

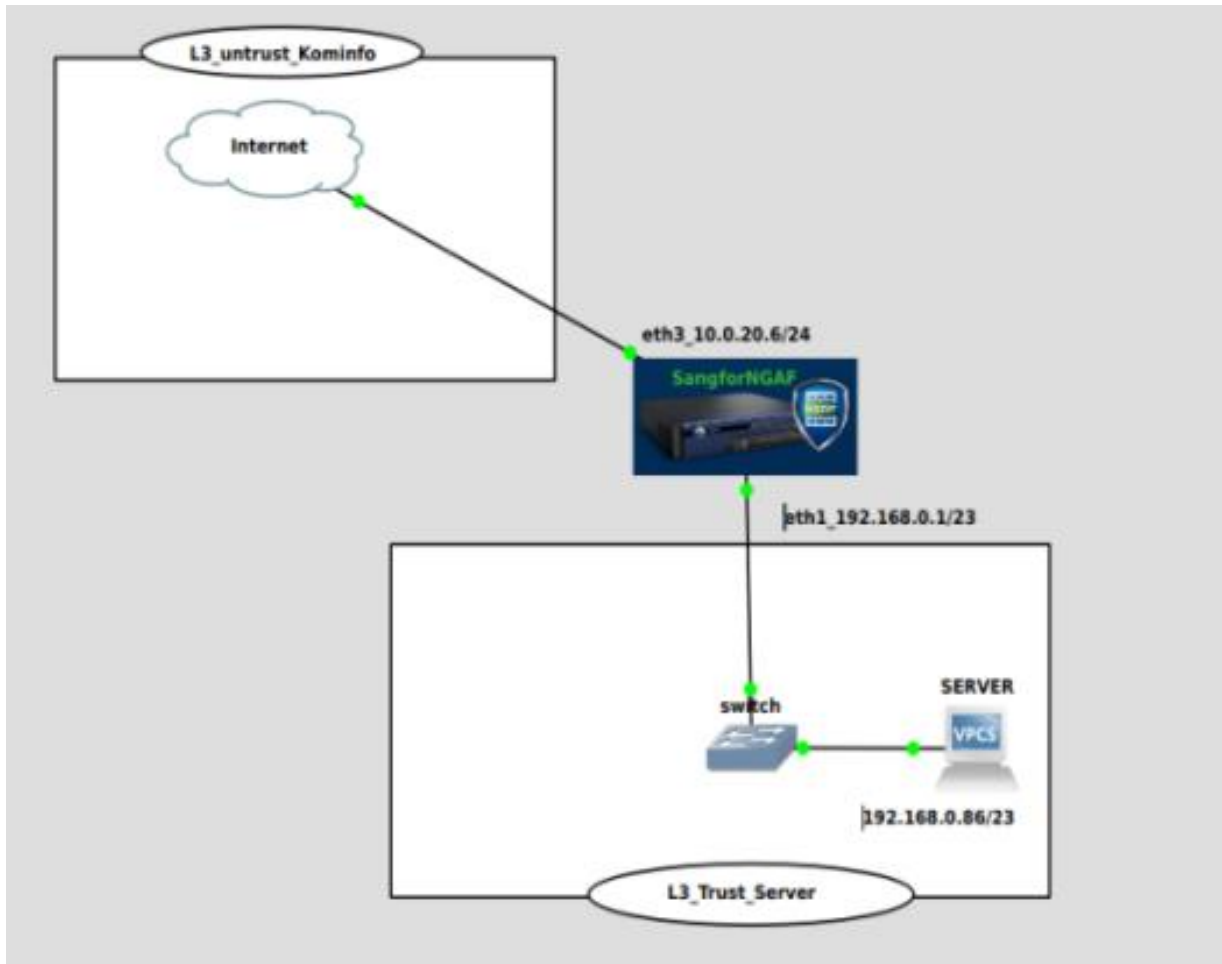
Distribusi Internet untuk User Pada Sangfor NGAF

***Product:**NGAF

***Version:**8.0.47

*1. Pengantar

1.1 Skenario



Pada tulisan kali ini, saya akan sharing terkait konfigurasi distribusi internet untuk pengguna/ server. Distribusi ini menggunakan firewall Sangfor. Skema topologi dalam tulisan ini adalah isp penyedia memberikan satu IP (10.0.20.6/24) kemudian masuk ke satu interface firewall sangfor dan didistribusikan ke IP server (192.168.0.86/23).

Hasil pengujian diperoleh bahwa internet dari ISP dapat didistribusikan ke server dengan baik. Untuk memastikan melalui PC Server dilakukan ping dan traceroute ke website global contohnya www.google.com. Adapun tahapan-tahapannya dapat mengikuti intuksi berikut dibawah ini.

1.2 Persyaratan

1. Pengguna memiliki perangkat Firewall NGAF
2. Memiliki minimal 1 ISP (Internet Service Provider)
3. Memiliki 1 PC untuk uji coba

*2. Panduan Konfigurasi

Segmen jaringan lokal untuk server dibuat class C dengan network 192.168.0.0/23, sedangkan dari penyedia ISP diperoleh IP 10.0.20.6/24 dengan gateway 10.0.20.1/24.

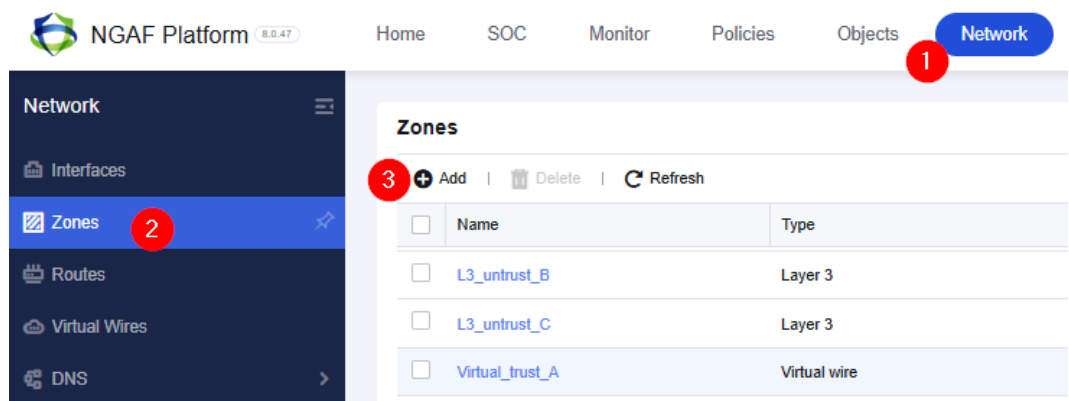
2.1. Membuat Zone

Pada skenario ini kita akan membuat 2 (dua) zona yaitu zona ISP yang dibuat dengan nama **L3_Untrust_Kominfo** dan satu zona lagi yaitu zona Server yang dibuat dengan nama **L3_Trust_Server**.

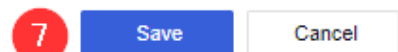
a. Zone Untrust Kominfo

Langkah-langkah nya seperti pada gambar berikut dibawah ini:

1. Klik **Network → Zones → Add**



2. Masukan **Name : L3_Untrust_Kominfo**
Type : Layer3
Interface : eth3



3. **Simpan**, jika berhasil maka seperti gambar dibawah ini

Zones			
+ Add Delete Refresh			
<input type="checkbox"/>	Name	Type	Interfaces
<input type="checkbox"/>	Virtual_trust_B	Virtual wire	-
<input type="checkbox"/>	Virtual_untrust_A	Virtual wire	-
<input type="checkbox"/>	Virtual_untrust_B	Virtual wire	-
<input type="checkbox"/>	L3_Untrust_Kominfo	Layer 3	eth3

b. Zone Trust Server

Langkah-langkah nya seperti pada gambar berikut dibawah ini:

1. Klik **Network → Zones → Add**

The screenshot shows the NGAF Platform interface. The top navigation bar includes 'Home', 'SOC', 'Monitor', 'Policies', 'Objects', and 'Network' (highlighted with a red circle 1). The left sidebar shows 'Network' as the selected section, with sub-items: 'Interfaces', 'Zones' (highlighted with a red circle 2), 'Routes', 'Virtual Wires', and 'DNS'. The main content area displays the 'Zones' table, which includes an 'Add' button (highlighted with a red circle 3) and a table with columns 'Name' and 'Type'. The table lists three zones: 'L3_untrust_B' (Layer 3), 'L3_untrust_C' (Layer 3), and 'Virtual_trust_A' (Virtual wire).

2. Masukkan **Name** : **L3_Trust_Server**
Type : **Layer3**
Interface : **eth1**

Name: **4** L3_Trust_Server

Type: ☐ Layer 2 **5** ☒ Layer 3 ☐ Virtual wire

Interfaces

Available (18)

Search

- ☐ veth.90
- ☐ veth.97
- ☐ veth.5
- ☐ veth.99
- ☐ veth.101
- ☐ vpntun
- 6** ☒ eth1

Selected (1) [Clear](#)

Search

eth1

7 [Save](#) [Cancel](#)

3. **Simpan**, jika berhasil maka seperti gambar dibawah ini

Zones

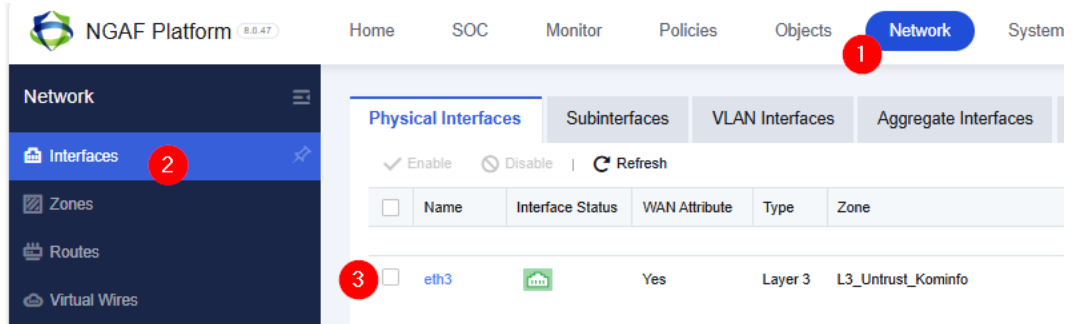
+ Add Delete Refresh			
<input type="checkbox"/>	Name	Type	Interfaces
<input type="checkbox"/>	L3_untrust_B	Layer 3	-
<input type="checkbox"/>	L3_untrust_C	Layer 3	-
<input type="checkbox"/>	Virtual_trust_A	Virtual wire	-
<input type="checkbox"/>	Virtual_trust_B	Virtual wire	-
<input type="checkbox"/>	Virtual_untrust_A	Virtual wire	-
<input type="checkbox"/>	Virtual_untrust_B	Virtual wire	-
<input type="checkbox"/>	L3_Untrust_Kominfo	Layer 3	eth3
<input type="checkbox"/>	L3_Trust_Server	Layer 3	eth1

2.2. Setting interface

Langkah selanjutnya setelah membuat zona adalah melakukan konfigurasi pada interface tempat kita akan memasukkan zona yang telah dibuat diatas. Interface **eth1** untuk Zona **L3_Trust_Server**, dan **eth3** untuk Zona **L3_Untrust_Kominfo**.

a. Konfigurasi eth3 (L3_Untrust_Kominfo)

1. Masuk ke menu **Network→Interface→Eth3**



2. Pilih **Status** : **enabled**

Description : WAN(Diskominfo)

Type : layer 3

Zone : L3_Untrust_Kominfo

Basic Attribute: WAN attribute (v)

Ip static: 10.0.20.6/24

Nexthop : 10.0.20.1 (ini adalah gateway dari ISP kominfo)

Klik **Save**, seperti gambar dibawah ini.

Name: eth3

Status: (4) ☒ Enabled ☐ Disabled

Description: (5) WAN (Diskominfo)

Type: (6) Layer 3

Zone: (7) L3_Untrust_Kominfo

Basic Attributes: ☒ WAN attribute (8)

System Upgrade: ☐ Temporarily use this interface for system upgrade ⓘ

IPv4 IPv6 Link State Detection Advanced

IP Assignment: ☒ Static ☐ DHCP ☐ PPPoE

Static IP: (9) 10.0.20.6/24 ⓘ

Next-Hop IP: (10) 10.0.20.1 ⓘ

Link Bandwidth: Outbound 1000 Mbps Inbound 1000 Mbps

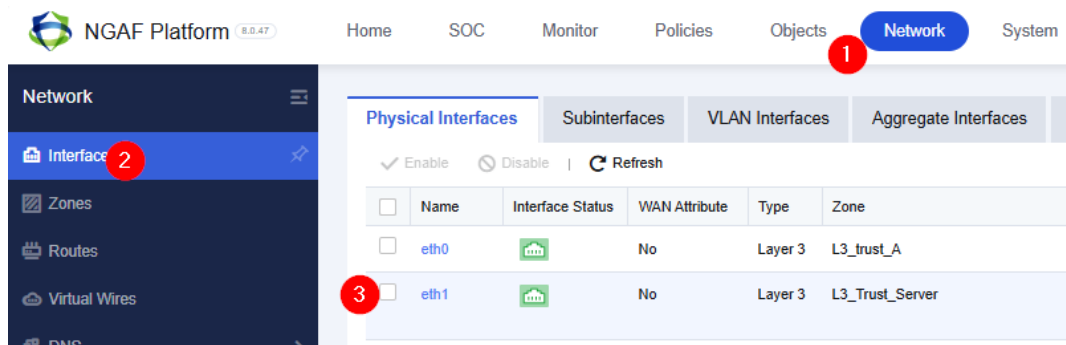
Management Service

Allow: ☒ WEBUI ☒ PING ☒ SNMP ☒ SSH

(11) **Save** Cancel

b. Konfigurasi eth1 (L3_Trust_Server)

1. Masuk ke menu **Network→Interface→Eth1**



2. Pilih **Status** : **enabled**
Description : **Server-DataCenter**
Type : **layer 3**
Zone : **L3_Trust_Server**
Ip static: 192.168.0.1/23
 Klik **Save**, seperti gambar dibawah ini.

Basics

Name: 4 eth1

Status: 5 ☒ Enabled ☐ Disabled

Description: 6 Server-DataCenter

Type: 7 Layer 3

Zone: 8 L3_Trust_Server

Basic Attributes: ☐ WAN attribute

System Upgrade: ☐ Temporarily use this interface for system upgrade ⓘ

IPv4 IPv6 Link State Detection Advanced

IP Assignment: 9 ☒ Static ☐ DHCP ☐ PPPoE

Static IP: 10 192.168.0.1/23 ⓘ

Next-Hop IP: ⓘ

Link Bandwidth: Outbound 10240 Mbps Inbound 10240 Mbps

Management Service

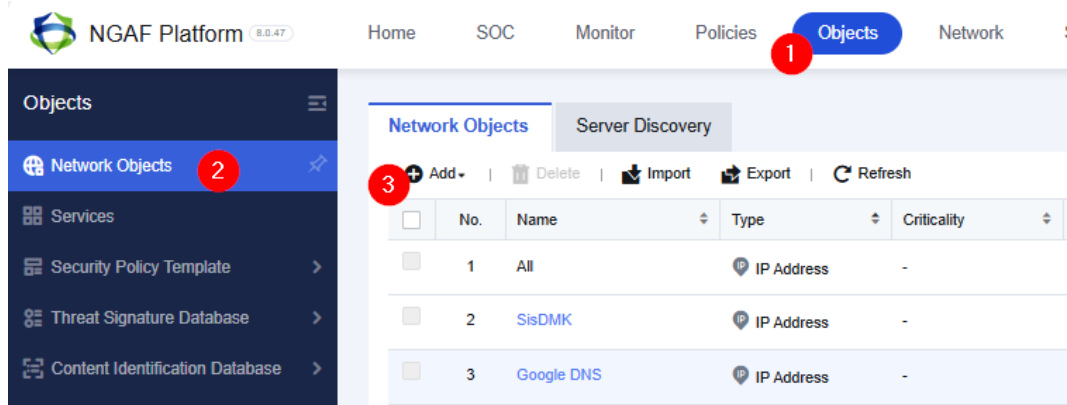
Allow: ☒ WEBUI ☒ PING ☒ SNMP ☒ SSH

11 **Save** Cancel

2.3. Buat Network Objects

Langkah selanjutnya membuat beberapa **network object**. Adapun langkah-langkahnya sebagai berikut:

1. Klik menu **Objects** → **Network Objects** → **Add**



2. Masukkan type : **IP Address**
 Name : **IP Address Server**
 Protocol : **IPV4**
 IP : **192.168.0.0/23**
 Klik **Save** seperti pada gambar dibawah ini.

Type: **4** ☒ IP Address ☐ Business Asset Address ☐ User IP Address

Basics

Name: **5** IP Address Server

Description: Optional

Address Group: Optional

IP Address

Protocol: ☒ IPv4 ☐ IPv6

6 IP Address: 192.168.0.2-192.168.0.79
 192.168.0.81-192.168.0.91
 192.168.0.93-192.168.0.254
 192.168.1.2-192.168.1.254

7 **Save** **Cancel**

3. Jika berhasil seperti gambar berikut ini

Network Objects

Server Discovery

Add

Delete

Export

Refresh

All

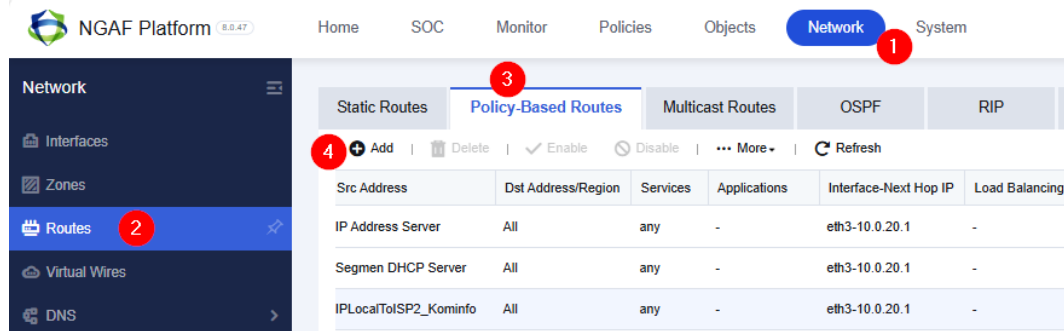
<input type="checkbox"/>	No.	Name	Type	Criticality	Address	Description
<div><div></div><div>IP Addr was found in 1 entries</div><div>Cancel</div></div>						
<input type="checkbox"/>	1	IP Address Server	<div><div></div><div>IP Address</div></div>	-	192.168.0.2-192.168.0.79 192.168.0.81-192.168.0.91 192.168.0.93-192.168.0.254 192.168.1.2-192.168.1.254	-

2.4. Menambahkan Konfigurasi di Policy Based Routes

Setelah tahapan diatas telah dilakukan, maka langkah selanjutnya adalah menambahkan

policy based routes. Dalam firewall Sangfor NGAF dapat dilakukan sebagai berikut:

1. Buka menu **Network→Routes→Policy →Based Routes→Add**



2. Masukkan

Route Type : source-based-route
Protocol : IPV4
Name : Internet ISP Kominfo
Status : enabled
Move to : Top
Src Zone : L3_Trust_Server
Src Address : IP Address Server
Destination : ISP → All
Services : Any
Outbound Interface: Interface → Eth3

Secara detil seperti gambar berikut dibawah ini,

Add Policy-Based Route

Route Type: **5** ☒ Source-based route ☐ Link load-balancing

Protocol: **6** ☒ IPv4 ☐ IPv6

Basics

Name: **7** Internet ISP Kominfo

Status: **8** ☒ Enabled ☐ Disabled

Description: Optional

Move To: **9** Top

Schedule: **10** All week

Data Packet

Src Zone: **11** L3_Trust_Server

Src Address: **12** IP Address Server

Destination: ☐ Network Object **13** ☒ ISP ☐ Country/Region

14 All

Services: **15** any

Others

Outbound Interface: ☒ Interface **16** ☐ Next-Hop IP

17 eth3

Link State Detection: Settings

Save and Copy

18 Save

Cancel

3. Klik **Save**, dan jika berhasil akan muncul seperti gambar berikut ini:

Static Routes

Policy-Based Routes

Multicast Routes

OSPF

RIP

BGP

All Routes

Route Testing

+

Add

✖

Delete

✓

Enable

⏻

Disable

⋮

More

↻

Refresh

IPv4

<input type="checkbox"/>	No.	Name	Protocol	Src Zone	Src Address	Dst Address/Region	Services	Applications	Interface-Next Hop IP
<input type="checkbox"/>	1	Internet ISP Kominfo	ipv4	L3_Trust_Server	IP Address Server	All	any	-	eth3-10.0.20.1

2.5. Menambahkan SNAT

Langkah selanjutnya adalah membuat NAT untuk akses ke internet.

1. Klik **Policies** → **NAT** → **Ipv4 NAT** → **add**

NGAF Platform 8.0.47 Home SOC Monitor **1** Policies Objects Network System

Policies

- Access Control
- NAT** **2**
- Network Security
- Decryption
- Bandwidth Management
- Authentication

IPv4 NAT DNS Mapping

3

+

 Add

✕

 Delete

✓

 Enable

⏻

 Disable

↕

 Move To

⋮

 More

↻

 Refresh

No.	Name	Type	Src Zone	Src Address	Dst Zone/Interface	Dst Address
2	PRT...	DNAT	L3_Untrust_Ko... L3_Untrust_MIK... L3_Untrust_Biznet	All	-	IP WAN Biznet-1

prtg was found in 5 entries [Cancel](#)

2. Kemudian isikan,

Type : Source NAT
Name : SNAT Internet Server
Status : enabled
Move To : Top
Src Zone : L3_Trust_Server
Src Address : IP Address Server
Dst Zone/Interface: Zone → L3_Untrust_Kominfo
Dst Address : All
Services : Any
Translate Src IP To: Outbound Interface
 Secara detail seperti gambar dibawah ini,

Add NAT Policy

Type: **4** ☒ Source NAT ☐ Destination NAT ☐ Bidirectional NAT

Basics

Name: **5** SNAT Internet Server

Status: **6** ☒ Enabled ☐ Disabled

Description: Optional

Move To: **7** Top

Schedule: All week

Original Data Packet

Src Zone: **8** L3_Trust_Server

Src Address: **9** IP Address Server

Dst Zone/Interface: ☒ Zone **10** ☐ Interface

11 L3_Untrust_Kominfo

Dst Address: **12** All

Services: **13** any

Translated Data Packet

Translate Src IP To: Outbound Interface **14**

Translate Dst IP To: Untranslated

Translate Dst Port To: Untranslated

15 Save and Copy Save Cancel

3. Klik **Save**, jika benar akan tampak seperti gambar berikut dibawah ini

IPv4 NAT									
DNS Mapping									
Add Delete Enable Disable Move To More Refresh									
	No.	Name	Type	Original Data Packet			Translated Data Packet		
				Src Zone	Src Address	Dst Zone/Interface	Dst Address	Services	Src Address
<input type="checkbox"/>	1	SNAT Internet Server	SNAT	L3_Trust_Server	IP Address Server	L3_Untrust_Kominfo	All	any	Outbound Interface

2.6. Melakukan Ujicoba

Tahap terakhir yang bisa dilakukan adalah dengan melakukan ujicoba di sisi komputer server. contoh (**ip 192.168.0.86/23**). Pertama kita masukan IP server yang telah berjalan. Kedua melakukan **ping** ke situs internet contoh www.google.com dan ketiga, kita lakukan traceroute ke situs global tersebut untuk memastikan jalur yang dilewati sudah benar.

Dari hasil pengecekan diperoleh sebagai berikut:

a. Cek IP Interface Server

```
Administrator: Command Prompt

Windows IP Configuration

Host Name . . . . . : WIN-8023IPQF8DU
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No

Ethernet adapter Ethernet:

Connection-specific DNS Suffix . :
Description . . . . . : Intel(R) PRO/1000 MT Desktop Adapter
Physical Address. . . . . : 08-00-27-09-27-C8
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . : Yes
Link-local IPv6 Address . . . . : fe80::d883:c0cc:9db6:f69212(Preferred)
IPv4 Address. . . . . : 192.168.0.86(Preferred)
Subnet Mask . . . . . : 255.255.254.0
Default Gateway . . . . . : 192.168.0.1
DHCPv6 Iaid . . . . . : 302514215
DHCPv6 Client DUID. . . . . : 00-01-00-01-25-C0-C5-F7-08-00-27-09-27-C8

DNS Servers . . . . . : 8.8.8.8
                       203.142.84.222
NetBIOS over Tcpip. . . . . : Enabled

Tunnel adapter isatap.{896CBEED-754F-4096-9D5A-5177A55D97AF}:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Description . . . . . : Microsoft ISATAP Adapter
Physical Address. . . . . : 00-00-00-00-00-00-E0
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . : Yes

C:\Users\Administrator>
```

b. Ping google.com

Komputer dapat melakukan **PING** dengan baik terhadap situs global www.google.com

```
Administrator: Command Prompt

C:\Users\Administrator>ping google.com

Pinging google.com [142.251.175.139] with 32 bytes of data:
Reply from 142.251.175.139: bytes=32 time=23ms TTL=105
Reply from 142.251.175.139: bytes=32 time=23ms TTL=105
Reply from 142.251.175.139: bytes=32 time=23ms TTL=105
Reply from 142.251.175.139: bytes=32 time=23ms TTL=105

Ping statistics for 142.251.175.139:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 23ms, Maximum = 23ms, Average = 23ms

C:\Users\Administrator>
```

c. Traceroute google.com

Komputer dapat melakukan **traceroute** ke situs global www.google.com dengan jalur yang dilalui yaitu gateway ISP Kominfo 10.0.20.1.

```
Administrator: Command Prompt - tracert google.com
15 * * ^C
C:\Users\Administrator>tracert google.com

Tracing route to google.com [142.251.175.139]
over a maximum of 30 hops:

  1  <1 ms    <1 ms    <1 ms    192.168.0.1
  2  5 ms     3 ms     1 ms     10.0.20.1
  3  <1 ms    <1 ms    <1 ms    192.168.253.1
  4  1 ms     <1 ms    <1 ms    10.127.252.1
  5  11 ms    11 ms    11 ms    ip-74.184.hsp.net [103.134.184.74]
  6  10 ms    11 ms    10 ms    ip-66.162.hsp.net [103.139.162.66]
  7  22 ms    25 ms    24 ms    ip-254.30.hsp.net.id [103.115.30.254]
  8  25 ms    24 ms    25 ms    72.14.195.20
  9  22 ms    22 ms    22 ms    142.250.238.115
 10  22 ms    23 ms    22 ms    192.178.109.94
 11  24 ms    24 ms    24 ms    209.85.255.43
 12  24 ms    24 ms    23 ms    142.251.252.41
 13  23 ms    22 ms    23 ms    142.251.247.197
 14
```

*3. Pencegahan

1. Sebelum melakukan setting untuk mendistribusikannya di firewall, anda bisa memastikan internet dari ISP dapat berfungsi dengan baik
2. IP yang kami gunakan dapat anda ganti dan disesuaikan dengan kondisi lingkungan anda
3. Pastikan mengikuti langkah-langkah tersebut dengan teliti dan periksa DNS yang anda gunakan