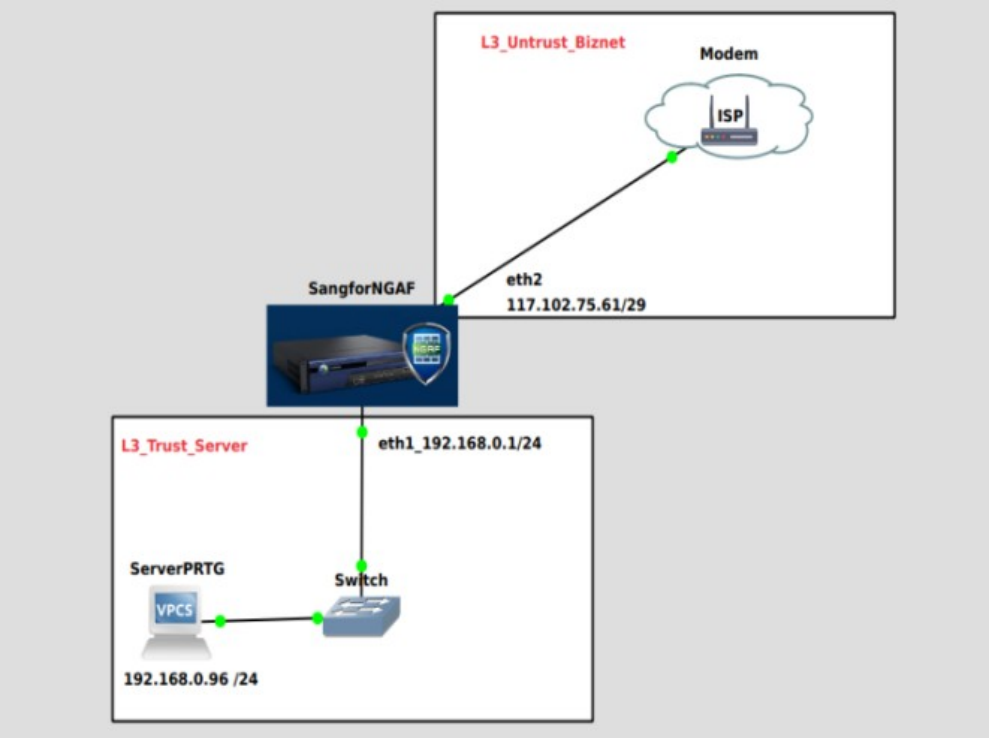
DNAT Configuration on Sangfor NGAF V8.0.47 for PRTG Admin Server

***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.

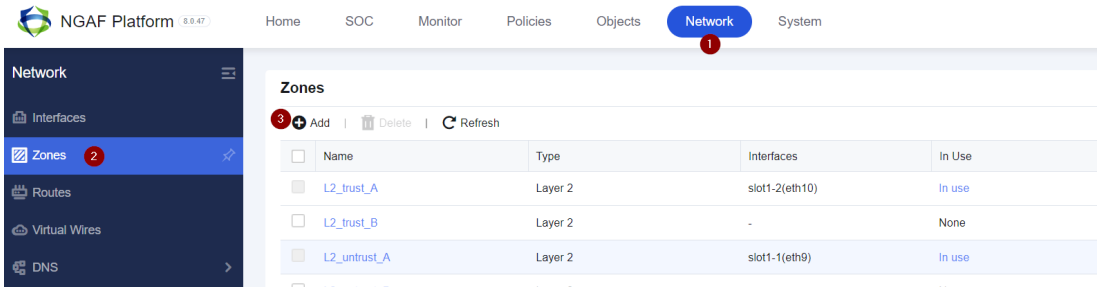
2.1. Creating Zone

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**

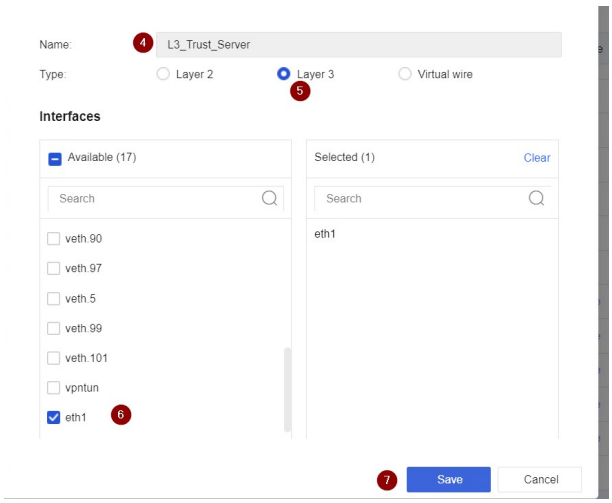


2) Complete the configuration below.

Enter name: L3_Trust_Server

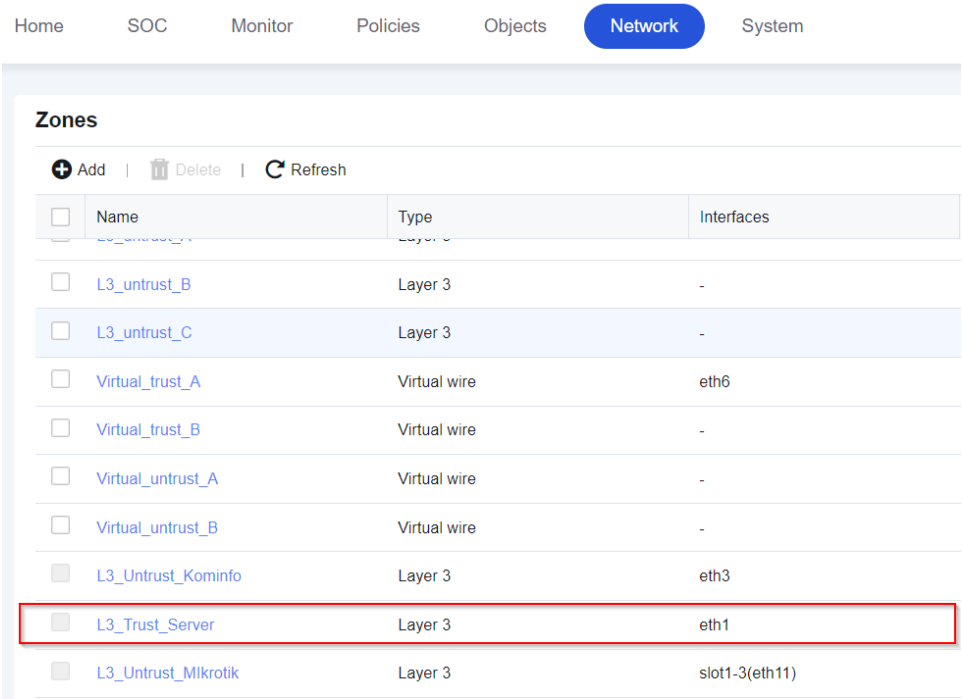
Type: Layer3

Interfaces:



3) Click **Save.**

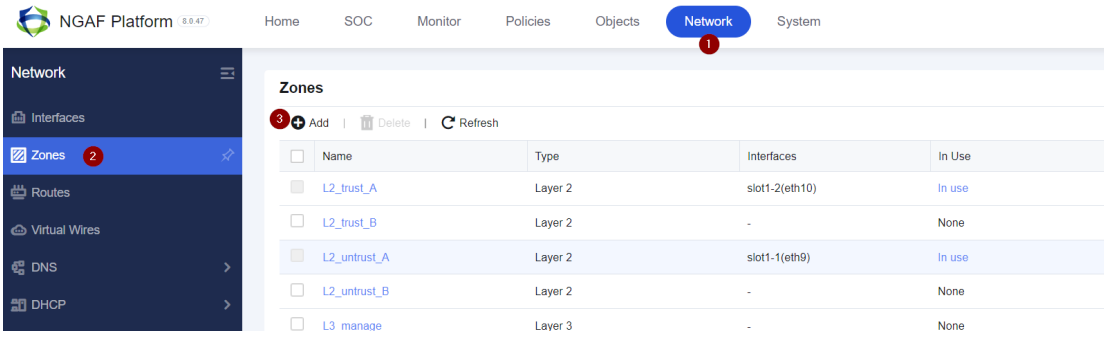
If successful, it will appear as shown below:



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,

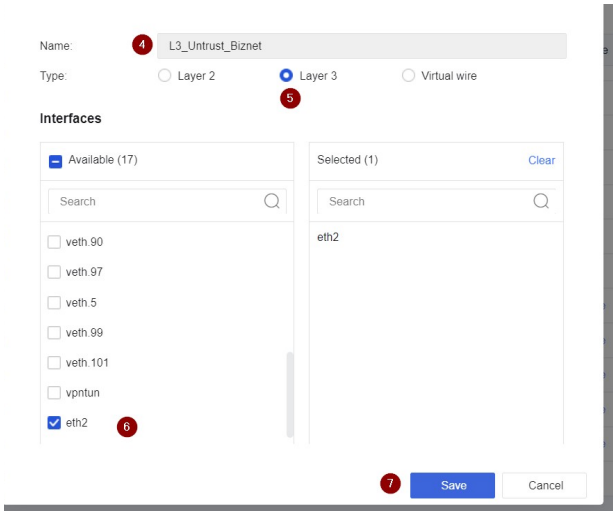
1) Click **Network →Zones→Add**



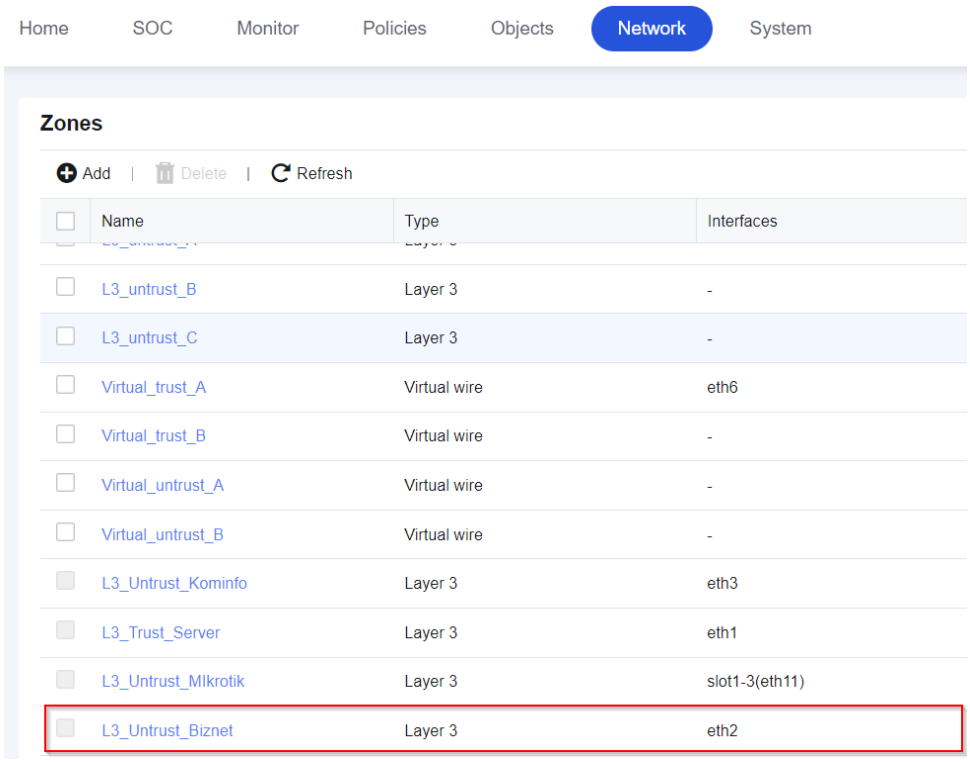
2) Name input: L3_Untrust_Biznet

Type: Layer3

Interfaces:



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

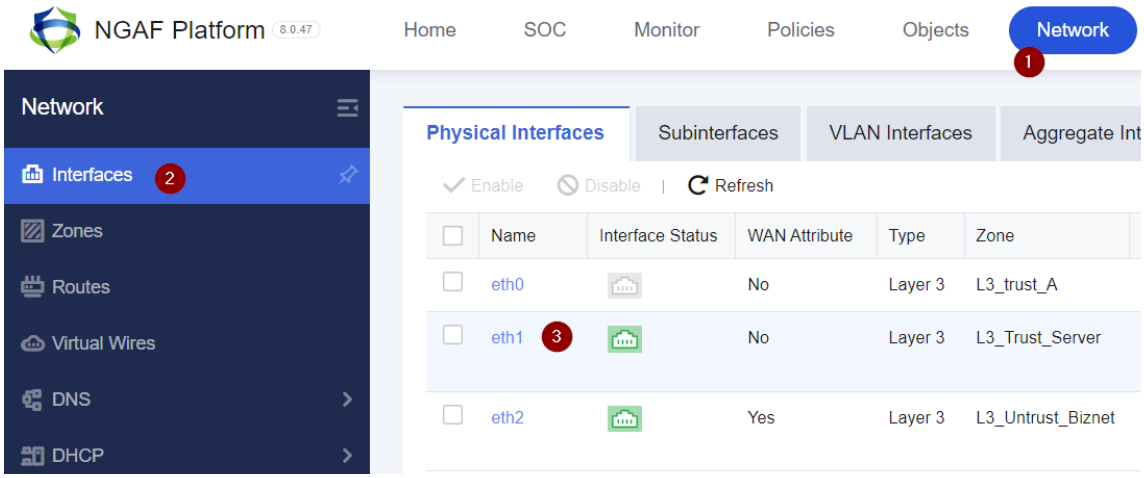


2.2. Interface settings

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**



2) Select **Relationship**

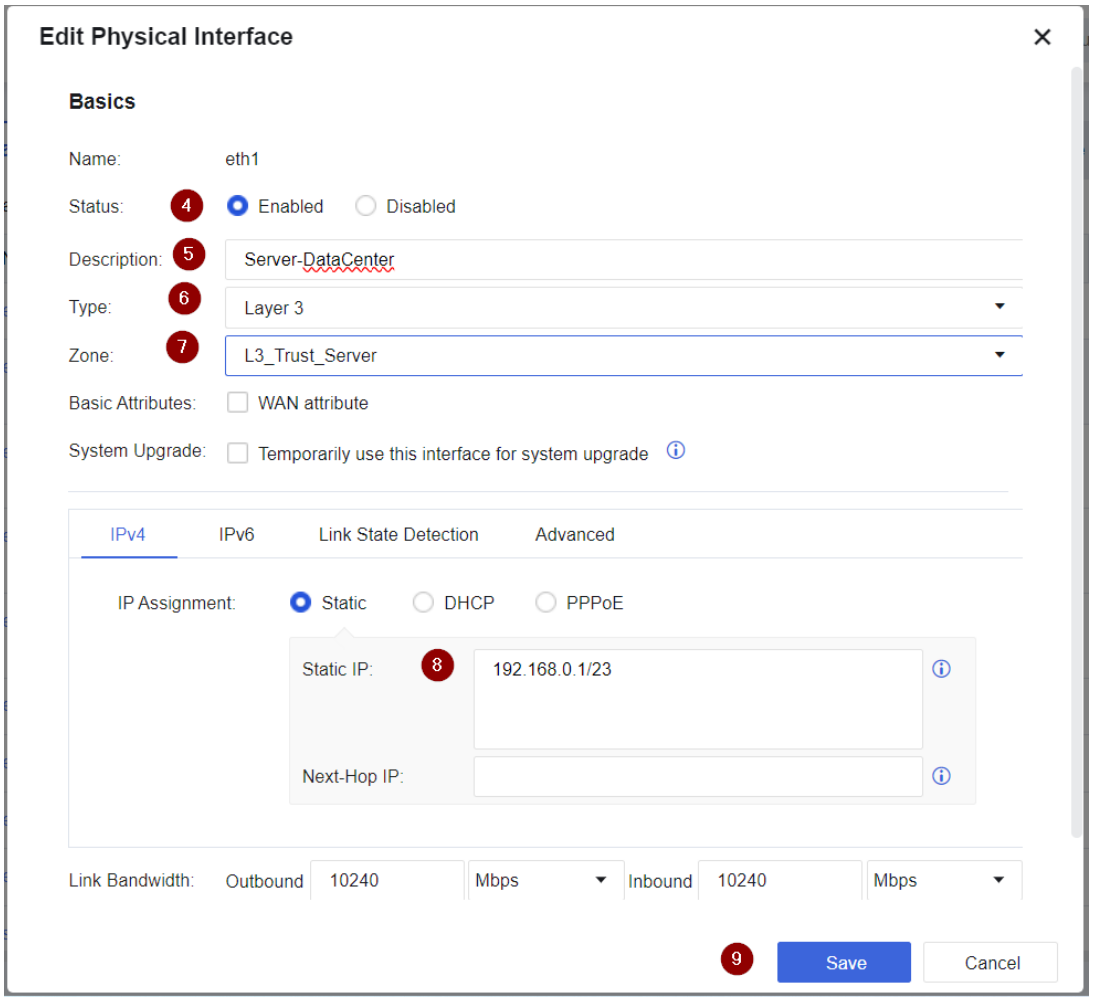
Description: server-data-center

Type: player 3

Zone: L3_Trust_Server

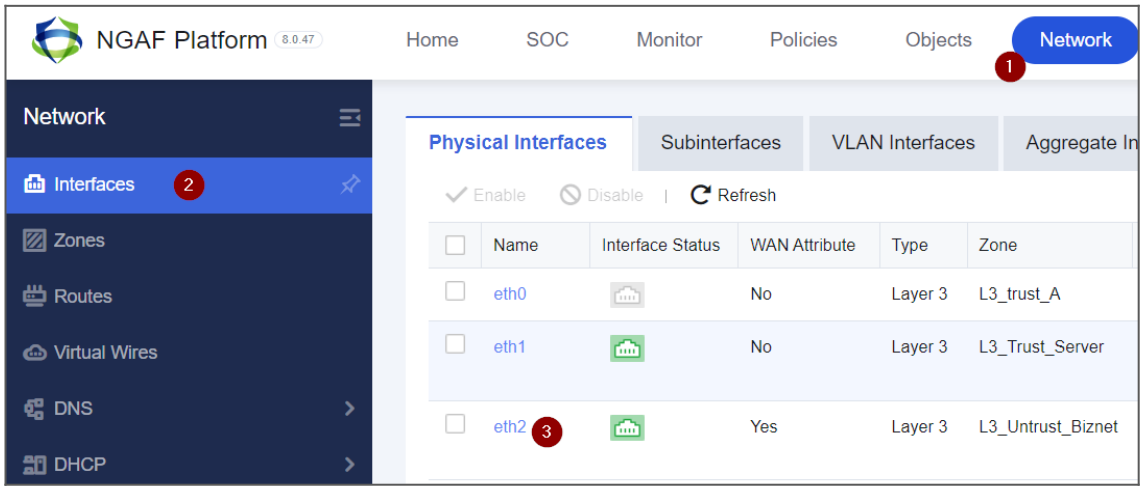
Static IP: 192.168.0.1/24

Then save it, like the picture below.



B. Eth2 configuration (L3_untrust_biznet)

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



2) Select **Relationship**

Description: WAN(Biznet1)

Type: layer 3

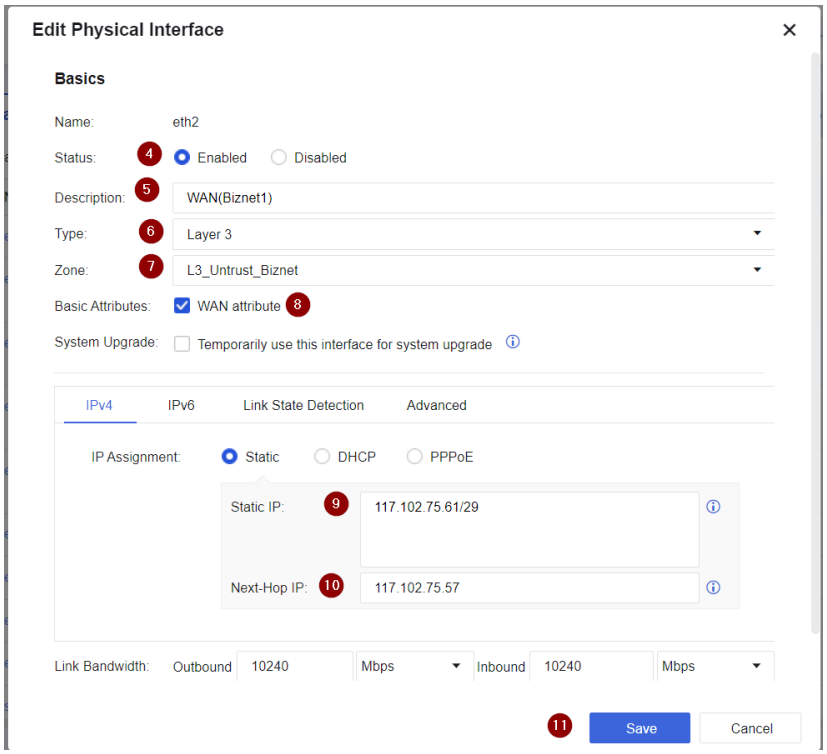
Zone: L3_Untrust_Biznet

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.

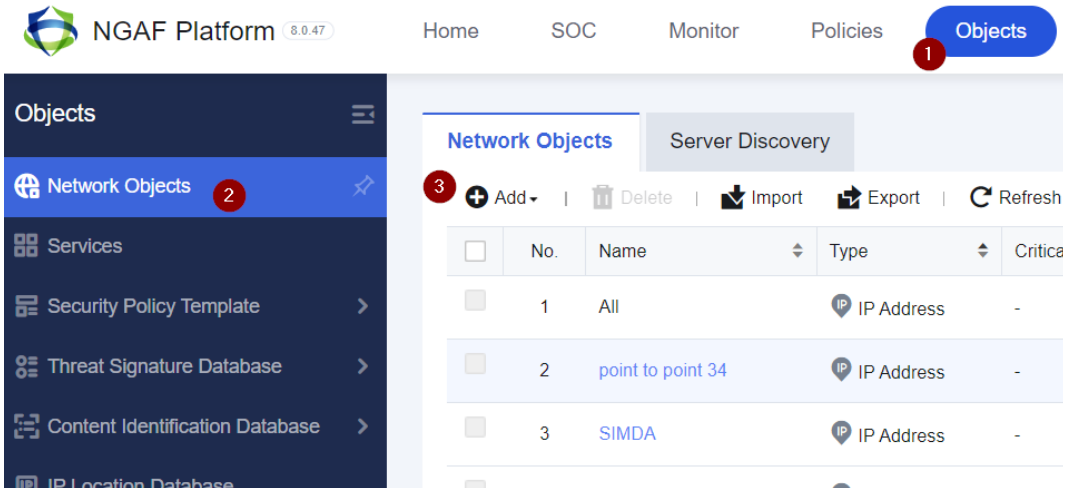


2.3. Create Network Objects

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**

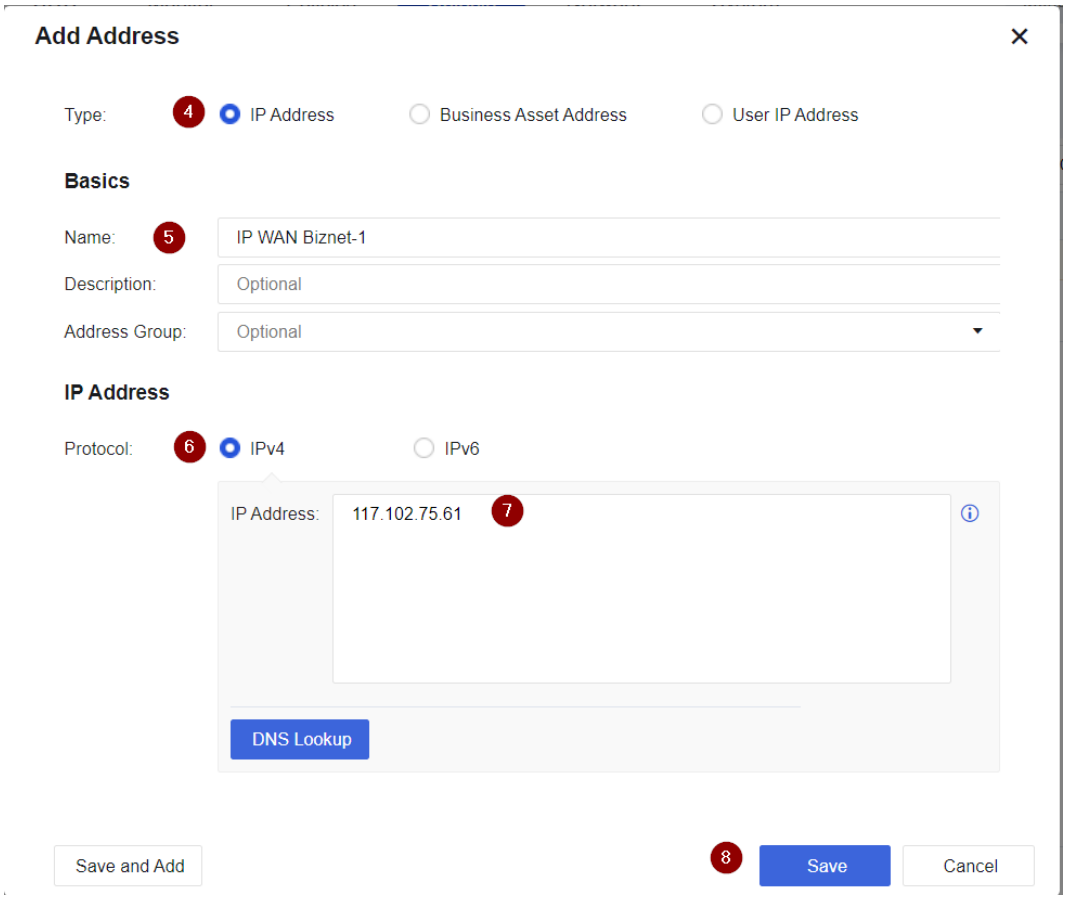


2) Input type: IP Address

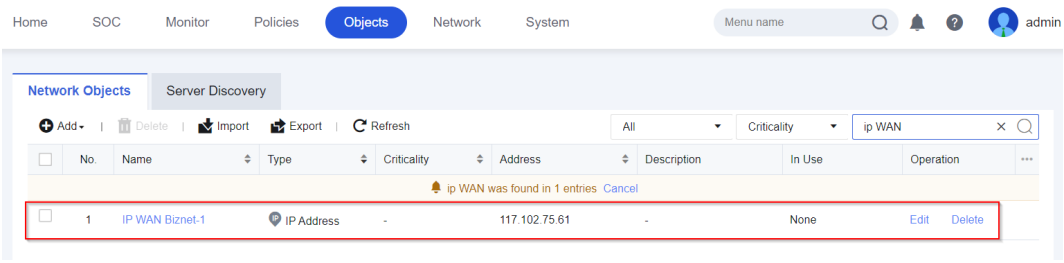
Name : IP WAN Biznet-1

IP: 117,102.75.61

As in the picture below:

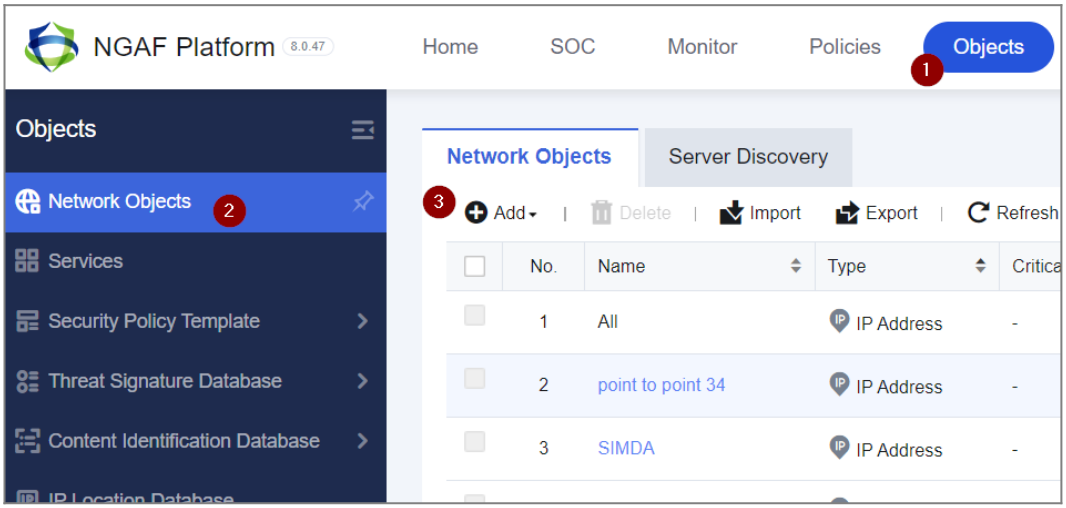


If it works, as shown below.



B. Creating PRTG SERVER IP Objects

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



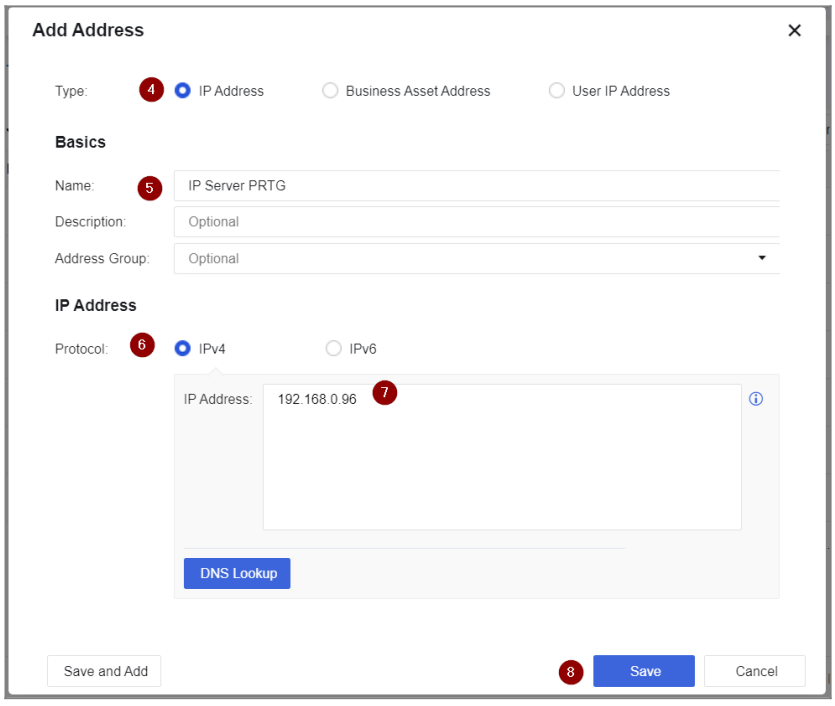
2) Input type: IP Address

Name : IP Server PRTG

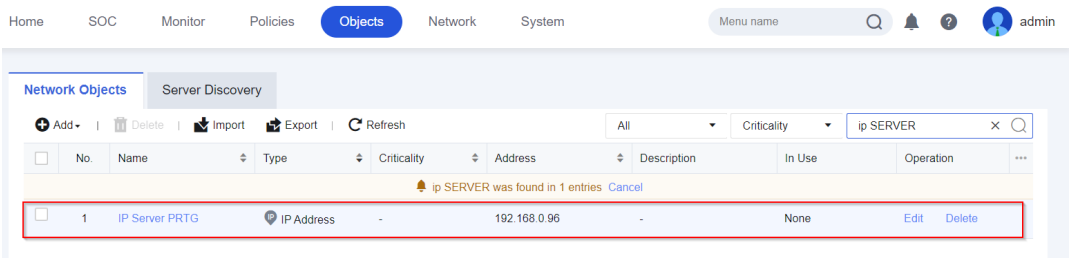
Protocol: IPv4

IP: 192.168.0.96

As in the picture below:



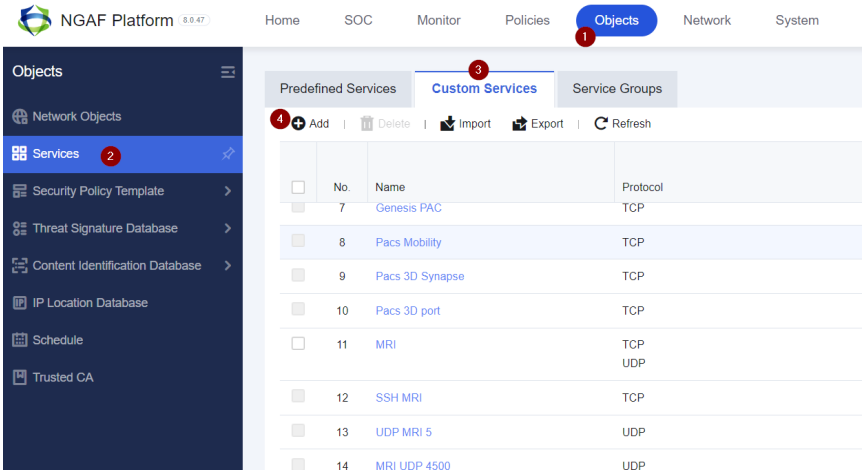
As in the picture below:



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:

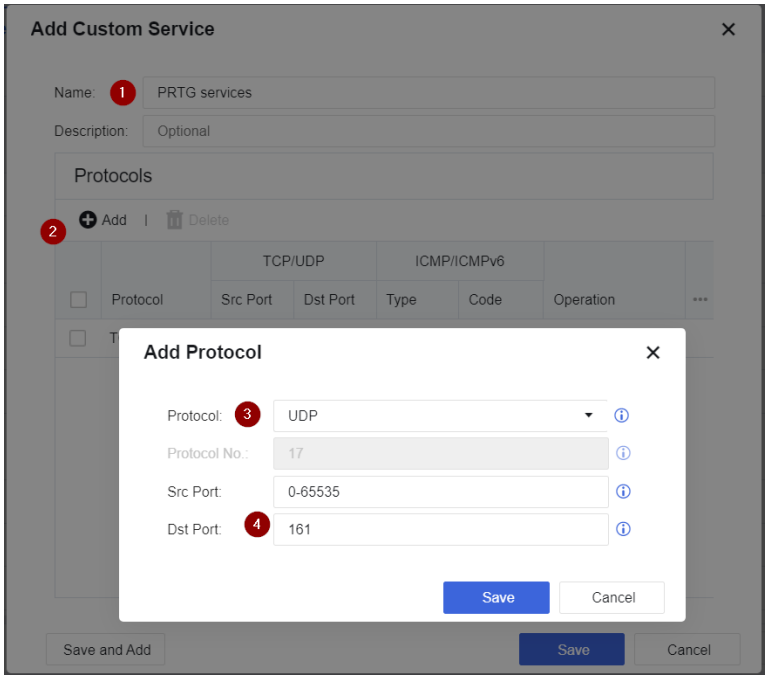
1) Click **Objects →Services→Custom Services→Add**

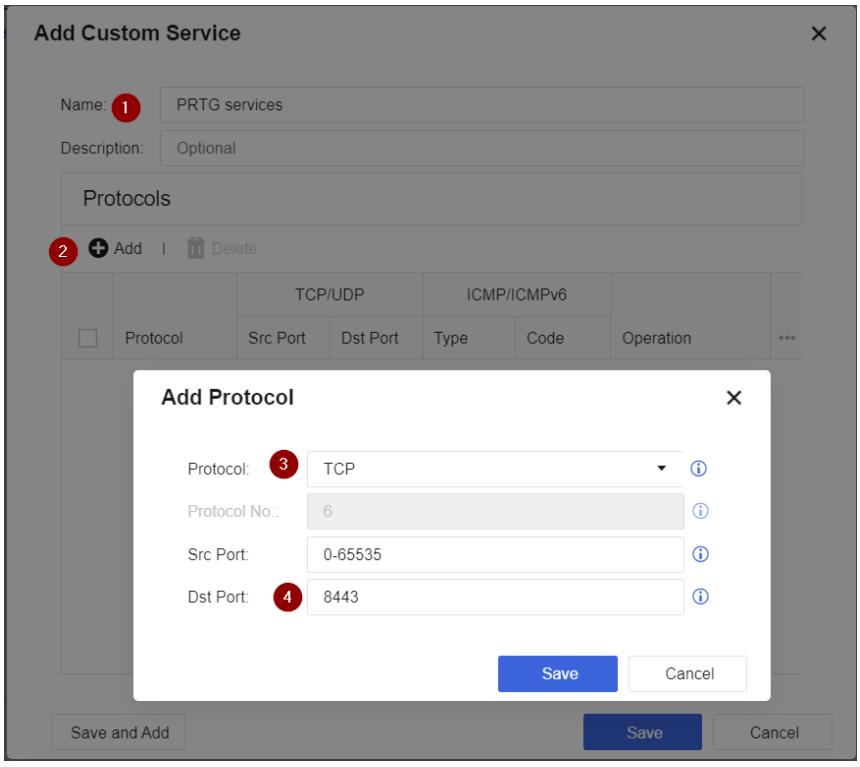


2) The custom services dialog appears. Then fill in the following fields:

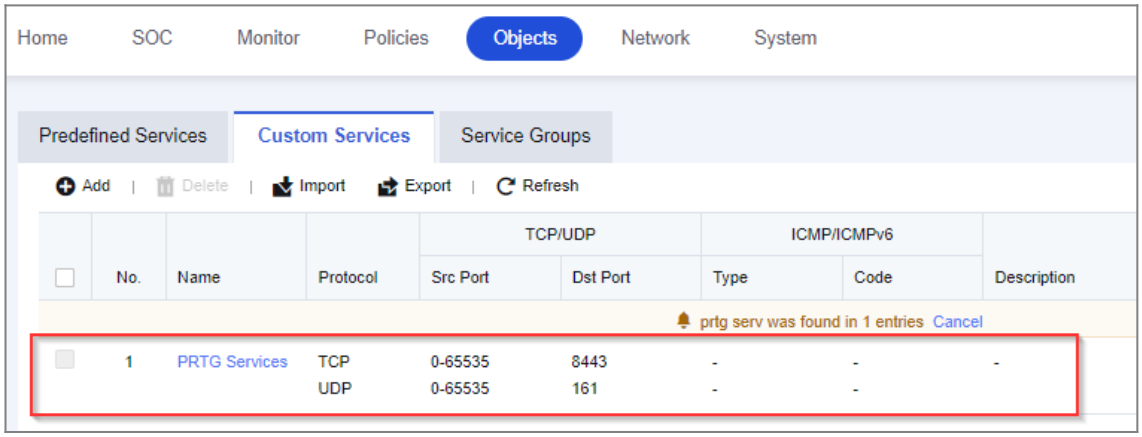
name: PRTG services

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





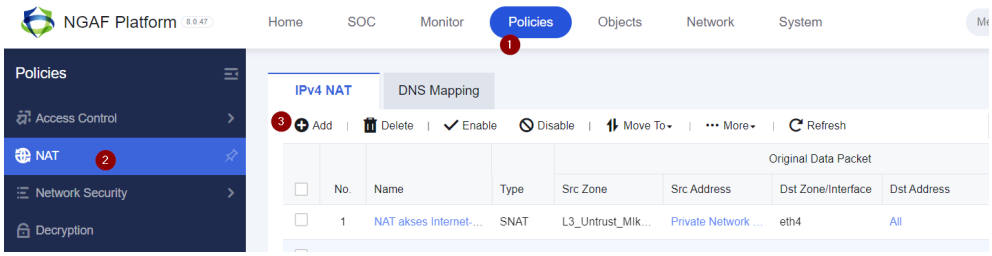
If successful, it will appear as the following figure:



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



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

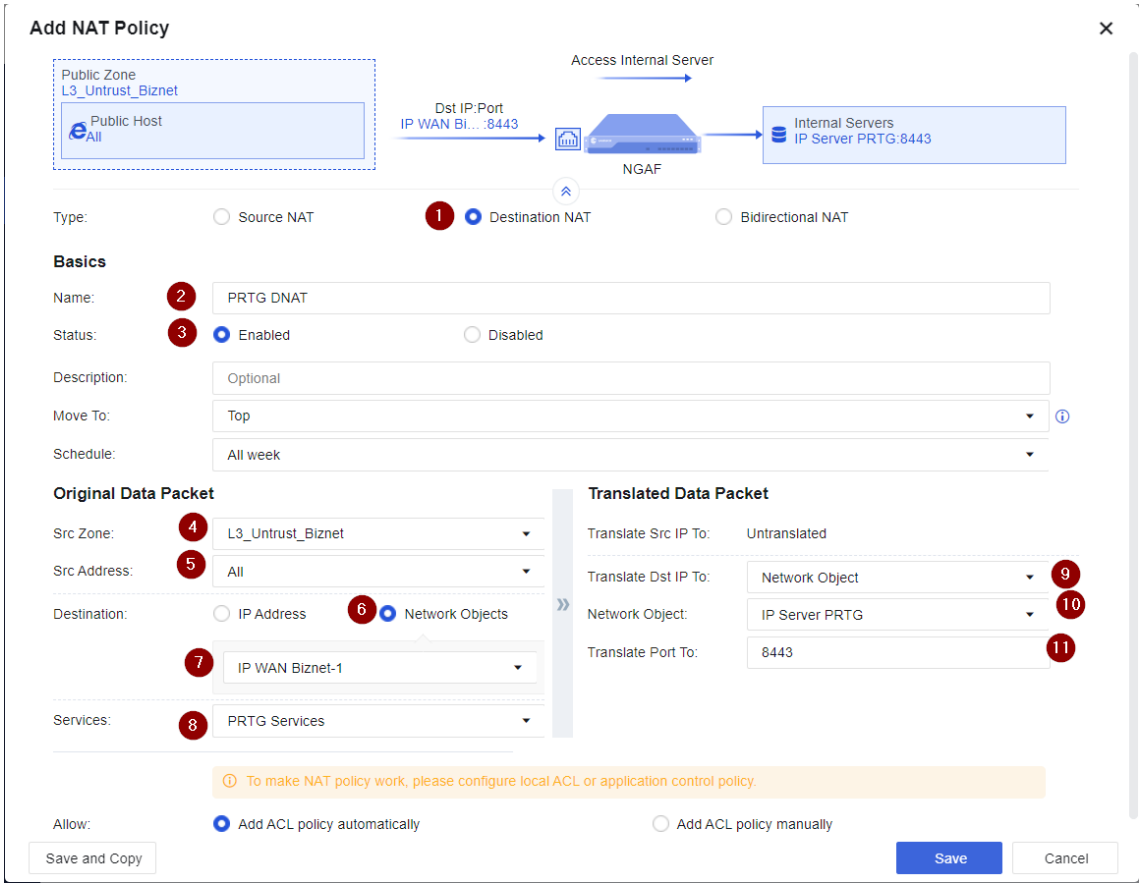
Services:PRTG Services

Translate DST IP to: Network Objects

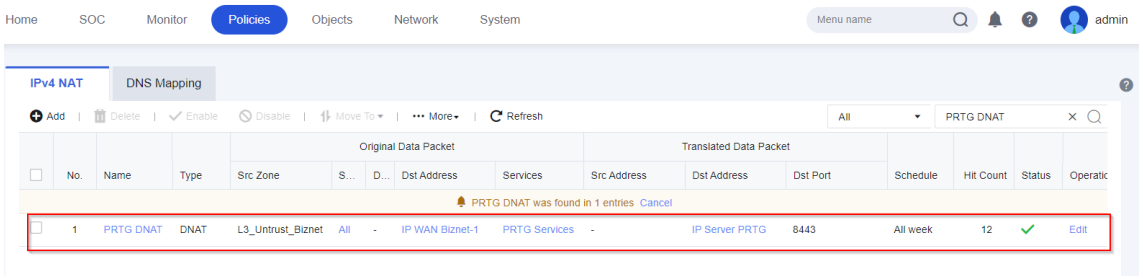
Network Objects:IP Server PRTG

Translate Port To: 8443

In detail as shown below,



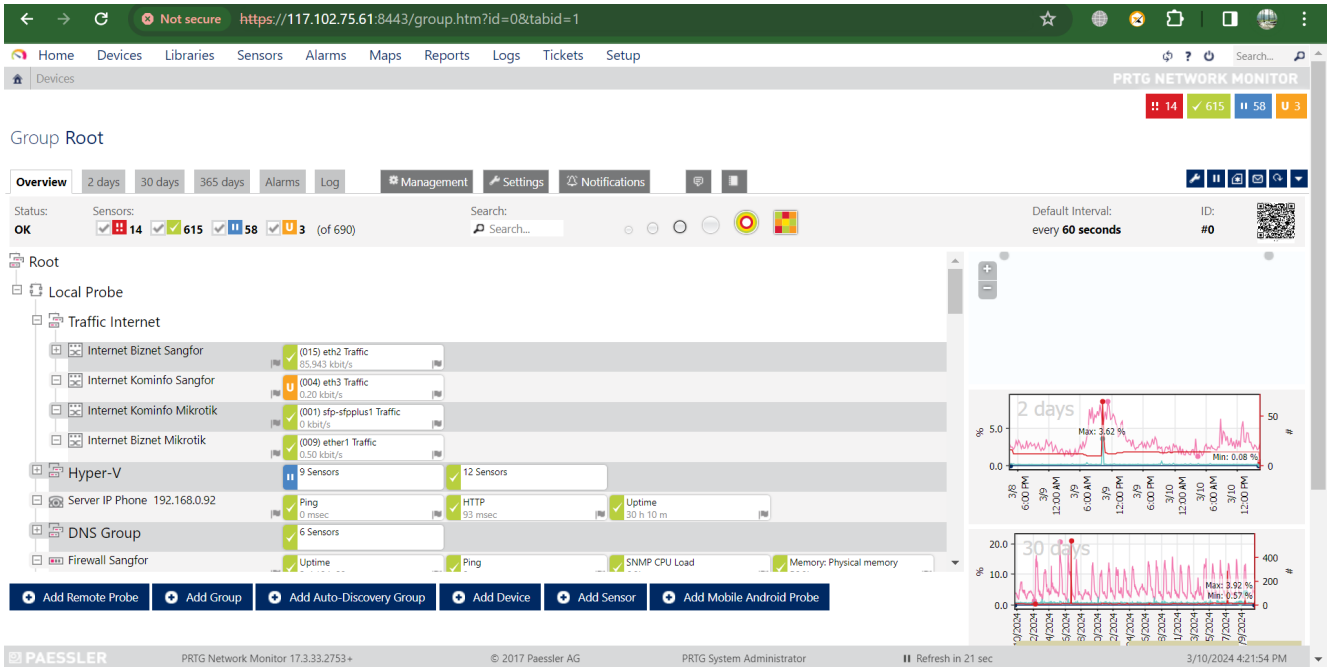
Then save it, and if successful it will appear like the following image:



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.