

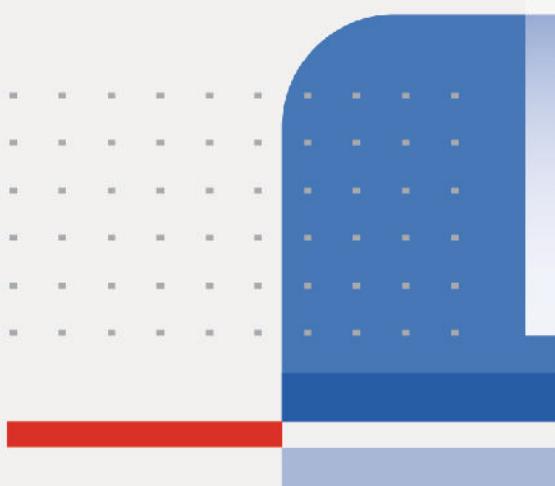
DO NOT REPRINT
© FORTINET



FortiGate Administrator Study Guide

FortiOS 7.4

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://kb.fortinet.com>

Fortinet Fuse User Community

<https://fusecommunity.fortinet.com/home>

Fortinet Forums

<https://forum.fortinet.com>

Fortinet Product Support

<https://support.fortinet.com>

FortiGuard Labs

<https://www.fortiguard.com>

Fortinet Training Program Information

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

Fortinet | Pearson VUE

<https://home.pearsonvue.com/fortinet>

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

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



TABLE OF CONTENTS

01 System and Network Settings.....	4
02 Firewall Policies and NAT.....	31
03 Routing.....	69
04 Firewall Authentication.....	95
05 Fortinet Single Sign-On (FSSO).....	123
06 Certificate Operations.....	158
07 Antivirus.....	192
08 Web Filtering.....	213
09 Intrusion Prevention and Application Control.....	237
10 SSL VPN.....	266
11 IPsec VPN.....	293
12 SD-WAN Configuration and Monitoring.....	342
13 Security Fabric.....	381
14 High Availability.....	408
15 Diagnostics and Troubleshooting.....	442

DO NOT REPRINT**© FORTINET**

FortiGate Administrator

System and Network Settings

A small red square icon containing a white square with a diagonal line, followed by the text "FortiOS 7.4".

Last Modified: 15 November 2023

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

DO NOT REPRINT**© FORTINET**

Objectives

- Configure FortiGate on factory default settings
- Configure FortiGate as the DHCP server
- Configure and control administrator access to FortiGate
- Back up and restore system configuration files
- Upgrade FortiGate firmware
- Check and verify FortiGuard licenses

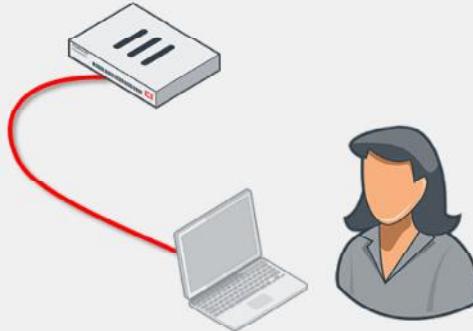
After completing this lesson, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in basic system and network administration, you will be able to install FortiGate into your network and configure basic networking settings. You will also be able to better manage administrative users to implement stronger security practices around administrative access.

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



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?

Now, you will take a look at how you set up FortiGate.

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, and you can begin setup.

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 logged in with default login details, you'll see a message to change the default blank password for the admin user password. Before you connect FortiGate to your network, you should set a complex password. You'll also be asked to apply additional configuration such as hostname, dashboard setup, register with FortiCare, and so on.

All FortiGate models have a console port and/or USB management port. 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

Interface IPs

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

The screenshot shows two side-by-side interface configuration pages from a FortiGate management interface.

Left Panel (Edit Interface):

- Name:** port5 (highlighted with a red box)
- Type:** Physical Interface
- VRF ID:** 0
- Role:** Undefined
- Addressing mode:** Manual (highlighted with a red box)
- IP/Netmask:** 0.0.0.0/0.0.0

Right Panel (Edit Interface):

- Name:** port5
- Type:** Physical Interface
- VRF ID:** 0
- Role:** Undefined
- Addressing mode:** DHCP (highlighted with a red box)
- Distance:** 5

Fortinet Training Institute logo and footer text: © Fortinet Inc. All Rights Reserved. 4

When FortiGate is operating in network address translation (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 list of policies
- Alias is a friendly descriptor for the interface:
 - Used in list of policies to label interfaces by purpose

The diagram illustrates the relationship between 'Alias' and 'Role' in Fortinet's interface configuration. Two blue rounded rectangles labeled 'Alias' and 'Role' have arrows pointing to two separate screenshots of the Fortinet GUI.

The top screenshot shows the 'Edit Interface' dialog. It displays an interface named 'port5' with an 'Alias' field containing 'Internal_Network'. The 'Role' dropdown menu is open, showing options: LAN, LAN, WAN, DMZ, and Undefined. The 'LAN' option is selected. Below the interface list, there are tabs for 'Manual' and 'DHCP'.

The bottom screenshot shows the 'Policy & Objects > Firewall Policy' list. It shows a policy entry for 'Full_access' that includes a source object 'Internal_Network (port5)'. This object is highlighted with a red box. The policy also specifies destination 'port1', source 'LOCAL_SUBNET', and action 'all'.

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 use of each interface, you can give them aliases. For example, you could call port3 **internal_network**. This can help to make your list of policies easier to comprehend.

DO NOT REPRINT
© FORTINET

FortiGate as a DHCP Server

Network > Interfaces

Edit Interface

Name: port3
 Alias: LAN
 Type: Physical Interface
 VRF ID: 0
 Role: LAN (highlighted)

Address

Addressing mode: Manual (highlighted)
 IP/Netmask: 10.0.1.254/255.255.255.0 (highlighted)

Administrative Access

IPv4: HTTPS (checked), HTTP (checked), PING (checked), FMG-Access (unchecked), SSH (unchecked), RADIUS Accounting (unchecked), Speed Test (unchecked), Use VDOM Setting (checked), Enable (checked), Disable (unchecked)

Receive LLDP (checked), Use VDOM Setting (checked), Enable (checked), Disable (unchecked)

Transmit LLDP (checked), Use VDOM Setting (checked), Enable (checked), Disable (unchecked)

DHCP Server

DHCP status: Enabled (radio button selected)
 Address range: 10.0.1.1-10.0.1.253
 Netmask: 255.255.255.0
 Default gateway: Same as Interface IP (radio button selected)
 DNS server: Same as System DNS (radio button selected)
 Lease time: 604800 second(s)

Advanced

Wireless clients are not the only ones that can use FortiGate as their DHCP server.

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

DO NOT REPRINT**© FORTINET**

VLANs

Physical
interfaces



VLANs

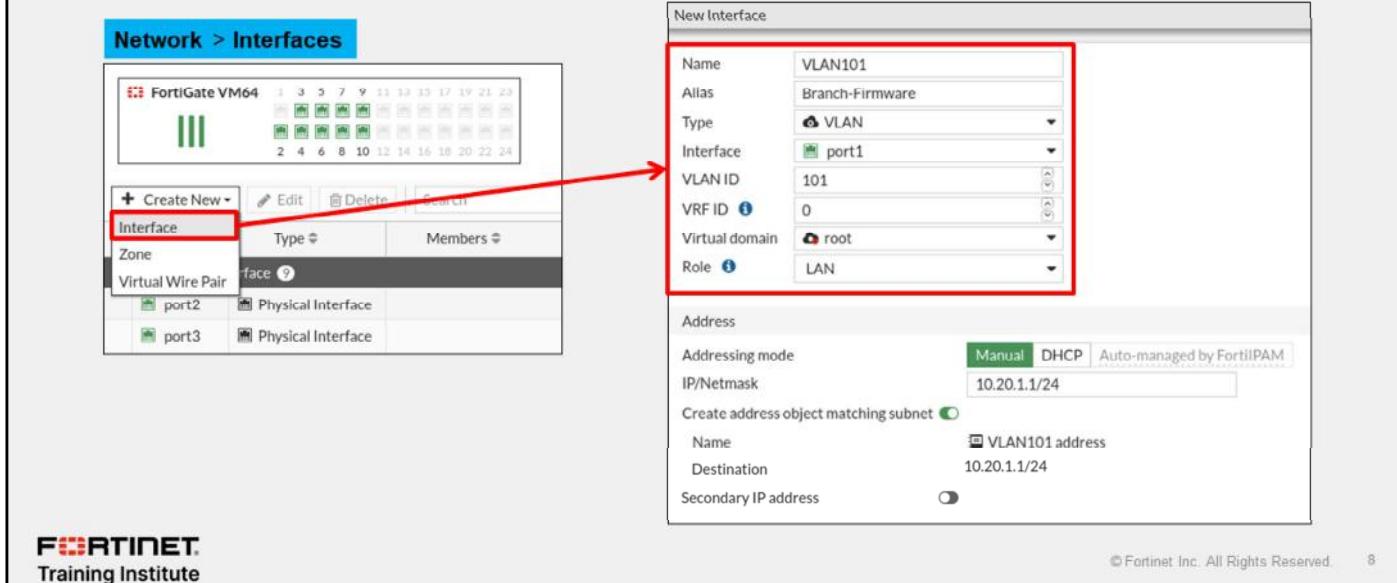
- *Logically* subdivide your physical layer 2 network into smaller segments
 - Each segment forms a separate broadcast domain
 - VLAN tags added to frames to identify their network segments

VLANs split your physical LAN into multiple, logical LANs. In NAT operation mode, each VLAN forms a separate broadcast domain. Multiple VLANs can coexist in the same physical interface, provided they have different VLAN IDs. In this way, a physical interface is split into two or more logical interfaces. A tag is added to each Ethernet frame to identify the VLAN to which it belongs.

DO NOT REPRINT
© FORTINET

Creating VLANs

- Frames sent or received by the physical interface segment are never tagged; they belong to the *native VLAN*



The screenshot shows the FortiGate Management Interface. On the left, under 'Network > Interfaces', there is a list of physical interfaces (port1, port2, port3) and a 'Create New' button. The 'Interface' button is highlighted with a red box. An arrow points from this button to the 'New Interface' dialog box on the right.

New Interface

Name	VLAN101
Alias	Branch-Firmware
Type	VLAN
Interface	port1
VLAN ID	101
VRF ID	0
Virtual domain	root
Role	LAN

Address

Addressing mode	Manual	DHCP	Auto-managed by FortiIPAM
IP/Netmask	10.20.1.1/24		

Create address object matching subnet

Name	<input checked="" type="checkbox"/> VLAN101 address
Destination	10.20.1.1/24
Secondary IP address	<input type="checkbox"/>

© Fortinet Inc. All Rights Reserved. 8

To create a VLAN using the GUI, click **Create New**, select **Interface**, and then, in the **Type** field, select **VLAN**. You must specify the VLAN ID and the physical interface to which the VLAN will be bound. Frames that belong to interfaces of that type are always tagged. On the other hand, frames sent or received by the physical interface segment are never tagged. They belong to what is called the *native VLAN* (VLAN ID 0).

Note that in a multi-VDOM environment, the physical interface and its VLAN subinterface can be in separate VDOMs.

DO NOT REPRINT

© FORTINET

Static Gateway

- Must be at least one default gateway
- If the interface is DHCP or PPPoE, you can add gateway dynamically

The screenshot shows the FortiGate Management Interface. On the left, under the 'Network' tab, 'Static Routes' is selected. A red box highlights the '+ Create New' button. On the right, a 'New Static Route' dialog box is open. It shows fields for Destination (Subnet: Internet Service, 0.0.0.0/0.0.0), Gateway Address (0.0.0.0), Interface (port1), Administrative Distance (10), and Status (Enabled). An 'Advanced Options' section is expanded, showing a Priority field set to 1. A callout bubble points to this field with the text: 'When multiple routes are equal in distance, routes with a lower priority value take precedence'.

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

9

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 probably also will not be able to connect to FortiGuard—important for FortiGate to access—for updates, and may not correctly route traffic.

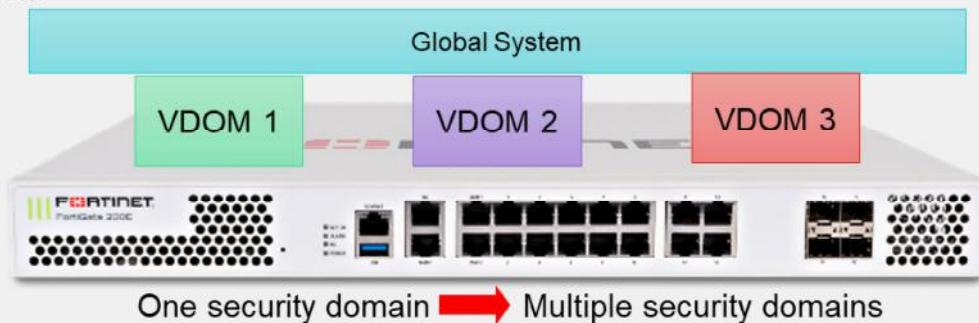
You should make sure that FortiGate has a route that matches all packets (destination is 0.0.0.0/0), known as a default route, and forwards them through the network interface that is connected to the internet, to the IP address of the next router.

Routing completes the basic network settings that are required before you can configure firewall policies.

You can expand **Advanced Options** and enter a priority value. When two routes have an equal distance, the route with a lower priority value takes precedence.

DO NOT REPRINT
© FORTINET

VDOMs



- VDOMs split FortiGate into multiple virtual devices
 - They employ independent security policies, routing tables, and so on
- Packets are confined to same VDOM
- By default, FortiGate supports up to 10 VDOMs
 - High-end models allow for the purchase of additional VDOMs

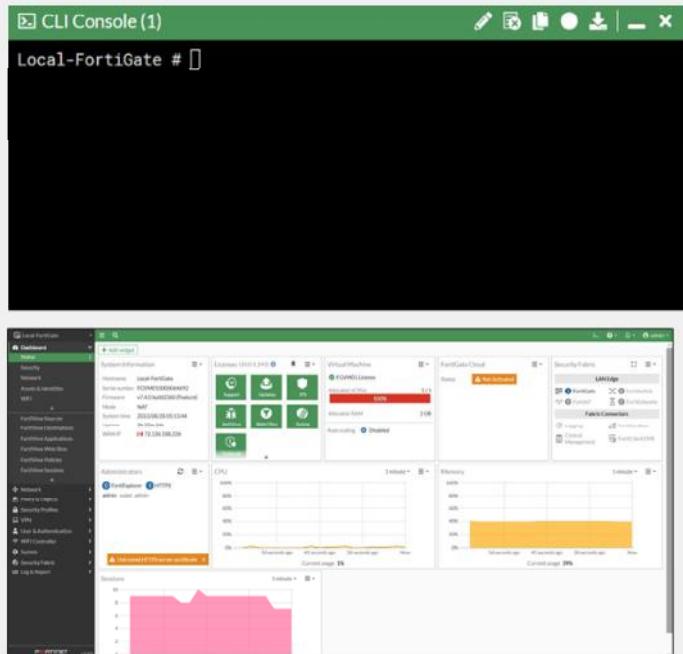
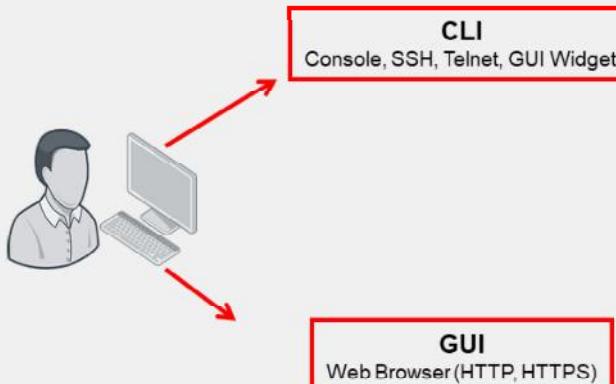
What if, more than segmenting your network, you want to subdivide policies and administrators into multiple security domains?

In that case, you can enable FortiGate VDOMs, which split your FortiGate into multiple logical devices. Each VDOM has independent security policies and routing tables. Also, and by default, traffic from one VDOM cannot go to a different VDOM. This means that two interfaces in different VDOMs can share the same IP address, without any overlapping subnet problems.

When you use VDOMs, a single FortiGate device becomes a virtual data center of network security, unified threat management (UTM) inspection, and secure communication devices.

DO NOT REPRINT
© FORTINET

Administration Methods



FORTINET
Training Institute

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 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 Telnet—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

Create an Administrative User

The screenshot illustrates the process of creating a new administrative user. On the left, the 'System > Administrators' page is displayed, showing the 'Create New' dropdown menu with 'Administrator' selected. A red arrow points from this selection to the 'New Administrator' configuration window on the right. The configuration window shows the following fields:

- Type:** Local User (selected)
- Password:** [REDACTED]
- Confirm Password:** [REDACTED]
- Comments:** Write a comment... (0/255)
- Administrator profile:** super_admin
- Other options:** Two-factor Authentication, Restrict login to trusted hosts, Restrict admin to guest account provisioning only.

Whichever method you use, start by logging in as admin. Begin by creating separate accounts for other administrators. For security and tracking purposes, it is a best practice for each administrator to have their own account.

In the **Create New** field, you can select either **Administrator** or **REST API Admin**. Typically, you will select **Administrator** and then assign an **Administrator Profile**, which specifies that user's administrative permissions. You could select **REST API Admin** to add an administrative user who would use a custom application to access FortiGate with a REST API. The application would allow you to log in to FortiGate and perform any task that your assigned **Administrator Profile** permits.

Other options, not shown here, include:

- Instead of creating accounts on FortiGate, you could configure FortiGate to query a remote authentication server.
- In place of passwords, your administrators could authenticate using digital certificates that are issued by your internal certification authority server.

If you do use passwords, ensure that they are strong and complex. For example, you could use multiple interleaved words with varying capitalization, and randomly insert numbers and punctuation. Do not use short passwords, or passwords that contain names, dates, or words that exist in any dictionary. These are susceptible to brute force attack. To audit the strength of your passwords, use tools such as L0phcrack (<http://www.l0phcrack.com/>) or John the Ripper (<http://www.openwall.com/john/>). Risk of a brute force attack is increased if you connect the management port to the internet.

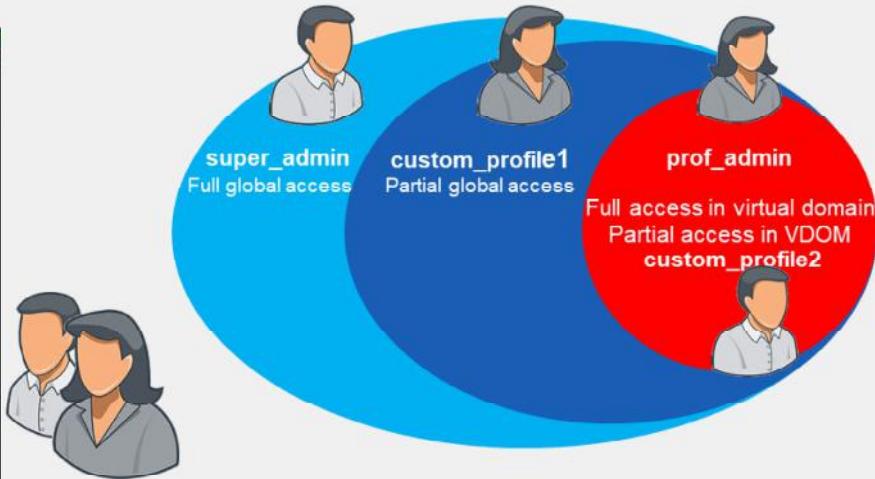
In order to restrict access to specific features, you can assign permissions.

DO NOT REPRINT
© FORTINET

Administrator Profiles

- Permissions

- Hierarchy



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. The `prof_admin` is another default profile. It also provides full access, but unlike `super_admin`, it applies only to its virtual domain—not the global settings of FortiGate you can change its permissions.

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, 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 per 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 log messages. Administrators may not be able to access global settings outside their assigned virtual domain either. Virtual domains (VDOMs) are a way of subdividing the resources and configurations on a single FortiGate. Administrators with a smaller scope of permissions cannot create, or even view, accounts with more permissions.

DO NOT REPRINT
© FORTINET

Administrative Access—Trusted Sources

The screenshot shows the FortiGate administrative interface under 'System > Administrators'. A red arrow points from the 'Trusted Host 1' field (containing '10.0.1.10/32') to a table listing administrators. The table shows a single entry for 'System Administrator' with 'admin' as the user and '10.0.1.10/32' as the trusted host. Below the interface, two callout boxes provide additional context:

- You can restrict admin user to manage guest users with a guest group in place to provision users**
- If the admin user attempts to log in to the FortiGate GUI from any IP other than 10.0.1.10, they receive this message**

On the right, a screenshot of the FortiGate GUI login page shows an 'Authentication failure' message.

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

14

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 for admin from which admin logs in. If admin attempts to log in from a machine with any other IP, 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. Instead, the administrator will receive this message: "Unable to contact server".

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

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

Another option to configure an administrator account to restrict access to only provision guest user accounts. By enabling this option, the administrator account will be able to provision guest user account given the fact a guest user group is available to provision guest users.

DO NOT REPRINT
© FORTINET

Administrative Access—Ports and Password

- Port numbers are customizable
- Using only secure access (SSH, HTTPS) is recommended
- Default **Idle timeout** is five minutes

System > Settings

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).

Administration Settings	
HTTP port	80
Redirect to HTTPS	(disabled)
HTTPS port	443
HTTPS server certificate	self-sign
SSH port	22
Telnet port	23
Idle timeout	5 Minutes (1 - 480)
ACME interface	(disabled)

Password Policy	
Password scope	Off Admin IPsec Both (Admin selected)
Minimum length	8
Minimum number of new characters	0
Character requirements	(disabled)
Allow password reuse	(disabled)
Password expiration	(disabled)

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

You can choose whether to allow concurrent sessions. You can use concurrent sessions to avoid accidentally overwriting settings, if you usually keep multiple browser tabs open, or accidentally leave a CLI session open without saving the settings, then begin a GUI session and accidentally edit the same settings differently.

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 (default is five minutes). A shorter idle timeout is more secure, but increasing the timer can help reduce the chance of administrators being logged out while testing changes.

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

You can configure an administrator profile to increase inactivity timeout and facilitate use of the GUI for central monitoring. The **Override Idle Timeout** setting allows the **admintimeout** value, under **config system accprofile**, to be overridden per access profile.

Note that you can do this on a per profile basis, to avoid the option from being unintentionally set globally.

DO NOT REPRINT

© FORTINET

Administrative Access—Protocols

- Enable acceptable management protocols on each interface independently:
 - Separate IPv4 and IPv6
 - IPv6 options hidden by default
- Also protocols where FortiGate is the destination IP:
 - 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 port3. The 'Name' field is set to 'port3'. The 'Address' section shows 'Addressing mode' as 'Manual' with IP/Netmask '10.0.1.254/255.255.255.0'. The 'Administrative Access' section is highlighted with a red box. It contains checkboxes for various protocols: HTTPS (checked), HTTP (unchecked), PING (checked), SSH (checked), TELNET (checked), FTM (unchecked), Security Fabric Connection (unchecked), and Speed Test (unchecked). Below this, there are two sections for LLDP: 'Receive LLDP' and 'Transmit LLDP', each with a 'Use VDOM Setting' checkbox and 'Enable' and 'Disable' buttons.

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 and TELNET 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 DoS attack. You should disable protocols that do not encrypt data flow, such as HTTP and TELNET. 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.

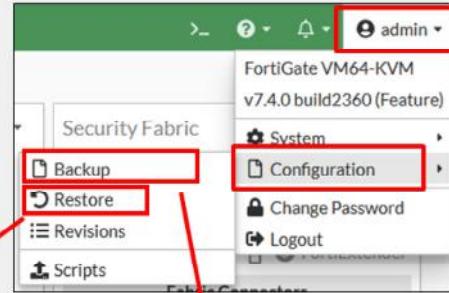
Security Fabric connection includes CAPWAP and FortiTelemetry. Protocols like FortiTelemetry are *not* for administrative access, but, like GUI and CLI access, they are protocols where the packets have FortiGate as a destination IP. Use the FortiTelemetry protocol specifically for managing FortiClient 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 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

Configuration File—Backup and Restore

- Configuration can be saved to an external device
 - It can mask passwords and secrets
 - Optional encryption
 - Can back up automatically
 - Upon logout
 - Not available on all models
- To restore a previous configuration, upload file
 - Reboots FortiGate



The dialog box shows fields for 'Restore from' (Local PC selected), 'File' (Upload button), and 'Password' (text input field).

The dialog box shows 'Backup to' (Local PC selected), 'File format' (YAML selected), and 'Password mask' (checkbox checked). A callout bubble says: 'You can export the config file in YAML format'. Other fields include 'Encryption' (checkbox checked) and password inputs.

Now that FortiGate has basic network settings and administrative accounts, you will learn how to back up the configuration. In addition to selecting the destination of the backup file, you can choose to encrypt or not to encrypt the backup file. Even if you choose not to encrypt the file, which is the default, the passwords stored in the file are hashed, and, therefore, obfuscated. The passwords that are stored in the configuration file would include passwords for the administrative users and local users, and preshared keys for your IPSec VPNs. It may also include passwords for the FSSO and LDAP servers.

The other option is to encrypt the configuration file with a password. Besides securing the privacy of your configuration, it also has some effects you may not expect. After encryption, the configuration file cannot be decrypted without the password and a FortiGate of the same model and firmware. This means that if you send an encrypted configuration file to Fortinet technical support, even if you give them the password, they cannot load your configuration until they get access to the same model of FortiGate. This can cause unnecessary delays when resolving your ticket. Instead, you can enable password masking option when creating a new backup file to replace all passwords and secrets in the config file and prevent unintentional data leak when sharing the backup file with a third-party.

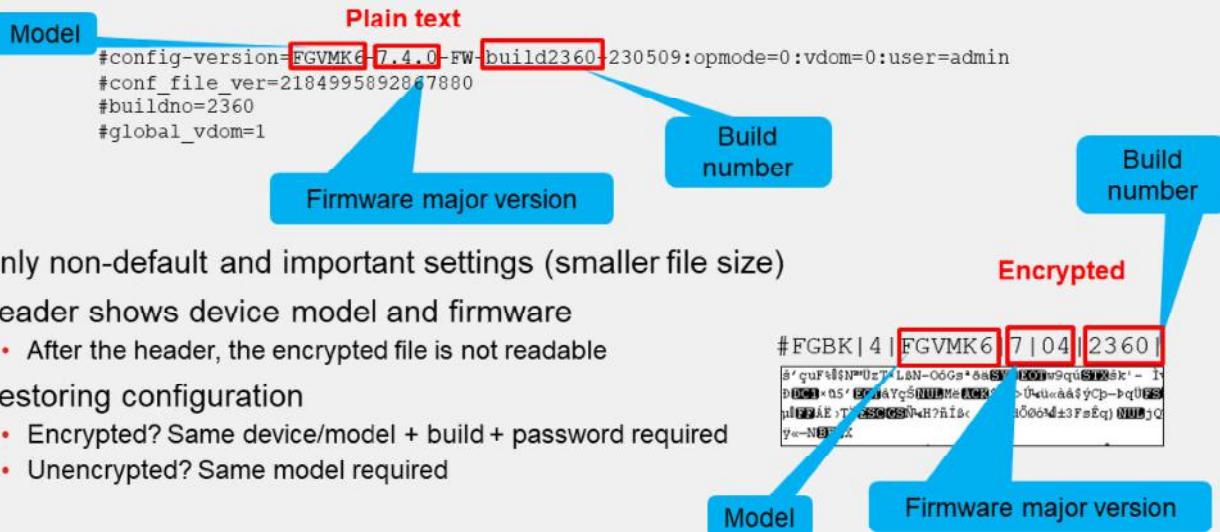
If you enable virtual domains (VDOMs), subdividing the resources and configuration of your FortiGate device, each VDOM administrator can back up and restore their own configurations. You don't have to back up the entire FortiGate configuration, however, it is still recommended.

Backups are needed to help speed up the return to production in the event of an unforeseen disaster that damages FortiGate. Having to recreate hundreds of policies and objects from scratch takes a significant amount of time, while loading a configuration file on a new device takes much less.

Restoring a configuration file is very similar to backing one up and restarts FortiGate.

DO NOT REPRINT
© FORTINET

Configuration File Format



If you open the configuration file in a text editor, you'll see that both encrypted and unencrypted configuration files contain a cleartext header that contains some basic information about the device. The example on this slide shows what information is included. To restore an encrypted configuration, you must upload it to a FortiGate device of the same model and firmware, then provide the password.

To restore an unencrypted configuration file, you are required to match only the FortiGate model. If the firmware is different, FortiGate will attempt to upgrade the configuration. This is similar to how it uses upgrade scripts on the existing configuration when upgrading firmware. However, it is still recommended to match the firmware on FortiGate to the firmware listed in the configuration file.

Usually, the configuration file contains only non-default settings, plus few default, yet crucial, settings. This minimizes the size of the backup, which could otherwise be several megabytes in size.

DO NOT REPRINT
© FORTINET

Configuration File Format—YAML Format

- Support YAML and can be backed up and restored by GUI and CLI

```
config_system_global:  
    admintimeout:480  
    alias:FortiGate-100F  
config_system_settings:  
    default-voip-alg-mode: kernel-helper-based  
    gui-dynamic-routing: enable  
config_system_interface:  
    - port1:  
        vdom: root  
        ip: "204.126.10.3 255.255.254.0"  
        allowaccess: ping  
        secondaryip:  
            - 0:  
                ip: "204.126.10.2 255.255.255.0"  
                allowaccess: ping
```

YAML Format

```
config system global  
    set admintimeout 480  
    set alias "FortiGate-100F"  
end  
config system settings  
    set default-voip-alg-mode kernel-helper-based  
    set gui-dynamic-routing enable  
end  
config system interface  
    edit "port1"  
        set vdom "root"  
        set ip 204.126.10.3 255.255.254.0  
        set allowaccess ping  
        config secondaryip  
            edit 1  
                set ip 204.126.10.2 255.255.255.0  
                set allowaccess ping  
            end  
        end
```

Default Format

YAML format becomes more and more popular often used to create configuration files. FortiOS now supports YAML format, you can take a backup as well as restore YAML configuration file using GUI.

This slide shows the sample configuration to understand the difference between the default file format and YAML format.

DO NOT REPRINT

© FORTINET

Upgrade Firmware

- You can view the current firmware version on the dashboard or in **System > Firmware & Registration** (or on the CLI: get system status)
- If there is an updated firmware version, you are notified
- You can update the firmware by clicking **Upgrade** and then selecting the **All Upgrades** or **File Upload** option
- Make sure you read the *Release Notes* to verify the upgrade path and other details

You can view the current firmware version in multiple places on the FortiGate GUI. When you first log in to FortiGate, the landing page is the dashboard. You can see the firmware version in the **System** widget. This information is also found at **System > Firmware & Registration**. And, of course, you can retrieve the information on the CLI using the command `get system status`.

If a new version of the firmware is available, you are notified on the dashboard and on the **Firmware & Registration** page. The **Firmware & Registration** page allows administrators to manage the firmware running on each FortiGate, FortiAP, and FortiSwitch in the Security Fabric, and to authorize and register these Fabric devices.

You can use **Upgrade** option to upgrade firmware of the selected device. The **Fabric Upgrade** option upgrades firmware for the root FortiGate as well as Fabric devices. You can also use this option to upgrade firmware for a non-Security Fabric FortiGate with managed FortiSwitch and FortiAP devices. The **Fabric Upgrade** option uses released firmware images from FortiGuard.

You can also use the **Register** option to register a selected device to FortiCare and an **Authorize** option to authorize a selected device for use in security fabric.

Remember to read the *Release Notes* to make sure that you understand the supported upgrade path. The *Release Notes* also provide pertinent information that may affect the upgrade.

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



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 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 Subscription Services (Contd)

- FortiGuard third party SSL certificate verification and OCSP stapling check
 - Default FortiGuard access mode is *anycast*
 - Optimize the routing performance to the FortiGuard servers
 - FortiGate gets a single IP address for the domain name of each FortiGuard service
 - FortiGuard servers query the CA OCSP responder every four hours
 - Enforce a connection to use protocol HTTPS and port 443



© Fortinet Inc. All Rights Reserved. 22

Now, third-party SSL certificate verification and OCSP stapling check has been implemented for all FortiGuard servers. By default, the FortiGuard access mode is *anycast* on FortiGate, to optimize the routing performance to the FortiGuard servers. The FortiGuard server has one IP address to match its domain name. FortiGate connects with a single server address, regardless of where the FortiGate device is located.

The domain name of each FortiGuard service is the common name in the certificate of that service. The certificate is signed by a third-party intermediate CA. The FortiGuard server uses the Online Certificate Status Protocol (OCSP) stapling technique, so that FortiGate can always validate the FortiGuard server certificate efficiently. FortiGate will complete the TLS handshake only with a FortiGuard server that provides a *good* OCSP status for its certificate. Any other status results in a failed SSL connection.

The FortiGuard servers query the OCSP responder of the CA every four hours and update its OCSP status. If FortiGuard is unable to reach the OCSP responder, it keeps the last known OCSP status for seven days.

FortiGate aborts the connection to the FortiGuard server if:

- The CN in the server certificate does not match the domain name resolved from the DNS.
- The OCSP status is not *good*.
- The issuer-CA is revoked by the root-CA.

The FortiGuard access mode *anycast* setting forces the rating process to use protocol HTTPS, and port 443.

DO NOT REPRINT**© FORTINET**

FortiGuard Subscription Services (Contd)

- Some of the FortiGuard domain name and their IP addresses:

Server	Domain name and IP address
Object download	globalupdate.fortinet.net - 173.243.140.6
Querying service (webfiltering, antispam)	globalguardservice.fortinet.net - 173.243.140.16
FortiGate Cloud logging	globallogctrl.fortinet.net - 173.243.132.25
FortiGate Cloud management	globalmgrctrl.fortinet.net - 173.243.132.26
FortiGate Cloud messaging	globalmsgctrl.fortinet.net - 173.243.132.27
FortiGate Cloud sandbox	globalaptctrl.fortinet.net - 184.94.112.22
The productapi used by OVPN registration and GUI icon download	globalproductapi.fortinet.net - 66.35.17.252

The table on this slide shows a list of some of the FortiGuard servers and their domain names and IP addresses.

DO NOT REPRINT**© FORTINET**

FortiGuard Licenses

System > FortiGuard

The screenshot shows the FortiGuard Distribution Network interface. On the left, there's a table titled "License Information" with columns for "Entitlement" and "Status". Most entries show "Valid" or "Licensed" status with expiration dates ranging from 2026/01/19 to 2026/01/18. A row for "FortiGate VM License" is present. On the right, there are sections for "FortiGuard Updates" (with a "Next Update" of 2023/09/03 14:52:00), "Manual Update" (with a "Upload License File" button), and "Fortinet Service Communications" (listing various services and their traffic volume over the last 24 hours). At the bottom, there's a note about activating FortiCare support contracts and a "Enter Registration Code" button. The bottom navigation bar includes tabs for "Scheduled updates" and "Kiosk", with "Automatic" selected.

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

24

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: 7.00015 signed
Contract Expiry Date: Mon Jan 19 2026
Last Updated using manual update on Thu Jul 13 02:54:00 2023
Last Update Attempt: Mon Aug 25 13:52:18 2023
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 2023
Last Update Attempt: Mon Aug 25 13:52:18 2023
Result: Updates Installed
```



© Fortinet Inc. All Rights Reserved.

25

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**

Knowledge Check

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

2. When restoring an encrypted system configuration file, in addition to the FortiGate model and firmware version from the time the configuration file was produced, what else must you provide?
 A. The password to decrypt the file
 B. The private decryption key to decrypt the file

3. To increase the chances of success, what document should you consult before upgrading or downgrading firmware?
 - A. *CLI Reference Guide*
 - B. *FortiOS Release Notes*

DO NOT REPRINT**© FORTINET**

Review

- ✓ Configure FortiGate on factory default settings
- ✓ Configure FortiGate as the DHCP server
- ✓ Configure and control administrator access to FortiGate
- ✓ Back up and restore system configuration files
- ✓ Upgrade FortiGate firmware
- ✓ Check and verify FortiGuard licenses



© Fortinet Inc. All Rights Reserved. 27

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**

FortiGate Administrator

Firewall Policies and NAT

A small red square icon containing a white square with a diagonal line, followed by the text "FortiOS 7.4".

Last Modified: 15 November 2023

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.

In this lesson, you will learn how to configure network address translation (NAT) and use it to implement source NAT (SNAT) and destination NAT (DNAT) for the traffic passing through FortiGate.

DO NOT REPRINT**© FORTINET**

Firewall Policies

Objectives

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



© Fortinet Inc. All Rights Reserved.

2

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

By demonstrating competence in 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 & Objects > Firewall Policy

ID	Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log
1	Internet_Access_ISP1	all	all	always	ALL	ACCEPT	NAT	AV default WEB default SR deep-inspection	UTM
2	Internet_Access_ISP2	all	all	always	ALL	ACCEPT	NAT	AV default WEB default SR deep-inspection	UTM
0	Implicit	all	all	always	ALL	DENY		Disabled	

Implicit Deny

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 network address translation (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**

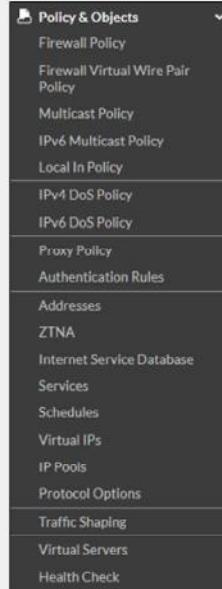
Components and Policy Types

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



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 identified (UUID)

The screenshot shows the FortiGate configuration interface. At the top right, there is a 'System > Feature Visibility' window with a checked checkbox for 'Allow Unnamed Policies'. Below it, the main configuration window shows a 'Training' policy being edited. The 'Source' section lists 'LOCAL_CLIENT' as the source. To the right, a 'Select Entries' dialog box is open, showing a list of entries including 'LOCAL_CLIENT', which is highlighted. A callout bubble points to the 'LOCAL_CLIENT' entry in the list with the text 'Universally unique identified (UUID)'. Another callout bubble points to the 'LOCAL_CLIENT' entry in the main configuration table with the text 'Enabled by default MUST specify unique name'. A third callout bubble points to the 'LOCAL_CLIENT' entry in the 'Select Entries' list with the text 'Highlights selected entry'.

When you configure a new firewall policy on the GUI, you *must* specify a unique name for the firewall policy because it is enabled by default, while it is optional on the CLI. This helps the administrator to quickly identify the policy that they are looking for. However, you can make this feature optional on the GUI on the **Feature Visibility** page by enabling **Allow Unnamed Policies**.

Note that if a policy is configured without a policy name on the CLI, and you modify that existing policy on the GUI, you *must* specify a unique name. The FortiGate flat GUI view allows you to select interfaces and other objects by clicking or dragging and dropping from the list populated on the right side.

You can select **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 that you can configure 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 universally unique identifier (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 need to create only one firewall policy that matches the direction of the traffic that initiates the session. FortiGate will automatically remember the source-destination pair and allow 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 ✓

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

Policy & Objects > Firewall Policy	
Name	Full_Access
Incoming Interface	LAN (port3)
Outgoing Interface	ISP1 (port1)
Source	LOCAL_SUBNET
Destination	all
Schedule	always
Service	ALL
Action	<input checked="" type="checkbox"/> ACCEPT <input type="checkbox"/> DENY

Authentication **Security Profile** **Logging**

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

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, source NAT, antivirus scanning, web filtering, and so on.

When FortiGate receives traffic, it evaluates the packet's 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**.

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 and the enabling of multiple interface policies.

Policy & Objects > Firewall Policy

Create New Policy

Name: Single_Interface
 Incoming Interface: port4
 Outgoing Interface: port5

A callout bubble points to the Outgoing Interface field with the text "Multiple interface policies disabled".

System > Feature Visibility

Multiple Interface Policies
 Allow the configuration of policies with multiple source/destination interfaces.

An arrow points from the Feature Visibility page down to the Firewall Policy page.

Policy & Objects > Firewall Policy

Create New Policy

Name: Multiple.Interfaces
 Incoming Interface: port7, port8
 Outgoing Interface: any

A callout bubble points to the Outgoing Interface field with the text "Multiple interface policies enabled".

© Fortinet Inc. All Rights Reserved. 7

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.

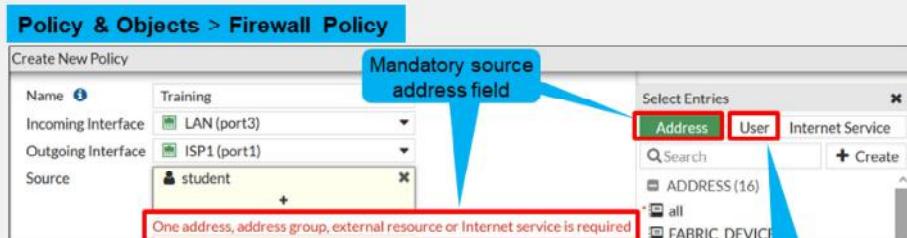
It is also worth mentioning that when you choose the **any** interface option, you cannot select multiple interfaces for that interface. In the example shown on this slide, because **any** is selected as the outgoing interface, you cannot add any additional interfaces, because **any** interface implies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

DO NOT REPRINT

© FORTINET

Matching by Source

- *Must* specify at least one source (address or Internet Service Database (ISDB) object)
 - 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



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 fully qualified domain name (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 ISDB and geography database and use them as firewall objects.

DO NOT REPRINT
© FORTINET

Example—Matching Policy by Source

- Matches by source address, user
- Source as ISDB objects

Policy & Objects > Firewall Policy

Name	Training
Incoming Interface	port3
Outgoing Interface	port1
Source	LOCAL_SUBNET student

User Address

Policy & Objects > Firewall Policy

Name	Training
Incoming Interface	port3
Outgoing Interface	port1
Source	Alibaba-Alibaba.Cloud Amazon-AWS

Internet service

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved. 9

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's 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

Policy & Objects > Firewall Policy

Security Profiles

AntiVirus	AV	default	<input type="button" value="Edit"/>
Web Filter	WEB	default	<input type="button" value="Edit"/>
Video Filter	VF	video_filter	<input type="button" value="Edit"/>
DNS Filter	DNS	default	<input type="button" value="Edit"/>
Application Control	APP	default	<input type="button" value="Edit"/>
IPS	IPS	default	<input type="button" value="Edit"/>
File Filter	FILE	default	<input type="button" value="Edit"/>
Email Filter	EMAIL	default	<input type="button" value="Edit"/>
DLP Profile	DLP	default	<input type="button" value="Edit"/>
SSL Inspection	SSL	deep-inspection	<input type="button" value="Edit"/>

Decrypted Traffic Mirror

Default profile not available, you need to manually create a profile

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**, and **Web Application Firewall** 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 primarily ordered on a top-down basis
- Policy IDs are identifiers:
 - The system assigns 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
```

Policy & Objects > Firewall Policy

ID	Name	Source	Destination	Schedule	Service	Action	NAT
1	LAN (port3) → DMZ (port2)	1					
3	DMZ	4 DMZ	4 all	always	ALL	✓ ACCEPT	✓ NAT
2	LAN (port3) → ISP1 (port1)	2					
2	Block_FTP	4 all	4 all	always	FTP	✗ DENY	
1	Full_Access	4 LOCAL_SUBNET	4 all	always	ALL	✓ ACCEPT	✓ NAT
+ Implicit	1						

Policy ID

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

An important concept to understand about how firewall policies work is the precedence of order, or, if you prefer a more recognizable term, first come, first served.

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 on the GUI. The policy ID never changes, even if you move the rule higher or lower in the sequence.

If you enable **Policy Advanced Options**, then you can manually assign a policy ID, while creating a new policy. If a duplicate entry is found, the system produces an error, so you can assign a different available policy ID number.

Policy Advanced Options is not available on the GUI by default, you must enable it on the **Feature Visibility** page.

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

ID	Name	Source	Destination	Schedule	Action	NAT	Type	Security	Bytes
1	LAN (port3) → DMZ (port2)	all	all	always	ALL	ACCEPT	NAT	Standard	no-inspection UTM 0 B
3	DMZ	all	all	always	FTP	DENY		Standard	no-inspection Disabled 0 B
2	Block_FTP	all	all	always	FTP	DENY		Standard	no-inspection Disabled 0 B
1	Full_Access	LOCAL_SUBNET	all	always	ALL	ACCEPT	NAT	Standard	no-inspection Disabled 454.63 kB

- **Sequence Grouping View and By Sequence**

- If policies are created using multiple source and destination interfaces or any interface

ID	Name	From	To	Source	Destination	Schedule	Action	NAT	Bytes
1	Block_FTP	LAN (port3)	ISP1 (port1)	all	all	always	FTP	DENY	0 B
2	Full_Access	LAN (port3)	ISP1 (port1)	LOCAL_SUBNET	all	always	ALL	ACCEPT	0 B
3	DMZ	LAN (port3)	DMZ (port2)	DMZ	all	always	ALL	ACCEPT	0 B
	any	any	any	all	all	always	ALL_ICMP	DENY	0 B

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

Adjusting Policy Order

- On the GUI, drag-and-drop

Before policy move

ID	Name	From	To	
1	Full_Access	LAN (port3) DMZ (port2)	ISP1 (port1)	4 4
2	Block_FTP	LAN (port3)	ISP1 (port1)	4
3	DMZ	LAN (port3)	DMZ (port2)	4

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

After policy move

ID	Name	From	To	
2	Block_FTP	LAN (port3)	ISP1 (port1)	4 a
1	Full Access	LAN (port3) DMZ (port2)	ISP1 (port1)	4 b
3	DMZ	LAN (port3)	DMZ (port2)	4 c

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.

Note that FortiGate assigns the next highest available ID number as policies are created.

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 & Objects > Firewall Policy

ID	Name	Source	Destination	Schedule	Service	Action	NAT	Type	Security Profiles	Log	Bytes
1	Full_Access	LOCAL_SUBNET DMZ	all	always	Web Access FTP	ACCEPT	NAT	Standard	AV default WEB default SSL deep-inspection	UTM	28.95 kB
2	ICMP	all	all	always	ALL ICMP	ACCEPT	NAT	Standard	SSL no-inspection	All	0 B
0	Implicit Deny	all	all	always	ALL	DENY				Disabled	58.21 kB

FORTINET.
Training Institute

© Fortinet Inc. All Rights Reserved. 15

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
 - Re-evaluate 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



© Fortinet Inc. All Rights Reserved.

16

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 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
 - Optimize performance
 - Proxy-based
 - Processed by CPU
 - Provides thorough inspection
 - Support advanced features like *safe search*

Enabling the security profiles on the FortiGate impacts on 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 typically 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, safe search, 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 CLI)
- Low-end platforms with 2 GB of RAM or less do not display the option on the GUI
 - Firewall inspection mode setting is not available on GUI—only on CLI
 - GUI option is available on low-end platforms when enabled on CLI:

```
config system settings  
    set gui-proxy-inspection enable  
end
```



© Fortinet Inc. All Rights Reserved.

18

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

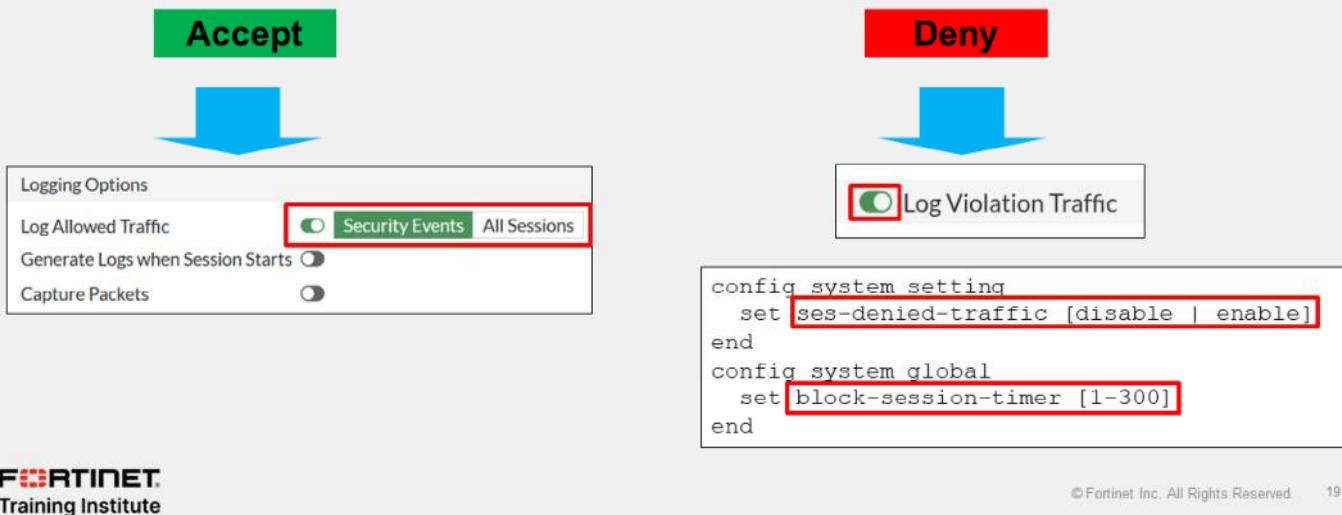
The option to configure proxy-based inspection mode on firewall policies and security profiles is available using the CLI command `config system settings`.

DO NOT REPRINT

© FORTINET

Logging

- By default, set to **Security Events**
 - Generates logs based on applied security profile only
- Can change to **All Sessions**



FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved. 19

If you have enabled 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. But 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 of 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 type 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

Date/Time	Source	Device	Destination	Application Name	Result	Policy ID
2023/09/10 06:24:34	10.0.1.200		208.91.112.63 (http1.fortiguard.com)	NTP	✓ Accept (76 B / 0 B)	1 (Full Access)
2023/09/10 06:24:34	10.0.1.200		208.91.112.02 (http1.fortiguard.com)	NTP	✓ Accept (76 B / 0 B)	1 (Full Access)
2023/09/10 06:24:35	10.0.1.200		208.91.112.61 (http2.fortiguard.com)	NTP	✓ Accept (76 B / 76 B)	1 (Full Access)
2023/09/10 06:24:08	10.0.1.200		208.91.112.00 (http2.fortiguard.com)	NTP	✓ Accept (76 B / 0 B)	1 (Full Access)
2023/09/10 06:23:46	10.0.1.200		192.168.4.46	tcp/853	✓ Accept (4.83 kB / 14.81 kB)	1 (Full Access)
2023/09/10 06:22:18	10.0.1.10		34.17.65.55 (push.services.mozilla.com)	HTTPS	✓ Accept (2.1 kB / 1.71 kB)	1 (Full Access)
2023/09/10 06:21:37	10.0.1.200		173.243.140.6	HTTPS	✓ Accept (5.08 kB / 9.5 kB)	1 (Full Access)
2023/09/10 06:20:58	10.0.1.200		96.45.46.46	tcp/853	✓ Accept (3.8 kB / 11.29 kB)	1 (Full Access)

Policy & Objects > Firewall Policy

Right-click context menu for a selected policy:

- Show matching logs (highlighted with red box)
- Show in FortiView
- Edit
- Edit in CLI
- Delete policy

© Fortinet Inc. All Rights Reserved. 20

FORTINET
Training Institute

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 on **Show matching logs**.

DO NOT REPRINT
© FORTINET

Geographic-Based Internet Service Database

- 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

Policy & Objects > Internet Service Database

Edit Internet Service

Name	Training-Location-ISDB	Primary Internet Service Name	Google-Other
Type	Predefined Geographic Based	Primary Internet Service ID	65536
Primary Internet Service	Google-Other	Direction	Both
Country/Region	United States	Entries	
Region	California		
City	Sunnyvale		

Geographic-based 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

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 must be selected in the **Source** field of a firewall policy?
 A. At least one address object
 B. At least one source user and one source address object

3. 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 URLs

DO NOT REPRINT**© FORTINET**

NAT

Objectives

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

Now, you'll learn about NAT with firewall policies.

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

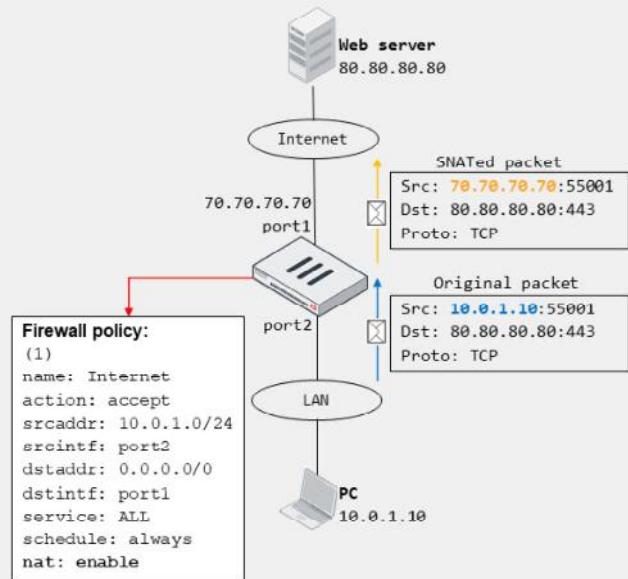
By demonstrating competence in these areas, you will be able to configure firewall policies and apply appropriate SNAT and DNAT, and understand how it is applied to the traffic traversing through FortiGate.

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



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 the dynamic IP pool

The screenshot shows the 'Policy & Objects > Firewall Policy' interface. In the 'Create New Policy' section, the 'Name' is set to 'Full_Access' and 'Type' is 'Standard ZTNA'. Under 'Source', 'LOCAL_SUBNET' is selected. The 'Outgoing Interface' dropdown lists 'LAN (port3)', 'ISP1 (port1)', and 'all'. The 'Destination' is set to 'all'. The 'Schedule' is 'always' and the 'Service' is 'ALL'. The 'Action' is 'ACCEPT'. In the 'Inspection Mode' section, 'Flow-based' is selected. The 'Firewall/Network Options' section is expanded, showing the 'NAT' tab selected. Three radio buttons are present: 'Use Outgoing Interface Address' (selected), 'Use Dynamic IP Pool', and 'Preserve Source Port'. Below these are 'Protocol Options' and a 'PROT' dropdown set to 'default'.

FORTINET
 Training Institute

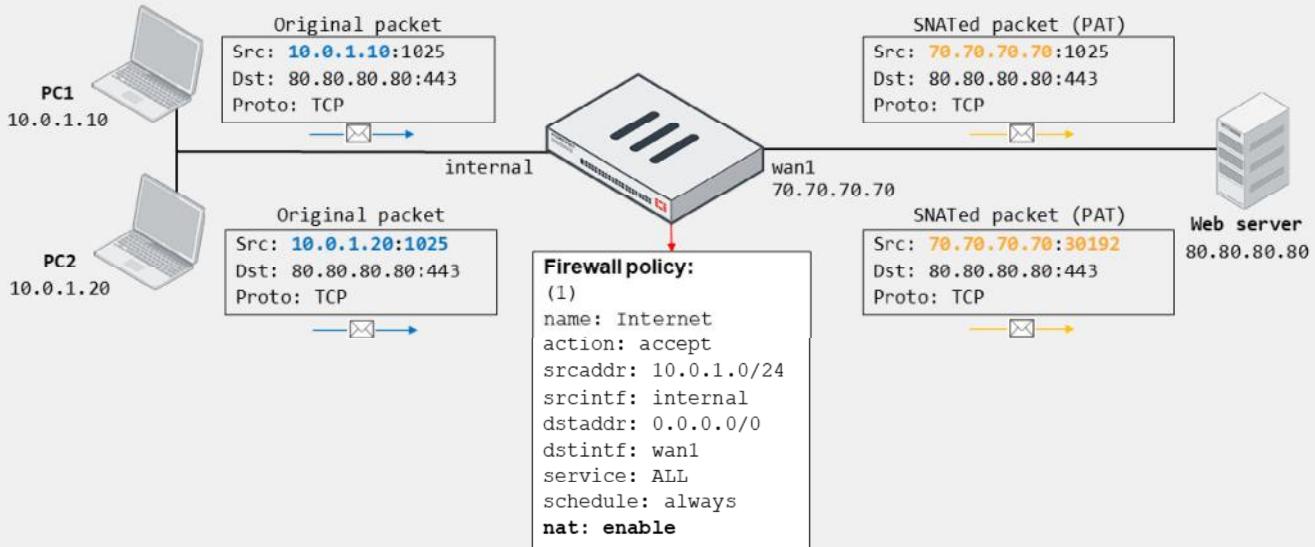
© Fortinet Inc. All Rights Reserved. 25

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 the 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
 Training Institute

© Fortinet Inc. All Rights Reserved. 26

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.

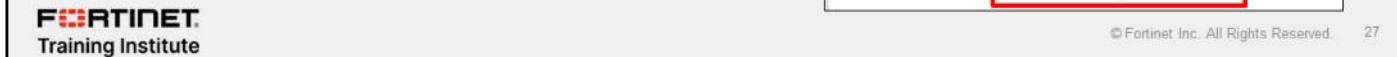
DO NOT REPRINT

© 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



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

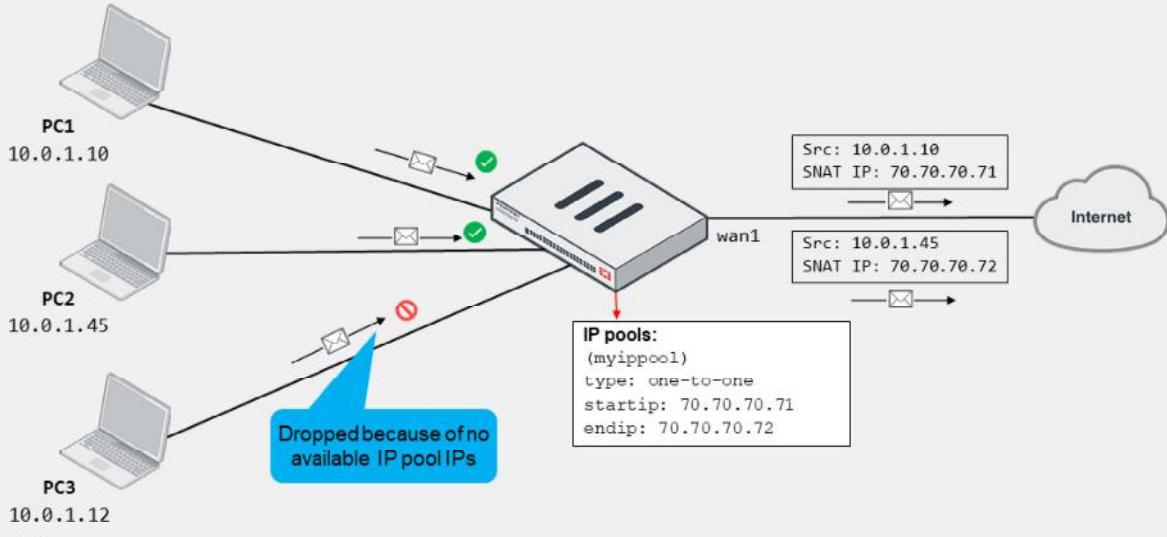
The fixed port range and port block allocation types are more common carrier-grade NAT (CGN) deployments.

DO NOT REPRINT

© FORTINET

IP Pool Type—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
Training Institute

© Fortinet Inc. All Rights Reserved.

28

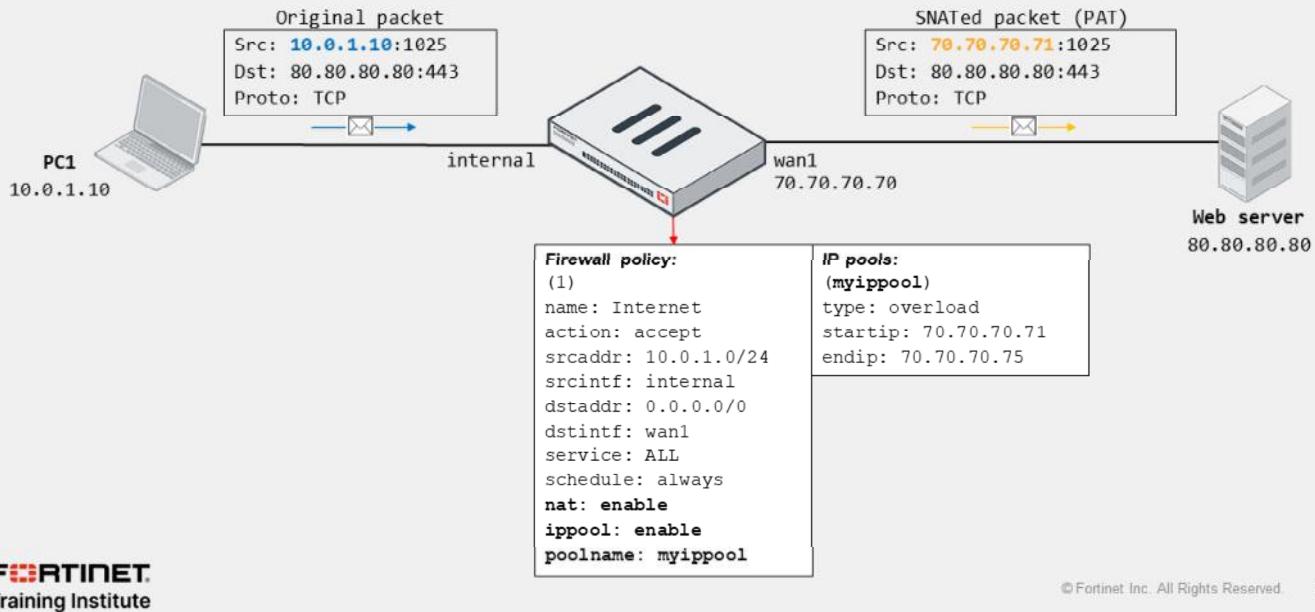
In the one-to-one pool type, FortiGate assigns an IP pool address to an internal host on a first-come, first-served basis.

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, served with 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

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

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 two windows from the FortiGate management interface:

- Policy & Objects > Virtual IPs**: A configuration window for a Virtual IP object named "VIP-INTERNAL-HOST". It specifies the interface as "port1", type as "Static NAT", and maps it to the external IP range "100.64.100.22" and the internal IP "10.0.1.10".
- Policy & Objects > Firewall Policy**: A configuration window for a firewall policy named "Web-Server Access". It defines an incoming interface "port1" and an outgoing interface "port3". The source is set to "all" and the destination is set to "VIP-INTERNAL-HOST". The action is set to "ACCEPT".

A blue callout bubble points from the "Destination" field in the Firewall Policy window to the "VIP used as destination in firewall policy" text below.

FORTINET
Training Institute

30

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:

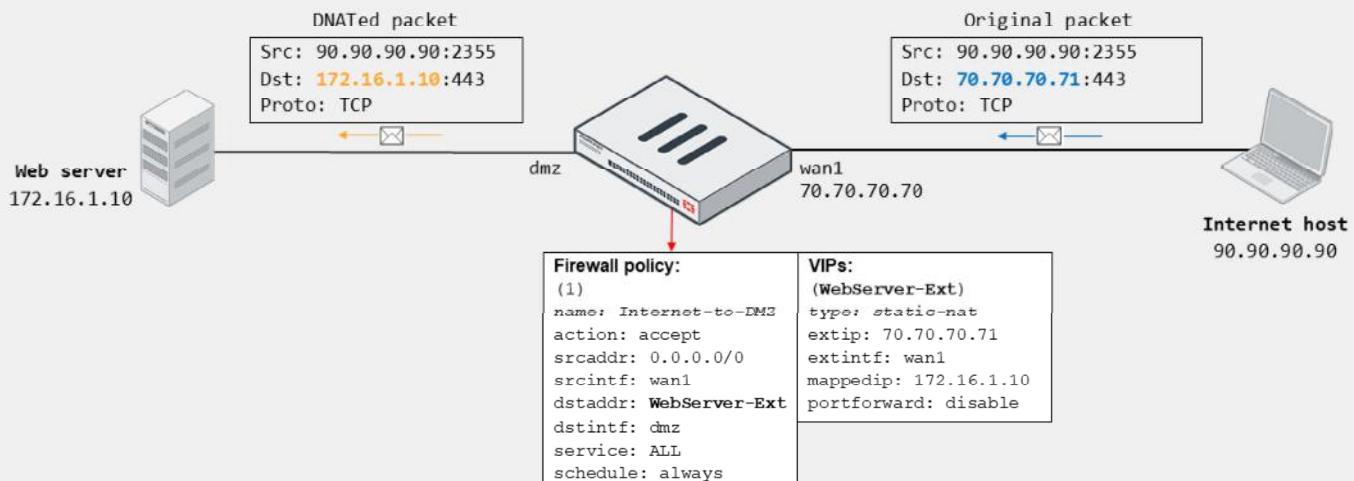
1. FortiGate performs DNAT on ingress traffic destined to the external IP address defined in the VIP, regardless of the protocol and port of the connection, provided the matching firewall policy references the VIP as **Destination**.
2. FortiGate uses as NAT IP the external IP address defined in the VIP 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 **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 70.70.70.70 on port 8080 map to the internal IP 192.168.0.70 on port 80. You can then configure another VIP so connections to the external IP 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

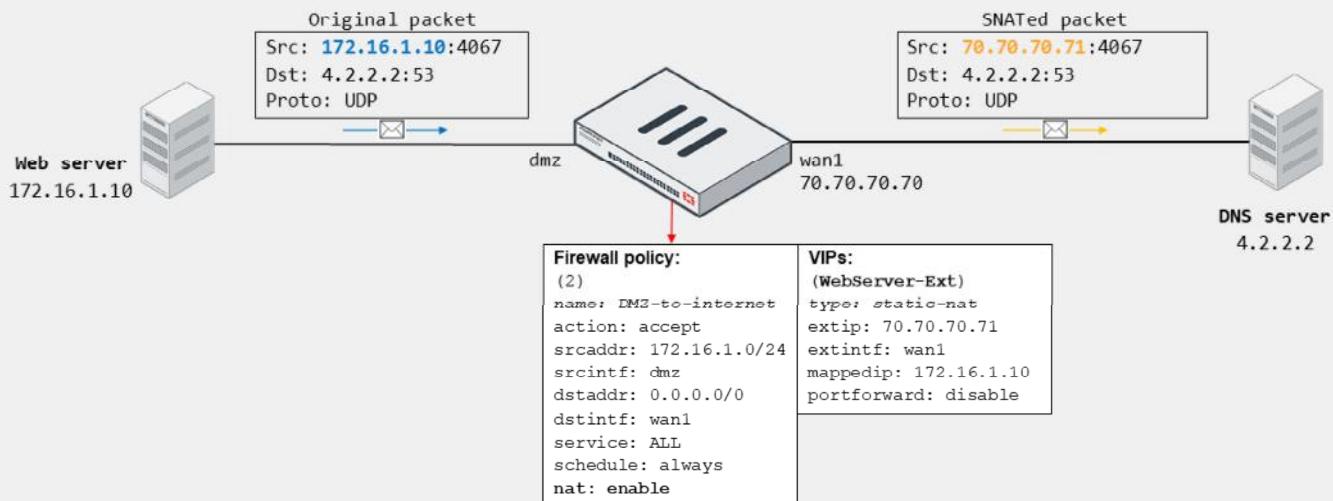


In the example shown on this slide, the internet host initiates a connection to 70.70.70.71 on TCP port 443. On FortiGate, the traffic matches the firewall policy ID 1, which references the WebServer-Ext VIP as destination. Because the VIP is configured as static NAT and has port forwarding disabled, 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 VPN (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

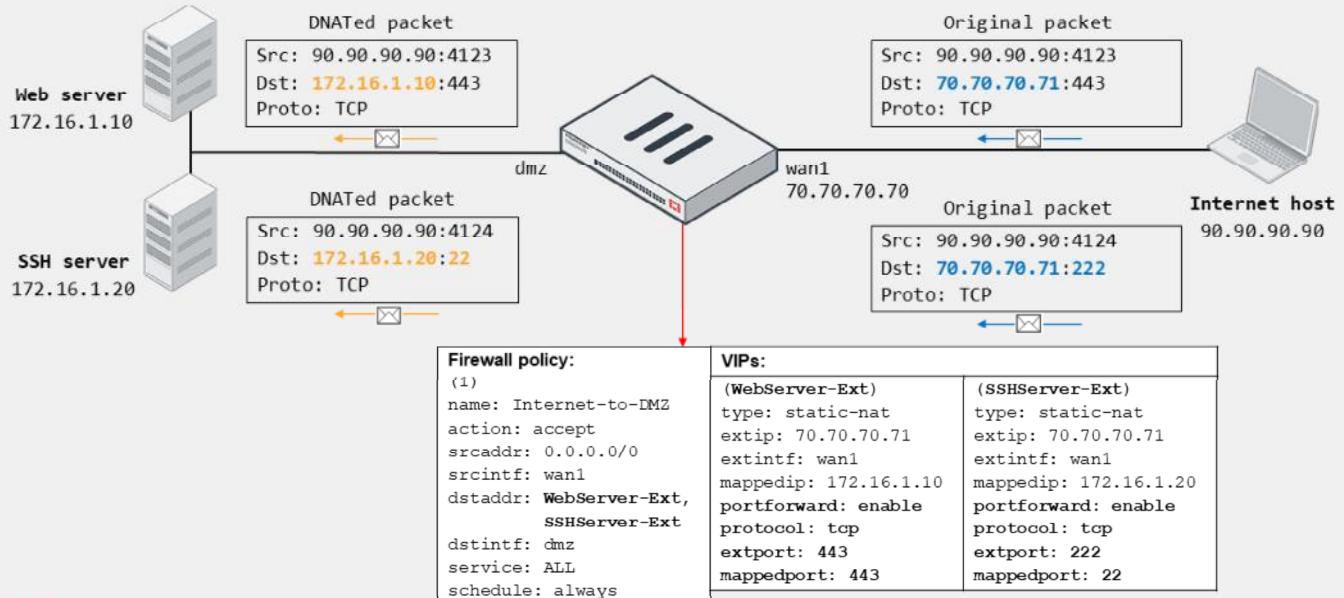


Now, suppose that the internal web server (172.16.1.10) initiates a DNS connection to the internet DNS server (4.2.2.2). On FortiGate, the traffic matches the firewall policy ID 2, which has `nat` enabled. Because the source address matches the internal address of the VIP, and because the VIP is configured 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
Training Institute

© Fortinet Inc. All Rights Reserved. 33

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 do not match VIPs
 - Doesn't block an egress-to-ingress connection, even when the deny policy is at the top of the list
- VIP policy (WAN to LAN)

ID	Name	Source	Destination	Schedule	Service	Action
port1 → port3 2						
4	Deny	Deny_IP	all	always	ALL	DENY
3	Allow_Access	all	Web_Server	always	HTTP HTTPS	ACCEPT

VIP access falls through to this policy, even though the deny policy is at the top of the list

- Two solutions:

- Enable `match-vip` on the deny policy

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

Setting available only when policy action is set to deny

- Set the VIP as destination

```
config firewall policy
  edit <deny policy ID>
    set dstaddr <VIP>
  next
end
```

In FortiOS, VIPs and firewall address objects are completely different. They are stored separately with no overlap. This means that, by default, firewall address objects do not match VIPs.

In the example shown on this slide, the destination of the first firewall policy is set to **all**. Even though this means all destination addresses (`0.0.0.0/0`), by default, this doesn't include the external addresses defined on the VIPs. The result is that traffic destined to the external address defined on the **Web_Server** VIP skips the first policy and matches the second policy instead.

But what if you want the first policy to block all incoming traffic to all destinations, including the traffic destined to any VIPs? This is useful if your network is under attack, and you want to temporarily block all incoming external traffic. You can do this by enabling `match-vip` on the first firewall policy. Enabling `match-vip` instructs FortiGate 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**.

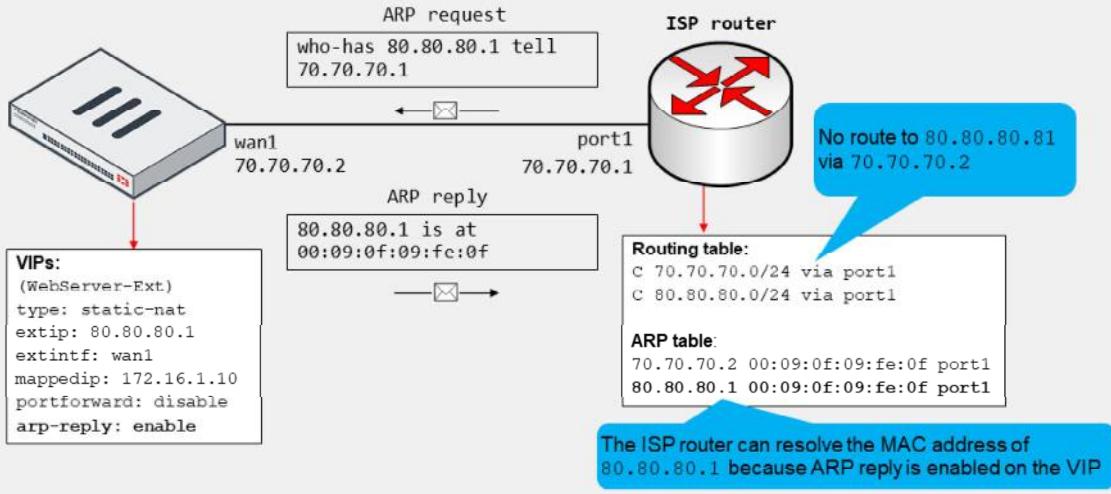
In case you want to block only traffic destined to one or more VIPs, you can reference the VIPs as the destination address on the deny firewall policy.

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
Training Institute

© Fortinet Inc. All Rights Reserved.

35

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 connected 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 maintenance window to make changes on NAT configuration



© Fortinet Inc. All Rights Reserved.

36

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 mode configuration since making changes could create a network outage.

DO NOT REPRINT

© FORTINET

Knowledge Check

1. What is the default IP pool type?

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

2. Which of the following is the default VIP type?

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

DO NOT REPRINT

© FORTINET

Review

- ✓ Configure IPv4 firewall policy
- ✓ Monitor traffic logs from firewall policy
- ✓ 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



FortiGate Administrator

Routing

 FortiOS 7.4

Last Modified: 15 November, 2023

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

DO NOT REPRINT

© FORTINET

Objectives

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

After completing this lesson, 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, understand the routing table, and implement routing load balancing.

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



© Fortinet Inc. All Rights Reserved. 3

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 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



© Fortinet Inc. All Rights Reserved.

4

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 on the GUI and CLI
- FIB
 - Routing table from kernel perspective
 - Composed mostly by RIB entries, plus system-specific entries
 - Used for route lookups
 - Visible on the CLI only:

```
FortiGate-VM64-KVM # get router info kernel
tab=255 vf=0 scope=253 type=3 proto=2 prio=0 0.0.0.0/0.0.0.0/0->10.0.1.0/32
pref=10.0.1.254 gwy=0.0.0.0 dev=5(port3)
tab=255 vf=0 scope=254 type=2 proto=2 prio=0 0.0.0.0/0.0.0.0/0->10.0.1.254/32
pref=10.0.1.254 gwy=0.0.0.0 dev=5(port3)
tab=255 vf=0 scope=253 type=3 proto=2 prio=0 0.0.0.0/0.0.0.0/0->10.0.1.255/32
pref=10.0.1.254 gwy=0.0.0.0 dev=5(port3)
...
...
```

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 is built mostly out of 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 by RIB entries, then the 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, a more accurate statement is to refer to it as the FIB lookup process.

You can display the RIB entries on the FortiGate GUI and CLI. However, for the FIB, you can display its entries on the FortiGate CLI only. The output on this slide shows the CLI command that displays the FIB. Note that the output has been cut to fit the slide. You will learn how to display the routing table entries in this lesson.

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

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

Network > Static Routes

Edit Static Route

Destination	Subnet Internet Service 0.0.0.0/0.0.0.0
Gateway Address	10.200.1.254
Interface	port1
Administrative Distance	10
Comments	Write a comment... 0/255
Status	Enabled
Advanced Options	
Priority	1

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.

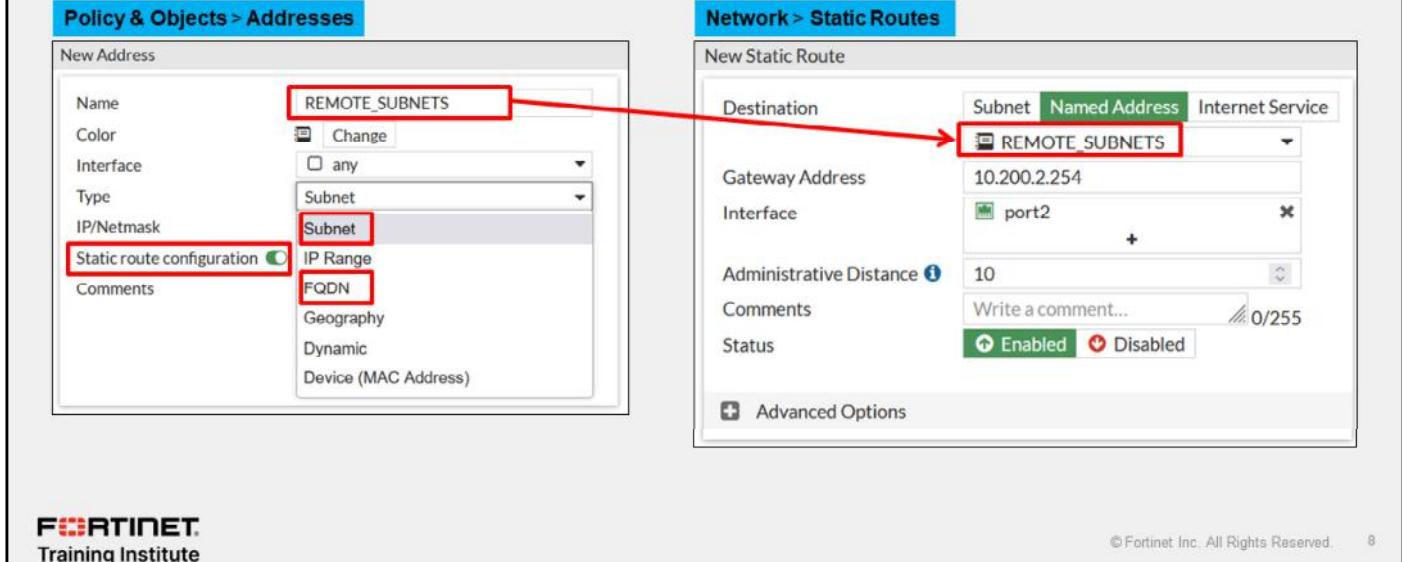
For example, in simple home networks, DHCP automatically retrieves and configures a route. Your modem then sends all outgoing traffic through your ISP internet router, which can relay packets to their destination. This is typically referred to as a default route, because all traffic not matching any 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 windows 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", with "Subnet" selected. The "Static route configuration" checkbox is checked. Other options like "IP Range" and "FQDN" are also visible.
- Network > Static Routes**: A "New Static Route" dialog. The "Destination" dropdown is set to "Named Address", and "REMOTE_SUBNETS" is selected. The "Gateway Address" is "10.200.2.254", the "Interface" is "port2", and the "Administrative Distance" is "10". The status is "Enabled".

A red arrow points from the "REMOTE_SUBNETS" entry in the "Address" dialog to the "Named Address" dropdown in the "Static Routes" dialog, indicating the connection between the two configurations.

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

8

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 **Static route 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 panels from the FortiGate management interface:

- Policy & Objects > Internet Service Database**: A table listing various internet services with their names, directions, number of entries, and references. One entry, "aws Amazon-AWS", is highlighted with a red box.
- Network > Static Routes**: A form for creating a new static route. The "Destination" field has a dropdown menu where "aws Amazon-AWS" is selected. This selection is highlighted with a red box and connected by a red arrow to the highlighted row in the ISDB table.

A callout bubble points to the ISDB table with the text: "Database containing IP addresses, protocols, and port numbers used by most common Internet services".

Fortinet Training Institute logo and copyright information are visible at the bottom.

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.

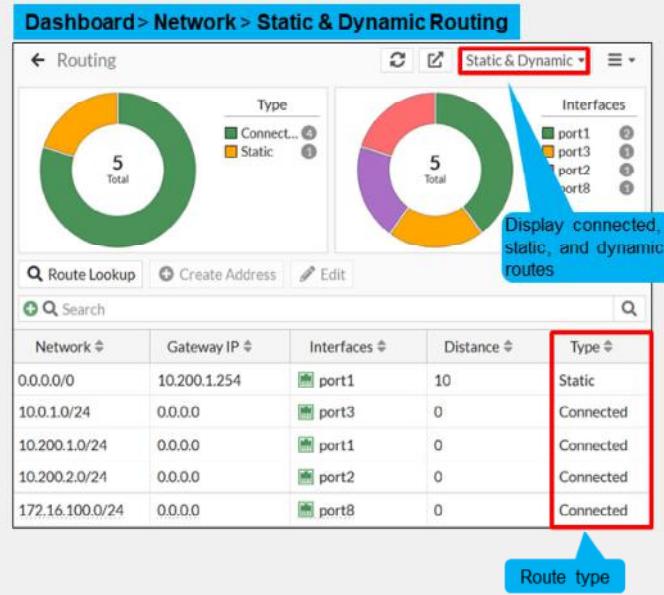
Even though they are configured as static routes, ISDB routes are actually policy routes and take precedence over any other routes in the routing table. As such, ISDB routes are added to the policy routing table.

DO NOT REPRINT

© FORTINET

Routing Monitor

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



FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved. 10

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 type:

- 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: static and connected routes whose interfaces are administratively down or whose links are down. Static routes are also marked inactive when their gateway is detected as dead by the link health monitor.
- Standby routes: These are active routes that are removed from the routing table because they are duplicate and have higher distances. For instance:
 - 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. To view the policy route table entries, select **Policy**.

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
 - Avoids 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.

13

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 ECMP static routes
 - ECMP static routes:
 - Equal-distance, equal-priority duplicate routes
 - All ECMP routes are installed in the routing table
 - The lower the priority, the higher the preference
- Best route is used during route lookup
- Applies to all routes except connected
 - Default value: 1
 - Hardcoded on all routes except static and BGP

Network > Static Routes

Edit Static Route

Destination	Subnet 0.0.0.0/0.0.0.0	Named Address	Internet Service
Gateway Address	10.200.1.254		
Interface	port1	+	
Administrative Distance	10	Write a comment... /255	
Comments			
Status	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled		
<input type="checkbox"/> Advanced Options			
Priority 10			

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	10
10.0.1.0/24	0.0.0.0	port3	0	Connected	0	0
10.0.3.0/24	10.0.1.200	port3	200	BGP	0	1
10.0.4.0/24	10.0.1.200	port3	120	OSPF	11	1
10.0.5.0/24	10.0.1.200	port3	120	RIP	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
172.16.100.0/24	0.0.0.0	port8	0	Connected	0	0

© Fortinet Inc. All Rights Reserved.

14

FORTINET
Training Institute

When there are two or more duplicate static routes that have the same distance, FortiGate installs all of them in the routing table. If they also have the same priority, then the routes are known as ECMP static routes, and you will learn more about them in this lesson.

The priority setting enables administrators to break the tie among ECMP static routes. The result is that, during the route lookup process, FortiGate selects as the best route 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. The use of the priority value in dynamic routes is useful for advanced routing deployments involving SD-WAN and multiple virtual routing and forwarding (VRF) IDs. The details on how the priority attribute is beneficial for such cases is outside the scope of this course.

For static routes, you can configure the priority setting under the **Advanced Options** on the FortiGate GUI, 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 on the routing table on the FortiGate CLI, which you will learn about later in this lesson.

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

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved. 15

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

Route Attributes

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

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

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

Enable the Metric column (disabled by default)



```
# 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 10.200.1.254, 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

Display routing table entries on the CLI

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

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 shows the FortiGate GUI interface. At the top, a navigation bar reads "Dashboard > Network > Static & Dynamic Routing". Below it is a "Route Lookup" search bar. A red arrow points from this bar down to a "Route Lookup" dialog box. This dialog has 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 blue callout bubble next to the dialog says "You are redirected to the policy page if you enter all attributes". Another red arrow points from the dialog to a "Matching route" callout bubble pointing at a row in a routing table below. The routing table has columns for Network, Gateway IP, Interfaces, Distance, and Type. It contains three rows: one static default route (0.0.0.0/0) and two dynamic routes (10.0.1.0/24 and 10.200.1.0/24). The first row (static default) is highlighted with a red background.

Network	Gateway IP	Interfaces	Distance	Type
0.0.0.0/0	10.200.1.254	port1	10	Static
10.0.1.0/24	0.0.0.0	port3	0	Connected
10.200.1.0/24	0.0.0.0	port1	0	Connected

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

ECMP

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



© Fortinet Inc. All Rights Reserved. 19

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

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
```

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
```

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

Default weight for
static routes using
the interface

- 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.

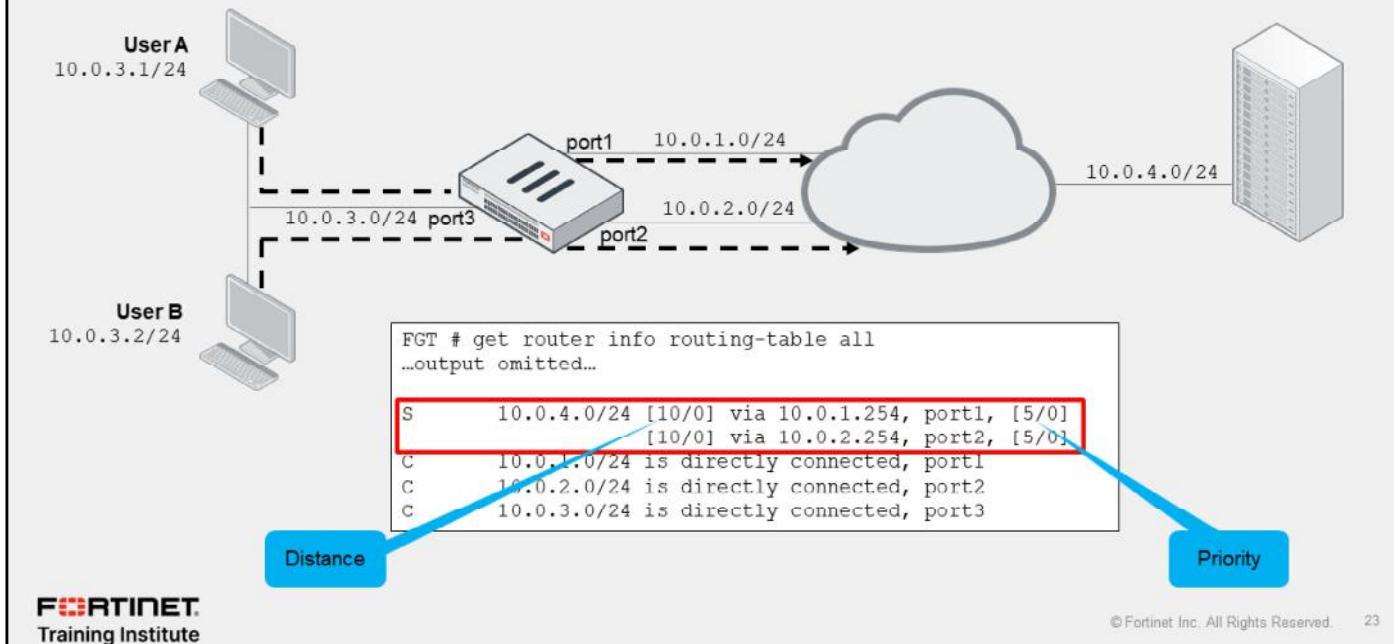
For spillover to work, you must also configure the egress and ingress spillover thresholds, as shown on this slide. The thresholds are set to 0 by default, which disables spillover check.

For a weighted algorithm, you must configure the weights on 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 in the percentage value.

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. In 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



© Fortinet Inc. All Rights Reserved. 24

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 applies to 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

Review

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



© Fortinet Inc. All Rights Reserved. 26

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 balancing the routes on FortiGate.

DO NOT REPRINT

© FORTINET



FortiGate Administrator

Firewall Authentication

FortiOS 7.4

Last Modified: 15 November 2023

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

DO NOT REPRINT**© FORTINET**

Objectives

- 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



© Fortinet Inc. All Rights Reserved.

2

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

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

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



 **Authentication Required**

Please enter your username and password to continue.

Username

Password

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)



© Fortinet Inc. All Rights Reserved.

4

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.

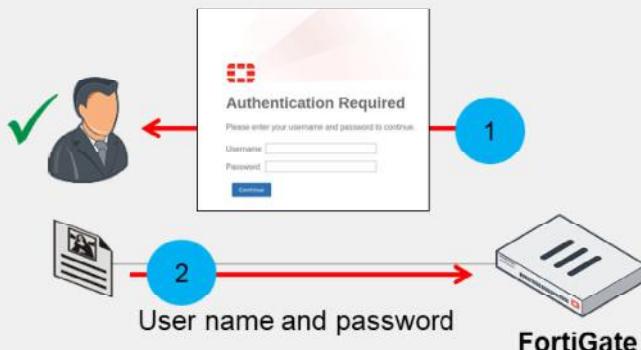
During this lesson, you will learn about each method of firewall authentication in detail.

DO NOT REPRINT

© FORTINET

Local Password Authentication

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



User & Authentication > User Definition

Users/Groups Creation Wizard

① User Type > ② Login Credentials > ③ Contact Info > ④ Extra Info

Local User

Remote RADIUS User

Remote TACACS+ User

Remote LDAP User

FSSO

Users/Groups Creation Wizard

① User Type > ② Login Credentials > ③ Contact Info > ④ Extra Info

Username: Student

Password: *****

Users/Groups Creation Wizard

① User Type > ② Login Credentials > ③ Contact Info > ④ Extra Info

Two-factor Authentication

Users/Groups Creation Wizard

① User Type > ② Login Credentials > ③ Contact Info > ④ Extra Info

User Account Status: Enabled

User Group: (radio button)

© Fortinet Inc. All Rights Reserved.

5

FORTINET
Training Institute

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.

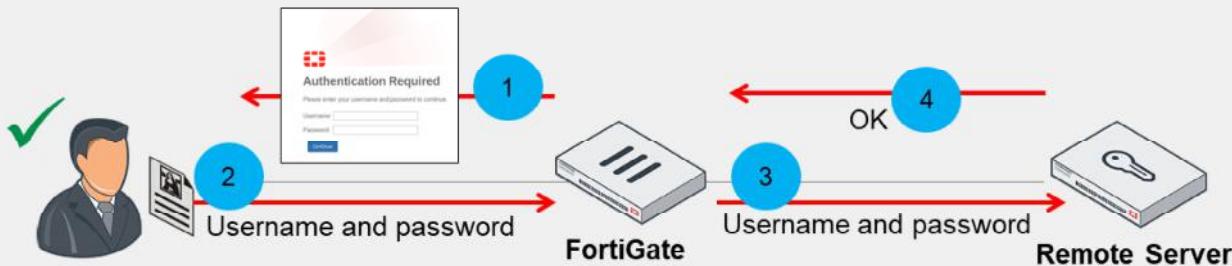
After you create the user, you can add the user—or any preconfigured user group in which the user is a member—to a firewall policy, in order to authenticate. You will learn about user groups and firewall policies in this lesson.

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



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, in the case of 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

Must be preconfigured on FortiGate

The screenshot shows the 'Edit User Group' dialog. In the 'Remote Groups' section, there is a table with one row. The 'Remote Server' column contains 'FortiAuth-RADIUS' and the 'Group Name' column contains 'Remote-users'. A large blue arrow points from the text 'Must be preconfigured on FortiGate' to this table.

User & Authentication > User Definition

The screenshot shows the 'User & Authentication > User Definition' wizard. Step 1: User Type. The 'Remote RADIUS User' option is selected and highlighted with a red box. Other options shown are Local User, Remote TACACS+ User, and Remote LDAP User. Below these are FSSO and FortiNAC User.

Must be preconfigured on FortiGate

The screenshot shows the 'User & Authentication > User Definition' wizard. Step 2: RADIUS Server. A dropdown menu labeled 'RADIUS Server' is open, showing 'FortiAuth-RADIUS' as the selected option. A large blue arrow points from the text 'Must be preconfigured on FortiGate' to this dropdown.

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

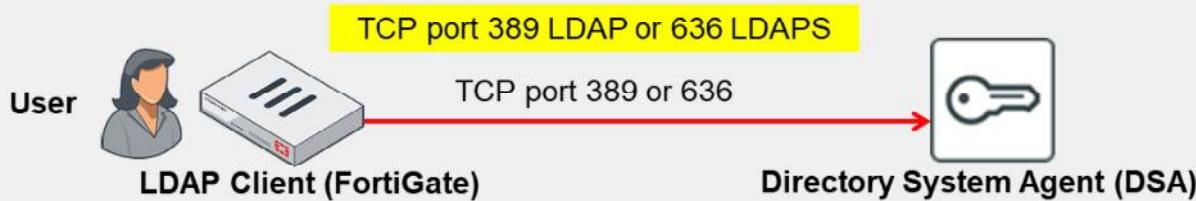
- Create user accounts on FortiGate. With this method, you must select the remote authentication server type (RADIUS, TACACS+, or LDAP), point FortiGate to your preconfigured remote authentication server, and add the user to an appropriate group. This is usually done when you want to add two-factor authentication to your remote users. Remember, POP3 is only configurable through the CLI.
- 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. 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=adadmin,cn=Users,dc=trainingAD,dc=local
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 to have 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.

The **Test Connectivity** button 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 the **Test User Credentials** button or use the CLI.

DO NOT REPRINT**© FORTINET**

RADIUS Overview

- RADIUS is a standard protocol that provides AAA services



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.

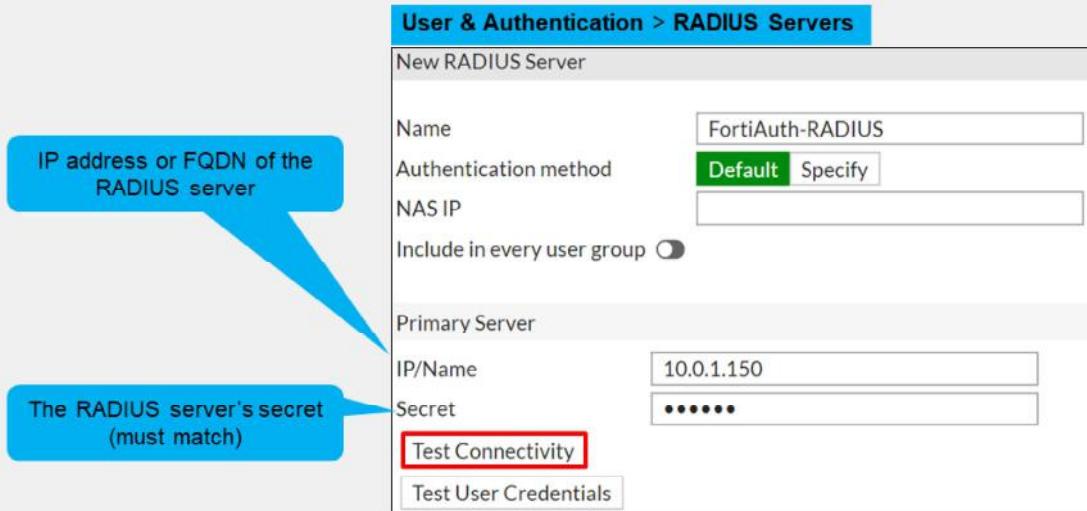
When a user is authenticating, the client (FortiGate) sends an ACCESS-REQUEST packet to the RADIUS server. The reply from the server is one of the following:

- 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



User & Authentication > RADIUS Servers

New RADIUS Server

Name	FortiAuth-RADIUS
Authentication method	Default Specify
NAS IP	<input type="text"/>
Include in every user group	<input checked="" type="checkbox"/>
Primary Server	
IP/Name	10.0.1.150
Secret	*****
<input type="button" value="Test Connectivity"/> <input type="button" value="Test User Credentials"/>	

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



13

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**

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



© Fortinet Inc. All Rights Reserved.

14

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)

- One-time passwords (OTPs) 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!



© Fortinet Inc. All Rights Reserved.

15

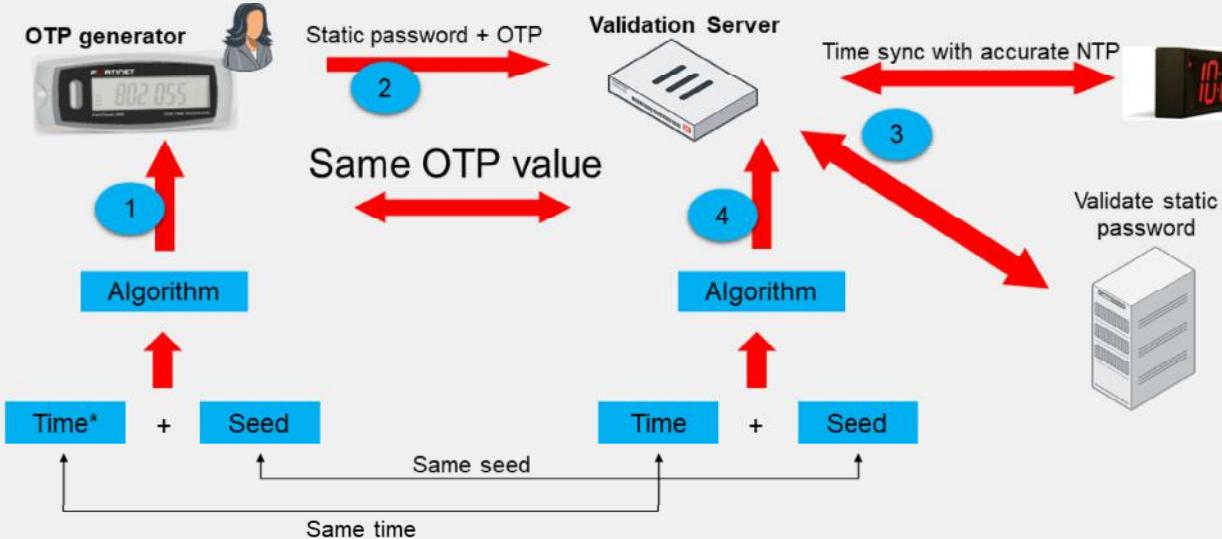
You can use one-time passwords (OTPs) as your second factor. OTPs are more secure than static passwords because the passcode changes at regular intervals and is valid for only a short amount of time. Once you use the OTP, you can't use it again. So, even if it is intercepted, it is useless. FortiGate 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
Training Institute

© Fortinet Inc. All Rights Reserved.

16

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 go through 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, a new passcode generates.

When using two-factor authentication using a token, the user must first log in with a static password followed by the passcode generated by the token. A validation server (FortiGate) receives the user's credentials and validates the static password first. The validation server then proceeds to validate 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 one 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 management interface under 'User & Authentication > FortiTokens'. A blue callout points to the 'Create New' button in the top-left corner of the token list table, with the text 'Two free FortiToken Mobile activations'. Another blue callout points to the 'Mobile Token' activation code field in the 'New FortiToken' dialog, with the text 'Can add a user to a group and create a firewall policy based on the user group'.

Type	Serial Number	Status	User	Drift	Comments
Mobile Token	FTKMOB6B91B33BE5	Available	0	0	
Mobile Token	FTKMOB6BCB3CCB31	Available	0	0	

New FortiToken

Type: Hard Token Mobile Token
Comments: Write a comment...
Serial Number:
Import:

New FortiToken

Type: Hard Token Mobile Token
Activation Code: 0000-0000-0000-0000-0000

User Account Edit

Username: student
User Account Status: Enabled
User Type: Local User
User Group: Remote-users
Two-factor Authentication: FortiToken Cloud
Authentication Type: FortiToken
Token: FTKMOB6B91B33BE5
Email Address:
SMS:

© Fortinet Inc. All Rights Reserved. 17

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 and Active Authentication

- Active
 - User receives a login prompt
 - Must manually enter 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



© Fortinet Inc. All Rights Reserved.

18

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 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

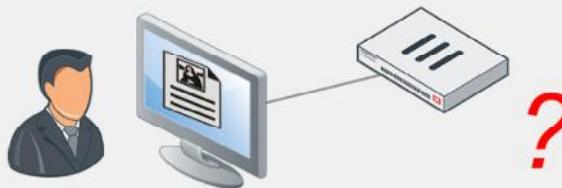
- Firewall policies can use user and user group objects to define the source. The objects include:
 - Local firewall accounts
 - External (remote) server accounts
 - PKI (certificate) users
 - FSSO users
- Anyone who belongs to the group and provides correct information will have a successful authentication

Policies & Objects > Firewall Policy

Name	Value
Name	Full_Access
Incoming Interface	port3
Outgoing Interface	port1
Source	<input checked="" type="checkbox"/> LOCAL SUBNET <input checked="" type="checkbox"/> External-Server-Users
Destination	<input checked="" type="checkbox"/> all
Schedule	always
Service	ALL
Action	<input checked="" type="checkbox"/> ACCEPT

Select Entries

Address	User	Internet Service
USER (2)	Local (2)	
	guest	
	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



© Fortinet Inc. All Rights Reserved.

20

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

Name	Source	Destination	Schedule	Service	Action	NAT
port3 → port1 1	Full_Access External-Server-Users LOCAL_SUBNET	all	always	DNS HTTP	ACCEPT	Enabled

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 on a policy does not always force an active authentication prompt

port5 → port1									
ID	User	Source	Action	Protocols	AV	SSL	Auth	Actions	Status
17	Guest	LOCAL_SUBNET	all		AV Guest_AV	SSL certificate-inspection	always	ALL	ACCEPT Enabled
18	Contractor	LOCAL_SUBNET	all		AV Contractor_AV	SSL certificate-inspection	always	ALL	ACCEPT Enabled
19	Other	LOCAL_SUBNET	all		AV default	SSL certificate-inspection	always	ALL	ACCEPT Enabled

- Three options:
 - Enable authentication on every policy that could match the traffic
 - Enforce authentication on demand option (CLI option 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 and user, and user group information (LOCAL_SUBNET and Guest-group respectively), and since 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 traffic is allowed with no need to authenticate.

When you use only active authentication, if all possible policies that could match the source IP 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

- Enable authentication on every policy that could match the traffic:
 - All firewall policies must have authentication enabled (active or passive)
 - If there is a fall-through policy in place, unauthenticated users are not prompted for authentication
 - 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.

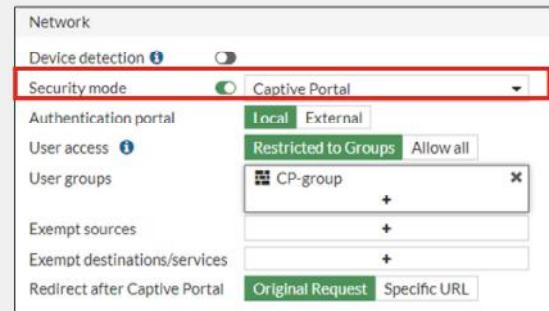
Alternatively, only on the CLI, you can change the auth-on-demand options. There are two options:

- 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)

- 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



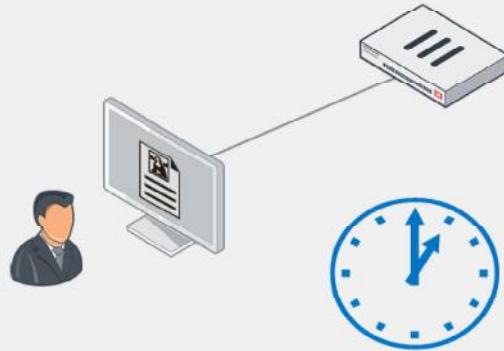
If you want to have all users connect to a specific interface, then it is better to enable captive portal authentication at the interface level. This way, all devices must authenticate before they are allowed to access any resources.

**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



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

| User Name | IP Address | User Group | Duration                    | Traffic Volume | Method   |
|-----------|------------|------------|-----------------------------|----------------|----------|
| student   | 10.0.1.10  | CP-group   | 1 minute(s) and 9 second(s) | 10.43 kB       | Firewall |

**Confirm**

⚠ Are you sure you want to deauthenticate the selected user(s)?

OK Cancel

**FORTINET.**  
Training Institute

© Fortinet Inc. All Rights Reserved. 26

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, and/or Telnet protocols in order for the user to be prompted for credentials.

**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



© Fortinet Inc. All Rights Reserved.

28

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

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

**DO NOT REPRINT****© FORTINET**

# FortiGate Administrator

## Fortinet Single Sign-On (FSSO)

A small red square icon containing a white square with a diagonal line, followed by the text "FortiOS 7.4".

Last Modified: 15 November, 2023

In this lesson, you will learn about Fortinet single sign-on (FSSO). When you use this feature, your users don't need to log on each time they access a different network resource.

**DO NOT REPRINT****© FORTINET**

## Objectives

- Install FSSO in DC agent mode
- Install collector agent
- Troubleshoot FSSO login issues



© Fortinet Inc. All Rights Reserved.

2

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

By demonstrating competence in understanding 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



© Fortinet Inc. All Rights Reserved.

3

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



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



© Fortinet Inc. All Rights Reserved.

5

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, this means that 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, 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. It then resolves the DNS of the client, and sends it to the collector agent.

The collector agent receives it and then performs a DNS resolution in order to check if the IP of the user 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 in order not to resolve the DNS:

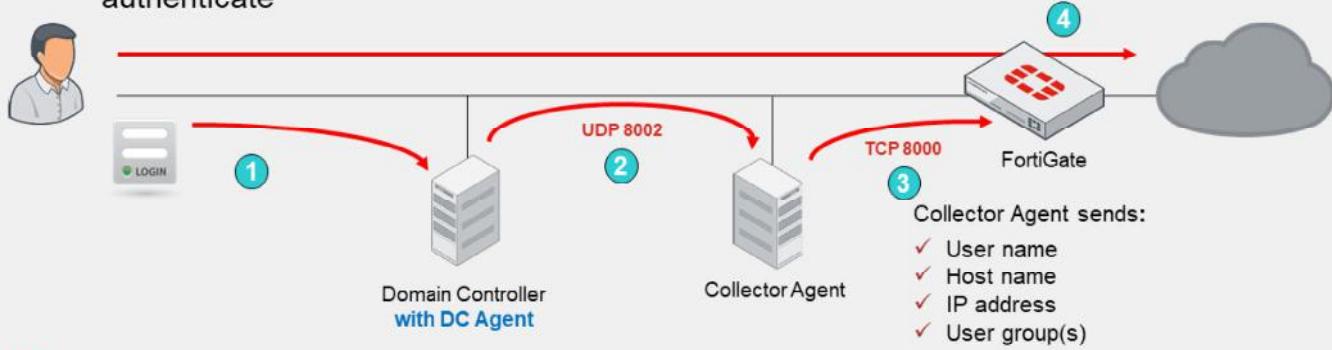
```
donot_resolve = (DWORD) 1 at HKLM\Software\Fortinet\FSAE/dcagent
```

**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**  
Training Institute

© Fortinet Inc. All Rights Reserved.

6

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)



© Fortinet Inc. All Rights Reserved.

7

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

- DC returns all requested login events every 3 seconds\*
  - Reads selected event logs
- Improves WinSec bandwidth usage
  - Reduces network load between collector agent and DC

### WinSecLog

- Polls all security events on DC every 10 seconds, or more\*
  - Log latency if network is large or system is slow
  - Requires fast network links
- Slower, but...
  - Sees all login events
  - Only parses known event IDs by collector agent

### NetAPI

- Polls the NetSessionEnum function on Windows every 9 seconds, or less\*
  - Authentication session table in RAM
- Retrieves login sessions, including DC login events
- Faster, but...
  - 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.

8

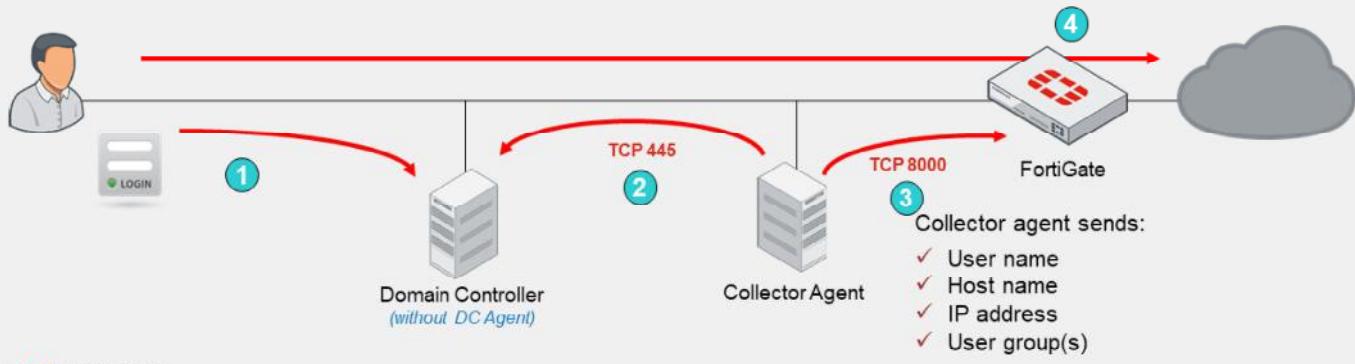
As previously stated, collector agent-based polling mode has three methods (or options) for collecting login information. The order on the slide from left to right shows most recommend to least recommended:

- **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**  
 Training Institute

© Fortinet Inc. All Rights Reserved.

9

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 (or, alternatively, dcagent.dll) 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



© Fortinet Inc. All Rights Reserved. 10

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.

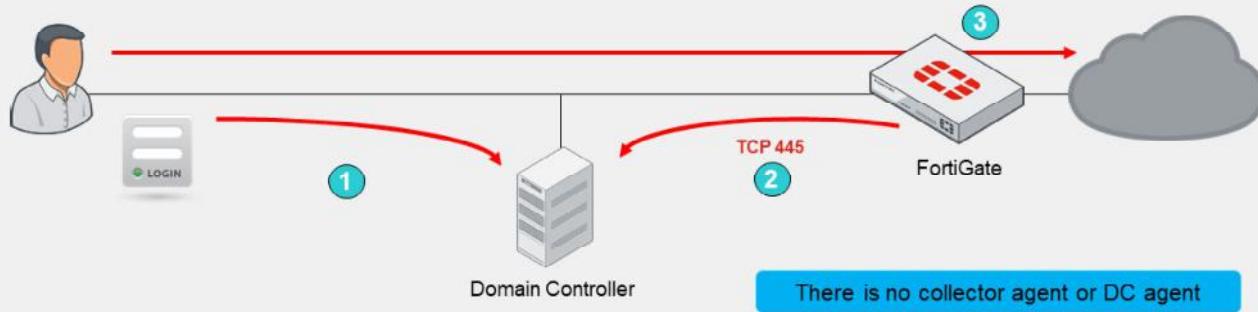
Agentless polling mode operates in a similar way to WinSecLog, but with only two event IDs: 4768 and 4769. Because there's no collector agent, FortiGate uses the SMB protocol to read the event viewer logs from the DCs.

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



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

|                            | <b>DC agent mode</b>                                          | <b>Polling mode</b>                                      |
|----------------------------|---------------------------------------------------------------|----------------------------------------------------------|
| <b>Installation</b>        | Complex—multiple installations (one per DC). Requires reboot. | Easy—one or no installations. No reboot required.        |
| <b>DC agent required</b>   | Yes                                                           | No                                                       |
| <b>Resources</b>           | Shares with DC agents                                         | Has own resources                                        |
| <b>Scalability</b>         | Higher                                                        | Lower                                                    |
| <b>Redundancy</b>          | Yes                                                           | Yes                                                      |
| <b>Level of confidence</b> | 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 work of capturing logins is done by the DC agents who pass their 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 machine 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:

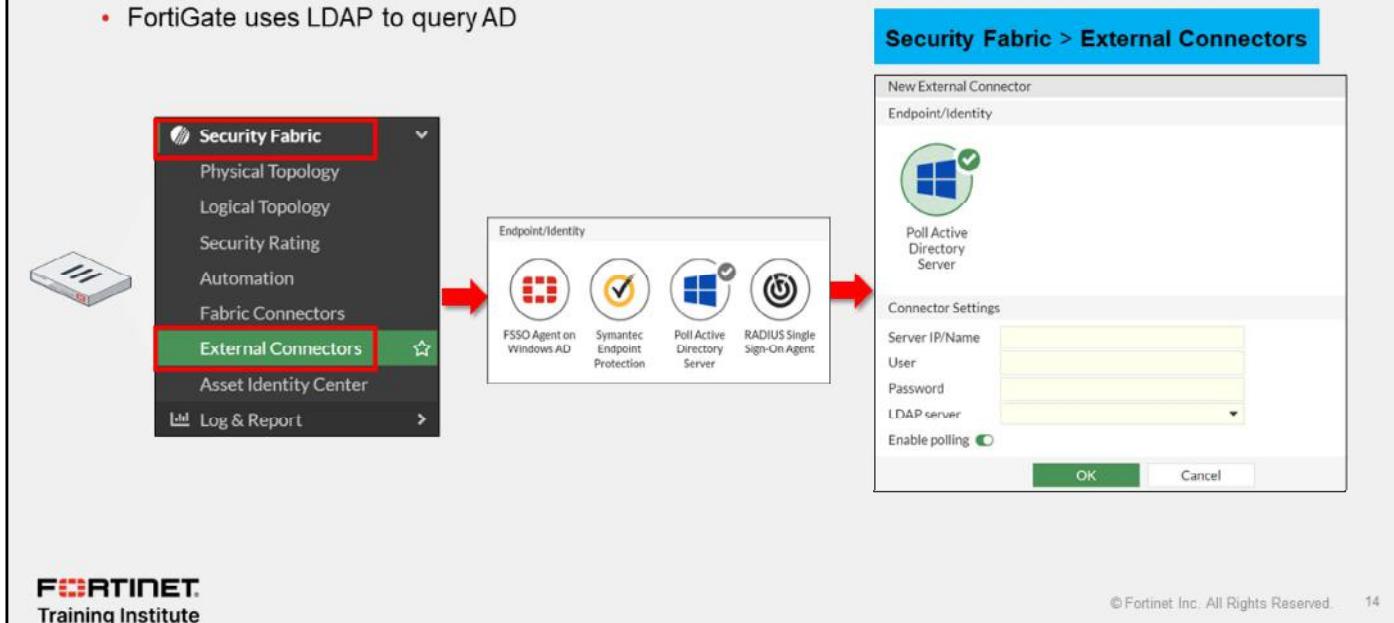
- Microsoft Windows login events have the workstation name and username, but not the workstation IP address. When the collector agent receives a login event, it queries a DNS server to resolve the IP address of the workstation. So, FSSO requires that you have your own DNS server. If a workstation IP 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**

## FSSO Configuration—Agentless Polling Mode

- Agentless polling mode:
  - FortiGate uses LDAP to query AD



**FORTINET**  
 Training Institute

© Fortinet Inc. All Rights Reserved. 14

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.

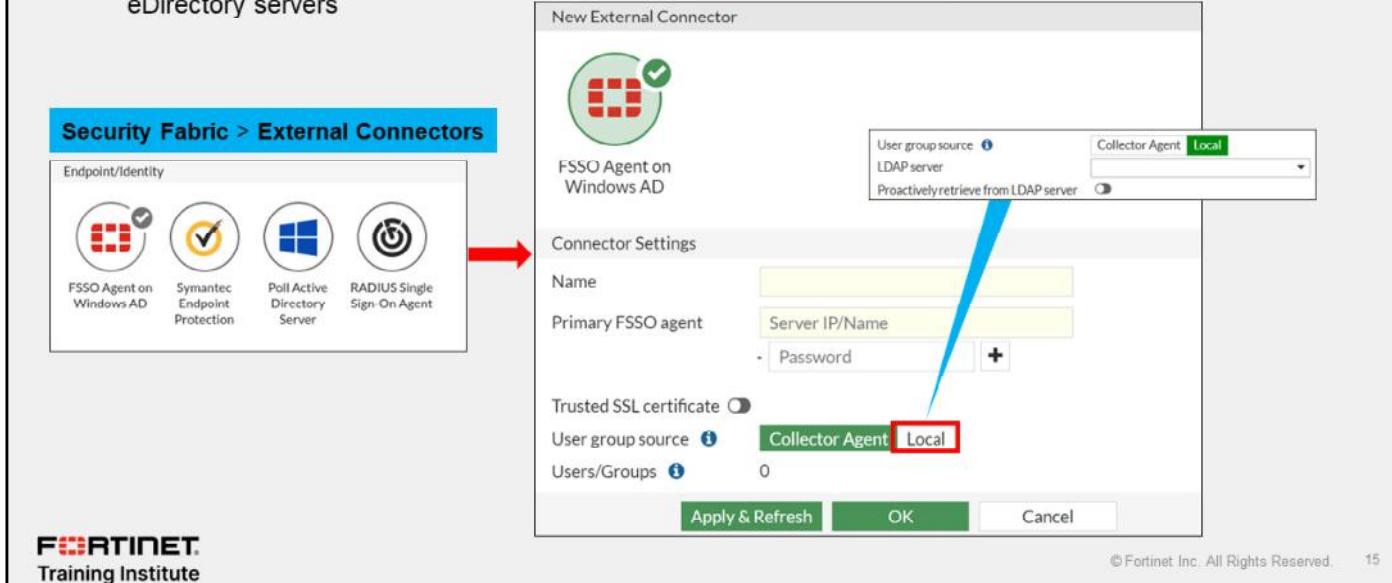
FortiGate uses LDAP to query AD to retrieve user group information. For this to happen, you must add the LDAP server to the **Poll Active Directory Server** configuration.

# 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**

The screenshot shows the FortiCloud Support interface. In the left sidebar under 'ASSET MANAGEMENT', there is a 'Products' section with a 'Dashboard' icon. In the main area, under 'DOWNLOADS', there is a 'Firmware Download' link. Other links include 'VM Images', 'Service Updates', 'HQIP Images', and 'Firmware Image Checksum'.

### Available agents:

- DC agent: DCAgent\_Setup
- CA for Microsoft servers: FSSO\_Setup
- CA for Novell: FSSO\_Setup\_edirectory
- TS Agent: TSAgent\_Setup

The screenshot shows the 'Select Product' page for FortiGate v7.00 > 7.4 > 7.4.1 > FSSO. The 'Download' tab is selected. A table lists various FSSO agent files:
 

| Name                               | Size (KB) | Date Created        | Date Modified       | HTTPS Checksum |
|------------------------------------|-----------|---------------------|---------------------|----------------|
| DCAgent_Setup_5.0.0312.exe         | 4,400     | 2023-08-31 12:08:15 | 2023-08-31 12:08:15 | HTTPS Checksum |
| DCAgent_Setup_5.0.0312.msi         | 4,094     | 2023-08-31 12:08:29 | 2023-08-31 12:08:29 | HTTPS Checksum |
| DCAgent_Setup_5.0.0312_x64.exe     | 5,238     | 2023-08-31 12:08:28 | 2023-08-31 12:08:28 | HTTPS Checksum |
| DCAgent_Setup_5.0.0312_x64.msi     | 4,932     | 2023-08-31 12:08:18 | 2023-08-31 12:08:18 | HTTPS Checksum |
| FSSO_Setup_5.0.0312.exe            | 11,952    | 2023-08-31 12:08:12 | 2023-08-31 12:08:13 | HTTPS Checksum |
| FSSO_Setup_5.0.0312_x64.exe        | 12,284    | 2023-08-31 12:08:23 | 2023-08-31 12:08:24 | HTTPS Checksum |
| FSSO_Setup_edirectory_5.0.0312.exe | 5,608     | 2023-08-31 12:08:29 | 2023-08-31 12:08:21 | HTTPS Checksum |
| install.msi                        | 4         | 2023-08-31 12:08:04 | 2023-08-31 12:08:06 | HTTPS Checksum |
| TSAgent_Setup_5.0.0312.exe         | 4,644     | 2023-08-31 12:08:31 | 2023-08-31 12:08:32 | HTTPS Checksum |
| TSAgent_Setup_5.0.0312.msi         | 4,308     | 2023-08-31 12:08:09 | 2023-08-31 12:08:10 | HTTPS Checksum |

**FORTINET**  
Training Institute

© Fortinet Inc. All Rights Reserved.

16

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 (TSAgent) installer for Citrix and terminal servers: TSAgent\_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**  
 Training Institute

17

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

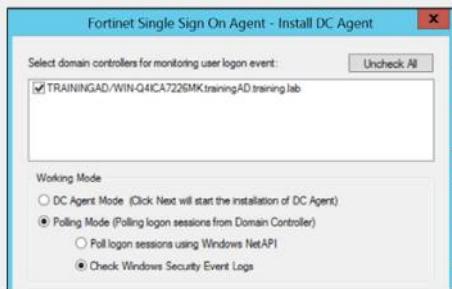
### 1 IP and port for collector agent



### 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

**FORTINET.**  
Training Institute

© Fortinet Inc. All Rights Reserved.

18

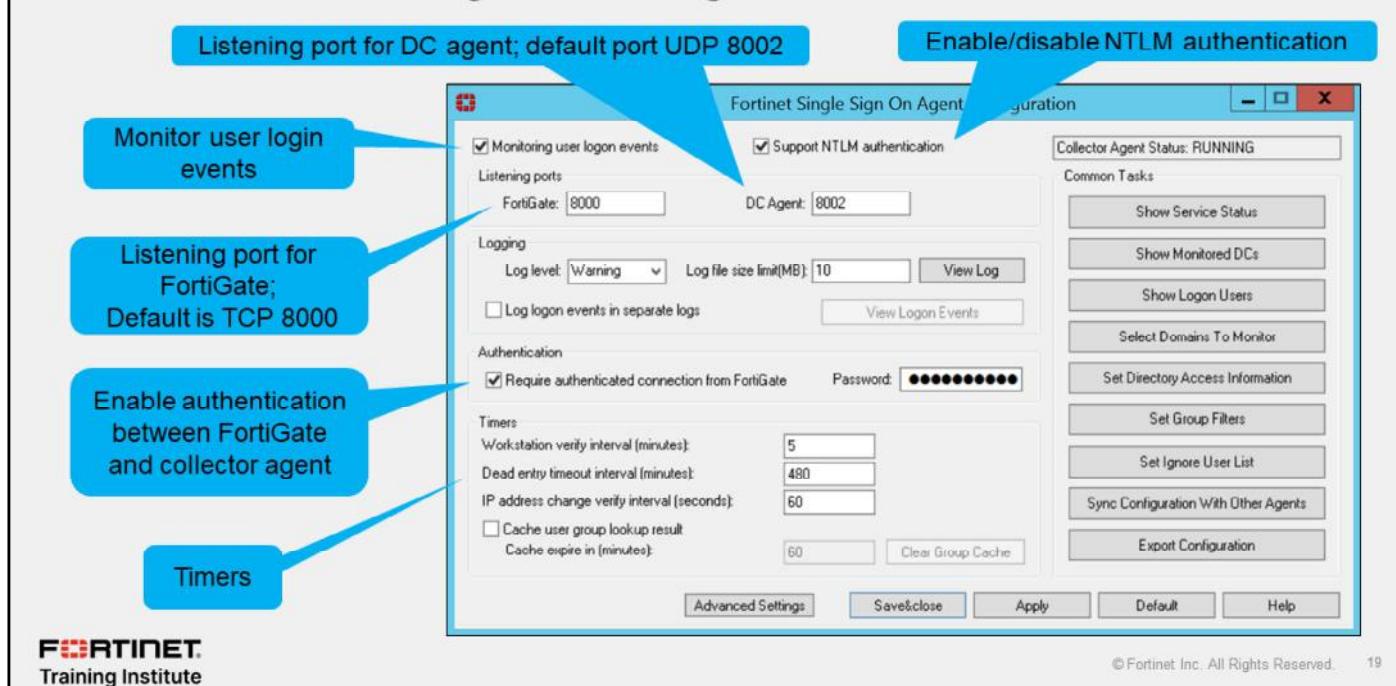
If you have just installed the collector agent and you selected **Launch DC Agent Install Wizard**, the installation process for domain controller agent automatically starts.

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



**FORTINET**  
 Training Institute

© Fortinet Inc. All Rights Reserved.

19

On the FSSO agent configuration GUI, you can configure settings such as:

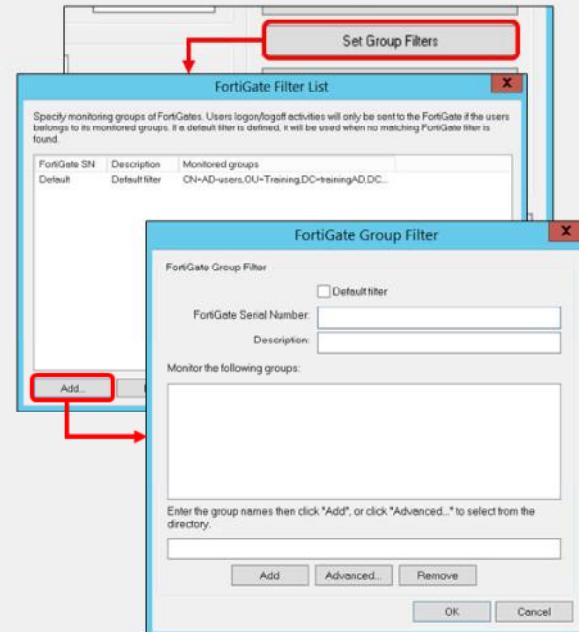
- The listening port for the communication with the DC agents (UDP)
- The listening port for the communication with FortiGate (TCP)
- NTLM authentication support
- Password authentication between the collector agent and FortiGate
- Timers

# 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.

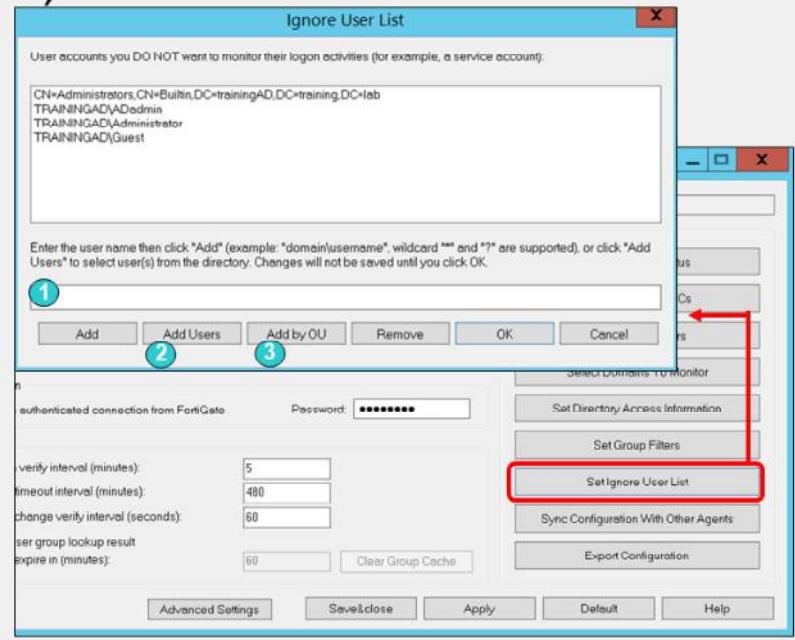
# DO NOT REPRINT

## © 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



**FORTINET**  
Training Institute

© Fortinet Inc. All Rights Reserved. 22

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

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**

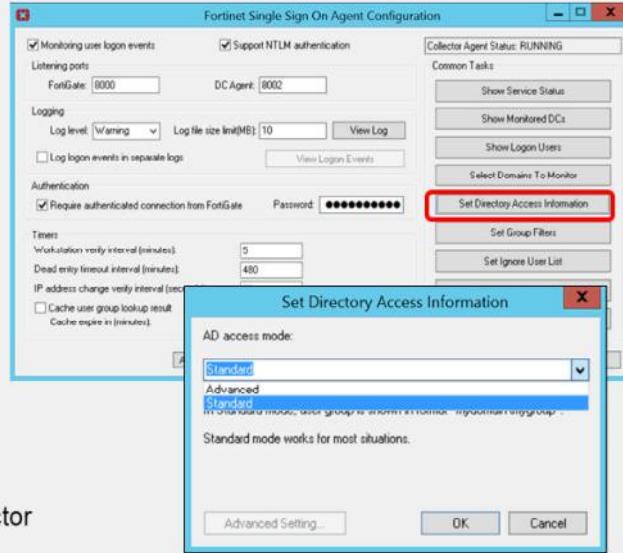
## AD Access Mode Configuration

### Standard access Mode

- Windows convention:
  - Domain\groups
- Firewall policy to groups
  - 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 to 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**. You can set the AD access mode by clicking **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 policies can be applied to individual users, user groups, and OUs.

In comparison, in standard mode, you can have a firewall policy with a security profile which can apply to user groups but not to individual users.

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 says, 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. So it is recommended that you create filters from the collector agent.

**DO NOT REPRINT**

**© FORTINET**

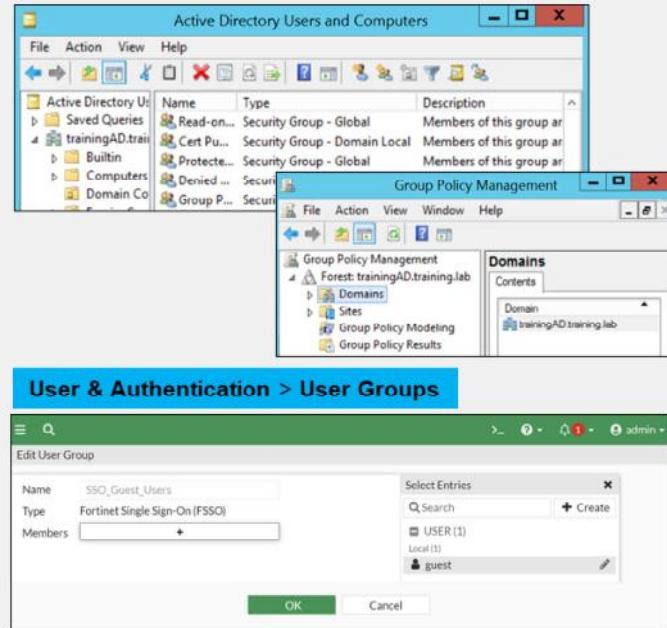
## AD Group Support

### 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**  
Training Institute

© Fortinet Inc. All Rights Reserved.

25

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.

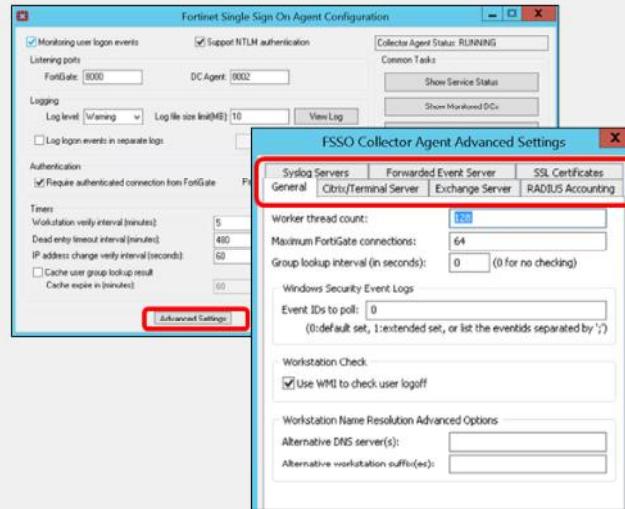
However, if both passive and active authentication are enabled for specific traffic, you cannot use **SSO\_Guest\_Users**, because traffic from IP addresses not on the FSSO user list must be prompted to enter their credentials.

**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

**FORTINET**  
 Training Institute

© Fortinet Inc. All Rights Reserved.

26

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**

## 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



© Fortinet Inc. All Rights Reserved. 27

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**

**1** 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   |

**2** 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

**3**

| 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     |
| <b>43014</b> | <b>Notification</b> | <b>FSSO user logged on</b>     |
| 43015        | Notification        | FSSO user logged off           |
| 43016        | Notification        | NTLM authentication successful |
| 43017        | Notification        | NTLM authentication failed     |

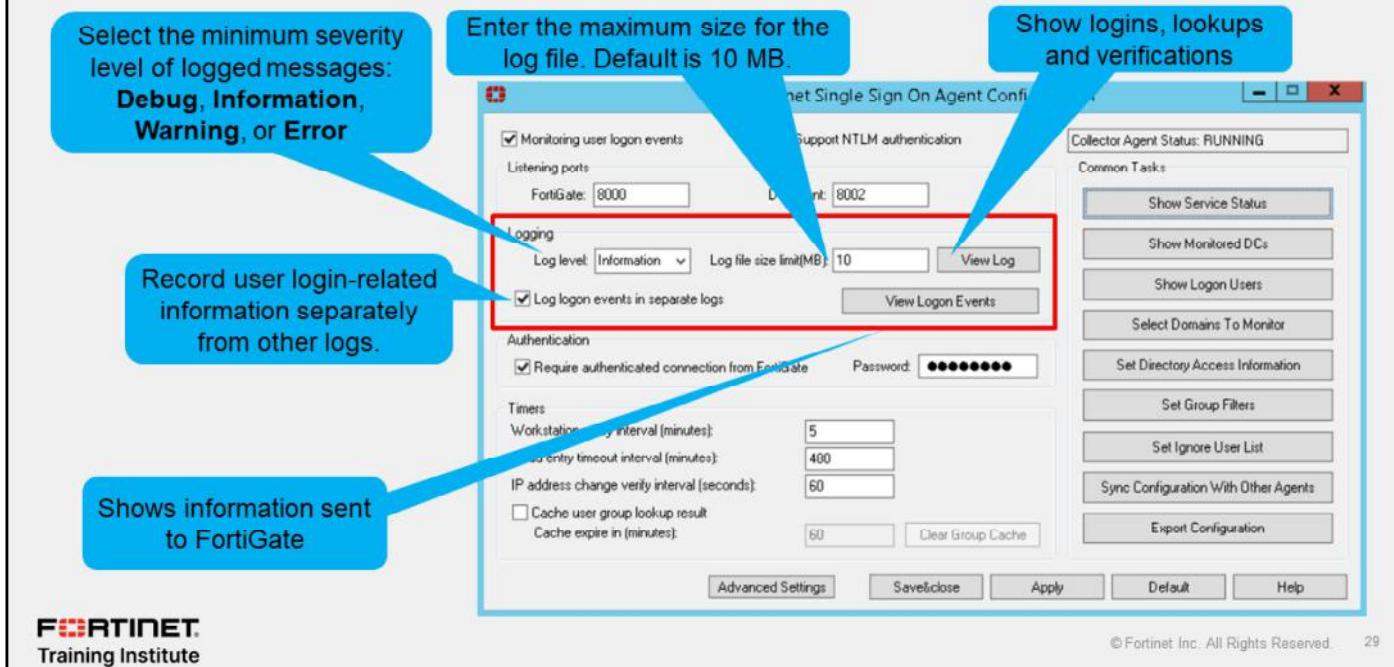
© Fortinet Inc. All Rights Reserved. 28

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



**FORTINET**  
Training Institute

© Fortinet Inc. All Rights Reserved. 29

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-On Users

The screenshot illustrates the integration of Fortinet Single Sign-On (FSSO) across different management interfaces.

**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-US...
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 in the first log entry (10.0.1.10).
- User name: Points to the user name in the first log entry (ADUSER1).
- User group: Points to the user group in the first log entry (TRAININGAD/AD-USERS).
- Workstation name: Points to the workstation name in the first log entry (WIN-INTERNAL).
- Group created on FortiGate: Points to the "MemberOf: Training" entry in the first log entry, indicating a local group was created on the FortiGate.

**Dashboard > Assets & Identities > Firewall Users:**

The dashboard shows a summary of users and their groups. A callout box contains the command:

```
execute fssso refresh
```

Annotations for the GUI:

- User Group: Points to the "Training" group listed under User Group.
- Members: Points to the "TRAININGAD/AD-USERS" members listed under Members.
- Group Type: Points to the "Fortinet Single Sign-On (FSSO)" group type listed under Group Type.

© Fortinet Inc. All Rights Reserved. 30

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 fssso <...>

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 fssso` 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.

diagnose sniffer packet any 'host ip address and tcp port 445'

diagnose debug application fssod -1

Active FSSO users

Sniff polls

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**

## Review

- ✓ Install FSSO in DC agent mode
- ✓ Install collector agent
- ✓ Troubleshoot FSSO login issues



© Fortinet Inc. All Rights Reserved. 35

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

By mastering the objectives covered in this lesson, you learned how to use FSSO so that your users don't need to log in each time they access a different network resource.

**DO NOT REPRINT****© FORTINET**

# FortiGate Administrator

## Certificate Operations

FortiOS 7.4

Last Modified: 15 November 2023

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**

## Objectives

- Configure FortiGate for full SSL/SSH inspection
- Install private CA certificates on endpoints
- Troubleshoot certificate issues



© Fortinet Inc. All Rights Reserved.

2

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

**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



© Fortinet Inc. All Rights Reserved.

3

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**

## FortiGate Uses SSL for Privacy

- SSL features:
  - Privacy of data
  - Identifies one or both parties using certificates
  - Uses symmetric and asymmetric (public key) cryptography
- Symmetric cryptography
  - Uses the same key to encrypt and decrypt data
  - Need safe way to exchange the single key
  - Faster than asymmetric cryptography
  - Used by FortiGate for exchange with other managed devices, for example, FortiManager
- Asymmetric cryptography
  - Uses two keys, one public and one private
  - Only the public key is shared with peers
  - Slower and more resource intensive than symmetric cryptography
  - Widely used, for example, HTTPS traffic



© Fortinet Inc. All Rights Reserved.

4

FortiGate uses SSL to ensure that data remains private when connecting with servers, such as FortiGuard, and with clients, such as a web browser. Another feature of SSL is that FortiGate can use it to identify one or both parties using certificates. SSL uses symmetric and asymmetric cryptography to establish a secure session between two points.

It is beneficial to understand the high-level process of an SSL handshake in order to understand how FortiGate secures private sessions.

For symmetric cryptography, the same key is used to encrypt and decrypt the traffic. This process requires fewer computing resources and is faster than asymmetric cryptography. However, one drawback is the requirement to share the key between participating devices in a safe way. When FortiGate establishes an SSL session between itself and another device, it must share the symmetric key (or rather the value required to produce it—usually the password you configure), so that data can be encrypted by one side, sent, and decrypted by the other side.

Asymmetric cryptography uses a pair of keys: One key performs one function, and the other key performs the opposite function. When FortiGate connects to a web server, for example, it uses the web server public key to encrypt a string known as the premaster secret. The web server private key decrypts the premaster secret.

**DO NOT REPRINT**  
**© FORTINET**

## Using Certificates to Identify a Person or Device

- What is a digital certificate?
  - A digital identity produced and signed by a certificate authority (CA)
  - Analogy: passport or driver's license
- 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...        |

### What is a digital certificate?

A digital certificate is a digital document produced, and signed by a certificate authority (CA). It identifies an end entity, such as a person (for example, Joe Bloggins), a device (for example, webserver.acme.com), or thing (for example, a certificate revocation list). FortiGate identifies the device or person by reading the common name (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**

## 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

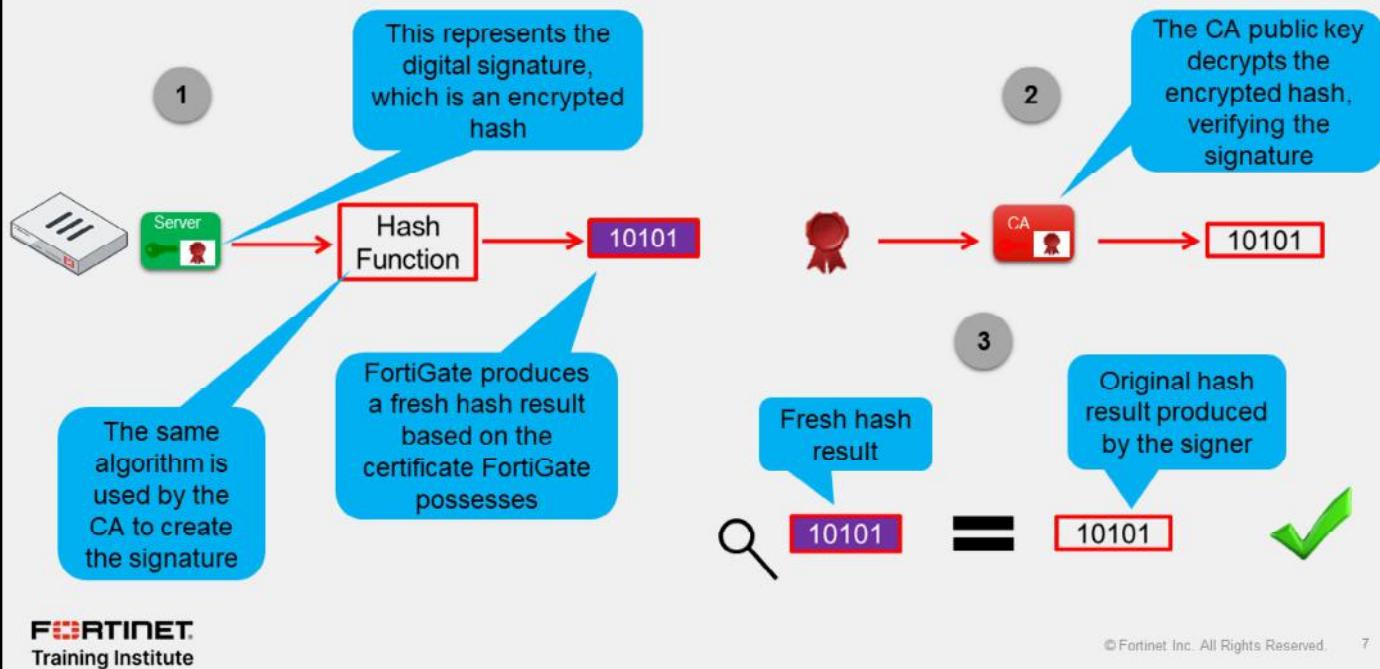
| Field                        | Value                               |
|------------------------------|-------------------------------------|
| Version                      | V3                                  |
| Serial number                | 0cacbf0403e86fc4ba3da5f26b...       |
| Signature algorithm          | 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...        |

FortiGate runs the following checks before it trusts the certificate:

- Checks the certificate revocation lists (CRLs) locally on FortiGate to verify if the certificate has been revoked by the CA.
  - FortiGate can download the relevant CRLs, 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.
  - FortiGate also supports the Online Certificate Status Protocol (OCSP). When FortiGate uses the OCSP, it interacts with an OCSP responder (FortiAuthenticator acts as the OCSP responder) to check if the certificate is still valid.
- 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



Before it generates a digital signature, the CA runs the content of the certificate through a hash function, which produces a hash result. The hash result, which is a mathematical representation of the data, is referred to as the *original hash result*. The CA encrypts the original hash result using its *private key*. The encrypted hash result is the digital signature.

When FortiGate verifies the digital signature, it 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.

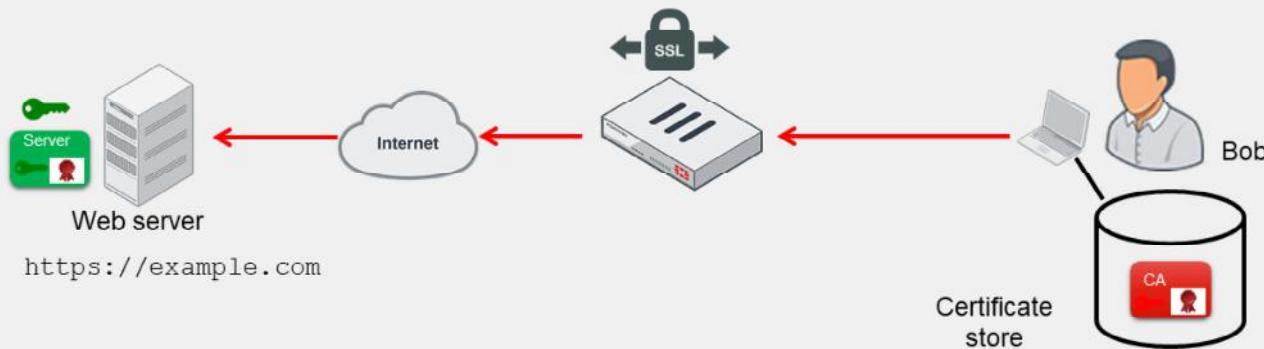
FortiGate decrypts the encrypted hash result (or digital signature) using the CA *public key* and applying the same algorithm that the CA used to encrypt the hash result. This process verifies the signature. If the key cannot restore the encrypted hash result to its original value, then the signature verification fails.

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.

**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**  
Training Institute

© Fortinet Inc. All Rights Reserved.

8

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.

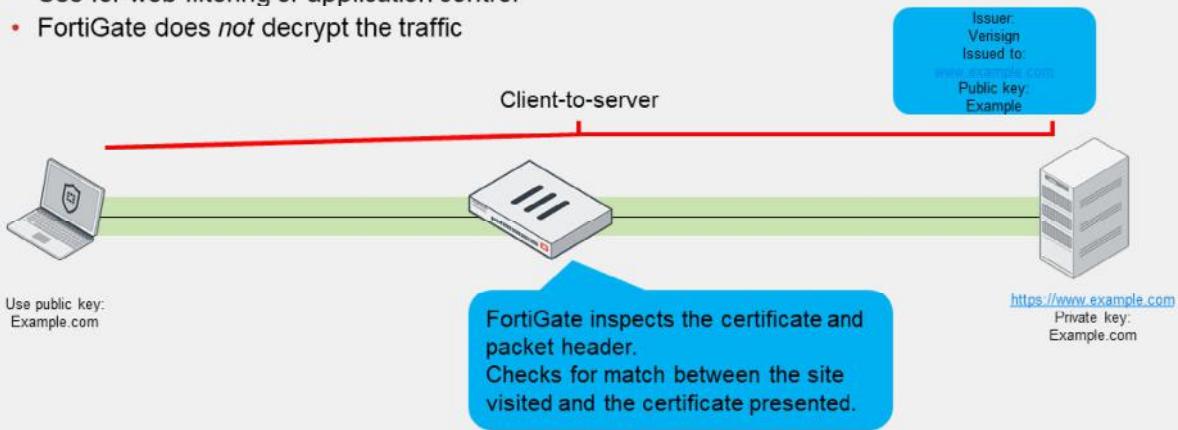
In the example shown on this slide, Bob connects to a site with a certificate issued by a legitimate CA. Because the CA is an approved CA, the CA verification certificate is in Bob's certificate store, and Bob's browser is able to establish an SSL session with the [example.com](https://example.com) site. However, unknown to Bob, the [example.com](https://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 Subject Alternative Name (**SAN**) fields
  - Use for web filtering or application control
  - FortiGate does *not* decrypt the traffic



**FORTINET**  
Training Institute

© Fortinet Inc. All Rights Reserved.

9

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 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 DNS name before receipt of the server certificate. If there is no SNI exchanged, then FortiGate identifies the server by the value in the **Subject** field or **SAN** (subject alternative name) 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.

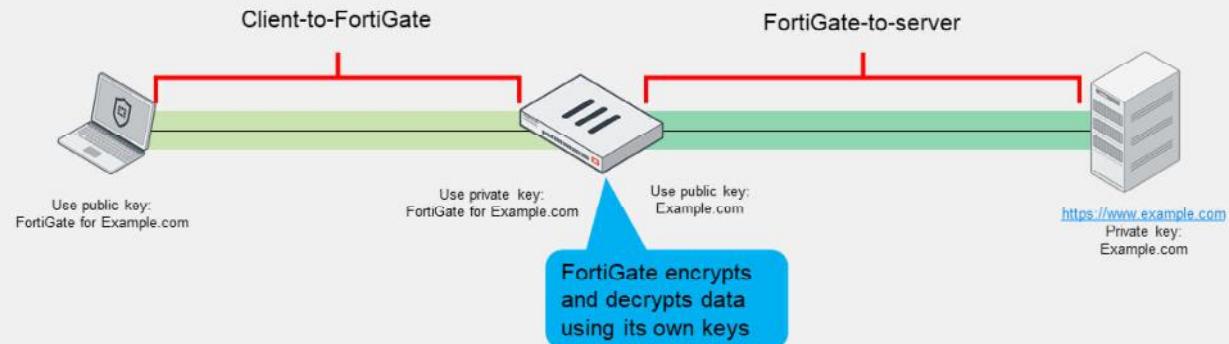
The only security features you can apply using SSL certificate inspection mode are web filtering and application control. SSL certificate inspection allows FortiGate to identify the website visited or the application in use and categorize it. You can, therefore, use it to make sure that the HTTPS protocol 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**  
Training Institute

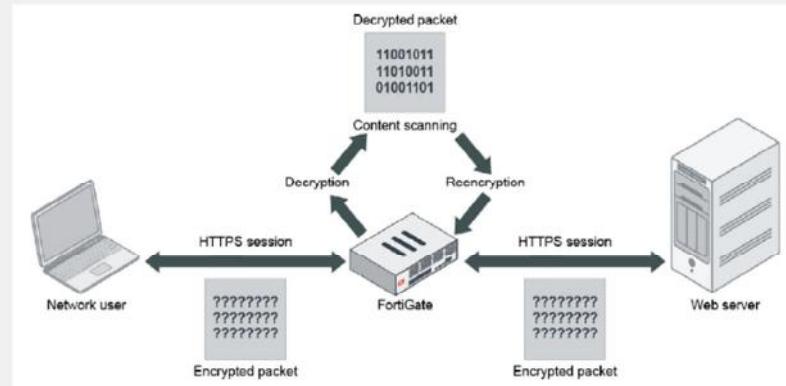
© Fortinet Inc. All Rights Reserved. 10

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

- 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



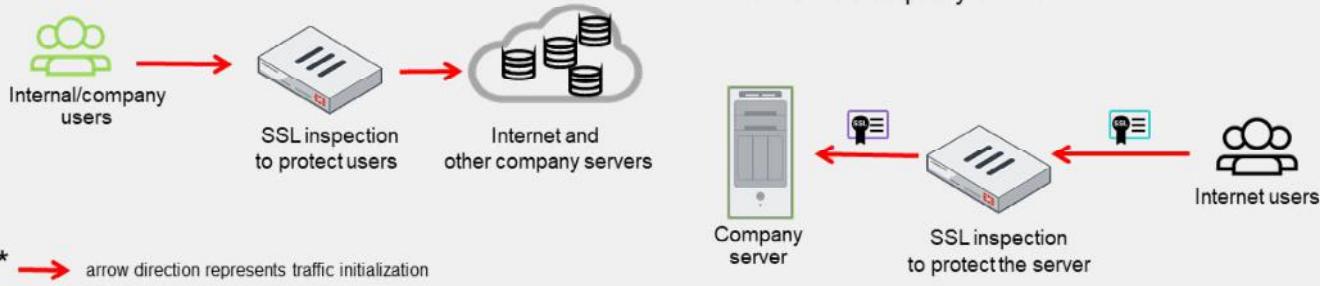
When you use deep inspection, FortiGate impersonates the recipient of the originating SSL session, and then decrypts and inspects the content to find threats and block them. It then re-encrypts the content and sends it to the real recipient. Deep inspection protects from attacks that use HTTPS and other commonly used SSL-encrypted protocols, such as SMTPS, POP3S, IMAPS, and FTPS.

# DO NOT REPRINT

## © FORTINET

### Inbound or Outbound SSL/SSH Inspection

- SSL/SSH inspection for outbound traffic
  - Protecting internal users
  - Multiple clients connecting to multiple servers
    - External web servers
    - External mail servers
    - External FTPS servers
- SSL/SSH inspection for inbound traffic
  - Protecting a single company server
    - HTTPS server
    - Mail server
    - FTPS server
  - FortiGate use a server certificate
  - FortiGate as proxy server



FortiGate can proceed to SSL/SSH inspection for inbound traffic. Usually, this is the traffic initiated by local users bound for web servers on the internet. FortiGate protects users from traffic received from outside servers.

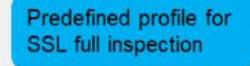
Conversely, you can use FortiGate to protect the company servers. Typically, you will protect the company web server from the outside world. For this purpose, FortiGate acts as a proxy server and presents the server certificate to internet users.

**DO NOT REPRINT**  
**© FORTINET**

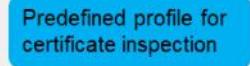
## SSL Inspection Profile Configuration

- Ready-to-use profiles for inspection of outbound encrypted sessions
  - SSL certificate inspection
  - SSL full inspection
- Customizable profile
  - Outbound deep inspection with options
- User-defined profile
  - Inbound traffic
  - Outbound traffic

| Security Profiles > SSL/SSH Inspection |                                             |
|----------------------------------------|---------------------------------------------|
| Name                                   | Comments                                    |
| SSL custom-deep-inspection             | Customizable deep inspection profile.       |
| SSL deep-inspection                    | Read-only deep Inspection profile.          |
| SSL no-inspection                      | Read-only profile that does no inspection.  |
| SSL certificate-inspection             | Read-only SSL handshake inspection profile. |



Predefined profile for  
SSL full inspection



Predefined profile for  
certificate inspection

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 the outbound traffic.

If you define an inspection profile for inbound traffic, or use some specific options for an outbound inspection profile, you can adjust the **custom-deep-inspection** profile or create your own profile.

**DO NOT REPRINT**  
**© FORTINET**

## SSL Inspection Profile Configuration (Contd)

- Customized SSL/SSH inspection profile
  - Based on deep inspection profile
  - User defined

The screenshot shows the 'Edit SSL/SSH Inspection Profile' screen. The profile name is 'custom-deep-inspection' and the comment is 'Customizable deep Inspection profile.' Under 'SSL Inspection Options', there are several settings:
 

- 'Enable SSL inspection of' is set to 'Multiple Clients Connecting to Multiple Servers' (Protecting SSL Server).
- 'Inspection method' is set to 'SSL Certificate Inspection' (Full SSL Inspection). A dropdown menu shows 'Fortinet\_CA\_SSL' with options 'Allow', 'Block', and 'View Blocked Certificates'.
- 'CA certificate' is set to 'Fortinet\_CA\_SSL' with options 'Allow', 'Block', and 'Download'.
- 'Blocked certificates' has actions 'Allow', 'Block', and 'Ignore'.
- 'Untrusted SSL certificates' has actions 'Allow', 'Block', and 'Ignore'.
- 'Server certificate SNI check' has actions 'Enable', 'Strict', and 'Disable'.
- 'Enforce SSL cipher compliance' is off.
- 'Enforce SSL negotiation compliance' is off.
- 'RPC over HTTPS' is off.

**FORTINET**  
 Training Institute

© Fortinet Inc. All Rights Reserved.

14

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 output 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 re-encryption 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 if 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)

| Exempt from SSL Inspection |                                     |
|----------------------------|-------------------------------------|
| Reputable websites         | <input checked="" type="checkbox"/> |
| Web categories             | <input type="checkbox"/>            |
| Addresses                  | <input type="checkbox"/>            |

Log SSL exemptions

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 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.

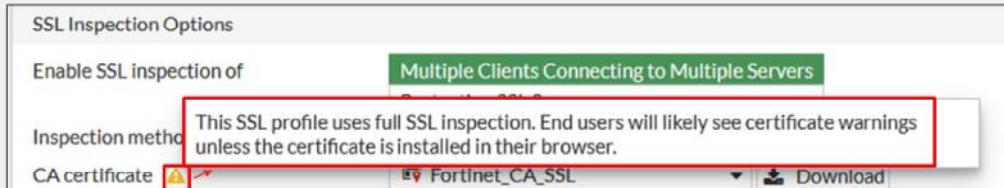
Laws protecting privacy might be another reason to bypass SSL inspection. For example, in some countries, it is illegal to inspect SSL bank-related traffic. Configuring an exemption for sites is simpler than setting up firewall policies for each individual bank. You can exempt sites based on their web 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 **Health 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**

## 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 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 re-encryption 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 trusted CA on the user devices. You can install it as part of the deployment process for all your company computers. Alternatively, you can install on FortiGate a CA certificate, used for traffic re-encryption, 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. You will discover them on the next slide.

**DO NOT REPRINT****© FORTINET**

## Full SSL Inspection—Certificate Requirements

- Full SSL inspection requires that FortiGate acts 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:
  - Preloaded, self-signed `Fortinet_CA_SSL` certificate
  - A certificate issued by the company CA
- The root CA certificate must be imported into the client machines



© Fortinet Inc. All Rights Reserved.

17

To perform full SSL inspection, FortiGate performs as a web proxy, and must act as a CA in order to re-encrypt the traffic. The FortiGate internal CA must generate an SSL private key and certificate each time it needs to re-encrypt 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 correspond 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 the **keyUsage** extension 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 request the CA administrator to issue a certificate for your FortiGate device. The FortiGate device then acts as a subordinate CA.

If you use the `Fortinet_CA_SSL` certificate, or a certificate issued by your company CA, to trust FortiGate and accept re-encrypted SSL sessions without warning, you must import the root CA certificate used to your client devices.

# 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

The screenshot shows the 'Policy & Objects > Firewall Policy' section of the FortiGate GUI. Under 'Security Profiles', several profiles are listed with their status (green circle) and name (orange box). The 'SSL Inspection' profile is highlighted with a red border and a warning icon (yellow triangle with an exclamation mark). A dropdown menu is open over this profile, showing five options: 'custom-deep-inspection' (selected), 'certificate-inspection', 'deep-inspection', and two 'SSL no-inspection' entries. A blue callout box points to the 'custom-deep-inspection' option with the text 'Select SSL inspection profiles'. Another blue callout box points to the 'Decrypted Traffic Mirror' checkbox below the SSL inspection profile with the text 'Enable to mirror decrypted SSL traffic'.

**FORTINET**  
Training Institute

© Fortinet Inc. All Rights Reserved.

18

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 that 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 warn about 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 only with flow-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 re-encrypts 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](http://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

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**  
Training Institute

© Fortinet Inc. All Rights Reserved. 20

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 your FortiGate devices and use them to secure HTTPS connections.

**DO NOT REPRINT**  
**© FORTINET**

## FortiGate HTTPS Server Certificates

- Default settings: self-sign
  - Default
  - Triggers warning on first connection from browsers
- Alternative: Fortinet\_GUI\_Server
  - Pre-loaded on FortiGate
  - Signed by Fortinet\_CA\_SSL

The screenshot shows two side-by-side FortiGate 'System > Settings' interfaces.

**Left Panel (Default Configuration):**

- HTTP port: 80
- Redirect to HTTPS: Enabled (switch is on)
- HTTPS port: 443
- HTTPS server certificate: self-sign (selected in dropdown)
- A yellow warning box states: "Port conflicts with the SSL-VPN port setting".
- A note below says: "A default certificate is being used, which will not be able to verify the server's domain name (admins will see a warning). To avoid this warning, switch to the FortiGate's 'Fortinet\_GUI\_Server' certificate or generate a trusted certificate using Let's Encrypt." It includes "Create Certificate" and "Download the CA certificate and import into the browser" buttons.

**Right Panel (Alternative Configuration):**

- HTTP port: 80
- Redirect to HTTPS: Enabled (switch is on)
- HTTPS port: 443
- HTTPS server certificate: Fortinet\_GUI\_Server (selected in dropdown)
- A yellow warning box states: "Port conflicts with the SSL-VPN port setting".
- A note below says: "For optimal security please generate a trusted certificate using Let's Encrypt." It includes "Create Certificate" and "Download HTTPS CA certificate" buttons.

**FORTINET**  
 Training Institute

© Fortinet Inc. All Rights Reserved. 21

You can select the certificate that FortiGate presents for HTTPS GUI access from the **Settings** menu. By default, FortiGate uses the `self-sign` certificate, which is not recognized as a trusted certificate by the browsers. Alternatively, you can select the `Fortinet_GUI_Server` certificate, which is signed by the `Fortinet_CA_SSL`. With this certificate, to avoid the browser warning on HTTPS access to the FortiGate GUI, you must import the `Fortinet_CA_SSL` certificate into your management devices.

**DO NOT REPRINT**  
© FORTINET

## Download Private CA Certificates From FortiGate

- Download `Fortinet_CA_SSL` private CA certificate

The screenshot shows the FortiGate configuration interface under the 'System' menu, specifically the 'Certificates' section. At the top, there are buttons for 'Create/Import', 'Edit', 'Delete', 'View Details', and a red-bordered 'Download' button. Below these are three columns: 'Name', 'Subject', and 'Comments'. A header row indicates 'Local CA Certificate' with a count of 2. Two entries are listed:

- `Fortinet_CA_SSL`: Subject is 'C = US, ST = California, L = Sunnyvale, O...'. Comment: 'This is the default CA certificate'.
- `Fortinet_CA_Untrusted`: Subject is 'C = US, ST = California, L = Sunnyvale, O...'. Comment: 'This is the default CA certificate'.

- 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.

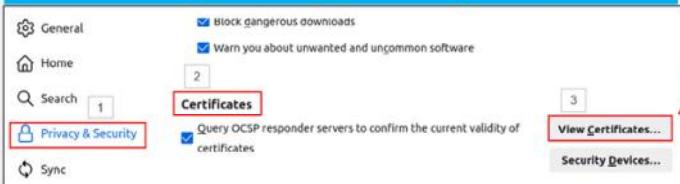
You can get it from the FortiGate certificate store available under the **System** menu. Upon download, FortiGate generates a `.cer` file that you can import into any device as required.

**DO NOT REPRINT**  
**© FORTINET**

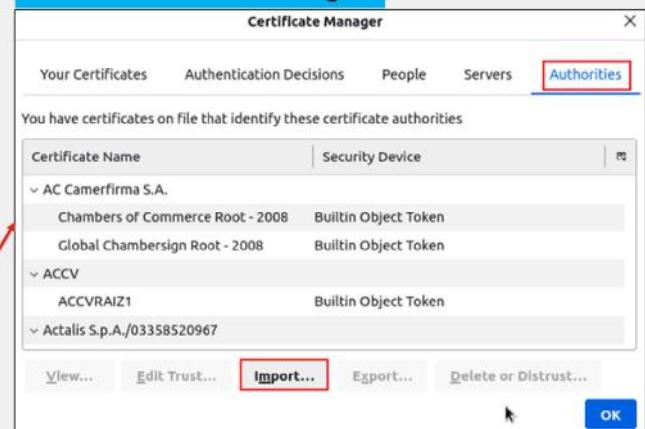
## Import Private CA Certificates Into Endpoints

- Import Fortinet\_CA\_SSL private CA certificate into user device
  - Exact process depends on the operating system
  - Example for Linux and Firefox
    - Open the browser setting menu
    - Open the certificate store
    - Import the certificate as a CA authority

### Firefox: Settings > Privacy & Security > Certificates



### Firefox: Certificate Manager



**FORTINET**  
 Training Institute

© Fortinet Inc. All Rights Reserved. 23

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.

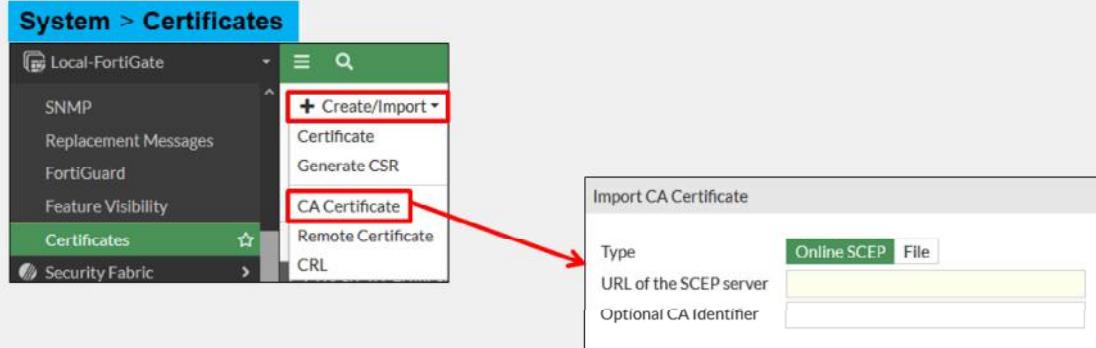
When you import the certificate, make sure that you save it to the certificate store for root authorities.

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.

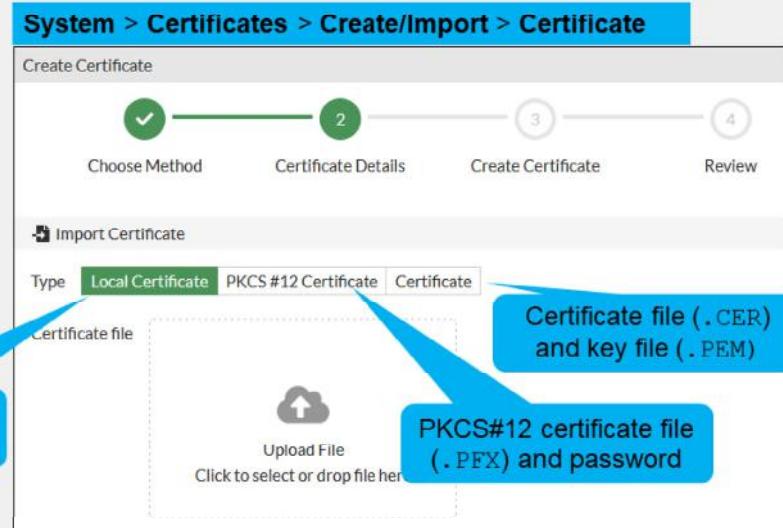
# DO NOT REPRINT

## © FORTINET

### Import a Certificate on FortiGate

- Import private certificates
- Used for:
  - FortiGate GUI
  - SSL-VPN tunnels
- Import options:
  - Certificate after CSR request
  - Certificate and associated key file
  - PKCS#12 certificate

**Certificate file (.CER) after CSR request**



If your company manages its own certificate authority, you can generate certificates for the FortiGate GUI or SSL access. You can also generate certificates that you will use for SSL-VPN tunnels.

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) 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

**System > Certificates > Create/Import > CRL**

|                                       |                                                                     |                                                  |
|---------------------------------------|---------------------------------------------------------------------|--------------------------------------------------|
| <b>Import CRL</b>                     |                                                                     |                                                  |
| Import Method                         | <input type="radio"/> File Based                                    | <input checked="" type="radio"/> Online Updating |
| <input checked="" type="radio"/> HTTP |                                                                     |                                                  |
| URL of the HTTP server                | <input type="text" value="http://crl3.digicert.com/DigiCertTLSRS"/> |                                                  |
| <input type="radio"/> LDAP            |                                                                     |                                                  |
| <input type="radio"/> SCEP            |                                                                     |                                                  |

**System > Certificates**

| Name                                                       | Subject                 | Comments               | Issuer       | Expires             | Status                                    | Source  |
|------------------------------------------------------------|-------------------------|------------------------|--------------|---------------------|-------------------------------------------|---------|
| <input checked="" type="checkbox"/> CRL ①                  |                         |                        |              |                     |                                           |         |
| <input checked="" type="checkbox"/> CRL_1                  |                         |                        | DigiCert Inc |                     | <input checked="" type="checkbox"/> Valid | User    |
| <input checked="" type="checkbox"/> Local CA Certificate ② |                         |                        |              |                     |                                           |         |
| <input checked="" type="checkbox"/> Fortinet_CA_SSL        | C = US, ST = Califor... | This is the default... | Fortinet     | 2030/04/25 13:37:28 | <input checked="" type="checkbox"/> Valid | Factory |
| <input checked="" type="checkbox"/> Fortinet_CA_Untrus...  | C = US, ST = Califor... | This is the default... | Fortinet     | 2030/04/25 12:21:58 | <input checked="" type="checkbox"/> Valid | Factory |

**FORTINET**  
Training Institute

© Fortinet Inc. All Rights Reserved. 26

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 management 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.

**System > Certificates**

| Name                    | Subject                                                      | Comments                               | Issuer       | Expires             | Status  | Source  |
|-------------------------|--------------------------------------------------------------|----------------------------------------|--------------|---------------------|---------|---------|
| CRL 1                   |                                                              |                                        | DigiCert Inc | 2024/09/27 06:21:00 | Valid   | User    |
| CRL_1                   |                                                              |                                        | DigiCert Inc | 2024/09/27 06:21:00 | Valid   | User    |
| 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**  
Training Institute

© Fortinet Inc. All Rights Reserved. 27

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

## Applications and SSL Inspection

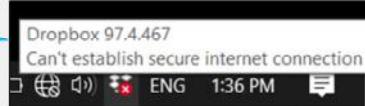
- Any SSL application might be impacted by SSL inspection (not just the browser)
  - The solution depends on the application security design
  - Consider other SSL-based protocols such as FTPS, SMTPS, and STARTTLS (not just HTTPS)
- Microsoft Outlook 365 for Windows error after enabling full SSL inspection:

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, then 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 MITM 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 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**

## 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 |
| Expired certificates              | Keep Untrusted & Allow | Block |
| Revoked certificates              | Keep Untrusted & Allow | Block |
| Validation timed-out certificates | Keep Untrusted & Allow | Block |
| Validation failed certificates    | Keep Untrusted & Allow | Block |
| Log SSL anomalies                 |                        |       |

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 or OCSP 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 because 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

The screenshot shows the 'SSL Inspection Options' section of the profile configuration. The 'Untrusted SSL certificates' dropdown is set to 'Block'. Other options shown include 'Protecting SSL Server', 'SSL Certificate Inspection' (set to 'Full SSL Inspection'), and 'CA certificate' (set to 'Fortinet\_CA\_SSL').

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.

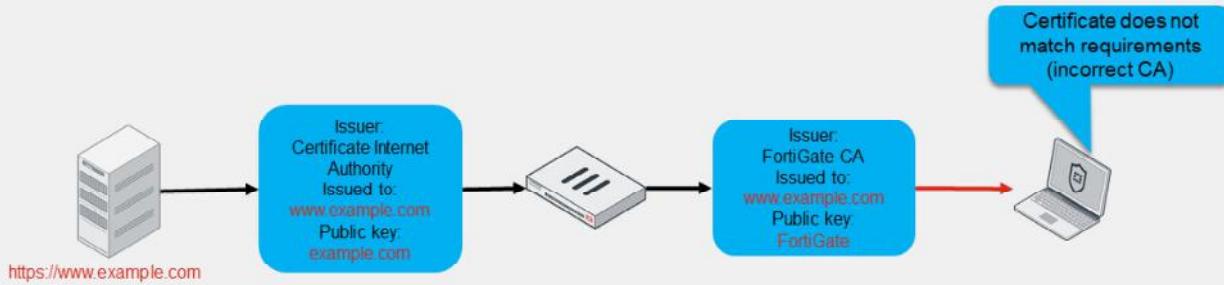
When the setting is set to **Block**, and FortiGate receives an untrusted SSL certificate, FortiGate blocks the connection outright, and the user cannot proceed.

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

## Full SSL Inspection and HSTS

- Some clients have specific requirements for SSL
  - HSTS: HTTPS Strict Transport Security
    - Example: Chrome requires a Google certificate when accessing any Google site
- HSTS common error message
  - “Privacy error: Your connection is not private” (NET::ERR\_CERT\_AUTHORITY\_INVALID)



Replacing the certificate for the traffic can cause problems. Some software and servers have specific limitations on the certificates that are allowed to be used.

HSTS is a security features designed to detect man-in-the-middle SSL attacks by making sure that any certificate presented when accessing a server resource is signed by a specific CA.

If the browser detects any other CA, it simply refuses to continue the SSL handshake, and prevents access to the website. If you are using a Chrome browser, for such sites, you will get the privacy error message “Your connection is not private” this slide shows.

# DO NOT REPRINT

## © FORTINET

## Visit Sites With HSTS Requirement

- Possible workarounds for sites with HSTS requirement
  - Exempt those websites from full SSL inspection
  - Use SSL certificate inspection instead
  - Adjust browser settings

**Security Profiles > SSL/SSH Inspection**

Exempt from SSL Inspection

Reputable websites

Web categories  +

Addresses  example.com  \*

Log SSL exemptions

Wildcard FQDN definition to exclude \*.example.com sites from SSL deep inspection

**Policy & Objects > Firewall Policy**

| ID | Name                   | Destination     | Security Profiles                         |
|----|------------------------|-----------------|-------------------------------------------|
| 2  | Exempt_Deep_Inspection | 4 Exception-Add | WEB default<br>SSL certificate-inspection |
| 1  | Full_Access            | 4 all           | WEB default<br>SSL deep-inspection        |
| 0  | Implicit Deny          | 4 all           |                                           |

Carefully define exception policy to exclude only sites that require it from deep inspection

When replacing the certificate for the traffic causes problems and prevents users from accessing some websites, the solutions available are limited. You can select one of the following workarounds according to the level at which you can act.

At the FortiGate level, you can exempt the affected websites from full SSL inspection and use certificate inspection instead. If you can act at the browser level, you can disable HSTS validation per website or globally (refer to the browser manual for the process).

If you want to use certificate inspection instead of deep inspection only for a few sites, you must be careful when defining the policy. It must be restrictive enough to match exclusively the sites that you want to allow, and which do not support deep inspection. Otherwise, you might get sites allowed to pass through with only certificate inspection instead of deep inspection.

**DO NOT REPRINT****© FORTINET**

## Knowledge Check

1. Which attribute or extension identifies the owner of a certificate?  
 A. The subject name in the certificate  
 B. The unique serial number in the certificate
  
2. Which configuration requires FortiGate to act as a CA for full SSL inspection?  
 A. Multiple clients connecting to multiple servers  
 B. Protecting the SSL server
  
3. Which inspection mode can protect your LAN devices from encrypted malware?  
 A. Certificate inspection  
 B. Deep inspection

**DO NOT REPRINT****© FORTINET**

## Review

- ✓ Describe certificate inspection and full SSL inspection
- ✓ Configure FortiGate for full SSL inspection
- ✓ Identify obstacles to implementing full SSL inspection and possible remedies



© Fortinet Inc. All Rights Reserved.

34

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



Training Institute



## FortiGate Administrator

Antivirus

FortiOS 7.4

Last Modified: 15 November 2023

In this lesson, you will learn how to use FortiGate to protect your network against viruses.

**DO NOT REPRINT****© FORTINET**

## Objectives

- Configure the antivirus profile in flow-based inspection mode
- Configure the antivirus profile in proxy-based inspection mode
- Configure protocol options
- Log and monitor antivirus events
- Troubleshoot common antivirus issues



© Fortinet Inc. All Rights Reserved.

2

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

By demonstrating competence in antivirus configuration, including reviewing antivirus logs, you will be able to use the antivirus profile effectively.

**DO NOT REPRINT**  
**© FORTINET**

## Antivirus and Inspection Modes

- Antivirus scanning engine uses antivirus signature databases to identify malicious codes

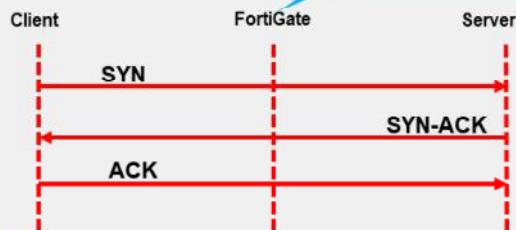


- Available inspection modes

- Flow-based inspection

- Default inspection mode

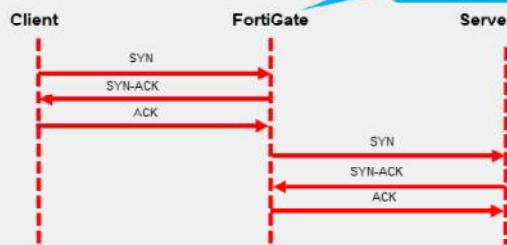
File is scanned  
on a flow basis



- Proxy-based inspection

- Provides additional options

Two TCP  
connections

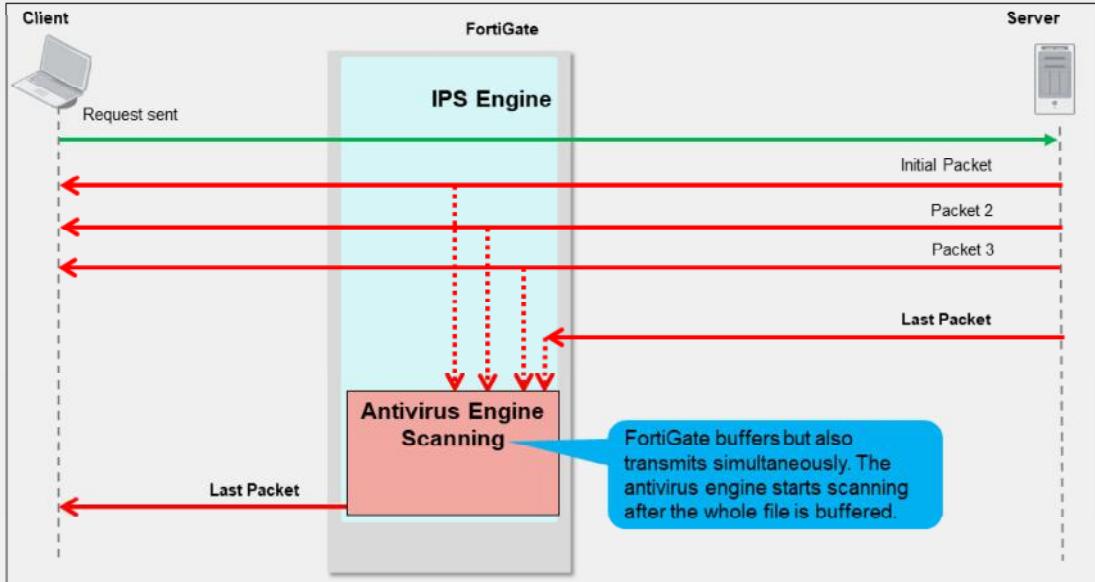


FortiGate with a valid antivirus license can update antivirus signature databases from FortiGuard servers.

Antivirus can operate in flow-based or proxy-based inspection mode.

**DO NOT REPRINT**  
**© FORTINET**

## Flow-Based Inspection Mode Packet Flow



Flow-based inspection mode uses a hybrid of two available scanning modes available: the default scanning mode and the legacy scanning mode. The default mode enhances the scanning of nested archive files without buffering the container archive file. The legacy mode buffers the full container, and then scans it.

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 a virus is found, FortiGate resets the connection and does not send the last piece of the file. Although the receiver got most of the file content, the file has been 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 then 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 SPUs to improve performance.

**DO NOT REPRINT**  
**© FORTINET**

## Flow-Based Inspection Mode

- Default mode

The image shows two screenshots of the FortiGate management interface. The left screenshot is titled "Security Profiles > AntiVirus" and shows the configuration for the "default" AntiVirus profile. It includes fields for Name (default), Comments (Scan files and block viruses. 29/255), and Action (Block or Monitor). Under "Inspected Protocols", several protocols are listed with checkboxes: HTTP, SMTP, POP3, IMAP, FTP, and CIFS. The "HTTP" checkbox is selected and highlighted with a red box. A callout bubble says "Select protocols to be scanned". Another callout bubble says "Action applied to the infected files". The right screenshot is titled "Policy & Objects > Firewall Policy" and shows the creation of a new policy. It includes fields for Name, Incoming Interface, Outgoing Interface, Source, Destination, Schedule (always), Service, and Action (ACCEPT or DENY). Under "Security Profiles", the "AntiVirus" profile is selected and highlighted with a red box. A callout bubble says "Select the antivirus profile". Other security profiles listed include Web Filter, DNS Filter, Application Control, IPS, File Filter, and SSL Inspection.

**FORTINET**  
Training Institute

© Fortinet Inc. All Rights Reserved.

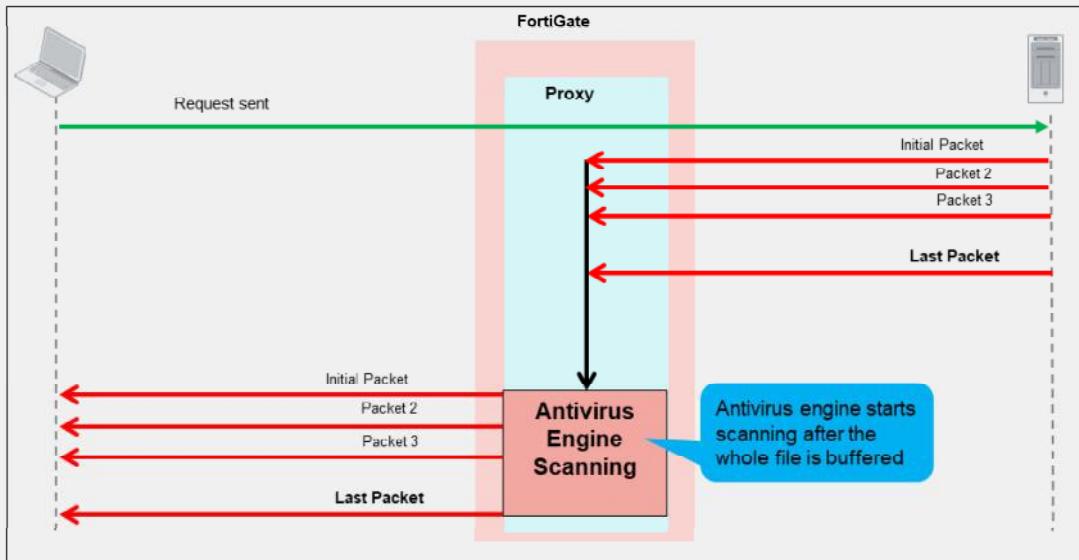
5

Flow-based inspection mode is the default mode, and its configuration consists of two steps:

- Creating an **AntiVirus Profile** with the selection of the inspected protocols, and the action taken when the FortiGate detects a virus infected file.
- Applying the flow-based **Antivirus Profile** to a firewall policy.

**DO NOT REPRINT**  
**© FORTINET**

## Proxy Inspection Mode Packet Flow



**FORTINET**  
 Training Institute

© Fortinet Inc. All Rights Reserved.

6

With a proxy inspection mode scan, the client sends a request and FortiGate starts buffering the whole file, then sends it to the antivirus engine for scanning. If the file is clean (without any viruses), FortiGate starts transmitting the file to the end client. If a virus is found, no packets are delivered to the end client and the proxy sends the replacement block message to the end client.

Because FortiGate has to buffer the whole file and then do the scanning, it takes a long time to scan. Also, from the client point of view, it has to wait for the scanning to finish and might terminate the connection because of lack of data.

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 some 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.

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.

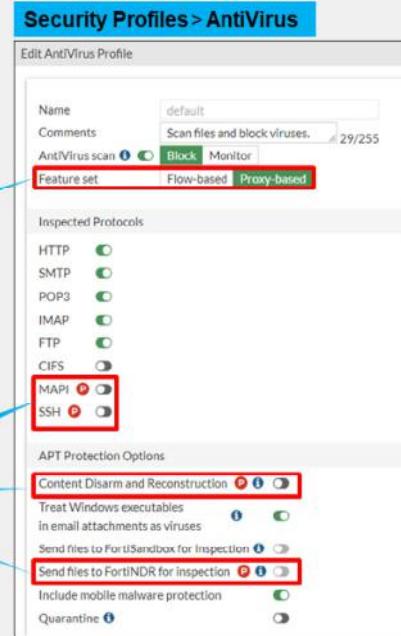
**DO NOT REPRINT**  
**© FORTINET**

## Proxy Inspection Mode Enabled

- Configure the antivirus profile
  - Feature set is Proxy-based**
- Provides additional antivirus support
  - MAPI and SSH protocols inspection
  - Content disarm and reconstruction (CDR)
  - FortiNDR inspection

Feature visibility activated through CLI

Available only in proxy inspection mode



© Fortinet Inc. All Rights Reserved.

7

**FORTINET**  
 Training Institute

Proxy-based inspection mode is applied when you set **Feature set** to **Proxy-based**. For low-end platforms, this feature is available on the GUI when you enable the CLI command `gui-proxy-inspection`.

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 content disarm and reconstruction (CDR) feature. It can also use FortiNDR to inspect high-risk files.

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 a new profile named 'Search' is being created. A third callout bubble points to the 'AntiVirus' dropdown, showing available profiles: 'default', 'Search', 'default', and 'with-default'. The interface includes fields for Name, Incoming Interface, Outgoing Interface, Source, Destination, Schedule, Service, Action (ACCEPT/DENY), NAT, IP Pool Configuration, and Firewall/Network Options.

Available only in proxy-based inspection mode

Set Inspection Mode to Proxy-based

Proxy-based and flow-based antivirus profiles available

**FORTINET**  
Training Institute

© Fortinet Inc. All Rights Reserved. 8

The next step is to apply the proxy-based antivirus profile to a firewall policy. You must set **Inspection Mode** to **Proxy-based**.

# 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, which displays a 'High Security Alert' stating that a file is infected with the virus 'EICAR\_TEST\_FILE'. It includes fields for 'File name', 'Virus name', 'Website host or URL', 'URL', and 'Reference URL'. A blue callout box labeled 'Link to FortiGuard Encyclopedia' points to the right screenshot. On the right is the 'Threat Encyclopedia' page from FortiGuard Labs, showing details for 'EICAR\_TEST\_FILE' with a release date of Oct 15, 1996, and a link to 'Analysis'.

**Antivirus Block Page Labels:**

- File name
- Virus name
- Website host or URL

**Link to FortiGuard Encyclopedia**

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
- User name 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

## Inspection Modes Use Cases

- Both use the full antivirus database

- Flow inspection mode

- Pattern matching can be offloaded to CP8 or CP9
- Priority on traffic throughput

Servers providing reliable service for large numbers of concurrent users



- Proxy inspection mode

- Required for its additional options
- Priority on network security

Protecting emails received by mail servers through SMTP or MAPI



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 then choose between the inspection modes?

If security is your priority, proxy inspection mode—with client comforting disabled—is more appropriate. If performance is your top priority, then flow 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. So, this acceleration does not apply to proxy-based inspection.

**DO NOT REPRINT**  
**© FORTINET**

## Configuring Protocol Options

- Available for both proxy-based and flow-based firewall policies

The screenshot shows two windows from the FortiGate management interface:

- Policy & Objects > Firewall Policy**: A window for creating a new policy. It includes fields for Name, Incoming Interface, Outgoing Interface, Source, Destination, Schedule, Service, Action (ACCEPT/DENY), Inspection Mode (Flow-based/Proxy-based), Firewall/Network Options (NAT, IP Pool Configuration, Preserve Source Port), and Protocol Options (Protocol Options dropdown set to 'default').
- Policy & Objects > Protocol Options**: A window titled 'New Protocol Options'. It has a 'Name' field, 'Protocol Port Mapping' table, and other sections for Common Options, Web Options, and Email Options.

Annotations highlight specific features:

- A red arrow points from the 'Protocol Options' dropdown in the Firewall Policy window to the 'Protocol Options' section in the Protocol Options window.
- A blue callout box states: "Port mapping only works in proxy-based inspection".
- A red box highlights the 'Name' field in the Protocol Options window, with a blue callout box stating: "Protocol options named to be applied in a firewall policy".
- A red box highlights the 'Specify' column in the 'Protocol Port Mapping' table, with a blue callout box stating: "You can specify more than one port number (separated by comma)".

Fortinet Training Institute logo and copyright information are visible at the bottom.

Protocol options provide more granular control than antivirus profiles. You can configure protocol port mappings, common options, web options, and email options, to name a few. Some options apply only to proxy-based inspection, like **Protocol Port Mapping**.

Protocol options are used by antivirus and other security profiles, such as web filtering, DNS filtering, and data loss prevention (DLP), to name a few.

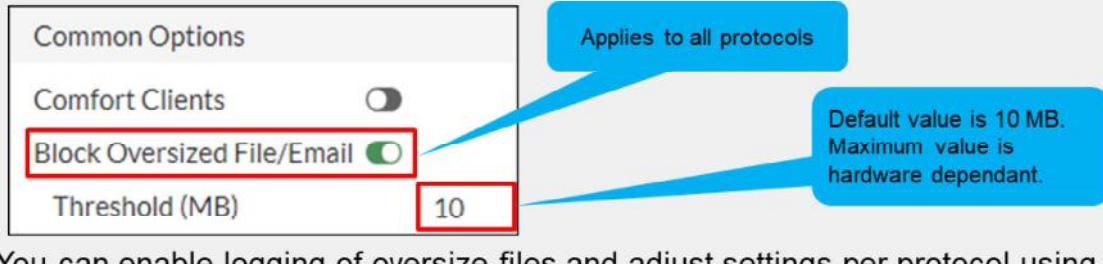
Once protocol options are configured, they are applied in the firewall policy.

# 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 files logging setting

Name of the specific protocol

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 the 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). Usually, you shouldn't increase this setting because it increases RAM usage.

# DO NOT REPRINT

## © FORTINET

## Antivirus Logs

**Log & Report > Security Events**

**Summary Logs**

**3 Events**

| Top Virus/Botnet | Action  | Count |
|------------------|---------|-------|
| EICAR TEST FILE  | Blocked | 3     |

**Summary Logs**

**Logs**

| Date/Time           | Service | Source    | File Name | Virus/Botnet    | User | Details                            | Action  |
|---------------------|---------|-----------|-----------|-----------------|------|------------------------------------|---------|
| 2023/09/13 00:49:19 | FTP     | 10.0.1.10 | elcar.com | EICAR_TEST_FILE |      | Host: 10.200.1.254                 | Blocked |
| 2023/09/13 00:49:19 | FTP     | 10.0.1.10 | elcar.com | EICAR_TEST_FILE |      | Host: 10.300.1.254                 | Blocked |
| 2023/09/13 00:49:19 | FTP     | 10.0.1.10 | elcar.com | EICAR_TEST_FILE |      | Host: 10.200.1.254                 | Blocked |
| 2023/09/13 00:43:57 | HTTP    | 10.0.1.10 | elcar.com | EICAR_TEST_FILE |      | URL: http://10.200.1.254/elcar.com | Blocked |
| 2023/09/13 00:43:12 | HTTP    | 10.0.1.10 | elcar.com | EICAR_TEST_FILE |      | URL: http://10.200.1.254/elcar.com | Blocked |

**Log Details**

Protocol: 6  
Service: HTTP

**Data**

File Name: elcar.com

**Action**

Action: Blocked  
Threat: 2  
Policy ID: 1 [Full Access]  
Policy UUID: b11ac58c-791b-51e7-4600-12f829a609d9  
Policy Type: Firewall

**Security**

Level: Warning  
Threat Level: Critical  
Threat Score: 50

**Cellular**

Service: HTTP

**AntiVirus**

Profile: default  
Virus/botnet: EICAR\_TEST\_FILE  
Virus ID: 2.172  
Reference: http://www.fortinet.com/vn?vn=EICAR\_TEST\_FILE  
Detection Type: cached  
Direction: incoming  
Quarantine skip: Quarantine-disabled  
Submitted to FortiSandbox: false  
Message: File is infected.

© Fortinet Inc. All Rights Reserved. 14

Logging is an important part of managing a secure network. When you enable logging, 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 what 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 files logging, a log entry is also created with the details including the message "Size limit is exceeded".

**DO NOT REPRINT**  
**© FORTINET**

## Forward Traffic Logs

**Log & Report > Forward Traffic**

| Date/Time           | Source    | Destination  | Application Name | Result                       | Policy ID       |
|---------------------|-----------|--------------|------------------|------------------------------|-----------------|
| 2023/09/13 00:50:20 | 10.0.1.10 | 10.200.1.254 | FTP              | ✓ Accept (1.41 kB / 1.73 kB) | 1 (Full_Access) |
| 2023/09/13 00:49:24 | 10.0.1.10 | 10.200.1.254 | tcp/63214        | ✗ Deny (Deny: UTM Blocked)   | 1 (Full_Access) |
| 2023/09/13 00:49:24 | 10.0.1.10 | 10.200.1.254 | tcp/21070        | ✗ Deny (Deny: UTM Blocked)   | 1 (Full_Access) |
| 2023/09/13 00:49:24 | 10.0.1.10 | 10.200.1.254 | tcp/35516        | ✗ Deny (Deny: UTM Blocked)   | 1 (Full_Access) |
| 2023/09/13 00:43:58 | 10.0.1.10 | 10.200.1.254 | HTTP             | ✗ Deny (Deny: UTM Blocked)   | 1 (Full_Access) |
| 2023/09/13 00:43:13 | 10.0.1.10 | 10.200.1.254 | HTTP             | ✗ Deny (Deny: UTM Blocked)   | 1 (Full_Access) |

**Forward traffic log entry**

**Security log details**

**Log Details**

**AntiVirus**

|                     |                                                                                |
|---------------------|--------------------------------------------------------------------------------|
| Agent               | Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:108.0) Gecko/20100101 Firefox/108.0 |
| Direction           | Incoming                                                                       |
| Detection Type      | cached                                                                         |
| Event Type          | Infected                                                                       |
| File Name           | eicar.com                                                                      |
| HTTP request method | GET                                                                            |
| Level               | Warning                                                                        |
| Profile             | default                                                                        |
| Quarantine Skip     | Quarantine-disabled                                                            |
| Reference           | http://www.fortinet.com/?v=vn=EICAR_TEST_FILE                                  |
| Referer URI         | http://10.200.1.254/test_av.html                                               |
| Sub Type            | virus                                                                          |
| Type                | utm                                                                            |
| 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                                             |

**FORTINET**  
Training Institute

© Fortinet Inc. All Rights Reserved.

15

You can also view log details on the **Forward Traffic** log page, where firewall policies record traffic activity. You'll 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

The screenshot shows the Fortinet Security Dashboard interface. At the top left, there's a 'Dashboard > Security' header. Below it, a 'Top Threats by Threat Level' card displays a threat named 'EICAR\_TEST\_FILE' categorized as 'Malware' with a 'Critical' threat level and a score of 750. A blue callout bubble points to this card with the text 'Drill down for further details'. To the right is a line chart showing network traffic over 24 hours, with a significant spike in bytes received at around 23:00. Below the chart is a table with columns for Source, Device, Threat Score, Bytes, and Sessions, showing data for an entry from '100.3.10'.

In the center, there's a 'Dashboard' card titled 'Advanced Threat Protection Statistics'. It features a green donut chart with the number '37' in the center, labeled 'Total'. A red arrow points to a small callout bubble above the chart stating 'Malicious: 1 files'. To the right of the chart is a legend for 'FortiGate Scanned Files' with categories: Clean (green), Malicious (red), Suspicious (blue), FortiGuard Outbreak Pct. (yellow), External Malware Block Lst. (orange), and EMS Threat Feed (grey). A blue callout bubble points to this card with the text 'Security widget'.

At the bottom left is the 'FORTINET Training Institute' logo. At the bottom right, there's a copyright notice: '© Fortinet Inc. All Rights Reserved.' and the page number '16'.

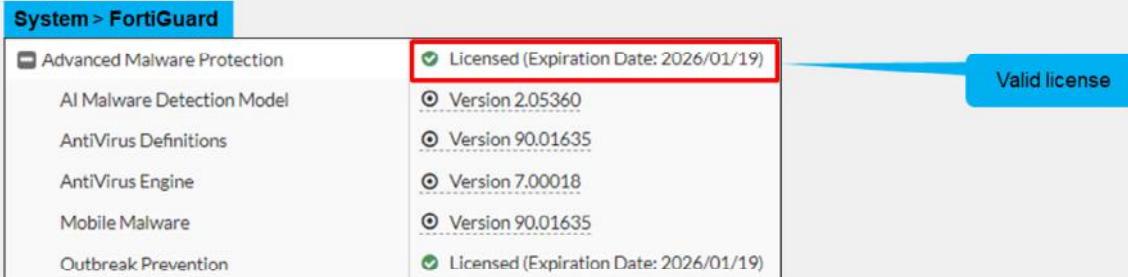
You can also use the **Security** dashboard to view relevant information regarding threats to your network. The security dashboard organizes information into source and destination and allows you to drill down with session logs details.

For the **Advanced Threat Protection Statistics**, you can add the corresponding widget on the dashboard for monitoring purposes.

**DO NOT REPRINT**  
**© FORTINET**

## Troubleshooting Common Antivirus Issues

- Verify FortiGuard antivirus license



The screenshot shows the FortiGuard interface under the 'System > FortiGuard' tab. On the left is a sidebar with options: Advanced Malware Protection, AI Malware Detection Model, AntiVirus Definitions, AntiVirus Engine, Mobile Malware, and Outbreak Prevention. On the right, there's a list of items with their status. Two items are highlighted with red boxes: 'Advanced Malware Protection' (status: Licensed (Expiration Date: 2026/01/19)) and 'Outbreak Prevention' (status: Licensed (Expiration Date: 2026/01/19)). A blue callout bubble points to the first item with the text 'Valid license'.

|                             |                                        |
|-----------------------------|----------------------------------------|
| Advanced Malware Protection | Licensed (Expiration Date: 2026/01/19) |
| AI Malware Detection Model  | Version 2.05360                        |
| AntiVirus Definitions       | Version 90.01635                       |
| AntiVirus Engine            | Version 7.00018                        |
| Mobile Malware              | Version 90.01635                       |
| Outbreak Prevention         | Licensed (Expiration Date: 2026/01/19) |

- 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 av-update`.

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 the FortiGate device.
- 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)

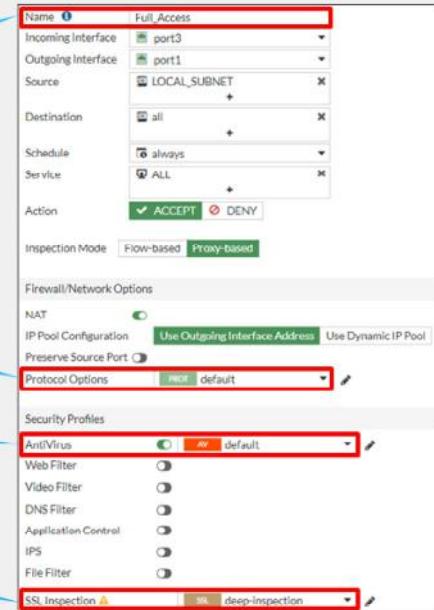
- Unable to catch viruses even with a valid contract?

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, and 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 right firewall policy.
- Make sure that the right protocol port is configured when the inspection mode is proxy-based.
- 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 versions 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

**FORTINET**  
Training Institute

© Fortinet Inc. All Rights Reserved.

19

To troubleshoot further common antivirus issues, you can check 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 type of inspection mode can be offloaded using CP processors?  
 A. Proxy-based  
 B. Flow-based

**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
- ✓ Log and 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



# FortiGate Administrator

## Web Filtering

 FortiOS 7.4

Last Modified: 15 November 2023

In this lesson, you will learn how to configure web filtering on FortiGate to control web traffic in your network.

**DO NOT REPRINT****© FORTINET**

## Objectives

- Select the correct inspection mode (flow or proxy) based on security needs
- 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
- Troubleshoot web filtering issues



© Fortinet Inc. All Rights Reserved. 2

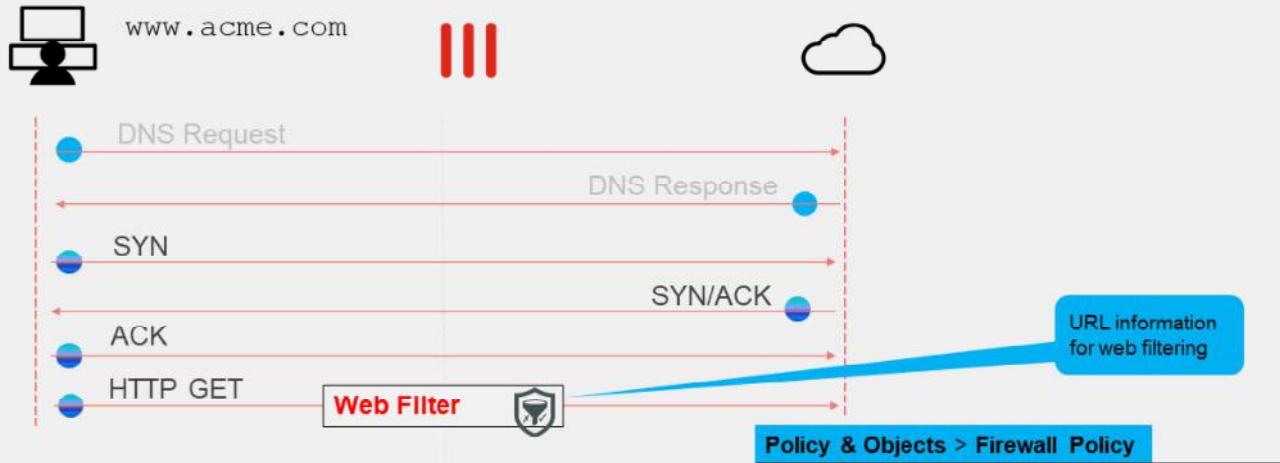
After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in web filtering configuration, you will be able to implement the web filter profile in an effective manner.

# DO NOT REPRINT

## © FORTINET

### When Does Web Filtering Activate?



- Two inspection modes defined per firewall policy

As shown in this HTTP filter process flow example, FortiGate looks for the `HTTP GET` request to collect URL information and perform web filtering.

In HTTP, the domain name and URL are separate parts. The domain name might look like the following in the header: `Host: www.acme.com`, and the URL might look like the following in the header: `/index.php?login=true`.

If you filter by domain, sometimes it blocks too much. For example, the blogs on `tumblr.com` are considered different content, because of all the different authors. In that case, you can be more specific, and block by the URL part, `tumblr.com/hacking`, for example.

In the default profile-based mode, FortiGate provides two inspection modes (flow-based and proxy-based) to perform web filtering.

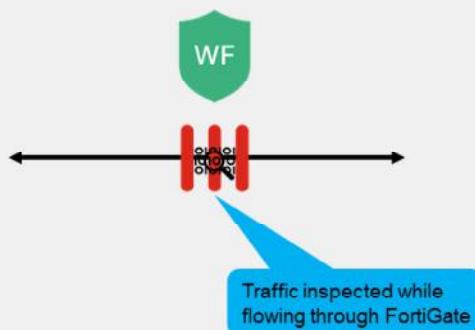
# DO NOT REPRINT

## © FORTINET

### Web Filtering Inspection Modes

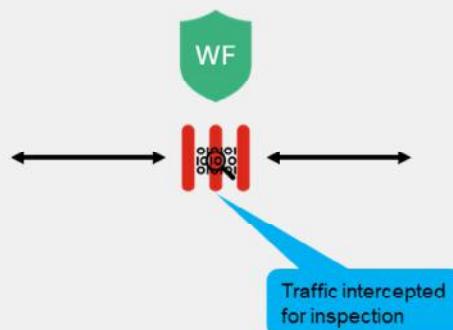
- Flow-based inspection

- Default inspection mode
- Requires fewer processing resources
- Faster scanning



- Proxy-based inspection

- More thorough inspection
- Provides additional options
- More resource intensive



You can configure web filtering in flow-based or proxy-based inspection mode.

Flow-based inspection mode examines the file as it passes through FortiGate. Packets are analyzed and forwarded as they are received. Original traffic is not altered. Therefore, advanced features that modify content, such as safe search enforcement, are not supported.

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.

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.

# DO NOT REPRINT

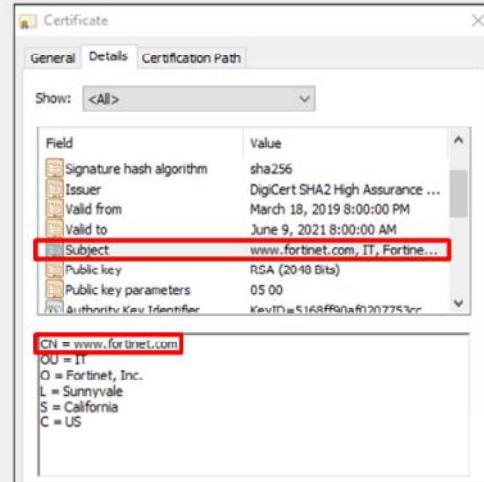
## © FORTINET

### SSL Certificate Inspection

- Uses the SNI extension from the Client Hello of the SSL handshake to obtain the FQDN

- If server name identification (SNI) is not present, FortiGate uses the CN field in the server certificate to obtain the FQDN

```
Secure Sockets Layer
TLSv1.2 Record Layer: Handshake Protocol: Client Hello
Content Type: Handshake (22)
Version: TLS 1.0 (0x0301)
Length: 512
Handshake Protocol: Client Hello
Handshake Type: Client Hello (1)
Length: 508
Version: TLS 1.2 (0x0303)
Cipher Suites Length: 36
Cipher Suites (18 suites)
Compression Methods (1 method)
Extension: server_name (len=21)
Type: server_name (0)
Length: 21
Server Name Indication extension
Server Name list length: 19
Server Name Type: host_name (0)
Server Name length: 16
Server Name: www.fortinet.com
```



For encrypted protocols, FortiGate requires additional inspection. When using SSL certificate inspection, 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 of the 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**

## 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** (Protecting SSL Server)

Inspection method: **SSL Certificate Inspection** (Full SSL Inspection)

CA certificate: Fortinet\_CA\_SSL (Download)

Blocked certificates: Allow, Block, View Blocked Certificates

Untrusted SSL certificates: Allow, Block, View Trusted CAs List

Server certificate SNI check: **Enable**, Strict, Disable

**Protocol Port Mapping**

Inspect all ports:

HTTPS: 443,10443

**Select Multiple Clients Connecting to Multiple Servers**

**Select SSL Certificate Inspection**

Action if the SNI does not match the CN or SAN fields (only in proxy-based inspection)

You can specify more than one port number (separated by comma)

**FORTINET.**  
Training Institute

© Fortinet Inc. All Rights Reserved. 6

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**.

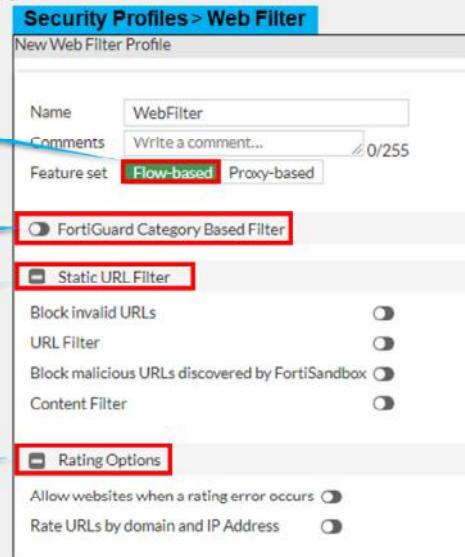
When the **Server certificate SNI check** configuration is **Enable**, FortiGate uses the domain in the **CN** field instead of the domain in the **SNI** field if the domain in the **SNI** field does not match any of the domains listed in the **CN** and **SAN** fields. With **Strict**, FortiGate closes 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 and configure **Static URL Filter** if needed
- Enable and configure **Rating Options** if needed



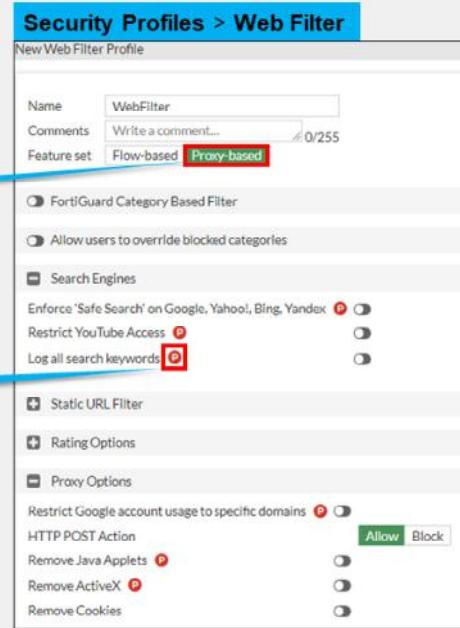
Now, you will look at the web filter profile.

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.

DO NOT REPRINT  
© FORTINET

## Configure Web Filter Profiles—Proxy Based

- Apply a web filter profile to a flow-based firewall policy



**FORTINET**  
Training Institute

© Fortinet Inc. All Rights Reserved.

8

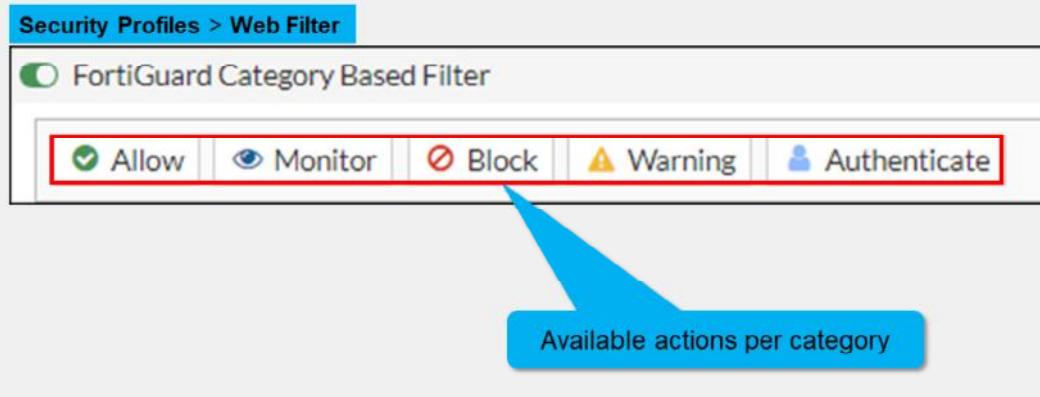
In the example shown on this slide, the security profile is configured to use a proxy-based feature set. It provides features specific to proxy-based configuration.

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.

**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. In the default profile-based mode, 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—Monitor

- Monitor action allows and logs web sites accesses

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.' The 'Proxy-based' feature set is selected. In the 'FortiGuard Category Based Filter' section, the 'Monitor' action is highlighted with a red box. Below it, a table lists a single entry: 'Education' with 'Action' set to 'Monitor'. A blue callout points to this row with the text 'Set action to monitor'. At the bottom, a table titled 'Category Usage Quotas' shows a single row for 'Education' with a total quota of '1024 MB'. A red box highlights the 'Category Usage Quotas' link. A blue callout points to this link with the text 'Quota configuration available in proxy-based mode'. The Fortinet Training Institute logo is in the bottom left, and copyright information is in the bottom right.

Besides the **Allow** and **Block** actions, which respectively permit and block access to the sites, the **Monitor** action allows access to the sites in the category and logs it at the same time. In proxy-based mode, you can also configure a usage quota.

DO NOT REPRINT  
© FORTINET

## Web Filter FortiGuard Category Action—Quotas

- Applies to **Monitor**, and also **Warning** and **Authenticate** actions
- Quotas available only in proxy-based mode

The screenshot shows the FortiGate UI for managing Web Filter Category Action—Quotas. On the left, under 'Security Profiles > Web Filter', there is a table of category usage quotas. A red arrow points from the '+ Create New' button in this table to the 'Create New' dialog on the right. The 'Create New' dialog has two tabs: 'Time' (selected) and 'Traffic'. It shows a 'Category' dropdown set to 'Education', a 'Quota Type' dropdown set to 'Time', and a 'Total quota' field set to '0 hour(s) 5 minute(s) 0 second(s)'. A blue callout bubble points to this dialog with the text 'Daily quotas based on time or traffic amount'. On the right side of the main window, there is another 'New/Edit Quota' dialog for 'Education' with 'Quota Type' set to 'Traffic' and 'Total quota' set to '1024 MB'.

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. Besides the **Monitor** action, you can also apply quotas to the **Warning** and **Authenticate** actions.

DO NOT REPRINT  
© FORTINET

## Web Filter FortiGuard Category Action—Warning

- Informs the user before proceeding

The screenshot shows the 'Security Profiles > Web Filter' interface. A new profile named 'Warning' is being created. The 'Feature set' is set to 'Proxy-based'. Under 'FortiGuard Category Based Filter', the 'Warning' action is selected. In the 'Edit Filter' section, the 'Warning Interval' is set to 5 hours. A blue callout bubble points to the 'Warning' action with the text 'Set action to warning'. A red callout bubble points to the 'Warning Interval' input field with the text 'Customizable warning interval'.

**FORTINET**  
Training Institute

© Fortinet Inc. All Rights Reserved.

12

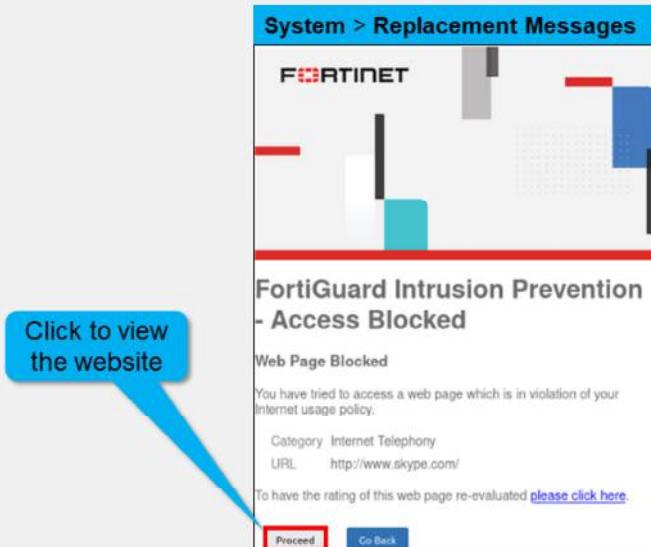
The **Warning** action informs users that the requested website is not allowed by the internet policies. However, the action gives the user the option to proceed to the requested website, or return to the previous website.

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.

DO NOT REPRINT  
© FORTINET

## Web Filter FortiGuard Category Action—Warning (Contd)

- Displays a customizable warning message



You can customize the warning replacement message. By default, it provides information of the URL and its corresponding category. With this information, the user can click **Proceed** to override the internet usage policy.

# DO NOT REPRINT

## © FORTINET

### Web Filter FortiGuard Category Action—Authenticate

- To configure the **Authenticate** action:
  - Define **Users** and **Group**
  - Set action to **Authenticate**
  - Select **User Group**

The screenshot shows the 'Security Profiles > Web Filter' interface. A 'FortiGuard Category Based Filter' is selected. In the 'Action' column, the 'Authenticate' button is highlighted with a red box and a callout 'Set action to authenticate'. Below the table, an 'Edit Filter' dialog is open, showing a 'Warning Interval' of 0 hour(s), 5 minute(s), and 0 second(s). The 'Selected User Groups' dropdown is also highlighted with a red box and a callout 'User groups allowed to authenticate'. A third callout 'Customizable authenticate interval' points to the 'Warning Interval' input fields.

**FORTINET**  
Training Institute

© Fortinet Inc. All Rights Reserved. 14

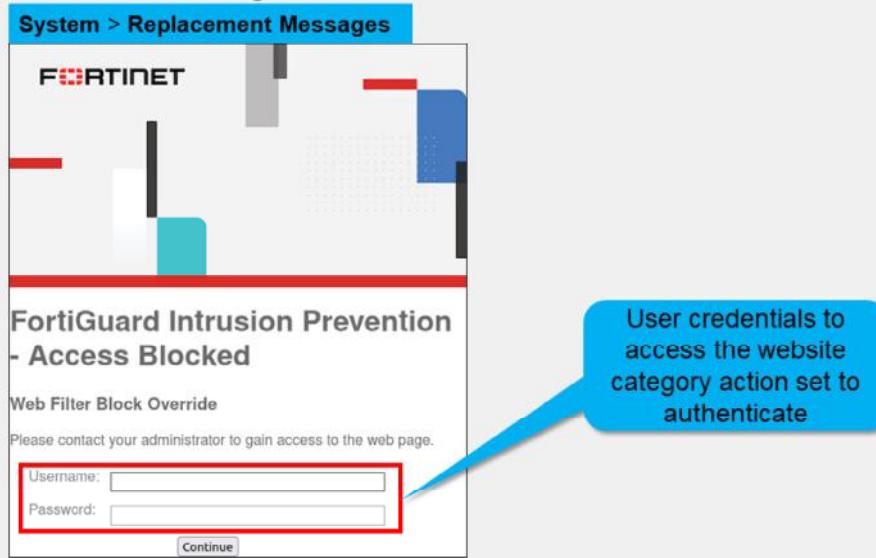
The **Authenticate** action blocks the requested websites, unless the user enters a successful username and password. FortiGate supports local and remote authentication using LDAP, RADIUS, and so on for web filtering authentication. Choosing this action prompts you to define user groups that are allowed 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.

DO NOT REPRINT  
© FORTINET

## Web Filter FortiGuard Category Action—Authenticate (Contd)

- User credentials requested in message



**FORTINET**  
Training Institute

© Fortinet Inc. All Rights Reserved.

15

Like the **Warning** action, FortiGate displays a replacement message to proceed and a second one asks for the user credentials. You can customize these replacement messages in **System > Replacement Messages**.

**DO NOT REPRINT**  
**© FORTINET**

## Web Rating Override

- Changes a website category, not the category action

| Security Profiles > Web Rating Overrides |                            |                                     |                                                   |
|------------------------------------------|----------------------------|-------------------------------------|---------------------------------------------------|
| <a href="#">Create New</a>               | <a href="#">Edit</a>       | <a href="#">Delete</a>              | Status                                            |
| <a href="#">Custom Categories</a>        |                            | Search                              | <input type="checkbox"/> Show original categories |
| URL                                      | Original Category          | Status                              | Comments                                          |
| <a href="#">Malicious Websites</a> 1     | Search Engines and Portals | Enable                              |                                                   |
| www.bing.com                             | Search Engines and Portals | <input checked="" type="checkbox"/> |                                                   |

[Edit Web Rating Override](#)

URL: www.bing.com   [Lookup rating](#)

|              |                             |
|--------------|-----------------------------|
| Category     | General Interest - Business |
| Sub-Category | Search Engines and Portals  |

Comments: Write a comment... /255

Override to:

|              |                    |
|--------------|--------------------|
| Category     | Security Risk      |
| Sub-Category | Malicious Websites |

Information on the original category

Adds information and the column **Original Category**

Configuration of the override category

**FORTINET**  
 Training Institute

© Fortinet Inc. All Rights Reserved. 16

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 |

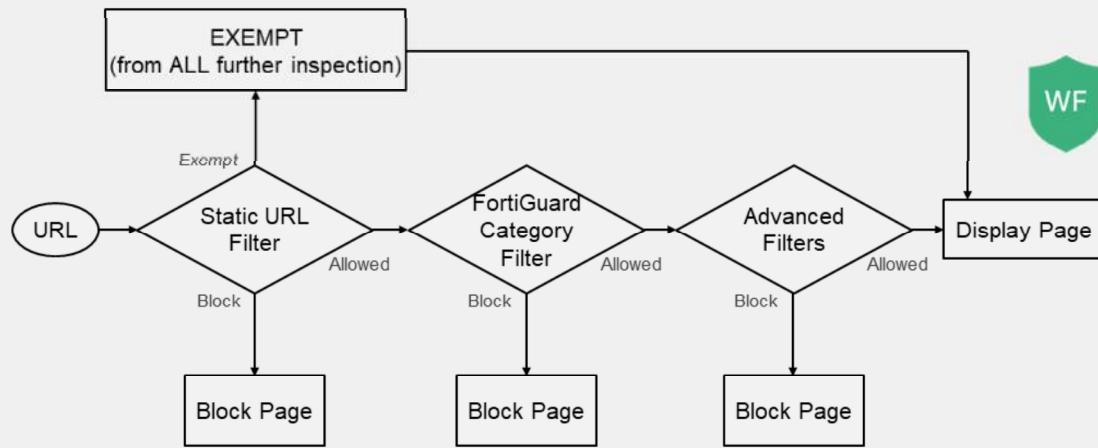
Static URL filtering is another web filter feature, which provides more granularity. Configured URLs in the URL filter are checked from top to bottom against the visited websites. If FortiGate finds a match, it applies the configured action. You can configure one of four actions:

- 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**

## HTTP 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

## 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

**System > FortiGuard**

Filtering

|                                                                                                                                                             |                                     |                   |    |         |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------|-------------------|----|---------|
| Web Filter cache                                                                                                                                            | <input checked="" type="checkbox"/> | Clear cache after | 60 | Minutes |
| Email Filter cache                                                                                                                                          | <input checked="" type="checkbox"/> | Clear cache after | 30 | Minutes |
| FortiGuard filtering services                                                                                                                               | HTTPS 8888                          |                   |    |         |
| <input checked="" type="checkbox"/> Test Connectivity<br><input checked="" type="checkbox"/> Web Filtering<br><input checked="" type="checkbox"/> Anti-Spam |                                     |                   |    |         |
| Request re-evaluation of a URL's category                                                                                                                   |                                     |                   |    |         |

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. Also, memory lookup is much quicker than packets travelling on the internet.

**DO NOT REPRINT**  
© FORTINET

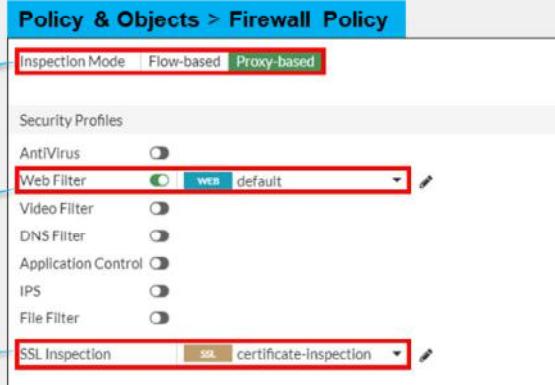
## Troubleshooting Web Filtering Issues

- 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, quota info

The screenshot shows the 'Log & Report > Security Events > Web Filter' section. A specific log entry is selected, highlighted by a red box. The log details are as follows:

| 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     |

Annotations with blue arrows point to specific fields:

- 'Click to download the raw log data' points to the download icon at the top of the log table.
- 'Information on action and policy ID' points to the 'Action' and 'Policy ID' fields in the expanded 'Details' window.
- 'Name of web filter profile' points to the 'Profile' field in the expanded 'Details' window.
- 'Name of web filter profile and replacement message used' points to the 'Category' and 'Message' fields in the expanded 'Details' window.

**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

**FOURINET**  
Training Institute

© Fortinet Inc. All Rights Reserved. 22

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 at the top of the GUI. The file downloaded is a plain text file in a syslog format.

**DO NOT REPRINT**

**© FORTINET**

## Knowledge Check

1. Which action in URL filtering bypasses all security profiles?

- A. Exempt
- B. Allow

2. Which statement about proxy-based web filtering is true?

- A. It requires fewer resources than flow-based.
- B. It transparently analyzes the TCP flow of the traffic.

**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



© Fortinet Inc. All Rights Reserved. 24

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

By mastering the objectives covered in this lesson, you learned how to configure web filtering on FortiGate to control web traffic in your network.

**DO NOT REPRINT****© FORTINET**

# FortiGate Administrator

## Intrusion Prevention and Application Control

A small red square icon containing a white square with a diagonal line, followed by the text "FortiOS 7.4".

Last Modified: 15 November 2023

In this lesson, you will learn how to use FortiGate to protect your network against intrusions and how to monitor and control network applications that may use standard or non-standard protocols and ports—beyond simply blocking or allowing a protocol, port number, or IP address.

**DO NOT REPRINT****© FORTINET**

## Objectives

- Configure an intrusion prevention system (IPS) sensor
- Troubleshoot IPS high-CPU usage
- Configure application control in profile mode
- Monitor application control events
- Troubleshoot traffic matching with application control profile issues



© Fortinet Inc. All Rights Reserved.

2

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

By demonstrating competence in intrusion prevention systems (IPS), you will be able to implement an effective IPS solution to protect your network from intrusion.

By demonstrating competence in configuring and monitoring the application control features that are available on FortiOS, you will be able to use and maintain application control in profile mode in an effective manner.

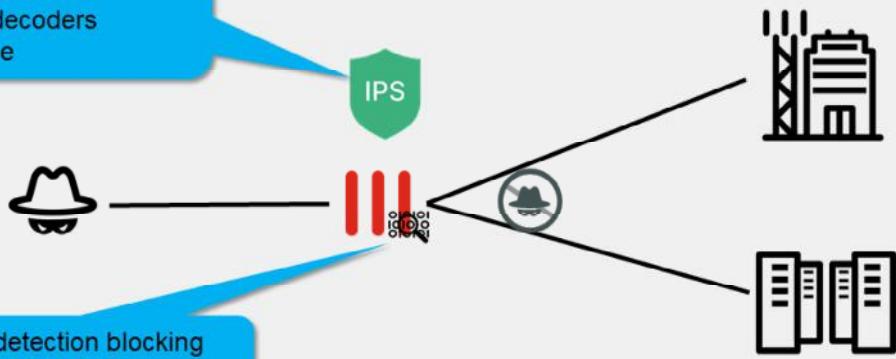
# DO NOT REPRINT

## © FORTINET

### IPS

IPS components include:

- IPS signature databases
- Protocol decoders
- IPS engine



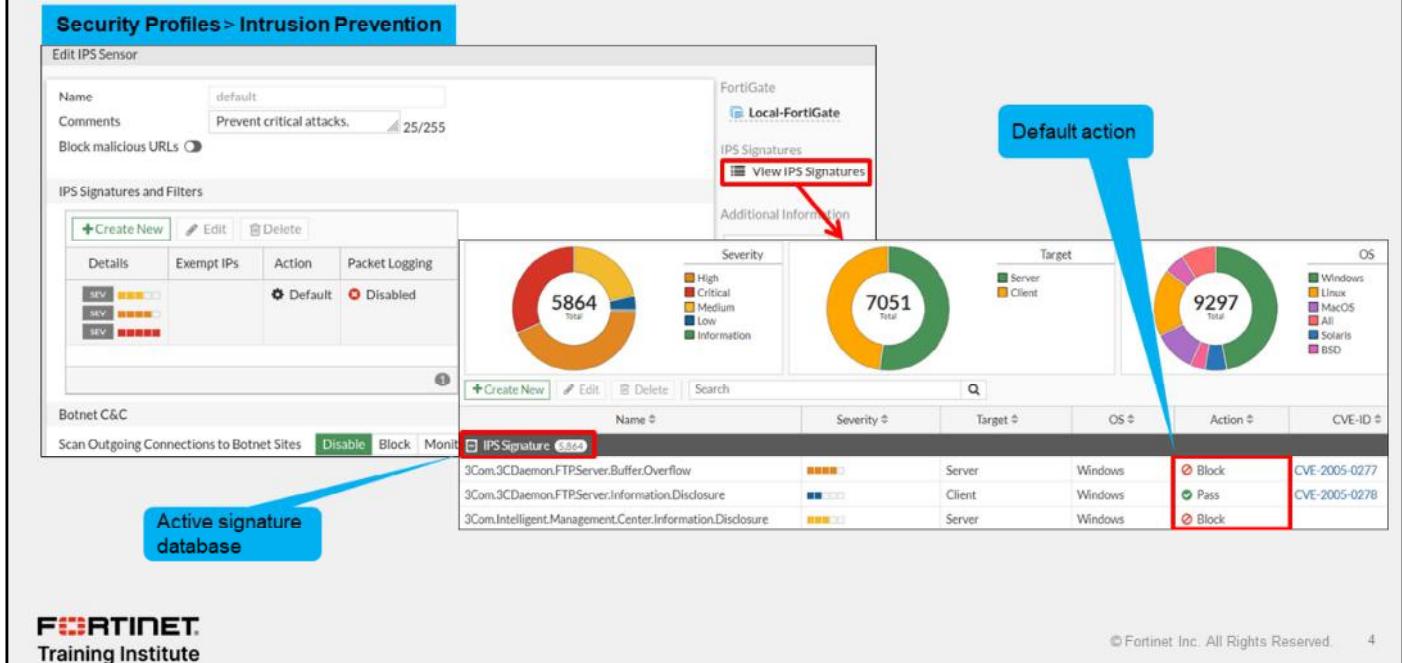
IPS on FortiGate uses signature databases to detect known attacks, like exploits. Rate-based IPS signatures also allows you to detect anomalies, which are unusual behaviors in the network, such as higher-than-usual CPU use or network traffic. Rate-based IPS signatures are part of behavioral analysis, 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-previously-seen attack.

Unlike proxy-based scans, IPS works in flow-based inspection and is not limited to IANA standard ports. Protocol decoders parse each packet according to the protocol specifications. 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.

Another important IPS component is the 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



The screenshot shows the FortiGate IPS Signature Management interface. At the top left, it says "Security Profiles > Intrusion Prevention". Below that is the "Edit IPS Sensor" section with fields for Name (default), Comments (Prevent critical attacks. 25/255), and Block malicious URLs (checkbox). To the right is a summary dashboard with three donut charts: "IPS Signatures" (5864 total), "Target" (7051 total), and "OS" (9297 total). A blue callout labeled "Default action" points to the "Action" column in the signature list table, which includes "Block", "Pass", and "Block" options for each row. Another blue callout labeled "Active signature database" points to the "IPS Signature" button in the toolbar. The bottom right corner of the interface shows copyright information: "© Fortinet Inc. All Rights Reserved. 4".

After FortiGate downloads a FortiGuard IPS package, new signatures 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 IPS Sensors. On the left, the 'New IPS Sensor' configuration page is shown with a 'Create New' button highlighted by a red box. On the right, two overlapping windows show how to add signatures: one window shows individual signatures being selected, and the other shows a 'Filter' section where multiple OS types like Server, Client, Mac, and Windows are selected.

Security Profiles > Intrusion Prevention

New IPS Sensor

|                                                                                                                                                   |                                                          |
|---------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------|
| Name                                                                                                                                              | IPS profile                                              |
| Comments                                                                                                                                          | Write a comment <span style="float: right;">0/255</span> |
| Block malicious URLs <input checked="" type="checkbox"/>                                                                                          |                                                          |
| IPS Signatures and Filters                                                                                                                        |                                                          |
| <span style="color: green; font-weight: bold;">+ Create New</span> <span style="color: blue;">Edit</span> <span style="color: red;">Delete</span> |                                                          |
| Details                                                                                                                                           | Exempt IPs                                               |
| Action                                                                                                                                            | Packet Logging                                           |

No results

Add Signatures

|                   |                                                                                                                |
|-------------------|----------------------------------------------------------------------------------------------------------------|
| Type              | <input checked="" type="radio"/> Signature                                                                     |
| Action            | <input checked="" type="radio"/> Default                                                                       |
| Packet logging    | <input checked="" type="radio"/> Enable <input type="radio"/> Disable                                          |
| Status            | <input checked="" type="radio"/> Enable <input type="radio"/> Disable <input checked="" type="radio"/> Default |
| Retained settings | <input checked="" type="radio"/> Default <input type="radio"/> Specify                                         |
| Exempt IPs        | <input type="radio"/> Edit IP Exemptions                                                                       |

**IPS Signature (4)**

| Name                                                      | Severity | Target | OS      | Action                                 | CVE-ID        |
|-----------------------------------------------------------|----------|--------|---------|----------------------------------------|---------------|
| 3Com.3CDaemon.FTP.Server.Buffer.Overflow                  | High     | Server | Windows | <input checked="" type="radio"/> Block | CVE-2005-0277 |
| 3Com.3CDaemon.FTP.Server.InformationDisclosure            | Medium   | Client | Windows | <input checked="" type="radio"/> Pass  | CVE-2005-0278 |
| 3Com.Intelligent.Management.Center.Information Disclosure | High     | Server | Windows | <input checked="" type="radio"/> Block |               |

Add Signatures

|                |                                                                                                                                                                                                        |
|----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Type           | <input checked="" type="radio"/> Signature                                                                                                                                                             |
| Action         | <input checked="" type="radio"/> Default                                                                                                                                                               |
| Packet logging | <input checked="" type="radio"/> Enable <input type="radio"/> Disable                                                                                                                                  |
| Status         | <input checked="" type="radio"/> Enable <input type="radio"/> Disable <input checked="" type="radio"/> Default                                                                                         |
| Filter         | <input checked="" type="radio"/> Server <input checked="" type="radio"/> Client <input checked="" type="radio"/> Mac <input checked="" type="radio"/> HTTP <input checked="" type="radio"/> OS Windows |

**IPS Signature (444-37)**

| Name                                                          | Severity | Target | OS     | Action                                 | CVE-ID        |
|---------------------------------------------------------------|----------|--------|--------|----------------------------------------|---------------|
| Adobe.Acrobat.And Reader.TrueTypeFont.Parsing.Buffer.Overflow | High     | Server | Client | <input checked="" type="radio"/> Block | CVE-2012-0774 |
| Adobe.Acrobat.BMPColors.Parsing.Memory.Corruption             | High     | Server | MacOS  | <input checked="" type="radio"/> Block | CVE-2011-4373 |

**FORTINET**  
Training Institute

© Fortinet Inc. All Rights Reserved.

5

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.

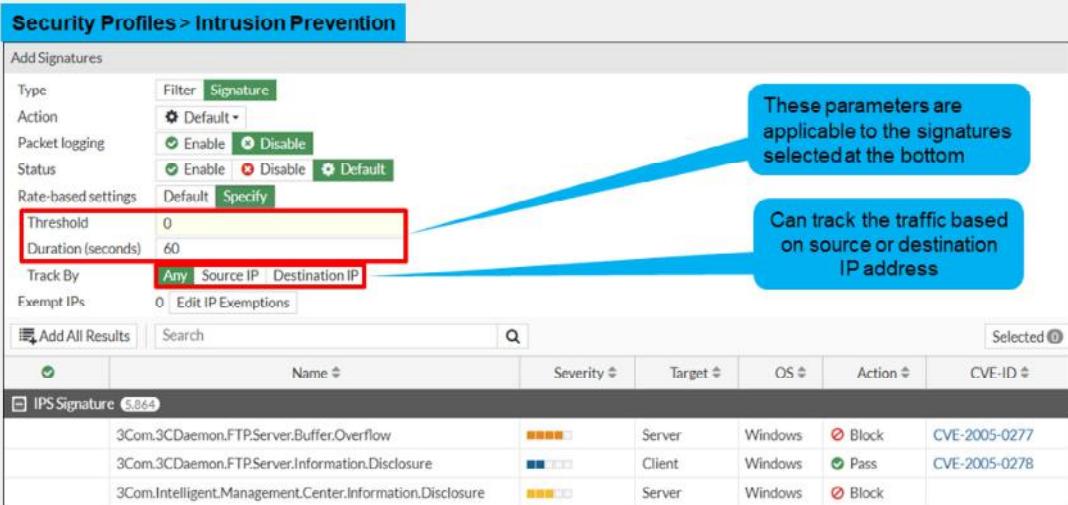
FortiGate 7.4 Administrator Study Guide

241

**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' interface. A red box highlights the 'Threshold' field set to 0 and the 'Duration (seconds)' field set to 60. A callout bubble states: 'These parameters are applicable to the signatures selected at the bottom'. Another callout bubble states: 'Can track the traffic based on source or destination IP address'. The 'Track By' dropdown is set to 'Any'. The table below lists three IPS signatures:

| IPS Signature                                             | 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  |               |

**FORTINET.**  
Training Institute

© Fortinet Inc. All Rights Reserved. 6

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<br><br>TGT Server<br>SEV<br>SEV<br>OS Windows | 0          | Monitor  Disabled | Default  Disabled |

**FORTINET**  
Training Institute

© Fortinet Inc. All Rights Reserved.

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.

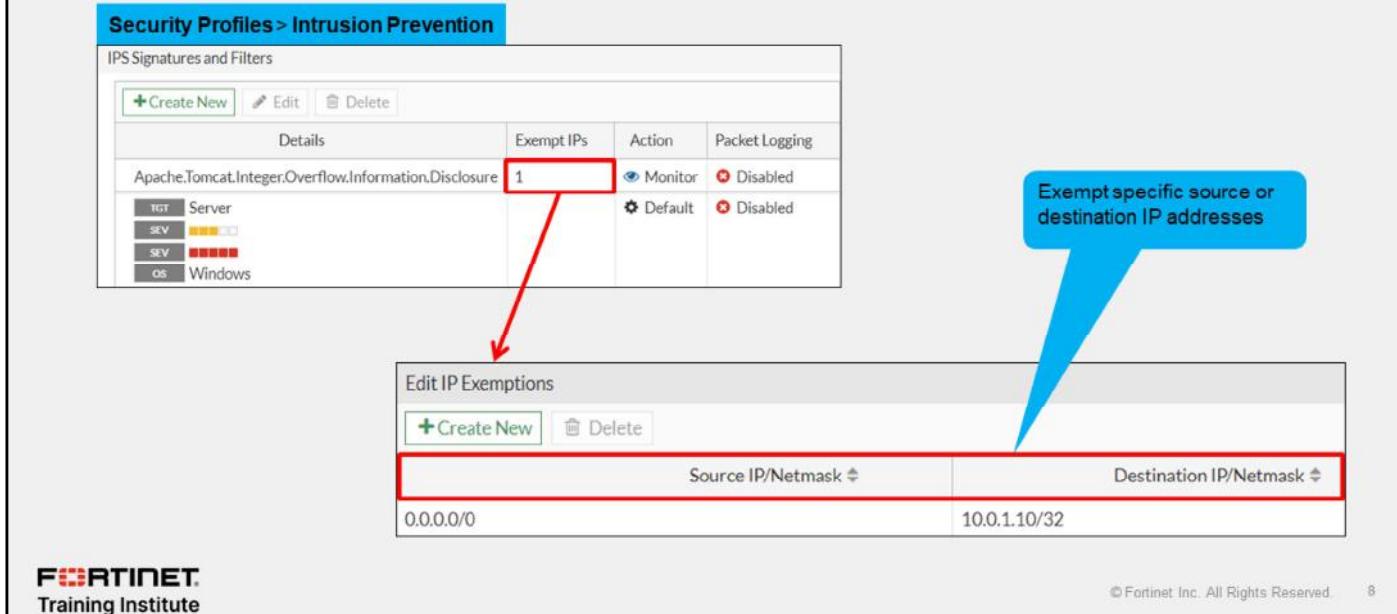
So, position the most likely matching filters, or signatures, at the top of the list. Avoid making too many filters, because this increases evaluations and CPU usage. Also, avoid making very large signature groups in each filter, which increase RAM use.

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 two windows from the FortiGate management interface. The top window is titled "Security Profiles > Intrusion Prevention" and displays a table of IPS signatures. One row is selected, showing details for "Apache.Tomcat.Integer.Overflow.Information.Disclosure". The "Exempt IPs" column contains the number "1", which is highlighted with a red box and connected by a red arrow to the "Edit IP Exemptions" window below. The "Edit IP Exemptions" window has a table with two columns: "Source IP/Netmask" and "Destination IP/Netmask". The "Source IP/Netmask" field contains "0.0.0.0/0" and the "Destination IP/Netmask" field contains "10.0.1.10/32", both of which are also highlighted with red boxes. A blue callout bubble on the right side of the "Edit IP Exemptions" window states: "Exempt specific source or destination IP addresses".

| Details                                                                                                                                       | Exempt IPs | Action                                                                    | Packet Logging                                                              |
|-----------------------------------------------------------------------------------------------------------------------------------------------|------------|---------------------------------------------------------------------------|-----------------------------------------------------------------------------|
| Apache.Tomcat.Integer.Overflow.Information.Disclosure                                                                                         | 1          | <input checked="" type="radio"/> Monitor<br><input type="radio"/> Default | <input checked="" type="radio"/> Disabled<br><input type="radio"/> Disabled |
| TGT Server<br>SEV <span style="background-color: yellow;">■■■■■</span><br>SEV <span style="background-color: red;">■■■■■</span><br>OS Windows |            |                                                                           |                                                                             |

| Edit IP Exemptions |                        |
|--------------------|------------------------|
| Source IP/Netmask  | Destination IP/Netmask |
| 0.0.0.0/0          | 10.0.1.10/32           |

**FORTINET**  
Training Institute

© Fortinet Inc. All Rights Reserved.

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

The screenshot shows the FortiGate configuration interface for 'Security Profiles > Intrusion Prevention'. On the left, there are filters for 'Type' (set to 'Signature'), 'Action' (set to 'Packet logging'), 'Status' (set to 'Enabled'), and 'Filter' (set to 'Default'). The main area displays a table of 'IPS Signature' entries. A callout box highlights the 'Action' column, which includes options: Allow (selected), Monitor, Block, Reset, Default, and Quarantine. Another callout box highlights the 'Packet logging' action, stating 'Copies the packets for later analysis'. A third callout box highlights the 'Default' action, stating 'Action to take when a signature is triggered'. The table lists four signatures:

| IPS Signature                                          | Severity | 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**  
Training Institute

© Fortinet Inc. All Rights Reserved.

9

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.

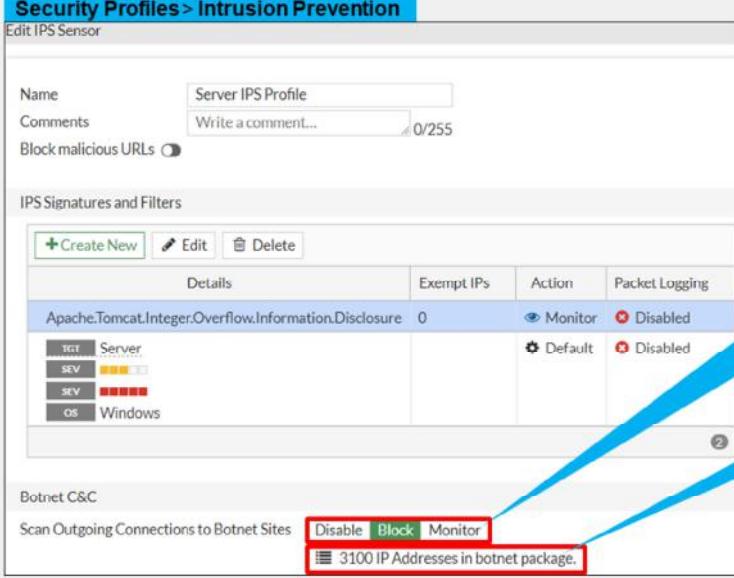
**Quarantine** allows you to quarantine the attacker's IP address for a set duration. You can set the quarantine duration to any number of days, hours, or minutes.

If you enable **Packet logging**, FortiGate saves a copy of the packet that matches the signature.

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 'Security Profiles > Intrusion Prevention' interface for an 'Edit IPS Sensor' named 'Server IPS Profile'. In the 'IPS Signatures and Filters' section, a signature for 'Apache.Tomcat.Integer.Overflow.Information.Disclosure' is listed with an 'Action' set to 'Monitor' and 'Disabled'. Below this, under 'Botnet C&C', there is a button labeled 'Scan Outgoing Connections to Botnet Sites' with three options: 'Disable', 'Block' (highlighted in red), 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 'Scan Outgoing Connections to Botnet Sites' button with the text 'Botnet database from FortiGuard (included with a valid IPS license)'.

**Set action to Block or Monitor**

**Botnet database from FortiGuard (included with a valid IPS license)**

© Fortinet Inc. All Rights Reserved. 10

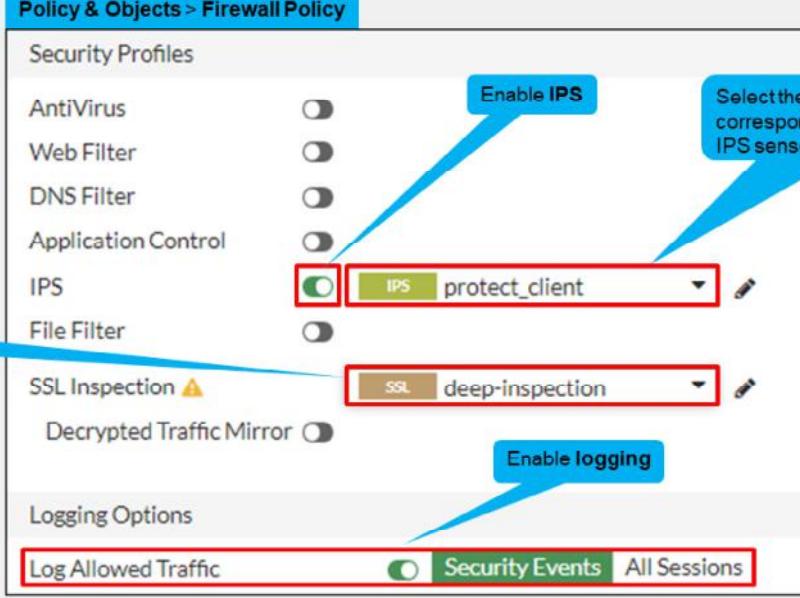
For consolidated botnet protection, you can enable botnet scanning on the IPS profile that you apply the firewall policy on.

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 (green switch). A callout points to this with the text 'Enable IPS'. Another callout points to the dropdown menu next to 'protect\_client' with the text 'Select the IPS security profile corresponding to the configured IPS sensors'. To the left, a callout points to the 'SSL Inspection' section with the text 'Set deep-inspection for encrypted protocols'. In the 'Logging Options' section, the 'Log Allowed Traffic' method is set to 'Security Events All Sessions', indicated by a red box around the 'All Sessions' button. A callout points to this with the text 'Enable logging'.

**Policy & Objects > Firewall Policy**

**Security Profiles**

- AntiVirus
- Web Filter
- DNS Filter
- Application Control
- IPS**  **IPS protect\_client**
- File Filter

**SSL Inspection**  **SSL deep-inspection**

**Decrypted Traffic Mirror**

**Logging Options**

**Log Allowed Traffic**  **Security Events** **All Sessions**

**© Fortinet Inc. All Rights Reserved. 11**

To apply an IPS sensor, you must enable **IPS** and then select the sensor in a firewall policy.

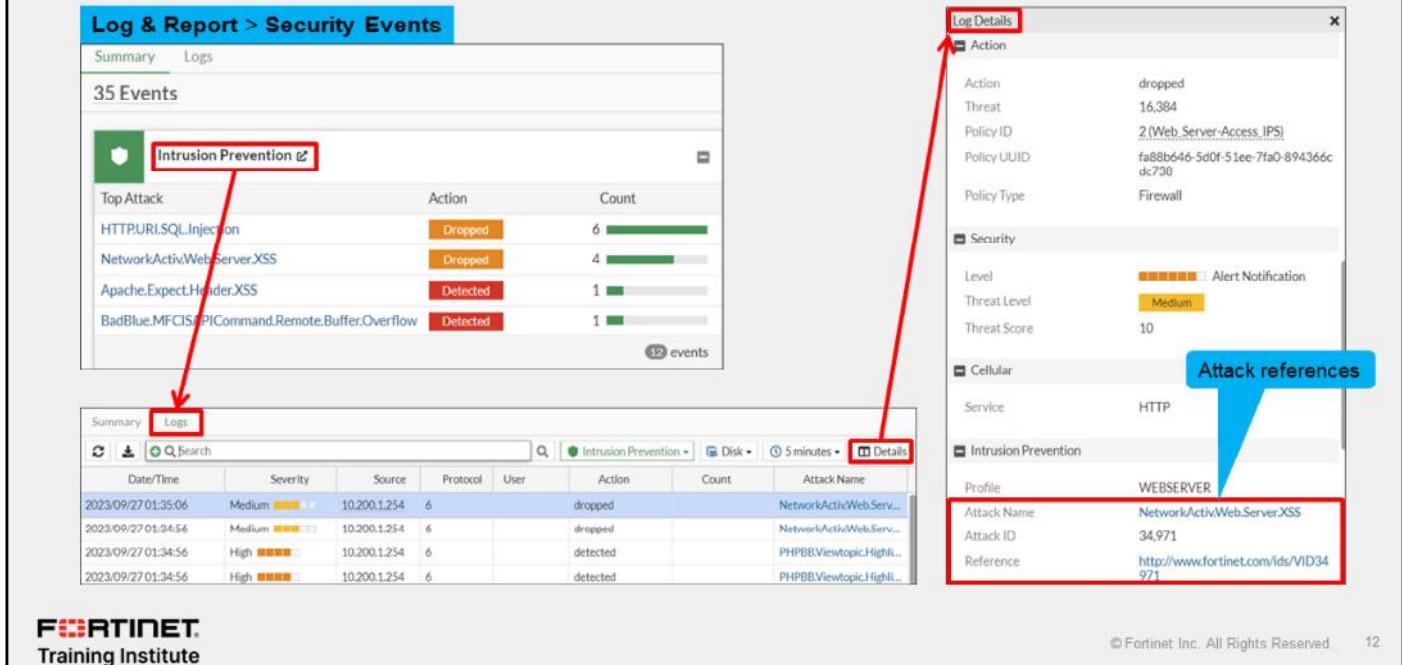
Certain vulnerabilities apply only to encrypted connections and FortiGate can't identify the threat reliably if it can't parse the payload. For this reason, you must use an SSL inspection profile, usually **deep-inspection**, if you want to get the maximum benefit from your IPS features.

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**

## 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. A red arrow points from the 'Intrusion Prevention' link in the chart to the 'Logs' tab below. Another red arrow points from the 'Details' button in the log table to a detailed log entry. To the right, a modal window titled 'Log Details' provides specific information about a single event, including policy details, security levels, and attack references. A blue callout bubble labeled 'Attack references' points to the 'Reference' field in the modal.

**Intrusion Prevention**

**Logs**

**Details**

**Log Details**

Action: dropped  
Threat: 16,384  
Policy ID: 2 (Web\_Server-Access\_IPS)  
Policy UUID: fa88bbe46-5d0f-51ee-7fa0-894366cd730  
Policy Type: Firewall

**Security**

Level: Alert Notification  
Threat Level: Medium  
Threat Score: 10

**Cellular**

Service: HTTP

**Intrusion Prevention**

Profile: WEB SERVER

Attack Name: NetworkActiv/Web.Server.XSS  
Attack ID: 34,971  
Reference: http://www.fortinet.com/ids/VID34971

**Attack references**

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 = 1949, engine count = 1 (+1)
0 - pid:1989:1989 cfg:1 master:0 run:1
1 - pid:2195:2195 cfg:0 master:1 run:1

pid: 2195 index:1 master
version: 07004000FLEN07600-00007.0004
up time: 0 days 4 hours 35 minutes
init time: 0 seconds
socket size: 256(MB)
database: ipsetdb appdb isdb fmwpdb
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, 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.

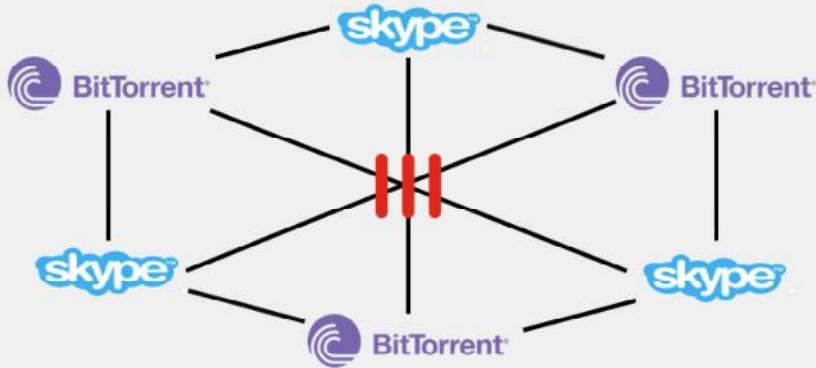
If the CPU use remains high after enabling IPS bypass mode, it usually indicates a problem in the IPS engine, which you must report to Fortinet support. You can disable the IPS engine completely using option 2. If you want to restore IPS inspection of traffic after you finish troubleshooting, use option 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**

## 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



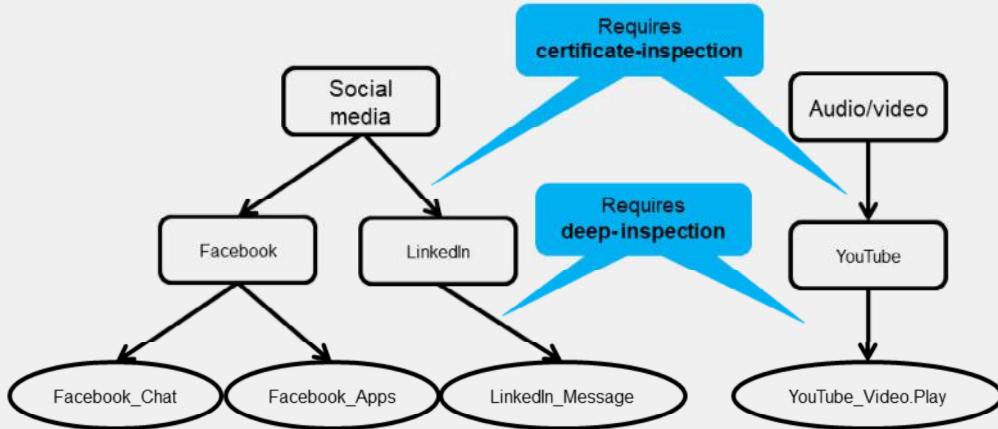
As previously mentioned, the IPS engine is also responsible for application control. You can configure application control in proxy-based and flow-based firewall policies. However, because application control uses the IPS engine, which uses flow-based inspection, the inspection is always flow-based.

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

## 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 Facebook **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 Facebook applications while allowing users to collaborate using Facebook chat.

**DO NOT REPRINT**  
**© FORTINET**

## List of Application Signatures

The screenshot shows the FortiGate Security Profiles > Application Control interface. At the top, it displays a message about 113 Cloud Applications requiring deep inspection. Below this are fields for Name and Comments, and a Categories section with a dropdown set to 'Mixed - All Categories'. A sidebar lists various application categories with their counts. On the right, there's a license information box and a 'View Application Signatures' button, which is highlighted with a red box and a blue arrow pointing to it from the text 'Filter option'. A callout bubble labeled 'Filter option' also points to the search bar in the signature list window. The main window shows three donut charts for Category (Social Media), Technology (Browser-Based), and Risk (Low). Below these is a table titled 'Application Signature' with columns for Name, Category, Technology, Popularity, and Risk. A search bar at the top of the table is also highlighted with a red box and a blue arrow. A callout bubble labeled 'Active signature database' points to the table header.

**Security Profiles > Application Control**

New Application Sensor

113 Cloud Applications require deep inspection.  
0 policies are using this profile.

Name:   
Comments:  0/255

Categories:

- Mixed - All Categories
- Business (157, △ 6)
- Cloud/IT (68, △ 1)
- Collaboration (271, △ 16)
- Email (77, △ 12)
- Game (86)
- General Interest (238, △ 12)
- Mobile (3)
- Network Service (333)
- P2P (56)
- Remote Access (99)
- Storage/Backup (160, △ 19)
- Update (49)
- Video/Audio (155, △ 17)
- Web Client (25)
- Unknown Applications

Firmware & General Updates License  
Licensed (Expiration Date: 2026/01/19)  
Application Control Signatures Package  
Version 25.00619

**View Application Signatures**

**Filter option**

**Active signature database**

**View Application Signatures**

Category: Social Media

Technology: Browser-Based

Risk: Low

| Name                   | Category     | Technology    | Popularity | Risk |
|------------------------|--------------|---------------|------------|------|
| LinkedIn               | Social Media | Browser-Based | ★★★★★      | Low  |
| LinkedIn_File.Download | Social Media | Browser-Based | ★★★☆☆      | Low  |
| LinkedIn_File.Upload   | Social Media | Browser-Based | ★★★☆☆      | Low  |
| LinkedIn_Login         | Social Media | Browser-Based | ★★○○○      | Low  |
| LinkedIn_Message       | Social Media | Browser-Based | ★★★○○      | Low  |
| LinkedIn_Post          | Social Media | Browser-Based | ★★★☆☆      | Low  |

**FOORTINET**  
Training Institute

© Fortinet Inc. All Rights Reserved. 16

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**

## Configuring an Application Control in Profile Mode

The screenshot shows the 'Edit Application Sensor' interface for a 'default' profile. At the top, it says '113 Cloud Applications require deep inspection. 0 policies are using this profile.' The 'Categories' section includes a 'Mixed' dropdown set to 'All Categories'. Below is a list of categories with their respective counts:

- Business (157)
- Email (77)
- Mobile (3)
- P2P (56)
- Social Media (118)
- Video/Audio (155)
- Unknown Applications** (highlighted with a red box)
- Cloud/IT (68)
- Game (86)
- Network Service (333)
- Proxy (184)
- Storage/Backup (160)
- VoIP (24)
- Collaboration (271)** (highlighted with a red box)
- General Interest (238)
- Operational Technology
- Remote Access (99)
- Update (49)
- WebClient (25)

Callouts provide additional context for specific elements:

- 'Applies an action to all categories at once' points to the 'All Categories' dropdown.
- 'Applies an action to one category' points to the 'Collaboration' category.
- 'The number to the right of the cloud symbol indicates the number of cloud applications in the category' points to the counts in the 'Cloud/IT' and 'Collaboration' rows.
- 'Creates specific actions for a single application or group of applications' points to the 'Unknown Applications' category.
- 'Matches traffic to unidentified applications' points to the 'Cloud/IT' category.

**FORTINET**  
Training Institute

© Fortinet Inc. All Rights Reserved. 17

In profile-based mode, you configure application control profiles on the **Application Control** page.

The application control profile consists of three different types of filters:

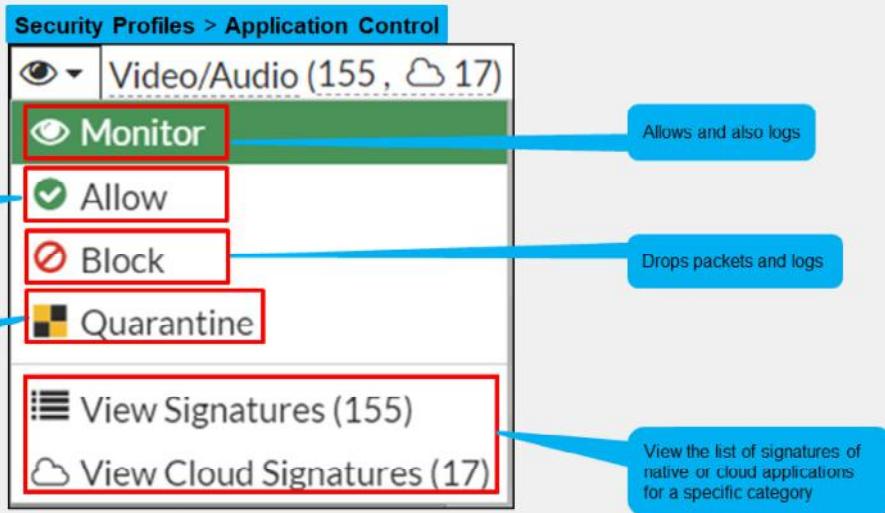
- **Categories:** Groups applications based on similarity. For example, all applications that are capable of providing remote access are grouped in the **Remote Access** category. The **Unknown Applications** category refers to traffic that can't be matched to any application control signature. You can configure an action per category or to all of them.
- **Application overrides:** Provides the flexibility to control specific signatures and applications.
- **Filter overrides:** Useful when a predefined category does not meet your requirements and you want to modify the action for all applications based on criteria that are not available in categories. Besides category, the additional criteria are behavior, protocol, vendor, popularity, risk, or the technology used by the applications.

At the top of the **Application Control** profile page, you will see a summary of how many cloud applications require deep inspection. Cloud applications that use SSL encryption cannot be scanned without a deep inspection profile. FortiGate must decrypt the traffic in order to perform inspection and control application traffic.

# DO NOT REPRINT

## © FORTINET

### Filters Actions



**FORTINET**  
Training Institute

© Fortinet Inc. All Rights Reserved.

18

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 an attacker IP address 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 FortiGate 7.4 Application Control configuration interface. On the left, under 'Network Protocol Enforcement', there is a table with columns: Port, Enforce protocols, and Violation Action. A red box highlights the 'Create New' button. A callout bubble says: 'Allows blocking or monitoring of known services on unknown ports'. Below it is an 'Application and Filter Overrides' section with a similar table and a 'Create New' button. A callout bubble says: 'Enforces applications to run on its default port'. Under 'Options', three checkboxes are highlighted with red boxes: 'Block applications detected on non-default ports', 'Allow and Log DNS Traffic', and 'Replacement Messages for HTTP-based Applications'. A callout bubble says: 'Applies only to HTTP/HTTPS applications'. On the right, a modal window titled 'New Default Network Service' shows a list of services: DNS, FTP, HTTP, HTTPS, IMAP, NNTP, POP3, SMTP, SNMP, SSH, and TELNET. The 'HTTP' service is selected. A callout bubble says: 'List of known services'.

The **Application Sensor** provides also additional options.

**Network Protocol enforcement** 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.

The 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.
- 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.

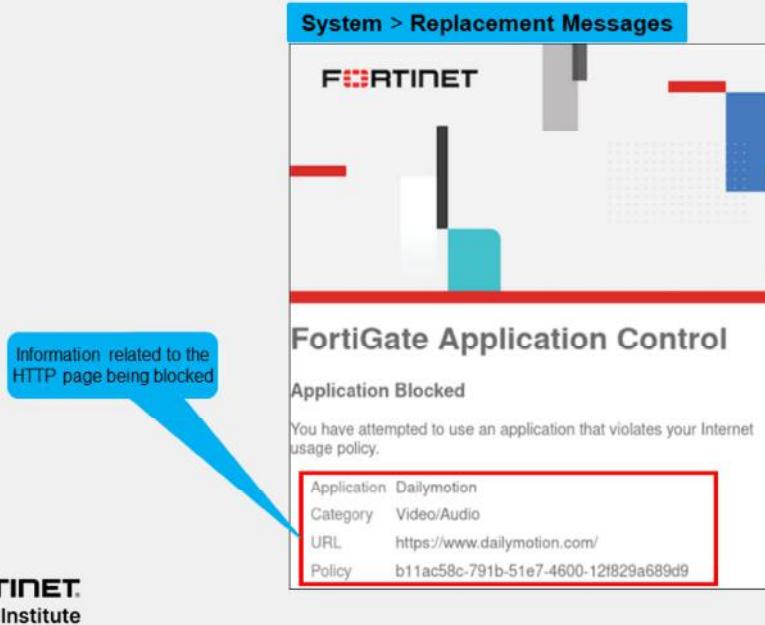
With the **Block applications detected on non-default ports** option, FortiGate compares the ports used by the application with the ones defined in FortiGuard application signatures. The traffic is blocked if it does not match.

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 pages in profile mode



**FORTINET**  
Training Institute

© Fortinet Inc. All Rights Reserved. 20

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's category (in this case, Video/Audio)
- URL that was specifically blocked (in this case, the index page of [www.dailymotion.com](https://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)
- 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 main sections: 'Categories' and 'Application and Filter Overrides'. The 'Categories' section contains a list of application categories with counts: Business (157), Email (77), Mobile (3), P2P (56), Social Media (118), Video/Audio (155), Unknown Applications, Cloud/IT (68), Game (86), Network Service (333), Proxy (194), Storage/Backup (160), VoIP (24), Collaboration (271), General Interest (238), Operational Technology, Remote Access (99), Update (49), and Web Client (25). The 'Application and Filter Overrides' section has a table with columns: Priority, Details, Type, and Action. A message at the bottom says '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've 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 list of application types. Three specific categories are highlighted with red boxes and circled numbers: 'Game (86)' (circled 3), 'Video/Audio (155, △ 17)' (circled 3), and 'Excessive-Bandwidth' (circled 2). A callout bubble for 'Game' says 'Application Overrides set for Battle Net and Dailymotion applications'. Another callout bubble for 'Video/Audio' says 'Filter Overrides set for applications that consume excessive bandwidth'. A third callout bubble at the bottom right says 'The Game and Video/Audio categories are set to Block and all other categories are set to Monitor'. The 'Application and Filter Overrides' table shows two rows: row 1 for 'Battle.Net' and 'Dailymotion' with 'Type: Application' and 'Action: Monitor'; row 2 for 'Excessive-Bandwidth' with 'Type: Filter' and 'Action: Block'. The Fortinet Training Institute logo is in the bottom left, and the copyright notice '© Fortinet Inc. All Rights Reserved. 22' is in 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 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 the application control profile scan is done, FortiGate 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 filter override entry is moved above the application override entry.

3

1

2

© Fortinet Inc. All Rights Reserved. 23

**Security Profiles > Application Control**

Name: default  
Comments: Monitor all applications. 25/255

Categories: Mixed - All Categories

- Business (157, △ 6)
- Email (77, △ 12)
- Mobile (3)
- P2P (56)
- Social Media (118, △ 30)
- Video/Audio (155, △ 17) ③
- Cloud/IT (68, △ 1)
- Game (86) ②
- Network Service (333)
- Proxy (184)
- Storage/Backup (160, △ 19)
- VoIP (24)
- Collaboration (271, △ 16)
- General Interest (238, △ 12)
- Operational Technology
- Remote Access (99)
- Update (49)
- Web Client (25)

Network Protocol Enforcement

Application and Filter Overrides:

| Priority | Details             | Type        | Action                                   |
|----------|---------------------|-------------|------------------------------------------|
| 1        | Excessive-Bandwidth | Filter      | Block <span style="color: red;">①</span> |
| 2        | Dailymotion         | Application | Monitor                                  |
|          | Battle.Net          |             |                                          |

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** under 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 in Profile Mode

- You must apply the **Application Control** profile on a firewall policy to scan the passing traffic

The screenshot shows the 'Policy & Objects > Firewall Policy' interface. Under 'Security Profiles', the 'Application Control' section is highlighted with a red box. It shows 'Application Control' is enabled (green switch), set to 'APP' mode, and the profile is 'default'. A callout bubble says 'Enable Application Control and select the profile'. Another callout bubble says 'Enable logging' pointing to the 'Log Allowed Traffic' checkbox. The 'SSL Inspection' section is also highlighted with a red box. It shows 'SSL Inspection' is enabled (green switch), set to 'sst' mode, and the profile is 'deep-inspection'. A callout bubble says 'Use deep-inspection profile to scan encrypted traffic'.

Policy & Objects > Firewall Policy

Security Profiles

AntiVirus

Web Filter

DNS Filter

Application Control  APP default

IPS

File Filter

SSL Inspection  sst deep-inspection

Decrypted Traffic Mirror

Logging Options

Log Allowed Traffic  Security Events All Sessions

Enable Application Control and select the profile

Enable logging

Use deep-inspection profile to scan encrypted traffic

**FORTINET**  
Training Institute

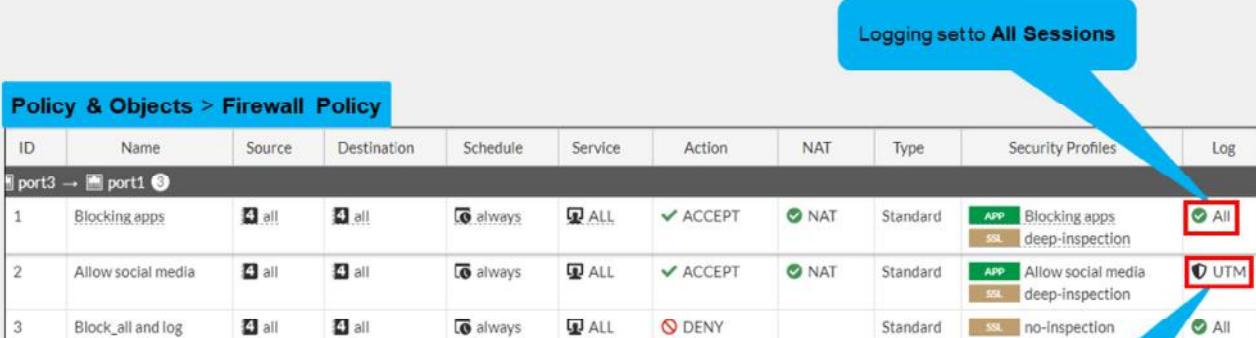
© Fortinet Inc. All Rights Reserved. 24

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.

**DO NOT REPRINT**  
**© FORTINET**

## Logging Application Control Events

- Example of NGFW profile-based mode firewall policies



The screenshot shows a 'Policy & Objects > Firewall Policy' table. A blue callout bubble points to the 'Log' column header with the text 'Logging set to All Sessions'. Another blue callout bubble points to the 'Log' column for the third policy entry with the text 'Logging set to Security Events'. The table has columns: ID, Name, Source, Destination, Schedule, Service, Action, NAT, Type, Security Profiles, and Log.

| ID | Name               | Source | Destination | Schedule | Service | Action   | NAT   | Type     | Security Profiles                             | Log                                     |
|----|--------------------|--------|-------------|----------|---------|----------|-------|----------|-----------------------------------------------|-----------------------------------------|
| 1  | Blocking apps      | all    | all         | always   | ALL     | ✓ ACCEPT | ✓ NAT | Standard | APP Blocking apps<br>SSL deep-inspection      | <input checked="" type="checkbox"/> All |
| 2  | Allow social media | all    | all         | always   | ALL     | ✓ ACCEPT | ✓ NAT | Standard | APP Allow social media<br>SSL deep-inspection | <input checked="" type="checkbox"/> UTM |
| 3  | Block_all and log  | all    | all         | always   | ALL     | ✗ DENY   |       | Standard | SSL no-inspection                             | <input checked="" type="checkbox"/> All |

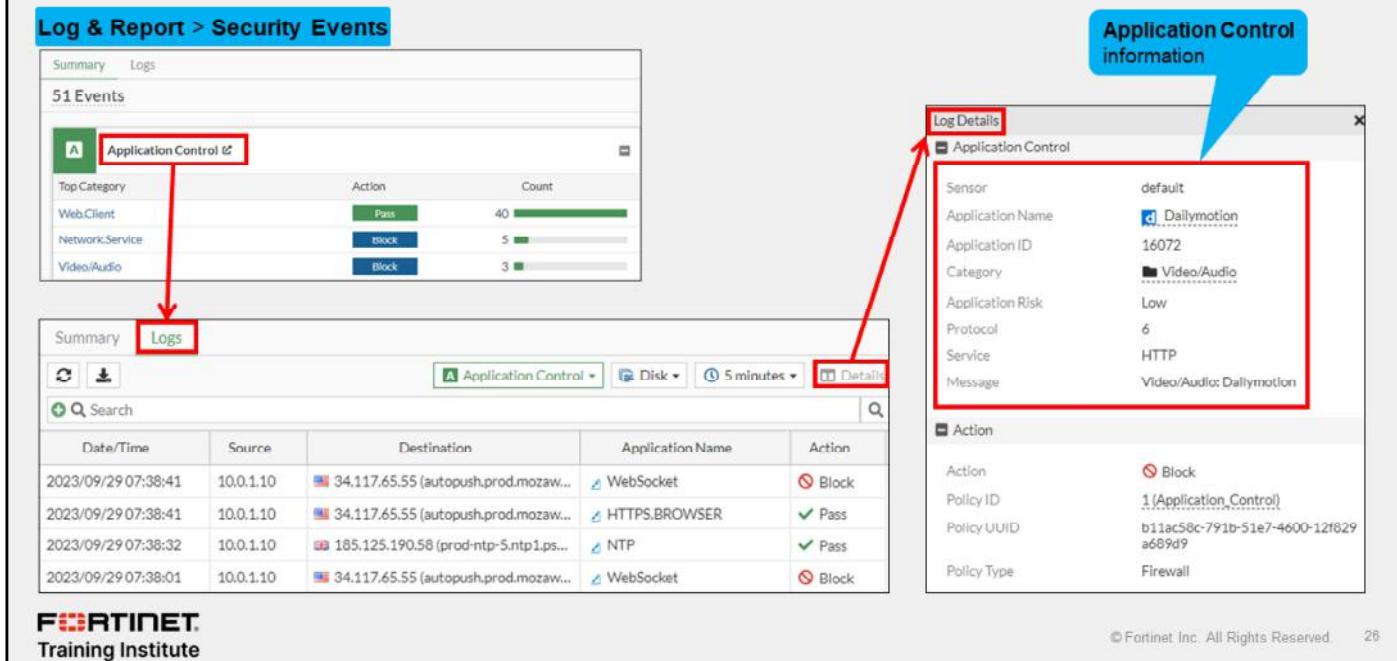
**FORTINET**  
Training Institute

© Fortinet Inc. All Rights Reserved. 25

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 left, under 'Log & Report > Security Events', there's a summary of 51 events. A red box highlights the 'Application Control' link in the summary table. Below it, a table shows 'Top Category' with 'Web.Client' having 40 Pass actions, 5 Block actions, and 3 Block actions. A red box highlights the 'Logs' tab in the main pane. To the right, a detailed log entry for 'Dailymotion' is shown in a modal window titled 'Log Details'. The modal has a blue speech bubble labeled 'Application Control information' pointing to it. The log details include: Sensor (default), Application Name (Dailymotion), Application ID (16072), Category (Video/Audio), Application Risk (Low), Protocol (HTTP), Service (Video/Audio: Dailymotion), and Action (Block). The log message also includes Policy ID (1 (Application\_Control)), Policy UUID (b11ac58c-791b-51e7-4600-12f829a689d9), and Policy Type (Firewall).

FortiGate logs all application control events on the **Log & Report > Security Events** page. You can view the logs by clicking on **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 pane, 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 apply according configuration modifications

The screenshot shows the FortiView Applications interface. On the left, a list of applications is shown with their bytes sent and received over a 24-hour period. A red arrow points from the 'Bytes Received' column in this list to a detailed view of the Dailymotion session on the right. A blue callout box labeled 'Information on traffic matching a specific application' points to this detailed view. Another blue callout box labeled 'Traffic matching an application over a defined time period' points to the main list of applications.

| Application     | Category         | Risk   | Bytes     | Sessions |
|-----------------|------------------|--------|-----------|----------|
| Dailymotion     | Video/Audio      | Low    | 569.12 kB | 13       |
| GoogleAnalytics | Business         | Medium | 262.55 kB | 3        |
| Facebook        | Social.Media     | Medium | 262.55 kB | 3        |
| Yahoo.Services  | General.Interest | Medium | 237.03 kB | 1        |
| Salesforce      | Business         | Medium | 204.34 kB | 1        |
| HTTPS.BROWSER   | WebClient        | Medium | 151.52 kB | 1        |
| UNO             | NetworkService   | Medium | 125.81 kB | 1        |

**Detailed View of Dailymotion Session:**

| Source    | Destination | Policies |
|-----------|-------------|----------|
| 10.0.1.10 | 10.0.1.11   | 0        |

Bytes Sent: 569.12 kB | Bytes Received: 13 kB

© Fortinet Inc. All Rights Reserved. 27

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 also in the **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 action allows traffic and logs the activity?  
 A. Allow  
 B. Monitor
  
2. Which statement about application control is true?  
 A. Application control uses the IPS engine to scan traffic for application patterns.  
 B. Application control is unable to scan P2P architecture traffic.
  
3. 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**

## Review

- ✓ Configure an intrusion prevention system (IPS) sensor
- ✓ Troubleshoot IPS high-CPU usage
- ✓ Configure application control in profile mode
- ✓ 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 gained the skills and knowledge you need 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



# FortiGate Administrator

## SSL VPN

 FortiOS 7.4

Last Modified: 15 November, 2023

In this lesson, you will learn how to configure and use SSL VPNs. SSL VPNs are an easy way to give remote users access to your private network.

**DO NOT REPRINT**

**© FORTINET**

## Objectives

- Configure SSL VPN portals
- Configure tunnel mode SSL VPN
- Monitor SSL VPN-connected users
- Troubleshoot common SSL VPN issues

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

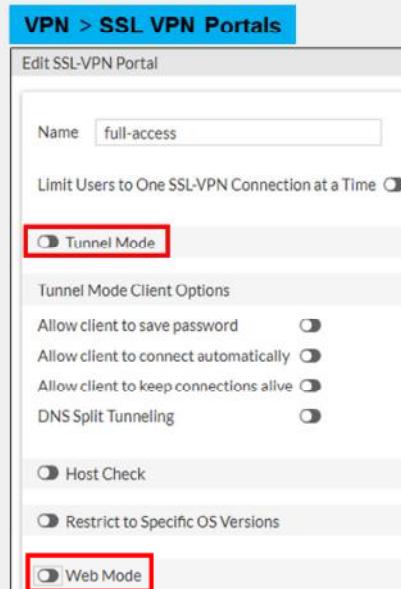
By demonstrating competence in understanding the different ways FortiGate allows SSL VPN connections, you will be able to better design the configuration and architecture of your SSL VPN. You will also be able to avoid, identify, and solve common issues and misconfigurations.

**DO NOT REPRINT****© FORTINET**

## SSL VPN Deployment Modes

- Tunnel mode
  - Accessed through a FortiClient
  - Requires a virtual adapter on the client host
  
- Web mode
  - Requires only a web browser
  - Supports a limited number of protocols:
    - FTP, HTTP/HTTPS, RDP, SMB/CIFS, SSH, Telnet, VNC, and Ping

```
config vpn ssl web portal
 edit <portal-name>
 set tunnel-mode [enable|disable]
 set web-mode [enable|disable]
 end
```



**FORTINET**  
Training Institute

© Fortinet Inc. All Rights Reserved. 3

There are two modes you can use to access an SSL VPN. Both can build an SSL VPN connection, but they don't support the same features.

Which should you choose?

It depends on which applications you need to send through the VPN, the technical knowledge of your users, and whether or not you have administrative permissions on their computers.

Tunnel mode supports the most protocols, but requires the installation of a VPN client, or more specifically, a virtual network adapter. To tunnel traffic using the virtual adapter, you must use the FortiClient remote access feature or FortiClient VPN-only client.

Web mode requires only a web browser, but supports a limited number of protocols. You will only learn SSL VPN tunnel mode in this lesson.

**DO NOT REPRINT****© FORTINET**

## Tunnel Mode

- Connect to FortiGate through FortiClient
  - Tunnel is up only while the SSL VPN client is connected
  - FortiClient adds a virtual network adapter called `fortissl`
- FortiGate establishes the tunnel
  - Assigns a virtual IP address to the client from a pool of reserved addresses
  - All traffic is encapsulated with SSL/TLS
  - Any IP network application on the client can send traffic through the tunnel
  - Requires the installation of a VPN client

<http://www.forticlient.com/>



# FortiClient

Next Generation Endpoint Protection

**FORTINET**  
Training Institute

© Fortinet Inc. All Rights Reserved.

4

Tunnel mode is the second option FortiGate provides to access resources within an SSL VPN.

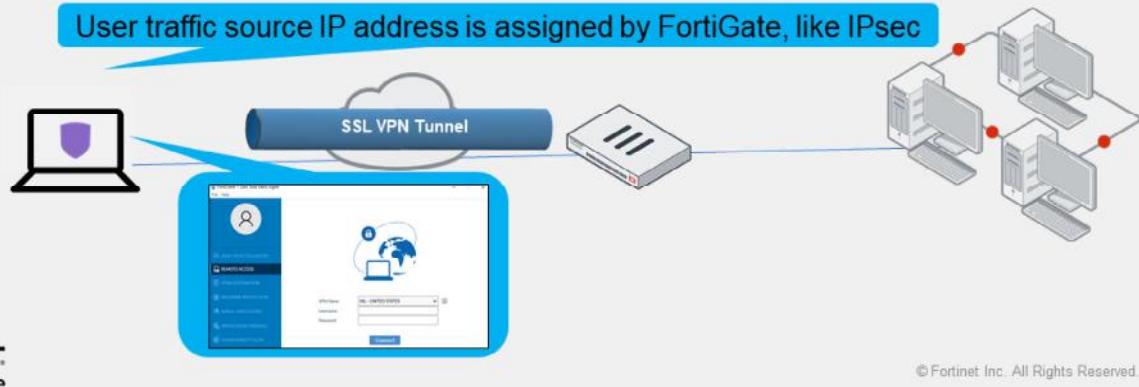
Tunnel mode requires FortiClient to connect to FortiGate. FortiClient adds a virtual network adapter identified as `fortissl` to the user's PC. This virtual adapter dynamically receives an IP address from FortiGate each time FortiGate establishes a new VPN connection. Inside the tunnel, all traffic is SSL/TLS encapsulated.

The main advantage of tunnel mode is that after the VPN is established, any IP network application running on the client can send traffic through the tunnel. The tunnel mode requires the installation of a VPN software client, which requires administrative privileges.

**DO NOT REPRINT****© FORTINET**

## Tunnel Mode (Contd)

1. Remote users connect to the SSL VPN gateway through the SSL VPN client
2. Users authenticate
3. The virtual adapter creates the tunnel
4. Users access resources through an encrypted tunnel (SSL/TLS)



**FORTINET**  
Training Institute

© Fortinet Inc. All Rights Reserved.

5

How does tunnel mode work?

1. Users connect to FortiGate through FortiClient.
2. Users provide credentials to successfully authenticate.
3. FortiGate establishes the tunnel and assigns an IP address to the client's virtual network adapter (fortissl1). This is the client's source IP address for the duration of the connection.
4. Then, users can access services and network resources through the encrypted tunnel.

FortiClient encrypts all traffic from the remote computer and sends it over the SSL VPN tunnel. FortiGate receives the encrypted traffic, de-encapsulates the IP packets, and forwards them to the private network as if the traffic originated from inside the network.

**DO NOT REPRINT****© FORTINET**

## Tunnel Mode—FortiGate as Client

- Connect to server FortiGate device as SSL VPN client
  - Use *SSL VPN Tunnel* interface type
  - Devices connected to client FortiGate can access the resources behind server FortiGate
- Tunnel establishes between two FortiGate devices
  - Hub-and-spoke topology
  - Client FortiGate dynamically adds route to remote subnets
  - Assigns a virtual IP address to the client FortiGate from a pool of reserved addresses



© Fortinet Inc. All Rights Reserved.

6

You can configure FortiGate as an SSL VPN client, using an *SSL-VPN Tunnel* interface type. When an SSL VPN client connection is established, the client dynamically adds a route to the subnets that the SSL VPN server returns. You can define policies to allow users who are behind the client to be tunneled through SSL VPN to destinations on the SSL VPN server.

**DO NOT REPRINT****© FORTINET**

## Tunnel Mode—FortiGate as Client (Contd)

- Advantages:

- Any IP network application on the user machines connected to client FortiGate device can send traffic through the tunnel
- Useful to avoid issues caused by intermediate devices, such as:
  - ESP packets being blocked
  - UDP ports 500 or 4500 being blocked
  - Fragments being dropped, causing IKE negotiation that uses large certificates to fail if the peer does not support IKE fragmentation

- Disadvantages:

- Requires correct CA certificate on SSL VPN server FortiGate
- SSL VPN client FortiGate user uses PSK and PKI client certificate to authenticate



© Fortinet Inc. All Rights Reserved.

7

This setup provides IP-level connectivity in tunnel mode and allows you to configure hub-and-spoke topologies with FortiGate devices as both the SSL VPN hub and spokes. This can be useful to avoid issues caused by intermediate devices, such as:

- ESP packets being blocked
- UDP ports 500 or 4500 being blocked
- Fragments being dropped, causing IKE negotiation that uses large certificates to fail if the peer does not support IKE fragmentation

If the client specified destination is *all*, a default route is effectively dynamically created on the SSL VPN client, and the new default route is added to the existing default route in the form of ECMP. You can modify the route distance or priority according to your requirements. To prevent a default route being learned on the SSL VPN client, define a specific destination on the SSL VPN server. Split tunneling is used so that only the destination addresses defined in the server firewall policies are routed to the server, and all other traffic is connected directly to the internet.

This configuration requires you to install the correct CA certificate because the SSL VPN client FortiGate/user uses PSK and a PKI client certificate to authenticate. You must install the correct CA certificate on the FortiGate devices to verify the certificate chain to the root CA that signed the certificate.

# DO NOT REPRINT

## © FORTINET

### Tunnel Mode—FortiGate as Client (Contd)

1. SSL VPN client FortiGate initiates connection to SSL VPN server FortiGate
2. SSL VPN client FortiGate uses PSK(local user account) and PKI client to authenticate
3. The virtual *SSL VPN tunnel* interface creates the tunnel
  - IP address assigned from SSL VPN server FortiGate
  - Route is added to client to access subnets on remote FortiGate
4. User's devices access resources through an encrypted tunnel (SSL/TLS)



© Fortinet Inc. All Rights Reserved.

8

How does tunnel mode work when FortiGate is configured as client?

1. Client FortiGate connects to server FortiGate using SSL/TLS
2. Client FortiGate provides credentials to successfully authenticate. It includes both PSK (local or remote user account) and PKI (certificate) accounts.
3. Server FortiGate establishes the tunnel and assigns an IP address to the client's virtual network adapter. This is the client's source IP address for the duration of the connection.
4. Then, users can access services and network resources through the encrypted tunnel behind client FortiGate.

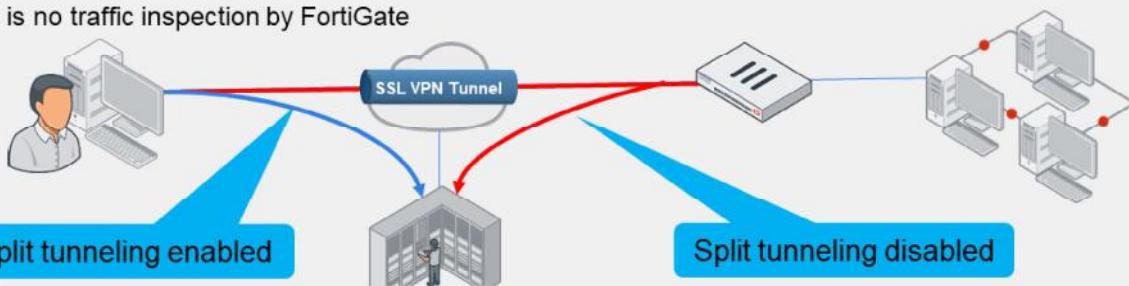
SSL VPN client FortiGate device encrypts all traffic from the remote computer and sends it over the SSL VPN tunnel. SSL VPN server FortiGate receives the encrypted traffic, de-encapsulates the IP packets, and forwards them to the private network as if the traffic originated from inside the network.

# DO NOT REPRINT

## © FORTINET

### Tunnel Mode—Split Tunneling

- **Disabled:**
  - All traffic routes through an SSL VPN tunnel to a remote FortiGate, then to the destination. This includes internet traffic
  - An egress firewall policy is required
  - Traffic inspection and security features can be applied
- **Enabled:**
  - Only traffic destined for the private network is routed through the remote FortiGate
  - Internet traffic uses the local gateway; unencrypted route
  - Conserves bandwidth and alleviates bottlenecks
  - There is no traffic inspection by FortiGate



**FORTINET**  
Training Institute

© Fortinet Inc. All Rights Reserved.

9

Tunnel mode also supports split tunneling.

When split tunneling is disabled, all IP traffic generated by the client's computer—including internet traffic—is routed across the SSL VPN tunnel to FortiGate. This sets up FortiGate as the default gateway for the host. You can use this method in order to apply security features to the traffic on those remote clients, or to monitor or restrict internet access. This adds more latency and increases bandwidth usage.

In a FortiGate (client) to FortiGate (server) setup, a default route is effectively dynamically created on the SSL VPN client FortiGate, and the new default route is added to the existing default route in the form of ECMP. The following options are available to configure routing:

- To make all traffic default to the SSL VPN server and still have a route to the server's listening interface, on the SSL VPN client, set a lower distance for the default route that is learned from the server.
- To include both default routes in the routing table, with the route learned from the SSL VPN server taking priority, on the SSL VPN client, set a lower distance for the route learned from the server. If the distance is already zero, then increase the priority on the default route.

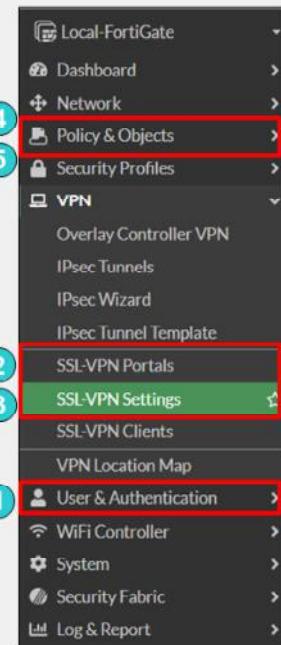
When split tunneling is enabled, only traffic that is destined for the private network behind the remote FortiGate is routed through the tunnel. All other traffic is sent through the usual unencrypted route. There is no traffic inspection by FortiGate.

Split tunneling helps to conserve bandwidth and alleviates bottlenecks.

**DO NOT REPRINT****© FORTINET**

## Configuring SSL VPN—User as Client

1. Set up user accounts and groups for remote SSL VPN users
2. Configure SSL VPN portals
3. Configure SSL VPN settings
4. Create a firewall policy to and from the SSL VPN interface
  - Accepts and decrypts packets
  - Allows traffic from SSL VPN clients to the internal network and the reverse
5. Optionally:
  - Create a firewall policy to allow SSL VPN traffic to the internet:
    - Useful to allow all clients traffic through FortiGate to internet when split tunneling is disabled
    - You can use FortiGate to apply security profiles



**FORTINET**  
Training Institute

© Fortinet Inc. All Rights Reserved. 10

The first step is to create the accounts and user groups for the SSL VPN clients.

You can use all FortiGate authentication methods, with the exception of remote password authentication using the Fortinet Single Sign-On (FSSO) protocol, for SSL VPN authentication. This includes local password authentication and remote password authentication (using the LDAP, RADIUS, and TACACS+ protocols).

This slide shows the steps an administrator must take to configure SSL VPN. You can configure some steps in a different order than what is shown on this slide.

# DO NOT REPRINT

## © FORTINET

### Configure the SSL VPN Portal

The screenshot shows the FortiGate UI for configuring SSL VPN portals. On the left, a list of portals is shown with 'full-access' and 'tunnel-access' selected. A red box highlights the 'Tunnel Mode' column for both entries. A blue arrow points from this list to a detailed configuration window on the right.

**Tunnel Mode Configuration:**

- Name:** tunnel-access
- Tunnel Mode:** Enabled (selected)
- Split tunneling:** Disabled
- Enabled Based on Policy Destination:** Selected. Description: Only client traffic in which the destination matches the destination configured on the SSL VPN firewall policy will be directed over the SSL-VPN tunnel.
- Enabled for Trusted Destinations:** Not selected. Description: Only client traffic which does not match explicitly trusted destinations will be directed over the SSL-VPN tunnel.
- Routing Address Override:** Source IP Pools: SSLVPN\_TUNNEL\_ADDR1
- Tunnel Mode Client Options:**
  - Allow client to save password: Enabled
  - Allow client to connect automatically: Enabled
  - Allow client to keep connections alive: Enabled
  - DNS Split Tunneling: Enabled
  - Host Check: Enabled

**FORTINET**  
Training Institute

© Fortinet Inc. All Rights Reserved. 11

The next step is to configure the SSL VPN portal(s). An SSL VPN portal contains tools and resource links for the users to access.

In tunnel mode, when you enable split tunneling, you need to select either **Enabled Based on Policy Destination** or **Enabled for Trusted Destination** setting, which usually specifies networks behind the FortiGate for the SSL VPN users to access. **Enabled Based on Policy Destination** allows client traffic in which destination is matched with the destination configured on the SSL VPN firewall policy where as **Enabled for Trusted Destination** allows client traffic that does not match the explicitly trusted destination.

**Routing Address Override** allows you to define the destination network (usually the corporate network) that routes through the tunnel. If you don't select the **Routing Address Override**, the destination address in the respective firewall policies defines the destination network.

Also, for tunnel mode you need to select an IP pool for users to acquire an IP address when connecting. There is a default pool available within the address objects if you do not create your own.

# DO NOT REPRINT

## © FORTINET

### Configure the SSL VPN Portal

**VPN > SSL VPN Portals**

| Name          | Tunnel Mode | Web Mode |
|---------------|-------------|----------|
| full-access   | Enabled     | Enabled  |
| tunnel-access | Enabled     | Disabled |
| web-access    | Disabled    | Enabled  |

- SSL VPN portals determine the access profiles
  - Configure portals for different user or groups
- SSL VPN portals can operate in:
  - Tunnel mode
    - Activate split tunneling in the **Enable Split Tunneling** option
    - Assign an IP address to the end user virtual network adapter in **Source IP Pool:** fortissl
  - Web mode
    - Use direct connection or bookmarks to several applications such as: FTP, HTTP/HTTPS, RDP, SMB/CIFS, SSH, TELNET, VNC

**Tunnel Mode**

**Web Mode**

**Administrator-defined bookmarks**

© Fortinet Inc. All Rights Reserved. 12

The next step is to configure the SSL VPN portal(s). An SSL VPN portal contains tools and resource links for the users to access.

In tunnel mode, when you enable split tunneling, you need to select either **Enabled Based on Policy Destination** or **Enabled for Trusted Destination** setting, which usually specifies networks behind the FortiGate for the SSL VPN users to access. **Enabled Based on Policy Destination** allows client traffic in which destination is matched with the destination configured on the SSL VPN firewall policy where as **Enabled for Trusted Destination** allows client traffic that does not match the explicitly trusted destination.

**Routing Address Override** allows you to define the destination network (usually the corporate network) that routes through the tunnel. If you don't select the **Routing Address Override**, the destination address in the respective firewall policies defines the destination network.

Also, for tunnel mode you need to select an IP pool for users to acquire an IP address when connecting. There is a default pool available within the address objects if you do not create your own.

If you enable web mode, you can customize the SSL VPN portal and preconfigure bookmarks to appear for all users who log in to the SSL VPN portal. Also, you can individually configure and link each portal to a specific user or user group, so they have access to only required resources.

# DO NOT REPRINT

## © FORTINET

## Configure SSL VPN Settings

- FortiGate interface for SSL VPN portal:
  - Default port is 443
  - By default, the admin GUI interface and the SSL VPN portal use same HTTPS port
  - Advised to use different interfaces for admin GUI access and SSL VPN portal
  - If both services use the same interface and port, only the SSL VPN portal appears
- Restrict access to known hosts
- SSL VPN time out:
  - Default idle: 300 sec (5 min)
- Digital server certificate:
  - Self-signed certificate used by default
  - To avoid browser security warnings, use a certificate issued by a public CA, generate a trusted certificate or install the self-signed certificate on all clients

After you configure the SSL VPN portal, the next step is to configure the SSL VPN settings.

Let's start with the **Connection Settings** section. Here, you need to map a FortiGate interface to the SSL VPN portal. The default port for the SSL VPN portal is 443. This means users need to connect to the IP address of the FortiGate interface mapped to the SSL VPN portal, using port443 HTTPS. If you enable **Redirect HTTP to SSL VPN**, users who connect using HTTP (TCP port 80) will be redirected to HTTPS.

Port 443 is the standard default port for administration of the HTTPS protocol. This is convenient because users do not need to specify the port in their browsers. For example, <https://www.example.com/> automatically uses port443 in any browser. This is considered a valid setup on FortiGate because you usually don't access the SSL VPN login through every interface. Likewise, you generally don't enable administrative access on every interface of your FortiGate. So, even though the ports may overlap, the interfaces that each one uses to access may not. However, if the SSL VPN login portal and HTTPS admin access both use the same port, and are both enabled on the same interface, only the SSL VPN login portal will appear. To have access to both portals on the same interface, you need to change the port number for one of the services. If you change the administrator access port, this will affect the port number for that service on all interfaces.

Also, an inactive SSL VPN is disconnected after 300 seconds (5 minutes) of inactivity. You can change this timeout using the **Idle Logout** setting on the GUI.

Finally, like other HTTPS websites, the SSL VPN portal presents a digital certificate when users connect. By default, the portal uses a self-signed certificate, which triggers the browser to show a certificate warning. To avoid the warning, you should use a digital certificate signed by a publicly known certificate authority (CA). You can also generate a certificate for interface. Alternatively, you can load the FortiGate self-signed digital certificate into the browser as a trusted authority.

**DO NOT REPRINT****© FORTINET**

## Configure SSL VPN Settings (Contd)

- Define the IP range for the SSL VPN
  - IPs are assigned to clients' virtual adapters while joined to VPN
- Resolve names by DNS server
  - Use internal DNS if resolving internal domain names
  - Optionally, resolve names by WINS servers
- Specify authentication portal mapping
  - Specify portals for each user or group
  - Define portal for all other users or groups
    - You cannot delete this portal

### VPN > SSL VPN Settings

The screenshot shows the 'Tunnel Mode Client Settings' section with 'Address Range' set to 'Automatically assign addresses'. It also shows 'DNS Server' set to 'Same as client system DNS' and 'Specify WINS Servers' checked. Under 'Web Mode Settings', 'Language' is set to 'Browser preference'. In the 'Authentication/Portal Mapping' section, there is a table:

| Users/Groups           | Portal         |
|------------------------|----------------|
| Accountants            | tunnel-access  |
| Teachers               | Teacher_Portal |
| All Other Users/Groups | full-access    |

Define the tunnel-mode client settings and the authentication rules that map users to the appropriate portal.

When users connect, the tunnel is assigned an IP address. You can choose to use the default range or create your own range. The IP range determines how many users can connect simultaneously.

DNS server resolution is effective only when the DNS traffic is sent over the VPN tunnel. Usually, this is the case only when split tunnel mode is disabled and all traffic is sent from the user's computer across the tunnel.

Finally, you can allow different groups of users to access different portals. In the example shown on this slide, teachers have access only to the **Teacher\_Portal**. Accountants can connect to **tunnel-access** portal.

# DO NOT REPRINT

## © FORTINET

## Firewall Policies to and from SSL VPN Interface

- Listens for connections to the SSL VPN portal
- **ssl.<vdom\_name>** policy enables portal with user authentication
- The selected **Incoming Interface** is the SSL VPN virtual interface
  - Example: **ssl.root** for root VDOM
- Passes decrypted traffic to the selected **Outgoing Interface**

**Policy & Objects > Firewall Policy**

|                    |                                                              |
|--------------------|--------------------------------------------------------------|
| Name               | SSL-VPN                                                      |
| Incoming Interface | SSL-VPN tunnel interface (ssl.root)                          |
| Outgoing Interface | port3                                                        |
| Source             | SSLVPN_TUNNEL_ADDR1<br>Accounts<br>SSL_VPN_USERS<br>Teachers |
| Destination        | LOCAL_SUBNET                                                 |
| Schedule           | always                                                       |
| Service            | ALL                                                          |
| Action             | ACCEPT                                                       |

The fourth, and last, mandatory step involves creating firewall policies for logging on.

SSL VPN traffic on FortiGate uses a virtual interface called `ssl.<vdom_name>`. Each virtual domain (VDOM) contains a different virtual interface based on its name. By default, if VDOMs are not enabled, then the device operates with a single VDOM called `root`.

To activate and successfully log in to the SSL VPN, there must be a firewall policy from the SSL VPN interface to the interface to which you want to allow access for the SSL VPN users, including all of the users and groups that can log in as the source. Without a policy like this, no login portal is presented to users.

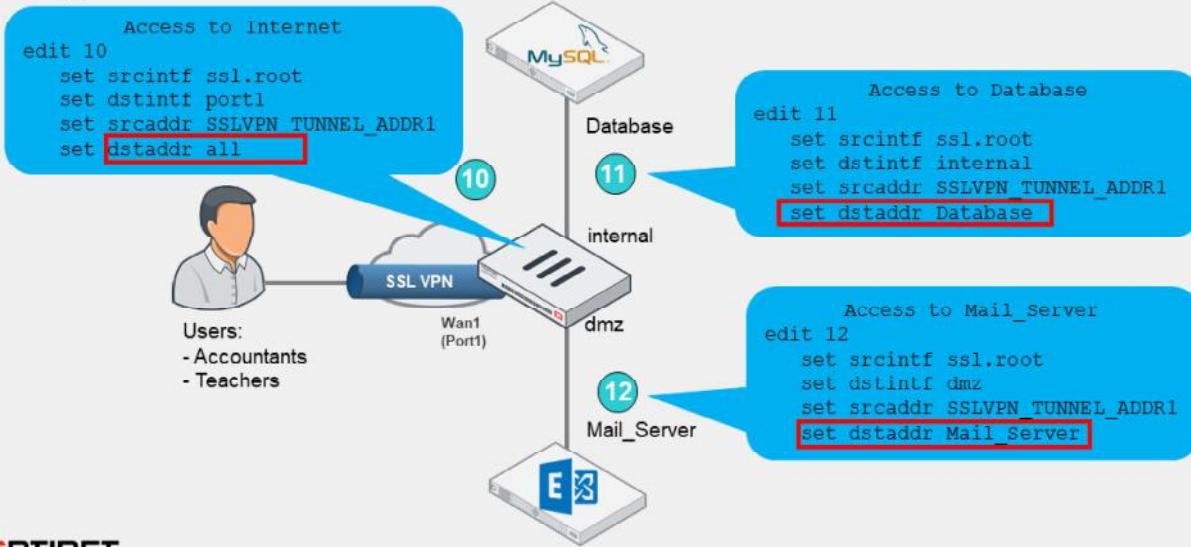
If there are resources behind other interfaces that users need access to, then you need to create additional policies that allow traffic from `ssl.root` to exit those interfaces.

# DO NOT REPRINT

## © FORTINET

### Example: Access to Resources

- All traffic generated by the user exits through the `ssl.<vdom_name>` interface
  - Applies to both web and tunnel mode



**FORTINET**  
Training Institute

© Fortinet Inc. All Rights Reserved. 16

Any traffic from SSL VPN users, whether in web portal or tunnel mode, exits from the `ssl.<vdom_name>` interface.

This slide shows an example of firewall policies that are configured to allow access to resources behind other interfaces that users need access to when connected through SSL VPN.

Optionally, if split tunneling is disabled, you need to create an additional firewall policy from `ssl.root` to the egress interface to allow clients access to the internet.

You can also apply security profiles to this firewall policy to restrict user access to the internet.

**DO NOT REPRINT**  
**© FORTINET**

## Configuring SSL VPN—FortiGate as Server

- SSL VPN Server FortiGate

- Set up user accounts and groups for remote SSL VPN users
  - Create two accounts: local/remote and PKI
  - Require clients to authenticate using their certificates as well as username and password
- Configure SSL VPN portals
- Configure SSL VPN settings
  - Authentication rules include both accounts using CLI
- Create a firewall policy to and from the SSL VPN interface
- Create a firewall policy to allow SSL VPN traffic to the internet (optional)

Use CLI to create first PKI user to get PKI menu on GUI

User & Authentication > User Definition

|                                                                         |                                                                         |
|-------------------------------------------------------------------------|-------------------------------------------------------------------------|
| Edit User                                                               |                                                                         |
| Username                                                                | clientfortigate                                                         |
| User Account Status                                                     | <input checked="" type="radio"/> Enabled <input type="radio"/> Disabled |
| User Type                                                               | Local User                                                              |
| Password                                                                | *****                                                                   |
| User Group                                                              | <input checked="" type="radio"/> SSL-VPN-Users <input type="radio"/> +  |
| <input type="checkbox"/> Two-factor Authentication                      |                                                                         |
| <input type="button" value="OK"/> <input type="button" value="Cancel"/> |                                                                         |

User & Authentication > PKI

|                                                                         |           |
|-------------------------------------------------------------------------|-----------|
| Edit PKI User                                                           |           |
| Name                                                                    | pki       |
| Subject                                                                 |           |
| CA                                                                      | CA Cert 1 |
| <input type="checkbox"/> Two-factor authentication                      |           |
| <input type="button" value="OK"/> <input type="button" value="Cancel"/> |           |

```
config user peer
edit pki
set ca "CA_Cert_1"
set cn "FGVM01TM905"
end
```

**FORTINET**  
 Training Institute

© Fortinet Inc. All Rights Reserved. 17

To configure FortiGate as an SSL VPN server, you must take the steps shown on this slide.

This includes local or remote user accounts or groups and PKI users. The PKI menu is available on the GUI only after you have created a PKI user using the CLI. You can configure a CN only on the CLI. If you do not specify a CN, then any certificate that is signed by the CA is considered valid and matched. Client authentication requires both the client certificate and username and password.

The other steps are identical to SSL VPN setup for remote users. You can configure some steps in a different order than what is shown on this slide.

# DO NOT REPRINT

## © FORTINET

## Configuring SSL VPN—FortiGate as Client

- SSL VPN Client FortiGate
  1. Create PKI user
    - Select CA certificate that allows FortiGate to complete the certificate chain and verify the server certificate
  2. Create SSL VPN tunnel interface using ssl.<vdom> interface
  3. Create and configure the SSL VPN Client settings on **VPN > SSL-VPN Clients**
  4. Create a firewall policy from internal interface to the SSL VPN interface

The screenshot displays two configuration windows side-by-side:

**Network > Interface > Create New**

- Name: ssclient\_port (highlighted by a blue box)
- Alias:
- Type: SSL-VPN Tunnel (highlighted by a blue box)
- Interface: port4 (highlighted by a blue box)
- VRF ID: 0
- Role: LAN
- Administrative Access (checkboxes):
  - IPv4:  HTTPS,  SSH,  RADIUS Accounting
  - IPv6:  PING,  SNMP,  Security Fabric Connection

**VPN > SSL-VPN Clients > Create New**

- Name: SSLClienttoHQ (highlighted by a blue box)
- Interface: ssclient\_port (highlighted by a blue box)
- Server: 10.200.1.1 (highlighted by a blue box)
- Port: 10443
- Username: ClientFortigate (highlighted by a red box)
- Pre-shared Key: (redacted)
- Client Certificate: (redacted)
- Peer: pki (highlighted by a blue box)
- Administrative Distance: 10
- Priority: 0
- Status: Enabled (highlighted by a green box)
- Comments: (redacted)

Annotations on the right side of the second window provide additional context:

- Client Name**: SSLClienttoHQ
- Virtual SSLInterface**: ssclient\_port
- Server FortiGate IP Address and SSL Port**: 10.200.1.1, 10443
- Local and PKI user details including local cert to identify this client**: ClientFortigate, Pre-shared Key, Client Certificate, Peer, Administrative Distance, Priority, Status
- Dynamic route priority and distance settings**: Priority (0), Status (Enabled)

FOURINET Training Institute

© Fortinet Inc. All Rights Reserved. 18

This slide shows the steps you must take to configure FortiGate as an SSL VPN client.

The PKI user must have the same CN if a CN is configured on the SSL VPN server FortiGate certificate. You must also select a CA certificate that allows FortiGate to complete the certificate chain and verify the server certificate. Next, create the SSL VPN tunnel interface using the ssl.<vdom> interface.

The **SSL-VPN Clients** settings include name, virtual SSL VPN interface, SSL VPN server FortiGate IP address and SSL port number, and local username, password and PKI(Peer) user. The **Client Certificate** as shown on this slide is the local certificate that is used to identify this client, and is assumed to already be installed on FortiGate. The SSL VPN server requires it for authentication.

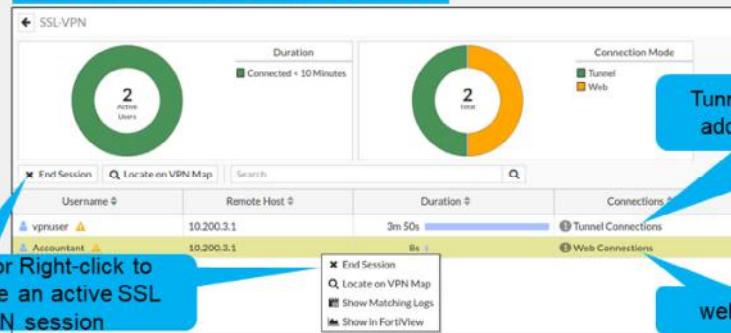
Lastly, you must create a firewall policy to allow traffic from the internal interface to the SSL VPN interface.

**DO NOT REPRINT**  
**© FORTINET**

## Monitoring SSL VPN Sessions

- Monitor which SSL VPN users are connected
  - GUI: Dashboard > Network > SSL VPN
- Shows SSL VPN user names, connection times, and IP addresses
  - For tunnel mode, **Active Connections** displays IP address assigned to `fortissl` virtual adapter
- Force end user disconnection
  - Right-click the user name and select **End Session**

Dashboard > Network > SSL VPN



© Fortinet Inc. All Rights Reserved. 19

**FORTINET.**  
 Training Institute

You can monitor which SSL VPN users are connected on the **SSL VPN** widget. This shows the names of all SSL VPN users who are currently connected to FortiGate, their IP addresses (both inside the tunnel and outside), and connection times.

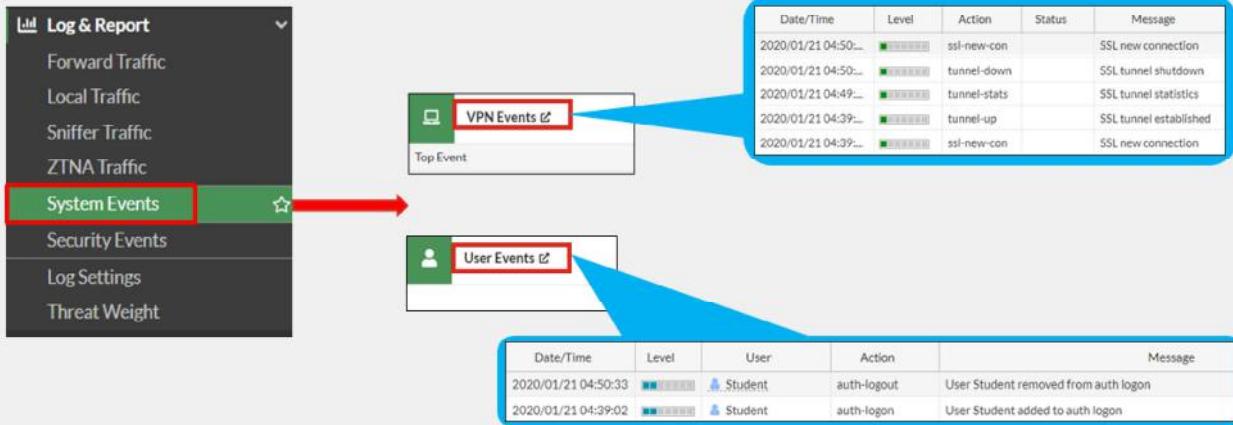
When a user connects using tunnel model, the **Active Connections** column shows the IP address assigned by FortiGate to the `fortissl` virtual adapter on the client's computer. Otherwise, the user is connected only to the web portal page.

# DO NOT REPRINT

## © FORTINET

### SSL VPN Logs

- Review if the SSL VPN tunnel is established or closed
- Review the authentication action related to SSL VPN users
- Review SSL VPN connections in tunnel mode with FortiClient



**FORTINET**  
Training Institute

© Fortinet Inc. All Rights Reserved. 20

You can also review SSL VPN logs. On **Log & Report > System Events**:

- Select the **VPN Events** widget to show new connection requests, and if the SSL VPN tunnel is established or closed.
- Select the **User Events** widget to see the authentication action related to SSL VPN users.

# DO NOT REPRINT

## © FORTINET

## SSL VPN Idle Timeout vs. Authentication Session

- Firewall policy authentication session is associated with SSL VPN tunnel session
  - Firewall policy authentication session is forced to end when SSL VPN tunnel session ends
  - Prevents reuse of authenticated SSL VPN firewall sessions (not yet expired) by a different user, after the initial user terminates the SSL VPN tunnel session
- SSL VPN authentication is not subject to the firewall authentication timeout setting
  - It has a separate idle setting: default 300 seconds

The screenshot shows the 'VPN > SSL VPN Settings' configuration page. A red box highlights the 'Idle Logout' section, which includes a toggle switch and a 'Inactive For' input field set to '300'. An arrow points from this highlighted area to a command-line interface (CLI) command:

```
config vpn ssl settings
 set idle-timeout <0-259200>
end
```

Below the interface, the Fortinet Training Institute logo is visible, along with copyright and page number information.

When an SSL VPN is disconnected, either by the user or through the SSL VPN idle setting, all associated sessions in the FortiGate session table are deleted. This prevents the reuse of authenticated SSL VPN sessions (not yet expired) after the initial user terminates the tunnel.

The SSL VPN user idle setting is not associated with the firewall authentication timeout setting. It is a separate idle option specifically for SSL VPN users. A remote user is considered idle when FortiGate does not see any packets or activity from the user within the configured timeout period.

**DO NOT REPRINT****© FORTINET**

## SSL VPN Timers

- Set up timers to avoid logouts when SSL VPN users are connected over high latency connections

- DTLS hello timeout—default 10 seconds
- Login timeout—default 30 seconds

```
config vpn ssl settings
 set login-timeout <10-180>
 set dtls-hello-timeout <10-60>
 [set http-request-header-timeout <1-60>
 Set http-request-body-timeout <1-60>
]
end
```

- Timers can also help to mitigate DoS attacks within SSL VPN caused by partial HTTP requests, such as Slowloris and R-U-Dead-Yet

When connected to SSL VPN over high latency connections, FortiGate can time out the client before the client can finish the negotiation process, such as DNS lookup and time to enter a token. Two new CLI commands under `config vpn ssl settings` have been added to address this. The first command allows you to set up the login timeout, replacing the previous hard timeout value. The second command allows you to set up the maximum DTLS hello timeout for SSL VPN connections.

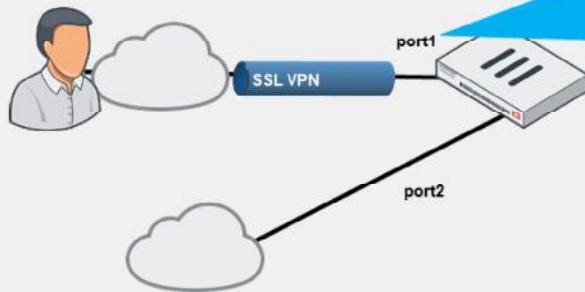
Also, timers can help you to mitigate vulnerabilities such as Slowloris and R-U-Dead-Yet, that allow remote attackers to cause a denial of service through partial HTTP requests.

**DO NOT REPRINT**  
**© FORTINET**

## SSL VPN—Session Preservation

- Set session preservation on interface to avoid SSL VPN disconnections
  - Multi-WAN setup

```
config system interface
 edit <interface_name>
 set preserve-session-route enable
end
```



### CLI Console(1)

```
Local-FortiGate # config sys interface
Local-FortiGate (interface) # edit port1
Local-FortiGate (port1) # set preserve-session-route enable
Local-FortiGate (port1) # end
Local-FortiGate #
```

In the typical enterprise network, there can be multiple WAN links. In the FortiGate, by default, any session with source NAT disabled go through the route lookup when routing table changes. The sessions are marked dirty after changes to routing table and reevaluated. Because of these route changes in multi-WAN setup, there is possibility that request comes from one interface and response goes out through other causing disconnections.

The `set preserve-session-route` command keeps the session on same interface even if session is eligible for routing changes. By default, route preservation is disabled on the interface.

The example on this slide shows `port1` is reserved for SSL VPN connections and `port2` is used for other services. Even if `port2` becomes primary connection because of route changes, FortiGate will keep the existing SSL VPN sessions on `port1` interface.

**DO NOT REPRINT****© FORTINET**

## Best Practices for Common SSL VPN Issues

- For tunnel mode connections, make sure that:
  - The FortiClient version is compatible with the FortiOS firmware
    - Refer to release notes for product compatibility and integration
  - Split tunneling is enabled to allow internet access without backhauling all user's data to the remote network, or
  - Split tunneling is disabled and an egress firewall policy is created for SSL VPN connections
- For general SSL VPN connections, make sure that:
  - Users are connecting to the correct port number
    - To check SSL VPN port assignment, click **VPN > SSL VPN Settings**
  - Firewall policies include SSL VPN groups or users, and the destination address
  - The timeout timer is configured to flush inactive sessions after a short time
  - Set DTLS timer for user's network connections with high latency
  - Users are encouraged to log out if they are not using the network resources only accessible by SSL VPN



© Fortinet Inc. All Rights Reserved. 24

The following are some best practices to keep in mind when using SSL VPNs. These best practices can also be helpful in many SSL VPN troubleshooting situations:

- Use a FortiClient version that is compatible with your FortiOS firmware
- Enable split tunneling or create an egress firewall policy for SSL VPN connections in order to allow access for external resources
- Connect to the correct port number
- Add SSL VPN groups, SSL VPN users, and destination addresses to the firewall policies
- Set DTLS timeout for high latency network connections
- Flush inactive sessions by timeout

**DO NOT REPRINT****© FORTINET**

## Useful Troubleshooting Commands

```
diagnose debug enable
diagnose vpn ssl <...>
 list → Show current connections
 info → General SSL VPN information
 statistics → Show statistics about memory usage on FortiGate, maximum and
 current connections
 debug-filter → Debug message filter for SSL VPN

 tunnel-test → Enable/disable SSL VPN old tunnel mode IP allocation method
 web-mode-test → Enable/disable random session ID in proxy URL for testing
diagnose debug application sslvpn -1
diagnose debug application fnbamd -1
diagnose debug console timestamp enable
diagnose debug enable
```

] Display debug messages for SSL VPN and user authentication; -1 debug level produces detailed results

Check logs on the FortiClient



© Fortinet Inc. All Rights Reserved. 25

There are several useful troubleshooting commands available under `diagnose vpn ssl`. They include:

- `list`: Lists logged-on users
- `info`: Shows general SSL VPN information
- `statistics`: Shows statistics about memory usage on FortiGate
- `tunnel-test`: Enables or disables SSL VPN old tunnel mode IP allocation method
- `web-mode-test`: Enables or disables random session ID in proxy URL for testing

The command `diagnose debug application sslvpn` shows the entire list of debug messages for SSL VPN connections.

Remember, to use the commands listed above, you must first run the `diagnose debug enable` command. Also, check SSL VPN debug logs on FortiClient.

**DO NOT REPRINT**

**© FORTINET**

## Knowledge Check

1. Which action may allow internet access in tunnel mode, if the remote network does not allow internet access to SSL VPN users?  
 A. Enable split tunneling  
B. Configure the DNS server to use the same DNS server as the client system DNS
  
2. Which statement about SSL VPN timers is correct?  
 A. SSL VPN timers can prevent logouts when SSL VPN users experience high network latency.  
B. The login timeout is a non-customizable hard value.

**DO NOT REPRINT**

**© FORTINET**

## Review

- ✓ Configure SSL VPN portals
- ✓ Configure tunnel mode SSL VPN
- ✓ Monitor SSL VPN-connected users
- ✓ Troubleshoot common SSL VPN 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 and use SSL VPNs to give remote users access to your private network.

**DO NOT REPRINT**

© FORTINET

**FORTINET**  
Training Institute



# FortiGate Administrator

IPsec VPN

FortiOS 7.4

Last Modified: 15 November, 2023

In this lesson, you will learn about the architectural components of IPsec VPN and how to configure them.

**DO NOT REPRINT****© FORTINET**

## Objectives

- 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

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

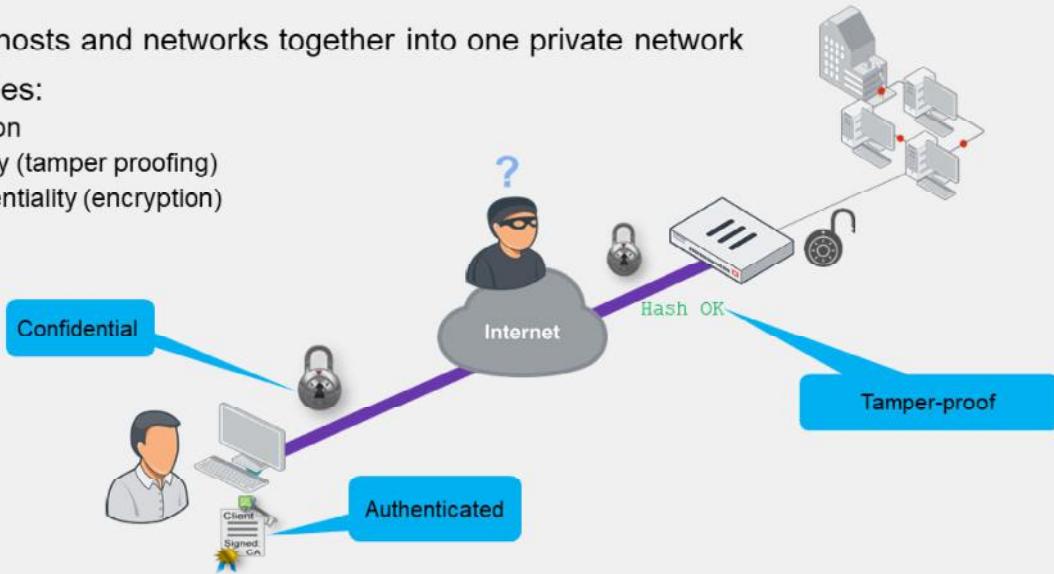
By demonstrating competence in IPsec, you will be able to understand IPsec concepts and benefits. You will also be able to successfully determine the settings required for your IPsec VPN deployment, set up appropriate routing and firewall policies on FortiGate, and add redundancy to your IPsec VPN deployment.

# 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**  
Training Institute

© Fortinet Inc. All Rights Reserved. 3

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).

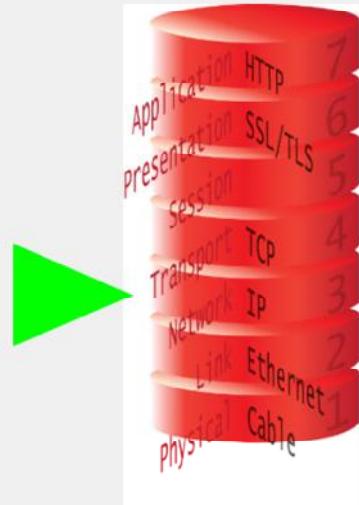
To set up a VPN, you must configure matching settings on both ends of the VPN—whether the VPN is between two FortiGate devices, FortiGate and FortiClient, or a third-party device and FortiGate. If the settings don't match, the tunnel setup fails.

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

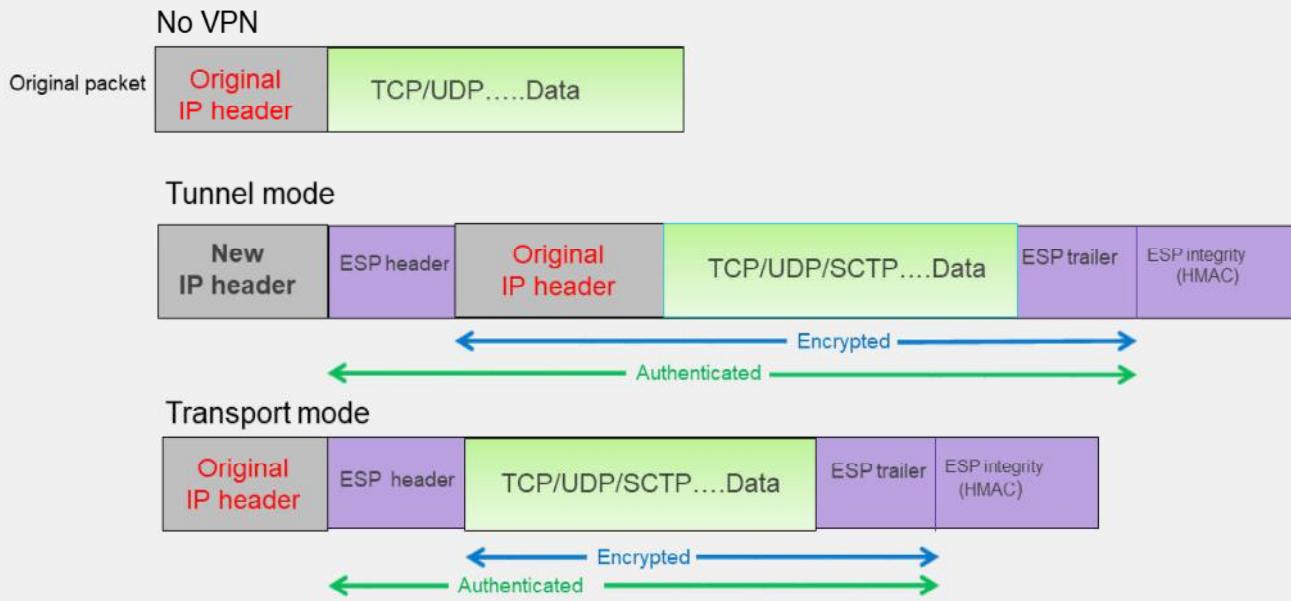


IPsec provides services at the IP (network) layer. During tunnel establishment, both ends negotiate the encryption and authentication algorithms to use.

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**  
Training Institute

© Fortinet Inc. All Rights Reserved.

6

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)



© Fortinet Inc. All Rights Reserved. 7

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"> <li>Main           <ul style="list-style-type: none"> <li>Total messages: 9 (6 for phase 1, 3 for phase 2)</li> </ul> </li> <li>Aggressive           <ul style="list-style-type: none"> <li>Total messages: 6 (3 for phase 1, 3 for phase 2)</li> </ul> </li> </ul> | <ul style="list-style-type: none"> <li>One exchange procedure only</li> <li>Total messages: 4 (one child SA only)</li> </ul>                   |
| Authentication methods         | Symmetric: <ul style="list-style-type: none"> <li>Pre-shared key (PSK)</li> <li>Certificate signature</li> <li>Extended authentication (XAuth)</li> </ul>                                                                                                                                              | Asymmetric: <ul style="list-style-type: none"> <li>PSK</li> <li>Certificate signature</li> <li>EAP (pass-through—no client support)</li> </ul> |
| 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"> <li>Peer ID + aggressive mode + PSK</li> <li>Peer ID + main mode + certificate signature</li> </ul>                                                                                                                                                                 | <ul style="list-style-type: none"> <li>Peer ID</li> <li>Network ID</li> </ul>                                                                  |
| 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



© Fortinet Inc. All Rights Reserved.

9

In order to create an IPsec tunnel, both devices must establish their SAs and secret keys, which are facilitated by the IKE protocol.

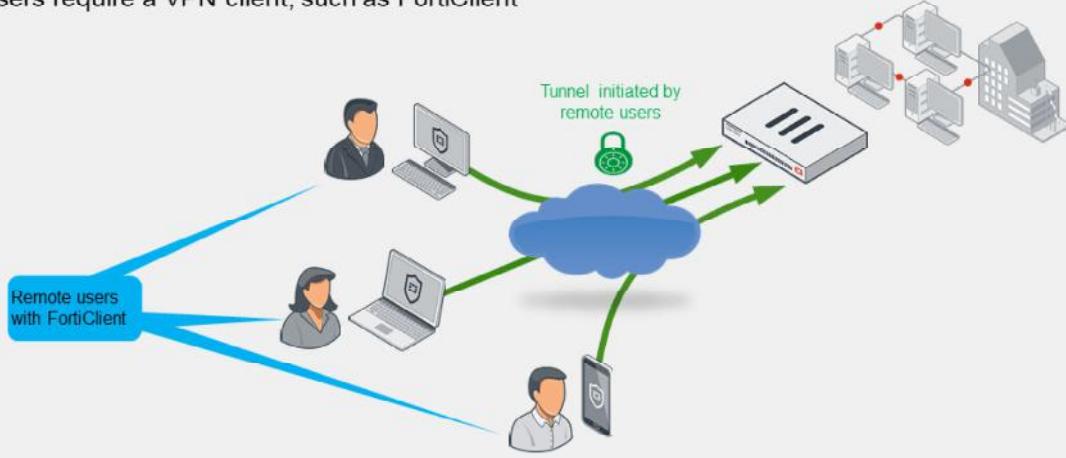
The IPsec architecture uses SAs as the basis for building security functions into IPsec. An SA is the bundle of algorithms and parameters being used to encrypt and authenticate data travelling through the tunnel. In normal two-way traffic, this exchange is secured by a pair of SAs, one for each traffic 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.

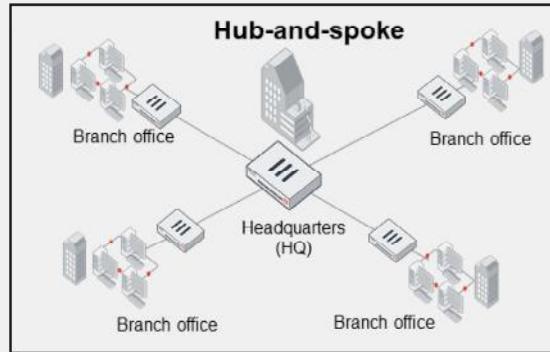
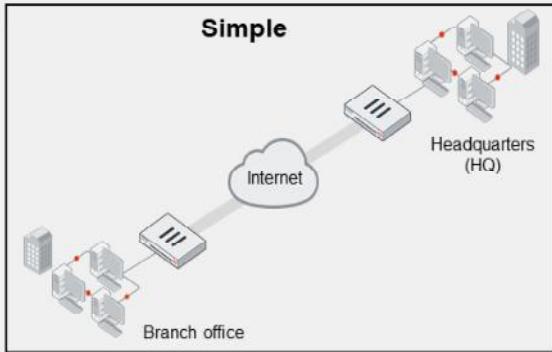
In a remote access VPN, FortiGate is usually configured as a dial-up server. You will learn more about dial-up VPNs in this lesson. The IP address of the remote internet user is usually dynamic. Because FortiGate does not know the IP address of the remote user, only the remote user can initiate a VPN 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



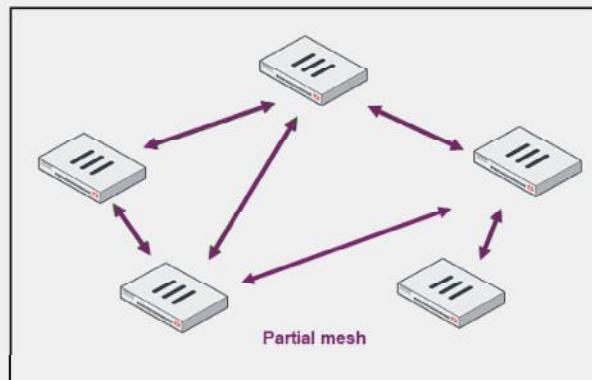
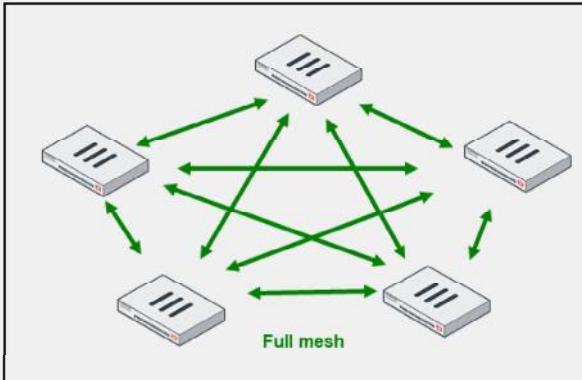
Site-to-site VPN is also known as LAN-to-LAN VPN. A simple site-to-site deployment involves two peers communicating directly to connect two networks located at different offices.

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



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

### IPsec Wizard

**VPN Creation Wizard**

**VPN Setup > Authentication > Policy & Routing > Review Settings**

**Name:** ToRemoteBackup  
**Template type:** Site to Site | Hub-and-Spoke | Remote Access | Custom  
**NAT configuration:** No NAT between sites  
 This site is behind NAT  
 The remote site is behind NAT  
**Remote device type:** FortiGate | Cisco

**Network diagram describing deployment type:** Site to Site - FortiGate. This FortiGate is connected via the Internet to a Remote FortiGate.

| Object Summary           |                           |
|--------------------------|---------------------------|
| Phase 1 interface        | ToRemoteBackup            |
| Local address group      | ToRemoteBackup_local      |
| Remote address group     | ToRemoteBackup_remote     |
| Phase 2 interface        | ToRemoteBackup            |
| Static route             | static                    |
| Blackhole route          | static                    |
| Local to remote policies | vpn_ToRemoteBackup_local  |
| Remote to local policies | vpn_ToRemoteBackup_remote |

**Summary of objects created by the IPsec wizard**

**In this lesson, you will learn only about IKEv1 configuration**

© Fortinet Inc. All Rights Reserved. 14

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.

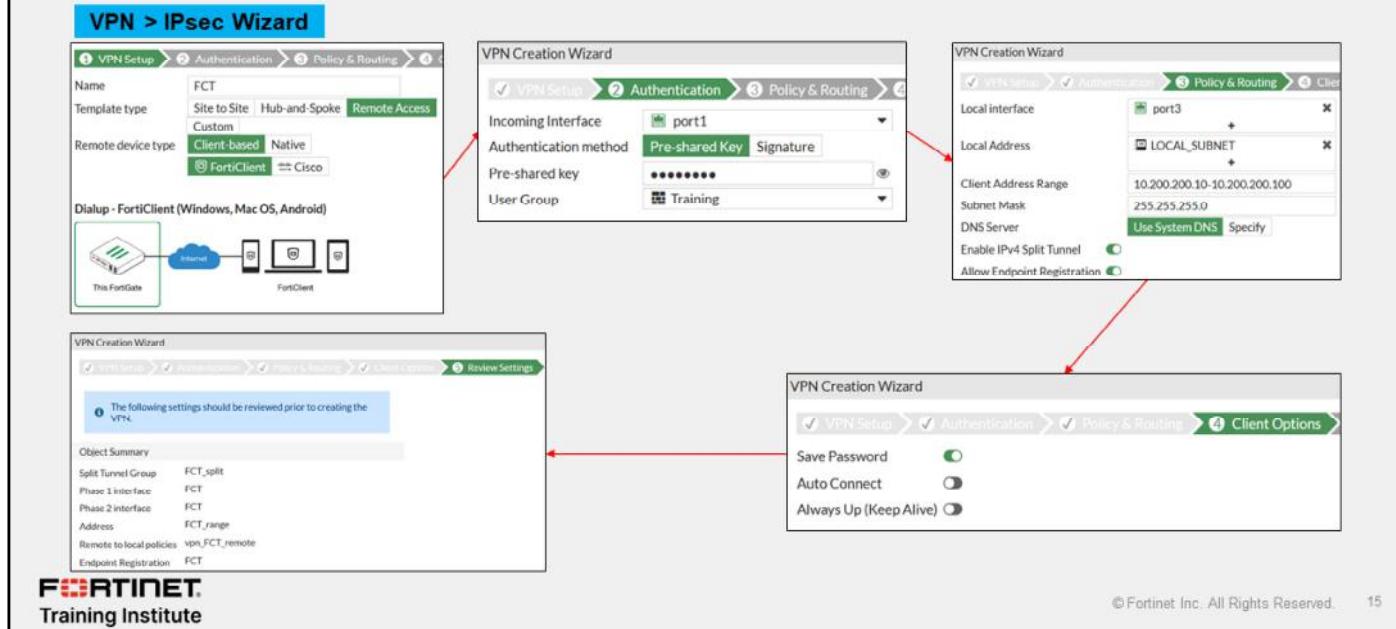
If you are new to FortiGate, or don't have much experience with IPsec VPNs, using the IPsec wizard is recommended. You can later adjust the configuration applied by the wizard to match your specific needs.

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**

## IPsec Tunnel Templates

| VPN > IPsec Tunnel Template                     |                                                                           |
|-------------------------------------------------|---------------------------------------------------------------------------|
| Template                                        | Description                                                               |
| Site to Site - FortiGate                        | Static tunnel between this FortiGate and a remote FortiGate.              |
| Site to Site - FortiGate (SD-WAN)               | Static tunnel between this FortiGate using SD-WAN and a remote FortiGate. |
| Dialup - FortiGate                              | On-demand tunnel between two FortiGate devices.                           |
| Site to Site - Cisco                            | Static tunnel between this FortiGate and a remote Cisco firewall.         |
| Dialup - Cisco Firewall                         | On-demand tunnel between a FortiGate device and a Cisco Firewall.         |
| Dialup - FortiClient (Windows, Mac OS, Android) | On-demand tunnel for users using the FortiClient software.                |
| Dialup - iOS (Native)                           | On-demand tunnel for iPhone/iPad users using the native iOS IPsec client. |
| Dialup - Android (Native L2TP/IPsec)            | On-demand tunnel for Android users using the native L2TP/IPsec client.    |
| Dialup - Windows (Native L2TP/IPsec)            | On-demand tunnel for Windows users using the native L2TP/IPsec client.    |
| Dialup - Cisco IPsec Client                     | On-demand tunnel for users using the Cisco IPsec client.                  |
| Hub-and-Spoke - FortiGate (Spoke)               | Spoke role in a Hub-and-Spoke auto-discovery VPN configuration.           |
| Hub-and-Spoke - FortiGate (Hub)                 | Hub role in a Hub-and-Spoke auto-discovery VPN configuration.             |

Click View to review the template details

**FORTINET**  
Training Institute

© Fortinet Inc. All Rights Reserved. 16

The IPsec wizard uses one of the templates shown on this slide when applying the configuration for the new IPsec tunnel. You can review the settings of a template by selecting the template, and then clicking **View**. You cannot change the template settings.

**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

Name: ToRemote

Comments:

**Network**

- IP Version: IPv4
- Remote Gateway: Static IP Address (highlighted)
- IP Address: 10.200.3.1
- Interface: port1
- Local Gateway:  (highlighted)
- Mode Config: Enable
- NAT Traversal: Keepalive Frequency: 10
- Dead Peer Detection: On Idle
- DPD retry count: 3
- DPD retry interval: 20 s
- Forward Error Correction: Egress, Ingress

Remote Gateway: Static IP Address (highlighted)

IP Address: Dialup User  
Dynamic DNS

Interface:

Local Gateway:

|             |              |         |
|-------------|--------------|---------|
| Primary IP  | Secondary IP | Specify |
| 10.200.10.1 |              |         |

**FORTINET.**  
Training Institute

© Fortinet Inc. All Rights Reserved. 19

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.

FortiGate 7.4 Administrator Study Guide

311

# DO NOT REPRINT

## © FORTINET

### Phase 1—Network (Contd)

The screenshot shows the FortiGate GUI for configuring a network tunnel. The main window displays fields for Name (ToRemote), IP Version (IPv4), Remote Gateway (Static IP Address: 10.200.3.1, Interface: port1), and various operational parameters like NAT Traversal (Enable), Keepalive Frequency (10), Dead Peer Detection (On Demand), DPD retry count (3), DPD retry interval (20), and Forward Error Correction (Egress, Ingress). A red box highlights the 'Advanced...' button at the bottom left of the main window. An arrow points from this button to a separate 'Advanced' settings window, which lists options such as Add route (Enabled), Auto discovery sender (Enabled), Auto discovery receiver (Enabled), Exchange interface IP (Enabled), Device creation (Enabled), and Aggregate member (Enabled).

**FORTINET.**  
Training Institute

© Fortinet Inc. All Rights Reserved. 20

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.

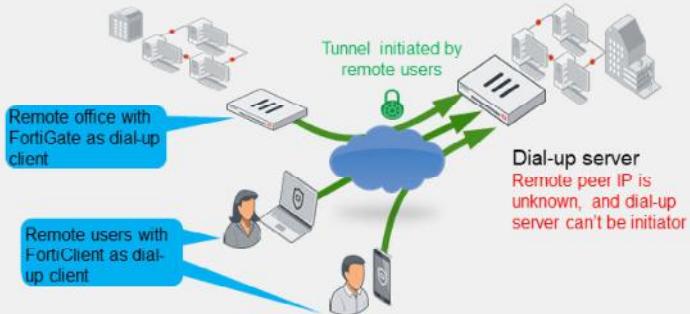
# DO NOT REPRINT

## © 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)



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.

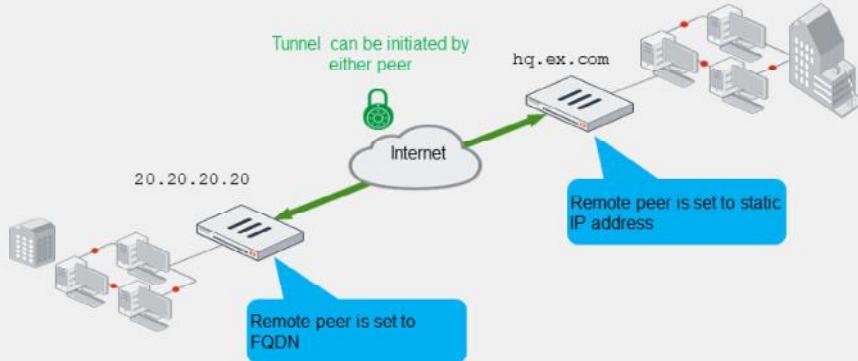
Usually, dial-up clients are remote and mobile employees with FortiClient on their computer or handheld devices. You can also have a FortiGate device acting as a dial-up client for a remote office. You can use one dial-up server configuration on FortiGate for multiple IPsec tunnels from many remote offices 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)



**FORTINET**  
 Training Institute

© Fortinet Inc. All Rights Reserved. 22

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.

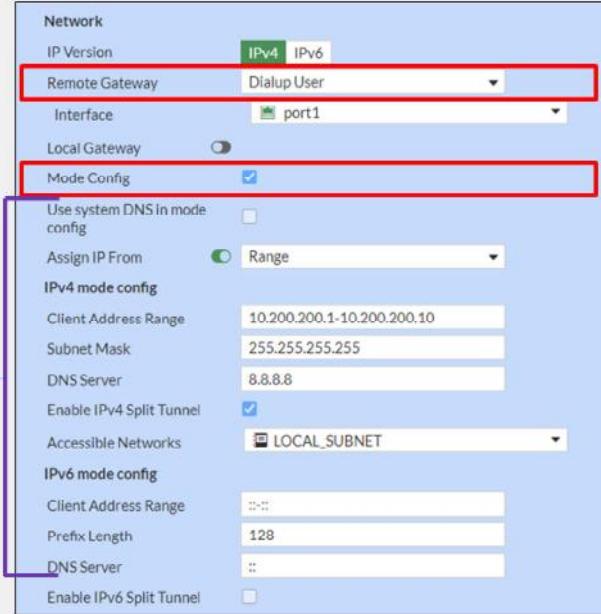
Note that in a dial-up setup, the dial-up client is just a VPN peer with the remote gateway set to **static IP address** or **dynamic DNS**. When setting your VPN, you can combine different types of remote gateways. For obvious reasons, a tunnel in which both peers have the remote gateway set to **Dialup 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



**FORTINET**  
Training Institute

© Fortinet Inc. All Rights Reserved.

23

**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

| Network                  |                                      |
|--------------------------|--------------------------------------|
| 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   Disable   Forced            |
| Keepalive Frequency      | 10                                   |
| Dead Peer Detection      | Disable   On Idle   <b>On Demand</b> |
| DPD retry count          | 3                                    |
| DPD retry interval       | 20                                   |
| Forward Error Correction | Egress   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.

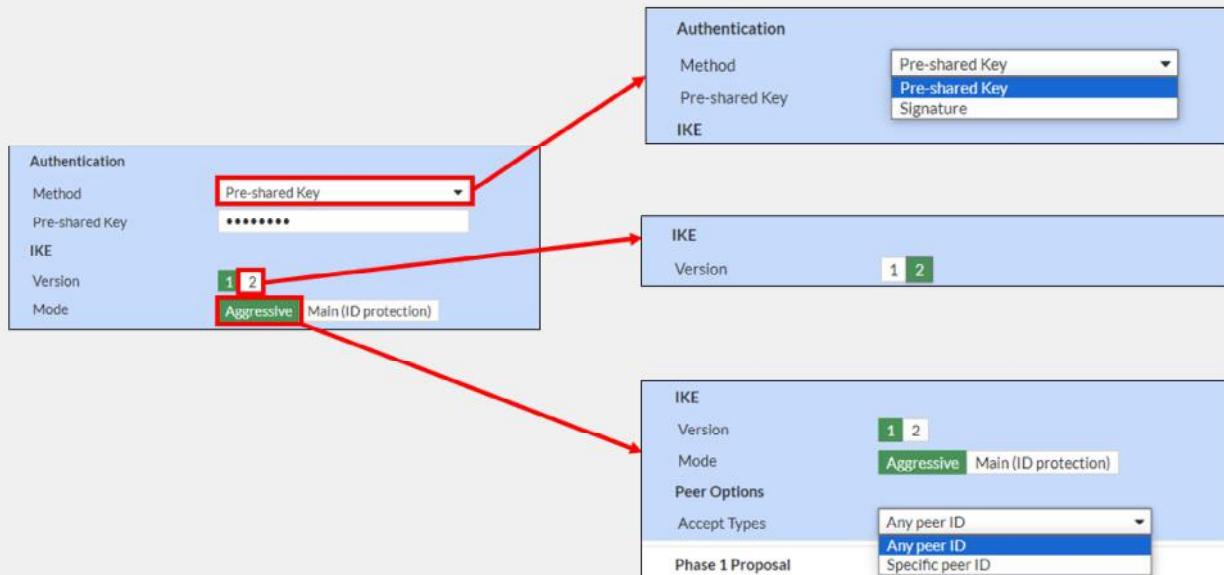
FortiGate supports three DPD modes:

- **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



**FORTINET**  
Training Institute

© Fortinet Inc. All Rights Reserved.

26

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

| Phase 1 Proposal       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Encryption             | AES128                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Encryption             | AES256                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Encryption             | AES128                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Encryption             | AES256                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Diffie-Hellman Groups  | <input type="checkbox"/> 32<br><input type="checkbox"/> 31<br><input type="checkbox"/> 30<br><input type="checkbox"/> 29<br><input type="checkbox"/> 28<br><input type="checkbox"/> 27<br><input type="checkbox"/> 21<br><input type="checkbox"/> 20<br><input type="checkbox"/> 19<br><input type="checkbox"/> 18<br><input type="checkbox"/> 17<br><input type="checkbox"/> 16<br><input checked="" type="checkbox"/> 15<br><input checked="" type="checkbox"/> 14<br><input checked="" type="checkbox"/> 5<br><input type="checkbox"/> 2<br><input type="checkbox"/> 1 |
| Key Lifetime (seconds) | 86400                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Local ID               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

Phase 1 Proposal [Add](#)

- Encryption AES128
- Encryption AES256
- Encryption DES
- Encryption 3DES
- Encryption AES128
- Encryption AES192
- Encryption AES256

Diffie-Hellman Groups  21

Authentication SHA256
 

- Authentication SHA256
- Authentication SHA256
- Authentication MD5
- Authentication SHA256
- Authentication SHA384
- Authentication SHA512

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

The screenshot shows the FortiGate configuration interface with three main sections:

- Remote Gateway:** Shows dropdown menus for IP Address (Static IP Address, Static IP Address is selected), Interface, and Local Gateway.
- XAUTH (Top Left):** Shows Type set to Auto Server, User Group set to Inherit from policy, and a dropdown menu showing Auto Server selected.
- XAUTH (Top Right):** Shows Type set to Client, Username set to Training, and Password set to a masked value.
- Bottom Left:** A expanded dropdown menu for the XAUTH Type setting, showing options: Auto Server (selected), Disabled, PAP Server, CHAP Server.

**FOURINET Training Institute** is at the bottom left, and © Fortinet Inc. All Rights Reserved. 29 is at the bottom right.

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 the traffic exchanged between sites, one outbound and one inbound.

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**

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.

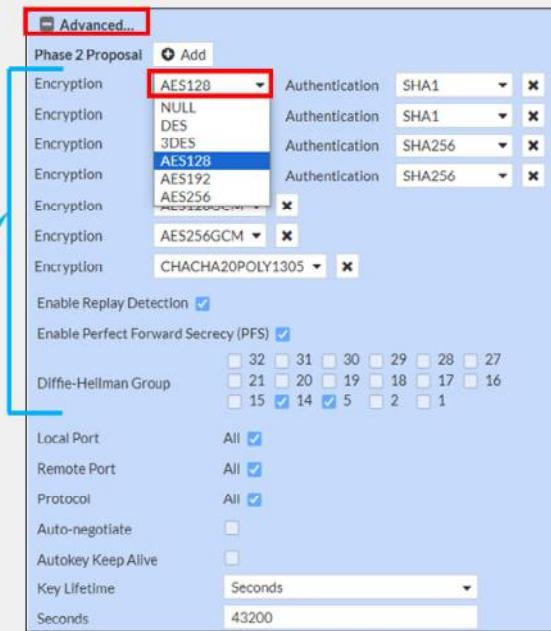
In addition, the phase 2 selector network parameters on both peers must match if the tunnel is point-to-point, that is, when the remote gateway is *not* set to dial-up user.

**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



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.

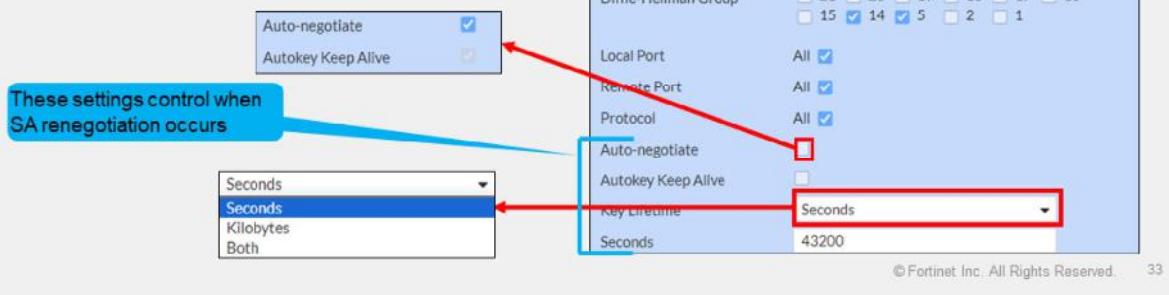
Also, if you enable **Perfect Forward Secrecy**, FortiGate uses DH to enhance security during the negotiation of IPsec SAs.

# 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



**FORTINET**  
Training Institute

© Fortinet Inc. All Rights Reserved.

33

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**

## 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



© Fortinet Inc. All Rights Reserved. 35

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

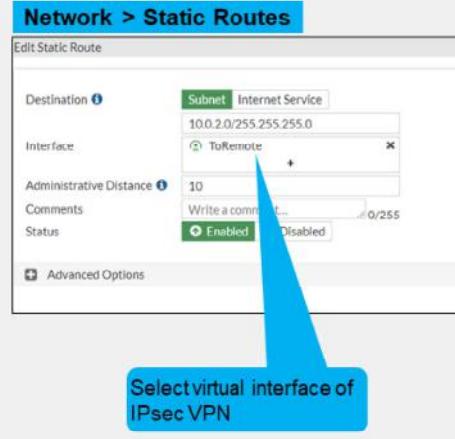
#### Dial-up user

```
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 separate 'Policy & Objects > Firewall Policy' windows.

**Left Window (Remote\_out):**

- Name: Remote\_out
- Incoming Interface: port3
- Outgoing Interface: ToRemote
- Source: LOCAL\_SUBNET
- Destination: REMOTE\_SUBNET
- Schedule: always
- Service: ALL
- Action: ACCEPT

**Right Window (Remote\_in):**

- Name: Remote\_in
- Incoming Interface: ToRemote
- Outgoing Interface: port3
- Source: REMOTE\_SUBNET
- Destination: LOCAL\_SUBNET
- Schedule: always
- Service: ALL
- Action: ACCEPT

Annotations explain the configuration:

- A blue arrow points from the 'ToRemote' outgoing interface in the first window to the 'ToRemote' incoming interface in the second window, with the text: "Virtual interface matches phase 1 name".
- A blue arrow points from the 'ACCEPT' button in the first window to the 'ACCEPT' button in the second window, with the text: "Allow and inspect the traffic coming from/going to the IPsec virtual interface".

**FORTINET**  
Training Institute

© Fortinet Inc. All Rights Reserved. 37

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

### IPsec VPN Status—IPsec Monitor Widget

- Monitor IPsec VPN tunnels
  - Display status and statistics
  - Bring up or bring down VPNs

Dashboard > Network > IPsec

VPN status

Bring down the entire tunnel or the phase 2 only

Data received Data sent

Phase 1 name and status Phase 2 name and status

All Phase 2 Selectors

Comments

More columns available

Apply Cancel

© Fortinet Inc. All Rights Reserved. 40

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 |
|----------|----------------|---------|
| Custom   |                |         |
| Dialup_0 | 10.9.15.30     |         |

Phase 2 is up

**Dashboard > Network > Static & Dynamic Routing**

| Route Lookup | Edit        | Create Address | Search   |
|--------------|-------------|----------------|----------|
| 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.

41

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 log interface with a table of events and a detailed log view for a specific entry.

**Log & Report > System Events > VPN Events**

| Date/Time           | Level  | Action           | Context | Message                        | VPN Tunnel |
|---------------------|--------|------------------|---------|--------------------------------|------------|
| 2023/09/13 06:24:16 | Notice | negotiate        | success | progress IPsec phase 2         | ToRemote   |
| 2023/09/13 06:24:16 | Notice | negotiate        | success | negotiate IPsec phase 2        | ToRemote   |
| 2023/09/13 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   |
| 2023/09/13 06:24:16 | Notice | phase2-up        |         | IPsec phase 2 status change    | ToRemote   |
| 2023/09/13 06:24:16 | Notice | install_sa       |         | Install IPsec SA               | ToRemote   |
| 2023/09/13 06:24:16 | Notice | negotiate        | success | progress IPsec phase 2         | ToRemote   |
| 2023/09/13 06:24:08 | Notice | negotiate        | success | progress IPsec phase 1         | ToRemote   |
| 2023/09/13 06:24:08 | Notice | negotiate        | success | progress IPsec phase 1         | ToRemote   |
| 2023/09/13 06:24:07 | Notice | delete_phase1_sa |         | delete IPsec phase 1 SA        | ToRemote   |
| 2023/09/13 06:24:07 | Notice | phase2-down      |         | IPsec phase 2 status change    | ToRemote   |
| 2023/09/13 06:24:07 | Notice | tunnel-down      |         | IPsec connection status change | ToRemote   |

**Phase 2 is up (tunnel is up)**

**Double-click any log to get more details**

**Log Details**

- General**
  - Absolute Date/Time: 2023-09-13 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

**Phase 1 is DONE (up)**

**FORTINET Training Institute**

© Fortinet Inc. All Rights Reserved. 42

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. 43

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 rcf=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

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
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
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>
```

When phase 1 was created

Is this gateway an initiator or responder?

Clear phase 1

**FORTINET**  
Training Institute

© Fortinet Inc. All Rights Reserved. 46

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<br>Enable NAT-Traversal |
| Tunnel is unstable                               | DPD packet lost                                       | ISP issue                                 | Check internet connection<br>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<br>Enable NAT-Traversal                            |



© Fortinet Inc. All Rights Reserved.

47

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?  
 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**

## Review

- ✓ Configure IPsec VPN manually
- ✓ Configure IPsec VPN using the IPsec wizard
- ✓ Configure 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



# FortiGate Administrator

## SD-WAN Configuration and Monitoring

FortiOS 7.4

Last Modified: 15 November, 2023

In this lesson, you will learn about the SD-WAN feature available on FortiGate.

**DO NOT REPRINT****© FORTINET**

## Objectives

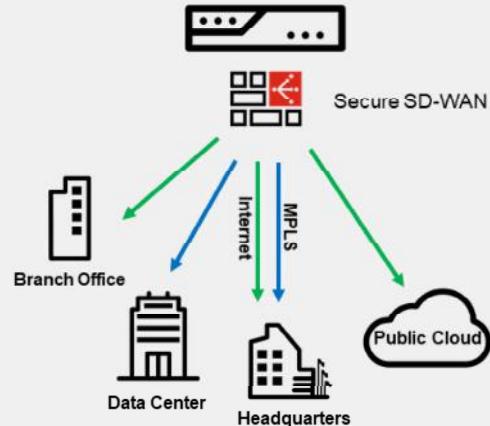
- Understand what SD-WAN is
- Identify the main use cases for SD-WAN
- Configure SD-WAN on FortiGate
- Understand and analyze routing behavior in an SD-WAN context
- Monitor SD-WAN behavior, link usage, and quality status

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

**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.

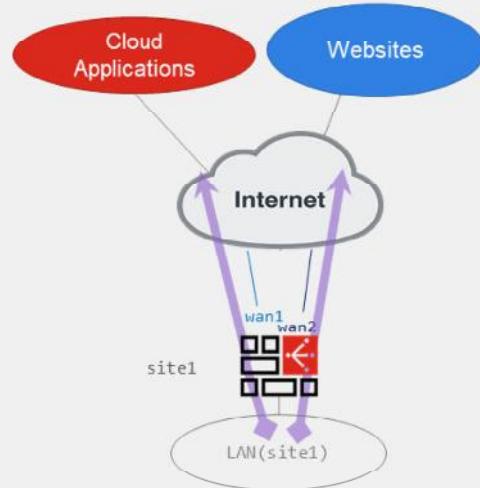
One benefit of SD-WAN is effective WAN use. That is, you can use public (for example, broadband or LTE) and private (for example, MPLS) links to securely steer traffic to different destinations: internet, public cloud, private cloud, and the corporate network. This approach of using different types of 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.

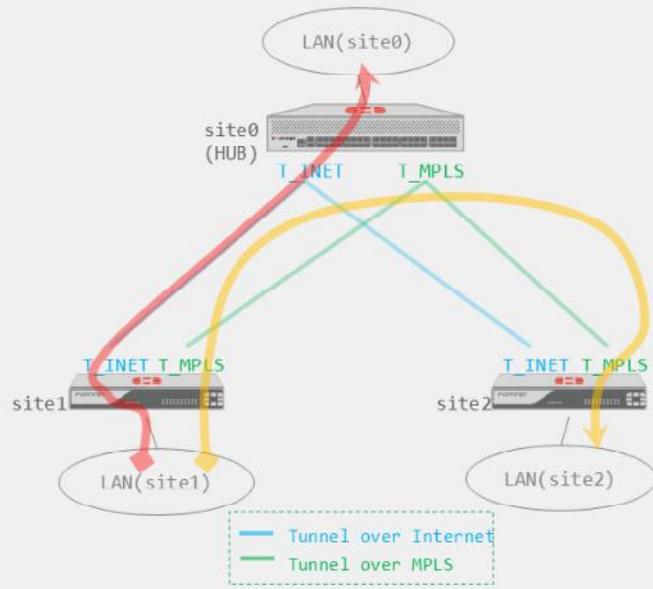
Because the internet traffic leaves the organization boundaries directly on the local site, administrators usually enforce strict security policies on the internet traffic. For routing, a typical configuration makes use of static default routes. However, in some cases, BGP is used between the ISP and 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



**FORTINET**  
 Training Institute

© Fortinet Inc. All Rights Reserved.

5

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.

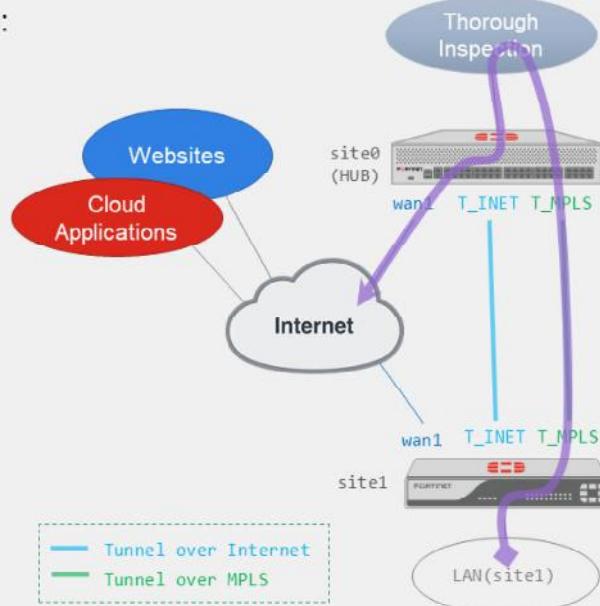
Similar to DIA, the hub FortiGate can run speed tests against the spokes to determine the upstream speed of tunnels. The hub FortiGate can then apply the speed test result as the upstream speed on the tunnel for traffic shaping purposes.

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**  
 Training Institute

© Fortinet Inc. All Rights Reserved.

6

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.

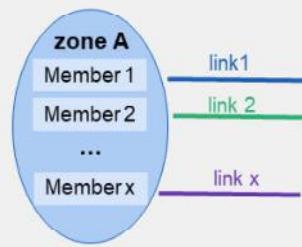
Another reason to use RIA is for DIA backup. For example, you could configure FortiGate to steer internet traffic through an MPLS link if the performance measured for internet applications on internet links is worse than on MPLS links, or simply if the internet links become unavailable.

**DO NOT REPRINT****© FORTINET**

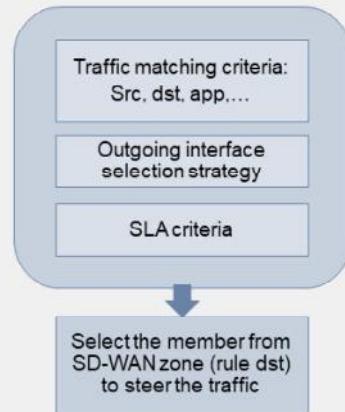
## SD-WAN Components

- 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

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 SLA members must meet
  - Strategy and quality criteria:
    - Manual, best quality, lowest cost
    - Latency, jitter, packet loss

| ID                  | Name             | Source       | Destination                                       | Criteria  | Members          | Performance SLA |
|---------------------|------------------|--------------|---------------------------------------------------|-----------|------------------|-----------------|
| <b>IPv4 (3)</b>     |                  |              |                                                   |           |                  |                 |
| 1                   | Critical-to-HQ   | LOCAL_SUBNET | HQ-Subnet                                         | Latency   | T_INET<br>T_MPLS | VPN_PING        |
| 2                   | Critical-DIA     | LOCAL_SUBNET | GoToMeeting<br>Microsoft.Office....<br>Salesforce |           | port1<br>port2   |                 |
| 3                   | Non-Critical-DIA | LOCAL_SUBNET | Facebook<br>Social.Media                          |           | port2<br>port1   |                 |
| <b>Implicit (1)</b> |                  |              |                                                   |           |                  |                 |
|                     | sd-wan           | all          | all                                               | Source IP | any              |                 |

SD-WAN rules combine traffic-matching criteria and traffic-steering preferences. They describe the administrator choices related to the SD-WAN solution and the software-defined aspect of it.

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 on a separate slide.

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 **Critical-to-HQ** which is used to steer critical traffic from the branch office to the headquarters. The rule steers traffic from LOCAL\_SUBNET to the HQ-Subnet through the overlay links (T\_INET and T\_MPLS). The member selection is done with a 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)

The screenshot shows the FortiGate SD-WAN Rules configuration interface. A vertical red arrow labeled 'Evaluation order' points downwards through the list of rules. A blue callout box labeled 'Implicit rule' points to the bottom-most row, which is highlighted with a red border. The table columns are: ID, Name, Source, Destination, Criteria, Members, Hit Count, and Last Used.

| ID                | Name           | Source       | Destination                                              | Criteria  | Members          | Hit Count | Last Used      |
|-------------------|----------------|--------------|----------------------------------------------------------|-----------|------------------|-----------|----------------|
| <b>IPv4 2</b>     |                |              |                                                          |           |                  |           |                |
| 1                 | Critical-to-HQ | LOCAL_SUBNET | HQ-Subnet                                                | Latency   | T_INET<br>T_MPLS | 0         | 43 minutes ago |
| 2                 | Critical-DIA   | LOCAL_SUBNET | GoToMeeting<br>Microsoft.Office.365.Portal<br>Salesforce |           | port1<br>port2   | 0         | 43 minutes ago |
| <b>Implicit 1</b> |                |              |                                                          |           |                  |           |                |
|                   | sd-wan         | all          | all                                                      | Source IP | any              |           |                |

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.

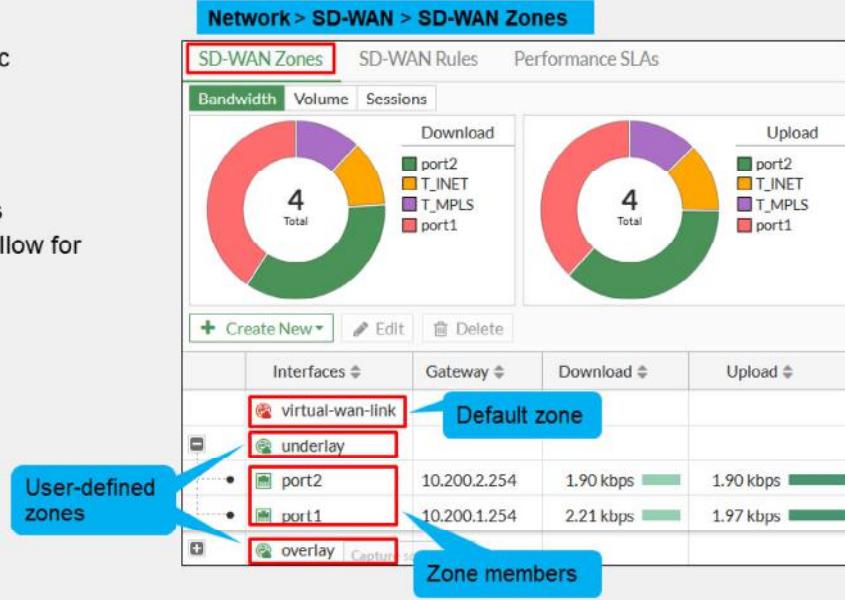
There is an implicit SD-WAN rule created by default. It is always present at the bottom of the SD-WAN rule list. If none of the user-defined SD-WAN rules are matched, then the implicit rule is used. This means that FortiGate routes the traffic according to the regular process. By default, the implicit 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/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/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/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.

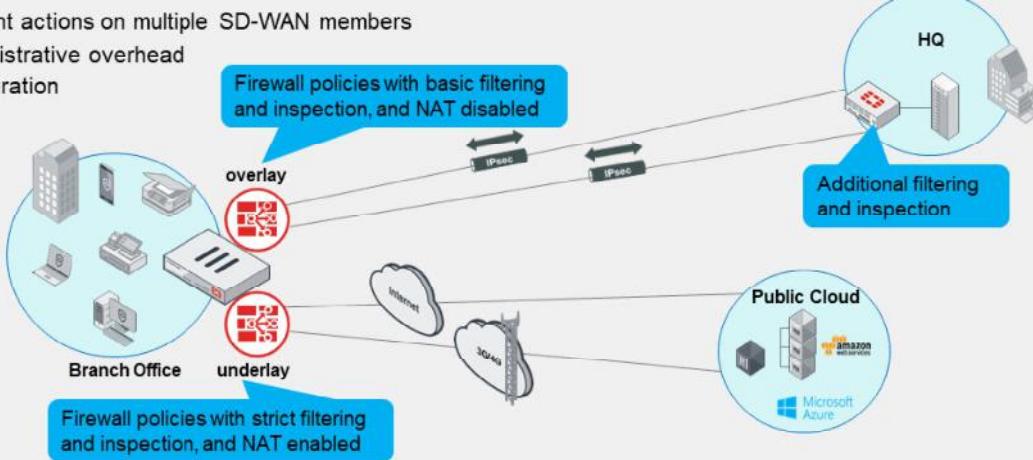
This slide shows the different underlay and overlay links supported by FortiGate as SD-WAN members.

# 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**  
Training Institute

© Fortinet Inc. All Rights Reserved.

12

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.

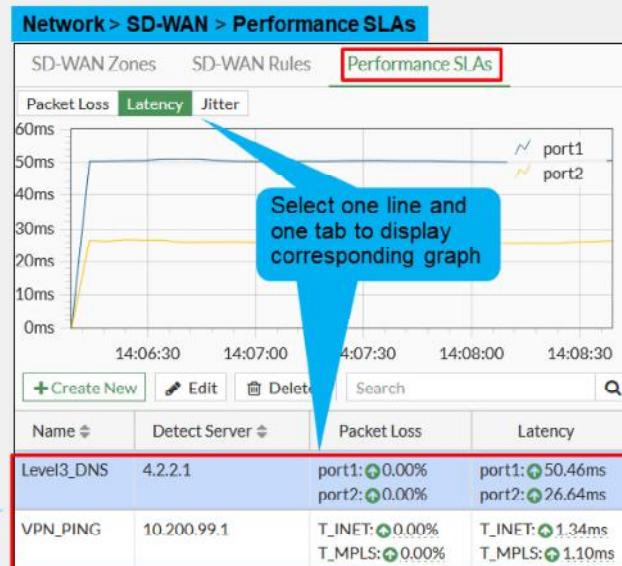
The topology shown on this slide shows a branch office with two SD-WAN zones configured: overlay and underlay. The overlay SD-WAN zone is composed of IPsec tunnels and the underlay SD-WAN zone is composed of an internet link and a 3G/4G link. The branch office uses the overlays to access the headquarter 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**  
Training Institute

© Fortinet Inc. All Rights Reserved. 13

After you define your SD-WAN members and assign them to zones, you will probably want to 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 **Level3\_DNS**. The entry contains the well-known **4.2.2.1** and **4.2.2.2** DNS 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 settings include:

- Name:** Level3.DNS
- Probe mode:** Active (selected)
- Protocol:** Ping, HTTP, DNS
- Server:** 4.2.2.1
- Participants:** All SD-WAN Members, Specify (selected), 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 (selected)

**FORTINET**  
Training Institute

© Fortinet Inc. All Rights Reserved. 14

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 of this slide shows the configuration of a performance SLA named `Level3_DNS`. 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 in **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.

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**

## Load Balancing Strategy

- Distribute traffic across multiple members
- Available as sub-strategy of:
  - Manual
    - Distribute among all available members
  - Lowest cost (SLA)
    - Distribute traffic out of all the interfaces that satisfy the SLA targets

The screenshot shows two configuration panels for SD-WAN Rules.

**Network > SD-WAN > SD-WAN Rules:** This panel shows the "Interface selection strategy". It has three options: "Manual" (selected), "Best quality", and "Lowest cost (SLA)". A callout bubble labeled "Strategy with load balancing option" points to the "Lowest cost (SLA)" option.

**Network > SD-WAN > SD-WAN Rules (bottom of menu):** This panel shows the "Load balancing" setting, which is currently enabled (indicated by a green switch icon). Other settings include "Measured SLA", "Required SLA target", and "Quality criteria" (Latency).

The load balancing strategies allow you to distribute the traffic among multiple SD-WAN members. To be eligible for traffic distribution the member must be alive, have a valid route to destination, and, in the case of **Lowest cost** strategy, meet the SLA target.

You can choose the load balancing strategy under the **Manual** and the **Lowest cost (SLA)** strategies. FortiGate applies load balancing as follows:

- Manual:** load balancing across all members available in the zone
- Lowest cost (SLA):** load balancing across all members that meet SLA targets

When you activate load balancing, by default, FortiGate distributes the traffic through all available members following the round-robin algorithm (sessions are distributed to selected interfaces in equal portions and circular order). Through CLI commands, you can select another load balancing algorithm. Some of the hash modes available are source-ip-based, source-dest-ip-based, and inbandwidth.

**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

The screenshot shows the 'Network > SD-WAN > SD-WAN Rules' interface. A red box highlights the 'Source' and 'Destination' sections. A blue callout bubble with the text 'Click to display internet service and application options' points to the 'Internet service' and 'Application' buttons in the 'Traffic criteria' section. To the right, a 'Select Entries' sidebar lists 'Application Categories (18)' including 'Business' and 'Cloud.IT'.

**FORTINET**  
 Training Institute

© Fortinet Inc. All Rights Reserved.

17

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**

## Firewall Policies With SD-WAN

- Steered traffic *must* be allowed by a firewall policy
- Reference normalized interface for SD-WAN zones only
  - Simplified configuration
- Can't reference a member directly

| ID | Name             | From    | To       | Source        | Destination   | Schedule | Service              | Action | NAT      |
|----|------------------|---------|----------|---------------|---------------|----------|----------------------|--------|----------|
| 1  | To-Hub-Overlay   | port3   | overlay  | LOCAL_SUBNET  | REMOTE_SUBNET | always   | ALL                  | ACCEPT | Disabled |
| 2  | From Hub-Overlay | overlay | port3    | REMOTE_SUBNET | LOCAL_SUBNET  | always   | ALL                  | ACCEPT | Disabled |
| 3  | DIA              | port3   | underlay | LOCAL_SUBNET  | all           | always   | FTP<br>HTTP<br>HTTPS | ACCEPT | NAT      |
| 0  | Implicit Deny    | any     | any      | all           | all           | always   | ALL                  | DENY   |          |

**Normalized interface for LAN port (individual)**

**SD-WAN zones**

**FORTINET Training Institute**

© Fortinet Inc. All Rights Reserved. 18

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 a normalized 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 normalized 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

**Matching criteria:**

- If Incoming traffic matches:
- Incoming Interface: port5
- Source Address: IP/Netmask: 10.0.1.0/24
- Destination Address: IP/Netmask: 10.10.10.10/32
- Protocol: TCP
- Source ports: 0 - 65535
- Destination ports: 10444 - 10444
- Type of service: 0x00 Bit Mask: 0x00

**Action:**

- Action: Forward Traffic
- Outgoing Interface: port1
- Gateway address: 192.2.0.2

Status: Enabled

**FORTINET**  
Training Institute

© Fortinet Inc. All Rights Reserved. 19

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**

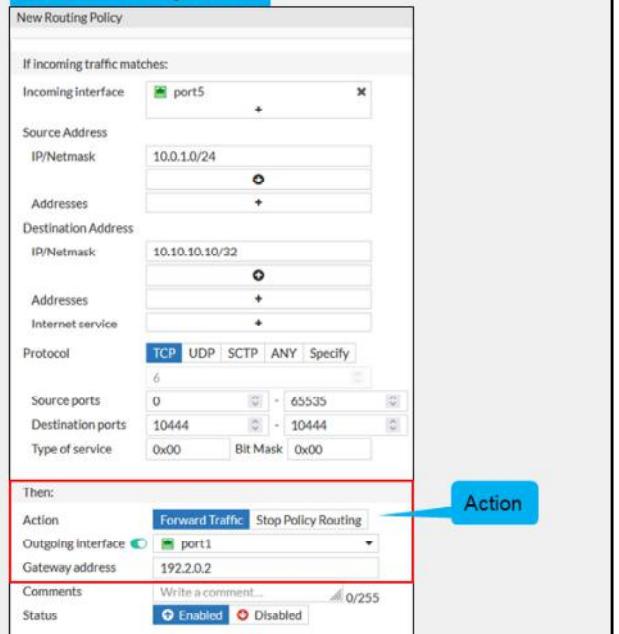
## Policy Route—Actions

- **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
- IP/Netmask: 10.10.10.10/32
- Addresses: (empty)
- Destination Address: 10.10.10.10/32
- IP/Netmask: 10.10.10.10/32
- Addresses: (empty)
- Internet service: (empty)

Protocol: TCP (selected)

Source ports: 0 - 65535

Destination ports: 10444 - 10444

Type of service: 0x00 Bit Mask: 0x00

Then:

|                     |                          |                     |
|---------------------|--------------------------|---------------------|
| Action:             | Forward Traffic          | Stop Policy Routing |
| Outgoing Interface: | port1                    | (dropdown menu)     |
| Gateway address:    | 192.2.0.2                |                     |
| Comments:           | Write a comment... 0/255 |                     |
| Status:             | Enabled                  | Disabled            |

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... | Interface | Status  | Comments |  |
| 0.0.0.0/0               |            | underlay  | Enabled |          |  |

A zone can be referenced

|                                                                             |
|-----------------------------------------------------------------------------|
| # get router info routing-table all<br>...omitted output...                 |
| S* 0.0.0.0/0 [1/0] via 10.200.1.254, port1<br>[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 'Edit Static Route'. The left panel shows a route for '0.0.0.0/0.0.0.0' via 'underlay' interface, which is highlighted as 'SD-WAN zone'. The right panel shows a route for '8.8.8.8/255.255.255.255' via 'port1', with 'Gateway' set to '10.200.1.199'. A callout indicates this is a 'Specific member from an SD-WAN zone'. Below the interface are two routing table entries:

```
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 entries: 'Individual ECMP routes for each member in the zone' points to the first entry; 'Part of SD-WAN zone' points to the second entry; and 'As individual interface' points to the gateway entry.

**Fortinet Training Institute**

© Fortinet Inc. All Rights Reserved. 22

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**

## Routing Behavior in an SD-WAN Context—Key Principles

- SD-WAN rules are policy routes
- Regular policy routes have precedence over SD-WAN rules
- Route lookup is done for new and dirty sessions
  - For original and reply traffic
  - Includes policy route lookup
- By default, SD-WAN rules are skipped if:
  - Best route to the destination isn't an SD-WAN member
  - None of the members have a valid route to the destination
  - If the preferred member doesn't have a valid route to the destination, the next member in the rule is checked
- Implicit SD-WAN rule equals standard forwarding information base (FIB) lookup
  - If lookup matches ECMP routes, traffic is load balanced using the configured algorithm

Routing is a core component of SD-WAN. Understanding how routing works in SD-WAN is essential for design and troubleshooting. The following are the SD-WAN key routing principles:

- SD-WAN rules are policy routes. Like regular policy routes, SD-WAN rules route traffic based on multiple criteria. That is, when you configure an SD-WAN rule, the kernel installs a corresponding policy route that reflects the source, destination, service, and outgoing interfaces configured in the SD-WAN rule.
- Regular policy routes have precedence over SD-WAN rules. Therefore, if you configure regular policy routes, you should ensure that their matching criteria is as narrow as possible. Otherwise, traffic that is intended to be handled by SD-WAN could end up being handled by regular policy routes instead.
- FortiGate performs route lookup on both new and dirty sessions. A dirty session is a session that must be re-evaluated by the kernel after it is impacted by a routing, firewall policy, or interface change. FortiGate performs route lookups for both original and reply traffic. During route lookup, FortiGate also checks policy routes.
- By default, FortiGate skips SD-WAN rules if the best route to the destination isn't an SD-WAN member. If the best route matches an SD-WAN member, then the selected member in the rule must have a valid route to the destination, otherwise FortiGate skips the member, and checks the next best member. If none of the members have a valid route to the destination, then FortiGate skips the rule.
- The implicit SD-WAN rule equals standard FIB lookup. That is, if the traffic doesn't match any of the SD-WAN rules, then FortiGate routes the traffic using the regular process, which consists of looking for the best route in the FIB. If the best route matches equal cost multipath (ECMP) routes—usually the case—then FortiGate load balances the traffic using the configured load balancing algorithm.

**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

| Relative Date/Time | Source     | Destination          | Destination Interface | Application Name | Result                        | Policy ID          | SD-WAN Rule Name |
|--------------------|------------|----------------------|-----------------------|------------------|-------------------------------|--------------------|------------------|
| 29 seconds ago     | 10.0.1.10  | 10.0.2.10            | T_MPLS                | FTP              | ✓ Accept (60 B / 40 B)        | 1 (To-Hub-Overlay) | Critical-to-HQ   |
| 2 minutes ago      | 10.0.1.200 | 96.45.45.45          | port2                 | tcp/853          | ✓ Accept (9.57 kB / 14.7 kB)  | 3 (DIA)            |                  |
| 2 minutes ago      | 10.0.1.200 | 96.45.45.45          | port2                 | tcp/853          | ✓ Accept (9.42 kB / 14.52 kB) | 3 (DIA)            |                  |
| 2 minutes ago      | 10.0.1.10  | 8.8.8.8 (dns.google) | port1                 | PING             | ✓ Accept (49.98 kB / 0 B)     | 3 (DIA)            |                  |
| 4 minutes ago      | 10.0.1.10  | 8.8.8.8 (dns.google) | port1                 | PING             | ✓ Accept (39.98 kB / 0 B)     | 3 (DIA)            |                  |
| 4 minutes ago      | 10.0.1.200 | 96.45.45.45          | port2                 | tcp/853          | ✓ Accept (8.76 kB / 12.94 kB) | 3 (DIA)            |                  |

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**

## Check Policy Routes Created by SD-WAN Rules

- SD-WAN rules create policy route-like entries
- Visible in Policy Route Table
- CLI command  
diagnose firewall proute list
- Shows:
  - Policy routes ( $ID \leq 65535$ )
  - ISDB routes
  - SD-WAN routes
- Do not show:
  - Static route
  - Dynamic routes (OSPF, BGP,...)
- Remember that policy routes take precedence over SD-WAN routes

```
diagnose firewall proute list
list route policy info(vf=root):

id=1 dscp_tag=0xff flags=0x0 tos=0x00 tos_mask=0x00
protocol=0 sport=0- iif=7 dport=0-65535 path(1) oif=21(T_MPLS)
source(1): 10.0.1.0-10.0.1.255
destination(1): 10.0.0.0-10.255.255.255
hit_count=18 last_used=2023-08-14 05:47:21
This is a regular policy route
(ID ≤ 65535)

id=2113929223 static_route=7 dscp_tag=0xff 0xff flags=0x0 tos=0x00
tos_mask=0x00 protocol=0 sport=0-0 iif=0 dport=1 65535 path(1)
oif=3(port1) gwy=192.2.0.2
source wildcard(1): 0.0.0.0/0.0.0.0
destination wildcard(1): 0.0.0.0/0.0.0.0
internet service(1): Fortinet-FortiGuard(1245324,0,0,0)
hit_count=0 last_used=2023-08-14 06:39:07
This is an ISDB route
(ID > 65535 and no vwl_service field)

id=2130903041(0x7f030001) vwl_service=1(Critical-DIA)
vwl_mbr_seq=1 2 dscp_tag=0x11 0x11 flags=0x0 tos=0x00
tos_mask=0x00 protocol=0 sport=0-65535 iif=0 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(4294837474,0,0,0, 41468)
Microsoft.Office.365.Portal(4294837474,0,0,0, 41468)
Salesforce(4294837976,0,0,0, 16920)
hit_count=0 last_used=2023-08-14 05:46:43
This is an SD-WAN rule
(ID > 65535 and
the vwl_service field is present)
```



© Fortinet Inc. All Rights Reserved.

25

FortiOS maintains a policy route table that you can view by running the `diagnose firewall proute list` command.

There are three types of policy routes displayed in the policy route table: regular policy routes, ISDB routes, and SD-WAN rules. Follow these rules to identify each type of policy route in the table:

- Regular policy routes are assigned an ID no higher than 65535. In the output shown on this slide, the first entry is assigned ID 1, which makes it a regular policy route.
- ISDB routes and SD-WAN rules are assigned an ID higher than 65535. However, SD-WAN rule entries include the `vwl_service` field, and ISDB route entries don't. The `vwl_service` field indicates the ID and the name of the rule from the SD-WAN configuration perspective. In the output shown on this slide, the second entry is an ISDB route and the third entry an SD-WAN rule.

In the output of some CLI commands related to SD-WAN you will notice some entries with VWL like `vwl_service` or `vwl_mbr_seq`. `vwl` stands for Virtual Wan Link, it corresponds to the former naming of SD-WAN.

**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

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=2023-08-24 04:04:15

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=2023-08-23 11:31:42
```

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
```

**Firewall policy ID**

**App ID (SSH)**

**SD-WAN member and rule IDs**

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



© Fortinet Inc. All Rights Reserved. 28

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 shows the Network dashboard with three main sections:

- Static & Dynamic Routing:** A donut chart showing 11 total routes, with 11 IPv4 routes.
- IPsec:** A table listing two tunnels:
 

| Name   | Remote Gateway | Peer ID    |
|--------|----------------|------------|
| T_INET | 10.200.4.1     | 10.200.4.1 |
| T_MPLS | 10.200.3.1     | 10.200.3.1 |
- SD-WAN:** A section with three sub-widgets:
  - A donut chart showing 4 SD-WAN links.
  - A chart showing Packet Loss levels (Low, Medium, High).
  - A chart showing Latency levels (Low, Medium, High).

A red box highlights the SD-WAN section, and a blue arrow points from a "Click to expand" callout to the SD-WAN interface table below. The table lists four interfaces with their status, sessions, upload, and download speeds:

| Interface | Status | Sessions | Upload    | Download  |
|-----------|--------|----------|-----------|-----------|
| port2     | Up     | 2 1      | 3.78 kbps | 4.33 kbps |
| T_INET    | Up     | 7 ■      | 640 bps   | 422 bps   |
| T_MPLS    | Up     | 1 1      | 640 bps   | 640 bps   |
| port5     | Up     | 46 ■■■■  | 3.26 kbps | 2.59 kbps |

**FORTINET**  
Training Institute

© Fortinet Inc. All Rights Reserved. 29

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

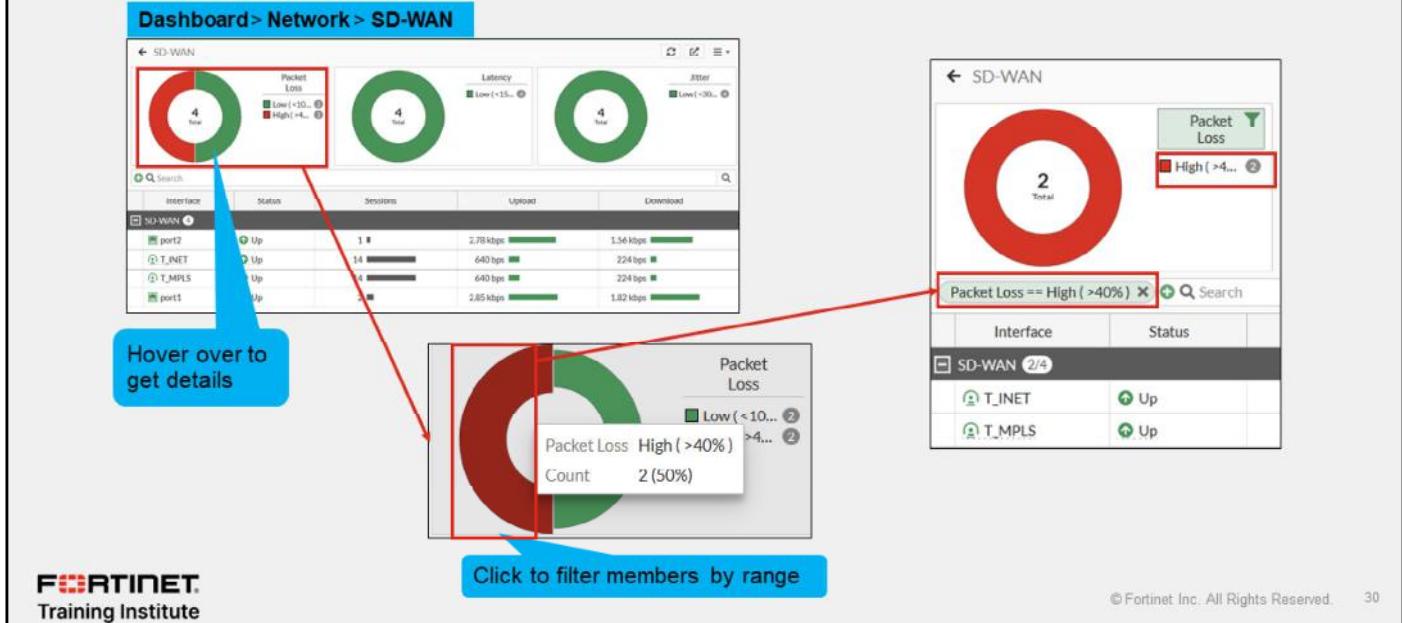
Click any widget to expand and get additional details per topic. The SD-WAN widget provides an overview of the status of each monitored SD-WAN link.

The example on this slide shows the details you can view by clicking the SD-WAN widget. Note that the packet loss diagram reports that one interface is at medium level, which means between 10%-40% of packet loss.

**DO NOT REPRINT**  
**© FORTINET**

## Dashboard—SD-WAN Widget details

- Consolidated view of member health and utilization



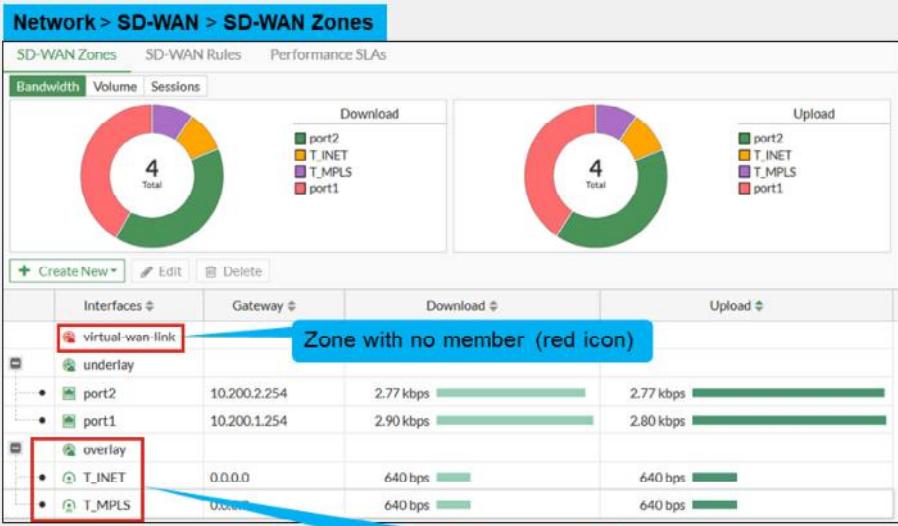
From the SD-WAN widget detailed view, you can hover over the graph to view details. You can also click a graph part to filter the member list and display only the members that match the selected criteria.

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 screenshot shows the SD-WAN Zones page with two donut charts at the top: one for Download traffic and one for Upload traffic, both divided into four segments: port2 (green), T\_INET (yellow), T\_MPLS (purple), and port1 (red). Below the charts is a table listing SD-WAN zones and their members. A red box highlights the 'virtual-wan-link' zone, which has a red icon and no members listed. A blue callout box says 'Zone with no member (red icon)'. Another red box highlights the 'overlay' zone, which has members T\_INET and T\_MPLS listed. A blue callout box says 'Zone with members, expanded to view members' details'. The table data is as follows:

| Interfaces       | Gateway      | Download  | Upload    |
|------------------|--------------|-----------|-----------|
| virtual-wan-link |              |           |           |
| underlay         |              |           |           |
| port2            | 10.200.2.254 | 2.77 kbps | 2.77 kbps |
| port1            | 10.200.1.254 | 2.90 kbps | 2.80 kbps |
| overlay          |              |           |           |
| T_INET           | 0.0.0.0      | 640 bps   | 640 bps   |
| T_MPLS           | 0.0.0.0      | 640 bps   | 640 bps   |

**FORTINET.**  
Training Institute

© Fortinet Inc. All Rights Reserved. 31

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**  
Training Institute

© Fortinet Inc. All Rights Reserved. 32

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

Network > SD-WAN > SD-WAN Rules

| ID                | Name             | Source       | Destination                                              | Criteria  | Members          | Hit Count | Last Used    | Performance SLA |
|-------------------|------------------|--------------|----------------------------------------------------------|-----------|------------------|-----------|--------------|-----------------|
| <b>IPv4 3</b>     |                  |              |                                                          |           |                  |           |              |                 |
| 1                 | Critical-to-HQ   | LOCAL_SUBNET | HQ-Subnet                                                | Latency   | T_INET<br>T_MPLS |           | 11 hours ago | VPN_PING        |
| 2                 | Critical-DIA     | LOCAL_SUBNET | GoToMeeting<br>Microsoft.Office.365.Portal<br>Salesforce |           | port1<br>port2   | 0         | 16 hours ago |                 |
| 3                 | Non-Critical-DIA | LOCAL_SUBNET | Facebook<br>Social.Media<br>General.Interest             |           | port2<br>port1   | 0         | 12 hours ago |                 |
| <b>Implicit 1</b> |                  |              |                                                          |           |                  |           |              |                 |
|                   | sd-wan           | all          | all                                                      | Source IP | any              |           |              |                 |

**FORTINET**  
Training Institute

© Fortinet Inc. All Rights Reserved. 33

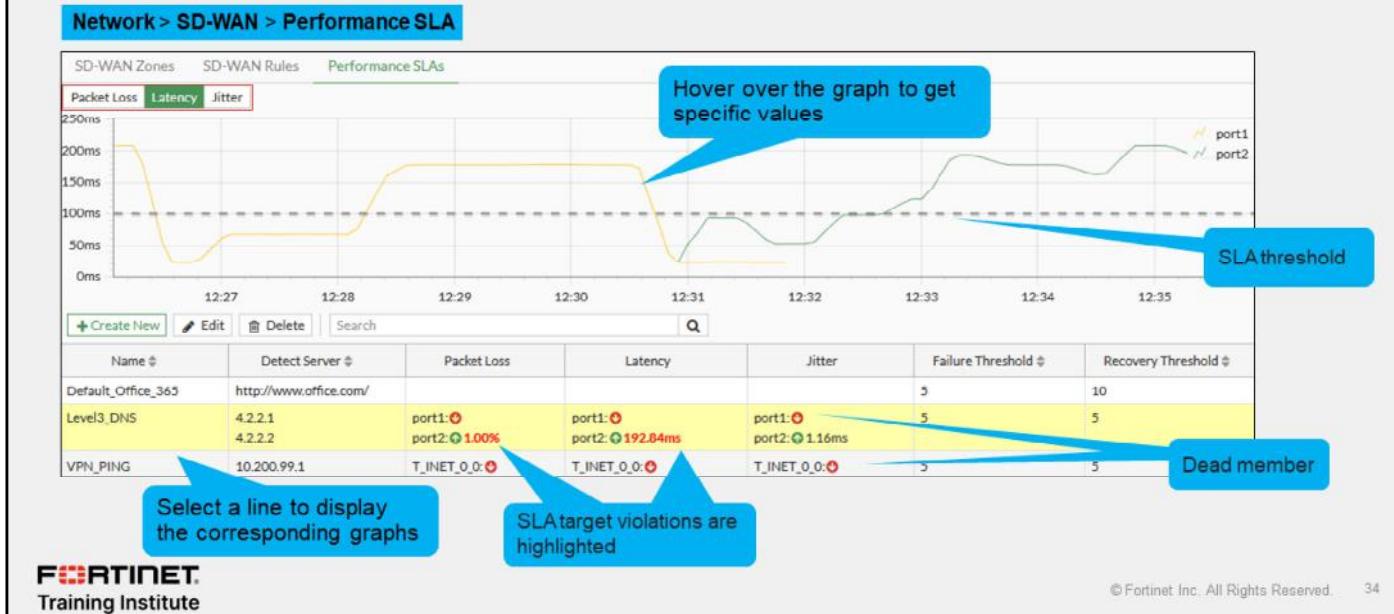
The **SD-WAN Rules** page in the menu **Network > SD-WAN**, provides a summary view of SD-WAN rules configuration. From this list you can quickly view the main configuration parameters of a rule, members in use, and the last time the rule was used to steer traffic. With drag-and-drop you can re-order 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 (Level3\_DNS in the example). The graphs on the page will 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 10 minutes.

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 **Level3\_DNS** performance SLA is selected and reports that **port2** is alive and **port1** is dead. The graph shows latency for both monitored interfaces over the past 10 minutes.

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

**Log & Report > System Events**

Summary | Logs  
1,931 Events

VPN Events (0)

| Top Event               | Level  | Count |
|-------------------------|--------|-------|
| Progress IPsec phase 1  | Notice | 452   |
| Negotiate IPsec phase 1 | Notice | 137   |
| Progress IPsec phase 2  | Notice | 121   |
| Phase 2                 | Notice | 110   |
| Phase 2                 | Notice | 110   |

General System Events (0)

| Top Event                   | Level       | Count |
|-----------------------------|-------------|-------|
| FortiGate update succeeded  | Notice      | 47    |
| Object attribute configured | Information | 12    |
| Automation stitch triggered | Notice      | 7     |
| Admin login successful      | Information | 4     |
| Admin logout successful     | Information | 3     |

SD-WAN Events (0)

| Top Event                     | Level       | Count |
|-------------------------------|-------------|-------|
| SDWAN status                  | Notice      | 772   |
| SDWAN SLA notification        | Notice      | 11    |
| SDWAN SLA information warning | Warning     | 7     |
| SDWAN status information      | Information | 2     |
| SDWAN status warning          | Warning     | 2     |

Security Rating Events (0)

| Top Event                     | Level  | Count |
|-------------------------------|--------|-------|
| Security Rating summary       | Notice | 21    |
| Security Rating result change | Notice | 2     |

Select time duration of summary widget display

24 hours | 5 minutes | 1 hour | 24 hours

SD-WAN event log summary

Click a line to filter on event type

**FORTINET**  
Training Institute

© Fortinet Inc. All Rights Reserved. 35

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

Log & Report > System Events > SD-WAN Events

| Relative Da... | Level           | Message                                                                 | Log Description               |
|----------------|-----------------|-------------------------------------------------------------------------|-------------------------------|
| 2 hours ago    | ■■■■■■■ Notice  | Service will be redirected in sequence order.                           | SDWAN status                  |
| 2 hours ago    | ■■■■■■■ Notice  | Member link is unreachable or miss threshold. Stop forwarding traffic.  | SDWAN status                  |
| 2 hours ago    | ■■■■■■■ Notice  | Service will be redirected in sequence order.                           | SDWAN status                  |
| 2 hours ago    | ■■■■■■■ Notice  | Member link is unreachable or miss threshold. Stop forwarding traffic.  | SDWAN status                  |
| 2 hours ago    | ■■■■■■■ Notice  | Service prioritized by performance metric will be redirected in sequ... | SDWAN status                  |
| 2 hours ago    | ■■■■■■■ Notice  | Member link is unreachable or miss threshold. Stop forwarding traffic.  | SDWAN status                  |
| 2 hours ago    | ■■■■■■■ Notice  | Number of pass member changed.                                          | SDWAN status                  |
| 2 hours ago    | ■■■■■■■ Notice  | Member status changed. Member out-of-sla.                               | SDWAN status                  |
| 2 hours ago    | ■■■■■■■ Warning | SD-WAN health-check member changed state.                               | SDWAN SLA information warning |
| 2 hours ago    | ■■■■■■■ Warning | SD-WAN health-check member changed state.                               | SDWAN SLA information warning |
| 2 hours ago    | ■■■■■■■ Notice  | Number of pass member changed.                                          | SDWAN status                  |
| 2 hours ago    | ■■■■■■■ Notice  | Member status changed. Member out-of-sla.                               | SDWAN status                  |
| 2 hours ago    | ■■■■■■■ Notice  | Member status changed. Member out-of-sla.                               | SDWAN status                  |
| 2 hours ago    | ■■■■■■■ Notice  | SD-WAN Health Check member(s) pass.                                     | SDWAN status                  |

port2 removed from the member preference list

Log details:  
Member state changed from alive to dead for port2

| Log Details                  |                                           |
|------------------------------|-------------------------------------------|
| General                      |                                           |
| Source                       |                                           |
| Interface                    | port2                                     |
| Data                         |                                           |
| Message                      | SD-WAN health-check member changed state. |
| Security                     |                                           |
| Level                        | ■■■■■■■ Warning                           |
| Other                        |                                           |
| Log event original timestamp | 1694398725897871400                       |
| Timezone                     | -0700                                     |
| Log ID                       | 0113022931                                |
| Type                         | event                                     |
| Sub Type                     | sdwan                                     |
| Event Type                   | Health Check                              |
| Health Check                 | Level3_DNS                                |
| Probe Protocol               | dns                                       |
| Old Value                    | alive                                     |
| New Value                    | dead                                      |

FORTINET  
Training Institute

Warning: port2 is detected dead  
and stopped forwarding traffic

© Fortinet Inc. All Rights Reserved. 36

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 above 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

**Log & Report > Forward Traffic**

| Date/Time  | Source     | Destination                        | Application Name           | Result               | Policy ID           | SD-WAN Rule Name | SD-WAN Quality                                     |
|------------|------------|------------------------------------|----------------------------|----------------------|---------------------|------------------|----------------------------------------------------|
| Minute ago | 10.0.1.101 | 172.232.20.35 (www.salesforce.com) | Salesforce                 | ✓ UTM Allowed        | LAN-to-underlay (1) | Critical-DIA     | Seq_num(1 port1), alive, latency: 23.558, selected |
| Minute ago | 10.0.1.101 | 157.240.3.35 (www.facebook.com)    | Facebook                   | ✓ 2.99 kB / 49.54 kB | LAN-to-underlay (1) | Non-Critical-DIA | Seq_num(2 port2), alive, selected                  |
| Minute ago | 10.0.1.101 | 104.244.42.193 (twitter.com)       | Twitter                    | ✓ UTM Allowed        | LAN-to-underlay (1) |                  |                                                    |
| Minute ago | 10.0.1.101 | 104.244.42.1 (twitter.com)         | Twitter                    | ✓ UTM Allowed        | LAN-to-underlay (1) |                  |                                                    |
| Minute ago | 10.0.1.101 | 31.13.80.36 (www.facebook.com)     | Facebook                   | ✓ 3.10 kB / 49.37 kB | LAN-to-underlay (1) |                  |                                                    |
| Minute ago | 10.0.1.101 | 13.107.9.156 (www.office.com)      | Microsoft.Offce.365.Portal | ✓ 1.75 kB / 29.47 kB | LAN-to-underlay (1) |                  |                                                    |
| Minute ago | 10.0.1.101 | 13.107.9.156 (www.office.com)      | Microsoft.Offce.365.Portal | ✓ 1.75 kB / 29.43 kB | LAN-to-underlay (1) |                  |                                                    |
| Minute ago | 10.0.1.101 | 13.107.9.156 (www.office.com)      | GoToMeeting                | ✓ UTM Allowed        | LAN-to-underlay (1) | Critical-DIA     | Seq_num(1 port1), alive, latency: 23.481, selected |
| Minute ago | 10.0.1.101 | 13.107.9.156 (www.office.com)      | Salesforce                 | ✓ UTM Allowed        | LAN-to-underlay (1) | Critical-DIA     | Seq_num(1 port1), alive, latency: 23.481, selected |

**Available columns**

**Select Columns**

- ✓ Destination
- ✓ Application Name
- ✓ Result
- ✓ Policy Name
- ✓ Destination Interface
- ✓ SD-WAN Quality
- ✓ SD-WAN Rule Name
- ✓ SD-WAN Internet Service
- ✓ SD-WAN Rule ID

**Rule name**

**Selected member and reason**

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 37

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 indicates the matched SD-WAN rule for a session, and the latter the member the session was steered to 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 first session in the table was identified as a **Salesforce** application, matched the **Critical-DIA** rule, and was sent to port1. The reason that port1 was selected was because it had the lowest latency.

The second session in the table, which was identified as a **Facebook** application, matched the **Non-Critical-DIA** rule, and was sent to port2. The **Non-Critical-DIA** rule instructs FortiGate to steer matching traffic to port2 only, provided the port is alive. This behavior matches the reason described in the **SD-WAN Quality** column for that session.

**DO NOT REPRINT****© FORTINET**

## Knowledge Check

1. Which 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. Which menu will you use to review the history of SD-WAN events?  
 A. Forward Traffic in Log & Report  
 B. SD-WAN widget on the Dashboard  
 C. SD-WAN widget in System Events

**DO NOT REPRINT**

**© FORTINET**

## Review

- ✓ Understand what SD-WAN is
- ✓ Identify the main use cases for SD-WAN
- ✓ Configure SD-WAN on FortiGate
- ✓ Understand and analyze routing behavior in an SD-WAN context
- ✓ Monitor SD-WAN behavior, link usage, and quality status



© Fortinet Inc. All Rights Reserved. 39

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

# FortiGate Security

## Security Fabric

FortiOS 7.4



Last Modified: 15 November 2023

In this lesson, you will learn about the Fortinet Security Fabric.

**DO NOT REPRINT****© FORTINET**

## Objectives

- Configure the Security Fabric
- Monitor physical and logical topology views
- Run and analyze the Security Fabric rating

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

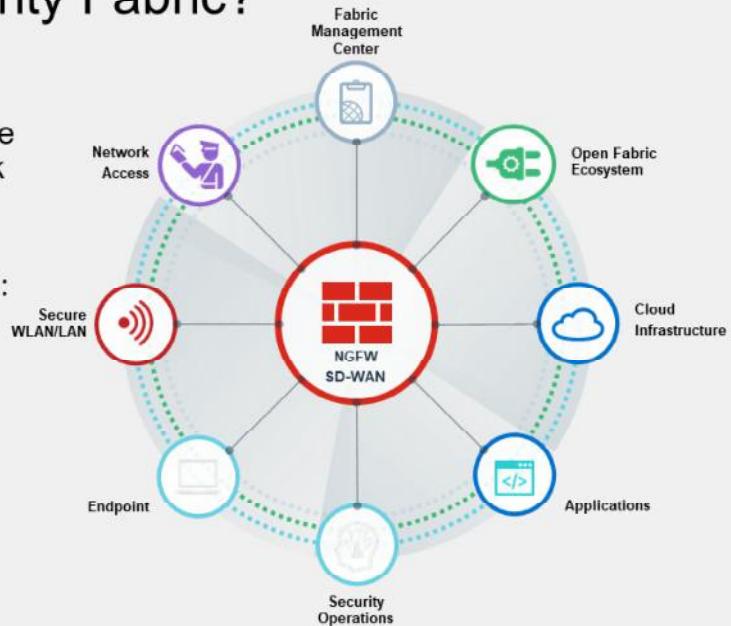
By demonstrating a competent understanding of key concepts of the Fortinet Security Fabric, you will better understand the value of the Security Fabric, the servers that comprise it, how to deploy it, and how it helps to manage all your network devices more efficiently and from a single point of view.

# DO NOT REPRINT

## © FORTINET

### What is the Fortinet Security Fabric?

- An enterprise solution that enables a holistic approach to network security, whereby the network landscape is visible through a single console and all network devices are integrated into a centrally managed and automated defence
- The Security Fabric has these attributes:
  - Broad
  - Integrated
  - Automated
- The API allows for third-party device integration



**FORTINET**  
Training Institute

© Fortinet Inc. All Rights Reserved.

3

#### What is the Fortinet Security Fabric?

It is a Fortinet enterprise solution that enables a holistic approach to network security, whereby the network landscape is visible through a single console and all network devices are integrated into a centrally managed and automated defence.

The network devices include all components, from physical endpoints to virtual devices in the cloud. Because devices are centrally managed and are sharing threat intelligence with one another in real time, and are receiving updates from Fortinet at the macro level, your network can quickly identify, isolate, and neutralize threats as they appear.

The Security Fabric has the following attributes:

- **Broad:** It provides visibility of the entire digital attack surface to better manage risk
- **Integrated:** It provides a solution that reduces the complexity of supporting multiple point products
- **Automated:** Threat intelligence is exchanged between network components in real-time allowing for automated response to threats

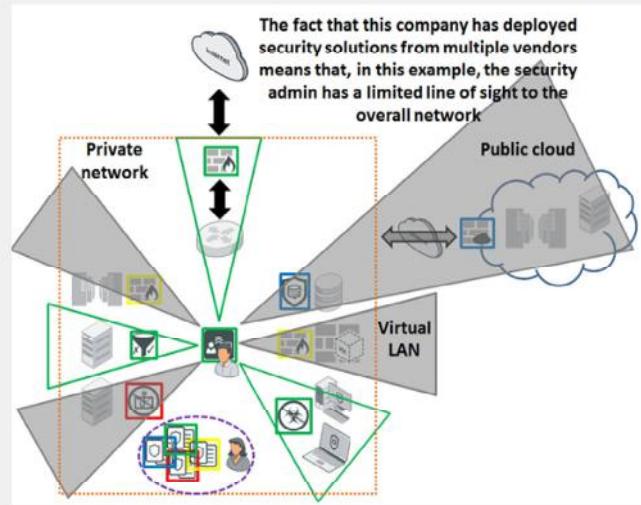
A fourth attribute could be added to this description of the Security Fabric: *open*. The API and protocol are available for other vendors to join and for partner integration. This allows for communication between Fortinet and third-party devices.

**DO NOT REPRINT**

**© FORTINET**

## Why a Security Fabric?

- Many administrators lack visibility of their network defences, making their networks more susceptible to undetected network infiltration
- Network complexity and sophisticated malware (soon to be augmented by AI), necessitates a centralized and holistic approach to security



Why has Fortinet deemed the Security Fabric an essential solution for a robust network defence?

As networks evolved and various new types of threats surfaced, point security products were deployed to address these emerging threats. Often, these piecemeal solutions were effective, but deploying products using different standards and protocols meant that defence assets could not be effectively coordinated.

The illustration on the right side of the slide tells a story of a network that has deployed security solutions from four different vendors. The administrator at the center, working from the security console, has visibility into only some of the security solutions. This lack of visibility of the entire network defence is a serious flaw, and could allow a foreign infiltrator to breach network defences undetected.

The sheer complexity of today's networks compounds this problem. In addition, increasingly sophisticated malware has an expanding attack surface on which to exploit, because networks have broken out of the confines of a traditional network perimeter and have expanded to virtualized networks and public clouds. Add to this mix, the ever growing numbers of unmanaged devices, as a result of BYOD programs, and you have the perfect security storm.

The most feasible solution is to build a centrally managed, holistic approach to security, whereby you have a clear line of sight to all potential infiltration points and can coordinate defences to contain and neutralize network breaches.

# DO NOT REPRINT

## © FORTINET

## Security Fabric Products

- Different consumption models available



As shown on this slide, the Fortinet Security Fabric offers eight solutions: network access, security WLAN/LAN, public and private cloud infrastructure, applications, endpoint, security operations, open fabric ecosystem, and fabric management center. Each of these solutions is based on specific use cases and involve the integration of specific Fortinet products.

The Fortinet Security Fabric offers network security with FortiGate, IPS, VPN, SD-WAN. It also offers multi-cloud strategy across public clouds, private clouds, hybrid clouds, and software as a service (SaaS). It also offers quite a sophisticated endpoint offering ranging from the Fabric Agent all the way up to full endpoint protection, email security, web application security, secure access across distributed enterprises and SD-WAN environments, advanced threat protection, management and analytics, and security information and event management (SIEM).

All of these are underscored and supported by FortiGuard Services, which deliver AI-powered intelligence and protection across the Security Fabric.

**DO NOT REPRINT**  
© FORTINET

## Devices That Comprise the Security Fabric



- Core:
  - FortiGate devices are core: one root, and one or more downstream
  - At least one of: FortiAnalyzer, FortiAnalyzer Cloud, or FortiGate Cloud
- Recommended—Adds significant visibility or control:
  - FortiManager, FortiAP, FortiSwitch, FortiClient, FortiClient EMS, FortiSandbox, FortiMail, FortiWeb, FortiNDR, FortiDeceptor
- Extended—Integrates with the Security Fabric, but may not apply to everyone:
  - Other Fortinet products and third-party products using the API

FortiGate devices are the core of the Security Fabric, plus one FortiAnalyzer or cloud logging solution. FortiAnalyzer Cloud or FortiGate Cloud can act as the cloud logging solution. The FortiGate devices must be running in NAT mode and can have one of the following roles:

- Root
- Downstream

Root FortiGate is the main component in the Security Fabric. It is typically located on the edge of the network and connects the internal devices and networks to the internet through your ISP. From the root FortiGate, you can see information about the entire Security Fabric on the Physical and Logical Topology pages in the GUI.

After a root FortiGate is installed, all other downstream FortiGate devices in the Security Fabric act as Internal Segmentation Firewalls (ISFWs), located at strategic points in your internal network, rather than on the network edge. This allows extra security measures to be taken around key network components, such as servers that contain valuable intellectual property. ISFW FortiGate devices create network visibility by sending traffic and information about the devices that are connected to them to the root FortiGate.

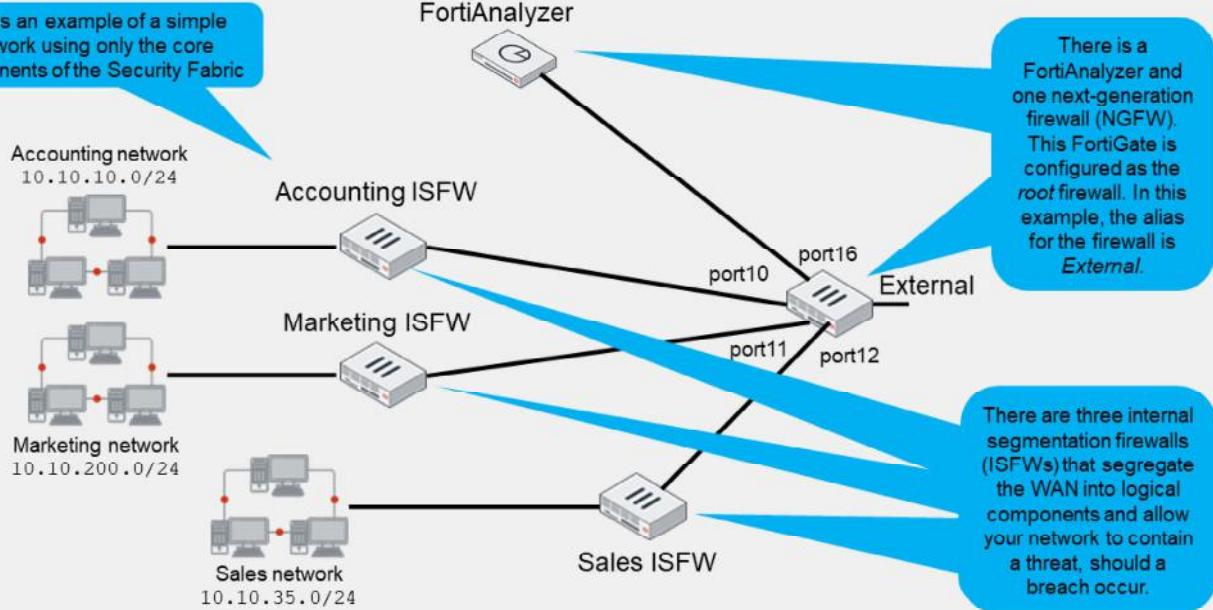
To add more visibility and control, Fortinet recommends adding FortiManager, FortiAP, FortiClient, FortiClient EMS, FortiSandbox, FortiMail, FortiWeb, FortiNDR, FortiDeceptor, and FortiSwitch.

The solution can be extended by adding other network security devices, including several third-party products.

**DO NOT REPRINT**  
**© FORTINET**

## How Do You Implement the Security Fabric?

This is an example of a simple network using only the core components of the Security Fabric



**FORTINET**  
Training Institute

© Fortinet Inc. All Rights Reserved.

7

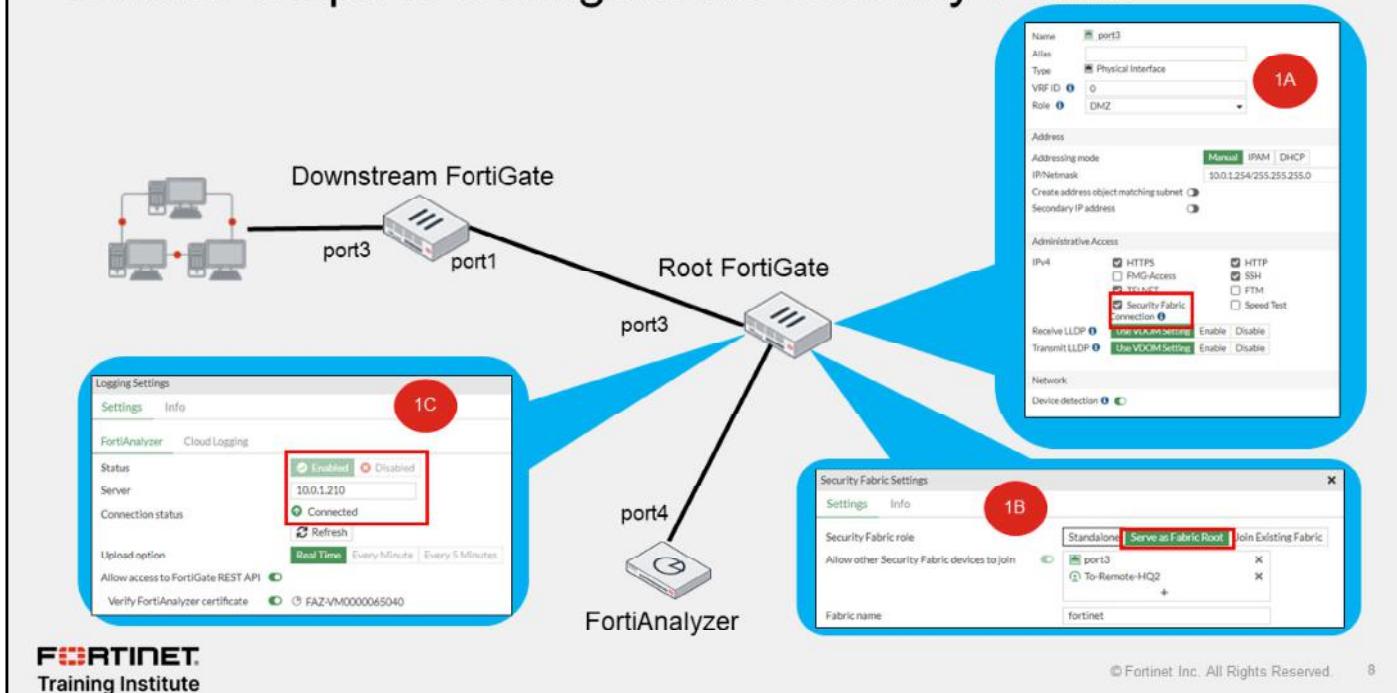
This simple network that comprises only the core devices of a Security Fabric includes one FortiAnalyzer and four next-generation firewall (NGFW) FortiGate devices.

The FortiGate device named External is acting as the edge firewall and is configured as the *root* firewall within the Security Fabric.

Downstream from the root firewall, three internal segmentation firewalls compartmentalize the WAN in order to contain breaches and to control access to various LANs. This example uses Accounting, Marketing, and Sales LANs.

**DO NOT REPRINT**  
**© FORTINET**

## General Steps to Configure the Security Fabric



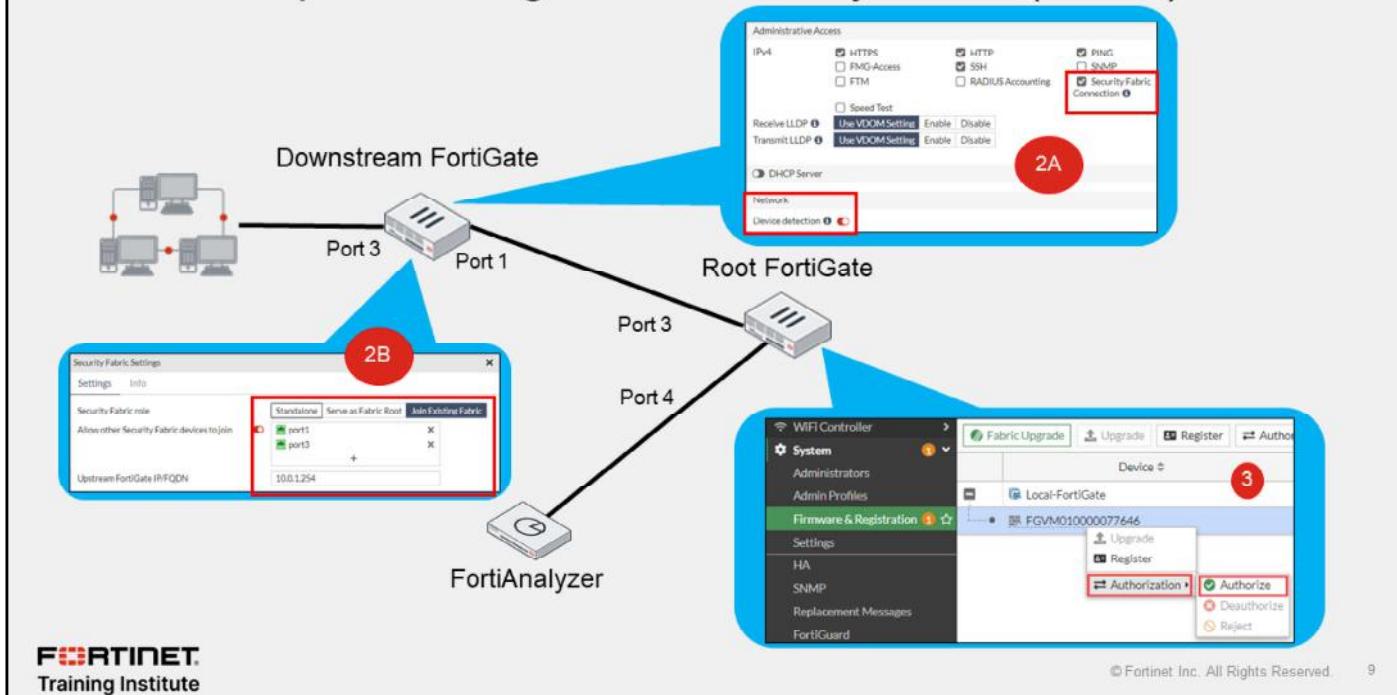
To configure a new Security Fabric, follow the general steps described here:

First, on the root FortiGate device, you must enable **Security Fabric Connection** on the interfaces that face any downstream FortiGate device. Then, enable the Security Fabric connector, and select **Serve as Fabric Root**. You also need to configure FortiAnalyzer or a cloud logging solution. This logging configuration is pushed to all the downstream FortiGate devices.

Optionally, you can preauthorize your downstream devices by adding their serial numbers. When you add the serial number of a Fortinet device to the trusted list on the root FortiGate device, the device can join the Security Fabric as soon as it connects. After you authorize the new FortiGate, additional connected FortiAP and FortiSwitch devices automatically appear in the topology tree.

**DO NOT REPRINT**  
**© FORTINET**

## General Steps to Configure the Security Fabric (Contd)



The second step in implementing the Security Fabric is configuring the downstream Fortinet devices. On the downstream FortiGate devices, you must enable **Security Fabric Connection** and **Device Detection** on the interfaces facing the downstream FortiGate devices. On the **Fabric Connectors** page, select **Join Existing Fabric** and add the root (upstream) FortiGate IP address.

The third step in implementing the Security Fabric is to authorize the downstream FortiGate devices on the root FortiGate.

**DO NOT REPRINT**  
**© FORTINET**

## Synchronizing Objects Across the Security Fabric

- By default, object synchronization is enabled in fabric settings

```
config system csf
set configuration-sync default
set fabric-object-unification default
end
```

| Parameter                                                                                     | Description                                                                                                                                                                                                                                                                                                                                                                                                |
|-----------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| fabric-object-unification                                                                     | default: Global CMDB objects are synchronized in the Security Fabric.<br>local: Global CMDB objects are not synchronized to and from this device.<br><br>This command is available only on the root FortiGate. If set to local, the device does not synchronize objects from the root, but sends the synchronized objects downstream.                                                                      |
| configuration-sync default                                                                    | default: Synchronize configuration for FortiAnalyzer, FortiSandbox, and Central Management to root node.<br>local: Do not synchronize configuration with the root node.<br><br>If downstream FortiGate devices are set to local, the synchronized objects from the root to downstream are not applied locally. However, the downstream FortiGate device send the configuration to lower FortiGate devices. |
| config firewall <object>     edit <name>         set fabric-object {enable   disable}     end | <object> can be address, address6, addrgrp, addrgrp6, service category, service custom, service group, and so on.<br>enable: sets the object as a Security Fabric-wide global object that is synchronized to downstream FortiGate devices.<br>disable: sets the object as local to this Security Fabric member.                                                                                            |



© Fortinet Inc. All Rights Reserved.

10

When the Security Fabric is enabled, settings to sync various objects, such as addresses, services, and schedules, from the upstream FortiGate device to all downstream FortiGate devices is enabled by default. Synchronization always happens from the root FortiGate to downstream FortiGate devices. Any object that can be synced will be available on downstream FortiGate devices after synchronization.

The CLI command `fabric-object-unification` is available only on the root FortiGate device. When set to `local`, global objects are not synchronized to downstream devices in the Security Fabric. The default value is `default`.

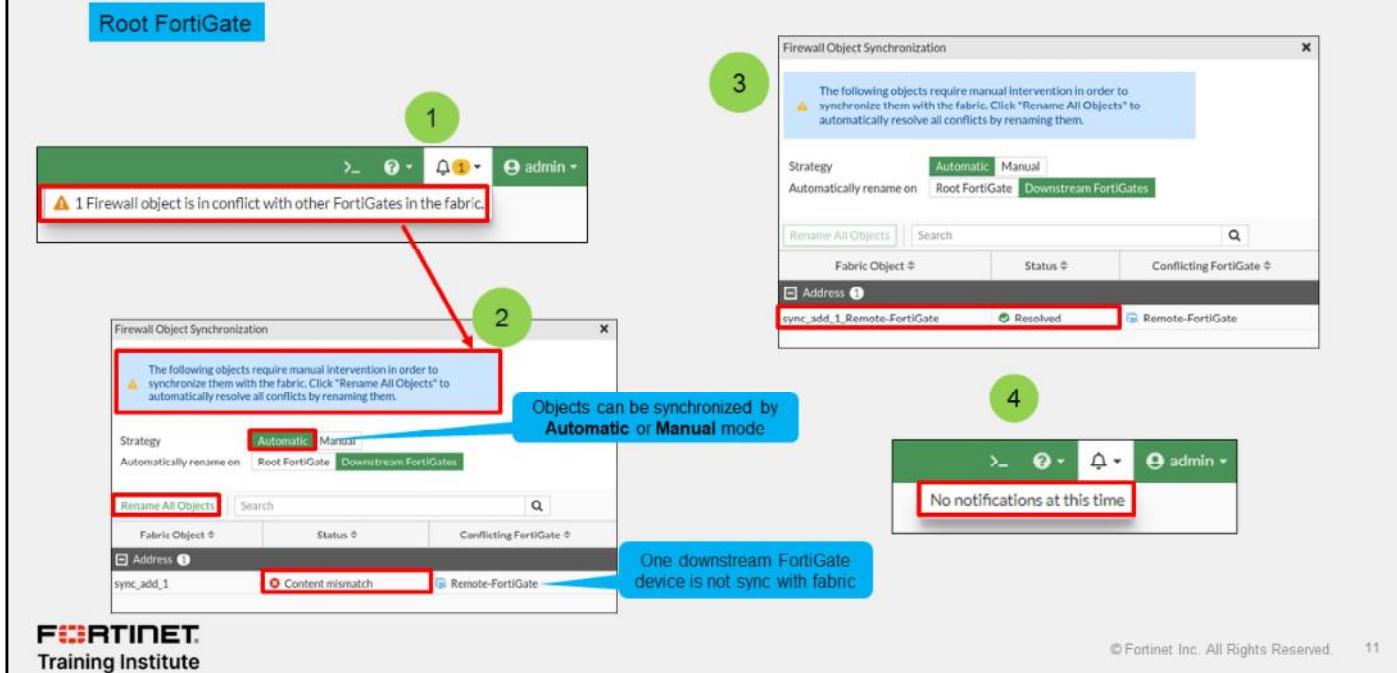
The CLI command `configuration-sync local` is used when a downstream FortiGate device doesn't need to participate in object synchronization. When set to `local` on a downstream FortiGate device, the device does not synchronize objects from the root, but still participates in sending the synchronized object downstream.

You can also enable or disable per-object synchronization in the Security Fabric. This option is not available for objects you create on a downstream FortiGate device. Security Fabric synchronization is disabled by default for supported Security Fabric objects, and these Security Fabric objects are kept as locally created objects on all the FortiGate devices in the Security Fabric. If object synchronization is disabled on the root FortiGate device, using the command `set fabric-object disable`, firewall addresses and address groups are not synchronized to downstream FortiGate devices.

Note that if a device in the Security Fabric is in multi-VDOM mode, the GUI does not display the Security Fabric synchronization option. Even if this is enabled in the CLI, the object is not synchronized to any downstream devices.

**DO NOT REPRINT**  
**© FORTINET**

## Synchronizing Objects Across the Security Fabric (Contd)



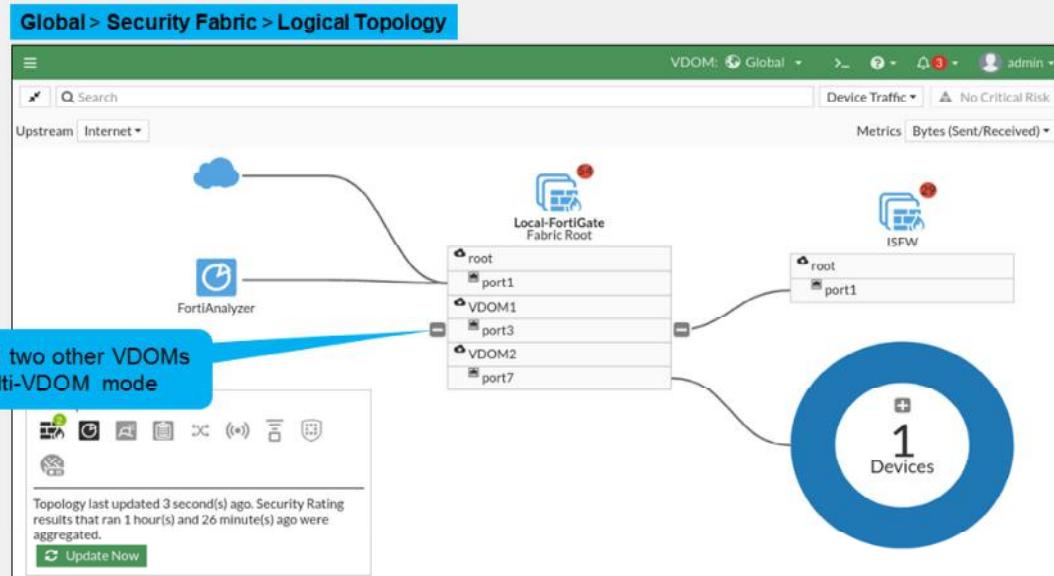
If an object conflict occurs during synchronization, you will get a notification in the topology tree.

The process to resolve a synchronization conflict is as follows:

1. Click the notification message: **1 Firewall objects is in conflict with other FortiGates in the fabric.** Click the notification message.
2. On the **Firewall Object Synchronization** page, you can see that both the root FortiGate and downstream FortiGate devices contain the **sync\_add\_1** object (with a different IP address/subnet schema on each device), causing a status of **Content mismatch**. The **Strategy** field, displays two options to resolve the conflict: **Automatic** and **Manual**. Select **Automatic**, as shown in this example, and then click **Rename All Objects**.
3. **Remote-FortiGate** is appended to the name of the downstream FortiGate device **sync\_add\_1** address object and the status changes to **Resolved**.
4. The conflict message disappears.

**DO NOT REPRINT**  
**© FORTINET**

## Multi-VDOM in the Security Fabric



When you configure FortiGate devices in multi-vdom mode and add them to the Security Fabric, each VDOM with its assigned ports is displayed when one or more devices are detected. Only the ports with discovered and connected devices appear in the Security Fabric view and, because of this, you must enable **Device Detection** on ports you want to have displayed in the **Security Fabric**. VDOMs without ports with connected devices are not displayed. All VDOMs configured must be part of a single **Security Fabric**. In the example shown on this slide, the Local-FortiGate is configured in multi-VDOM mode, and has three VDOMs (root, VDOM1, and VDOM2), each with ports that have connected devices.

# DO NOT REPRINT

## © FORTINET

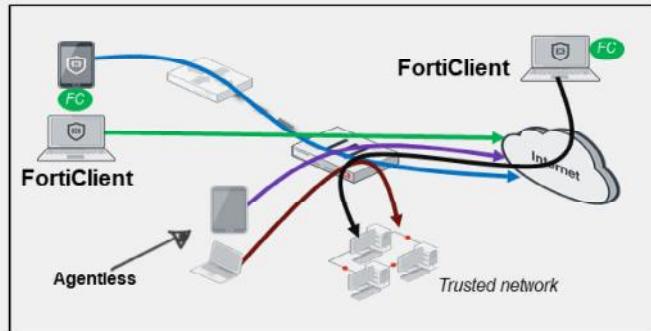
### Device Identification—Agentless vs. Agent

#### Agentless

- Useful feature for the Security Fabric topology view
- Requires direct connectivity to FortiGate
- Detection methods:
  - HTTP user agent
  - TCP fingerprinting
  - MAC address vendor codes
  - DHCP
  - Microsoft Windows browser service (MWBS)
  - SIP user agent
  - Link Layer Discovery Protocol (LLDP)
  - Simple Service Discovery Protocol (SSDP)
  - QUIC
  - FortiOS-VM detection
    - FortiOS-VM vendor ID in IKE messages
    - FortiOS-VM vendor ID in FortiGuard web filter and spam filter requests

#### Agent (FortiClient)

- Location and infrastructure independent



Device identification is an important component in the Security Fabric. FortiGate detects most of the third-party devices in your network and add them into the topology view in the Security Fabric. There are two device identification techniques: with an agent and without an agent (agentless).

Agentless identification uses traffic from the device. Devices are indexed by their MAC address and there are various ways to identify devices, such as HTTP user-Agent header, TCP fingerprint, MAC address OUI, and FortiOS-VM detection methods, to name a few. Agentless device identification is only effective if FortiGate and the workstations are directly connected network segments, where traffic is sent directly to FortiGate, and there is no intermediate router or Layer 3 device between FortiGate and the workstations.

Note that FortiGate uses a *first come, first served* approach to determine the device identity. For example, if a device is detected by the HTTP user agent, FortiGate updates its device table with the detected MAC address and scanning stops as soon as the type has been determined for that MAC address.

Agent-based device identification uses FortiClient. FortiClient sends information to FortiGate, and the device is tracked by its unique FortiClient user ID (UID).

# DO NOT REPRINT

## © FORTINET

## Device Identification

Enable **Device Detection** on interface(s)

**Network > Interfaces**

**Edit Interface** (port1)

Name: port1  
Alias: Physical Interface  
VIF ID: 0  
Role: DMZ

Address  
Addressing mode: Manual (DHCP) Auto-managed by FortiGate  
IP/Mask: 10.0.1.254/255.255.255.0  
Create address object matching subnet: Secondary IP Address

Administrative Access  
IPv4: HTTPS, FMG-Access, TELNET, Security Fabric Connection, PING, SSH, FTN  
IPv6: (disabled)  
Receive LLDP: Use VDOM Setting, Enable  
Transmit LLDP: Use VDOM Setting, Enable

Network  
Device detection: **Enable**

**Security Fabric > Logical Topology**

Upstream Internet Local FortiGate Fabric Root IPW PortAnalyzer

Metrics Bytes (Sent/Received)

Ubuntu machine detected upon traffic from the PC to the FortiGate

**Enable Device Detection**

© Fortinet Inc. All Rights Reserved. 14

By default, FortiGate uses device detection (passive scanning), which runs scans based on the arrival of traffic.

**DO NOT REPRINT****© FORTINET**

## Extending the Security Fabric

- Central management integration
  - FortiManager
- FortiMail integration
  - FortiMail
- Web application integration
  - FortiWeb
- FortiClient integration
  - FortiClient
  - FortiClient EMS
- Advanced threat protection integration
  - FortiSandbox
- Access device integration
  - FortiAP
  - FortiSwitch
- AI-driven breach protection
  - FortiNDR
- Advanced Threat Deception
  - FortiDeceptor
- Other optional devices
  - FortiADC
  - FortiDDoS
  - FortiWLC
  - FortiAuthenticator
  - FortiSIEM
  - FortiCache
  - FortiToken



© Fortinet Inc. All Rights Reserved.

15

The slide shows the list of products that Fortinet recommends to extend the Security Fabric.

For example, Fortinet recommends using a FortiManager for centralized management of all FortiGate devices and to access devices in the Security Fabric. You can also extend the Security Fabric down to the access layer by integrating FortiSwitch and FortiAP devices.

**DO NOT REPRINT****© FORTINET**

## Automation Stitches



- Consist of a trigger and one or more configurable actions
- Can be created only on the root FortiGate in the Security Fabric
- Are available as predefined stitches, or you can create custom ones
- Can run actions sequentially or in parallel
- Some actions include a minimum **Minimum interval** setting to make sure they don't run more often than needed

**FORTINET**  
Training Institute

The screenshot shows the 'Security Fabric > Automation' interface. In the center, there's a dialog box titled 'Create New Automation Stitch' with fields for 'Name', 'Status' (Enable/Disable), 'FortiGate(s)' (All FortiGates), 'Action execution' (Sequential/Parallel), and a 'Description'. Below these are two buttons: 'Add Trigger' and 'Add Action'. A red box highlights the 'Add Trigger' button. To the right of the dialog is a list of 'Select Entries' with a '+ Create' button at the top. Another red box highlights the '+ Create' button. Below the list are sections for 'Security Policies', 'Fabric Connector Event', 'FortiAnalyzer Event Handler', and 'Miscellaneous'. At the bottom right of the main window, there are icons for 'FortiOS Event Log' and 'Incoming Webhook'.

© Fortinet Inc. All Rights Reserved.

16

Administrator-defined automated workflows (called stitches) cause FortiOS to automatically respond to an event in a preprogrammed way. Because this workflow is part of the Security Fabric, you can set up automation stitches for any device in the Security Fabric. However, the Security Fabric is not required to use stitches.

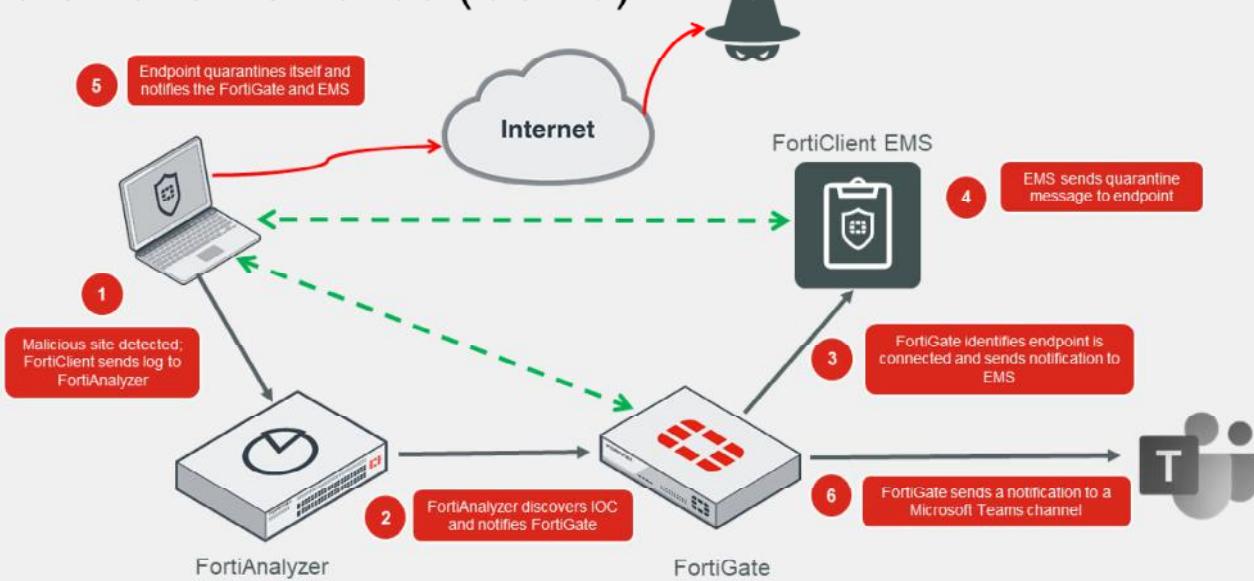
Each automation stitch pairs a trigger and one or more actions. FortiOS has several predefined stitches, triggers and actions. However, you can create custom automation based on the available options.

Automation stitches allow you to monitor your network and take appropriate action when the Security Fabric detects a threat. You can use automation stitches to detect events from any source in the Security Fabric and apply actions to any destination.

You can configure the **Minimum internal (seconds)** setting on some of the available actions to make sure they don't run more often than needed.

**DO NOT REPRINT**  
**© FORTINET**

## Automation Stitches (Contd)



This slide shows an example of how automation stitches can be configured to work in the Security Fabric:

1. FortiClient sends logs to FortiAnalyzer.
2. FortiAnalyzer discovers IoCs in the logs and notifies FortiGate.
3. FortiGate identifies whether FortiClient is a connected endpoint, and whether it has the login credentials for the FortiClient EMS that FortiClient is connected to. With this information, FortiGate sends a notification to FortiClient EMS to quarantine the endpoint.
4. FortiClient EMS searches for the endpoint and sends a quarantine message to it.
5. The endpoint receives the quarantine message and quarantines itself, blocking all network traffic. The endpoint notifies FortiGate and EMS of the status change.
6. FortiGate sends a notification to a Microsoft Teams channel to alert the administrators about the event.

**DO NOT REPRINT**  
**© FORTINET**

## External Connectors

- Security Fabric multi-cloud support adds external connectors to the Security Fabric configuration
- Allow you to integrate, among others:
  - Amazon Web Services (AWS)
  - Microsoft Azure
  - Oracle Cloud Infrastructure (OCI)
  - Google Cloud Platform (GCP)

The screenshot shows the FortiGate Management Interface. On the left, the navigation bar includes 'Local FortiGate', 'Security Fabric' (selected), 'Fabric Connectors', and 'FortiAnalyzer'. The main pane displays 'External Connectors' with sections for 'Public SDN' and 'Private SDN'. In the 'Public SDN' section, the 'aws' icon is highlighted with a red box and has a red arrow pointing from it to a detailed configuration dialog on the right. This dialog is titled 'New External Connector' and 'Public SDN'. It shows the 'Amazon Web Services (AWS)' connector selected. The 'Connector Settings' section includes fields for 'Name' (set to 'AWS'), 'Status' (set to 'Enabled'), and 'Update interval' (set to 'Use Default'). The 'AWS Connector' section contains fields for 'Access key ID' (set to 'AKIxxxxxxxxxxxx'), 'Secret access key' (redacted), 'Region name' (set to 'US-East'), and 'VPC ID' (set to 'vpc-e315g651').

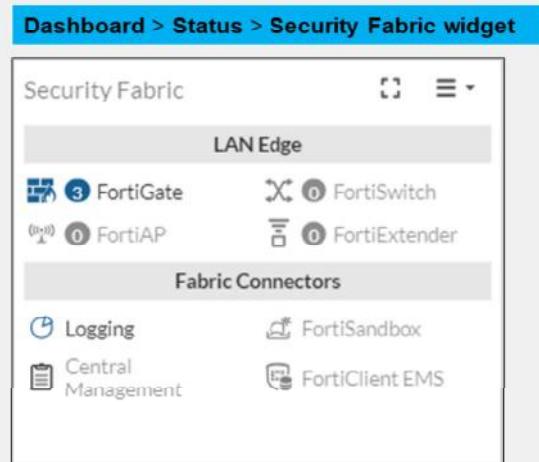
External connectors allow you to integrate multi-cloud support, such as Microsoft Azure and AWS, among others.

In an application-centric infrastructure (ACI), the SDN connector serves as a gateway bridging SDN controllers and FortiGate devices. For example, the SDN connector can register itself to APIC in the Cisco ACI fabric, polls objects of interest, and translates them into address objects. The translated address objects and associated endpoints populate on FortiGate.

**DO NOT REPRINT**  
© FORTINET

## The Security Fabric Status Widget

- The summary of your Security Fabric
- Icons indicating the other devices in the Security Fabric
- Click on the expand button to view the topology



The **Security Fabric Status** widget shows a summary of the devices in the Security Fabric.

You can hover over the icons at the top of the widget to display a quick view of their statuses. From here, you can click to authorize FortiAP and FortiSwitch devices that are connected to an authorized FortiGate.

Icons represent the other Fortinet devices that can be used in the Security Fabric:

- Devices in blue are connected in your network.
- Devices in gray are not configured, or not detected in your network.
- Devices in red are no longer connected, or not authorized in your network.

# DO NOT REPRINT

## © FORTINET

## Security Fabric Rating

- Three major scorecards:
  - Security Posture**
  - Fabric Coverage**
  - Optimization**
- Provide executive summaries of the three largest areas of security focus
- Clicking a scorecard drills down to a report of itemized results and compliance recommendations
- In multi-VDOM mode, reports can be generated in the Global VDOM for all the VDOMs



**FORTINET.**  
Training Institute

© Fortinet Inc. All Rights Reserved.

20

Security rating is a subscription service that requires a security rating license. This service provides the ability to perform many *best practices*, including password checks, to audit and strengthen your network security.

The **Security Rating** page is separated into three major scorecards: **Security Posture**, **Fabric Coverage**, and **Optimization**.

These scorecards provide executive summaries of the three largest areas of security focus in the Security Fabric.

The scorecards show an overall letter grade and breakdown of the performance in subcategories. Click a scorecard to drill down to a detailed report of itemized results and compliance recommendations. The point score represents all passed and failed items in that area. The report includes the security controls that were tested, linking them to specific FSBP or PCI compliance policies. You can click **FSBP** and **PCI** to reference the corresponding standard.

In multi-VDOM mode, administrators with read/write access can generate security rating reports in the Global VDOM for all the VDOMs on the device. Administrators with read-only access can view the report, but not generate it.

On the scorecards, the **Scope** column shows the VDOM or VDOMs that the security rating checked. On checks that support **Easy Apply**, you can run the remediation on all the associated VDOMs.

The security rating event log is available on the root VDOM.

# DO NOT REPRINT

## © FORTINET

## Security Posture

The Security Rating Score helps you to identify the security issues in your network and to prioritize your tasks.

Security issues that are labelled EZ can be resolved immediately.

Identifies critical security gaps.

**Score Details:**

- Score: -416.04
- Last Run: 2 hour(s) and 17 minute(s) ago
- Endpoints: 11
- Trends:
  - High: 65
  - Low: -416.04
  - Change: -740.06%

**Failed Security Controls:**

| Control                                | Device           | Status             |
|----------------------------------------|------------------|--------------------|
| Unsecure Protocol - HTTP               | Local-FortiGate  | Failed             |
| Unsecure Protocol - HTTP               | Remote-FortiGate | Failed             |
| Unsecure Protocol - HTTP               | FAZVM64          | Failed             |
| Unsecure Protocol - HTTP               | ISFW             | Unknown Dependency |
| Log Capacity Management (Local Device) | Local Device     | Failed             |

**FORTINET**  
Training Institute

© Fortinet Inc. All Rights Reserved. 21

Click the **Security Posture** scorecard on the **Security Rating** page to expand the scorecard and see more details.

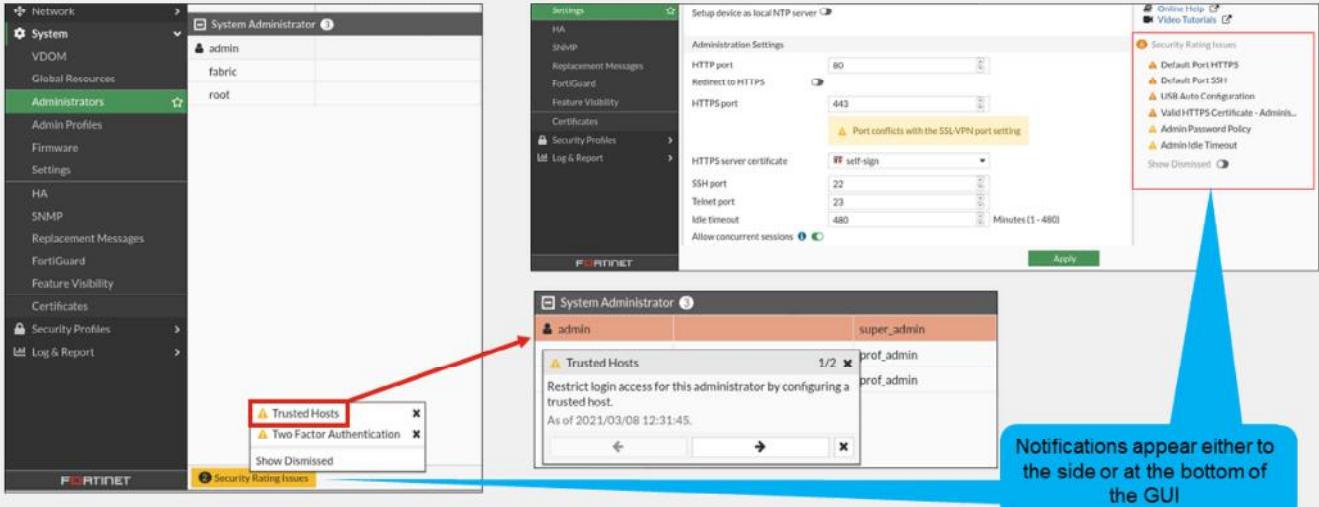
The security posture service now supports the following:

- Customer rankings by percentile using security audit (FortiGuard data): Security rating now supports sending results to FortiGuard, and receiving statistics from FortiGuard. Results are displayed to customer in the form of percentile.
- Security audits running in the background, not just on demand, when an administrator is logged in to the GUI. When you view the security audit page, the latest saved security audit data is loaded. From the GUI, you can run audits on demand and view results for different devices in the Security Fabric. You can also view all results or just failed test results.
- New security checks that can help you make improvements to your organization's network. These results include enforcing password security, applying recommended login attempt thresholds, encouraging two-factor authentication, and more.

**DO NOT REPRINT**  
**© FORTINET**

## Security Rating Notifications

- Display recommendations determined by security rating
- Appear on various setting pages



**FORTINET**  
Training Institute

© Fortinet Inc. All Rights Reserved.

22

Security rating provides recommendations and highlights issues with the configuration of the FortiGate settings. These recommendations and issues appear as notifications on the **Settings** page.

Click a notification to display the page where the setting needs to be fixed. This prevents you from having to go back and forth between the **Security Fabric > Security Rating** page and the various settings pages.

Notifications appear either to the side or at the bottom of the GUI. You can also dismiss the notifications.

In the example shown on this slide, some of the issues found are that FortiGate is using the default HTTPS and SSH ports, and that the administrator password policy is not enabled. The security rating check also recommends that you configure trusted hosts and two-factor authentication.

**DO NOT REPRINT****© FORTINET**

## Security Rating Check Schedule

- Security checks by default are scheduled to run automatically every 4 hours
- Enable or disable security checks using the CLI:

```
#config system global
(global)# set security-rating-run-on-schedule [enable/disable]
(global)# end
```

- Manually run a rating check using the CLI:

```
#diagnose report-runner trigger
```

Security rating checks by default are scheduled to run automatically every four hours.

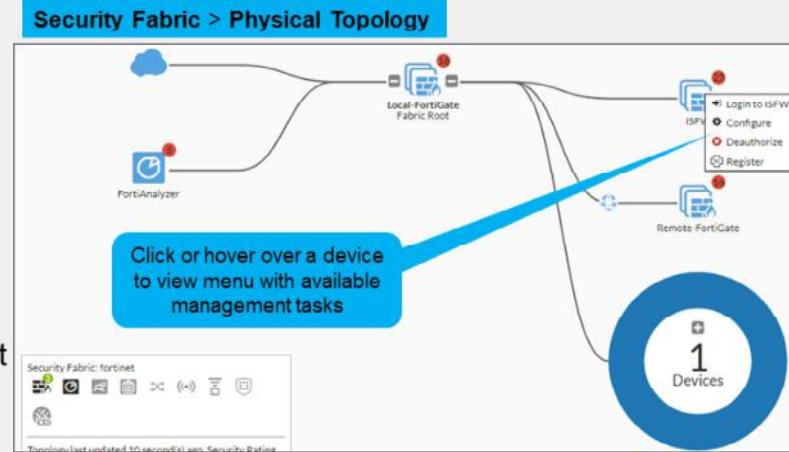
Use the commands shown on this slide to enable or disable security checks and manually run a rating check using the CLI.

# DO NOT REPRINT

## © FORTINET

### Topology Views

- Some device management tasks:
  - Login
  - Configure devices
  - Authorize or deauthorize devices
  - Register devices
  - Ban compromised clients
  - Quarantine hosts
  - Create address objects
- Full view available only at the root FortiGate



You can view the Security Fabric topology on the FortiGate GUI, from the **Security Fabric** menu. You can select the **Physical Topology** or **Logical Topology** view. To view the complete network, you must access the topology views on the root FortiGate in the Security Fabric.

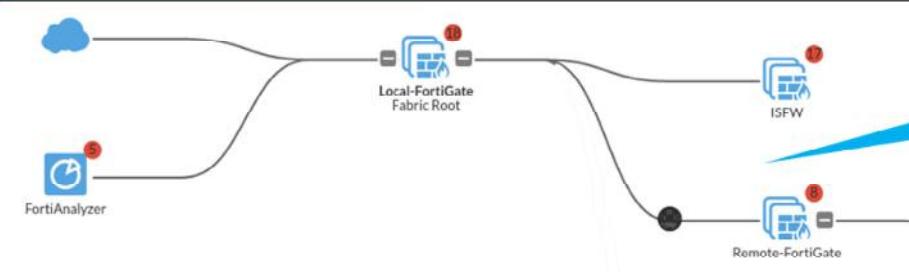
The **Physical Topology** view displays your network as a bubble chart of interconnected devices. These devices are grouped based on the upstream device they are connected to. The bubbles appear smaller or larger, based on their traffic volume. You can double-click any bubble to resize it and view more information about the device.

The **Logical Topology** view is similar to the **Physical Topology** view, but it shows the network interfaces, logical or physical, that are used to connect devices in the Security Fabric.

DO NOT REPRINT  
© FORTINET

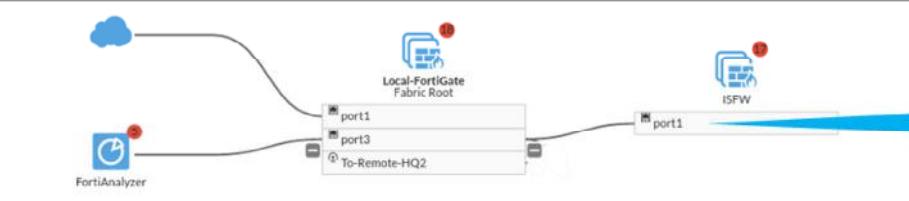
## Topology Views (Contd)

### Security Fabric > Physical Topology



Visualization of access layer devices in the Security Fabric

### Security Fabric > Logical Topology



Information about the interfaces that each device in the Security Fabric connects

This slide shows the difference between the **Physical Topology** view and the **Logical Topology** view.

**DO NOT REPRINT****© FORTINET**

## Knowledge Check

1. What is the Fortinet Security Fabric?

- A. A Fortinet solution that enables communication and visibility among devices in your network
- B. A device that can manage all your firewalls

2. What is the purpose of Security Fabric external connectors?

- A. External connectors allow you to integrate multi-cloud support with the Security Fabric.
- B. External connectors allow you to connect the FortiGate CLI.

3. From which view can an administrator deauthorize a device from the Security Fabric?

- A. From the physical topology view
- B. From FortiView

**DO NOT REPRINT**

**© FORTINET**

## Review

- ✓ Configure the Security fabric
- ✓ Monitor physical and logical topology views
- ✓ Run and analyze the Security Fabric rating



© Fortinet Inc. All Rights Reserved. 27

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

By mastering the objectives covered in this lesson, you learned how to configure and use the Fortinet Security Fabric.

**DO NOT REPRINT****© FORTINET**

# FortiGate Administrator

## High Availability

A small red square icon containing a white square with a diagonal line, followed by the text "FortiOS 7.4".

Last Modified: 15 November, 2023

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**

## Objectives

- Configure HA (FGCP)
- Configure HA failover
- Configure HA session synchronization
- Configure the HA management interface
- Verify the normal operation of an HA cluster
- Upgrade an HA cluster

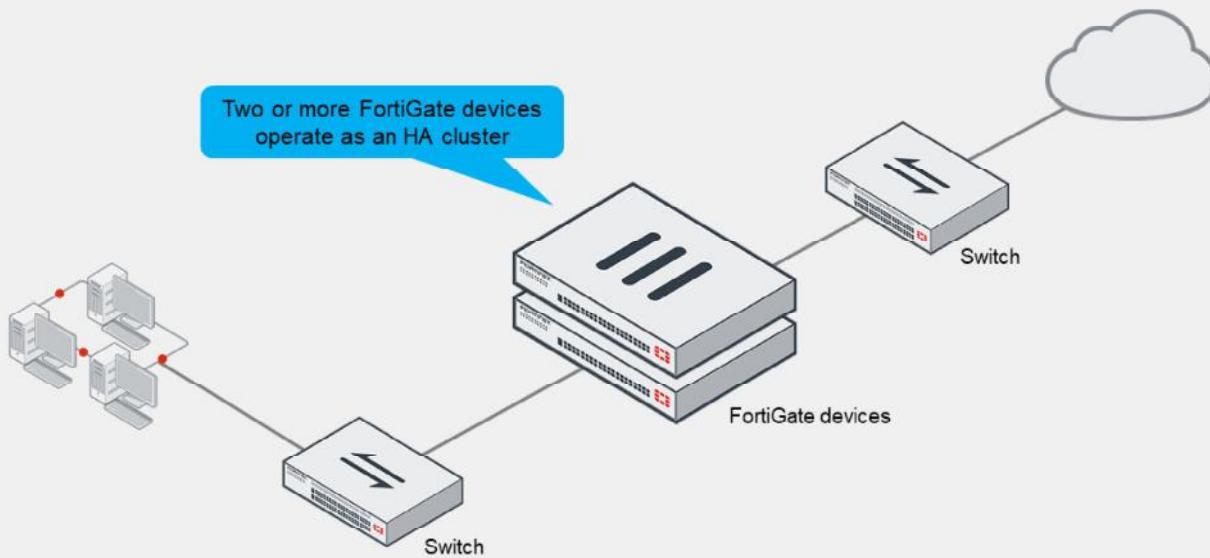
After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in FortiGate HA, you will be able to configure a redundant firewall cluster in your network, verify its operational status, and make changes to suit your business and security requirements.

# DO NOT REPRINT

## © FORTINET

### What Is FortiGate HA?



**FORTINET**  
Training Institute

© Fortinet Inc. All Rights Reserved. 3

FortiGate HA uses the FortiGate Clustering Protocol (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.

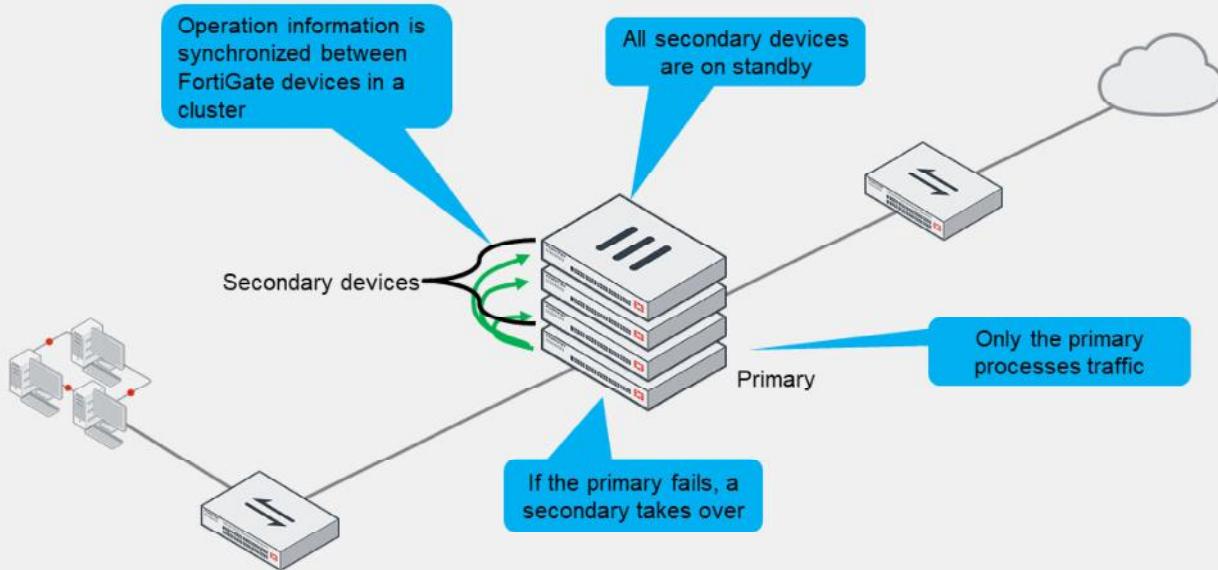
A cluster includes one device that acts as the primary FortiGate (also called the active FortiGate). The primary sends its complete configuration to other members that join the cluster, overwriting their configuration (except for a few settings). It also synchronizes session information, FIB entries, 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**  
Training Institute

© Fortinet Inc. All Rights Reserved.

4

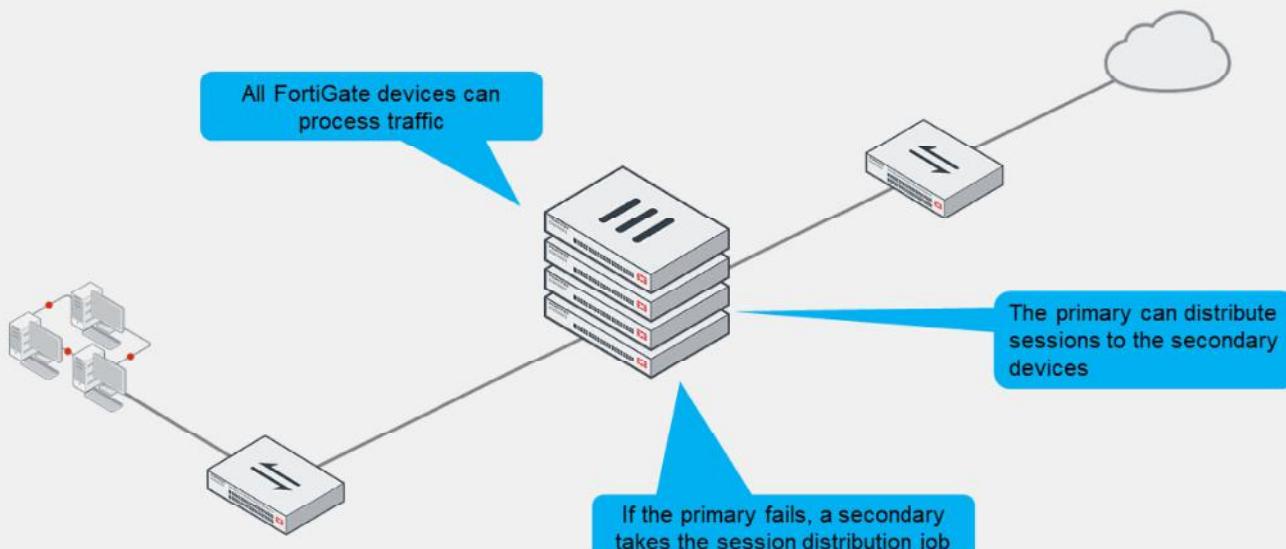
In active-passive mode, the primary FortiGate is the only FortiGate that actively processes traffic. Secondary FortiGate devices remain in passive mode, monitoring the status of the primary device.

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**  
Training Institute

© Fortinet Inc. All Rights Reserved.

5

The other HA mode is active-active.

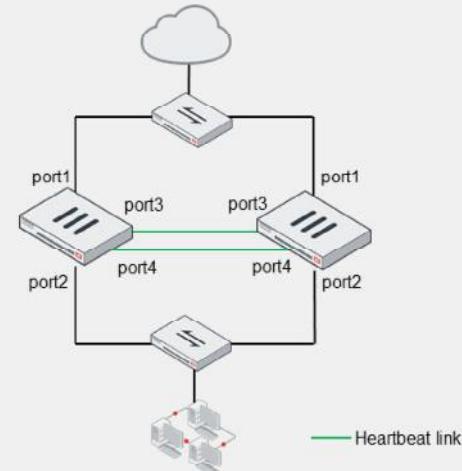
Like active-passive HA, in active-active HA, the operation-related data is synchronized between devices in the cluster. Also, if a problem is detected on the primary device, one of the secondary devices takes over the role of the primary to process the traffic.

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
- 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.

6

**FORTINET**  
Training Institute

To successfully form an HA cluster, you must ensure that the members have the same:

- Model: the same 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. The priority is defined as seen on this slide, and a higher value means higher priority.

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:

Difference measured in seconds

```
diagnose sys ha dump-by vcluster
...
FGVMxx92:...uptime/reset_cnt=7814/0
FGVMxx93:...uptime/reset_cnt=0/1
```

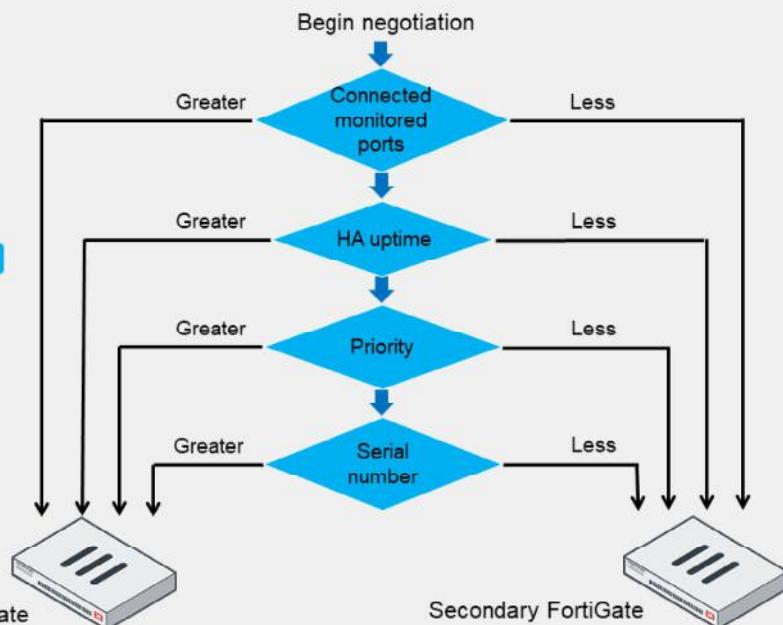
0 is for the device with the lowest HA uptime

Number of times HA uptime has been reset for this device

**FORTINET**  
Training Institute

© Fortinet Inc. All Rights Reserved.

7



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**

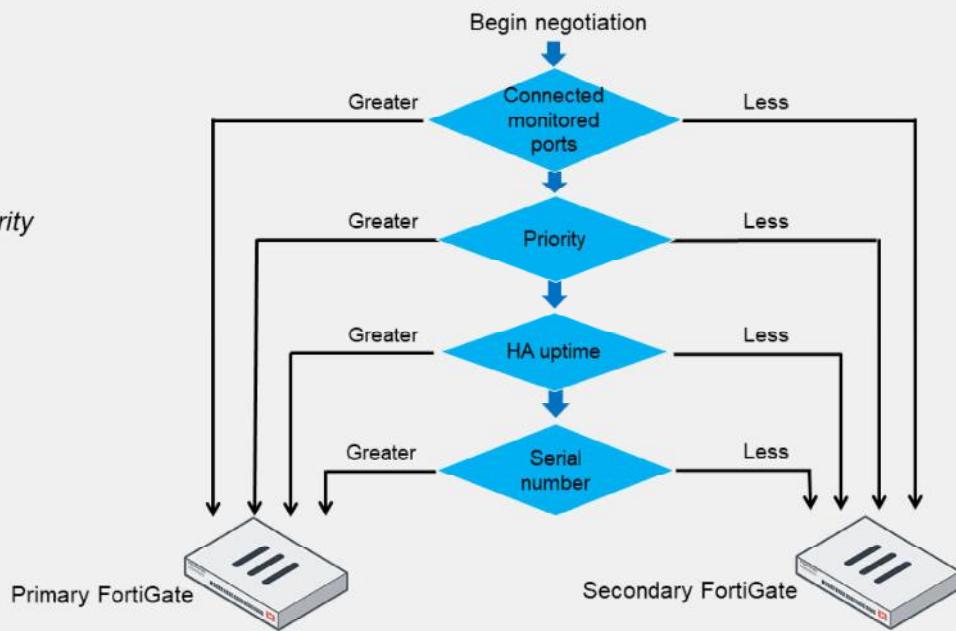
## Primary FortiGate Election—Override Enabled

- Override enabled

```
config system ha
 set override enable
end
```

- Force a failover

- Change the HA priority



**FORTINET**  
Training Institute

© Fortinet Inc. All Rights Reserved.

8

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**

## 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



© Fortinet Inc. All Rights Reserved.

9

So, what are the tasks of a primary FortiGate?

It monitors the cluster by broadcasting hello packets and listening for hello packets from other members in the cluster. The members use the hello packets to identify if 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. You will learn which types of sessions you can enable synchronization for later in the lesson.

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



© Fortinet Inc. All Rights Reserved. 10

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**

## Heartbeat Interface IP Addresses

- The cluster assigns addresses to heartbeat interfaces based on the serial number of each member
  - 169.254.0.1: for the highest serial number
  - 169.254.0.2: for the second highest serial number
  - 169.254.0.3: for the third highest serial number (and so on)
- Members keep their heartbeat IP addresses regardless of any change in their role (primary or secondary)
  - The IP address assignment may change only when a member leaves or joins the cluster
- The cluster uses the heartbeat IP addresses to:
  - Distinguish the members
  - Synchronize data with members



© Fortinet Inc. All Rights Reserved. 11

FGCP automatically assigns the heartbeat IP addresses based on the serial number of each device. The IP address 169.254.0.1 is assigned to the device with the highest serial number. The IP address 169.254.0.2 is assigned to the device with the second highest serial number, and so on. The IP address assignment does not change when a failover happens. Regardless of the device role at any time (primary or secondary), its heartbeat IP address remains the same.

A change in the heartbeat IP addresses may happen when a FortiGate device joins or leaves the cluster. In those cases, the cluster renegotiates the heartbeat IP address assignment, this time taking into account the serial number of any new device, or removing the serial number of any device that left the cluster.

The HA cluster uses the heartbeat IP addresses to distinguish the cluster members and synchronize data. These IPs are non-routable and are used for FGCP operations only.

**DO NOT REPRINT****© FORTINET**

## Heartbeat and Monitored Interfaces

- Heartbeat interfaces exchange sensitive data and may use a fair amount of bandwidth
  - If using a switch, use a dedicated switch or dedicated VLAN
  - Configure at least one heartbeat interface
    - It's a best practice to configure at least two for redundancy
    - Must be a physical port
- Monitored interfaces
  - Required for link failover
  - Choose interfaces that are critical for user traffic
    - Physical, redundant, and LAG interfaces are supported
  - Don't monitor heartbeat interfaces
  - Configure link failover after the cluster is formed
    - Prevents unwanted failover events during initial setup

Heartbeat interfaces exchange sensitive information about the cluster operation and may require a fair amount of bandwidth for data synchronization. For this reason, if you use a switch to connect the heartbeat interfaces, it's recommended that you use a dedicated switch or, at least, that you place the heartbeat traffic on a dedicated VLAN.

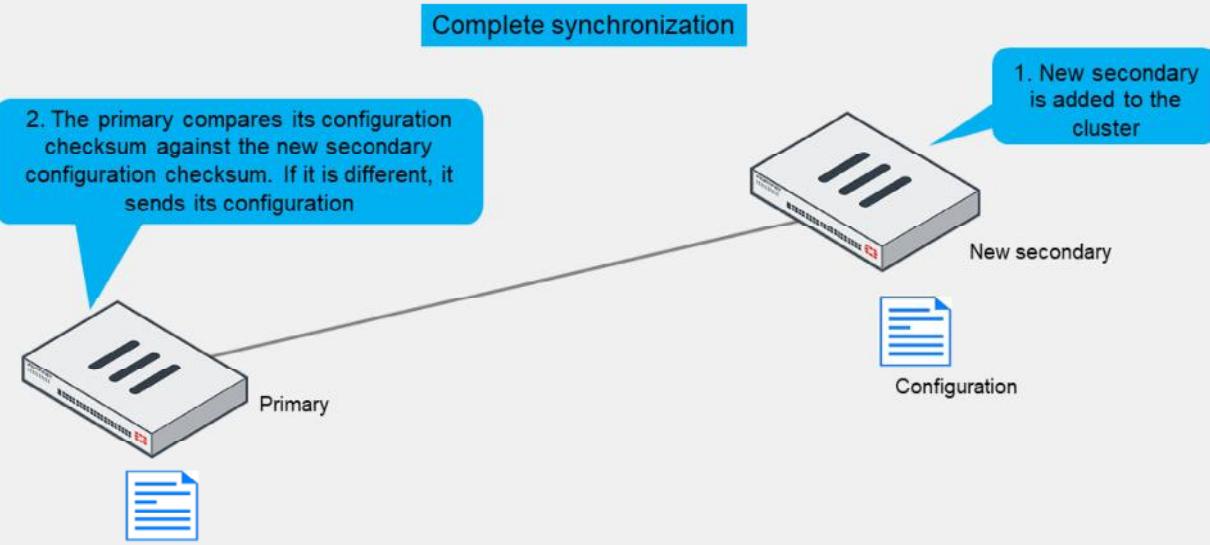
In addition, you must configure at least one port as a heartbeat interface, but preferably two for redundancy. For heartbeat interfaces, you can use physical interfaces only. That is, you can't use VLAN, IPsec VPN, redundant, or 802.3ad aggregate interfaces. You cannot use FortiGate switch ports either.

For link failover to work, you must configure one or more monitored interfaces. A monitored interface should be an interface whose failure has a critical impact in the network, and therefore, should trigger a device failover. For example, your LAN or WAN interfaces are usually good choices for monitored interfaces. Heartbeat interfaces, however, should not be configured as monitored interfaces because they are not meant to handle user traffic. Note that you can monitor physical ports, redundant interfaces, and link aggregation group (LAG) interfaces.

As a best practice, wait until a cluster is up and running and all interfaces are connected before configuring link failover. This is because a monitored interface can be disconnected during the initial setup and, as a result, trigger a failover before the cluster is fully configured and tested.

DO NOT REPRINT  
© FORTINET

## HA Complete Configuration Synchronization



To prepare for a failover, an HA cluster keeps its configurations in sync.

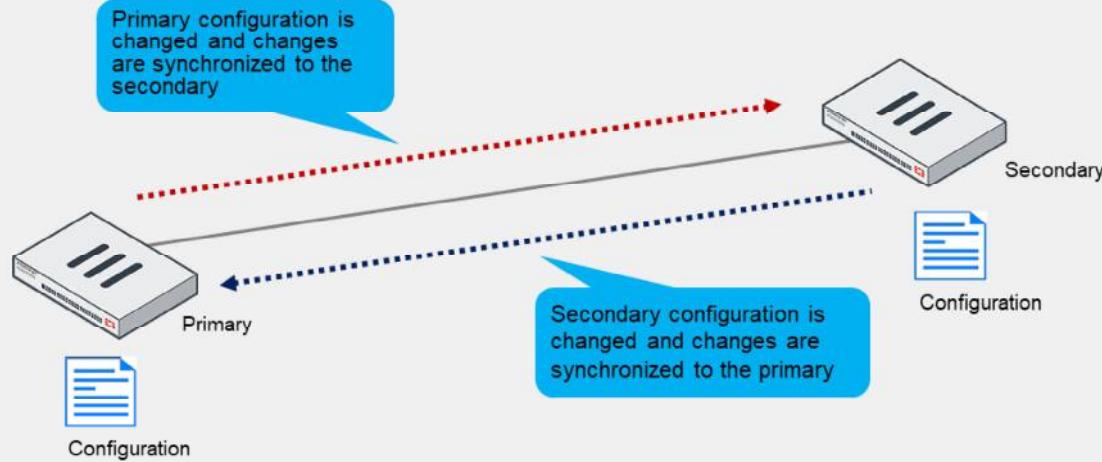
FortiGate HA uses a combination of both incremental and complete synchronizations.

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.

**DO NOT REPRINT****© FORTINET**

## HA Configuration Synchronization

- Incremental synchronization also includes:
  - Dynamic data such as DHCP leases, FIB entries, IPsec SAs, session information, and so on
- Periodically, HA checks for synchronization
  - If the checksums match, the cluster is in sync
  - If the checksums don't match after five attempts, the secondary downloads the whole configuration from the primary

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, a complete resynchronization to that secondary device is done.

**DO NOT REPRINT**  
© FORTINET

## 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



© Fortinet Inc. All Rights Reserved.

16

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

## Session Synchronization

- Provides seamless failover
  - Network applications don't need to restart connections
    - Minimum or no impact
- Firewall sessions
  - TCP sessions are synced
    - Unless they are subject to proxy inspection
  - Optionally, sync UDP and ICMP sessions
    - Usually not required
  - Multicast sessions are not synced
    - Multicast routes are
  - SIP sessions inspected by SIP ALG are synced
- Local sessions
  - Not synced, must be restarted

- Configure session synchronization on the CLI:

```
config system ha
 set session-pickup enable
 set session-pickup-connectionless enable
 set multicast-ttl <5 - 3600 sec>
end
```

The time multicast routes remain in multicast forwarding table after failover (recommended = 120 seconds; default = 600 seconds)

Enable UDP and ICMP session synchronization

Enable non-proxy TCP session sync synchronization

Session synchronization provides seamless session failover. When the primary fails, the new primary can resume traffic for synchronized sessions without network applications having to restart the connections.

By default, the feature synchronizes TCP firewall sessions that are not subject to proxy-based inspection. An exception to this rule is TCP SIP sessions inspected by SIP ALG. Even though SIP ALG performs proxy-based inspection on SIP sessions, FortiGate can still synchronize such SIP sessions. Firewall sessions, also known as pass-through sessions, are user traffic sessions that travel across FortiGate. TCP firewall sessions that are subject to flow-based inspection or no inspection at all, are synchronized to secondary members.

You can also enable the synchronization of UDP and ICMP sessions. Although both protocols are connectionless protocols, FortiGate still allocates sessions for UDP and ICMP connections in its session table. Usually, the synchronization of UDP and ICMP sessions is not required because most UDP and ICMP connections can resume communication if their session information is lost.

For multicast traffic, FortiGate synchronizes multicast routes only. That is, FortiGate doesn't synchronize multicast sessions, which should be fine because multicast sessions are mostly UDP-based and, as mentioned before, UDP sessions can usually resume communication if their session information is lost. To ensure the multicast routing information across members is accurate, you can adjust the multicast time to live (TTL) timer. The timer controls how long the new primary keeps the synced multicast routes in the multicast forwarding table. The smaller the timer value, the more often the routes are refreshed, and so the more accurate the multicast forwarding table is. The recommended timer value is 120 seconds.

Local-in and local-out sessions, which are sessions that are terminated at or initiated by FortiGate, respectively, are not synchronized either. For example, BGP peerings, OSPF adjacencies, as well as SSH and HTTPS management connections must be restarted after a failover.

**DO NOT REPRINT****© FORTINET**

## IPsec and SSL VPN Synchronization

- FortiGate automatically synchronizes data for:
  - IPsec
    - IKE and IPsec SAs
      - Tunnels continue to be up after failover
    - Sessions over IPsec require you to enable session synchronization for session failover
- FortiGate doesn't synchronize data for SSL VPN users
  - Users must restart the SSL VPN tunnel after a failover by reconnecting to the VPN



© Fortinet Inc. All Rights Reserved.

18

The primary FortiGate automatically synchronizes all IKE and IPsec security associations (SAs) to secondary members. This enables the new primary to resume existing IPsec tunnels after a failover. Note that you must also enable session synchronization if you want the new primary to also resume existing IPsec sessions. Otherwise, after a failover, you must still restart existing TCP connections made over IPsec tunnels, even though the IPsec tunnels continue to be up on the new primary.

For SSL VPN, users have to restart the SSL VPN tunnel after a failover by reconnecting to the VPN.

# 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



© Fortinet Inc. All Rights Reserved. 19

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.

Make sure that you enable session pickup for sessions you want to protect from a failover event. This way, the new primary can resume traffic for these sessions.

## Failover Protection Configuration

- Device failover
  - Always enabled
  - Adjust the failover time:

```
config system ha
 set hb-interval <1 - 20>
 set hb-interval-in-milliseconds 100ms | 10ms
 set hb-lost-threshold <1 - 60>
end
```

Number of failed heartbeats before device is dead  
 Heartbeat interval  
 Number of heartbeat interval units

- Default values vary by model
  - FortiGate 2000E:
    - hb-interval: 2
    - hb-interval-in-milliseconds: 100ms
    - hb-lost-threshold: 6
    - Total failover time =  $2 \times 100\text{ ms} \times 6 = 1200\text{ ms}$

- Link failover

- Configure one or more monitored interfaces:

```
config system ha
 set monitor <interface1> <interface2> ...
end
```

- Supported interfaces:

- Physical
- Redundant
- LAG

When you configure HA, device failover is always enabled. However, you can adjust the settings that dictate the failover time. To speed up failover, you can reduce the values for all three settings shown on this slide. To reduce false positives, increase their values.

The default values for the three settings vary by model. For example, using the default values on a FortiGate 2000E model results in a device failover time of 1200 milliseconds (1.2 seconds).

To configure link failover, you must configure one or more monitored interfaces, as shown on this slide. Note that you can configure only physical, redundant, and LAG interfaces as monitored interfaces.

## Failover Protection Configuration (Contd)

- Remote link failover
  - Configure link health monitor:

```
config system link-monitor
 edit "port1-ha"
 set srcintf "port1"
 set server "4.2.2.1" "4.2.2.2"
 set ha-priority 10
 next
end
```

Dead link nominal penalty—not synchronized

- Configure HA settings:

```
config system ha
 set pingserver-monitor-interface port1
 set pingserver-failover-threshold 5
 set pingserver-secondary-force-reset enable
 set pingserver-flip-timeout 30
end
```

Perform remote link failover on port1

Elect a new primary if the accumulated penalty reaches this threshold (5)

Elect a new primary again at the end of the flip timeout

The next remote link failover event cannot occur until at least 30 minutes have passed

This slide shows a configuration example for remote link failover.

First, you configure the link health monitor. The `ha-priority` setting in the link health monitor configuration defines the penalty applied to the member after the link is detected as dead. Note that the `ha-priority` setting has local significance only, and therefore, is not synchronized with other members.

The next step is to configure the HA settings related to remote link failover. The configuration on this slide instructs FortiGate to perform remote link failover on port1 as follows:

- When port1 is detected as dead, the nominal penalty (10) is added to the global penalty, which is initially set to 0.
- If the accumulated penalty reaches the penalty threshold (5), then the cluster elects a new primary. A failover occurs when a secondary member has a lower accumulated penalty than the primary. If so, the secondary member with the lowest accumulated penalty becomes the new primary.
- The cluster doesn't elect a new primary again until the pingserver flip timeout has passed. In other words, in this case the cluster can only encounter one remote link failover event per every 30 minutes or more. This prevents a flapping connection from continuously triggering HA failover.

If during the primary election the accumulated penalty of all members is the same, then other criteria, such as monitored interfaces, priority, uptime, and so on, are used as tiebreakers to elect the new primary.

**DO NOT REPRINT**  
**© FORTINET**

## Failover Protection Configuration (Contd)

- Memory-based failover

```
config system ha
```

```
 set memory-based-failover enable
 set memory-failover-threshold 70
 set memory-failover-monitor-period 30
 set memory-failover-sample-rate 2
 set memory-failover-flip-timeout 20
end
```

Enable memory-based failover

The memory usage threshold is 70%

Elect a new primary when the memory usage exceeds 70% for 30 seconds

Time to wait between subsequent memory-based failovers is 20 minutes

Check memory usage every 2 seconds

- SSD failover

```
config system ha
```

```
 set ssd-failover enable
end
```

Enable SSD-based failover

The HA configuration shown on this slide instructs FortiGate to perform memory-based failover as follows:

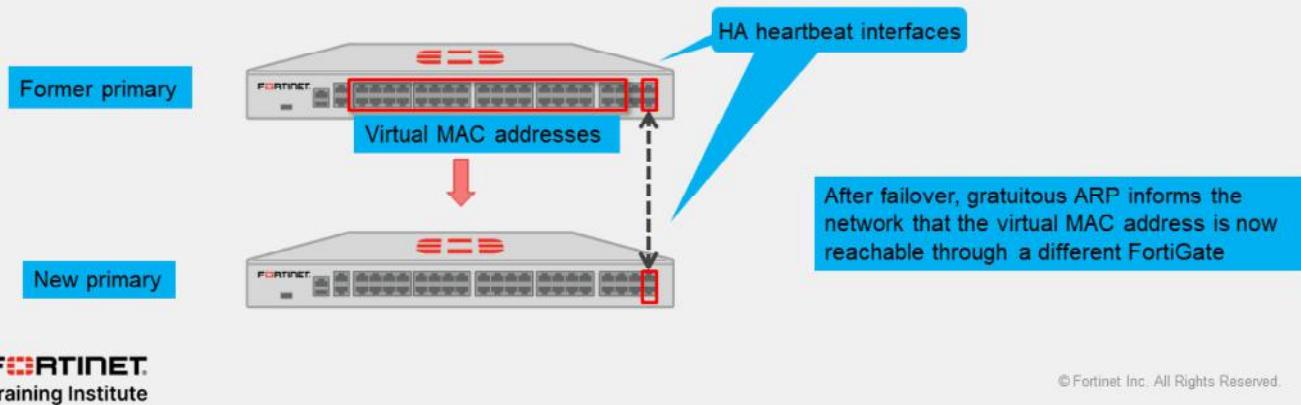
- When the memory on the primary reaches the threshold (70%) and stays like that for 30 seconds, then the cluster elects a new primary.
- During primary election, a failover occurs when the memory usage on a secondary member is lower than the configured memory threshold (70%). If so, the secondary member becomes the new primary.
- After a memory-based failover, the same FortiGate member waits at least 20 minutes before another memory-based failover can occur. Other cluster members can still initiate a memory-based failover if they meet their criteria.
- Each member in the cluster checks its memory usage every 2 seconds.

If during the primary election, the memory usage of all members is below or above the threshold, then other criteria, such as monitored interfaces, priority, uptime, and so on, are used as tiebreakers to elect 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



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.

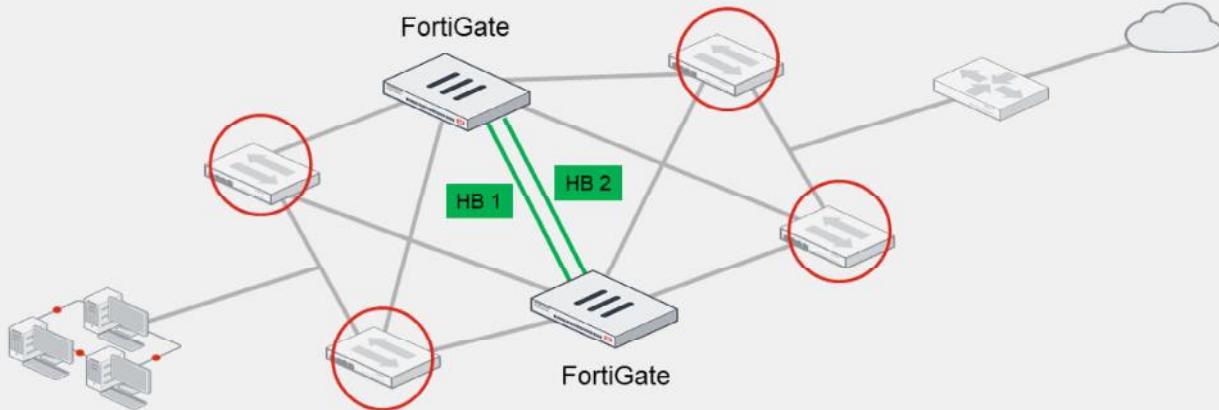
Note that the MAC address of a reserved HA management interface is not changed to a virtual MAC address. Instead, the reserved management interface keeps its original MAC address.

# DO NOT REPRINT

## © FORTINET

### Full Mesh HA

- Eliminates a single point of failure by having redundant switches
- Requires redundant or LAG interfaces
  - If using LAG interfaces, the switch must support MCLAG or a similar protocol
  - FortiSwitch supports MCLAG



At the beginning of this lesson, you reviewed a simple HA topology. Now, take a look at a more robust topology. It is called *full mesh HA*.

The goal of a full mesh HA topology is to eliminate a single point of failure, not only by having multiple FortiGate devices forming a cluster, but also by having redundant links to the adjacent switches. The goal is to have two switches for both upstream and downstream links, and then connect the redundant links to different switches. For example, the topology on this slide shows two FortiGate devices forming a cluster, and each FortiGate is connected to two redundant switches, using two different interfaces.

To achieve redundancy with adjacent switches, you must deploy redundant or LAG interfaces. If you use redundant interfaces, only one interface remains active. This prevents a Layer 2 loop and a standard switch should suffice. However, if you want to use LAG interfaces, then you must ensure that the switch supports multichassis link aggregation group (MCLAG) or a similar virtual LAG technology that enables you to form a LAG whose interface members connect to different switches. FortiSwitch, which is a Fortinet Ethernet switch, supports MCLAG. You can use FortiSwitch as the adjacent switch to deploy a full mesh HA topology with FortiGate.

**DO NOT REPRINT**  
**© FORTINET**

## Checking the HA Status on the GUI

**System > HA**

| FortiGate VM64-KVM                               |                                     | 1 3 5 7 9 11 13 15 17 19 21 23                         | 2 4 6 8 10 12 14 16 18 20 22 24                              | FortiGate VM64-KVM           |          | 1 3 5 7 9 11 13 15 17 19 21 23 | 2 4 6 8 10 12 14 16 18 20 22 24 |      |               |          |            |
|--------------------------------------------------|-------------------------------------|--------------------------------------------------------|--------------------------------------------------------------|------------------------------|----------|--------------------------------|---------------------------------|------|---------------|----------|------------|
|                                                  |                                     |                                                        |                                                              |                              |          |                                |                                 |      |               |          |            |
| Local-FortiGate (Primary)                        |                                     |                                                        |                                                              | Remote-FortiGate (Secondary) |          |                                |                                 |      |               |          |            |
| <input type="checkbox"/> Refresh                 | <input type="button" value="Edit"/> | <input type="button" value="Pin interface faceplate"/> | <input type="button" value="Remove device from HA cluster"/> | Status                       | Priority | Hostname                       | Serial No.                      | Role | System Uptime | Sessions | Throughput |
| <input checked="" type="checkbox"/> Synchronized | 200                                 | Local-FortiGate                                        | FGVM010000064692                                             | Primary                      | 37m 20s  | 18                             | 67.00 kbps                      |      |               |          |            |
| <input checked="" type="checkbox"/> Synchronized | 100                                 | Remote-FortiGate                                       | FGVM010000065036                                             | Secondary                    | 37m 16s  | 12                             | 30.00 kbps                      |      |               |          |            |

**Dashboard > Status**

| HA Status     |                                                      |
|---------------|------------------------------------------------------|
| Mode          | Active-Passive                                       |
| Group         | Training                                             |
| Primary       | <input checked="" type="checkbox"/> Local-FortiGate  |
| Secondary     | <input checked="" type="checkbox"/> Remote-FortiGate |
| Uptime        | 20m 32s                                              |
| State Changed | 19m 35s                                              |

**More columns available**

**Best Fit All Columns** **Reset Table**

**Select Columns**

- Status
- Priority
- Hostname
- Serial No.
- Role
- System Uptime
- Sessions
- Throughput
- AV Events
- Bytes
- Checksum
- Cluster Uptime
- CPU
- Down Ports
- IPS Events
- Packets
- RAM
- Virtual Domains

© Fortinet Inc. All Rights Reserved. 25

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 0:11:20
Cluster state change time: 2023-09-15 15:01:48
Primary selected using:
<2023/09/15 15:01:48> vcluster-1: FGVM010000064692 is selected as the primary because its override priority is
larger than peer member FGVM010000065036.
ses_pickup: disable
override: disable
Configuration Status:
FGVM010000064692(updated 4 seconds ago): in-sync
FGVM010000064692 cksum dump: 31 4e 3e b6 07 3d 5d 90 10 80 c4 c3 0d 86 64 99
FGVM010000065036(updated 2 seconds ago): in-sync
FGVM010000065036 cksum dump: 31 4e 3e b6 07 3d 5d 90 10 80 c4 c3 0d 86 64 99
System Usage stats:
FGVM010000064692(updated 4 seconds ago):
sessions=8, average-cpu-user/nice/system/idle=1%/0%/0%/98%, memory=38%
FGVM010000065036(updated 2 seconds ago):
sessions=0, average-cpu-user/nice/system/idle=0%/0%/0%/100%, memory=36%
...
```



© Fortinet Inc. All Rights Reserved.

26

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:
 FGVM010000064692(updated 3 seconds ago):
 port2: physical/10000full, up, rx-bytes/packets/dropped/errors=4029545/11074/0/0, tx=5360086/11576/0/0
 FGVM010000065036(updated 1 seconds ago):
 port2: physical/10000full, up, rx-bytes/packets/dropped/errors=5377151/11684/0/0, tx=4023101/10991/0/0
MONDEV stats:
 FGVM010000064692(updated 3 seconds ago):
 port1: physical/10000full, up, rx-bytes/packets/dropped/errors=42166263/29629/0/0, tx=570354/5486/0/0
 FGVM010000065036(updated 1 seconds ago):
 port1: physical/10000full, up, rx-bytes/packets/dropped/errors=14470/141/0/0, tx=0/0/0/0
PINGSVR stats:
 FGVM010000064692(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 2023/09/15 15:29:58), server=8.8.8.8, ha_prio=5
 FGVM010000065036(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 2023/09/15 15:30:00), server=8.8.8.8, ha_prio=5
Primary : Local-FortiGate , FGVM010000064692, HA cluster index = 1
Secondary : Remote-FortiGate, FGVM010000065036, HA cluster index = 0
number of vcluster: 1
vcluster 1: work 169.254.0.2
Primary: FGVM010000064692, HA operating index = 0
Secondary: FGVM010000065036, 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 Local-FortiGate and Remote-FortiGate 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
=====
===== FGVM010000064692 =====

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
===== FGVM010000065036 =====

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.

28

**FORTINET**  
Training Institute

The `diagnose sys ha checksum` command tree enables you to check the cluster configuration sync status. In most cases, you want to 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 properly, or if there are heartbeat communication issues, then the command may not show the checksum for members other than the one you run the command on. An alternative is to connect to each member individually and run the `diagnose sys ha checksum show` command instead. This command displays only the checksum of the member you are connected to.

After you obtain the checksums of each member, you can identify the configuration sync status by comparing the checksums. If all members show the exact 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**

## Checking the Configuration Synchronization (GUI)

- Right-click the table header row and select the **Checksum** column
- After enabling it, you can compare checksums for members in the HA cluster

| Status                                              | Priority | Hostname         | Checksum                         | Role      |
|-----------------------------------------------------|----------|------------------|----------------------------------|-----------|
| <span style="color: green;">✓</span> Synchronized   | 200      | Local-FortiGate  | 9da6935ad11a1093675bf55f72a4b33d | Primary   |
| <span style="color: red;">✗</span> Not Synchronized | 100      | Remote-FortiGate | cbf3d163ffa8363a738c90d8486582ed | Secondary |

Secondary device is not synchronized, and the checksum value is different from the primary

| Status                                            | Priority | Hostname         | Checksum                         | Role      |
|---------------------------------------------------|----------|------------------|----------------------------------|-----------|
| <span style="color: green;">✓</span> Synchronized | 200      | Local-FortiGate  | cfb4f9c0ac340d93f60306a66093596e | Primary   |
| <span style="color: green;">✓</span> Synchronized | 100      | Remote-FortiGate | cfb4f9c0ac340d93f60306a66093596e | Secondary |

After synchronization is complete, the checksums now match

You can also view FortiGate device checksums in the **System > HA** interface. To enable the column, right-click on the top header row, and then select the **Checksum** column to display.

**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 FGVM010000065036
```



© Fortinet Inc. All Rights Reserved. 30

When troubleshooting HA, you may need to connect to the CLI of another member from the CLI of the member you are currently connected to. You do this by using the `execute ha manage` command to connect to the other member.

For example, when you connect to the cluster over SSH using any of the cluster virtual IP addresses, you connect to the primary member. If you then want to connect to another member, you can use the `execute ha manage` command to access its CLI.

This command requires you to indicate the ID of the member you want to connect to and the username you will use to log in. To get the list of member IDs, you can add a question mark to the end of the `execute ha manage` command, as shown on this slide.

**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

## Firmware Upgrade

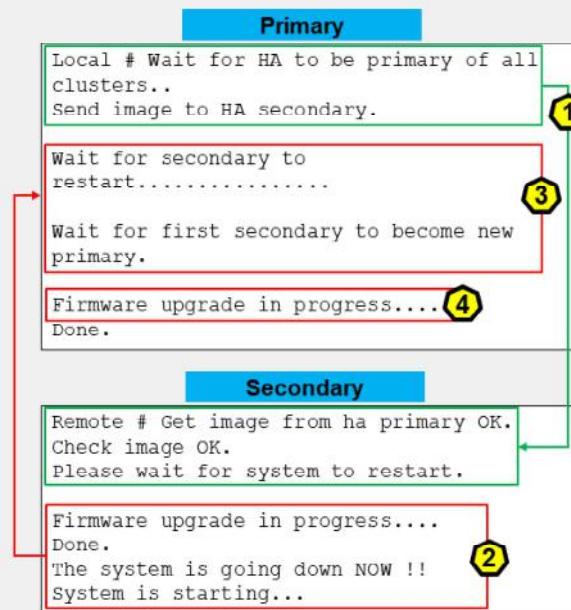
- Use the GUI or CLI
- Uninterruptible upgrade is enabled by default:

```
config system ha
 set upgrade-mode simultaneous | uninterruptible | local-only | secondary-only
end
```

- Upgrade process (uninterruptible upgrade):
  1. The primary sends the firmware image to the secondary devices
  2. The secondary devices upgrade their firmware
  3. The first secondary to finish becomes the primary\*
  4. The former primary becomes a secondary device and upgrades its firmware

**Note:**

\* If HA mode is active-active, the primary temporarily takes over all the traffic



**FORTINET**  
Training Institute

© Fortinet Inc. All Rights Reserved.

32

You upgrade an HA cluster in the same way you do for standalone FortiGate devices. That is, you can apply the new firmware using the GUI firmware upgrade tool. In HA, this usually means connecting to the primary FortiGate GUI to apply the new firmware. You can also use the CLI if you prefer.

Also, like on standalone FortiGate devices, the device must reboot to apply the new firmware. However, uninterrupted upgrade is enabled by default, so that secondary members in a cluster are upgraded first. After the administrator applies the new firmware on the primary, uninterrupted upgrade works as follows:

1. The primary sends the firmware to all secondary members using the heartbeat interface.
2. The secondary devices upgrade their firmware first. If the cluster is operating in active-active mode, the primary temporarily takes over all traffic.
3. The first secondary that finishes upgrading its firmware takes over the cluster.
4. The former primary becomes a secondary device and upgrades its firmware next.

Note that depending on the HA settings and uptime, the original primary may remain as a secondary after the upgrade. Later, if required, you can issue a manual failover. Alternatively, you can enable the `override` setting on the primary FortiGate to ensure it takes over the cluster again after it upgrades its firmware, as long as the device is assigned the higher priority.

If you want the cluster to upgrade all members at the same time to expedite the process, you can enable simultaneous upgrade. However, this option will have a service impact. The local-only option allows you to upgrade only the local device. The secondary-only option allows you to upgrade the secondary members, but the primary FortiGate will not be upgraded. The local-only and secondary-only options are only meant to temporarily put the cluster on different firmware versions—to provide more control on which member to upgrade, and when. Configurations will not synchronize while the cluster has different firmware versions.

**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 session type can you synchronize in an HA cluster?  
 A. BGP peerings  
 B. Non-proxy TCP sessions
  
3. Which statement about the firmware upgrade process in an HA cluster is true?  
 A. You upload the new firmware to the primary FortiGate only.  
 B. The members do not reboot.

**DO NOT REPRINT**

**© FORTINET**

## Review

- ✓ Configure HA (FGCP)
- ✓ Configure HA failover
- ✓ Configure HA session synchronization
- ✓ Configure the HA management interface
- ✓ Verify the normal operation of an HA cluster
- ✓ Upgrade the HA cluster

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**

# FortiGate Administrator

## Diagnostics and Troubleshooting

A small red square icon containing a white graphic of a network device or server.

FortiOS 7.4

Last Modified: 15 November, 2023

In this lesson, you will learn about using diagnostic commands and tools.

**DO NOT REPRINT****© FORTINET**

## Objectives

- 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

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

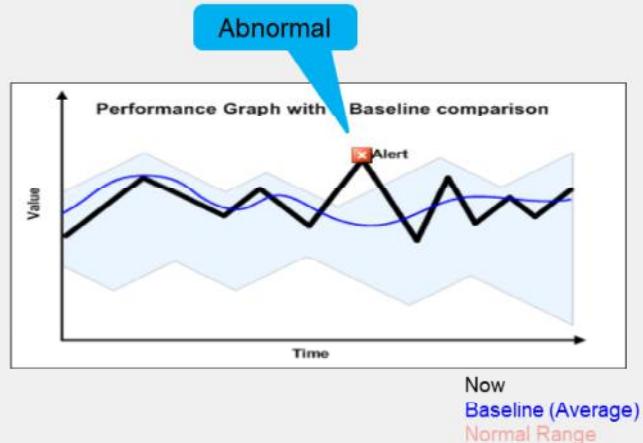
By demonstrating competence in general diagnosis, you will be able to discover general information about the status of FortiGate.

# 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.

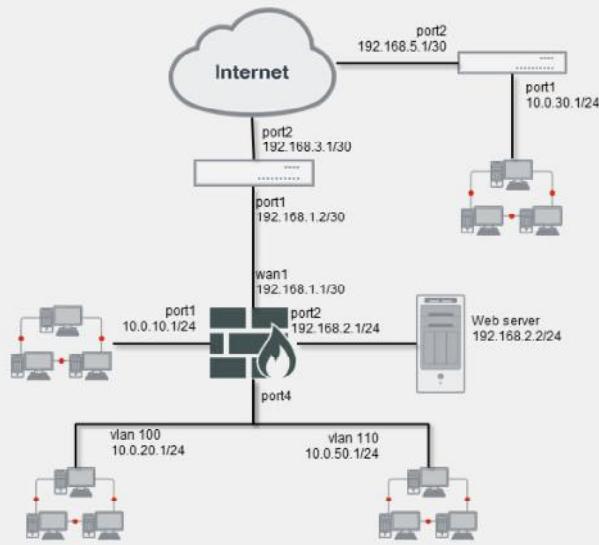
In the graph shown on this slide, the range that indicates *normal* is shown in blue. What exactly is this blue line? It indicates the averages—our baseline. What is the thick black line? It's the current behavior. When the current behavior (black line) leaves the normal range, an abnormal event is happening.

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



What is the first way to define what is *normal* for your network?

Flows and other specifications of *normal* behaviour are derived from 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.

**DO NOT REPRINT**  
**© FORTINET**

## Monitoring Traffic Flows and Resource Usage

- Get normal data before problems or complaints
- Tools:
  - Security Fabric
  - Dashboard
  - SNMP
  - Alert email
  - Logging/Syslog/FortiAnalyzer
  - CLI debug commands



**FORTINET**  
 Training Institute

© Fortinet Inc. All Rights Reserved.

5

Another way to define normal is to know the average performance range. On an ongoing basis, collect data that shows normal usage.

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?

# DO NOT REPRINT

## © FORTINET

### System Information

**FortiGate physical appliance**

```
FortiGate-61E # get system status
Version: FortiGate-61E v7.4.1,build2463,230030 (GA.F)
```

**FortiGate VM**

```
Local-FortiGate # get system status
Version: FortiGate-VM64-KVM v7.4.1,build2463,230030 (GA.F)
```

**FORTINET**  
Training Institute

© Fortinet Inc. All Rights Reserved.

6

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"
```



© Fortinet Inc. All Rights Reserved.

7

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**

## Packet Capture

- 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     | ✓          | ✓          | ✓                | ✓          |



© Fortinet Inc. All Rights Reserved.

8

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 Capture 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

**FORTINET**  
Training Institute

© Fortinet Inc. All Rights Reserved.

9

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**

## 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



© Fortinet Inc. All Rights Reserved. 10

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

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:
  - Available on devices with internal storage

**Network > Diagnostics > Debug Flow**

Packet Capture **Debug Flow**

NPU hardware acceleration must be disabled on the respective firewall policy to see all packets. To do so, set "auto-asic-offload" to "disable" in the CLI.

Number of packets: 100

**Select a protocol or Any**

Filters

Filter type: Basic Advanced

IP type: IPv4 IPv6

IP address: 8.8.8.8

Port: 1

Protocol: ICMP, Any, Specify, TCP, UDP, SCTP, ICMP

**Network > Diagnostics > Debug Flow**

Packet Capture **Debug Flow**

NPU hardware acceleration must be disabled on the respective firewall policy to see all packets. To do so, set "auto-asic-offload" to "disable" in the CLI.

Number of packets: 100

**Select source IP address, source port, destination IP address, destination port, and protocol**

Filters

Filter type: Basic Advanced

IP type: IPv4 IPv6

Source IP: 10.0.1.10

Source port: 8.8.8.8

Destination IP: 8.8.8.8

Destination port: 1

Protocol: ICMP

Start debug flow

**FORTINET.**  
Training Institute

© Fortinet Inc. All Rights Reserved. 13

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=0, 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=match
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 | 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=0, 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=match                                                                                                                    |
| 07:08:02 | policy=0 is matched, act=drop                                                                                                |
| 07:08:02 | after lsoope_captive_check(): is_captive=0, ret=match                                                                        |
| 07:08:02 | after lsoope_captive_check(): is_captive=0, ret-matched,act=drop                                                             |
| 07:08:02 | Denied by forward policy check [policy 0]                                                                                    |

**FORTINET**  
Training Institute

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**

## 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



© Fortinet Inc. All Rights Reserved. 15

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.

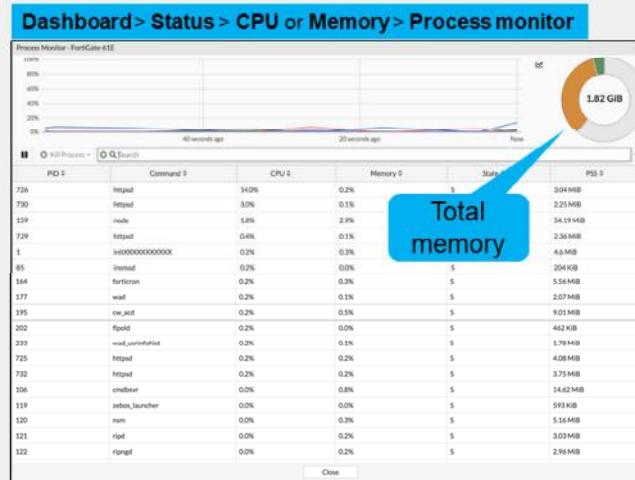
If usage is high, there are tools that can identify which feature is consuming the most CPU. Additionally, you can troubleshoot faster if you know precisely which change (if any) corresponds with the time the problem began.

# 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
 pyfcgid 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
 pyfcgid 249 S 0.0 3.0
 pyfcgid 246 S 0.0 2.8
reportd 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
- reportdk
- 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-red <percentage>
 set memory-use-threshold-extreme <percentage>
 set memory-use-threshold-green <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: Packets are dropped for new incoming sessions.
```



© Fortinet Inc. All Rights Reserved. 19

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:

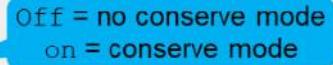
- off:** All new sessions with content scanning enabled are not passed but FortiGate processes the current active sessions.
- pass (default):** All new sessions pass without inspection until FortiGate switches back to non-conserve mode.
- one-shot:** Similar to `pass` in that traffic passes without inspection. 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. 21

The diagnose hardware sysinfo conserve command is used to identify if a FortiGate device is currently in memory conserve mode.

**DO NOT REPRINT****© FORTINET**

## Fail-Open Session Setting

- The following setting controls how FortiOS handles a session that is impacted by a unified threat management (UTM) scan error when doing http/mapi proxy or explicit webproxy

```
config system global
 set av-failopen-session [enable | disable]
```

- enable = Sessions are allowed
- disable(default) = Block all new sessions that require proxy-based inspection



© Fortinet Inc. All Rights Reserved. 22

Another undesirable state for FortiGate is the fail-open session mode. This mode kicks in, not during a high-memory situation, but when a proxy on FortiGate runs out of available sockets to process more proxy-based inspected traffic.

If `av-failopen-session` is enabled, FortiGate allows all the sessions. Otherwise, by default, it blocks new sessions that require proxy-based inspection until new sockets become available.

**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**

## 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®**



**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© 2023 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.