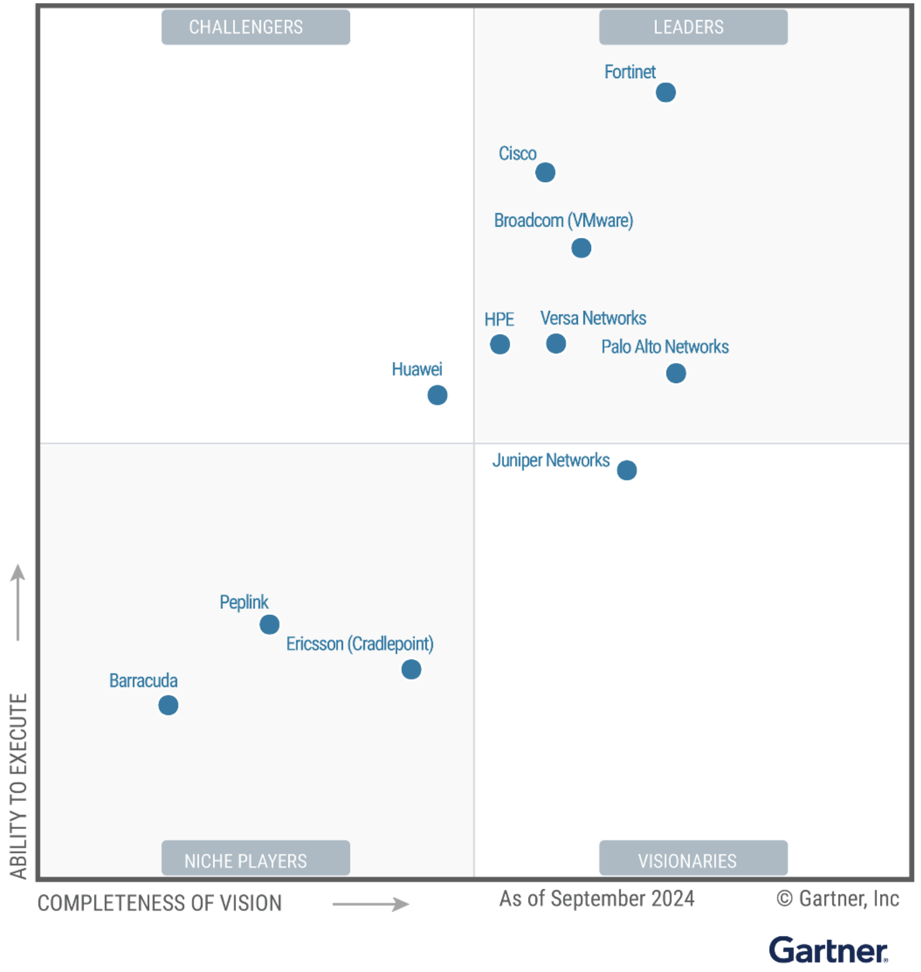
FORTINET®

March SUNY Office Hours

SD-WAN Local Internet Breakout

Fortinet Recognized as a Leader in the 2024 Gartner® Magic Quadrant™ for SD-WAN

Figure 1: Magic Quadrant for SD-WAN



5x a Leader.

4x Highest Ability to Execute.

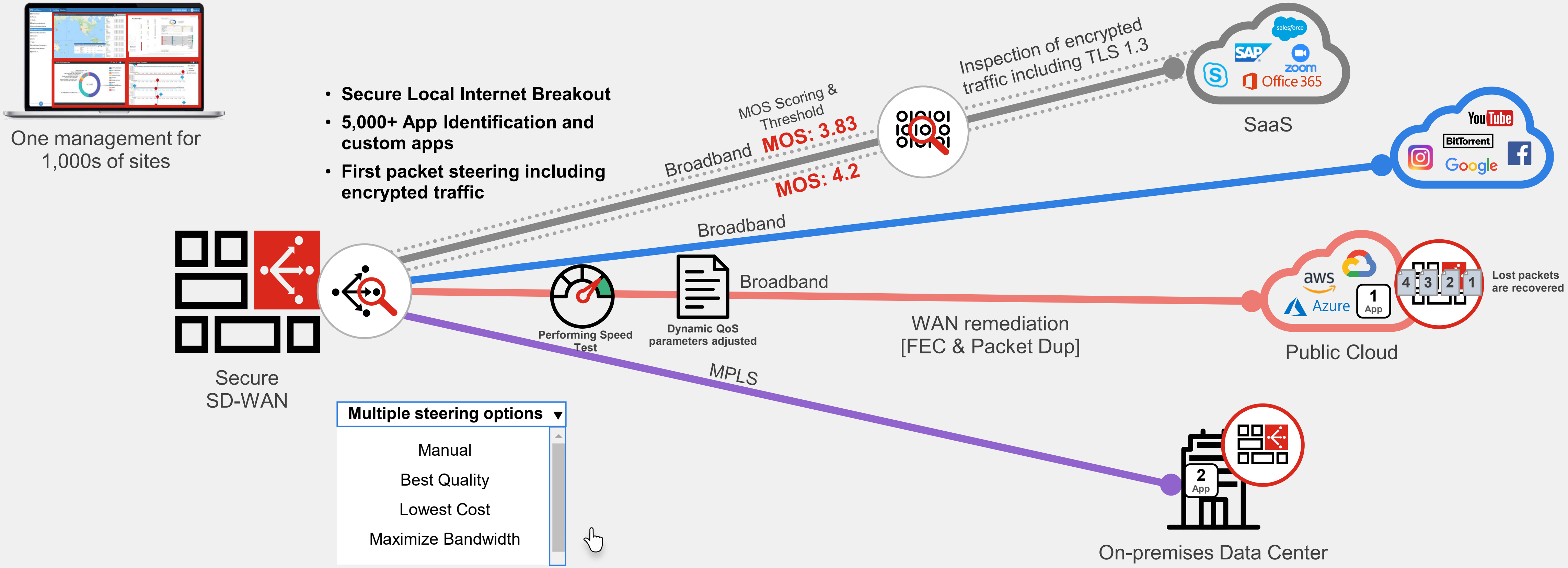
Only Leader to Have Received the Highest Placement in the Ability to Execute for Four Consecutive Years.

Gartner, Magic Quadrant for SD-WAN, Jonathan Forest, Karen Brown, Nauman Raja, 30 September 2024

GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally, and MAGIC QUADRANT is a registered trademark of Gartner, Inc. and/or its affiliates and are used herein with permission. All rights reserved. Gartner does not endorse any vendor, product or service depicted in its research publications and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's Research & Advisory organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose. This graphic was published by Gartner, Inc. as part of a larger research document and should be evaluated in the context of the entire document. The Gartner document is available upon request from Fortinet at https://global.fortinet.com/lp-en-ap-2023-sase-mq

Enabling Application Resilient Networks, No Matter of Location

Enhance user experience and business productivity

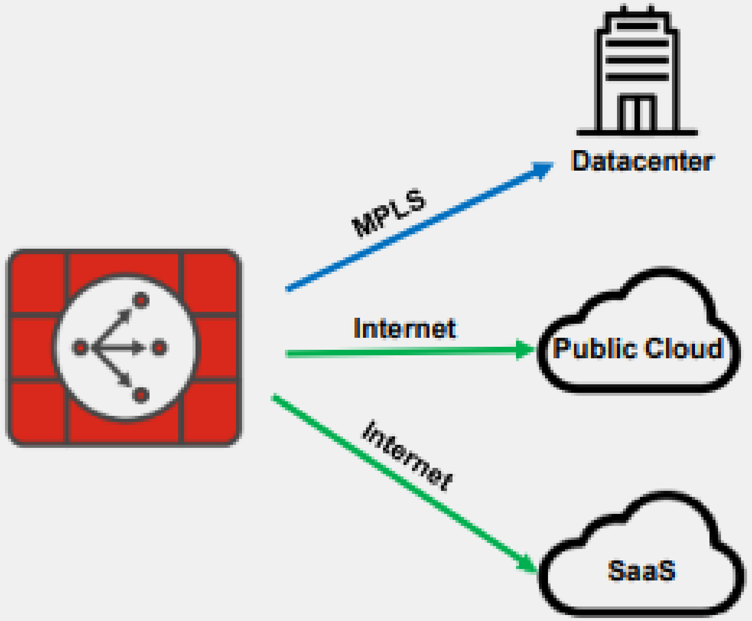


- **Secure Local Internet Breakout**
- **5,000+ App Identification and custom apps**
- **First packet steering including encrypted traffic**

Intelligent Steering	Reliable Accuracy	Continuous Learning	Self-healing
Traffic Agnostic	Including encrypted traffic	Broadest support 5k+ apps	Realtime Optimization

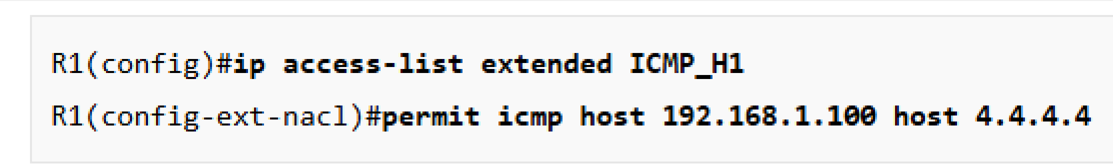
How does Fortinet Define SD-WAN

- Intelligent application/traffic steering based on link performance
- Local Internet Breakout
- Site-to-Site Connectivity
    - IPsec
    - ADVPN

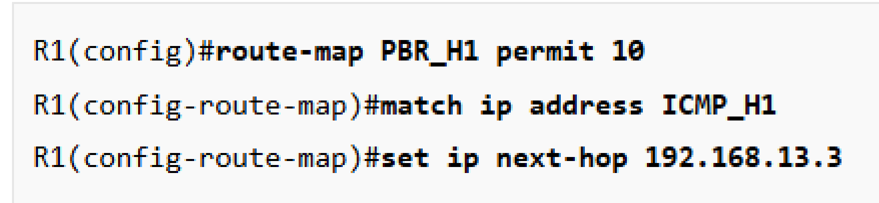


What is Policy Routing?

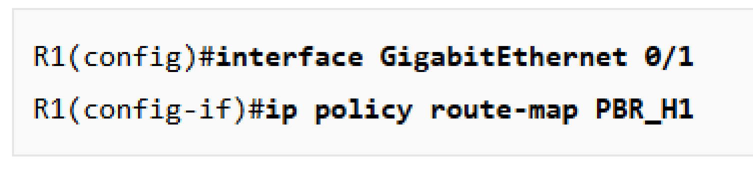
- Route by admin defined policy – not routing table best match
- Select traffic and manually send to desired interface



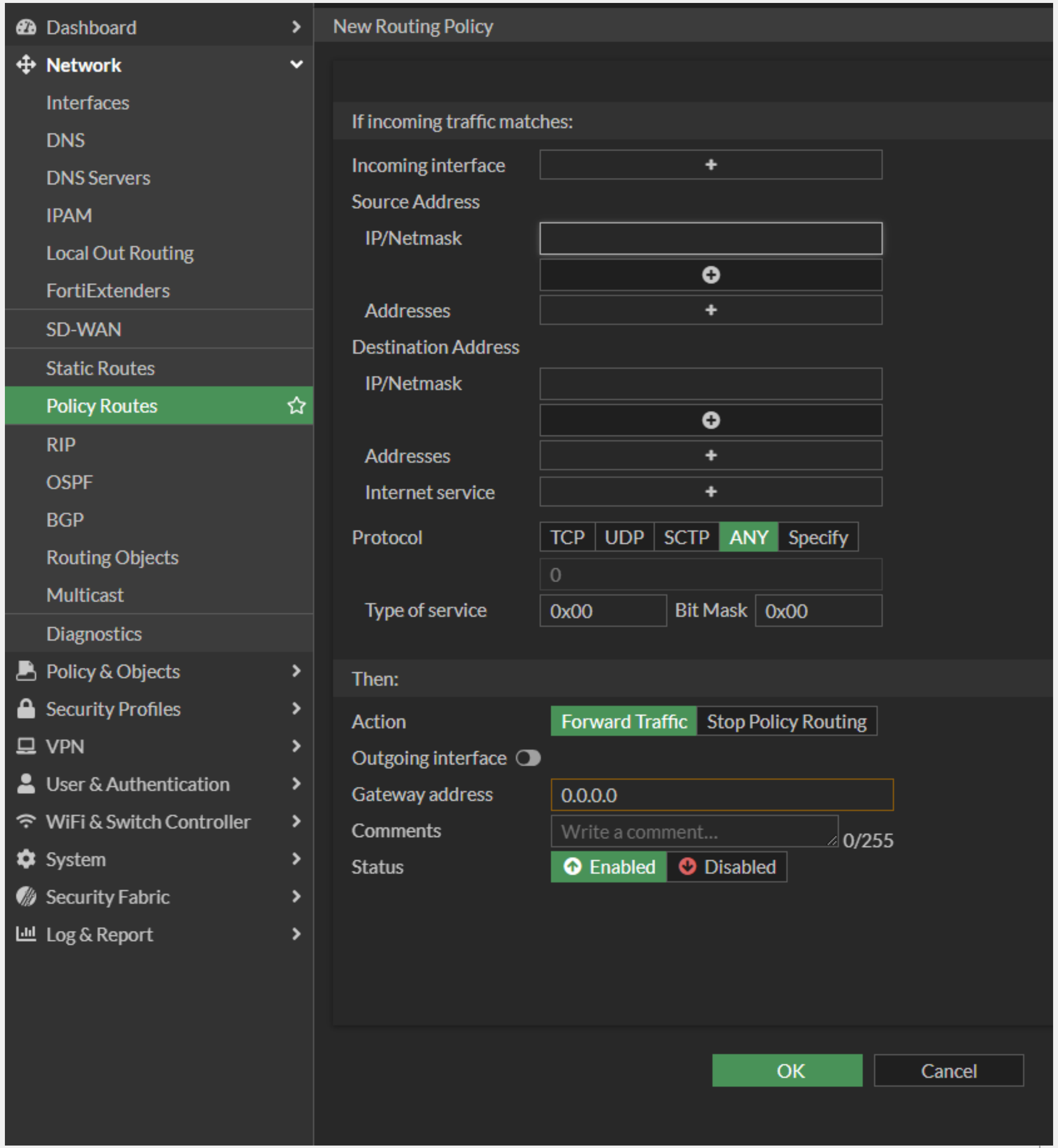
```
R1(config)#ip access-list extended ICMP_H1
R1(config-ext-nacl)#permit icmp host 192.168.1.100 host 4.4.4.4
```



```
R1(config)#route-map PBR_H1 permit 10
R1(config-route-map)#match ip address ICMP_H1
R1(config-route-map)#set ip next-hop 192.168.13.3
```



```
R1(config)#interface GigabitEthernet 0/1
R1(config-if)#ip policy route-map PBR_H1
```



New Routing Policy

If incoming traffic matches:

Incoming interface: +

Source Address

IP/Netmask:

Addresses: +

Destination Address

IP/Netmask:

Addresses: +

Internet service: +

Protocol: TCP | UDP | SCTP | [✓ ANY] | Specify

0

Type of service: 0x00 Bit Mask 0x00

Then:

Action: [✓ Forward Traffic] | Stop Policy Routing

Outgoing interface

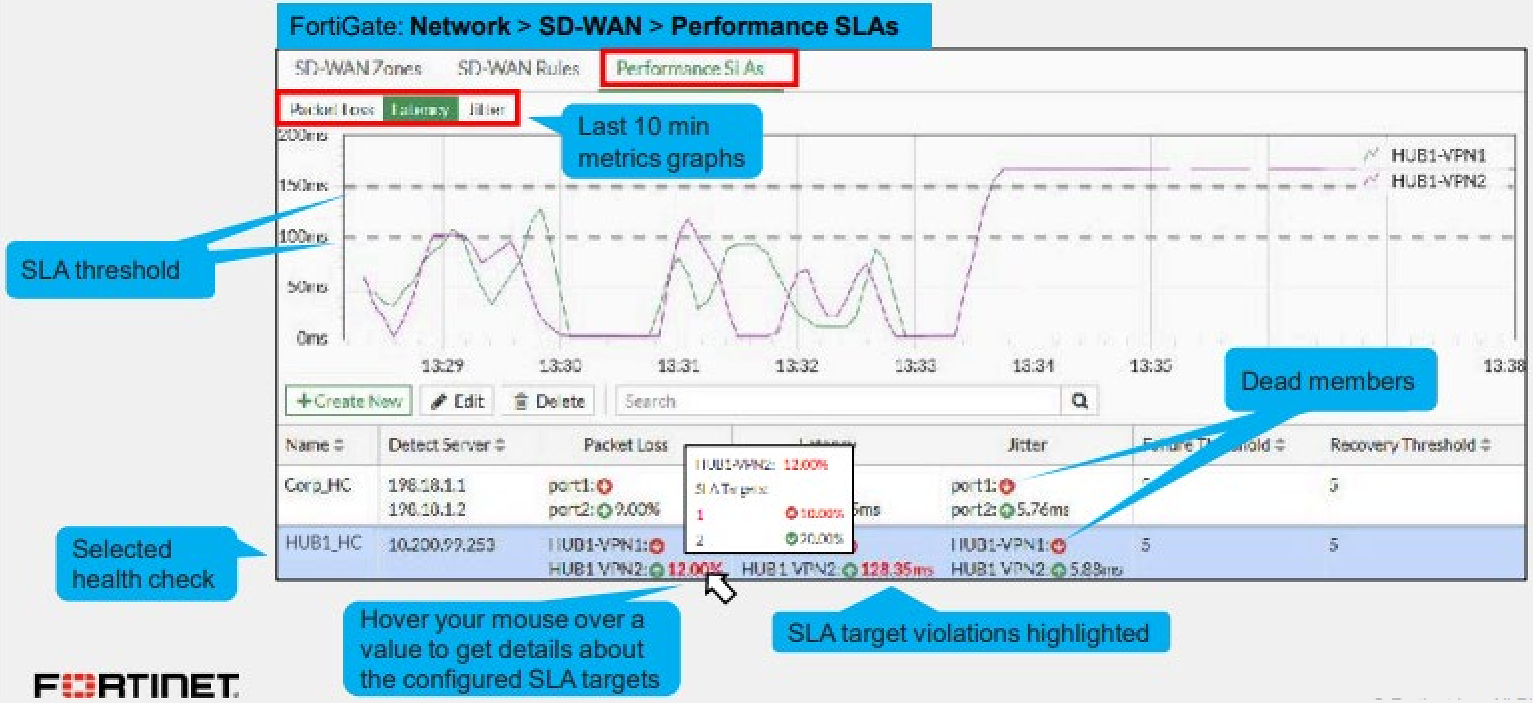
Gateway address: 0.0.0.0

Comments: Write a comment... 0/255

Status: [✓ Enabled] | Disabled

Intelligent PBR with link monitoring – SD-WAN

- Monitor health of links
- Detect performance issues – not just up/down interfaces
- Latency, Jitter, Packet loss
- Various monitoring methods
  - Active/Passive
  - Ping/HTTP/TCP



FortiGate: **Network > SD-WAN > Performance SLAs**

Name	Detect Server	Packet Loss	Latency	Jitter	Failure Threshold	Recovery Threshold
Corp_HC	198.18.1.1 198.18.1.2	port1: ⊖ port2: ⊕ 9.00%	5ms	port1: ⊖ port2: ⊕ 5.76ms	5	5
HUB1_HC	10.200.99.253	HUB1-VPN1: ⊖ HUB1-VPN2: ⊕ 12.00%	HUB1-VPN2: ⊕ 128.35ms	HUB1-VPN1: ⊖ HUB1-VPN2: ⊕ 5.88ms	5	5

HUB1-VPN2: 12.00%
SLA Targets:
1 ⊖ 10.00%
2 ⊕ 20.00%

Last 10 min metrics graphs

SLA threshold

Dead members

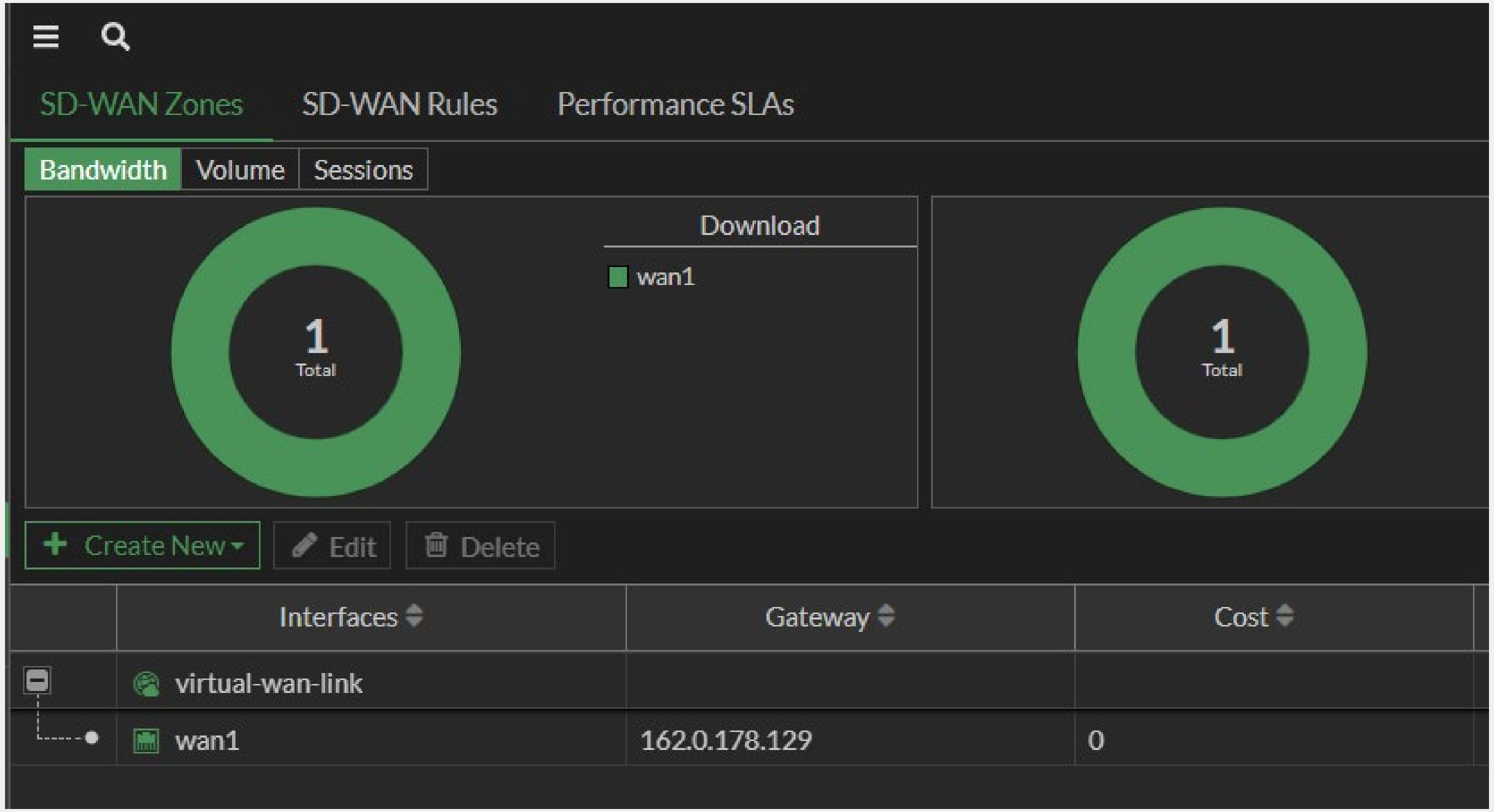
Selected health check

Hover your mouse over a value to get details about the configured SLA targets

SLA target violations highlighted

SD-WAN Components: Members and Zones

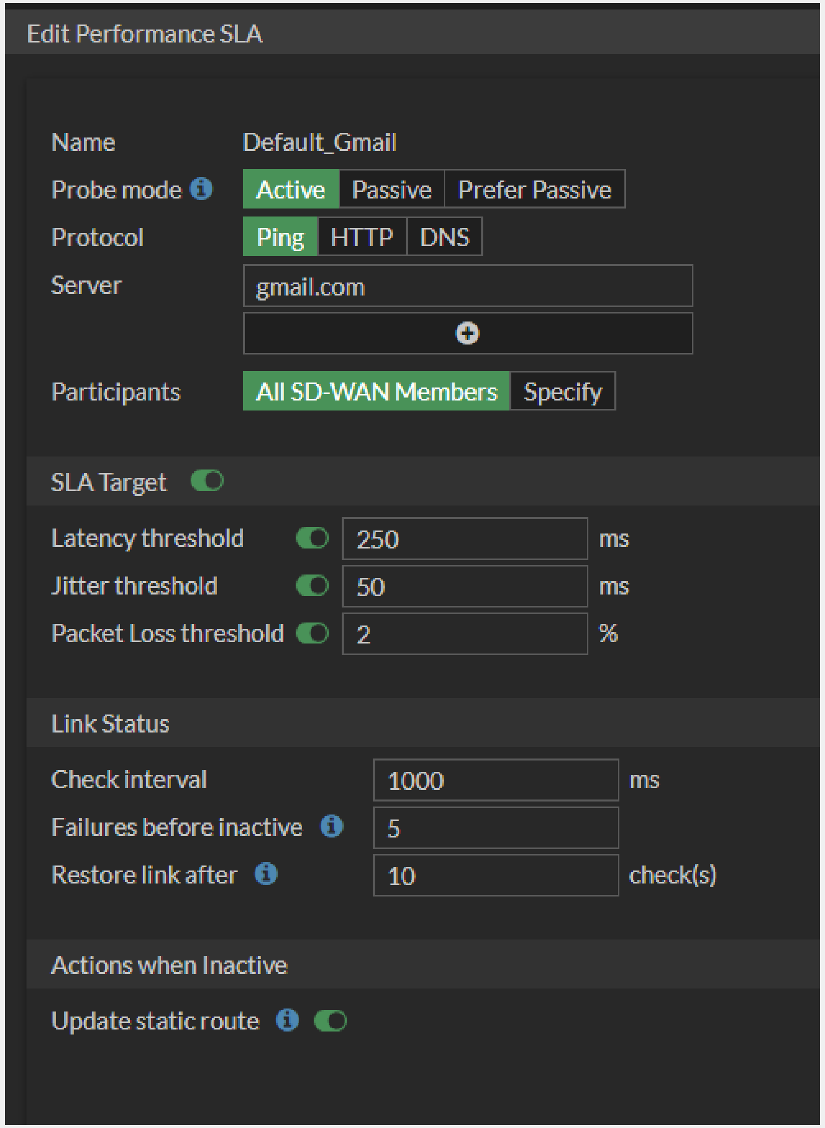
- Create Zones
  - Overlay/Underlay
- Members can belong to 1 zone
- Members can't be referenced individually in FW policies
- Static routes can be created to zone or member for granular control
- Cost – used as SD-WAN tiebreaker
- Priority – used for routing preference
- Could also use routing best match as tie break



Interfaces	Gateway	Cost
virtual-wan-link		
wan1	162.0.178.129	0

SD-WAN Components: Performance SLA

- Monitor health of members
  - Define destinations to monitor
- Active, passive, prefer passive
  - Passive monitors real-time traffic but requires CPU processing on FW rule
- Set targets for link performance
  - Latency, jitter, packet loss
    - Optionally combine in MOS
- Define minimum performance required for steering traffic
- Assign to all or specific members
- Multiple servers protects against server failure



Edit Performance SLA

Name: Default_Gmail

Probe mode: [✓ Active] Passive Prefer Passive

Protocol: [✓ Ping] HTTP DNS

Server: gmail.com

Participants: [✓ All SD-WAN Members] Specify

SLA Target ●

Latency threshold ● 250 ms

Jitter threshold ● 50 ms

Packet Loss threshold ● 2 %

Link Status

Check interval: 1000 ms

Failures before inactive: 5

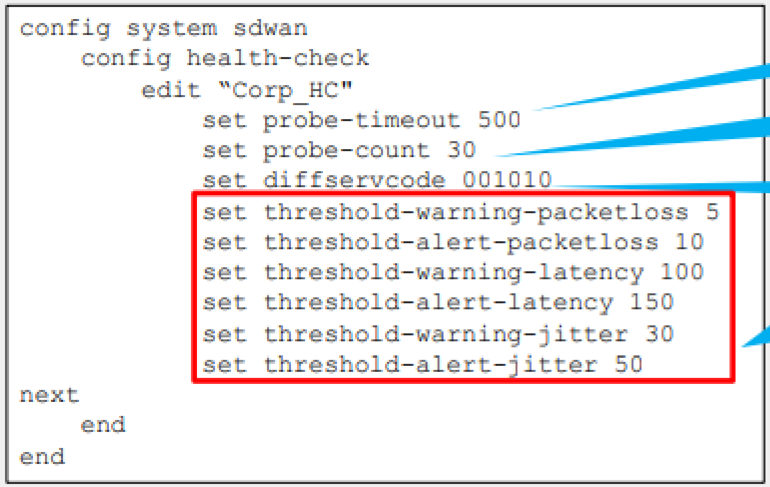
Restore link after: 10 check(s)

Actions when Inactive

Update static route ●

SD-WAN Components: Performance SLA

FortiGate Advanced SLA Settings—Warning and Alert



```
config system sdwan
    config health-check
        edit "Corp_HC"
            set probe-timeout 500
            set probe-count 30
            set diffservcode 001010
            set threshold-warning-packetloss 5
            set threshold-alert-packetloss 10
            set threshold-warning-latency 100
            set threshold-alert-latency 150
            set threshold-warning-jitter 30
            set threshold-alert-jitter 50
next
    end
end
```

Time to wait for probe response (default = `500`)

Number of most recent probes to use for latency and jitter calculation (default = `30`)

DSCP code to be used by probes (default = `000000`)

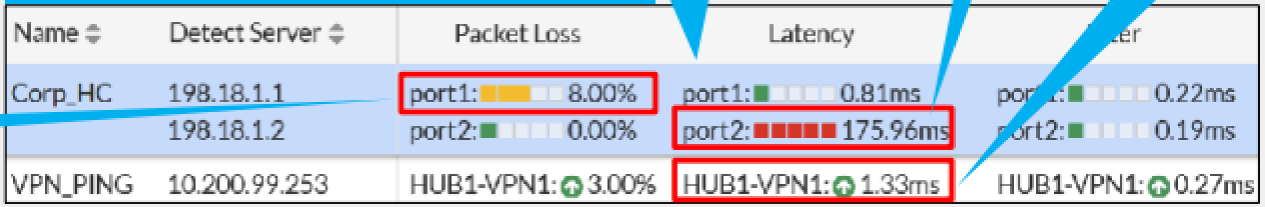
Warning and alert thresholds for metrics; used by the FortiGate GUI for visual notification and to trigger log messages

No SLA threshold configured

Alert

Warning

FortiGate: **Network > SD-WAN > Performance SLAs**



Name ≑	Detect Server ≑	Packet Loss	Latency	Jitter
Corp_HC	198.18.1.1 198.18.1.2	port1: 8.00% port2: 0.00%	port1: 0.81ms port2: 175.96ms	port1: 0.22ms port2: 0.19ms
VPN_PING	10.200.99.253	HUB1-VPN1: ⬆ 3.00%	HUB1-VPN1: ⬆ 1.33ms	HUB1-VPN1: ⬆ 0.27ms

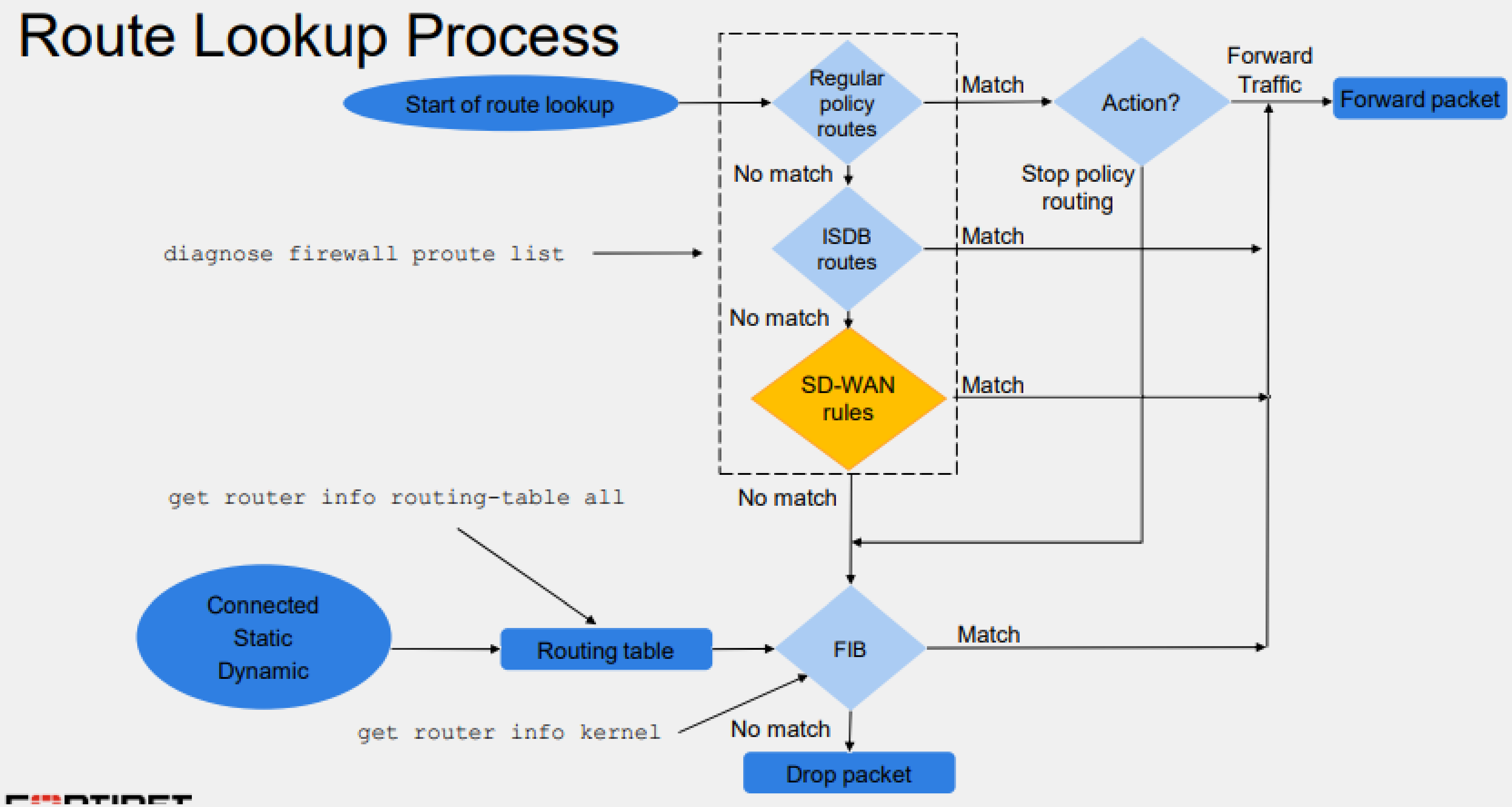
FORTINET Training Institute

SD-WAN: Routing

Key Routing Principles

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

SD-WAN: Routing



Route Lookup Process

Start of route lookup

Regular policy routes

No match

ISDB routes

No match

SD-WAN rules

No match

Match

Action?

Forward Traffic

Forward packet

Stop policy routing

Match

Match

```
diagnose firewall proute list
```

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

Connected
Static
Dynamic

Routing table

FIB

Match

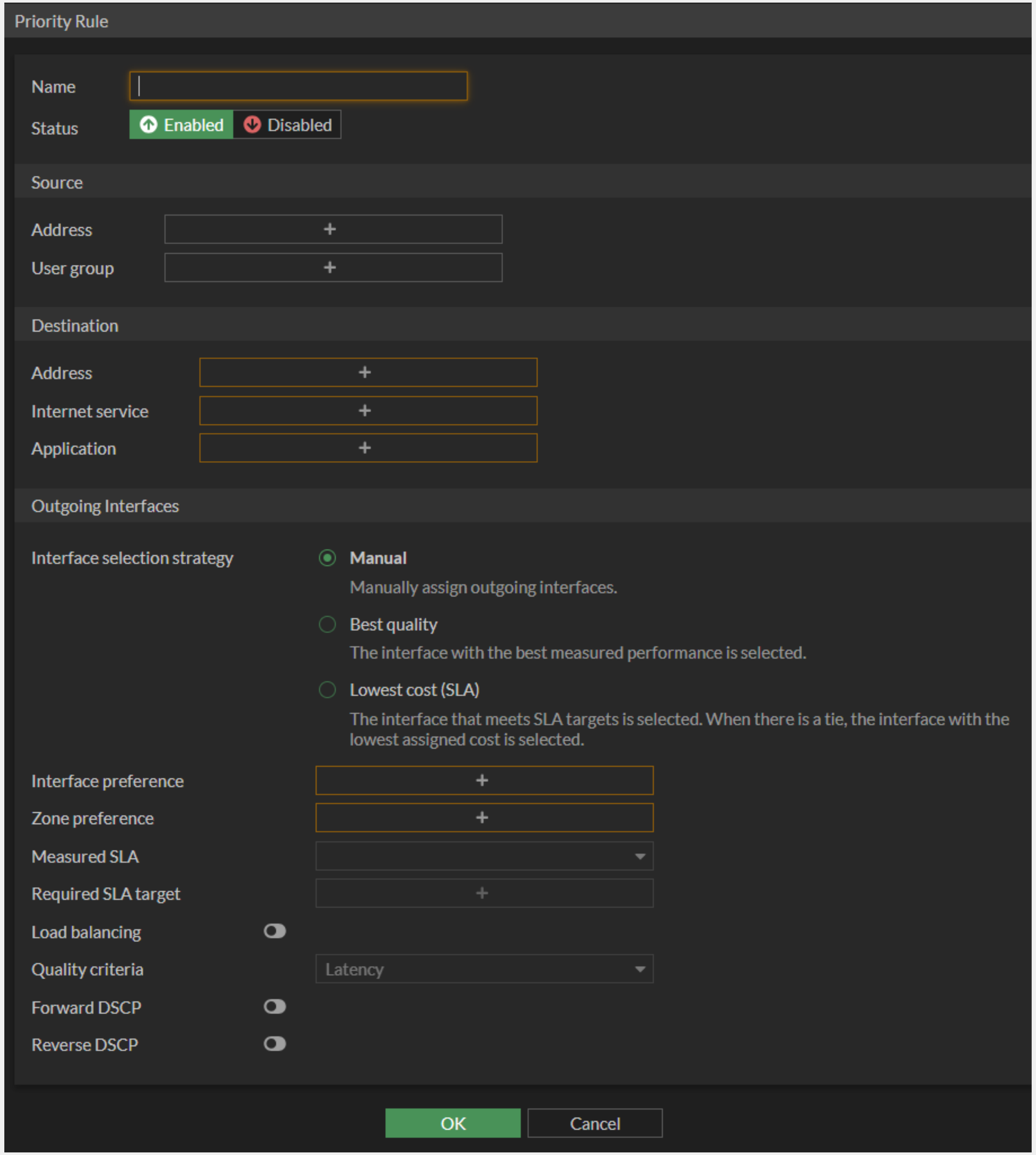
No match

Drop packet

```
get router info kernel
```

SD-WAN: Rules

- Specify criteria for matching traffic
- Source/Destination/User
- Can specify destination applications or categories
  - Can use Route Tags
  - Application required application profile on FW rule
- Specify outgoing interface selection
- Optional SLA requirements



Priority Rule

Name

Status: Enabled | Disabled

Source

Address +

User group +

Destination

Address +

Internet service +

Application +

Outgoing Interfaces

Interface selection strategy

● **Manual**
Manually assign outgoing interfaces.

○ Best quality
The interface with the best measured performance is selected.

○ Lowest cost (SLA)
The interface that meets SLA targets is selected. When there is a tie, the interface with the lowest assigned cost is selected.

Interface preference +

Zone preference +

Measured SLA

Required SLA target +

Load balancing

Quality criteria: Latency

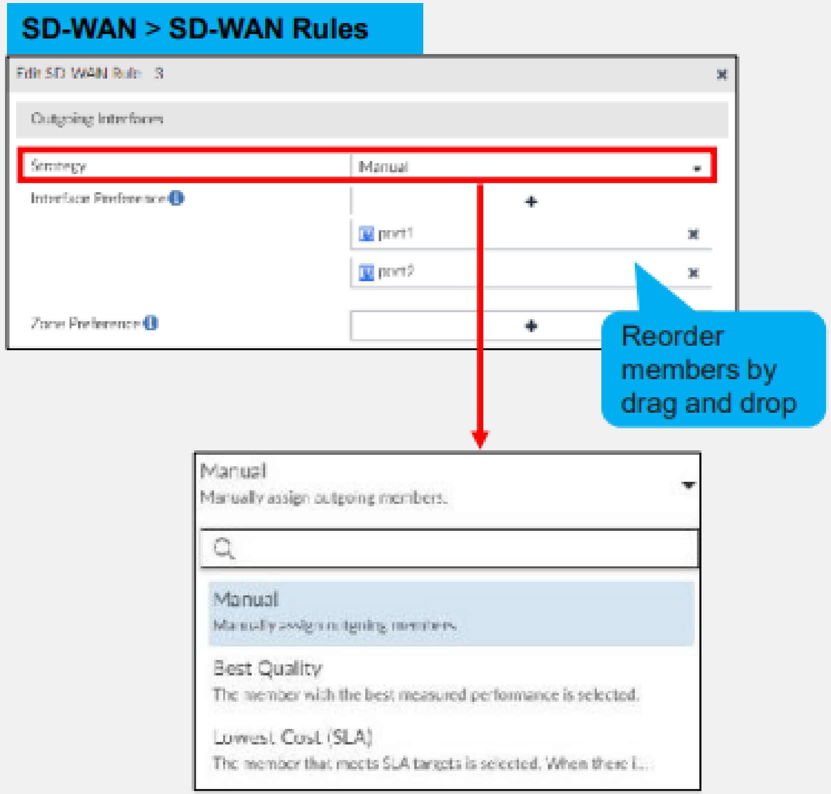
Forward DSCP

Reverse DSCP

SD-WAN: Rule Strategy

Strategies

- Define:
  - Requirements for preferred members
- Preferred members:
  - Best candidates to steer traffic
  - Are used only if they have a valid route to the destination
- Member selection:
  - **Manual**:
    - Configuration order-based preference
  - **Best Quality**:
    - Best performing member based on quality criteria
  - **Lowest Cost (SLA)**:
    - Member that meets SLA target (tiebreakers: cost and configuration order)
- Load balancing:
  - By default, each strategy selects a single member
  - Load balancing option to distribute the traffic through multiple members



SD-WAN > SD-WAN Rules

Edit SD-WAN Rule 3

Outgoing Interfaces

Strategy: Manual

Interface Preference: port1, port2

Zone Preference

Reorder members by drag and drop

Manual
Manually assign outgoing members.

Manual
Manually assign outgoing members.

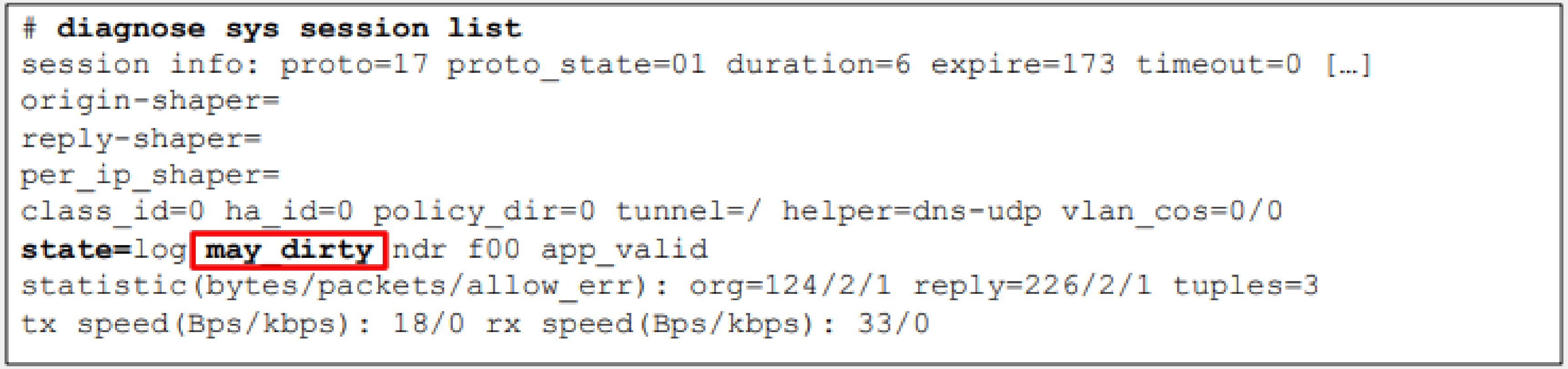
Best Quality
The member with the best measured performance is selected.

Lowest Cost (SLA)
The member that meets SLA targets is selected. When there i...

SD-WAN Caveats: Sessions

May_Dirty Sessions

- New firewall sessions created after matching a firewall policy with `accept` action
  - A firewall policy lookup is done (top-down)
  - Flagged as `may_dirty`
- Lookup process
  - First original packet (route and firewall policy lookup)
  - First reply packet (route lookup only)
  - No additional lookups unless session is flagged as `dirty`

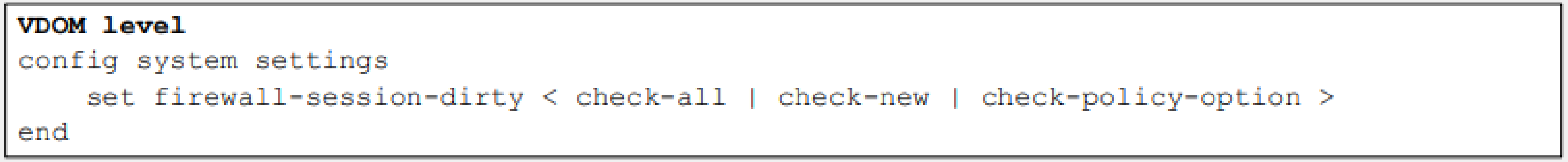


```
# diagnose sys session list
session info: proto=17 proto_state=01 duration=6 expire=173 timeout=0 […]
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ helper=dns-udp vlan_cos=0/0
state=log may_dirty ndr f00 app_valid
statistic(bytes/packets/allow_err): org=124/2/1 reply=226/2/1 tuples=3
tx speed(Bps/kbps): 18/0 rx speed(Bps/kbps): 33/0
```

SD-WAN Caveats: Sessions

Limit the Session Reevaluation

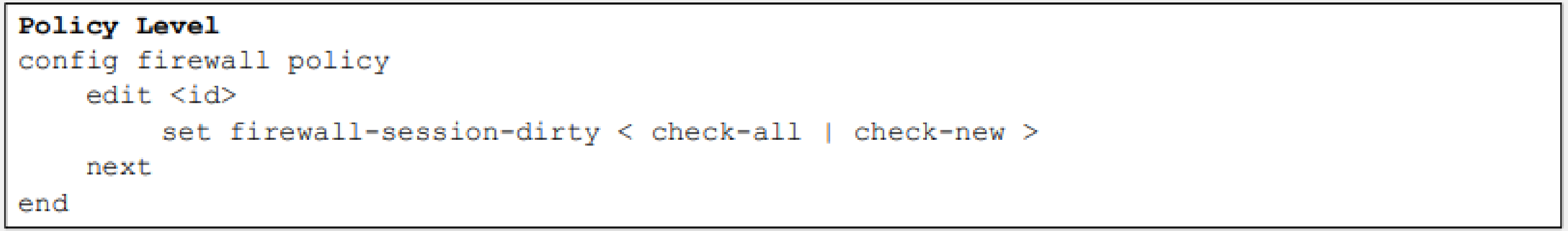
- Session reevalutation can lead to high CPU utilization
- Select which sessions in the VDOM are flagged as `dirty` (default = `check-all`):



```
VDOM level
config system settings
    set firewall-session-dirty < check-all | check-new | check-policy-option >
end
```

  - `check-all`: All sessions are flagged as dirty
  - `check-new`: New sessions are flagged as dirty and existing sessions are not affected.
  - `check-policy-option`: Follow firewall policy-level configuration

- Firewall policy-level configuration (default = `check-all`):



```
Policy Level
config firewall policy
    edit <id>
        set firewall-session-dirty < check-all | check-new >
    next
end
```

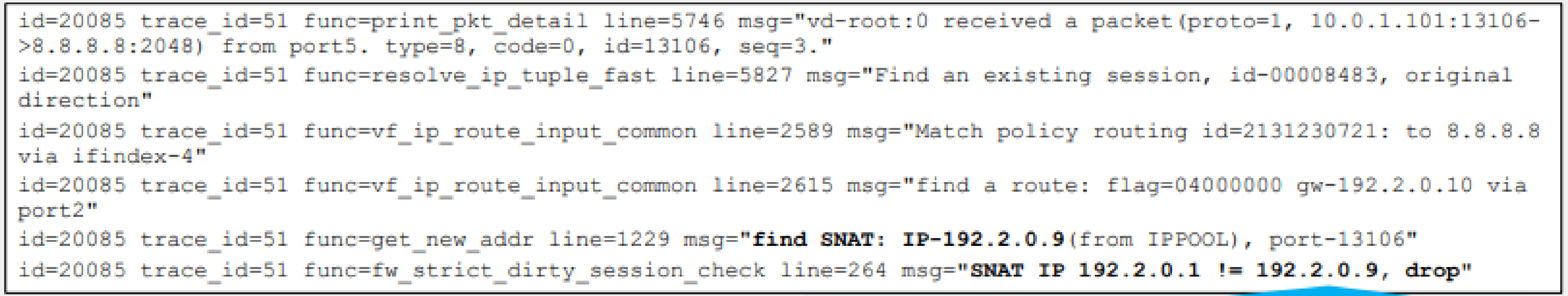
SD-WAN Caveats: Sessions

Routing Changes and SNAT Sessions

- By default, SNAT sessions are not flagged as `dirty` after a routing change
  - Exception: The route in use is removed from FIB
- Force reevaluation of SNAT sessions after a routing change (default = `disable`):

```
config system global
    set snat-route-change < enable | disable >
end
```

- If SNAT IP changes during reevaluation, packet is dropped, and session is cleared



```
id=20085 trace_id=51 func=print_pkt_detail line=5746 msg="vd-root:0 received a packet(proto=1, 10.0.1.101:13106-
>8.8.8.8:2048) from port5. type=8, code=0, id=13106, seq=3."
id=20085 trace_id=51 func=resolve_ip_tuple_fast line=5827 msg="Find an existing session, id-00008483, original
direction"
id=20085 trace_id=51 func=vf_ip_route_input_common line=2589 msg="Match policy routing id=2131230721: to 8.8.8.8
via ifindex-4"
id=20085 trace_id=51 func=vf_ip_route_input_common line=2615 msg="find a route: flag=04000000 gw-192.2.0.10 via
port2"
id=20085 trace_id=51 func=get_new_addr line=1229 msg="find SNAT: IP-192.2.0.9(from IPPOOL), port-13106"
id=20085 trace_id=51 func=fw_strict_dirty_session_check line=264 msg="SNAT IP 192.2.0.1 != 192.2.0.9, drop"
```

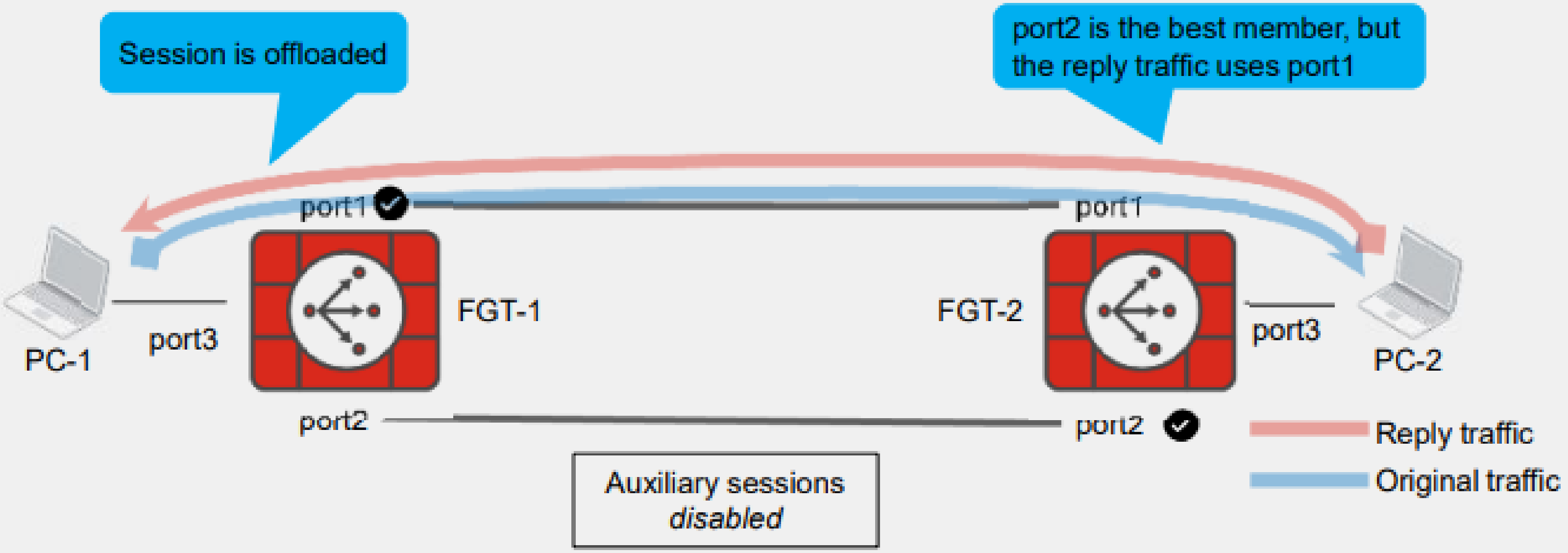
Different SNAT IP; drop the packet and clear the session

- Enable `snat-route-change` if using the same IP address pool for the old and new paths

SD-WAN Caveats: Sessions

Auxiliary Sessions

- Dirty sessions are also triggered by a change in the reply traffic interface
  - Sessions handled by system CPU (no hardware offload)
- By default, route lookup for reply traffic considers routes over the original ingress interface only
  - Reply traffic can't be routed over another member with better performance



Session is offloaded

port2 is the best member, but the reply traffic uses port1

Auxiliary sessions *disabled*

Resources

Fortinet Training Academy

Library: FCSS – SD-WAN 7.4 Architect Self-Paced

https://training.fortinet.com/course/view.php?id=58092

FORTINET®