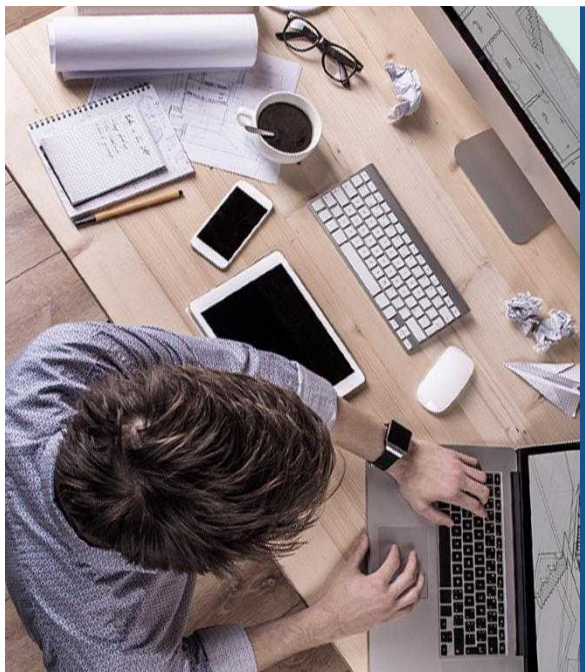




Sangfor NSF V8.0.85 Associate

VPN





1 IPsec VPN

2 Sangfor VPN

3 SSL VPN

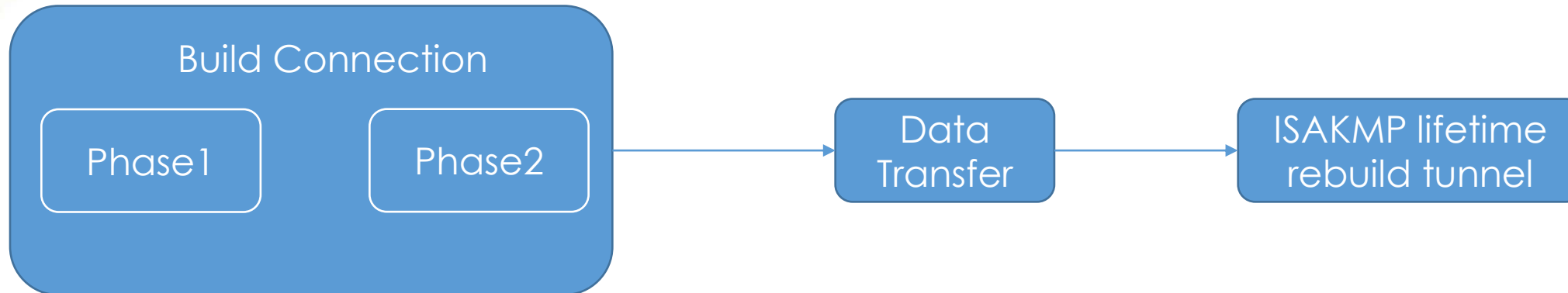
PART 1

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.



Phase1:

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

Phase2:

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

1. NSF must have Branch VPN Sites license to establish a IPsec VPN. Another requirement, the encrypted network segments in both sides of IPsec VPN shouldn't conflict. **Licensing**

Basic Settings

Status: ✔ Activated (auto-updated if the internet is connected) | [Manual Update](#)

Type: test

Version: 8.0.85

Time Activated: 2024-01-17 15:41:51

Authorized User: 20624-IMD-John [Details](#)

Gateway ID: E14D36AB

Licensing

[How to Renew License?](#) ⓘ

Network

 **Gateway** Activated

Determine how many WAN links and VPN branch sites are allowed

Expiration Date: Never

- Branch VPN Sites: 10
- Lines: 10

 **SSL VPN** Activated

Determine the maximum number of concurrent users

Expiration Date: Never

- Max Concurrent Users: 10

 **SOFAST Optimization & BEST Path Selection** Activated

This applies to authorizing Sangfor VPN path selection templates and SD-WAN path selection

Expiration Date: 2024-04-16

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

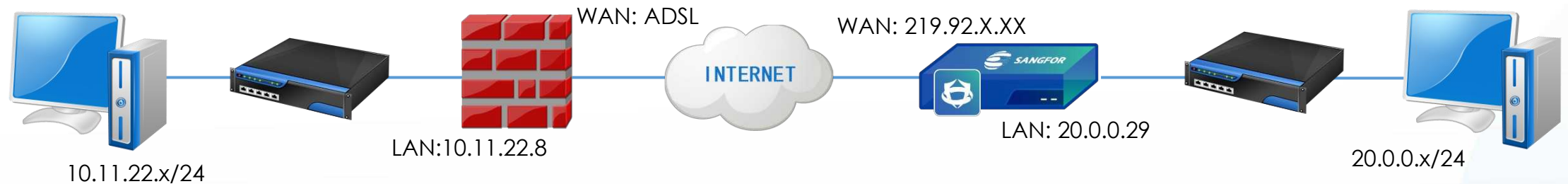
Sangfor:

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



Precautions: Dynamic IP needs to apply for a domain name and use Aggressive mode.

1. Configure the interface and the zone, Configuration path: **Network > Interfaces**.

Edit Physical Interface ×

Basics

Name: eth1

Status: Enabled Disabled

Description: Optional

Type: Layer 3

Zone: L3_untrust_A

Basic Attributes: WAN attribute

Reverse Routing ⓘ: Enabled

IPv4 IPv6 Advanced

IP Assignment: Static DHCP PPPoE

Static IP: 219.92.2.8/24 ⓘ

Default Gateway: 219.92.2.10

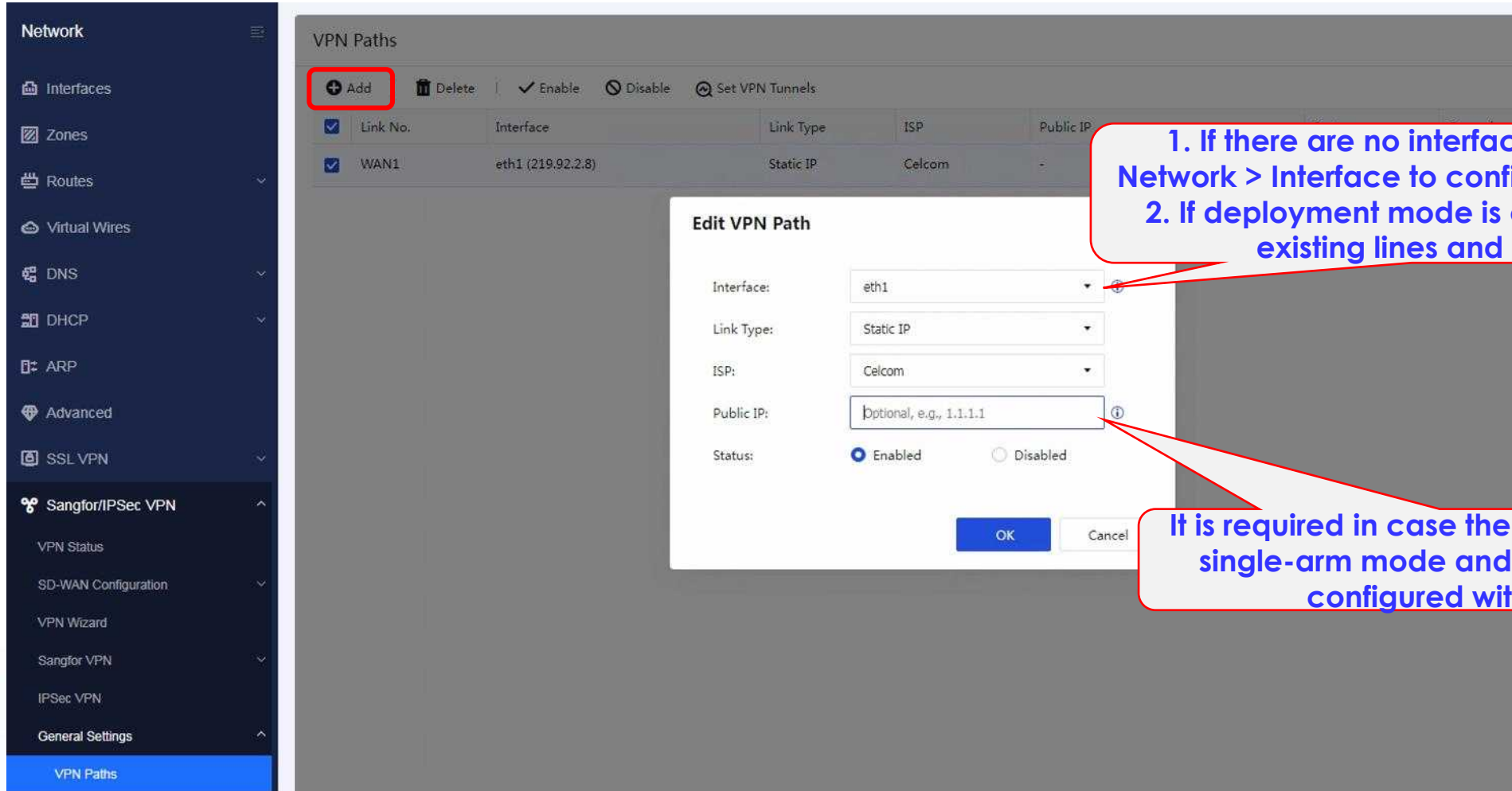
Link Bandwidth: Outbound 1000 Mbps Inbound 1000 Mbps

Management Service

Allow: WEBUI PING SNMP SSH

OK Cancel

2. Configure the VPN Path, go to **Network > Sangfor/IPSec VPN > General Settings > VPN Pat**



The screenshot displays the Sangfor VPN configuration interface. On the left is a navigation menu with the following items: Network, Interfaces, Zones, Routes, Virtual Wires, DNS, DHCP, ARP, Advanced, SSL VPN, Sangfor/IPSec VPN, VPN Status, SD-WAN Configuration, VPN Wizard, Sangfor VPN, IPsec VPN, General Settings, and VPN Paths. The main area shows the 'VPN Paths' configuration page. At the top, there are buttons for '+ Add', 'Delete', 'Enable', 'Disable', and 'Set VPN Tunnels'. Below these is a table with columns: Link No., Interface, Link Type, ISP, and Public IP. The table contains one entry: WAN1, eth1 (219.92.2.8), Static IP, Celcom, and -. An 'Edit VPN Path' dialog box is open in the foreground. It has the following fields: Interface (dropdown menu with 'eth1' selected), Link Type (dropdown menu with 'Static IP' selected), ISP (dropdown menu with 'Celcom' selected), Public IP (text input field with 'Optional, e.g., 1.1.1.1' and an information icon), and Status (radio buttons for 'Enabled' and 'Disabled', with 'Enabled' selected). At the bottom of the dialog are 'OK' and 'Cancel' buttons. Two red callout boxes with blue text provide instructions: one points to the '+ Add' button and the other points to the 'Public IP' field.

Link No.	Interface	Link Type	ISP	Public IP
WAN1	eth1 (219.92.2.8)	Static IP	Celcom	-

1. If there are no interfaces available, go to Network > Interface to configure a WAN interface.
2. If deployment mode is changed, delete the existing lines and add it again.

It is required in case the device is deployed in single-arm mode and no WAN interface is configured with IP address.

3. Basics

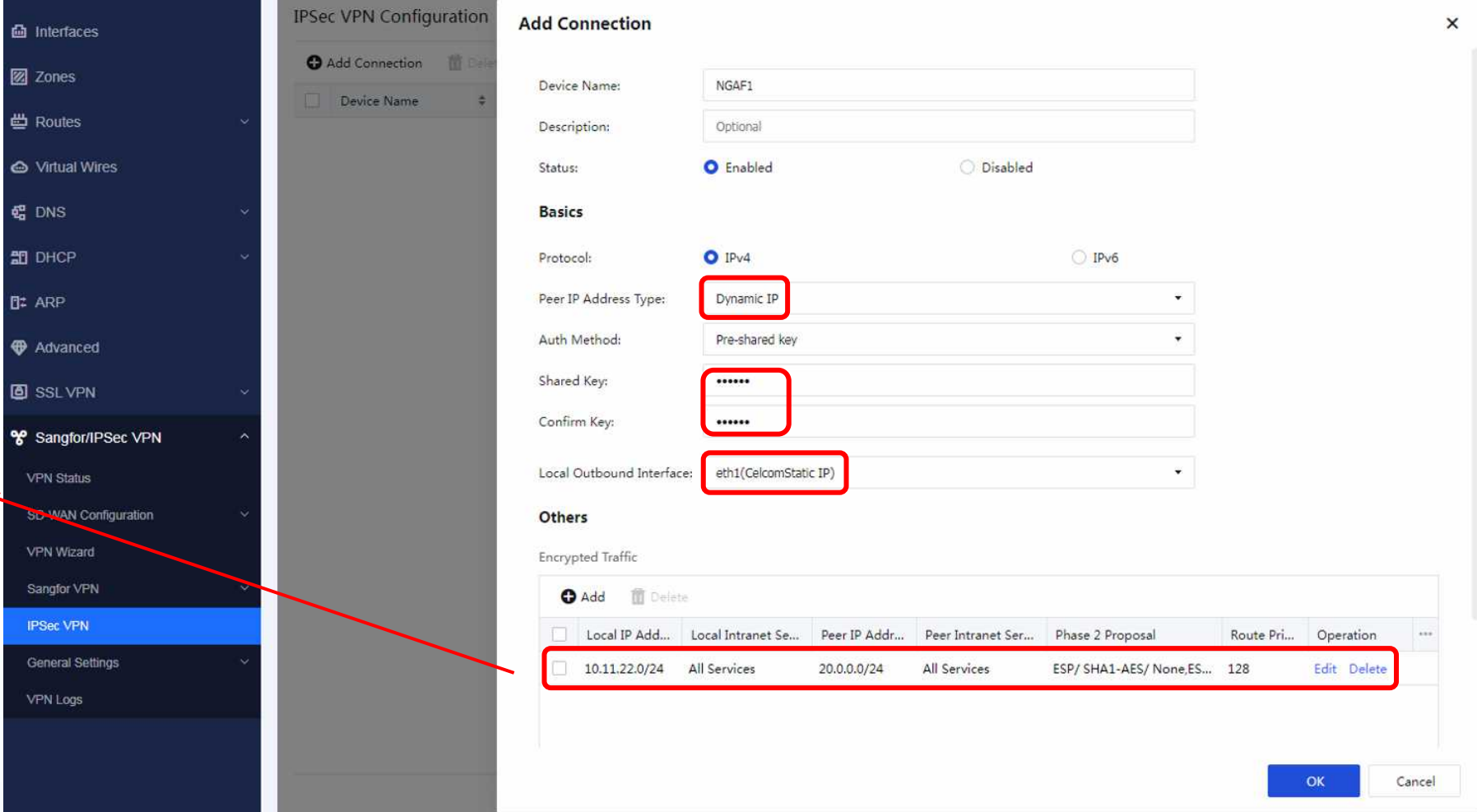
Configuration Path: **Network > Sangfor/IPSec VPN > IPSec VPN**

Local IP Address:

Input the intranet network segment of the local device.

Peer IP Address:

Input the intranet network segment of the peer device.

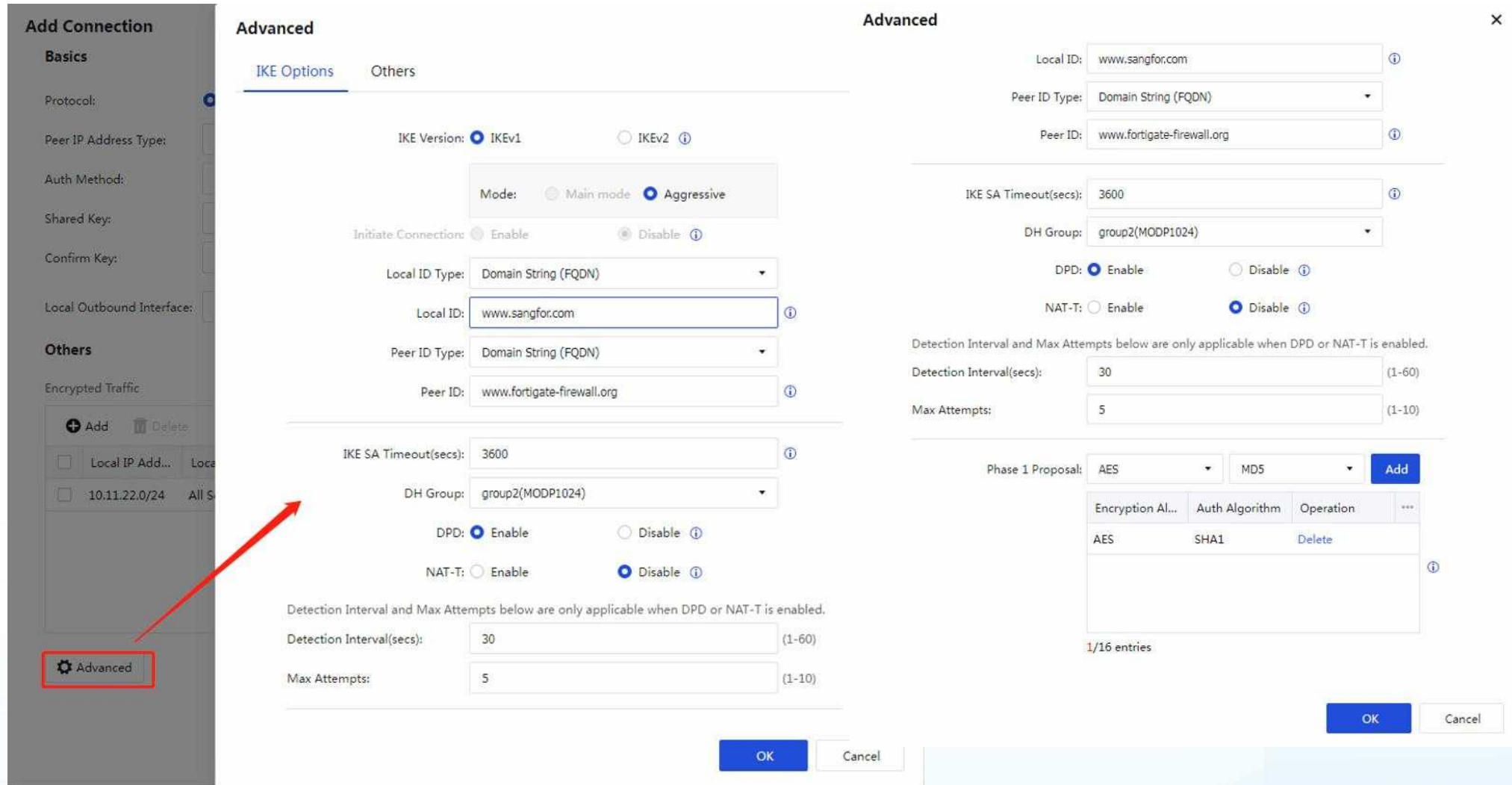


The screenshot shows the Sangfor management console interface for configuring an IPSec VPN connection. The left sidebar contains a navigation menu with options like Interfaces, Zones, Routes, Virtual Wires, DNS, DHCP, ARP, Advanced, SSL VPN, Sangfor/IPSec VPN, VPN Status, SD-WAN Configuration, VPN Wizard, Sangfor VPN, IPSec VPN (highlighted), General Settings, and VPN Logs. The main area displays the 'Add Connection' configuration window for device 'NGAF1'. The 'Basics' section is expanded, showing the following settings: Protocol: IPv4 (selected), Peer IP Address Type: Dynamic IP (highlighted with a red box), Auth Method: Pre-shared key, Shared Key: [masked], Confirm Key: [masked], and Local Outbound Interface: eth1(CelcomStatic IP) (highlighted with a red box). The 'Others' section shows a table for 'Encrypted Traffic' with one entry highlighted by a red box:

	Local IP Add...	Local Intranet Se...	Peer IP Addr...	Peer Intranet Ser...	Phase 2 Proposal	Route Pri...	Operation	...
<input type="checkbox"/>	10.11.22.0/24	All Services	20.0.0.0/24	All Services	ESP/ SHA1-AES/ None,ES...	128	Edit Delete	

Buttons for 'OK' and 'Cancel' are located at the bottom right of the configuration window.

4. IKE Options



The screenshot displays the configuration interface for an IPSEC VPN connection. On the left, a sidebar shows the 'Advanced' tab selected. The main area is divided into two panels: 'Advanced' and 'Others'. The 'Advanced' panel contains the following settings:

- IKE Version: IKEv1 IKEv2
- Mode: Main mode Aggressive
- Initiate Connections: Enable Disable
- Local ID Type: Domain String (FQDN)
- Local ID: www.sangfor.com
- Peer ID Type: Domain String (FQDN)
- Peer ID: www.fortigate-firewall.org
- IKE SA Timeout(secs): 3600
- DH Group: group2(MODP1024)
- DPD: Enable Disable
- NAT-T: Enable Disable
- Detection Interval and Max Attempts below are only applicable when DPD or NAT-T is enabled.
- Detection Interval(secs): 30 (1-60)
- Max Attempts: 5 (1-10)

The 'Others' panel contains the following settings:

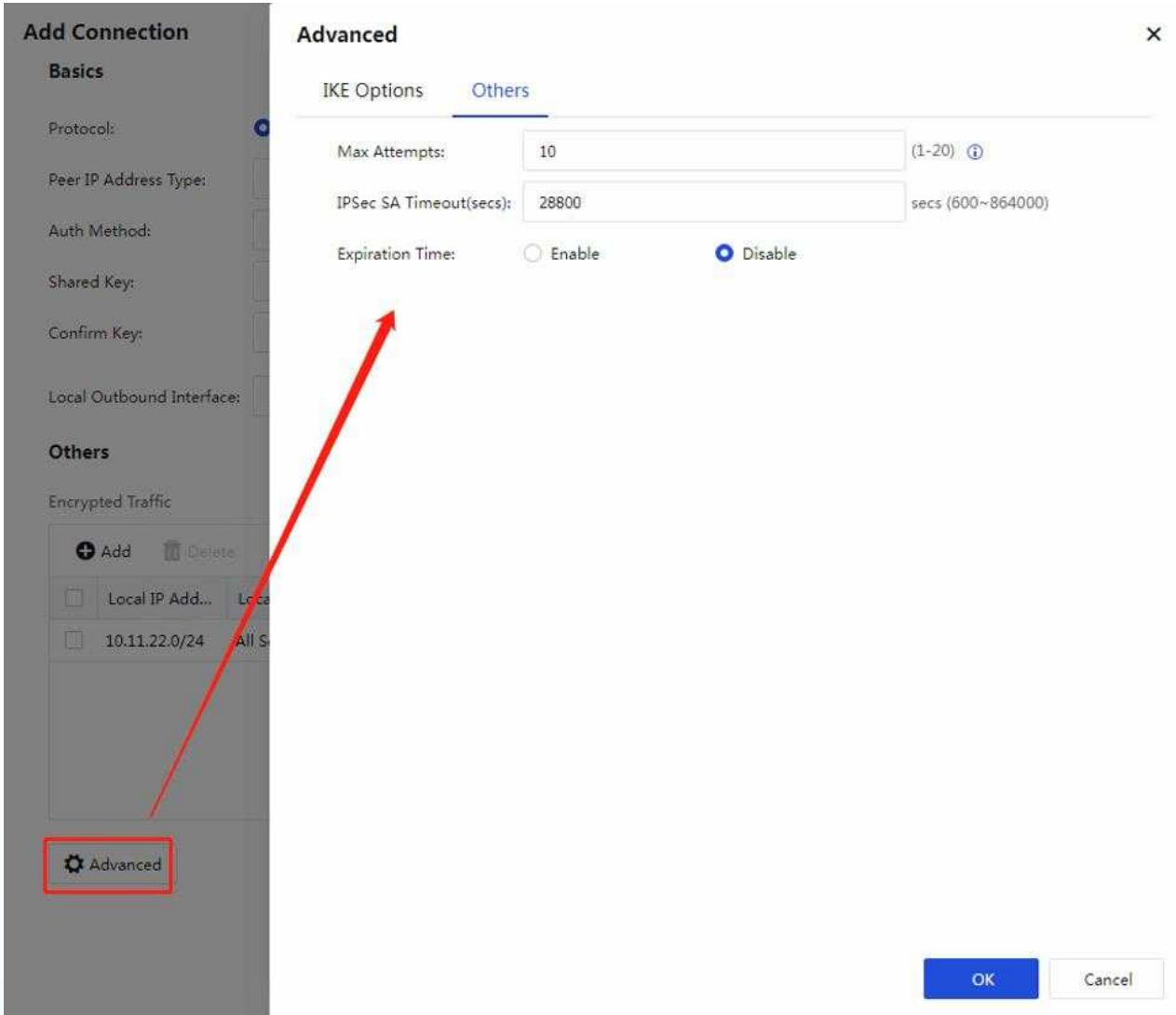
- Local ID: www.sangfor.com
- Peer ID Type: Domain String (FQDN)
- Peer ID: www.fortigate-firewall.org
- IKE SA Timeout(secs): 3600
- DH Group: group2(MODP1024)
- DPD: Enable Disable
- NAT-T: Enable Disable
- Detection Interval and Max Attempts below are only applicable when DPD or NAT-T is enabled.
- Detection Interval(secs): 30 (1-60)
- Max Attempts: 5 (1-10)

At the bottom right, there is a 'Phase 1 Proposal' section with a table of proposals:

Encryption Al...	Auth Algorithm	Operation	...
AES	SHA1	Delete	

Buttons for 'OK' and 'Cancel' are present at the bottom of both panels.

5. Other Options



The screenshot displays the 'Add Connection' configuration window, specifically the 'Advanced' tab. The left sidebar shows the 'Advanced' option selected and highlighted with a red box. A red arrow points from this box to the 'Expiration Time' setting in the main panel. The 'Advanced' tab is divided into 'IKE Options' and 'Others'. The 'Others' sub-tab is active, showing the following settings:


- Max Attempts: 10 (range 1-20)
- IPSec SA Timeout(secs): 28800 (range 600-864000)
- Expiration Time: Enable Disable


At the bottom right of the window are 'OK' and 'Cancel' buttons.


6. After successfully configuration, we can see the tunnel in the **IPSec VPN > Status**.

Status

Start VPN service

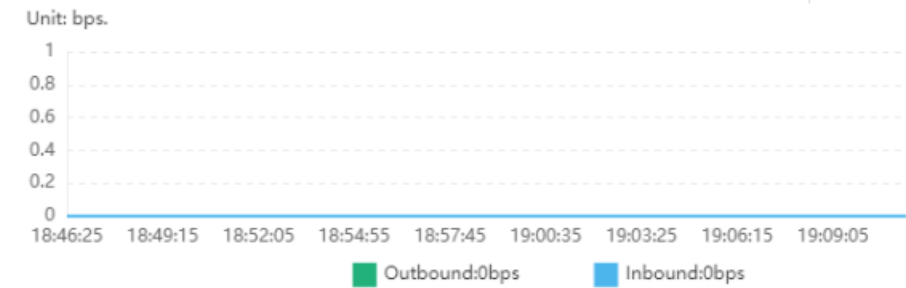
 Connection to Sangfor Device (Hub)
Connected:0 | Enabled Connections:0

 Connection to Sangfor Device (Spoke)
Connected:0 | Enabled Connections:0

 Connection to Third-Party Device
Connected:1 | Enabled Connections:1


Throughput on VPN Interface Last hour



Unit: bps.



■ Outbound:0bps ■ Inbound:0bps

Tunnels

 Alarm Trigger Peer Name Type here

Status	Peer Name	Peer Device T...	Peer's Public IP	Peer's Internal IP	Outbound	Inbound	Sent Packet L...	Rcvd Packet L...	Latency	Jitter	Operation
Normal	NGAF1	Sangfor Appli...			0 bps	0 bps	0.00%	0.00%	-	-	View Details Disc...

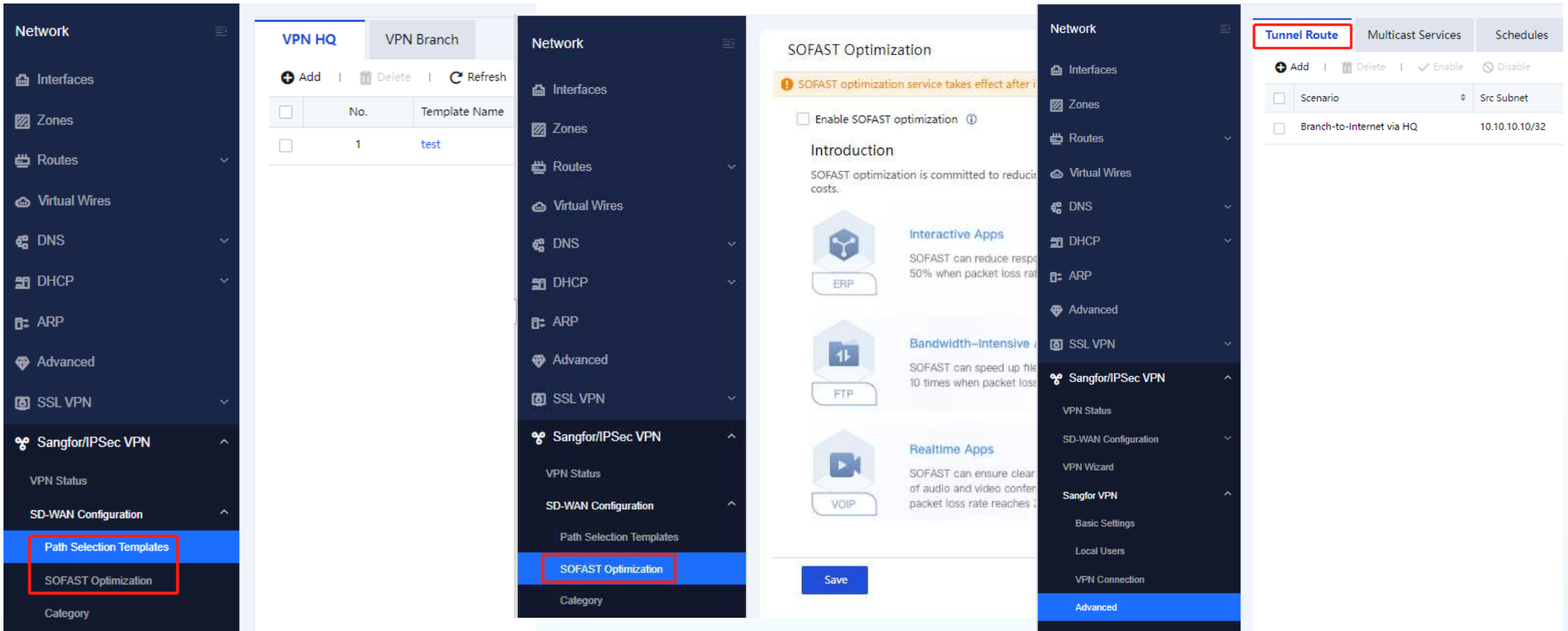
PART 2

Sangfor VPN

Sangfor NSF provides two types of VPN connections namely, standard IPSEC VPN, and a self-developed SANGFOR VPN, providing the device-to-device connection. SANGFOR VPN 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.

Sangfor VPN is a core component for SD-WAN scenario in NSF, and many features shown as below, are based on Sangfor VPN.



The screenshot displays the Sangfor VPN management interface with several panels:

- VPN HQ Panel:** Shows a table with columns 'No.' and 'Template Name'. One entry is visible: No. 1, Template Name 'test'.
- SOFAST Optimization Panel:** Features a toggle for 'Enable SOFAST optimization'. Below, it lists application categories: 'Interactive Apps' (ERP), 'Bandwidth-Intensive' (FTP), and 'Realtime Apps' (VOIP). A 'Save' button is at the bottom.
- Tunnel Route Panel:** Shows a table with columns 'Scenario' and 'Src Subnet'. One entry is visible: Scenario 'Branch-to-Internet via HQ', Src Subnet '10.10.10.10/32'.

Navigation menus on the left and right sides include: Interfaces, Zones, Routes, Virtual Wires, DNS, DHCP, ARP, Advanced, Sangfor/IPSec VPN, VPN Status, SD-WAN Configuration, Path Selection Templates, SOFAST Optimization, Category, Network, and Tunnel Route.

Usages of Sangfor VPN:

HQ:

Provides VPN access services, and provides access to account verification of other VPN users. Sangfor VPN in HQ side 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.

A VPN device can act as a HQ or branch.

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**

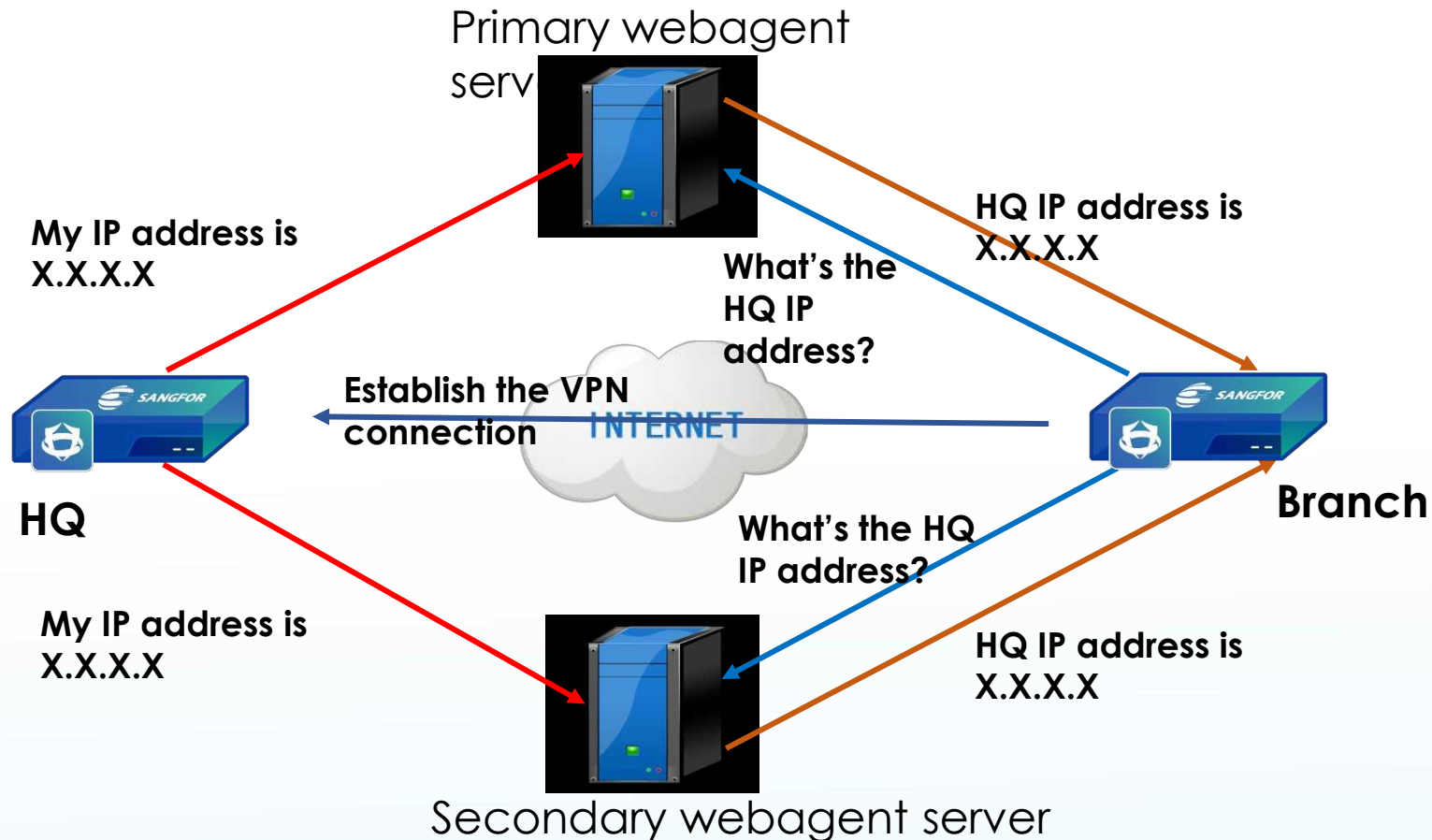
HQ VPN device that has multiple lines with fixed IP, and require VPN backups or for load balance.

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.

WEBAGENT addressing process:

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

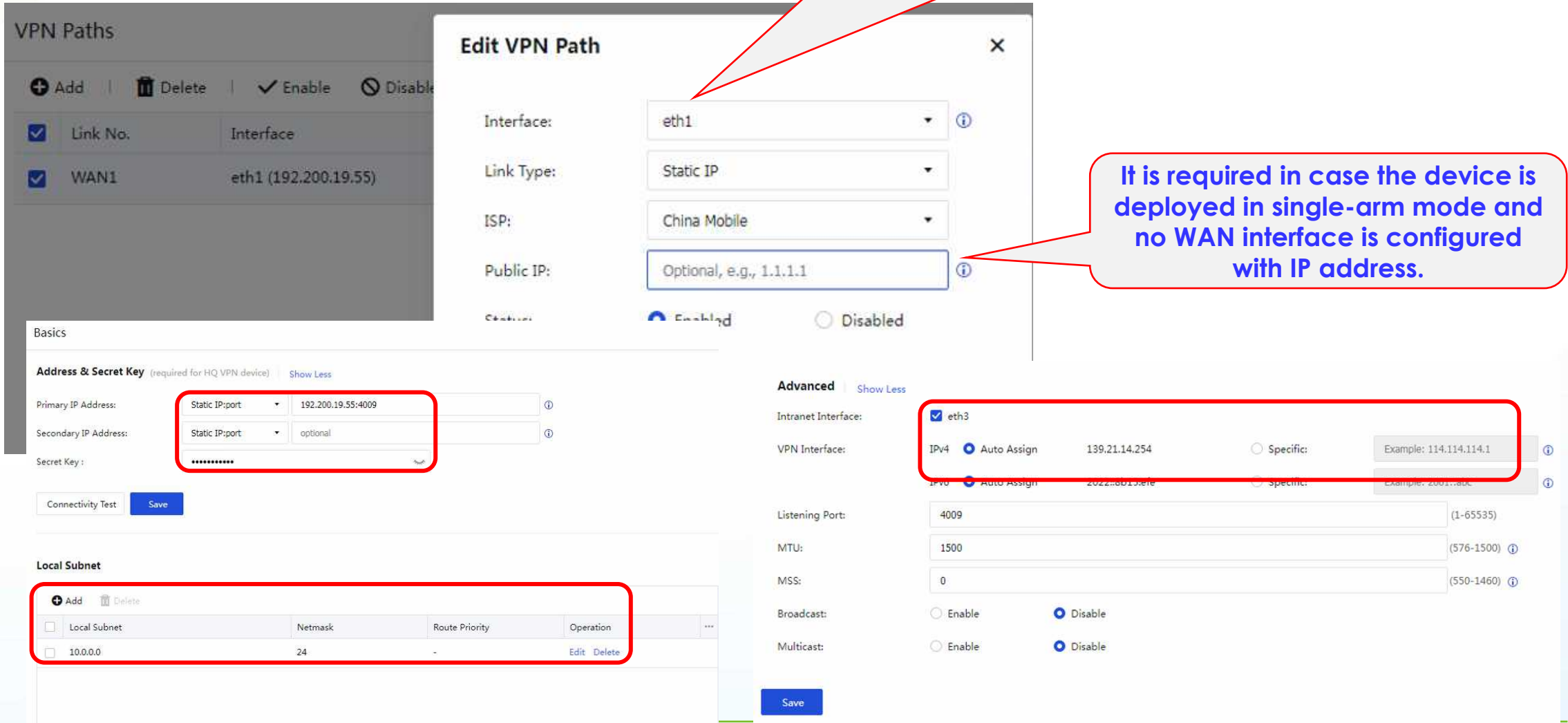


The basic configurations for establishing a VPN connection between HQ and branch or mobile are as follow:

- (1) HQ: Need to configure VPN path, webagent, and local users.
- (2) Branch: Just configure the connection management.

HQ Basic Settings

1. If there are no interfaces available, go to Network > Interface to configure a WAN interface.
2. If deployment mode is changed, delete the existing lines and add it again.



The screenshot displays the Sangfor VPN configuration interface. On the left, the 'VPN Paths' table shows a single entry:

Link No.	Interface
WAN1	eth1 (192.200.19.55)

The 'Edit VPN Path' dialog box is open, showing the following configuration:

- Interface: eth1
- Link Type: Static IP
- ISP: China Mobile
- Public IP: Optional, e.g., 1.1.1.1
- Deployment Mode: Enabled

The 'Basics' section includes the 'Address & Secret Key' fields:

- Primary IP Address: Static IP:port, 192.200.19.55:4009
- Secondary IP Address: Static IP:port, optional
- Secret Key: [Redacted]

The 'Advanced' section includes the 'Intranet Interface' and 'VPN Interface' settings:

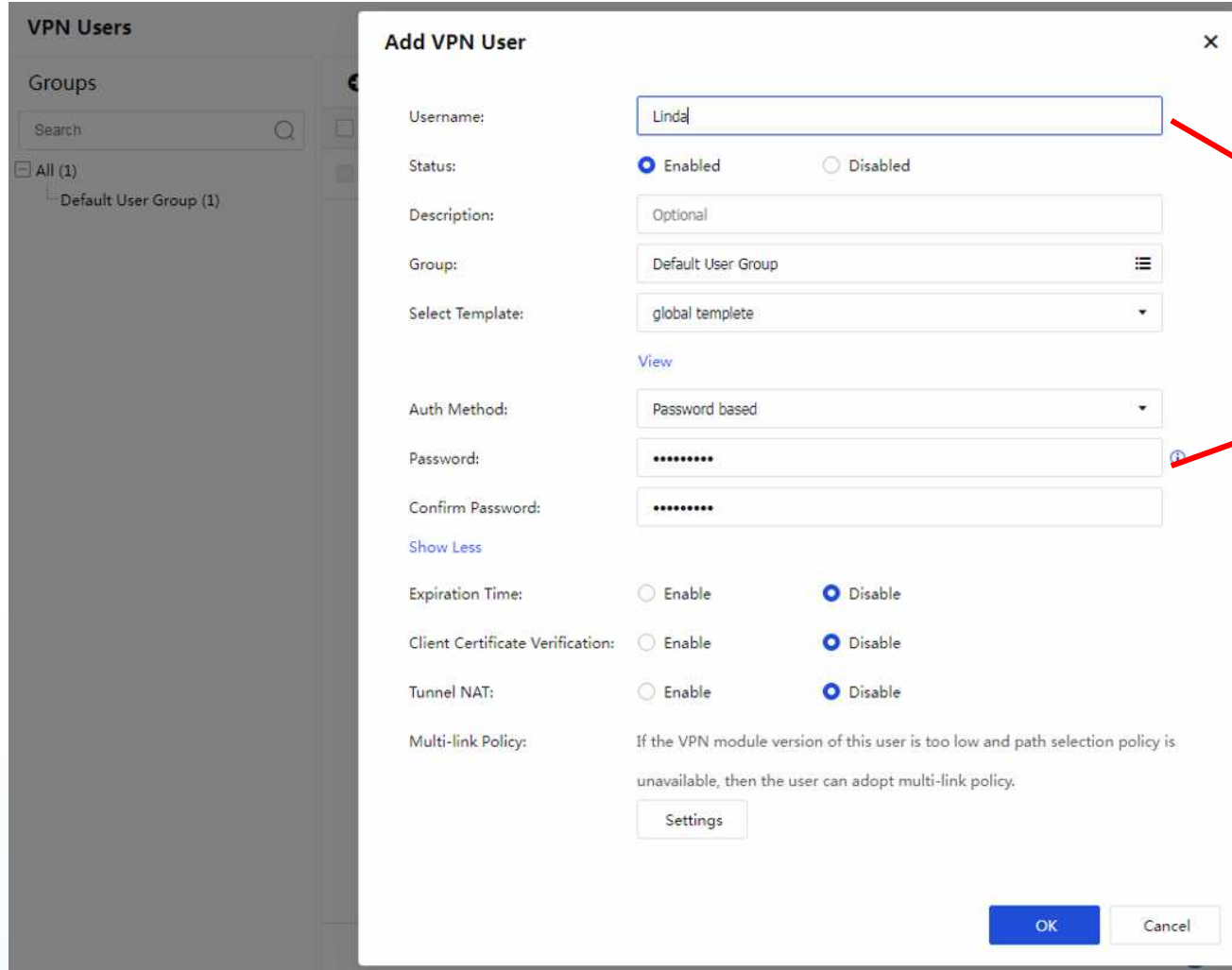
- Intranet Interface: eth3
- VPN Interface: IPv4, Auto Assign, 139.21.14.254

The 'Local Subnet' table is also visible:

Local Subnet	Netmask	Route Priority	Operation
10.0.0.0	24	-	Edit Delete

It is required in case the device is deployed in single-arm mode and no WAN interface is configured with IP address.

HQ Local Users setting



VPN Users

Groups

Search

All (1)

Default User Group (1)

Add VPN User

Username:

Status: Enabled Disabled

Description:

Group:

Select Template:

View

Auth Method:

Password:

Confirm Password:

Show Less

Expiration Time: Enable Disable

Client Certificate Verification: Enable Disable

Tunnel NAT: Enable Disable

Multi-link Policy: If the VPN module version of this user is too low and path selection policy is unavailable, then the user can adopt multi-link policy.

Settings

OK Cancel

Set the Username and password for VPN authentication

Branch setting: VPN connection:

VPN Connection

+ Add - Delete

HQ Device

VPN Connection [X]

HQ Device:

Status: Enabled Disabled

Description:

Shared Key:

Primary IP Address: ⓘ

Secondary IP Address: ⓘ

Username:

Auth Method:

Password:

Protocol:

[VPN Connection Auto Recovery](#)

[Show More](#)

Set the peer name

Set the Shared Key, it must be same with HQ

Set the HQ webagent

Set the username and password

Protocol can be TCP or UDP

	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	No
Multicast service	No	Yes
Static public IP	At least one	No
Company support	Most company	Only Sangfor

PART 3

SSL VPN

SSL VPN for client VPN connection, making customer work convenient anywhere and anytime.

SSL VPN support:

Win XP, Win 7, Win 8, Win 10;

Linux Ubuntu 12.04.5, 14.04.5, 14.04.6, 17.04, 18.04.1

Linux Kylin v6.0, v7.0(64bits)

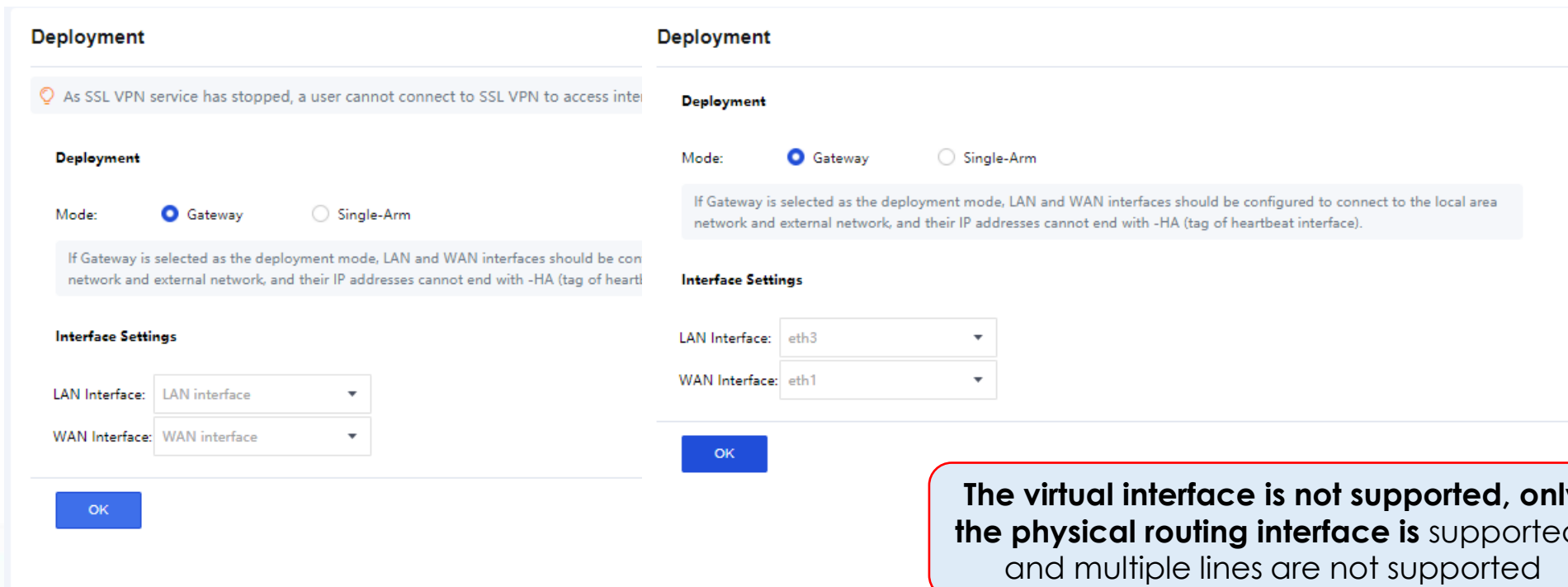
Mac OS 10.8/10.9/10.10/10.11/10.12/10.13/10.14/10.15;

Android 4.0 and later versions;

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

SSL VPN setting:

SSL Deployment, go to **Network > SSL VPN > Deployment**. Before you configure the deployment, you will need to start the SSL VPN service:



The screenshot displays the 'Deployment' configuration page for SSL VPN. It is divided into two panels. The left panel shows a warning message: 'As SSL VPN service has stopped, a user cannot connect to SSL VPN to access inter...'. Below this, the 'Deployment' mode is set to 'Gateway' (selected with a radio button) and 'Single-Arm' (unselected). A note states: 'If Gateway is selected as the deployment mode, LAN and WAN interfaces should be con... network and external network, and their IP addresses cannot end with -HA (tag of heartl...'. Under 'Interface Settings', 'LAN Interface' is set to 'LAN interface' and 'WAN Interface' is set to 'WAN interface'. An 'OK' button is at the bottom. The right panel also shows 'Deployment' mode with 'Gateway' selected. A note explains: 'If Gateway is selected as the deployment mode, LAN and WAN interfaces should be configured to connect to the local area network and external network, and their IP addresses cannot end with -HA (tag of heartbeat interface)'. Under 'Interface Settings', 'LAN Interface' is set to 'eth3' and 'WAN Interface' is set to 'eth1'. 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

Users management:

Local Users

| | | | | | | | | Unfold All >> | Search by Name | Search

Search

Default Group

Local Users

Fields marked * are required

Basic Attributes

Name:

Description:

Password:

Confirm:

Mobile Number:

Added To:

Inherit authentication settings from parent group

Authentication Options

User Type: Public user Private user

Primary Authentication: Local password Local database

Virtual IP Assignment: Automatic Specified 0.0.0.0

Expire: Never expire On date 2029-02-22

Status: Enabled Disabled

Secondary Authentication

Hardware ID

Dynamic Token Authentication Select

Assigned Roles

Roles:

The authentication options only support local password as well as Hardware ID and TOTP secondary authentication

Resources:

Resources

- TCP app
- L3VPN**
- Resource group

Resources

Edit L3VPN

Basic Attributes

Fields marked * are required

Name: *

Description:


Type: Protocol:

Address:

Program Path:

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

Added To:

Icon: 

Enable resource

Visible for user

Roles:

Roles

Roles

Fields marked * are required

Basic Attributes

Name: * Role1

Description:

Assigned To: User1

Enable Role

Associated Resources

Select Resource

Name	Type	Description	...
<input type="checkbox"/> WebServer	Other		

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

Login Options:

Login Options

Login Port

HTTPS Port:

Disconnect user if inacti

SSL/TLS Options

SSL/TLS Algorithm: RSA

WebAgent Settings


Enable WebAgent f

+ Add



WebAgent Ad

Login Options

<input type="checkbox"/>	WebAgent Address	Status	...
 No data available			

Defense Against Man-in-the-Middle Attack

Enable defense against man-in-the-middle attack

(It helps to prevent data from being intercepted while user is accessing SSL VPN. If it is checked, user will be required to type word verification code to log in)

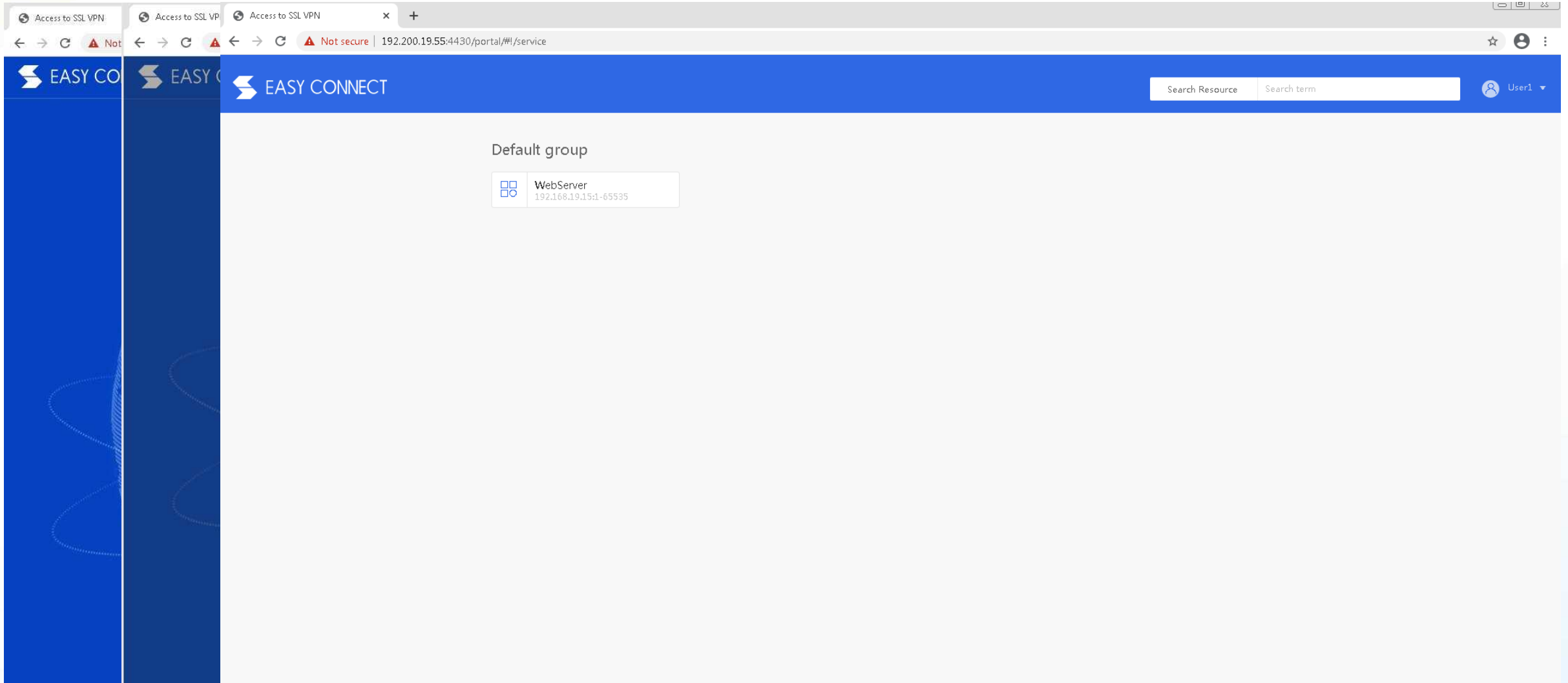
Defense Against Host Header Attack

Enable defense against host header attack

(Access to the following addresses is allowed only. One entry per row, wildcards ? * support)

OK

Client access to SSL



Access to SSL VPN

Access to SSL VPN


Access to SSL VPN

Not secure | 192.200.19.55:4430/portal/#!/service

EASY CONNECT

Search Resource Search term User1

Default group

	WebServer 192.168.19.15:1-65535
---	------------------------------------

THANK YOU

Technical Support Service

Email: tech.support@sangfor.com

Community: community.sangfor.com