

Configurazione VPN Site-to-Site tramite IPsec

ID documento	Configurazione VPN Site-to-Site tramite Ipsec
Versione	2.2
Stato	Stesura finale
Data d'emissione	03.2021

Centro Business
Guida alla
configurazione

Swisscom (Svizzera) SA
3050 Berna



Sommario

1.1 Esigenza	3
1.2 Descrizione	3
1.3 Requisiti/limitazioni	3
1.4 Immagine	3
1.5 Configurazione VPN su Centro Business	4
1.6 Controllo dello stato di connessione	5
1.7 Visualizzazione dei parametri VPN	5

Configurazione VPN Site-to-Site tramite IPsec

1.1 Esigenza

Desiderate scambiare dati tra due o più siti tramite un collegamento sicuro.
Desiderate accedere da un sito ad apparecchi di altri siti tramite un collegamento sicuro per monitorare ad esempio un'area.

1.2 Descrizione

Nel router Centro Business potete attivare facilmente una rete privata (VPN) nella Router-GUI. Avete quindi la possibilità di accedere tramite tunnel VPN a host di un massimo di dieci siti. Ogni sito riceve in questo caso un indirizzamento IP LAN univoco diverso. Gli indirizzi IP per la Peer's subnet possono essere utilizzati come da RFC1918 (10.0.0.0/8 + 172.16.0.0/12 + 192.168.0.0/16). Per raggiungere un sito, ogni sito necessita di un indirizzo IP fisso pubblico o di un account dynDNS.

1.3 Requisiti/limitazioni

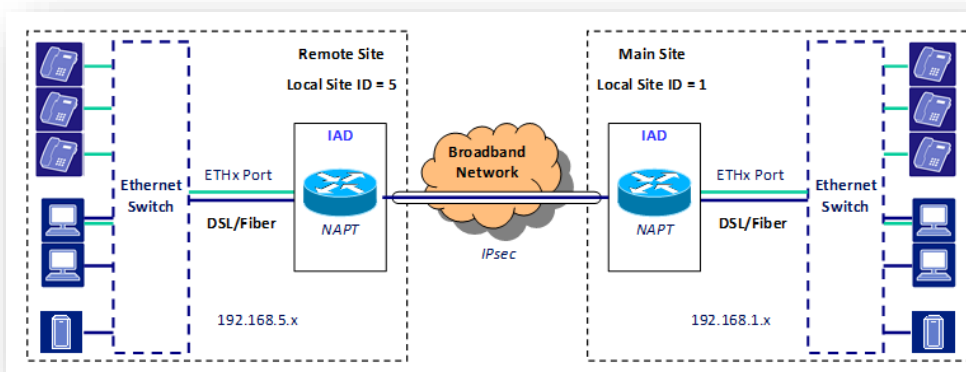
Requisiti:

- Contratto Swisscom: My PMI Office , inOne PMI office, Business Internet Services, Enterprise Connect XS, Business Internet Light
- Centro Business 2.0 con l'attuale versione del firmware. Il firmware è disponibile nella pagina di aiuto ufficiale di Centro Business alla voce [Aggiorna firmware](#).
- l'accesso al portale router è stabilito
- reperibilità: min. un indirizzo IP fisso o dynDNS

Limitazioni:

- il Passthrough PPP non deve essere attivato
- le sottoreti 192.168.11.0/24 e 192.168.13.0/24 non possono essere utilizzate nei siti VPN.
- QoS o una riserva di banda larga fissa sul tunnel VPN IPsec non sono supportate. È sconsigliabile un collegamento in rete per VoIP.
- il servizio è stato testato con Zyxel 2802, Zywall e Fortigate.

1.4 Immagine



1.5 Configurazione VPN su Centro Business

Nel router selezionate il comando del menu **Rete, Peer-to-Peer VPN**. Impostate il segno di spunta nel campo **Abilita**. Salvate le impostazioni con il pulsante **Salva**. Con il pulsante **Siti VPN** è possibile configurare ora una nuova sede VPN.



Nella sezione **Siti VPN**, in corrispondenza di **Indirizzo Peer-IP/Nome DNS del peer**, inserite l'indirizzo IP WAN o il vostro nome DNS del nuovo sito. Compilate l'indirizzamento IP LAN del nuovo sito VPN nel campo **Sottorete Peer-IP**. L'inserimento avviene ad esempio nel formato 192.168.N.0/24, dove N rappresenta un valore che va da uno a dieci. Notate che ciascun sito necessita di un indirizzamento LAN differente. Per ciascun tunnel VPN potete stabilire una vostra password. Notate che è necessario inserire la stessa password anche sul sito remoto. Terminate la procedura con il pulsante **Aggiungi**. Per dotare il vostro VPN di ulteriori siti, ripetete questi passaggi per ciascuno di essi.



1.6 Controllo dello stato di connessione

Alla voce **Siti remoti** ora sono elencati tutti i siti VPN configurati. Ogni sito può essere disattivato e attivato singolarmente. Lo stato di ciascun tunnel VPN viene raffigurato con un colore.

- Grigio: il nome DNS non può essere slegato
- Verde: il tunnel è attivo.
- Rosso: il tunnel è offline, non viene inviato traffico o il tunnel non è stato stabilito correttamente.

Attenzione! Lo stato del tunnel VPN recentemente installato viene attivato solo quando il traffico attraversa la connessione. Testi pertanto la connessione VPN con un Ping.

Attivo	Stato	Indirizzo IP/Nome DNS del peer	Sottorete IP del peer	Password	Azioni
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	213.200.240.161	192.168.1.0/24	*****	Mostra Modifica Cancella
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	85.0.122.173	192.168.3.0/24	*****	Mostra Modifica Cancella

1.7 Visualizzazione dei parametri VPN

Nel menu **Peer to Peer VPN**, con il pulsante «Mostra i parametri di configurazione VPN» è possibile visualizzare le impostazioni corrette e inserire quindi correttamente le impostazioni su un'applicazione locale 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	Aiuto
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	Aiuto
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	Aiuto
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	Disabilitato	Disabilitato	Curve25519	