



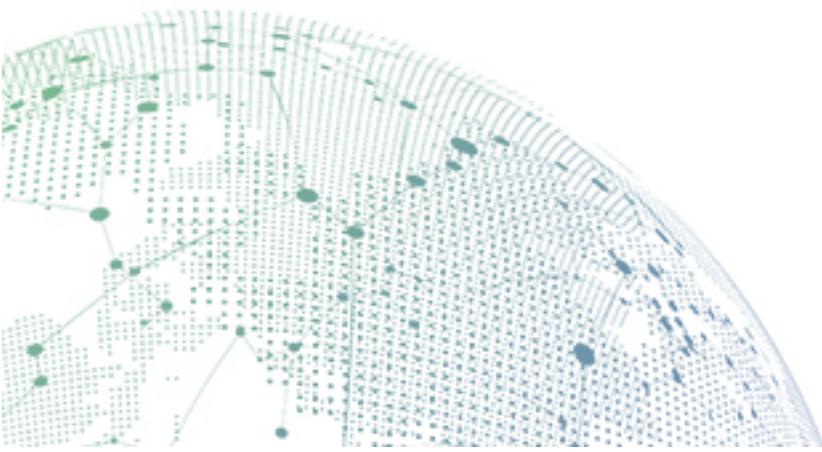
SANGFOR



NGAF

Sangfor VPN Configuration Guide

Version 8.0.5



Change Log

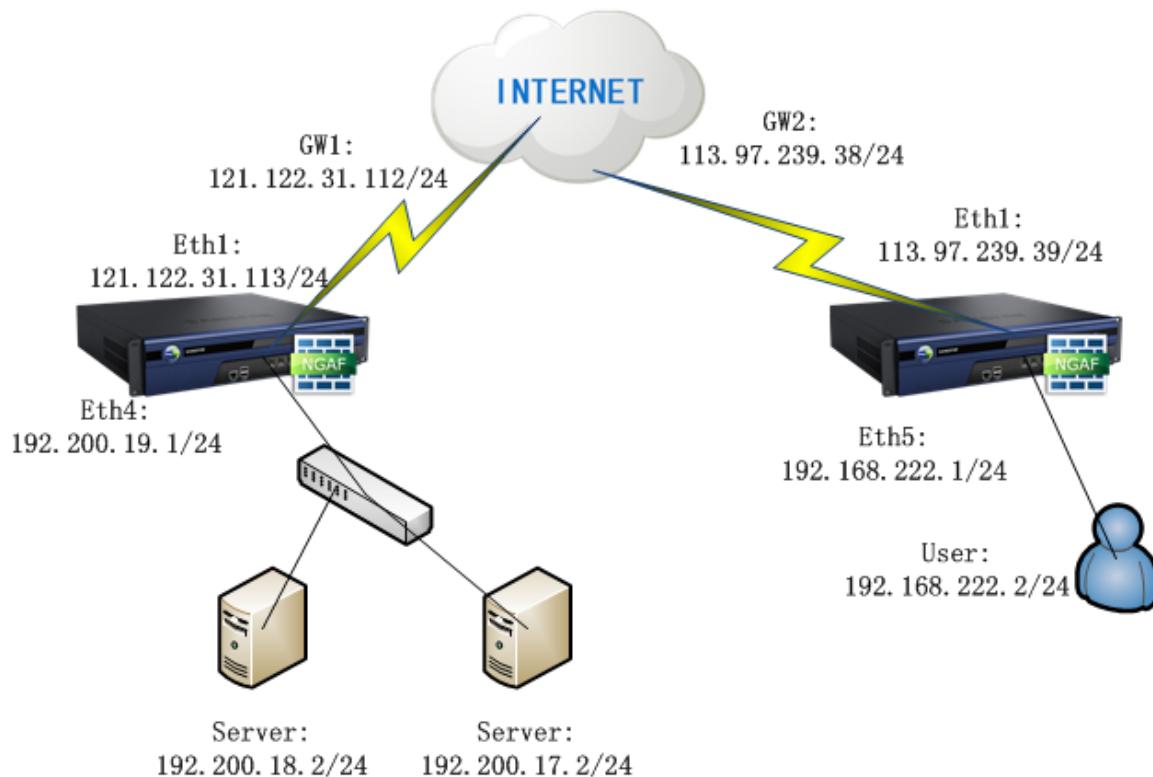
Date	Change Description
Oct 22, 2018	Version 8.0.5 document release.

CONTENT

Chapter 1 Background	1
1 Network Topology.....	1
2 NGAF Configuration.....	1
2.1 HQ NGAF Configuration	1
2.2 Branch NGAF Configuration	4
3 Verify the connection	5

Chapter 1 Network Topology

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



Chapter 2 NGAF Configuration

2.1 HQ NGAF Configuration

1. Configure interface and zone.

Specially build a zone for VPN, chose vpntun interface.

Interfaces							
		Physical Interface	Sub-Interface	VLAN Interface	Aggregate Interface	GRE Tunnel	
		Zone					
+ Add		- Delete	Refresh				
Zone Name	Forward Mode	Interfaces	Device Mgt Privilege	Allowed Address	Delete		
- LAN	Bridge(layer 2)	eth4			In use		
- WAN	Bridge(layer 2)	eth5			In use		
- Mgmt	Route(layer 3)	veth.1,veth.4	WebUI,ssh	All	In use		
- vpntun	Route(layer 3)	vpntun	WebUI	All	In use		

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

Priority	Name	Group	Src Zone	Source Network Obj...	Dst Zone	Destination Netw...	Service/Application	Schedule	Time Updated	Action
1	VPN_Allow2	Default group	LAN Mgmt	All	vpntun	All	Predefined Service/any	All week	10-25 14:35:35	Allow
2	VPN_Allow	Default group	vpntun	All	LAN Mgmt	All	Predefined Service/any	All week	10-25 14:35:46	Allow

3. Build VPN 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)

Interface Status	LAN Interface	Subnet Mask	Operation
Enabled	eth2	255.255.255.0	Edit

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

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

The screenshot shows the NGAF configuration interface with the following navigation path:

- Navigation: Status, Network (highlighted), Interfaces, Routing, Virtual Wire, Advanced Options, Optical Bypass Module, NAT, SSLVPN, IPSecVPN (highlighted), Status, Certificate Management, Basics, Local Users, VPN Connections, Virtual IP Pool, Multiline Options, VPN Interface, Multiline Policy, Local Subnet (highlighted).
- Local Subnet tab selected.
- Table: 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
- Buttons: Add, OK.

5. Set webagent and listening port

The screenshot shows the NGAF configuration interface with the following navigation path:

- Navigation: Status, Network, Security Databases, VPN (highlighted), IPSec VPN, Status, Basics (highlighted), Local Users, VPN Connections, Virtual IP Pool, VPN WAN Interface, VPN LAN Interface.
- Basic Settings tab selected.
- Form fields:
 - Primary WebAgent: webagent.sangfor.net.cn/webagent/vpn
 - Secondary WebAgent: 121.122.31.113:4009
 - MTU (224-2000): 1500
 - Min Compression Value(99-5000): 100
 - VPN Listening Port(default 4009): 4009
 - MSS Change(UDP only): Allow
 - Internet Connection: Directly Indirectly
- Buttons: Advanced, Test, Save and Apply.

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

Name	Status	Users	Type	Inherited Attr.	Algorithm	Virtual IP	My Network
Default group	Enabled	3	Branch user	No	AES	Disabled	
Local user vpntest	Enabled		Branch user	No	AES	Disabled	
Local user:Guest	Disabled		Branch user	No	AES	Disabled	
Default user	Disabled		Branch user	No	AES	Disabled	

2.2 Branch NGAF Configuration

1. Configure interface and zone.

Specially build a zone for VPN, chose vpntun interface.

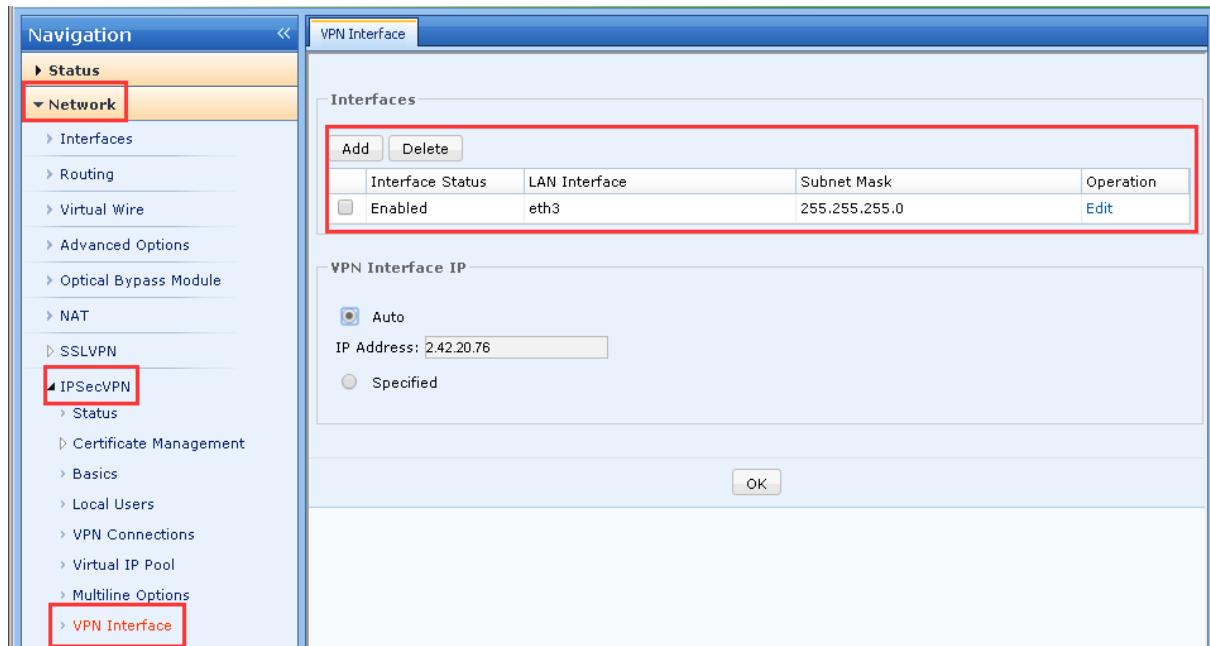
Zone Name	Forward Mode	Interfaces	Device Mgt Privilege	Allowed Address	Delete
LAN	Bridge(layer 2)	eth4			In use
WAN	Bridge(layer 2)	eth5			In use
Mgmt	Route(layer 3)	veth.1,veth.4	WebUI,ssh	All	In use
vpntun	Route(layer 3)	vpntun	WebUI	All	In use

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

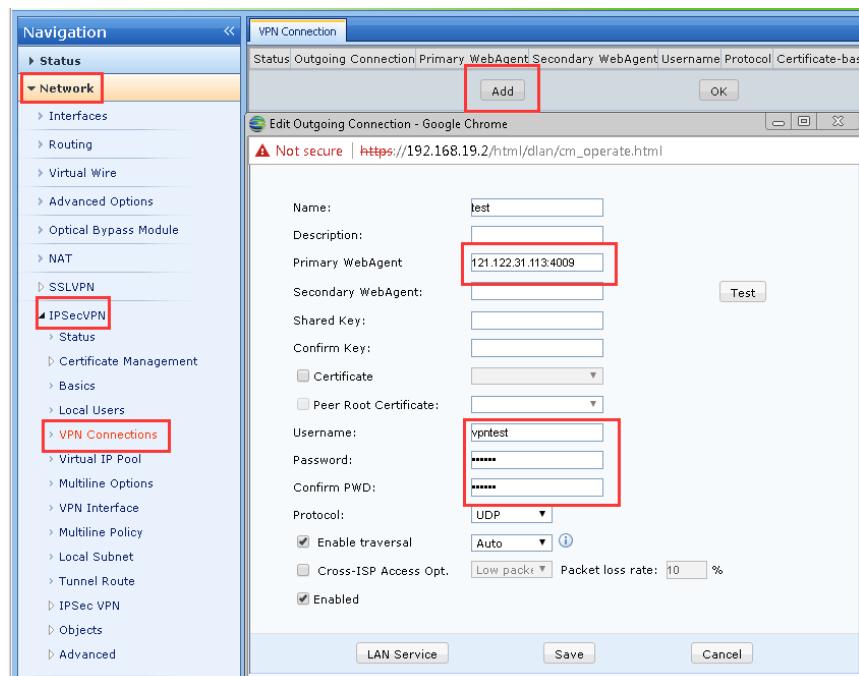
Priority	Name	Group	Src Zone	Source Network Obj...	Dst Zone	Destination Netw...	Service/Application	Schedule	Time Updated	Action
1	VPN_Allow2	Default group	LAN Mgmt	All	vpntun	All	Predefined Service/any	All week	10-25 14:35:35	Allow
2	VPN_Allow	Default group	vpntun	All	LAN Mgmt	All	Predefined Service/any	All week	10-25 14:35:46	Allow

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.



3 Verify the connection

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



SANGFOR

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