

**DO NOT REPRINT**  
**© FORTINET**



# FortiGate Infrastructure Study Guide

for FortiOS 7.2



**FORTINET®**  
Training Institute

# DO NOT REPRINT © FORTINET

## **Fortinet Training**

<https://training.fortinet.com>

## **Fortinet Document Library**

<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 Support**

<https://support.fortinet.com>

## **FortiGuard Labs**

<https://www.fortiguards.com>

## **Fortinet Network Security Expert Program (NSE)**

<https://training.fortinet.com/local/staticpage/view.php?page=certifications>

## **Fortinet | Pearson VUE**

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

## **Feedback**

Email: [askcourseware@fortinet.com](mailto:askcourseware@fortinet.com)



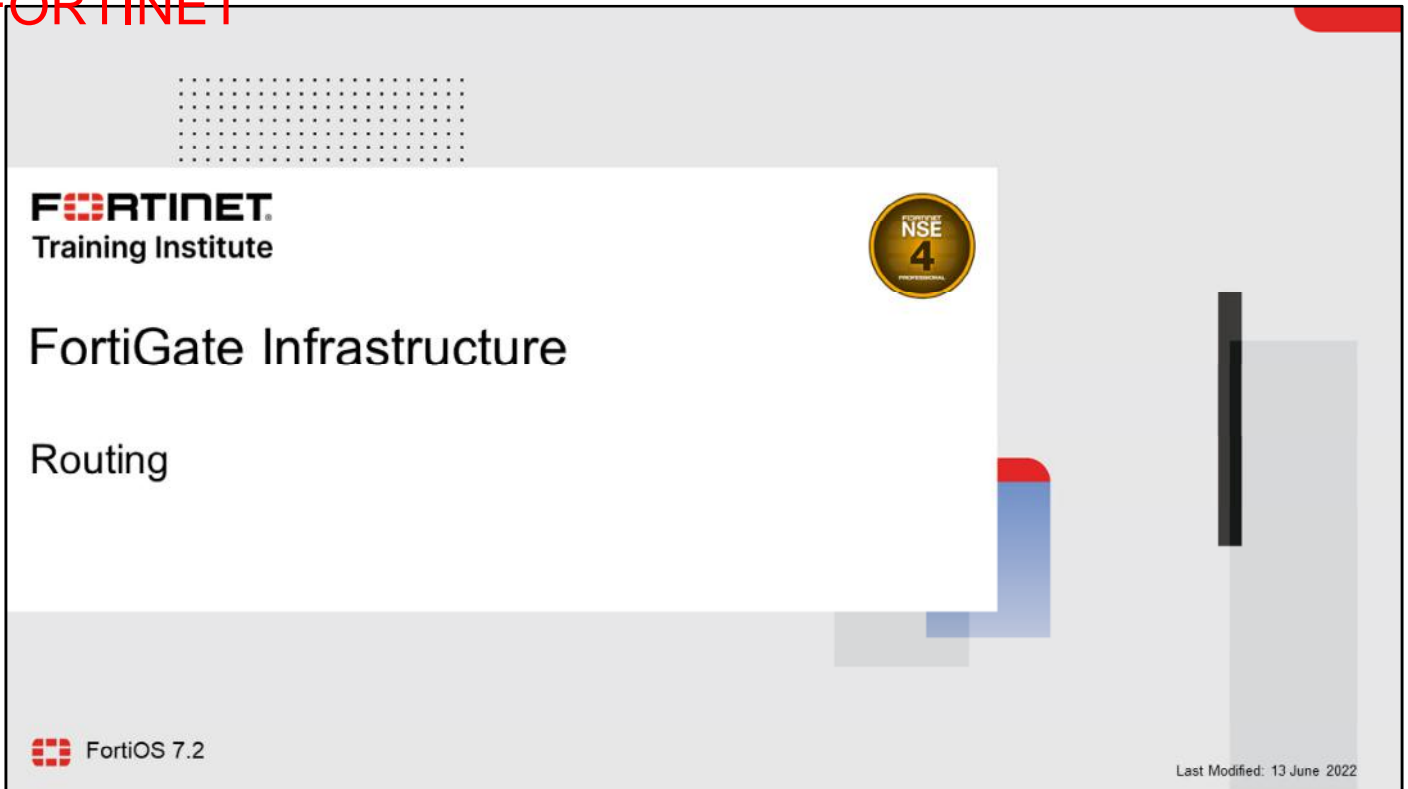
6/13/2022

## TABLE OF CONTENTS



<b>01 Routing</b> .....	<b>4</b>
<b>02 Virtual Domains (VDOMs)</b> .....	<b>67</b>
<b>03 Fortinet Single Sign-On (FSSO)</b> .....	<b>115</b>
<b>04 ZTNA</b> .....	<b>161</b>
<b>05 SSL VPN</b> .....	<b>191</b>
<b>06 IPsec VPN</b> .....	<b>228</b>
<b>07 High Availability</b> .....	<b>285</b>
<b>08 Diagnostics</b> .....	<b>342</b>

DO NOT REPRINT  
© FORTINET



The slide features a white background with a grid of dots in the top left corner. The Fortinet logo is positioned in the top left, with the text "FORTINET Training Institute" below it. To the right of the logo is a gold circular badge with "NSE 4" and "PROFESSIONAL" text. The main title "FortiGate Infrastructure" is centered, with "Routing" below it. In the bottom left, there is a FortiOS 7.2 logo. In the bottom right, it says "Last Modified: 13 June 2022". The slide is decorated with various geometric shapes in red, blue, and grey.

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

**DO NOT REPRINT**  
**© FORTINET**

## Lesson Overview

- Routing on FortiGate
- Routing Monitor and Route Attributes
- Equal Cost Multipath Routing (ECMP)
- Reverse Path Forwarding (RPF)
- Link Health Monitor and Route Failover
- Diagnostics

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

DO NOT REPRINT  
© FORTINET

## Routing on FortiGate

### Objectives

- Identify the routing capabilities on FortiGate
- Configure static routing
- Implement policy routes
- Route traffic for well-known internet services

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

By demonstrating competence in routing on FortiGate, you should be able to implement static and policy routing. You will also be able to route traffic for well-known internet services.

## What Is IP Routing?

- FortiGate acts as an IP router in 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 or another router along the path
- 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
    - Routes 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

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

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

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—that is, multiple routes to the same destination—it uses various route attributes as a tiebreak 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.

## 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:

```
# 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)
tab=255 vf=0 scope=253 type=3 proto=2 prio=0 0.0.0.0/0.0.0.0/0->10.200.1.0/32 pref=10.200.1.1 gwy=0.0.0.0 dev=3(port1)
...
```

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

## 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

## Static Routes

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

Network > Static Routes

New Static Route

Destination	Subnet	Named Address	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  Disabled

Advanced Options

Priority: 1

Default route

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 **IP/Netmask** or **FQDN** can be used as destinations for static routes

The screenshot displays two configuration windows from the Fortinet GUI. On the left, the 'Policy & Objects > Addresses' window shows the 'New Address' configuration. The 'Name' field is 'REMOTE\_SUBNET2'. The 'Type' is 'Subnet'. The 'Static route configuration' checkbox is checked. On the right, the 'Network > Static Routes' window shows the 'New Static Route' configuration. The 'Destination' dropdown is set to 'Named Address' and 'REMOTE\_SUBNET2'. The 'Gateway Address' is '10.200.2.254', the 'Interface' is 'port2', and the 'Administrative Distance' is '10'. A red arrow points from the 'REMOTE\_SUBNET2' field in the 'New Address' window to the 'REMOTE\_SUBNET2' field in the 'New Static Route' window.

If you create a firewall address object with the type **IP/Netmask** 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.

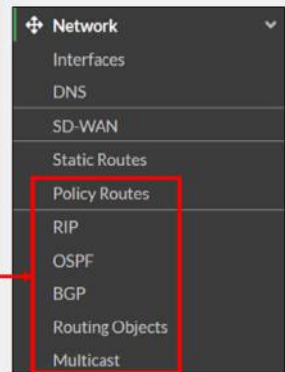
DO NOT REPRINT  
© FORTINET

## Dynamic Routes

- Routes are automatically learned
  - FortiGate exchanges routes with trusted adjacent routers
  - No need to configure manual routes
    - Useful for large networks with multiple subnets
- Supported dynamic routing protocols:
  - Routing Information Protocol (RIP)
  - Open Shortest Path First (OSPF)
  - Border Gateway Protocol (BGP)
  - Intermediate System to Intermediate System (IS-IS)
    - Must be configured on the FortiGate CLI

Enable **Advanced Routing** to display the GUI configuration pages for policy routes, RIP, OSPF, BGP, routing objects, and multicast

### System > Feature Visibility



**FORTINET**  
Training Institute

© Fortinet Inc. All Rights Reserved.

9

For large networks, manually configuring hundreds of static routes may not be practical. Your FortiGate can help, by learning routes automatically. FortiGate supports several dynamic routing protocols: RIP, OSPF, BGP, and IS-IS.

In dynamic routing, FortiGate communicates with trusted adjacent routers to exchange routing information about their known networks. Then, FortiGate adds the learned routes into its local routing table and considers them during the route lookup process.

You can configure dynamic routing for RIP, OSPF, and BGP protocols using the FortiGate GUI. You just need to make sure that the **Advanced Routing** option in the **Feature Visibility** page is enabled—it's enabled by default. However, for configuring IS-IS, you must use the FortiGate CLI.

Note that when you enable **Advanced Routing** on the **Feature Visibility** page, you also enable the configuration pages for other advanced routing features such as **Policy Routes**, **Routing Objects**, and **Multicast**. You will learn more about policy routes in this lesson.

Larger networks also may need to balance the routing load among multiple valid paths and detect and avoid routers that are down. You will learn more about that in this lesson.

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 routing table entries
- Separate table: policy route table
- Best practice: narrow down matching criteria

Network > Policy Routes

New Routing Policy

If incoming traffic matches:

Incoming interface: port5

Source Address: IP/Netmask 10.0.1.0/24

Addresses: +

Destination Address: IP/Netmask 10.10.10.10/32

Addresses: +

Internet service: +

Protocol: TCP UDP SCTP ANY Specify

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

Gateway address: 192.2.0.2

Comments: Write a comment... 0/255

Status: Enabled Disabled

Matching criteria

Action

**FORTINET**  
Training Institute

© Fortinet Inc. All Rights Reserved.

10

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.

Policy routes are maintained in a separate routing table by FortiGate and have precedence over the entries in the routing table. Because of its precedence, it is a best practice to narrow down the matching criteria of policy routes as much as possible. Otherwise, traffic that is expected to be routed using standard routing, that is, based on the destination address only and the routing table entries, could be handled by 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—**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: IP/Netmask 10.0.1.0/24

Destination Address: IP/Netmask 10.10.10.10/32

Protocol: TCP UDP SCTP ANY Specify

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

Gateway address: 192.2.0.2

Comments: Write a comment... 0/255

Status: Enabled Disabled

Action

**FORTINET**  
Training Institute

© Fortinet Inc. All Rights Reserved.

11

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—**Forward Traffic** action—or it stops checking the policy routes—**Stop Policy Routing** action—so the packet is routed based on the routing table.

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.

DO NOT REPRINT  
© FORTINET

## Internet Services Routing

- Route well-known internet services through specific interfaces

**Policy & Objects > Internet Service Database**

Name	Direction	Number of Entries
Amazon-AWS	Both	14,015
Amazon-AWS.WorkSpaces.Gateway	Destination	27
Amazon-DNS	Destination	41,821
Amazon-FTP	Destination	41,821
Amazon-ICMP	Destination	41,821

**Network > Static Routes**

New Static Route

Destination:  Subnet  Named Address  Internet Service

Destination: Amazon-AWS

Gateway Address: 10.200.1.254

Interface: port1

Comments: Write a comment... 0/255

Status:  Enabled  Disabled

OK Cancel

Database containing IP addresses, protocols, and port numbers used by most common Internet services

**FORTINET**  
Training Institute

© Fortinet Inc. All Rights Reserved.

12

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

## IPv6 Routing

- Enable the IPv6 feature to support IPv6 routing configuration using the GUI
  - Allows static and policy route configuration using IPv6 addresses
  - Enables GUI configuration options of IPv6 versions of dynamic routing protocols

The screenshot displays the Fortinet GUI configuration interface. On the left, the 'System > Feature Visibility' menu is open, showing 'Core Features' with 'IPv6' highlighted by a red box. A red arrow points from this box to the 'IPv6 Static Route' option in the 'Network > Static Routes' dropdown menu. The main area shows a table of static routes with two entries, both enabled.

Gateway IP	Interface	Status	Comments
0.0.0.0/0	port1	Enabled	
0.0.0.0/0	port2	Enabled	

**FORTINET**  
Training Institute

© Fortinet Inc. All Rights Reserved.

13

To enable routing configuration for IPv6 addresses using the GUI, you must enable **IPv6** in the **Feature Visibility** menu. Then, you can create static routes and policy routes with IPv6 addresses. Enabling the IPv6 feature also enables GUI configuration options for IPv6 versions of the dynamic routing protocols.

DO NOT REPRINT  
© FORTINET

## Knowledge Check

1. Which objects can you use to create static routes?
  - ✓ A. ISDB objects
  - B. Service objects
2. When the **Stop policy routing** action is used in a policy route, which behavior is expected?
  - A. FortiGate skips over this policy route and tries to match another in the list.
  - ✓ B. FortiGate routes the traffic based on the regular routing table.

DO NOT REPRINT  
© FORTINET

## Lesson Progress

- Routing on FortiGate
- Routing Monitor and Route Attributes
- Equal Cost Multipath Routing (ECMP)
- Reverse Path Forwarding (RPF)
- Link Health Monitor and Route Failover
- Diagnostics

Good job! You now understand routing on FortiGate.

Now, you will learn about routing monitor and route attributes.

DO NOT REPRINT  
© FORTINET

## Routing Monitor and Route Attributes

### Objectives

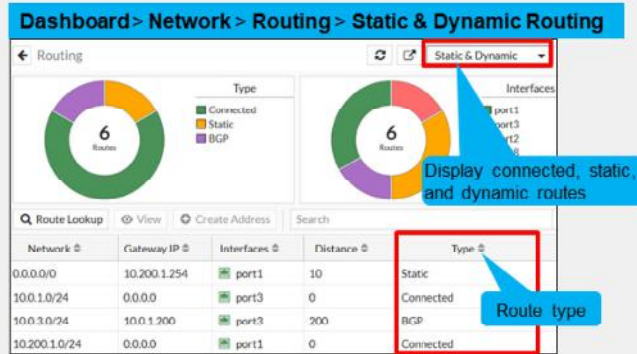
- Interpret the routing table on FortiGate
- Identify how FortiGate decides which routes are installed in the routing table
- Identify how FortiGate chooses the best route using route attributes

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

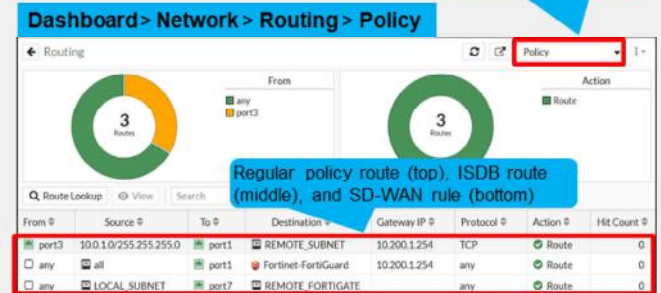
By demonstrating competence in understanding the routing monitor and route attributes, you should be able to interpret the routing table, identify which routes are installed in the routing table, and identify how FortiGate chooses the best route using route attributes.

## 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



- Policy route table (**Policy**) view
  - Displays all configured policy routes:
    - Regular policy routes, ISDB routes, and SD-WAN rules



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

## GUI Route Lookup Tool

- Look up route by:
  - Destination address (required)
  - Destination port, source address, 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

Dashboard > Network > Routing

Route Lookup

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
10.0.3.0/24	10.0.1.200	port3	200	BGP

Route Lookup

FortiGate

Destination: 8.8.8.8

Destination Port: 1-65535

Source: IP or FQDN

Protocol: TCP

Source Interface:

You are redirected to the policy page if you enter all attributes

Matching route

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

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, 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

## Route Attributes

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

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

Dashboard > Network > Routing > Static & Dynamic Routing

Network	Gateway IP	Interfac...	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)

Best Fit All Columns

Reset Table

Select Columns

- Network
- Gateway IP
- Interfaces
- Distance
- Type
- Metric
- Priority
- Up Since
- VRF

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

Display routing table entries on the CLI

```
...
Routing table for VRF=0
S* 0.0.0.0/0 [10/0] via 10.200.1.254, port1, [10/0]
C 10.0.1.0/24 is directly connected, port3
R 10.0.3.0/24 [200/0] via 10.0.1.200 (recursive is directly connected, port3), 23:21:46, [1,0]
O 10.0.4.0/24 [110/2] via 10.0.1.200, port3, 17:29:25, [1,0]
R 10.0.5.0/24 [120/2] via 10.0.1.200, port3, 00:05:29, [1,0]
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
```

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.

# 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
  - Multiple equal-distance duplicate routes but different protocol:
    - FortiGate keeps the route that was learned last (*avoid*)
- Default distance per route type:

Dashboard > Network > Routing > Static & Dynamic

Network	Gateway IP	Interfac...	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

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

\* Hardcoded

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. You will learn more about the routing table database in this lesson.

You can set the distance for all route types except connected and IS-IS routes. 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.

## 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 > Routing > Static & Dynamic

Network ↕	Gateway IP ↕	Interfac... ↕	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

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

Destination: Subnet | Named Address  
0.0.0.0/0.0.0.0

Gateway Address: 10.200.1.254

Interface: port1

Administrative Distance: 10

Comments: Write a comment...

Status: Enabled | Disable

Advanced Options

Priority: 10

### Dashboard > Network > Routing > 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

New in FortiOS 7.2; useful for advanced routing deployments

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.

Starting FortiOS 7.2, the priority attribute applies to all routes except connected routes and is set to 1 by default. Before FortiOS 7.2, the attribute applied to static routes only and was set to 0 by default. When you upgrade to FortiOS 7.2, FortiOS automatically increases the priority of static routes by 1, and a value of 0 is not longer valid.

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

## 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. Which routes are installed in the routing table?  
 A. Best active routes  
 B. Policy routes

DO NOT REPRINT  
© FORTINET

## Lesson Progress

- Routing on FortiGate
- Routing Monitor and Route Attributes
- Equal Cost Multipath Routing (ECMP)
- Reverse Path Forwarding (RPF)
- Link Health Monitor and Route Failover
- Diagnostics

Good job! You now understand the routing monitor and route attributes.

Now, you will learn about ECMP routing.

DO NOT REPRINT  
© FORTINET

## ECMP Routing

### Objectives

- Identify the requirements for ECMP routing
- Implement route redundancy and load balancing

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

By demonstrating competence in ECMP, you should be able to identify the requirements for implementing ECMP and ECMP load balancing.

# DO NOT REPRINT © FORTINET

## ECMP

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

### Dashboard > Network > Routing > Static & Dynamic

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

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

```
...
```

```
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
```

Two ECMP static routes, two ECMP BGP routes, and two ECMP OSPF routes (same destination, distance, metric, and priority)

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.

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.

## 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
```

- Configure spillover thresholds on the CLI (kbps):

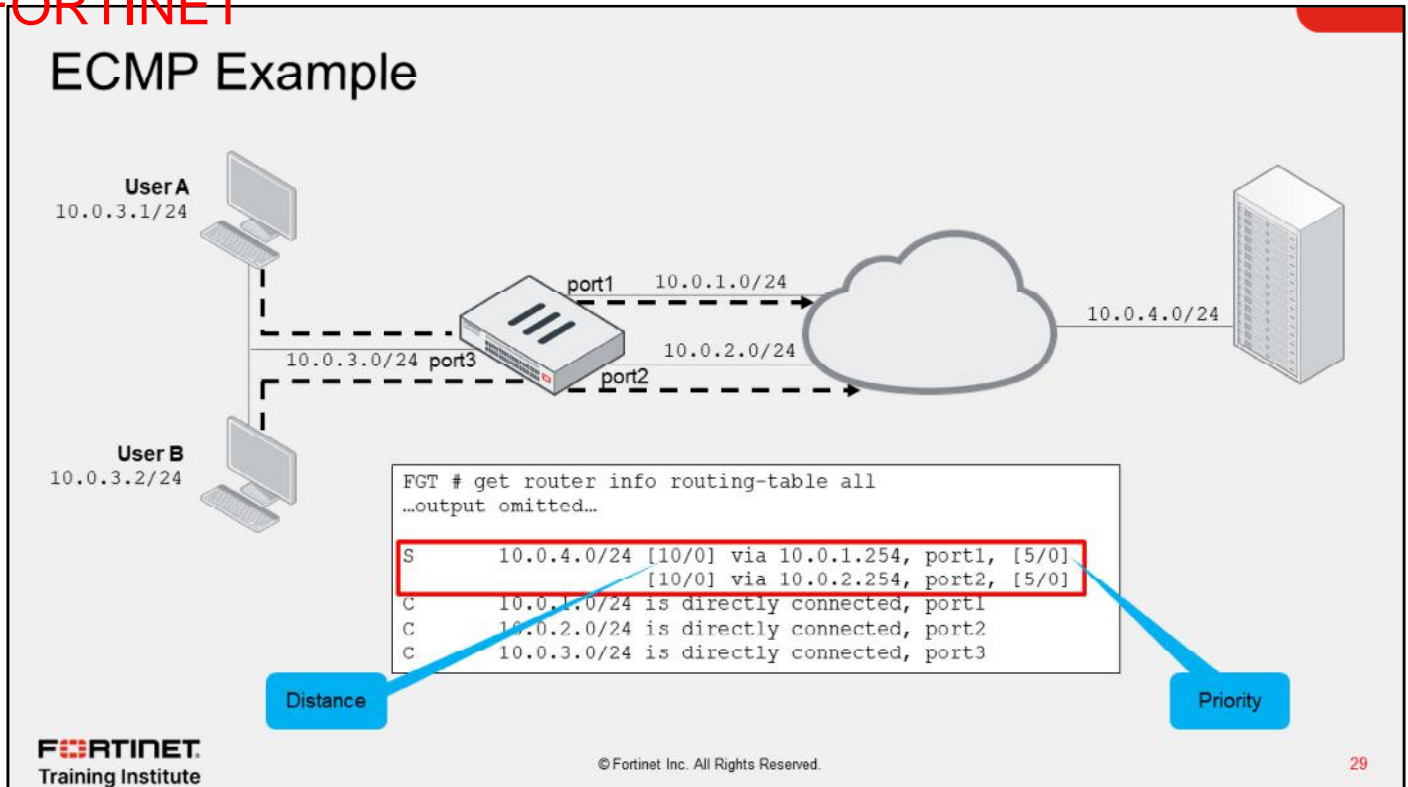
```
config system interface
  edit <interface name>
    set spillover-threshold <0-16776000>
    set ingress-spillover-threshold <0-16776000>
  next
end
```

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 weighted algorithm, you must configure the weights on the interface level or route level, as shown on this slide.

DO NOT REPRINT  
© FORTINET



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.

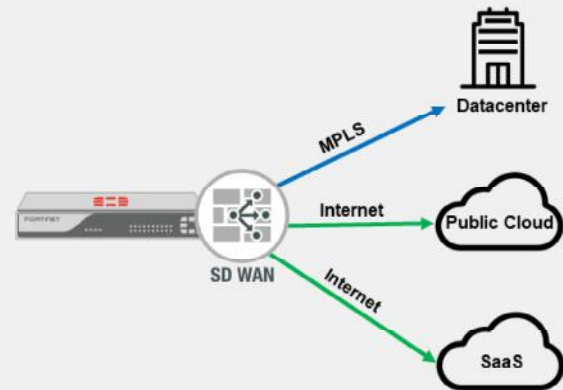
In the example shown on this slide, FortiGate selects the route over port1 for user A, and the route over port2 for user B. FortiGate continues to use the same selected routes for the same traffic. In the route over port1 is removed from the routing table, FortiGate automatically starts to forward the 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.

## What Is SD-WAN?

- Software-defined approach to steer WAN traffic using:
  - A collection of FortiOS features
  - 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 usage
  - 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. Fortinet implementation of SD-WAN is called secure SD-WAN because it also provides security by leveraging the built-in security features available in FortiOS.

Secure SD-WAN relies on well-known FortiOS features such as IPsec, auto-discovery VPN (ADVPN), 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.

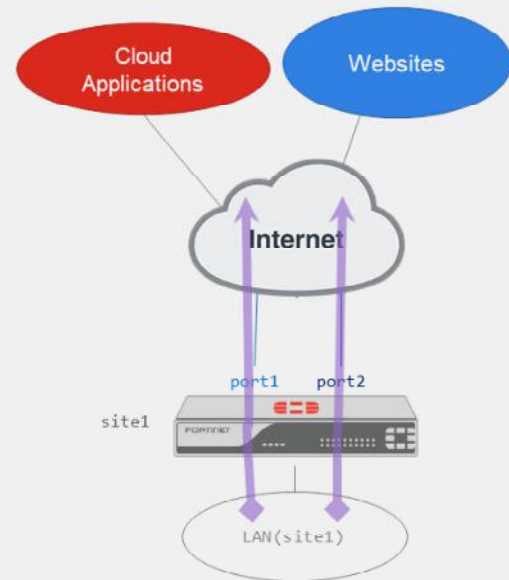
One benefit of SD-WAN is effective WAN usage. That is, you can use public (for example, broadband, LTE) and private (for example, MPLS) links to securely steer traffic to different destinations: internet, public cloud, private cloud, and the corporate network. This approach of using different types of links to connect sites to private and public networks is known as hybrid WAN. A hybrid WAN reduces costs mainly because administrators usually steer more traffic over low-cost fast internet links than 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 an 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. Also, the support of ADVPN shortcuts enables SD-WAN to use direct IPsec tunnels between sites to steer traffic, resulting in lower latency for traffic between the sites (spokes), and less load on the central locations (hubs).

**DO NOT REPRINT**  
**© FORTINET**

## Direct Internet Access With SD-WAN

- Traffic steered across multiple 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



**FORTINET**  
 Training Institute

© Fortinet Inc. All Rights Reserved.

31

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 (also known as members). The links are connected to FortiGate using different types of physical interfaces: physical port, VLAN, link aggregation (LAG), USB modem, or through FortiExtender.

Usually, sensitive traffic is expedited and steered over the best performing links, while non-critical traffic is distributed 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.

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.

The example on this slide shows a basic DIA deployment. FortiGate has two internet links. One link is connected to port1 and the other to port2. FortiGate uses both links to steer traffic sourced from the LAN and destined to cloud applications and websites on the internet.

# DO NOT REPRINT © FORTINET

## SD-WAN Rules

- Define steering rules based on:
  - Matching traffic criteria
  - Member preference
  - Member performance
- Evaluated from top to bottom:
  - Rules are used to steer traffic
    - Firewall policy required
  - Implicit rule
    - Used if user-defined rules are not matched
    - Usually, traffic is load balanced
- SD-WAN rules are policy routes
  - Route lookup order:
    - Regular policy routes
    - ISDB routes
    - SD-WAN rules
    - FIB entries

ID	Name	Source	Destination	Criteria	Members	Hit Count
1	Critical-DIA	all	GoToMeeting Microsoft.Office.365.Portal Salesforce	Latency	port1 <input checked="" type="checkbox"/> port2 <input type="checkbox"/>	0
2	Non-Critical-DIA	all	Facebook Twitter		port2 <input type="checkbox"/>	0
Implicit						
	sd-wan	all	all	Source IP	any	

SD-WAN rules represent the intelligence of the SD-WAN solution and the software-defined aspect of it. When you configure an SD-WAN rule, you first define the application or traffic pattern to match. After that, you indicate the preferred members and/or zones to steer the matching traffic to, and in some cases, the performing metrics that the member must meet to be eligible for steering traffic.

SD-WAN rules are evaluated 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, and *not* to allow traffic. That is, you must configure corresponding firewall policies to allow the SD-WAN traffic. If none of the user-defined SD-WAN rules are matched, then the implicit rule is used. The implicit rule instructs FortiGate to perform standard routing on traffic. Because SD-WAN deployments usually have multiple routes to the same destination—that is, ECMP routes—then traffic that matches the implicit rule is usually load balanced across multiple SD-WAN members.

SD-WAN rules are essentially 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. When FortiGate performs a route lookup, it checks the routes in the order of sequence shown on this slide. For example, SD-WAN rules have precedence over FIB entries, but not over regular policy routes.

The example on this slide shows two user-defined rules named **Critical-DIA** and **Non-Critical-DIA**, which are used to steer traffic in our basic DIA setup. The **Critical-DIA** steers **GoToMeeting**, **Microsoft.Office.365.Portal**, and **Salesforce** traffic to the member with the lowest latency, between **port1** and **port2**. The example shows that **port1** is selected because it is the member with the check mark beside it. The **Non-Critical-DIA** rule steers Facebook and Twitter traffic to **port2**. The implicit rule, located at the bottom of the list, is used if none of the two user-defined rules are matched.

## System Settings Algorithm vs. Implicit Rule Algorithm

- Both `v4-ecmp-mode` and `load-balance-mode` control the ECMP algorithm
  - `load-balance-mode` replaces `v4-ecmp-mode` when SD-WAN is enabled
- Differences:
  - `load-balance-mode` supports the volume algorithm, `v4-ecmp-mode` does not
  - `load-balance-mode` uses the weight defined under the SD-WAN member configuration, `v4-ecmp-mode` the weight defined in the static route
  - `load-balance-mode` uses the spillover thresholds defined under the SD-WAN member configuration, `v4-ecmp-mode` the spillover thresholds defined in the interface settings
- Volume algorithm:
  - FortiGate tracks the cumulative number of bytes of the member
  - The higher the member weight, the higher the target volume, the more traffic is sent to it

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

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

When you set the ECMP algorithm to volume, 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. What is the default ECMP algorithm on FortiGate?
  - A. Weighted
  - ✓ B. Source IP
  
2. How does FortiGate load balance traffic when using the spillover algorithm in ECMP routing?
  - ✓ A. Sessions are distributed based on interface threshold.
  - B. Sessions are distributed based on route weight.

DO NOT REPRINT  
© FORTINET

## Lesson Progress

- Routing on FortiGate
- Routing Monitor and Route Attributes
- Equal Cost Multipath Routing (ECMP)
- Reverse Path Forwarding (RPF)
- Link Health Monitor and Route Failover
- Diagnostics

Good job! You now understand ECMP routing.

Now, you will learn about reverse path forwarding.

DO NOT REPRINT  
© FORTINET

## RPF

### Objectives

- Identify how FortiGate detects IP spoofing
- Block traffic from spoofed IP addresses
- Differentiate between and implement the different RPF check methods

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

By demonstrating competence in RPF, you should be able to identify and block IP spoofing attacks in your network.

# DO NOT REPRINT © FORTINET

## RPF

- 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:

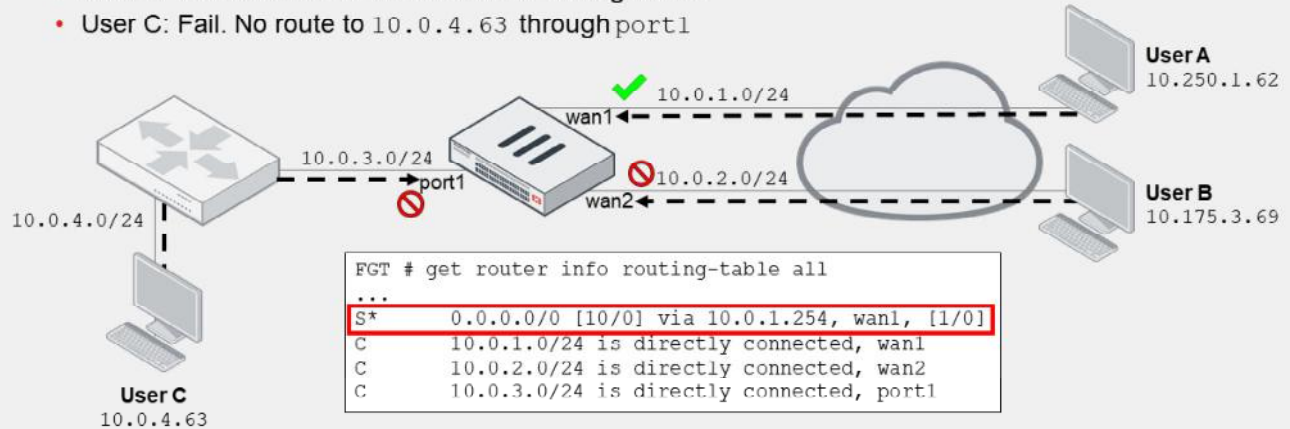
- Feasible path: Formerly known as loose, it's the default mode. In this mode, FortiGate verifies that the routing table contains a route that matches the source address of the packet and the incoming interface. The matching route doesn't have to be the best route in the routing table for that source 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

## RPF—Feasible Path Example

- FortiGate checks for a route matching source address and incoming interface
- RPF check results:
  - User A: Pass. Default route through wan1
  - User B: Fail. No route to 10.175.3.69 through wan2
  - User C: Fail. No route to 10.0.4.63 through port1



The example on this slide shows a FortiGate device using the feasible path RPF check mode. When FortiGate performs RPF check, it checks in the routing table for a route that matches the source address and the incoming interface of the first original packet.

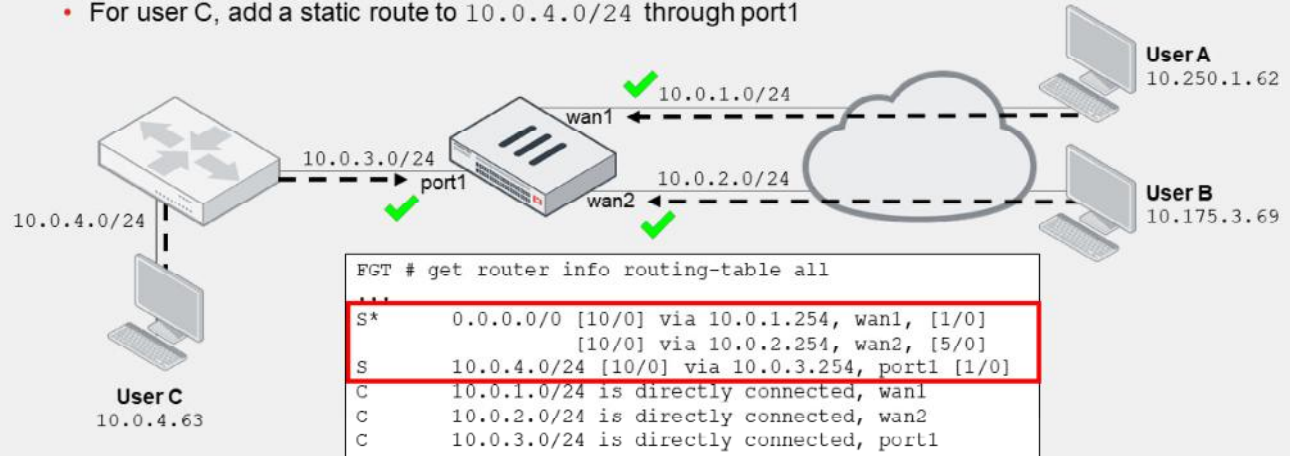
Based on the topology and routing table shown on this slide, the RPF check results for traffic sourced from each user are:

- User A: Pass. There is a default route through wan1. This means that, all packets received at wan1 pass the RPF check regardless of the source address.
- User B: Fail. FortiGate doesn't have a route to 10.175.3.69 through wan2 in its routing table.
- User C: Fail. Like the user B case, FortiGate doesn't have a route to 10.0.4.63 through port1 in its routing table.

DO NOT REPRINT  
© FORTINET

## RPF—Feasible Path Example (Contd)

- Solution:
  - For user B, add a second static default route, with the same distance, through wan2
    - Use different priority values if you don't want ECMP
  - For user C, add a static route to 10.0.4.0/24 through port1



**FORTINET**  
Training Institute

© Fortinet Inc. All Rights Reserved.

39

If you consider the packets from user B and user C to be legit packets, you can solve the RPF check fail issue by making sure the routing table contains routes for the return path.

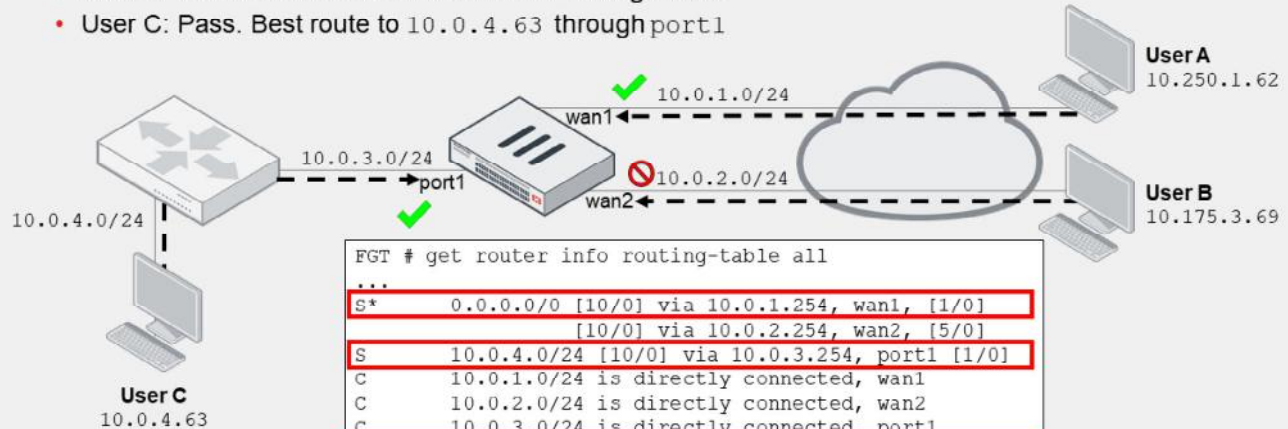
In the example shown on this slide, the administrator adds two new static routes. The static route through wan2 is a duplicate default route of wan1, but has a lower priority. The two default routes are not ECMP routes because of the priority difference, but FortiGate keeps both routes in the routing table. The result is that packets from user B now pass the RPF check.

The static route through port1 references the 10.0.4.0/24 subnet. The subnet includes user C address (10.0.4.63), and as result, packets from user C also pass the RPF check.

# DO NOT REPRINT © FORTINET

## RPF—Strict Example

- FortiGate also checks if the return path is the best route
- RPF check results:
  - User A: Pass. Best route to 10.250.1.62 through wan1 (default route)
  - User B: Fail. Best route to 10.175.3.69 through wan1
  - User C: Pass. Best route to 10.0.4.63 through port1



The example on this slide shows a FortiGate device using the strict RPF check mode. In strict mode, FortiGate also checks if the matching route is the best route to the source.

Based on the topology and routing table shown on this slide, the RPF check results for traffic sourced from each user are:

- User A: Pass. There is a default route through wan1. The route is also the best (and only) route to 10.250.1.62.
- User B: Fail. There is a default route through wan2. However, there is better (more specific) static route to 10.175.3.69 through wan1.
- User C: Pass. FortiGate has a route to 10.0.4.63 through port1 in its routing table. Although the default routes through wan1 and wan2 are also valid routes for 10.0.4.63, the best route to user C is the route through port1.

Like the feasible path example, you can solve the RPF fail issue for user B by making the respective changes in the routing table so the best route to user B is through wan2.

DO NOT REPRINT  
© FORTINET

## Knowledge Check

1. What is the default RPF check method on FortiGate?
  - ✓ A. Feasible path
  - B. Strict
2. Which route lookup scenario satisfies the RPF check for a packet?
  - A. Routing table has a route to the destination IP of the packet through the incoming interface.
  - ✓ B. Routing table has a route for the source IP of the packet through the incoming interface.

DO NOT REPRINT  
© FORTINET

## Lesson Progress

- Routing on FortiGate
- Routing Monitor and Route Attributes
- Equal Cost Multipath Routing (ECMP)
- Reverse Path Forwarding (RPF)
- Link Health Monitor and Route Failover
- Diagnostics

Good job! You now understand RPF.

Now, you will learn about the link health monitor and route failover.

DO NOT REPRINT  
© FORTINET

## Link Health Monitor and Route Failover

### Objectives

- Configure the link health monitor
- Implement route failover
- Use the forward traffic logs

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

By demonstrating competence in configuring link health monitor and implementing route failover, you should be able to monitor the health of your interfaces and then, when a link is detected as dead, configure FortiGate to fail over the traffic to healthy links to minimize service disruption.

## Link Health Monitor

- Detect dead links when failure is beyond local physical connection
- Periodically send probes to up to four servers (beacons)
  - Choose at least two reliable servers to guard against server failure
  - Supported protocols: ping, TCP echo, UDP echo, HTTP, and TWAMP
- FortiGate operates as follows:
  - Initially, links are marked alive
  - Marks a link as dead after five consecutive failed probes from all configured servers
    - Performs any of the following actions: update static route, update policy route, and update cascade interface
  - Marks a link alive again after five consecutive successful probes from at least one server
    - Reverts any of the previous actions taken
  - The number of failed and successful probes can be adjusted (default = 5)

Static routes are kept in the routing table unless the associated interface is administratively down, its link goes down, or there is a duplicate route with a lower distance. Because it is possible that the link circuit is dead somewhere along the path to the destination, even though the interface link is up, then it is also possible that FortiGate continues to route traffic through a dead link, which would result in service impact. A common example is the Ethernet connection provided by your ISP modem. The Ethernet connection remains physically up even though the upstream ISP network is down. The devices behind your modem will continue to use the internet connection but they won't receive any replies.

Link health monitor enables FortiGate to detect dead links when the failure is beyond the local physical connection. FortiGate periodically sends probes through the configured gateway and interface to up to four servers that act as beacons. A server can be any host that is normally reachable through that path. It's best practice to configure at least two reliable servers to guard against false positives caused by the server being at fault, and not the link. For probes, you should also use a protocol that the server normally responds to.

Initially, FortiGate considers a link as alive. However, if FortiGate detects five consecutive failed probes from each of the configured servers, FortiGate marks the link as dead. FortiGate considers a failed probe a probe for which it does not receive a reply, or whose reply isn't valid. After FortiGate detects the link as dead, it performs any of the actions shown on this slide. The goal of these actions is to redirect the impacted traffic to other healthy links.

After FortiGate detects the link as dead, it continues to monitor the link. As soon as FortiGate receives five successful replies from at least one of the configured servers, it marks the link as alive again, and then reverts any of the previous actions taken on that link.

The number of failed and successful probes is set to five by default, but can be changed if required.

## Link Health Monitor Protocols

- Ping:
  - Most deployed
  - Sends ICMP echo requests and waits for ICMP echo replies
- TCP echo and UDP echo:
  - Sends TCP/UDP requests on port 7
  - Any data received by the server is sent back
- TWAMP:
  - Client-side implementation
  - Most accurate protocol
  - Two sessions:
    - Control: TCP 862 by default (if authentication is enabled)
    - Test: UDP 862 by default
- HTTP:
  - Sends an HTTP GET request and waits for response
  - Optionally, checks if the response contains the configured string

This slide describes the probe protocols supported by link health monitor.

Ping is the most used network monitoring protocol because it is supported by virtually all network devices. When you use ping, FortiGate sends ICMP echo requests to the configured target servers and waits for the respective ICMP echo replies. Because some ISPs and content providers block or limit ICMP traffic on their network, you may want to switch to TCP echo, UDP echo, or TWAMP.

When you use TCP echo and UDP echo, FortiGate sends periodic packets to the configured target servers, which are listening for connections on port 7 for both TCP and UDP. Upon reception of the packets, the server sends back an identical copy of the data it received from FortiGate.

Two-Way Active Measurement Protocol (TWAMP) is the most accurate protocol among the five. Link health monitor uses the client-side implementation of TWAMP. There are two sessions used in TWAMP: control and test. The former is used to authenticate the endpoints, and the latter to exchange packets used to measure the performance. Note that if authentication is disabled—it is disabled by default—FortiGate generates the test session only. FortiGate uses port 862 as default port for both control and test sessions, but you can configure a different port.

When you configure HTTP as the protocol, FortiGate sends periodic HTTP GET requests to the target server, and then waits for a response. Optionally, you can configure FortiGate to check if the response contains a specific string in the HTML content.

## Link Health Monitor Actions

Action	Dead	Alive	Effect during dead state
Update static route*	Flag associated static routes as inactive	Flag associate static routes as active	Static routes are removed from routing table
Update policy route**	Disable associated policy routes	Re-enable associated policy routes	Policy routes are skipped
Update cascade interface***	Bring down alert interfaces	Bring back up alert interfaces	Route LAN-originated traffic to a different device

\* Associated static routes match the configured gateway and interface in the link health monitor settings

\*\* Associated policy routes match the configured gateway and interface in the link health monitor settings

\*\*\* Require the configuration of alert interfaces (usually, your LAN-facing interfaces)

This slide describes the actions taken by link health monitor when the state of an interface changes from alive to dead, and vice-versa. All three actions are enabled by default.

When you enable update static route and link health monitor detects an interface as dead, FortiGate marks the associated static routes—those matching the configured gateway and interface—as inactive. The result is that the inactive static routes are removed from the routing table. The absence of such routes can then force FortiGate to redirect the traffic to other valid routes, if any. Note that this action applies to static routes only.

The update policy route action works the same as the update static route action, except that instead of marking the associated static routes as inactive after an interface is detected as dead, FortiGate disables the associated policy routes. For that, FortiGate checks the policy route table and disables the policy routes whose outgoing interface and gateway match the configured interface and gateway in the link health monitor settings. Like the update static route action, the goal is for FortiGate to skip the disabled policy route during the route lookup process, so the traffic matches another policy route or FIB route in the system.

The update cascade interface action requires you to configure one or more alert interfaces. FortiGate then brings down the alert interfaces after the monitoring interface is detected dead. The goal is to force the traffic from networks behind the alert interfaces to be routed through a different device after an important interface, such as the internet-facing interface, is dead, which could mean that FortiGate is unable to forward traffic to the WAN. For example, if you are using dynamic routing or Virtual Router Redundancy Protocol (VRRP) on your LAN interface, which is configured as an alert interface, then bringing down the interface can trigger a routing failover to a backup gateway.

If FortiGate detects the interface as alive again, it reverts any action taken so far for the link. That is, FortiGate restores static routes, re-enables policy routes, and brings back up alert interfaces.

## Link Health Monitor Configuration Example

- Configure link health monitor on the FortiGate CLI:

```
config system link-monitor
  edit port1-health
    set srcintf port1
    set server 4.2.2.1 4.2.2.2 8.8.8.8 8.8.4.4
    set gateway-ip 10.200.1.254
    set protocol ping
    set update-cascade-interface enable
    set update-static-route enable
    set update-policy-route enable
  next
end
```

Four servers (maximum is four)

Actions during dead state

- Configure port3 as alert interface if port1 is detected dead:

```
config system interface
  edit port1
    set fail-detect enable
    set fail-detect-option detectserver
    set fail-alert-method link-down
    set fail-alert-interfaces "port3"
  next
end
```

Detection by link health monitor

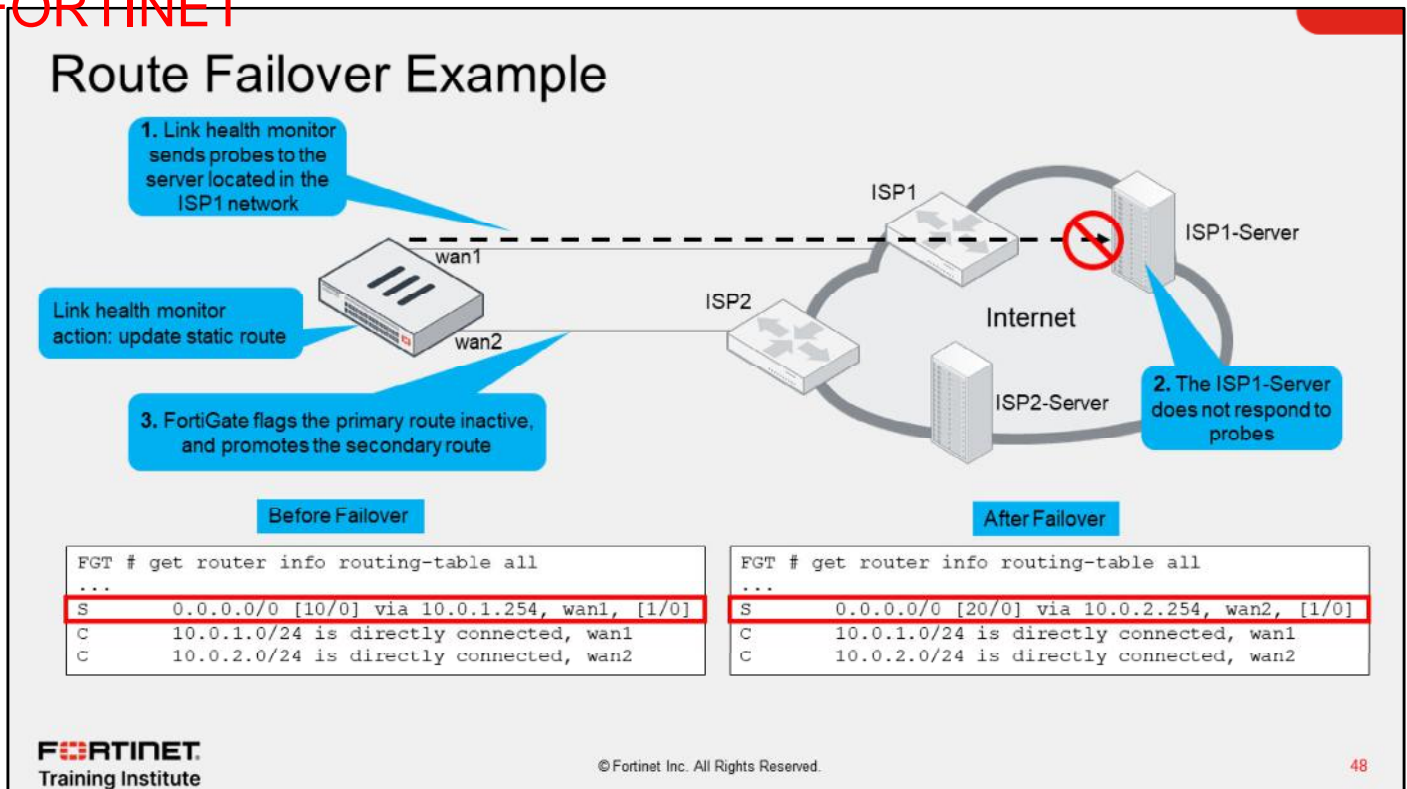
Action: bring down alert interfaces

port3 is the only alert interface

This slide shows a configuration example for link health monitor. FortiGate monitors the health of port1 against Level3 and Google DNS servers (four in total). For sending the probes, FortiGate uses 10.200.1.254 as gateway and ping as protocol.

When the state of port1 changes, FortiGate updates cascade interfaces, static routes, and policy routes. For the update cascade interface action to work, you must configure the alert interfaces. This slide also shows an example of the alert interface configuration required on the monitoring interface (port1). The configuration instructs FortiGate to bring down port3 if port1 is detected dead by the link health monitor feature.

DO NOT REPRINT  
© FORTINET



In the example shown on this slide, FortiGate has two internet connections. wan1 is connected to ISP1, and wan2 to ISP2. Within each ISP network, there is a server that FortiGate sends probes to for link health monitoring purposes. For link health monitor, the update static route action is enabled. The administrator configured two static default routes, one through wan1 and the other wan2. The static default routes are assigned a distance of 10 and 20, respectively.

Before failover, the default route over wan1 is installed in the routing table because it has a lower distance, and the default route through wan2 is present in the routing table database as a standby route. The link health monitor sends probes to ISP1-Server located within the ISP1 network through wan1. When FortiGate detects five consecutive failed probes for ISP1-Server, FortiGate flags the default route over wan1 as inactive, which results in the route being removed from the routing table. This also results in the standby default route through wan2 to be installed in the routing table. Then, FortiGate starts using the new default route to route traffic to the internet.

The example shown on this slide makes use of different distance values to control the primary and standby routes. The result is that one default route only is installed in the routing table at any time. In case you always need to have both routes installed in the routing table, you can configure the same distance on both routes, but different priorities. You assign a lower priority number to your primary route, and a higher priority number to your standby route. Having both routes in the routing table is required if you use the interfaces to terminate IPsec VPN tunnels and you want to speed up failover by ensuring the tunnel over the secondary ISP link is already up before failover.

## Best Practices—Forward Traffic Logs

- Use the **Destination Interface** column in the **Forward Traffic** logs to determine the egress interface for all traffic

### Log & Report > Forward Traffic

Date/Time	Source	Device	Destination	Application Name	Result	Policy ID	Destination Interface
11 seconds ago	10.0.1.200		208.91.112.52 (fortinet-public-dns-52.fortinet.com)		✓ 3.07 kB / 13.12 kB	Full_Access (1)	port1
13 seconds ago	10.0.1.200		208.91.112.53 (fortinet-public-dns-53.fortinet.com)		✓ 3.48 kB / 14.79 kB	Backup_Access (2)	port2
29 seconds ago	10.0.1.200		208.91.112.63 (ntp1.fortiguard.com)		✓ 76 B / 76 B	Backup_Access (2)	port2
30 seconds ago	10.0.1.200		208.91.112.61 (ntp1.fortiguard.com)		✓ 76 B / 76 B	Full_Access (1)	port1
39 seconds ago	10.0.1.200		208.91.112.62 (ntp2.fortiguard.com)		✓ 76 B / 76 B	Full_Access (1)	port1
45 seconds ago	10.0.1.200		208.91.112.60 (ntp2.fortiguard.com)		✓ 76 B / 76 B	Full_Access (1)	port1
Minute ago	10.0.1.10		54.186.52.97 (autopush.prod.mozaws.net)		✓ 6.01 kB / 9.76 kB	Full_Access (1)	port1
2 minutes ago	10.0.1.10		8.8.8.8 (dns.google)		✓ 92 B / 120 B	Backup_Access (2)	port2
2 minutes ago	10.0.1.10		8.8.8.8 (dns.google)		✓ 92 B / 108 B	Backup_Access (2)	port2

If you enable the **Destination Interface** column in the **Forward Traffic** logs, you can view the egress interface for traffic passing through your FortiGate device. You can use this information to determine which route is applied to which traffic stream, as well as identify any routing configuration issues.

If your firewall policies do not have any security profiles applied, you should enable logging for all sessions in your policies; otherwise, FortiGate does not generate any **Forward Traffic** logs. Use this feature with some caution, since enabling all sessions logging can generate a lot of logs if the firewall policy is handling a high volume of traffic. You should enable it when necessary, and disable it immediately afterwards.

DO NOT REPRINT  
© FORTINET

## Knowledge Check

1. What is the purpose of the link health monitor setting `update-static-route`?
  - A. It creates a new static route for the backup interface.
  - ✓ B. It removes all static routes associated with an interface detected as dead by the link health monitor.
2. When using link health monitoring, which route attribute can you configure to achieve route failover protection?
  - ✓ A. Distance
  - B. Metric

DO NOT REPRINT  
© FORTINET

## Lesson Progress

- Routing on FortiGate
- Routing Monitor and Route Attributes
- Equal Cost Multipath Routing (ECMP)
- Reverse Path Forwarding (RPF)
- Link Health Monitor and Route Failover
- Diagnostics

Good job! You now understand the link health monitor and route failover.

Now, you will learn about routing diagnostics.

**DO NOT REPRINT  
© FORTINET**

## Diagnostics

### Objectives

- View active, standby, and inactive routes
- View policy routes on the CLI
- Use the built-in packet capture tool

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

By demonstrating competence in routing diagnostics, you should be able to view the entries in the routing table and routing table database, as well as to identify how packets flow across FortiGate.

DO NOT REPRINT  
© FORTINET

## Routing Table

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

Routing table for VRF=0
S* 0.0.0.0/0 [10/0] via 10.200.1.254, port1, [10/2]
C 10.0.1.0/24 is directly connected, port3
B 10.0.3.0/24 [200/10] via 10.0.1.200 (recursive is directly connected, port3), 23:21:46, [1,0]
O 10.0.4.0/24 [110/2] via 10.0.1.200, port3, 17:29:25, [1,0]
R 10.0.5.0/24 [120/2] via 10.0.1.200, port3, 00:05:29, [1,0]
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

Priority/Weight

Priority/Weight

Distance/Metric

**FORTINET**  
Training Institute

© Fortinet Inc. All Rights Reserved.

53

The CLI command shown on this slide displays all entries in the routing table. The routing table displays the routes that make it to the FIB. That is, 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

## Routing Table Database

```
# get router info routing-table database
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
> - selected route, * - FIB route, p - stale info

Routing table for VRF=0
S *> 0.0.0.0/0 [10/0] via 10.200.1.254, port1, [1/10]
S 0.0.0.0/0 [20/0] via 10.200.2.254, port2, [5/0]
S 8.8.8.8/32 [10/0] via 172.16.100.254, port8 inactive, [1/0]
O 10.0.1.0/24 [110/1] is directly connected, port3, 00:05:47, [1/0]
C *> 10.0.1.0/24 is directly connected, port3
O 10.0.2.0/24 [110/1] is directly connected, port4, 00:05:47, [1/0]
C *> 10.0.2.0/24 is directly connected, port4
B *> 10.0.3.0/24 [200/10] via 10.0.1.200 (recursive is directly connected, port3), 00:05:40, [1/0]
O *> 10.0.4.0/24 [110/2] via 10.0.1.200, port3, 00:05:27, [1/0]
B 10.0.4.0/24 [200/10] via 10.0.1.200 (recursive is directly connected, port3), 00:05:40, [1/0]
C *> 10.200.1.0/24 is directly connected, port1
C *> 10.200.2.0/24 is directly connected, port2
```

If you want to view active, standby, and inactive routes, use the CLI command shown on this slide to display the routing table database entries.

In the example on this slide, the command shows two standby routes, one static and the other BGP. Both standby routes are standby because there are better routes—lower distance—to the same destination. The better routes show an asterisk next to the route source to indicate they are FIB entries, and therefore, are used for routing traffic.

The output also shows one inactive route. Routes are marked as inactive where the corresponding interface is administratively down, has its link down, or when the interface is detected dead by link health monitor and the update static route action is enabled.

## Policy Route Table

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

```
id=1 dscp_tag=0xff 0xff flags=0x0 tos=0x00 tos_mask=0x00 protocol=0 sport=0-0 iif=7 dport=0-65535
path(1) oif=21(T_MPLS_0)
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=2022-02-23 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=2022-02-23 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=0xff 0xff 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(4294836966,0,0,0, 16354)
Microsoft.Office.365.Portal(4294837474,0,0,0, 41468) Salesforce(4294837976,0,0,0, 16920)
hit_count=0 last_used=2022-02-23 05:46:43
```

This is an SD-WAN rule (ID > 65535 and the vwl\_service field is present)

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.

Note that although IDs for regular policy routes are in the 1 to 65535 range, the maximum number of regular policy routes that you can configure are much lower and varies among models. For example, you can configure up to 512 regular policy routes in a FortiGate 300D device. For more information about the maximum supported values per model, refer to the [FortiOS Maximum Values Table](https://docs.fortinet.com) on [docs.fortinet.com](https://docs.fortinet.com). Alternatively, you can run the `print tablesizes` command on the FortiGate CLI to get the maximum values for your device.

## Packet Capture

- Can be used to verify the ingress and egress interface of packets

```
# diagnose sniffer packet <interface> '<filter>' <verbosity> <count> <timestamp> <frame size>
```

- <interface> can be any or a specific interface (that is port1 or internal)
- <filter> follows tcpdump format
- <verbosity> specifies how much information to capture
- <count> number of packets to capture
- <timestamp> print time stamp information
  - a – prints absolute timestamp
  - l – prints local timestamp
- <frame size> specify length of up to a maximum size of 65K

Packet captures, or *sniffers*, are one of the most useful sources of information for debugging routing problems. FortiGate includes a built-in traffic sniffer tool. You can use it to verify the ingress and egress interfaces of packets as they pass through. You can run the built-in sniffer from either the GUI or the CLI. The syntax of the CLI command is shown on this slide.

The <interface> option is the name of the physical or logical interface to run the sniffer on. Most of the times, you want to indicate *any* to capture packets on all interfaces. This enables you to see how packets flow across the different interfaces. Another option is to indicate the name of the interface, which is useful when you want to narrow down the packet capture to that interface. Indicating the name of the interface is also required if you want the tool to capture the MAC address information. That is, when you use *any*, the sniffer doesn't capture the real MAC addresses used by the packet.

The filter follows the Berkeley Packet Filter (BPF) syntax used by the well-known tcpdump tool. You should configure specific filters to ensure you're only capturing what you need. You can also specify a <count> value to automatically stop the sniffer after capturing a specific number of packets. Otherwise, the sniffer continues capturing packets until you manually stop it using `Ctrl + C`. You can use the <time stamp> option to print the time stamp information. Use *a* to print the absolute time stamp, or *l* (lowercase L) to print the local time-zone based time stamp. Time stamp information is particularly useful when correlating sniffer output to debug flow messages. You will learn more about debug flow in another lesson.

By default, the sniffer uses the MTU configured on the interface to limit the packet length during the capture. Using the <frame size> argument, you can specify a length larger or smaller than the interface MTU. Note that if you use the *any* interface, the sniffer will default to 1600 bytes.

**DO NOT REPRINT**  
**© FORTINET**

## Packet Capture Verbosity Level

Level	IP Headers	Packet Payload	Ethernet Headers	Interface Name
1	•			
2	•	•		
3	•	•	•	
4	•			•
5	•	•		•
6	•	•	•	•

- The most common levels are:
  - 4 – Prints the ingress and egress interfaces
    - You can verify how traffic is being routed, or if FortiGate is dropping packets
  - 3 or 6 – Prints the packet payload
    - You can convert this output to a packet capture (pcap) file that can be opened with a packet analyzer
  - If you don't specify a level, the sniffer uses level 1 by default

The verbosity level specifies how much information you want to display. There are six different levels and this table shows which ones display the IP headers, packet payload, Ethernet headers, and interface names.

Use verbosity level 4 to take a quick look at how the traffic is flowing through FortiGate (if packets are arriving and how FortiGate is routing them out). You can also use level 4 to check if FortiGate is dropping packets.

Verbosity levels 3 and 6 provide the most output. Both show the IP payloads and Ethernet headers. You can save the output and export it to a packet capture (pcap) file using a Perl script. The pcap file can then be opened with a packet analyzer, such as Wireshark, for further investigation. You can locate the Perl script that converts the sniffer output to pcap on the Fortinet Knowledge Base website ([kb.fortinet.com](http://kb.fortinet.com)).

## Packet Capture Examples

```
# diagnose sniffer packet any "port 443" 4
```

All traffic to or from port 443 with verbosity 4

```
...
5.455914 port3 in 10.1.10.1.59785 -> 100.64.3.1.443: syn 457459
5.455930 port1 out 100.64.1.1.59785 -> 100.64.3.1.443: syn 457459
5.455979 port1 in 100.64.3.1.443 -> 100.64.1.1.59785: syn 163440 ack 457460
5.455991 port3 out 100.64.3.1.443 -> 10.1.10.1.59785: syn 163440 ack 457460
5.456012 port3 in 10.1.10.1.59785 -> 100.64.3.1.443: ack 725411
5.456025 port1 out 100.64.1.1.59785 -> 100.64.3.1.443: ack 725411
```

```
# diagnose sniffer packet Students "icmp and host 10.0.10.254" 6 0 1
```

All ICMP traffic to or from 10.0.10.254 with verbosity 6, no packet count (0), and with local timestamps (1)

```
...
2021-05-26 07:43:28.653443 Students -- 10.0.10.2 -> 10.0.10.254: icmp: e
0x0000 0009 0f09 0003 5c85 7e32 16a2 0800 4500 .....\.~2....E.
0x0010 0054 9fef 4000 4001 71ba 0a00 0a02 0a00 .T..@.@.q.....
0x0020 0afe 0800 cec5 1686 0001 905e ae60 dff0 .....^.\..
0x0030 0900 0809 0a0b 0c0d 0e0f 1011 1213 1415 .....
0x0040 1617 1819 1a1b 1c1d 1e1f 2021 2223 2425 .....!"#$%
0x0050 2627 2829 2a2b 2c2d 2e2f 3031 3233 3435 &'()*+,-./012345
0x0060 3637
```

This slide shows two examples of packet capture outputs.

The first example captures all traffic to and from port 443. It uses verbosity 4, so the information is easy to read. It displays one packet per line, containing the incoming and outgoing interface, IP addresses, port numbers, and type of packet (SYN, SYN/ACK, and so on). Note that the interface is set to `any`, which is useful to capture packets that enter or exit multiple interfaces in the device. This enables you to have a better understanding of how packets flow through the firewall. For example, the output shows a three-way handshake established across FortiGate. From the packet capture, you can conclude that the connection is initiated by `10.1.10.1`, which is behind `port3`, and is destined to `100.64.3.1`, which is behind `port1`. You can also conclude that FortiGate performs SNAT for the connection. That is, in the original direction, FortiGate translates the source address to `100.64.1.1` when packets leave `port1`. FortiGate then translates the reply packets back to `10.1.10.1` when they exit `port3`.

The second example captures all ICMP traffic coming from or going to `10.0.10.254`. Unlike the first example, which captures packets on any interface, this example limits the capture to packets that enter or leave the `Students` interface. Although not shown on this slide, the `Students` interface is a VLAN interface. In addition, the verbosity level is set to 6, which includes the full packet IP payload details. The output is longer and more difficult to read. However, this is one of the two verbosity levels to use (3 being the other one) if you need to export the output to pcap format. You can then view the pcap file using Wireshark or any other compatible packet analysis tool. Moreover, the additional arguments in the command instruct the sniffer to not set a packet count limit (0) and to print the local timestamp for each packet (1).

# DO NOT REPRINT © FORTINET

## Packet Capture From the GUI

- Available on devices with internal storage
- Automatically convert packet capture to pcap
- Embedded real-time analysis page

Select interface name or any (GUI doesn't show matching interface)

Select **Advanced** if you want to indicate the BPF filter to use

Set up filter to narrow down packet capture as much as possible

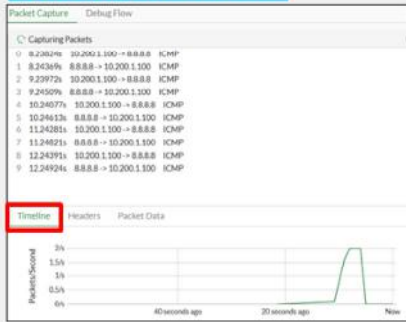
If your FortiGate model has internal storage, you can capture packets on the GUI. Starting FortiOS 7.2, the GUI packet capture tool was improved to also include a real-time analysis tool that enables you to examine the packet capture details directly on the GUI. You also download the respective pcap file in case you prefer to review it using Wireshark or your preferred packet analysis tool.

Before starting the packet capture, you should set up the packet capture filter by using either **Basic** or **Advanced** filter options. When you choose **Basic**, you indicate basic filter options such as host address, port number, and protocol number. In case you want to use your own BPF filter like you do in the CLI, you can choose **Advanced**.

Regardless of which method you use (CLI or GUI), packet capture filters should be very specific to make sure only the relevant packets are captured, and large amounts of data are not being written to the disk.

# Packet Capture From the GUI (Contd)

## Packet Capture > Timeline



- Useful to identify important traffic events

## Packet Capture > Headers

The screenshot shows a table of captured packets with columns for time, source IP, destination IP, and protocol. The 'Headers' tab is highlighted with a red box. Below the table is a detailed view of the selected packet's headers.

IP	L4
Source IP 10.200.1.100	Type 8
Destination IP 8.8.8.8	Code 0
Protocol ICMP	Checksum 0x1eca

- Basic IP and Layer 4 data

## Packet Capture > Packet Data

The screenshot shows the packet data in both hexadecimal and ASCII formats. The 'Packet Data' tab is highlighted with a red box. The data is displayed in a grid format with columns for time, source IP, destination IP, and protocol.

- Full packet data in HEX and ASCII formats

This slide shows an example of the embedded real-time analysis tool included in the GUI packet capture tool starting FortiOS 7.2. After you start the packet capture, the GUI starts displaying the captured packets based on the filter set.

The **Timeline** tab displays a graph with the number of captured packets per second. The graph is useful to quickly identify peaks of traffic related by important events in the network.

The **Headers** tab enables you to examine basic IP (Layer 3) and Layer 4 information on the packet.

The **Packet Data** tab enables you to examine the full packet data using hexadecimal format. Next to the hexadecimal packet data, FortiOS displays the equivalent output in ASCII format.

**DO NOT REPRINT**  
**© FORTINET**

## Knowledge Check

1. What is the distance value for this route?

`10.200.2.0/24 [110/2] via 10.200.2.254, [25/0]`

- A. 110
- B. 2

2. Which CLI command can you use to view standby and inactive routes?







- A. `get router info routing-table all`
- B. `get router info routing-table database`

3. Which CLI packet capture verbosity level prints interface names?

- A. 3
- B. 4

**DO NOT REPRINT**  
**© FORTINET**

## Lesson Progress

-  Routing on FortiGate
-  Routing Monitor and Route Attributes
-  Equal Cost Multipath Routing (ECMP)
-  Reverse Path Forwarding (RPF)
-  Best Practices
-  Diagnostics

Congratulations! You have completed this lesson.

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

**DO NOT REPRINT**  
**© FORTINET**

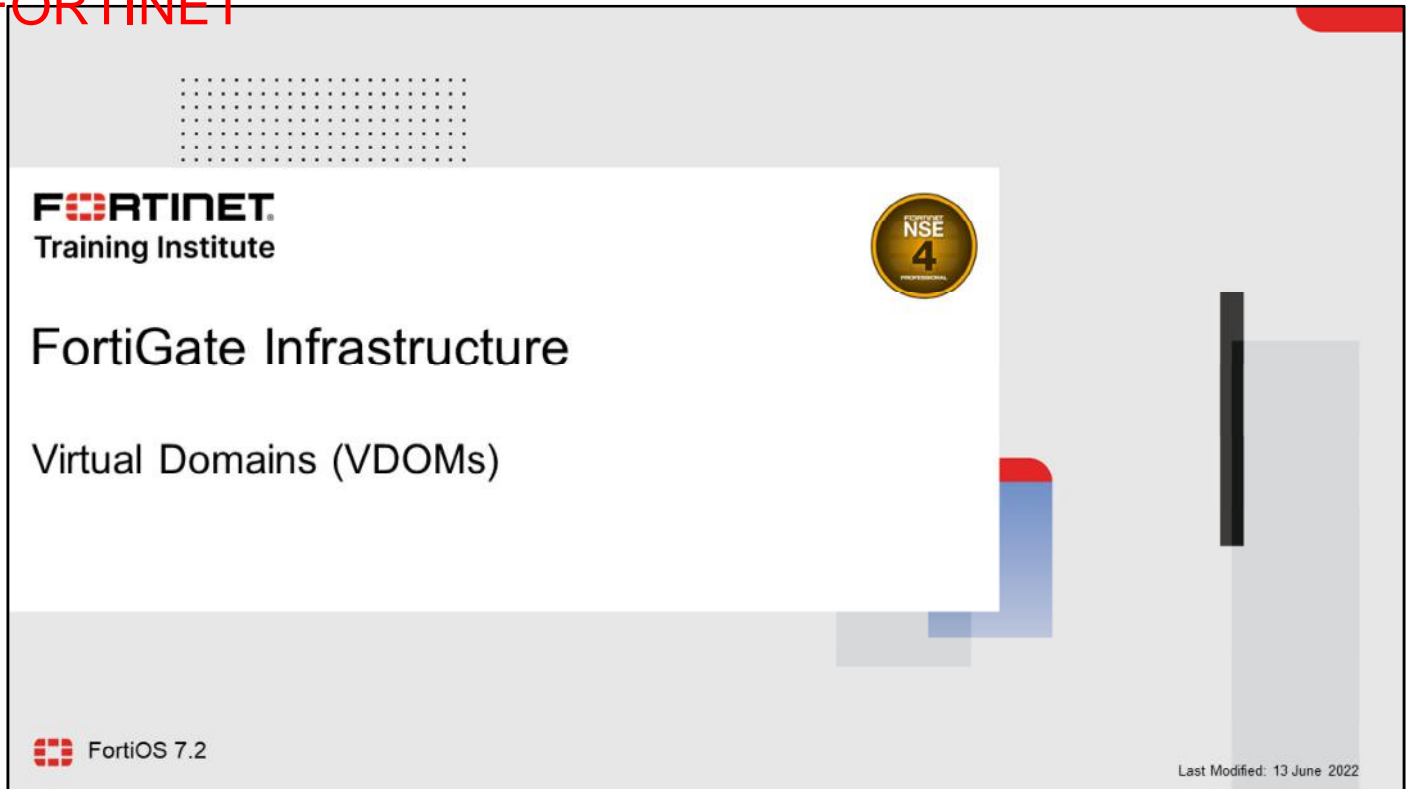
## Review

- ✓ Configure static routing
- ✓ Configure and view policy routes
- ✓ Route traffic for well-known internet services using ISDB routes
- ✓ Interpret the routing table on FortiGate
- ✓ Implement ECMP routing
- ✓ Block traffic from spoofed IP addresses using RPF
- ✓ Understand route failover
- ✓ Explore the routing table and routing table database entries
- ✓ Use the built-in sniffer GUI and CLI tools

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

By mastering the objectives covered in this lesson, you learned how to configure, maintain, and troubleshoot the FortiGate routing configuration.

DO NOT REPRINT  
© FORTINET



In this lesson, you will learn how to configure VDOMs, and examine examples of common use.

**DO NOT REPRINT  
© FORTINET**

## Lesson Overview

- VDOM Concepts
- VDOM Administrators
- Configuring VDOMs
- Inter-VDOM Links
- Best Practices and Troubleshooting

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

DO NOT REPRINT  
© FORTINET

The slide features a light gray background with a white content area. At the top left, the title 'VDOM Concepts' is displayed in a large, black, sans-serif font. Below the title, the word 'Objectives' is written in a bold, black, sans-serif font. Underneath, a single bullet point is listed: '• Define and describe VDOMs'. The slide is decorated with several abstract geometric shapes: a red rounded rectangle in the top right corner, a cyan vertical bar with a red top edge, a dark gray vertical bar, and a light gray vertical bar. In the bottom left corner, the Fortinet logo is shown, consisting of the word 'FORTINET' in a bold, black, sans-serif font with a red square containing a white grid pattern to its left, and the words 'Training Institute' in a smaller, black, sans-serif font below it. In the bottom right corner, the number '3' is displayed in a small, red, sans-serif font.

## VDOM Concepts

### Objectives

- Define and describe VDOMs

**FORTINET**  
Training Institute

3

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

By demonstrating competence in VDOMs, you will be able to understand the key benefits and use cases for VDOMs.

DO NOT REPRINT  
© FORTINET

## VDOMs

One physical firewall → Multiple virtual firewalls

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

**FORTINET**  
Training Institute

© Fortinet Inc. All Rights Reserved.

4

What if a campus wants to keep its departments separate? A datacenter wants to implement various security implementations in a cost-effective manner that maintains all customer traffic separate and secure while also reducing space and making configuration easier? What if you want to segment your network, and subdivide policies and administrators into multiple security domains?

The best solution is to enable FortiGate VDOMs.

A VDOM splits your FortiGate into multiple logical devices and divides one security domain into multiple security domains.

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, UTM inspection, and secure communication devices.

**DO NOT REPRINT  
© FORTINET**

## Multi-VDOM Mode

- Can create multiple VDOMs that function as multiple independent units
- FortiGate has two types of multi-VDOMs:
  - **Admin VDOM** :
    - Used for management purposes only
    - Does not pass any data
  - **Traffic VDOM** :
    - Processes all network traffic through FortiGate
    - Can provide separate security policies
- Three main use cases for multi-VDOM mode:
  - Management VDOM
  - Independent VDOM
  - Meshed VDOM

Use multi-VDOM mode when you want to create multiple logical firewalls from a single FortiGate. Each VDOM acts as an independent FortiGate.

Multi-VDOM mode works well for managed service providers leveraging multi-tenant configurations, or large enterprise environments that desire departmental segmentation. You can give each individual tenant or department, visibility and control of their VDOM, while keeping other VDOMs independent and unseen.

Two types of VDOMs can be created in multi-VDOM Mode: An admin VDOM and a traffic VDOM. Admin VDOMs are for FortiGate administration, and traffic VDOMs permit traffic to travel through FortiGate.

Upon upgrade, if a FortiGate is in split-vdom mode, it is converted to multi-vdom mode. The FG-traffic VDOM becomes a traffic type VDOM. The root VDOM becomes an admin VDOM.

## Management VDOM

- Where all the management traffic for FortiGate originates
- It *must* have access to all global services that FortiGate requires:
  - NTP
  - FortiGuard updates and queries
  - SNMP
  - DNS filtering
  - Logs—both FortiAnalyzer and syslog
  - As well as other FortiGate management-related services
- By default, the management VDOM is **root**
  - Can be reassigned to any VDOM in multi-vdom mode, but direct internet access is recommended because specific services, such as web filtering using the public FortiGuard servers, will not work without it

Until now, you've learned about traffic passing *through* FortiGate, from one VDOM to another.

What about traffic originating *from* FortiGate? Some system daemons, such as NTP and FortiGuard updates, generate traffic coming from FortiGate.

Traffic coming from FortiGate to those global services originates from the *management* VDOM. One, and only one, of the VDOMs on a FortiGate device is assigned the role of the management VDOM.

By default, the root VDOM acts as the management VDOM, but you can manually reassign this task to a different VDOM in multi-vdom mode.

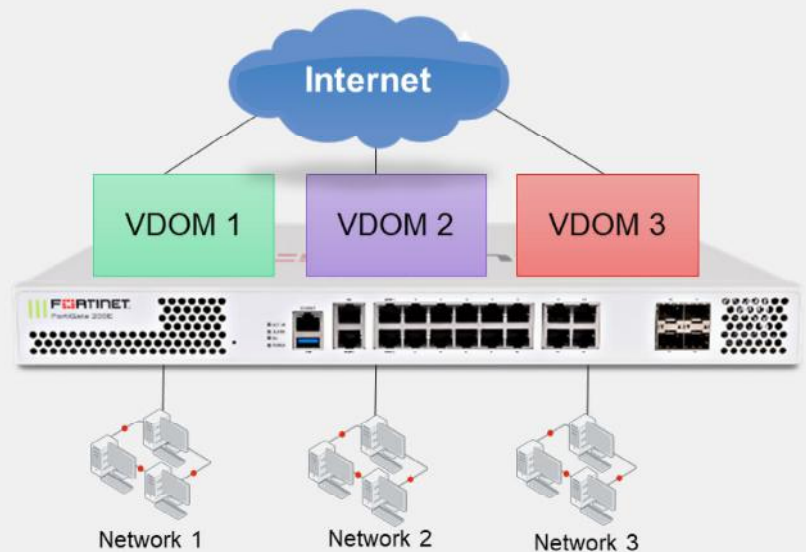
It is important to note that the management VDOM designation is solely for traffic originated by FortiGate, such as FortiGuard updates, and has no effect on traffic passing through FortiGate. As such, the management function can be performed by any designated VDOM.

Similar to FortiGate without VDOMs enabled, the administrative VDOM should have outgoing internet access. Otherwise, features such as scheduled FortiGuard updates, fail.

**DO NOT REPRINT  
© FORTINET**

## Independent VDMs

- Multiple VDMs are completely separated
- There is no communication between VDMs
- Each VDM has its own physical interface link to the internet



**FORTINET**  
Training Institute

© Fortinet Inc. All Rights Reserved.

7

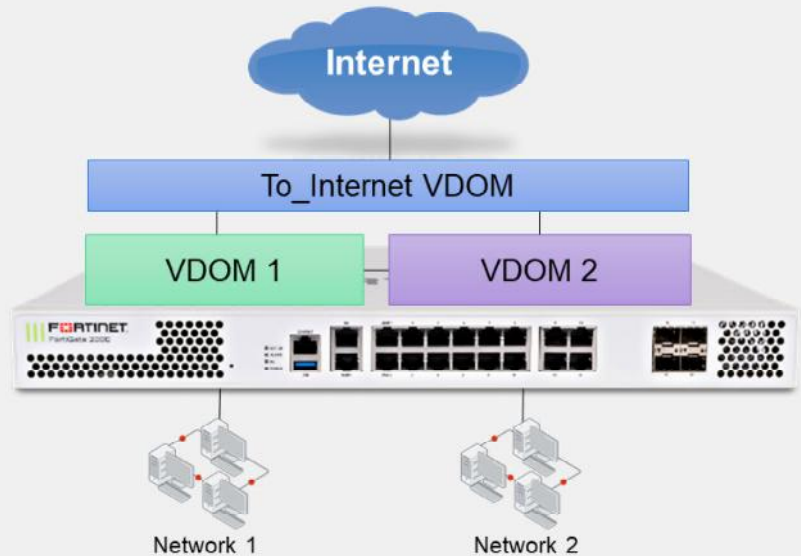
There are a few ways you can arrange your VDMs. In the topology shown on this slide, each network accesses the internet through its own VDM.

Notice that there are no inter-VDM links. So, inter-VDM traffic is not possible unless it physically leaves FortiGate, toward the internet, and is rerouted back. This topology would be most suitable in a scenario where multiple customers are sharing a single FortiGate, each in their own VDM, with physically separated ISPs.

DO NOT REPRINT  
© FORTINET

## Meshed VDOMs

- VDOMs connect to other VDOMs through inter-VDOM links
  - Only Internet traffic needs to go through the **To\_Internet** VDOM
  - Only the **To\_Internet** VDOM is physically connected to the internet



**FORTINET**  
Training Institute

© Fortinet Inc. All Rights Reserved.

8

In the example topology shown on this slide, traffic again flows through a single pipe in the **To\_Internet** VDOM toward the internet. Traffic between VDOMs doesn't need to leave FortiGate.

However, now inter-VDOM traffic doesn't need to flow through the **To\_Internet** VDOM. Inter-VDOM links between VDOMs allow more direct communication.

Similar to the previous example topology, inspection can be done by either the **To\_Internet** or originating VDOM, depending on your requirements.

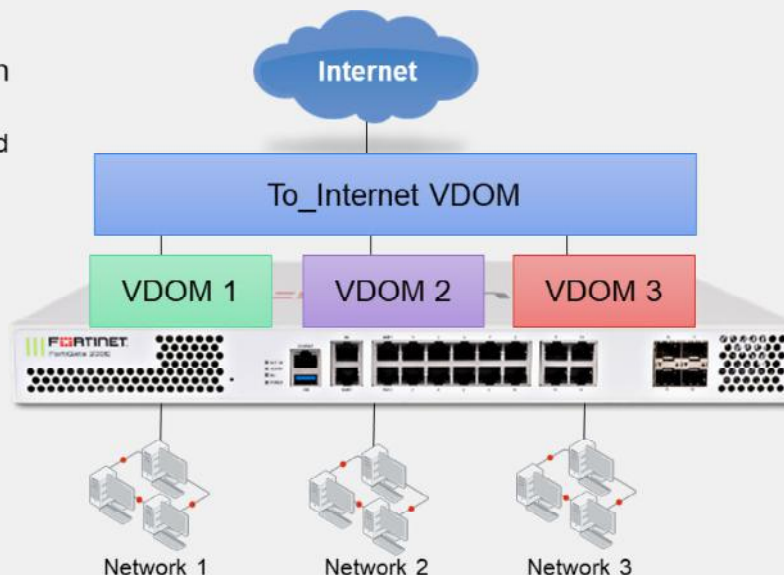
Because of the number of inter-VDOM links, the example shown on this slide is the most complex, requiring the most routes and firewall policies. Troubleshooting meshed VDOMs can also be more time consuming.

However, meshed VDOMs also provide the most flexibility. For large businesses, inter-VDOM communication may be required. Also, inter-VDOM traffic performance may be better because of a shorter processing path, which bypasses intermediate VDOMs.

DO NOT REPRINT  
© FORTINET

## Routing Through a Single VDOM

- Traffic destined to the internet will *always* be routed through *the designated VDOM (To\_Internet in this example)*
  - The **To\_Internet** VDOM is connected to other VDOMs using inter-VDOM links
  - Only the **To\_Internet** VDOM is physically connected to the Internet



**FORTINET**  
Training Institute

© Fortinet Inc. All Rights Reserved.

9

Like the topology shown on the previous slide, each network in the example topology shown on this slide sends traffic through its VDOM. However, after that, traffic is routed through the **To\_Internet** VDOM. So, internet-bound traffic flows through a single pipe in the **To\_Internet** VDOM.

This could be suitable in a scenario where multiple customers are sharing a single FortiGate, each in their own VDOM. In this case, the internet-facing VDOM could log and monitor traffic, or provide standard services like antivirus scanning, or both.

The topology shown on this slide has inter-VDOM links. VDOMs are linked only with the **To\_Internet** VDOM, but not with each other. If **VDOM1** needs to communicate with **VDOM3**, this traffic would need to be routed through the **To\_Internet** VDOM through IP routing decisions and is subject to all firewall policies.

Inspection could be done by either the internet-facing or originating VDOM, depending on your requirements. Alternatively, you could split inspection so that some scans occur in the internet-facing VDOM—ensuring a common security baseline—while other more intensive scans occur in the originating VDOM.

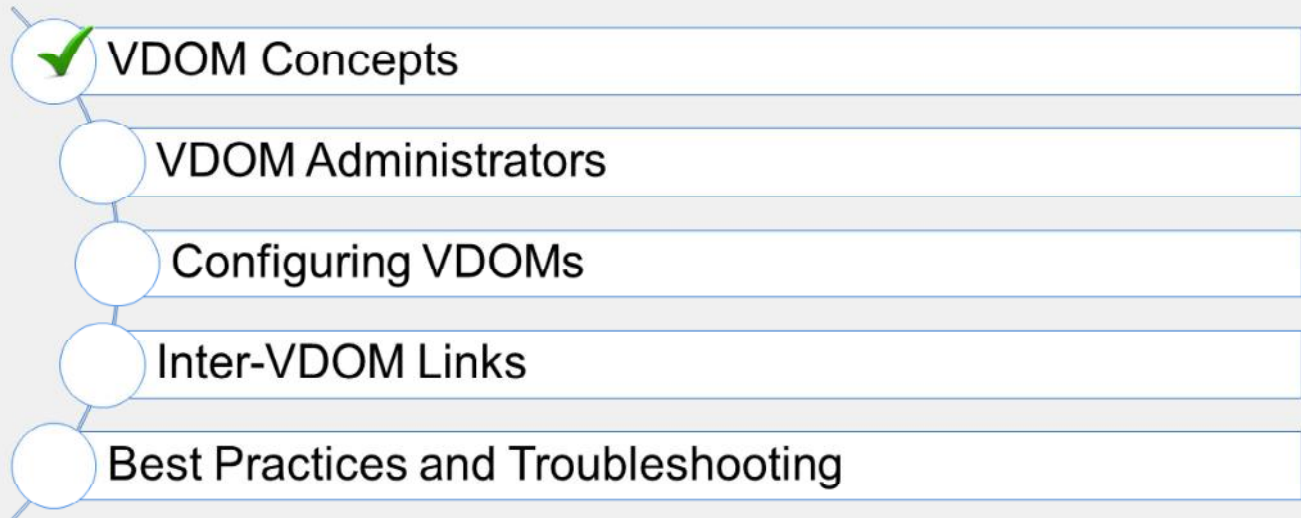
DO NOT REPRINT  
© FORTINET

## Knowledge Check

1. Which traffic is always generated from the management VDOM?
  - A. Link Health Monitor
  - ✓ B. FortiGuard
2. Which statement about the management VDOM is true?
  - A. It is **root** by default and cannot be changed in multi-vdom mode.
  - ✓ B. It is **root** by default, but can be changed to any VDOM in multi-vdom mode.

**DO NOT REPRINT**  
**© FORTINET**

## Lesson Progress



Good job! You now understand some basic concepts about VDOMs.

Now, you'll learn about VDOM administrators.

**DO NOT REPRINT  
© FORTINET**

**VDOM Administrators**

**Objectives**

- Create administrative accounts with access limited to one or more VDOMs

**FORTINET**  
Training Institute

12

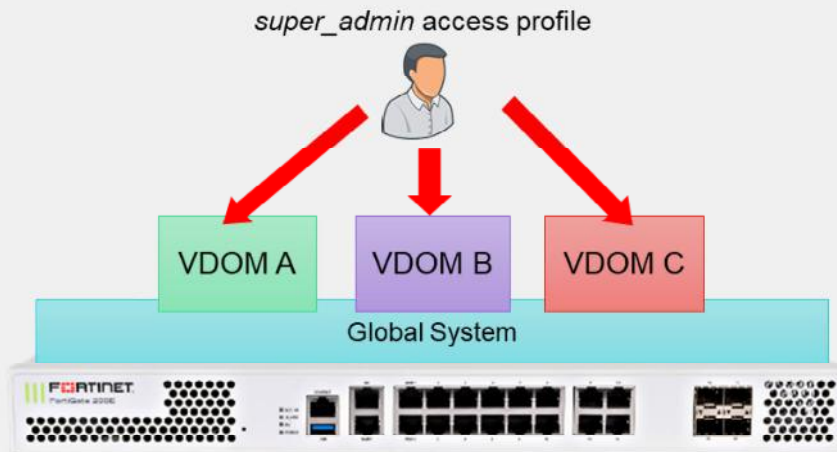
After completing this section, you should be able to achieve the objective shown on this slide.

By demonstrating competence in creating VDOM administrative accounts, you will be able to understand the differences between the various levels and types of VDOM administrators.

DO NOT REPRINT  
© FORTINET

## VDOM Administration

- Only the account named **admin** or accounts with the **super\_admin** profile can configure and back up all VDOMs



**FORTINET**  
Training Institute

© Fortinet Inc. All Rights Reserved.

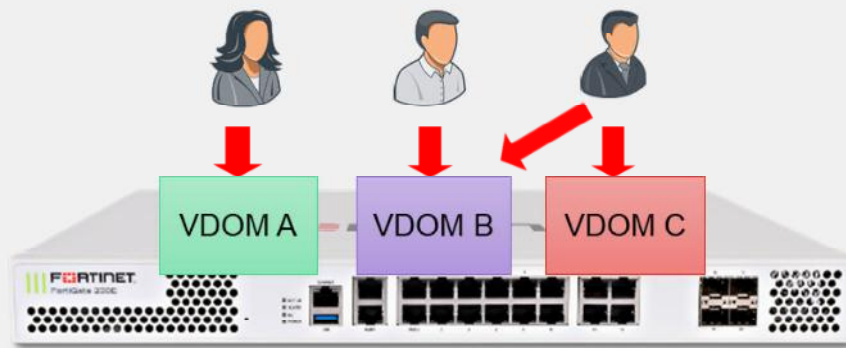
13

If you want to grant access to all VDOMs and global settings, select **super\_admin** as the access profile when configuring the administrator account. Similar to the account named **admin**, this account can configure all VDOMs.

DO NOT REPRINT  
© FORTINET

## Per-VDOM Administration

- Other administrators can access only their *assigned* VDOMs
  - Cannot access the global settings



**FORTINET**  
Training Institute

© Fortinet Inc. All Rights Reserved.

14

In most cases, you start by creating one administrator account per VDOM. That administrator is chiefly responsible for that domain, including the configuration backups of that VDOM. In larger organizations, you may need to make multiple VDOM administrators. You can assign multiple administrators to each VDOM. You can subdivide permissions using access profiles, in order to follow best practices for segregation of duties.

The converse is also possible. If required, you can assign an administrator to multiple VDOMs.

DO NOT REPRINT  
© FORTINET

## Creating VDOM Administrators

**Global > System > Administrators**

New Administrator

Username: customer-admin

Type: Local User  
Match a user on a remote server group  
Match all users in a remote server group  
Use public key infrastructure (PKI) group

Password: .....

Confirm Password: .....

Comments: Write a comment... 0/255

Administrator profile: prof\_admin

Virtual Domains: customer, root

Two-factor Authentication ⓘ

Restrict login to trusted hosts

Restrict admin to guest account provisioning only

OK Cancel

**FORTINET**  
Training Institute

© Fortinet Inc. All Rights Reserved.

15

To create new administrator accounts and assign them to a VDOM, click **Global > System > Administrators**.

DO NOT REPRINT  
© FORTINET

## Knowledge Check

1. Which type of administrator can make changes to all VDOMs?
  - A. A custom VDOM administrator
  - ✓ B. An administrator with the **super\_admin** profile
2. Which statement about VDOM administrators is true?
  - A. There can be only one administrator per VDOM.
  - ✓ B. Each VDOM can have multiple administrators.

**DO NOT REPRINT**  
**© FORTINET**

## Lesson Progress

- VDOM Concepts
- VDOM Administrators
- Configuring VDOMs
- Inter-VDOM Links
- Best Practices and Troubleshooting

Good job! You now understand VDOM administrators.

Now, you'll learn how to configure VDOMs.

DO NOT REPRINT  
© FORTINET

The slide features a light gray background with a white content area. The title 'Configuring VDOMs' is in a large, dark font. Below it, the word 'Objectives' is in a bold, dark font. A bulleted list follows, containing two items. The Fortinet logo and 'Training Institute' are in the bottom left, and the number '18' is in the bottom right. The slide is decorated with several abstract geometric shapes in shades of gray, red, and teal.

## Configuring VDOMs

### Objectives

- Configure VDOMs to split a FortiGate into multiple virtual devices
- Multi VDOM types

**FORTINET**  
Training Institute

18

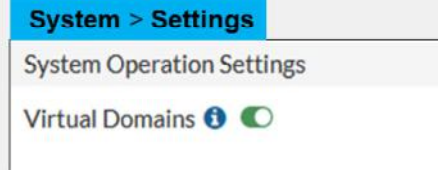
After completing this section, you will be able to achieve the objective shown on this slide.

By demonstrating competence in configuring VDOMs, you will be able to effectively implement VDOMs on your FortiGate.

DO NOT REPRINT  
© FORTINET

## Enabling VDOMs

- FortiGate supports only multi-VDOM Mode
- From the GUI:
  - Available only on specific higher-end models
  - If the option does not exist, use the CLI command



- From the CLI:

```
#config system global
  set vdom-mode [no-vdom/multi-vdom]
end
```

On the GUI, you can enable VDOMs under **System > Settings**. The GUI option is available only on higher-end FortiGate Models. Most of the FortiGate models, you can enable VDOMs on the CLI only.

Enabling VDOMs does not cause your FortiGate device to reboot, but it does log out all active administrator sessions. Traffic continues to pass through FortiGate.

Enabling VDOMs restructures both the GUI and CLI, which you will see when you log in again.

DO NOT REPRINT  
© FORTINET

## Multi-VDOM Mode

- Effective solution for managed service providers with multi-tenant configurations, or large enterprises that desire departmental segmentation
  - Logically segmented traffic
  - Each tenant, or department, can be provided full visibility and management control independently

Global > System > VDOM

Name	Management VDOM	Type	NGFW Mode	Operation Mode	Status
ADMIN-VDOM		Admin			Enabled
VDOM1		Traffic	Profile-based	NAT	Enabled
root		Traffic	Profile-based		

multi-vdom mode

System Information	
Hostname	Local-FortiGate
Serial Number	FGVM010000064692
Firmware	v7.2.0 build1157 (Feature)
Virtual Domains	<input checked="" type="checkbox"/>
Mode	NAT
System Time	2022/04/04 08:28:50

**FORTINET**  
Training Institute

© Fortinet Inc. All Rights Reserved.

20

In *multi-vdom* mode, you can create multiple VDOMs that function as multiple independent units. By default, the root is the management VDOM and can be used to do both management tasks and allow other traffic. You can select any VDOM to act as the management VDOM.

DO NOT REPRINT  
© FORTINET

## Multi-VDOM types

- Multi-VDOMs can be one of the following types:
  - Admin type
  - Traffic type
- Admin type:
  - Used for administrative purposes only
  - Administrators can log in using SSH/HTTPS

New Virtual Domain

Virtual Domain: admin.vdom

Type: **Admin**

Traffic:

Comments:

Admin type

### Global > System > VDOM

Name	Management VDOM	Type	NGFW Mode	Operation Mode	Status	CPU
root		Traffic	Profile-based	NAT	Enabled	8%

### Global > System > VDOM

Name	Management VDOM	Type	NGFW Mode	Operation Mode	Status	CPU
root		Traffic	Profile-based	NAT	Enabled	8%

When you enable multi-vdom mode, the root VDOM exists. It is the default management VDOM and is a traffic VDOM. You can create another VDOM (traffic or admin). FortiGate supports only one admin VDOM.

**DO NOT REPRINT**  
**© FORTINET**

## Multi -VDM types (Contd)

- Traffic type:
  - Can pass traffic like regular VDMs

- From CLI:

```
config vdom
edit <vdom>
  config system settings
    set vdom-type [traffic/admin]
end
```

### Global > System > VDM

Name	Management VDM	Type	NGFW Mode	Operation Mode	Status	CPU
root		Traffic	Profile-based	NAT	Enabled	0%



New Virtual Domain

Virtual Domain: VDOM1

Type: **Traffic** Admin

NGFW Mode: Profile-based Policy-based

Central SNAT:

WiFi country/region: Canada

Comments:

When the VDM type is set to Traffic, the VDM can pass traffic like a regular VDM. If an admin VDM exists, all newly created VDMs are configured as traffic VDMs.

# DO NOT REPRINT © FORTINET

## Creating VDOMs

- By default, only the **root** management VDOM exists
  - You can create additional VDOMs.
- NGFW mode per VDOM:
  - Profile-based
  - Policy-based
- Operation mode per VDOM:

```
config vdom
edit <vdom>
  config system settings
    set opmode [nat | transparent]
end
```

Global > System > VDOM

Name	Management VDOM	NGFW Mode	Operation Mode	Status	CPU	Memory
root	<input checked="" type="checkbox"/>	Profile-based	NAT	Enabled	15%	36%

<VDOM> > System > Settings

New Virtual Domain

Virtual Domain: VDOM1

Type: Traffic Admin

NGFW Mode: Profile-based Policy-based

Central SNAT:

WiFi country/region: Canada

Comments:

After enabling VDOMs in multi-vdom mode, by default, only one VDOM exists: the root VDOM. It's the default management VDOM.

You need to add a VDOM for each of your security domains. If you're an MSSP, for example, you might add one VDOM for each client company. If you are an enterprise business, you might add one VDOM for each division of your company.

The default inspection-mode is flow, so you can change **NGFW Mode** from **Profile-based** (default) to **Policy-based** directly in **System > Settings** for the VDOM.

The **profile-based** NGFW is the traditional mode and you must create antivirus, web filter, and IPS profiles, which are then applied to the policy. **Policy-based** mode is actually a new policy mode. You can add applications and web filtering categories directly to a policy without having to first create and configure application control or web filtering profiles. NGFW mode is a per-VDOM setting. If you set NGFW mode to **Profile-based**, you can configure policies in that VDOM for either flow or proxy inspection. However, if NGFW mode is **Policy-based**, then the inspection mode for all policies in that VDOM is always flow and there is no option available in the policy to change it.

*Switching between NGFW modes results in the loss of all current policies configured in the VDOM.* If you don't want this to happen, or you just want to experiment with a particular NGFW mode, consider creating a new VDOM for testing purposes. You could also back up your configuration before switching modes.

Operation mode is a per-VDOM setting. You can combine transparent mode VDOMs with NAT mode VDOMs on the same physical FortiGate.

## FortiGate Operation Modes

- Operation mode defines how FortiGate handles traffic
  - NAT mode:
    - Routes according to OSI Layer 3 (IP address), as a *router*
    - FortiGate interfaces have IP addresses associated with them
  - Transparent mode:
    - Forwards according to OSI Layer 2 (MAC address), as a transparent *bridge*
    - FortiGate interfaces usually have no IP addresses
    - Requires no IP address changes in the network
  
- FortiGate as a Transparent Bridge
  - Transparent to IP-layer hosts
  - Builds a table for traffic forwarding by analyzing the source MAC addresses of incoming frames
  - Splits your network into multiple collision domains:
    - Reduces traffic and collision levels seen on individual domains
    - Improves network response time

Traditional IPv4 firewalls and NAT mode FortiGate devices handle traffic the same way that routers do. Each interface must be in a different subnet and each subnet forms a different broadcast domain. FortiGate routes IP packets based on the IP header information, overwriting the source MAC address. So, if a client sends a packet to a server connected to a different FortiGate interface, the packet arrives at the server with a FortiGate MAC address, instead of the client MAC address.

In transparent operation mode, FortiGate forwards frames without changing the MAC addresses. When the client receives a packet from a server connected to a different FortiGate interface, the frame contains the real MAC address of the server—FortiGate doesn't rewrite the MAC header. FortiGate acts as a Layer 2 bridge or switch. So, the interfaces do not have IP addresses and, by default, all belong to the same broadcast domain.

This means that you can install a transparent mode FortiGate in a customer network without having to change the customer's IP address plan. Some customers, especially large organizations, don't want to reconfigure thousands of devices to define a new internal network that is separate from their external network.

A transparent mode FortiGate device acts as a transparent bridge. What does that mean? It means that FortiGate has a MAC address table that contains, among other things, the interface that must be used to reach each MAC address. FortiGate populates this table with information taken from the source MAC address of each frame.

FortiGate, as a transparent switch, splits the network into multiple collision domains, reducing the traffic in the network and improving the response time.

# DO NOT REPRINT © FORTINET

## Forward Domains

- By default, *all* interfaces on a VDOM belong to the same broadcast domain; even interfaces with different VLAN IDs
  - Broadcast domains that contain multiple interfaces can be very large and add unnecessary broadcast traffic to some LAN segments
- Use this command to subdivide a VDOM into multiple broadcast domains:

```
config system interface
  edit <interface_name>
    set forward-domain <domain_ID>
end
```

- Interfaces with the same domain ID belong to the same broadcast domain

By default, in transparent operation mode, each VDOM forms a separate forward domain; however, interfaces do not. How does this affect the network?

Until you change the initial VDOM configuration, all interfaces, regardless of their VLAN ID, are part of the same broadcast domain. FortiGate broadcasts from every interface in the VDOM in order to find any unknown destination MAC address. On large networks, this could generate massive broadcast traffic and overwhelming replies—a broadcast storm.

# DO NOT REPRINT © FORTINET

## Confirmation Prompt When Creating VDOMs

- VDOM confirmation prompt added
  - So that users do not create new VDOMs accidentally in CLI

```
config system global
  set edit-vdom-prompt [enable | disable]
end
```

- Disabled by default
- When enabled, if administrator creates a new VDOM, FortiGate displays prompt:

```
# config vdom
  edit student
  The input VDOM name doesn't exist.
  Do you want to create a new VDOM?
  Please press 'y' to continue, or press 'n' to cancel. (y/n)y

current vf=student:3
```

Prompt to confirm before  
the new VDOM is created

A VDOM confirmation prompt has been added so users do not create new VDOMs accidentally on the CLI. This setting is disabled by default. Once enabled, when an administrator creates a new VDOM, FortiGate displays a prompt to confirm before the VDOM is created.

# DO NOT REPRINT © FORTINET

## Assigning Interfaces to a VDOM

- You can assign an interface to each VDOM you create

- From CLI:

```
config global
config system interface
edit <interface_name>
set vdom <vdom-name>
end
```

**Global > Network > Interfaces**

Edit Interface

Name: port4

Alias:

Type: Physical Interface

VRF ID: 0

Virtual domain: root

Role:

Address:

Addressing mode:  Manual  DHCP  Auto-managed by FortiIPAM

IP/Netmask: 192.168.10.254/24

Secondary IP address:

After adding a VDOM, you can specify which interface belongs to it. Each interface (physical or VLAN) can belong to only one VDOM.

You can move an interface from one VDOM to another, provided it is not associated with any references, such as firewall policies.

DO NOT REPRINT  
© FORTINET

## Global and Per-VDOM Settings



### Global settings

- Affect all configured VDOMs:
  - Hostname
  - HA settings
  - FortiGuard settings
  - System time
  - Administrative accounts

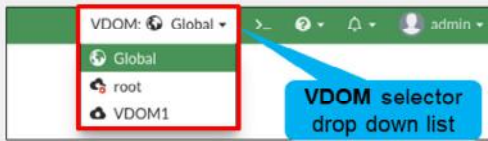
### Per-VDOM settings

- Configured separately for each VDOM:
  - Operating mode (transparent, NAT/route)
  - NGFW mode (profile-based, policy-based)
  - Routes and network interfaces
  - Firewall policies
  - Security profiles

Global resource limits are an example of global settings. The firmware on your FortiGate device and some settings, such as system time, apply to the entire device—they are not specific to each VDOM.

However, you can configure most settings differently for each VDOM. Some examples are firewall policies, firewall objects, static routes, and protection profiles.

## Accessing Global and Per-VDOM Settings



- Accessing global settings:

```
config global
(global) #
```

- Accessing per-VDOM settings:

```
config vdom
(vdom) # edit <vdom-name>
(vdom-name) #
```

VDOM names are case sensitive. Use the correct case for the VDOM name or FortiGate will create a new VDOM

- Executing global and per-VDOM commands from any context:

```
[global | vdom-name] # sudo [global | vdom-name] [diagnose | execute | show | get]
```

When you log with a regular administrator account, you automatically enter the VDOM associated with that account.

When you log in with the account named admin, you have access to all VDOMs. To access a specific VDOM, select it in the drop-down list at the top of the page.

The VDOM submenu should be familiar; it is essentially the same navigation menu from before you enabled VDOMs. However, the global settings are moved to the Global menu.

To access the global configuration settings on the CLI, you must enter `config global` to enter into the global context. After that, you can run global commands and change global configuration settings.

To access per-VDOM configuration settings on the CLI, you must enter `config vdom`, then enter `edit` followed by the VDOM name. From the VDOM context, you can run VDOM-specific commands and change per-VDOM configuration settings. It is important to note that VDOM names are case sensitive. If you enter the name using the incorrect case, FortiGate creates a new VDOM.

Regardless of which context you are in (global or VDOM), you can use the `sudo` keyword to run diagnostics commands in a context different from your current one. This allows you to run global and per-VDOM commands, for example, without switching back and forth between the global and per-VDOM contexts.

DO NOT REPRINT  
© FORTINET

## Global Security Profiles

- Global security profiles for multiple VDOMs
- Global profiles support the following features
  - Antivirus
  - Application control
  - Intrusion prevention
  - Web filtering
- Profiles are read-only for VDOM-level administrators
  - Must edit, or delete from global settings
- Global profile name must start with "g-" for identification

### Global > Security Profiles > Web Filter

VDOM: Global

Edit Web Filter Profile

Name: g-default

Comments: Default web filtering. 22/255

Feature set: Flow-based Proxy-based

FortiGuard Category Based Filter

Allow Monitor Block Warning

Name	Action
Potentially Liable 12	
Adult/Mature Content 15	
Bandwidth Consuming 2	
Security Risk 4	

### Customer VDOM > Web Filter

VDOM: VDOM1

+ Create New Edit Clone Delete Search

Name	Comments	Scope	Ref.
WEB g-default	Default web filtering.	Global	0
WEB g-wifi-default	Default configuration for offload...	Global	1

**FORTINET**  
Training Institute

© Fortinet Inc. All Rights Reserved.

30

You can configure security profiles globally for use by multiple VDOMs, to avoid creating identical profiles for each VDOM separately. Global profiles are available for the following security features:

- Antivirus
- Application control
- Intrusion prevention
- Web filtering

Some security profile features, such as URL filters, are not available for use in a global profile. The name for any global profile must start with "g-" for identification. Global profiles are available as read-only for VDOM-level administrators and can be edited or deleted only in the global settings. Each security feature has at least one default global profile.

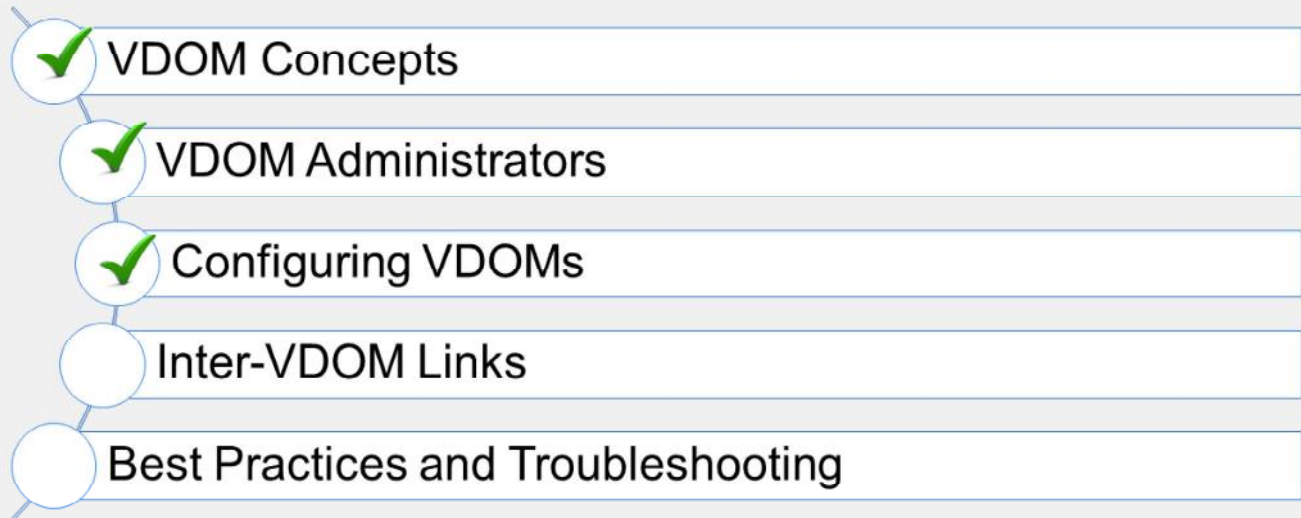
**DO NOT REPRINT**  
**© FORTINET**

## Knowledge Check

1. Which configuration settings are global settings?
  - A. Firewall policies
  - ✓ B. FortiGuard settings
  
2. Which configuration settings are per-VDOM settings?
  - A. Host name
  - ✓ B. NGFW mode

**DO NOT REPRINT**  
**© FORTINET**

## Lesson Progress



Good job! You now understand how to configure VDOMs.

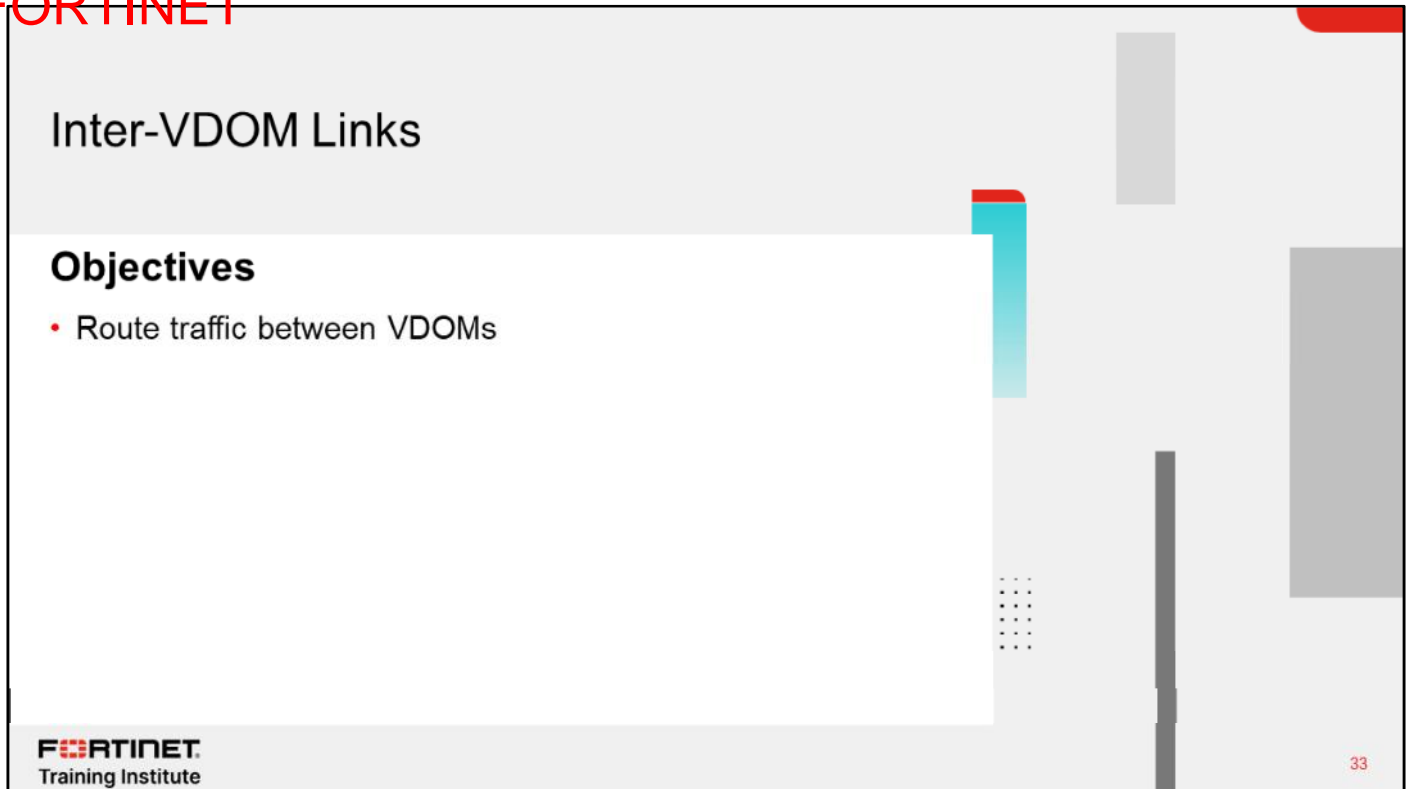
Now, you'll learn about inter-VDOM links.

DO NOT REPRINT  
© FORTINET

## Inter-VDOM Links

### Objectives

- Route traffic between VDOMs



**FORTINET**  
Training Institute

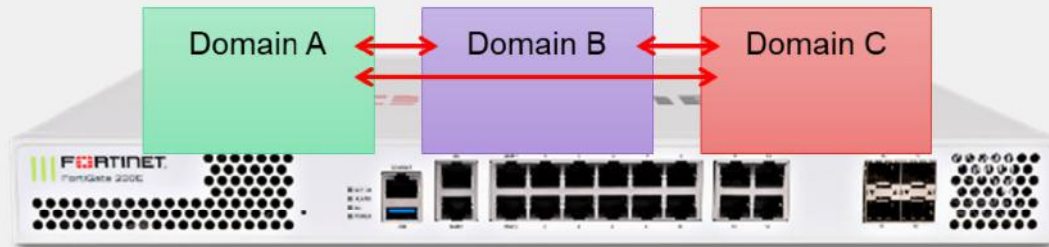
33

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

By demonstrating competence in inter-VDOM links, you will be able to effectively and efficiently route traffic between VDOMs on FortiGate.

DO NOT REPRINT  
© FORTINET

## Inter-VDOM Links



- Can connect different VDOMs
- Support varies by VDOM operating mode
  - NAT-to-NAT ✓
  - NAT-to-transparent and transparent-to-NAT ✓
  - Transparent-transparent (no Layer 3; potential Layer 2 loops) ✗

To review, each VDOM behaves like it is on a separate FortiGate device. With separate FortiGate devices, you would normally connect a network cable and configure routing and policies between them. But VDOMs are on the same FortiGate. So, how should you route traffic between them? The solution is inter-VDOM links. Inter-VDOM links are a type of virtual interface that route traffic between VDOMs. This removes the need to loop a physical cable between two VDOMs.

In the case of a NAT-to-NAT inter-VDOM link, both sides of the link must be on the same IP subnet, because you are creating a point-to-point network connection.

Note that like using inter-VLAN routing, Layer 3 must be involved—you cannot create an inter-VDOM link between Layer 2 transparent mode VDOMs. At least one of the VDOMs must be operating in NAT mode. This, among other benefits, prevents potential Layer 2 loops.

**DO NOT REPRINT  
© FORTINET**

## Inter-VDOM Links (Contd)

- Inter-VDOM links allow VDOMs to communicate
  - Traffic is not required to leave a physical interface then re-enter FortiGate
  - Fewer physical interfaces or cables are required
    - This prevents the wasting of physical interfaces, and eliminates the need for a loopback cable
- Routes are required to forward the traffic from one VDOM to another
- Firewall policies are also required to allow traffic from other VDOMs, the same as traffic coming from physical interfaces

When creating inter-VDOM links, you must create the virtual interfaces. You must also create the appropriate firewall policies in each VDOM, just as you would if the traffic were arriving on a network cable, otherwise, FortiGate will block it.

Additionally, routes are required to correctly route packets between two VDOMs.

DO NOT REPRINT  
© FORTINET

## Creating Inter-VDOM Links

The screenshot displays the FortiGate GUI for creating inter-VDOM links. The breadcrumb navigation shows 'Global > Network > Interfaces'. A 'Create New' dropdown menu is open, with 'VDOM Link' selected and highlighted by a red box. A red arrow points from this selection to the 'New VDOM Link' configuration window. The configuration window is titled 'New VDOM Link' and shows two interfaces being configured:

- Interface 0 (vlink0):**
  - Name: vlink
  - Virtual Domain: root
  - IP/Netmask: 10.10.100.1/30
  - Administrative Access:  HTTPS,  SSH,  PING,  SNMP
  - Comments: Write a comment... (0/255)
  - Status:  Enabled,  Disabled
- Interface 1 (vlink1):**
  - Virtual Domain: VDOM1
  - IP/Netmask: 10.10.100.2/30
  - Administrative Access:  HTTPS,  SSH,  PING,  SNMP
  - Comments: Write a comment... (0/255)
  - Status:  Enabled,  Disabled

At the bottom of the configuration window are 'OK' and 'Cancel' buttons. The Fortinet logo and 'Training Institute' text are visible in the bottom left corner. The copyright notice '© Fortinet Inc. All Rights Reserved.' is in the bottom center, and the page number '36' is in the bottom right corner.

On the GUI, you create a network interface in the **Global** settings. To create the virtual interface, click **Create New**, and then select **VDOM Link**.

## Inter-VDOM Link Acceleration

- FortiGate devices with NP4 or NP6 processors include inter-VDOM links that FortiGate can use to accelerate inter-VDOM link traffic
- For a FortiGate device with two NP4 or NP6 processors, there are two accelerated inter-VDOM links, each with two interfaces:
  - **npu0\_vlink:**
    - npu0\_vlink0
    - npu0\_vlink1
  - **npu1\_vlink:**
    - npu1\_vlink0
    - npu1\_vlink1
- These interfaces are visible on the GUI and CLI

FortiGate devices with NP4 or NP6 processors include inter-VDOM links that FortiGate can use to accelerate inter-VDOM link traffic. For a FortiGate with two NP4 or NP6 processors, there are two accelerated inter-VDOM links, each with two interfaces:

- **npu0\_vlink:**
  - npu0\_vlink0
  - npu0\_vlink1
- **npu1\_vlink:**
  - npu1\_vlink0
  - npu1\_vlink1

These interfaces are visible on the GUI and CLI. By default, the interfaces in each inter-VDOM link are assigned to the root VDOM. To use these interfaces to accelerate inter-VDOM link traffic, assign each interface in the pair to the VDOMs that you want to offload traffic between. For example, if you have added a VDOM named *New-VDOM* to a FortiGate with NP4 processors, you can click **System > Network > Interfaces** and edit the **npu0-vlink1** interface and set the VDOM to *New-VDOM*. This results in an accelerated inter-VDOM link between *root* and *New-VDOM*.

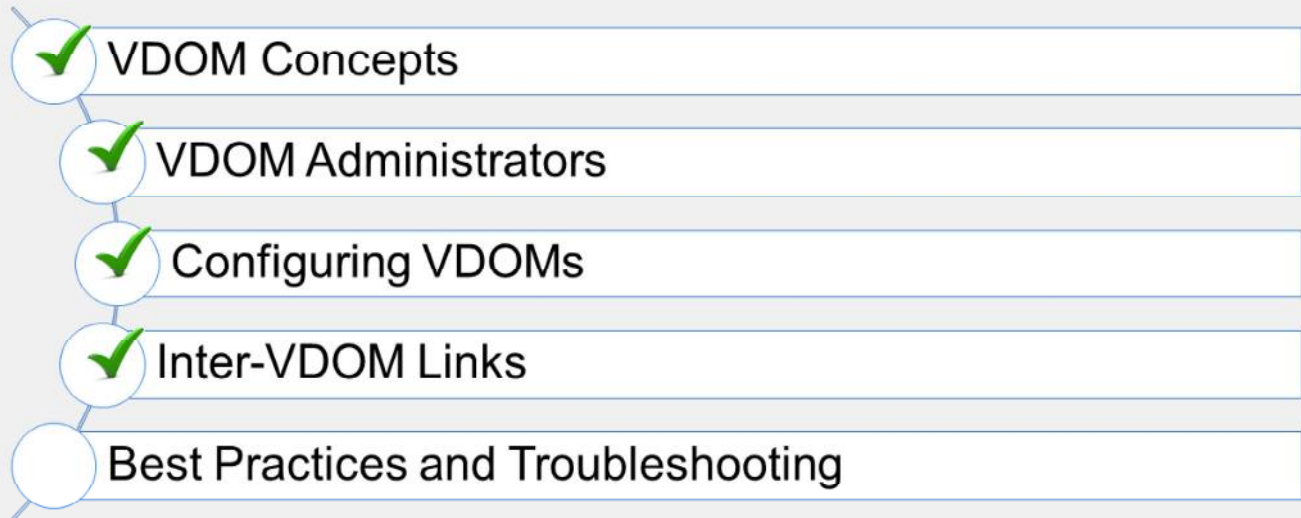
**DO NOT REPRINT**  
**© FORTINET**

## Knowledge Check

1. What is a requirement for creating an inter-VDOM link between two VDOMs?
  - A. The NGFW mode of at least one VDOM must be profile based.
  - ✓ B. At least one of the VDOMs must be operating in NAT mode.
2. Which type of VDOM link requires that both sides of the link be assigned an IP address within the same subnet?
  - A. NAT-to-transparent
  - ✓ B. NAT-to-NAT

DO NOT REPRINT  
© FORTINET

## Lesson Progress



Good job! You now understand inter-VDOM Links.

Now, you'll learn about VDOM best practices and troubleshooting.

DO NOT REPRINT  
© FORTINET

## Best Practices and Troubleshooting

### Objectives

- Limit the resources allocated globally and per VDOM
- Troubleshoot common VDOM issues

**FORTINET**  
Training Institute

40

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

By demonstrating competence in VDOM best practices and troubleshooting, you will be able to prevent, identify, and solve common VDOM issues.

DO NOT REPRINT  
© FORTINET

## System Resource Allocation

- Global resources limit: apply to resources that are shared by the whole FortiGate
- VDOM resources limit: per-VDOM resources are specific to each VDOM
  - Default per-VDOM resource settings are set to have **no limits**.
  - Guarantees a per-VDOM minimum resource allocation
  - No VDOM can starve the others of all the device resources

Remember, VDOMs are only a *logical* separation—each VDOM shares physical resources with the others.

By default, all per-VDOM resource settings are set to have no limits. This means that any single VDOM can use all of the FortiGate device's resources. This could deprive other VDOMs of the resources that they require, to the point that could be unable to function.

Unlike FortiGate-VM, VDOMs are not allocated and balanced with weighted vCPU cores, vRAM, and other virtualized hardware.

To fine-tune performance, you can configure resource limits for each feature—IPsec tunnels, address objects, and so on—at the global level and at each VDOM level. This controls the ratio of the system resource usage of each VDOM to the total available resources.

DO NOT REPRINT  
© FORTINET

## Global and Per-VDOM Resource Limits

**Global > System > Global Resources**

Resource	Current Usage	Default Maximum	Override Maximum
Active Sessions	239	No Limit Set	<input type="checkbox"/>
<b>Policy &amp; Objects</b>			
Firewall Policies	24	21024	<input type="checkbox"/>
Firewall Address	54	11024	<input type="checkbox"/>
Firewall Address Groups	10	5000	<input type="checkbox"/>
Firewall Custom Services	107	No Limit Set	<input type="checkbox"/>
Firewall Service Groups	8	No Limit Set	<input type="checkbox"/>
Firewall One-time Schedules	0	No Limit Set	<input type="checkbox"/>
Firewall Recurring Schedules	5	No Limit Set	<input type="checkbox"/>
<b>User &amp; Device</b>			

**Global > System > VDOM** Per-VDOM resource limits

Virtual Domain: VDOM3  
 NGFW Mode: Profile-based  
 Central SRAAT:   
 WiFi country/region: United States

Resource Usage

Resource	Current Usage	Global Maximum	Override Maximum	Guaranteed
Active Sessions	0	No Limit Set	<input type="checkbox"/>	
<b>Policy &amp; Objects</b>				
Firewall Policies	0	21024	<input type="checkbox"/>	
Firewall Address	0	11024	<input type="checkbox"/>	
VPN IPsec Phase1 Tunnels	0	2000	<input checked="" type="checkbox"/> 1900	1000
Firewall Service Groups	0	No Limit Set	<input type="checkbox"/>	
Firewall One-time Schedules	0	No Limit Set	<input type="checkbox"/>	

© Fortinet Inc. All Rights Reserved. 42

For example, a FortiGate with hardware powerful enough to handle up to 2000 IPsec VPN tunnels and configured with three VDOMs, could be configured as follows to meet specific criteria: VDOM1 and VDOM2 don't use IPsec VPN tunnels often. So, they are allowed to have up to 50 tunnels each. VDOM3, however, uses VPN extensively. Therefore, this FortiGate device is configured to allow VDOM3 to have up to 1900 tunnels, with 1000 guaranteed.

Configure your FortiGate device with global limits for critical features, such as sessions, policies, and so on. Then, configure each VDOM with its own quotas and minimums, within the global limits.

DO NOT REPRINT  
© FORTINET

## Monitoring VDOM Resources

- VDOM monitor displays:
  - CPU utilization
  - Memory utilization

### Global > System > VDOM

Name	Management VDOM	NGFW Mode	Operation Mode	Status	CPU	Memory	Interfaces
customer		Profile-based	NAT	Enabled	0%	7%	port3 SSL-VPN tunnel interface (ssl.customer)
root		Profile-based	NAT	Enabled	0%	38%	port1 port2 port4 port5

On the GUI, you can click **Global > System > VDOM** to see the VDOM monitor. It displays the CPU and memory usage for each VDOM.

## VDOM Administrator Has Difficulty Gaining Access

- Confirm the administrator VDOM
- Confirm the VDOM interfaces
- Confirm the VDOM administrator's access privileges
- Confirm trusted host and IP
  
- Best Practices
  - Create a VDOM-specific administrator account for each VDOM
  - Avoid giving **super\_admin** access

With VDOMs configured, administrators have an extra layer of permissions and may have problems accessing the desired information. If an administrator cannot gain access, check the following:

- Confirm the administrator's VDOM: each administrator account, other than the **super\_admin** account, is tied to one or more specific VDOMs. That administrator is not able to access any other VDOM. It may be possible they are trying to access the wrong VDOM (one that they do not have permissions for).
- Confirm the VDOM interfaces: an administrator can access their VDOM only through interfaces that are assigned to that VDOM. If interfaces on that VDOM are disabled or unavailable, there will be no method of accessing that VDOM by its local administrator. The **super\_admin** is required to either bring up the interfaces, fix the interfaces, or move another interface to that VDOM to restore access.
- Confirm the VDOM admin access: as with all FortiGate devices, administration access on the VDOM's interfaces must be enabled for the administrators of that VDOM to gain access. For example, if SSH is not enabled, that is not available to administrators. To enable admin access, the **super\_admin** clicks **Global > Network > Interfaces** and enables administrator access for the interface in question.
- Confirm trusted host and IP: if trusted hosts are enabled on the administrator account, ensure the user is connecting from the correct, specified host address, and that no intermediate devices are performing NAT functions on the connection.

Best practice dictates that you should usually avoid unnecessary security holes. Do not provide **super\_admin** access, if possible. Instead, restrict each administrator to their relevant domain. That way, they cannot accidentally or maliciously impact other VDOMs, and any damage or mistakes will be limited in scope.

DO NOT REPRINT  
© FORTINET

## General VDOM Troubleshooting Tips

- Perform a sniffer trace

```
diagnose sniffer packet <interface_name> <'filter'> <verbose> <count>
```

- Perform a packet flow trace

```
diagnose debug enable  
diagnose debug flow filter addr <PC1>  
diagnose debug flow trace start 100
```

Besides ping and traceroute, there are additional tools for troubleshooting your VDOM configurations. The primary tools for VDOM troubleshooting include packet sniffing and debugging the packet flow.

- Perform a sniffer trace: when troubleshooting networks, it helps to look inside the headers of packets to determine if they are traveling along the expected route. Packet sniffing can also be called a network tap, packet capture, or logic analyzing. The sniffer also indicates what traffic is entering or leaving the egress and ingress interfaces in all VDOMS. This makes it extremely useful for troubleshooting inter-VDOM routing issues.
- Debug the packet flow: traffic should enter and leave the VDOM. If you have identified that network traffic is not entering and leaving the VDOM as expected, debug the packet flow. You can debug only using CLI commands. This tool provides more granular details for help in troubleshooting inter-VDOM traffic because it gives details of routing selection, NAT, and policy selection.

**DO NOT REPRINT**  
**© FORTINET**

## Knowledge Check

1. Of these options, what is a possible reason why an administrator might not be able to gain access to a specific VDOM?
  - ✓ A. The administrator is using an IP address that is not specified as a trusted host.
  - B. The administrator is using the super\_admin profile.
2. Which troubleshooting tool is most suitable when trying to verify the firewall policy used by an inter-VDOM link?
  - A. Sniffer trace
  - ✓ B. Packet flow trace

**DO NOT REPRINT**  
**© FORTINET**

## Lesson Progress

- ✓ VDOM Concepts
- ✓ VDOM Administrators
- ✓ Configuring VDOMs
- ✓ Inter-VDOM Links
- ✓ Best Practices and Troubleshooting

Congratulations! You have completed this lesson.

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

**DO NOT REPRINT  
© FORTINET**

## Review

- ✓ Define and describe VDOMs
- ✓ Create administrative accounts with access limited to one or more VDOMs
- ✓ Configure VDOMs to split FortiGate into multiple virtual devices
- ✓ Route traffic between VDOMs
- ✓ Limit the resources allocated globally and per VDOM

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

By mastering the objectives covered in this lesson, you learned how to configure VDOMs, and examined examples of common use.

DO NOT REPRINT  
© FORTINET

**FORTINET.**  
Training Institute

**FortiGate Infrastructure**

Fortinet Single Sign-On (FSSO)

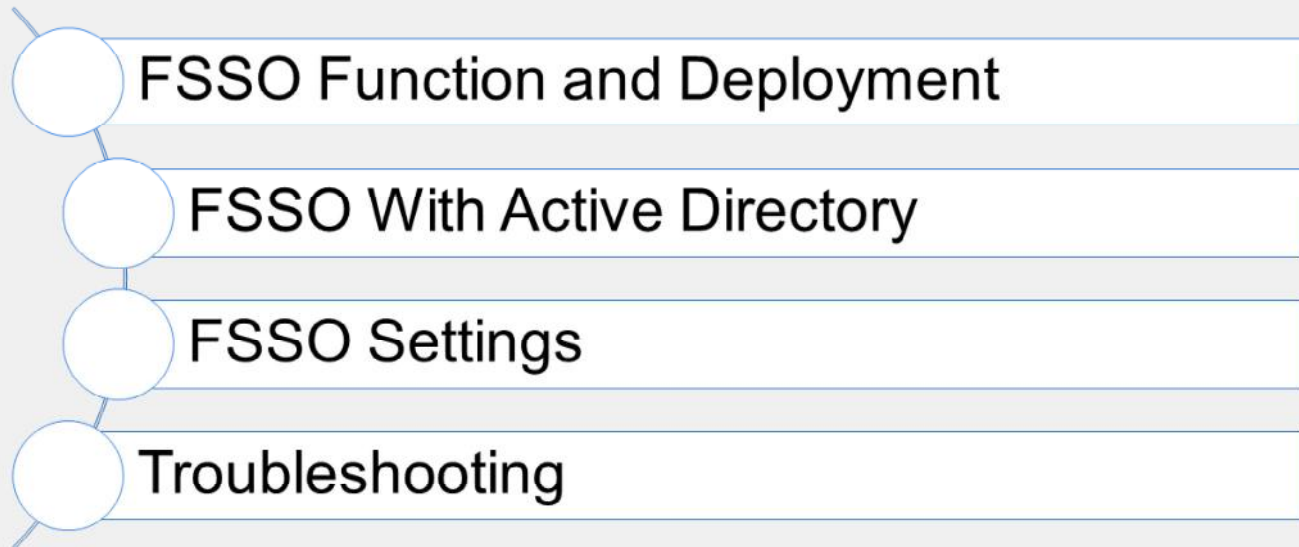
FortiOS 7.2

Last Modified: 13 June 2022

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**

## Lesson Overview



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

DO NOT REPRINT  
© FORTINET

## FSSO Function and Deployment

### Objectives

- Define single sign-on (SSO) and Fortinet single sign-on (FSSO)
- Understand FSSO deployment and configuration

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 re-authenticate
- 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 of them
- Each FSSO method gathers login events differently
- FSSO is typically used with directory services, such as Windows Active Directory or Novell eDirectory

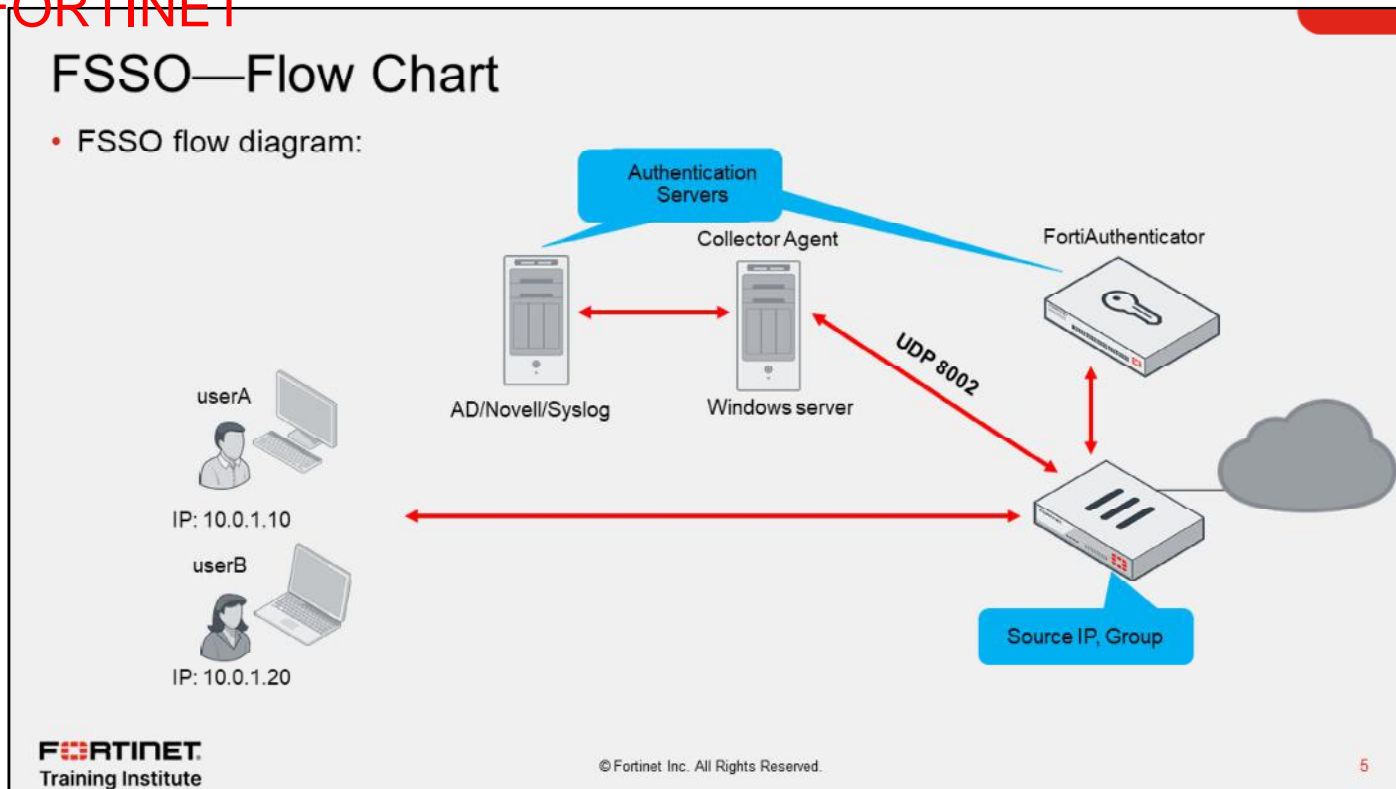
SSO is a process that allows users to be automatically logged in to every application after being identified, regardless of platform, technology, and domain.

FSSO is a software agent that enables FortiGate to identify network users for security policies or for VPN access, in advanced deployments with FortiAuthenticator, 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



This slide shows the FSSO flow we discussed in the previous slide.

**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**

## Knowledge Check

1. In FSSO, FortiGate allows network access based on \_\_\_\_\_.
  - A. Active user authentication with username and password
  - ✓ B. Passive user identification by user ID, IP address, and group membership
2. Which working mode is used for monitoring user sign-on activities in Windows AD?
  - ✓ A. Polling mode (collector agent-based or agentless)
  - B. eDirectory agent mode

**DO NOT REPRINT**  
**© FORTINET**

## Lesson Progress

- FSSO Function and Deployment
- FSSO With Windows Active Directory
- FSSO Settings
- Troubleshooting

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

Now, you'll learn about user login events in Windows Active Directory using FSSO.

DO NOT REPRINT  
© FORTINET

**FSSO With Windows Active Directory**

**Objectives**

- Detect user login events in Windows AD using FSSO
- Identify FSSO modes for Windows AD

**FORTINET**  
Training Institute

9

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

By demonstrating competence in understanding the different ways you can configure FSSO for Windows AD, you will be better able to design the architecture of your SSO system.

**DO NOT REPRINT**  
**© FORTINET**

## DC Agent Mode

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

DC agent mode is considered the recommended mode for FSSO.

DC agent mode requires:

- One DC agent installed on each Windows DC  
 If you have multiple DCs, 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.

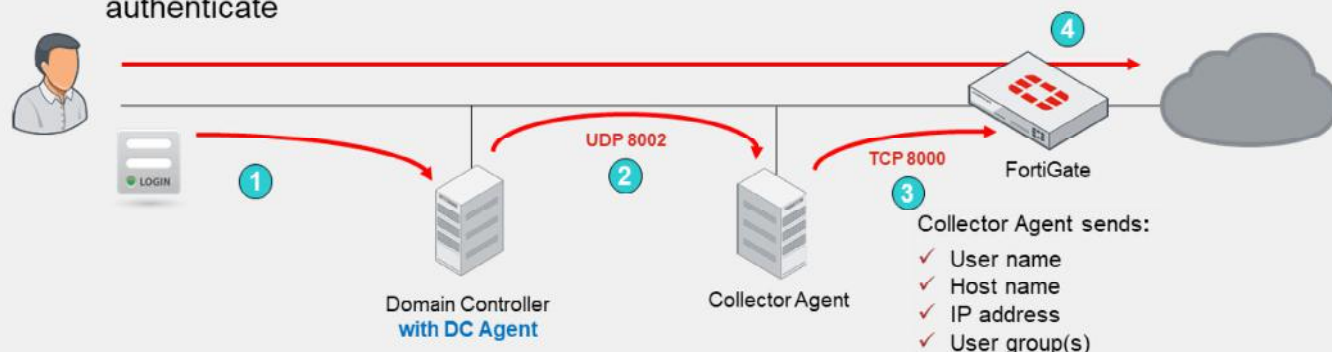
In some configurations, double DNS resolution is a problem. In this case, you may configure a registry key on the domain controller that hosts the DC agent in order not to resolve the DNS:

```
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.

11

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

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

**DO NOT REPRINT**  
**© FORTINET**

## Collector Agent-Based Polling Mode

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

Polling mode can be collector agent-based or agentless.

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

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

DO NOT REPRINT  
© FORTINET

## Collector Agent-Based Polling Mode Options

### WMI

- 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

Most recommended → Least recommended

### 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

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

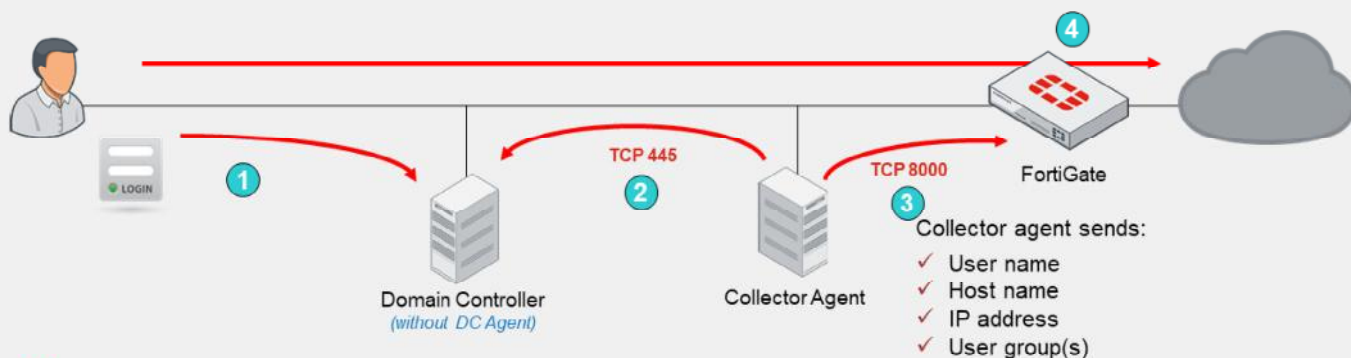
As previously stated, collector agent-based polling mode has three methods (or options) for collecting login information. The order on the slide from left to right shows most recommend to least recommended:

- **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. For a full list of supported event IDs, visit the Fortinet Knowledge Base (<http://kb.fortinet.com>).
- **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.

14

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

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.

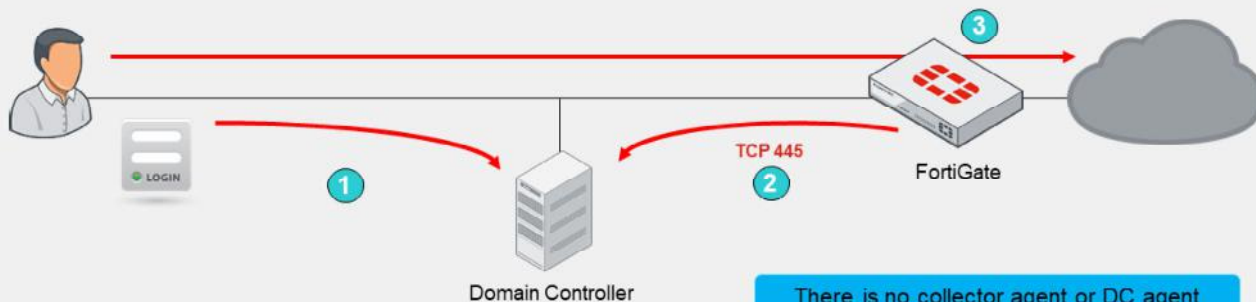
Agentless polling mode operates in a similar way to WinSecLog, but with only two event IDs: 4768 and 4769. Because there's no collector agent, FortiGate uses the SMB protocol to read the event viewer logs from the DCs.

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



**FORTINET**  
Training Institute

© Fortinet Inc. All Rights Reserved.

16

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

1. FortiGate polls the DC TCP port 445 to collect user login events.
2. After the user authenticates with the DC, FortiGate registers a login event during its next poll, obtaining the following information: the user name, the host name, and the IP address. FortiGate then queries for the user's user group(s).
3. When the user sends traffic, FortiGate already knows whose traffic it is receiving; therefore, the user does not need to authenticate.

**DO NOT REPRINT**  
**© FORTINET**

## Comparing Modes

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

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

DC agent mode is more complex. It requires not only a collector agent, but also a DC agent for each monitored domain controller. However, it is also more scalable because the 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 might 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
  - Remote registry service might be needed on each workstation

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 them 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.
- 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 if the IP of the user has changed.

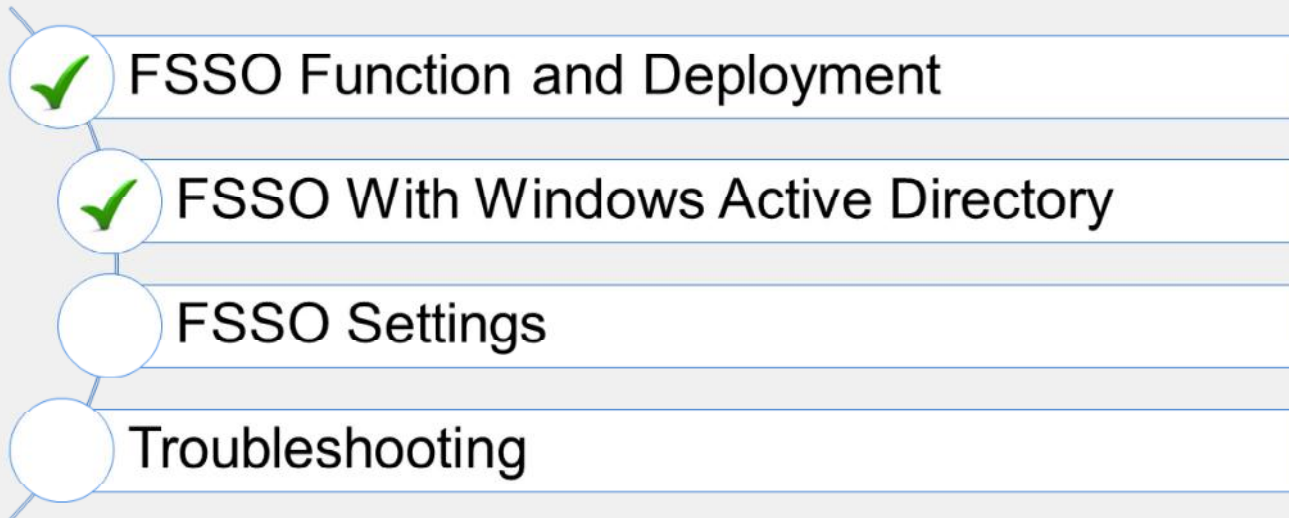
**DO NOT REPRINT**  
**© FORTINET**

## Knowledge Check

1. Which is the recommended mode for FSSO deployments?
  - ✓ A. DC agent mode
  - B. Polling mode: Agentless
2. Which FSSO mode requires more FortiGate system resources (CPU and RAM)?
  - A. Polling mode: Collector agent-based
  - ✓ B. Polling mode: Agentless

**DO NOT REPRINT**  
**© FORTINET**

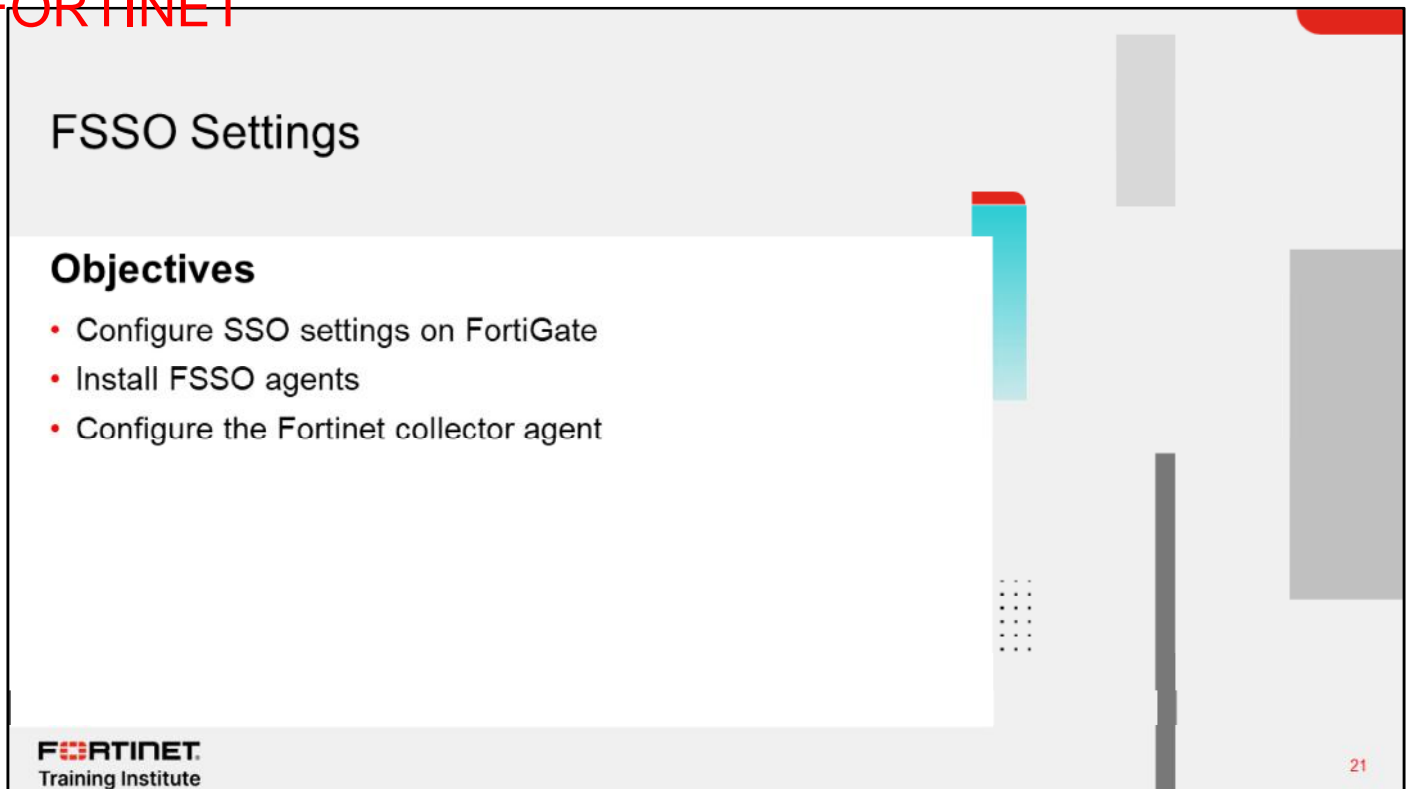
## Lesson Progress



Good job! You now understand how FortiGate detects login events in Windows Active Directory (AD) using FSSO.

Now, you'll learn how to configure FSSO settings.

**DO NOT REPRINT  
© FORTINET**



## FSSO Settings

### Objectives

- Configure SSO settings on FortiGate
- Install FSSO agents
- Configure the Fortinet collector agent

**FORTINET**  
Training Institute

21

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

By demonstrating competence in configuring the FSSO settings on FortiGate, and installing and configuring the FSSO agents, you will be able to implement FSSO within your network.

DO NOT REPRINT  
© FORTINET

## FSSO Configuration—Agentless Polling Mode

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

The diagram illustrates the configuration steps for FSSO in Agentless Polling Mode. It begins with the FortiGate interface showing the **Security Fabric** menu, where **External Connectors** is highlighted. This leads to a selection screen for **Endpoint/Identity**, where **Poll Active Directory Server** is selected. The final step is the **New External Connector** configuration screen, which includes fields for **Server IP/Name**, **User**, **Password**, and **LDAP server**, along with an **Enable polling** checkbox.

**FORTINET**  
Training Institute

© Fortinet Inc. All Rights Reserved.

22

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

The screenshot shows the 'New External Connector' configuration window for 'FSSO Agent on Windows AD'. The 'User group source' is set to 'Collector Agent' and 'Local' is selected. A blue arrow points to the 'Local' selection. The 'Connector Settings' section includes fields for Name, Primary FSSO agent (Server IP/Name and Password), Trusted SSL certificate, User group source, and Users/Groups. The 'Apply & Refresh', 'OK', and 'Cancel' buttons are at the bottom.

© Fortinet Inc. All Rights Reserved. 23

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:

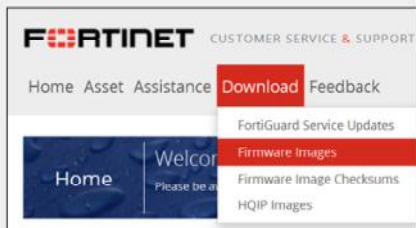
- Collector Agent:** You create group filters are created on the collector agent. You can set FortiGate to **Collector Agent** mode, and the collector agent can still use **Advanced** mode to access nested groups.
- Local:** You create group filters on FortiGate, using the LDAP server. If you set FortiGate 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 **Download > Firmware Images**
3. Select **FortiGate**, then click **Download**.
4. Click **v7.00 > 7.2 > 7.2.0 > FSSO**

Example image below:



### Available agents:

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

Image Folders/Files				
<a href="#">Link to browser-level directory</a>				
Name	Size (KB)	Date Created	Date Modified	HTTPS Checksum
DCAgent_Setup_5.0.0295.exe	3,445	2021-03-30 16:03:42	2021-03-30 16:03:43	HTTPS Checksum
DCAgent_Setup_5.0.0295.msi	3,112	2021-03-30 16:03:47	2021-03-30 16:03:48	HTTPS Checksum
DCAgent_Setup_5.0.0295_x64.exe	4,105	2021-03-30 16:03:53	2021-03-30 16:03:55	HTTPS Checksum
DCAgent_Setup_5.0.0295_x64.msi	3,772	2021-03-30 16:03:58	2021-03-30 16:03:00	HTTPS Checksum
FSSO_Setup_5.0.0295.exe	9,617	2021-03-30 16:03:36	2021-03-30 16:03:39	HTTPS Checksum
FSSO_Setup_5.0.0295_x64.exe	9,909	2021-03-30 16:03:04	2021-03-30 16:03:07	HTTPS Checksum
FSSO_Setup_edirectory_5.0.0295.exe	5,549	2021-03-30 16:03:56	2021-03-30 16:03:57	HTTPS Checksum
FSSOVS00M15_build0295.aam	1	2021-03-30 16:03:45	2021-03-30 16:03:45	HTTPS Checksum
TSAgent_Setup_5.0.0295.exe	4,465	2021-03-30 16:03:01	2021-03-30 16:03:03	HTTPS Checksum
TSAgent_Setup_5.0.0295.msi	4,132	2021-03-30 16:03:50	2021-03-30 16:03:52	HTTPS Checksum

**FORTINET**  
Training Institute

© Fortinet Inc. All Rights Reserved.

24

The FSSO agents are available on the Fortinet Support website. There you will find the following:

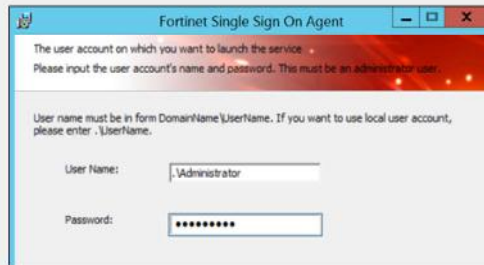
- The DC agent
- The collector agent for Microsoft servers: FSSO\_Setup
- The collector agent for Novell directories: FSSO\_Setup\_edirectory
- The terminal server agent (TSAgent) installer for Citrix and terminal servers: TSAgent\_Setup

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.

## 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




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: **DomainNameUserName**.
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.

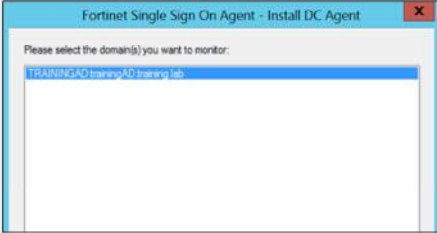
**DO NOT REPRINT**  
**© FORTINET**

## DC Agent Installation Process

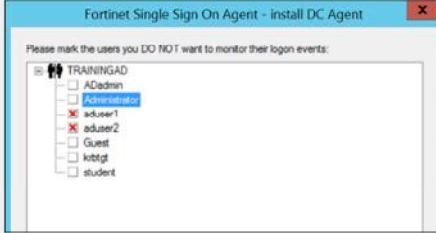
**1** IP and port for collector agent



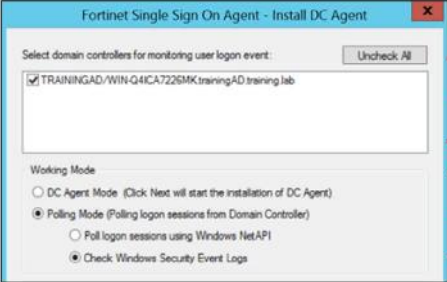
**2** Domains to monitor



**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 Inc. All Rights Reserved. 26

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

The screenshot shows the 'Fortinet Single Sign On Agent Configuration' window. Several settings are highlighted with blue callouts:

- Listening port for DC agent; default port UDP 8002:** Points to the 'DC Agent' port field, which is set to 8002.
- Enable/disable NTLM authentication:** Points to the 'Support NTLM authentication' checkbox, which is checked.
- Monitor user login events:** Points to the 'Monitoring user logon events' checkbox, which is checked.
- Listening port for FortiGate; Default is TCP 8000:** Points to the 'FortiGate' port field, which is set to 8000.
- Enable authentication between FortiGate and collector agent:** Points to the 'Require authenticated connection from FortiGate' checkbox, which is checked.
- Timers:** Points to the 'Timers' section, which includes fields for 'Workstation verify interval (minutes): 5', 'Dead entry timeout interval (minutes): 480', and 'IP address change verify interval (seconds): 60'.

Other visible settings include 'Log level: Warning', 'Log file size limit(MB): 10', and a 'Password' field. The 'Collector Agent Status' is shown as 'RUNNING'. The 'Common Tasks' panel on the right includes buttons for 'Show Service Status', 'Show Monitored DCs', 'Show Logon Users', 'Select Domains To Monitor', 'Set Directory Access Information', 'Set Group Filters', 'Set Ignore User List', 'Sync Configuration With Other Agents', and 'Export Configuration'.

**FORTINET**  
Training Institute

© Fortinet Inc. All Rights Reserved.

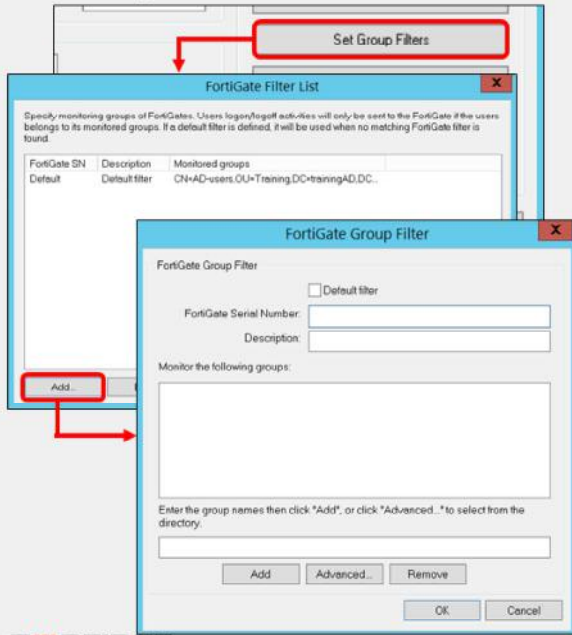
27

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
- All FortiGate devices support at least 256 Windows AD user groups
  - The group filter support is for VDOMs
- If FortiGate FSSO is set up in user group source local mode (group filtering configured on FortiGate is pushed to Collector agent), FortiGate filter will take precedence over filter set on collector agent
- The default filter applies to any FortiGate device that does not have a specific filter defined in the list
- You can set filters for groups, OUs, users, or a combination

**FORTINET**  
Training Institute

© Fortinet Inc. All Rights Reserved.

28

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.

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

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
  - All users under the selected OU are added to the **Ignore User List**

**FORTINET**  
Training Institute

© Fortinet Inc. All Rights Reserved.

29

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.

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.

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

### 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

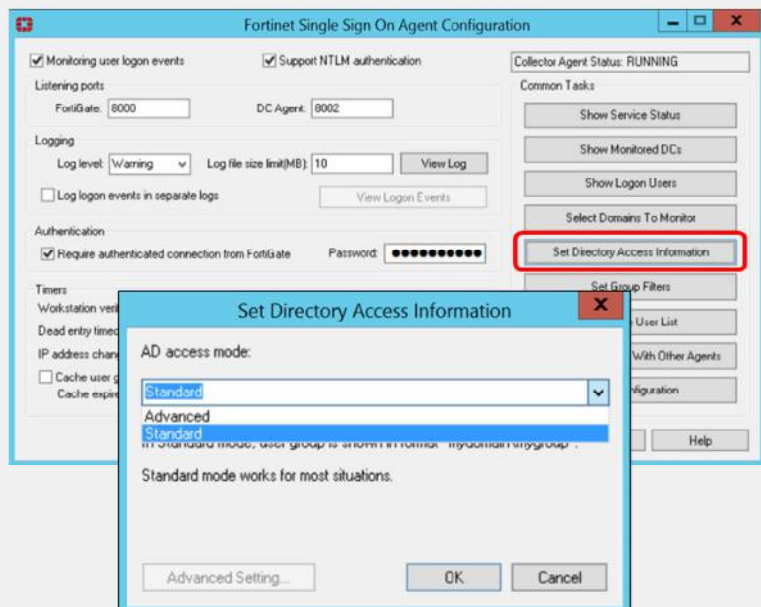
The FSSO collector agent timers play an important role in ensuring the correct operation of FSSO.

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
- UTM profiles 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
- UTM profile 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

**FORTINET**  
Training Institute

© Fortinet Inc. All Rights Reserved.

31

Another important FSSO setting is the 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, while
- **Advanced** mode uses the LDAP convention: CN=User, OU=Name, DC=Domain.

Also, 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 can apply security profiles to individual users, user groups, and OUs.

In comparison, in standard mode, you can apply security profiles only to user groups, not 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 the FortiGate says, FSSO won't work. If the FortiGate LDAP fails, but the LDAP on the collector agent is still running, the FortiGate may not be able to collect logs, but the collector agent still collects logs.

Fortinet strongly encourages users to create filters from the collector agent.

**DO NOT REPRINT  
© FORTINET**

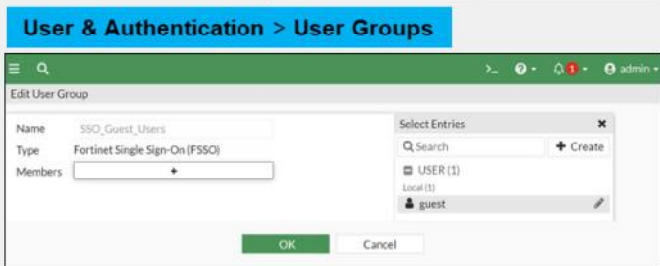
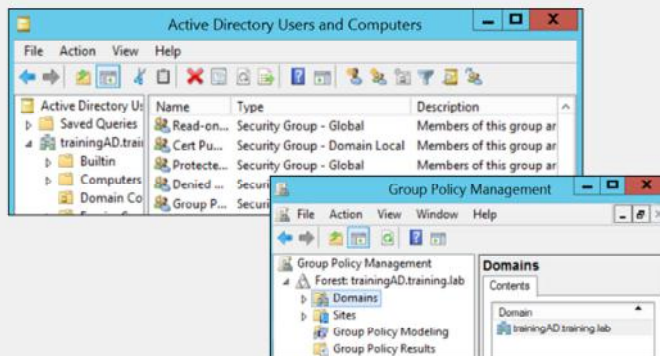
## AD Group Support

### 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.

32

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

The image shows two overlapping windows from the Fortinet Single Sign-On Agent Configuration interface. The background window is titled 'Fortinet Single Sign-On Agent Configuration' and contains various settings for monitoring, logging, authentication, and timers. A red box highlights the 'Advanced Settings' button at the bottom right of this window. The foreground window is titled 'FSSO Collector Agent Advanced Settings' and is divided into several tabs: 'Syslog Servers', 'Forwarded Event Server', 'SSL Certificates', 'General', 'Citrix/Terminal Server', 'Exchange Server', and 'RADIUS Accounting'. The 'RADIUS Accounting' tab is currently selected and highlighted with a red box. It contains fields for 'Worker thread count' (set to 128), 'Maximum FortiGate connections' (set to 64), and 'Group lookup interval (in seconds)' (set to 0). Below these are sections for 'Windows Security Event Logs' (with 'Event IDs to poll' set to 0), 'Workstation Check' (with 'Use WMI to check user logoff' checked), and 'Workstation Name Resolution Advanced Options' (with fields for 'Alternative DNS server(s)' and 'Alternative workstation suffix(es)').

### 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

### Exchange Server

- Monitor MS Exchange Server
- Allow users access to emails through the domain account
  - Accessing from the domain or not

**FORTINET**  
Training Institute

© Fortinet Inc. All Rights Reserved.

33

Depending on your network, you might need to configure advanced settings in your FSSO collector agent.

Citrix servers support FSSO. Terminal server (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 only from Citrix servers if each user gets their own IP address. Otherwise, if multiple users share the same IP address, the TS agent is needed so that it can report to the collector agent the user, IP address, and source port range assigned to that user. 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.

The FSSO collector agent can also monitor a Microsoft Exchange server, which is useful when users access their email using their domain account.

For **Windows Security Event Logs** polling mode, you can configure **Event IDs to poll** here. For specific event IDs, visit the Fortinet Knowledge Base (<http://kb.fortinet.com>).

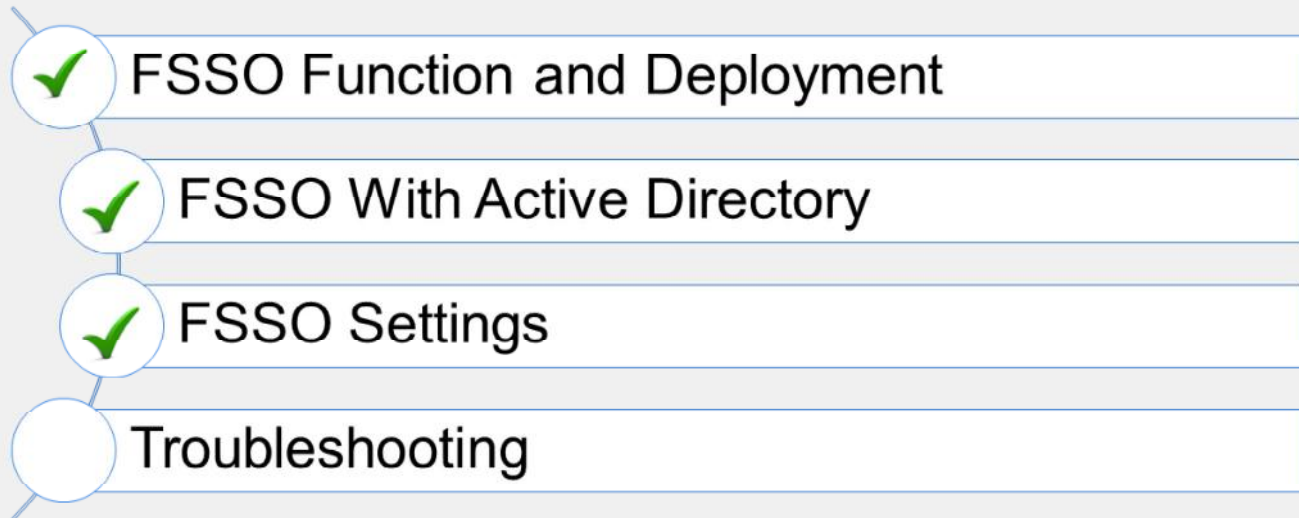
DO NOT REPRINT  
© FORTINET

## Knowledge Check

1. If you have collector agents using either the DC agent mode or the collector agent-based polling mode, which fabric connector should you select on FortiGate?
  - A. Poll Active Directory Server
  - ✓ B. Fortinet Single Sign-On Agent
  
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

**DO NOT REPRINT**  
**© FORTINET**

## Lesson Progress



Good job! You now understand how to configure the SSO settings on FortiGate and the FSSO collector agent.

Now, you'll learn about some basic troubleshooting options.

DO NOT REPRINT  
© FORTINET

## Troubleshooting

### Objectives

- Recognize and monitor FSSO-related log messages
- Perform basic FSSO troubleshooting

**FORTINET**  
Training Institute

36

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

By demonstrating competence in FSSO monitoring and troubleshooting, you will be able to prevent, identify, and solve common issues related to FSSO.



DO NOT REPRINT  
© FORTINET

## Log Messages on FSSO Collector Agent

Select the minimum severity level of logged messages:  
**Debug, Information, Warning, or Error**

Enter the maximum size for the log file. Default is 10 MB.

Show logins, lookups and verifications

Record user login-related information separately from other logs. Includes:

- Data received from DC agents
- User login/logout information
- Workstation IP change
- Data sent to FortiGate devices

Shows information sent to FortiGate

The screenshot shows the 'Fortinet Single Sign On Agent Configuration' window. The 'Logging' section is highlighted with a red box. Callouts point to the 'Log level' dropdown (set to 'Information'), the 'Log file size limit(MB)' field (set to '10'), and the 'View Log' button. Other callouts point to the 'Log level' dropdown, the 'Log file size limit(MB)' field, and the 'View Log' button. The 'Log login events in separate logs' checkbox is also checked.

**FORTINET**  
Training Institute

© Fortinet Inc. All Rights Reserved.

38

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.

## Troubleshooting Tips for FSSO

1. Ensure all firewalls allow the FSSO required ports
  - For example: ports 139 (workstation verification), 445 (workstation verification and event log polling), 389 (LDAP), 445, 636 (LDAPS), and 3268, 3269 (TLS)
2. Guarantee at least 64 Kbps bandwidth between FortiGate and domain controllers
  - Configure traffic shaping to ensure the minimum bandwidth is always available
3. Configure the timeout timer to flush inactive sessions after a shorter time
  - Alternatively, encourage users to log out of one machine before logging in to another machine
4. Ensure DNS is configured and updating IP addresses if the host IP address changes
5. Never set the timer workstation verify interval to 0
  - This prevents the collector agent from aging out stale entries. They can be removed only by a new event overwriting them
  - This can be dangerous in environments where FSSO and non-FSSO users share the same DHCP pool
6. Include all FSSO groups in the firewall policies when using passive authentication
  - Even add the SSO\_Guest\_Users to an identity-based security policy to allow traffic
  - If active authentication is used as a backup, ensure that SSO\_Guest\_User is not added to polices

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 between FortiGate and the domain controllers to ensure that the minimum bandwidth is always available. If there is insufficient bandwidth, some FSSO information might not reach FortiGate.
- In an all-Windows environment, flush inactive sessions. Otherwise, you can have a session for a non-authenticated machines go out 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 indeed logged out.
- Ensure DNS is configured correctly and updating IP addresses, if workstation IP addresses change.
- Never set the workstation verify interval to 0. This prevents the collector agent from aging out stale entries. 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 polices. SSO\_Guest\_User and active authentication are mutually exclusive.

DO NOT REPRINT  
© FORTINET

## Currently Logged-On Users

```
# diagnose debug authd fssso list
----FSSO logins----
IP: 10.0.1.10 User: ADUSER1 Groups: TRAININGAD/AD-USERS
Workstation: WIN-INTERNAL MemberOf: Training
IP: 192.168.131.5 User: ADUSER1 Groups: TRAININGAD/AD-USERS
Workstation: WIN-INTERNAL MemberOf: Training

Total number of logins listed: 2, filtered: 0
----end of FSSO logins----
```

IP address

Workstation name

User name

User group

Group created on FortiGate

Dashboard > Users & Devices > Firewall Users

# execute fssso refresh

User Group Training  
Members TRAININGAD/AD-USERS  
Group Type Fortinet Single Sign-On (FSSO)

© Fortinet Inc. All Rights Reserved.

40

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 enable
# 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`.

However, before you use that command, you must first run the command `diagnose debug enable`.

DO NOT REPRINT  
© FORTINET

## Additional Commands

```
# diagnose debug authd fsso <...>
```

```
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-logins
```

Delete cached login status

```
refresh-logins
```

Resynchronize login database

```
server-status
```

Show status of FSSO server connection

```
# 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

Also, available under `diagnose debug authd fsso` 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 fsso-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 Feb 4 09:47:31 2015
```

```
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 fsso-polling refresh-user
```

```
refresh completes. All login users are obsolete. Please re-login to make them available.
```

Active FSSO users

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

Sniff polls

```
diagnose debug application fssod -1
```

**FORTINET**  
Training Institute

© Fortinet Inc. All Rights Reserved.

43

The command `diagnose debug fsso-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 fsso-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 logging level shows the login events on the collector agent?
  - ✓ A. Information
  - B. Warning
2. The command `diagnose debug fssso-polling detail` displays information for which mode of FSSO?
  - ✓ A. Agentless polling
  - B. Collector agent-based polling

**DO NOT REPRINT**  
**© FORTINET**

## Lesson Progress

-  Fortinet FSSO Function and Deployment
-  FSSO with Active Directory
-  FSSO Settings
-  Troubleshooting

Congratulations! You have completed this lesson.

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

**DO NOT REPRINT**  
**© FORTINET**

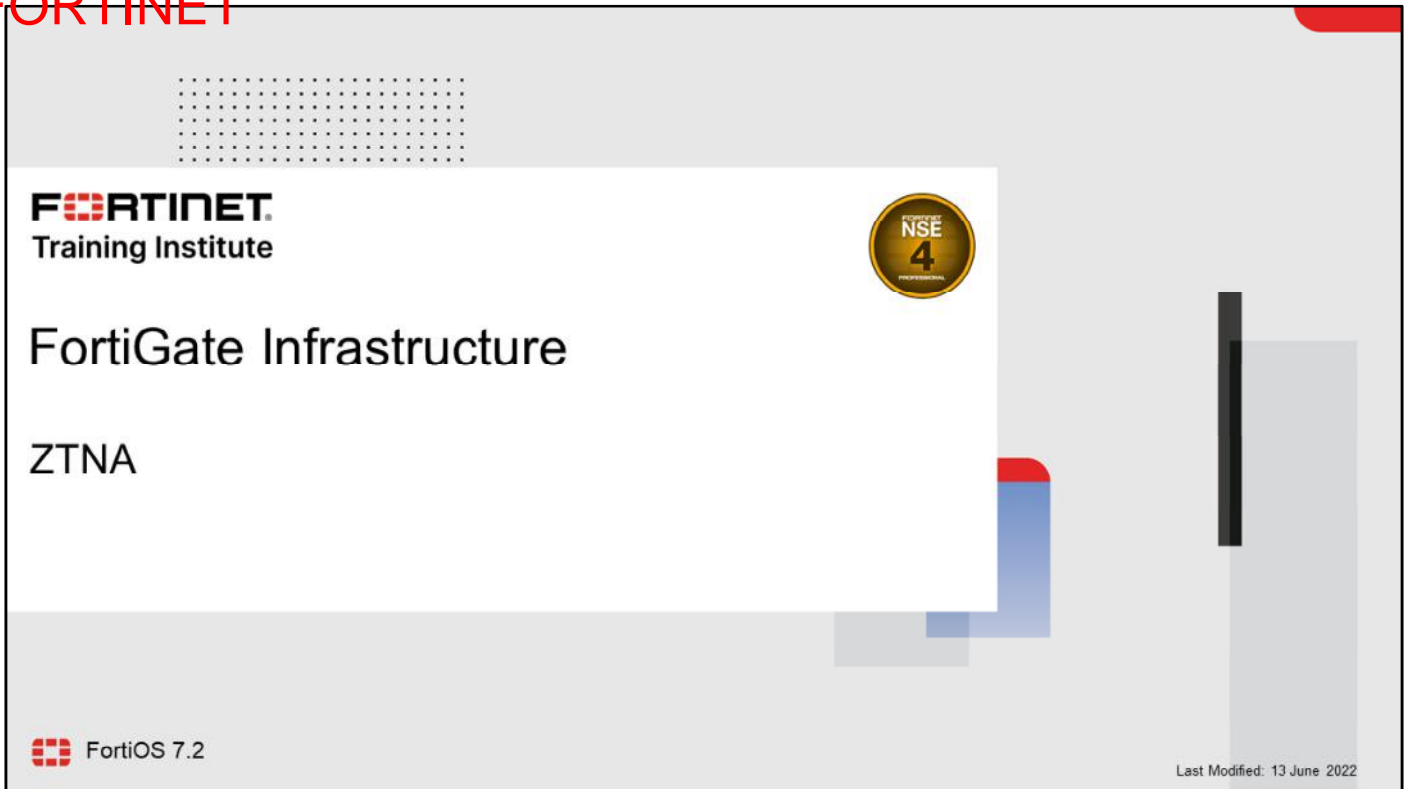
## Review

- ✓ Define SSO and FSSO
- ✓ Understand FSSO deployment and configuration
- ✓ Detect user login events in Windows AD using FSSO
- ✓ Identify FSSO modes for Windows AD
- ✓ Configure SSO settings on FortiGate
- ✓ Install FSSO agents
- ✓ Configure a Fortinet collector agent
- ✓ Recognize and monitor FSSO-related messages
- ✓ Perform basic FSSO troubleshooting

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



The slide features a white background with a grid of dots in the top left corner. The Fortinet logo is in the top left, followed by 'Training Institute'. A gold NSE 4 Professional badge is in the top right. The main title 'FortiGate Infrastructure' is centered, with 'ZTNA' below it. The FortiGate logo and 'FortiOS 7.2' are in the bottom left. The text 'Last Modified: 13 June 2022' is in the bottom right. The slide is framed by a grey border with a red corner in the top right and a blue and red corner in the bottom right.

**FORTINET**  
Training Institute

NSE  
4  
PROFESSIONAL

FortiGate Infrastructure

ZTNA

FortiOS 7.2

Last Modified: 13 June 2022

In this lesson, you will learn about zero-trust network access (ZTNA).

**DO NOT REPRINT**  
**© FORTINET**

## Lesson Overview



ZTNA Introduction



Comparing ZTNA to SSL and IPSec  
VPN

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

**DO NOT REPRINT  
© FORTINET**

## ZTNA

### Objectives

- Understand the benefits of using ZTNA
- Understand the fundamentals of ZTNA
- Understand how to establish device identity and trust
- Understand SSL certificate-based authentication
- Configure ZTNA access on FortiOS
- Describe types of ZTNA configuration

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

By demonstrating competence in ZTNA, you will be able to understand key ZTNA concepts and how to configure ZTNA.

## What is ZTNA?

- Access control method that provides role-based application access
- ZTNA method uses:
  - Client device identification
  - Authentication
  - Zero-trust tags
- Provides flexibility to manage both on-net and off-net users
- ZTNA has two modes:
  - ZTNA access proxy
  - IP/MAC-based access control (on-fabric, devices for IT compliances, and rules enforcement)

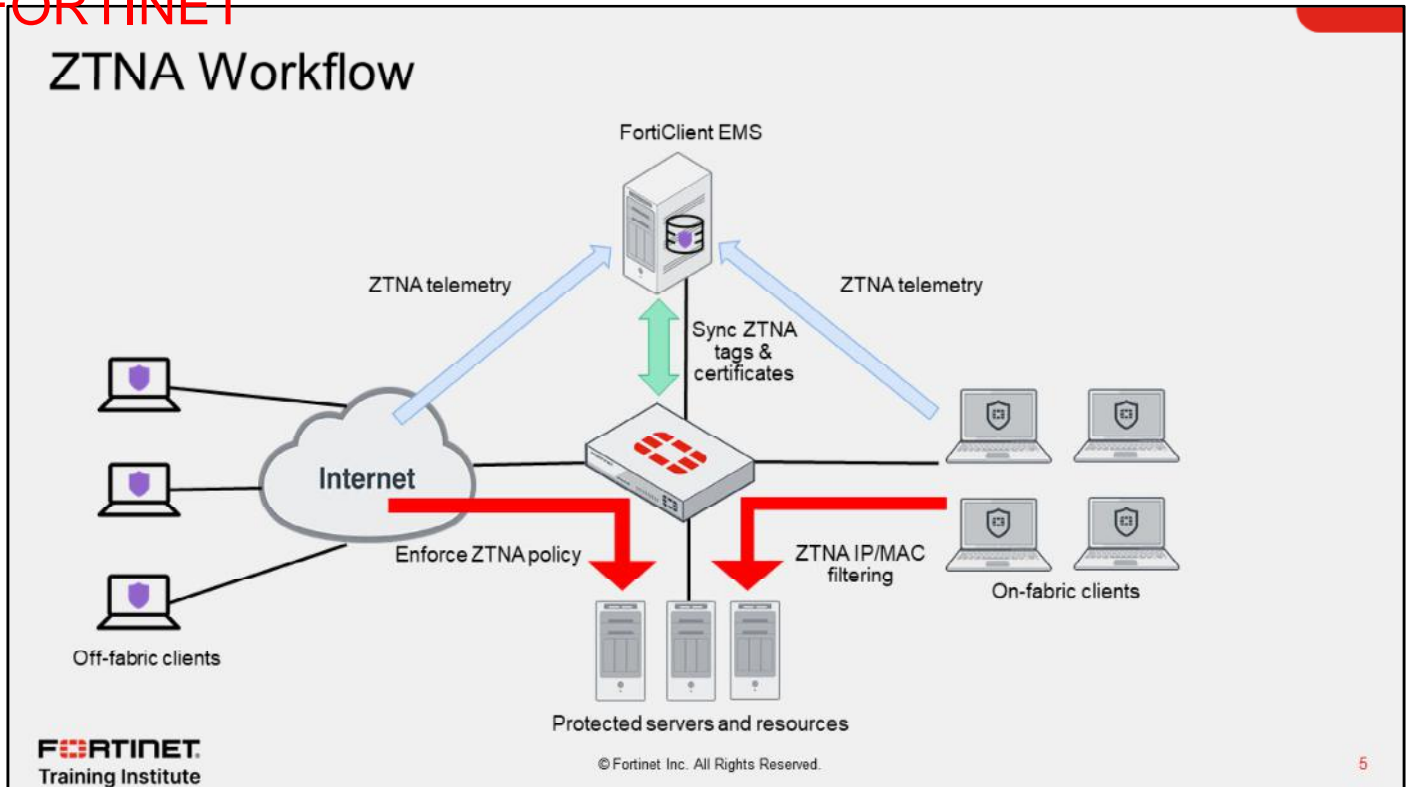
ZTNA is an access control method that uses client device identification, authentication, and zero-trust tags to provide role-based application access. ZTNA gives administrators the flexibility to manage network access for on-fabric local users and off-fabric remote users. ZTNA grants access to applications only after a device verification, authenticating the user's identity, authorizing the user, and then performing context-based posture checks using zero-trust tags.

Traditionally, a user and a device have different sets of rules for on-fabric access and off-fabric VPN access to company resources. With a distributed workforce, and access that spans company networks, data centers, and the cloud, managing the rules can be complex. User experience is also affected when an organization needs multiple VPNs to access various resources.

ZTNA has two modes:

- ZTNA access proxy allows users to securely access resources through an SSL-encrypted access proxy. This simplifies remote access by eliminating the use of VPNs.
- IP/MAC filtering uses ZTNA tags to provide an additional factor for identification, and a security posture check to implement role-based zero-trust access. IP/MAC-based access control enhances security when endpoints are physically located on the corporate network, whereas ZTNA access proxy focuses on access for remote users. IP/MAC-based access control combines IP/MAC with ZTNA tags for identification and security posture check to implement role-based zero-trust access. Firewall policies are configured that use ZTNA tags to control access between on-net devices and an internal webserver. This mode does not require the use of the access proxy, and only uses ZTNA tags for access control.

DO NOT REPRINT  
© FORTINET



This slide demonstrates ZTNA telemetry, tags, and policy enforcement. You configure ZTNA tag conditions and policies on FortiClient EMS. FortiClient EMS shares the tag information with FortiGate through Security Fabric integration. FortiClient communicates directly with FortiClient EMS to continuously share device status information through ZTNA telemetry. FortiGate can then use ZTNA tags to enforce access control rules to incoming traffic through ZTNA access.

# DO NOT REPRINT © FORTINET

## Device Roles

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

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

FortiClient provides the following information to FortiClient EMS when it registers:

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

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

FortiClient EMS issues and signs the client certificate with the FortiClient UID, certificate serial number, and EMS serial number. FortiClient EMS then synchronizes the certificate with FortiGate. FortiClient EMS also shares its EMS ZTNA CA certificate with FortiGate, so that FortiGate can use it to authenticate the clients. FortiClient EMS uses zero-trust tagging rules to tag endpoints based on the information that it has on each endpoint. FortiClient EMS also shares the tags with FortiGate.

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

**DO NOT REPRINT  
© FORTINET**

## FortiClient

- Provides a comprehensive network security solution for endpoints while improving your visibility and control
  - Allows you to manage security of multiple endpoints from the FortiClient EMS
  - Allows you to manage endpoints locally or remotely, stationary or mobile, using FortiClient EMS
  - Supports multiple platform protection:
    - Windows devices
    - Mac OS devices
    - Linux OS devices
    - iOS devices
    - Android mobile devices
    - Chromebook

FortiClient provides comprehensive endpoint protection for your Windows-based, Mac-based, and Linux-based desktops, laptops, file servers, and mobile devices such as iOS and Android. It helps you to safeguard your systems with advanced security technologies, all of which you can manage from a single management console.

FortiClient enables every device—local or remote, stationary or mobile—to integrate with your FortiClient EMS and FortiGate. FortiClient supports Windows, Mac OS, Linux, iOS, Android mobile devices and Chromebook, and also integrates your home offices, mobile workers, and visiting partners.

## FortiClient (Contd)

- FortiClient is used with EMS to use all APT and security features
- FortiClient must connect to FortiClient EMS to activate the license
- You can change FortiClient configurations only from the management device
- FortiClient is either used with FortiClient EMS only or in the Security Fabric
- Enforces endpoint compliance and provides endpoint awareness
- Automates prevention of known and unknown threats
- Provides secure remote access

FortiClient must be used with FortiClient EMS. FortiClient must connect to FortiClient EMS to activate its license and become provisioned by the endpoint profile that the administrator configured in FortiClient EMS. You cannot use any FortiClient features until FortiClient is connected to FortiClient EMS and licensed.

When FortiClient is connected only to FortiClient EMS, FortiClient EMS provisions and manages FortiClient. FortiClient EMS also sends zero-trust tagging rules to FortiClient, and uses the results from FortiClient to dynamically group endpoints in EMS. Only FortiClient EMS can control the connection between FortiClient and FortiClient EMS. However, FortiClient cannot participate in the Fortinet Security Fabric.

FortiClient in the security fabric connects to FortiClient EMS to receive a profile of configuration information as part of an endpoint policy. FortiClient EMS is connected to FortiGate to participate in the Security Fabric. FortiClient EMS sends FortiClient endpoint information to FortiGate. FortiGate can also receive dynamic endpoint group lists from FortiClient EMS and use them to build dynamic firewall policies.

FortiClient also provides secure remote access to corporate assets through VPN.

## FortiClient EMS

- FortiClient EMS is a security management solution that enables:
  - Scalable and centralized management of multiple endpoints (computers)
  - Efficient and effective administration of endpoints running FortiClient
- Provides visibility across the network to securely share information and assign security profiles to endpoints
- Works with the FortiClient Web Filter extension to provide web filtering for Google Chromebook users
- Designed to meet the needs of small to large enterprises that deploy FortiClient on endpoints and/or provide web filtering for Google Chromebook users

FortiClient EMS is a security management solution that enables scalable and centralized management of multiple endpoints (computers). It also provides efficient and effective administration of endpoints running FortiClient, and visibility across the network to securely share information and assign security profiles to endpoints. It is designed to maximize operational efficiency and includes automated capabilities for device management and troubleshooting.

FortiClient EMS also works with the FortiClient Web Filter extension to provide web filtering for Google Chromebook users.

The benefits of deploying FortiClient EMS include:

- Remotely deploying FortiClient software to Windows computers
- Updating profiles for endpoint users regardless of access location
- Administering FortiClient endpoint connections, such as accepting, disconnecting, and blocking connections
- Managing and monitoring endpoints, such as status, system, and signature information
- Identifying outdated versions of FortiClient software
- Defining web filtering rules in a profile, and remotely deploying the profile to the FortiClient Web Filter extension on Google Chromebook endpoints

You can manage endpoint security for Windows and macOS platforms using a unified organizational security policy. An organizational security policy provides a full, understandable view of the security policies defined in the organization. You can see all policy rules, assignments, and exceptions in a single unified view. FortiClient EMS is part of the Fortinet Endpoint Security Management suite, which ensures comprehensive policy administration and enforcement for an enterprise network.

## FortiGate and FortiClient EMS Connectivity

- FortiGate uses FortiClient EMS fabric connector to connect
- FortiGate must verify the FortiClient EMS server certificate
  - Need to install CA certificate on FortiGate, otherwise certificate is not trusted
- FortiClient EMS must authorize the FortiGate as fabric device

The image displays three screenshots from the FortiGate GUI illustrating the configuration process:

- Security Fabric > Fabric Connectors:** Shows the configuration page for a FortiClient EMS connector. A yellow warning box states: "In order for the FortiGate EMS and FortiClient to communicate, the following certificate must be installed on the FortiGate EMS and accepted for importation, and accepted in the device trust." The configuration includes fields for Name, ID, HTTP port, and EMS server address.
- Administration > Fabric Devices:** Shows a "Fabric Device Authorization Requests" dialog box. It displays system information for a device (Serial Number, IP Address, Last Seen) and buttons for "Authorize", "Deny", "View Detail", and "Cancel".
- Fabric Connectors:** Shows a list of external connectors, including "FortiClient EMS" and "EMSServer". A callout bubble points to the "FortiClient EMS" entry, labeled "Fabric connector status".

You can configure the on-premises FortiClient EMS connector on FortiGate by clicking **Security Fabric > Fabric Connectors**. After applying the FortiClient EMS settings, FortiGate must accept the FortiClient EMS server certificate. However, when you configure a new connection to FortiClient EMS server, the certificate might not be trusted. To resolve, you must manually export and install the root CA certificate on FortiGate. The FortiClient EMS certificate that is used by default for the SDN connection is signed by the CA certificate that is saved on the Windows server when you first install FortiClient EMS. This certificate is stored in the **Trusted Root Certification Authorities** folder on the server. For more information about exporting and installing certificates on FortiGate, refer to the *FortiOS-7.0.1 Administration Guide*.

Next, you must authorize FortiGate on FortiClient EMS. If you log in to FortiClient EMS, a pop-up window opens, requesting you to authorize FortiGate. If you do not log in, you can click **Administration > Devices**, select the FortiGate device, and then authorize it. Note that the FortiClient EMS connector status appears down until you authorize FortiGate on FortiClient EMS.

FortiGate automatically synchronizes ZTNA tags after it connects to FortiClient EMS.

# DO NOT REPRINT © FORTINET

## Zero-Trust Tagging Rules

- You can create, edit, and delete zero-trust tagging rules for Windows, macOS, Linux, iOS, and Android
- When using tagging rules with EMS and FortiClient
  - EMS sends zero-trust tagging rules to endpoints
  - FortiClient checks endpoints using the provided rules and sends the results to EMS
  - EMS dynamically groups endpoints together using the tag configured for each rule
  - You can view the dynamic endpoint groups in **Zero Trust Tags > Zero Trust Tag Monitor**

**zero-trust Tags > zero-trust Tagging Rules**

Zero Trust Tagging Rule Set

Name: Malicious-File-Detected

Tag EndpointAs: Malicious-File-Detected

Enabled:

Comments: Optional

Rules: Edit Log: Add Rule

Type	Value
Windows (1)	
File	C:\virus.txt

Save Cancel

**zero-trust Tags > zero-trust Tagging Monitor**

Endpoint with Tag Refresh

Remote-Endpoints (1)

Endpoint	User	OS	IP	Tagged on
Remote-Client	Administrator	Microsoft Windows Ser...	10.0.2.20	2021-08-25 02:43:06

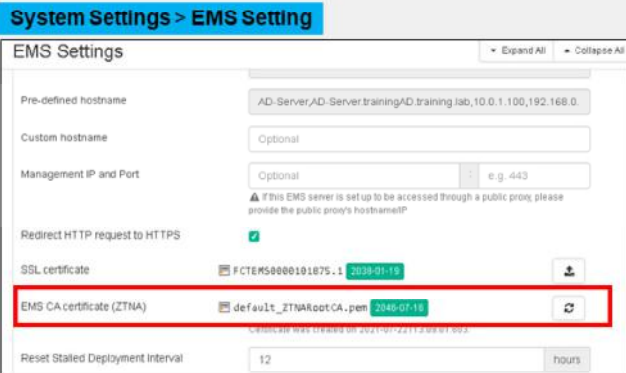
You can create, edit, and delete zero-trust tagging rules for Windows, macOS, Linux, iOS, and Android endpoints. The following happens when using zero-trust tagging rules with FortiClient EMS and FortiClient:

- FortiClient EMS sends zero-trust tagging rules to endpoints through telemetry communication.
- FortiClient checks endpoints using the provided rules and sends the results to FortiClient EMS.
- FortiClient EMS receives the results from FortiClient.
- FortiClient EMS dynamically groups endpoints together using the tag configured for each rule. You can view the dynamic endpoint groups by clicking **Zero Trust Tags > Zero Trust Tag Monitor**.

Note that when the endpoint network changes or user login and logout events occur, FortiClient triggers an X-FFCK-TAG message to EMS, even if there are no tag changes. After FortiClient EMS receives the tags, it processes them immediately, and updates the FortiOS tags within five seconds of the REST API response. For other tag changes, FortiClient sends the information to FortiClient EMS regularly.

## FortiClient EMS Certificate Management

- FortiClient EMS has a default root CA certificate
- ZTNA CA uses root certificate to sign CSRs from the FortiClient endpoints
- You can revoke and update root CA
  - Force updates to the FortiGate and FortiClient endpoints by generating new certificates
- FortiClient EMS manages individual client certificates



FortiClient EMS has a **default\_ZTNArootCA** certificate generated by default that the ZTNA CA uses to sign CSRs from the FortiClient endpoints. Clicking the refresh button revokes and updates the root CA, forcing updates to the FortiGate and FortiClient endpoints by generating new certificates for each client. FortiClient EMS can also manage individual client certificates. You can also revoke the certificate that is used by the endpoint when certificate private keys show signs of being compromised. Click **Endpoint > All Endpoints**, select the client, and then click **Action > Revoke Client Certificate**.

Do not confuse the FortiClient EMS CA certificate (ZTNA) with the SSL certificate. The latter is the server certificate that is used by FortiClient EMS for HTTPS access and fabric connectivity to the FortiClient EMS server.

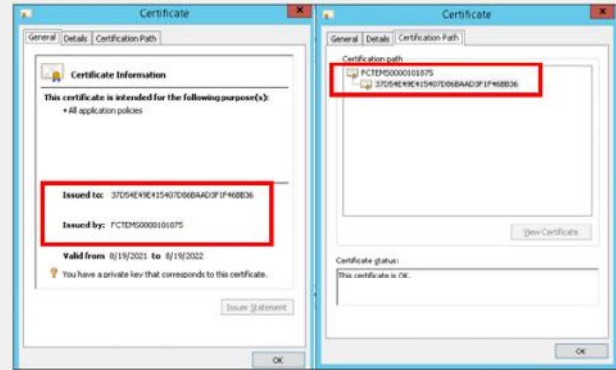
## FortiClient EMS Certificate Management (Contd)

- On Windows endpoints, FortiClient automatically installs certificates in the certificate store
  - Certificate information, such as certificate UID and SN, should match the information on FortiClient EMS and FortiGate
  - Certificates > Personal > Certificates**
- You can verify by CLI command on FortiGate
  - diagnose endpoint record list <optional IP address>

```

HQ-FortiGate # diagnose endpoint record list
Record #1:
IP Address = 10.0.1.100
MAC Address = 00:50:56:a1:1b:15
MAC List = 00:50:56:a1:19:7a:00:50:56:a1:1b:15;
VLAN = root (0)
EMS serial number: FCTEMS0000101075
Client cert SN: 37054E49E415407D06BAAD31F46B36
Public IP address: 206.47.132.124
Quarantined: no
Online status: online
Registration status: registered
On-net status: on-net
Gateway Interface: port3
FortiClient version: 7.0.0
AVDS version: 88.336
FortiClient app signature version: 18.143
FortiClient vulnerability scan engine version: 2.31
FortiClient UID: 37054E49E415407D06BAAD31F46B36
Host Name: AD-Server
OS Type: W864
OS Version: Microsoft Windows Server 2012 R2 Standard Edition, 6
4-bit (Build 9600)
Host Description:
Domain: trainingAD.training.lab
Last Login User: Administrator
Owner:
Host Model: VMware Virtual Platform
Host Manufacturer: VMware, Inc.

```



In Windows, FortiClient automatically installs certificates in the certificate store. The certificate information in the store, such as certificate UID and SN, should match the information on FortiClient EMS and FortiGate. To locate certificates on other operating systems, consult the vendor documentation.

You can use the CLI command `diagnose endpoint record list a` to verify the presence of a matching endpoint record, and information such as the client UID, client certificate SN, and EMS certificate SN on the FortiGate. If any of the information is missing or incomplete, client certificate authentication might fail because FortiClient cannot locate the corresponding endpoint entry.

This slide shows that client certificate information is synchronized with FortiGate.

## SSL Certificate-Based Authentication

- An endpoint obtains a client certificate when it registers to FortiClient EMS
- FortiClient automatically submits CSR request
- FortiClient EMS signs and returns the client certificate
- Certificate is stored in OS certificate store
- By default:
  - Client certificate authentication is enabled on access proxy
  - Empty certificate response is set to block
  - Options can be configured on CLI only

```
config firewall access-proxy
  edit <name>
    set client-cert enable
    set empty-cert-action block
  end
```

- Currently, ZTNA supports the Microsoft Edge and Google Chrome browsers

Endpoint obtains a client certificate when it registers to FortiClient EMS. FortiClient automatically submits a CSR request and the FortiClient EMS signs and returns the client certificate. This certificate is stored in the operating system certificate store for subsequent connections. The endpoint information is synchronized between FortiGate and FortiClient EMS. When an endpoint disconnects or is unregistered from FortiClient EMS, its certificate is removed from the certificate store and revokes on FortiClient EMS. The endpoint obtains a certificate again when it reconnects to the FortiClient EMS.

By default, client certificate authentication is enabled on the access proxy, so when FortiGate receives the HTTPS request, the FortiGate WAD process challenges the client to identify itself with its certificate. The FortiGate makes a decision based on specific possibilities.

If the client responds with the correct certificate that the client UID and certificate SN can be extracted from:

- If the client UID and certificate SN match the record on FortiGate, the client is allowed to continue with the ZTNA proxy rule processing.
- If the client UID and certificate SN do not match the record on FortiGate, the client is blocked from further ZTNA proxy rule processing.

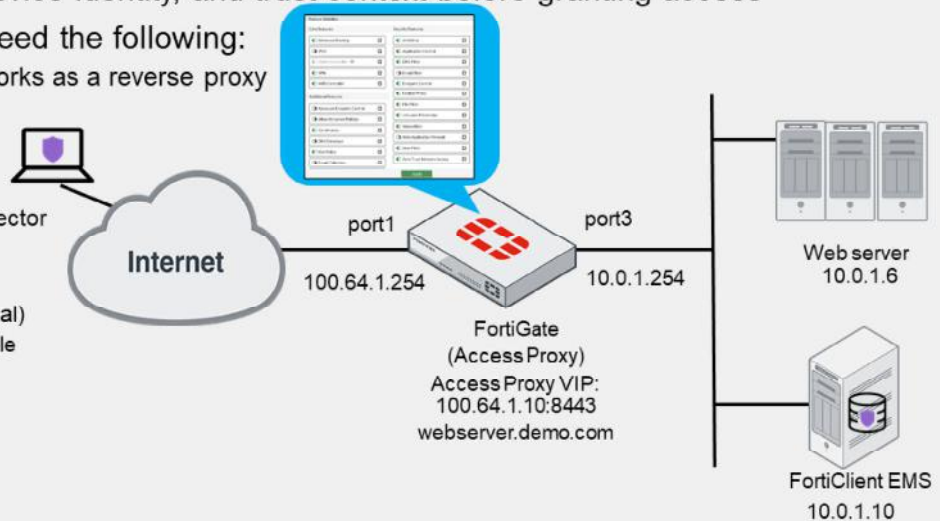
If the client cancels and responds with an empty client certificate, the client is allowed to continue with ZTNA proxy rule processing when you can set `empty-cert-action` to `accept`. If `empty-cert-action` is set to `block`, FortiGate blocks the client from further ZTNA proxy rule processing.

## ZTNA HTTPS Access Proxy

- HTTPS access proxy works as a reverse proxy
- Verifies user identity, device identity, and trust context before granting access

- To deploy ZTNA, you need the following:

- HTTPS access proxy works as a reverse proxy
- FortiClient endpoint
- FortiClient EMS
- FortiGate
  - FortiClient EMS connector
  - ZTNA server
  - ZTNA rule
  - Authentication (optional)
    - Explicit proxy enable



The FortiGate HTTPS access proxy works as a reverse proxy for the HTTP server. When a client connects to a web page hosted by the protected server, the address resolves to the FortiGate access proxy VIP (100.64.1.10:8443), as shown on this slide. FortiGate proxies the connection and takes steps to authenticate the device. It prompts the user for the endpoint certificate on the browser, and verifies this against the ZTNA endpoint record that is synchronized from the FortiClient EMS.

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

ZTNA configuration on FortiGate requires the following configuration:

- FortiClient EMS adds a fabric connector in the Security Fabric. FortiGate maintains a continuous connection to the EMS server to synchronize endpoint device information, and also automatically synchronizes ZTNA tags. You can create groups and add tags to use in the ZTNA rules and firewall policies.
- The ZTNA server defines the access proxy VIP and the real servers that clients connect to. You can also enable authentication.
- A ZTNA rule is a proxy policy used to enforce access control. You can define ZTNA tags or tag groups to enforce zero-trust role-based access. You can configure security profiles to protect this traffic.

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

DO NOT REPRINT  
© FORTINET

## ZTNA HTTPS Access Proxy (Contd)

- ZTNA server

Policy & Objects > ZTNA > ZTNA Servers

ZTNA Rules ZTNA Servers ZTNA Tags

+ Create New Edit Delete Search

Name: ZTNA-webserver

Comments:

Network:

Service: HTTPS

External interface: 10.0.1.250

External port: 9443

Services and Servers:

Default certificate: Fortinet\_SSL

Service/Server mapping:

Service: 0

Server: 0

HTTPS: www.example2.com/hapi

Virtual Host:

Match by: Any Host Specify

Host: www.example2.com

Use certificate: Fortinet\_CA\_SSL

Match path by: Substring Wildcard Regular Expression

Path: /hapi

Servers:

IP	Port	Status
10.0.1.250	443	Active

IP: 10.0.1.250

Port: 443

Status: Active Standby Disable

Virtual host matching rules

Real server IP address and port

- ZTNA rule

Policy & Objects > ZTNA > ZTNA Rules

ZTNA Rules ZTNA Servers ZTNA Tags

+ Create New Edit Delete Search

Name: ZTNA-Deny-Malicious

Source: all

ZTNA Tag: Remote-Endpoint

ZTNA Server: ZTNA-webserver

Action: ACCEPT DENY

Security Profiles:

AntiVirus:

WebFilter:

VirusFilter:

Application Control:

IPS:

File Filter:

SSL Inspection:

Logging Options:

Log Allowed Traffic:  Security Events:

Denying access based on malicious tag

FORTINET  
Training Institute

© Fortinet Inc. All Rights Reserved.

16

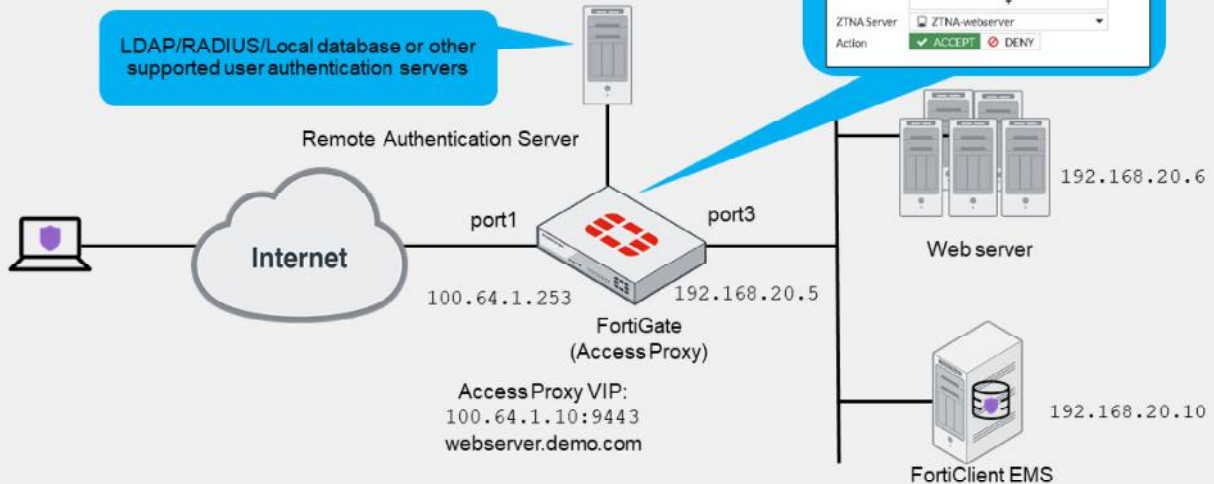
After you configure FortiClient EMS as the fabric connector and you sync ZTNA tags with FortiGate, you must create a ZTNA server or access proxy. The access proxy VIP is the FortiGate ZTNA gateway that clients make HTTPS connections to. The service and server mappings define the virtual host matching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

A ZTNA rule is a proxy policy used to enforce access control. You can define ZTNA tags or tag groups to enforce zero-trust role-based access. To create a rule, type a rule name, and add IP addresses and ZTNA tags or tag groups that are allowed or blocked access. You also select the ZTNA server as the destination. You can also apply security profiles to protect this traffic.

Note that UTM processing of the traffic happens at the ZTNA rule.

## ZTNA HTTPS Access Proxy With Basic Authentication

- You can add authentication to the access proxy
- Requires authentication scheme and authentication rule
  - To authenticate proxy-based policies



You can add authentication to the access proxy, which requires you to configure an authentication scheme and authentication rule on the FortiGate CLI. You use authentication schemes and authentication rules to authenticate proxy-based policies, similar to configuring authentication for explicit and transparent proxy.

The authentication scheme defines the method of authentication that is applied. ZTNA supports basic HTTP and SAML methods. Each method has additional settings to define the data source. For example, with basic HTTP authentication, a user database can reference an LDAP server, RADIUS server, local database, or other supported authentication servers that the user is authenticated against.

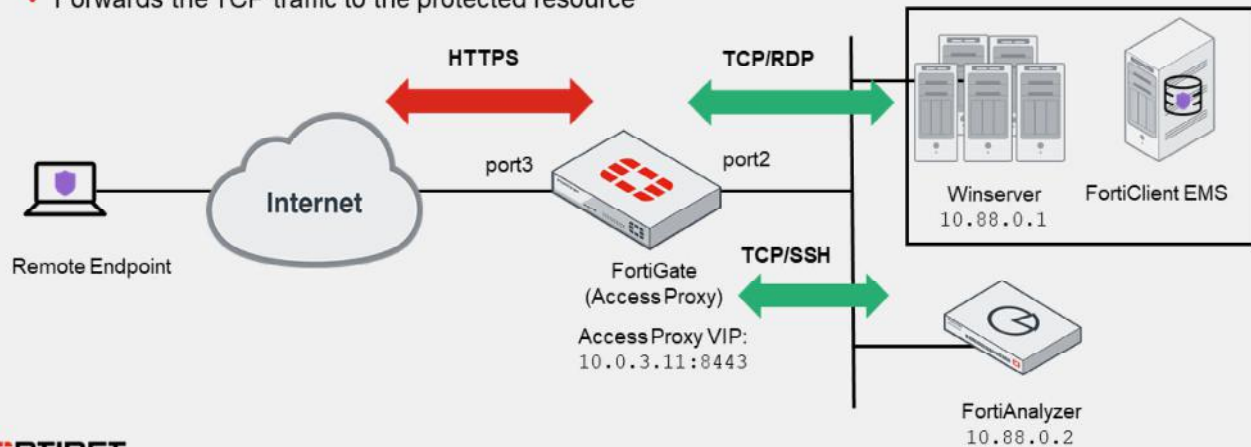
The authentication rule defines the proxy sources and destinations that require authentication, and which authentication scheme to apply. ZTNA supports the active authentication method. The active authentication method references a scheme where users are actively prompted for authentication, as they are with basic authentication. After the authentication rule triggers the method to authenticate the user, a successful authentication returns the groups that the user belongs to.

In the ZTNA rule and proxy policy, you can define a user or user group as the allowed source. Only users that match that user or group are allowed through the proxy policy. This slide shows the ZTNA rule example that user group **ZTNAAccess\_group** was added to the authentication configuration after the authentication scheme and authentication rule were added to FortiGate.

DO NOT REPRINT  
© FORTINET

## ZTNA TCP Forwarding Access Proxy

- TCP forwarding access proxy demonstrates an HTTPS reverse proxy that forwards TCP traffic to the resource
- TCP forwarding access proxy:
  - Tunnels TCP traffic between the client and FortiGate over HTTPS
  - Forwards the TCP traffic to the protected resource



**FORTINET**  
Training Institute

© Fortinet Inc. All Rights Reserved.

18

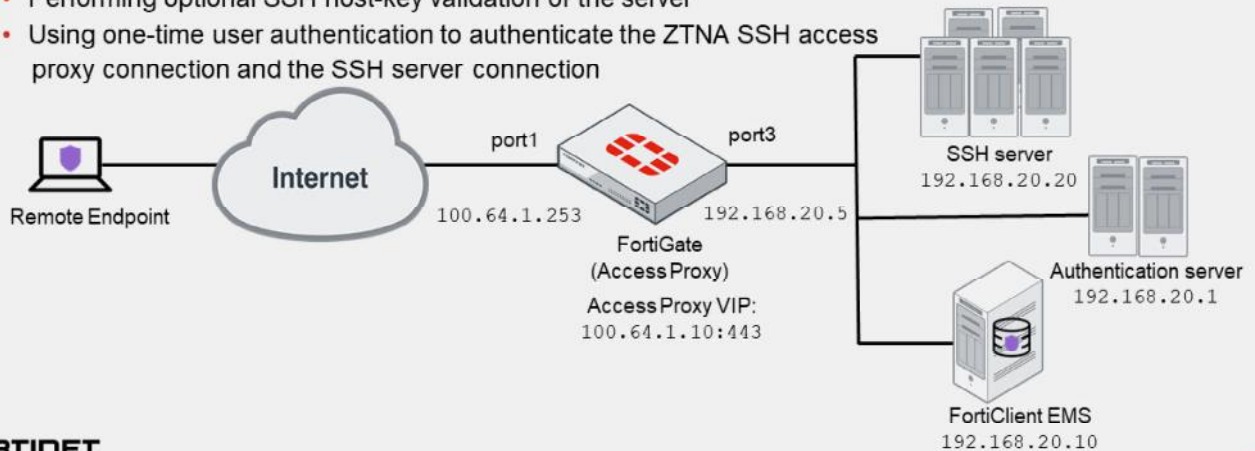
In the example shown on this slide, a TCP forwarding access proxy (TFAP) is configured to demonstrate an HTTPS reverse proxy that forwards TCP traffic to the designated resource. The access proxy tunnels TCP traffic between the client and FortiGate over HTTPS, and forwards the TCP traffic to the protected resource. It verifies user identity, device identity, and trust context, before granting access to the protected source.

RDP access is configured to Winserver, and SSH access to FortiAnalyzer. The topology shown on this slide uses IP address 10.0.3.11 and port-8443 for the external access proxy VIP.

You can also add authentication and a security posture check for TCP Forwarding Access Proxy, which you learned about earlier in this lesson.

## ZTNA SSH Access Proxy

- ZTNA supports SSH access proxy to provide seamless SSH connection
- Advantages over TCP forwarding access proxy:
  - Establishing device trust context with user identity and device identity checks
  - Applying SSH deep inspection to the traffic through the SSH related profile
  - Performing optional SSH host-key validation of the server
  - Using one-time user authentication to authenticate the ZTNA SSH access proxy connection and the SSH server connection



You can configure ZTNA with an SSH access proxy to provide a seamless SSH connection to the server.

Advantages of using an SSH access proxy instead of a TCP forwarding access proxy include:

- Establishing device trust context with user identity and device identity checks
- Applying SSH deep inspection to the traffic through the SSH related profile
- Performing optional SSH host-key validation of the server
- Using one-time user authentication to authenticate the ZTNA SSH access proxy connection and the SSH server connection

To act as a reverse proxy for the SSH server, FortiGate must perform SSH host-key validation to verify the identity of the SSH server. FortiGate does this by storing the public key of the SSH server in its SSH host-key configurations. When endpoint makes a connection to the SSH server, if the public key matches one that is used by the server, then the connection is established. If there is no match, then the connection fails.

**DO NOT REPRINT**  
**© FORTINET**

## ZTNA IP/MAC-Based Access Control

- ZTNA IP/MAC-based access control enhances security when endpoints are physically on the corporate network
  - Use ZTNA tags to control access
- IP/MAC-based access control focuses on access for remote users
- This mode does not require the use of the access proxy, and only uses ZTNA tags for access control

**ZTNA IP/MAC-based firewall policy**

Name	Block-Malicious
Incoming Interface	port3
Outgoing Interface	port1
Source	all
IP/MAC Based Access Control	FCTEMS_ALL_FORTICLOUD_SEF
Destination	all
Schedule	always
Service	ALL
Action	ACCEPT DENY
<input checked="" type="checkbox"/> Log Violation Traffic	
Comments	Write a comment... 0/1023
Enable this policy <input checked="" type="checkbox"/>	

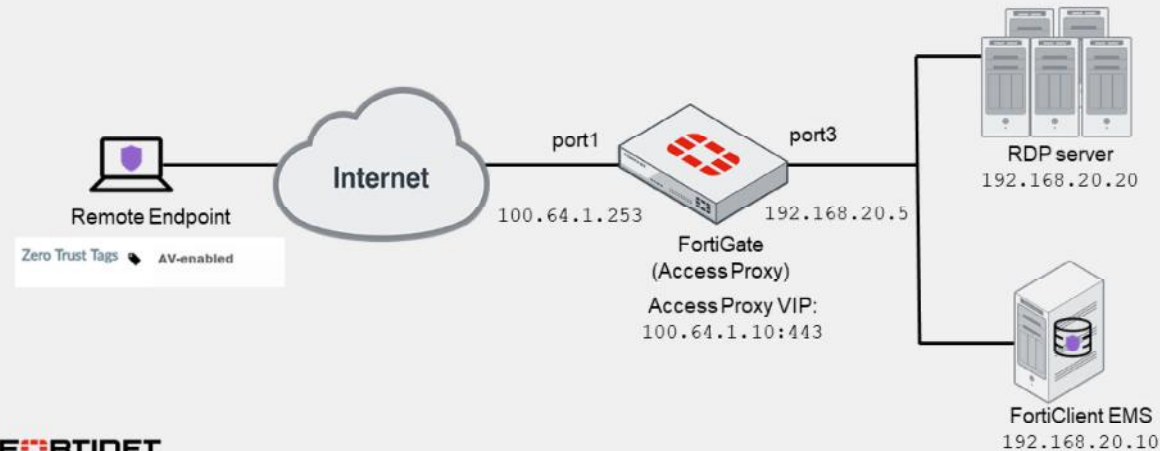
ZTNA IP/MAC-based access control enhances security when endpoints are physically located on the corporate network, whereas ZTNA access proxy focuses on access for remote users. IP/MAC-based access control combines IP/MAC with ZTNA tags for identification and security posture check, to implement role-based zero-trust access. Firewall policies are configured that use ZTNA tags to control access between on-net devices and an internal webserver. This mode does not require the use of the access proxy, and only uses ZTNA tags for access control.

The example firewall policy on this slide uses the existing tag to control access. Traffic is denied to the internet when the FortiClient endpoint is tagged with **FCTEMS\_ALL\_FORTICLOUD\_Malicious**.

DO NOT REPRINT  
© FORTINET

## Posture Check Verification for Active ZTNA Session

- Endpoint posture changes trigger active ZTNA proxy sessions to be re-verified
  - Terminates session if the endpoint is no longer compliant with the ZTNA policy
- FortiGate monitors changes to the endpoint tags, when FortiGate detects change:
  - The endpoint's active session must reevaluate again to match the ZTNA policy before a data can pass



**FORTINET**  
Training Institute

© Fortinet Inc. All Rights Reserved.

21

Endpoint posture changes trigger active ZTNA proxy sessions to be re-verified and terminated if the endpoint is no longer compliant with the ZTNA policy. The FortiGate monitors changes to the endpoint tags that are updated by FortiClient EMS. When a change is detected, the endpoint's active ZTNA sessions must match the ZTNA policy again before data can pass.

Note that changes to the ZTNA policy, such as changing the ZTNA tag matching logic, will also trigger re-verification of the client device against the policy.

In the example on this slide, a ZTNA rule is configured to allow access for endpoints that have the *AV-enabled* tag. After an RDP sessions is established, Windows antivirus is disabled on the remote endpoint. The FortiGate re-verifies the session and the active RDP session is removed from the FortiGate session table, causing the RDP session to be disconnected.

**DO NOT REPRINT**  
**© FORTINET**


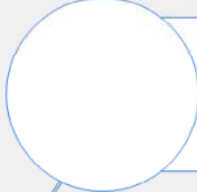
## Knowledge Check

1. Which component issues and signs the client certificate?
  - ✓ A. FortiClient EMS
  - B. FortiClient
  
2. Which internet browser supports Fortinet ZTNA?
  - A. Firefox
  - ✓ B. Chrome

DO NOT REPRINT  
© FORTINET

## Lesson Progress

The diagram shows a vertical sequence of two steps. The first step, 'ZTNA Introduction', is marked as completed with a green checkmark icon. The second step, 'Comparing ZTNA to SSL and IPSec VPN', is marked as pending with an empty circle icon. A vertical line connects the two circles, and horizontal lines extend from each circle to its respective text box.

-  ZTNA Introduction
-  Comparing ZTNA to SSL and IPSec VPN

**FORTINET**  
Training Institute

© Fortinet Inc. All Rights Reserved.

23

Good job! You now understand key ZTNA concepts and how to configure ZTNA

Now, you will compare ZTNA to SSL and IPsec VPN.

DO NOT REPRINT  
© FORTINET

## Comparing ZTNA to SSL and IPsec VPN

### Objectives

- Describe the differences between SSL VPN, IPsec VPN, and ZTNA access
- Understand the evolution of teleworker remote access with ZTNA

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

By demonstrating competence in understanding the evolution of remote access with ZTNA, you will be able to migrate from VPN to ZTNA HTTPS access proxy.

## Comparing SSL VPN, IPsec VPN, and ZTNA Access

	IPsec VPN	SSL VPN	ZTNA
<b>Tunnel type:</b>	IPsec tunnel only	Session-based OR tunnel	Session-based only
<b>Configured between:</b>	FortiClient and FortiGate FortiGate and FortiGate FortiGate and compatible third-party IPsec VPN gateway FortiGate and compatible third-party IPsec VPN clients	Browser and FortiGate FortiClient and FortiGate FortiGate (SSL Client) and FortiGate (SSL Server)	Browser and FortiGate FortiClient and FortiGate (TCP forwarding access)
<b>Log in through:</b>	IPsec client	HTTPS web page on FortiGate FortiClient FortiGate (SSL Client)	HTTPS hostname or IP and port number  FortiClient (TCP forwarding access)

How are SSL VPN and ZTNA access different from IPsec VPNs?

SSL and TLS are commonly used to encapsulate and secure e-commerce and online banking on the internet (HTTP). SSL VPNs and ZTNA use a similar technique, and support non-HTTP protocol encapsulation as well. SSL resides higher up on the network stack than IP and, therefore, it usually requires more bits—more bandwidth—for SSL VPN headers. In comparison, IPsec uses some different methods to provide confidentiality and integrity. The primary protocol used in IPsec is ESP, which encapsulates and encrypts UDP, RDP, HTTP, or other protocols inside the IPsec tunnel.

IPsec is also an industry-standard protocol that can work with multiple vendors and supports peers that are devices and gateways—not just user clients with FortiGate only, like SSL VPN or ZTNA does.

The client software is also different. In an SSL VPN or ZTNA, your web browser might be the only client software you need. You can go to the FortiGate SSL VPN portal (an HTTPS web page) and then log in. Alternatively, you can install FortiClient or configure FortiGate as an SSL VPN client. In comparison, to use IPsec VPN, install special client software or have a local gateway, such as a desktop model FortiGate, to connect to the remote gateway. You might also need to configure firewalls between VPN peers to allow IPsec protocols.

## Comparing SSL VPN, IPsec VPN, and ZTNA Access (Contd)

	IPsec VPN	SSL VPN	ZTNA
<b>Category:</b>	Industry standard	Vendor specific	Vendor specific
<b>Ease of use (Configuration):</b>	<ul style="list-style-type: none"> <li>Requires installation</li> <li>Flexible setup               <ul style="list-style-type: none"> <li>Mesh and star topologies</li> <li>For clients or peer gateways</li> </ul> </li> <li>Performance based: IPsec cryptography is faster in FortiOS</li> </ul>	<ul style="list-style-type: none"> <li>Does not require installation</li> <li>Simpler setup               <ul style="list-style-type: none"> <li>Client-to-FortiGate</li> <li>FortiGate-to-FortiGate</li> <li>No user-configured settings</li> </ul> </li> <li>Technical support less requested</li> </ul>	<ul style="list-style-type: none"> <li>Does not require installation</li> <li>Simpler setup               <ul style="list-style-type: none"> <li>Only client-to-FortiGate</li> </ul> </li> <li>No user-configured settings</li> <li>Technical support less requested</li> </ul>
<b>Better for:</b>	Office-to-office traffic Data centers	Provides flexibility tunnel-mode or session-based access	Session-based access only
<b>Attack surface protection</b>	<ul style="list-style-type: none"> <li>Traditional perimeter protection:               <ul style="list-style-type: none"> <li>Defends against external threats only</li> <li>Doesn't address threat inside the network</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>Traditional perimeter protection:               <ul style="list-style-type: none"> <li>Defends against external threats only</li> <li>Doesn't address threat inside the network</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>zero-trust philosophy               <ul style="list-style-type: none"> <li>No one inside or outside should be trusted</li> <li>Based on identity authentication</li> </ul> </li> </ul>

After you log in, the SSL VPN connects your computer to your private network. No user-configured settings are required, and firewalls are typically configured to allow outgoing HTTP, so technical support calls are less likely. Simplicity makes ZTNA and SSL VPN ideal for non-technical users, or users who connect from public computers, such as those found in public libraries and internet cafés. ZTNA takes this a step further and makes it easier for administrators to perform device compliance checks and configuration. ZTNA also provides an additional authentication mechanism for access control without any interaction required from the end user.

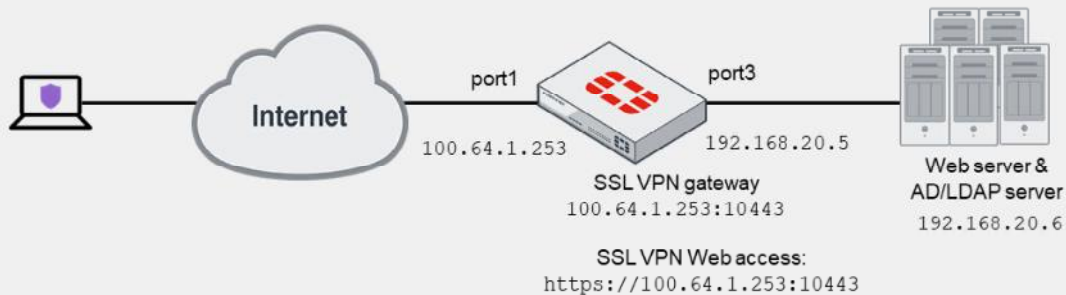
ZTNA follows the zero-trust philosophy to protect the attack surface that states no one inside or outside the network should be trusted unless their identification has been thoroughly checked. zero-trust also assumes that every attempt to access the network or an application is a threat.

Both IPsec and SSL VPN are traditional perimeter-based security approach that only distrusts factors outside the existing network and fail to address threats that already exist within the network.

# DO NOT REPRINT © FORTINET

## Moving to ZTNA From SSL VPN

- You can migrate teleworking configurations that use SSL VPN tunnel or web portal mode access to ZTNA with HTTPS access proxy



You can use ZTNA to replace VPN-based teleworking solutions. The example on this slide shows that you can migrate teleworking configurations that use SSL VPN tunnel or web portal mode access to ZTNA with HTTPS access proxy, and continue to use the same authentication server and groups to authenticate your remote users.

In addition, by integrating with FortiClient EMS, you can also ensure that FortiGate performs device identification is using client certificates, and checks the security posture before allowing the remote user into the website. This provides granular control over who can access the web resource using role-based access control. It also gives the user transparent access to the website using only their browser. You can even configure ZTNA IP/MAC filtering mode for on-fabric devices to provide similar access control while users are on the network.

DO NOT REPRINT  
© FORTINET

## Knowledge Check

1. Which remote access solution proxies HTTP and TCP over a secure HTTPS connection?  
✓ A. ZTNA  
B. IPSec
  
2. What does FortiClient EMS integration ensure?  
✓ A. Device identification  
B. User identification

**DO NOT REPRINT**  
**© FORTINET**

## Lesson Progress



ZTNA Introduction



Comparing ZTNA to SSL and IPSec  
VPN

Congratulations! You have completed this lesson.

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

**DO NOT REPRINT  
© FORTINET**

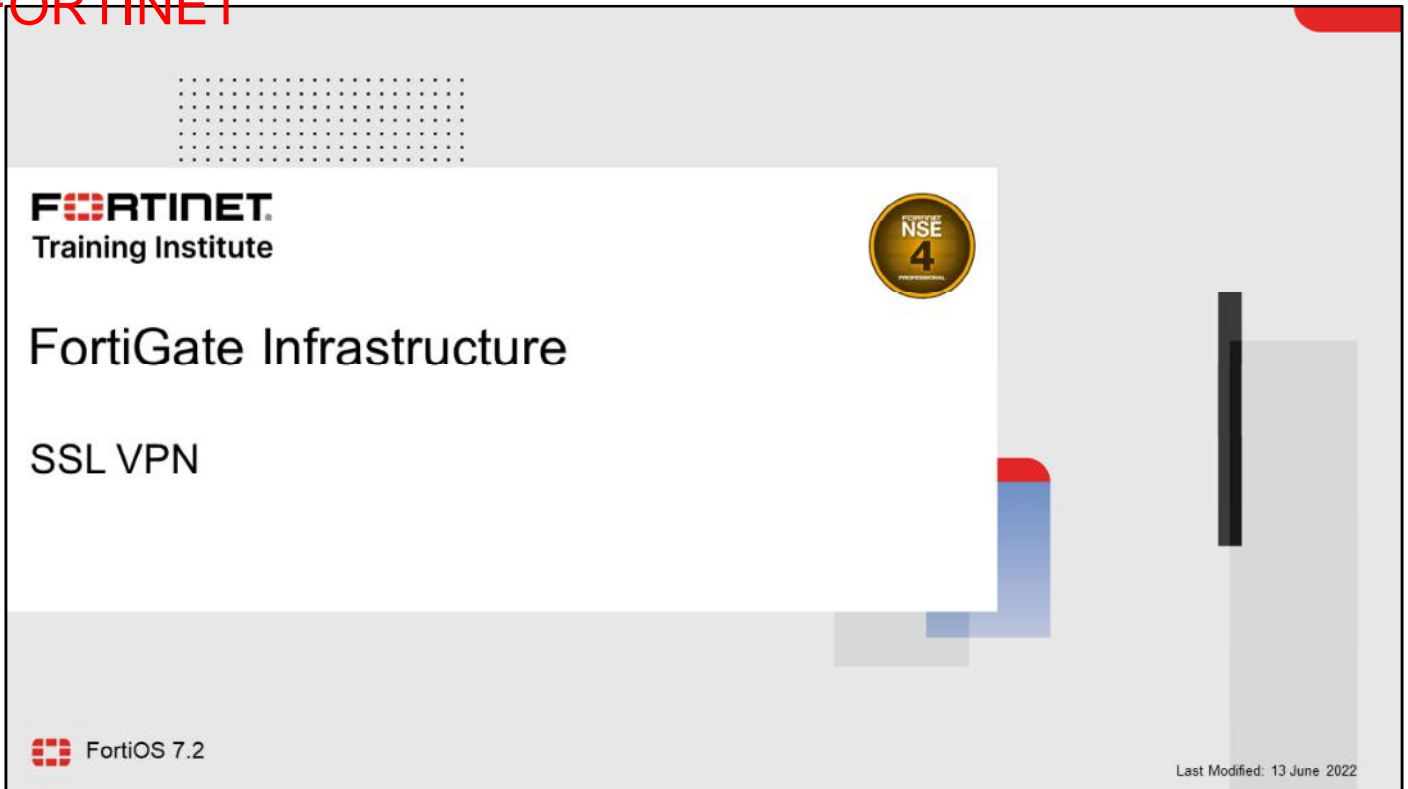
## Review

- ✓ Understand the benefits and fundamentals of ZTNA
- ✓ Understand how to establish device identity and trust
- ✓ Understand SSL certificate-based authentication
- ✓ Configure ZTNA access on FortiOS
- ✓ Describe types of ZTNA configuration

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

By mastering the objectives covered in this lesson, you learned about how to configure and use ZTNA.

DO NOT REPRINT  
© FORTINET



The slide features a white background with a grid of dots in the top left corner. The Fortinet logo and 'Training Institute' text are in the top left. A gold NSE 4 Professional badge is in the top right. The main title 'FortiGate Infrastructure' and subtitle 'SSL VPN' are centered. The FortiOS 7.2 logo is in the bottom left, and the date 'Last Modified: 13 June 2022' is in the bottom right. The slide is framed by a grey border with a red corner in the top right.

**FORTINET**  
Training Institute

NSE  
4  
PROFESSIONAL

FortiGate Infrastructure

SSL VPN

FortiOS 7.2

Last Modified: 13 June 2022

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**

## Lesson Overview

- 1 SSL VPN Deployment Modes
- 2 Configuring SSL VPNs
- 3 Monitoring and Troubleshooting

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

DO NOT REPRINT  
© FORTINET

## SSL VPN Deployment Modes

### Objectives

- Describe the differences between SSL VPN modes

After completing this section, you should be able to achieve the objective 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 of your SSL VPN.

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

VPN > SSL VPN Portals

Edit SSL-VPN Portal

Name: full-access

Limit Users to One SSL-VPN Connection at a Time:

Tunnel Mode

Tunnel Mode Client Options

Allow client to save password:

Allow client to connect automatically:

Allow client to keep connections alive:

DNS Split Tunneling:

Restrict to Specific OS Versions

Web Mode

```
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.

4

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?

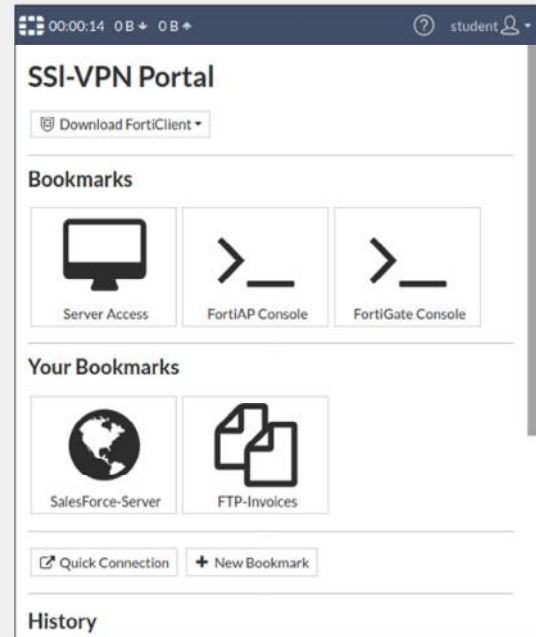
It depends on which applications you need to send through the VPN, the technical knowledge of your users, and whether or not you have administrative permissions on their computers.

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.

## Web Mode

- Connect to the FortiGate SSL VPN portal from any browser
  - The web portal displays the status of SSL VPN
  - The SSL VPN stays up only while the SSL VPN portal page is open
- Access internal network resources easily using:
  - Bookmarks
  - Quick connection
- Disadvantages:
  - Interaction with the internal network exclusively by browser
    - Through the SSL VPN portal
    - External network applications cannot send data across the VPN
  - Limited number of protocols supported



Web mode is the simplest SSL VPN mode.

Like you would with any other HTTPS website, you simply log in to the SSL VPN portal web page on FortiGate. It acts like a server-side reverse proxy, or a simple secure HTTP/HTTPS gateway, that connects you with the applications on the private network.

The **Bookmarks** section on the **SSL VPN Portal** page contains links to all or some of the resources available for the user to access. The **Quick Connection** widget allows users to type the URL or IP address of the server they want to reach. A web SSL VPN user makes use of these two widgets to access the internal network. The main advantage of web mode is that it does not usually require you to install extra software.

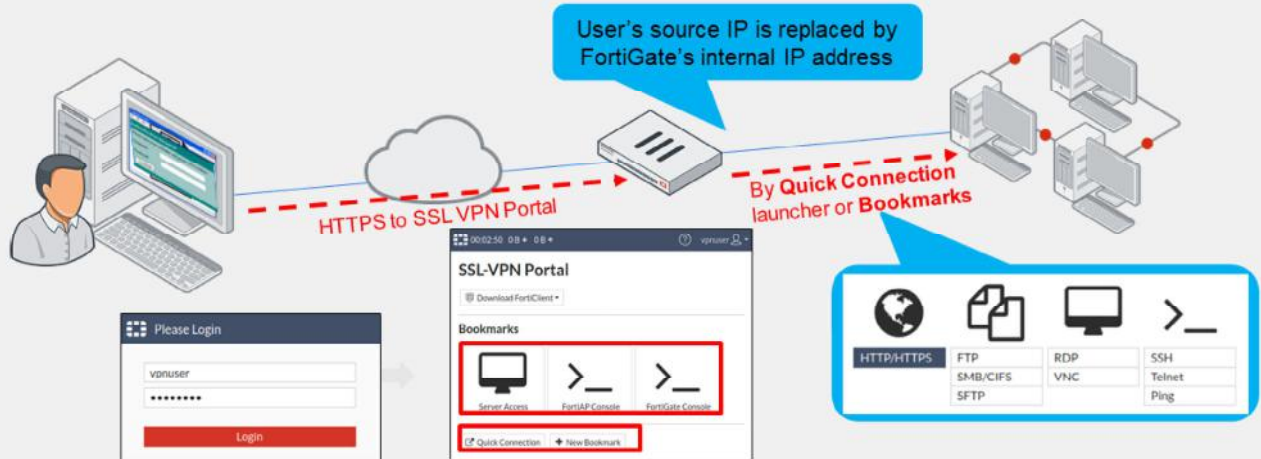
Web mode has two main disadvantages:

- All interaction with the internal network must be done using the browser exclusively (through the web portal). External network applications running on the user's PC cannot send data across the VPN.
- This a secure HTTP/HTTPS gateway mechanism that doesn't work for accessing everything, but just few popular protocols, such as HTTP, FTP, and Windows shares.

# DO NOT REPRINT © FORTINET

## Web Mode (Contd)

1. Remote users connect to the SSL VPN portal—HTTPS web page on FortiGate
2. Users authenticate
3. Users access resources through the **Quick Connection** launcher or **Bookmarks**



**FORTINET**  
Training Institute

© Fortinet Inc. All Rights Reserved.

6

How does web mode work?

1. Remote users establish a secure connection between the SSL security in the web browser and the FortiGate SSL VPN portal, using HTTPS.
2. Once connected, users provide credentials in order to pass an authentication check.
3. Then, FortiGate displays the SSL VPN portal that contains services and network resources for users to access.

Different users can have different portals with different resources and access permissions. Also notice the source IP seen by the remote resources is FortiGate's internal IP address and not the user's IP address.

# 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
- Advantage:
  - Any IP network application on the client can send traffic through the tunnel
- Disadvantage:
  - Requires the installation of a VPN client  
<http://www.forticlient.com/>



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 over web mode is that after the VPN is established, any IP network application running on the client can send traffic through the tunnel. The main disadvantage is that 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.

8

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 (`fortissl`). 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.

## Tunnel Mode—FortiGate as Client

- Connect to server FortiGate device as SSL VPN client
  - Use *SSL VPN Tunnel* interface type
  - Devices connect to client FortiGate device 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 device from a pool of reserved addresses
- Advantage:
  - Any IP network application on the user machines connect 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.
- Disadvantage:
  - Requires proper CA certificate on SSL VPN Server FortiGate
  - SSL VPN Client FortiGate user uses PSK and PKI client certificate to authenticate

The FortiGate can be configured 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 are returned by the SSL VPN server. Policies can be defined to allow users that are behind the client to be tunneled through SSL VPN to destinations on the SSL VPN server.

This setup provides IP-level connectivity in tunnel mode and allows hub-and-spoke topologies to be configured with FortiGates 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 route's distance or priority according to your requirements. To avoid a default route being learned on the SSL VPN client, on the SSL VPN server define a specific destination. Split tunneling is used so that only the destination addresses defined in the server's firewall policies are routed to the server, and all other traffic is connected directly to the internet.

This configuration requires proper CA certificate installation as the SSL VPN client FortiGate/user uses PSK and a PKI client certificate to authenticate. The FortiGate devices must have the proper CA certificate installed to verify the certificate chain to the root CA that signed the certificate.

## 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)



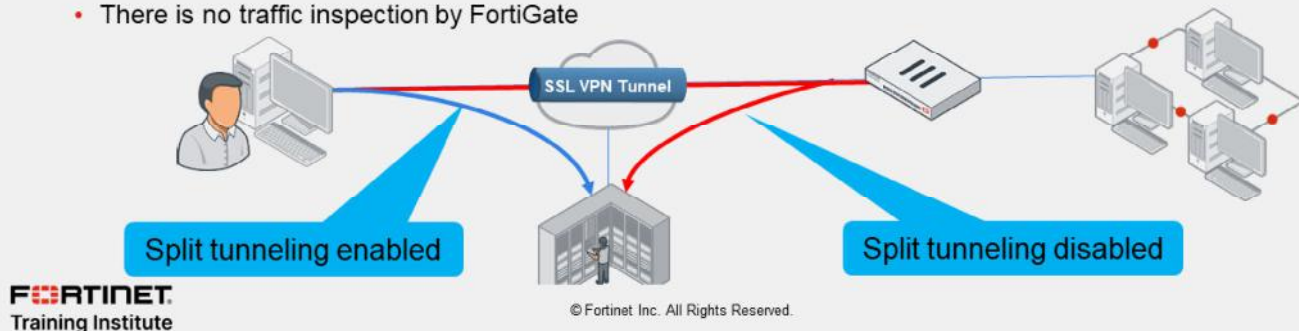
How does tunnel mode work when FortiGate is configured as client?

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.

## 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



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**

## Knowledge Check

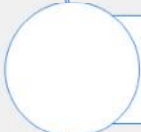
1. A web-mode SSL VPN user connects to a remote web server. What is the source IP address of the HTTP request the web server receives?
  - A. The remote user IP address
  - ✓ B. The FortiGate device internal IP address
2. Which statement about tunnel-mode SSL VPN is correct?
  - ✓ A. It supports split tunneling.
  - B. It requires bookmarks.
3. A web-mode SSL VPN user uses \_\_\_\_\_ to access internal network resources.
  - ✓ A. bookmarks
  - B. FortiClient

**DO NOT REPRINT**  
**© FORTINET**

## Lesson Progress



**SSL VPN Deployment Modes**



**Configuring SSL VPNs**



**Monitoring and Troubleshooting**

Good job! You now understand the SSL VPN operation modes supported by FortiGate.

Now, you will learn about how to configure SSL VPNs.

DO NOT REPRINT  
© FORTINET

## Configuring SSL VPNs

### Objectives

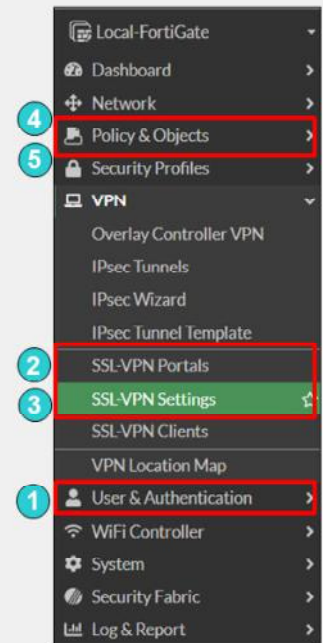
- Define authentication for SSL VPN users
- Configure SSL VPN portals
- Configure SSL VPN settings
- Define firewall policies for SSL VPNs
- Configure client integrity check

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

By demonstrating competence in configuring the SSL VPN settings on FortiGate, you will be able to better design the architecture of your SSL VPN tunnels.

## 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
    - FortiGate can be used to apply security profiles



To configure SSL VPN, you must take these steps:

1. Configure user accounts and groups.
2. Configure the SSL VPN portal.
3. Configure SSL VPN settings.
4. Create a firewall policy to accept and decrypt packets. This policy is also used to provide access to internal networks.
5. Optionally, configure a firewall policy to allow traffic from the SSL VPN client to the internet and apply security profiles. User traffic will go to the internet through FortiGate, where you can monitor or restrict client access to the internet.

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

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

Some steps can be configured in a different order than what is shown on this slide.

## 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**

Split tunneling:  Enabled Based on Policy Destination

**Web Mode**

Portal Message: SSL VPN Portal

Theme: NewAdmin

**Administrator-defined bookmarks**

Name #	Type #	Location #	Description #
FortiAP Console	TELNET	10.0.1.2	Road AP / Mesh-1

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 whereas **Enabled for Trusted Destination** allows client traffic that does not match the explicitly trusted destination.

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.

## Configure SSL VPN Settings

### VPN > 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.

## Configure SSL VPN Settings (Contd)

- Define the IP range for the SSL VPN
  - IPs are assigned to clients' virtual adapters while joined to VPN
  - IP allocation has two methods:
    - First-available (default) or Round robin
    - CLI only

```
conf vpn ssl settings
  set tunnel-addr-assigned-method first-available/round-robin
end
```

- 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
    - It cannot be deleted



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. There are two IP allocation methods and only available in CLI as shown in the slide:

- First-available (default setting)
- Round robin

Please note when round-robin is used, address pools defined in web portal is ignored, and the `tunnel-ip-pools` or `tunnel-ipv6-pools` under `ssl vpn` setting must be set. Only one set of IP pool address is allowed.

DNS server resolution is effective only when the DNS traffic is sent over the VPN tunnel. Generally, this will be the case only when split tunnel mode is disabled and all traffic is being 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 web portal. Accountants can use FortiClient to connect in tunnel mode.

# 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 Accountants SSL_VPN_USERS Teachers
Destination	LOCAL_SUBNET
Schedule	always
Service	ALL
Action	ACCEPT DENY

Add the user/groups for SSL VPN authentication.

Otherwise, users will be denied permission

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`.

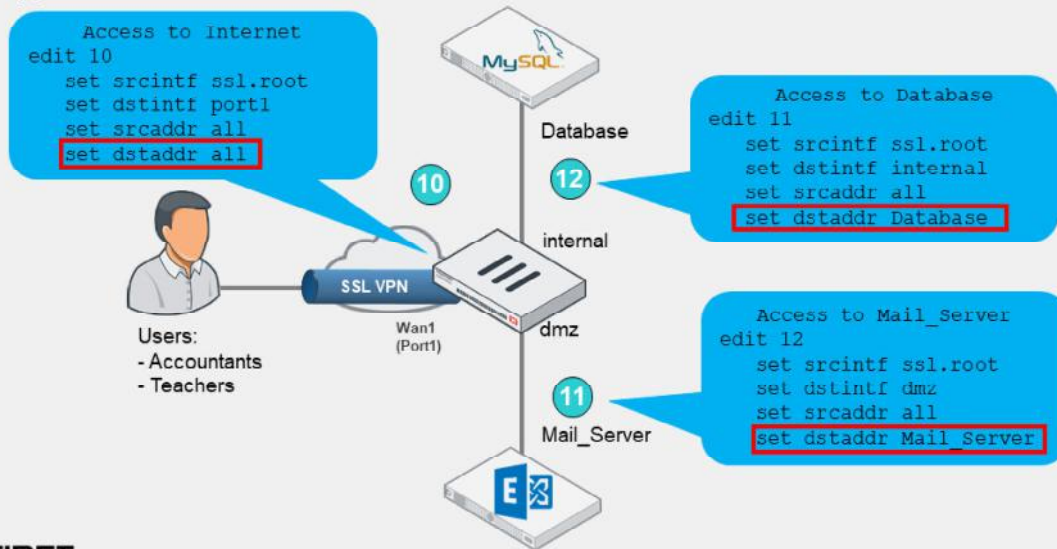
To activate and successfully log in to the SSL VPN, there must be a firewall policy from the SSL VPN interface to the interface to which you want to allow access for the SSL VPN users, including all of the users and groups that can log in as the source. Without a policy like this, no login portal is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

20

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

1. 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
2. Configure SSL VPN portals
3. Configure SSL VPN settings
  - Authentication rules include both accounts using CLI
4. Create a firewall policy to and from the SSL VPN interface
5. Create a firewall policy to allow SSL VPN traffic to the internet (optional)

#### User & Authentication > User Definition

#### User & Authentication > PKI

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

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

To configure SSL VPN, you must take these steps:

SSL VPN server FortiGate:

1. Set up user accounts and groups for remote SSL VPN users.
  - Create two accounts: local/remote and PKI. The PKI menu is only available in the GUI after a PKI user has been created using the CLI, and a CN can only be configured in the CLI. If no CN is specified, then any certificate that is signed by the CA will be valid and matched.
  - Require clients to authenticate using their certificates as well as username and password.
2. Configure SSL VPN portals.
3. Configure SSL VPN settings.
  - Authentication rules include both accounts using CLI.
4. Create a firewall policy to and from the SSL VPN interface.
5. Create a firewall policy to allow SSL VPN traffic to the internet (optional).

## Configuring SSL VPN—FortiGate as Client

### • SSL VPN Client FortiGate

1. Create PKI user
  - Select CA certificate that allows the FortiGate to complete the certificate chain and verify the server's certificate
2. Create SSL VPN tunnel interface using `ssl.<vdom_name>` 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

**Network > Interface > Create New**

- Name: sslclient\_port (Interface Name)
- Type: SSL-VPN Tunnel (Type: ssl.<vdom\_name>)
- Interface: port4 (Select port to reach server FortiGate)
- Administrative Access:
  - IPv4:  HTTPS,  PING,  SSH,  SNMP
  - RADIUS Accounting,  Security Fabric Connection

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

- Client Name: SSLClienttoHQ
- Virtual SSL interface: sslclient\_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: Username: clientfortigate, Pre-shared Key: [redacted], Client Certificate: [redacted], Peer: pki
- Dynamic route priority and distance settings: Administrative Distance: 10, Priority: 0, Status: Enabled

FORTINET Training Institute © Fortinet Inc. All Rights Reserved. 22

To configure SSL VPN, you must take these steps:  
SSL VPN Client FortiGate:

1. Create PKI user:
  - Set the same CN using CLI if PKI user on server FortiGate has CN configured.
  - Select CA certificate that allows the FortiGate to complete the certificate chain and verify the server's certificate.
2. Create SSL VPN tunnel interface using `ssl.<vdom_name>` interface.
3. Create and configure the SSL VPN client settings on **VPN > SSL-VPN Clients**, it includes:
  - Client name
  - Virtual SSL VPN interface
  - SSL VPN server FortiGate IP address and SSL port number
  - Local username and password and PKI(Peer) user. The **Client Certificate** is the local certificate that is used to identify this client, and is assumed to already be installed on the FortiGate. The SSL VPN server requires it for authentication.
  - When split tunnel is disabled, new default route is added and priority and distance plays an important role.
4. Create a firewall policy to allow traffic from internal interface to the SSL VPN interface.

## Client Integrity Checking

- SSL-VPN gateway checks client integrity
  - Requires Microsoft Windows
  - Supported in SSL VPN tunnel mode only
- Detects client security applications recognized by the Windows Security Center
  - Antivirus and firewall software
  - Security attributes recorded on the client's computer
- Checks the status of applications through their globally unique identifier (GUID)
  - Custom host checks
- Determines the state of the applications
  - Active/inactive
  - Current version number
  - Signature updates



When a user connects to your network through an SSL-VPN, a portal is established between your network and the user's PC. The VPN session is secured natively in two ways: the connection is encrypted and the user must log in with their credentials, such as a username and password. However, you can configure additional checks to increase the security of the connection.

One method of increasing your security is by using client integrity checking. Client integrity ensures that the connecting computer is secure by checking whether specific security software, such as antivirus or firewall software, is installed and running. This feature supports only Microsoft Windows clients, because it accesses the Windows Security Center to perform its checks. Alternatively, you can customize this feature to check the status of other applications using their GUIDs. A GUID is a unique ID in the Windows Configuration Registry that identifies each Windows application. Client integrity can also check the current software and signature versions for the antivirus and firewall applications.

Client integrity checking is applicable to tunnel mode only.

## Configure the Client Integrity Check

- Uses external vendor software to ensure client integrity:  
FortiClient, AVG, CA, F-Secure, Kaspersky, McAfee, Norton, Symantec, Panda, Sophos, Trend-Micro, Zone Alarm,...
- Checks whether the software is installed on host client:
  - Configure through CLI or GUI
  - Software must be updated and recognized by Windows Security Center
    - None – No host checking
    - av – Verify if there is any antivirus software
    - fw – Verify if there is any firewall software
    - av-fw – Verify if there is both antivirus and firewall software
    - Custom – Verify custom or proprietary software
  - If the software is not installed, FortiGate rejects SSL-VPN connection attempt

```
config vpn ssl web host-check-software
show
```

### VPN > SSL-VPN Portals > portal-name

Host Check

Type **Realtime AntiVirus** Firewall Enable both

Restrict to specific OS versions

```
config vpn ssl web portal
edit <portal_name>
set host-check [none|av|fw|av-fw|custom]
set host-check-interval <seconds>
end
```

Administrators should have in-depth knowledge of the Windows OS to use and maintain this feature

FortiGate performs the client integrity check while the VPN is still establishing, just after user authentication has finished. If the required software is not running on the user's PC, FortiGate rejects the VPN connection attempt, even with valid user credentials. You enable client integrity for each web portal, and you configure it using CLI commands or the FortiGate GUI.

The list of recognized software, along with the associated registry key value, is available on the CLI only. Software is split into three categories: antivirus (*av*), firewall (*fw*), and *custom*. Custom is used for customized or proprietary software that an organization may require. Administrators can configure *av*, *fw*, or both settings on the GUI or CLI, but the custom setting is available only on the CLI.

Administrators can also configure OS versions and patch settings to allow or deny VPN connections from specific OS versions.

The disadvantage of enabling client integrity checking is that it can result in a lot of administrative overhead because of the following factors:

- All users must have their security software up to date in order to successfully establish a connection.
- Software updates can result in a change to the registry key values, which can also prevent a user from successfully connecting.

As such, administrators must have in-depth knowledge of the Windows operating system and subsequent registry behavior in order to properly make extended use of and maintain this feature.

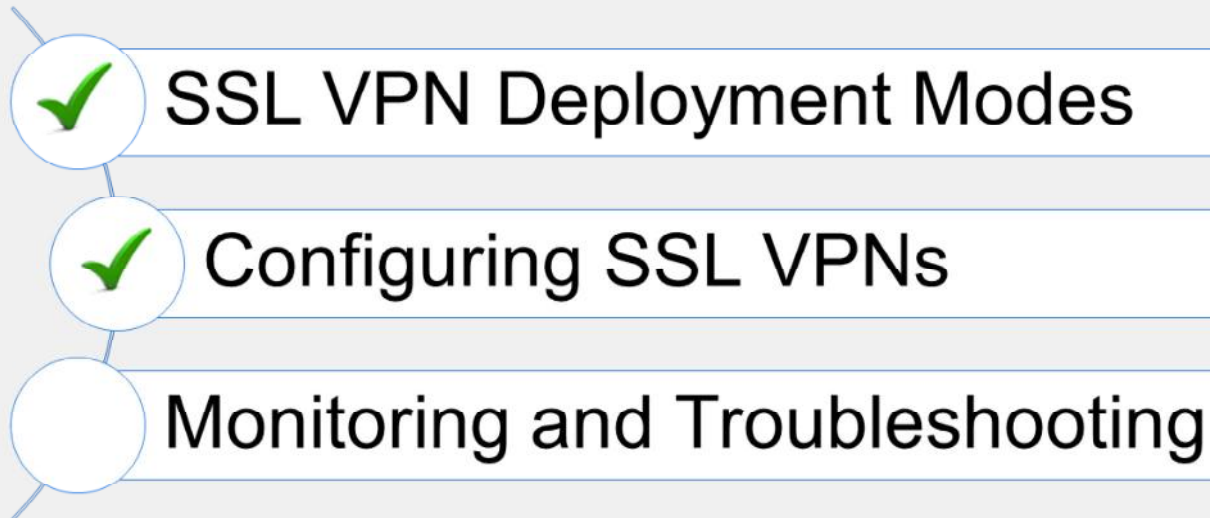
**DO NOT REPRINT**  
**© FORTINET**

## Knowledge Check

1. Which step is necessary to configure SSL VPN connections?
  - ✓ A. Create a firewall policy from the SSL VPN interface to the resource's interface.
  - B. Enable event logs for SSL VPN traffic: users, VPN, and endpoints.
2. 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

**DO NOT REPRINT**  
**© FORTINET**

## Lesson Progress



Good job! You now understand how to configure FortiGate for SSL VPN connections.

Now, you'll learn how to monitor SSL VPN sessions, review logs, configure SSL VPN timers, and troubleshoot common issues.

**DO NOT REPRINT  
© FORTINET**

## Monitoring and Troubleshooting

### Objectives

- Monitor SSL VPN-connected users
- Review SSL VPN logs
- Configure SSL VPN timers
- Troubleshoot common SSL VPN issues
- Identify hardware acceleration components for SSL VPN

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

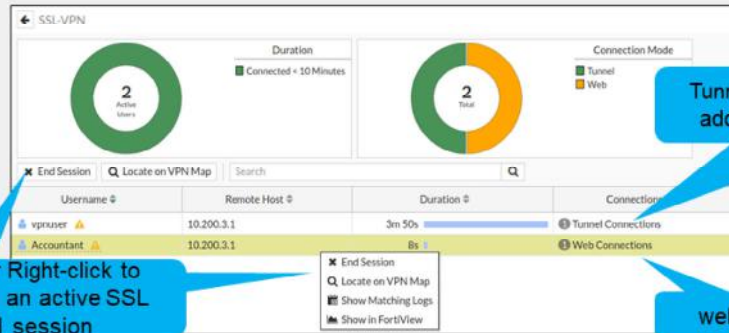
By demonstrating competence in SSL VPN monitoring and troubleshooting, you will be able to avoid, identify, and solve common issues and misconfigurations.

# 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  
Training Institute

© Fortinet Inc. All Rights Reserved.

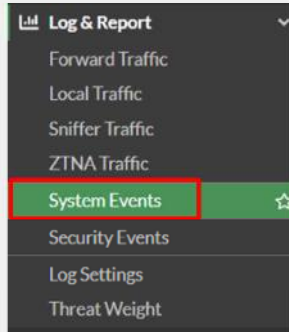
28

You can monitor which SSL VPN users are connected on the **SSL VPN** widget. This shows the names of all SSL VPN users that 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



Date/Time	Level	Action	Status	Message
2020/01/21 04:50:...	■	ssl-new-con		SSL new connection
2020/01/21 04:50:...	■	tunnel-down		SSL tunnel shutdown
2020/01/21 04:49:...	■	tunnel-stats		SSL tunnel statistics
2020/01/21 04:39:...	■	tunnel-up		SSL tunnel established
2020/01/21 04:39:...	■	ssl-new-con		SSL new connection

The screenshot shows the 'User Events' widget with a red box around the title and a red arrow pointing from the 'System Events' menu item in the previous image.

Date/Time	Level	User	Action	Message
2020/01/21 04:50:33	■	Student	auth-logout	User Student removed from auth logon
2020/01/21 04:39:02	■	Student	auth-logon	User Student added to auth logon

- 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

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

- Select **VPN Events** widget to show new connection requests, and if the SSL VPN tunnel is established or closed.
- Select **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

### VPN > SSL VPN Settings

Redirect HTTP to SSL-VPN	<input type="checkbox"/>
Restrict Access	<input checked="" type="radio"/> Allow access from any host <input type="radio"/> Limit access
Idle Logout	<input checked="" type="checkbox"/>
Inactive For	<input type="text" value="300"/> Seconds

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

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.

## 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.

## Best Practices for Common SSL VPN Issues

- For web mode connections, make sure that:
  - Cookies are enabled and the internet privacy options are set to high in your web browser
  - SSL VPN clients are following the proper URL structure: `https://<FortiGateIP>:<port>`
- 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
  - Users are encouraged to log out if they are not using the network resources only accessible by SSL VPN

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:

- Enable cookies in your web browser
- Set internet privacy options to high in your web browser
- 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
- 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
```

```
hw-acceleration-status → Display the status of SSL hardware acceleration
```

```
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 enable
```

Display debug messages for SSL VPN; -1 debug level produces detailed results

- Check debug logs on the FortiClient

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
- `hw-acceleration-status`: Displays the status of SSL hardware acceleration
- `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.

## Hardware Acceleration for SSL VPN

- FortiGate devices with content processors (CP8 or CP9), which offload specific CPU-intensive operations, support high-performance SSL VPN bulk data engines
  - SSL/TLS protocol processor
- Administrators can disable CP offloading through firewall policies
  - For example: test purposes

```
config firewall policy
  edit 1
    set auto-asic-offload [enable |disable]
  end
```

- To view the status of SSL VPN acceleration, use the following command:

```
get vpn status ssl hw-acceleration-status
```

```
Acceleration hardware detected: kxp=on      No acceleration hardware detected
cipher=on
```

FortiGate devices that have CP8 or CP9 content processors, which accelerate many common resource-intensive, security-related processes, can offload SSL VPN traffic to a high-performance VPN bulk data engine.

This specialized IPsec and SSL/TLS protocol processor processes most of the latest well-known algorithms for encryption.

By default, the offloading process is set up. If, for testing purposes you want to disable it, you can do it using the CLI only at the firewall policy configuration level.

You can also view the status of SSL VPN acceleration using the CLI.




**DO NOT REPRINT**  
**© FORTINET**

## Knowledge Check

1. What does the SSL VPN monitor feature allow you to do?
  - A. Monitor SSL VPN user actions, such as authentication
  - ✓ B. Force SSL VPN user disconnections
2. Which statement about SSL VPN timers is correct?
  - ✓ A. SSL VPN timers can prevent logouts when SSL VPN users experience long network latency.
  - B. The login timeout is a non-customizable hard value.

**DO NOT REPRINT**  
**© FORTINET**

## Lesson Progress

-  SSL VPN Deployment Modes
-  Configuring SSL VPNs
-  Monitoring and Troubleshooting

Congratulations! You have completed this lesson.

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

**DO NOT REPRINT**  
**© FORTINET**

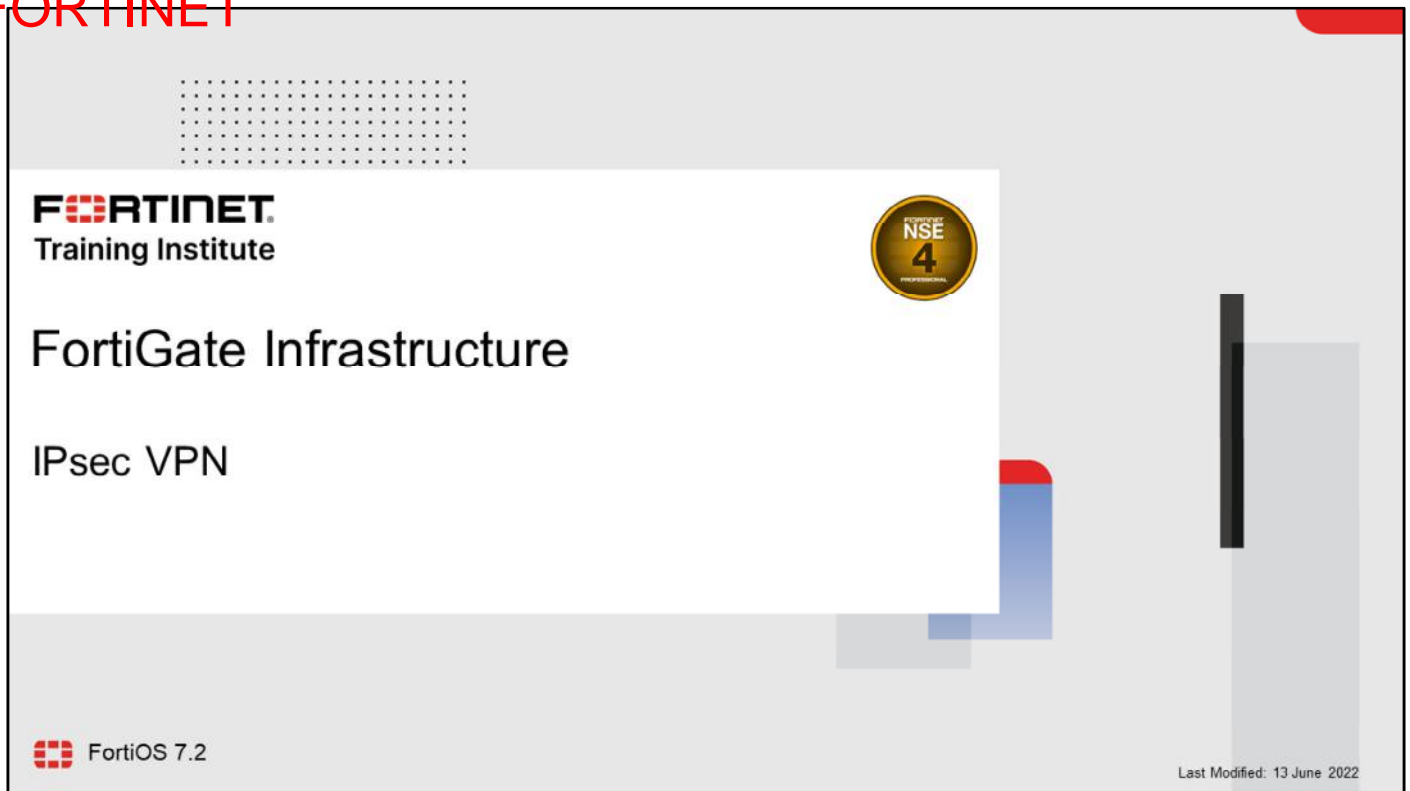
## Review

- ✓ Describe the differences between SSL VPN modes
- ✓ Define authentication for SSL VPN users
- ✓ Configure SSL VPN portals
- ✓ Configure SSL VPN settings
- ✓ Define firewall policies for SSL VPN
- ✓ Configure the client integrity check
- ✓ Monitor SSL VPN connected users
- ✓ Review SSL VPN logs
- ✓ Configure SSL VPN timers
- ✓ 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



The slide features a white background with a grid of dots in the top left corner. The Fortinet logo is positioned in the upper left, with the text 'FORTINET Training Institute' below it. To the right of the logo is a gold circular badge with 'NSE 4' and 'PROFESSIONAL' text. The main title 'FortiGate Infrastructure' is centered, followed by the subtitle 'IPsec VPN'. In the bottom left, there is a red Fortinet logo and the text 'FortiOS 7.2'. In the bottom right, it says 'Last Modified: 13 June 2022'. The slide is decorated with abstract geometric shapes in blue and red.

**FORTINET**  
Training Institute

NSE  
4  
PROFESSIONAL

FortiGate Infrastructure

IPsec VPN

FortiOS 7.2

Last Modified: 13 June 2022

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

**DO NOT REPRINT**  
**© FORTINET**

## Lesson Overview

- IPsec Introduction
- IPsec Configuration
- Routing and Firewall Policies
- Redundant VPNs
- Monitoring and Logs

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

DO NOT REPRINT  
© FORTINET

## IPsec Introduction

### Objectives

- Describe the benefits of IPsec VPN
- Be familiar with the IPsec protocol
- Understand how IPsec works
- Select an appropriate VPN topology

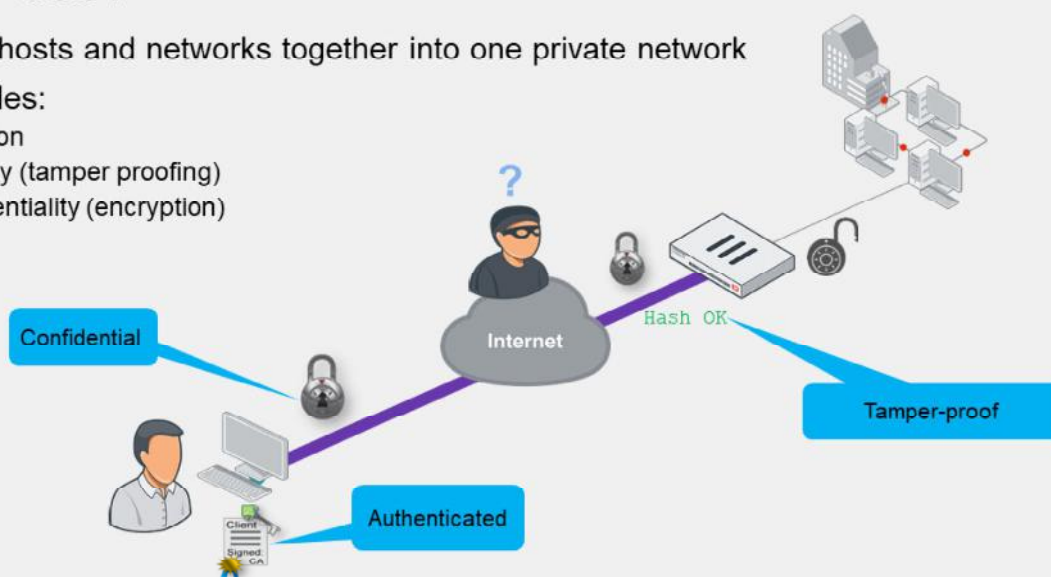
After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in IPsec basics, you will be able to understand IPsec concepts and benefits.

# DO NOT REPRINT © FORTINET

## What Is IPsec?

- Joins remote hosts and networks together into one private network
- Usually provides:
  - Authentication
  - Data integrity (tamper proofing)
  - Data confidentiality (encryption)



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

## 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 RFC 2409 (IKEv1) RFC 4306 (IKEv2)	IP protocol 17: UDP port 500 (UDP 4500 for rekey, quick mode, mode-cfg)	IP protocol 17: UDP port 500
ESP RFC 4303	IP protocol 17: UDP port 4500 (encapsulated)	IP protocol 50

- 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 will be 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 is 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

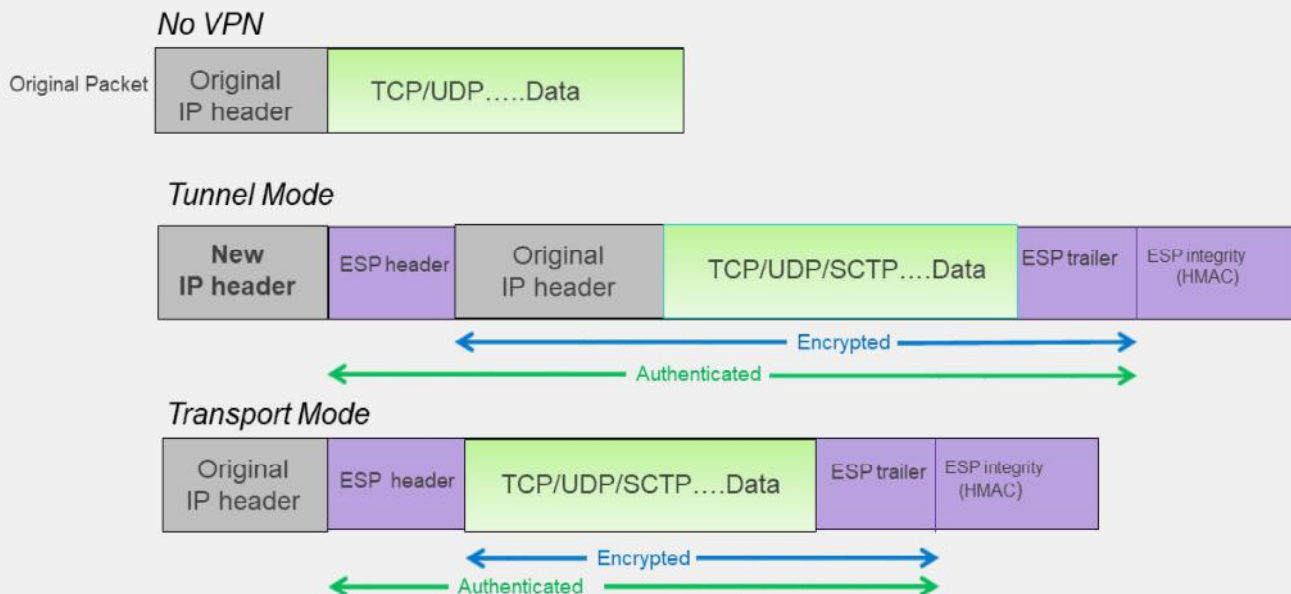


IPsec provides services at the IP (network) layer. During tunnel establishment, both ends negotiate the encryption and authentication algorithms to use.

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.

7

What's encapsulated? It depends on the encapsulation mode being used. IPsec can operate in two modes: transport mode and tunnel mode.

- Transport mode directly encapsulates and protects the fourth layer (transport) and above. The original IP header is not protected and no additional IP header is added.
- Tunnel mode is a true tunnel. The whole IP packet is encapsulated and a new IP header is added at the beginning. After the IPsec packet reaches the remote LAN and is unwrapped, the original packet can continue on its journey.

Note that after you remove the VPN-related headers, a transport mode packet can't be transmitted any further; it has no second IP header inside, so it's not routable. For that reason, this mode is usually used only for end-to-end (or client-to-client) VPNs.

DO NOT REPRINT  
© FORTINET

## What Is IKE?

- Default ports: UDP port 500 (and UDP port 4500 when crossing NAT)
- Negotiates a tunnel's private keys, authentication, and encryption
- Phases:
  - Phase 1
  - Phase 2
- Versions
  - IKEv1 (legacy, wider adoption)
  - IKEv2 (new, simpler operation)

IKE uses UDP port 500. If NAT-T is enabled in a NAT scenario, IKE uses UDP port 4500.

IKE establishes an IPsec VPN tunnel. FortiGate uses IKE to negotiate with the peer and determine the IPsec security association (SA). The IPsec SA defines the authentication, keys, and settings that FortiGate uses to encrypt and decrypt that peer's packets. It is based on the Internet Security Association and Key Management Protocol (ISAKMP).

IKE defines two phases: phase 1 and phase 2.

There are two IKE versions: IKEv1 and IKEv2. Even though IKEv2 is a newer version and features a simpler protocol operation, this lesson focuses on IKEv1 only, because of its much wider adoption.

## 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

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

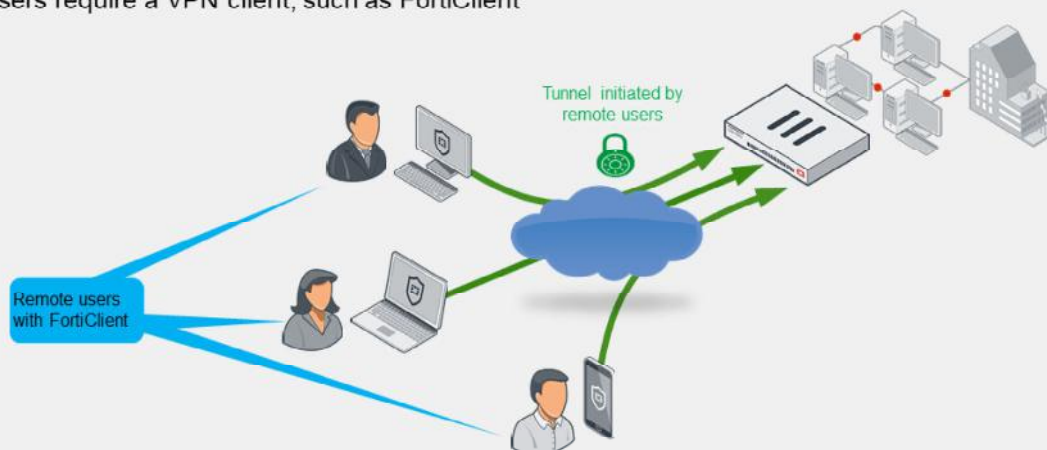
The IPsec architecture uses SAs as the basis for building security functions into IPsec. An SA is the bundle of algorithms and parameters being used to encrypt and authenticate data travelling through the tunnel. In normal two-way traffic, this exchange is secured by a pair of SAs, one for each traffic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



**FORTINET**  
Training Institute

© Fortinet Inc. All Rights Reserved.

11

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.

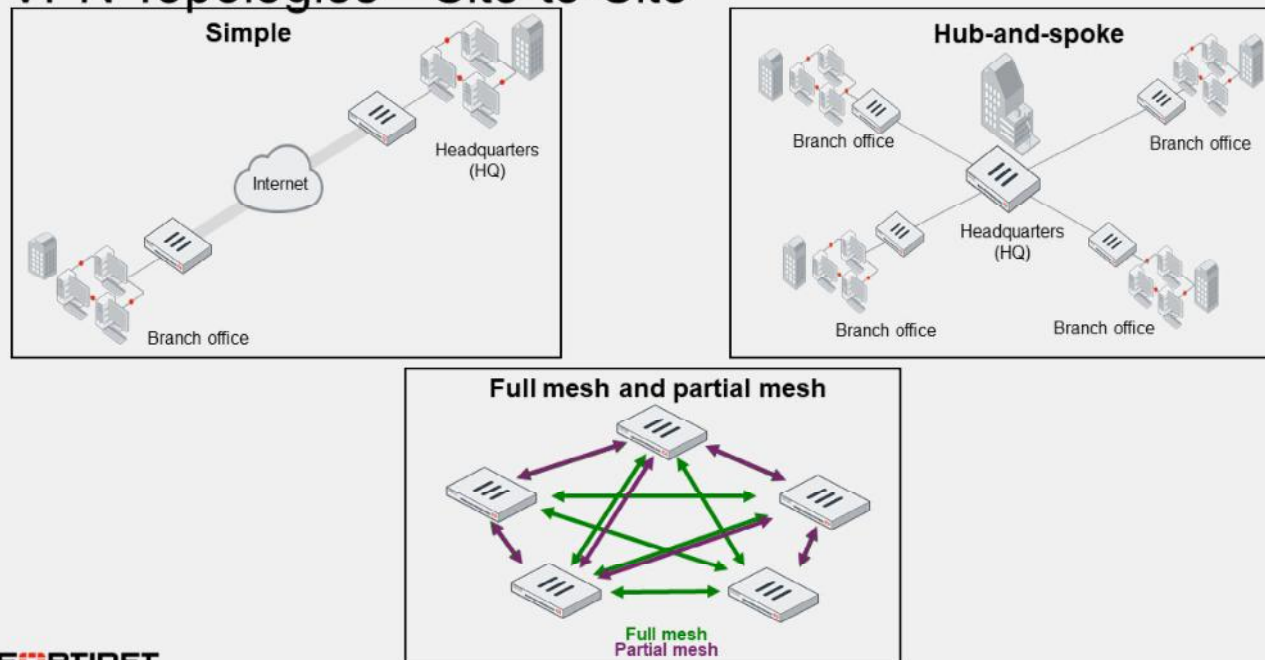
In a remote access VPN, FortiGate is usually configured as a dial-up server. You will learn more about dial-up VPNs in this lesson. The IP address of the remote internet user is usually dynamic. Because FortiGate does not know the IP address of the remote user, only the remote user can initiate a VPN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



**FORTINET**  
Training Institute

© Fortinet Inc. All Rights Reserved.

12

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.

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**

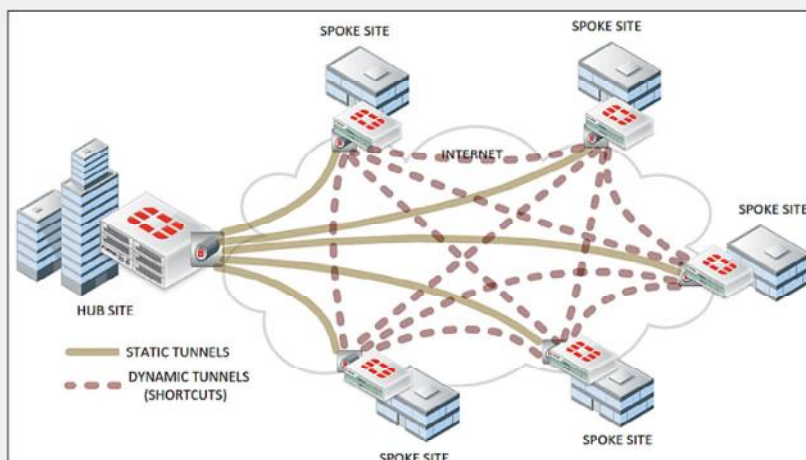
## VPN Topologies—Comparison

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.

## Auto-Discovery VPN

- Dynamically negotiates on-demand direct VPNs between spokes
  - Provides the benefits of a full mesh topology over a hub-and-spoke or partial mesh deployment
  - Dynamic routing is recommended to learn routes between hub and spokes and scale up easier
  - Static routing also works, but should be used for small deployments only



Each VPN topology has its advantages and disadvantages.

Auto-discovery VPN (ADVPN) is a FortiGate feature that achieves the benefits of a full-mesh topology with the easier configuration and scalability benefits of hub-and-spoke and partial-mesh topologies.

First, you add the VPN configurations for building either a hub-and-spoke or a partial-mesh topology, to the FortiGate devices. Then, you enable ADVPN on the VPNs. ADVPN dynamically negotiates tunnels between spokes (without having them preconfigured) to get the benefits of a full-mesh topology.

You can use dynamic routing and static routing to deploy ADVPN. A dynamic routing protocol, such as BGP, is usually deployed in large networks because it enables you to exchange routing information between spokes and hub easier, and as a result, to scale up. You can also use static routing to deploy ADVPN, but it is recommended to do so in small networks that are not likely to grow considerably.

Whether you use dynamic routing or not, after a shortcut is negotiated, FortiGate automatically adds routes through the shortcut to redirect spoke-to-spoke traffic through it.

DO NOT REPRINT  
© FORTINET

## Knowledge Check

1. Which IPsec protocol is not supported by FortiGate?

- A. IKEv2
- ✓ B. AH

2. Which VPN topology is the most fault tolerant?

- ✓ A. Full mesh
- B. Hub-and-spoke

**DO NOT REPRINT**  
**© FORTINET**

## Lesson Progress

- IPsec Introduction
- IPsec Configuration
- Routing and Firewall Policies
- Redundant VPNs
- Monitoring and Logs

Good job! You have now been introduced to IPsec.

Now, you will learn about IPsec configuration.

DO NOT REPRINT  
© FORTINET

## IPsec Configuration

### Objectives

- Learn about the IPsec wizard
- Identify and understand the phases of IKEv1
- Understand IPsec phase 1 and phase 2 settings

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

By demonstrating competence in IPsec configuration, you will be able to successfully determine the settings required for your IPsec VPN deployment.

DO NOT REPRINT  
© FORTINET

## IPsec Wizard

VPN > IPsec Wizard

VPN Creation Wizard

1 VPN Setup 2 Authentication 3 Policy & Routing 4 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

Site to Site - FortiGate

Network diagram describing deployment type

This FortiGate --- Internet --- Remote FortiGate

Summary of objects created by the IPsec wizard

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

© Fortinet Inc. All Rights Reserved.

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 provided. 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 received.

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.

DO NOT REPRINT  
© FORTINET

## Using the IPsec Wizard for a FortiClient VPN

- Simplifies IPsec configuration for a FortiClient VPN

### VPN > IPsec Wizard

VPN Setup

Name: FCT

Template type: Site to Site | Hub-and-Spoke | Remote Access

Remote device type: Client-based | Native

Dialup - FortiClient (Windows, Mac OS, Android)

VPN Creation Wizard

Incoming Interface: port1

Authentication method: Pre-shared Key | Signature

Pre-shared key: .....

User Group: Training

VPN Creation Wizard

Local interface: port3

Local Address: LOCAL\_SUBNET

Client Address Range: 10.200.200.10-10.200.200.100

Subnet Mask: 255.255.255.0

DNS Server: Use System DNS | Specify

VPN Creation Wizard

The following settings should be reviewed prior to creating the VPN.

Object Summary

Split Tunnel Group	FCT_split
Phase 1 interface	FCT
Phase 2 interface	FCT
Address	FCT_range
Remote to local policies	VPN_FCT_remote
Endpoint Registration	FCT

VPN Creation Wizard

Save Password:

Auto Connect:

Always Up (Keep Alive):

**FORTINET**  
Training Institute

© Fortinet Inc. All Rights Reserved.

19

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

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.

## 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)
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.

To authenticate each other, the peers use two methods: pre-shared key or digital signature. You can also enable an additional authentication method, XAuth, to enhance authentication.

In IKEv1, there are two possible modes in which the IKE SA negotiation can take place: main, and aggressive mode. Settings on both ends must agree; otherwise, phase 1 negotiation fails and both IPsec peers are not able to establish a secure channel.

At the end of phase 1, the negotiated IKE SA is used to negotiate the DH keys that are used in phase 2. DH uses the public key (that both ends know) plus a mathematical factor called a nonce, in order to generate a common private key. With DH, even if an attacker can listen to the messages containing the public keys, they cannot determine the secret key.

DO NOT REPRINT  
© FORTINET

## Phase 1—Network

**FORTINET**  
Training Institute

© Fortinet Inc. All Rights Reserved.

23

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.

## Phase 1—Network (Contd)

New VPN Tunnel

Name: ToRemote

Comments: Comments 0/255

**Network**

IP Version: IPv4 IPv6

Remote Gateway: Static IP Address

IP Address: 10.200.3.1

Interface: port1

Local Gateway:

Mode Config:

NAT Traversal:  Enable  Disable  Forced

Keepalive Frequency: 10

Dead Peer Detection:  Disable  On Idle  On Demand

DPD retry count: 3

DPD retry interval: 20

Forward Error Correction:  Egress  Ingress

**Advanced...**

Add route	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Disabled
Auto discovery sender	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Disabled
Auto discovery receiver	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Disabled
Exchange interface IP	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Disabled
Device creation	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Disabled
Aggregate member	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Disabled

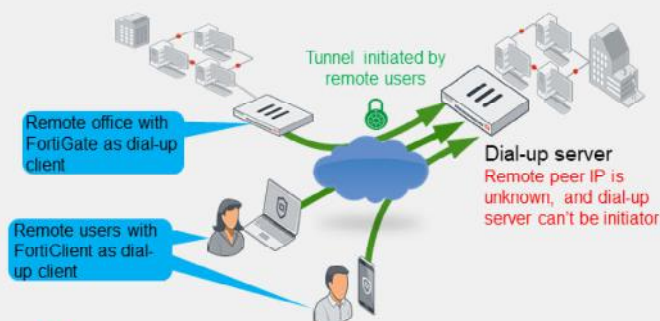
The following are the other options available on the GUI in the **Network** section:

- **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.

## Phase 1—Network—Remote Gateway

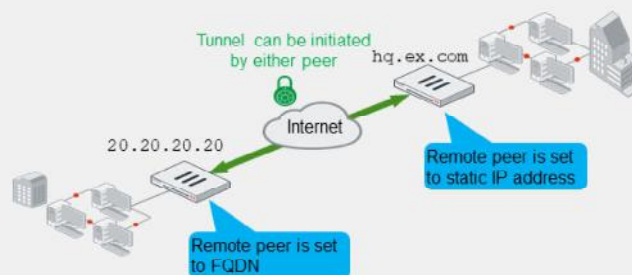
### Dial-up user

- 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)



### 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)



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. One dial-up server configuration on FortiGate can be used for multiple IPsec tunnels from many remote offices or users.

Use **Static IP Address** or **Dynamic DNS** when you know the remote peer address. If you select **Static IP Address**, then you need to provide an IP address. If you select **Dynamic DNS**, then you need to 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 has 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

The screenshot shows the 'Network' configuration page for IKE Mode Config. The 'Remote Gateway' is set to 'Dialup User' and 'Mode Config' is checked. The 'IPv4 mode config' section is expanded, showing the following settings:

- Use system DNS in mode config:
- Assign IP From:  Range
- Client Address Range: 10.200.200.1-10.200.200.10
- Subnet Mask: 255.255.255.255
- DNS Server: 8.8.8.8
- Enable IPv4 Split Tunnel:
- Accessible Networks: LOCAL\_SUBNET
- IPv6 mode config:
  - Client Address Range: ::::
  - Prefix Length: 128
  - DNS Server: ::
  - Enable IPv6 Split Tunnel:

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.

## 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

Network	
IP Version	IPv4 IPv6
Remote Gateway	Static IP Address
IP Address	10.200.3.1
Interface	port1
Local Gateway	<input type="checkbox"/>
Mode Config	<input type="checkbox"/>
NAT Traversal	Enable Disable Forced
Keepalive Frequency	10

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.

## Phase 1—Network—Dead Peer Detection (DPD)

- Mechanism to detect a dead tunnel
- Useful in redundant VPNs, where multiple paths are available
- Three modes:
  - **On Demand:** DPD probes are sent when there is no inbound traffic
  - **On Idle:** DPD probes are sent when there is no traffic
  - **Disabled:** only reply to DPD probes—don't send probes

The screenshot shows the 'Network' configuration page for an IPsec VPN. The 'Dead Peer Detection' section is highlighted with a red box. It contains three radio button options: 'Disable', 'On Idle', and 'On Demand'. The 'On Demand' option is selected. Other visible settings include: IP Version (IPv4), Remote Gateway (Static IP Address), IP Address (10.200.3.1), Interface (port1), Local Gateway (disabled), Mode Config (disabled), NAT Traversal (Enable, Disable, Forced), Keepalive Frequency (10), DPD retry count (3), and DPD retry interval (20 s).

After the peers negotiate the IPsec SAs of a tunnel and, therefore, the tunnel is considered up, the peers usually don't negotiate another IPsec SA until it expires. In most cases, the IPsec SA expires every few hours. This means that if there is a network disruption along the path of the tunnel before the IPsec SA expires, the peers will continue to send traffic through the tunnel even though the communication between the sites is disrupted.

When you enable DPD, DPD probes are sent to detect a failed (or dead) tunnel and bring it down before its IPsec SAs expire. This failure detection mechanism is very useful when you have redundant paths to the same destination, and you want to fail over to a backup connection when the primary connection fails to keep the connectivity between the sites up.

FortiGate supports three DPD modes:

- **On Demand:** FortiGate sends DPD probes if there is only outbound traffic through the tunnel, but no inbound. Because network applications are usually bidirectional, observing only traffic on the outbound direction could be an indication of a network failure.
- **On Idle:** FortiGate sends DPD probes when no traffic is observed in the tunnel. An idle tunnel does not necessarily mean the tunnel is dead. Avoid this mode if you have many tunnels, because the overhead introduced by DPD can be very resource intensive.
- **Disabled:** FortiGate replies only to DPD probes received. FortiGate never sends DPD probes to the remote peer and therefore cannot detect a dead tunnel.

The default DPD mode is **On Demand**. In terms of scalability, **On Demand** is a better option than **On Idle**.

DO NOT REPRINT  
© FORTINET

## Phase 1—Authentication

The screenshot displays the configuration interface for Phase 1 Authentication. It is divided into three main sections:

- Authentication:** Contains a dropdown menu for 'Method' set to 'Pre-shared Key', a text field for 'Pre-shared Key' (masked with dots), and a dropdown for 'IKE' set to 'Signature'.
- IKE:** Contains a dropdown for 'Version' with options '1' and '2' selected.
- IKE (continued):** Contains a dropdown for 'Mode' with options 'Aggressive' and 'Main (ID protection)' selected. Below this is the 'Peer Options' section, which includes a dropdown for 'Accept Types' set to 'Specific peer ID', and a dropdown for 'Peer ID' with options 'Any peer ID' and 'Specific peer ID'.

Red arrows point from the 'Pre-shared Key' dropdown in the Authentication section to the 'Pre-shared Key' dropdown in the Authentication section. Another red arrow points from the 'Aggressive' mode in the Mode dropdown to the 'Aggressive' mode in the Mode dropdown. A third red arrow points from the 'Main (ID protection)' mode in the Mode dropdown to the 'Main (ID protection)' mode in the Mode dropdown.

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.

## 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

The screenshot displays the 'Phase 1 Proposal' configuration interface. The main window shows three proposals with the following configurations:

Proposal	Encryption	Authentication
1	AES128	SHA256
2	AES256	SHA256
3	AES128	SHA1
4	AES256	SHA1

Below the proposals, the 'Diffie-Hellman Groups' section shows a grid of checkboxes for groups 1 through 32. Groups 14 and 5 are checked. The 'Key Lifetime (seconds)' is set to 86400. The 'Local ID' field is empty.

Two inset windows show dropdown menus for encryption and authentication algorithms. The top inset shows encryption algorithms: AES128, DES, 3DES, AES128, AES192, and AES256. The bottom inset shows authentication algorithms: SHA256, MD5, SHA256, SHA384, and 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.

## Phase 1—Extended Authentication (XAuth)

- XAuth adds stronger authentication: username + password
- You can authorize all users who belong to a specific user group or inherit it from the matching policy

Phase 1 supports two types of authentication: pre-shared keys and digital signatures. The XAuth extension, sometimes called phase 1.5, forces remote users to authenticate additionally with their credentials (username and password). So, additional authentication packets are exchanged if you enable it. What is the benefit? Stronger authentication.

When you set **Remote Gateway** to **Dialup User**, FortiGate acts as the authentication server. The **XAUTH** section shows the authentication server type options: **PAP Server**, **CHAP Server**, and **Auto Server**. In the example shown on this slide, **Auto Server** is selected, which means that FortiGate automatically detects the authentication protocol used by the client.

After you select the authentication server type, you configure how user group matching is performed. There are two options: **Inherit from policy** and **Choose**. The latter is used in the example on this slide, and allows you to select one of the user groups available on FortiGate. Note that, when you select **Choose**, you must configure a separate dial-up VPN for every group of users that require a different network access policy.

The other way to authenticate VPN users with XAuth is by selecting **Inherit from policy**. When you select this option, FortiGate authenticates users based on their matching IPsec policy and, as a result, the configuration for controlling network access is simpler. That is, you control network access by configuring multiple policies for different user groups, instead of configuring multiple tunnels for different user groups. The **Inherit from policy** option follows a similar authentication approach used for SSL VPN remote users. You will learn more about SSL VPN in another 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.

## Phase 2—How it Works

- Negotiates two unidirectional IPsec SAs for ESP
  - Protected by phase 1 IKE SA
- 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.

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.

## 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**

The screenshot displays the 'Phase 2 Selectors' configuration page. At the top, a table lists existing selectors, with 'ToRemote' having local and remote addresses of 0.0.0.0/0.0.0.0. Below this, the 'New Phase 2' configuration form is shown. The 'Name' field is 'ToRemote'. The 'Local Address' and 'Remote Address' fields both have a 'Subnet' dropdown selected and the address '0.0.0.0/0.0.0.0'. The 'Advanced...' button is highlighted with a red box. Below it, the 'Advanced' section is expanded, showing 'Local Port', 'Remote Port', and 'Protocol' all set to 'All' with checked checkboxes. To the right, a dropdown menu for 'Subnet' is open, listing various address types: 'Subnet', 'IP Range', 'IP Address', 'Named Address', 'IPv6 Subnet', 'IPv6 Range', 'IPv6 Address', and 'Named IPv6 Address'.

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.

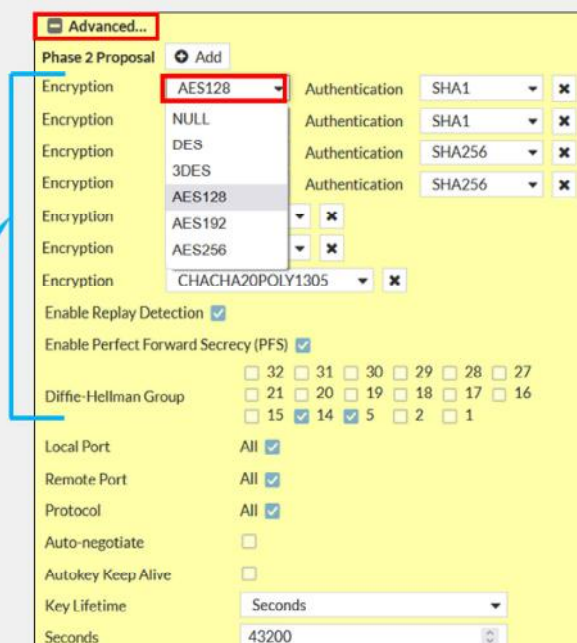
Note that after the traffic is accepted by a firewall policy, traffic is dropped before entering the IPsec tunnel if the traffic does not match any of the phase 2 selectors configured. For this reason, usually, it's more intuitive to filter traffic with firewall policies. So, if you don't want to use 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.

## 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.

## 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

These settings control when SA renegotiation occurs

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 phase1-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**

## Knowledge Check

1. Which type of VPN peer can initiate a VPN tunnel?  
 A. Dial-up server  
 B. Dial-up client
  
2. On which phase do you configure the algorithms used for traffic encryption?  
 A. Phase 1  
 B. Phase 2
  
3. Which IKEv1 negotiation mode is faster?  
 A. Aggressive  
 B. Main

**DO NOT REPRINT**  
**© FORTINET**

## Lesson Progress

- IPsec Introduction
- IPsec Configuration
- Routing and Firewall Policies
- Redundant VPNs
- Monitoring and Logs

Good job! You now understand IPsec configuration.

Now, you will learn about routing and firewall policies for IPsec traffic.

**DO NOT REPRINT  
© FORTINET**

## Routing and Firewall Policies

### Objectives

- Understand route-based IPsec VPNs
- Learn how to configure routing and firewall policies for IPsec traffic

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

By demonstrating competence in routing and firewall policies for IPsec VPNs, you will be able to set up appropriate routing and firewall policies for your IPsec VPN deployment.

## Route-Based IPsec VPNs

- Types of IPsec VPNs:
  - Route-based
    - Virtual interface for each VPN: VPN matching based on routing
  - Policy-based
    - Legacy: VPN matching based on policy. Not recommended.
- Route-based VPNs benefits:
  - Simpler operation and configuration
    - Redundancy
  - Support for:
    - L2TP-over-IPsec
    - GRE-over-IPsec
    - Dynamic routing protocols

FortiGate supports two types of IPsec VPNs: route-based and policy-based. Policy-based is a legacy IPsec VPN that is supported only for backward compatibility reasons, and its use *is not recommended* for new deployments. Unless otherwise stated, all IPsec VPN references in this lesson are for route-based IPsec VPNs.

In a route-based IPsec VPN, FortiGate automatically adds a virtual interface with the VPN name. This means that not only can you configure routing and firewall policies for IPsec traffic in the same way you do for non-IPsec traffic, but you also can leverage the presence of multiple connections to the same destination to achieve redundancy.

Another benefit of route-based IPsec VPNs is that you can deploy variations of IPsec VPNs such as L2TP-over-IPsec and GRE-over-IPsec. In addition, you can also enable dynamic routing protocols for scalability purposes and best path selection.

## Routes for IPsec VPNs

### Dial-up user

```
config vpn ipsec phase1-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

**Network > Static Routes**

Edit Static Route

Destination **Subnet** Internet Service  
10.0.2.0/255.255.255.0

Interface **ToRemote**

Administrative Distance **10**

Comments Write a comment

Status **Enabled** Disabled

Advanced Options

OK Cancel

Select virtual interface of IPsec VPN

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

### Policy & Objects > Firewall Policy

New Policy

Name **Traffic to Remote**

Incoming Interface **port3**

Outgoing Interface **ToRemote**

Source **LOCAL\_SUBNET**

Destination **REMOTE\_SUBNET**

Schedule **always**

Service **ALL**

Action **ACCEPT**  **DENY**

Inspection Mode **Flow-based**  **Proxy-based**

Firewall / Network Options

NAT

Virtual interface matches phase 1 name

Allow and inspect the traffic coming from/going to the IPsec virtual interface

### Policy & Objects > Firewall Policy

New Policy

Name **Traffic from Remote**

Incoming Interface **ToRemote**

Outgoing Interface **port3**

Source **REMOTE\_SUBNET**

Destination **LOCAL\_SUBNET**

Schedule **always**

Service **ALL**

Action **ACCEPT**  **DENY**

Inspection Mode **Flow-based**  **Proxy-based**

Firewall / Network Options

NAT

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**

## Knowledge Check

1. Which IPsec VPN type is legacy and not recommended for new deployments?
  - A. Route-based IPsec VPN
  - ✓ B. Policy-based IPsec VPN
  
2. 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

DO NOT REPRINT  
© FORTINET

## Lesson Progress

- IPsec Introduction
- IPsec Configuration
- Routing and Firewall Policies
- Redundant VPNs
- Monitoring and Logs

Good job! You now understand routing and firewall policies for IPsec traffic.

Now, you will learn about redundant VPNs.

DO NOT REPRINT  
© FORTINET

## Redundant VPNs

### Objectives

- Learn about redundant VPNs
- Understand redundant VPN configuration between two FortiGate devices

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

By demonstrating competence in redundant VPNs, you will be able to add redundancy to your IPsec VPN deployment.

## 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.

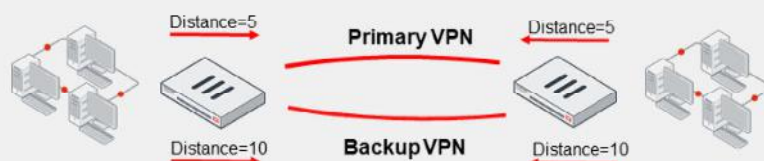
There are two types of redundant VPNs:

- 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**

## Knowledge Check

1. Which feature should be enabled in a redundant IPsec VPN deployment?  
 A. DPD  
 B. XAuth
  
2. Which setting determines whether a tunnel is used as primary or backup?  
 A. Routing  
 B. Firewall policies

DO NOT REPRINT  
© FORTINET

## Lesson Progress

- IPsec Introduction
- IPsec Configuration
- Routing and Firewall Policies
- Redundant VPNs
- Monitoring and Logs

Good job! You now understand redundant VPNs.

Now, you will learn about monitoring IPsec VPNs and reviewing their logs.

DO NOT REPRINT  
© FORTINET

## Monitoring and Logs

### Objectives

- Learn how to monitor an IPsec VPN status
- Check IPsec VPN logs

**FORTINET**  
Training Institute

51

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

By demonstrating competence in monitoring and logs, you will be able to monitor IPsec VPN and review past events.

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

Name	Remote Gateway	Peer ID	Incoming Data	Outgoing Data	Phase 1	Phase 2 Selectors
ToRemote	10.200.1.1		2.18 kB	2.18 kB	Phase 1	ToRemote1 ToRemote2

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

More columns available

© Fortinet Inc. All Rights Reserved. 52

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 (**ToRemote1**) 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

Phase 1 is up

Dashboard > Network > Static & Dynamic Routing

Network	Gateway IP	Interfaces	Distance
0.0.0.0/0	10.9.15.254	port1	10
10.0.2.0/24	10.9.15.23	ToRemote	10

- Phase 2 comes up, if the remote gateway is set to dial-up user

Dashboard > Network > IPsec

Phase 2 is up

Name	Remote Gateway	Peer ID
Custom		
Dialup_0	10.9.15.30	

Dashboard > Network > Routing (Static & Dynamic Routing)

Network	Gateway IP	Interfaces	Distance
0.0.0.0/0	10.9.15.254	port1	10
10.0.2.0/24	10.9.15.30	Dialup	15

FORTINET  
Training Institute

© Fortinet Inc. All Rights Reserved.

53

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

Log & Report > System Events > VPN Events

Phase 2 is up (tunnel is up)

Double-click any log to get more details

Date/Time	Level	Action	Status	Message	VPN Tunnel
Yesterday	INFO	negotiate	success	progress IPsec phase 2	ToRemote
Yesterday	INFO	negotiate	success	progress IPsec phase 2	ToRemote
Yesterday	INFO	phase2-up		IPsec phase 2 status change	ToRemote
Yesterday	INFO	install_sa		install IPsec SA	ToRemote
Yesterday	INFO	phase2-down		IPsec phase 2 status change	ToRemote
Yesterday	INFO	tunnel-stats		IPsec tunnel statistics	ToRemote
Yesterday	INFO	negotiate	success	negotiate IPsec phase 2	ToRemote
Yesterday	INFO	negotiate	success	progress IPsec phase 2	ToRemote
Yesterday	INFO	tunnel-up		IPsec connection status change	ToRemote
Yesterday	INFO	phase2-up		IPsec phase 2 status change	ToRemote
Yesterday	INFO	install_sa		install IPsec SA	ToRemote
Yesterday	INFO	negotiate	success	progress IPsec phase 2	ToRemote
Yesterday	INFO	negotiate	success	progress IPsec phase 1	ToRemote
Yesterday	INFO	negotiate	success	progress IPsec phase 1	ToRemote
Yesterday	INFO	negotiate	success	progress IPsec phase 1	ToRemote
Yesterday	INFO	negotiate	success	progress IPsec phase 1	ToRemote
Yesterday	INFO	negotiate	failure	progress IPsec phase 1	N/A

Log Details	
General	
Date	2021/03/22
Time	10:33:52
Virtual Domain	root
Log Description	Progress IPsec phase 1
Source	
Local IP	10.200.1.1
User	Remote-FortiGate
Group	N/A
XAUTH User	N/A
XAUTH Group	N/A
Action	
Action	negotiate
Status	success
Result	DONE
Security	
Level	INFO
Event	
Assigned IP	N/A
Cookies	02e4b2193e41051c/93ac47b04378fabd
Direction	inbound

Phase 1 is DONE (up)

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**

## Knowledge Check

1. The IPsec monitor widget enables you to bring down the \_\_\_\_\_ of an IPsec VPN.
  - A. Phase 1
  - ✓ B. Entire tunnel
  
2. When the remote gateway is set to dial-up user, a static route to the remote network is added to the routing table after \_\_\_\_\_.
  - A. Phase 1 comes up
  - ✓ B. Phase 2 comes up

**DO NOT REPRINT**  
**© FORTINET**

## Lesson Progress

-  IPsec Introduction
-  IPsec Configuration
-  Routing and Firewall Policies
-  Redundant VPNs
-  Monitoring and Logs

Congratulations! You have completed this lesson.

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

**DO NOT REPRINT**  
**© FORTINET**

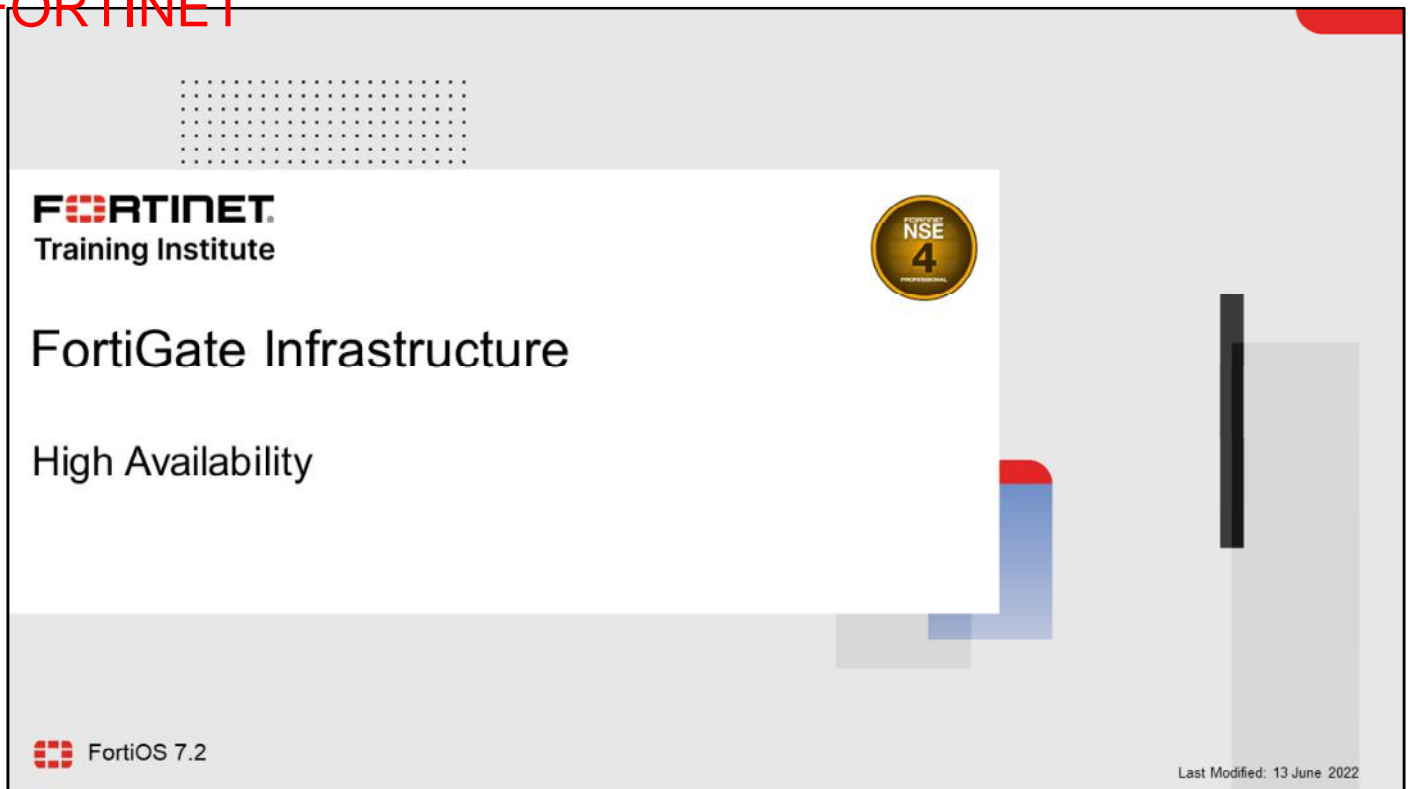
## Review

- ✓ Describe the benefits of IPsec VPN
- ✓ Understand how IPsec works
- ✓ Learn about the IPsec wizard
- ✓ Identify and understand the phases of IKEv1
- ✓ Understand phase 1 and phase 2 settings
- ✓ Understand redundant VPN configuration between two FortiGate devices
- ✓ Monitor IPsec VPNs and review logs

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



The slide features a white background with a grid of dots in the top left corner. The Fortinet logo is in the top left, followed by 'Training Institute'. A gold NSE 4 Professional badge is in the top right. The main title 'FortiGate Infrastructure' and subtitle 'High Availability' are centered. The FortiGate logo is in the bottom left, and 'FortiOS 7.2' is next to it. The date 'Last Modified: 13 June 2022' is in the bottom right. The slide is decorated with a red and blue L-shaped graphic on the right side and a vertical black bar on the far right.

**FORTINET**  
Training Institute

NSE  
4  
PROFESSIONAL

# FortiGate Infrastructure

## High Availability

FortiGate

FortiOS 7.2

Last Modified: 13 June 2022

In this lesson, you will learn about the fundamentals of FortiGate high availability (HA) and how to configure it. FortiGate HA provides a solution for enhanced reliability and increased performance.

**DO NOT REPRINT**  
**© FORTINET**

## Lesson Overview

- HA Operation Modes
- HA Cluster Synchronization
- HA Failover and Workload
- Monitoring and Troubleshooting

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

DO NOT REPRINT  
© FORTINET

## HA Operation Modes

### Objectives

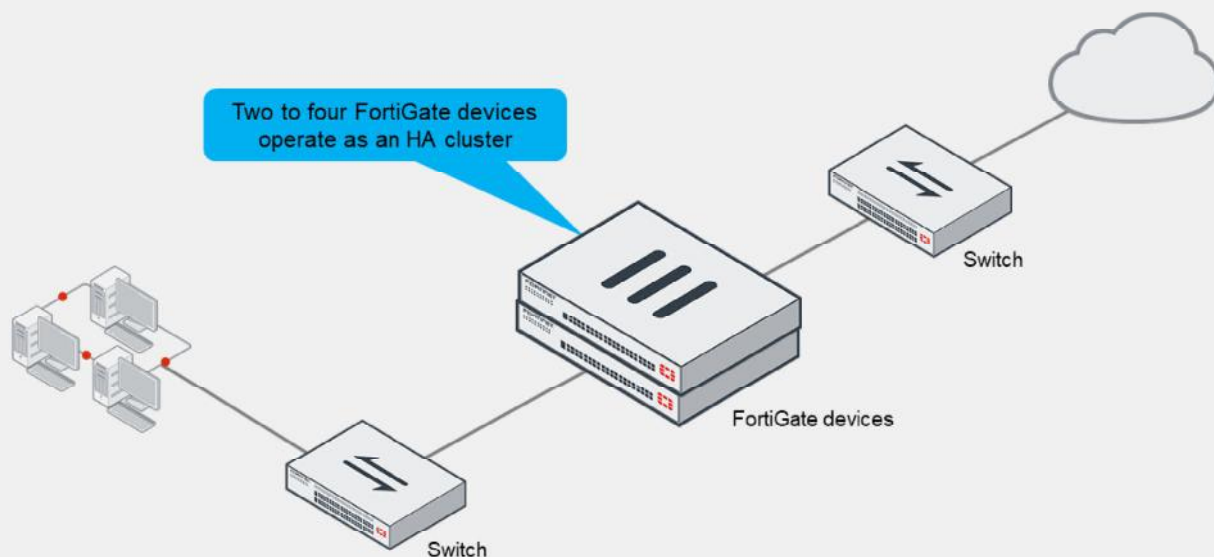
- Identify the different operation modes for HA
- Understand the primary FortiGate election in an HA cluster

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

By demonstrating competence in HA operation modes and primary FortiGate election, you will be able to choose and implement the right HA operation mode in your network based on your requirements. You will be able to use FortiGate devices effectively in your network.

DO NOT REPRINT  
© FORTINET

## What Is FortiGate HA?



**FORTINET**  
Training Institute

© Fortinet Inc. All Rights Reserved.

4

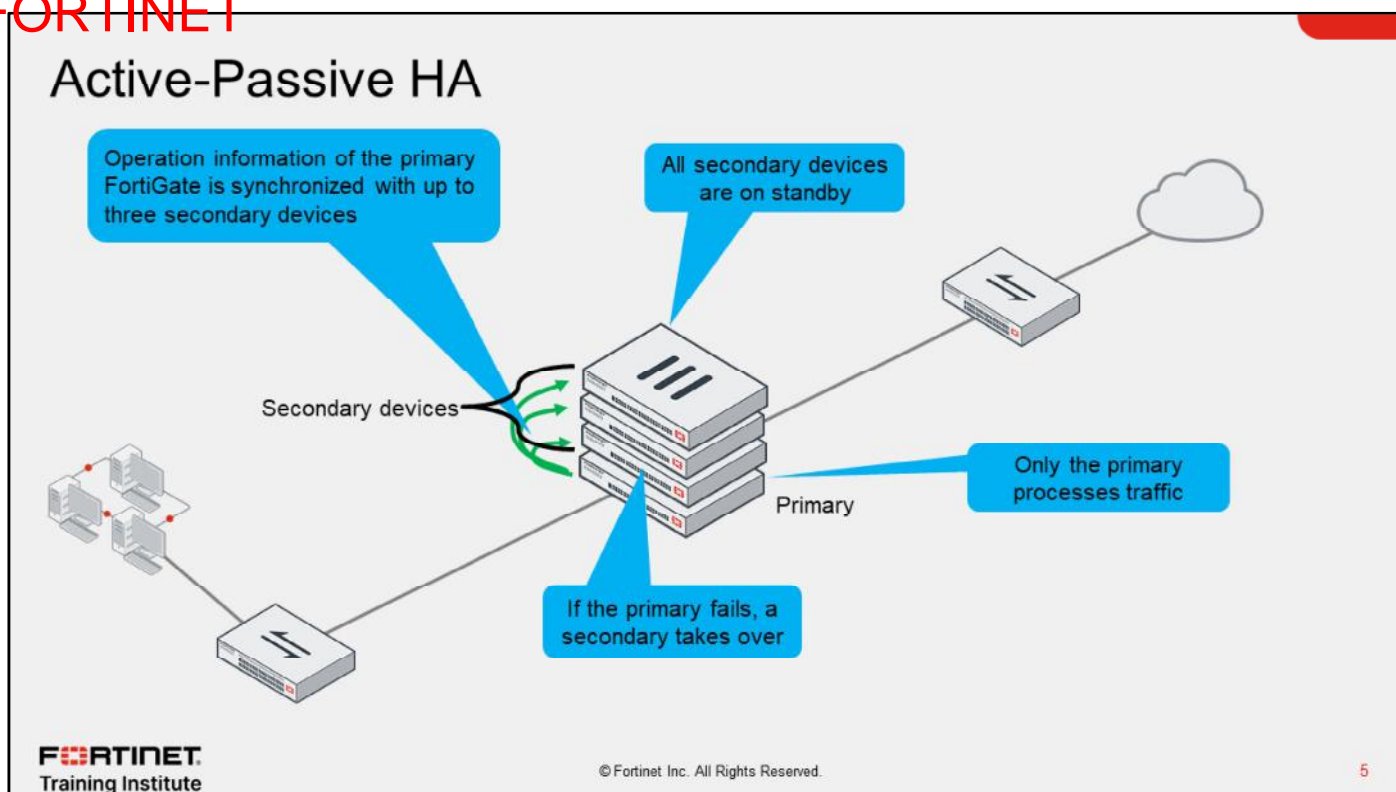
The idea of HA is simple. HA links and synchronizes two to four FortiGate devices to form a cluster for redundancy and performance purposes.

A cluster includes one device that acts as the primary FortiGate (also called the active FortiGate). The primary synchronizes its configuration, 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 currently two HA operation modes available: active-active (A-A) and active-passive (A-P). Now, you will examine the differences.

DO NOT REPRINT  
© FORTINET

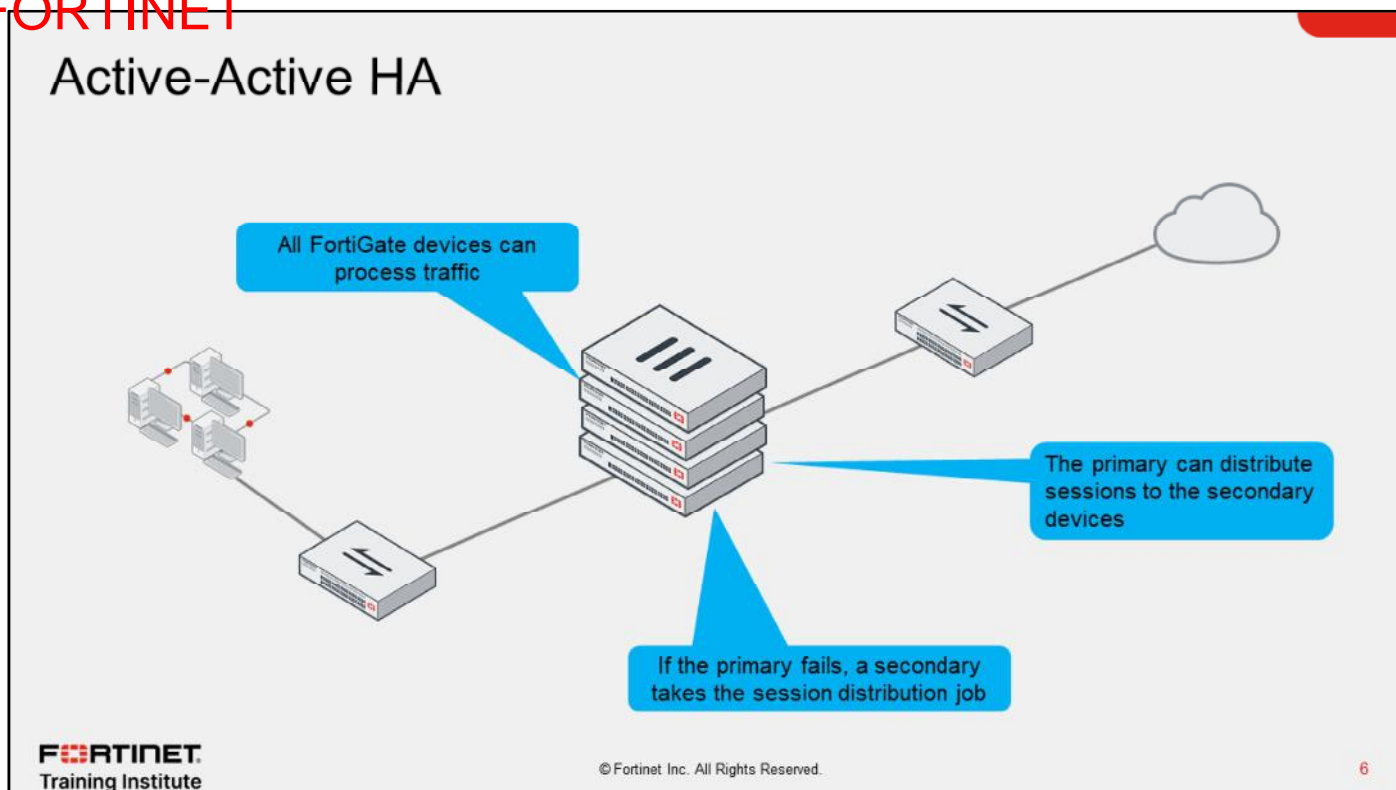


First, take a look at active-passive mode. In either of the two HA operation modes, the operation information (configuration, sessions, FIB entries, and so on) of the primary FortiGate is synchronized with secondary devices.

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.

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*.

DO NOT REPRINT  
© FORTINET



The other HA mode is active-active.

Like active-passive HA, in active-active HA, the operation-related data of the primary FortiGate is synchronized to the secondary FortiGate devices. 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 sessions to the secondary devices.

## FortiGate Clustering Protocol

- Used for:
  - Member discovery
  - Primary election
  - Data synchronization
  - Member health monitoring
- Failover trigger events:
  - Dead member
  - Failed link
  - Failed remote link (link health monitoring)
  - High memory usage
  - Failed solid state disk (SSD)
  - Admin-triggered
- Ethernet types and ports:
  - Heartbeat:
    - Ethernet type 0x8890 (NAT mode)
    - Ethernet type 0x8891 (Transparent mode)
  - Data synchronization, logging, and CLI management:
    - Frame: Ethernet type 0x8893
    - Inner packet:
      - TCP/703 and UDP/703 (data sync)
      - TCP/700 (logging and alert emails)
      - TCP/22 (CLI management)
  - A-A load balancing (first packet only):
    - Frame: Ethernet type 0x8891
    - Inner packet: Original packet (MAC rewrite)

FortiGate HA uses the Fortinet-proprietary FortiGate Clustering Protocol (FGCP) to discover members, elect the primary FortiGate, synchronize data among members, and monitor the health of members.

To discover and monitor members, the members broadcast heartbeat packets over all configured heartbeat interfaces. If the cluster operates in NAT mode, the heartbeat frames are type 8890. In transparent mode, the heartbeat frames are type 8891. If the cluster operates in active-active mode, the first packet of a session distributed to the secondary is encapsulated in Ethernet frames type 8891.

The members also exchange frames type 8893 for data synchronization, local CLI management, and logging purposes. For data synchronization, the inner packet can be TCP port 703 or UDP port 703, depending on the type of data to synchronize. The primary also relays logs and alert emails from secondary devices over TCP port 700. For local HA management using the CLI, the inner packet is SSH.

You can configure the cluster to perform HA failover based on the following events:

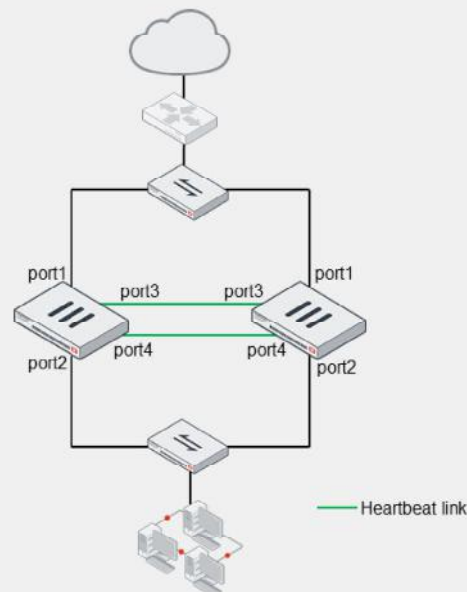
- Dead member: The primary FortiGate is unresponsive.
- Failed link: The link of one or more monitored interfaces on the primary FortiGate goes down.
- Failed remote link: FortiGate uses the link health monitor feature to monitor the health of one or more interfaces. The primary fails if the accumulated penalty of all failed interfaces reaches the set threshold.
- High memory usage: The primary fails if its memory utilization reaches the configured threshold.
- Failed SSD: FortiOS detects a failure in an SSD. Only available for devices with SSDs.
- Admin-triggered: The administrator issues a manual failover.

For any of the failover trigger events, the result is that the cluster promotes one of the secondary devices to the new primary FortiGate role.

# DO NOT REPRINT © FORTINET

## HA Requirements

- All members must have the same:
  - Firmware version
  - Model
  - 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
  - Heartbeat interfaces can see each other
- Best practice:
  - Use at least two heartbeat interfaces (maximum 8)
  - Initially, switch DHCP and PPPoE interfaces to static configuration



To successfully form an HA cluster, you must ensure that the members have the same:

- Firmware version
- Model: the same hardware model or VM model
- Licensing: includes the FortiGuard license, 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

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.

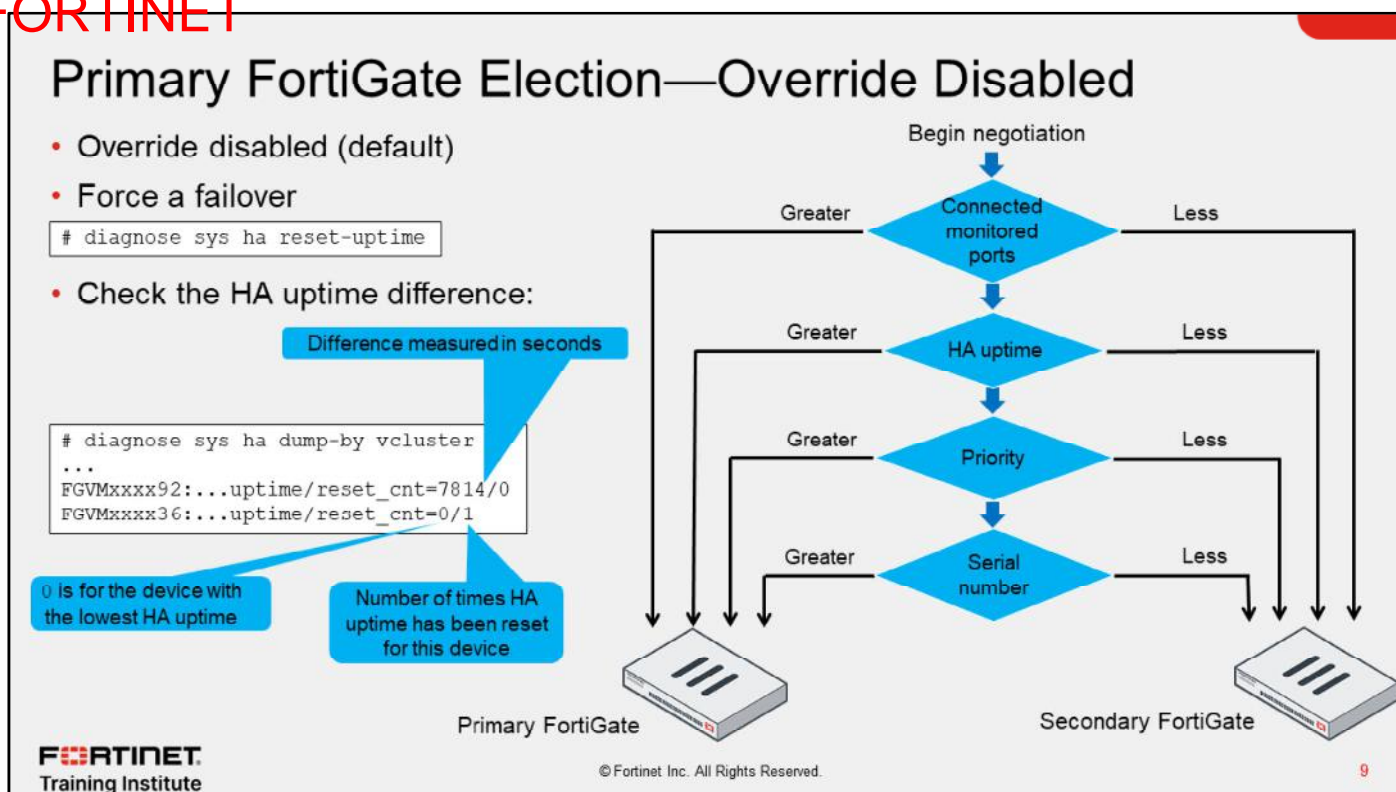
From a configuration and setup point of view, you must also make sure that:

- The HA settings on each member have the same group ID, group name, password, and heartbeat interface settings.
- The heartbeat interfaces on each member can see each other. This usually means placing all heartbeat interfaces in the same broadcast domain, or for two-member clusters, connecting 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.
- If using DHCP or PPPoE interfaces, use static configuration during the cluster initial setup to prevent incorrect address assignment. After the cluster is formed, you can put back the original interface settings.

DO NOT REPRINT  
© FORTINET



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.

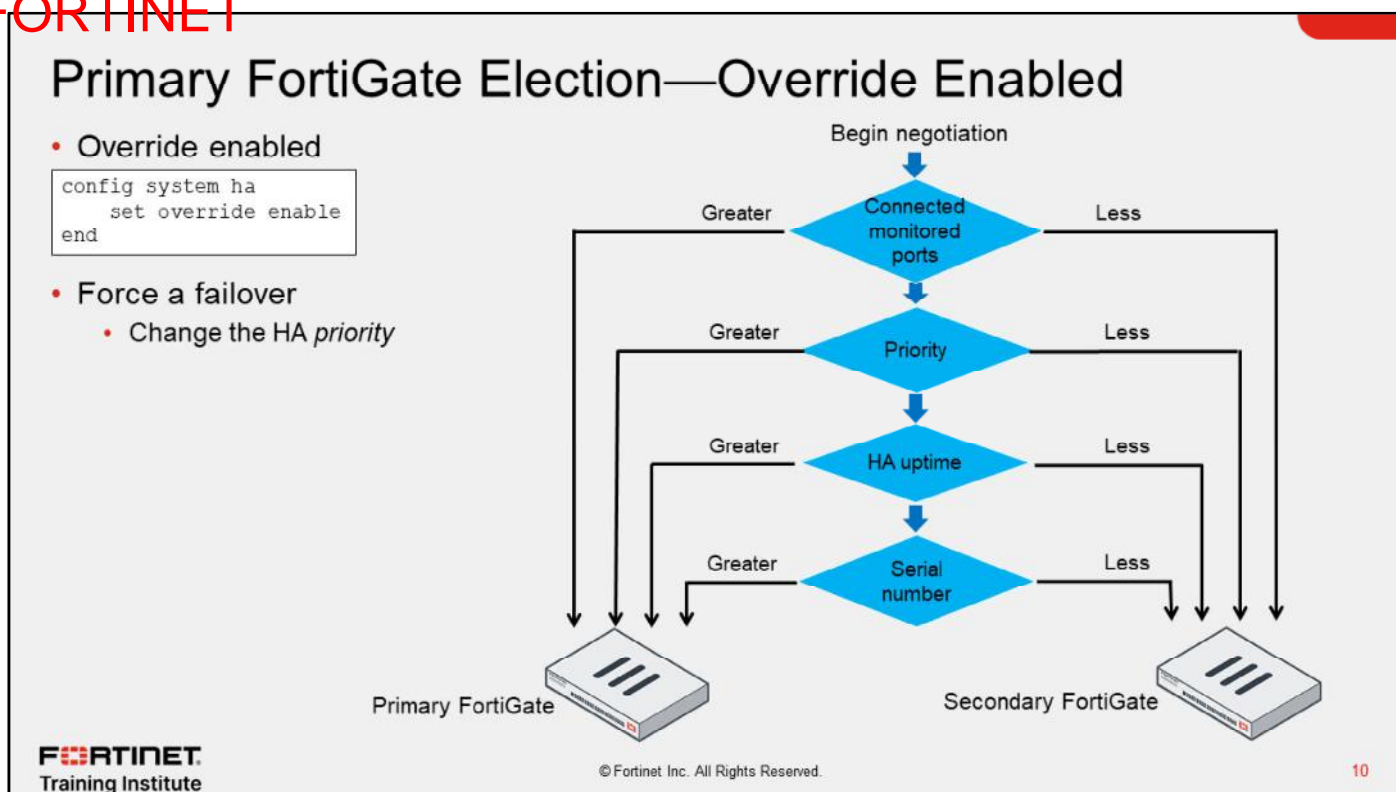
1. The cluster compares the number of monitored interfaces that have a status of up. The member with the most available monitored interfaces becomes the primary.
2. The cluster compares the HA uptime of each member. The member with the highest HA uptime, by at least five minutes, becomes the primary.
3. The member with the highest priority becomes the primary.
4. The member with the lowest 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 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



10

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. That is, on each member, you must manually enable override and adjust the priority.

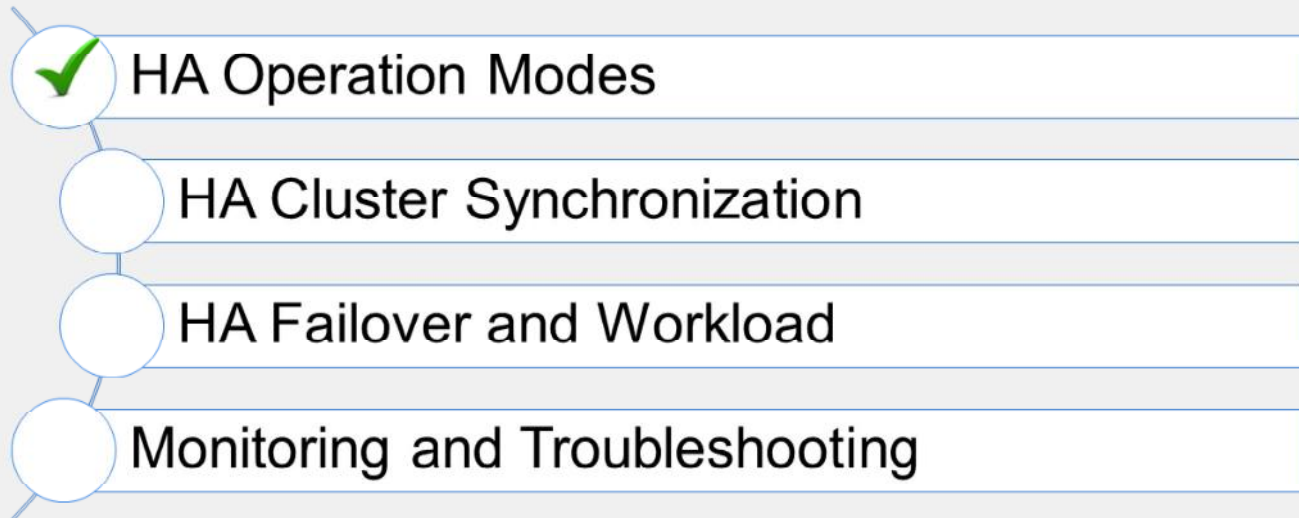
**DO NOT REPRINT**  
**© FORTINET**

## Knowledge Check

1. What is a requirement for members to form an HA cluster?
  - A. They must have same host name
  - ✓ B. They must run the same firmware version
2. What is the default order criteria (override disabled) for selecting the primary in an HA cluster?
  - ✓ A. Connected monitored ports > HA uptime > priority > serial number
  - B. Priority > HA uptime > connected monitored ports > serial number

**DO NOT REPRINT**  
**© FORTINET**

## Lesson Progress



Good job! You now understand HA operation modes and the election of the primary FortiGate in an HA cluster.

Now, you will learn about HA cluster synchronization.

DO NOT REPRINT  
© FORTINET

## HA Cluster Synchronization

### Objectives

- Identify the primary and secondary device tasks in an HA cluster
- Identify what is synchronized between HA cluster members
- Configure session synchronization for seamless failover

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

By demonstrating competence in cluster synchronization, you will be able to identify the tasks assigned to members based on their roles, as well as what information is synchronized between members. You will also learn how to configure session synchronization to perform session failover to specific types of traffic.

## Primary FortiGate Tasks

- Broadcasts hello packets for member discovery and monitoring
- Synchronizes operation-related data such as:
  - Configuration (some settings are not synchronized)
  - FIB entries
  - DHCP leases
  - ARP table
  - FortiGuard definitions
  - IPsec tunnel SAs
  - Sessions (must be enabled)
- In active-active mode only:
  - Distributes sessions to secondary members

So, what are the tasks of a primary FortiGate?

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
- Monitors the health of the primary
  - If the primary fails, the secondary devices elect a new primary
- In active-active mode only:
  - Processes traffic distributed by the primary

Now, take a look at the tasks of secondary FortiGate devices.

Like the primary, secondary members also broadcast hello packets for discovery and monitoring purposes.

In addition, in active-passive mode, the secondary devices act as a standby device, receiving synchronization data but not actually processing any traffic. If the primary FortiGate fails, the secondary devices elect a new primary.

In active-active mode, the secondary devices don't wait passively. They process all traffic assigned to them by the primary device.

## 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

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.

## 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

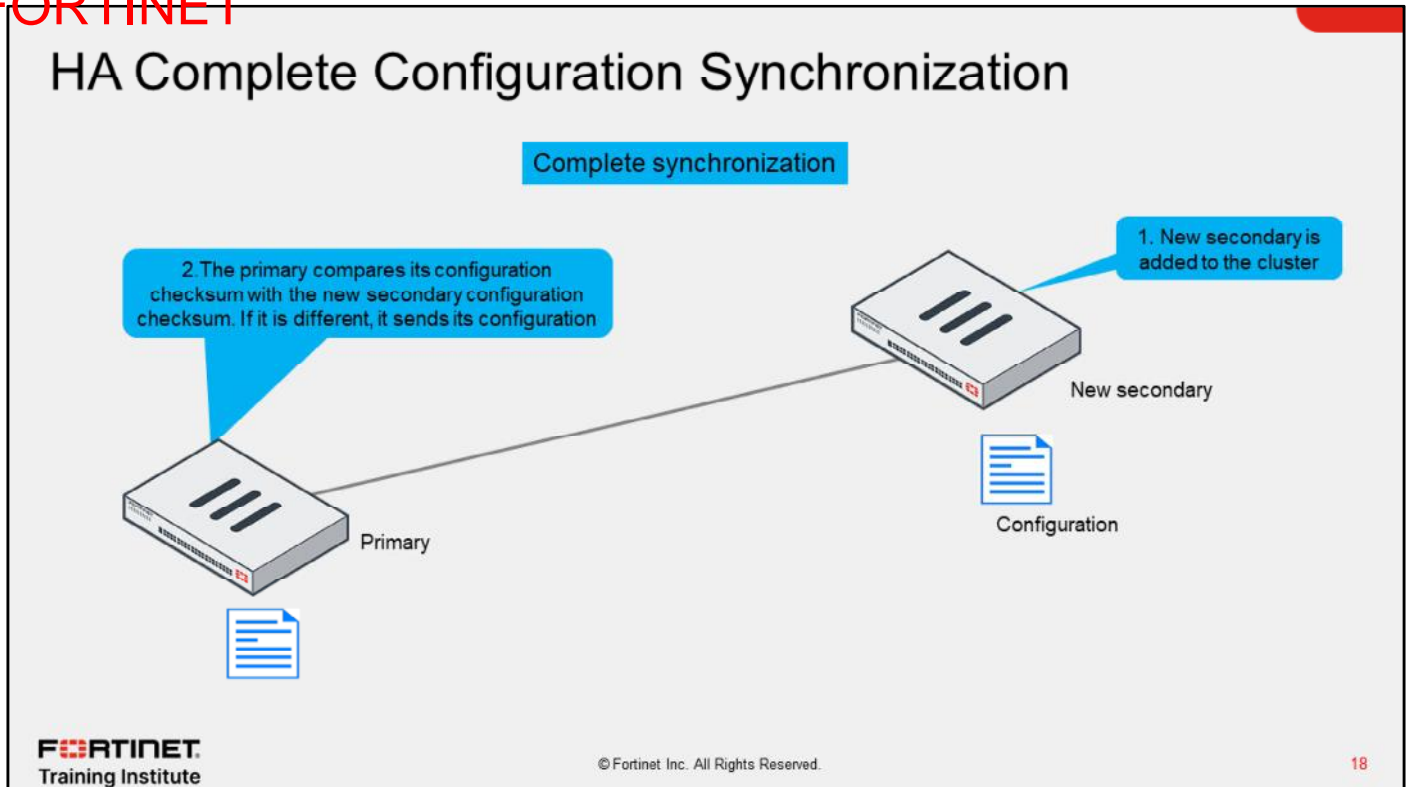
Heartbeat interfaces exchange sensitive information about the cluster operation and may require a fair amount of bandwidth for data synchronization. For this reason, if you use a switch to connect the heartbeat interfaces, it's recommended that you use a dedicated switch or, at least, that you place 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



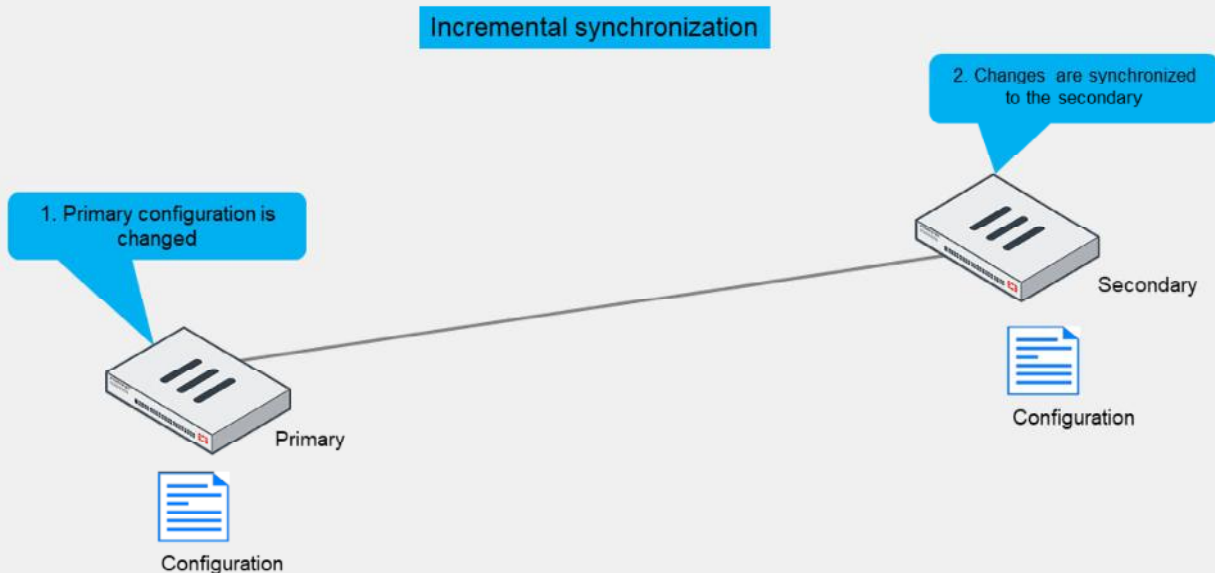
To prepare for a failover, an HA cluster keeps its configurations in sync. You will explore that now.

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



**FORTINET**  
Training Institute

© Fortinet Inc. All Rights Reserved.

19

After the initial synchronization is complete, the primary sends any further configuration changes made by an administrator to all the secondary devices. 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.

## What Is Not Synchronized?

- These configuration settings are *not* synchronized between cluster members:
  - HA management interface settings
    - HA 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
- The primary FortiGate synchronizes all other configuration settings

**Note:**

\* FortiToken licenses (serial numbers) are synchronized

Not all the configuration settings are synchronized. 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

The primary FortiGate synchronizes all other configuration settings, including all other HA settings.

## Session Synchronization

- Provides seamless failover
  - Network applications don't need to restart connections
    - Minimum or no impact
- Firewall sessions
  - TCP sessions are synced by default
    - 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
- 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.

## 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
  - SSL VPN web mode
    - Authentication information
    - Web mode users don't have to reauthenticate after failover
      - They must still restart connections over SSL VPN
- FortiGate doesn't synchronize data for SSL VPN tunnel mode users
  - Tunnel mode users must restart the SSL VPN tunnel after failover

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, the primary FortiGate synchronizes the authentication information for SSL VPN web mode users only. That is, they are using SSL VPN web mode, the SSL VPN users don't have to authenticate again after a failover. However, the users must still restart the connections made using SSL VPN web mode to regain access to protected resources. Note that FortiGate doesn't synchronize any information for SSL VPN tunnel mode. That is, after a failover, SSL VPN tunnel mode users must restart their SSL VPN tunnel connection, as well as any connection made through the tunnel.

**DO NOT REPRINT**  
**© FORTINET**

## Knowledge Check

1. Which information is synchronized in an HA cluster?
  - ✓ A. Firewall policies and objects
  - B. FortiGate host name
  
2. Which one of the following session types can be synchronized in an HA cluster?
  - A. BGP peerings
  - ✓ B. Non-proxy TCP sessions

DO NOT REPRINT  
© FORTINET

## Lesson Progress

- HA Operation Modes
- HA Cluster Synchronization
- HA Failover and Workload
- Monitoring and Troubleshooting

Good job! You now understand HA cluster synchronization.

Now, you will learn about HA cluster failover protection types and workload for primary and secondary FortiGate devices in an HA cluster.

DO NOT REPRINT  
© FORTINET

## HA Failover and Workload

### Objectives

- Identify the HA failover types
- Interpret how an HA cluster in active-active mode distributes traffic
- Implement virtual clustering per VDOM in an HA cluster

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

By demonstrating competence in failover types and workload, you will be able to identify how enhanced reliability is achieved through HA failover protection. You will also learn about the distribution of traffic in an active-active cluster and distributing traffic using virtual clustering.

## 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
    - Only available for devices with SSDs
- Identify failover protection type by looking at:
  - Event logs, SNMP traps, and alert email record failover events
- Enable session synchronization for seamless session failover

The most common types of failovers are device failovers and link failovers. However, you can also configure remote link failover and memory-based failover. When a failover event is triggered, the secondary devices elect a new primary.

A device failover is triggered when the secondary devices stop receiving the heartbeat 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 or an issue on one of the interfaces on the primary. 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 <l - 20>
set hb-interval-in-milliseconds 100ms | 10ms
set hb-lost-threshold <l - 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 x 100 ms x 6 = 1200 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). Note that the 10-millisecond heartbeat interval is supported on NP6 platforms only.

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 primary election is in 30 minutes

This slide shows a configuration example for remote link failover.

First, you configure link health monitor, as shown in the *Routing* lesson. 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 to 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 flip timeout (30 minutes) has passed.

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.

## Failover Protection Configuration (Contd)

- Memory-based failover

- Configure HA settings:

```
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

Check memory usage every 2 seconds

The next primary election is in 20 minutes

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.
- The cluster doesn't elect a new primary again until the flip timeout (20 minutes) has passed.
- Each member in the cluster checks its memory usage every 2 seconds.

If during the primary election, the memory usage of all members are 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

## Failover Protection Configuration (Contd)

- SSD failover

- Configure HA settings:

```
config system ha
  set ssd-failover enable
end
```

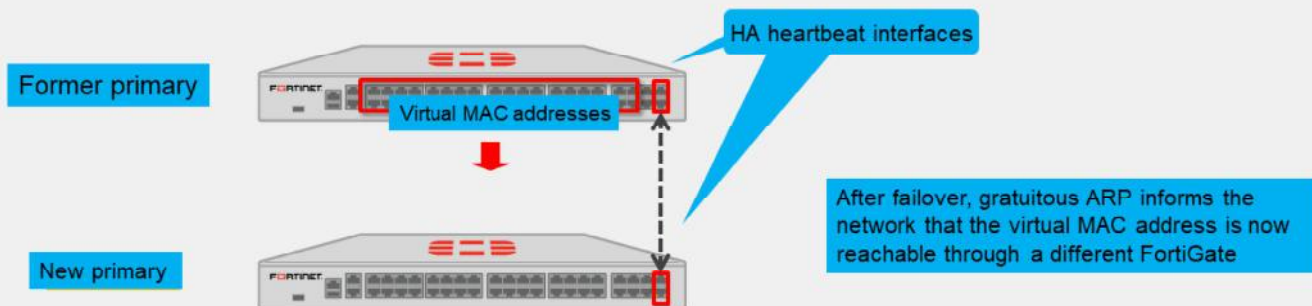
Enable memory-based failover

The HA configuration shown on this slide instructs FortiGate to perform a failover when any of the SSD disks on the primary FortiGate report Ext-fs errors. Note that this feature is supported only on FortiGate models with SSD disks.

DO NOT REPRINT  
© FORTINET

## Virtual MAC Addresses and Failover

- On the primary, each interface is assigned a virtual MAC address
  - HA heartbeat interfaces are not assigned a virtual MAC address
- Upon failover, the newly elected primary adopts the same virtual MAC addresses as the former primary



**FORTINET**  
Training Institute

© Fortinet Inc. All Rights Reserved.

32

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 is 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**

## Failure of a Secondary FortiGate

- Active-passive HA cluster
  - The primary updates the list of available secondary FortiGate devices
  
- Active-active HA cluster
  - The primary updates the list of available secondary FortiGate devices and redistributes sessions to prevent failed secondary devices

As you learned earlier in this lesson, if a primary fails, a new primary is elected. But what happens if a secondary FortiGate device fails? It depends on the HA mode.

In an active-passive cluster, the primary only updates its list of available secondary FortiGate devices. It also starts monitoring for the failed secondary, waiting for it to come online again.

However, in an active-active cluster, the secondary devices can handle traffic. So, the primary (which tracks and assigns sessions to each secondary) must not only update its list of available secondary FortiGate devices, but also reassign sessions from the failed FortiGate to a different secondary FortiGate.

DO NOT REPRINT  
© FORTINET

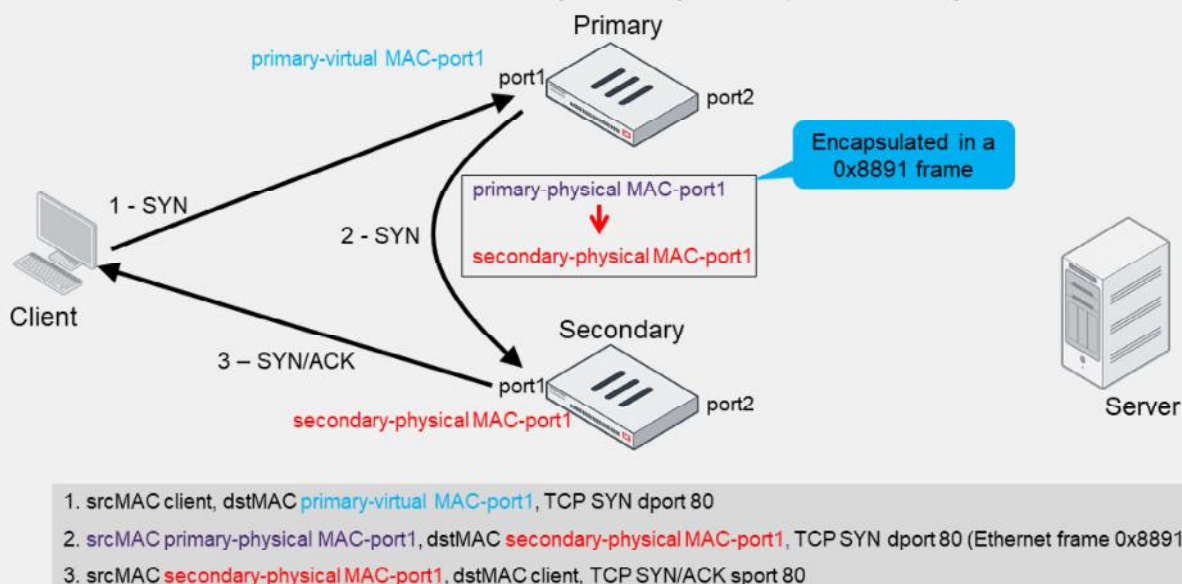
## Workload

- Active-passive HA cluster
  - The primary receives and processes all traffic
  - The secondary waits passively
  
- Active-active HA cluster
  - The primary receives all traffic and redirects some proxy-based sessions to secondary devices
    - Enable `load-balance-all` to force distribution of all sessions

This is how the workload is distributed between roles, depending on the HA mode.

Notice that traffic workload is distributed in active-active mode only. However, keep in mind that by default, only sessions that are subject to proxy inspection are distributed to secondary devices. If you want to force the distribution of sessions that are subject to flow inspection or no inspection at all, then you must enable the `load-balance-all` setting under HA configuration—this setting is disabled by default.

## Active-Active Traffic Flow (Proxy Inspection)



In active-active mode, the following occurs:

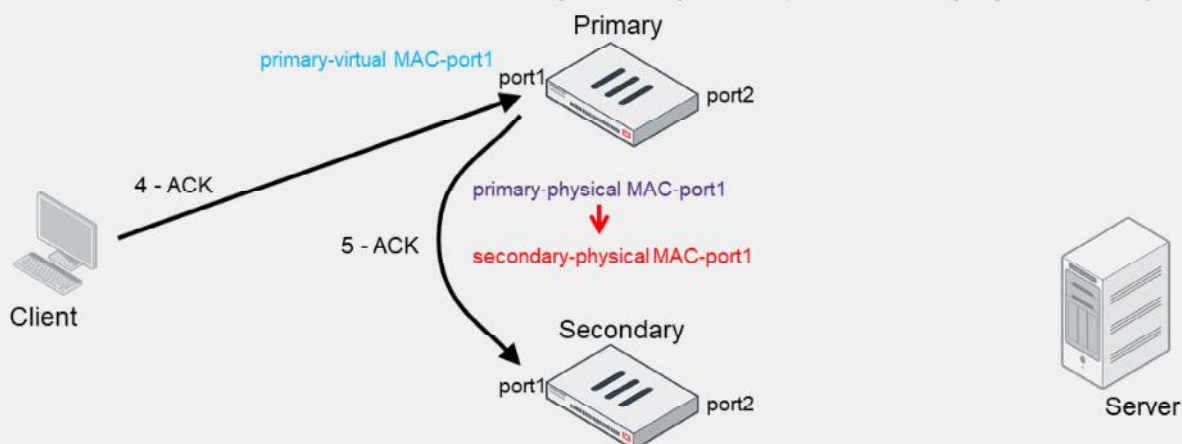
- The traffic destined to the cluster is sent to the primary. Because all network ports on the primary—except the heartbeat ports—are assigned a virtual MAC address, the traffic is destined to the virtual MAC address of the receiving port on the primary FortiGate.
- For traffic that is distributed to the secondary, the traffic destined to the endpoints is sent by the secondary. The traffic is sourced from the physical MAC address of the egressing port on the secondary.

This slide shows the flow for distributed traffic that is subject to proxy inspection:

1. The client sends a SYN packet, which is forwarded to port1 on the primary. The packet destination MAC address is the virtual MAC address on port1.
2. The primary forwards the SYN packet to the selected secondary. In this example, the source MAC address of the packet is changed to the physical MAC address of port1 on the primary and the destination MAC address to the physical MAC address of port1 on the secondary. This is also known as MAC address rewrite. In addition, the primary encapsulates the packet in an Ethernet frame type 0x8891. The encapsulation is done only for the first packet of a load balanced session. The encapsulated packet includes the original packet plus session information that the secondary requires to process the traffic.
3. The secondary responds to the client with a SYN/ACK packet that contains the physical MAC address of port1 on the secondary as the source and the MAC address of the client as the destination.

DO NOT REPRINT  
© FORTINET

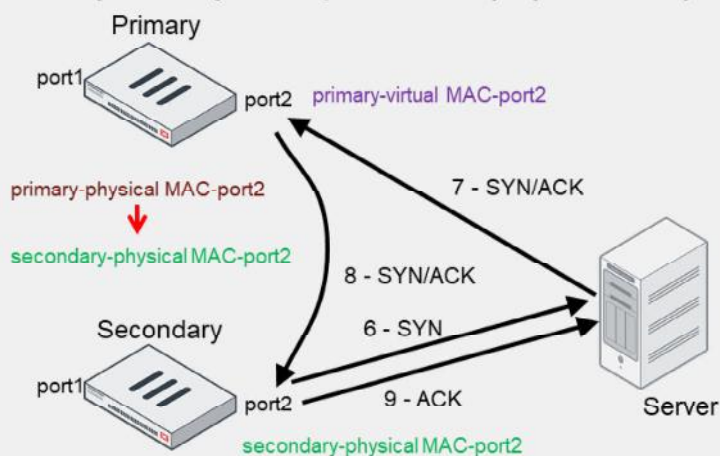
## Active-Active Traffic Flow (Proxy Inspection) (Contd)



4. srcMAC client, dstMAC **primary-virtual MAC-port1**, TCP ACK dport 80
5. srcMAC **primary-physical MAC-port1**, dstMAC **secondary-physical MAC-port1**, TCP ACK dport 80

4. The client acknowledges the SYN/ACK by sending an ACK to the cluster. The ACK packet is destined to port1 on the primary.
5. The primary receives the packet and knows that it matches a session that was previously distributed to the secondary. As a result, the primary forwards the ACK packet to the corresponding secondary FortiGate. The packet is sourced from the physical MAC address of port1 on the primary and destined to the physical MAC address of port1 on the secondary. The three-way handshake on the client side is complete.

## Active-Active Traffic Flow (Proxy Inspection) (Contd)



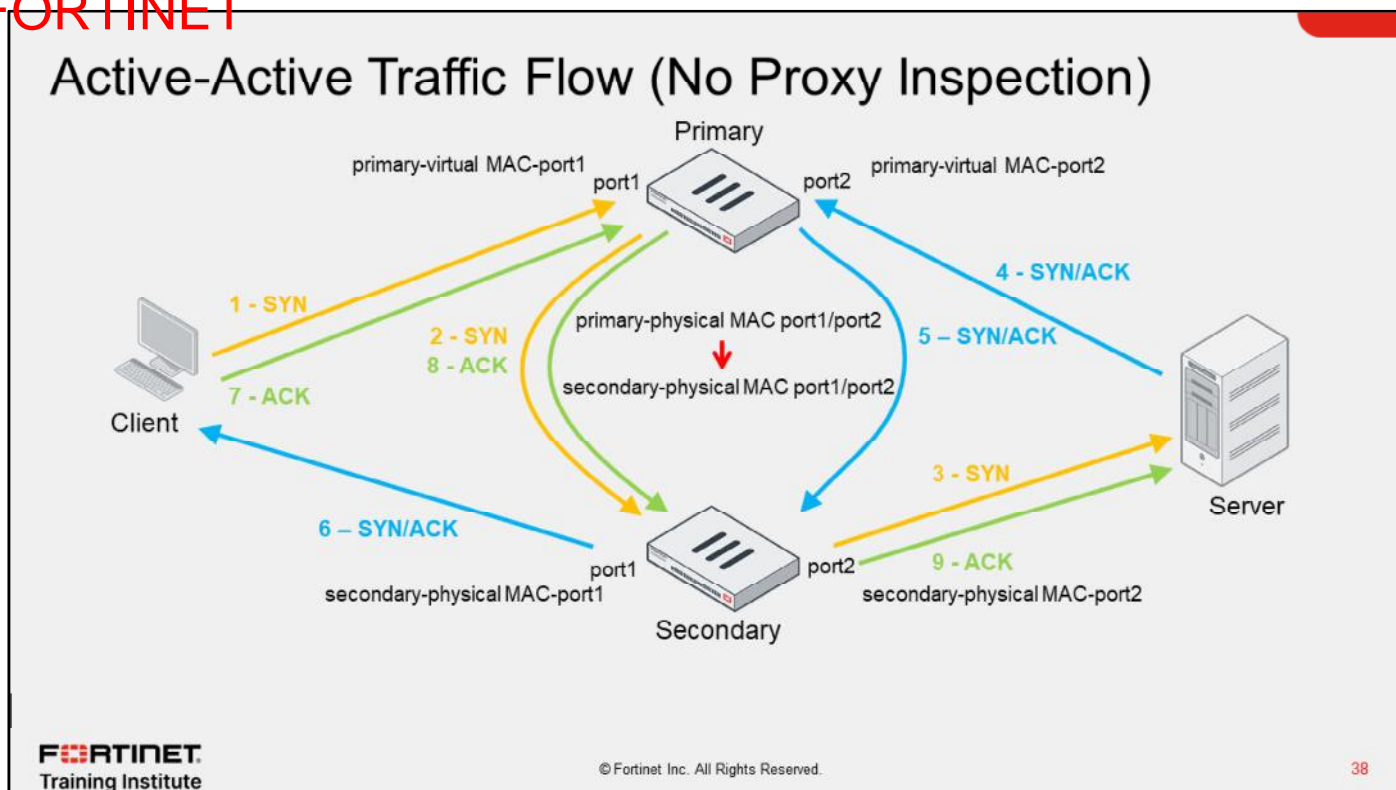
6. srcMAC secondary-physical MAC-port2, dstMAC server, TCP SYN dport 80
7. srcMAC server, dstMAC primary-virtual MAC-port2, TCP SYN/ACK sport 80
8. srcMAC primary-physical MAC-port2, dstMAC secondary-physical MAC-port2, TCP SYN/ACK sport 80
9. srcMAC secondary-physical MAC-port2, dstMAC server, TCP ACK dport 80

6. The secondary starts the connection with the server by sending a SYN packet using the physical MAC address of port2 as the source. Note that FortiGate contacts the server after it finishes the three-way handshake to the client, not before. The same behavior is seen when FortiGate operates in standalone mode and performs proxy-based inspection.
7. The SYN/ACK packet from the server is sent to port2 on the primary. The destination MAC address is the virtual MAC address of port2.
8. The primary receives the packet and knows that it matches a session that was previously distributed to the secondary. The primary forwards the SYN/ACK packet to the corresponding secondary FortiGate. The packet is sourced from the physical MAC address of port2 on the primary and destined to the physical MAC address of port2 on the secondary.
9. The secondary responds to the server with an ACK packet that contains the physical MAC address of port2 on the secondary as the source and the MAC address of the server as the destination.

The three-way handshake on the server side is also complete. From now on, packets that the client sends follow the same flow. For example, an HTTP GET request packet from the client is first received by the primary, which then forwards it to the secondary for proxy-based inspection. If the packet is allowed, the secondary forwards the packet to the server. Any server response packets to the client HTTP GET request are sent to the primary, which then forwards the packets to the secondary for inspection, and so on.

Note that the goal of active-active mode is to leverage unused CPU and memory resources on secondary devices. The intention is not really to load balance traffic. In fact, because the traffic from endpoints is always sent to the primary, you usually see more traffic on the primary than any secondary devices.

DO NOT REPRINT  
© FORTINET



When there is no proxy inspection, that is, when traffic is either subject to flow inspection or no inspection at all, sessions are distributed to the secondary FortiGate only if you enable the `load-balance-all` setting (which is disabled by default) under HA configuration. In addition, as in proxy inspection, you will also see the following behavior:

- Traffic sourced from the client or server and destined to the FortiGate cluster is sent to the primary FortiGate. The source and destination MAC addresses are the endpoint (client or server) and the primary FortiGate virtual MAC address, respectively.
- The primary FortiGate may, in turn, forward the traffic to the secondary if the session is to be load balanced.
- When distributing the traffic to the secondary, FortiGate uses the physical MAC addresses of the primary and secondary devices interfaces as the source and destination MAC addresses, respectively.
- If traffic is load balanced to the secondary FortiGate, any traffic sourced from the cluster and destined to the endpoint is sourced from the secondary FortiGate. This means that the source MAC address is the physical address of the secondary egress interface.

When compared to proxy inspection, the difference is that FortiGate does not reply to packets on behalf of the client or server. For example, instead of replying to the SYN packet that the client sends, FortiGate forwards the packet to the server through the secondary. Similarly, FortiGate forwards packets that the server sends to the client through the secondary.

## Unsupported Sessions for Active-Active Load Balancing

- Sessions that can't be load balanced
  - ICMP, multicast, broadcast, SIP ALG, IM, P2P, and IPsec VPN
  - SSL VPN, HTTP multiplexing, SSL offloading, WAN optimization, explicit web proxy, and WCCP
- HTTPS sessions are not load balanced if they are subject to proxy-based inspection
- HTTPS sessions are load balanced only when `load-balance-all` is enabled and:
  - The inspection mode is set to flow mode, or
  - The inspection mode is set to proxy mode and the HTTPS traffic is not inspected
- Session failover and session load balancing
  - Some sessions can be synced, but not necessarily load balanced
  - For example, ICMP sessions can be synced (`session-pickup-connection` must be enabled) but can't be load balanced

In active-active mode, not all sessions qualify for active-active load balancing. This slide shows a list of sessions that can't be load balanced.

Most of the internet traffic nowadays is HTTPS. For this reason, it is important to understand the limitations for HTTPS traffic load balancing. You must know that HTTPS sessions are not load balanced if they are subject to proxy-based inspection. In fact, the only two scenarios in which HTTPS sessions are load balanced is when the `load-balance-all` setting is enabled and:

- The inspection mode is set to flow mode, or
- The inspection mode is set to proxy mode and the HTTPS traffic is not inspected.

Do not confuse session failover with session load balancing. While some sessions can be synchronized to secondary members for session failover protection, those same sessions aren't necessarily supported for active-active load balancing. For example, ICMP sessions can be synchronized to secondary members if you enable the `session-pickup-connectionless` setting, but they cannot be load balanced.

## Active-Active Load Balancing Methods

Method	Description
none	The primary handles all sessions
leastconnection	Sessions are sent to the member with the least number of sessions
round-robin	Default method. Sessions are distributed equally across members
weight-round-robin	The more weight a member is assigned, the more sessions it handles
random	Sessions are distributed randomly across members
ip hub	Sessions with the same source and destination IP pair are handled by the same member
ipport	Distribution based on source address, source port, destination address, and destination port information

In active-active mode, when the primary device distributes sessions, it uses one of the following load balancing methods:

- `none`: Load balancing is turned off. The primary handles all sessions.
- `leastconnection`: The primary distributes sessions to the member with the least number of sessions.
- `round-robin`: This is the default method. The primary distributes sessions equally across members.
- `weight-round-robin`: The primary distributes sessions across members based on the member weight. The higher the member weight, the more sessions are distributed to that member.
- `random`: The primary distributes sessions randomly across members.
- `ip` and `hub`: The primary distributes sessions with the same source and destination IP pair to the same member. Both methods, `ip` and `hub`, work the same way. Both names in the configuration were kept for legacy compatibility purposes. The `hub` schedule will be removed in a future FortiOS version.
- `ipport`: The primary distributes sessions based on the source address, source port, destination address, and destination port information. The more diverse the traffic is, the more evenly the traffic is distributed across members.

## Active-Active Load Balancing Methods (Contd)

- Configure link health monitor:

```
config system ha
  set schedule none | hub | leastconnection | round-robin | weight-round-robin | random | ip | ipport
end
```

- If using `weight-round-robin`, configure the member weight on the primary FortiGate:

```
config system ha
  set weight <id> <weight>
end
```

- Example—33% of sessions to primary and 67% to secondary

```
# get system ha status
...
Primary: FGVM010000064692, HA operating index = 0
Secondary: FGVM010000065036, HA operating index = 1

# config system ha
# set weight 0 1
# set weight 1 2
# end
```

You set the load balancing method by configuring the `schedule` setting, as shown on this slide.

When you select the `weight-round-robin` method, you must also configure the weight for each member, as shown on this slide. You indicate the member ID followed by its weight. The higher the member weight, the more sessions are distributed to that member. You can obtain the member ID from the output of the `get system ha status` command.

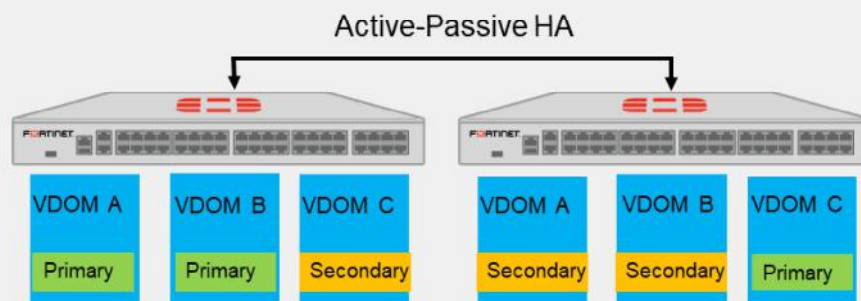
This slide also shows a configuration example for a weight-based distribution of 67% of sessions to the secondary FortiGate and 33% of sessions to the primary device. That is, for every three connections that qualify for load balancing, two of them are distributed to the secondary, and one of them to the primary.

Note that you apply the member weight configuration for all members on the primary device. That is, you don't have to apply the weight on each member individually. The cluster will synchronize the configuration to each member for you.

# DO NOT REPRINT © FORTINET

## Virtual Clustering

- Virtual clusters are an extension of FGCP for FortiGate with multiple VDOMs
  - The HA cluster *must* consist of *only two* FortiGate devices
- Allows FortiGate to be the primary for some VDOMs and the secondary for the other VDOMs



So far, you've learned about HA clustering where each FortiGate device acts as a whole security domain.

But, if you have an HA cluster with multiple VDOMs, you can configure *virtual clusters*.

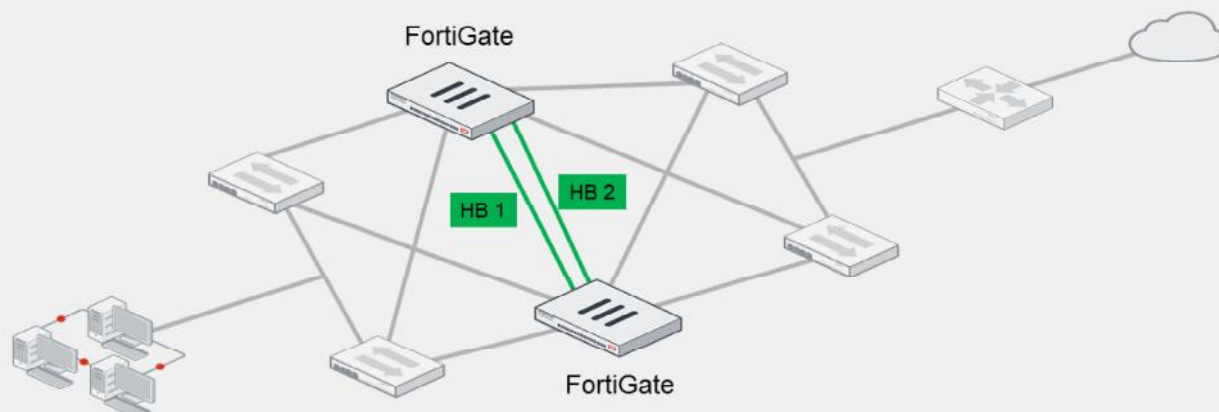
Virtual clusters allow you to have one device acting as the primary for one VDOM, and as the secondary for a different VDOM. Each VDOM has a primary and a secondary FortiGate. Any device can act as the primary for some VDOMs, and the secondary for the other VDOMs, at the same time. Because traffic from different VDOMs can go to different primary FortiGate devices, you can use virtual clustering to manually distribute your traffic between the two cluster devices, and allow the failover mechanism for each VDOM between two FortiGate devices.

Note that you can configure virtual clustering between *only two* FortiGate devices with multiple VDOMs.

# DO NOT REPRINT © FORTINET

## Full Mesh HA

- Eliminates a single point of failure
- Requires redundant or LAG interfaces
  - If using LAG interfaces, the switch must support MCLAG or something similar
  - 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 avoids 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**

## Knowledge Check

1. An HA failover occurs when the link status of a monitored interface on the \_\_\_\_\_ goes down.
  - ✓ A. Primary FortiGate
  - B. Secondary FortiGate
2. In an active-passive HA cluster, you can configure virtual clustering between only \_\_\_\_ FortiGate devices with multiple VDOMs.
  - ✓ A. Two
  - B. Four

DO NOT REPRINT  
© FORTINET

## Lesson Progress

-  HA Operation Modes
-  HA Cluster Synchronization
-  HA Failover and Workload
-  Monitoring and Troubleshooting

Good job! You now understand HA failover and workload.

Now, you will learn about monitoring and troubleshooting an HA cluster.

DO NOT REPRINT  
© FORTINET

## Monitoring and Troubleshooting

### Objectives

- Verify the normal operation of an HA cluster
- Configure an HA management interface
- Upgrade the HA cluster firmware

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

By demonstrating competence in monitoring and troubleshooting, you will be able to make sure the cluster is synchronized properly. You will also learn how to configure and access secondary devices in an HA cluster and how to upgrade the firmware on the HA cluster.

## Checking the HA Status on the GUI

**System > HA**

Local-FortiGate (Primary)      Remote-FortiGate (Secondary)

Status	Priority	Hostname	Serial No.	Role	Uptime	Sessions	Throughput
Synchronized	200	Local-FortiGate	FGVM010000064692	Primary	3d 23h	11	22.00 kbps
Synchronized	100	Remote-FortiGate	FGVM010000065036	Secondary	0s	5	17.00 kbps

**Dashboard > Status**

HA Status

Mode: Active-Active

Group: Training

Primary: Local-FortiGate

Secondary: Remote-FortiGate

Uptime: 03:23:55:59

State Changed: 03:23:54:10

© Fortinet Inc. All Rights Reserved. 47

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, and active sessions.

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.

## Checking the HA Status on the CLI

```
# get system ha status
HA Health Status: OK
Model: FortiGate-VM64-KVM
Mode: HA A-P
Group: 210
Debug: 0
Cluster Uptime: 2 days 21:28:23
Cluster state change time: 2022-04-20 18:28:23
Primary selected using:
<2022/04/20 18:28:23> vcluster-1: SN1 is selected as the primary because its uptime is larger than peer member SN2.
<2022/04/20 16:13:49> vcluster-1: SN2 is selected as the primary because its uptime is larger than peer member SN1.
ses_pickup: enable, ses_pickup_delay=disable
override: disable
Configuration Status:
SN1(updated 4 seconds ago): in-sync
SN2(updated 4 seconds ago): in-sync
System Usage stats:
SN1(updated 4 seconds ago):
sessions=17, average-cpu-user/nice/system/idle=0%/0%/0%/100%, memory=57%
SN2(updated 4 seconds ago):
sessions=1, average-cpu-user/nice/system/idle=0%/0%/0%/100%, memory=56%
...
```

Cluster status, member model, HA mode, and cluster uptime

Latest primary election results and the reason

Configuration sync status

Performance stats of each member

Note: Displayed serial numbers are not real

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. Note that the serial numbers of members have been replaced by fake ones (SN1 and SN2), so the output fits on this slide.

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. The cluster has also been up for almost three days.

Next, you can see the latest primary election events, the result, and the reason. The output indicates that a different member was elected as the primary during the last two election events. In both cases, the member was elected because it had a higher HA uptime.

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.

## Checking the HA Status on the CLI (Contd)

```

...
HBDEV stats:
  SN1(updated 4 seconds ago):
    port9: physical/10000full, up, rx-bytes/packets/dropped/errors=154684218/384596/0/0, tx=352015560/498020/0/0
  SN2(updated 4 seconds ago):
    port9: physical/10000full, up, rx-bytes/packets/dropped/errors=386075683/578563/0/0, tx=269160874/516602/0/0
MONDEV stats:
  SN1(updated 4 seconds ago):
    port1: physical/10000full, up, rx-bytes/packets/dropped/errors=238546316/964449/0/0, tx=13209070/157763/0/0
  SN2(updated 4 seconds ago):
    port1: physical/10000full, up, rx-bytes/packets/dropped/errors=214804265/993451/0/0, tx=6345393/37126/0/0
PINGSVR stats:
  SN1(updated 4 seconds ago):
    port1: physical/10000full, up, rx-bytes/packets/dropped/errors=238546316/964449/0/0, tx=13209070/157763/0/0
    pingsvr: state=up(since 2022/04/20 16:13:50), server=10.9.15.40, ha_prio=5
  SN2(updated 4 seconds ago):
    port1: physical/10000full, up, rx-bytes/packets/dropped/errors=214804265/993451/0/0, tx=6345393/37126/0/0
    pingsvr: state=N/A(since 2022/04/20 16:13:54), server=10.9.15.40, ha_prio=5
Primary   : Local-FortiGate , SN1, HA cluster index = 0
Secondary : Remote-FortiGate, SN2, HA cluster index = 1
number of vcluster: 1
vcluster 1: work 169.254.0.1
Primary: SN1, HA operating index = 0
Secondary: SN2, HA operating index = 1

```

Heartbeat, monitored, and remote link interfaces status

Member role, host name, serial number, and ID

Note: Displayed serial numbers are not real

This slide shows the second part of the example output that the `diagnose 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.

## Checking the Configuration Synchronization

- Display the member checksum:

```
# diagnose sys ha checksum show

is_manage_primary()=1, is_root_primary()=1
debugzone
global: 22 9a 60 e6 65 a9 86 4f e4 a2 d6 13 1c 22 35 94
root:  cb ab 48 ab 62 d3 2c d0 21 d4 ce 6b e8 7d 05 16
all:   98 2b 5a 36 88 aa 76 31 0c 98 11 ff cc d2 0b 11

checksum
global: 22 9a 60 e6 65 a9 86 4f e4 a2 d6 13 1c 22 35 94
root:  cb ab 48 ab 62 d3 2c d0 21 d4 ce 6b e8 7d 05 16
all:   98 2b 5a 36 88 aa 76 31 0c 98 11 ff cc d2 0b 11
```

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

===== FGVM010000112065 =====

is_manage_primary()=1, is_root_primary()=1
debugzone
global: 22 9a 60 e6 65 a9 86 4f e4 a2 d6 13 1c 22 35 94
root:  cb ab 48 ab 62 d3 2c d0 21 d4 ce 6b e8 7d 05 16
all:   98 2b 5a 36 88 aa 76 31 0c 98 11 ff cc d2 0b 11

checksum
global: 22 9a 60 e6 65 a9 86 4f e4 a2 d6 13 1c 22 35 94
root:  cb ab 48 ab 62 d3 2c d0 21 d4 ce 6b e8 7d 05 16
all:   98 2b 5a 36 88 aa 76 31 0c 98 11 ff cc d2 0b 11

===== FGVM010000065036 =====

is_manage_primary()=0, is_root_primary()=0
debugzone
global: 22 9a 60 e6 65 a9 86 4f e4 a2 d6 13 1c 22 35 94
root:  cb ab 48 ab 62 d3 2c d0 21 d4 ce 6b e8 7d 05 16
all:   98 2b 5a 36 88 aa 76 31 0c 98 11 ff cc d2 0b 11

checksum
global: 22 9a 60 e6 65 a9 86 4f e4 a2 d6 13 1c 22 35 94
root:  cb ab 48 ab 62 d3 2c d0 21 d4 ce 6b e8 7d 05 16
all:   98 2b 5a 36 88 aa 76 31 0c 98 11 ff cc d2 0b 11
```

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

## 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.  
<1>   Subsidiary unit FGVM0100000xxxxxx
```

- The CLI connection is made over SSH and Ethernet frames type 0x8893

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.

Note that when you switch to the CLI of another member, FortiGate establishes an SSH session to that member over the heartbeat interface. The SSH session is then encapsulated in Ethernet frames type 0x8893.

## Force a Permanent Secondary Role on the Primary

- Set the primary to have a permanent secondary:

```
Local-FortiGate # execute ha failover set
Caution: This command will trigger an HA failover.
It is intended for testing purposes.
Do you want to continue? (y/n)
```

- A failover occurs, and the device remains as secondary device
  - Use the command for testing, demo, or troubleshooting purposes only
  - Not recommended in production networks
- To view the permanent secondary role status:

```
Local-FortiGate # execute ha failover status
failover status: set
```

- Revert the permanent secondary role state:

```
Local-FortiGate # execute ha failover unset
```

You can set the primary FortiGate to have a permanent secondary role using the `execute ha failover set` command. When you do this, a failover occurs, and the former primary member remains as a secondary member permanently, regardless of the status of other members in the cluster. That is, the impacted member never takes over the cluster even if it's the best candidate for the primary role.

You can revert the permanent secondary role state by running the `execute ha failover unset` command. Note that you should set the primary member to a permanent secondary role for testing, troubleshooting, and demonstration purposes only. Do not use this feature in production networks.

## 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):
- 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 ha
  set ha-mgmt-status enable
  config ha-mgmt-interfaces
    edit 1
      set interface "port10"
      set gateway 192.168.100.254
    next
  end
end
config system interface
  edit "port10"
    set ip 192.168.100.1 255.255.255.0
    set allowaccess ping https ssh snmp
  next
end
```

```
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

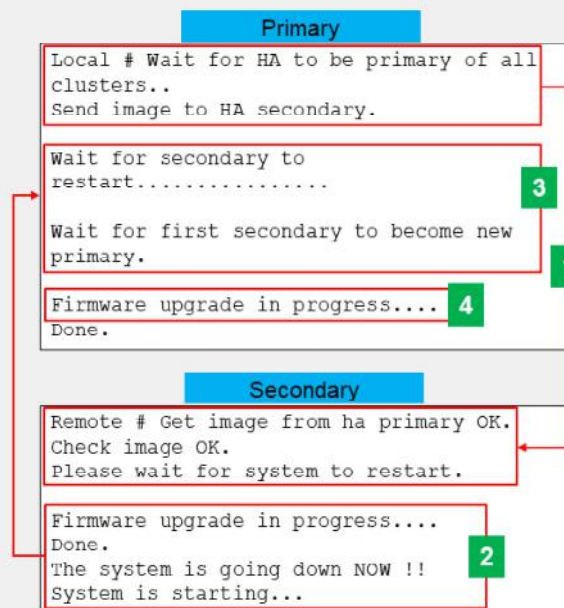
- Apply the new firmware using the GUI or CLI
- Uninterruptible upgrade is enabled by default:

```
config system ha
  set uninterruptible-upgrade enable | disable
end
```

- Firmware upgrade process (uninterruptible upgrade enabled):
  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.
- \*\* Enable the `override` setting on the primary to ensure it takes over the cluster after the firmware upgrade completes.



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, by default, members in a cluster are upgraded one at a time to minimize service disruption. This feature is called uninterruptible upgrade and is enabled by default. After the administrator applies the new firmware on the primary, uninterruptible 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 speed up the firmware upgrade process, you can disable uninterruptible upgrade, as shown on this slide. Just keep in mind this will result in a service impact during the firmware upgrade.





**DO NOT REPRINT**  
**© FORTINET**

## Knowledge Check

1. Which member is the heartbeat interface IP address 169.254.0.1 assigned to?
  - ✓ A. The member with the highest serial number
  - B. The member with the highest priority
2. Which statement about the firmware upgrade process on 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**

## Lesson Progress

-  HA Operation Modes
-  HA Cluster Synchronization
-  HA Failover and Workload
-  Monitoring and Troubleshooting

Congratulations! You have completed this lesson.

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

**DO NOT REPRINT**  
**© FORTINET**

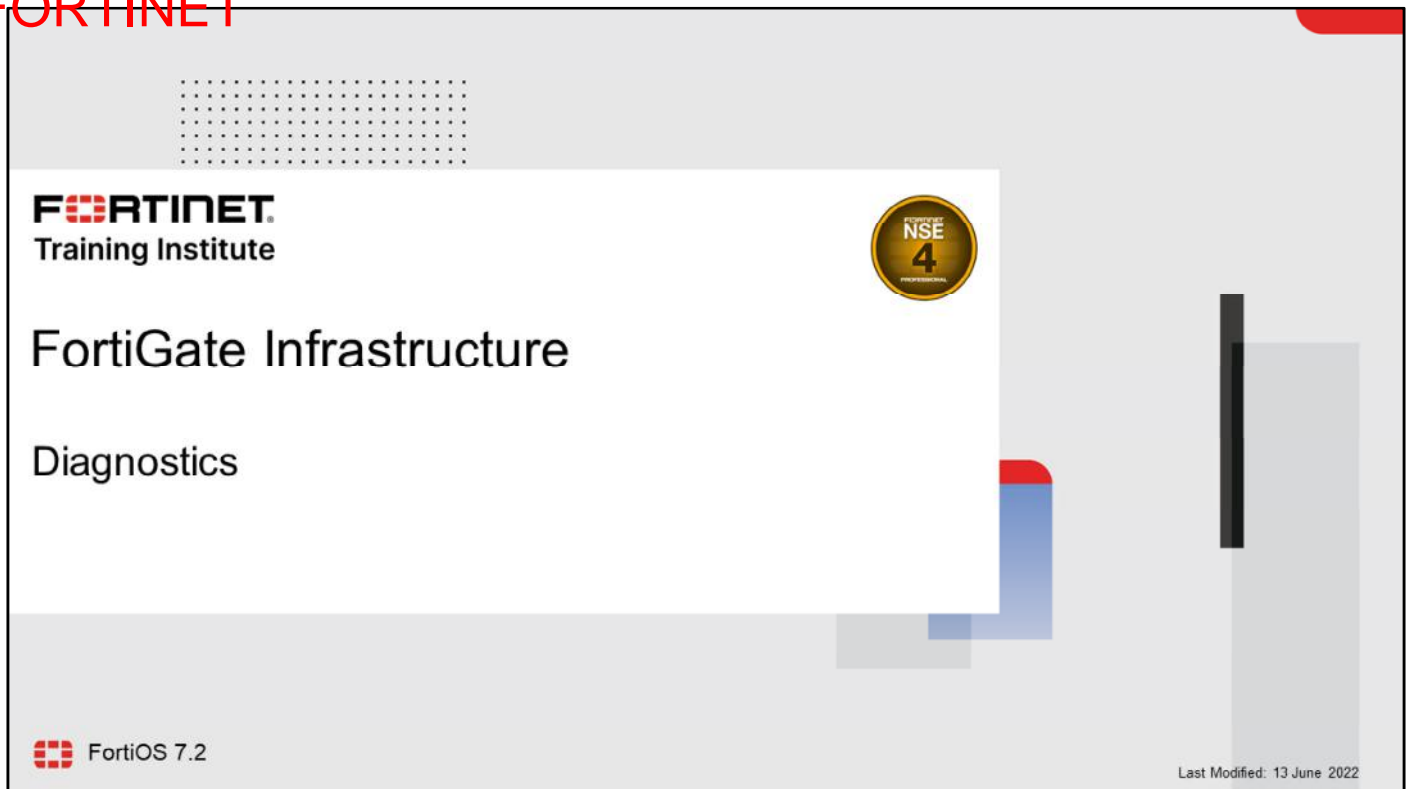
## Review

- ✓ Identify the different operation modes for HA
- ✓ Understand the primary FortiGate election in an HA cluster
- ✓ Identify the primary and secondary device tasks in an HA cluster
- ✓ Identify what is synchronized between HA cluster members
- ✓ Configure session synchronization for seamless failover
- ✓ Identify the HA failover types
- ✓ Interpret how an HA cluster in active-active mode distributes traffic
- ✓ Implement virtual clustering per VDOM in an HA cluster
- ✓ Verify the normal operation of an HA cluster
- ✓ Configure an HA management interface
- ✓ Upgrade the HA cluster firmware

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



The slide features a white background with a grid of dots in the top left corner. The Fortinet logo is in the top left, followed by 'Training Institute'. A gold NSE 4 Professional badge is in the top right. The main title 'FortiGate Infrastructure' and subtitle 'Diagnostics' are centered. The FortiOS 7.2 logo is in the bottom left, and 'Last Modified: 13 June 2022' is in the bottom right. The slide is framed by a grey border with red and blue accents.

**FORTINET**  
Training Institute

NSE  
4  
PROFESSIONAL

FortiGate Infrastructure

Diagnostics

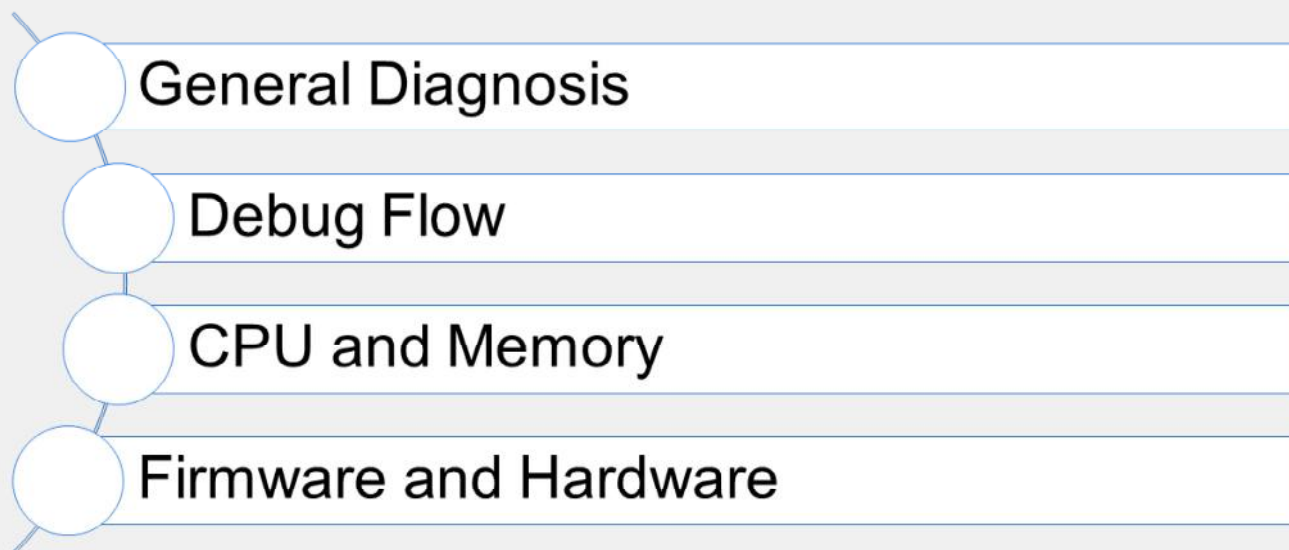
FortiOS 7.2

Last Modified: 13 June 2022

In this lesson, you will learn about using diagnostic commands and tools.

**DO NOT REPRINT**  
**© FORTINET**

## Lesson Overview



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

DO NOT REPRINT  
© FORTINET

## General Diagnosis

### Objectives

- Identify your network's normal behavior
- Monitor for abnormal behavior, such as traffic spikes
- Diagnose problems at the physical and network layers

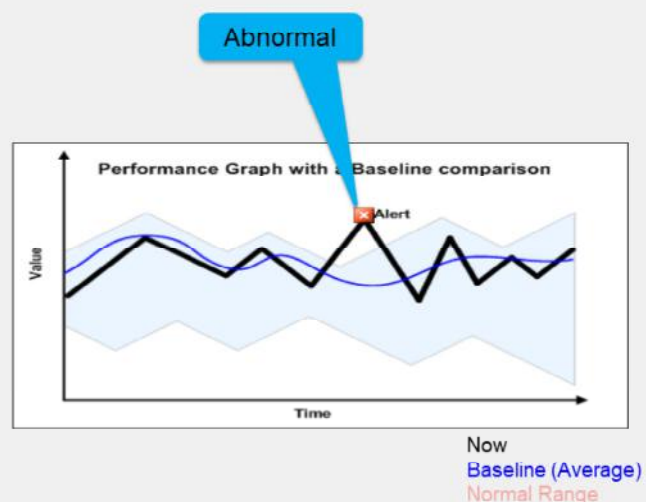
After completing this section, you should be able to achieve the objectives shown on this slide.

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.

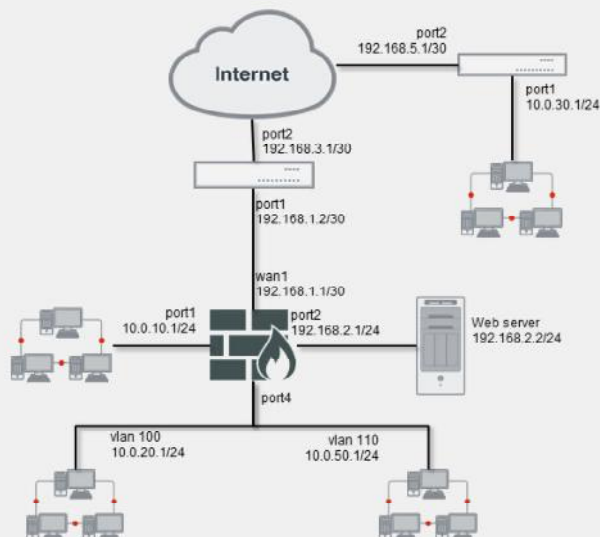
In the graph shown on this slide, the range that indicates *normal* is shown in blue. What exactly is this blue line? It indicates the averages—our baseline. What is the thick black line? It's the current behavior. When the current behavior (black line) leaves the normal range, an abnormal event is happening.

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.

6

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# get system status

```

Version: FortiGate-40F-3G4G v7.2.0,build1157,220331 (GA.F)
Firmware Signature: certified
Virus-DB: 90.01760(2022-04-26 16:26)
Extended DB: 90.01760(2022-04-26 16:26)
AV AI/ML Model: 2.05403(2022-04-26 16:26)
IPS-DB: 20.00304(2022-04-26 00:08)
IPS-ETDB: 0.00000(2001-01-01 00:00)
APP-DB: 20.00304(2022-04-26 00:08)
INDUSTRIAL-DB: 6.00741(2015-12-01 02:30)
IPS Malicious URL Database: 3.00331(2022-04-25 16:10)
IoT-Detect: 0.00000(2001-01-01 00:00)
Serial-Number: FG40F1TKXXXXXX
BIOS version: 05000004
System Part-Number: P24695-03
Log hard disk: Not available
Hostname: FortiGate
Private Encryption: Disable
Operation Mode: NAT
Current virtual domain: root
Max number of virtual domains: 10
Virtual domains status: 1 in NAT mode, 0 in TP mode
Virtual domain configuration: disable
FIPS-CC mode: disable
Current HA mode: standalone
Branch point: 1157
Release Version Information: GA
System time: Wed Apr 27 12:43:57 2022
Last reboot reason: power cycle

```

FortiGate physical  
appliance

FortiGate # get system status

```

Version: FortiGate-VM64-KVM v7.2.0,build1157,220331 (GA.F)
Firmware Signature: certified
Virus-DB: 81.00091(2020-10-14 16:20)
Extended DB: 81.00091(2020-10-14 16:20)
Extreme DB: 1.00000(2018-04-09 16:20)
AV AI/ML Model: 0.00000(2001-01-01 00:00)
IPS-DB: 6.00741(2015-12-01 02:30)
IPS-ETDB: 6.00741(2015-12-01 02:30)
APP-DB: 6.00741(2015-12-01 02:30)
INDUSTRIAL-DB: 6.00741(2015-12-01 02:30)
IPS Malicious URL Database: 2.00797(2020-10-14 05:06)
IoT-Detect: 0.00000(2001-01-01 00:00)
Serial-Number: FGVN010000064692
License Status: Valid
VM Resources: 1 CPU/1 allowed, 2007 MB RAM
Log hard disk: Available
Hostname: FortiGate
Private Encryption: Disable
Operation Mode: NAT
Current virtual domain: root
Max number of virtual domains: 10
Virtual domains status: 1 in NAT mode, 0 in TP mode
Virtual domain configuration: disable
FIPS-CC mode: disable
Current HA mode: standalone
Branch point: 1157
Release Version Information: GA
FortiOS x86-64: Yes
System time: Wed Apr 27 04:16:15 2022
Last reboot reason: shutdown

```

FortiGate VM



© Fortinet Inc. All Rights Reserved.

7

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

## Hardware Interface Information

```
FortiGate # get hardware nic <interface_name>
```

```
Description      :FortiASIC NP6XLITE Adapter
Driver Name      :FortiASIC NP6XLITE Driver
Board           :40Flif
id              :0lif
oid             :64
netdev oid      :64
Current_Hwaddr  e0:23:ff:65:19:c8
Permanent_Hwaddr e0:23:ff:65:19:c8
```

```
===== Link Status =====
```

```
Admin           :up
netdev status   :up
autonego_setting :1
link_setting    :1
speed_setting   :1000
duplex_setting  :0
Speed           :1000
Duplex          :Full
link_status     :Up
```

```
===== Counters =====
```

```
Rx Pkts         :509427
Rx Bytes        :231539694
Tx Pkts         :513489
Tx Bytes        :132128420
Host Rx Pkts    :343935
Host Rx Bytes   :56092804
Host Tx Pkts    :365879
Host Tx Bytes   :51129548
Host Tx dropped :0
FragTxCreate    :0
FragTxOk        :0
FragTxDrop     :0
```

FortiGate physical interface

**FORTINET**  
Training Institute

© Fortinet Inc. All Rights Reserved.

8

At the physical layer, troubleshooting analyzes which ports are plugged in, media capacity, and negotiated speed and duplex mode.

At the data link layer, diagnostics often analyze how many frames are being dropped because of CRC errors or collisions.

*The get hardware nic* command is used to display the FortiGate interface hardware and status information. The output might vary depending on the model and NIC driver version.

DO NOT REPRINT  
© FORTINET

## Hardware Interface Information (Contd)

```
FortiGate # get hardware nic <interface_name>
```

```
Name:          port1
Driver:        virtio_net
Version:       1.0.0
Bus:           0000:00:03.0
Hwaddr:        02:09:0f:00:00:00
Permanent Hwaddr: 02:09:0f:00:00:00
State:         up
Link:          up
Mtu:           1500
Supported:     1000full 10000full
Advertised:
Speed:         10000full
Auto:          disabled
RX Ring:       256
TX Ring:       256
Rx packets:    670785
Rx bytes:      949908714
Rx compressed: 0
Rx dropped:    0
...
```

```
...
Rx errors:     0
  Rx Length err: 0
  Rx Buf overflow: 0
  Rx Crc err:   0
  Rx Frame err: 0
  Rx Fifo overrun: 0
  Rx Missed packets: 0
Tx packets:    57752
Tx bytes:      4993066
Tx compressed: 0
Tx dropped:    0
Tx errors:     0
  Tx Aborted err: 0
  Tx Carrier err: 0
  Tx Fifo overrun: 0
  Tx Heartbeat err: 0
  Tx Window err: 0
Multicasts:    0
Collisions:    0
```

The output on this slide shows the driver name, hardware address, administrative status, and link status, along with send and receive packets and errors.

DO NOT REPRINT  
© FORTINET

## ARP Table

```
# get system arp
```

Address	Age (min)	Hardware Addr	Interface
10.0.1.10	0	00:0c:29:e0:c1:87	port3
10.200.1.254	0	00:0c:29:1c:28:d7	port1

Connecting device IP address and MAC address

FortiGate Interface

**FORTINET**  
Training Institute

© Fortinet Inc. All Rights Reserved.

10

If you suspect that there is an IP address conflict, or that an IP has been assigned to the wrong device, you may need to look at the ARP table. The `get system arp` command is used for that purpose. It shows the FortiGate interface, IP address, and associated MAC address. This command lists the information for all external devices connected to the same LAN segments where FortiGate is connected. The current IP and MAC addresses of FortiGate are not included.

**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 <ip> IP address or domain name

# execute traceroute <dest> IP address or hostname
```

Say that FortiGate can contact some hosts through port1, but not others. Is the problem in the physical layer or the link layer? Neither. Connectivity has been proven with at least part of the network. Instead, you should check the network layer. To test this, as usual, start with ping and traceroute.

The same commands exist for IPv6: `execute ping` becomes `execute ping6`, for example.

Remember: location matters. Tests are accurate only if you use the same path as the traffic that you are troubleshooting. To test from FortiGate (to FortiAnalyzer or FortiGuard, for example), use the FortiGate `execute ping` and `execute traceroute` CLI commands. But, to test the path through FortiGate, also use `ping` and `tracert` or `traceroute` from the endpoint—from the Windows, Linux, or Mac OS X computer—not only from the FortiGate CLI.

Because of NAT and routing, you might need to specify a different ping source IP address—the default address is the IP of the outgoing interface. If there is no response, verify that the target is configured to reply to ICMP echo requests.

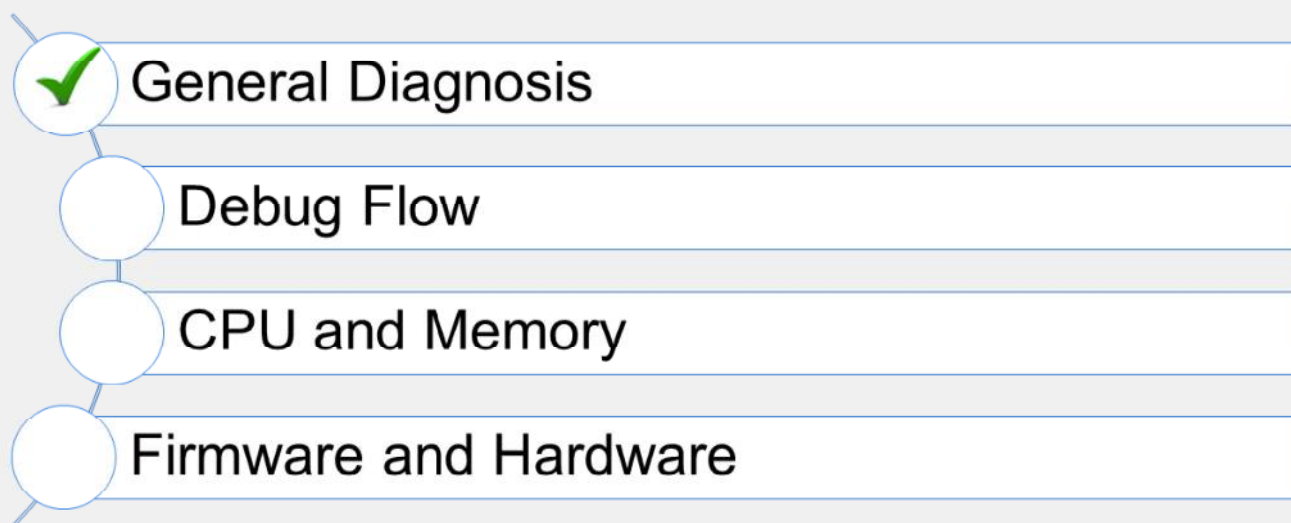
**DO NOT REPRINT**  
**© FORTINET**

## Knowledge Check

1. Which CLI command can be used to determine the MAC address of a FortiGate default gateway?
  - ✓ A. `get system arp`
  - B. `get hardware nic`
2. Which CLI command can be used to diagnose a physical layer problem?
  - A. `execute traceroute`
  - ✓ B. `get hardware nic`

DO NOT REPRINT  
© FORTINET

## Lesson Progress



Good job! You now understand general diagnostics.

Now, you will learn about debug flow.

DO NOT REPRINT  
© FORTINET

## Debug Flow

### Objectives

- Diagnose connectivity problems using the debug flow

**FORTINET**  
Training Institute

14

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

By demonstrating competence in the debug flow, you will be able to diagnose connectivity problems.

**DO NOT REPRINT  
© FORTINET**

## Debug Flow

- Shows what the CPU is doing, step-by-step, with the packets
  - If a packet is dropped, it shows the reason
- Multi-step command
  1. Define a filter: `diagnose debug flow filter <filter>`
  2. Enable debug output: `diagnose debug enable`
  3. Start the trace: `diagnose debug flow trace start <xxx> Repeat number`
  4. Stop the trace: `diagnose debug flow trace stop`

If FortiGate is dropping packets, can a packet capture (sniffer) be used to identify the reason? To find the cause, you should use the debug (packet) flow.

The debug flow shows, step-by-step, how the CPU is handling each packet.

To use the debug flow, follow these steps:

1. Define a filter.
2. Enable debug output.
3. Start the trace.
4. Stop the trace when it's finished.

# DO NOT REPRINT © FORTINET

## Debug Flow Example—SYN

```
#diagnose debug flow filter addr 66.171.121.44
#diagnose debug flow filter port 80
#diagnose debug flow trace start 20
#diagnose debug enable
```

```
id=2 line=4677 msg="vd-root received a packet(proto=6,
10.0.1.10:49886->66.171.121.44:80) from port3. flag [S], seq 2176715501,
ack 0, win 8192"
```

IP addresses, port numbers,  
and incoming interface

```
id=2 line=4831 msg="allocate a new session-00007fc0"
```

Create a new  
session

```
id=2 line=2582 msg="find a route: flag=04000000
gw-10.200.1.254 via port1"
```

Found a matching route.  
Shows next-hop IP address  
and outgoing interface

```
id=2 line=699 msg="Allowed by Policy-1: SNAT"
```

Matching firewall  
policy

```
id=2 line=2719 msg="SNAT 10.0.1.10->10.200.1.1:49886"
```

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

```
id=2 line=4677 msg="vd-root received a packet(proto=6,
66.171.121.44:80->10.200.1.1:49886) from port1. flag [S.],
seq 3567496940, ack 2176715502, win 5840"
```

IP addresses, port numbers,  
and incoming interface

```
id=2 line=4739 msg="Find an existing session,
id-00007fc0,reply direction"
```

Using an existing session

```
id=2 line=2733 msg="DNAT 10.200.1.1:49886->10.0.1.10:49886"
```

Destination NAT

```
id=2 line=2582 msg="find a route: flag=00000000 gw-10.0.1.10 via port3"
```

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 CLL.

Number of packets: 100

Filters

Filter type: Basic | Advanced

IP type: IPv4 | IPv6

IP address: 8.8.8.8

Port: 8.8.8.8

Protocol: ICMP

Start debug flow

Select a protocol or Any

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 CLL.

Number of packets: 100

Filters

Filter type: Basic | Advanced

IP type: IPv4 | IPv6

Source IP: 10.0.1.10

Source port:

Destination IP: 8.8.8.8

Destination port:

Protocol: ICMP

Start debug flow

Select source IP address, source port, destination IP address, destination port, and protocol

**FORTINET**  
Training Institute

© Fortinet Inc. All Rights Reserved.

18

The Debug Flow tool allows you to view debug flow output on the GUI in real time until you stop the debug process.

This tool helps you to examine the packet flow details directly on the GUI.

After you stop the debug flow, you can view the completed output, and filter it by time, message, or function. You can also export the output as a CSV file.

You can set up the Debug Flow tool to use either Basic or Advanced filter options. **Basic** allows you to filter using basic criteria such as host address, port number, and protocol name. **Advanced** allows you to filter by source IP address, source port, destination IP address, destination port, and protocol.

DO NOT REPRINT  
© FORTINET

## Debug Flow—GUI (Contd)

- Real Time Analysis
  - Embedded real-time analysis page
  - Save and download the packet trace output as a CSV file

### Real-time flow output

```

Packet Capture  Debug Flow
Capturing Packets
07:08:02 165 vd-root0 received a packet(proto=1, 10.0.1.10:2480->8.8.8.8:2048) tun_id=0.0.0.0 from port3, type=8, code=0, id=2480, seq=7.
07:08:02 165 allocate a new session-0000513b, tun_id=0.0.0.0
07:08:02 165 In [port3], out []
07:08:02 165 len=0
07:08:02 165 result: skb_flag=02000000, vid=0, ret=no-match, act=accept, flag=00000000
07:08:02 165 find a route: flag=04000000 gw=10.200.1.254 via port1
07:08:02 165 In [port3], out [port1], skb_flag=02000000, vid=0, app_id=0, uri_cat_id=0
07:08:02 165 gnum=100004, use addr/first hash, len=2
07:08:02 165 checked gnum=100004 policy=1, ret=no-match, act=accept
07:08:02 165 checked gnum=100004 policy=0, ret=matched, act=accept
07:08:02 165 ret=matched
07:08:02 165 policy=0 is matched, act=drop
07:08:02 165 after (prope_captive_check): is_captive=0, ret=matched, act=drop, idx=0
07:08:02 165 after (prope_captive_check): is_captive=0, ret=matched, act=drop, idx=0
07:08:02 165 Denied by forward policy check (policy 0)
  
```

Embedded real-time analysis

### Packet Trace output

Time #	Message #
07:08:01	vd-root0 received a packet(proto=1, 10.0.1.10:2480->8.8.8.8:2048) tun_id=0.0.0.0 from port3, type=8, code=0, id=2480, seq=7.
07:08:01	allocate a new session-0000513b, tun_id=0.0.0.0
07:08:01	In [port3], out []
07:08:01	len=0
07:08:01	result: skb_flag=02000000, vid=0, ret=no-match, act=accept, flag=00000000
07:08:01	find a route: flag=04000000 gw=10.200.1.254 via port1
07:08:01	In [port3], out [port1], skb_flag=02000000, vid=0, app_id=0, uri_cat_id=0
07:08:01	gnum=100004, use addr/first hash, len=2
07:08:01	checked gnum=100004 policy=1, ret=no-match, act=accept
07:08:01	checked gnum=100004 policy=0, ret=matched, act=accept
07:08:01	ret=matched
07:08:01	policy=0 is matched, act=drop
07:08:01	after (prope_captive_check): is_captive=0, ret=matched, act=drop, idx=0
07:08:01	after (prope_captive_check): is_captive=0, ret=matched, act=drop, idx=0
07:08:01	Denied by forward policy check (policy 0)

Packet Trace output after you click Stop Debug Flow

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.

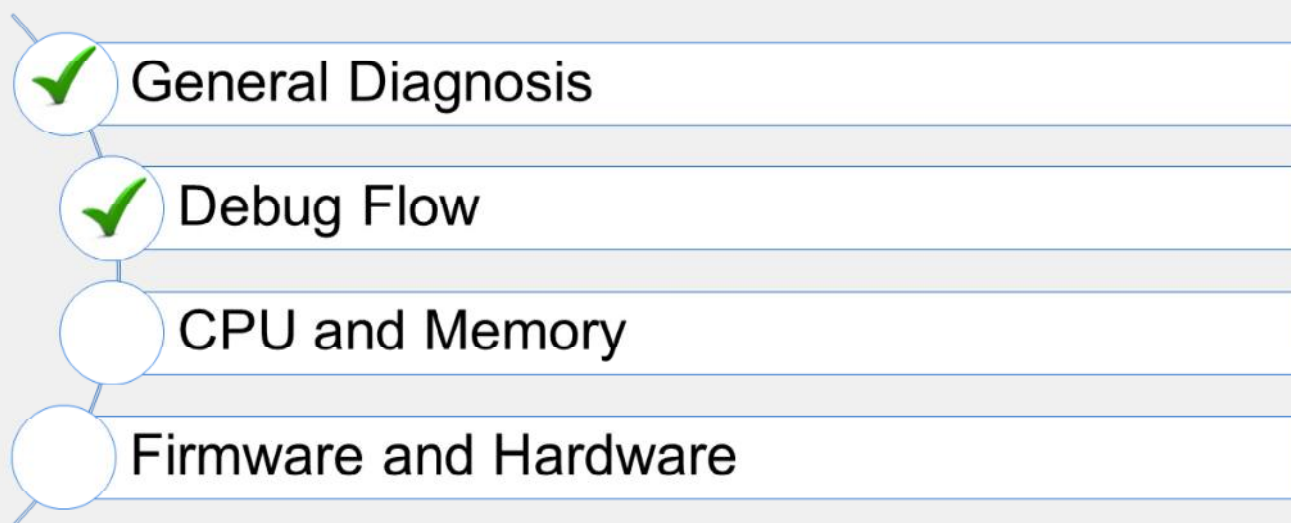
**DO NOT REPRINT**  
**© FORTINET**

## 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 allowed
  - B. When a SYN/ACK packet is allowed

DO NOT REPRINT  
© FORTINET

## Lesson Progress



Good job! You now understand debug flow.

Now, you will learn about FortiGate CPU and memory diagnosis.

DO NOT REPRINT  
© FORTINET

## CPU and Memory

### Objectives

- Diagnose resource problems, such as high CPU or memory usage
- Diagnose memory conserve mode
- Diagnose fail-open session mode

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

By demonstrating competence in CPU and memory, you will be able to diagnose the most common CPU and memory problems.

DO NOT REPRINT  
© FORTINET

## Slowness

- High CPU usage
- High memory usage
  
- What was the last feature you enabled?
  - Enable one at a time
  
- How high is the CPU usage? Why?
  - # get system performance status
  - # diagnose sys top 1

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

```
# 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  
(%)

**FORTINET**  
Training Institute

© Fortinet Inc. All Rights Reserved.

24

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
- `reportd`
- `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`.

## 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.

## 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, but FortiGate tries to make the existing sessions work in the same way as non-conserve mode

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, but allow FortiOS to try to make the existing sessions work in the same way as non-conserve mode.

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.

## 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: on
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
```

Off = no conserve mode  
on = conserve mode

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 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

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.

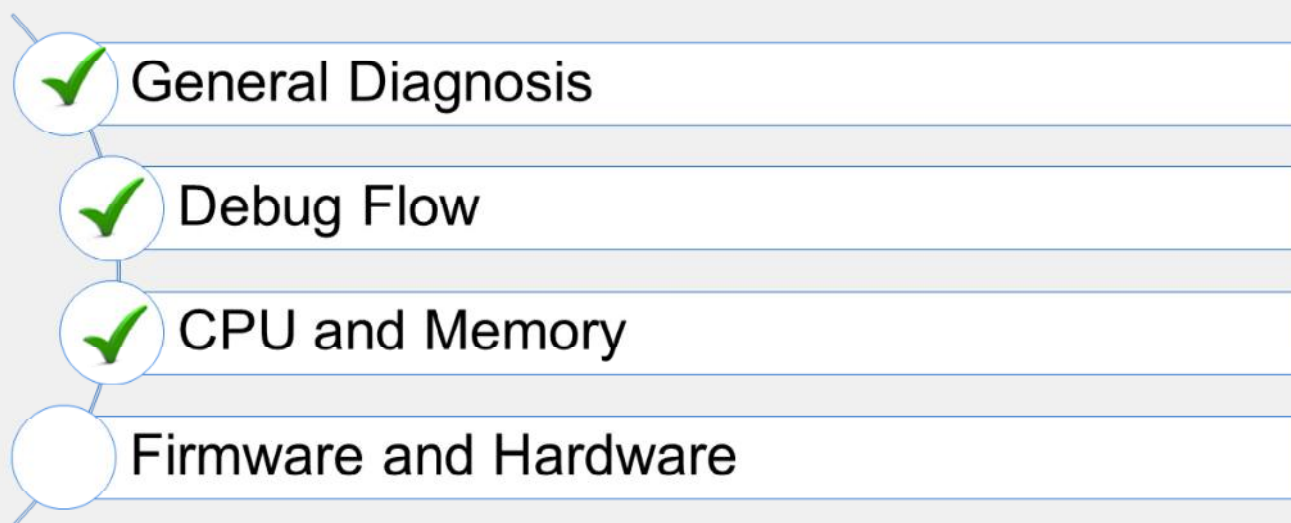
**DO NOT REPRINT**  
**© FORTINET**

## Knowledge Check

1. Which action does FortiGate take during memory conserve mode?
  - ✓ A. Configuration changes are not allowed.
  - B. Administrative access is denied.
2. Which threshold is used to determine when FortiGate enters conserve mode?
  - A. Green
  - ✓ B. Red

DO NOT REPRINT  
© FORTINET

## Lesson Progress



Good job! You now understand FortiGate CPU and memory diagnosis.

Now, you will learn about FortiGate firmware and hardware diagnosis.

DO NOT REPRINT  
© FORTINET

## Firmware and Hardware

### Objectives

- Format the flash memory
- Load a firmware image from the BIOS menu
- Run hardware tests
- Display crash log information

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

By demonstrating competence in firmware and hardware, you will be able to diagnose the most common firmware and hardware problems.

**DO NOT REPRINT**  
**© FORTINET**

## Access to BIOS Menu

```
FortiGate-81E-POE (12:25-10.04.2016)
```

```
ver:05000003
```

BIOS version. Options in the BIOS menu depend on the version

```
Serial number: FG81EPxxxxxxxxxx
```

```
CPU: 1000MHz
```

```
Total RAM: 2 GB
```

```
Initializing boot device...
```

```
Initializing MAC... nplite#0
```

```
Please wait for OS to boot or press any key to display configuration menu
```

```
[C]: Configure TFTP parameters.
[R]: Review TFTP parameters.
[T]: Initiate TFTP firmware transfer.
[F]: Format boot device.
[I]: System information.
[B]: Boot with backup firmware and set as default.
[Q]: Quit menu and continue to boot.
[H]: Display this list of options.
```

Press any key at this prompt to enter the BIOS menu

```
Enter C,R,T,F,I,B,Q, or H:
```

**FORTINET**  
 Training Institute

© Fortinet Inc. All Rights Reserved.

33

On the FortiGate BIOS, administrators can run some operations over the flash memory and firmware images. To access the BIOS menu, you must reboot the device while connected to the console port. The booting process, at one point, shows the following message:

Press any key to display configuration menu

While this prompt is displayed, press any key to interrupt the booting process and display the BIOS menu. In the BIOS menu, you can see the options shown on this slide.

DO NOT REPRINT  
© FORTINET

## Firmware Installation From Console

Make sure that a TFTP server application is installed on your PC

Configure the TFTP server directory and copy the FortiGate firmware [image.out]

Connect your PC NIC to the FortiGate TFTP install interface

Select `get firmware image` from the BIOS menu

After reformatting the flash memory, you must install the firmware image from the BIOS menu. Follow these steps:

1. Run a TFTP server.
2. Configure the TFTP server with the folder where the firmware image file is stored.
3. Connect the PC Ethernet port to the FortiGate TFTP installation interface.
4. Select `get firmware image` from the BIOS menu.

The interface assigned as the TFTP installation interface depends on the model. However, and in most cases, it is either the *port1* or *internal* interface.

DO NOT REPRINT  
© FORTINET

## Format Flash Memory

```
[C]: Configure TFTP parameters.  
[R]: Review TFTP parameters.  
[T]: Initiate TFTP firmware transfer.  
[F]: Format boot device.  
[I]: System information.  
[B]: Boot with backup firmware and set as default.  
[Q]: Quit menu and continue to boot.  
[H]: Display this list of options.
```

Enter C,R,T,F,I,B,Q,or H: F

```
All data will be erased,continue:[Y/N]?  
Formatting boot device...  
.....  
Format boot device completed.
```

Recommended for a clean installation and problems possibly related to corrupted firmware

CAUTION: Formatting the flash memory deletes the firmware, configuration, and digital certificates

**FORTINET**  
Training Institute

© Fortinet Inc. All Rights Reserved.

35

From the BIOS menu, select **F** to format the flash memory.

Doing this might be required if the firmware gets corrupted, or if the administrator wants to do a clean installation of new firmware. Keep in mind, though, that formatting the flash memory deletes any information stored on it, such as firmware images, configuration, and digital certificates.

DO NOT REPRINT  
© FORTINET

## Configure TFTP Parameters

Enter C,R,T,F,I,B,Q, or H: C

[P]: Set firmware download port.  
[D]: Set DHCP mode.  
[I]: Set local IP address.  
[S]: Set local subnet mask.  
[G]: Set local gateway.  
[V]: Set local VLAN ID.  
[T]: Set remote TFTP server IP address.  
[F]: Set firmware file name.  
[E]: Reset TFTP parameters to factory defaults.  
[R]: Review TFTP parameters.  
[N]: Diagnose networking(ping).  
[Q]: Quit this menu.  
[H]: Display this list of options.

Enter P,D,I,S,G,V,T,F,E,R,N,Q, or H:

From the BIOS menu, select C to configure TFTP parameters. Use the menu options to configure parameters, such as local IP address, subnet mask, gateway address, and firmware file name.

**DO NOT REPRINT**  
**© FORTINET**

## FortiGate and TFTP Server Configuration Settings

Enter P,D,I,S,G,V,T,F,E,R,N,Q, or H: R

```
Image download port:  MGMT
DHCP status:         Disabled
Local VLAN ID:      <NULL>
Local IP address:   192.168.1.99
Local subnet mask:  255.255.255.0
Local gateway:     192.168.1.1
TFTP server IP address: 192.168.1.1
Firmware file name: image.out
```

FortiGate TFTP settings

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

Obtain an IP address automatically

Use the following IP address:

IP address:

Subnet mask:

Default gateway:

Obtain DNS server address automatically

Use the following DNS server addresses:

Preferred DNS server:

Alternate DNS server:

Validate settings upon exit

Advanced...

OK Cancel

TFTP server IP address configuration

**FORTINET**  
 Training Institute

© Fortinet Inc. All Rights Reserved.

37

Press R to review the TFTP configuration settings.

After you have configured the TFTP parameters, press Q to return to the main configuration menu.

**DO NOT REPRINT**  
**© FORTINET**

## BIOS Firmware Transfer

**CAUTION: Transferring a firmware image deletes the configuration and installs the factory default configuration**

```

Enter C,R,T,F,I,B,Q,or H: T

Enter TFTP server address []: 192.168.1.1
Enter local address []:192.168.1.99
Enter firmware image file name []:image.out
MAC:00090FC371BE
#####
Total 23299683 bytes data downloaded.
Verifying the integrity of the firmware image.

Total 40000kB unzipped.
Save as Default firmware/Backup firmware/Run image without saving:[D/B/R]? D
Programming the boot device now.
.....
Reading boot image 1375833 bytes.
Initializing firewall...
System is started.
Formatting shared data partition ... done!

```

**FORTINET**  
 Training Institute

© Fortinet Inc. All Rights Reserved.

38

From the BIOS menu, press **T** to initiate the TFTP firmware transfer.

The BIOS requires you to enter:

- The IP address of the TFTP server
- The FortiGate IP address (it must be in the same class-C subnet as the TFTP server)
- The name of the firmware image

If everything is OK, you should see a series of pound signs, indicating that the device is downloading the image. The BIOS will then verify the integrity of the file and give you the following three options:

- Save it as the default firmware
- Save it as the backup firmware
- Run the image without saving it

If the firmware is going to be used in production, select the first option: Save it as the default firmware.

The last option (Run the image without saving it) allows you to run and test firmware without overwriting any existing firmware in the memory. After you have finished the tests and are ready to roll back the change, you must reboot the device, and the previously existing firmware will be used.

DO NOT REPRINT  
© FORTINET

## Hardware Tests

- Designed for both manufacturing testing and for end users to verify major hardware components:
  - CPU
  - RAM memory
  - Network interfaces
  - Hard disk
  - Flash memory
  - USB interface
  - Front panel LEDs
  - Wi-Fi
  - And so on

As with any other electronic device, damage to RAM can cause intermittent crashes.

If you suspect hardware failure, you can run hardware tests.

How do you run the hardware tests? It depends on the FortiGate model.

**DO NOT REPRINT**  
**© FORTINET**

## How to Run the Hardware Tests

- In some E,F, and D-series models, the hardware tests can be run directly from FortiOS
  - Can run a single test, or multiple tests
- For other models, a special HQIP image must be loaded using TFTP and run from the BIOS menu
  - Instructions: <https://support.fortinet.com/Download/HQIPImages.aspx>

For some FortiGate E, F, and D-series models, you can run the hardware tests directly from the FortiOS CLI.

For other models, you must download special HQIP hardware testing images from the Fortinet Technical Support website.

The steps for uploading the hardware test image are the same as the ones used for uploading a firmware image. You can run the hardware test image without saving it in the flash memory, so any existing firmware image won't be overwritten.

**DO NOT REPRINT**  
**© FORTINET**

## FortiOS Hardware Tests Command

```
# diagnose hardware test suite all
```

```
- Please connect ethernet cables:
```

```
[WAN - Any of PORT1...PORT4]
```

```
To skip this test, please press 'N'.
```

```
Do you want to continue? (y/n) (default is n) N
```

```
Following tests will request you to check the colours of the system LEDs.
```

```
To skip this test, please press 'N'.
```

```
Do you want to continue? (y/n) (default is n) N
```

```
Following tests will request you to check the colours of the NIC LEDs.
```

```
- Please connect ethernet cables:
```

```
[WAN - Any of PORT1...PORT4]
```

```
To skip this test, please press 'N'.
```

```
Do you want to continue? (y/n) (default is n) N
```

```
Test Begin at UTC Time Wed May 05 21:08:53 2021
```

For some models, the command `diagnose hardware test suite all` runs the hardware tests from FortiOS. The hardware tests require user interaction while running. Users can skip some of the steps. Some tests require connecting external devices (such as USB flash drives) or network cables to FortiGate.

# DO NOT REPRINT © FORTINET

## Crash Logs

- Inspect crash logs for debugging purposes
- Any time a process closes, it is recorded as *killed*
  - Some are normal (for example, closing `scanunit` to update definitions)

```
# diagnose debug crashlog history
Crash log interval is 3600 seconds
httpsd crashed 1 times. The last crash was at 2022-06-03 02:31:34

# diagnose debug crashlog read
97: 2022-05-24 01:59:31 from=license sn=FGVM010000060036 msg=License status changed to VALID
98: 2022-06-03 02:31:34 Signal <11> was sent to process <31308> by user <admin>
99: 2022-06-03 02:31:34 <31308> firmware FortiGate-VM64-KVM v7.2.0,build1157b1157,220331 (GA.F)
100: 2022-06-03 02:31:34 <31308> application httpsd
101: 2022-06-03 02:31:34 <31308> *** signal 11 (Segmentation fault) received ***
102: 2022-06-03 02:31:34 <31308> Register dump:
103: 2022-06-03 02:31:34 <31308> RAX: 000000000000002b   RBX: 0000000000000000
```

The https process was restarted by the administrator

Another area you might want to monitor, purely for diagnostics, is the crash logs. Crash logs are available through the CLI.

Any time a process is closed for any reason, the crash log records this as a crash. Most of the logs in the crash log are normal. For example, any time the antivirus definitions package is updated, the `scanunit` process needs to close down in order to apply the new package. This is a normal shutdown. Some logs in the crash log shows they are initiated by a user, which indicates the administrator manually restarted a process.

Some logs in the crash log might indicate problems. For that reason, the crash logs are frequently requested by Fortinet Technical Support for troubleshooting purposes.

This slide shows the commands you have to use to get a crash log. The crashlog output shows the http process is restarted by the administrator.

Two commands can show information from the crash logs:

- `diagnose debug crashlog history` lists a summary of the processes that have crashed, how many crashes have happened, and the time of the last crash.
- `diagnose debug crashlog read` provides details about each crash, in addition to other system events, such as conserve mode entry and exit times.

DO NOT REPRINT  
© FORTINET

## Conserve Mode Events in Crash Logs

- The crash log also records conserve mode events

- Entering:

```
12: 2021-04-06 14:10:16 logdesc="Kernel enters conserve mode" service=kernel  
conserve-on free="127962"
```

```
13: 2021-04-06 14:10:16 pages" red="128000 pages" msg="Kernel enters conserve  
mode"
```

- Exiting:

```
14: 2021-04-06 14:19:55 logdesc="Kernel leaves conserve mode" service=kernel  
conserve=exit
```

```
15: 2021-04-06 14:19:55 free="192987 pages" green="192000 pages" msg="Kernel  
leaves conserve mode"
```

This slide shows the entries generated in the crash logs when FortiGate enters and exits memory conserve mode.





**DO NOT REPRINT**  
**© FORTINET**

## Knowledge Check

1. Which types of information are stored in the crash log?
  - ✓ A. Process crashes and conserve mode events
  - B. Traffic logs and security logs
2. Which protocol is used to upload new firmware from the console?
  - A. HTTP/HTTPS
  - ✓ B. TFTP

**DO NOT REPRINT**  
**© FORTINET**

## Lesson Progress

-  General Diagnosis
-  Debug Flow
-  CPU and Memory
-  Firmware and Hardware

Congratulations! You have completed the lesson.

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

**DO NOT REPRINT**  
**© FORTINET**

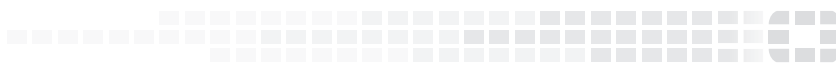
## Review

- ✓ Identify the normal behavior of your network
- ✓ Monitor for abnormal behavior, such as traffic spikes
- ✓ Diagnose problems at the physical and network layers
- ✓ Diagnose connectivity problems using the debug flow
- ✓ Diagnose resource problems, such as high CPU or memory usage
- ✓ Diagnose memory conserve mode
- ✓ Diagnose fail-open session mode
- ✓ Format the flash memory
- ✓ Load a firmware image from the BIOS menu
- ✓ Run hardware tests
- ✓ Display crash log information

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.

DO NOT REPRINT  
© 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© 2022 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.