

DNAT Configuration on Sangfor NGAF V8.0.47 for PRTG Admin

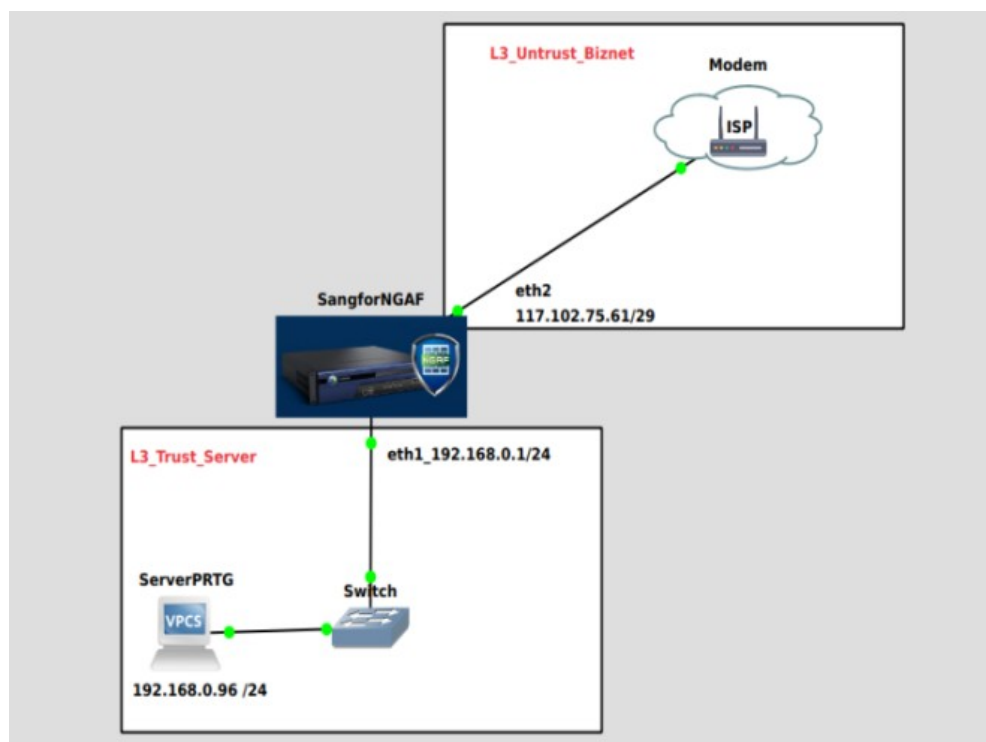
Server

***Product: NGAF**

***Version:8.0.47**

***1. Introduction**

1.1 Scenario



In this case study, we tried to write a DNAT configuration on a PRTG Admin network monitoring server. Where the configuration is carried out inside the Sangfor NGAF. Utilizing DNAT is certainly very helpful for admins to manage PRTG servers. The test was carried out using a laptop to open access to PTG servers from outside which are connected to the internet. By typing Public IP into the browser. The result is that the PRTG admin server can real-time send notifications to the client browser on the laptop. As for monitoring incoming and outgoing DNAT traffic, it can be seen from the number of counts in Sangfor NGAF. For the steps to make it, we use the following method.

1.2 Requirements

1. Users have an NGAF Firewall pre-set
2. Have a public IP
3. The user has a PRTG installed server

2. Configuration Guide

We have a local network segment with IP 192.168.0.1/24 as the gateway. As for the server we give the IP 192.168.0.96/24.

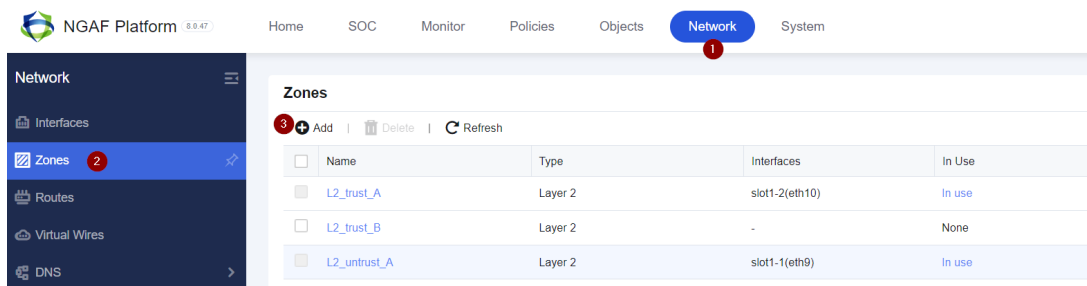
2.1. Creating Zone

A. Zone Trust Server

The Trust Server Zone is a zone created as a marker that the location of all data centers, including in this case the PRTG Admin server is here.

The steps were as follows:

- 1) Click **Network→Zones→Add**

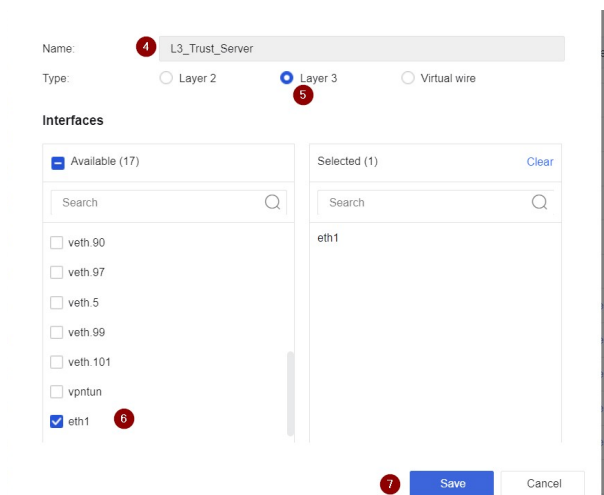


- 2) Complete the configuration below.

Enter name: L3_Trust_Server

Type: Layer3

Interfaces:



- 3) Click **Save**.

If successful, it will appear as shown below:

Home	SOC	Monitor	Policies	Objects	Network	System
Zones						
+ Add Delete Refresh						
<input type="checkbox"/>	Name	Type	Interfaces			
<input type="checkbox"/>	L3_untrust_A	Layer 3	-			
<input type="checkbox"/>	L3_untrust_B	Layer 3	-			
<input type="checkbox"/>	L3_untrust_C	Layer 3	-			
<input type="checkbox"/>	Virtual_trust_A	Virtual wire	eth6			
<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			
<input type="checkbox"/>	L3_Untrust_Mikrotik	Layer 3	slot1-3(eth11)			

B. Biznet Untrust Zone

You have successfully created a Trust Server zone, then create one more zone we call Biznet Untrust zone. The steps are the same as above,

1) Click **Network → Zones → Add**

NGAF Platform 8.0.47	Home	SOC	Monitor	Policies	Objects	Network	System
Zones							
+ Add Delete Refresh							
<input type="checkbox"/>	Name	Type	Interfaces	In Use			
<input type="checkbox"/>	L2_trust_A	Layer 2	slot1-2(eth10)	In use			
<input type="checkbox"/>	L2_trust_B	Layer 2	-	None			
<input type="checkbox"/>	L2_untrust_A	Layer 2	slot1-1(eth9)	In use			
<input type="checkbox"/>	L2_untrust_B	Layer 2	-	None			
<input type="checkbox"/>	L3_manage	Layer 3	-	None			

2) Name input: L3_Untrust_Biznet

Type: Layer3

Interfaces:

Name: **L3_Untrust_Biznet**

Type: ☐ Layer 2 ☒ Layer 3 ☐ Virtual wire

Interfaces

Available (17)

Search

☐ veth.90
☐ veth.97
☐ veth.5
☐ veth.99
☐ veth.101
☐ vptun
☒ eth2

Selected (1)

Clear

Search

eth2

Save **Cancel**

3) Click **Save**. If it works then like the picture below.

Home
SOC
Monitor
Policies
Objects
Network
System

Zones

Add
Delete
Refresh

	Name	Type	Interfaces
<input type="checkbox"/>	L3_untrust_A	Layer 3	-
<input type="checkbox"/>	L3_untrust_B	Layer 3	-
<input type="checkbox"/>	L3_untrust_C	Layer 3	-
<input type="checkbox"/>	Virtual_trust_A	Virtual wire	eth6
<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
<input type="checkbox"/>	L3_Untrust_Mikrotik	Layer 3	slot1-3(eth11)
<input type="checkbox"/>	L3_Untrust_Biznet	Layer 3	eth2

2.2. Interface settings

The next step after creating a zone is to configure the interface where we will enter the zones that have been created above. Eth1 **interface** for L3_Trust_Server Zone, and **eth2** for L3_Untrust_Biznet Zone.

A. Configure eth1 (L3_trust_server)

1) Go to the **Network→Interface menu→ Select Eth1**

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

Network

- Interfaces**
- Zones
- Routes
- Virtual Wires
- DNS
- DHCP

Physical Interfaces Subinterfaces VLAN Interfaces Aggregate Int

✓ Enable ⏏ Disable | ↻ Refresh

<input type="checkbox"/>	Name	Interface Status	WAN Attribute	Type	Zone
<input type="checkbox"/>	eth0		No	Layer 3	L3_trust_A
<input type="checkbox"/>	eth1		No	Layer 3	L3_Trust_Server
<input type="checkbox"/>	eth2		Yes	Layer 3	L3_Untrust_Biznet

2) Select Relationship

Description: server-data-center

Type: player 3

Zone: L3_Trust_Server

Static IP: 192.168.0.1/24

Then save it, like the picture below.

Edit Physical Interface

Basics

Name: eth1

Status: ☒ Enabled ☐ Disabled

Description: Server-DataCenter

Type: Layer 3

Zone: L3_Trust_Server

Basic Attributes: ☐ WAN attribute

System Upgrade: ☐ Temporarily use this interface for system upgrade

IPv4 IPv6 Link State Detection Advanced

IP Assignment: ☒ Static ☐ DHCP ☐ PPPoE

Static IP: 192.168.0.1/23

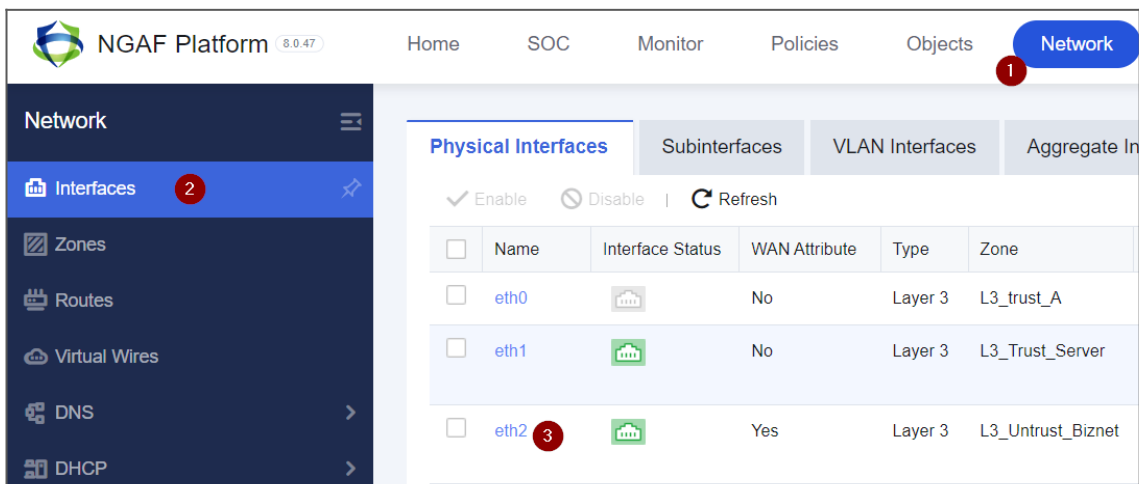
Next-Hop IP:

Link Bandwidth: Outbound 10240 Mbps Inbound 10240 Mbps

Save Cancel

B. Eth2 configuration (L3_untrust_biznet)

1) Go to the **Network→Interface menu→ Select Eth2**



2) Select **Relationship**

Description: WAN(Biznet1)

Type: layer 3

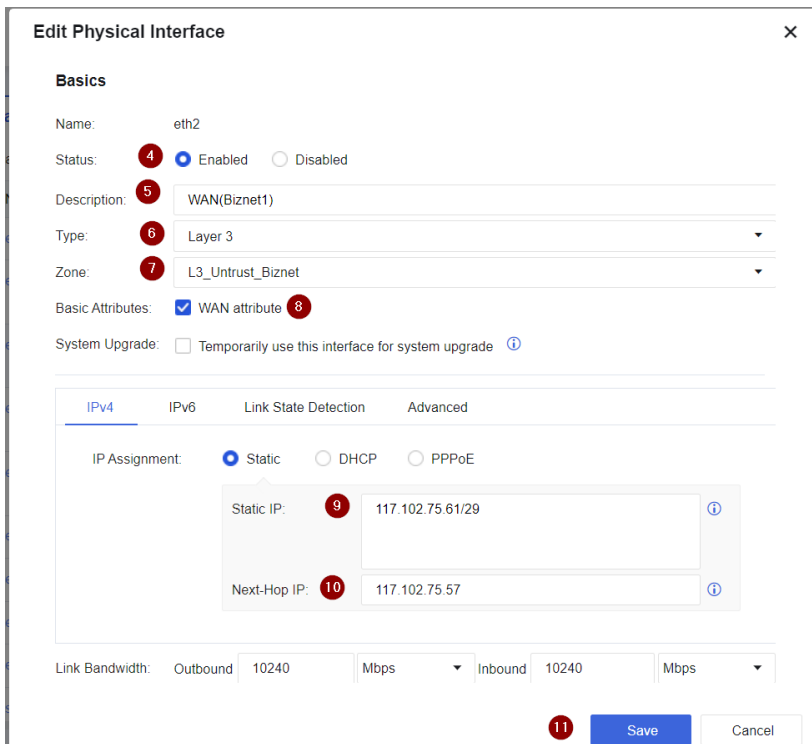
Zone: L3_Untrust_Biznet

Basic Attribute: WAN attribute (tick)

Static IP: 117.102.75.61/29

Next-Hop IP: 117.102.75.57 (this is the gateway of the ISP)

Then save it, like the picture below.

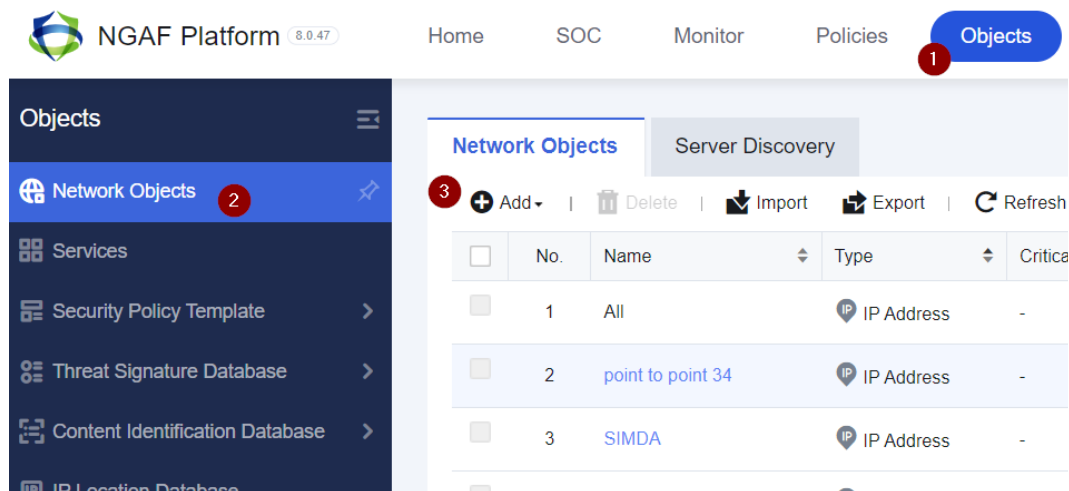


2.3. Create Network Objects

The next step is to make the network object on massing- IP WAN and IP server PRTG, respectively.

A. Creating an object for a WAN IP

1) Click the **Objects** → **Network Objects** → **Add** menu



2) Input type: IP Address

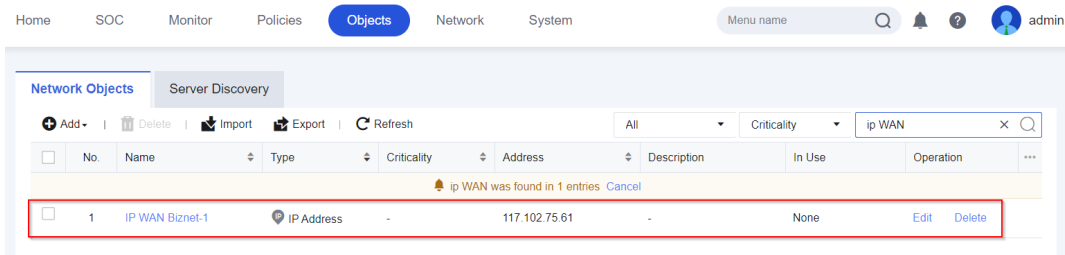
Name : IP WAN Biznet-1

IP: 117,102.75.61

As in the picture below:

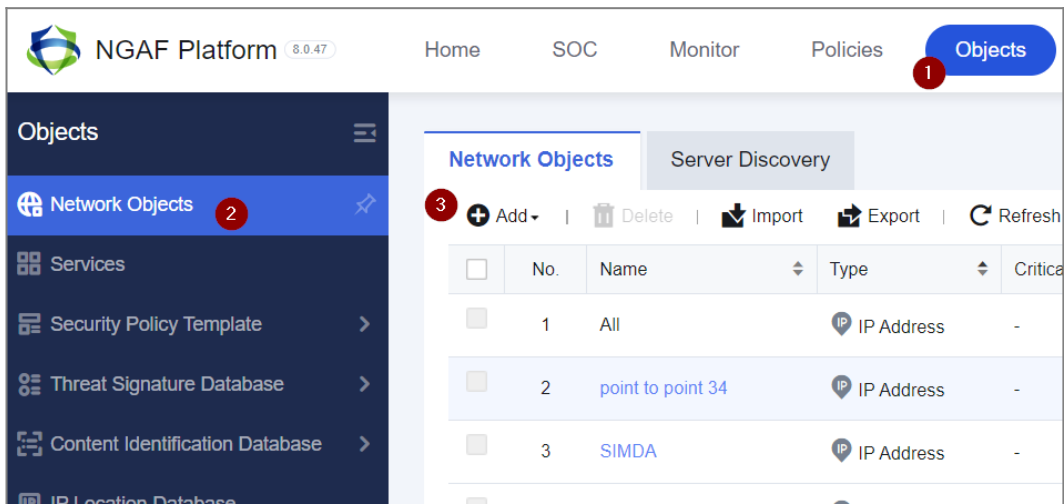
The 'Add Address' dialog box is shown. It has a 'Type' section with three radio buttons: 'IP Address' (selected, marked with a red circle 4), 'Business Asset Address', and 'User IP Address'. Below this is the 'Basics' section with fields for 'Name' (IP WAN Biznet-1, marked with a red circle 5), 'Description' (Optional), and 'Address Group' (Optional). The 'IP Address' section has a 'Protocol' section with two radio buttons: 'IPv4' (selected, marked with a red circle 6) and 'IPv6'. Below this is a large text area for 'IP Address' containing '117.102.75.61' (marked with a red circle 7). At the bottom of the dialog is a 'DNS Lookup' button. At the very bottom of the screen are three buttons: 'Save and Add', 'Save' (marked with a red circle 8), and 'Cancel'.

If it works, as shown below.



B. Creating PRTG SERVER IP Objects

1) Click the **Objects** → **Network Objects** → **Add** menu



2) Input type: IP Address

Name : IP Server PRTG

Protocol: IPv4

IP: 192.168.0.96

As in the picture below:

Add Address

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

Basics

Name: IP Server PRTG

Description: Optional

Address Group: Optional

IP Address

Protocol:
☒ IPv4
☐ IPv6

IP Address: 192.168.0.96

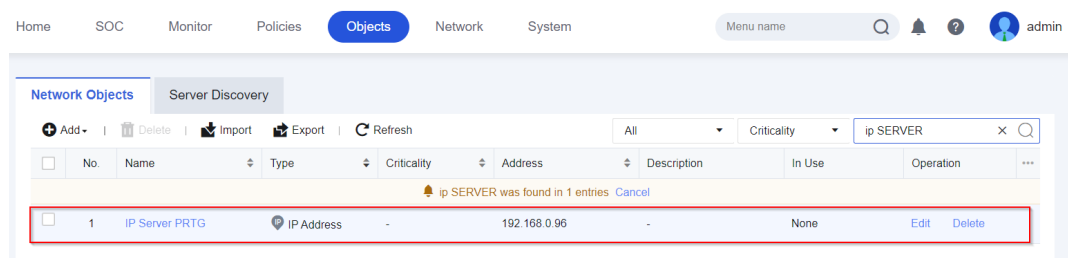
DNS Lookup

Save and Add

Save

Cancel

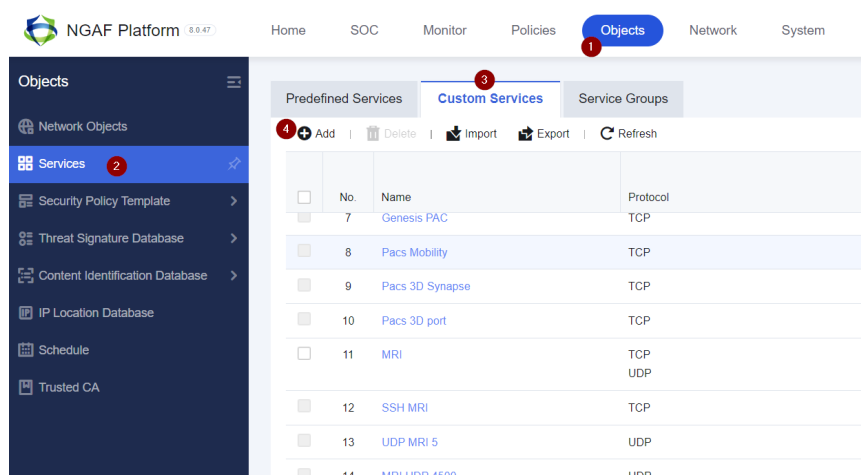
As in the picture below:



2.4. Create Services for PRTG servers

The next step that must be done is to make active services in accordance with each. This can vary depending on needs. Here for PTG TCP server DST port: 8443 while UDP DST port: 161. Details can be made in Sangfor with the following steps:

1) Click **Objects** → **Services** → **Custom Services** → **Add**



2) The custom services dialog appears. Then fill in the following fields:

name: PRTG services

protocols: add TCP src port:0-65535 DST port: 8443

Add Custom Service

Name: 1

PRTG services

Description:

Optional

Protocols

2

+ Add

|

🗑 Delete

		TCP/UDP		ICMP/ICMPv6		
<input type="checkbox"/>	Protocol	Src Port	Dst Port	Type	Code	Operation
<input type="checkbox"/>	T					

Add Protocol

3

Protocol: UDP

17

Protocol No.:

0-65535

Src Port:

161

Dst Port: 4

Save

Cancel

Save and Add

Save

Cancel

Add Custom Service

Name: 1

PRTG services

Description:

Optional

Protocols

2

+ Add

|

🗑 Delete

		TCP/UDP		ICMP/ICMPv6		
<input type="checkbox"/>	Protocol	Src Port	Dst Port	Type	Code	Operation
<input type="checkbox"/>	T					

Add Protocol

3

Protocol: TCP

6

Protocol No.:

0-65535

Src Port:

8443

Dst Port: 4

Save

Cancel

Save and Add

Save

Cancel

If successful, it will appear as the following figure:

HomeSOCMonitorPoliciesObjectsNetworkSystem

Predefined ServicesCustom ServicesService Groups

+ Add

Delete

Import

Export

Refresh

<input type="checkbox"/>	No.	Name	Protocol	TCP/UDP		ICMP/ICMPv6		Description
				Src Port	Dst Port	Type	Code	
<div> prt看 serv was found in 1 entries Cancel</div>								
<input type="checkbox"/>	1	PRTG Services	TCP	0-65535	8443	-	-	-
			UDP	0-65535	161	-	-	-

2.5. Configuring NAT

After all the above steps have been done, the next step is to do DNAT. The firewall can be explained as follows:

1) Open →NAT→Add Policies menu

NGAF Platform 5.9.47	Home	SOC	Monitor	Policies	Objects	Network	System
----------------------	------	-----	---------	-----------------	---------	---------	--------

Policies		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
<input type="checkbox"/>	1	NAT akses Internet...	SNAT	L3_Untrust_Milk...	Private Network ...	eth4	All

2) Input the followig information.

Type:destination NAT

Name:PRTG DNAT

Status:enabled

Src Zone: L3_Untrust_Biznet

Alamat:

Destination:Network Objects → Select BIZNET-1 WAN IP

Services:PRTG Services

Translate DST IP to: Network Objects

Network Objects:IP Server PRTG

Translate Port To: 8443

In detail as shown below,

Add NAT Policy

Type: ☐ Source NAT **1** ☒ Destination NAT ☐ Bidirectional NAT

Basics

Name: **2** PRTG DNAT

Status: **3** ☒ Enabled ☐ Disabled

Description: Optional

Move To: Top

Schedule: All week

Original Data Packet

Src Zone: **4** L3_Untrust_Biznet

Src Address: **5** All

Destination: ☐ IP Address **6** ☒ Network Objects

7 IP WAN Biznet-1

Services: **8** PRTG Services

Translated Data Packet

Translate Src IP To: Untranslated

Translate Dst IP To: Network Object **9**

Network Object: IP Server PRTG **10**

Translate Port To: 8443 **11**

1 To make NAT policy work, please configure local ACL or application control policy.

Allow: ☒ Add ACL policy automatically ☐ Add ACL policy manually

Save and Copy Save Cancel

Then save it, and if successful it will appear like the following image:

Home SOC Monitor **Policies** Objects Network System

Menu name

IPv4 NAT DNS Mapping

+ Add | Delete | Enable | Disable | Move To | More | Refresh

All PRTG DNAT

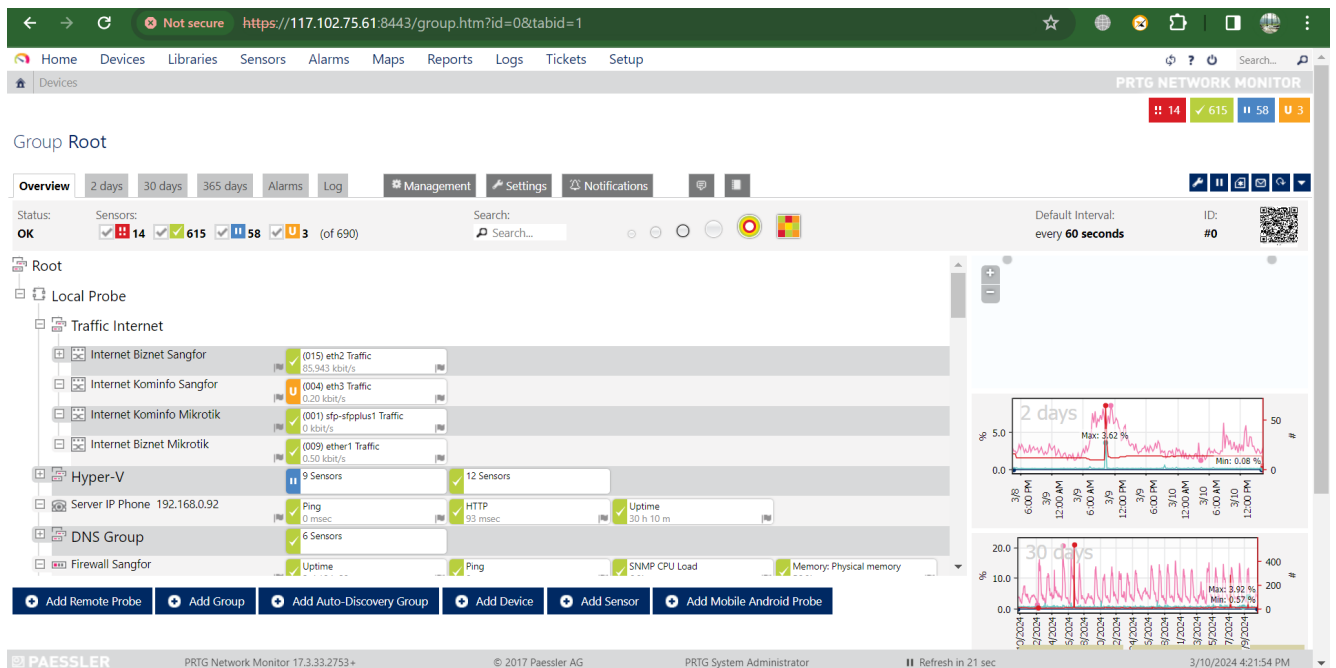
Original Data Packet								Translated Data Packet			Schedule	Hit Count	Status	Operatic
No.	Name	Type	Src Zone	S...	D...	Dst Address	Services	Src Address	Dst Address	Dst Port				
1	PRTG DNAT	DNAT	L3_Untrust_Biznet	All	-	IP WAN Biznet-1	PRTG Services	-	IP Server PRTG	8443	All week	12	✓	Edit

PRTG DNAT was found in 1 entries Cancel

2.6. Conducting Trials

DNAT configuration has been completed, it's time to test PRTG Admin server access via the internet.

From the results of testing via the internet, the following are obtained:



3. Precaution

- 1) It is necessary to pay attention to security aspects on local servers and in terms of network infrastructure access, because it is accessed by the public from the internet.
- 2) Configure destination port.

