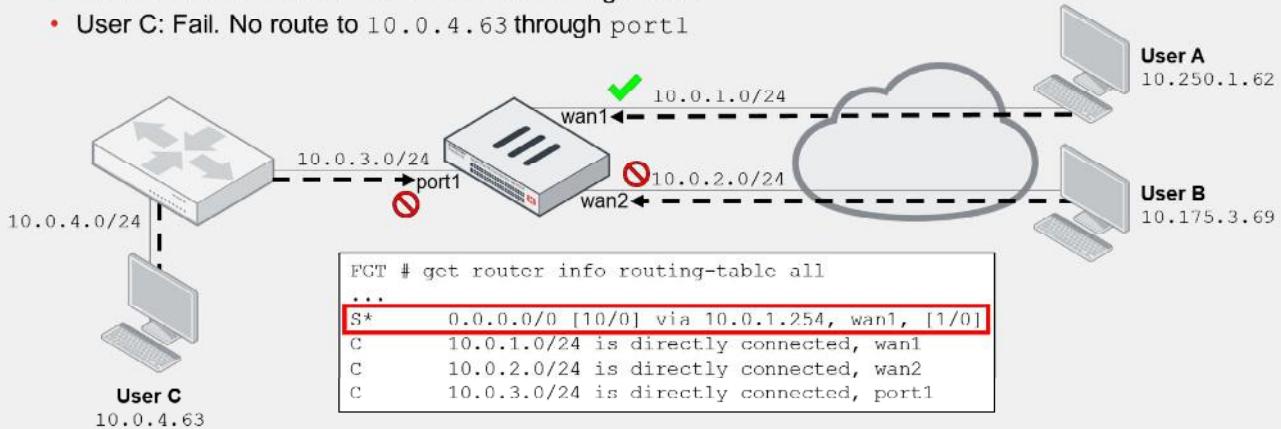


**DO NOT REPRINT**

**© 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:

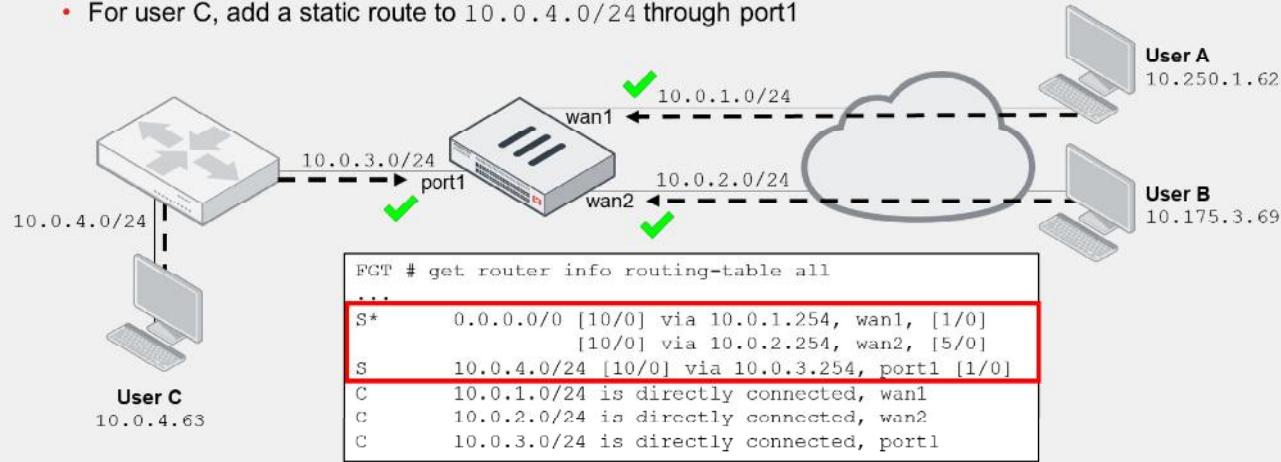
- User A: Pass. There is a default route through wan1. This means that, all packets received at wan1 pass the RPF check regardless of the source address.
- User B: Fail. FortiGate doesn't have a route to 10.175.3.69 through wan2 in its routing table.
- User C: Fail. Like the user B case, FortiGate doesn't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



If you consider the packets from user B and user C to be legit packets, you can solve the RPC 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.

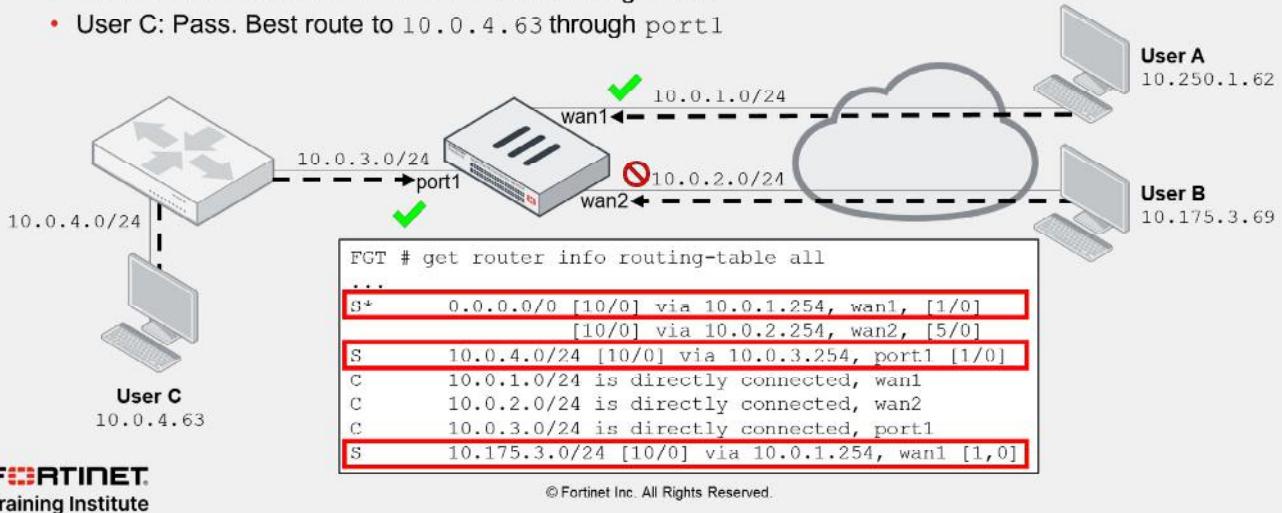
The static route through port1 references the 10.0.4.0/24 subnet. The subnet includes user C address (10.0.4.63), and as result, packets from user C also pass the RPF check.

**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



40

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.

**DO NOT REPRINT****© FORTINET**

## 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.

**DO NOT REPRINT****© FORTINET**

## 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



© Fortinet Inc. All Rights Reserved.

45

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.

**DO NOT REPRINT**

© FORTINET

## 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
```

- 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
```

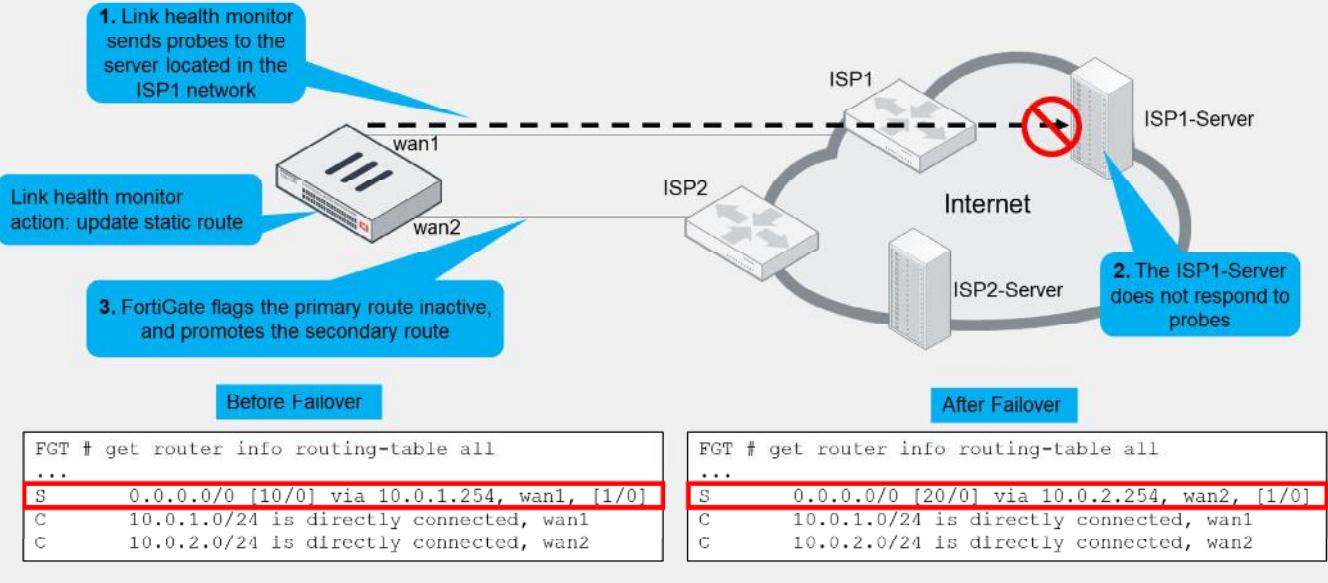
This slide shows a configuration example for link health monitor. FortiGate monitors the health of port1 against Level3 and Google DNS servers (four in total). For sending the probes, FortiGate uses 10.200.1.254 as gateway and ping as protocol.

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**

## Route Failover Example



**FORTINET**  
Training Institute

© Fortinet Inc. All Rights Reserved.

48

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.

# DO NOT REPRINT

## © FORTINET

## 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, port0

```

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] Active route
S  0.0.0.0/0 [20/0] via 10.200.2.254, port2, [5/0] Inactive route
S  8.8.8.8/32 [10/0] via 172.16.100.254, port8 inactive, [1/0] Standby route
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.

# DO NOT REPRINT

© FORTINET

## 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)
```



© Fortinet Inc. All Rights Reserved.

55

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 on [docs.fortinet.com](https://docs.fortinet.com). Alternatively, you can run the `print tablesize` command on the FortiGate CLI to get the maximum values for your device.

# DO NOT REPRINT

© FORTINET

## 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)).

**DO NOT REPRINT**  
**© FORTINET**

## 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..@.0.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 2c2f 3031 3233 3435 & '() *+,-./012345
0x0060 3637
```

This slide shows two examples of packet capture outputs.

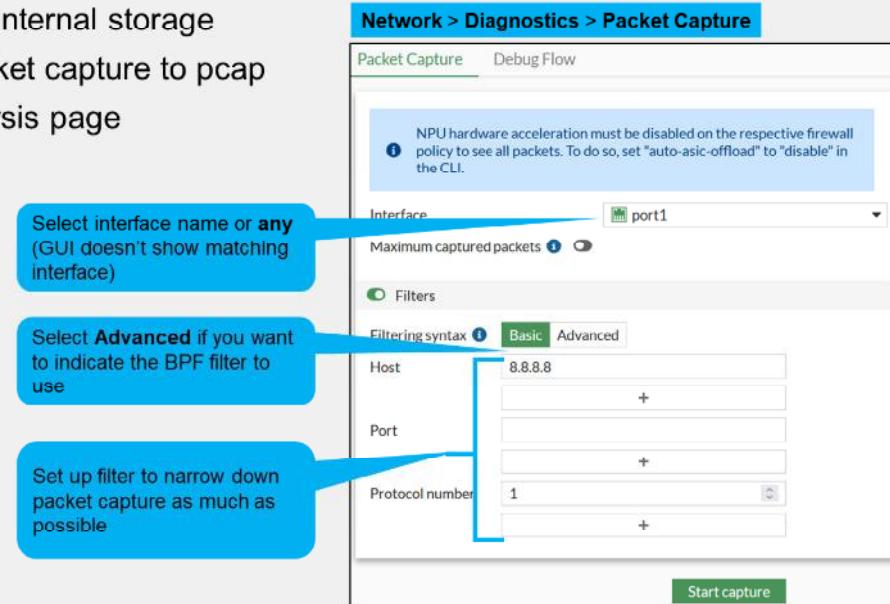
The first example captures all traffic to and from port 443. It uses verbosity 4, so the information is easy to read. It displays one packet per line, containing the incoming and outgoing interface, IP addresses, port numbers, and type of packet (SYN, SYN/ACK, and so on). Note that the interface is set 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



**FORTINET**  
 Training Institute

© Fortinet Inc. All Rights Reserved.

59

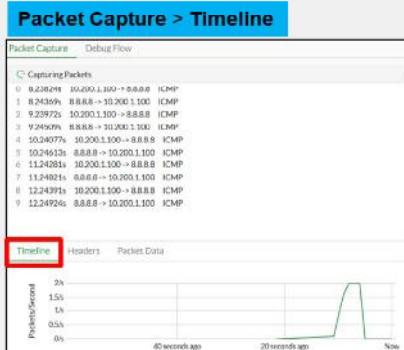
If your FortiGate model has internal storage, you can capture packets on the GUI. Starting FortiOS 7.2, the GUI packet capture tool was improved to also include a real-time analysis tool that enables you to examine the packet capture details directly on the GUI. You also download the respective pcap 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**.

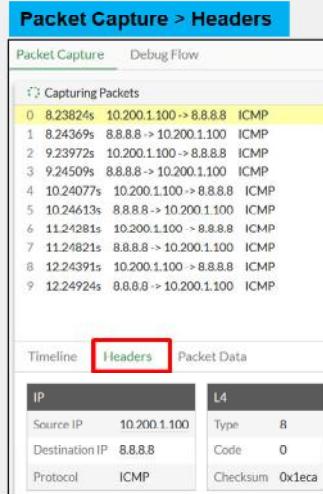
Regardless of which method you use (CLI or GUI), packet capture filters should be very specific to make sure only the relevant packets are captured, and large amounts of data are not being written to the disk.

**DO NOT REPRINT**  
**© FORTINET**

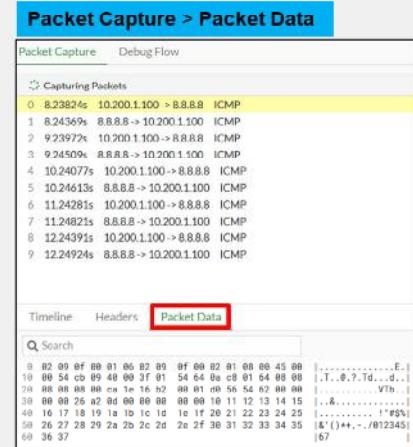
## Packet Capture From the GUI (Contd)



- Useful to identify important traffic events



- Basic IP and Layer 4 data



- Full packet data in HEX and ASCII formats

**FORTINET**  
 Training Institute

© Fortinet Inc. All Rights Reserved.

60

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

**FORTINET**  
Training Institute



## FortiGate Infrastructure

### Virtual Domains (VDOMs)

FortiOS 7.2

Last Modified: 13 June 2022

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

## VDOM Concepts

### Objectives

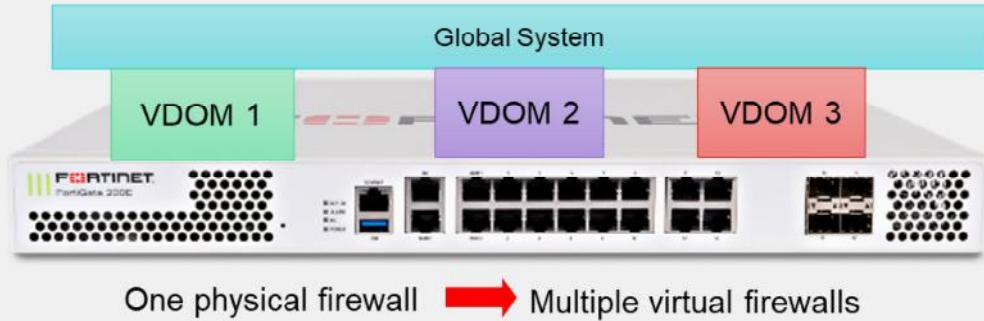
- Define and describe VDOMs

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



- 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

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



© Fortinet Inc. All Rights Reserved.

5

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-vgm mode, it is converted to multi-vgm mode. The FG-traffic VDOM becomes a traffic type VDOM. The root VDOM becomes an admin VDOM.

**DO NOT REPRINT****© FORTINET**

## 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



© Fortinet Inc. All Rights Reserved.

6

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.

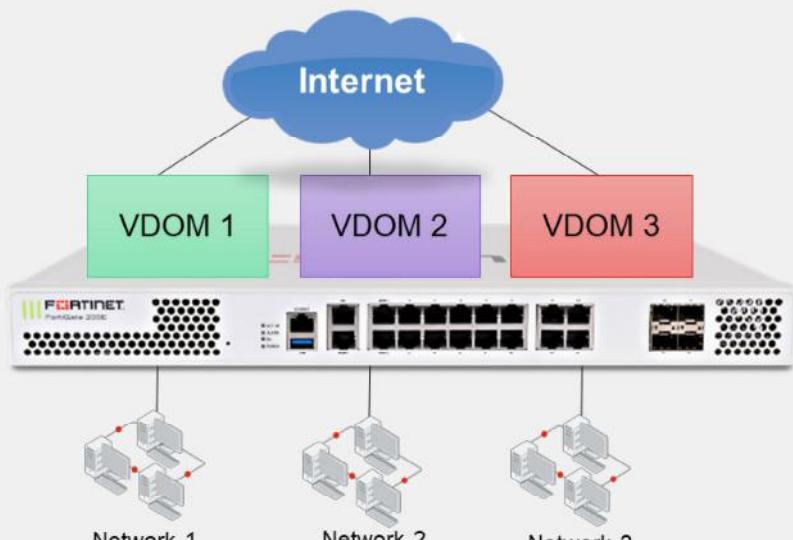
It is important to note that the management VDOM designation is solely for traffic originated by FortiGate, such as FortiGuard updates, and has no effect on traffic passing through FortiGate. As such, the management function can be performed by any designated VDOM.

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 VDOMs

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



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

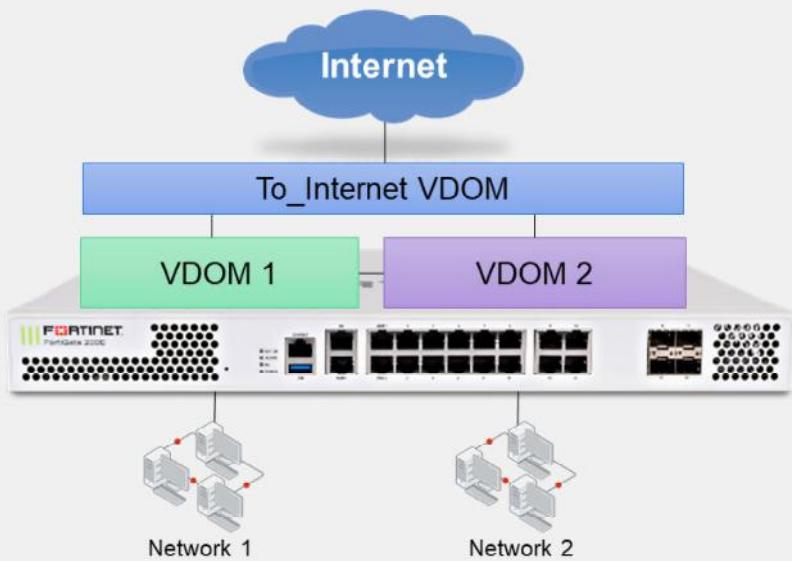
Notice that there are no inter-VDOM links. So, inter-VDOM traffic is not possible unless it physically leaves FortiGate, toward the internet, and is rerouted back. This topology would be most suitable in a scenario where multiple customers are sharing a single FortiGate, each in their own VDOM, with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



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.

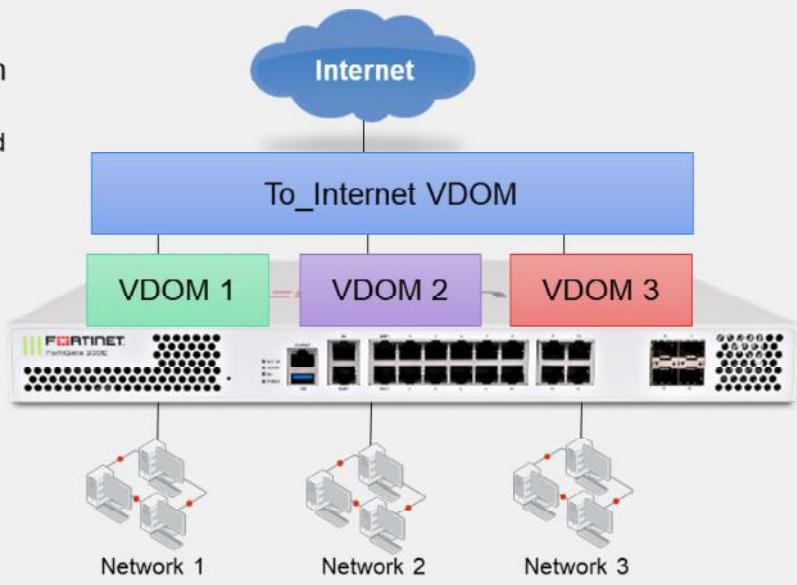
However, meshed VDOMs also provide the most flexibility. For large businesses, inter-VDOM communication may be required. Also, inter-VDOM traffic performance may be better because of a shorter processing path, which bypasses intermediate VDOMs.

# 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



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



VDOM Concepts



VDOM Administrators



Configuring VDOMs



Inter-VDOM Links



Best Practices and Troubleshooting

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

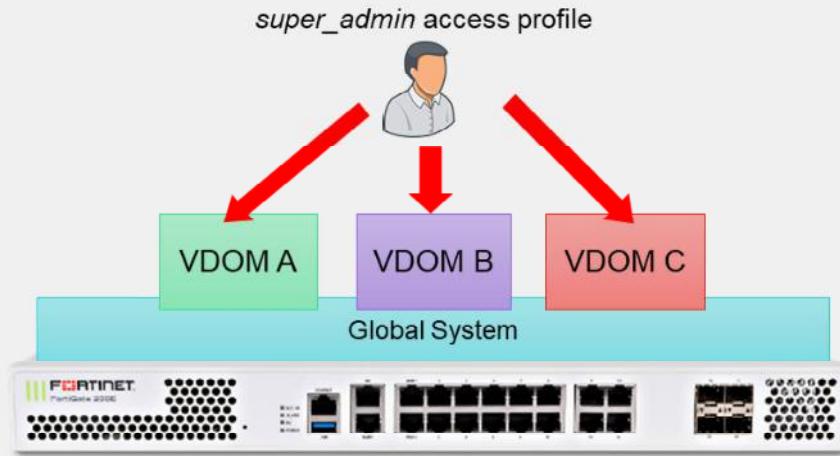
After completing this section, you should be able to achieve the objective shown on this slide.

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

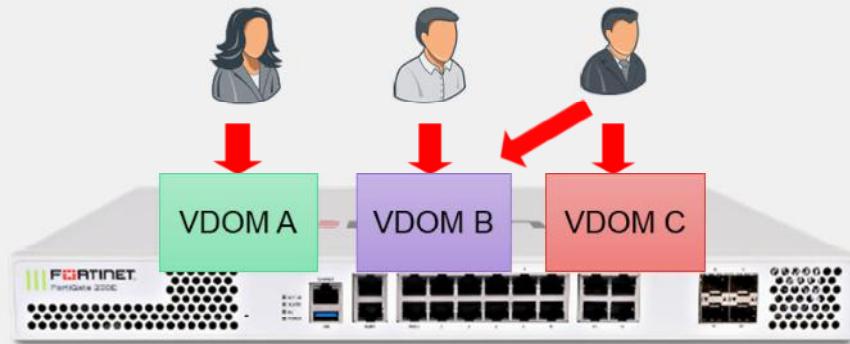


If you want to grant access to all VDOMs and global settings, select **super\_admin** as the access profile when configuring the administrator account. Similar to the account named **admin**, this account can configure all VDOMs.

**DO NOT REPRINT**  
© FORTINET

## Per-VDOM Administration

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



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

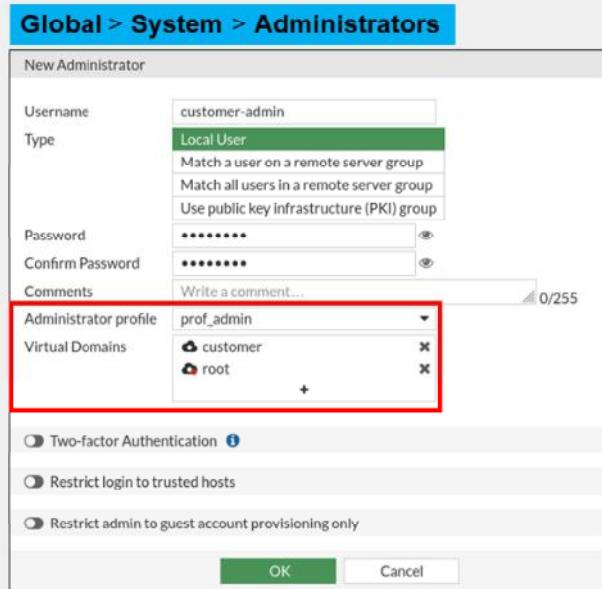
Username	customer-admin
Type	Local User
	Match a user on a remote server group
	Match all users in a remote server group
	Use public key infrastructure (PKI) group
Password	*****
Confirm Password	*****
Comments	Write a comment... 0/255
Administrator profile	prof_admin
Virtual Domains	<ul style="list-style-type: none"><li>customer</li><li>root</li></ul>

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

## Configuring VDOMs

### Objectives

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

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
```

#### System > Settings

System Operation Settings

Virtual Domains  

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.

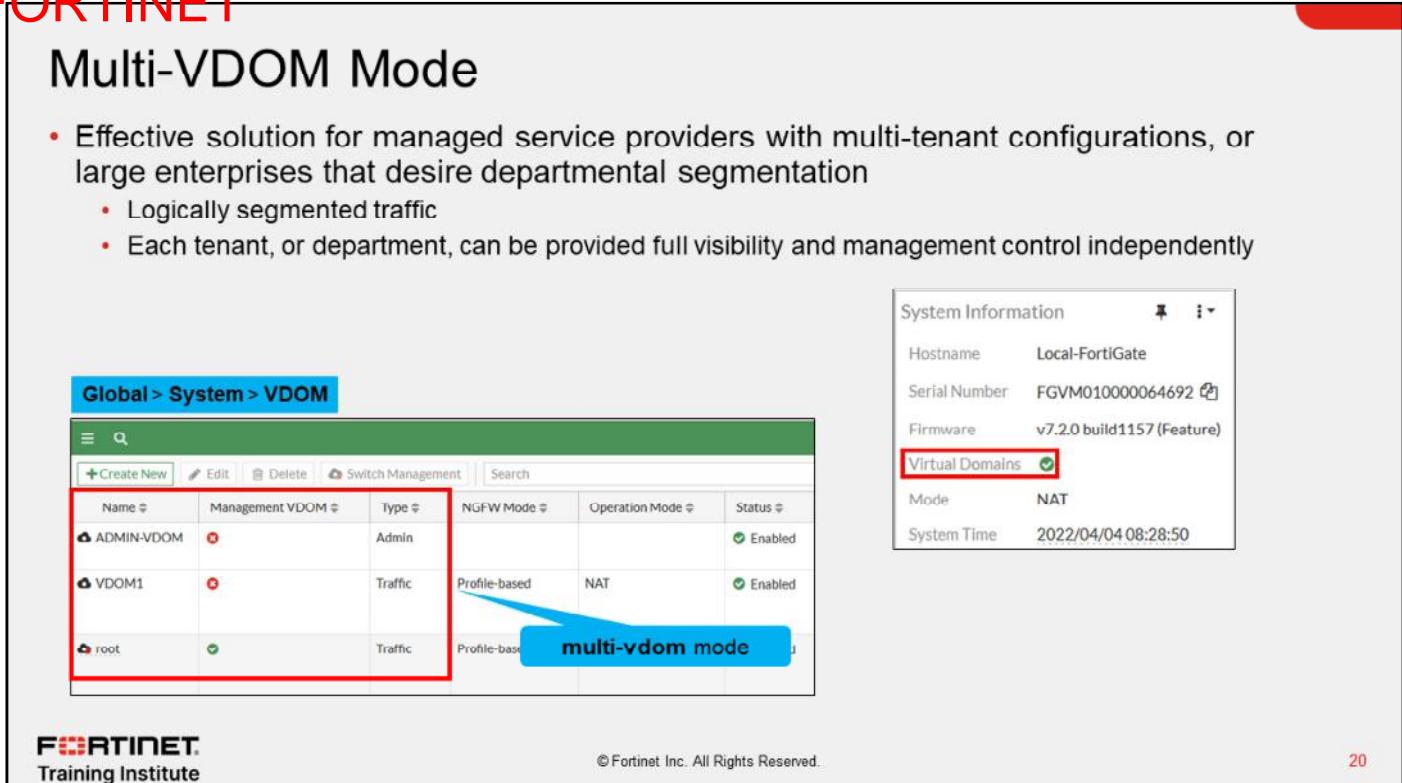
Enabling VDOMs restructures both the GUI and CLI, which you will see when you log in again.

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



The screenshot shows the FortiGate Management Interface. On the left, the 'Global > System > VDOM' page is displayed, showing a list of VDOMs: 'ADMIN-VDOM' (Management, Admin, Profile-based), 'VDOM1' (Traffic, Profile-based), and 'root' (Traffic, Profile-based). A red box highlights the first two VDOMs. A blue callout box labeled 'multi-vdom mode' points to the 'Profile-based' entry for VDOM1. On the right, the 'System Information' panel shows the following details:

System Information	
Hostname	Local-FortiGate
Serial Number	FGVM01000064692
Firmware	v7.2.0 build1157 (Feature)
Virtual Domains	<input checked="" type="checkbox"/>
Mode	NAT
System Time	2022/04/04 08:28:50

At the bottom left is the Fortinet Training Institute logo, and at the bottom right is the page number '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



#### Global > System > VDOM

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

#### Global > System > VDOM

Name	Management VD...	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 -VDOM types (Contd)

- Traffic type:
  - Can pass traffic like regular VDOMs

Global > System > VDOM						
Name	Management VD...	Type	NGFWMode	Operation Mode	Status	CPU
root	✓	Traffic	Profile-based	NAT	Enabled	0%

- From CLI:

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



New Virtual Domain

Virtual Domain	VDOM1
Type	Traffic
NGFW Mode	Profile-based
Central SNAT	<input checked="" type="radio"/>
WiFi country/region	Canada
Comments	

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

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	Global	Profile-based	NAT	Enabled	15%	36%

Red arrow pointing from the 'Operation mode per VDOM:' section to this screen.

**<VDOM> > System > Settings**

New Virtual Domain

Virtual Domain	VDOM1
Type	Traffic Admin
NGFW Mode	Profile-based Policy-based
Central SNAT	<input checked="" type="checkbox"/>
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.

**DO NOT REPRINT****© FORTINET**

## 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

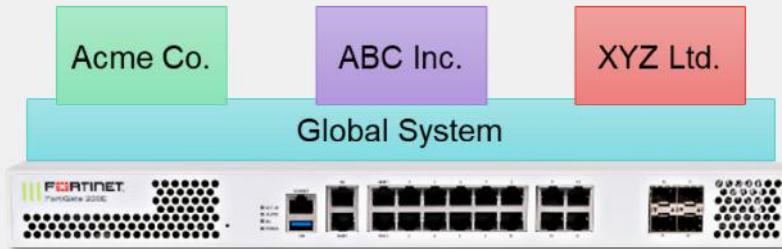
Name	port4
Alias	
Type	Physical Interface
VRF ID	0
Virtual domain	<input type="button" value="root"/> <input type="button" value="root"/> <input type="button" value="VDOM1"/>
Role	<input type="button" value="root"/>
Address	
Addressing mode	Manual <input type="button" value="DHCP"/> <input type="button" value="Auto-managed by FortiPAM"/>
IP/Netmask	192.168.10.254/24
Secondary IP address	<input type="checkbox"/>

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

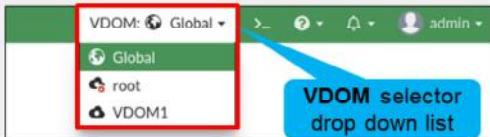
- Configured separately for each VDOM:
  - Operating mode (transparent, NAT/route)
  - NGFW mode (profile-based, policy-based)
  - Routes and network interfaces
  - Firewall policies
  - Security profiles

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.

**DO NOT REPRINT**  
**© FORTINET**

## 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

The screenshot displays two FortiGate management interface windows. The top window, titled 'Global > Security Profiles > Web Filter', shows the configuration of a global security profile named 'g-default'. The profile is set to 'Default web filtering' and 'Flow-based'. The bottom window, titled 'Customer VDOM > Web Filter', shows the list of security profiles for the 'Customer VDOM'. It lists two profiles: 'g-default' and 'g-wifi-default'. Both profiles are set to 'Default web filtering' and have a 'Scope' of 'Global'. A red arrow points from the 'g-default' profile in the Global window down to the 'g-default' profile in the Customer VDOM window.

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

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



VDOM Concepts



VDOM Administrators



Configuring VDOMs



Inter-VDOM Links



Best Practices and Troubleshooting

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

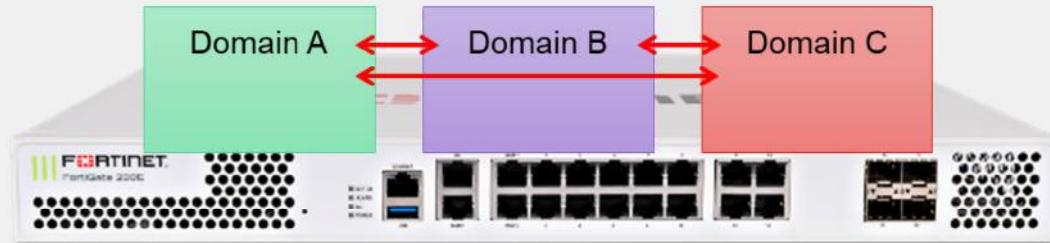
- Route traffic between VDOMs

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



© Fortinet Inc. All Rights Reserved.

35

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 shows the FortiGate GUI under the 'Global > Network > Interfaces' section. A red arrow highlights the 'Create New' dropdown and points to the 'VDOM Link' option in the list. The 'New VDOM Link' dialog box is open on the right, showing the configuration for a new VDOM link. The dialog includes fields for 'Name' (vlink), 'Interface 0 (vlink0)' (Virtual Domain: root, IP/Netmask: 10.10.100.1/30, Admin Access: HTTPS, PING, SSH, SNMP), and 'Interface 1 (vlink1)' (Virtual Domain: VDOM1, IP/Netmask: 10.10.100.2/30, Admin Access: HTTPS, PING, SSH, SNMP). The status for both interfaces is 'Enabled'. The Fortinet Training Institute logo is in the bottom left, and the page number 36 is in the bottom right.

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**.

**DO NOT REPRINT****© FORTINET**

## 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

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

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

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



© Fortinet Inc. All Rights Reserved.

41

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

The diagram illustrates a FortiGate device with three virtual domains (VDOMs): Global, VDOM1, and VDOM3. Arrows point from the 'Global' and 'VDOM3' labels to their respective configuration screens.

**Global > System > Global Resources**

Resource	Current Usage	Default Maximum	Override Maximum
Active Sessions	(289)	No Limit Set	<input checked="" type="checkbox"/>
<b>Policy &amp; Objects</b>			
Firewall Policies	(24)	21024	<input checked="" type="checkbox"/>
Firewall Addresses	(54)	11024	<input checked="" type="checkbox"/>
Firewall Address Groups	(10)	5000	<input checked="" type="checkbox"/>
Firewall Custom Services	(107)	No Limit Set	<input checked="" type="checkbox"/>
Firewall Service Groups	(8)	No Limit Set	<input checked="" type="checkbox"/>
Firewall One-time Schedules	(0)	No Limit Set	<input checked="" type="checkbox"/>
Firewall Recurring Schedules	(5)	No Limit Set	<input checked="" type="checkbox"/>
<b>User &amp; Device</b>			

**Global > System > VDOM**

Per-VDOM resource limits

Resource	Current Usage	Global Maximum	Override Maximum	Guaranteed
Active Sessions	(0)	No Limit Set	<input checked="" type="checkbox"/>	
<b>Policy &amp; Objects</b>				
Firewall Policies	(0)	21024	<input checked="" type="checkbox"/>	
Firewall Address Groups	(0)	11024	<input checked="" type="checkbox"/>	
Firewall One-time Schedules	(0)	No Limit Set	<input checked="" type="checkbox"/>	
<b>VPN IPsec Phase1 Tunnels</b>	(0)	2000	<input checked="" type="checkbox"/>	<b>1900</b>
Firewall Service Groups	(4)	No Limit Set	<input checked="" type="checkbox"/>	
Firewall One-time Schedules	(0)	No Limit Set	<input checked="" type="checkbox"/>	

**Fortinet Training Institute**

© 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.

**DO NOT REPRINT****© FORTINET**

## 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



## FortiGate Infrastructure

Fortinet Single Sign-On (FSSO)



Last Modified: 13 June 2022

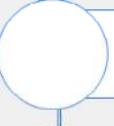
In this lesson, you will learn about Fortinet single sign-on (FSSO). When you use this feature, your users don't need to log on each time they access a different network resource.

**DO NOT REPRINT****© FORTINET**

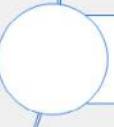
## Lesson Overview



### FSSO Function and Deployment



### FSSO With Active Directory



### FSSO Settings



### Troubleshooting

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



© Fortinet Inc. All Rights Reserved.

4

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.

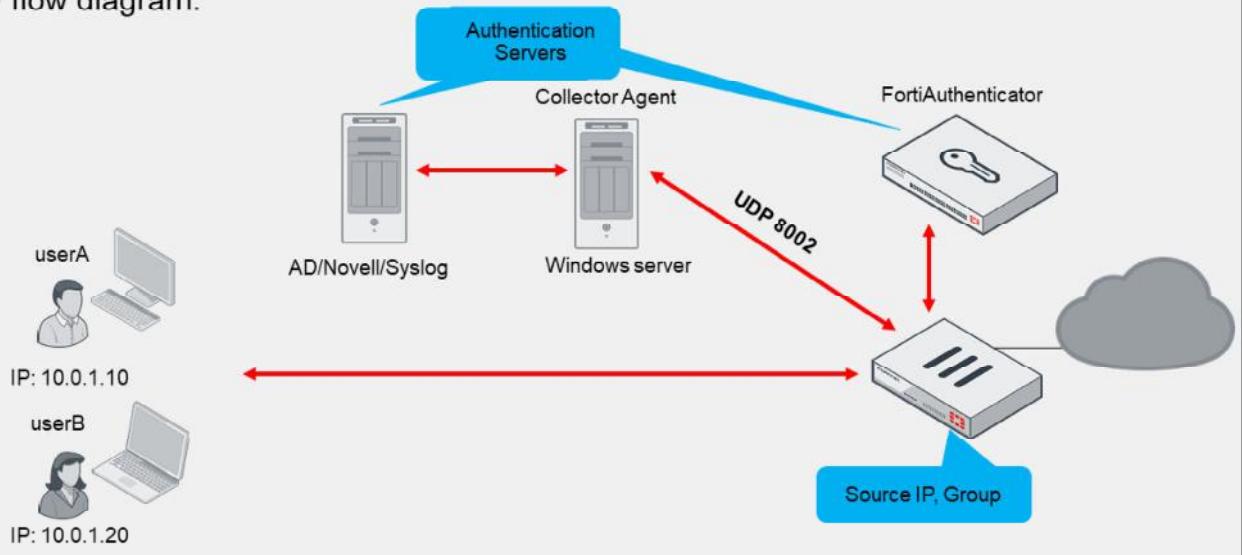
Because the domain controller authenticates users, FortiGate does not perform authentication. When the user tries to access network resources, FortiGate selects the appropriate security policy for the destination. If the user belongs to one of the permitted user groups, the connection is allowed.

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

**DO NOT REPRINT****© FORTINET**

## FSSO—Flow Chart

- FSSO flow diagram:



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

**DO NOT REPRINT****© FORTINET**

## FSSO Deployment and Configuration



Microsoft

Active Directory

### 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

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



© Fortinet Inc. All Rights Reserved.

10

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:

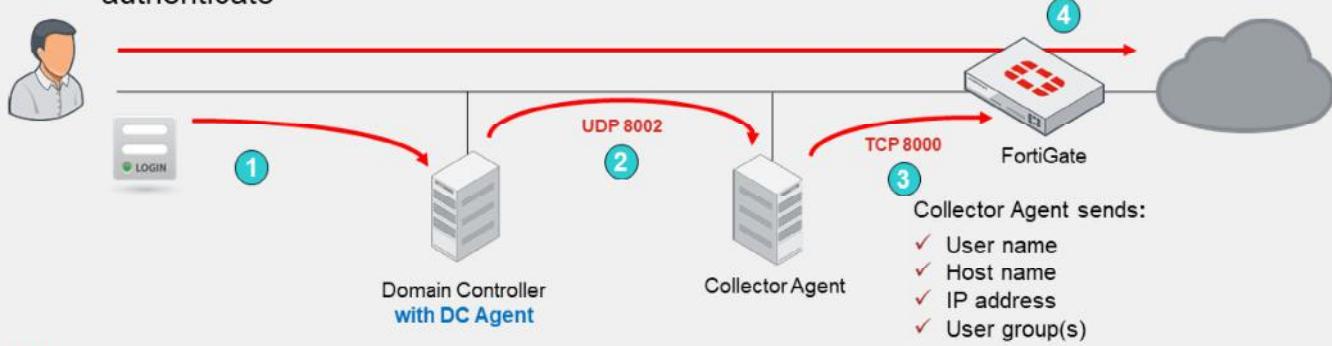
```
donot_resolve = (DWORD) 1 at HKLM\Software\Fortinet\FSAE/dcagent
```

**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

### WinSecLog

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

### NetAPI

- Polls the NetSessionEnum function on Windows every 9 seconds, or less\*
  - Authentication session table in RAM
- Retrieves login sessions, including DC login events
- Faster, but...
  - If DC has heavy system load, can miss some login events

Most recommended → Least recommended

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

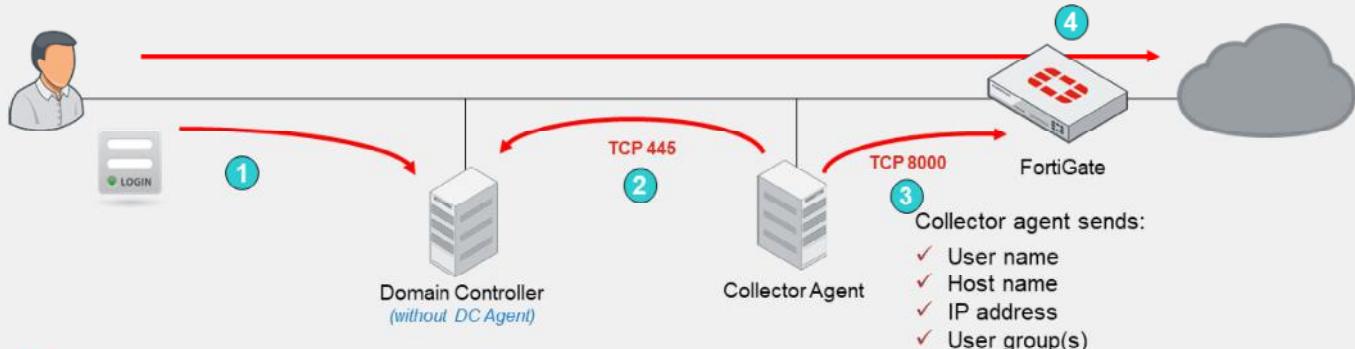
As previously stated, collector agent-based polling mode has three methods (or options) for collecting login information. The order on the slide from left to right shows most recommend to least recommended:

- **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.

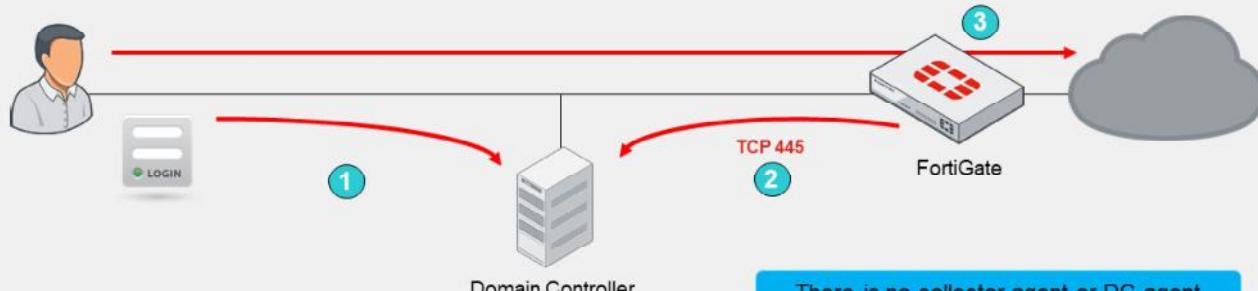
Agentless polling mode operates in a similar way to WinSecLog, but with only two event IDs: 4768 and 4769. Because there's no collector agent, FortiGate uses the SMB protocol to read the event viewer logs from the DCs.

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
  - o FortiGate discovers the login event in next poll
3. The user does not need to authenticate
  - o FortiGate already knows whose traffic it is receiving



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

1. 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
<b>Installation</b>	Complex—multiple installations (one per DC). Requires reboot.	Easy—one or no installations. No reboot required.
<b>DC agent required</b>	Yes	No
<b>Resources</b>	Shares with DC agents	Has own resources
<b>Scalability</b>	Higher	Lower
<b>Redundancy</b>	Yes	Yes
<b>Level of confidence</b>	Captures all logins	Might miss a login (NetAPI), or have a delay (WinSecLog)

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

DC agent mode is more complex. It requires not only a collector agent, but also a DC agent for each monitored domain controller. However, it is also more scalable because the work of capturing logins is done by the DC agents who pass their information directly to the collector.

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

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

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

**DO NOT REPRINT****© FORTINET**

## Additional FSSO AD Requirements

- The DNS server must be able to resolve all workstation names
  - Microsoft login events contain workstation names, but 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

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

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

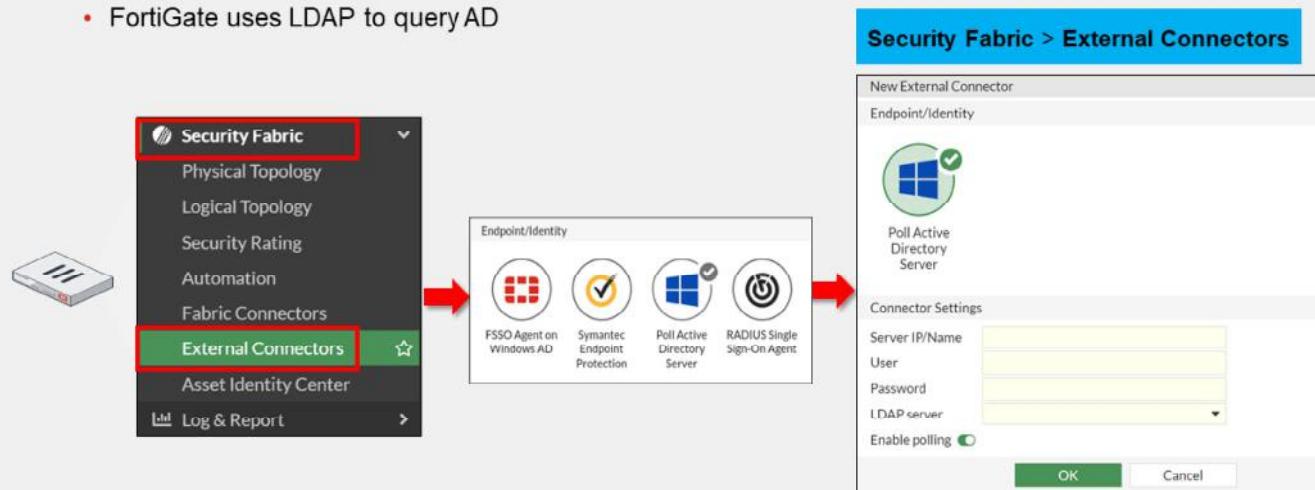
After completing this section, you should be able to achieve the objectives shown on this slide.

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



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 'Security Fabric > External Connectors' page. On the left, under 'Endpoint/Identity', there are four icons: 'FSSO Agent on Windows AD' (selected), 'Symantec Endpoint Protection', 'Poll Active Directory Server', and 'RADIUS Single Sign-On Agent'. A red arrow points from the 'FSSO Agent on Windows AD' icon to the 'User group source' dropdown in the configuration dialog. The configuration dialog is titled 'New External Connector' and shows the following settings:

- User group source:** Collector Agent Local (highlighted with a red box)
- LDAP server:** (dropdown menu)
- Proactively retrieve from LDAP server:** (radio button)
- Connector Settings:**
  - Name:** (input field)
  - Primary FSSO agent:** (input field) Server IP/Name, with a 'Password' field and a '+' button.
  - Trusted SSL certificate:** (checkbox)
  - User group source:** (dropdown menu) Collector Agent Local (highlighted with a red box)
  - Users/Groups:** 0
- Buttons:** Apply & Refresh, OK, Cancel

At the bottom of the interface, it says '© Fortinet Inc. All Rights Reserved.' and '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:

The screenshot shows the Fortinet Support website interface. At the top, there is a navigation bar with links for Home, Asset Assistance, Download (which is highlighted in red), and Feedback. Below the navigation bar, there is a 'Customer Service & Support' section with a 'Welcome' message and links for Home, Firmware Images (which is highlighted in red), Firmware Image Checksums, and HQIP Images. The main content area is titled 'Select Product' and shows a dropdown menu for 'FortiGate'. Below the dropdown are buttons for 'Release Notes', 'Download' (which is highlighted in blue), 'Upgrade Path', and 'FortiGate Support Tool'. The 'Image File Path' field contains the URL '/FortiGate/v7.00/7.2/7.2.0/FSSO/'. The 'Image Folders/Files' section shows a table of files with the following data:

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 16:03:59	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_x64.exe	3,549	2021-03-30 16:03:56	2021-03-30 16:03:57	HTTPS Checksum
FSSO500WATs_build0295.sum	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 14:03:01	2021-03-30 14:03:03	HTTPS Checksum
TSAgent_Setup_5.0.0295.msi	4,132	2021-03-30 16:03:50	2021-03-30 16:03:52	HTTPS Checksum

#### Available agents:

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

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

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

Also, for each agent, there are two versions: the executable (.exe) and Microsoft Installer (.msi).

Notice that you do not need to match the FSSO version with your exact FortiGate firmware version. When installing FSSO, grab the latest collector agent for your major release. You do however, need to match the DC agent version to the collector agent version.

**DO NOT REPRINT**  
**© FORTINET**

## FSSO Collector Agent Installation Process

1. Run the installation process as Administrator
2. Enter the user name in the following format:
  - DomainName\UserName
3. Configure the collector agent for:
  - Monitoring logins
  - NTLM authentication
  - Directory access
4. Optionally, launch the DC agent installation wizard before exiting the collector agent installation wizard



**FORTINET**  
 Training Institute

© Fortinet Inc. All Rights Reserved.

25

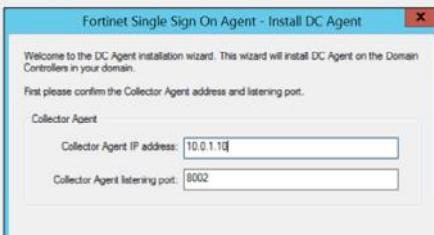
After you've downloaded the collector agent, run the installation process as Administrator and follow these steps in the installation wizard:

1. Read and accept the license agreement.
2. Optionally, change the installation location. The default folder is named **FSAE** (Fortinet Server Authentication Extension).
3. Enter the username. By default, the agent uses the name of the currently running account; however, you can change it using the format: **DomainName\UserName**.
4. Alternatively, configure your collector agent for monitoring, NTLM authentication, and directory access. These options are also customizable after installation. Although the default is **Standard** mode, when doing new FSSO setups it is always a best practice to install in **Advanced** mode. You will look at some of the advantages in this lesson.
5. If you want to use DC agent mode, make sure that **Launch DC Agent Install Wizard** is selected. This automatically starts the DC agent installation.

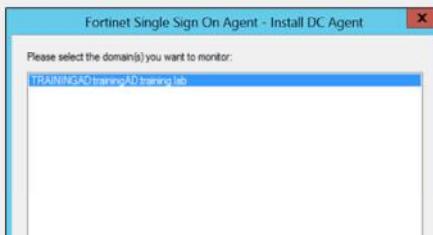
**DO NOT REPRINT**  
**© FORTINET**

## DC Agent Installation Process

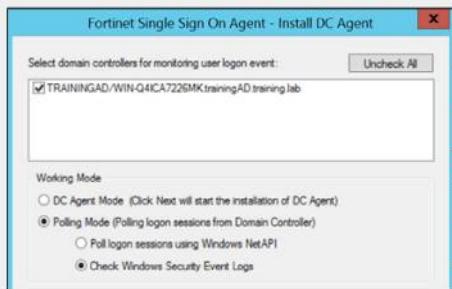
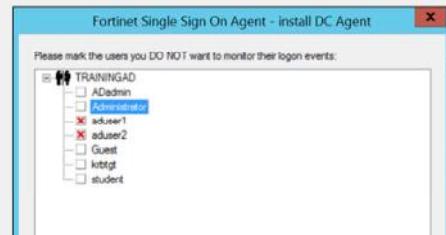
### 1 IP and port for collector agent



### 2 Domains to monitor



### 3 Remove users



4 Select domain controllers to install the DC agent

5 **DC Agent Mode** – to install DC agent on selected DC  
**Polling Mode** – DC agent will not be installed

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

1. Enter the IP address for the collector agent. Optionally, you can customize the listening port, if the default value is already used by another service.
2. Select the domains to monitor. If any of your required domains are not listed, cancel the wizard and set up the correct trusted relationship with the domain controller. Then, run the wizard again. Note that this could also be a result of using an account without all the necessary permissions.
3. Optionally, select users that you do not want to monitor; these users' login events are not recorded by the collector and therefore are not passed to FortiGate. While these users are still able to generate login events to the domain, when they are detected by the collector agent, they are discarded so as to not interfere with the logged in user. This is especially useful in environments with a centrally managed antivirus solution, or a scheduled backup service that uses an AD account to start. These accounts can create login events for the collector agent that overwrite existing user logins. This may result in FortiGate applying the incorrect policies and profiles based on the overriding account. You can also customize the option to ignore users after installation is complete.
4. Optionally, clear the checkboxes of domain controllers that you don't want to install the DC agent on. Remember, for DC agent mode FSSO, at least one domain controller must have the DC agent installed. Also remember that installing the DC agent requires a reboot of the DC before it will start gathering login events. You can add or remove the DC agent to DCs at any time after the installation is complete.
5. Select **DC Agent Mode** as the working mode. If you select **Polling Mode**, the DC agent will not be installed.

Finally, the wizard requests a system reboot.