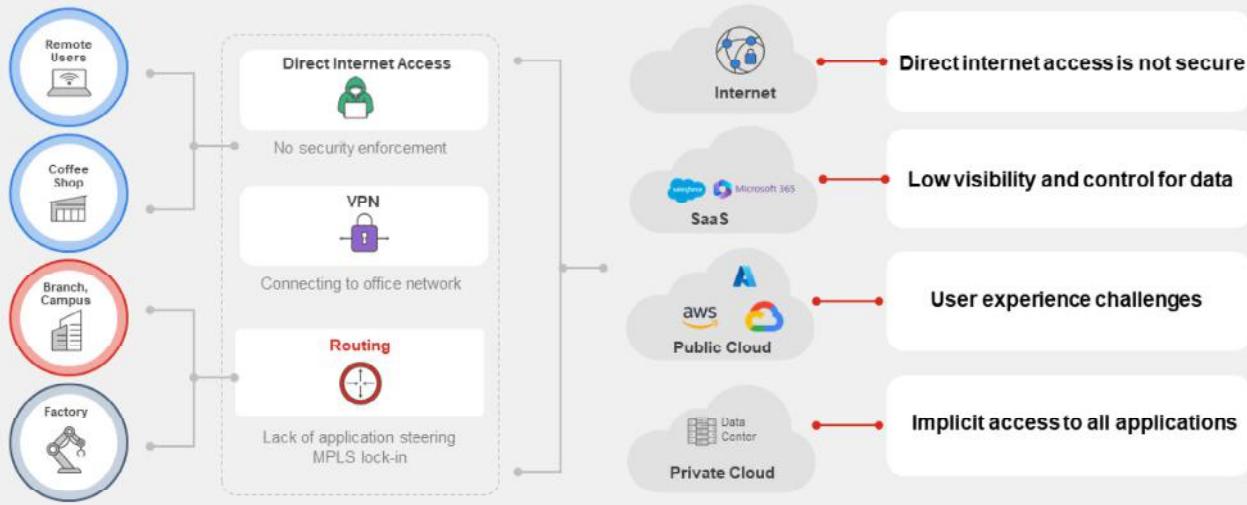
© Fortinet Inc. All Rights Reserved. 3

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

By demonstrating a competent understanding of FortiSASE, you will be able to describe the associated issues and identify FortiSASE solutions.

DO NOT REPRINT
© FORTINET

Challenges of Work-From-Anywhere



© Fortinet Inc. All Rights Reserved.

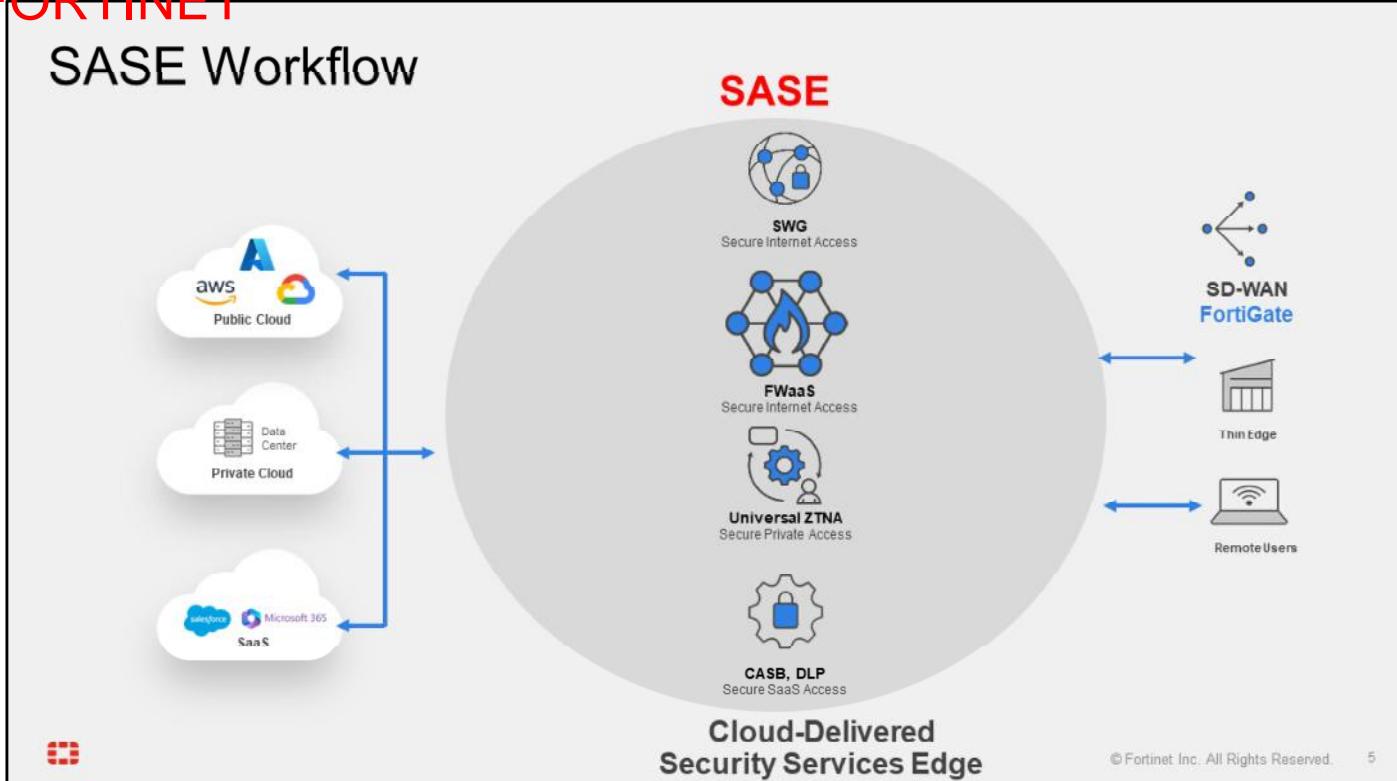
4

The current network infrastructure—relying on corporate VPNs and data centers for access—combined with the growing use of hybrid work models and distributed applications, presents the following challenges:

- Inconsistent security: Users receive different levels of access based on their "trust profile". For example, a remote worker outside the corporate network is considered "untrusted" and must use a VPN to connect to the internal network. On the other hand, a branch office employee is deemed "trusted" and can connect directly. Additionally, remote internet access from endpoints like BYOD devices isn't protected by the same corporate policies as office access. This gap allows malware to enter through endpoint devices and potentially spread to the corporate network when the endpoint devices reconnect.
- Lack of visibility and control: When securing data in Software-as-a-Service (SaaS) applications, corporate infrastructures and data centers lack visibility into remotely accessed SaaS traffic, creating a blind spot in the security framework.
- Performance issues: Routing all user traffic through a VPN to access the internet and SaaS applications can degrade performance for the end user. VPNs also pose security risks by granting broad network access, allowing malware to infiltrate and spread across systems.

DO NOT REPRINT
© FORTINET

SASE Workflow



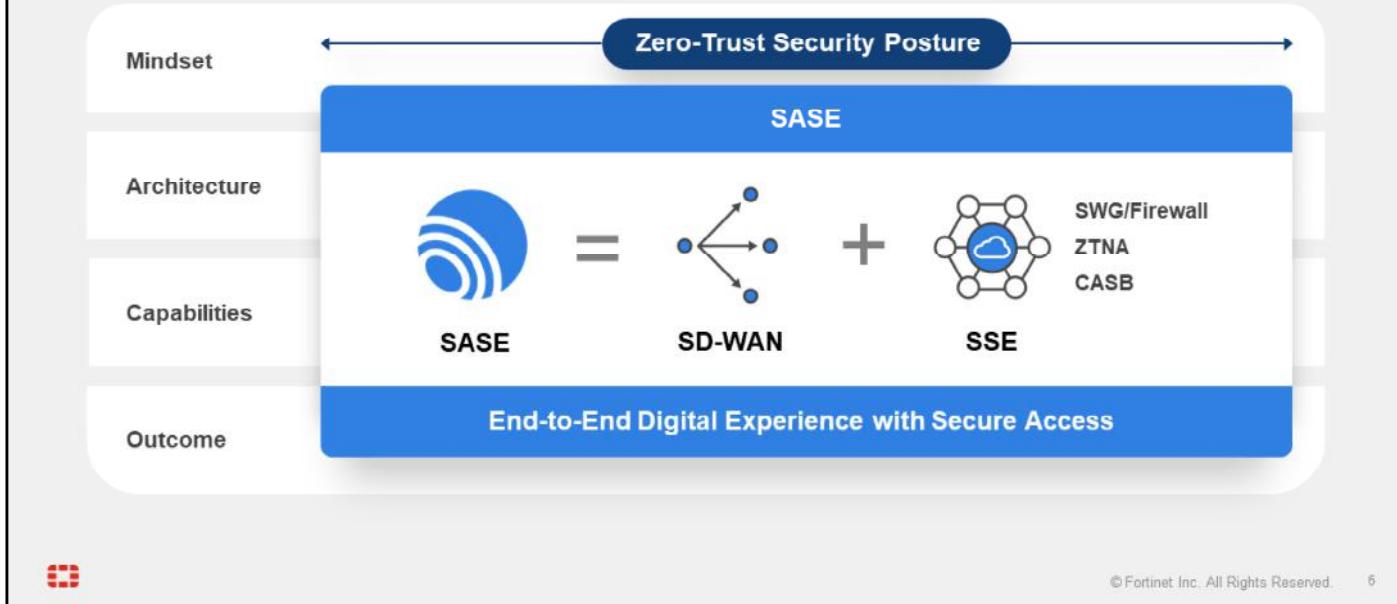
SASE provides hybrid and remote workers with secure access to corporate applications, data, and services so they can work from anywhere, no matter where the resources are located. SASE secures hybrid work by converging cloud-delivered security services with advanced networking capabilities to improve workers' productivity with consistently secure access and connectivity from edge to edge.

The main objectives and goals of the SASE architecture are as follows:

- Achieve secure internet access for off-net endpoints that connect to a cloud-delivered security service that is located between a user and the internet.
- Reduce latency by having off-net endpoints connect to the closest point of presence (POP) offered by a cloud-delivered security service.
- Meet the traffic demands of off-net endpoints by providing a cloud-delivered security service that scales dynamically.
- Reduce congestion by distributing endpoint traffic to different POPs with sufficient geographical spread and avoiding a single point required for traffic flow.
- Enforce a zero-trust model to provide protected network access for off-net endpoints.

DO NOT REPRINT
© FORTINET

A Solution to Simplify and Enable Secure Access



SASE is built on a zero-trust security posture, emphasizing the principle of “never trust, always verify”. Zero-trust ensures that every user, device, and application is continuously authenticated and authorized, no matter where they are.

SASE is composed of two parts: on-premises security and networking with SDWAN and cloud-delivered security service edge (SSE) for remote worker security and visibility. SSE includes essential security services such as:

- Secure web gateway (SWG) and Firewall-as-a-Service (FwaaS) to protect users and devices from web-based threats
- Zero trust network access (ZTNA) that delivers secure, explicit, identity-based access
- Cloud access security broker (CASB) that ensures secure access to SaaS applications and protects sensitive data

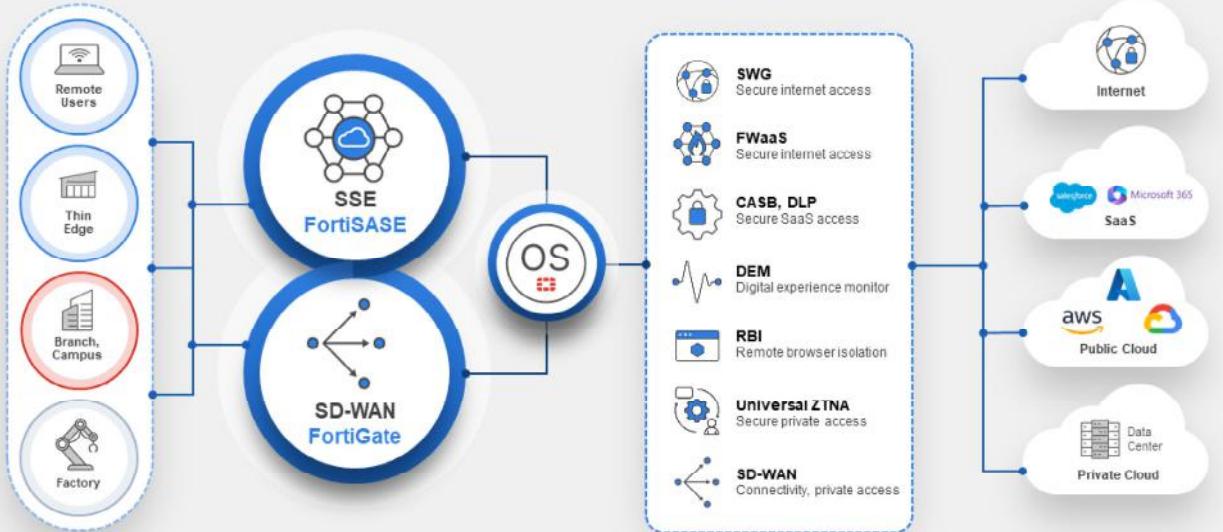
By integrating SD-WAN and SSE, SASE provides an end-to-end secure and optimized digital experience. It enables secure access for users working remotely, in the office, or across hybrid environments while simplifying IT operations and improving productivity.

DO NOT REPRINT

© FORTINET

Fortinet Unified SASE

- The unified SASE solution includes the FortiSASE SSE solution with secure SD-WAN



© Fortinet Inc. All Rights Reserved.

7

FortiSASE, the Fortinet unified 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.

At its core, the Fortinet SASE solution comprises two key elements: FortiSASE for SSE and secure SD-WAN for SD-WAN. Both are built on the unified, robust foundation of FortiOS, ensuring seamless integration and avoiding the complexities often associated with acquired technologies. The cloud-delivered security service is located between the remote endpoints and any networks that 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.

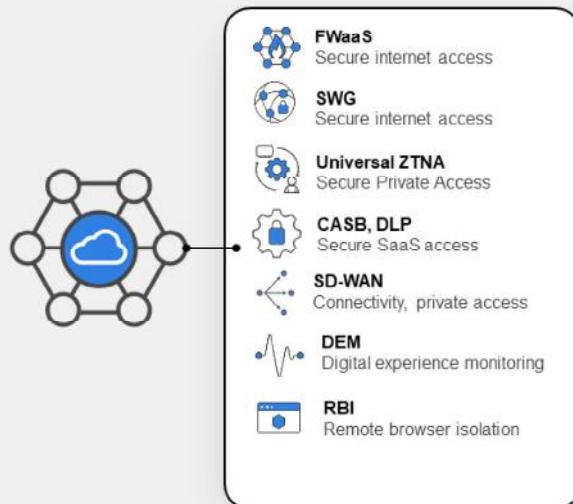
The primary objective of the Fortinet SASE offering is to provide global protection for users, enabling secure access to any application from any location. SSE and SD-WAN serve as the critical security gatekeepers.

In summary, the Fortinet SASE solution delivers a unified, flexible, and intelligent platform that ensures superior security and performance.

DO NOT REPRINT**© FORTINET**

Fortinet SASE Solution

- FortiSASE provides secure access to remote users for the following use cases:
 - Secure internet access (SIA)
 - Secure Private Access (SPA)
 - Secure SaaS access (SSA)
- Supports FWaaS
 - Same features as FortiGate next-generation firewall (NGFW)
- Supports SWG
 - Uses FortiOS explicit web proxy, captive portal, and authentication features



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

- SIA enables secure web browsing for remote users to protect from known and unknown threats
- SPA enables explicit application access under a zero-trust access or with SD-WAN integration to ensure secure application access
- SSA addresses shadow IT visibility challenges and safeguards data loss prevention

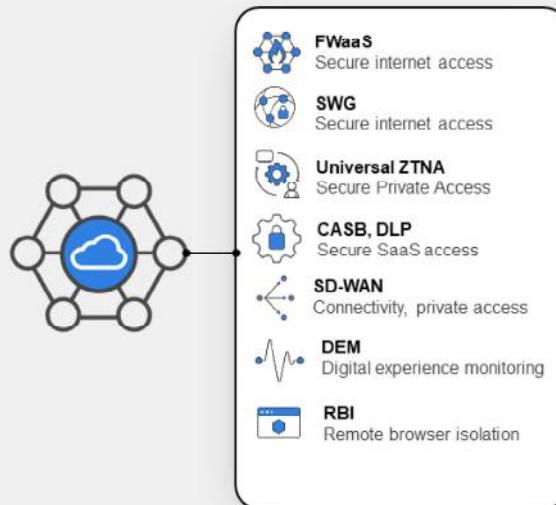
FortiSASE supports FWaaS and SWG functionality, both of which rely on threat intelligence that FortiGuard Labs provides. The FortiSASE FWaaS delivers the same features, security, and reliability as Fortinet FortiGate NGFW physical devices and virtual instances, which customers have long relied on. Likewise, FortiSASE SWG relies on the 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. To connect to FortiSASE in secure web gateway (SWG) mode, each endpoint client must configure proxy settings within its network or browser settings to point to the FortiSASE servers. You can configure this individually on the endpoint or, if you are using an enterprise management system, push it out to managed endpoints centrally.

DO NOT REPRINT

© FORTINET

Fortinet SASE Solution (Contd)

- Supports ZTNA
 - Provides secure, identity-based access with explicit control
- CASB and DLP
 - Supports both data at rest and in motion
- FortiGate SD-WAN integration
 - FortiSASE security POPs act as spokes to the FortiGate hub
- DEM
 - Monitor and troubleshoot user-to-SaaS application performance issues
- RBI
 - Protect against web-based threats for end users



FortiSASE supports ZTNA. Applying ZTNA everywhere for all users and devices—regardless of location—shifts implicit access to explicit control. Granular controls applied for each application, combine user authentication, continuous identity, context validation, and integration. Full support is also available for agentless devices.

FortiCASB provides cloud-based and API-based features to enable deep inspection of SaaS applications to enable detailed monitoring, analysis, and reporting features. FortiSASE also provides inline CASB functionality with web filter and application control security features. Data loss prevention (DLP) helps to identify, monitor, and protect organizational data at rest and in motion.

Organizations can integrate FortiSASE with existing FortiGate SD-WAN deployments to provide remote users access to private resources.

Digital experience monitoring (DEM) can assist administrators with troubleshooting remote user connectivity slowness with enhanced health check visibility of SaaS applications, endpoint devices, network paths, and LAN health, reducing resolution times and ensuring a positive user experience.

Remote browser isolation (RBI) isolates browser sessions for specific websites or categories within a secure environment, safely rendering content in a remote container.

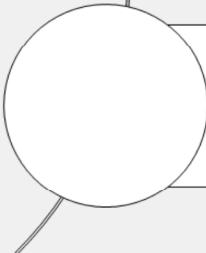
DO NOT REPRINT

© FORTINET

Lesson Progress



FortiSASE Solution Overview



FortiSASE Use Cases



© Fortinet Inc. All Rights Reserved.

10

Good job! You now understand the current challenges of work-from-anywhere and FortiSASE solutions.

Now, you will learn about FortiSASE use cases.

DO NOT REPRINT

© FORTINET

FortiSASE Use Cases

Objectives

- Describe user onboarding with SAML single sign-on (SSO)
- Identify agent-based and agentless modes
- Describe SIA for edge devices
- Identify site-based remote user internet access
- Describe SSA using inline CASB
- Describe SSA using FortiCASB



© Fortinet Inc. All Rights Reserved. 11

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

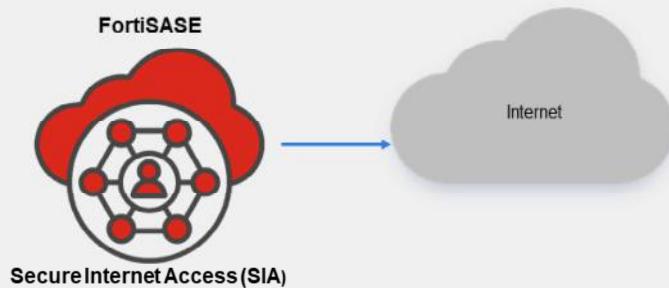
By demonstrating a competent understanding of secure access service edge (SASE) use cases, you will understand the purpose and capabilities of SASE.

DO NOT REPRINT

© FORTINET

SIA

- SIA extends an organization's security perimeter
- SIA enforces common security policies for the following:
 - Intrusion prevention systems (IPS)
 - Application control
 - Web and DNS filtering
 - Antimalware
 - Sandboxing
 - Antibotnet/command and control (C&C)



SIA is one of the FortiSASE use cases. The comprehensive FWaaS and SWG capabilities secure managed and unmanaged devices by supporting agent and agentless approaches. Natively integrated FortiGuard AI-Powered Security Services protect content and users from ransomware and other sophisticated attacks. SIA extends an organization's security perimeter that an NGFW typically achieves to remote users by enforcing common security policies for the IPS, application control, web filtering, DNS filtering, antimalware, sandboxing, antibotnet, and C&C.

DO NOT REPRINT

© FORTINET

SIA (Contd)

- For remote users, thin edge, and branch locations



Flexible steering methods

Agent, agentless, thin edge, and branch access
Branch access can be either through a third-party router or FortiGate



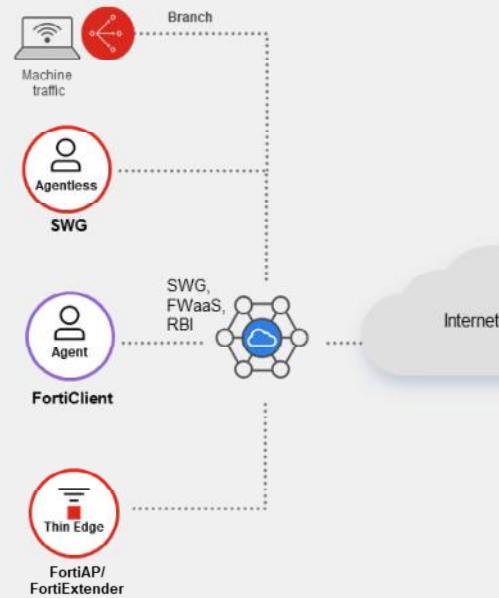
Malware and ransomware prevention

Prevent threats with cloud-based firewall, IPS, web filtering, antivirus, DNS and file filtering, sandboxing, and RBI



Full threat protection

Deep SSL inspection of web and SaaS applications for threats, best-in-class security efficacy, and zero-day threat protection with FortiGuard AI-Powered Security Services



In the past, remote users were typically secured using VPN, and many organizations still rely on this approach today. Unfortunately, this method isn't secure enough and is a significant factor in the increasing frequency of breaches.

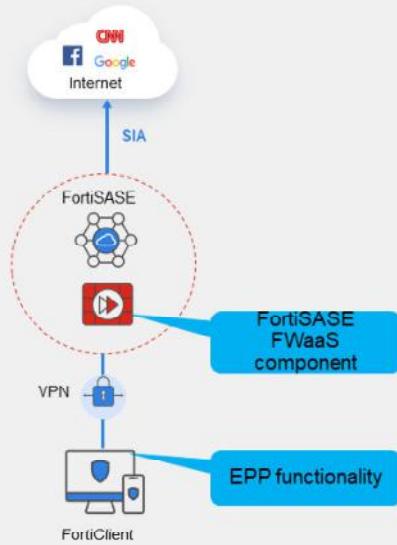
Securing internet access is more important than ever, especially with the rise in remote work. Without adequate protection at users' locations, any malware attack on a remote worker can easily spread across your entire organization, putting everyone at risk. FortiSASE supports agent, agentless, thin edge, and branch access deployments. Branch access can be either through a third-party router or FortiGate. FortiSASE SIA extends the security of an organization by applying a common security policy to remote users for IPS, application control, web filtering, antimalware, sandboxing, and so on. FortiSASE also provides native support for full SSL inspection at no additional cost, ensuring that even encrypted traffic is fully protected. FortiSASE redirects the internet traffic of remote users to the closest FortiSASE POP using geolocation selection.

DO NOT REPRINT

© FORTINET

SIA—Agent-Based Use Case

- Most typical use case
- Install FortiClient on managed endpoints
 - Lightweight agent
 - EPP functionality
- FortiSASE FWaaS is located between the FortiClient endpoint and the internet
- FortiClient connects to FortiSASE using a VPN tunnel
- VPN policies on FortiSASE secure all internet traffic
- User-based licensing is required



© Fortinet Inc. All Rights Reserved. 14

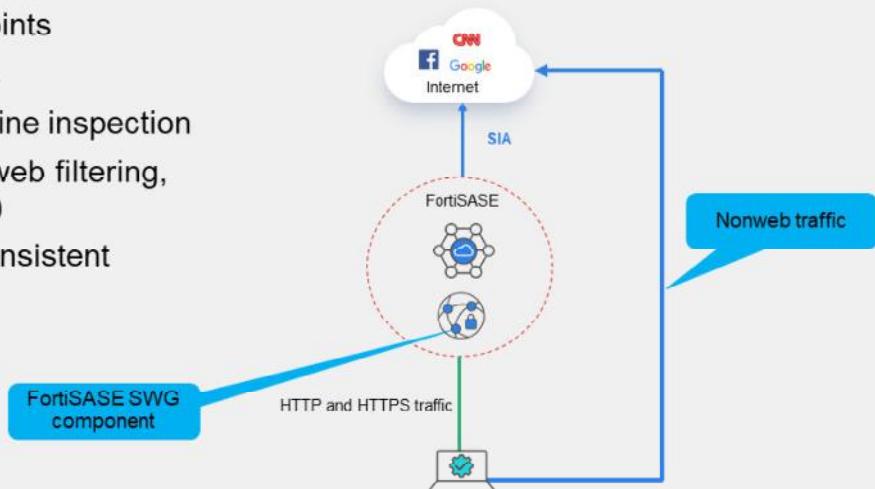
Agent-based deployment is the most common FortiSASE deployment use case. In agent-based mode, FortiClient connects to FortiSASE using a secure VPN tunnel. Once the connection is established, FortiSASE acts as a firewall and is placed between the endpoint and the internet. The VPN policy on FortiSASE is configured with the required security components, such as web filtering, application control, and so on, to secure the internet traffic. Agent-based mode also supports configuring ZTNA for compliance checks.

By default, FortiSASE supports remote user connectivity using IPsec VPN.

DO NOT REPRINT
© FORTINET

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 filtering, application control, and so on)
- Shared security profiles for consistent protection



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 an SWG and distributes a proxy auto-configuration (PAC) file to end users, enabling the FortiSASE SWG service as an explicit web proxy. SWG deployment secures only web traffic protocols, such as HTTP and HTTPS. The web browser redirects HTTP and HTTPS traffic to FortiSASE, which secures user web traffic by implementing SWG security policies. The SWG component on FortiSASE offers a full security stack with antivirus, web filtering, application control, and so on.

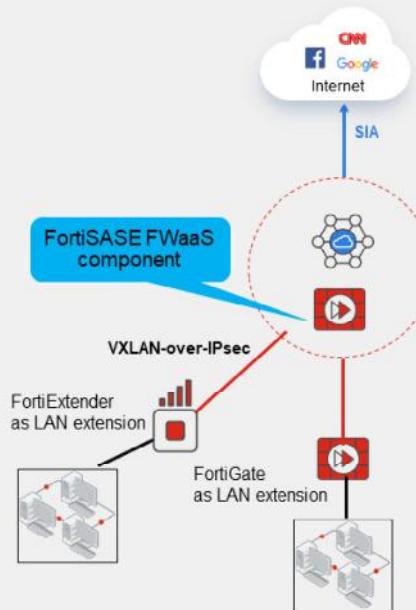
All other nonweb traffic bypasses FortiSASE and is forwarded directly to the internet.

The security profiles can be shared between agent and agentless deployments for consistent protection. This use case is usually recommended for unmanaged endpoints like contractors or temporary employees.

DO NOT REPRINT
© FORTINET

Site-based Remote User Internet Access

- Usually for microbranch offices
- Requires configuring FortiExtender or FortiGate as a LAN extension
- FortiExtender or FortiGate is responsible for centralizing site connectivity to the FortiSASE FWaaS
- FortiExtender, FortiBranchSASE, or FortiGate establishes a secure VXLAN-over-IPsec with FortiSASE



© Fortinet Inc. All Rights Reserved. 16

In the example deployment shown on this slide, FortiExtender and FortiGate are used as LAN extensions.

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

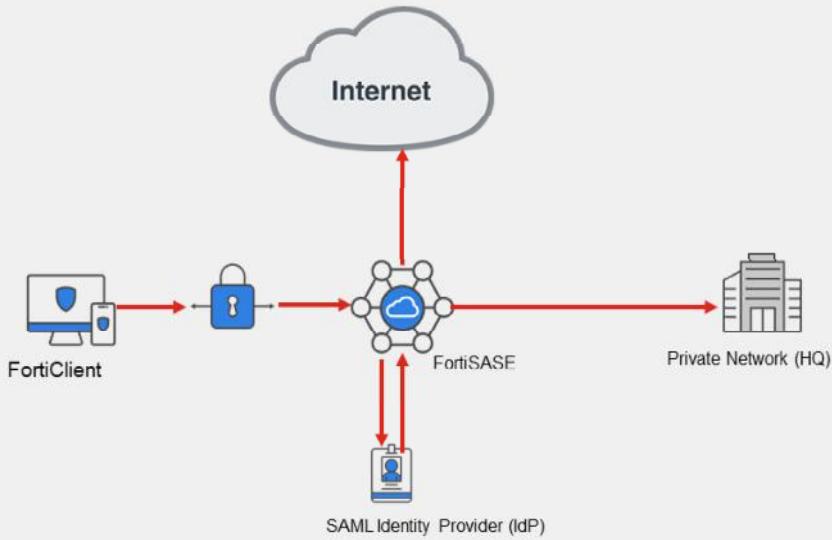
When you deploy an edge FortiGate as a FortiSASE LAN extension, FortiSASE can inspect traffic for users connected to the LAN extension. This can help offload some of the security inspection tasks from the edge FortiGate. You can also use the SD-WAN functionality on the edge FortiGate to apply application steering to FortiSASE.

DO NOT REPRINT

© FORTINET

User onboarding with SAML SSO

- FortiSASE is the service provider
- Products such as FortiAuthenticator, Okta, Entra ID, and so on can act as identity providers



© Fortinet Inc. All Rights Reserved. 17

SSO works by sharing and verifying login credentials between service and identity providers. A service provider is typically a vendor who provides products, solutions, and services to users and organizations, such as an application or website. An identity provider (IdP) is a system that creates, manages, and maintains user identities and provides authentication services to verify users. These trusted providers enable users to use SSO to access applications and websites and improve user experience by reducing password fatigue.

FortiSASE provides support for many authentication servers, including local database, RADIUS, LDAP, and SAML for SSO. You can configure local users on FortiSASE. These users will directly authenticate with FortiSASE.

You can configure SSO authentication for user onboarding on the **User Onboarding SSO** page. The service provider fields are preconfigured and should be added to your IdP server. You must enter the IdP configuration on FortiSASE to complete the SSO configuration.

DO NOT REPRINT

© FORTINET

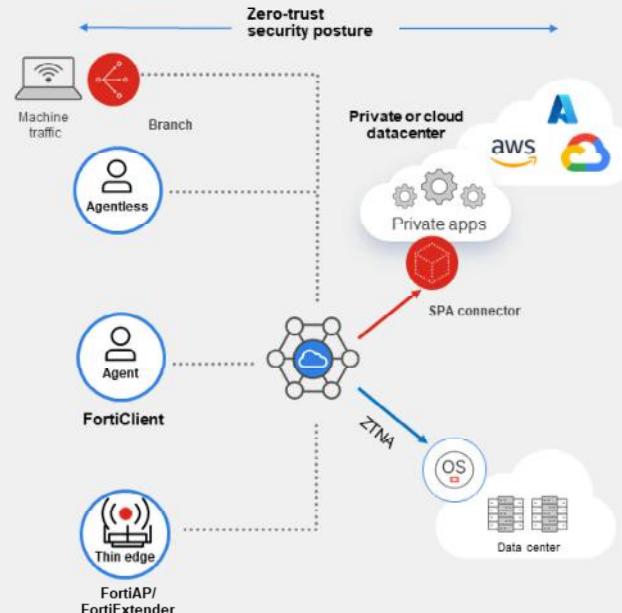
SPA

- With ZTNA and SD-WAN integration

Secure cloud and data-center application access
Secure anywhere access to corporate applications in data center and cloud with deep security inspection

Universal zero trust network access (ZTNA)
User identity and device context-based zero-trust access to explicit applications from remote or on-premises location
Agentless flexibility through portal

SPA connector (two options)
Lightweight VM to integrate FortiSASE with the customer's private applications
Can leverage existing FortiGate in data center to integrate FortiSASE with the customer's private applications in minutes



© Fortinet Inc. All Rights Reserved. 18

When it comes to SPA, FortiSASE offers two main options:

- Direct application access without traversing FortiSASE POPs: This option is ideal for latency-sensitive applications. With this setup, ZTNA capabilities are enforced for user traffic along this path, ensuring that users are continuously verified before gaining access. However, since the traffic doesn't pass through FortiSASE POPs, it is not inspected inline.
- Application access through FortiSASE POPs for inline inspection: In this approach, traffic is routed through FortiSASE POPs before it reaches your private applications. This gives two major advantages:
 - Inline security inspection, which provides robust protection against threats.
 - The benefits of SD-WAN, which optimizes traffic flow between the POP and your SD-WAN hub or FortiGate at the datacenter. This method is particularly useful if your organization has mission-critical applications that require an extra layer of security and optimization.

Both options support ZTNA, and user traffic undergoes continuous posture verification. This process checks the user's identity and device posture in near real time, creating a dynamic security model.

DO NOT REPRINT
© FORTINET

SPA With SD-WAN Integration

SD-WAN Private Access



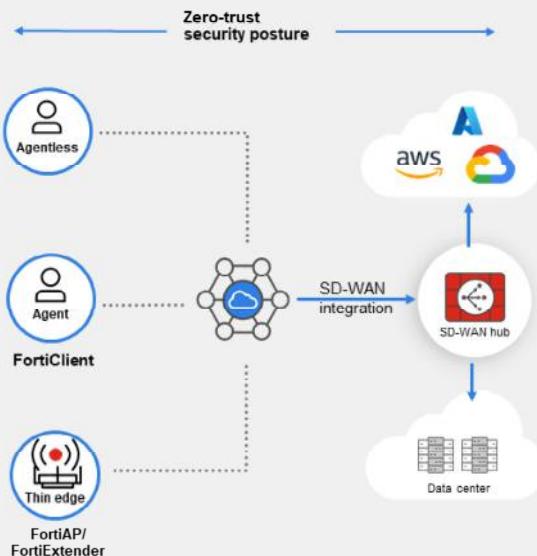
SD-WAN integration with existing SD-WAN hub from any **SASE POP**



Fast access to applications using **SD-WAN** from SASE POP to SD-WAN hub



Broader application support (UDP-based VoIP, video, unified communications)



© Fortinet Inc. All Rights Reserved.

19

Integrating SD-WAN with FortiSASE creates a truly powerful solution for secure and optimized access to applications, regardless of where users are located.

FortiSASE integrates seamlessly with SD-WAN to enhance security and performance. By routing traffic through FortiSASE POPs, user data is protected by zero-trust security, which includes real-time threat inspection. SD-WAN optimizes traffic routing based on real-time network conditions, ensuring that data bound for cloud services, SaaS applications, or private data centers is always routed over the most efficient path for a smooth user experience.

A key advantage of combining SD-WAN with FortiSASE is end-to-end optimization. By directing traffic from branch offices or remote workers through FortiSASE POPs, organizations can implement security measures such as SSL inspection, CASB, and FWaaS while benefiting from SD-WAN performance enhancements, which facilitate low-latency access.

This integration leverages SD-WAN to prioritize traffic according to business needs. Critical applications can be given higher priority, while less essential traffic can be handled with lower urgency. This approach optimizes bandwidth use and improves the overall user experience.

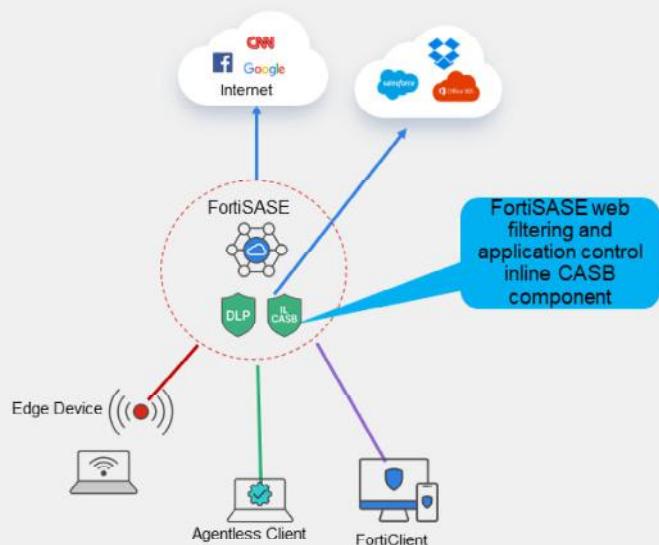
In summary, the combination of FortiSASE and SD-WAN creates a robust, flexible, and highly efficient security solution for optimizing the path and performance of users accessing applications in hybrid or remote work environments.

DO NOT REPRINT

© FORTINET

CASB Use Case

- FortiSASE uses its application control and SSL deep inspection to control SaaS cloud application traffic
- FortiSASE uses web filtering 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
- Supports integration with FortiCASB



© Fortinet Inc. All Rights Reserved. 20

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 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.

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. FortiSASE uses web filtering 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 restricts tenant access to control SaaS application behavior.

FortiSASE also uses 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.

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 uses an API to connect to the cloud application and scans the data at rest, meaning the data has already been uploaded to the SaaS application. Access to the FortiCASB portal is included with per-user and per-endpoint FortiSASE licensing. Out-of-band CASB is configured on the FortiCASB portal and is independent of FortiSASE configurations.

DO NOT REPRINT

© FORTINET

Knowledge Check

1. Which device acts as a service provider when SSO is configured on FortiSASE?
 - A. FortiAuthenticator
 - B. FortiSASE

2. Which file does FortiSASE distribute to users in an agentless deployment?
 - A. The PAC file
 - B. The FortiClient config file



DO NOT REPRINT

© FORTINET

Lesson Progress



FortiSASE Solution Overview



FortiSASE Use Cases



© Fortinet Inc. All Rights Reserved.

22

Congratulations! You have completed this lesson.

Now, you will review the objectives that you covered in this lesson.

DO NOT REPRINT

© FORTINET

Review

- ✓ Describe the challenges with remote work
- ✓ Describe SASE architecture
- ✓ Identify FortiSASE components
- ✓ Describe security features
- ✓ Describe user onboarding with SAML SSO
- ✓ Identify agent-based and agentless modes
- ✓ Describe SIA for edge devices
- ✓ Identify site-based remote user internet access
- ✓ Describe SSA using inline CASB
- ✓ Describe SSA using FortiCASB



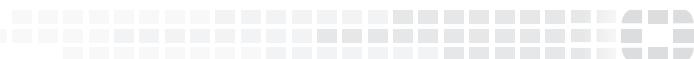
This slide shows the objectives that you covered in this lesson.

By mastering the objectives covered in this lesson, you how to use the FortiSASE components and the FortiSASE solution.

DO NOT REPRINT
© FORTINET



FORTINET®



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© 2025 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.