Site-to-Site VPN über IPsec einrichten

Dokument-ID	**Site-to-Site VPN über IPsec einrichten**
Version	2.2
Status	Final
Ausgabedatum	03.2021

Centro Business
Configuration instructions

Swisscom (Switzerland) Ltd
3050 Bern

Inhalt

Swisscom (Schweiz) AG
3050 Bern

Site-to-Site VPN über IPsec einrichten

1.1 Bedürfnis

Sie möchten zwischen zwei oder mehrere Standorte Daten über eine sicher Verbindung austauschen. Sie möchten von einem Standort über eine sichere Verbindung auf Geräte weiterer Standorts zugreifen um Beispielsweise einen Raum zu überwachen.

1.2 Beschreibung

Im Centro Business Router können Sie ein Virtuelles Pivates Netzwerk (VPN) einfach im Router-GUI aktivieren. Sie haben danach die Möglichkeit via VPN-Tunnel auf Hosts von bis zu 10 Standorten zuzugreifen. Jeder Standort erhält dabei eine andere eindeutige LAN-IP-Adressierung. Die IP-Adressen für die Peer's subnet können gemäss RFC1918 (10.0.0.0/8 + 172.16.0.0/12 + 192.168.0.0/16) verwendet werden. Um einen Standort zu erreichen braucht jeder Standort eine fixe public-IP-Adresse oder einen dynDNS-Account.

1.3 Voraussetzung/Einschränkungen

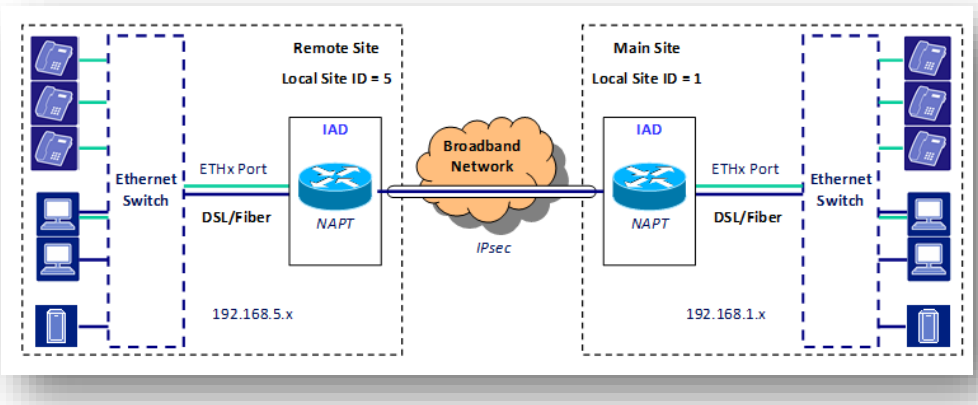
Voraussetzungen:

- Swisscom Vertrag: Business Internet Services, My KMU Office, inOne KMU office, Enterprise Connect XS, Business Internet Light
- Centro Business 2.0 mit aktueller Firmware Version. Die Firmware finden Sie auf der offiziellen Centro Business Hilfeseite unter Firmware aktualisieren
- Der Zugriff auf das Routerportal ist hergestellt
- Erreichbarkeit: Min. 1 fixe IP-Adresse oder dynDNS

Einschränkungen:

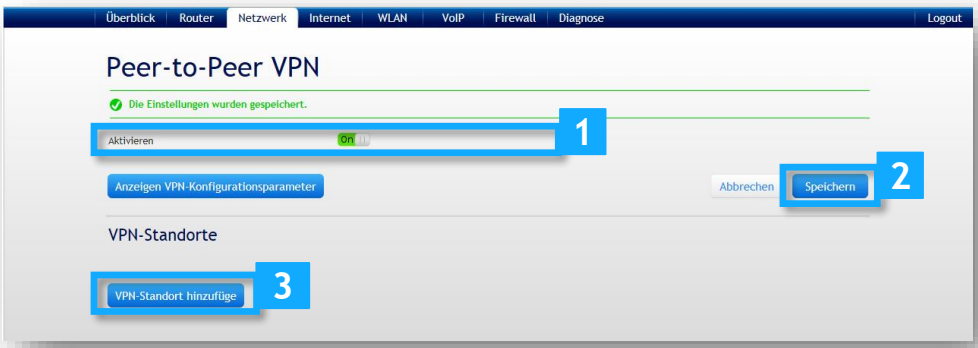
- PPPoE Passtruogh darf nicht aktiviert sein
- Die Subnetze 192.168.11.0/24 und 192.168.13.0/24 können nicht an den VPN-Standorte genutzt werden.
- QoS oder eine fixe Bandbreitenreservation auf dem IPsec VPN-Tunnel wird nicht unterstütz. Eine Vernetzung für VoIP wird nicht empfohlen.
- Der Service wurde mit Zyxel 2802, Zywall und Fortigate getestet.

1.4 Abbildung

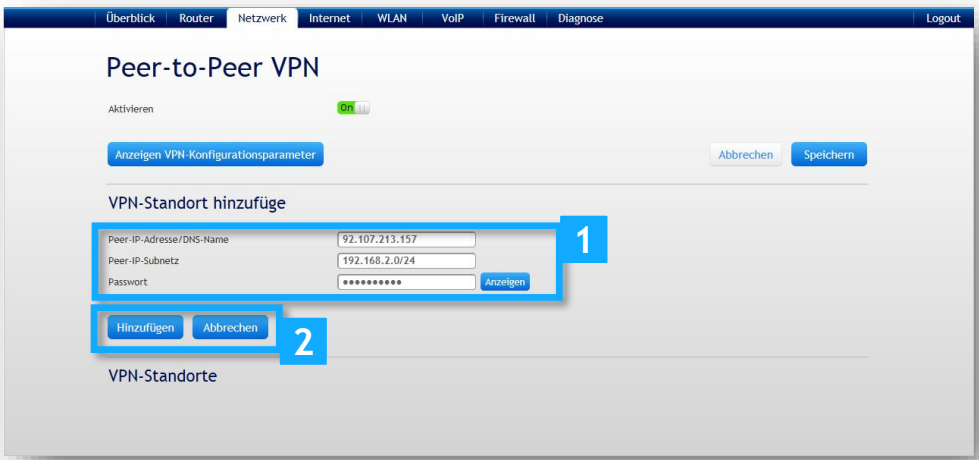


1.5 VPN auf Centro Business einrichten

Wählen Sie im Router den Menüpunkt **Netzwerk, Peer-to-Peer VPN**. Setzen Sie den Schalter «Aktivieren» auf on und speichern Sie die Einstellungen mit dem Button **Speichern** ab. Mit dem Button **VPN Standorte hinzufügen** können Sie nun einen neuen VPN-Standort konfigurieren.



Tragen Sie im Abschnitt **VPN-Standort hinzufügen** unter **Peer-IP-Adresse/DNS-Name** die WAN-IP-Adresse oder den DNS-Namen des neuen Standortes ein. Ergänzen Sie die LAN-IP-Adressierung des neuen VPN-Standortes im Feld **Peer-IP-Subnetz.** Der Eintrag wird zum Beispiel im Format 192.168.N.0/24 gemacht, wobei für N ein Wert von 1 bis 10 empfohlen wird. Beachten Sie dass jeder Standort eine abweichende LAN-Adressierung benötigt. Für jeden VPN-Tunnel können Sie ein eigenes Passwort bestimmen, beachten Sie dass das gleiche Passwort auch auf der Gegenstelle eingetragen werden muss. Schliessen Sie den Vorgang mit dem Button **Hinzufügen** ab. Um Ihrem VPN weitere Standorte zuzufügen, wiederholen Sie diese Schritte je Standort.

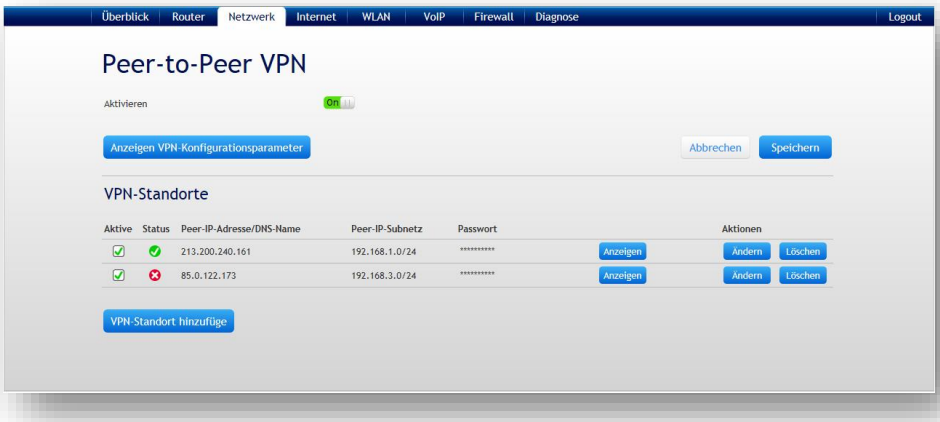


1.6 Kontrolle Verbindungsstatus

Unter **Gegenstellen** sind nun alle eingerichteten VPN-Standorte aufgelistet. Jeder Standort kann einzeln deaktiviert und aktiviert werden. Der Status jedes VPN-Tunnels wird mit einer Farbe dargestellt.

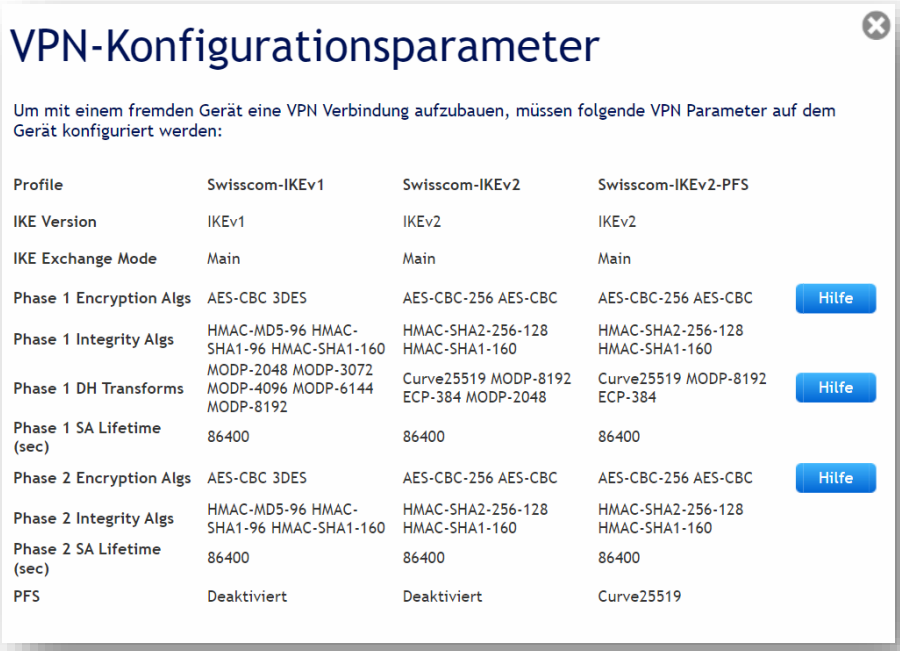
- Grau: DNS Name kann nicht aufgelöst werden.
- Grün: der Tunnel ist aktiv.
- Rot: der Tunnel ist offline, es wird kein Traffic gesendet oder der Tunnel konnte nicht aufgebaut werden

Achtung! Der Status des neu eingerichteten VPN-Tunnels aktiviert sich erst, wenn Traffic über die Verbindung läuft. Testen Sie deswegen die VPN-Verbindung mit einem Ping.



1.7 VPN-Parameter anzeigen

Im Menü **Peer to Peer VPN** können Sie mit dem Button „Anzeigen VPN Konfigurationsparameter“ die korrekten Einstellungen anzeigen und somit die Einstellungen auf einem VPN Client richtig eintragen.



VPN-Konfigurationsparameter

Um mit einem fremden Gerät eine VPN Verbindung aufzubauen, müssen folgende VPN Parameter auf dem Gerät konfiguriert werden:

Profile	Swisscom-IKEv1	Swisscom-IKEv2	Swisscom-IKEv2-PFS	
IKE Version	IKEv1	IKEv2	IKEv2	
IKE Exchange Mode	Main	Main	Main	
Phase 1 Encryption Algs	AES-CBC 3DES	AES-CBC-256 AES-CBC	AES-CBC-256 AES-CBC	Hilfe
Phase 1 Integrity Algs	HMAC-MD5-96 HMAC-SHA1-96 HMAC-SHA1-160	HMAC-SHA2-256-128 HMAC-SHA1-160	HMAC-SHA2-256-128 HMAC-SHA1-160	
Phase 1 DH Transforms	MODP-2048 MODP-3072 MODP-4096 MODP-6144 MODP-8192	Curve25519 MODP-8192 ECP-384 MODP-2048	Curve25519 MODP-8192 ECP-384	Hilfe
Phase 1 SA Lifetime (sec)	86400	86400	86400	
Phase 2 Encryption Algs	AES-CBC 3DES	AES-CBC-256 AES-CBC	AES-CBC-256 AES-CBC	Hilfe
Phase 2 Integrity Algs	HMAC-MD5-96 HMAC-SHA1-96 HMAC-SHA1-160	HMAC-SHA2-256-128 HMAC-SHA1-160	HMAC-SHA2-256-128 HMAC-SHA1-160	
Phase 2 SA Lifetime (sec)	86400	86400	86400	
PFS	Deaktiviert	Deaktiviert	Curve25519	