



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.



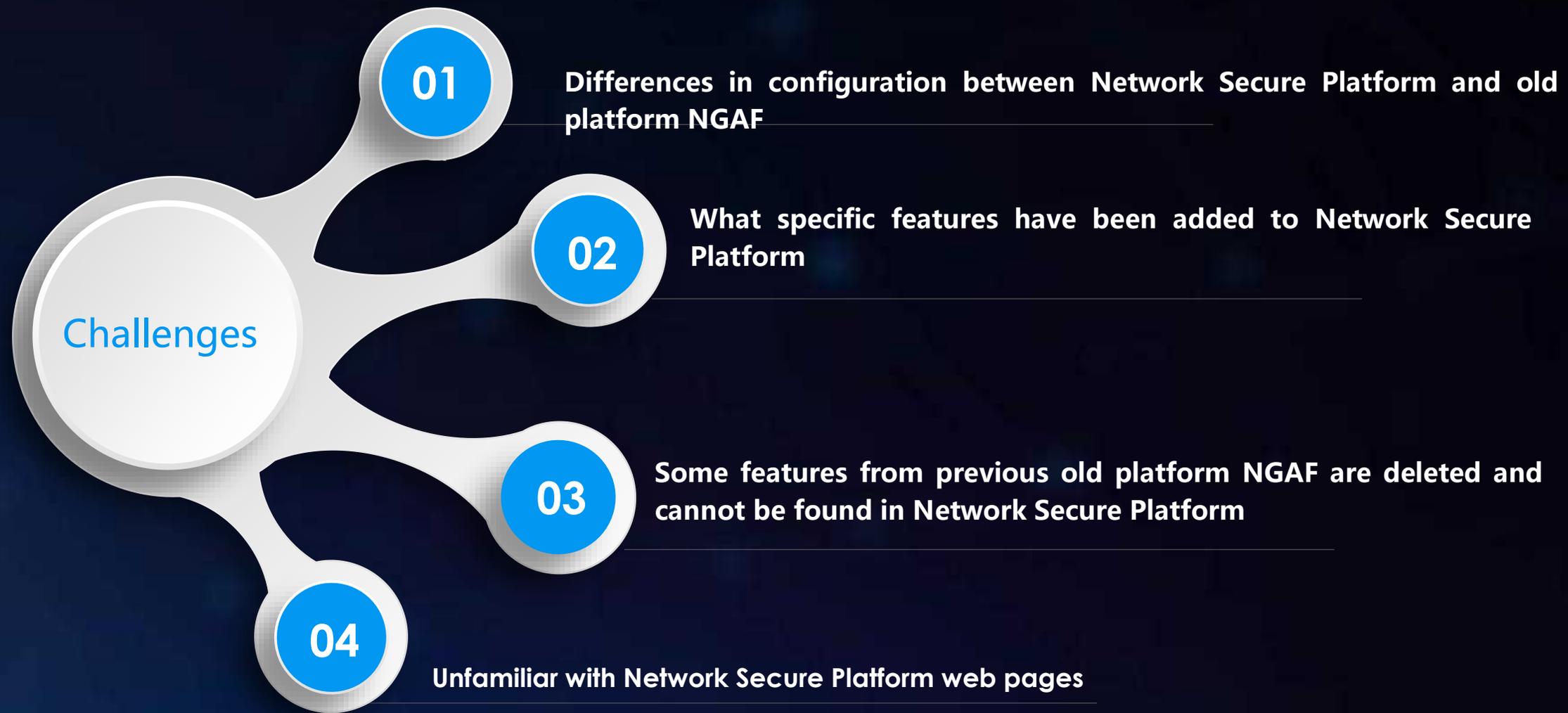
Providing a unified and shared underlying platform

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

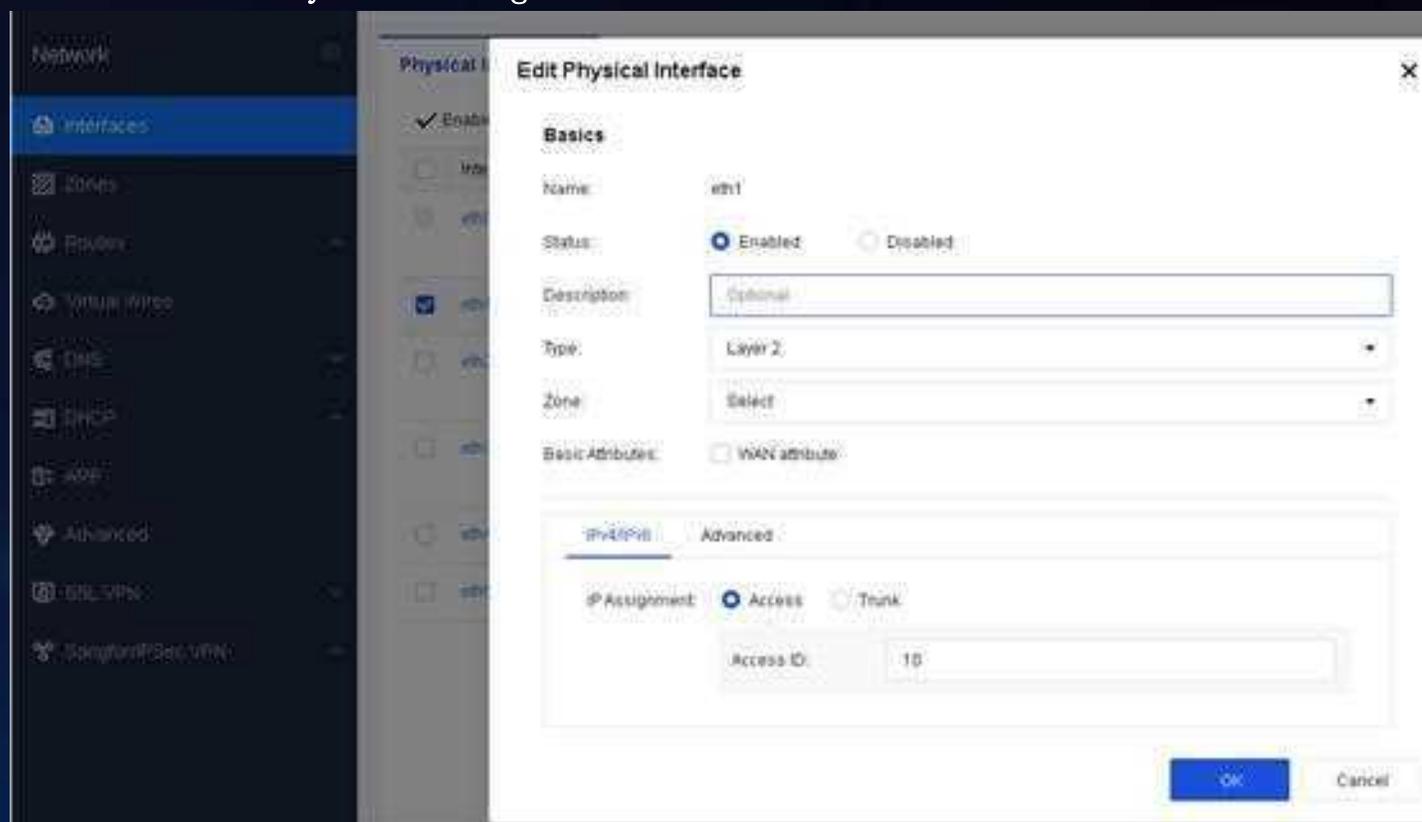


Old platform NGAF processing method:

- ◆ 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

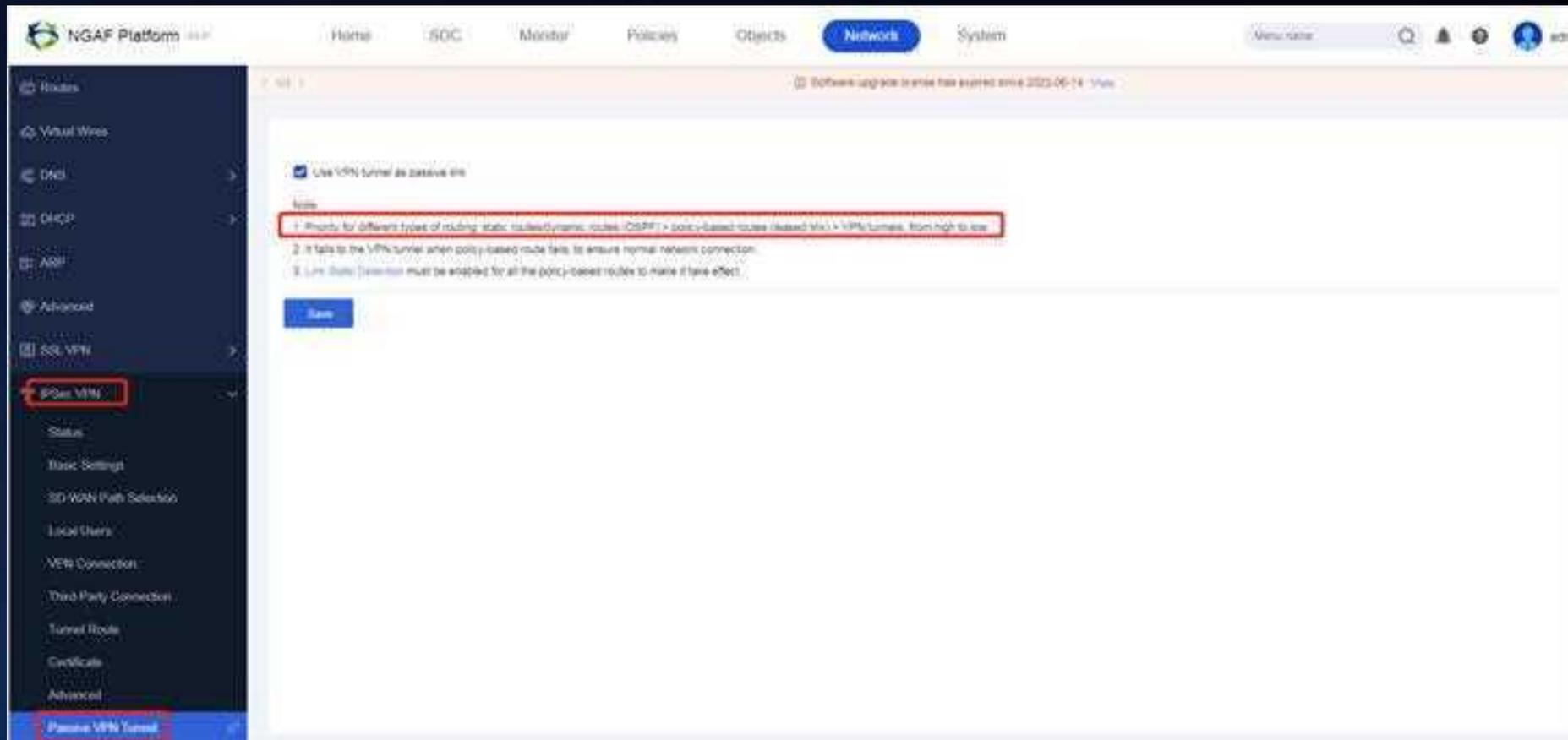


Situation 1: Default route types priority

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.

The image displays two screenshots of the Sangfor Network Secure Platform interface, illustrating the configuration of route priority settings.

Left Screenshot (Default Priority):

- The **System** menu is highlighted in red.
- The **Network** menu is highlighted in blue.
- The **Route Priority** dropdown menu is set to **Default**, highlighted in red.
- The **Route Priority Settings** dialog box is open, showing the **Default** mode selected.
- The **Route Priority** list is as follows:

Priority	Route Type
1	Direct Route
2	Policy-Based Route
3	SSL VPN Tunnel
4	IPSec VPN Tunnel
5	Destination Route (Static Route, Dynamic Route)
6	Default Route

Right Screenshot (Custom Priority):

- The **System** menu is highlighted in red.
- The **Network** menu is highlighted in blue.
- The **Route Priority** dropdown menu is set to **Custom**, highlighted in red.
- The **Route Priority Settings** dialog box is open, showing the **Custom** mode selected.
- The **Route Priority** list is as follows:

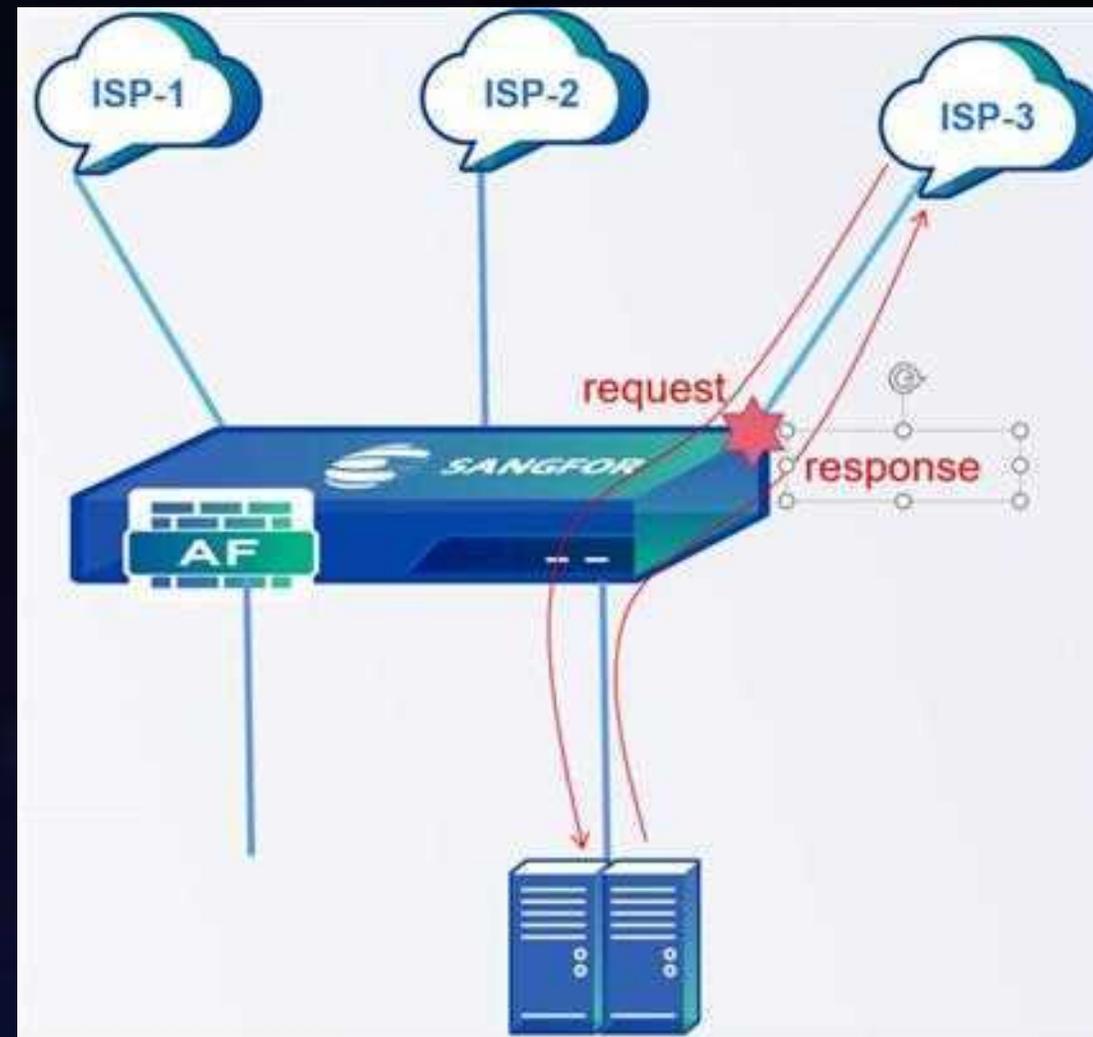
Priority	Route Type
1	Direct Route
2	Policy-Based Route 1
3	Policy-Based Route 2
4	SSL VPN Tunnel
5	IPSec VPN Tunnel
6	Destination Route (Static Route, Dynamic Route)
7	Default Route

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.

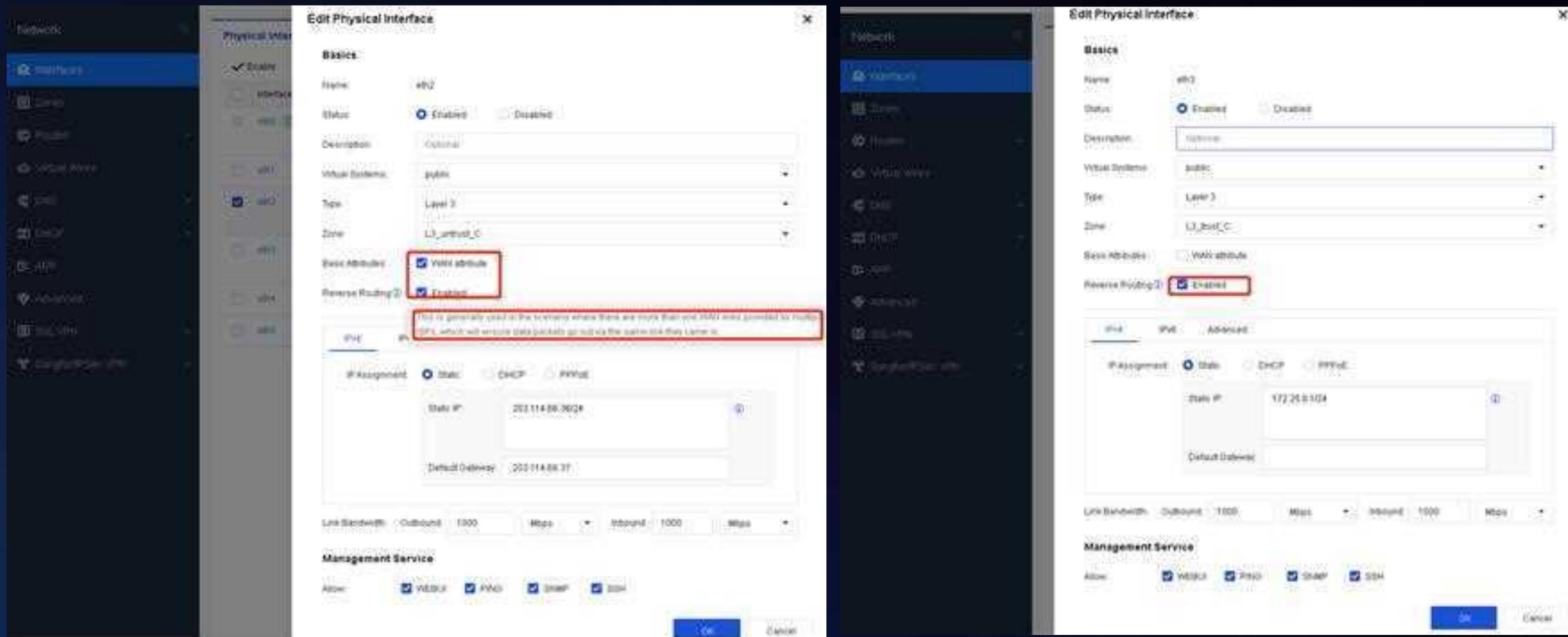
The screenshot displays the Sangfor NGAF management interface. The main view is the 'Policy-Based Routes' configuration page. A table lists several routes, with the first row highlighted. A red box highlights the 'Interface-Next Hop IP' field, which is set to 'eth2/2.2.2.2'. A red arrow points to this field. Below the table, the 'Basics' configuration for the selected route is shown. The 'Name' is 'eth2', 'Status' is 'Enabled', and 'Basic Attributes' includes 'Only Interface' (checked). The 'IP Assignment' section shows 'Static IP' as '2.2.2.2' and 'Next Hop IP' as '2.2.2.2'. A red box highlights the 'Only Interface' checkbox.

No.	Name	Protocol	Src Zone	Src Address	Dest Address/Region	Services	Applications	Interface-Next Hop IP	Load Balancing Method	Schedule	Link State	Status
1	eth2	any						eth2/2.2.2.2		All week	Not detected	✓
2	eth2	any						eth2/44.44.44.44.2		All week	Not detected	✓
3	eth2	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 shows the 'Static Routes' configuration page. The left sidebar has 'Static Routes' highlighted. The main content area shows a table with the following data:

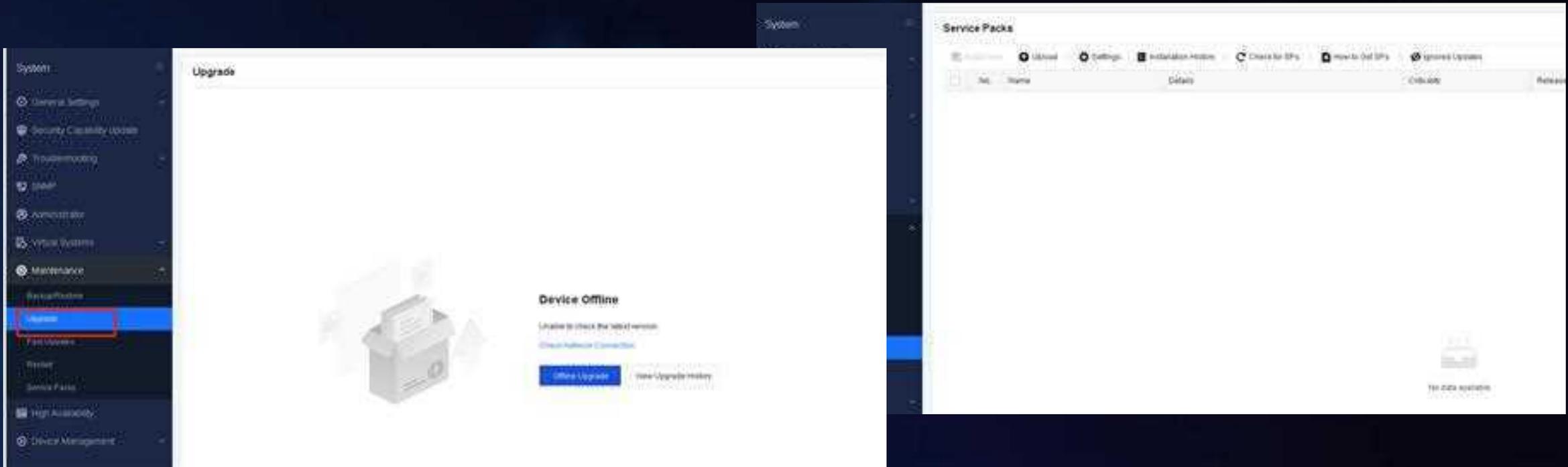
No.	Dest IP/Netmask	Next-hop IP	Administrative Distance	Interface	Metric	Reliability Detection	Validity	Status	Description	Operation
1	99.99.99.0/30	3.3.3.2	1	Auto	10	-	Valid	✓	-	Edit Delete
2	99.99.99.0/30	4.4.4.2	1	Auto	10	-	Valid	✓	-	Edit Delete

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.



Upgrade---Network Secure Platform

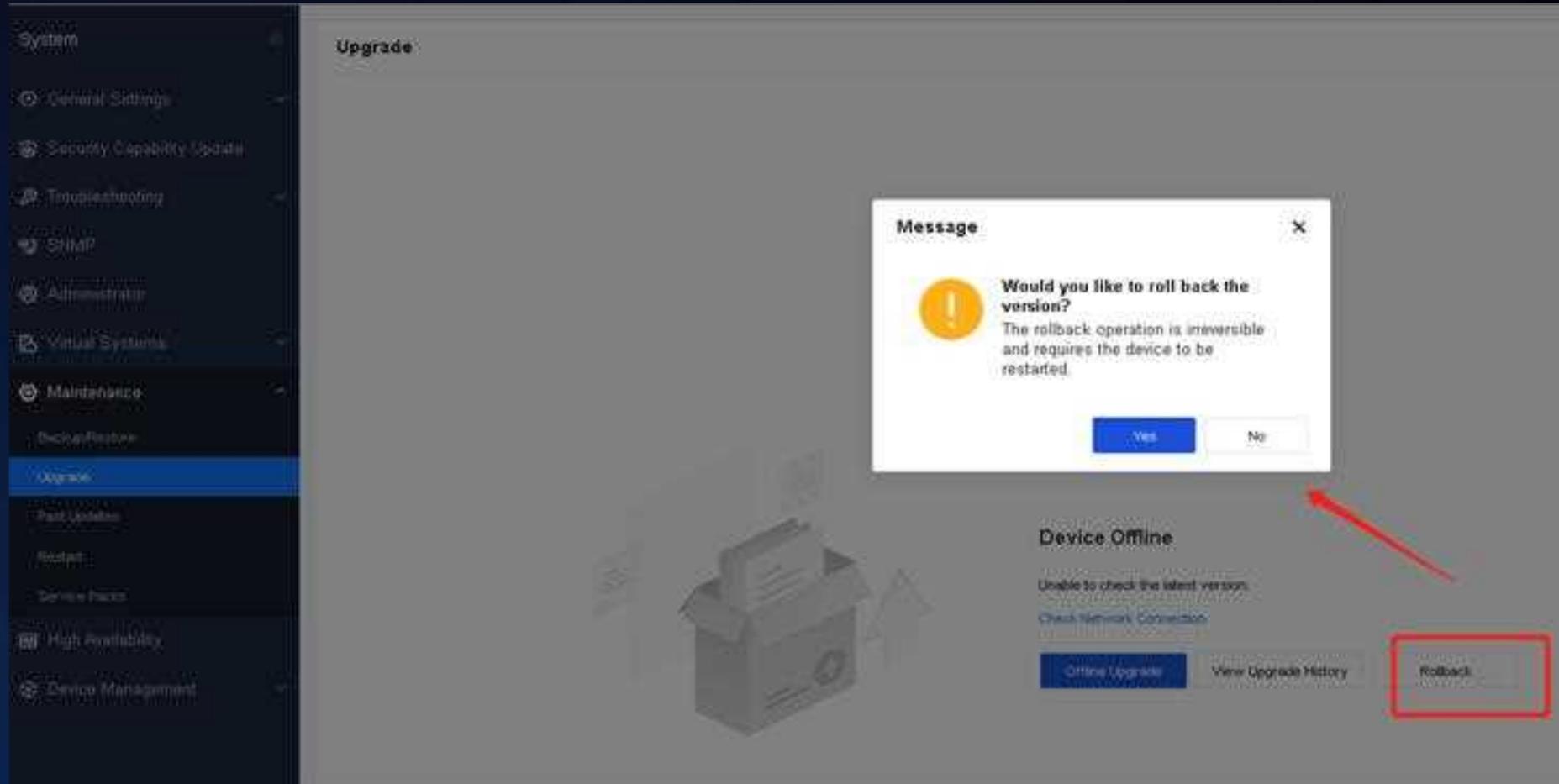


- It is unnecessary to stop and separate the high availability configuration in active/standby mode when you plan to upgrade the system version, compared to the old platform NGAF. You are instructed to upgrade the standby device firstly, and then perform the switchover, and then upgrade the new standby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

The screenshot displays the NGAF Platform web console interface. The top navigation bar includes 'Home', 'SOC', 'Monitor', 'Policies', 'Objects', 'Network', and 'System'. A left sidebar menu is visible with categories like 'System', 'General Settings', 'Security Capability Update', 'Troubleshooting', 'Tools', 'Logs', 'SNMP', 'Administrator', 'Maintenance', 'High Availability', and 'Device Management Platform'. The 'Tools' menu item is selected. The main content area shows three tabs: 'Web Console', 'Packet Capture', and 'Technical Support'. The 'Web Console' tab is active, displaying a list of supported commands and their descriptions:

Command	Description
sh[clear][ctrl+H]	Clear
term[ctrl+q]	End current program
vlan	View the interfaces on a VLAN and flag is not supported
mode_switch	View the current mode
arp	Display ARP table cache entries. Command can be appended with flag -n
mi-tool	Show connection status of each network interface
ifconfig	View information of network interfaces and flag is not supported
switch_mac	View forwarding table and flag is not supported
ping	Check connectivity to a host. Command can be appended with flag -i
telnet	Check connectivity to a port over Telnet protocol <host> <port>
ethtool	Display Ethernet card settings and flag is not supported
ping6	Check connectivity to a host by IPv6. Command can be appended with flag -i
route	Show IP routing table and flag is not supported
tracert	Trace how packets are forwarded using traceroute <host>
tcpdump	The command cannot be run with the -w, -W, -F, -E, -n or -M flag, but can be run with the flag -l, -nn or -c by default. -c flag supports up to 10000 packets

At the bottom of the console area, there is a prompt: 'Type and Execute commands here. Type 'help' for help.'

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 web console interface for the Network Secure Platform. On the left, a sidebar menu includes sections like System, General Settings, Security Capability Update, Troubleshooting, Tools, Packet Replay, Logs, SNMP, Administrator, and Virtual Systems. The 'Web Console' option is highlighted in blue. The main area is split into two panels. The left panel shows a list of commands such as 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 right panel shows the configuration options for the 'config' command, including 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. A red box highlights the 'config' command list and the 'config' command in the terminal view.

Web Console---Network Secure Platform



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

The screenshot displays the Web Console interface. On the left is a navigation menu with options like System, General Settings, Security Capability Update, Troubleshooting, Tools, Packet Replay, Logs, Web Console (highlighted), SNMP, and Administrator. The main area is split into two panes. The left pane shows a terminal window with the following CLI commands:

```
telnet
traceroute
undebug
upgrade
admin!
admin! config
admin(config)# ?
access-list
app-signature
application
application-type
arp
arp-defend
arp-proxy
asset-access
asset-discover
assetlist
auth-orig
auth-policy
auth-redirect
auth-status
auth-user
auth-zone
banner
blacklist
blacklist-aging
```

The right pane shows a terminal window with the following text:

```
Test port connectivity
Trace route packets to a host
Disable debugging mode
Upgrade
ACL configuration
Add or modify custom application signature
```

In the top right corner of the terminal area, there are links for 'API Documentation' and 'CLI Documentation' (highlighted with a red box).

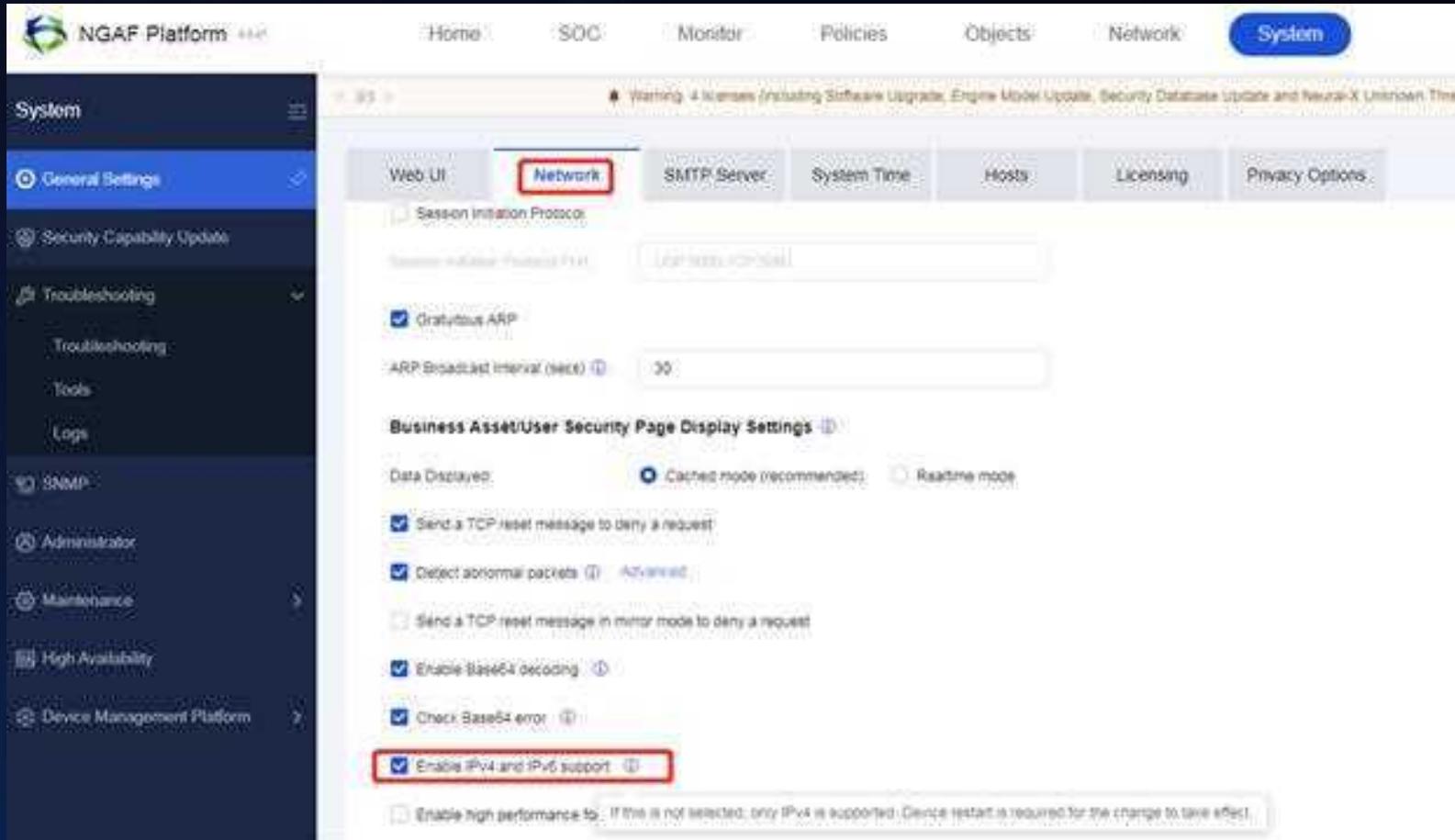
The right pane also shows a 'CLI Documentation' page for the 'blacklist' command. The page includes a search bar, a navigation tree, and a table of contents. The main content area is divided into sections: 1. Command Name, 2. Syntax, 3. Description, and 4. Parameters. The Parameters section contains a table with the following data:

Name	Value	Format	Description
host-address	length(1-255)	AACD	Specify the destination host to be blocked.
		AACD/W	If address format: AACD/W
		AACD+IPD	If ipge format: AACD+IPD
		AACD/S	Address format: AACD/S
		AACD/WM	Address format: AACD/WM
		AACD/S+M	Address format: AACD/S+M

IPv6 Feature---Old Platform NGAF



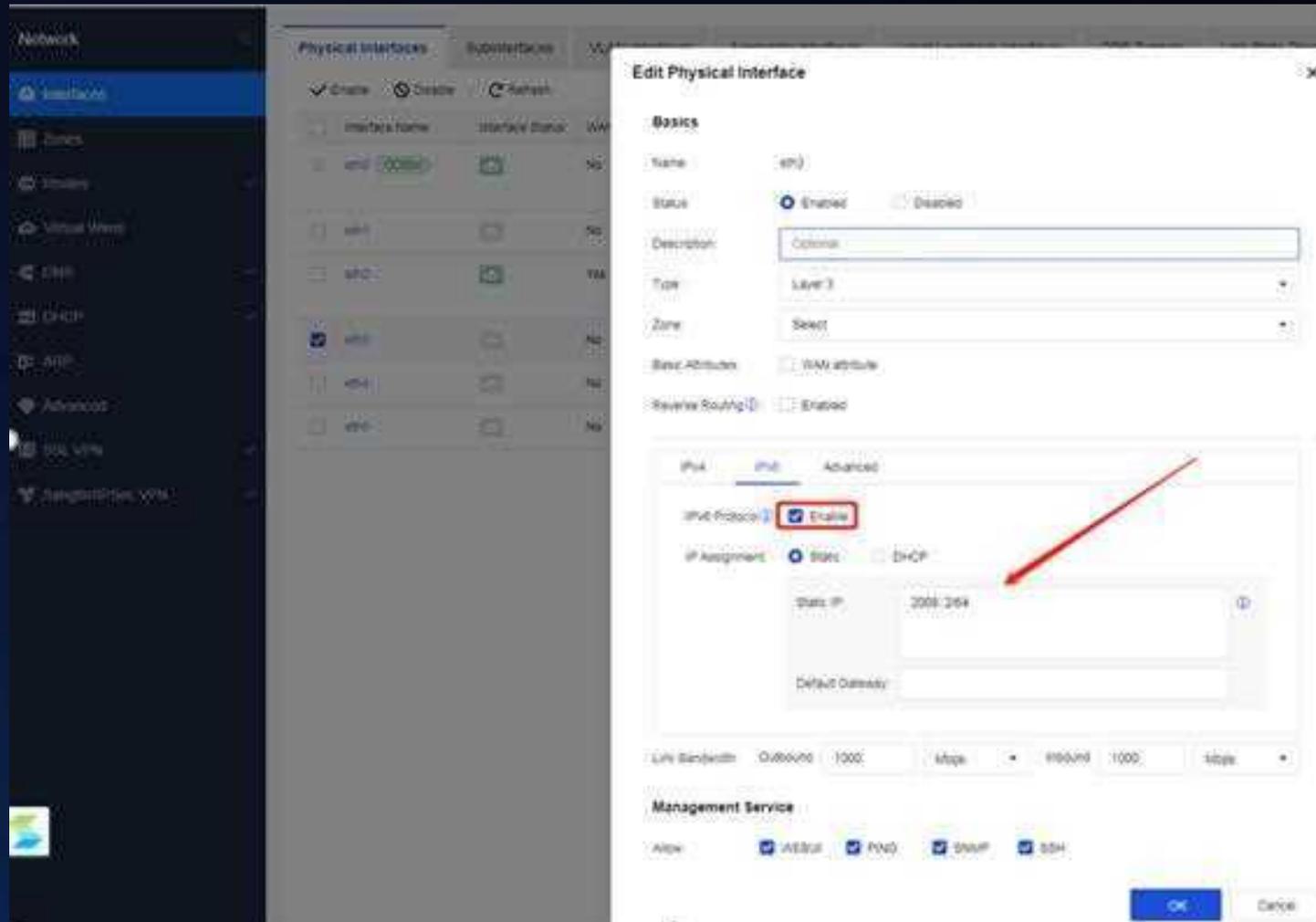
To support IPv6 on old platform NGAF, firstly it is necessary to enable the “Enable IPv4 and IPv6 support” feature in the network parameters which will cause to restart the device, and then configure IPv6 content in corresponding interfaces.



IPv6 Feature---Network Secure Platform



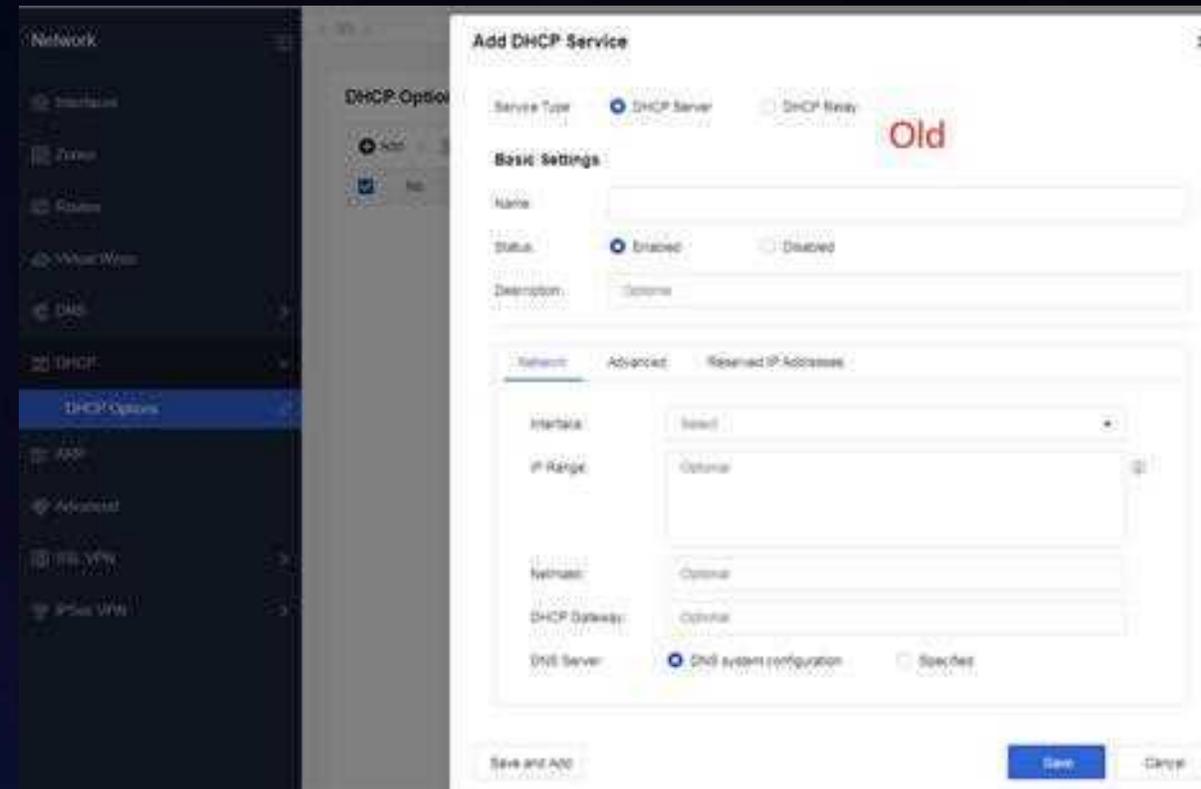
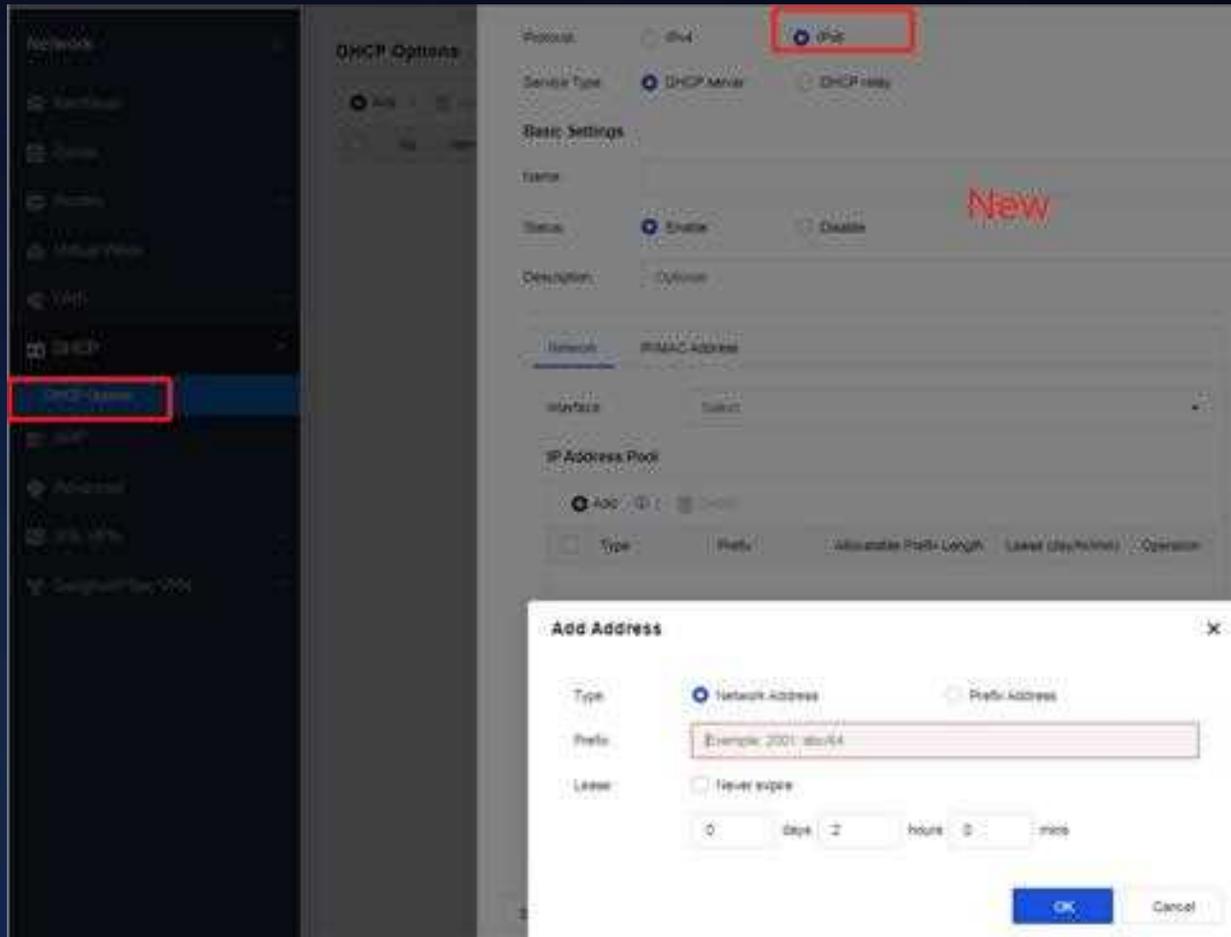
The Network Secure Platform supports IPv6 feature without other extra settings. This feature can be directly configured in the interface **without restarting the device**.



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

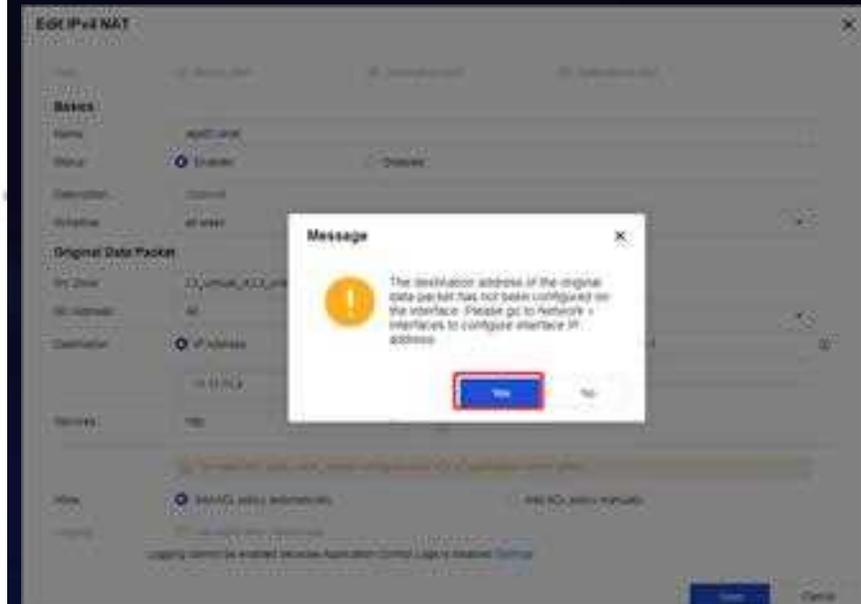
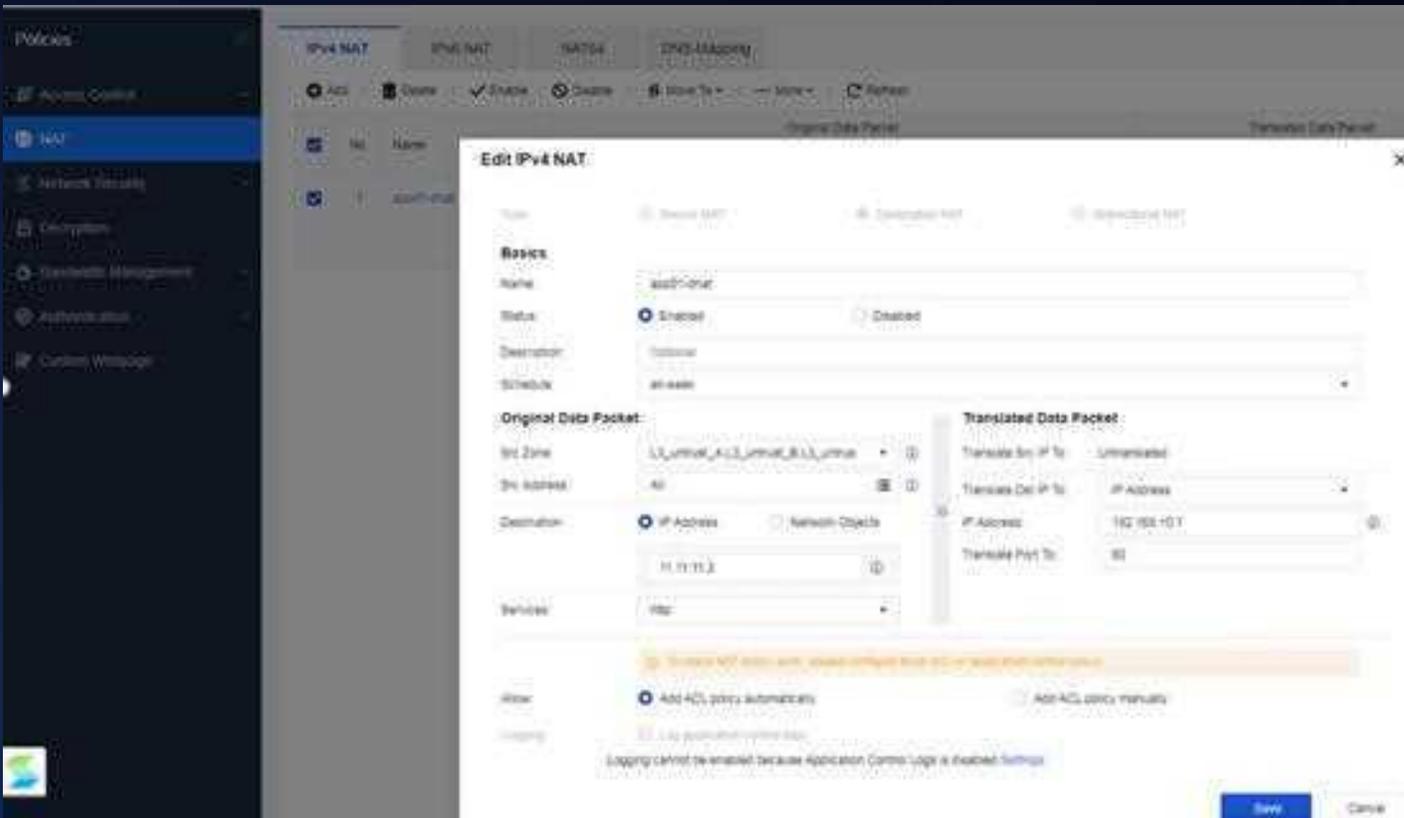
DNAT---Network Secure Platform



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.

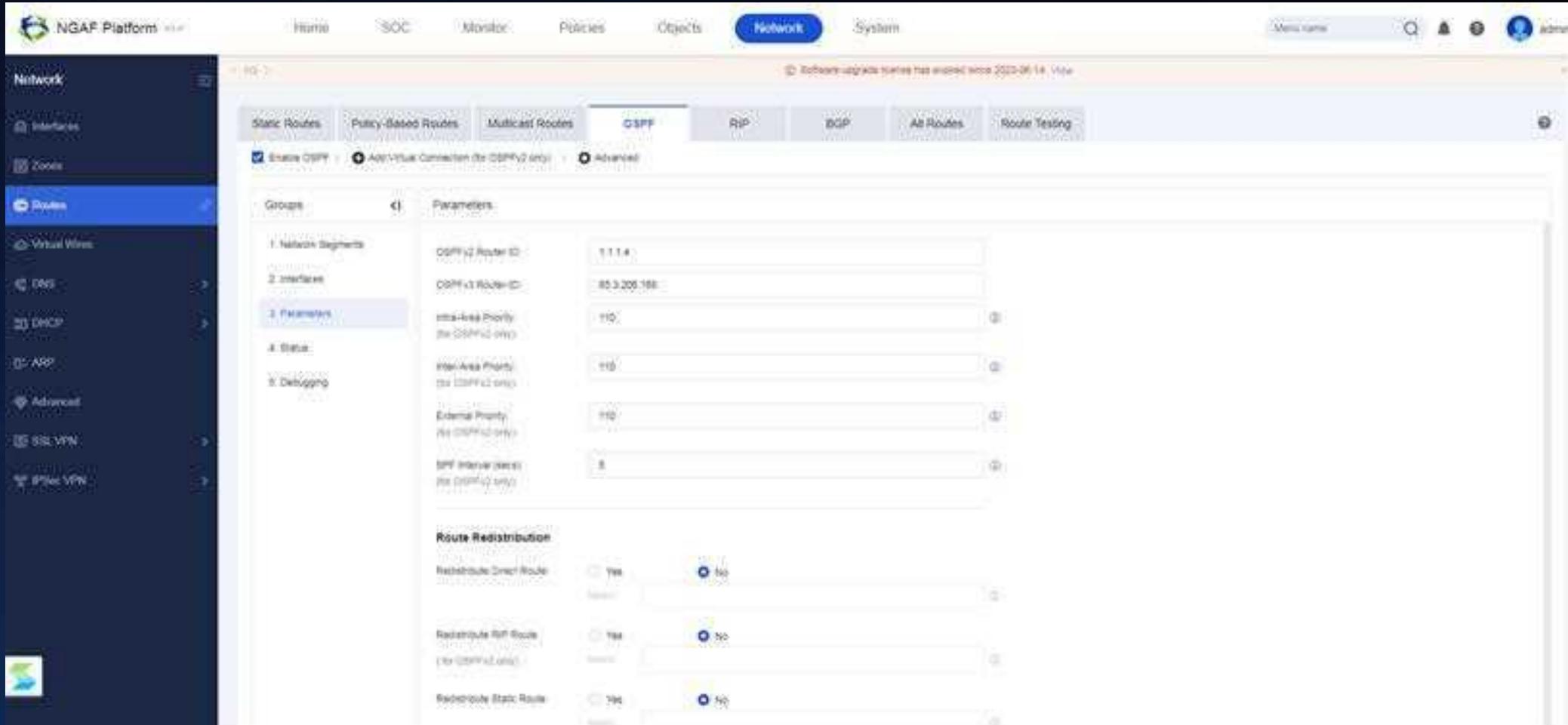
However, you probably will encounter the notifying message below before you save it, just click 'Yes' and ignore it.



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.

Type	Router ID	Intra-Area Priority	Inter-Area Priority	External Priority	Operation
OSPFv2	1.1.1.1	110	110	110	Edit Basics Edit Advanced Delete
OSPFv3	2.2.2.2	110	110	110	Edit Basics 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 lists various network functions, with 'OSPF' selected. The main area shows the OSPF configuration page, including a table of OSPF instances and an 'Edit Basics' dialog box. The dialog box contains the following fields:

Field	Value
Router ID	5.5.5.5
OSPF Calculation Delay	1
OSPF Calculation Interval	3000
Internal Priority	100
External Priority	10
Default Metric of Nondefault Priority	20

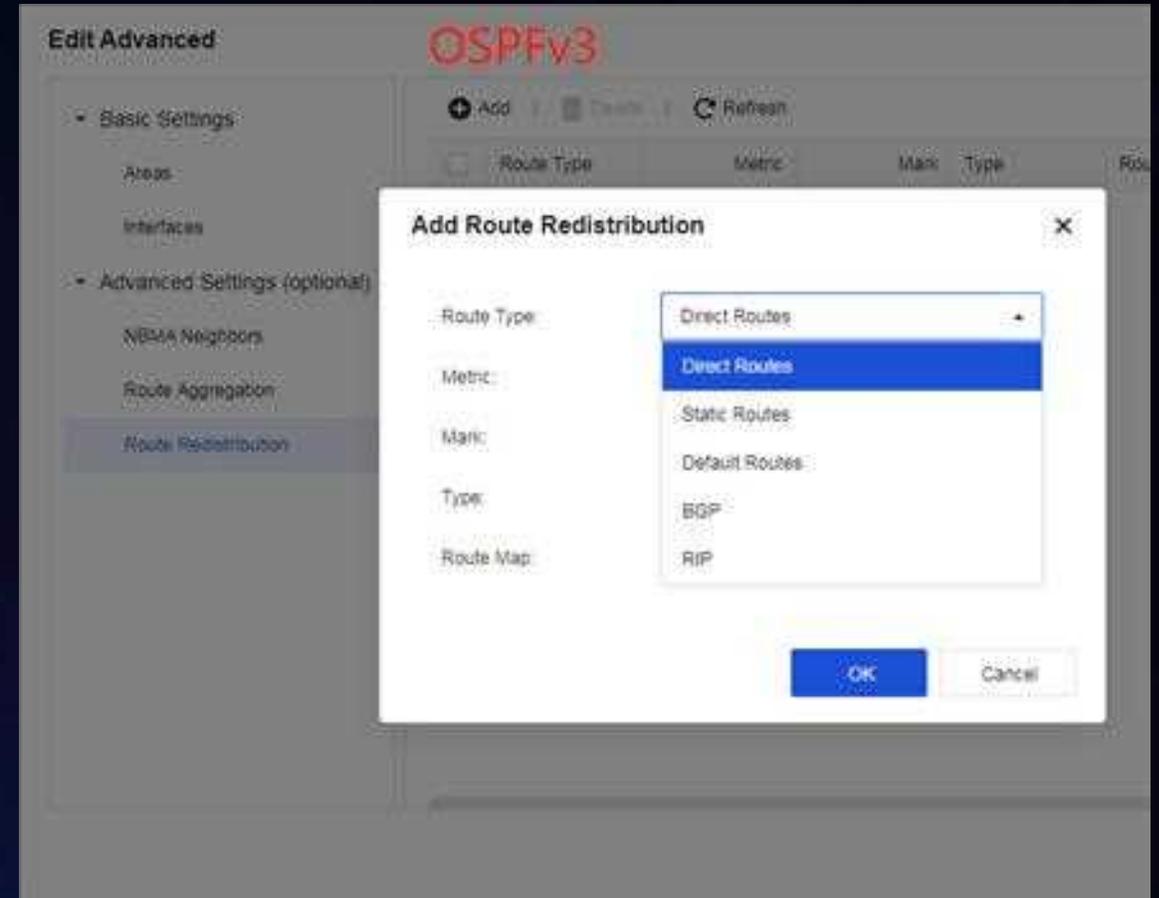
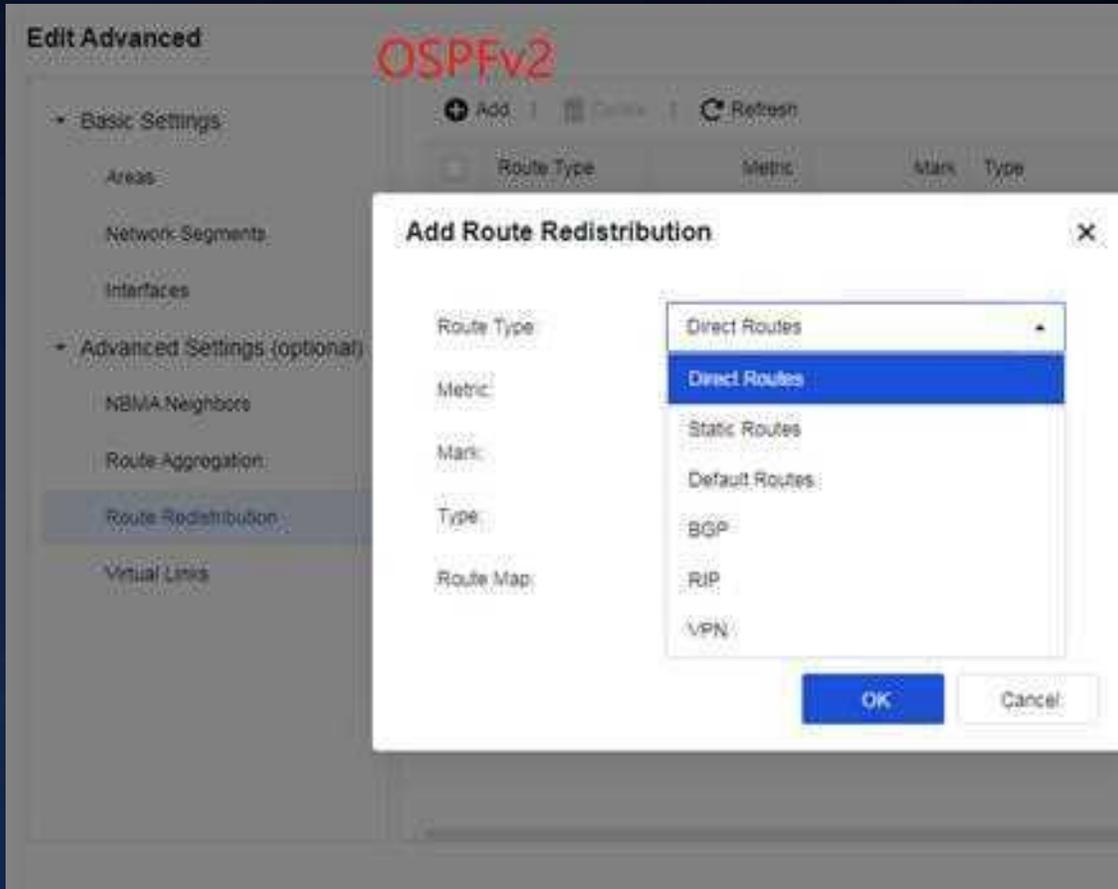
The 'BFD' checkbox is checked and highlighted with a red box. Below the dialog box, there is a 'Web Console' button. To the right of the main interface, a vertical menu lists system management options, with 'Web Console' highlighted in blue. Further to the right, a terminal window shows the following commands and output:

```
AFS.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



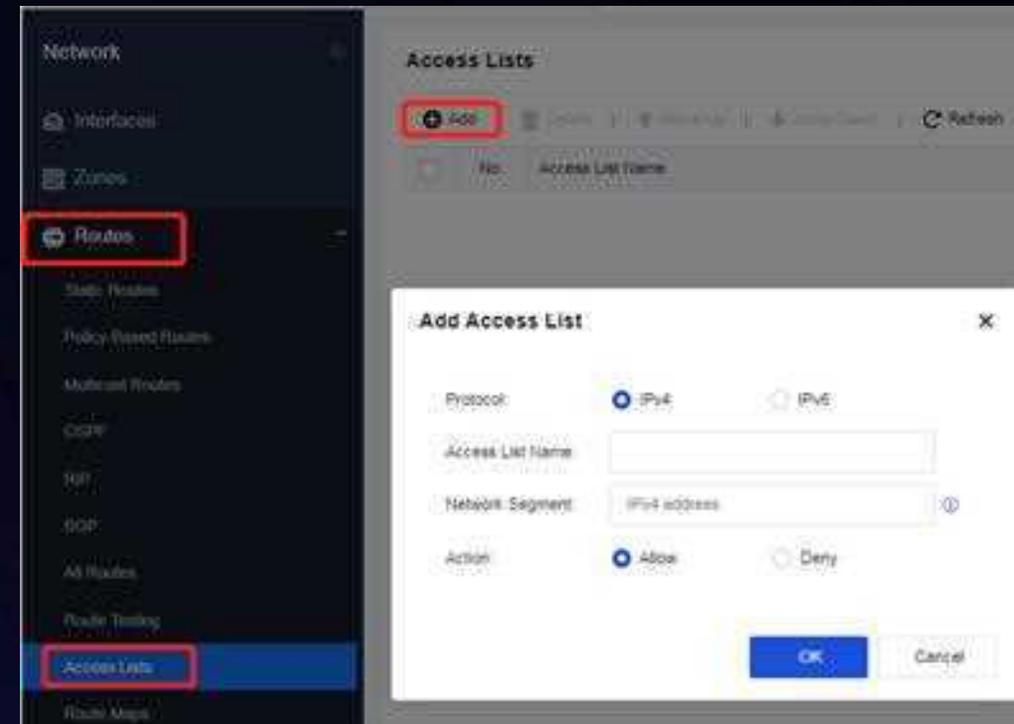
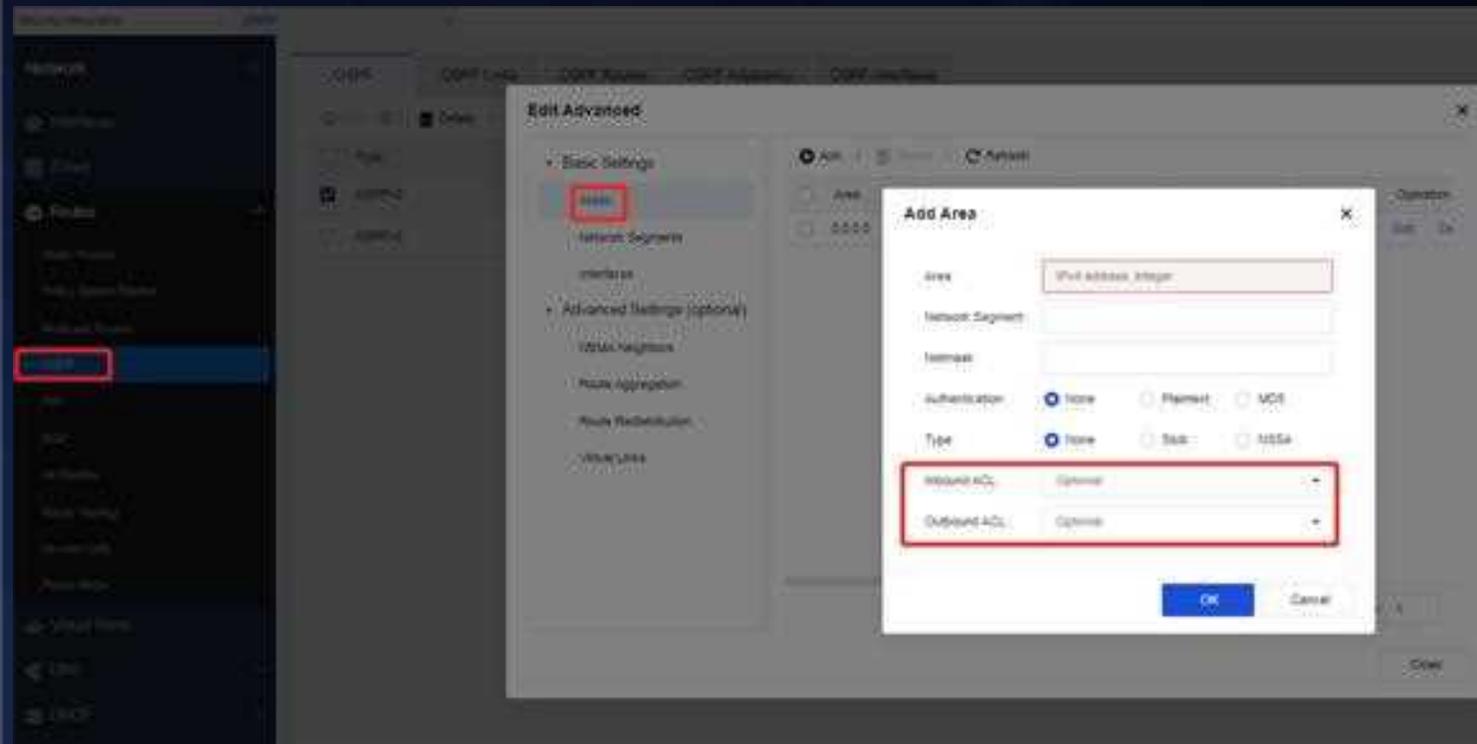
- OSPFv2 route redistribution supports direct routes, static routes, default routes, BGP routes, RIP routes and VPN routes.
- OSPFv3 route redistribution supports direct routes, static routes, default routes, BGP routes and RIP routes.



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 image consists of four overlapping screenshots from the Sangfor Network Secure Platform interface, illustrating the configuration process for OSPF route redistribution with a route map. Red boxes highlight key UI elements:

- Top Left:** The 'Network' sidebar menu with 'Routes' and 'OSPF' highlighted.
- Top Middle:** The 'Edit Advanced' configuration page for OSPF, with the 'Route Redistribution' section expanded and 'Route Map' selected.
- Top Right:** The 'Route Maps' configuration page, with the 'Add' button highlighted.
- Bottom Right:** The 'Add Route Map' dialog box, showing fields for 'Route Map Tag', 'Priority', 'IPv4/IPv6 Access List', 'AS Path Prepend', 'Origin' (set to 'Not activated'), 'Local-Pref Value', and 'Action' (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 'Interfaces' configuration page in the Sangfor Network Secure Platform. The left sidebar shows a navigation menu with 'Interfaces' selected. The main area is divided into two panels: 'Physical Interfaces' and 'Basics'.

Physical Interfaces Panel:

Interface Name	Interface Status	WAN
eth0	Enabled	No
eth1	Disabled	No
eth2	Enabled	Yes
eth3	Enabled	No
eth4	Disabled	No
eth5	Disabled	No

Basics Panel:

Basics

Name: eth2

Status: Enabled Disabled

Description: Optional

Virtual Systems: public

Type: Layer 3

Zone: L3_untrust_A

Basic Attributes: WAN attribute

Reverse Routing: Enabled

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.

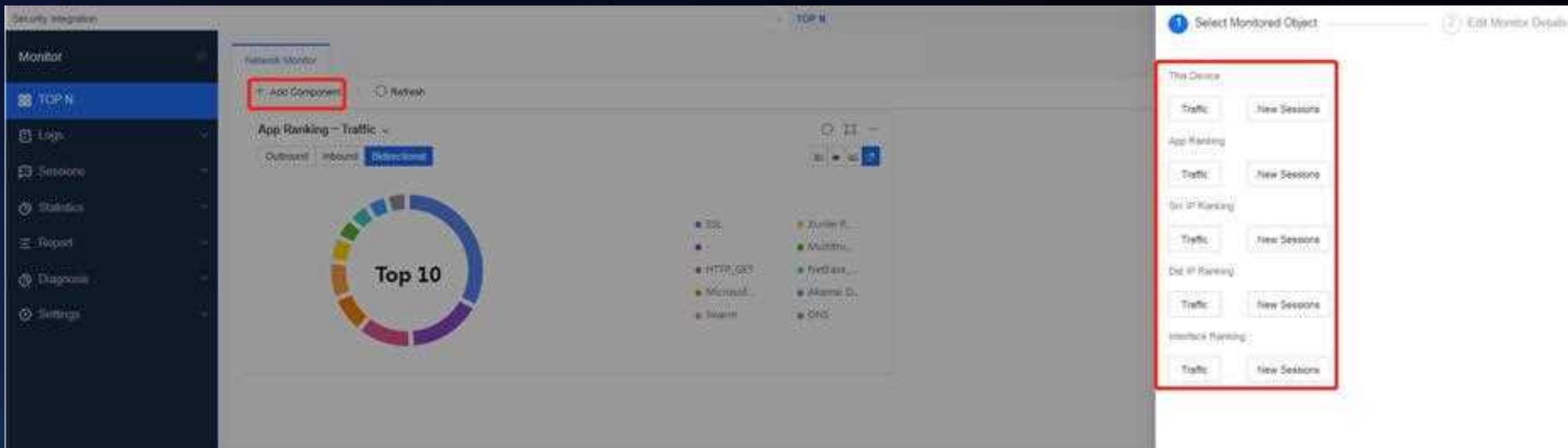
The screenshot displays the 'User Security' section of the Sangfor Network Secure Platform. It features a 'Summary' tab and a 'Refresh' button. A donut chart shows 'User Security by Severity' with 2 users. A legend indicates the severity levels: Compromised (0), High (2), Medium (0), and Low (0). Below the chart is a table of users with the following columns: No., User, Event Status, Severity, Attack Type, Attack Stage, Detections, Integration, Scan Status, Pending Malice, and Operation. Two users are listed, both with 'Pending' event status and 'Compromised (High)' severity. The first user is 'DESKTOP-REUQFPA' and the second is '41.10.100.41'. The 'Operation' column for the second user shows 'Quick Scan' and 'Full Scan' options.

No.	User	Event Status	Severity	Attack Type	Attack Stage	Detections	Integration	Scan Status	Pending Malice	Operation
1	DESKTOP-REUQFPA (1...	Pending	Compromised (High)	Remote (IP Domain C&C)	C&C Command	18	18	Scanned	0 / 0	Quick Scan
2	41.10.100.41	Pending	Compromised (High)	Remote (IP Domain C&C)	C&C Command	1	1	Unavailable	0 / 0	Quick Scan Full Scan

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.

The screenshot displays the 'Intrusion Prevention' configuration interface. On the left, a sidebar menu has 'Intrusion Prevention' selected. The main area shows a table of templates and a modal dialog for adding a new one.

No.	Name
1	Default Template_Internet Access
2	Default Template_Server Scan

Add Intrusion Prevention Template

Template Name:

Description:

Protection Features

- Server Protection: Selected System: Shellcode, Scan, Custom IPS Rules, Database, Mal, W...
- Endpoint Protection: Selected System: Shellcode, Scan, Custom IPS Rules, Web Access, Web...
- Brute-Force Attack Protection: Selected FTP, TELNET, Ubuntu, IMAP, Standard, RLOGIN, TELNET, Microsoft, ...
- Anti-malware: Selected Backdoor, Spyware, Trojan, Worm...
- C&C Attack Detection Engine: Select C&C attack detection engine.
- Semantic Web Engine: Selected Enable Java deserialization prevention.

Buttons: Save and Add, Save, Cancel

Domain Name Object



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

The screenshot displays the Sangfor Network Secure Platform interface. On the left, a sidebar menu has 'Application Control' highlighted. The main area shows the 'Add Application Control Policy' dialog box. Within this dialog, the 'Source' section is set to 'Network Objects'. A 'Select Network Object' modal is open, showing a table of available network objects. The 'test' object, which is a 'Domain Name' with the address 'www.test.com', is selected and highlighted with a red box.

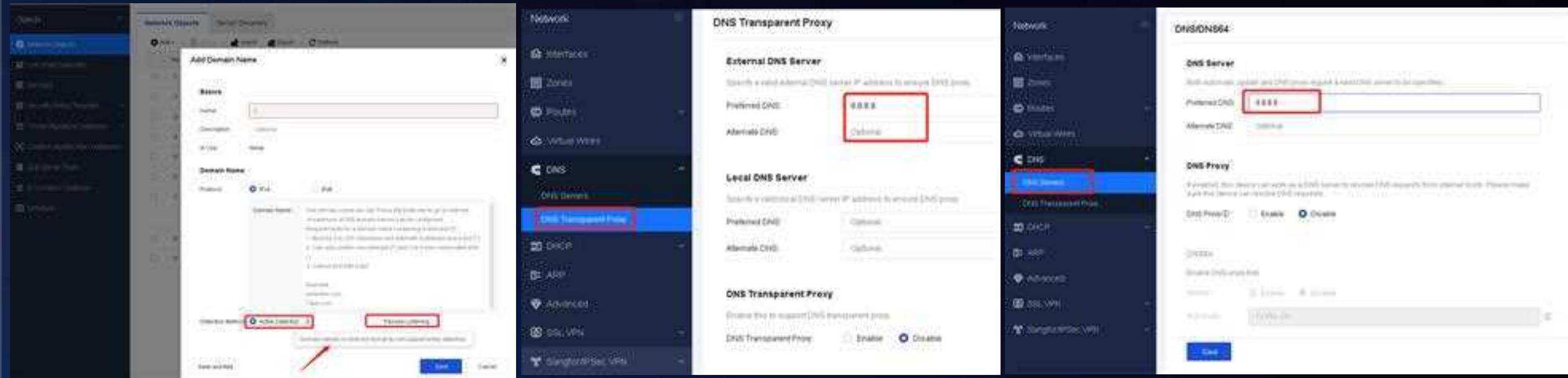
Name	Type	Address	Operate
All	IP Address	All	Edit
<input checked="" type="checkbox"/> test	Domain Name	www.test.com	Edit
1.1.1.1	IP Address	1.1.1.1	Edit
2.2.2.2	IP Address	2.2.2.2	Edit
3.3.3.3	IP Address	3.3.3.3	Edit
private-network	IP Address	10.0.0.0-10.255.255.255, 172.16.0.0-1	Edit
DHAP pool	IP Address	11.11.11.0-11.11.11.5	Edit
22.22.22.0	IP Address	22.22.22.0-22.22.22.255	Edit
44.44.44.0	IP Address	44.44.44.0-44.44.44.255	Edit

Domain Name Object



Domain name object contains active detection mode and passive listening.

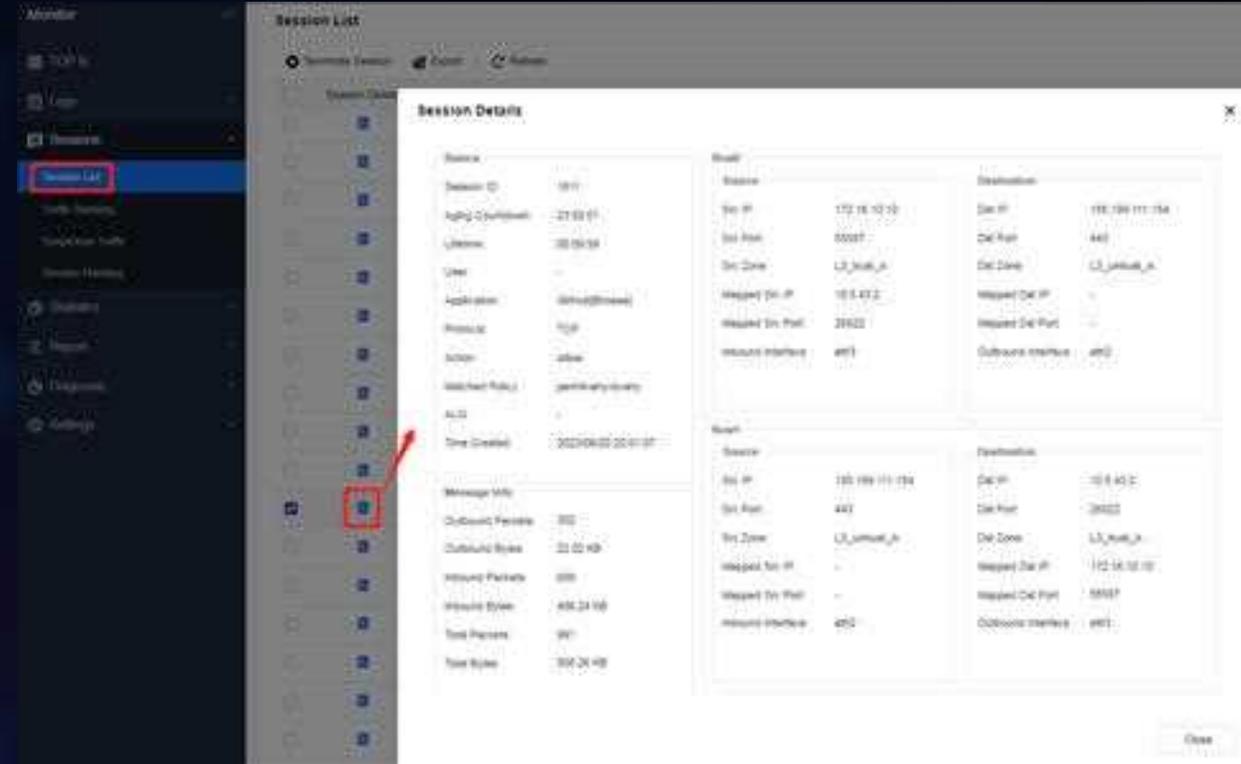
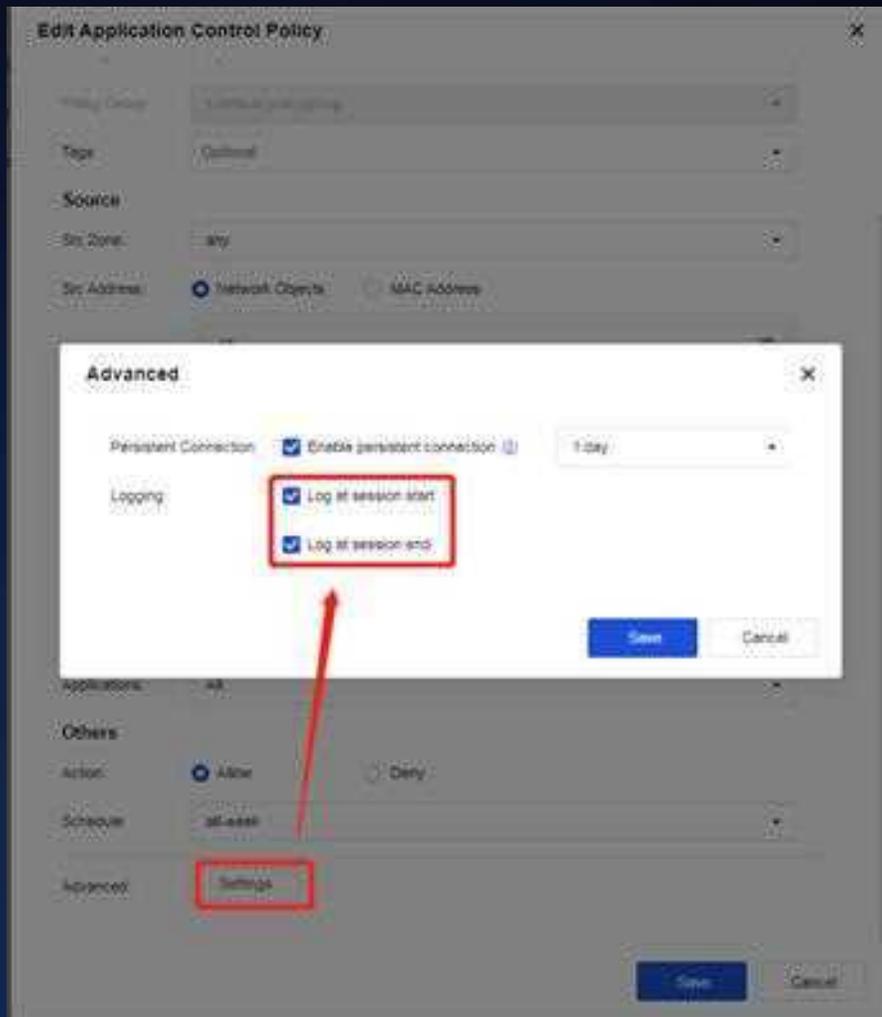
- In active detection mode, it is unnecessary that the DNS traffic has to go through NGAF, while NGAF has to connect the DNS server for resolving the domains. It will adjust DNS server in DNS Transparent Proxy configuration module firstly, then to DNS Server module, so you need to make sure both those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

The screenshot displays the 'Security Integration' interface with the 'Access Logs' menu item highlighted. The search filters are as follows:

- Start Time:** 2023-06-25 00:00
- End Time:** 2023-06-25 23:59
- Src Zone:** All
- Src IP/User:** All (selected), IP, User, Group
- Dst Zone:** All
- Dst IP:** All
- Service/Application:** All
- Action:** Allow (checked), Deny (checked), Integratedly Deny (checked)
- Session Logging:** At Start (checked), At Rejection, At End

Buttons: Search, Open in Quick Tab

INP Audit Logs



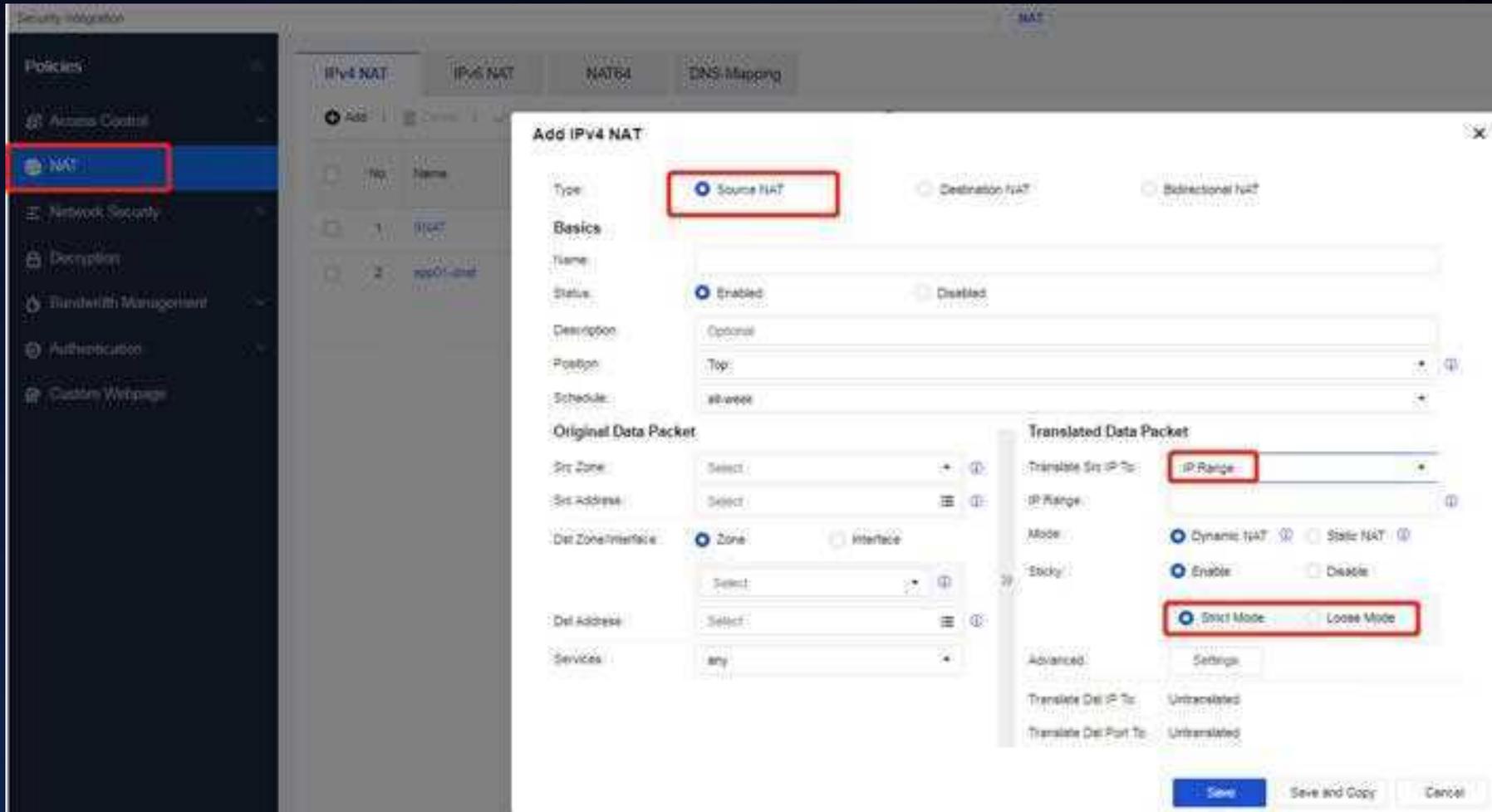
In Network Secure Platform, it can audit some INP protocols, and so far the supporting protocol types including opeda, s7, s7-plus, modbus, iec104, and profinetI0.

The screenshot displays the 'Security Integration' interface with the 'Access Logs' menu item highlighted in the left sidebar. The main content area shows the 'INP Audit Logs' configuration page, which includes the following fields:

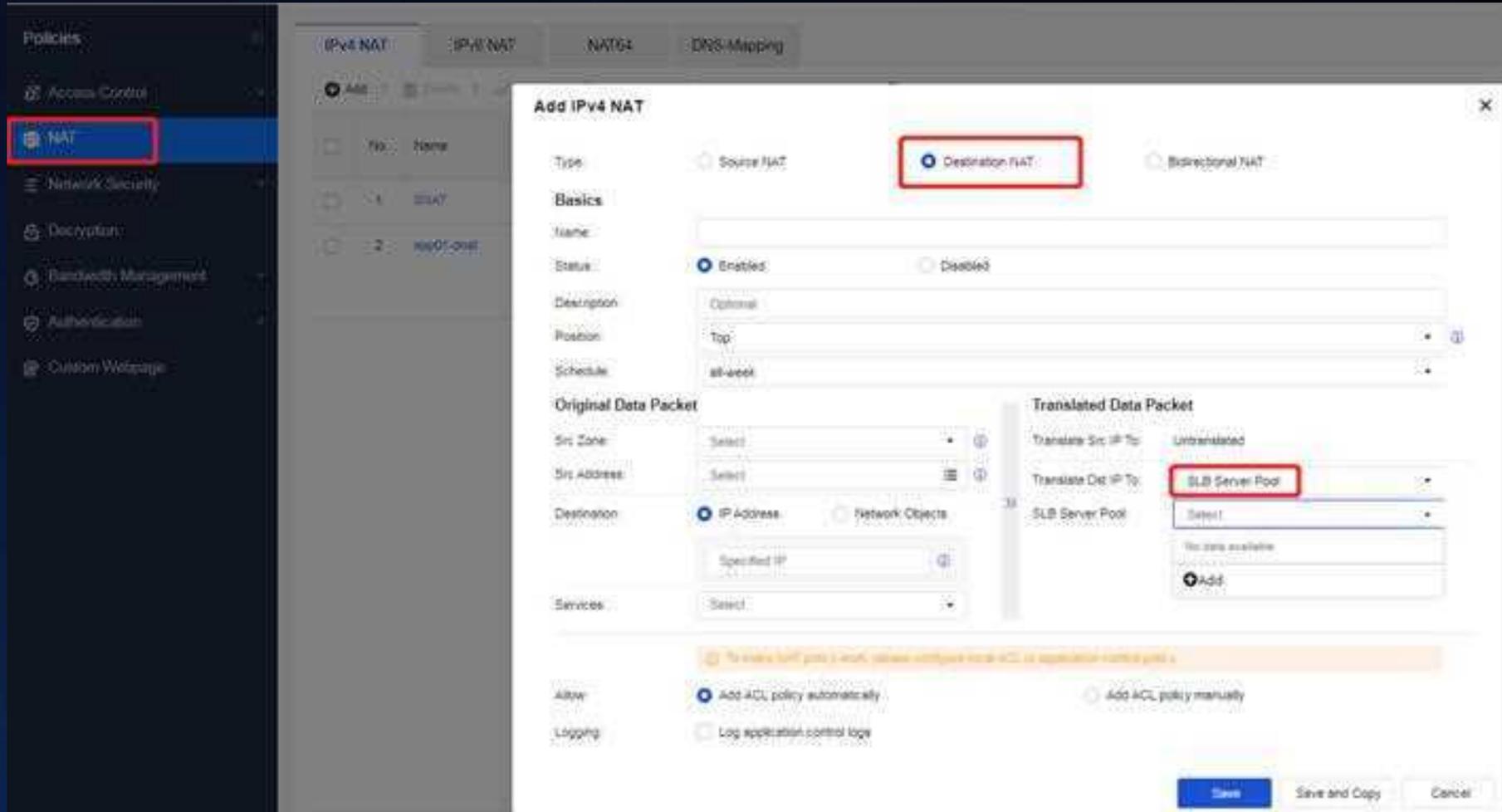
- Start Time:** 2023-06-25 00:00
- End Time:** 2023-06-25 23:59
- Src IP:** All
- Dst IP:** All
- Protocol:** A dropdown menu is open, showing a list of protocols with checkboxes: mms, ctp, scnet, smtp, sonet, tv, BACnet, ENIP-IO, ENIP, and goose.

A 'Search' button is located below the protocol list.

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.



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.

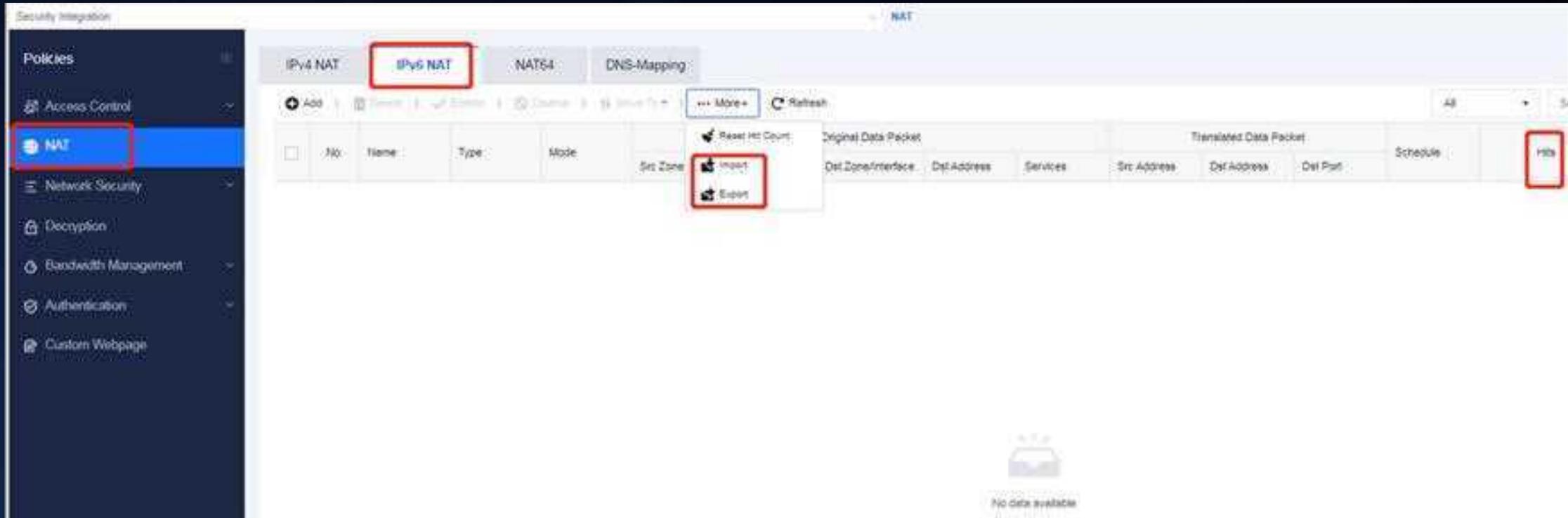


The screenshot displays the 'Add IPv4 NAT' configuration window in the Sangfor Network Secure Platform. The interface is divided into a left sidebar with navigation options like 'Policies', 'Access Control', and 'NAT', and a main configuration area. The 'NAT' option is highlighted in the sidebar. The main area shows a list of NAT policies and a detailed configuration form for a new 'IPv4 NAT' policy. The 'Type' is set to 'Destination NAT'. Under 'Basics', the status is 'Enabled'. The 'Original Data Packet' section has 'Destination' set to 'IP Address' with a 'Specified IP' field. The 'Translated Data Packet' section has 'Translate Dest IP To' set to 'SLB Server Pool', with a dropdown menu showing 'Select' and an 'Add' button. At the bottom, there are options for 'Allow' (Add ACL policy automatically) and 'Logging' (Log application control logs).

IPv6 NAT



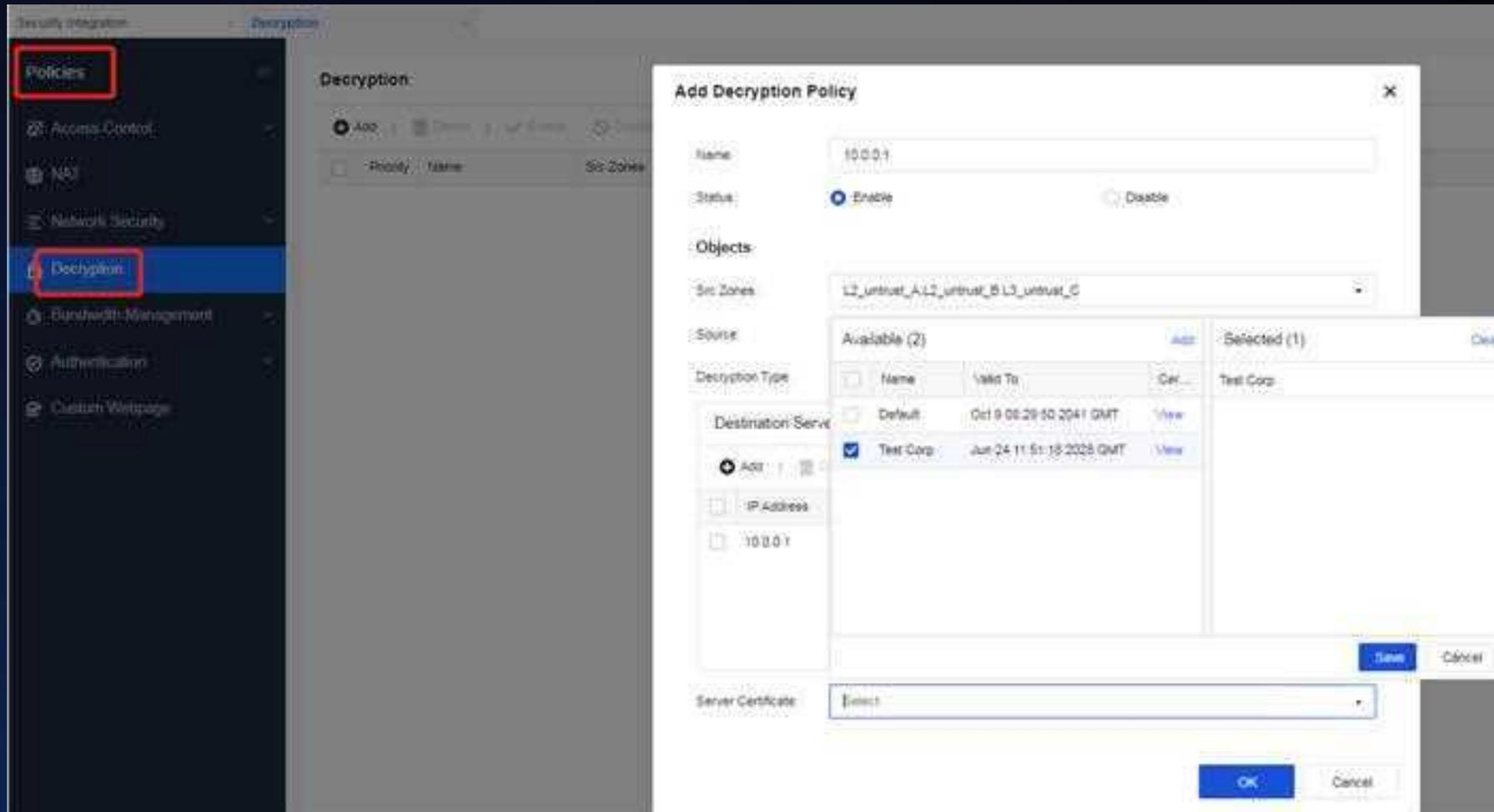
In Network Secure Platform, IPv6 NAT adds the feature of import and export operations, meanwhile every NAT item can display the hit counts.



Decryption



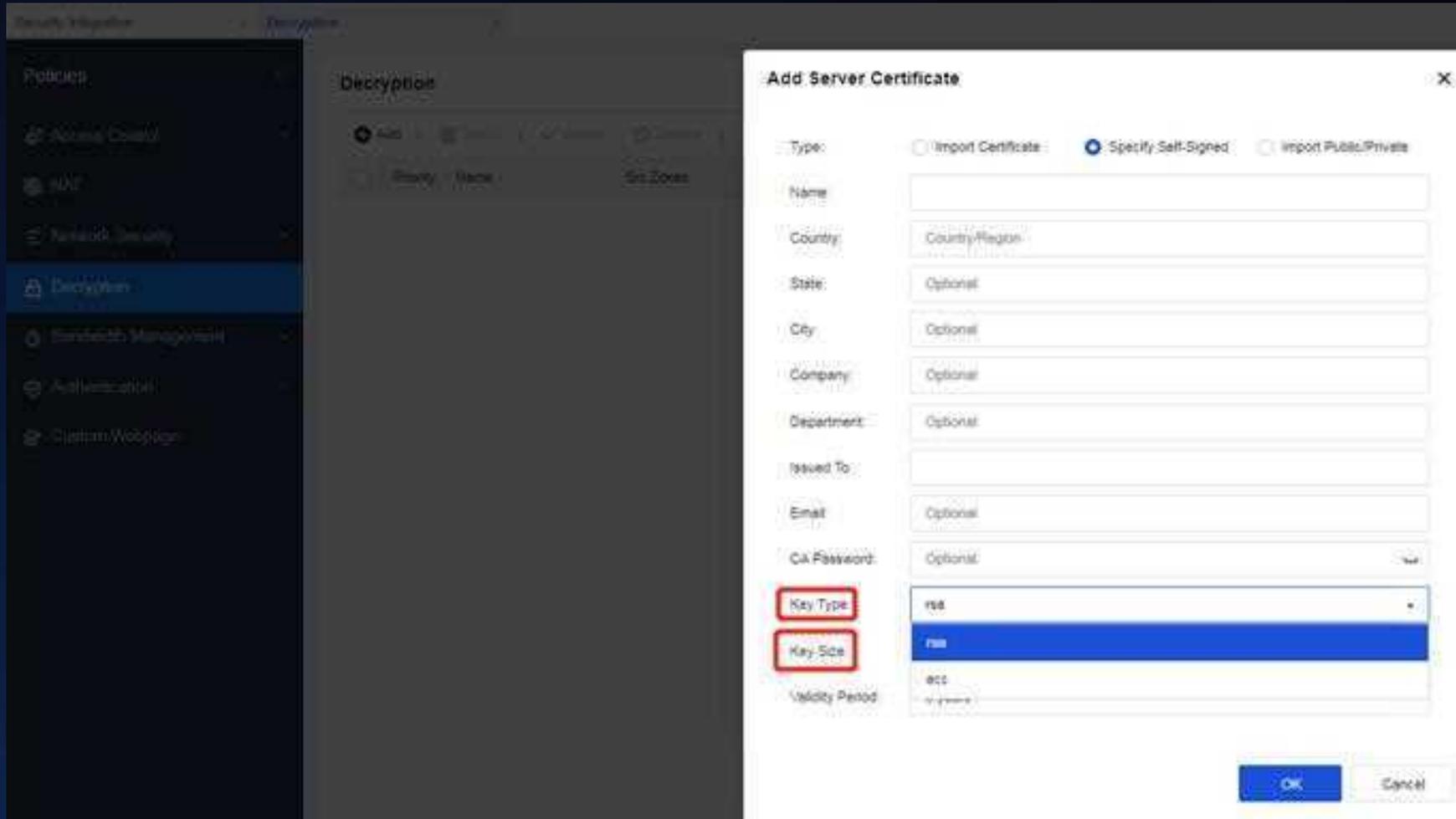
In Network Secure Platform, decryption policy supports TLS 1.3 and allows the selection of multiple server certificates within a single policy, supporting up to 8 certificates simultaneously.



Decryption



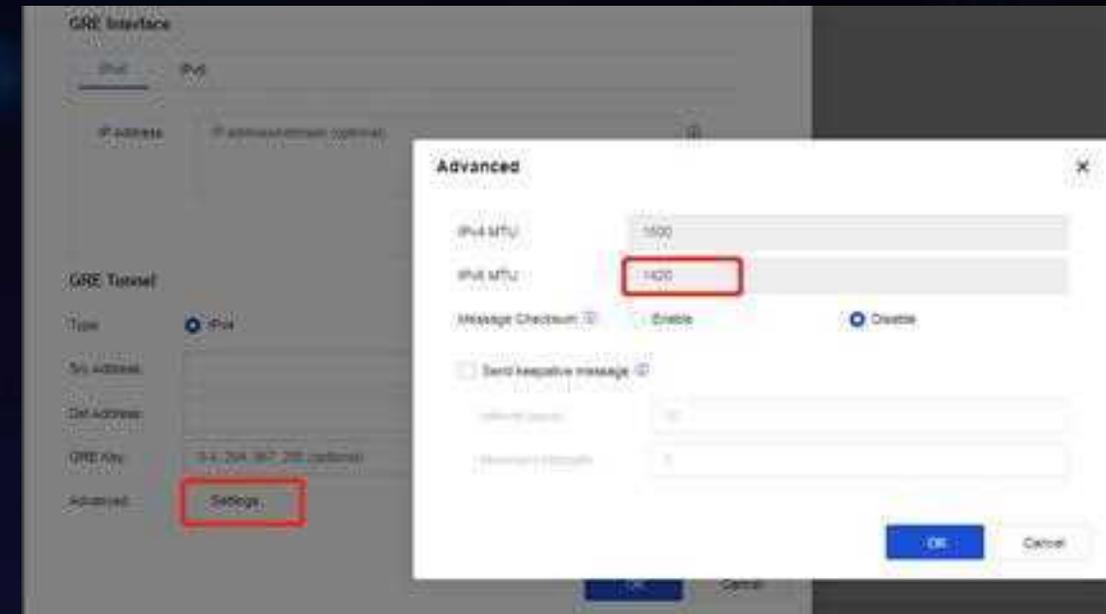
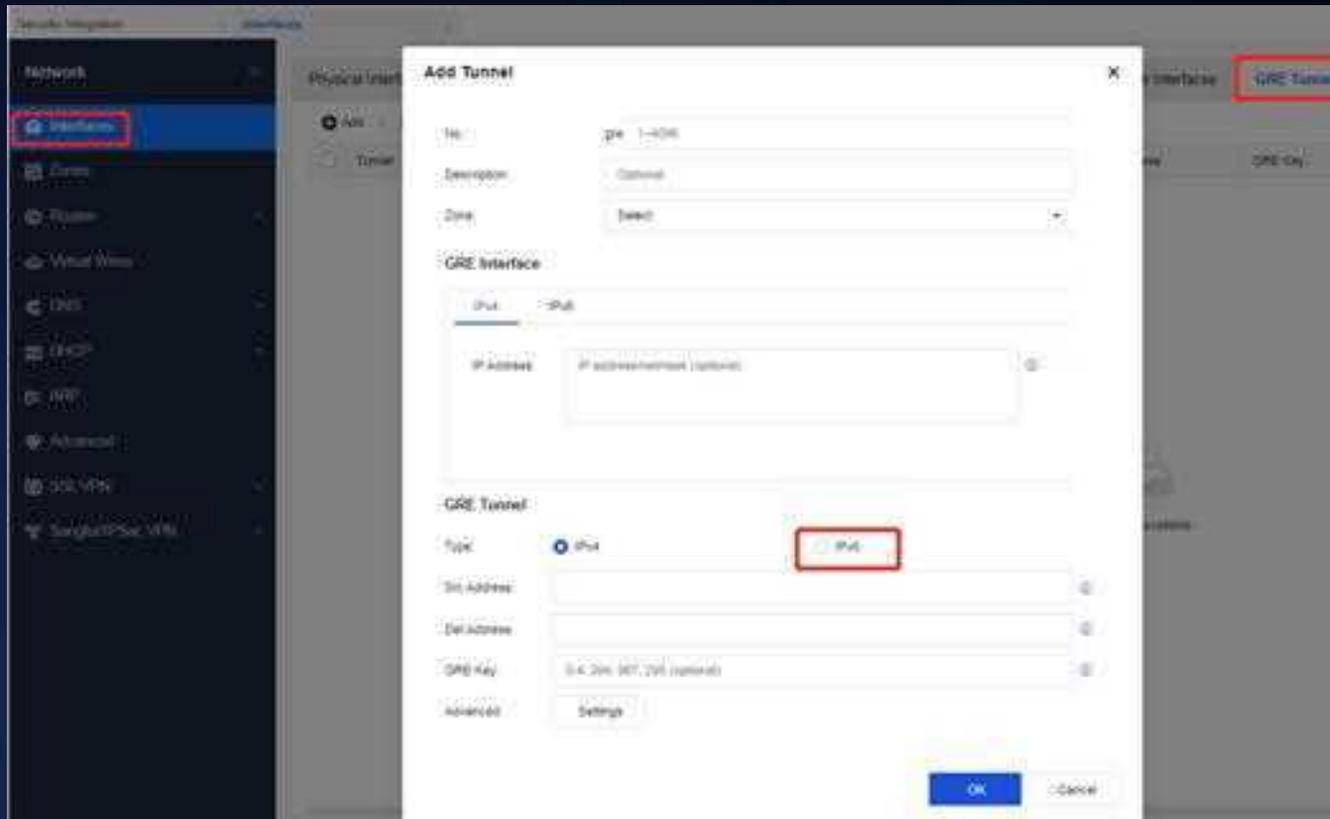
In Network Secure Platform, self-signed server certificate supports a dropdown menu to select the encryption key type and key size. Key types include RSA and ECC, while key size includes 2048 and 4096



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.

The screenshot displays the 'HA Policy Settings' configuration page. On the left, a navigation menu highlights 'High Availability'. The main content area is divided into several sections:

- HA Policy:** Includes a checked 'Enable' checkbox.
- Mode:** Radio buttons for 'Active/Standby' (selected) and 'Active/Active'.
- Device Name:** A text field containing 'sg101-0-08_VGAP'.
- Control Link:** A dropdown menu set to 'GigabitEthernet0/0/10', with 'Local' and 'Peer IP' options.
- Data Link:** A dropdown menu set to 'GigabitEthernet0/0/10', with 'Local' and 'Peer IP' options.
- Mirror Mode:** An unchecked 'Enable' checkbox.
- Advanced:** A 'Settings' button.

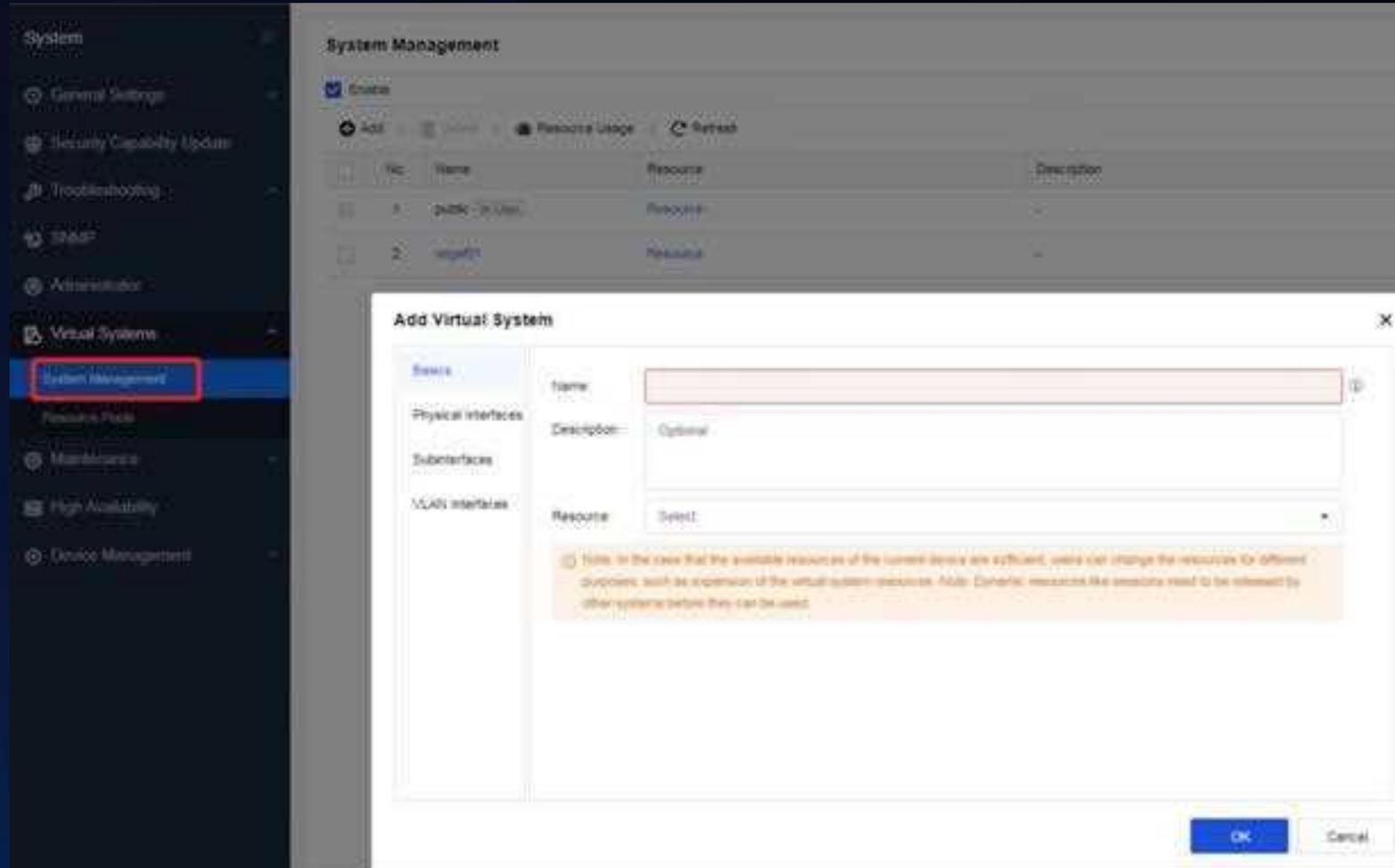
Below these settings is the 'Group 1' configuration section:

- Description:** A text field with 'General' entered.
- Priority:** A text field with '100' entered.
- Proactive Preemption:** An unchecked 'Enable' checkbox.
- Virtual IP Address:** A table with columns for 'Interface', 'Virtual IP Address', 'Virtual MAC', and 'Operation'. The table is currently empty, with a 'No data available' message at the bottom.

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 'Edit Physical Interface' configuration window for the eth0 interface. The 'Basics' section shows the following settings:

- Name: eth0
- Status: Enabled
- Description: Optional
- Virtual System: public
- Type: Layer 3
- Zone: admin-zone
- OSM: Enabled Settings

The 'IPV4' tab is selected, showing the following configuration:

- IP Assignment: Static
- Static IP: 192.168.251.251/24
- Default Gateway: 192.168.0.254

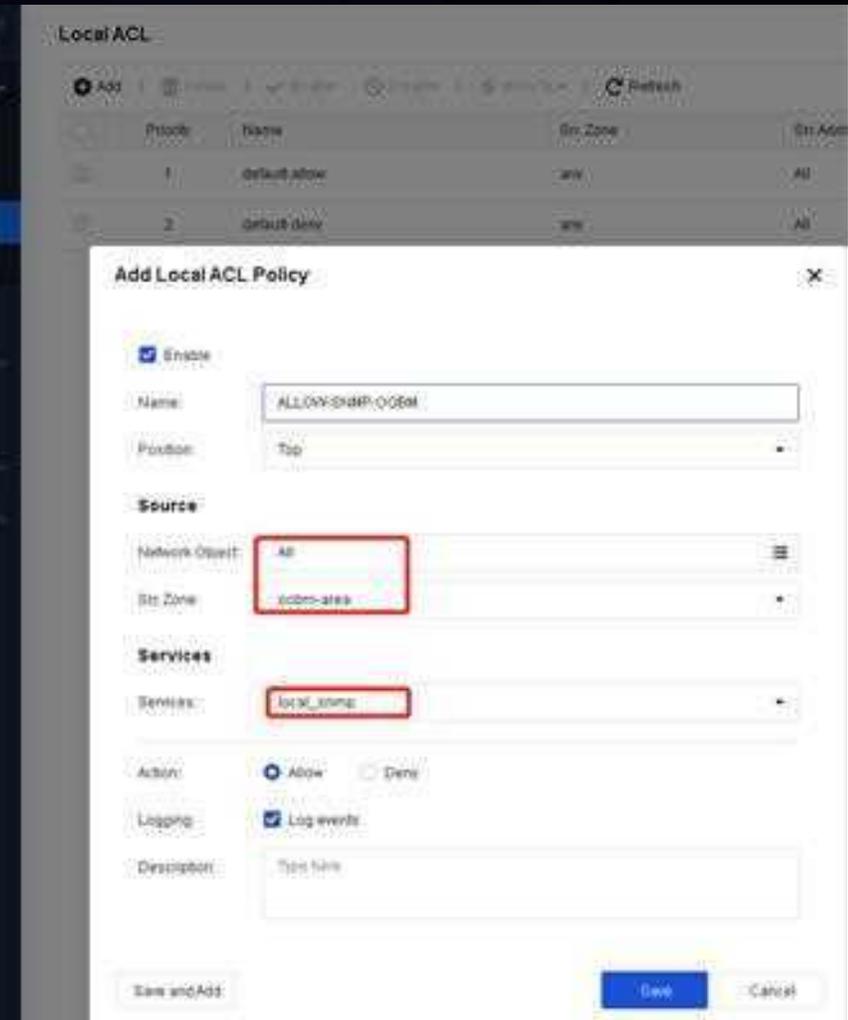
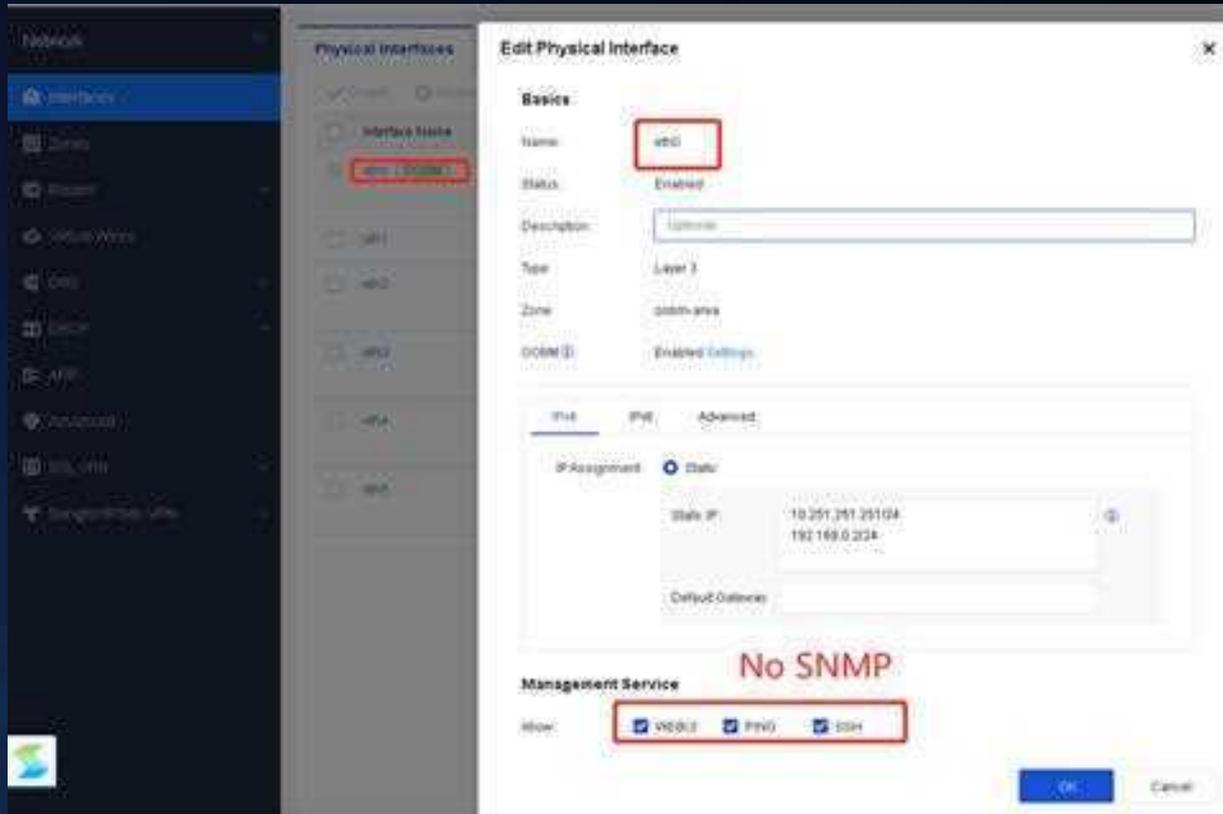
The background interface shows a list of physical interfaces, with eth0 highlighted in red. The 'Link State Propagation' table on the right lists various link modes and their statuses.

Link Mode	MTU (IPv4/IPv6)	Status	Operation
Full-duplex 100Mbps	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

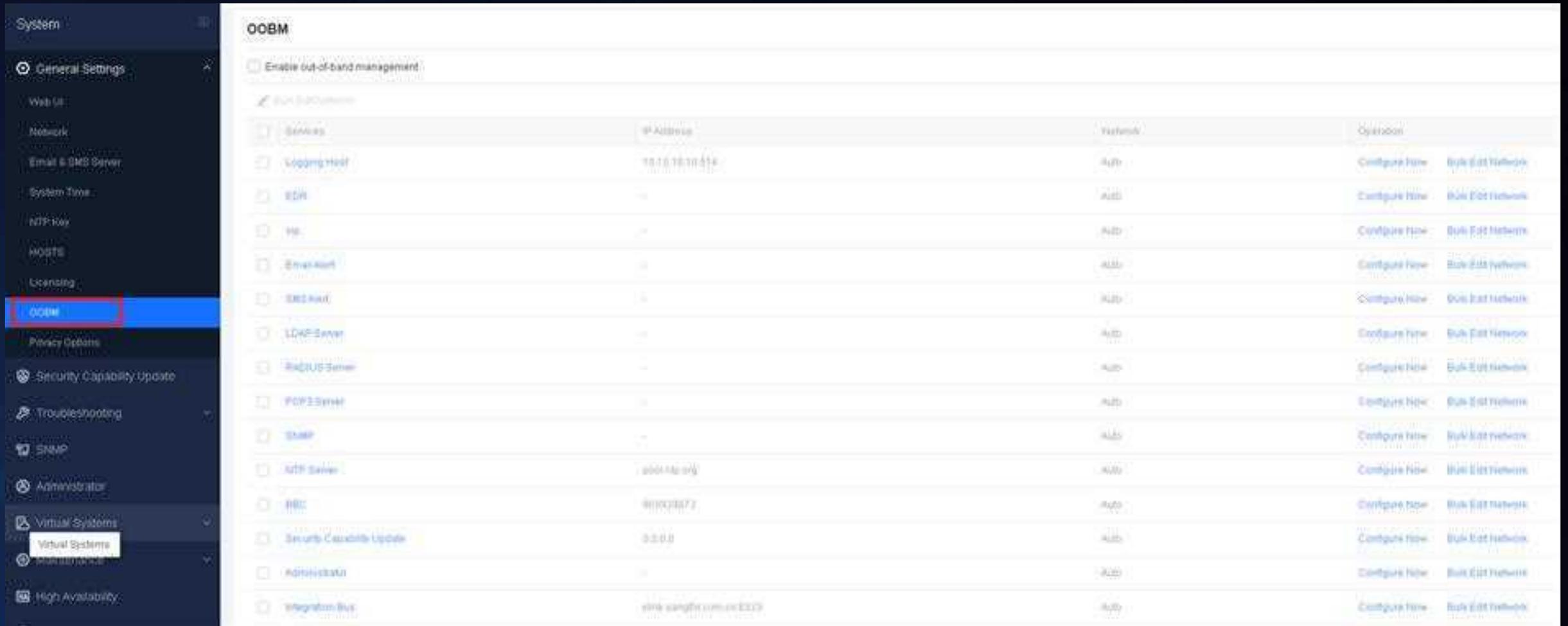
SNMP--Out-of-band Management Interface



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.



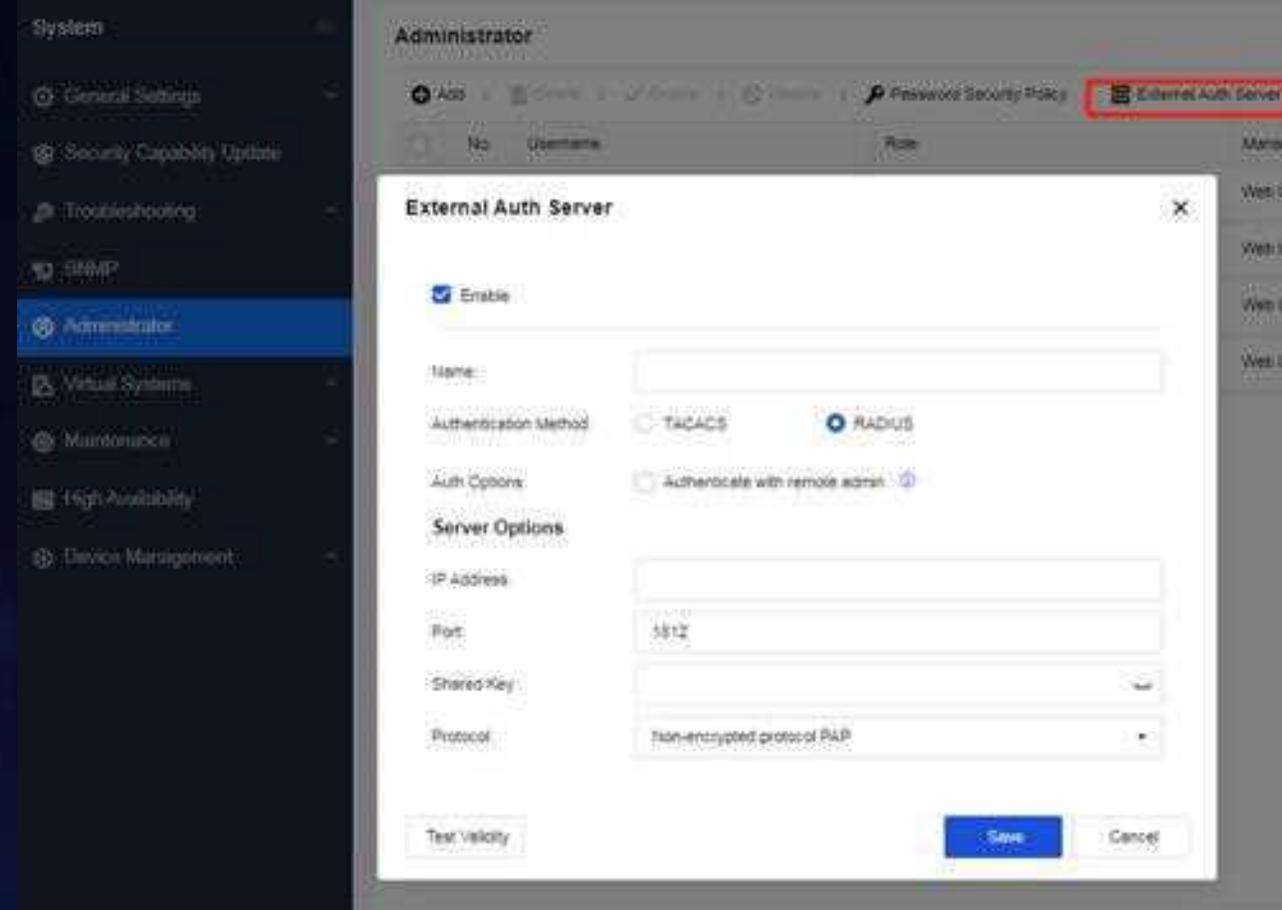
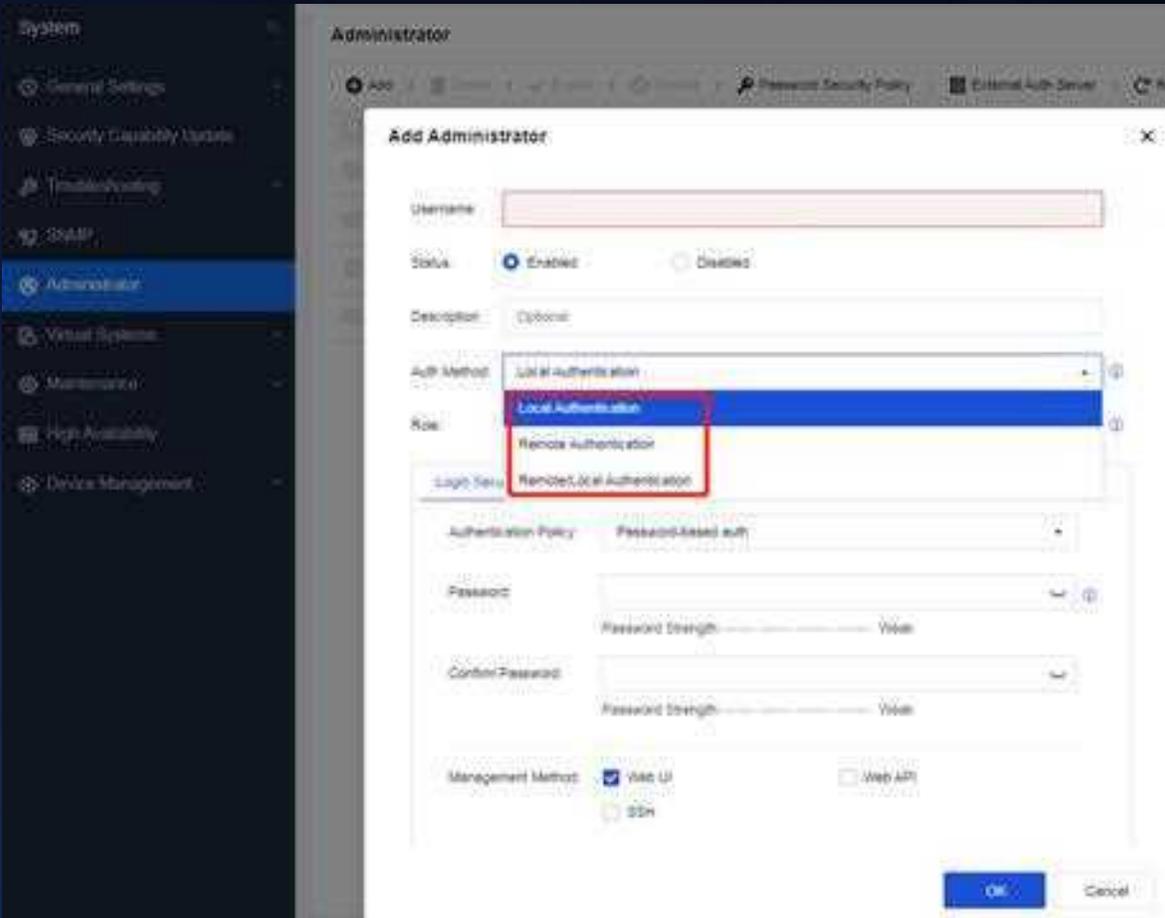
The screenshot shows the OoBM configuration interface. On the left is a navigation menu with 'OoBM' highlighted. The main area contains a table of services and their configurations.

Service	IP Address	Version	Operation
<input type="checkbox"/> Services			
<input type="checkbox"/> Logging Host	10.10.10.10/24	Auto	Configure Now Bulk Edit Network
<input type="checkbox"/> EDN	-	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	200.142.0/24	Auto	Configure Now Bulk Edit Network
<input type="checkbox"/> NTP	80/0.0.0.0/24	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"/> Registration Bus	10.10.10.10/24	Auto	Configure Now Bulk Edit Network

Administrator



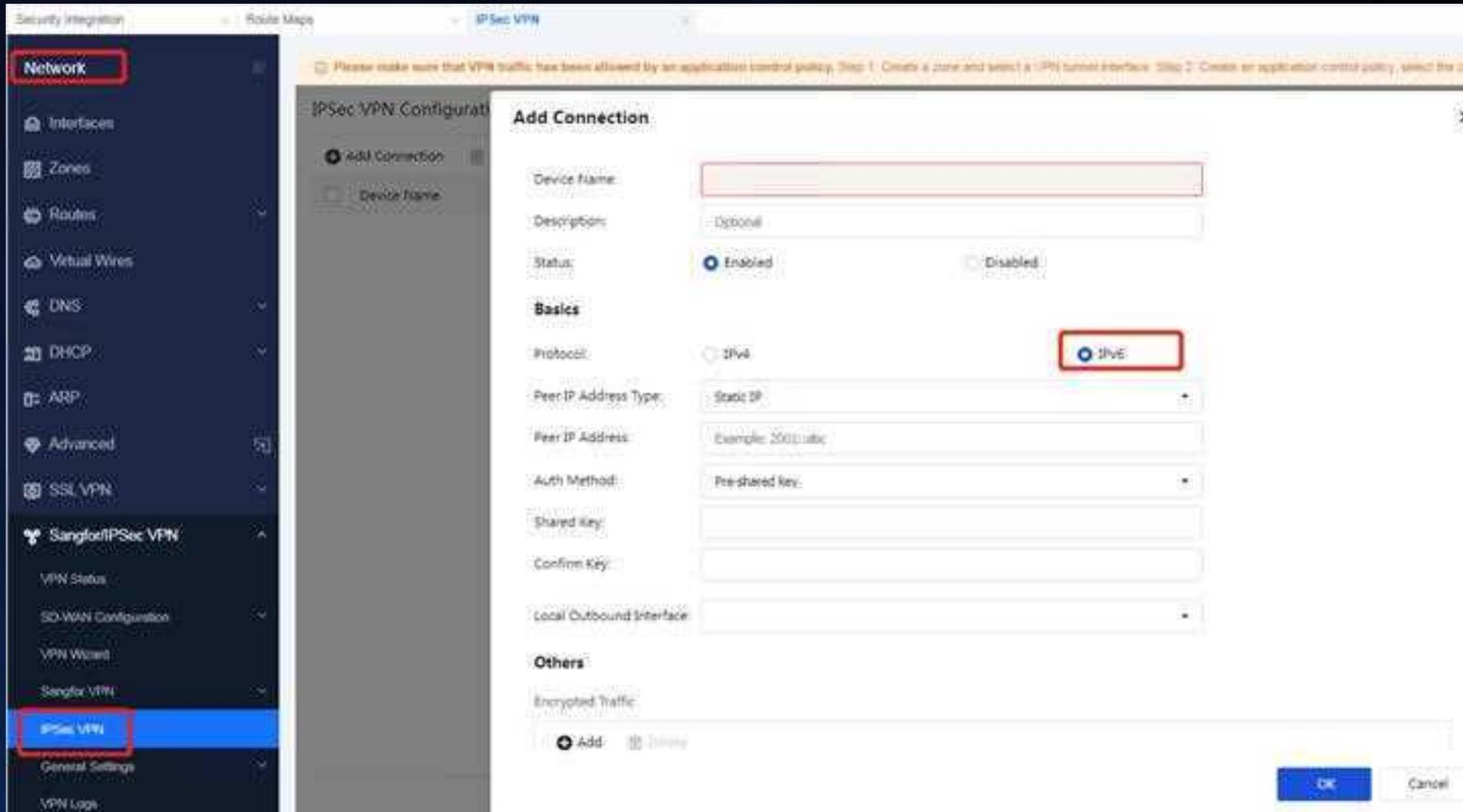
In Network Secure Platform, it adds extra authentication types, including local authentication, remote authentication, and remote/local authentication. When selecting remote/local authentication, external servers that have been previously configured are preferred for authentication. If the server cannot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

The screenshot displays the 'SD-WAN Path Selection Template (VPN HQ): 0630' configuration page. On the left, a navigation menu includes 'Network', 'Interfaces', 'Zones', 'Routes', 'Virtual Wires', 'DNS', 'DHCP', 'ARP', 'Advanced', 'SSL VPN', 'SangforIPSec VPN', 'VPN Status', 'SD-WAN Configuration', 'Path Selection Template' (highlighted with a red box), 'SOPAST Optimization', 'Category', 'VPN Wizard', 'Sangfor VPN', 'IPSec VPN', 'General Settings', and 'VPN Log'. The main area shows a list of policies with '1' selected. An 'Edit Policy' dialog box is open, showing the following settings:

- Policy Name: 0701
- App Identification: Mode set to 'Auto Ident'.
- Path Selection Settings: Mode set to 'By path quality' (highlighted with a red box). Other options include 'AutoGO Smart Path Selection', 'By specified path order', and 'By bandwidth remaining ratio'.
- Paths: A table with columns 'Local Path', 'Peer Path', and 'Operation'. It lists two paths: 'Path 1 (Static IP-China Mobile)' and 'Path 2 (Static IP-China Unicom)'. Below the table are 'Select local path', 'Select peer path', and 'Add' buttons, and a 'Clear All' link.
- More Options: 'Advanced' and 'Settings' buttons.
- Buttons: 'OK' and 'Cancel' at the bottom right.

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.

The screenshot shows the SOFAST Optimization configuration page. On the left is a dark sidebar menu with the following items: Network, Interfaces, Zones, Routes, Virtual Wire, DNS, DHCP, ARP, Advanced, SSL VPN, SangforIPSec VPN, VPN Status, SO-VPN Configuration, Path Selection Templates, SOFAST Optimization (highlighted in blue), Category, VPN Wizard, Sangfor VPN, and IPSec VPN. The main content area is titled 'SOFAST Optimization' and features a toggle switch for 'Enable SOFAST optimization' which is currently turned on. Below this is an 'Introduction' section with a warning banner: 'SOFAST optimization service takes effect after it is enabled on both the local and peer devices. Please enable it on the peer device.' The introduction text states: 'SOFAST optimization is committed to reducing packet loss rate for business apps and accelerating data transfer for bandwidth-intensive apps to leased lines, reducing operational costs.' Three application categories are listed: 'Interactive Apps' (with an icon of a person and a gear) where SOFAST can reduce response time by over 50% when packet loss rate is high; 'Bandwidth-intensive Apps' (with an icon of a download arrow) where SOFAST can speed up the transfer by over 10 times when packet loss rate is high; and 'Realtime Apps' (with an icon of a video call) where SOFAST can ensure clear and smooth quality of audio and video conferences even when packet loss rate reaches 50%. A 'Save' button is located at the bottom of the configuration area.

Application Category



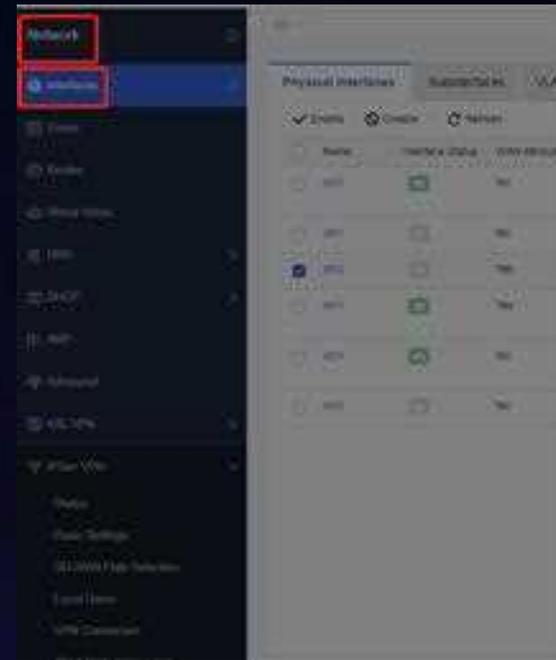
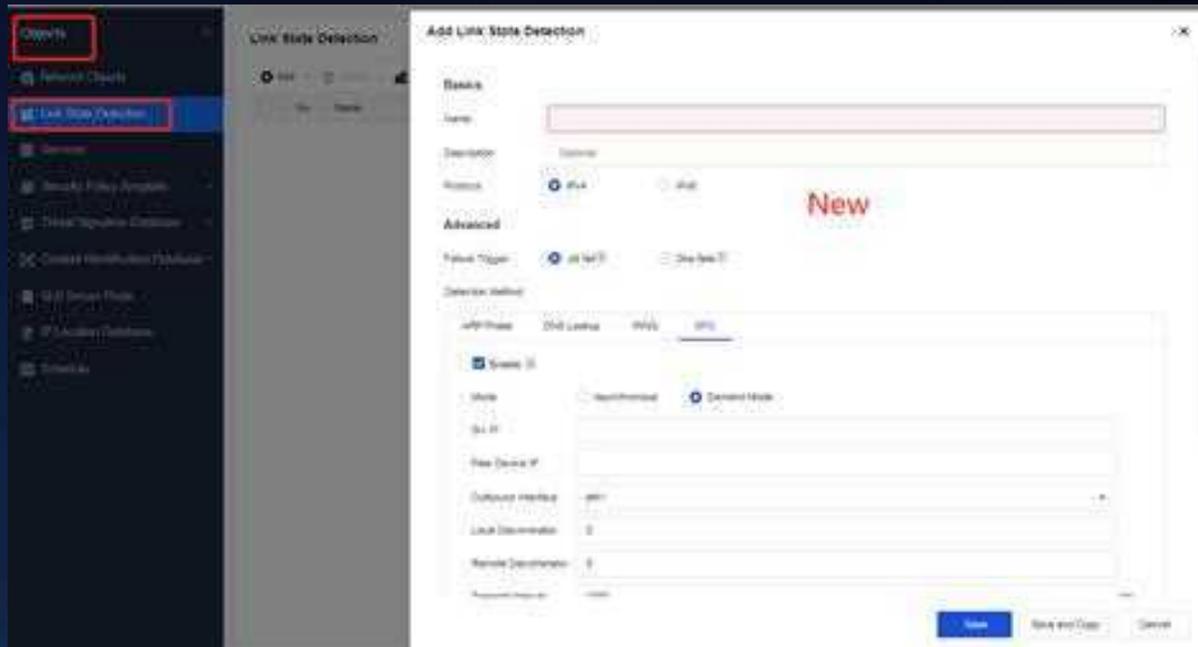
In Network Secure Platform, it add new application categories, and can define related business applications for reference in SDWAN path selection.

The screenshot shows the 'App Categories' configuration page in the Network Secure Platform. The left sidebar contains a navigation menu with 'SD-WAN Configuration' and 'Category' highlighted. The main content area shows a table of application categories with columns for 'Name' and 'Form'. An 'Add' dialog box is open, allowing the user to define a new category. The dialog includes fields for 'Name', 'Type', 'Criticality', and 'Applications'. A list of available applications is shown, including 'All', 'Others', 'DNS', 'Web Site', 'Mail', 'IM', 'Social Networking', and 'IM'. The 'Add' dialog also has 'OK' and 'Cancel' buttons.

Link State Detection



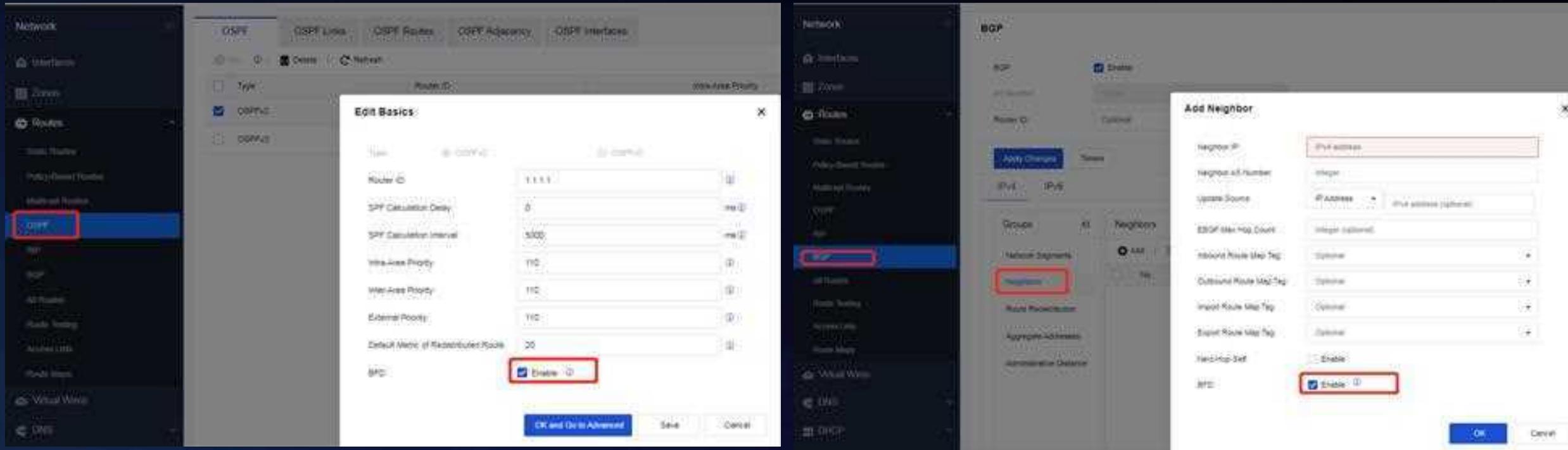
In Network Secure Platform, it adds a new menu page for link state detection, which allows configuration of link state detection for interfaces. Meanwhile, BFD link detection method has also been added.



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 management console interface. On the left, the 'Objects' menu is visible, with 'Link State Detection' highlighted. The main panel shows the 'Link State Detection' configuration page, which includes a table with the following data:

No.	Name	Protocol
1	0025	IPv4

Below the table, the 'Add Static Route' dialog box is open. In the 'Advanced' section, the 'Resilience Detection' dropdown menu is set to 'Link State', which is highlighted with a red box. The 'Link State' option is also highlighted in the dropdown list below it.

Local Loopback Interface



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

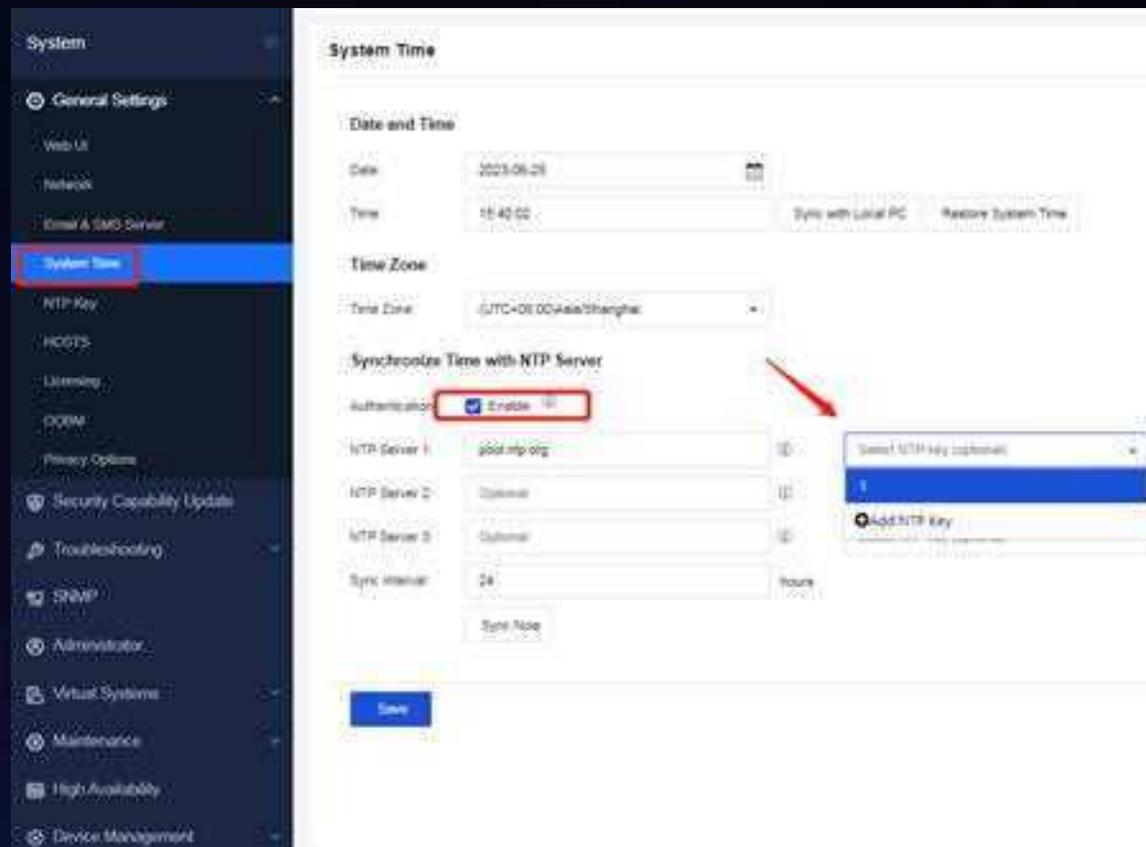
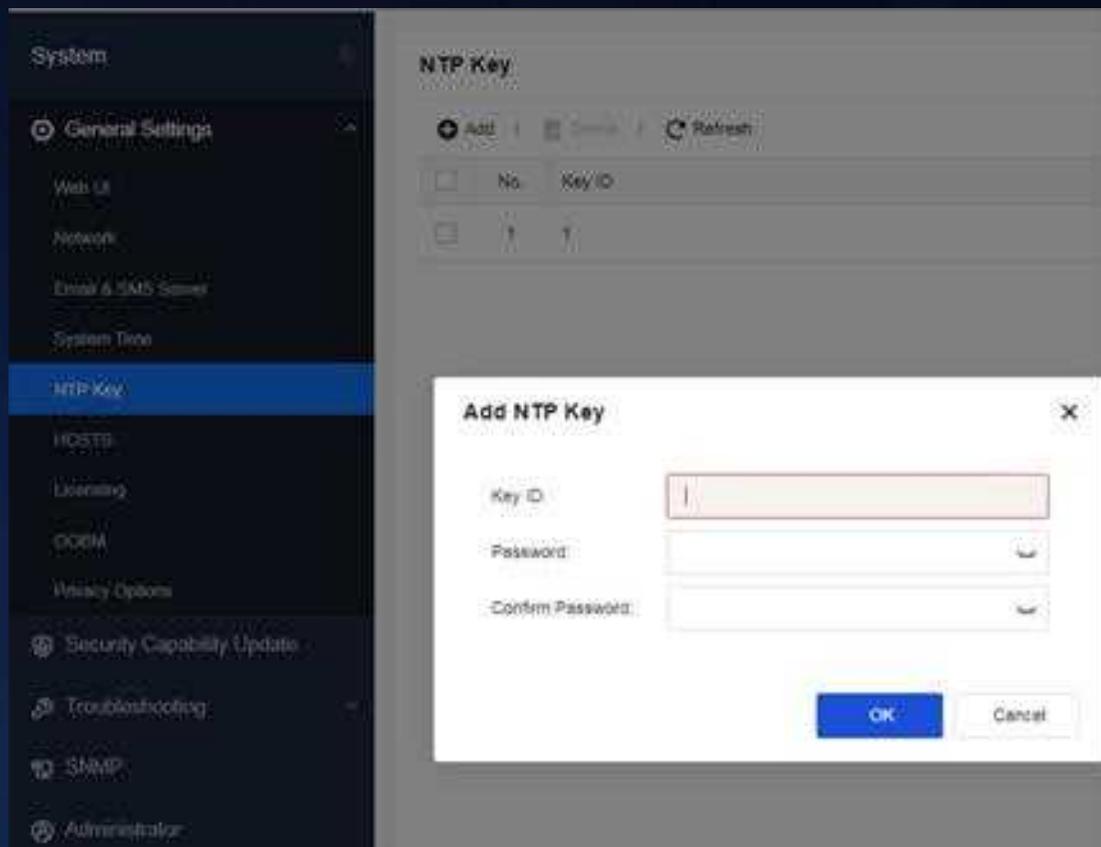
The screenshot displays the 'Local Loopback Interfaces' configuration page. The left sidebar shows a navigation menu with 'Interfaces' selected. The main content area has tabs for 'Physical Interfaces', 'Subinterfaces', 'VLAN Interfaces', 'Virtual Interfaces', 'Aggregate Interfaces', and 'Local Loopback Interfaces'. Below the tabs are 'Add', 'Delete', and 'Refresh' buttons. A table lists the configured interfaces:

Interface Name	IPv4 Address	IPv6 Address
loopback1	10.10.10.10/32	

NTP Key



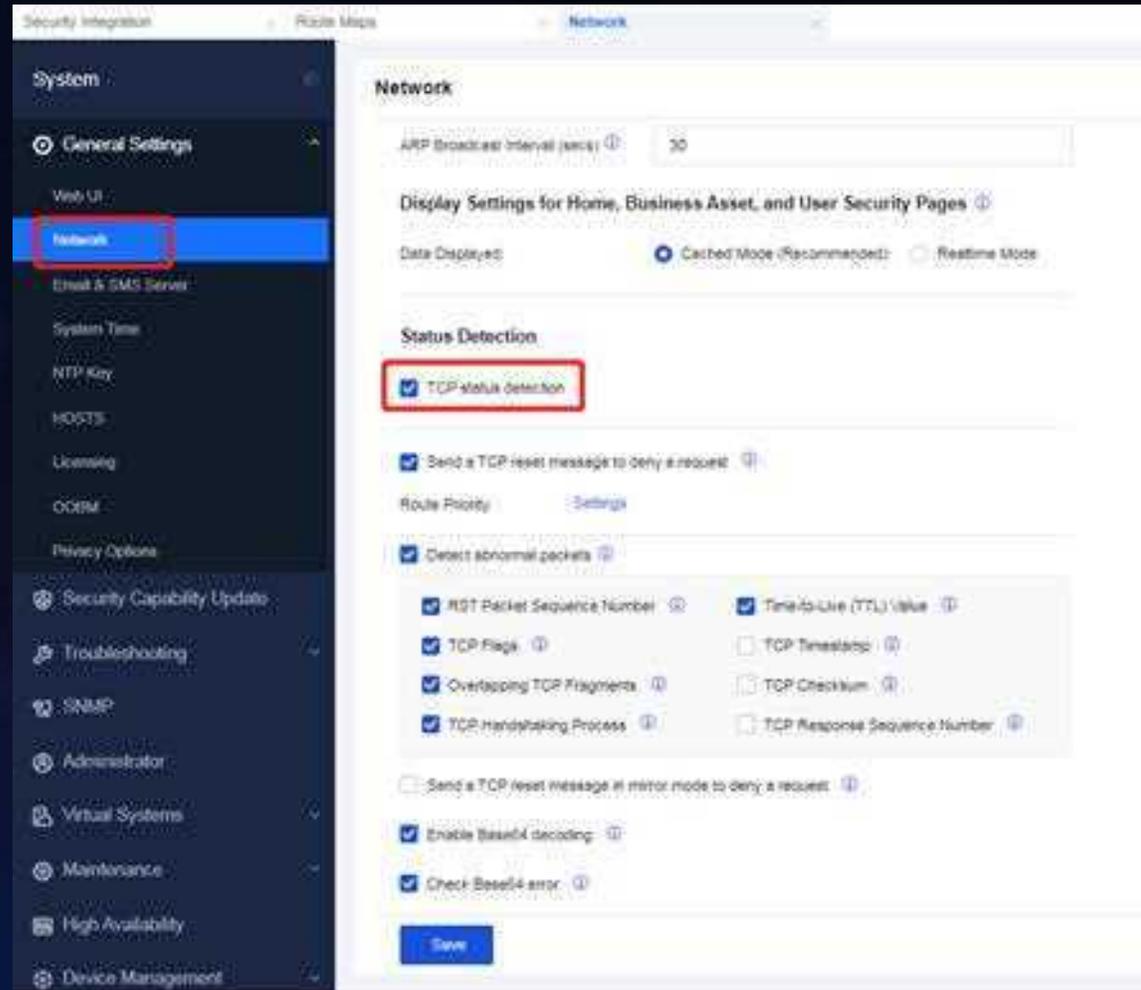
In Network Secure Platform, it adds NTP key feature which can meet the scenario of enabling NTP server authentication.



Network Parameter



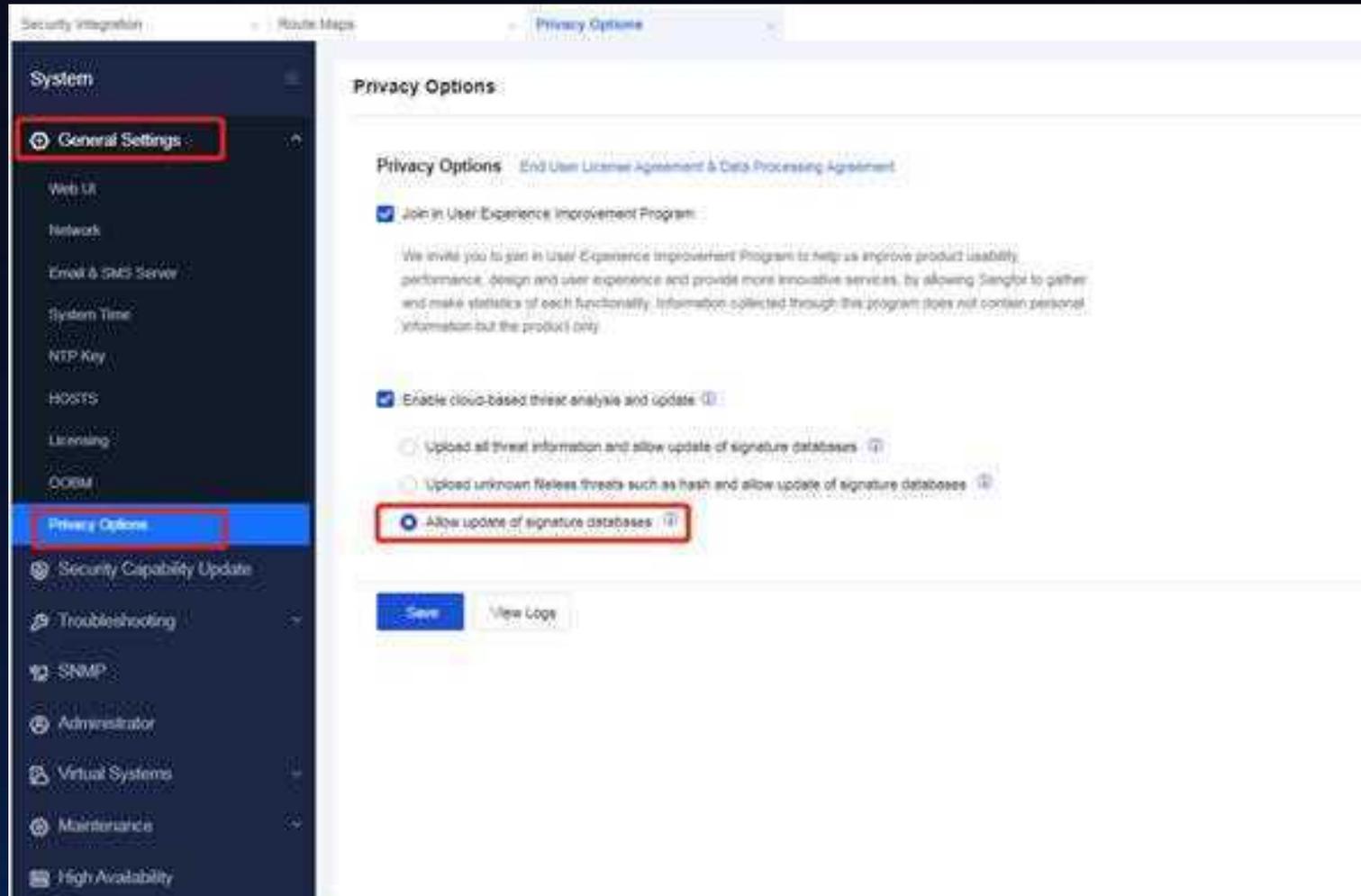
In Network Secure Platform, it adds the global network parameter of TCP status detection, which checks the state of flag bits in the first TCP data packet transmitted through to TCP malformed packet attacks and enhance the security of TCP connections.



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' section has 'Analysis of Traffic to NGAF' selected. The 'Status' is set to 'Allowed'. A 'Turn On' button is visible. Below the configuration, a message states 'Packet is allowed as per matched policy'. The 'Results (20)' table shows the following data:

No.	Time Occurred	Src IP	Dest IP	Dest Port	Protocol	Inbound Interface	Status	Description	View
1	18:18:37	172.16.10.10	172.16.10.1	840	TCP	eth0	allowed	Passed Through the Firewall	detail view
2	18:18:38	172.16.10.10	172.16.10.1	110	TCP	eth0	allowed	Passed Through the Firewall	detail view
3	18:18:38	172.16.10.10	172.16.10.1	443	TCP	eth0	allowed	Passed Through the Firewall	detail view
4	18:18:38	172.16.10.10	172.16.10.1	178	TCP	eth0	allowed	Passed Through the Firewall	detail view

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,

The screenshot displays the Sangfor Network Secure Platform interface. On the left, a navigation menu is visible with 'Troubleshooting' and 'Tools' highlighted. The main area shows the 'Packet Capture' section with a 'Create Capture Task' button. A 'Settings' dialog box is open, showing the following configuration:

- Max Files: 10
- Packets per File: 10000
- Mode: Non-promiscuous (selected), Promiscuous
- Timeout: 10 minutes

The 'Settings' dialog also includes an 'Interfaces' section with an 'Add' button and a table with columns for 'Interface', 'Filter Expression', and 'Operation'. The table is currently empty, displaying 'No data available'. At the bottom of the dialog are 'Capture' and 'Cancel' buttons.

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

Mode: Src IP (172.16.10.10) | Src Port (44) | Dest IP (44) | Dest Port (44) | Protocol (all) | Inbound Interface (all)

Flows	No.	Status	Inbound Interface	Outbound Interface	Time
Flow 1 172.16.10.10:1001 → 142.252.188.74:443	Packet 1	Forwarded	eth0	eth0	2023
Flow 2 172.16.10.10:1002 → 1.2.3.4:80	Packet 2	Forwarded	eth0	eth0	2023
Flow 3 172.16.10.10:1003 → 10.0.0.0:8080	Packet 3	Forwarded	eth0	eth0	2023
Flow 4 172.16.10.10:1004 → 10.0.0.0:8080	Packet 4	Forwarded	eth0	eth0	2023
Flow 5 172.16.10.10:1005 → 10.0.0.0:8080	Packet 5	Forwarded	eth0	eth0	2023
Flow 6 172.16.10.10:1007 → 52.182.143.210:443	Packet 6	Forwarded	eth0	eth0	2023
Flow 7 172.16.10.10:1008 → 172.217.27.10:443	Packet 7	Forwarded	eth0	eth0	2023
Flow 8 172.16.10.10:1009 → 10.0.0.0:8080	Packet 8	Forwarded	eth0	eth0	2023
Flow 9 172.16.10.10:1034 → 10.0.0.0:8080	Packet 9	Forwarded	eth0	eth0	2023
Flow 10					

Flow 3 - Packet 5 | 510 packets | Previous | Next | X

Forwarding | Forwarded

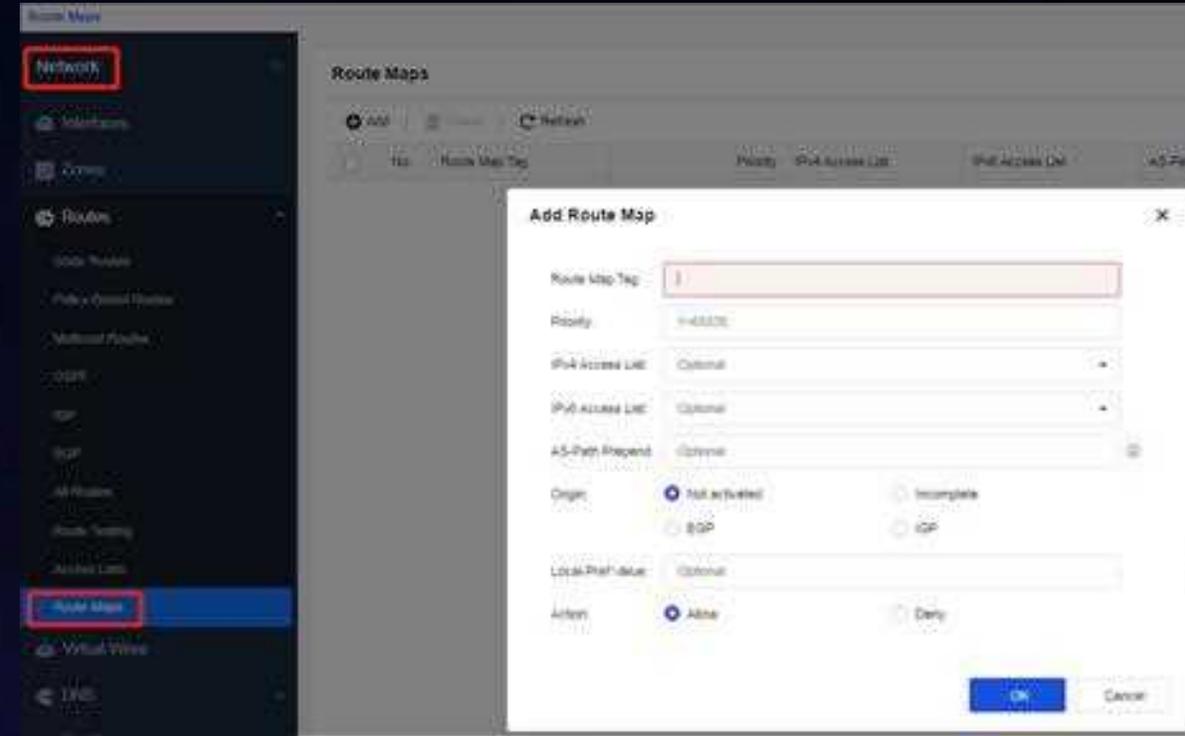
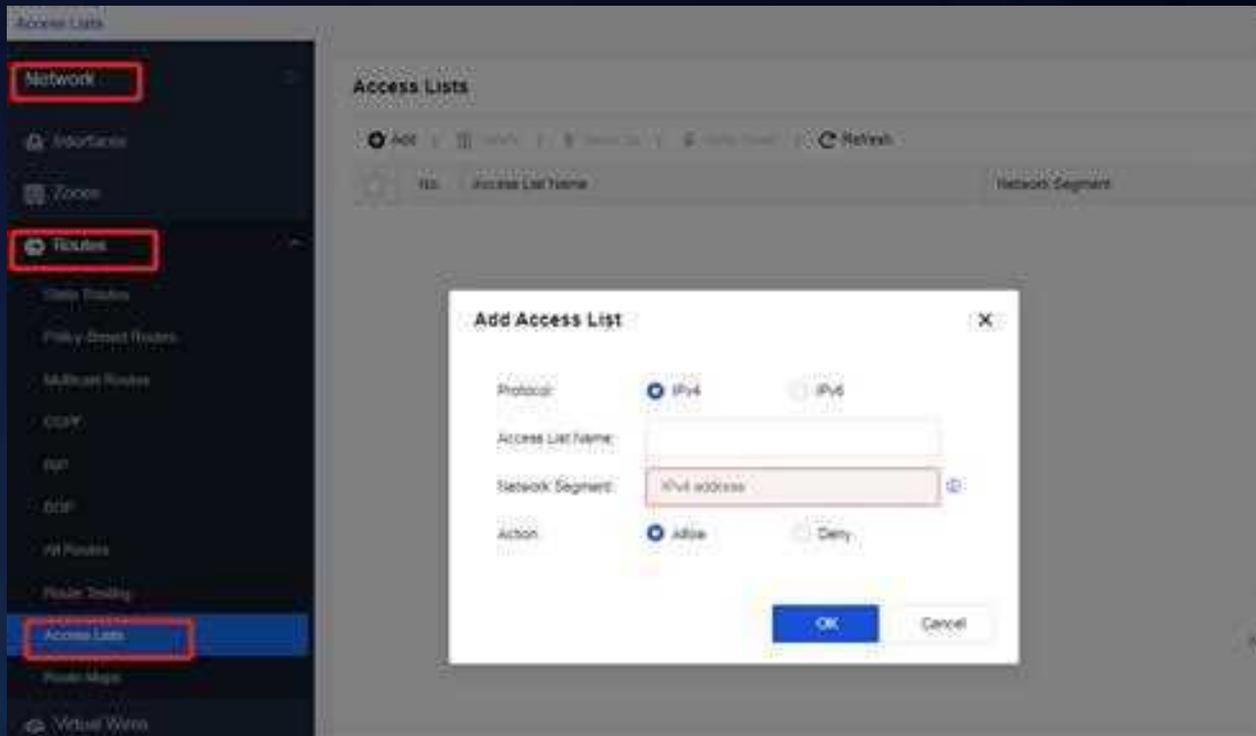
Inbound interface: eth0 | Outbound interface: eth0

- 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: 430C
- Session update
- TCP packet processing
- Packet modification during NAT
- TTL processing for IP headers
- Packet sending on interface
- NIC 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.



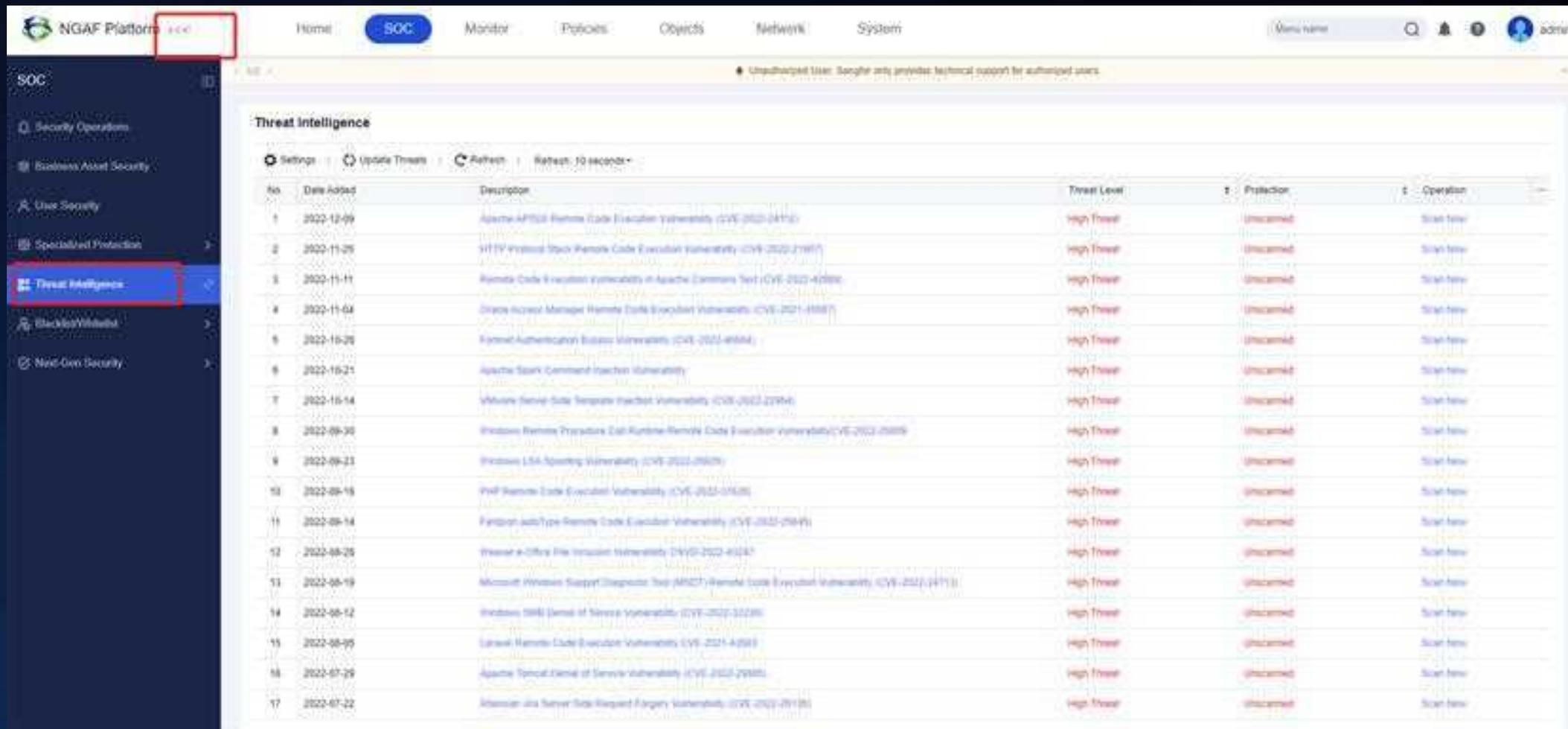
PART 4

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 shows the NGAF Platform interface. The top navigation bar includes 'Home', 'SOC', 'Monitor', 'Policies', 'Objects', 'Network', and 'System'. The left sidebar lists various security modules, with 'Threat Intelligence' highlighted in blue. The main content area displays a table of threat intelligence entries.

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	VMware vSphere Stack Remote Code Execution Vulnerability (CVE-2022-1997)	High Threat	Unscanned	Scan Now
3	2022-11-11	Remote Code Execution Vulnerability in Apache Commons Text (CVE-2022-42859)	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	Kernel Authentication Bypass Vulnerability (CVE-2022-08584)	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-2022-2794)	High Threat	Unscanned	Scan Now
8	2022-09-30	Windows Remote Procedure Call Runtime Remote Code Execution Vulnerability (CVE-2022-3665)	High Threat	Unscanned	Scan Now
9	2022-09-23	Windows LSA Spooling Vulnerability (CVE-2022-3662)	High Threat	Unscanned	Scan Now
10	2022-09-16	PDF Remote Code Execution Vulnerability (CVE-2022-3742)	High Threat	Unscanned	Scan Now
11	2022-09-14	Fortinet autoType Remote Code Execution Vulnerability (CVE-2022-2944)	High Threat	Unscanned	Scan Now
12	2022-08-26	Wondershare PDFElement File Inclusion Vulnerability (CVE-2022-42247)	High Threat	Unscanned	Scan Now
13	2022-08-19	Microsoft Windows Support Diagnostic Tool (MSDT) Remote Code Execution Vulnerability (CVE-2022-3411)	High Threat	Unscanned	Scan Now
14	2022-08-12	Windows DNS Service of Service Vulnerability (CVE-2022-3228)	High Threat	Unscanned	Scan Now
15	2022-08-05	Drupal Remote Code Execution Vulnerability (CVE-2021-4-288)	High Threat	Unscanned	Scan Now
16	2022-07-29	Apache Tomcat Denial of Service Vulnerability (CVE-2022-2905)	High Threat	Unscanned	Scan Now
17	2022-07-22	Atlassian Jira Server Side Request Forgery Vulnerability (CVE-2022-29126)	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 top navigation bar includes Home, SOC, Monitor, Policies (highlighted), Objects, Network, and System. A notification banner at the top states: "Cloud-Delivered Protection is activated. NGAF will compare IP addresses with the IP reputation database and block the ones that match. View".

The left sidebar menu is titled "Policies" and includes the following items: Access Control, Application Control, Geolocation Blocking, Local ACL, Connection Control, NAT, Network Security (expanded), Policies, Anti-DDoS, **Signature Model Training** (highlighted with a red box), Server Access Authentication, Risk Analysis, Decryption, Bandwidth Management, Authentication, and Custom Webpage.

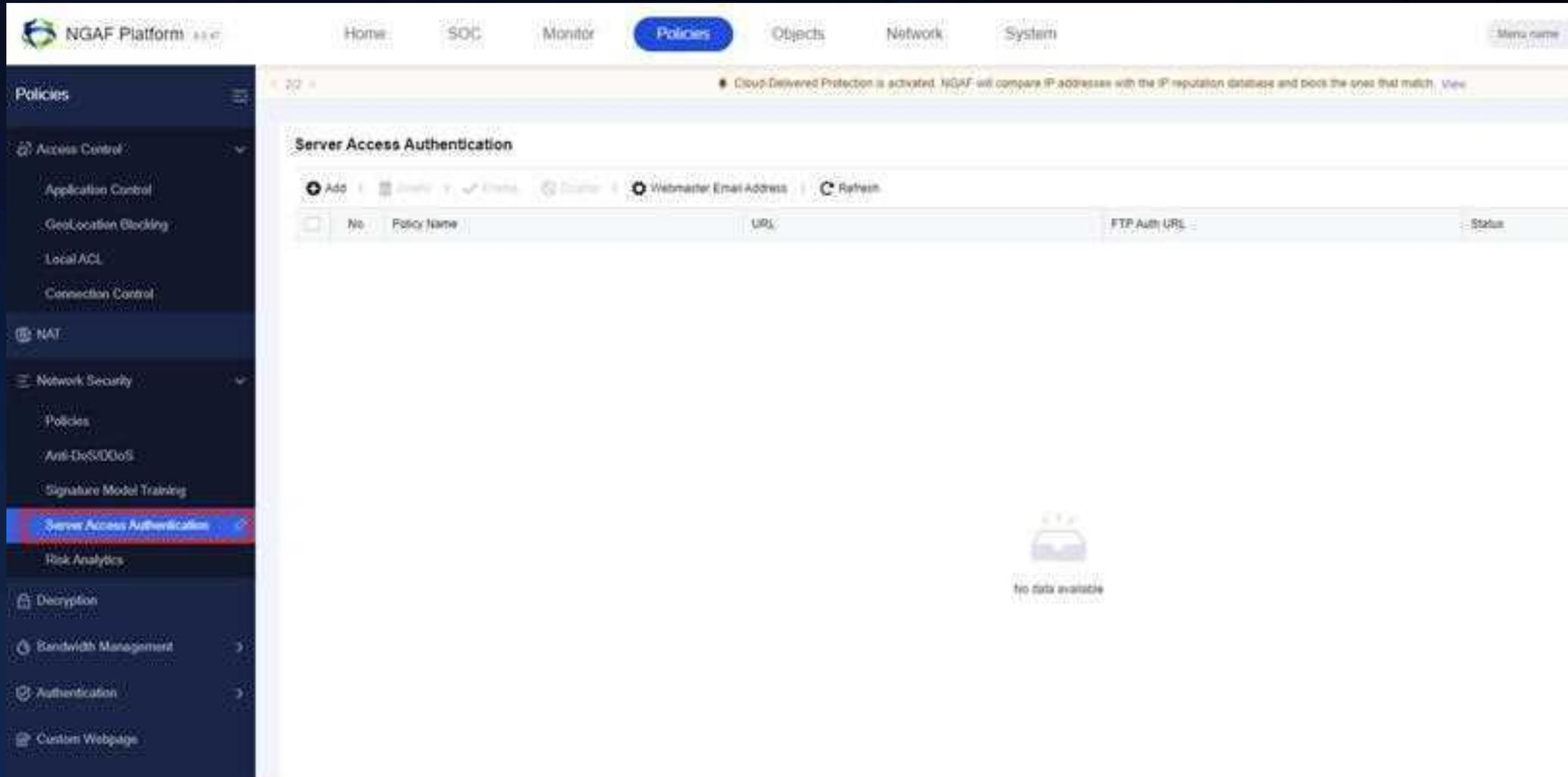
The main content area is titled "Signature Model Training" and features a "Refresh" button. It is divided into several sections:

- Business Assets (0):** A search box for "Name, IP address" and a "No data available" message.
- Why Business Asset Signature Model?** A text box explaining: "Fix false positives caused by conflicts between WAF codes and rules and prevent impacts on business asset. NGAF uses big data analytics engine to analyze business asset traffic and build a web application-based signature model, in order to eliminate false positives caused by improper programming and security policy contradictions, and enhance business asset stability."
- Pending Threat Signatures (0) / Marked Threat Signatures (0):** A table with columns: No., Signature Model, URL, Statement, Visits, Time, and Operation. The table is currently empty, showing a "No data available" message.

Server Access Authentication



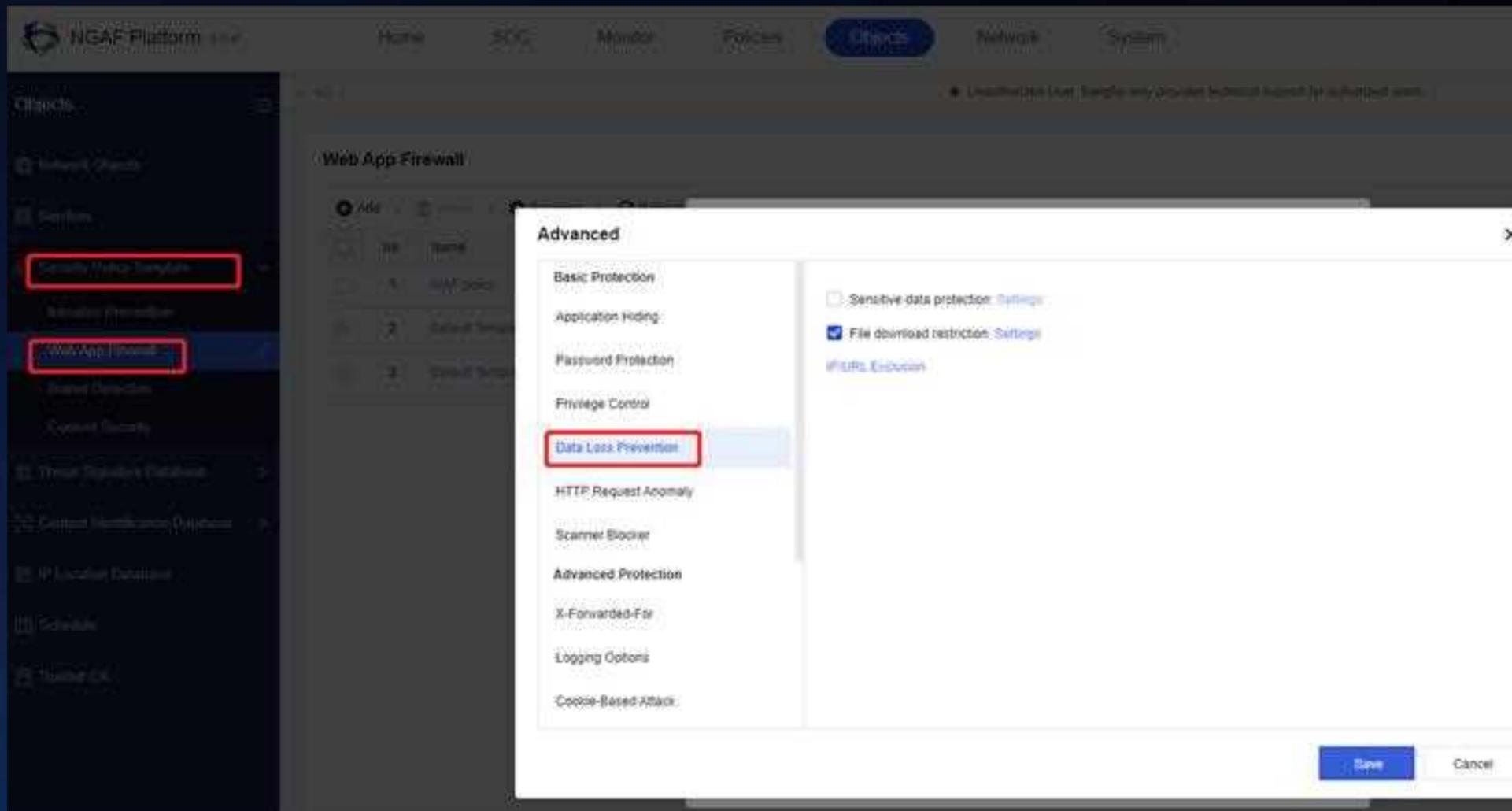
In Network Secure Platform, it deletes the Server Access Authentication module.



Server Access Authentication



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





THANK YOU

