



Network Secure Platform 8.0.85

New Version Technical Training

By John.Qiao



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

- 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 upgraded to Network Secure Platform.

Why needs Network Secure Platform



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.

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



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.



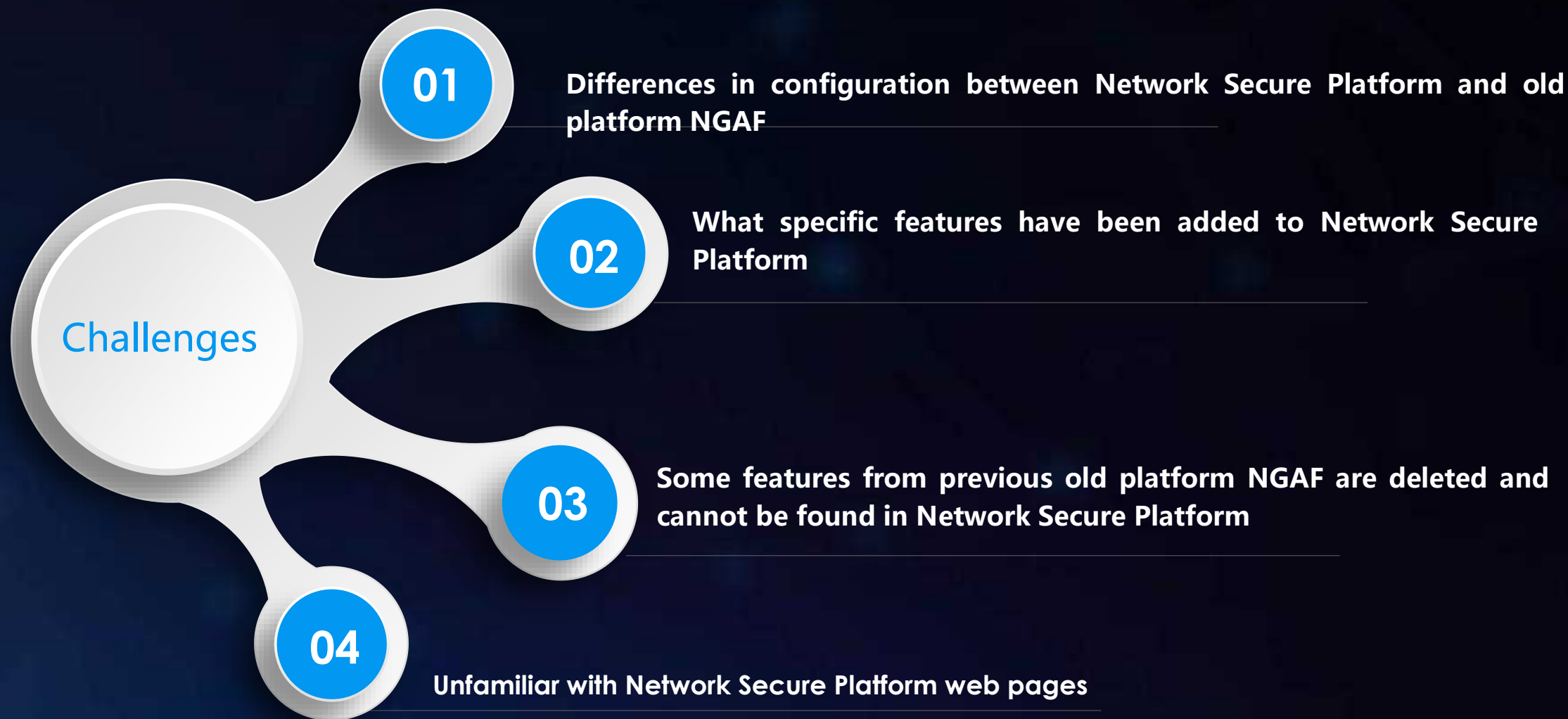
Providing a unified and shared underlying platform

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.

The Challenges of Network Secure Platform Delivery



PART 2

Main Feature Difference (compared to 8.0.47 version)

Layer-2 Port-ACCESS Type Port Processing Logic

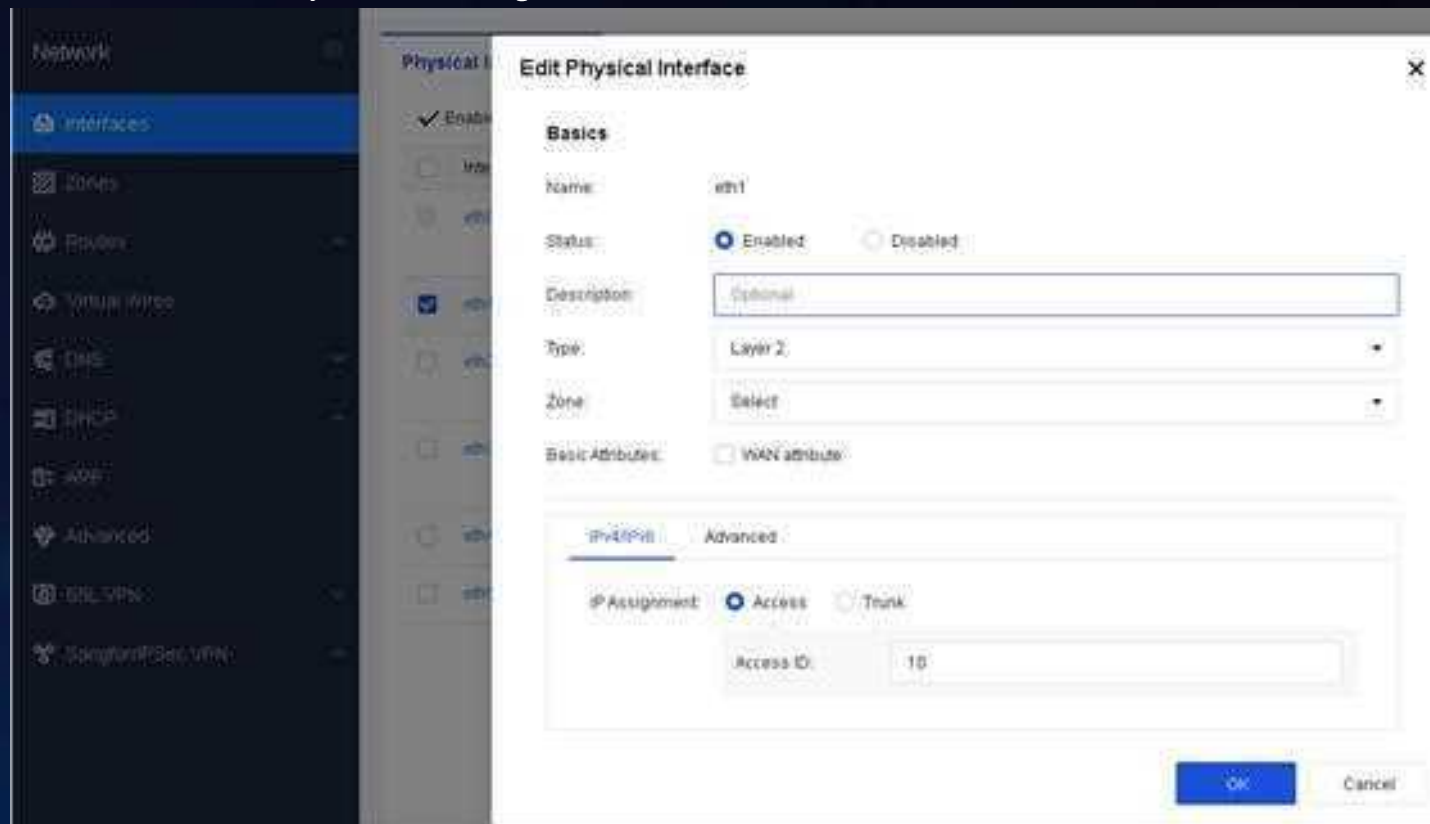


Old platform NGAF processing method:

- ◆ 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

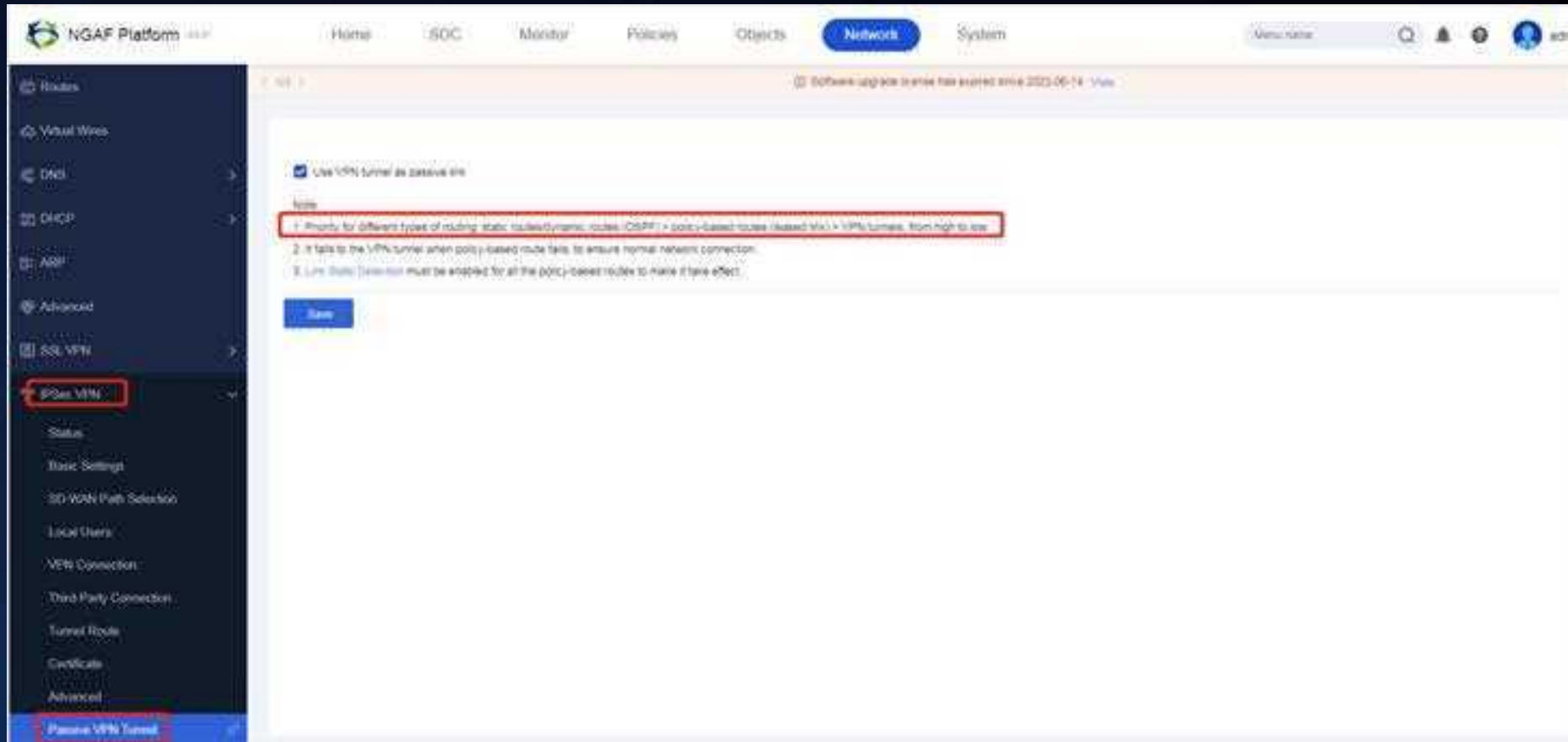


Situation 1: Default route types priority

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

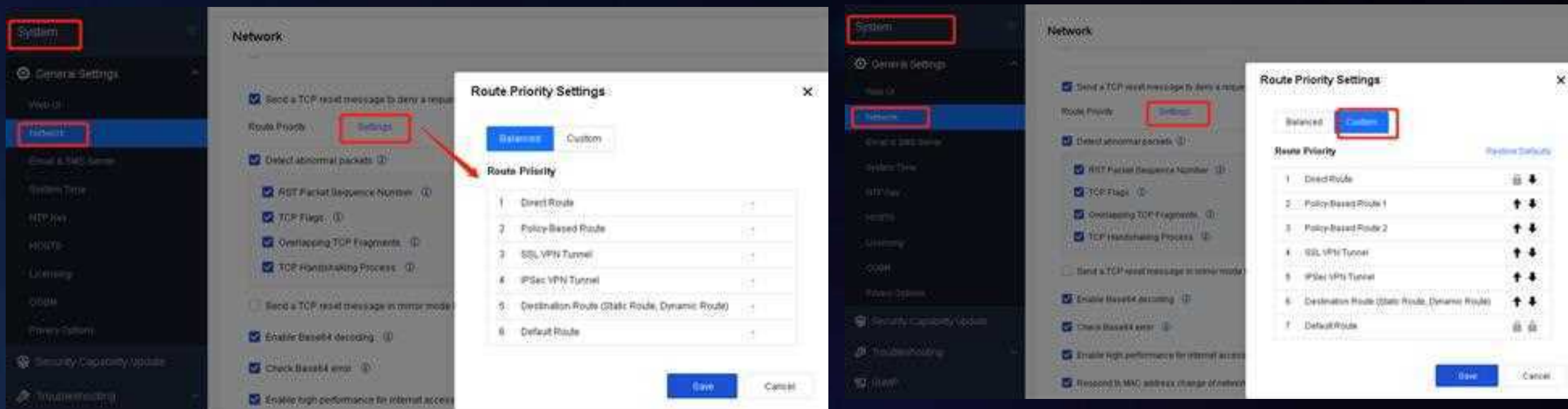


Situation 1: Default route types priority

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 divided 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.

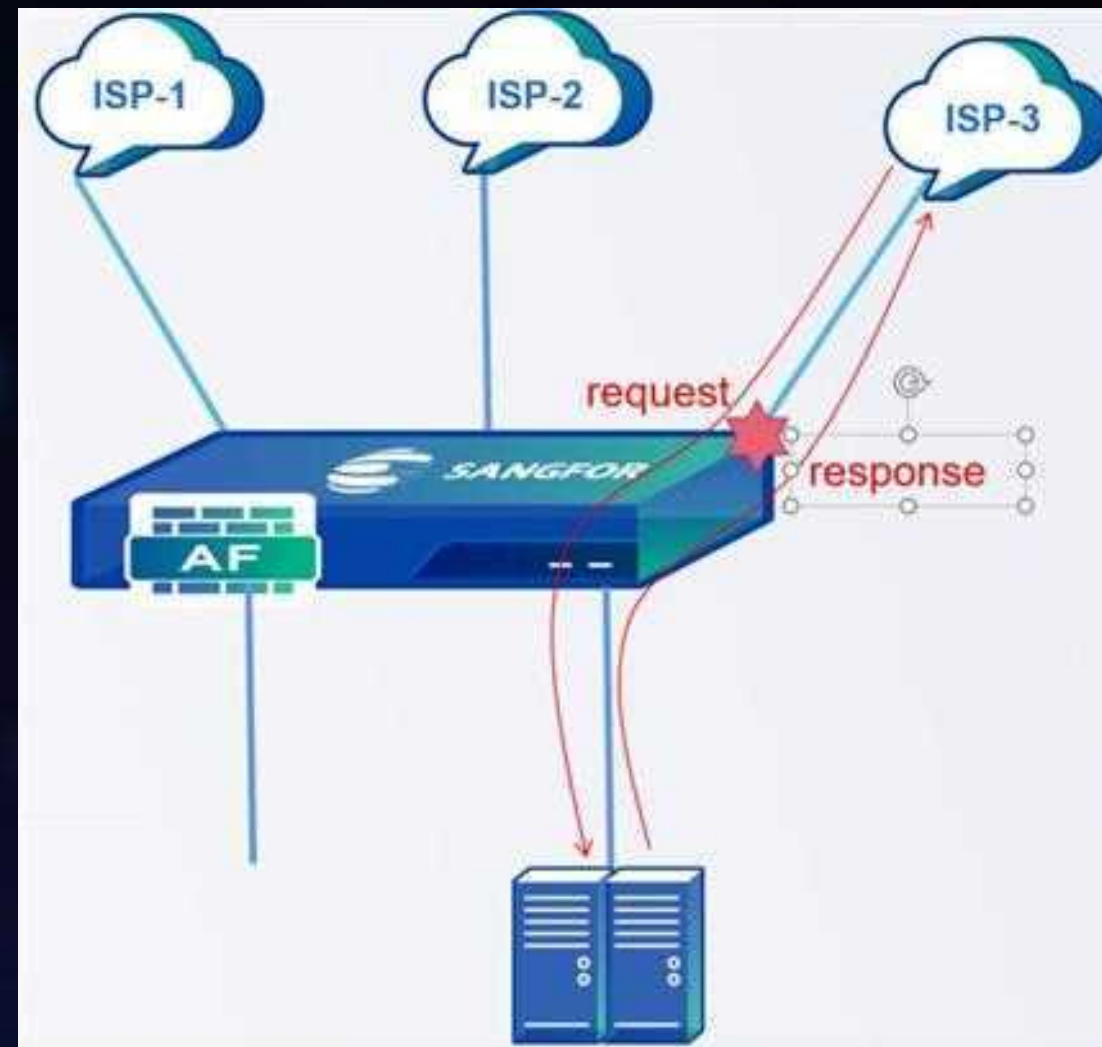


Reverse Routing---Old Platform NGAF



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.

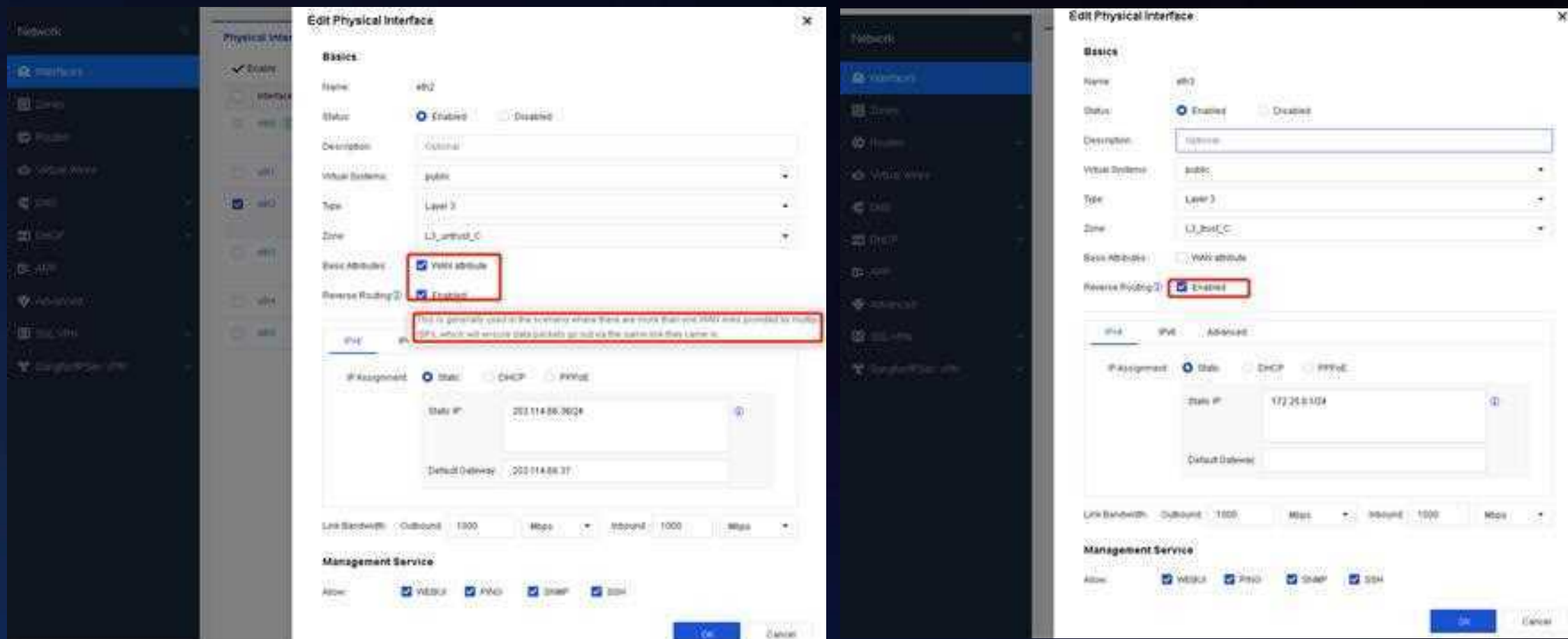
The screenshot displays the Sangfor NGAF web interface. On the left, a sidebar menu shows 'Network' > 'Interfaces'. The main panel is titled 'Policy-Based Routes' and contains a table of configured routes. A red box highlights the 'eth2' interface in the 'Interface-Next-Hop IP' column of the first row. Another red box highlights the 'eth2' interface in the 'Basic Attributes' section, where the 'Reverse Routing' checkbox is checked. Below this, the 'IP Assignment' section shows 'Static IP' as '5.5.5.100' and 'Next-Hop IP' as '5.5.5.2'.

No.	Name	Protocol	Src Zone	Src Address	Dest Address/Region	Services	Applications	Interface-Next-Hop IP	Load Balancing Method	Schedule	Link State	Status
1		any						eth2 5.5.5.2		All week	Not detected	✓
2		any						eth2 44.44.44.44.2		All week	Not detected	✓
3		any						eth2 33.33.33.33.2		All week	Not detected	✓

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 manual.



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.

The screenshot displays the 'Static Routes' configuration page in the Network Secure Platform. The left sidebar shows the 'Network' menu with 'Static Routes' highlighted. The main content area shows a table of static routes with two entries, both highlighted with a red border. The table has columns for No., Dest IP/Netmask, Next-hop IP, Administrative Distance, Interface, Metric, Reliability Detection, Validity, Status, Description, and Operation. The two routes are:

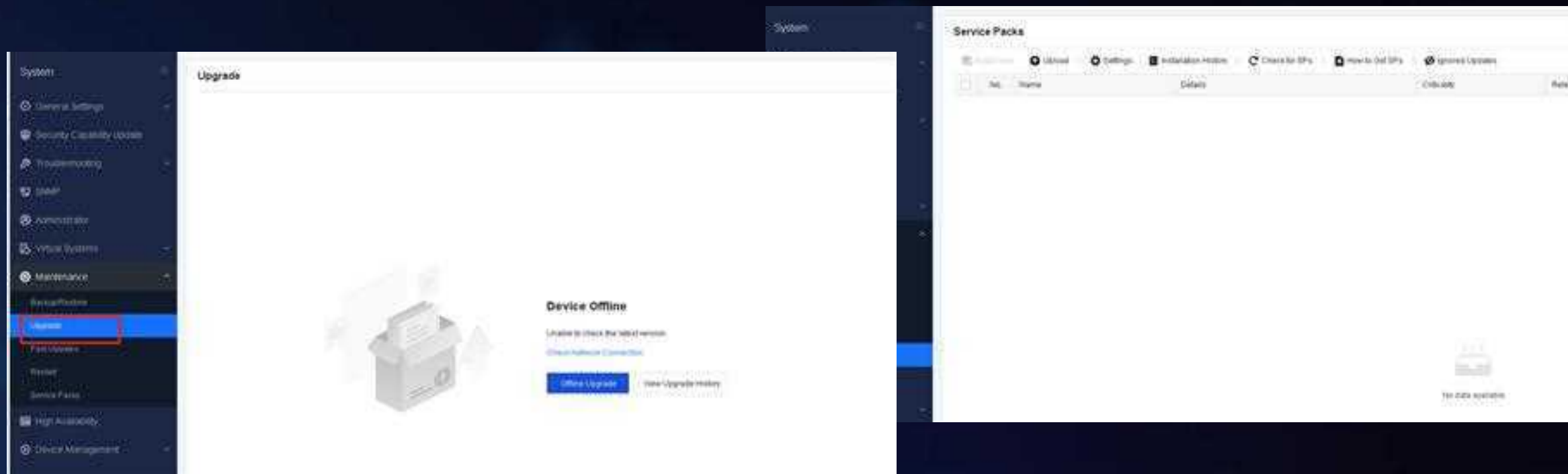
No.	Dest IP/Netmask	Next-hop IP	Administrative Distance	Interface	Metric	Reliability Detection	Validity	Status	Description	Operation
1	99.99.99.0/30	3.3.3.2	1	Auto	0	-	Valid	✓	-	Edit Delete
2	99.99.99.0/30	4.4.4.2	1	Auto	0	-	Valid	✓	-	Edit Delete

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.

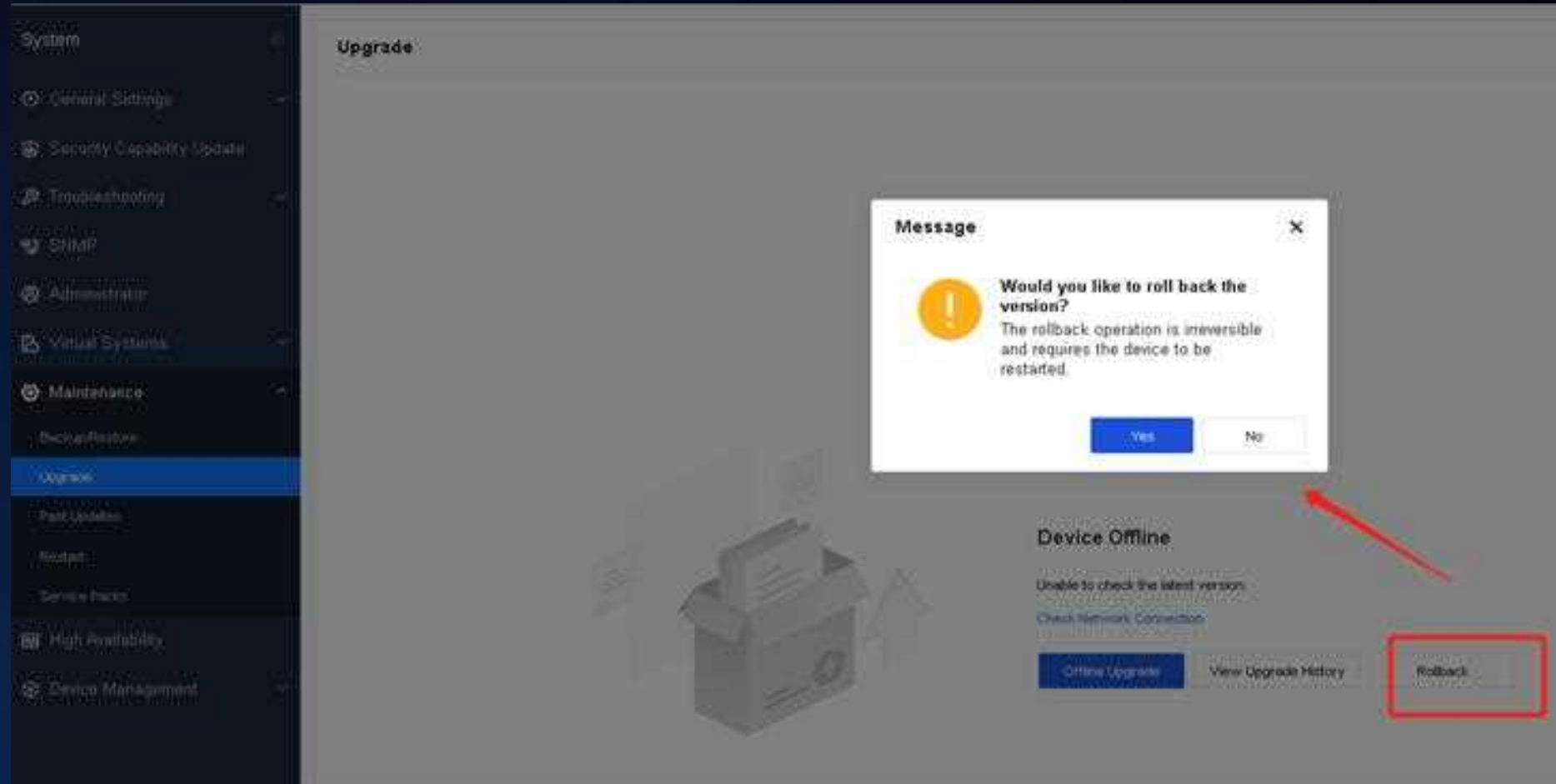


- It is unnecessary to stop and separate the high availability configuration in active/standby mode when you plan to upgrade the system version, compared to the old platform NGAF. You are instructed to upgrade the standby device firstly, and then perform the switchover, and then upgrade the new standby 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 automatically which depends on specific service packs.

Rollback---Network Secure Platform



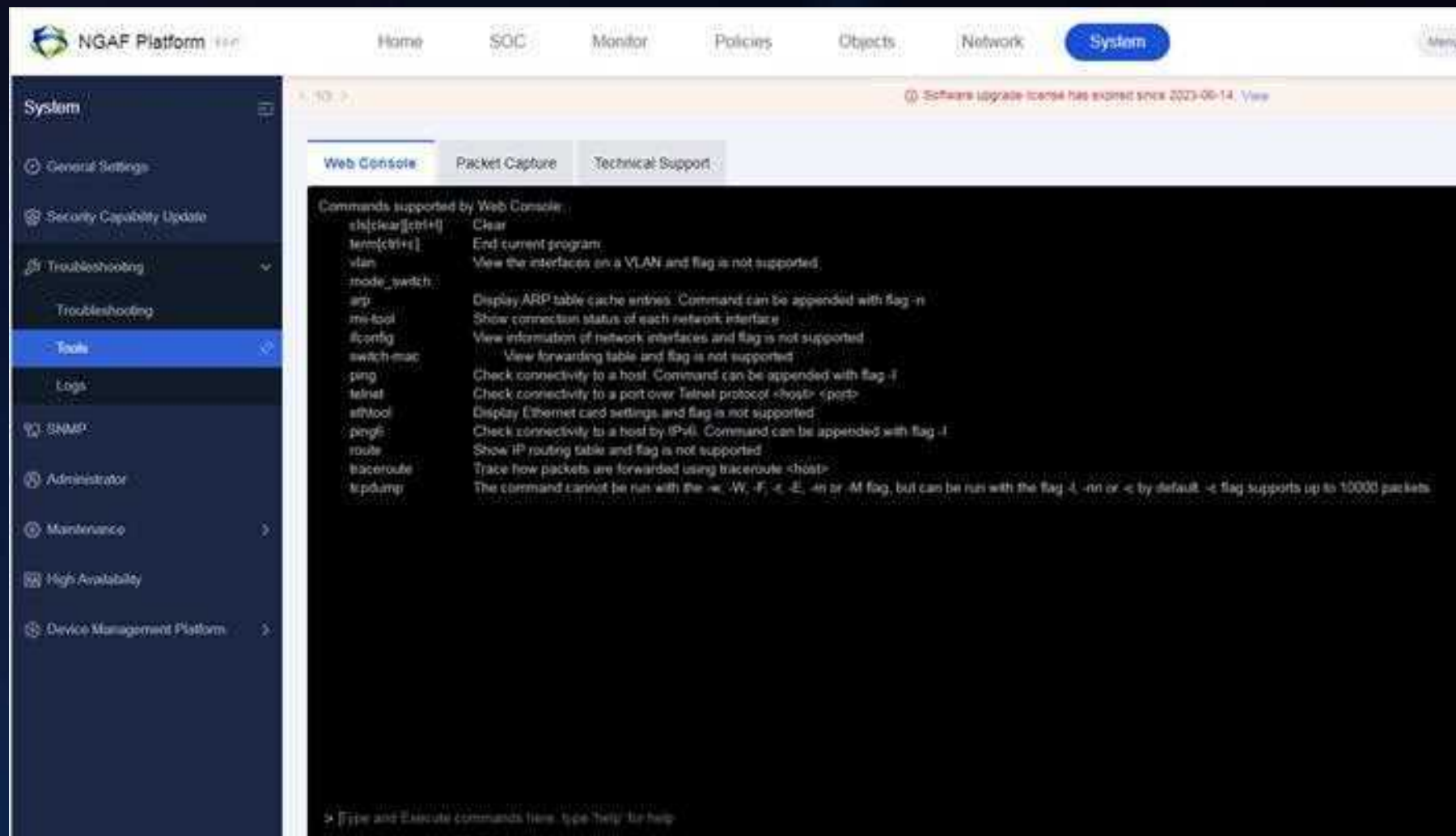
The Network Secure Platform supports version and service pack rollback, allowing you to roll back to the previous version or service pack before the upgrade was completed. Any configurations made on the new version or service pack will be cleared. After you perform version or service pack rollback, the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

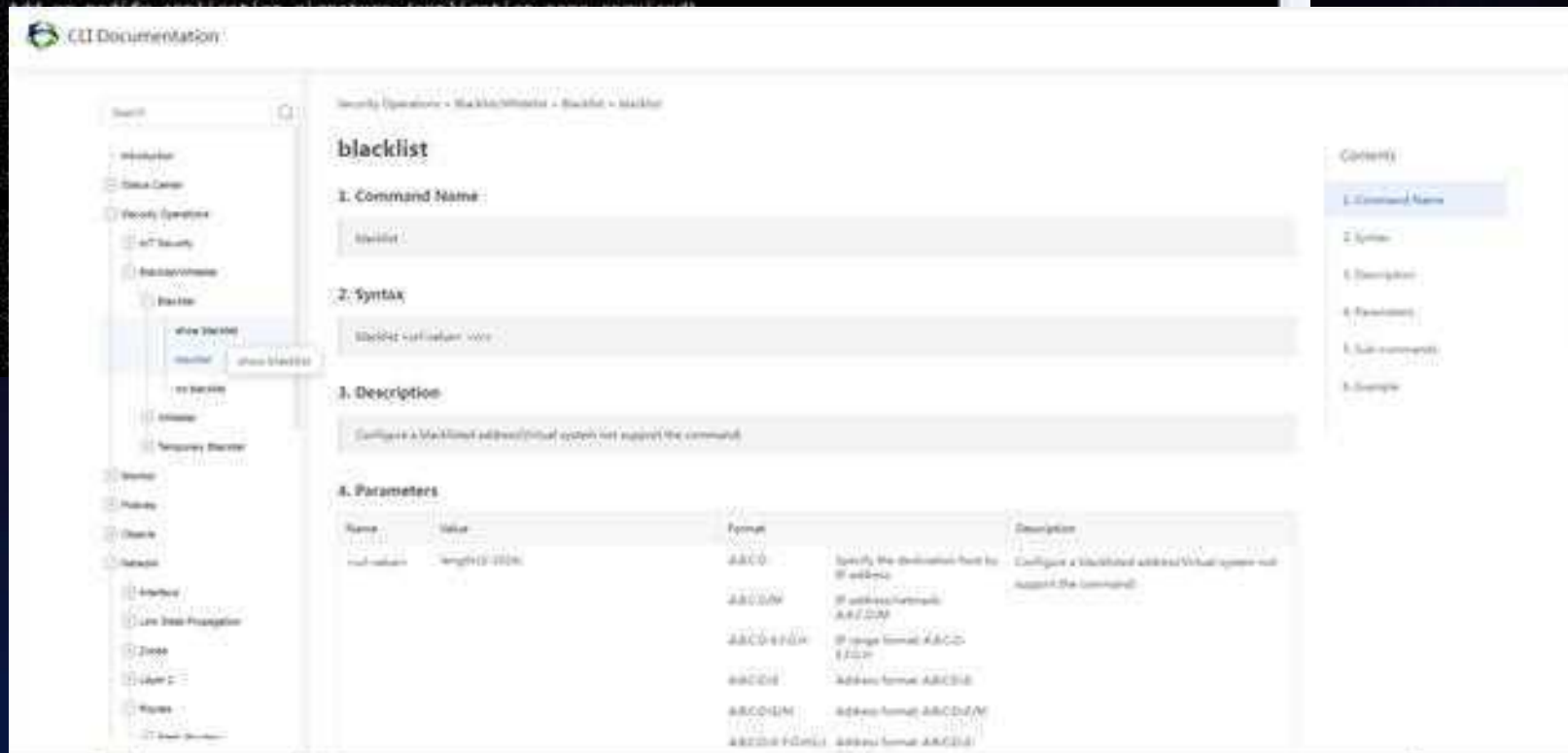
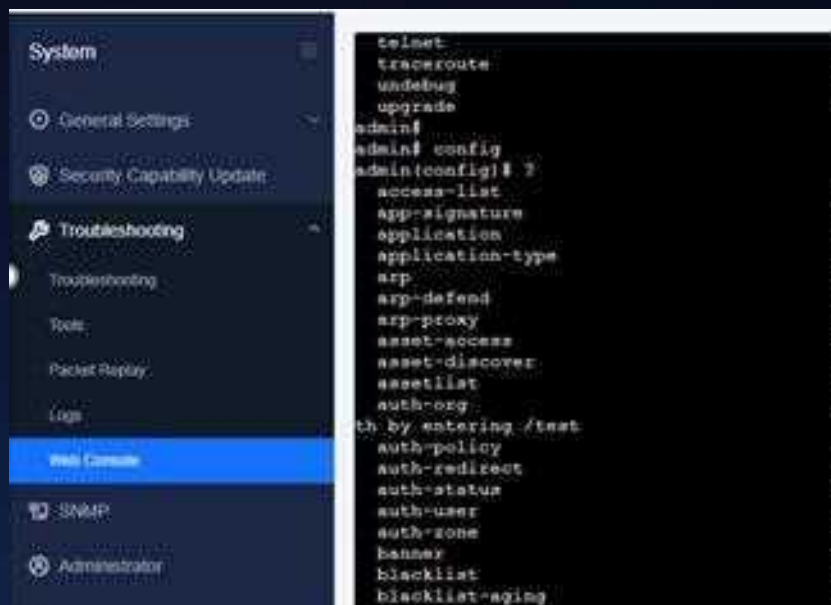
The screenshot displays the Sangfor Network Secure Platform Web Console interface, which is divided into several sections:

- System:** This section contains a list of system commands, including `config`, `debug`, `end`, `ethtool`, `exec`, `exit`, `export`, `export-hardware-info`, `help`, `import`, `import-image-from-ftp`, `import-image-from-tftp`, `import-license-file`, `license-active`, `login`, `passwd`, `ping`, `reboot`, `save-configuration`, `show`, `topdump`, `telnet`, `traceroute`, `undebug`, and `upgrade`. The `config` command is highlighted with a red box.
- General Settings:** This section includes options for `General Settings`, `Security Capability Update`, `Troubleshooting`, `Tools`, `Packet Replay`, `Logs`, `Web Console`, `SNMP`, `Administrator`, `Virtual Systems`, `Maintenance`, `High Availability`, and `Device Management`.
- Configuration:** This section shows a list of configuration commands, including `telnet`, `traceroute`, `undebug`, `upgrade`, `admin`, `admin(config)# ?`, `access-list`, `app-signature`, `application`, `application-type`, `arp`, `arp-defend`, `arp-proxy`, `asset-access`, `asset-discover`, `assetlist`, `auth-org`, `auth-policy`, `auth-redirect`, `auth-status`, `auth-user`, `auth-zone`, `banner`, `blacklist`, `blacklist-aging`, `block-session`, `bnat-rule`, `bnat6-rule`, `botnet-detection`, `clear`, `clock`, `configuration-auto-backup`, `content-security`, `country-blocking`, `country-blocking-blocked-ip`, `country-blocking-whitelist`, `ddos-defense`, `decrypt-certificate`, `decrypt-policy`, and `decrypt-whitelist`. The `admin` command is highlighted with a red box.
- Help:** This section provides detailed information about the commands, including their syntax and usage. For example, the `access-list` command is described as "Add or modify custom application signature" and the `auth-policy` command is described as "Configure authentication policy".

Web Console---Network Secure Platform



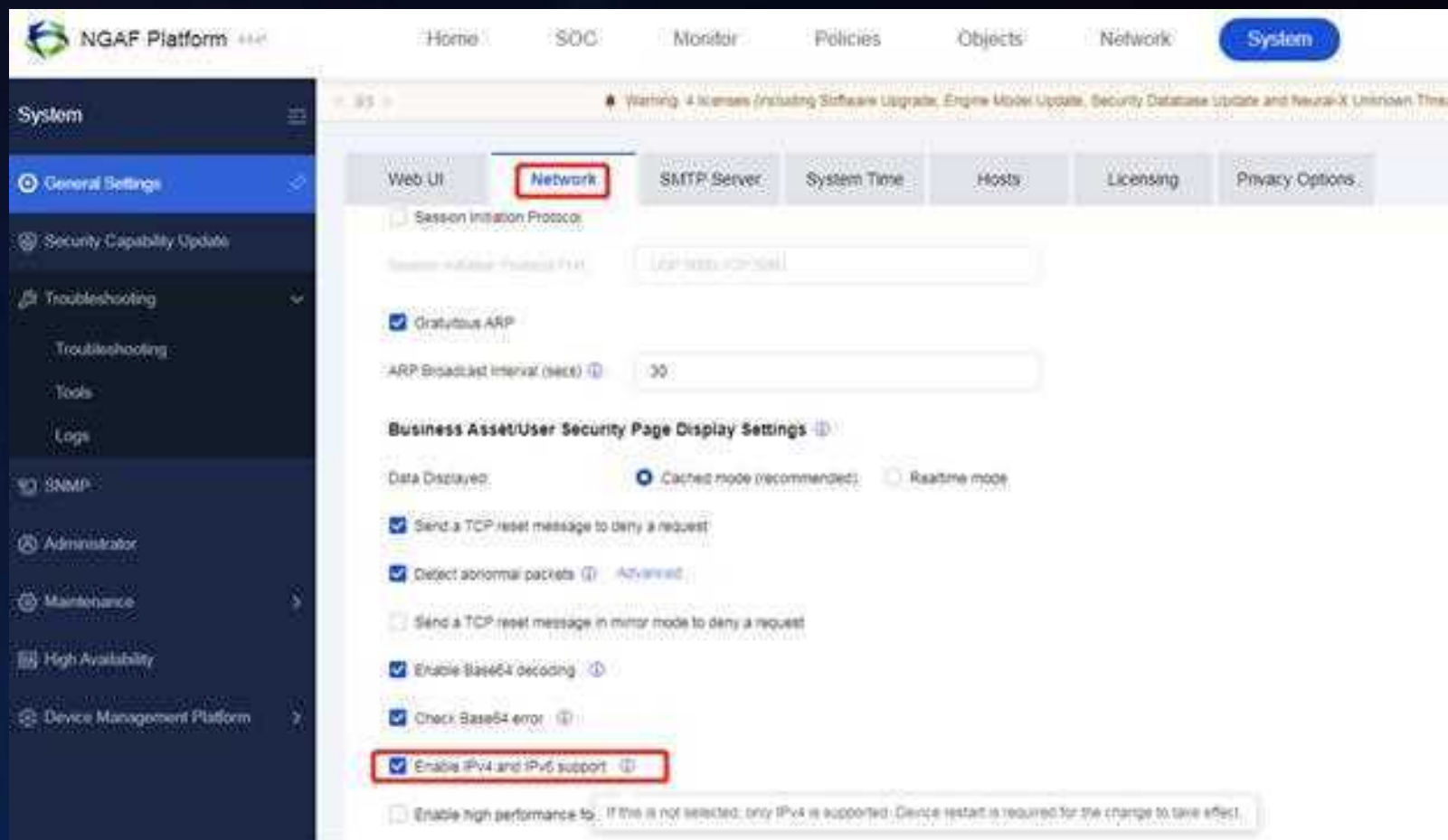
For more command lines instruction, you can refer to the CLI Document in the right top.



IPv6 Feature---Old Platform NGAF



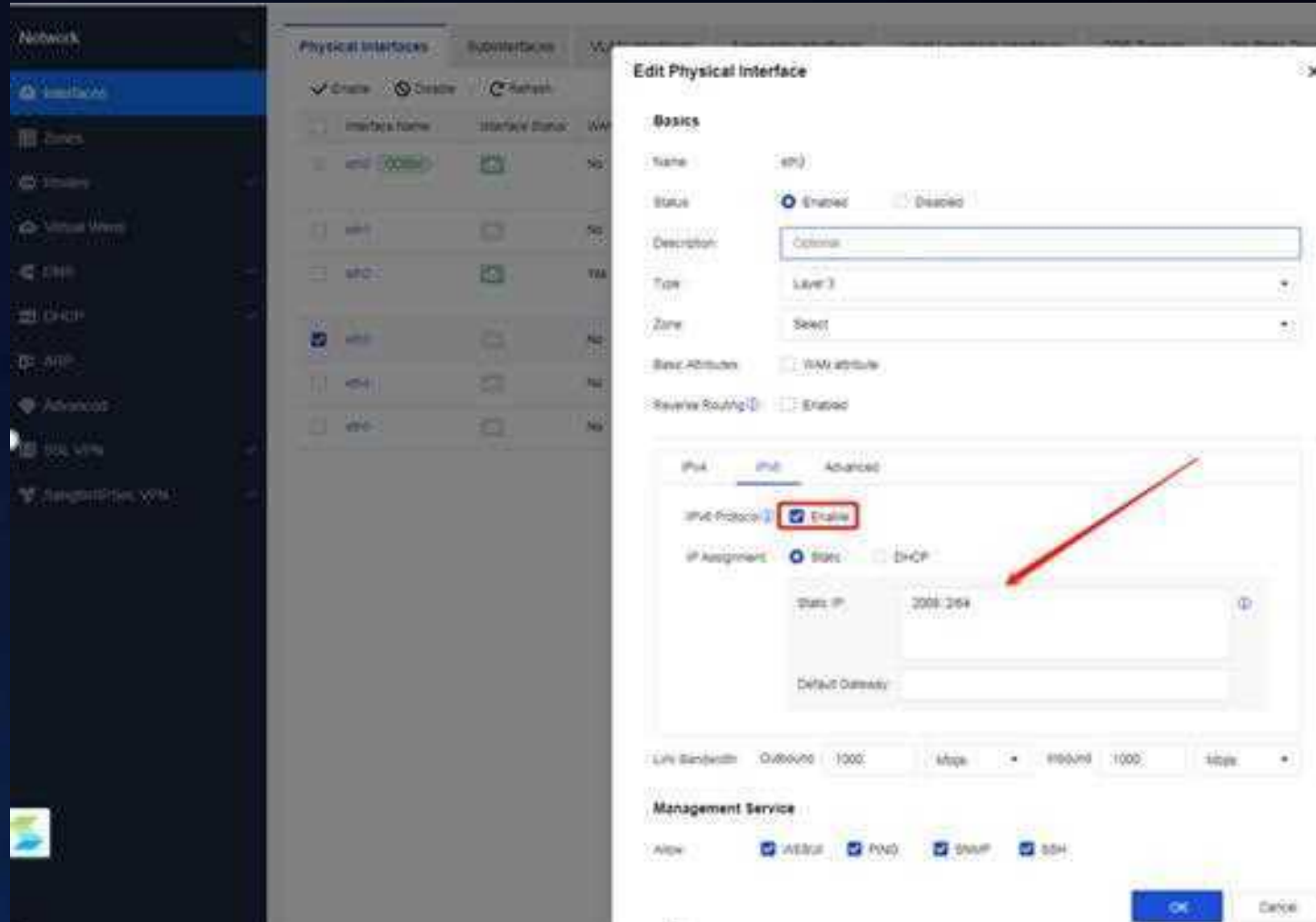
To support IPv6 on old platform NGAF, firstly it is necessary to enable the “Enable IPv4 and IPv6 support” feature in the network parameters which will cause to restart the device, and then configure IPv6 content in corresponding interfaces.



IPv6 Feature---Network Secure Platform



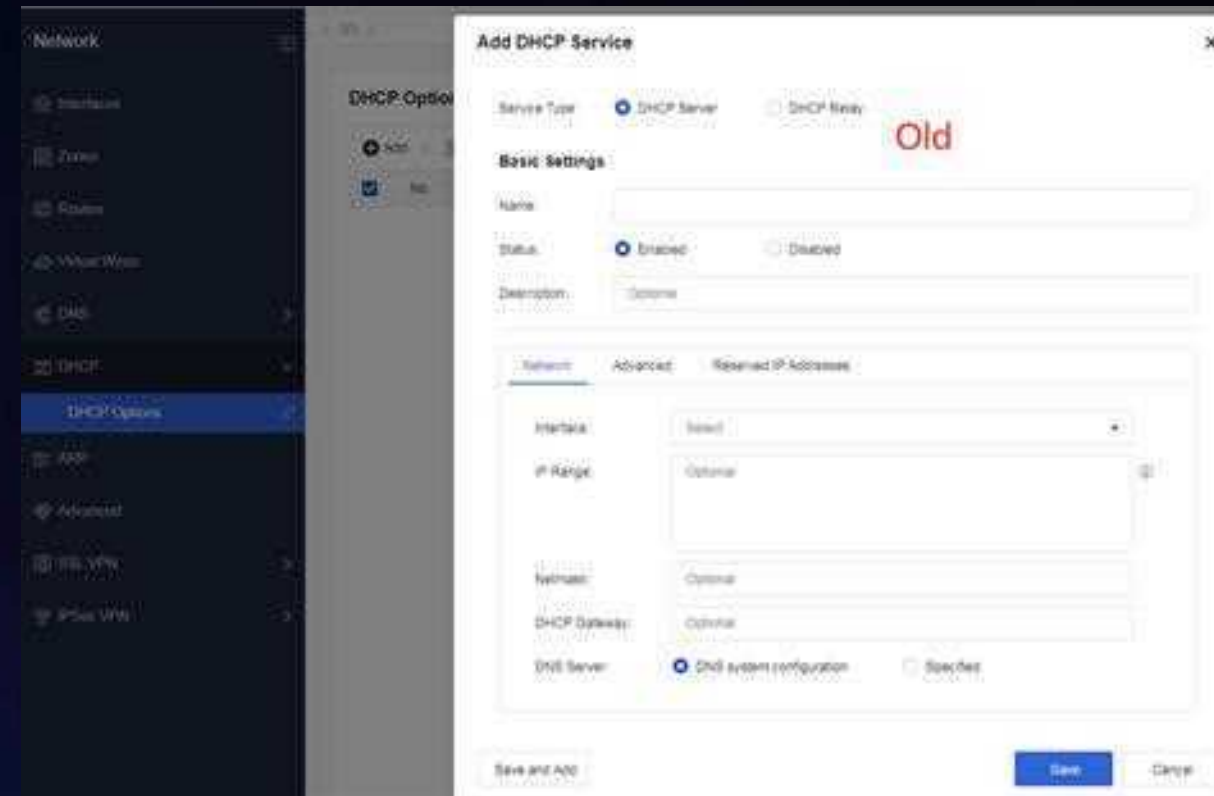
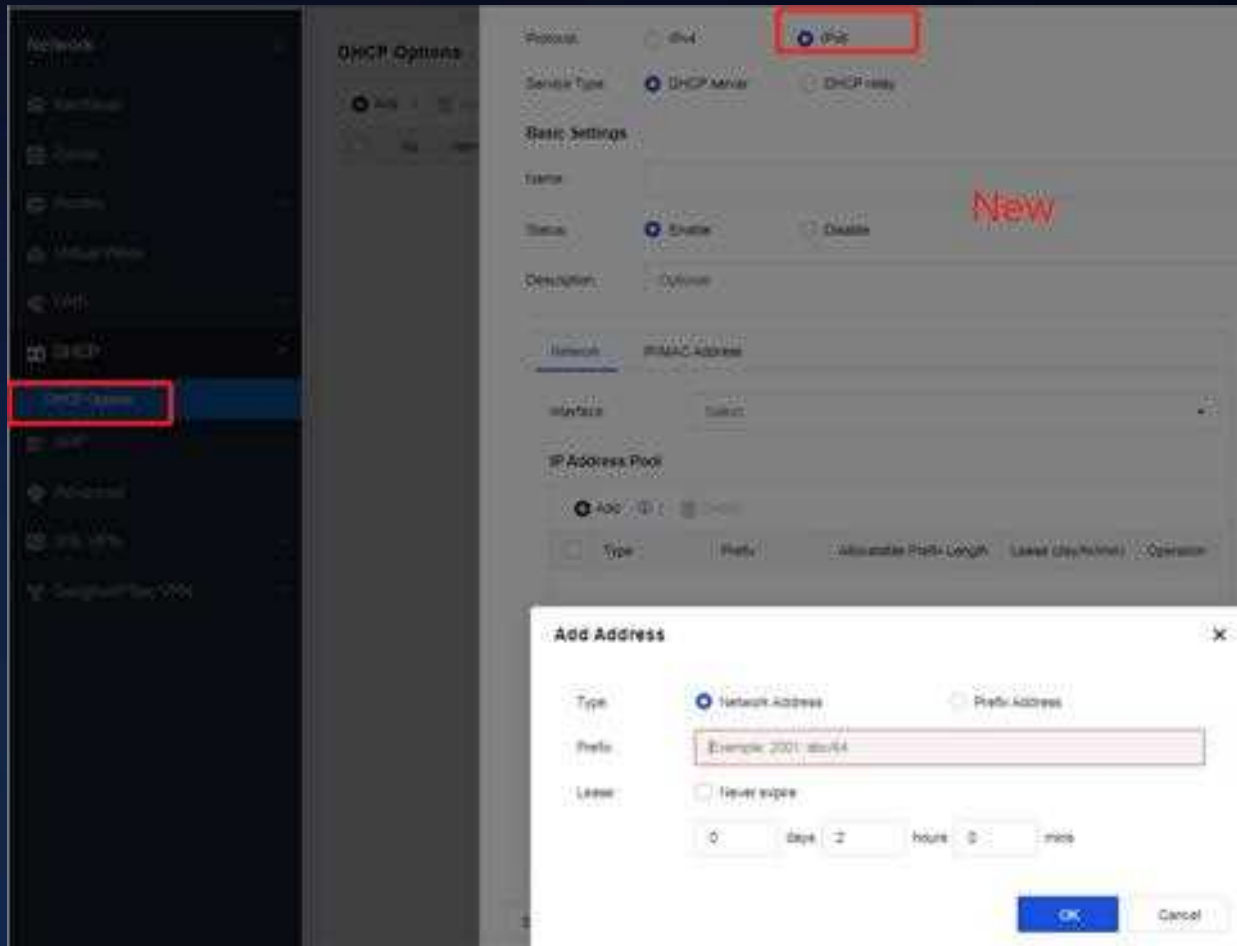
The Network Secure Platform supports IPv6 feature without other extra settings. This feature can be directly configured in the interface **without restarting the device**.



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 Protocol 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

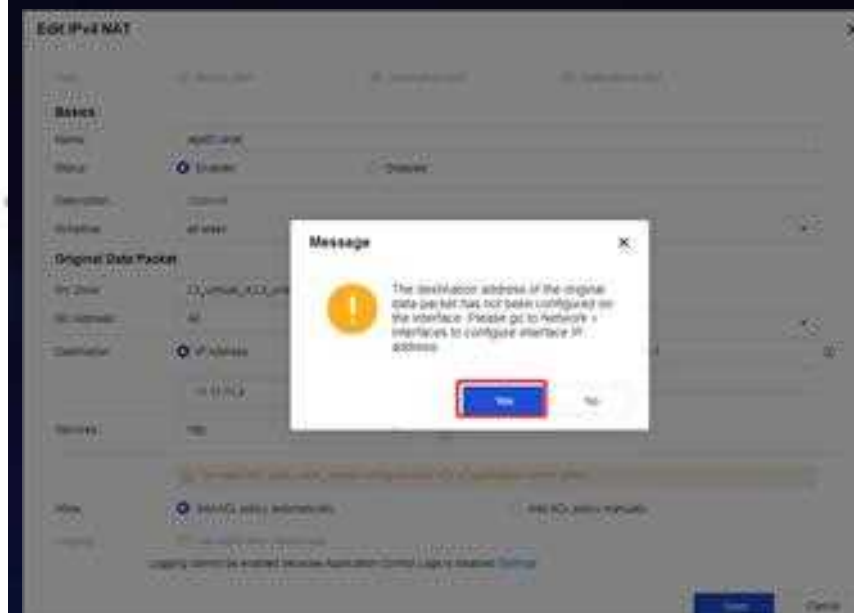
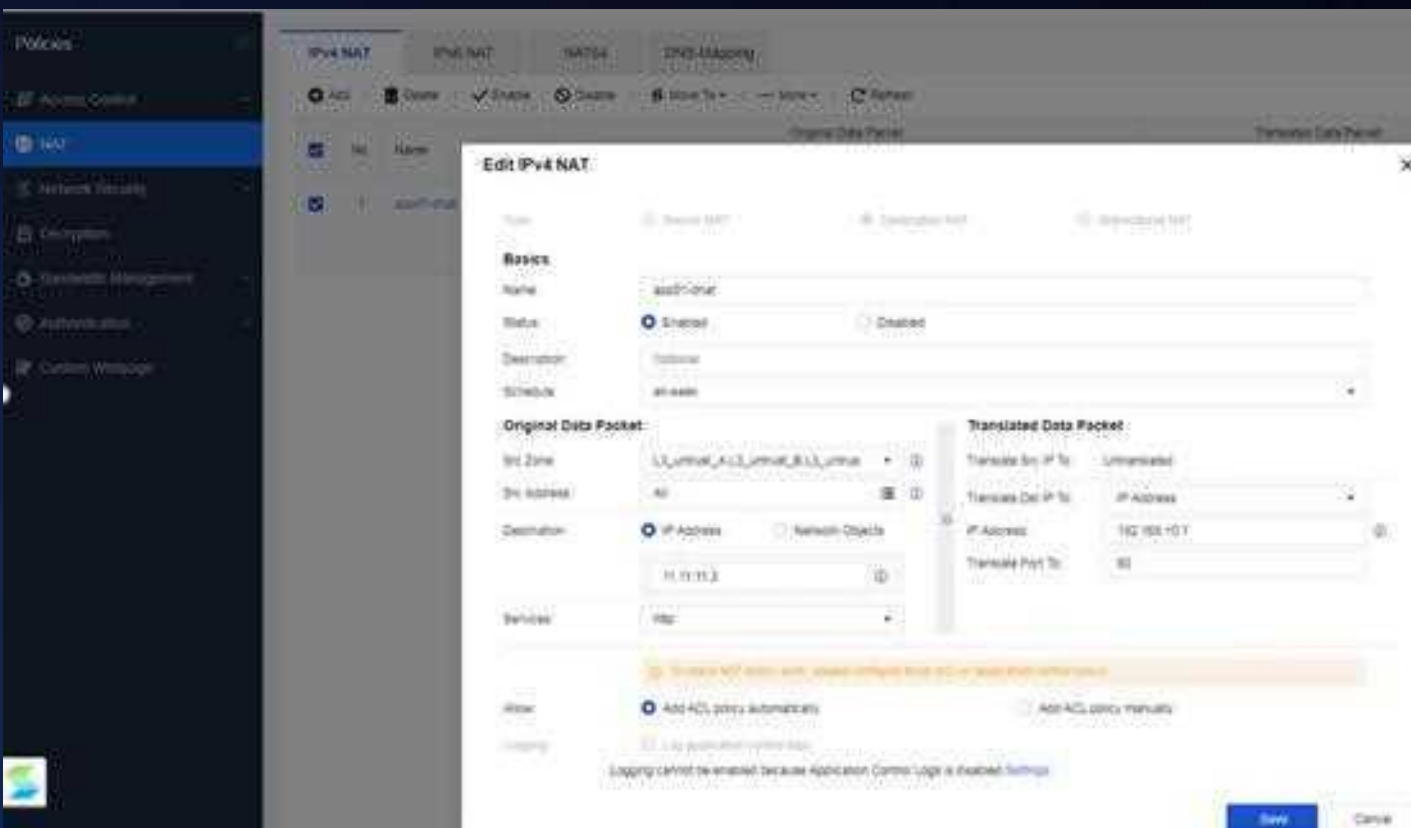
DNAT---Network Secure Platform



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.

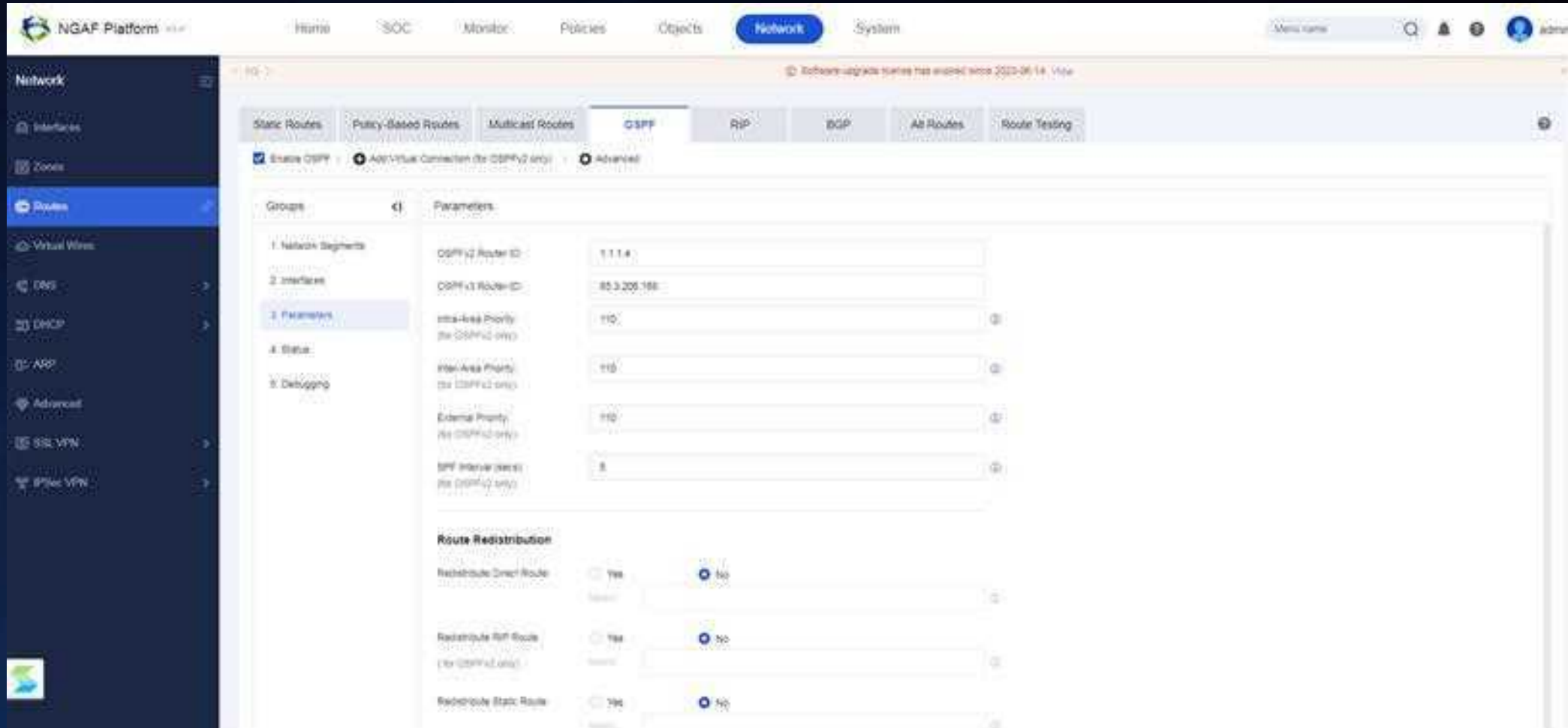
However, you probably will encounter the notifying message below before you save it, just click 'Yes' and ignore it.



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.

Type	Router ID	Intra-Area Priority	Inter-Area Priority	External Priority	Operation
OSPFv2	1.1.1.1	110	110	110	Edit Basic Edit Advanced Delete
OSPFv3	2.2.2.2	110	110	110	Edit Basic Edit Advanced Delete

OSPF---Network Secure Platform



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

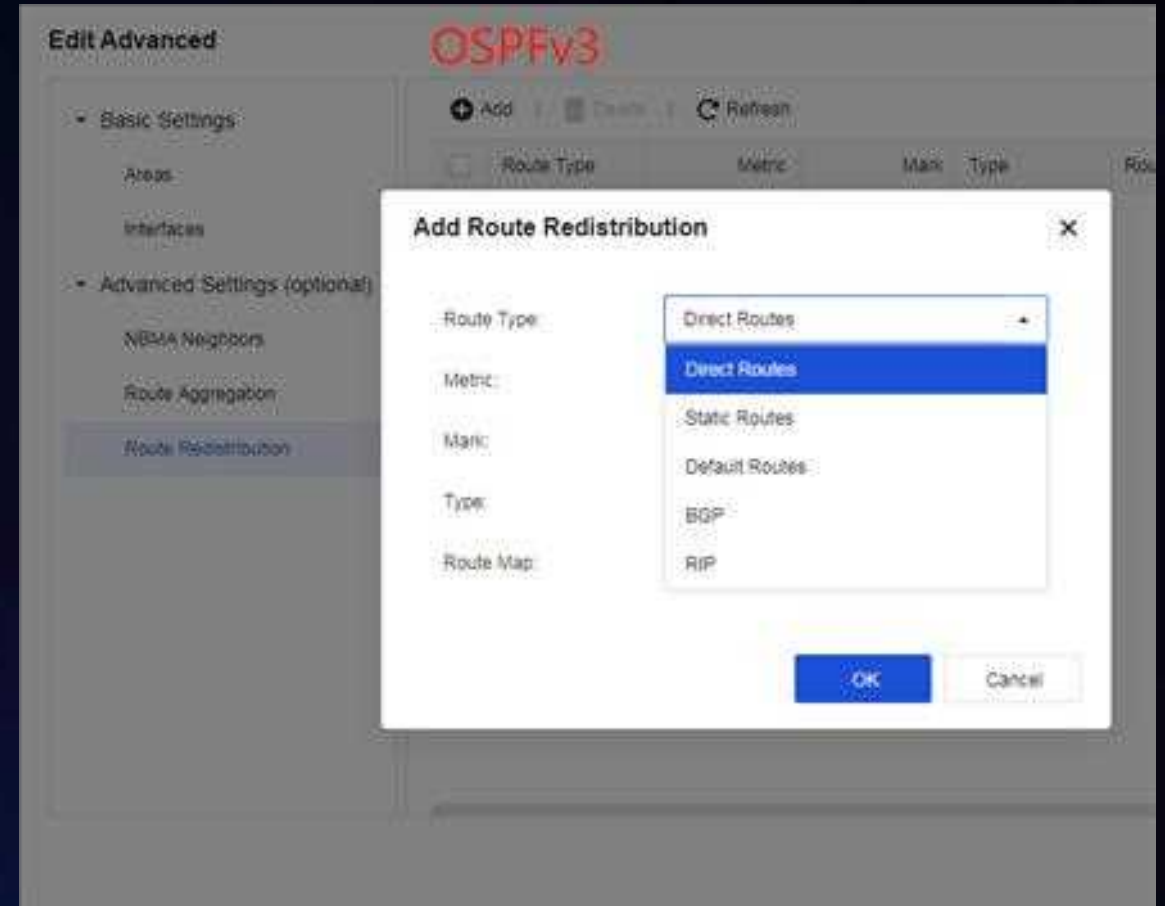
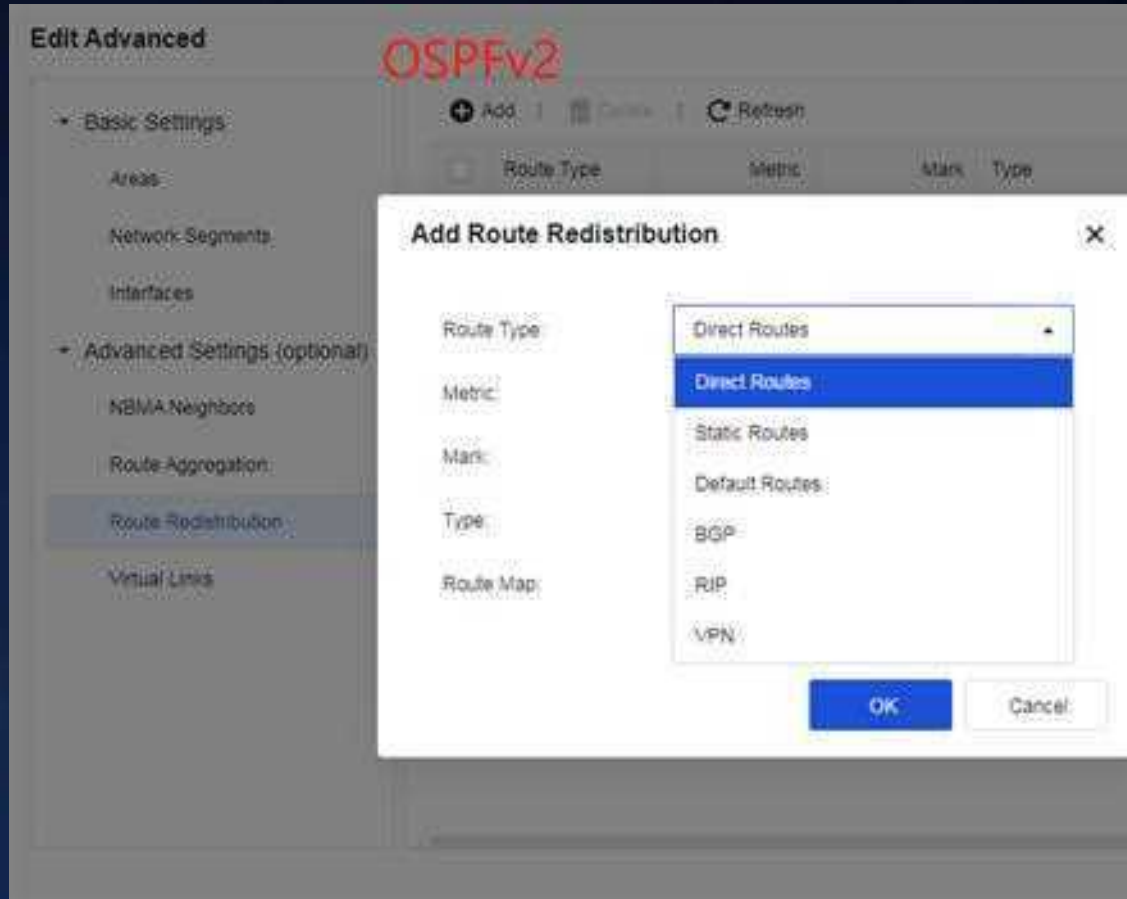
The screenshot displays the Sangfor Network Secure Platform interface. On the left, a sidebar menu shows various network management options. The main area is divided into two panels. The left panel, titled 'OSPF', shows a table of OSPF instances. The right panel, titled 'Edit Basics', shows the configuration for a specific OSPF instance. The 'Edit Basics' panel includes fields for Router ID, OSPF Calculation Delay, OSPF Calculation Interval, OSPF Area Priority, OSPF Area Priority, OSPF Area Priority, Default Metric of Redistributed Routes, and BFD. The BFD field is highlighted with a red box. The right panel shows a terminal window with the following commands:

```
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



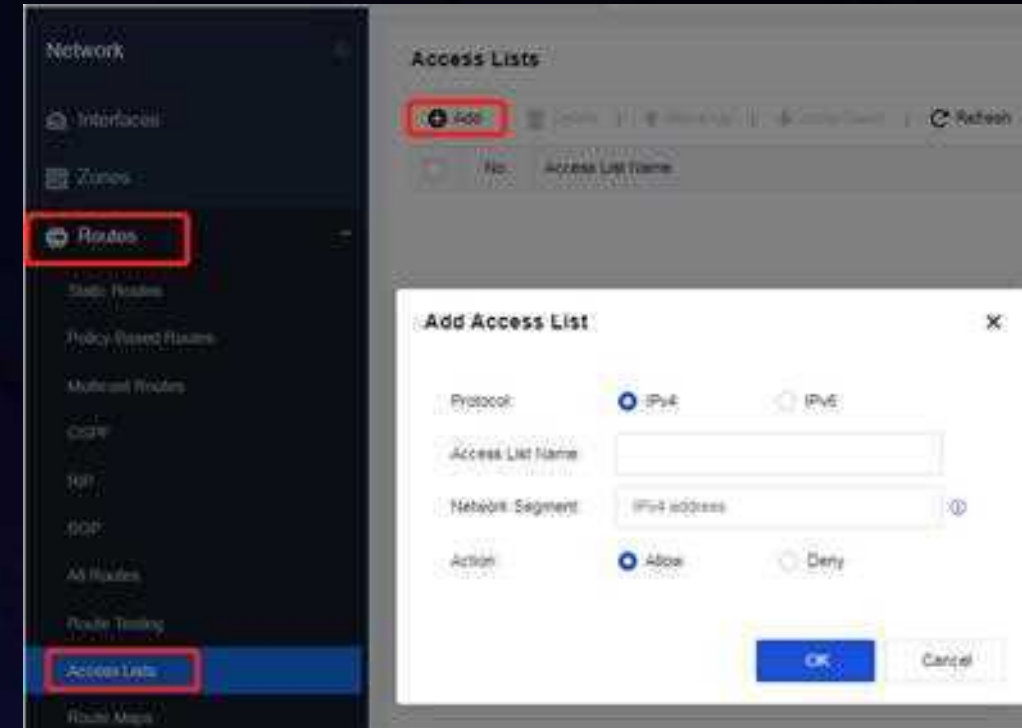
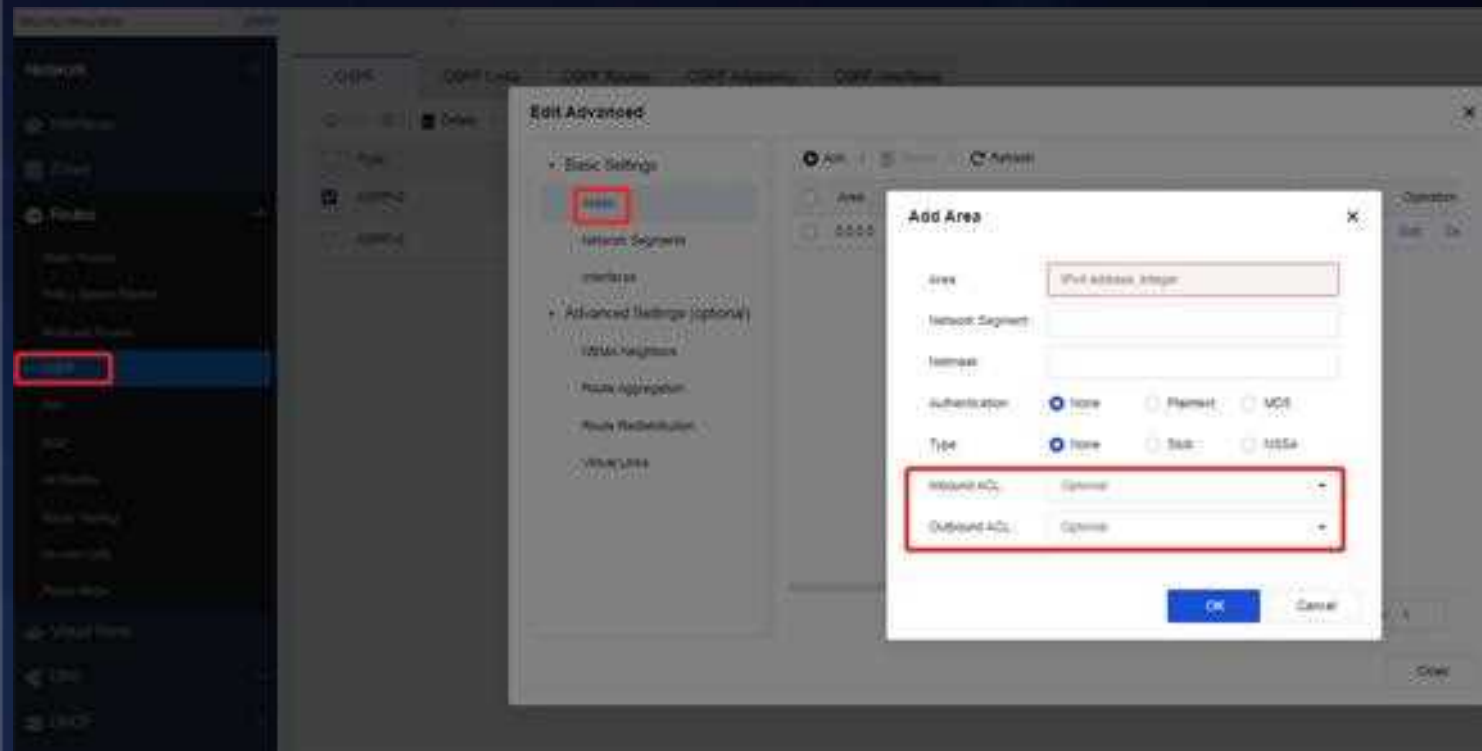
- OSPFv2 route redistribution supports direct routes, static routes, default routes, BGP routes, RIP routes and VPN routes.
- OSPFv3 route redistribution supports direct routes, static routes, default routes, BGP routes and RIP routes.



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.

The screenshot illustrates the configuration process for OSPF routes in the Sangfor Network Secure Platform. It is divided into three main sections:

- Left Panel (Network Configuration):** Shows the 'Network' menu with 'Routes' highlighted. The 'Edit Advanced' tab is selected, and the 'Route Map' option under 'Advanced Settings (optional)' is highlighted.
- Center Panel (Add Route Redistribution):** A dialog box for adding route redistribution. The 'Route Type' is set to 'Direct Route', and the 'Route Map' is set to 'Optional'. The 'Add Route Map' button is highlighted.
- Right Panel (Route Maps):** Shows the 'Route Maps' configuration page. The 'Add' button is highlighted. Below it, the 'Add Route Map' dialog box is open, showing fields for 'Route Map Tag', 'Priority', 'IPv4 Access List', 'IPv6 Access List', 'AS Path Prepend', 'Origin', 'Local Pref Value', and 'Action'. The 'Origin' is set to 'Not activated' and the 'Action' is set to 'Allow'.

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.

The screenshot displays the Sangfor Network Secure Platform interface. On the left, a sidebar menu shows various network management options, with 'Interfaces' selected. The main panel is divided into two sections: 'Physical Interfaces' and 'Subinterfaces'. The 'Physical Interfaces' section shows a table of interfaces, including eth0, eth1, eth2, eth3, eth4, and eth5. The 'eth2' interface is highlighted, and its configuration details are shown on the right.

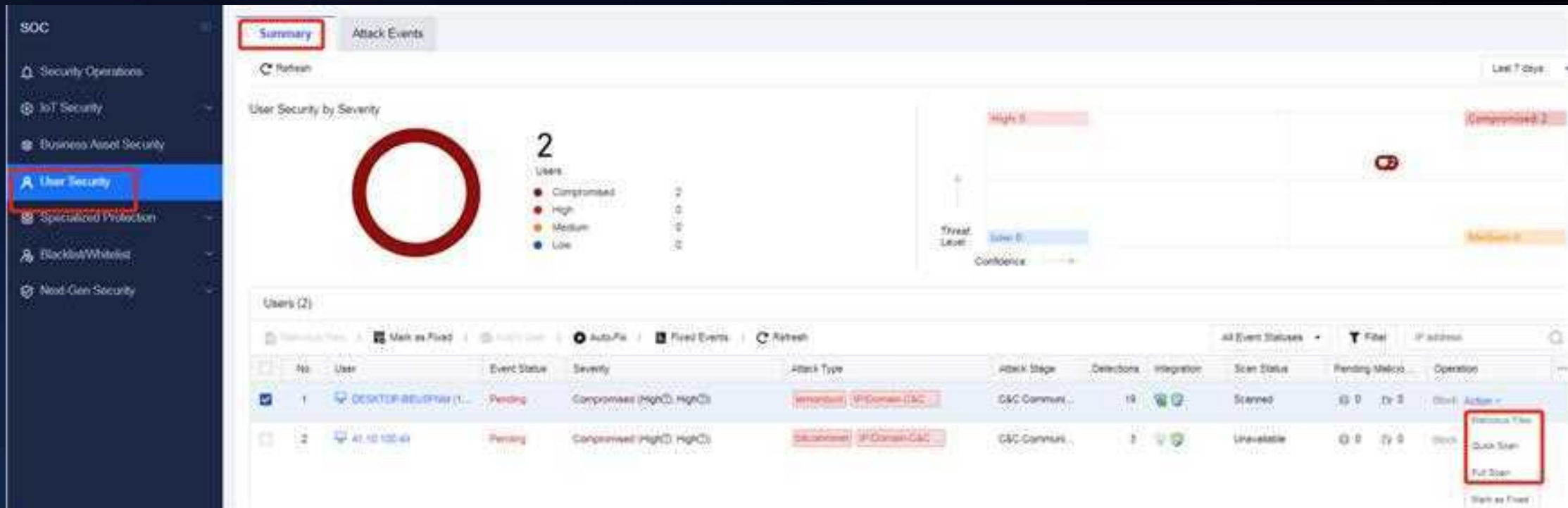
The configuration details for interface eth2 are as follows:

- Basics:**
 - Name: eth2
 - Status: ☒ Enabled ☐ Disabled
 - Description: Optional
 - Virtual Systems: public
 - Type: Layer 3
 - Zone: L3_untrust_4
 - Basic Attributes: ☒ WAN attribute
 - Reverse Routing: ☒ Enabled
- IP Assignment:**
 - IP Assignment: ☐ Static ☒ DHCP ☐ PPPoE
 - Default Route: ☒ Obtain default route
 - Communication Mode: ☐ Unicast ☒ Broadcast
 - Taken as preferred DNS server: ☒ Enable
- Link Bandwidth:**
 - Outbound: 1000 Mbps
 - Inbound: 1000 Mbps
- Management Service:**

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.





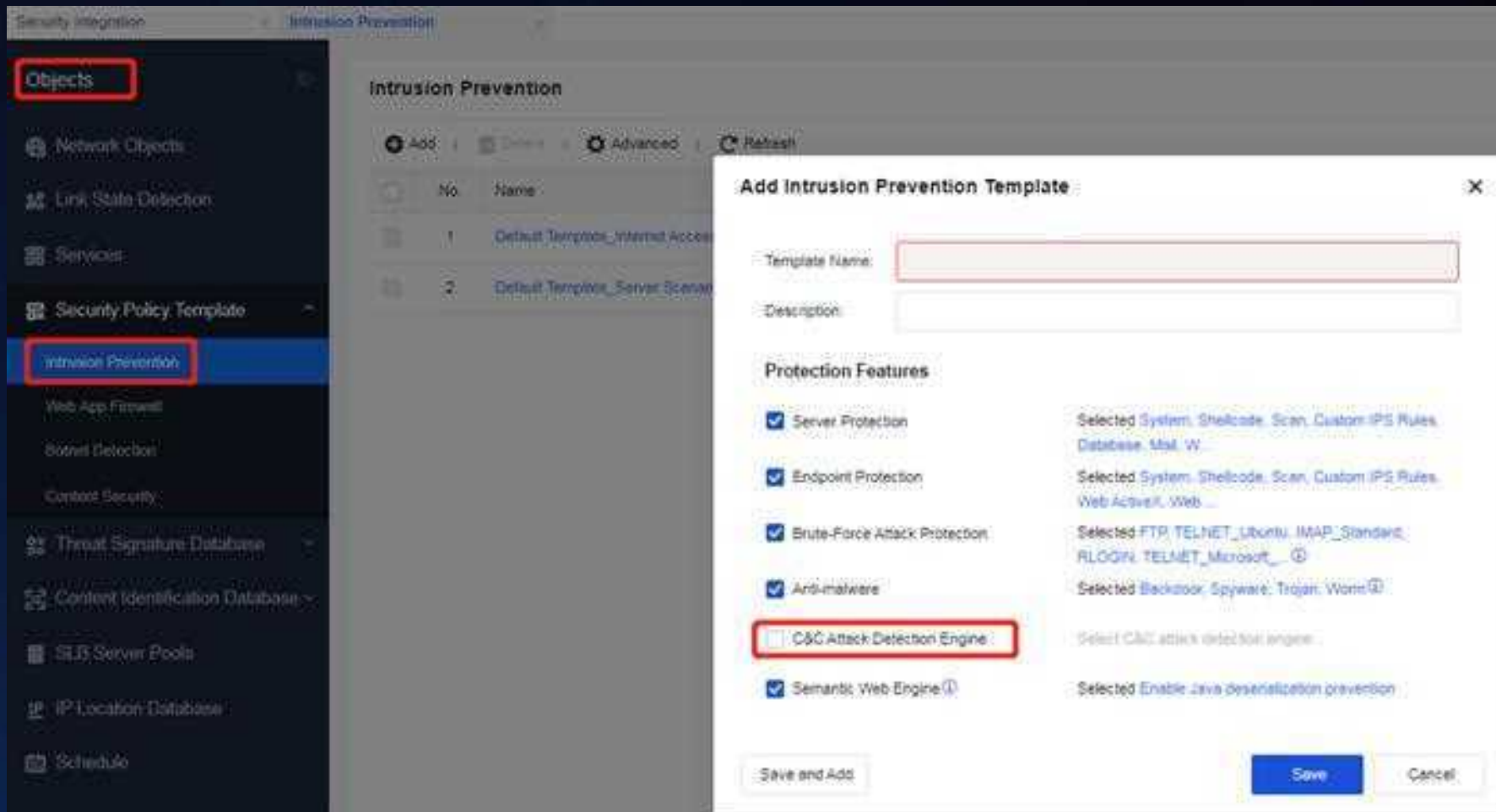
In Network Secure Platform , it adds TOP N feature which ranks network activities based on traffic and number of new sessions in two dimensions according to devices, app ranking, source IP ranking, destination IP ranking, and interface ranking.



Intrusion Prevention



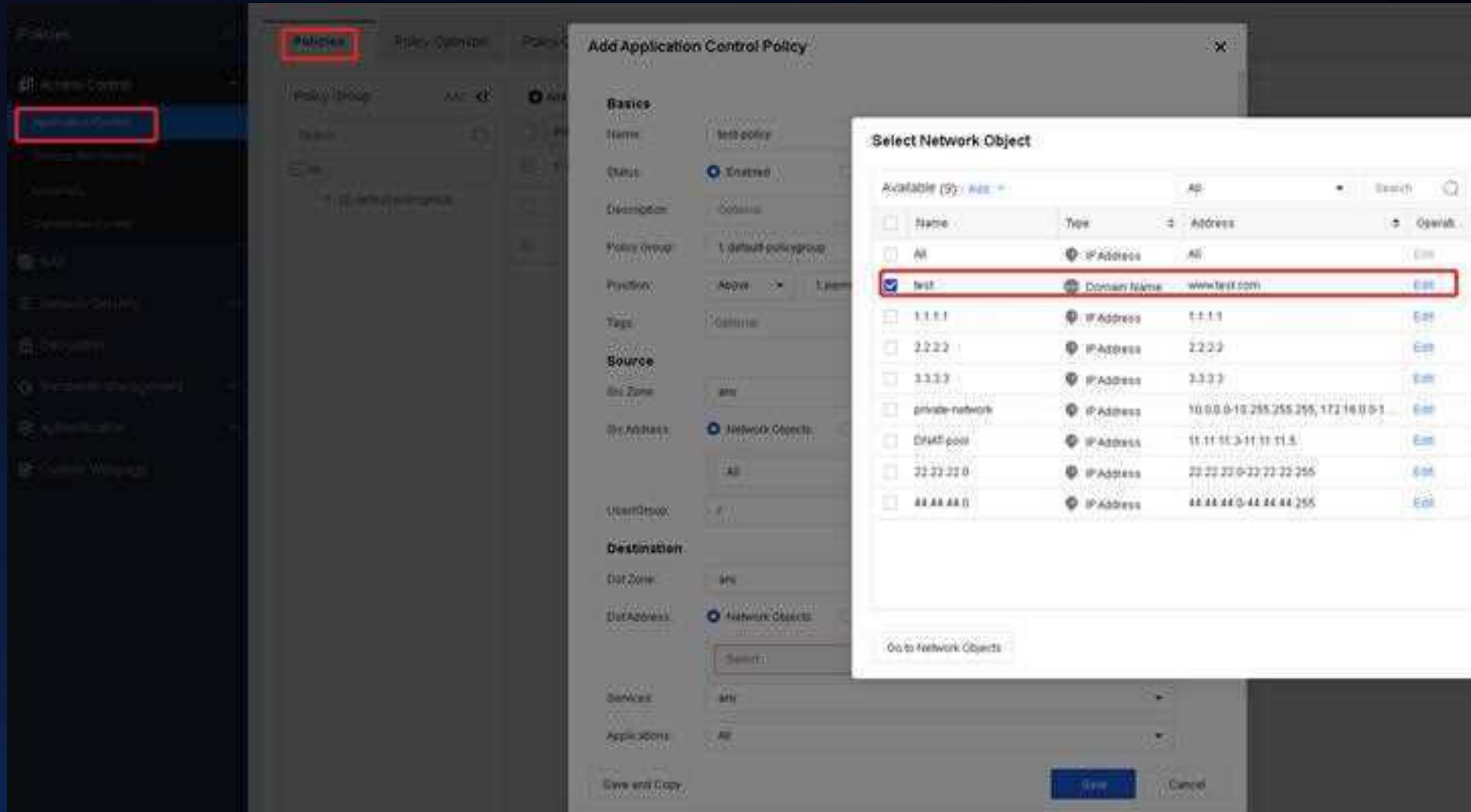
In Network Secure Platform, the intrusion protection module adds C&C attack detection engine, which audits protocols and reports to cloud platform to empower the NGAF capabilities, thereby improving the C&C attack detection ability.



Domain Name Object



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

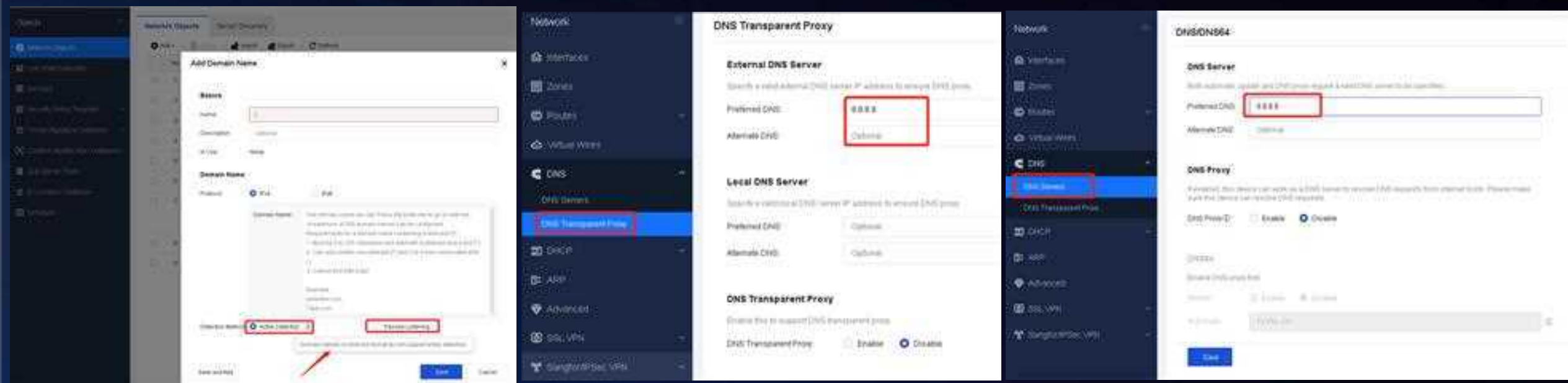


Domain Name Object



Domain name object contains active detection mode and passive listening.

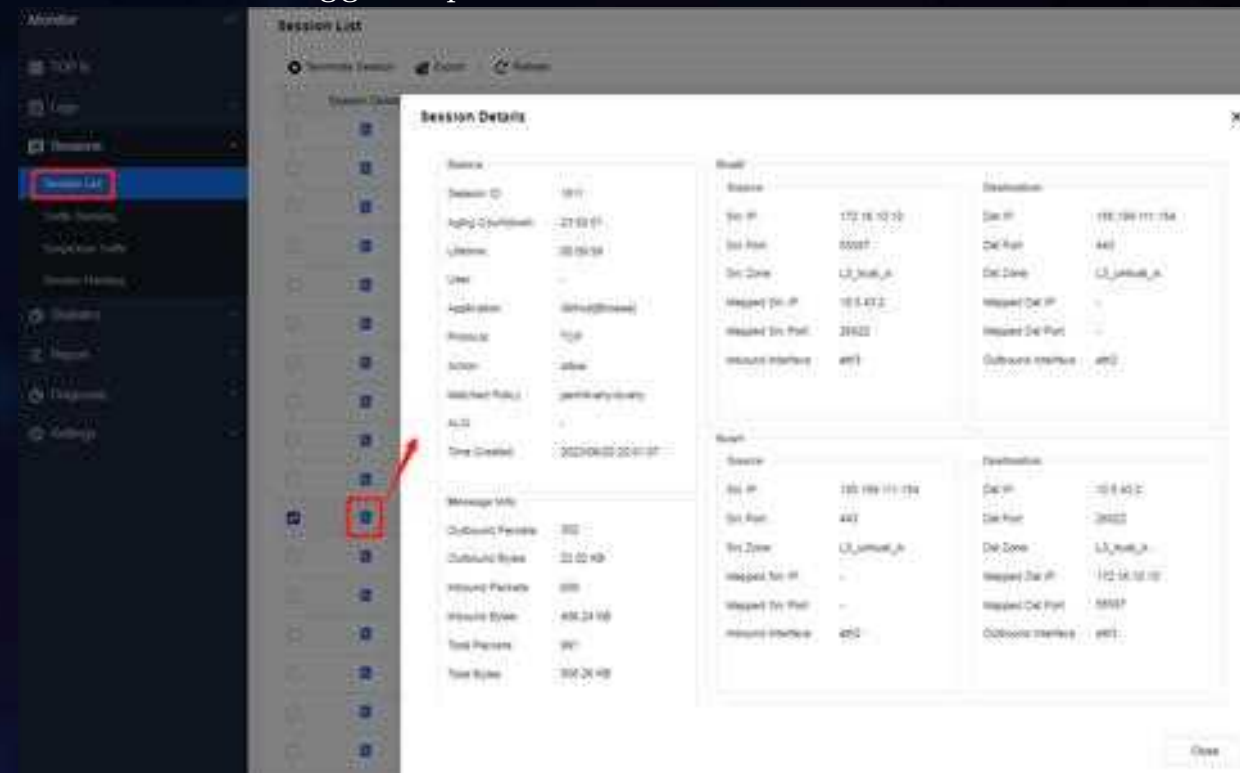
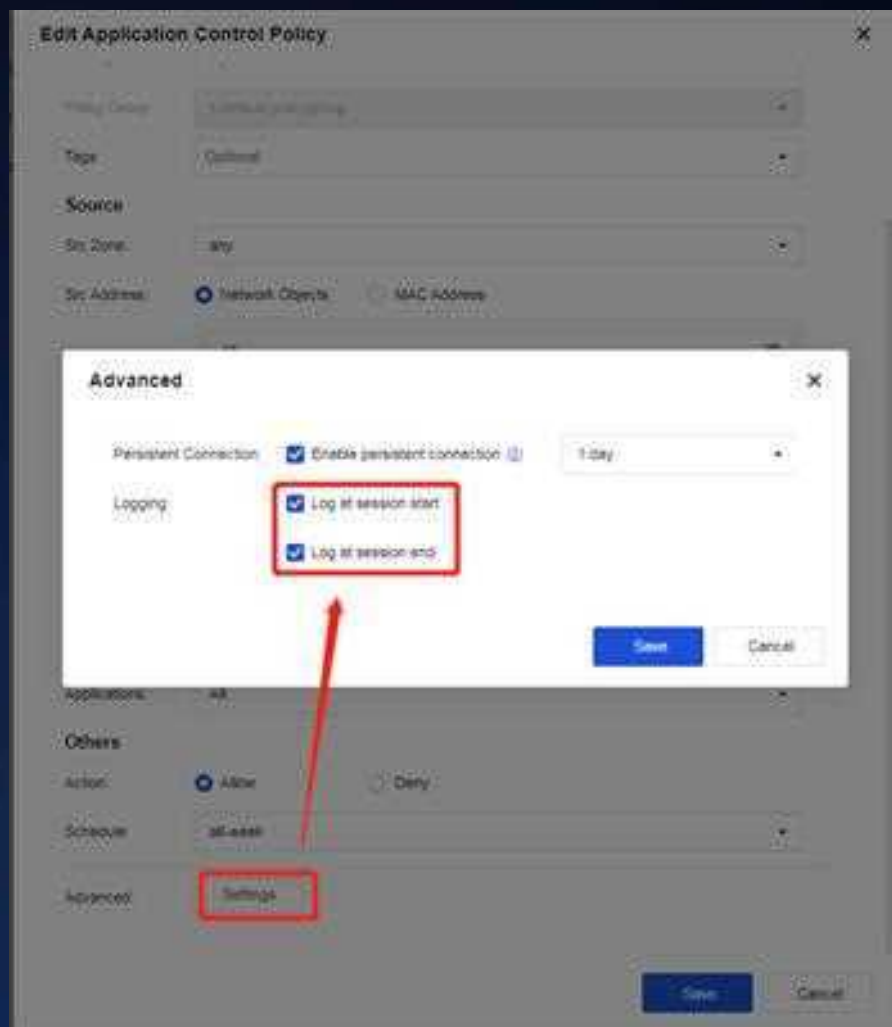
- In active detection mode, it is unnecessary that the DNS traffic has to go through NGAF, while NGAF has to connect the DNS server for resolving the domains. It will adjust DNS server in DNS Transparent Proxy configuration module firstly, then to DNS Server module, so you need to make sure both those 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 login options in advance.



Session List



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

Security Integration Access Logs

Monitor

TOP N

Logs

Security Logs

Access Logs

System Logs

Sessions

Statistics

Report

Diagnosis

Settings

Session Logs User Login/Logout Logs SSL VPN Logs INP Audit Logs

Start Time: 2023-06-25 00:00

End Time: 2023-06-25 23:59

Src Zone: All

Src IP/User: ☒ All ☐ IP ☐ User ☐ Group

Dst Zone: All

Dst IP: All

Service/Application: All

Action: ☒ Allow ☒ Deny ☒ Integratedly Deny

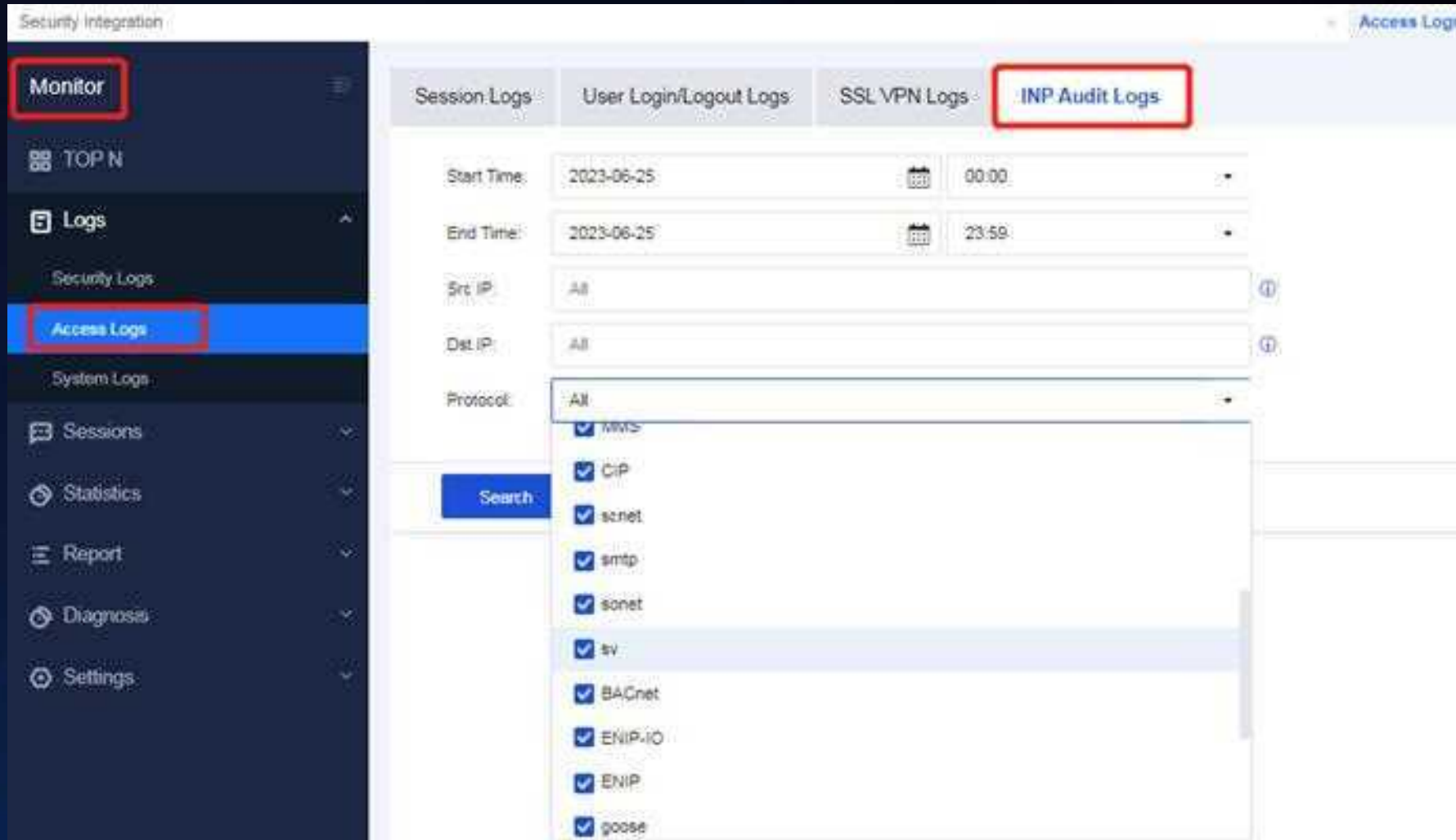
Session Logging: ☒ At Start ☐ At Rejection ☐ At End

Search ☐ Open in Quick Tab

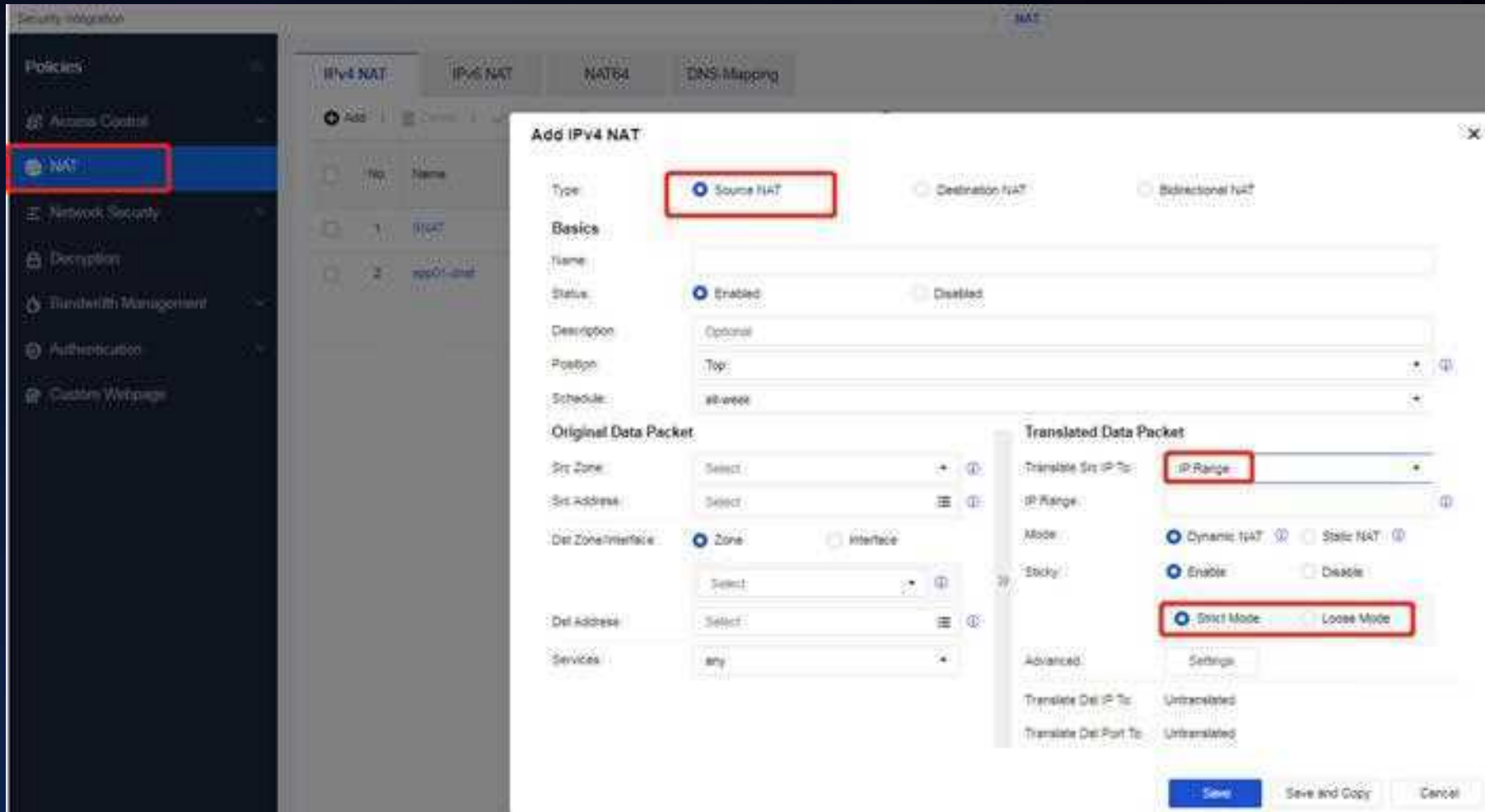
INP Audit Logs



In Network Secure Platform, it can audit some INP protocols, and so far the supporting ptotocal types including opeda, s7, s7-plus, modbus, iec104, and profinetI0.

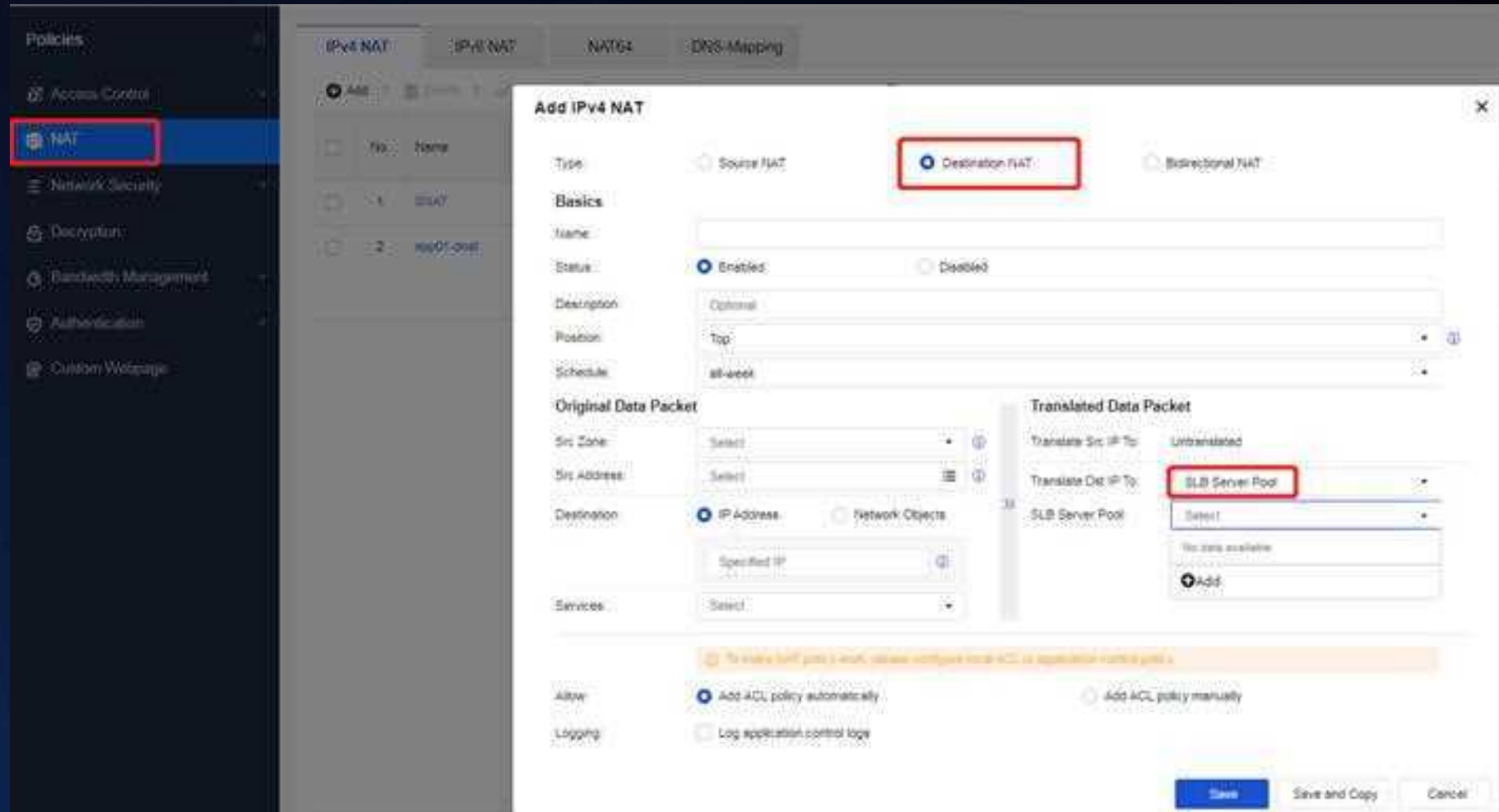


In new platform NGAF, it adds the options of strict mode and loose mode in dynamic SNAT scenario when the translated addresses belong IP range or network object.



The screenshot displays the Sangfor NGAF web interface. On the left, the 'Policies' menu is open, and 'NAT' is highlighted. The main area shows the 'Add IPv4 NAT' configuration window. The 'Type' is set to 'Source NAT'. The 'Status' is 'Enabled'. The 'Original Data Packet' section has 'Src Zone' set to 'Select', 'Src Address' set to 'Select', 'Dst Zone/Interface' set to 'Zone', and 'Dst Address' set to 'Select'. The 'Translated Data Packet' section has 'Translate Src IP To' set to 'IP Range', 'Mode' set to 'Dynamic NAT', and 'Strict Mode' selected. The 'Advanced' section has 'Translate Dst IP To' set to 'Untranslated' and 'Translate Dst Port To' set to 'Untranslated'. The 'Save' button is highlighted.

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.

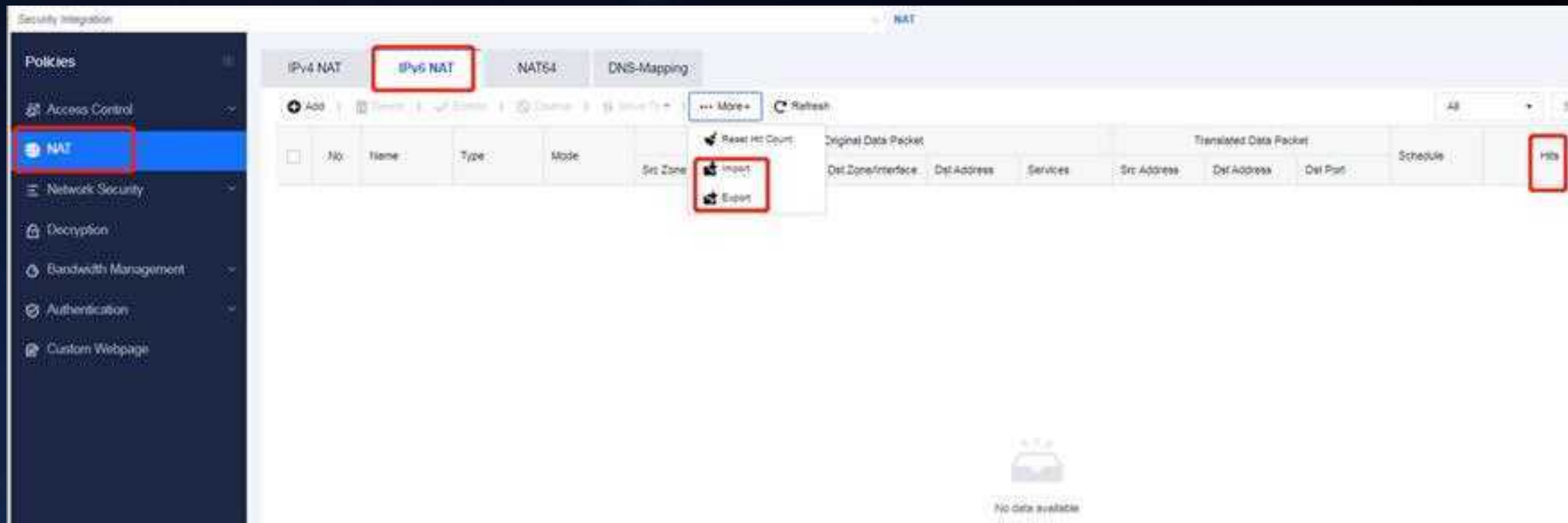


The screenshot displays the 'Add IPv4 NAT' configuration window in the Sangfor Network Secure Platform. The left sidebar shows the 'Policies' menu with 'NAT' highlighted. The main window has tabs for 'IPv4 NAT', 'IPv6 NAT', 'NAT64', and 'DNS-Mapping'. The 'Add IPv4 NAT' window is open, showing the following configuration options:

- Type:** ☒ Destination NAT, ☐ Source NAT, ☐ Bidirectional NAT
- Basics:**
 - Name: [Empty field]
 - Status: ☒ Enabled, ☐ Disabled
 - Destination: [Optional]
 - Position: Top
 - Schedule: all-week
- Original Data Packet:**
 - Src Zone: [Select]
 - Src Address: [Select]
 - Destination: ☒ IP Address, ☐ Network Objects
 - Specified IP: [Empty field]
 - Services: [Select]
- Translated Data Packet:**
 - Translate Src IP To: Untranslated
 - Translate Dest IP To: SLB Server Pool
 - SLB Server Pool: [Select]
 - [No data available]
 - [Add]
- Allow:** ☒ Add ACL policy automatically, ☐ Add ACL policy manually
- Logging:** ☐ Log application control logs

At the bottom of the window, there are buttons for 'Save', 'Save and Copy', and 'Cancel'.

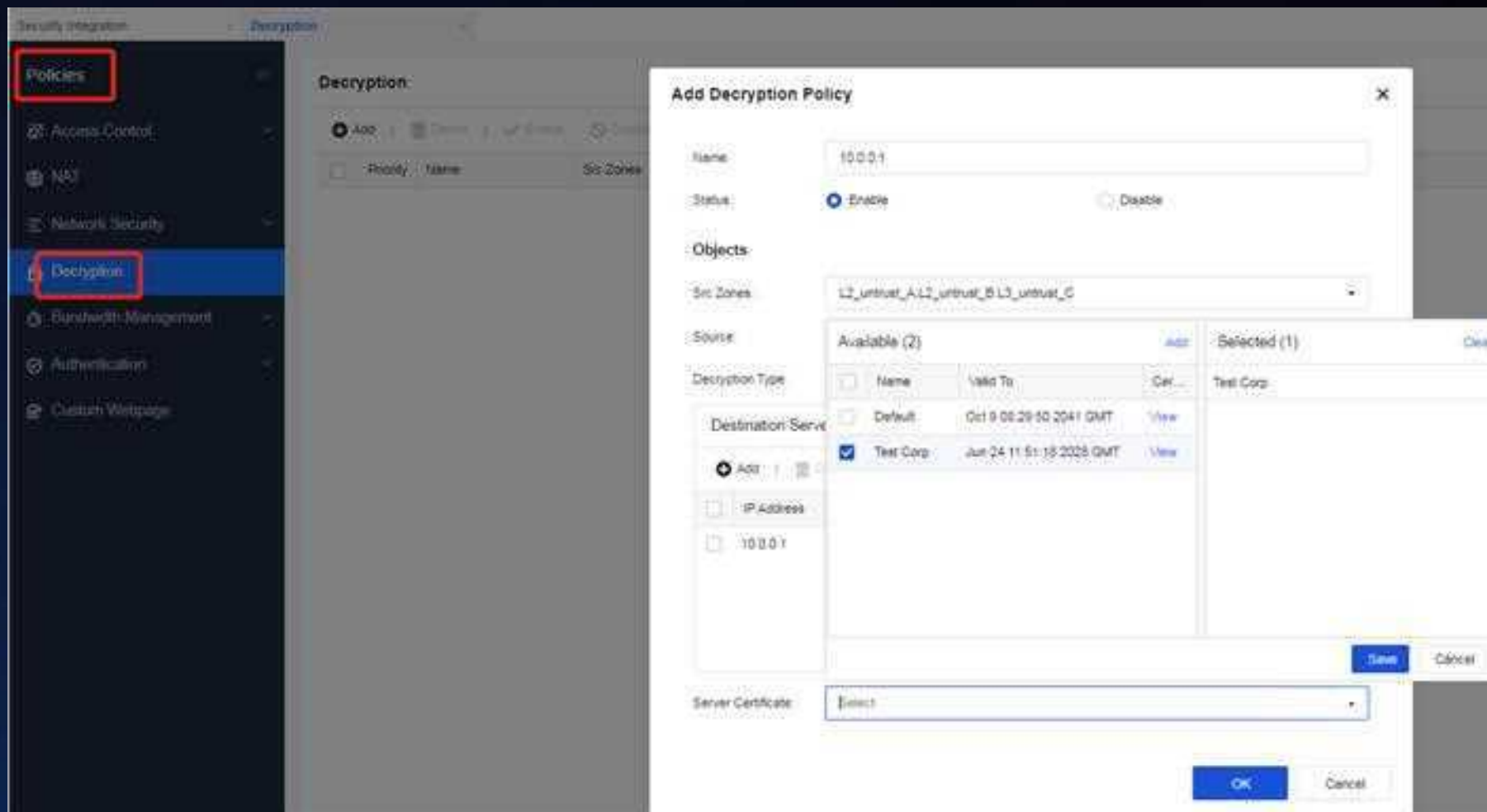
In Network Secure Platform, IPv6 NAT adds the feature of import and export operations, meanwhile every NAT item can display the hit counts.



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

The screenshot displays the 'Add Server Certificate' dialog box within the Sangfor Network Secure Platform. The dialog box is titled 'Add Server Certificate' and has a close button (X) in the top right corner. It features three tabs: 'Import Certificate', 'Specify Self-Signed' (which is selected), and 'Import Public/Private'. The 'Specify Self-Signed' tab contains the following fields:

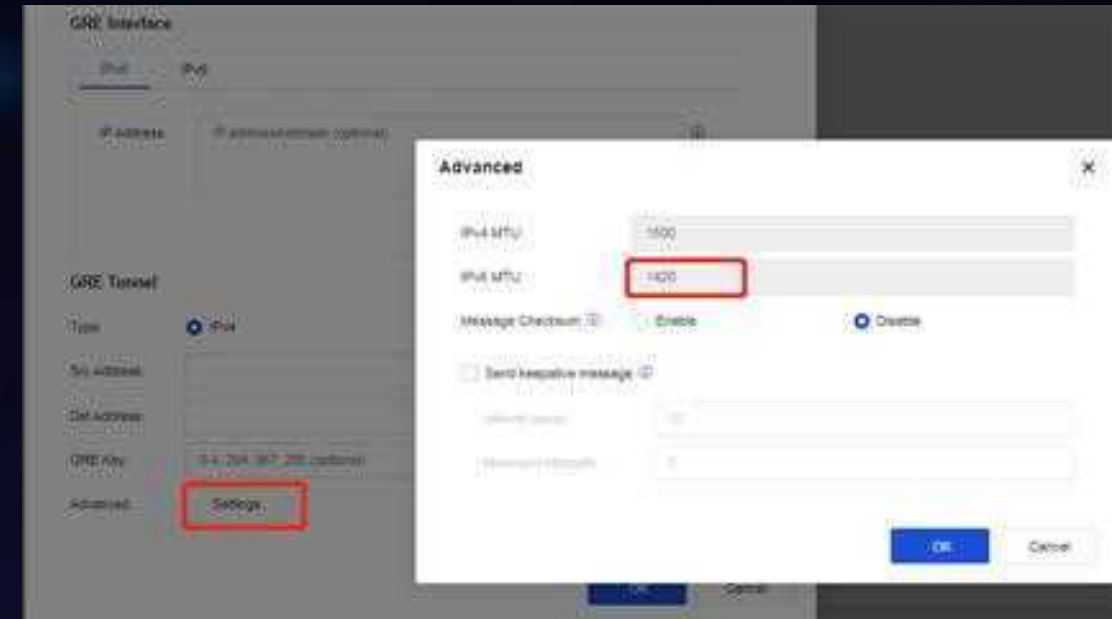
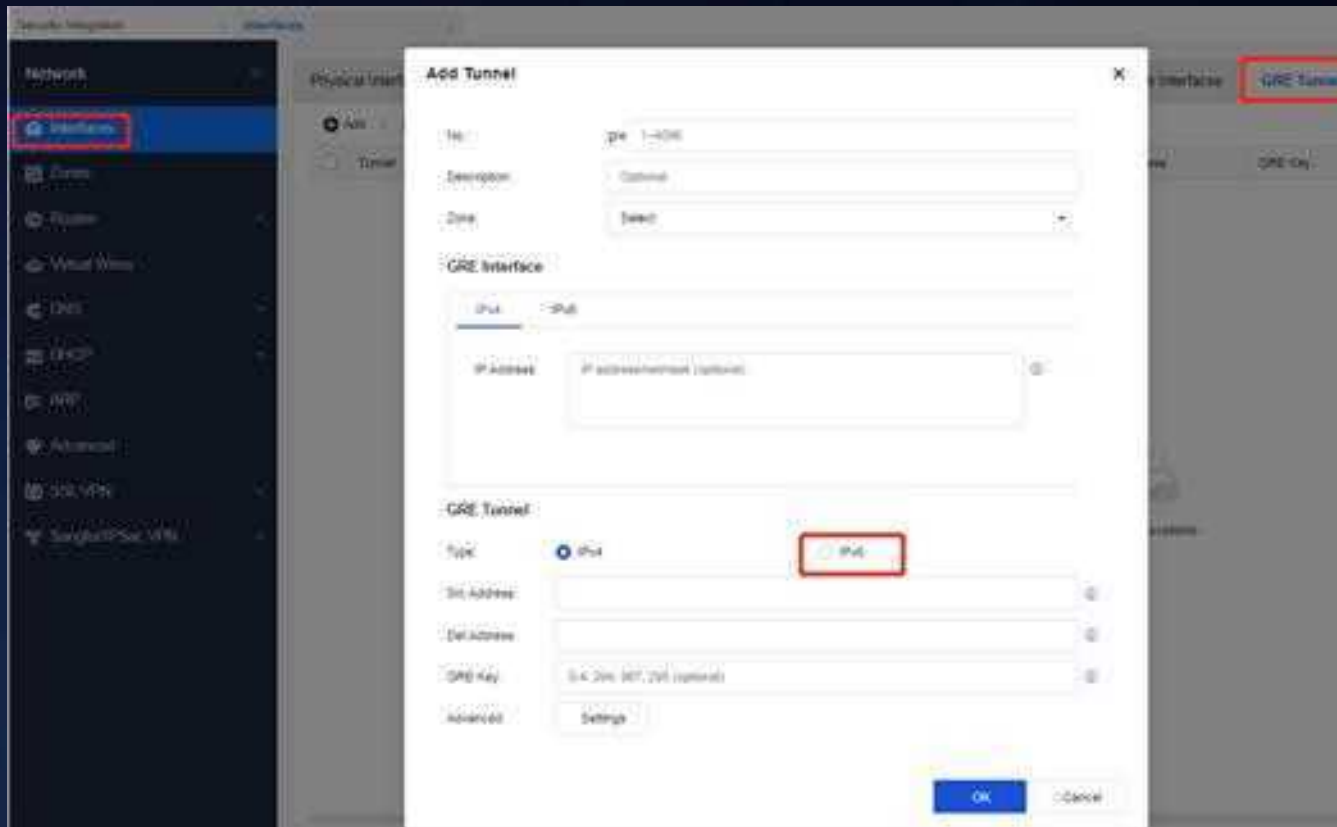
- Type: ☐ Import Certificate, ☒ Specify Self-Signed, ☐ Import Public/Private
- Name: [Text Input]
- Country: [Text Input]
- State: [Text Input]
- City: [Text Input]
- Company: [Text Input]
- Department: [Text Input]
- Issued To: [Text Input]
- Email: [Text Input]
- CA Password: [Text Input]
- Key Type: [Dropdown Menu] (Options: rsa, ecc)
- Key Size: [Dropdown Menu] (Options: 2048, 4096)
- Validity Period: [Text Input]

The background of the screenshot shows the 'Decryption' section of the Sangfor Network Secure Platform, with a sidebar on the left containing various security management options.

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



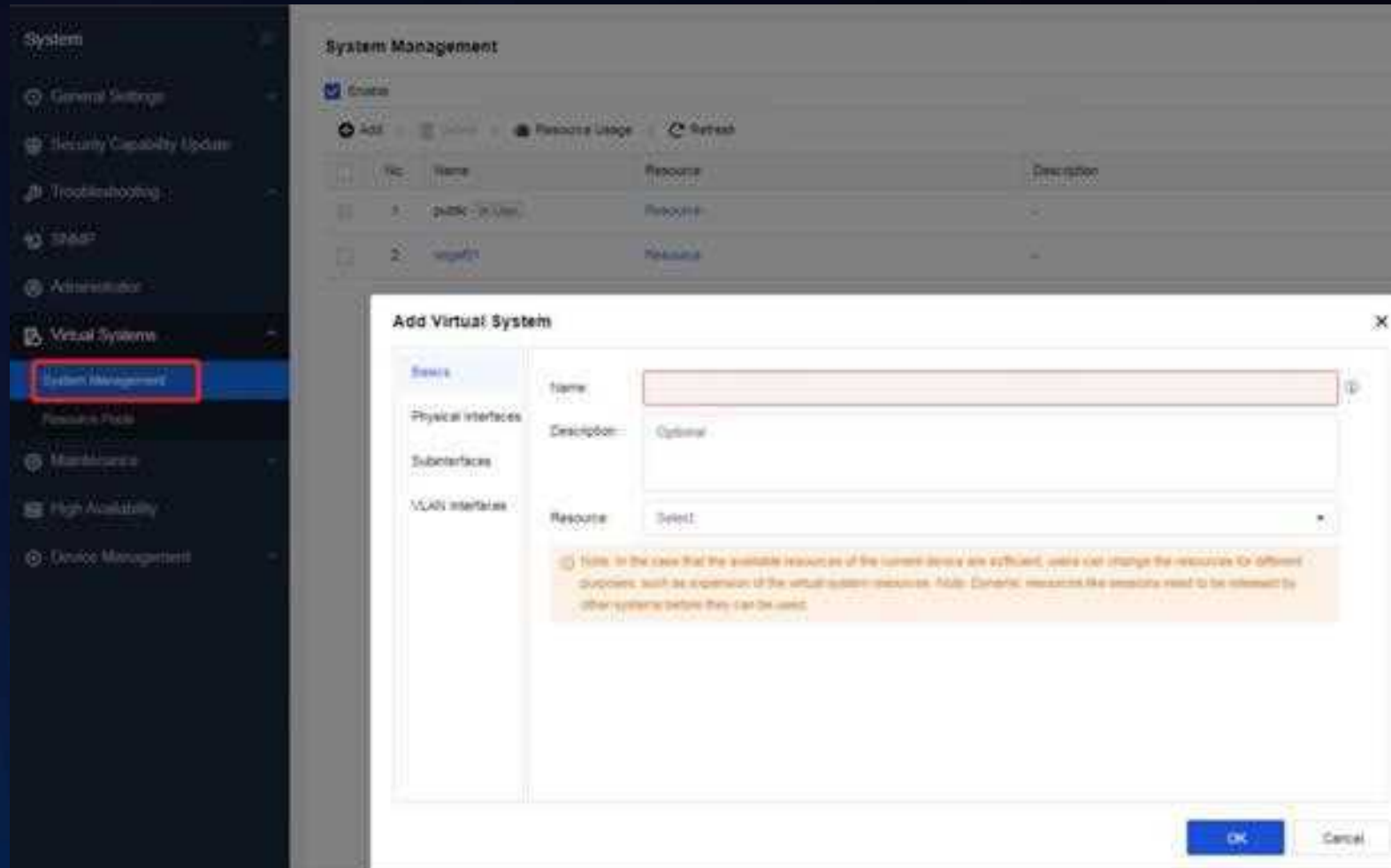
In Network Secure Platform, there is an huge modification in HA module to meet flexible network circumstances, for example it adds HA traffic, link aggregation, virtual IP and Group1. For this part we will introduce it in the doc file.

The screenshot shows the 'HA Policy Settings' page in the Network Secure Platform. On the left is a dark sidebar with a menu containing 'System', 'General Settings', 'Security Capability Update', 'Troubleshooting', 'SNMP', 'Administrator', 'Virtual Systems', 'Maintenance', 'High Availability' (highlighted with a red box), and 'Device Management'. The main content area is titled 'HA Policy Settings' and includes sections for 'HA Policy' (with 'Enable' checked and 'Active/Standby' selected), 'Mode' (set to 'standby 0.0.0.0/0.0.0.0'), 'Device Name', 'Control Link' (set to 'Select'), 'Data Link' (set to 'Optional'), 'Mirror Mode' (set to 'Enable'), and an 'Advanced' settings button. Below this is the 'Group 0' configuration section, which includes fields for 'Description', 'Priority' (set to 100), 'Proactive Preemption' (set to 'Enable'), and 'Virtual IP Address'. At the bottom, there is a table with columns for 'Interface', 'Virtual IP Network', 'Virtual MAC', and 'Operation'. The table is currently empty, and a message 'No data available' is displayed below it.

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.

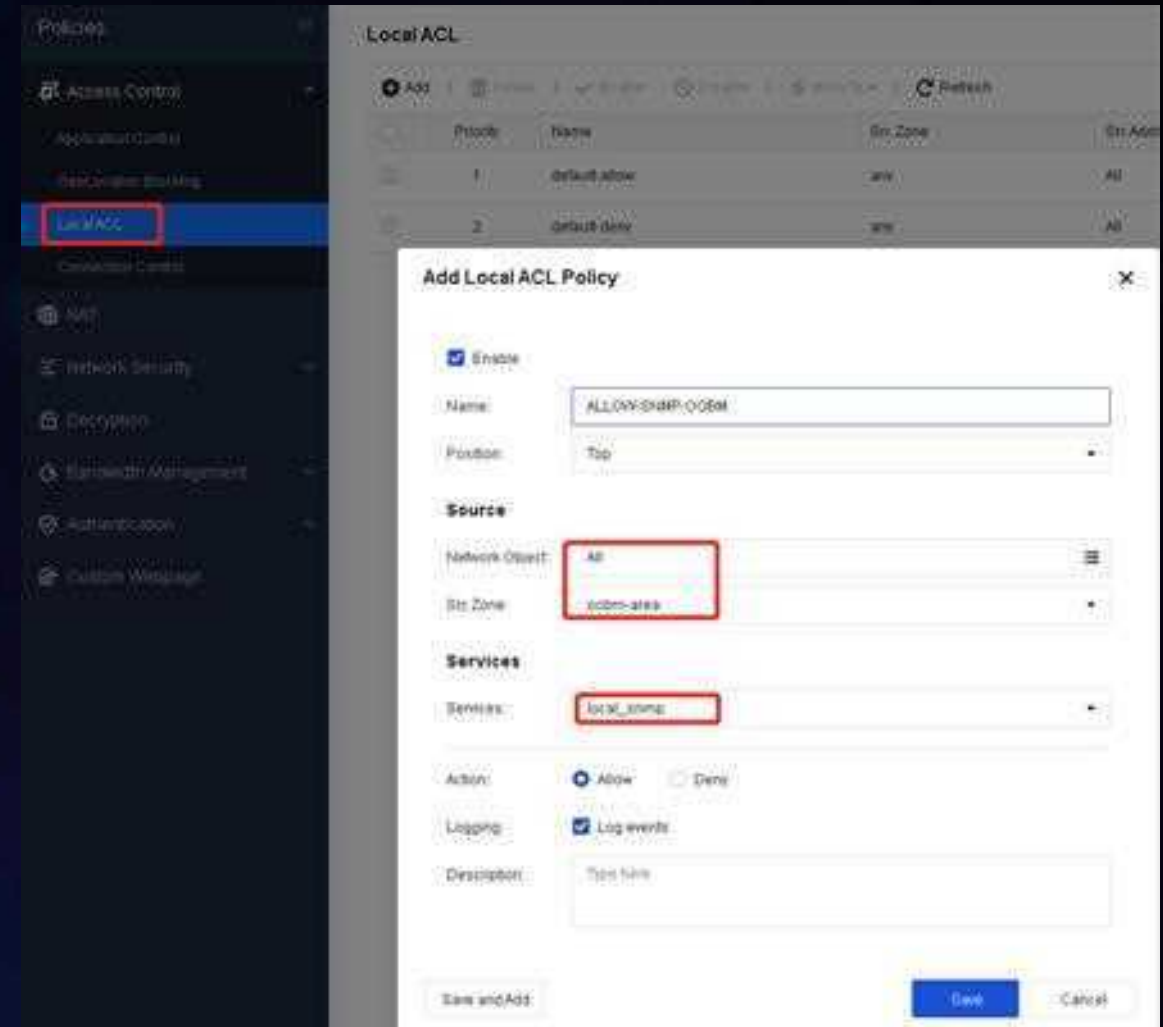
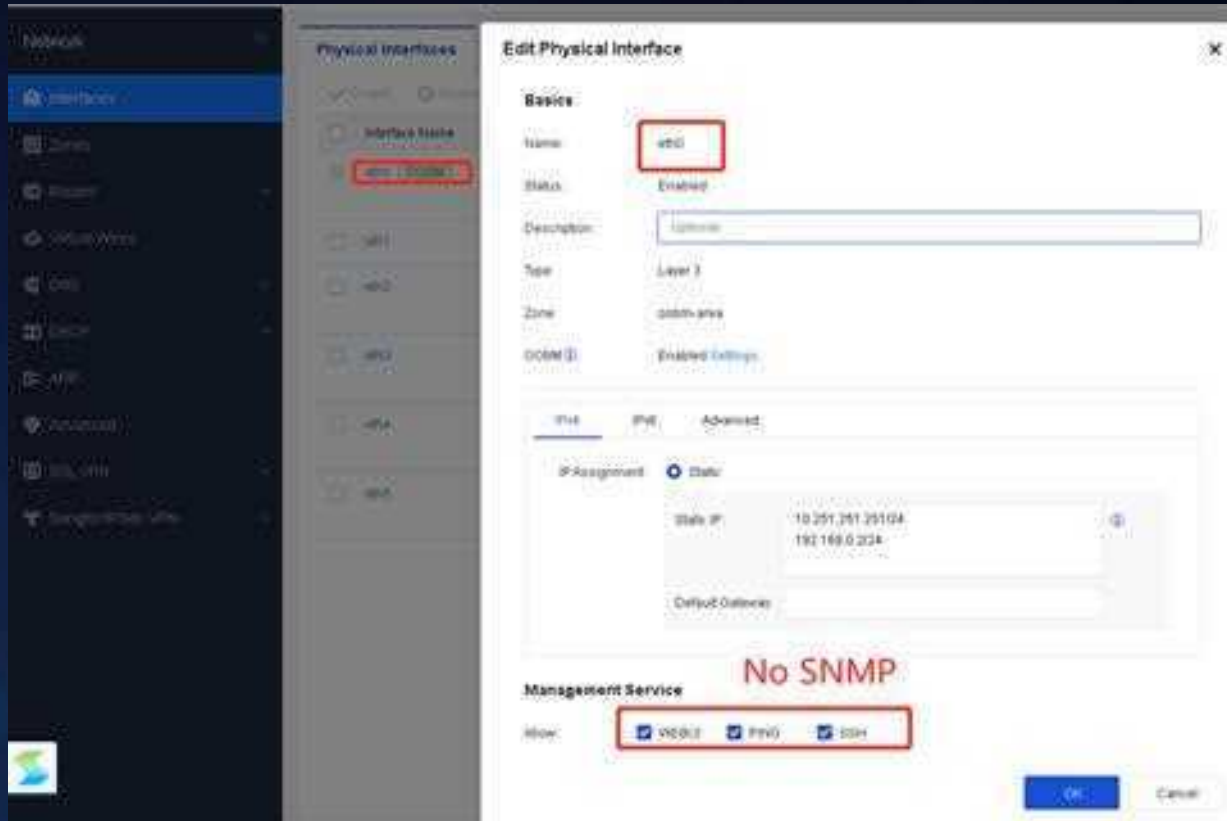
The screenshot displays the 'Physical Interfaces' configuration page in the Sangfor Network Secure Platform. A red box highlights the 'eth0' interface in the list. An 'Edit Physical Interface' dialog box is open, showing the configuration for 'eth0'. The 'Description' field is set to 'Optional'. The 'Type' is 'Layer 3'. The 'Zone' is 'admin-area'. The 'OSM' is 'Enabled Settings'. The 'IP Assignment' section shows 'Static' IP configuration. The 'Static IP' field contains '10.251.251.251/24' and '192.168.0.1/24'. The 'Default Gateway' field is set to '192.168.0.254', which is highlighted with a red box.

Link Mode	MTU (IPv4/IPv6)	Status	Operation
Full-duplex 1000Mbps	1500/1500	✓	Edit
Auto-negotiation failed	1500/1500	✓	Edit
Full-duplex 100Mbps	1500/1500	✓	Edit
Auto-negotiation failed	1500/1500	✓	Edit
Full-duplex 100Mbps	1500/1500	✓	Edit
Auto-negotiation failed	1500/1500	✓	Edit
Auto-negotiation failed	1500/1500	✓	Edit

SNMP--Out-of-band Management Interface



In Network Secure Platform, some customers would like to add SNMP monitoring 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.



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.

System

General Settings

Web UI

Network

Email & SMS Server

System Time

NTP Key

HOSTS

Licensing

OoBM

Policy Options

Security Capability Update

Troubleshooting

SNMP

Administrator

Virtual Systems

Virtual Systems

High Availability

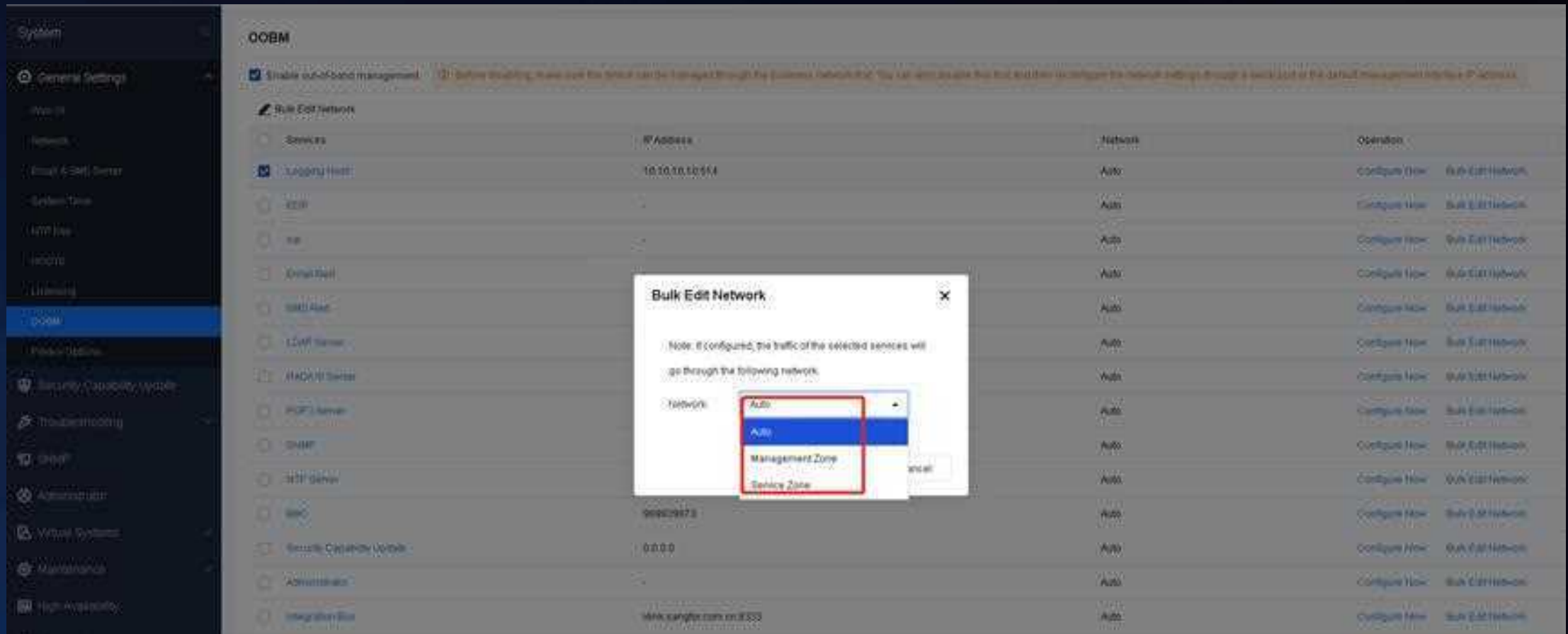
OoBM

☐ Enable out-of-band management

☒ Run Out-Of-Band

Service	IP Address	Version	Options
<input type="checkbox"/> Logging Host	10.10.10.10	Auto	Configure Now Bulk Edit Network
<input type="checkbox"/> EDH	-	Auto	Configure Now Bulk Edit Network
<input type="checkbox"/> HA	-	Auto	Configure Now Bulk Edit Network
<input type="checkbox"/> Email host	-	Auto	Configure Now Bulk Edit Network
<input type="checkbox"/> SMS host	-	Auto	Configure Now Bulk Edit Network
<input type="checkbox"/> LDAP Server	-	Auto	Configure Now Bulk Edit Network
<input type="checkbox"/> Radius Server	-	Auto	Configure Now Bulk Edit Network
<input type="checkbox"/> POP3 Server	-	Auto	Configure Now Bulk Edit Network
<input type="checkbox"/> SMTP	-	Auto	Configure Now Bulk Edit Network
<input type="checkbox"/> NTP Server	2004:12:04	Auto	Configure Now Bulk Edit Network
<input type="checkbox"/> RBC	801000072	Auto	Configure Now Bulk Edit Network
<input type="checkbox"/> Security Capability Update	0.0.0.0	Auto	Configure Now Bulk Edit Network
<input type="checkbox"/> Administrator	-	Auto	Configure Now Bulk Edit Network
<input type="checkbox"/> Integration Bus	http://sangfor.com.cn:8229	Auto	Configure Now Bulk Edit Network

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.

Add Administrator

Username:

Status: ☒ Enabled ☐ Disabled

Description:

Auth Method:

Role:

Local authentication
Local Authentication
Remote Authentication
Remote/Local Authentication

Auth Policy:

Password:

Confirm Password:

Management Method: ☒ Web UI ☐ SSH

OK Cancel

External Auth Server

☒ Enable

Name:

Authentication Method: ☐ TACACS ☒ RADIUS

Auth Options: ☒ Authenticate with remote admin

Server Options

IP Address:

Port:

Shared Key:

Protocol:

Test Validity

Save Cancel

IPSec VPN



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

The screenshot displays the Sangfor Network Secure Platform's configuration interface. On the left, a dark sidebar contains a menu with options like Network, Interfaces, Zones, Routes, Virtual Wires, DNS, DHCP, ARP, Advanced, SSL VPN, SangforIPSec VPN, and IPSec VPN (which is highlighted with a red box). The main area shows the 'IPSec VPN Configuration' wizard. A red box highlights the 'Add Connection' button. The 'Add Connection' dialog box is open, showing fields for Device Name, Description, Status (Enabled/Disabled), Protocol (IPv4/IPv6, with IPv6 selected and highlighted by a red box), Peer IP Address Type (Static IP), Peer IP Address (Example: 2001::1::1), Auth Method (Pre-shared Key), Shared Key, Confirm Key, and Local Outbound Interface. The 'Others' section includes an 'Encrypted Traffic' checkbox and 'Add'/'Delete' buttons. 'OK' and 'Cancel' buttons are at the bottom right.

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.

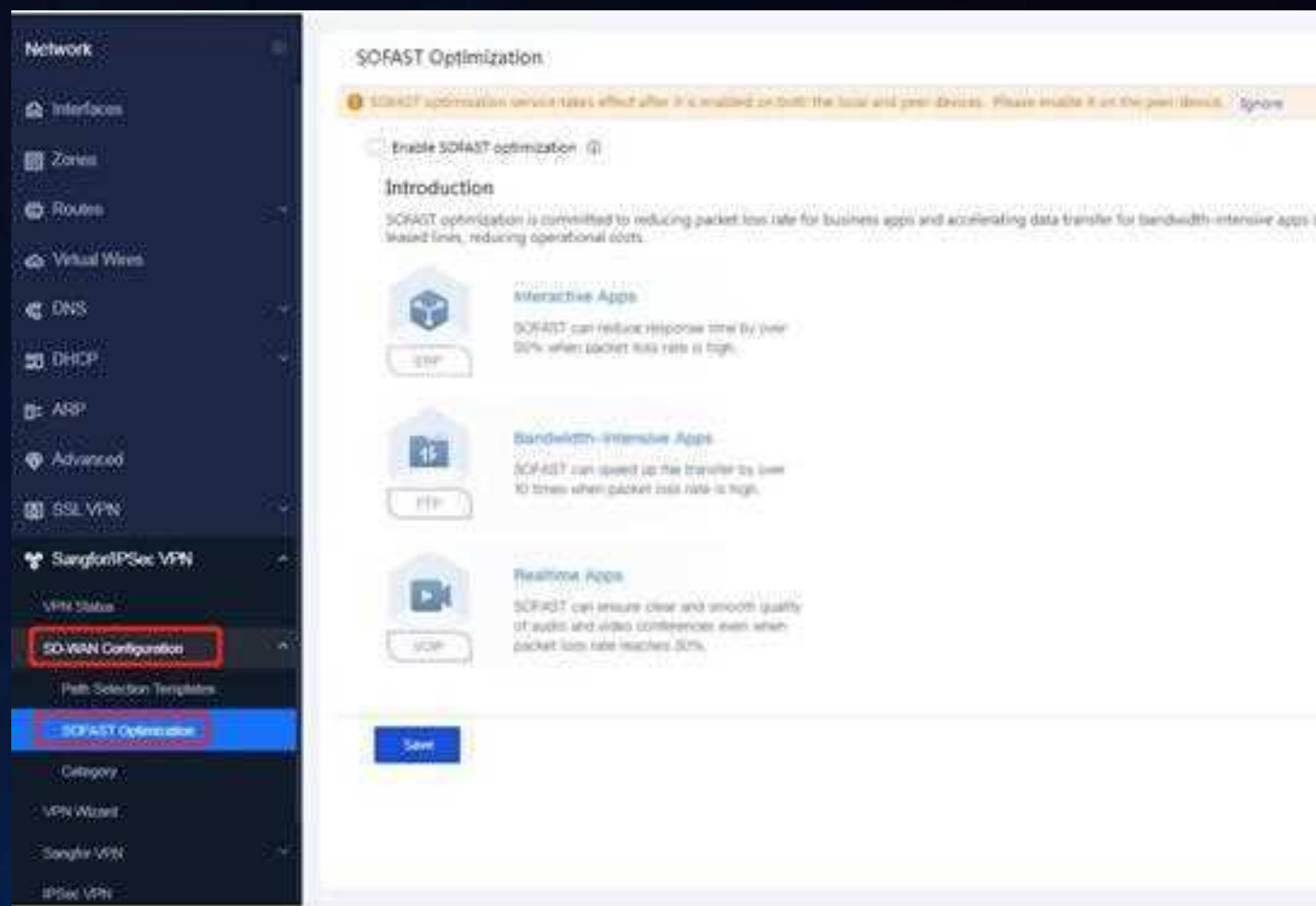
The screenshot displays the 'SD-WAN Path Selection Template (VPN HQ): 0630' configuration page. On the left, a sidebar menu lists various network settings, with 'Path Selection Template' highlighted. The main panel shows a list of policies, including 'VPN' and 'Default Policy'. The 'Edit Policy' dialog is open, showing the 'Path Selection Settings' section. This section includes a 'Mode' dropdown set to 'AutoGO Smart Path Selection', a 'Specify Src/Dst IP' field, and a 'Paths' table. The 'Paths' table lists two paths: 'Path 1 (Static IP-China Mobile)' and 'Path 2 (Static IP-China Unicom)'. The 'Operation' column for each path has a 'Delete' button. The 'More Options' section at the bottom has an 'Advanced' button.

Local Path	Peer Path	Operation
Path 1 (Static IP-China Mobile)	Link 1	Delete
Path 2 (Static IP-China Unicom)	Link 1	Delete

SOFAST Optimization



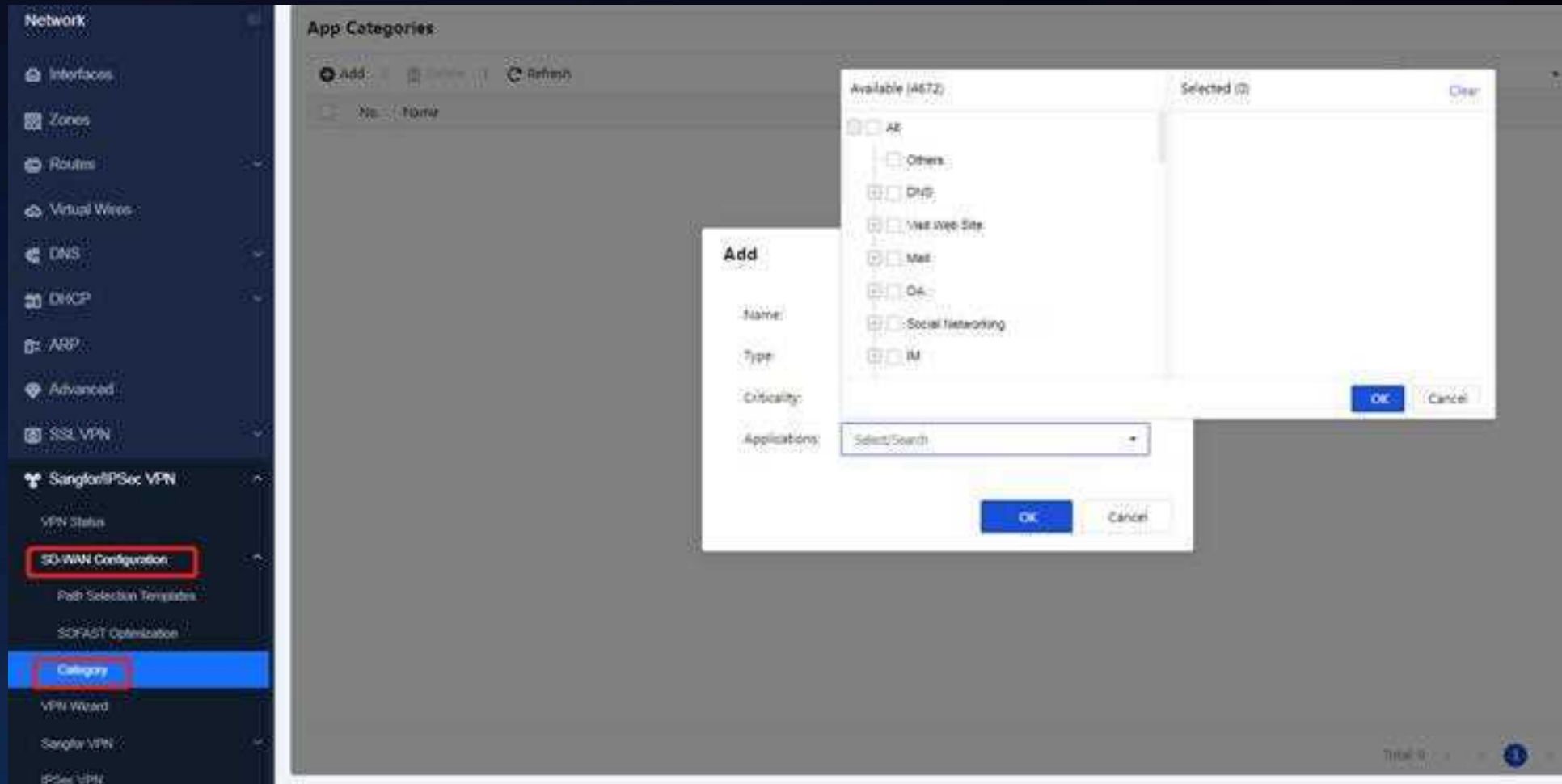
In Network Secure Platform, SOFAST optimization is committed to reducing packet loss rate for business apps and accelerating data transfer for bandwidth-intensive apps so that the user experience of using apps with data going through common lines can be almost the same as that provided by leased lines,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



Application Category



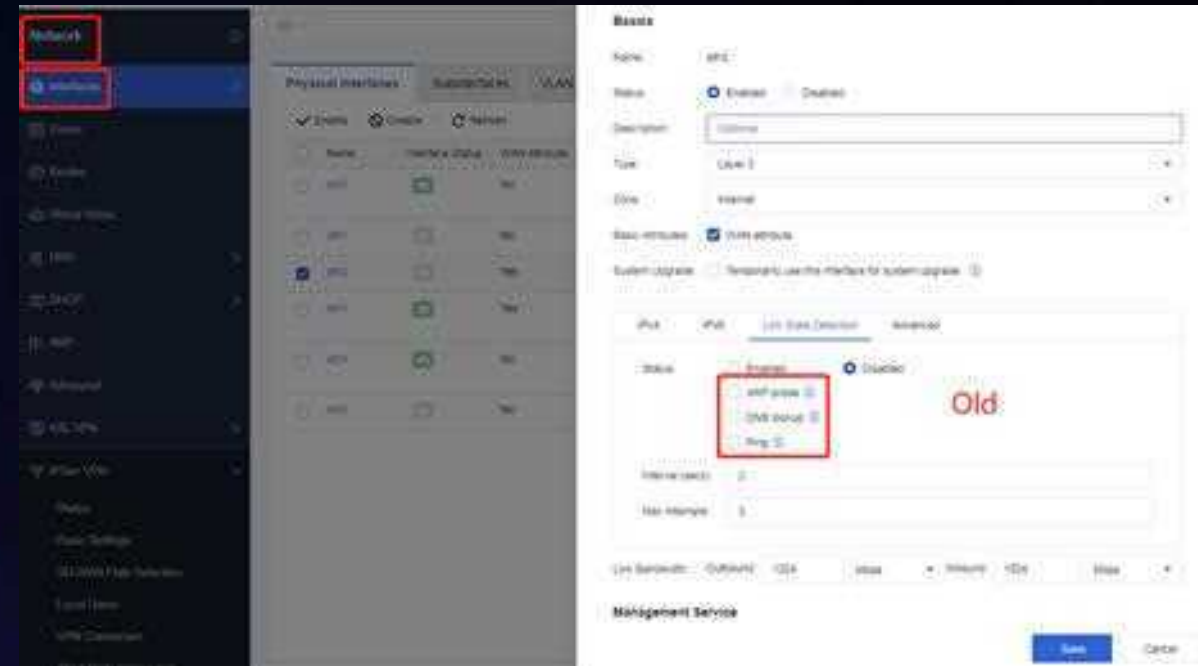
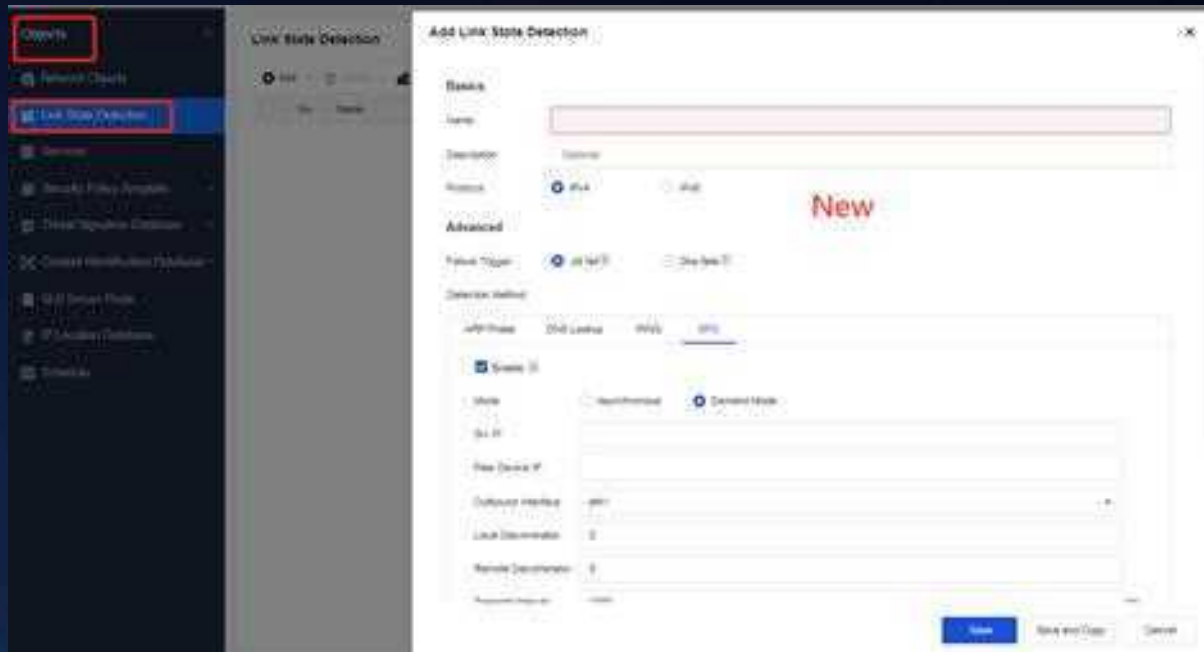
In Network Secure Platform, it add new application categories, and can define related business applications for reference in SDWAN path selection.



Link State Detection



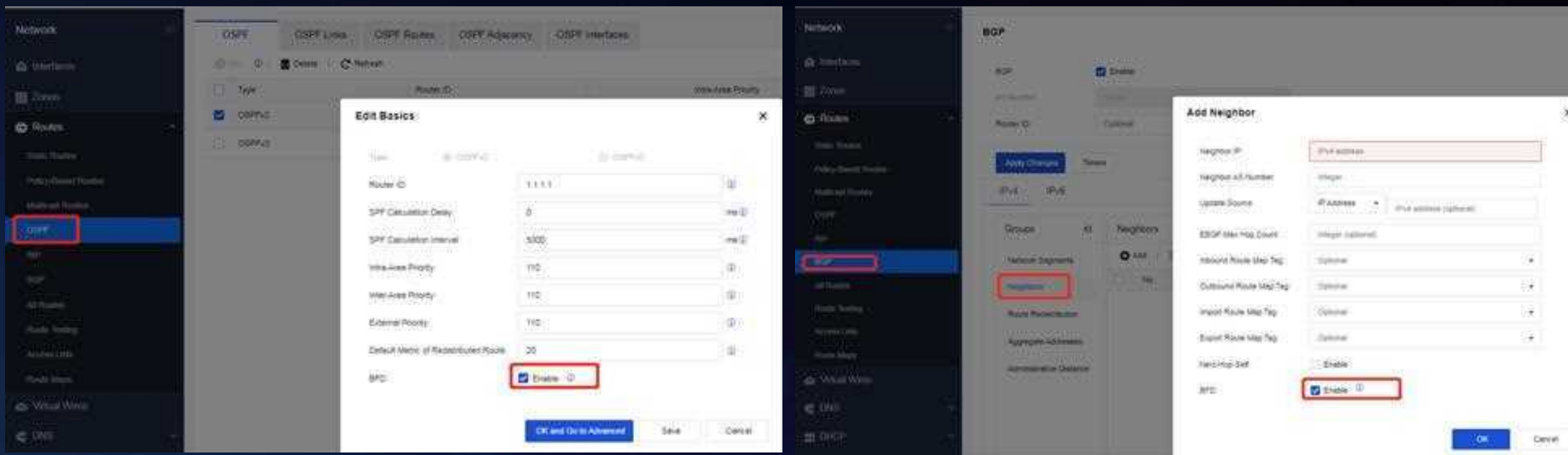
In Network Secure Platform, it adds a new menu page for link state detection, which allows configuration of link state detection for interfaces. Meanwhile, BFD link detection method has also been added.



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.

The screenshot displays the Sangfor Network Security Manager interface. On the left, the 'Objects' menu is open, with 'Link State Detection' highlighted. The main panel shows the 'Link State Detection' configuration page, which includes a table with columns 'No.', 'Name', and 'Protocol'. The table contains one entry with 'No.' 1, 'Name' 0625, and 'Protocol' IPv4. To the right, the 'Static Routes' configuration page is visible, showing a list of static routes. The 'Add Static Route' dialog box is open, showing the 'Advanced' tab. In the 'Advanced' tab, the 'Link State' checkbox is checked, and the 'Link State' dropdown menu is set to 'Link State'.

Link State Detection

No.	Name	Protocol
1	0625	IPv4

Static Routes

Add Static Route

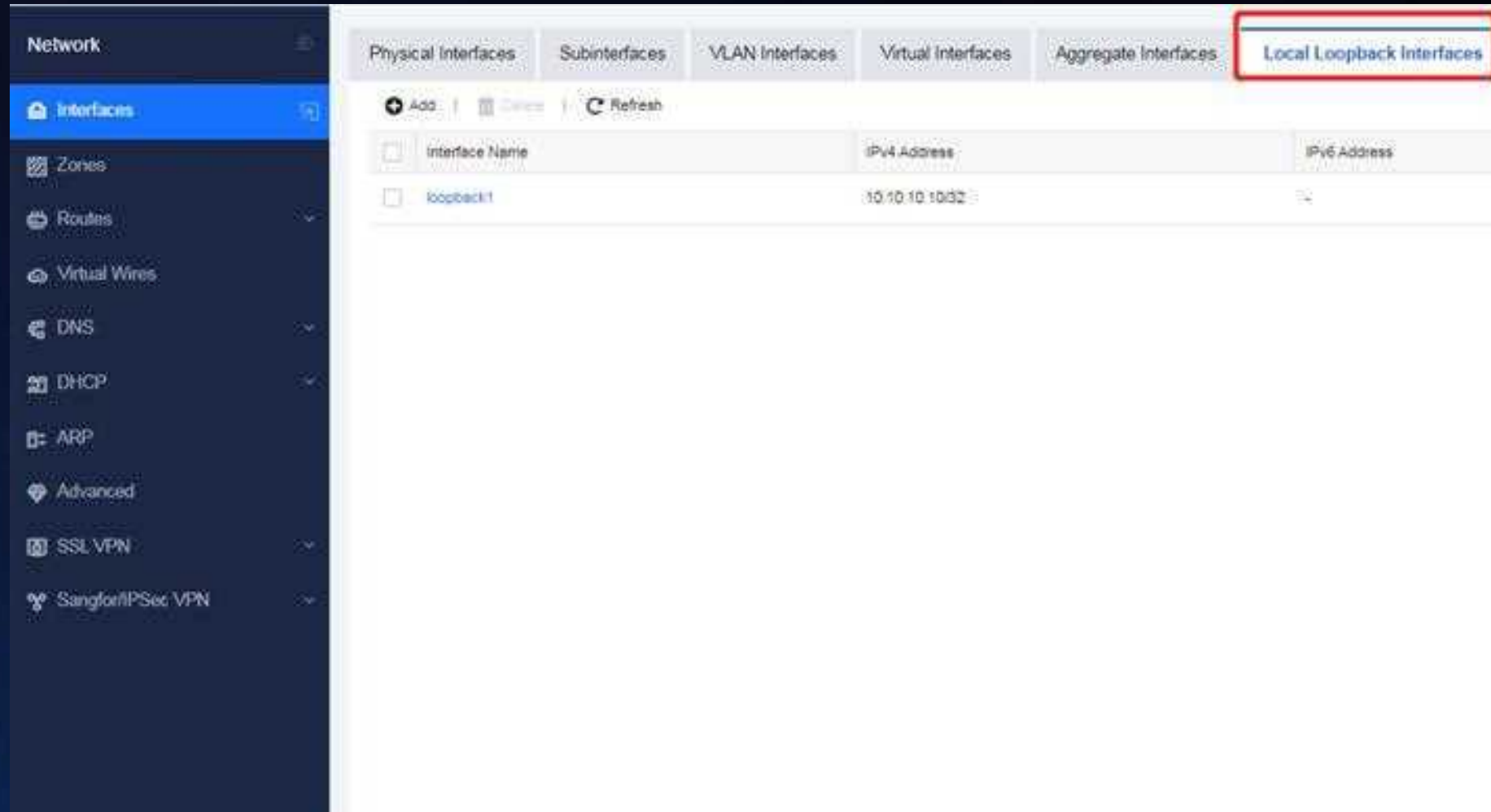
Advanced

Link State

Local Loopback Interface



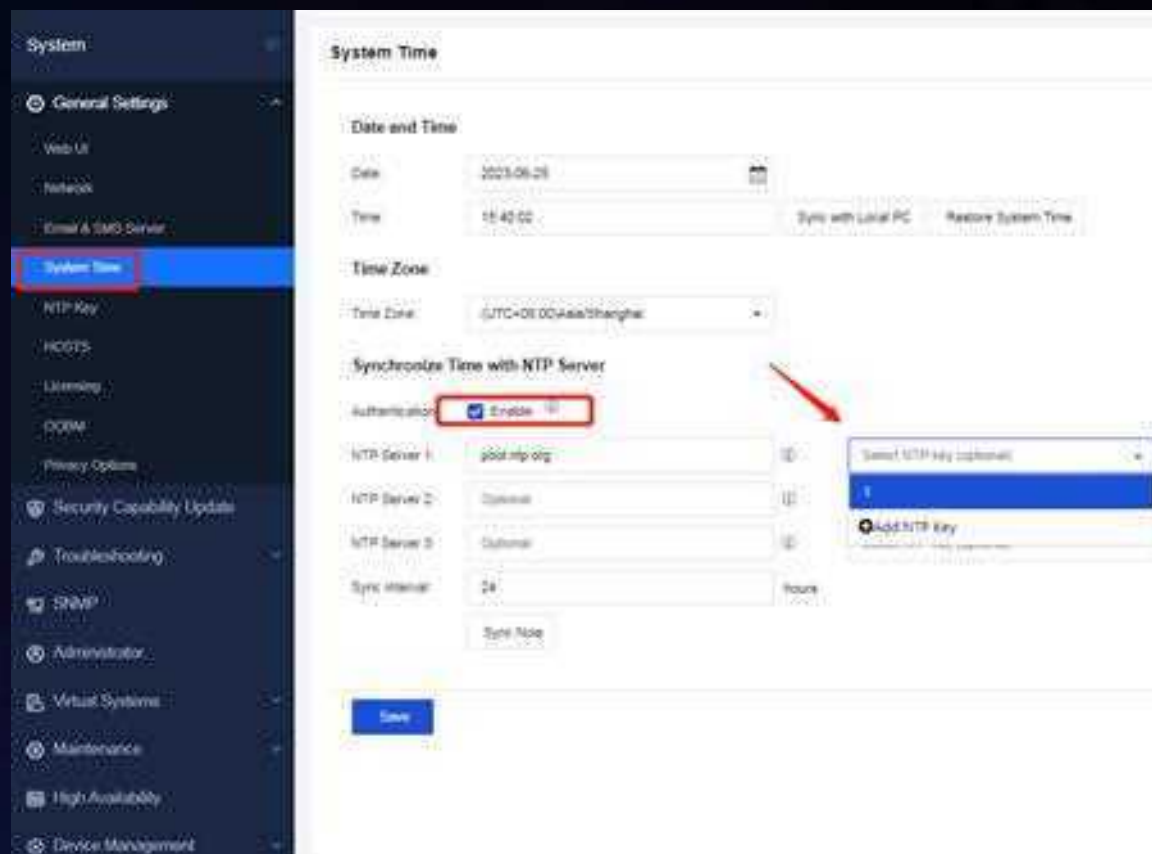
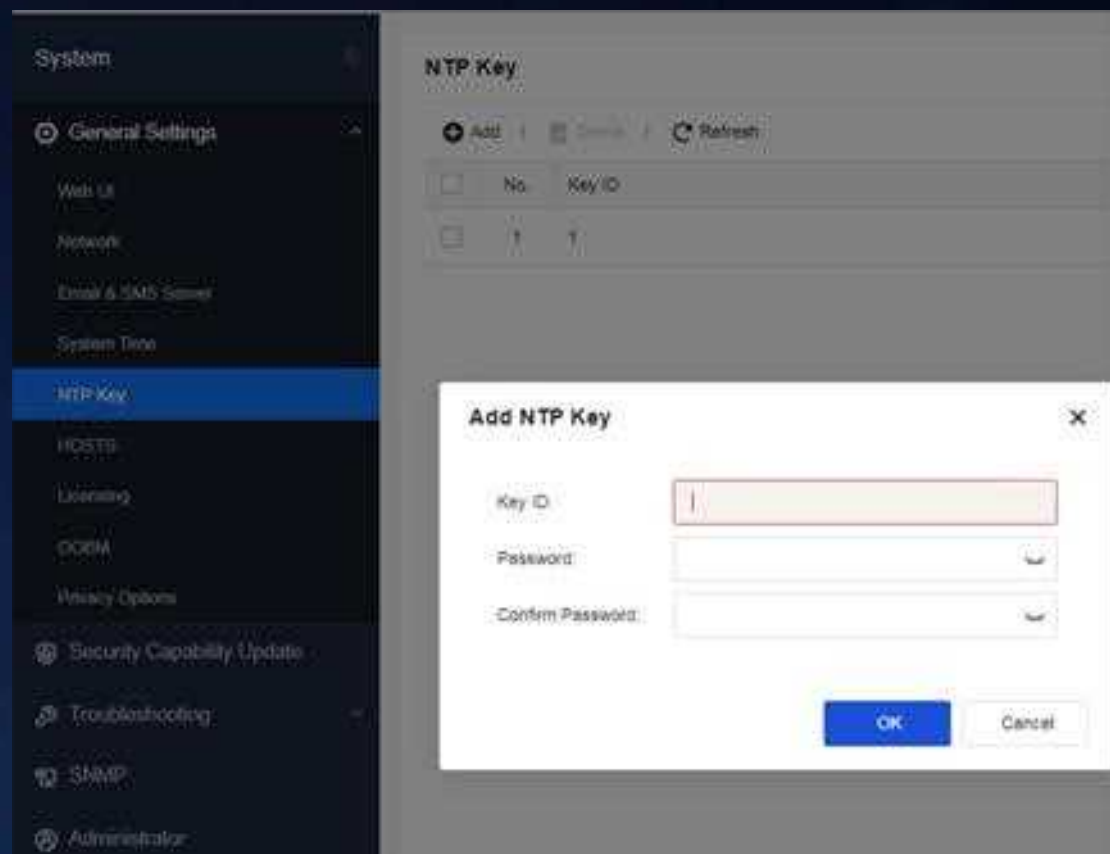
In Network Secure Platform, it adds the local loopback type interface which is an ordinary layer-3 interface and always up.



NTP Key



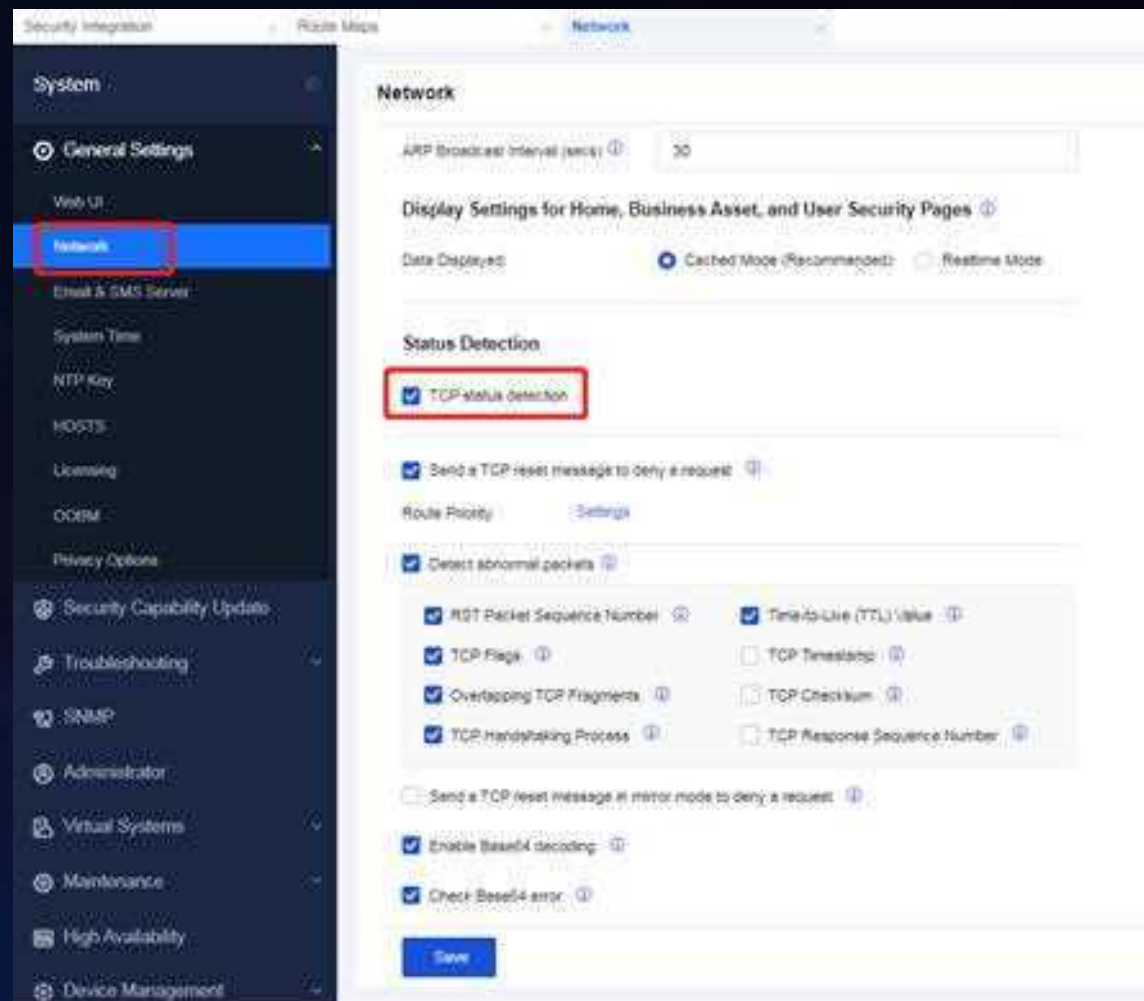
In Network Secure Platform, it adds NTP key feature which can meet the scenario of enabling NTP server authentication.



Network Parameter



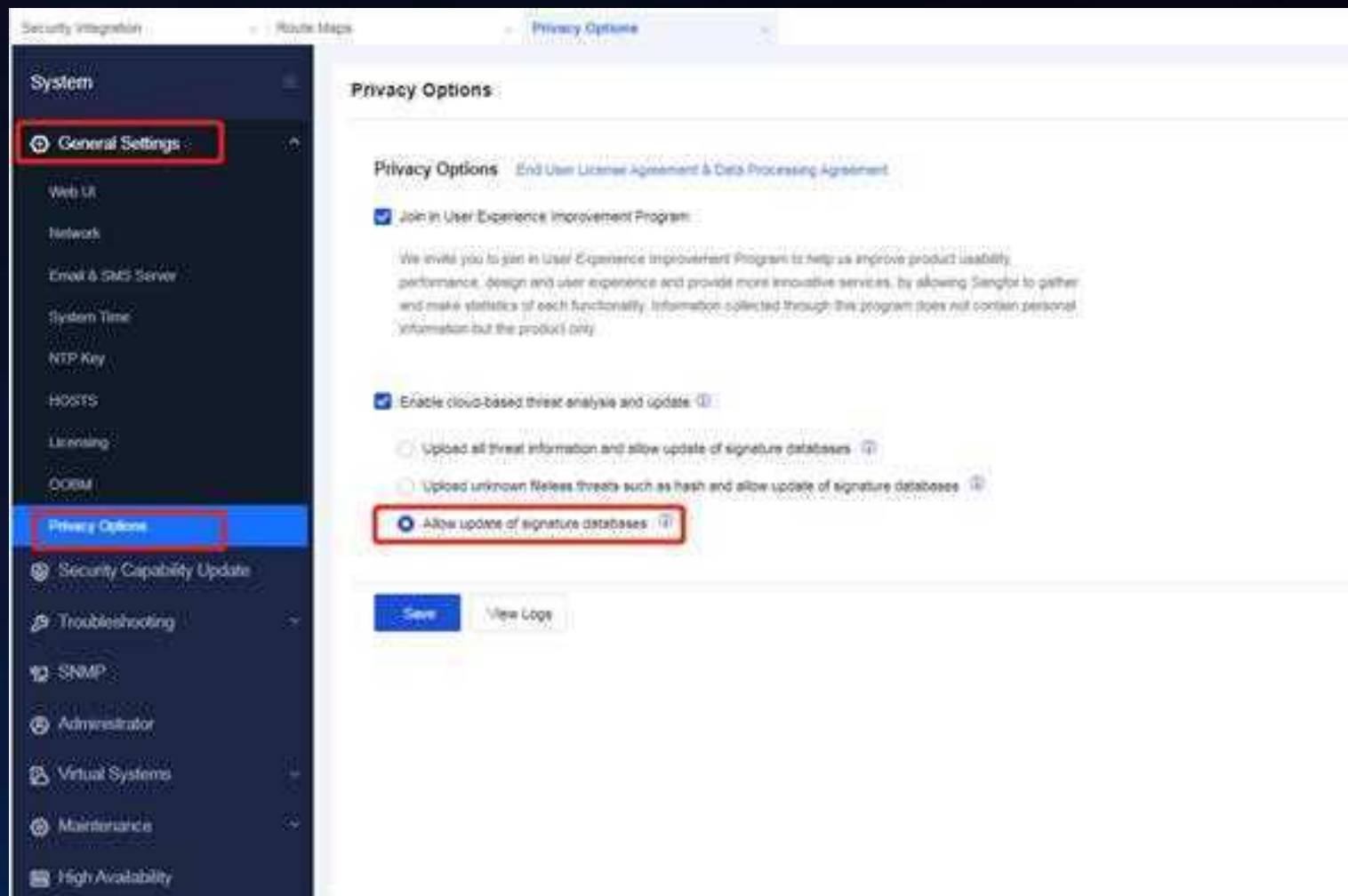
In Network Secure Platform, it adds the global network parameter of TCP status detection, which checks the state of flag bits in the first TCP data packet transmitted through to TCP malformed packet attacks and enhance the security of TCP connections.



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.

The screenshot displays the 'Troubleshooting' section of the Sangfor Network Secure Platform. The 'Method' dropdown is set to 'Analysis of Traffic to NGAF'. The 'Status' is 'Allowed'. The 'Src IP' is '172.16.10.10' and the 'Protocol' is 'All'. A red box highlights the 'Analysis of Traffic to NGAF' method. Another red box highlights the status 'Allowed'. A third red box highlights the message 'Packet is allowed as per matched policy'.

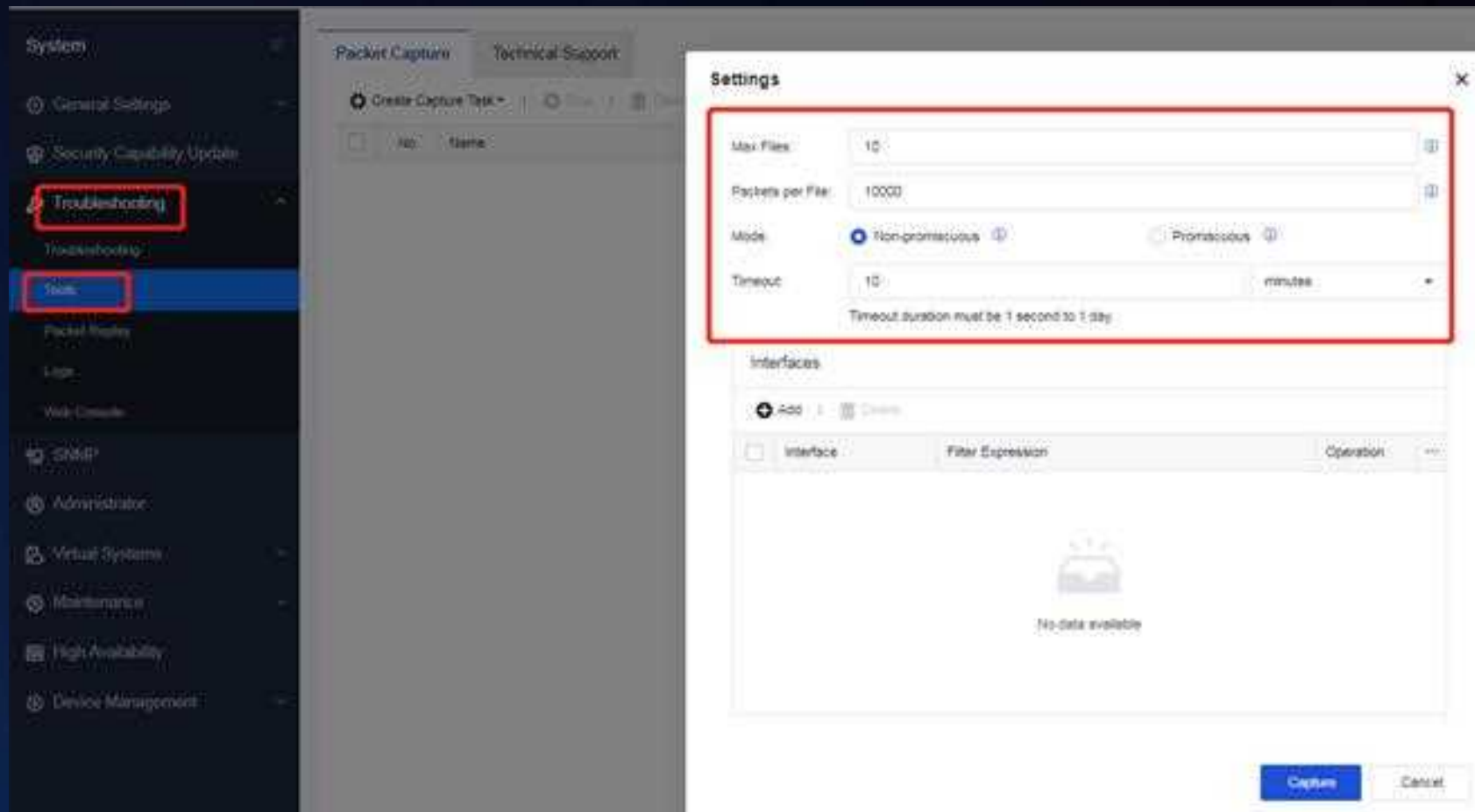
Below the configuration, there is a 'Run OK' button and a 'Results (20)' section. The results are displayed in a table with columns: No., Time Occurred, Src IP, Dest IP, Dest Port, Protocol, Inbound Interface, Status, Description, and Name.

No.	Time Occurred	Src IP	Dest IP	Dest Port	Protocol	Inbound Interface	Status	Description	Name
1	10/10/20	172.16.10.10	172.16.10.1	8080	TCP	eth0	allowed	Passed Through the Firewall	default policy
2	10/10/20	172.16.10.10	172.16.10.1	8080	TCP	eth0	allowed	Passed Through the Firewall	default policy
3	10/10/20	172.16.10.10	172.16.10.1	8080	TCP	eth0	allowed	Passed Through the Firewall	default policy
4	10/10/20	172.16.10.10	172.16.10.1	8080	TCP	eth0	allowed	Passed Through the Firewall	default policy

Rolling Capture Packet



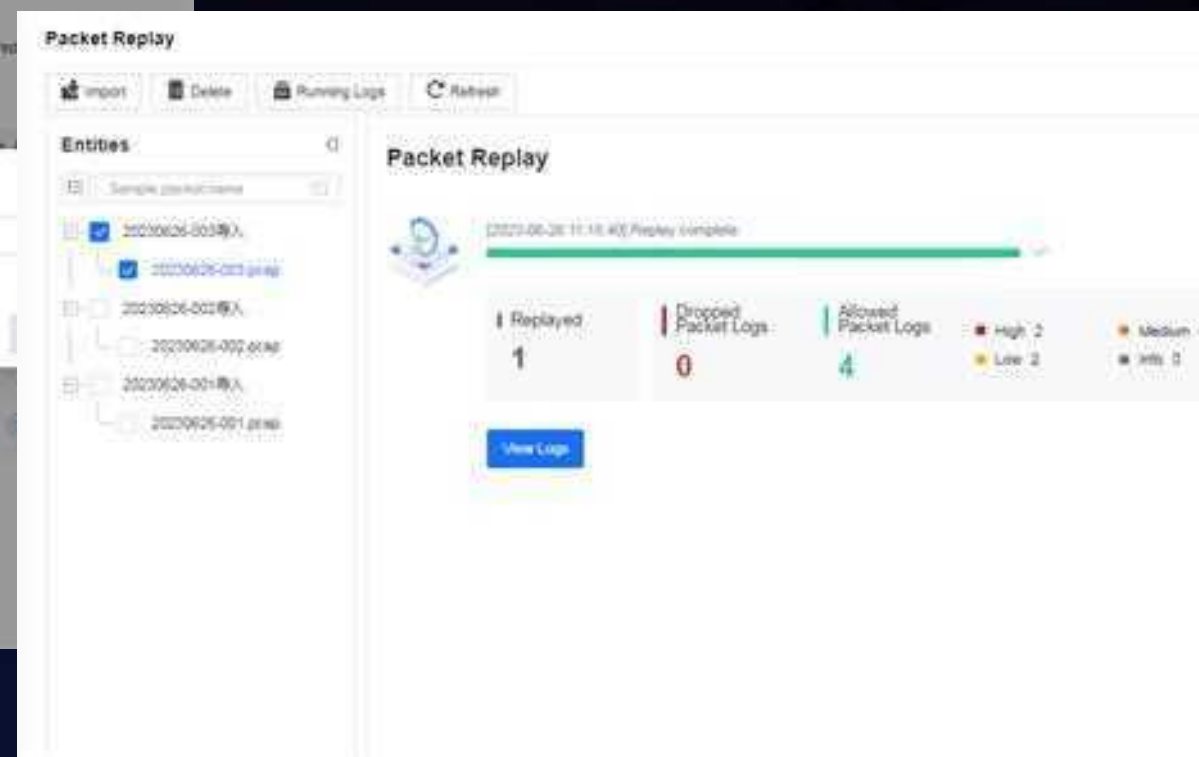
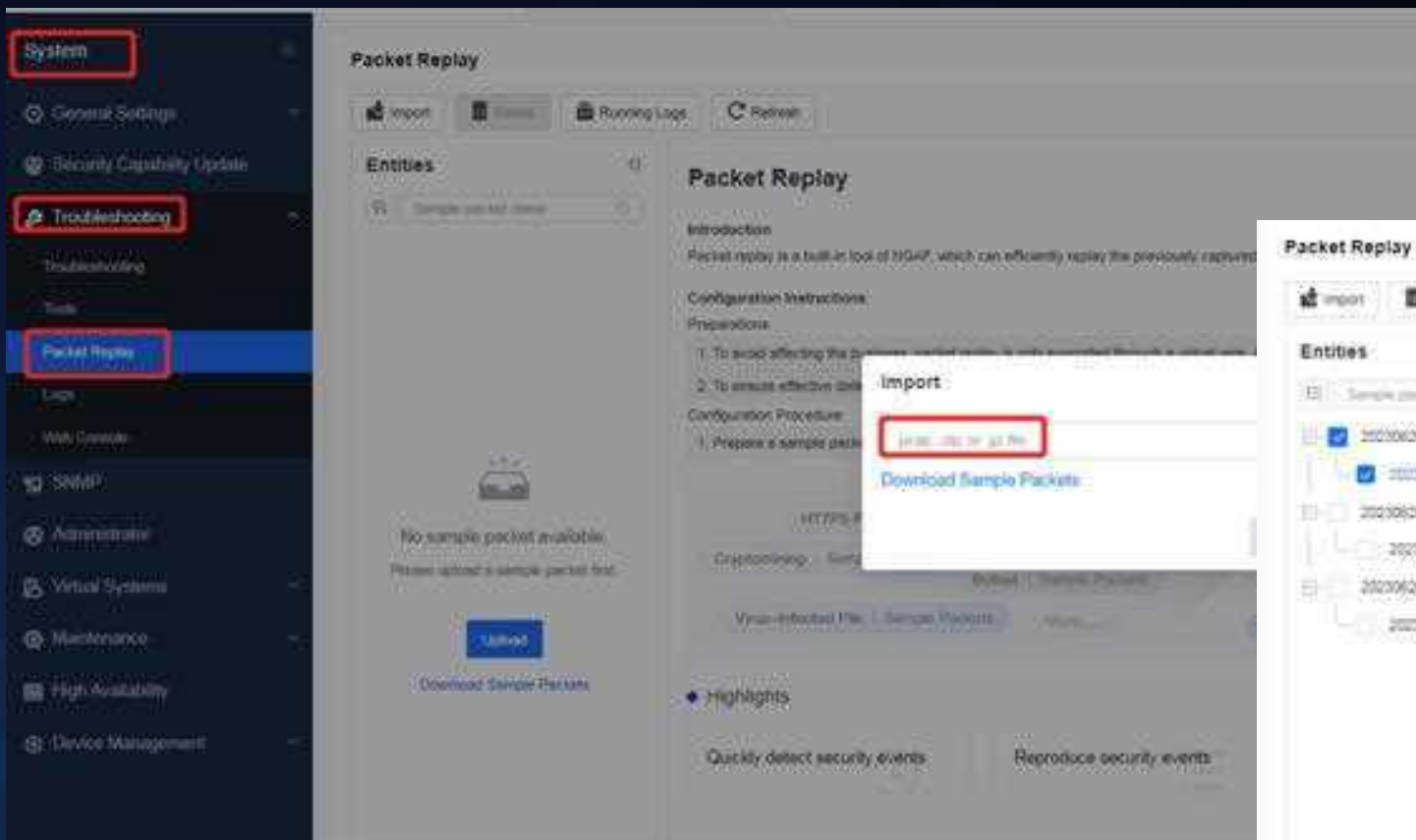
In Network Secure Platform, it adds rolling capture packet feature which is mainly used for troubleshooting intermittent network issues. Main settings of this feature contains max files and packets per file, and if the task exceeds max files counts it will delete earlier data. The timeout range is 24 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.

Packet Tracing

Monitor | TOP N | Logs | Sessions | Statistics | Report | Diagnose | **Packet Tracing** | Settings

Packet Tracing

Refresh | Export | Clear Analysis Results

Week: Src IP (172.16.10.10) | Src Port (443) | Dst IP (443) | Dst Port (443) | Protocol (443) | Inbound interface (eth0)

Flows	No.	Status	Inbound Interface	Outbound Interface	Time
Flow 1 172.16.10.10:10000 → 142.250.186.74:443	Packet 1	Forwarded	eth0	eth0	2023
Flow 2 172.16.10.10:10000 → 142.250.186.74:443	Packet 2	Forwarded	eth0	eth0	2023
Flow 3 172.16.10.10:10000 → 142.250.186.74:443	Packet 3	Forwarded	eth0	eth0	2023
Flow 4 172.16.10.10:10000 → 142.250.186.74:443	Packet 4	Forwarded	eth0	eth0	2023
Flow 5 172.16.10.10:10000 → 142.250.186.74:443	Packet 5	Forwarded	eth0	eth0	2023
Flow 6 172.16.10.10:10000 → 142.250.186.74:443	Packet 6	Forwarded	eth0	eth0	2023
Flow 7 172.16.10.10:10000 → 142.250.186.74:443	Packet 7	Forwarded	eth0	eth0	2023
Flow 8 172.16.10.10:10000 → 142.250.186.74:443	Packet 8	Forwarded	eth0	eth0	2023
Flow 9 172.16.10.10:10000 → 142.250.186.74:443	Packet 9	Forwarded	eth0	eth0	2023
Flow 10 172.16.10.10:10000 → 142.250.186.74:443	Packet 10	Forwarded	eth0	eth0	2023

Flow 3 - Packet 5 510 packets Preview Test

L3 Forwarding Forwarded

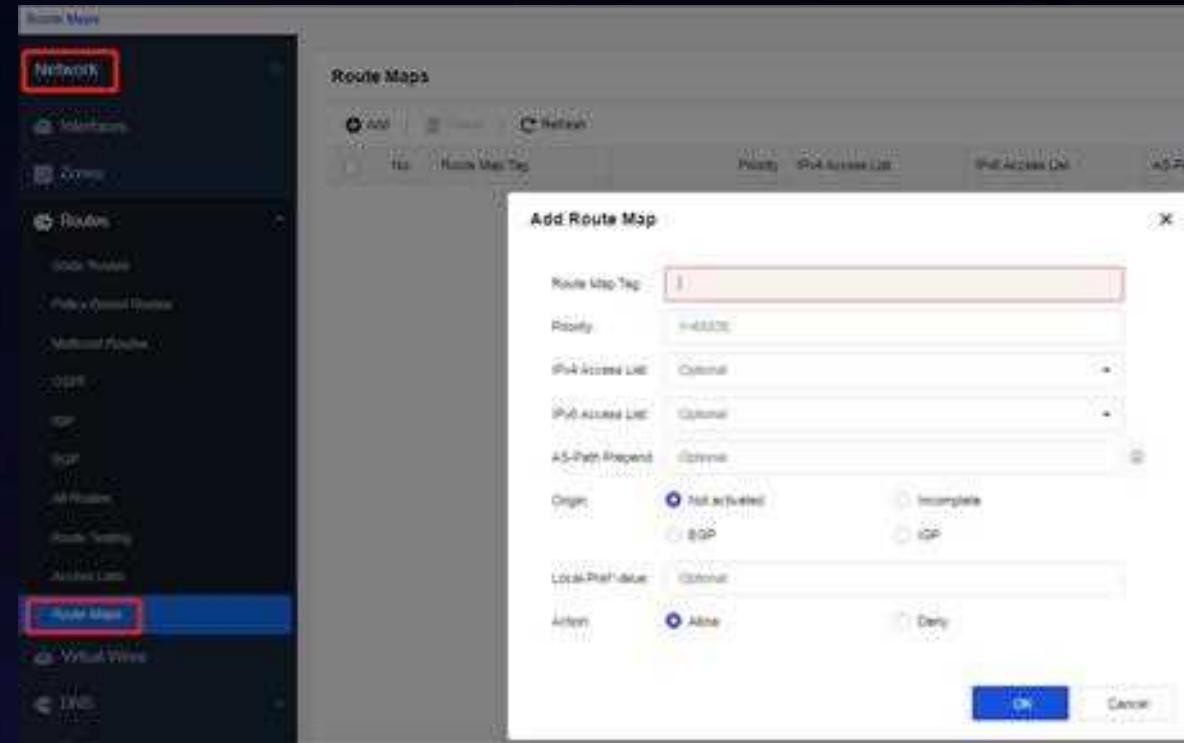
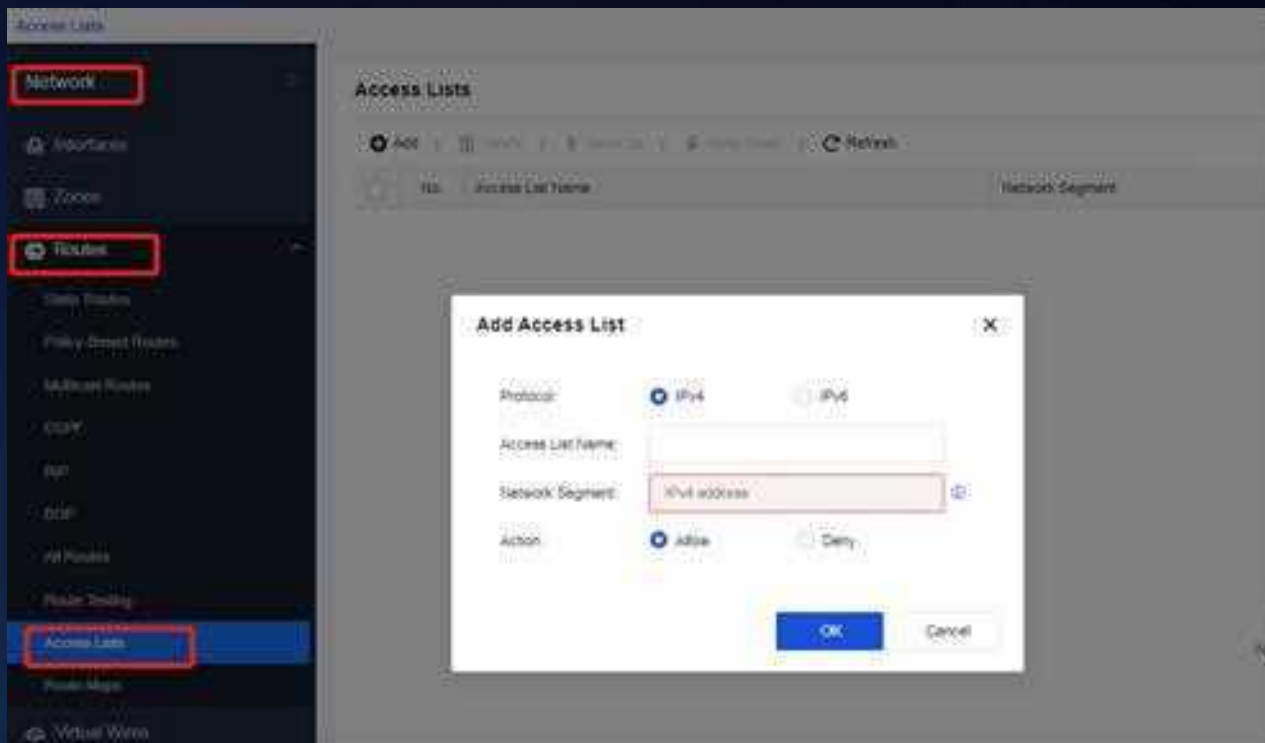
Inbound interface: eth0 Outbound interface: eth0

- Receive Packet
- Pre-check Data Link Layer
- Check Inbound Interface
- Packet integrity check
- Special packet processing
- Session Details
 - An existing session was matched. Session ID: 432C
- Session update
- TCP packet processing
- Packet modification during NAT
- TTL processing for IP headers
- Packet sending on interface
- NAT packet sending
- Send Packet

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.

The screenshot displays the NGAF Platform interface, specifically the Threat Intelligence module. The left sidebar shows the SOC menu with Threat Intelligence highlighted. The main content area displays a table of vulnerabilities.

No.	Date Added	Description	Threat Level	Protection	Operation
1	2022-12-09	Apache APISIX Remote Code Execution Vulnerability (CVE-2022-4111)	High Threat	Unscanned	Scan Now
2	2022-11-26	HTTP Protocol Stack Remote Code Execution Vulnerability (CVE-2022-1987)	High Threat	Unscanned	Scan Now
3	2022-11-11	Remote Code Execution Vulnerability in Apache Commons Text (CVE-2022-42889)	High Threat	Unscanned	Scan Now
4	2022-11-04	Oracle Access Manager Remote Code Execution Vulnerability (CVE-2021-45887)	High Threat	Unscanned	Scan Now
5	2022-10-26	Format Authentication Bypass Vulnerability (CVE-2022-45584)	High Threat	Unscanned	Scan Now
6	2022-10-21	Apache Spark Command Injection Vulnerability	High Threat	Unscanned	Scan Now
7	2022-10-14	VMware Server Side Template Injection Vulnerability (CVE-2022-27946)	High Threat	Unscanned	Scan Now
8	2022-09-30	Windows Remote Procedure Call Runtime Remote Code Execution Vulnerability (CVE-2022-35029)	High Threat	Unscanned	Scan Now
9	2022-09-23	Windows LSA Spoofing Vulnerability (CVE-2022-35029)	High Threat	Unscanned	Scan Now
10	2022-09-16	PDF Remote Code Execution Vulnerability (CVE-2022-31526)	High Threat	Unscanned	Scan Now
11	2022-09-14	Firefox autoType Remote Code Execution Vulnerability (CVE-2022-29445)	High Threat	Unscanned	Scan Now
12	2022-08-26	Microsoft Office File Injection Vulnerability (CVE-2022-43247)	High Threat	Unscanned	Scan Now
13	2022-08-19	Microsoft Windows Support Diagnostic Tool (MSDT) Remote Code Execution Vulnerability (CVE-2022-34711)	High Threat	Unscanned	Scan Now
14	2022-08-12	Windows SMB (Send of Notifications) Vulnerability (CVE-2022-33236)	High Threat	Unscanned	Scan Now
15	2022-08-05	Linux Remote Code Execution Vulnerability (CVE-2021-42889)	High Threat	Unscanned	Scan Now
16	2022-07-26	Apache Tomcat Denial of Service Vulnerability (CVE-2022-29055)	High Threat	Unscanned	Scan Now
17	2022-07-22	Atlassian Jira Server Side Request Forgery Vulnerability (CVE-2022-29136)	High Threat	Unscanned	Scan Now

Signature Model Training



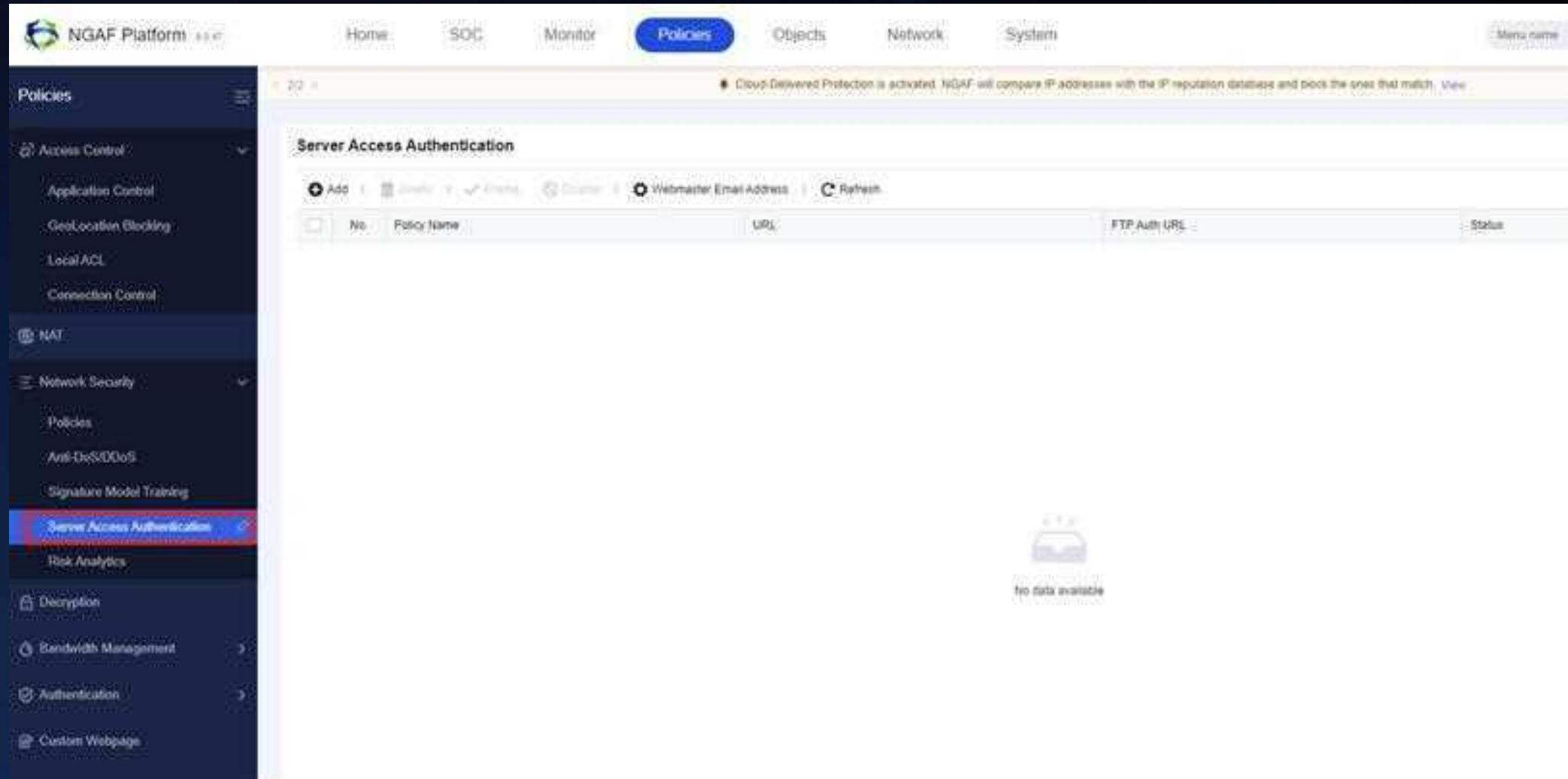
In Network Secure Platform, it deletes the Signature Model Training module.

The screenshot displays the NGAF Platform interface. The left sidebar contains a navigation menu with the following items: Policies, Access Control, Application Control, GeoLocation Blocking, Local ACL, Connection Control, NAT, Network Security, Policies, Anti-DDoS, **Signature Model Training** (highlighted with a red box), Server Access Authentication, Risk Analytics, Decryption, Bandwidth Management, Authentication, and Custom Webpage. The main content area is titled "Signature Model Training" and includes a "Business Assets (0)" section with a search bar and a "No data available" message. Below this, there is a "Pending Threat Signatures (0)" and "Marked Threat Signatures (0)" section, also with a "No data available" message. A table is visible at the bottom with columns: No., Signature Model, URL, Statement, Visits, Time, and Operation. The table is currently empty.

Server Access Authentication



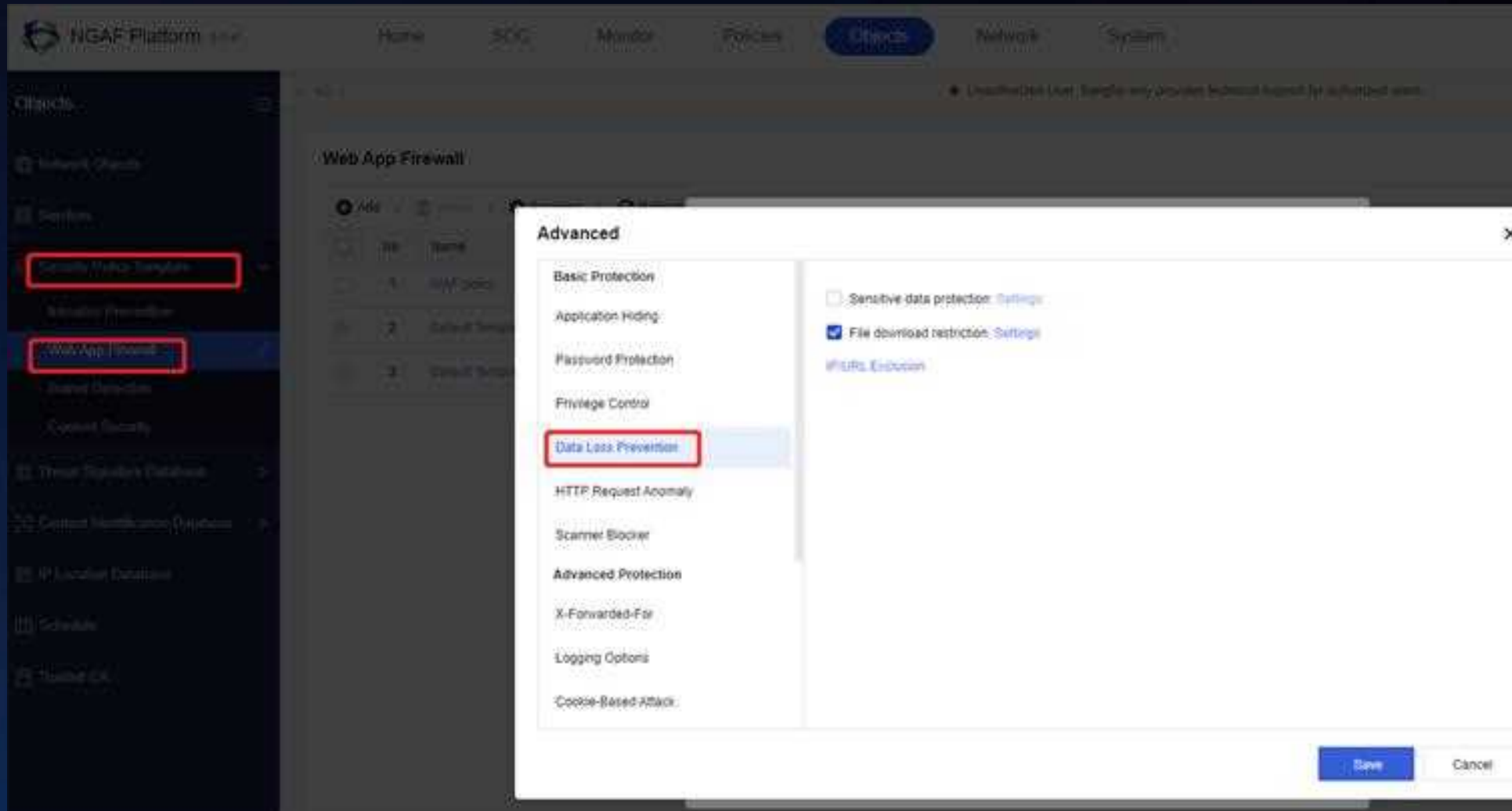
In Network Secure Platform, it deletes the Server Access Authentication module.



Server Access Authentication



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





THANK YOU

