

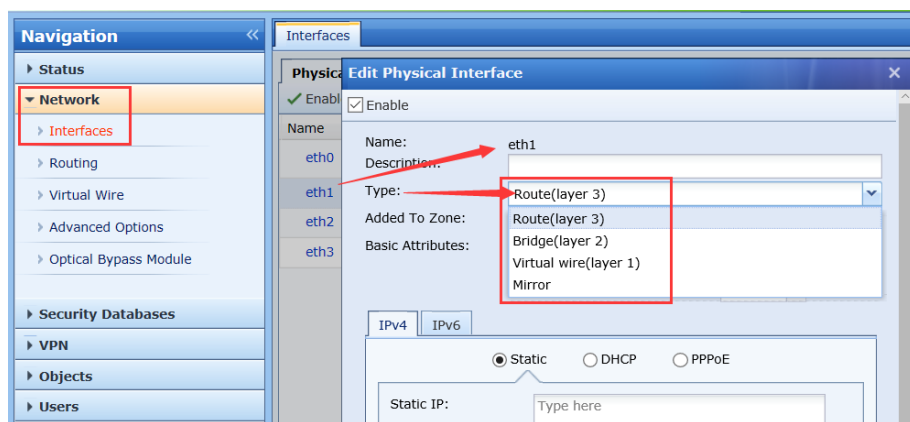
Target

- 1) Network deployment.
- 2) Access Control.
- 3) IPS.
- 4) Server Security.
- 5) Bandwidth Management.
- 6) Scanners.

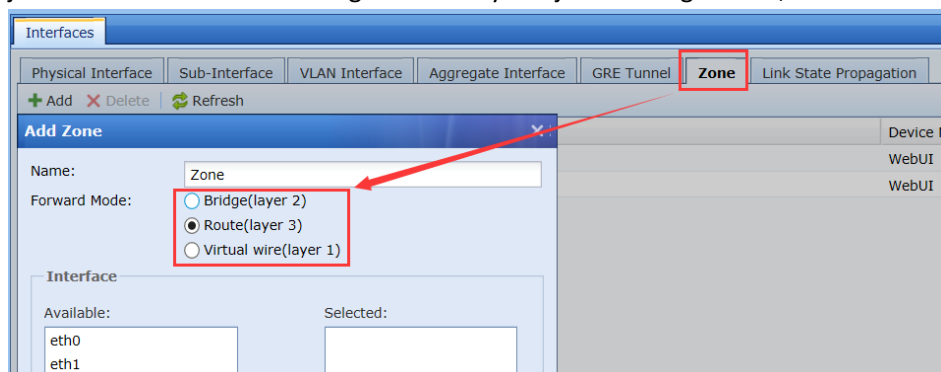
For login to NGAF, this is a **Management port** which default ip is **10.251.251.251/24**, and we cannot change this ip. Default username and password are 'admin'.

1, Network Deployment

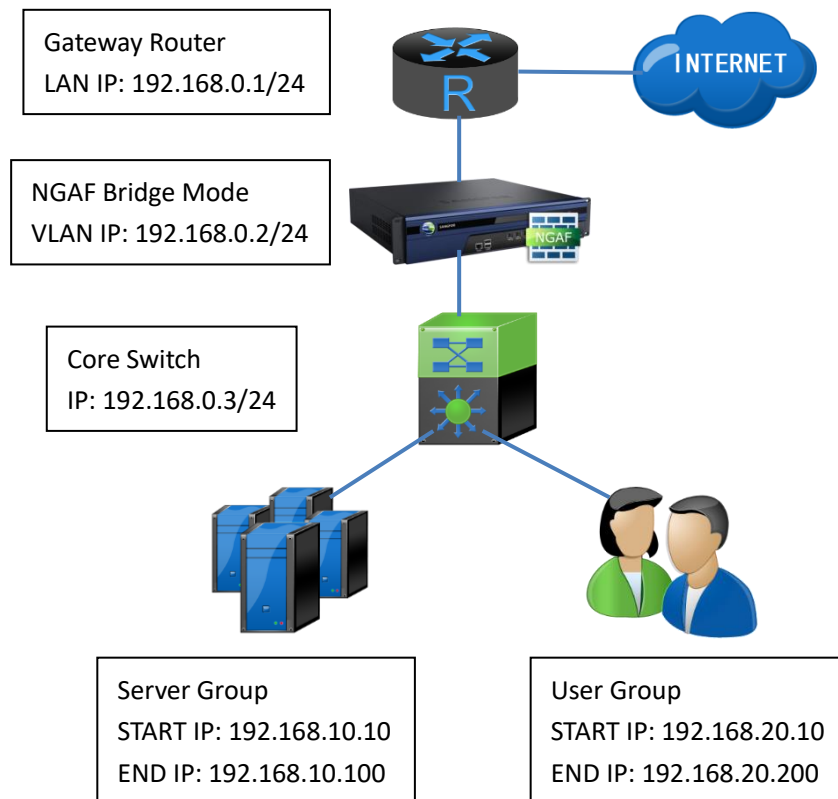
- 1) Port Type: Route, Bridge, Virtual wire.
 - a. Route Mode: Port work as a route port, it can configure ip address.
 - b. Bridge Mode: Port work as a switch port, it means no ip required and it forward packages by mac address.
 - c. Virtual Wire: 2 ports make a Virtual wire group. One port always transmits to the other interface.



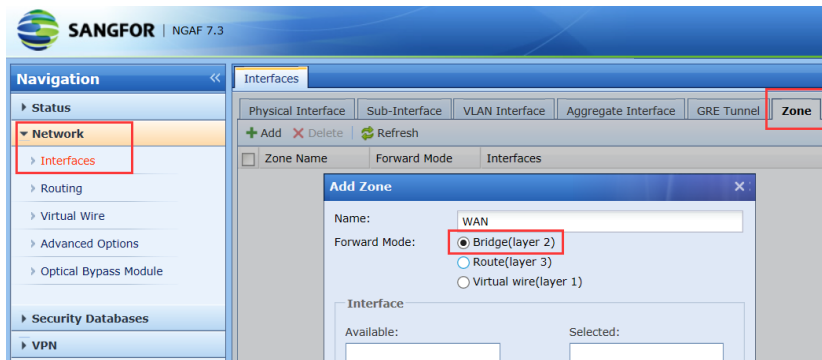
- 2) Zone
 - 3 types mode, Bridge mode, Route mode and virtual wire mode. Route mode port only can join to Route mode Zone. Bridge mode only can join to Bridge mode, same to virtual wire.



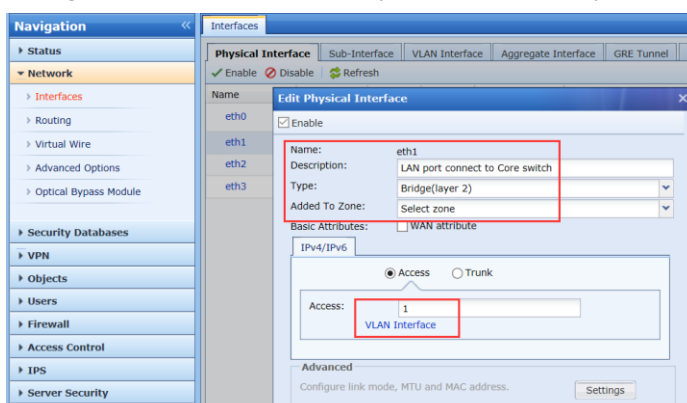
1.1 Bridge Mode Deployment

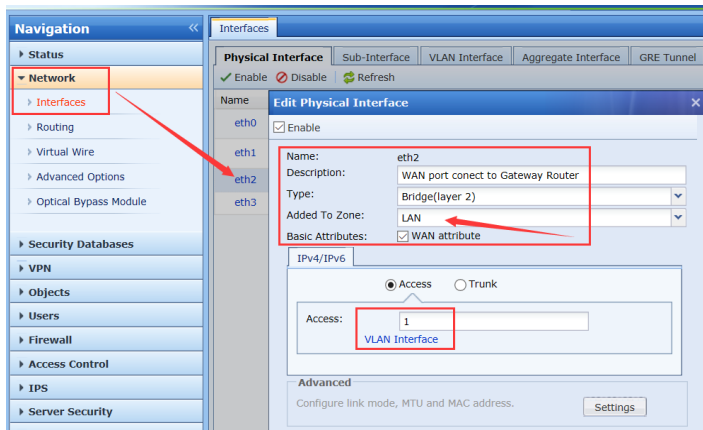


- 1) Add Zone. WAN Zone and LAN Zone.

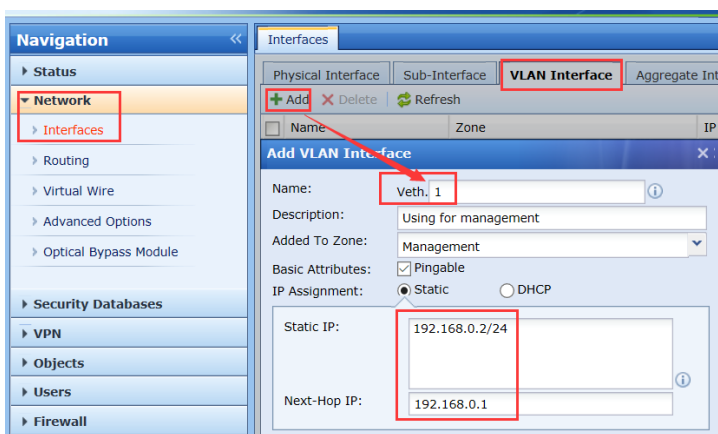


- 2) Configure interface. Eth1 to LAN port, eth2 to WAN port.

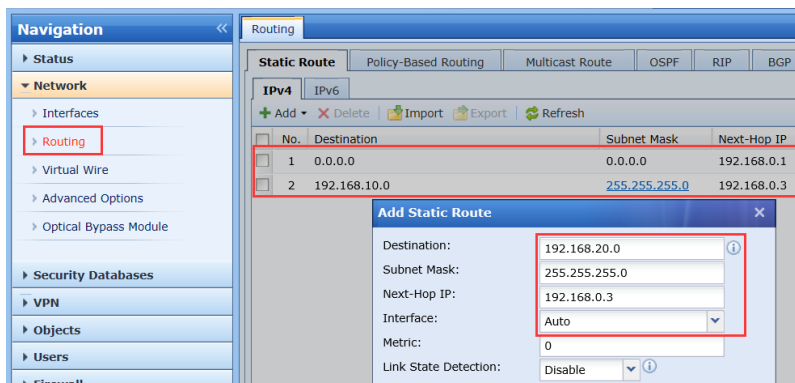




And create a vlan interface, set a ip address to this vlan interface which is used for NGAF management.

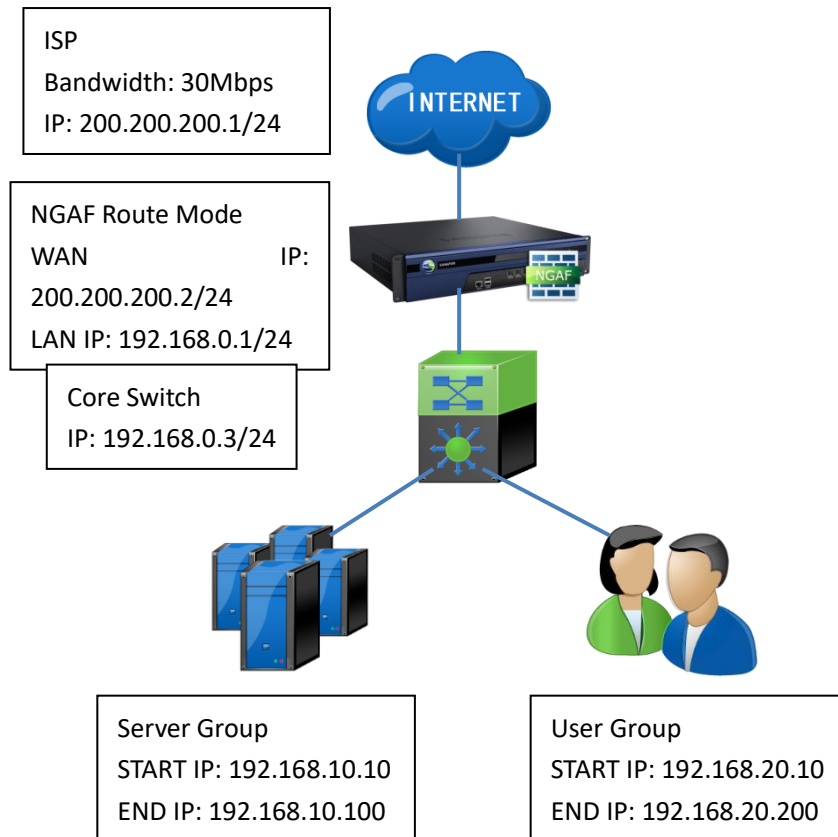


3) Route, in this case, we need add 3 static routes, default route and 2 return routes.

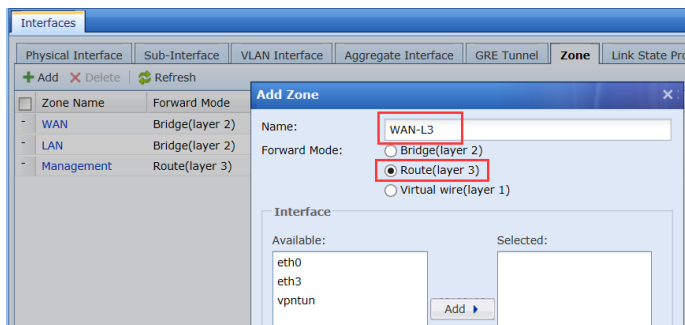


4) One more important thing, NGAF blocks all data forwarding by default, so we need add a Access Control policy to allow some legal visit.

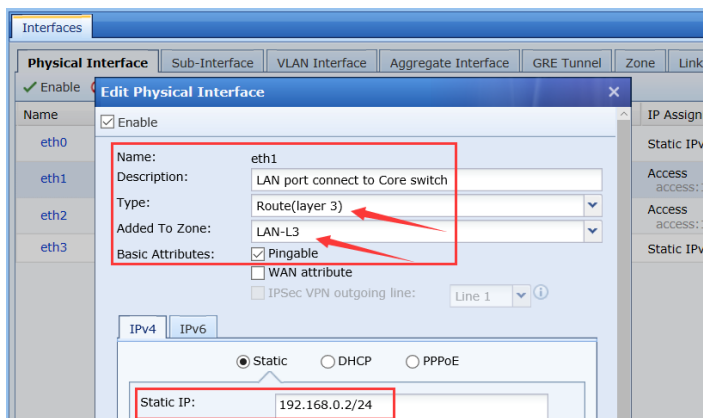
1.2 Route Mode Deployment

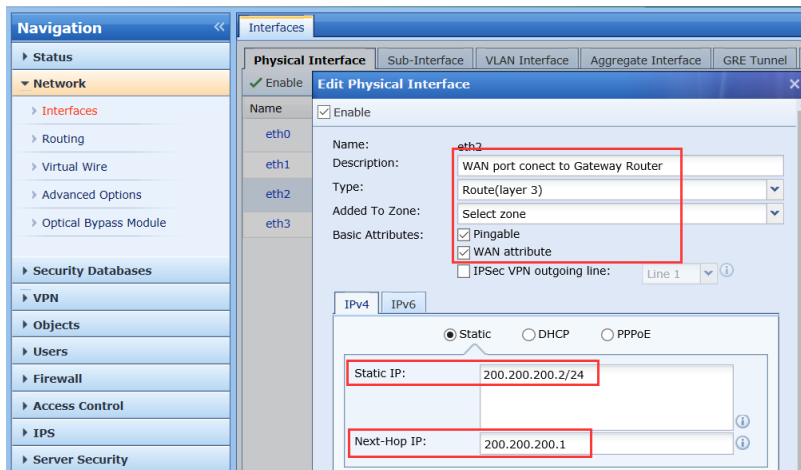


- 1) Add Zone. WAN Zone and LAN Zone.

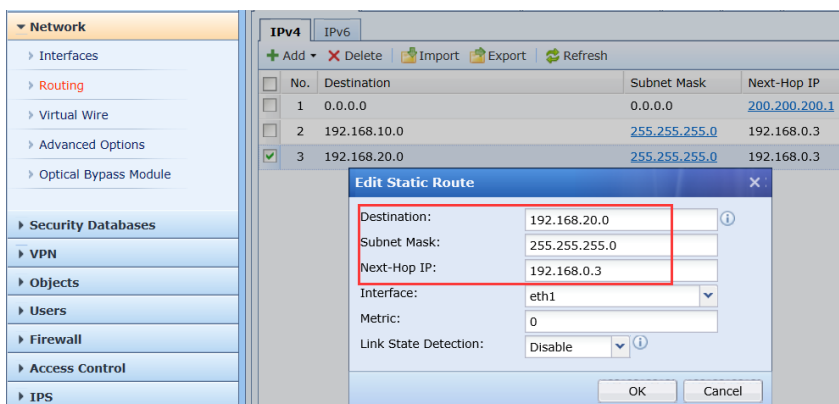


- 2) Configure interface. Eth1 to LAN port, eth2 to WAN port.

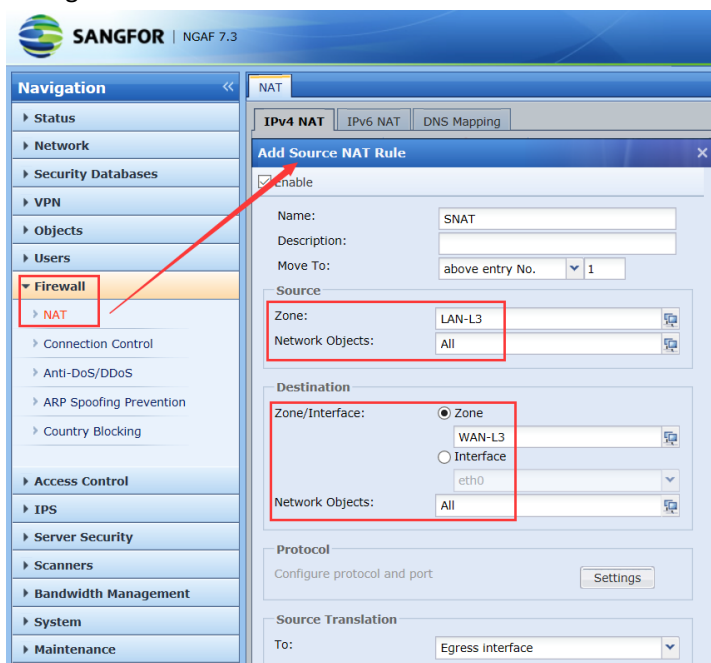




- 3) Route, in this case, we need add 3 static routes, default route and 2 return routes.



- 4) Configure Source NAT.



- 5) One more **important** thing, NGAF blocks all data forwarding by default, so we need add a Access Control policy to allow some legal visit.

2, Objects

In this case, we have 2 groups need created, one is server ip group, another one is user ip group.

The screenshot shows the Sangfor NGAF interface for managing Network Objects. The left sidebar has a 'Network Objects' menu item highlighted. The main panel shows a table of existing IP groups. A red arrow points from the 'Add' button to the 'Edit IP Group' dialog box. In the dialog, the 'Name' field is 'Users', the 'Description' is 'user group', and the 'IP Address' field is '192.168.20.10-192.168.20.200'.

No.	Name	Type	IP Range
1	All	IP Group	All
2	Private Network Segment	IP Group	10.0.0.0-10.255.255.255 172.16.0.0-172.31.255.255 192.168.0.0-192.168.255.255
3	Server IP Group	IP Group	192.168.10.0/24
4	Users	IP Group	192.168.20.0/24

Edit IP Group

Name: Users

Description: user group

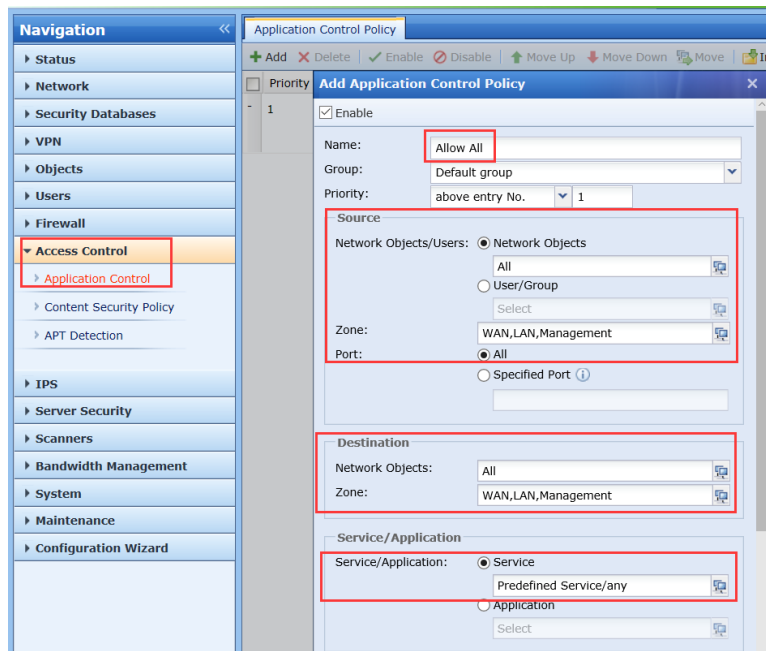
IP Version: ☒ IPv4 ☐ IPv6

IP Address: 192.168.20.10-192.168.20.200

Resolve Domain

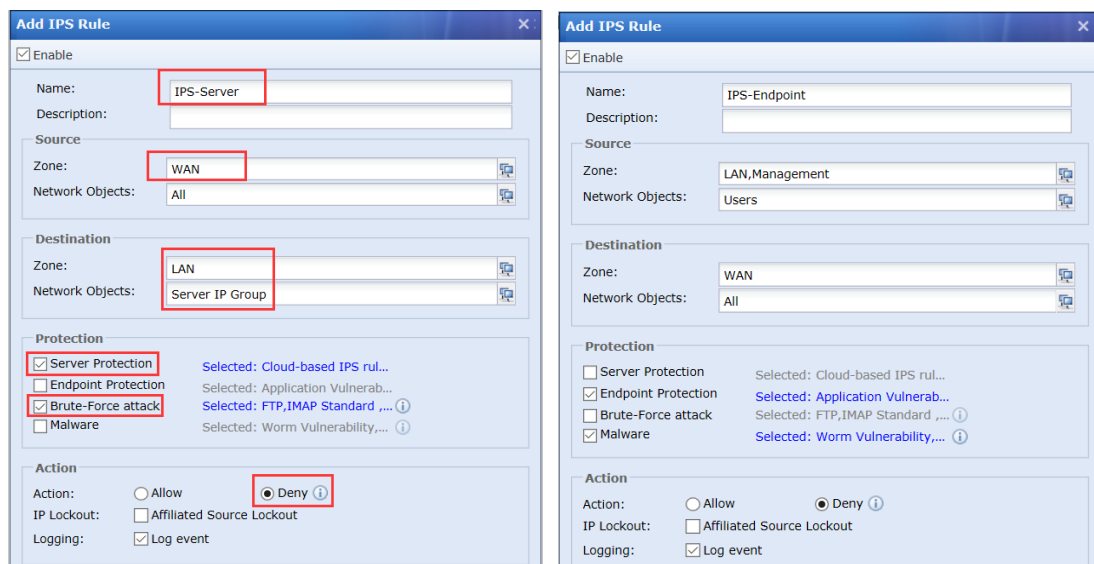
3, Access Control

Path: Access Control-> Application Control



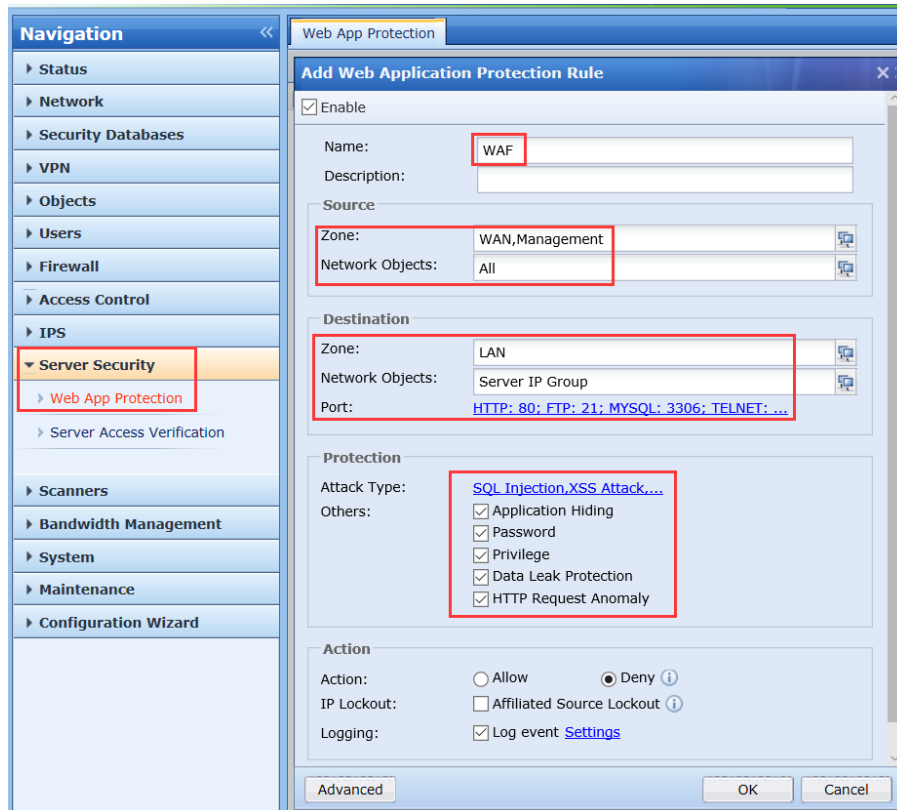
4, IPS

IPS policy can protect server and endpoint. So we can add 2 policies, 1 for server, 1 for endpoint.



5, Server Security

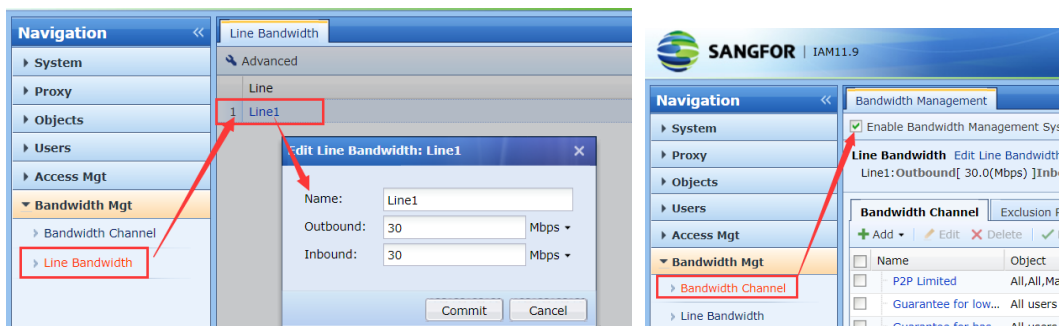
Web Application Protection. Protect the web server from attacks which from WAN zone.



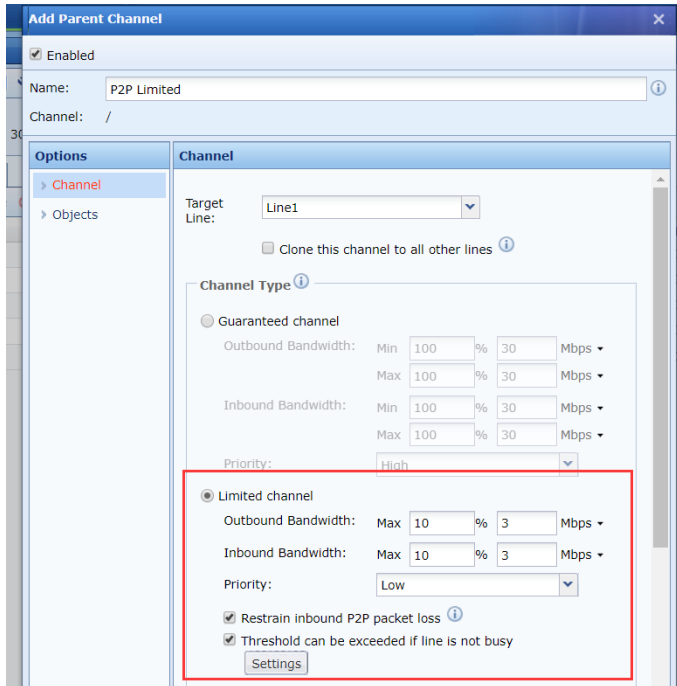
6, Bandwidth Management

- All P2P applications' traffic can't more than 10% of total bandwidth.
- Create a Guaranteed channel for Mail service at least 50% of the total bandwidth, but per user cannot more than 2 Mbps/s.

1) Define the total bandwidth. In this case, the bandwidth is 30 Mbps. Enable BM function.



2) Create a parent channel for P2P limited. And select Applications to 'P2P' and user to 'Users & Manager'



Add Parent Channel

☒ Enabled

Name: P2P Limited

Channel: /

Options

- Channel
- Objects

Channel

Target Line: Line1

☐ Clone this channel to all other lines

Channel Type

☒ Guaranteed channel

Outbound Bandwidth: Min 100 % 30 Mbps

Max 100 % 30 Mbps

Inbound Bandwidth: Min 100 % 30 Mbps

Max 100 % 30 Mbps

Priority: High

☒ Limited channel

Outbound Bandwidth: Max 10 % 3 Mbps

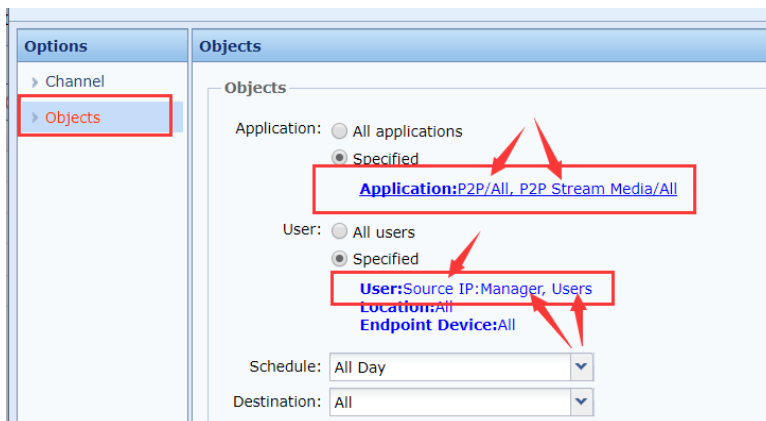
Inbound Bandwidth: Max 10 % 3 Mbps

Priority: Low

☒ Restrain inbound P2P packet loss

☒ Threshold can be exceeded if line is not busy

Settings



Options

- Channel
- Objects

Objects

Application: ☒ All applications

☒ Specified

Application: P2P/All, P2P Stream Media/All

User: ☒ All users

☒ Specified

User: Source IP:Manager, Users

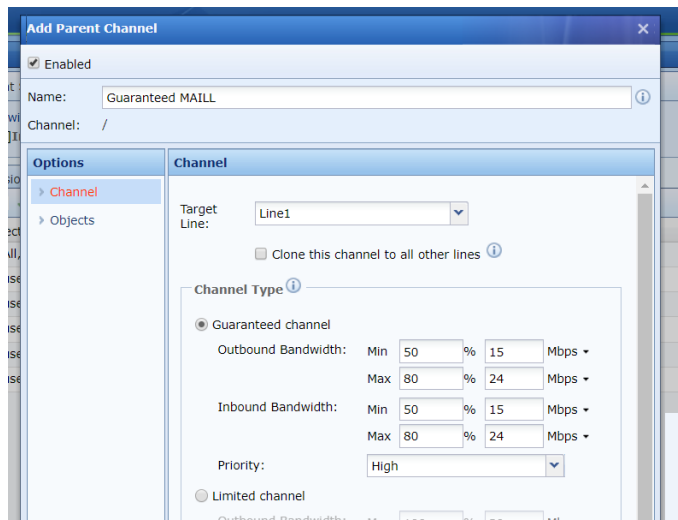
Location: All

Endpoint Device: All

Schedule: All Day

Destination: All

3) Create a parent channel for Mail service.



Add Parent Channel

☒ Enabled

Name: Guaranteed MAILL

Channel: /

Options

- Channel
- Objects

Channel

Target Line: Line1

☐ Clone this channel to all other lines

Channel Type

☒ Guaranteed channel

Outbound Bandwidth: Min 50 % 15 Mbps

Max 80 % 24 Mbps

Inbound Bandwidth: Min 50 % 15 Mbps

Max 80 % 24 Mbps

Priority: High

☐ Limited channel

Outbound Bandwidth: Max 100 % 30 Mbps



☒ Max Bandwidth Per User

Outbound: 2 Mbps

Inbound: 2 Mbps

Advanced

☐ Take every WAN IP as a channel user so that it can share bandwidth with LAN users equally and comply with Max Bandwidth Per User (this is often selected for server providing external service)

OK Cancel

☒ Enabled

Name: Guaranteed MAILL

Channel: /

Options

- Channel
- Objects**

Objects

Application: ☐ All applications ☒ Specified
Application:Mail/All

User: ☐ All users ☒ Specified
User:Source IP:Manager, Users
Location:All
Endpoint Device:All

Schedule: All Day

Destination: All

OK Cancel

7, Scanners

RT Vulnerability Scanner

Realtime Vulnerability Scanner

+ Add - Delete Enable Disable Scan Again Refresh Ad

No.	Name
-----	------

Add

☒ Enable

Name: RealtimeVulnerabilityScanner

Description: Select server ip group

Server Zone: LAN,Management

Network Object: Server IP Group

Save and Add OK Cancel