



# NGAF

## Sangfor VPN Configuration Guide



---

## Change Log

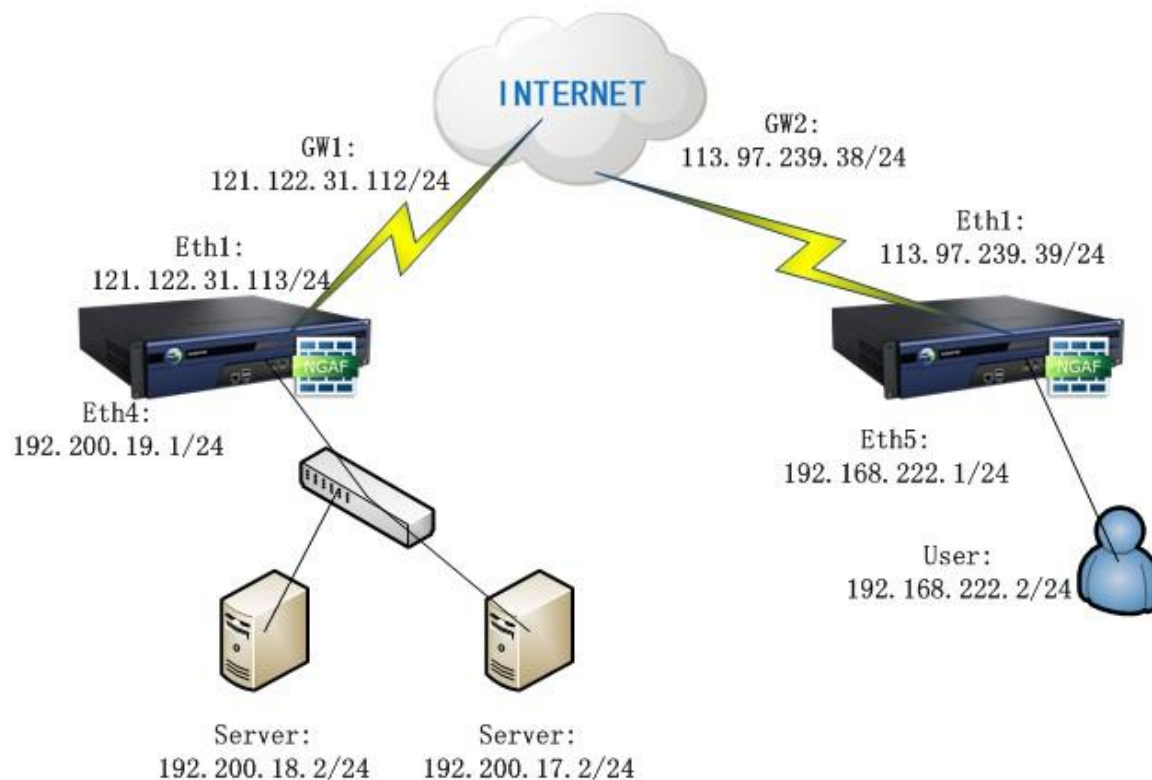
Date	Change Description
Jun 16, 2021	Version 8.0.35 document release.

# Contents

<b>Chapter 1 Network Topology .....</b>	<b>1</b>
<b>Chapter 2 NGAF Configuration .....</b>	<b>2</b>
<b>2.1 Version 8.0.26 .....</b>	<b>2</b>
<b>2.1.1 HQ NGAF Configuration.....</b>	<b>2</b>
<b>2.1.2 Branch NGAF Configuration .....</b>	<b>4</b>
<b>2.1.3 Verify the connection .....</b>	<b>5</b>
<b>2.2 Version 8.0.35 .....</b>	<b>6</b>
<b>2.2.1 HQ NGAF Configuration.....</b>	<b>6</b>
<b>2.2.2 Branch NGAF Configuration .....</b>	<b>11</b>
<b>2.2.3 Verify the connection .....</b>	<b>13</b>

# Chapter 1 Network Topology

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



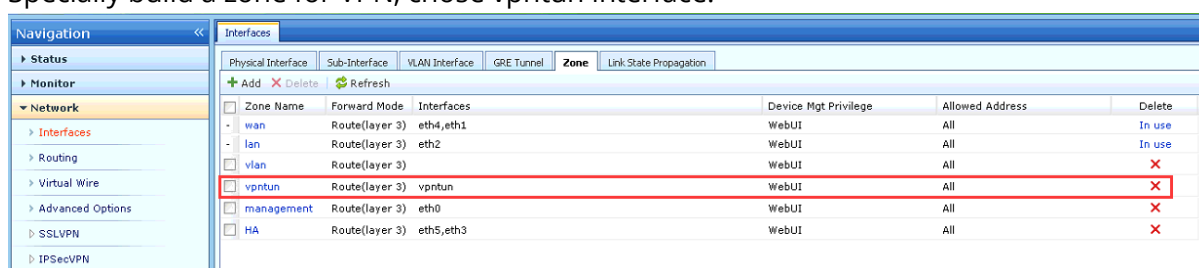
# Chapter 2 NGAF Configuration

## 2.1 Version 8.0.26

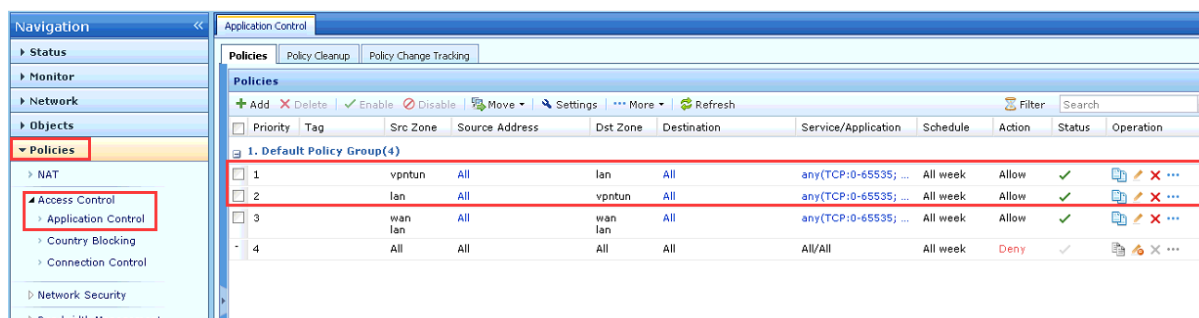
### 2.1.1 HQ NGAF Configuration

1. Configure interface and zone.

Specially build a zone for VPN, chose vpntun interface.



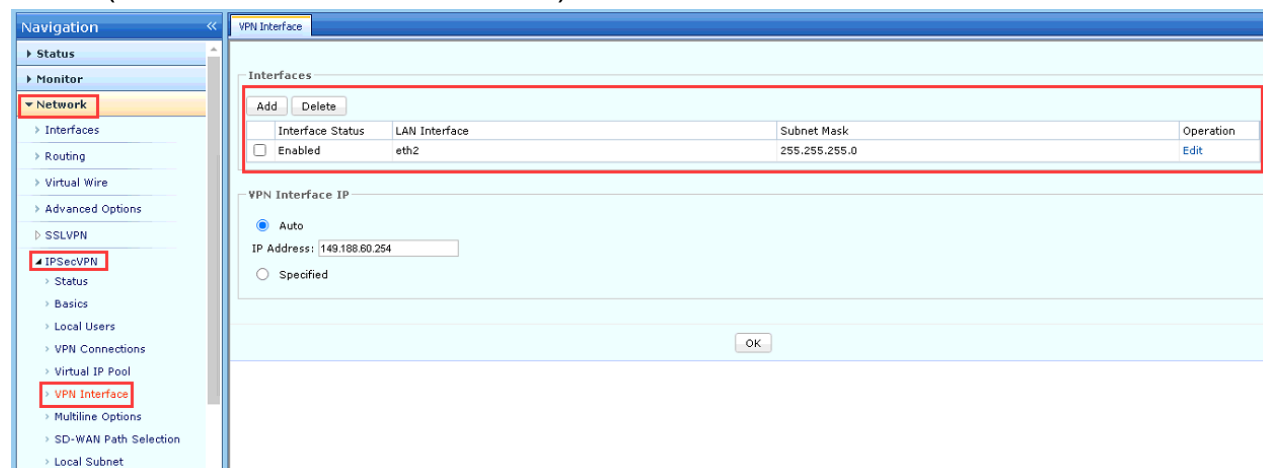
2. Allow traffic in Access control from VPN zone to Server zone and Server zone to VPNzone.



3. Build VPN interface.

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

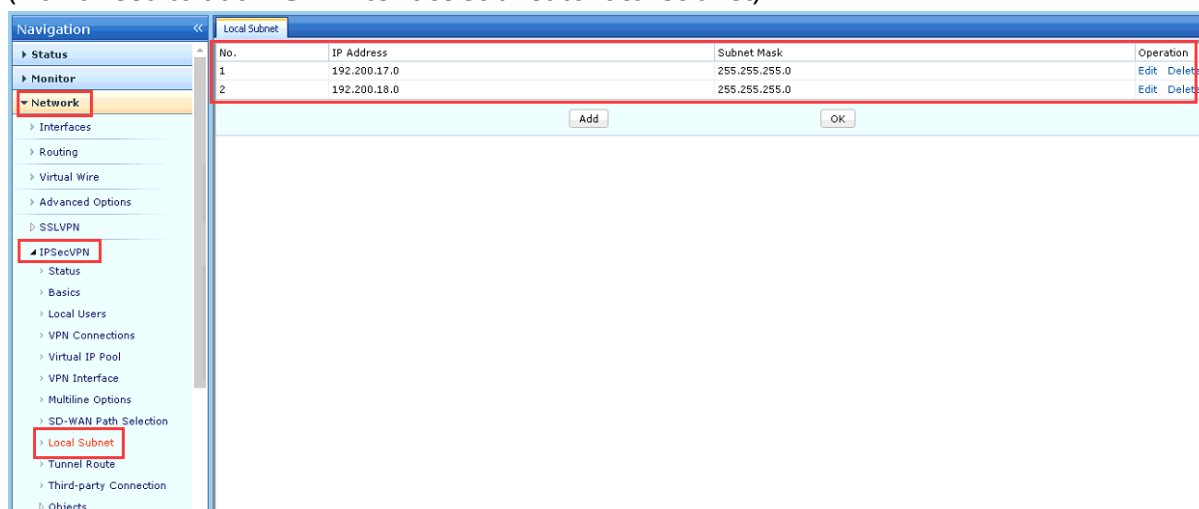
(Add all NGAF LAN interface to this)



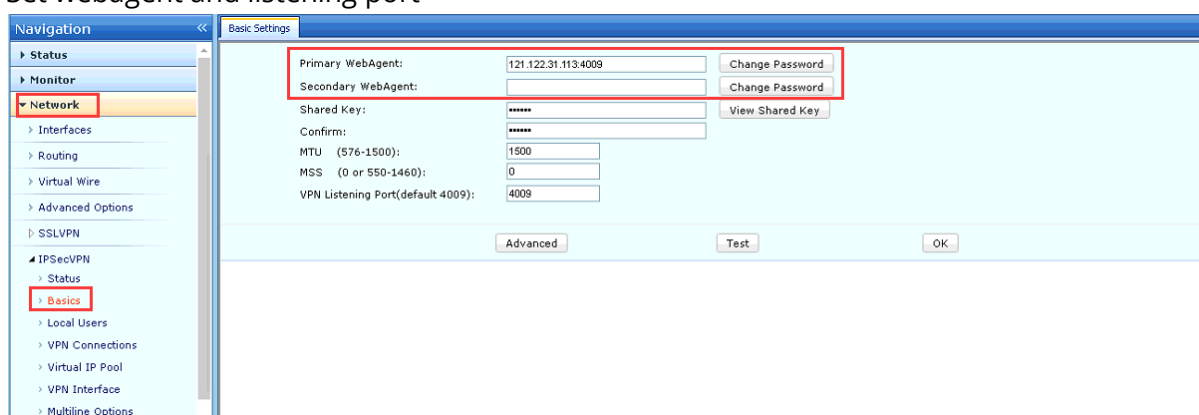
4. Add local subnet.

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.

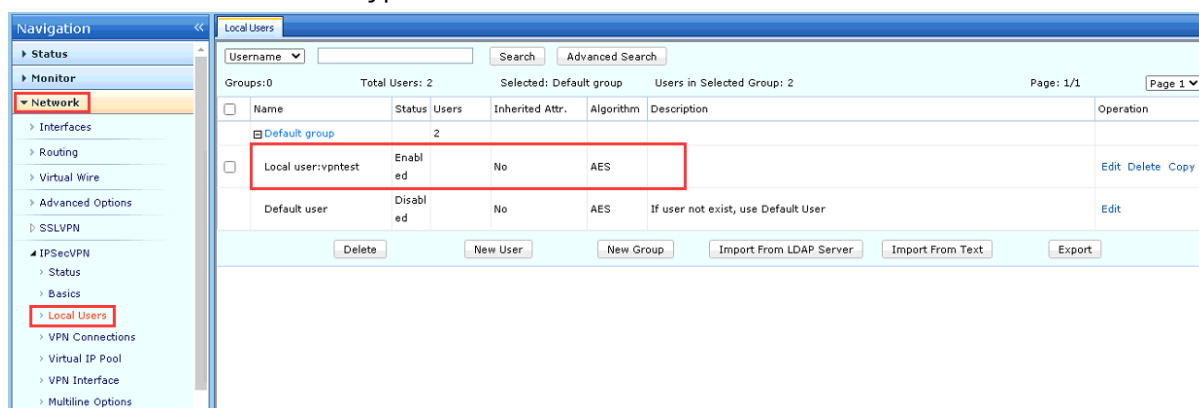
(Don't need to add NGAF interface subnet to local subnet)



## 5. Set webagent and listening port



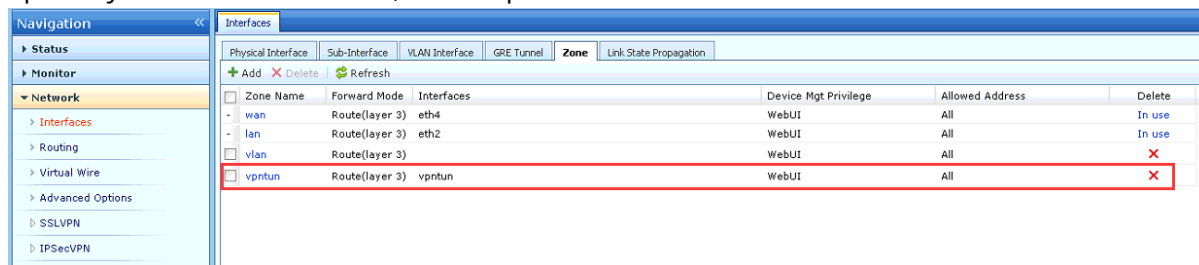
## 6. Create a branch user, user type: branch user



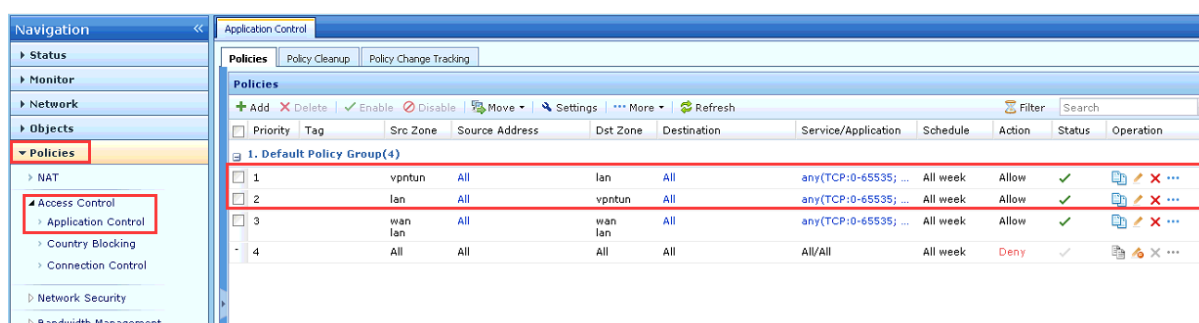
## 2.1.2 Branch NGAF Configuration

1. Configure interface and zone.

Specially build a zone for VPN, chose vpntun interface.

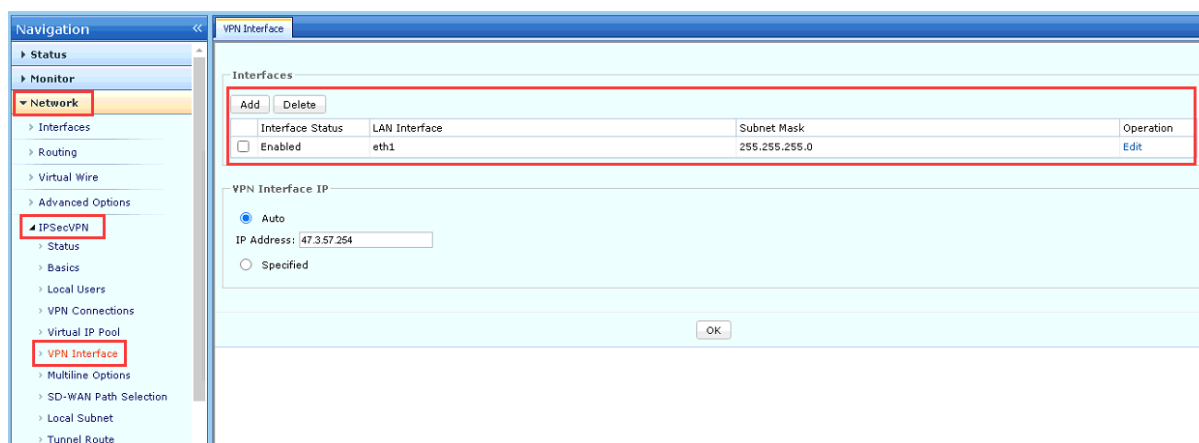


2. Allow traffic in Access control from VPN zone to Server zone and Server zone to VPNzone.

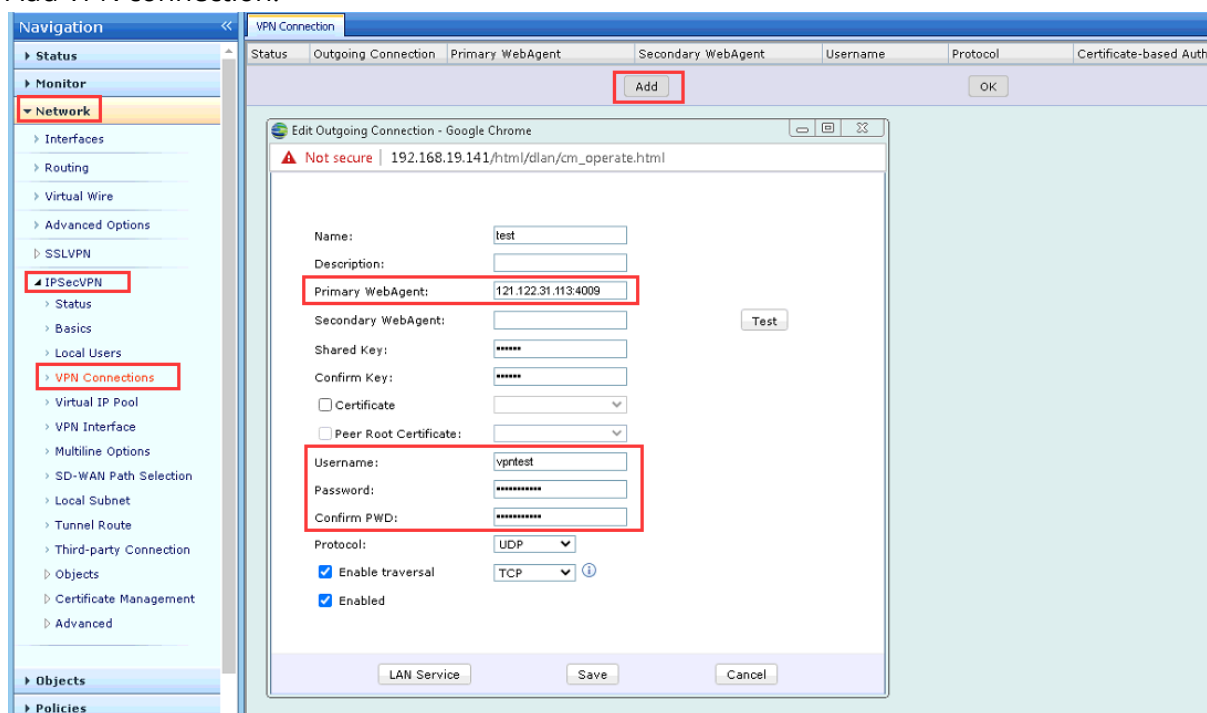


3. Build VPN LAN interface.

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)



#### 4. Add VPN connection.



### 2.1.3 Verify the connection

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



## 2.2 Version 8.0.35

### 2.2.1 HQ 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.

**Policies**

Priority	Name	Tags	Src Zone	Src Address	Dst Zone	Dst Address	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 week	Deny	0
4	AllowApp	-	LAN	Internal S...	WAN	All	any	MailFace... Social Net... Social Net... IM/Youtub... IM/Facebo...	All week	Deny	0
5	AllowAll	-	any	All	any	All	any	All	All week	Allow	54,1E
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)

The screenshot displays the NGAF Platform configuration interface. The top navigation bar includes 'Home', 'SOC', 'Monitor', 'Policies', 'Objects', 'Network' (highlighted with a red box), and 'System'. The left sidebar shows the 'IPSec VPN' menu item highlighted with a red box, and its sub-menu 'Basic Settings' is also highlighted with a red box. The main content area is titled 'Basics' and shows a 'No data available' message. Below this, the 'Advanced' section is expanded, showing the 'Intranet Interface' settings. The 'Intranet Interface' section has a red box around it, containing checkboxes for 'eth0', 'eth2', and 'eth3'. 'eth2' and 'eth3' are checked. The 'VPN Interface' section shows 'Auto assigned' selected, with the IP address '91.238.173.86'. Other settings include 'Listening Port' (4009), 'MTU' (1500), 'MSS' (0), 'Broadcast' (Disable), and 'Multicast' (Disable). A 'Save' button is at the bottom.

NGAF Platform 6.0.35

Home SOC Monitor Policies Objects **Network** System

Interfaces

- Zones
- Routes
- Virtual Wires
- DNS
- DHCP
- ARP
- Advanced
- SSL VPN
- IPSec VPN**
- Status
- Basic Settings**
- SD-WAN Path Selection
- Local Users
- VPN Connection
- Third-Party Connection
- Tunnel Route
- Certificate
- Advanced
- Passive VPN Tunnel

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

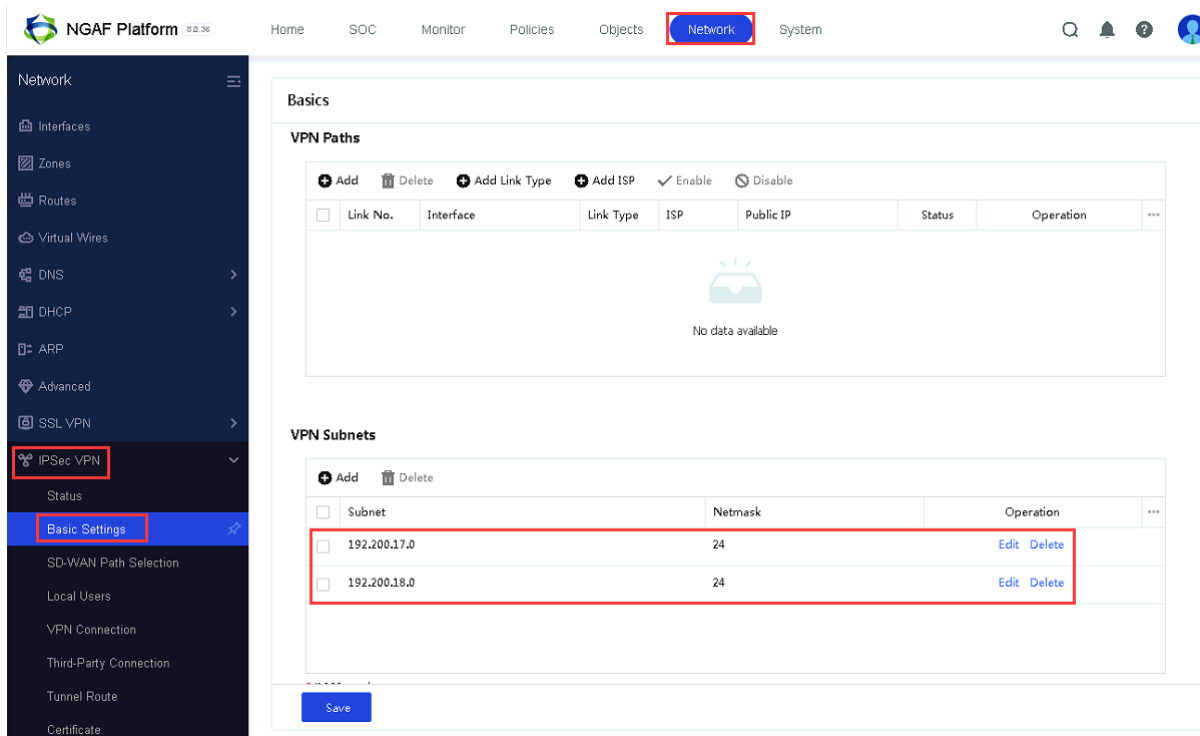
Multicast: ☐ Enable ☒ Disable

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)



The screenshot displays the NGAF Platform interface. The left sidebar shows the 'Network' menu with 'IPSec VPN' and 'Basic Settings' highlighted. The main panel shows the 'VPN Subnets' table with two entries: 192.200.17.0/24 and 192.200.18.0/24. The 'VPN Paths' section above it is empty, showing 'No data available'.

Link No.	Interface	Link Type	ISP	Public IP	Status	Operation
No data available						

Subnet	Netmask	Operation
192.200.17.0	24	Edit Delete
192.200.18.0	24	Edit Delete

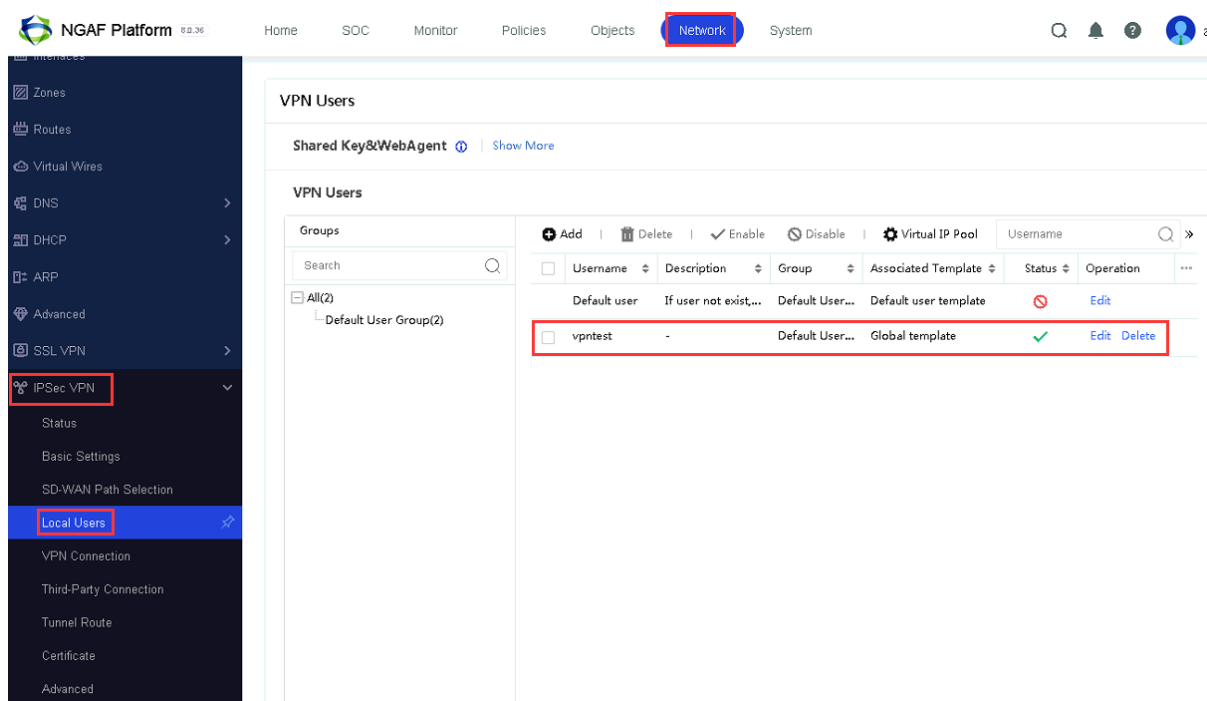
Save

## 5. Set webagent and listening port

The first screenshot shows the NGAF Platform interface with the 'Network' tab selected. In the left sidebar, 'IPSec VPN' is highlighted, and 'Local Users' is selected under it. The main content area shows the 'VPN Users' configuration page. The 'Shared Key' and 'WebAgent' section is highlighted with a red box. It contains fields for 'Shared Key', 'Primary WebAgent' (121.122.31.113:4009), 'Secondary WebAgent', and a 'Test WebAgent' button. There are also 'Change Password' links for the Primary and Secondary WebAgent fields. A 'Save' button is at the bottom.

The second screenshot shows the NGAF Platform interface with the 'Network' tab selected. In the left sidebar, 'IPSec VPN' is highlighted, and 'Basic Settings' is selected under it. The main content area shows the 'Basics' configuration page. The 'Advanced' section is expanded, and the 'Listening Port' section is highlighted with a red box. It contains fields for 'Listening Port' (4009), 'MTU' (1500), and 'MSS' (0). There are also radio buttons for 'Intranet Interface' (eth0, eth2, eth3) and 'VPN Interface' (Auto assigned, Specified). There are also radio buttons for 'Broadcast' and 'Multicast' (Enable, Disable). A 'Save' button is at the bottom.

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



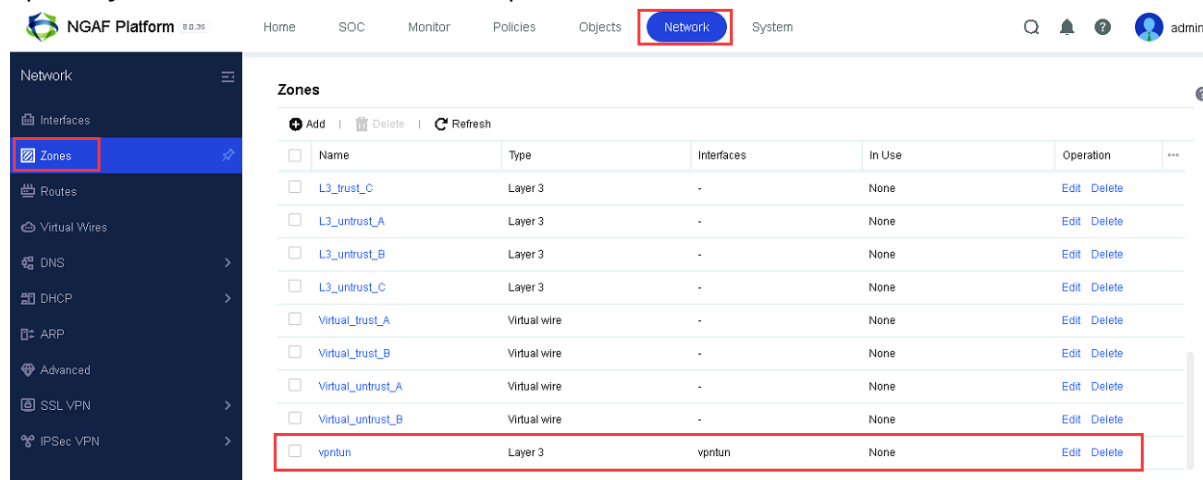
The screenshot displays the NGAF Platform interface. The top navigation bar includes 'Home', 'SOC', 'Monitor', 'Policies', 'Objects', 'Network', and 'System'. The left sidebar shows the configuration menu with 'IPSec VPN' and 'Local Users' highlighted. The main content area shows the 'VPN Users' configuration page. The 'VPN Users' table is displayed with the following data:

Groups	Username	Description	Group	Associated Template	Status	Operation
All(2)	Default user	If user not exist...	Default User...	Default user template	✖	Edit
Default User Group(2)	vpntest	-	Default User...	Global template	✔	Edit Delete

## 2.2.2 Branch NGAF Configuration

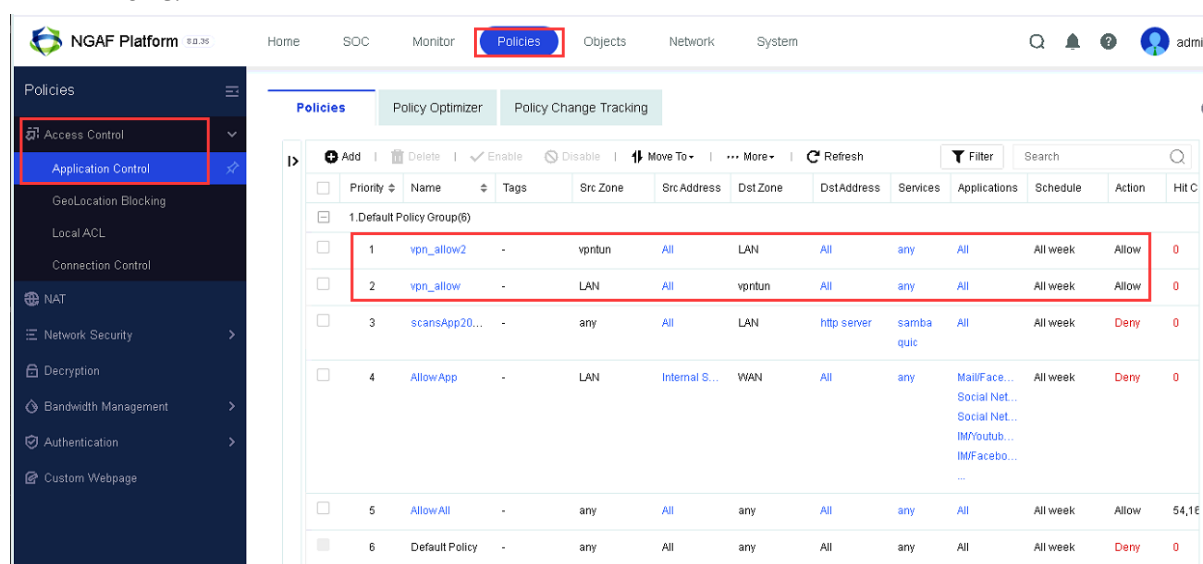
1. Configure interface and zone.

Specially build a zone for VPN, chose vpntun interface.



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.



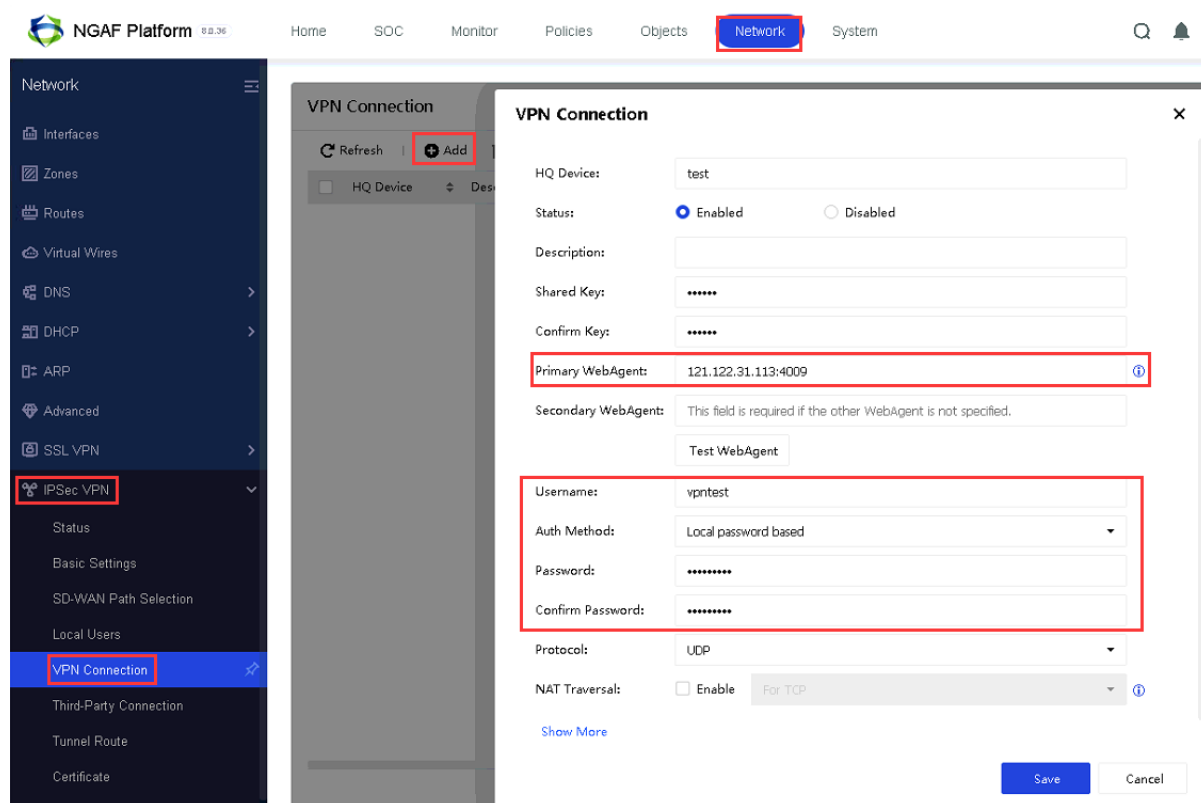
Priority	Name	Tags	Src Zone	Src Address	Dst Zone	Dst Address	Services	Applications	Schedule	Action	Hit C
1	vpn_allow2	-	vpntun	All	LAN	All	any	All	All week	Allow	0
2	vpn_allow	-	LAN	All	vpntun	All	any	All	All week	Allow	0
3	scansApp20...	-	any	All	LAN	http server	samba	quic	All week	Deny	0
4	AllowApp	-	LAN	Internal S...	WAN	All	any	MailFace... Social Net... Social Net... IM/YouTub... IM/Facebo...	All week	Deny	0
5	AllowAll	-	any	All	any	All	any	All	All week	Allow	54,1E
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)

The screenshot displays the NGAF Platform configuration interface. The top navigation bar includes 'Home', 'SOC', 'Monitor', 'Policies', 'Objects', 'Network' (highlighted with a red box), and 'System'. The left sidebar shows the 'Network' menu with 'IPSec VPN' (highlighted with a red box) and 'Basic Settings' (highlighted with a blue box). The main content area is titled 'Basics' and features a table with columns 'Subnet', 'Netmask', and 'Operation'. Below the table, it indicates '0/1000 entries'. The 'Advanced' section is expanded, showing 'Intranet Interface' with 'eth4' selected (highlighted with a red box). Other settings include 'VPN Interface' set to 'Auto assigned' with IP '166.111.28.41', 'Listening Port' set to '4009', 'MTU' set to '1500', 'MSS' set to '0', and both 'Broadcast' and 'Multicast' set to 'Disable'. A 'Save' button is located at the bottom of the configuration area.

#### 4. Add VPN connection.



### 2.2.3 Verify the connection

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





Copyright © SANGFOR Technologies Inc. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of SANGFOR Technologies Inc.

SANGFOR is the trademark of SANGFOR Technologies Inc. All other trademarks and trade names mentioned in this document are the property of their respective holders. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

The information in this document is subject to change without notice.

To obtain the latest version, contact the international service center of SANGFOR Technologies Inc