

Paramétrer un VPN intersite via IPsec

ID document	Paramétrer un VPN intersite via Ipsec
Version	2.2
Statut	Version finale
Date d'édition	01.2023

Instructions de
configuration Centro
Business

Swisscom (Suisse) SA
3050 Berne



swisscom

Contenu

1.1 Besoins	3
1.2 Description	3
1.3 Conditions/Restrictions	3
1.4 Illustration	3
1.5 Paramétrer un VPN sur le routeur Centro Business	4
1.6 Contrôle du statut de la connexion	5
1.7 Afficher les paramètres du VPN	5

Paramétrer un VPN intersite via IPsec

1.1 Besoins

Vous souhaitez échanger des données par une connexion sécurisée entre deux sites ou plus. Vous souhaitez accéder depuis un site aux appareils d'autres sites par une connexion sécurisée, par exemple pour assurer la surveillance d'un local.

1.2 Description

Vous pouvez simplement activer un réseau privé virtuel (VPN) sur l'interface (GUI) du routeur Centro Business. Ensuite, vous avez la possibilité d'accéder aux hôtes de 10 sites max. via le tunnel VPN. Chaque site reçoit une adresse LAN IP distincte. Les adresses IP pour le sous-réseau du peer sont utilisables conformément à RFC1918 (10.0.0.0/8 + 172.16.0.0/12 + 192.168.0.0/16). Pour atteindre un site, chaque site a besoin d'une adresse IP fixe publique ou d'un compte dynDNS.

1.3 Conditions/restrictions

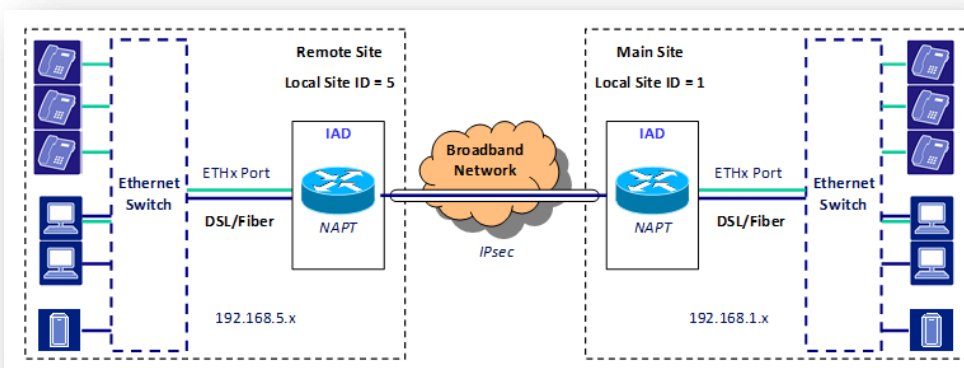
Conditions:

- Contrat Swisscom: Business Site Internet Services, My PME Office, Enterprise Connex XS, Business Internet Light
- Centro Business 2.0 avec la version actuelle du firmware. Vous pouvez trouver le firmware sur la page d'aide officielle de Centro Business sous [Mise à jour du firmware](#).
- L'accès est configuré sur le portail du routeur
- Joignabilité: au moins une adresse IP fixe ou dynDNS

Restrictions:

- PPPoE Passtrough ne doit pas être activé.
- Les sous-réseaux 192.168.11.0/24 et 192.168.13.0/24 ne sont pas utilisables comme sites VPN.
- Le QoS ou une réservation de large bande fixe n'est pas prise en charge sur le tunnel VPN IPsec. Une mise en réseau pour VoIP n'est pas recommandée.
- Le service a été testé avec Zyxel 2802, Zywall et Fortigate.
- Les connexions VPN fonctionnant sans adresse IP fixe ne peuvent pas être établies si l'un des deux sites communique sur le réseau mobile (Failover ou Mobile-only) (en raison du CGMAT).

1.4 Illustration



1.5 Paramétrer un VPN sur le routeur Centro Business

Sur le routeur, sélectionnez l'option du menu **Réseau, Peer-to-Peer VPN**. Cochez la case «Activer». Enregistrez ces paramètres avec le bouton **Enregistrer**. Avec le bouton **Ajouter site VPN** vous pouvez maintenant configurer un nouveau site VPN.



Dans la partie **Ajouter site VPN**, saisissez sous **Adresse IP/Nom DNS du peer** l'adresse IP WAN ou le nom DNS du nouveau site. Complétez l'adresse IP LAN du nouveau site VPN dans le champ **Sous-réseau IP du peer**. La saisie s'effectue par exemple au format 192.168.N.0/24, avec N représentant une valeur comprise entre 1 et 10. Veuillez tenir compte du fait que tous les sites ont besoin d'une adresse LAN différente. Vous pouvez définir un mot de passe propre à chaque tunnel VPN. Veuillez tenir compte du fait que le même mot de passe doit être saisi sur le site distant. Bouclez le processus en cliquant sur le bouton **Ajouter**. Pour ajouter d'autres sites à votre VPN, répétez ces étapes pour chaque site.



1.6 Contrôle du statut de la connexion

Sous **Sites distants** figurent tous les sites VPN configurés. Chaque site peut être activé et désactivé. Le statut de chaque tunnel VPN est représenté par une couleur.

- Gris: le nom DNS ne peut pas être supprimé.
- Vert: le tunnel est actif.
- Rouge: le tunnel est désactivé, le trafic est nul ou le tunnel n'a pas pu être constitué.

Attention! Le statut du tunnel VPN récemment configuré n'est activé que lorsque le trafic passe par la connexion. Par conséquent, testez la connexion VPN avec un Ping.

Active	Statut	Adresse IP/Nom DNS du peer	Sous-réseau IP du peer	Mot de passe	Actions
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	213.200.240.161	192.168.1.0/24	*****	Afficher Modifier Supprimer
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	85.0.122.173	192.168.3.0/24	*****	Afficher Modifier Supprimer

1.7 Afficher les paramètres du VPN

Dans le menu **Peer to Peer VPN**, vous pouvez afficher les paramètres corrects avec le bouton «Afficher les paramètres de configuration VPN», et saisir les paramètres exacts sur un client VPN.

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	Aide
Phase 1 Integrity Algs	HMAC-MD5-96 HMAC-SHA1-96 HMAC-SHA1-160 MODP-2048 MODP-3072	HMAC-SHA2-256-128 HMAC-SHA1-160	HMAC-SHA2-256-128 HMAC-SHA1-160	
Phase 1 DH Transforms	MODP-4096 MODP-6144 MODP-8192	Curve25519 MODP-8192 ECP-384 MODP-2048	Curve25519 MODP-8192 ECP-384	Aide
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	Aide
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	Désactivé	Désactivé	Curve25519	