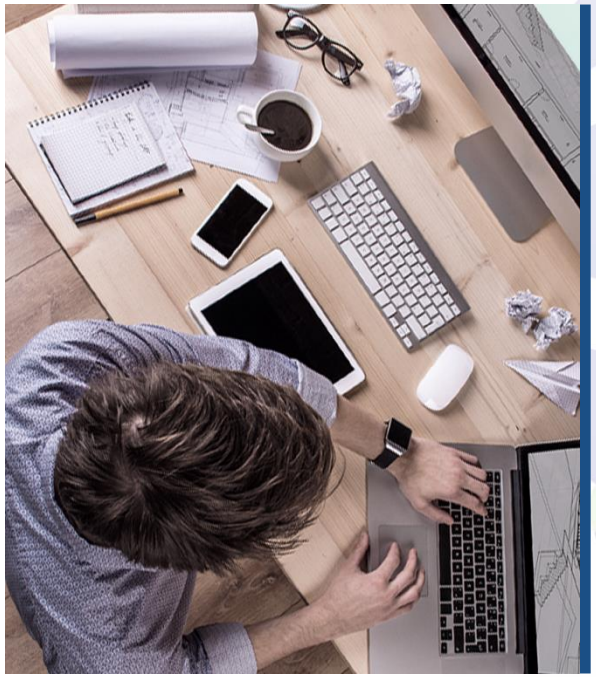
SANGFOR

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

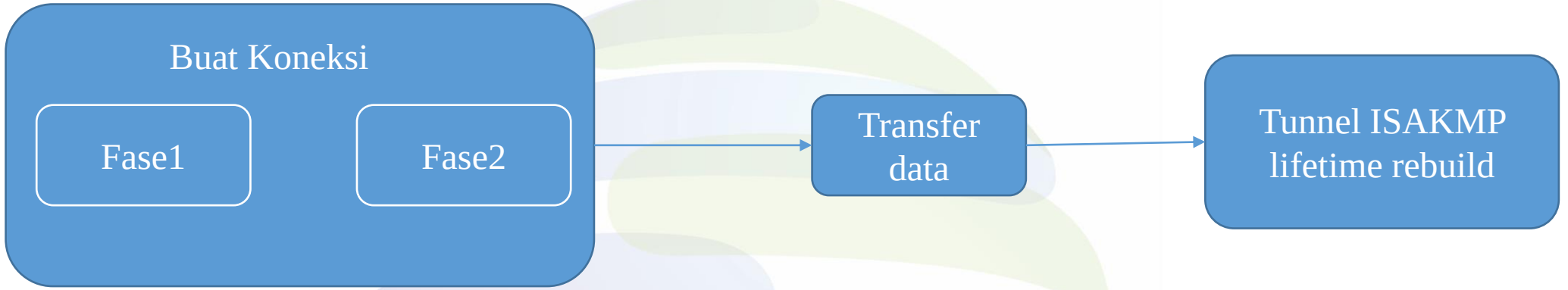
IPSEC VPN

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:

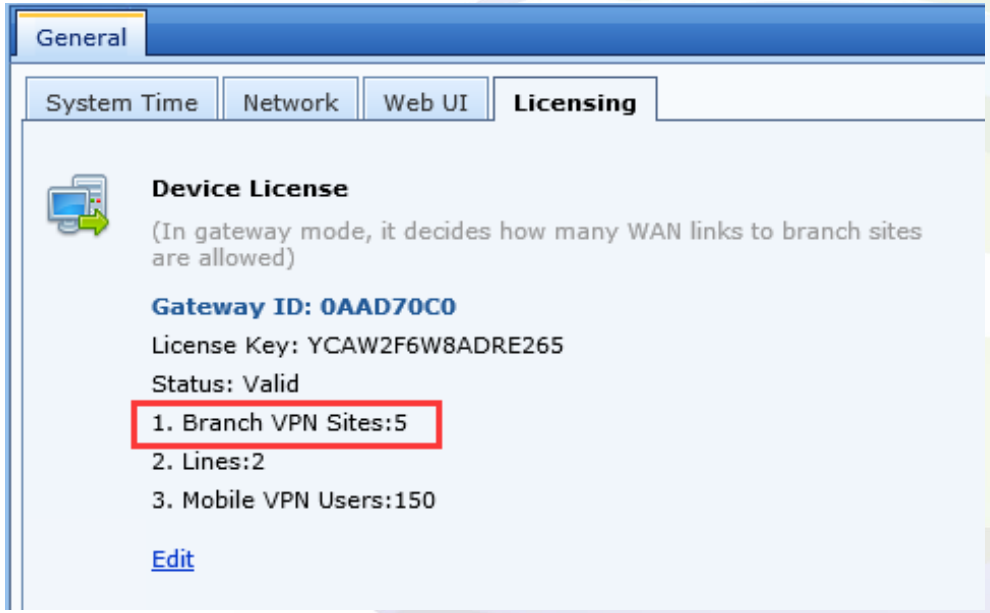
1. Mode: Utama / Agresif
2. Pertukaran SA: Algoritma otentikasi / Algoritma enkripsi / Grup DH / life time ISAKMP
3. Pertukaran Pre-Shared Key
4. Tukar dan Verifikasi ID
5. Lainnya: NAT / DPD

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 :

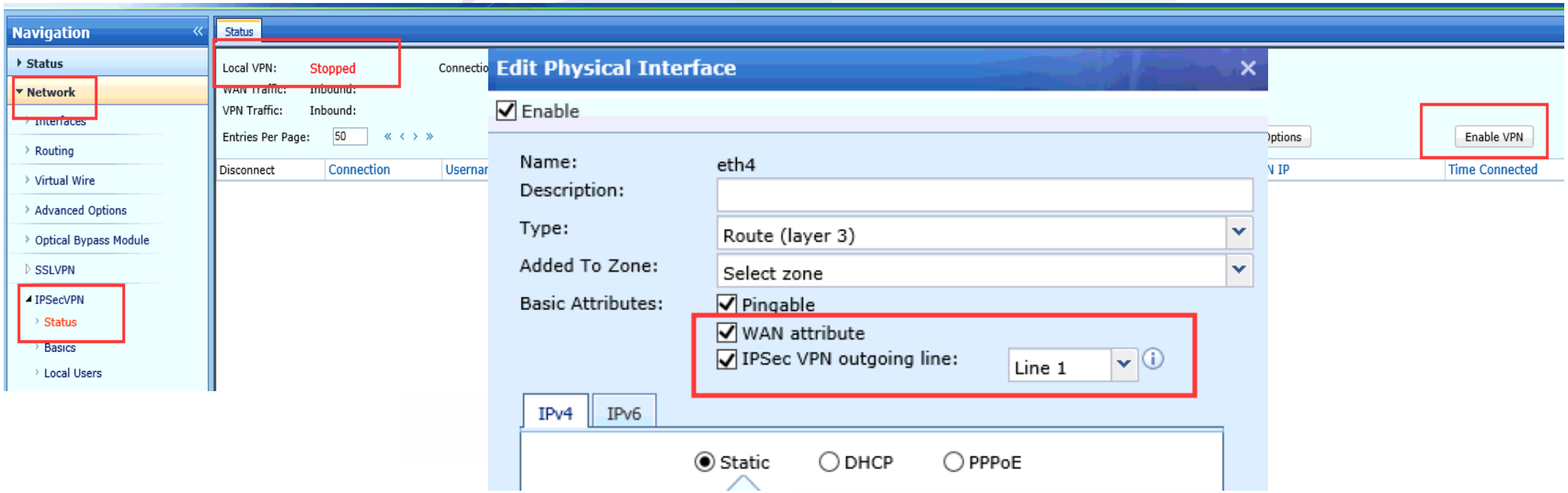


2. Mulai versi 8.0.2, route interface WAN-attribute (interface non-manajemen Eth0) tidak lagi dibutuhkan dalam IPSec.

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.



Studi Kasus VPN IPSEC

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

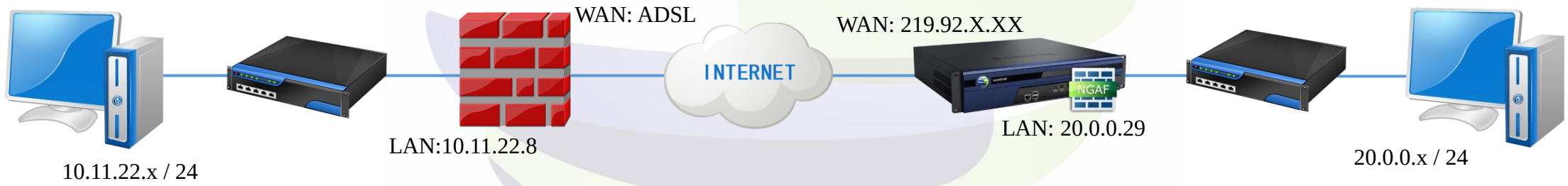
Sangfor:

IP publik statis, langsung terhubung ke internet.

Fortinet / FortiGate:

ADSL, langsung terhubung ke internet.

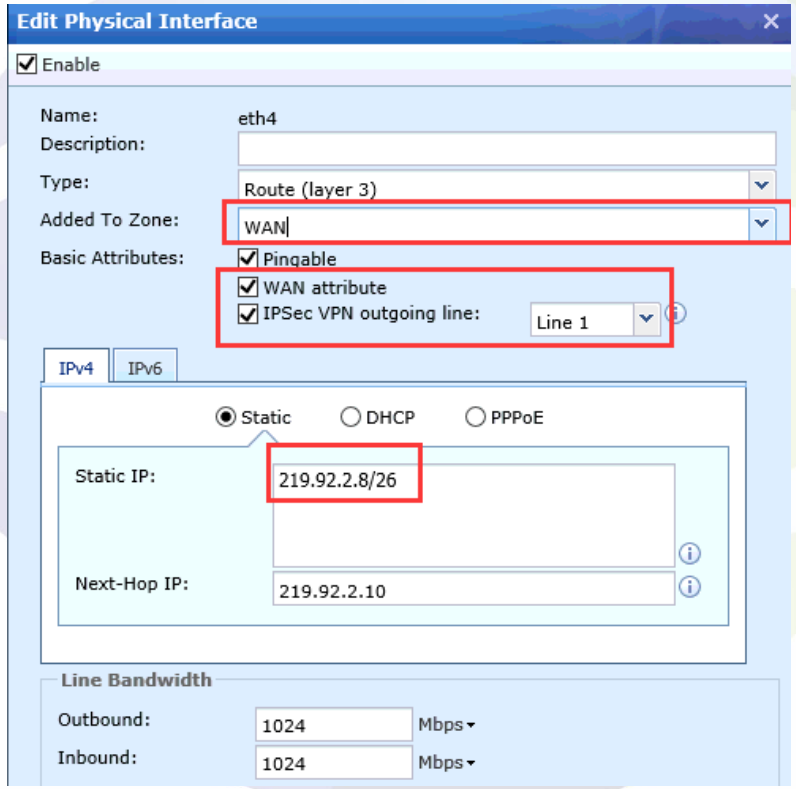
Pelanggan ingin menghubungkan sisi intranet satu sama lain menggunakan IPSec VPN



Kedua site ini dapat dihubungkan dengan IPsec VPN.

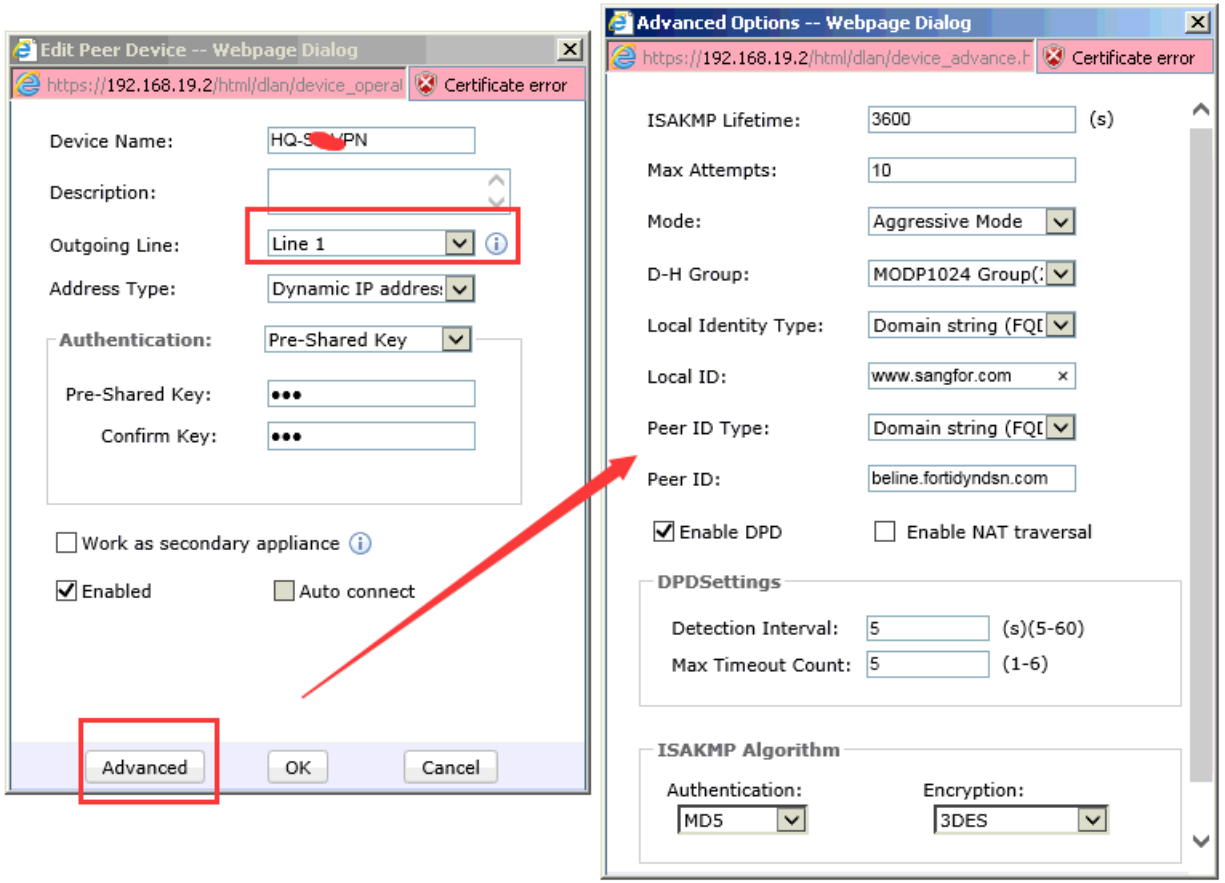
IPSEC VPN

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



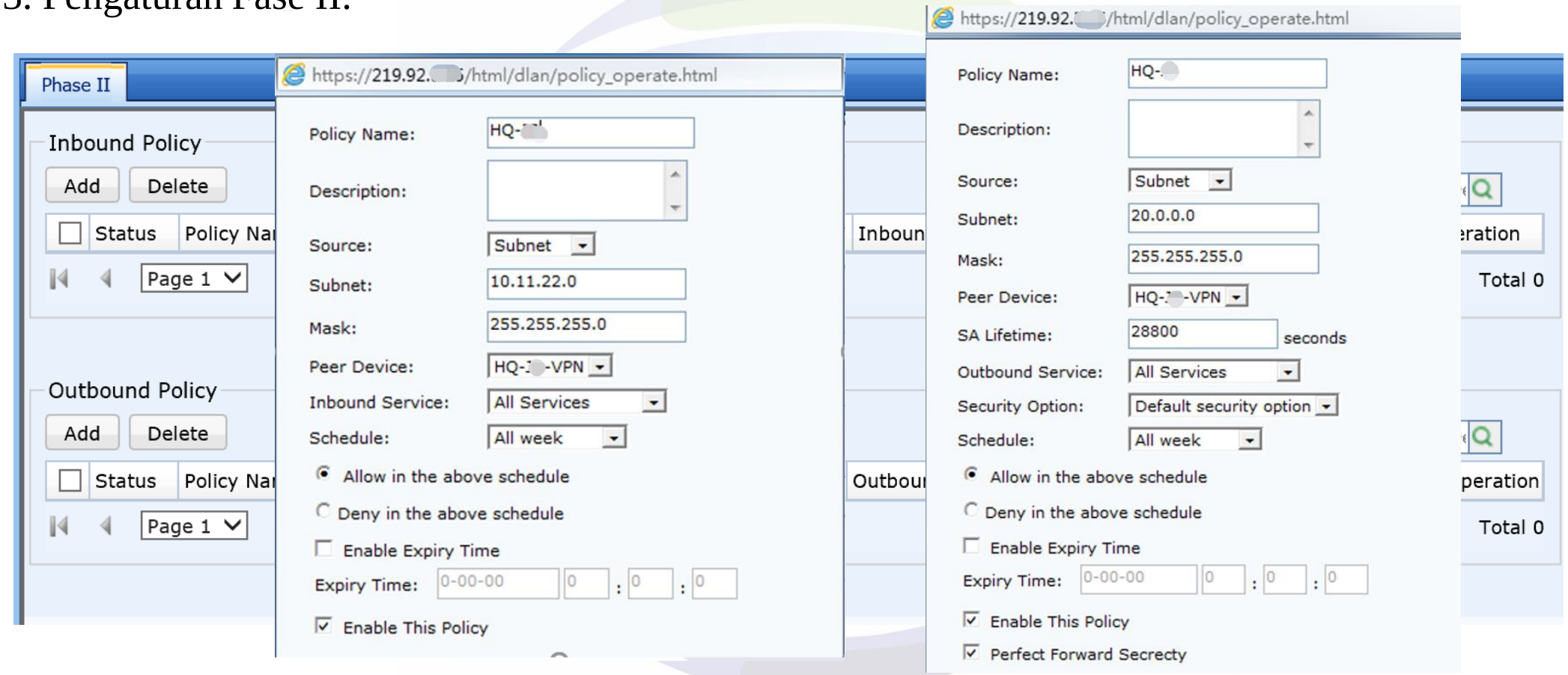
IPSEC VPN

2. Pengaturan Fase I.



IPSEC VPN

3. Pengaturan Fase II.

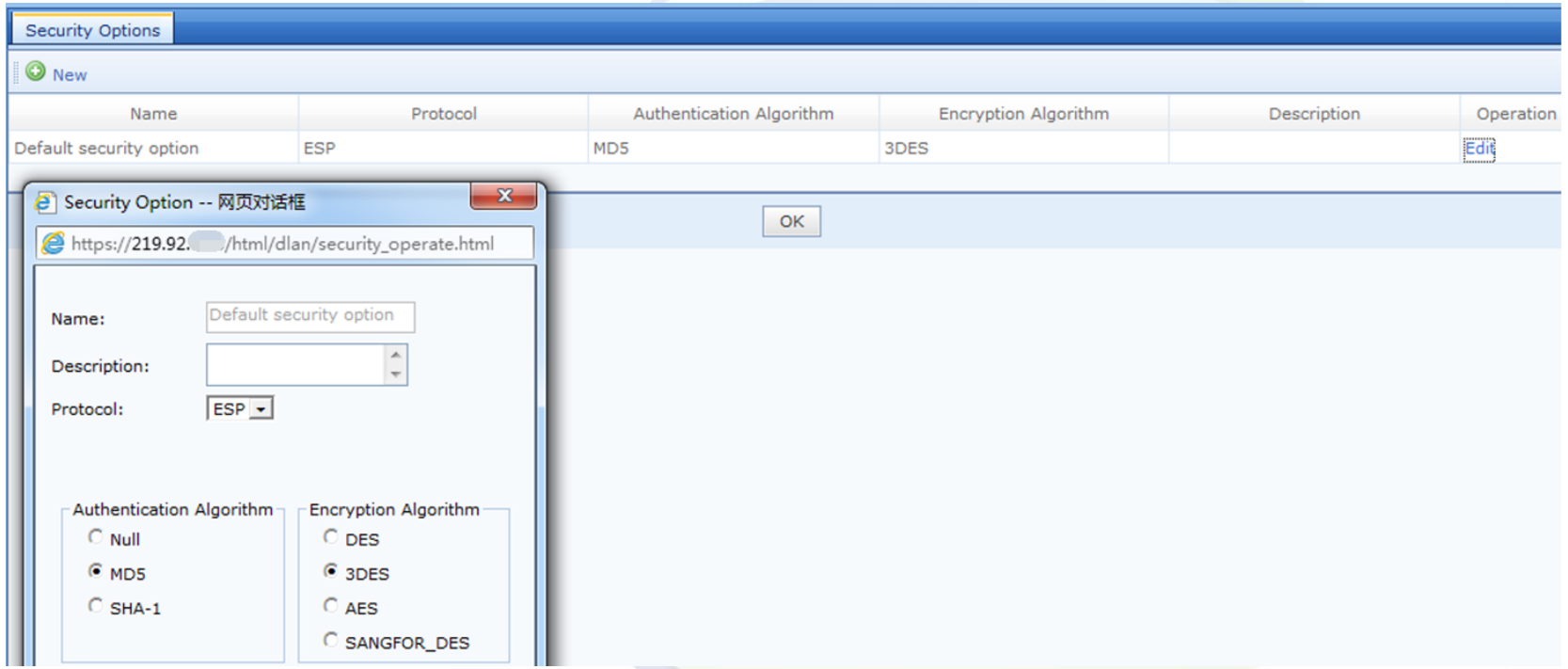


Kebijakan koneksi masuk

Kebijakan koneksi keluar

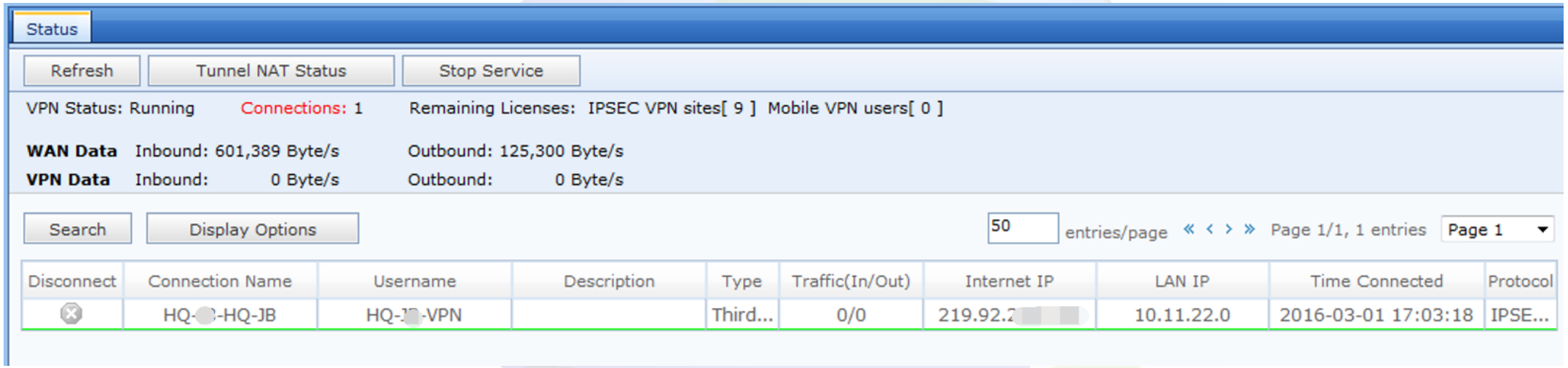
IPSEC VPN

4. Opsi keamanan di-setting sama seperti peer.



IPSEC VPN

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



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:

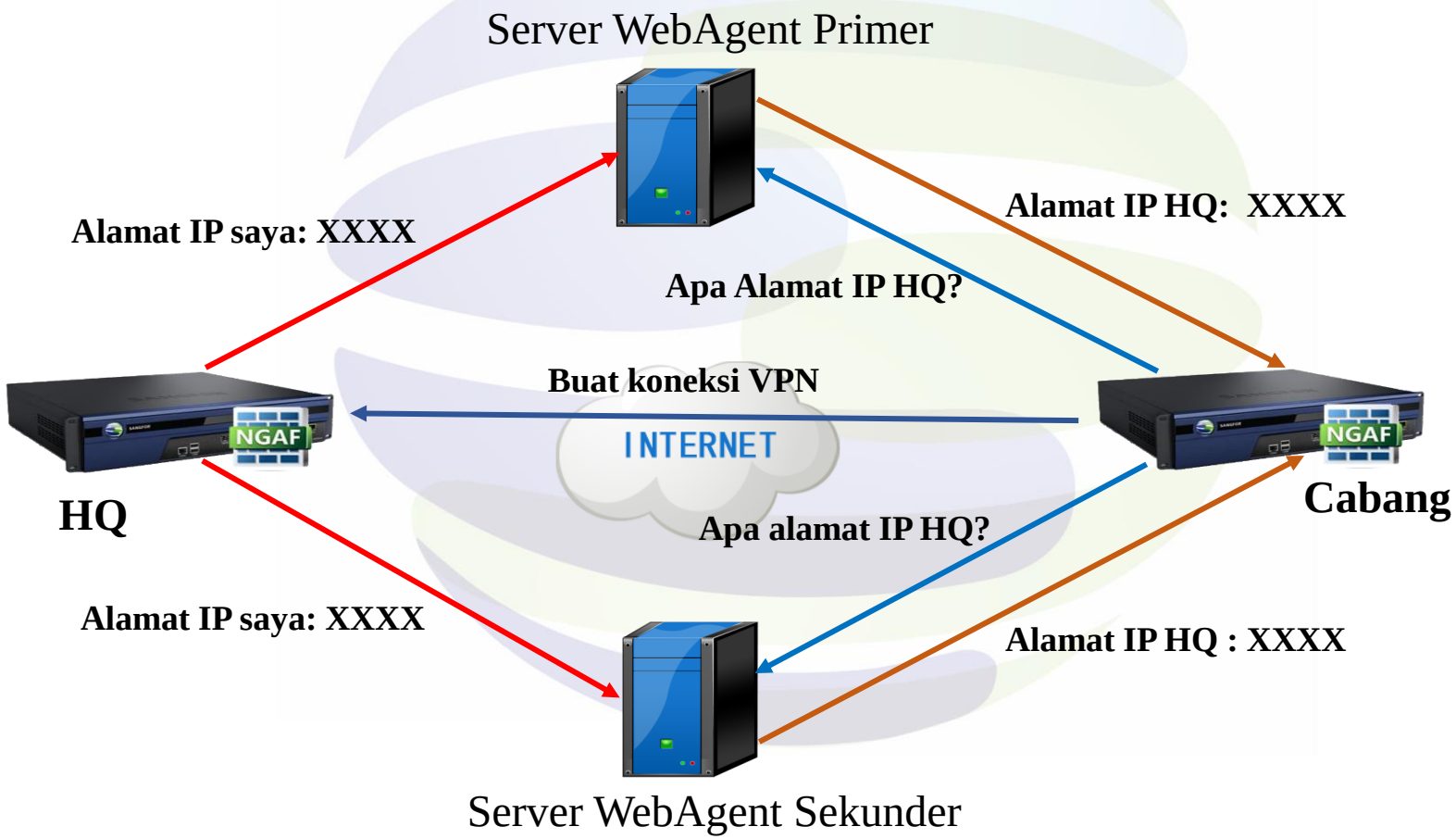
1. IP:Port, misalnya.123.123.123.123:4009
Cocok digunakan apabila Perangkat VPN HQ memiliki sebuah alamat IP publik statik.

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.

Sangfor VPN

Proses pengalamatan WebAgent:
(Selama proses pengalamatan, informasi dienkripsi dengan DES.)



Sangfor VPN

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

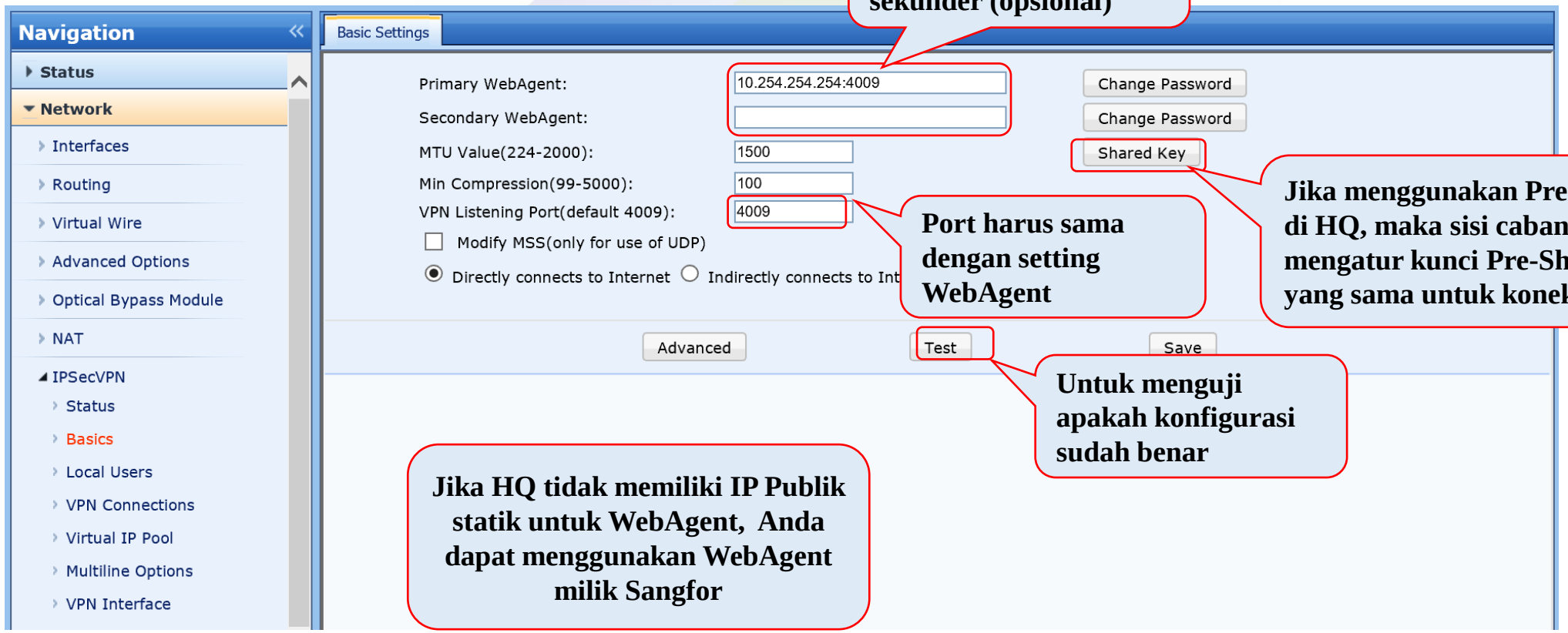
1) HQ: Perlu mengkonfigurasi WebAgent, pool IP virtual (opsional), dan pengguna.
2) Cabang: hanya perlu mengkonfigurasi manajemen koneksi.
3) Mobile: Install software mobile PDLAN, konfigurasi pengaturan dasar dan pengaturan parameter koneksi utama.

NGAF 8.0.7 tidak lagi mendukung PDLAN.

Sangfor VPN

Pengaturan HQ:

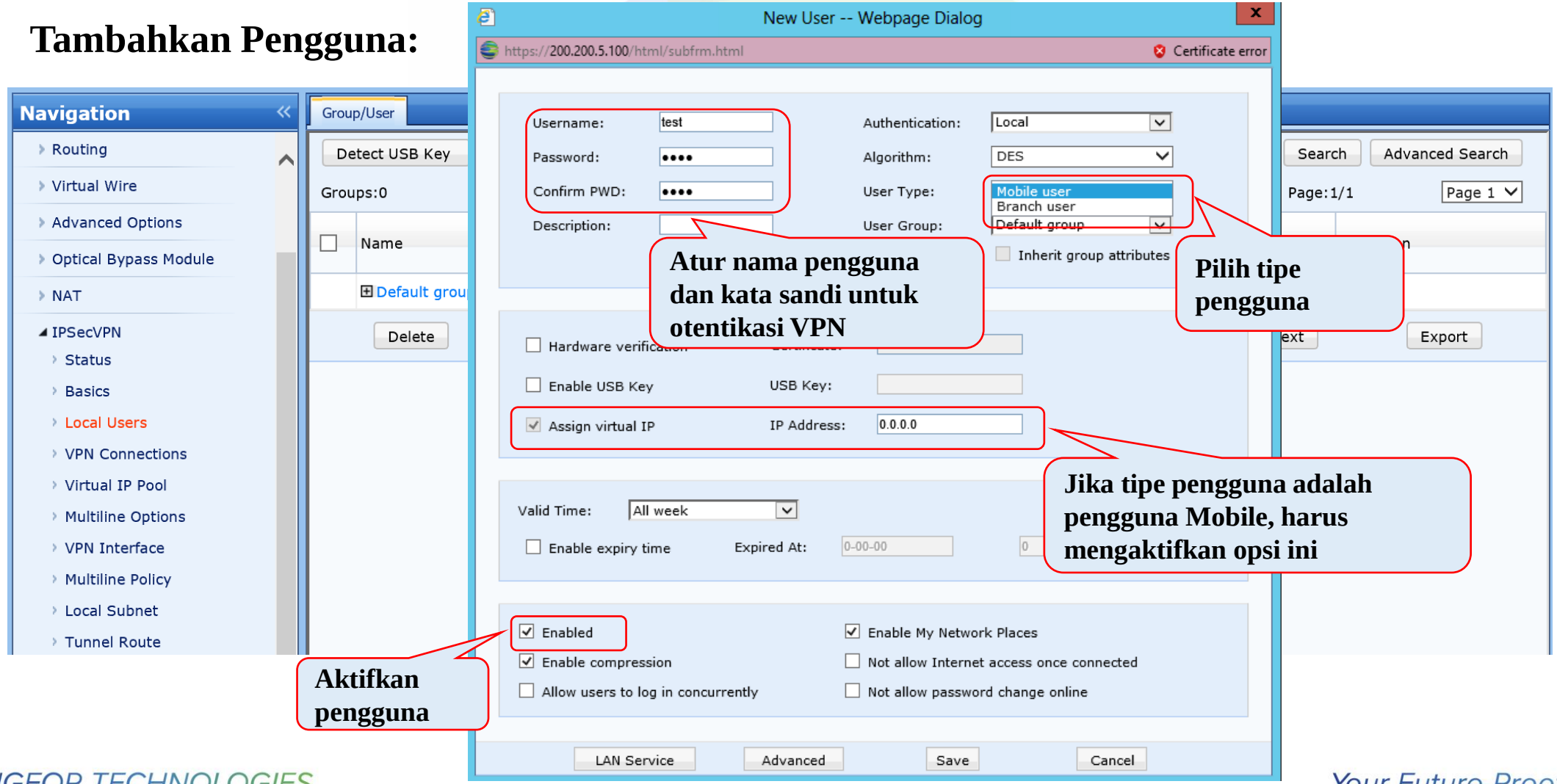
Pengaturan WebAgent:



Sangfor VPN

Pengaturan HQ:

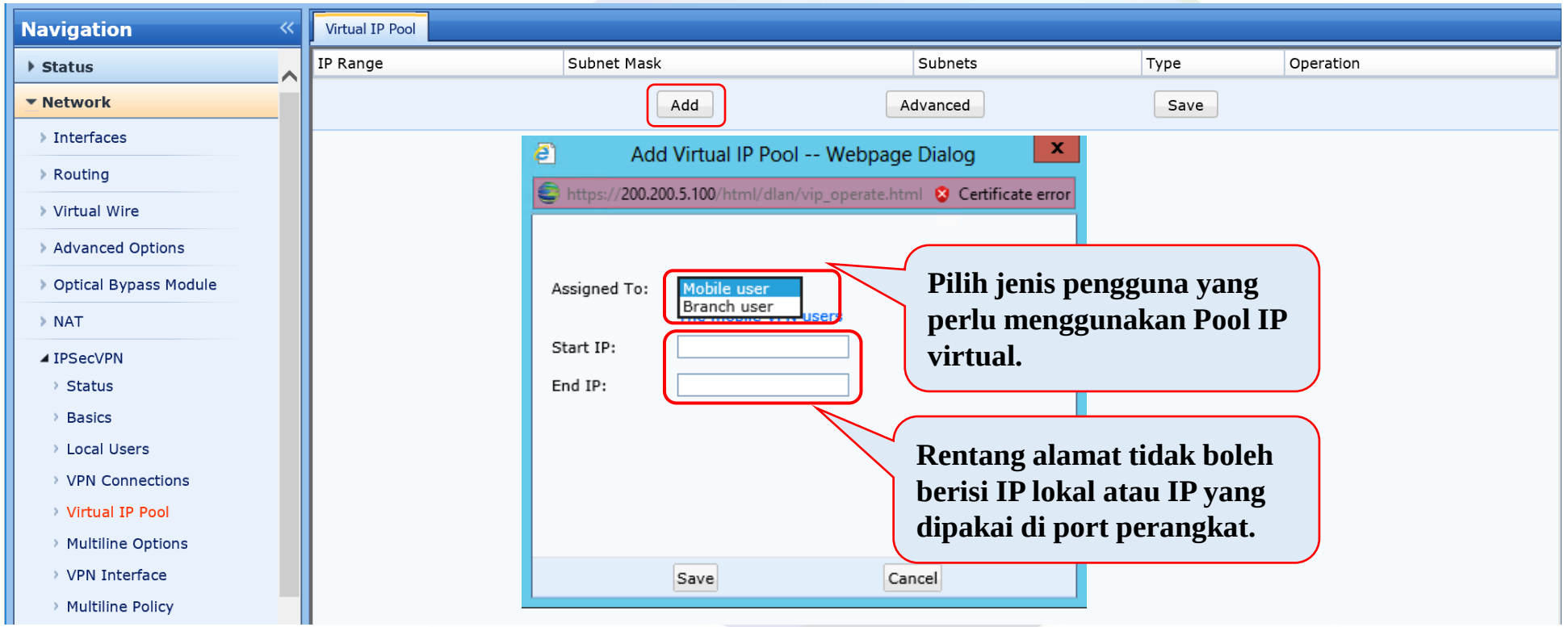
Tambahkan Pengguna:



Sangfor VPN

Pengaturan HQ:

Pool IP Virtual:

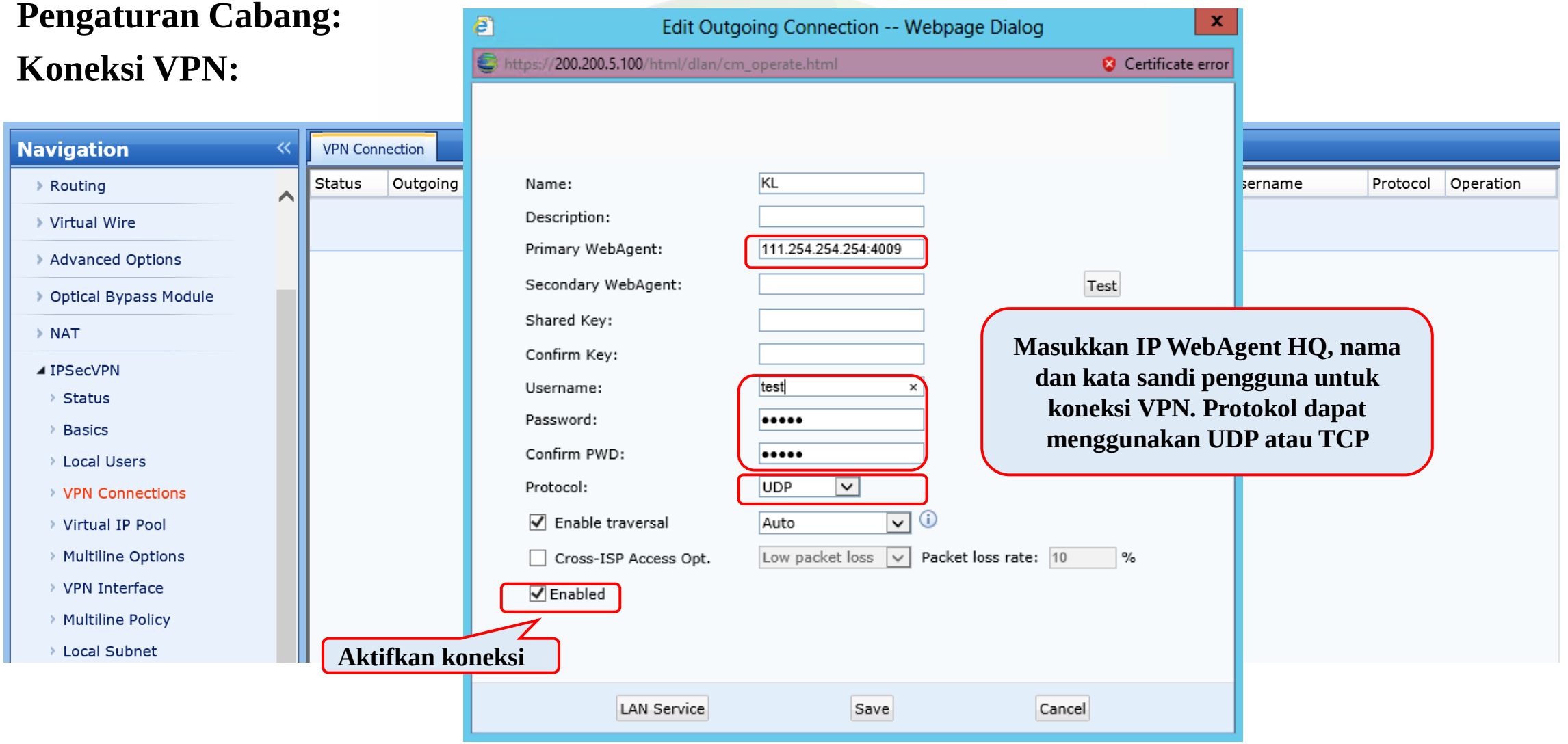


Apabila pengguna VPN mobile ataupun cabang mengaktifkan NAT Tunnel, Anda perlu mengkonfigurasi pool IP virtual, jika tidak maka tidak dapat dikonfigurasi.

Sangfor VPN

Pengaturan Cabang:

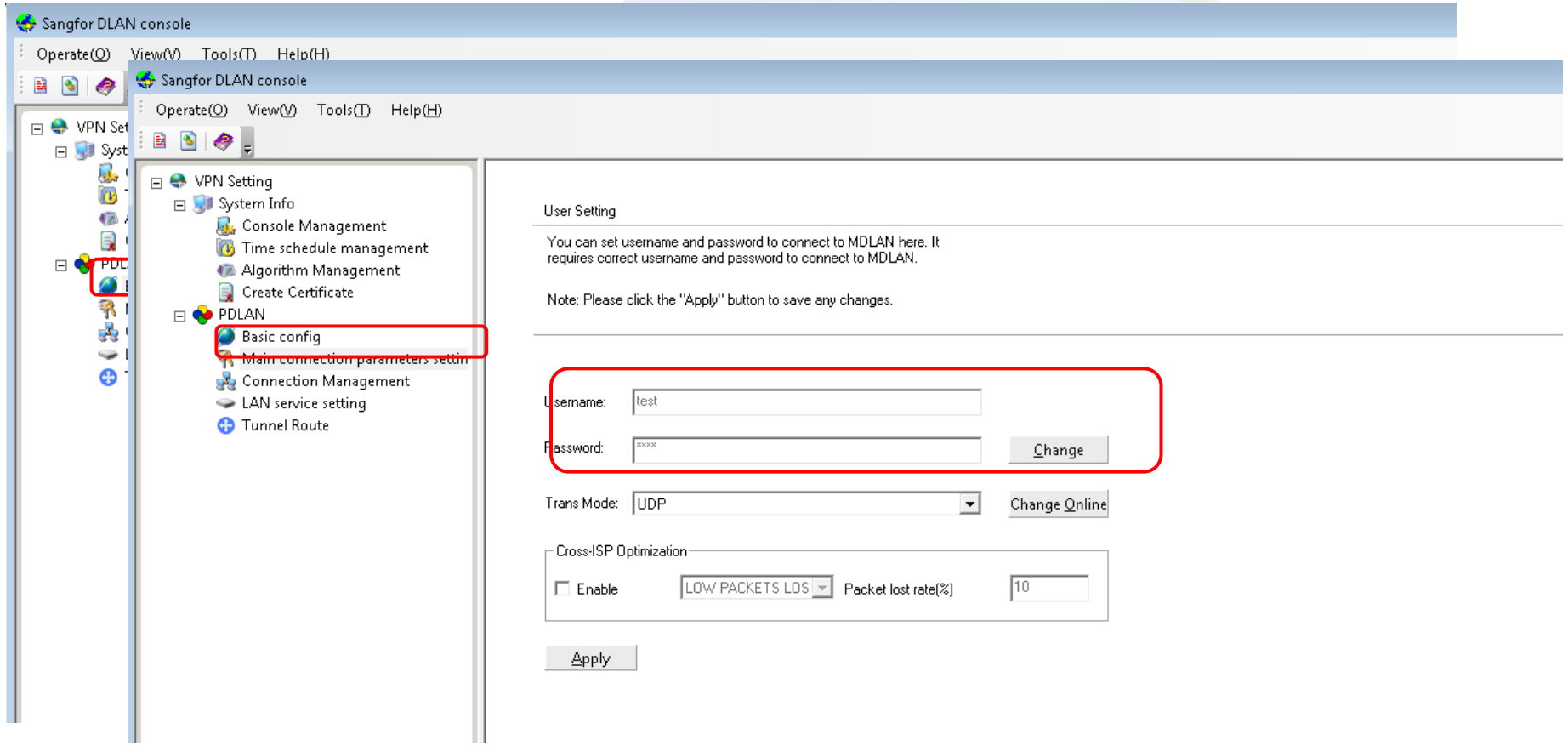
Koneksi VPN:



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;

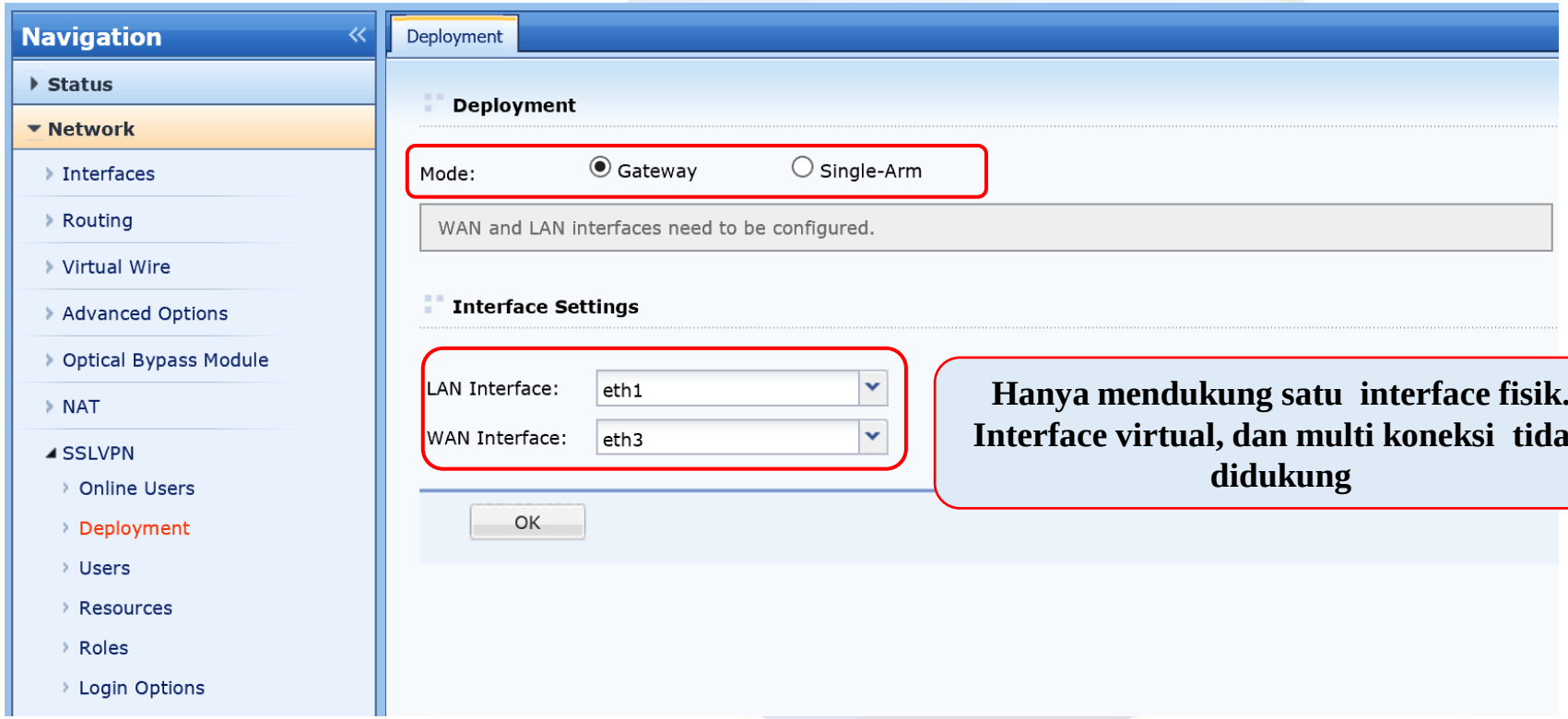
Android 4.0 dan versi yang lebih baru;

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

VPN SSL

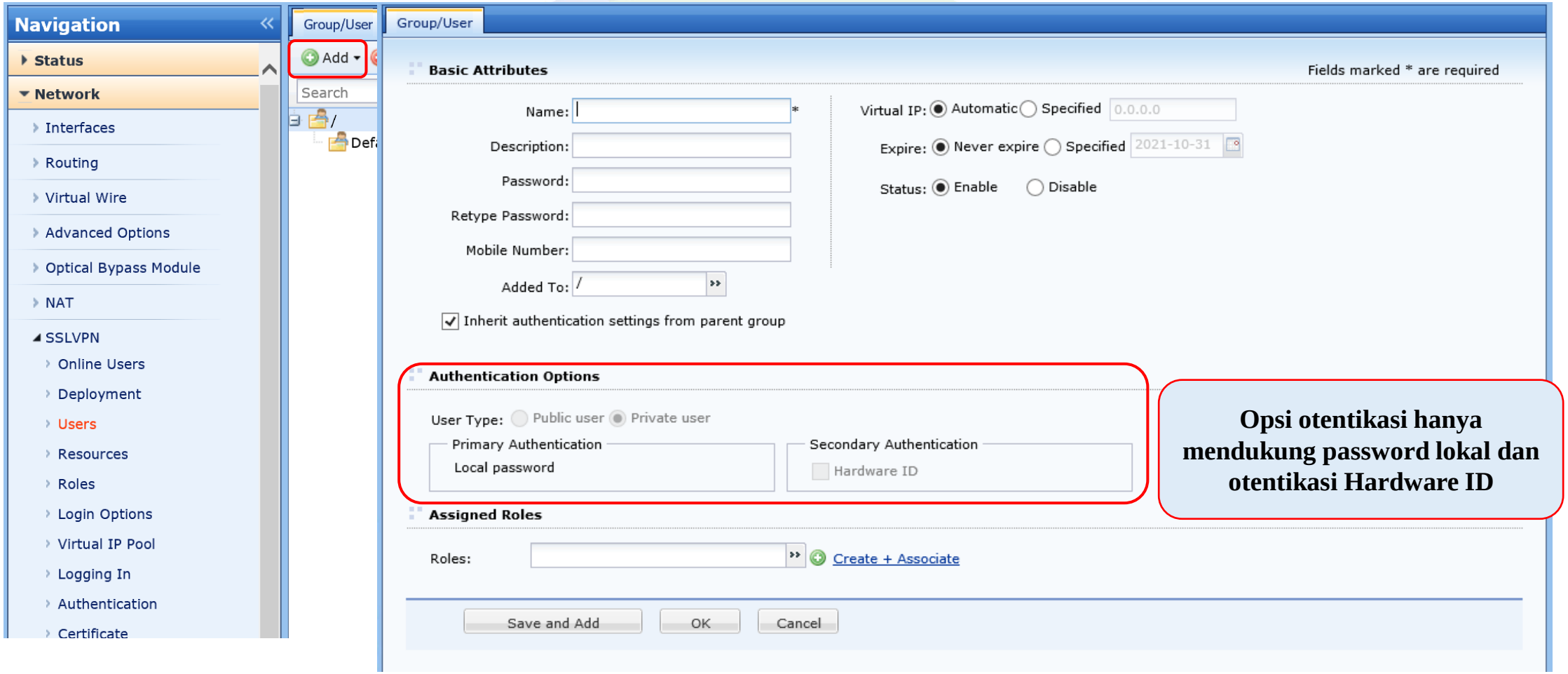
Pengaturan SSL VPN:

Deployment SSL:



VPN SSL

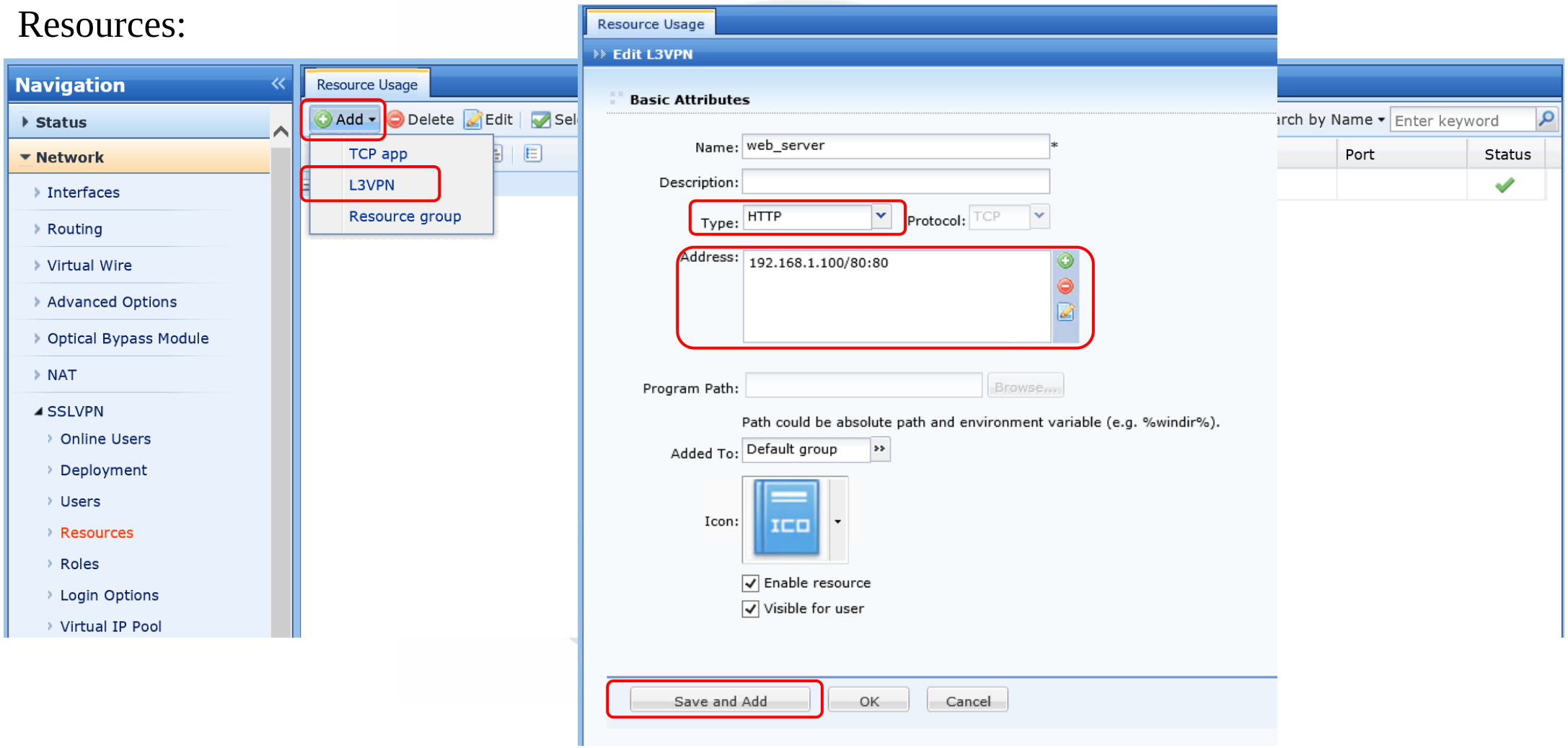
Manajemen pengguna:



Opsi otentikasi hanya mendukung password lokal dan otentikasi Hardware ID

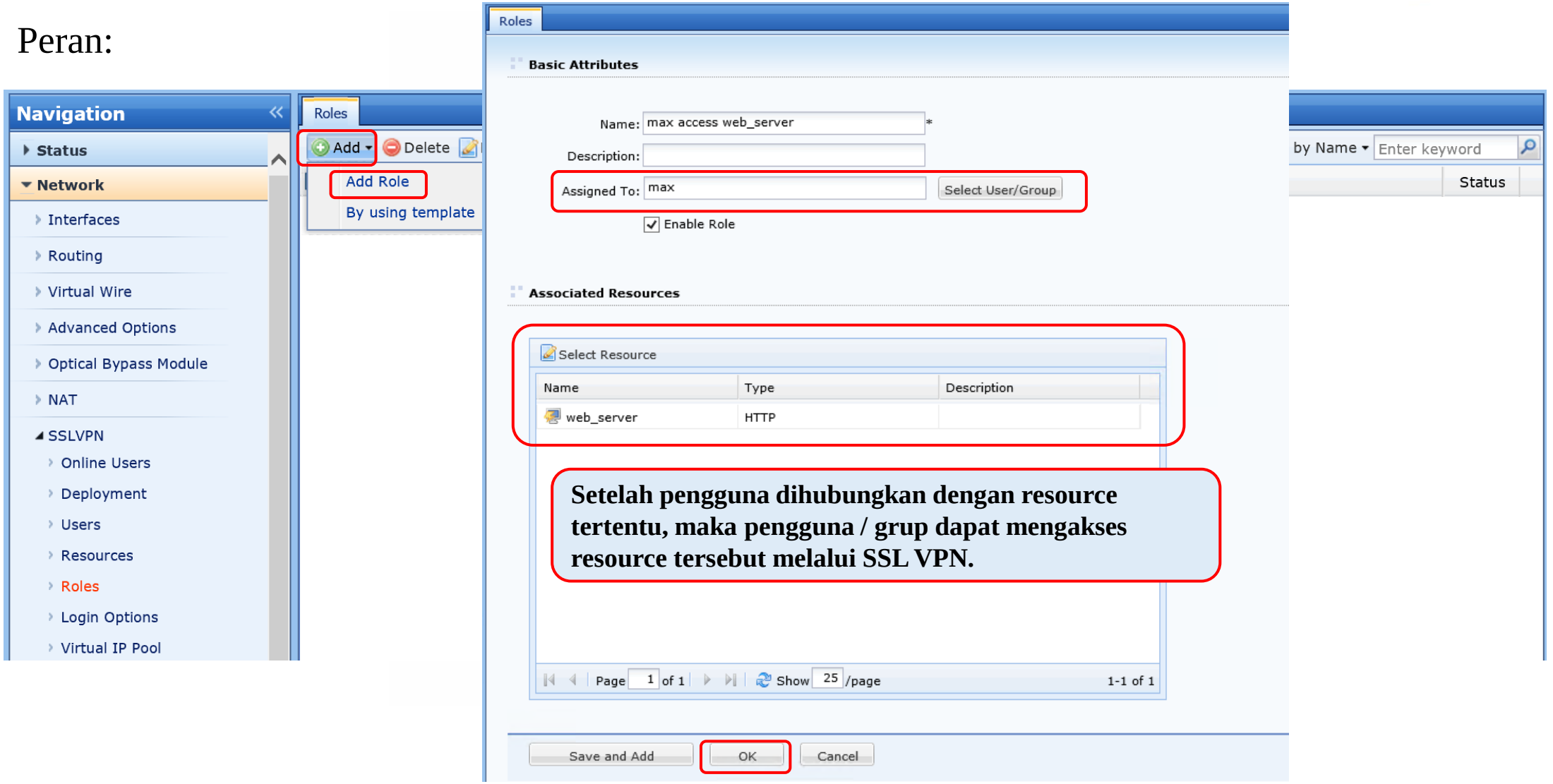
VPN SSL

Resources:



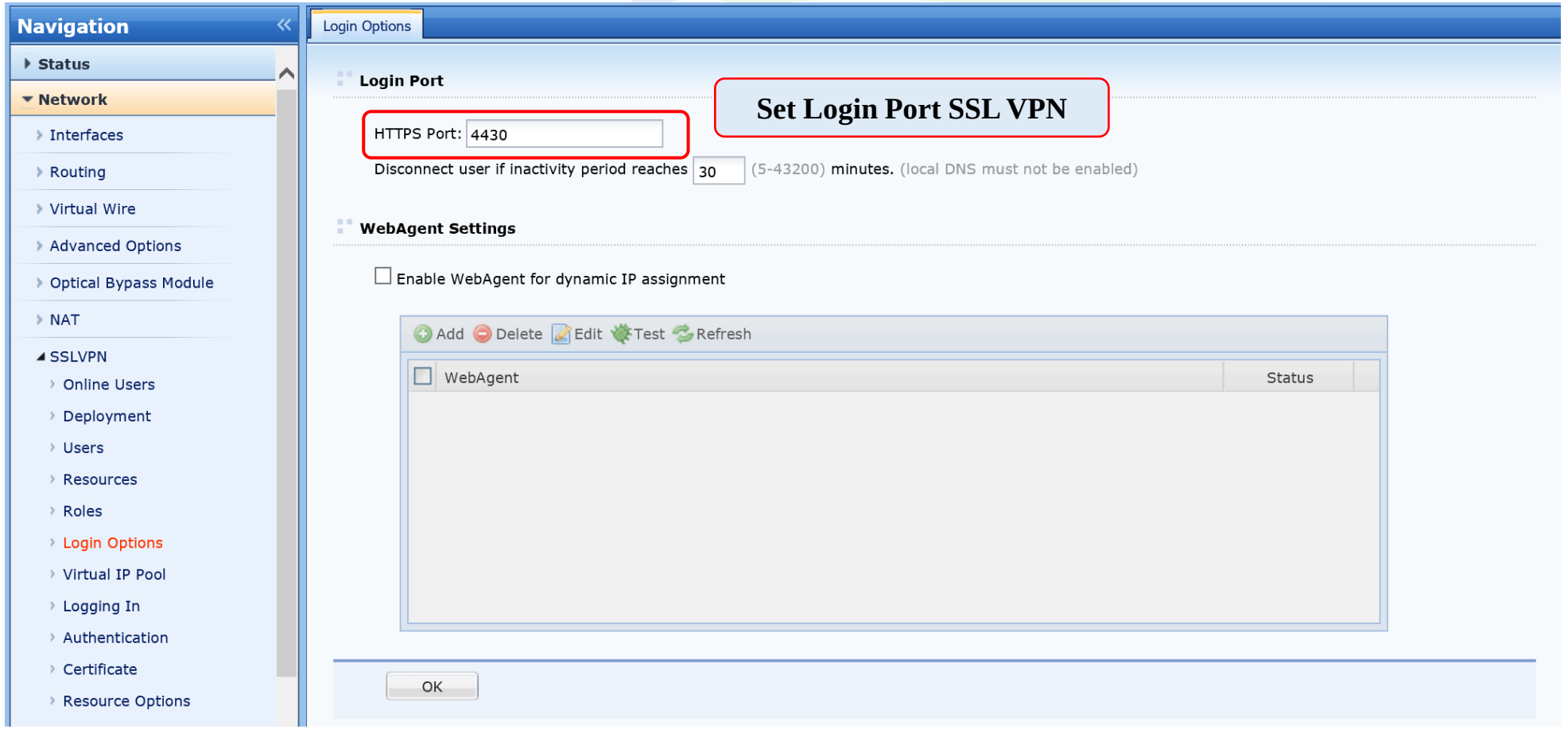
SSL VPN

Peran:



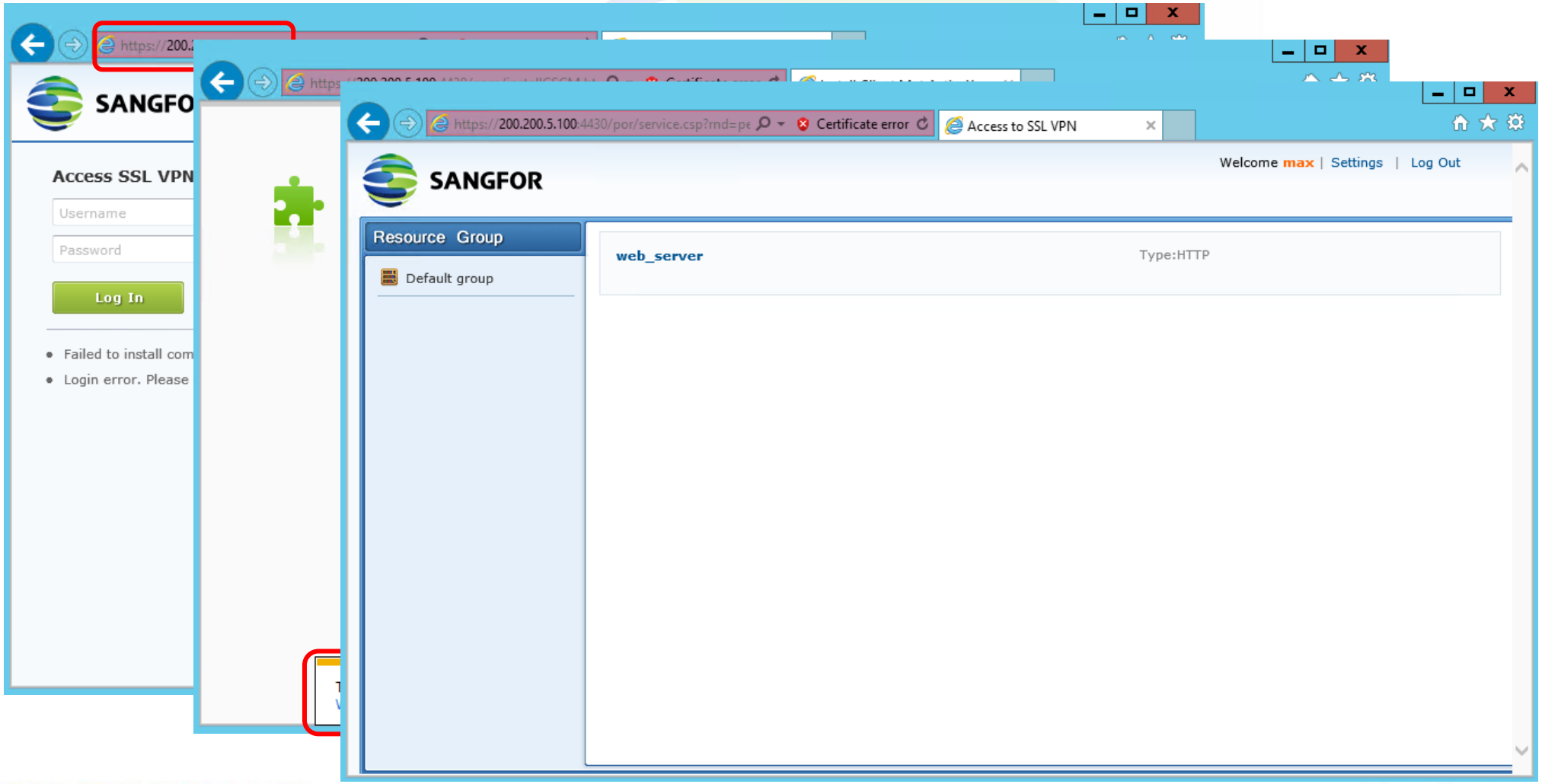
VPN SSL

Opsi Masuk:



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)