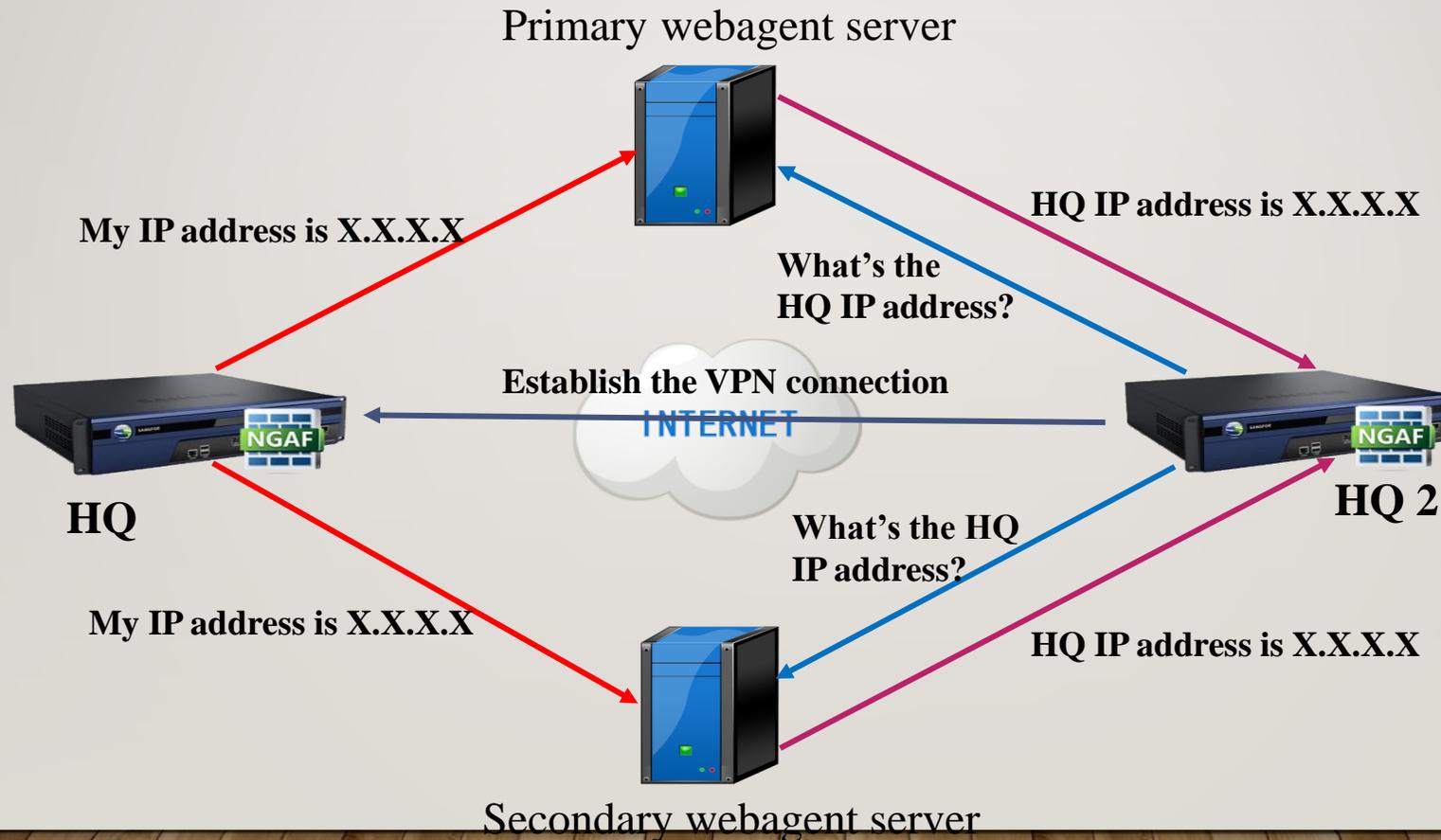


# Sangfor VPN

## 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 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 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 in red callouts provide additional instructions:

- Set the primary and secondary(optional) webagent(s).** (points to the Primary and Secondary WebAgent fields)
- If set shared key here, branch/mobile need to set the same shared key for VPN connection.** (points to the Shared Key button)
- The ports need to be the same as webagent** (points to the VPN Listening Port field)
- 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 image shows a screenshot of the Sangfor VPN management interface. On the left is a navigation menu with categories 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. A 'New User -- Webpage Dialog' window is open, displaying the configuration for a new user. The dialog has several fields and options, with red callouts providing instructions:

- Set the username and password for VPN authentication:** Points to the Username (test), Password (masked), and Confirm PWD (masked) fields.
- Set the user type:** Points to the User Type dropdown menu, which is set to 'Mobile user'.
- If the user type is mobile user, must enable this option:** Points to the 'Assign virtual IP' checkbox, which is checked.
- Enable user:** Points to the 'Enabled' checkbox at the bottom of the dialog, which is checked.

Other visible fields in the dialog include: Authentication (Local), Algorithm (DES), User Group (Default group), Inherit group attributes (unchecked), Hardware verification (unchecked), Enable USB Key (unchecked), USB Key (empty), IP Address (0.0.0.0), Valid Time (All week), Enable expiry time (unchecked), Expired At (0-00-00), Enable My Network Places (checked), Enable compression (checked), Not allow Internet access once connected (unchecked), Allow users to log in concurrently (unchecked), and Not allow password change online (unchecked). Buttons at the bottom include LAN Service, Advanced, Save, and Cancel.

# Sangfor VPN

HQ setting:

Virtual IP Pool:

The screenshot displays the Sangfor VPN management interface. On the left is a navigation menu with categories like Status, Network, and IPsecVPN. 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 contains a 'Certificate error' message and a 'Tips' section. The 'Assigned To:' field is a dropdown menu with 'Mobile user' selected and 'Branch user' visible below it. The 'Start IP:' and 'End IP:' fields are empty text boxes. 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 another points to the IP input fields with the text 'Address range cannot contain IP of internal network or device port.' The dialog also has 'Save' and 'Cancel' buttons at the bottom.

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 menu with categories 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, and Local Subnet. The main area shows the 'VPN Connection' configuration for an outgoing connection named 'KL'. The 'Edit Outgoing Connection -- Webpage Dialog' window is open, showing the following fields and options:

- 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 (set to Auto)
- Cross-ISP Access Opt. (set to Low packet loss)
- Packet loss rate: 10 %
- Enabled

Buttons at the bottom include LAN Service, Save, and Cancel. A 'Test' button is also present. A 'Certificate error' message is visible in the browser window above the dialog.

**Enable connection**

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