SANGFOR

NGAF

Pedoman terbaik untuk Skenario IPsecVPN

Versi 8.0.17

Data Perubahan

Tanggal	Keterangan Perubahan
July 31, 2020	Rilis dokumen Versi 8.0.17
May 17, 2021	Pembaruan dokumen

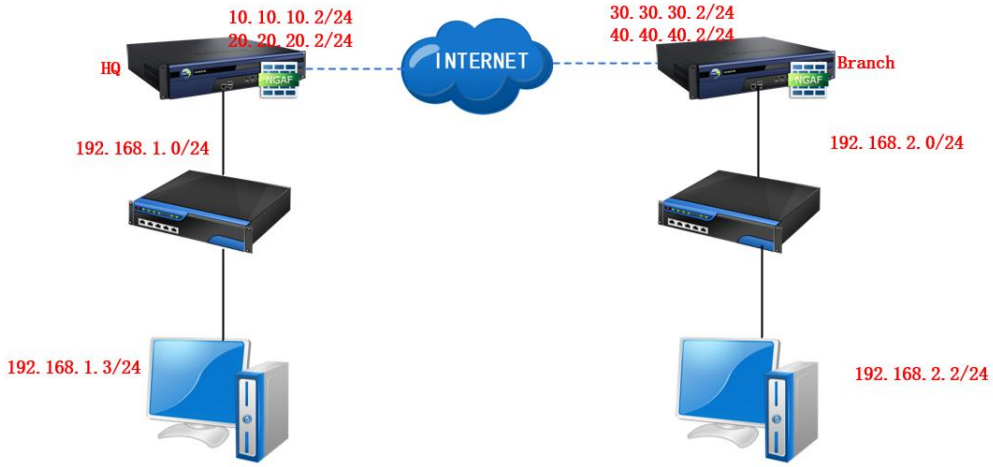
DAFTAR ISI

BAB 1 Skenario

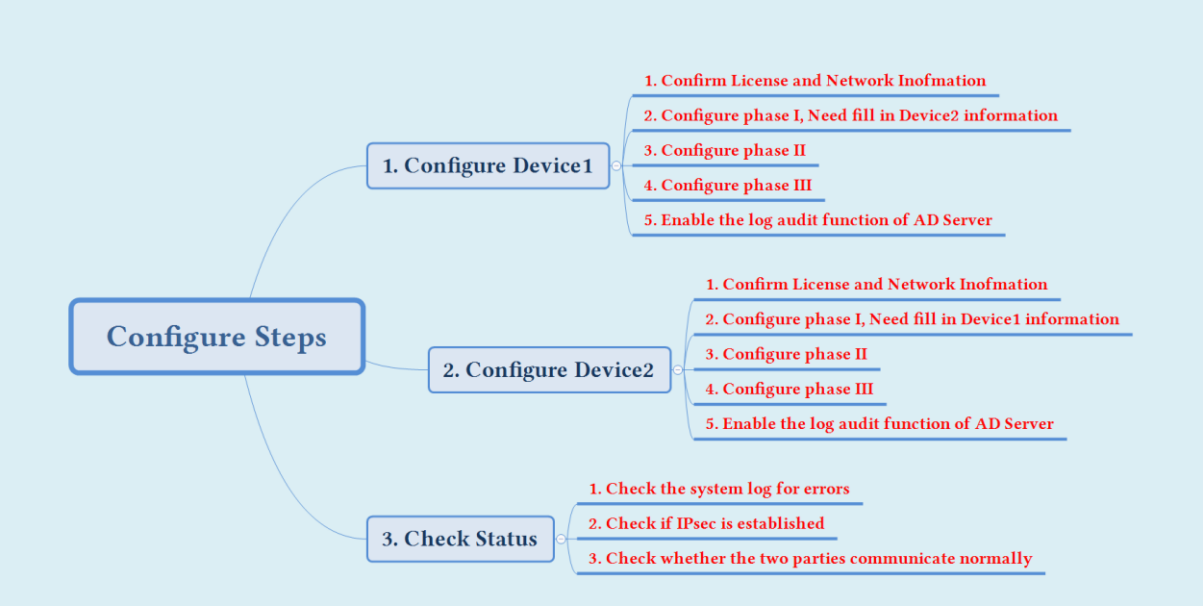
Perusahaan National Postal memiliki banyak cabang dan toko diberbagai propinsi dan kota. Saat ini pelanggan memiliki permintaan untuk melakukan akses layanan web dari cabang dan toko ke kantor pusat, dan ingin memastikan transmisi data aman dan teracak/enkripsi. Pelanggan memiliki sistem bisnis secara terpusat yang berlokasi di kantor pusat, dan sudah lama menghadapi serangan dari hacker dan berbagai masalah keamanan lainnya. Pelanggan sudah bertahun-tahun menggunakan perangkat firewall, tetapi tidak dapat menghadapi serangan dari para hacker. Untuk memenuhi kebutuhan fungsi proteksi keamanan, pelanggan mengambil keputusan untuk mengganti perangkat di kantor pusat saat ini dengan perangkat dari Sangfor. Bagaimanapun pelanggan memiliki cabang yang sangat banyak, oleh sebab itu cabang tidak akan menganti perangkat untuk sementara. Dikarenakan cabang tidak memiliki perangkat dari Sangfor, jadi hanya bisa mengunakan solusi standar IPsecVPN dan tidak bisa menggunakan SangforVPN.

Tentang IPsecVPN: koneksi IPSec VPN hanya dapat digunakan jika kedua tempat memiliki IP Publik yang tetap dan tidak mengunakan NAT. Rekomendasi untuk menggunakan koneksi mode aggresive ketika pasangan mengunakan alamat IP dinamik atau NAT.

Pada lingkungan cabang dan kantor pusat saat ini mengunakan statik IP, jadi pilih untuk gunakan mode utama. Artikel ini akan mengunakan NGAF sebagai contoh untuk kedua tempat antara cabang dan kantor pusat.

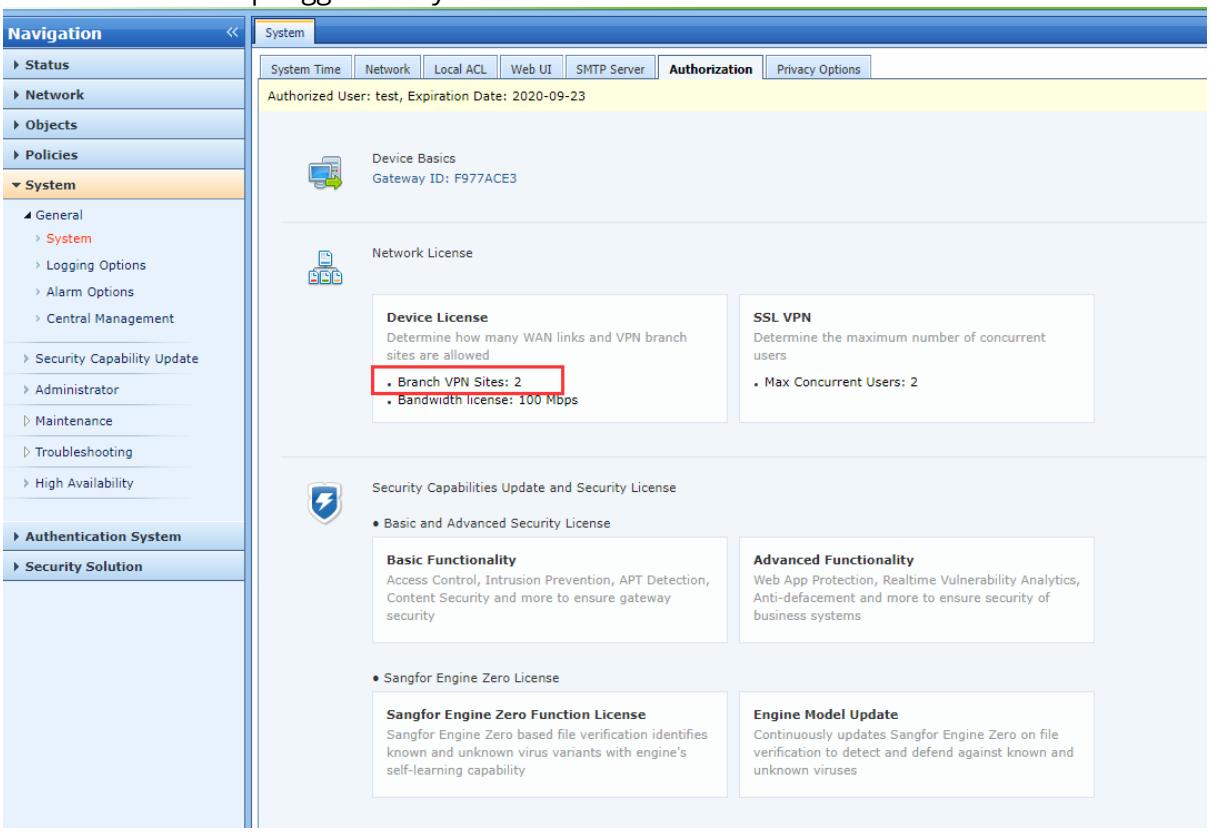


1.1 Langkah Konfigurasi

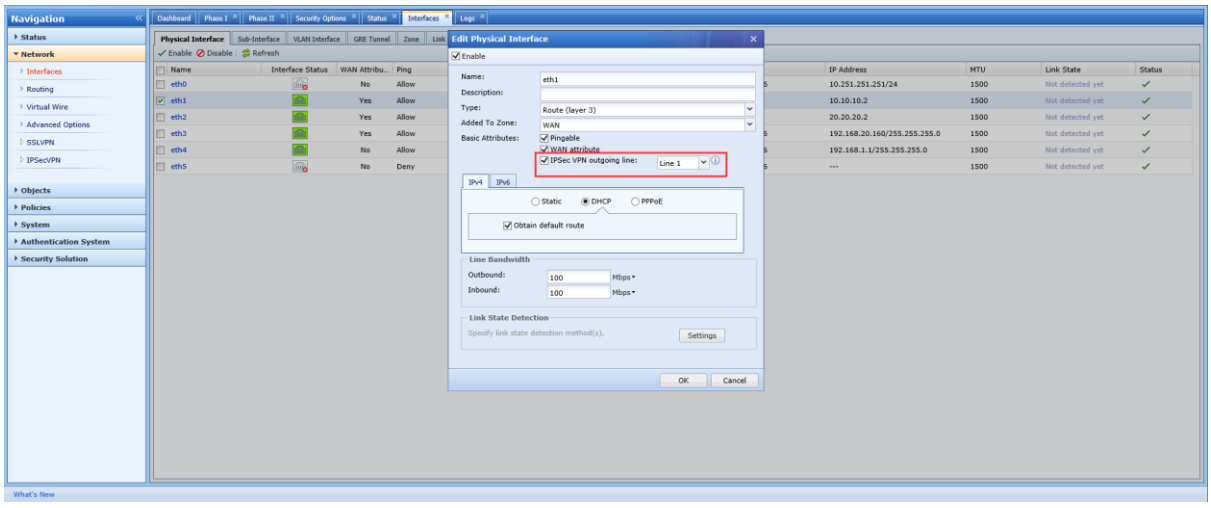


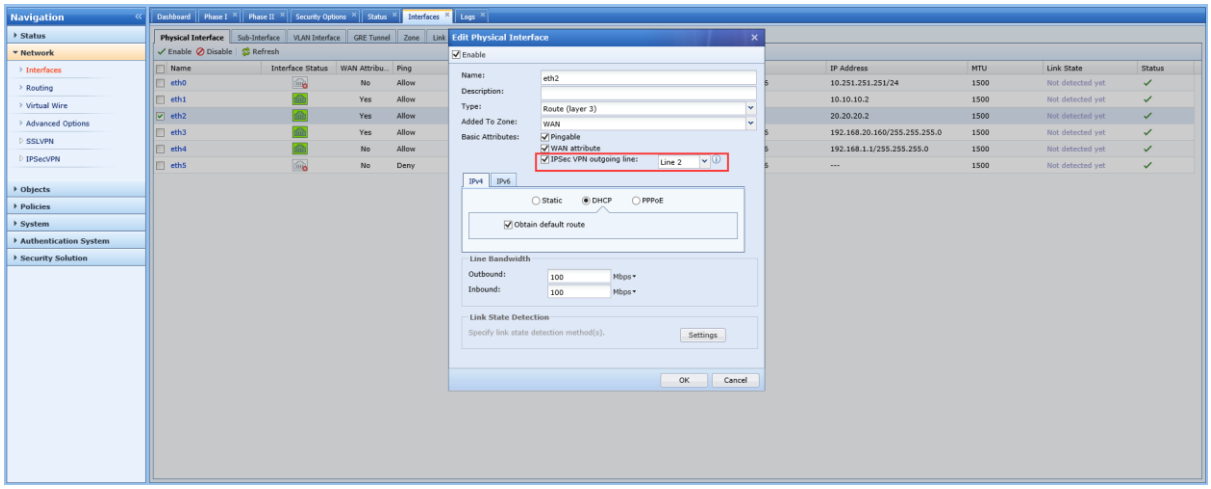
BAB 2 Konfigurasi HQ Perangkat A

1. Periksa apakah lisensi IPSec telah aktif pada perangkat. Otorisasi IPSec memerlukan lisensi IPSec untuk penggunaannya.

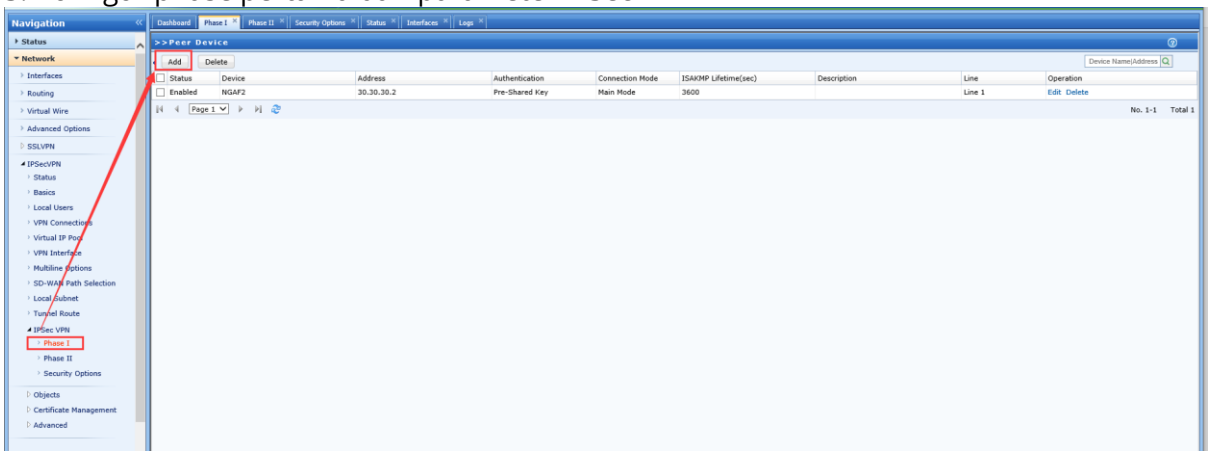


2. Pilih port WAN untuk digunakan sebagai antarmuka jalur keluar dari IPSecVPN dan jadikan sebagai jalur yang dipilih.

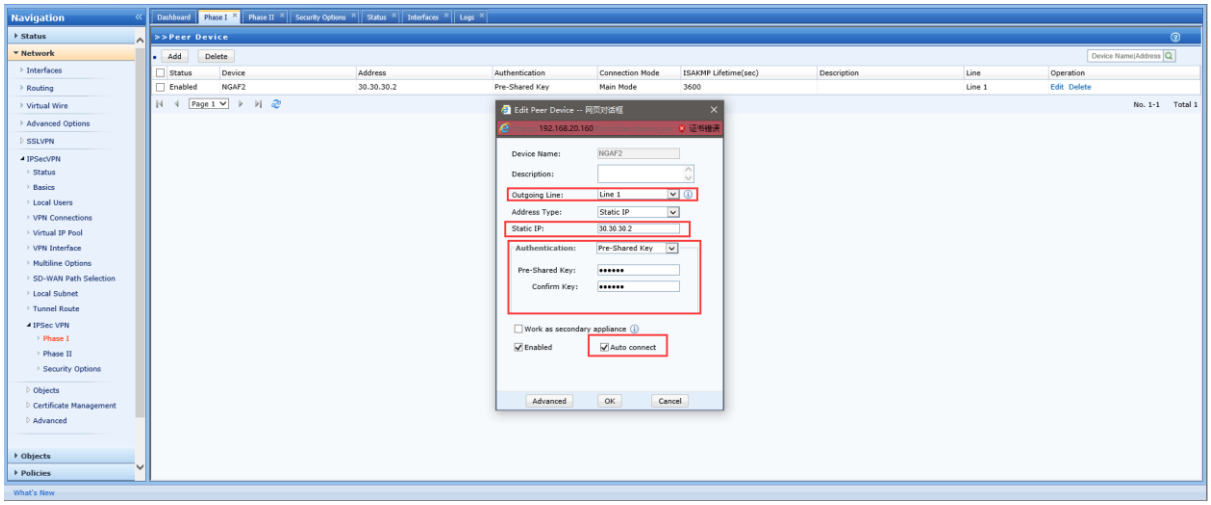




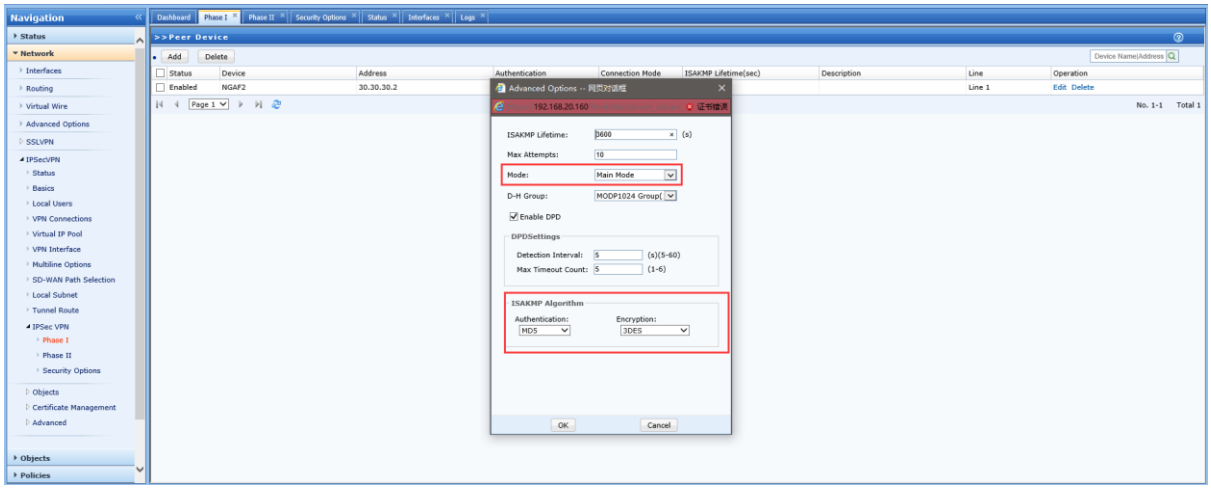
3. Konfigur phase pertama dari parameter IPSec



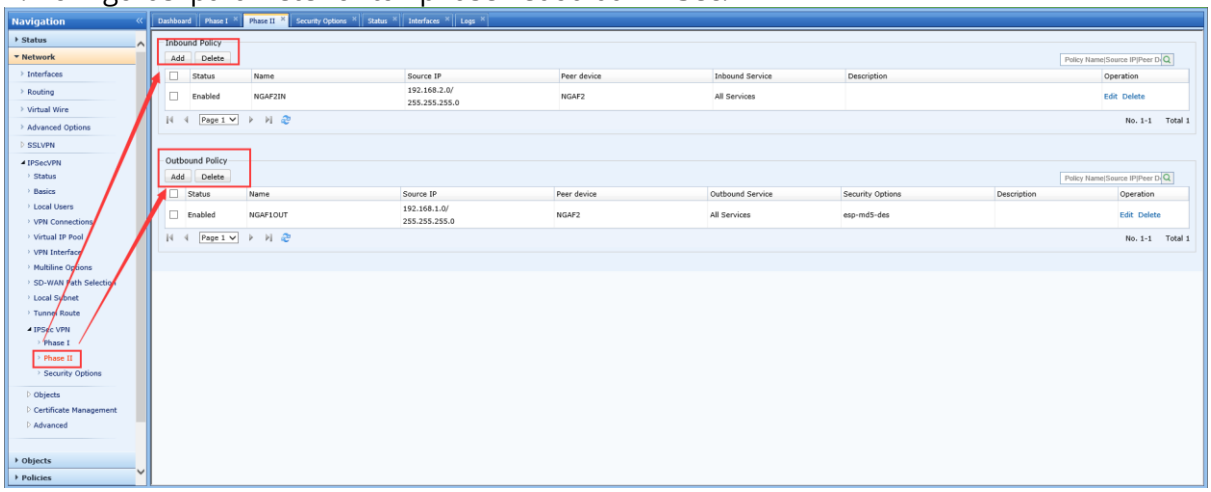
Perlu di pilih jalur keluar, contoh, line 1 sebagai jalur utama, maka pilih line 1 sebagai jalur tetap untuk IPSecVPN. Masukan IP dari perangkat cabang dan “shared key”; nama dari perangkat pasangan/peer, contohnya untuk nama pasangannya adalah NGAF2.



Klik “Advanced”, pilih mode utama, dan konfirmasi algoritma authentikasi dan algoritma pengacakan/enkripsi. Ketika konfigurasi pada perangkat lainnya diperlukan untuk memiliki algoritma yang sama pada perangkat pasangannya.

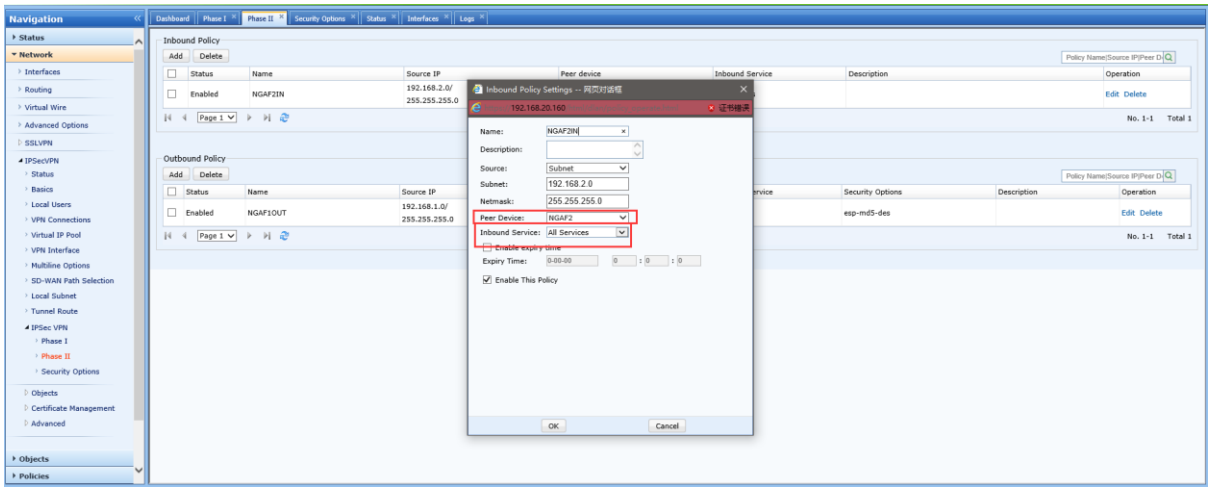


4. Konfigurasi parameter untuk phase kedua dari IPSec.

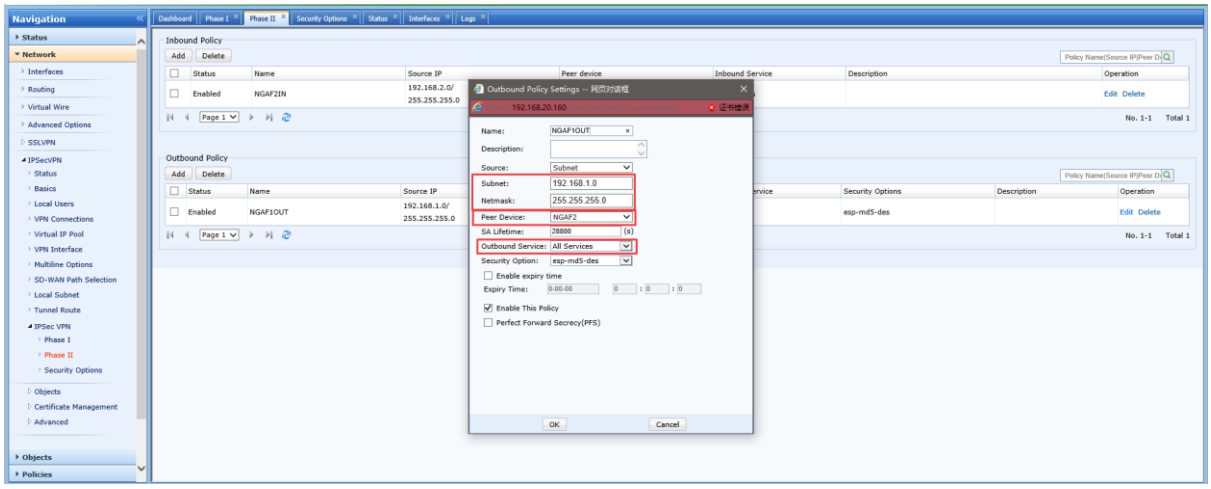


Policy Inbound di isi dengan segmentasi jaringan dari cabang, dimana segmentasi jaringan dari paket data cabang yang perlu di kirimkan ke tunnel VPN pada perangkat sehingga perangkat saat ini dapat dibuat route untuk return paket, dan pilih perangkat NGAF2 yang telah kita beri nama pada langkah pertama. Inbound Service biasanya perlu dipilih “All Services”, dan opsi adalah “All TCP Services”. Jika opsi ini digunakan , pengujian mengunakan

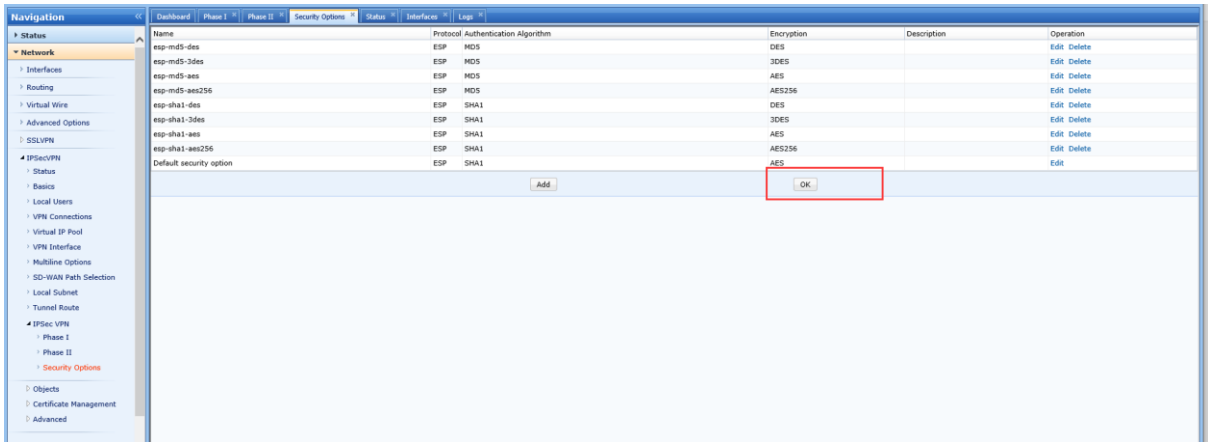
ping akan gagal dikarenakan hanya layanan TCP yang diperbolehkan untuk melewati tunnel VPN.



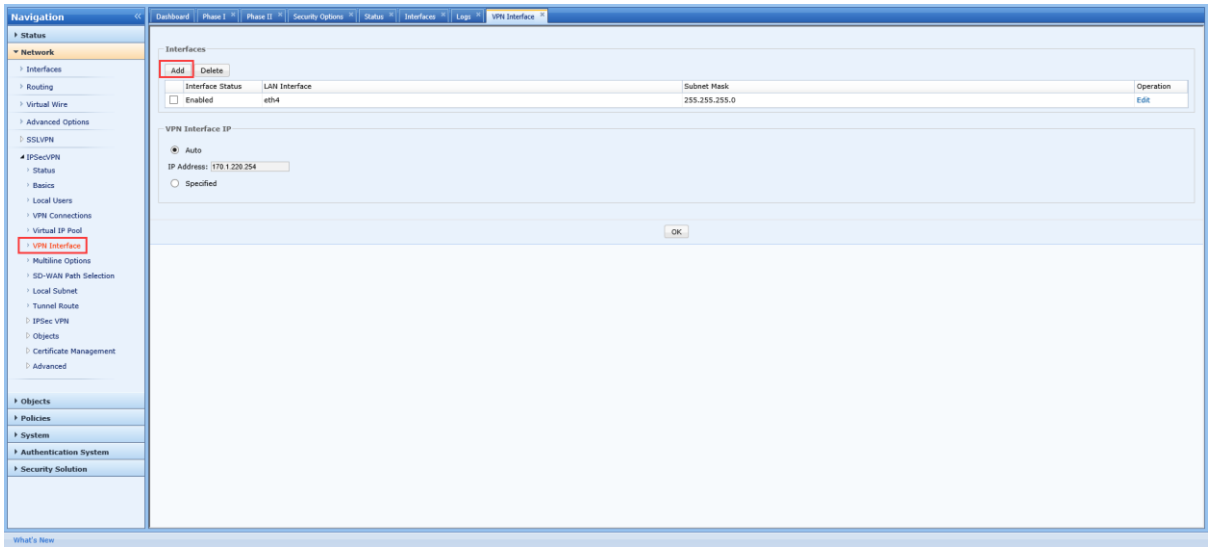
Outbound Policy berarti memperkenalkan segmen jaringan internal dari perangkat saat ini jadi perangkat pasangan dapat membuat route untuk return paket. Outbound Service biasanya perlu untuk memilih “All Service”, dan opsi umum “All TCP Services”. Jika opsi umum ini digunakan, ping akan gagal karena trafik UDP tidak boleh melewati tunnel VPN.



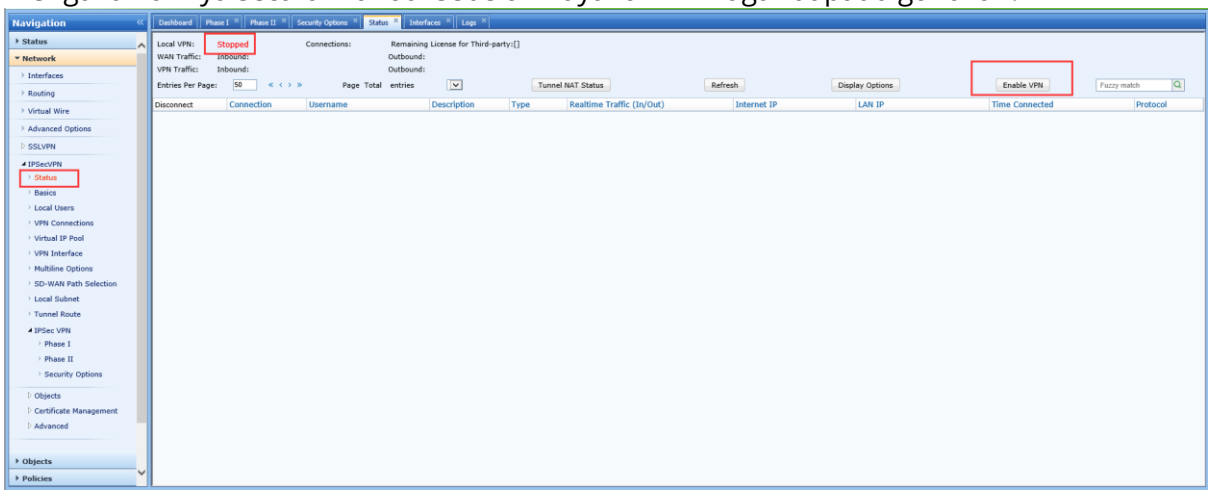
5. Langkah ke tiga untuk IPSec. Langkah ketiga biasanya adalah algoritma dari pengacakan/enkripsi umumnya tidak perlu dilakukan perubahan cukup lakukan klik tombol OK.



6. Konfigurasi antarmukan jaringan internal dan segmen jaringan.

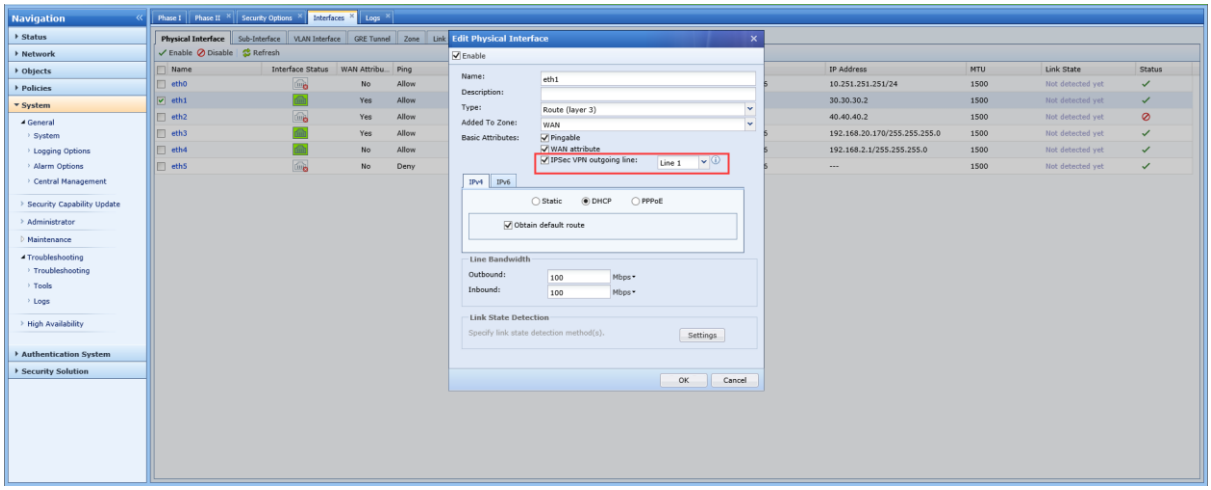


7. Aktifkan layanan VPN. Layanan VPN pada umumnya tidak aktif. Anda perlu mengaktifkannya secara manual sebelum layanan VPN agar dapat digunakan.

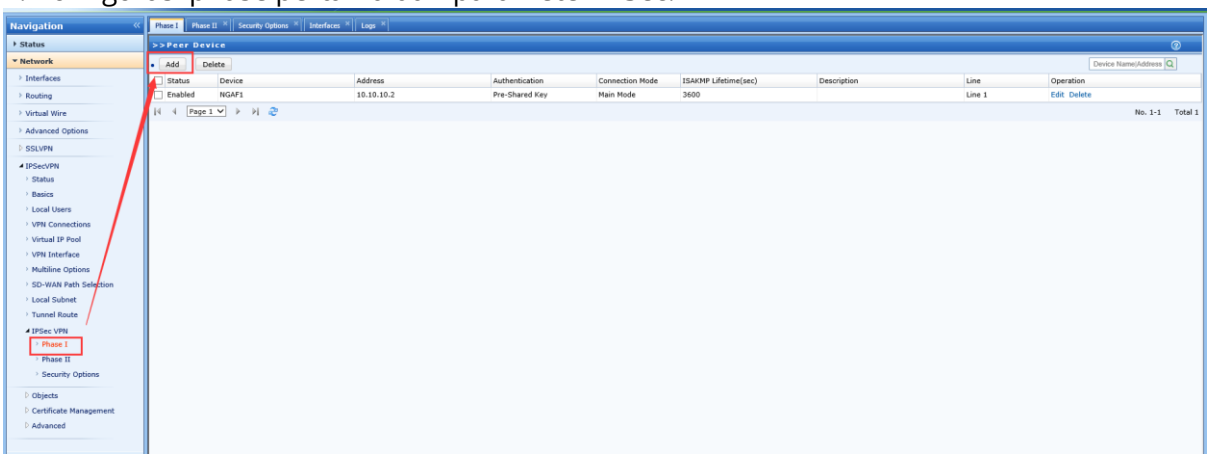


BAB 3 Konfigurasi Cabang Perangkat B

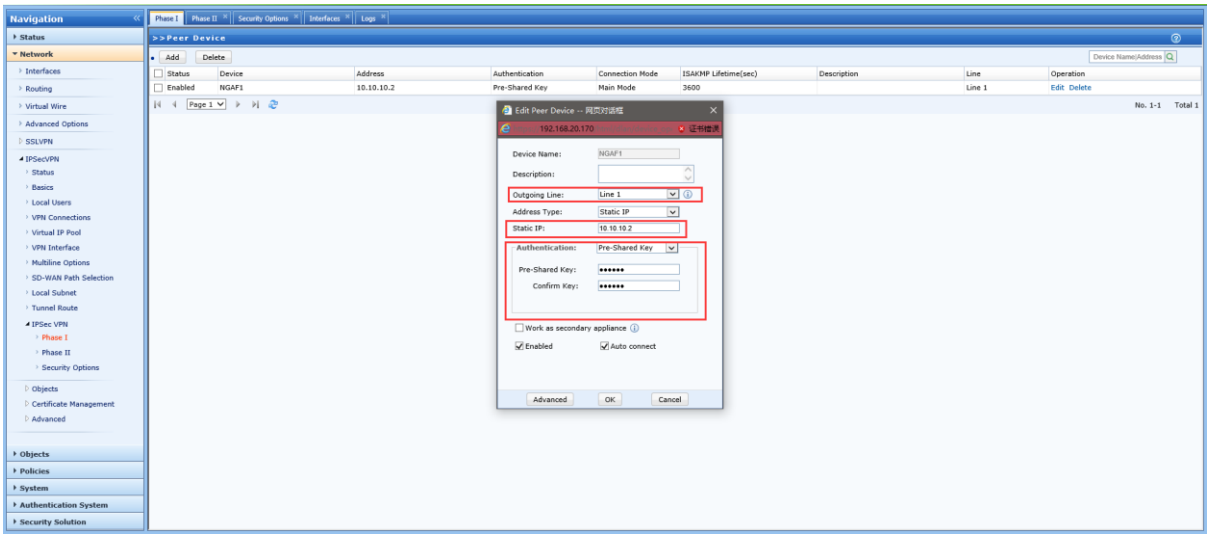
1. Pilih port WAN untuk digunakan sebagai antarmuka jalur keluar dari IPSecVPN dan jadikan sebagai jalur yang dipilih



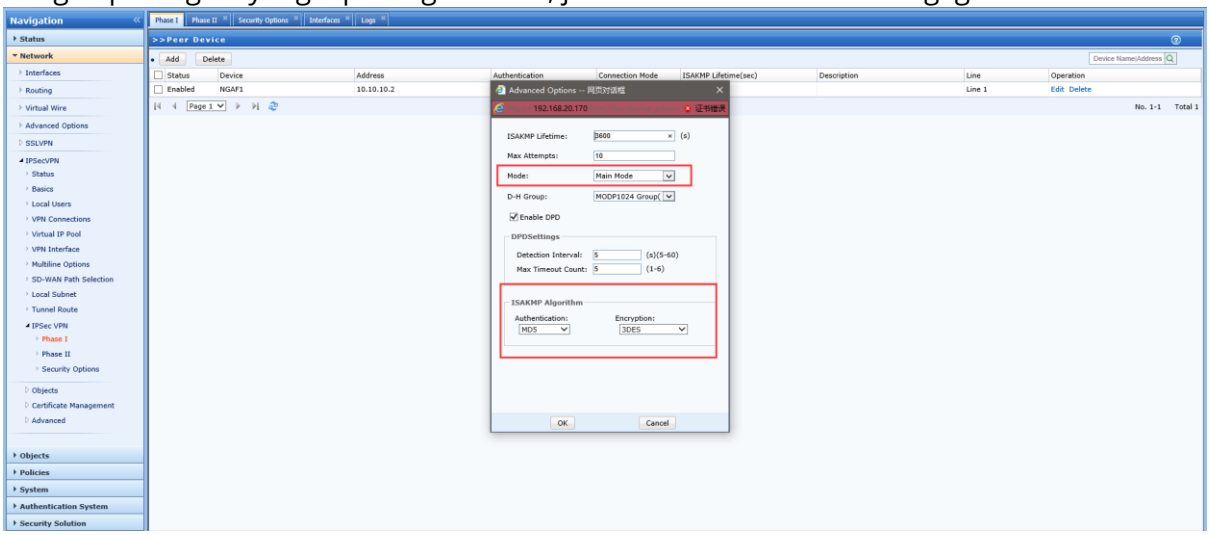
2. Konfigurasi phase pertama dari parameter IPSec.



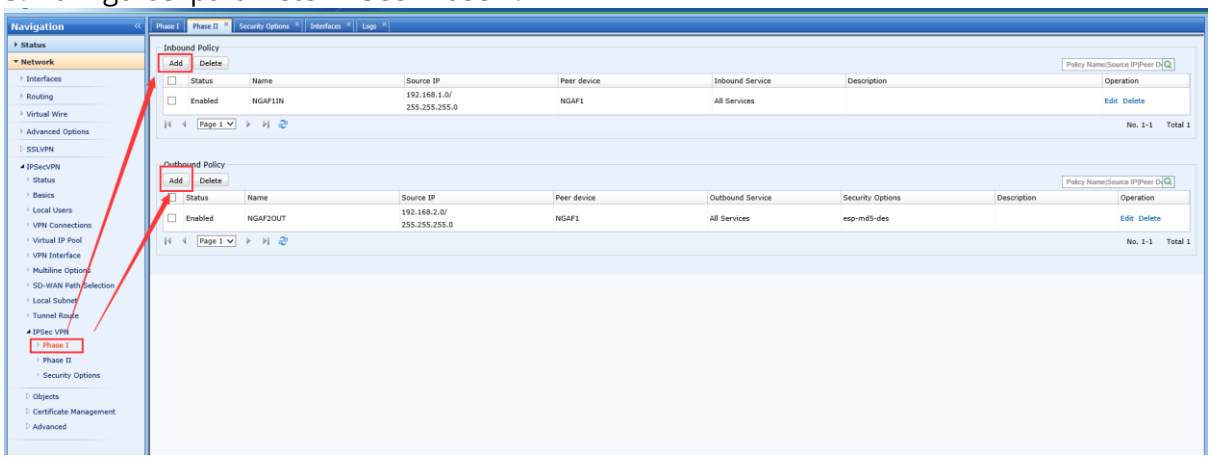
Konfigurasi parameter termasuk IP dan shared key dari kantor pusat. Shared key harus sama dengan shared key yang telah dikonfigurasi pada perangkat di Pusat. Perlu diperhatikan untuk mengaktifkan dengan memilih “Auto connect”. Setidaknya salah satu dari perangkat tersebut harus diaktifkan “Auto connect”. Jika kedua perangkat tidak ada yang menggunakan “Auto connect”, koneksi VPN tidak akan terjadi.



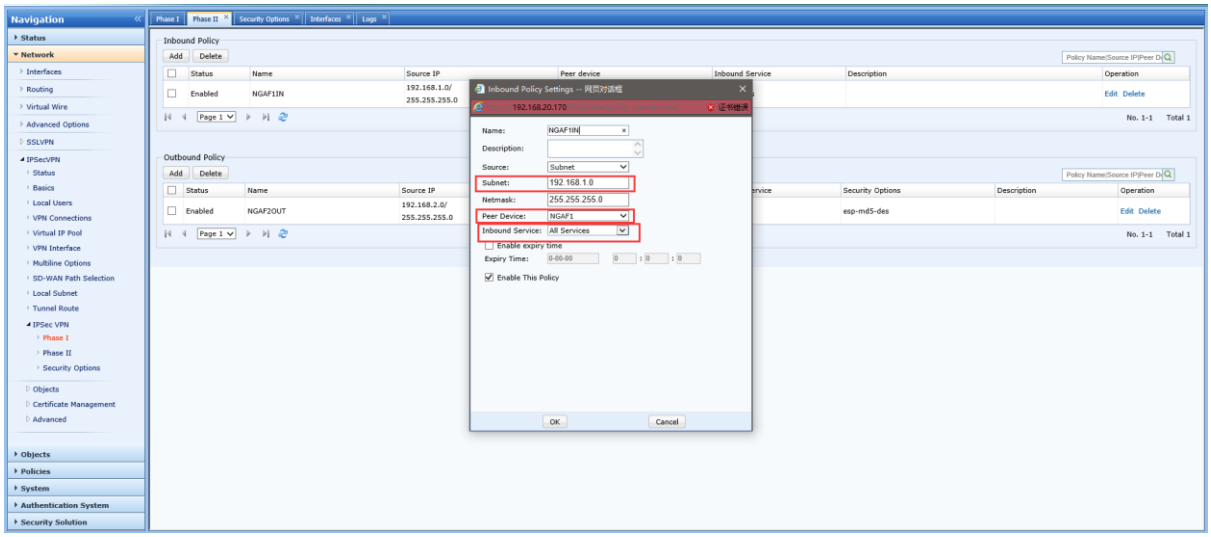
Mode algoritma authentikasi, dan algoritma pengacakan dari perangkat cabang harus sama dengan perangkat yang dipasang di Pusat, jika tidak authentikasi akan gagal.



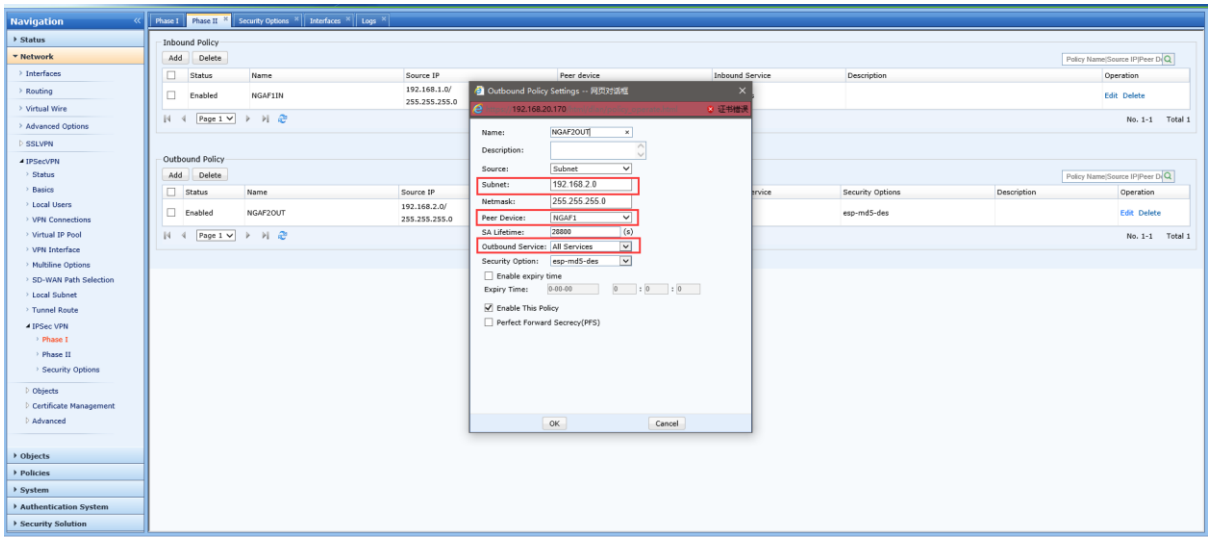
3. Konfigurasi parameter IPSec Phase 2.



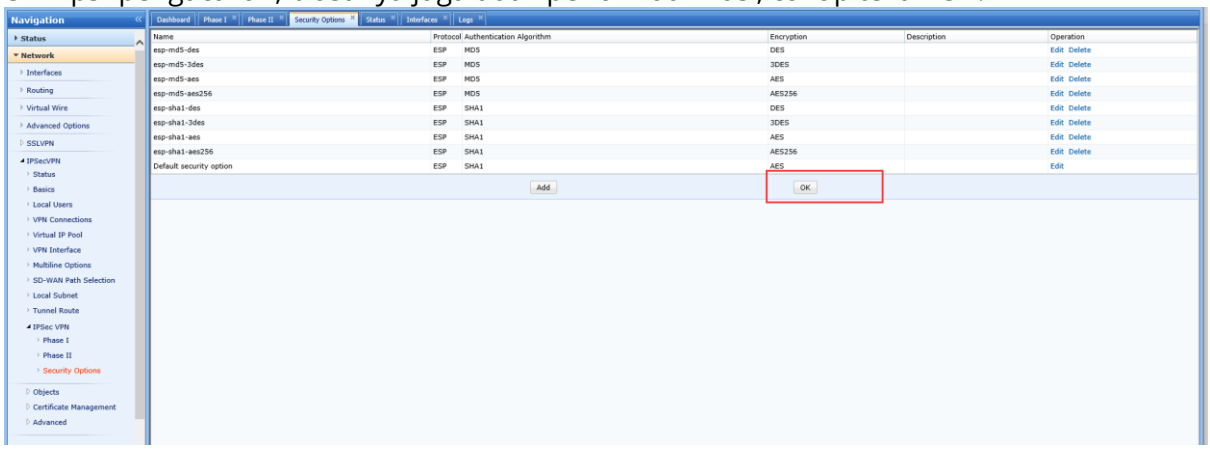
Pada Inbound Policy masukan segmen jaringan intranet dari cabang, yang artinya perangkat ini akan membandingkan segmen jaringan mana dari paket data cabang yang akan dibawa melalui tunnel VPN sehingga perangkat dapat menetapkan route untuk mengembalikan paket data saat ini, dan pada Peer device pilih NGAF1 yang telah kita buat pada tahap pertama. Inbound Service perlu kita ubah isinya menjadi “All Services”, dan opsi ini perlu dirubah karena secara default berisi “All TCP Services”. Jika opsi default ini kita gunakan, maka pengujian dengan mengunakan ping akan gagal karena hanya layanan TCP saja yang diperbolehkan untuk melalui tunnel VPN ini.



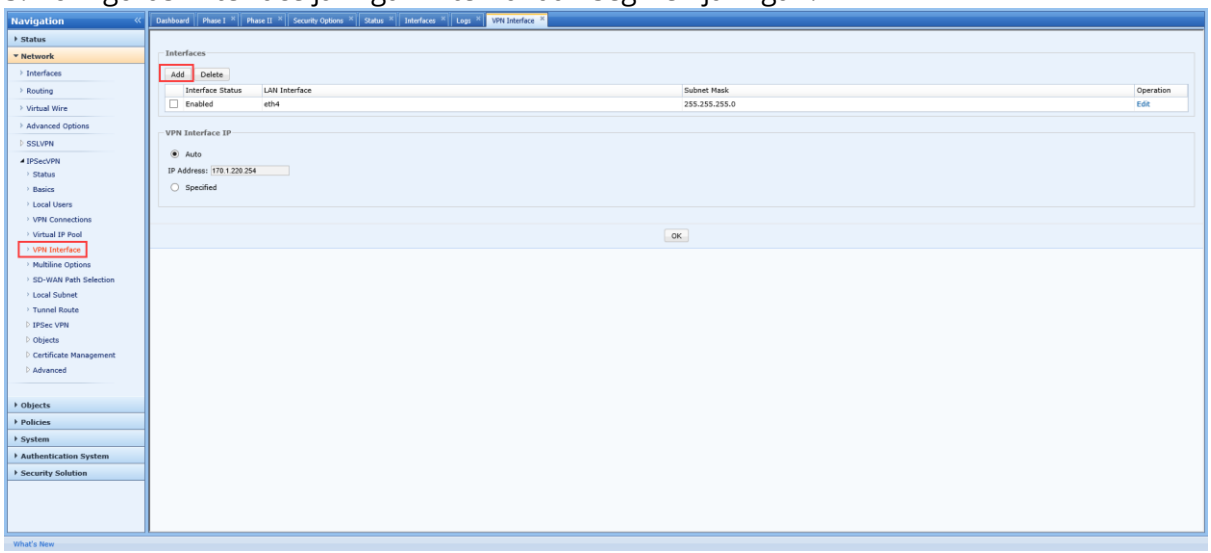
Outbound Policy berarti memperkenalkan segmen jaringan internal pada perangkat sehingga perangkat pasangannya dapat menetapkan route untuk pengembalian paket. Outbound Policy perlu kita ubah menjadi “All Services”, dan opsi ini dirubah karena secara default berisi “All TCP Services”. Jika opsi default ini kita gunakan, maka pengujia n dengan mengunakan ping akan gagal kerna hanya layanan TCP saja yang diperbolehkan untuk melalui tunnel VPN ini.



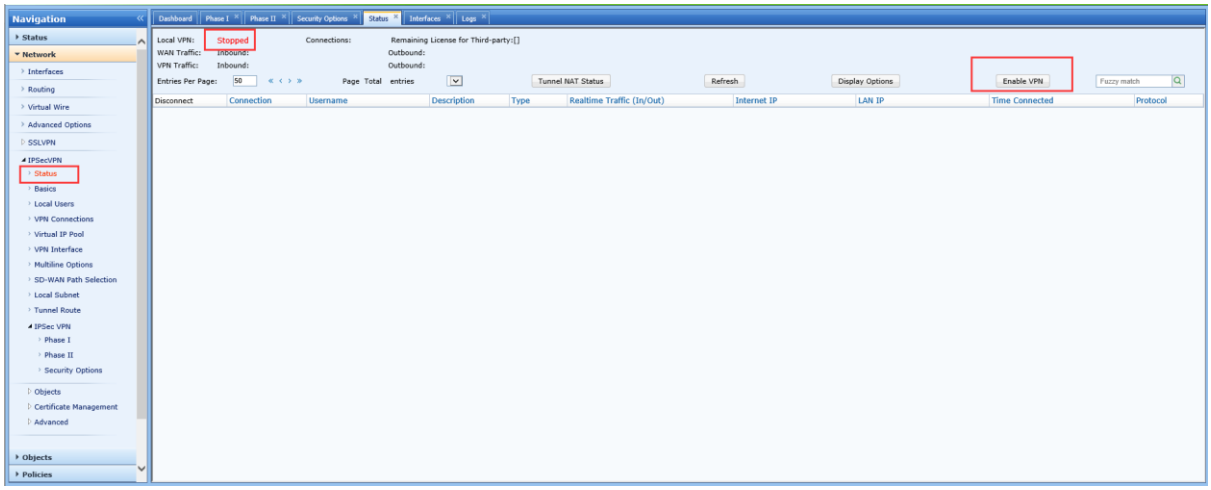
4. Langkah ke tiga dari konfigurasi IPSec. Langkah ke tiga biasanya adalah algoritma enkripsi/pengacakan, biasanya juga tidak perlu modifikasi, cukup tekan OK.



5. Konfigurasi interface jaringan internal dan segmen jaringan.

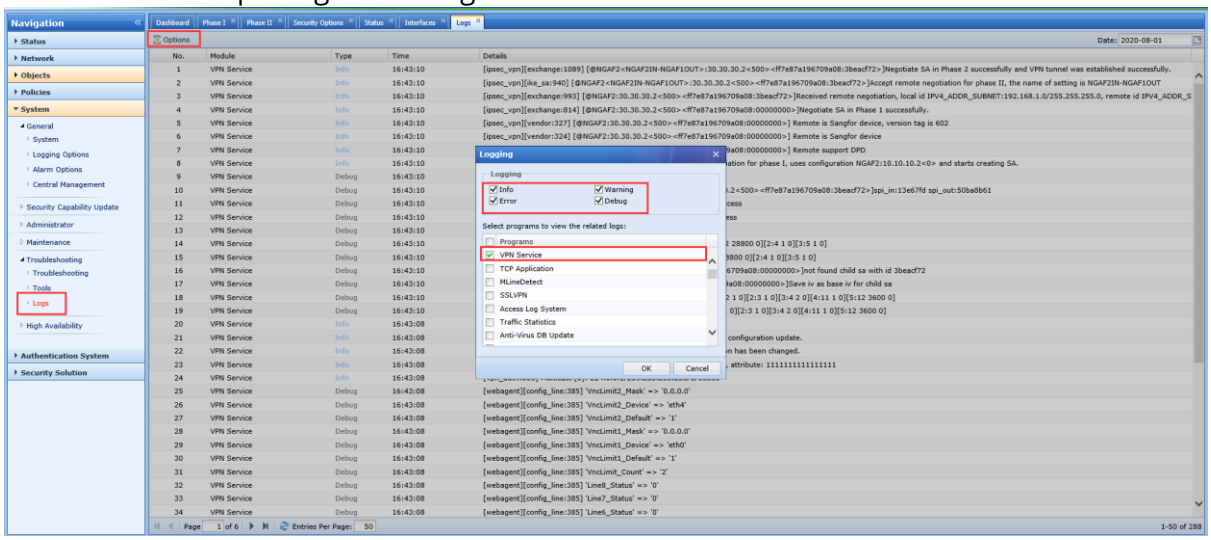


6. Aktifkan layanan VPN. Pada layanan VPN secara default adalah non-aktif. Anda perlu secara manual untuk mengaktifkan layanan VPN agar layanan dapat berjalan normal.



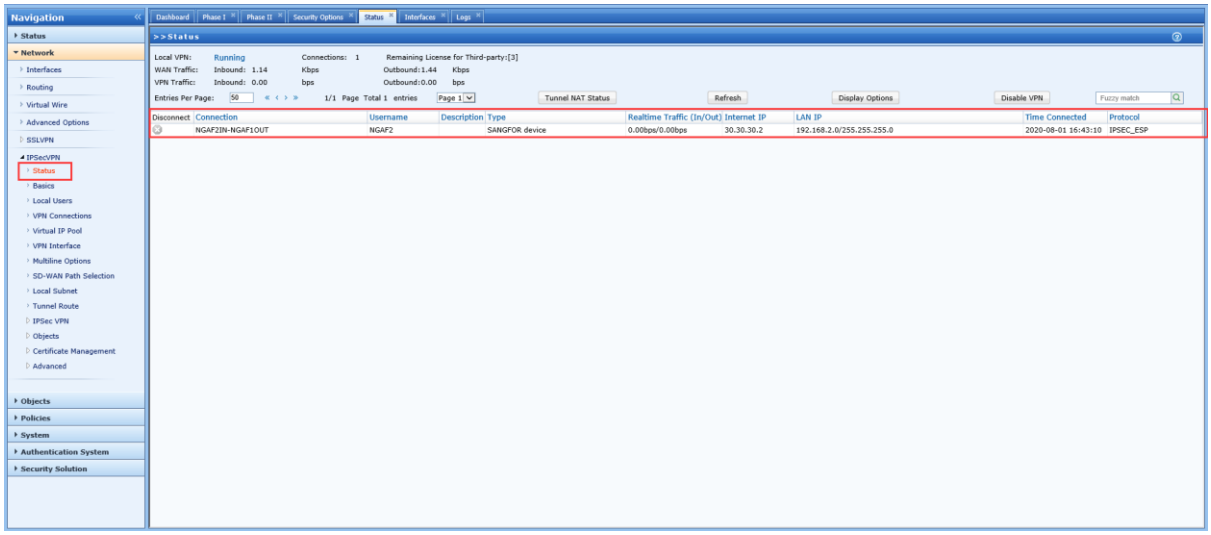
BAB 4 Mengetahui Status IPsecVPN

1. Mengetahui pencatatan sistem yang berhubungan dengan layanan VPN pada perangkat Kantor Pusat dan perangkat Cabang.

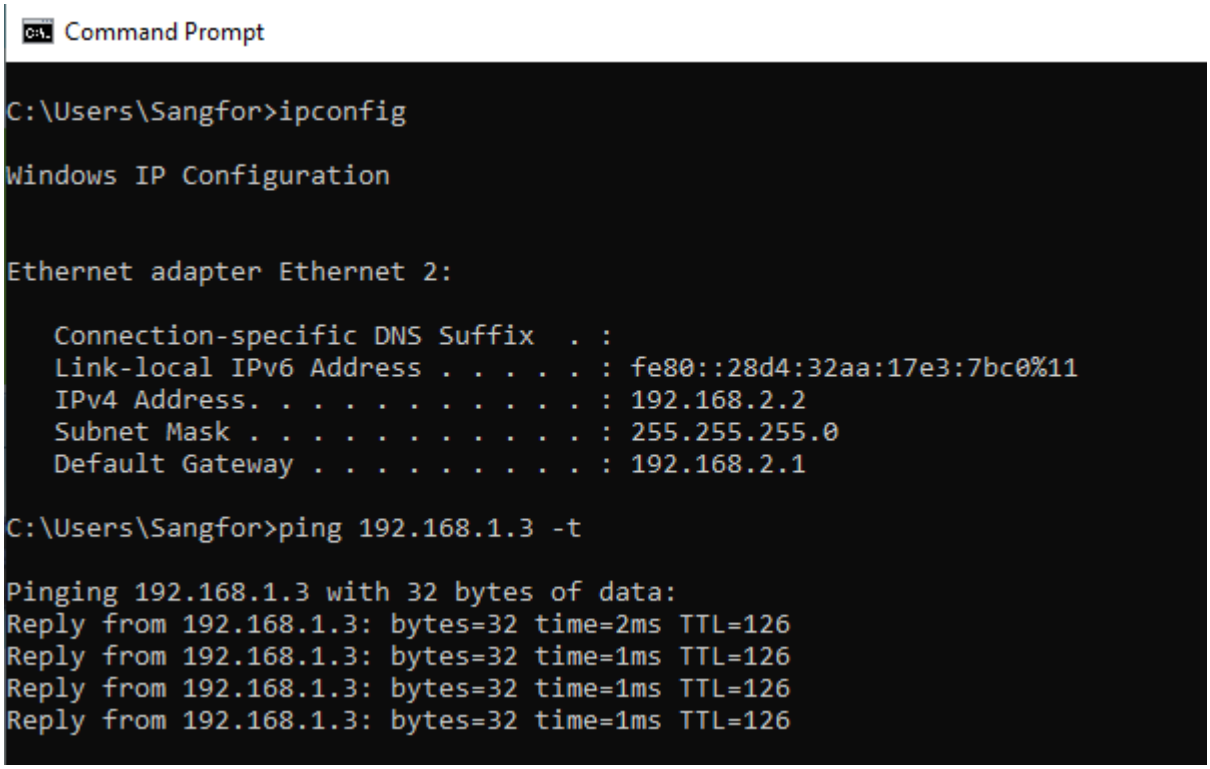


perhatikan apakah ada catatan peringatan dan kesalahan. Jika ada pencatatan kesalahan, anda perlu merubah konfigurasi sehubungan dengan pencatatan kesalahan tersebut.

2. Ketahui status dari layanan dari VPN. Jika informasi sehubungan dengan tunnel dapat tersaring, berarti VPN telah berhasil terjalin antara Kantor Pusat dengan Kantor Cabang.

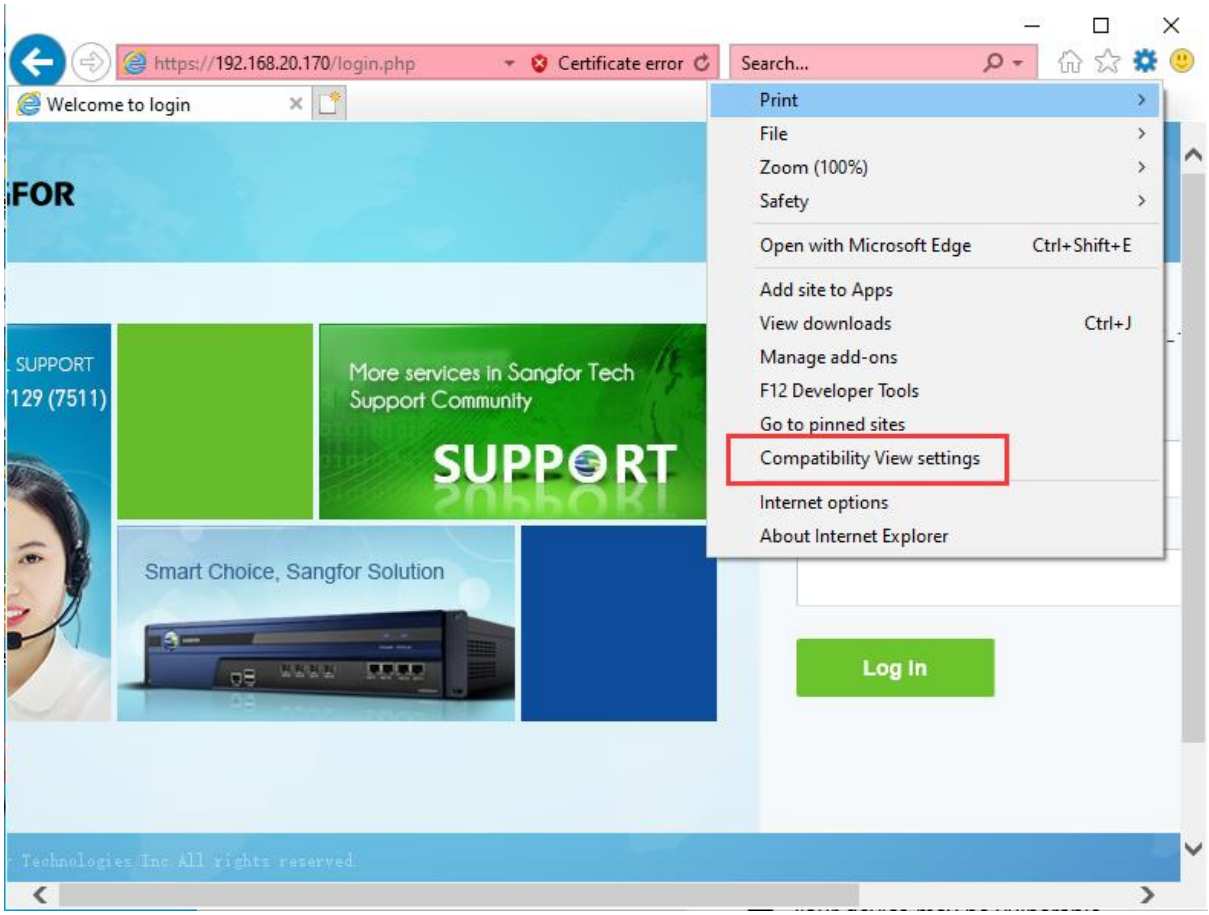


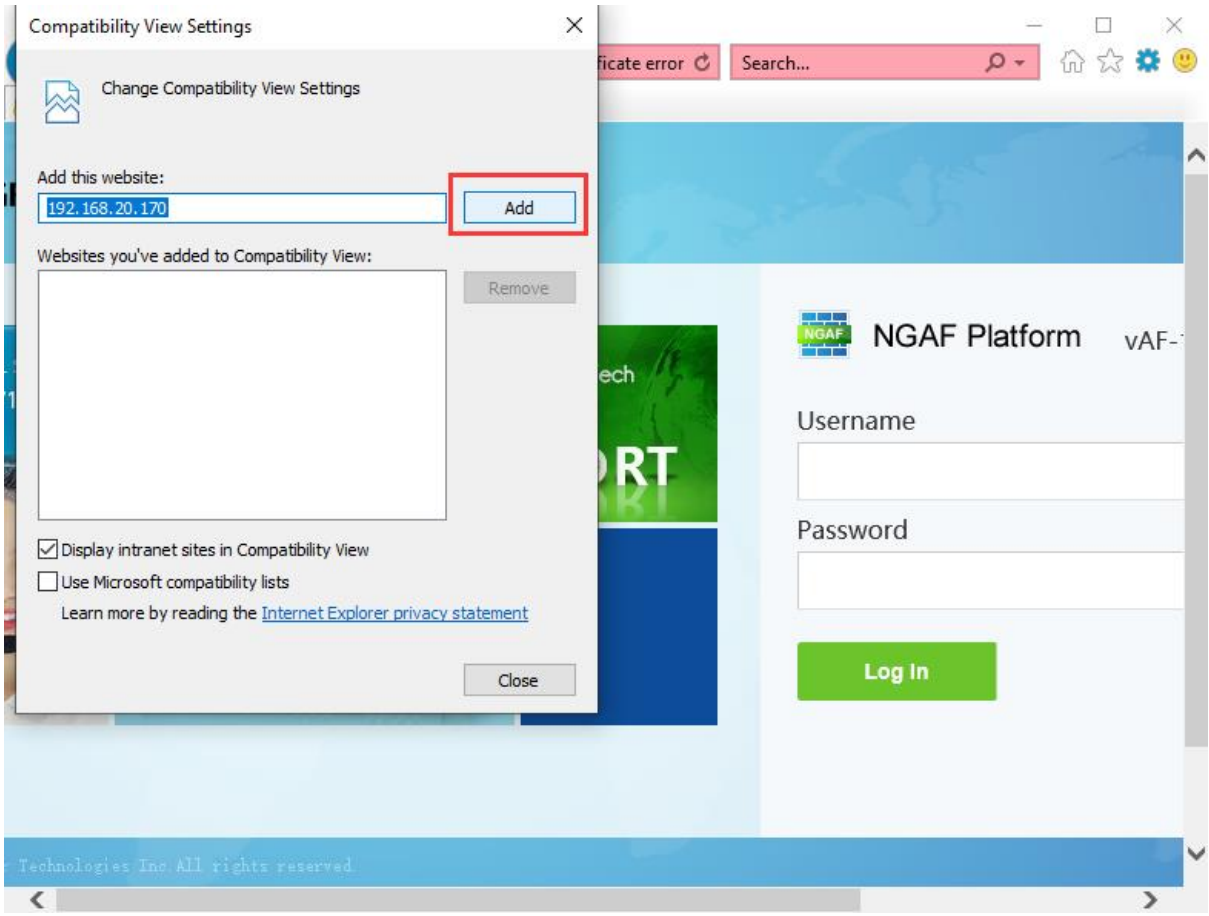
3. Pada PC intranet Cabang, coba lakukan ping ke PC intranet kantor Pusat, dan uji apakah PC 192.168.2.2 pada kantor cabang dapat melakukan ping kepada PC 192.168.1.3. Jika ping berhasil makan komunikasi normal.



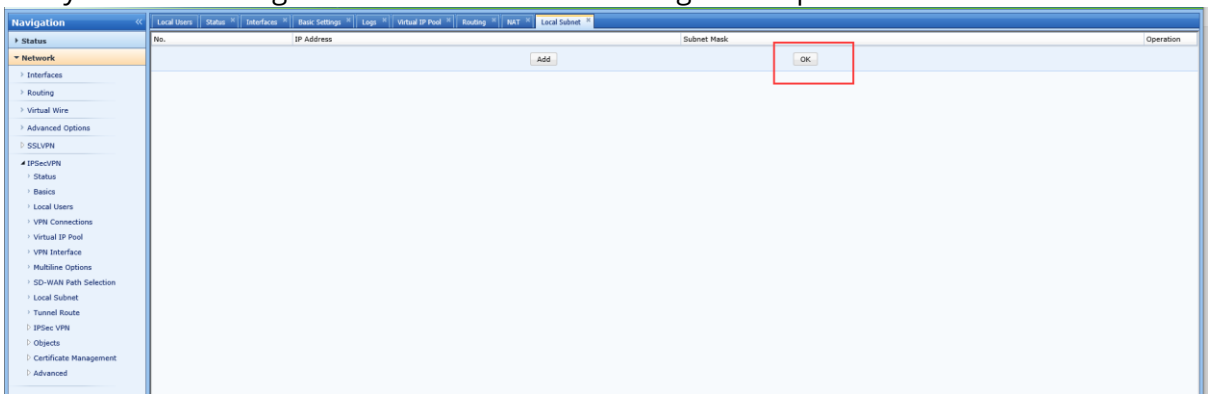
BAB 5 Perhatian

1. Disarankan untuk mengunakan perambah/browser IE untuk melakukan konfigurasi perangkat VPN dan gunakan fungsi kompabilitas perambah.

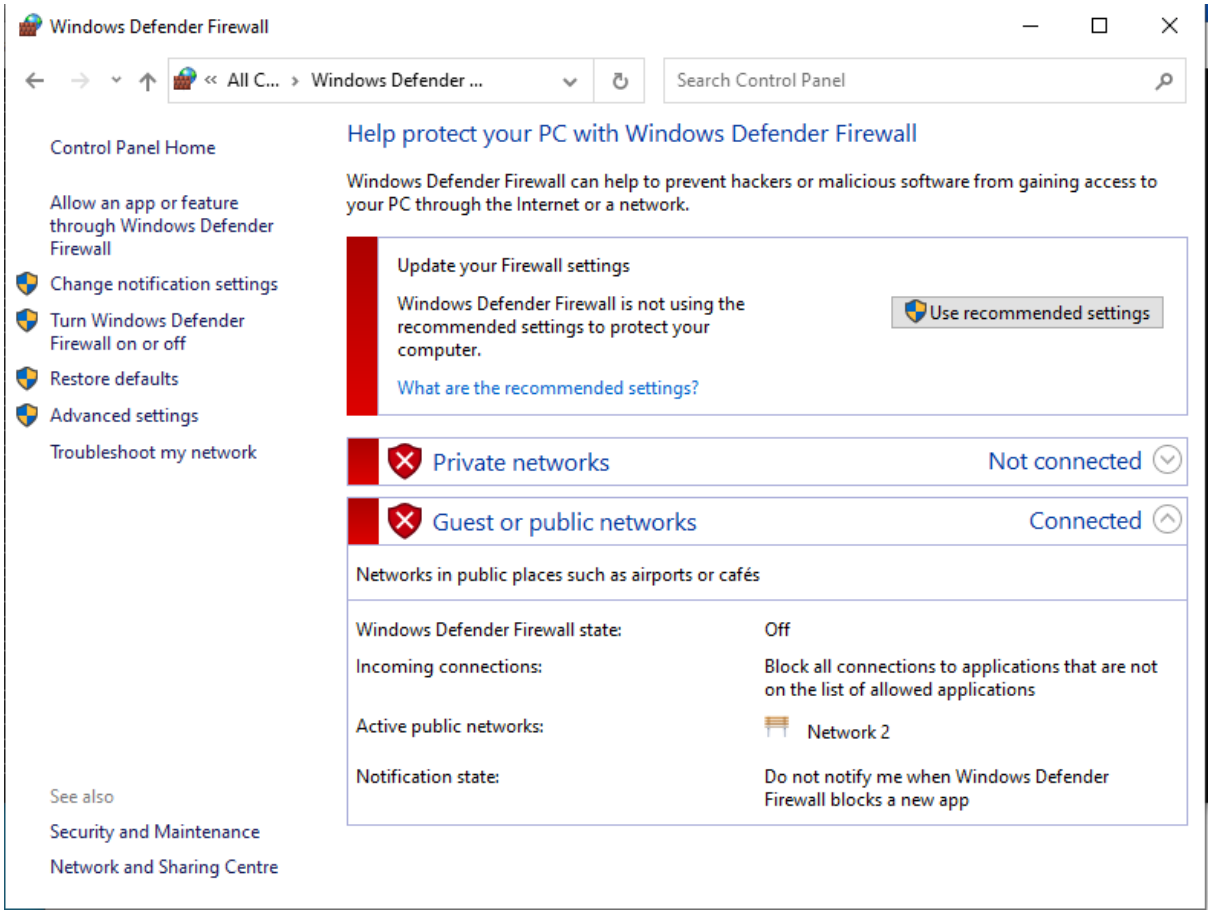

https://192.168.20.170/login.php
Certificate error
Search...
Welcome to login
Print
File
Zoom (100%)
Safety
Open with Microsoft Edge Ctrl+Shift+E
Add site to Apps
View downloads Ctrl+J
Manage add-ons
F12 Developer Tools
Go to pinned sites
Compatibility View settings
Internet options
About Internet Explorer
More services in Sangfor Tech Support Community
SUPPORT
Smart Choice, Sangfor Solution
Log In

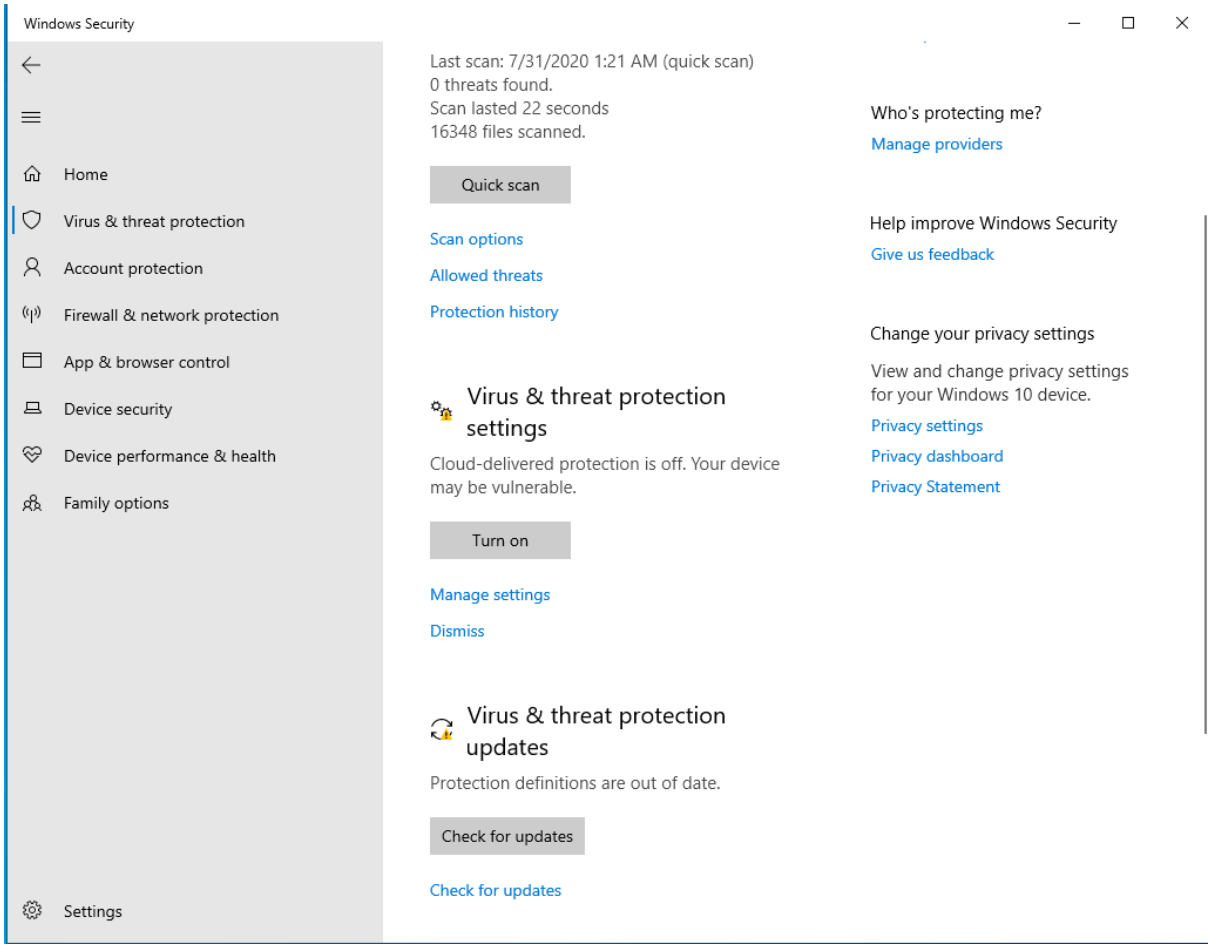

Compatibility View Settings
Change Compatibility View Settings
Add this website:
192.168.20.170
Add
Websites you've added to Compatibility View:
Remove
Display intranet sites in Compatibility View
Use Microsoft compatibility lists
Learn more by reading the Internet Explorer privacy statement
Close
Search...
NGAF Platform
Username
Password
Log In

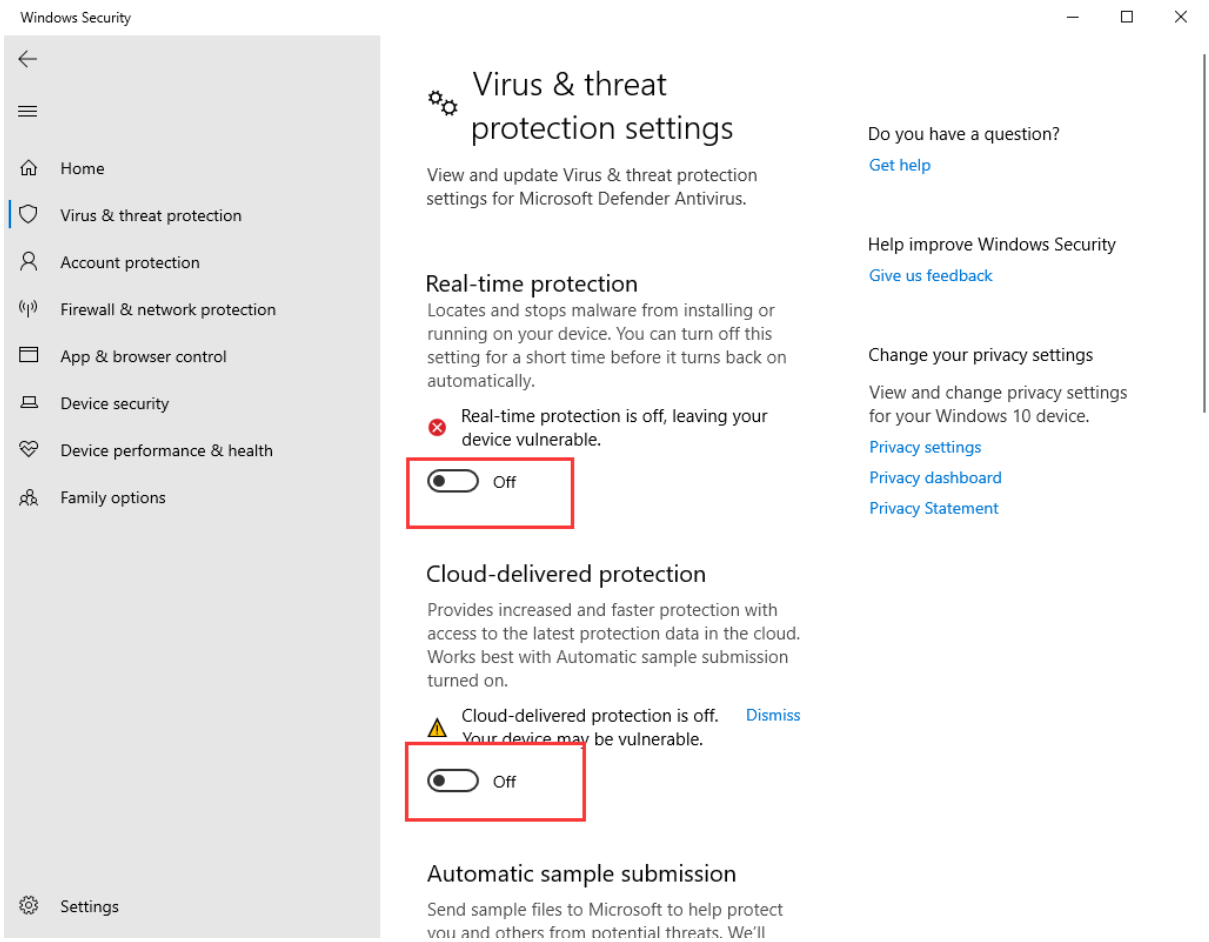
2. Konfigurasi VPN memiliki opsi “OK” yang banyak, pastikan melakukan klik “OK” setelah menyelesaikan konfigurasi untuk memastikan konfigurasi dapat berlaku.



3. Saat pengujian konektivitas, disarankan untuk mematikan firewall pada PC intranet kantor pusat dan cabang untuk menghindari kegagalan uji ping karena sistem firewall tidak dimatikan.




Windows Security
Home
Virus & threat protection
Account protection
Firewall & network protection
App & browser control
Device security
Device performance & health
Family options
Settings
Last scan: 7/31/2020 1:21 AM (quick scan)
0 threats found.
Scan lasted 22 seconds
16348 files scanned.
Quick scan
Scan options
Allowed threats
Protection history
Virus & threat protection settings
Cloud-delivered protection is off. Your device may be vulnerable.
Turn on
Manage settings
Dismiss
Virus & threat protection updates
Protection definitions are out of date.
Check for updates
Check for updates
Who's protecting me?
Manage providers
Help improve Windows Security
Give us feedback
Change your privacy settings
View and change privacy settings for your Windows 10 device.
Privacy settings
Privacy dashboard
Privacy Statement



4. Pemecahan masalah dapat diaktifkan untuk uji IP untuk menghindari pencegatan paket data karena konfigurasi policy NGAF.