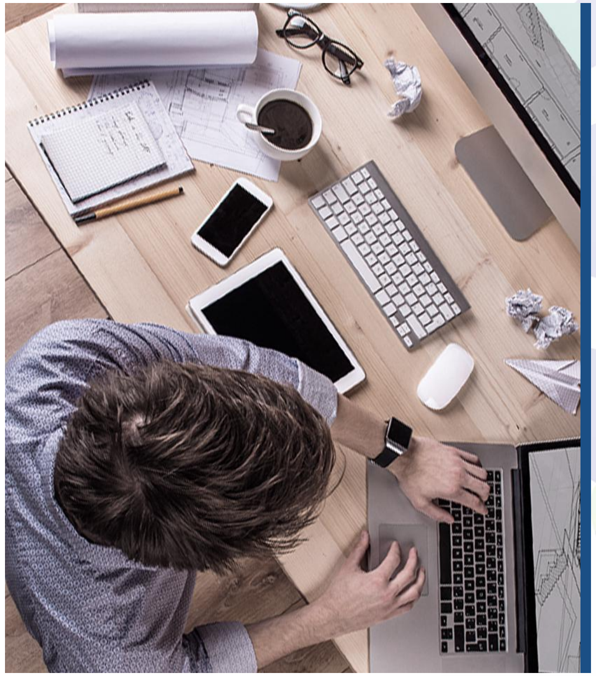
Sangfor NGAF v8.0.6 Associate

VPN

SANGFOR



1 IPSec VPN

2 Sangfor VPN

3 SSL VPN

1. IPSec VPN

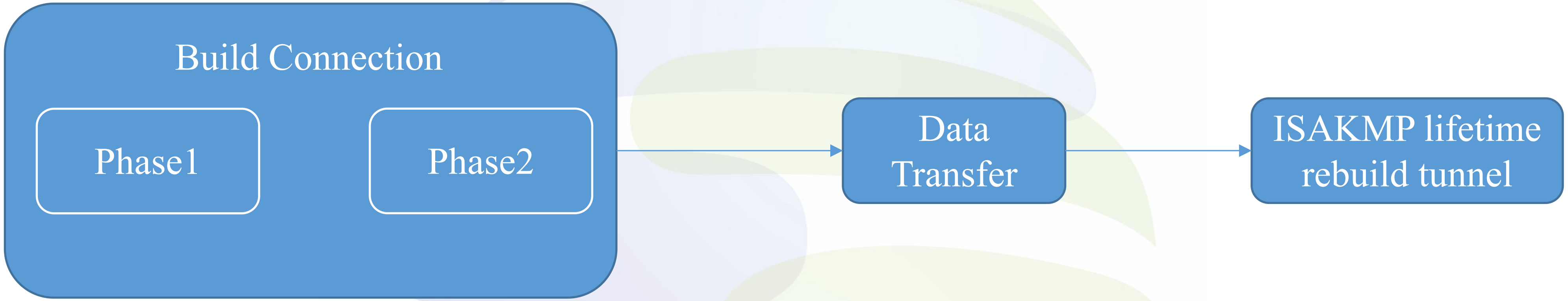
IPSEC VPN

A virtual private network (VPN) extends a private network across a public network, and enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network.

Internet Protocol Security (IPsec) is a network protocol suite that authenticates and encrypts the packets of data sent over a network.
IPsec supports network-level peer authentication, **data-origin authentication**, **data integrity**, **data confidentiality (encryption)**, and replay protection.

All Sangfor security products support the IPsec VPN.

IPSEC VPN



Build Connection

Phase1

Phase2

Data Transfer

ISAKMP lifetime rebuild tunnel

Phase1:

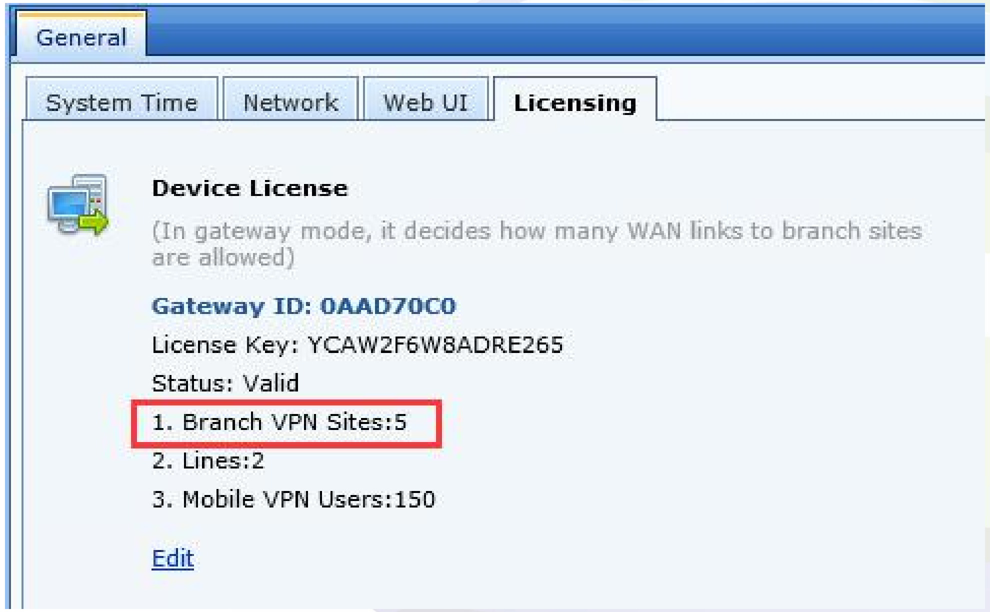
1. Mode: Main/Aggressive
2. SA exchange: Authentication algorithm/Encryption algorithm/DH Group/ISAKMP life time
3. Exchange Pre-shared key
4. Exchange and Verify ID
5. Other: NAT/DPD

Phase2:

1. Protocol :AH/ESP
2. PFS
3. Encryption : DES/3DES/AES128
   Hash:MD5/SHA
4. SA lifetime
5. Local subnet and peer subnet

IPSEC VPN

1. NGAF must have Branch VPN Sites license to establish a IPsec VPN:



Device License

(In gateway mode, it decides how many WAN links to branch sites are allowed)

Gateway ID: 0AAD70C0

License Key: YCAW2F6W8ADRE265

Status: Valid

1. Branch VPN Sites:5

2. Lines:2

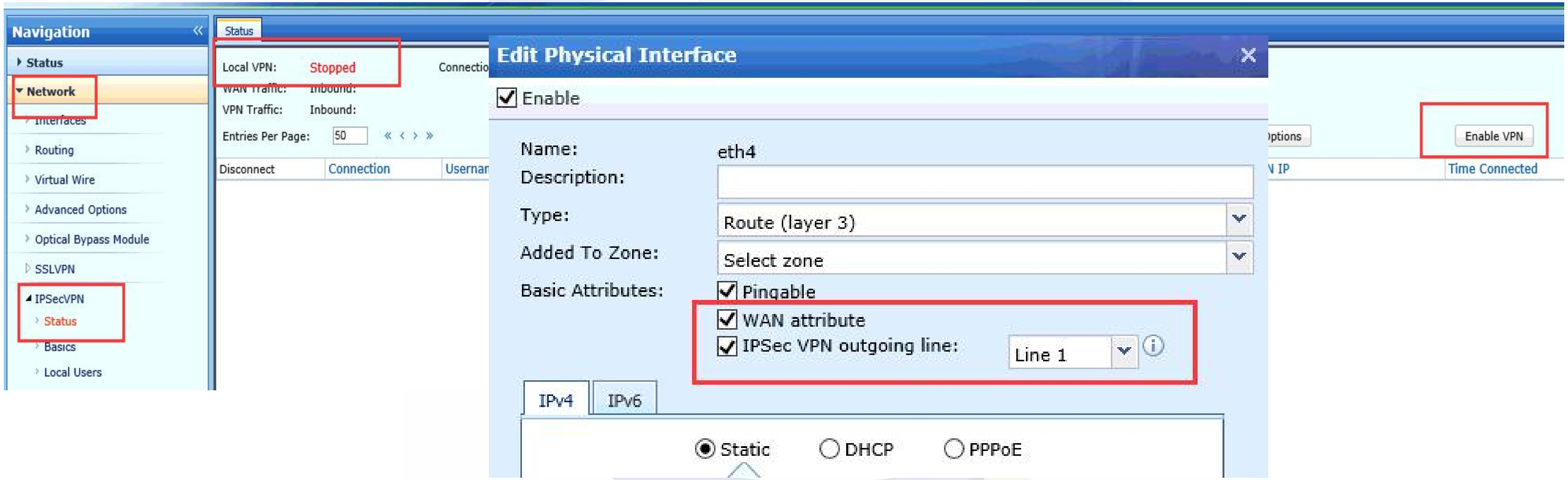
3. Mobile VPN Users:150

2. Since version 8.0.2, WAN-attribute route interface (non-management interface Eth0) no longer required in IPSec.

3. Since version 8.0.2, sub interface, VLAN interface and aggregate interface is now supported to configure VPN.

IPSEC VPN

If you would like to establish VPN, you need to enbale the VPN service and set up the line on the interface, outgoing line at phase I must be the same as outgoing line at wan-attribute route interface.



Local VPN: Stopped

VPN Traffic: Inbound:

Entries Per Page: 50

Edit Physical Interface

☑ Enable

Name: eth4

Description:

Type: Route (layer 3)

Added To Zone: Select zone

Basic Attributes:
☑ Pingable
☑ WAN attribute
☑ IPSec VPN outgoing line: Line 1

IPv4 | IPv6

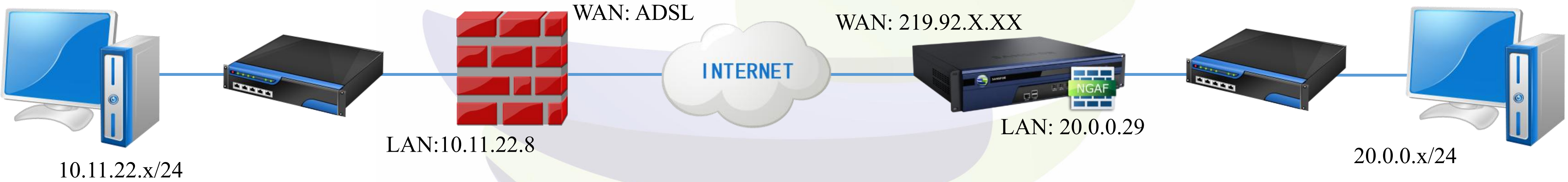
● Static ○ DHCP ○ PPPoE

IPSEC VPN Case Study

Customer wants to communicate in two sites by using internal IP address.

Sangfor:
Static public IP, directly connect to internet.

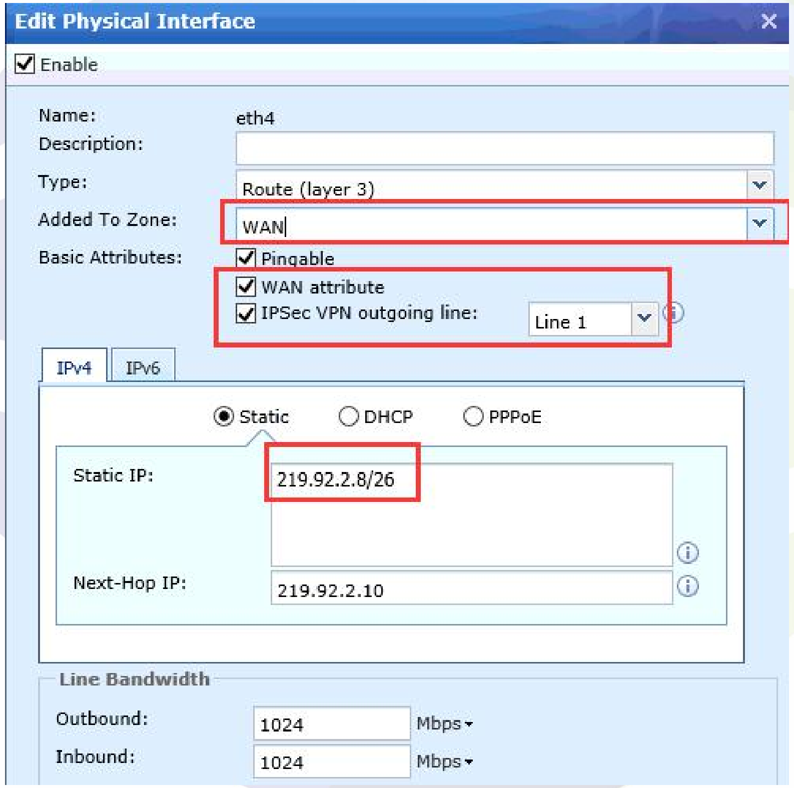
Fortinet/FortiGate:
ADSL, directly connect to internet.
Customer want to side intranet visit each other via IPSec
VPN



We connect these two sites with IPsec VPN.

IPSEC VPN

1. Configure the interface and the zone,Configuration path:[Network]->[Interfaces].



Edit Physical Interface

☑ Enable

Name: eth4

Description:

Type: Route (layer 3)

Added To Zone: WAN

Basic Attributes: ☑ Pingable

☑ WAN attribute

☑ IPSec VPN outgoing line: Line 1

IPv4 IPv6

● Static ○ DHCP ○ PPPoE

Static IP: 219.92.2.8/26

Next-Hop IP: 219.92.2.10

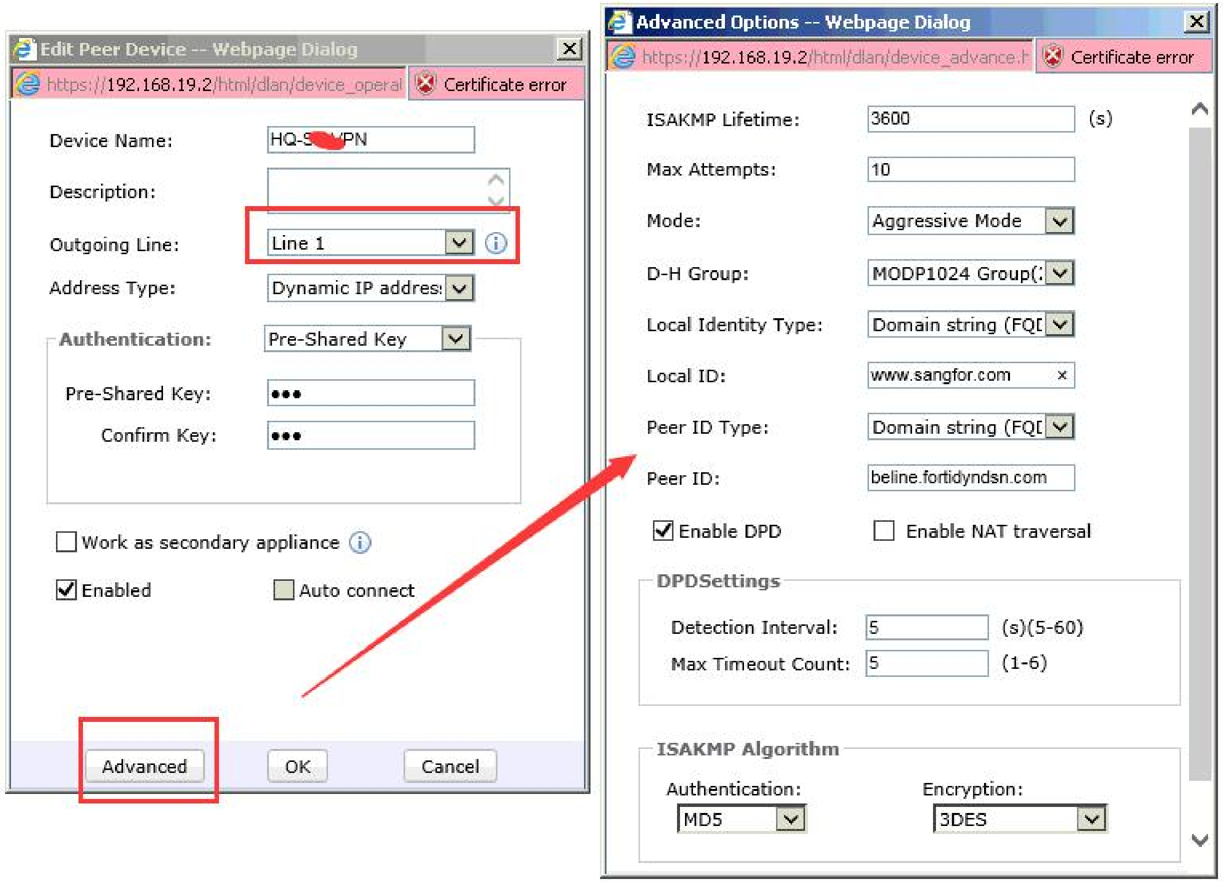
Line Bandwidth

Outbound: 1024 Mbps

Inbound: 1024 Mbps

IPSEC VPN

2. Phase I setting.



Edit Peer Device -- Webpage Dialog

https://192.168.19.2/html/dlan/device_operat Certificate error

Device Name: HQ-S[redacted]PN

Description:

Outgoing Line: Line 1

Address Type: Dynamic IP addres:

Authentication: Pre-Shared Key

Pre-Shared Key: •••

Confirm Key: •••

□ Work as secondary appliance

☑ Enabled □ Auto connect

Advanced Options -- Webpage Dialog

https://192.168.19.2/html/dlan/device_advance.h Certificate error

ISAKMP Lifetime: 3600 (s)

Max Attempts: 10

Mode: Aggressive Mode

D-H Group: MODP1024 Group(:

Local Identity Type: Domain string (FQD

Local ID: www.sangfor.com

Peer ID Type: Domain string (FQD

Peer ID: beline.fortidyndsn.com

☑ Enable DPD □ Enable NAT traversal

DPDSettings

Detection Interval: 5 (s)(5-60)

Max Timeout Count: 5 (1-6)

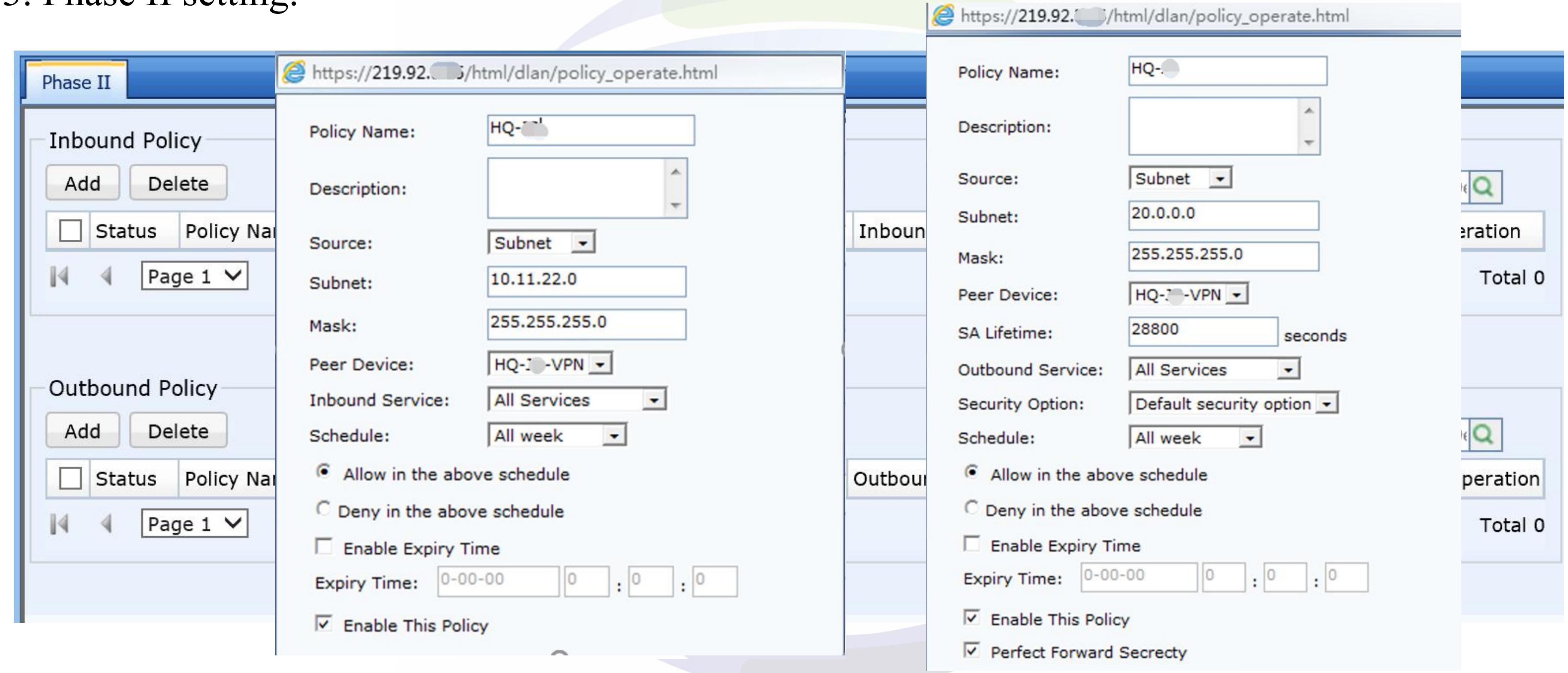
ISAKMP Algorithm

Authentication: MD5

Encryption: 3DES

IPSEC VPN

3. Phase II setting.



https://219.92.[redacted]/html/dlan/policy_operate.html

Policy Name: HQ-[redacted]

Description:

Source: Subnet

Subnet: 10.11.22.0

Mask: 255.255.255.0

Peer Device: HQ-[redacted]-VPN

Inbound Service: All Services

Schedule: All week

● Allow in the above schedule

○ Deny in the above schedule

□ Enable Expiry Time

Expiry Time: 0-00-00 0 : 0 : 0

☑ Enable This Policy

https://219.92.[redacted]/html/dlan/policy_operate.html

Policy Name: HQ-[redacted]

Description:

Source: Subnet

Subnet: 20.0.0.0

Mask: 255.255.255.0

Peer Device: HQ-[redacted]-VPN

SA Lifetime: 28800 seconds

Outbound Service: All Services

Security Option: Default security option

Schedule: All week

● Allow in the above schedule

○ Deny in the above schedule

□ Enable Expiry Time

Expiry Time: 0-00-00 0 : 0 : 0

☑ Enable This Policy

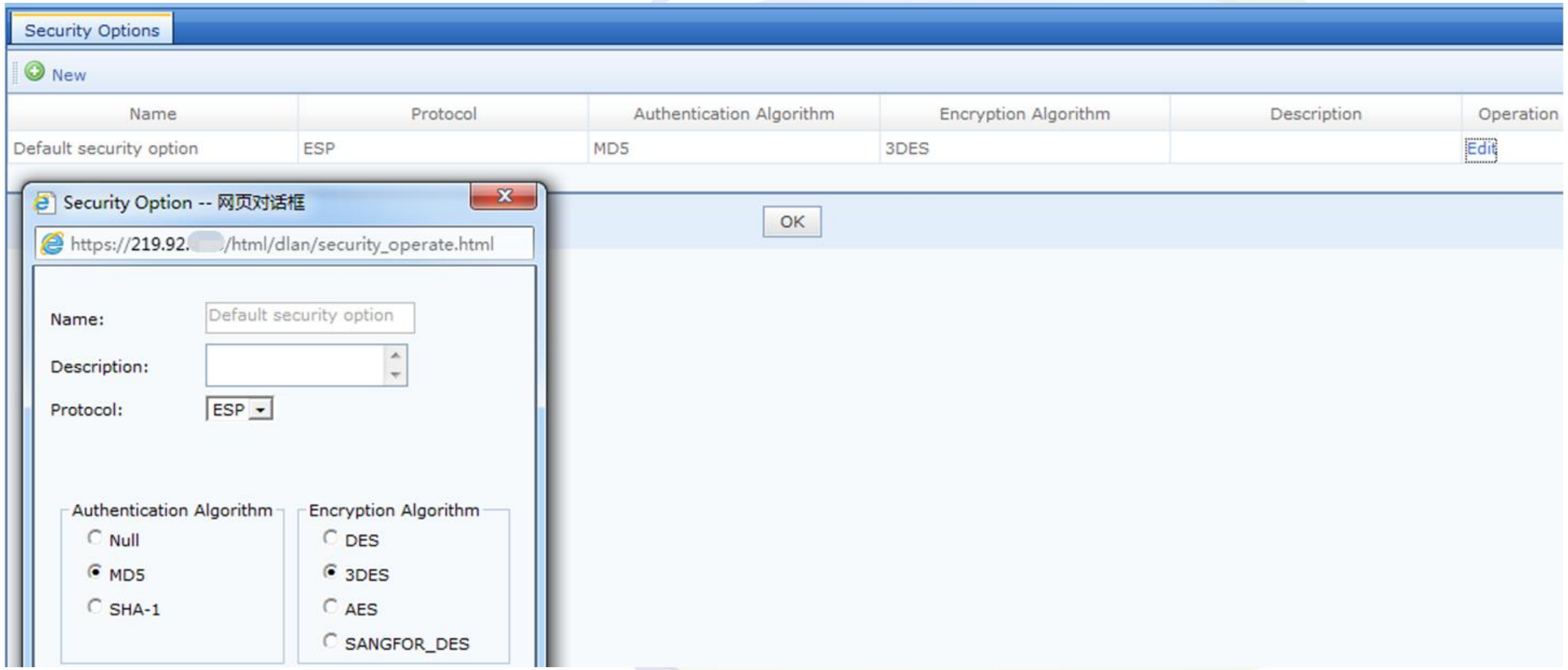
☑ Perfect Forward Secrecty

Inbound policy

Outbound policy

IPSEC VPN

4. Security options set the same as the peer.



Name	Protocol	Authentication Algorithm	Encryption Algorithm	Description	Operation
Default security option	ESP	MD5	3DES		Edit

Security Option -- 网页对话框

https://219.92.[redacted]/html/dlan/security_operate.html

Name: Default security option

Description:

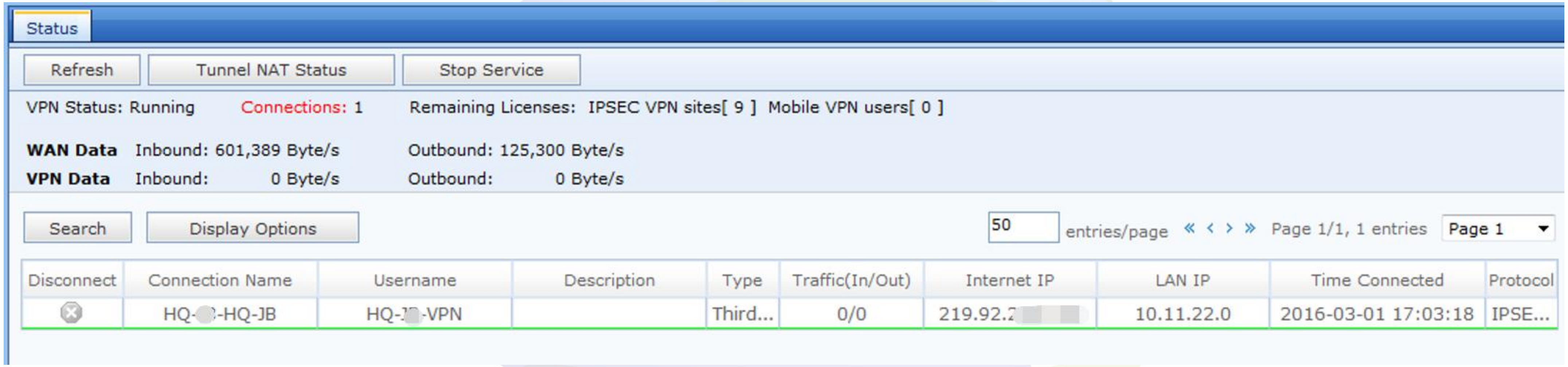
Protocol: ESP

Authentication Algorithm
- ○ Null
- ● MD5
- ○ SHA-1

Encryption Algorithm
- ○ DES
- ● 3DES
- ○ AES
- ○ SANGFOR_DES

IPSEC VPN

5. After successfully configuration, we can see the tunnel in the IPSec VPN status.



VPN Status: Running   Connections: 1   Remaining Licenses: IPSEC VPN sites[9] Mobile VPN users[0]

WAN Data Inbound: 601,389 Byte/s   Outbound: 125,300 Byte/s

VPN Data Inbound: 0 Byte/s   Outbound: 0 Byte/s

50 entries/page « ‹ › » Page 1/1, 1 entries Page 1

Disconnect	Connection Name	Username	Description	Type	Traffic(In/Out)	Internet IP	LAN IP	Time Connected	Protocol
⊗	HQ-[redacted]-HQ-JB	HQ-[redacted]-VPN		Third...	0/0	219.92.2[redacted]	10.11.22.0	2016-03-01 17:03:18	IPSE...

2. Sangfor VPN

SANGFOR
深信服科技

Sangfor VPN

Sangfor provide two types of VPN connection namely, standard IPSEC VPN, and a self-developed SANGFOR VPN, providing the device-to-device and PC(windows)-to-device connection. SANGFOR DLAN has the following advantages in comparison to standard IPSEC VPN:

1. Support both ends that are non-fixed IP public network environment.
2. Existence of VPN multi-line technology to achieve VPN link load balancing.
3. Branch users are connected through the HQ Internet to achieve unified control of the HQ via the tunnel route.
4. The tunnel NAT technology are used to solve problems of multiple branch network which IP segments conflict.
5. The tunnel flow control technology are used to achieve bandwidth allocation.

Sangfor VPN

Usages of Sangfor VPN:

HQ:

Provides VPN access services, and provides access to account verification of other VPN users. DLAN in HQ requires WEBAGENT configuration and VPN account for access. Generally, server side of the network is HQ.

Branch:

Access to HQ side. Generally, branch as client network.

Mobile:

The SANGFOR VPN software client, also known as PDLAN is usually a single client software that access through HQ as mobile users.

A VPN device can act as a HQ or branch.

Sangfor VPN

The term of Sangfor VPN:

Webagent:
For SANGFOR VPN interconnection, branch and mobile users look for HQ address to establish a VPN connection.

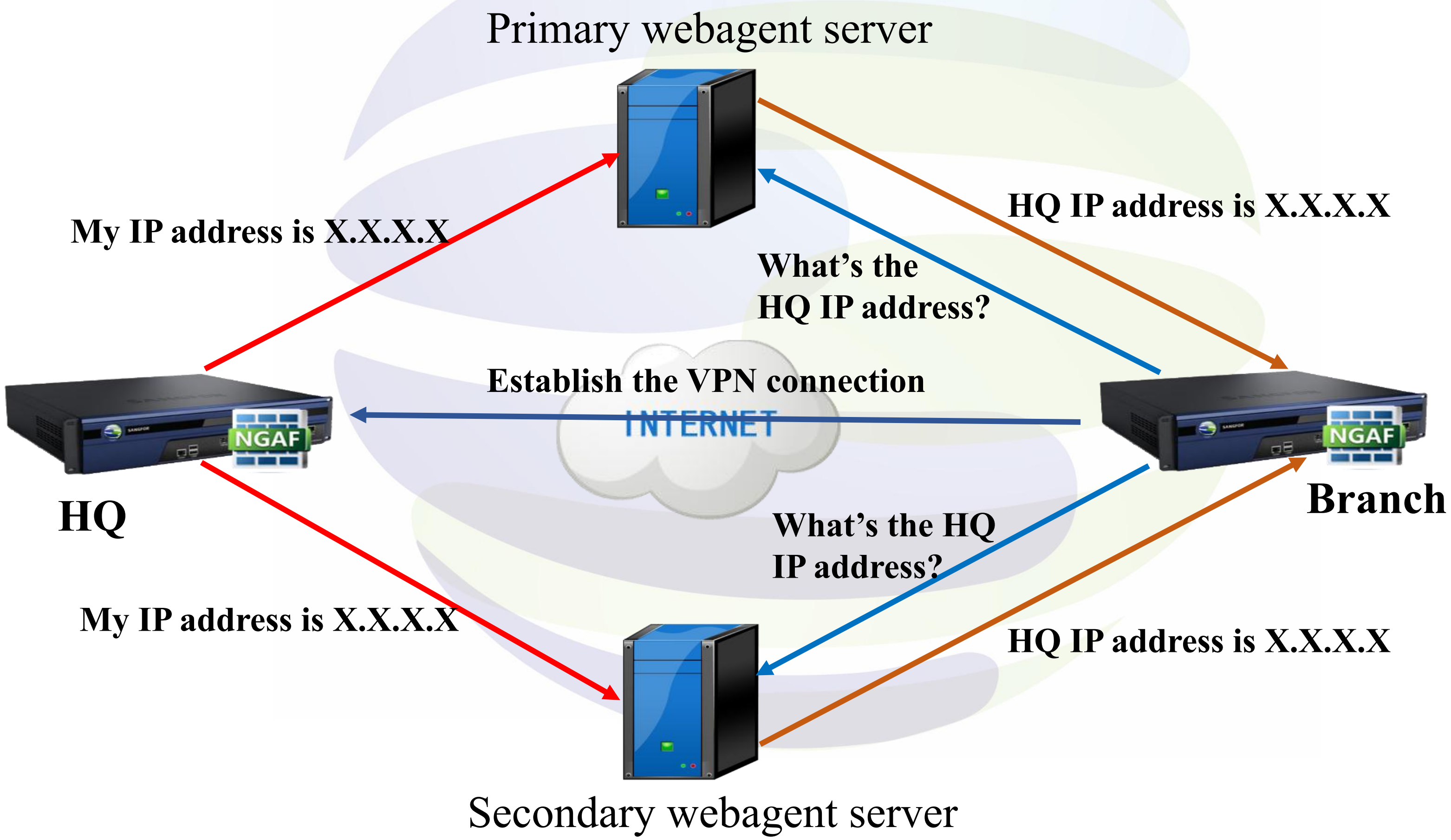
You can configure webagent in several ways:
1. IP: Port, eg.123.123.123.123:4009
Applicable to HQ VPN device that has a fixed public IP address of the environment.

2. IP1 # IP2: Port, such as 123.123.123.123 # 221.221.221.221: 4009
HQ VPN device that has multiple lines with fixed IP, and require VPN backups or for load balance.

3. Web URL format, such as: webagent.sangfor.com.cn/webagent/123.php
HQ VPN device that has no fixed IP environment, such as ADSL lines.

Sangfor VPN

WEBAGENT addressing process:
(During the addressing process, information is encrypted with DES.)



Sangfor VPN

The basic configurations for establishing a VPN connection between HQ and branch or mobile are as follow:

(1) HQ: Need to configure webagent, virtual IP pool (optional), users.

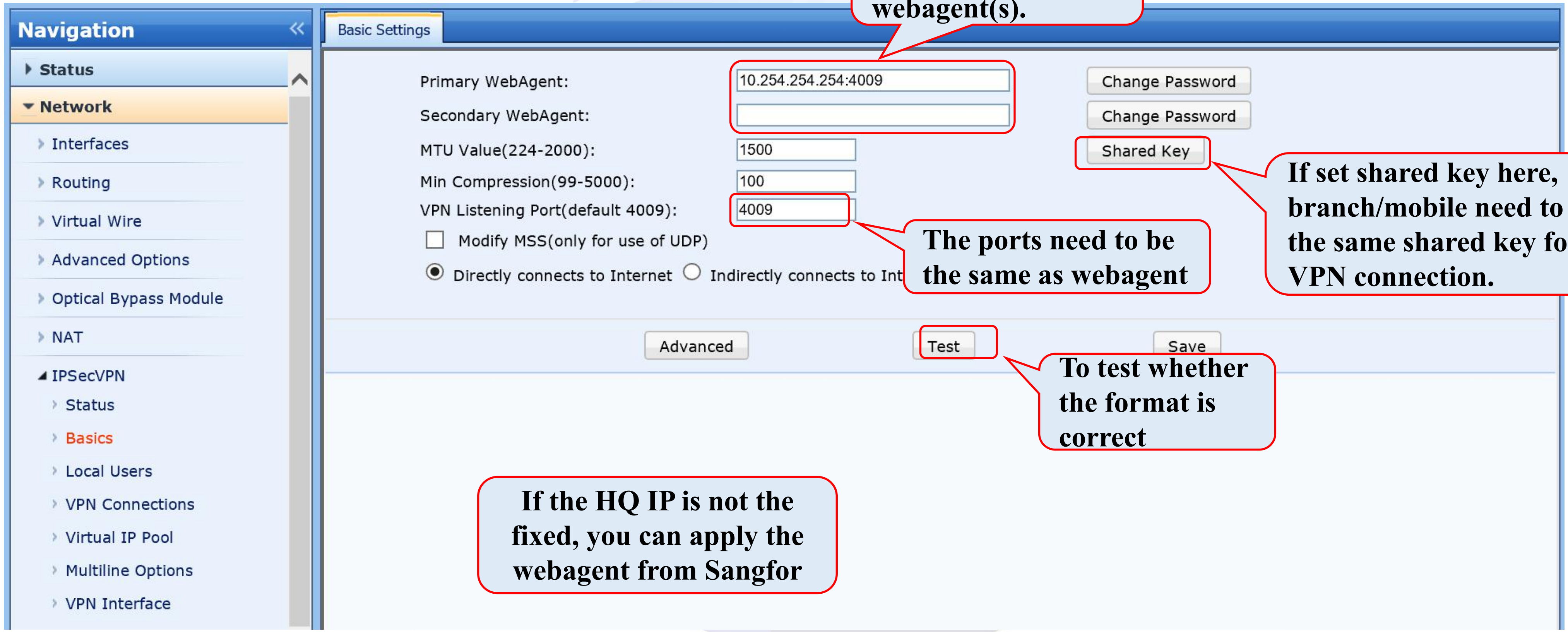
(2) Branch: Just configure the connection management.

(3) Mobile: Install PDLAN mobile software, configure the basic settings and main connection parameter settings,NGAF 8.0.7 no longer supports PDLAN.

Sangfor VPN

HQ setting:

Webagent setting:



Primary WebAgent: 10.254.254.254:4009

Secondary WebAgent:

MTU Value(224-2000): 1500

Min Compression(99-5000): 100

VPN Listening Port(default 4009): 4009

☐ Modify MSS(only for use of UDP)

● Directly connects to Internet ○ Indirectly connects to Int

Set the primary and secondary(optional) webagent(s).

If set shared key here, branch/mobile need to set the same shared key for VPN connection.

The ports need to be the same as webagent

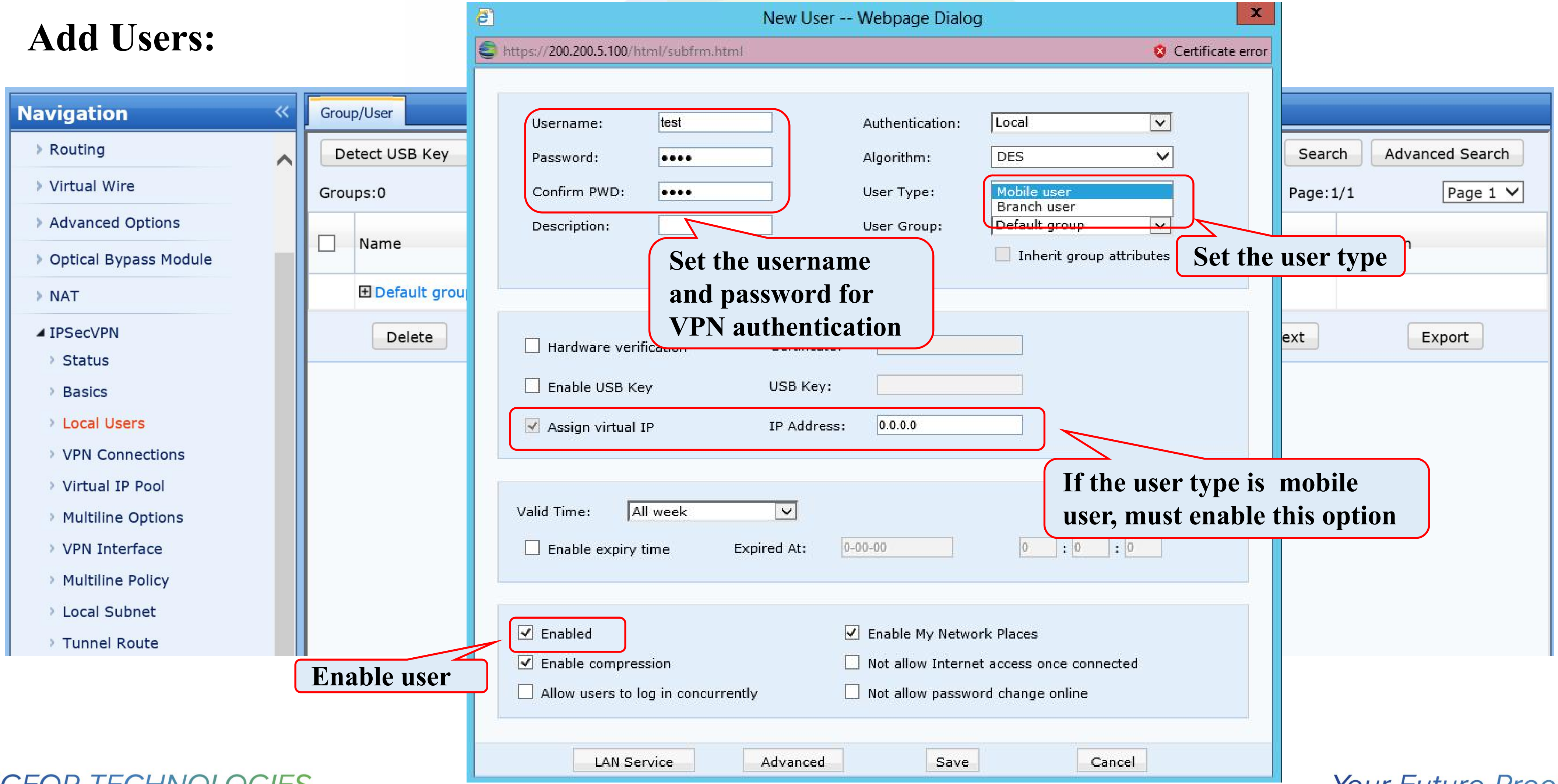
To test whether the format is correct

If the HQ IP is not the fixed, you can apply the webagent from Sangfor

Sangfor VPN

HQ setting:

Add Users:



New User -- Webpage Dialog

https://200.200.5.100/html/subfrm.html Certificate error

Username: test

Password: ••••

Confirm PWD: ••••

Description:

Authentication: Local

Algorithm: DES

User Type: Mobile user / Branch user

User Group: Default group

□ Inherit group attributes

□ Hardware verification Certificate:

□ Enable USB Key USB Key:

☑ Assign virtual IP IP Address: 0.0.0.0

Valid Time: All week

□ Enable expiry time Expired At: 0-00-00 0 : 0 : 0

☑ Enabled

☑ Enable compression

□ Allow users to log in concurrently

☑ Enable My Network Places

□ Not allow Internet once connected

□ Not allow password change online

LAN Service | Advanced | Save | Cancel

Set the username and password for VPN authentication

Set the user type

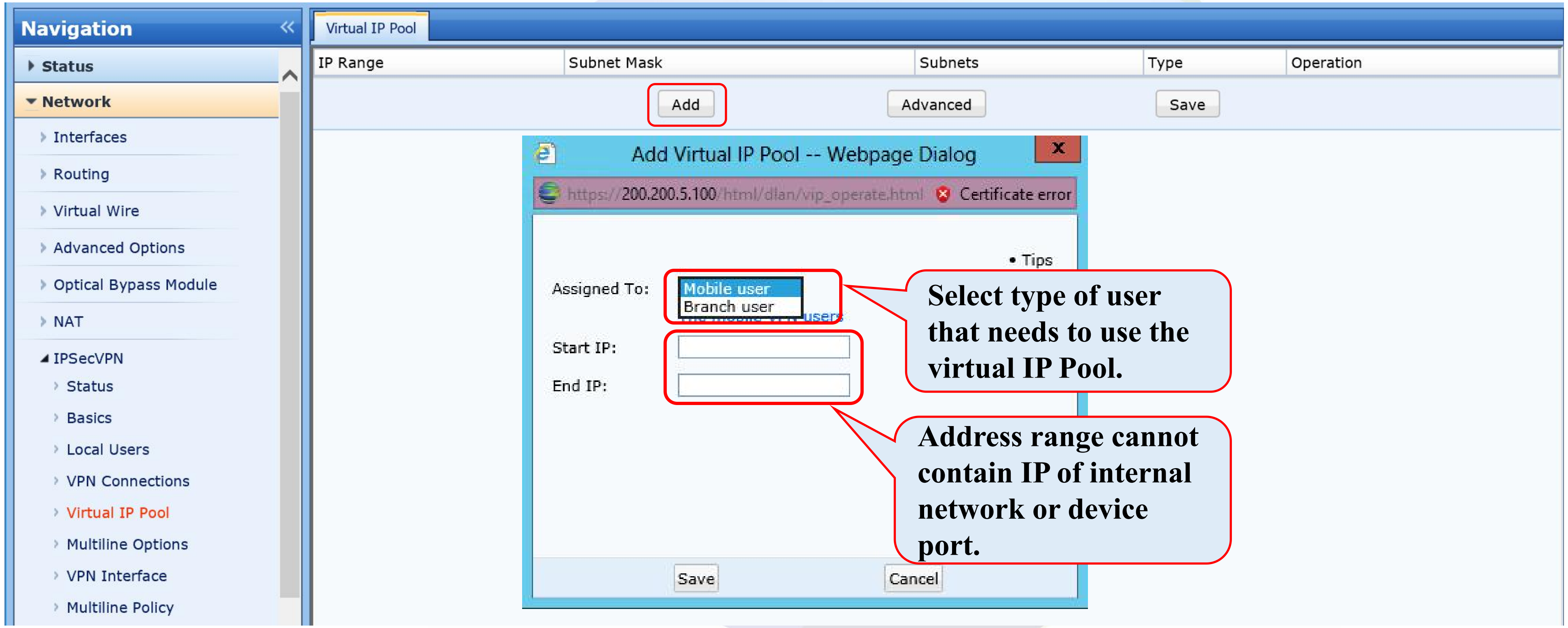
If the user type is mobile user, must enable this option

Enable user

Sangfor VPN

HQ setting:

Virtual IP Pool:



IP Range	Subnet Mask	Subnets	Type	Operation

Assigned To: Mobile user / Branch user

Start IP:

End IP:

Select type of user that needs to use the virtual IP Pool.

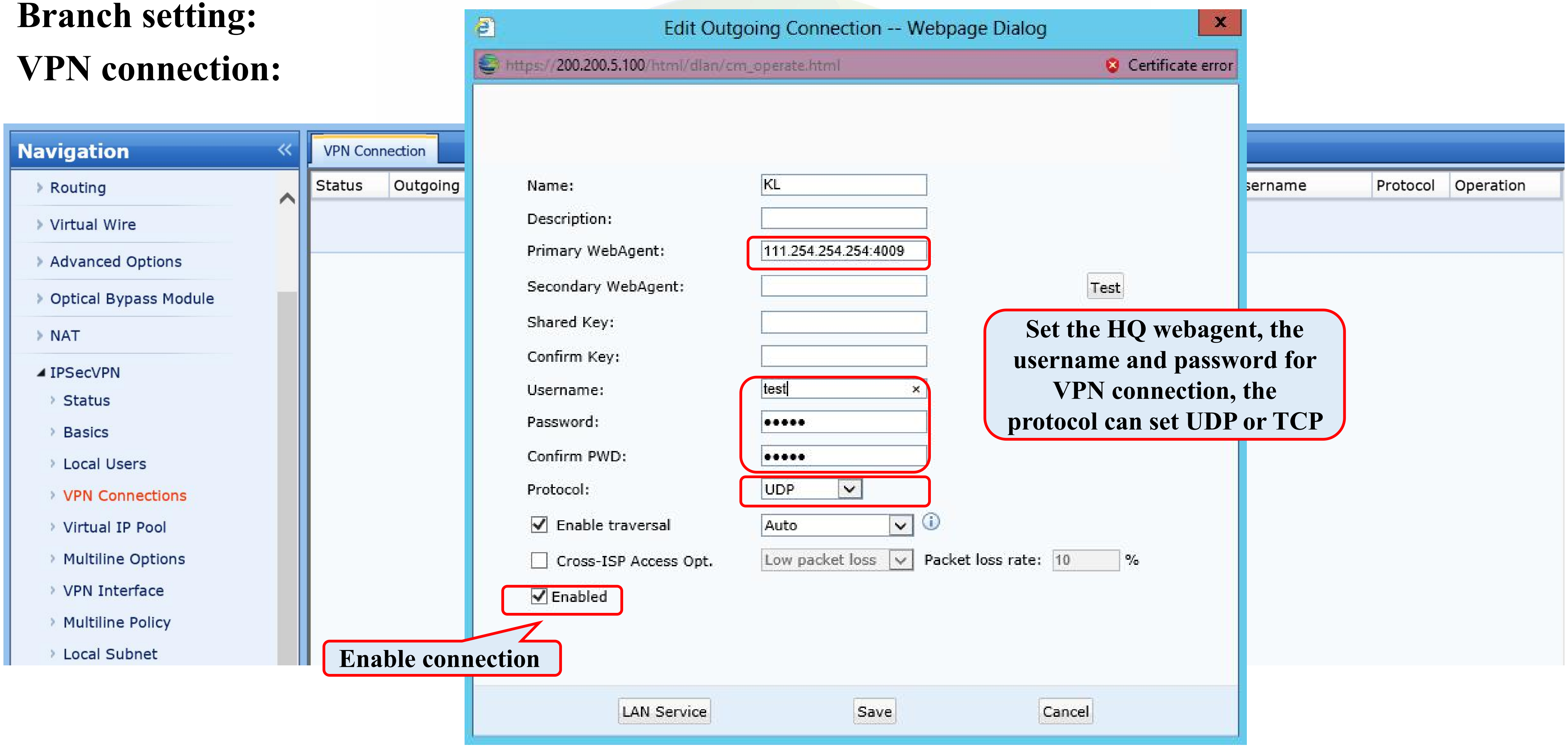
Address range cannot contain IP of internal network or device port.

When VPN uses a mobile user or VPN branch users enable the tunnel NAT, you need to configure virtual IP pool, otherwise it cannot be configured.

Sangfor VPN

Branch setting:

VPN connection:



Name: KL

Description:

Primary WebAgent: 111.254.254.254:4009

Secondary WebAgent:

Shared Key:

Confirm Key:

Username: test

Password: •••••

Confirm PWD: •••••

Protocol: UDP

☑ Enable traversal: Auto

□ Cross-ISP Access Opt.: Low packet loss; Packet loss rate: 10 %

☑ Enabled

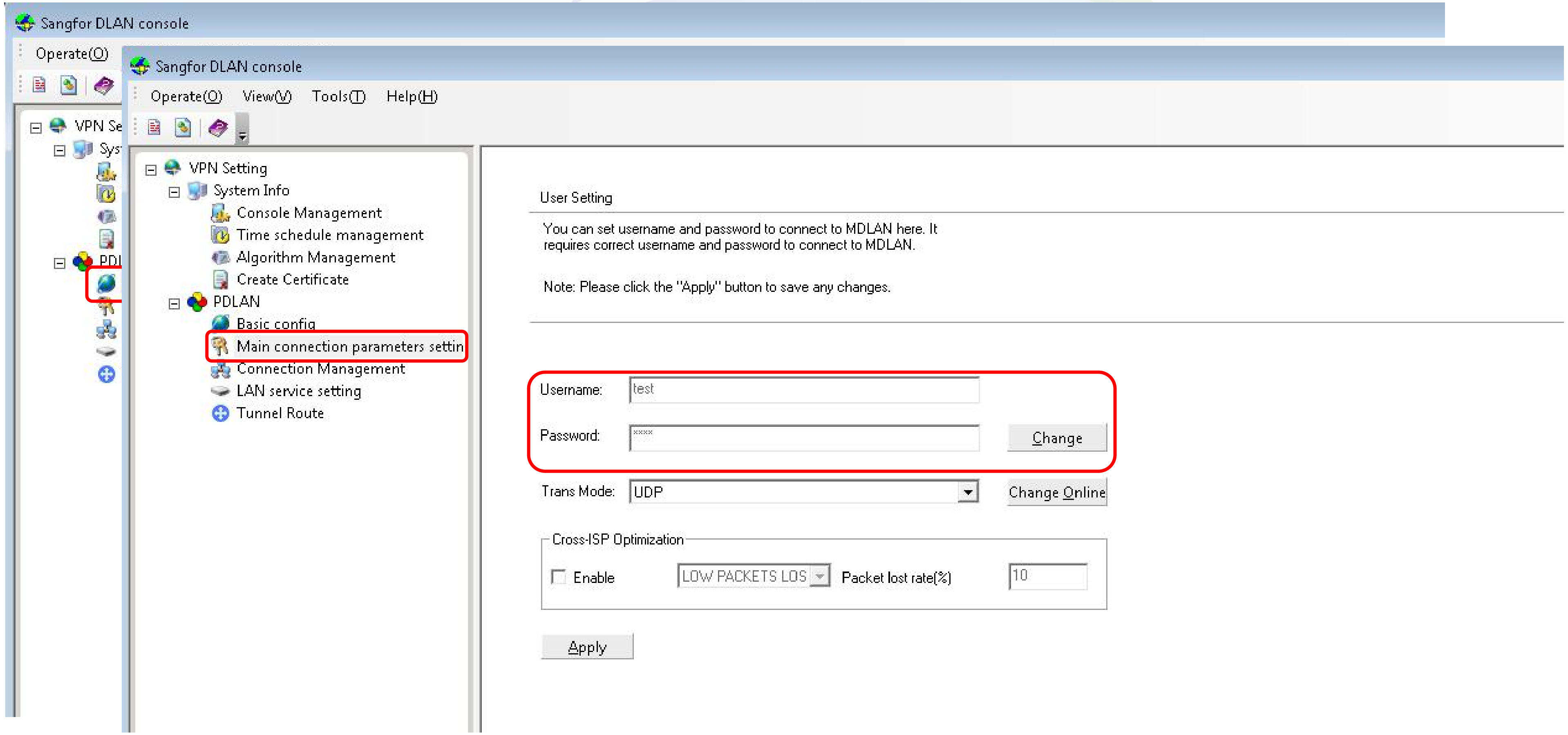
Set the HQ webagent, the username and password for VPN connection, the protocol can set UDP or TCP

Enable connection

Sangfor VPN

Mobile (PDLAN):

After Install the PDLAN software, Set the HQ Webagent, the username and password for VPN connection.



User Setting

You can set username and password to connect to MDLAN here. It requires correct username and password to connect to MDLAN.

Note: Please click the "Apply" button to save any changes.

Username: test

Password: ****

Trans Mode: UDP

Cross-ISP Optimization

□ Enable LOW PACKETS LOS Packet lost rate(%) 10

You can download PDLAN from our website: http://www.sangfor.com/service/firmware.html

Sangfor VPN

	IPSec VPN	Sangfor VPN
Port	UDP 500,4500	Default TCP/UDP 4009; can modify
Tunnel NAT	No	Yes
Multi line support	No	Yes
Tunnel route	No	Yes
Tunnel service control	No	Yes
Tunnel traffic control	No	Yes
Multicast service	No	Yes
Static public IP	At least one	No
Mobile support	Different software	PDLAN (only windows PC)
Company support	Most company	Only Sangfor

3. SSL VPN

SSL VPN

Sangfor NGAF not only provide PDLAN, but also SSL VPN for client VPN connection, making customer work convenient anywhere and anytime.

SSL VPN support:

Win XP, Win 7, Win 8, Win 10; (Only support IE browser)

Mac OS 10.8/10.9/10.10/10.11;

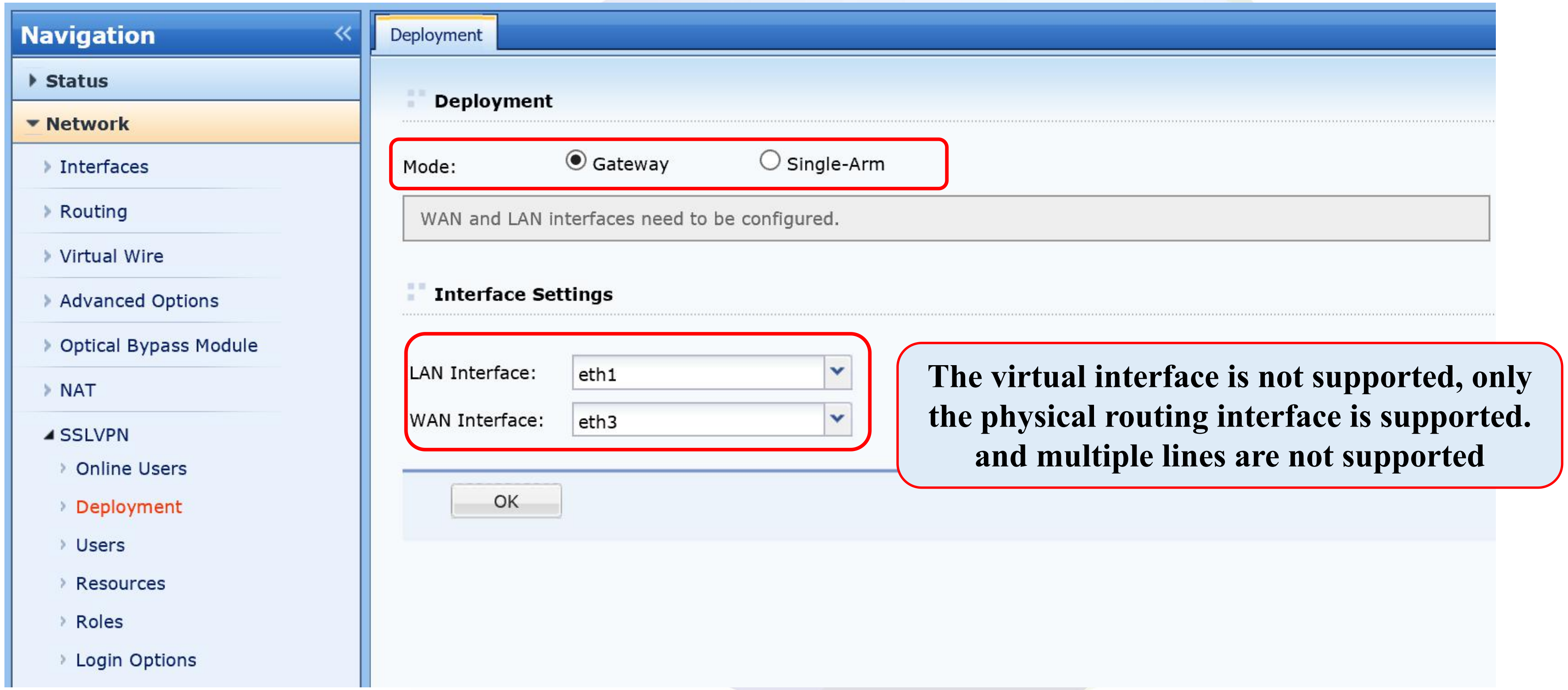
Android 4.0 and later versions;

IOS 9 and later versions; (Need to download a software called Easy Connect from APP Store)

SSL VPN

SSL VPN setting:

SSL Deployment:



Deployment

Mode: ● Gateway ○ Single-Arm

WAN and LAN interfaces need to be configured.

Interface Settings

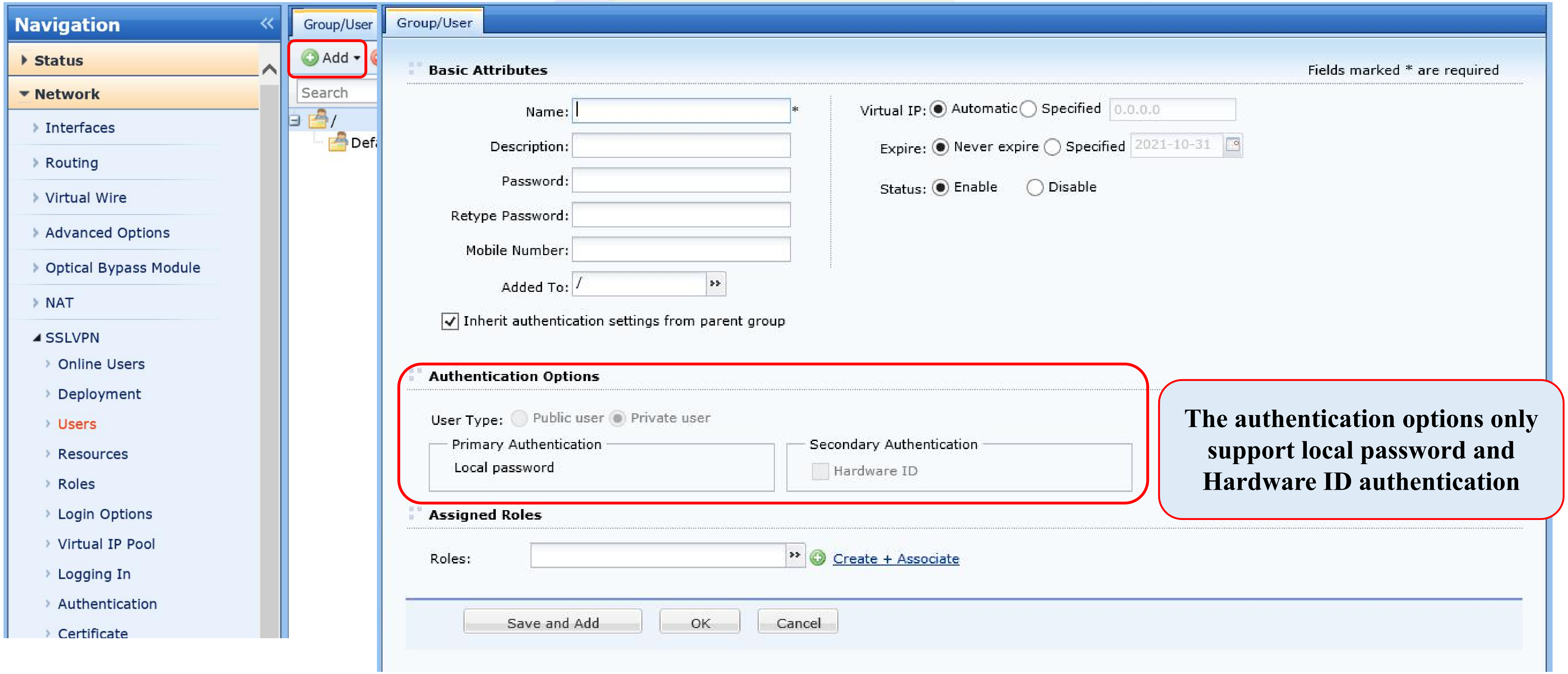
LAN Interface: eth1

WAN Interface: eth3

The virtual interface is not supported, only the physical routing interface is supported. and multiple lines are not supported

SSL VPN

Users management:



Basic Attributes

Fields marked * are required

Name:	*
Description:	
Password:	
Retype Password:	
Mobile Number:	
Added To:	/

☑ Inherit authentication settings from parent group

Virtual IP: ● Automatic ○ Specified 0.0.0.0

Expire: ● Never expire ○ Specified 2021-10-31

Status: ● Enable ○ Disable

Authentication Options

User Type: ○ Public user ● Private user

Primary Authentication: Local password

Secondary Authentication: □ Hardware ID

Assigned Roles

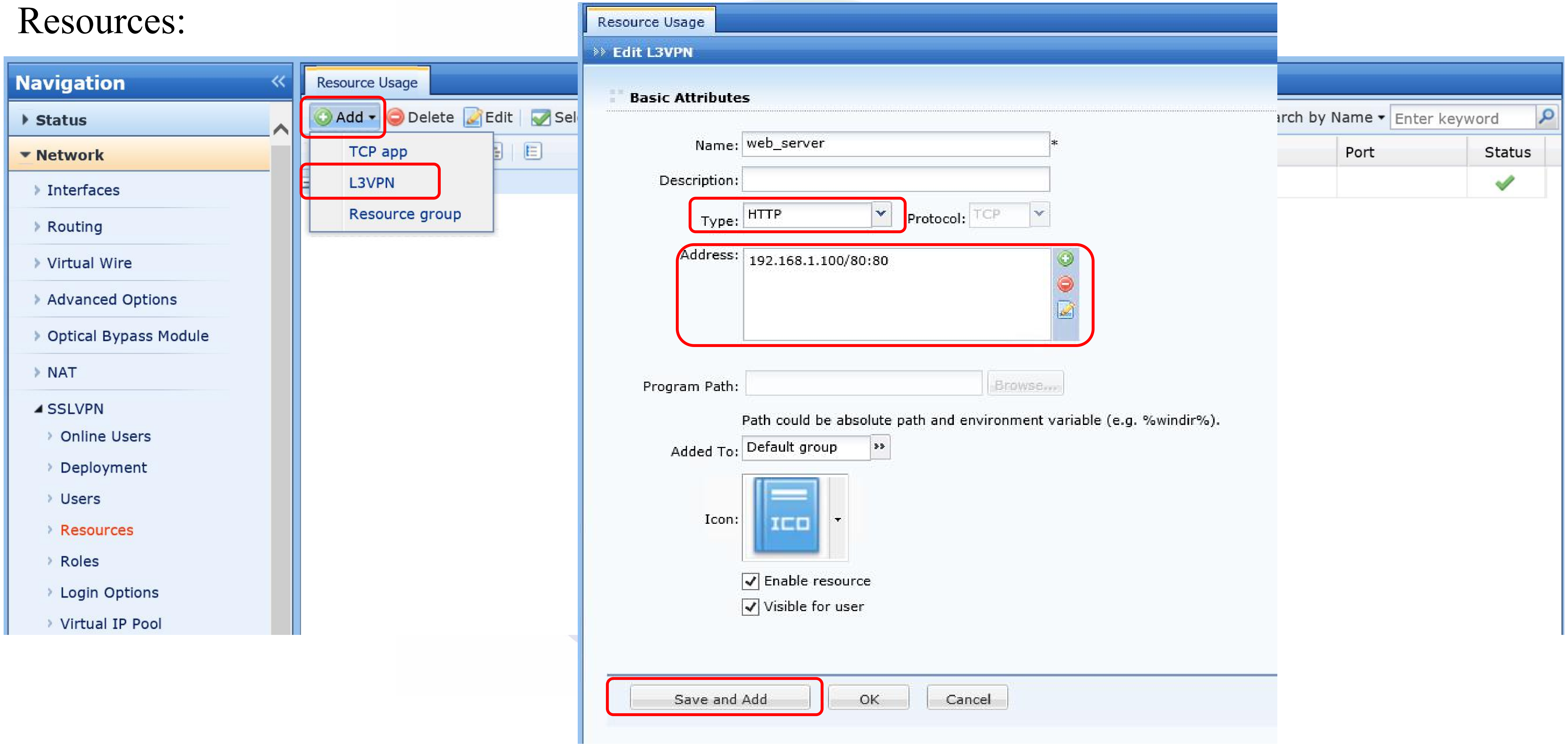
Roles: Create + Associate

Save and Add | OK | Cancel

The authentication options only support local password and Hardware ID authentication

SSL VPN

Resources:



Name: web_server *

Description:

Type: HTTP Protocol: TCP

Address: 192.168.1.100/80:80

Program Path: Browse...

Path could be absolute path and environment variable (e.g. %windir%).

Added To: Default group

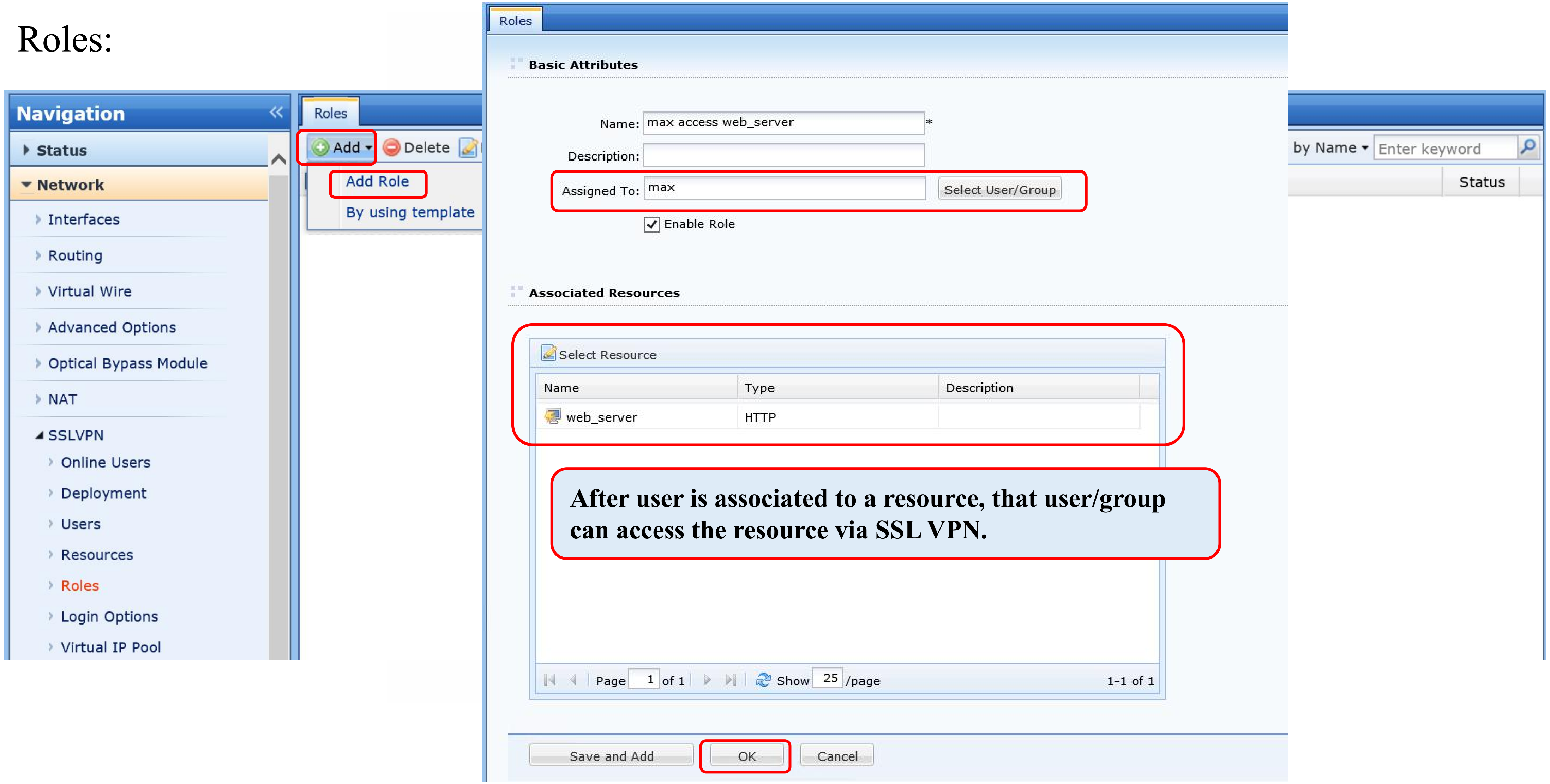
Icon: ICO

☑ Enable resource

☑ Visible for user

SSL VPN

Roles:



Basic Attributes

Name: max access web_server *

Description:

Assigned To: max   Select User/Group

☑ Enable Role

Associated Resources

Select Resource

Name	Type	Description
web_server	HTTP	

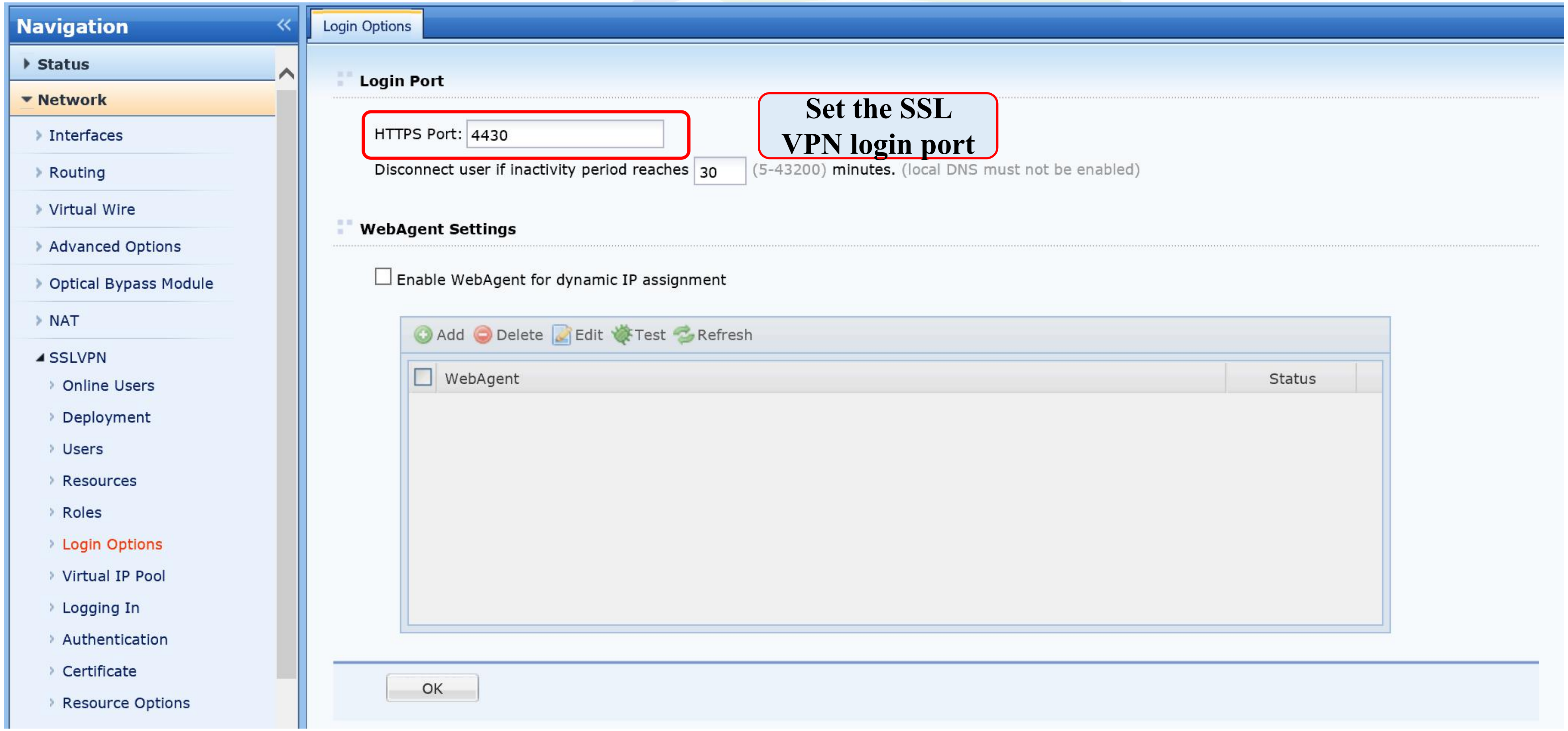
Page 1 of 1   Show 25 /page   1-1 of 1

Save and Add   OK   Cancel

After user is associated to a resource, that user/group can access the resource via SSL VPN.

SSL VPN

Login Options:



Login Port

HTTPS Port: 4430

Set the SSL VPN login port

Disconnect user if inactivity period reaches 30 (5-43200) minutes. (local DNS must not be enabled)

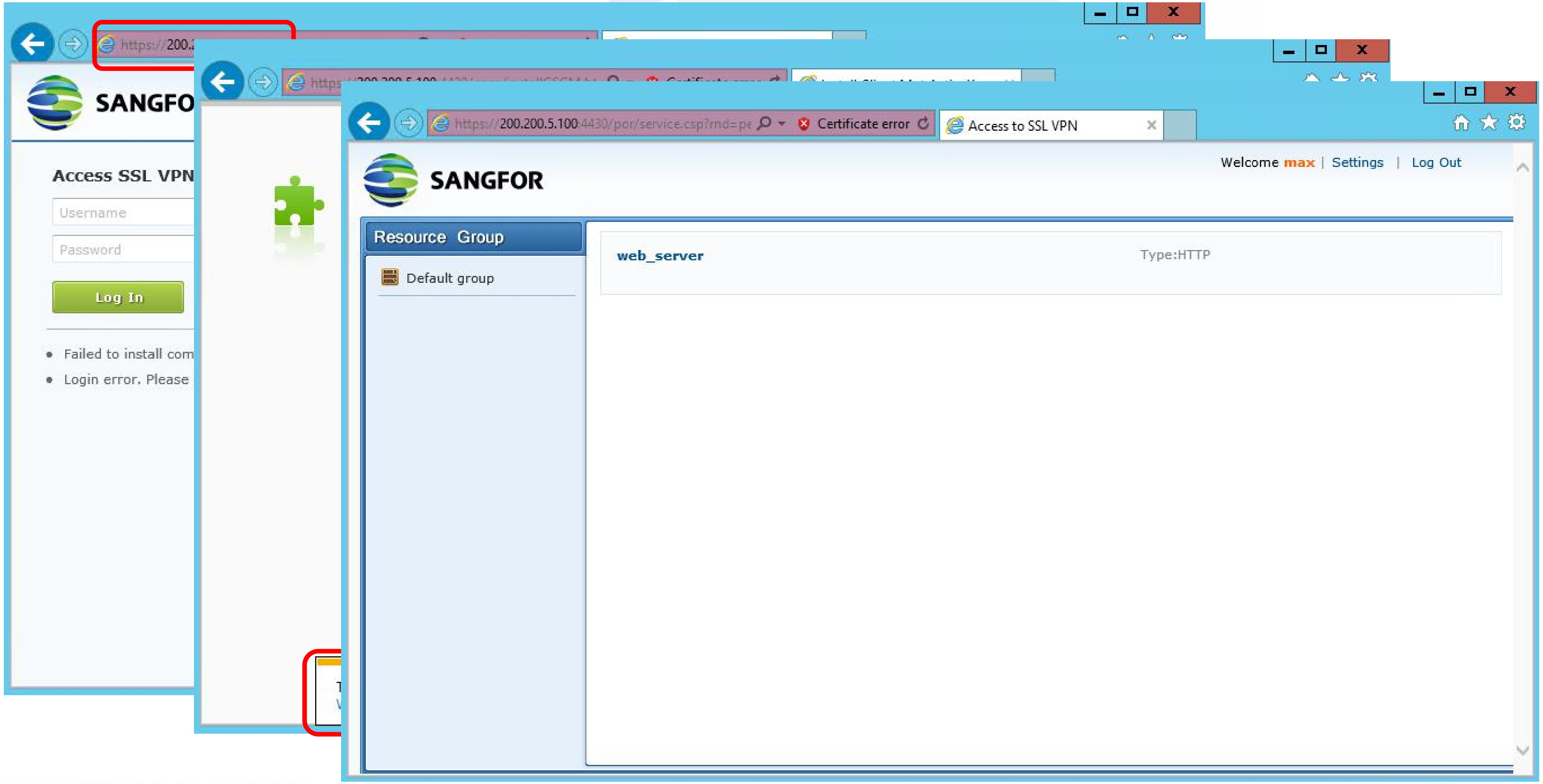
WebAgent Settings

☐ Enable WebAgent for dynamic IP assignment

☐ WebAgent	Status

SSL VPN

Client access to SSL VPN:



https://200.200.5.100:4430/por/service.csp?rnd=pe

Certificate error

Access to SSL VPN

Welcome max | Settings | Log Out

Access SSL VPN

Username

Password

Log In

- Failed to install com
- Login error. Please

Resource Group	
Default group	web_server Type:HTTP

Thank you !

tech.support@sangfor.com
community.sangfor.com

Sangfor Technologies (Headquarters)
Block A1, Nanshan iPark, No.1001
Xueyuan Road, Nanshan District,
Shenzhen, Guangdong Province,
P. R. China (518055)