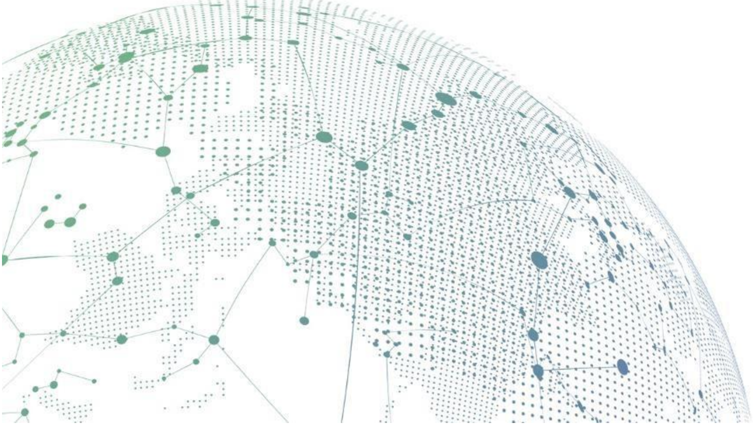
NGAF

Sangfor VPN Configuration Guide



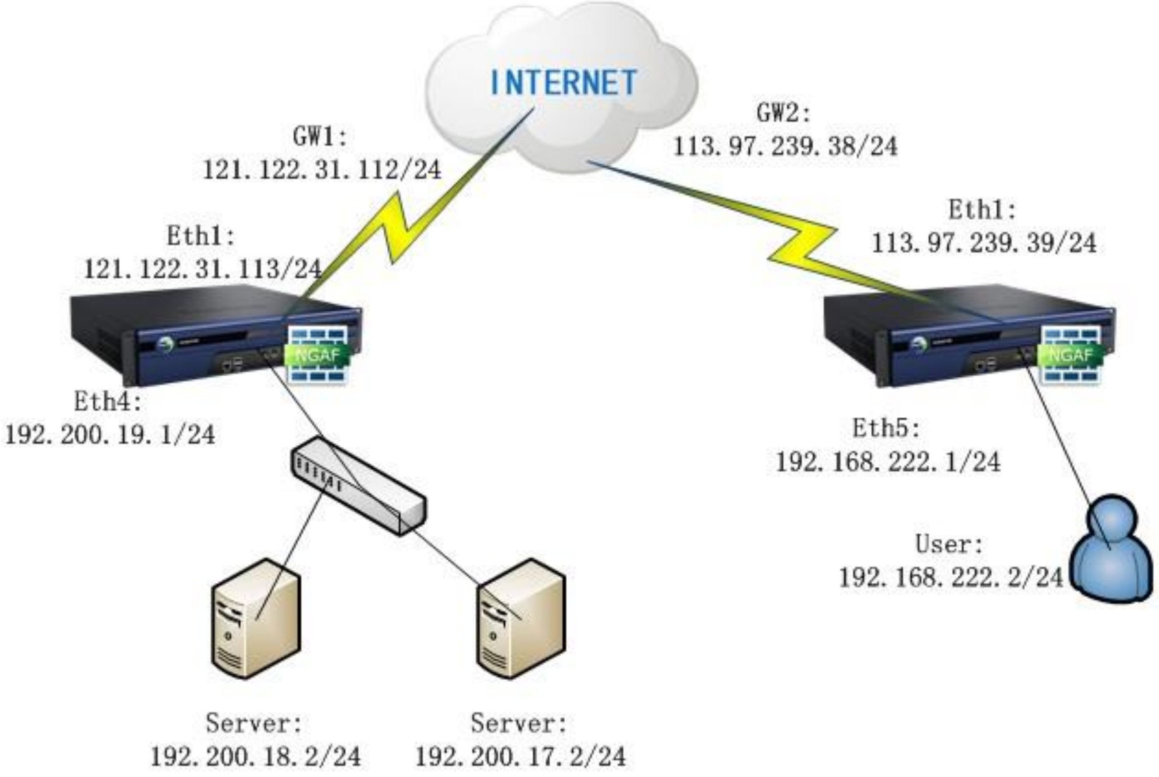
Change Log

Date	Change Description
Jun 16, 2021	Version 8.0.35 document release.

Contents

Chapter 1 Network Topology

One customer has two sites, they want to use Sangfor NGAF build VPN tunnel between HQ and branch.



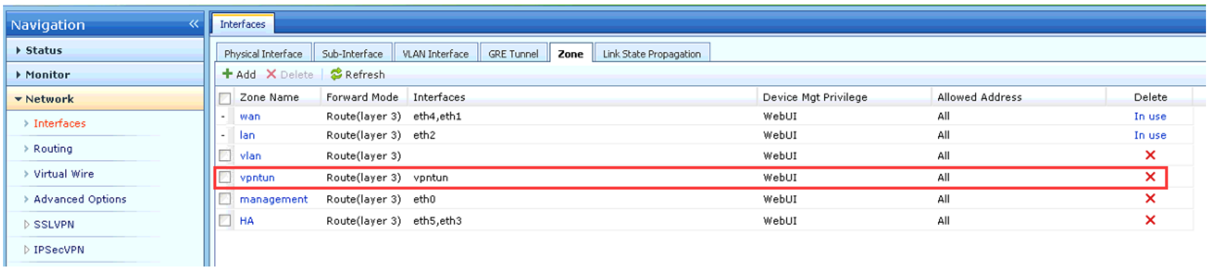
Chapter 2 NGAF Configuration

2.1 Version 8.0.26

2.1.1 HQ NGAF Configuration

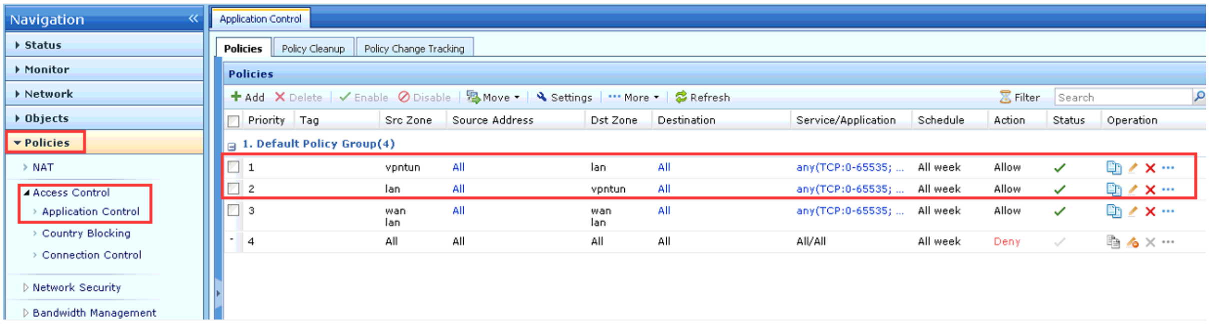
1. Configure interface and zone.

   Specially build a zone for VPN, chose vpntun interface.



Zone Name	Forward Mode	Interfaces	Device Mgt Privilege	Allowed Address	Delete
wan	Route(layer 3)	eth4,eth1	WebUI	All	In use
lan	Route(layer 3)	eth2	WebUI	All	In use
vlan	Route(layer 3)		WebUI	All	✕
vpntun	Route(layer 3)	vpntun	WebUI	All	✕
management	Route(layer 3)	eth0	WebUI	All	✕
HA	Route(layer 3)	eth5,eth3	WebUI	All	✕

2. Allow traffic in Access control from VPN zone to Server zone and Server zone to VPNzone.

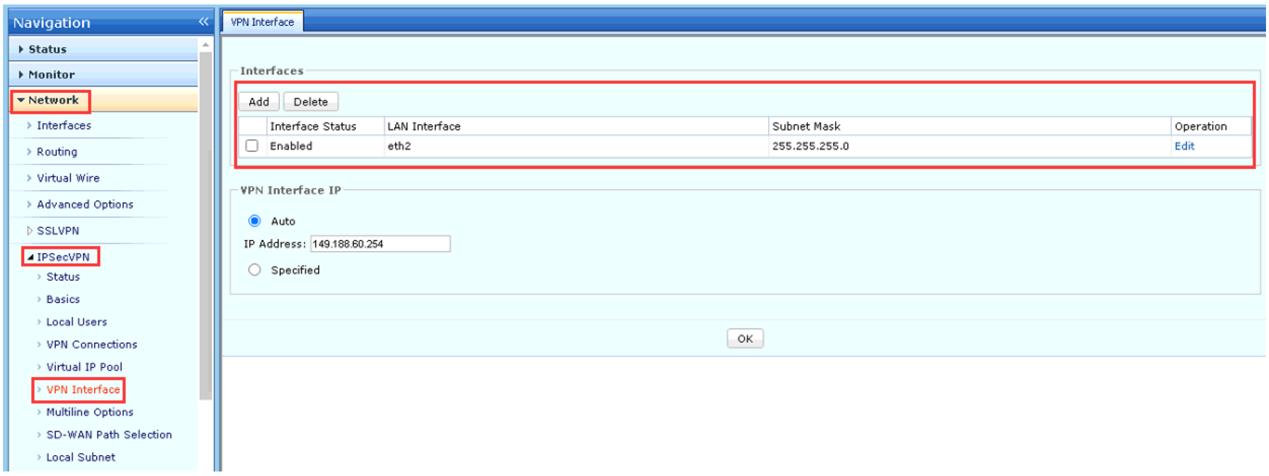


Priority	Tag	Src Zone	Source Address	Dst Zone	Destination	Service/Application	Schedule	Action	Status	Operation
1. Default Policy Group(4)										
1		vpntun	All	lan	All	any(TCP:0-65535; ...	All week	Allow	✓	
2		lan	All	vpntun	All	any(TCP:0-65535; ...	All week	Allow	✓	
3		wan lan	All	wan lan	All	any(TCP:0-65535; ...	All week	Allow	✓	
4		All	All	All	All	All/All	All week	Deny	✓	

3. Build VPN interface.

   This step used to notice other side that HQ has a subnet 192.200.19.0/24

   (Add all NGAF LAN interface to this)



Interfaces

Interface Status	LAN Interface	Subnet Mask	Operation
Enabled	eth2	255.255.255.0	Edit

VPN Interface IP

● Auto

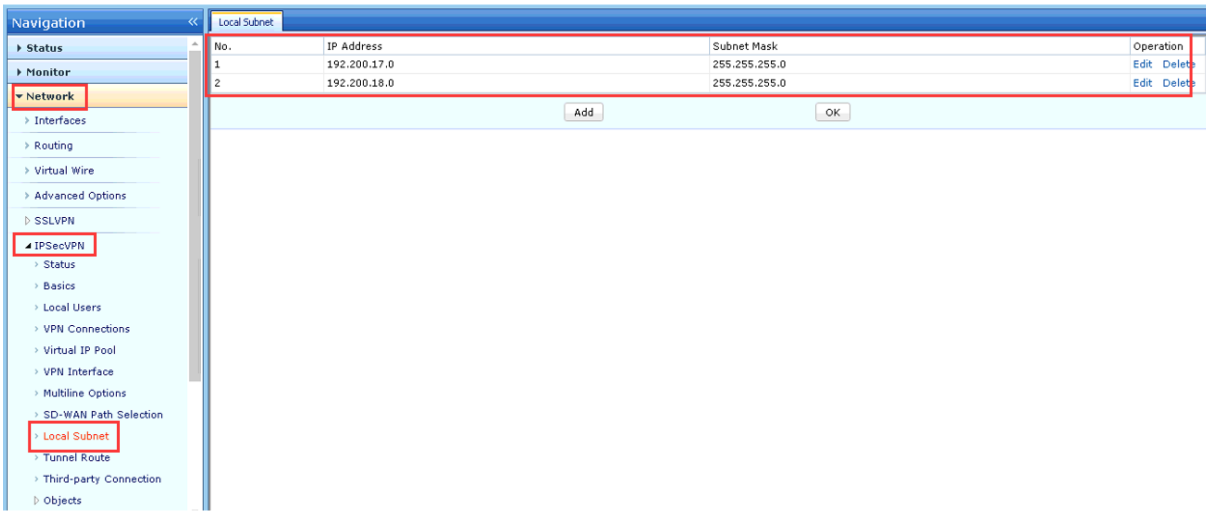
IP Address: 149.188.60.254

○ Specified

4. Add local subnet.

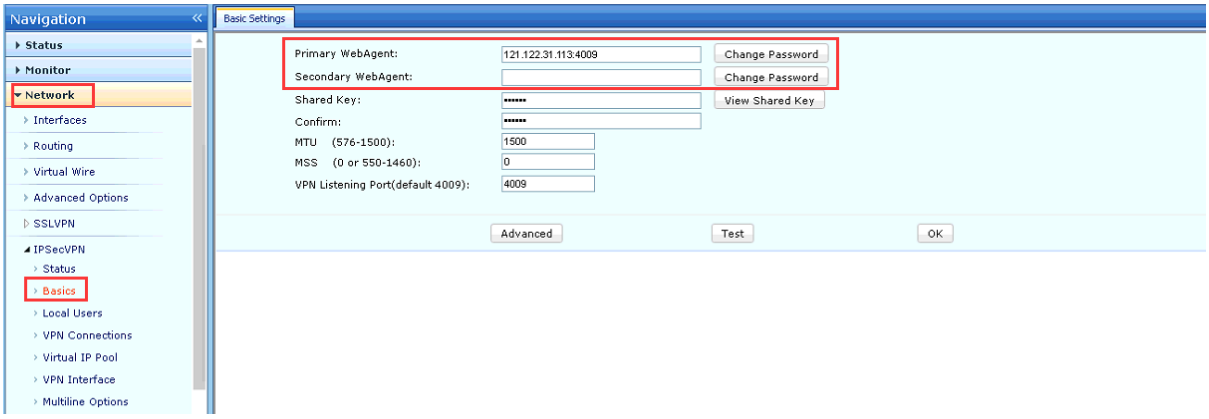
This step used to notice other side that HQ also has 192.200.17.0/24 and 192.200.19.18.0/24 which are not directly configure on NGAF Lan port.

(Don't need to add NGAF interface subnet to local subnet)



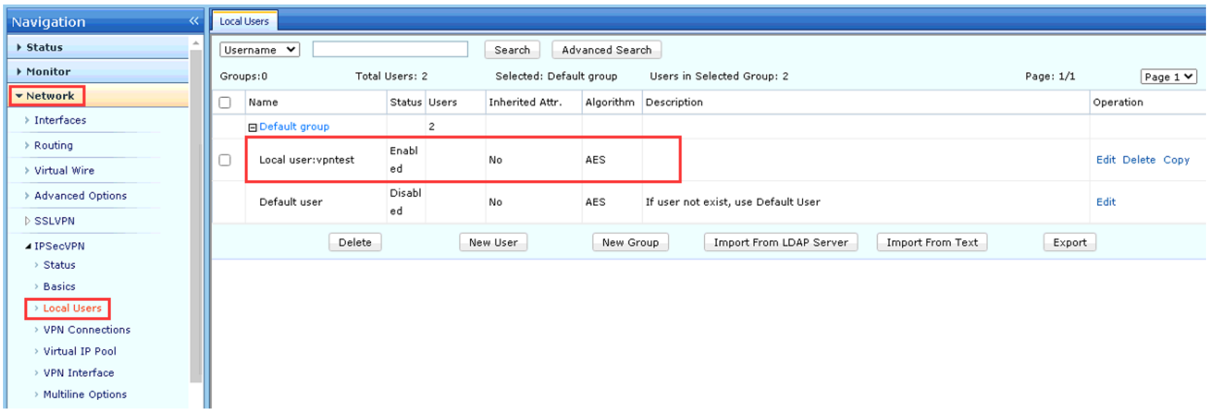
No.	IP Address	Subnet Mask	Operation
1	192.200.17.0	255.255.255.0	Edit Delete
2	192.200.18.0	255.255.255.0	Edit Delete

5. Set webagent and listening port



Primary WebAgent: 121.122.31.113:4009
Secondary WebAgent:
Shared Key: ••••••
Confirm: ••••••
MTU (576-1500): 1500
MSS (0 or 550-1460): 0
VPN Listening Port(default 4009): 4009

6. Create a branch user, user type：branch user



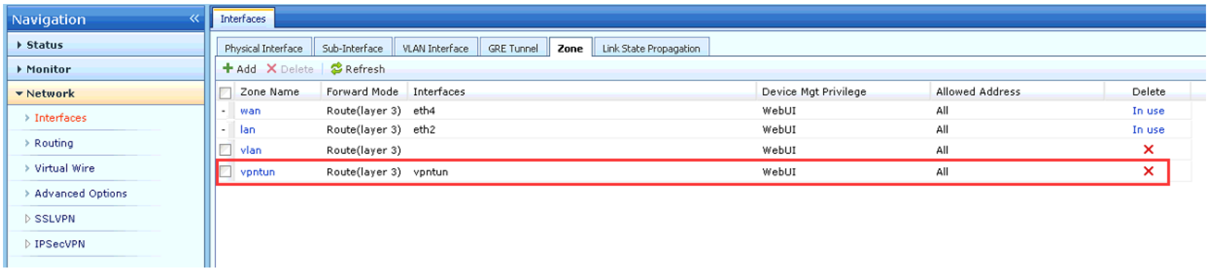
Groups:0 Total Users: 2 Selected: Default group Users in Selected Group: 2 Page: 1/1

□	Name	Status	Users	Inherited Attr.	Algorithm	Description	Operation
	⊟ Default group		2				
□	Local user:vpntest	Enabled		No	AES		Edit Delete Copy
	Default user	Disabled		No	AES	If user not exist, use Default User	Edit

2.1.2 Branch NGAF Configuration

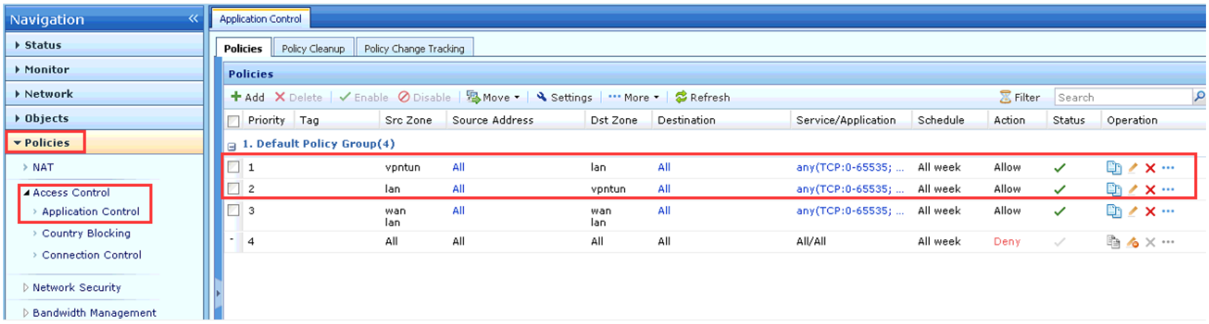
1. Configure interface and zone.

   Specially build a zone for VPN, chose vpntun interface.



	Zone Name	Forward Mode	Interfaces	Device Mgt Privilege	Allowed Address	Delete
-	wan	Route(layer 3)	eth4	WebUI	All	In use
-	lan	Route(layer 3)	eth2	WebUI	All	In use
□	vlan	Route(layer 3)		WebUI	All	✕
□	vpntun	Route(layer 3)	vpntun	WebUI	All	✕

2. Allow traffic in Access control from VPN zone to Server zone and Server zone to VPNzone.

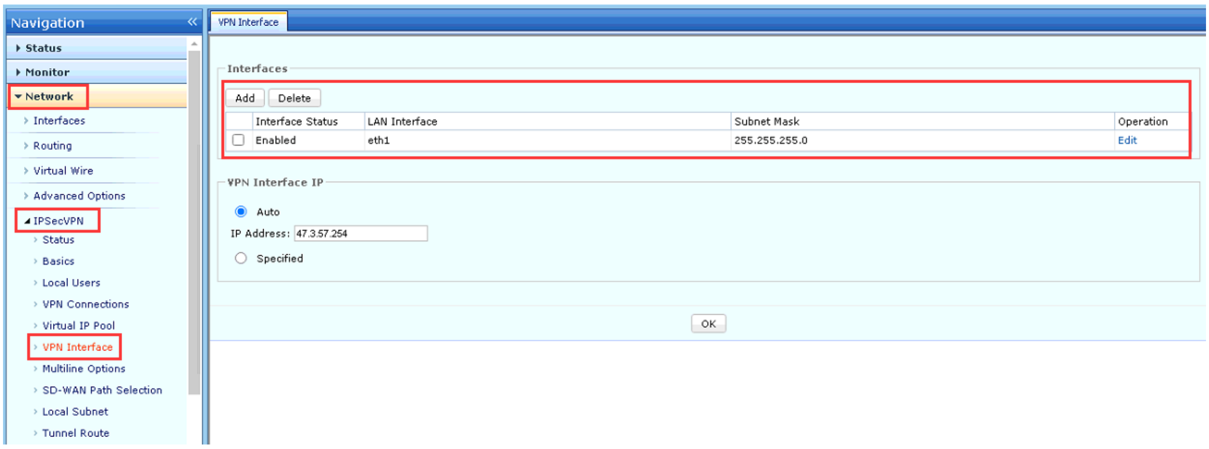


	Priority	Tag	Src Zone	Source Address	Dst Zone	Destination	Service/Application	Schedule	Action	Status	Operation
⊟	1. Default Policy Group(4)										
□	1		vpntun	All	lan	All	any(TCP:0-65535; ...	All week	Allow	✓	
□	2		lan	All	vpntun	All	any(TCP:0-65535; ...	All week	Allow	✓	
□	3		wan lan	All	wan lan	All	any(TCP:0-65535; ...	All week	Allow	✓	
-	4		All	All	All	All	All/All	All week	Deny	✓	

3. Build VPN LAN interface.

   This step used to notice other side that HQ has a local subnet 192.200.19.0/24 (Add

   all NGAF LAN interface to this)



Interfaces

	Interface Status	LAN Interface	Subnet Mask	Operation
□	Enabled	eth1	255.255.255.0	Edit

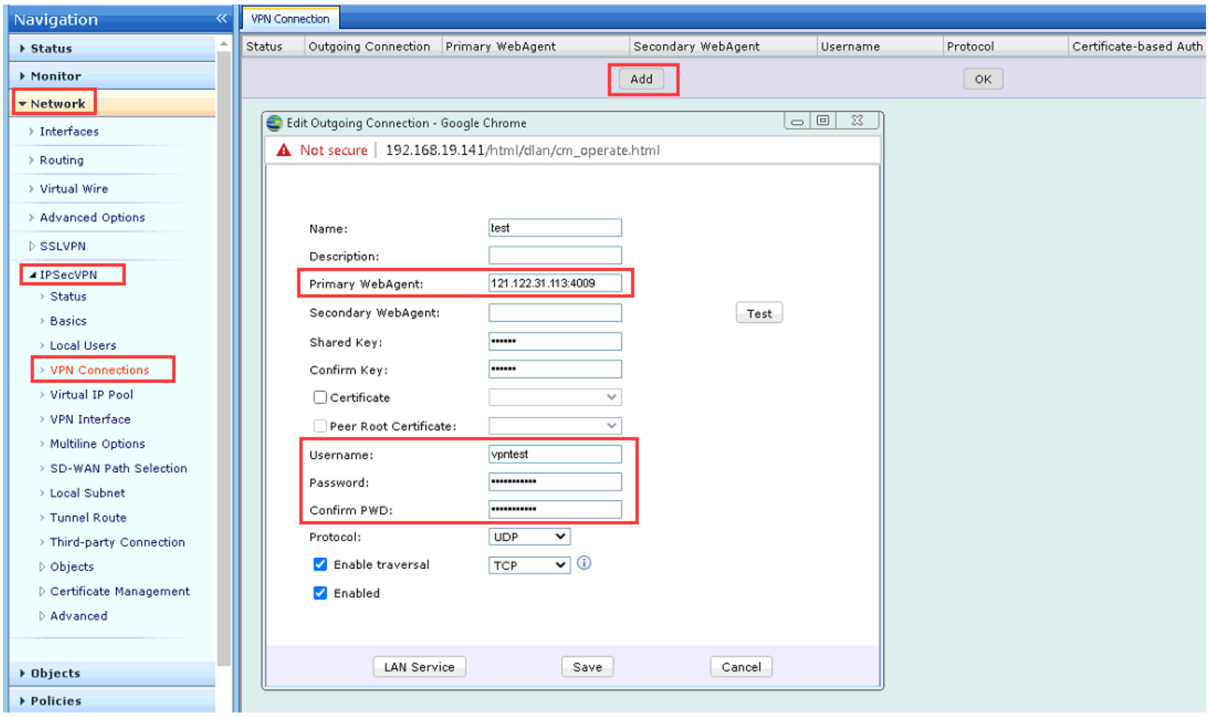
VPN Interface IP

● Auto

IP Address: 47.3.57.254

○ Specified

4. Add VPN connection.



Name: test

Description:

Primary WebAgent: 121.122.31.113:4009

Secondary WebAgent:

Shared Key: ••••••

Confirm Key: ••••••

□ Certificate

□ Peer Root Certificate:

Username: vpntest

Password: •••••••••••

Confirm PWD: •••••••••••

Protocol: UDP

☑ Enable traversal TCP

☑ Enabled

2.1.3 Verify the connection

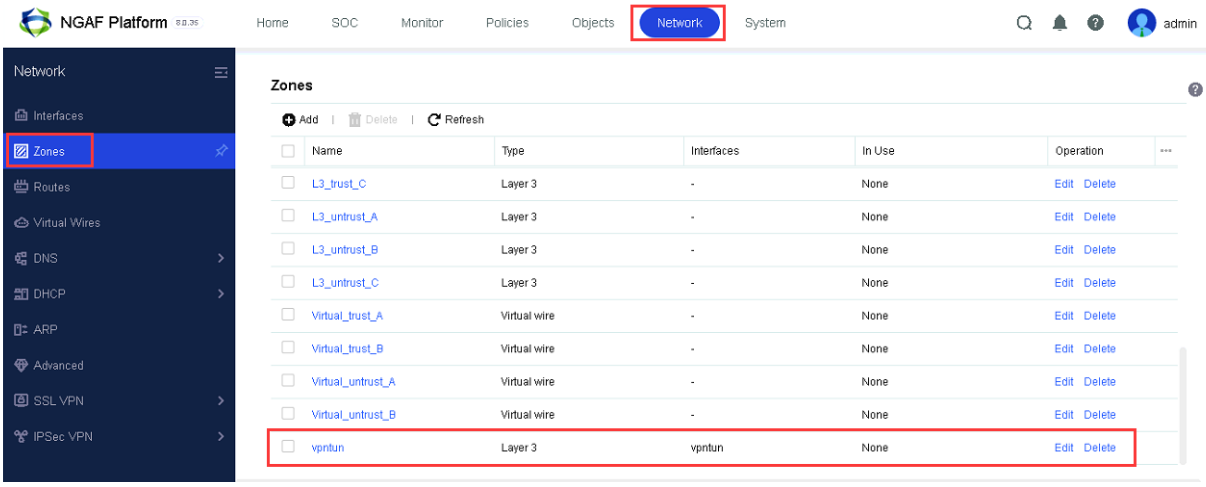
You can verify the connection by navigating to **Network** > **IPSec VPN** > **Status**.

2.2 Version 8.0.35

2.2.1HQ NGAF Configuration

1. Configure interface and zone.

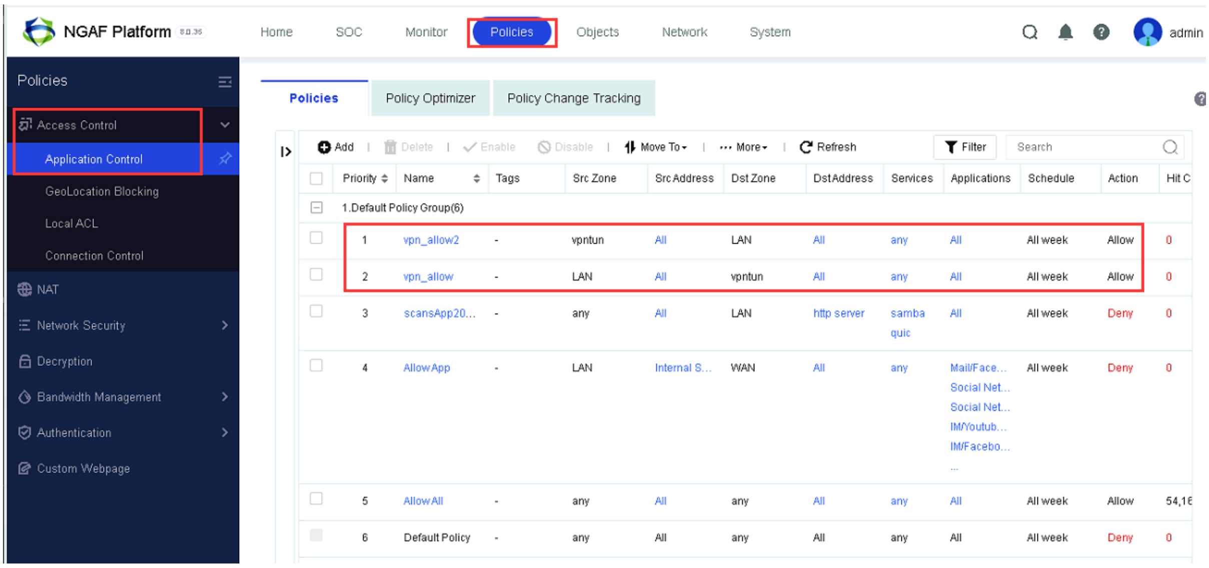
Specially build a zone for VPN, chose vpntun interface.



Zones

Name	Type	Interfaces	In Use	Operation
L3_trust_C	Layer 3	-	None	Edit Delete
L3_untrust_A	Layer 3	-	None	Edit Delete
L3_untrust_B	Layer 3	-	None	Edit Delete
L3_untrust_C	Layer 3	-	None	Edit Delete
Virtual_trust_A	Virtual wire	-	None	Edit Delete
Virtual_trust_B	Virtual wire	-	None	Edit Delete
Virtual_untrust_A	Virtual wire	-	None	Edit Delete
Virtual_untrust_B	Virtual wire	-	None	Edit Delete
vpntun	Layer 3	vpntun	None	Edit Delete

2. Allow traffic in Access control from VPN zone to Server zone and Server zone to VPNzone.

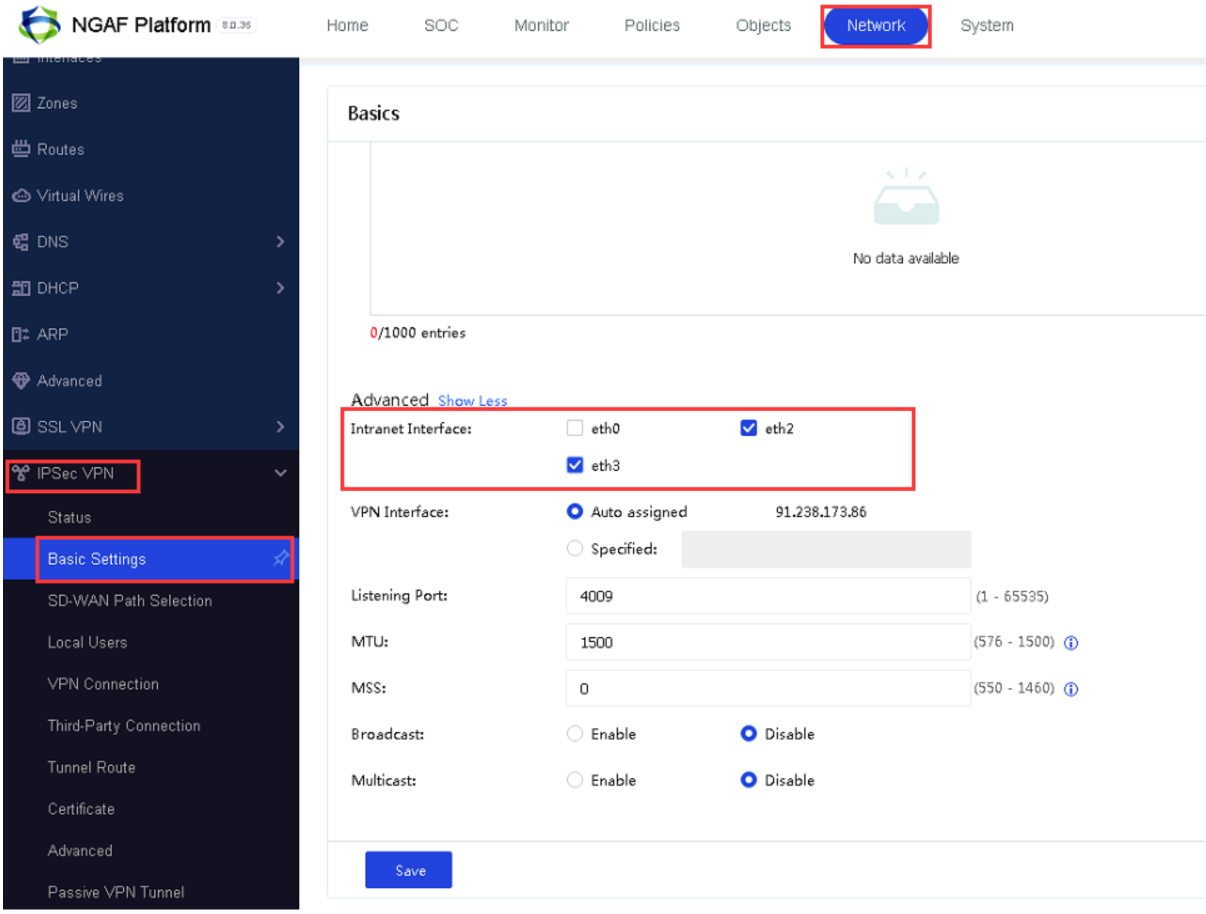


Priority	Name	Tags	Src Zone	Src Address	Dst Zone	DstAddress	Services	Applications	Schedule	Action	Hit C
1.Default Policy Group(6)											
1	vpn_allow2	-	vpntun	All	LAN	All	any	All	All week	Allow	0
2	vpn_allow	-	LAN	All	vpntun	All	any	All	All week	Allow	0
3	scansApp20...	-	any	All	LAN	http server	samba quic	All	All week	Deny	0
4	AllowApp	-	LAN	Internal S...	WAN	All	any	Mail/Face... Social Net... Social Net... IM/Youtub... IM/Facebo... ...	All week	Deny	0
5	AllowAll	-	any	All	any	All	any	All	All week	Allow	54,16
6	Default Policy	-	any	All	any	All	any	All	All week	Deny	0

3. Build VPN interface.

This step used to notice other side that HQ has a subnet 192.200.19.0/24

(Add all NGAF LAN interface to this)



Basics

No data available

0/1000 entries

Advanced Show Less

Intranet Interface: □ eth0 ☑ eth2 ☑ eth3

VPN Interface: ● Auto assigned 91.238.173.86 ○ Specified:

Listening Port: 4009 (1 - 65535)

MTU: 1500 (576 - 1500)

MSS: 0 (550 - 1460)

Broadcast: ○ Enable ● Disable

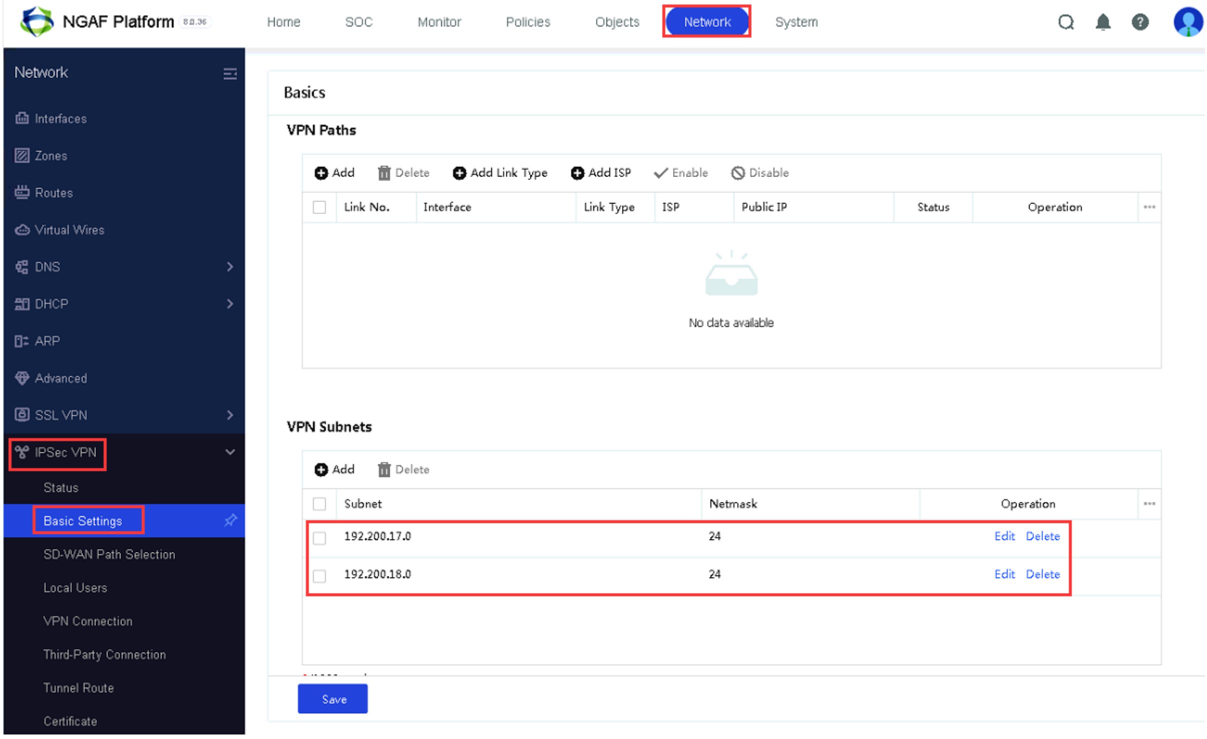
Multicast: ○ Enable ● Disable

Save

4. Add local subnet.

This step used to notice other side that HQ also has 192.200.17.0/24 and 192.200.19.18.0/24 which are not directly configure on NGAF Lan port.

(Don't need to add NGAF interface subnet to local subnet)



Basics

VPN Paths

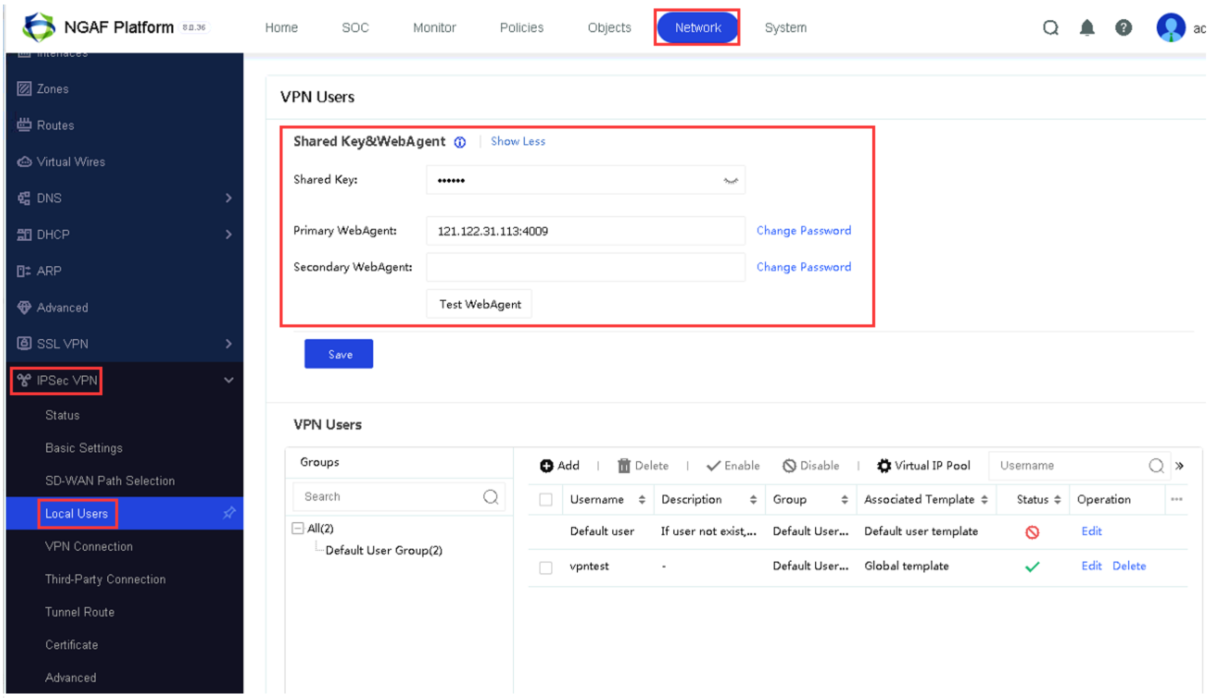
□	Link No.	Interface	Link Type	ISP	Public IP	Status	Operation

No data available

VPN Subnets

□	Subnet	Netmask	Operation
□	192.200.17.0	24	Edit Delete
□	192.200.18.0	24	Edit Delete

5. Set webagent and listening port



VPN Users

Shared Key&WebAgent

Shared Key: ••••••

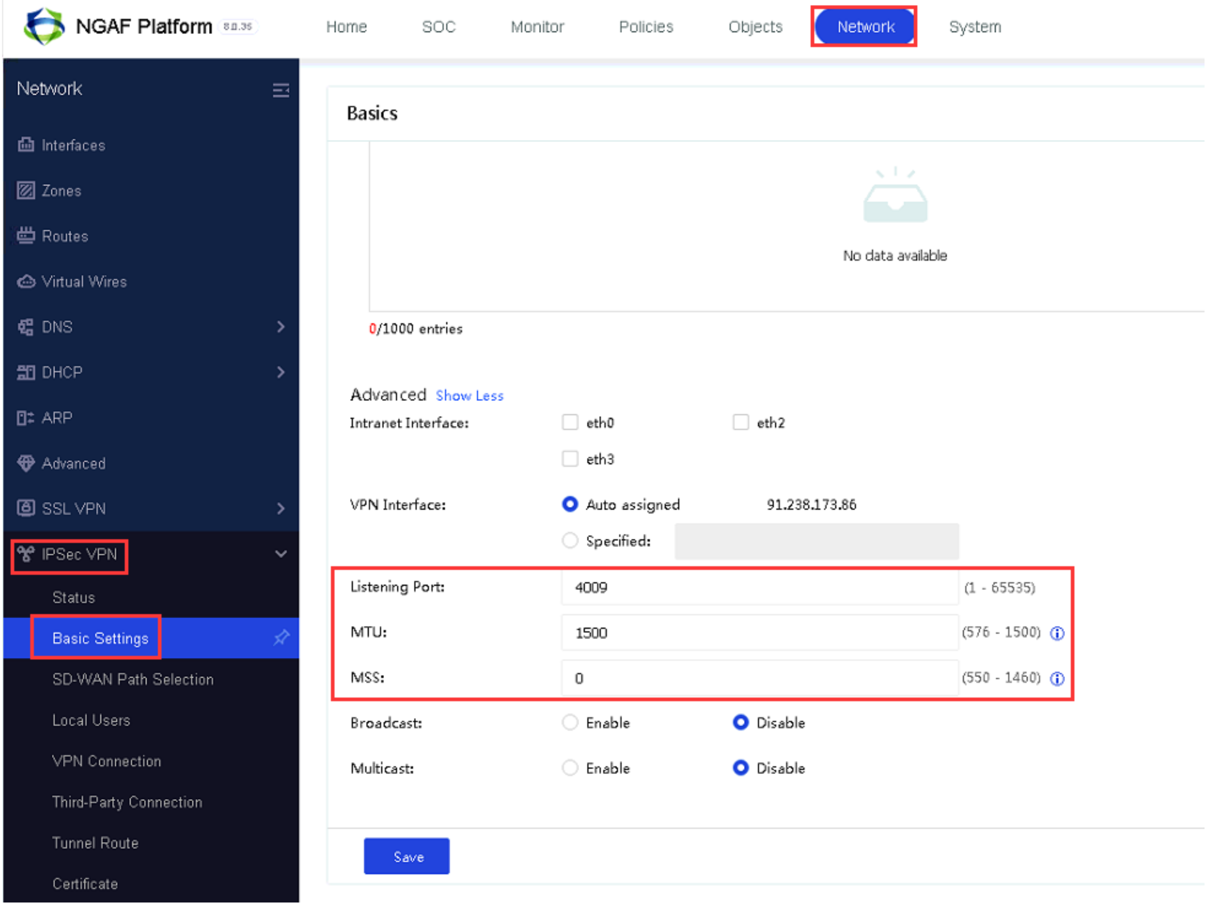
Primary WebAgent: 121.122.31.113:4009

Secondary WebAgent:

VPN Users

Groups: All(2), Default User Group(2)

Username	Description	Group	Associated Template	Status	Operation
Default user	If user not exist,...	Default User...	Default user template	🚫	Edit
vpntest	-	Default User...	Global template	✓	Edit Delete



Basics

No data available

0/1000 entries

Advanced

Intranet Interface: □ eth0 □ eth2 □ eth3

VPN Interface: ● Auto assigned 91.238.173.86 ○ Specified:

Listening Port: 4009 (1 - 65535)

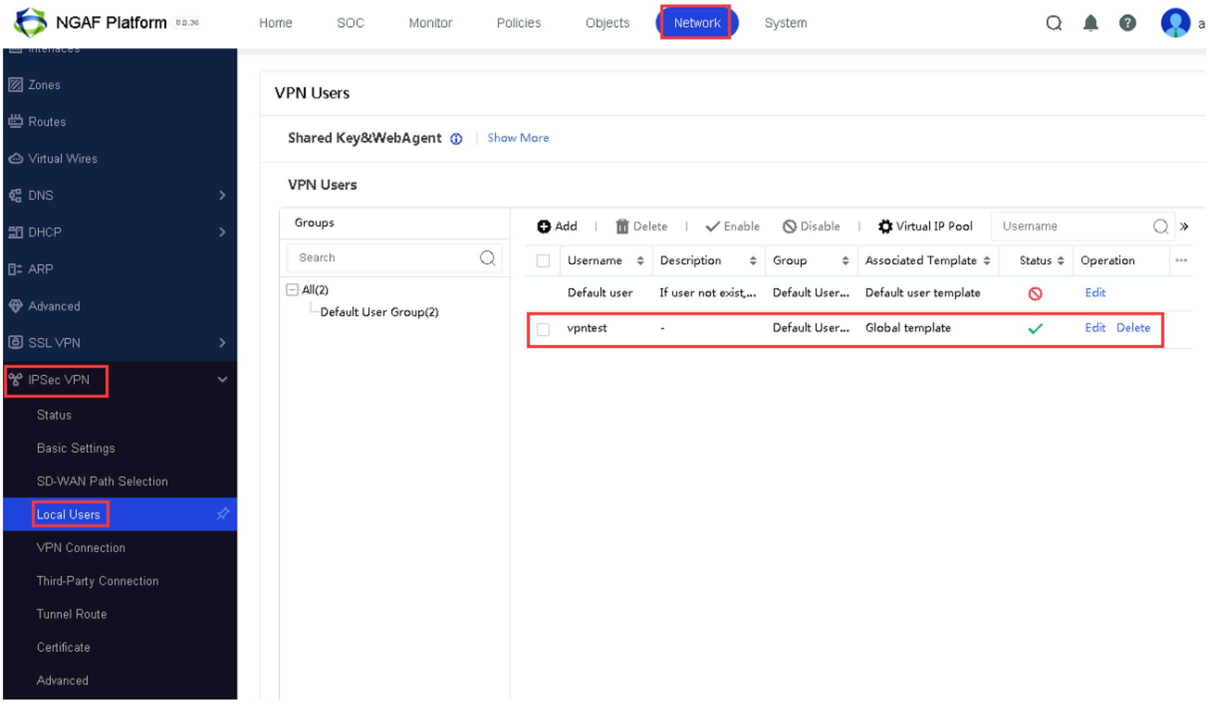
MTU: 1500 (576 - 1500)

MSS: 0 (550 - 1460)

Broadcast: ○ Enable ● Disable

Multicast: ○ Enable ● Disable

6. Create a branch user, user type：branch user



VPN Users

Shared Key&WebAgent ⓘ | Show More

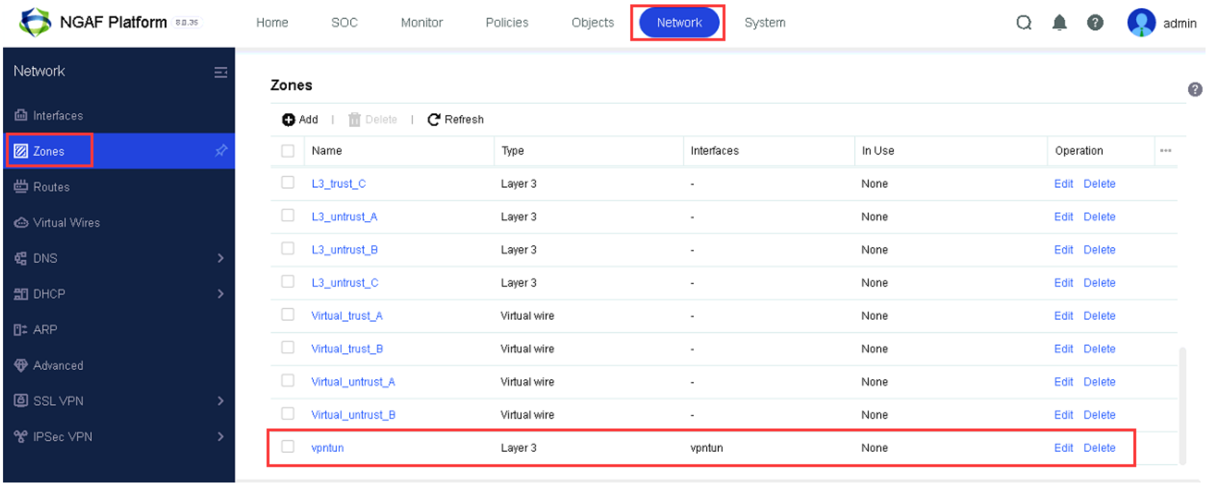
VPN Users

□	Username	Description	Group	Associated Template	Status	Operation
□	Default user	If user not exist,...	Default User...	Default user template	⃠	Edit
□	vpntest	-	Default User...	Global template	✓	Edit Delete

2.2.2 Branch NGAF Configuration

1. Configure interface and zone.

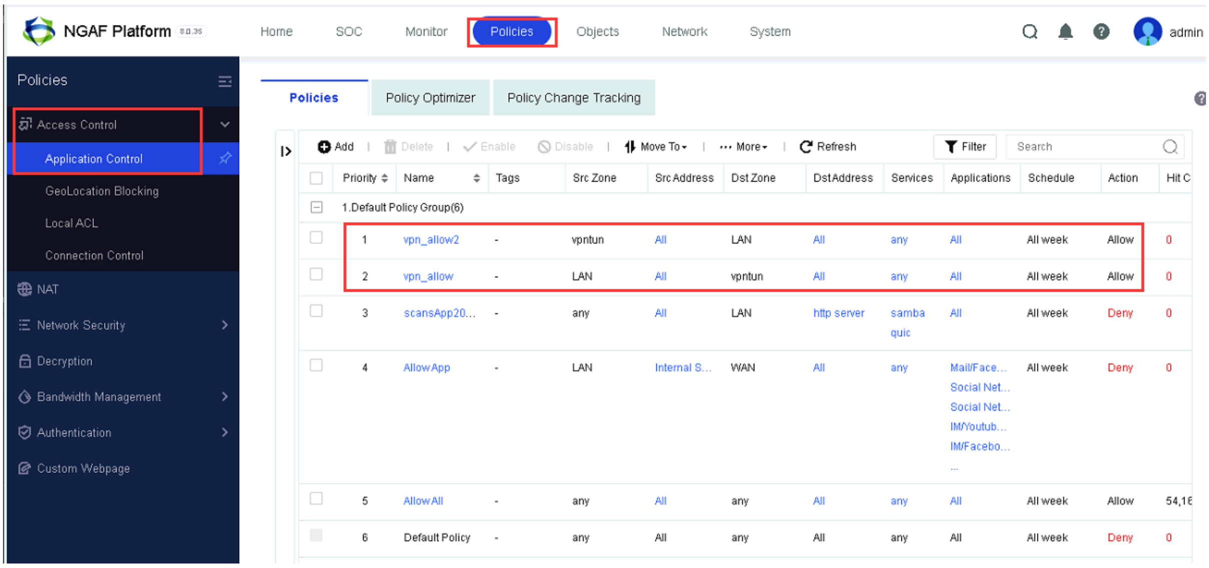
Specially build a zone for VPN, chose vpntun interface.



Zones

Name	Type	Interfaces	In Use	Operation
L3_trust_C	Layer 3	-	None	Edit Delete
L3_untrust_A	Layer 3	-	None	Edit Delete
L3_untrust_B	Layer 3	-	None	Edit Delete
L3_untrust_C	Layer 3	-	None	Edit Delete
Virtual_trust_A	Virtual wire	-	None	Edit Delete
Virtual_trust_B	Virtual wire	-	None	Edit Delete
Virtual_untrust_A	Virtual wire	-	None	Edit Delete
Virtual_untrust_B	Virtual wire	-	None	Edit Delete
vpntun	Layer 3	vpntun	None	Edit Delete

2. Allow traffic in Access control from VPN zone to Server zone and Server zone to VPNzone.

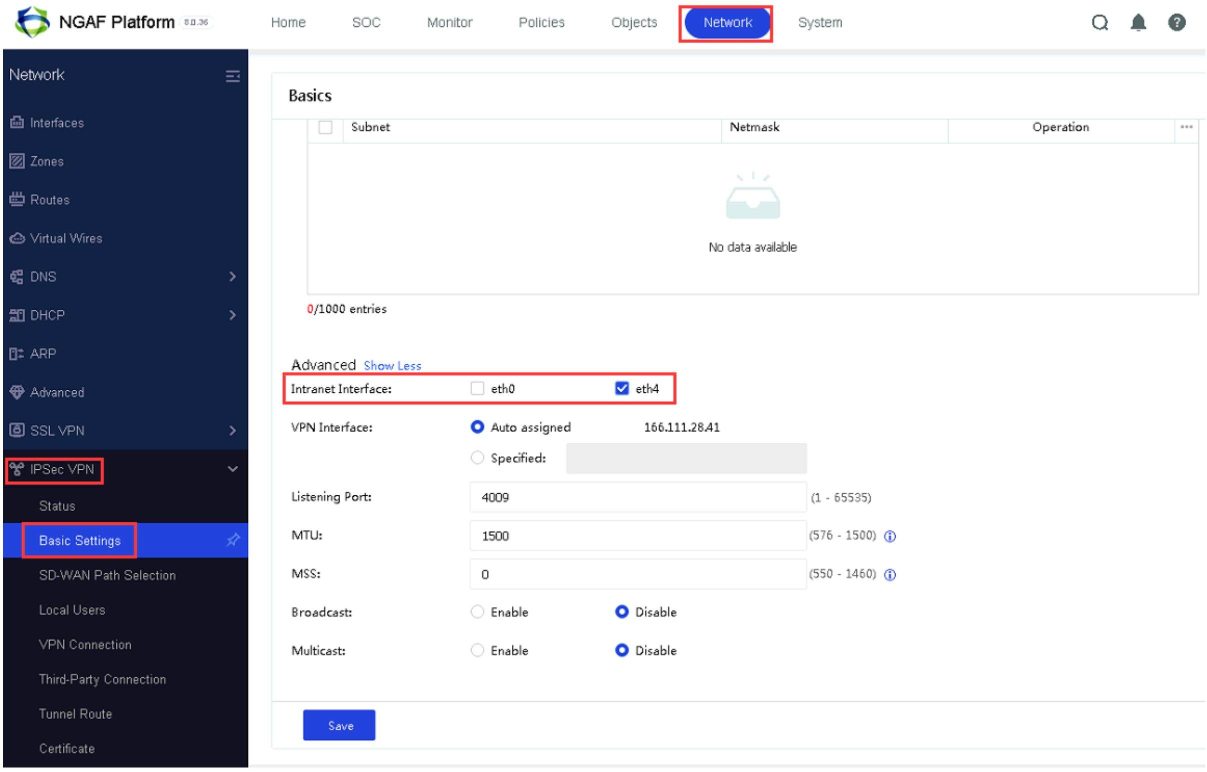


1.Default Policy Group(6)

Priority	Name	Tags	Src Zone	Src Address	Dst Zone	DstAddress	Services	Applications	Schedule	Action	Hit C
1	vpn_allow2	-	vpntun	All	LAN	All	any	All	All week	Allow	0
2	vpn_allow	-	LAN	All	vpntun	All	any	All	All week	Allow	0
3	scansApp20...	-	any	All	LAN	http server	samba quic	All	All week	Deny	0
4	AllowApp	-	LAN	Internal S...	WAN	All	any	Mail/Face... Social Net... Social Net... IM/Youtub... IM/Facebo... ...	All week	Deny	0
5	AllowAll	-	any	All	any	All	any	All	All week	Allow	54,16
6	Default Policy	-	any	All	any	All	any	All	All week	Deny	0

3. Build VPN LAN interface.

This step used to notice other side that HQ has a local subnet 192.200.19.0/24 (Add all NGAF LAN interface to this)



Basics

□	Subnet	Netmask	Operation

No data available

0/1000 entries

Advanced Show Less

Intranet Interface: □ eth0 ☑ eth4

VPN Interface: ● Auto assigned 166.111.28.41 ○ Specified:

Listening Port: 4009 (1 - 65535)

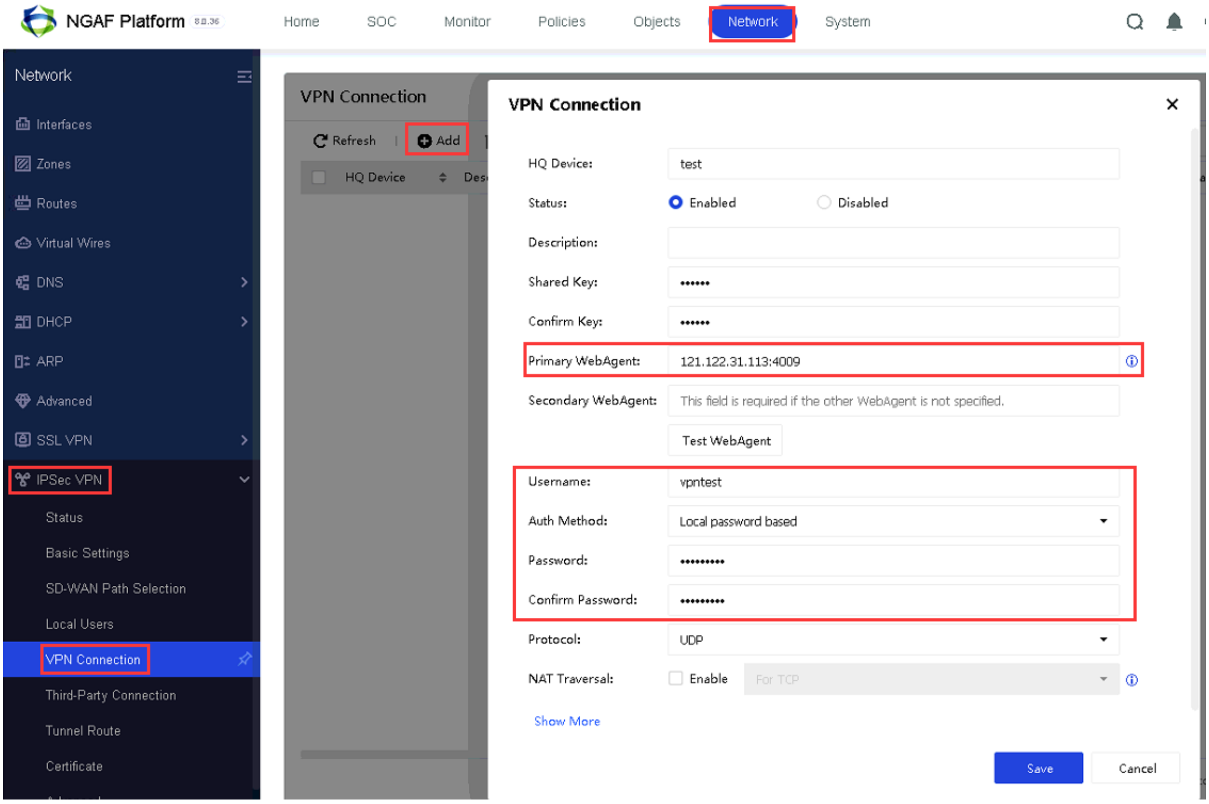
MTU: 1500 (576 - 1500)

MSS: 0 (550 - 1460)

Broadcast: ○ Enable ● Disable

Multicast: ○ Enable ● Disable

4. Add VPN connection.



VPN Connection

HQ Device: test

Status: ● Enabled ○ Disabled

Description:

Shared Key: ••••••

Confirm Key: ••••••

Primary WebAgent: 121.122.31.113:4009

Secondary WebAgent: This field is required if the other WebAgent is not specified.

Test WebAgent

Username: vpntest

Auth Method: Local password based

Password: •••••••••

Confirm Password: •••••••••

Protocol: UDP

NAT Traversal: □ Enable For TCP

Show More

Save Cancel

2.2.3 Verify the connection

You can verify the connection by navigating to **Network** > **IPSec VPN** > **Status**.