SANGFOR

IPsec VPN
Standard Configuration Guide

Perubahan Catatan

Tanggal	Deskripsi Perubahan
19 Agustus, 2019	Panduan konfigurasi IPsec VPN.

Daftar Isi

Bab 1 Panduan Konfigurasi IPSEC VPN

1.1 Dokumen Teknis

SANGFOR_IPSECVPN _ STANDARD_CONFIGURATION_GUIDE_201908919

Bab 2 Versi Produk

Setiap dokumen harus ditulis dengan versi produk terbaru kecuali ada instruksi khusus. DLAN Versi 5.0 dan yang lebih baru.

Bab 3 Persiapan

3.1 Persyaratan Inspeksi

Sebelum melakukan konfigurasi standar IPSEC, perlu dikonfirmasi beberapa kondisi berikut ini :

1) Standar IPSEC Sangfor mengikuti protokol IPSEC VPN standar internasional, selama VPN peer juga menggunakan protokol standar IPSEC, maka kami dapat menggunakan koneksi VPN dengan peer.
2) Kebutuhan Peralatan Sangfor dan kebutuhan peralatan pihak ketiga untuk koneksi VPN, perlu ada otorisasi untuk menghubungkan kedua peer, perlu ditinjau kembali license yang diperlukan di management WEBUI Perangkat.
3) Jika perangkat Sangfor digunakan dalam mode single-arm, untuk melakukan IPSEC standar, periksa versi DLAN dari perangkat Sangfor.

Apakah DLAN yang digunakan menggunakan versi 5.0 atau diatasnya. Jika tidak, hubungi vendor untuk memastikan apakah hal ini bisa diupgrade.

3.2 Konfirmasi Lingkungan

Standar koneksi IPSEC memiliki dua mode, Main mode dan aggressive mode. Lalu kita perlu tahu, dalam situasi seperti apa harus memilih mode koneksi yang sesuai, Berikut ini beberapa kondisi yang dapat digunakan sebagai acuan:

1. Ketika terdapat konfigurasi NAT pada kedua sisi perangkat yang terkoneksi VPN, Anda harus menggunakan aggressive mode.
   a. Jika kedua sisi menggunakan IP Statis dan tidak ada konfigurasi NAT, anda dapat menggunakan aggressive mode atau main mode!
   b. Jika salah satu sisi menggunakan ADSL dan tidak terdapat konfigurasi NAT.

      Jika lalu lintas data dari ADSL ke IP statis intranet, If the traffic is sent from ADSL to the static ip intranet, anda bisa memilih menggunakan main mode atau aggressive mode.

      Jika lalu lintas data dikirim dari IP statis intranet ke ADSL intranet, kemudian harus menerapkan shell untuk ADSL, pastikan situs ip statis harus mengaktifkan nama domain dari koneksi ADSL!
   c. Jika kedua belah pihak adalah ADSL, harus ada nama domain untuk menerapkan shell guna memastikan bahwa satu situs dapat terhubung melalui nama domain ke VPN situs lain!

   (PS: ADSL dapat diperoleh dari alamat jaringan pribadi operator, jika operator memiliki NAT, maka harus terhubung dalam mode agresif)

2. Di dalam default main mode Sangfor VPN hanya mendukung alamat ip sebagai ID! Mode agresif VPN Sangfor hanya mendukung FQDN sebagai id secara default (tetapi mode agresif DLAN 5.x dan di atasnya dapat mendukung alamat IP sebagai ID)
3. Sangfor VPN hanya mendukung IPsec berbasis Kebijakan, tidak mendukung IPsec berbasis rute (IPsec berbasis rute: IPsec didasarkan pada terowongan GRE)
4. Sangfor VPN fase kedua hanya mendukung menggunakan mode Tunnel, tidak mendukung mode Transport!
5. Sangfor vpn tahap pertama hanya mendukung menggunakan versi protokol IKE versi 1, tidak mendukung IKE versi 2!

Bab 4 Panduan Konfigurasi

4.1 Contoh kasus koneksi Main mode

Sebagai contoh, terdapat satu kasus dibawah ini:

Kantor pusat sebuah perusahaan menggunakan perangkat Sangfor sebagai gateway.

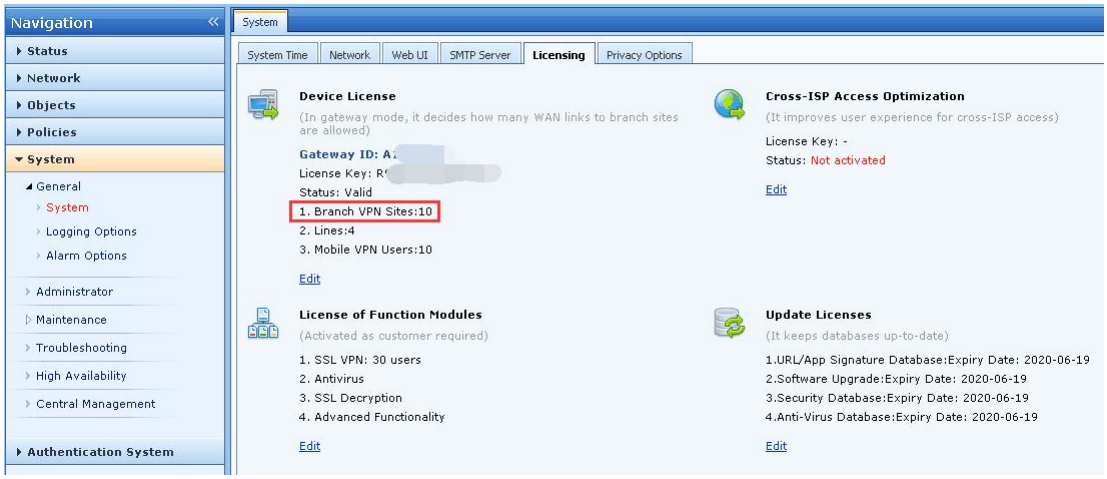
Perangkat dengan mode Gateway memiliki IP Jaringan publik statis 1.1.1.1 jaringan intranet memiliki segmen 192.168.1.0/24. Pelanggan memiliki kantor cabang yang menjadi peer firewall untuk melakukan proses ekspor. IP public statis cabang adalah 2.2.2.2 dan jaringan internalnya menggunakan segment 192.168.2.0/24. Saat ini customer ingin perangkat Sangfor terkoneksi dengan firewall yang berada di cabang menggunakan koneksi vpn. Diharapkan, segmen internal pada kantor pusat 192.168.1.0 dapat berkomunikasi dengan segmen internal kantor cabang 192.168.2.0

Persiapan:

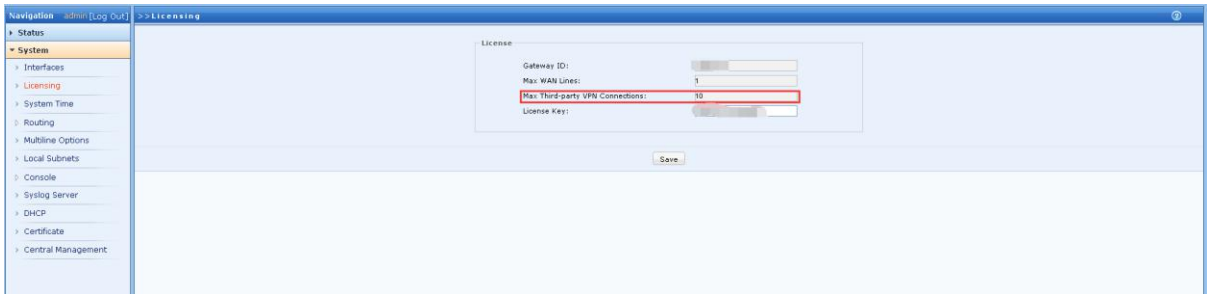
1) Pastikan bahwa VPN pada firewall cabang menggunakan standar protocol IPSEC dan dapat terkoneksi.
2) Pastikan bahwa perangkat sangfor memiliki lisensi untuk standar koneksi IPSEC. Seperti ditampilkan pada gambar dibawah ini, tidak terdapat otorisasi, perlu melakukan aktivasi lisensi. Hubungi personil sales pemasaran lokal mengenai hal ini.

IAM

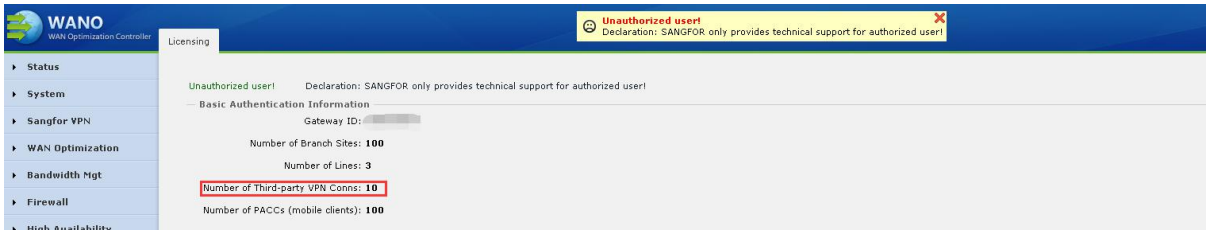
NGAF



MIG



WANO



Koneksi VPN dapat dilakukan setelah proses otorisasi telah selesai.

4.1.1 Pemilihan Mode

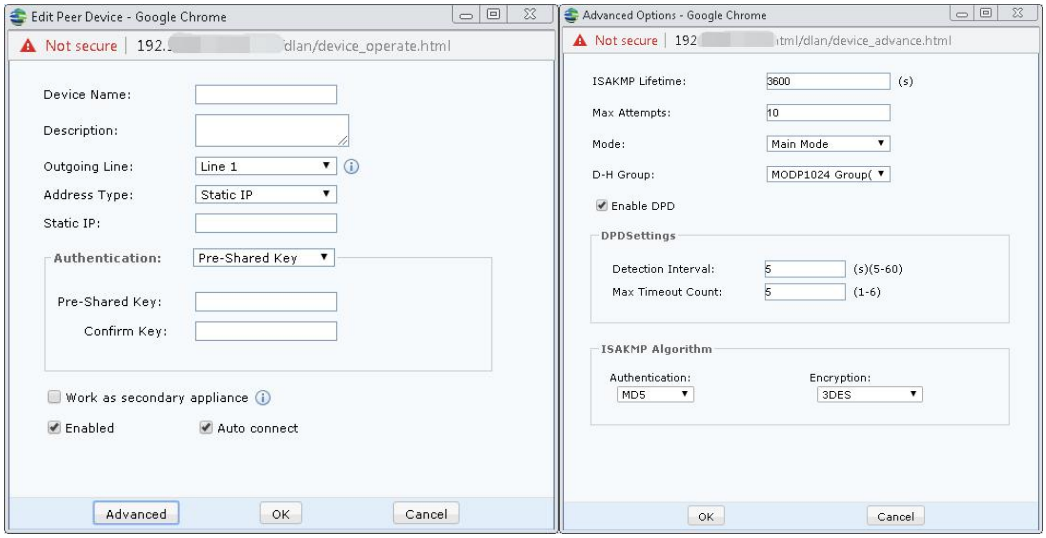
Pelanggan tidak menggunakan konfigurasi NAT. Kedua sisi memiliki alamat IP publik statis, dan kedua sisi memiliki alamat IP publik. Anda dapat memilih main mode atau aggressive mode. Dalam hal ini, main modedipilih untuk koneksi.

4.1.2 Implementasi Konfigurasi

Konfigurasi pada perangkat Sangfor sesuai dengan kebutuhan spesifik pelanggan. Konfigurasi spesifiknya ditunjukkan di bawah ini:

Fase pertama konfigurasi:

IAM, NGAF, MIG, dan WANO menggunakan interface konfigurasi yang sama.



Device Name: Nama Perangkat disisi lawan

Static IP: IP Publik Perangkat disisi lawan

Pre-Share Key: Sama seperti konfigurasi perangkat disisi lawan

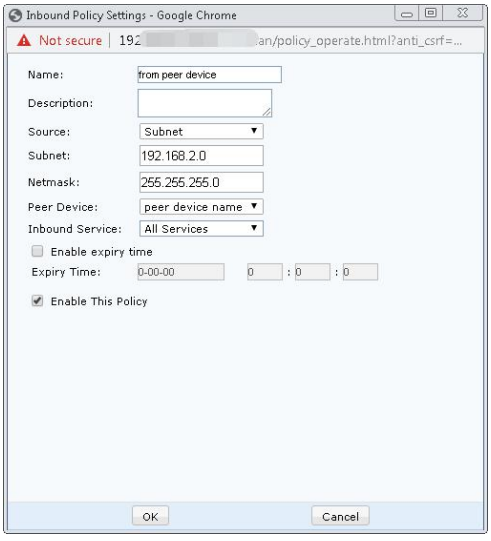
Confirm Key: Sama seperti konfigurasi perangkat disisi lawan

Pastikan seluruh konfigurasi yang dilakukan sama seperti perangkat disisi lawan.

Konfigurasi tahap kedua :

Pertama, buat kebijakan data yang akan masuk kedalam jaringan. Kebijakan traffic yang masuk ini untuk segmen jaringan yang akan diakses oleh sisi lawan. Jika ada beberapa segmen jaringan yang mengisi beberapa kebijakan, dalam hal ini peer hanya memiliki satu segmen jaringan dengan 192.168.2.0/24. Saat ini menetapkan kebijakan akses kedalam jaringan dapat digunakan. Konfigurasi spesifiknya terlihat pada gambar berikut:

IAM, NGAF, MIG, dan WANO menggunakan antarmuka konfigurasi yang sama.

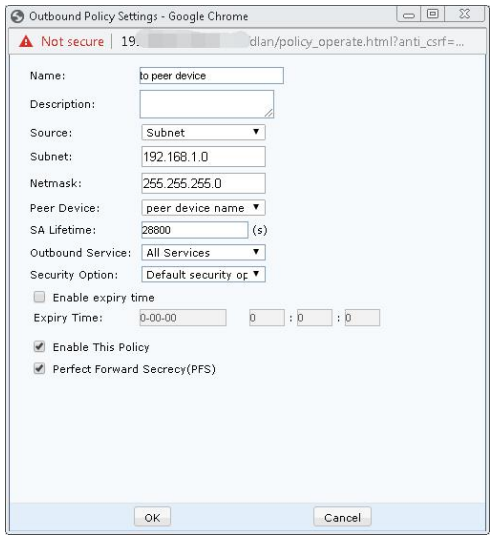


Subnet/Netmask: Subnet local milik perangkat disisi lawan

Peer Device: Perangkat disisi lawan yang dibuat pada tahap 1

Kemudian Anda dapat membuat kebijakan data keluar. Kebijakan outbound ini mendefinisikan segmen jaringan apa yang akan diakses oleh segmen jaringan lokal, jika terdapat beberapa segmen jaringan yang mengisi beberapa kebijakan. Konfigurasi spesifiknya adalah sebagai berikut:

IAM, NGAF, MIG, dan WANO menggunakan antarmuka konfigurasi yang sama.



Subnet/Netmask: Subnet Local.

Peer Device: Perangkat disisi lawan yang dibuat pada tahap 1.

Perfect Forward Secrecy(PFS) : sama seperti perangkat disisi lawan.

The second phase of the security option selects the default Security option, which reads as follows:

IAM, NGAF, MIG, and WANO is using pretty much same interface.

Fase kedua dari opsi keamanan memilih opsi Keamanan default, seperti berikut ini:

IAM, NGAF, MIG, dan WANO menggunakan antarmuka yang hampir sama.

Pada titik ini, konfigurasi perangkat Sangfor telah selesai. Jika pihak ketiga telah dikonfigurasi, kita dapat melihat koneksi yang sudah terhubung pada status DLAN yang terlah diperbolehkan ;

Selebihnya adalah konfigurasi peer. Konfigurasi masing-masing vendor mungkin sedikit berbeda. Konfigurasi peer sesuai dengan persyaratan konfigurasi pabrikan mereka.

Bab 5 Precautions

1) Standar IPSEC Sangfor perlu disahkan. Untuk otorisasi khusus, Anda dapat menghubungi tim penjualan untuk konsultasi..
2) Jika konfigurasi VPN tidak terhubung setelah konfigurasi selesai, Anda dapat membuka log sistem untuk melihat apakah ada kesalahan, ubah konfigurasi sesuai dengan pesan kesalahan
3) Saat melakukan interkoneksi IPSEC standar, peralatan pabrikan peer harus memperhatikan antara VPN dan LAN memungkinkan dalam aturan firewall.