

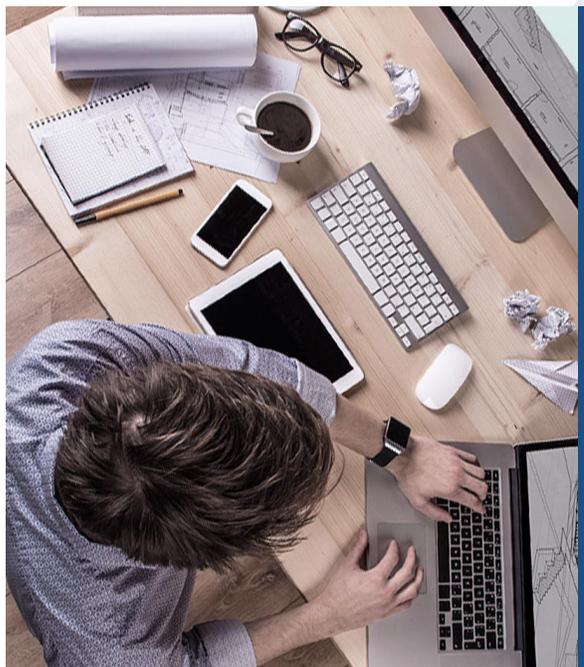


SANGFOR

Sangfor NGAF v8.0.6 Associate

VPN





1 IPsec VPN

2 Sangfor VPN

3 SSL VPN

1. IPSec VPN



IPSEC VPN

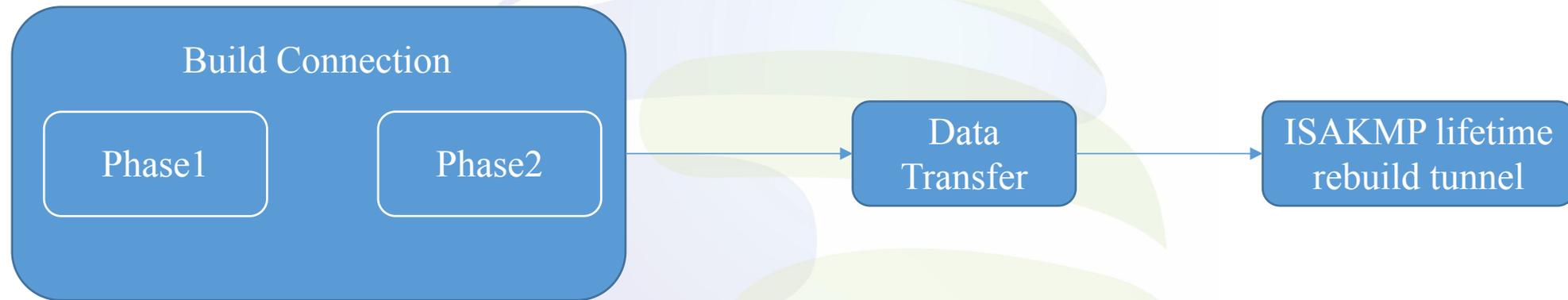
A virtual private network (VPN) extends a private network across a public network, and enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network.

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



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:

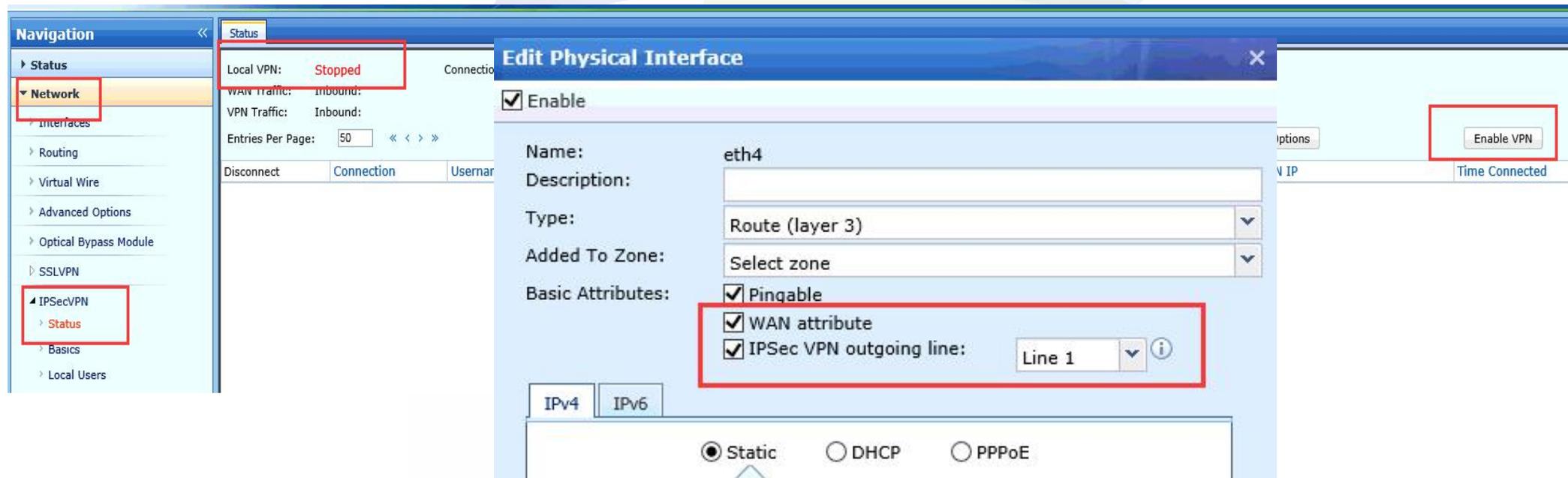


2. Since version 8.0.2, WAN-attribute route interface (non-management interface Eth0) no longer required in IPsec.

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 'Network' and 'IPSecVPN' expanded, with 'Status' selected. The main area shows the 'Status' of the VPN service as 'Stopped'. A modal window titled 'Edit Physical Interface' is open for the 'eth4' interface. In this window, the 'Enable' checkbox is checked, and the 'Basic Attributes' section is highlighted with a red box, showing 'WAN attribute' and 'IPSec VPN outgoing line' (set to 'Line 1') both checked. An 'Enable VPN' button is also highlighted with a red box in the top right corner of the modal.

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.

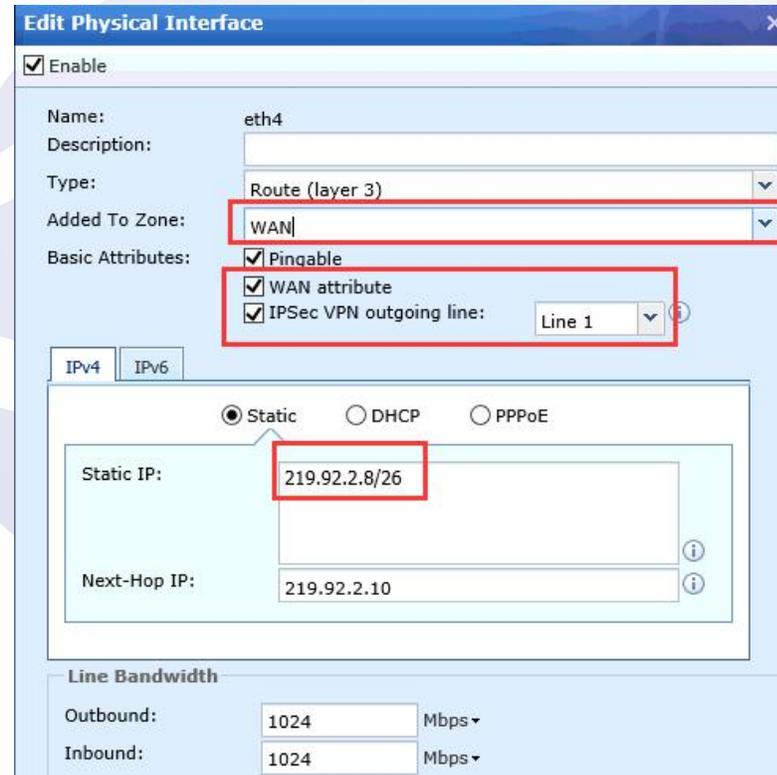
Customer want to side intranet visit each other via IPsec VPN



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

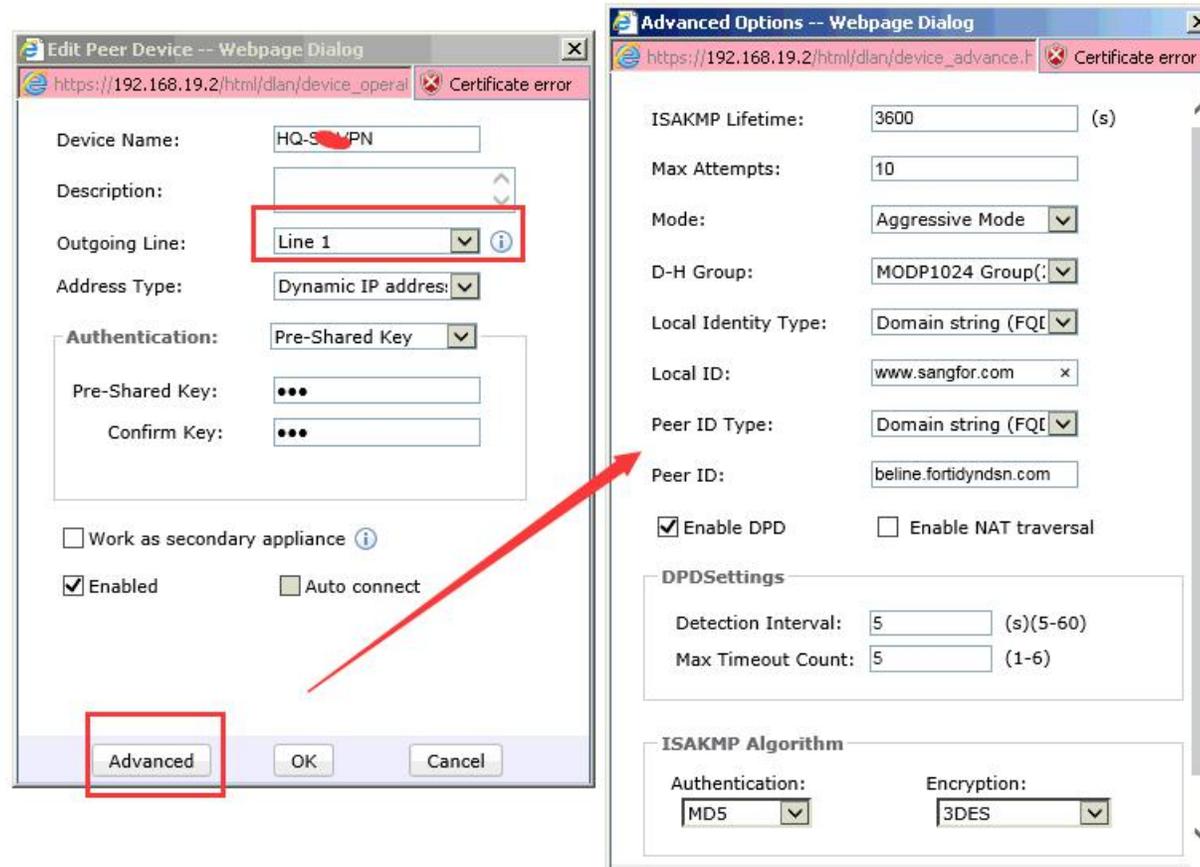
Static DHCP PPPoE

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.



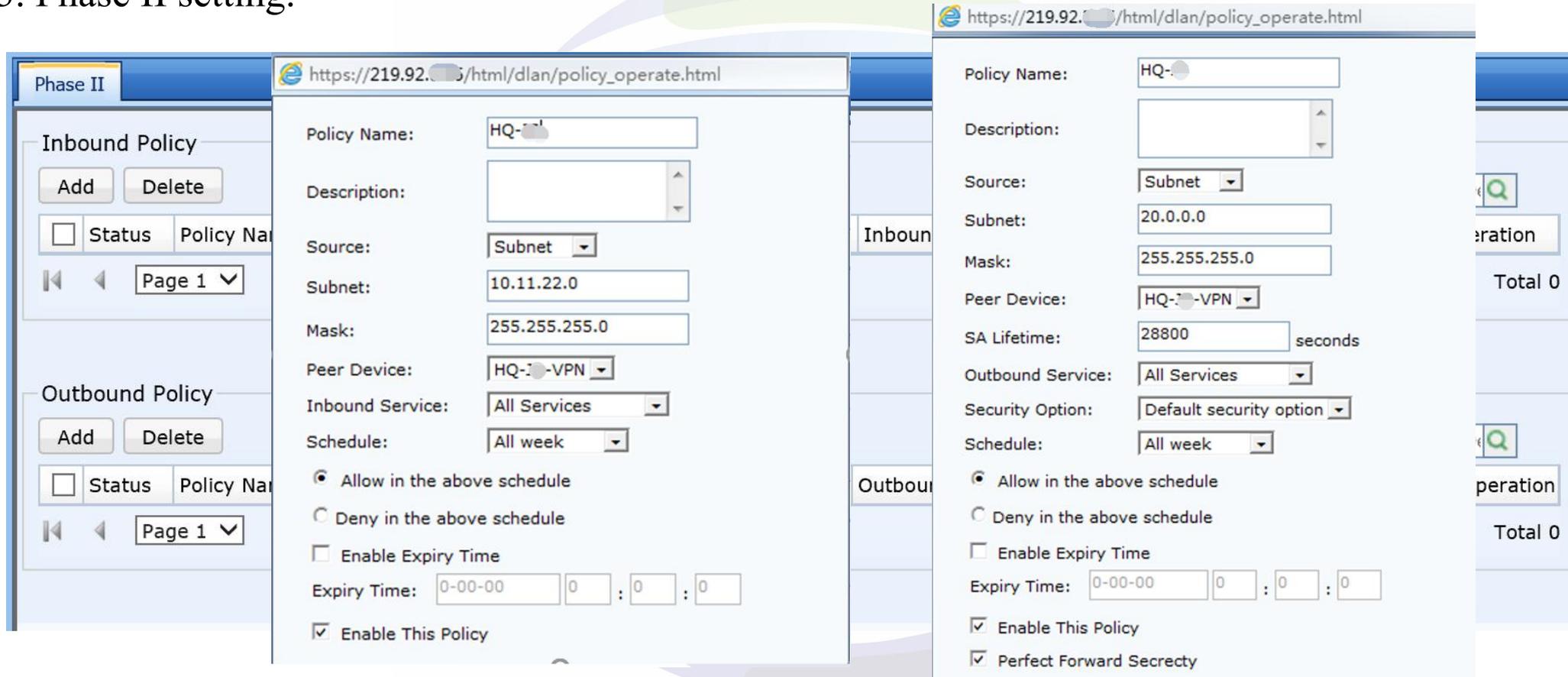
The image shows two overlapping web browser windows. The left window, titled "Edit Peer Device -- Webpage Dialog", displays the main configuration for a peer device named "HQ-S-VPN". The "Outgoing Line" is set to "Line 1", and the "Authentication" is set to "Pre-Shared Key". The "Advanced" button at the bottom is highlighted with a red box. A red arrow points from this button to the right window.

The right window, titled "Advanced Options -- Webpage Dialog", shows the detailed Phase I settings:

- 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.



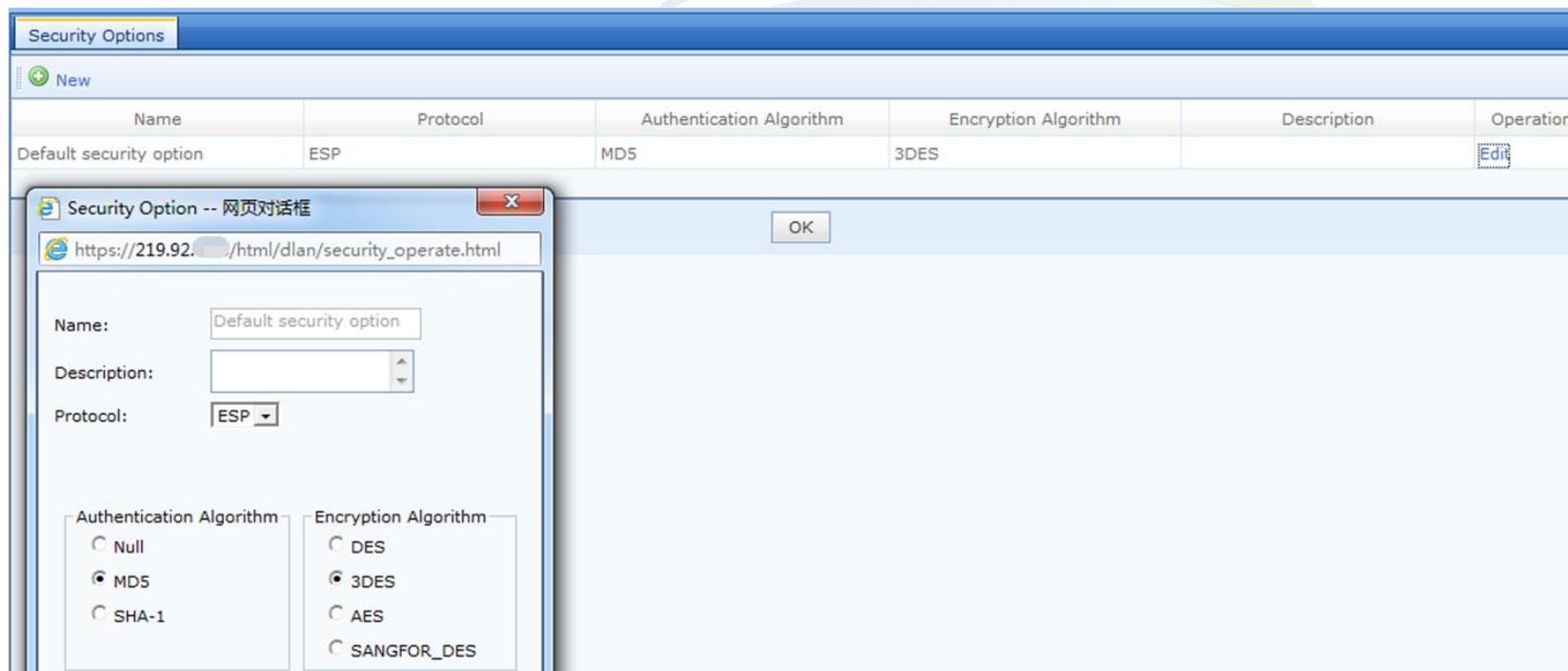
The screenshot displays the Phase II configuration interface for IPSEC VPN. It is divided into two main sections: Inbound Policy and Outbound Policy. Each section includes a list of policies with 'Add' and 'Delete' buttons, and a detailed configuration form for a selected policy. The Inbound policy is named 'HQ-VPN' and is configured with Source: Subnet, Subnet: 10.11.22.0, Mask: 255.255.255.0, Peer Device: HQ-VPN, Inbound Service: All Services, and Schedule: All week. The Outbound policy is also named 'HQ-VPN' and is configured with Source: Subnet, Subnet: 20.0.0.0, Mask: 255.255.255.0, Peer Device: HQ-VPN, Outbound Service: All Services, and Schedule: All week. Both policies are set to 'Allow in the above schedule' and have 'Enable This Policy' checked. The interface also shows a search bar and a 'Total 0' indicator for each policy list.

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. /html/dlan/security_operate.html

Name: Default security option

Description:

Protocol: ESP

Authentication Algorithm:

- Null
- MD5
- SHA-1

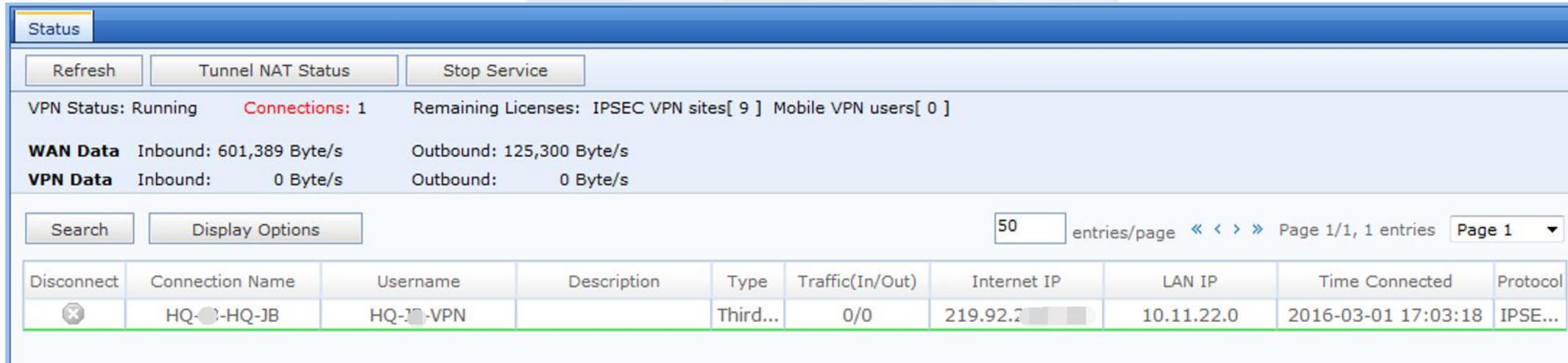
Encryption Algorithm:

- DES
- 3DES
- AES
- SANGFOR_DES

OK

IPSEC VPN

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



Status

Refresh Tunnel NAT Status Stop Service

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

Search Display Options 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-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.

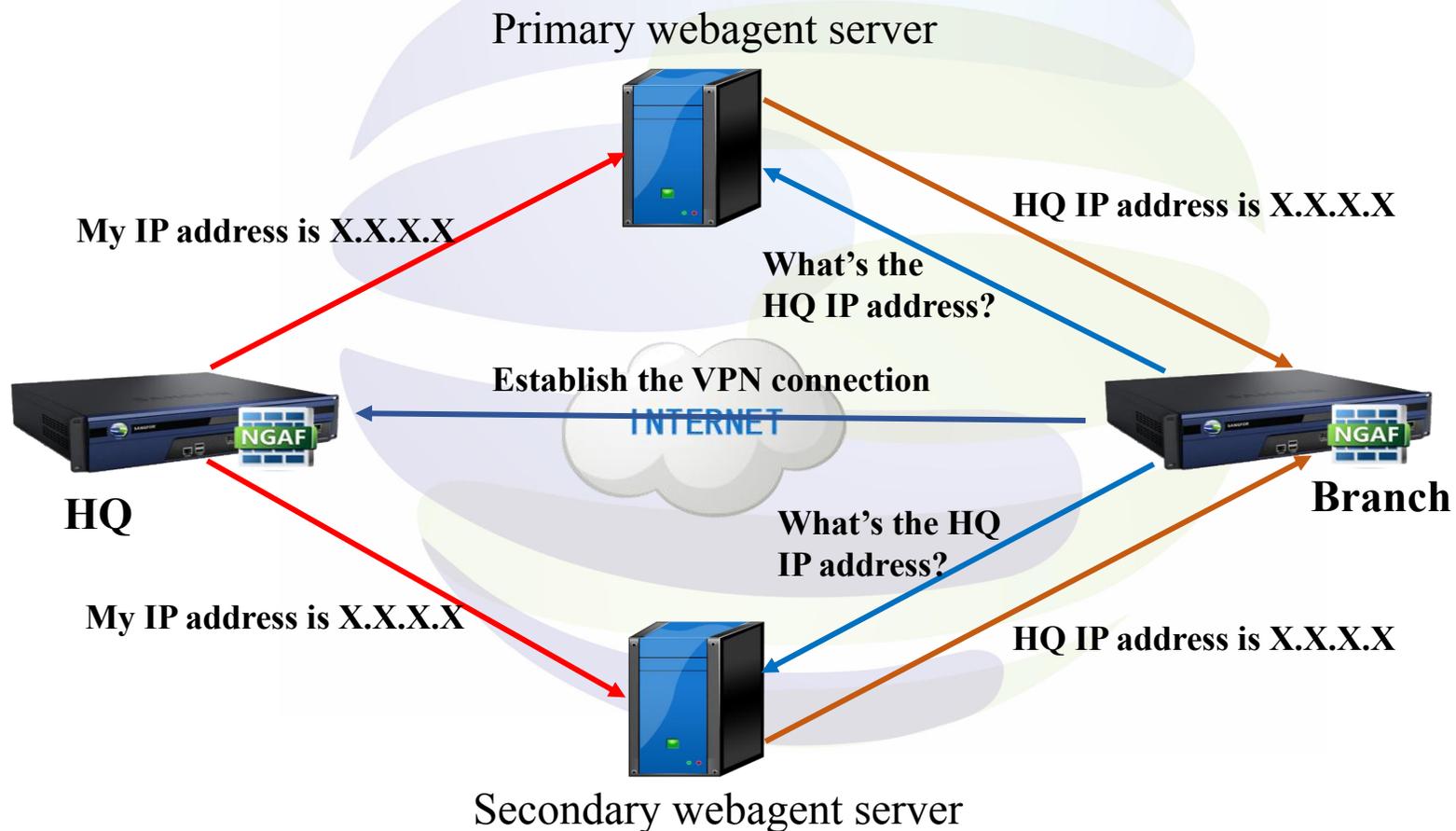
3. Web URL format, such as: webagent.sangfor.com.cn/webagent/123.php

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

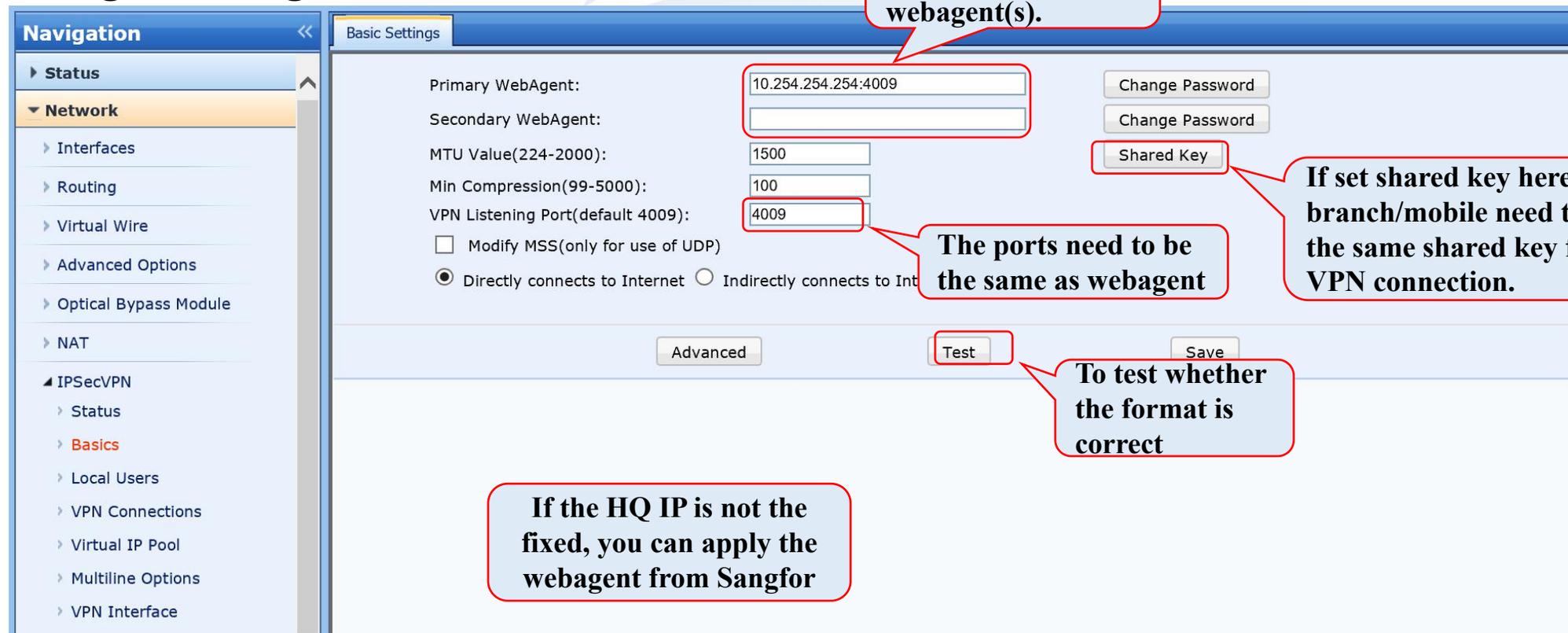
The basic configurations for establishing a VPN connection between HQ and branch or mobile are as follow:

- (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 like Status, Network, Interfaces, Routing, Virtual Wire, Advanced Options, Optical Bypass Module, NAT, and IPsecVPN. The main content area is titled 'Basic Settings' and includes fields for Primary WebAgent (10.254.254.254:4009), Secondary WebAgent, MTU Value (1500), Min Compression (100), and VPN Listening Port (4009). There are also checkboxes for 'Modify MSS' and connection options ('Directly connects to Internet' is selected). Buttons for 'Change Password', 'Shared Key', 'Advanced', 'Test', and 'Save' are visible. Five callout boxes provide instructions: 1. 'Set the primary and secondary(optional) webagent(s)' points to the Primary and Secondary WebAgent fields. 2. 'The ports need to be the same as webagent' points to the VPN Listening Port field. 3. 'If set shared key here, branch/mobile need to set the same shared key for VPN connection.' points to the Shared Key field. 4. 'To test whether the format is correct' points to the Test button. 5. 'If the HQ IP is not the fixed, you can apply the webagent from Sangfor' points to the Primary WebAgent field.

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

Basic Settings

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 Internet

Change Password

Change Password

Shared Key

Advanced

Test

Save

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.

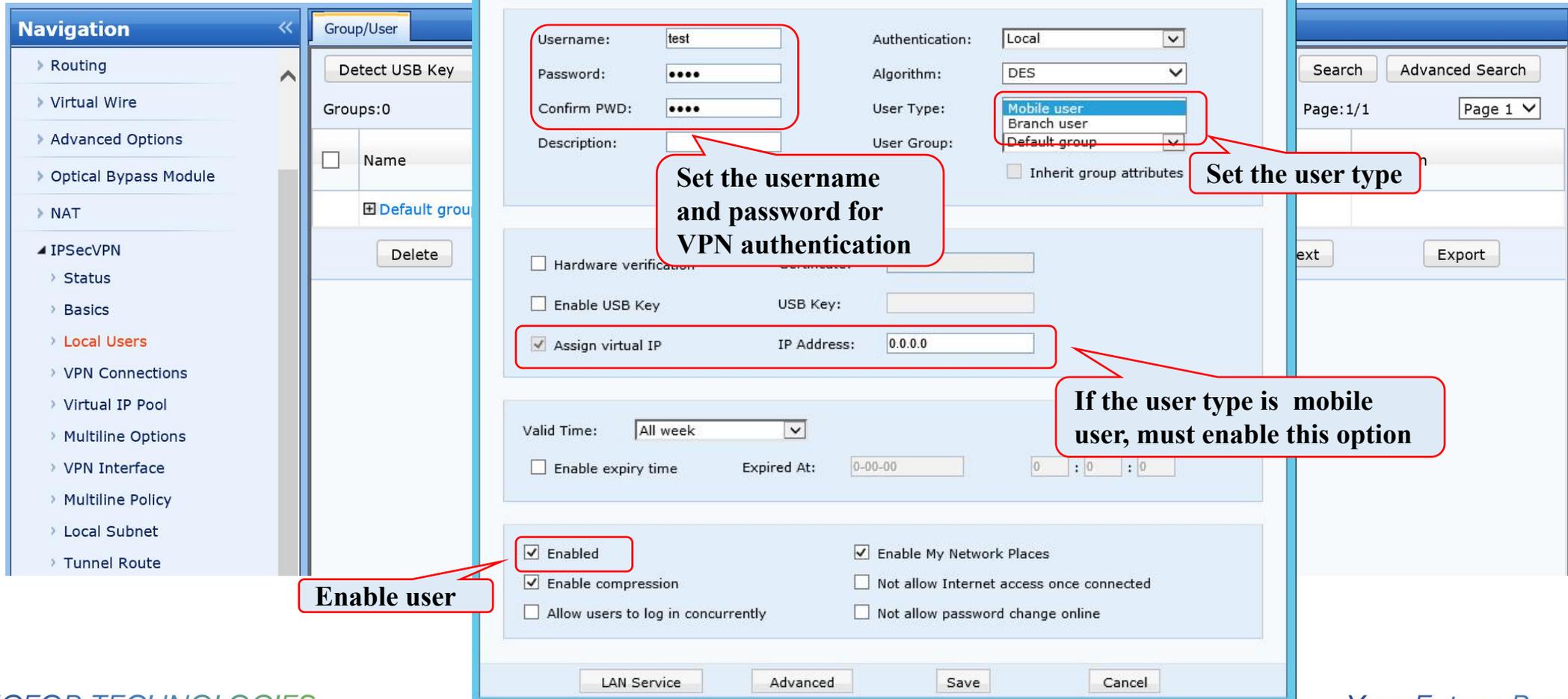
To test whether the format is correct

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 menu with categories like Routing, Virtual Wire, and IPsecVPN. The main area shows the 'New User -- Webpage Dialog' window. This dialog has several sections: 'Basic Information' with fields for Username (test), Password (masked), Confirm PWD (masked), and Description; 'Authentication' with dropdowns for Local, DES, and User Type (Mobile user selected); 'Advanced Settings' with checkboxes for Hardware verification, Enable USB Key, and Assign virtual IP (checked with IP Address 0.0.0.0); and 'User Management' with checkboxes for Enabled, Enable compression, Allow users to log in concurrently, Enable My Network Places, and Not allow Internet access once connected. Red callout boxes highlight these key settings.

Set the username and password for VPN authentication

Set the user type

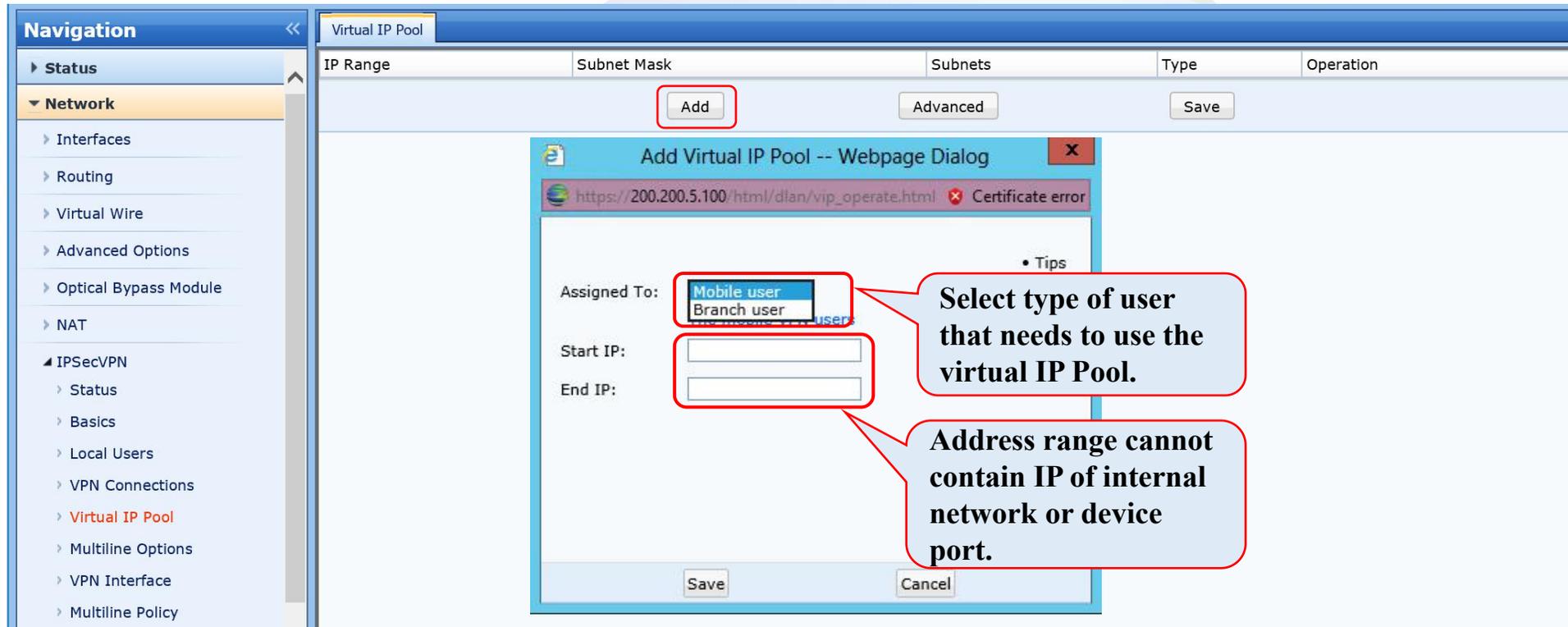
If the user type is mobile user, must enable this option

Enable user

Sangfor VPN

HQ setting:

Virtual IP Pool:



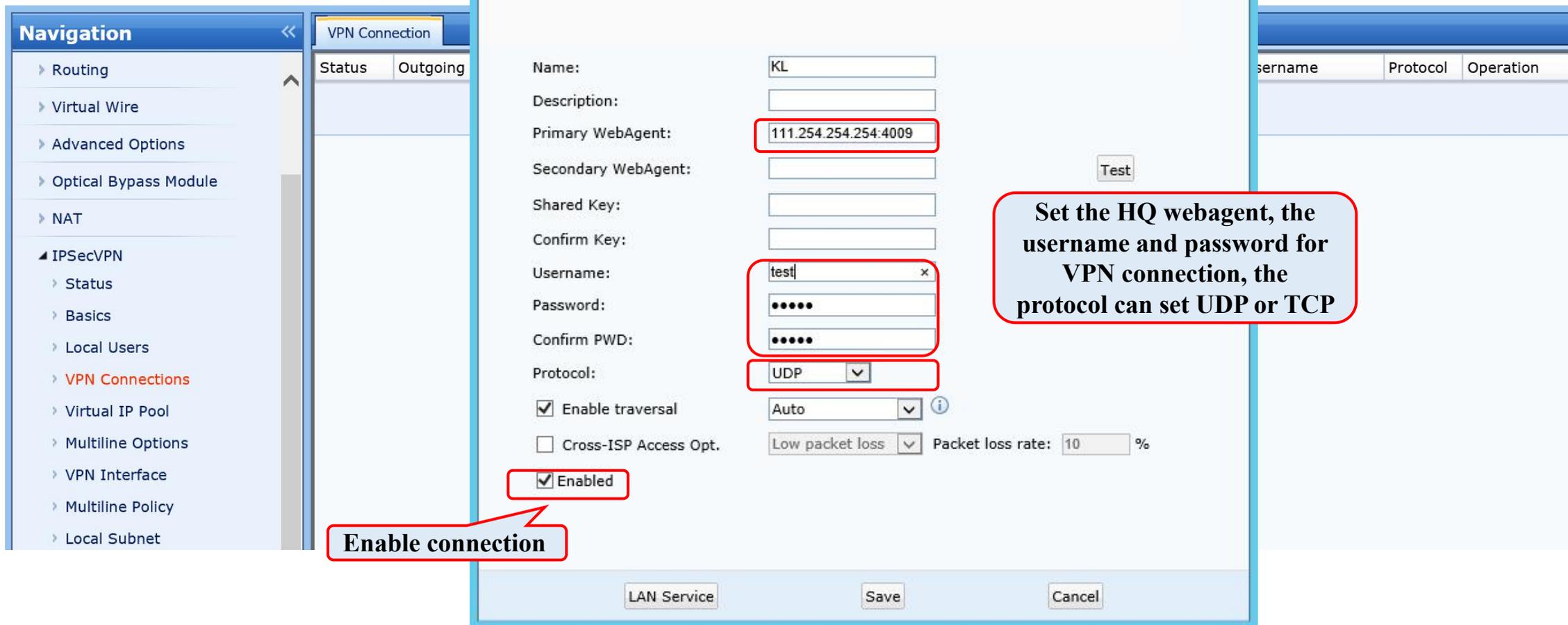
The screenshot shows the Sangfor VPN management interface. On the left is a navigation menu with categories like Status, Network, and IPsecVPN. The main area displays the 'Virtual IP Pool' configuration page. A table with columns 'IP Range', 'Subnet Mask', 'Subnets', 'Type', and 'Operation' is visible, with an 'Add' button highlighted. A 'Webpage Dialog' is open, titled 'Add Virtual IP Pool -- Webpage Dialog'. It contains a 'Certificate error' message and a 'Tips' section. The 'Assigned To' dropdown is set to 'Mobile user'. Below it are 'Start IP' and 'End IP' input fields. Two callouts provide instructions: one points to the 'Assigned To' dropdown stating 'Select type of user that needs to use the virtual IP Pool.', and another points to the IP input fields stating '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, a navigation pane shows the 'VPN Connections' section expanded. The main area shows the 'Edit Outgoing Connection -- Webpage Dialog' window. The dialog contains the following fields and settings:

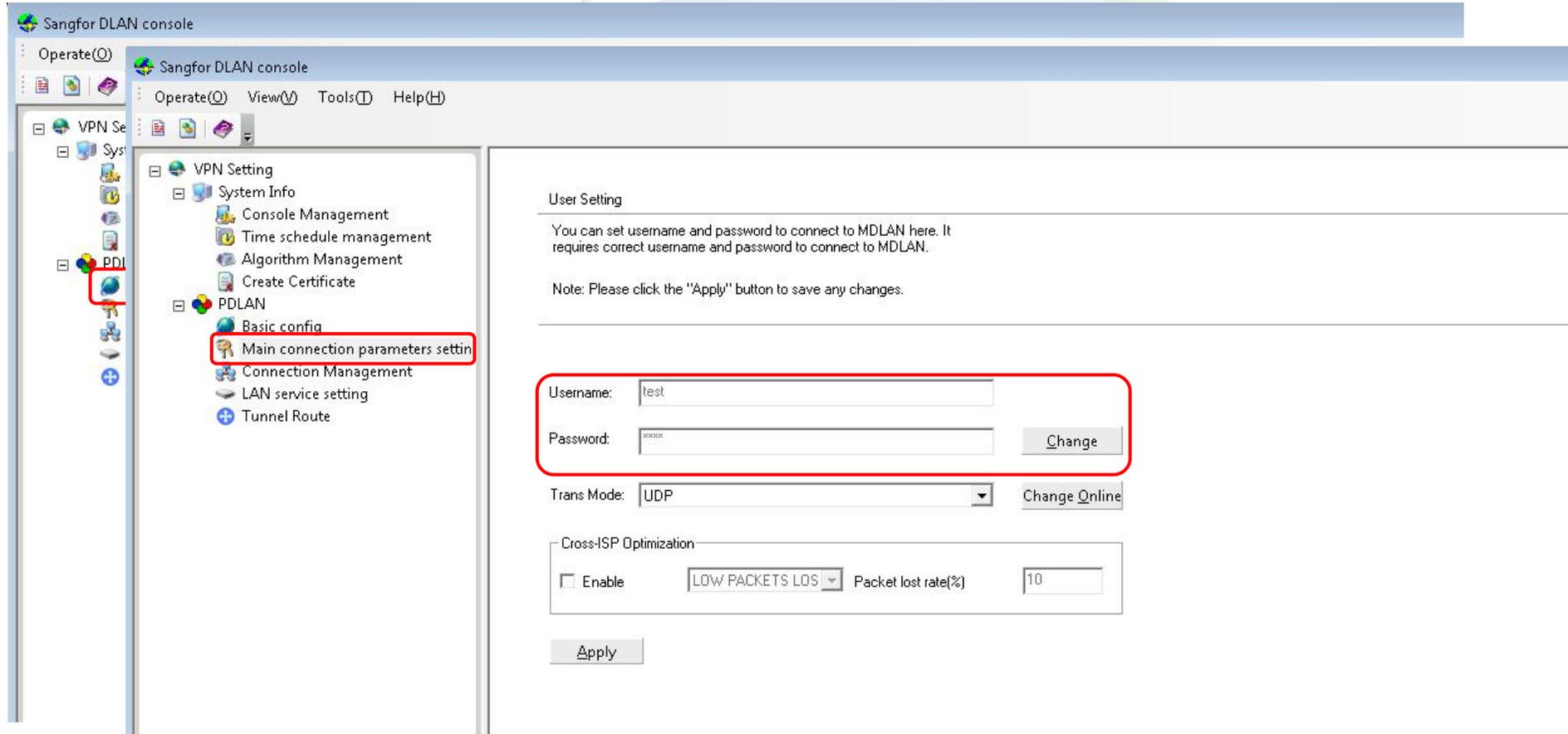
- Name: KL
- Description: (empty)
- Primary WebAgent: 111.254.254.254:4009
- Secondary WebAgent: (empty)
- Shared Key: (empty)
- Confirm Key: (empty)
- Username: test
- Password: (masked with dots)
- Confirm PWD: (masked with dots)
- Protocol: UDP
- Enable traversal: Auto
- Cross-ISP Access Opt.: Low packet loss
- Packet loss rate: 10 %
- Enabled

Annotations in red boxes highlight the 'Enabled' checkbox, the 'Primary WebAgent' field, the 'Username' field, and the 'Protocol' dropdown. A text box on the right states: 'Set the HQ webagent, the username and password for VPN connection, the protocol can set UDP or TCP'. The dialog also features a 'Test' button and 'LAN Service', 'Save', and 'Cancel' buttons at the bottom.

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



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;

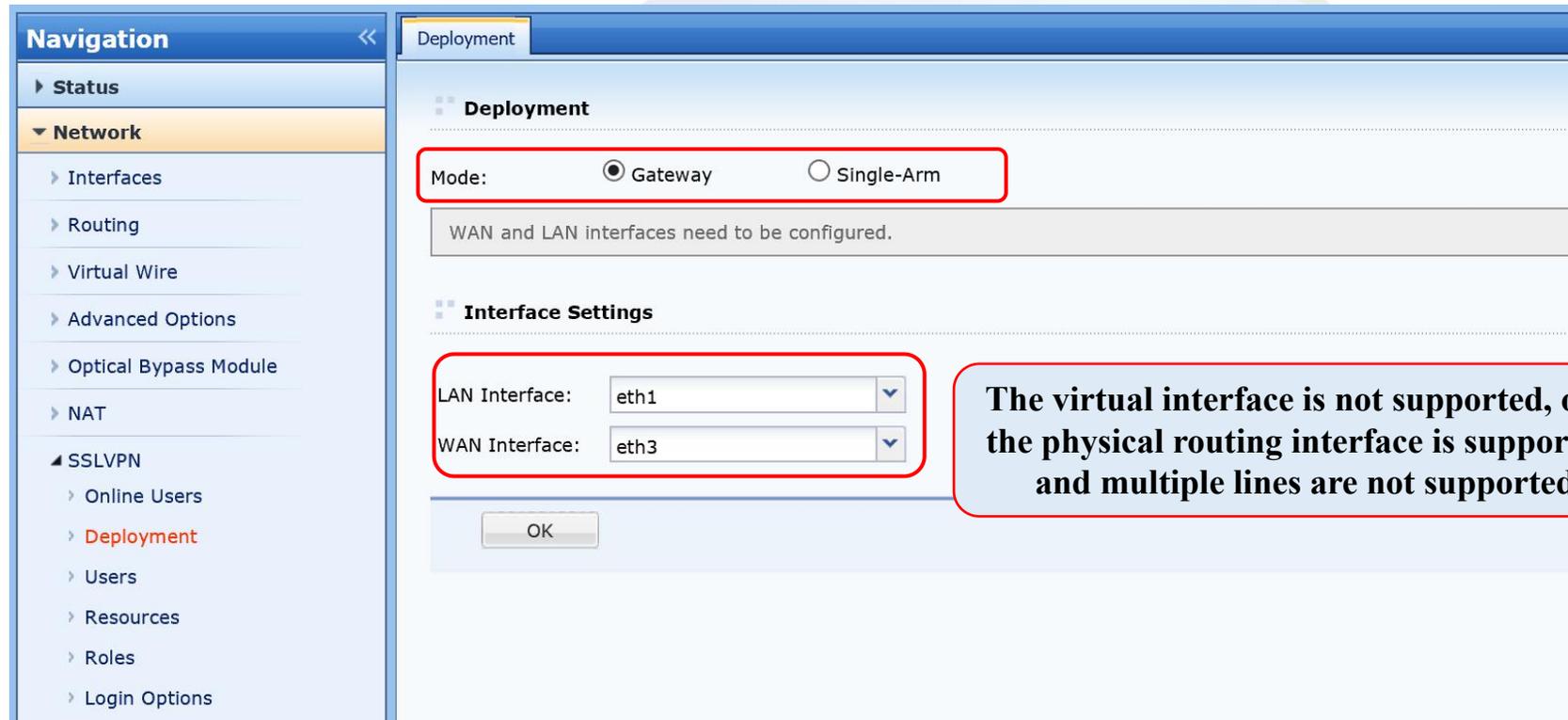
Android 4.0 and later versions;

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

SSL VPN

SSL VPN setting:

SSL Deployment:

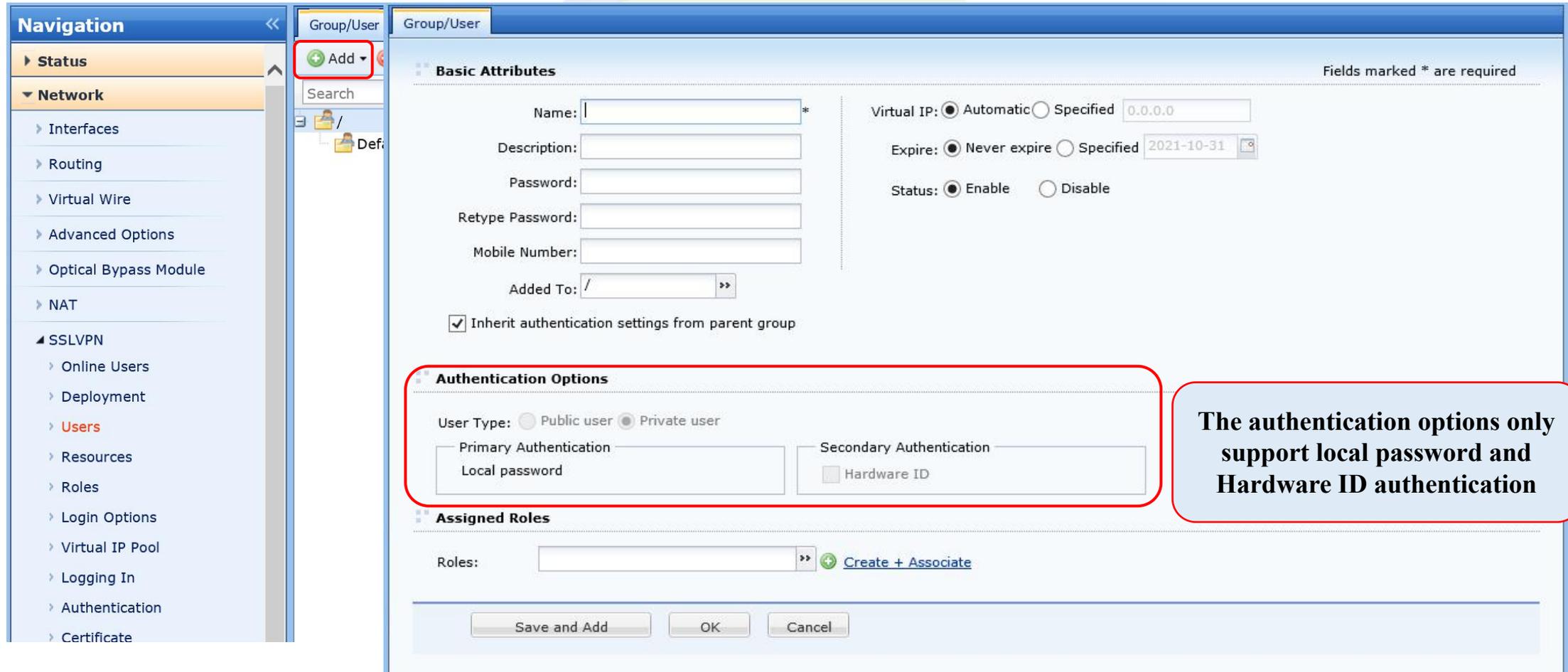


The screenshot shows the 'Deployment' configuration page for SSL VPN. The left sidebar contains a 'Navigation' menu with 'Network' expanded to show 'Interfaces', 'Routing', 'Virtual Wire', 'Advanced Options', 'Optical Bypass Module', 'NAT', and 'SSLVPN'. Under 'SSLVPN', 'Deployment' is selected. The main content area is titled 'Deployment' and includes a 'Mode' section with radio buttons for 'Gateway' (selected) and 'Single-Arm'. Below this is a message: 'WAN and LAN interfaces need to be configured.' The 'Interface Settings' section has dropdown menus for 'LAN Interface' (set to 'eth1') and 'WAN Interface' (set to 'eth3'). An 'OK' button is at the bottom.

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

SSL VPN

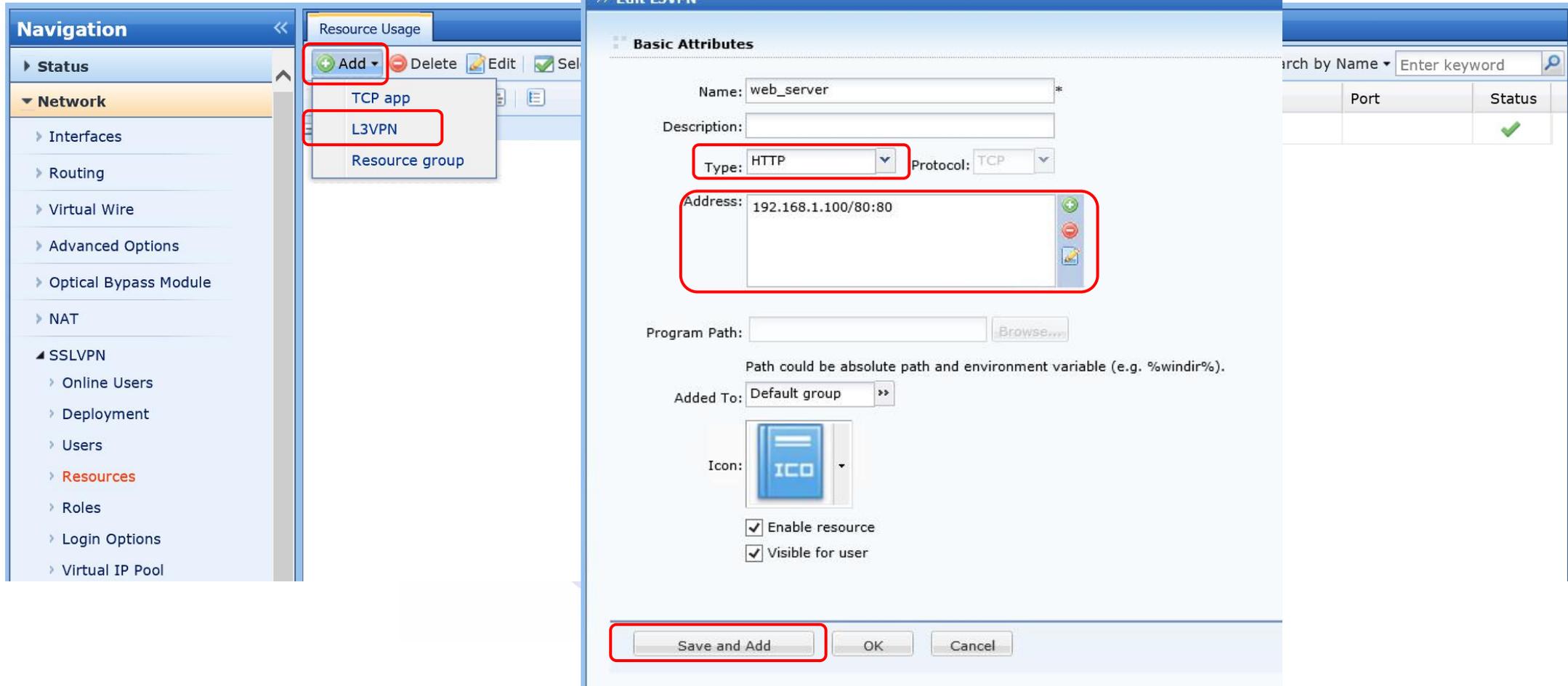
Users management:



The screenshot shows the Sangfor SSL VPN user management interface. On the left is a navigation pane with categories like Status, Network, and SSLVPN. The 'Users' option under SSLVPN is highlighted. The main area shows a 'Group/User' configuration form. A red box highlights the '+ Add' button in the top left of the form area. Another red box highlights the 'Authentication Options' section, which includes fields for 'User Type' (Public user, Private user), 'Primary Authentication' (Local password), and 'Secondary Authentication' (Hardware ID). A text box on the right states: 'The authentication options only support local password and Hardware ID authentication'. The form also includes sections for 'Basic Attributes' (Name, Description, Password, Retype Password, Mobile Number, Added To) and 'Assigned Roles'. Buttons for 'Save and Add', 'OK', and 'Cancel' are at the bottom.

SSL VPN

Resources:



The screenshot displays the Sangfor SSL VPN management interface. On the left, the 'Navigation' pane shows the 'Resources' section under 'SSLVPN'. The main area shows the 'Resource Usage' tab with a context menu open, highlighting the 'Add' button and the 'L3VPN' option. The 'Edit L3VPN' dialog box is open, showing the configuration for a resource named 'web_server'. The 'Type' is set to 'HTTP' and the 'Protocol' is 'TCP'. The 'Address' field contains '192.168.1.100/80:80'. The 'Program Path' is empty, and the 'Added To' field is set to 'Default group'. The 'Icon' is set to 'ICO'. The 'Enable resource' and 'Visible for user' checkboxes are checked. The 'Save and Add' button is highlighted at the bottom of the dialog.

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

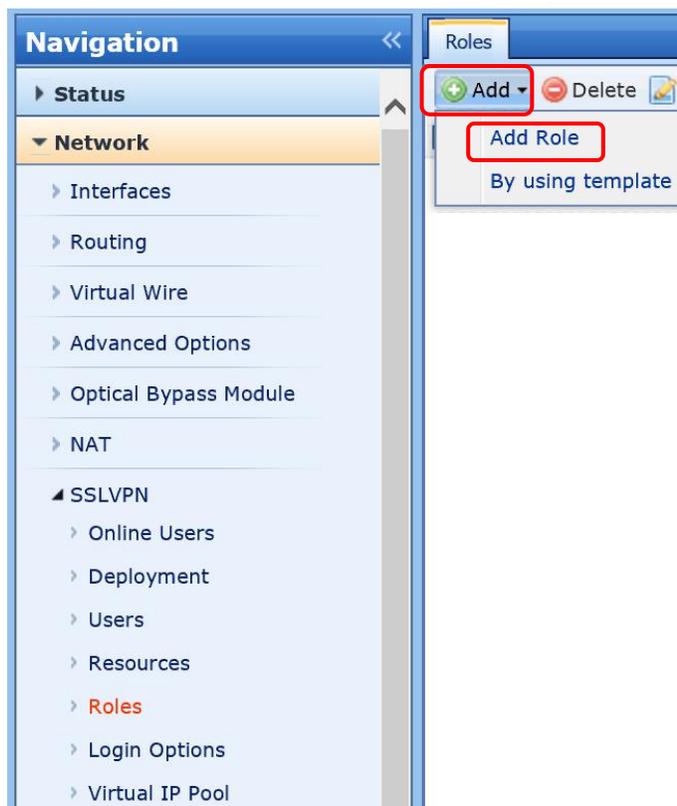
Enable resource

Visible for user

Save and Add OK Cancel

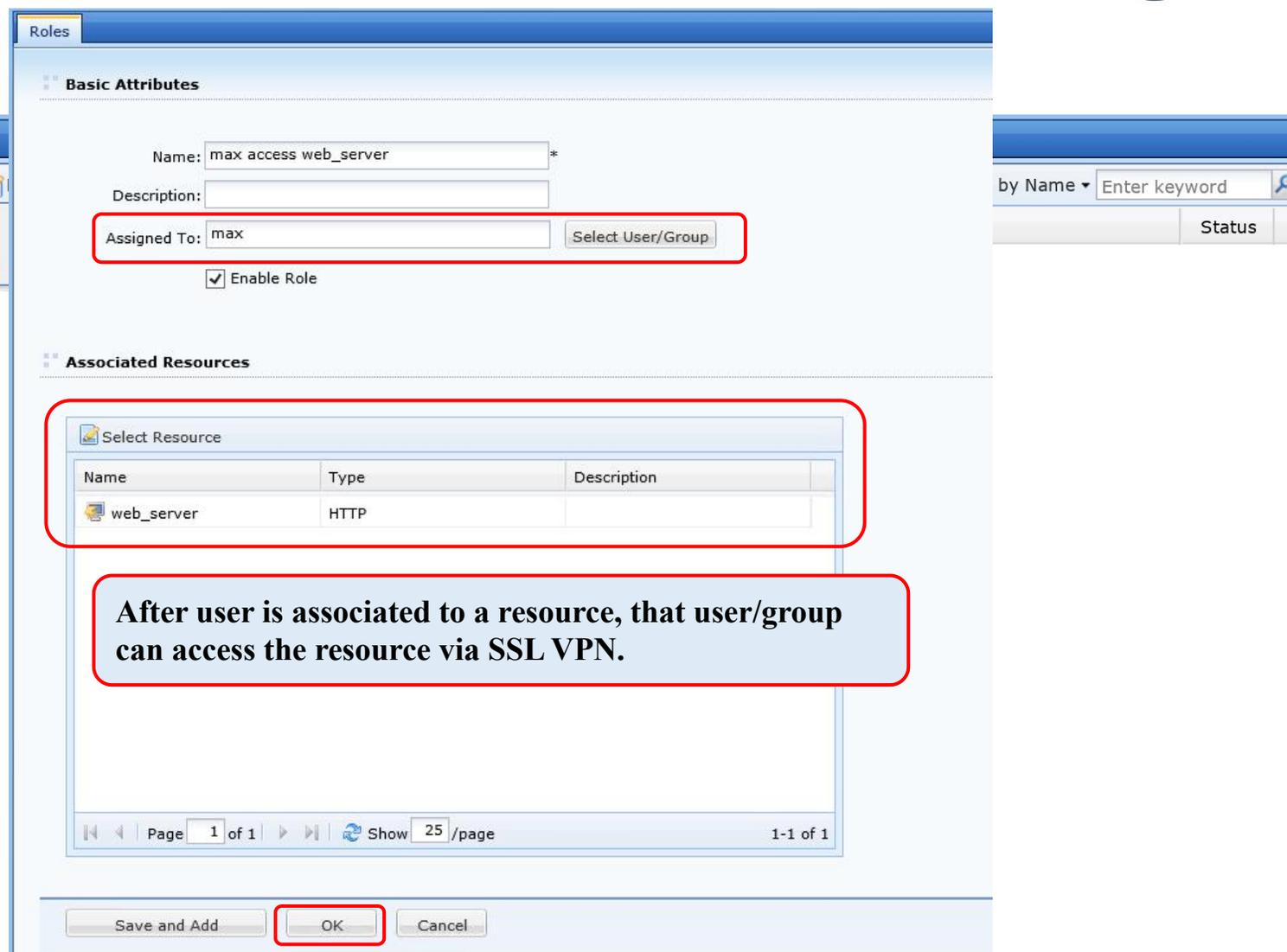
SSL VPN

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

Basic Attributes

Name: max access web_server *

Description:

Assigned To: max

Enable Role

Associated Resources

Select Resource

Name	Type	Description
 web_server	HTTP	

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

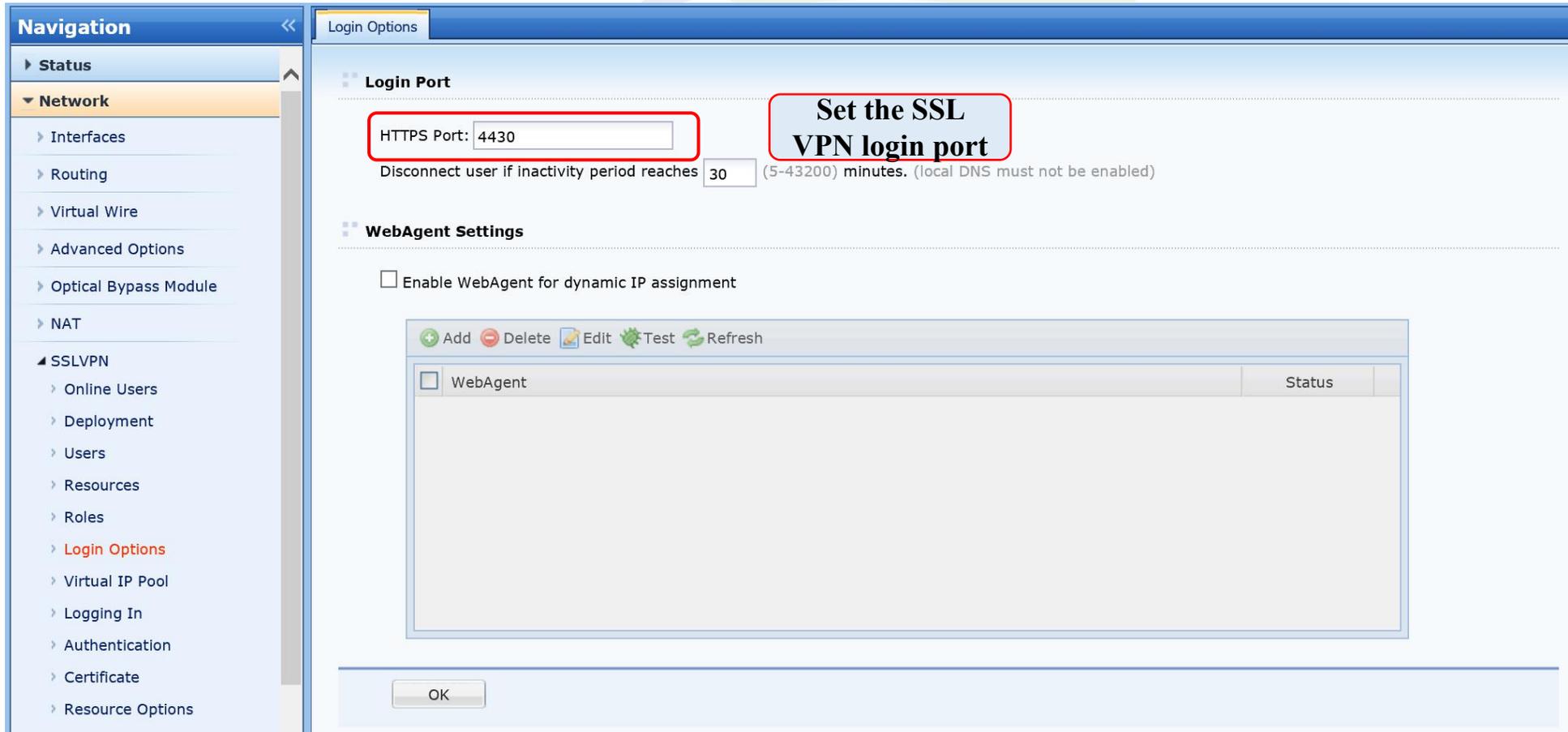
by Name

Status

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

SSL VPN

Login Options:



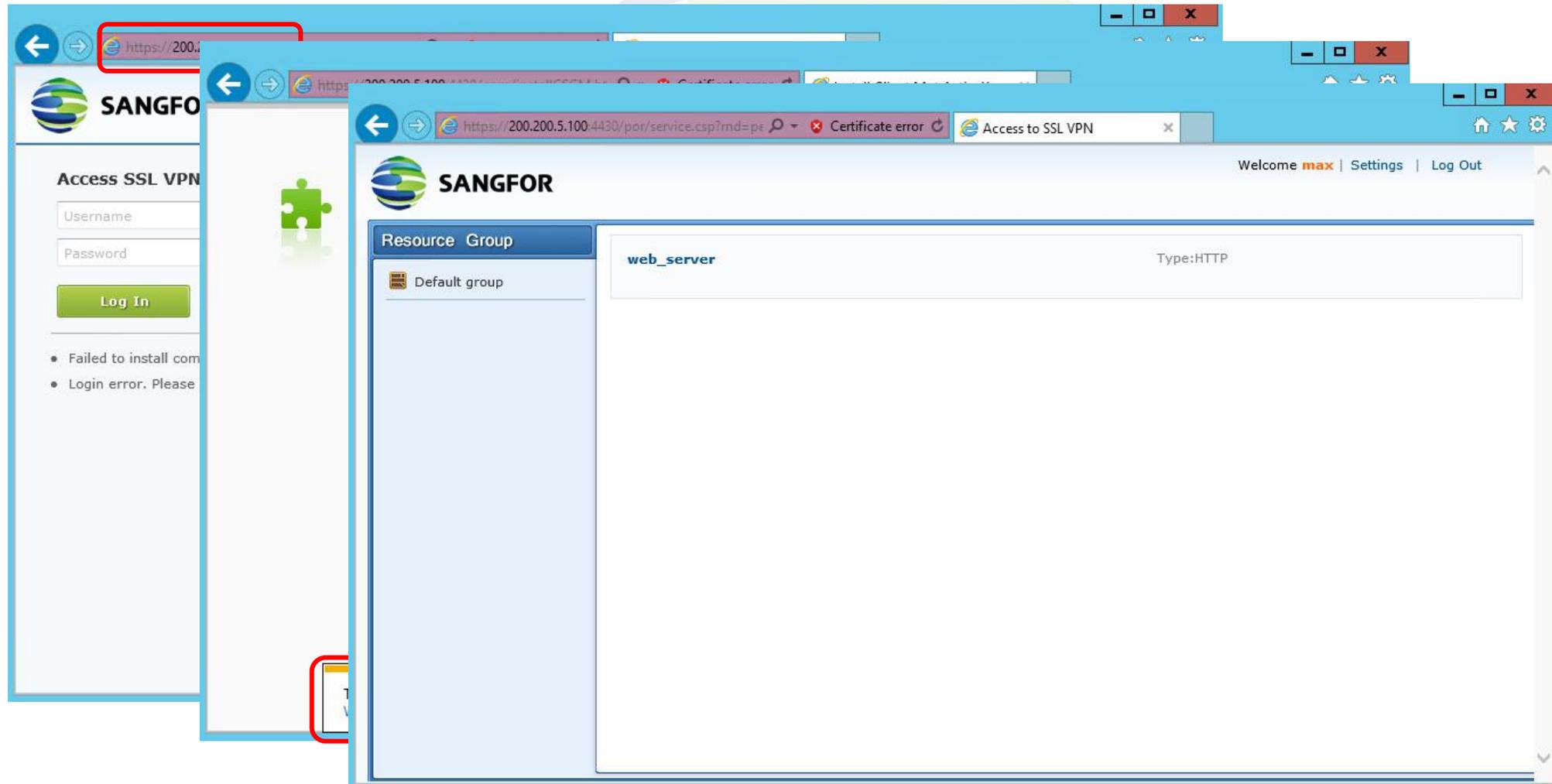
The screenshot displays the 'Login Options' configuration page in the SANGFOR SSL VPN management console. The left sidebar shows a navigation menu with 'Login Options' highlighted under the 'SSLVPN' section. The main content area is titled 'Login Options' and contains the following settings:

- Login Port:** A text box labeled 'HTTPS Port:' contains the value '4430'. This text box is highlighted with a red border. A red callout box with the text 'Set the SSL VPN login port' points to this field.
- Inactivity Timeout:** A label 'Disconnect user if inactivity period reaches' is followed by a spinner box set to '30' and the text '(5-43200) minutes. (local DNS must not be enabled)'.
- WebAgent Settings:** A checkbox labeled 'Enable WebAgent for dynamic IP assignment' is currently unchecked.
- WebAgent Table:** A table with a toolbar (Add, Delete, Edit, Test, Refresh) and one row containing a checkbox, the text 'WebAgent', and a 'Status' column.

An 'OK' button is located at the bottom of the configuration area.

SSL VPN

Client access to SSL VPN:



The screenshot displays a web browser interface for SANGFOR SSL VPN access. The browser's address bar shows a URL starting with 'https://200.'. The page content is divided into two main sections:

- Access SSL VPN:** This section contains a login form with fields for 'Username' and 'Password', and a green 'Log In' button. Below the form, there are two error messages:
 - Failed to install com
 - Login error. Please
- Resource Group:** This section displays a table with the following data:

Resource Group	Type
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)

