GAPTECH

# IPsec with SD-WAN
# Fortinet

Huda -

Information available in audio.

# Overview

Briefly elaborate on what you want to discuss.

## IPsec Tunnel VPN

untuk mengamankan komunikasi data antara dua jaringan yang terhubung melalui internet

## SD-WAN

konsep jaringan yang ditentukan software untuk mendistribusikan traffic di jaringan area yang luas

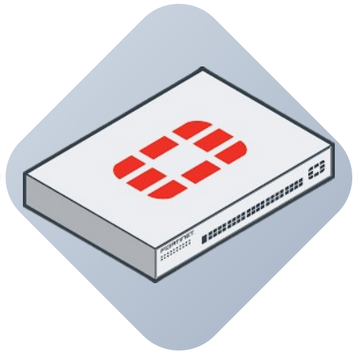
# Reqruitment Project

| | | | |
|---|---|---|---|
| IPSec Tunnels SD-WAN | 1 | IP-Tunnel via ISP1 Site-To-Site | 6 |
| Kantor Pusat JKT | 2 | IP-Tunnel via ISP2 Dial-up | 7 |
| Brance Office: JABAR, JATENG, Yogya | 3 | Dapat berkomunikasi antar cabang via HQ | 8 |
| 2 WAN | 4 | Server Farm Tidak terkoneksi internet | 9 |
| ISP1 Static IP & ISP2 Dynamic IP | 5 | | |

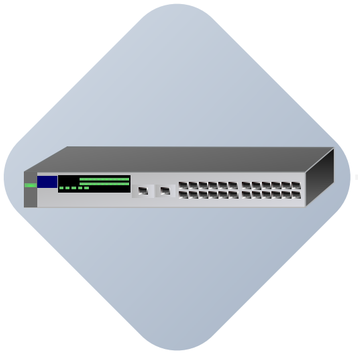
# Hardware Overview

Briefly elaborate on what you want to discuss.


Router Mikrotik



Fortigate



Switch Cisco

End Device

Back to Agenda

# Router

Router HQ dan Router Brance

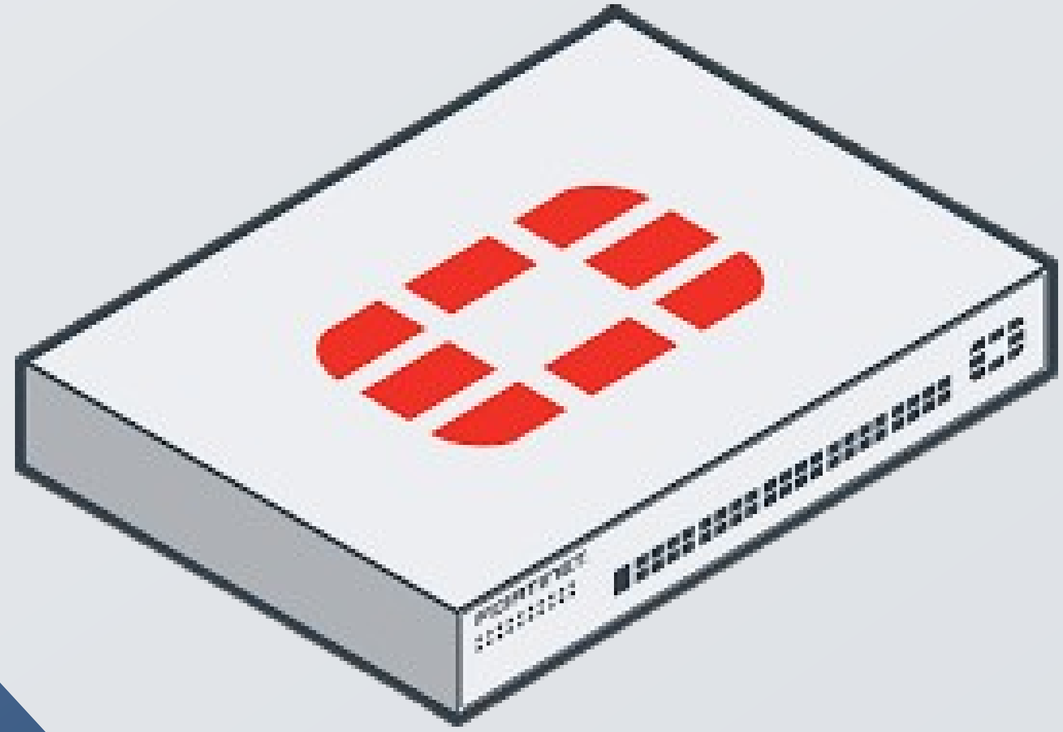
| | |
|---|---|
| 7.0.10 | Version |
| 736 MB | RAM |
| 1 | CPU |


Back to Agenda

# Fortigate

FGT-HQ-DC , FGT-JBR,
FGT-JTG, FGT-YK

| | |
|---|---|
| V7.0.11 | Version |
| 2048 MB | RAM |
| 1 | CPU |



Back to Agenda

# Switch Cisco

SW-HA > HQ Office

| | |
|---|---|
| IOS_L2 | Version |
| 1638 MB | RAM |
| 1 | CPU |

# Planning

Briefly elaborate on what you want to discuss.

Back to Agenda

## Topology Design

Elaborate on your first goal here.

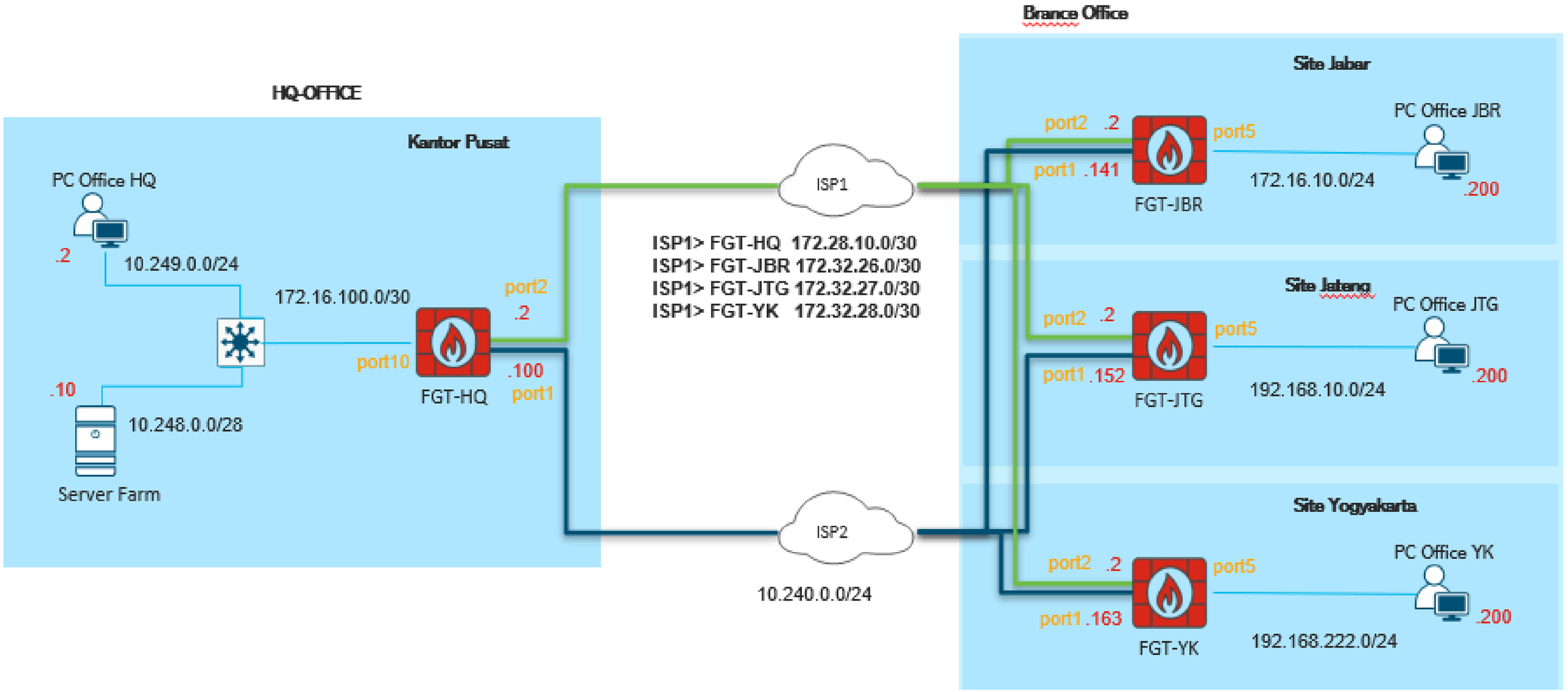
## Mapping Interfaces

Elaborate on your second goal here.

## Implementasi

Elaborate on your third goal here.

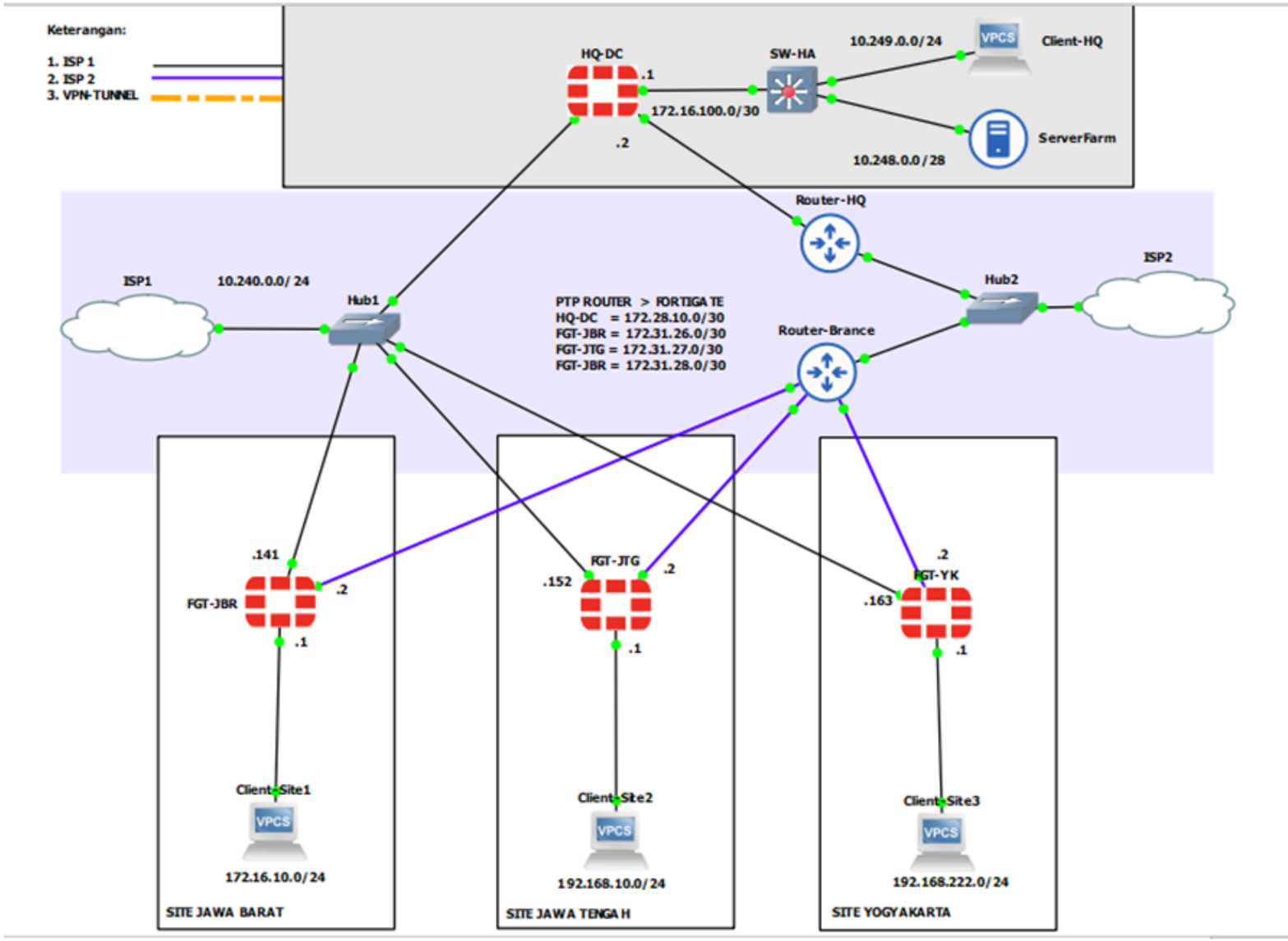
# Planning Design



# Design Implementasi

**Tip:** Collaboration makes teamwork easier! Click "Share" and invite your teammates to fill this up. Use this page for bulletins, brainstorms, and other fun team ideas.

**Right-click** on the **background** of the slide, or on the **thumbnail** below, for the option to **expand** this page into a **whiteboard** for more space!



# Mapping Interface

Briefly elaborate on what you want to discuss.

Back to Agenda

| No | Device | Interface | IP Address | Netmask | Keterangan |
|---|---|---|---|---|---|
| 1 | FGT-HQ-DC | Port1 | 10.240.0.100 | /24 | Static, IP-mgmt |
| | | Port 2 | 172.28.10.2 | /30 | Dynamic |
| | | Port 10 | 172.16.100.1 | /30 | To_Switch_HA |
| 2 | FGT-JABAR | Port1 | 10.240.0.141 | /24 | Static, IP-mgmt |
| | | Port 2 | 172.32.26.2 | /30 | Dynamic |
| | | Port 5 | 172.16.10.1 | /24 | PC-Client |
| 3 | FGT-JATENG | Port1 | 10.240.0.152 | /24 | Static, IP-mgmt |
| | | Port 2 | 172.32.27.2 | /30 | Dynamic |
| | | Port 5 | 192.168.10.1 | /24 | PC-Client |
| 4 | FGT-YK | Port1 | 10.240.0.163 | /24 | Static, IP-mgmt |
| | | Port 2 | 172.32.28.2 | /30 | Dynamic |
| | | Port 5 | 192.168.222.1 | /24 | PC-Client |

# Implementasi
# Configuration

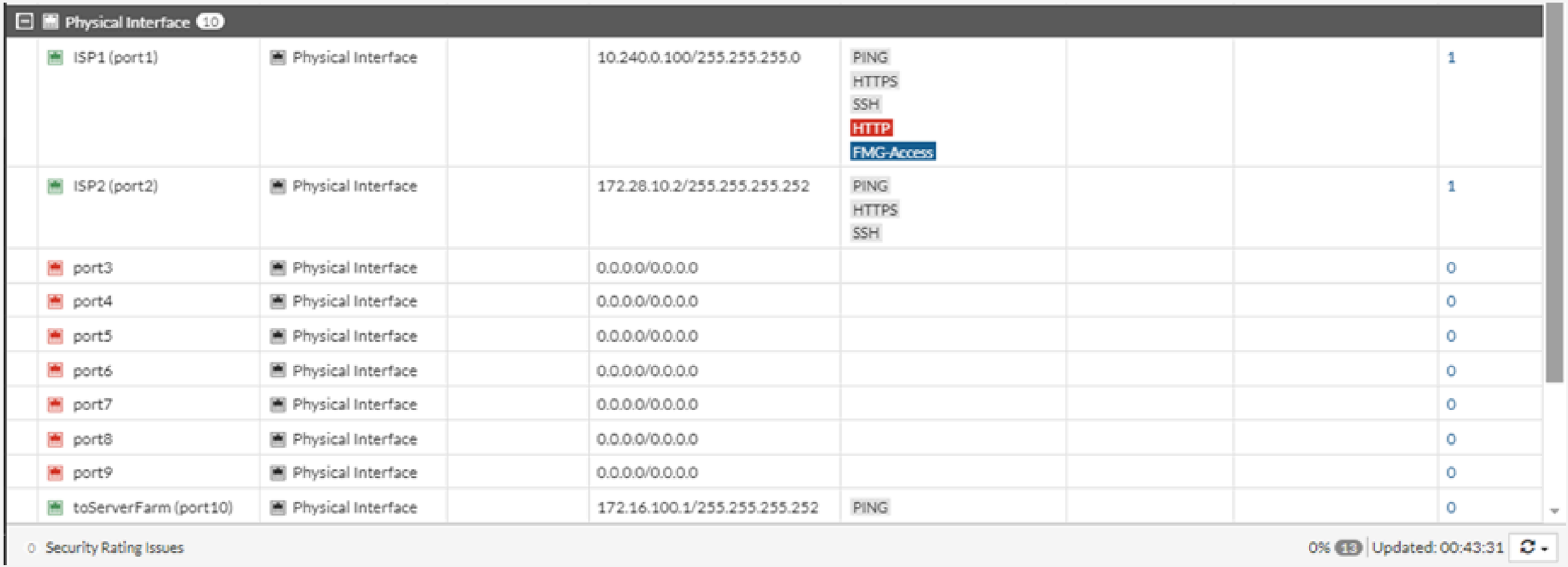
Briefly elaborate on what you want to discuss.

- Network Interfaces
- Network SD-WAN
- IP-Sec Tunnel
- Routing
- Policy

Back to Agenda

# Network Interfaces

## Interface HQ-DC-JKT



| Physical Interface 10 | | | | | | | |
|---|---|---|---|---|---|---|---|
| ISP1 (port1) | Physical Interface | | 10.240.0.100/255.255.255.0 | PING<br>HTTPS<br>SSH<br>HTTP<br>FMG-Access | | | 1 |
| ISP2 (port2) | Physical Interface | | 172.28.10.2/255.255.255.252 | PING<br>HTTPS<br>SSH | | | 1 |
| port3 | Physical Interface | | 0.0.0.0/0.0.0.0 | | | | 0 |
| port4 | Physical Interface | | 0.0.0.0/0.0.0.0 | | | | 0 |
| port5 | Physical Interface | | 0.0.0.0/0.0.0.0 | | | | 0 |
| port6 | Physical Interface | | 0.0.0.0/0.0.0.0 | | | | 0 |
| port7 | Physical Interface | | 0.0.0.0/0.0.0.0 | | | | 0 |
| port8 | Physical Interface | | 0.0.0.0/0.0.0.0 | | | | 0 |
| port9 | Physical Interface | | 0.0.0.0/0.0.0.0 | | | | 0 |
| toServerFarm (port10) | Physical Interface | | 172.16.100.1/255.255.255.252 | PING | | | 0 |

0 Security Rating Issues

0% 13 | Updated: 00:43:31

# Network Interfaces

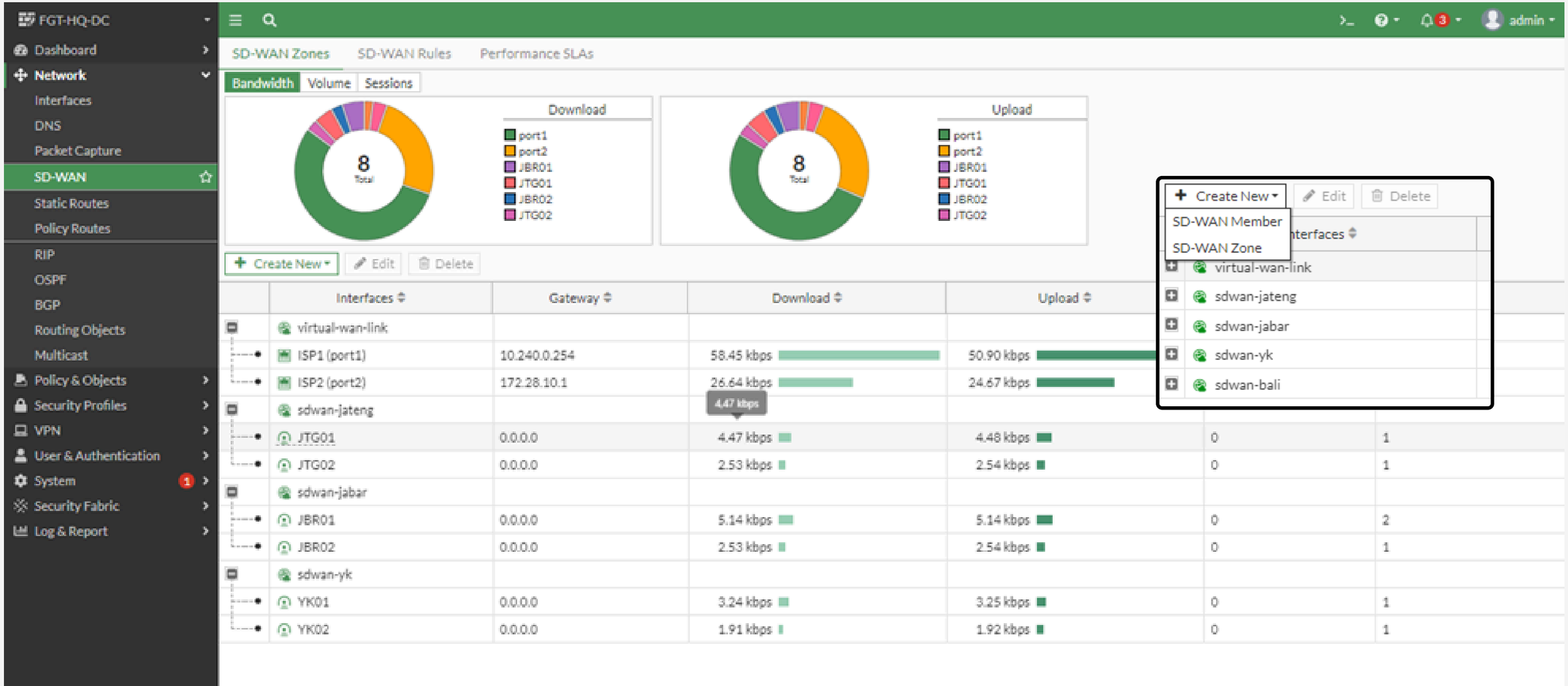
Interface FGT-JBR

| Physical Interface 10 | | | | | | | |
|---|---|---|---|---|---|---|---|
| ISP1 (port1) | Physical Interface | | 10.240.0.141/255.255.255.0 | PING<br>HTTPS<br>SSH<br>HTTP | | | 0 |
| ISP2 (port2) | Physical Interface | | 172.32.26.2/255.255.255.252 | PING<br>HTTPS<br>SSH | | | 0 |
| port3 | Physical Interface | | 0.0.0.0/0.0.0.0 | | | | 0 |
| port4 | Physical Interface | | 0.0.0.0/0.0.0.0 | | | | 0 |
| port5 | Physical Interface | | 172.16.10.1/255.255.255.0 | PING | | | 0 |
| port6 | Physical Interface | | 0.0.0.0/0.0.0.0 | | | | 0 |
| port7 | Physical Interface | | 0.0.0.0/0.0.0.0 | | | | 0 |
| port8 | Physical Interface | | 0.0.0.0/0.0.0.0 | | | | 0 |
| port9 | Physical Interface | | 0.0.0.0/0.0.0.0 | | | | 0 |
| port10 | Physical Interface | | 0.0.0.0/0.0.0.0 | | | | 0 |

# Network SD-WAN

**FGT-HQ-DC**

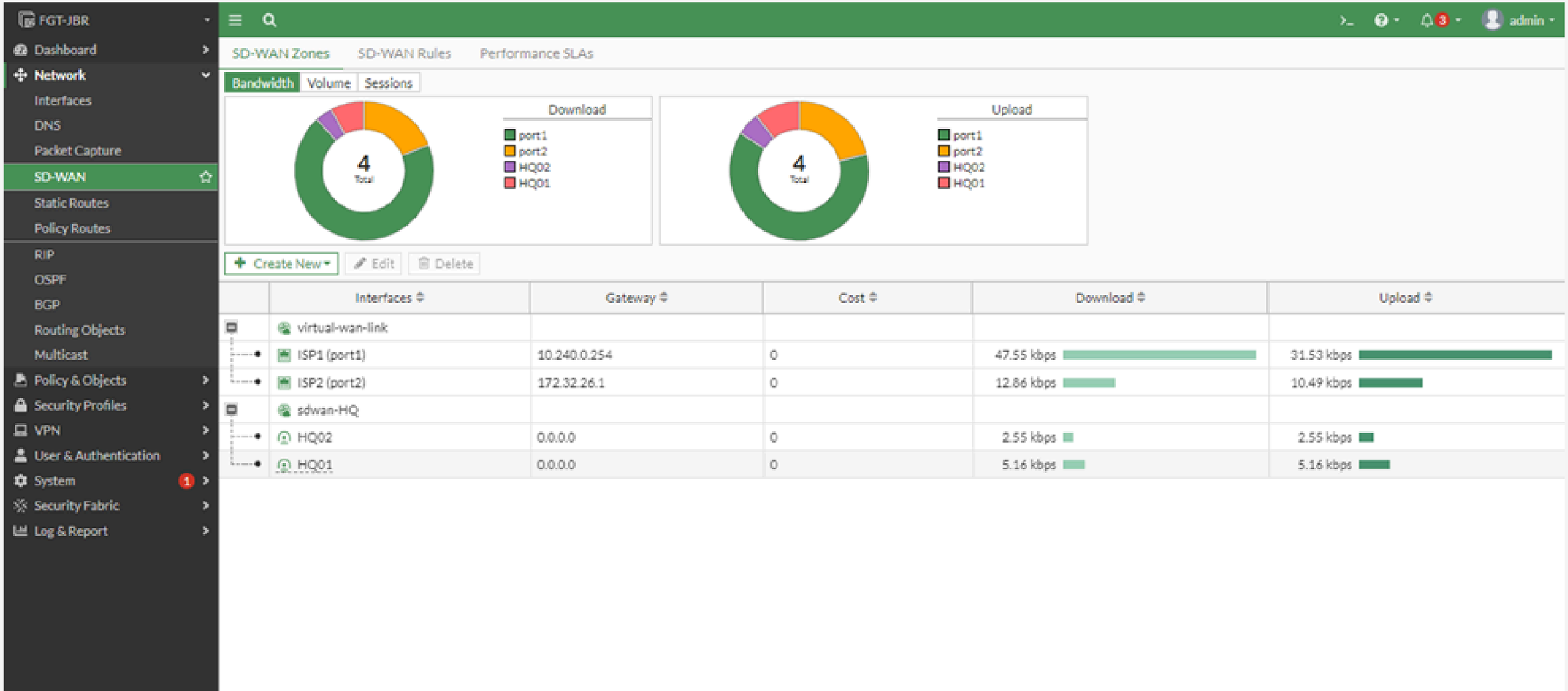
Create SD-WAN Internet Connection  Network > SD-WAN  > SD-WAN Zones > add link port ISP1 and ISP2.



# Network SD-WAN

FGT-JBR

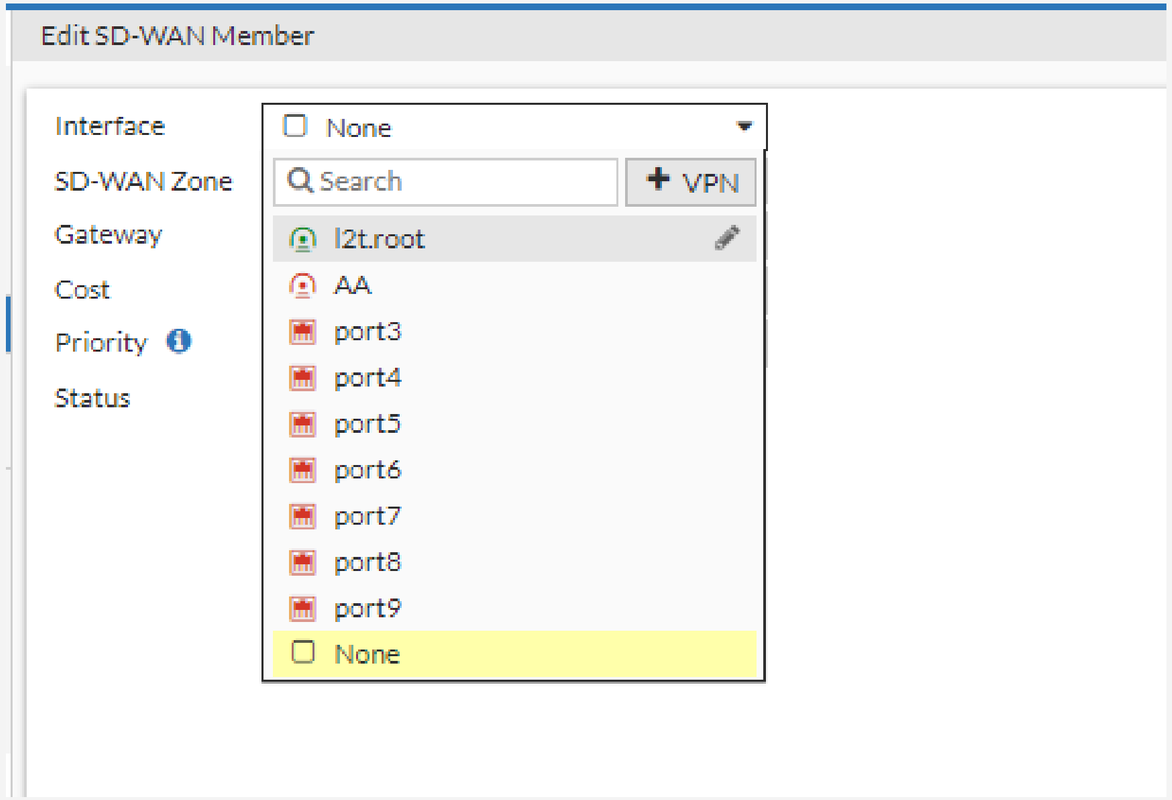
Create SD-WAN Internet Connection  Network > SD-WAN  > SD-WAN Zones > add link port ISP1 and ISP2.



# IP-Sec Tunnel VPN

FGT-HQ-DC

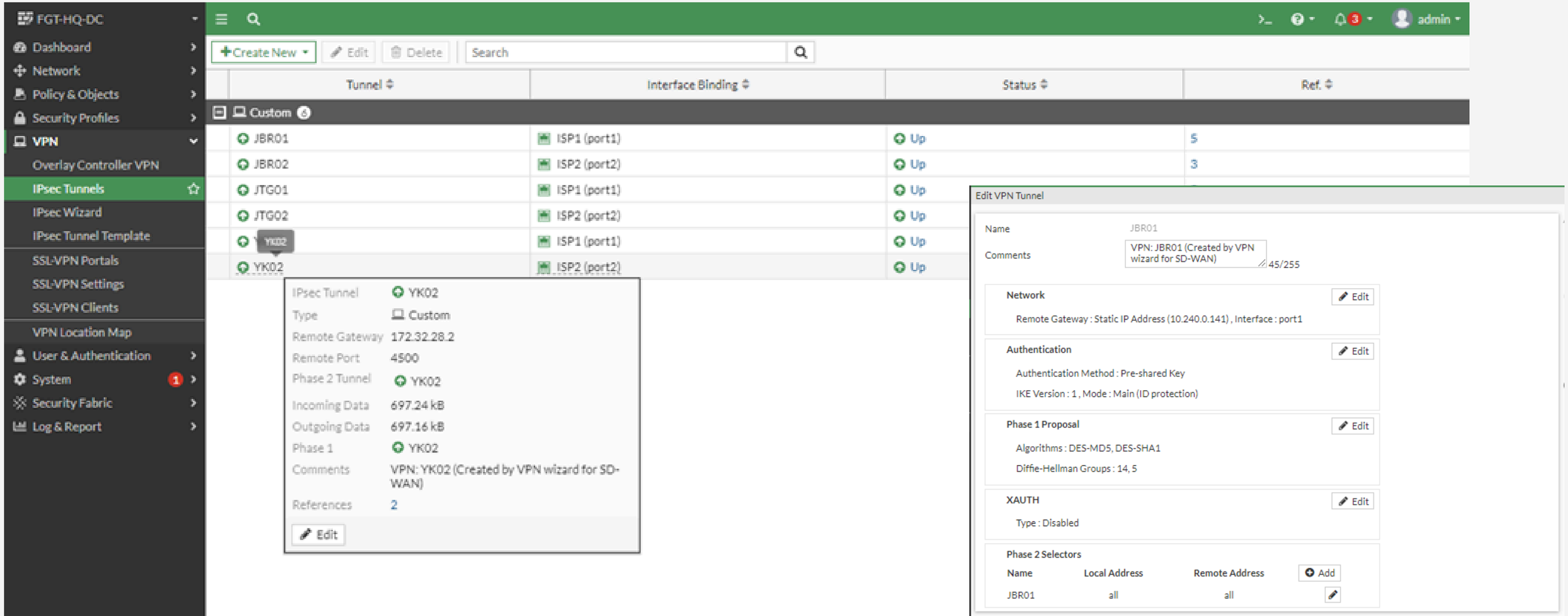
Network > SD-WAN > SD-WAN Zone > Create new > SD-WAN member > Interface > Create VPN.
create via members SD-WAN



# IP-Sec Tunnel VPN

FGT-HQ-DC

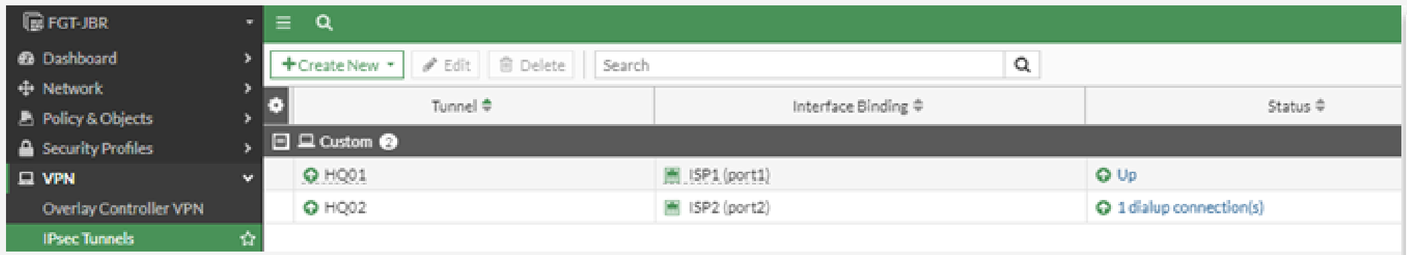
Network > SD-WAN > SD-WAN Zone > Create new > SD-WAN member > Interface > Create VPN.
create via members SD-WAN

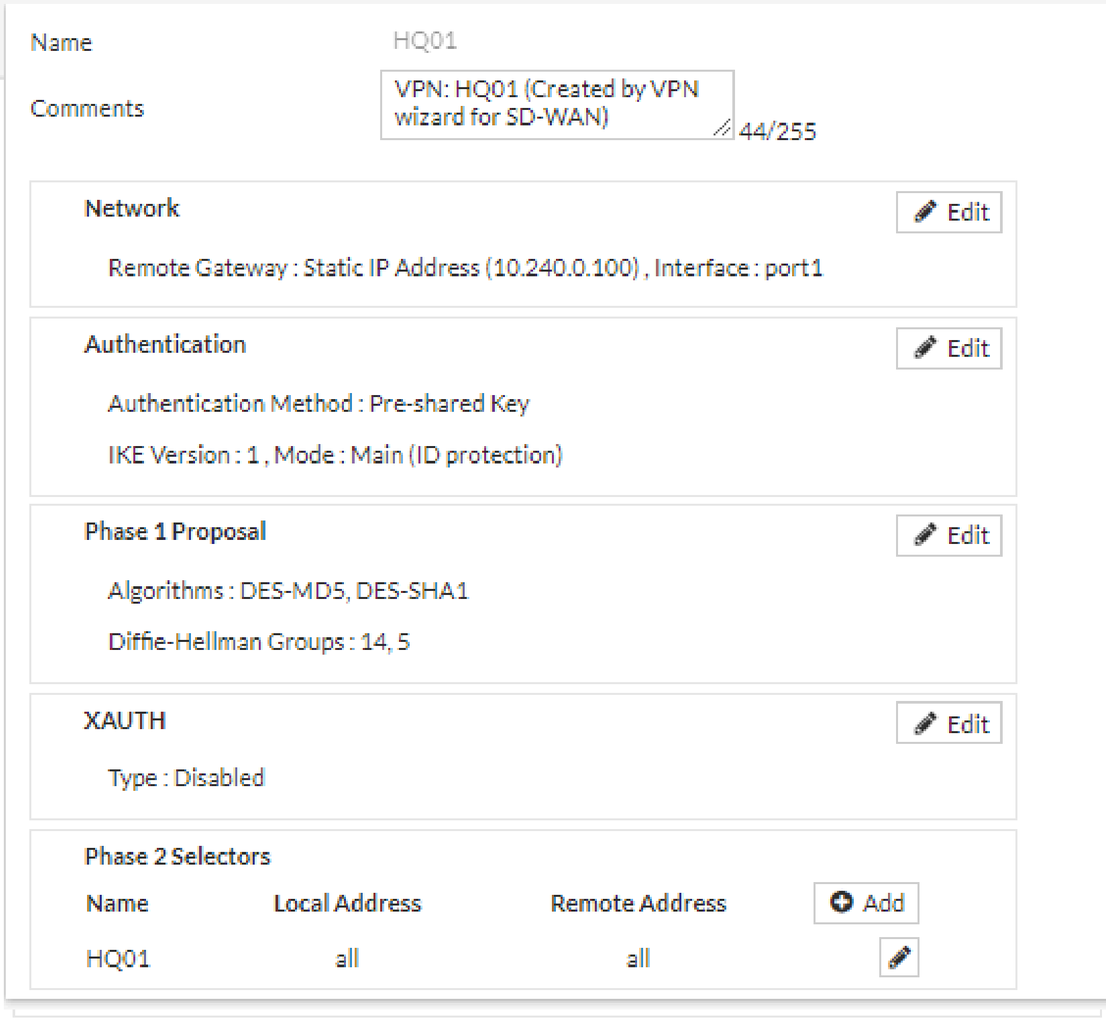


# IP-Sec Tunnel VPN

FGT-JBR

Network > SD-WAN > SD-WAN Zone > Create new > SD-WAN member > Interface > Create VPN.
create via members SD-WAN

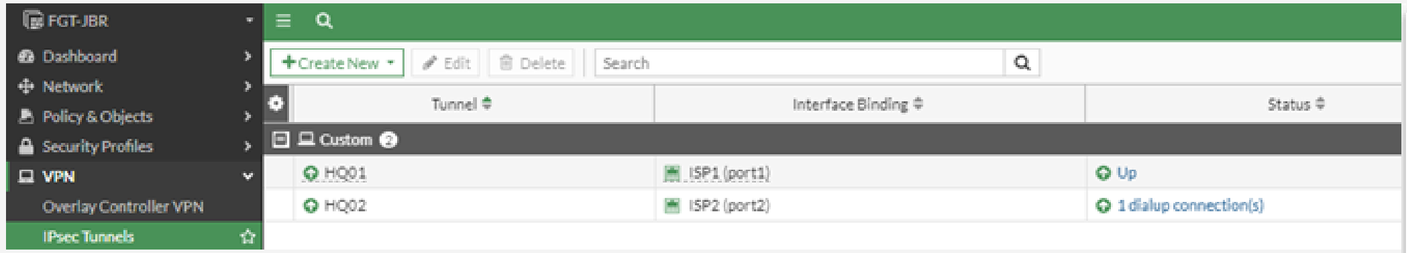


# IP-Sec Tunnel VPN

FGT-JBR

Network > SD-WAN > SD-WAN Zone > Create new > SD-WAN member > Interface > Create VPN.
create via members SD-WAN




Name HQ01

Name HQ02

Comments VPN: HQ02 (Created by VPN wizard for SD-WAN) 44/255

**Network** Edit

Remote Gateway : Dialup User , Interface : port2

**Authentication** Edit

Authentication Method : Pre-shared Key

IKE Version : 2

**Phase 1 Proposal** Edit

Algorithms : DES-SHA1

Diffie-Hellman Groups : 14, 5

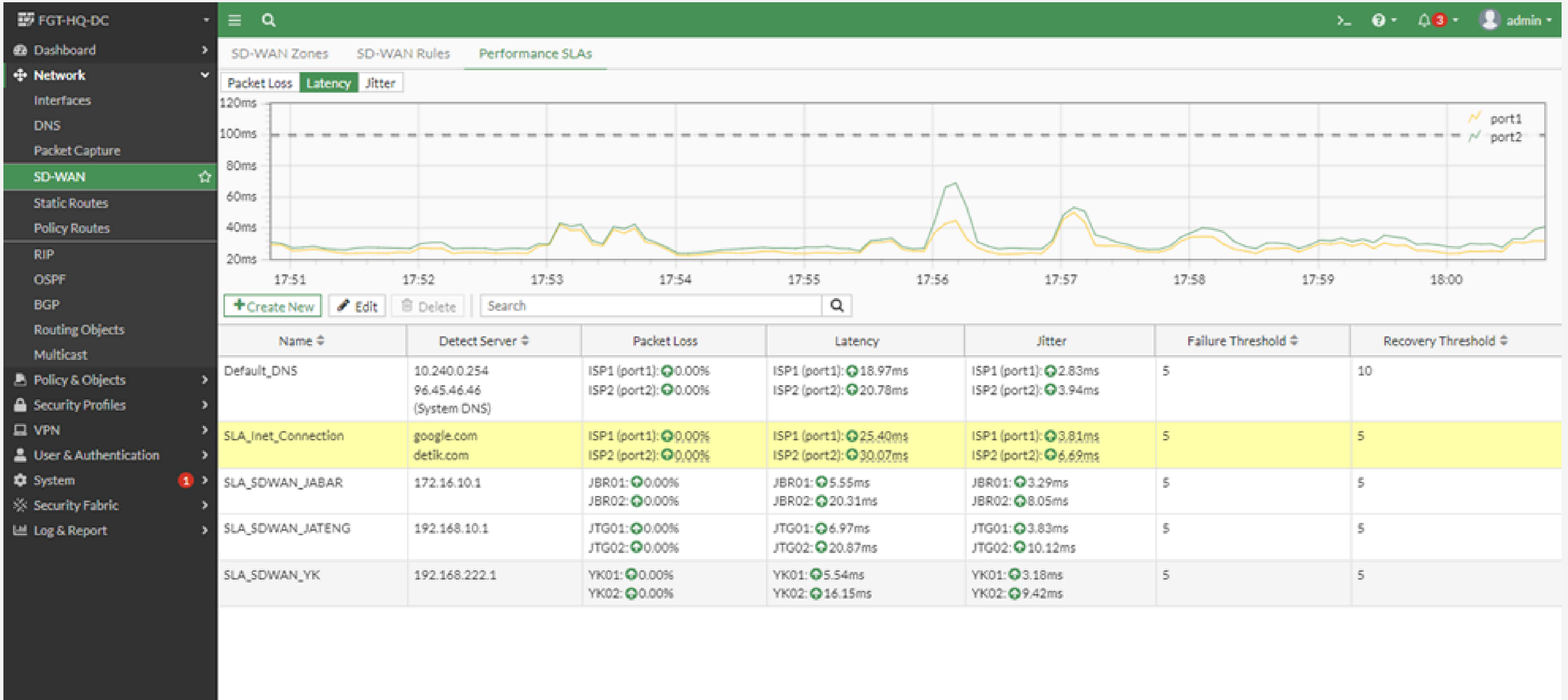
**Phase 2 Selectors**

| Name | Local Address | Remote Address | Add |
|---|---|---|---|
| HQ02 | all | all | |

# Network SD-WAN

FGT-HQ-DC

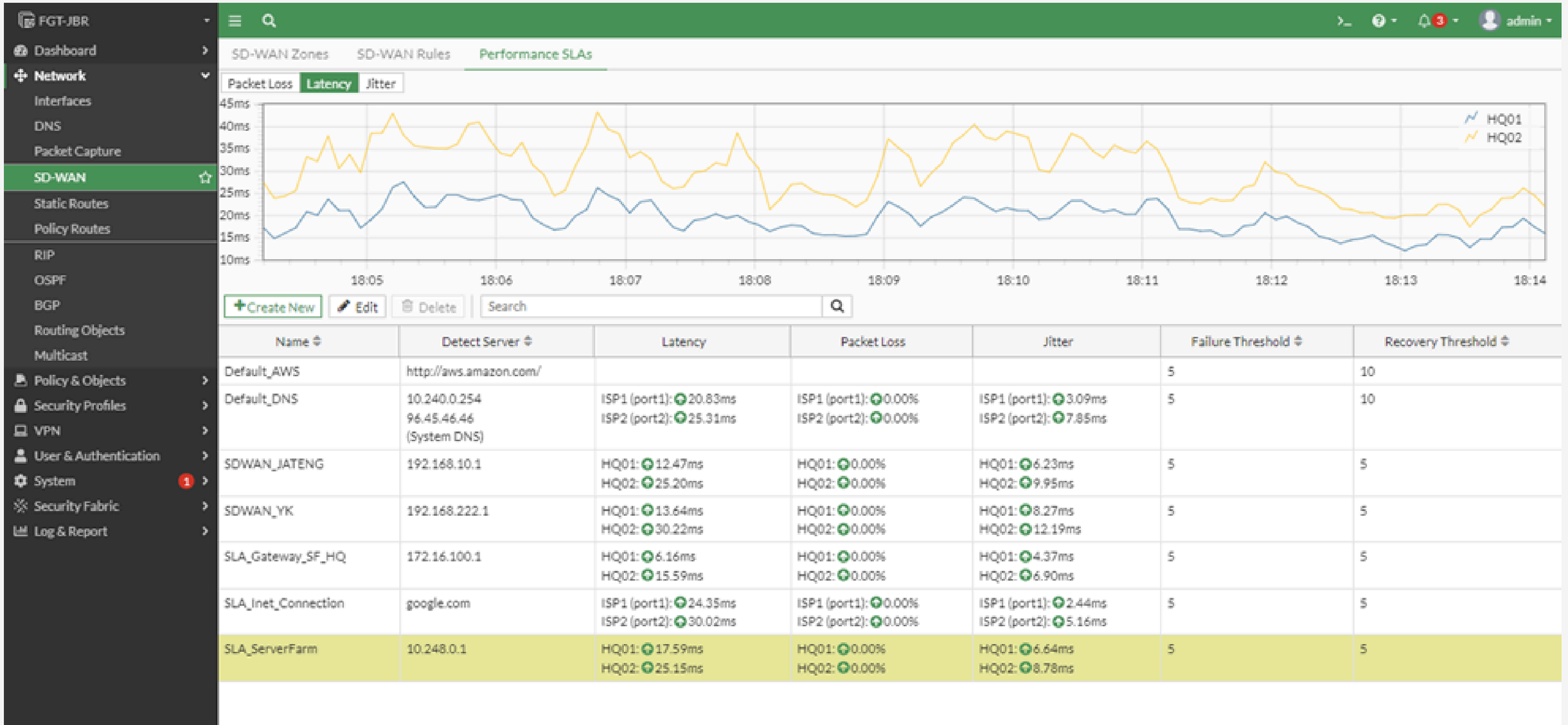
## Create SLA SD-WAN > Performance SLAs



# Network SD-WAN

FGT-JBR

## Create SLA SD-WAN > Performance SLAs

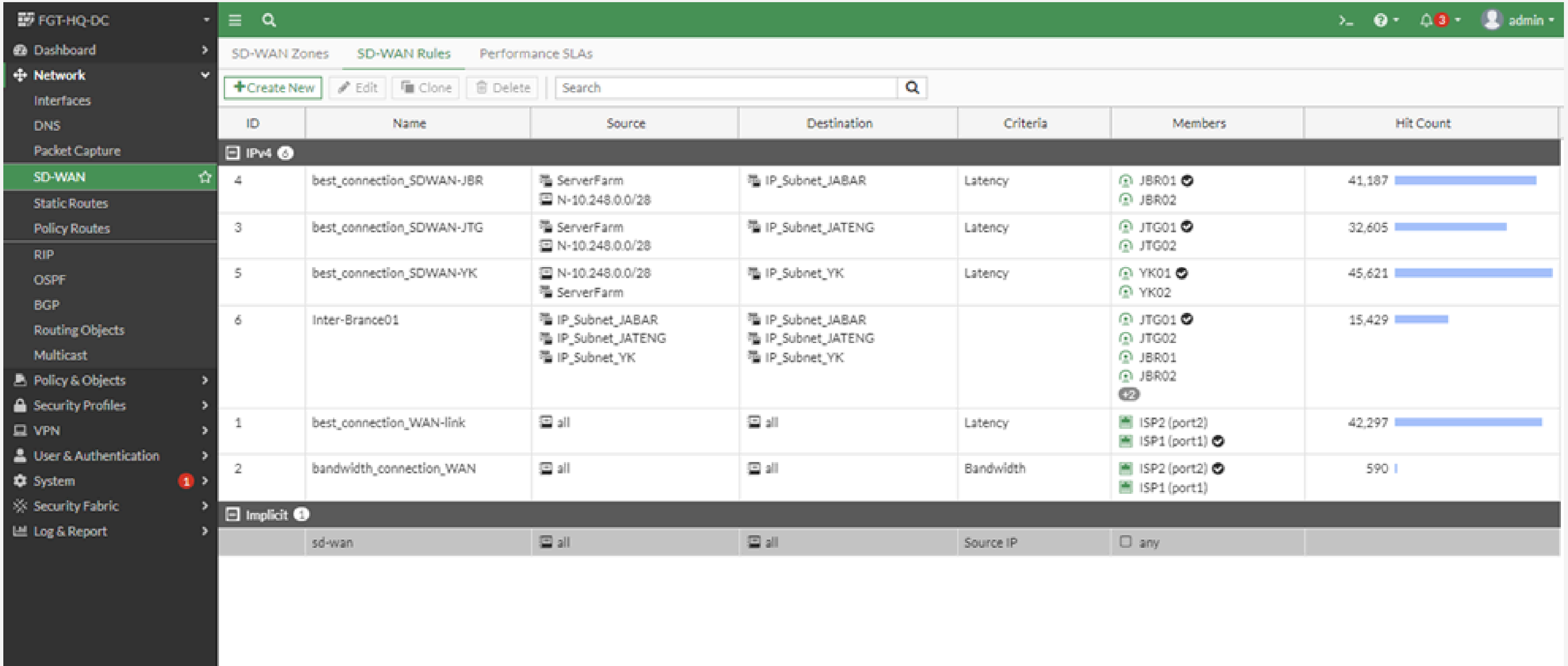



| Name | Detect Server | Latency | Packet Loss | Jitter | Failure Threshold | Recovery Threshold |
|---|---|---|---|---|---|---|
| Default_AWS | http://aws.amazon.com/ | | | | 5 | 10 |
| Default_DNS | 10.240.0.254<br>96.45.46.46<br>(System DNS) | ISP1 (port1): 20.83ms<br>ISP2 (port2): 25.31ms | ISP1 (port1): 0.00%<br>ISP2 (port2): 0.00% | ISP1 (port1): 3.09ms<br>ISP2 (port2): 7.85ms | 5 | 10 |
| SDWAN_JATENG | 192.168.10.1 | HQ01: 12.47ms<br>HQ02: 25.20ms | HQ01: 0.00%<br>HQ02: 0.00% | HQ01: 6.23ms<br>HQ02: 9.95ms | 5 | 5 |
| SDWAN_YK | 192.168.222.1 | HQ01: 13.64ms<br>HQ02: 30.22ms | HQ01: 0.00%<br>HQ02: 0.00% | HQ01: 8.27ms<br>HQ02: 12.19ms | 5 | 5 |
| SLA_Gateway_SF_HQ | 172.16.100.1 | HQ01: 6.16ms<br>HQ02: 15.59ms | HQ01: 0.00%<br>HQ02: 0.00% | HQ01: 4.37ms<br>HQ02: 6.90ms | 5 | 5 |
| SLA_Inet_Connection | google.com | ISP1 (port1): 24.35ms<br>ISP2 (port2): 30.02ms | ISP1 (port1): 0.00%<br>ISP2 (port2): 0.00% | ISP1 (port1): 2.44ms<br>ISP2 (port2): 5.16ms | 5 | 5 |
| SLA_ServerFarm | 10.248.0.1 | HQ01: 17.59ms<br>HQ02: 25.15ms | HQ01: 0.00%<br>HQ02: 0.00% | HQ01: 6.64ms<br>HQ02: 8.78ms | 5 | 5 |

# Network SD-WAN

FGT-HQ-DC

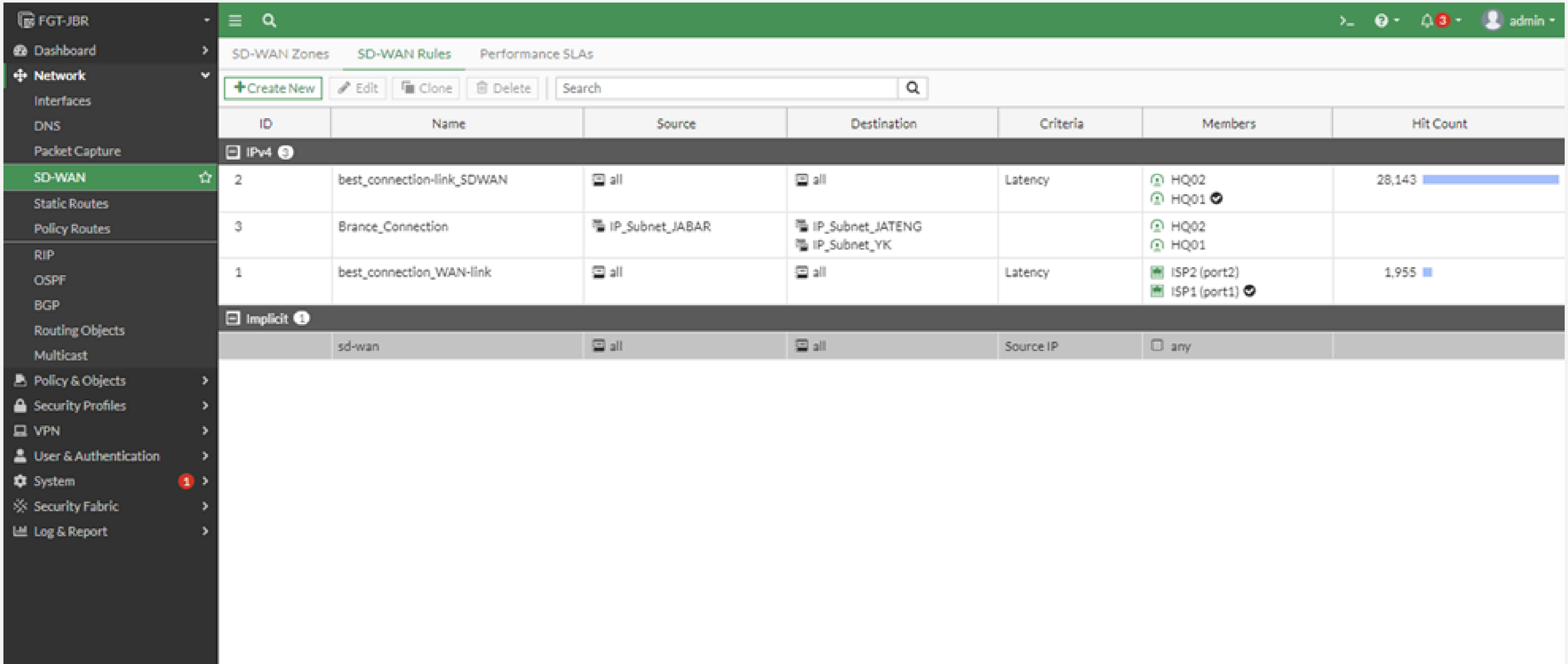
## Create Rules SD-WAN > SD-WAN Rules



# Network SD-WAN

FGT-JBR

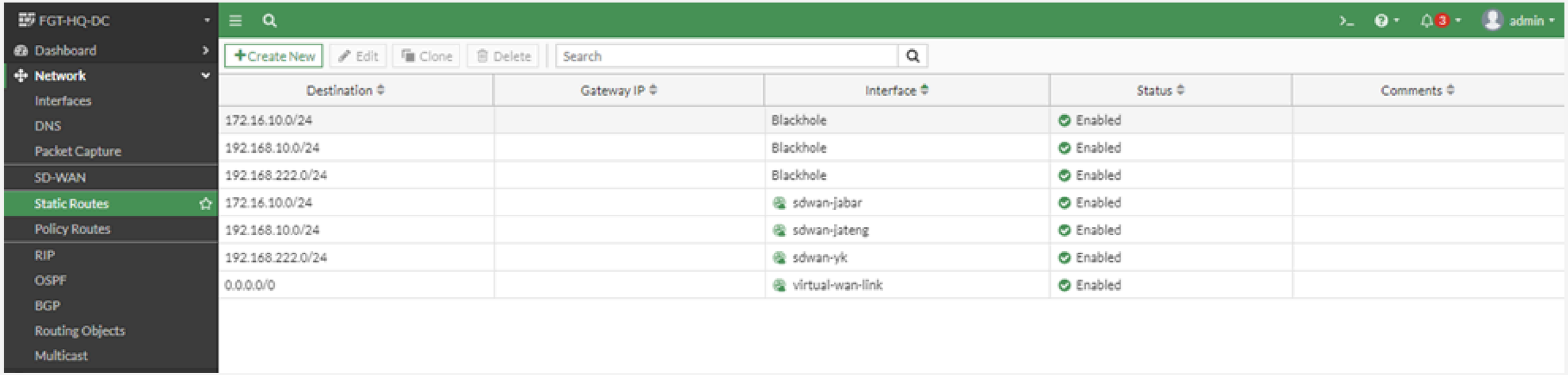
## Create Rules SD-WAN > SD-WAN Rules



# Network SD-WAN

FGT-HQ-DC

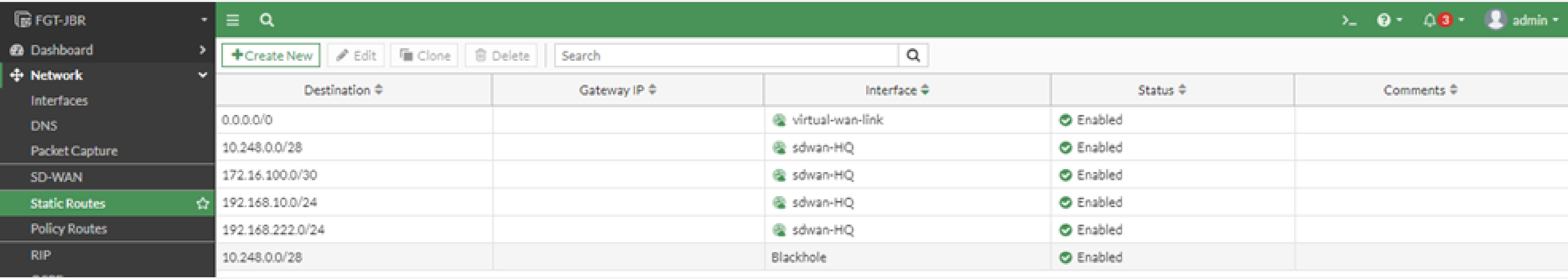
Network > Static Routes



# Network SD-WAN

FGT-JBR

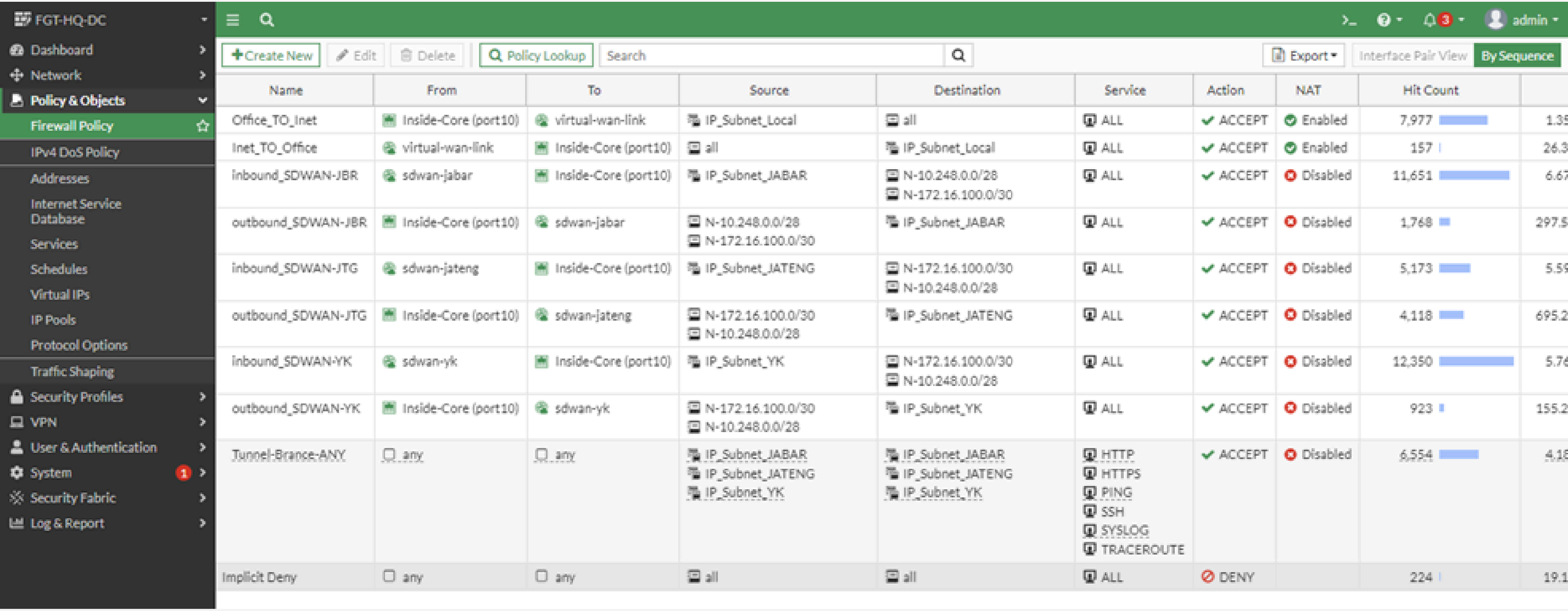
Network > Static Routes



# Network SD-WAN

FGT-HQ-DC

Policy. & Object > Firewall Policy

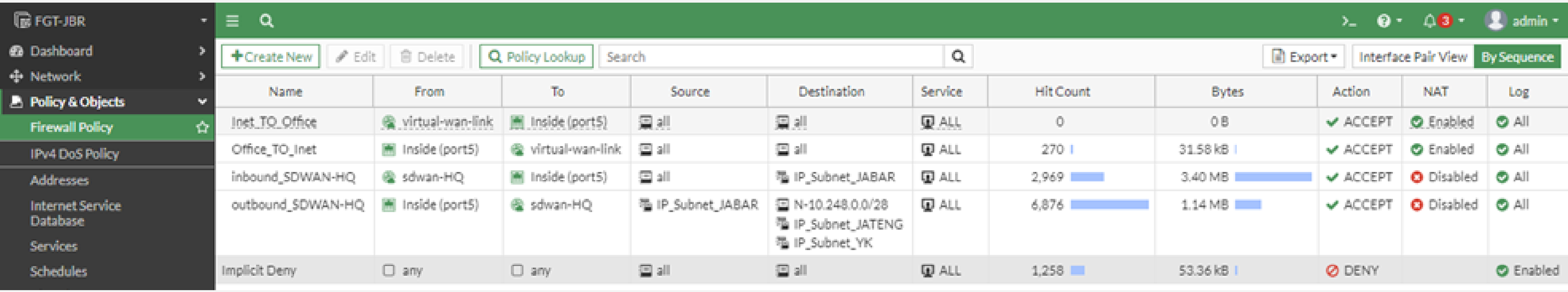



| Name | From | To | Source | Destination | Service | Action | NAT | Hit Count |
|---|---|---|---|---|---|---|---|---|
| Office_TO_Inet | Inside-Core (port10) | virtual-wan-link | IP_Subnet_Local | all | ALL | ACCEPT | Enabled | 7,977 |
| Inet_TO_Office | virtual-wan-link | Inside-Core (port10) | all | IP_Subnet_Local | ALL | ACCEPT | Enabled | 157 |
| Inbound_SDWAN-JBR | sdwan-jabar | Inside-Core (port10) | IP_Subnet_JABAR | N-10.248.0.0/28<br>N-172.16.100.0/30 | ALL | ACCEPT | Disabled | 11,651 |
| outbound_SDWAN-JBR | Inside-Core (port10) | sdwan-jabar | N-10.248.0.0/28<br>N-172.16.100.0/30 | IP_Subnet_JABAR | ALL | ACCEPT | Disabled | 1,768 |
| Inbound_SDWAN-JTG | sdwan-jateng | Inside-Core (port10) | IP_Subnet_JATENG | N-172.16.100.0/30<br>N-10.248.0.0/28 | ALL | ACCEPT | Disabled | 5,173 |
| outbound_SDWAN-JTG | Inside-Core (port10) | sdwan-jateng | N-172.16.100.0/30<br>N-10.248.0.0/28 | IP_Subnet_JATENG | ALL | ACCEPT | Disabled | 4,118 |
| Inbound_SDWAN-YK | sdwan-yk | Inside-Core (port10) | IP_Subnet_YK | N-172.16.100.0/30<br>N-10.248.0.0/28 | ALL | ACCEPT | Disabled | 12,350 |
| outbound_SDWAN-YK | Inside-Core (port10) | sdwan-yk | N-172.16.100.0/30<br>N-10.248.0.0/28 | IP_Subnet_YK | ALL | ACCEPT | Disabled | 923 |
| Tunnel-Brance-ANY | any | any | IP_Subnet_JABAR<br>IP_Subnet_JATENG<br>IP_Subnet_YK | IP_Subnet_JABAR<br>IP_Subnet_JATENG<br>IP_Subnet_YK | HTTP<br>HTTPS<br>PING<br>SSH<br>SYSLOG<br>TRACEROUTE | ACCEPT | Disabled | 6,554 |
| Implicit Deny | any | any | all | all | ALL | DENY | | 224 |

# Network SD-WAN

FGT-JBR

Policy. & Object > Firewall Policy



# Testing Connection

```
NAME    IP/MASK              GATEWAY          MAC                LPORT  RHOST:PORT
ServerF10.248.0.10/28        10.248.0.1       00:50:79:66:68:03  20164  127.0.0.1:20165
       fe80::250:79ff:fe66:6803/64

ServerFarm> ping 172.16.10.200 -t

84 bytes from 172.16.10.200 icmp_seq=1 ttl=61 time=7.185 ms
84 bytes from 172.16.10.200 icmp_seq=2 ttl=61 time=24.054 ms
84 bytes from 172.16.10.200 icmp_seq=3 ttl=61 time=28.907 ms
^C
ServerFarm> ping 192.168.10.200 -t

84 bytes from 192.168.10.200 icmp_seq=1 ttl=61 time=5.151 ms
84 bytes from 192.168.10.200 icmp_seq=2 ttl=61 time=7.355 ms
84 bytes from 192.168.10.200 icmp_seq=3 ttl=61 time=15.793 ms
^C
ServerFarm> ping 192.168.222.200 -t

84 bytes from 192.168.222.200 icmp_seq=1 ttl=61 time=9.027 ms
84 bytes from 192.168.222.200 icmp_seq=2 ttl=61 time=7.464 ms
84 bytes from 192.168.222.200 icmp_seq=3 ttl=61 time=14.381 ms
^C
ServerFarm> ping 8.8.8.8 -t

8.8.8.8 icmp_seq=1 timeout
8.8.8.8 icmp_seq=2 timeout
8.8.8.8 icmp_seq=3 timeout
^C
ServerFarm> ping 10.249.0.1 -t

84 bytes from 10.249.0.1 icmp_seq=1 ttl=255 time=2.203 ms
84 bytes from 10.249.0.1 icmp_seq=2 ttl=255 time=2.121 ms
84 bytes from 10.249.0.1 icmp_seq=3 ttl=255 time=2.095 ms
^C
ServerFarm>
```

```
NAME    IP/MASK              GATEWAY          MAC                LPORT  RHOST:PORT
Client-172.16.10.200/24      172.16.10.1      00:50:79:66:68:01  20108  127.0.0.1:20109
       fe80::250:79ff:fe66:6801/64

Client-Site1> ping 10.248.0.10 -t

84 bytes from 10.248.0.10 icmp_seq=1 ttl=61 time=27.547 ms
84 bytes from 10.248.0.10 icmp_seq=2 ttl=61 time=16.806 ms
84 bytes from 10.248.0.10 icmp_seq=3 ttl=61 time=9.487 ms
^C
Client-Site1> ping 8.8.8.8 -t

84 bytes from 8.8.8.8 icmp_seq=1 ttl=127 time=31.763 ms
84 bytes from 8.8.8.8 icmp_seq=2 ttl=127 time=36.377 ms
84 bytes from 8.8.8.8 icmp_seq=3 ttl=127 time=29.010 ms
^C
Client-Site1> ping 192.168.10.200 -t

84 bytes from 192.168.10.200 icmp_seq=1 ttl=61 time=7.012 ms
84 bytes from 192.168.10.200 icmp_seq=2 ttl=61 time=6.600 ms
84 bytes from 192.168.10.200 icmp_seq=3 ttl=61 time=6.943 ms
^C
Client-Site1> ping 192.168.222.200 -t

84 bytes from 192.168.222.200 icmp_seq=1 ttl=61 time=23.089 ms
84 bytes from 192.168.222.200 icmp_seq=2 ttl=61 time=4.983 ms
84 bytes from 192.168.222.200 icmp_seq=3 ttl=61 time=5.969 ms
^C
Client-Site1>
```

```
Client-Site1> trace 10.248.0.10
trace to 10.248.0.10, 8 hops max, press Ctrl+C to stop
 1   172.16.10.1    1.009 ms  0.718 ms  1.242 ms
 2   10.240.0.100    3.775 ms  2.653 ms  2.782 ms
 3   172.16.100.2    9.298 ms  11.742 ms  6.503 ms
 4   *10.248.0.10    6.448 ms (ICMP type:3, code:3, Destination port unreachable)
```

Back to Agenda

# Thank You

Email

**hello@reallygreatsite.com**

Social Media

**@reallygreatsite**

Call us

**123-456-789**