



SIMULATION/LAB FORTIGATE FUNDAMENTAL

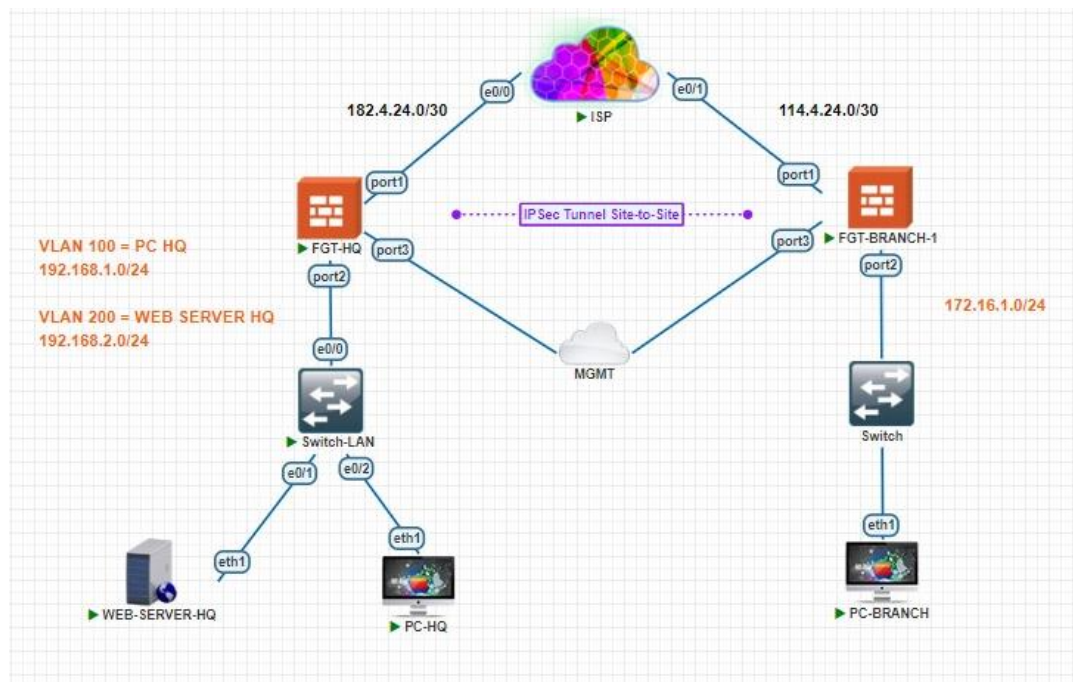
Implementation IPSec Tunnel Site-to-Site

- ✓ Interface (VLAN & LAN)
- ✓ Firewall Policy (FGT-HQ and FGT-Branch)
- ✓ IPSec Tunnel (FGT-HQ and FGT-Branch)
- ✓ Static Route (FGT-HQ and FGT-Branch)

Annisa Hadita

Mentor: Dito Prasetya

1. Topology



2. Task

Lab kesembilan ini bertujuan untuk membuat IPsec tunnel Site-to-Site dengan membuat jalur aman (tunnel) melalui internet publik untuk mengamankan komunikasi antara dua jaringan yang berbeda. Sehingga, Web-server dan PC-HQ dapat berkomunikasi dengan PC-Branch, dan sebaliknya.

#Configure Interface

Konfigurasi ini dilakukan untuk mengatur VLAN100 dan VLAN200 pada interface port2 di FGT-HQ serta jaringan LAN pada interface port2 di FGT-BRANCH. VLAN100 dan VLAN200 dibuat untuk memisahkan traffic jaringan yang berbeda, sedangkan jaringan LAN pada interface port2 di FGT-BRANCH memastikan bahwa PC-BRANCH dapat berkomunikasi dengan jaringan dengan PC-HQ dan WEB-SERVER melalui tunnel IPsec yang telah dikonfigurasi.

FGT-HQ

Name	Type	Members	IP/Netmask	Administrative Access	DHCP Clients
FGT-HQ (port2)	Physical Interface		0.0.0.0/0.0.0.0	PING HTTPS SSH HTTP FMG-Access	
PC-HQ (VLAN100)	VLAN		192.168.1.1/255.255.255.0	PING HTTPS SSH HTTP FMG-Access	
WEB-SERVER-HQ (VLAN200)	VLAN		192.168.2.1/255.255.255.0	PING HTTPS SSH	

FGT-Branch

Name	Type	Members	IP/Netmask	Administrative Access	DHCP Clients
FGT-BRANCH (port2)	Physical Interface		172.16.1.1/255.255.255.0	PING HTTPS SSH FMG-Access	
port1	Physical Interface		114.4.24.2/255.255.255.252	PING HTTPS SSH HTTP FMG-Access	
TO HQ	Tunnel Interface		0.0.0.0/0.0.0.0		
port3	Physical Interface		10.20.8.114/255.255.255.0	PING HTTPS	

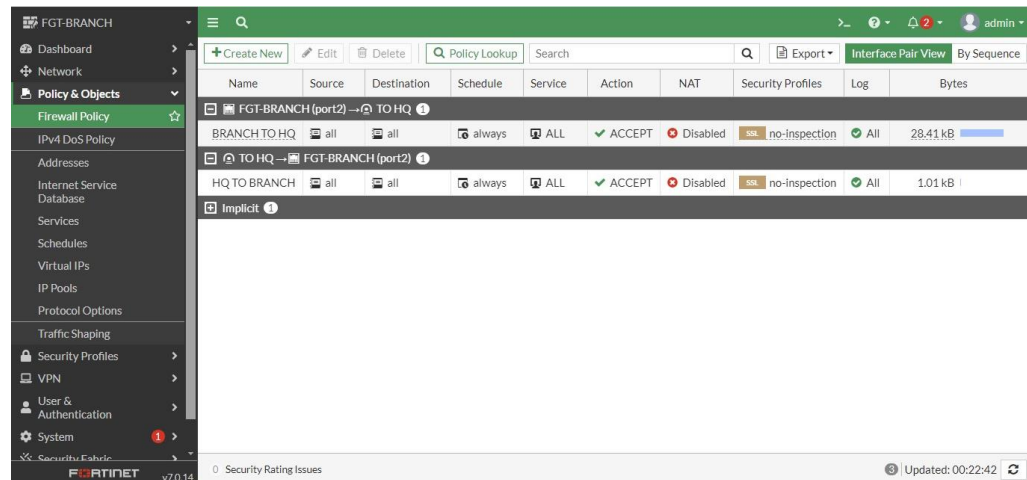
#Configure Firewall Policy

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

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

FGT-Branch



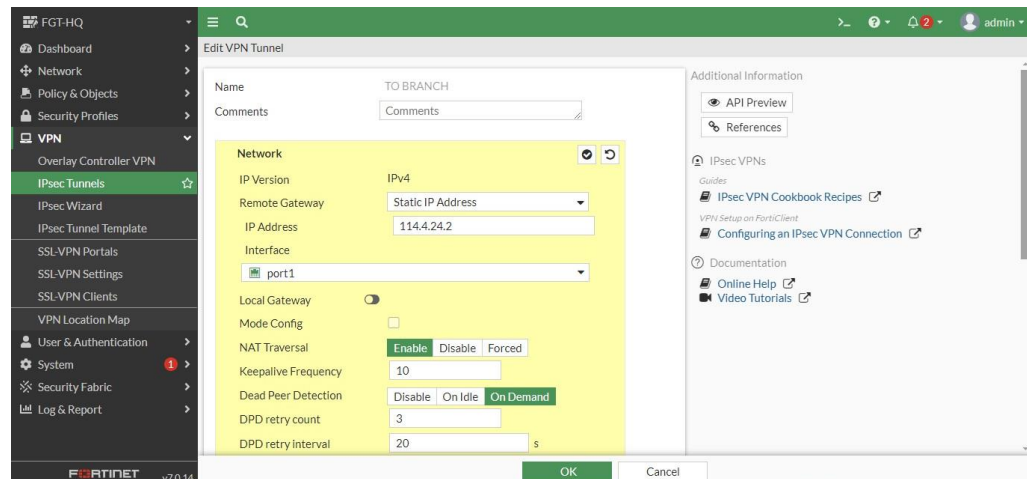
The screenshot shows the FortiGate FGT-BRANCH Firewall Policy configuration page. The left sidebar contains navigation options: Dashboard, Network, Policy & Objects, Firewall Policy, IPv4 DoS Policy, Addresses, Internet Service Database, Services, Schedules, Virtual IPs, IP Pools, Protocol Options, Traffic Shaping, Security Profiles, VPN, User & Authentication, and System. The main content area displays a table of firewall policies. The table has columns: Name, Source, Destination, Schedule, Service, Action, NAT, Security Profiles, Log, and Bytes. The policies listed are: FGT-BRANCH (port2) -> TO HQ, BRANCH TO HQ, TO HQ -> FGT-BRANCH (port2), HQ TO BRANCH, and Implicit. The 'Implicit' policy is highlighted.

Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	Bytes
FGT-BRANCH (port2) -> TO HQ	all	all	always	ALL	ACCEPT	Disabled	SSL no-inspection	All	28.41 kB
BRANCH TO HQ	all	all	always	ALL	ACCEPT	Disabled	SSL no-inspection	All	1.01 kB
TO HQ -> FGT-BRANCH (port2)	all	all	always	ALL	ACCEPT	Disabled	SSL no-inspection	All	1.01 kB
HQ TO BRANCH	all	all	always	ALL	ACCEPT	Disabled	SSL no-inspection	All	1.01 kB
Implicit									

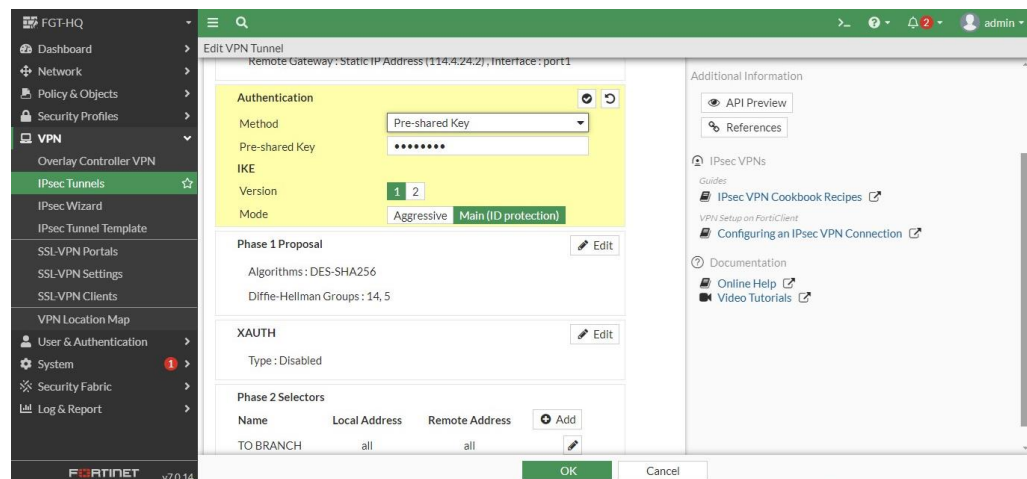
#Configure IPSec Tunnel

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

FGT-HQ



The screenshot shows the FortiGate FGT-HQ Edit VPN Tunnel configuration page. The left sidebar contains navigation options: 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, and Log & Report. The main content area displays the 'Edit VPN Tunnel' configuration page. The 'Name' field is set to 'TO BRANCH'. The 'Network' section is highlighted in yellow and contains the following fields: IP Version (IPv4), Remote Gateway (Static IP Address), IP Address (114.4.24.2), Interface (port1), Local Gateway (disabled), Mode Config (disabled), NAT Traversal (Enable, Disable, Forced), Keepalive Frequency (10), Dead Peer Detection (Disable, On Idle, On Demand), DPD retry count (3), and DPD retry interval (20 s). The 'Additional Information' section on the right contains links for 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 shows the FortiGate FGT-HQ Edit VPN Tunnel configuration page. The left sidebar contains navigation options: 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, and Log & Report. The main content area displays the 'Edit VPN Tunnel' configuration page. The 'Name' field is set to 'TO BRANCH'. The 'Authentication' section is highlighted in yellow and contains the following fields: Method (Pre-shared Key), Pre-shared Key (*****), IKE Version (1, 2), and Mode (Aggressive, Main (ID protection)). The 'Phase 1 Proposal' section contains the following fields: Algorithms (DES-SHA256) and Diffie-Hellman Groups (14, 5). The 'XAUTH' section contains the following field: Type (Disabled). The 'Phase 2 Selectors' section contains the following fields: Name, Local Address, Remote Address, and Add. The 'Additional Information' section on the right contains links for 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

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

Edit VPN Tunnel

Name: TO HQ

Comments: Comments

Network

IP Version: IPv4

Remote Gateway: Static IP Address

IP Address: 182.4.24.2

Interface: 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 ☐

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

Edit VPN Tunnel

Remote Gateway: Static IP Address (182.4.24.2) . Interface: port1

Authentication

Method: Pre-shared Key

Pre-shared Key: *****

IKE

Version: 1 2

Mode: Aggressive Main (ID protection)

Phase 1 Proposal

Algorithms: DES-SHA256

Diffie-Hellman Groups: 14, 5

XAUTH

Type: Disabled

Phase 2 Selectors

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

Edit VPN Tunnel

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

Phase 1 Proposal

Encryption: DES

Authentication: SHA256

Diffie-Hellman Groups

Key Lifetime (seconds): 86400

Local ID:

XAUTH

Type: Disabled

Phase 2 Selectors

Name: TO HQ

Local Address: all

Remote Address: all

Additional Information

API Preview

References

IPsec VPNs

Guides

IPsec VPN Cookbook Recipes

VPN Setup on FortiClient

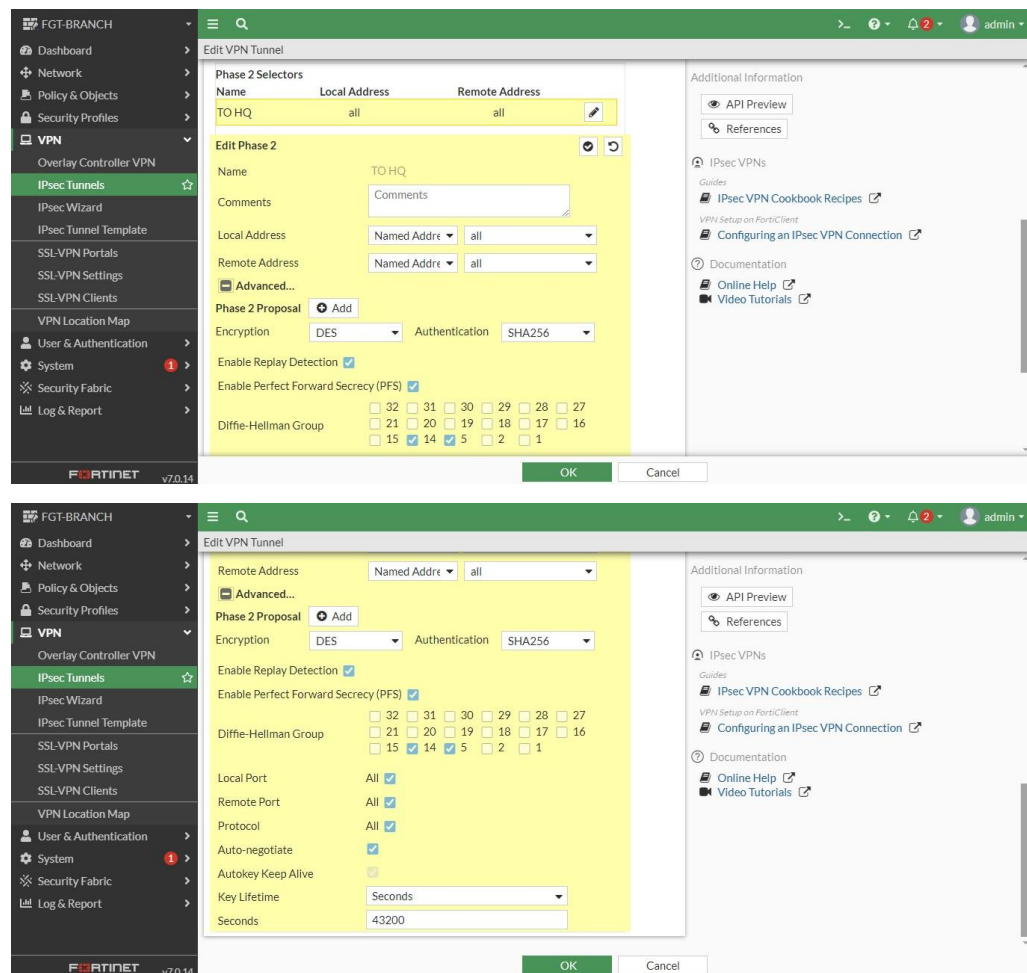
Configuring an IPsec VPN Connection

Documentation

Online Help

Video Tutorials

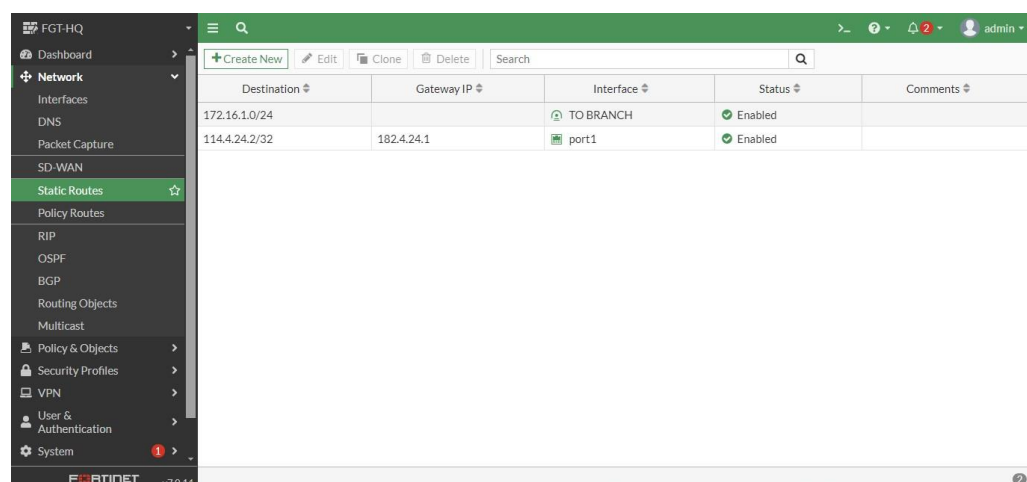
OKCancel



#Configure 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



FGT-Branch

FGT-BRANCH

Dashboard

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

Create New

Edit

Clone

Delete

Search

Destination	Gateway IP	Interface	Status	Comments
192.168.1.0/24		TO HQ	Enabled	
192.168.2.0/24		TO HQ	Enabled	
182.4.24.2/32	114.4.24.1	port1	Enabled	

FGTINET

v7.0.14

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=8.40 ms
64 bytes from 172.16.1.1: icmp_seq=2 ttl=254 time=2.84 ms
64 bytes from 172.16.1.1: icmp_seq=3 ttl=254 time=3.24 ms
64 bytes from 172.16.1.1: icmp_seq=4 ttl=254 time=3.05 ms
64 bytes from 172.16.1.1: icmp_seq=5 ttl=254 time=3.08 ms
^C
--- 172.16.1.1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4005ms
rtt min/avg/max/mdev = 2.839/4.122/8.403/2.144 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=3.27 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=254 time=1.97 ms
64 bytes from 192.168.1.1: icmp_seq=3 ttl=254 time=2.12 ms
64 bytes from 192.168.1.1: icmp_seq=4 ttl=254 time=2.51 ms
64 bytes from 192.168.1.1: icmp_seq=5 ttl=254 time=2.32 ms
^C
--- 192.168.1.1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4006ms
rtt min/avg/max/mdev = 1.970/2.437/3.268/0.453 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=2.74 ms
64 bytes from 192.168.2.1: icmp_seq=2 ttl=254 time=2.10 ms
64 bytes from 192.168.2.1: icmp_seq=3 ttl=254 time=1.81 ms
64 bytes from 192.168.2.1: icmp_seq=4 ttl=254 time=2.19 ms
64 bytes from 192.168.2.1: icmp_seq=5 ttl=254 time=2.12 ms
^C
--- 192.168.2.1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4006ms
rtt min/avg/max/mdev = 1.808/2.192/2.743/0.304 ms
root@PC-BRANCH:/#
```

- Akses WEB-SERVER dari PC-Branch

