



## SIMULATION/LAB FORTIGATE FUNDAMENTAL

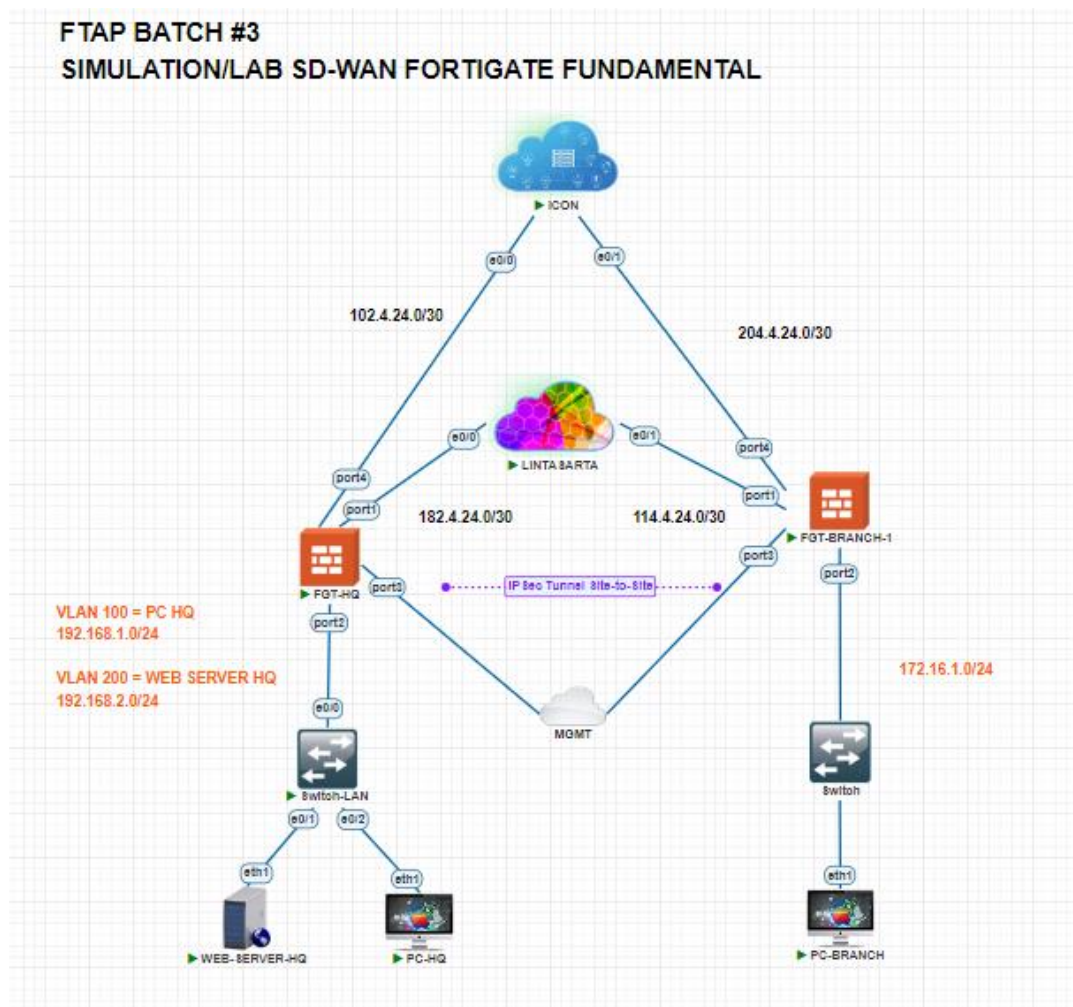
Implementation IPSec Tunnel Site-to-Site With SD-WAN Method

- ✓ Interface
- ✓ IPSec Tunnel
- ✓ SD-WAN Tunnel
- ✓ Static Route
- ✓ Firewall Policy

Annisa Hadita

Mentor: Dito Prasetya

## 1. Topology



## 2. Task

Lab selanjutnya bertujuan untuk membuat terowongan IPsec Site-to-Site menggunakan metode SD-WAN, dengan membangun jalur aman (tunnel) melalui internet publik untuk mengamankan komunikasi antara dua jaringan yang berbeda. Pada lab ini, menggunakan dua ISP untuk meningkatkan fleksibilitas dan efisiensi jaringan, serta memastikan konektivitas yang lebih baik jika salah satu ISP mengalami gangguan. Lab ini dilakukan agar Web-server dan PC-HQ dapat berkomunikasi dengan PC-Branch, dan sebaliknya, dengan aman dan efisien.

## #Configure Interface

Konfigurasi ini dilakukan untuk mengatur interface port4 dan port1 pada perangkat FGT-HQ dan FGT-BRANCH, dengan menambahkan alamat IP dan subnet mask.

### FGT-HQ

The screenshot shows the FortiGate VM64-KVM configuration page for FGT-HQ. The left sidebar shows the 'Network' menu with 'Interfaces' selected. The main area displays a table of interfaces:

Name	Type	Members	IP/Netmask	Administrative Access	DHCP Clients
TO ICON (port4)	Physical Interface		102.4.24.2/255.255.255.252	PING HTTPS SSH HTTP FMG-Access	
TO BRANCH ICON	Tunnel Interface		0.0.0.0/0.0.0.0		
TO LA (port1)	Physical Interface		182.4.24.2/255.255.255.252	PING HTTPS SSH HTTP FMG-Access	
TO BRANCH LA	Tunnel Interface		0.0.0.0/0.0.0.0		

### FGT-Branch

The screenshot shows the FortiGate VM64-KVM configuration page for FGT-BRANCH. The left sidebar shows the 'Network' menu with 'Interfaces' selected. The main area displays a table of interfaces:

Name	Type	Members	IP/Netmask	Administrative Access	DHCP Clients
TO ICON (port4)	Physical Interface		204.4.24.2/255.255.255.252	FMG-Access PING HTTPS SSH HTTP FMG-Access	
TO HQ ICON	Tunnel Interface		0.0.0.0/0.0.0.0		
TO LA (port1)	Physical Interface		114.4.24.2/255.255.255.252	PING HTTPS SSH HTTP FMG-Access	
TO HQ LA	Tunnel Interface		0.0.0.0/0.0.0.0		

## #Configure IPSec Tunnel

Konfigurasi ini dibuat untuk menyediakan jalur komunikasi yang aman dan terenkripsi antara dua jaringan yang berbeda, misalnya antara HQ dan Branch.

### FGT-HQ (TO BRANCH ICON)

The screenshot shows the 'Edit VPN Tunnel' configuration page for a tunnel named 'TO BRANCH ICON'. The left sidebar contains the navigation menu with 'VPN' > 'IPsec Tunnels' selected. The main configuration area is divided into sections: 'Name' (TO BRANCH ICON), 'Comments' (empty), 'Network' (IP Version: IPv4, Remote Gateway: Static IP Address, IP Address: 204.4.24.2, Interface: TO ICON (port4)), 'Local Gateway' (disabled), 'Mode Config' (disabled), 'NAT Traversal' (Enable, Disable, Forced), 'Dead Peer Detection' (Disable, On Idle, On Demand), 'DPD retry count' (3), 'DPD retry interval' (20 s), and 'Forward Error Correction' (Egress, Ingress). The 'Advanced...' button is visible at the bottom. The right sidebar shows 'Additional Information' with links to API Preview, References, and documentation.

The screenshot shows the 'Authentication' and 'Phase 1 Proposal' configuration for the 'TO BRANCH ICON' tunnel. The 'Authentication' section includes 'Method' (Pre-shared Key), 'Pre-shared Key' (masked), 'IKE Version' (1, 2), and 'Mode' (Aggressive, Main (ID protection)). The 'Phase 1 Proposal' section shows 'Algorithms' (DES-SHA256) and 'Diffie-Hellman Groups' (14, 5). The 'XAUTH' section shows 'Type: Disabled'. The 'Phase 2 Selectors' table lists the tunnel name and addresses.

Name	Local Address	Remote Address
TO BRANCH ICON	all	all

The screenshot shows the 'Phase 1 Proposal' configuration for the 'TO BRANCH ICON' tunnel. The 'Encryption' is set to DES and 'Authentication' is set to SHA256. The 'Diffie-Hellman Groups' are selected as 14, 5, 2, and 1. The 'Key Lifetime (seconds)' is set to 86400. The 'Local ID' field is empty. The 'XAUTH' section shows 'Type: Disabled'. The 'Phase 2 Selectors' table is empty.

FGT-HQ

Dashboard

Network

Policy & Objects

Security Profiles

VPN

Overlay Controller VPN

**IPsec Tunnels**

IPsec Wizard

IPsec Tunnel Template

SSL-VPN Portals

SSL-VPN Settings

SSL-VPN Clients

VPN Location Map

User & Authentication

System

Security Fabric

Log & Report

FGT-HQ

Search

Edit VPN Tunnel

Phase 2 Selectors

Name	Local Address	Remote Address
TO BRANCH ICON	all	all

Edit Phase 2

Name: TO BRANCH ICON

Comments: Comments

Local Address: Named Address all

Remote Address: Named Address all

Advanced...

Phase 2 Proposal Add

Encryption: DES Authentication: SHA256

Enable Replay Detection ☒

Enable Perfect Forward Secrecy (PFS) ☒

Diffie-Hellman Group

<input type="checkbox"/> 32	<input type="checkbox"/> 31	<input type="checkbox"/> 30	<input type="checkbox"/> 29	<input type="checkbox"/> 28	<input type="checkbox"/> 27
<input type="checkbox"/> 21	<input type="checkbox"/> 20	<input type="checkbox"/> 19	<input type="checkbox"/> 18	<input type="checkbox"/> 17	<input type="checkbox"/> 16
<input type="checkbox"/> 15	<input checked="" type="checkbox"/> 14	<input checked="" type="checkbox"/> 5	<input type="checkbox"/> 2	<input type="checkbox"/> 1	

OK Cancel

Additional Information

API Preview

References

IPsec VPNs

Guides

IPsec VPN Cookbook Recipes

VPN Setup on FortiClient

Configuring an IPsec VPN Connection

Documentation

Online Help

Video Tutorials

FGT-HQ

Dashboard

Network

Policy & Objects

Security Profiles

VPN

Overlay Controller VPN

**IPsec Tunnels**

IPsec Wizard

IPsec Tunnel Template

SSL-VPN Portals

SSL-VPN Settings

SSL-VPN Clients

VPN Location Map

User & Authentication

System

Security Fabric

Log & Report

FGT-HQ

Search

Edit VPN Tunnel

Remote Address: Named Address all

Advanced...

Phase 2 Proposal Add

Encryption: DES Authentication: SHA256

Enable Replay Detection ☒

Enable Perfect Forward Secrecy (PFS) ☒

Diffie-Hellman Group

<input type="checkbox"/> 32	<input type="checkbox"/> 31	<input type="checkbox"/> 30	<input type="checkbox"/> 29	<input type="checkbox"/> 28	<input type="checkbox"/> 27
<input type="checkbox"/> 21	<input type="checkbox"/> 20	<input type="checkbox"/> 19	<input type="checkbox"/> 18	<input type="checkbox"/> 17	<input type="checkbox"/> 16
<input type="checkbox"/> 15	<input checked="" type="checkbox"/> 14	<input checked="" type="checkbox"/> 5	<input type="checkbox"/> 2	<input type="checkbox"/> 1	

Local Port: All ☒

Remote Port: All ☒

Protocol: All ☒

Auto-negotiate ☒

Autokey Keep Alive ☐

Key Lifetime: Seconds

Seconds: 43200

OK Cancel

Additional Information

API Preview

References

IPsec VPNs

Guides

IPsec VPN Cookbook Recipes

VPN Setup on FortiClient

Configuring an IPsec VPN Connection

Documentation

Online Help

Video Tutorials

## FGT-HQ (TO BRANCH LA)

FGT-HQ

Dashboard

Network

Policy & Objects

Security Profiles

VPN

Overlay Controller VPN

**IPsec Tunnels**

IPsec Wizard

IPsec Tunnel Template

SSL-VPN Portals

SSL-VPN Settings

SSL-VPN Clients

VPN Location Map

User & Authentication

System

Security Fabric

Log & Report

FGT-HQ

Search

Edit VPN Tunnel

Name: TO BRANCH LA

Comments: Comments

Network

IP Version: IPv4

Remote Gateway: Static IP Address

IP Address: 114.4.24.2

Interface: TO LA (port1)

Local Gateway: ☐

Mode Config: ☐

NAT Traversal: Enable Disable Forced

Dead Peer Detection: Disable On Idle On Demand

DPD retry count: 3

DPD retry interval: 20 s

Forward Error Correction: Egress ☐ Ingress ☐

Advanced...

OK Cancel

Additional Information

API Preview

References

IPsec VPNs

Guides

IPsec VPN Cookbook Recipes

VPN Setup on FortiClient

Configuring an IPsec VPN Connection

Documentation

Online Help

Video Tutorials



The screenshot displays the Fortinet FortiGate web interface for configuring an IPsec tunnel. The left sidebar shows the navigation menu with categories like Dashboard, Network, Policy & Objects, Security Profiles, VPN, User & Authentication, System, Security Fabric, and Log & Report. The main area is titled "Edit VPN Tunnel".

**Phase 2 Proposal Configuration:**

- Remote Address:** Named Addr [all]
- Advanced... Phase 2 Proposal:** Add
- Encryption:** DES
- Authentication:** SHA256
- Enable Replay Detection:** ☒
- Enable Perfect Forward Secrecy (PFS):** ☒

<input type="checkbox"/> 32	<input type="checkbox"/> 31	<input type="checkbox"/> 30	<input type="checkbox"/> 29	<input type="checkbox"/> 28	<input type="checkbox"/> 27
<input type="checkbox"/> 21	<input type="checkbox"/> 20	<input type="checkbox"/> 19	<input type="checkbox"/> 18	<input type="checkbox"/> 17	<input type="checkbox"/> 16
<input type="checkbox"/> 15	<input checked="" type="checkbox"/> 14	<input checked="" type="checkbox"/> 5	<input type="checkbox"/> 2	<input type="checkbox"/> 1	
- Diffie-Hellman Group:** (Same options as PFS)
- Local Port:** All ☒
- Remote Port:** All ☒
- Protocol:** All ☒
- Auto-negotiate:** ☒
- Autokey Keep Alive:** ☐
- Key Lifetime:** Seconds
- Seconds:** 43200

**Additional Information:**

- API Preview
- References
- IPsec VPNs Guides
  - IPsec VPN Cookbook Recipes
  - VPN Setup on FortiClient
  - Configuring an IPsec VPN Connection
- Documentation
  - Online Help
  - Video Tutorials

At the bottom, there are "OK" and "Cancel" buttons.

v70.14

Dashboard
Network
Policy & Objects
Security Profiles
VPN
Overlay Controller VPN
IPsec Tunnels
IPsec Wizard
IPsec Tunnel Template
SSL-VPN Portals
SSL-VPN Settings
SSL-VPN Clients
VPN Location Map
User & Authentication
System
Security Fabric
Log & Report

Edit VPN Tunnel
Name: TO HQ ICON
Comments:
Network
IP Version: IPv4
Remote Gateway: Static IP Address
IP Address: 102.4.24.2
Interface: TO ICON (port4)
Local Gateway:
Mode Config:
NAT Traversal: Enable | Disable | Forced
Dead Peer Detection: Disable | On Idle | On Demand
DPD retry count: 3
DPD retry interval: 20 s
Forward Error Correction: Egress | Ingress
Advanced...

Additional Information
API Preview
References
IPsec VPNs
Guides
IPsec VPN Cookbook Recipes
VPN Setup on FortiClient
Configuring an IPsec VPN Connection
Documentation
Online Help
Video Tutorials

The screenshot displays the FortiGate web interface for configuring an IPsec Tunnel. The left sidebar shows the navigation menu with 'IPsec Tunnels' selected. The main area is titled 'Edit VPN Tunnel' and shows the configuration for 'IKE Version: 1, Mode: Main (ID protection)'. The 'Phase 1 Proposal' section is highlighted in yellow and includes settings for Encryption (DES), Authentication (SHA256), and Diffie-Hellman Groups (32, 31, 30, 29, 28, 27, 21, 20, 19, 18, 17, 16, 15, 14, 5, 2, 1). The 'Key Lifetime (seconds)' is set to 86400. The 'Local ID' field is empty. The 'XAUTH' section shows 'Type: Disabled'. The 'Phase 2 Selectors' table shows 'Name' as 'TO BRANCH ICON', 'Local Address' as 'all', and 'Remote Address' as 'all'. The right sidebar contains 'Additional Information' with links to 'API Preview', 'References', 'IPsec VPNs', 'Guides', 'IPsec VPN Cookbook Recipes', 'VPN Setup on FortiClient', 'Configuring an IPsec VPN Connection', 'Documentation', 'Online Help', and 'Video Tutorials'.

The screenshot displays the Fortinet FortiGate Web User Interface (WUI) for configuring an IPsec tunnel. The left sidebar shows the navigation menu with options like 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, Security Fabric, Log & Report, and Fortinet logo.

The main content area is titled "Edit VPN Tunnel". It contains several sections:

- Phase 2 Selectors**: A table with columns Name, Local Address, and Remote Address. The entry "TO BRANCH ICON" has both local and remote addresses set to "all".
- Edit Phase 2**: Fields for Name ("TO BRANCH ICON"), Comments, Local Address (Named Address dropdown), and Remote Address (Named Address dropdown). There are also checkboxes for Advanced... and Add.
- Phase 2 Proposal**: Includes Encryption (DES), Authentication (SHA256), Enable Replay Detection (checked), and Enable Perfect Forward Secrecy (PFS) (checked).
- Diffe-Hellman Group**: A grid of checkboxes for various groups. Groups 14 and 5 are selected.

The right sidebar provides additional information, including API Preview, References, IPsec VPNs guides, IPsec VPN Cookbook Recipes, VPN Setup on FortiClient, Configuring an IPsec VPN Connection, Documentation, Online Help, and Video Tutorials.

The screenshot displays the Fortinet FortiGate web interface for configuring an IPsec tunnel. The left-hand navigation pane is expanded, showing the 'IPsec Tunnels' section. The main configuration area, titled 'Edit VPN Tunnel', is divided into two panes. The left pane contains the primary configuration settings, including 'Remote Address' (set to 'Named Addr'), 'Advanced...' (Phase 2 Proposal), 'Encryption' (DES), 'Authentication' (SHA256), 'Enable Replay Detection' (checked), 'Enable Perfect Forward Secrecy (PFS)' (checked), 'Diffie-Hellman Group' (32, 31, 30, 29, 28, 27, 21, 20, 19, 18, 17, 16, 15, 14, 5, 2, 1), 'Local Port' (All), 'Remote Port' (All), 'Protocol' (All), 'Auto-negotiate' (checked), 'Autokey Keep Alive' (unchecked), 'Key Lifetime' (Seconds), and 'Seconds' (43200). The right pane, titled 'Additional Information', provides links to 'API Preview', 'References', 'IPsec VPNs', 'Guides', 'IPsec VPN Cookbook Recipes', 'VPN Setup on FortiClient', 'Configuring an IPsec VPN Connection', 'Documentation', 'Online Help', and 'Video Tutorials'.



## FGT-BRANCH (TO HQ LA)

FGT-BRANCH

Dashboard

Network

Policy & Objects

Security Profiles

VPN

Overlay Controller VPN

IPsec Tunnels

IPsec Wizard

IPsec Tunnel Template

SSL-VPN Portals

SSL-VPN Settings

SSL-VPN Clients

VPN Location Map

User & Authentication

System

Security Fabric

Log & Report

FGTINET v7.0.14

Edit VPN Tunnel

Name

TO HQ LA

Comments

Comments

Network

IP Version

IPv4

Remote Gateway

Static IP Address

IP Address

182.4.24.2

Interface

TO LA (port1)

Local Gateway

Mode Config

NAT Traversal

Enable

Disable

Forced

Dead Peer Detection

Disable

On Idle

On Demand

DPD retry count

3

DPD retry interval

20

s

Forward Error Correction

Egress

Ingress

Advanced...

Additional Information

API Preview

References

IPsec VPNs

Guides

IPsec VPN Cookbook Recipes

VPN Setup on FortiClient

Configuring an IPsec VPN Connection

Documentation

Online Help

Video Tutorials

OKCancel

FGT-BRANCH

Dashboard

Network

Policy & Objects

Security Profiles

VPN

Overlay Controller VPN

IPsec Tunnels

IPsec Wizard

IPsec Tunnel Template

SSL-VPN Portals

SSL-VPN Settings

SSL-VPN Clients

VPN Location Map

User & Authentication

System

Security Fabric

Log & Report

FGTINET v7.0.14

Edit VPN Tunnel

Authentication

Method

Pre-shared Key

Pre-shared Key

\*\*\*\*\*

IKE

Version

1

2

Mode

Aggressive

Main (ID protection)

Phase 1 Proposal

Algorithms: DES-SHA256

Diffie-Hellman Groups: 14, 5

Edit

XAUTH

Type: Disabled

Edit

Phase 2 Selectors

Name

Local Address

Remote Address

Add

TO HQ LA

all

all

Additional Information

API Preview

References

IPsec VPNs

Guides

IPsec VPN Cookbook Recipes

VPN Setup on FortiClient

Configuring an IPsec VPN Connection

Documentation

Online Help

Video Tutorials

OKCancel

FGT-BRANCH

Dashboard

Network

Policy & Objects

Security Profiles

VPN

Overlay Controller VPN

IPsec Tunnels

IPsec Wizard

IPsec Tunnel Template

SSL-VPN Portals

SSL-VPN Settings

SSL-VPN Clients

VPN Location Map

User & Authentication

System

Security Fabric

Log & Report

FGTINET v7.0.14

Edit VPN Tunnel

IKE Version: 1, Mode: Main (ID protection)

Phase 1 Proposal

Add

Encryption

DES

Authentication

SHA256

Diffie-Hellman Groups

32

31

30

29

28

27

21

20

19

18

17

16

15

14

5

2

1

Key Lifetime (seconds)

86400

Local ID

XAUTH

Type: Disabled

Edit

Phase 2 Selectors

Name

Local Address

Remote Address

Add

TO HQ LA

all

all

Additional Information

API Preview

References

IPsec VPNs

Guides

IPsec VPN Cookbook Recipes

VPN Setup on FortiClient

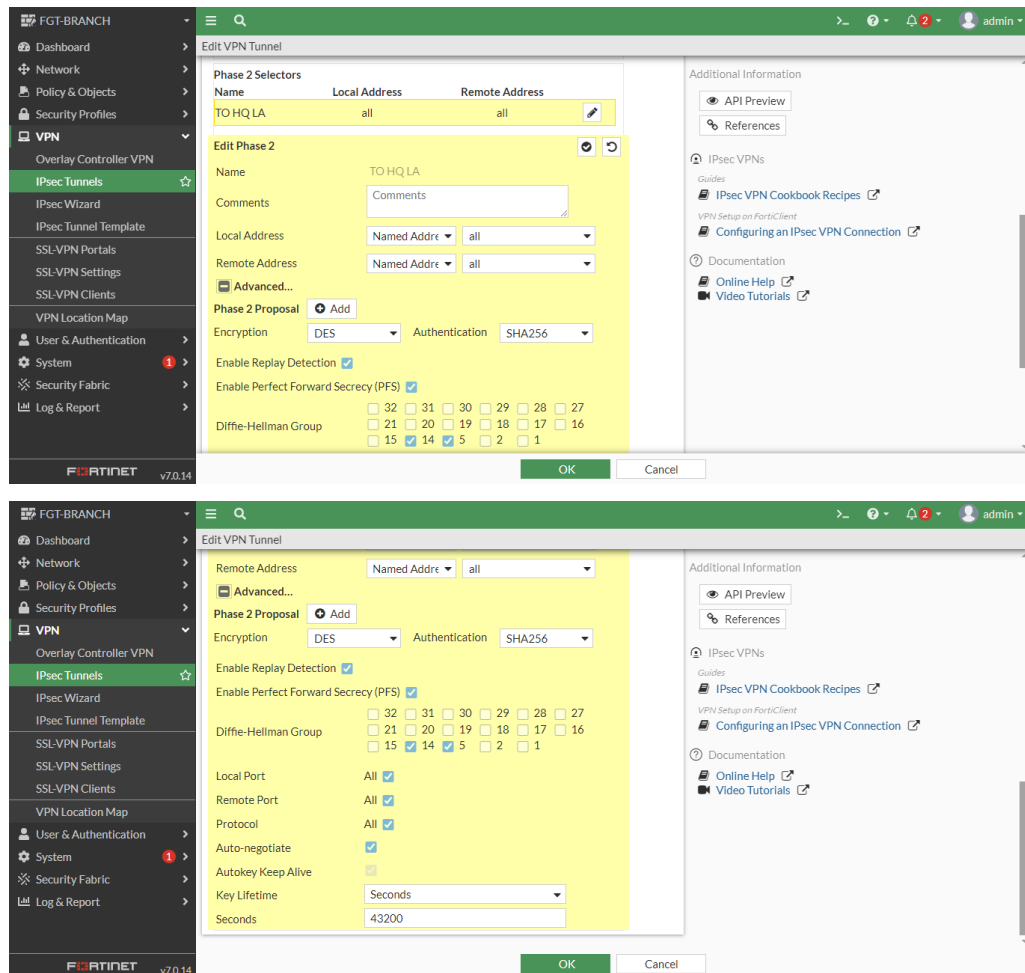
Configuring an IPsec VPN Connection

Documentation

Online Help

Video Tutorials

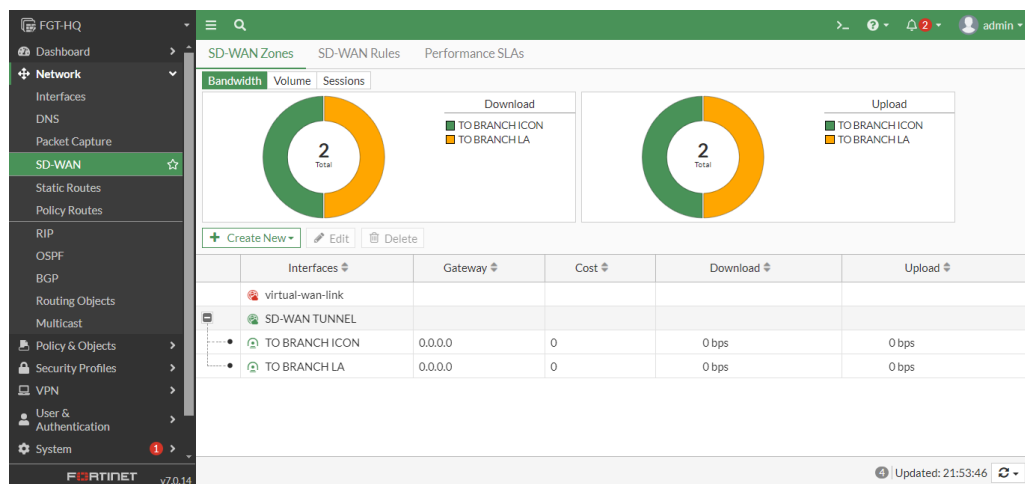
OKCancel



## #Configure SD-WAN Tunnel

Konfigurasi ini bertujuan untuk mengelompokkan interface yang digunakan oleh perangkat FortiGate ke dalam satu kelompok yang disebut SD-WAN Zone.

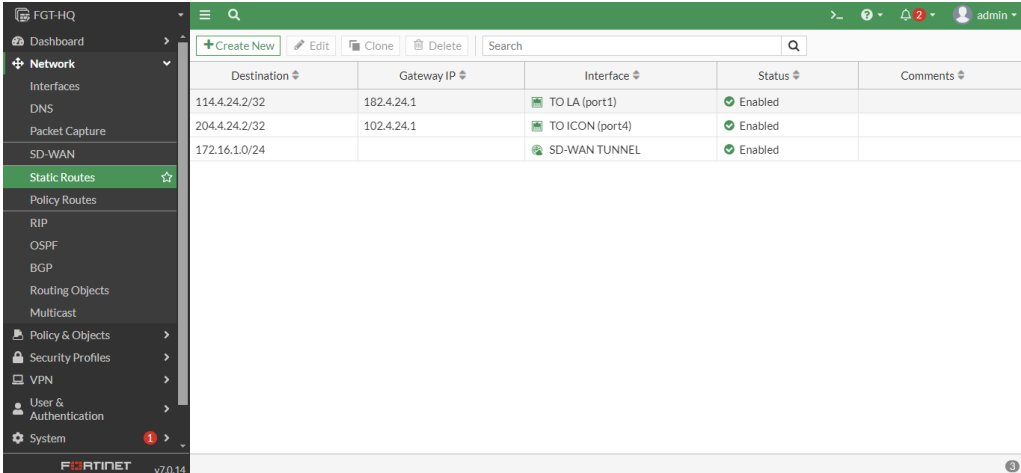
### FGT-HQ



## #Configure Static Route

Konfigurasi ini dilakukan untuk perangkat FGT-HQ dan FGT-BRANCH yang bertujuan untuk mengarahkan traffic jaringan melalui jalur yang sesuai dan memastikan dapat melakukan komunikasi antara jaringan yang berbeda.

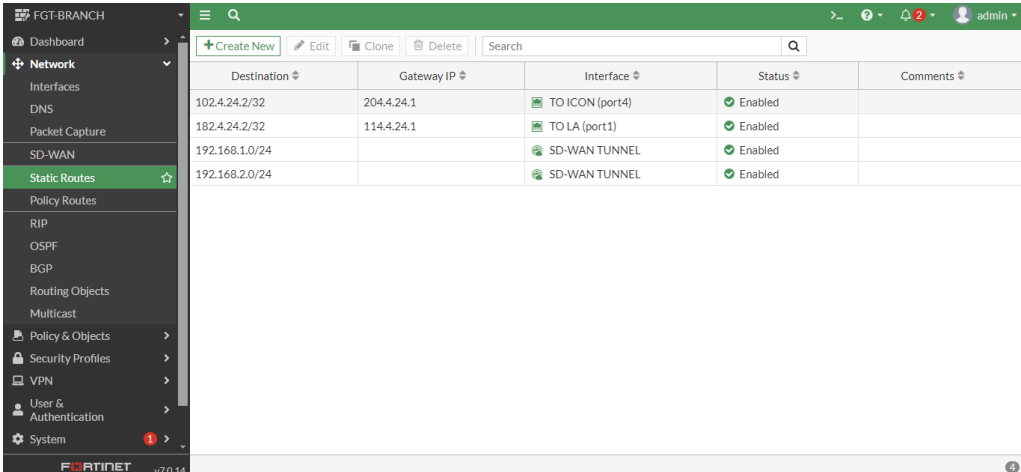
### FGT-HQ



The screenshot shows the 'Static Routes' configuration page for FGT-HQ. The left sidebar contains a menu with 'Static Routes' highlighted. The main area displays a table with three rows of static routes. The table has columns for Destination, Gateway IP, Interface, Status, and Comments. The first row shows a route to 114.4.24.2/32 via gateway 182.4.24.1 on interface TO LA (port1). The second row shows a route to 204.4.24.2/32 via gateway 102.4.24.1 on interface TO ICON (port4). The third row shows a route to 172.16.1.0/24 via the SD-WAN TUNNEL interface. All routes are marked as 'Enabled'.

Destination	Gateway IP	Interface	Status	Comments
114.4.24.2/32	182.4.24.1	TO LA (port1)	Enabled	
204.4.24.2/32	102.4.24.1	TO ICON (port4)	Enabled	
172.16.1.0/24		SD-WAN TUNNEL	Enabled	

### FGT-BRANCH



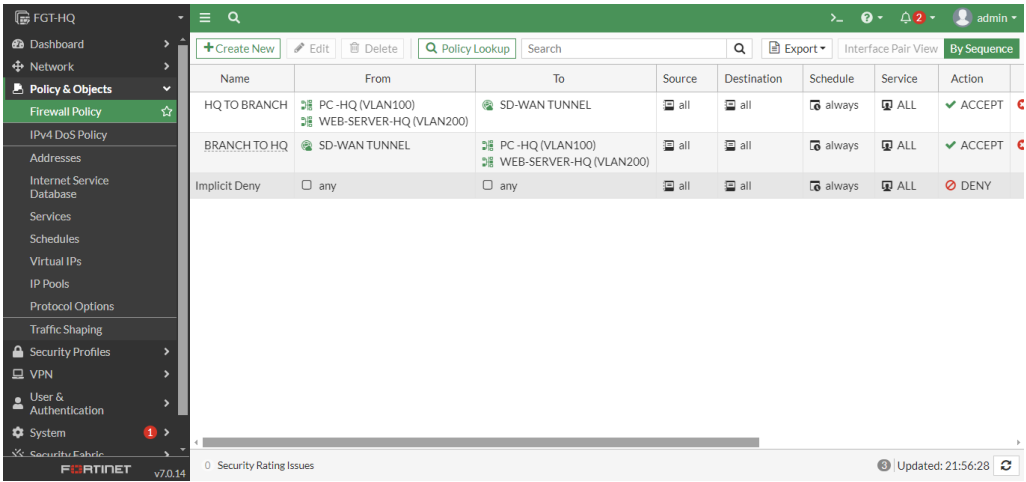
The screenshot shows the 'Static Routes' configuration page for FGT-BRANCH. The left sidebar contains a menu with 'Static Routes' highlighted. The main area displays a table with four rows of static routes. The table has columns for Destination, Gateway IP, Interface, Status, and Comments. The first row shows a route to 102.4.24.2/32 via gateway 204.4.24.1 on interface TO ICON (port4). The second row shows a route to 182.4.24.2/32 via gateway 114.4.24.1 on interface TO LA (port1). The third row shows a route to 192.168.1.0/24 via the SD-WAN TUNNEL interface. The fourth row shows a route to 192.168.2.0/24 via the SD-WAN TUNNEL interface. All routes are marked as 'Enabled'.

Destination	Gateway IP	Interface	Status	Comments
102.4.24.2/32	204.4.24.1	TO ICON (port4)	Enabled	
182.4.24.2/32	114.4.24.1	TO LA (port1)	Enabled	
192.168.1.0/24		SD-WAN TUNNEL	Enabled	
192.168.2.0/24		SD-WAN TUNNEL	Enabled	

## #Configure Firewall Policy

Konfigurasi ini dilakukan untuk perangkat FGT-HQ dan FGT-BRANCH yang bertujuan untuk mengontrol traffic jaringan antara HQ dan Branch agar kedua lokasi dapat berkomunikasi dengan aman dan efisien.

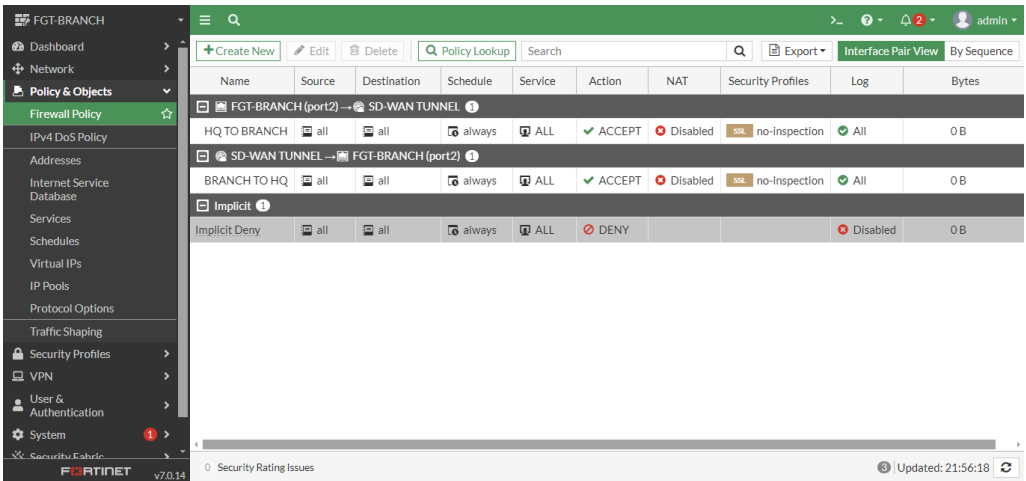
### FGT-HQ



The screenshot shows the FGT-HQ Firewall Policy configuration page. The left sidebar contains a navigation menu with options like 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, and System. The main area displays a table of firewall policies.

Name	From	To	Source	Destination	Schedule	Service	Action
HQ TO BRANCH	PC-HQ (VLAN100) WEB-SERVER-HQ (VLAN200)	SD-WAN TUNNEL	all	all	always	ALL	ACCEPT
BRANCH TO HQ	SD-WAN TUNNEL	PC-HQ (VLAN100) WEB-SERVER-HQ (VLAN200)	all	all	always	ALL	ACCEPT
Implicit Deny	any	any	all	all	always	ALL	DENY

### FGT-BRANCH



The screenshot shows the FGT-BRANCH Firewall Policy configuration page. The left sidebar contains a navigation menu with options like 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, and System. The main area displays a table of firewall policies.

Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	Bytes
HQ TO BRANCH	all	all	always	ALL	ACCEPT	Disabled	SSL no-inspection	All	0 B
BRANCH TO HQ	all	all	always	ALL	ACCEPT	Disabled	SSL no-inspection	All	0 B
Implicit Deny	all	all	always	ALL	DENY			Disabled	0 B

### 3. Pengujian

- Ping dari PC-HQ ke PC-Branch

```
PC-HQ x
root@PC-HQ:/#
root@PC-HQ:/# ping 172.16.1.1
PING 172.16.1.1 (172.16.1.1) 56(84) bytes of data.
64 bytes from 172.16.1.1: icmp_seq=1 ttl=254 time=8.16 ms
64 bytes from 172.16.1.1: icmp_seq=2 ttl=254 time=2.80 ms
64 bytes from 172.16.1.1: icmp_seq=3 ttl=254 time=2.87 ms
64 bytes from 172.16.1.1: icmp_seq=4 ttl=254 time=2.92 ms
64 bytes from 172.16.1.1: icmp_seq=5 ttl=254 time=2.87 ms
^C
--- 172.16.1.1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4006ms
rtt min/avg/max/mdev = 2.796/3.921/8.159/2.119 ms
root@PC-HQ:/# █
```

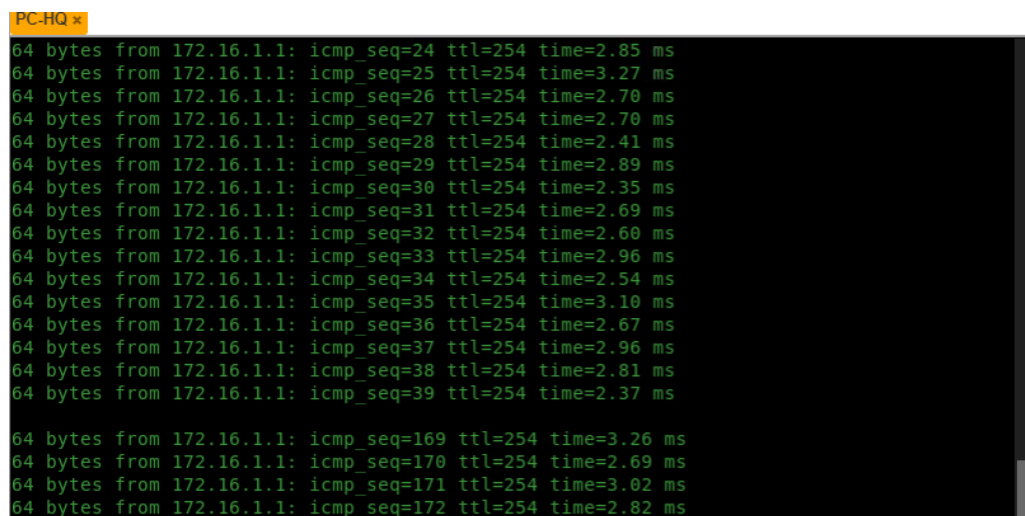
- Ping dari PC-Branch ke PC-HQ dan WEB-SERVER

```
PC-HQ x PC-BRANCH x
root@PC-BRANCH:/# ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data.
64 bytes from 192.168.1.1: icmp_seq=1 ttl=254 time=4.70 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=254 time=2.76 ms
64 bytes from 192.168.1.1: icmp_seq=3 ttl=254 time=2.48 ms
64 bytes from 192.168.1.1: icmp_seq=4 ttl=254 time=2.61 ms
64 bytes from 192.168.1.1: icmp_seq=5 ttl=254 time=2.57 ms
^C
--- 192.168.1.1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4008ms
rtt min/avg/max/mdev = 2.481/3.024/4.696/0.840 ms
root@PC-BRANCH:/# ping 192.168.2.1
PING 192.168.2.1 (192.168.2.1) 56(84) bytes of data.
64 bytes from 192.168.2.1: icmp_seq=1 ttl=254 time=2.65 ms
64 bytes from 192.168.2.1: icmp_seq=2 ttl=254 time=2.46 ms
64 bytes from 192.168.2.1: icmp_seq=3 ttl=254 time=2.39 ms
64 bytes from 192.168.2.1: icmp_seq=4 ttl=254 time=2.34 ms
64 bytes from 192.168.2.1: icmp_seq=5 ttl=254 time=2.32 ms
^C
--- 192.168.2.1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4006ms
rtt min/avg/max/mdev = 2.317/2.432/2.648/0.118 ms
root@PC-BRANCH:/# █
```

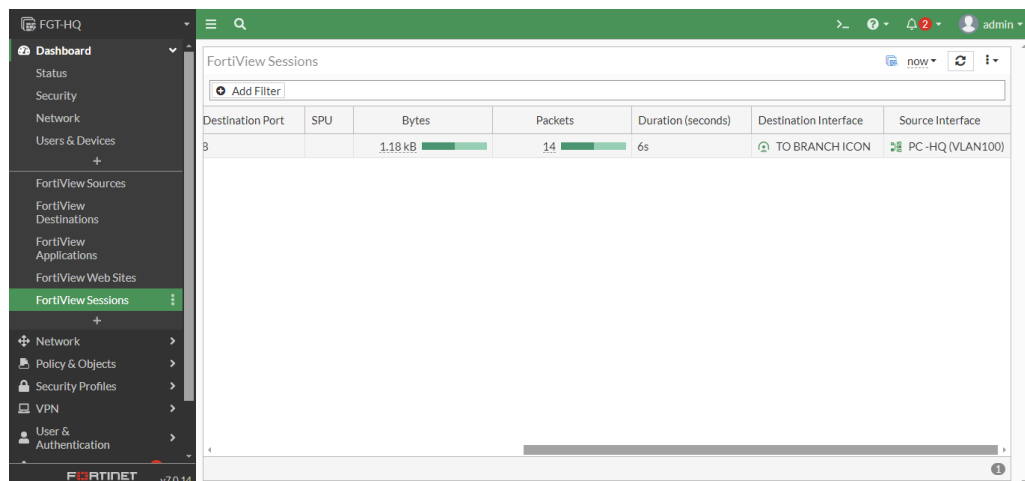
- **Akses WEB-SERVER dari PC-Branch**



- **Failover PC-HQ ke PC-BRANCH**



**FortiView Session (Sebelum Disbale Tunnel)**



## Disbale Tunnel port4

FortiGate VM64-KVM

Name	Type	Members	IP/Netmask	Administrative Access	DHCP Clients	DHCP Range
port3	Physical Interface		10.20.8.112/255.255.255.0	PING HTTPS SSH HTTP FtMG-Access		
TO ICON (port4)	Physical Interface		102.4.24.2/255.255.255.252	PING HTTPS SSH HTTP FtMG-Access		
TO LA (port1)	Physical Interface		182.4.24.2/255.255.255.252	PING HTTPS SSH HTTP FtMG-Access		

0 Security Rating Issues 54% Updated: 20:11:23

## FortiView Session (Disbale Tunnel)

FortiView Sessions

Destination Port	SPU	Bytes	Packets	Duration (seconds)	Destination Interface	Source Interface
8		31.08 kB	370	3m 6s	TO BRANCH ICON	PC-HQ (VLAN100)

## FortiView Session (Setelah Disbale Tunnel)

FortiView Sessions

Destination Port	SPU	Bytes	Packets	Duration (seconds)	Destination Interface	Source Interface
8		2.52 kB	30	1m 9s	TO BRANCH LA	PC-HQ (VLAN100)
8		2.86 kB	34	35s	TO BRANCH ICON	PC-HQ (VLAN100)
8		3.19 kB	38	55s	TO BRANCH LA	PC-HQ (VLAN100)
8		504 B	6	2s	TO BRANCH ICON	PC-HQ (VLAN100)
8		2.86 kB	34	18s	TO BRANCH ICON	PC-HQ (VLAN100)