



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

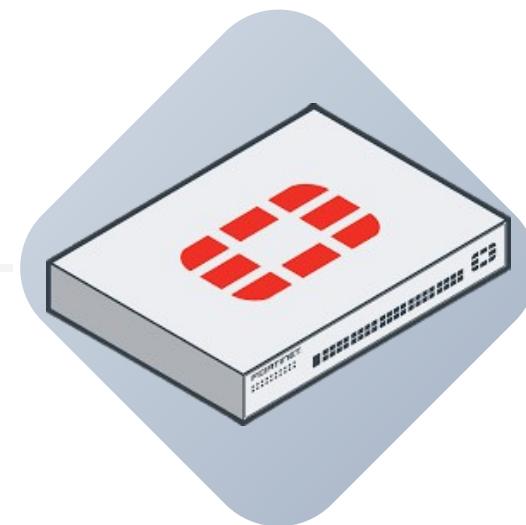
IPSec Tunnels SD-WAN	1	IP-Tunnel via ISP1 Site-To-Site	6
Kantor Pusat JKT	2	IP-Tunnel via ISP2 Dial-up	7
Brance Office: JABAR, JATENG, Yogya	3	Dapat berkomunikasi antar cabang via HQ	8
2 WAN	4	Server Farm Tidak terkoneksi internet	9
ISP1 Static IP & ISP2 Dynamic IP	5		

# Hardware Overview

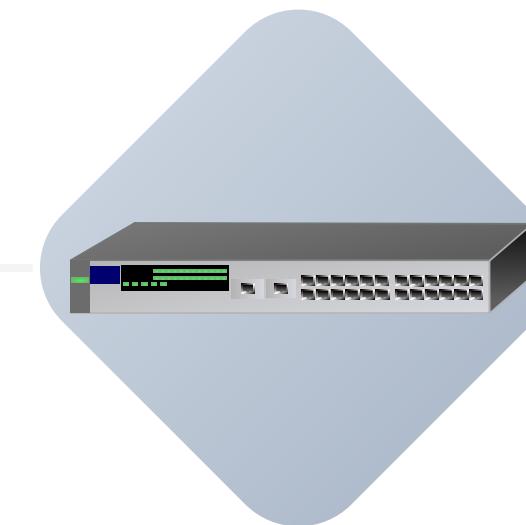
Briefly elaborate on what you want to discuss.



Router Mikrotik



Fortigate



Switch Cisco



End Device

# 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

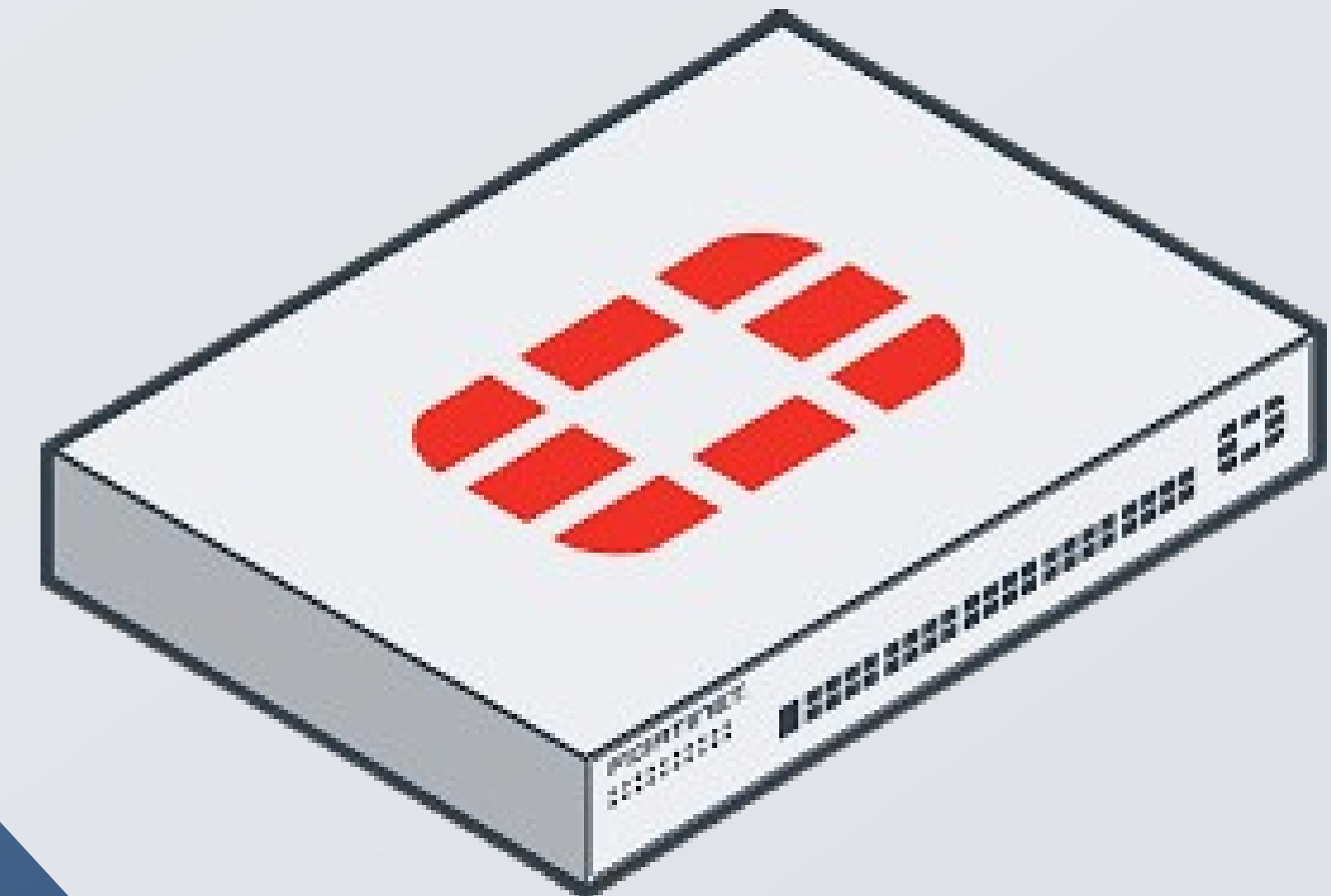
Version

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

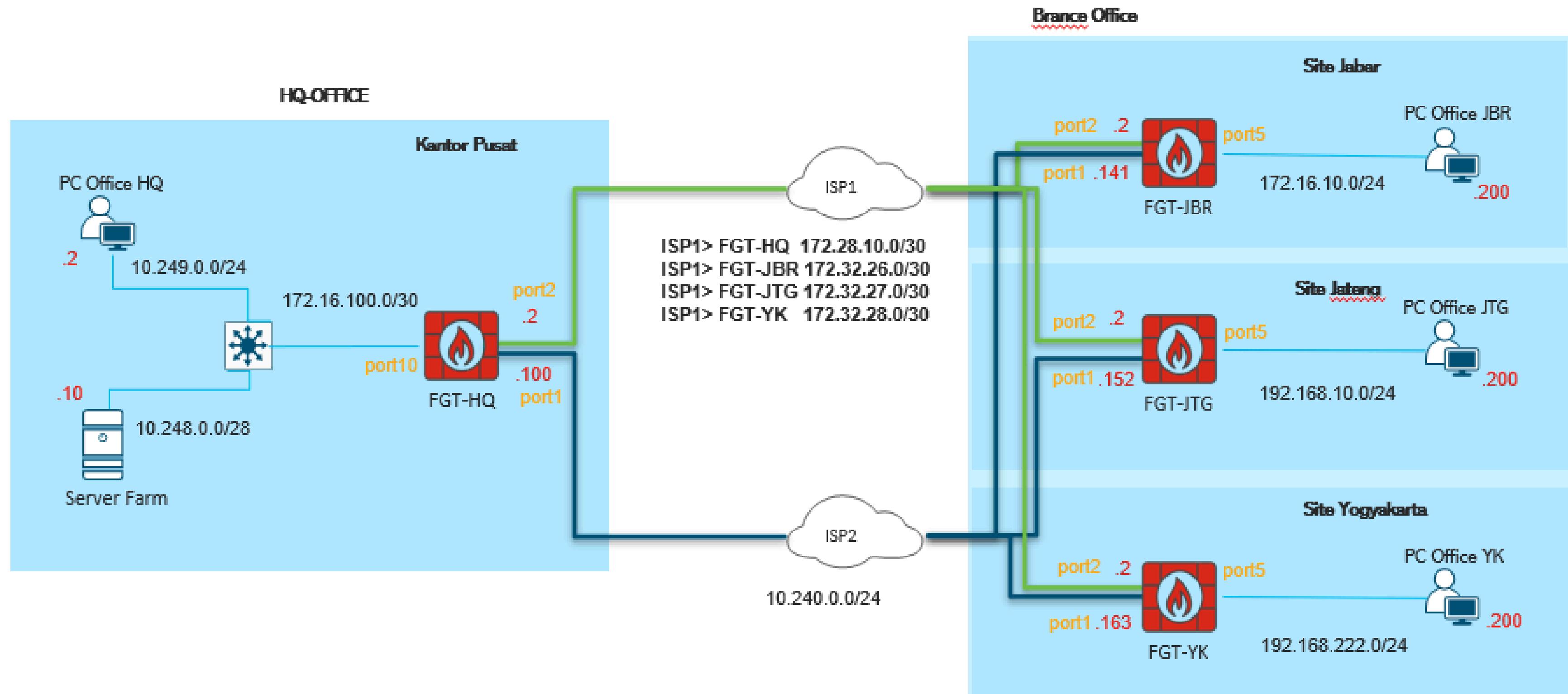
Elaborate on your second goal here.



## Implementasi

Elaborate on your third goal here.

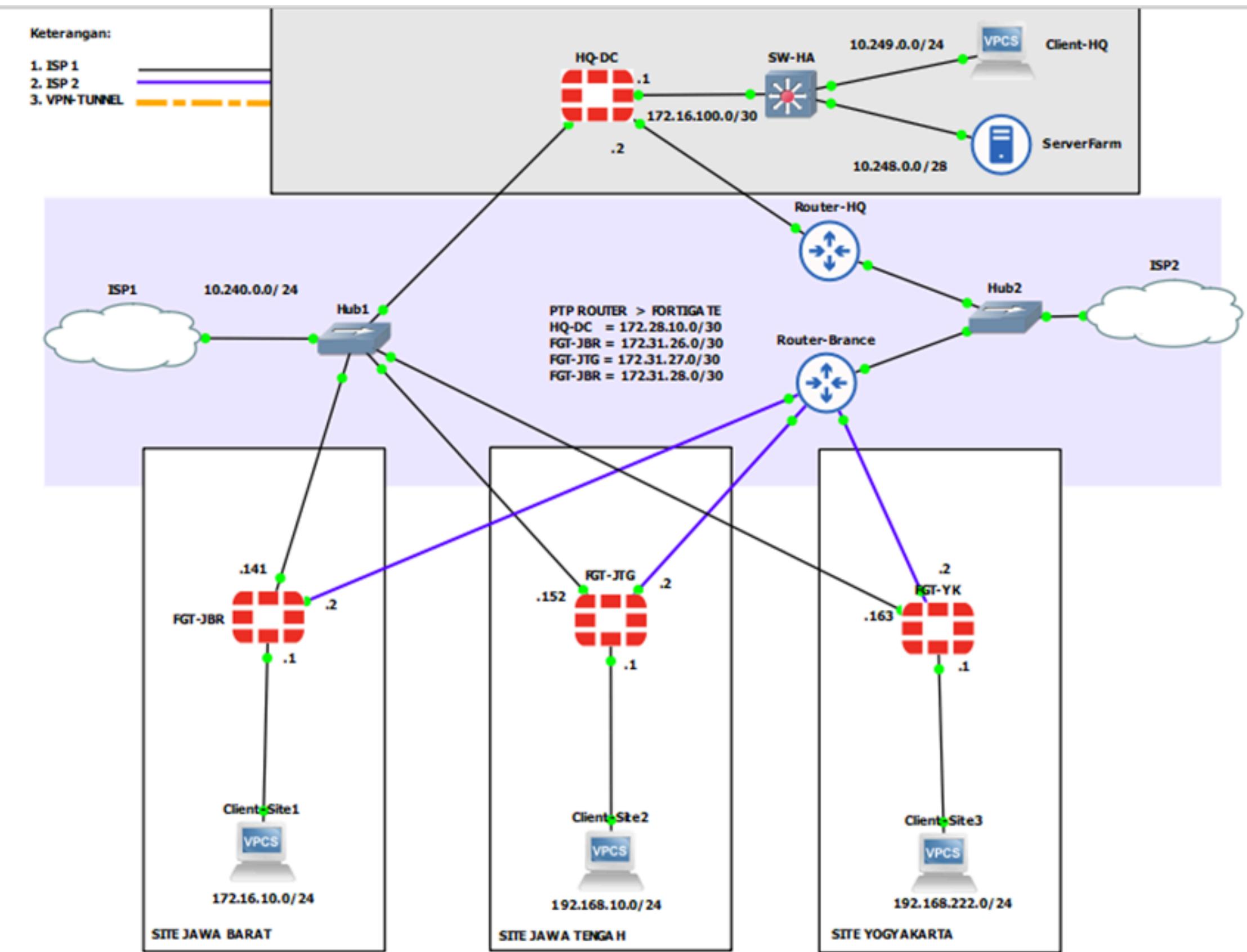
# Planning Design



# 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					
Icon	Name	Type	IP Address	Status	Action
Green	ISP1 (port1)	Physical Interface	10.240.0.100/255.255.255.0	PING HTTPS SSH <b>HTTP</b> FMG-Access	1
Green	ISP2 (port2)	Physical Interface	172.28.10.2/255.255.255.252	PING HTTPS SSH	1
Red	port3	Physical Interface	0.0.0.0/0.0.0		0
Red	port4	Physical Interface	0.0.0.0/0.0.0		0
Red	port5	Physical Interface	0.0.0.0/0.0.0		0
Red	port6	Physical Interface	0.0.0.0/0.0.0		0
Red	port7	Physical Interface	0.0.0.0/0.0.0		0
Red	port8	Physical Interface	0.0.0.0/0.0.0		0
Red	port9	Physical Interface	0.0.0.0/0.0.0		0
Green	toServerFarm (port10)	Physical Interface	172.16.100.1/255.255.255.252	PING	0

0 Security Rating Issues 0% (13) | Updated: 00:43:31 C -

# Network Interfaces

## Interface FGT-JBR

Physical Interface 10					
Icon	Name	Type	IP Address	Protocols	Count
	ISP1 (port1)		10.240.0.141/255.255.255.0	PING HTTPS SSH <b>HTTP</b>	0
	ISP2 (port2)		172.32.26.2/255.255.255.252	PING HTTPS SSH	0
	port3		0.0.0.0/0.0.0.0		0
	port4		0.0.0.0/0.0.0.0		0
	port5		172.16.10.1/255.255.255.0	PING	0
	port6		0.0.0.0/0.0.0.0		0
	port7		0.0.0.0/0.0.0.0		0
	port8		0.0.0.0/0.0.0.0		0
	port9		0.0.0.0/0.0.0.0		0
	port10		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.

The screenshot shows the Fortinet Giga-Manager interface for managing SD-WAN zones. The left sidebar navigation includes Network, SD-WAN, Static Routes, Policy Routes, RIP, OSPF, BGP, Routing Objects, Multicast, Policy & Objects, Security Profiles, VPN, User & Authentication, System, Security Fabric, and Log & Report. The SD-WAN menu is selected. The main content area displays two donut charts for Download and Upload bandwidth distribution across various interfaces (port1, port2, JBR01, JTG01, JBR02, JTG02). Below the charts is a table listing SD-WAN members and their interfaces, gateways, and bandwidth usage. A context menu is open over the 'sdwan-jateng' member, showing options to Create New, Edit, or Delete. The table data is as follows:

	Interfaces	Gateway	Download	Upload		
virtual-wan-link						
ISP1 (port1)	10.240.0.254	58.45 kbps	50.90 kbps			
ISP2 (port2)	172.28.10.1	26.64 kbps	24.67 kbps			
sdwan-jateng	JTG01	0.0.0	4.47 kbps	4.48 kbps	0	1
	JTG02	0.0.0	2.53 kbps	2.54 kbps	0	1
sdwan-jabar	JBR01	0.0.0	5.14 kbps	5.14 kbps	0	2
	JBR02	0.0.0	2.53 kbps	2.54 kbps	0	1
sdwan-yk	YK01	0.0.0	3.24 kbps	3.25 kbps	0	1
	YK02	0.0.0	1.91 kbps	1.92 kbps	0	1

# Network SD-WAN

FGT-JBR

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

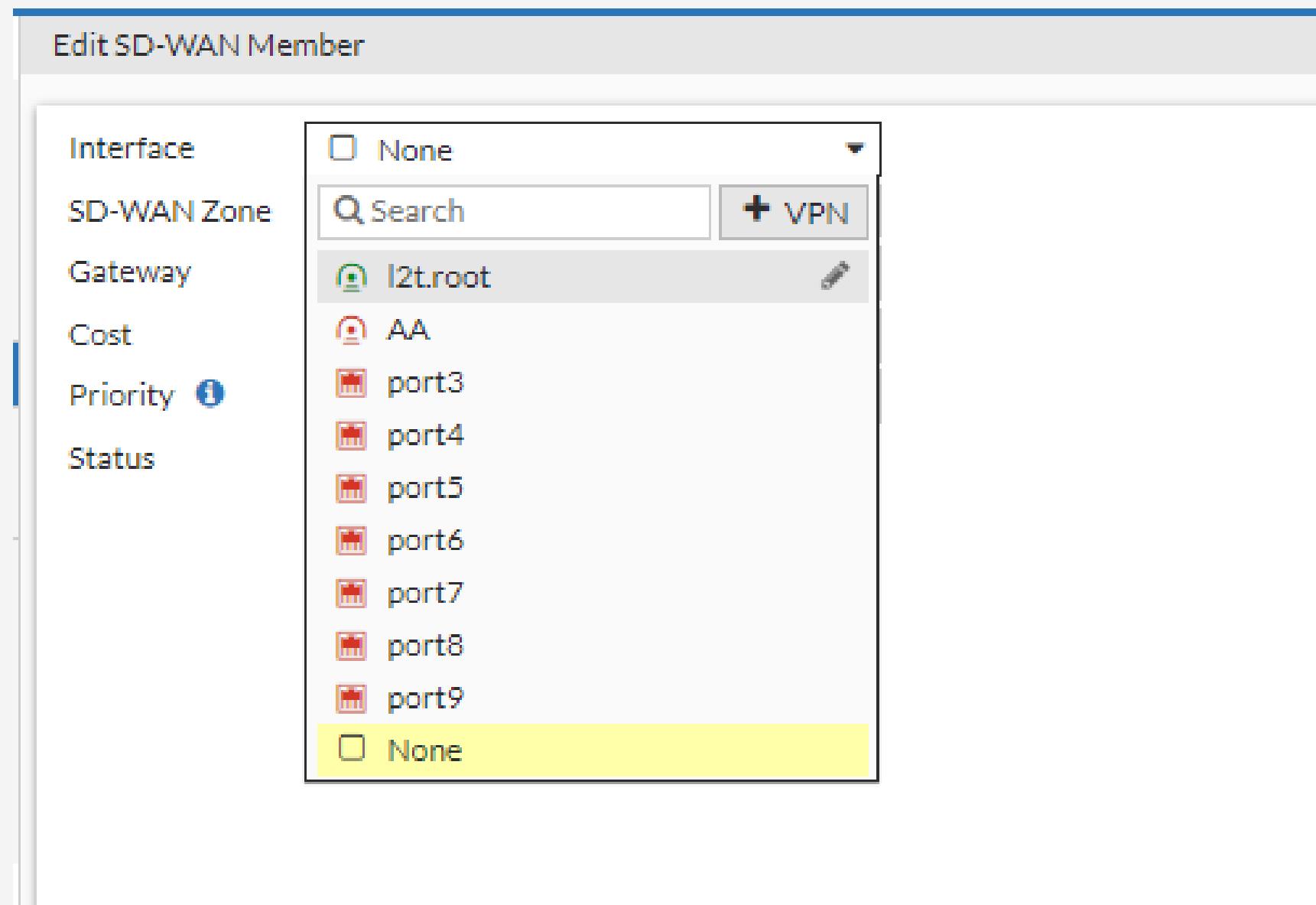
The screenshot shows the Fortinet GTR (Global Traffic Router) interface under the 'SD-WAN' tab. The left sidebar includes options like Dashboard, Network (Interfaces, DNS, Packet Capture), SD-WAN (selected), Static Routes, Policy Routes, RIP, OSPF, BGP, Routing Objects, Multicast, Policy & Objects, Security Profiles, VPN, User & Authentication, System (with a red notification dot), Security Fabric, and Log & Report. The main area has tabs for SD-WAN Zones, SD-WAN Rules, and Performance SLAs, with 'SD-WAN Zones' selected. Below are three donut charts: 'Bandwidth' (Download and Upload), each showing four segments (port1, port2, HQ02, HQ01) totaling 4. Below the charts is a table of SD-WAN zones:

	Interfaces	Gateway	Cost	Download	Upload
virtual-wan-link					
ISP1 (port1)	10.240.0.254	0	47.55 kbps	31.53 kbps	
ISP2 (port2)	172.32.26.1	0	12.86 kbps	10.49 kbps	
sdwan-HQ					
HQ02	0.0.0.0	0	2.55 kbps	2.55 kbps	
HQ01	0.0.0.0	0	5.16 kbps	5.16 kbps	

# 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

The screenshot shows the Fortinet GTR (Global Traffic Router) interface for managing IPsec Tunnels. The left sidebar navigation includes: Dashboard, Network, Policy & Objects, Security Profiles, VPN (Overlay Controller VPN, IPsec Tunnels selected), IPsec Wizard, IPsec Tunnel Template, SSL-VPN Portals, SSL-VPN Settings, SSL-VPN Clients, VPN Location Map, User & Authentication, System (with a red '1' notification), Security Fabric, and Log & Report.

The main content area displays a table of IPsec Tunnels:

Tunnel	Interface Binding	Status	Ref.
JBR01	ISP1 (port1)	Up	5
JBR02	ISP2 (port2)	Up	3
JTG01	ISP1 (port1)	Up	-
JTG02	ISP2 (port2)	Up	-
YK02	ISP1 (port1)	Up	-
YK02	ISP2 (port2)	Up	-

A modal window titled "Edit VPN Tunnel" is open for the tunnel named "JBR01". The configuration details are as follows:

- Name:** JBR01
- Comments:** VPN: JBR01 (Created by VPN wizard for SD-WAN)
- Network:** Remote Gateway: Static IP Address (10.240.0.141), Interface: port1
- Authentication:** Authentication Method: Pre-shared Key, IKE Version: 1, Mode: Main (ID protection)
- Phase 1 Proposal:** Algorithms: DES-MD5, DES-SHA1, Diffie-Hellman Groups: 14, 5
- XAUTH:** Type: Disabled
- Phase 2 Selectors:** Name: JBR01, Local Address: all, Remote Address: all

# 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

The screenshot shows the Fortinet FGT-JBR interface for creating a new IPsec Tunnel VPN. On the left, the navigation menu includes options like Dashboard, Network, Policy & Objects, Security Profiles, VPN, Overlay Controller VPN, and IPsec Tunnels. The IPsec Tunnels section is currently selected.

The main window displays a table with columns: Tunnel, Interface Binding, and Status. Two entries are listed: HQ01 (ISP1 (port1), Up) and HQ02 (ISP2 (port2), 1 dialup connection(s)).

To the right, a detailed configuration pane for VPN HQ01 is shown:

- Name:** HQ01
- Comments:** VPN: HQ01 (Created by VPN wizard for SD-WAN) // 44/255
- Network:** Remote Gateway: Static IP Address (10.240.0.100), Interface: port1
- Authentication:** Authentication Method: Pre-shared Key, IKE Version: 1, Mode: Main (ID protection)
- Phase 1 Proposal:** Algorithms: DES-MD5, DES-SHA1, Diffie-Hellman Groups: 14, 5
- XAUTH:** Type: Disabled
- Phase 2 Selectors:** A table with columns Name, Local Address, and Remote Address. One entry is listed: HQ01, all, all.

# 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

The screenshot shows the FortiGate Management UI for creating a new IPsec Tunnel VPN. The left sidebar navigation includes: FGT-JBR, Dashboard, Network, Policy & Objects, Security Profiles, VPN (selected), Overlay Controller VPN, and IPsec Tunnels.

The main interface displays a table of existing tunnels:

Tunnel	Interface Binding	Status
HQ01	ISP1 (port1)	Up
HQ02	ISP2 (port2)	1 dialup connection(s)

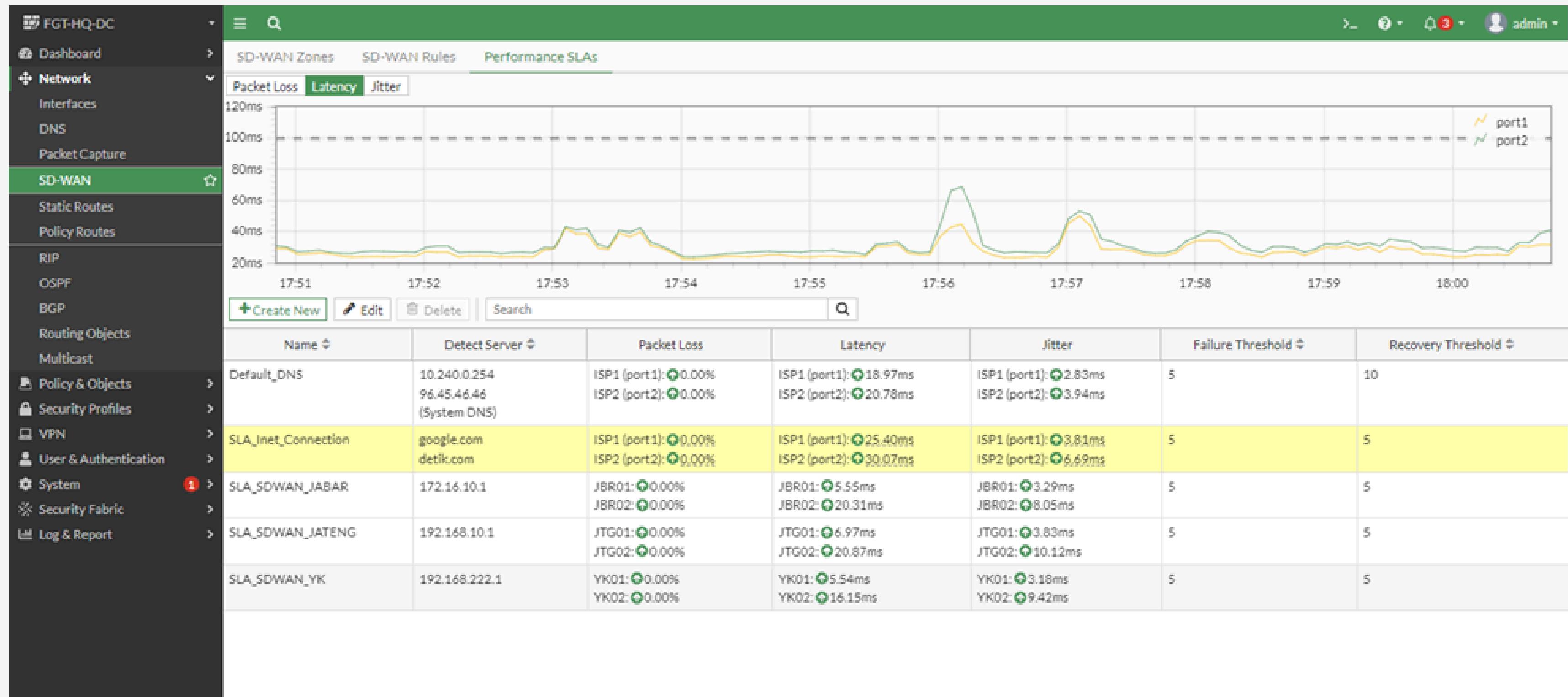
A modal window for creating a new tunnel is open, showing the configuration details:

- Name:** HQ01
- Comments:** VPN: HQ02 (Created by VPN wizard for SD-WAN) // 44/255
- Network:** Remote Gateway: Dialup User, Interface: port2
- Authentication:** Authentication Method: Pre-shared Key, IKE Version: 2
- Phase 1 Proposal:** Algorithms: DES-SHA1, Diffie-Hellman Groups: 14, 5
- Phase 2 Selectors:** Name: HQ02, Local Address: all, Remote Address: all

# Network SD-WAN

FGT-HQ-DC

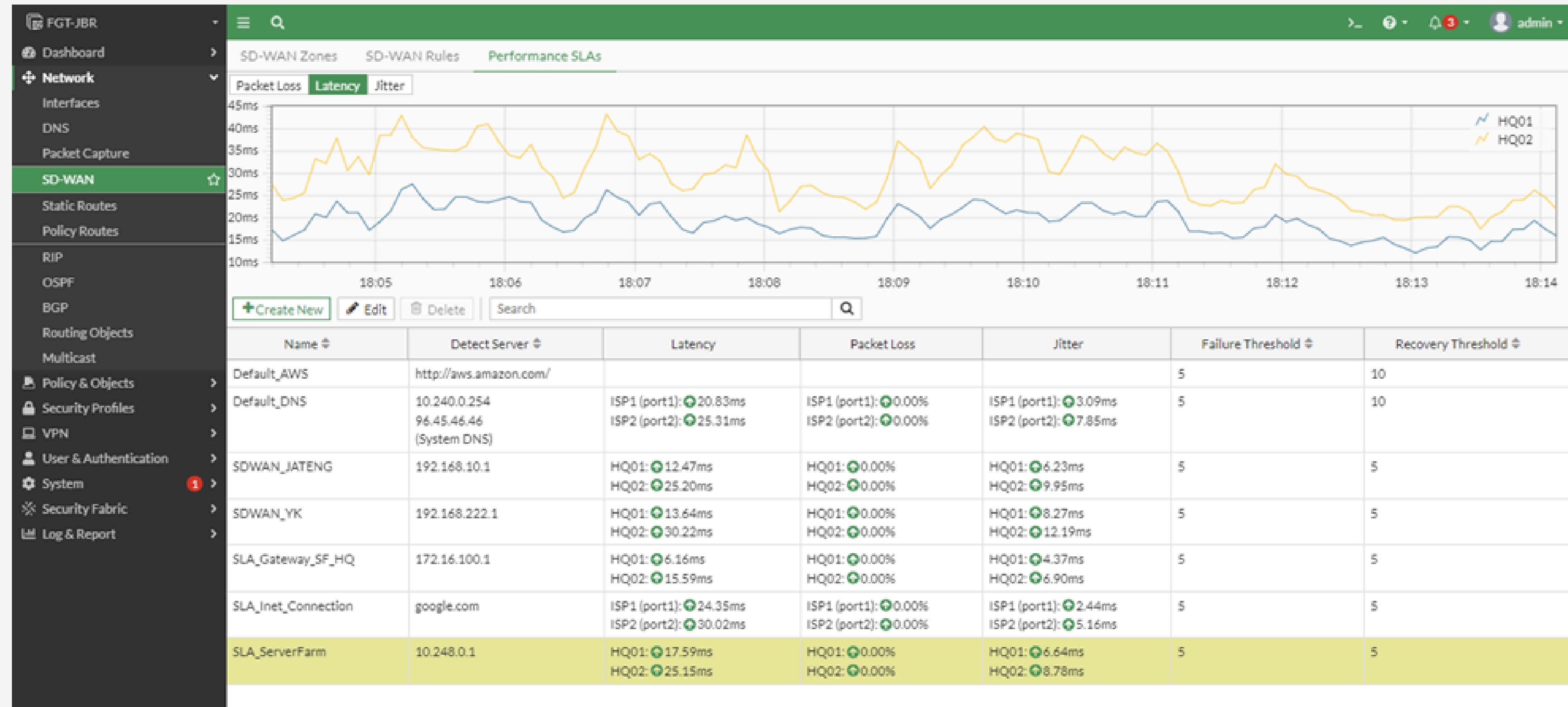
Create SLA SD-WAN > Performance SLAs



# Network SD-WAN

FGT-JBR

Create SLA SD-WAN > Performance SLAs



# Network SD-WAN

FGT-HQ-DC

Create Rules SD-WAN > SD-WAN Rules

The screenshot shows the Fortinet Giga-Manager interface for managing SD-WAN rules. The left sidebar navigation includes Network, SD-WAN, Policy Objects, and System sections. The main content area displays a table of SD-WAN Rules with the following data:

ID	Name	Source	Destination	Criteria	Members	Hit Count
4	best_connection_SDWAN-JBR	ServerFarm N-10.248.0.0/28	IP_Subnet_JABAR	Latency	JBR01 JBR02	41,187
3	best_connection_SDWAN-JTG	ServerFarm N-10.248.0.0/28	IP_Subnet_JATENG	Latency	JTG01 JTG02	32,605
5	best_connection_SDWAN-YK	N-10.248.0.0/28 ServerFarm	IP_Subnet_YK	Latency	YK01 YK02	45,621
6	Inter-Brance01	IP_Subnet_JABAR IP_Subnet_JATENG IP_Subnet_YK	IP_Subnet_JABAR IP_Subnet_JATENG IP_Subnet_YK		JTG01 JTG02 JBR01 JBR02 +2	15,429
1	best_connection_WAN-link	all	all	Latency	ISP2 (port2) ISP1 (port1)	42,297
2	bandwidth_connection_WAN	all	all	Bandwidth	ISP2 (port2) ISP1 (port1)	590

A search bar at the bottom allows filtering by SD-WAN rule name.

# Network SD-WAN

FGT-JBR

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

The screenshot shows the Fortinet Giga-Manager interface for managing SD-WAN rules. The left sidebar navigation includes Network (Interfaces, DNS, Packet Capture), SD-WAN, Static Routes, Policy Routes, RIP, OSPF, BGP, Routing Objects, Multicast, Policy & Objects, Security Profiles, VPN, User & Authentication, System (with a red notification dot), Security Fabric, and Log & Report.

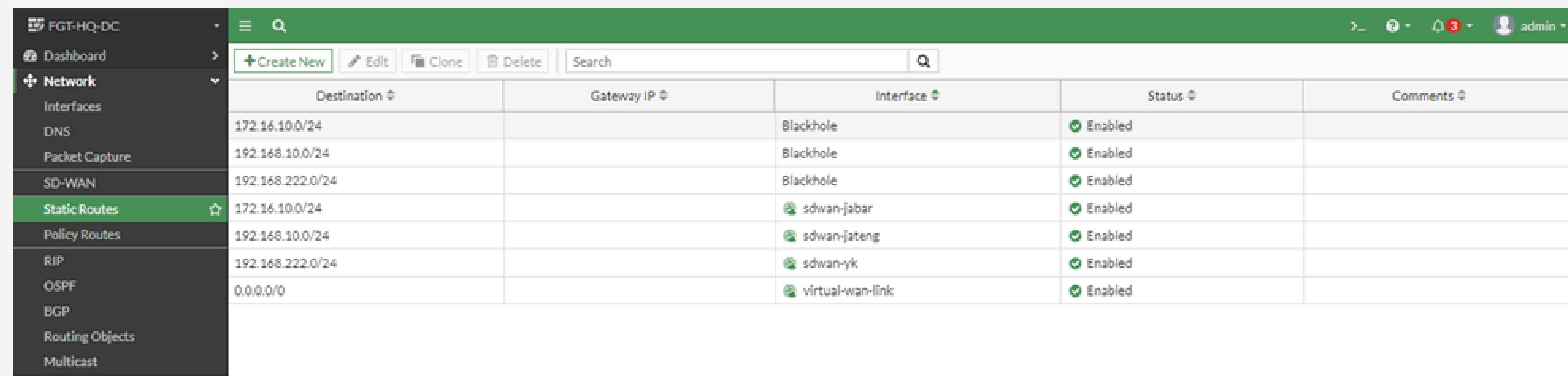
The main content area displays the SD-WAN Rules table. The table has columns: ID, Name, Source, Destination, Criteria, Members, and Hit Count. There are two sections: IPv4 (3 rules) and Implicit (1 rule).

ID	Name	Source	Destination	Criteria	Members	Hit Count
2	best_connection-link_SDWAN	<input type="checkbox"/> all	<input type="checkbox"/> all	Latency	<span>HQ02</span> <span>HQ01</span>	28,143
3	Brance_Connection	<input type="checkbox"/> IP_Subnet_JATENG	<input type="checkbox"/> IP_Subnet_YK		<span>HQ02</span> <span>HQ01</span>	
1	best_connection_WAN-link	<input type="checkbox"/> all	<input type="checkbox"/> all	Latency	<span>ISP2 (port2)</span> <span>ISP1 (port1)</span>	1,955
	sd-wan	<input type="checkbox"/> all	<input type="checkbox"/> all	Source IP	<input type="checkbox"/> any	

# Network SD-WAN

FGT-HQ-DC

Network > Static Routes



The screenshot shows the Fortinet Giga-Analyzer interface for managing static routes. The left sidebar navigation includes options like Dashboard, Network Interfaces, DNS, Packet Capture, SD-WAN, Static Routes (which is currently selected), Policy Routes, RIP, OSPF, BGP, Routing Objects, and Multicast. The main content area displays a table of static routes with columns for Destination, Gateway IP, Interface, Status, and Comments. There are buttons for Create New, Edit, Clone, Delete, and Search.

Destination	Gateway IP	Interface	Status	Comments
172.16.10.0/24		Blackhole	<input checked="" type="checkbox"/> Enabled	
192.168.10.0/24		Blackhole	<input checked="" type="checkbox"/> Enabled	
192.168.222.0/24		Blackhole	<input checked="" type="checkbox"/> Enabled	
172.16.10.0/24		sdwan-jabar	<input checked="" type="checkbox"/> Enabled	
192.168.10.0/24		sdwan-jateng	<input checked="" type="checkbox"/> Enabled	
192.168.222.0/24		sdwan-yk	<input checked="" type="checkbox"/> Enabled	
0.0.0.0/0		virtual-wan-link	<input checked="" type="checkbox"/> Enabled	

# Network SD-WAN

# FGT-JBR

## Network > Static Routes

# Network SD-WAN

FGT-HQ-DC

## Policy & Object > Firewall Policy

FGT-HQ-DC

Dashboard >

Network >

**Policy & Objects** >

**Firewall Policy**

IPv4 DoS Policy

Addresses

Internet Service

Database

Services

Schedules

Virtual IPs

IP Pools

Protocol Options

Traffic Shaping

Security Profiles

VPN

User & Authentication

System

1

Security Fabric

Log & Report

Q 3 admin

Create New Edit Delete Policy Lookup Search Export Interface Pair View By Sequence

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 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 N-172.16.100.0/30	IP_Subnet_JABAR	ALL	✓ ACCEPT	✗ Disabled	1,769
inbound_SDWAN-JTG	sdwan-jateng	Inside-Core (port10)	IP_Subnet_JATEG	N-172.16.100.0/30 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 N-10.248.0.0/28	IP_Subnet_JATEG	ALL	✓ ACCEPT	✗ Disabled	4,118
Inbound_SDWAN-YK	sdwan-yk	Inside-Core (port10)	IP_Subnet_YK	N-172.16.100.0/30 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 N-10.248.0.0/28	IP_Subnet_YK	ALL	✓ ACCEPT	✗ Disabled	923
Tunnel-Branco-ANY	any	any	IP_Subnet_JABAR IP_Subnet_JATEG IP_Subnet_YK	IP_Subnet_JABAR IP_Subnet_JATEG IP_Subnet_YK	HTTP HTTPS PING SSH SYSLOG TRACEROUTE	✓ ACCEPT	✗ Disabled	6,554
Implicit Deny	any	any	all	all	ALL	✗ DENY		224

# Network SD-WAN

FGT-JBR

Policy & Object > Firewall Policy

The screenshot shows the Firewall Policy list interface. The left sidebar navigation includes Dashboard, Network, Policy & Objects (selected), Firewall Policy (selected), IPv4 DoS Policy, Addresses, Internet Service Database, Services, and Schedules. The main content area displays a table with columns: Name, From, To, Source, Destination, Service, Hit Count, Bytes, Action, NAT, and Log. The table lists the following policies:

Name	From	To	Source	Destination	Service	Hit Count	Bytes	Action	NAT	Log
Inet_TO_Office	virtual-wan-link	Inside (port5)	<input type="checkbox"/> all	<input type="checkbox"/> all	<input checked="" type="checkbox"/> ALL	0	0 B	ACCEPT	Enabled	All
Office_TO_Inet	Inside (port5)	virtual-wan-link	<input type="checkbox"/> all	<input type="checkbox"/> all	<input checked="" type="checkbox"/> ALL	270	31.58 kB	ACCEPT	Enabled	All
inbound_SDWAN-HQ	sdwan-HQ	Inside (port5)	<input type="checkbox"/> all	<input checked="" type="checkbox"/> IP_Subnet_JABAR	<input checked="" type="checkbox"/> ALL	2,969	3.40 MB	ACCEPT	Disabled	All
outbound_SDWAN-HQ	Inside (port5)	sdwan-HQ	<input checked="" type="checkbox"/> IP_Subnet_JABAR	<input checked="" type="checkbox"/> N-10.248.0.0/28 <input checked="" type="checkbox"/> IP_Subnet_JATEENG <input checked="" type="checkbox"/> IP_Subnet_YK	<input checked="" type="checkbox"/> ALL	6,876	1.14 MB	ACCEPT	Disabled	All
Implicit Deny	<input type="checkbox"/> any	<input type="checkbox"/> any	<input type="checkbox"/> all	<input type="checkbox"/> all	<input checked="" type="checkbox"/> ALL	1,258	53.36 kB	DENY		Enabled

# Testing Connection

```
NAME    IP/MASK          GATEWAY      MAC           LPORT   RHOST:PORT
ServerF1 10.248.0.10/28  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-1 172.16.10.200/24  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**