FortiGate Infrastructure Study Guide

for FortiOS 7.2

FORTINET®
Training Institute

Fortinet Training Institute - Library

https://training.fortinet.com

Fortinet Product Documentation

https://docs.fortinet.com

Fortinet Knowledge Base

https://kb.fortinet.com

Fortinet Fuse User Community

https://fusecommunity.fortinet.com/home

Fortinet Forums

https://forum.fortinet.com

Fortinet Product Support

https://support.fortinet.com

FortiGuard Labs

https://www.fortiguard.com

Fortinet Training Program Information

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

Fortinet | Pearson VUE

https://home.pearsonvue.com/fortinet

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

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

FORTINET

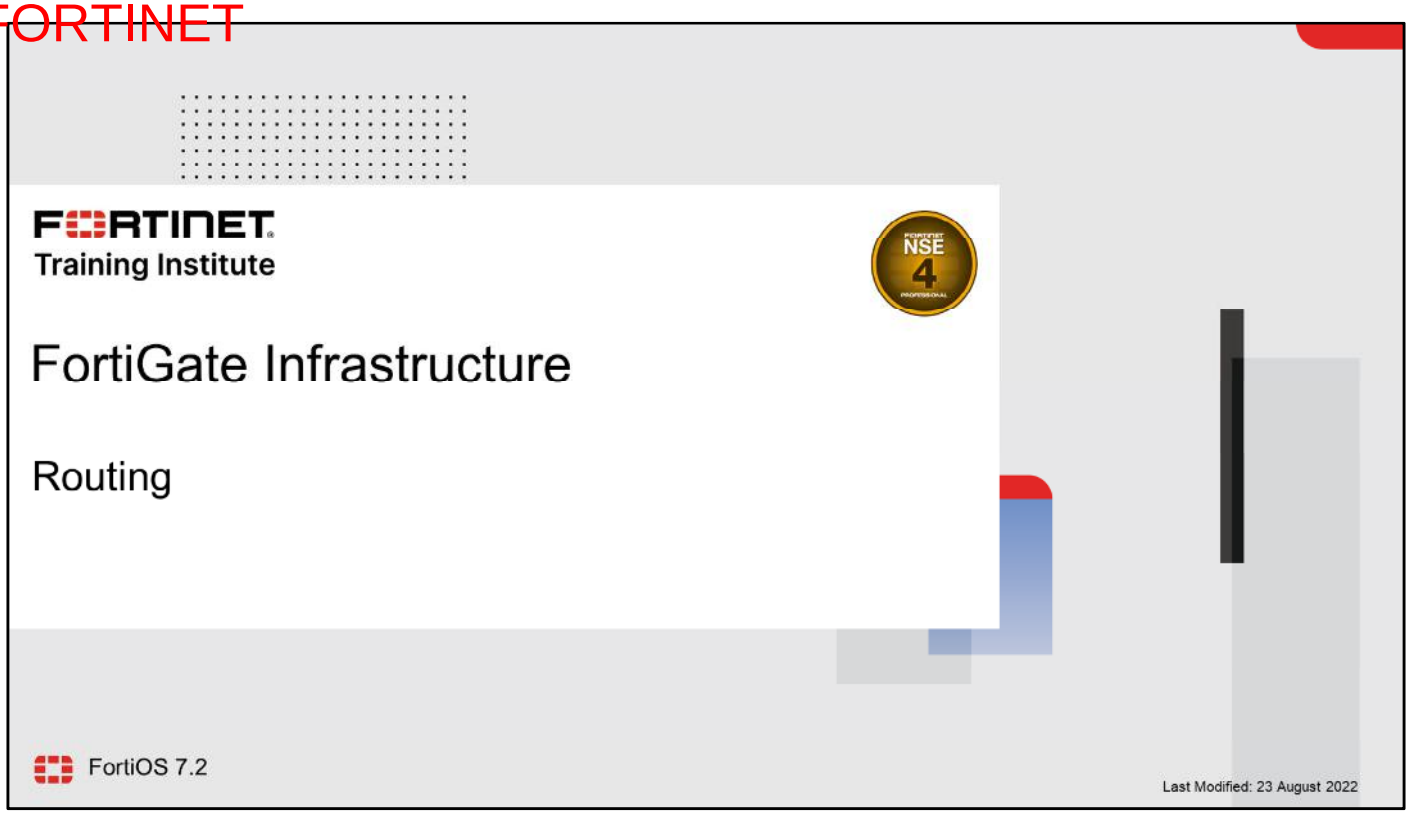
8/30/2022

TABLE OF CONTENTS

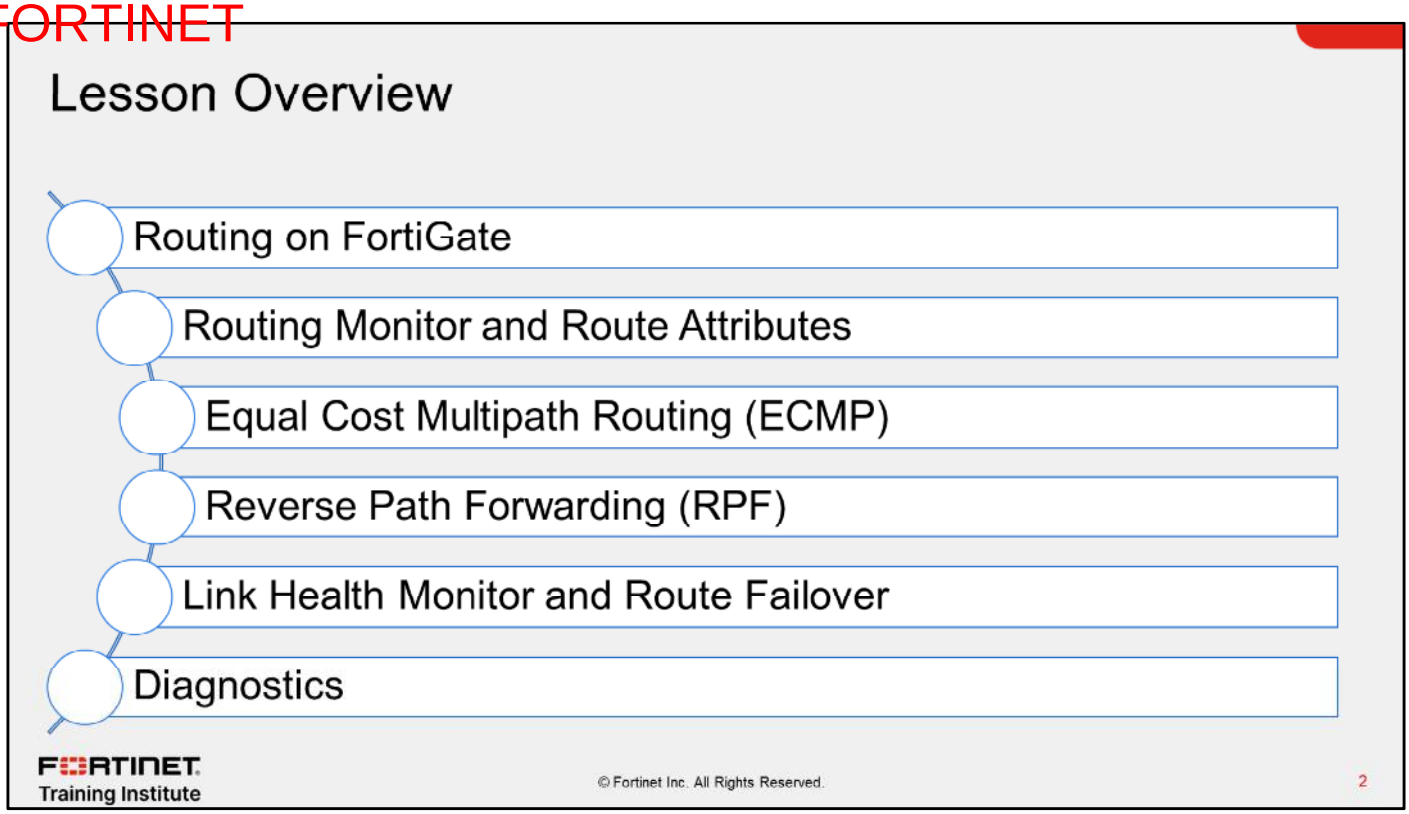
Change Log

This table includes updates to the *FortiGate Infrastructure 7.2 Study Guide* dated 6/13/2022 to the updated document version dated 8/30/2022.

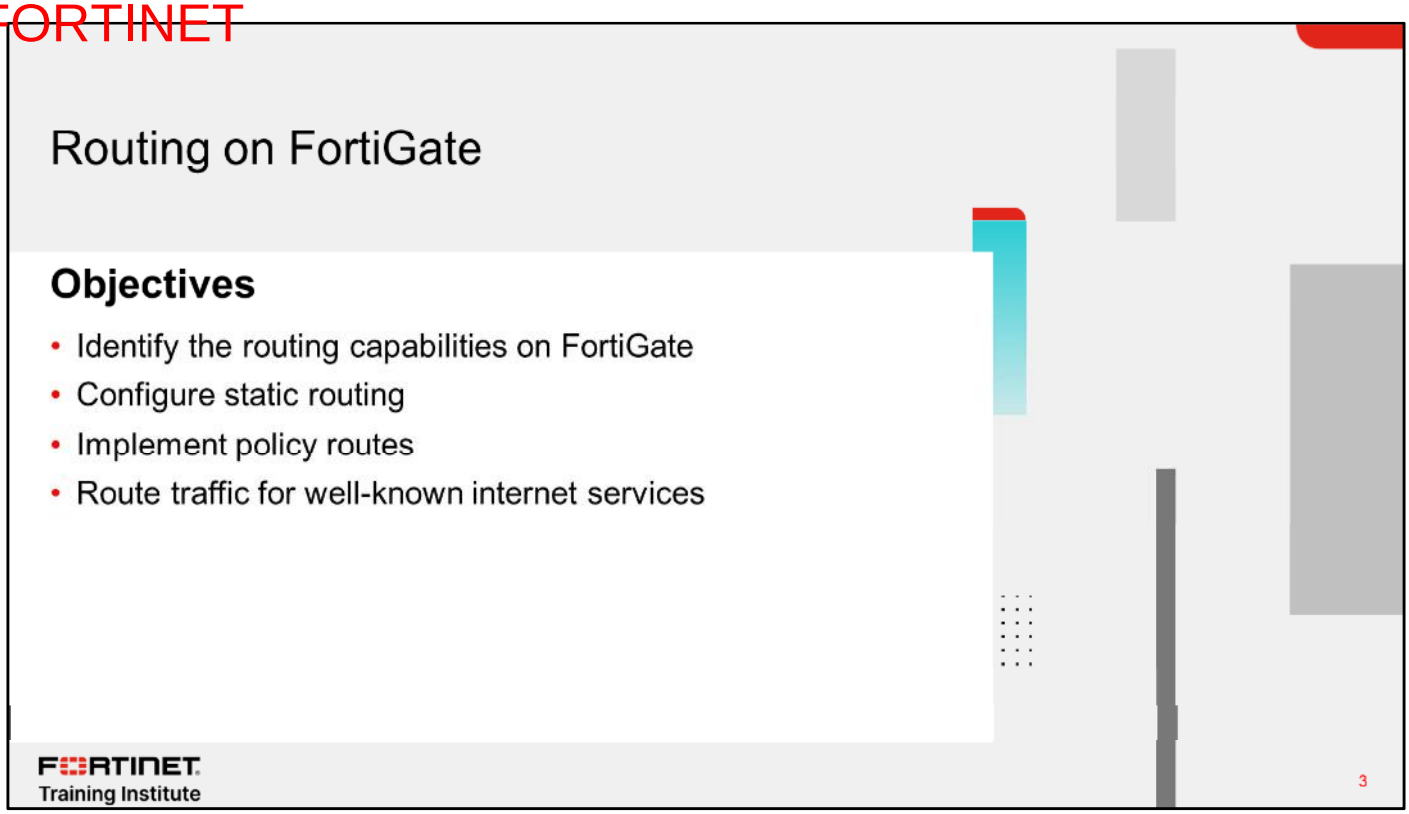
Change	Location
Various formatting fixes	Entire Guide
Fixed notes	Lesson 6, slide 50
Updated notes	Lesson 7, slide 19 and 42



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

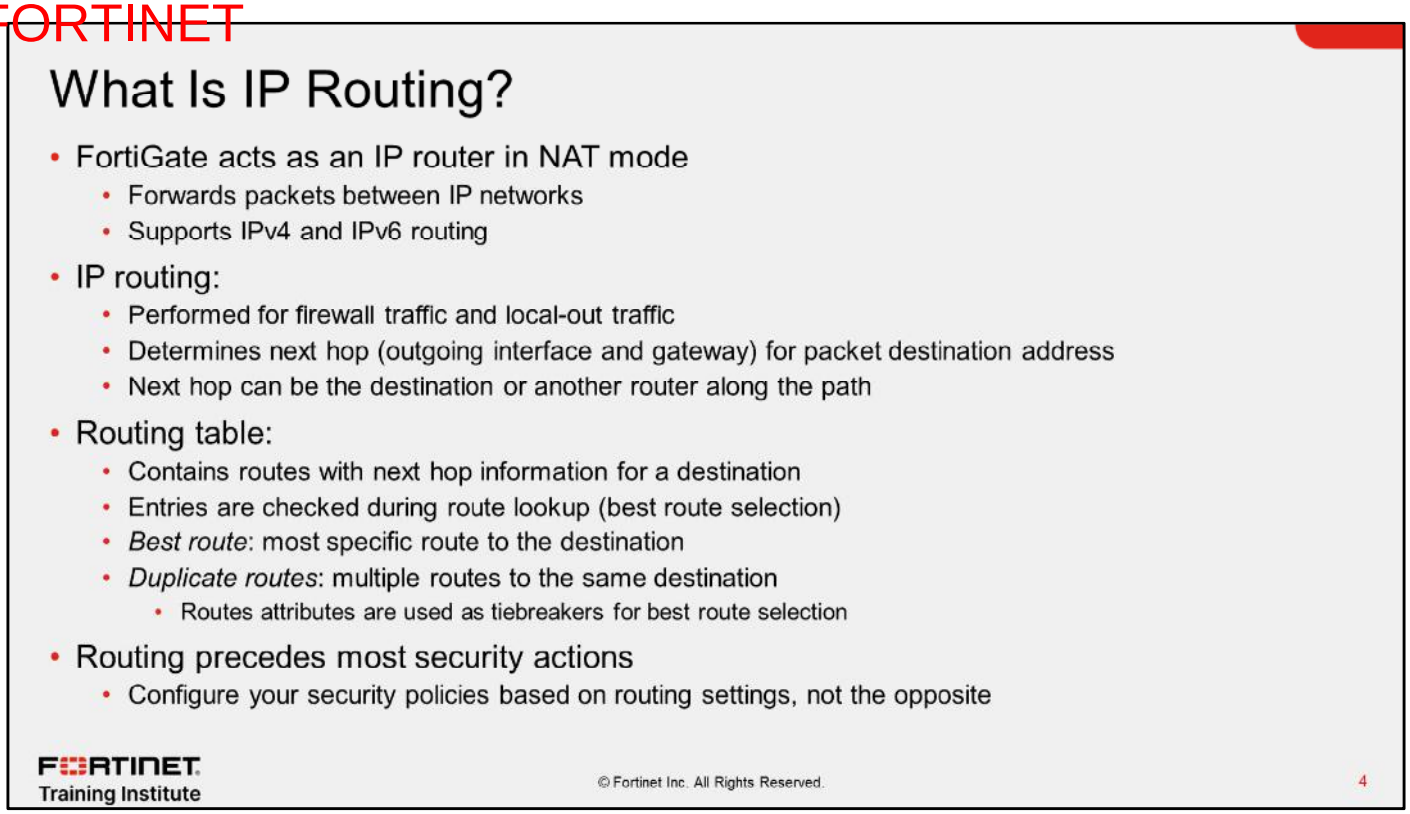


In this lesson, you will learn about the topics shown on this slide.



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

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



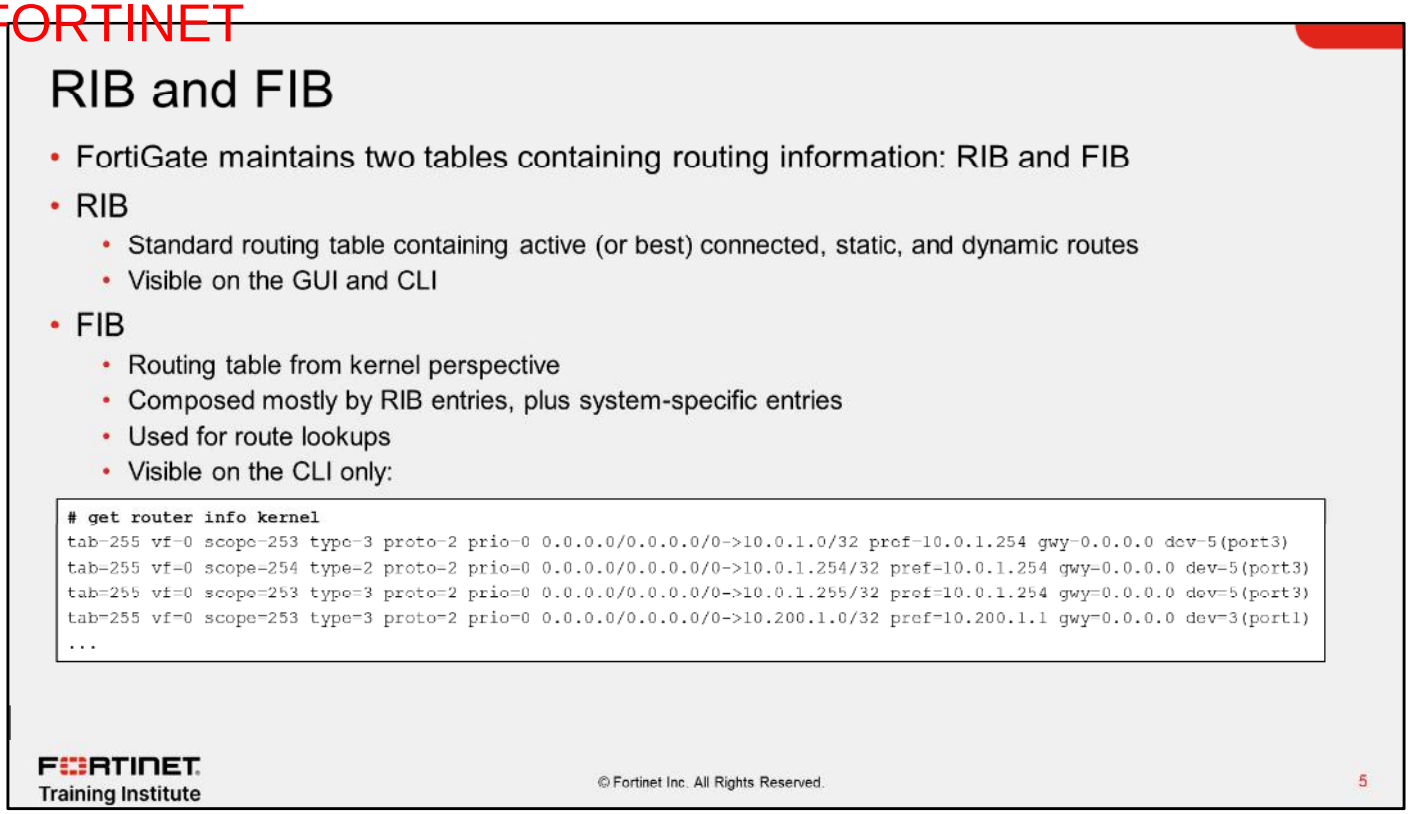
When FortiGate operates in NAT mode—the default operation mode—FortiGate behaves as an IP router. An IP router is a device that forwards packets between IP networks. For that, a router performs IP routing, which is the process of determining the next hop to forward a packet to based on the packet destination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

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

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

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

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

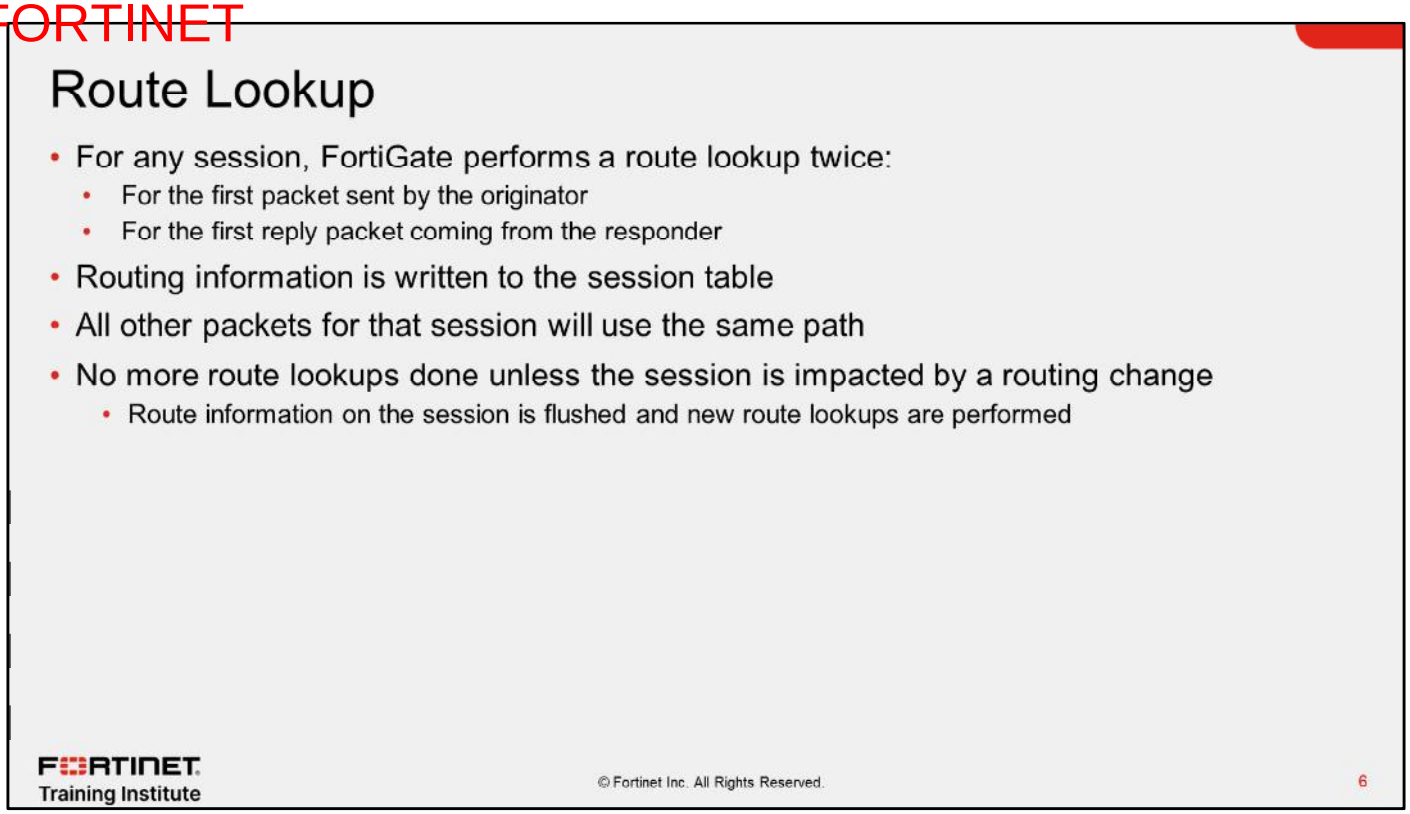


FortiGate maintains its routing information in two tables: RIB and FIB. The routing table, also known as the routing information base (RIB), is a standard routing table containing active (or the best) connected, static, and dynamic routes. The forwarding information base (FIB) can be described as the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

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

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

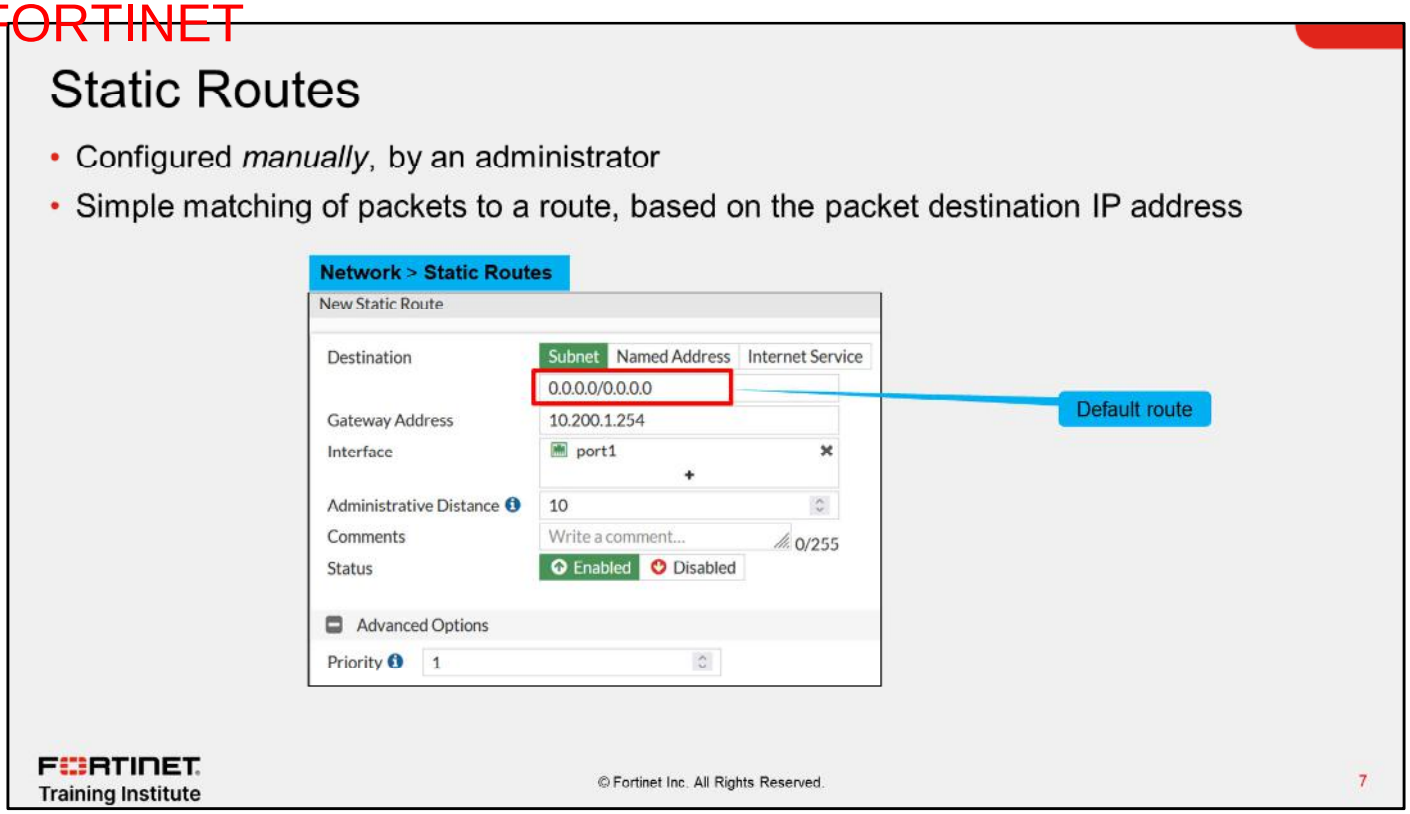
This lesson focuses on the RIB (or routing table) only, and you will learn more about it, including how to monitor its entries, in this lesson.



For each session, FortiGate performs two route lookups:

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

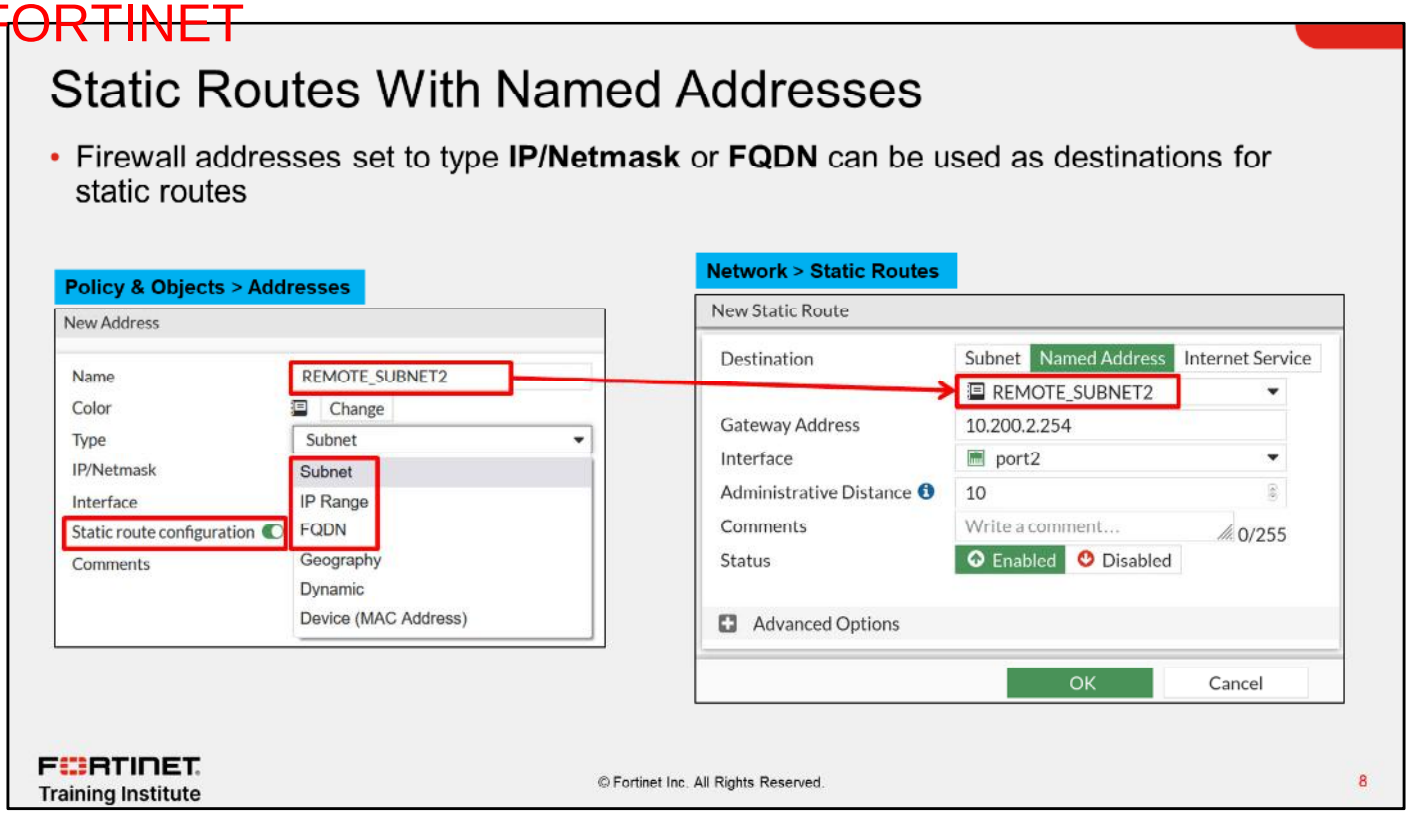
After completing these two lookups, FortiGate writes the routing information to its session table. Subsequent packets are routed according to the *session table*, not the routing table. So, all packets that belong to the same session follow the same path. However, there is an exception to this rule: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



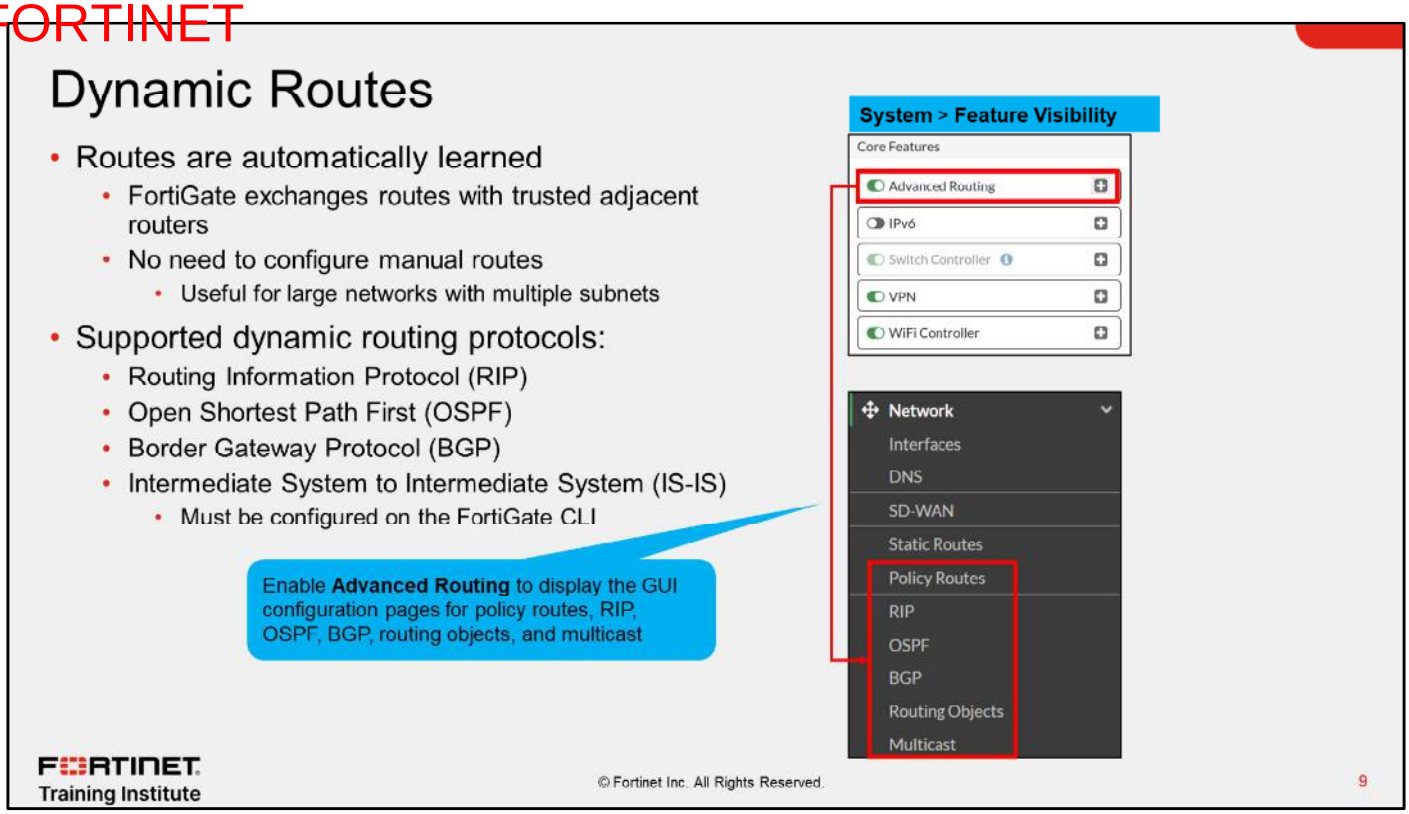
One type of manually configured route is called a static route. When you configure a static route, you are telling FortiGate, “When you see a packet whose destination is within a specific range, send it through a specific network interface, towards a specific router.” You can also configure the distance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

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

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



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



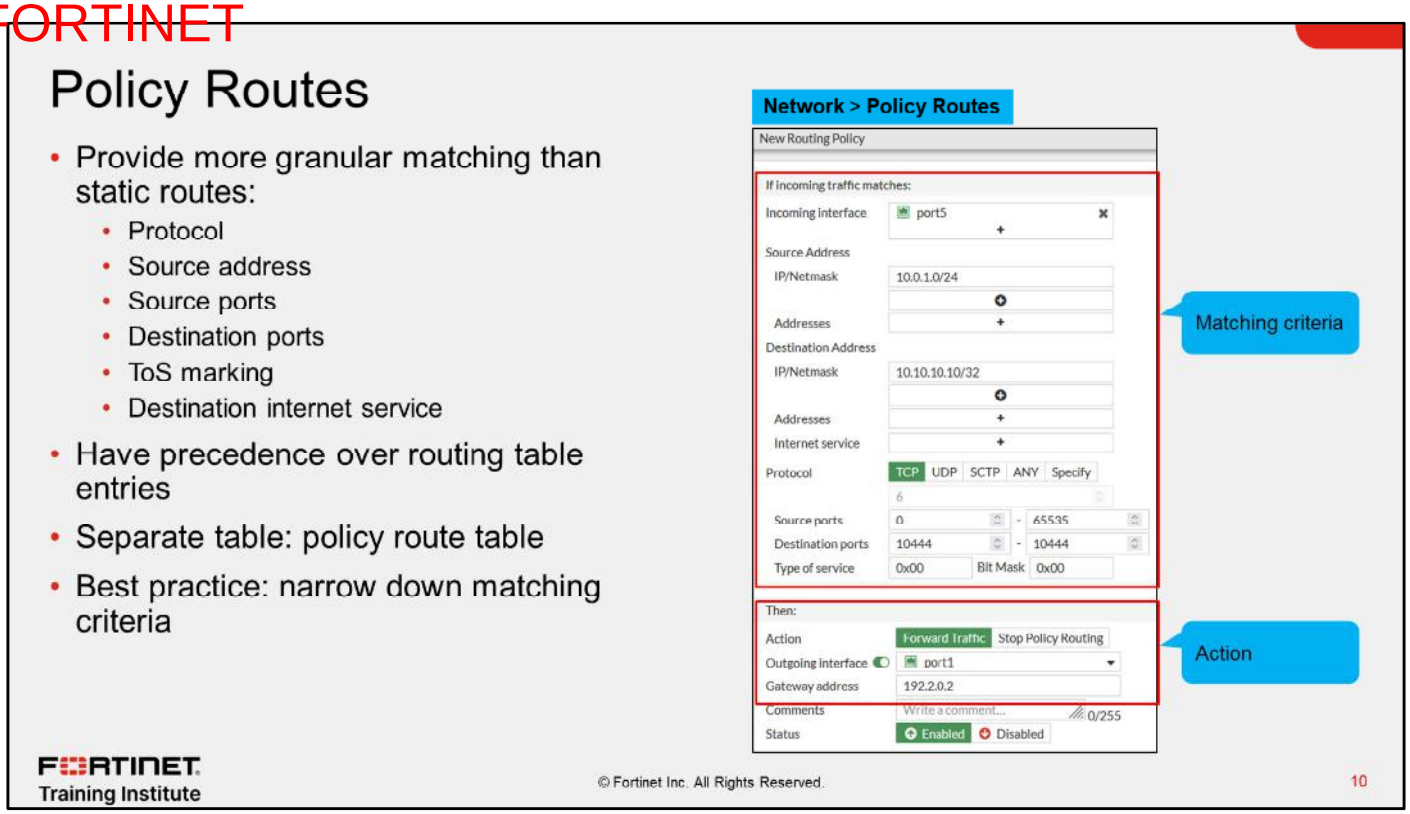
For large networks, manually configuring hundreds of static routes may not be practical. Your FortiGate can help, by learning routes automatically. FortiGate supports several dynamic routing protocols: RIP, OSPF, BGP, and IS-IS.

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

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

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

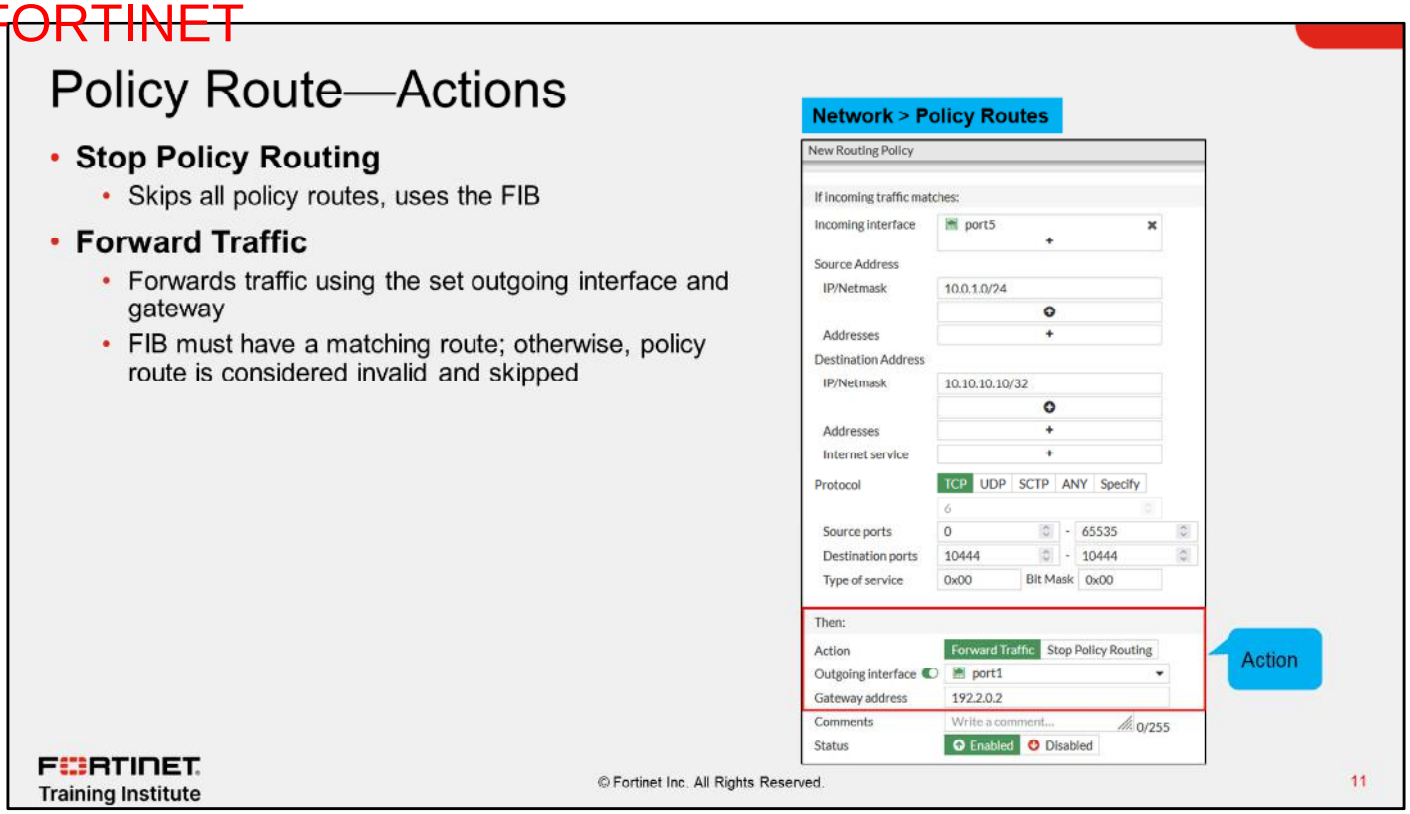
Larger networks also may need to balance the routing load among multiple valid paths and detect and avoid routers that are down. You will learn more about that in this lesson.



Static routes are simple and are often used in small networks. Policy routes, however, are more flexible because they can match more than just the destination IP address. For example, you can configure as matching criteria the incoming interface, the source and destination subnets, protocol, and port number.

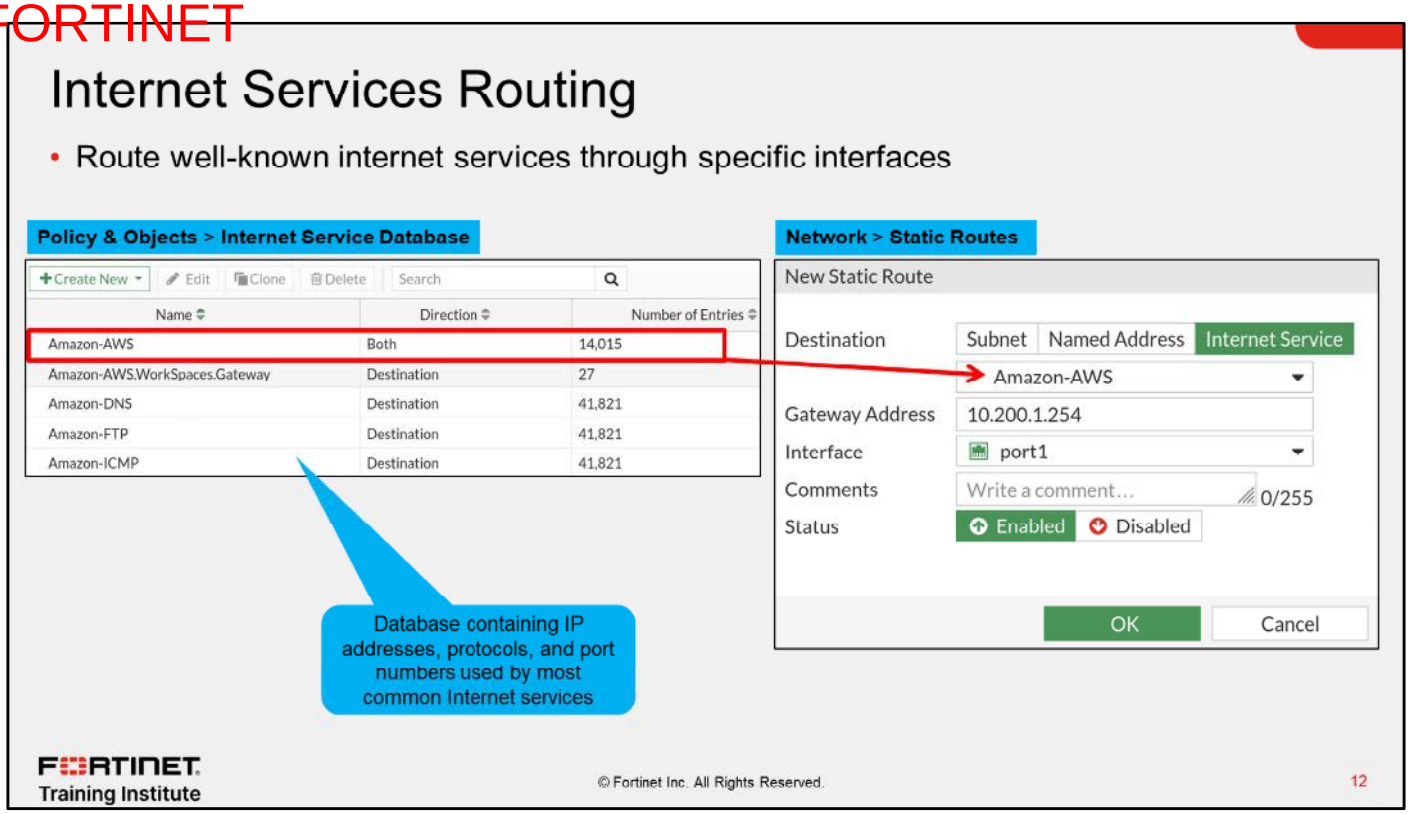
Policy routes are maintained in a separate routing table by FortiGate and have precedence over the entries in the routing table. Because of its precedence, it is a best practice to narrow down the matching criteria of policy routes as much as possible. Otherwise, traffic that is expected to be routed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

This slide shows an example of a policy route configured using the FortiGate GUI. The policy route instructs FortiGate to match traffic received at **port5**, sourced from `10.0.1.0/24` and destined to the host `10.10.10.10`. The traffic must also be destined to TCP port 10444 for the policy route to match. FortiGate then forwards the traffic—**Forward Traffic** action—to **port1** through the gateway `192.2.0.2`.



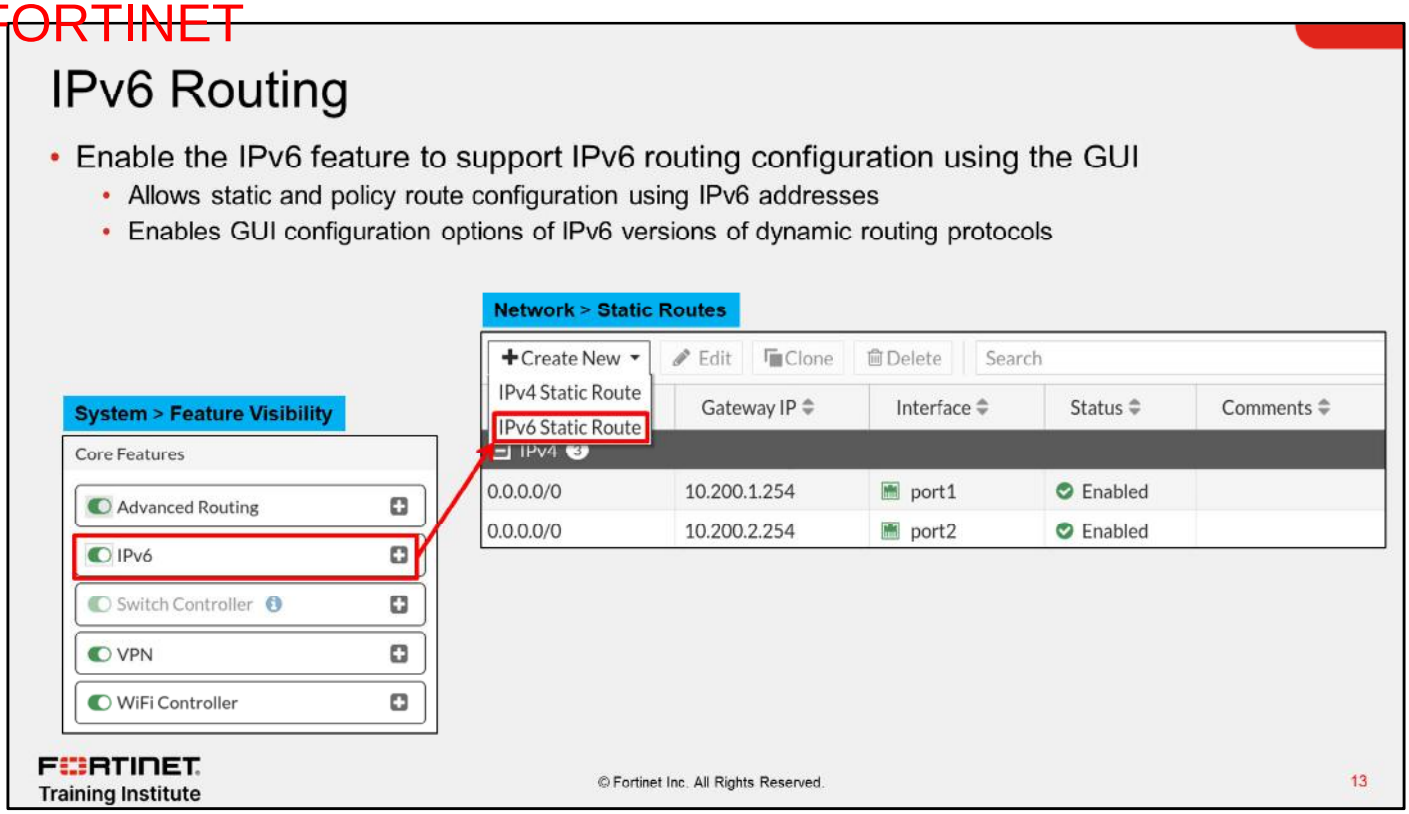
When a packet matches a policy route, FortiGate takes one of two actions. Either it routes the packet to the configured outgoing interface and gateway—**Forward Traffic** action—or it stops checking the policy routes—**Stop Policy Routing** action—so the packet is routed based on the routing table.

Note that when you configure **Forward Traffic** as the action, the **Destination Address**, **Outgoing interface**, and the **Gateway address** settings must match a route in the FIB. Otherwise, the policy route is considered invalid and, as a result, skipped.



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

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



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

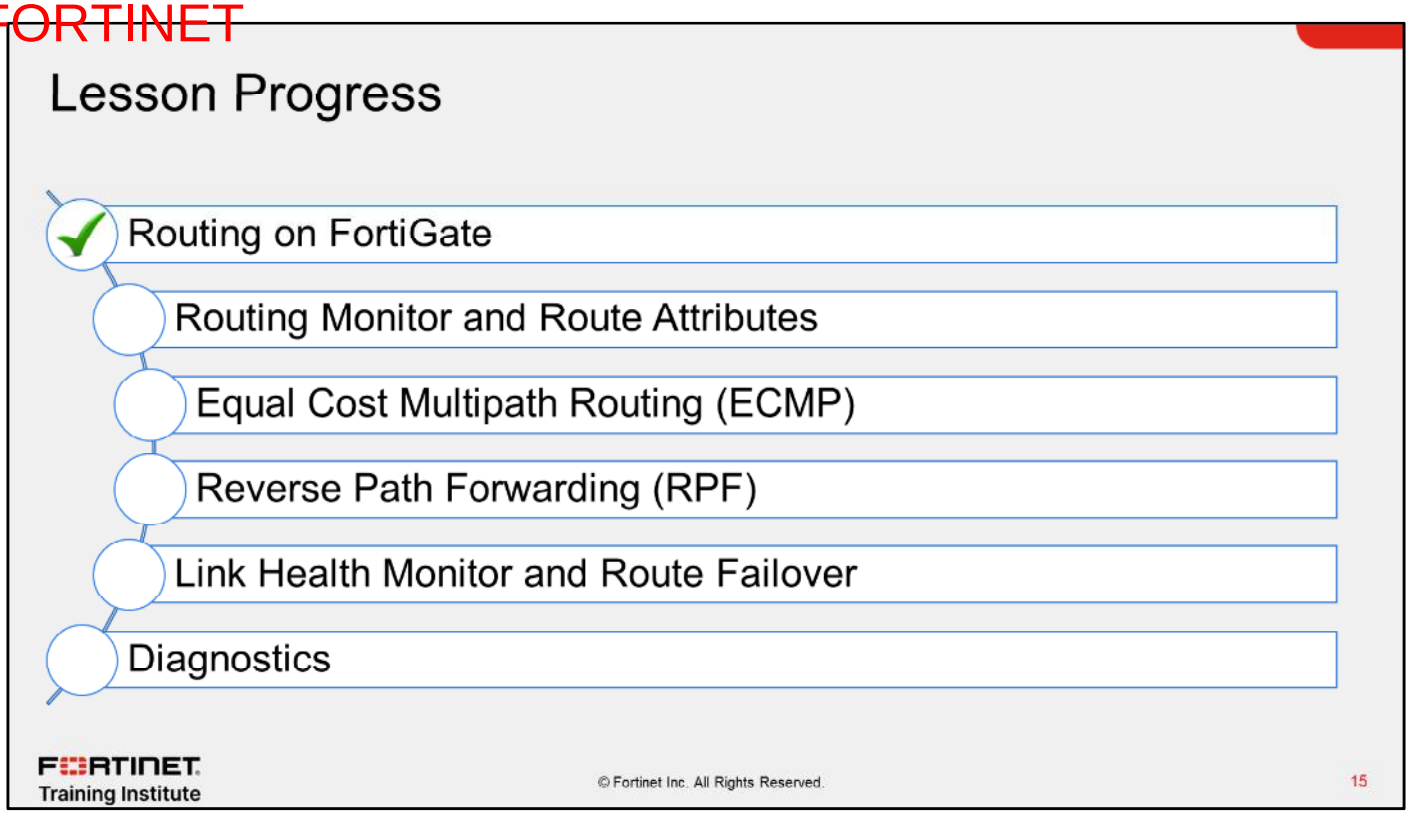
Knowledge Check

1. Which objects can you use to create static routes?
   - ✓ A. ISDB objects
   - B. Service objects

2. When the **Stop policy routing** action is used in a policy route, which behavior is expected?
   - A. FortiGate skips over this policy route and tries to match another in the list.
   - ✓ B. FortiGate routes the traffic based on the regular routing table.

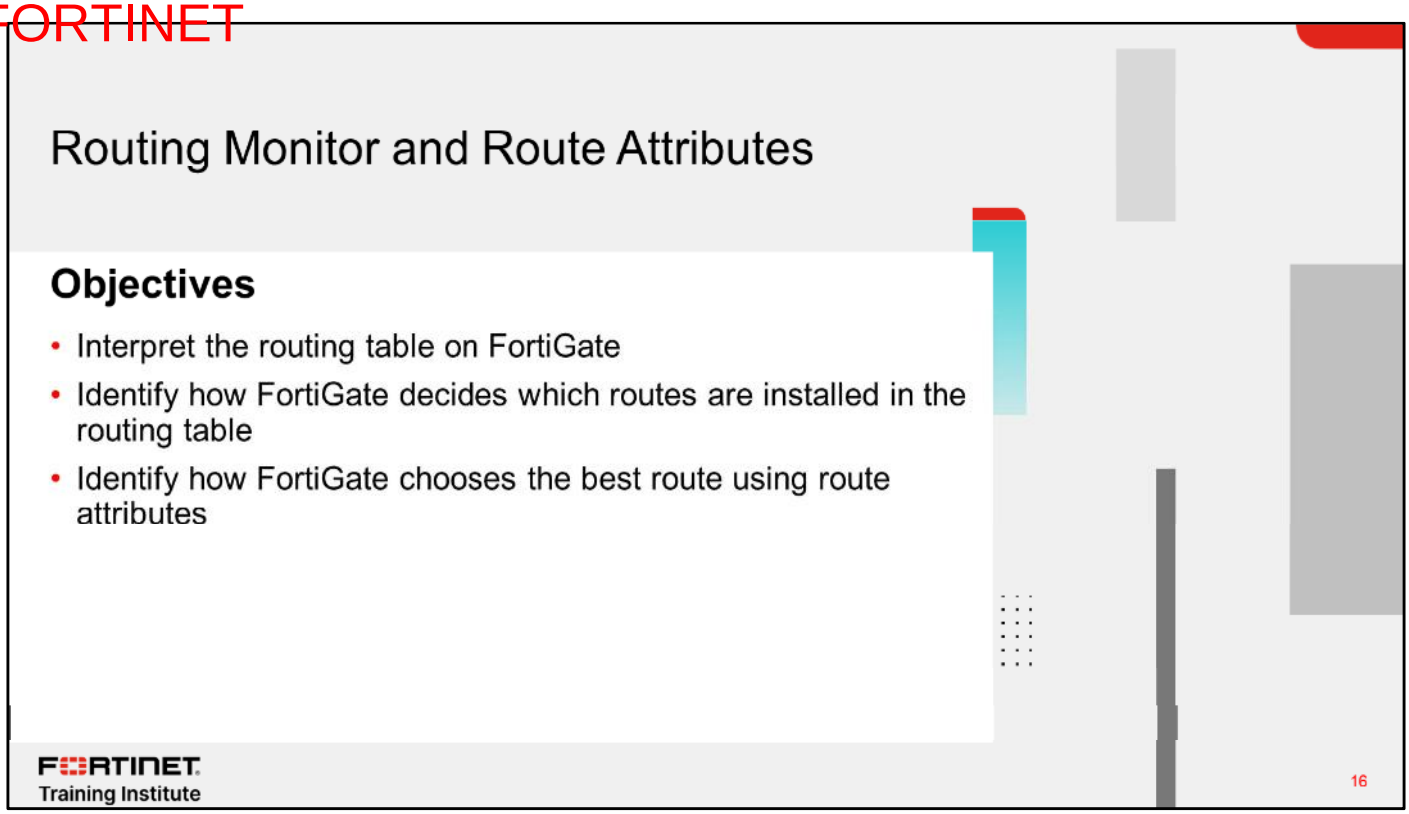
FORTINET Training Institute

14



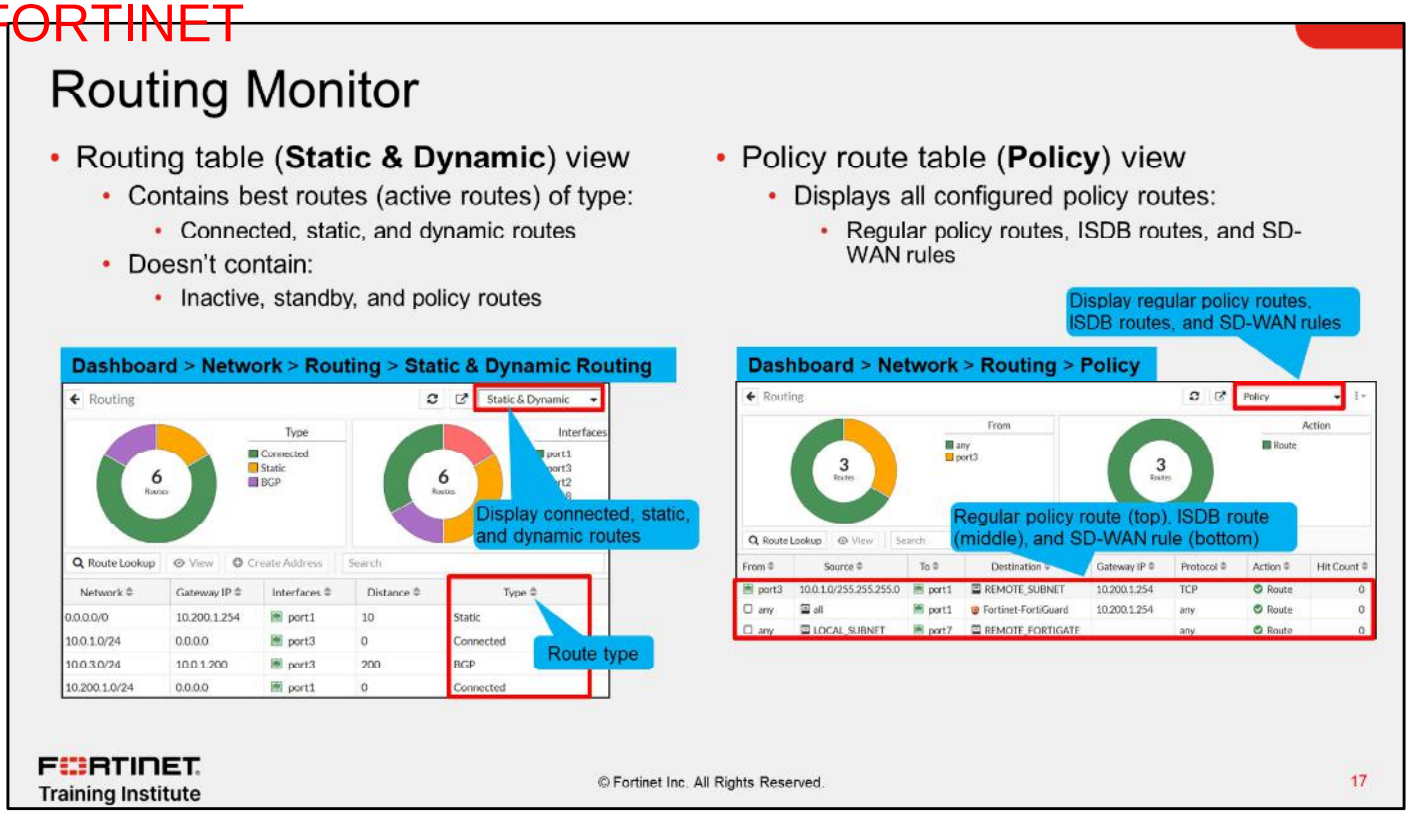
Good job! You now understand routing on FortiGate.

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



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

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



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

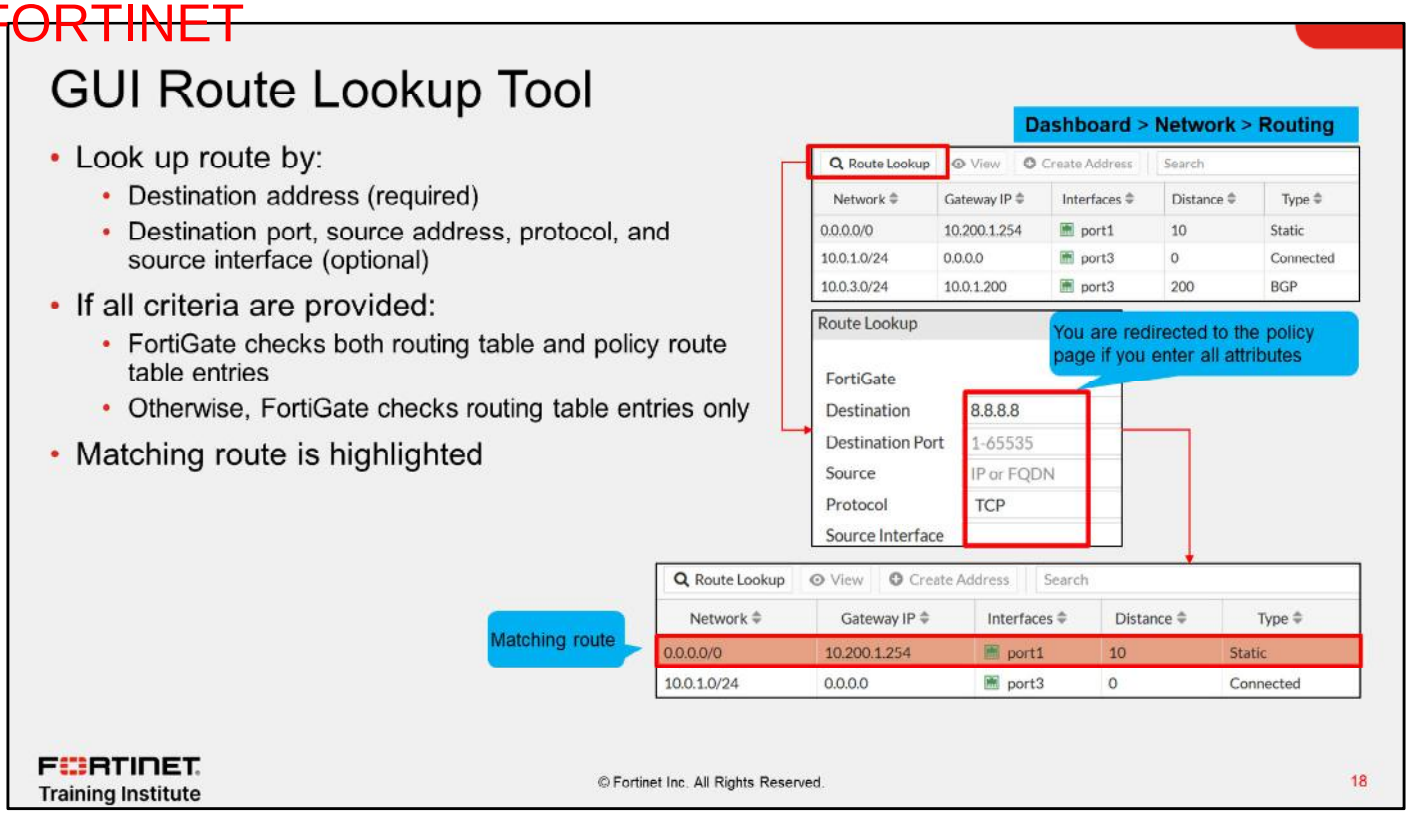
- Static: manual routes that are configured by the administrator.
- Connected: automatic routes added by FortiOS after an interface is assigned an IP address. A connected route references the interface IP address subnet.
- Dynamic: routes learned using a dynamic routing protocol such as BGP or OSPF.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

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

- Inactive routes: static and connected routes whose interfaces are administratively down or whose links are down. Static routes are also marked inactive when their gateway is detected as dead by the link health monitor.

- Standby routes: These are active routes that are removed from the routing table because they are duplicate and have higher distances. For instance:
  - A second static default route with a higher distance than another static default route.
  - A dynamic route such as BGP or OSPF, to the same destination as another static route. However, the dynamic route is not displayed in the routing table because the static route has a lower distance.

- Policy routes: These include regular policy routes, ISDB routes, and SD-WAN rules. Policy routes are viewed in a separate table—the policy route table. To view the policy route table entries, select **Policy**.

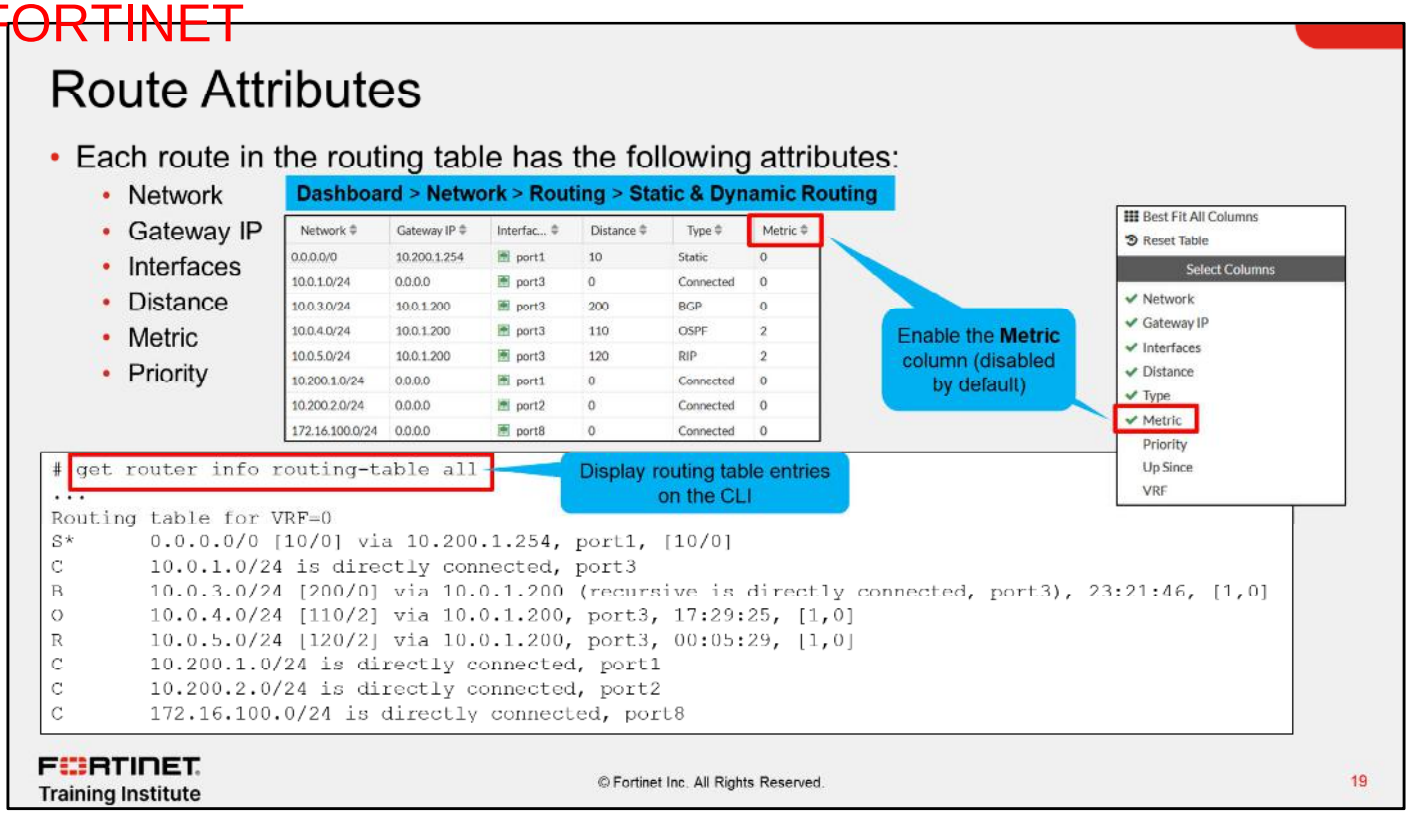


You can perform a route lookup on the routing monitor widget by clicking **Route Lookup**. Then, you must indicate at least the destination address to look up for, and optionally, the destination port, source address, protocol, and source interface.

The way the route lookup works is as follows:

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

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



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

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

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

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

Distance

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

Dashboard > Network > Routing > Static & Dynamic

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

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

* Hardcoded

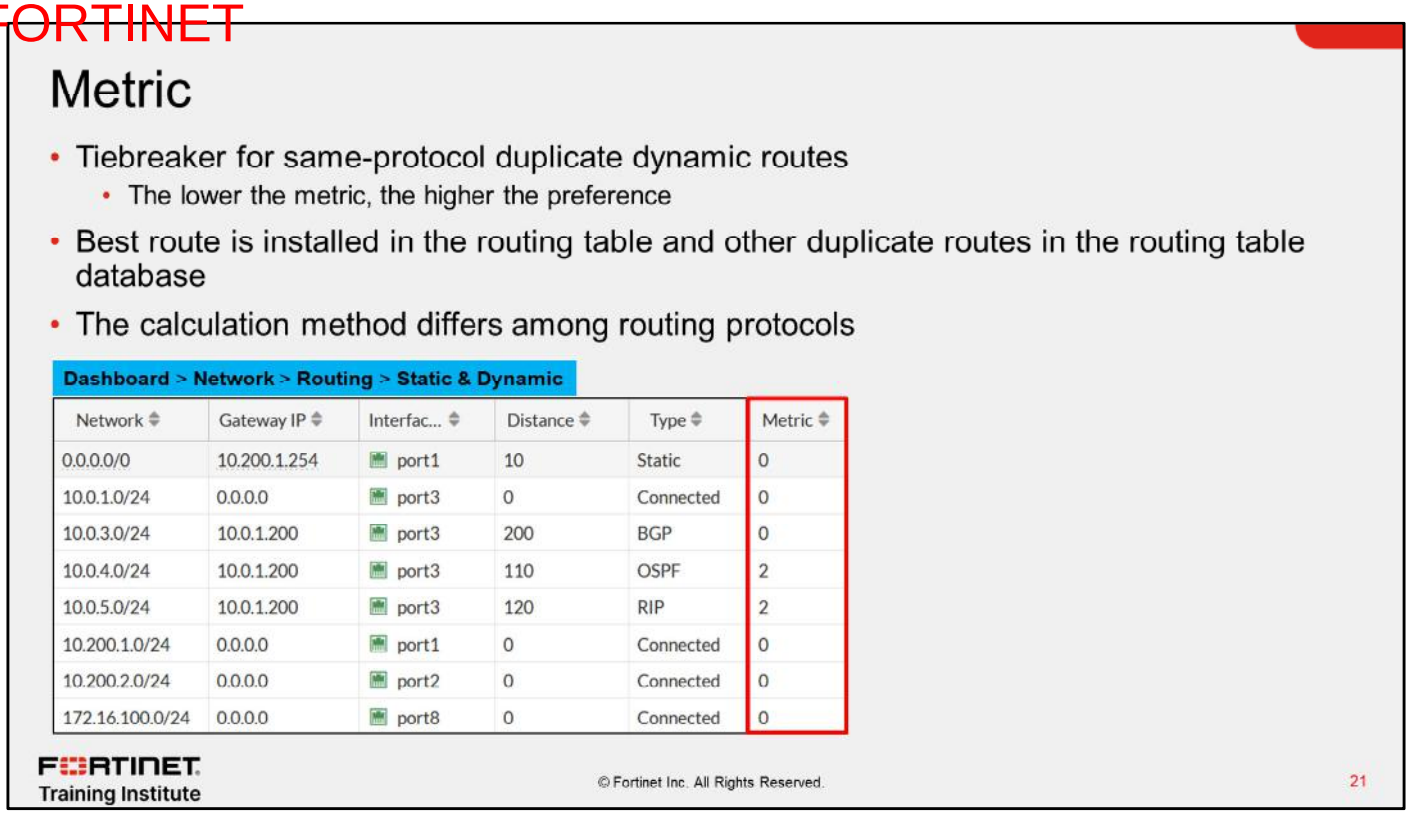
FORTINET Training Institute

20

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

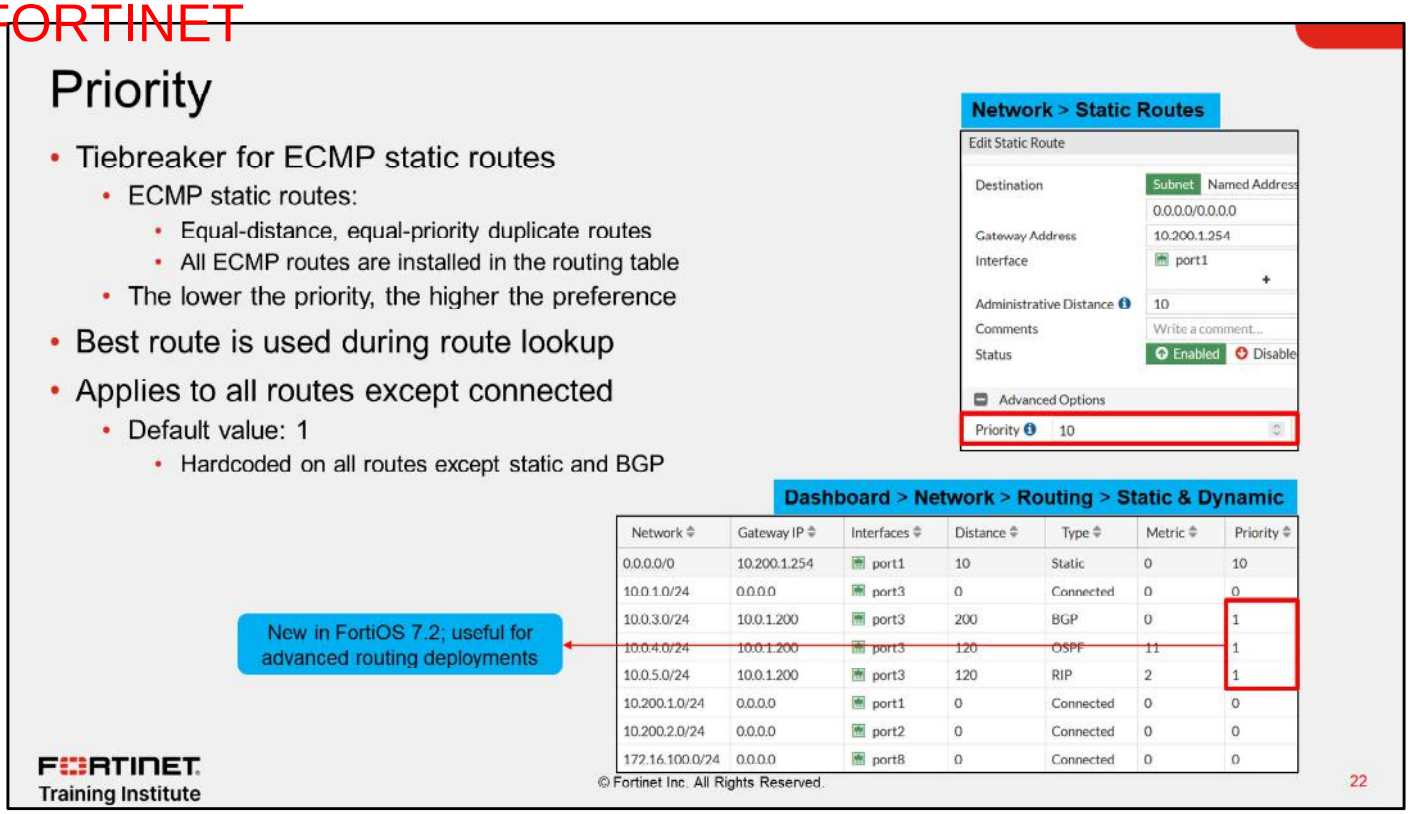
You can set the distance for all route types except connected and IS-IS routes. This slide shows the default values per type of route.

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



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

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



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

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

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

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

For static routes, you can configure the priority setting under the **Advanced Options** on the FortiGate GUI, as shown on this slide.

To view the priority in the routing monitor widget, you must enable the priority column (disabled by default). You can also view the priority on the routing table on the FortiGate CLI, which you will learn about later in this lesson.

Knowledge Check

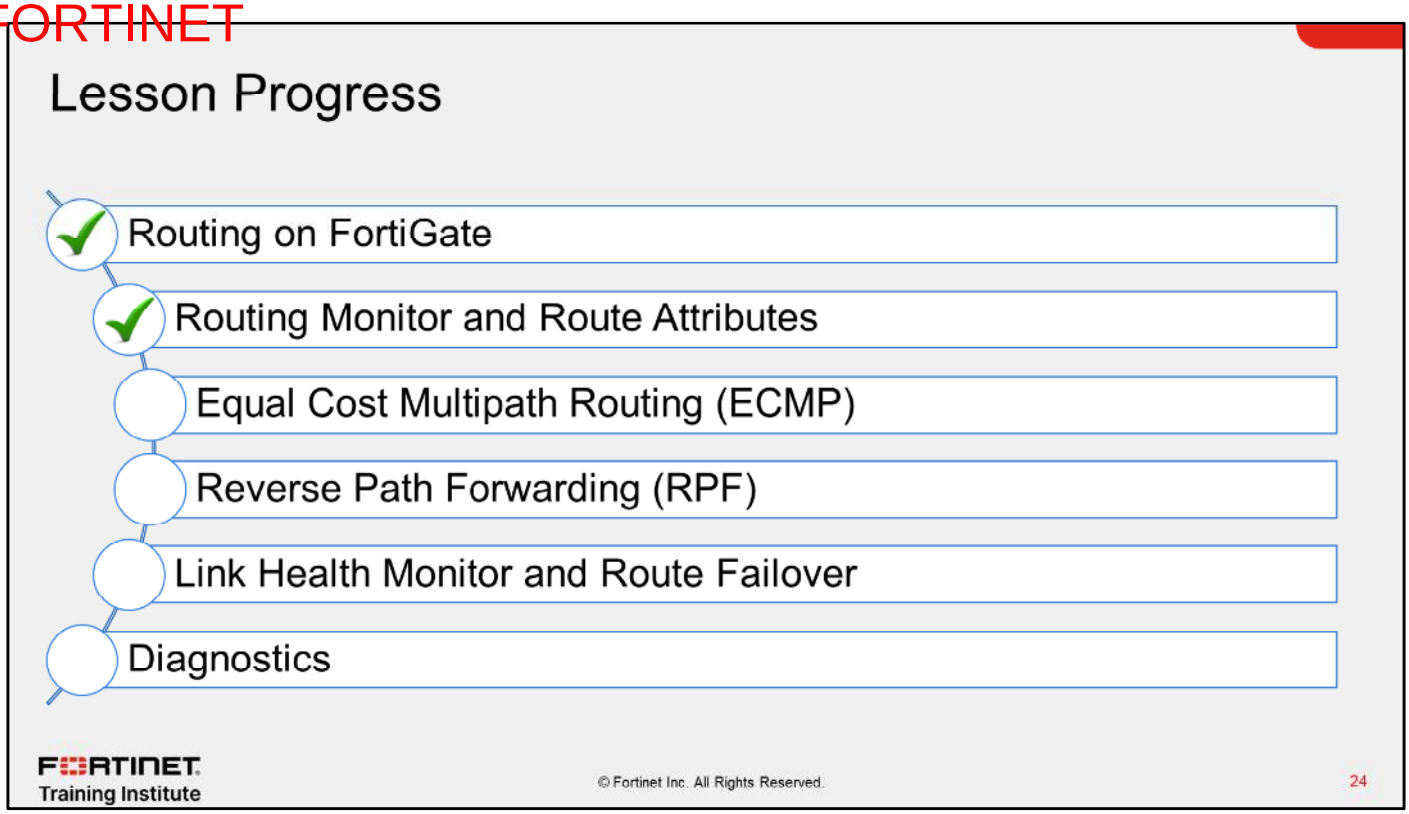
1. The priority attribute applies to which type of routes?
   - ✓ A. Static
   - B. Connected

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

3. Which routes are installed in the routing table?
   - ✓ A. Best active routes
   - B. Policy routes

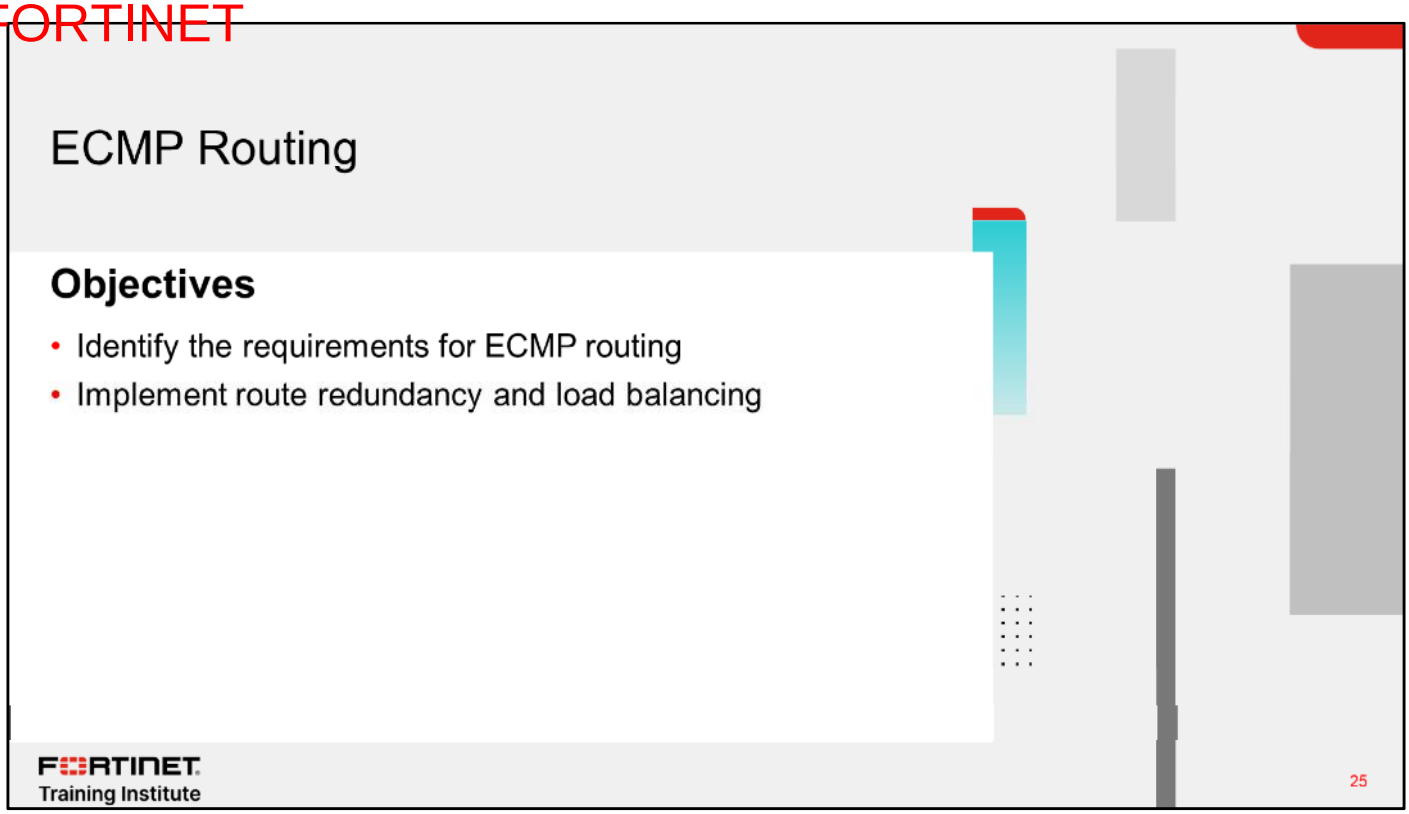
FORTINET Training Institute

23



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

Now, you will learn about ECMP routing.



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

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

ECMP

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

Dashboard > Network > Routing > Static & Dynamic

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

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

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

FORTINET Training Institute

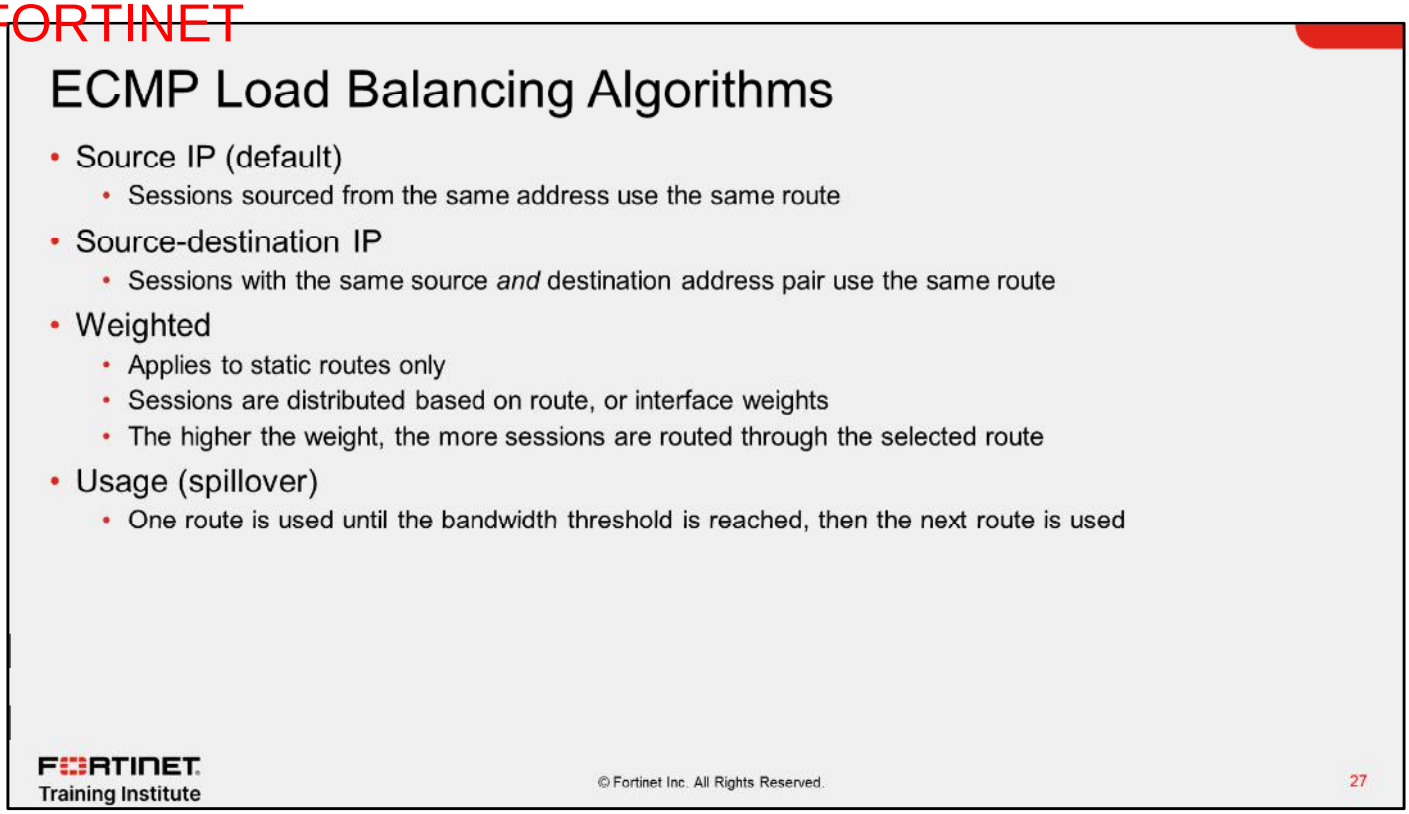
26

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

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

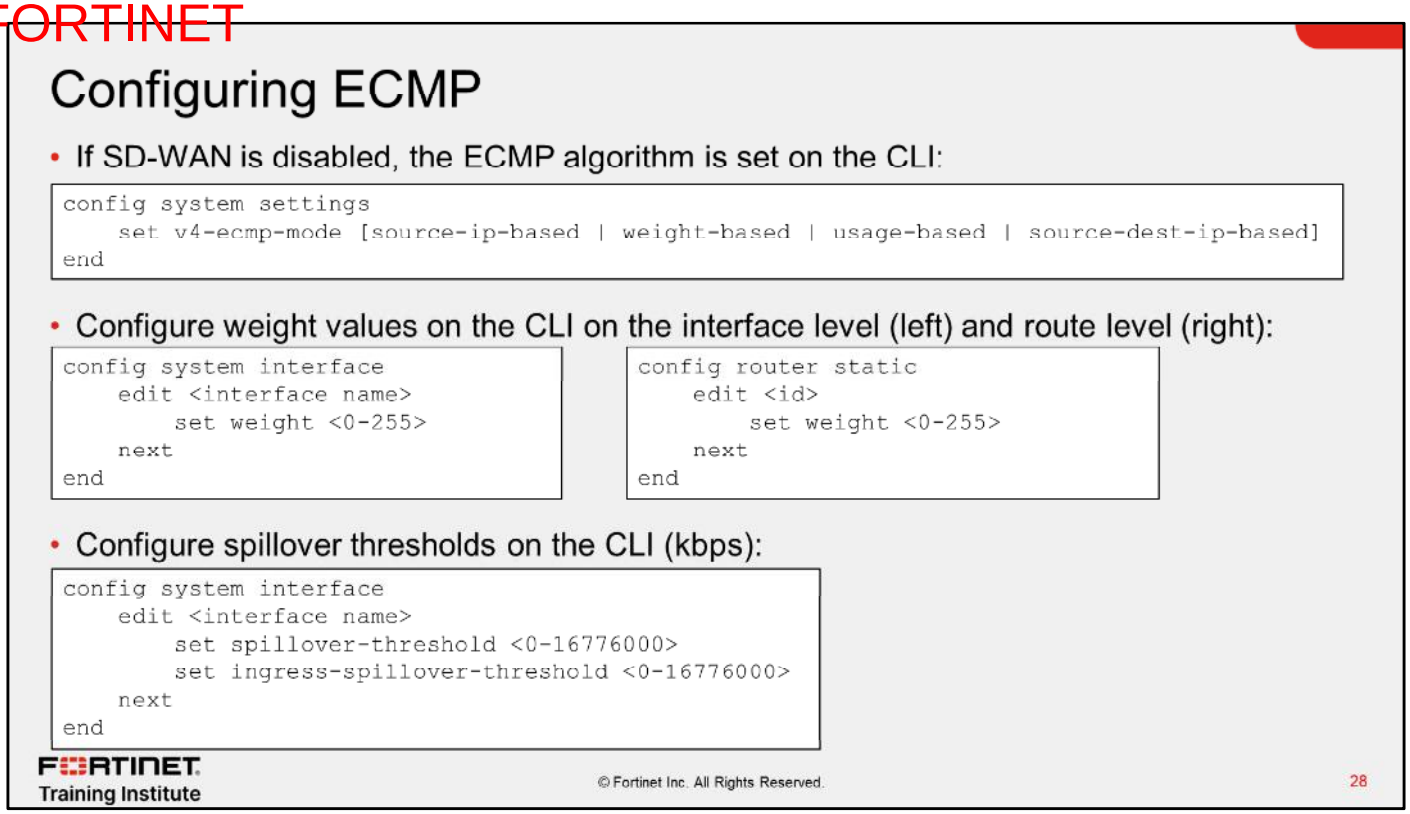
The example on this slide shows two ECMP static routes, two ECMP BGP routes, and two ECMP OSPF routes. For each ECMP group, the destination subnet, distance, metric, and priority are the same.

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



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

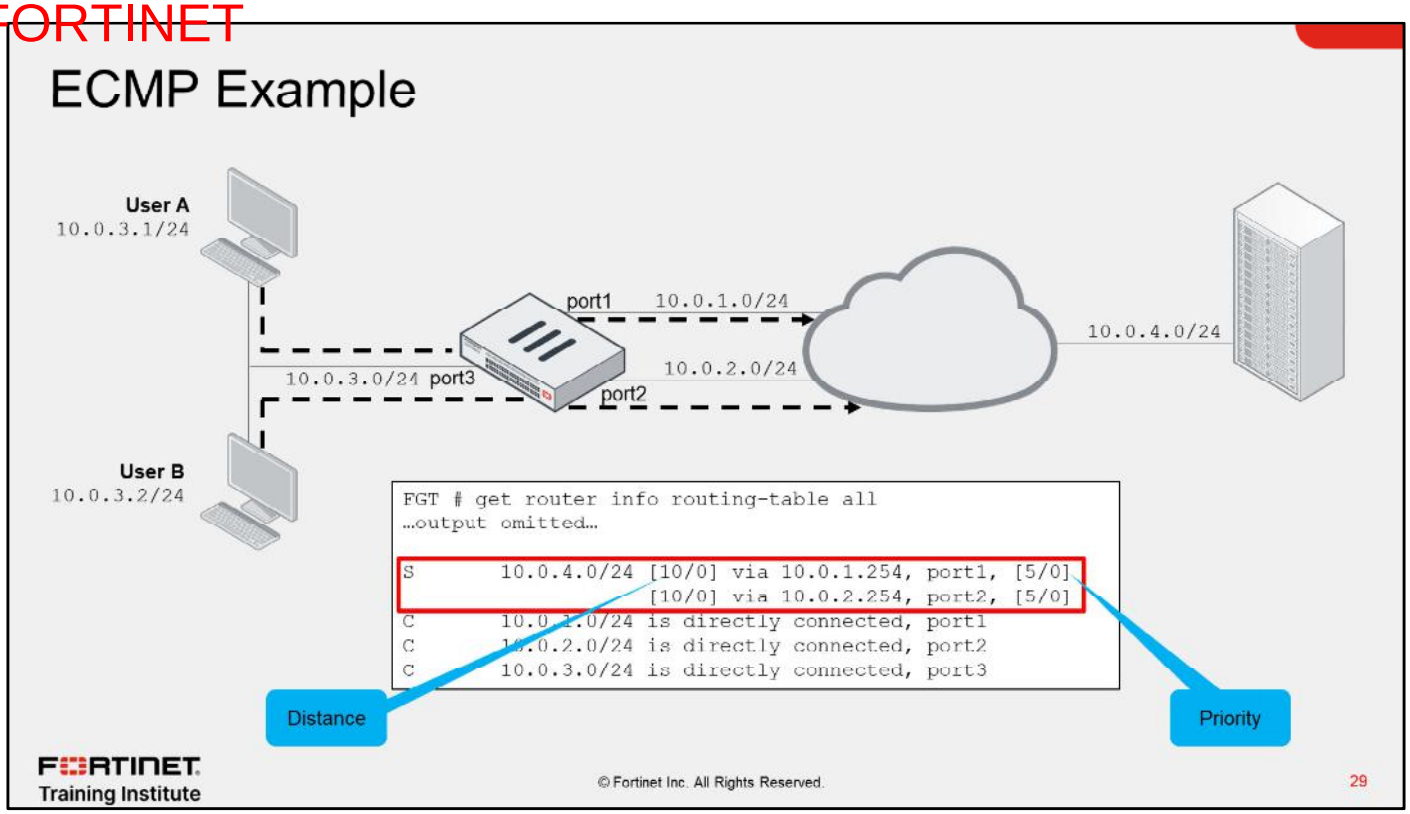
- Source IP: This is the default algorithm. FortiGate uses the same ECMP route to route sessions sourced from the same address.
- Source-destination IP: FortiGate uses the same ECMP route to route sessions with the same source-destination IP address pair.
- Weighted: Applies to static routes only. FortiGate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



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

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

For spillover to work, you must also configure the egress and ingress spillover thresholds, as shown on this slide. The thresholds are set to `0` by default, which disables spillover check. For weighted algorithm, you must configure the weights on the interface level or route level, as shown on this slide.

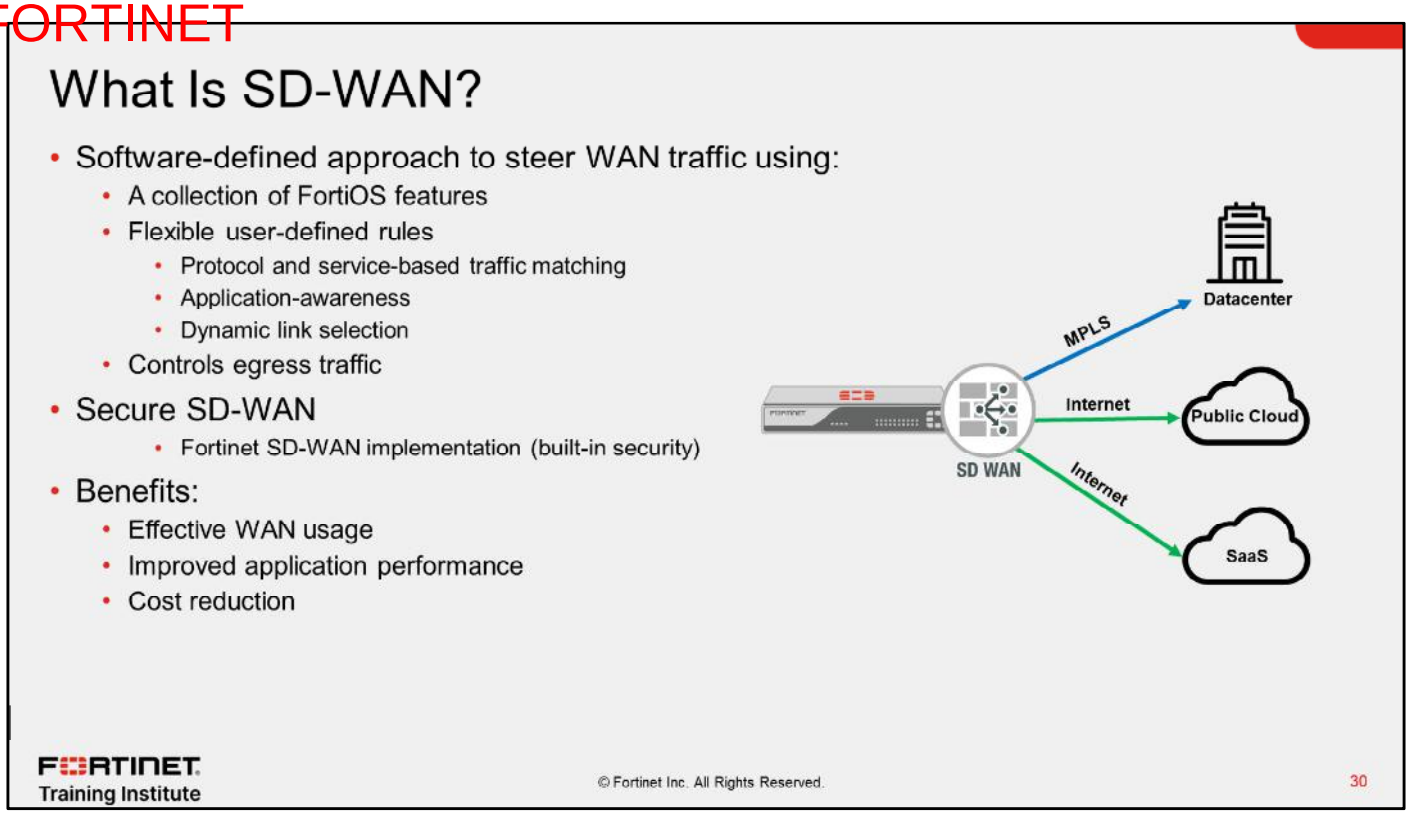


In the scenario shown on this slide, FortiGate has ECMP routes for the `10.0.4.0/24` subnet on port1 and port2. Using the default ECMP algorithm (source IP based), FortiGate may use any of the two routes to route traffic from user A and user B.

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

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

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



According to Gartner, software-defined WAN (SD-WAN) provides dynamic, policy-based, application path selection across multiple WAN connections and supports service chaining for additional services such as WAN optimization and firewalls. Fortinet implementation of SD-WAN is called secure SD-WAN because it also provides security by leveraging the built-in security features available in FortiOS.

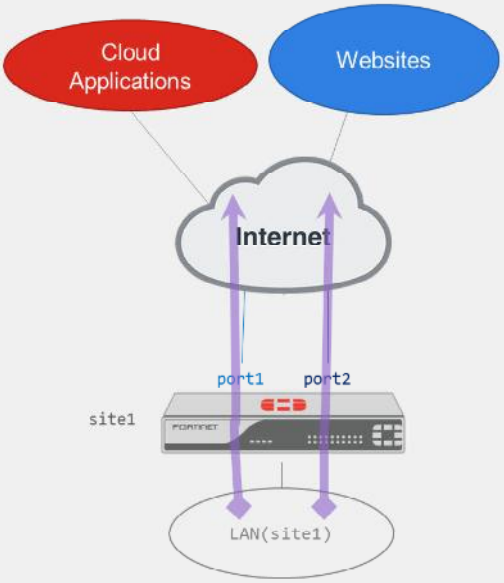
Secure SD-WAN relies on well-known FortiOS features such as IPsec, auto-discovery VPN (ADVPN), link monitoring, advanced routing, internet services database (ISDB), traffic shaping, UTM inspection, and load balancing. The administrator can then combine these features and set rules that define how FortiGate steers traffic across the WAN based on multiple factors such as the protocol, service, or application identified for the traffic, and the quality of the links. Note that SD-WAN controls egress traffic, not ingress traffic. This means that the return traffic may use a different link from the one SD-WAN chose for egress.

One benefit of SD-WAN is effective WAN usage. That is, you can use public (for example, broadband, LTE) and private (for example, MPLS) links to securely steer traffic to different destinations: internet, public cloud, private cloud, and the corporate network. This approach of using different types of links to connect sites to private and public networks is known as hybrid WAN. A hybrid WAN reduces costs mainly because administrators usually steer more traffic over low-cost fast internet links than high-cost slow private links. The result is that private links, such as MPLS links, are often used to steer critical traffic only, or as failover links for high availability.

Another benefit of SD-WAN is an improved application performance because you can steer traffic through the best link that meets the application requirements. During congestion, you can leverage traffic shaping to prioritize sensitive and critical applications over less important ones. Also, the support of ADVPN shortcuts enables SD-WAN to use direct IPsec tunnels between sites to steer traffic, resulting in lower latency for traffic between the sites (spokes), and less load on the central locations (hubs).

Direct Internet Access With SD-WAN

- Traffic steered across multiple internet links
- Typical operation:
  - Critical/sensitive traffic expedited and steered over best performing links
  - Costly links used for critical traffic or failover
  - Static default routing



FORTINET Training Institute

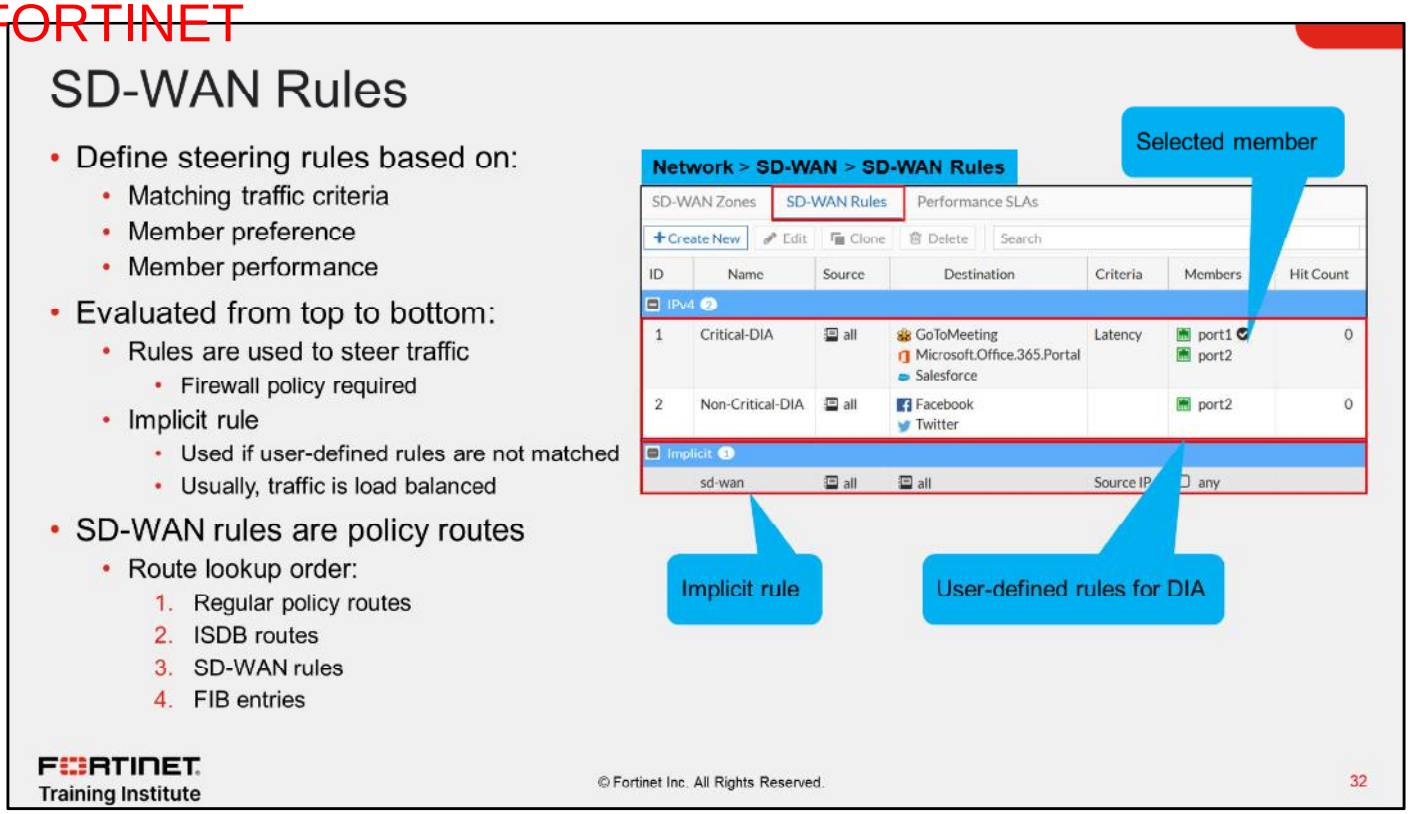
31

Direct internet access (DIA), also known as local breakout, is arguably the most common use case for SD-WAN. A site has multiple internet links (also known as underlay links), and the administrator wants FortiGate to steer internet traffic across the links (also known as members). The links are connected to FortiGate using different types of physical interfaces: physical port, VLAN, link aggregation (LAG), USB modem, or through FortiExtender.

Usually, sensitive traffic is expedited and steered over the best performing links, while non-critical traffic is distributed across one or more links using a best effort approach. Costly internet links are commonly used as backup links, or to steer critical traffic only.

For routing, a typical configuration makes use of static default routes. However, in some cases, BGP is used between the ISP and FortiGate, especially if the site must advertise a public IP prefix.

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

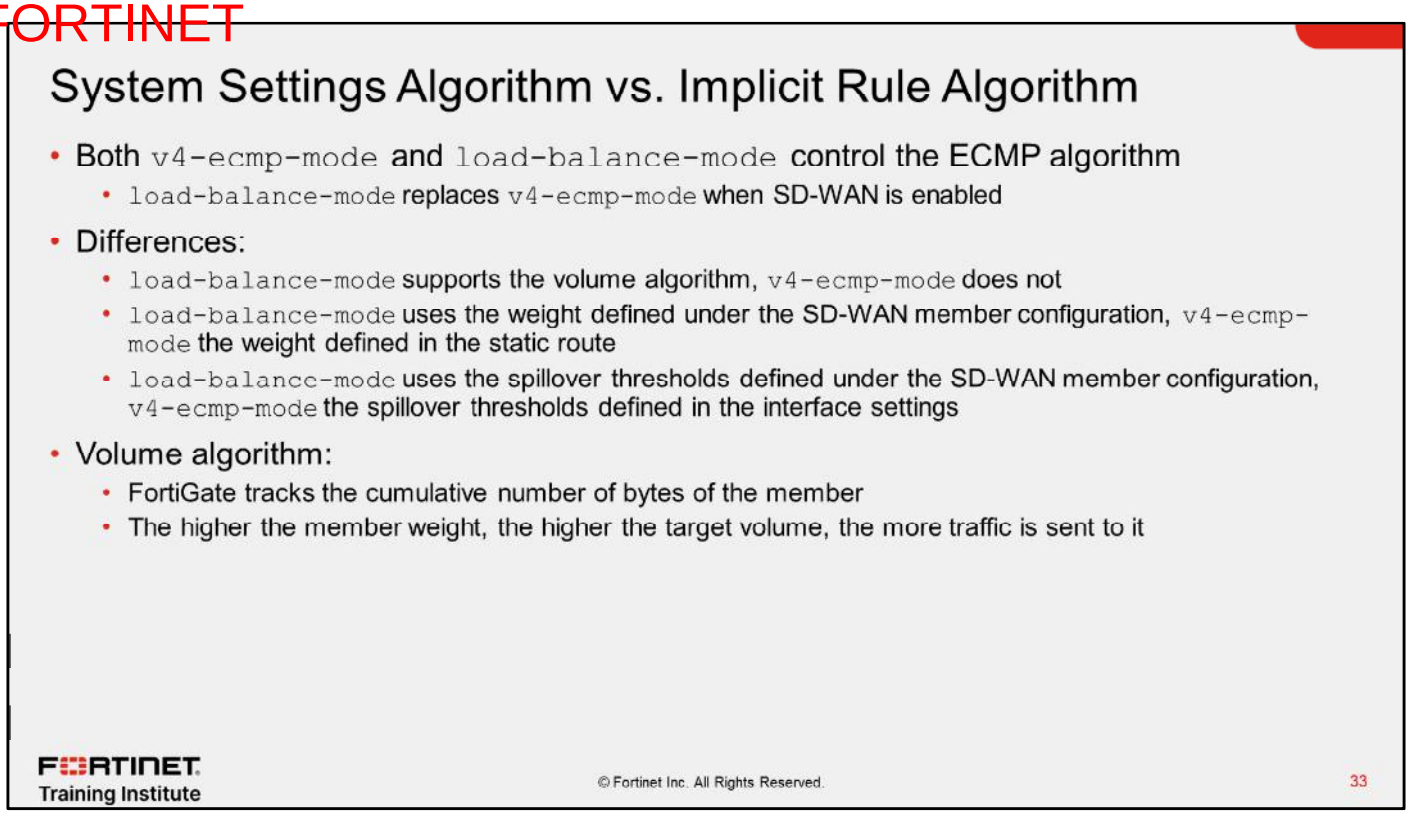


SD-WAN rules represent the intelligence of the SD-WAN solution and the software-defined aspect of it. When you configure an SD-WAN rule, you first define the application or traffic pattern to match. After that, you indicate the preferred members and/or zones to steer the matching traffic to, and in some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

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

SD-WAN rules are essentially policy routes. Like regular policy routes, SD-WAN rules route traffic based on multiple criteria. That is, when you configure an SD-WAN rule, the kernel installs a corresponding policy route that reflects the source, destination, service, and outgoing interfaces configured in the SD-WAN rule. When FortiGate performs a route lookup, it checks the routes in the order of sequence shown on this slide. For example, SD-WAN rules have precedence over FIB entries, but not over regular policy routes.

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



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

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

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

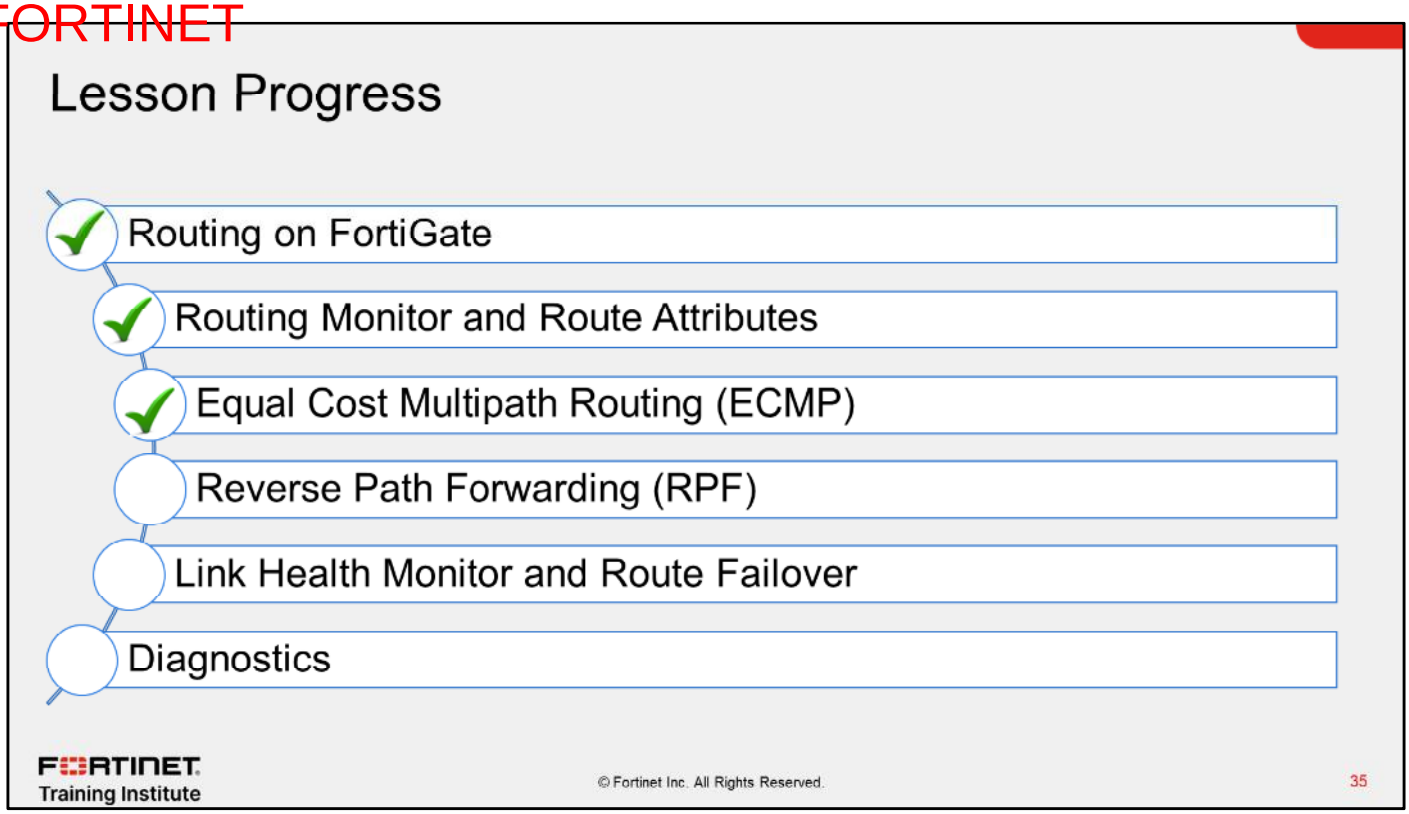
Knowledge Check

1. What is the default ECMP algorithm on FortiGate?
   - A. Weighted
   - ✓ B. Source IP

2. How does FortiGate load balance traffic when using the spillover algorithm in ECMP routing?
   - ✓ A. Sessions are distributed based on interface threshold.
   - B. Sessions are distributed based on route weight.

FORTINET Training Institute

34

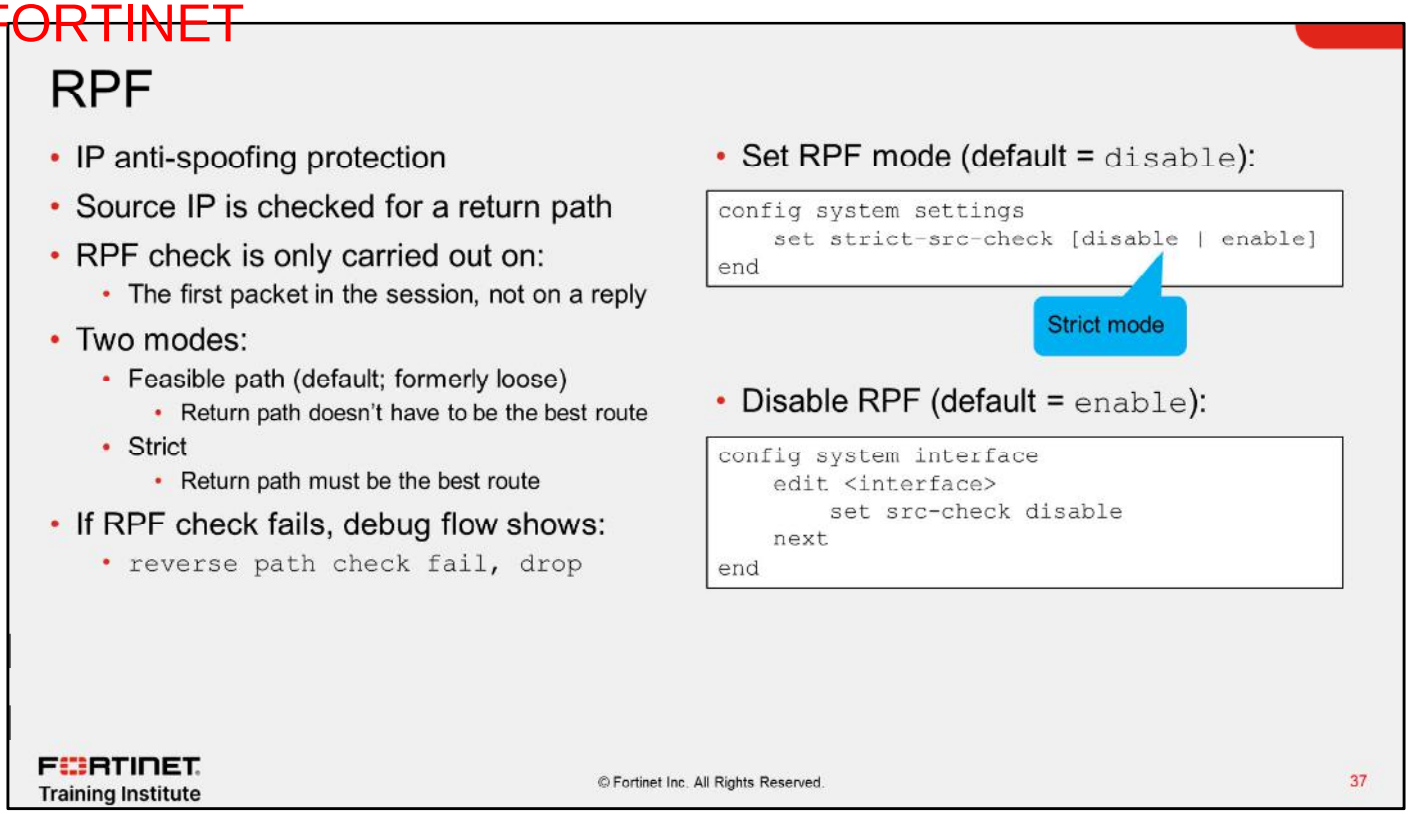


Good job! You now understand ECMP routing.

Now, you will learn about reverse path forwarding.

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

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



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

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

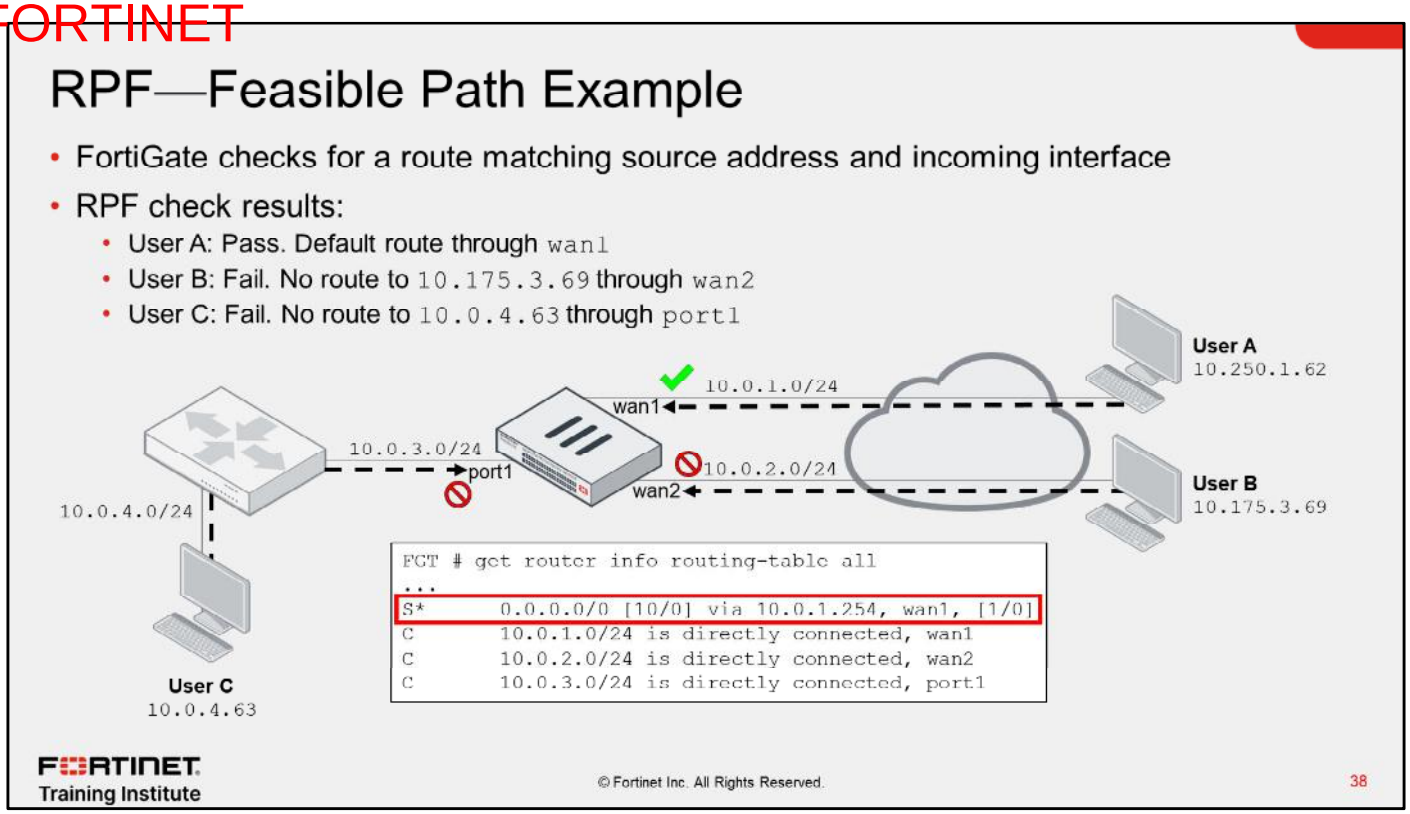
FortiGate performs an RPF check only on the first packet of a new session. That is, after the first packet passes the RPF check and FortiGate accepts the session, FortiGate doesn't perform any additional RPF checks on that session.

There are two RPF check modes:

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

- Strict: In this mode, FortiGate also verifies that the matching route is the best route in the routing table. That is, if the routing table contains a matching route for the source address and incoming interface, but there is a better route for the source address through another interface, then, the RPF check fails.

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



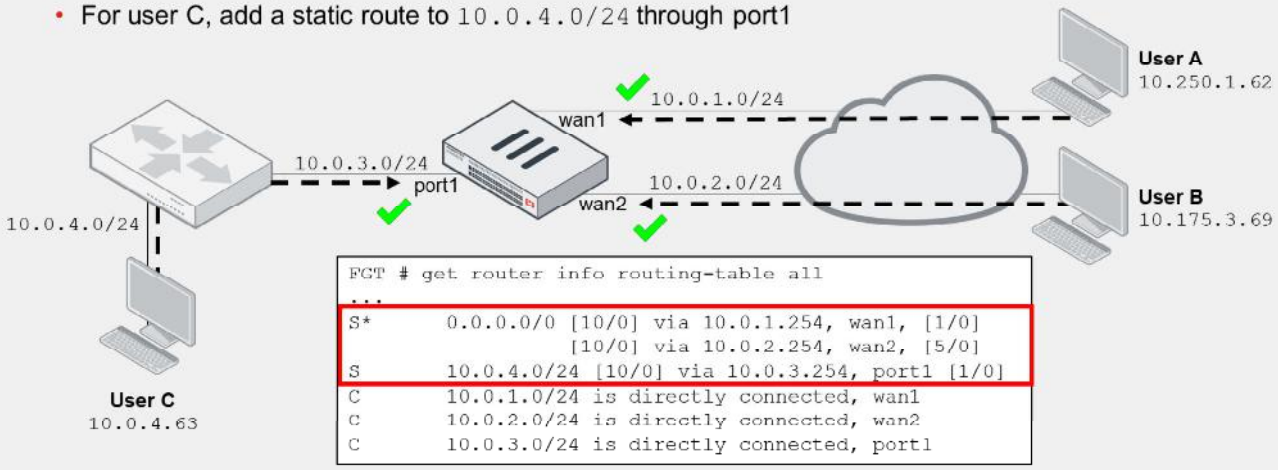
The example on this slide shows a FortiGate device using the feasible path RPF check mode. When FortiGate performs RPF check, it checks in the routing table for a route that matches the source address and the incoming interface of the first original packet.

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.

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




```
FCT # get router info routing-table all
...
S*      0.0.0.0/0 [10/0] via 10.0.1.254, wan1, [1/0]
                 [10/0] via 10.0.2.254, wan2, [5/0]
S       10.0.4.0/24 [10/0] via 10.0.3.254, port1 [1/0]
C       10.0.1.0/24 is directly connected, wan1
C       10.0.2.0/24 is directly connected, wan2
C       10.0.3.0/24 is directly connected, port1
```

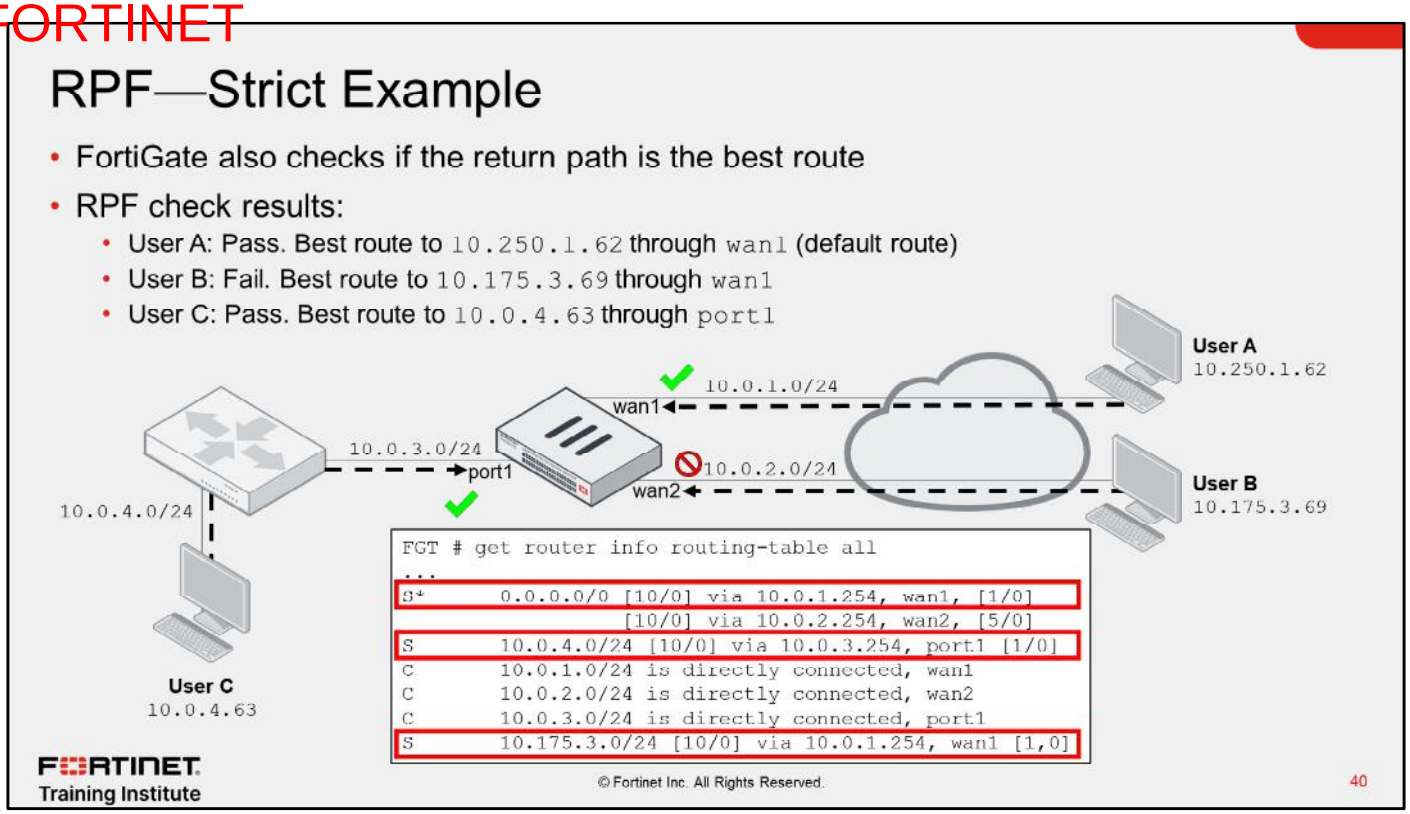
FORTINET Training Institute

39

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.



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.

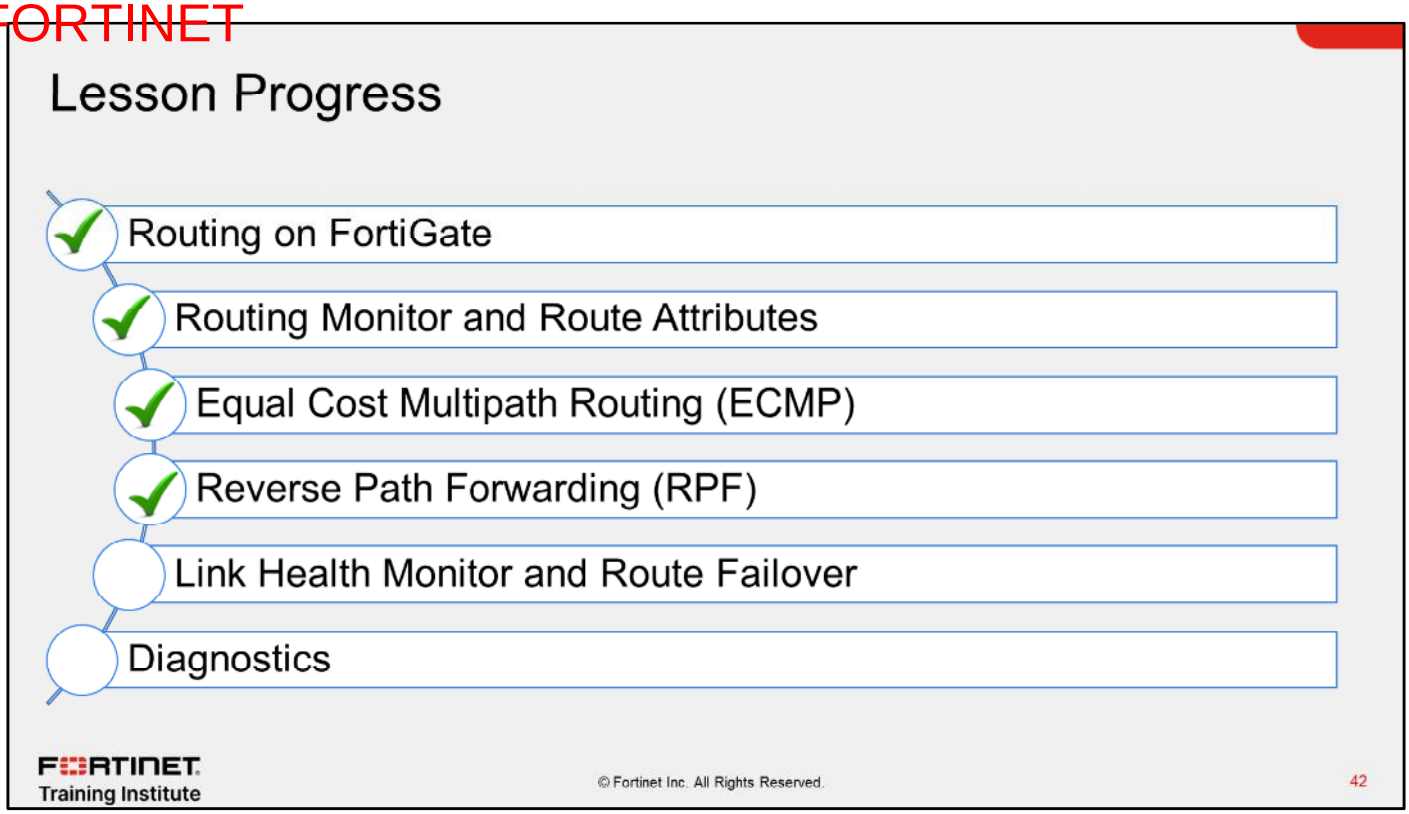
Knowledge Check

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.

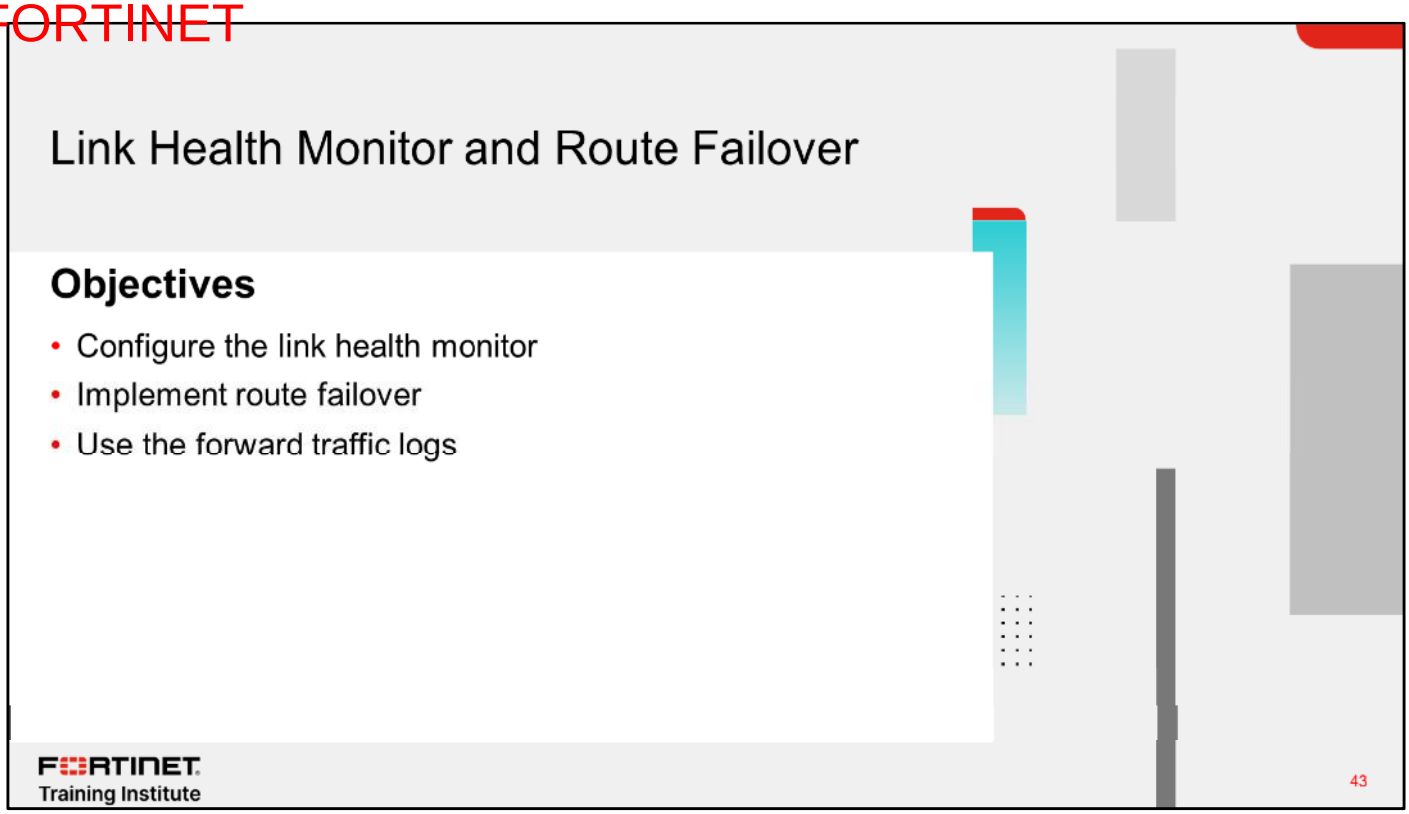
FORTINET Training Institute

41



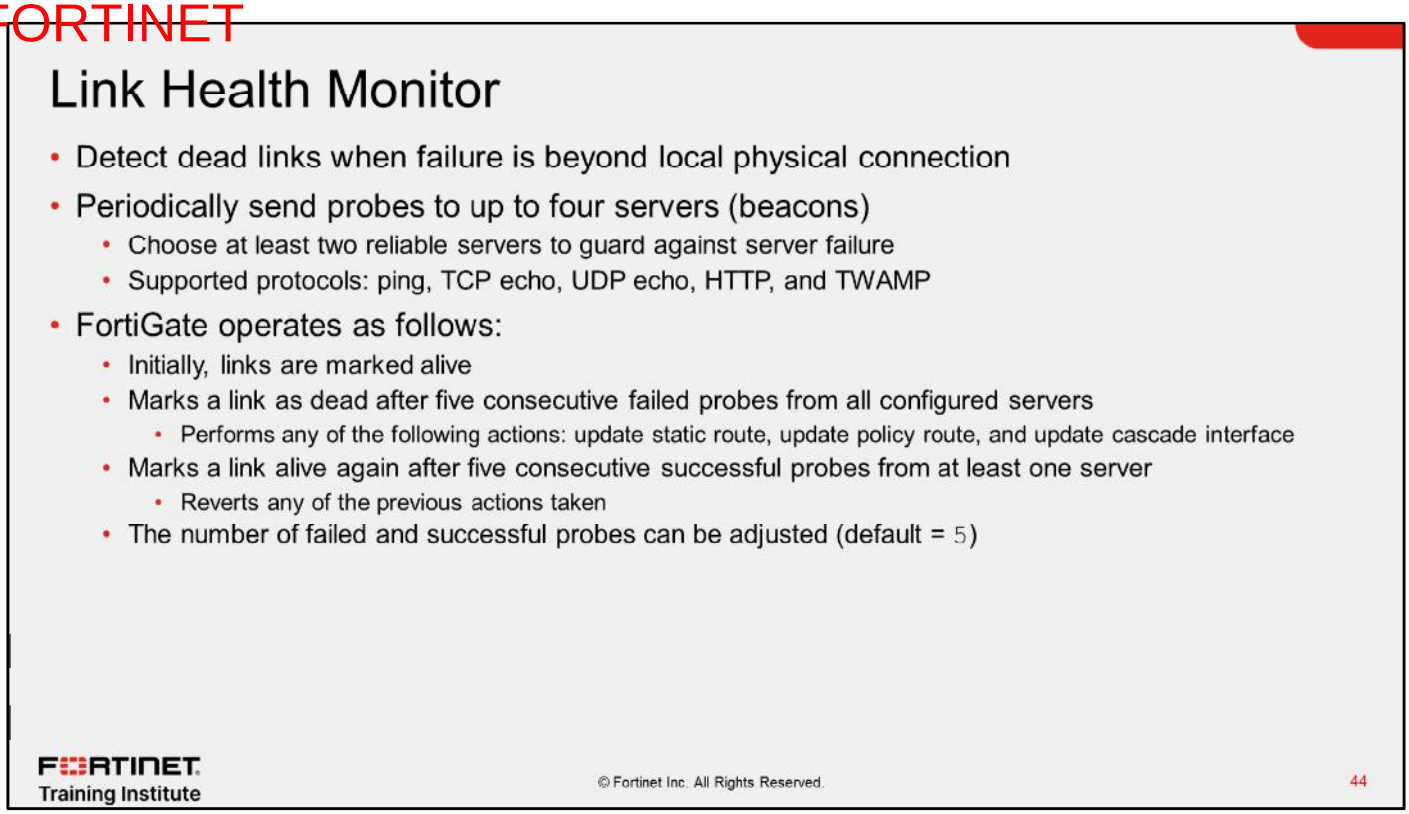
Good job! You now understand RPF.

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



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.



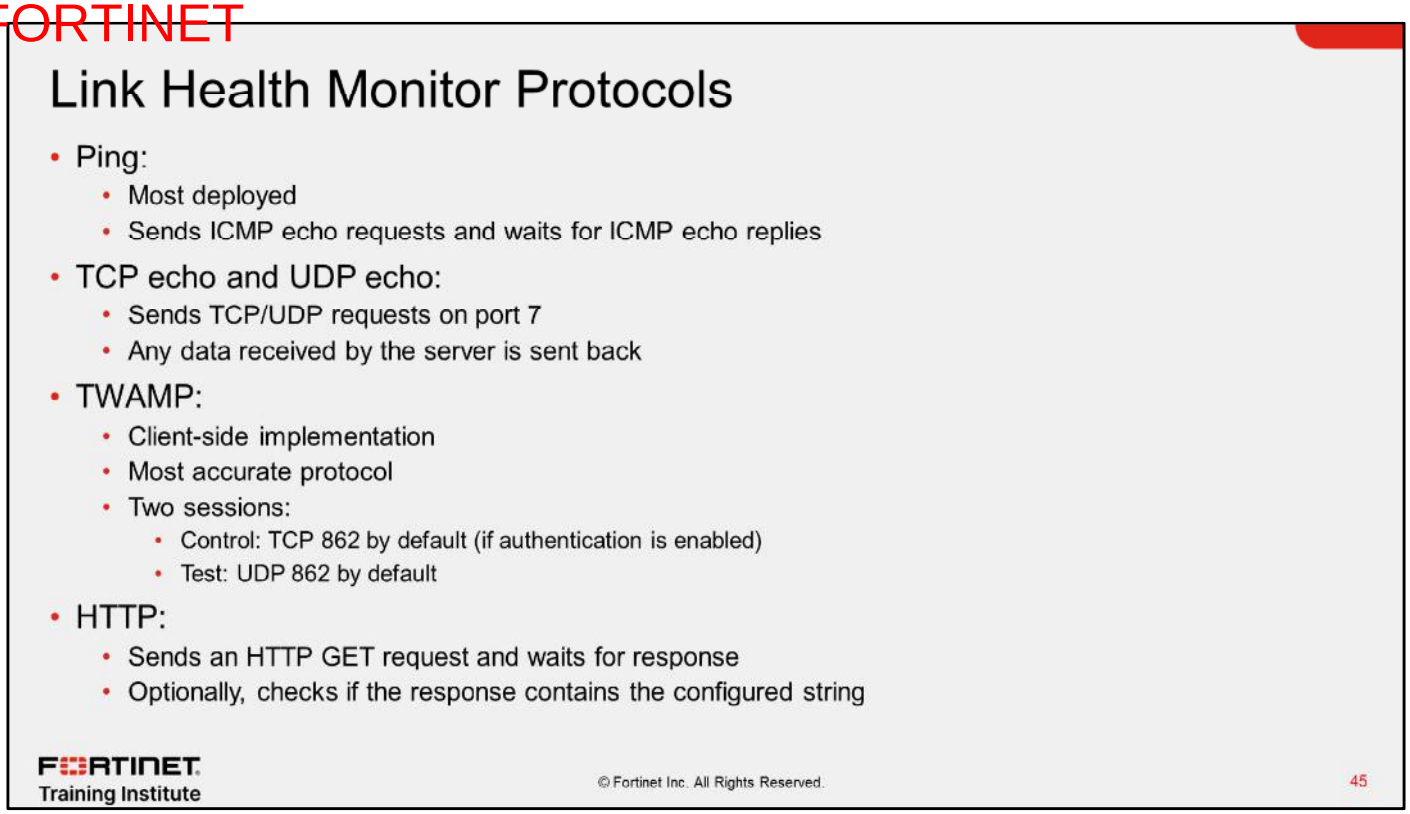
Static routes are kept in the routing table unless the associated interface is administratively down, its link goes down, or there is a duplicate route with a lower distance. Because is possible that the link circuit is dead somewhere along the path to the destination, even though the interface link is up, then it is also possible that FortiGate continues to route traffic though 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.



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

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

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

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

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

Link Health Monitor Actions

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

* Associated static routes match the configured gateway and interface in the link health monitor settings
** Associated policy routes match the configured gateway and interface in the link health monitor settings
*** Require the configuration of alert interfaces (usually, your LAN-facing interfaces)

FORTINET Training Institute

46

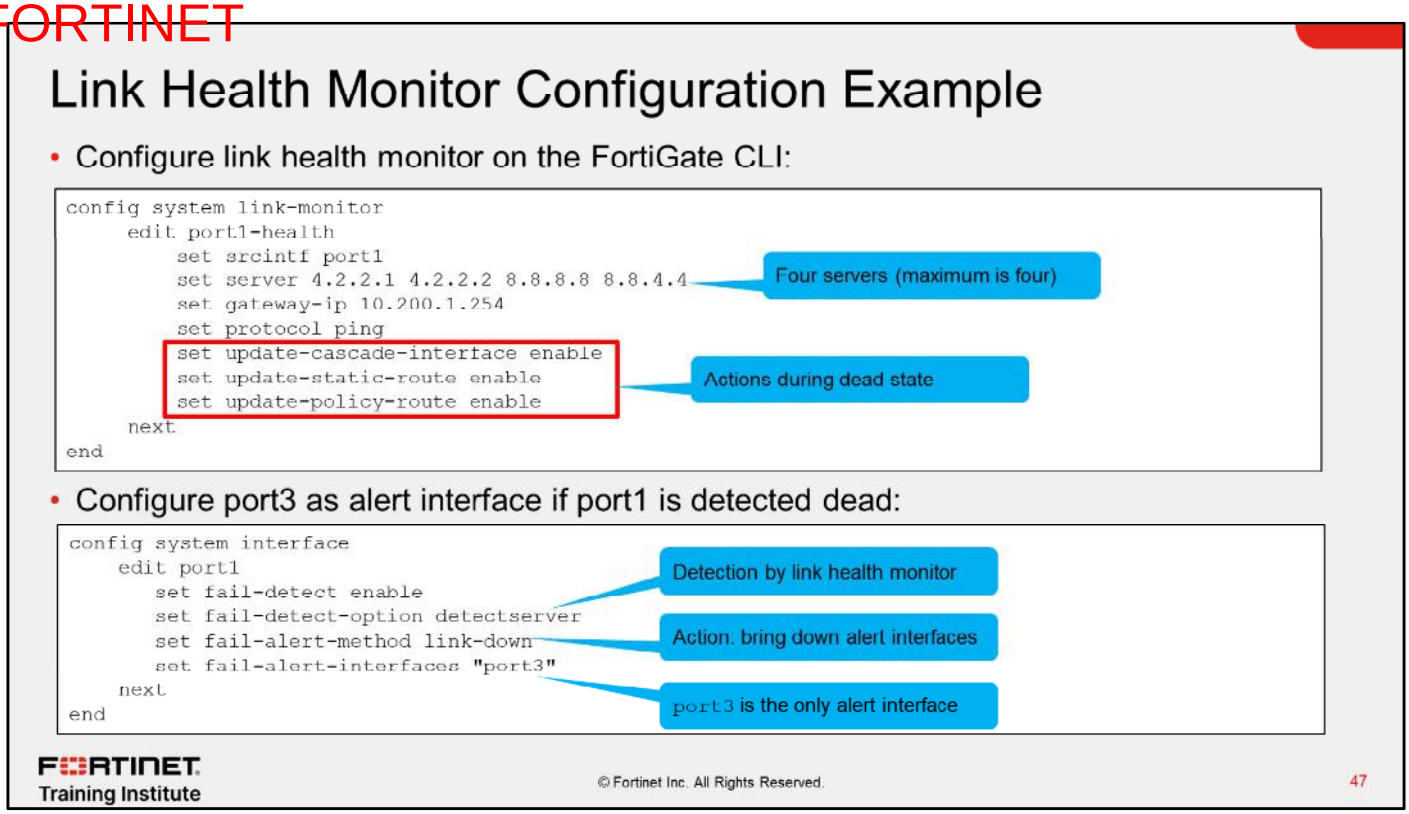
This slide describes the actions taken by link health monitor when the state of an interface changes from alive to dead, and vice-versa. All three actions are enabled by default.

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.

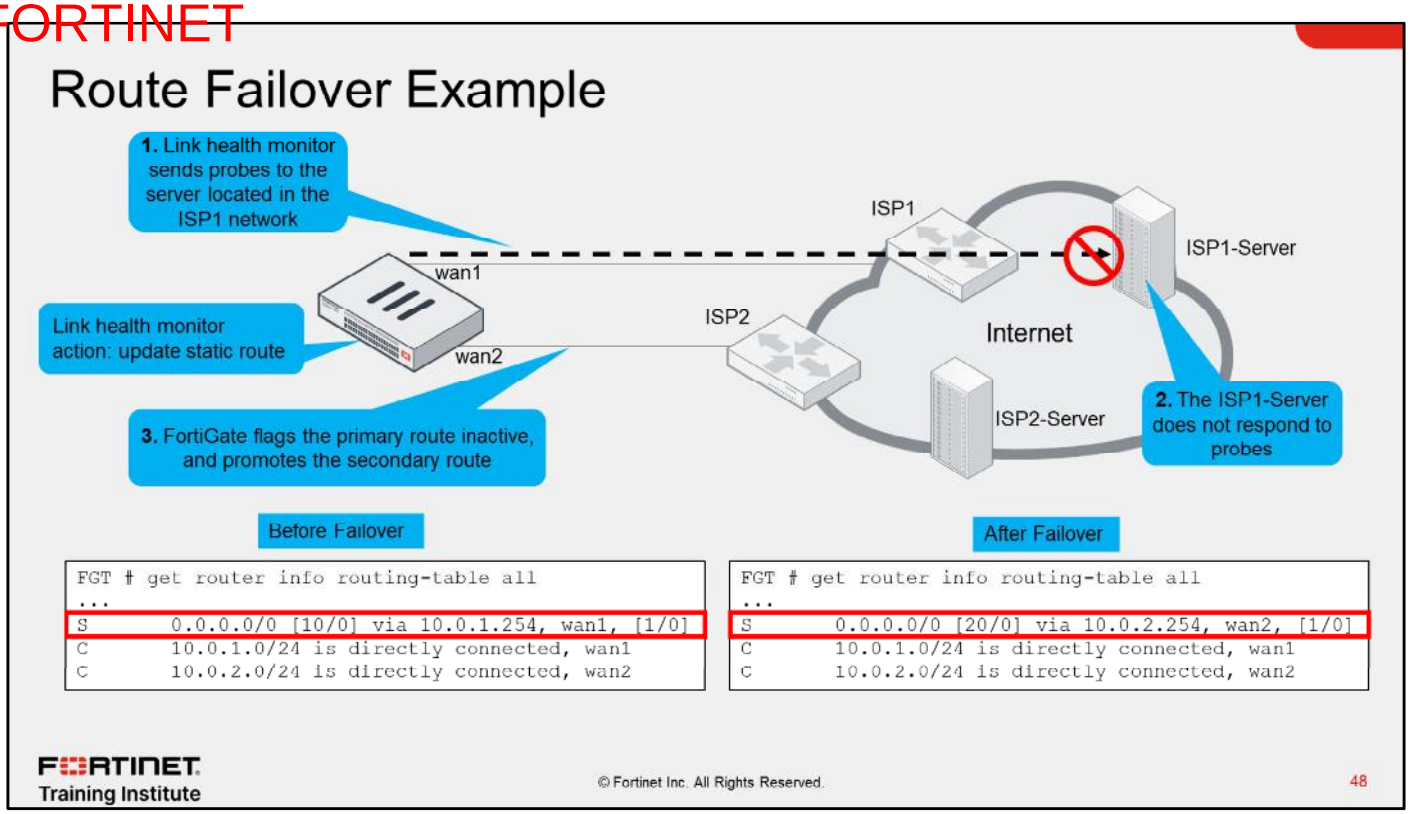
The update cascade interface action requires you to configure one or more alert interfaces. FortiGate then brings down the alert interfaces after the monitoring interface is detected dead. The goal is to force the traffic from networks behind the alert interfaces to be routed through a different device 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.



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.

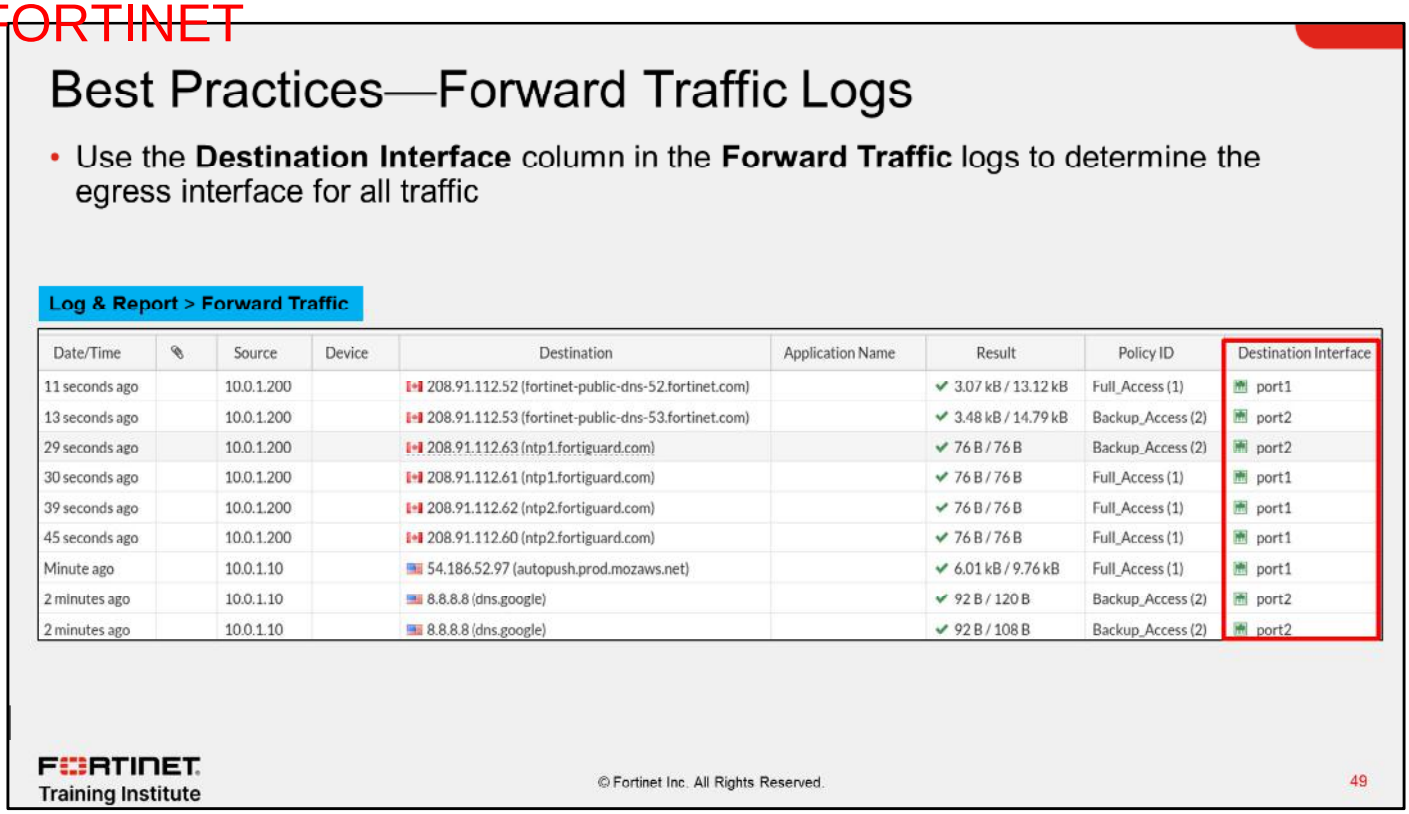
When the state of port1 changes, FortiGate updates cascade interfaces, static routes, and policy routes. For the update cascade interface action to work, you must configure the alert interfaces. This slide also shows an example of the alert interface configuration required on the monitoring interface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



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.



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.

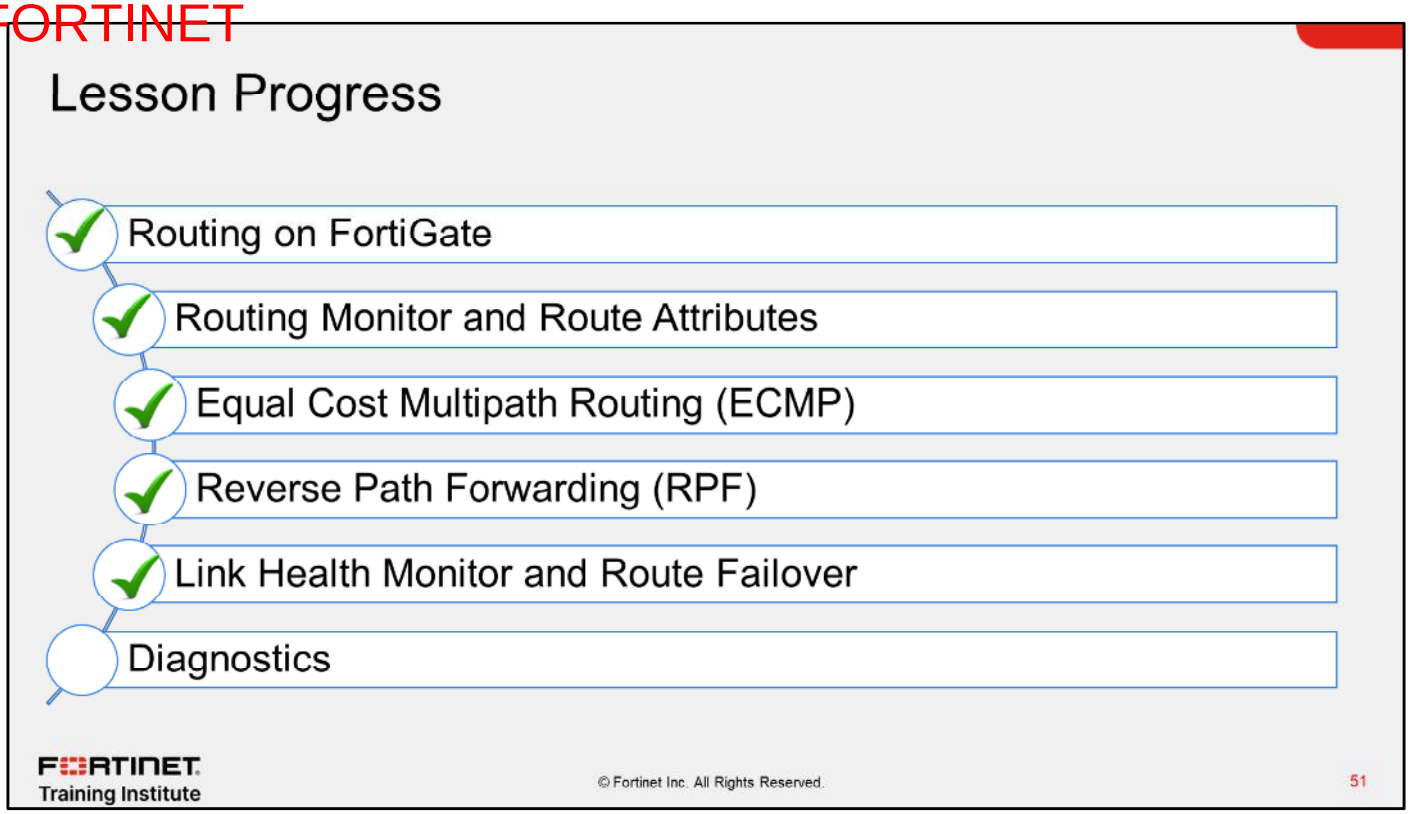
Knowledge Check

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

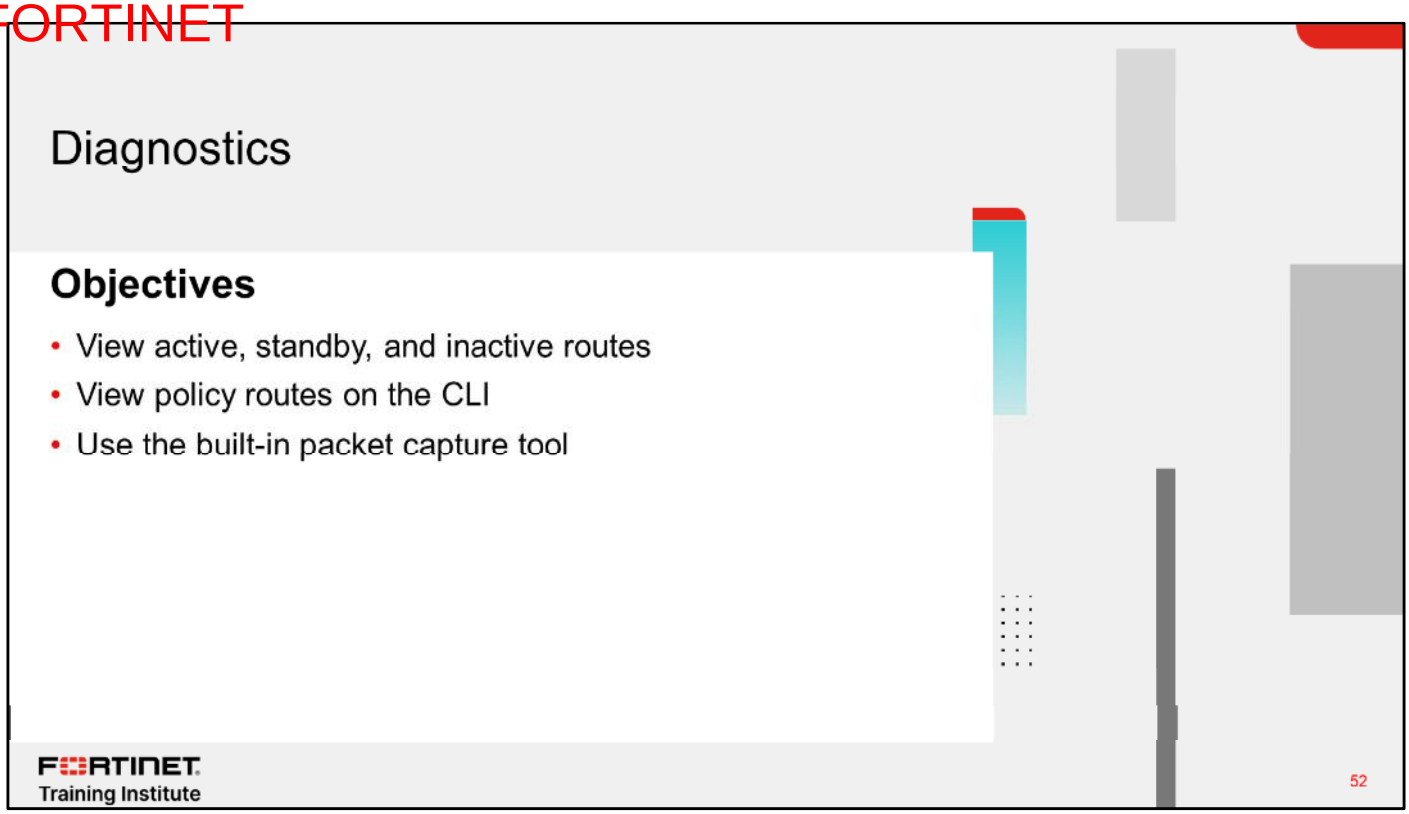
FORTINET Training Institute

50



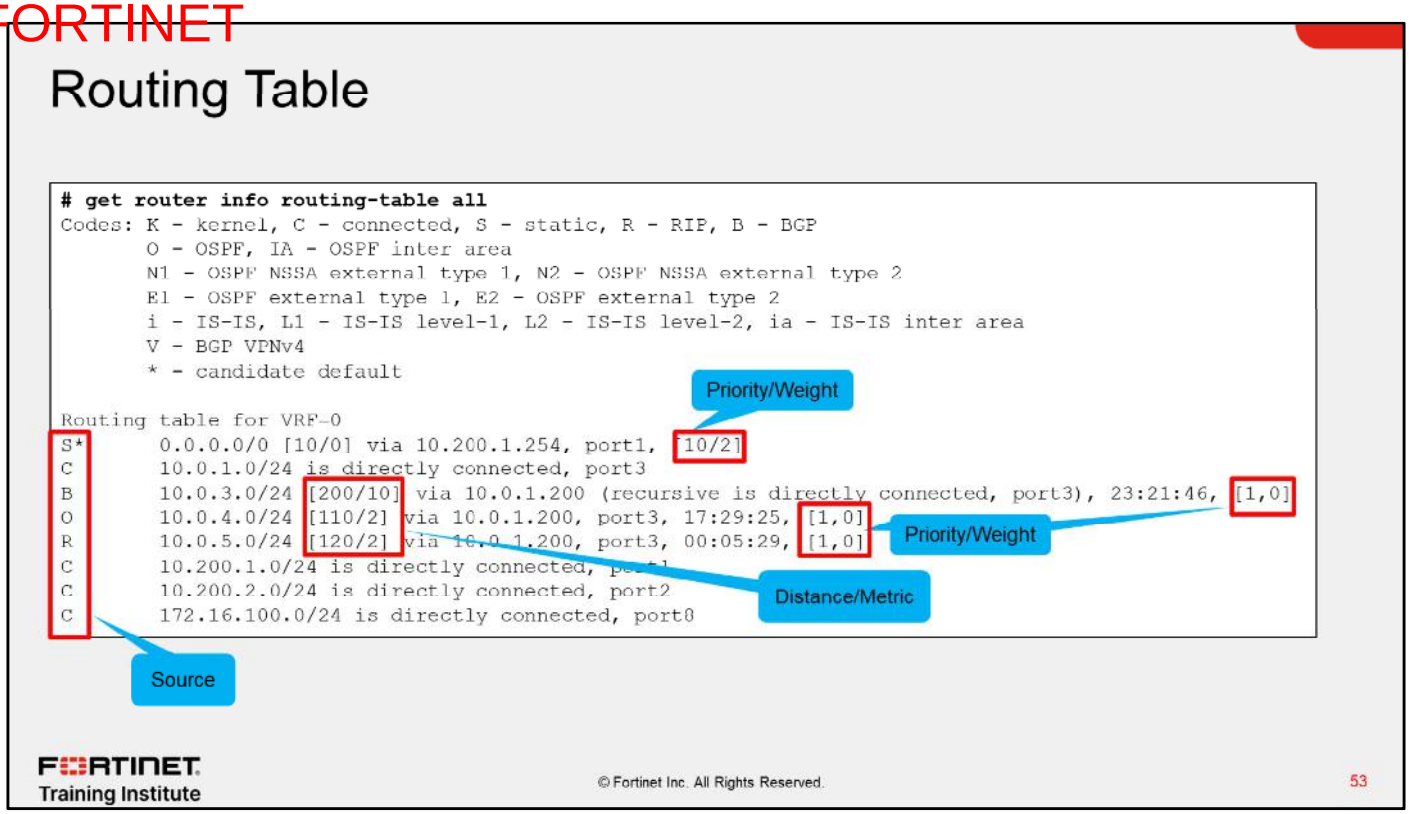
Good job! You now understand the link health monitor and route failover.

Now, you will learn about routing diagnostics.



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.



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.

Routing Table Database

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

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

Active route

Inactive route

Standby route

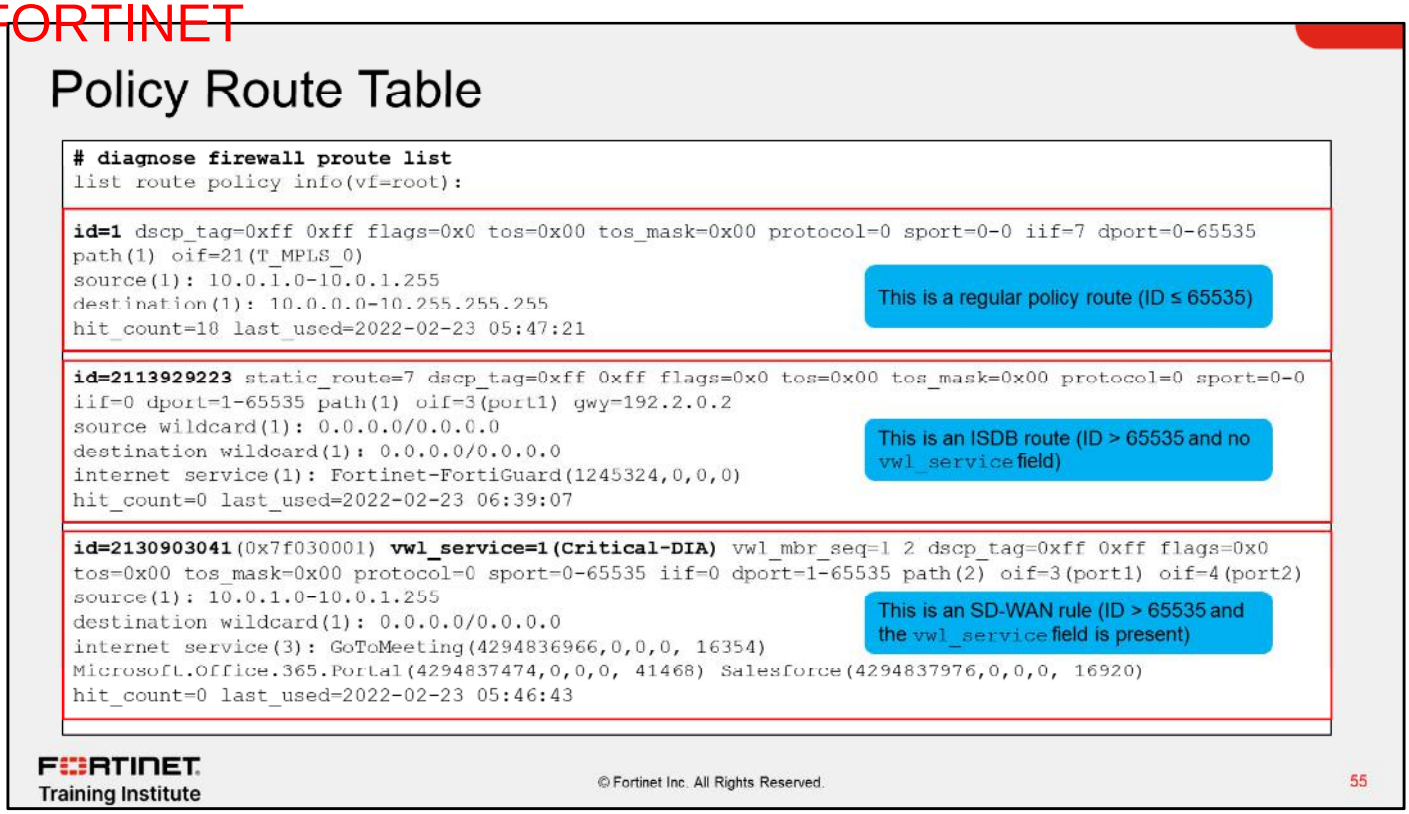
FORTINET Training Institute

54

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.

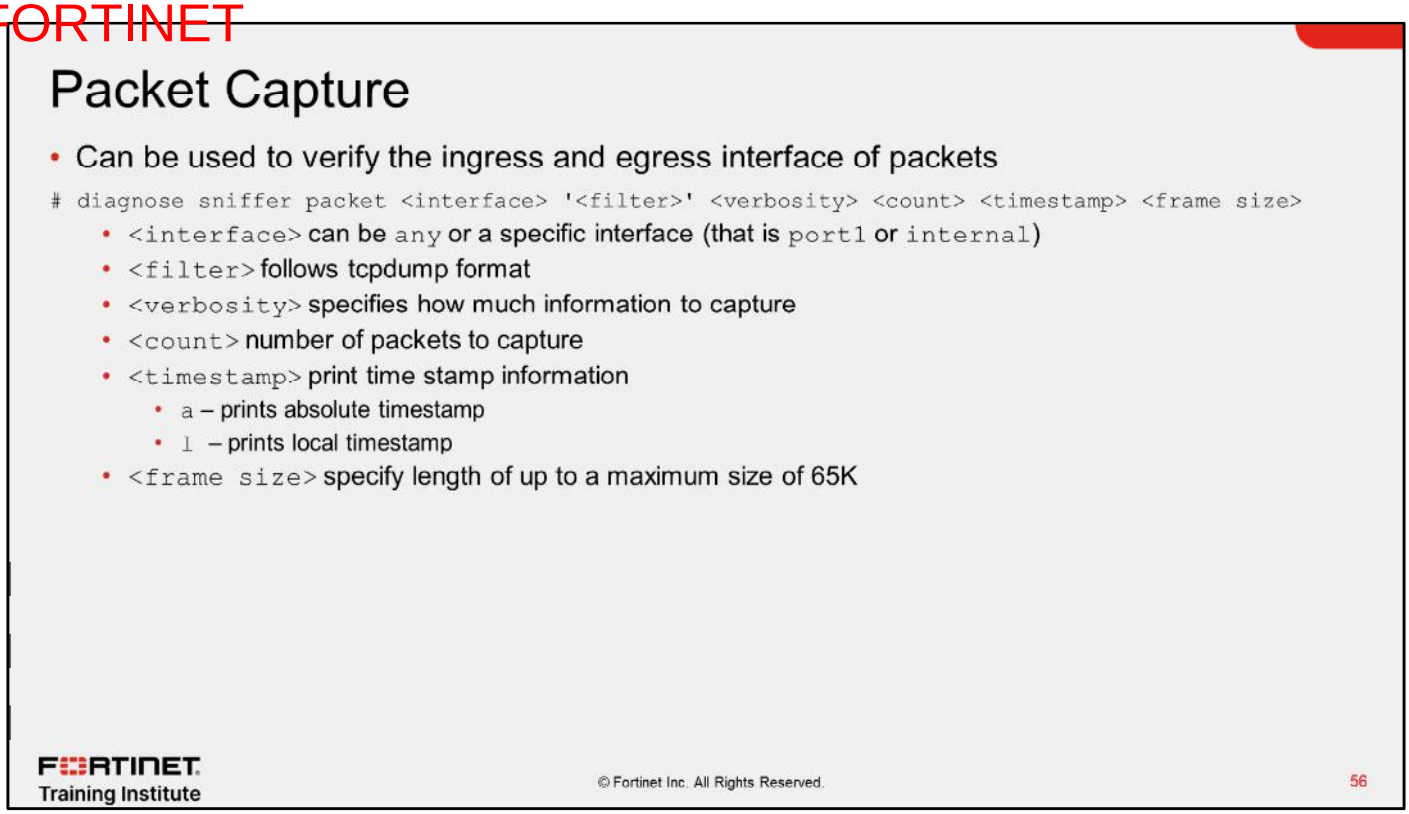


FortiOS maintains a policy route table that you can view by running the `diagnose firewall proute list` command.

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`. Alternatively, you can run the `print tablesize` command on the FortiGate CLI to get the maximum values for your device.



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 f you use the `any` interface, the sniffer will default to 1600 bytes.

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

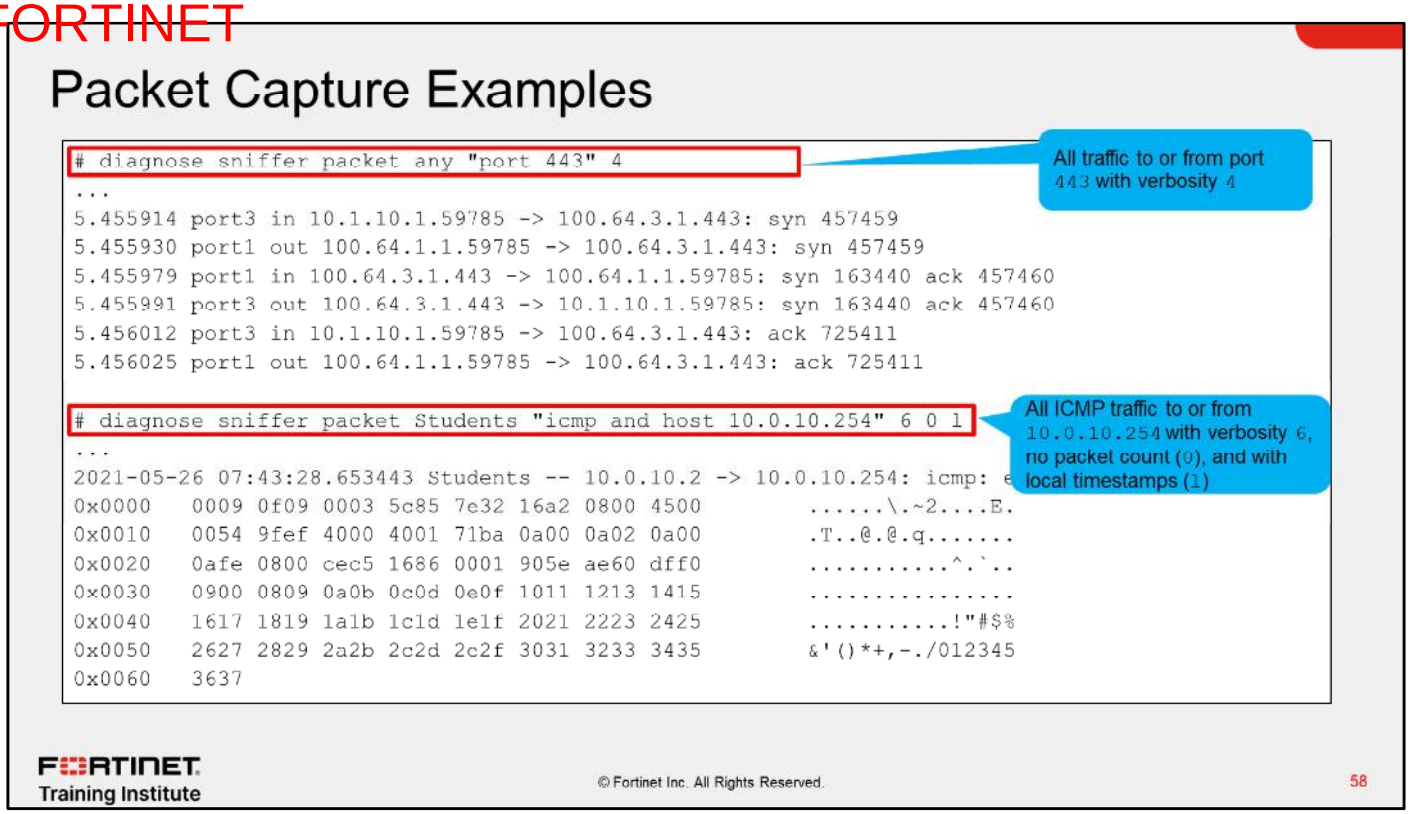
FORTINET Training Institute

57

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.

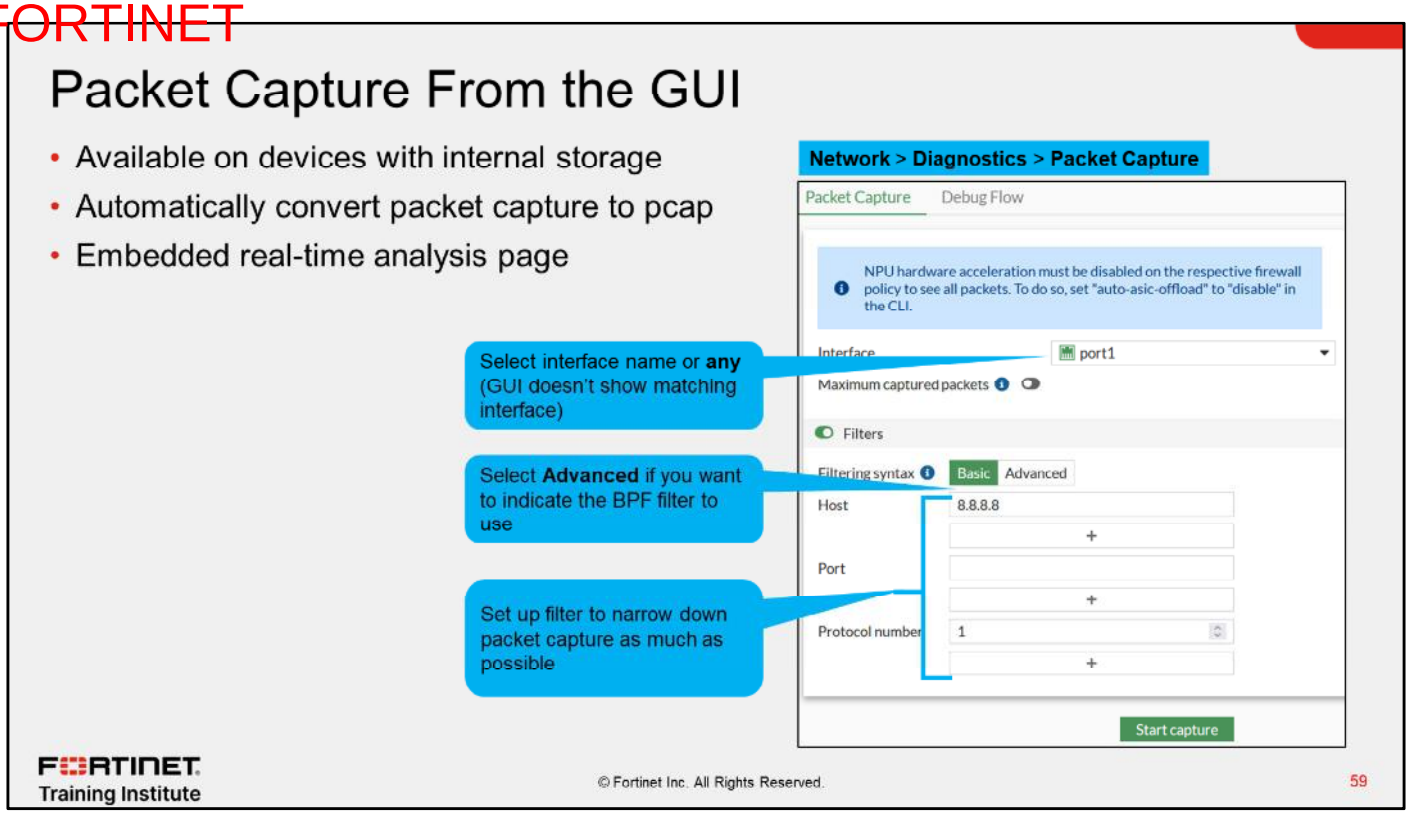
Verbosity levels `3` and `6` provide the most output. Both show the IP payloads and Ethernet headers. You can save the output and export it to a packet capture (pcap) file using a Perl script. The pcap file can then be opened with a packet analyzer, such as Wireshark, for further investigation. You can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



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`.

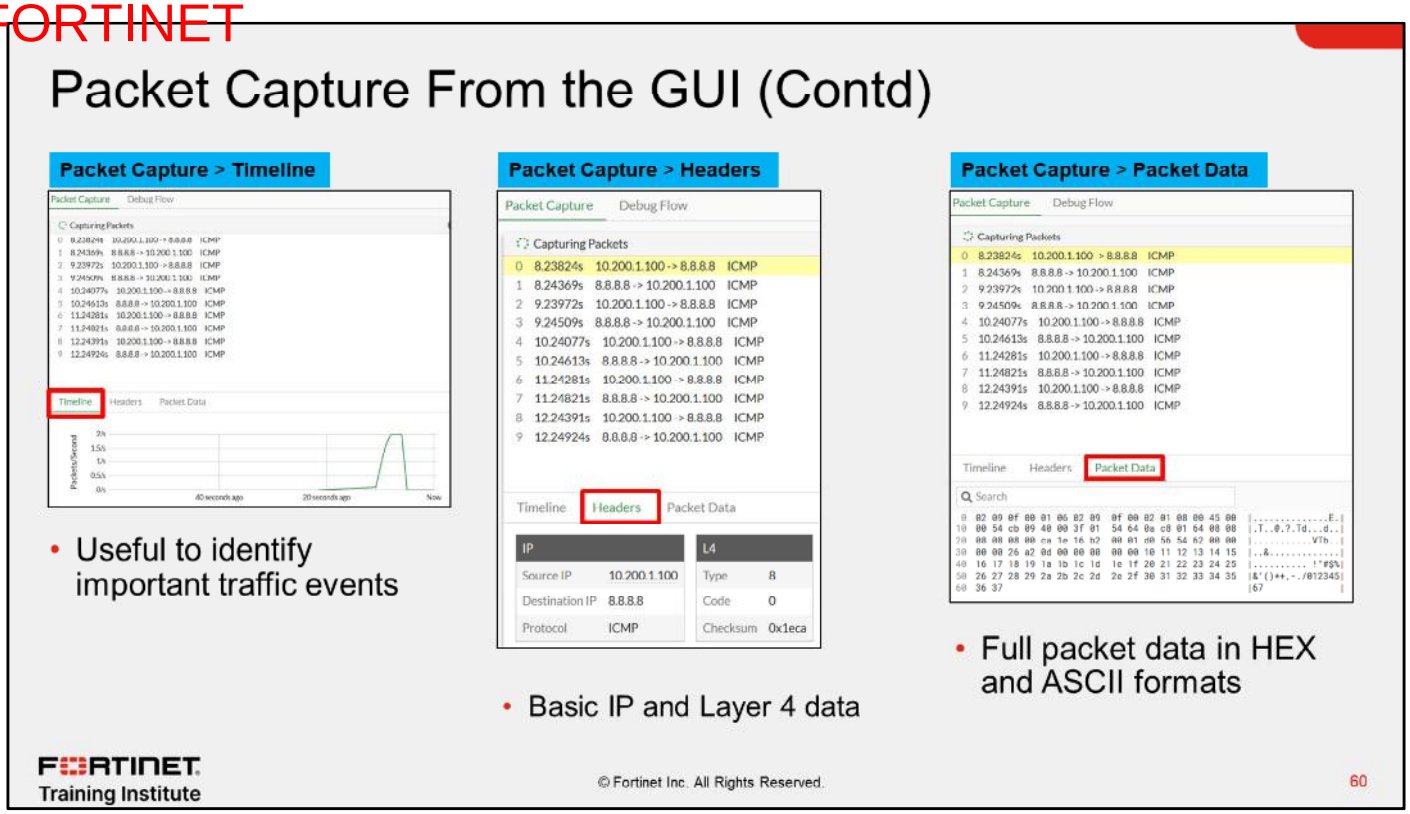
The second example captures all ICMP traffic coming from or going to `10.0.10.254`. Unlike the first example, which captures packets on any interface, this example limits the capture to packets that enter or leave the `Student` interface. Although not shown on this slide, the `Students` interface is 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`).



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 to 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.



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 quicky 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.

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?

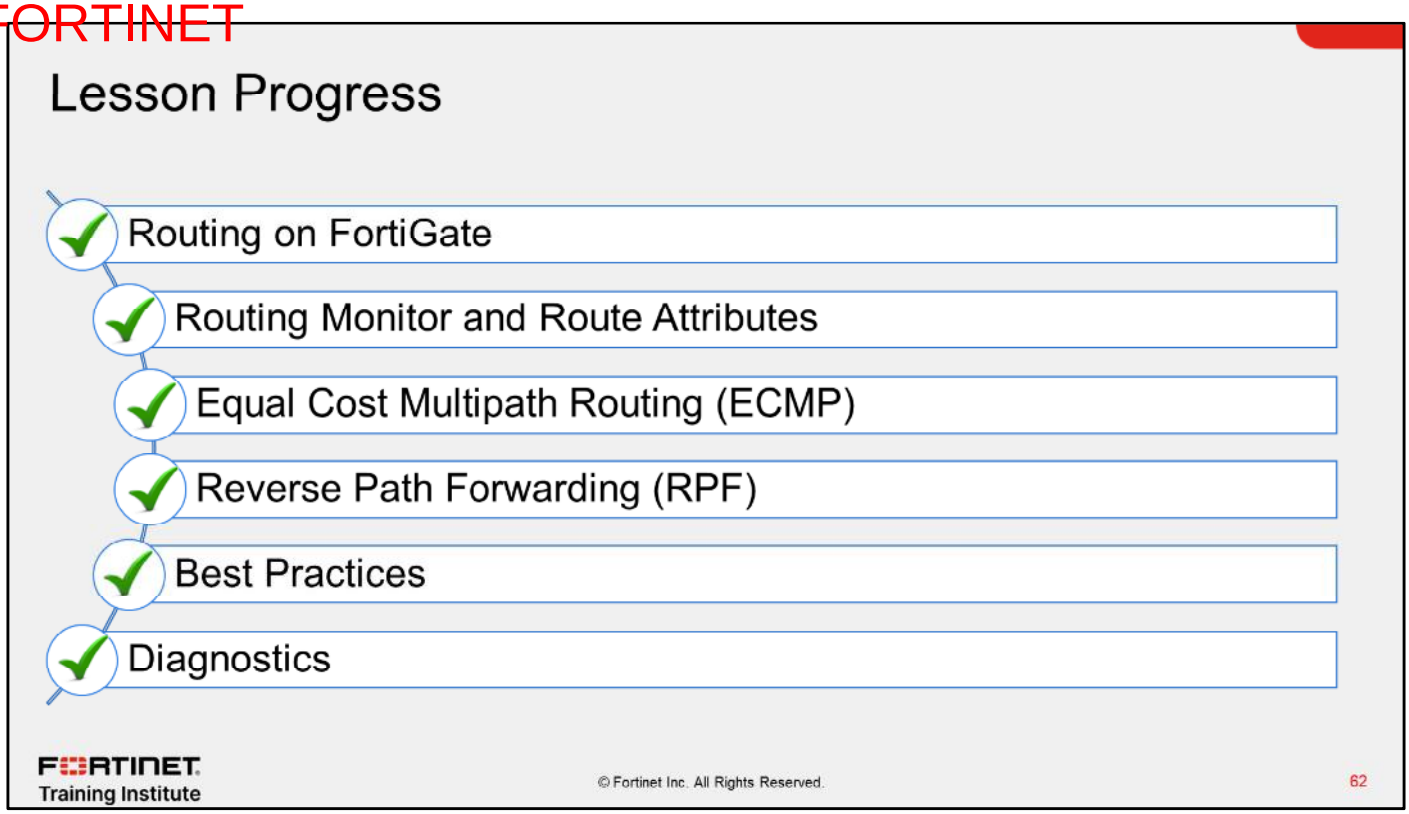
A. `get router info routing-table all`
✓B. `get router info routing-table database`

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

A. 3
✓B. 4

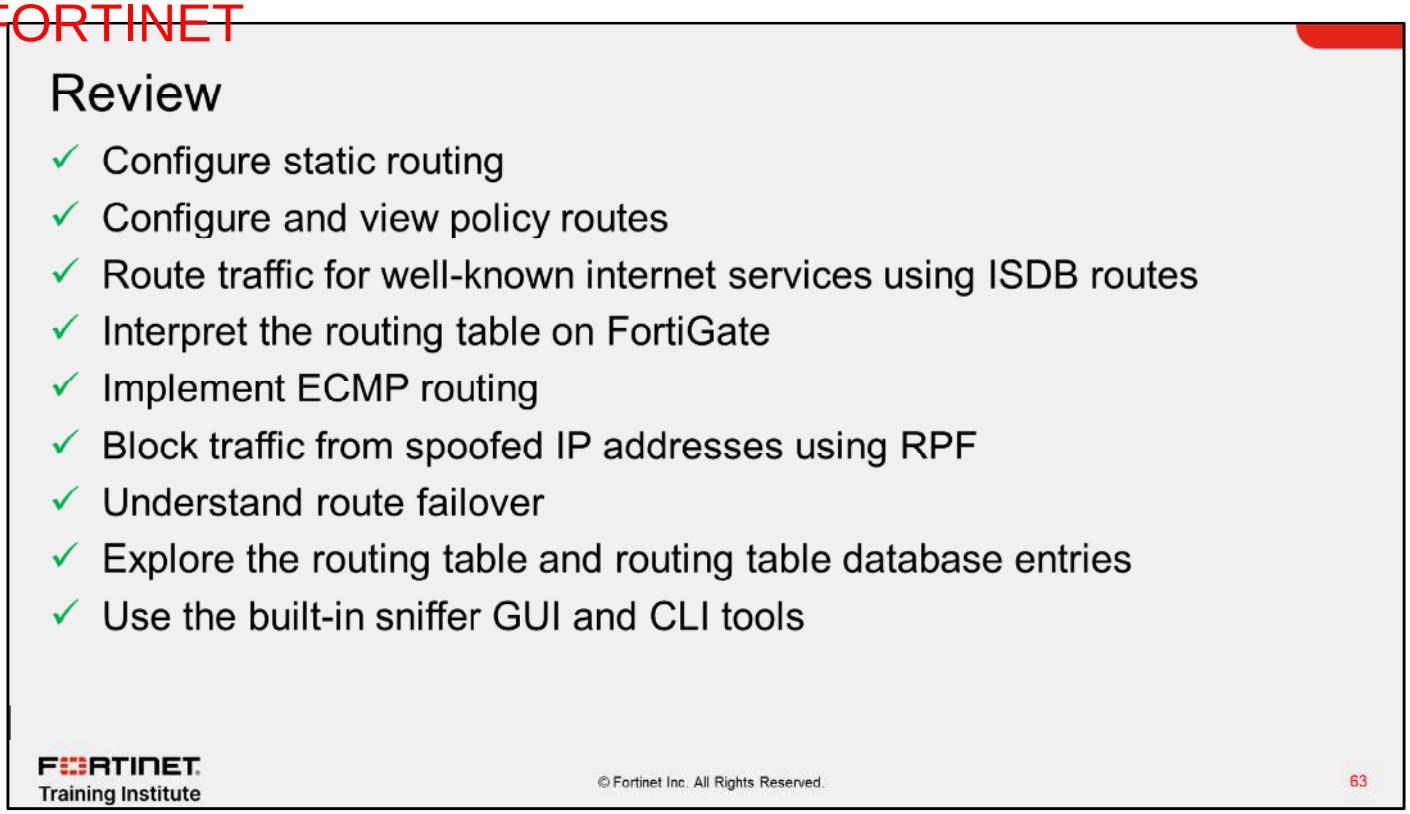
FORTINET Training Institute

61



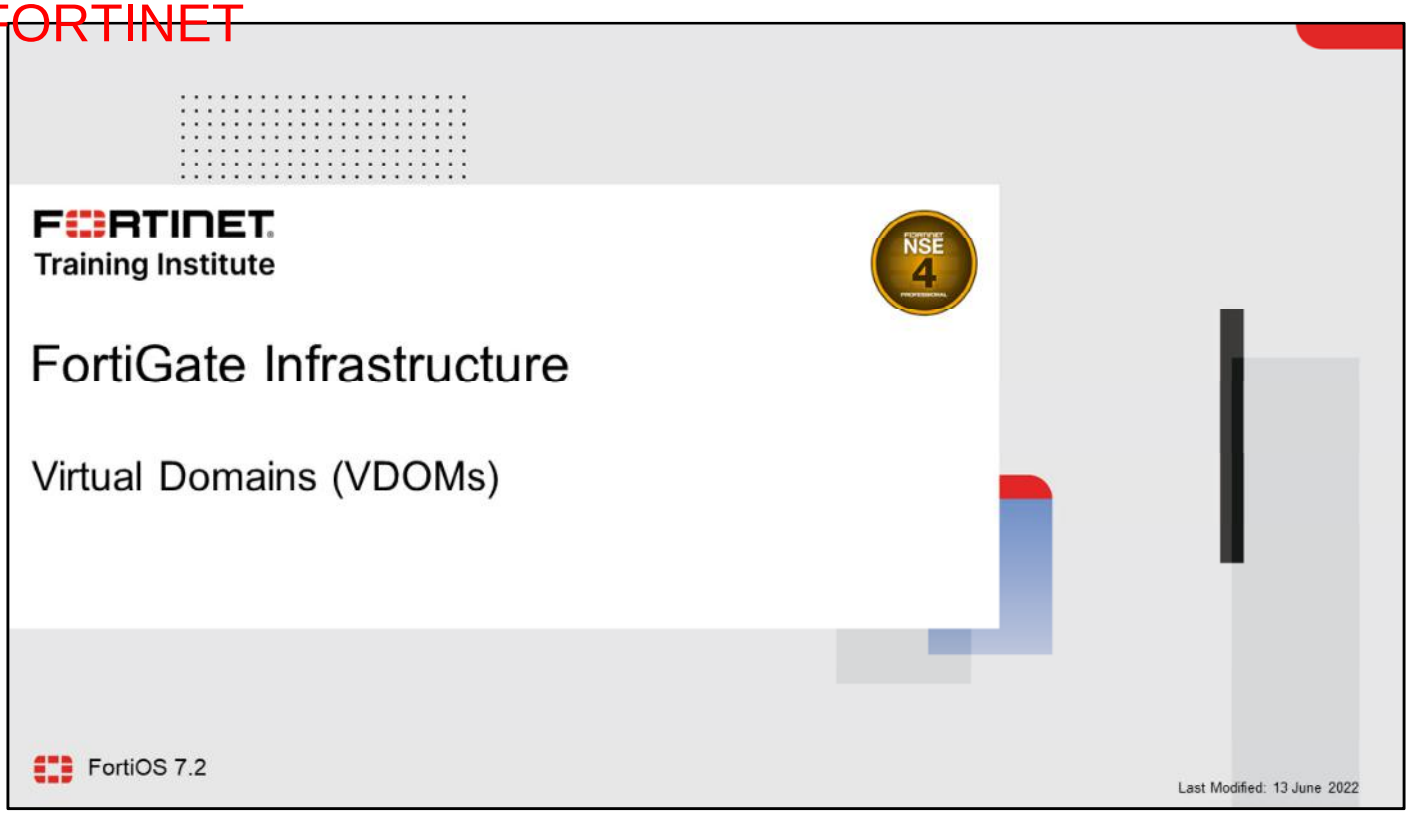
Congratulations! You have completed this lesson.

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

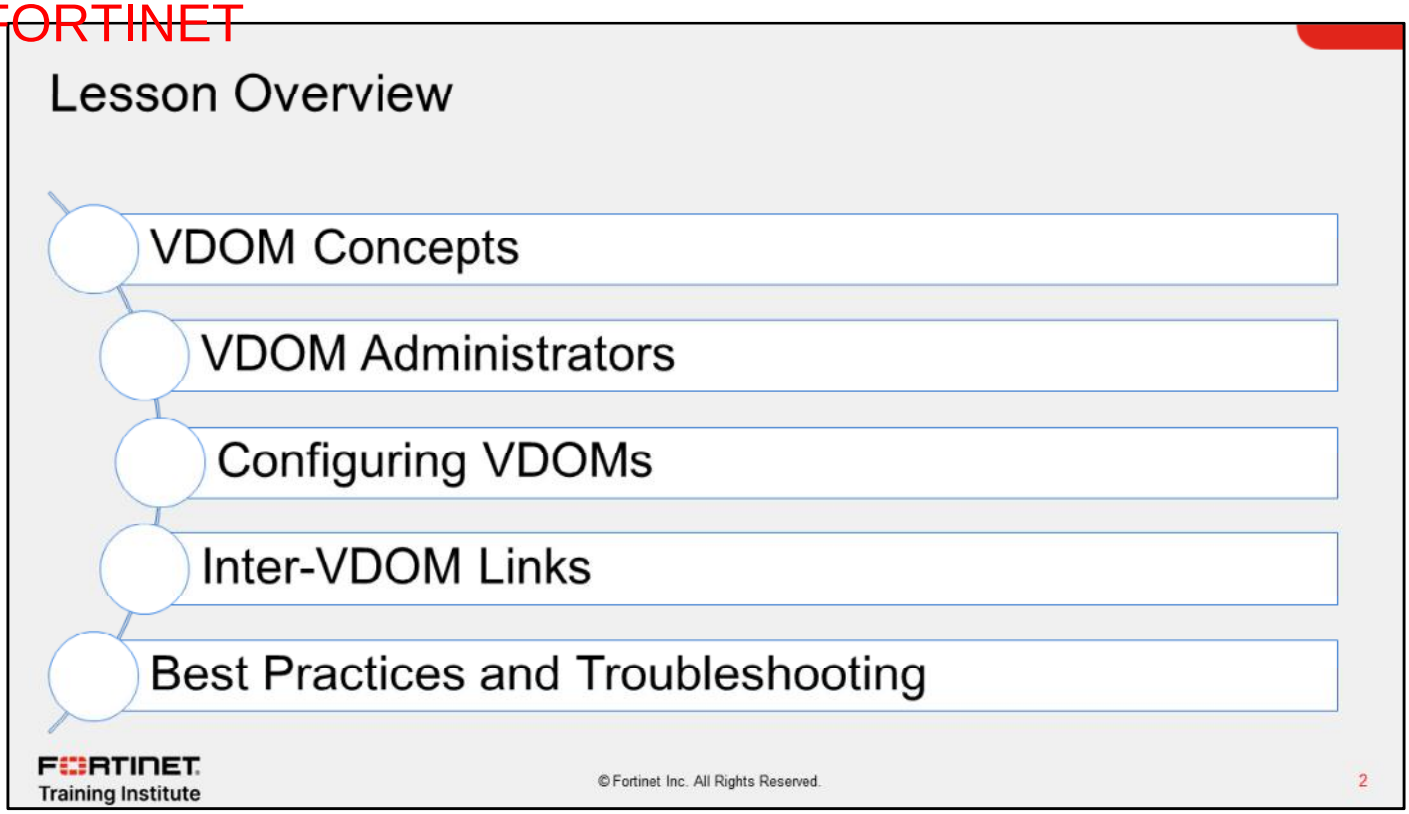


This slide shows the objectives that you covered in this lesson.

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



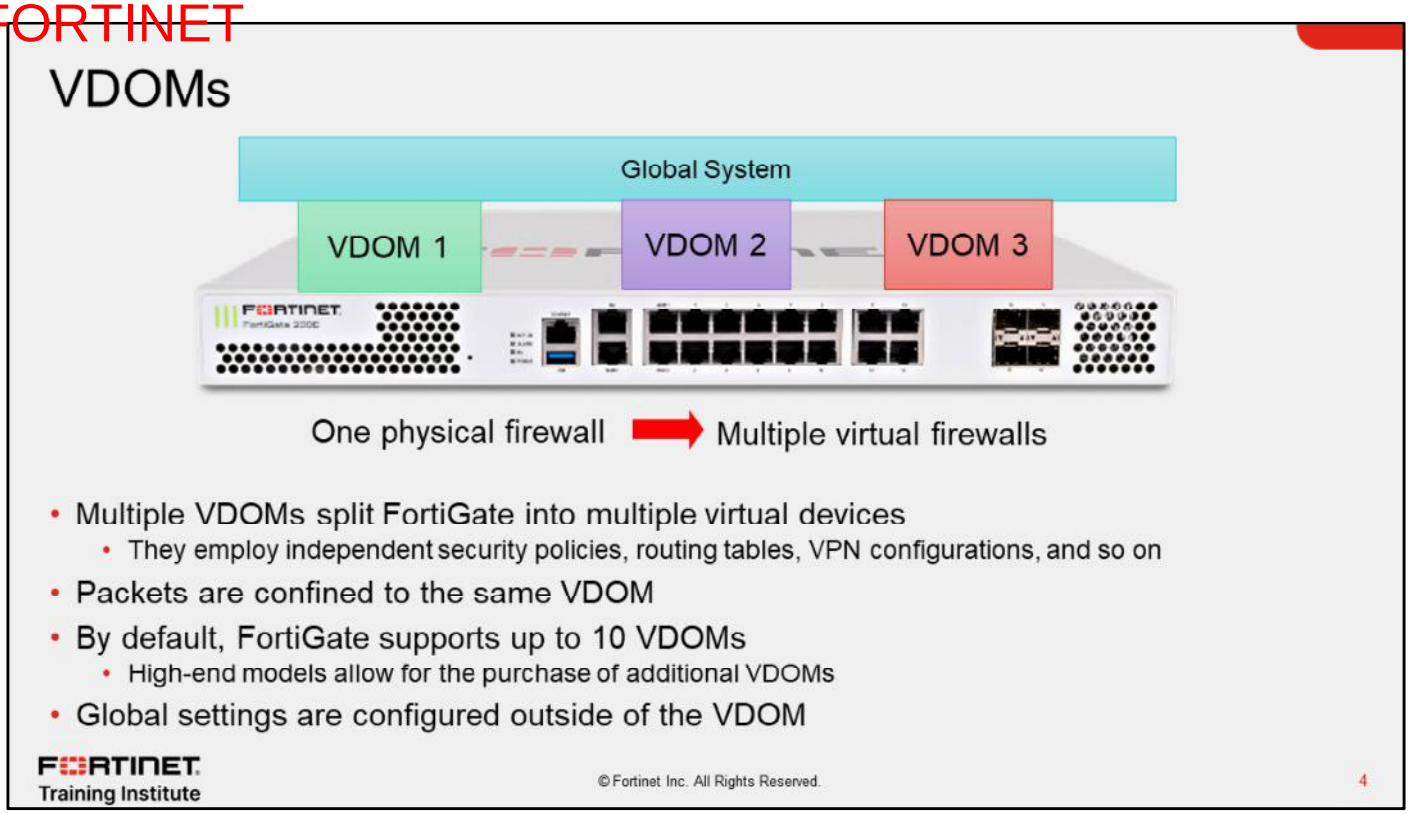
In this lesson, you will learn how to configure VDOMs, and examine examples of common use.



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

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.



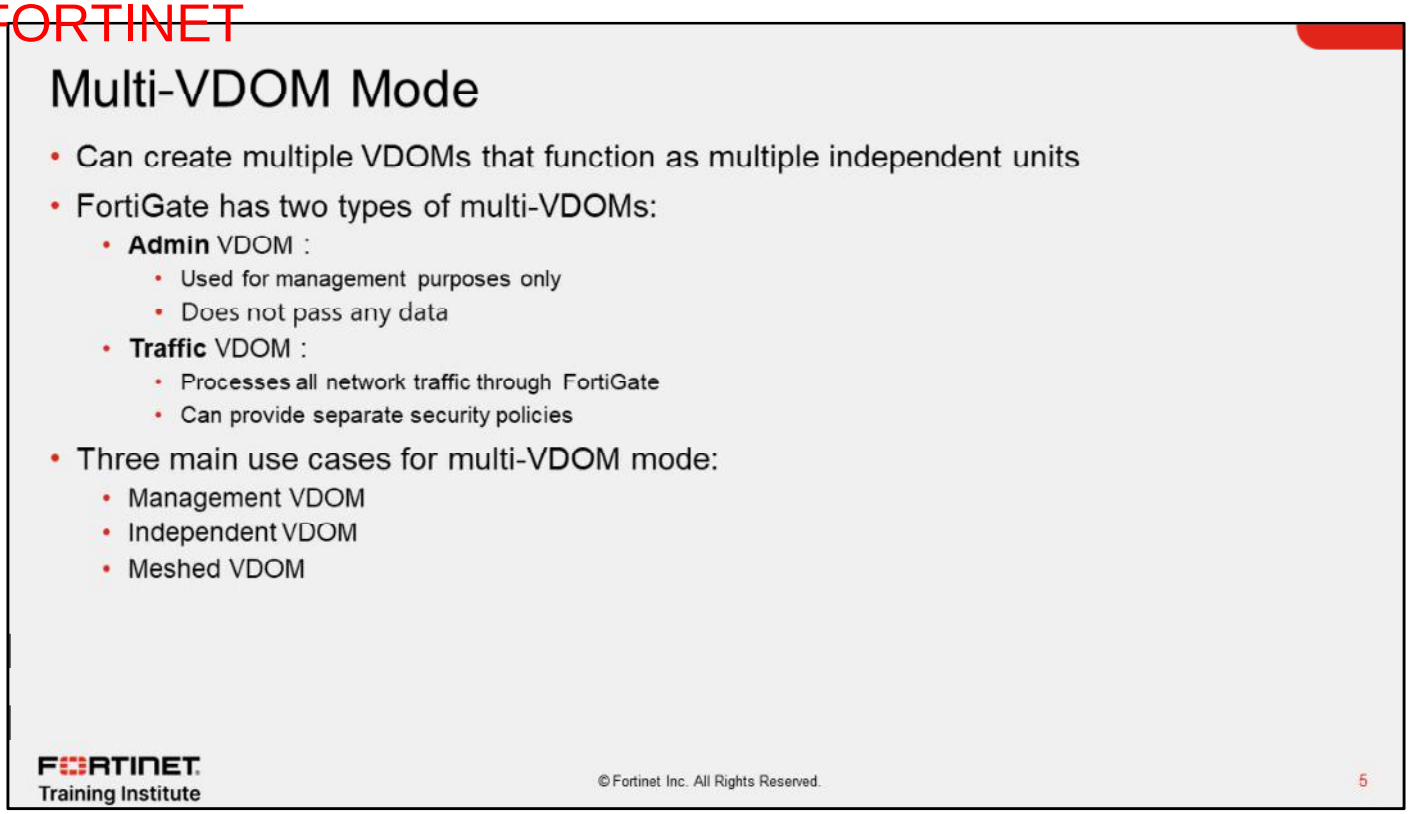
What if a campus wants to keep its departments separate? A datacenter wants to implement various security implementations in a cost-effective manner that maintains all customer traffic separate and secure while also reducing space and making configuration easier? What if you want to segment your network,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

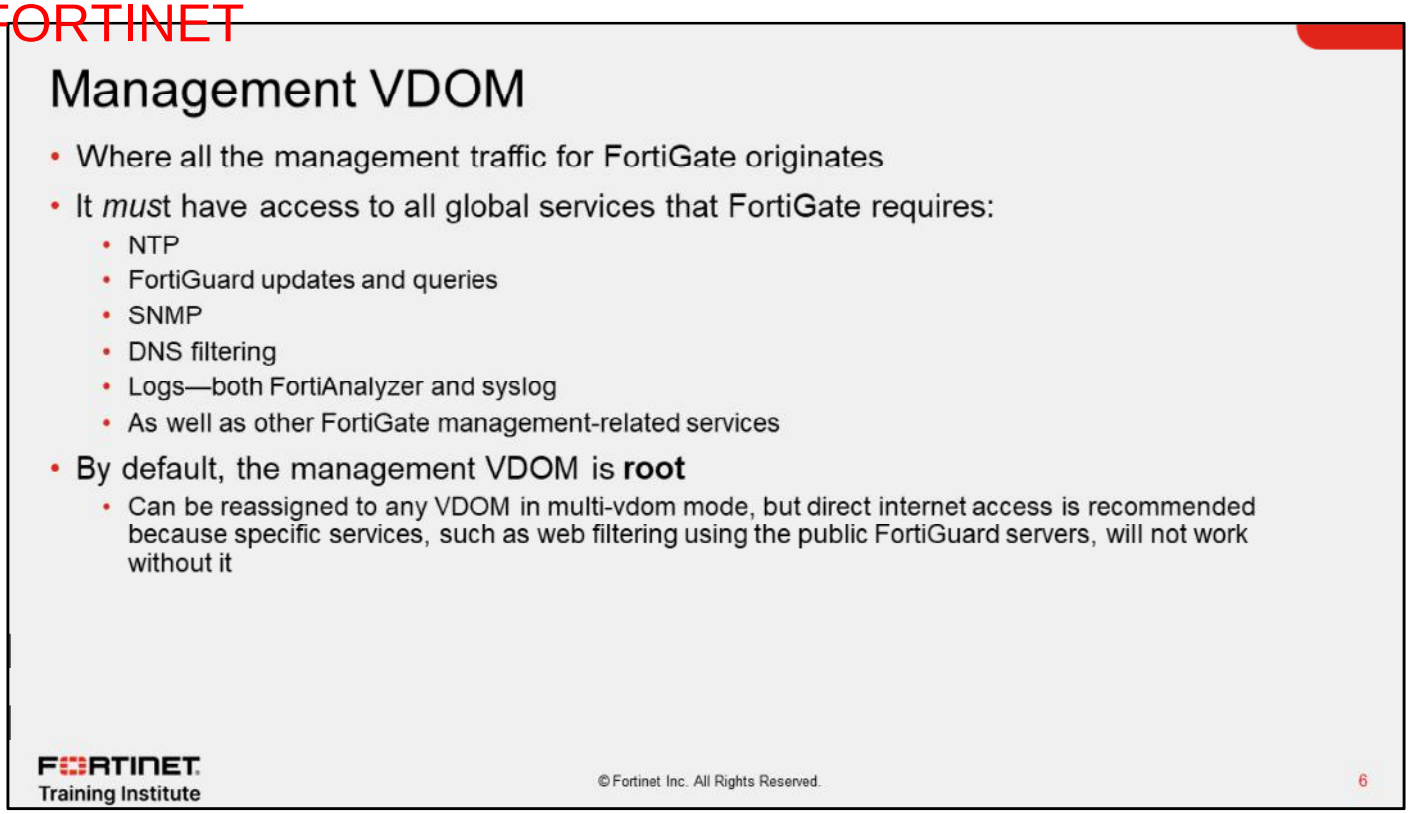


Use multi-VDOM mode when you want to create multiple logical firewalls from a single FortiGate. Each VDOM acts as an independent FortiGate.

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

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



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

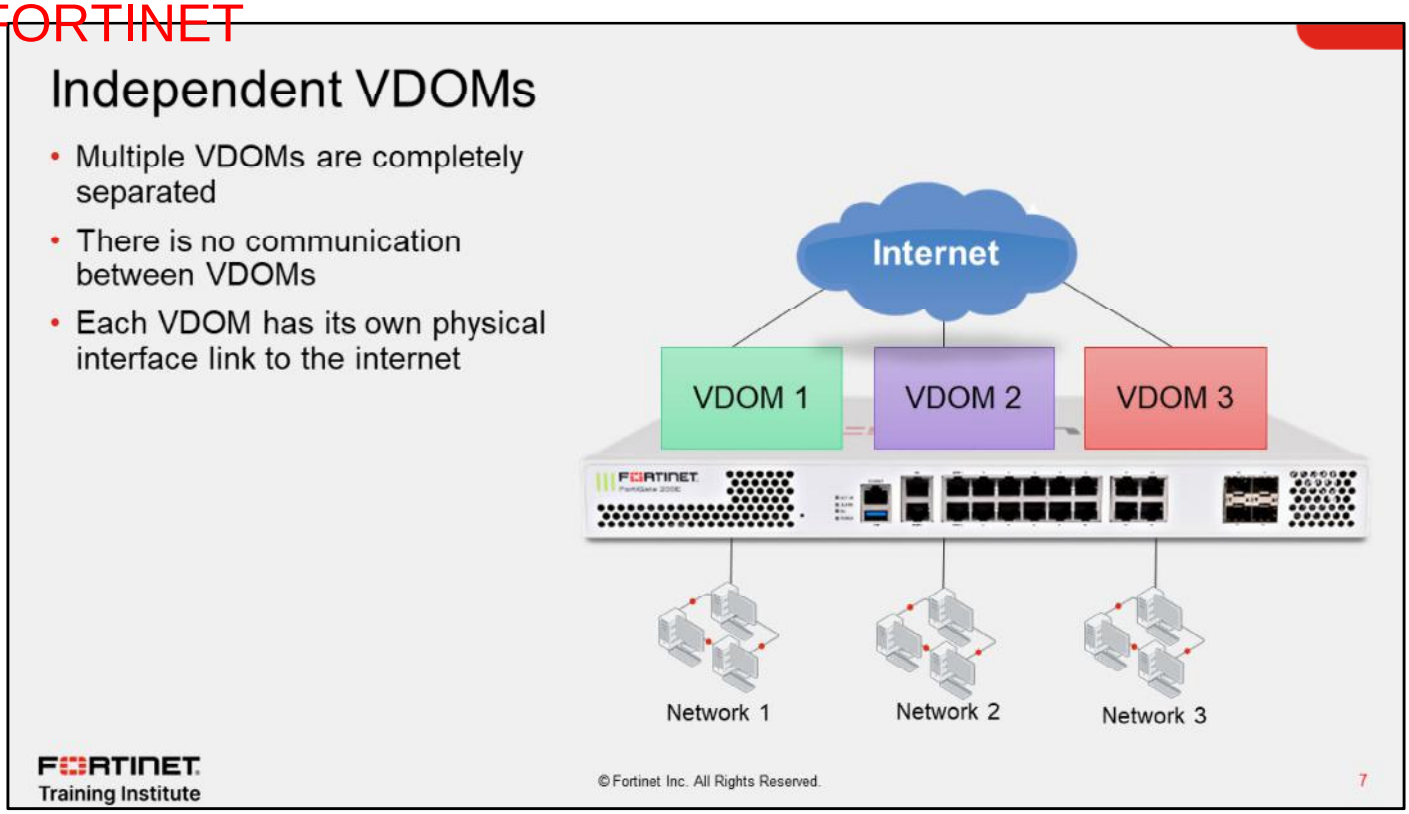
What about traffic originating *from* FortiGate? Some system daemons, such as NTP and FortiGuard updates, generate traffic coming from FortiGate.

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.

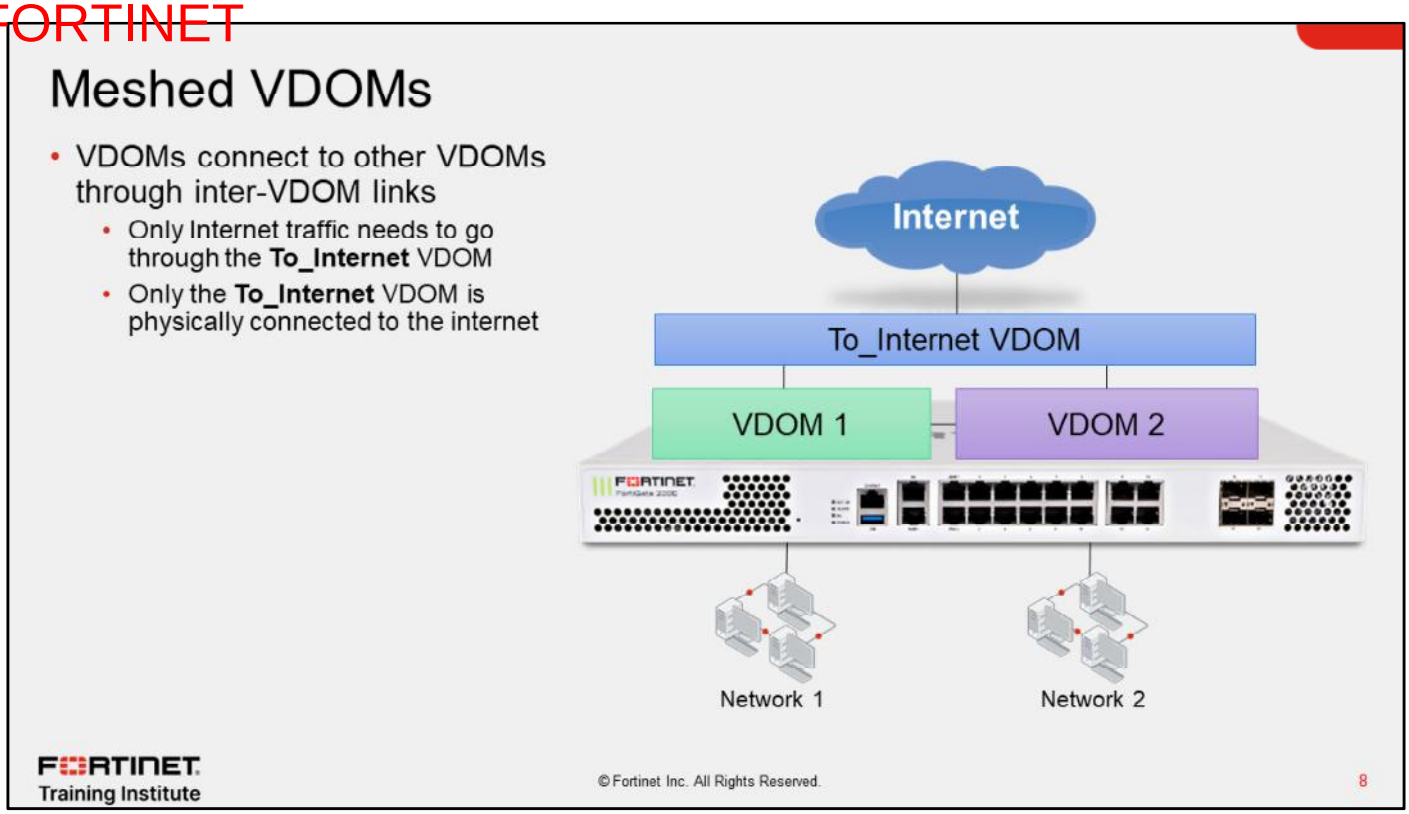
It is important to note that the management VDOM designation is solely for traffic originated by FortiGate, such as FortiGuard updates, and has no effect on traffic passing through FortiGate. As such, the management function can be performed by any designated VDOM.

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



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.



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.

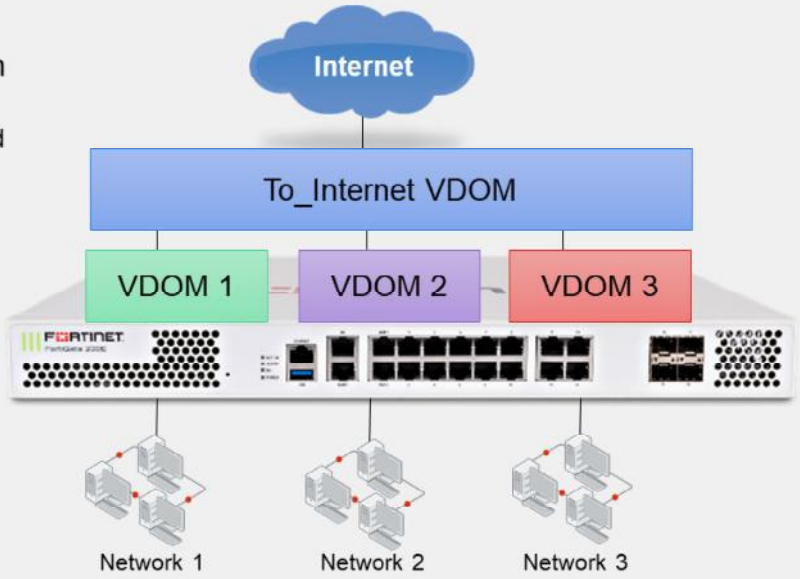
Similar to the previous example topology, inspection can be done by either the **To_Internet** or originating VDOM, depending on your requirements.

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.

Routing Through a Single VDOM

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



FORTINET Training Institute

9

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

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

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

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

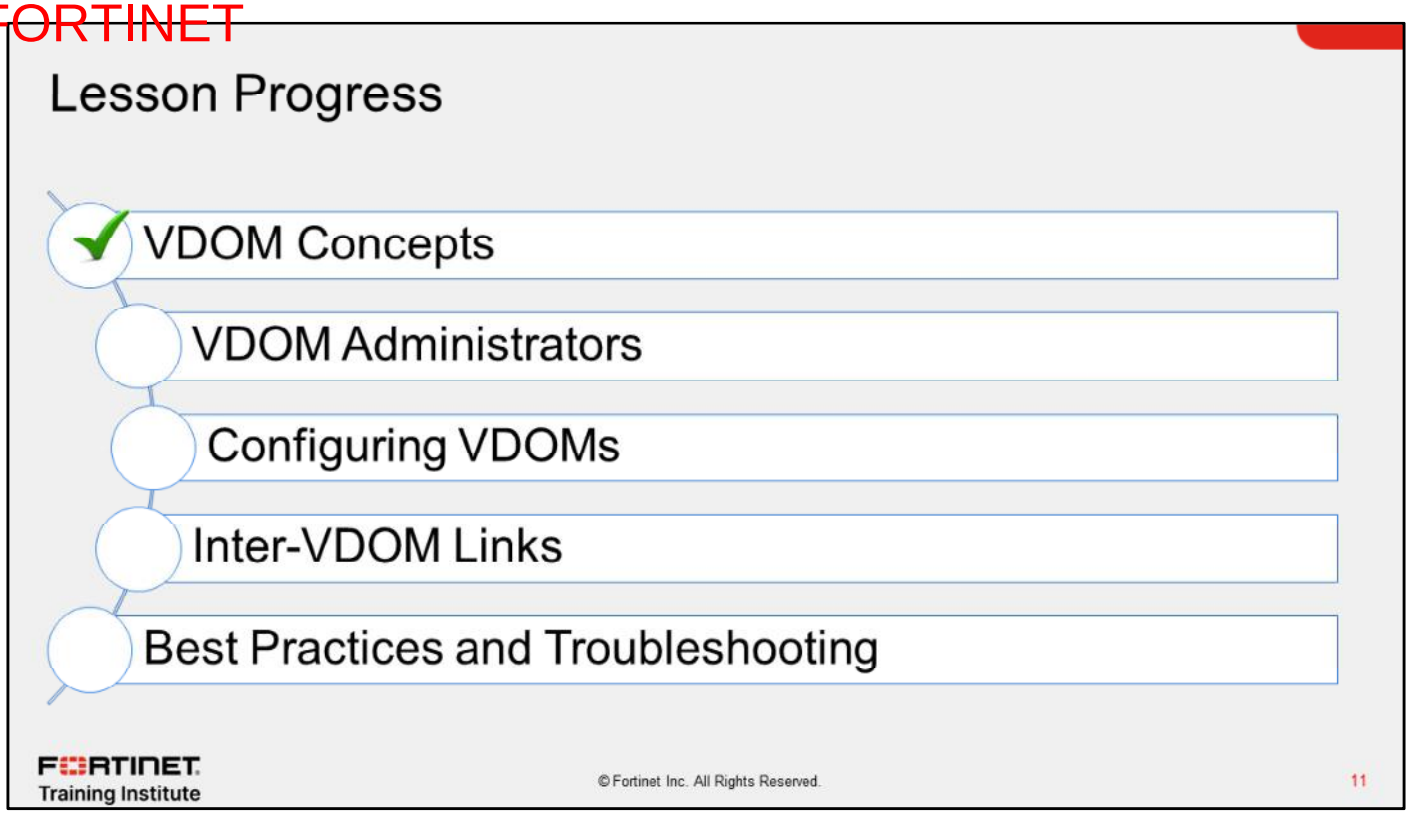
Knowledge Check

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.

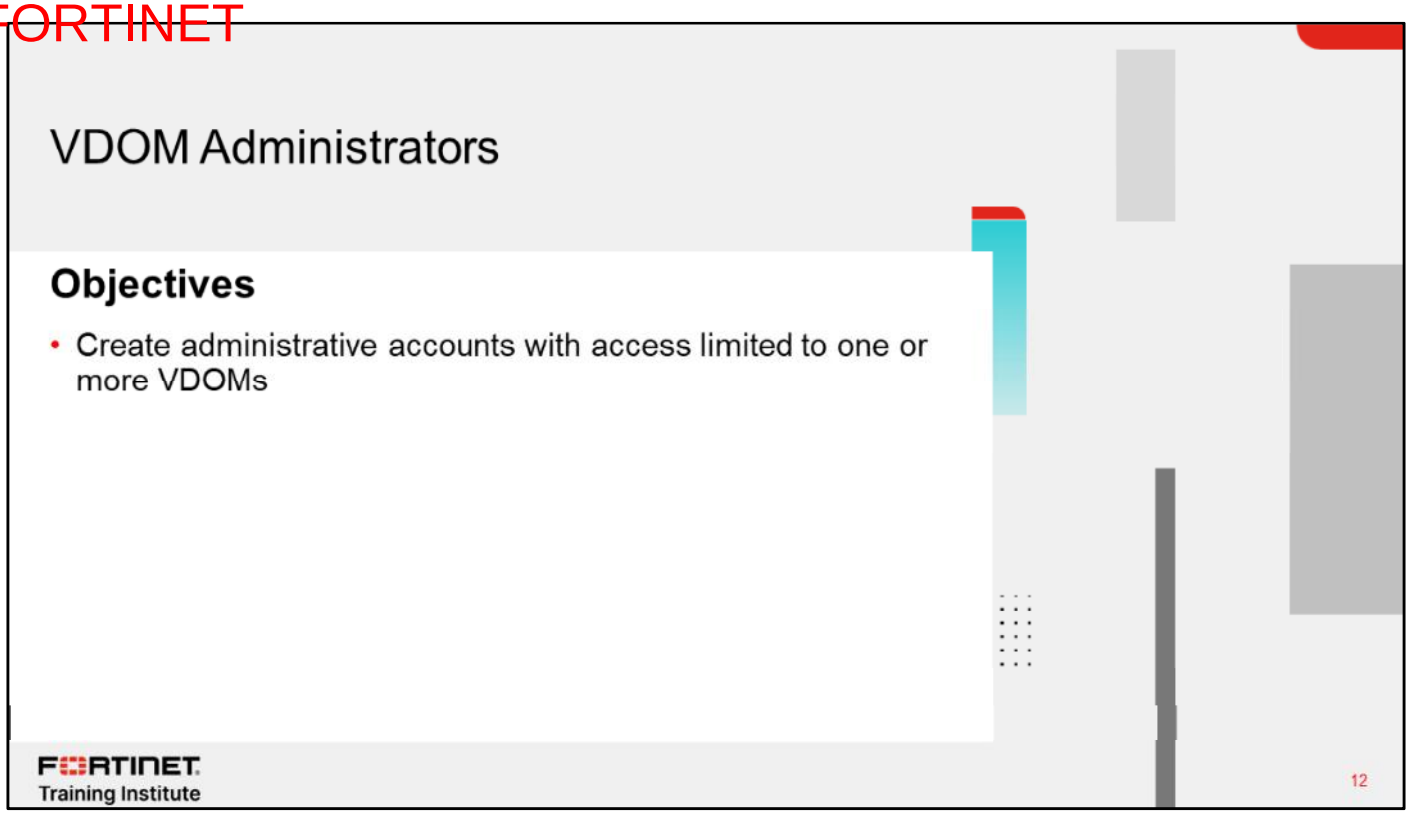
FORTINET Training Institute

10



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

Now, you'll learn about VDOM administrators.

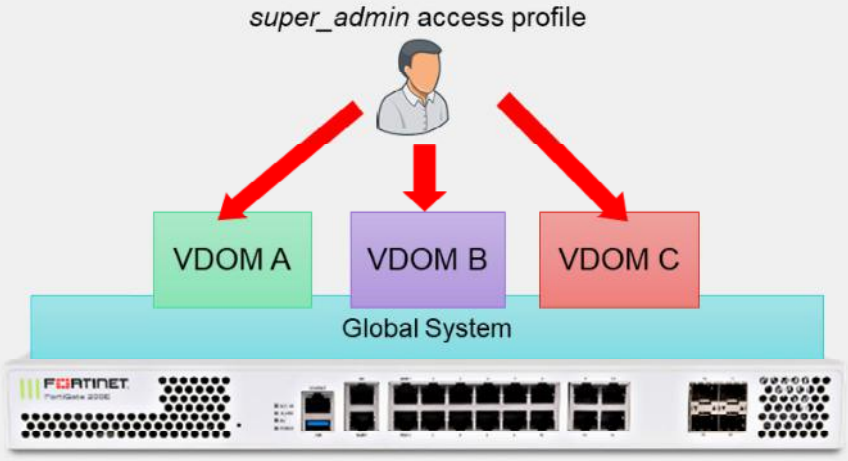


After completing this section, you should be able to achieve the objective shown on this slide.

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.

VDOM Administration

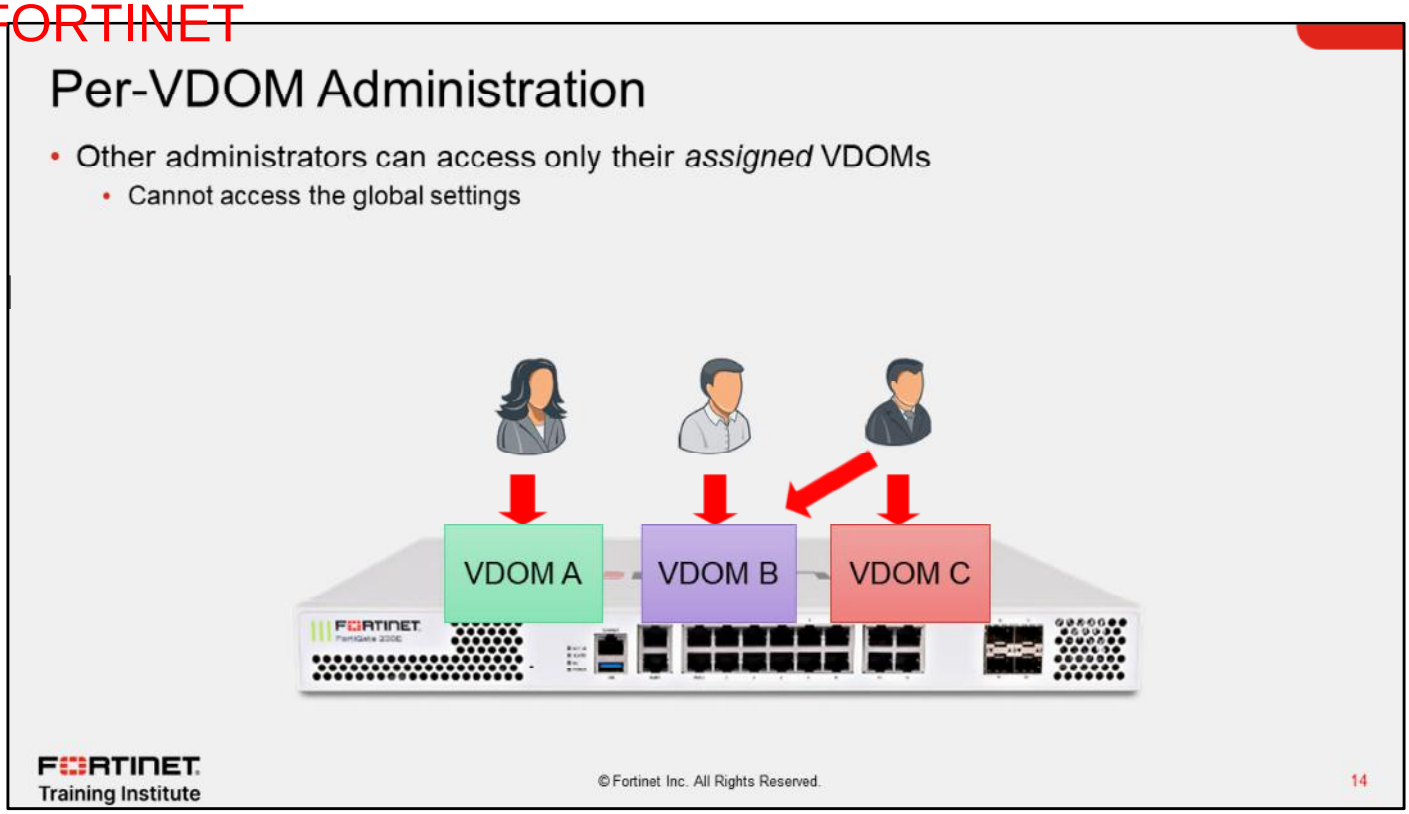
- Only the account named **admin** or accounts with the **super_admin** profile can configure and back up all VDOMs



FORTINET Training Institute

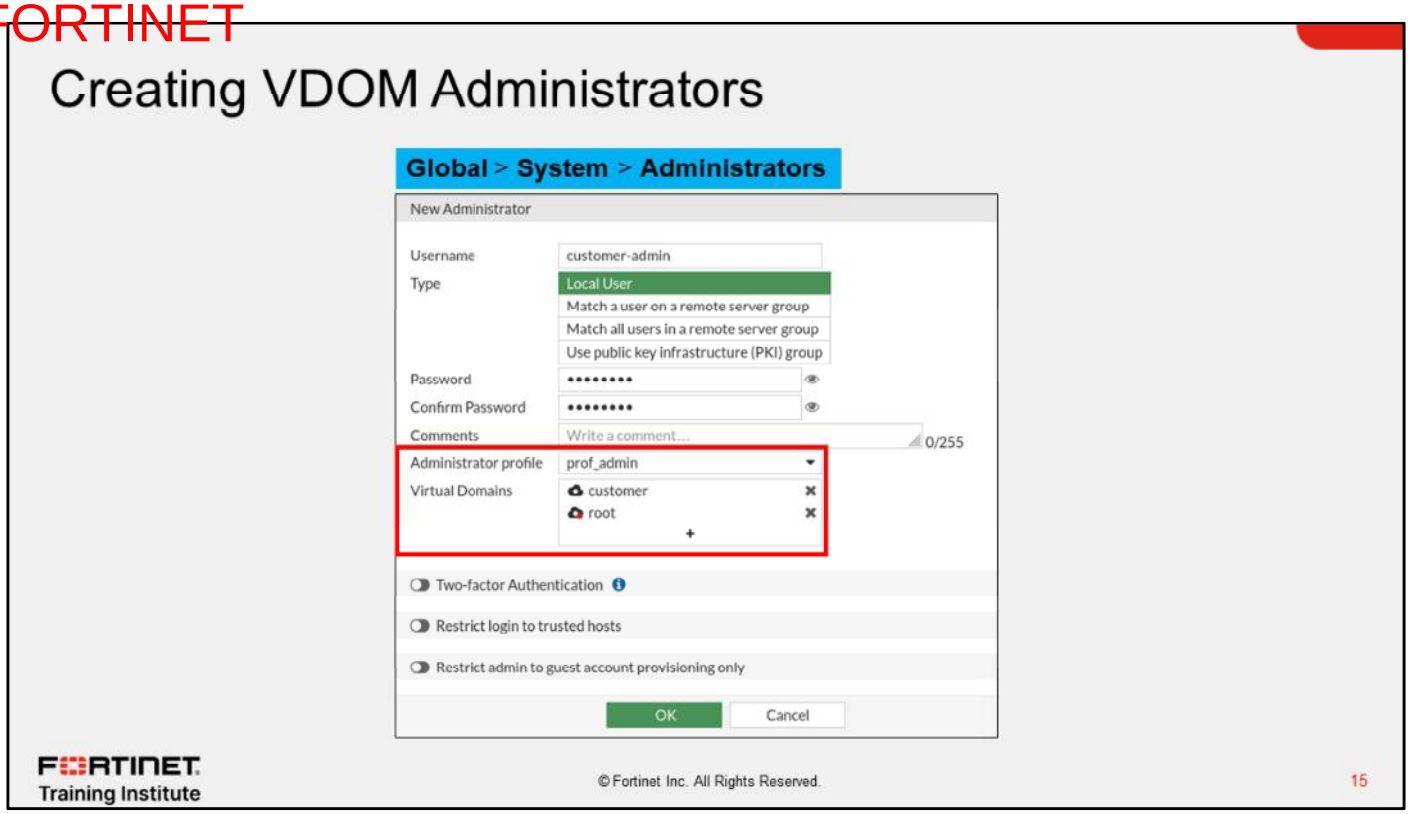
13

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



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.



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

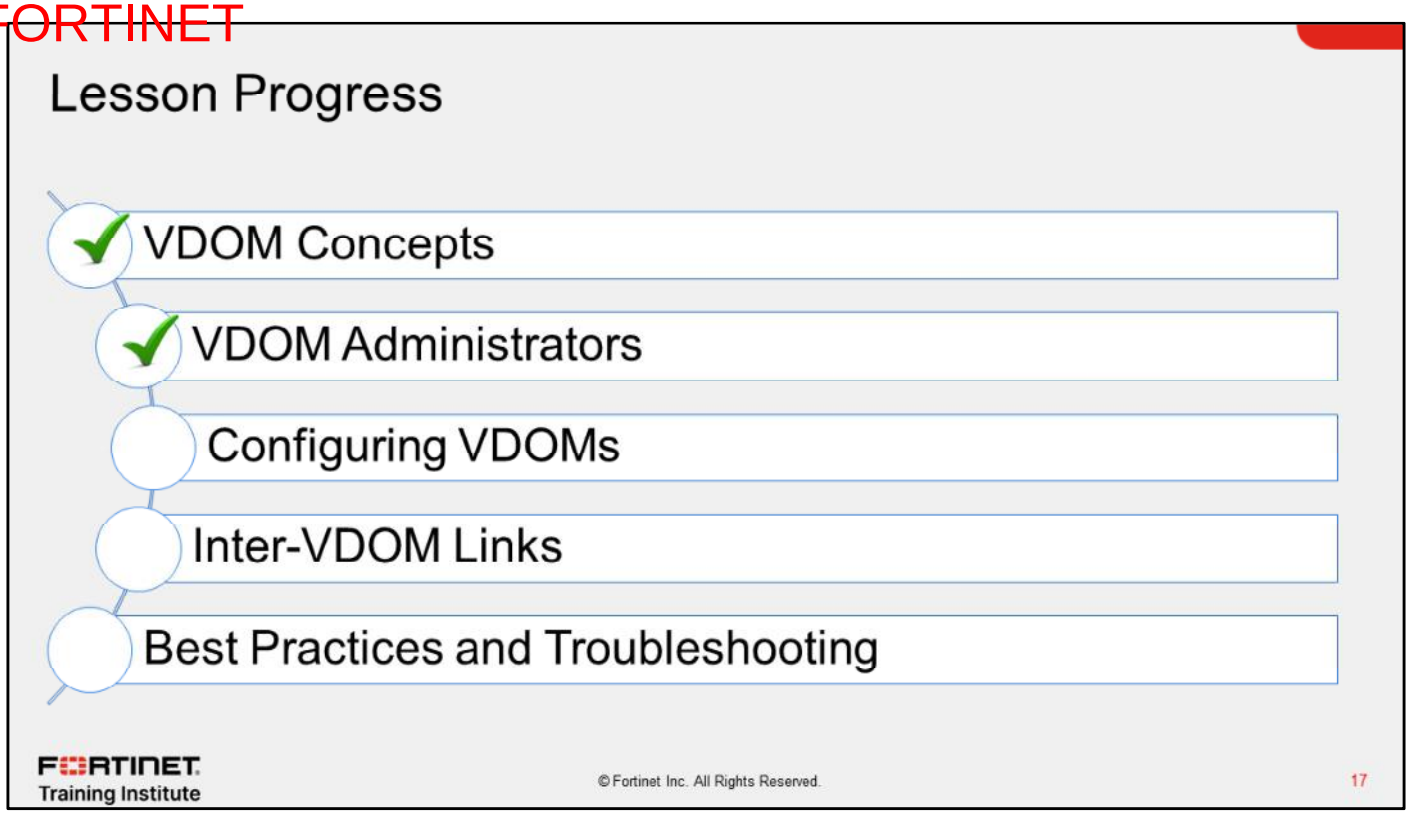
Knowledge Check

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.

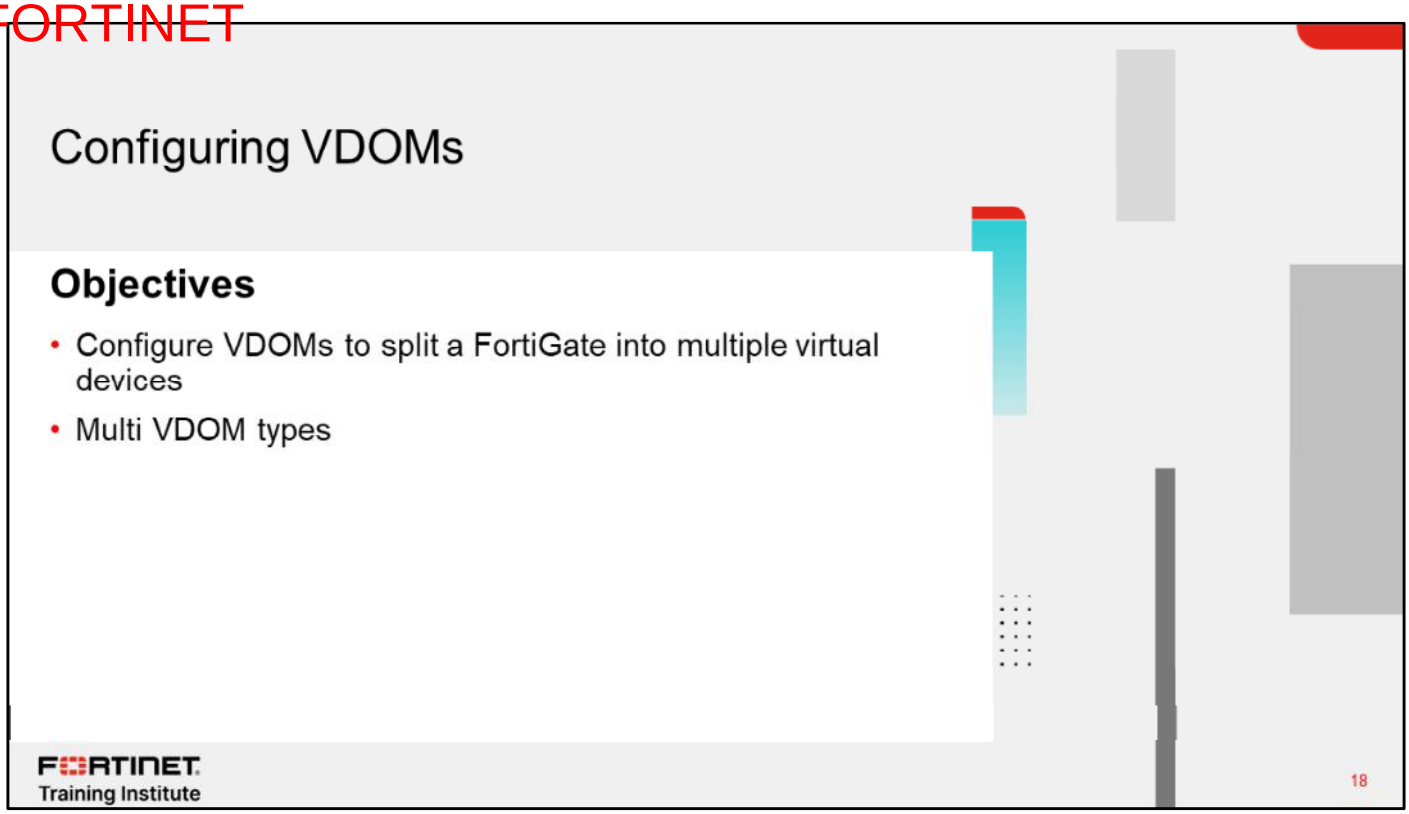
FORTINET Training Institute

16



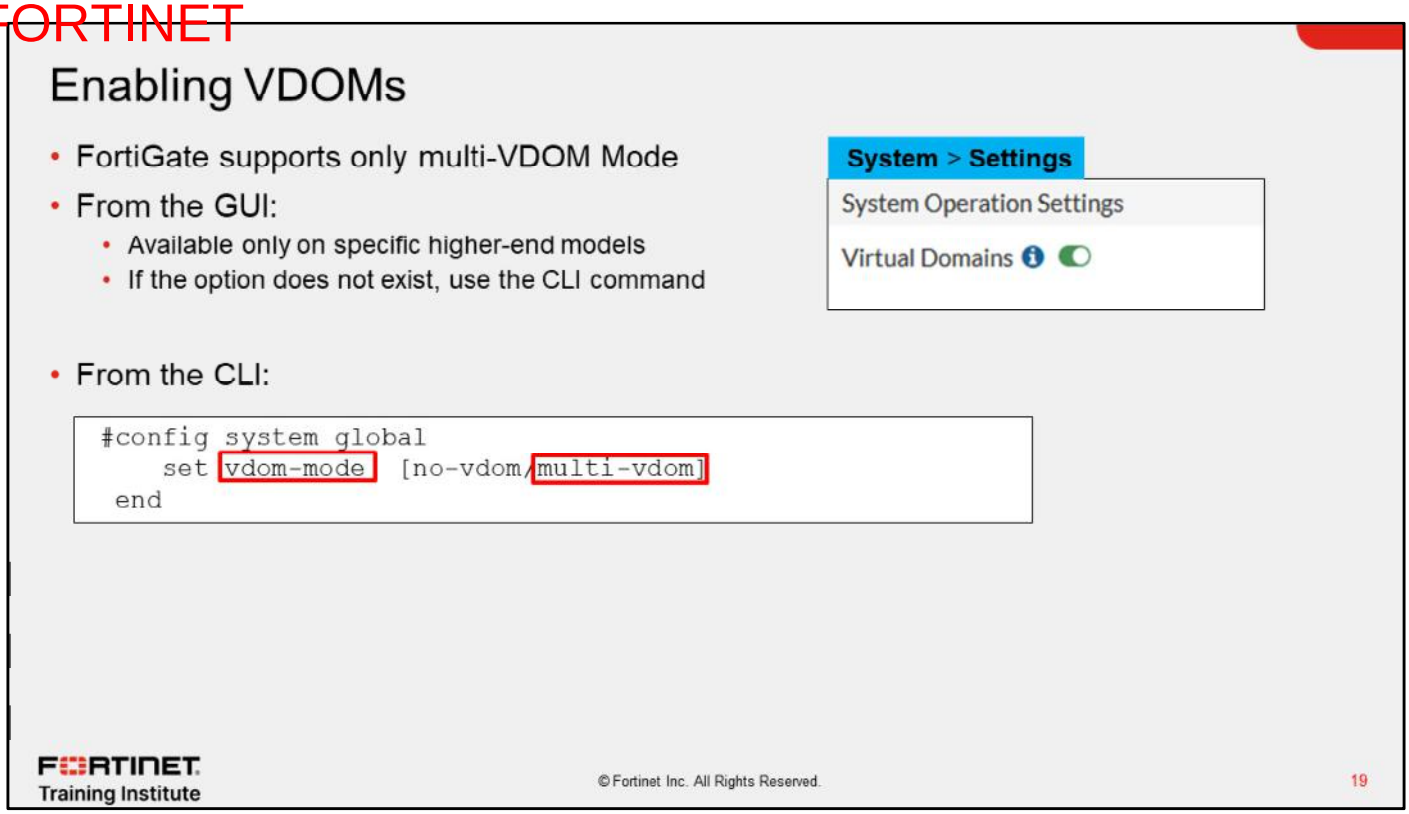
Good job! You now understand VDOM administrators.

Now, you'll learn how to configure VDOMs.



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

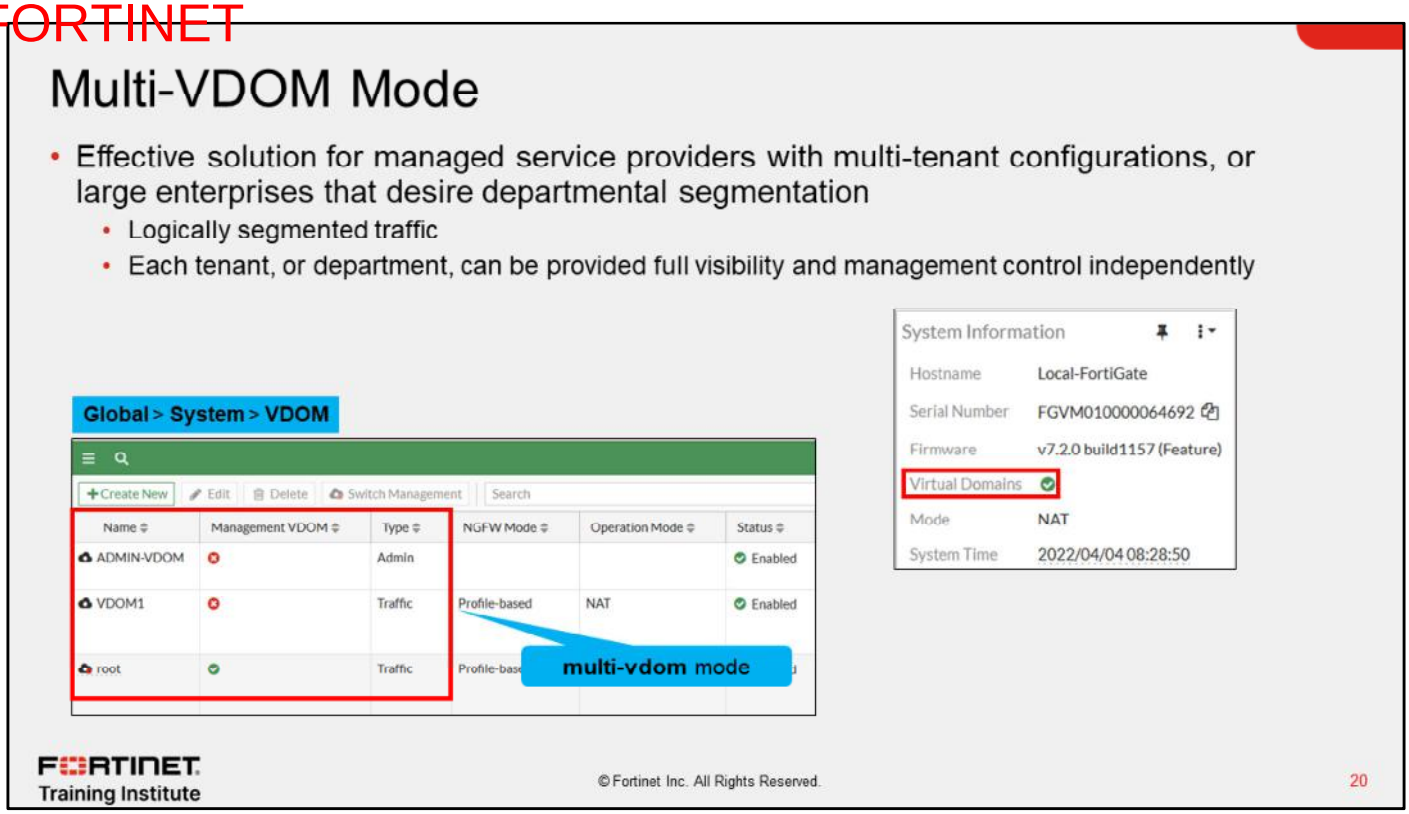
By demonstrating competence in configuring VDOMs, you will be able to effectively implement VDOMs on your FortiGate.



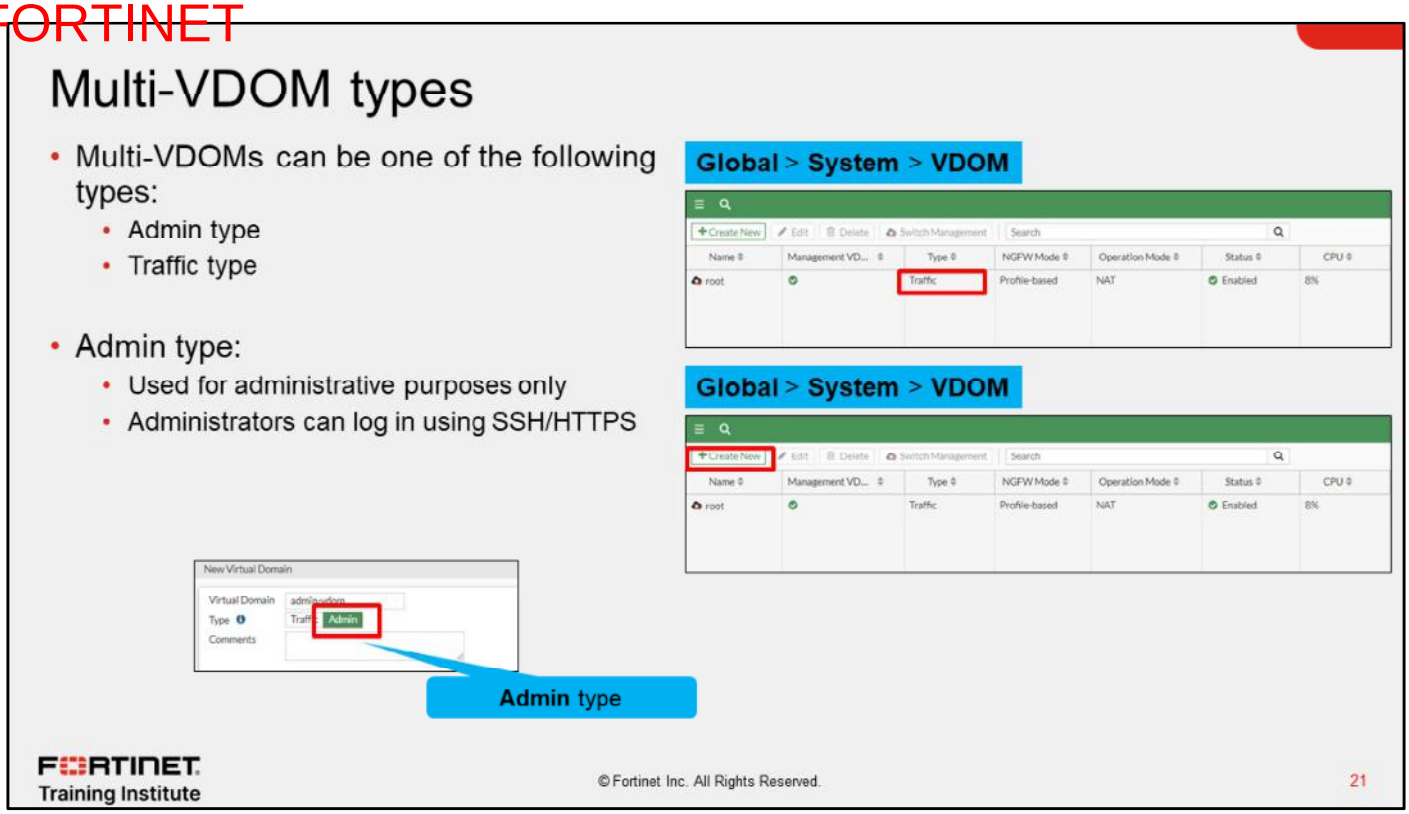
On the GUI, you can enable VDOMs under **System** > **Settings**. The GUI option is available only on higher-end FortiGate Models. Most of the FortiGate models, you can enable VDOMs on the CLI only.

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.



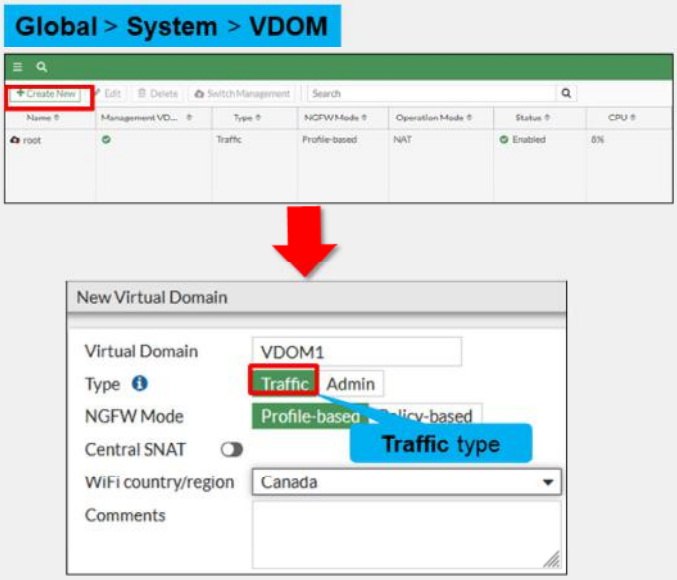
In *multi-vdom* mode, you can create multiple VDOMs that function as multiple independent units.
By default, the root is the management VDOM and can be used to do both management tasks and allow other traffic. You can select any VDOM to act as the management VDOM.



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.

Multi -VDOM types (Contd)

- Traffic type:
  - Can pass traffic like regular VDOMs



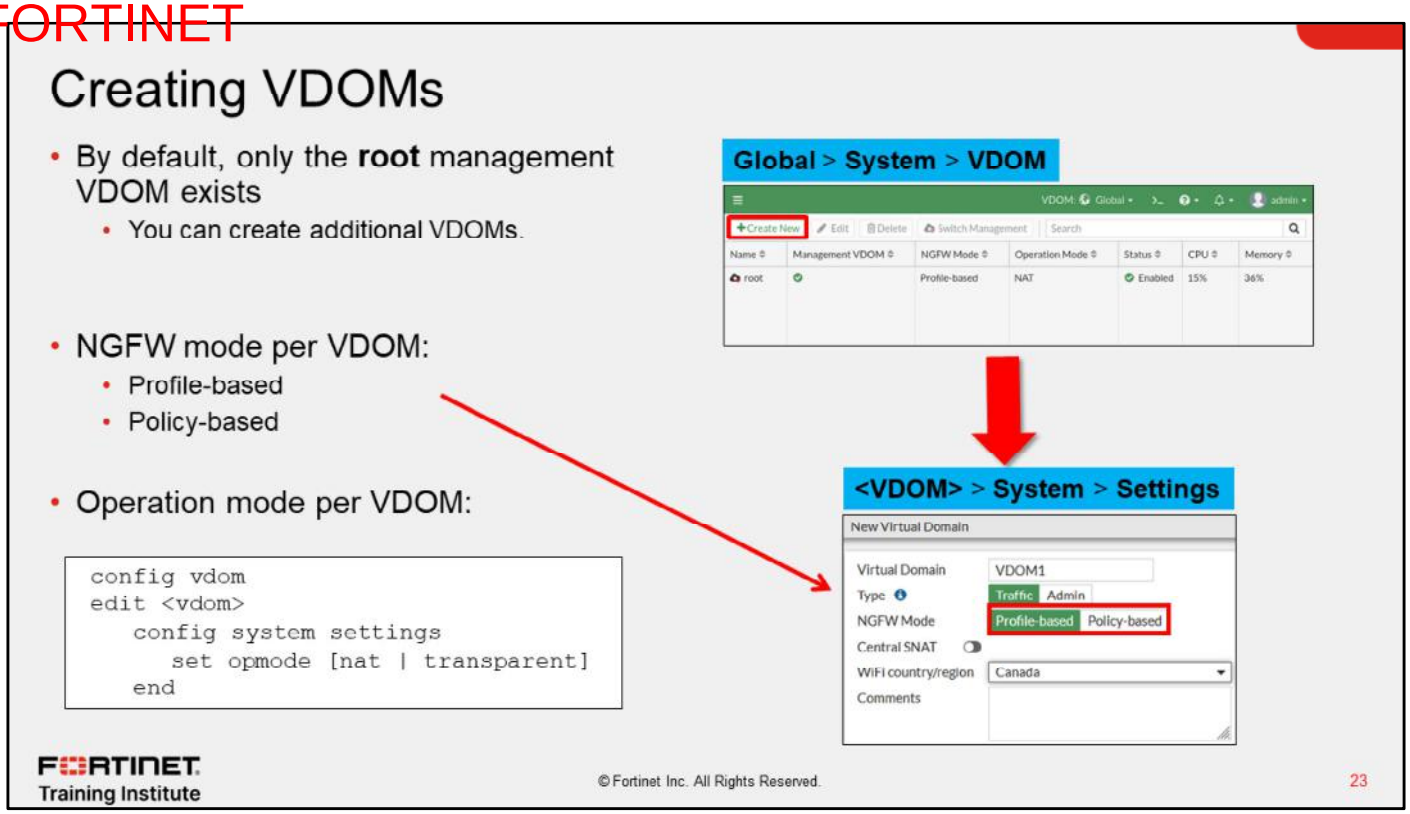
- From CLI:

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

FORTINET Training Institute

22

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.



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

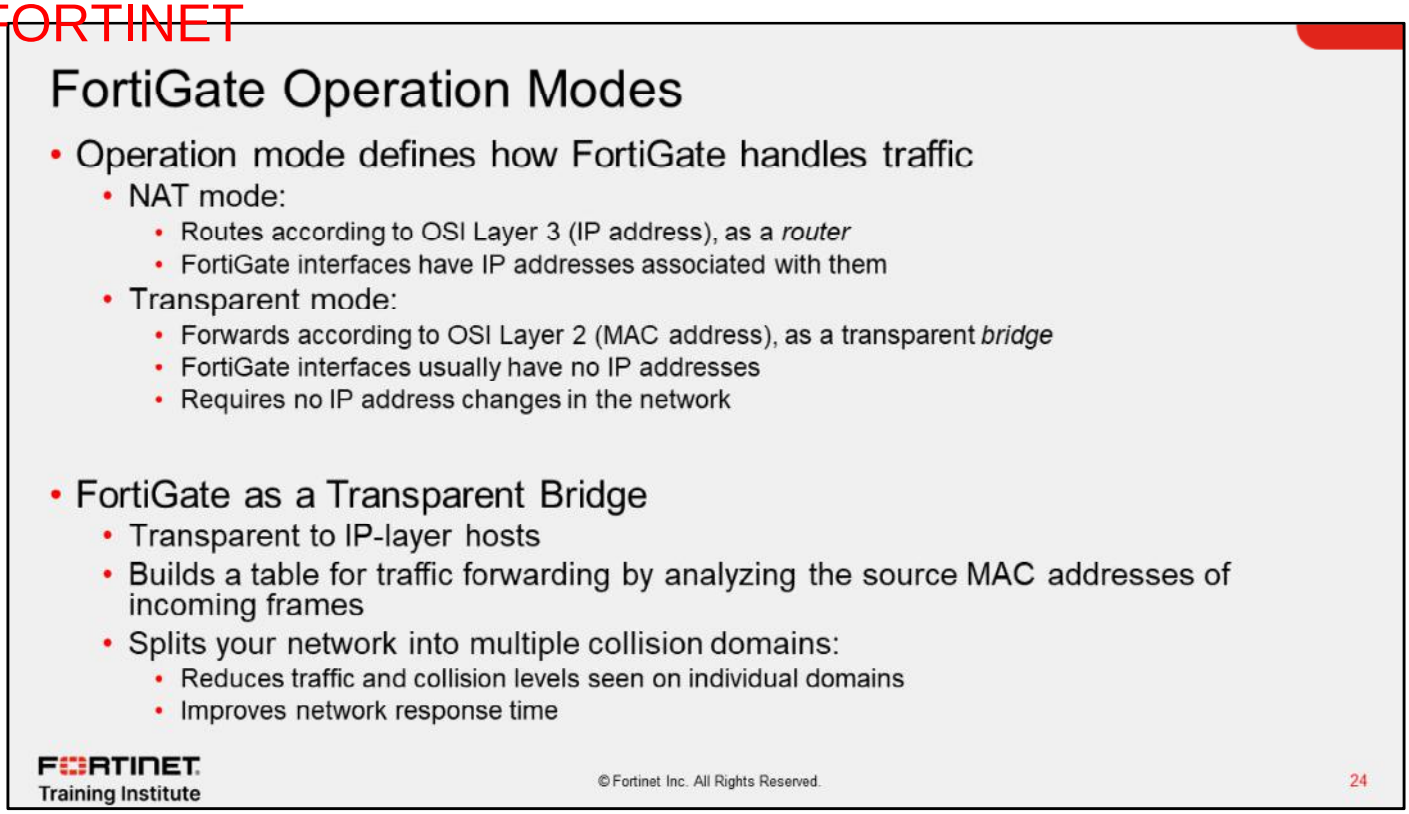
You need to add a VDOM for each of your security domains. If you're an MSSP, for example, you might add one VDOM for each client company. If you are an enterprise business, you might add one VDOM for each division of your company.

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.

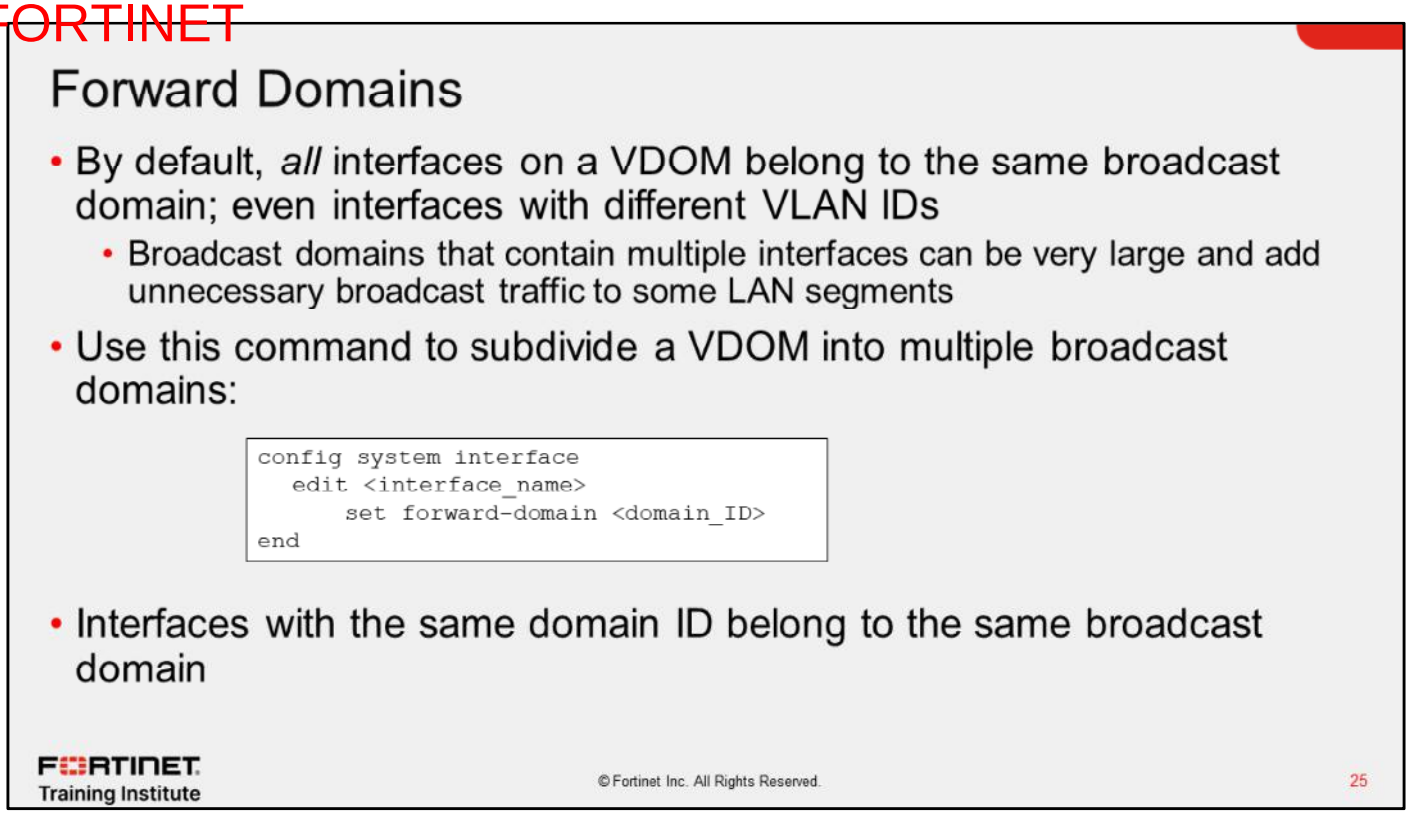


Traditional IPv4 firewalls and NAT mode FortiGate devices handle traffic the same way that routers do. Each interface must be in a different subnet and each subnet forms a different broadcast domain. FortiGate routes IP packets based on the IP header information, overwriting the source MAC address. So, 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.



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.

Confirmation Prompt When Creating VDOMs

- VDOM confirmation prompt added
  - So that users do not create new VDOMs accidently 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

FORTINET Training Institute

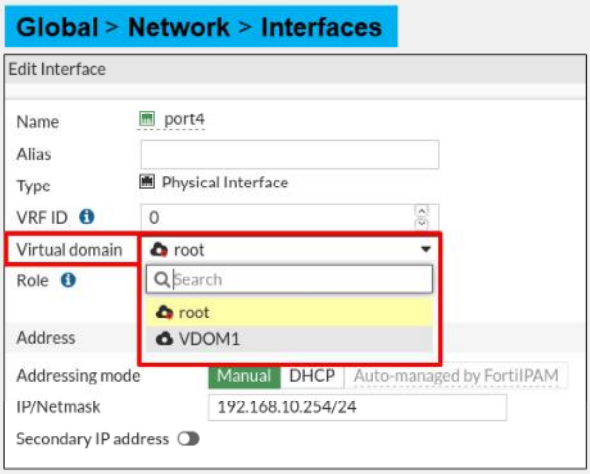
26

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.

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
```

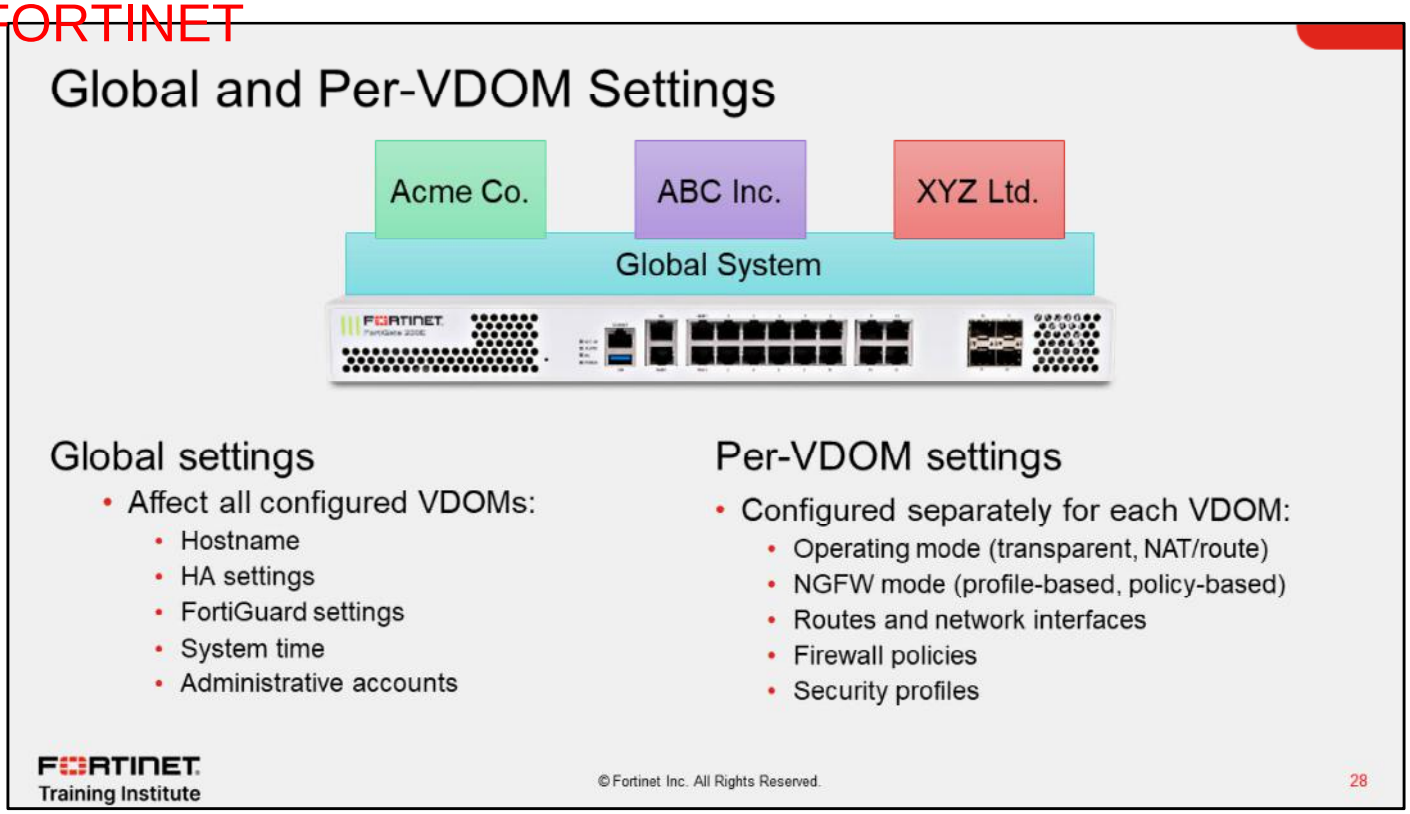


FORTINET Training Institute

27

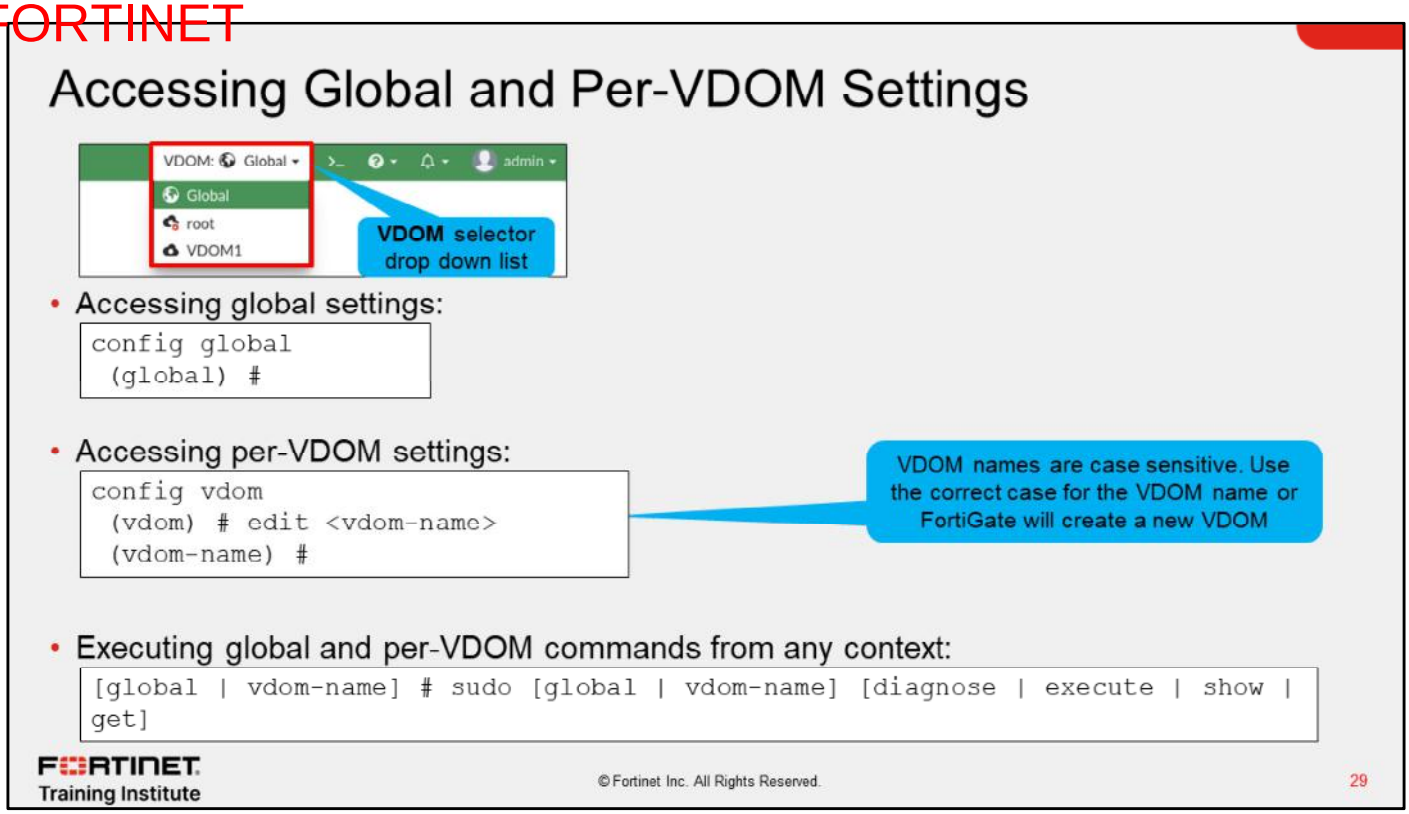
After adding a VDOM, you can specify which interface belongs to it. Each interface (physical or VLAN) can belong to only one VDOM.

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



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.



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

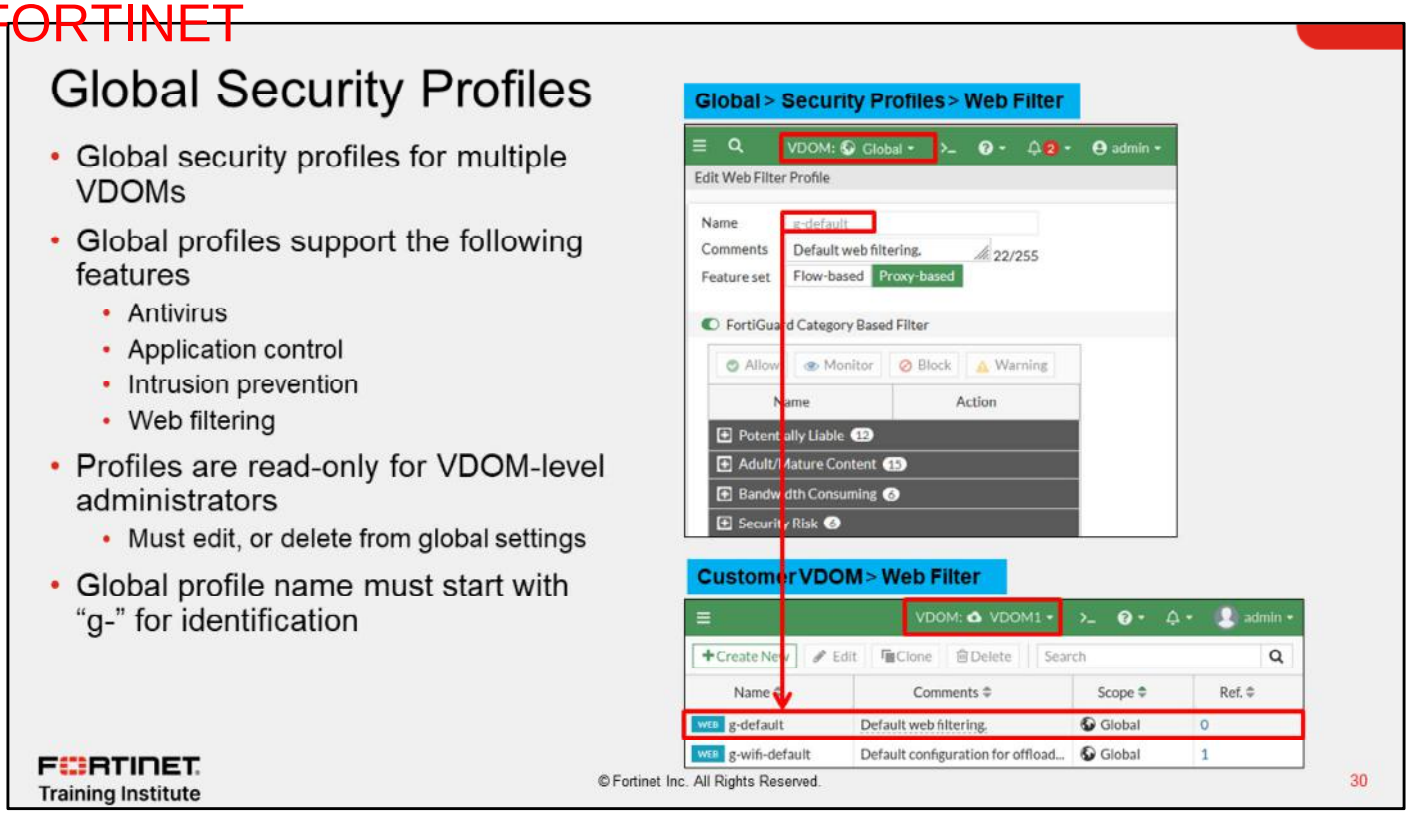
When you log in with the account named admin, you have access to all VDOMs. To access a specific VDOM, select it in the drop-down list at the top of the page.

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.



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.

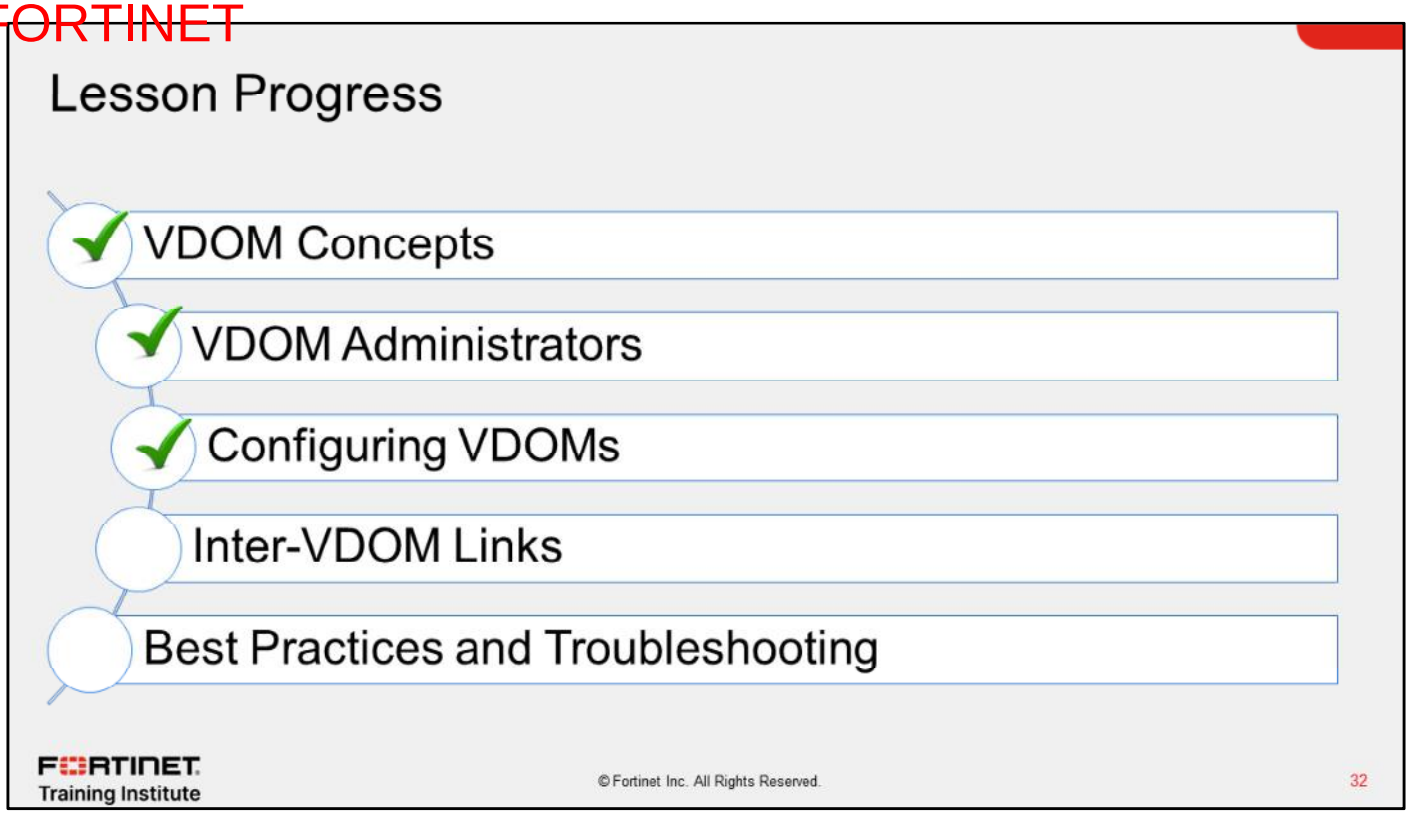
Knowledge Check

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

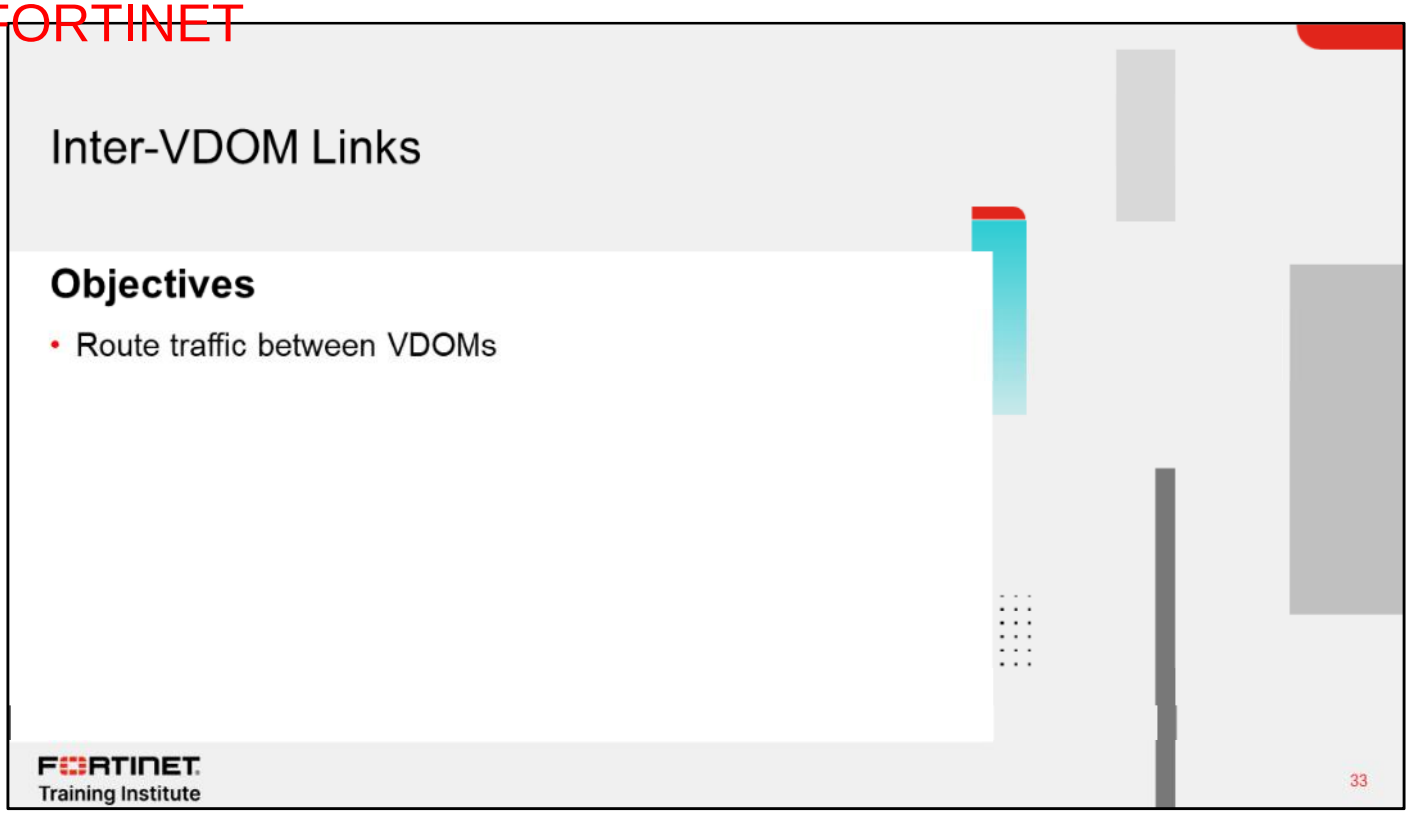
FORTINET Training Institute

31



Good job! You now understand how to configure VDOMs.

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



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.