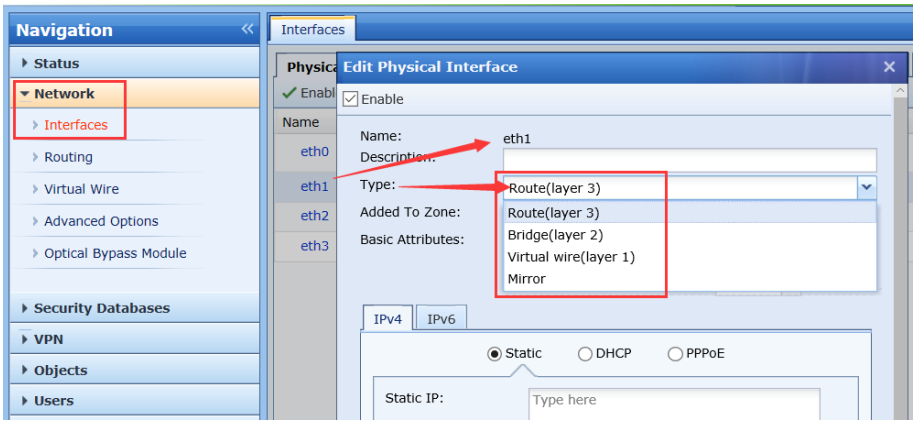
Target

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'.

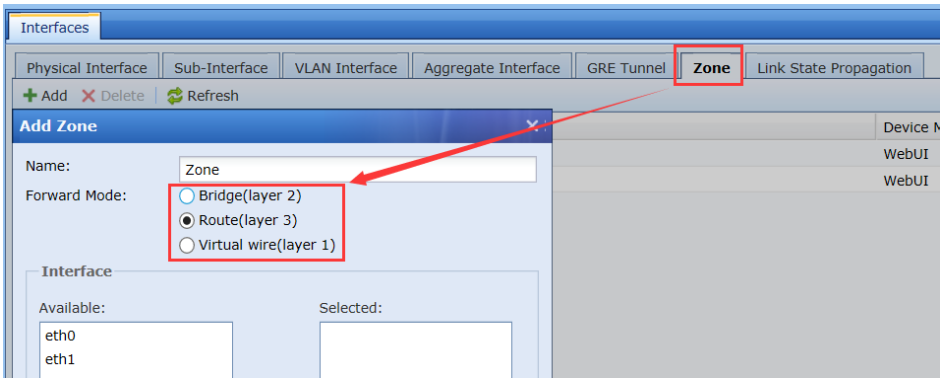
1, Network Deployment

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.

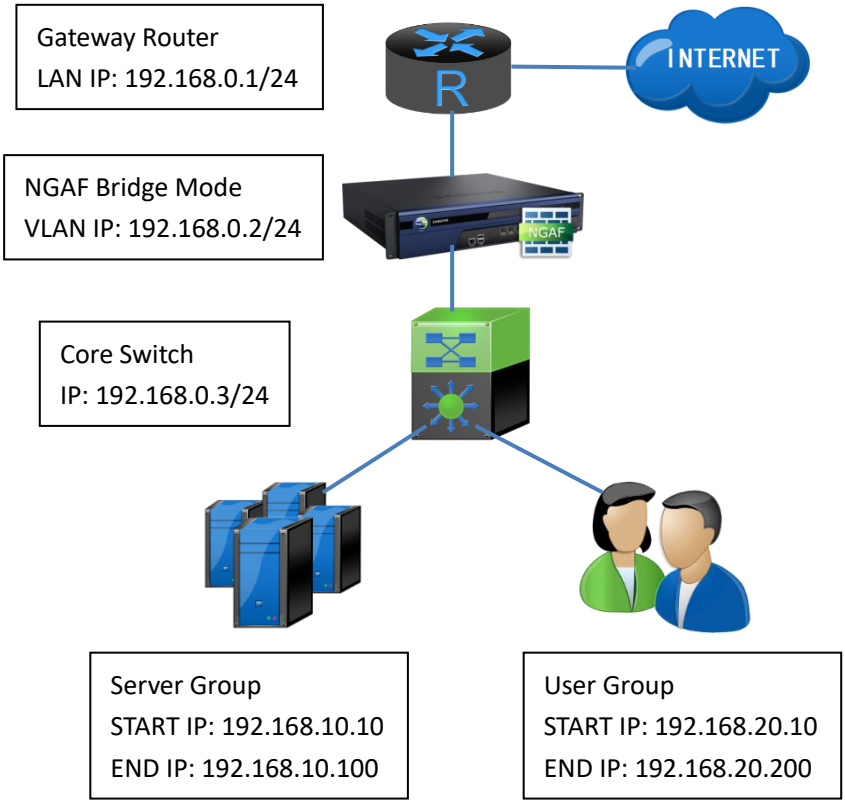


2) Zone

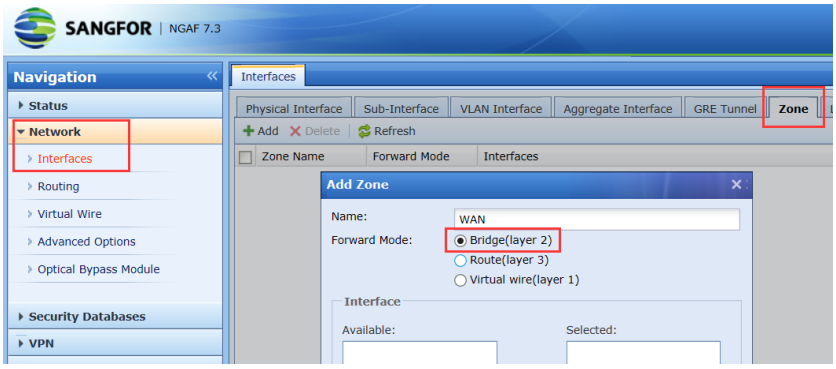
   3 types mode, Bridge mode, Route mode and virtual wire mode. Route mode port only can join to Route mode Zone. Bridge mode only can join to Bridge mode, same to virtual wire.



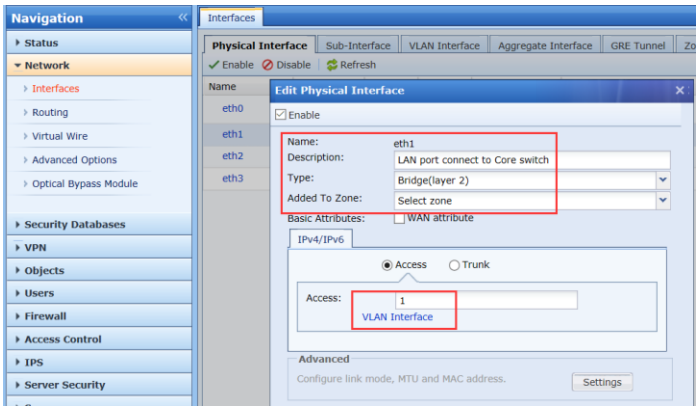
1.1 Bridge Mode Deployment

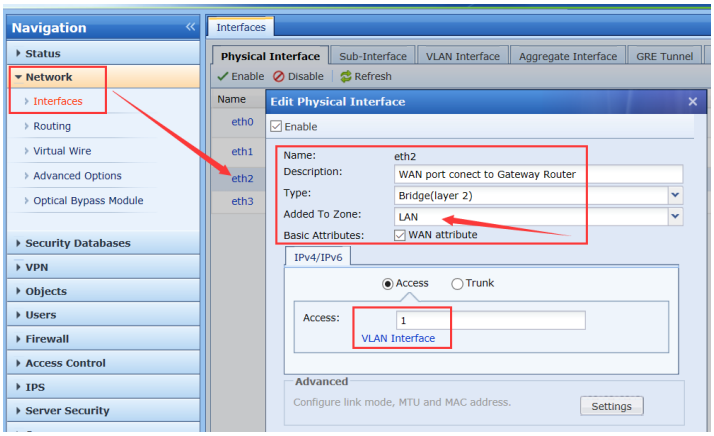


1) Add Zone. WAN Zone and LAN Zone.

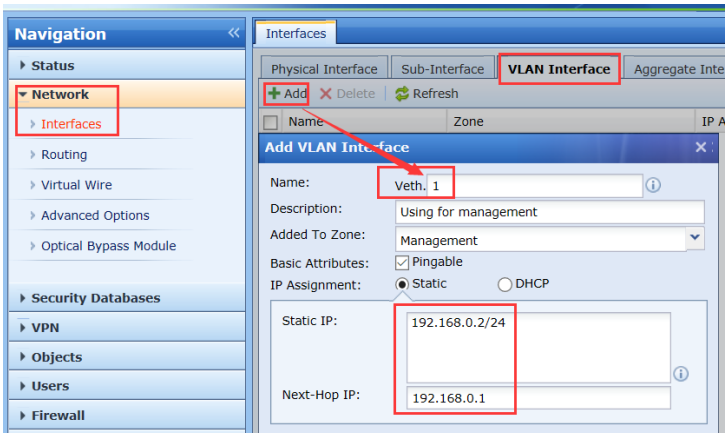


2) Configure interface. Eth1 to LAN port, eth2 to WAN port.

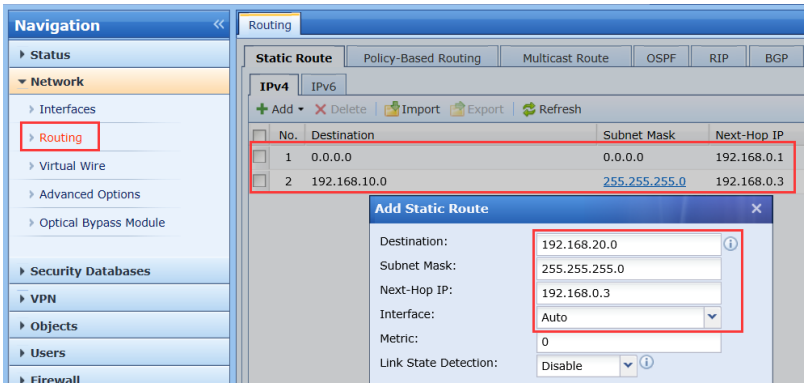




And create a vlan interface, set a ip address to this vlan interface which is used for NGAF management.

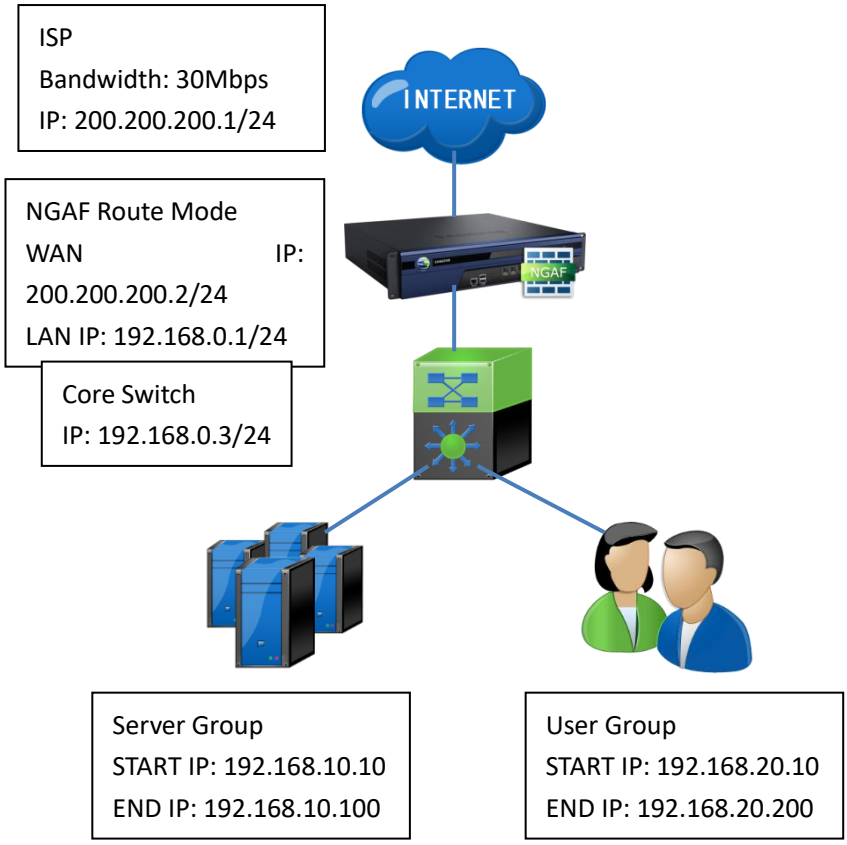


3) Route, in this case, we need add 3 static routes, default route and 2 return routes.

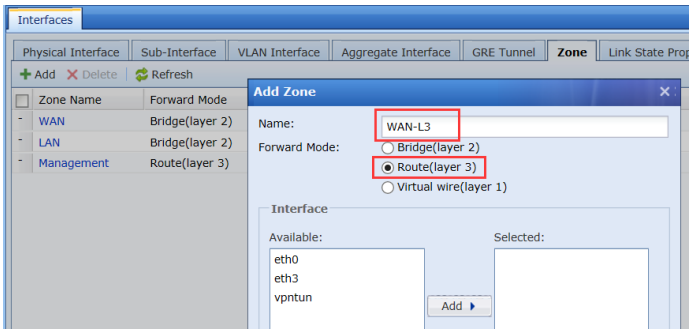


4) One more important thing, NGAF blocks all data forwarding by default, so we need add a Access Control policy to allow some legal visit.

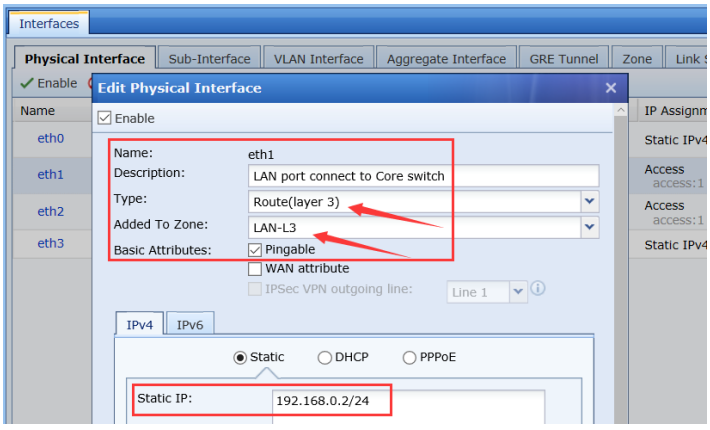
1.2 Route Mode Deployment

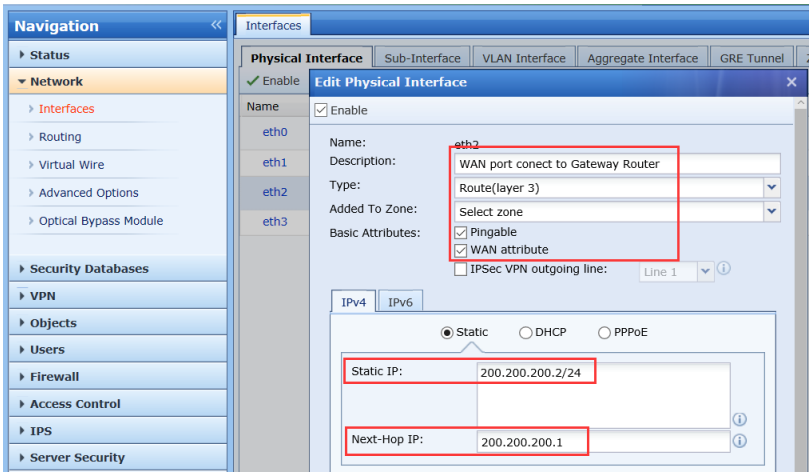


1) Add Zone. WAN Zone and LAN Zone.

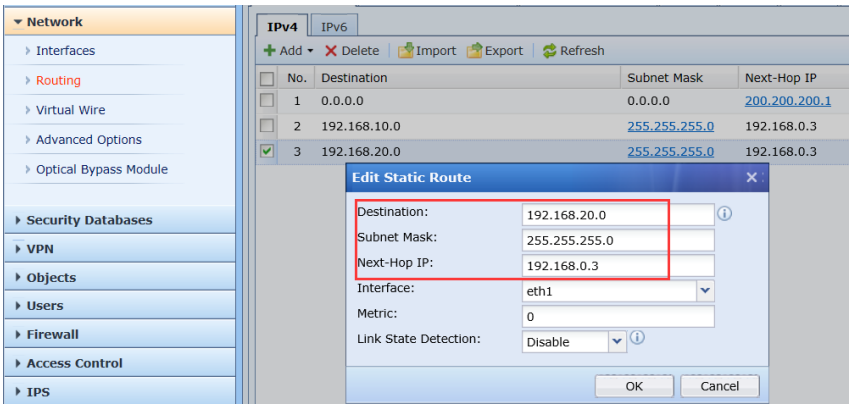


2) Configure interface. Eth1 to LAN port, eth2 to WAN port.

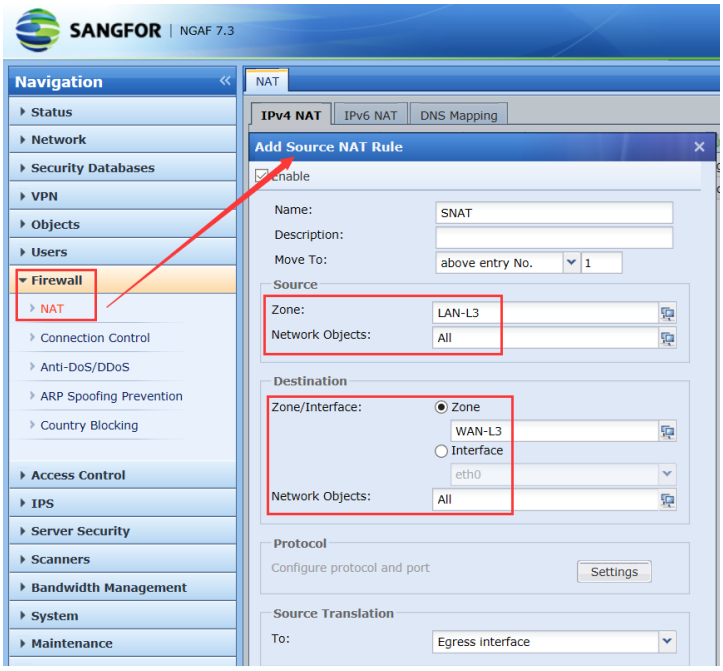




3) Route, in this case, we need add 3 static routes, default route and 2 return routes.



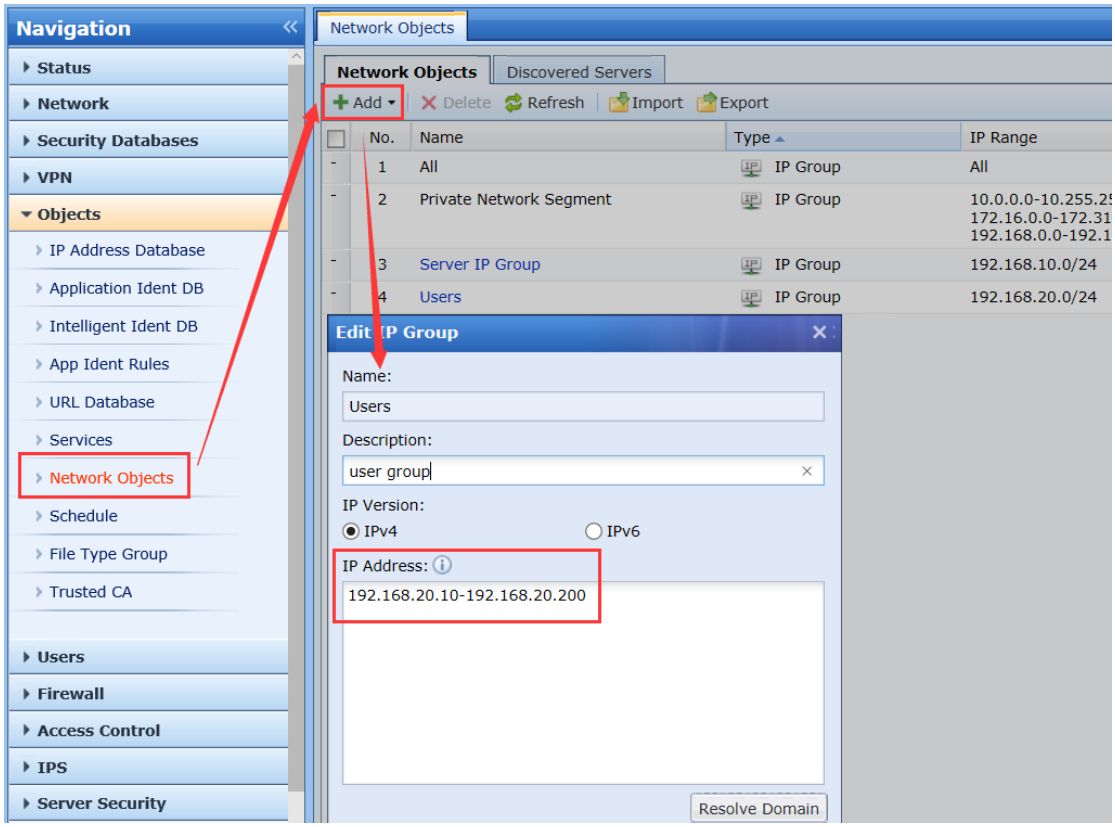
4) Configure Source NAT.



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.

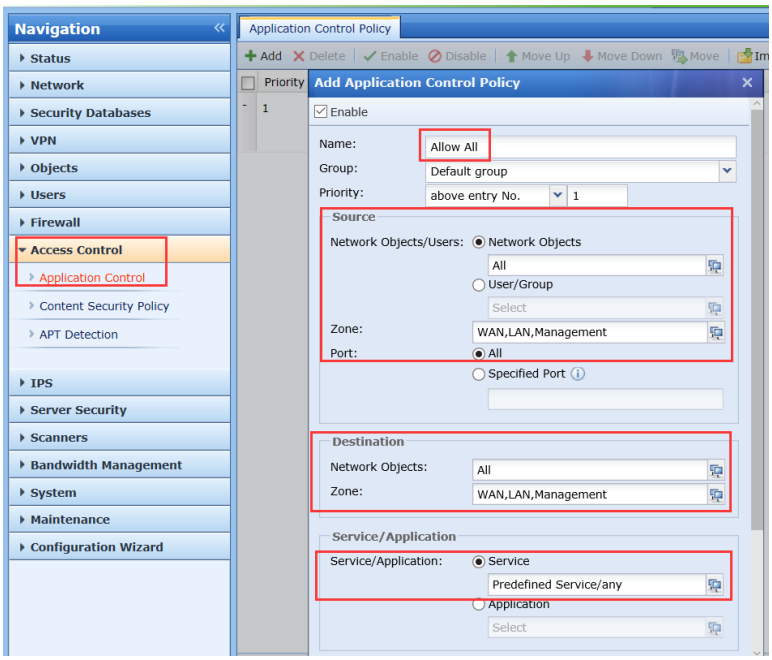
2, Objects

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



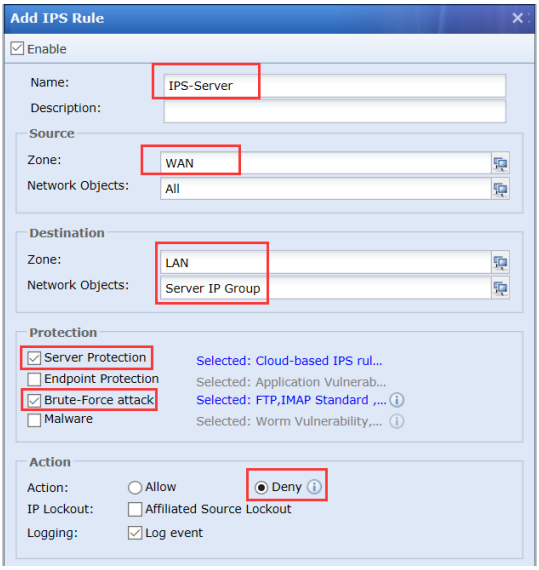
3, Access Control

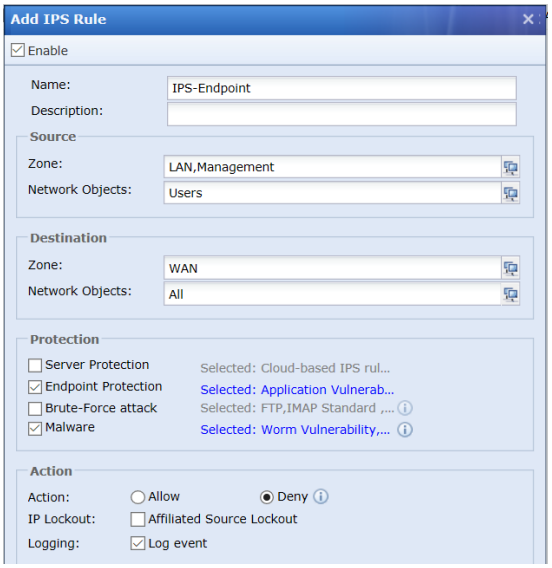
Path: Access Control-> Application Control



4, IPS

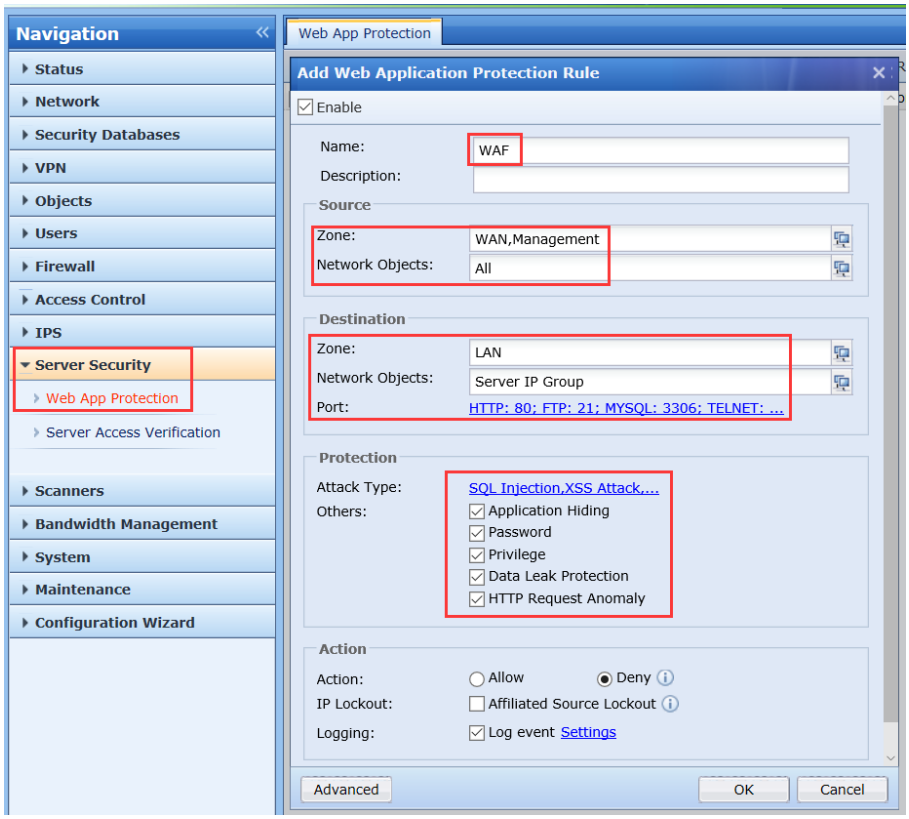
IPS policy can protect server and endpoint. So we can add 2 policies, 1 for server, 1 for endpoint.





5, Server Security

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

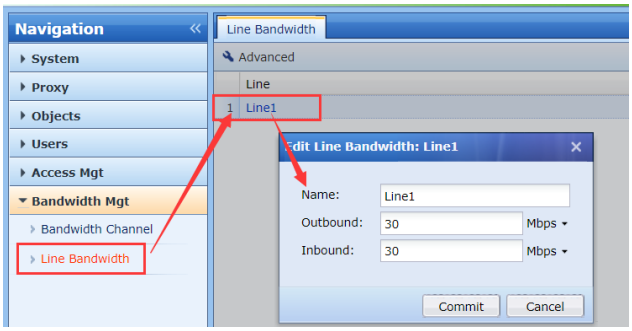


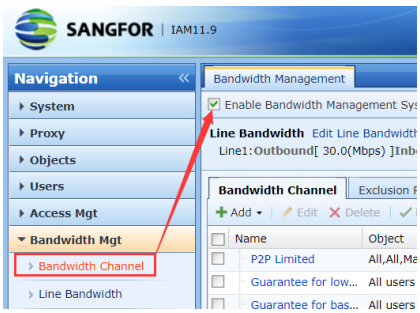
6, Bandwidth Management

• All P2P applications' traffic can't more than 10% of total bandwidth.

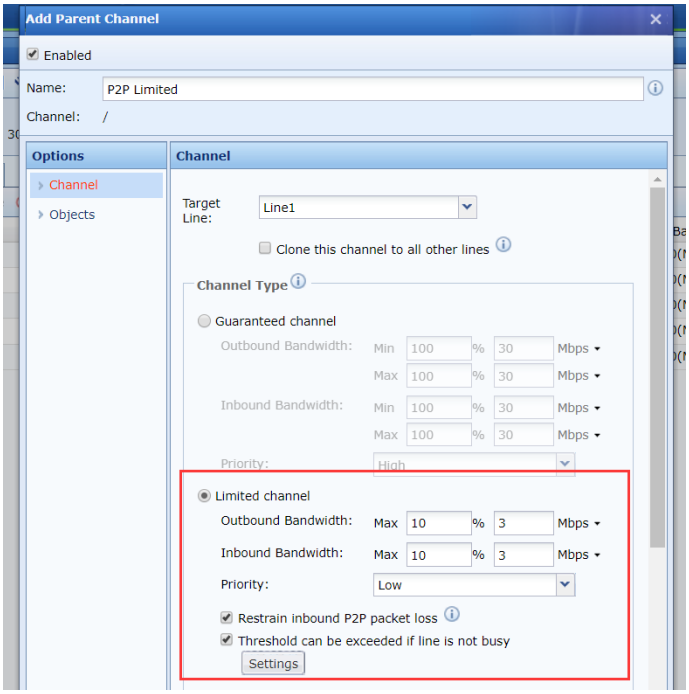
• Create a Guaranteed channel for Mall service at least 50% of the total bandwidth, but per user cannot more than 2 Mbps/s.

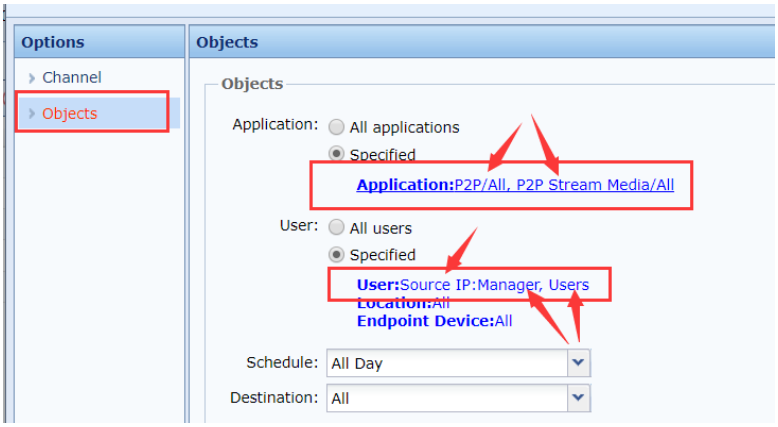
1) Define the total bandwidth. In this case, the bandwidth is 30 Mbps. Enable BM function.



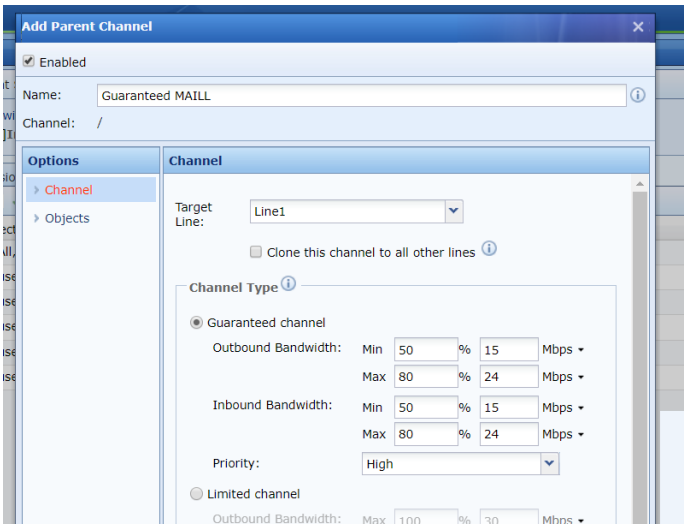


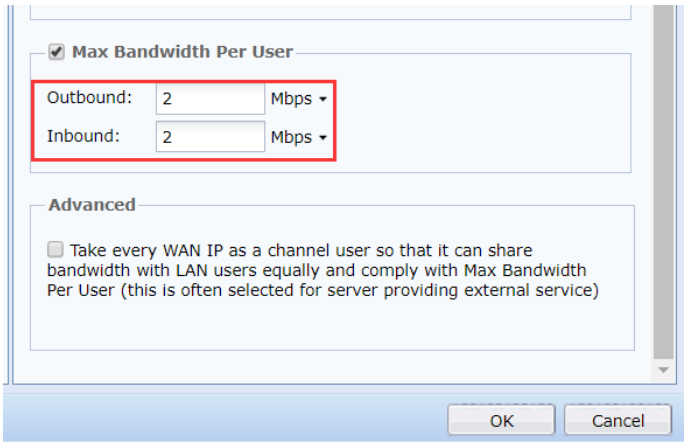
2) Create a parent channel for P2P limited. And select Applications to 'P2P' and user to 'Users & Manager'

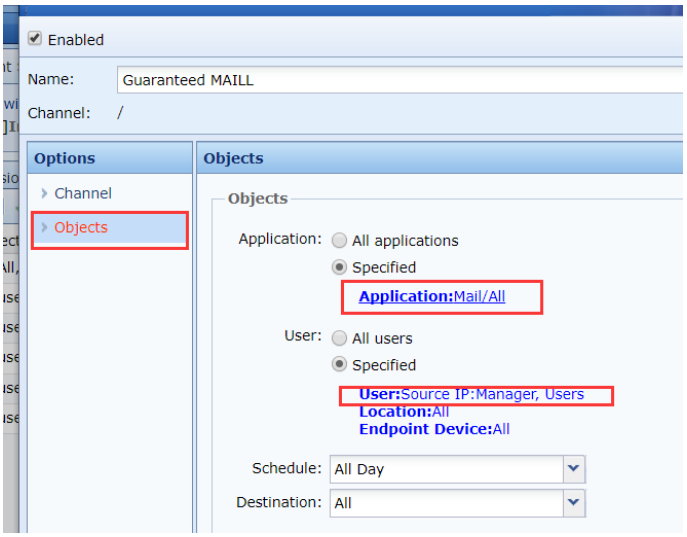




3) Create a parent channel for Mail service.







7, Scanners

RT Vulnerability Scanner