LAB 10

SIMULATION/LAB FORTIGATE FUNDAMENTAL

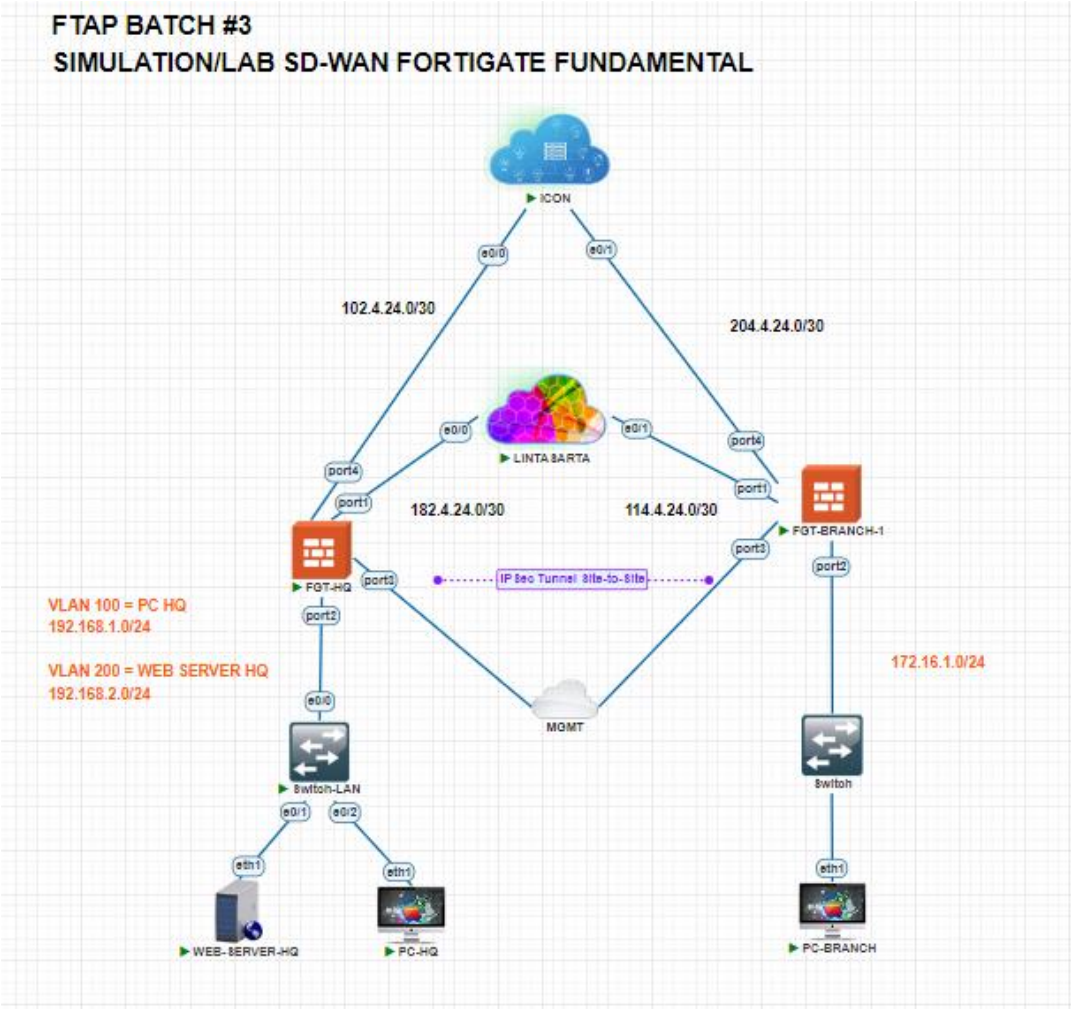
Implementation IPSec Tunnel Site-to-Site With SD-WAN Method

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

Annisa Hadita

Mentor: Dito Prasetya

1. **Topology**



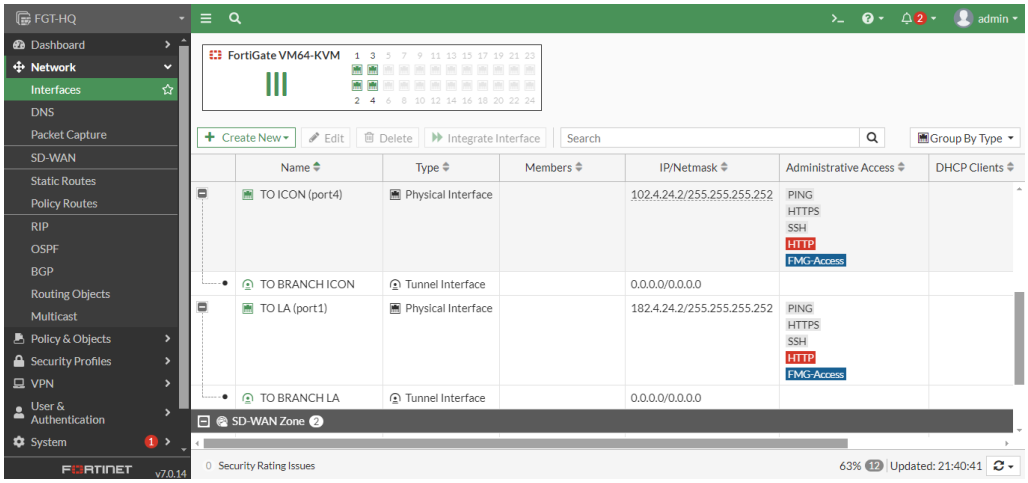
2. **Task**

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.

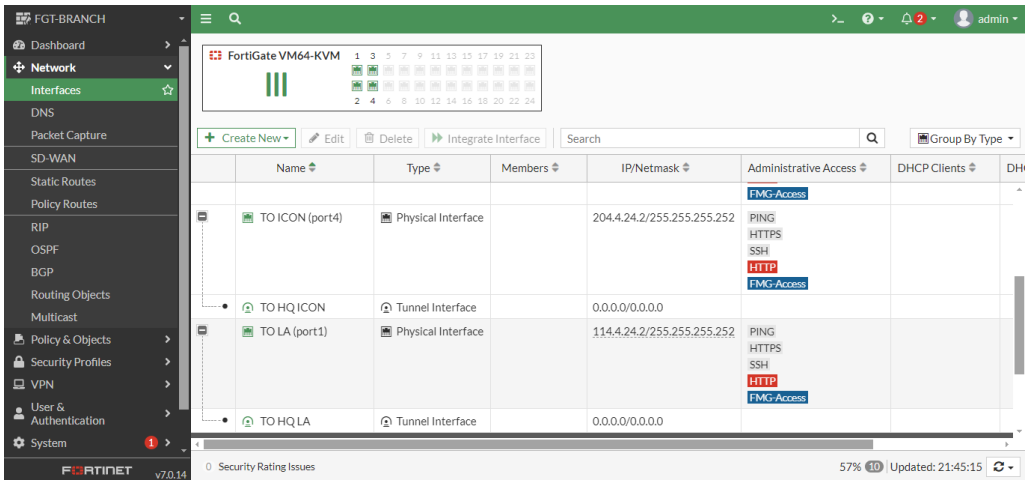
#Configure Interface

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



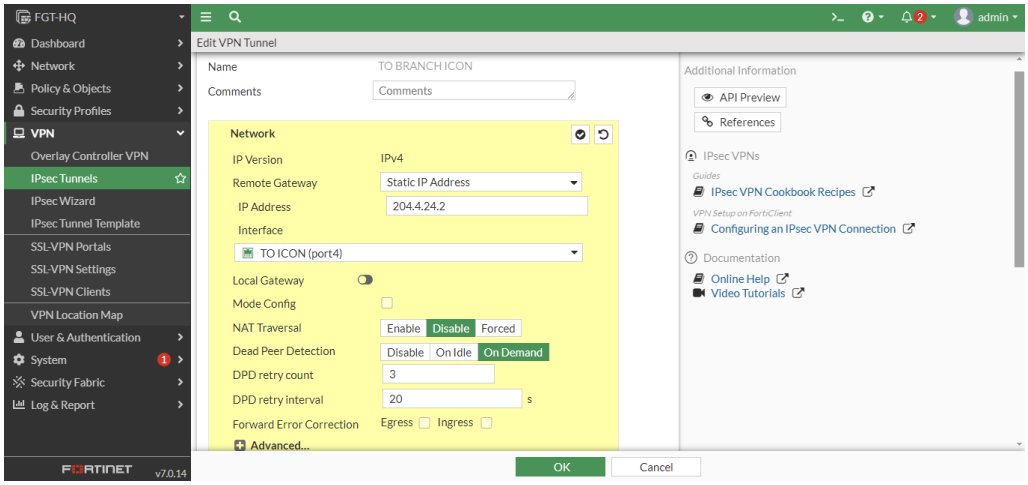
FGT-Branch

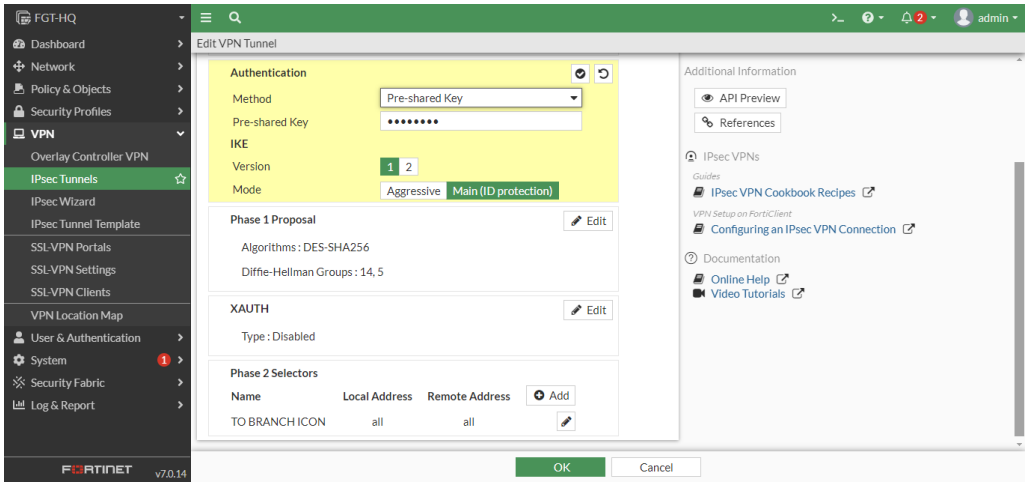


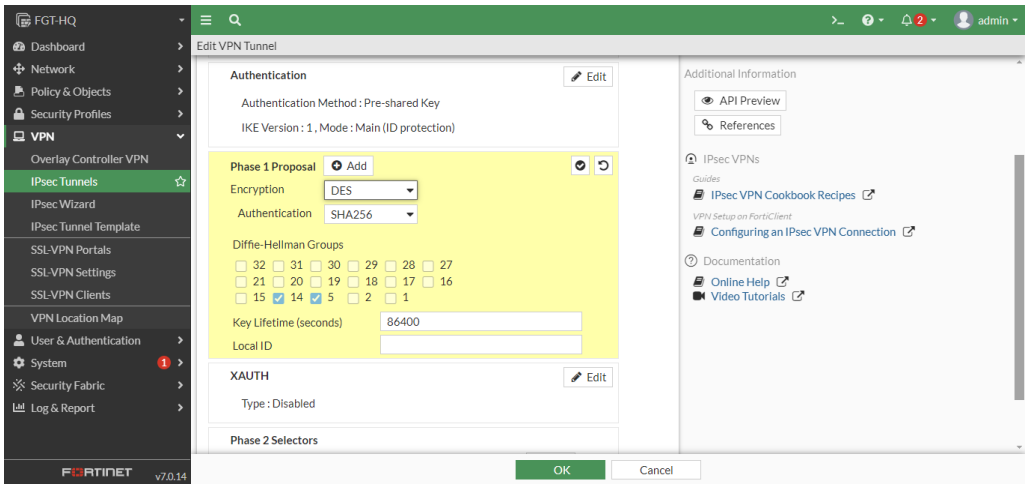
#Configure IPSec Tunnel

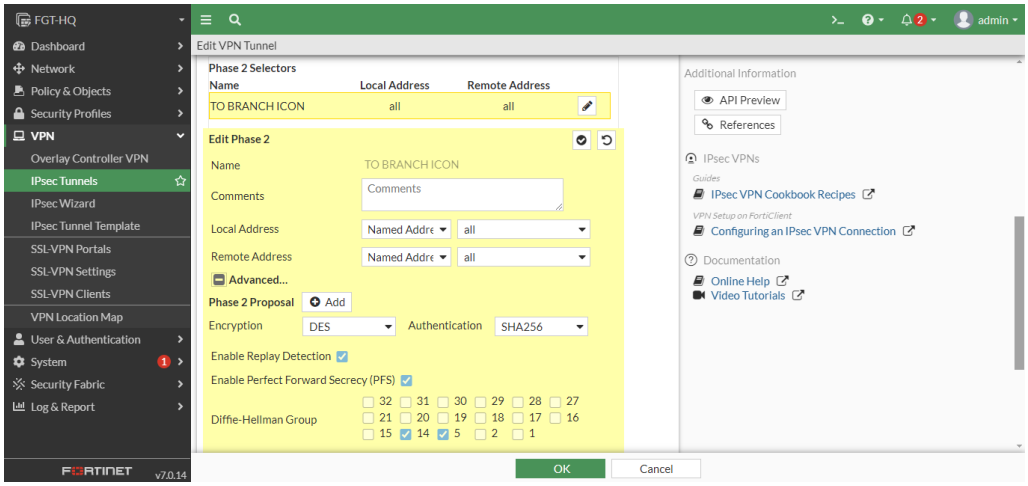
Konfigurasi ini dibuat untuk menyediakan jalur komunikasi yang aman dan terenkripsi antara dua jaringan yang berbeda, misalnya antara HQ dan Branch.

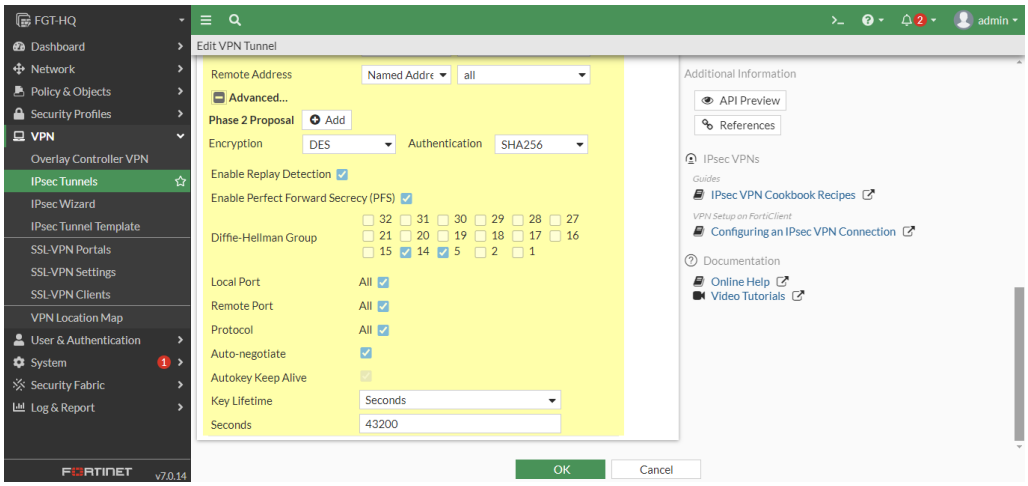
FGT-HQ (TO BRANCH ICON)



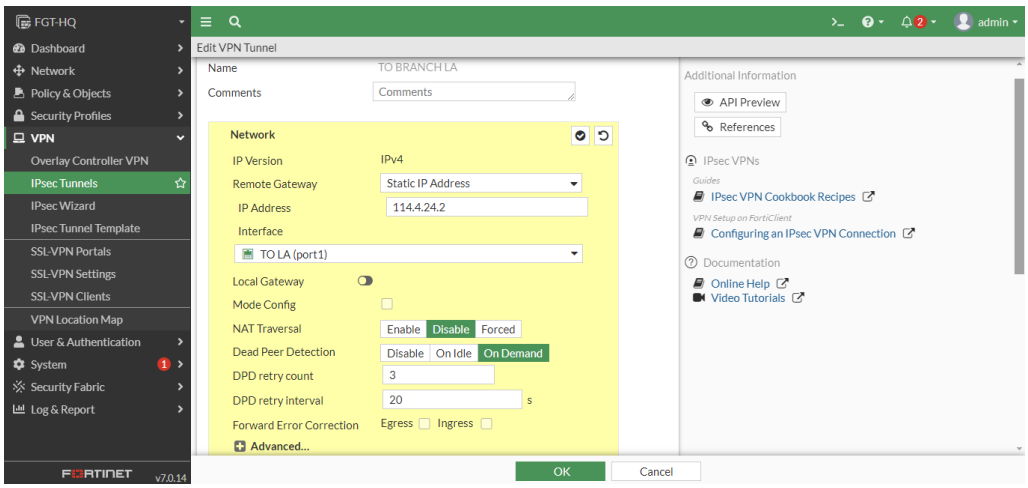


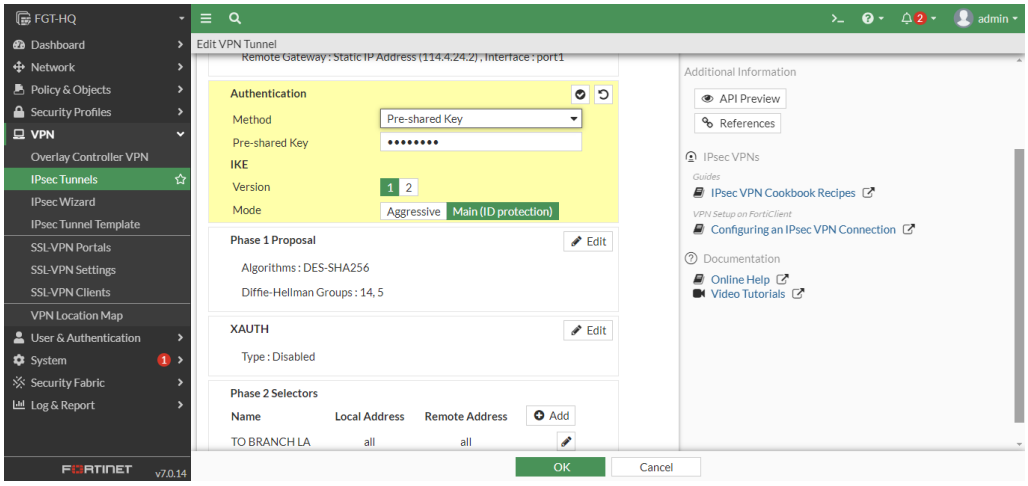


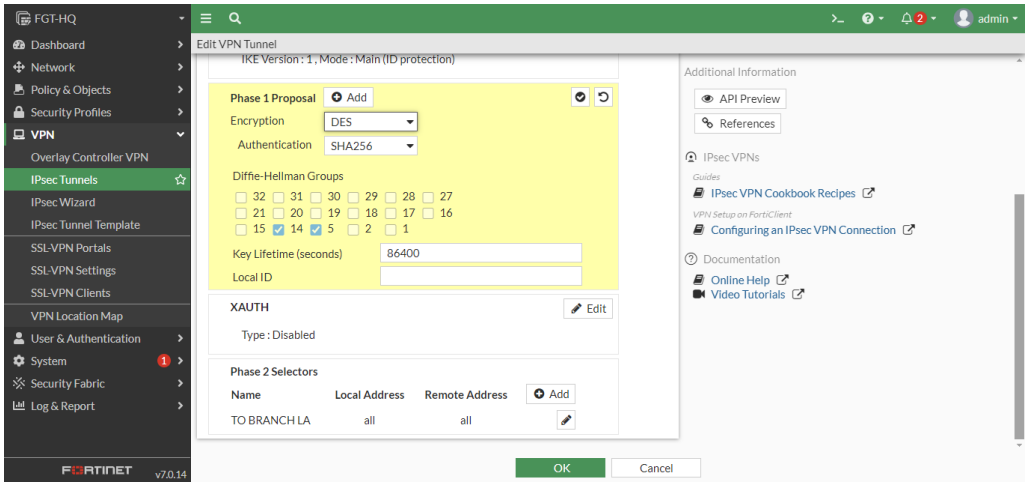


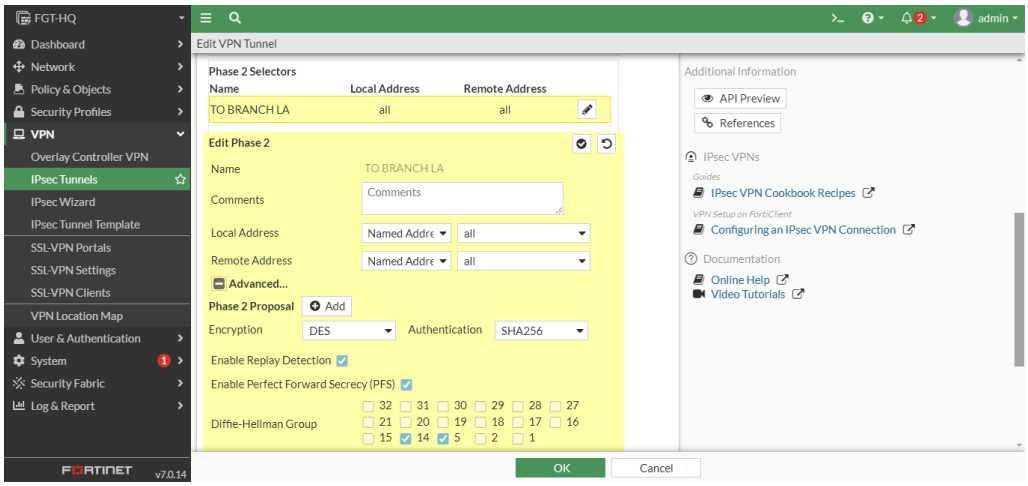


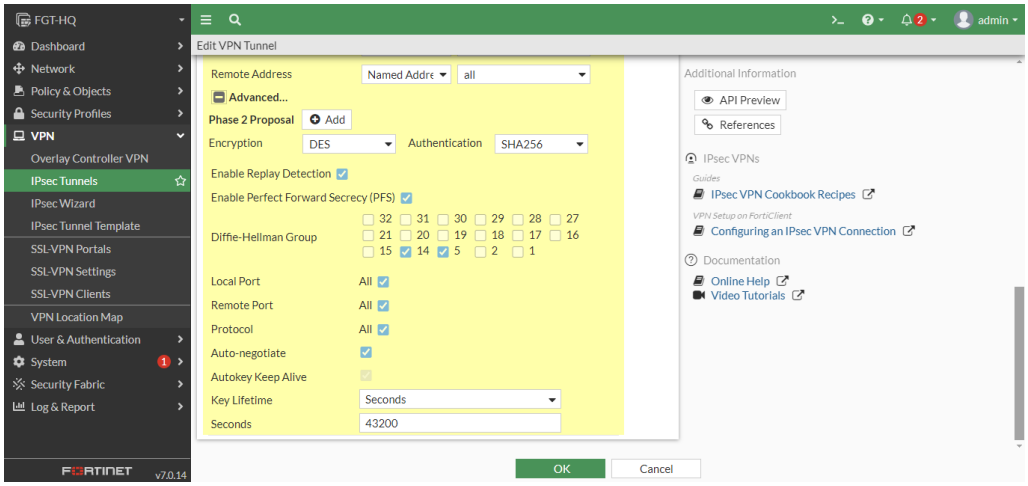
FGT-HQ (TO BRANCH LA)



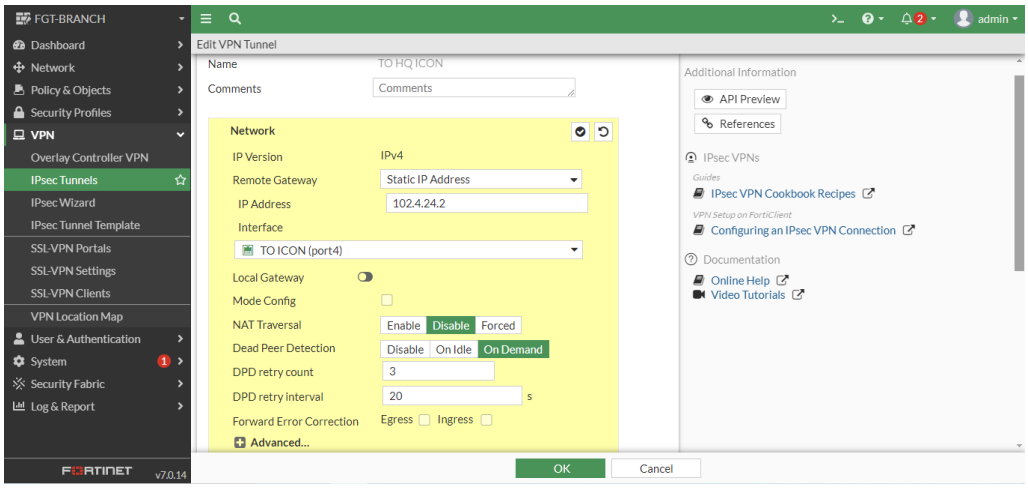

FGT-HQ
Dashboard
Network
Policy & Objects
Security Profiles
VPN
Overlay Controller VPN
IPsec Tunnels
IPsec Wizard
IPsec Tunnel Template
SSL-VPN Portals
SSL-VPN Settings
SSL-VPN Clients
VPN Location Map
User & Authentication
System
Security Fabric
Log & Report
FORTINET v7.0.14
admin
Edit VPN Tunnel
Remote Gateway : Static IP Address (114.4.24.2) , Interface : port1
Authentication
Method
Pre-shared Key
Pre-shared Key
IKE
Version
1 2
Mode
Aggressive
Main (ID protection)
Phase 1 Proposal
Edit
Algorithms : DES-SHA256
Diffie-Hellman Groups : 14, 5
XAUTH
Edit
Type : Disabled
Phase 2 Selectors
Name
Local Address
Remote Address
Add
TO BRANCH 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
OK
Cancel

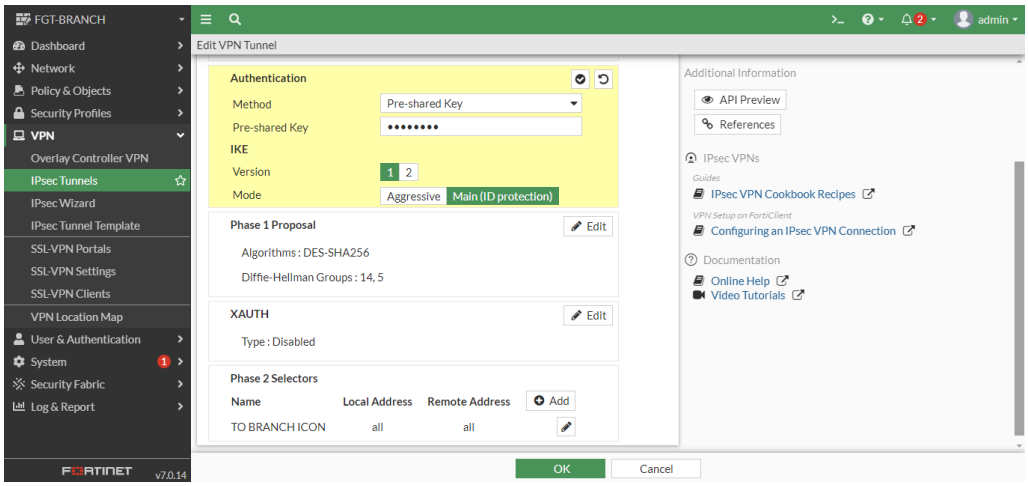

FGT-HQ
Dashboard
Network
Policy & Objects
Security Profiles
VPN
Overlay Controller VPN
IPsec Tunnels
IPsec Wizard
IPsec Tunnel Template
SSL-VPN Portals
SSL-VPN Settings
SSL-VPN Clients
VPN Location Map
User & Authentication
System
Security Fabric
Log & Report
FORTINET v7.0.14
admin
Edit VPN Tunnel
IKE 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
Edit
Type : Disabled
Phase 2 Selectors
Name
Local Address
Remote Address
Add
TO BRANCH 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
OK
Cancel

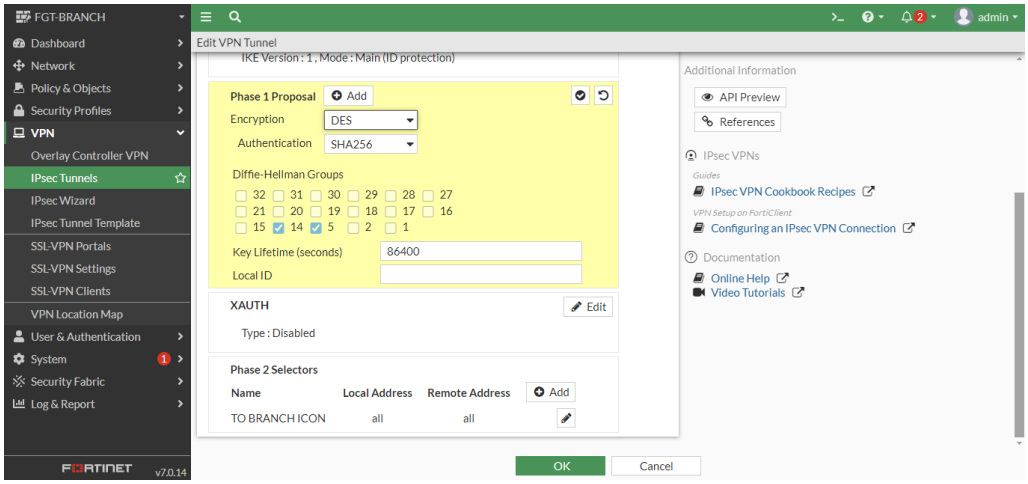

FGT-HQ
Dashboard
Network
Policy & Objects
Security Profiles
VPN
Overlay Controller VPN
IPsec Tunnels
IPsec Wizard
IPsec Tunnel Template
SSL-VPN Portals
SSL-VPN Settings
SSL-VPN Clients
VPN Location Map
User & Authentication
System
Security Fabric
Log & Report
FORTINET v7.0.14
admin
Edit VPN Tunnel
Phase 2 Selectors
Name
Local Address
Remote Address
TO BRANCH LA
all
all
Edit Phase 2
Name
TO BRANCH LA
Comments
Comments
Local Address
Named Addre
all
Remote Address
Named Addre
all
Advanced...
Phase 2 Proposal
Add
Encryption
DES
Authentication
SHA256
Enable Replay Detection
Enable Perfect Forward Secrecy (PFS)
Diffie-Hellman Group
32 31 30 29 28 27
21 20 19 18 17 16
15 14 5 2 1
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
OK
Cancel

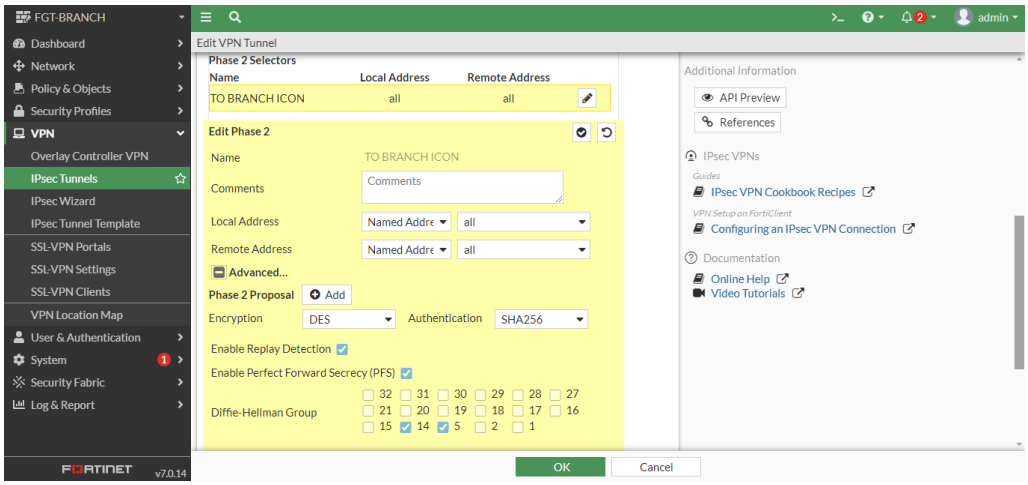


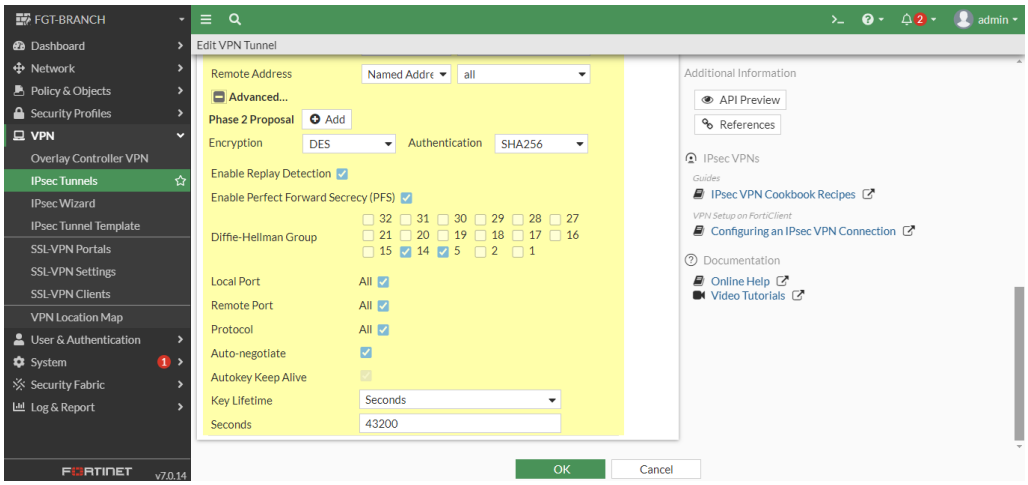
FGT-BRANCH (TO HQ ICON)



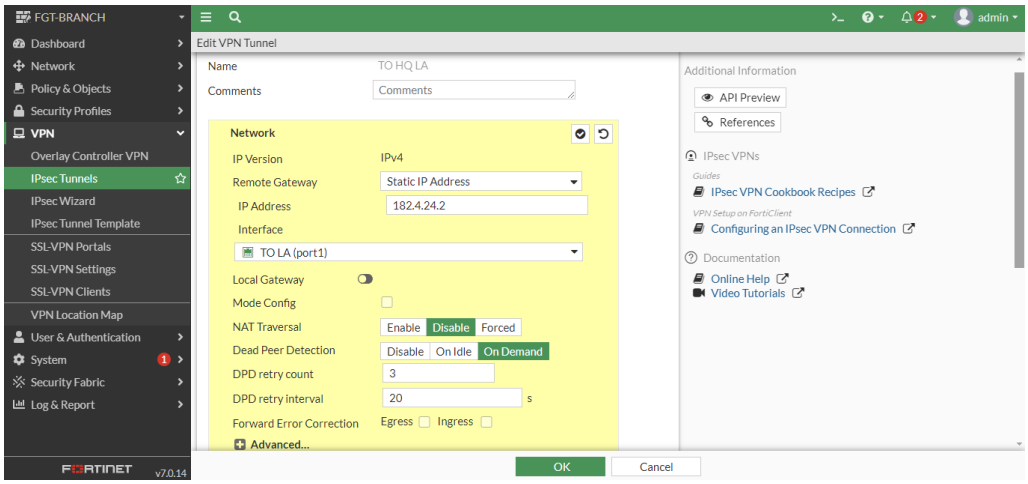


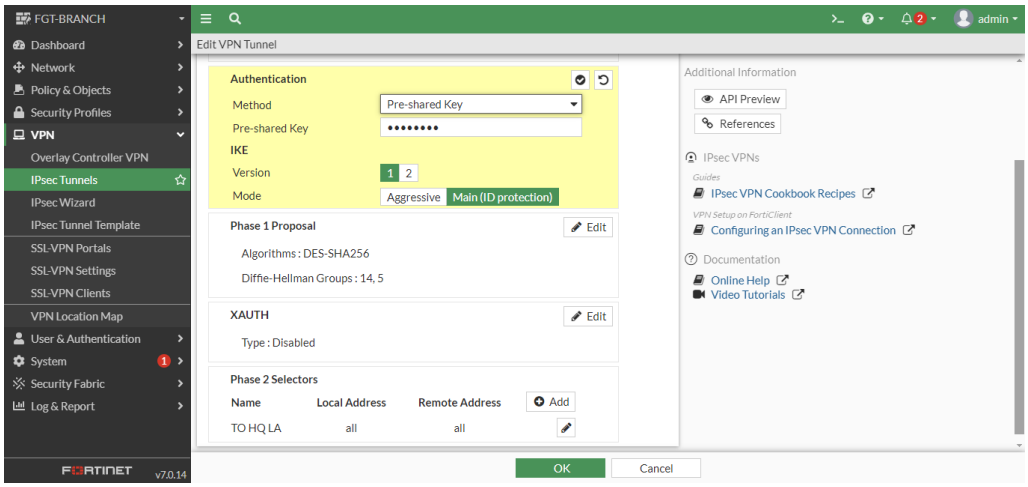

FGT-BRANCH
admin
Dashboard
Network
Policy & Objects
Security Profiles
VPN
Overlay Controller VPN
IPsec Tunnels
IPsec Wizard
IPsec Tunnel Template
SSL-VPN Portals
SSL-VPN Settings
SSL-VPN Clients
VPN Location Map
User & Authentication
System
Security Fabric
Log & Report
FORTINET
v7.0.14
Edit VPN Tunnel
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
Edit
Type : Disabled
Phase 2 Selectors
Name
Local Address
Remote Address
Add
TO BRANCH ICON
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
OK
Cancel

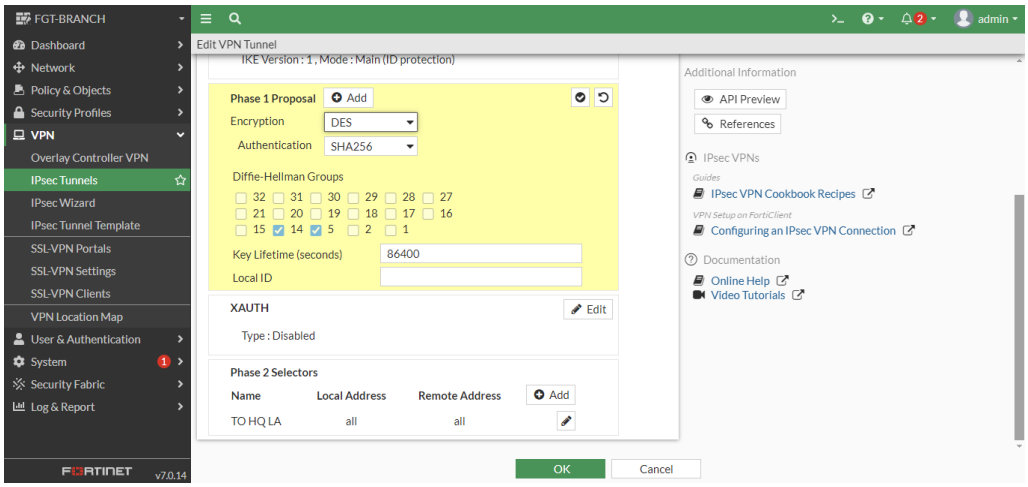

FGT-BRANCH
admin
Dashboard
Network
Policy & Objects
Security Profiles
VPN
Overlay Controller VPN
IPsec Tunnels
IPsec Wizard
IPsec Tunnel Template
SSL-VPN Portals
SSL-VPN Settings
SSL-VPN Clients
VPN Location Map
User & Authentication
System
Security Fabric
Log & Report
FORTINET
v7.0.14
Edit VPN Tunnel
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 Addre
all
Remote Address
Named Addre
all
Advanced...
Phase 2 Proposal
Add
Encryption
DES
Authentication
SHA256
Enable Replay Detection
Enable Perfect Forward Secrecy (PFS)
Diffie-Hellman Group
32 31 30 29 28 27
21 20 19 18 17 16
15 14 5 2 1
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
OK
Cancel

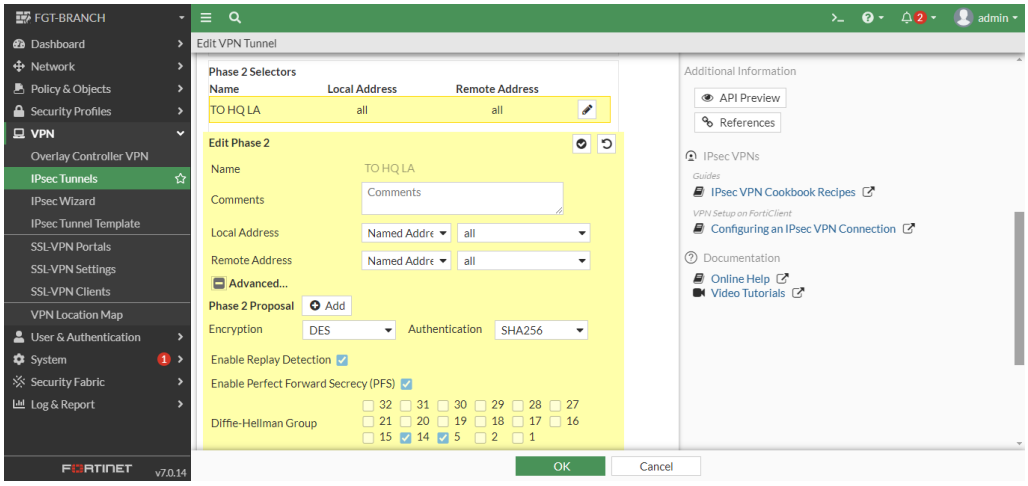

FGT-BRANCH
admin
Dashboard
Network
Policy & Objects
Security Profiles
VPN
Overlay Controller VPN
IPsec Tunnels
IPsec Wizard
IPsec Tunnel Template
SSL-VPN Portals
SSL-VPN Settings
SSL-VPN Clients
VPN Location Map
User & Authentication
System
Security Fabric
Log & Report
FORTINET
v7.0.14
Edit VPN Tunnel
Remote Address
Named Addre
all
Advanced...
Phase 2 Proposal
Add
Encryption
DES
Authentication
SHA256
Enable Replay Detection
Enable Perfect Forward Secrecy (PFS)
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
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
OK
Cancel

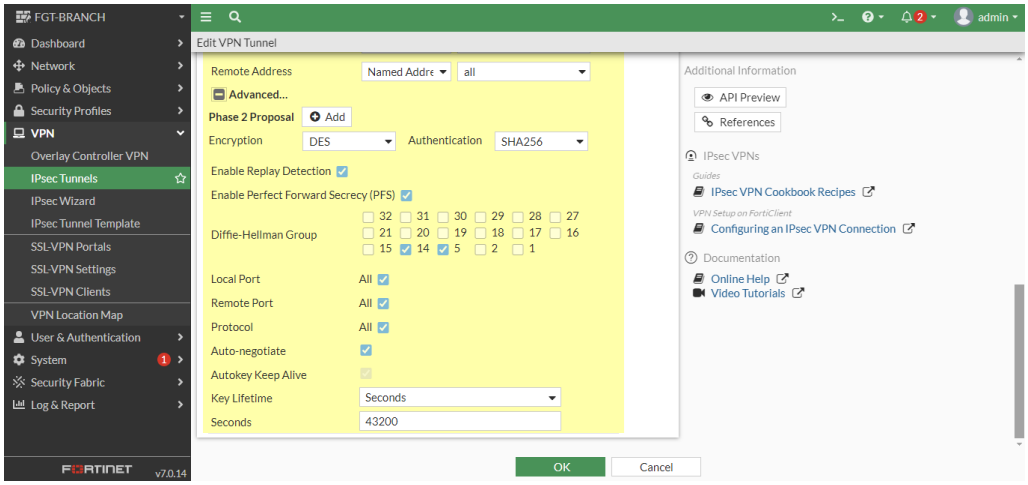
FGT-BRANCH (TO HQ LA)







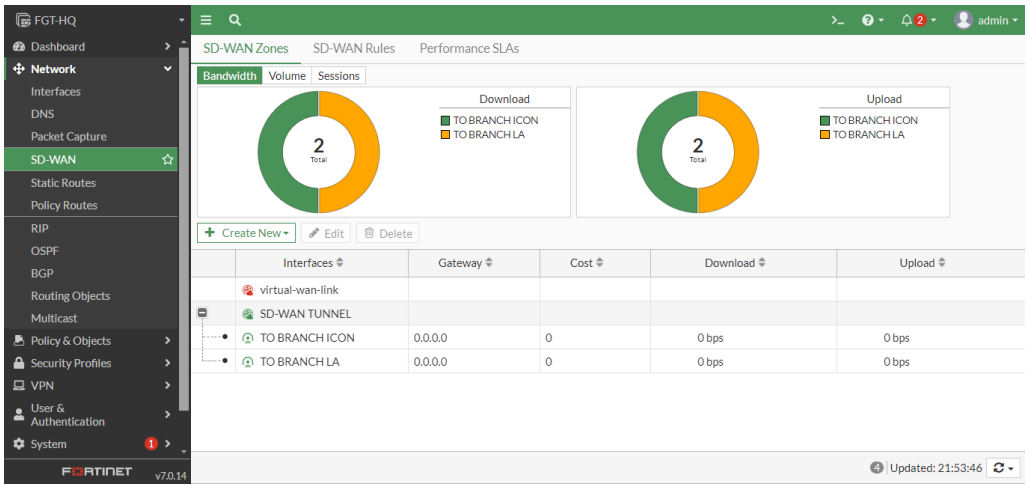




#Configure SD-WAN Tunnel

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

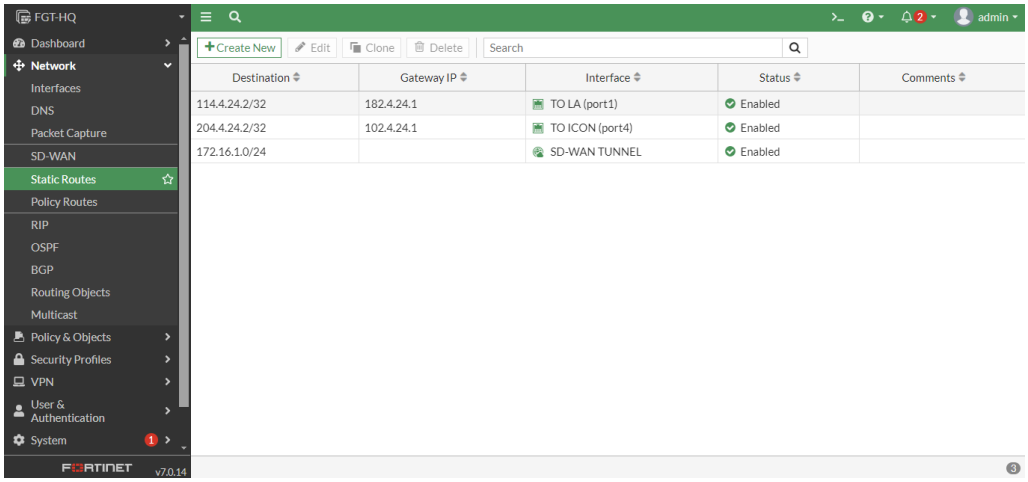
FGT-HQ



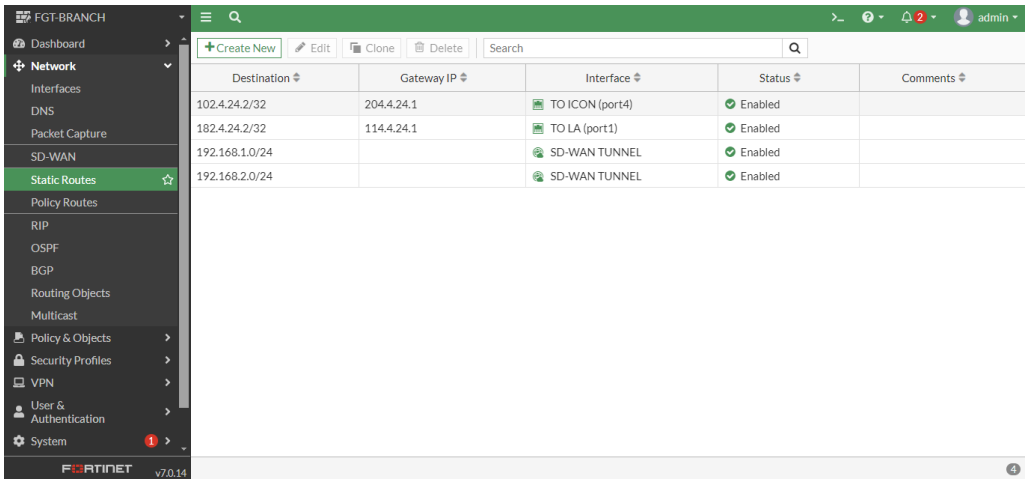
#Configure Static Route

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

FGT-HQ



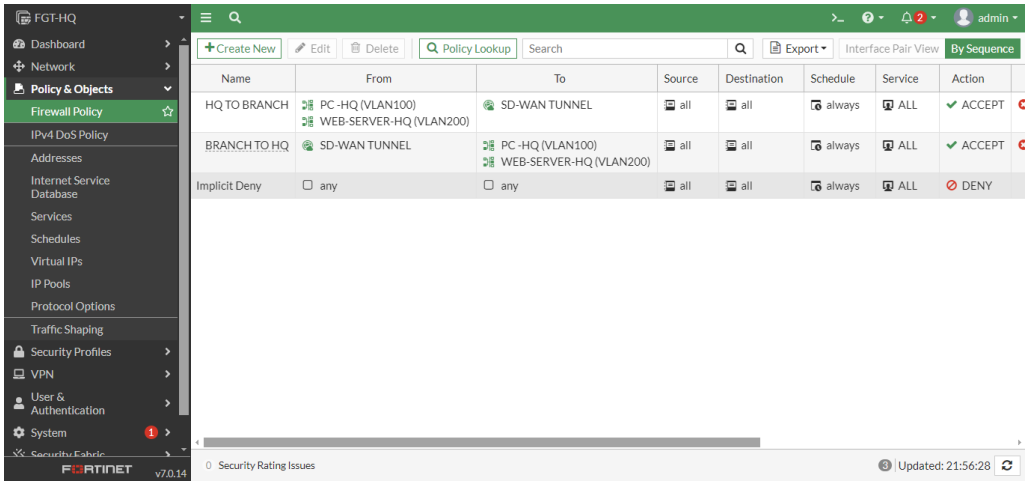
FGT-BRANCH



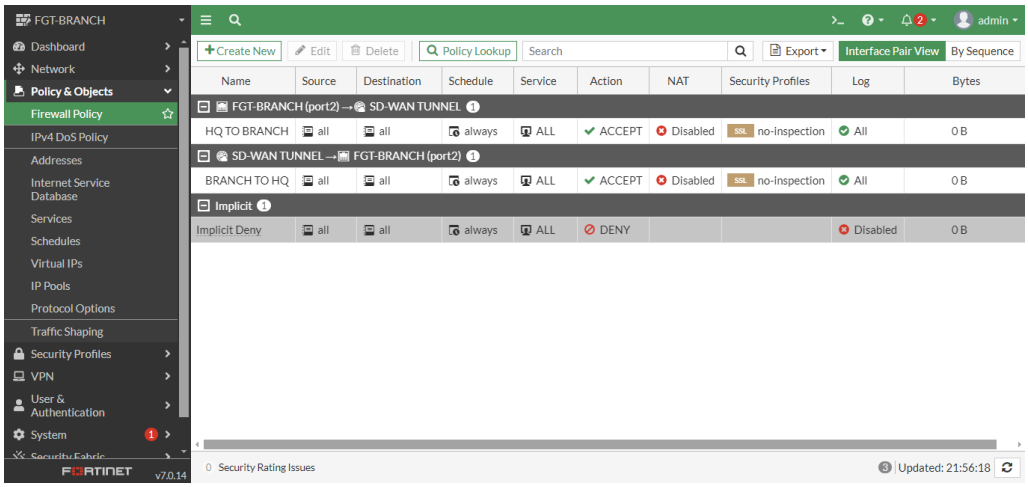
#Configure Firewall Policy

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



FGT-BRANCH



3. Pengujian

- **Ping dari PC-HQ ke PC-Branch**

PC-HQ ×

```
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:/#
```

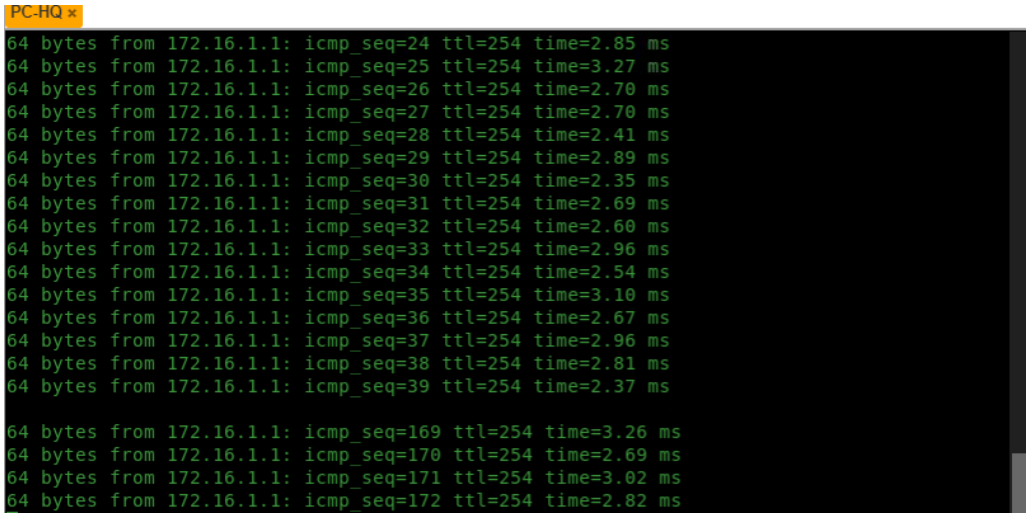
- **Ping dari PC-Branch ke PC-HQ dan WEB-SERVER**

PC-HQ × PC-BRANCH ×

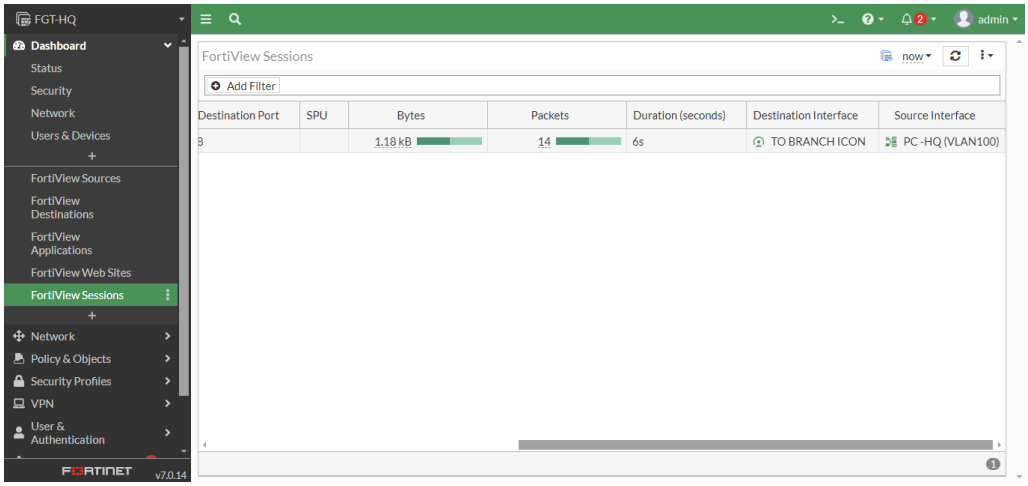
```
root@PC-BRANCH:/# ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data.
64 bytes from 192.168.1.1: icmp_seq=1 ttl=254 time=4.70 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=254 time=2.76 ms
64 bytes from 192.168.1.1: icmp_seq=3 ttl=254 time=2.48 ms
64 bytes from 192.168.1.1: icmp_seq=4 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**

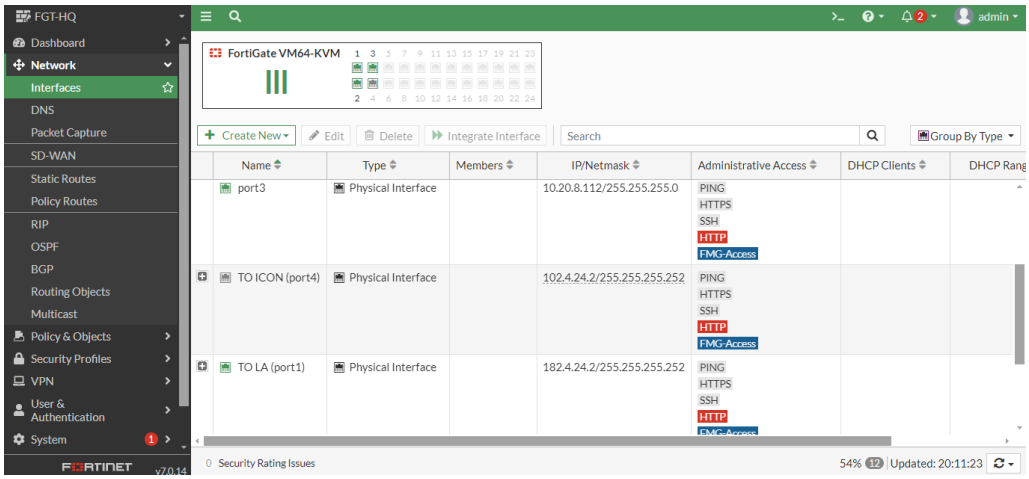
- **Failover PC-HQ ke PC-BRANCH**



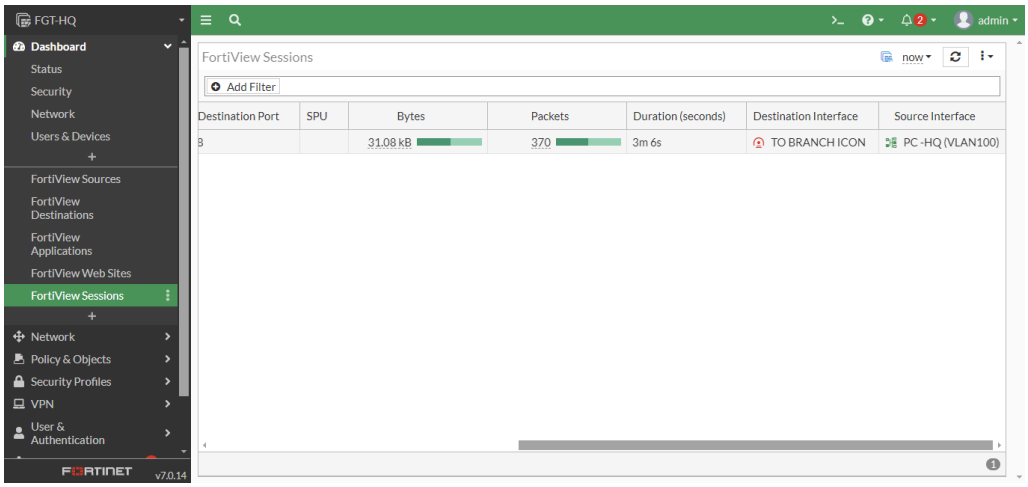
FortiView Session (Sebelum Disbale Tunnel)



Disbale Tunnel port4



FortiView Session (Disbale Tunnel)



FortiView Session (Setelah Disbale Tunnel)