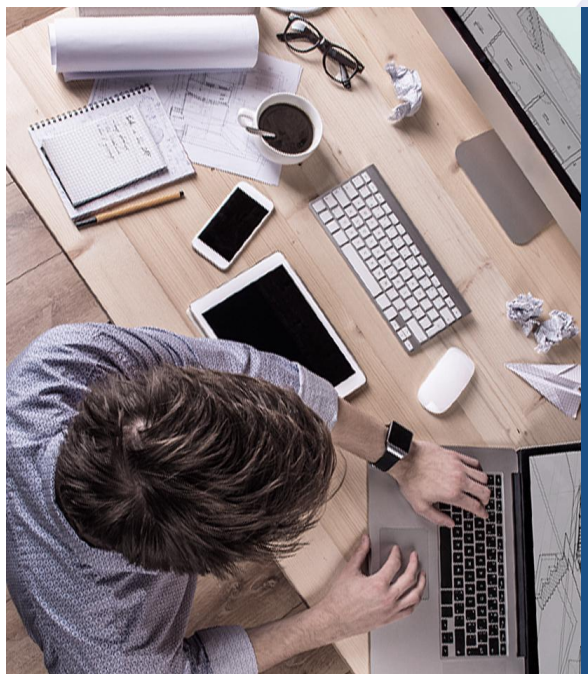




Sangfor NGAF v8.0.6 Associate

VPN





1 IPsec VPN

2 Sangfor VPN

3 SSL VPN

1. IPSec VPN



SANGFOR
深信服科技

IPSEC VPN

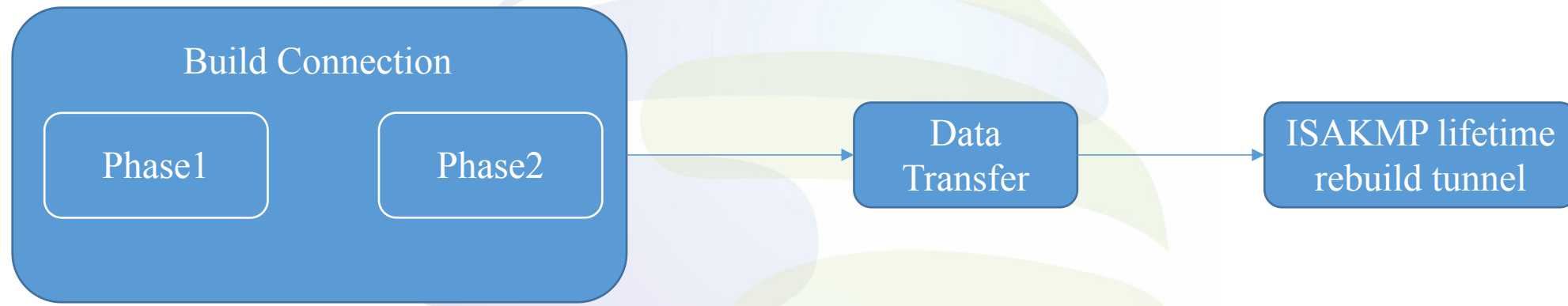
A virtual private network (VPN) extends a private network across a public network, and enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network.

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



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:

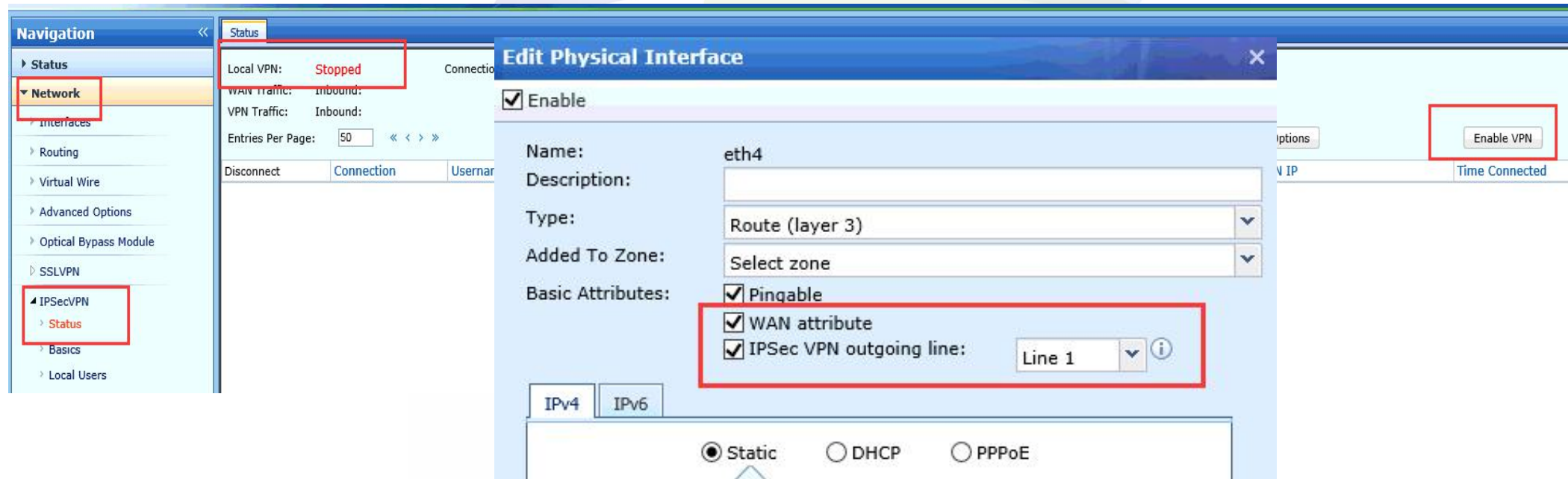


2. Since version 8.0.2, WAN-attribute route interface (non-management interface Eth0) no longer required in IPsec.

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 enable 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.



The screenshot displays the Sangfor VPN configuration interface. On the left, the 'Navigation' pane shows a tree structure with 'Network' expanded, and 'IPSecVPN' > 'Status' selected. The main area is divided into two panes: 'Status' and 'Edit Physical Interface'. The 'Status' pane shows 'Local VPN: Stopped' and 'WAN Traffic: Inbound:'. The 'Edit Physical Interface' pane shows the configuration for 'eth4', including 'Type: Route (layer 3)', 'Added To Zone: Select zone', and 'Basic Attributes' with checkboxes for 'Pinqable', 'WAN attribute', and 'IPSec VPN outgoing line: Line 1'. A red box highlights the 'IPSec VPN outgoing line' dropdown. In the top right corner, there is a button labeled 'Enable VPN'.

IPSEC VPN Case Study

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

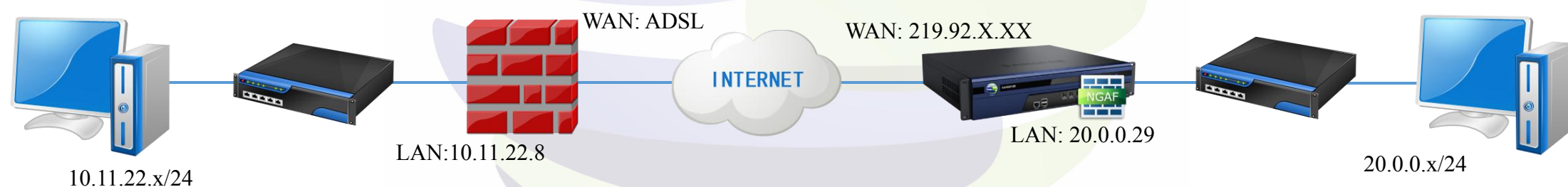
Sangfor:

Static public IP, directly connect to internet.

Fortinet/FortiGate:

ADSL, directly connect to internet.

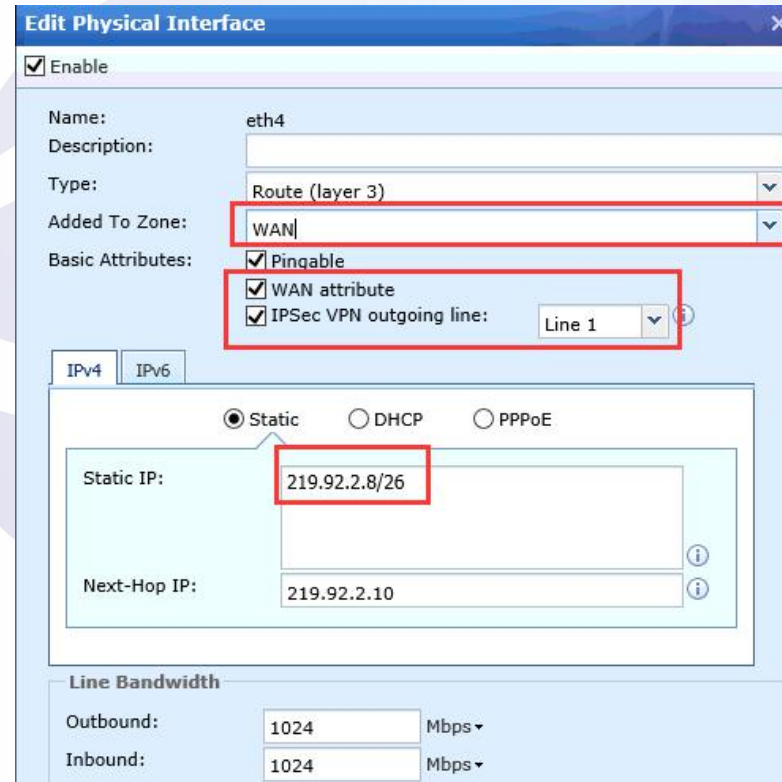
Customer want to side intranet visit each other via IPsec VPN



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

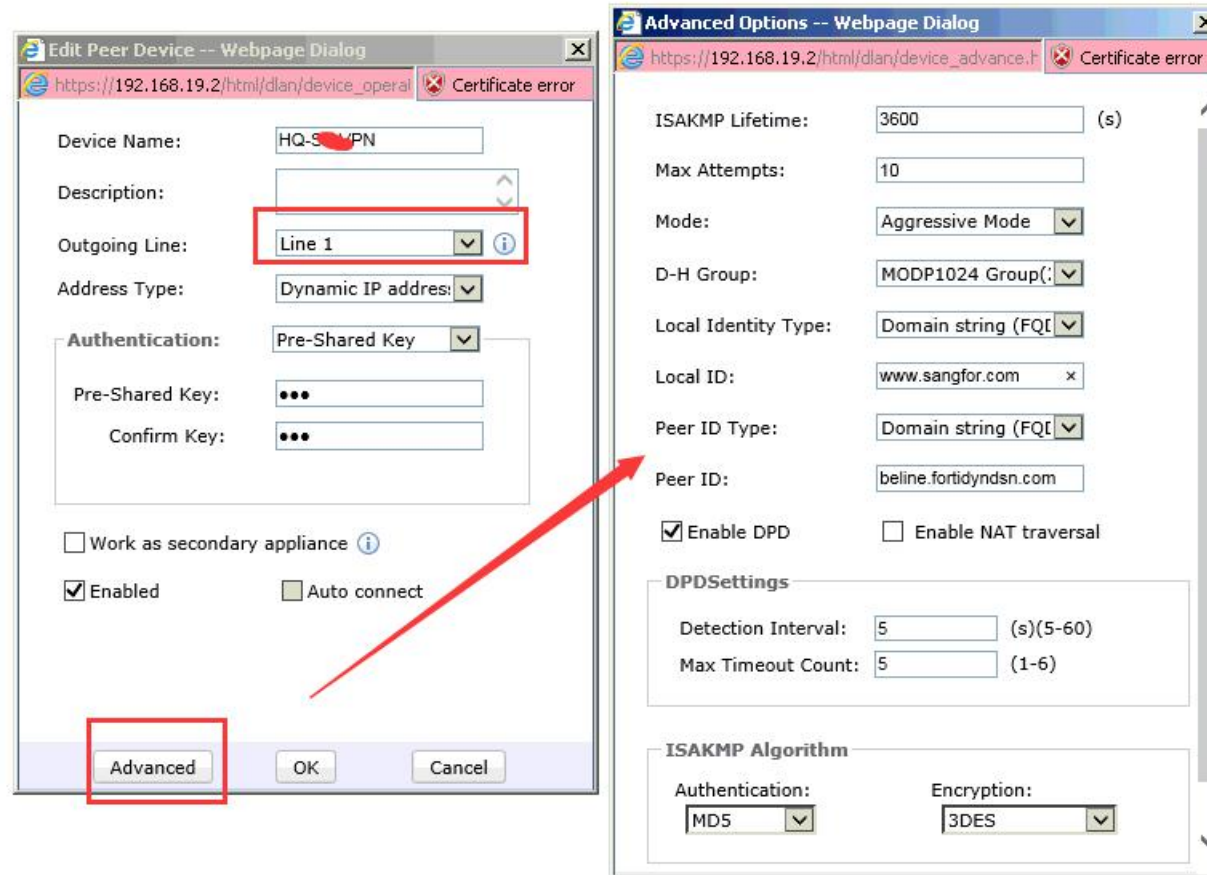
Line Bandwidth

Outbound: 1024 Mbps

Inbound: 1024 Mbps

IPSEC VPN

2. Phase I setting.



The image displays two overlapping web-based configuration windows for a Sangfor VPN device. The left window, titled "Edit Peer Device -- Webpage Dialog", shows the main configuration for a peer device named "HQ-S-VPN". The "Outgoing Line" is set to "Line 1", and the "Authentication" is set to "Pre-Shared Key". The "Advanced" button at the bottom is highlighted with a red box. The right window, titled "Advanced Options -- Webpage Dialog", shows the advanced configuration for the same peer device. It includes settings for "ISAKMP Lifetime" (3600s), "Max Attempts" (10), "Mode" (Aggressive Mode), "D-H Group" (MODP1024 Group), "Local Identity Type" (Domain string (FQDN)), "Local ID" (www.sangfor.com), "Peer ID Type" (Domain string (FQDN)), and "Peer ID" (beline.fortidyndsn.com). The "Enable DPD" checkbox is checked, and the "DPDSettings" section shows a "Detection Interval" of 5s and a "Max Timeout Count" of 5. The "ISAKMP Algorithm" section shows "Authentication" set to MD5 and "Encryption" set to 3DES. A red arrow points from the "Advanced" button in the left window to the "Advanced Options" window.

Edit Peer Device -- Webpage Dialog

Device Name: HQ-S-VPN

Description:

Outgoing Line: Line 1

Address Type: Dynamic IP address

Authentication: Pre-Shared Key

Pre-Shared Key: ●●●

Confirm Key: ●●●

☐ Work as secondary appliance

☒ Enabled ☐ Auto connect

Advanced OK Cancel

Advanced Options -- Webpage Dialog

ISAKMP Lifetime: 3600 (s)

Max Attempts: 10

Mode: Aggressive Mode

D-H Group: MODP1024 Group

Local Identity Type: Domain string (FQDN)

Local ID: www.sangfor.com

Peer ID Type: Domain string (FQDN)

Peer ID: beline.fortidyndsn.com

☒ Enable DPD ☐ Enable NAT traversal

DPDSettings

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

Max Timeout Count: 5 (1-6)

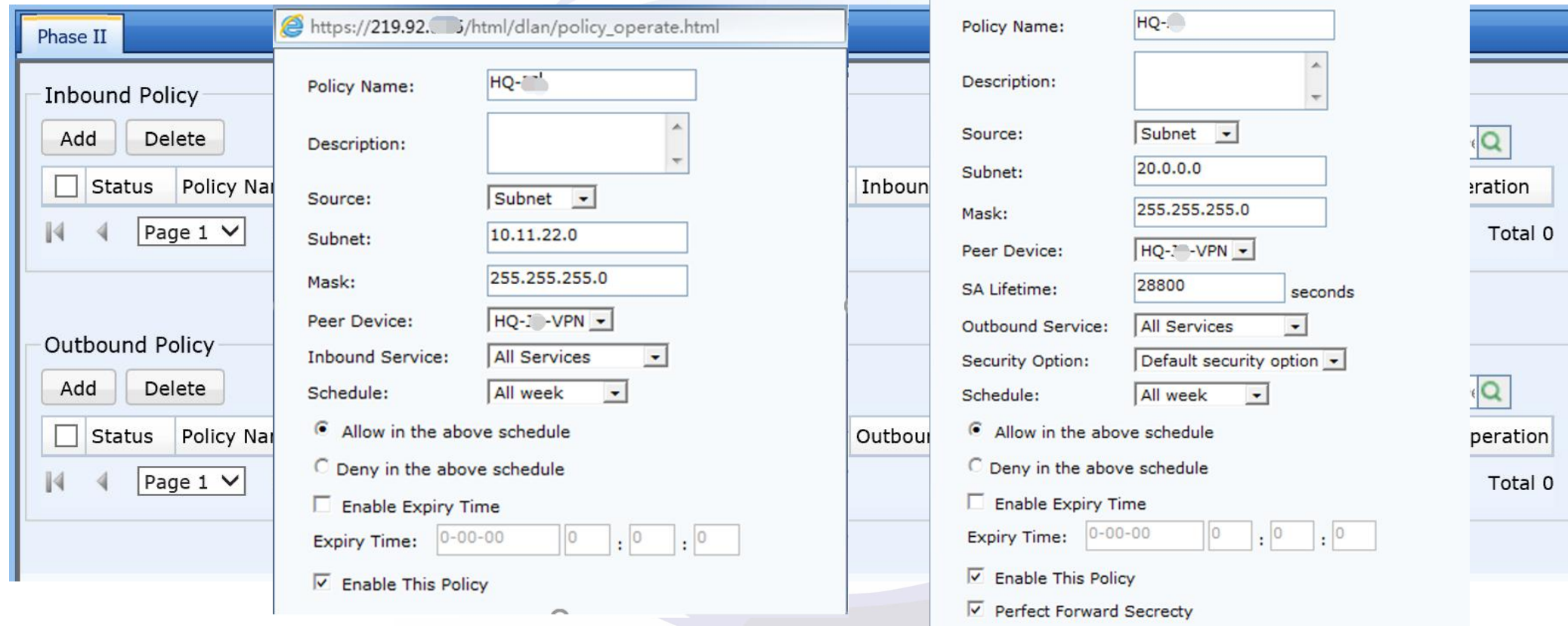
ISAKMP Algorithm

Authentication: MD5

Encryption: 3DES

IPSEC VPN

3. Phase II setting.



The screenshot displays the Sangfor IPSEC VPN management interface for Phase II settings. It is divided into two main sections: Inbound Policy and Outbound Policy. Both sections show a list of policies on the left and a detailed configuration form on the right. The Inbound Policy form is for policy 'HQ-1' and the Outbound Policy form is for policy 'HQ-1-VPN'. Both policies are configured with the same parameters: Source (Subnet 10.11.22.0/255.255.255.0), Peer Device (HQ-1-VPN), Inbound Service (All Services), and Schedule (All week). The 'Allow in the above schedule' option is selected for both, and 'Enable This Policy' is checked. The 'Perfect Forward Secrecy' option is also checked for the Outbound policy.

Inbound Policy Configuration:

- Policy Name: HQ-1
- Description:
- Source: Subnet (10.11.22.0)
- Mask: 255.255.255.0
- Peer Device: HQ-1-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
- ☒ Enable This Policy

Outbound Policy Configuration:

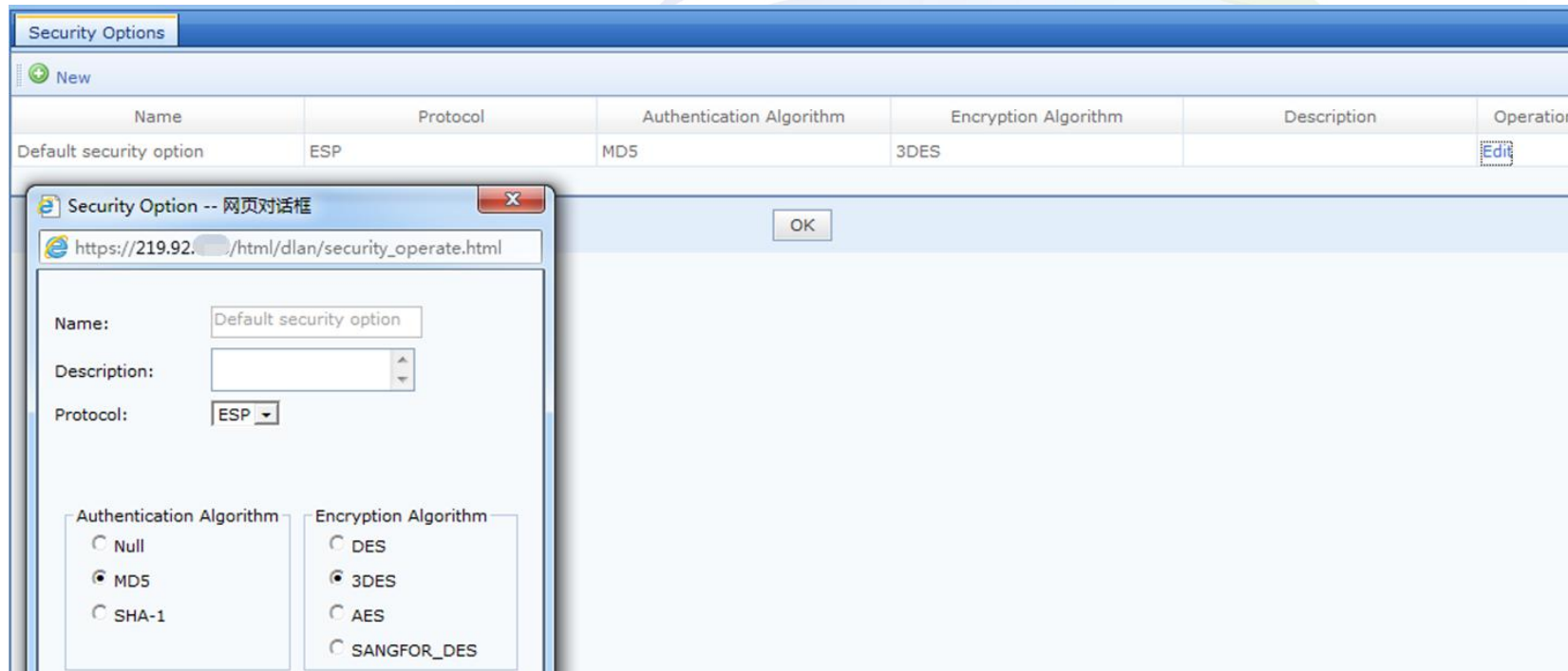
- Policy Name: HQ-1-VPN
- Description:
- Source: Subnet (20.0.0.0)
- Mask: 255.255.255.0
- Peer Device: HQ-1-VPN
- SA Lifetime: 28800 seconds
- Outbound Service: All Services
- Security Option: Default security option
- Schedule: All week
- ☒ Allow in the above schedule
- ☐ Deny in the above schedule
- ☐ Enable Expiry Time
- Expiry Time: 0-00-00 : 0 : 0
- ☒ Enable This Policy
- ☒ Perfect Forward Secrecy

Inbound policy

Outbound policy

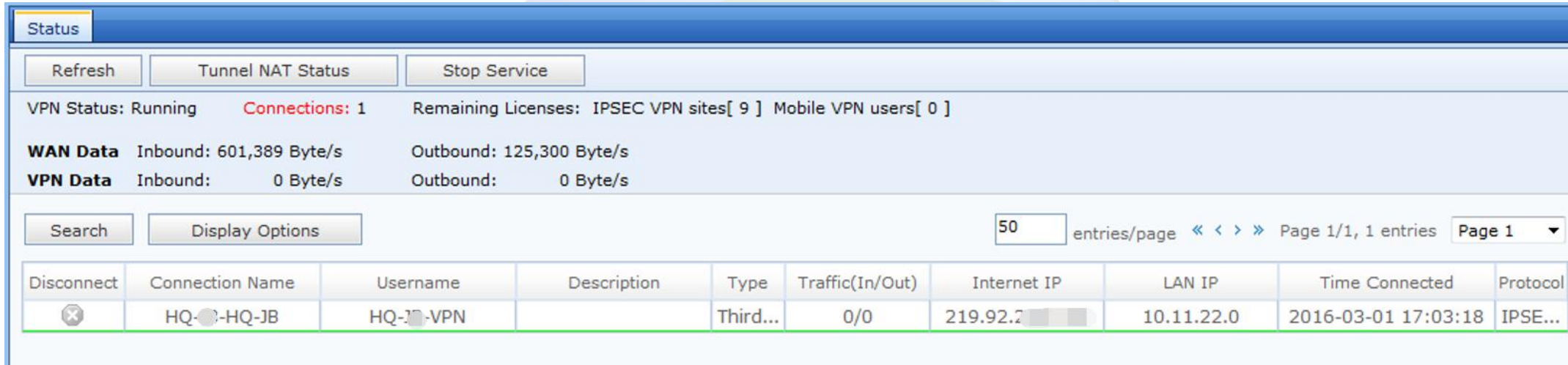
IPSEC VPN

4. Security options set the same as the peer.




IPSEC VPN

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



The screenshot displays the 'Status' page of the SANGFOR IPsec VPN management interface. At the top, there are three buttons: 'Refresh', 'Tunnel NAT Status', and 'Stop Service'. Below these, the VPN status is shown as 'Running' with 'Connections: 1' in red. It also indicates 'Remaining Licenses: IPSEC VPN sites[9] Mobile VPN users[0]'. The 'WAN Data' section shows 'Inbound: 601,389 Byte/s' and 'Outbound: 125,300 Byte/s'. The 'VPN Data' section shows 'Inbound: 0 Byte/s' and 'Outbound: 0 Byte/s'. A search bar and 'Display Options' button are present. A table lists the active connection with 50 entries per page. The table has columns for Disconnect, Connection Name, Username, Description, Type, Traffic(In/Out), Internet IP, LAN IP, Time Connected, and Protocol. One connection is listed: HQ-JB-HQ-JB, HQ-JB-VPN, with a Type of 'Third...' and a Protocol of 'IPSE...'. The interface is styled with a blue header and a light blue background.

Disconnect	Connection Name	Username	Description	Type	Traffic(In/Out)	Internet IP	LAN IP	Time Connected	Protocol
	HQ-JB-HQ-JB	HQ-JB-VPN		Third...	0/0	219.92.2...	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.

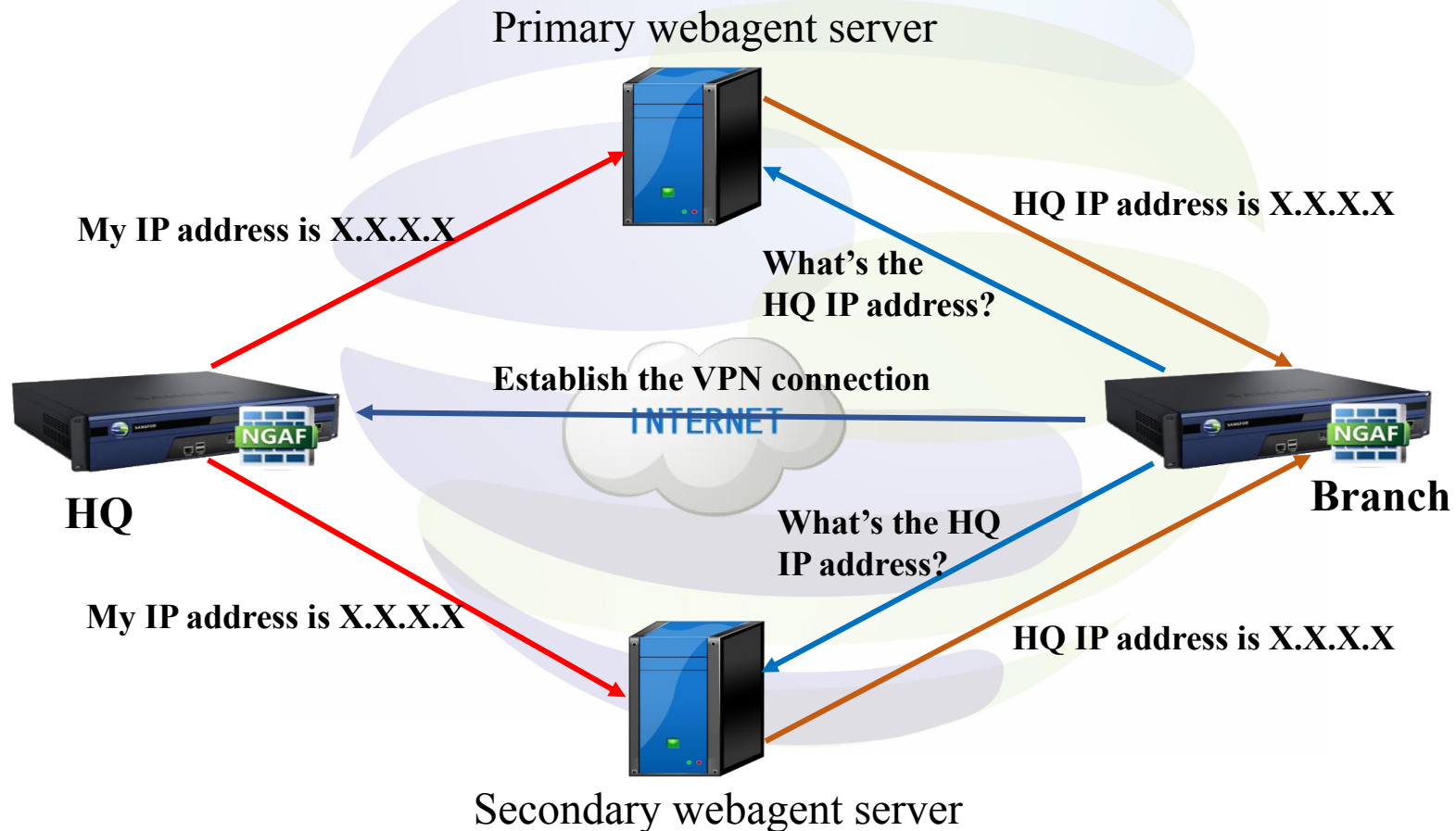
3. Web URL format, such as: **webagent.sangfor.com.cn/webagent/123.php**

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:

The screenshot shows the 'Basic Settings' page for Sangfor VPN. The left sidebar contains a 'Navigation' menu with options: Status, Network (expanded), Interfaces, Routing, Virtual Wire, Advanced Options, Optical Bypass Module, NAT, IPSecVPN (expanded), Status, Basics (highlighted), Local Users, VPN Connections, Virtual IP Pool, Multiline Options, and VPN Interface. The main content area is titled 'Basic Settings' and contains the following fields and controls:

- Primary WebAgent: 10.254.254.254:4009
- Secondary WebAgent: (empty)
- 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 Internet
- Buttons: Change Password, Change Password, Shared Key, Advanced, Test, Save

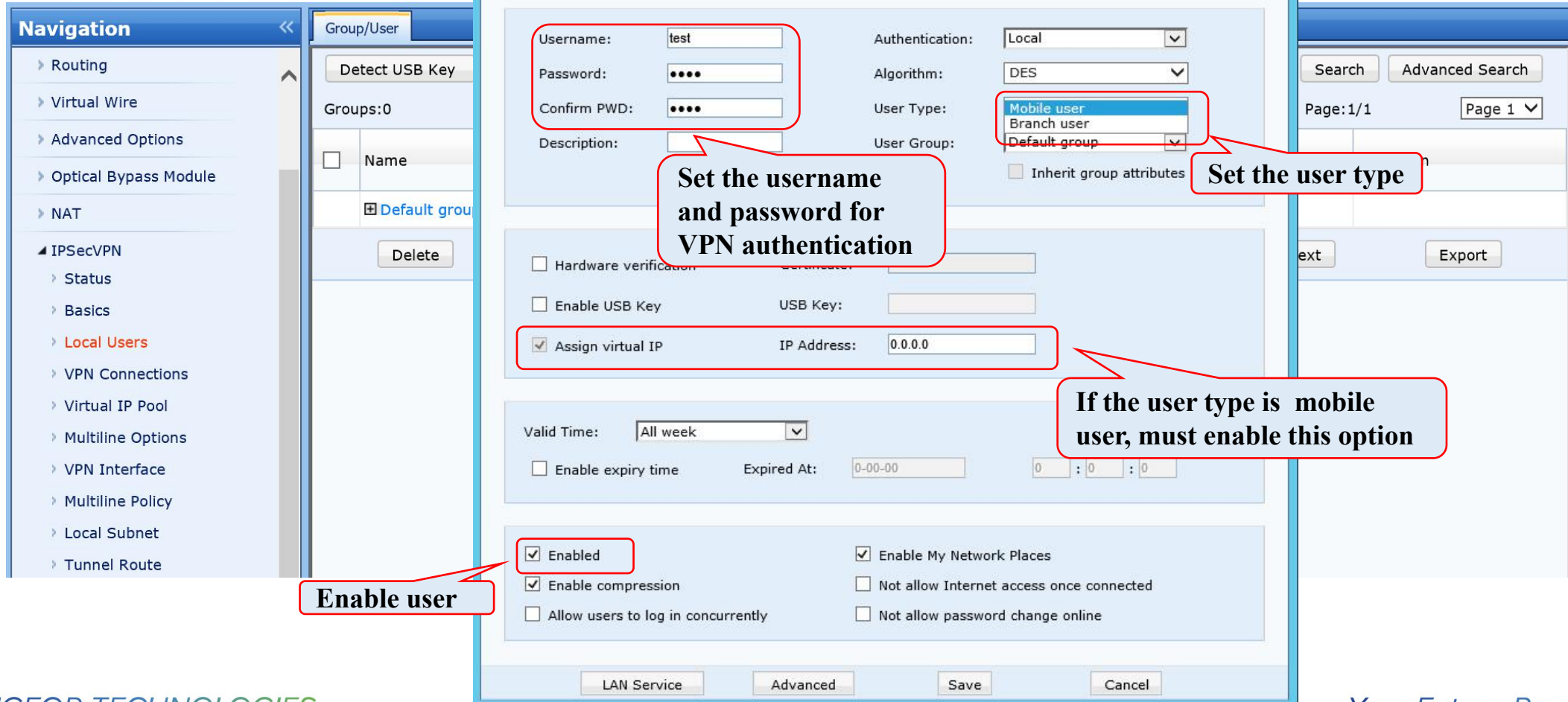
Annotations (red boxes with text) are present:

- Set the primary and secondary(optional) webagent(s).
- The ports need to be the same as webagent
- If set shared key here, branch/mobile need to set the same shared key for VPN connection.
- 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:



The screenshot displays the Sangfor VPN management interface. On the left is a 'Navigation' sidebar with options like Routing, Virtual Wire, Advanced Options, Optical Bypass Module, NAT, IPsecVPN, Status, Basics, Local Users, VPN Connections, Virtual IP Pool, Multiline Options, VPN Interface, Multiline Policy, Local Subnet, and Tunnel Route. The main area shows the 'Group/User' management page with a 'Detect USB Key' button and a table of users. Overlaid on this is a 'New User -- Webpage Dialog' window. The dialog has a 'Certificate error' message at the top. It contains fields for Username (test), Password (masked), Confirm PWD (masked), Authentication (Local), Algorithm (DES), User Type (Mobile user), User Group (Default group), and Description. Below these are checkboxes for Hardware verification, Enable USB Key, and Assign virtual IP (checked). The IP Address field is set to 0.0.0.0. There are also fields for Valid Time (All week), Enable expiry time, and Expired At. At the bottom, there are checkboxes for Enabled (checked), Enable compression, Allow users to log in concurrently, Enable My Network Places, Not allow Internet access once connected, and Not allow password change online. Annotations with red boxes and arrows point to specific fields: 'Set the username and password for VPN authentication' points to the Username and Password fields; 'Set the user type' points to the User Type dropdown; 'If the user type is mobile user, must enable this option' points to the 'Assign virtual IP' checkbox; and 'Enable user' points to the 'Enabled' checkbox.

Navigation

- Routing
- Virtual Wire
- Advanced Options
- Optical Bypass Module
- NAT
- IPsecVPN
 - Status
 - Basics
 - Local Users
 - VPN Connections
 - Virtual IP Pool
 - Multiline Options
 - VPN Interface
 - Multiline Policy
 - Local Subnet
 - Tunnel Route

Group/User

Detect USB Key

Groups:0

Name
Default group

Delete

New User -- Webpage Dialog

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

Username: test Password: **** Confirm PWD: **** Authentication: Local Algorithm: DES User Type: Mobile user User Group: Default group Description: Inherit group attributes

Set the username and password for VPN authentication

Set the user type

☐ Hardware verification ☐ Enable 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 access once connected ☐ Not allow password change online

LAN Service Advanced Save Cancel

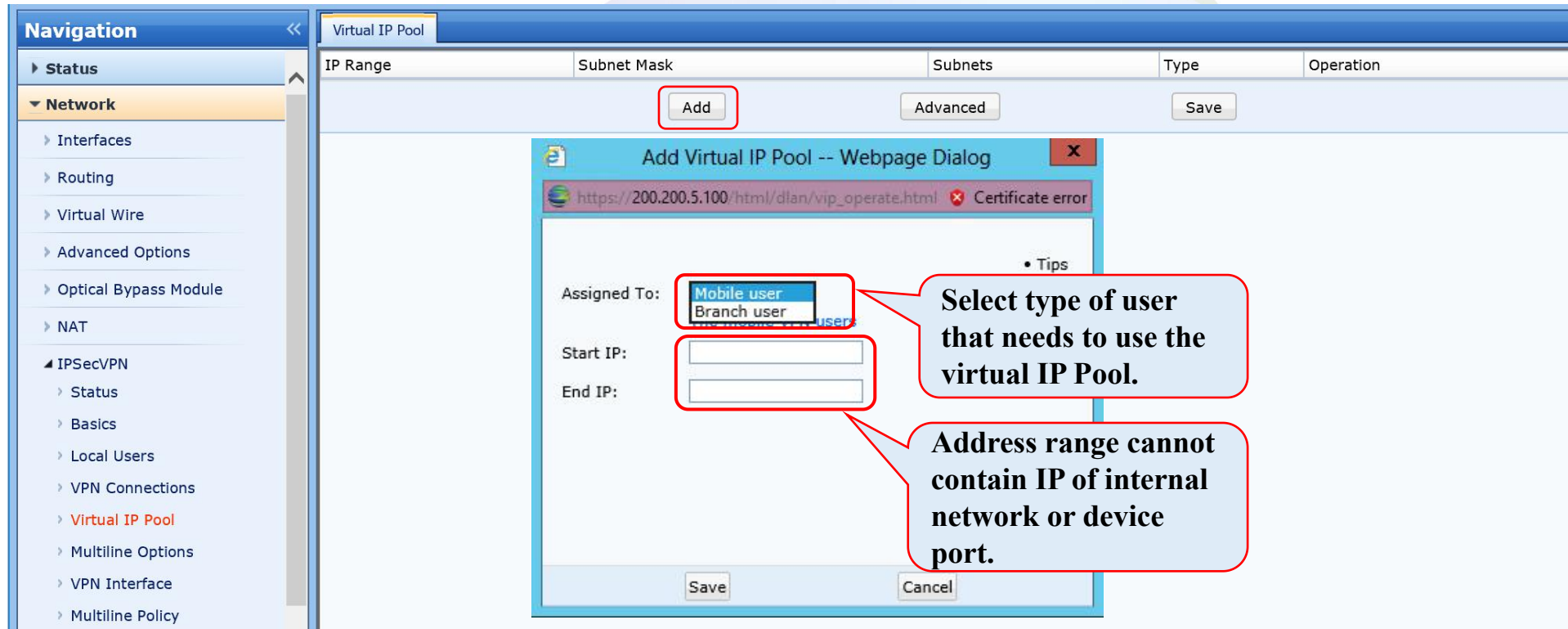
Search Advanced Search Page:1/1 Page 1

Export

Sangfor VPN

HQ setting:

Virtual IP Pool:



The screenshot displays the Sangfor VPN management interface. On the left is a navigation pane with a tree structure. The 'Virtual IP Pool' option under the 'IPSecVPN' section is highlighted. The main area shows the 'Virtual IP Pool' configuration page with a table header containing 'IP Range', 'Subnet Mask', 'Subnets', 'Type', and 'Operation'. An 'Add' button is highlighted with a red box. A 'Webpage Dialog' is open over the main area, titled 'Add Virtual IP Pool -- Webpage Dialog'. It shows a URL 'https://200.200.5.100/html/dlan/vip_operate.html' with a 'Certificate error' message. The dialog has fields for 'Assigned To:', 'Start IP:', and 'End IP:'. The 'Assigned To:' dropdown is open, showing 'Mobile user' and 'Branch user' as options. Two red callout boxes provide instructions: one points to the 'Assigned To:' dropdown with the text 'Select type of user that needs to use the virtual IP Pool.', and the other points to the 'Start IP:' and 'End IP:' fields with the text 'Address range cannot contain IP of internal network or device port.'.

Navigation

- Status
- Network
 - Interfaces
 - Routing
 - Virtual Wire
 - Advanced Options
 - Optical Bypass Module
 - NAT
 - IPSecVPN
 - Status
 - Basics
 - Local Users
 - VPN Connections
 - Virtual IP Pool
 - Multiline Options
 - VPN Interface
 - Multiline Policy

Virtual IP Pool

IP Range	Subnet Mask	Subnets	Type	Operation
----------	-------------	---------	------	-----------

Add Advanced Save

Add Virtual IP Pool -- Webpage Dialog

https://200.200.5.100/html/dlan/vip_operate.html Certificate error

Assigned To: Mobile user Branch user

Start IP:

End IP:

Save Cancel

• Tips

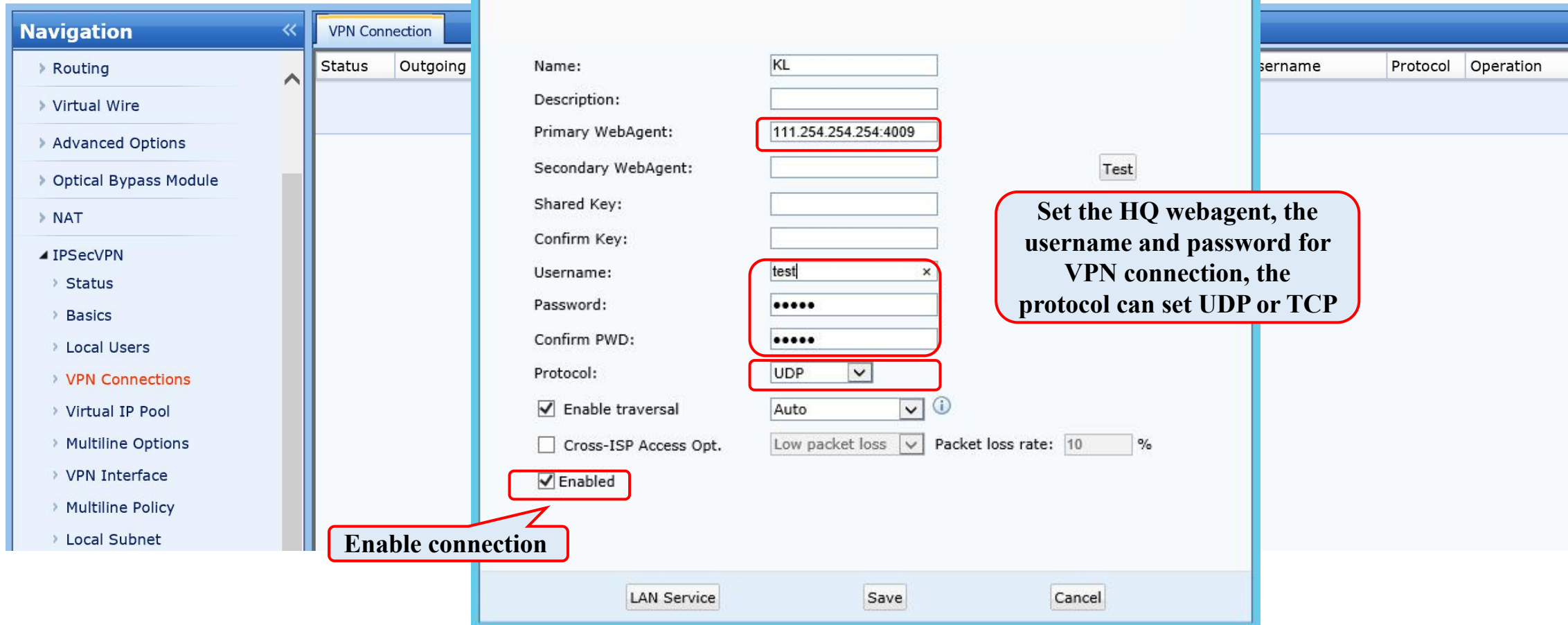
Select type of user that needs to use the virtual IP Pool.

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:



The screenshot displays the Sangfor VPN configuration interface. On the left is a 'Navigation' sidebar with a tree view containing: Routing, Virtual Wire, Advanced Options, Optical Bypass Module, NAT, IPsecVPN (expanded), Status, Basics, Local Users, **VPN Connections** (highlighted in orange), Virtual IP Pool, Multiline Options, VPN Interface, Multiline Policy, and Local Subnet. The main area shows the 'VPN Connection' tab with 'Status' and 'Outgoing' sub-tabs. A modal dialog titled 'Edit Outgoing Connection -- Webpage Dialog' is open, showing a 'Certificate error' at the top. The dialog contains the following fields and controls:

- Name: KL
- Description: (empty)
- Primary WebAgent: 111.254.254.254:4009 (highlighted with a red box)
- Secondary WebAgent: (empty)
- Shared Key: (empty)
- Confirm Key: (empty)
- Username: test (highlighted with a red box)
- Password: (masked with dots, highlighted with a red box)
- Confirm PWD: (masked with dots, highlighted with a red box)
- Protocol: UDP (highlighted with a red box)
- ☒ Enable traversal (set to Auto)
- ☐ Cross-ISP Access Opt. (set to Low packet loss)
- Packet loss rate: 10 %
- ☒ Enabled (highlighted with a red box and a callout bubble saying 'Enable connection')
- Buttons: LAN Service, Save, Cancel

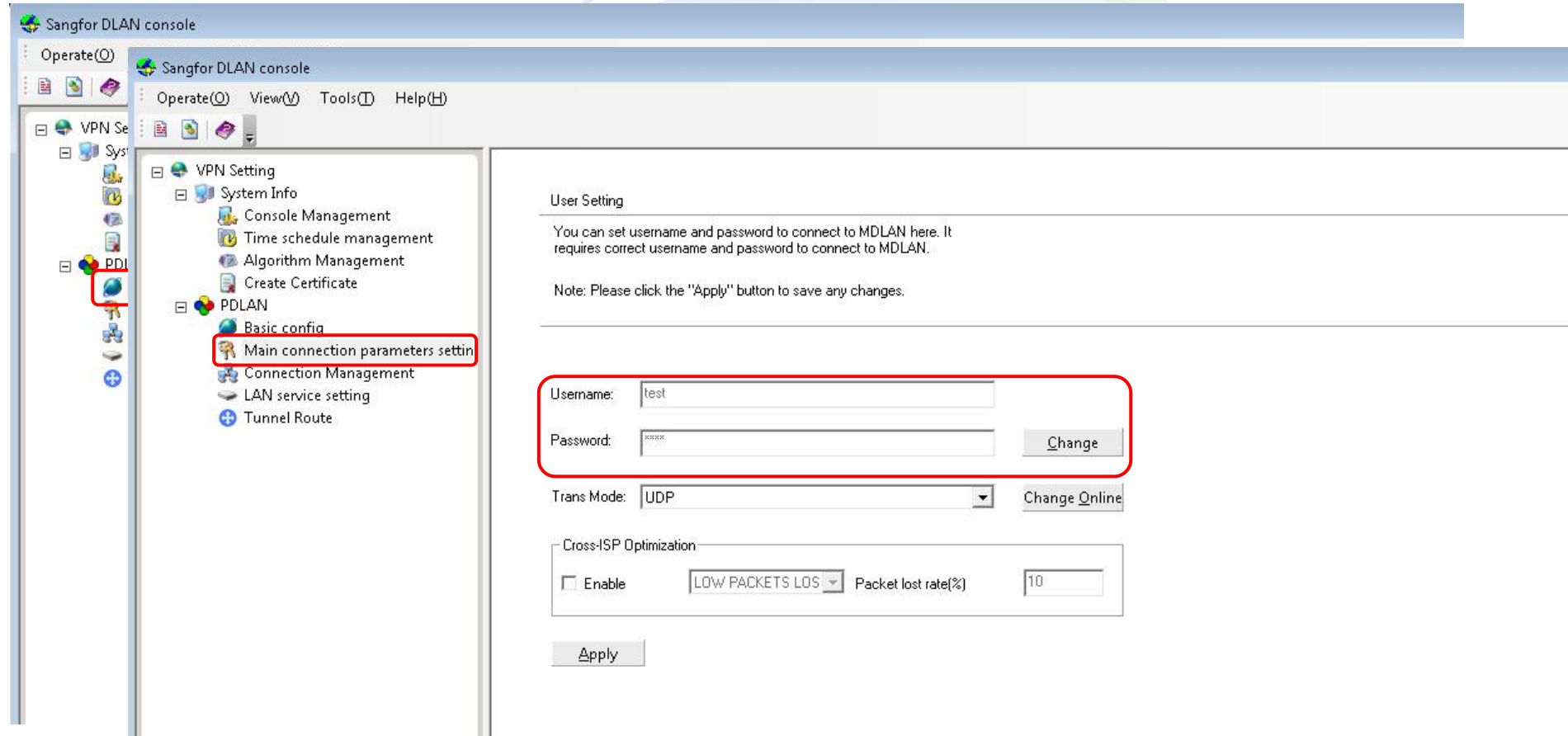
A red callout bubble on the right side of the dialog contains the text: 'Set the HQ webagent, the username and password for VPN connection, the protocol can set UDP or TCP'.

Sangfor VPN



Mobile (PDLAN):

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



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



SANGFOR
深信服科技

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;

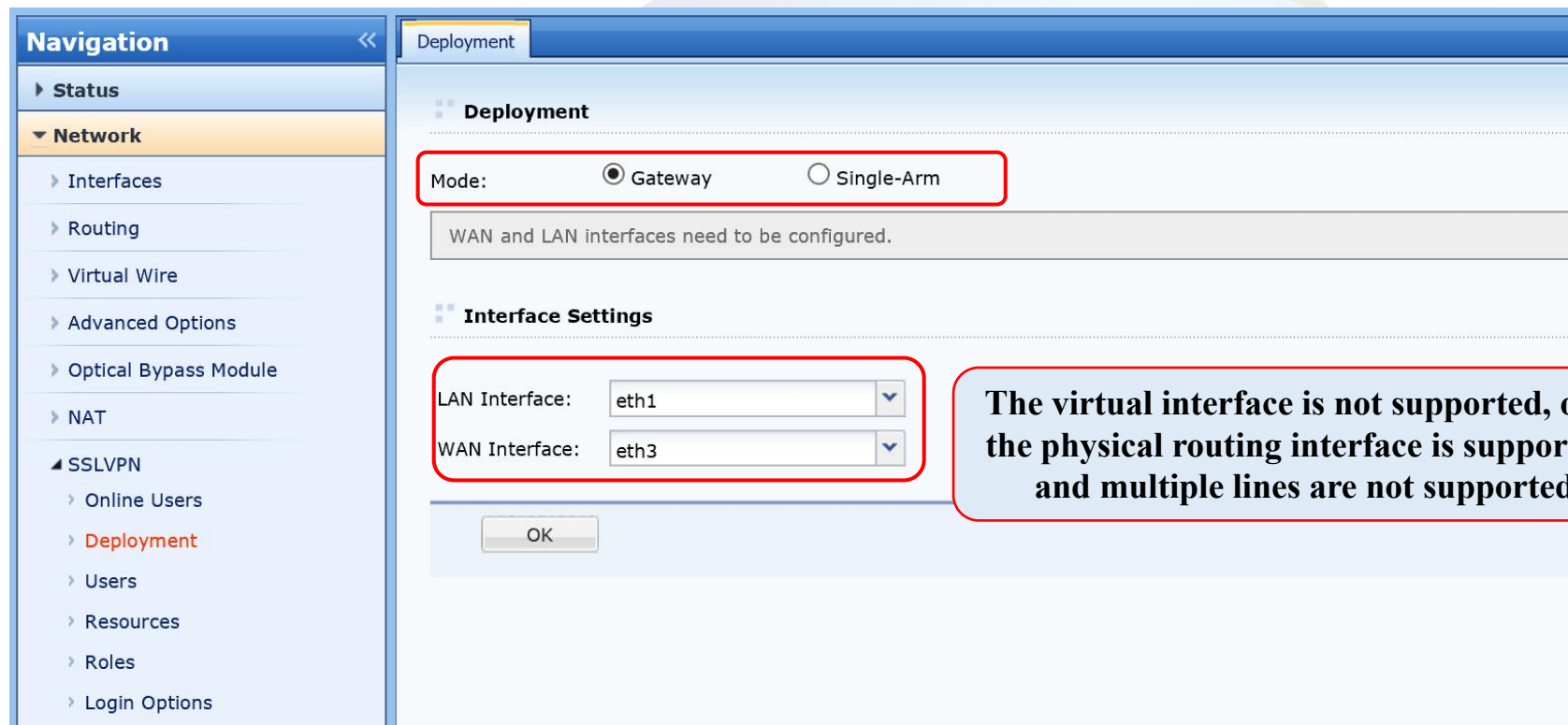
Android 4.0 and later versions;

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

SSL VPN

SSL VPN setting:

SSL Deployment:



Navigation <<

- Status
- ▼ **Network**
 - Interfaces
 - Routing
 - Virtual Wire
 - Advanced Options
 - Optical Bypass Module
 - NAT
 - ▲ **SSLVPN**
 - Online Users
 - **Deployment**
 - Users
 - Resources
 - Roles
 - Login Options

Deployment

Deployment

Mode: ☒ Gateway ☐ Single-Arm

WAN and LAN interfaces need to be configured.

Interface Settings

LAN Interface: eth1

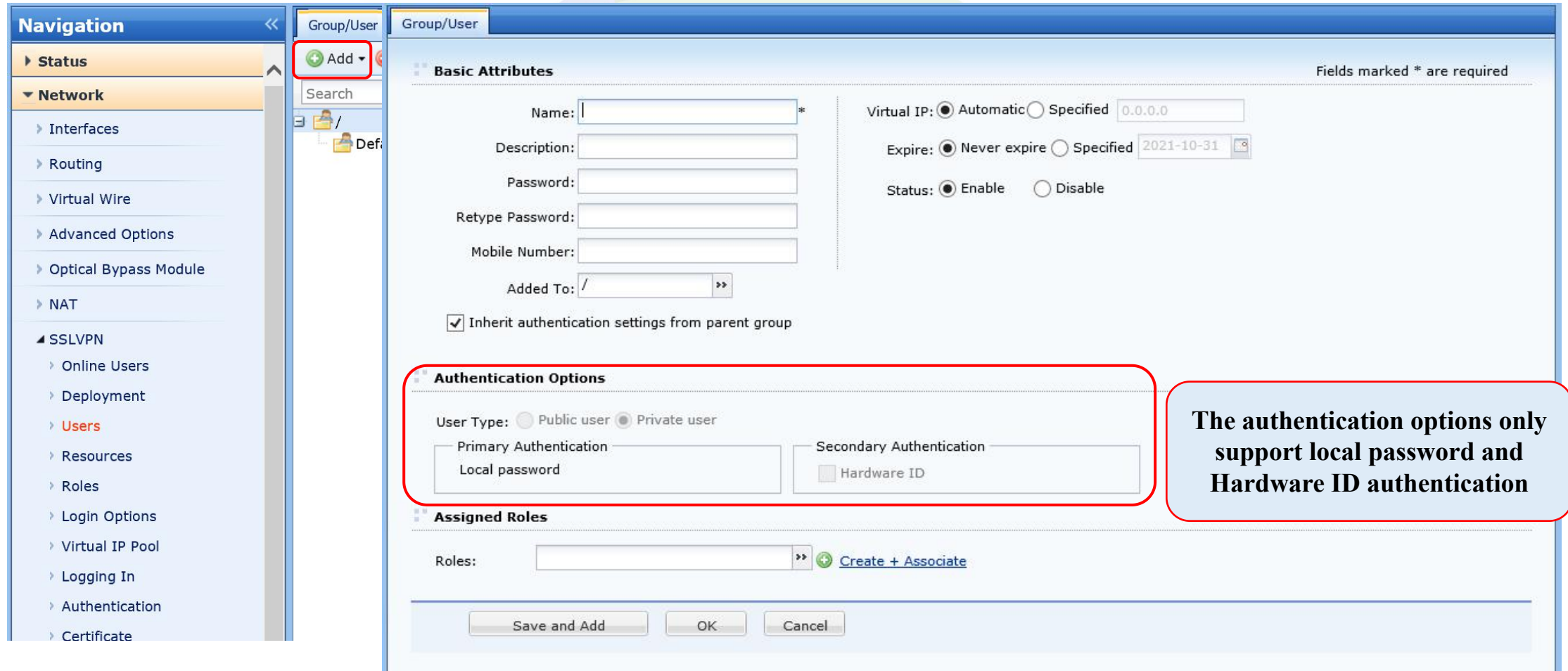
WAN Interface: eth3

OK

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

SSL VPN

Users management:



Navigation

- Status
- ▼ Network
 - Interfaces
 - Routing
 - Virtual Wire
 - Advanced Options
 - Optical Bypass Module
 - NAT
- ▲ SSLVPN
 - Online Users
 - Deployment
 - **Users**
 - Resources
 - Roles
 - Login Options
 - Virtual IP Pool
 - Logging In
 - Authentication
 - Certificate

Group/User

Basic Attributes Fields marked * are required

Name: *

Description:

Password:

Retype Password:

Mobile Number:

Added To: >>

☒ Inherit authentication settings from parent group

Authentication Options

User Type: ☐ Public user ☒ Private user

Primary Authentication: Local password

Secondary Authentication: Hardware ID

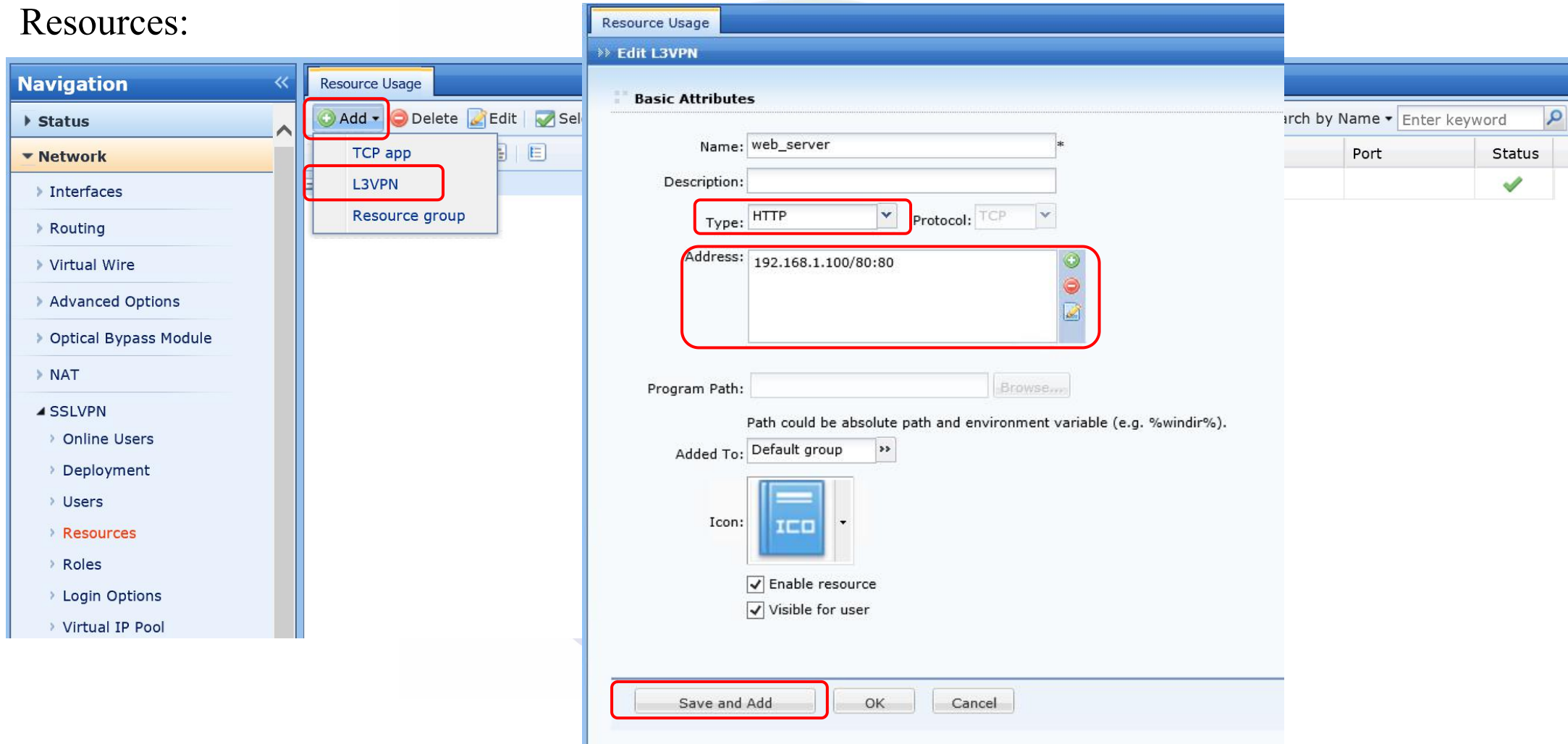
Assigned Roles

Roles: >> [Create + Associate](#)

The authentication options only support local password and Hardware ID authentication

SSL VPN

Resources:



The screenshot displays the Sangfor SSL VPN management interface. On the left, the 'Navigation' pane shows the 'Network' section expanded, with 'SSLVPN' selected. The 'Resource Usage' tab is active, showing a list of resources. The 'Add' button is highlighted, and a dropdown menu shows 'TCP app', 'L3VPN', and 'Resource group'. The 'L3VPN' option is selected. The 'Edit L3VPN' dialog box is open, showing the 'Basic Attributes' section. The 'Name' field is 'web_server'. The 'Description' field is empty. The 'Type' dropdown is set to 'HTTP', and the 'Protocol' dropdown is set to 'TCP'. The 'Address' field is '192.168.1.100/80:80'. The 'Program Path' field is empty, with a 'Browse...' button. The 'Added To' dropdown is set to 'Default group'. The 'Icon' dropdown is set to 'ICO'. The 'Enable resource' and 'Visible for user' checkboxes are checked. The 'Save and Add' button is highlighted.

Navigation

- Status
- ▼ Network
 - Interfaces
 - Routing
 - Virtual Wire
 - Advanced Options
 - Optical Bypass Module
 - NAT
 - ▲ SSLVPN
 - Online Users
 - Deployment
 - Users
 - Resources
 - Roles
 - Login Options
 - Virtual IP Pool

Resource Usage

- Add
- Delete
- Edit
- Select

TCP app
L3VPN
Resource group

Edit L3VPN

Basic Attributes

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

Save and Add OK Cancel

SSL VPN

Roles:

Navigation

- Status
- ▼ Network
 - Interfaces
 - Routing
 - Virtual Wire
 - Advanced Options
 - Optical Bypass Module
- NAT
- ▲ SSLVPN
 - Online Users
 - Deployment
 - Users
 - Resources
 - **Roles**
 - Login Options
 - Virtual IP Pool

Roles

+ Add - Delete

Add Role

By using template

Roles

Basic Attributes

Name: max access web_server *

Description:

Assigned To: max

☒ Enable Role

Associated Resources

Select Resource

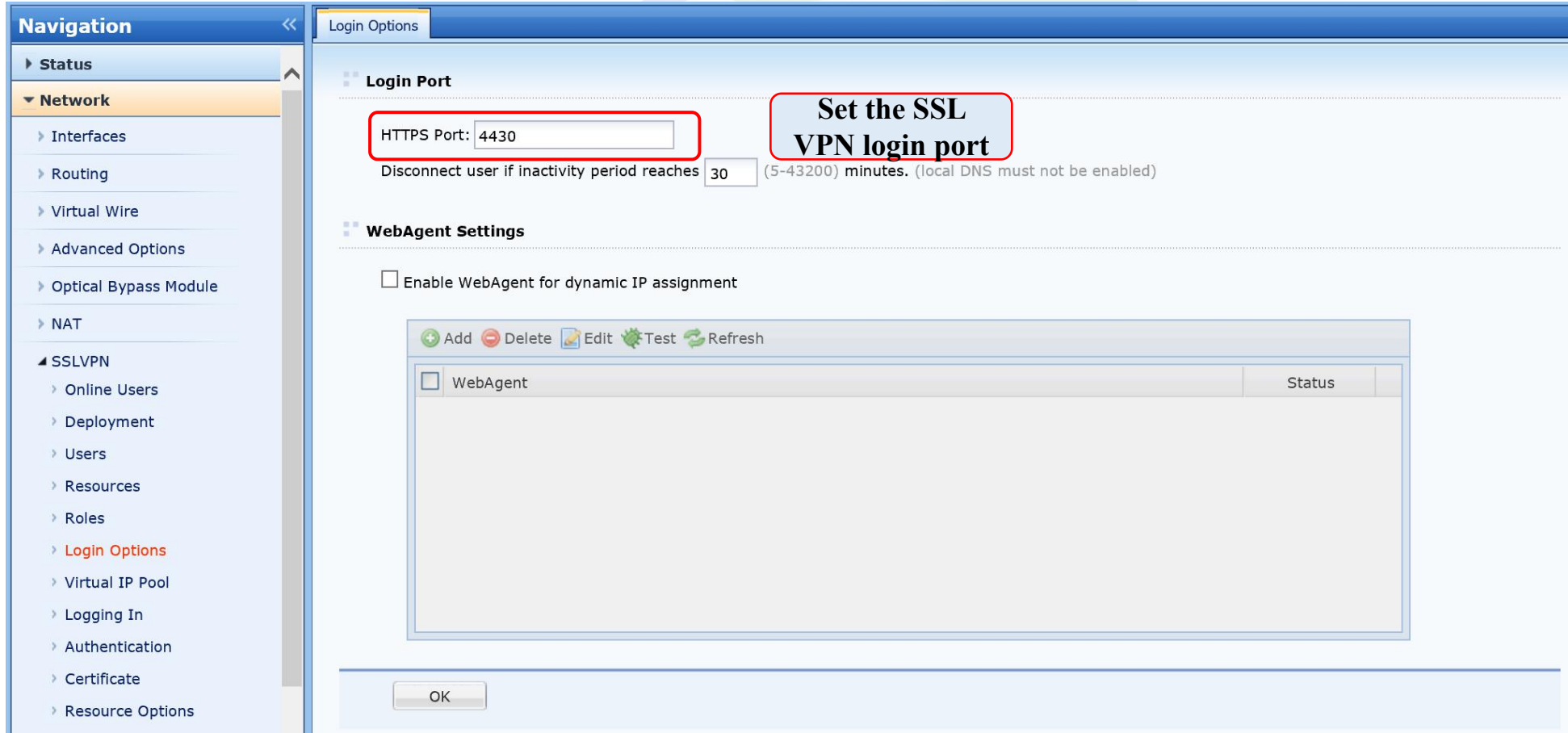
Name	Type	Description
web_server	HTTP	

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

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

SSL VPN

Login Options:



Navigation

- Status
- ▼ Network
 - Interfaces
 - Routing
 - Virtual Wire
 - Advanced Options
 - Optical Bypass Module
 - NAT
- ▲ SSLVPN
 - Online Users
 - Deployment
 - Users
 - Resources
 - Roles
 - Login Options
 - Virtual IP Pool
 - Logging In
 - Authentication
 - Certificate
 - Resource Options

Login Options

Login Port

HTTPS Port:

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

WebAgent Settings

☐ Enable WebAgent for dynamic IP assignment

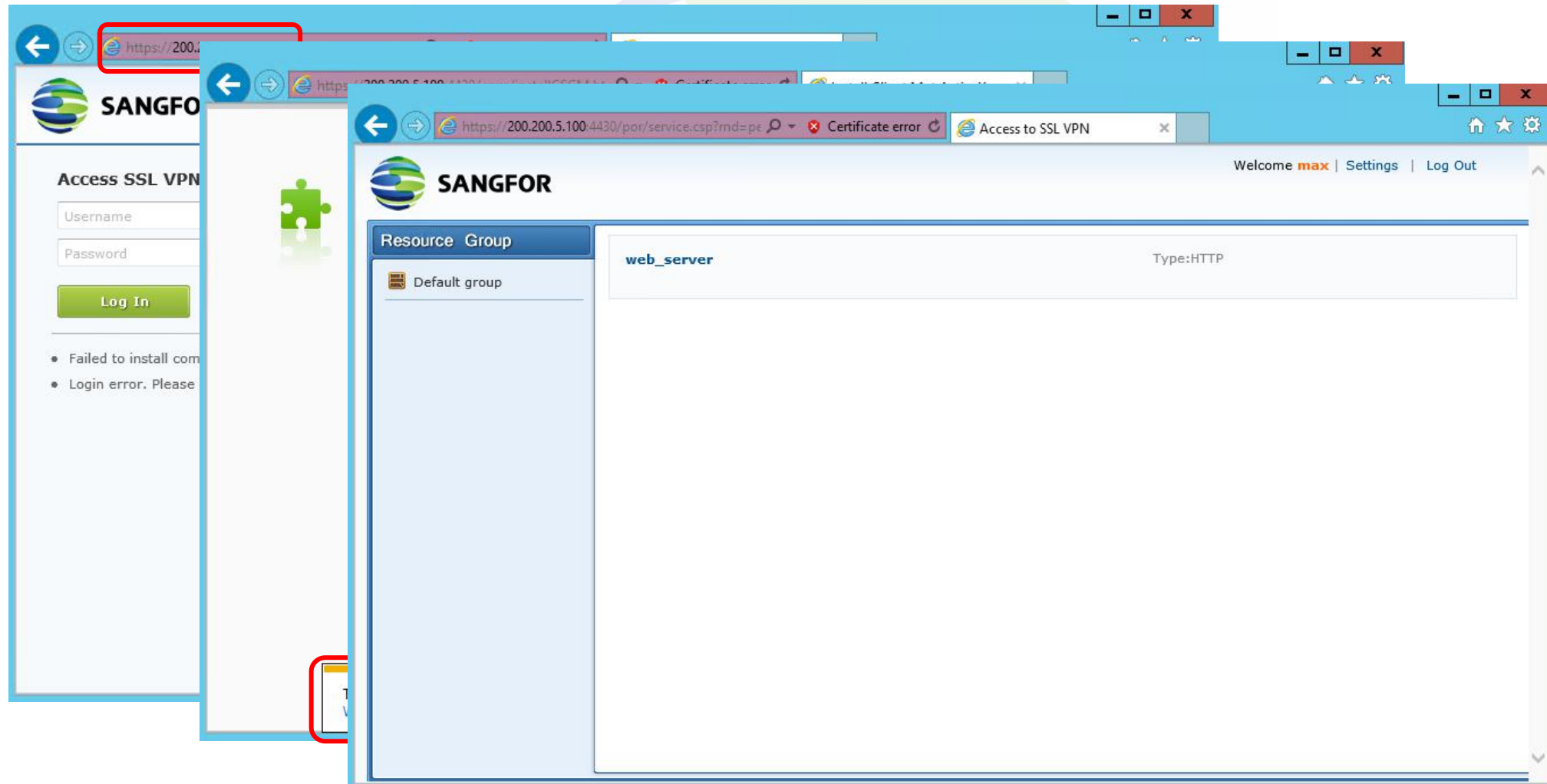
Add Delete Edit Test Refresh

<input type="checkbox"/>	WebAgent	Status
--------------------------	----------	--------

OK

SSL VPN

Client access to SSL VPN:



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)

