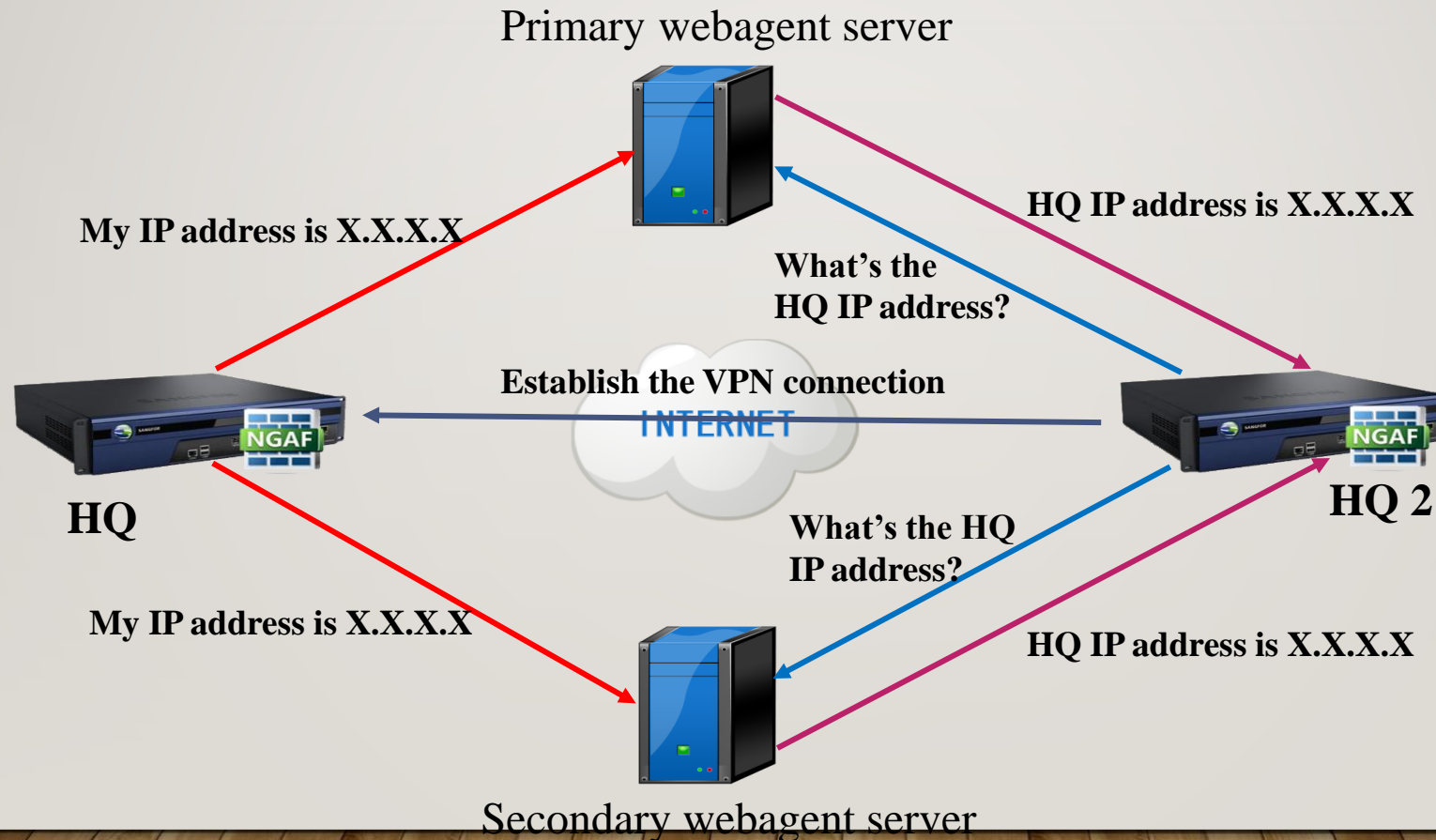


Sangfor VPN

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 for both HQ:

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, and IPsecVPN (expanded). Under IPsecVPN, there are sub-options: Status, Basics (highlighted in red), 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:** A text box containing '10.254.254.254:4009'.
- Secondary WebAgent:** An empty text box.
- MTU Value(224-2000):** A text box containing '1500'.
- Min Compression(99-5000):** A text box containing '100'.
- VPN Listening Port(default 4009):** A text box containing '4009'.
- Modify MSS(only for use of UDP):** An unchecked checkbox.
- Connection Type:** Two radio buttons: 'Directly connects to Internet' (selected) and 'Indirectly connects to Int'.
- Buttons:** 'Change Password' (twice), 'Shared Key', 'Advanced', 'Test', and 'Save'.

Annotations in red speech bubbles provide additional instructions:

- Set the primary and secondary(optional) webagent(s).** Points to the Primary and Secondary WebAgent fields.
- The ports need to be the same as webagent** Points to the VPN Listening Port field.
- If set shared key here, branch/mobile need to set the same shared key for VPN connection.** Points to the Shared Key button.
- To test whether the format is correct** Points to the Test button.
- If the HQ IP is not the fixed, you can apply the webagent from Sangfor** Points to the Primary WebAgent field.

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 section with a 'Detect USB Key' button and a table of groups. Overlaid on this is a 'New User -- Webpage Dialog' window. The dialog has a browser address bar showing 'https://200.200.5.100/html/subfrm.html' and a 'Certificate error' message. The form contains fields for Username (test), Password (masked), Confirm PWD (masked), Authentication (Local), Algorithm (DES), User Type (Mobile user), and User Group (Default group). 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. The dialog has buttons for LAN Service, Advanced, Save, and Cancel. Red callout boxes with black text provide instructions: '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 Branch user Default group

User Group: Default group

☐ Inherit group attributes

☐ Hardware verification

☐ 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 My Network Places

☒ Enable compression ☐ Not allow Internet access once connected

☐ Allow users to log in concurrently ☐ 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:

The screenshot displays the Sangfor VPN management interface. On the left is a 'Navigation' sidebar with a tree structure. The 'Network' section is expanded, showing options like 'Interfaces', 'Routing', 'Virtual Wire', 'Advanced Options', 'Optical Bypass Module', 'NAT', 'IPSecVPN', 'Status', 'Basics', 'Local Users', 'VPN Connections', 'Virtual IP Pool' (highlighted in red), 'Multiline Options', 'VPN Interface', and 'Multiline Policy'. The main content area is titled 'Virtual IP Pool' and contains a table with columns: 'IP Range', 'Subnet Mask', 'Subnets', 'Type', and 'Operation'. Below the table are buttons for 'Add', 'Advanced', and 'Save'. A modal dialog titled 'Add Virtual IP Pool -- Webpage Dialog' is open, showing a browser address bar with 'https://200.200.5.100/html/dlan/vip_operate.html' and a 'Certificate error' message. The dialog has a 'Tips' section and the following fields: 'Assigned To:' with a dropdown menu showing 'Mobile user' and 'Branch user'; 'Start IP:' with an input field; and 'End IP:' with an input field. 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 IP input fields with the text 'Address range cannot contain IP of internal network or device port.' At the bottom of the dialog are 'Save' and 'Cancel' buttons.

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**

• Tips

Assigned To: **Mobile user**
Branch user

Start IP:

End IP:

Save **Cancel**

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:

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

VPN Connection

Status	Username	Protocol	Operation
--------	----------	----------	-----------

Edit Outgoing Connection -- Webpage Dialog

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

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

Test

LAN Service Save Cancel

Enable connection

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