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

Objectives

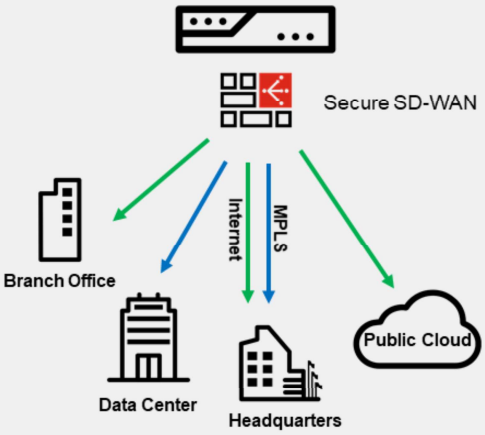
- Understand what SD-WAN is
- Identify the main use cases for SD-WAN
- Configure SD-WAN on FortiGate
- Understand and analyze routing behavior in an SD-WAN context
- Monitor SD-WAN behavior, link usage, and quality status

FORTINET Training Institute

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

What Is SD-WAN?

- Software-defined approach to steer WAN traffic using:
  - Flexible user-defined rules
    - Protocol and service-based traffic matching
    - Application-awareness
    - Dynamic link selection
  - Controls egress traffic
- Secure SD-WAN
  - Fortinet SD-WAN implementation (built-in security)
- Benefits:
  - Effective WAN use
  - Improved application performance
  - Cost reduction



FORTINET Training Institute

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

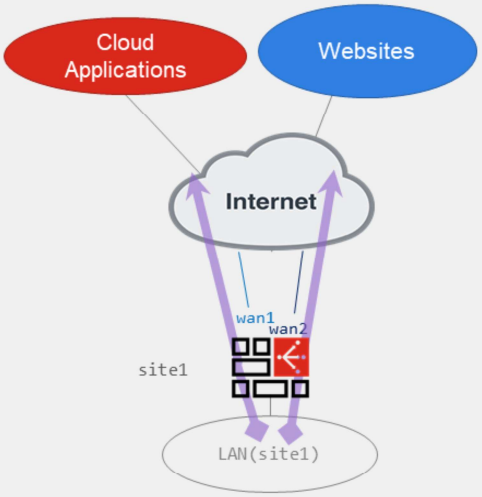
Secure SD-WAN relies on well-known FortiOS features, such as IPsec, link monitoring, advanced routing, internet services database (ISDB), traffic shaping, UTM inspection, and load balancing. The administrator can then combine these features and set rules that define how FortiGate steers traffic across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

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

Another benefit of SD-WAN is improved application performance because you can steer traffic through the best link that meets the application requirements. During congestion, you can leverage traffic shaping to prioritize sensitive and critical applications over less important ones.

SD-WAN Use Cases—Direct Internet Access

- Traffic steered across multiple physical internet links
- Typical operation:
  - Critical/sensitive traffic expedited and steered over best performing links
  - Costly links used for critical traffic or failover
  - Static default routing
- Example:
  - Two internet links (wan1 and wan2)
  - Both steer traffic from the LAN
  - Use best-performing link for critical applications
  - Use low-cost link for web surfing



FORTINET Training Institute

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

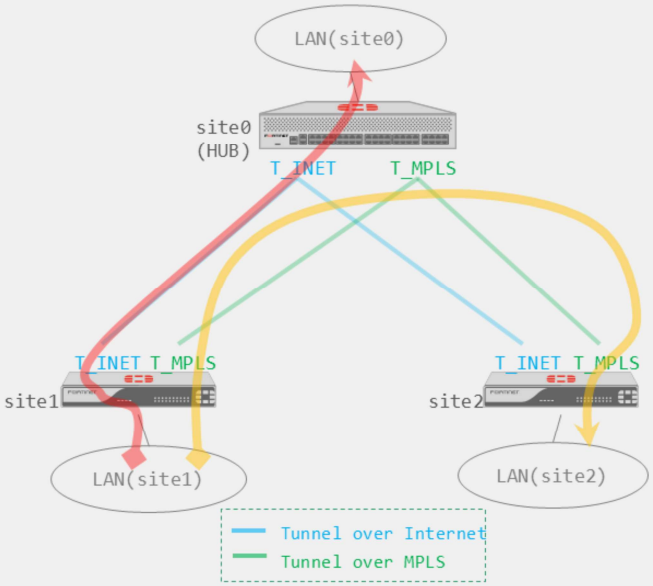
Usually, the administrator chooses to send sensitive traffic over the best-performing links, while distributing non-critical traffic across one or more links using a best-effort approach. Costly internet links are commonly used as backup links, or to steer critical traffic only.

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

Administrators can also manually define the upstream and downstream speeds of each link to prevent saturation during traffic distribution. Alternatively, they can configure FortiGate to use the SD-WAN bandwidth monitoring service to run speed tests against FortiGuard, and then automatically adjust the upstream and downstream speeds of the links based on the test results.

SD-WAN Use Cases—Site-to-Site Traffic

- Use overlay links to steer site-to-site corporate traffic
  - Overlay: tunnels
  - Underlay: physical links
- Typical operation:
  - Hub-and-spoke topologies
  - Dynamic IPsec tunnels used for overlay
  - Dynamic routing



FORTINET Training Institute

You can use SD-WAN to steer corporate site-to-site traffic. Usually, companies follow a hub-and-spoke topology, and use VPN tunnels—typically dynamic IPsec tunnels—to transport the traffic between the sites. The tunnels (also known as overlay links) are established over internet or MPLS links (also known as underlay links). Tunnels can also carry internet traffic from a spoke to a hub where it then exits to the internet.

SD-WAN can monitor the link quality of the tunnels and select the best performing link for sensitive and critical traffic

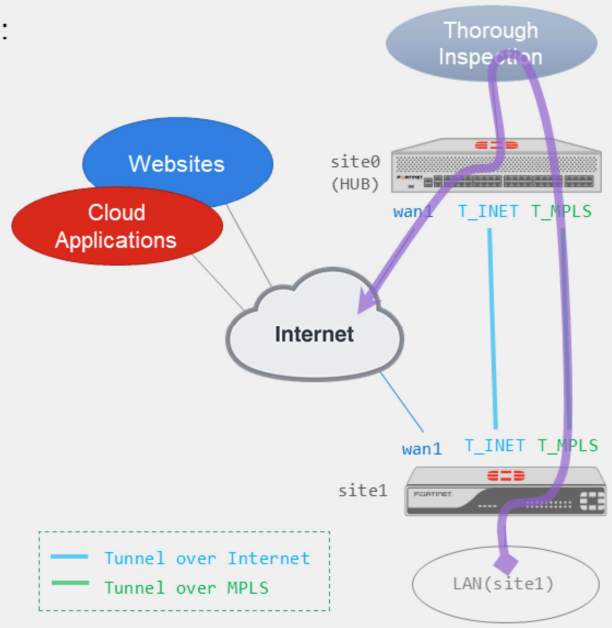
For routing, static routing is possible, but a dynamic routing protocol, such as BGP, is often used to exchange routing information through the tunnels. Dynamic routing scales more easily when adding new sites.

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

In the example shown on this slide, each site has two overlays configured, one using the internet underlay and the other the MPLS underlay. SD-WAN steers spoke-to-hub traffic.

SD-WAN Use Cases—Remote Internet Access

- Internet traffic steered across overlay links to:
  - Centralize inspection on hub
  - Improve performance if DIA performance is poor
  - Provide internet access if DIA is unavailable
- Typical operation:
  - Limited inspection on spokes
  - Hub performs thorough inspection
  - Backup direct internet access

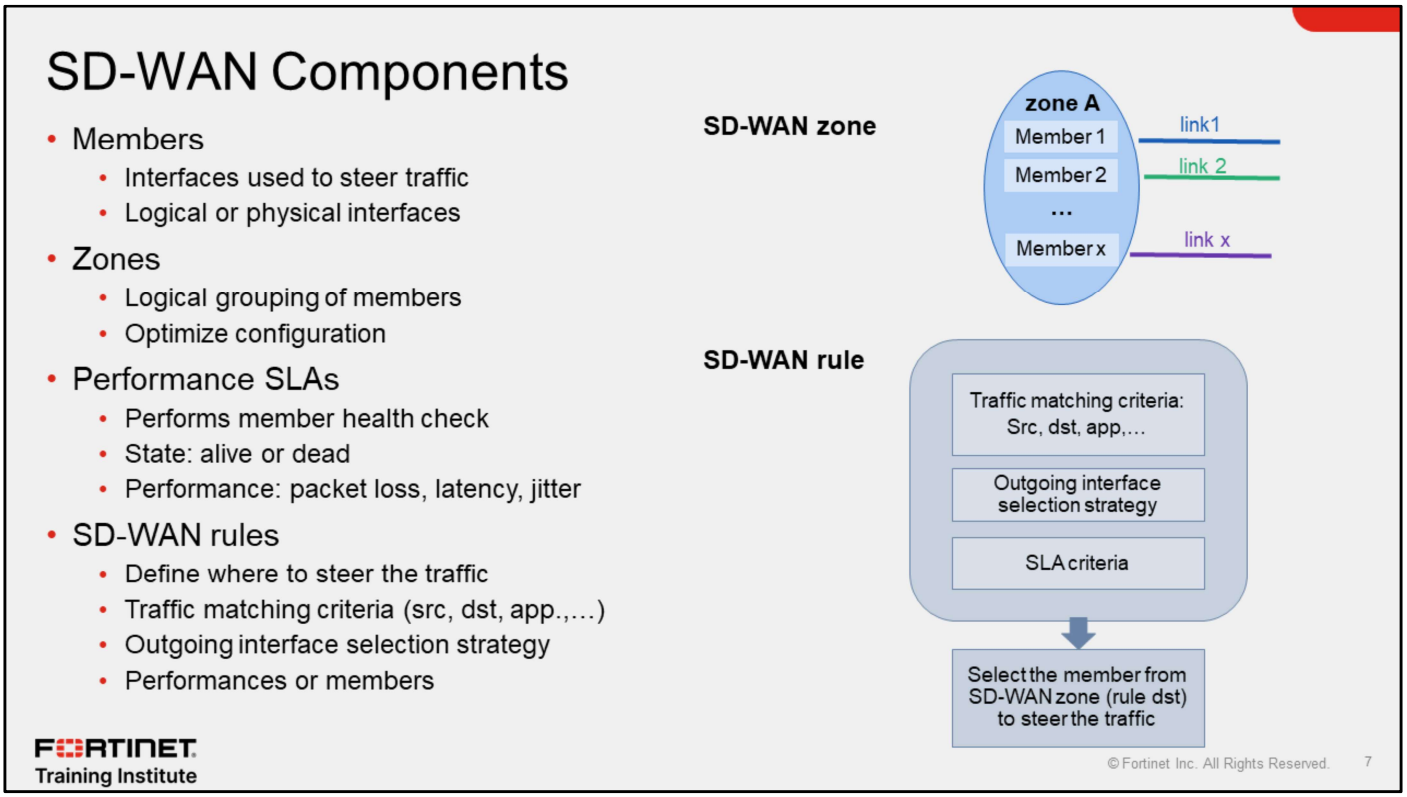


FORTINET Training Institute

Remote Internet Access (RIA), also known as remote breakout, is another use case for SD-WAN. Internet traffic from the spokes is backhauled through the WAN using overlay links. When the traffic arrives at the hub, it breaks out to the internet.

The most common reason to use RIA is to centralize security inspection and internet access on the hub. For example, you can have a central high-end FortiGate device that inspects all the internet traffic that leaves the organization and conforms with the company policy, instead of having each low-end spoke FortiGate device to inspect traffic, thus reducing costs and administrative overhead.

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



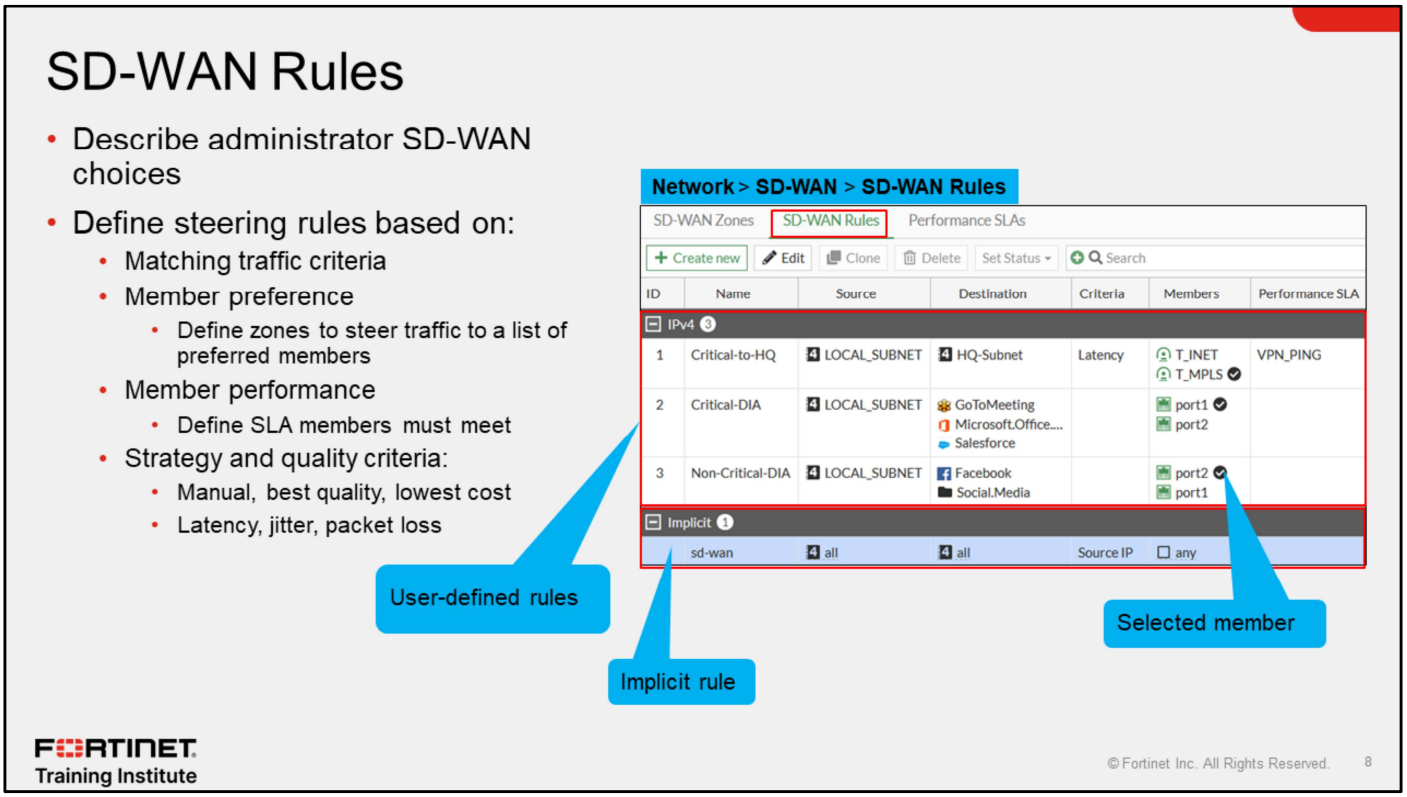
On FortiGate, an SD-WAN configuration is built on SD-WAN rules. SD-WAN rules combine traffic matching criteria and traffic steering preferences. They describe the administrator choices related to the SD-WAN solution.

To define SD-WAN rules use:

- Members: These are the logical or physical interfaces used to steer the traffic.
- Zones: Zones are groups of members used to optimize the configuration.
- Performances SLA rules: With the performance SLA rules you can define how you want to monitor the status of members and the performance criteria that you want to monitor. It can be packet loss, jitter, latency, or a weighted mix of a few criteria.

You first define the criteria of the application or traffic to match. Then, you indicate the forward policy to follow for steering traffic across one or more members and zones, including the strategy to apply and the performance metrics to determine the preferred members.

In the next few slides, you will learn more about each element that composes an SD-WAN rule.



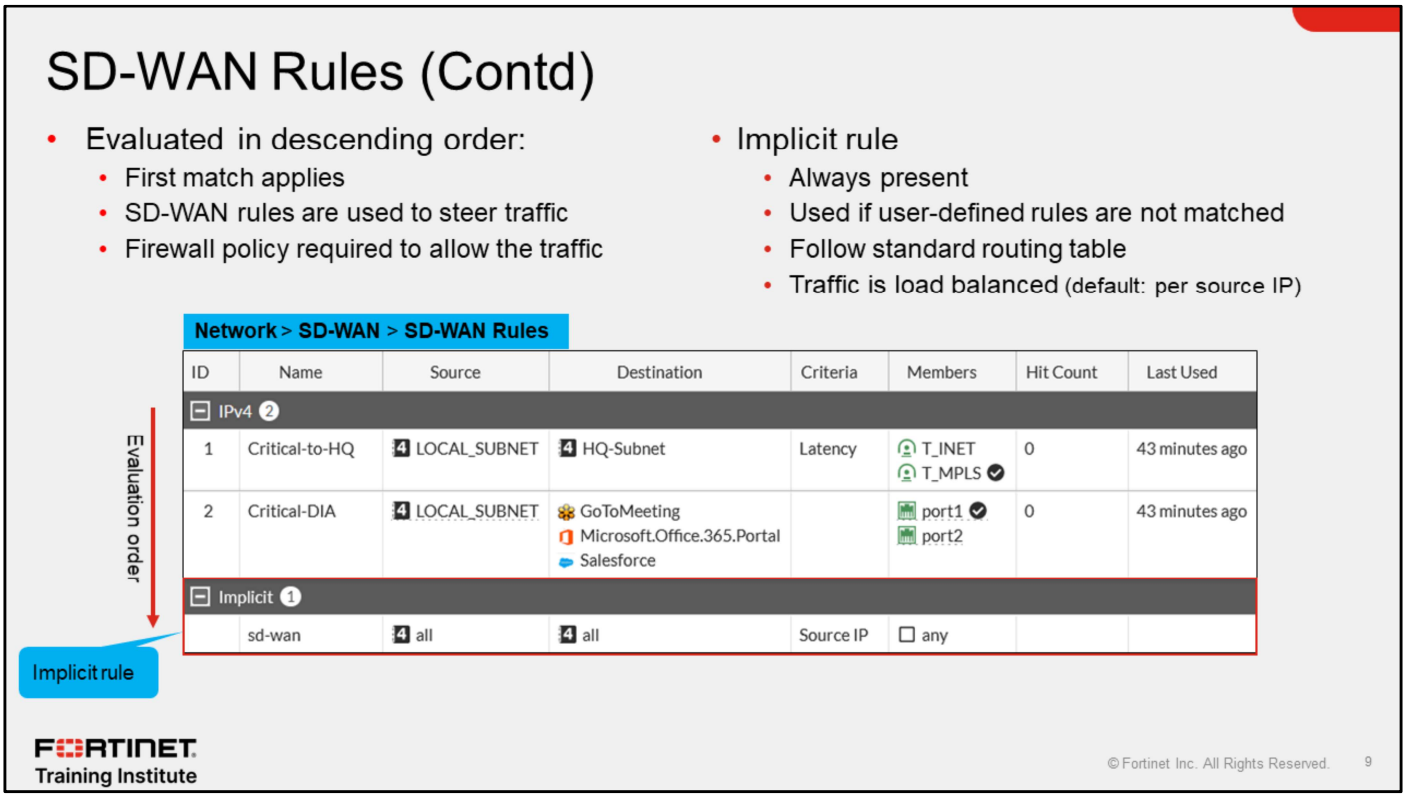
SD-WAN rules combine traffic-matching criteria and traffic-steering preferences. They describe the administrator choices related to the SD-WAN solution and the software-defined aspect of it.

You first define the criteria of the application or traffic to match. Then, you indicate the forward policy to follow for steering traffic across one or more members and zones, including the strategy to apply and the performance metrics to determine the preferred members.

Preferred members are the best alive members in a zone based on the strategy in use. FortiGate then uses the preferred members—provided they are acceptable—to steer traffic. For all strategies, if you don't activate a load balancing mode, FortiGate chooses a single member to steer traffic. You will discover the strategies available on a separate slide.

If none of the user-defined SD-WAN rules are matched, then FortiGate uses the implicit rule.

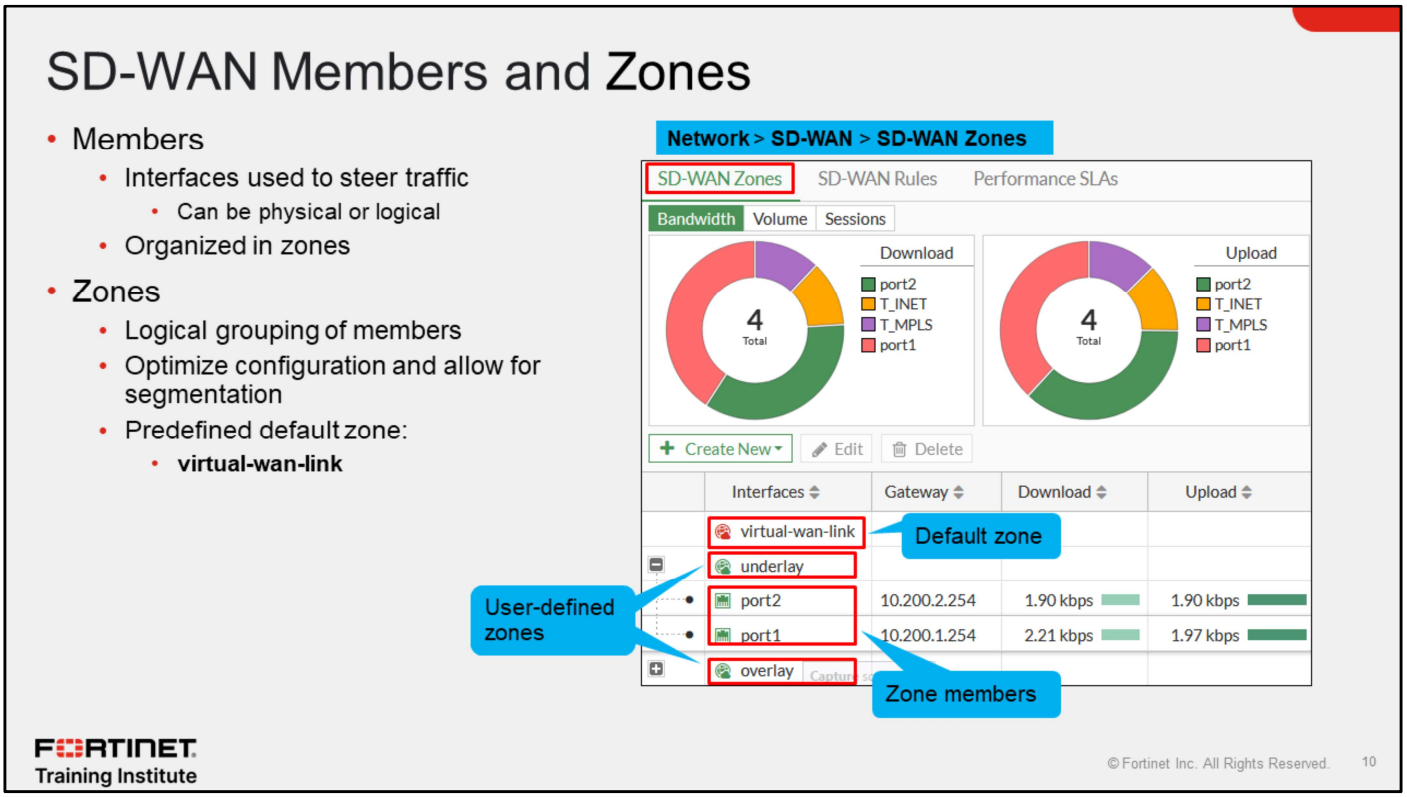
The example on this slide shows three user-defined rules. A rule named **Critical-to-HQ** which is used to steer critical traffic from the branch office to the headquarters. The rule steers traffic from LOCAL_SUBNET to the HQ-Subnet through the overlay links (T_INET and T_MPLS). The member selection is done with a latency criteria and T_MPLS is the selected member. The rules **Critical-DIA** and **Non-Critical-DIA**, which FortiGate uses to steer traffic for DIA through the underlay zone (port1 and port2), differentiate the link selection according to the application in use. Note that only the most significant parts of rule configuration are shown in the output.



FortiGate evaluates SD-WAN rules in the same way as firewall policies: from top to bottom, using the first match. However, unlike firewall policies, they are used to steer traffic, *not* to allow traffic. When you use SD-WAN rules, you *must* configure corresponding firewall policies to allow SD-WAN traffic.

There is an implicit SD-WAN rule created by default. It is always present at the bottom of the SD-WAN rule list. If none of the user-defined SD-WAN rules are matched, then the implicit rule is used. This means that FortiGate routes the traffic according to the regular process. By default, the implicit rule load balances the traffic across all available SD-WAN members. In the example above, the implicit rule can steer the traffic through overlay (T_INET, T_MPLS) or underlay (port1, port2) members, according to the best match in the routing table.

You can double-click the implicit rule to display the load balancing options. By default, the implicit rule load balances the traffic according to **Source IP**. You can decide to load balance according to **Source-Destination IP**, **Sessions**, **Volume**, or **Spillover**.



The first step to configure SD-WAN is to define the members and assign them to zones. This configuration is done on the **SD-WAN Zones** page.

Members (also known as links) are existing physical or logical FortiOS interfaces that you select to be part of SD-WAN. FortiGate then uses the interfaces to steer traffic based on the SD-WAN rules configured.

When you configure a member in SD-WAN, you must assign it to a zone and, optionally, set a gateway. Zones are logical groupings of interfaces. The interfaces in a zone have similar configuration requirements. Like FortiGate interface zones, the goal with SD-WAN zones is to reference them in the configuration instead of individual members to optimize the configuration by avoiding duplicate settings. When set, FortiGate uses the **Gateway** setting as the next hop to forward traffic through the member.

FortiGate creates one zone by default, called **virtual-wan-link** zone. It is where FortiGate places any new member if you don't assign them to a user-defined zone.

The example on this slide shows the default SD-WAN zone—**virtual-wan-link**—and two user-defined zones: **underlay** and **overlay**. The **underlay** zone contains **port1** and **port2** as members, which are used for a basic DIA setup. Note that although the zone is named **underlay** because it contains this type of members, you can assign any name you like.

SD-WAN Members—Underlay and Overlay Links

- Underlay:
  - Physical links provided by ISP
    - Cable, DSL, fiber, MPLS, 3G/4G/LTE, ATM
  - Restricted routing
  - No added security
- Overlay:
  - Virtual links built on top of underlay links
    - IPsec, GRE, IP-in-IP
  - Flexible routing
  - Enhanced security

Supported SD-WAN Members*	
Interface	**Type**
Physical	Underlay
VLAN	
LAG	
3G/4G/LTE USB modems	
FortiExtender	
IPsec (including ADVPN)	Overlay
GRE	
IP-in-IP	

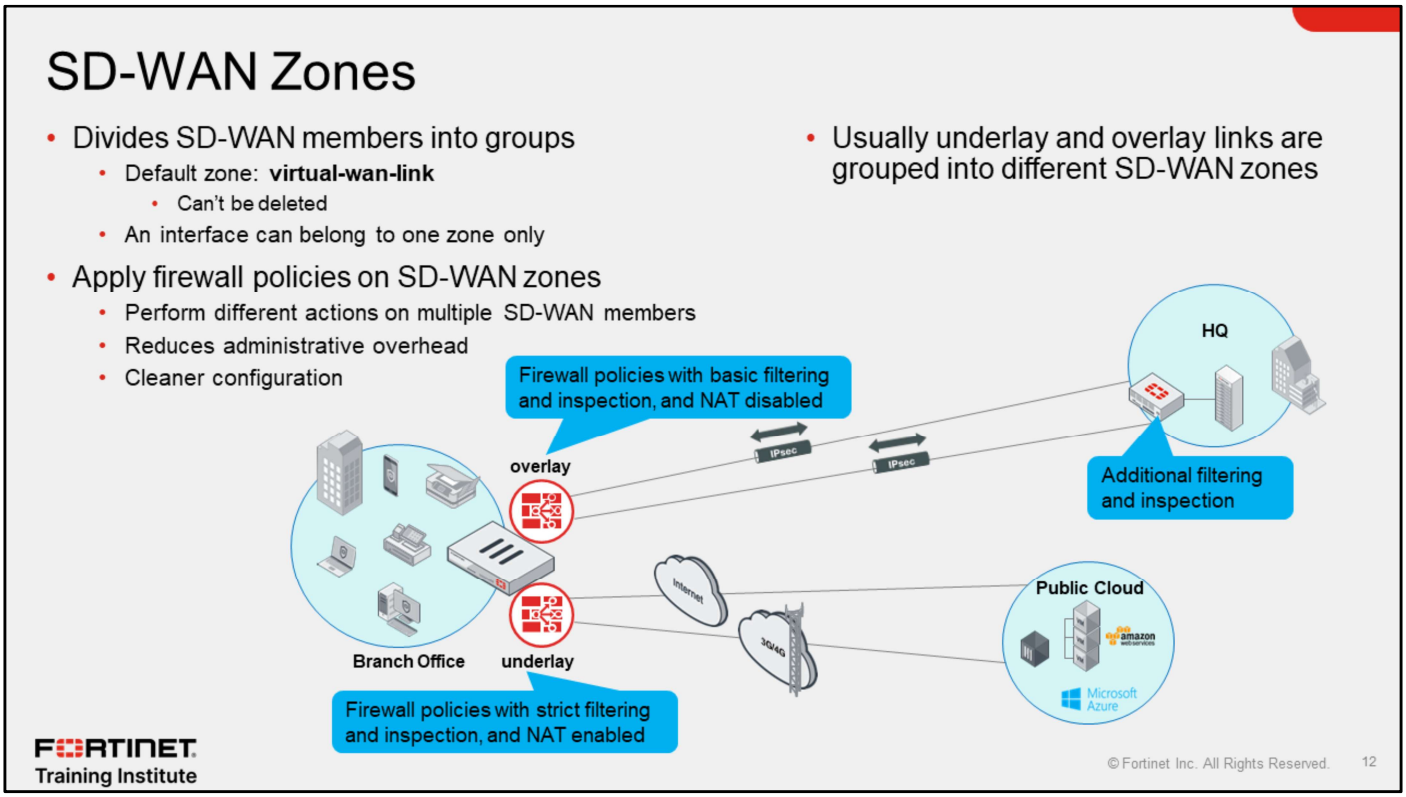
FORTINET Training Institute

In an SD-WAN environment, the terms *underlay* and *overlay* are commonly used to describe the link type of an SD-WAN member.

Underlays refer to the physical links that you can rent or buy from an ISP, such as cable, DSL, fiber, MPLS, 3G/4G/LTE, and ATM links. These links are part of the ISP physical infrastructure that is responsible for delivering packets across networks. The traffic that travels through underlays is restricted to the routing policies deployed by the ISP and, therefore, the packet source and destination IP addresses must be routable within the ISP network. This restriction leaves you with limited options to define your network addressing plan. In addition, traffic transmitted through underlays is usually not encrypted by the ISP network, which means that unauthorized parties can access sensitive data if the sender does not encrypt the data.

Overlays are virtual links that you build on top of underlays. A common example of an overlay is an IPsec tunnel. Because original packets are often encapsulated in ESP packets, the networks that communicate through the IPsec tunnel are no longer restricted to the routing policies of the ISP. In addition, the privacy and authentication features provided by IPsec protect your traffic from unauthorized access.

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

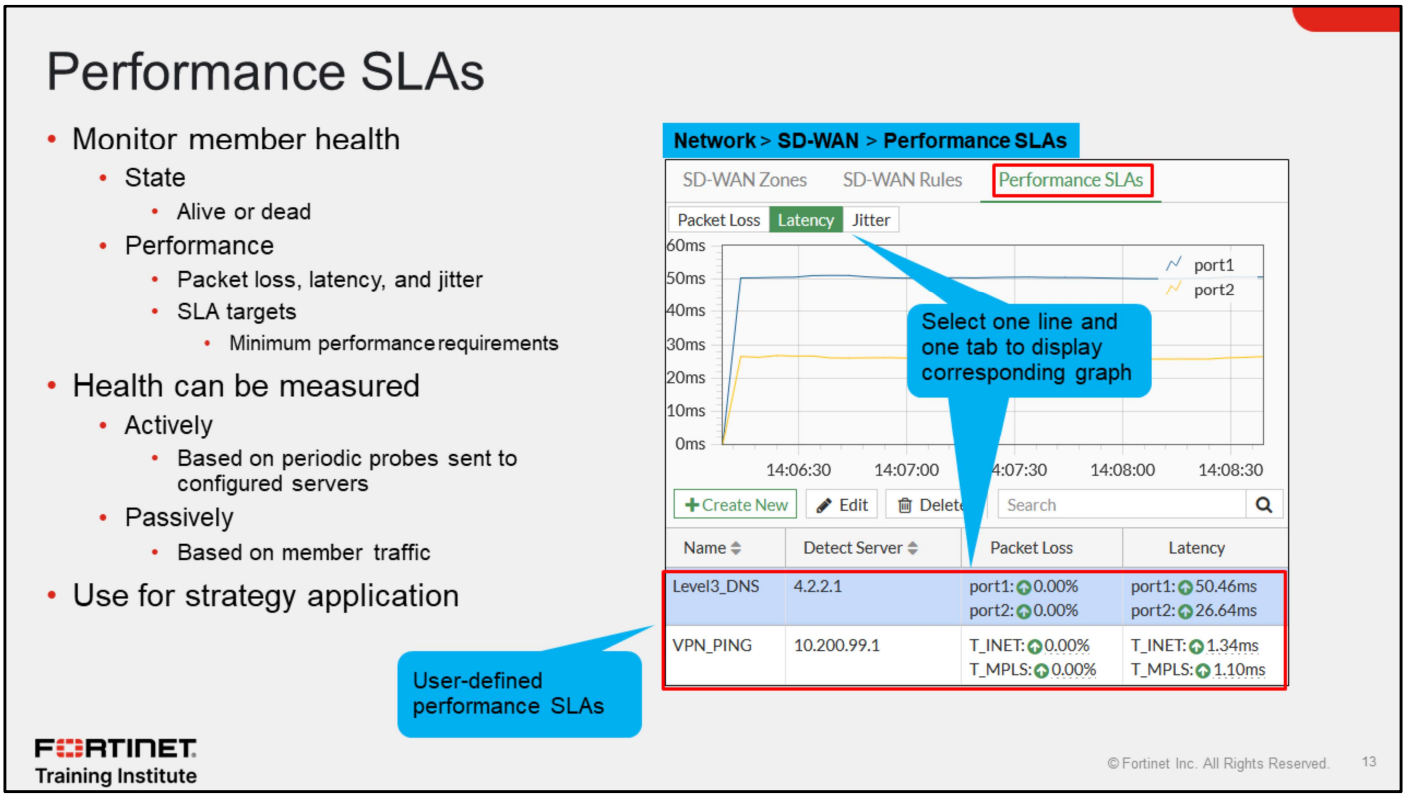


Usually, you should apply a different set of policies based on the link type of your SD-WAN members. For example, you may want to enable NAT and apply strict security policies to internet traffic sent through underlay links, because the traffic directly leaves the site boundaries. Conversely, you may want to disable NAT and apply basic filtering and inspection to traffic sent through overlay links, because the remote site is fully routable and performs additional filtering and inspection on the traffic.

SD-WAN zones allow administrators to group members that require a similar set of firewall policies. Usually, this means grouping underlays and overlays into different SD-WAN zones.

FortiGate creates the **virtual-wan-link** SD-WAN zone by default, which you can't delete. It contains any SD-WAN member not explicitly assigned to a user-defined SD-WAN zone. Firewall policies defined for your SD-WAN traffic, must reference the SD-WAN zones, and cannot reference individual SD-WAN members.

The topology shown on this slide shows a branch office with two SD-WAN zones configured: overlay and underlay. The overlay SD-WAN zone is composed of IPsec tunnels and the underlay SD-WAN zone is composed of an internet link and a 3G/4G link. The branch office uses the overlays to access the headquarter networks, and the underlays to access services in the public cloud. By dividing SD-WAN members into zones, you can apply the same set of firewall policies to a zone instead of having to apply them to their individual members, thus reducing the administrative overhead and building a cleaner configuration.

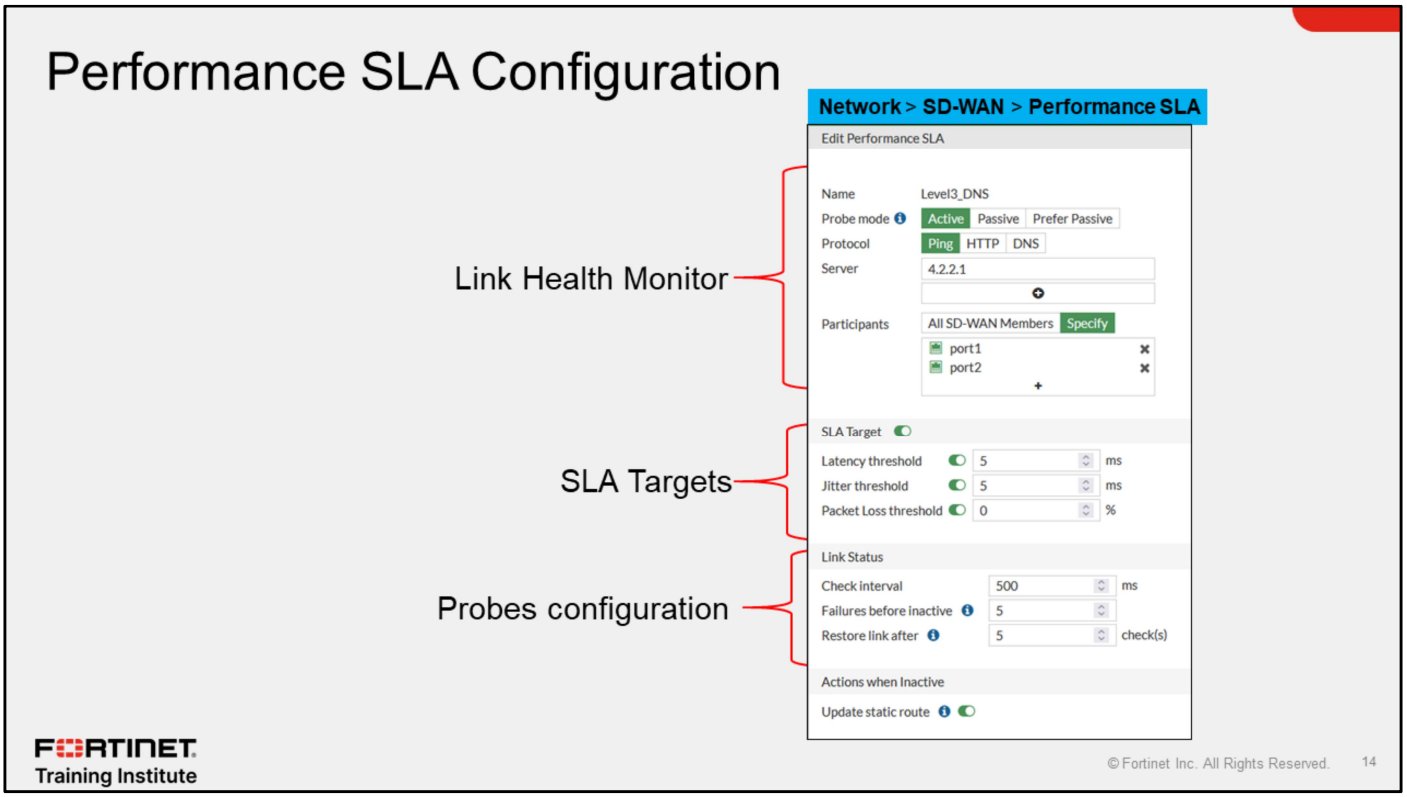


After you define your SD-WAN members and assign them to zones, you will probably want to monitor the health of your SD-WAN members on the **Performance SLAs** page. Although configuring performance SLAs is optional, you should configure them to ensure members meet the health and performance requirements for steering traffic, which is critical for effective WAN use with SD-WAN.

FortiGate performance SLAs monitor the state of each member—whether it is alive or dead—and measures the member packet loss, latency, and jitter. SD-WAN then uses the member health information to make traffic steering decisions based on the configured SD-WAN rules. For example, you can instruct FortiGate to steer internet traffic to a member, provided the member is alive and its latency doesn't exceed a given threshold. Performance SLAs also detect situations where the interface is physically up, but FortiGate is unable to reach the desired destination and flags the corresponding link as dead.

When you configure a performance SLA, you can decide whether you want to monitor the link health actively or passively. In active monitoring, the performance SLA checks the health of the member periodically—by default every 500ms— sending probes from the member to one or two servers that act as a beacon. In passive monitoring, the performance SLA determines the health of a member based on the traffic passing through the member. Note that only active monitoring can detect if a link is alive or dead.

The example on this slide shows an entry named **Level3_DNS**. The entry contains the well-known **4.2.2.1** and **4.2.2.2** DNS servers, both of which are used to monitor the health of **port1** and **port2**. The performance SLA **VPN_PING** monitors the health of the two overlay tunnels, T_INET and T_MPLS. The results show that the members are alive (green arrow), report no packet loss, and have average values for latency (jitter is also measured but not visible in this example).



When you configure a performance SLA rule, you first define the link health monitor parameters.

In this section you will define the detection mode that FortiGate uses to monitor the link quality:

- **Active**: FortiGate sends active probes to the configured server to monitor the link health.
- **Passive**: FortiGate uses traffic through the link to evaluate the link health. It uses session information from traffic on selected firewall policies (firewall policies with the parameter `passive-wan-health-measurement` enabled).
- **Prefer Passive**: FortiGate uses passive monitoring and, only if there is no traffic through the link, sends probes.

You can specify up to two servers to act as your beacons. This guards against the server being at fault, and not the link.

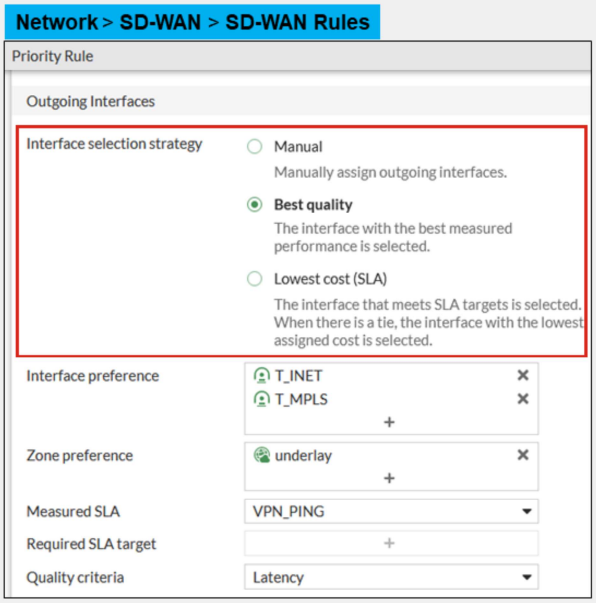
The SLA target section is optional. It's where you define the performance requirements of alive members (latency, jitter, and packet loss thresholds). The performance SLA uses SLA targets with some SD-WAN rule strategies, like **Lowest Cost (SLA)**, to decide if the link is eligible for traffic steering or not.

The link status section is available for **Active** and **Prefer Passive** probe mode. It is where you define how often FortiGate sends probes through each monitored link, and how many failed probes you accept before declaring a link as dead.

The example of this slide shows the configuration of a performance SLA named Level3_DNS. It is defined with **Active** probe mode, and default values for SLA target and probe configuration. It monitors the status and performances of two underlay interfaces, port1 and port2.

SD-WAN Rules Strategies

- Define
  - Requirements for preferred members
  - Single or multiple member traffic distribution
- Preferred members
  - Best candidates to steer traffic
  - Are used only if they have a valid route to the destination
- Member selection
  - **Manual**
    - Configuration order preference
  - **Best Quality**
    - Best performing member based on quality criteria
  - **Lowest Cost (SLA)**
    - Member that meets SLA target (tiebreakers: cost and priority)



FORTINET Training Institute

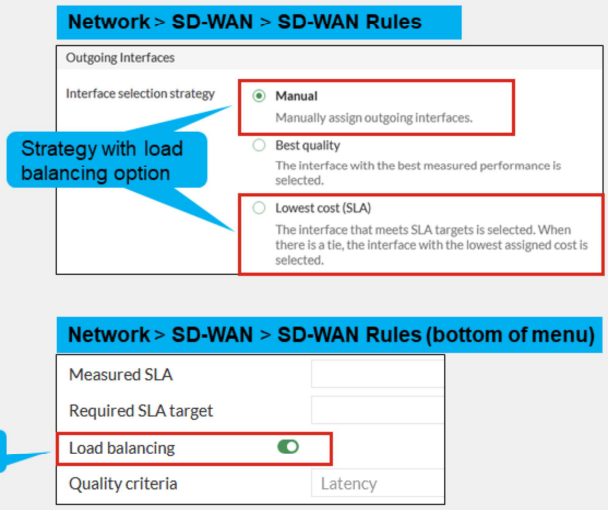
The strategy in a rule defines the requirements for preferred members. The preferred members are the best members from the outgoing interface (`oif`) list—based on the strategy in use—that meet the SLA requirements (if applicable). The `oif` list sorts the configured members by preference. That is, although the members are the same, their order in the `oif` list, and in **Interface Preference** list, can be different. There are three strategies you can chose from:

- **Manual**: FortiGate prefers members according to configuration order. Member metrics are not considered for member preference.
- **Best Quality:** FortiGate prefers the best-performing member based on the configured quality criteria.
- **Lowest Cost (SLA)**: FortiGate prefers the member that meets the configured SLA target. If multiple members meet the SLA target, member cost, followed by the configuration order, are used as tiebreakers.

Note that for all strategies, by default, FortiGate must check that the preferred member has a valid route to the destination. If the member doesn't have a valid route, then FortiGate checks the next member in the `oif` list, and so on, until it finds an acceptable member. Moreover, all strategies, except **Manual**, consider the member metrics for member preference.

Load Balancing Strategy

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



FORTINET Training Institute

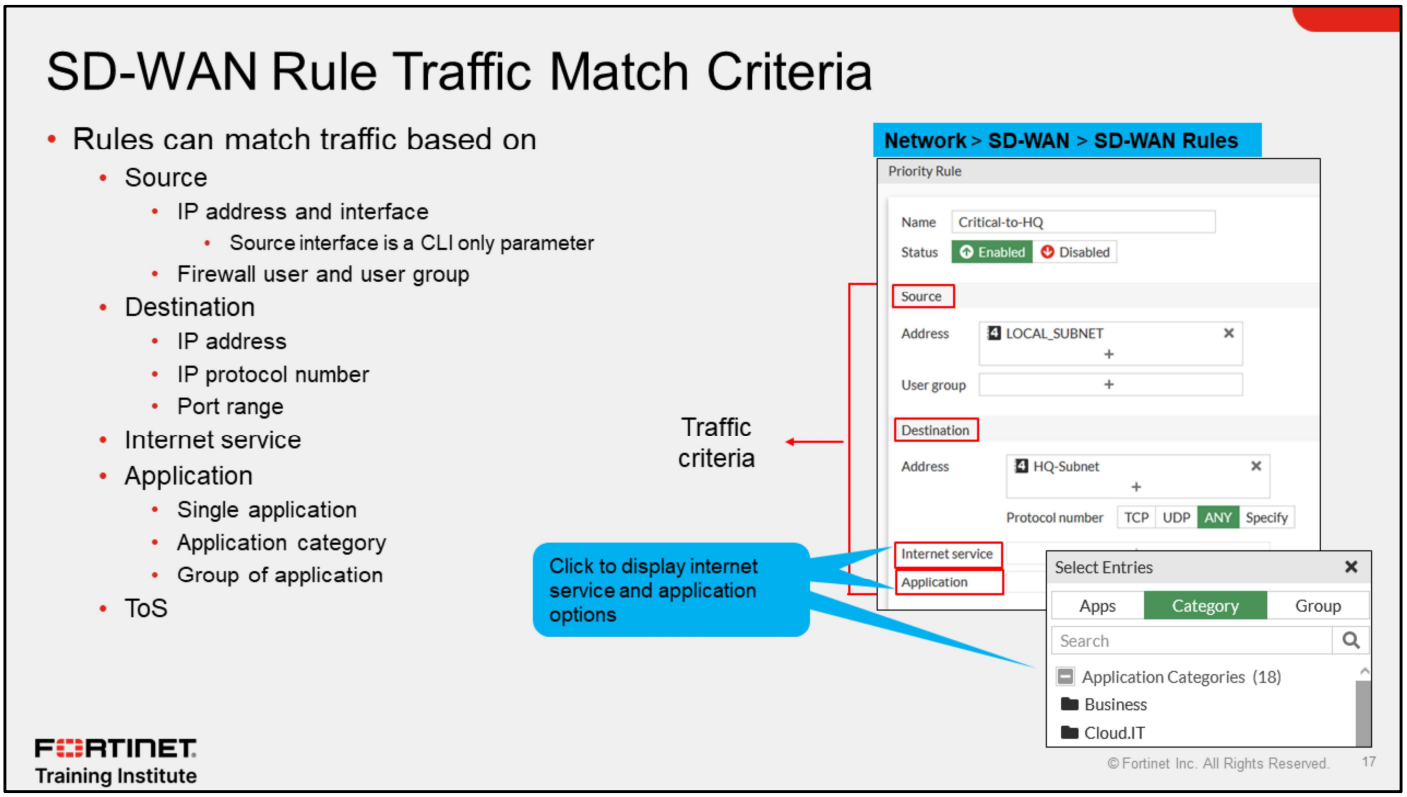
 16

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

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

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

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



You can configure rules to match traffic based on the following criteria:

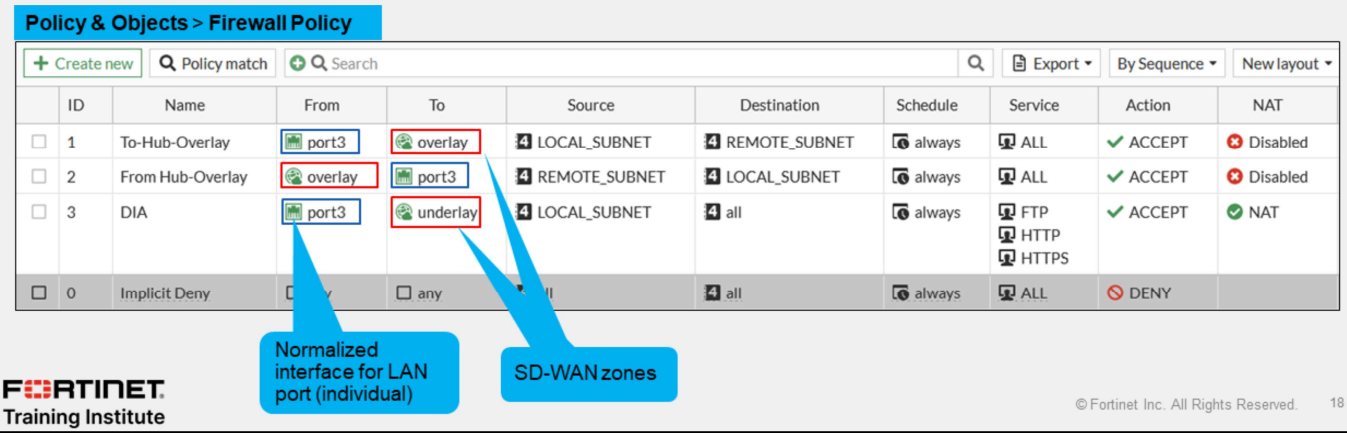
- Source IP address, source interface, firewall user, and firewall user group. If you want to specify the source interface, you should use the CLI commands `input-device` and `input-device-negate`.
- Destination IP address, IP protocol, destination port number
- Internet service
- Application: single application, application category, or group of applications
- Type of Service (ToS)

SD-WAN rules offer great flexibility for traffic matching. For example, you can match Netflix traffic sourced from specific authenticated users, or match the ICMP traffic—IP protocol 1—destined to a particular address.

Note that, by default, the GUI rule configuration menu does not display the application criteria field. If you want to use this feature, you should enable the criteria visibility from the CLI under `config system global`.

Firewall Policies With SD-WAN

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



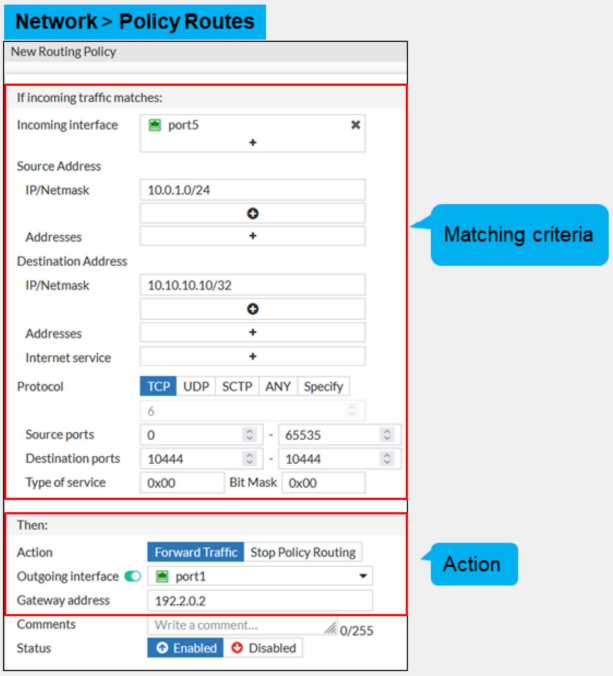
To be allowed by FortiGate, the traffic steered by an SD-WAN rule *must* also be allowed by a firewall policy.

You configure SD-WAN firewall policies in the same way as regular firewall policies, except that, when selecting an outgoing or incoming interface, you must reference a normalized interface that refers to an SD-WAN zone. When you reference a zone, you simplify the configuration by avoiding duplicate firewall policies. You can't use individual members of an SD-WAN zone in firewall policies.

The example on this slide shows firewall policies that reference the **underlay** and **overlay** SD-WAN zones. The **underlay** zone contains port1 and port2 as members, and the **overlay** zone contains T_INET and T_MPLS. Those policies also contain, as source or destination, the normalized interface for the individual port port3. This interface is *not* part of an SD-WAN zone.

Policy Routes

- Provide more granular matching than static routes
  - Protocol
  - Source address
  - Source ports
  - Destination ports
  - ToS marking
  - Destination internet service
- Have precedence over SD-WAN rules and entries in the FIB
- Best practice
  - Narrow down matching criteria
- SD-WAN rules are essentially policy routes with additional software-defined criteria



FORTINET Training Institute

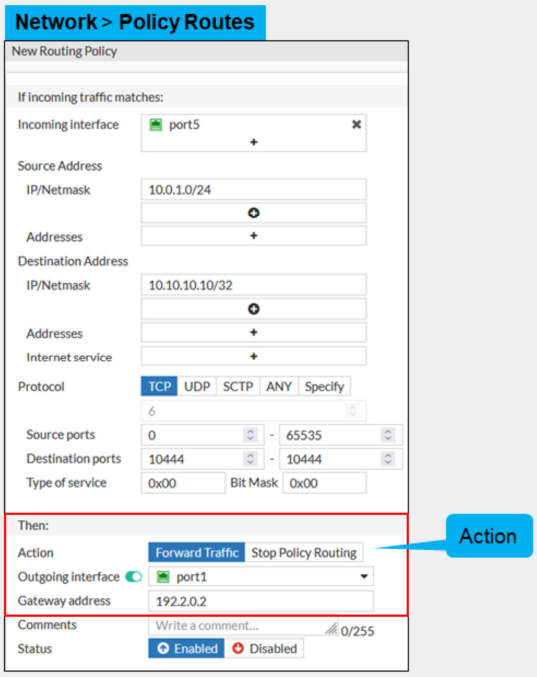
When you configure an SD-WAN rule, FortiGate essentially applies a policy route on FortiOS. For this reason, before learning how routing in SD-WAN works, it is useful to first understand policy routes.

Static routes are simple and are often used in small networks. Policy routes, however, are more flexible because they can match more than just the destination IP address. For example, you can configure as matching criteria the incoming interface, the source and destination subnets, protocol, and port number. *Because regular policy routes have precedence over any other routes*, it is a best practice to narrow down the matching criteria as much as possible. Otherwise, traffic that is expected to be routed by SD-WAN rules or other routes in the forwarding information base (FIB) could be handled by regular policy routes instead.

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

Policy Route—Actions

- **Stop Policy Routing**
  - Skips all policy routes, uses the FIB
- **Forward Traffic**
  - Forwards traffic using the set outgoing interface and gateway
  - FIB must have a matching route; otherwise, policy route is considered invalid and skipped

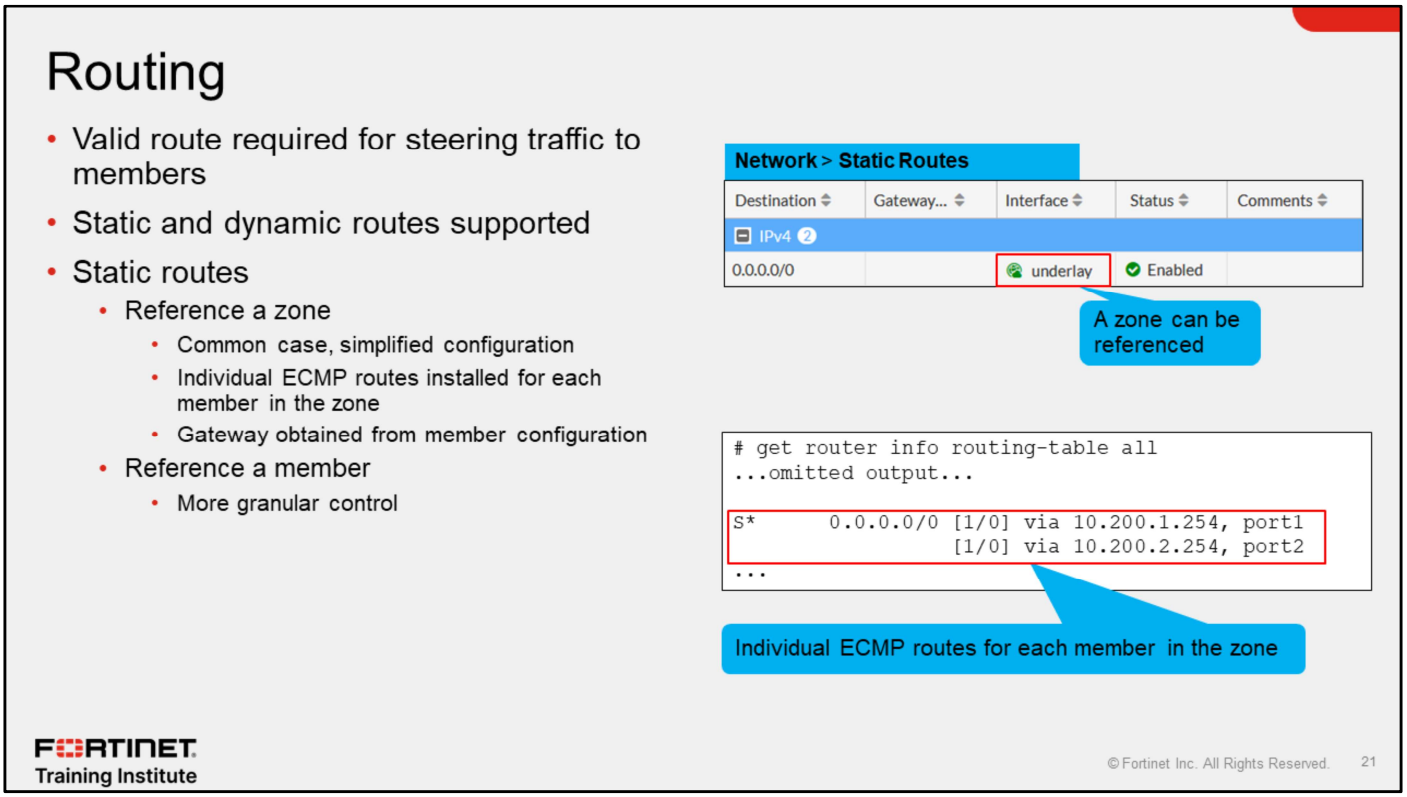


FORTINET Training Institute

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

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

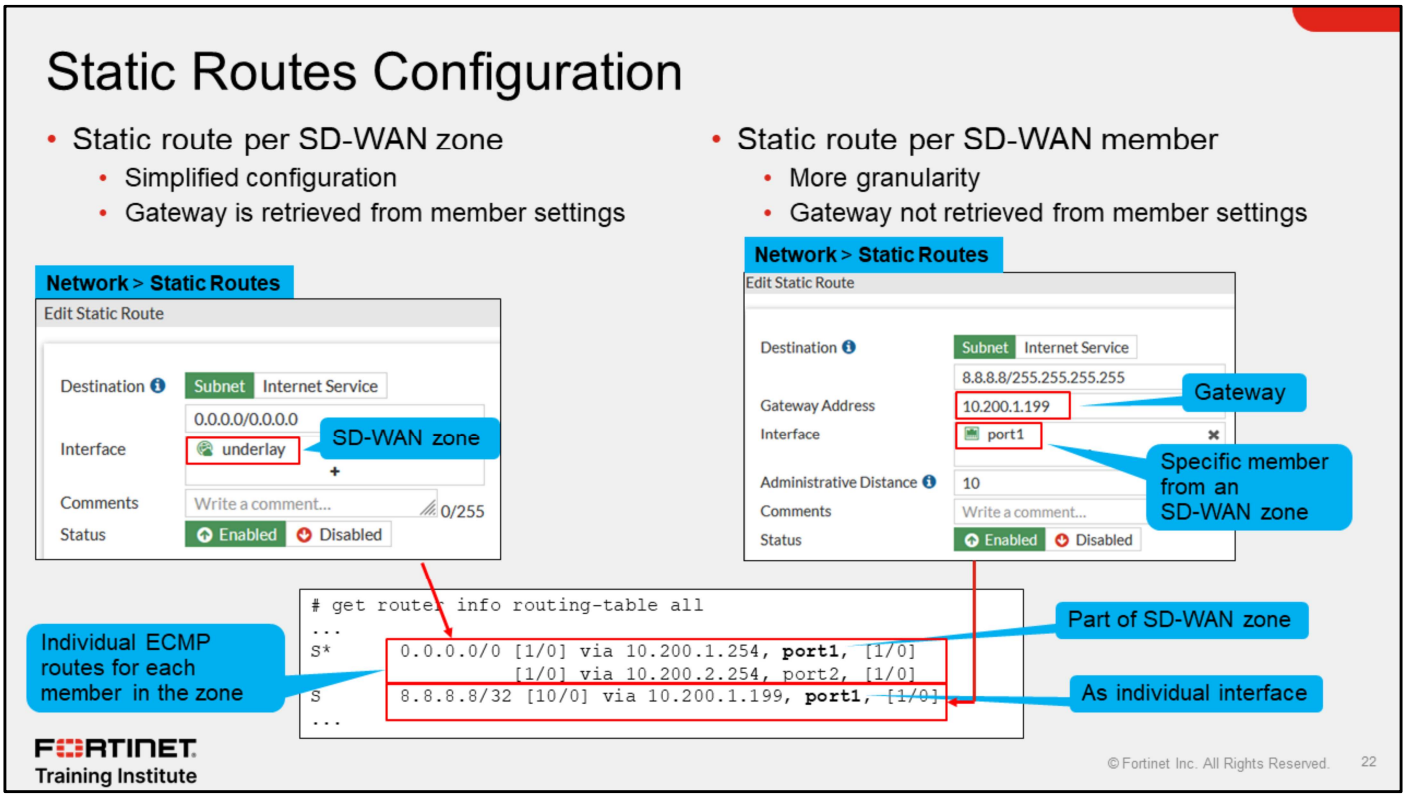
Also note that policy routes have precedence over SD-WAN rules, and over any routes in the FIB. That is, if a packet matches a policy route and the policy route has a matching route in the FIB, then FortiGate doesn't check any of the configured SD-WAN rules or the routes in the FIB.



SD-WAN rules define the traffic steering policies in SD-WAN. However, traffic won't be forwarded to an SD-WAN member unless there is a valid route that matches the destination address of the traffic through the SD-WAN member.

Because the goal is to have SD-WAN pick the best member to forward the traffic to, based on the SD-WAN rule criteria, it's a best practice to configure your routing setup so your SD-WAN sites know all possible routes to all possible destinations that are intended for handling by SD-WAN. Otherwise, SD-WAN may fail to choose the best member, not because it doesn't meet the application requirements, but because FortiGate doesn't have a route for the destination and member.

You can use static and dynamic routing in SD-WAN. This slide shows an example of a static default route configured for the **underlay** zone, which is used to route traffic in a basic DIA setup.

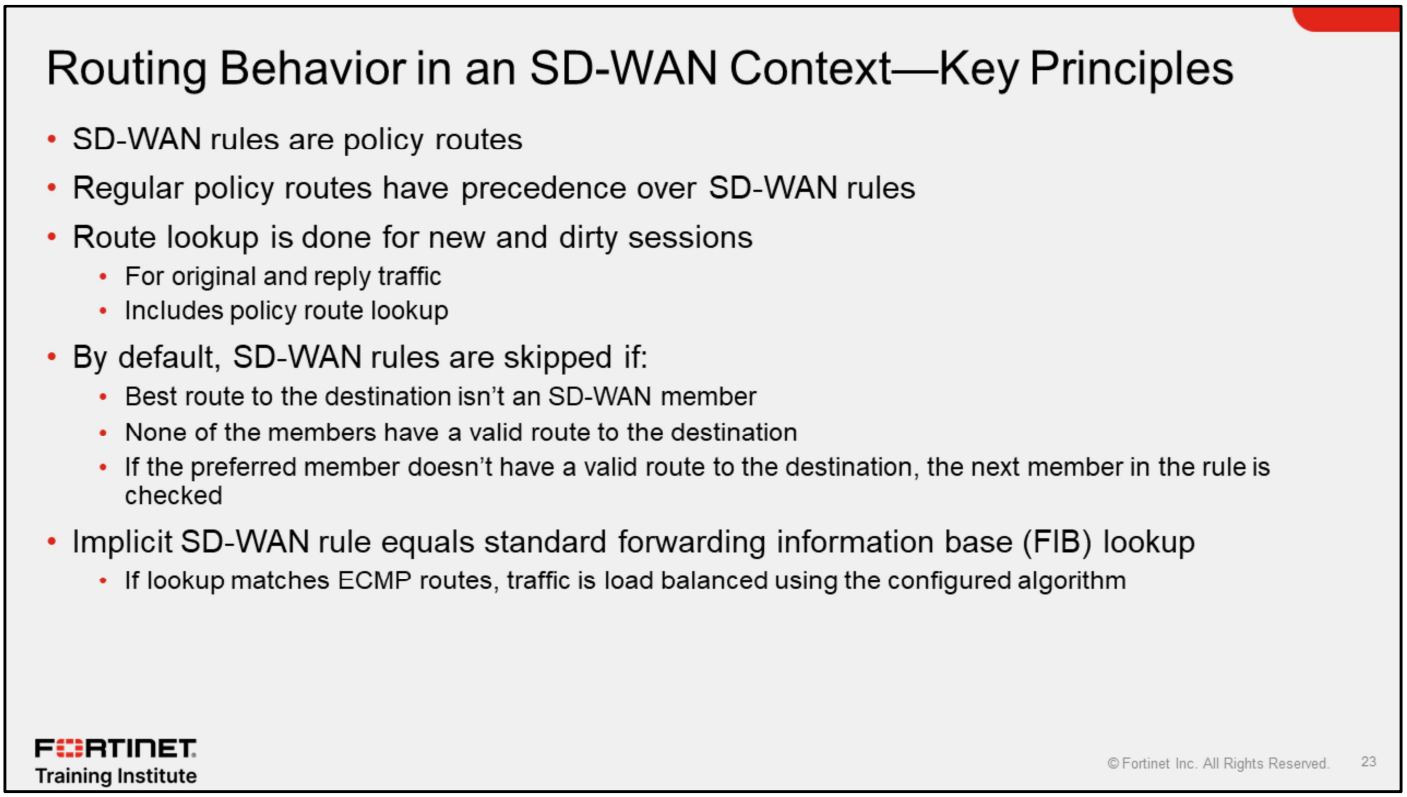


When you configure a static route, you can reference one or more zones as the outgoing interface. As a result, FortiOS installs a static route in the routing table for every member configured in the zone. Because the static routes share the same distance, they become ECMP routes. FortiOS uses the gateway defined for each zone member.

Alternatively, you can configure per-member static routes for more granular control over traffic. However, unlike static routes for zones, which retrieve the member gateway from the member configuration, with per-member static routes, you must specify a gateway if the interface type requires it.

When you create a static route for a zone, FortiOS assigns the routes with a distance of `1` by default. FortiOS assigns such a low distance by default because administrators usually want their SD-WAN routes to have preference over other routes in the FIB. However, you can change the distance to a different value if required. Static routes for individual members have default distance of `10`.

In the example shown on this slide, `port1` and `port2` are members of the `underlay` zone. The administrator created a default static route that references this zone. The result is that the routing table displays ECMP routes for each member of the zone. In addition, the administrator created a per-member static route for 8.8.8.8 through port1. All three routes can then be used by SD-WAN rules to route traffic, or by the FIB to route traffic when no rule is matched.



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

- SD-WAN rules are policy routes. Like regular policy routes, SD-WAN rules route traffic based on multiple criteria. That is, when you configure an SD-WAN rule, the kernel installs a corresponding policy route that reflects the source, destination, service, and outgoing interfaces configured in the SD-WAN rule.

- Regular policy routes have precedence over SD-WAN rules. Therefore, if you configure regular policy routes, you should ensure that their matching criteria is as narrow as possible. Otherwise, traffic that is intended to be handled by SD-WAN could end up being handled by regular policy routes instead.

- FortiGate performs route lookup on both new and dirty sessions. A dirty session is a session that must be re-evaluated by the kernel after it is impacted by a routing, firewall policy, or interface change. FortiGate performs route lookups for both original and reply traffic. During route lookup, FortiGate also checks policy routes.

- By default, FortiGate skips SD-WAN rules if the best route to the destination isn't an SD-WAN member. If the best route matches an SD-WAN member, then the selected member in the rule must have a valid route to the destination, otherwise FortiGate skips the member, and checks the next best member. If none of the members have a valid route to the destination, then FortiGate skips the rule.

- The implicit SD-WAN rule equals standard FIB lookup. That is, if the traffic doesn't match any of the SD-WAN rules, then FortiGate routes the traffic using the regular process, which consists of looking for the best route in the FIB. If the best route matches equal cost multipath (ECMP) routes—usually the case—then FortiGate load balances the traffic using the configured load balancing algorithm.

Verify SD-WAN Traffic Routing

- Use the **Forward Traffic** logs or the packet capture tool to verify traffic routing

Log & Report > Forward Traffic

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

SD-WAN rule match
Empty for **Implicit** rule

```
# diagnose sniffer packet any 'tcp[13]&2==2 and port 443' 4
5.455914 port1 out 192.168.1.254.59785 -> 192.168.1.11.443: syn 457459
5.455930 port2 out 192.168.1.11.443 -> 192.168.1.254.59785: syn 163440 ack 457460
5.455979 port2 out 192.168.1.32.49573 -> 192.168.1.25.443 : syn 927943
5.456043 port1 out 192.168.1.21.54711 -> 192.168.1.114.443: syn 930863
```

Use verbosity level 4 to 6 to see egress interface

FORTINET Training Institute

To verify SD-WAN traffic routing, for logged flows, you can use the forward traffic logs. You can use the **Destination Interface** column in the **Forward Traffic** logs to verify that traffic is egressing the SD-WAN member interfaces. The column SD-WAN Rule Name indicates the name of the SD-WAN rule that applies. No name in this column means that the flow was routed according to the default **Implicit** SD-WAN rule.

Alternatively, you can use verbosity levels `4` to `6` to view the egress interface using the CLI packet capture tool.

The example on this slide shows a capture with a filter that matches any packets with the `SYN` flag on and port 443. So, the sniffer output shows all `SYN` packets to port `443` (HTTPS).

Check Policy Routes Created by SD-WAN Rules

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

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

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

id=2113929223 static_route=7 dscp_tag=0xff 0xff flags=0x0 tos=0x00
tos_mask=0x00 protocol=0 sport=0-0 iif=0 dport=1-65535 path(1)
oif=3(port1) gwy=192.2.0.2
source wildcard(1): 0.0.0.0/0.0.0.0
destination wildcard(1): 0.0.0.0/0.0.0.0
internet service(1): Fortinet-FortiGuard(1245324,0,0,0)
hit_count=0 last_used=2023-08-14 06:39:07

id=2130903041(0x7f030001) vwl_service=1(Critical-DIA)
vwl_mbr_seq=1 2 dscp_tag=0xff 0xff flags=0x0 tos=0x00
tos_mask=0x00 protocol=0 sport=0-65535 iif=0 dport=1-65535 path(2)
oif=3(port1) oif=4(port2)
source(1): 10.0.1.0-10.0.1.255
destination wildcard(1): 0.0.0.0/0.0.0.0
internet service(3): GoToMeeting(4294836
Microsoft.Office.365.Portal(4294837474,0,0,0, 41468)
Salesforce(4294837976,0,0,0, 16920)
hit_count=0 last_used=2023-08-14 05:46:43
```

This is a regular policy route (ID ≤ 65535)

This is an ISDB route (ID > 65535 and no `vwl_service` field)

This is an SD-WAN rule (ID > 65535 and the `vwl_service` field is present)

FORTINET Training Institute

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

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

- Regular policy routes are assigned an ID no higher than 65535. In the output shown on this slide, the first entry is assigned ID 1, which makes it a regular policy route.

- ISDB routes and SD-WAN rules are assigned an ID higher than 65535. However, SD-WAN rule entries include the `vwl_service` field, and ISDB route entries don't. The `vwl_service` field indicates the ID and the name of the rule from the SD-WAN configuration perspective. In the output shown on this slide, the second entry is an ISDB route and the third entry an SD-WAN rule.

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

Policy Route Lookup

- SD-WAN fields in proute list

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

id=2131034113(0x7f050001) vwl_service=1(Critical-DIA) vwl_mbr_seq=1 2 dscp_tag=0xfc despite flags=0x0 tos=0x00
tos_mask=0x00 protocol=0 sport=0-65535 iif=0(any) dport=1-65535 path(2) oif=3(port1) oif=4(port2)
source(1): 10.0.1.0-10.0.1.255
destination wildcard(1): 0.0.0.0/0.0.0.0
internet service(3): GoToMeeting(4294836842,0,0,0,0, 16354) Microsoft.Office.365.Portal(4294837313,0,0,0,0,
41468) Salesforce(4294837785,0,0,0,0, 16920)
hit_count=34219 last_used=2023-08-24 04:04:15

id=2131034115(0x7f050003) vwl_service=3(Corp) vwl_mbr_seq=3 4 dscp_tag=0xfc last used flags=0x0 tos=0x00
tos_mask=0x00 protocol=0 sport=0-65535 iif=0(any) dport=1-65535 path(3) oif=19(T_INET) oif=20(T_MPLS)
source(1): 10.0.1.0-10.0.1.255
destination(1): 10.0.0.0-10.255.255.255
hit_count=13 last_used=2023-08-23 11:31:42
```

SD-WAN rule ID and rule name

SD-WAN members by order of preference

Outgoing interface by order of preference

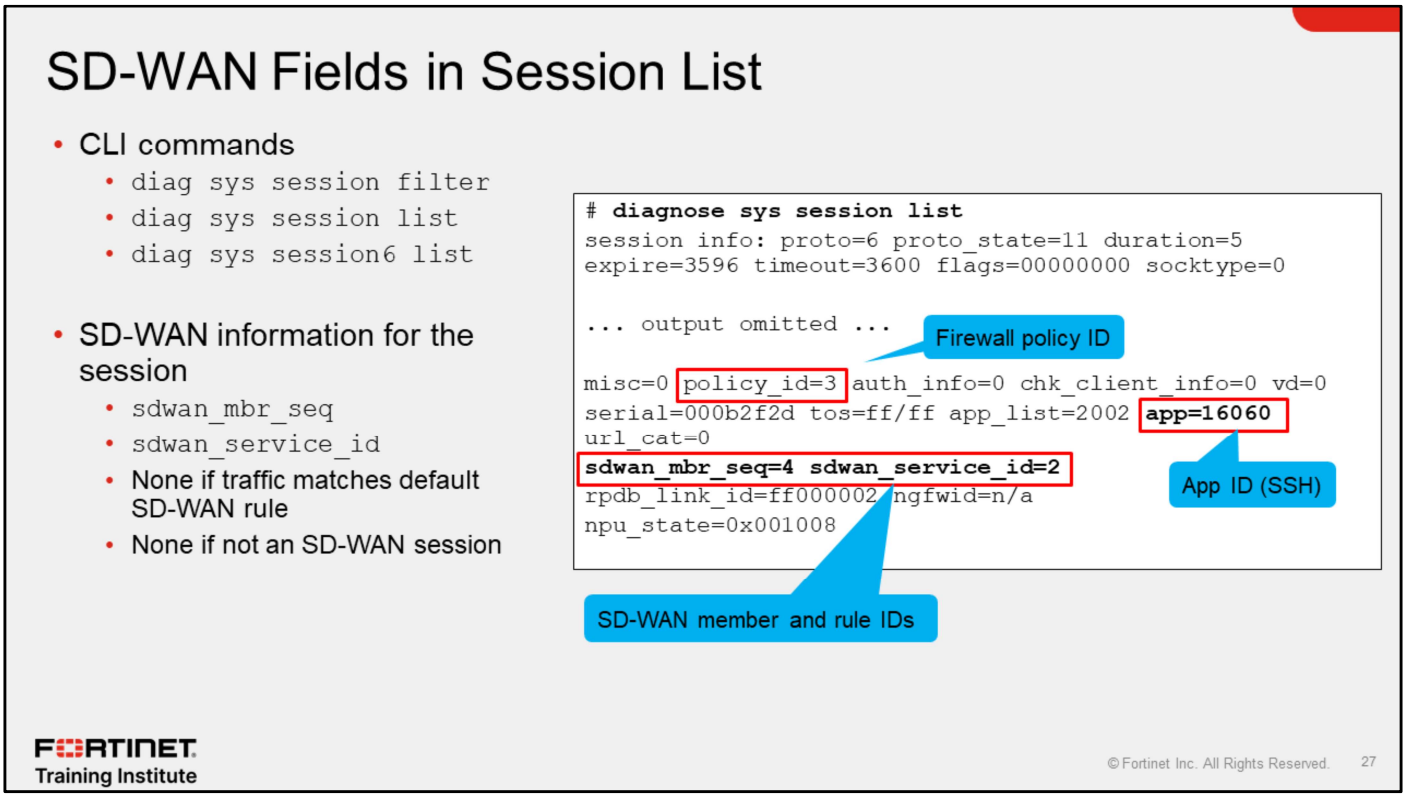
FORTINET Training Institute

This slide shows an example of a policy route list output.

Note the fields `vwl_service` and `vwl_mbr`, which indicate the SD-WAN rule that allowed the route creation and the SD-WAN member used to steer the traffic.

The ID displayed in the `diagnose firewall proute list` command output corresponds to the ID displayed in the debug flow output when a packet matches a rule. The output also includes the outgoing interface list, with the interface preference sorted from left to right.

For troubleshooting purposes, the output of the `diagnose firewall proute list` command also displays the rule hit count and the last time the rule was hit.



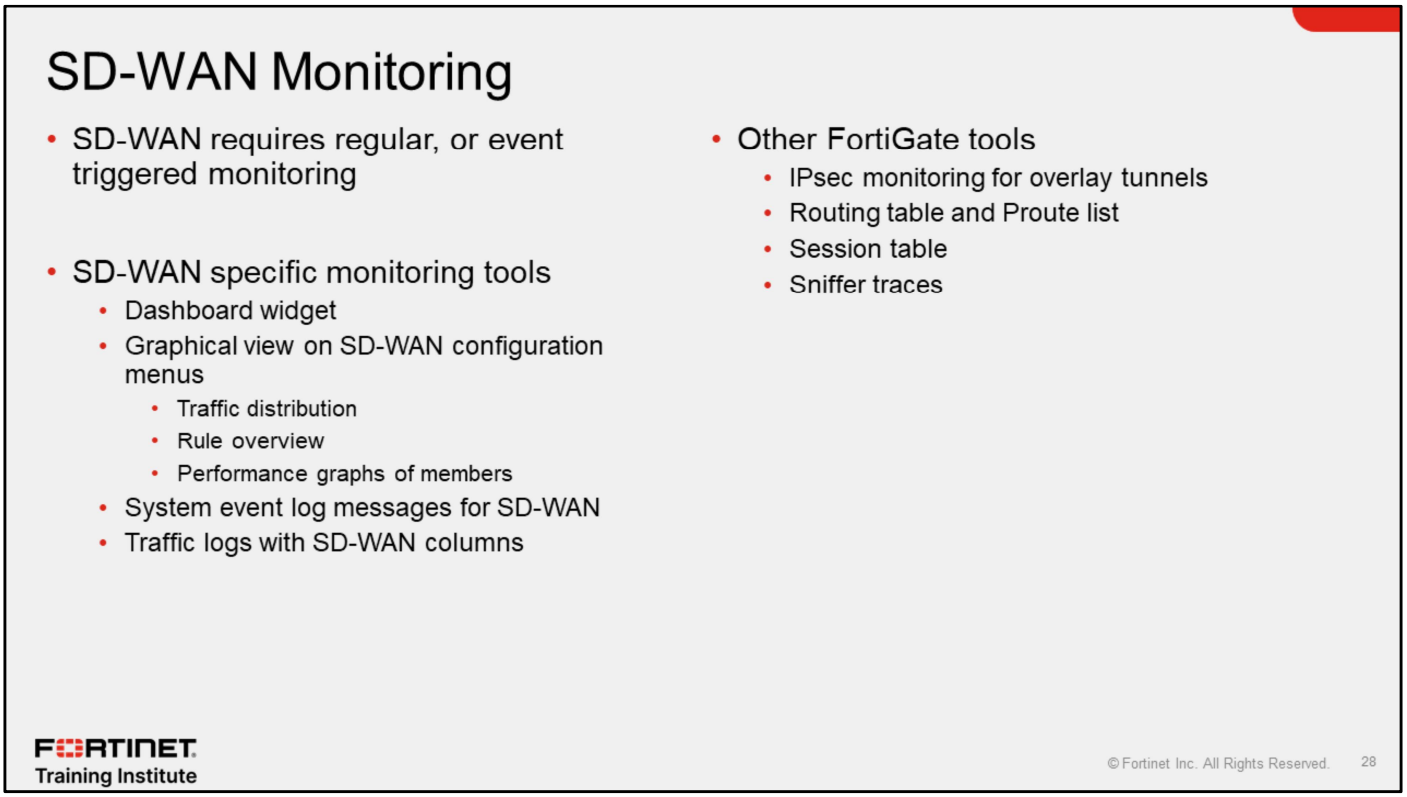
The CLI command `diagnose sys session filter` allows you to filter the sessions to display. Then, use the command `diagnose sys session list` to display the session detail.

You can use `diagnose sys session filter ?` to view available filters, `diagnose sys session filter` to see active filters, and `diagnose sys session filter clear` to reset the filters settings. Use the command `diagnose sys session list` for IPv4 traffic, and `diagnose sys session6 list` for IPv6 traffic.

The right part of this slide shows an example output with detailed information about the session table entry.

Only information related to SD-WAN is highlighted. From left to right, and from top to bottom:

- The ID of the matching policy
- The application ID (used for SD-WAN rules with application criteria)
- The SD-WAN-specific session information. `sdwan_mbr_seq` and `sdwan_service_id` indicate the SD-WAN member ID and the SD-WAN rule ID in use, respectively. If the session matched the SD-WAN implicit rule, and therefore was handled using standard FIB routing, those SD-WAN fields do not appear.

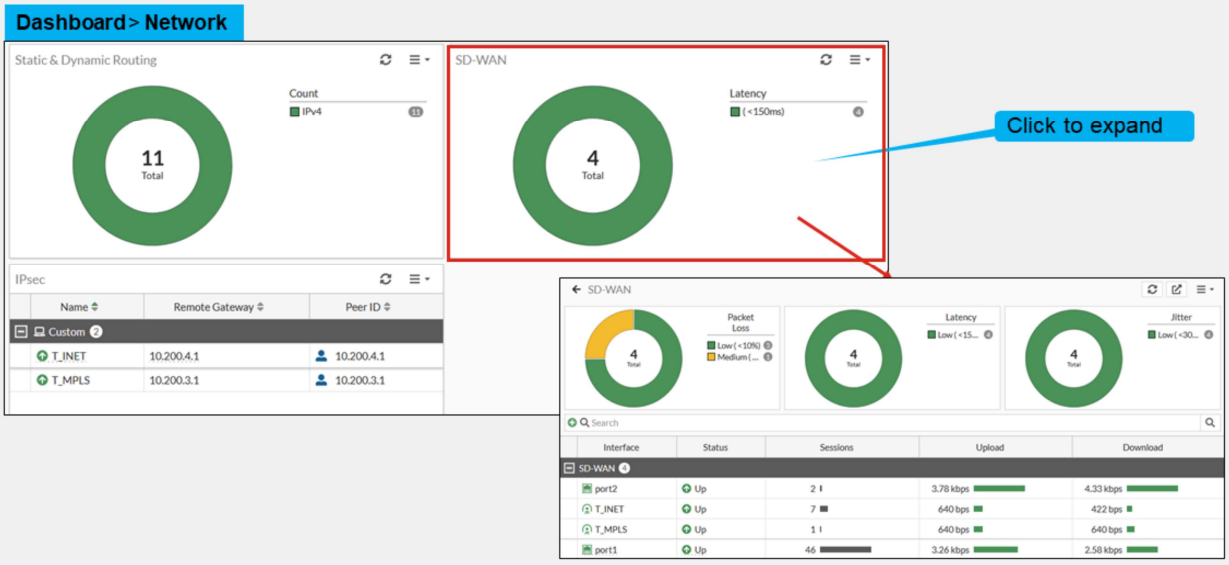


Because of the dynamic nature of SD-WAN routing, you should periodically check the link health, routing behavior, and traffic distribution of your SD-WAN devices. You might want to check that traffic distribution corresponds to expectations with, for instance, only critical traffic steered through the costliest links. On the other hand, when you detect an unexpected event on your network, you want to be able to easily understand the impact on SD-WAN traffic steering and routing decisions.

For those activities, you can count on some general FortiGate monitoring tools you already know, like the routing table, the session table or the embedded packet capture tool. You can also benefit from dedicated SD-WAN monitoring tools provided by the FortiGate GUI interface. Through the next few slides, you will discover the SD-WAN monitoring tools provided by the FortiGate GUI.

Dashboard—Network

- Network dashboard pane with SD-WAN, routing, and IPsec widgets



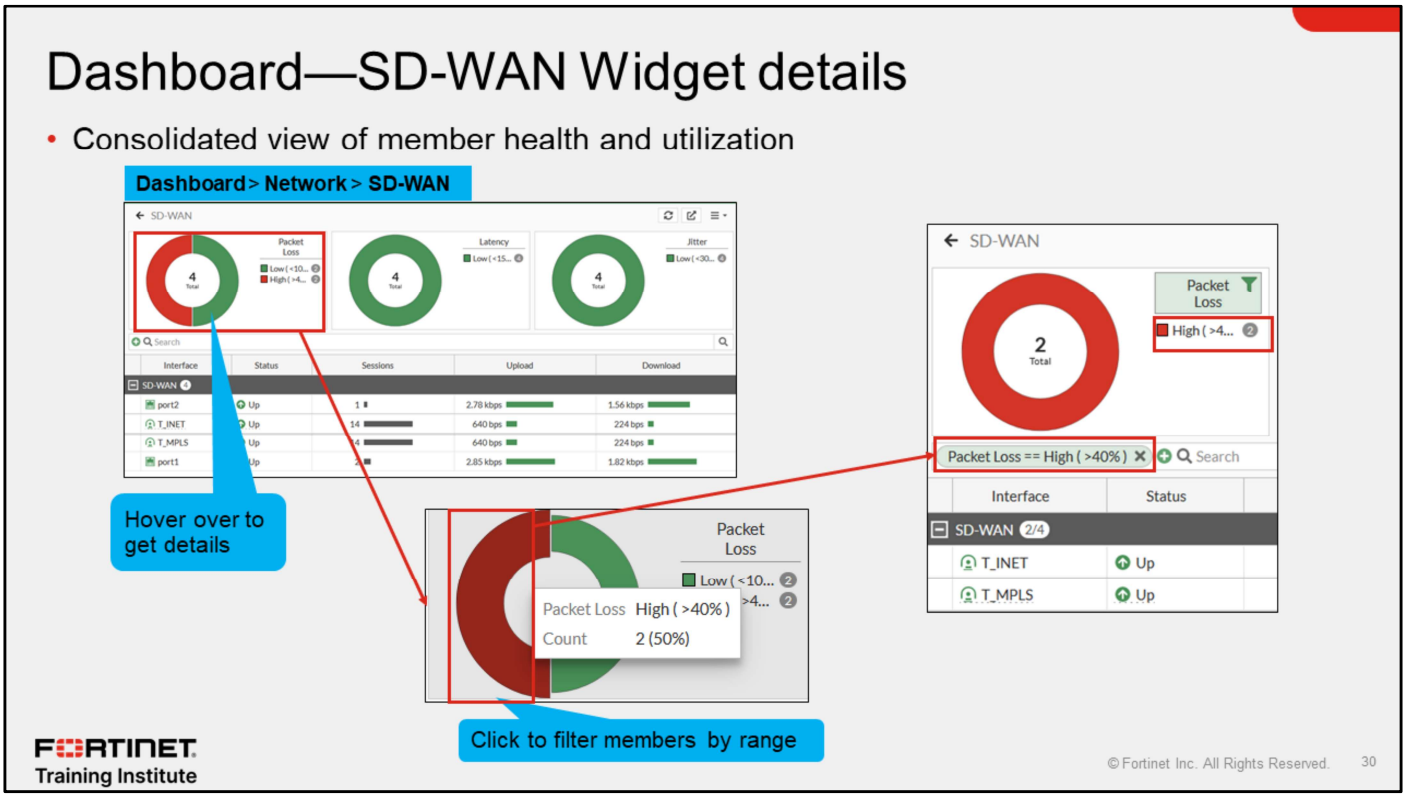
FORTINET Training Institute

By default, the **Network** dashboard includes three widgets useful for SD-WAN monitoring. It should be the first place you look when you want to check the SD-WAN behavior on a FortiGate device.

From this page you can view:
- Static and dynamic routing
- IPsec tunnels status
- SD-WAN interfaces performances

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

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

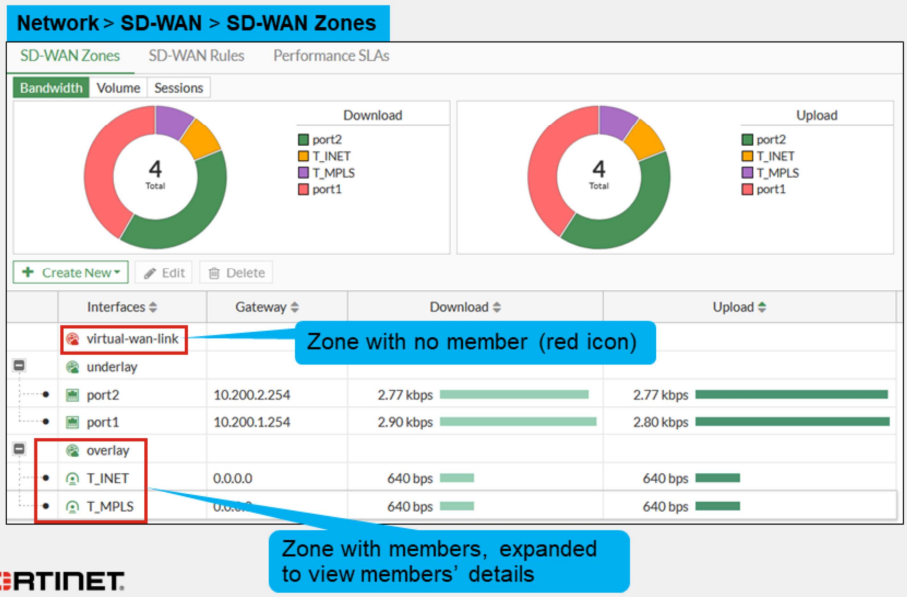


From the SD-WAN widget detailed view, you can hover over the graph to view details. You can also click a graph part to filter the member list and display only the members that match the selected criteria.

In the example shown on this slide, two members have a high rate of packet loss—above 40%. This is displayed on the diagram as the red part of the circle. When you click this red part of the circle, FortiGate filters the member list to display only members with a high rate of packet loss—for this example, T_INET and T_MPLS.

SD-WAN Interfaces and Zones Summary

- Synthetic view of zones and members configuration and status

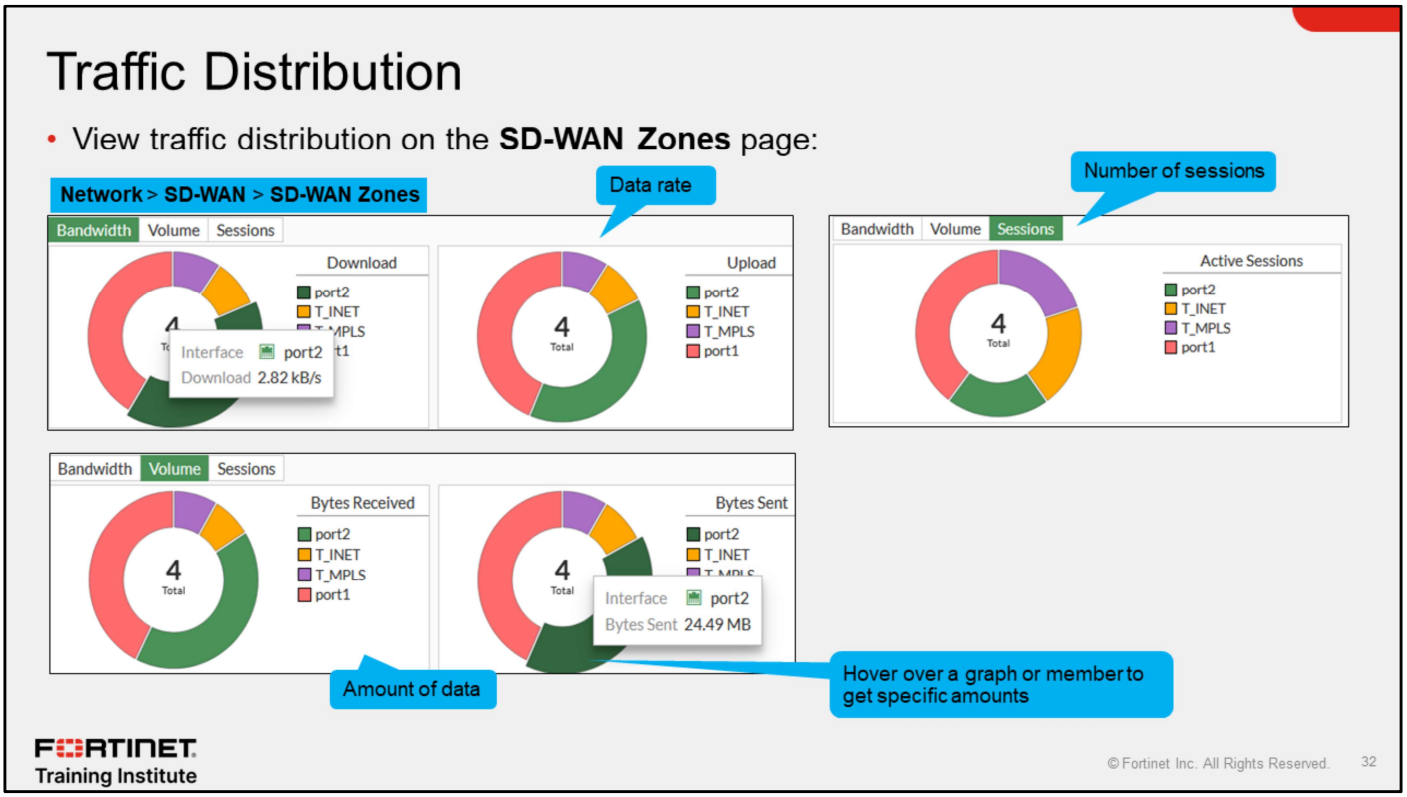


FORTINET Training Institute

The **SD-WAN Zones** page in the menu **Network** > **SD-WAN**, provides a synthetic view of the SD-WAN zones and members configuration. Note that zones with no member appear with a red icon. Next to zones with members is a + sign that you can click to display the members.

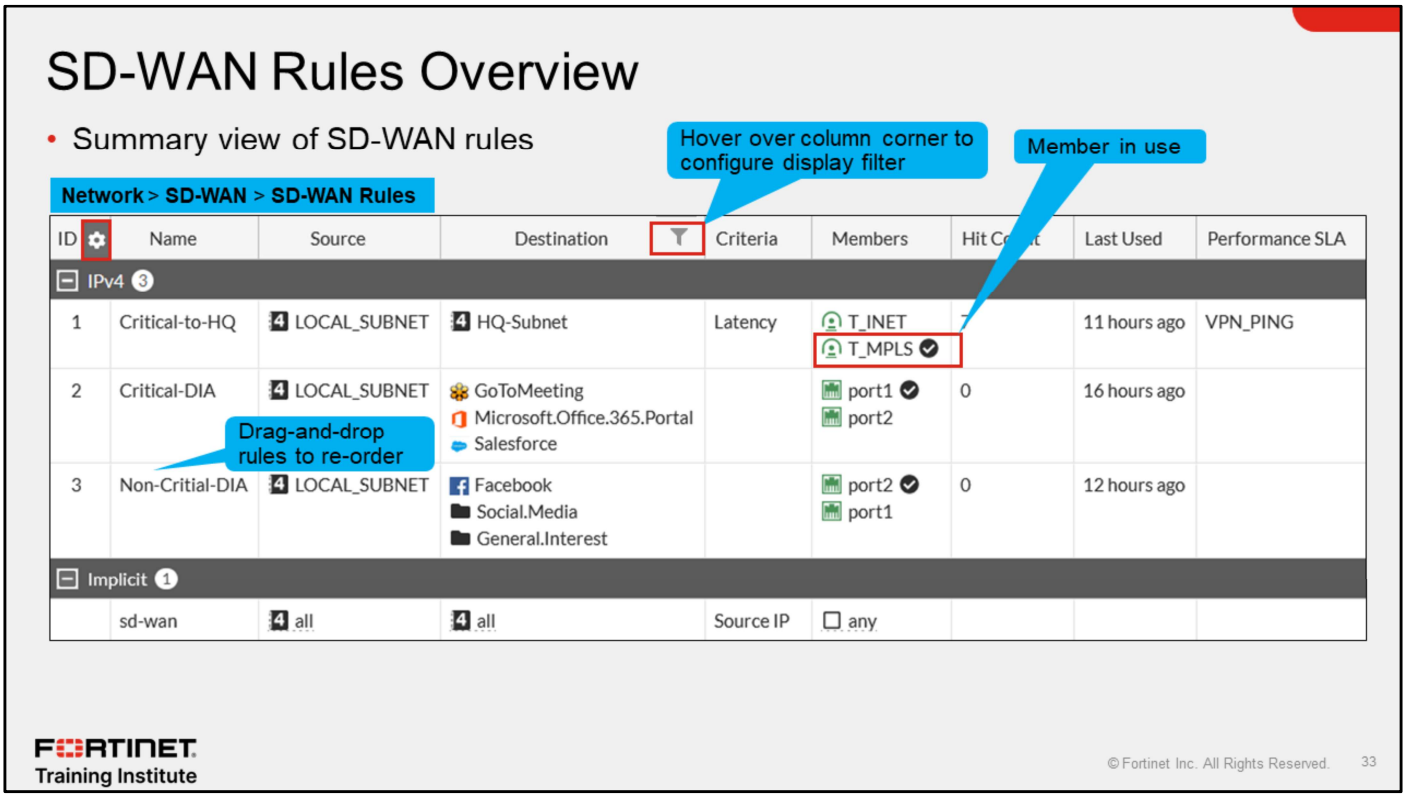
The diagram at the top of the page displays traffic allocation per interface, evaluated by bandwidth use, volume, or number of sessions.

From this menu, you can double-click zone or interface lines to adjust their configurations.



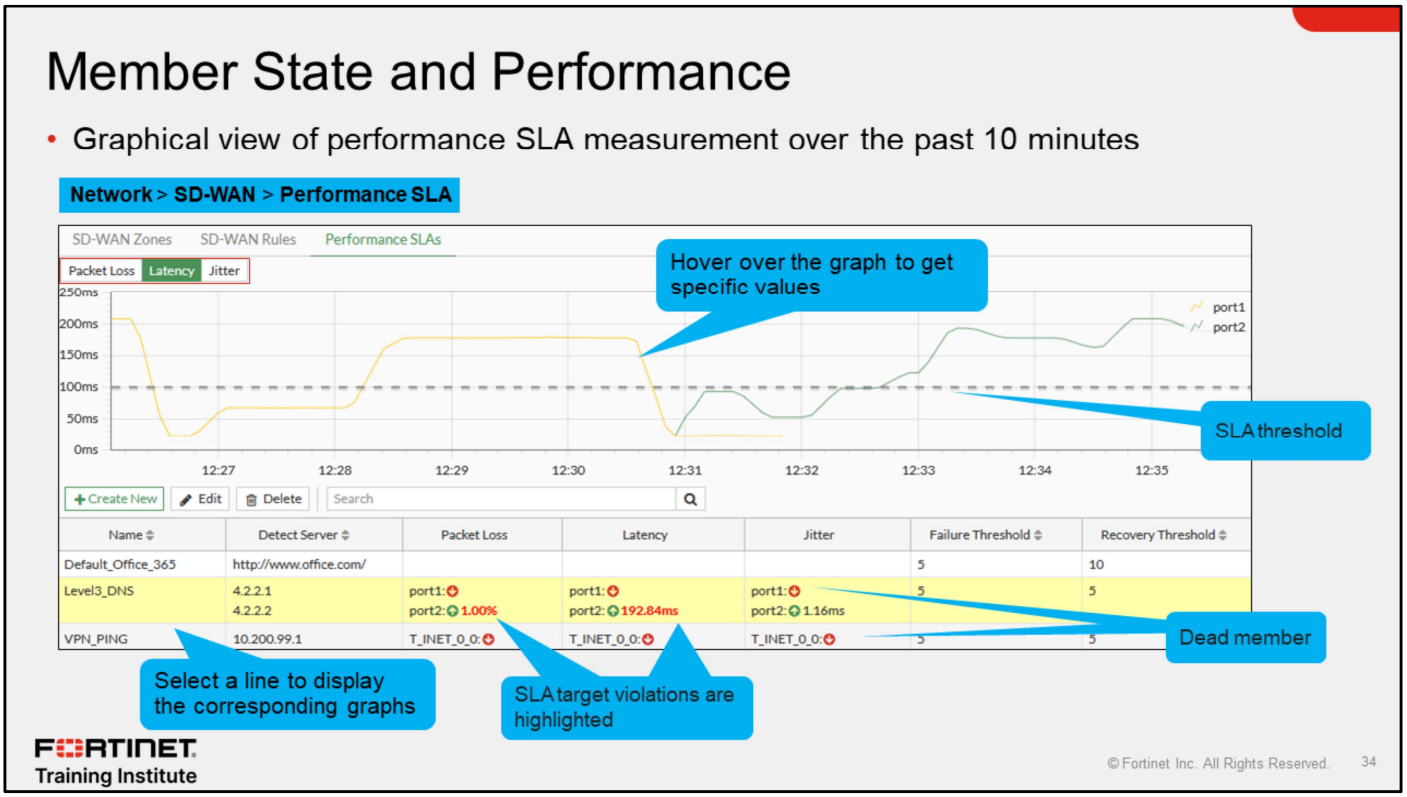
From the SD-WAN zone page presented on the previous slide, you can monitor the traffic distribution over the SD-WAN members. The page contains graphs that display traffic distribution based on bandwidth, volume, or sessions. Note that bandwidth refers to the data rate, while volume refers to the amount of data.

You can also hover over a member or the graph to get a specific amount of bandwidth, volume, or sessions.



The **SD-WAN Rules** page in the menu **Network** > **SD-WAN**, provides a summary view of SD-WAN rules configuration. From this list you can quickly view the main configuration parameters of a rule, members in use, and the last time the rule was used to steer traffic. With drag-and-drop you can re-order the rules. You can also double-click any user-defined rule to adjust its configuration.

If you want to adjust the view, you can reorder the column with drag-and-drop, add or remove columns with the parameter menu on the left side of the top bar. You can also filter on any column to adjust the display to what you are looking for. Hover over the columns corner to view the filter configuration icon.



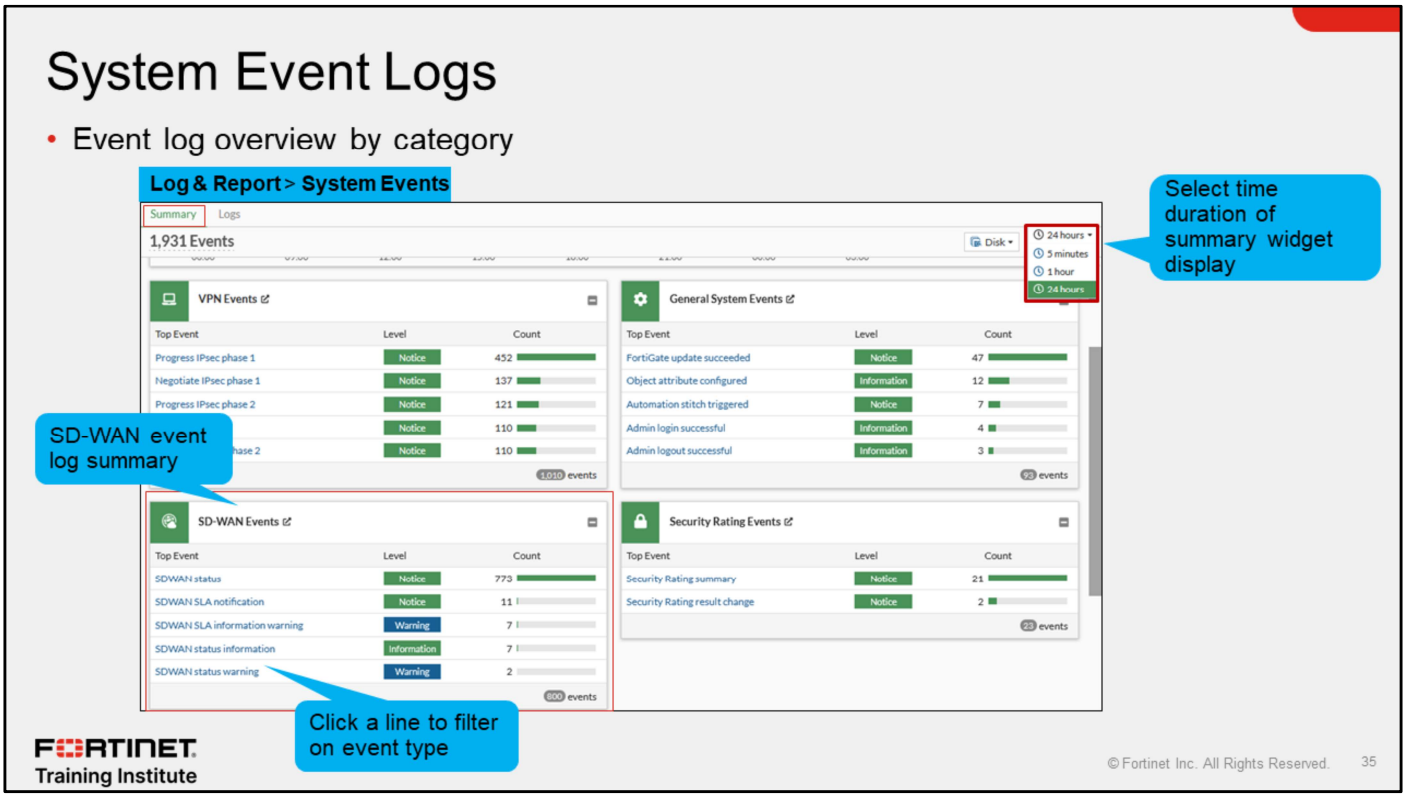
You can browse to the **Performance SLAs** page to monitor the health of your members. You first select the performance SLA you want to check (Level3_DNS in the example). The graphs on the page will then display the packet loss, latency, and jitter of each member using the selected performance SLA. Note that the information shown on the graphs is limited to the last 10 minutes.

If you configured an SLA target, it appears on the graph as a horizontal dotted line. You can quickly detect the member status. The FortiGate GUI shows alive members with a green up arrow icon, and dead members with a red down arrow icon. For a missed SLA target, FortiGate highlights the impacted metric in red. It is important to note that the green up arrows indicate only that the server is responding to the health check, regardless of the packet loss, latency, and jitter values. It is not an indication that any of the SLAs are being met.

You can display graphs for **Packet Loss**, **Latency**, or **Jitter** by selecting the upper tabs. You can also hover over the graph to get a specific amount of packet loss, latency, or jitter. Because link quality plays an important role in link selection when using SD-WAN, monitoring the link quality status of the SD-WAN member interfaces is a good practice. You should investigate any prolonged issues with packet loss, latency, or jitter to ensure your network traffic does not experience outages or degraded performance.

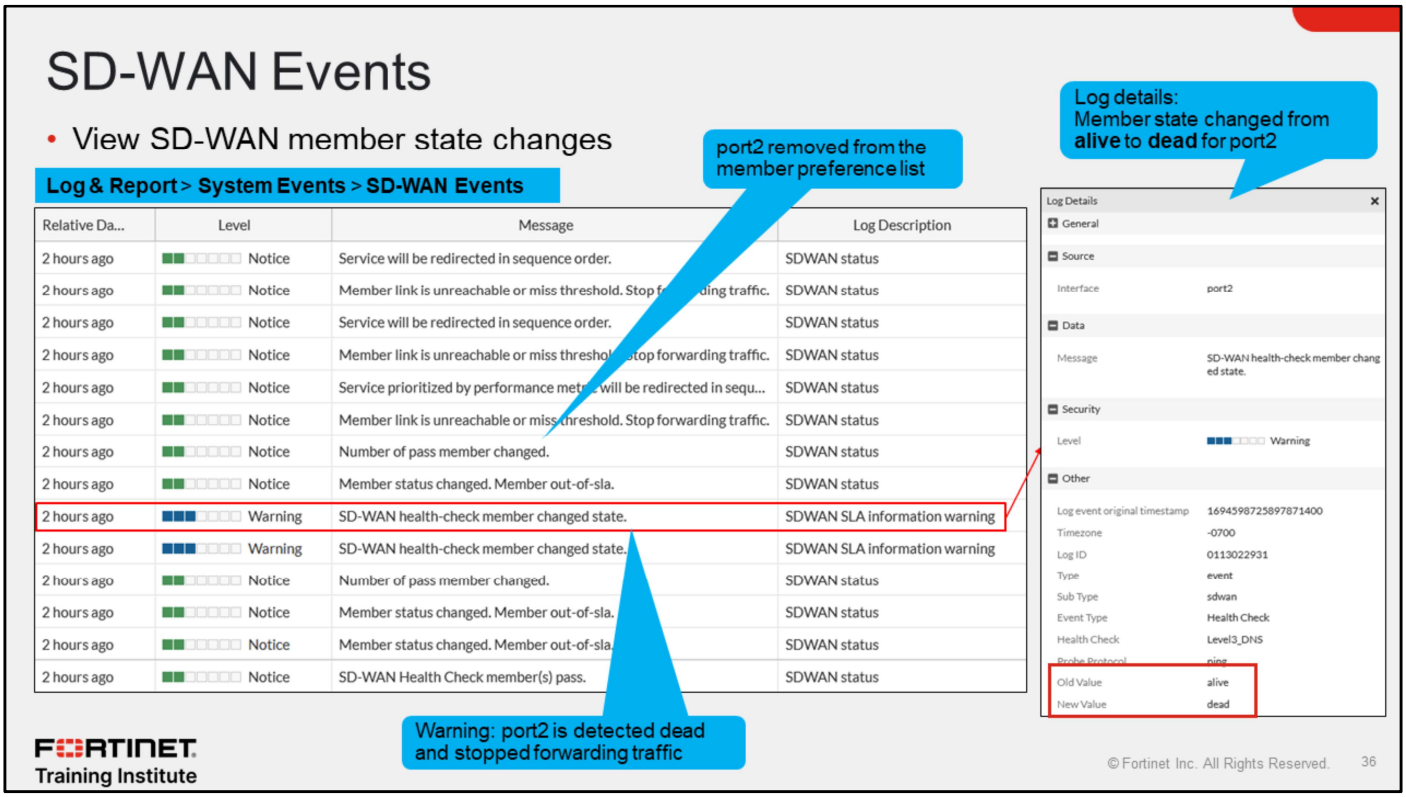
In the example shown on this slide, the **Level3_DNS** performance SLA is selected and reports that **port2** is alive and **port1** is dead. The graph shows latency for both monitored interfaces over the past 10 minutes.

From this page you can also update a performance SLA configuration, or create a new one.



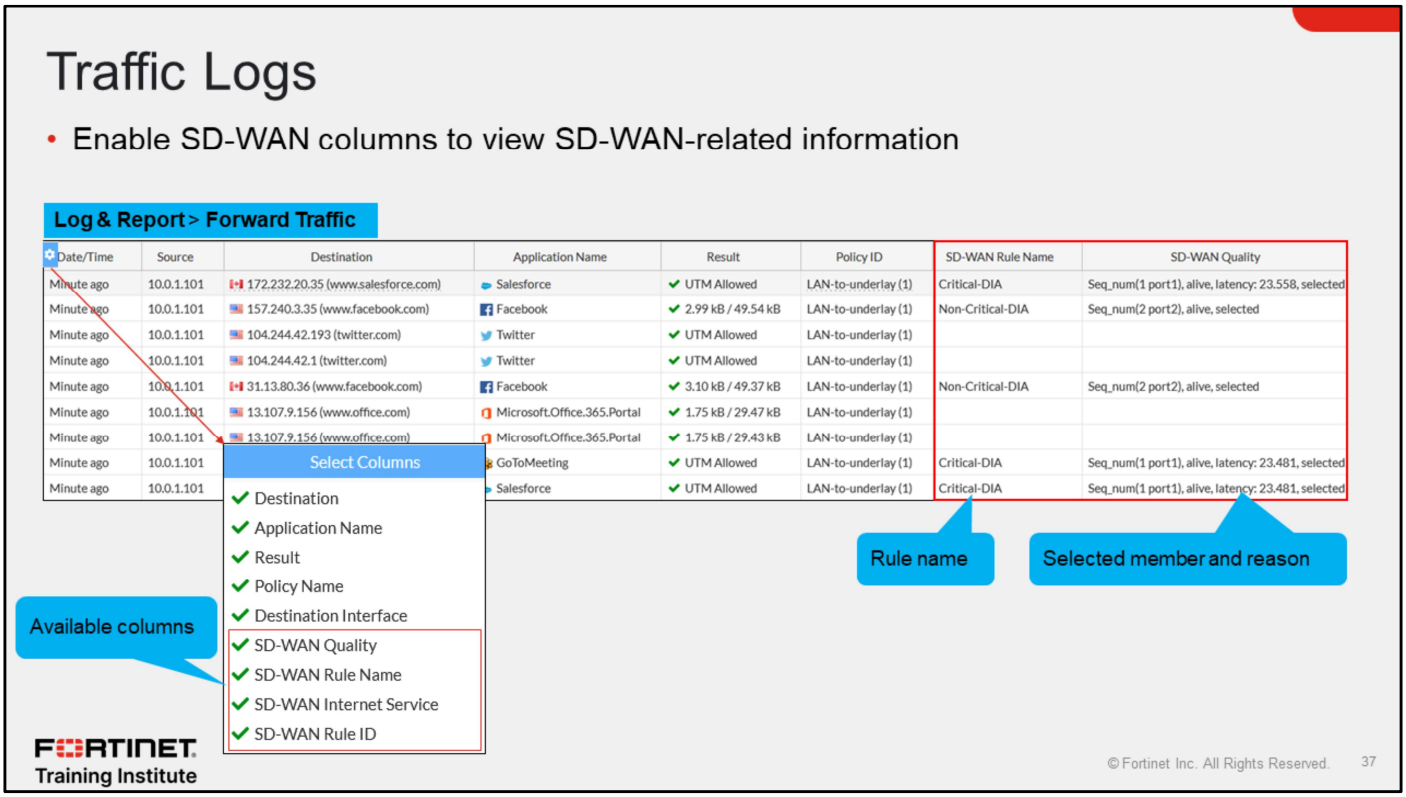
From the **System Events** log summary menu, you get an overview of recent events ordered by category and message type. By default, the summary page considers logs received over the past 5 minutes. You can adjust to get a summary over the past 1 hour or past 24 hours. In the **SD-WAN Events** summary widget, you will log events about SLA status changes, priority member order changes, and so on. The **VPN Events** widget provides useful information to understand overlay links behavior.

Click the widget title to view the corresponding logs in detail. Click an event name to view the logs filtered by event name.



The **SD-WAN Events** subsection on the **Events** page displays logs that report the state changes of the SD-WAN members.

In most cases, you want to click a log to fully understand the event. For example, the warning log message highlighted in the table indicates that the state of **port2** changed from **alive** to **dead**. Although the details above this one are not shown, the logs report that port2 stopped forwarding traffic, and that the member preference in the rule that uses port2 was updated to remove port2.



The **Forward Traffic** logs page is useful to identify how sessions are distributed in SD-WAN and the reason. Make sure to enable the **SD-WAN Rule Name** and **SD-WAN Quality** columns, which are disabled by default. The former indicates the matched SD-WAN rule for a session, and the latter the member the session was steered to and the reason.

Note that the **Implicit** SD-WAN rule name does not appear in the **SD-WAN Rule Name** column. When the traffic is steered according to this rule the field remains empty.

The table on this slide shows multiple sessions. The first session in the table was identified as a **Salesforce** application, matched the **Critical-DIA** rule, and was sent to port1. The reason that port1 was selected was because it had the lowest latency.

The second session in the table, which was identified as a **Facebook** application, matched the **Non-Critical-DIA** rule, and was sent to port2. The **Non-Critical-DIA** rule instructs FortiGate to steer matching traffic to port2 only, provided the port is alive. This behavior matches the reason described in the **SD-WAN Quality** column for that session.

Knowledge Check

1. Which item is defined in an SD-WAN rule?

✓ A. SLA criteria
B. Security profile
C. Logging options

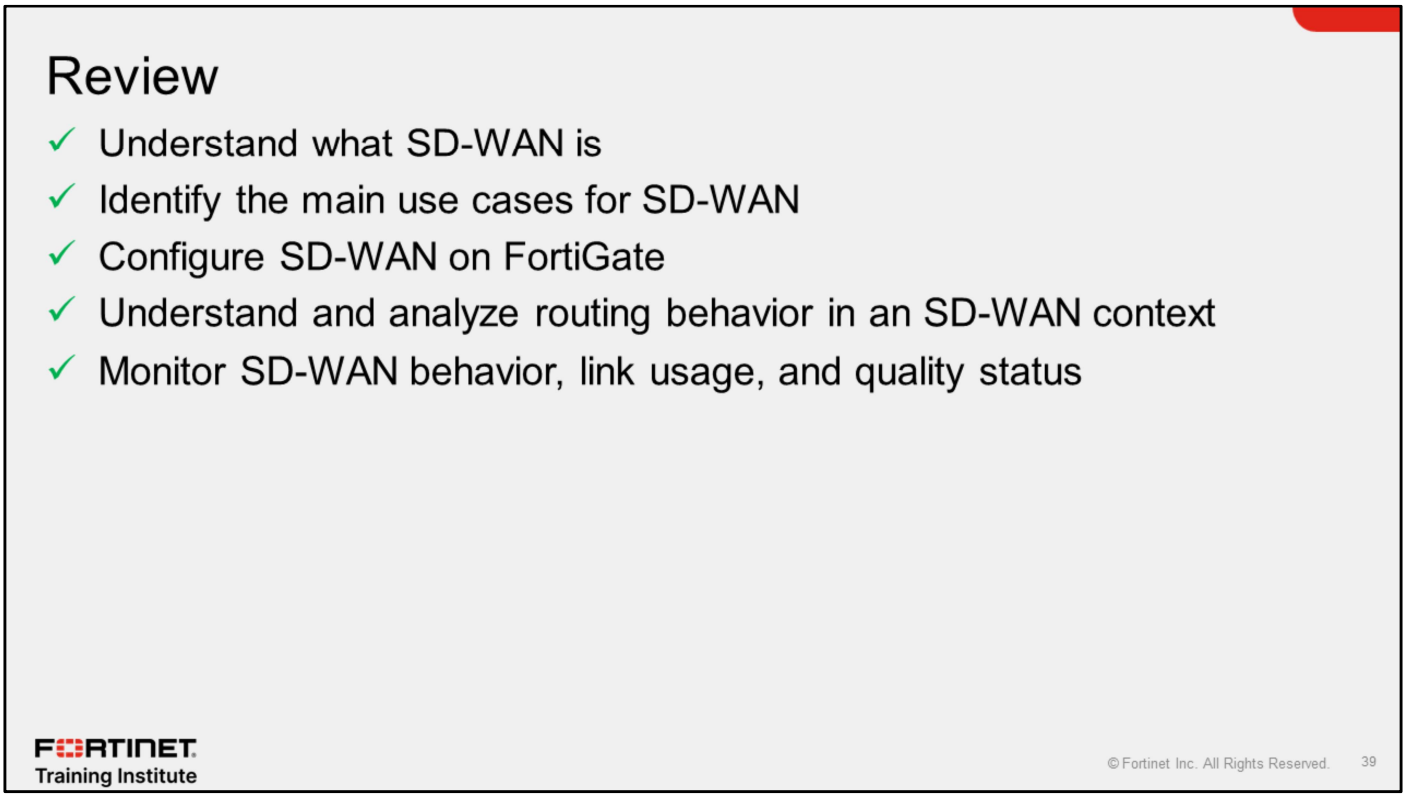
2. What is the routing behavior in an SD-WAN context?

A. Static routes apply first.
✓ B. Regular policy routes apply first.
C. SD-WAN policy routes apply first.

3. Which menu will you use to review the history of SD-WAN events?

A. Forward Traffic in Log & Report
B. SD-WAN widget on the Dashboard
✓ C. SD-WAN widget in System Events

FORTINET Training Institute



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

By mastering the objectives covered in this lesson, you learned how to configure, maintain, and monitor a FortiGate SD-WAN solution.