

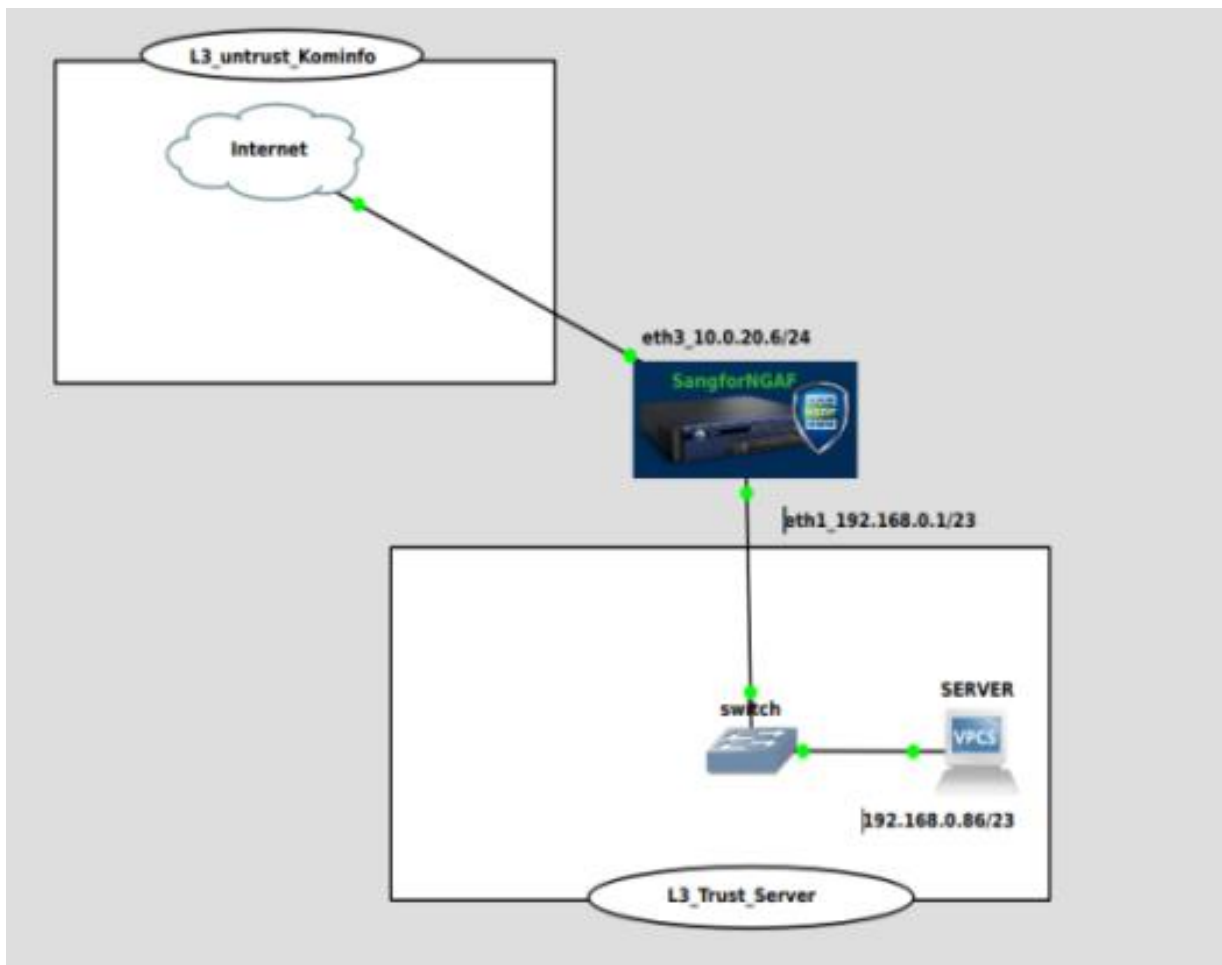
Internet Distribution At Sangfor NGAF Device

***Product:** NGAF

***Version:** 8.0.47

*1. Introduction

1.1 Scenario



In this article, I will share internet distribution configurations for users/servers. This distribution uses the Sangfor firewall. The topology scheme in this paper is that the ISP provider provides one IP (10.0.20.6/24) which is then set in the Sangfor interface and distributed to the server IP (192.168.0.86/23).

The test results showed that the internet from the ISP could be distributed to the server well. To ensure that via the PC Server, ping and traceroute are carried out to a global website, for example, www.google.com. As for the steps, you can follow the instructions

below.

1.2 Requirements

- 1) The organization has an NGAF Firewall device
- 2) Have at least 1 ISP (Internet Service Provider)
- 3) Have 1 PC for testing

*2. Configuration Guide

The local network segment for the server is made class C with network 192.168.0.0/23, from the ISP provider we get IP 10.0.20.6/24 and the gateway is 10.0.20.1/24.

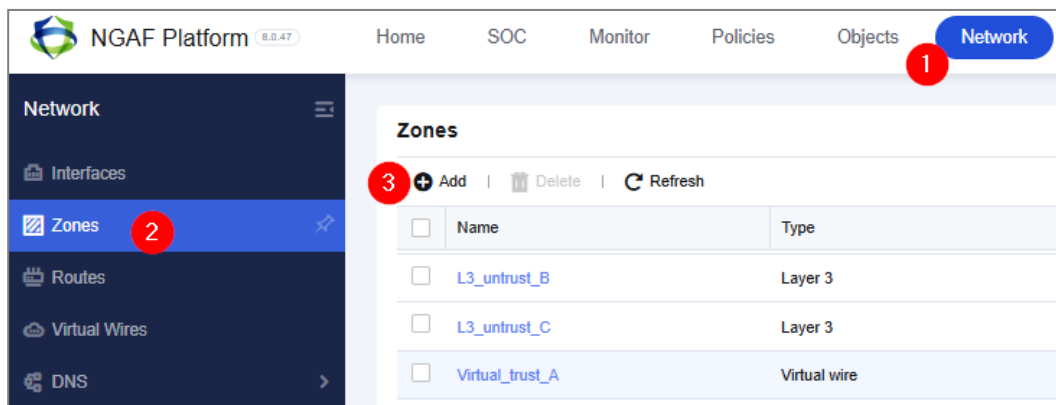
2.1. Create Zones

In this scenario, we will create 2 (two) zones, namely the ISP zone created with the name **L3_Untrust_Kominfo**, and another zone, namely the Server zone created with the name **L3_Trust_Server**.

a. Untrust Kominfo Zone

The steps are as follows below::

1. Click **Network → Zones → Add**



2. Insert **Name: L3_Untrust_Kominfo**

Type: Layer3

Interface: eth3

Name: **4** L3_Untrust_Kominfo

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

Interfaces

Available (17)

Search

- ☐ veth.90
- ☐ veth.97
- ☐ veth.5
- ☐ veth.99
- ☐ veth.101
- ☐ vpntun
- 6** ☒ eth3

Selected (1) [Clear](#)

Search

- eth3

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

3. Click Save, If successful it will look like the image below

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 checked="" type="checkbox"/>	L3_Untrust_Kominfo	Layer 3	eth3

b. Trust Server Zone

The steps are as follows below:

1. Click **Network → Zones → Add**

NGAF Platform 8.0.47

Home SOC Monitor Policies Objects **1** [Network](#)

Network

- Interfaces
- 2** [Zones](#)
- Routes
- Virtual Wires
- DNS

Zones

3 [+ Add](#) | [Delete](#) | [Refresh](#)

<input type="checkbox"/>	Name	Type
<input type="checkbox"/>	L3_untrust_B	Layer 3
<input type="checkbox"/>	L3_untrust_C	Layer 3
<input type="checkbox"/>	Virtual_trust_A	Virtual wire

2. Insert **Name: L3_Trust_Server**

Type: Layer3

Interface: eth1

The screenshot shows a configuration form for a new zone. At the top, the 'Name' field is set to 'L3_Trust_Server' (callout 4). Below it, the 'Type' is set to 'Layer 3' (callout 5), with 'Layer 2' and 'Virtual wire' as options. Under the 'Interfaces' section, there are two panels: 'Available (18)' and 'Selected (1)'. In the 'Available' panel, 'eth1' is selected with a checkmark (callout 6). In the 'Selected' panel, 'eth1' is listed. At the bottom right, there is a 'Save' button (callout 7) and a 'Cancel' button.

3. Save, If successful it will look like the image below

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

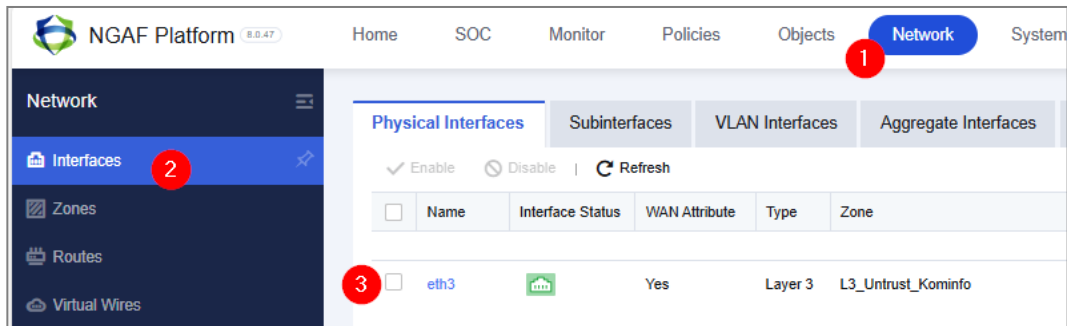
2.2. Setting the Interfaces

The next step after creating the zones is to configure the interface where we will enter the zone that was created above. **eth1** interface for **L3_Trust_Server** Zone, and **eth3** for

L3_Untrust_Kominfo Zone.

a. Configure eth3 (L3_Untrust_Kominfo)

1. Click the menu Network→Interface→ Eth3



2. Choose **Status: enabled**

Description: WAN(Diskominfo)

Type: layer 3

Zone: L3_Untrust_Kominfo

Basic Attribute: WAN attribute (checklist)

Ip static: 10.0.20.6/24

Nexhope: 10.0.20.1 (this is a gateway from ISP)

Click **Save**, like the image below.

The screenshot shows the configuration page for the eth3 interface. The form includes the following fields and options:

- Name: eth3
- Status: ☒ Enabled ☐ Disabled (highlighted with a red circle 4)
- Description: WAN (Diskominfo) (highlighted with a red circle 5)
- Type: Layer 3 (highlighted with a red circle 6)
- Zone: L3_Untrust_Kominfo (highlighted with a red circle 7)
- Basic Attributes: ☒ WAN attribute (highlighted with a red circle 8)
- System Upgrade: ☐ Temporarily use this interface for system upgrade

The IP Configuration section is expanded, showing the following options:

- IPv4: ☒ Static ☐ DHCP ☐ PPPoE
- Static IP: 10.0.20.6/24 (highlighted with a red circle 9)
- Next-Hop IP: 10.0.20.1 (highlighted with a red circle 10)

The Link Bandwidth section shows Outbound and Inbound bandwidths set to 1000 Mbps.

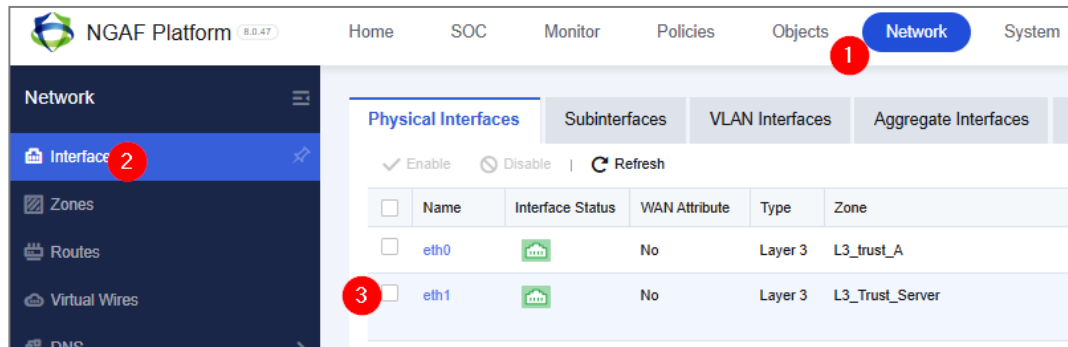
The Management Service section shows the following options:

- Allow: ☒ WEBUI ☒ PING ☒ SNMP ☒ SSH

The bottom of the form includes a Save button (highlighted with a red circle 11) and a Cancel button.

b. Configure eth1 (L3_Trust_Server)

1. Click menu **Network→Interface→Eth1**



2. Choose **Status :enabled**

Description : Server-DataCenter

Type : layer 3

Zone : L3_Trust_Server

Ip static: 192.168.0.1/23

Click **Save**, like the image below.

The screenshot shows the configuration page for the 'eth1' interface. The 'Basics' tab is active, and the following fields are filled out:

- Name: eth1 (red circle 4)
- Status: Enabled (red circle 5)
- Description: Server-DataCenter (red circle 6)
- Type: Layer 3 (red circle 7)
- Zone: L3_Trust_Server (red circle 8)
- Basic Attributes: ☐ WAN attribute
- System Upgrade: ☐ Temporarily use this interface for system upgrade

The 'IPv4' tab is active, and the following fields are filled out:

- IP Assignment: Static (red circle 9)
- Static IP: 192.168.0.1/23 (red circle 10)
- Next-Hop IP: (empty)
- Link Bandwidth: Outbound 10240 Mbps, Inbound 10240 Mbps

The 'Management Service' section shows the following services checked:

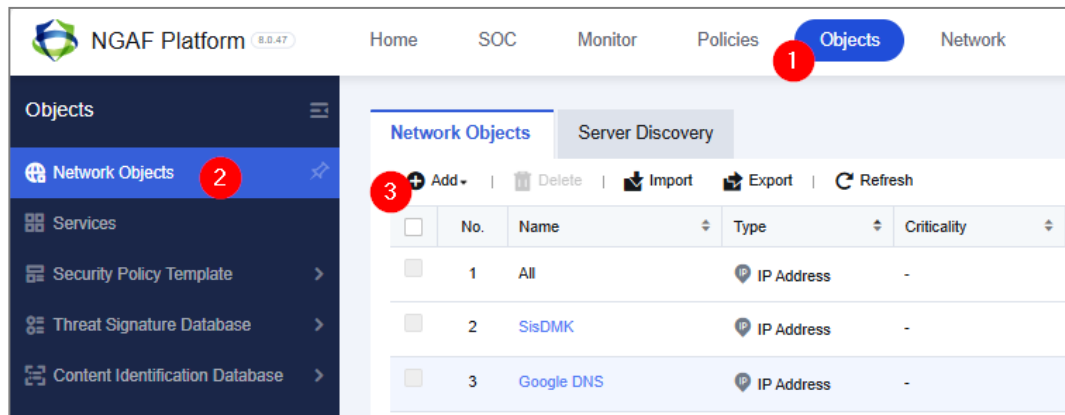
- Allow: ☒ WEBUI, ☒ PING, ☒ SNMP, ☒ SSH

The 'Save' button is highlighted with a red circle 11.

2.3. CreateThe Network Objects

The next step is to create a network object. The steps are as follows:

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



2. Choose **Type** : IP Address

Name : IP Address Server

Protocol : IPV4

IP : 192.168.0.0/23

Click **Save** like the image below

The screenshot shows the 'Add Network Object' form. At the top, there are radio buttons for 'Type': **IP Address** (selected, highlighted with a red circle 4), Business Asset Address, and User IP Address. Below this is the 'Basics' section with fields for 'Name' (IP Address Server, highlighted with a red circle 5), 'Description' (Optional), and 'Address Group' (Optional). The 'IP Address' section has radio buttons for 'Protocol': **IPv4** (selected) and IPv6. Below this is the 'IP Address' field (highlighted with a red circle 6) containing the range 192.168.0.2-192.168.0.79, 192.168.0.81-192.168.0.91, 192.168.0.93-192.168.0.254, and 192.168.1.2-192.168.1.254. At the bottom right, there is a 'DNS Lookup' button and a 'Save' button (highlighted with a red circle 7) next to a 'Cancel' button.


3. If successful it will look like the image below

Network Objects		Server Discovery				
<div> <div>+</div> Add </div> <div> <div>✕</div> Delete </div> <div> <div>📄</div> Export </div> <div> <div>🔄</div> Refresh </div> <div>All</div>						
<input type="checkbox"/>	No.	Name	Type	Criticality	Address	Description
<div> <div>🔔</div> IP Addr was found in 1 entries <div>Cancel</div> </div>						
<input type="checkbox"/>	1	IP Address Server	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	-

2.4. AddPolicy Based Routes

After the above steps have been carried out, the next step is to add **policy based routes**. In the Sangfor NGAF firewall this can be done as follows:

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

 NGAF Platform 8.0.47

Home

SOC

Monitor

Policies

Objects

Network

System

Network

Interfaces

Zones

Routes

Virtual Wires

DNS

Static Routes

Policy-Based Routes

Multicast Routes

OSPF

RIP

+

Add

✕

Delete

✓

Enable

🚫

Disable

⋮

More

🔄

Refresh

Src Address	Dst Address/Region	Services	Applications	Interface-Next Hop IP	Load Balancing
IP Address Server	All	any	-	eth3-10.0.20.1	-
Segmen DHCP Server	All	any	-	eth3-10.0.20.1	-
IPLocalToISP2_Kominfo	All	any	-	eth3-10.0.20.1	-

2. Input the information:

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

In detail as in the following image below,

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

18 Save and Copy Save Cancel

3. Click **Save**, if successful it will look like the image below

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. Add SNAT

The next step is to create NAT for access to the internet.

1. Click **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. Then choose,

Type : Source NAT
Name : SNAT Internet Server
status : Pilih 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

In detail as in the following image below,

3. Click **Save**, If successful it will look like the image below

IPv4 NAT									
DNS Mapping									
+ Add Delete Enable Disable Move To More Refresh									
Original Data Packet									
	No.	Name	Type	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

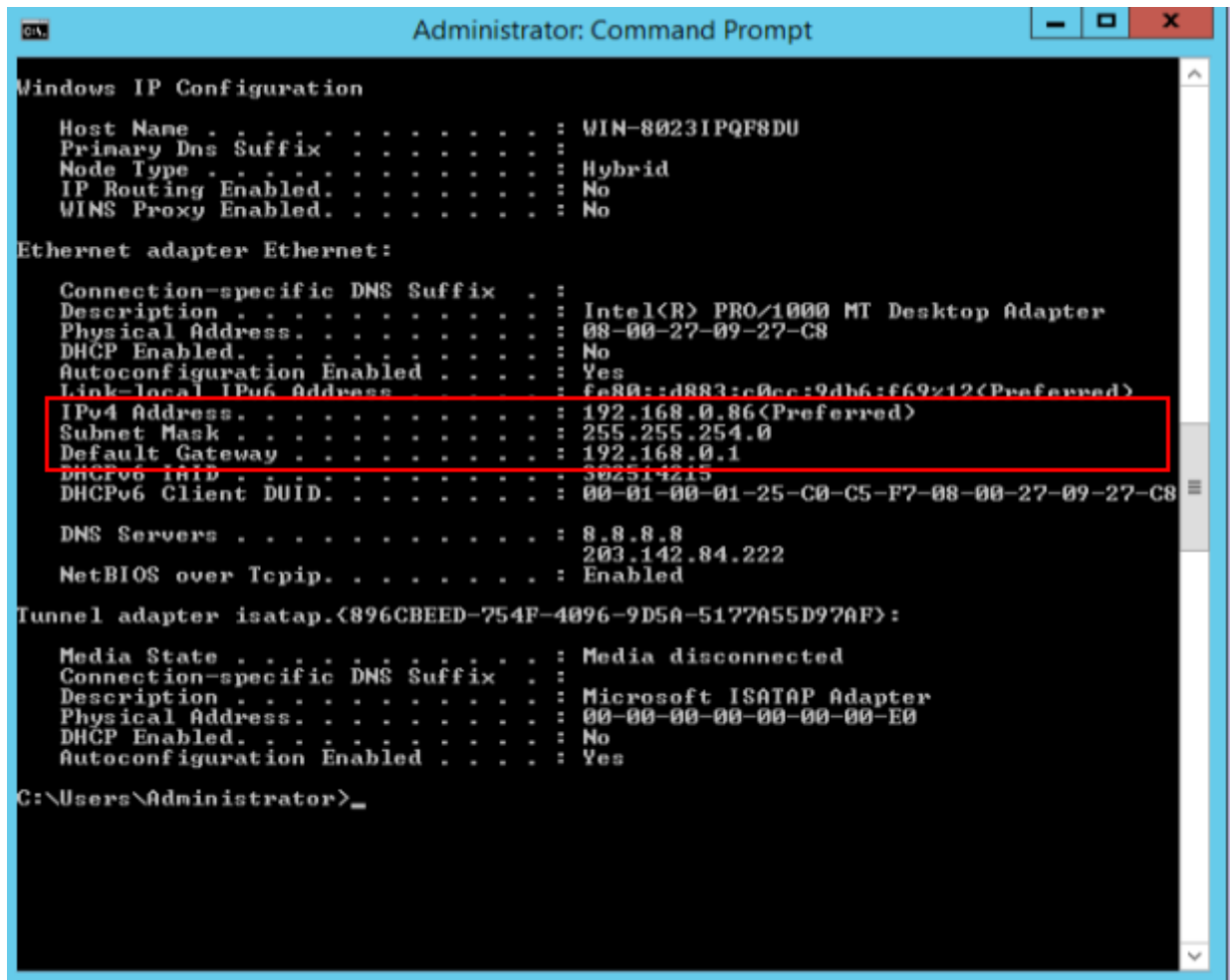
2.6. Testing

The final stage that can be done is to carry out tests on the server computer side.

example (ip 192.168.0.86/23). First, we enter the IP of the server that is already running. Second, we **ping** an internet site, for example **www.google.com**, and third, we do a **tracert** to the global site to ensure that the path we take is correct.

From the checking results, the following were obtained:

a. 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 IPID . . . . . : 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

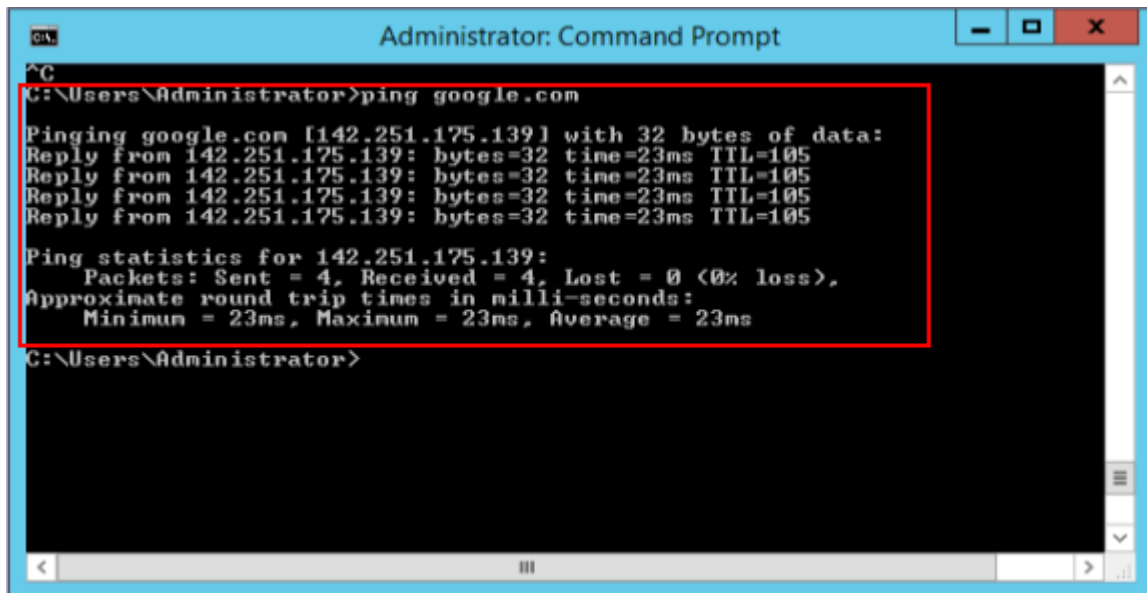
Tunnel adapter isatap.{896CBEED-754F-4096-9D5A-5177A55D97AF}:

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

The computer successfully **pinged** the global site **www.google.com**



```
Administrator: Command Prompt
C:\Users\Administrator>ping google.com

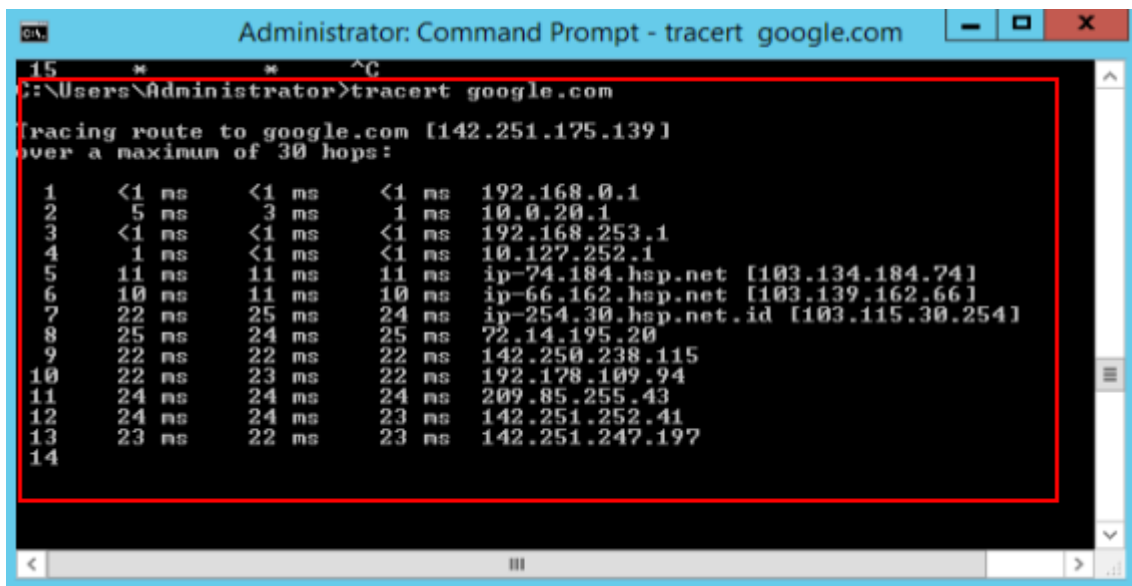
Pinging google.com [142.251.175.139] with 32 bytes of data:
Reply from 142.251.175.139: bytes=32 time=23ms TTL=105
Reply from 142.251.175.139: bytes=32 time=23ms TTL=105
Reply from 142.251.175.139: bytes=32 time=23ms TTL=105
Reply from 142.251.175.139: bytes=32 time=23ms TTL=105

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

The computer can do a **tracert** to the global site **www.google.com** with the path that is taken, namely the ISP Kominfo gateway 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:
  0  <1 ms    <1 ms    <1 ms    192.168.0.1
  1  5 ms      3 ms      1 ms      10.0.20.1
  2  <1 ms     <1 ms     <1 ms      192.168.253.1
  3  1 ms      <1 ms     <1 ms      10.127.252.1
  4  11 ms     11 ms     11 ms      ip-74.184.hsp.net [103.134.184.74]
  5  10 ms     11 ms     10 ms      ip-66.162.hsp.net [103.139.162.66]
  6  22 ms     25 ms     24 ms      ip-254.30.hsp.net.id [103.115.30.254]
  7  25 ms     24 ms     25 ms      72.14.195.20
  8  22 ms     22 ms     22 ms      142.250.238.115
  9  22 ms     23 ms     22 ms      192.178.109.94
 10  24 ms     24 ms     24 ms      209.85.255.43
 11  24 ms     24 ms     23 ms      142.251.252.41
 12  23 ms     22 ms     23 ms      142.251.247.197
 13
 14
```

*3. Precaution

- 1) Before setting up distribution on the firewall, you can ensure that the internet from your ISP is functioning normally.
- 2) You can change the IP that we use and adapt it to your environmental conditions.
- 3) Make sure to follow these steps carefully and check the DNS you are using.