Network Secure Platform 8.0.85

New Version Technical Training

By John.Qiao

Contents

Chapter	Training Contents	Training Objective
1	Overview About Network Secure Platform	Understand what the Network Secure Platform is
2	Main Features Difference(Compared to 8.0.47 version)	Understand the main existing functional differences compared to old platform NGAF(8.0.47 version)
3	New Features About Network Secure Platform	Understand the new features compared to the old platform by Network Secure Platform
4	Permanently Deleted Features(Compared to 8.0.47 version)	Understand the permanent deletion function for old platform in the new architecture, which will not be supported in the future.

PART 1

Overview About Network Secure Platform

General Introduction

- Network Secure Platform is not a new product, it is still NGAF product, but it uses the new platform and it also modify the name from the perspective of marketing.
- In following pages, there will mention the old platform NGAF for times, which can be understood those NGAF 8.0.47 and below version.
- At present, old platform NGAF cannot be ugraded to Network Secure Platform.

Why needs Network Secure Platform

The current OS of the old platform NGAF is facing difficulties.

Gateway-type products are upgraded and updated with a slow pace

- Each product line uses a separate OS system without a unified OS platform, which makes it difficult to reuse many product capabilities.
- The R&D teams of each product line have to do repetitive development work at the OS level, resulting in low product development efficiency.

Some features not supported by old platform NGAF

- old platform NGAF does not support hardware virtualization due to the old OS architecture, and some projects are unable to participate.
- old platform NGAF does not support BFD protocol due to the old OS architecture
- old platform NGAF supports a maximum of 32 “business port + management port” combinations, which results that some projects are unable to participate...

The reliability of the old platform NGAF is low

- The high difficulty in debugging the kernel architecture, which limits the stability improvement of the product, and which also limits its ability for product extension.

The Benefits of the Network Secure Platform

Network Secure Platform uses the excellent Sangfor OS operating system, based on a multi-core parallel processing architecture and DPDK technology, to maintain high processing performance even under complex network traffic after enabling multiple security functions. At the same time, the Sangfor OS operating system implements independent operation of the security detection plane and network forwarding plane, ensuring that NGAF remain stable and reliable even in extreme and special application scenarios.。

Complete some common product features

After applying Sangfor OS to NGAF product, hardware that is not supported by the old platform NGAf can be virtualized into several NGAFs, dual-machine BFD, out-of-band management, and some IPv6 features can all be achieved, eliminating obvious shortcomings in competing projects

Product performance improvement

After applying Sangfor OS, NGAF network layer small packet throughput, new connection count, IPSec VPN and other performance indicators have significantly improved. This can reduce business costs and adapt to more special application scenarios.

Providing a unified and shared underlying platform

Our company's central platform department is responsible for the development and maintenance of the general Sangfor OS, while the NGAF product line focuses on the development of specialized features to improve product evolution and hardware adaptation efficiency.

Product reliability is higher

Sangfor OS adopts an architecture decoupling and flat separation design, and provides core process hot backup and product overload protection, greatly improving product reliability.

What are the differences in configuration between the new architecture and the old platform?

The Challenges of Network Secure Platformin Delivery

Differences in configuration between Network Secure Platform and old platform NGAF

What specific features have been added to Network Secure Platform

Some features from previous old platform NGAF are deleted and cannot be found in Network Secure Platform

Unfamiliar with Network Secure Platform web pages

PART 2

Main Feature Difference (compared to 8.0.47 version)

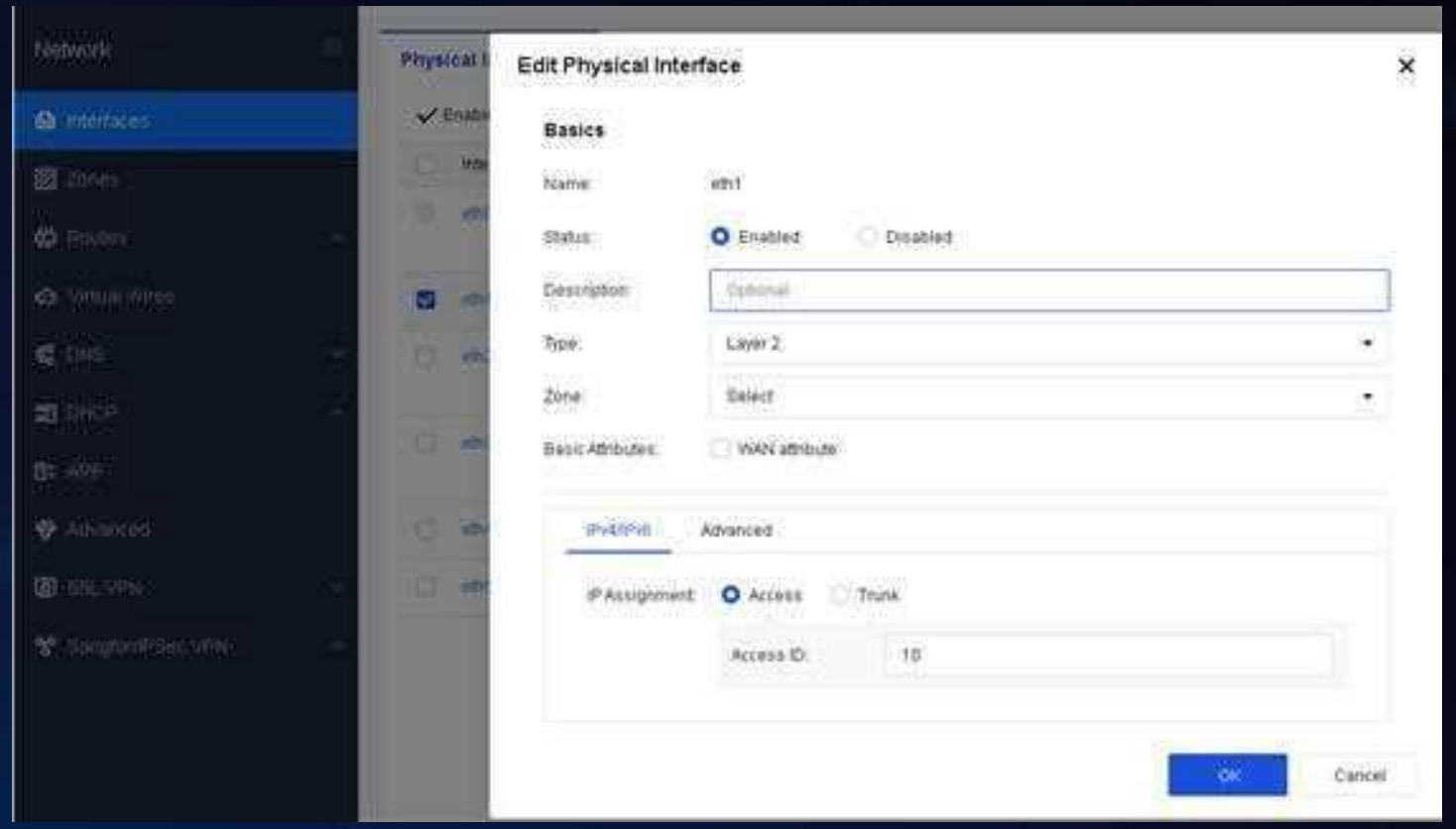
Layer-2 Port-ACCESS Type Port Processing Logic

Old platform NGAF processing method:

- If the ACCESS VLAN is 10, then regardless of whether the received packet carries a VLAN tag with VLAN10 or not, NGAF will process it both.

Network Secure Platform processing method:

- If the ACCESS VLAN is 10 and the received packet carries a VLAN tag with VLAN10, NGAF will directly discard it. NGAF only processes packets that do not carry a VLAN tag.



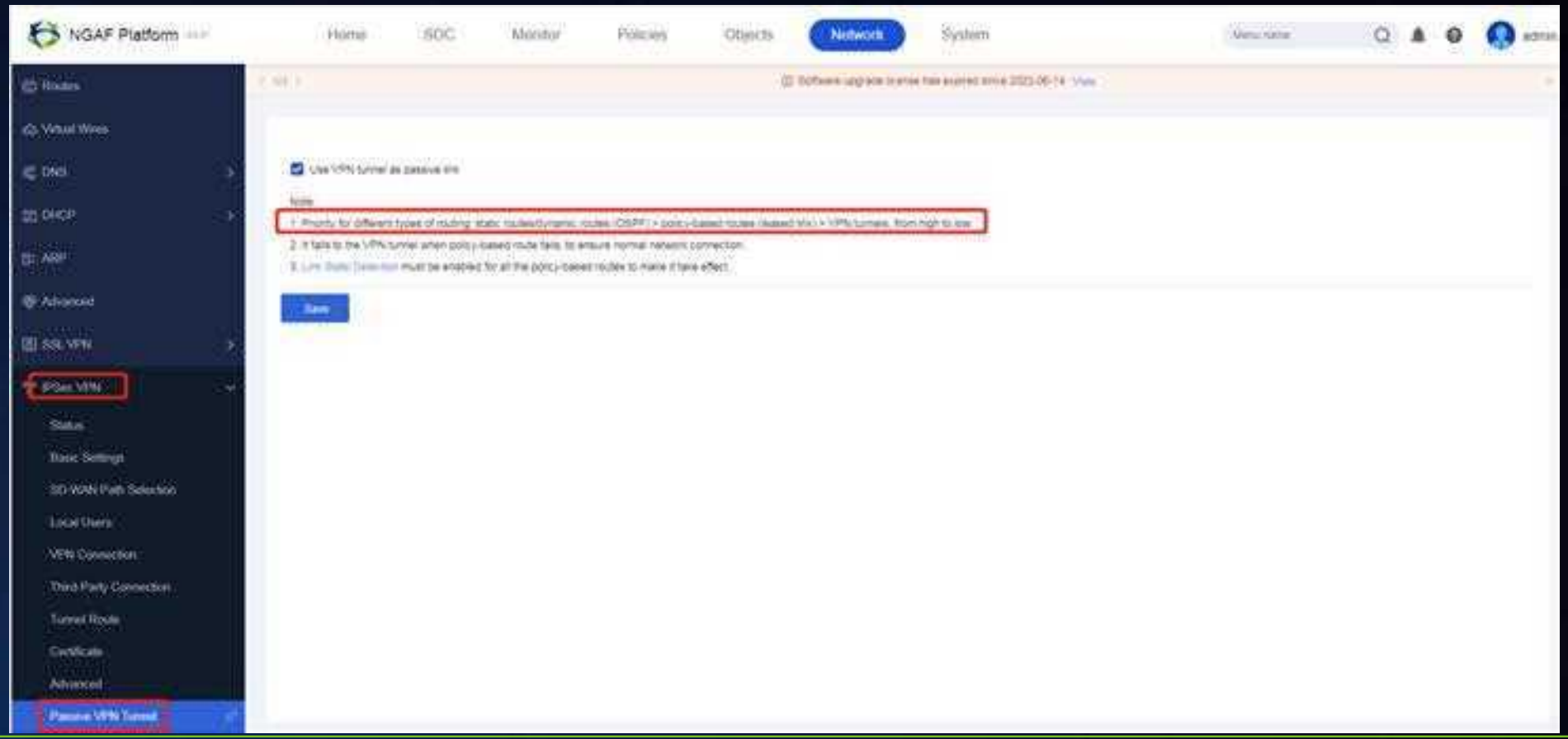
Route Types Priority---Old Platform NGAF

Situation 1: Default route types priority

SSL VPN Route > VPN Route > Static, Direct Route > Dynamic Route > Policy-based Route > Default Route

Situation 2: After enabling VPN tunnel as passive

SSL VPN Route > Static, Direct Route > Dynamic Route > Policy-based Route > VPN Route > Default Route



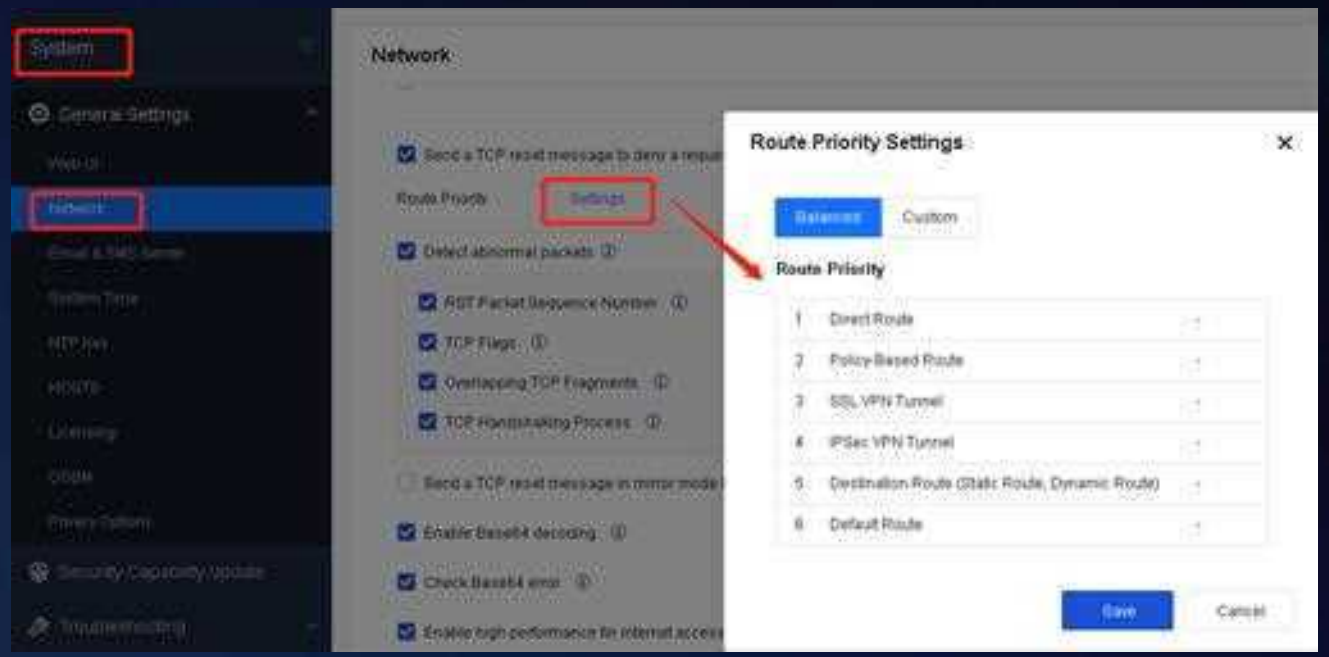
Route Types Priority---Network Secure Platform

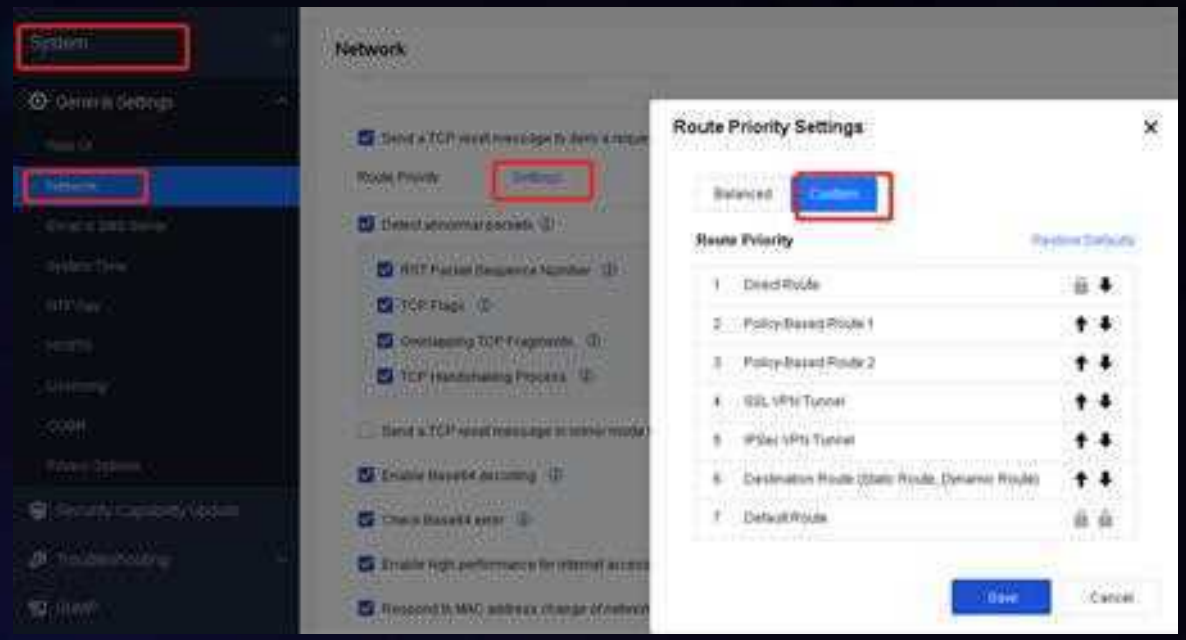
Situation 1: Default route types priority

Direct Route > Policy-based Route > SSL VPN Route > VPN Route > Static, Dynamic Route > Default Route

Situation 2: Custom the route types priority as you need

The switch for enabling VPU tunnel as passive link has been removed, and a custom mode has been added,policy-based route is devided into 2 types which represent 2 route tables, per table can support up to 256 route items. Policy-Based Policy 2 is met for route expansion scenario.



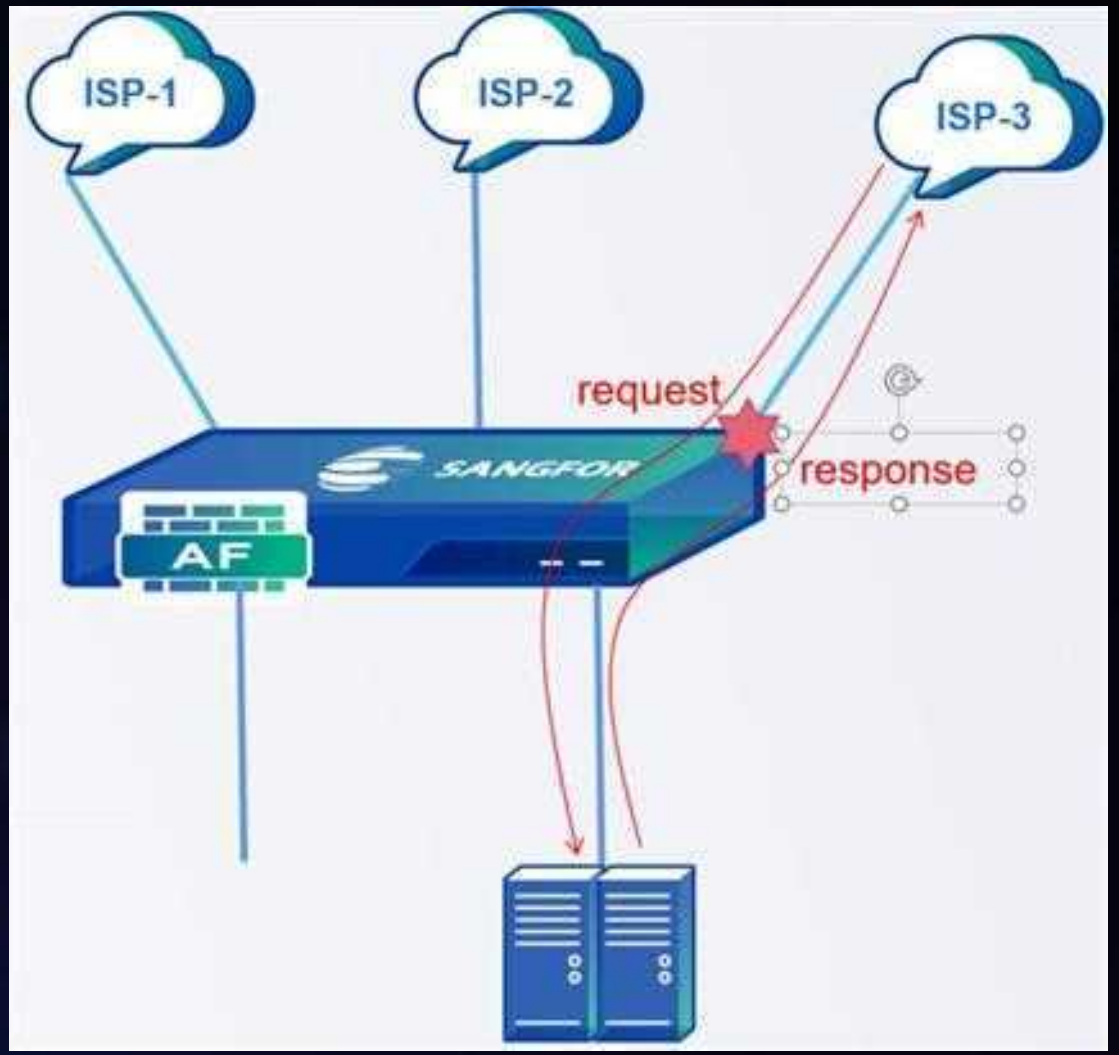


Reverse Routing---Old Platform NGAF

There is no a function switch to turn on or off the routing reverse in old platform NGAF as it it related to interface configuration as well as policy-based routing. Two conditions should be met.

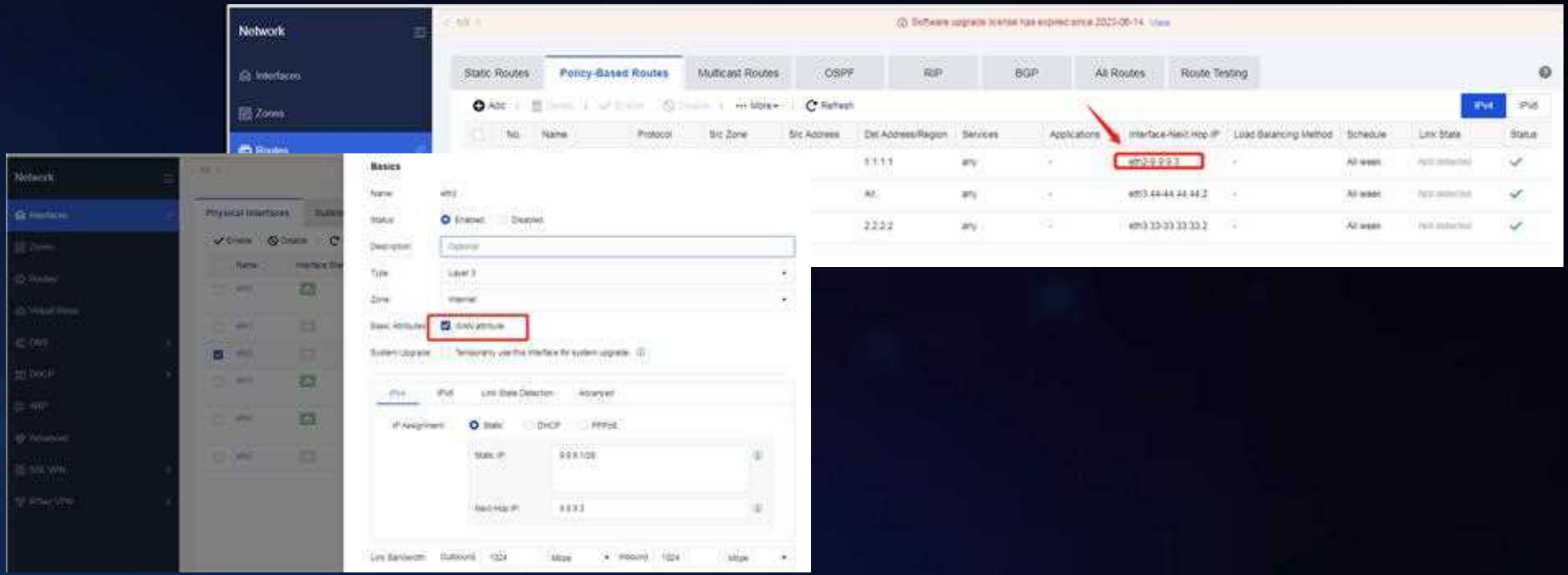
A. **The inbound interface must have the "WAN" attribute. (inbound interface concept: such as the interface connecting ISP-3 line**;

B. **There must be policy-based routes (the source and destination IP ranges do not matter, but the next hop interface of the policy-based routes must include the inbound interface);**



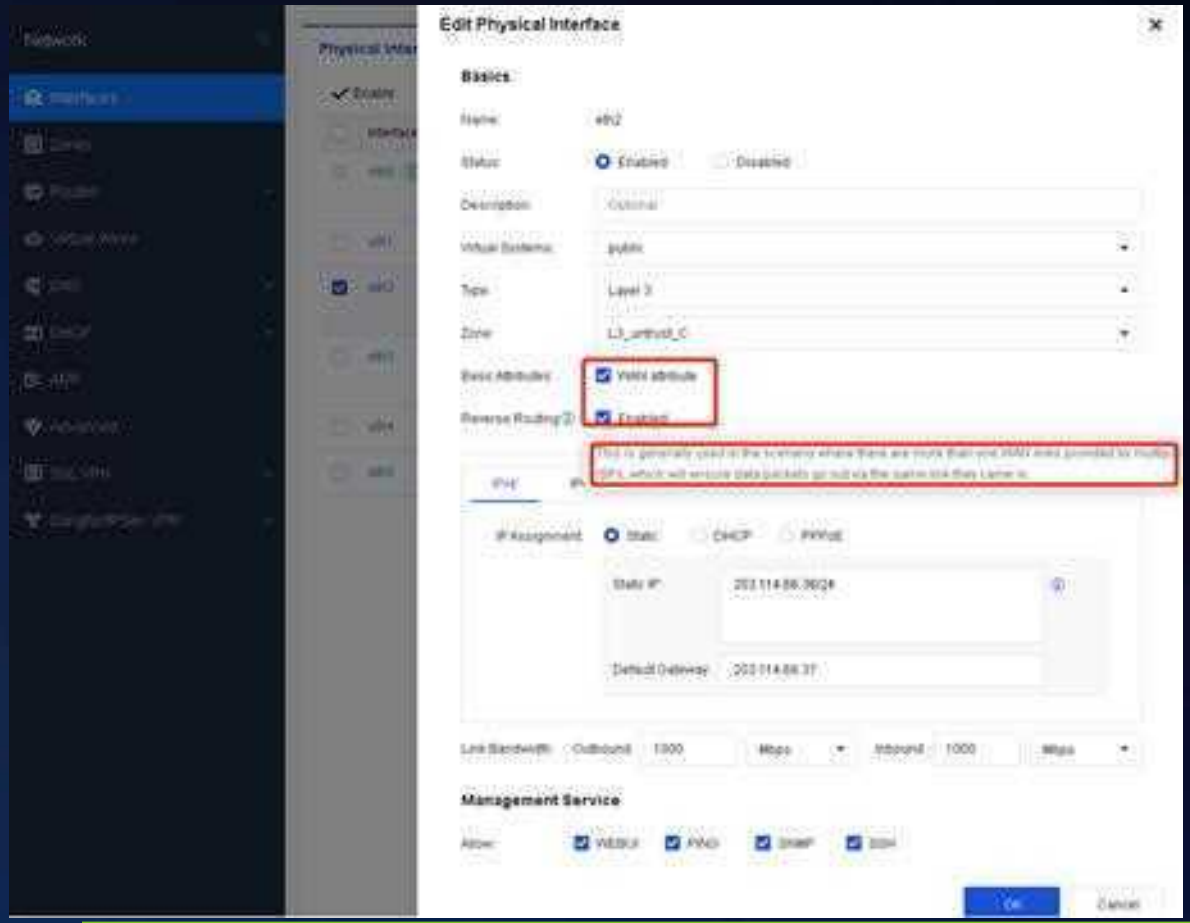
Reverse Routing---Old Platform NGAF

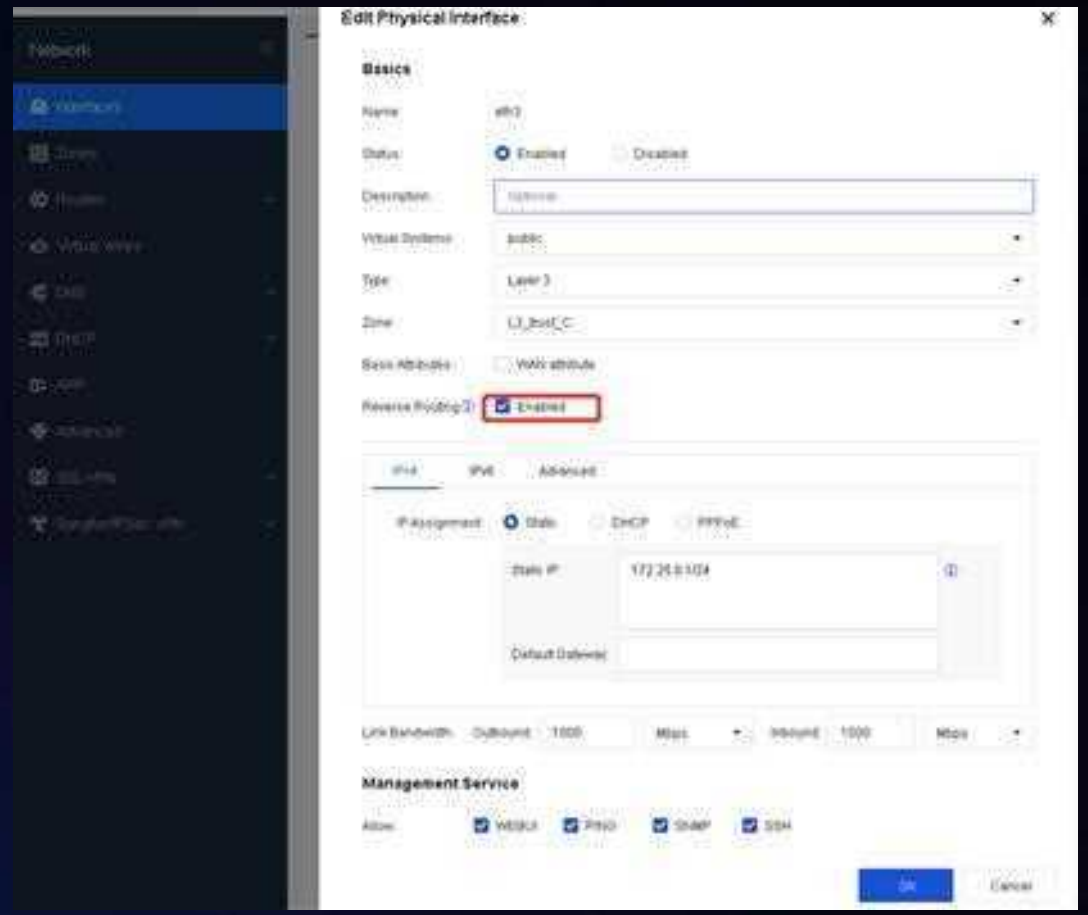
For example: the below diagram shows that eth2 interface has turn on the reverse routing feature. Do not pay much attention about policy-based routes as long as its interface is eth2, no relationship with zones, source addresses, and destination addresses.



Reverse Routing---Network Secure Platform

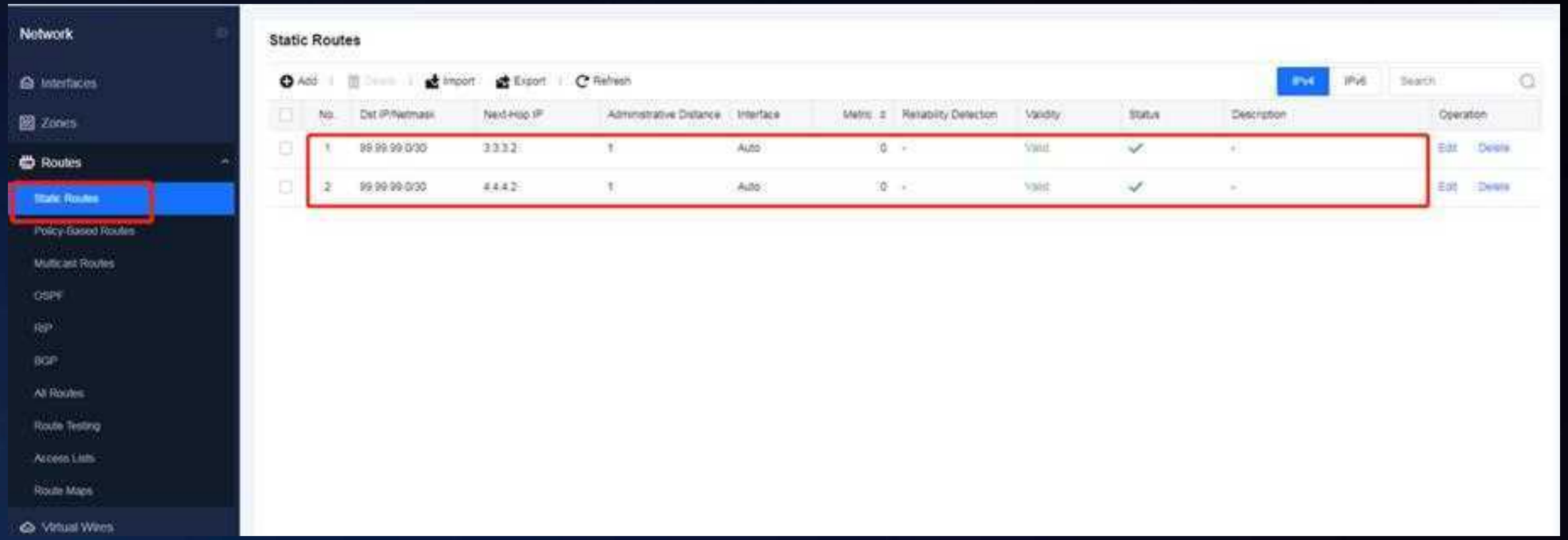
The reverse routing of the Network Secure Platform is only related to the interface. If a reverse routing is configured on the interface, the data packet will maintain its source input and output regardless of other configurations. When there are multiple ISP lines on the external network that require port mapping, the corresponding interface must be selected for routing reverse . When selecting the WAN attributes, routing reverse will be selected automatically, while for internal interfaces you can select it in manaual.





Equal Route---Network Secure Platform

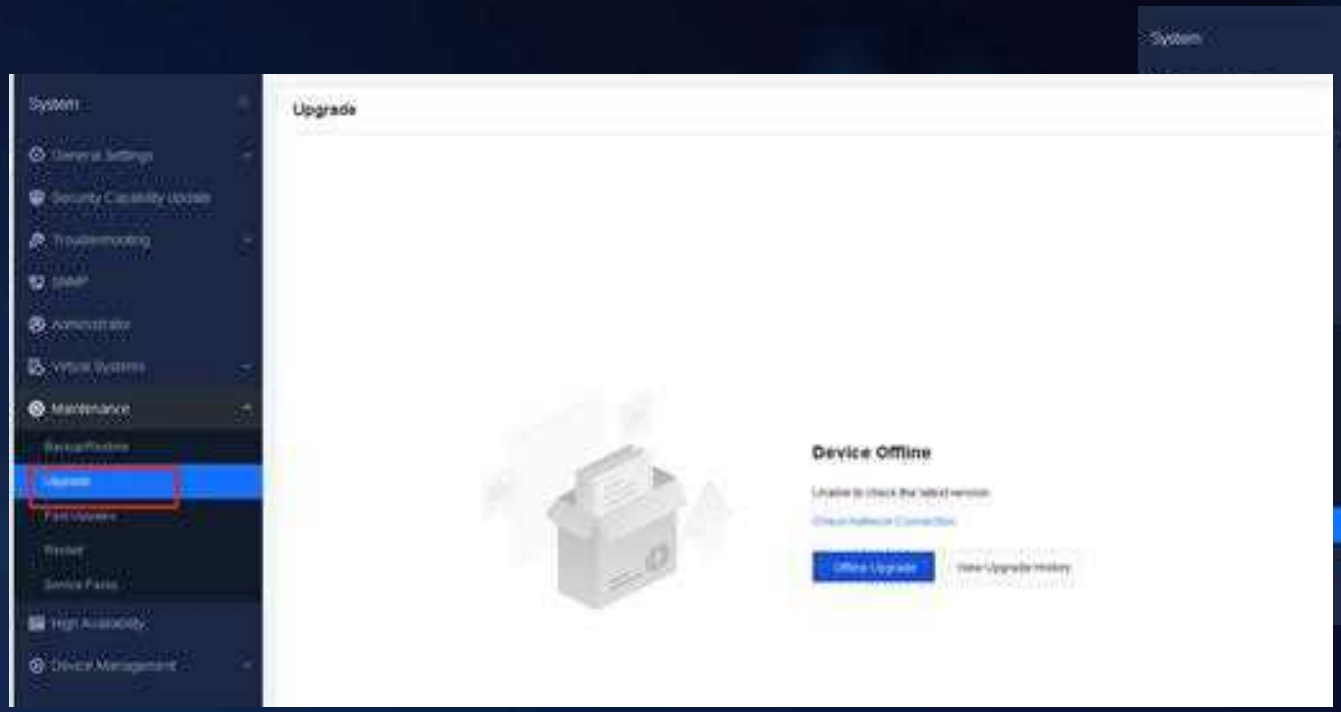
The Network Secure Platform supports for equivalent routes with the configuration of same destination network and metric value, and it forward packets in different routes based on the source and destination IP address hash algorithm.



Upgrade---Network Secure Platform

The Network Secure Platform no longer supports the upgrading client to upgrades new versions. Only webpage method is supported for upgrades, and the upgrade package is in *.bin format. In addition to upgrade new version, this change also applies to packages and service pack(SP) upgrades. After the upgrade is completed, it will not automatically restart.

You can manually restart it at a suitable time on the webpage to enter the upgraded version, but before you restart it you can not make other configurations and the security detection function will not work temporarily as well.

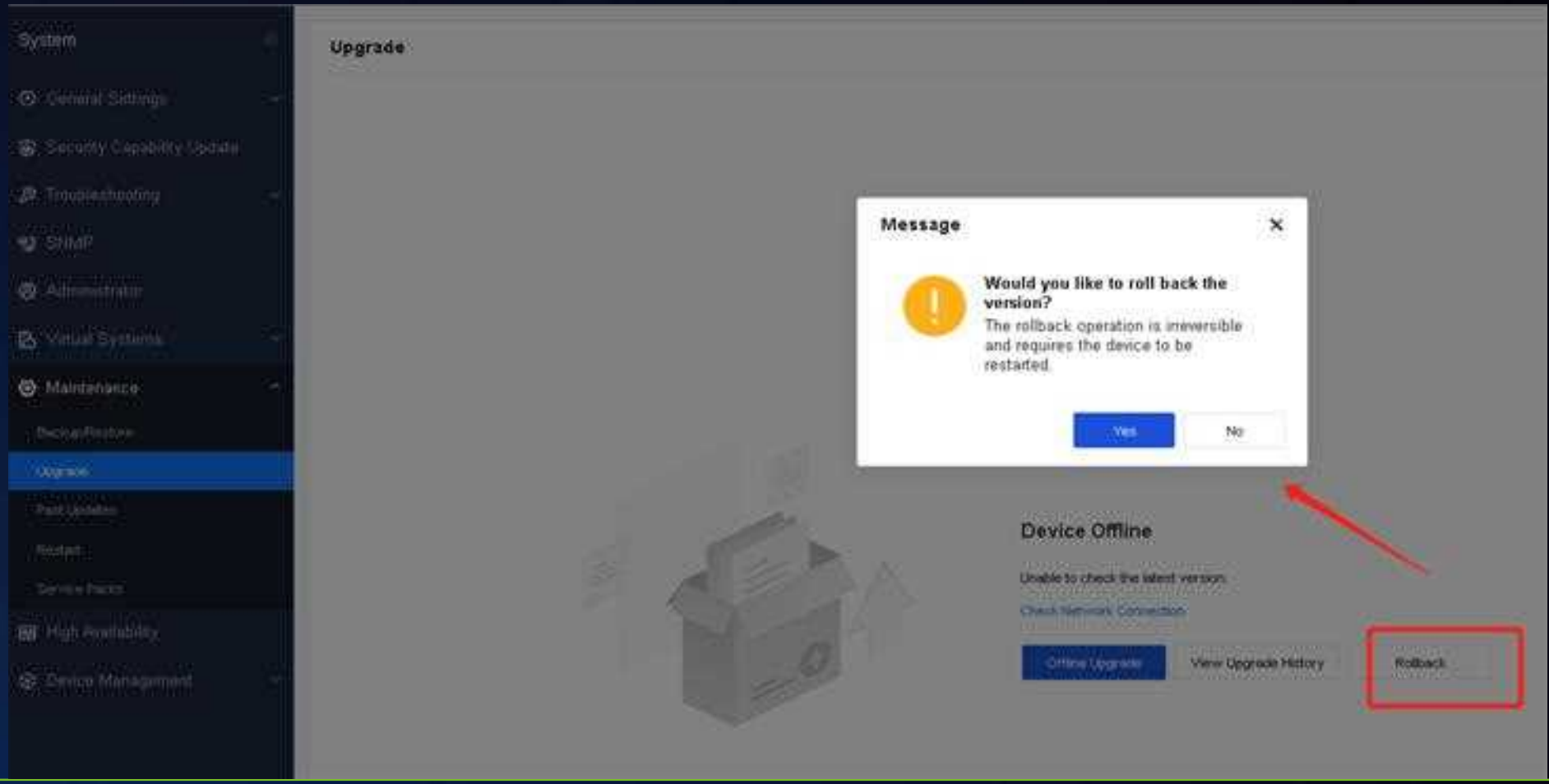


Upgrade---Network Secure Platform

- It is unnecessary to stop and separate the high availiability configuration in active/standby mode when you plan to upgrade the system version, compared to the old platform NGAF. You are instructed to upgrade the standby device firstly, and then perform the switchover, and then upgrade the new standby device(previous active device);
- It will not restart the device if you just upgrade service packs, while it may restart some certain services in backend autobatically which depends on specific service packs.

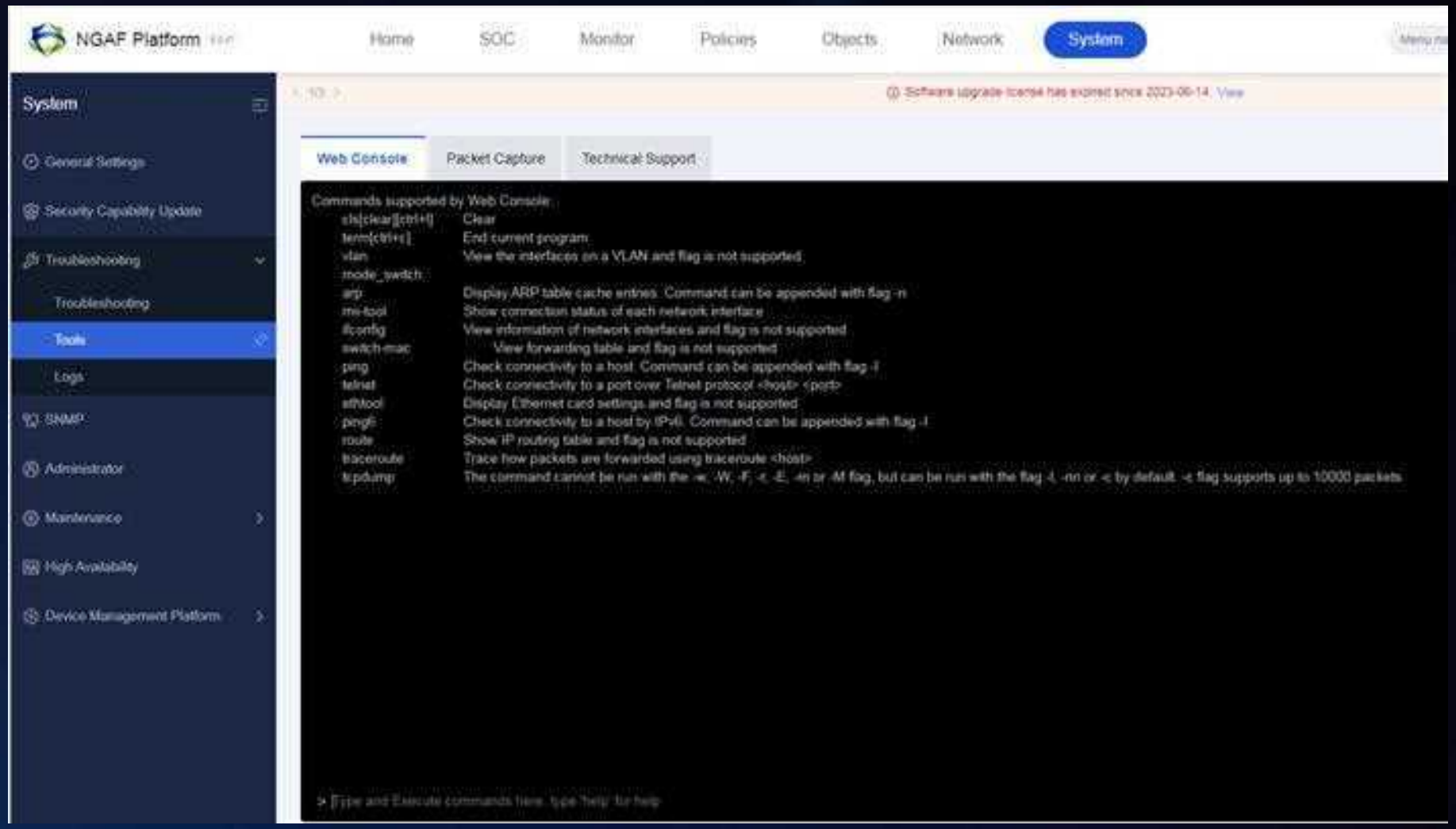
Rollback---Network Secure Platform

The Network Secure Platform supports version and service pack rollback, allowing you to roll back to the previous version or service pack before the upgrade was completed. Any configurations made on the new version or service pack will be cleared. After you perform version or service pack rollback, the configuration in old version is the same with the moment before you perform upgrade.



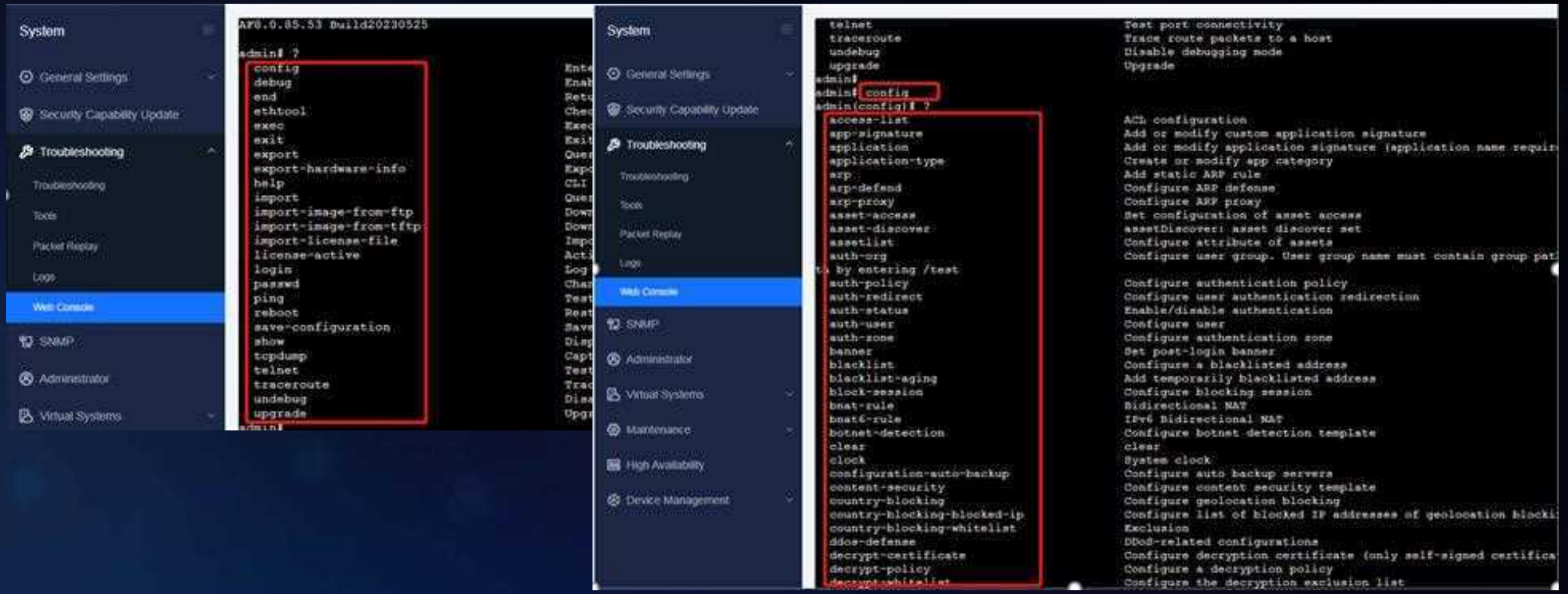
Web Console---Old Platform NGAF

The old platform NGAF only support several common commands, see as below.



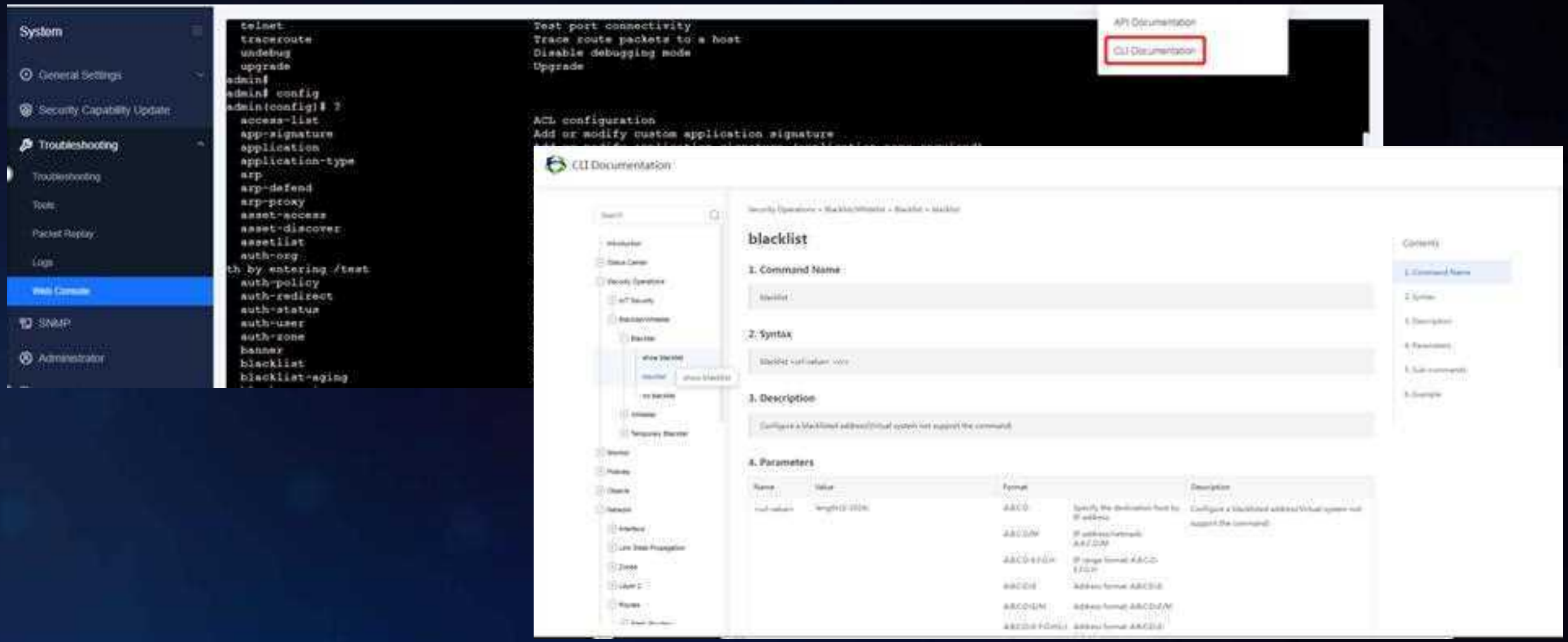
Web Console---Network Secure Platform

Network Secure Platform web console supports much more commands for configuring and viewing operations, besides the command lines is login-free.



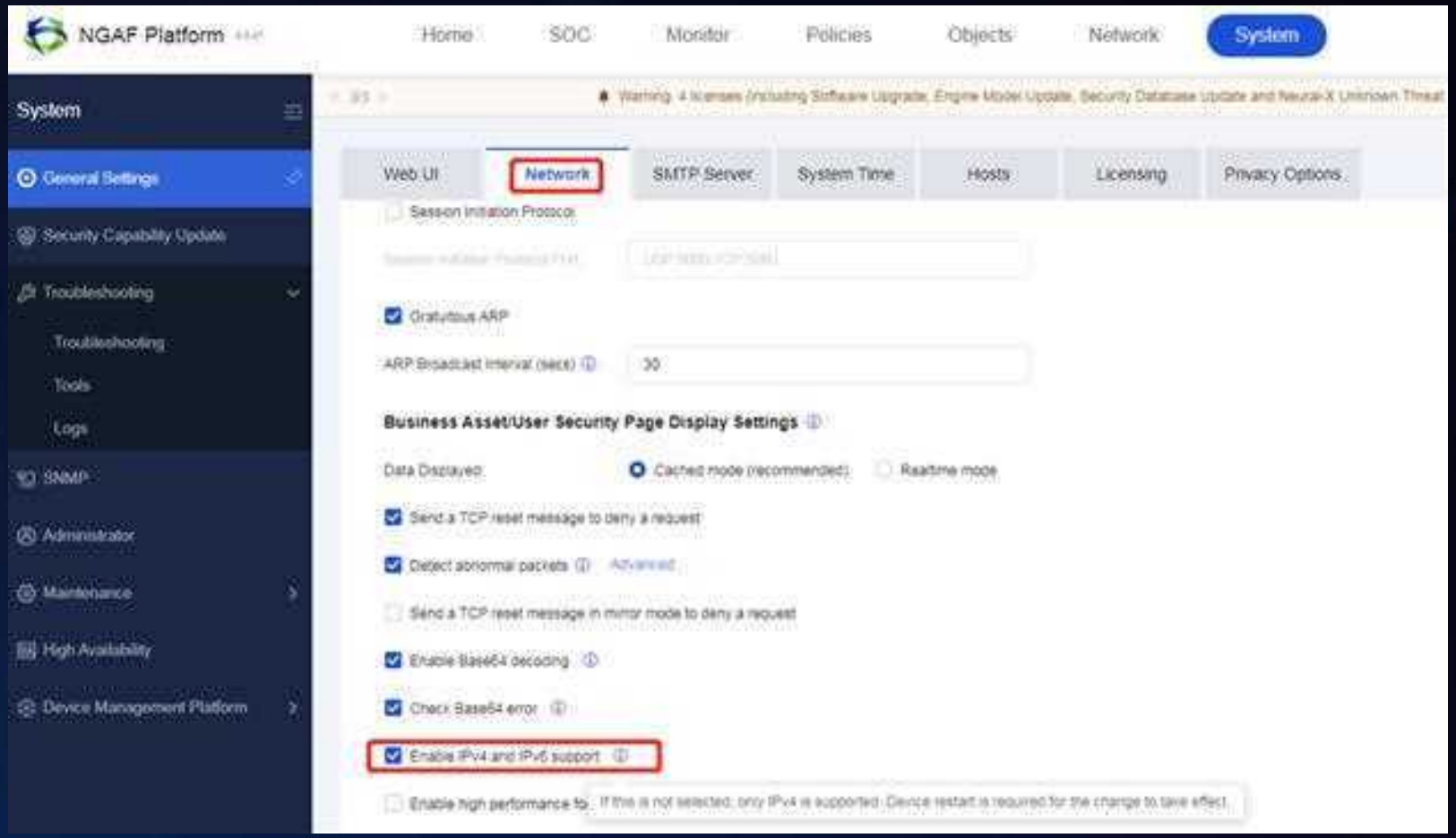
Web Console---Network Secure Platform

For more command lines instruction, you can refer to the CLI Document in the right top.



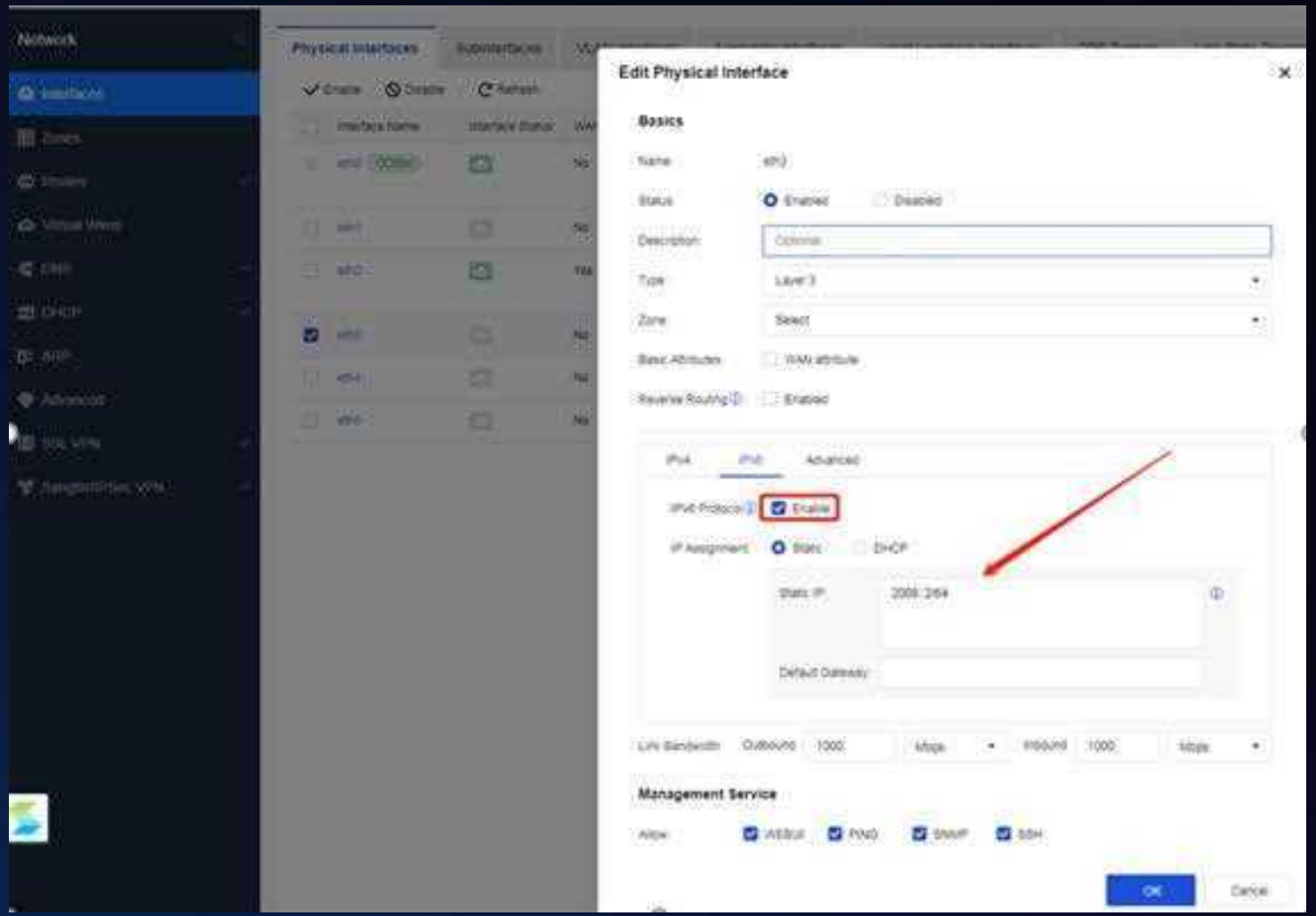
IPv6 Feature---Old Platform NGAF

To support IPv6 on old platform NGAF, firstly it is necessary to enable the “Enable IPv4 and IPv6 support” feature in the network parameters which will cause to restart the device, and then configure IPv6 content in corresponding interfaces.



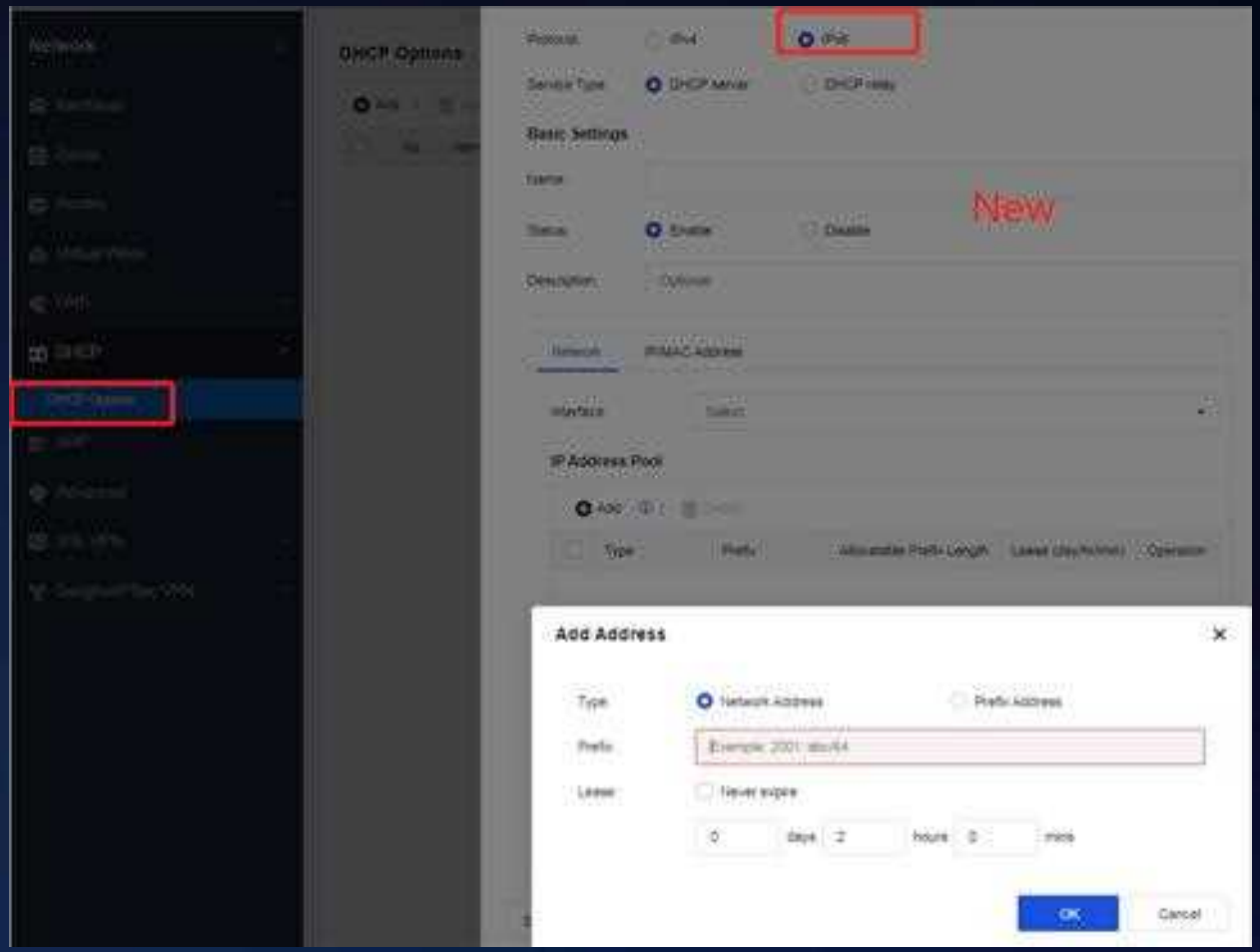
IPv6 Feature---Network Secure Platform

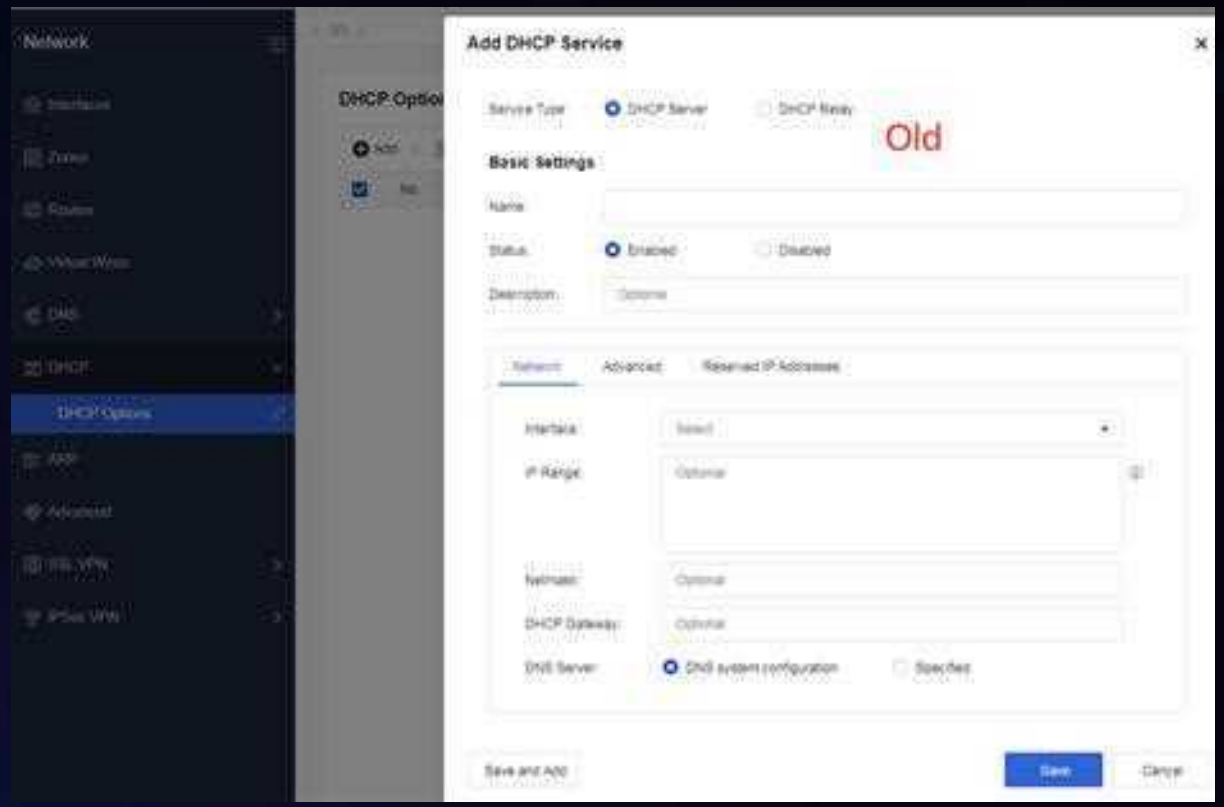
The Network Secure Platform supports IPv6 feature without other extra settings. This feature can be directly configured in the interface without restarting the device.



IPv6 Feature in DHCP Server Module

Network Secure Platform supports IPv6 DHCP server, and the old platform NGAF does not.





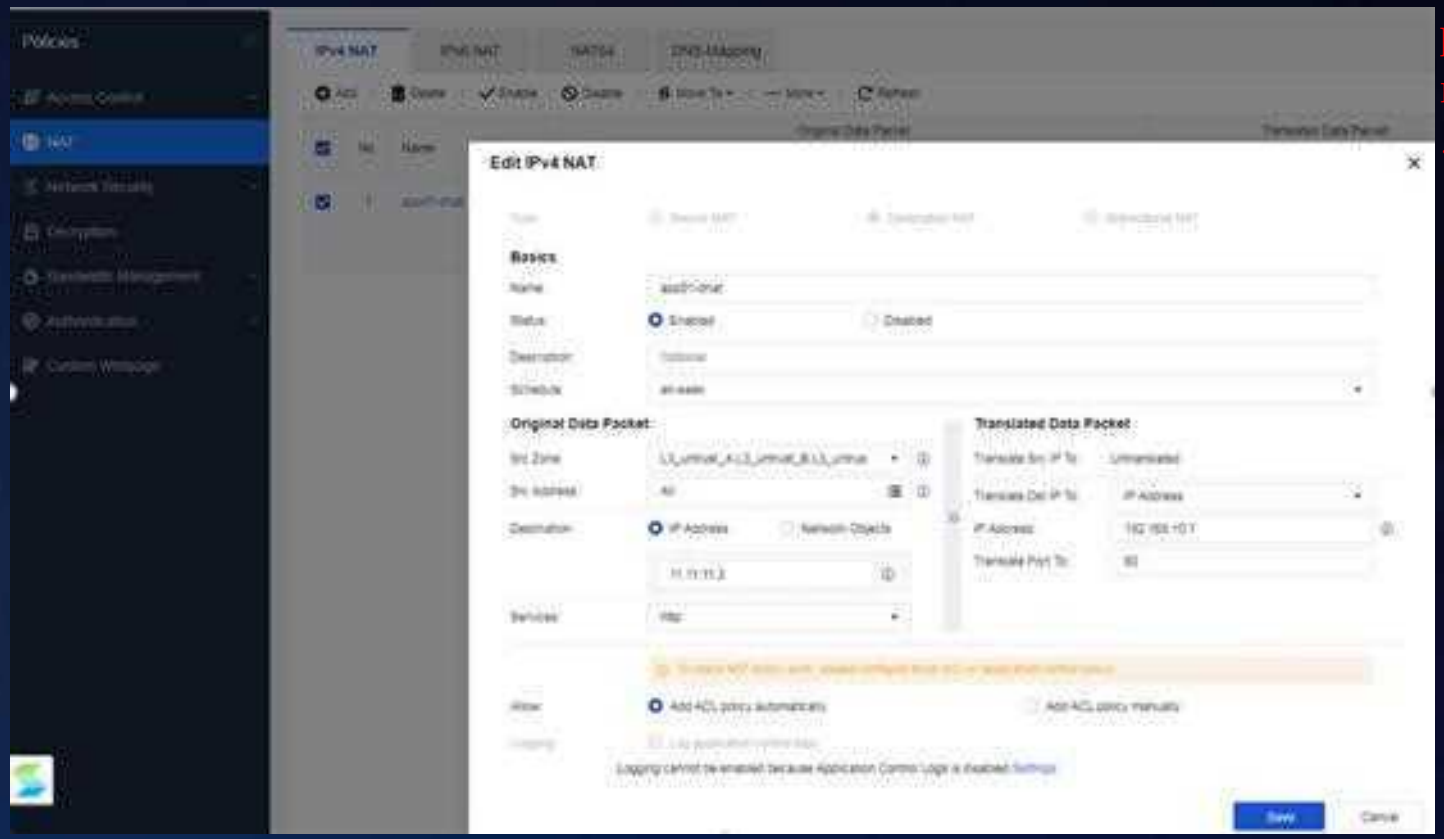
IPv6 Feature Support Scope---Network Secure Platform

Module	Sub Function	Supporting Specification
Network	Interface	support physical interfaces, sub-interfaces, vlan interfaces, and aggregate interfaces
	Route	support static route and policy-based route under IPv6, support OSPFv3 and BGP4+ dynamic routing.
	DNS proxy	support
	DHCP	support
	GRE Tunnel	support IPv6 over IPv4
	IPv4/v6 Dual Protocal Stack	support
NAT	NAT	support NAT64, NAT46, and NAT66
Access Control	ACL	support application control, geolocation blocking and connection control under IPv6.
Network Security	Bandwidth Management	support
	Intrusion Prevention	support
	Anti-virus	support
	URL Filtering	support
	Web App Firewall	support

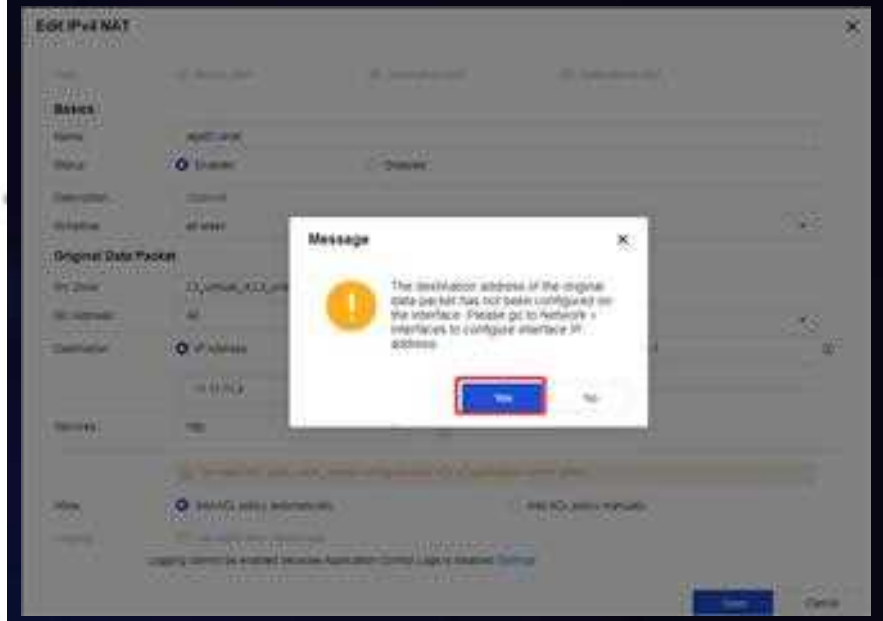
DNAT---Network Secure Platform

For the old platform NGAF, the destination IP of DNAT needs to be configured on the interface to take effect, otherwise it will not respond to ARP requests.

For **Network Secure Platform, destination IP of DNAT does not need to be** configured on the interface. It is already a resource pool in DNAT and will automatically perform ARP proxy to response the ARP requests for IP addresses of the DNAT section.

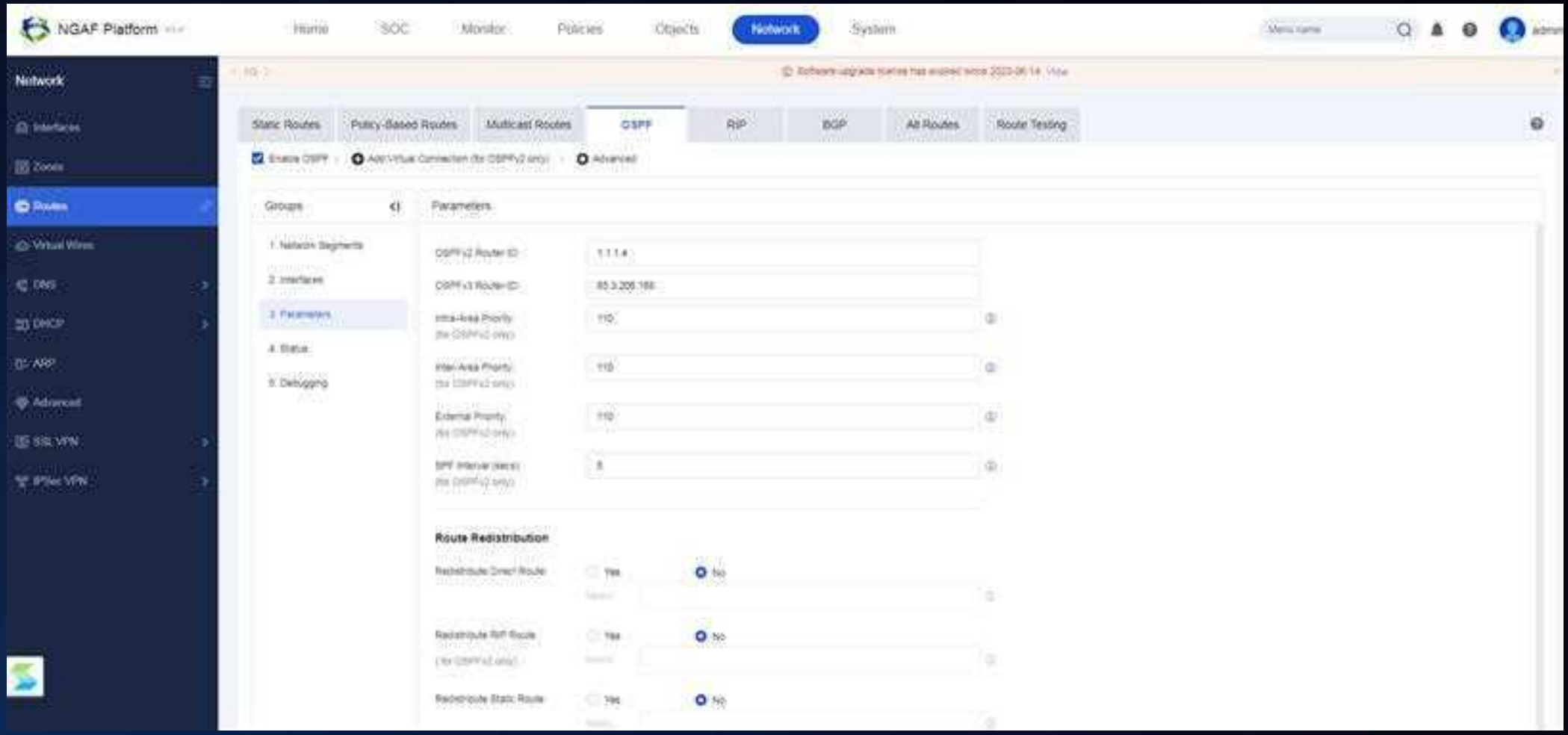


However, you probably will encounter the notifying message below before you save it, just click 'Yes' and ignore it.



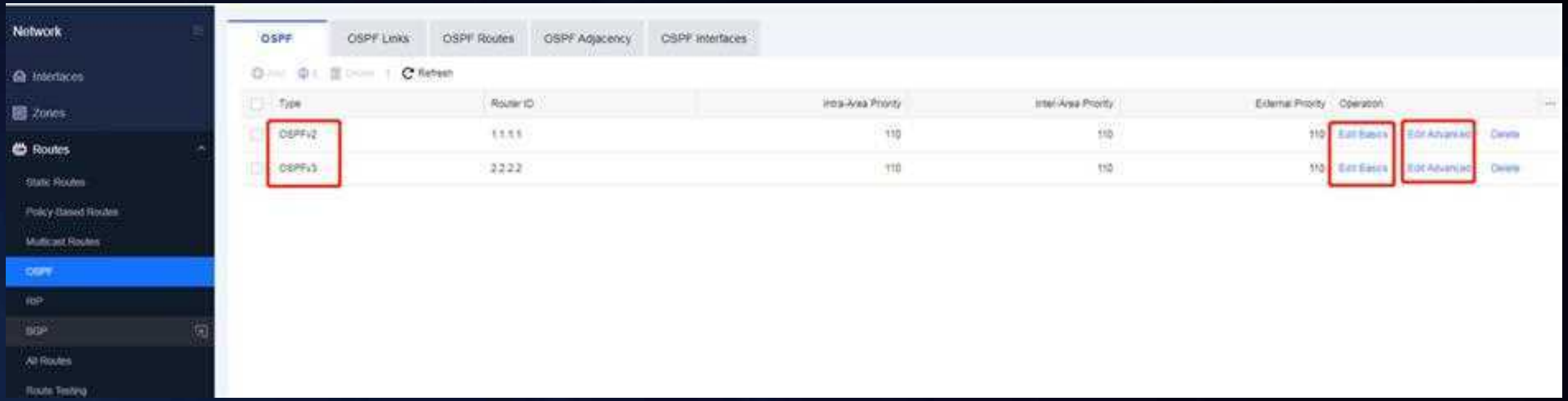
OSPF---Old Platform NGAF

In the old platform NGAF, OSPF dynamic routing feature, v2 and v3 are configured together. The route redistribution supports directly connected routes, RIP routes, static routes and default routes. However, it does not support some features such as OSPF BFD and OSPF GR.



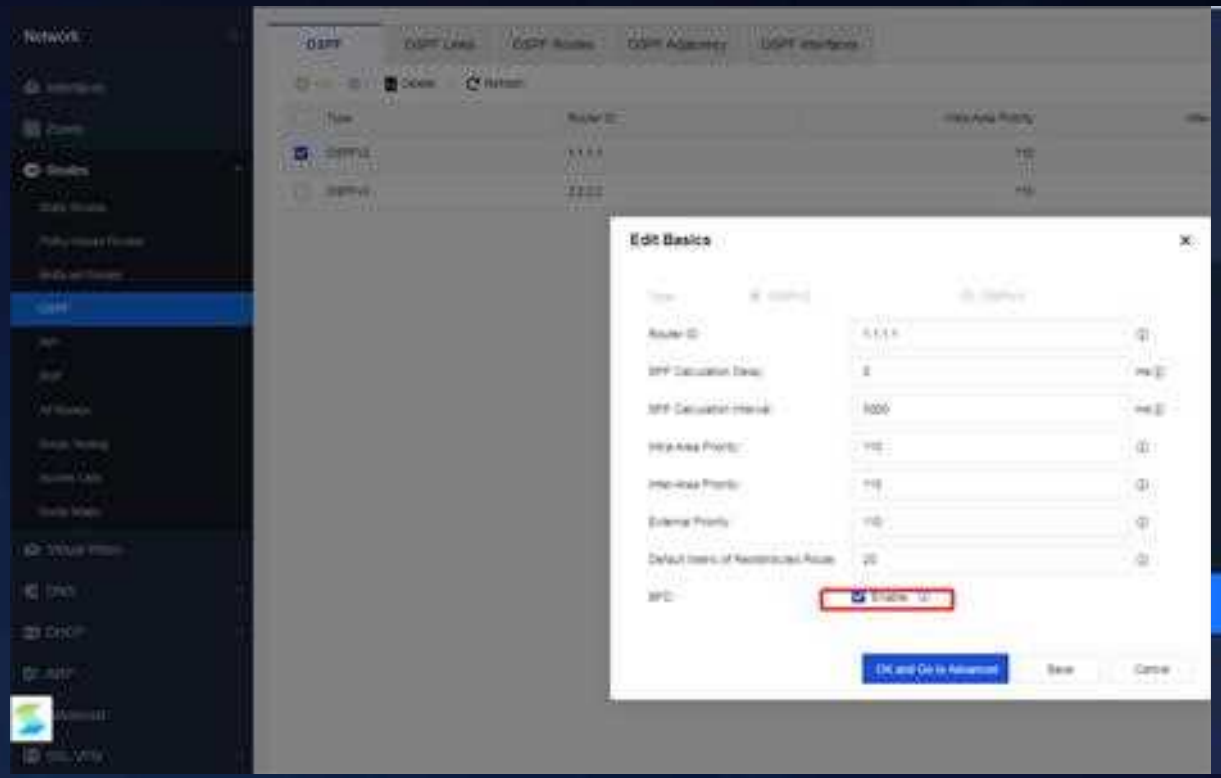
OSPF---Network Secure Platform

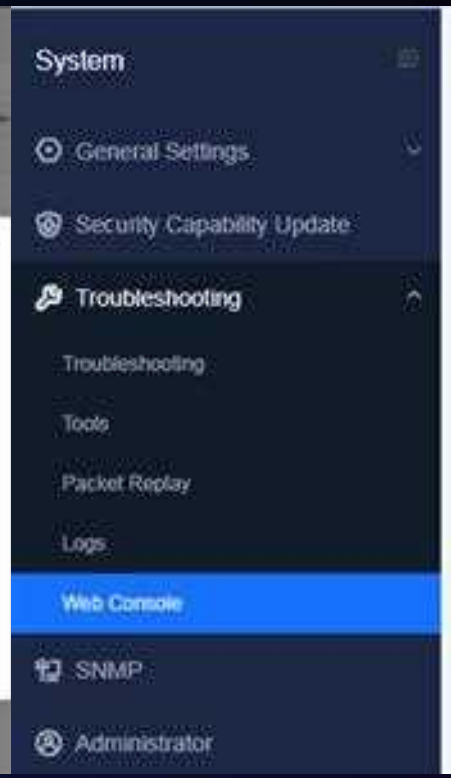
In Network Secure Platform, OSPF dynamic routing v2 and v3 can be configured separately, and they are divided into basic configuration and advanced configuration.



OSPF---Network Secure Platform

In Network Secure Platform, both OSPFv2 and OSPFv3 support BFD and GR features.

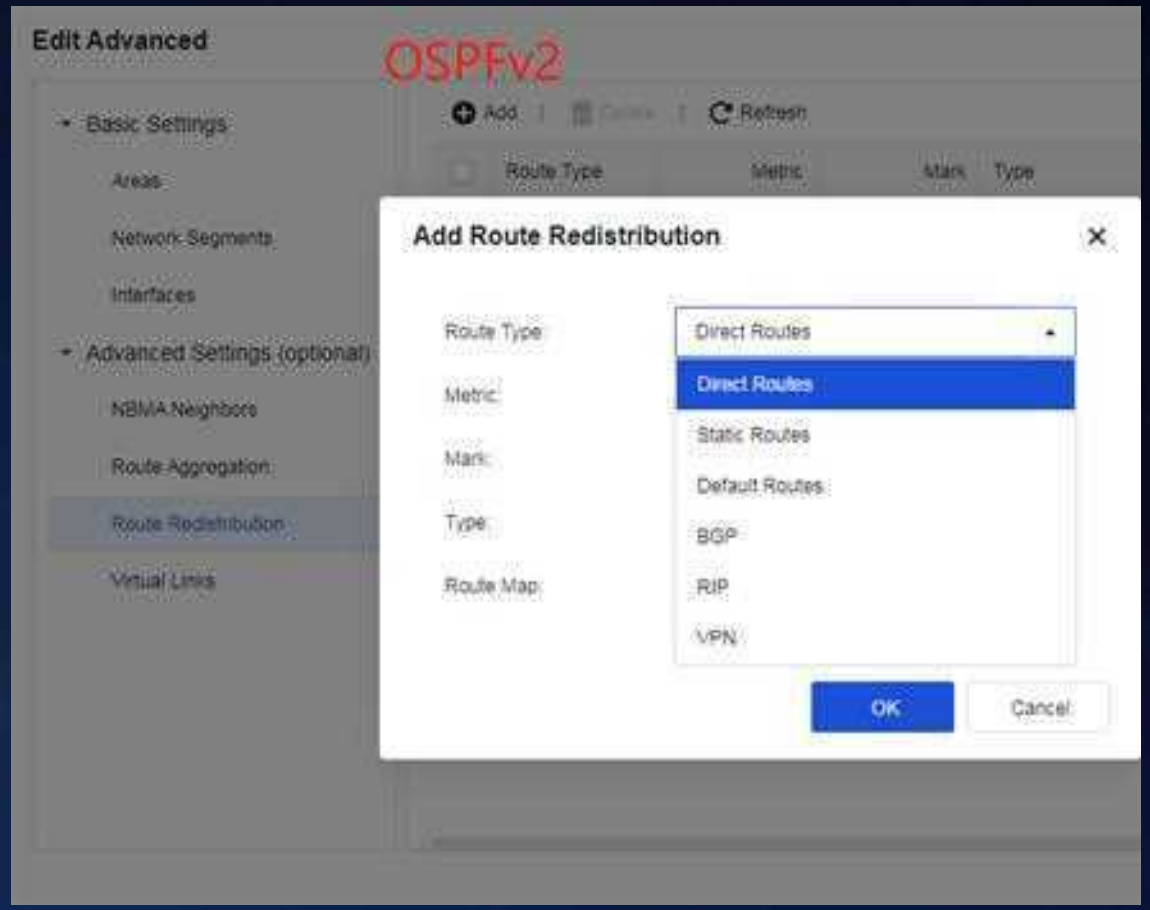


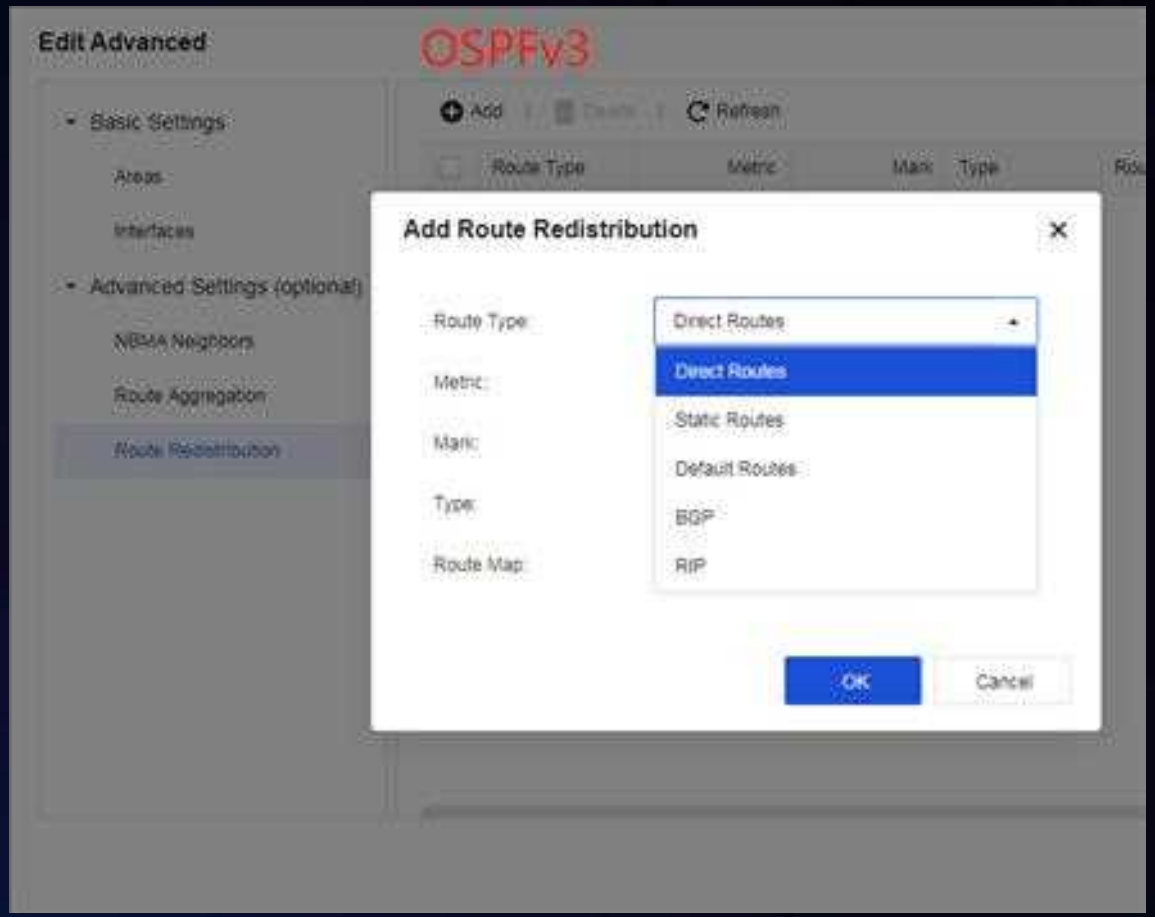



```
AF8.0.85.53 Build20230525
admin# config
admin(config)# router ospf
admin(config-ospf)# graceful-restart ?
  <cr>
  helper                                   GR helper
  period                                   GR interval
admin(config-ospf)# graceful-restart
```

OSPF---Network Secure Platform

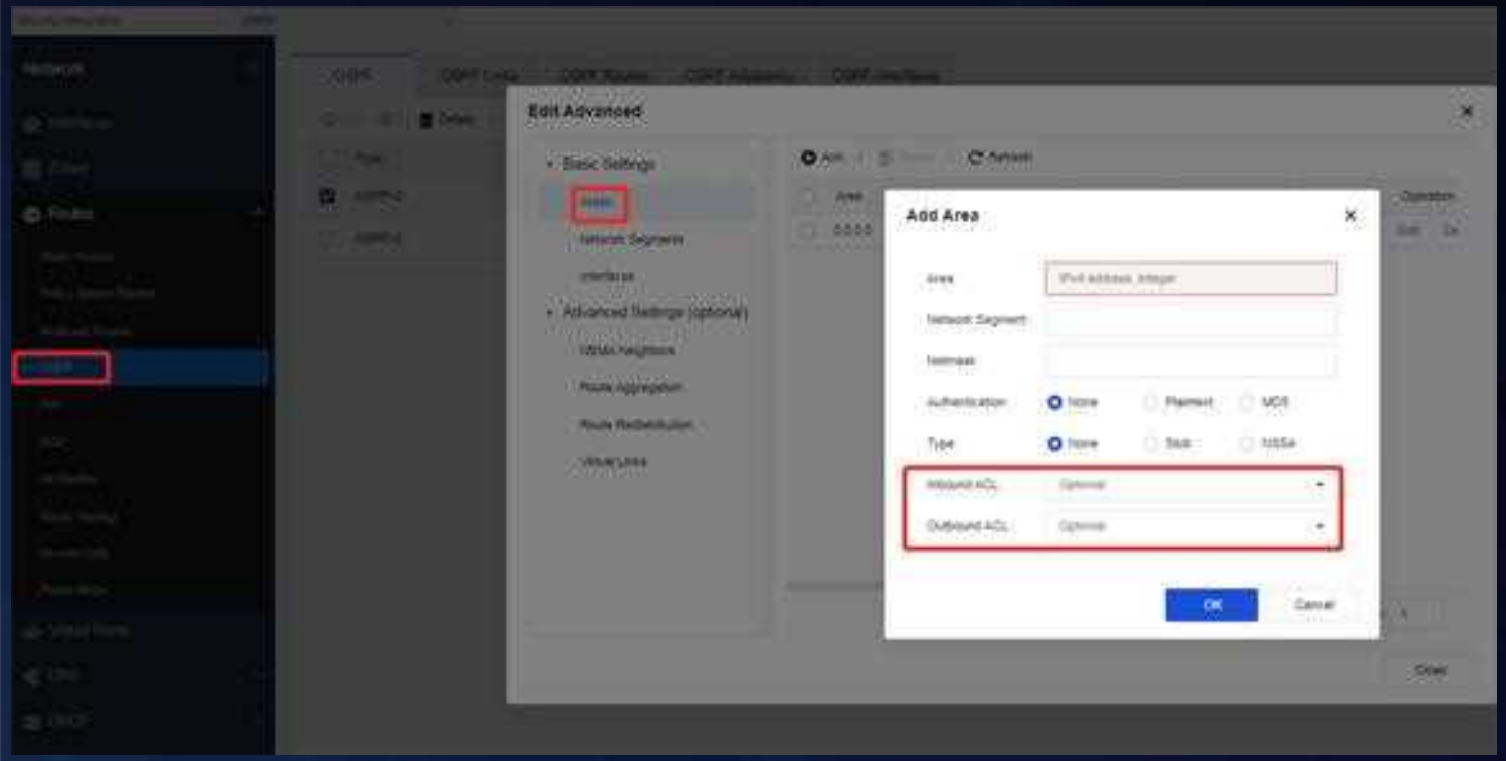
- OSPFv2 route redistribution supports direct routes, static routes, default routes, BGP routes, RIP routes and VPN routes.
- OSPFv3 route redistribution supports direct routes, static routes, default routes, BGP routes and RIP routes.

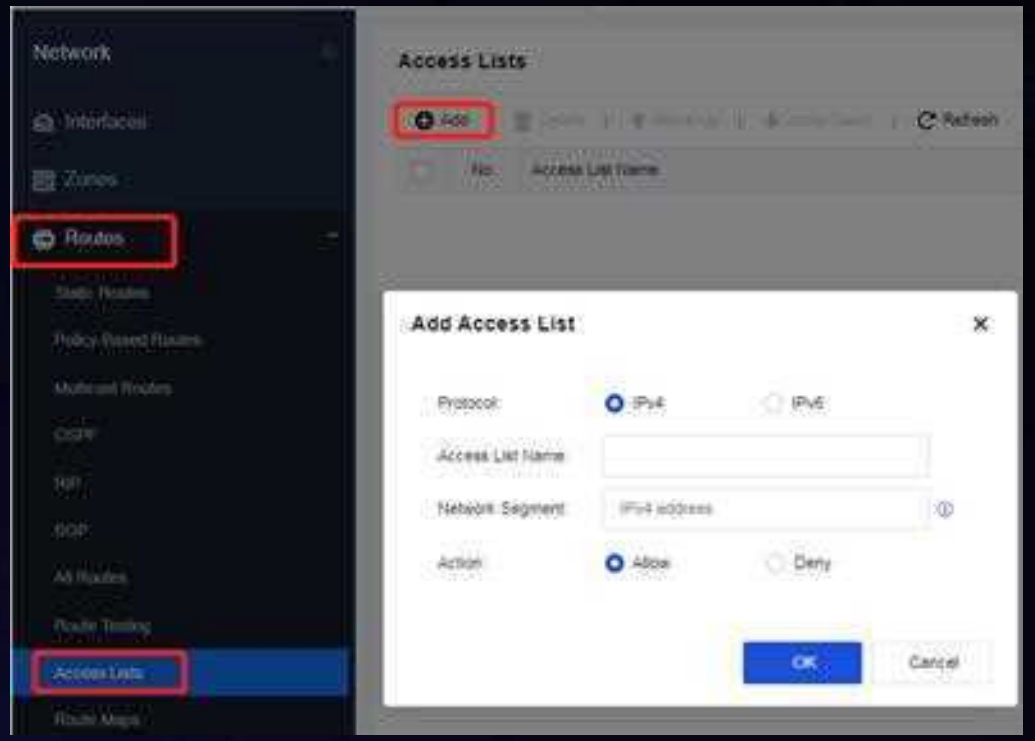




OSPF---Network Secure Platform

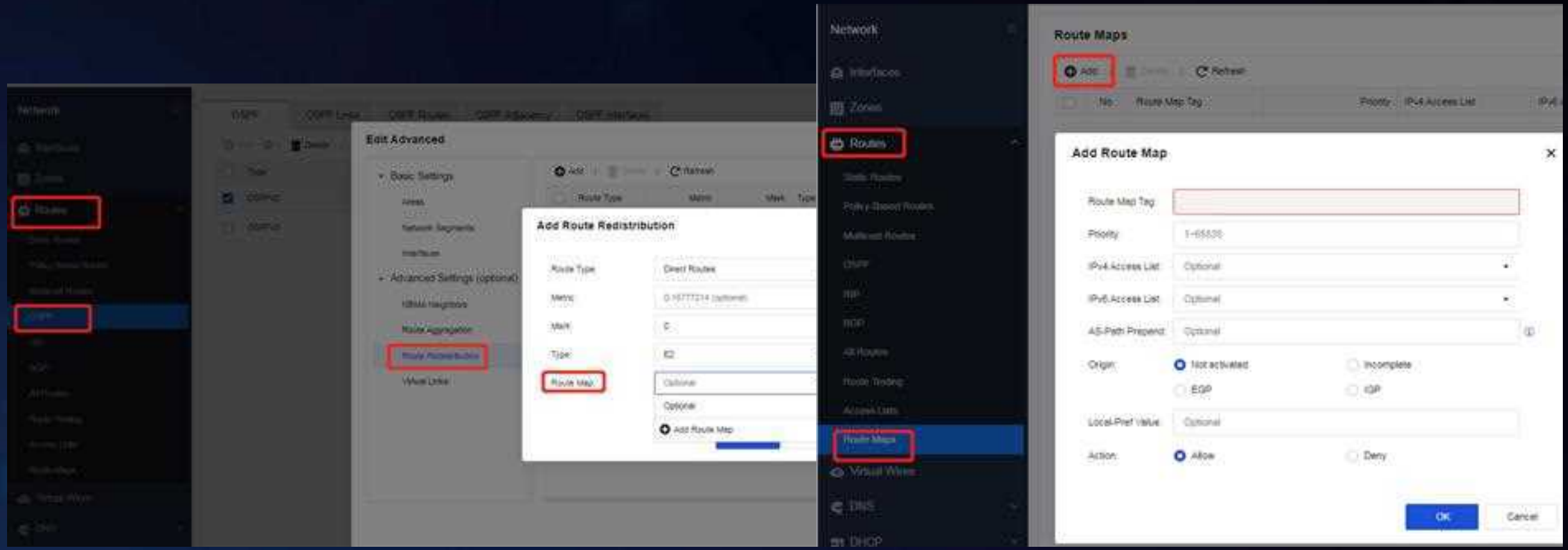
In Network Secure Platform, OSPF route supports inbound and outbound ACL, which represents access lists





OSPF---Network Secure Platform

In Network Secure Platform, OSPF route supports route map.

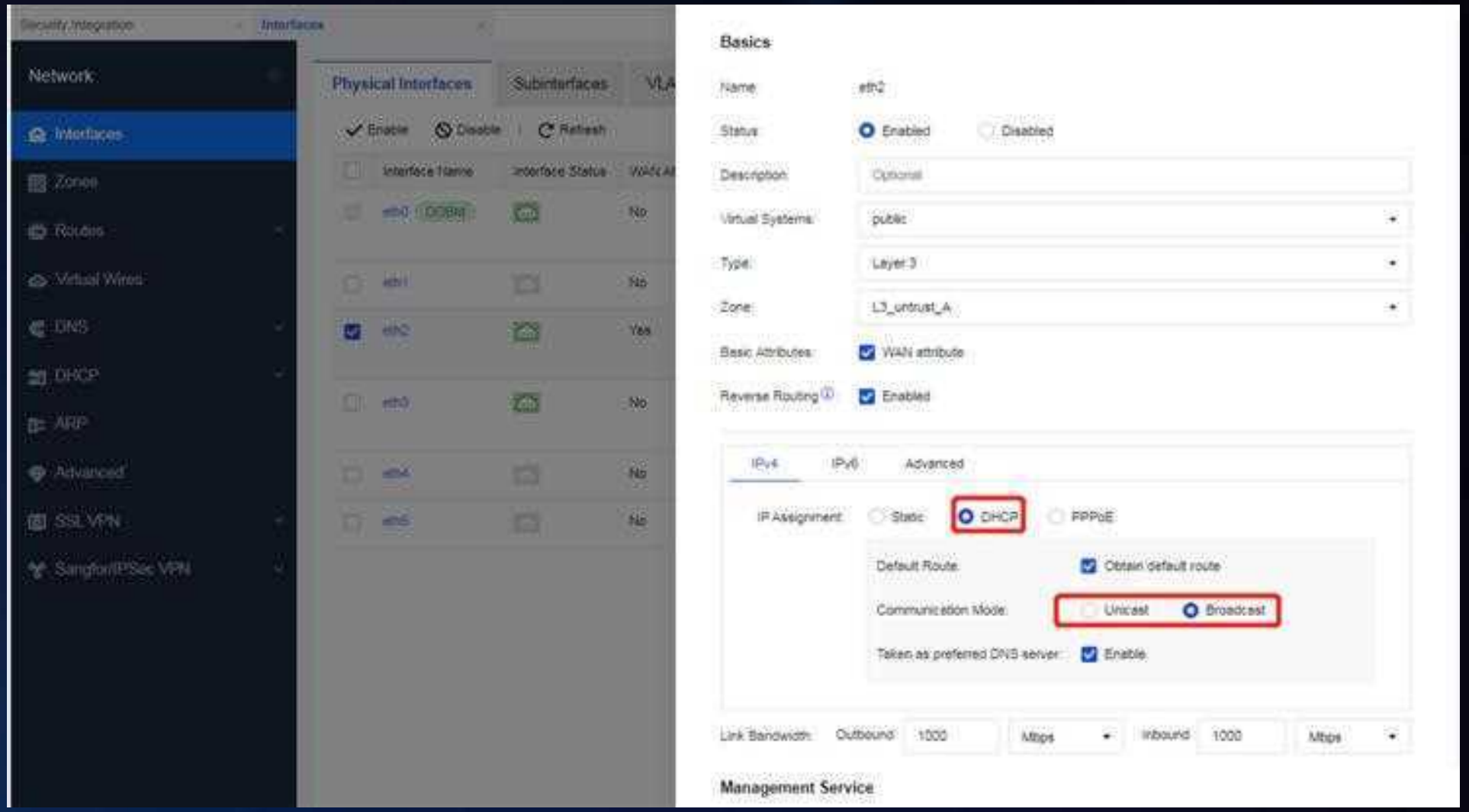


PART 3

New Feature About Network Secure Platform

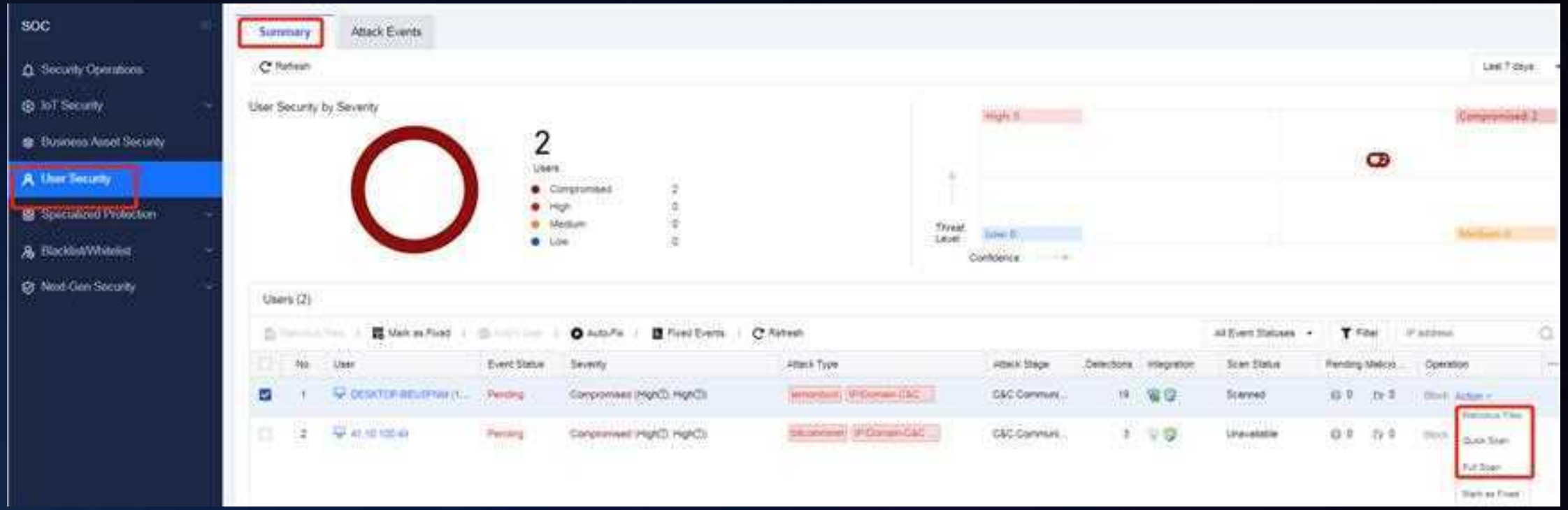
DHCP Interface

In Network Secure Platform, it supports selecting unicast or broadcast mode in the DHCP setting of interfaces.



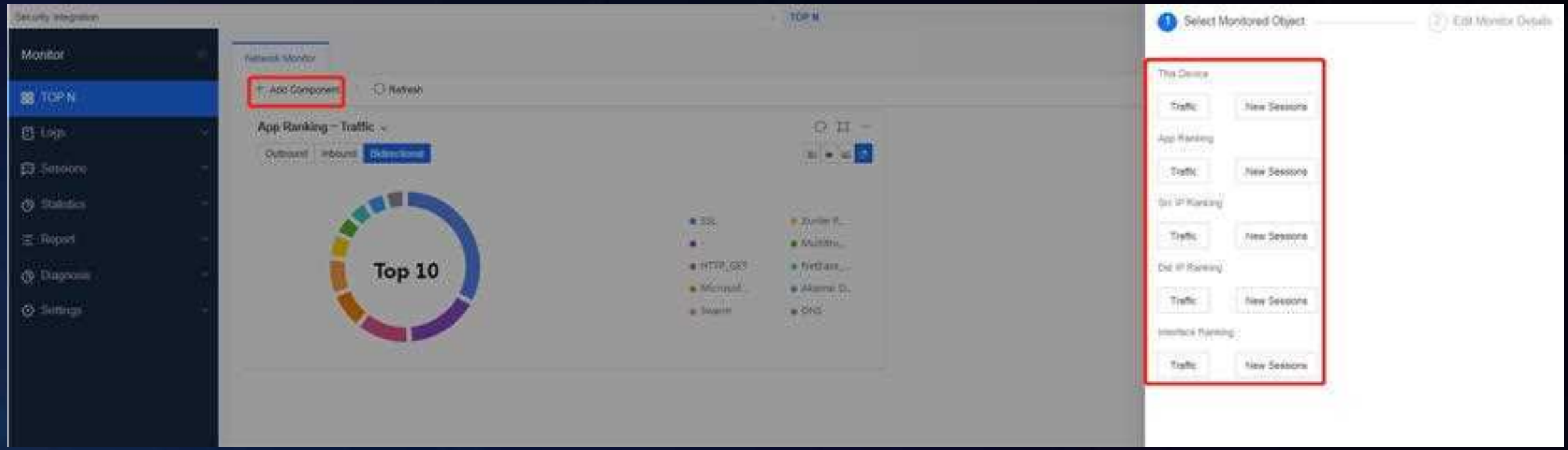
User Security

In Network Secure Platform, it adds blocking, handling of malicious files, quick scan, and full scan features. Before you use it, it is necessary to make sure that terminals installed Endpoint Secure client are online,and configure the correlation with Endpoint Secure.



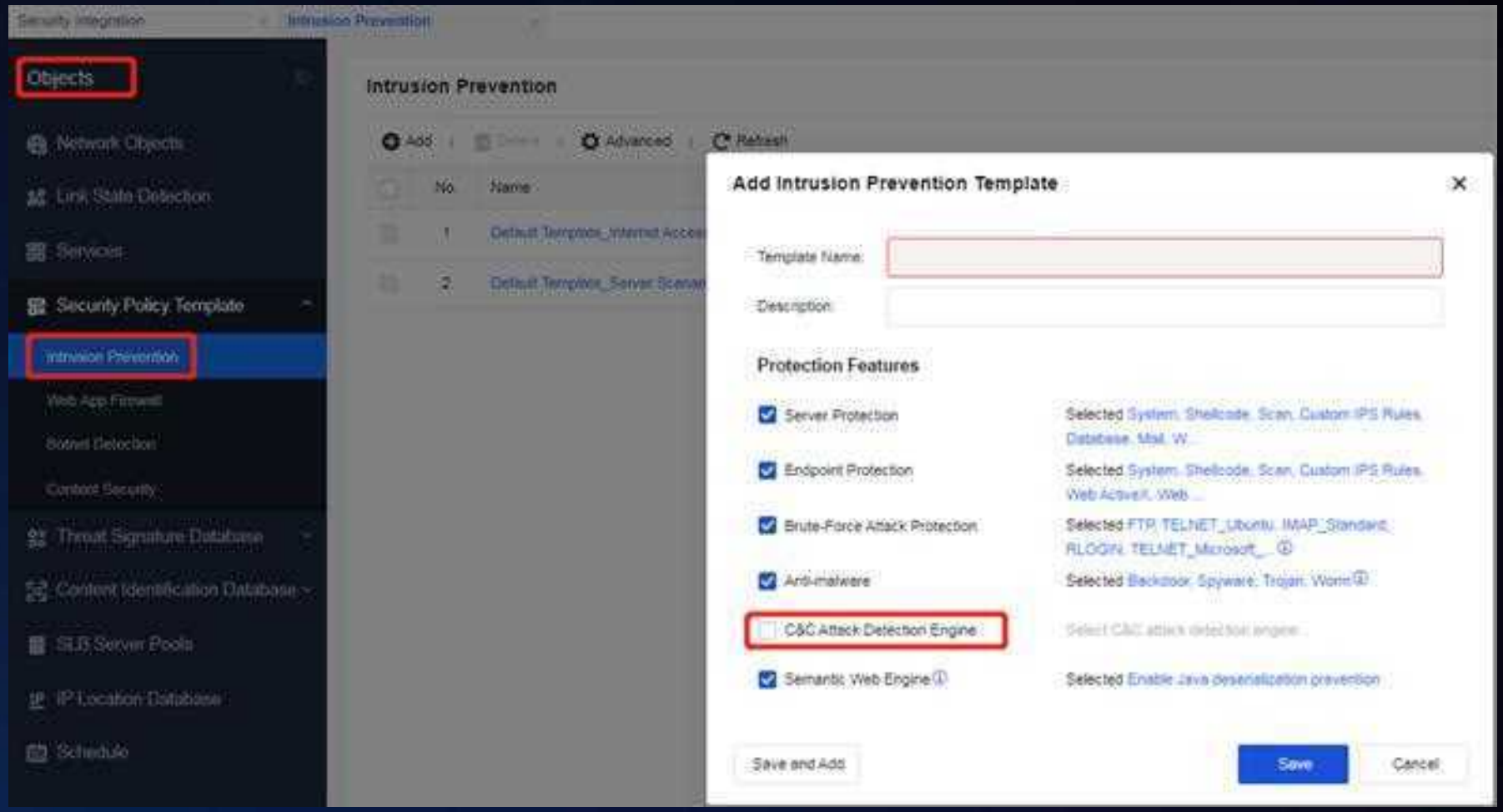
TOP N Feature

In Network Secure Platform , it adds TOP N feature which ranks network activities based on traffic and number of new sessions in two dimensions according to devices, app ranking, source IP ranking, destination IP ranking, and interface ranking.



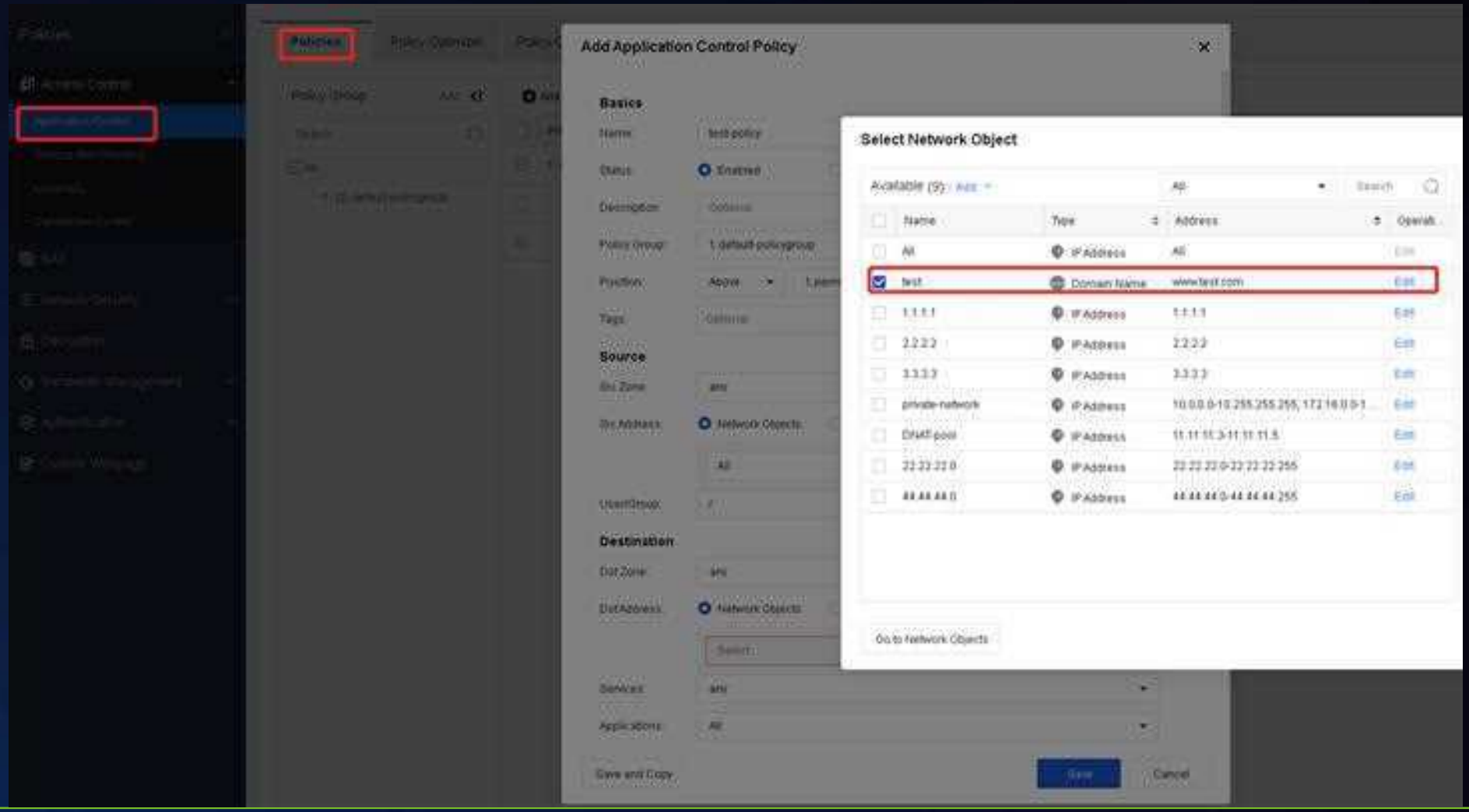
Intrusion Prevention

In Network Secure Platform, the intrusion protection module adds C&C attack detection engine, which audits protocols and reports to cloud platform to empower the NGAF capabilities, thereby improving the C&C attack detection ability.



Domain Name Object

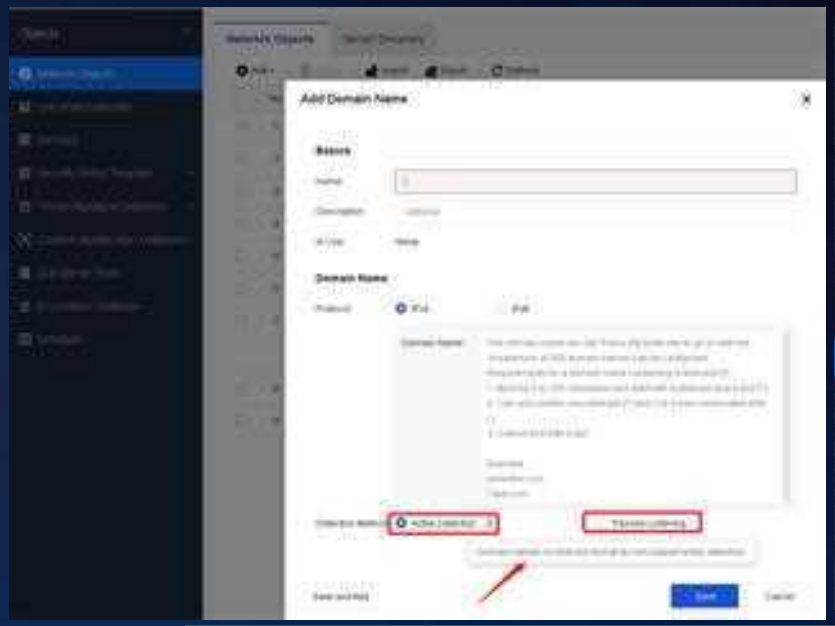
In Network Secure Platform, domain name can be added to network object and referenced in application control policies

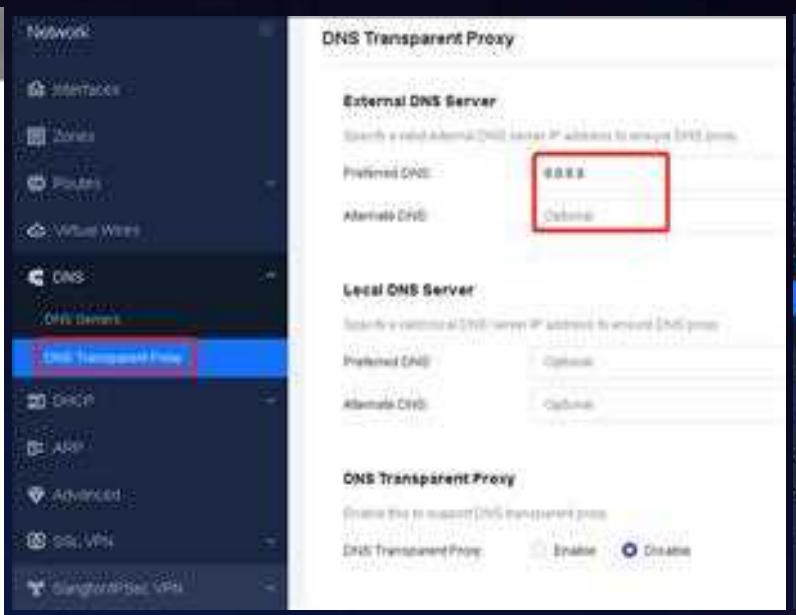


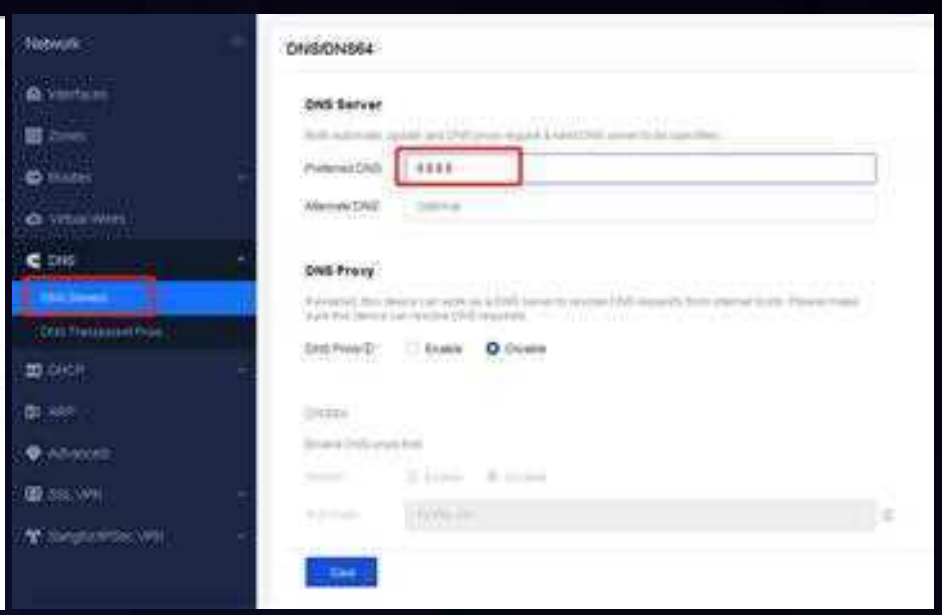
Domain Name Object

Domain name object contains active detection mode and passive listening.

- In active detection mode,it is unnecessary that the DNS traffic has to go through NGAF,while NGAF has to connect the DNS server for resolving the domains. It will adjust DNS server in DNS Transparent Proxy configuration module firstly, then to DNS Server module, so you need to make sure both those configuration are consistent or clear the former address even though the DNS Transparent Proxy is disabled by default.
- In passive listening mode, it is necessary to make sure the DNS traffic has been gone through the NGAF.
- Domain names in wildcard format do not support active detection mode.

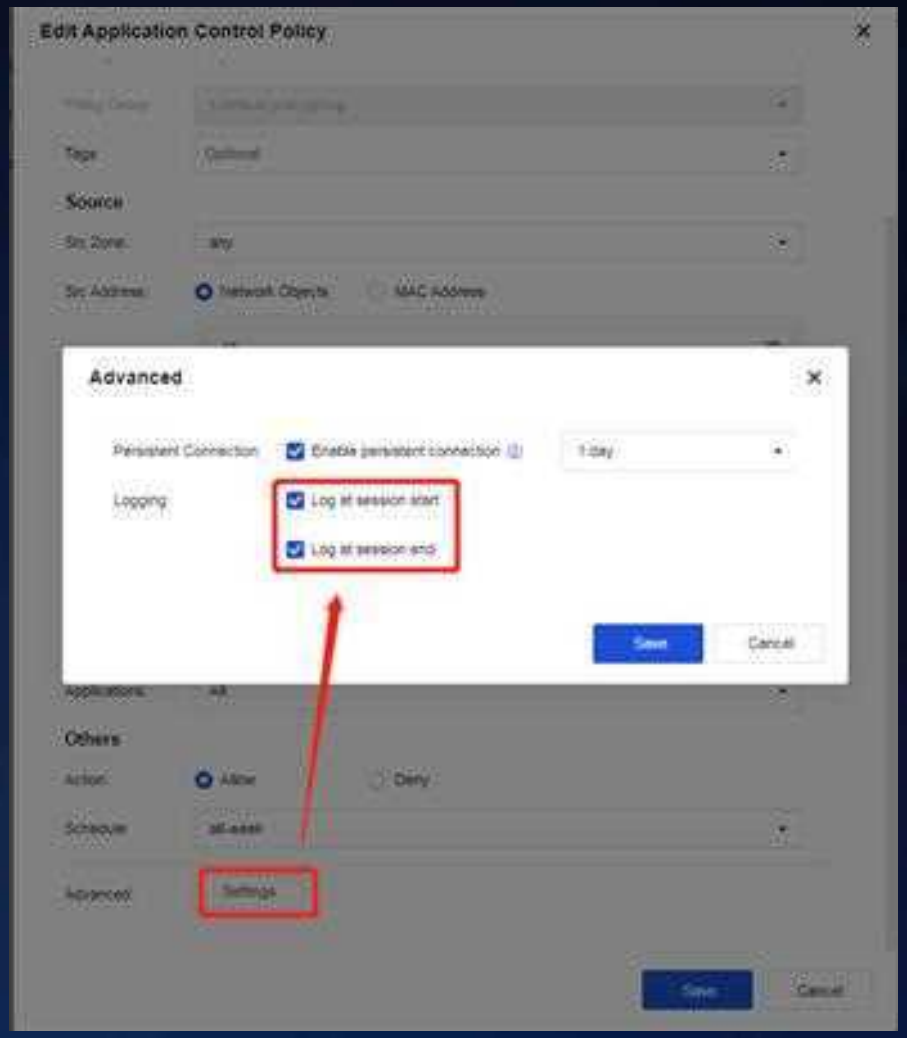


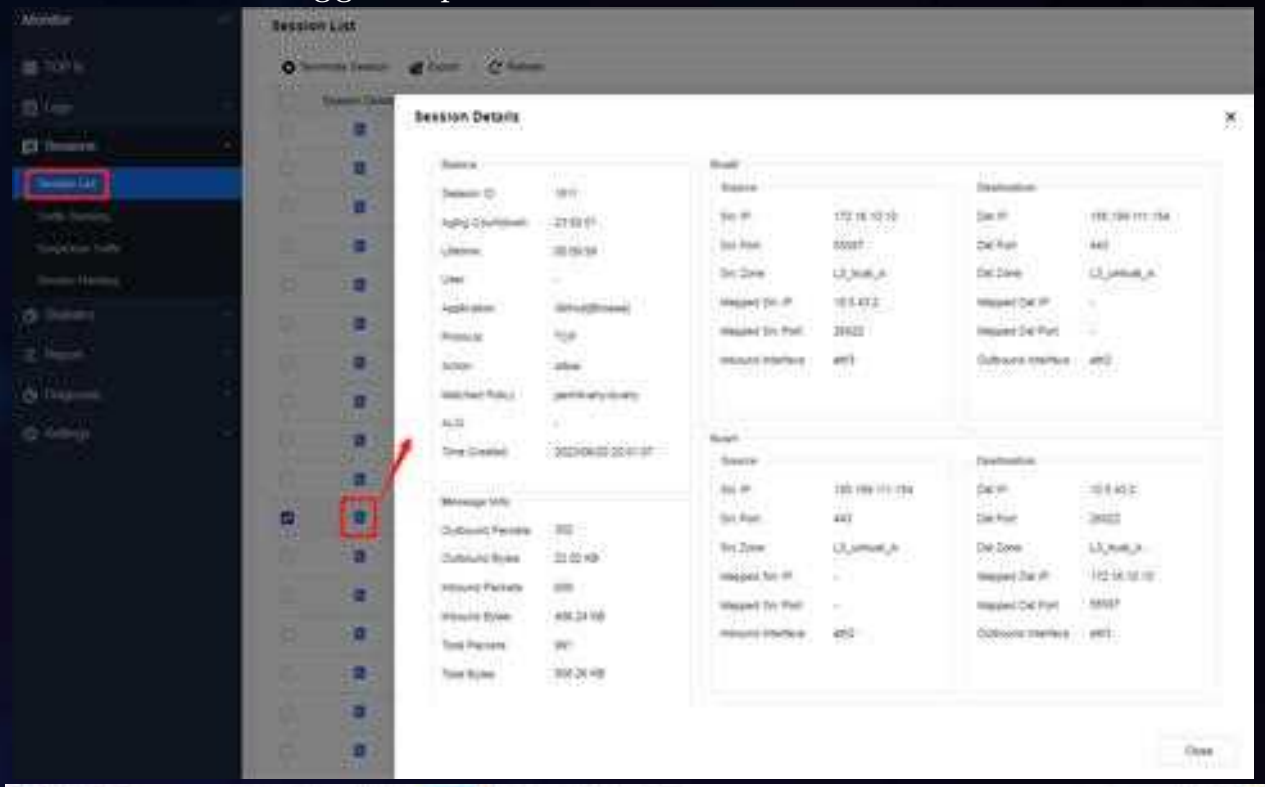




Session List

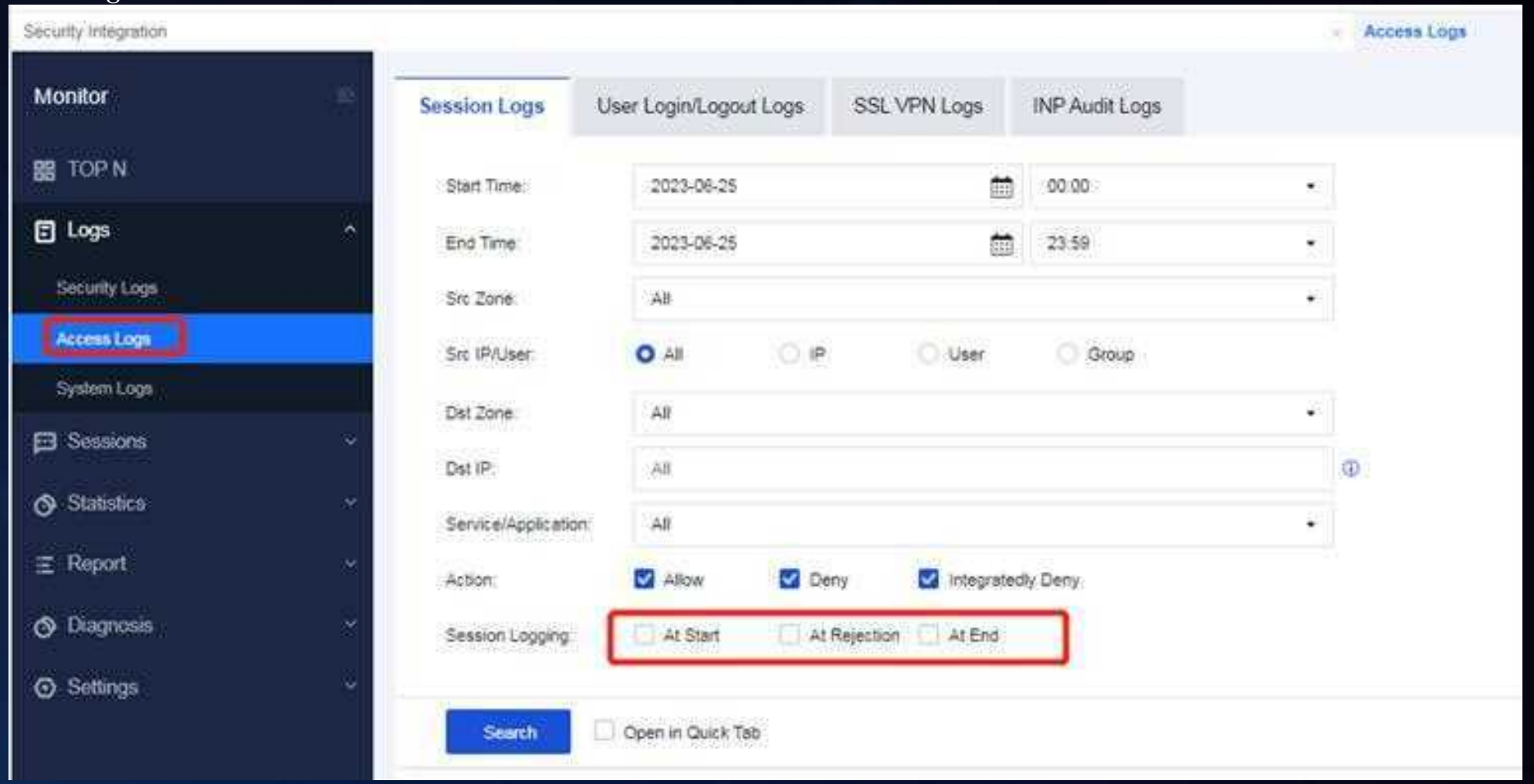
In Network Secure Platform, session list can display the entire attributes you want in details,which is a good way to daily utilization, but you are required to enable loggin options in advance.





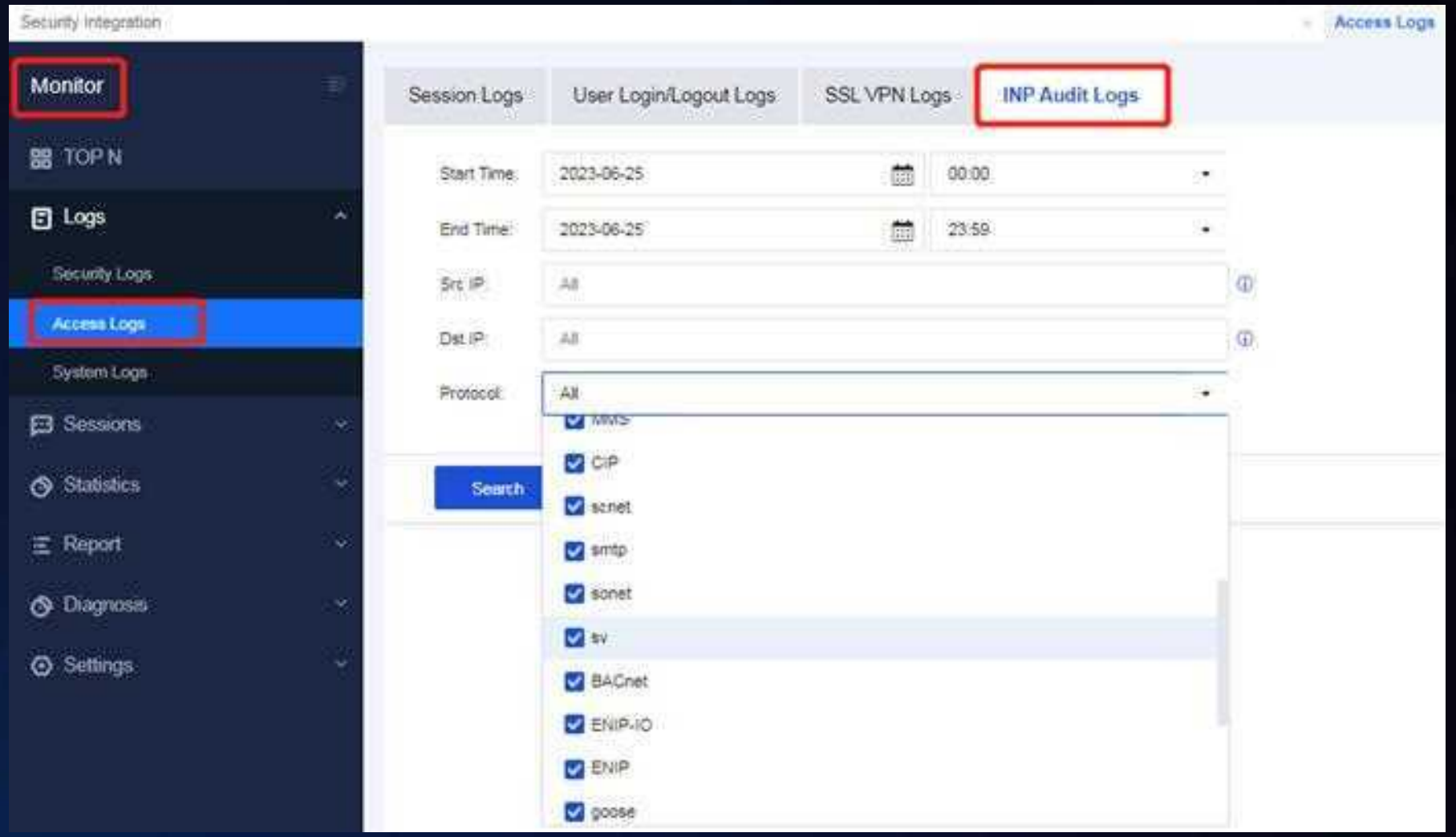
Session List

According to this feature, Network Secure Platform supports below options when you want to search specific types of logs.



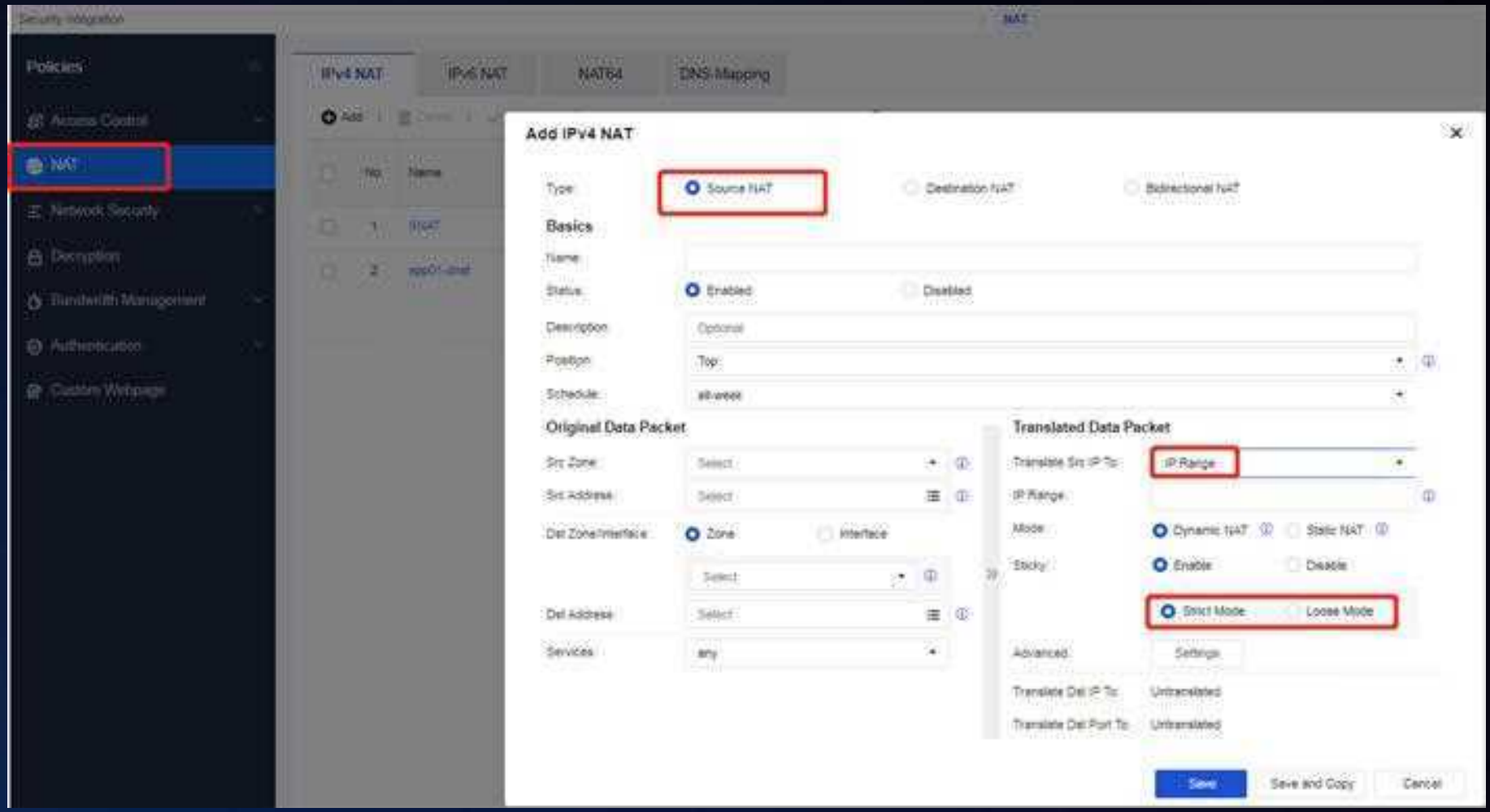
INP Audit Logs

In Network Secure Platform, it can audit some INP protocols, and so far the supporting ptotocal types including opcda, s7, s7-plus, modbus, iec104, and profinetIO.



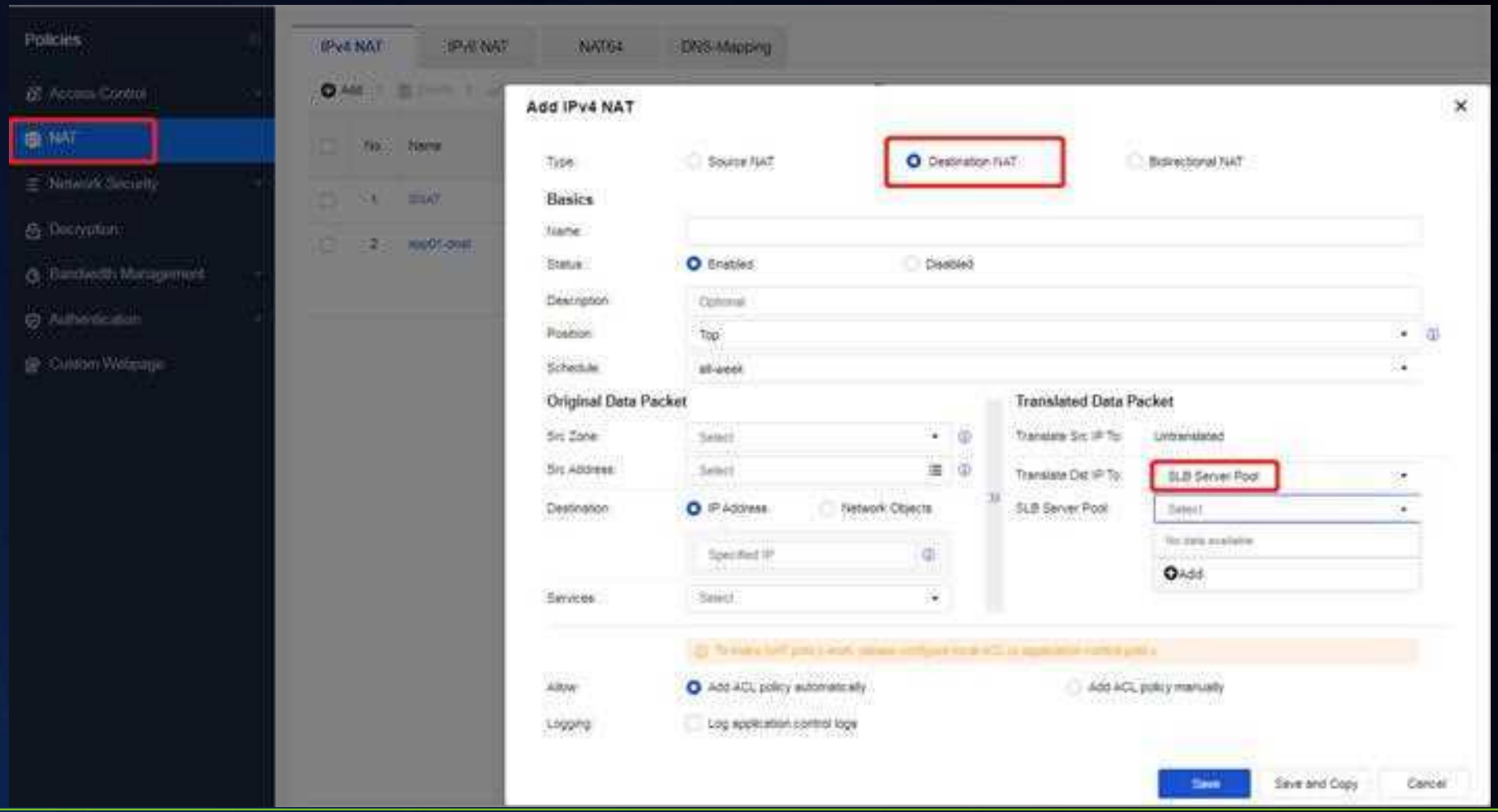
SNAT

In new platform NGAF, it adds the options of strict mode and loose mode in dynamic SNAT scenario when the translated addresses belong IP range or network object.



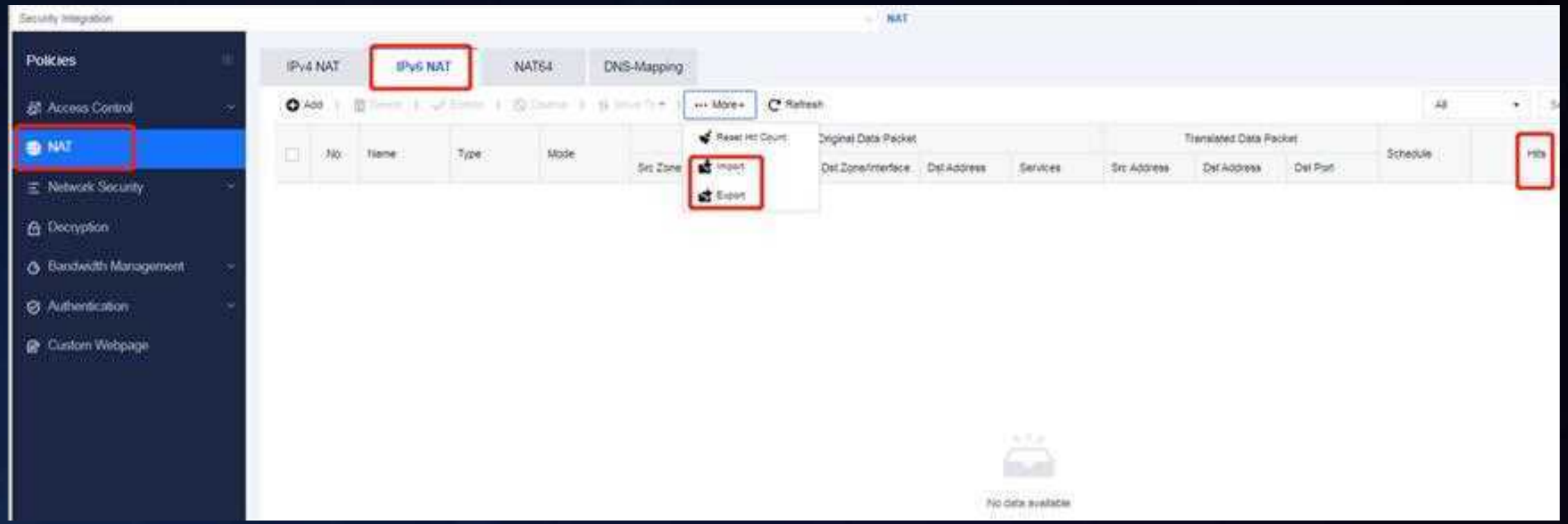
DNAT

In Network Secure Platform, the DNAT supports selecting SLB server pools as the translated target, and an IP in the address pool can be selected as the destination address by using round-robin algorithm to achieve load balancing of traffic on different servers.



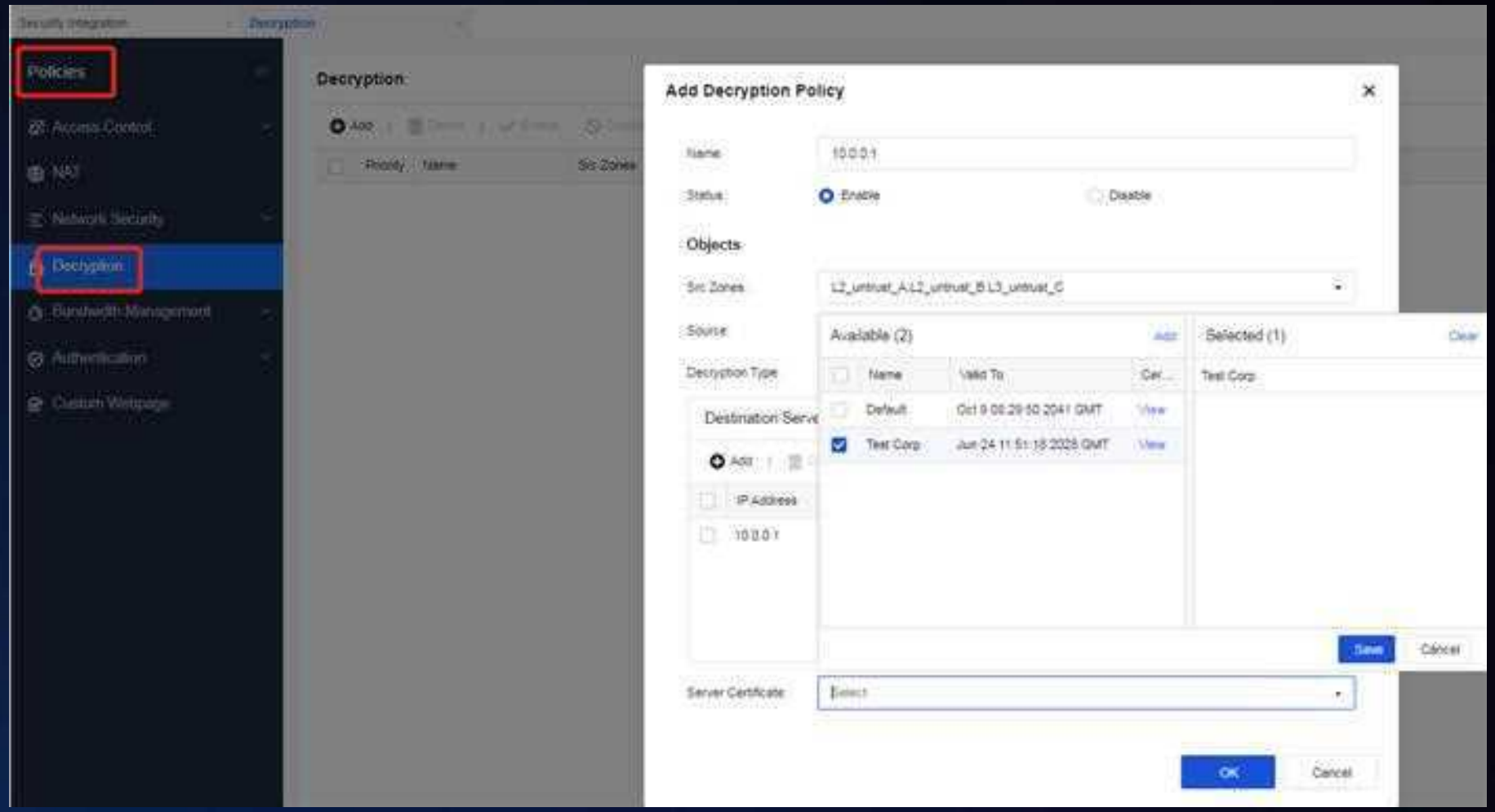
IPv6 NAT

In Network Secure Platform, IPv6 NAT adds the feature of import and export operations, meanwhile every NAT item can display the hit counts.



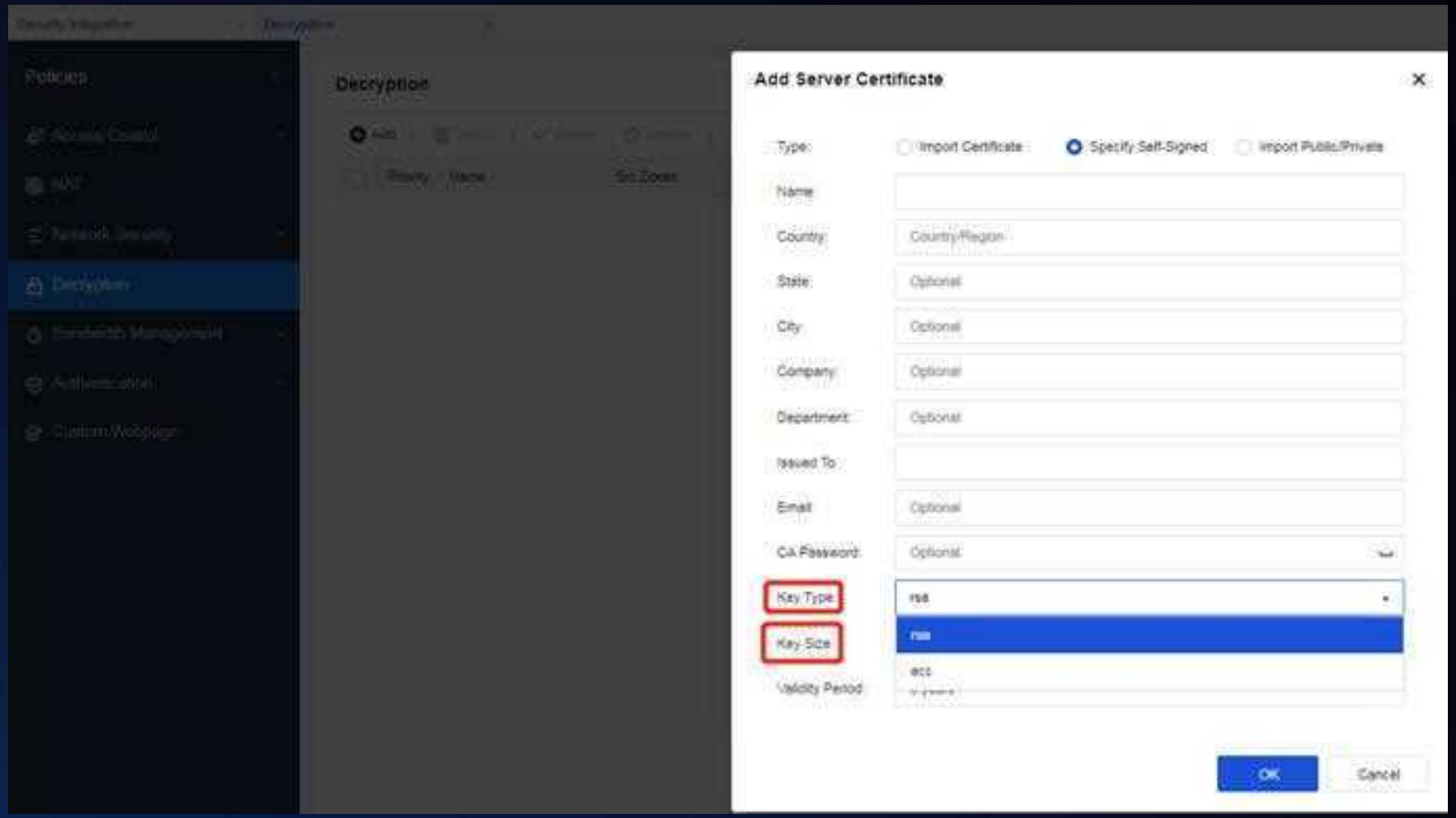
Decryption

In Network Secure Platform, decryption policy supports TLS 1.3 and allows the selection of multiple server certificates within a single policy, supporting up to 8 certificates simultaneously.



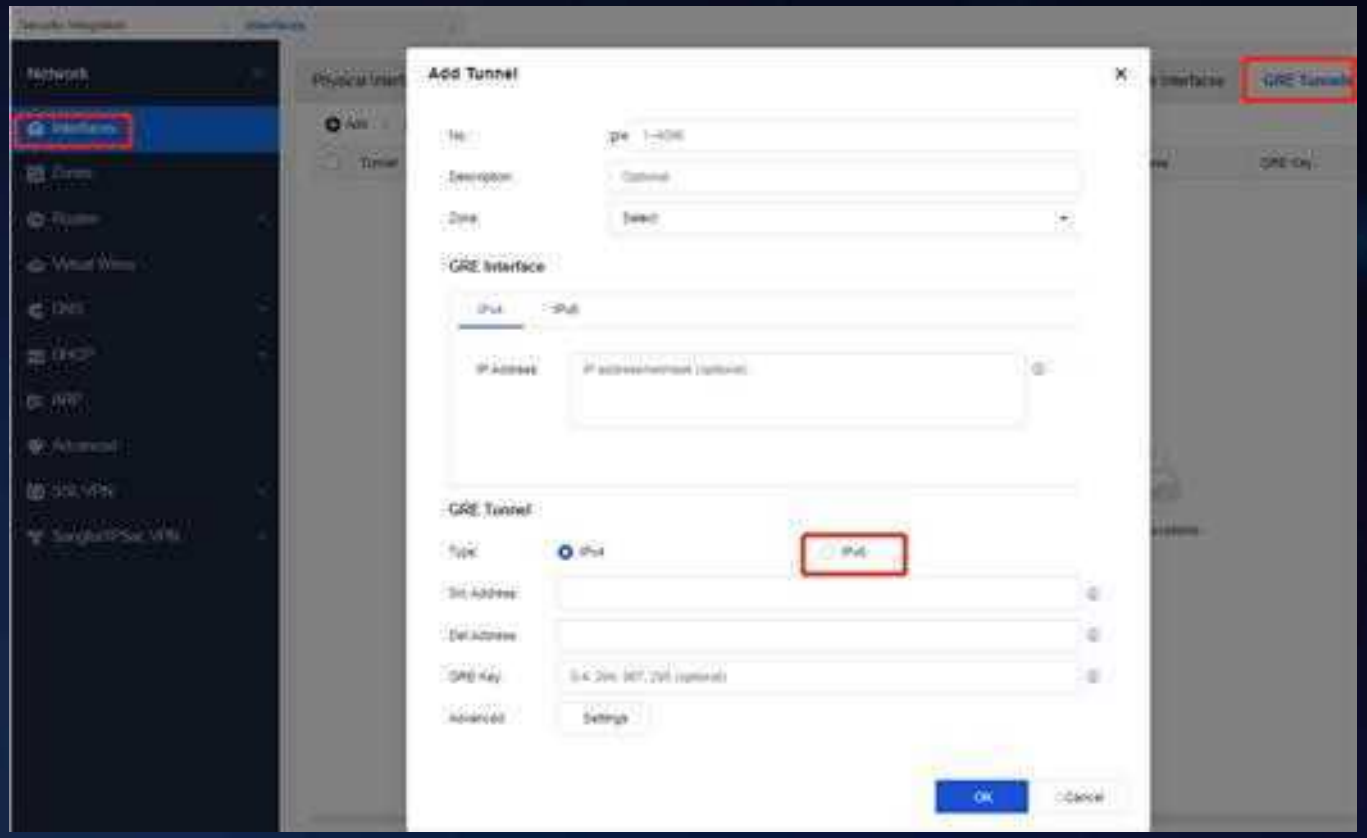
Decryption

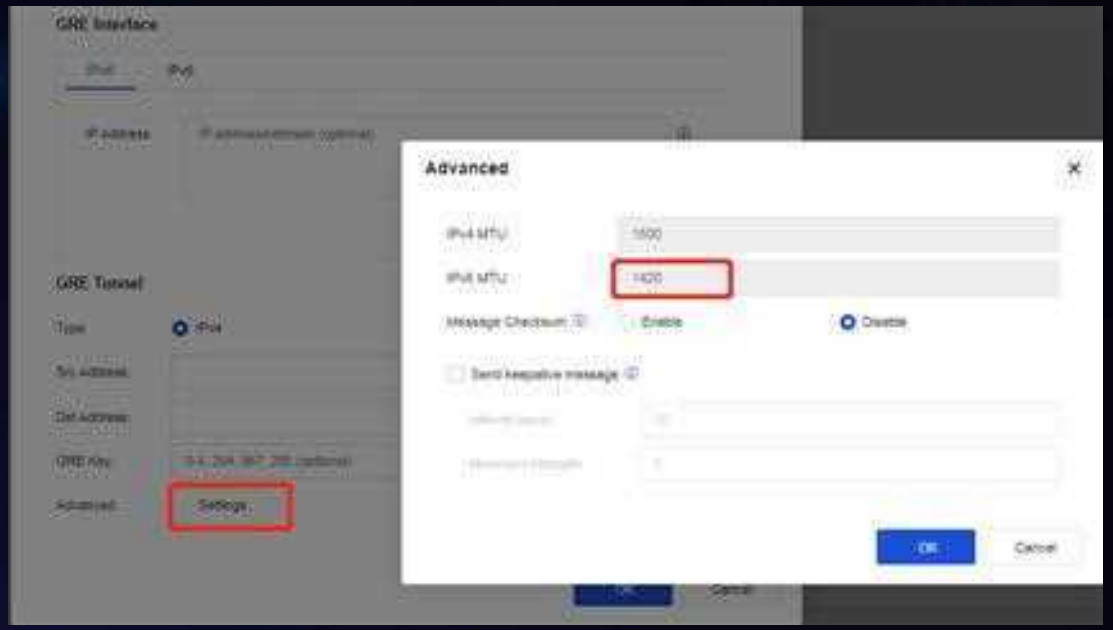
In Network Secure Platform, self-signed server certificate supports a dropdown menu to select the encryption key type and key size. Key types include RSA and ECC, while key size includes 2048 and 4096



GRE Tunnel

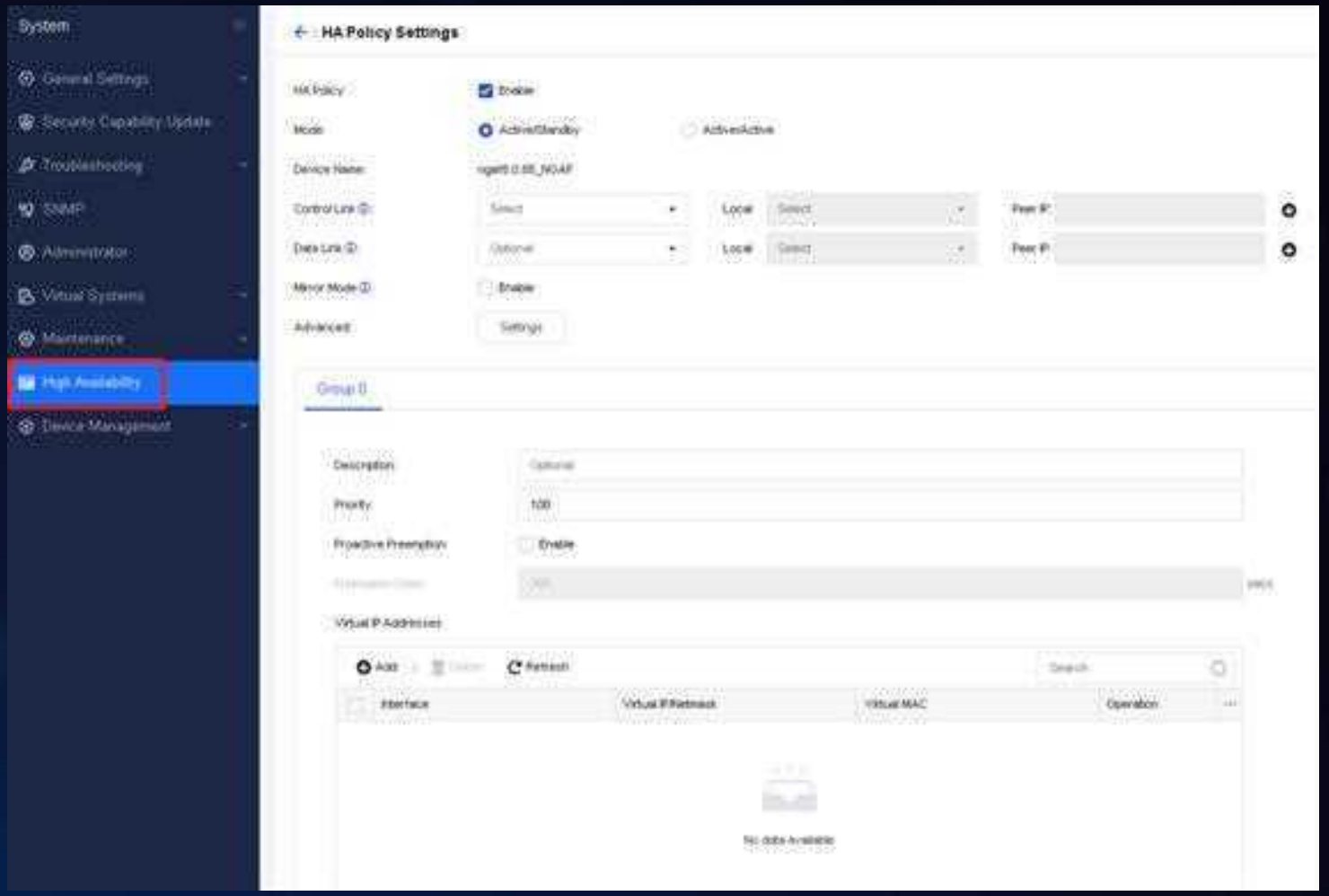
In Network Secure Platform, it support GRE tunnel with IPv6 type, besides the advanced settings for GRE tunnels include the addition of IPv6 MTU configuration.





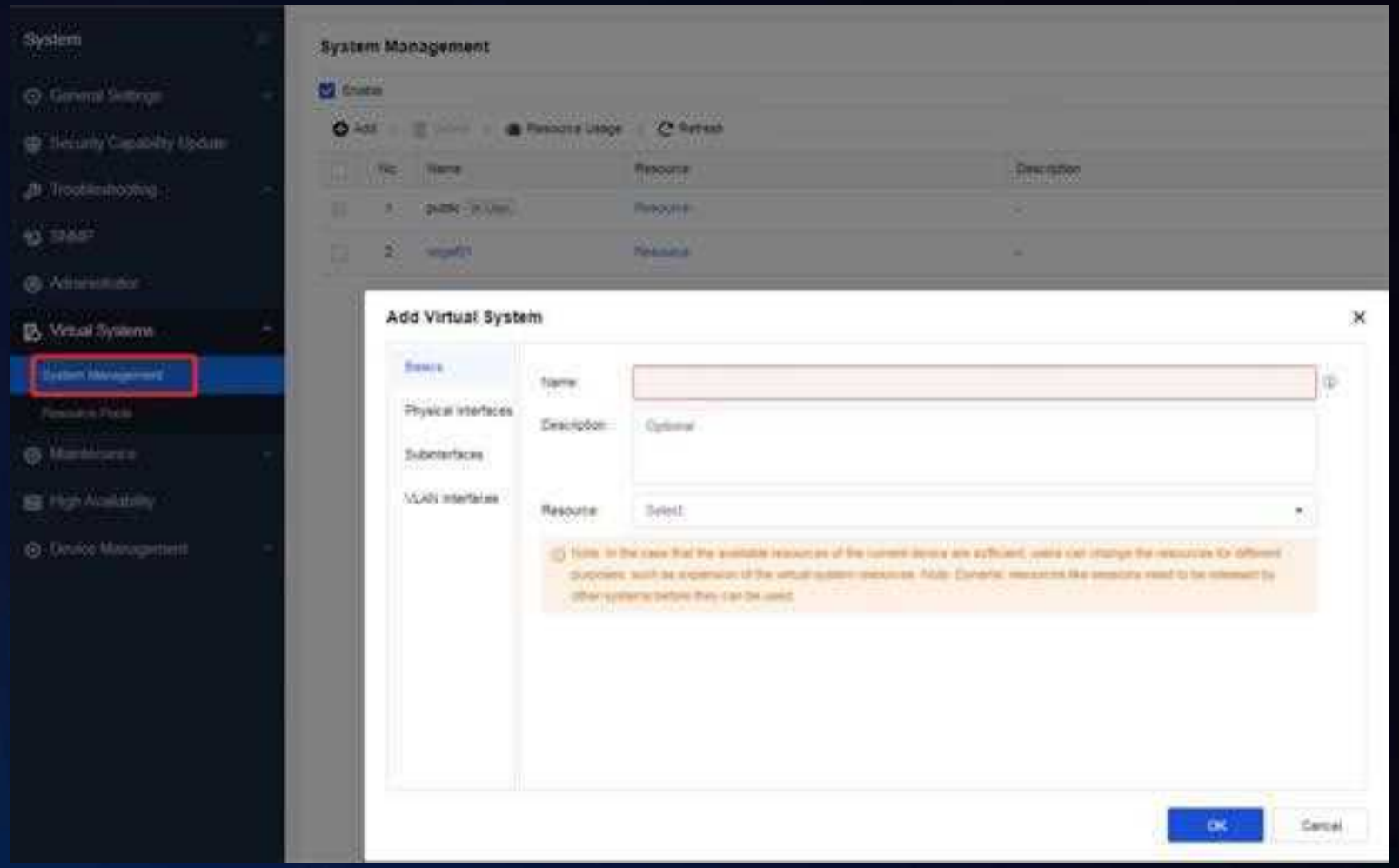
High Availability

In Network Secure Platform, there is an huge modification in HA module to meet flexible network circumstances, for example it adds HA traffic, link aggregation, virtual IP and Group1. For this part we will introduce it in the doc file.



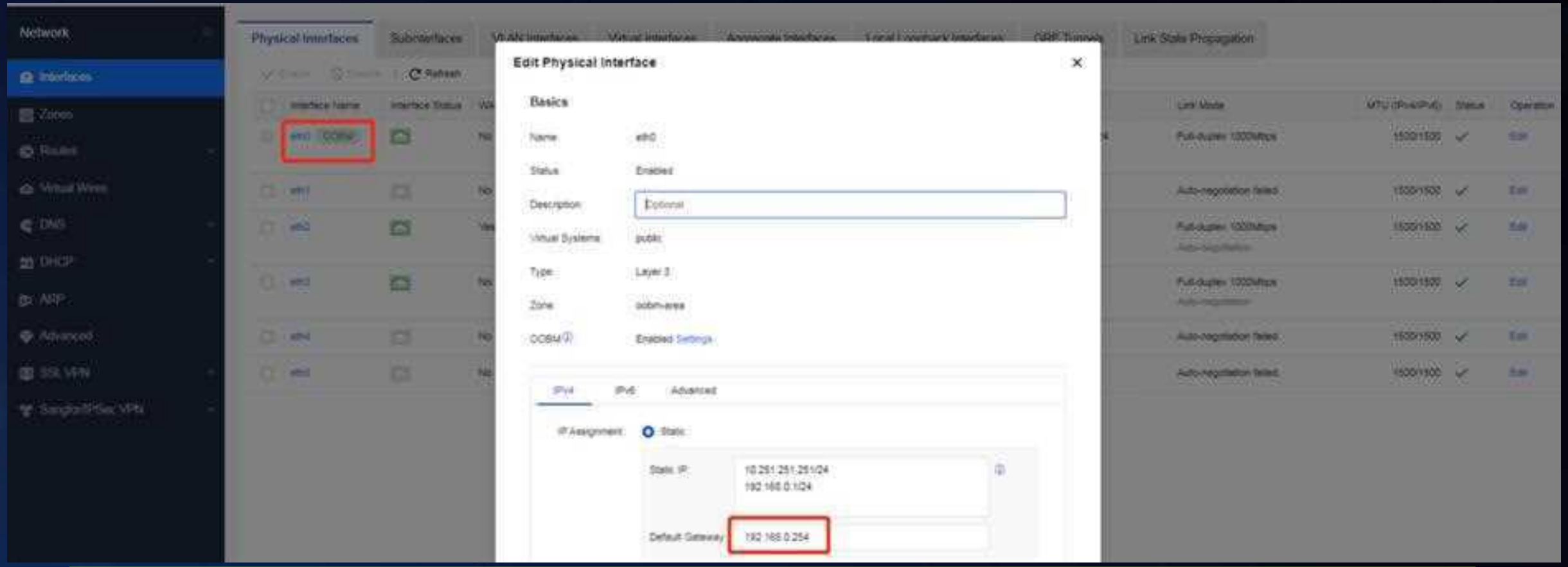
Virtual System

In Network Secure Platform, it adds virtual systems feature, logically dividing one NGAF device into multiple virtual systems. Each virtual system is equivalent to a real NGAF device, with its own interfaces, network objects, routing table, and policies, and can be independently configured and managed by virtual system administrators.



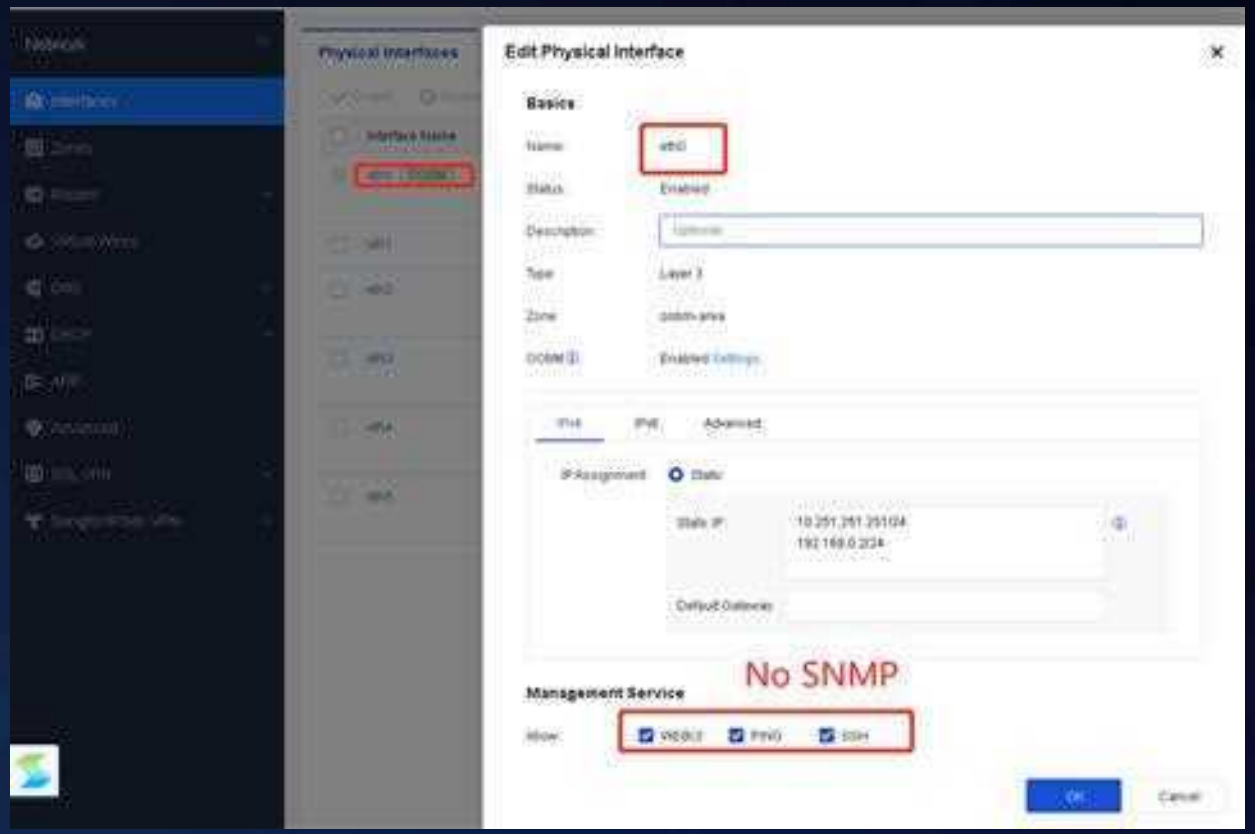
Out-of-band Management

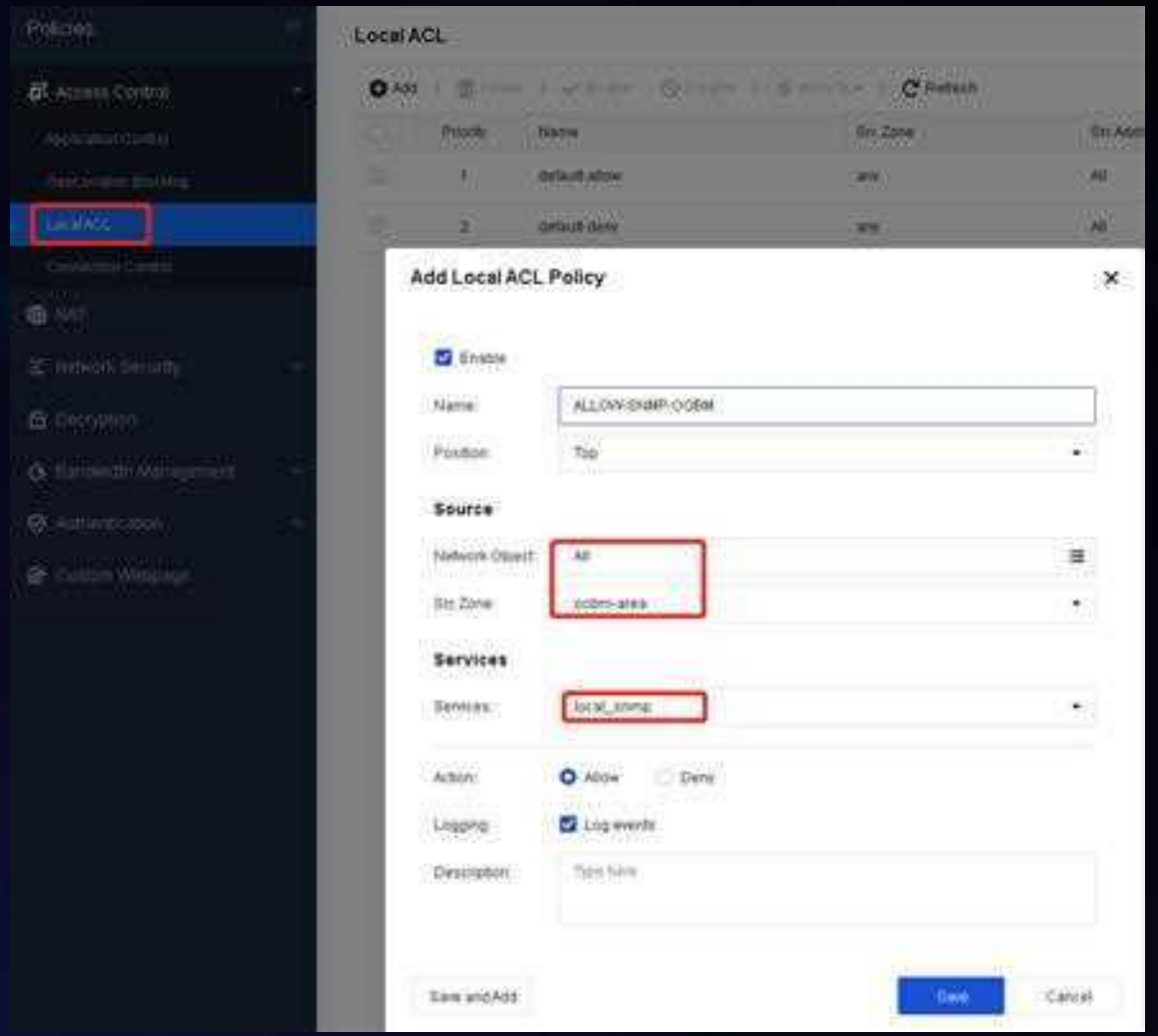
In Network Secure Platform, it adds out-of-band management feature, which can effectively isolate client's business network from management network. It also allows for configuration of specified traffic to match designated routes for forwarding. Currently, the out-of-band management of the Network Secure Platform can only be used by eth0 port. After configuring the next hop address on the eth0 port, a default route of management network will be created.



SNMP--Out-of-band Management Interface

In Network Secure Platform, some customers would like to add SNMP mornitoring by out-of-band management interface, you have to add an local access control list to turn on the service since the management service in out-of-band management interface is not bonded.



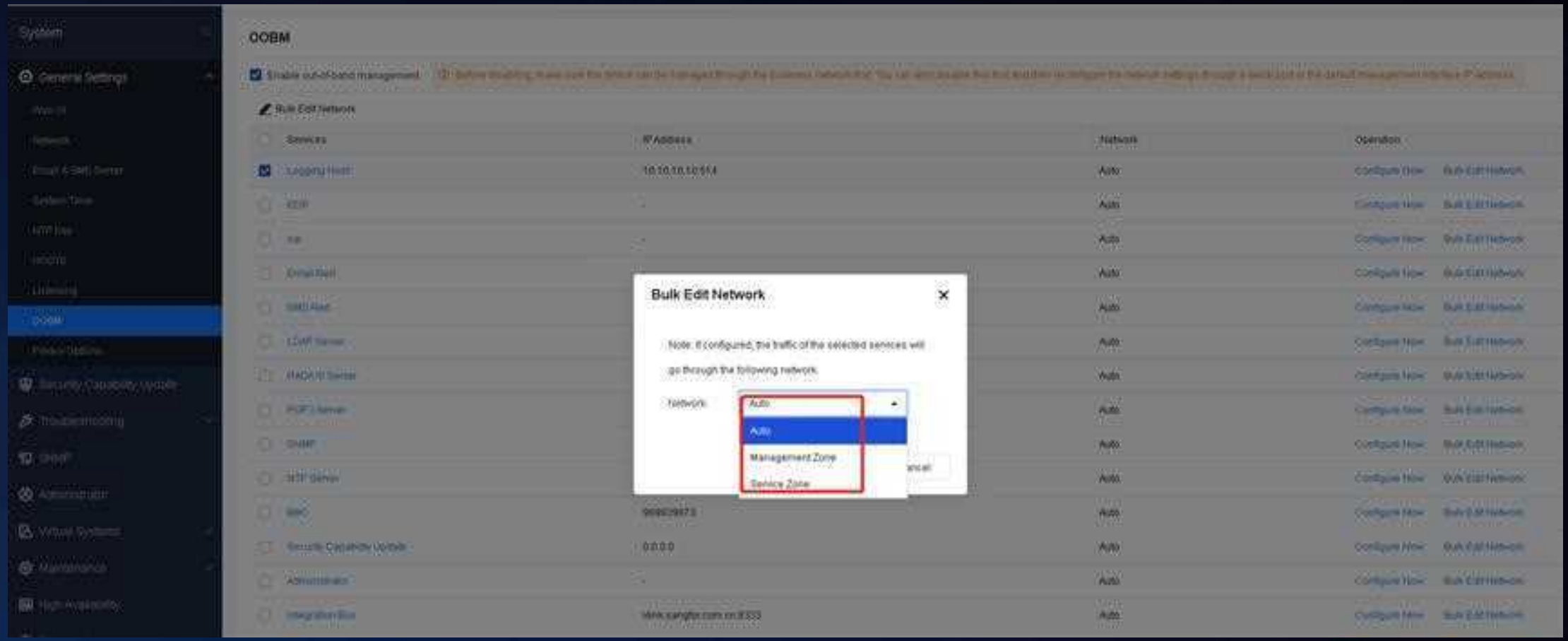


OOBM

In Network Secure Platform, it adds the concept of OOBM zone and some relative management service, such as logging host, external authentication platform, and some docking devices have an extra option to connect through out-of-band management network.

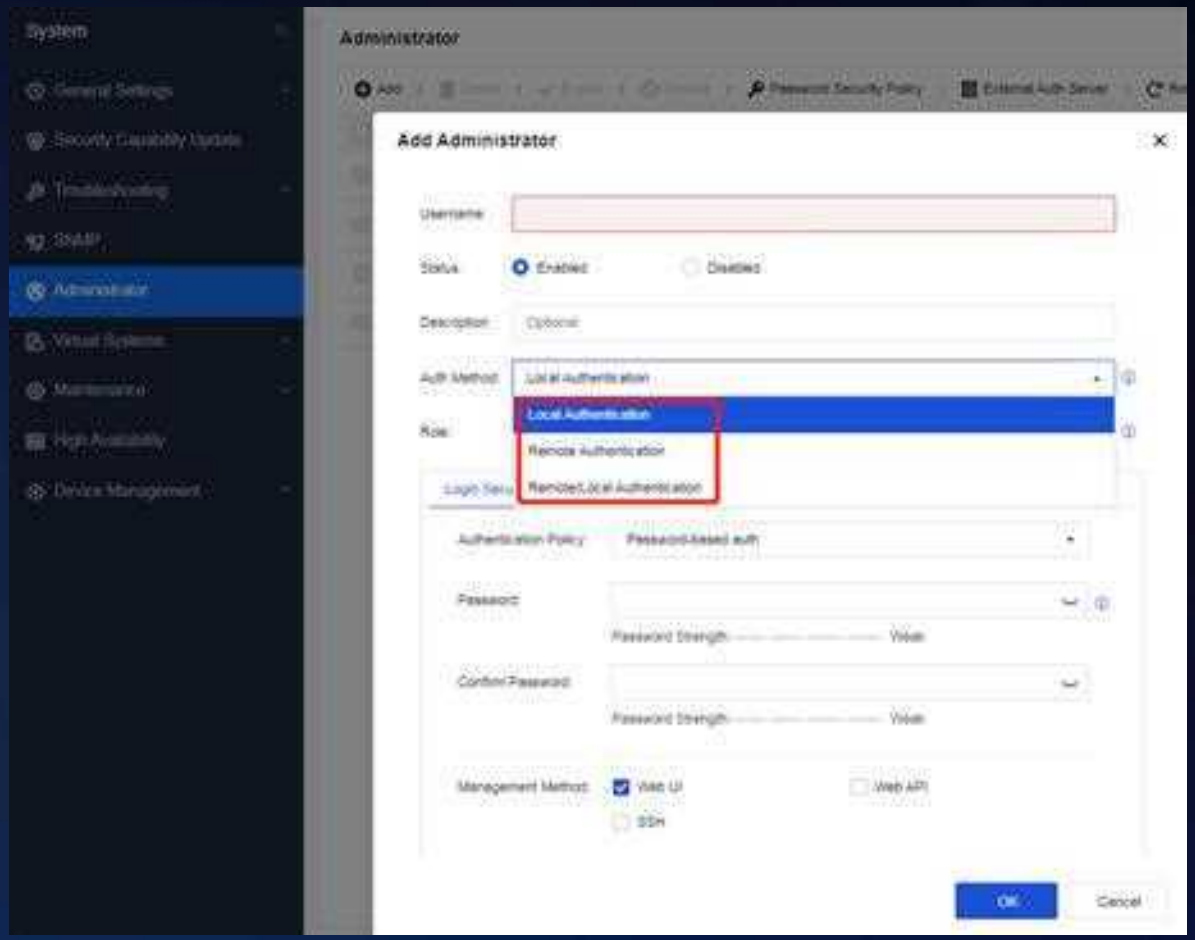
OOBM

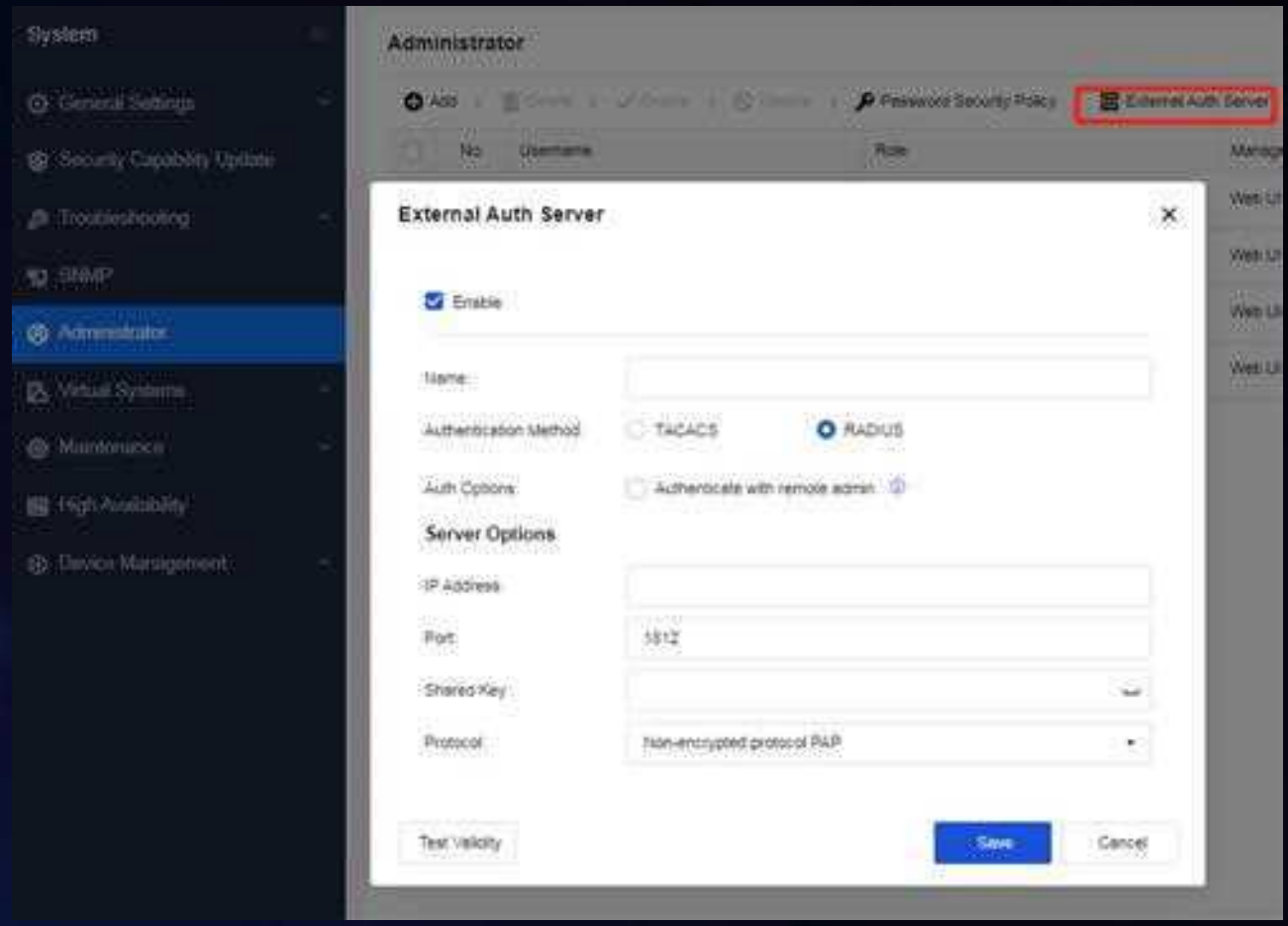
In Network Secure Platform, it adds the concept of OOBM zone and some relative management service, such as logging host, external authentication platform, and meanwhile every docking device has an option to connect through out-of-band management network or business network. If you select "Auto" when you "Bulk Edit Network",it will query routing table in the order of business network first, followed by management network.



Administrator

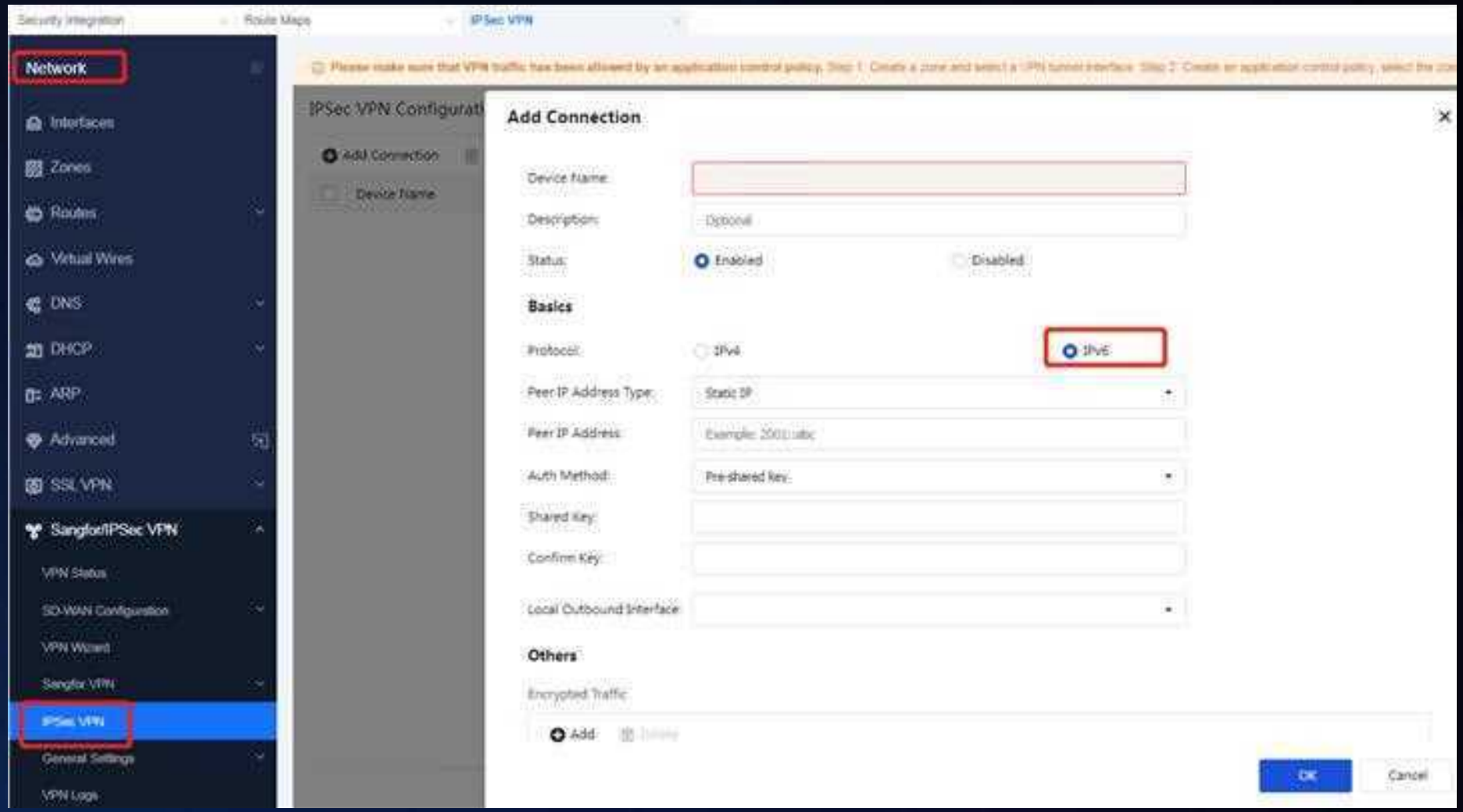
In Network Secure Platform, it adds extra authentication types, including local authentication, remote authentication, and remote/local authentication. When selecting remote/local authentication, external servers that have been previously configured are preferred for authentication. If the server cannot be connected, local authentication will be performed.





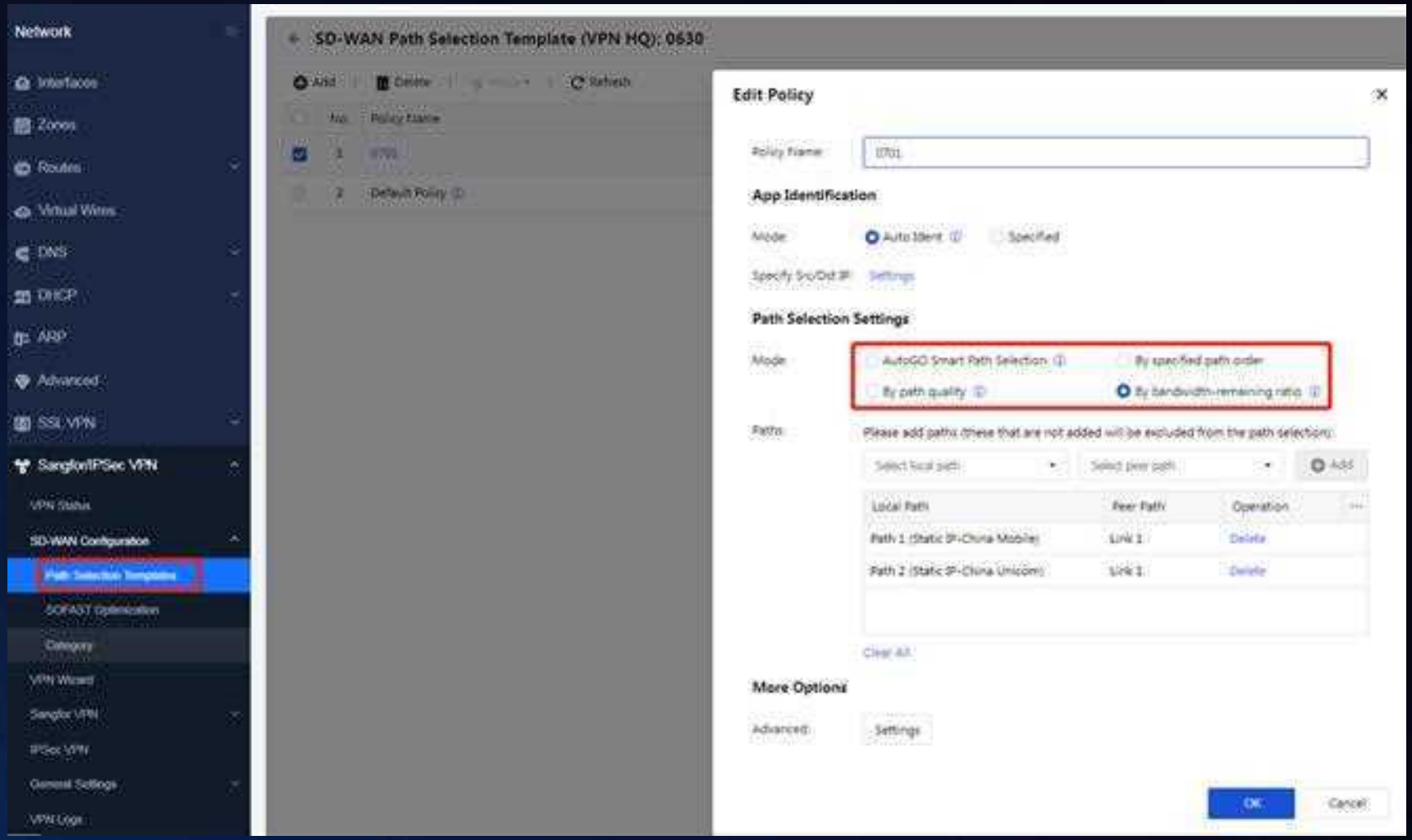
IPSec VPN

In Network Secure Platform, it supports establishing IPv6 IPSec VPN tunnels, where IPv6 can be selected as a protocol type.



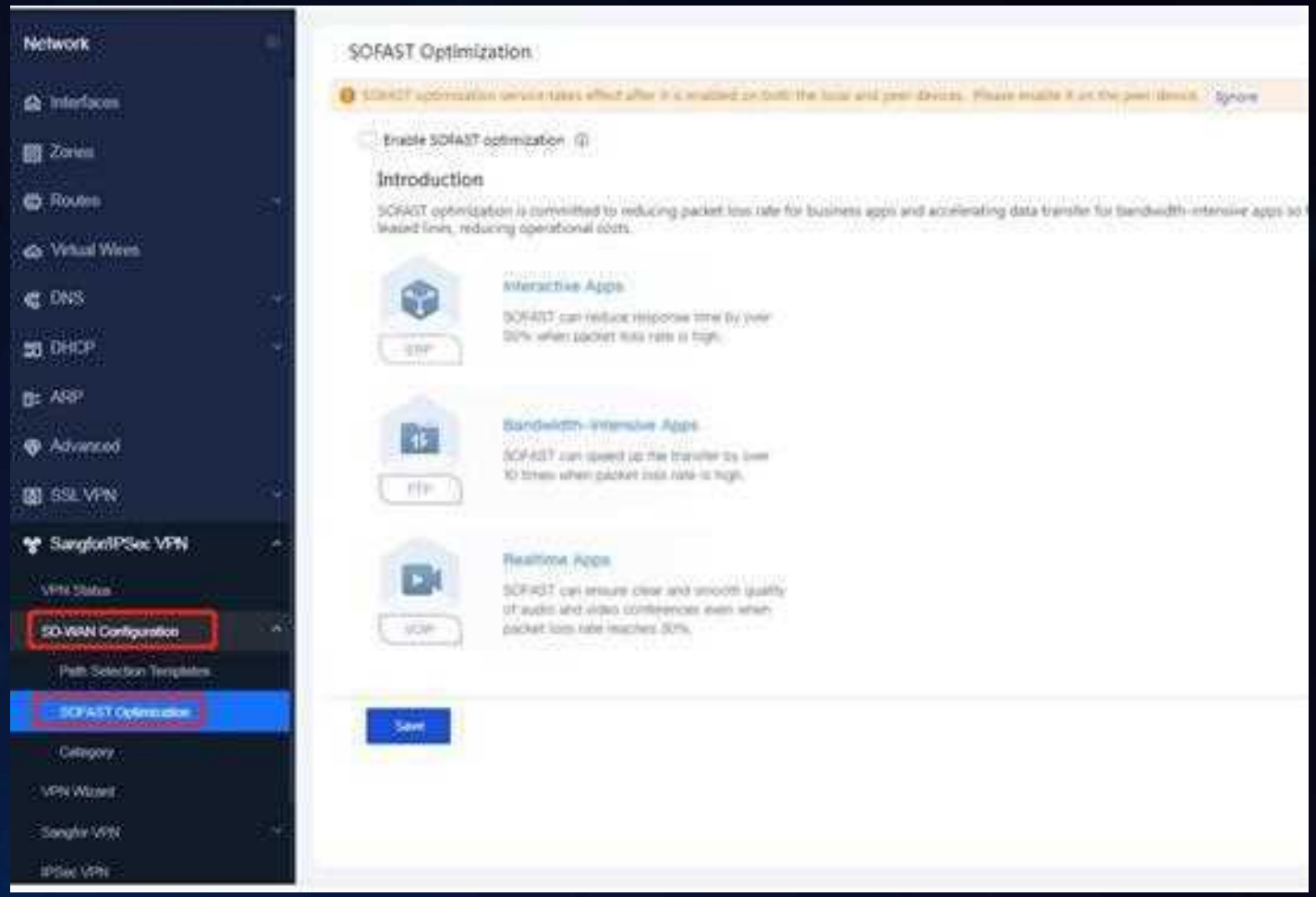
SDWAN Path Selection

In Network Secure Platform, it adds SDWAN path selection feature, which can provide the most suitable path for Sangfor VPN applications with path selection mode and path quality.



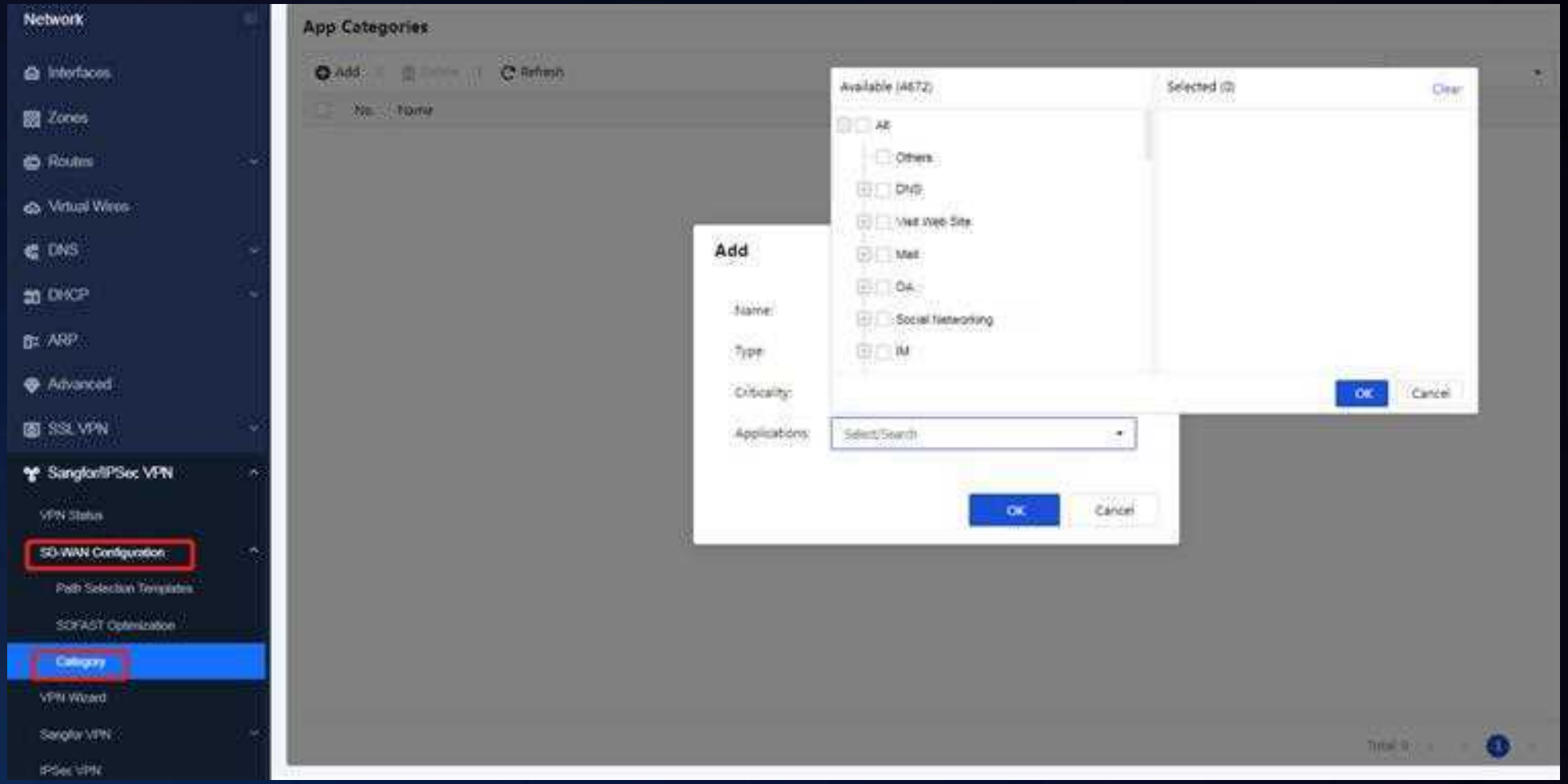
SOFAST Optimization

In Network Secure Platform, SOFAST optimization is committed to reducing packet loss rate for business apps and accelerating data transfer for bandwidth-intensive apps so that the user experience of using apps with data going through common lines can be almost the same as that provided by leased lines, reducing operational costs.



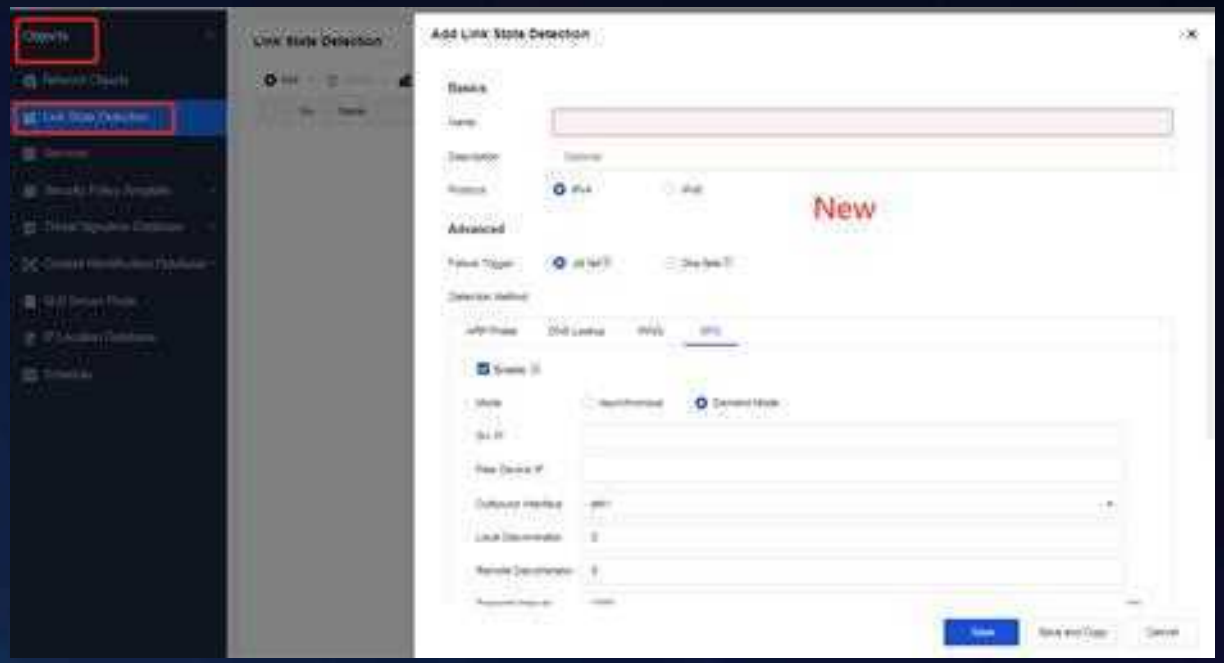
Application Category

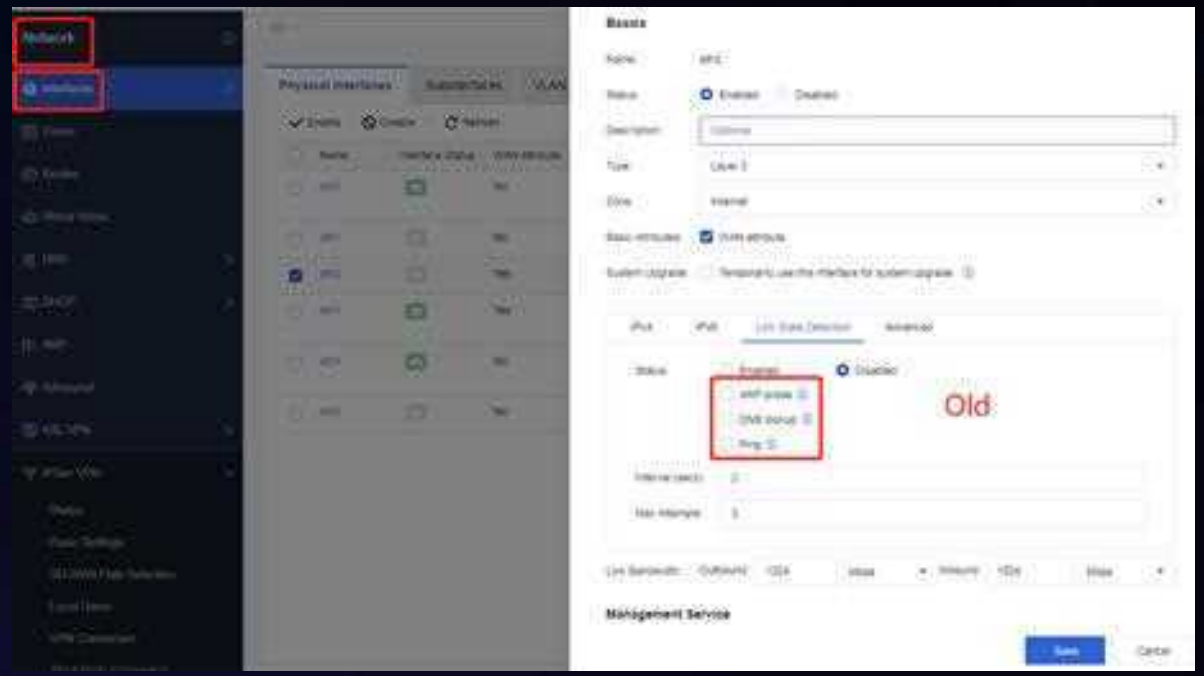
In Network Secure Platform, it add new application categories, and can define related business applications for reference in SDWAN path selection.



Link State Detection

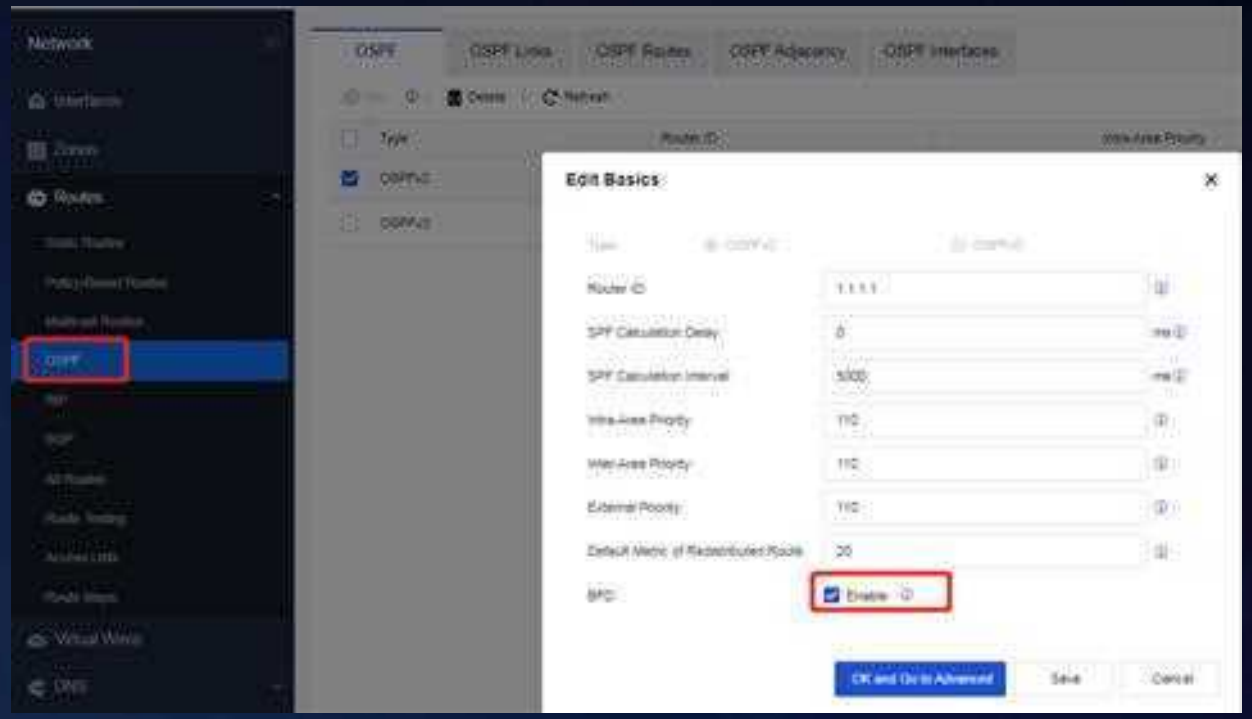
In Network Secure Platform, it adds a new menu page for link state detection, which allows configuration of link state detection for interfaces. Meanwhile, BFD link detection method has also been added.

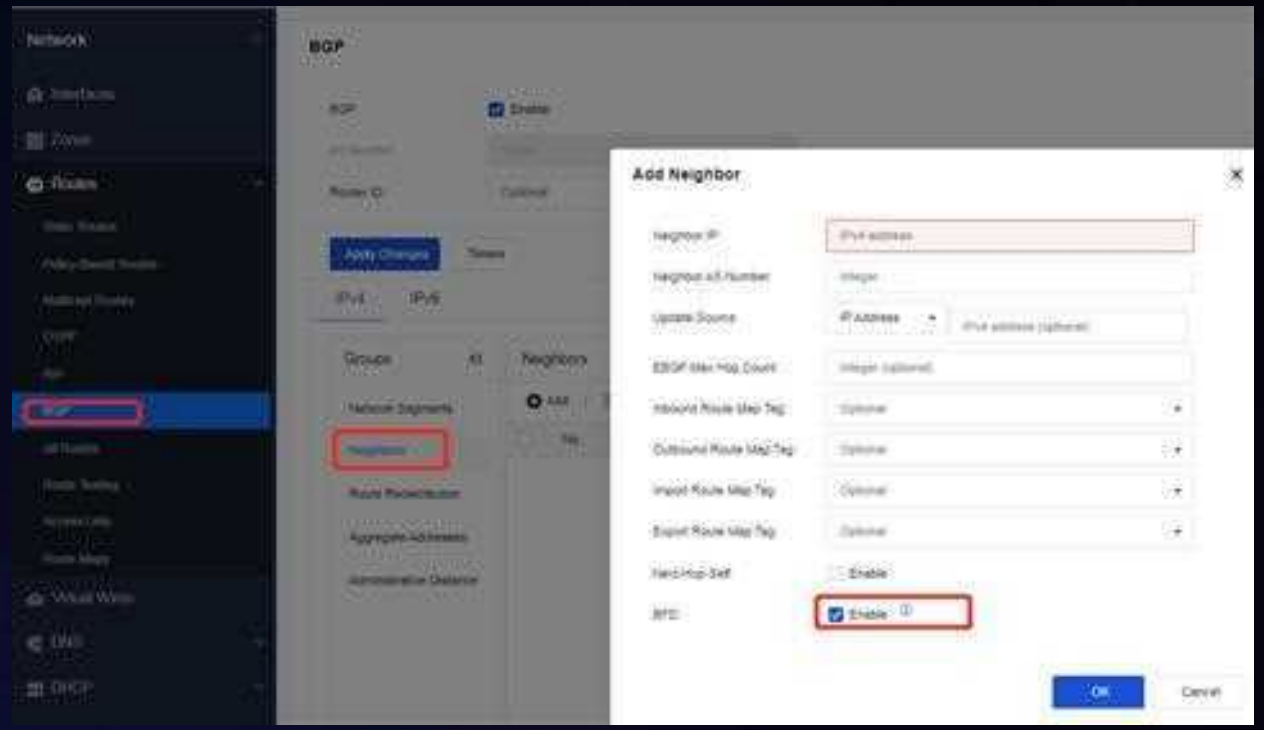




Link State Detection-Dynamic Routing

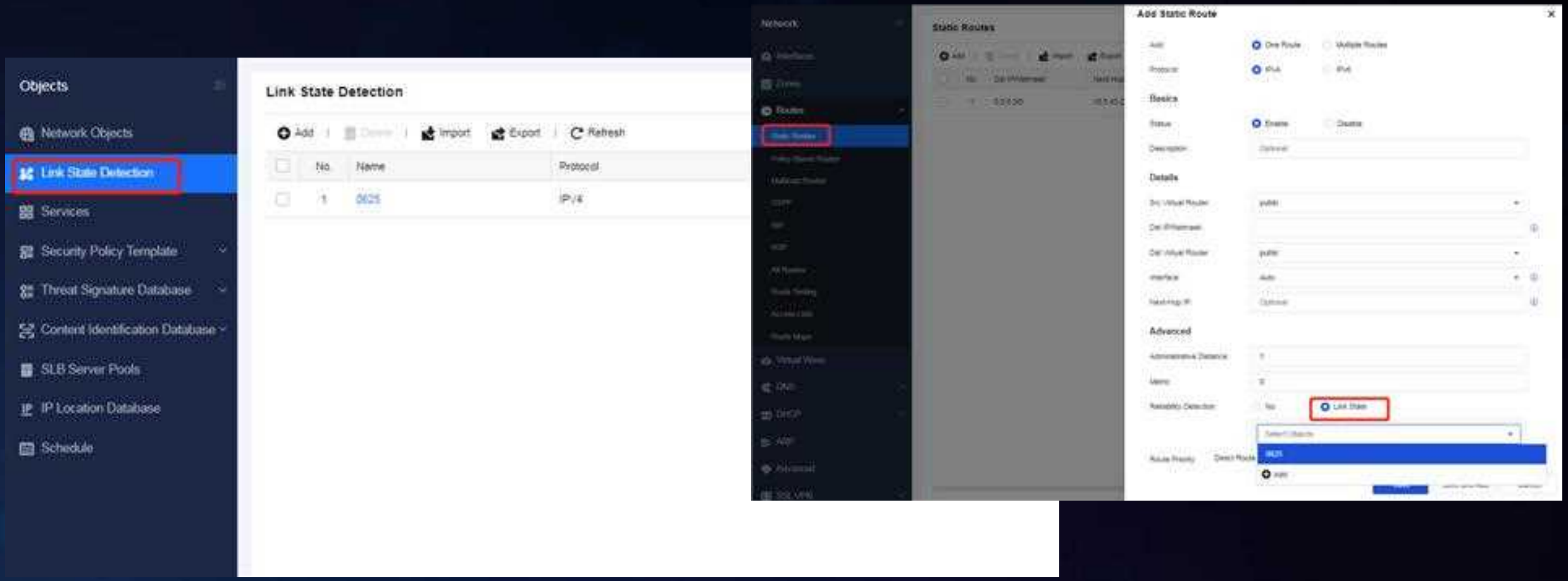
In Network Secure Platform, the BFD link detection is mainly used some scenarios, such as static routes, dynamic routes, and dual-machine configuration. After enabling the BFD function in dynamic routing setting, the corresponding global BFD configuration in those interfaces can be directly used..





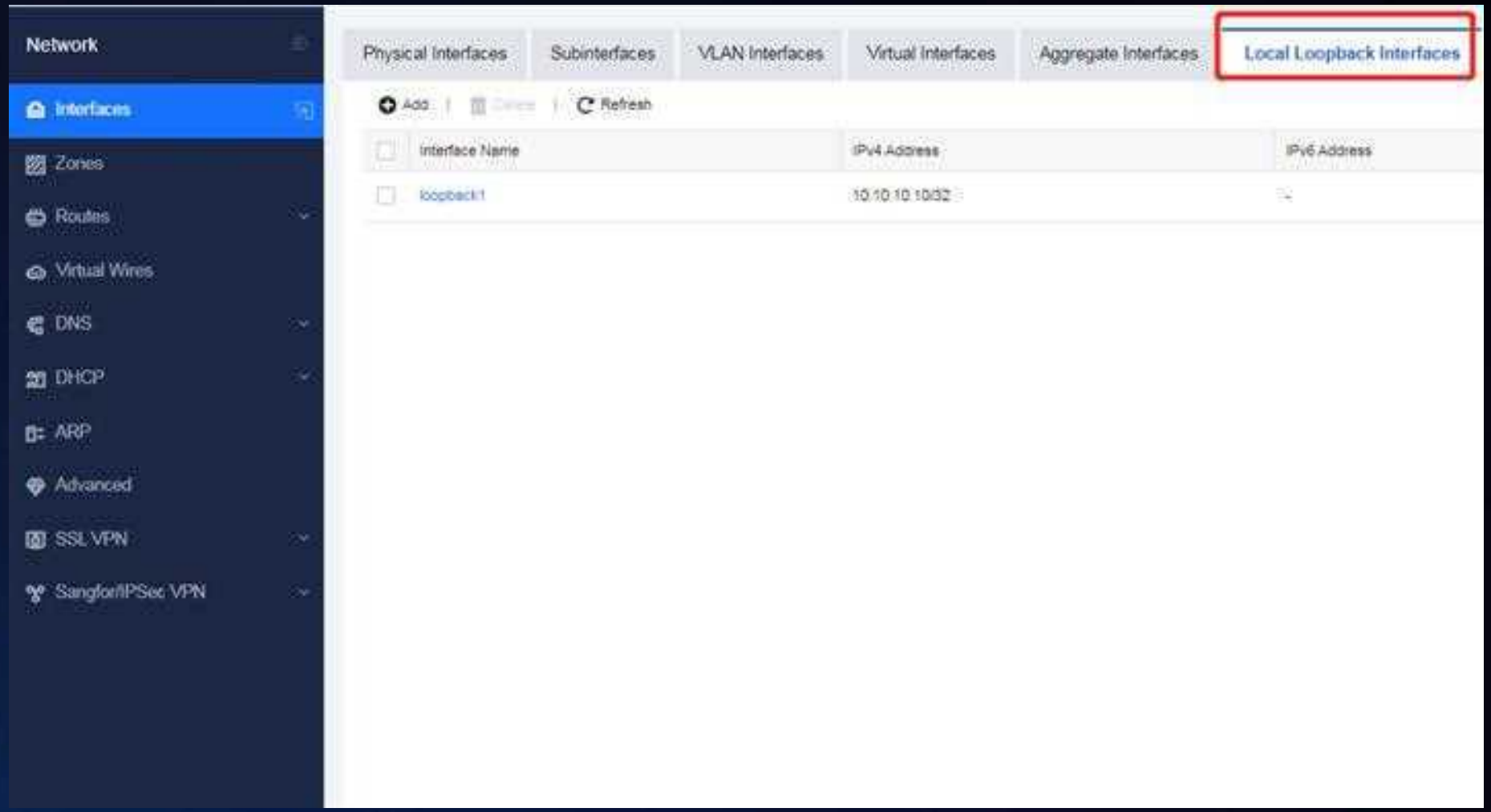
Link State Detection-Static Routing

Static routes can select global link state detection as well.



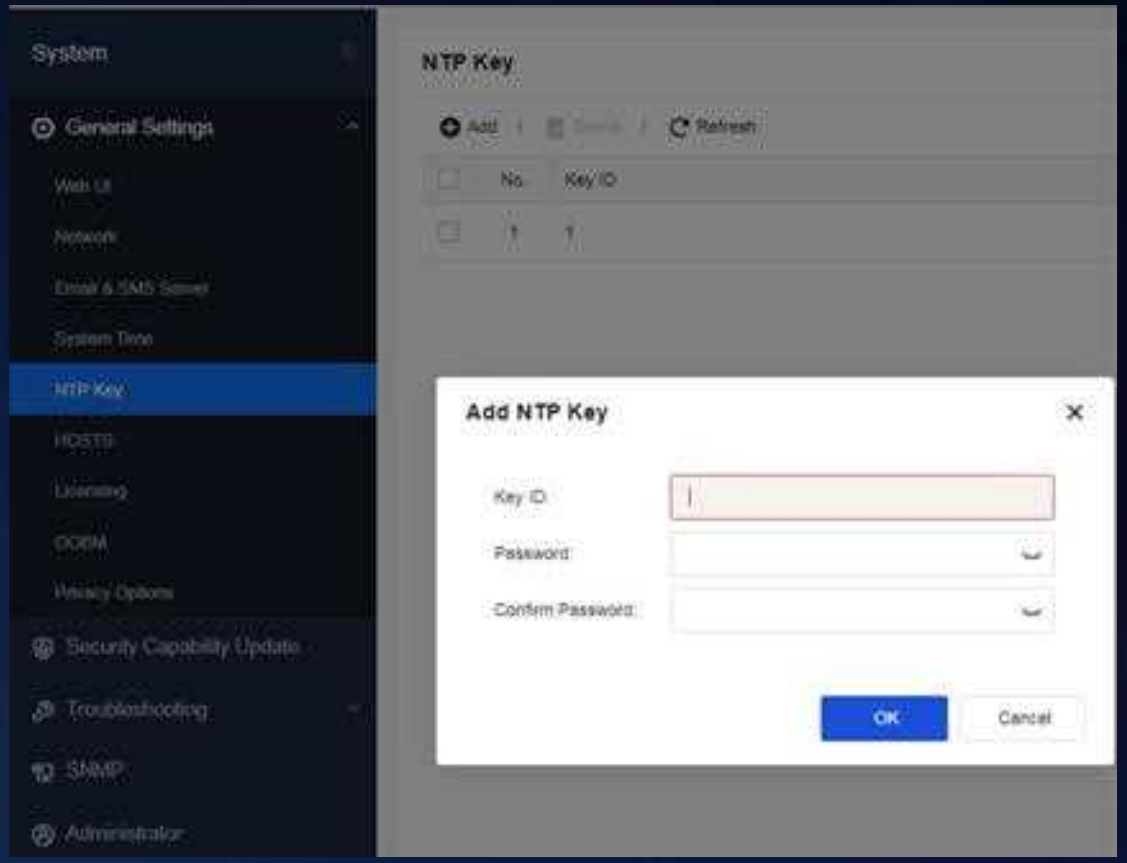
Local Loopback Interface

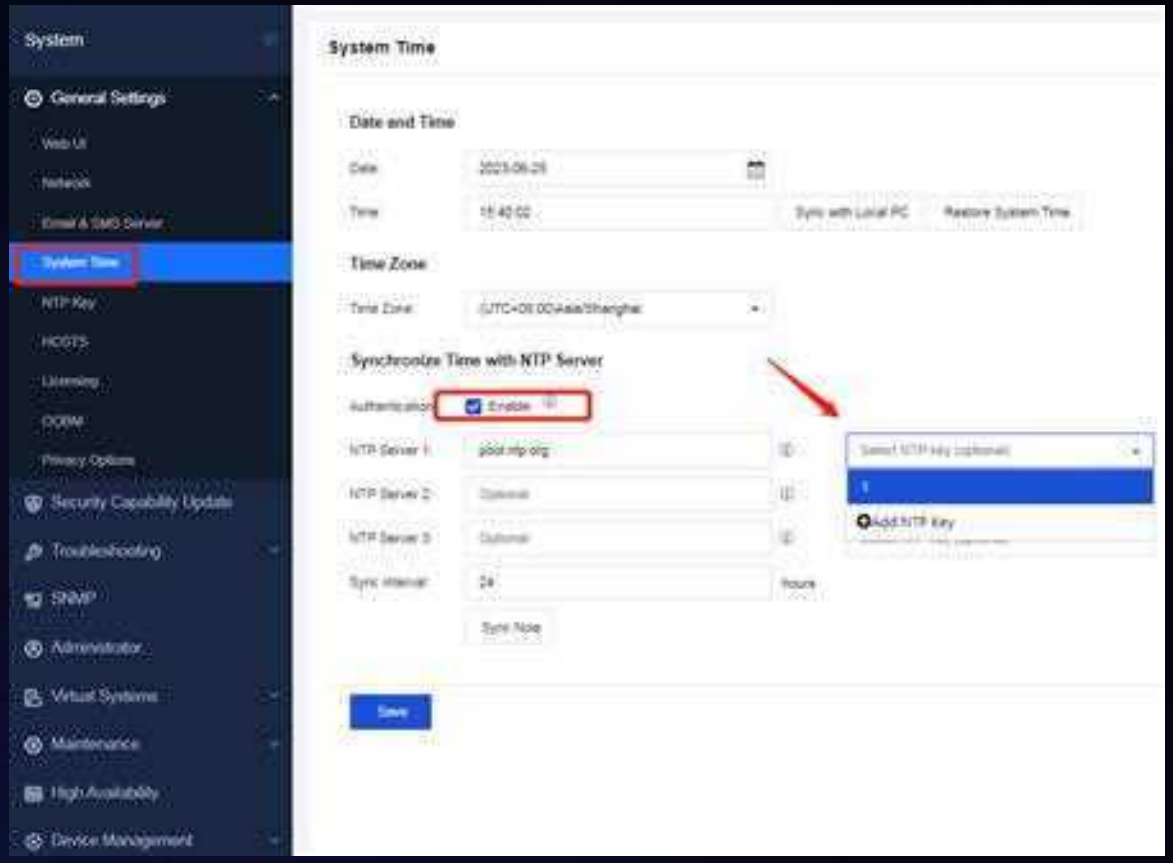
In Network Secure Platform, it adds the local loopback type interface which is an ordinary layer-3 interface and always up.



NTP Key

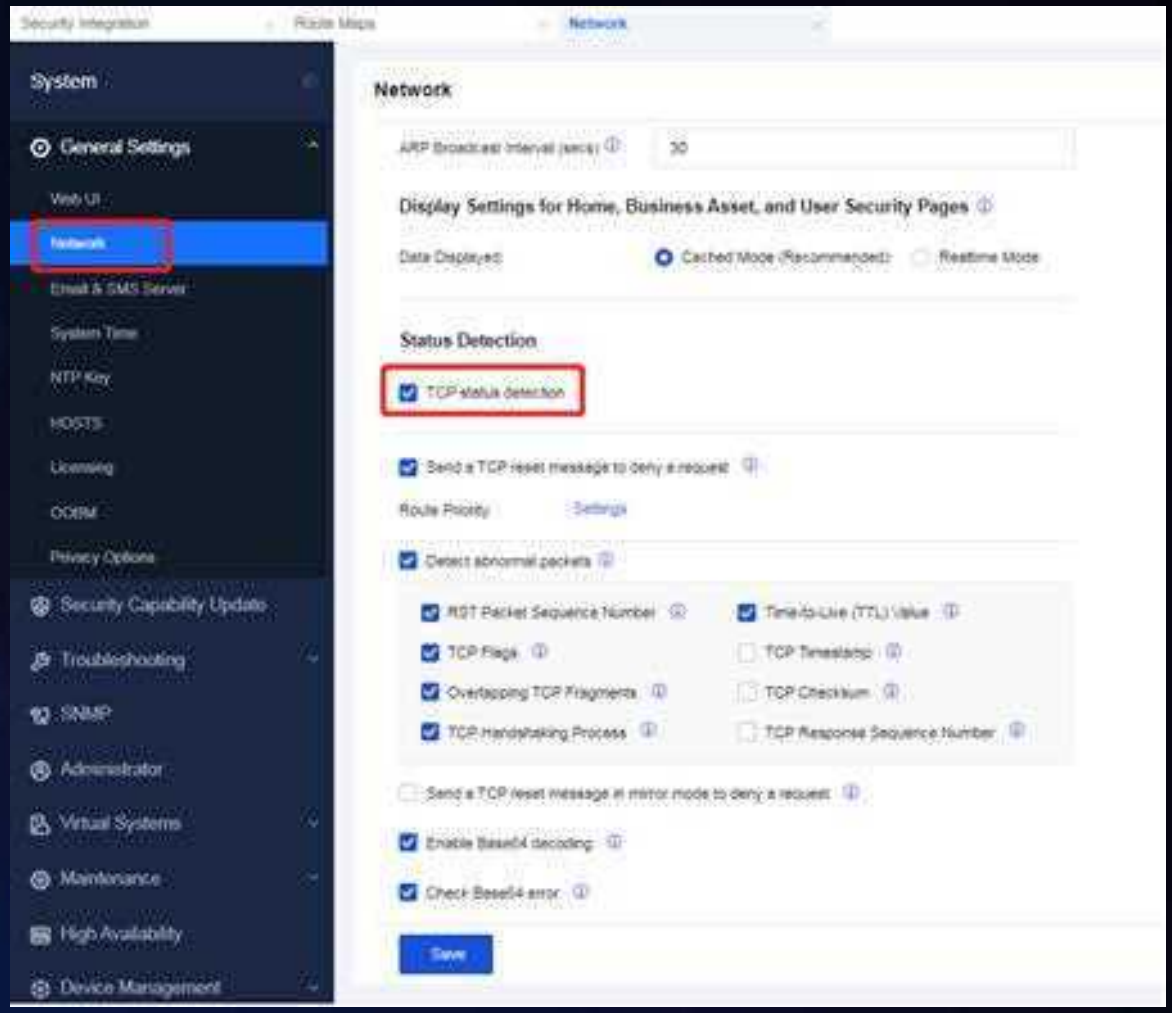
In Network Secure Platform, it adds NTP key feature which can meet the scenario of enabling NTP server authentication.





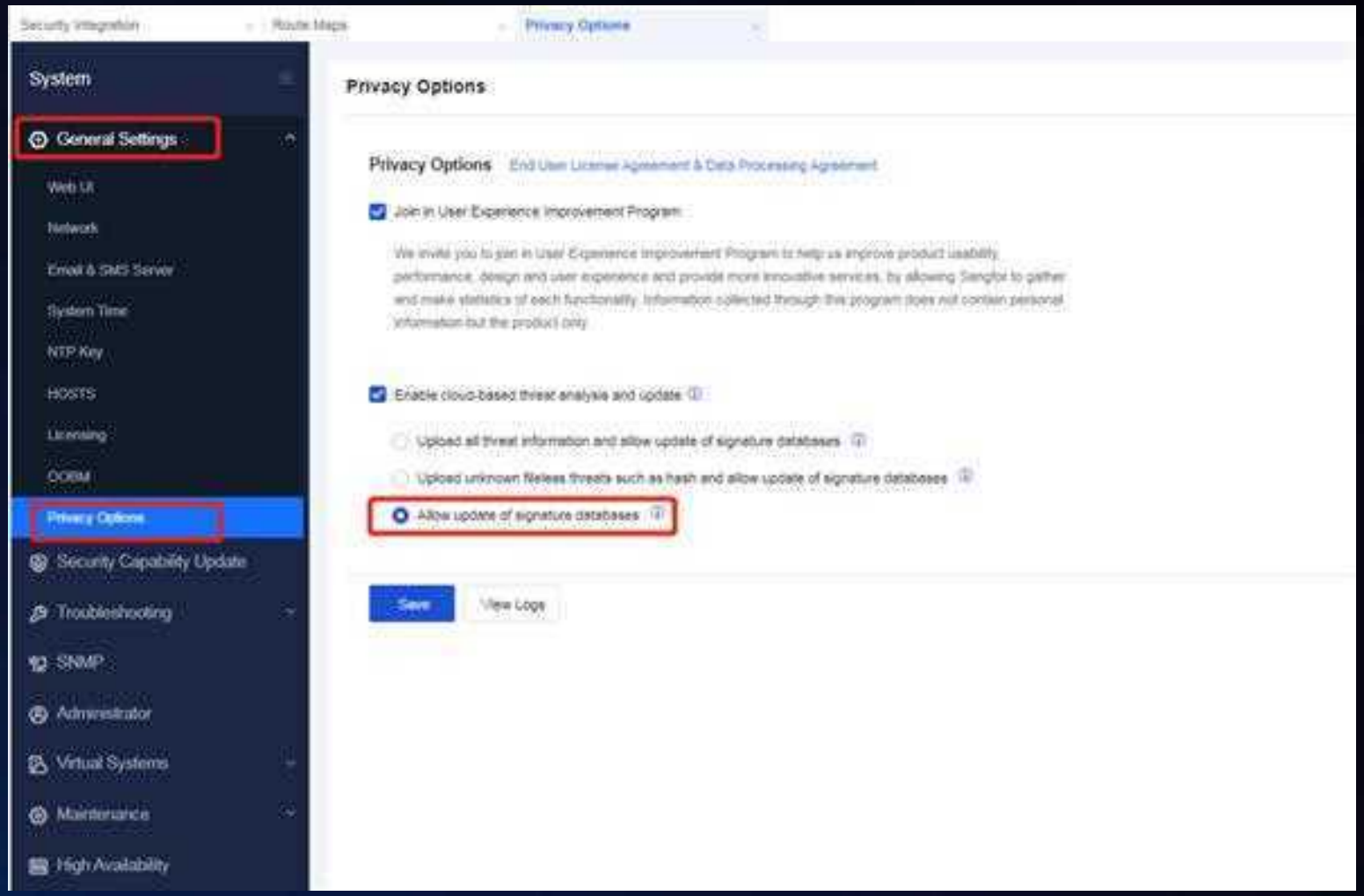
Network Parameter

In Network Secure Platform, it adds the global network parameter of TCP status detection, which checks the state of flag bits in the first TCP data packet transmitted through to TCP malformed packet attacks and enhance the security of TCP connections.



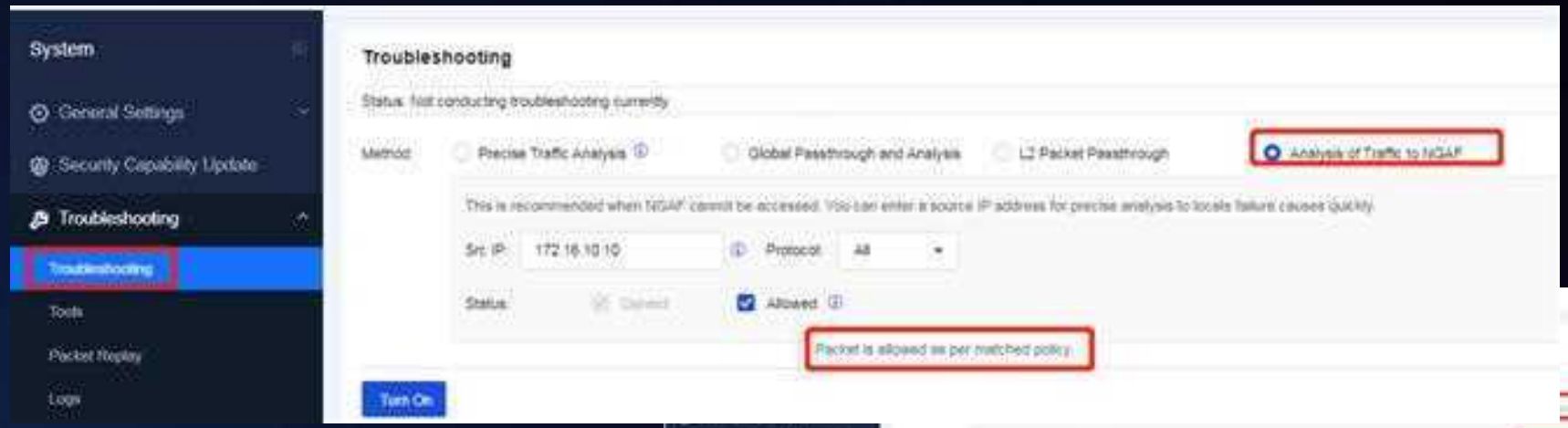
Privacy Options

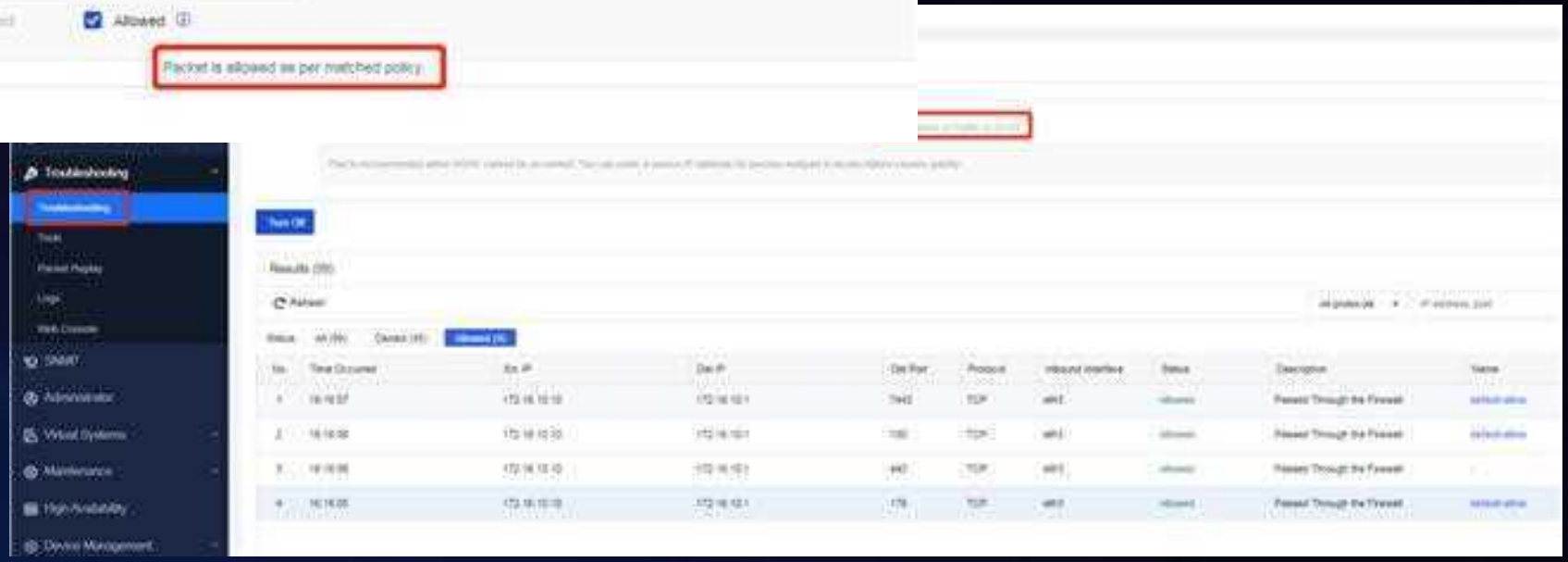
In Network Secure Platform, it adds the option of allowing update of signature databases, which can update local signature databases from cloud sites, but does not upload unknown threat information.



Analysis of Traffic to NGAF

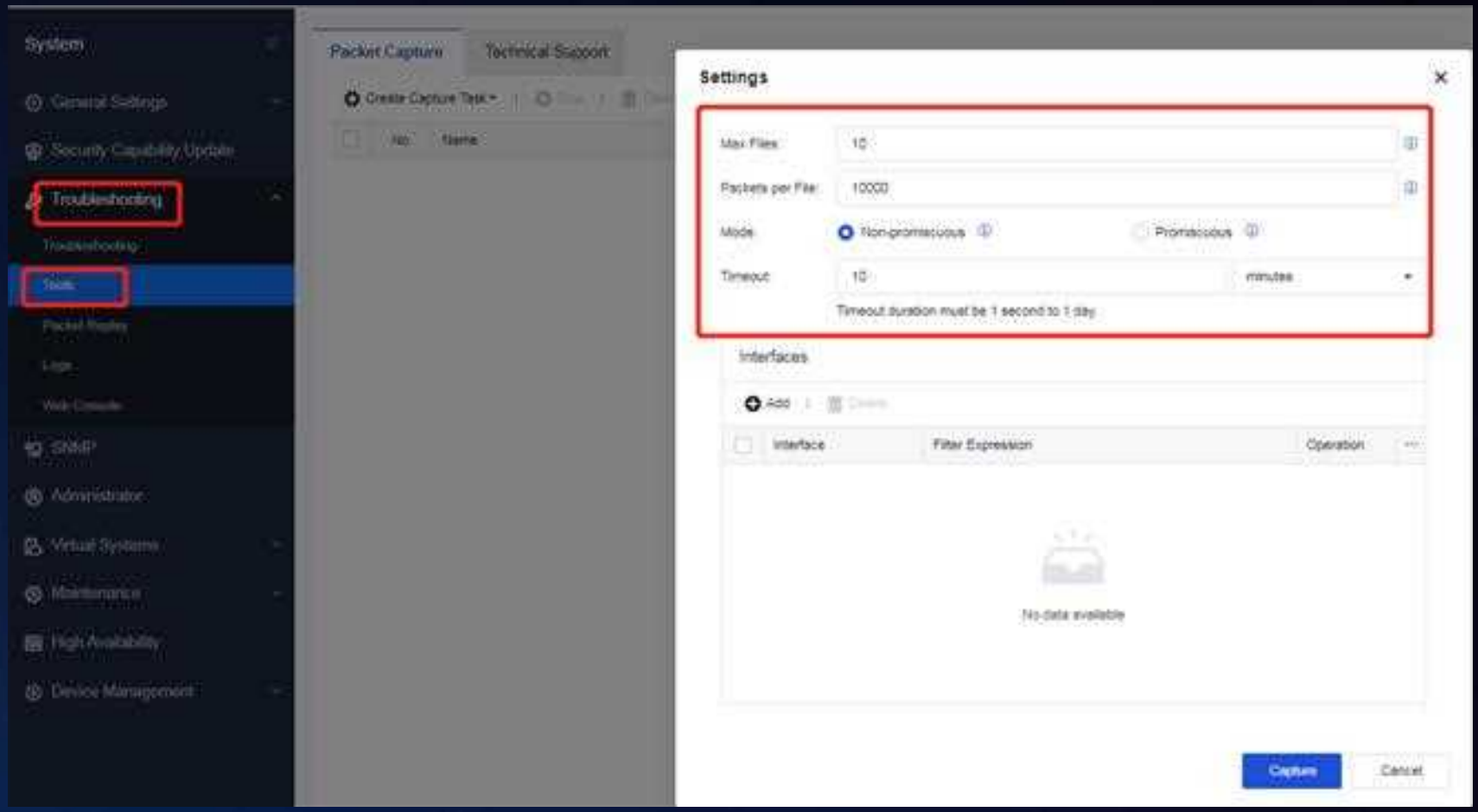
In Network Secure Platform, it adds analysis of traffic to NGAF feature, which has a separate local data stream analysis mode dedicated to inbound traffic analysis for traffic with destination address being the NGAF interface addresses.





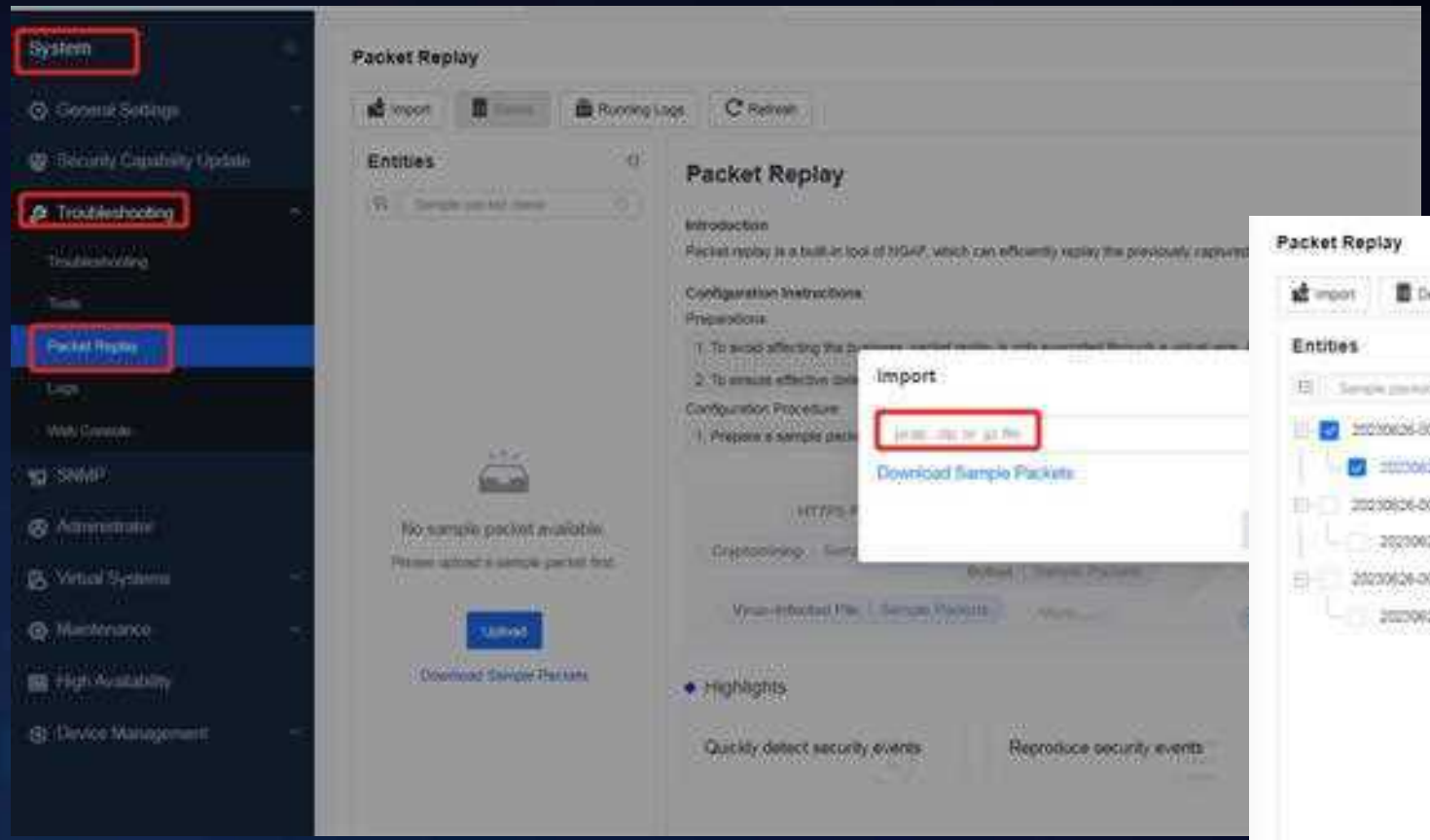
Rolling Capture Packet

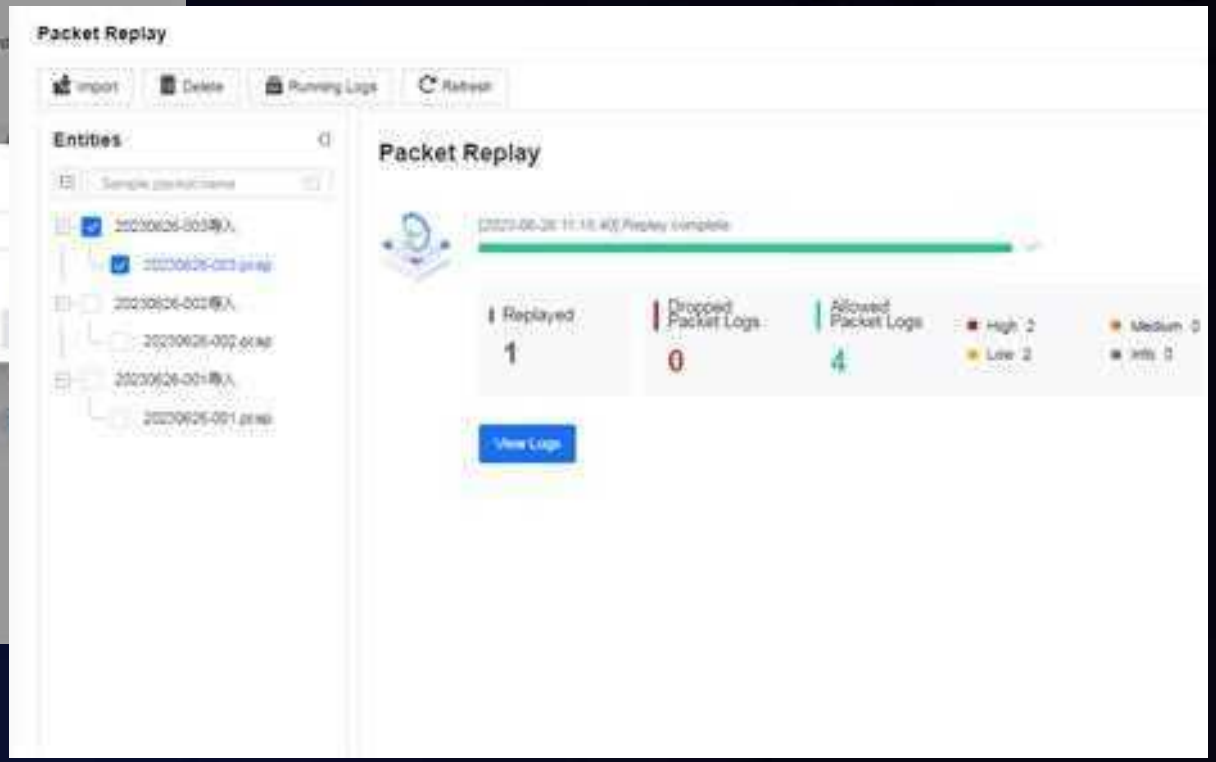
In Network Secure Platform, it adds rolling capture packet feature which is mainly used for troubleshooting intermittent network issues. Main settings of this feature contains max files and packets per file, and if the task exceeds max files counts it will delete earlier data. The timeout range is 24 hours and the task will stop after 24 hours even it is not performed in manual,



Packet Replay

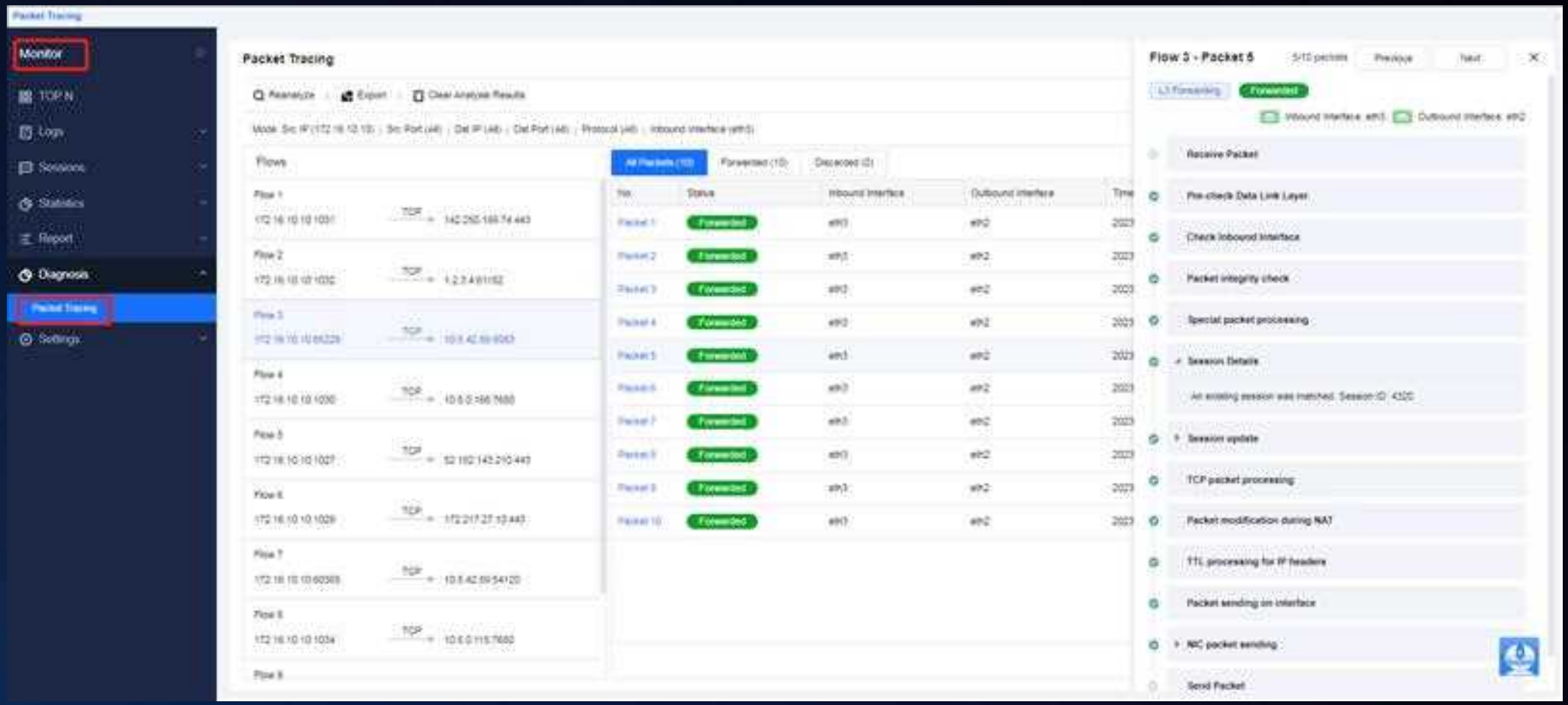
In Network Secure Platform, it adds packet replay feature which can restore network attacks and provide an useful tool for network forensics and verification.





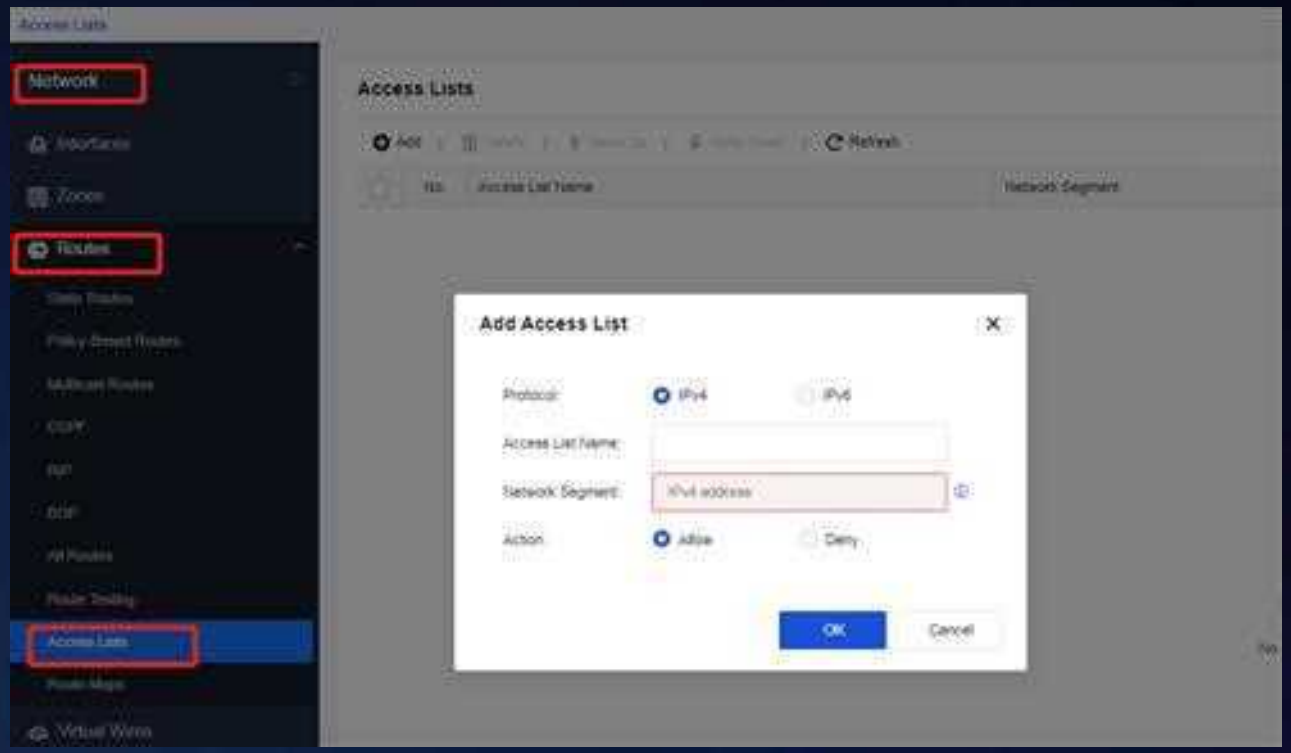
Packet Tracing

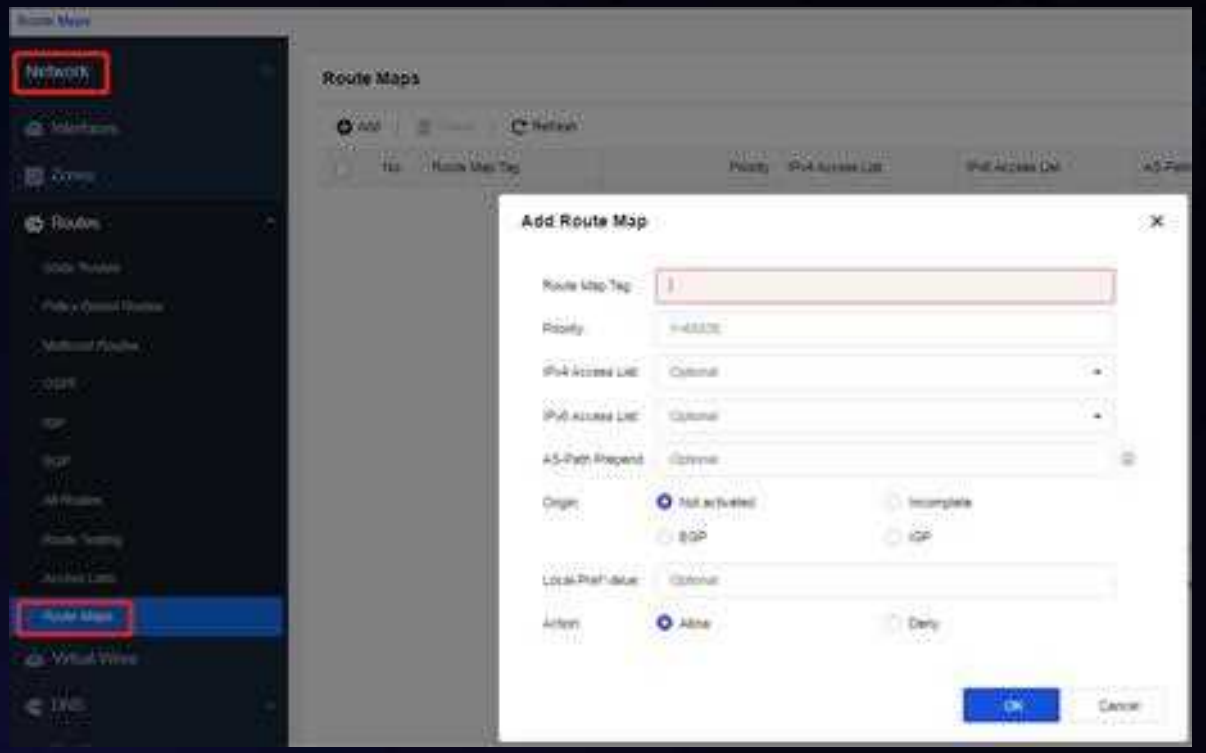
In Network Secure Platform, it adds packet tracing feature which can clearly illustrate the entire process of traffic being processed. This feature can benefit that not only how the traffic is processed for analysis from administrator, but also it can prove some evidence to adjust whether current configuration is reasonable or not, which is also a major enhancement regarding of the availability of NGAF and ease to end users.



Route Maps

In Network Secure Platform, it adds access list feature as a reference object for route maps. meanwhile it adds route maps feature to modify BGP route attributes.



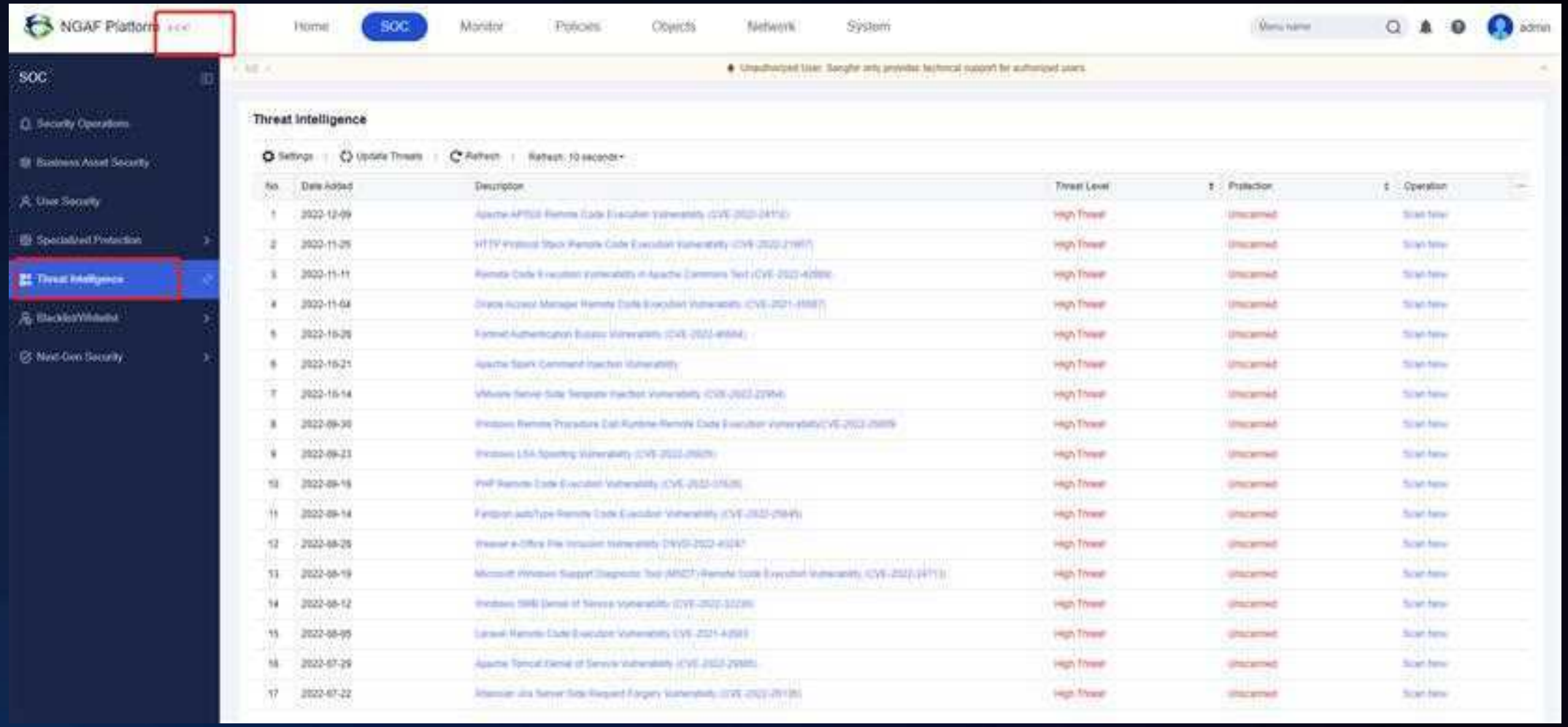


PART 4

Permanently Deleted Feature in Network Secure Platform(Compared to 8.0.47 version)

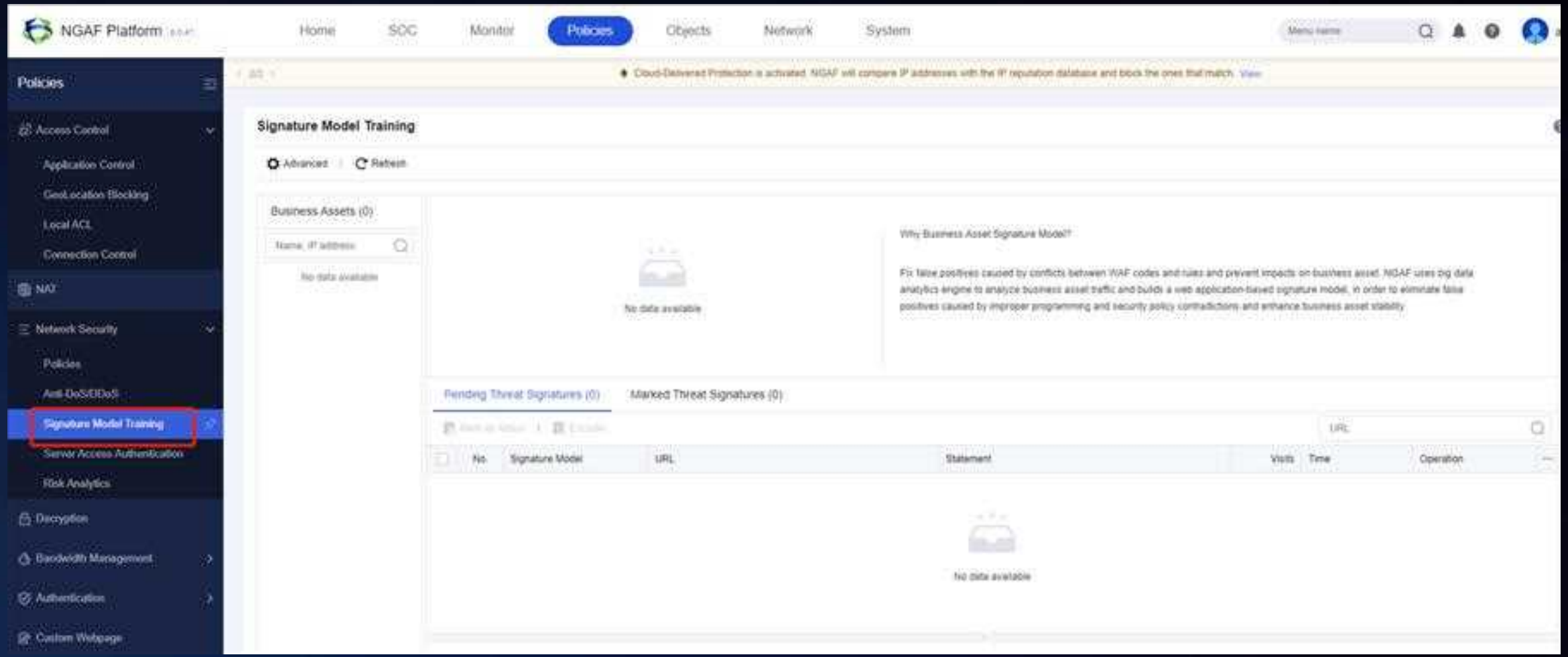
Threat Intelligence

In Network Secure Platform, it deletes the Threat Intelligence module.



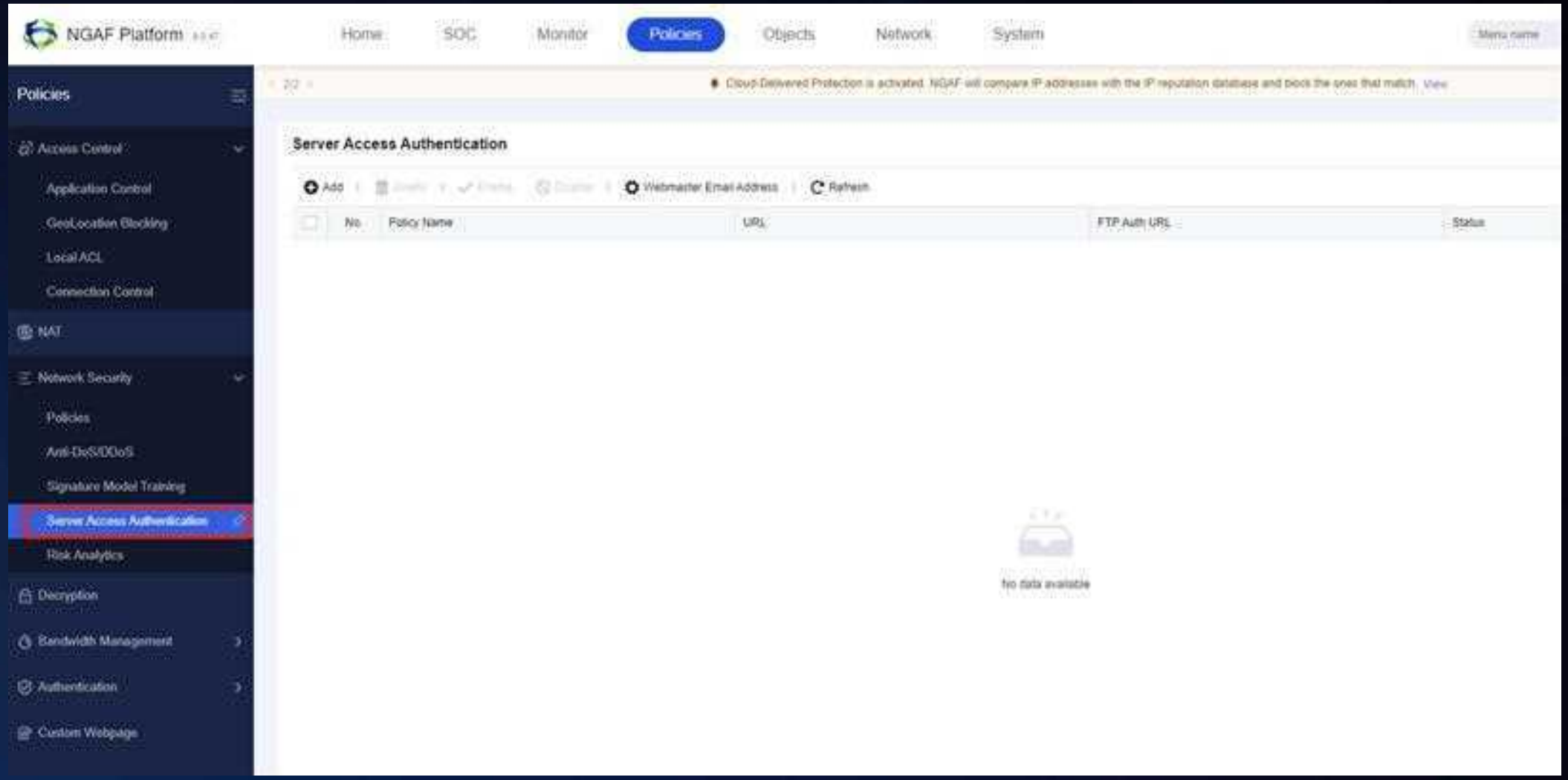
Signature Model Training

In Network Secure Platform, it deletes the Signature Model Training module.



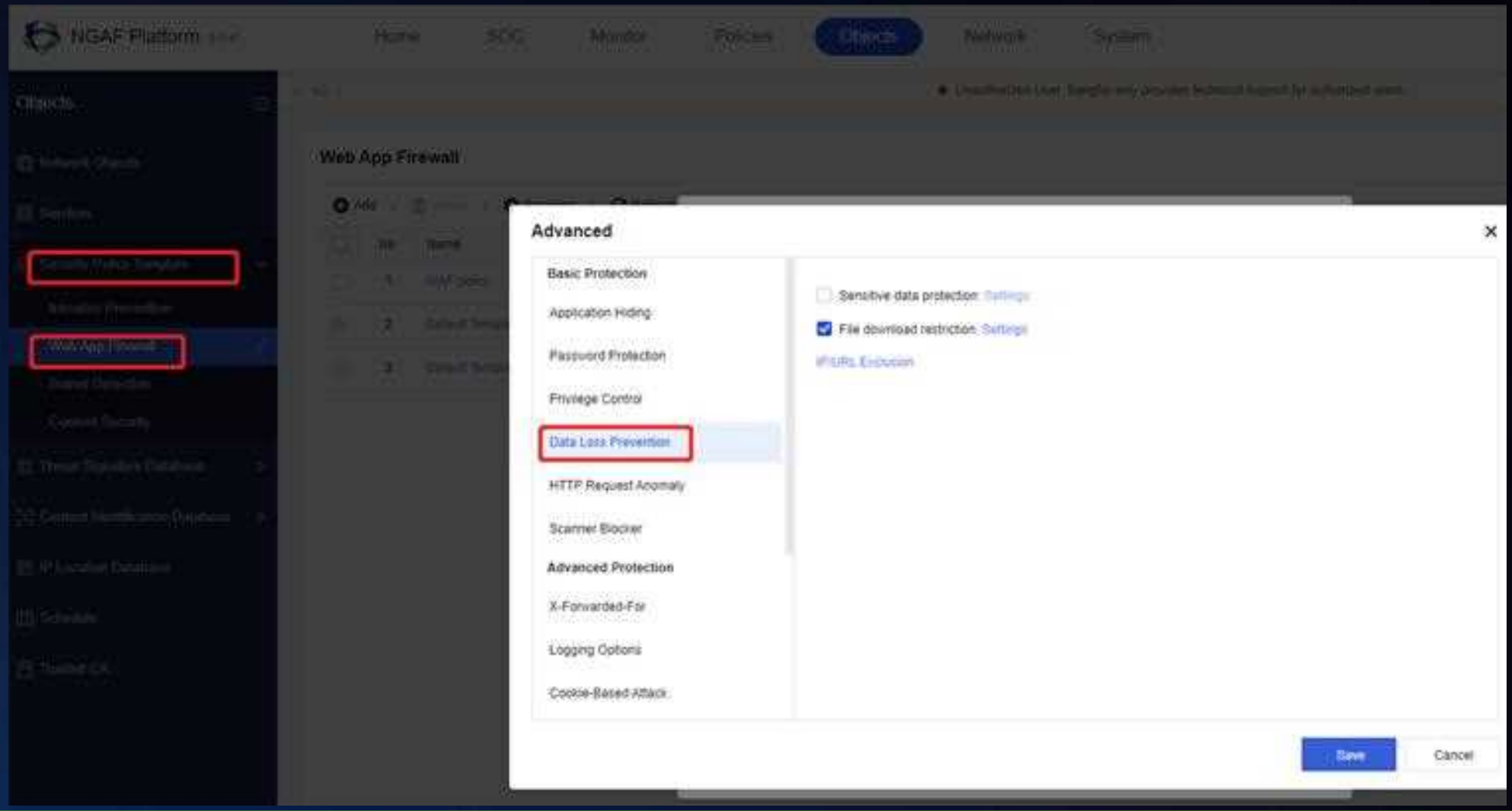
Server Access Authentication

In Network Secure Platform, it deletes the Server Access Authentication module.



Server Access Authentication

In Network Secure Platform, it deletes the Data Loss Prevention module.



SANGFOR

THANK YOU