



SANGFOR



NGAF

Panduan Konfigurasi GRE melalui IPsec VPN

Versi 8.0.8



Perubahan Catatan

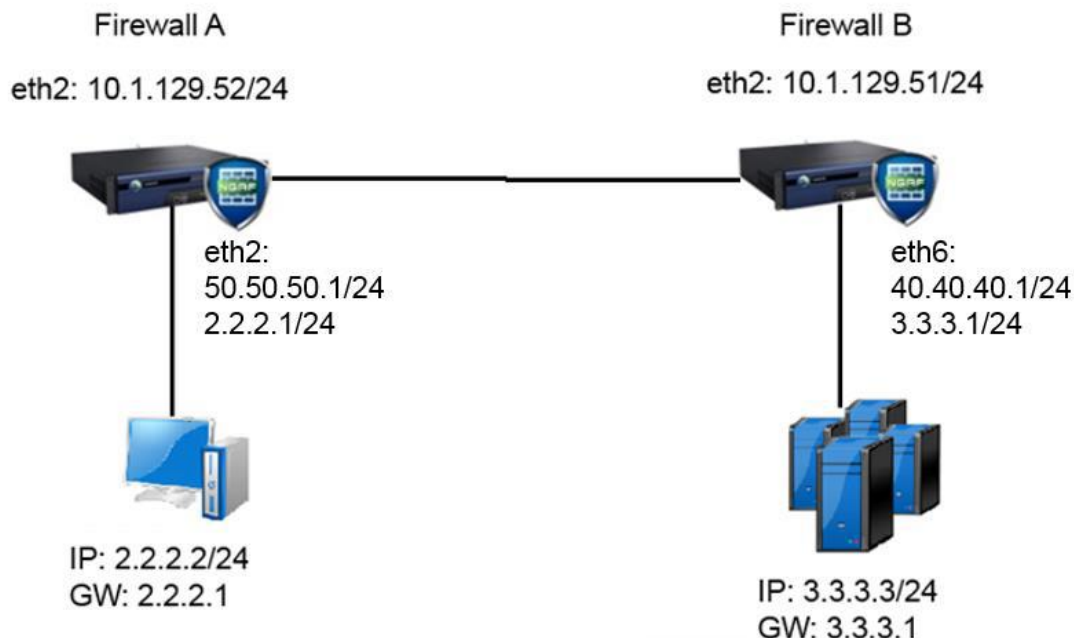
Tanggal	Deskripsi Perubahan
27 Nov, 2019	Panduan Konfigurasi GRE over IPsec VPN

Daftar Isi

Bab 1 Skenario Aplikasi.....	1
Bab 2 Metode Konfigurasi.....	1
Bab 3 Tindakan Pencegahan.....	7

Bab 1 Skenario Aplikasi

GRE melalui IPsec VPN, seperti yang ditunjukkan di bawah ini:



Kebutuhan:

1. Versi NGAF minimal harus 7.1.
2. NGAF mampu berkomunikasi dengan rekan.
3. Kedua NGAF harus menggunakan VPN IPsec untuk membuat koneksi.
4. Dalam antarmuka VPN LAN jaringan yang berbeda segmen IP harus ditambahkan di atas IP gateway yang ada. IP baru digunakan untuk memecahkan masalah pengaruh kebijakan masuk VPN dan kebijakan keluar yang secara langsung memungkinkan IP LAN berkomunikasi melalui VPN tunnel.

Bab 2 Metode Konfigurasi

1. Konfigurasi jaringan dasar perlu memastikan bahwa antarmuka, bawaan route dan zona dikonfigurasi dengan benar. Kebijakan keamanan konten harus diijinkan semua. Detailnya bisa merujuk ke “SANGFOR_NGAF_V8.0.5_Panduan Penyebaran Mode Route”, seperti yang ditampilkan di bawah:
http://community.sangfor.com/plugin.php?id=sangfor_databases:index&mod=viewdatabase&tid=975

Sebuah segmen jaringan tambahan ditambahkan dalam antarmuka NGAF LAN, Firewall A tambah 50.50.50.1, Firewall B tambah 40.40.40.1

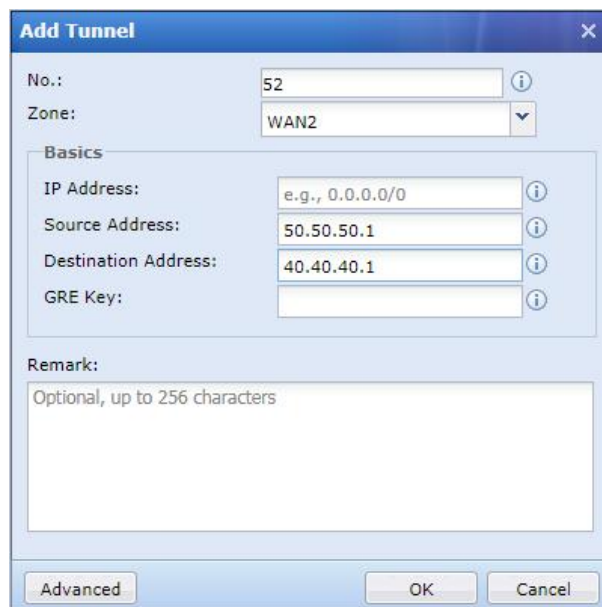
Firewall A

Firewall B

Catatan: Kecuali NAT tidak perlu dikonfigurasi, konfigurasi lain dapat merujuk ke berkas yang disediakan.

- Setelah konfigurasi jaringan dasar telah selesai, kemudian masuk Network > Interface > GRE Tunnel untuk mengkonfigurasi antarmuka GRE, seperti yang ditampilkan:

Firewall A



Add Tunnel

No.: 52

Zone: WAN2

Basics

IP Address: e.g., 0.0.0.0/0

Source Address: 50.50.50.1

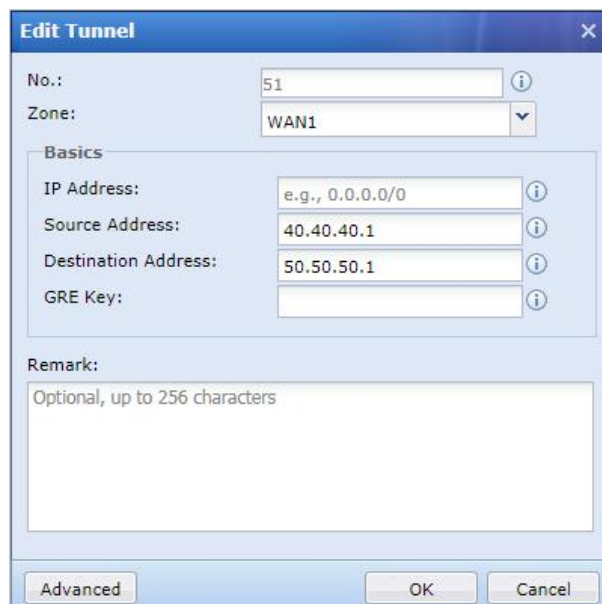
Destination Address: 40.40.40.1

GRE Key:

Remark:
Optional, up to 256 characters

Advanced OK Cancel

Firewall B



Edit Tunnel

No.: 51

Zone: WAN1

Basics

IP Address: e.g., 0.0.0.0/0

Source Address: 40.40.40.1

Destination Address: 50.50.50.1

GRE Key:

Remark:
Optional, up to 256 characters

Advanced OK Cancel

Catatan:

Alamat IP: Antarmuka GRE alamat IP, IP ini adalah alamat IP baru, PC lokal dan IP antarmuka peer tidak boleh memiliki konflik IP. Konfigurasi skenario OSPF harus dikonfigurasi.

Alamat IP sumber: Alamat IP antarmuka lokal WAN

Alamat IP tujuan: Alamat IP antarmuka WAN

GRE Kunci: Harus sama di kedua sisi, tidak dapat dikonfigurasi.

- Konfigurasi IPsec VPN, dengan menggunakan antarmuka yang baru ditambahkan alamat IP untuk membangun koneksi CPN, detail konfigurasi seperti yang ditunjukkan:

Firewall A

Fase 1 Konfigurasi:

Device Name: FirewallA

Description:

Outgoing Line: Line 1

Address Type: Static IP

Static IP: 10.1.129.51

Authentication: Pre-Shared Key

Pre-Shared Key: *****

Confirm Key: *****

☐ Work as secondary appliance

☒ Enabled ☒ Auto connect

Advanced OK Cancel

Fase 2 Konfigurasi:
Inbound Policy:

Name: Firewall B inbound

Description:

Source: Subnet

Subnet: 40.40.40.0

Netmask: 255.255.255.0

Peer Device: FirewallA

Inbound Service: All Services

☐ Enable expiry time

Expiry Time: 0-00-00 0 : 0 : 0

☒ Enable This Policy

OK Cancel

Outbound Policy:

Outbound Policy Settings - Google Chrome

Not secure | /clu~d75eedd0-706b-4899-9668-7ff...

Name: Firewall A outbound

Description:

Source: Subnet

Subnet: 50.50.50.0

Netmask: 255.255.255.0

Peer Device: FirewallA

SA Lifetime: 28800 (s)

Outbound Service: All Services

Security Option: Default security opt

☐ Enable expiry time

Expiry Time: 0-00-00 0 : 0 : 0

☒ Enable This Policy

☐ Perfect Forward Secrecy(PFS)

OK Cancel

Firewall B

Fase 1 Konfigurasi:

Edit Peer Device - Google Chrome

Not secure | /clu~d75eedd0-706b-4899-9668-7ff...

Device Name: Firewall A

Description:

Outgoing Line: Line 1

Address Type: Static IP

Static IP: 10.1.129.52

Authentication: Pre-Shared Key

Pre-Shared Key: *****

Confirm Key: *****

☐ Work as secondary appliance

☒ Enabled ☒ Auto connect

Advanced OK Cancel

Fase 2 Konfigurasi:

Inbound policy:

Outbound policy:

4. Konfigurasi static route yang akan mengarahkan paket ke GRE tunnel, seperti yang ditunjukkan di bawah ini:

Firewall A:

Destination:	3.3.3.0
Subnet Mask:	255.255.255.0
Next-Hop IP:	0.0.0.0
Interface:	Tunnel52
Metric:	0
Link State Detection:	Disable

Firewall B:

Destination:	2.2.2.0
Subnet Mask:	255.255.255.0
Next-Hop IP:	0.0.0.0
Interface:	Tunnel51
Metric:	0
Link State Detection:	Disable

Sebagai VPN tunnel telah dienkripsi, oleh karena itu jika paket diambil dari antarmuka WAN tidak dapat menangkap paket yang dienkapsulasi GRE. Tetapi GRE tunnel di lingkungan pengujian ini harus dibangun, kemudian LAN PC dan IP server dapat melakukan ping satu sama lain. Ini karena kebijakan masuk dan keluar VPN tidak mengandung LAN PC dan IP server, paket ping PC tidak dapat memasuki VPN tunnel. Karena itu, jika ada salah konfigurasi, paket tidak akan memasuki GRE tunnel, PC tidak dapat ping server.

Bab 3 Tindakan Pencegahan

1. Dalam antarmuka VPN LAN berbeda segmen jaringan IP harus ditambahkan di atas IP gateway yang ada. IP yang baru ditambahkan akan bertindak sebagai alamat VPN route.
2. Perlu mengkonfigurasi static route untuk membiarkan paket melalui GRE tunnel. Antarmuka GRE tunnel akan dipilih sebagai antarmuka static route, next-hop IP akan 0.0.0.0
3. Layanan VPN harus diaktifkan di Network > IPsec VPN > Status.



Hak cipta (c) Sangfor Technologies Inc. Hak cipta dilindungi oleh undang-undang. Dilarang menyebarkan atau memproduksi ulang sebagian dari atau seluruh dokumen ini tanpa persetujuan tertulis dari Sangfor Technologies Inc. SANGFOR adalah merek dagang dari Sangfor Technologies Inc. Semua merek dagang dan nama dagang lain yang disebutkan dalam dokumen ini adalah milik dari pemegangnya masing-masing. Segala upaya telah dilakukan dalam mempersiapkan dokumen ini untuk memastikan keakuratan konten, namun semua pernyataan, informasi, dan rekomendasi dalam dokumen ini bukan merupakan jaminan dalam bentuk apa pun, tersurat maupun tersirat. Informasi dalam dokumen ini dapat berubah tanpa pemberitahuan. Untuk mendapatkan versi terbaru, hubungi pusat layanan internasional SANGFOR Technologies Inc.