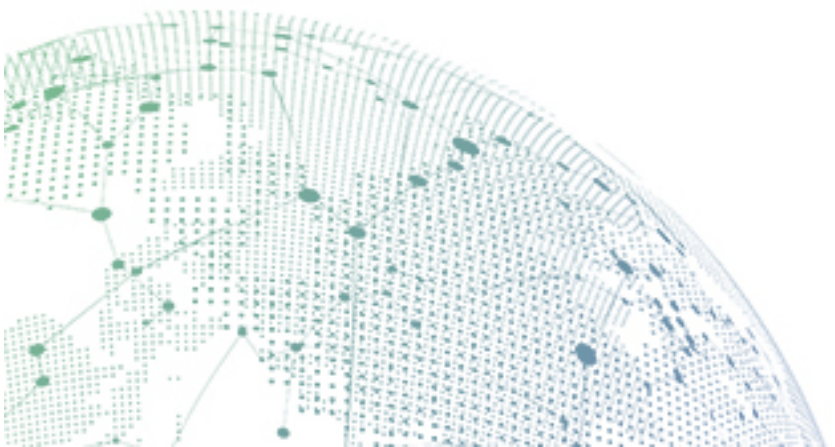
SANGFOR

# NGAF

## Case Study - NGAF deployment at the network-edge

Version 7.5.1



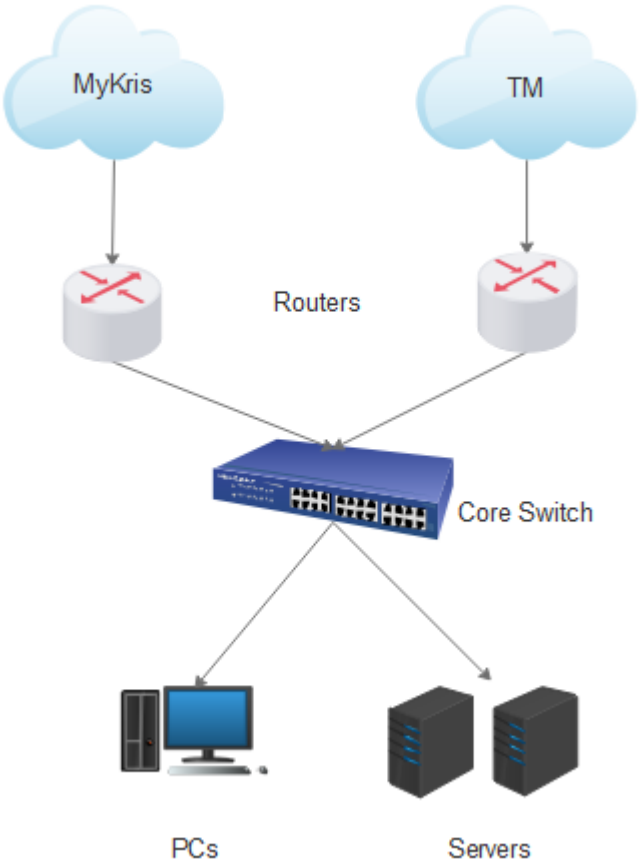
## Change Log

| Date | Change Description |
| --- | --- |
| May 20, 2018 | Version 7.5.1document release. |
| | |

# CONTENT

# Chapter 1 Introduction

Current environment got 2 ISP line with the dial-up different router (Topology as below). We need to deploy the NGAF in this network.




# Chapter 2 Requirement & Solution

- **Requirement:** Customer wishes to achieve 2 routers become one device to manage, PPPOE require;

  **Solution:** Replace routers with NGAF's dial-up feature. We need to use Sub-interface to configure dial-up instead of the usual physical interface because Malaysia SIP dial-up is trunk mode with VLAN.

- **Requirement:** Two ISP line would like to combine and share bandwidth;

  **Solution:** Configure Link load balancing policy

- **Requirement:** Protection of server zone to prevent outsider attack;

  **Solution:** Configure IPS, APT and WAF policy

- **Requirement:** Branches users want to access headquarters servers via internal segment;

  **Solution:** Using NGAF to Establish IPSecVPN Tunnel between branch and headquarters

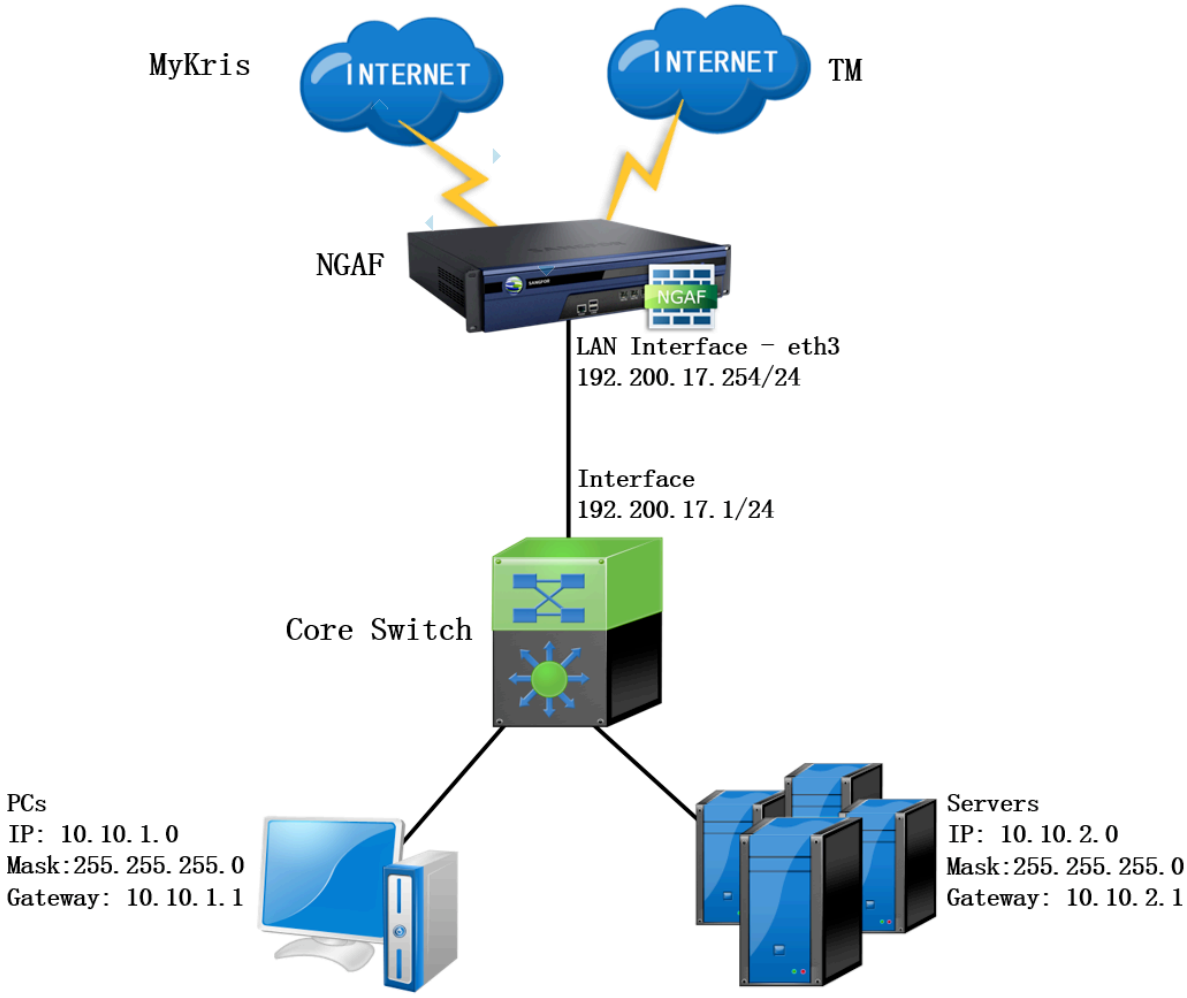
- **Requirement:** User wants work from home or outstation via can connect back to HQ access the applications servers;

  **Solution:** Using NGAF's SSL VPN function to implement remote access servers

- **Requirement:** Would like to allow customers or reader can access their website;

  **Solution:** Configure Destination NAT

Above the solution provided able to achieve customer requirement. Below are after deciding topology.

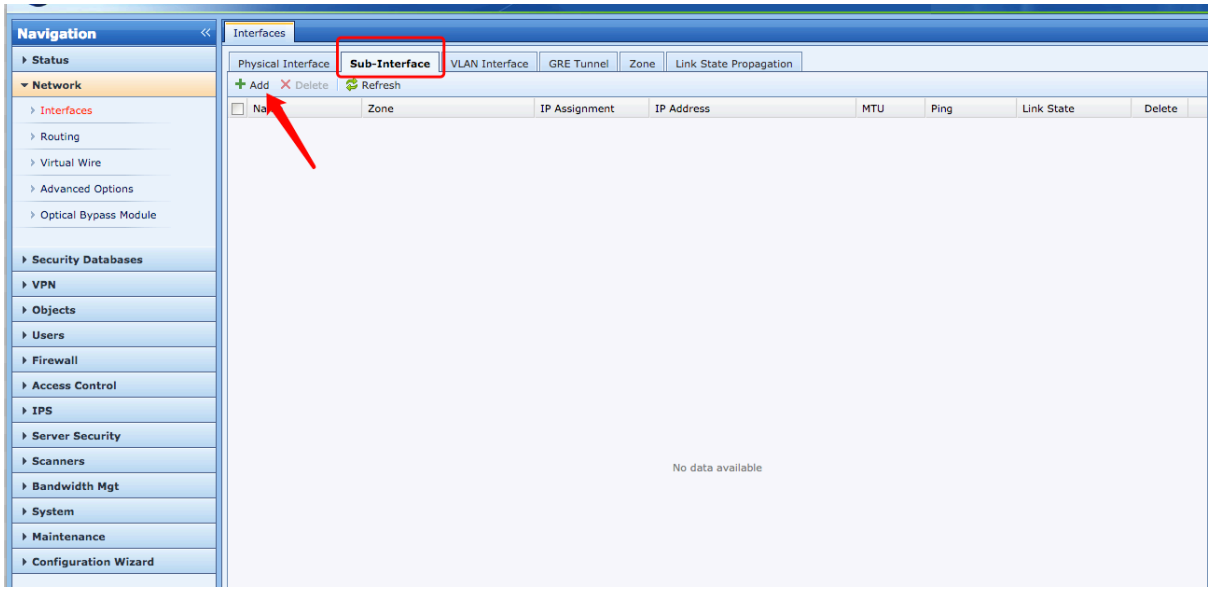


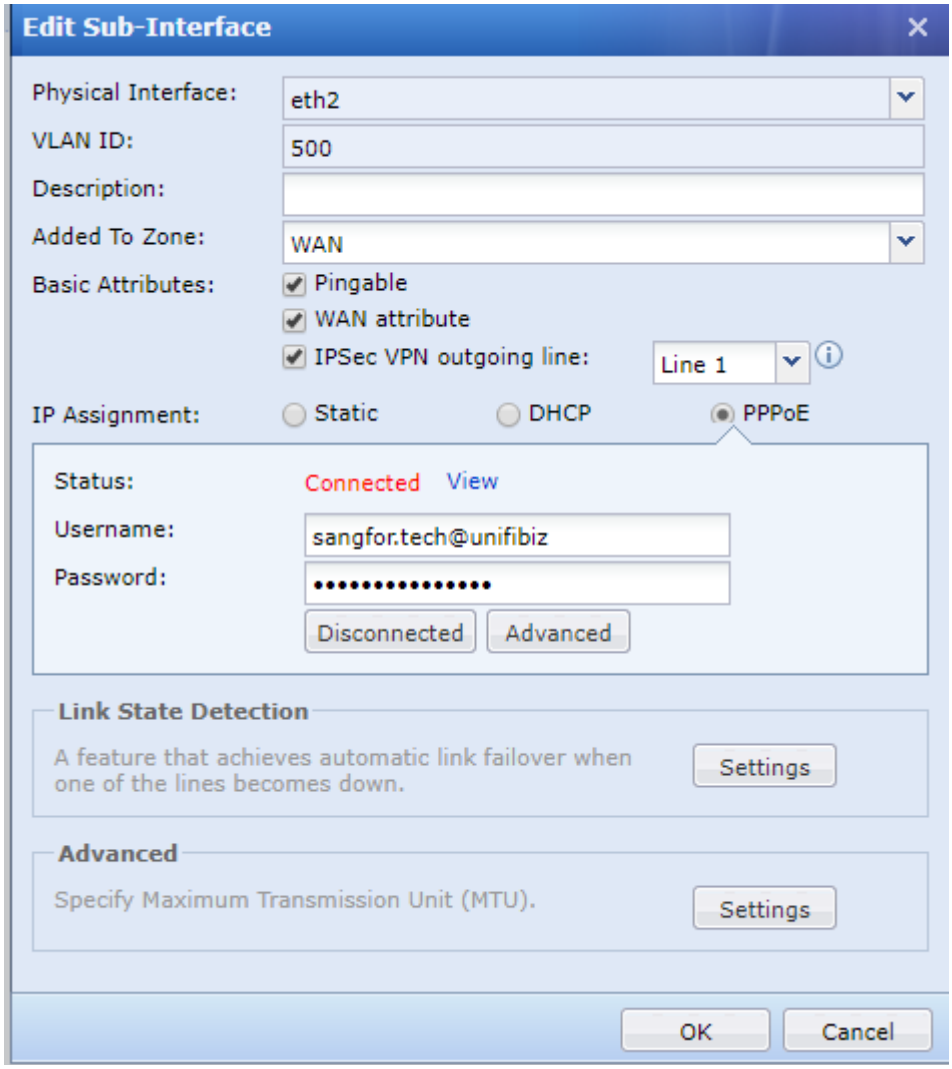

# Chapter 3. Configuration Steps

## 1 Configure Dial-up

Dial up 2 ISP from NGAF.

Login administrator console go to **Network > Interfaces > Sub interfaces,** Click **Add** to add a new Sub-Interface.




**Physical Interface:** assign the physical port as you want to use
**VLAN ID:** define the correct dial up VLAN
**Added to Zone:** define the zone as WAN

**Basic Attributes:** tick Pingable to allow to ping physical IP tick WAN attribute to assign the physical port as WAN & tick IPSecVPN outgoing line to allow VPN to go thought this port.

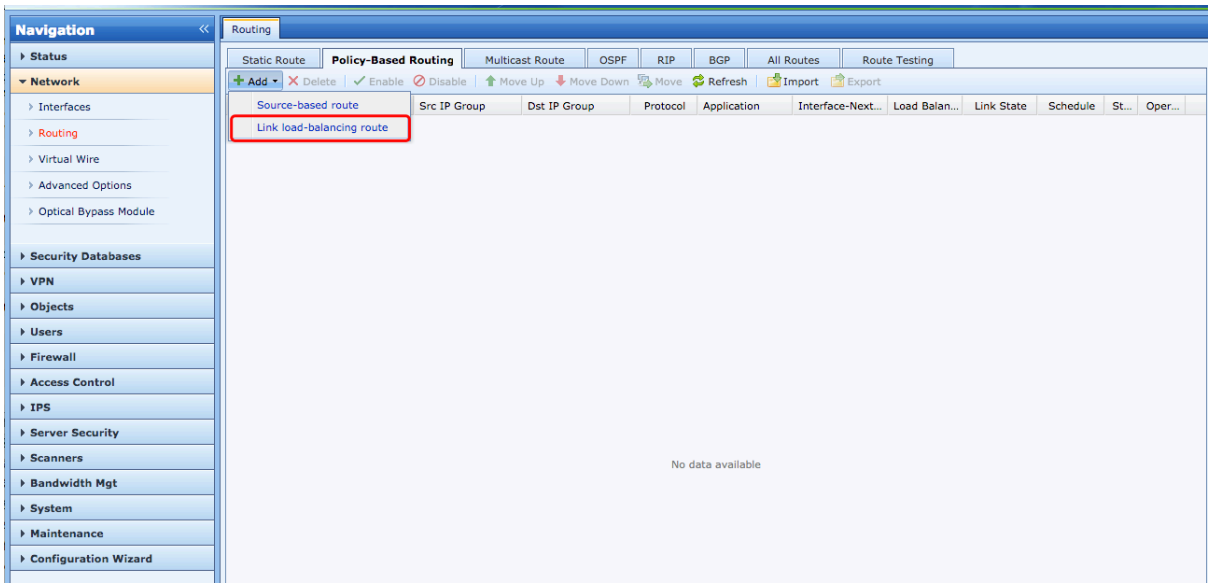
**IP Assignment:** select PPPOE for dial up. Username to fill up dial up ID & Password to key in dial up password and connect.

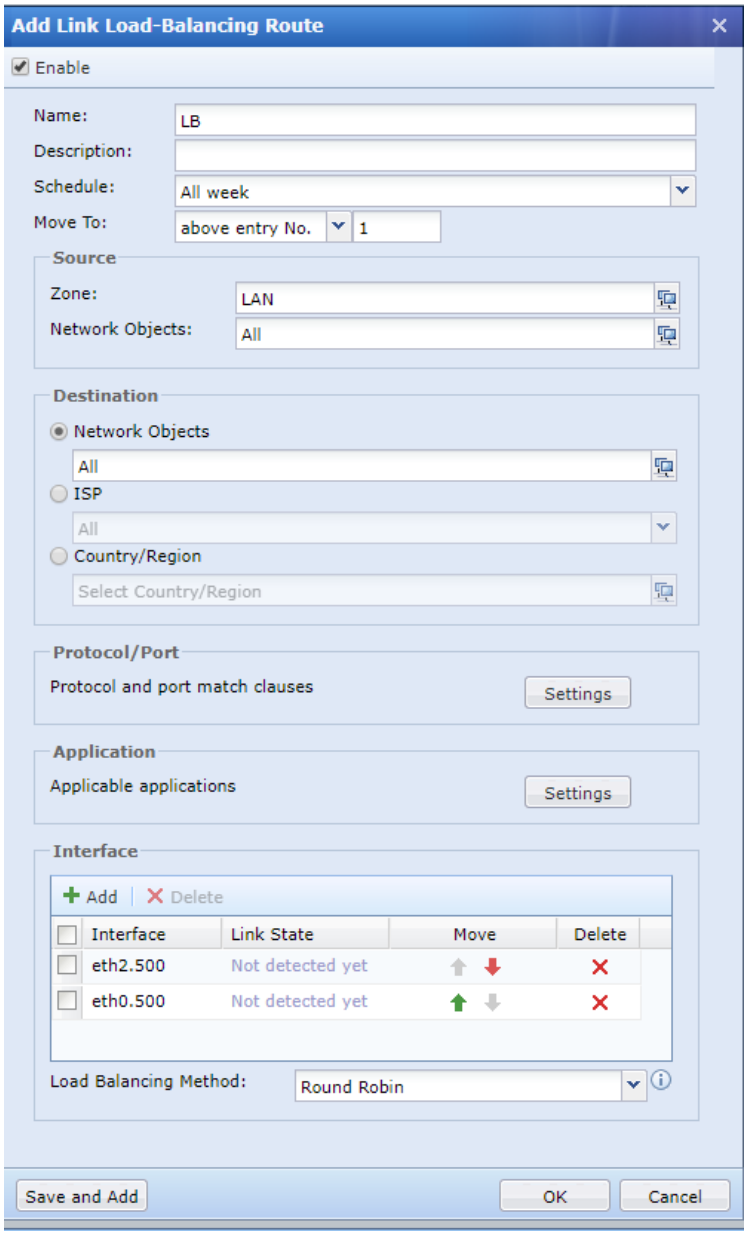
**Remark:** Second ISP dial up configure same as above, from physical interface assign to another available port.

# 2 Configure Link Load Balancing

Configured Link load balancing for 2 ISP line.

Navigate to **Network > Routing > Policy-Based Routing**, Click **Add Link load balancing route** to add a new policy:






**Name:** define the name

**Source Zone:** select LAN for internal segment

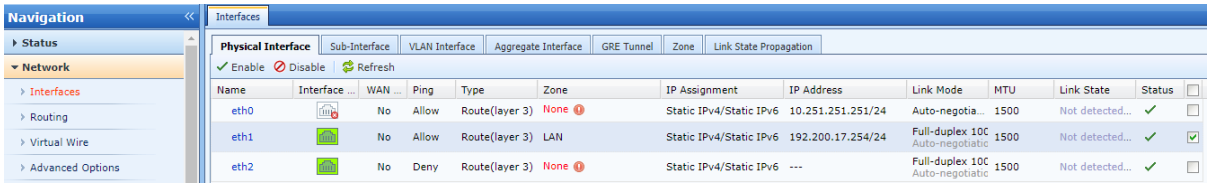
**Destination Zone:** select All from Network Objects

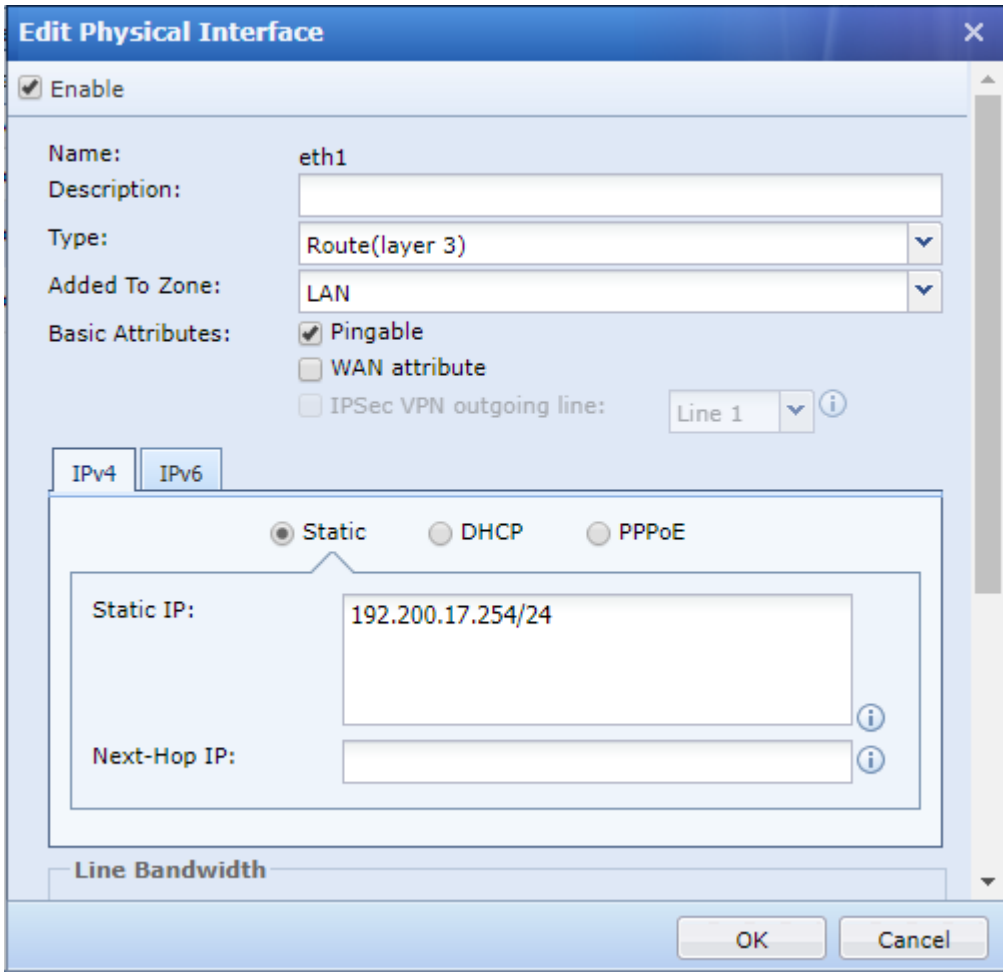
**Interface:** add 2 WAN dial up physical port

# 3 Configure Other Network Configurations

## 3.1 LAN Interface

Go to **Network > Interface > Physical interface,** Click **eth1** to edit it as LAN Interface and LAN Zone.




**Type:** Route mode

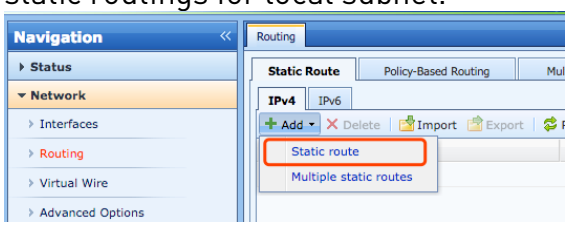
**Added to Zone:** create the LAN zone

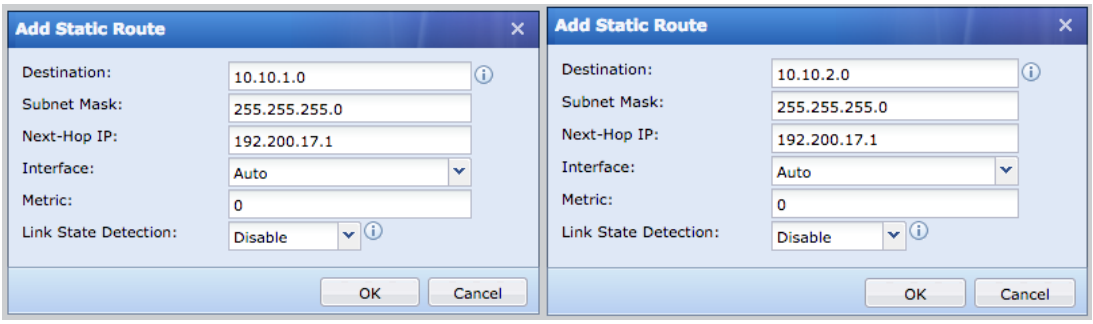
**Basic Attributes:** tick Pingable

**IPv4:** define the static IP for LAN

## 3.2 Routing

Go to **Network > Routing > Static Route > IPv4**, click **Add Static route** to add two static routings for local subnet.

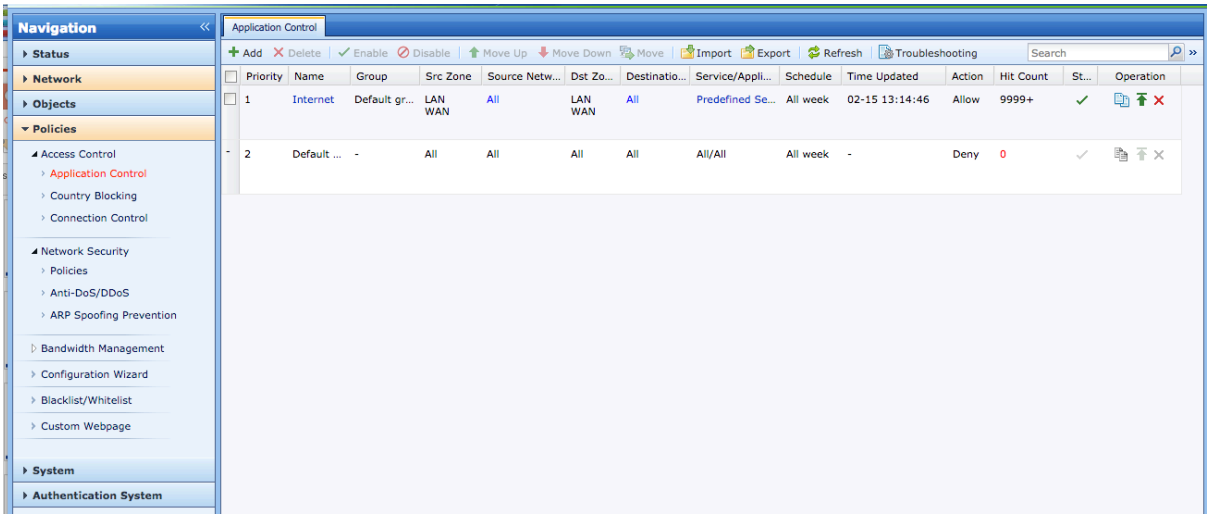




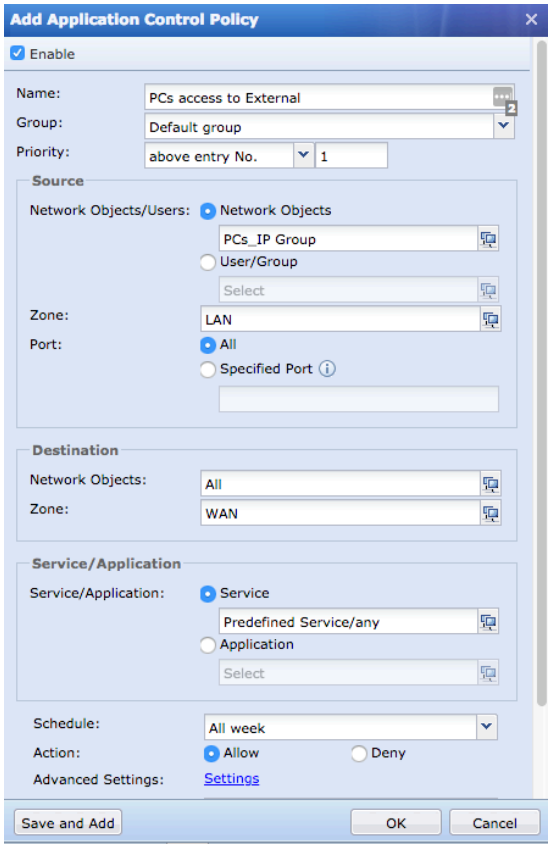

# 4 Configure Application/Service Control

NGAF deny all applications and services by default policy. You need to set the Application control policy to allow the traffic.

Go to **Policies > Access Control > Application Control**, click **Add** to add new policy to allow the traffic.




For Examples, allow intranet access to external.

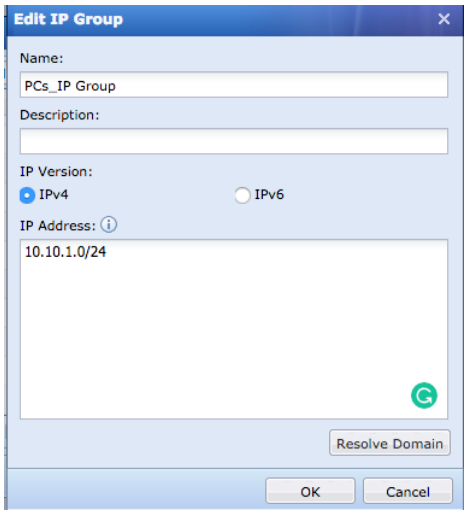



**Source:**

**Network Objects:** create an IP group containing the PCs segment and select it

**Zone:** select LAN zone

**Port:** select All



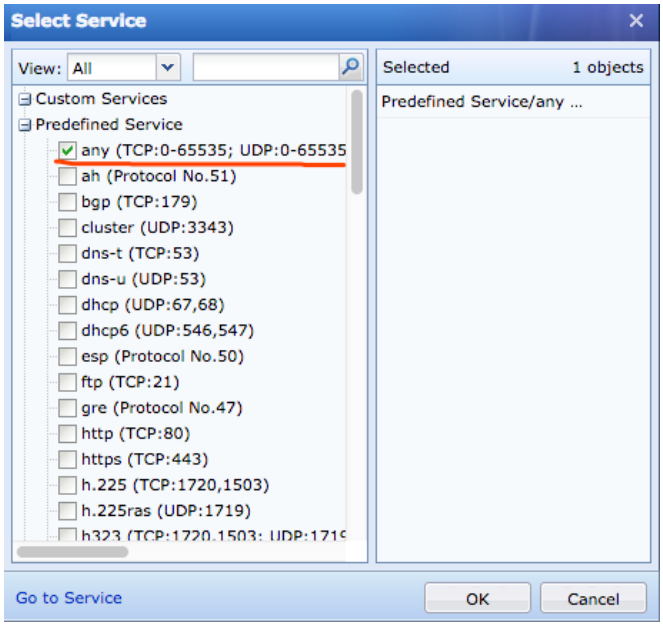

**Destination:**

**Network Objects:** select All

**Zone:** select WAN zone

**Service/Application:**

**Service:** select any

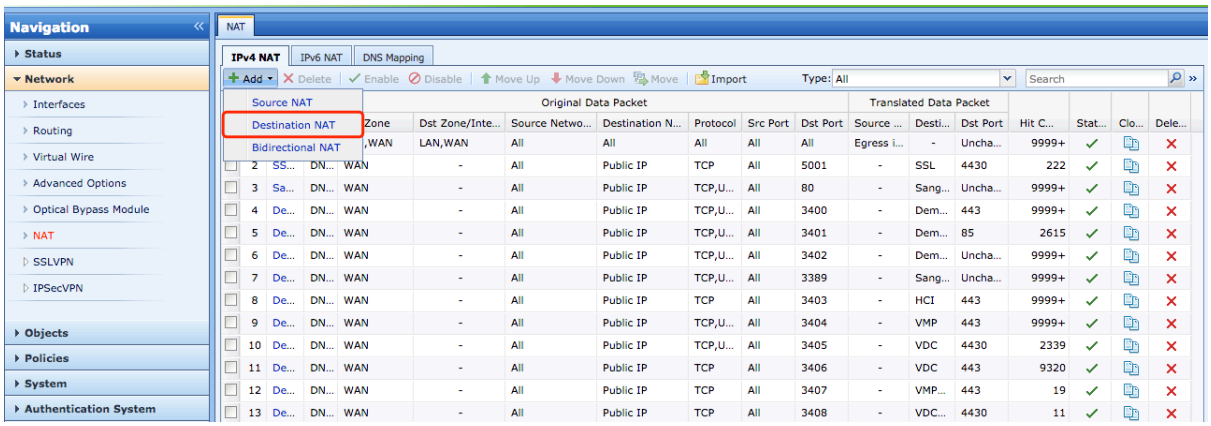


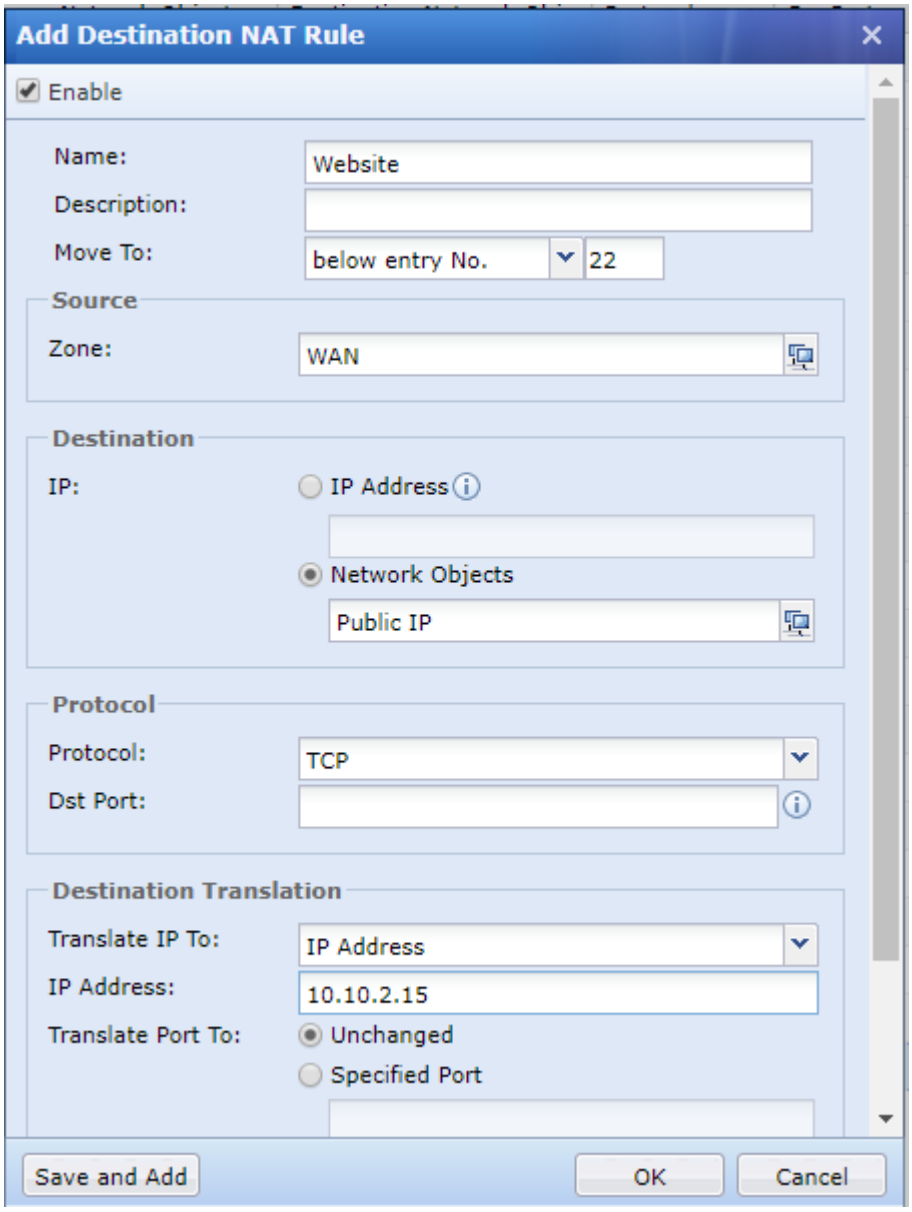

**Schedule:** select All week
**Action:** select Allow

# 5 Configure Destination NAT

Configure DNAT for customers or reader can access their website.

Go to **Network > NAT**, Click **Add Destination NAT** to add a new Destination NAT policy.






**Name:** decide the name

**Source:** select zone as WAN

**Destination:** select either IP address or Network Objects for WAN public IP

**Destination Translation:** select translate IP to IP address, IP address put the web server IP

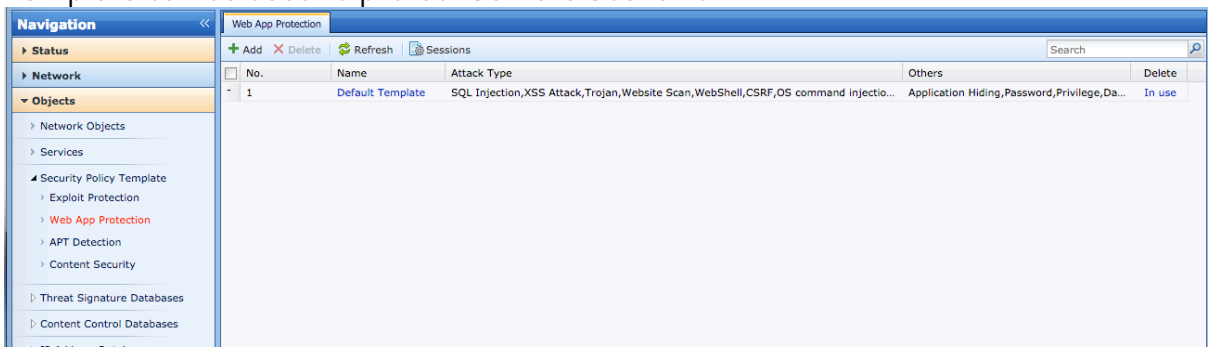
# 6 Configure IPS&WAF&ATP Policy

## 6.1 Use the default IPS Objects

Go to **Objects > Security Policy Template > Exploit Protection**. There are two templates we can use, one is for Internet Access Scenario, the other is for Server Scenario.

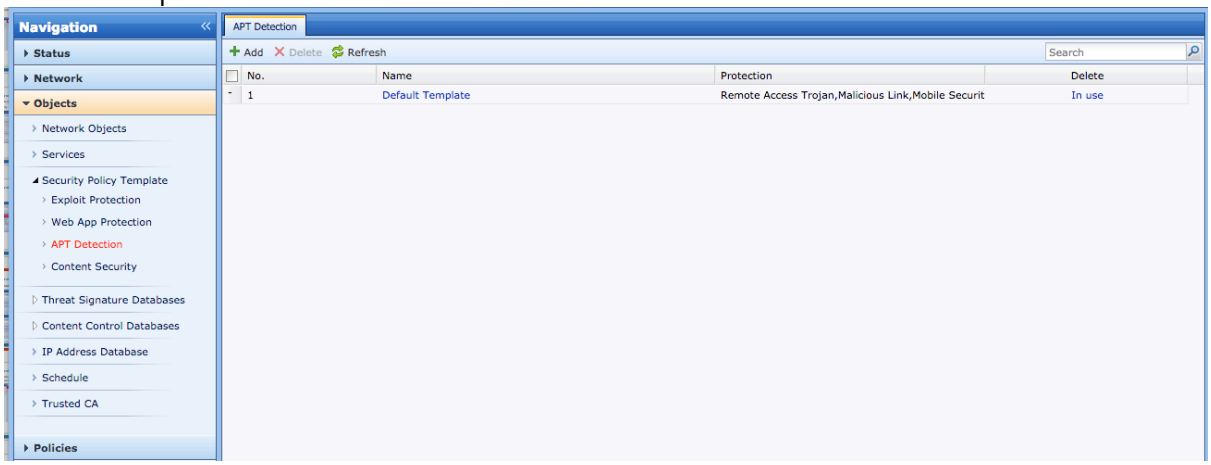

## 6.2 Use the default WAF Objects

Go to **Objects > Security Policy Template > Web App Protection**. This Default Template can be used to protect Servers Scenario.



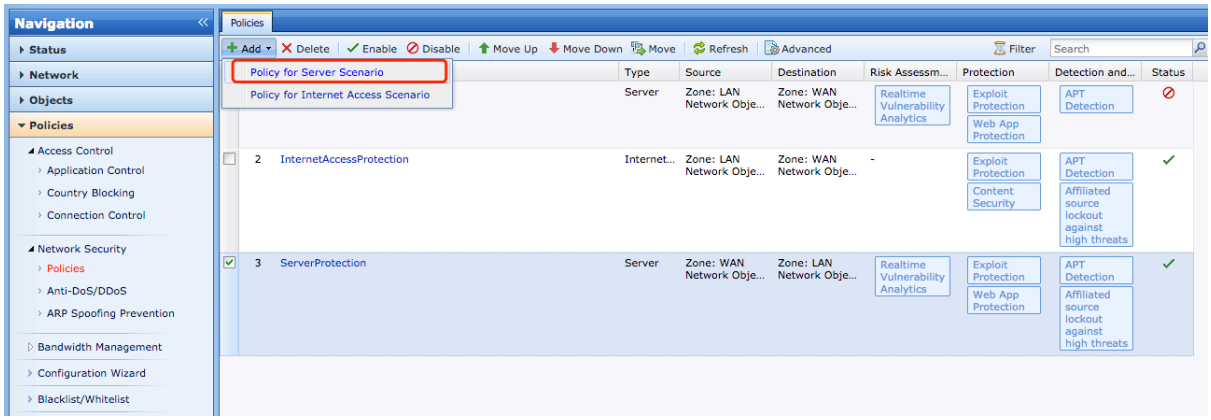

## 6.3 Use the default APT Objects

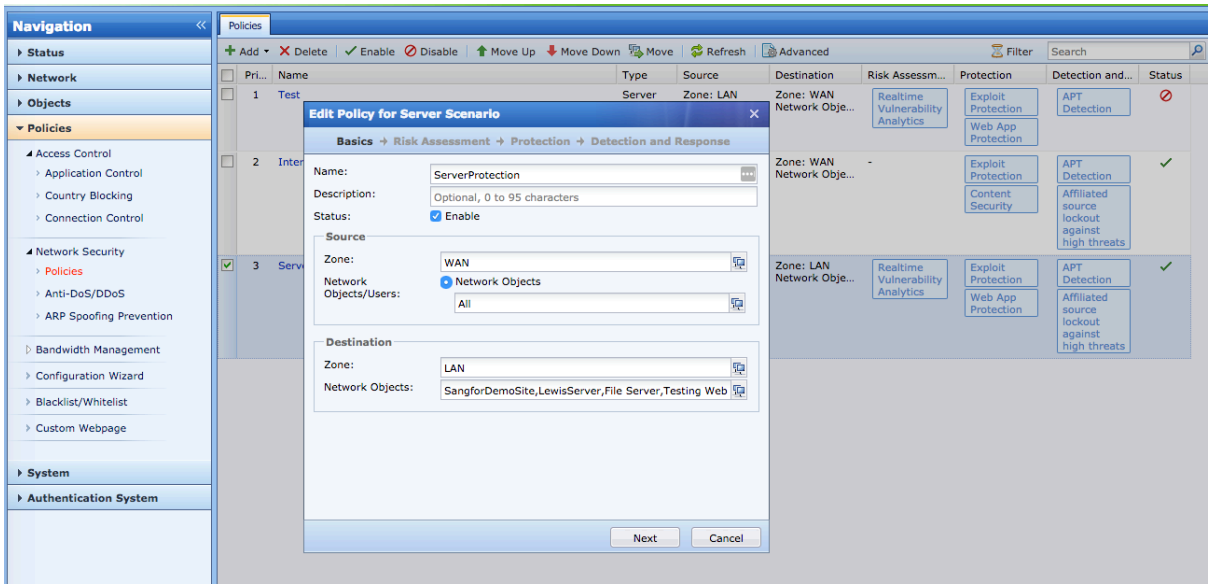
Go to **Objects > Security Policy Template > ATP Detection**. This Default Template can be used to protect Internet Access Scenario.




## 6.4 Configure Security Ploicies for Server Scenario

Go to **Policies > Network Security > Policies**, click **Add > Policy for Server Scenario,** to add a new policy.




**Name:** define the policy name

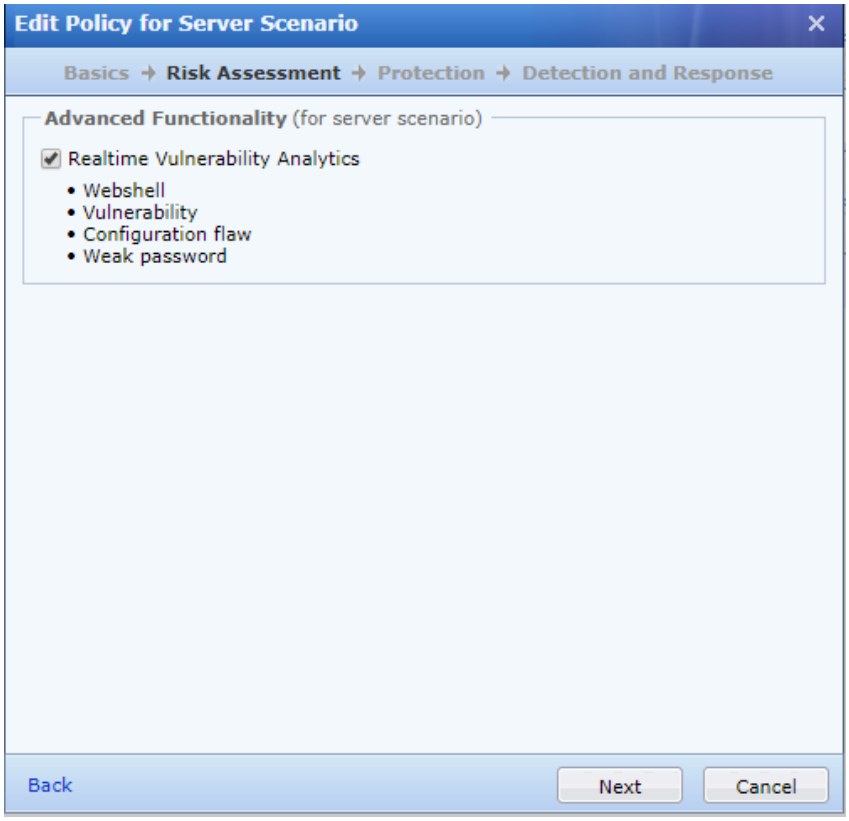
**Status:** make to Enable for this policy

**Source:** select WAN Zone and Network Objects/Users select All to prevent from outside. We do not know which public IP access server, so the source IP selects all

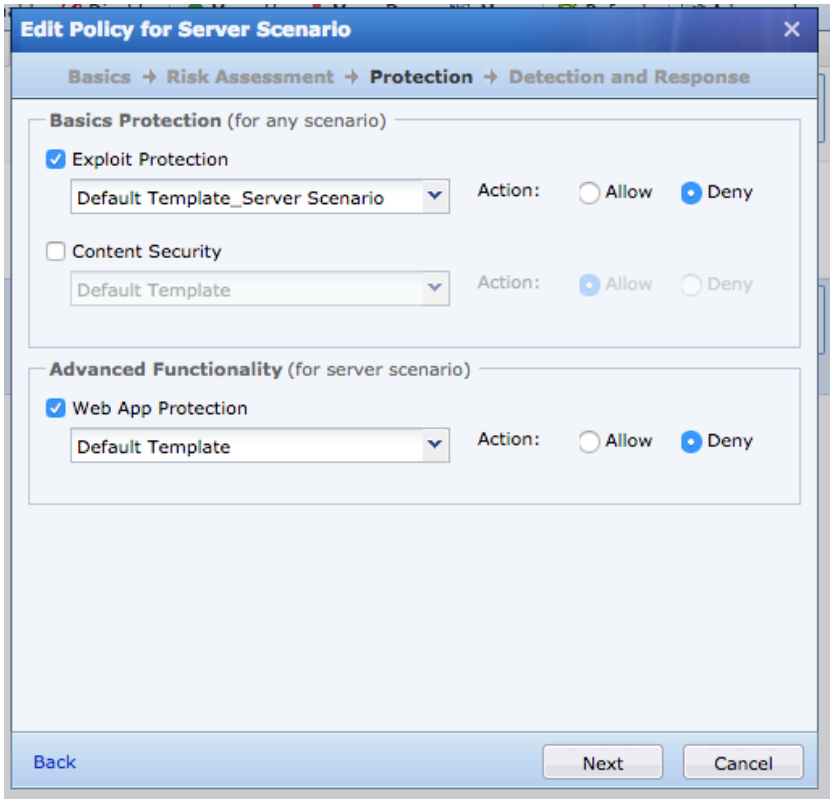
**Destination:** Zone select LAN to protect internal and Network Objects to protect selected servers

Source zone is the initiator of the TCP link. In the Server Scenario, the source zone is outside. And we do not know which public IP access server, so the source Network Objects selects All.

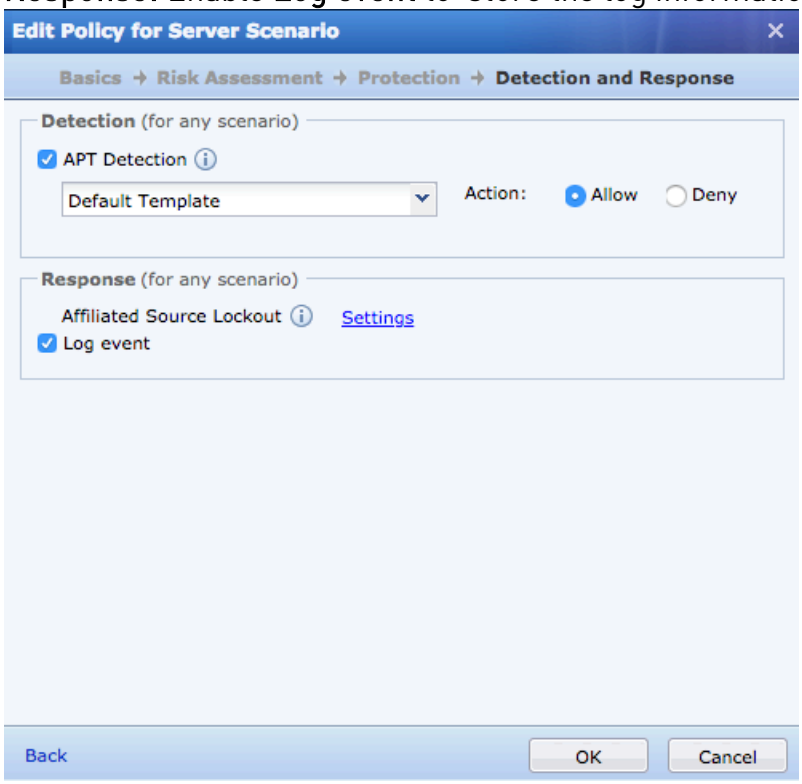
And then click **Next,** to configure **Realtime Vulnerability Analytics**




Click **Next**, to configure IPS and WAF policy.
**Exploit Protection (IPS):** Enable it, select **Default Template_Server Scenario** and select **Deny** Action.
**Web App Protection (WAF):** Enable it, select **DefaultTemplate** and select Deny Action.




Click **Next**, to configure **Detection and Response** policy.
**APT Dectection:** Enable it, select **Default Template** and select **Allow** Action.
**Response:** Enable **Log event** to store the log information.



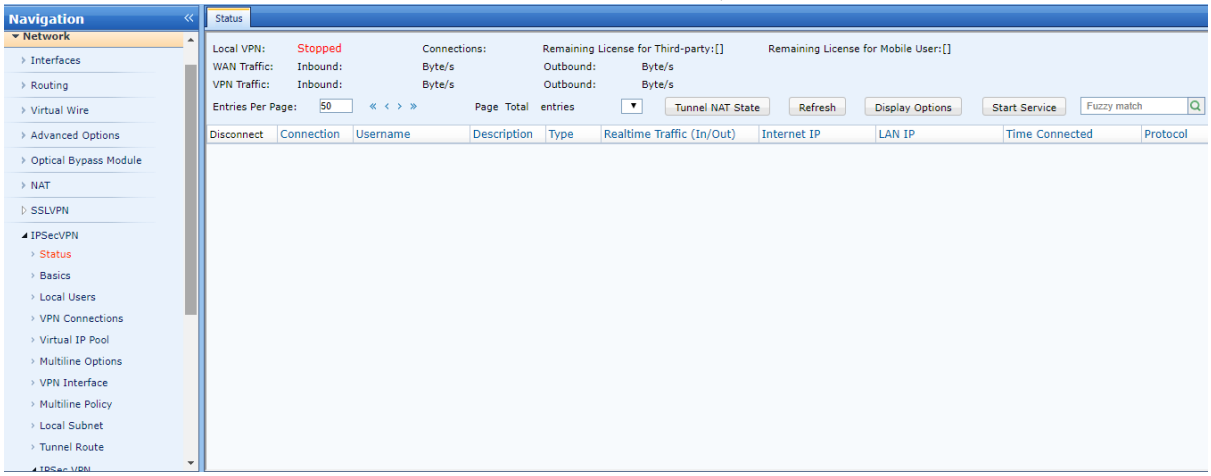

Click OK, complete the configuration.

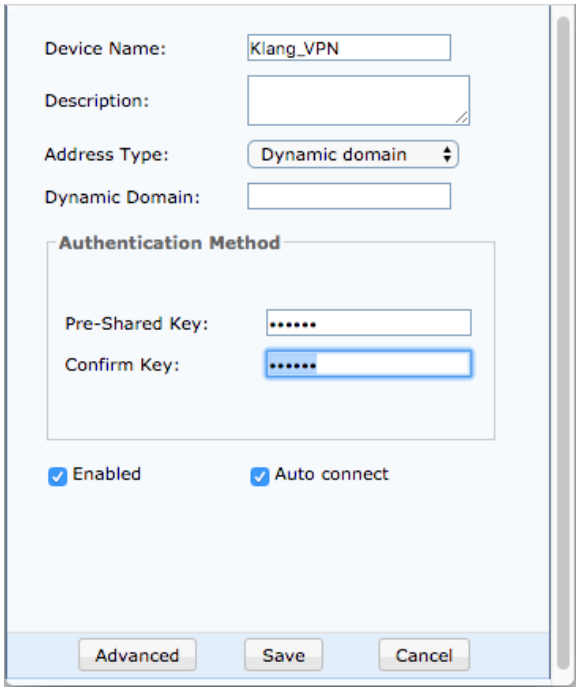
# 7 Configure IPSecVPN

Build IPSecVPN with third party devices. NGAF as Master, third party as Client.

## 7.1 Configure Phase I

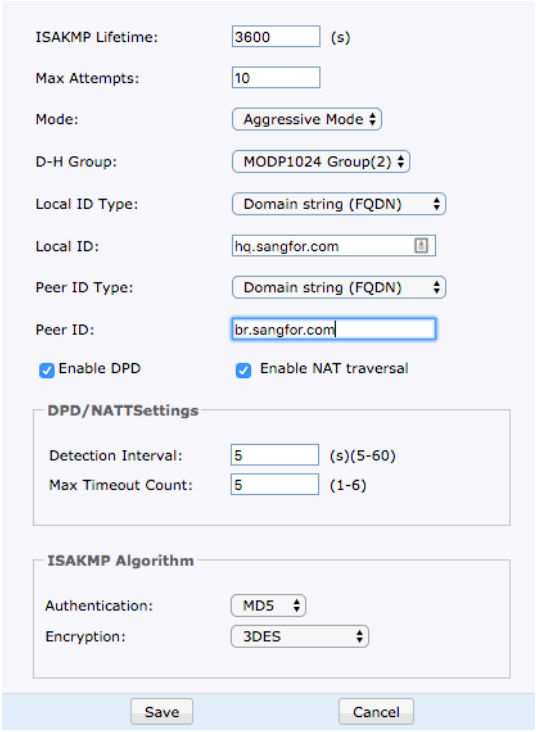
Go to **Network > IPSecVPN > IPSecVPN > Phase I**, click **Add** to add a Peer Device.




**Device Name:** define the name
**Address Type:** set Dynamic IP address (because the opposite is dynamic public IP)
**Pre-Shared Key:** Create the Pre-share key for authentication
**Confirm Key:** Create the password for authentication

Cilck **Advanced** to edit the options.

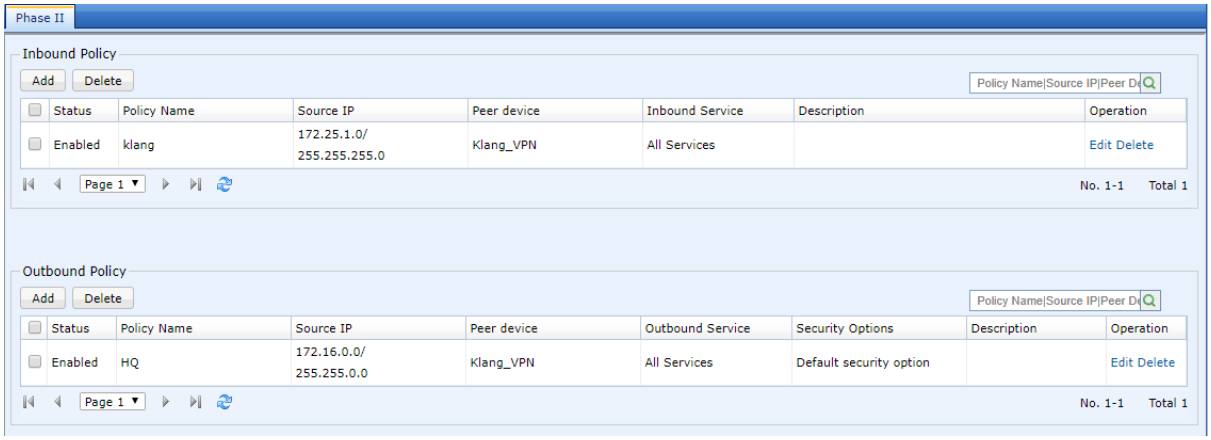


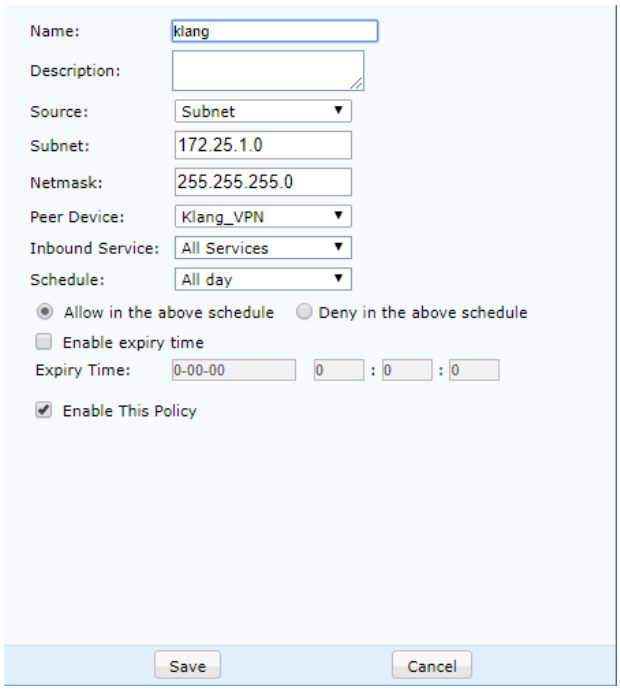

**Mode:** choose the **aggressive mode**
**D-H Group:** by default, is **MODP1024 Group2**
**Local ID Type:** select **Domain string (FQDN)**
**Local ID:** define the local ID name
**Peer ID Type:** select **Domain string (FQDN)**
**Peer ID:** get the Peer-ID from third-party device
**Enable DPD**
**Enable NAT traversal**
**DPD/NATTSettings:** Detection Interval as 5s and Max Timeout Count 5s
**ISAKMP Algorithm:** define the Authentication as MD5 and Encryption as 3DES (by default setting)

Make sure third-party device setting same as above of NGAF.

## 7.2 Configure Phase II

Go to **Phase II > Inbound Policy**, click **Add** to add a new inbound policy.

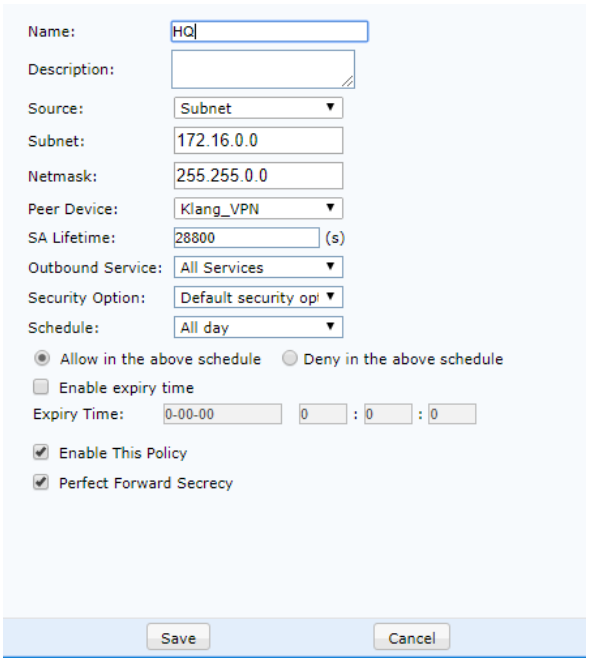



**Name:** define the name
**Source:** select subnet
**Subnet:** configure Peer IP subnet
**Netmask:** configure Peer Netmask
**Peer Device:** select the Phase I policy

Inbound Policy is configuring Peer IP segment into access Local segment.

Go to **Phase II > Outbound Policy**, click **Add** to add a new outbound policy.

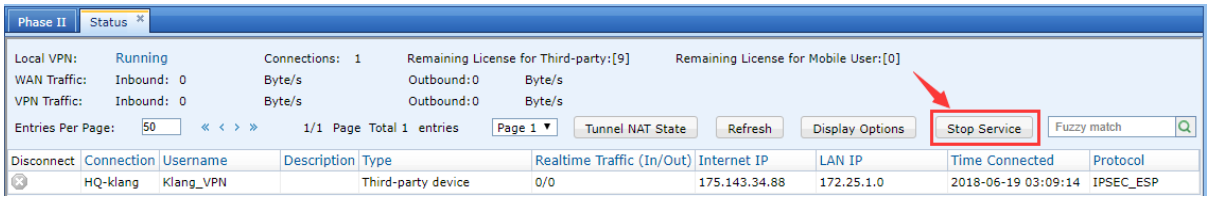



Name: define the name
Source: select subnet
Subnet: configure internal IP segment
Netmask: configure internal Netmask
Peer Device: select Phase 1 policy

Outbound Policy is configuring Local IP segment go to Peer segment.

## 7.3 Check the IPSecVPN status

Go to **Network > IPSecVPN > Status**, confirm the **Service** is enabled and the connection has been established.

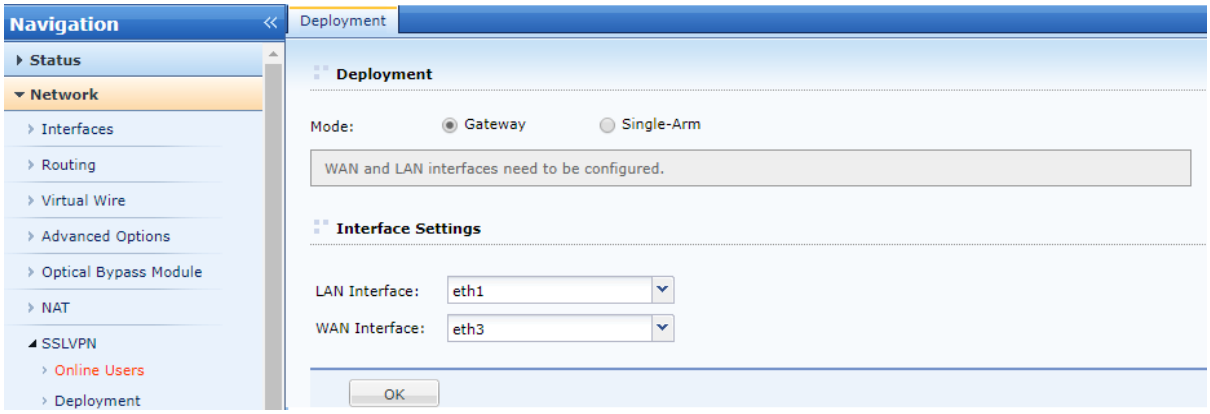



# 8 Configure SSLVPN

Configure SSLVPN to allow users access for internal application/servers via outside.

## 8.1 Configure Deployment Model

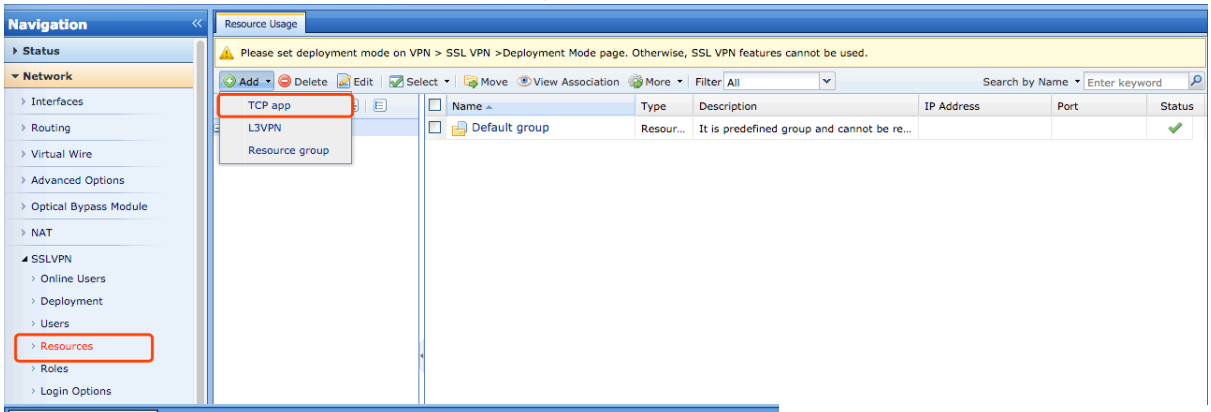
Go to **Network > SSLVPN > Deployment**, click **Gateway Mode**.

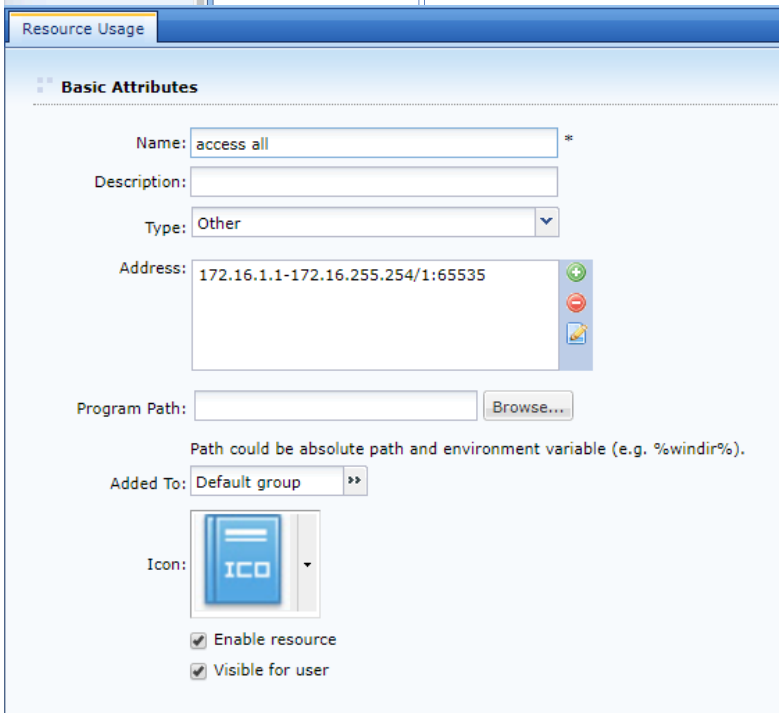



**LAN Interface:** eth1 (the port that assign to LAN zone, inbound traffic)
**WAN Interface:** eth3 (the port that assign to WAN zone, outbound traffic)

## 8.2 Configure Resource

Go to **Network > SSLVPN > Resource**, click Add to a new TCP Resource



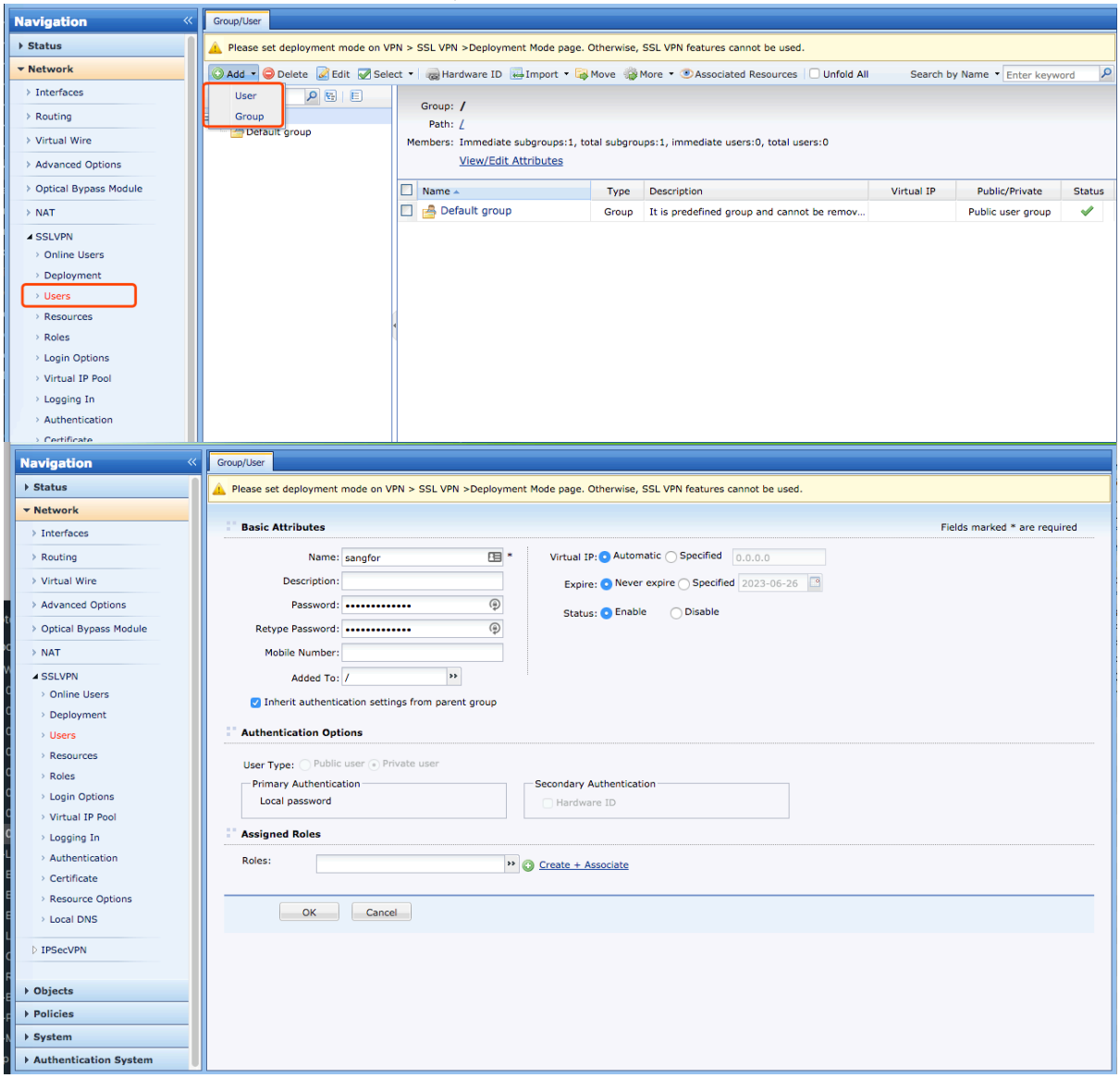

**Name:** define the resource name
**Type:** select Other

**Address:** input Internal segment range, port input 1:65535

This address and port is for SSLVPN users to access.

## 8.3 Add SSLVPN Account

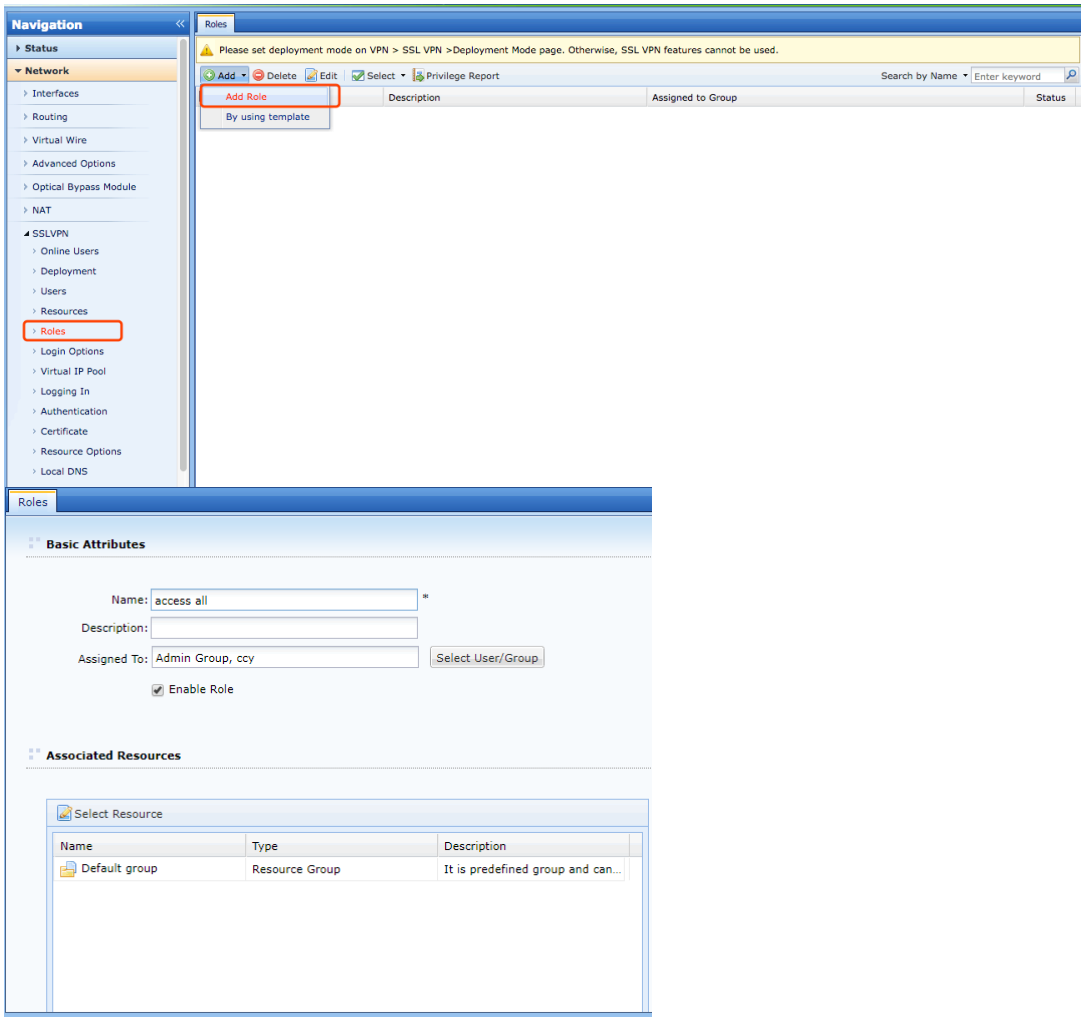
Go to **Network > SSLVPN > Users**, click **Add User** to add a new account.




**Name:** define the user name
**Password:** define the user password
**Retype Password:** reconfirm password
**Assigned Roles:** temporarily left bank, configured it on the Role's configuration page

## 8.4 Configure Role

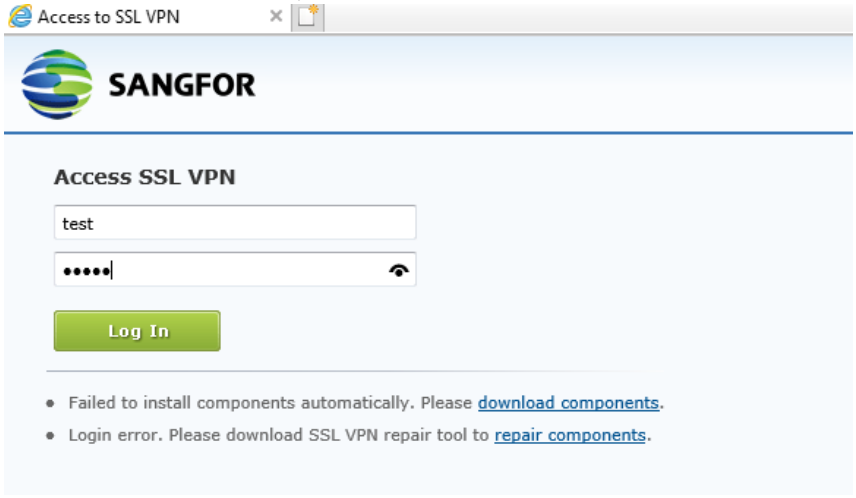
Go to **Network > SSLVPN > Roles**, click **Add Role** to add new role.




**Name:** define the roles name
**Assigned to:** select users who will give the same rights
**Associated Resources:** select the Resource that you want users in this role to access.

## 8.5 Access SSLVPN From The Internet

Access SSLVPN via Public IP port is 4430, example; https://xx.xx.xx.xx.xx:4430, screenshot as below;



SANGFOR