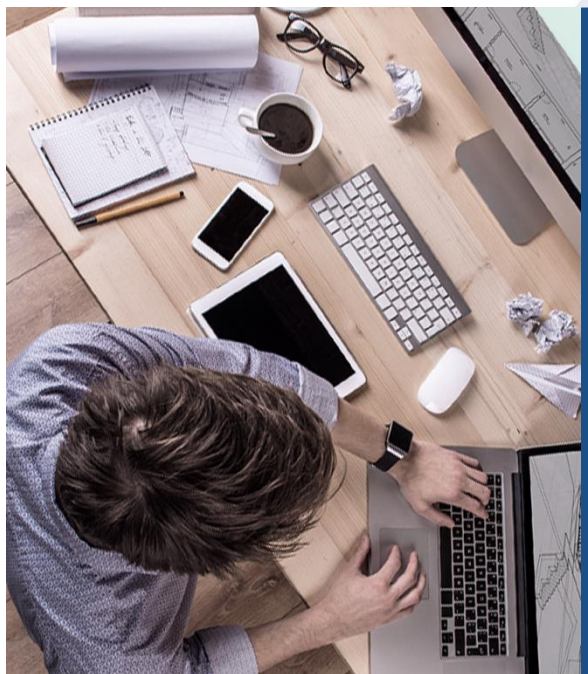




Sangfor NGAF v8.0.6 Associate

VPN





- 1 IPsec VPN
- 2 Sangfor VPN
- 3 VPN SSL

1. IPSec VPN



SANGFOR
深信服科技

IPSEC VPN

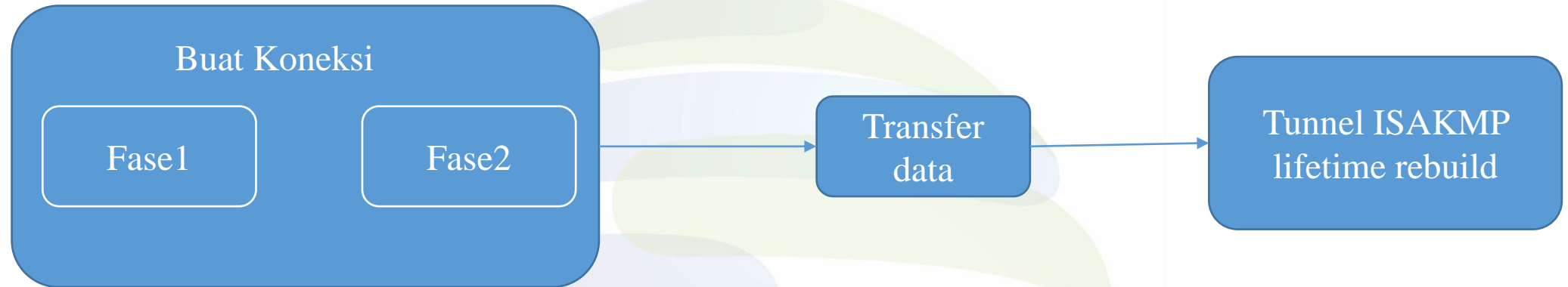
Virtual Private Network (VPN) memperluas jaringan pribadi di atas jaringan internet publik, dan memungkinkan pengguna untuk mengirim dan menerima data melalui jaringan bersama atau jaringan publik seolah-olah perangkat komputasi mereka terhubung langsung ke jaringan pribadi.

Internet Protocol Security (IPsec) adalah rangkaian protokol jaringan yang mengotentikasi dan mengenkripsi paket data yang dikirim melalui jaringan.

IPsec mendukung otentikasi peer tingkat jaringan, **otentikasi asal data, integritas data, kerahasiaan data (enkripsi)**, dan proteksi reply.

Semua produk keamanan Sangfor mendukung IPsec VPN.

IPSEC VPN



Tahap1:

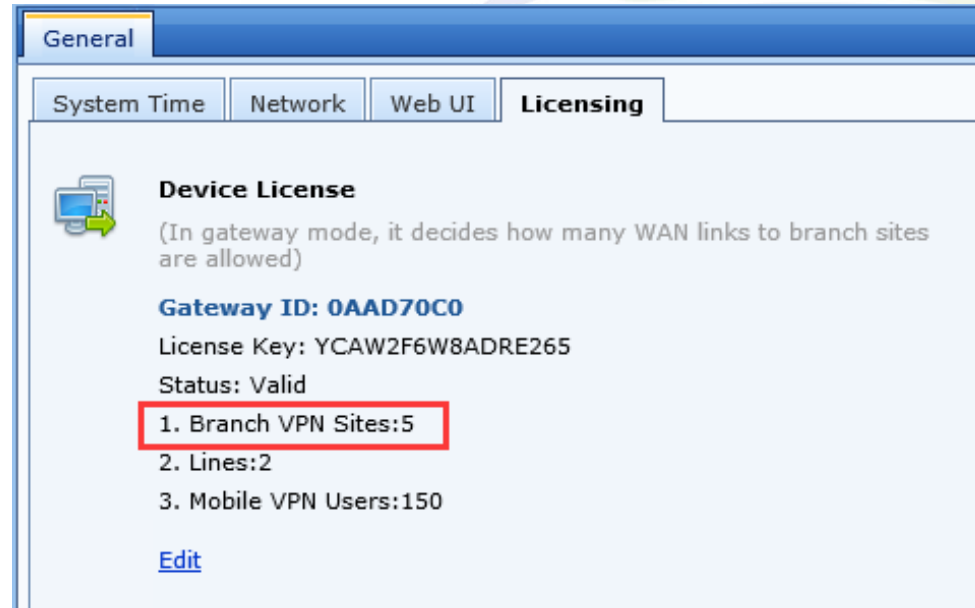
1. Mode: Utama / Agresif
2. Pertukaran SA: Algoritma otentikasi / Algoritma enkripsi / Grup DH / life time ISAKMP
3. Pertukaran Pre-Shared Key
4. Tukar dan Verifikasi ID
5. Lainnya: NAT / DPD

Fase2:

1. Protokol: AH / ESP
2. PFS
3. Enkripsi: DES / 3DES / AES128. Hash: MD5 / SHA
4. SA lifetime
5. Subnet lokal dan subnet peer

IPSEC VPN

1. NGAF harus memiliki lisensi site VPN Cabang (Branch) untuk membentuk IPsec VPN :



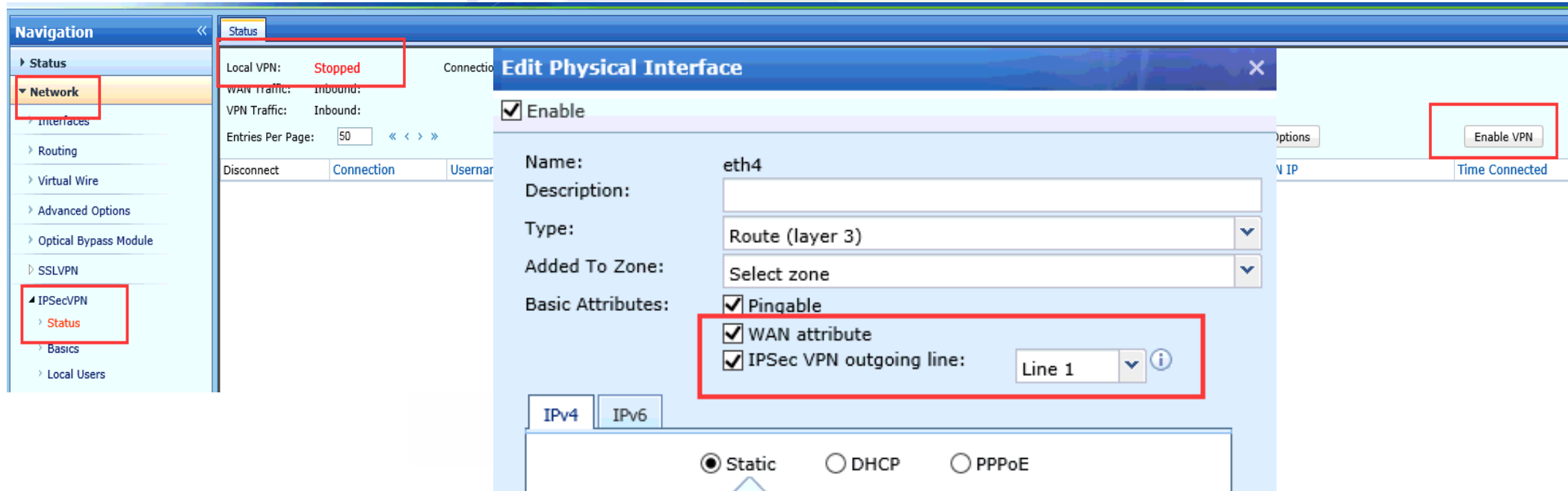
2. Mulai versi 8.0.2, route interface WAN-attribute (interface non-manajemen Eth0) tidak lagi dibutuhkan dalam IPsec.

3. Mulai versi 8.0.2, sub-interface, interface VLAN dan interface agregat dapat digunakan untuk membentuk VPN.

IPSEC VPN

Jika Anda ingin membangun VPN, Anda perlu mengaktifkan (enable) layanan VPN dan mengatur jalur pada interface.

Jalur keluar pada fase I harus sama dengan jalur keluar pada route interface WAN attribute.



The screenshot displays the Sangfor VPN configuration interface. On the left, the 'Navigation' pane shows the 'Network' section expanded, with 'IPSecVPN' and its 'Status' sub-item highlighted. The main area is titled 'Edit Physical Interface' and shows the configuration for interface 'eth4'. Key settings include:

- Local VPN:** Stopped (highlighted with a red box).
- Enable:** Checked (checkbox).
- Name:** eth4.
- Type:** Route (layer 3).
- Added To Zone:** Select zone.
- Basic Attributes:**
 - ☒ Pingable
 - ☒ WAN attribute
 - ☒ IPSec VPN outgoing line: Line 1 (highlighted with a red box).
- Enable VPN:** Button (highlighted with a red box).

At the bottom, the 'Static' radio button is selected for the interface configuration.

Studi Kasus VPN IPSEC

Pelanggan ingin berkomunikasi di dua site dengan menggunakan alamat IP internal.

Sangfor:

IP publik statis, langsung terhubung ke internet.

Fortinet / FortiGate:

ADSL, langsung terhubung ke internet.

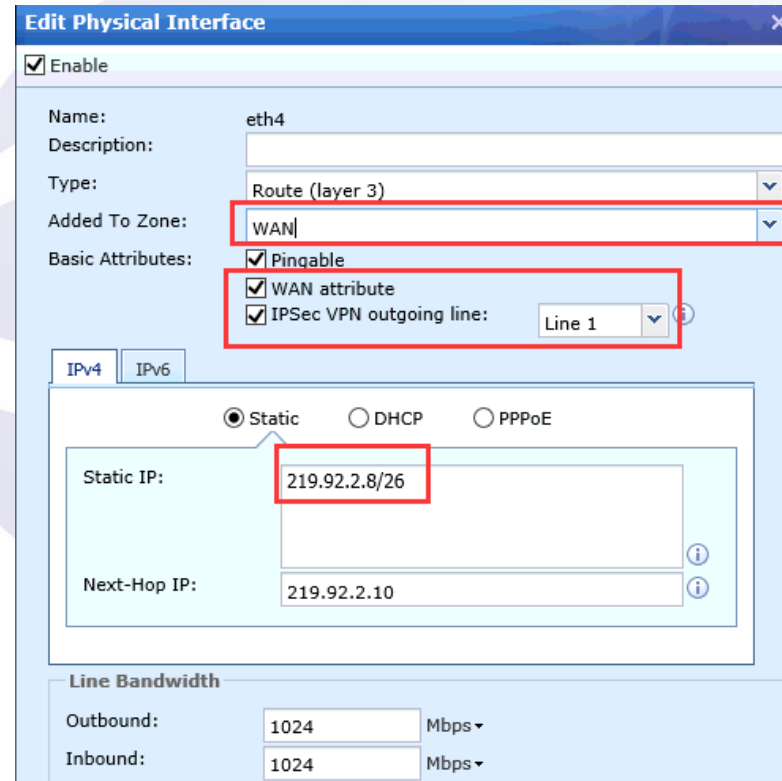
Pelanggan ingin menghubungkan sisi intranet satu sama lain menggunakan IPSec VPN



Kedua site ini dapat dihubungkan dengan IPsec VPN.

IPSEC VPN

1. Konfigurasi interface dan zona, Jalur konfigurasi: [Network] -> [Interface].



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

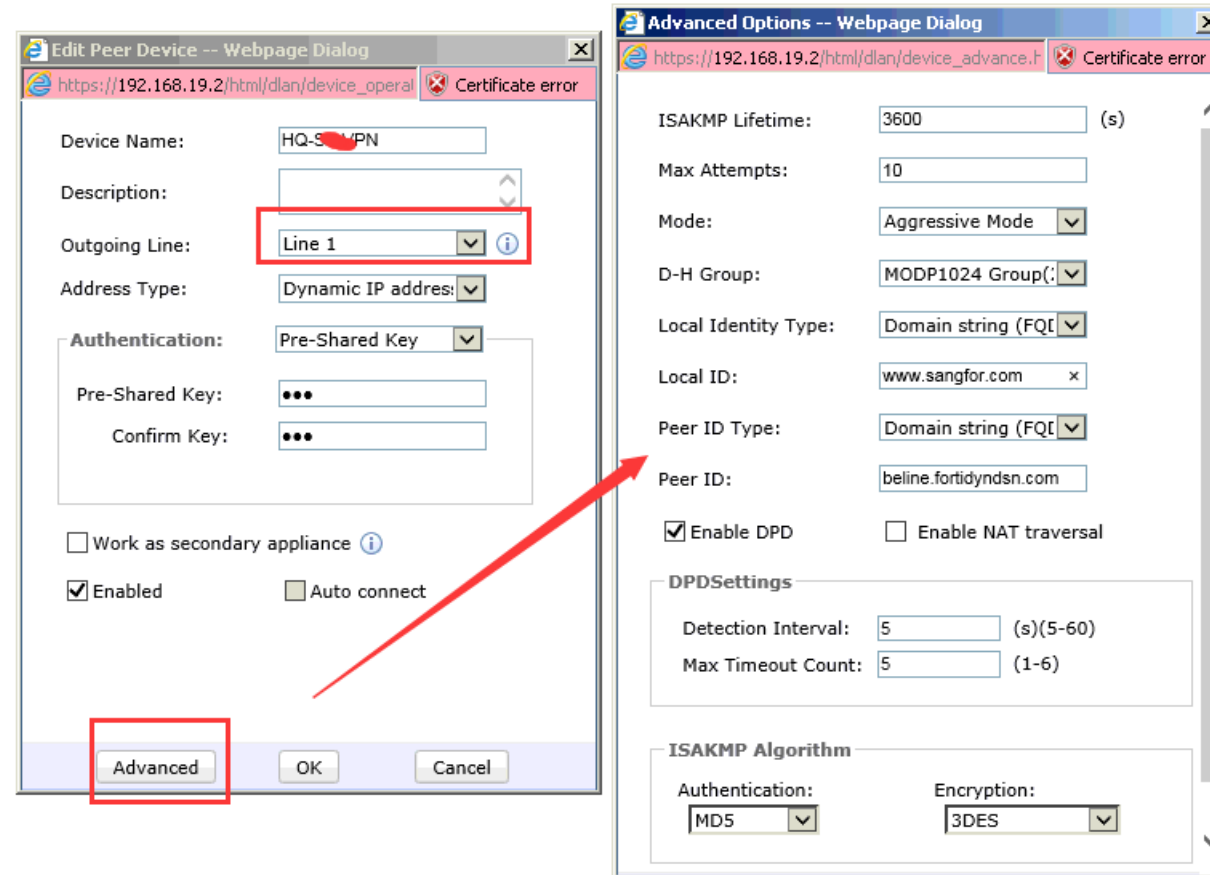
Line Bandwidth

Outbound: 1024 Mbps

Inbound: 1024 Mbps

IPSEC VPN

2. Pengaturan Fase I.



The image displays two overlapping web browser windows from the Sangfor VPN management interface. 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 detailed Phase 1 settings. It includes fields 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 "Enable NAT traversal" is unchecked. 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
https://192.168.19.2/html/dlan/device_operal Certificate error

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
https://192.168.19.2/html/dlan/device_advance Certificate error

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. Pengaturan Fase II.

Phase II

https://219.92.100.1/html/dlan/policy_operate.html

Inbound Policy

Add Delete

☐ Status Policy Name

Page 1

Outbound Policy

Add Delete

☐ Status Policy Name

Page 1

Policy Name: HQ-1

Description:

Source: Subnet

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 : 0

☒ Enable This Policy

Kebijakan koneksi masuk

https://219.92.100.1/html/dlan/policy_operate.html

Policy Name: HQ-1

Description:

Source: Subnet

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 : 0

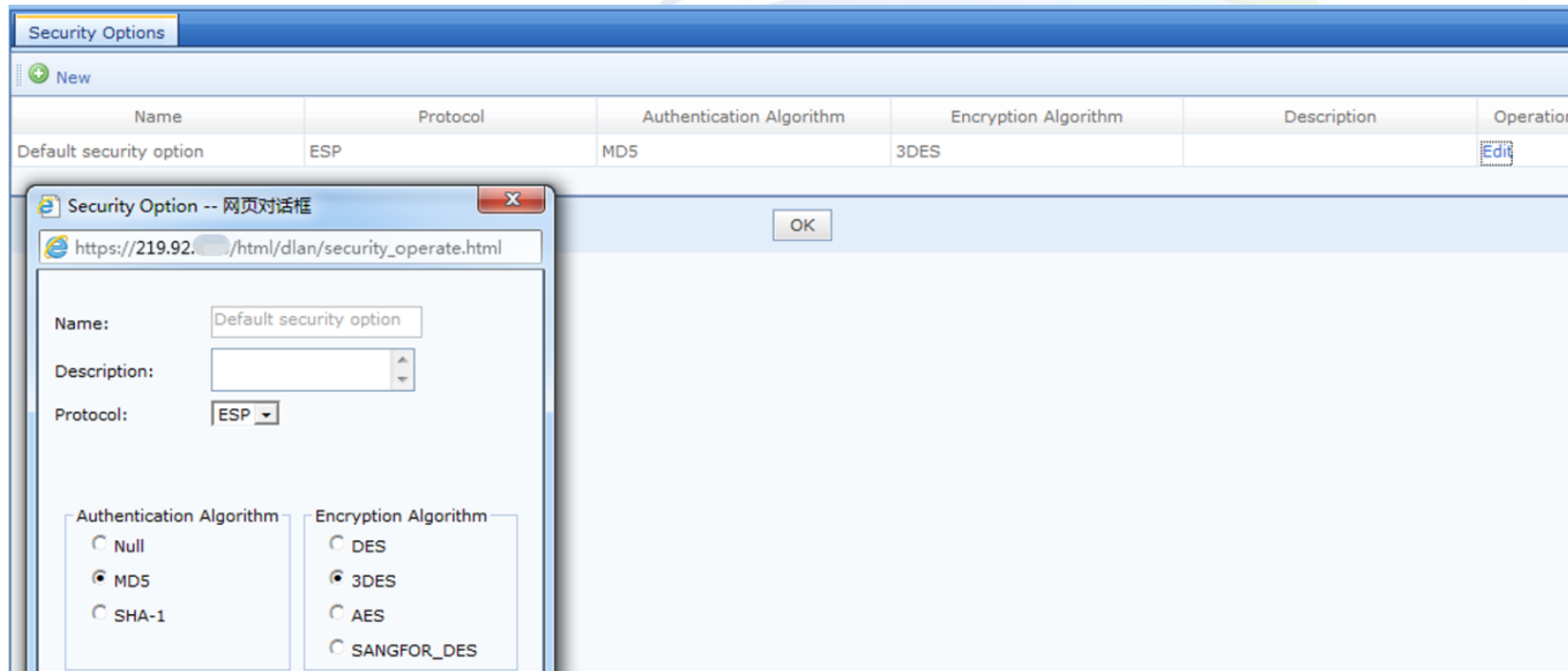
☒ Enable This Policy

☒ Perfect Forward Secrecy

Kebijakan koneksi keluar

IPSEC VPN

4. Opsi keamanan di-setting sama seperti peer.



IPSEC VPN

5. Setelah konfigurasi berhasil, kita dapat melihat tunnel di status VPN IPsec.

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-  -HQ-JB	HQ-  -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 menyediakan dua jenis koneksi VPN yaitu, IPSEC VPN standar, dan SANGFOR VPN yang dikembangkan sendiri, untuk menyediakan koneksi perangkat-ke-perangkat dan PC (windows)-ke-perangkat. SANGFOR DLAN memiliki keuntungan sebagai berikut jika dibandingkan dengan IPSEC VPN standar :

1. Mendukung kedua ujungnya meskipun keduanya menggunakan IP publik dinamis (tidak tetap).
2. Kemampuan teknologi multi-jalur VPN untuk load balancing jalur VPN.
3. Pengguna di cabang terhubung ke HQ untuk mendapat koneksi internet sehingga dapat dikontrol sepenuhnya dari HQ melalui jalur tunnel.
4. Teknologi tunnel NAT digunakan untuk memecahkan masalah apabila beberapa cabang menggunakan segmen IP yang sama (konflik).
5. Teknologi flow-control pada tunnel digunakan untuk menjamin alokasi bandwidth.

Sangfor VPN

Penggunaan Sangfor VPN:

HQ:

Menyediakan layanan akses VPN, dan menyediakan verifikasi akun dari pengguna VPN lainnya. DLAN di HQ membutuhkan konfigurasi WebAgent dan Akun VPN untuk akses. Umumnya, HQ berfungsi sebagai jaringan server.

Cabang:

Akses ke sisi HQ. Umumnya, cabang berfungsi sebagai jaringan klien.

Mobile:

SANGFOR VPN, yang juga dikenal sebagai PDLAN merupakan perangkat lunak yang dapat dipakai oleh pengguna (klien) individu untuk membangun akses VPN ke HQ sebagai pengguna mobile.

Perangkat VPN bisa bertindak sebagai HQ ataupun cabang.

Sangfor VPN

Istilah Sangfor VPN:

WebAgent:

Untuk melakukan interkoneksi SANGFOR VPN.

Baik site cabang maupun pengguna individu harus mengetahui alamat IP HQ untuk membuat koneksi VPN.

Anda dapat mengkonfigurasi WebAgent dengan beberapa cara:

1. IP:Port, misalnya.123.123.123.123:4009

Cocok digunakan apabila Perangkat VPN HQ memiliki sebuah alamat IP publik statik.

2. IP1 # IP2:Port, misalnya 123.123.123.123 # 221.221.221.221:4009

Apabila perangkat VPN HQ memiliki lebih dari satu IP Publik statik ke beberapa fixed line, untuk keperluan back up koneksi dan load balancing.

3. Format Web URL, misalnya: webagent.sangfor.com.cn/webagent/123.php

Apabila perangkat VPN HQ tidak memiliki IP Publik statik, seperti bila menggunakan koneksi ADSL.

(Selama proses pengalamatan, informasi dienkripsi dengan DES.)



Sangfor VPN



Konfigurasi dasar untuk membuat koneksi VPN antara HQ dan cabang atau mobile adalah sebagai berikut:

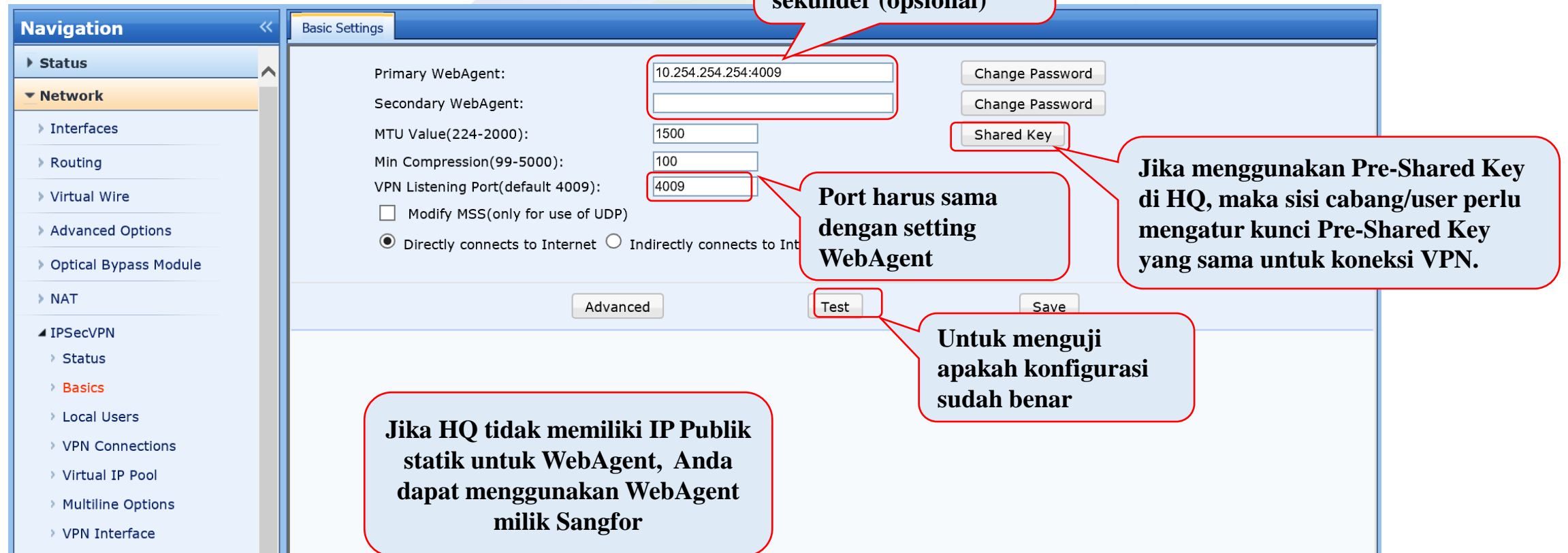
- 1) HQ: Perlu mengkonfigurasi WebAgent, pool IP virtual (opsional), dan pengguna.
- 2) Cabang: hanya perlu mengkonfigurasi manajemen koneksi.
- 3) Mobile: Install software mobile PDLAN, konfigurasi pengaturan dasar dan pengaturan parameter koneksi utama.

NGAF 8.0.7 tidak lagi mendukung PDLAN.

Sangfor VPN

Pengaturan HQ:

Pengaturan WebAgent:



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 area is titled 'Basic Settings' and contains 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 'Directly connects to Internet'. Buttons for 'Change Password', 'Shared Key', 'Test', and 'Save' are visible. Several red callout boxes provide instructions: 'Masukkan IP & Port WebAgent primer & sekunder (opsional)' points to the Primary and Secondary WebAgent fields; 'Port harus sama dengan setting WebAgent' points to the VPN Listening Port field; 'Jika menggunakan Pre-Shared Key di HQ, maka sisi cabang/user perlu mengatur kunci Pre-Shared Key yang sama untuk koneksi VPN.' points to the Shared Key field; 'Untuk menguji apakah konfigurasi sudah benar' points to the Test button; and 'Jika HQ tidak memiliki IP Publik statik untuk WebAgent, Anda dapat menggunakan WebAgent milik Sangfor' points to the Primary WebAgent field.

Masukkan IP & Port WebAgent primer & sekunder (opsional)

Port harus sama dengan setting WebAgent

Jika menggunakan Pre-Shared Key di HQ, maka sisi cabang/user perlu mengatur kunci Pre-Shared Key yang sama untuk koneksi VPN.

Untuk menguji apakah konfigurasi sudah benar

Jika HQ tidak memiliki IP Publik statik untuk WebAgent, Anda dapat menggunakan WebAgent milik Sangfor

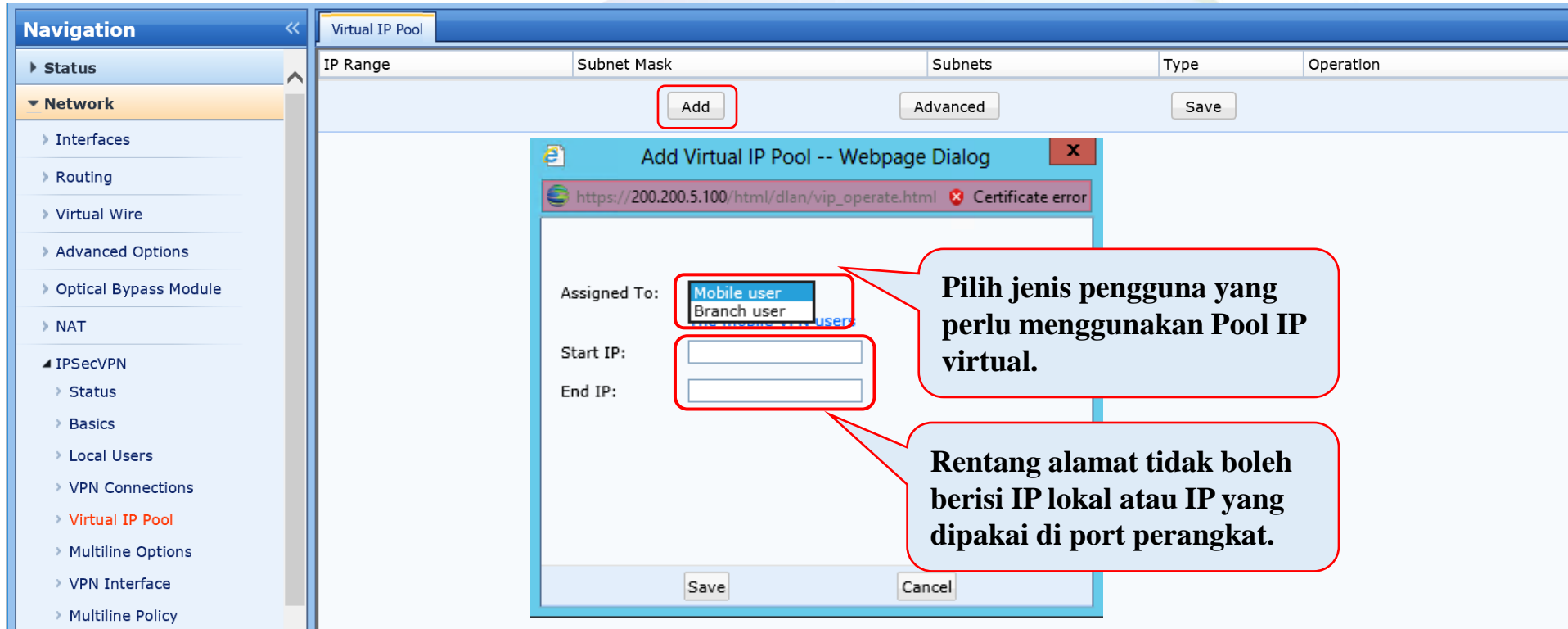
Tambahkan Pengguna:

SANGFOR TECHNOLOGIES

Sangfor VPN

Pengaturan HQ:

Pool IP Virtual:



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. 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', showing a 'Certificate error' message. The dialog contains fields for 'Assigned To' (with a dropdown menu showing 'Mobile user' and 'Branch user'), 'Start IP', and 'End IP'. Two red callout boxes provide instructions: one points to the 'Assigned To' dropdown with the text 'Pilih jenis pengguna yang perlu menggunakan Pool IP virtual.' and the other points to the IP range fields with the text 'Rentang alamat tidak boleh berisi IP lokal atau IP yang dipakai di port perangkat.'

Apabila pengguna VPN mobile ataupun cabang mengaktifkan NAT Tunnel, Anda perlu mengkonfigurasi pool IP virtual, jika tidak maka tidak dapat dikonfigurasi.

Sangfor VPN

Pengaturan Cabang: Koneksi VPN:



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	Outgoing

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

Masukkan IP WebAgent HQ, nama dan kata sandi pengguna untuk koneksi VPN. Protokol dapat menggunakan UDP atau TCP

Aktifkan koneksi

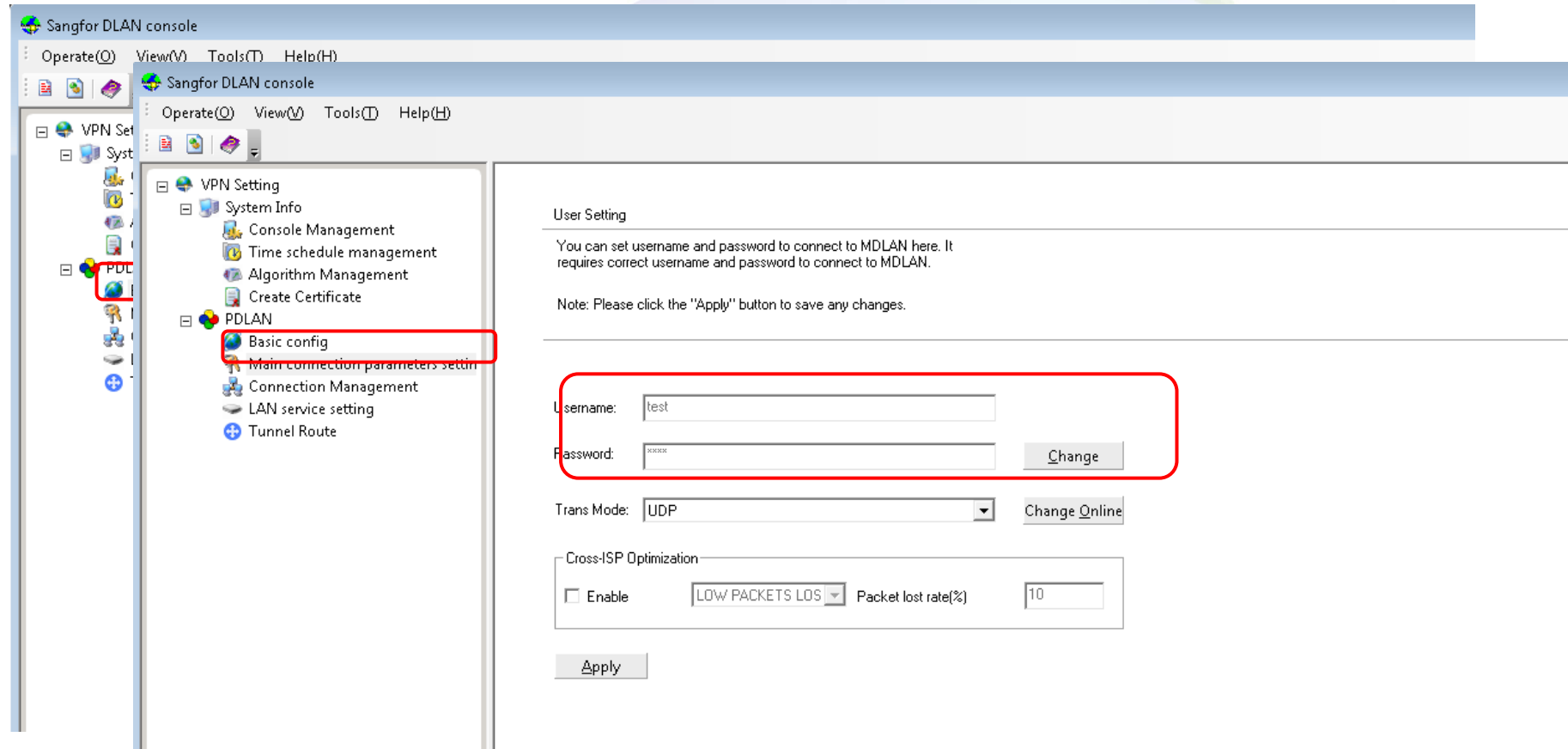
LAN Service Save Cancel

Sangfor VPN



Mobile (PDLAN):

Setelah menginstal PDLAN, masukkan WebAgent HQ, nama dan kata sandi pengguna untuk koneksi VPN.



PDLAN dapat diunduh dari web Sangfor: <http://www.sangfor.com/service/firmware.html>

Sangfor VPN



	IPSec VPN	Sangfor VPN
Port	UDP 500, 4500	TCP/UDP 4009 default; dapat diganti
NAT Tunnel	Tidak	Ya
Mendukung Multiple Line	Tidak	Ya
Route Tunnel	Tidak	Ya
Tunnel Service Control	Tidak	Ya
Tunnel Traffic Control	Tidak	Ya
Layanan multicast	Tidak	Ya
IP Publik Statik	Setidaknya satu	Tidak
Dukungan Mobile	Software Lain	PDLAN (hanya PC windows)
Dukungan perusahaan	Sebagian besar perusahaan	Hanya Sangfor

3. SSL VPN



SANGFOR
深信服科技

VPN SSL

Sangfor NGAF tidak hanya menyediakan PDLAN, tetapi juga mendukung SSL VPN untuk koneksi VPN klien, membuat klien bekerja dengan nyaman di mana saja dan kapan saja.

Dukungan SSL VPN:

Win XP, Win 7, Win 8, Win 10; (Hanya mendukung browser IE)

Mac OS 10.8 / 10.9 / 10.10 / 10.11;

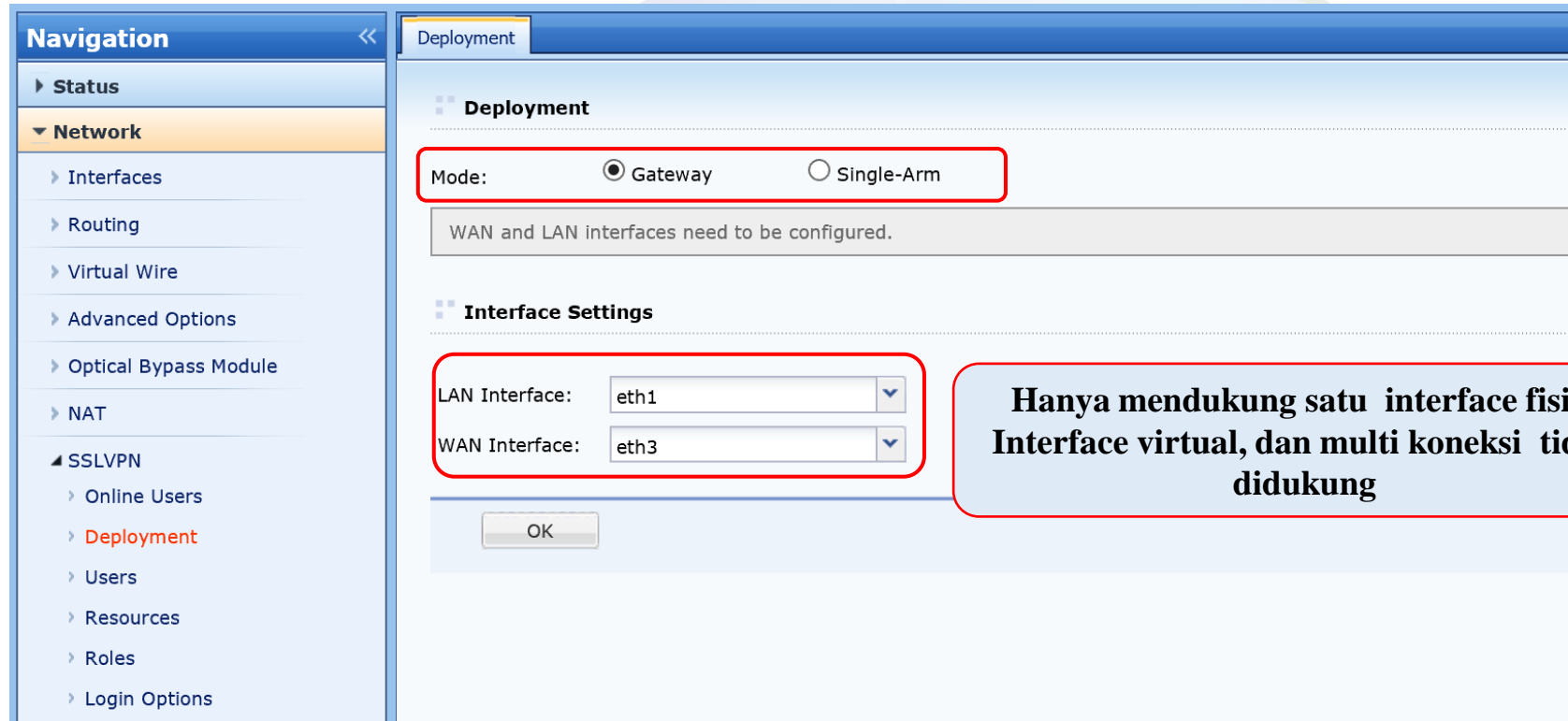
Android 4.0 dan versi yang lebih baru;

IOS 9 dan versi yang lebih baru; (Perlu mengunduh perangkat lunak bernama Easy Connect dari App Store)

VPN SSL

Pengaturan SSL VPN:

Deployment SSL:



The screenshot shows the Sangfor SSL VPN management interface. On the left is a 'Navigation' sidebar with a tree view containing 'Status', 'Network' (expanded), 'Interfaces', 'Routing', 'Virtual Wire', 'Advanced Options', 'Optical Bypass Module', 'NAT', 'SSLVPN' (selected), 'Online Users', 'Deployment' (highlighted in red), 'Users', 'Resources', 'Roles', and 'Login Options'. The main content area is titled 'Deployment' and contains two sections: 'Deployment' and 'Interface Settings'. In the 'Deployment' section, the 'Mode' is set to 'Gateway' (selected with a radio button) and 'Single-Arm' (unselected). Below this, a message states 'WAN and LAN interfaces need to be configured.' The 'Interface Settings' section shows 'LAN Interface' set to 'eth1' and 'WAN Interface' set to 'eth3', both in dropdown menus. A red box highlights these two interface settings. At the bottom of the main area is an 'OK' button. A red box also highlights the 'Mode' selection.

Deployment

Mode: ☒ Gateway ☐ Single-Arm

WAN and LAN interfaces need to be configured.

Interface Settings

LAN Interface: eth1

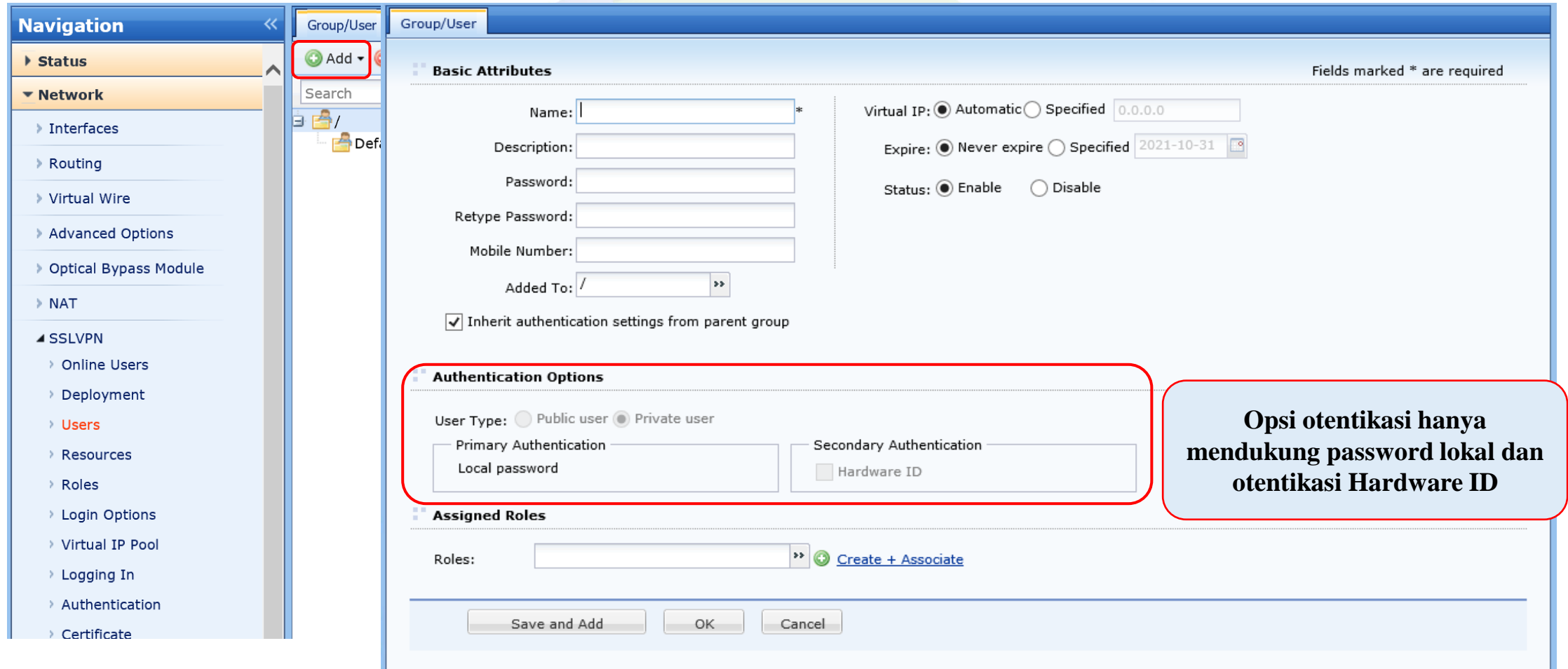
WAN Interface: eth3

OK

**Hanya mendukung satu interface fisik.
Interface virtual, dan multi koneksi tidak didukung**

VPN SSL

Manajemen pengguna:



The screenshot displays the Sangfor SSLVPN management interface. On the left is a 'Navigation' sidebar with categories like Status, Network, and SSLVPN. The 'Add' button in the 'Group/User' section is highlighted with a red box. The main area shows the 'Basic Attributes' and 'Authentication Options' for a new user or group. The 'Authentication Options' section, also highlighted with a red box, shows 'User Type' set to 'Private user' and 'Primary Authentication' set to 'Local password'. A text box on the right states: 'Opsi otentikasi hanya mendukung password lokal dan otentikasi Hardware ID'. The 'Assigned Roles' section at the bottom has a 'Roles' field and a 'Create + Associate' button. At the very bottom are 'Save and Add', 'OK', and 'Cancel' buttons.

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

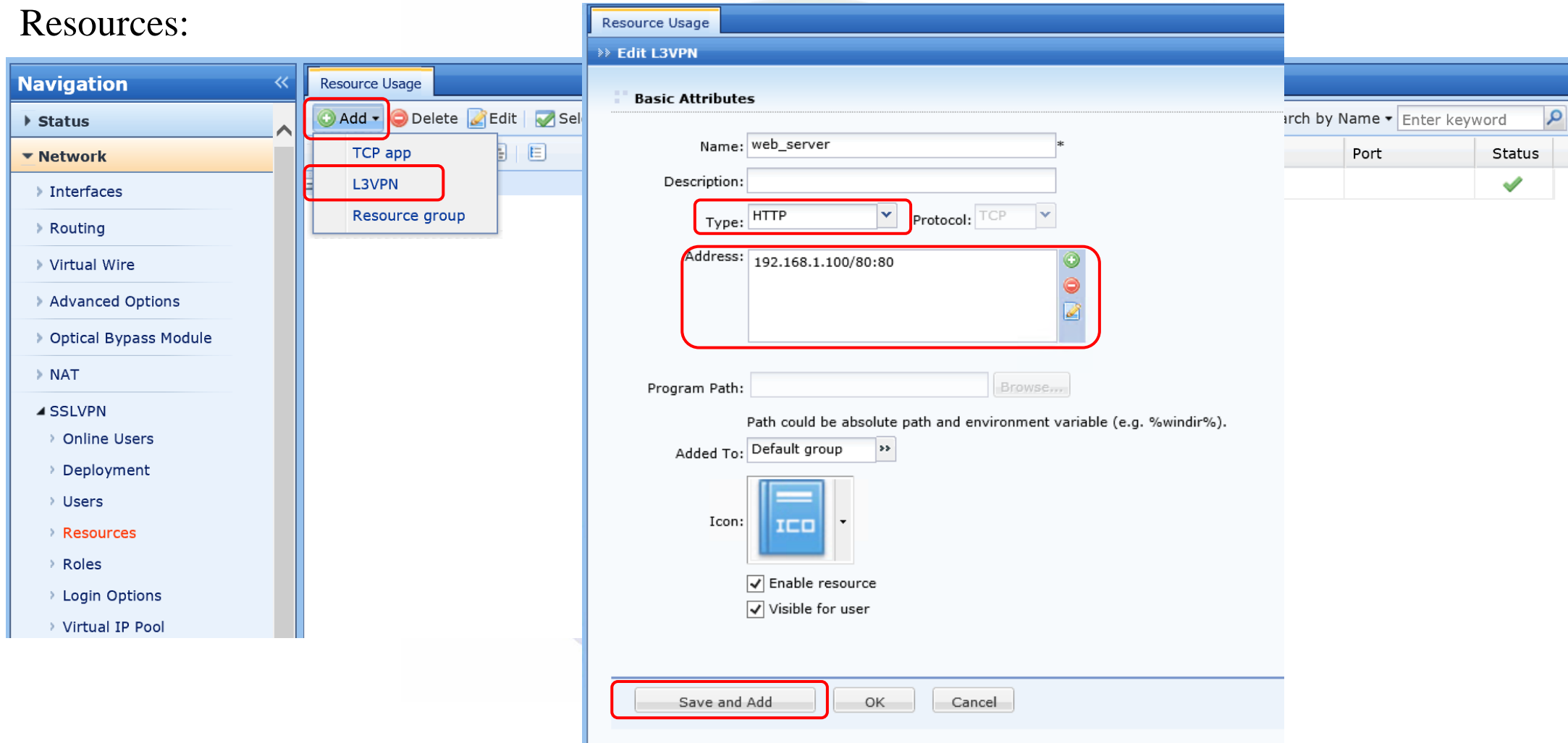
Assigned Roles

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

Opsi otentikasi hanya mendukung password lokal dan otentikasi Hardware ID

VPN SSL

Resources:



The screenshot displays the Sangfor VPN SSL management interface. On the left, the 'Navigation' pane shows the 'Resources' section under 'SSLVPN'. The 'Resource Usage' tab is active, showing a list of resources with 'Add', 'Delete', 'Edit', and 'Select' buttons. 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' field shows a blue folder icon. The 'Enable resource' and 'Visible for user' checkboxes are both checked.

The 'Save and Add' button is highlighted at the bottom of the dialog box.

SSL VPN

Peran:

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

Setelah pengguna dihubungkan dengan resource tertentu, maka pengguna / grup dapat mengakses resource tersebut melalui SSL VPN.

VPN SSL

Opsi Masuk:

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: 4430

Disconnect user if inactivity period reaches 30 (5-43200) minutes. (local DNS must not be enabled)

WebAgent Settings

☐ Enable WebAgent for dynamic IP assignment

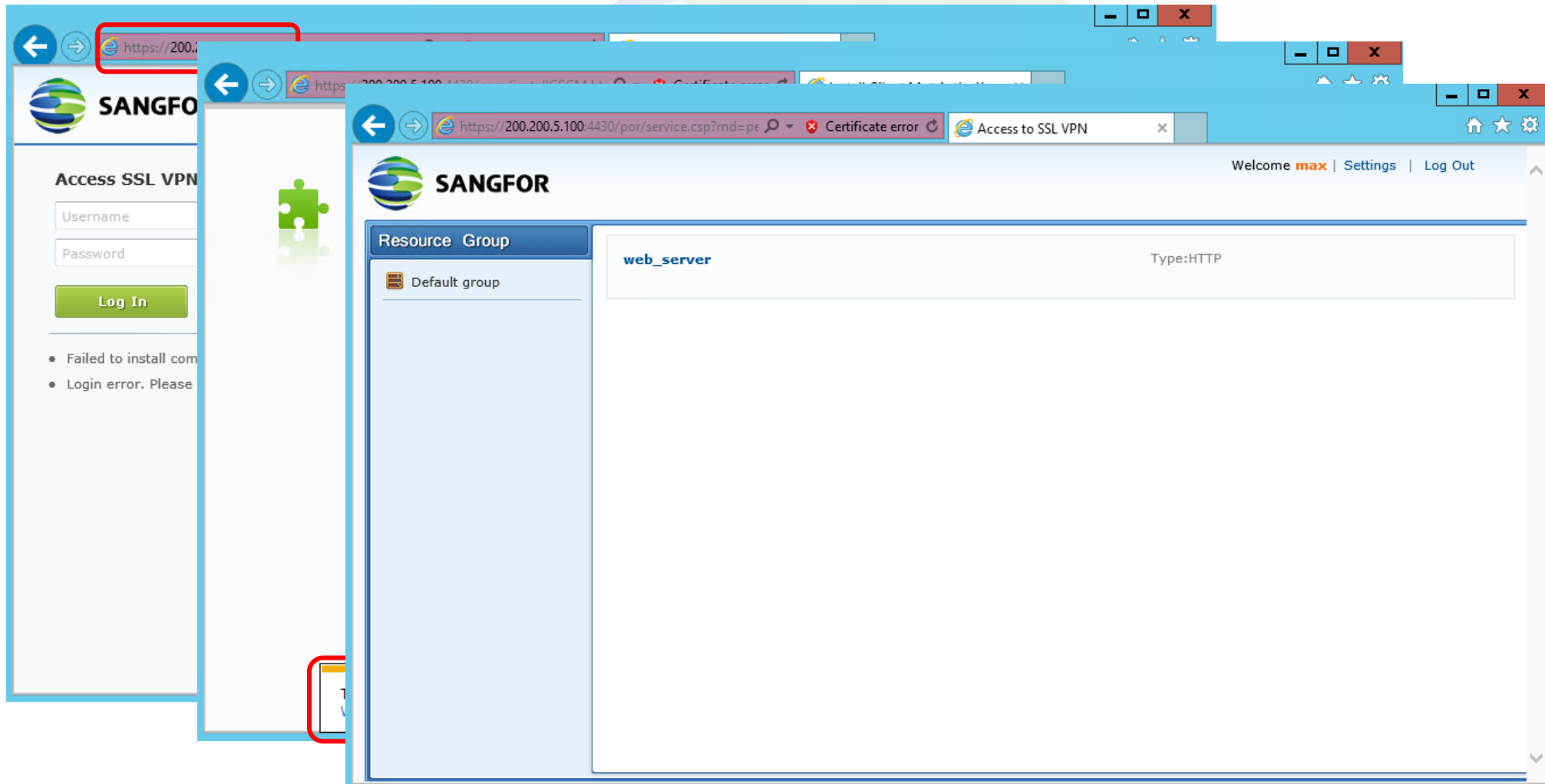
+ Add - Delete Edit Test Refresh

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

OK

VPN SSL

Akses klien ke SSL VPN:



Terima kasih !

tech.support@sangfor.com
community.sangfor.com

Sangfor Technologies (HQ)
Block A1, Nanshan iPark, No.1001
Xueyuan Road, Nanshan District,
Shenzhen, Guangdong Province,
P. R. China (518055)

