SANGFOR

NGAF

Pedoman Terbaik untuk Konfigurasi SangforVPN

Version 8.0.35

Data Perubahan

Tanggal	Keterangan Perubahan
May 5, 2021	Rilis Dokumen
May 17, 2021	Pembaruan Dokumen

DAFTAR ISI

BAB 1 Pedoman

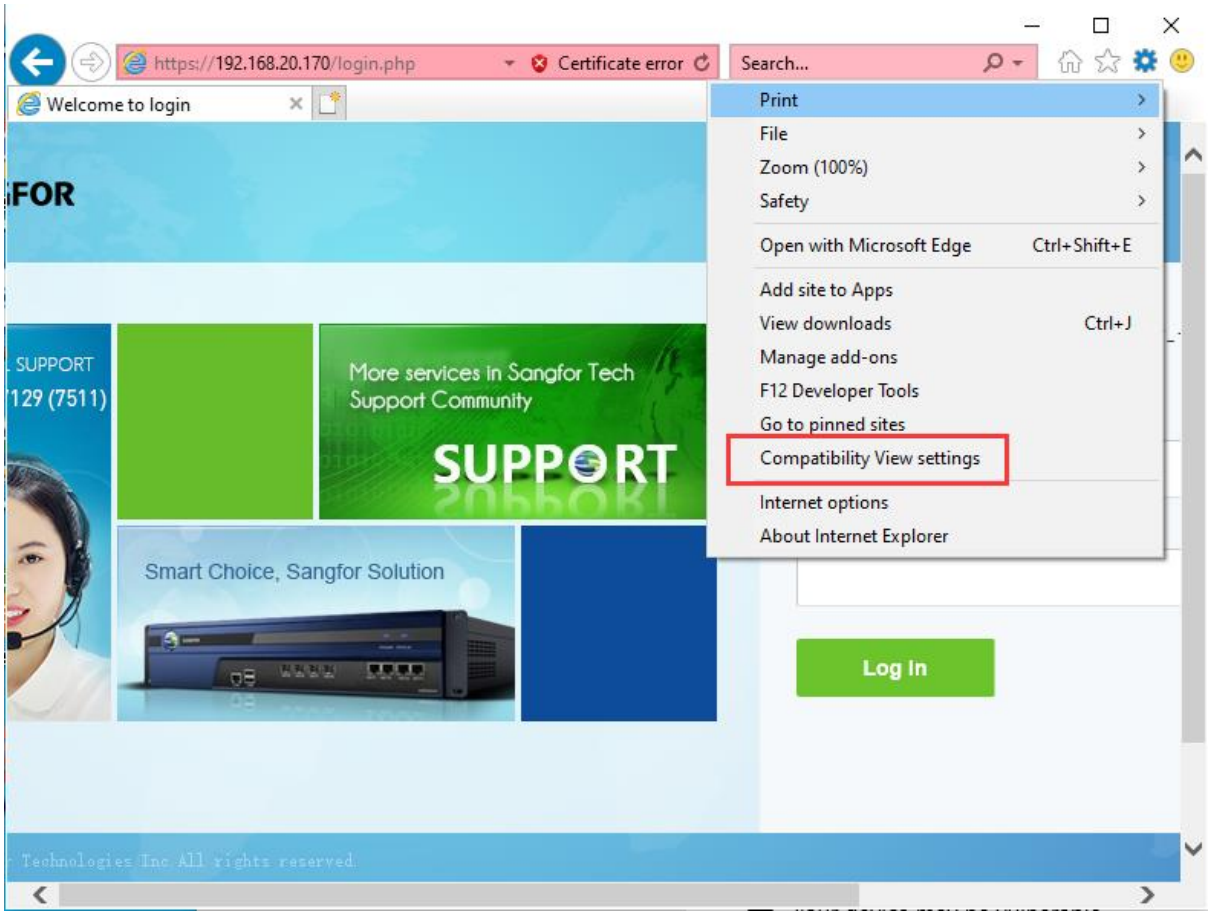
Dokumen terkait:

Pedoman ini untuk melakukan Konfigurasi yang biasanya mencakup pemilihan "deployment mode", ide konfigurasi, informasi yang diambil, limitasi fungsi, perbedaan fungsi. Mengenai ketetapan IPSecVPN, jika anda ingin mempelajari tentan skenario POC dan rincian langkah konfigurasi, silahkan merujuk pada tautan berikut:

https://sangforltd.sharepoint.com/:w:/s/PMO/ESPQS42Oql9HjS-k3hCnNOcBNzltE3YeH5FQeENkLFcs7w?e=Dx72P2

1.1 Pengenalan Dasar

1. Jika pengguna menggunakan NGAF sebelum versi 8.0.26. disarankan untuk mengunakan perambah IE untuk mengkonfigurasi fungsi VPN dan aktifkan fungsi adaptasi kompabilitas pada perambah.



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

3. Dibandingkan dengan IPSecVPN standar, SANGFOR VPN memiliki keunggulan sebagai

berikut:

Mendukung lingkup jaringan publik dimana kedua sisi menggunakan IP yang tidak tetap.

Teknologi VPN dengan multi-line multiplexing untuk mencapai load-balancing dan backup jaringan VPN

Teknologi VPN dengan line dedicated untuk mengwujudkan isolasi antara jaringan VPN dan jaringan publik

Teknologi Inter-tunnel routing, pengguna cabang online melalui jaringan kantor pusat, dapat mengwujudkan manajemen terpadu dan kontrol dari kantor pusat.

Teknologi NAT antar tunnel untuk memecahkan masalah konflik segmen IP di beberapa jaringan cabang.

Teknologi Flow control dalam tunnel untuk mewujudkan alokasi bandwidth yang wajar

1.2 Konfirmasi Kebutuhan dan Penerapan

1. Konfirmasi apakah nama pengguna dan kata kunci yang diisi untuk manajemen koneksi dari perangkat cabang telah sama dengan nama pengguna dan kata kunci yang dikonfigurasi dari manajemen pengguna perangkat kantor pusat, dan pastikan bahwa alamat webagent diisi dengan alamat perangkat kantor pusat pada perangkat kantor cabang.

2. Skenario kantor pusat dengan Multi-IP

Untuk mengkonfirmasi apakah format sudah benar, klik tombol test selama konfigurasi manajemen koneksi (catatan: uji hanya untuk memastikan format, bukan koneksivitas).

3. Ada skenario dimana perangkat kantor pusat dan cabang adalah peran kantor pusat

Konfigurasi webagent utama dan cadangan dari cabang akses harus sama persis dengan kantor pusat (termasuk format, IP, port);

4. Skenario single-armed pada perangkat kantor pusat

1) Walaupun perangkat jaringan dengan jalur keluar mengunakan Port Mapping untuk UDP dan TCP dengan port 4009 (dengan asumsi bahwa port VPN adalah default tidak dirubah; gunakan UDP untuk VPN, perangkat gateway jalur keluarnya harus dilakukan pemetaan port secara simetris); Gunakan telnet untuk menguji port 4009 dari alamat IP jaringan publik kantor pusat dapat terkoneksi ke komputer melalui internet (hanya port TCP yang berlaku, tidak bisa untuk UDP)

2) Skenarion Single-arm perlu dilakukan pemetaan ke multiple line IP, tetapi tidak dapat dipetakan ke IP Port LAN;

3) Untuk DLAN620 dan yang terbaru, pada skenarion single-arm, jika multiple line diaktifkan, IP Internet harus terhubung langsung ke IP jaringan publik pada beberapa line/jalur;

5. Ketika perangkat gateway keluar dari kantor pusat atau perangkat kantor pusat

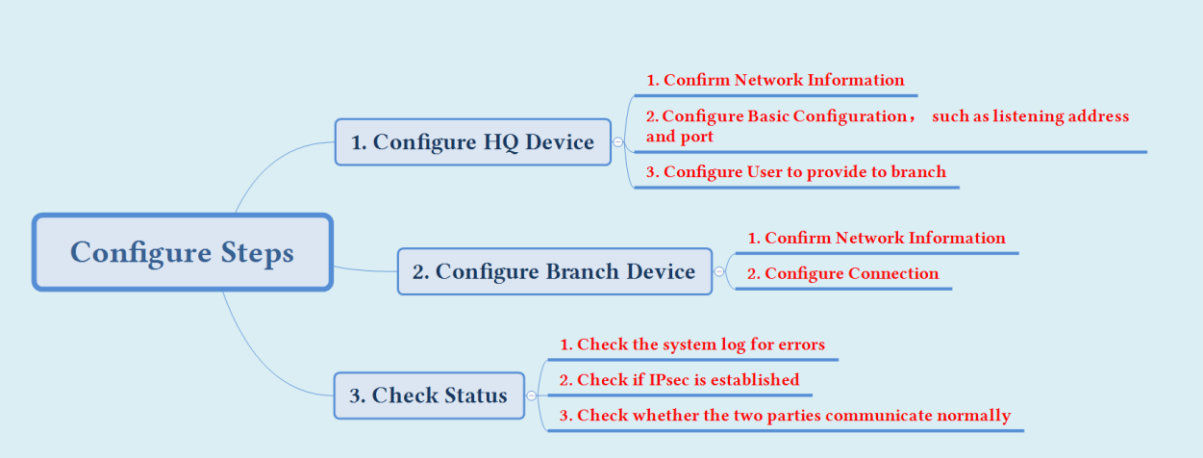
digunakan sebagai gerbang keluar dan menggunakan dial-up PPPoE untuk akses Internet

Satu hal yang perlu diperhatikan yaitu PPPoE tidak mendapatkan IP yang diberikan oleh operator. IP yang didapat dari PPPoE tidak dapat diubah, tetapi harus merupakan IP publik. Jika anda menemukan hal ini, harap hubungi operator/ISP untuk mendapatkan IP publik langsung dari pada IP private/pribadi.

6. Konfirmasi apakah perangkat cabang dapat mengakses Internet dan koneksi jaringan keluar normal. telnet pada perangkat cabang untuk menguji koneksi ke port 4009 perangkat kantor pusat

1.3 Konfigurasi untuk Pedoman

1.3.1 Langkah Konfigurasi



3. Dibandingkan dengan standar IPSecVPN, SANGFOR VPN memiliki keunggulan sebagai berikut:

Mendukung jaringan publik dimana kedua sisi tidak memiliki IP tetap

Teknologi VPN dengan multi-line multiplexing untuk mencapai load-balancing dan backup jaringan VPN

Teknologi VPN dengan line dedicated untuk mengwujudkan isolasi antara jaringan VPN dan jaringan publik

Teknologi Inter-tunnel routing, pengguna cabang online melalui jaringan kantor pusat, dapat mengwujudkan manajemen terpadu dan kontrol dari kantor pusat.

Teknologi NAT antar tunnel untuk memecahkan masalah konflik segmen IP di beberapa jaringan cabang.