# How to set up site-to-site VPN through IPsec

| | |
|---|---|
| **Dokument-ID** | How to set up site-to-site VPN through IPsec |
| **Version** | 2.2 |
| **Status** | Final Version |
| **Date of publication** | 03.2011 |

Centro Business
Konfigurationsanleitung

Swisscom (Schweiz) AG
3050 Bern

# Contents






Swisscom (Switzerland) Ltd
3050 Bern


# How to set up site-to-site VPN through IPsec



## 1.1 Need

Your objective is to exchange data securely between two or more sites. A further objective is to securely access devices located at remote sites from one other site to, for example, monitor a room.

## 1.2 Description

The Centro Business Router allows you to easily activate a virtual private network (VPN) in the router GUI. It will allow you to then access the hosts of up to 10 sites via the VPN tunnel. Each site receives its own individual, distinct LAN IP address. The IP addresses for the peers' subnet are used in accordance with RFC1918 (10.0.0.0/8 + 172.16.0.0/12 + 192.168.0.0/16). In order to reach a site, each site will require a fixed public IP addresses or a dynDNS account.

## 1.3 Requirements/limitations

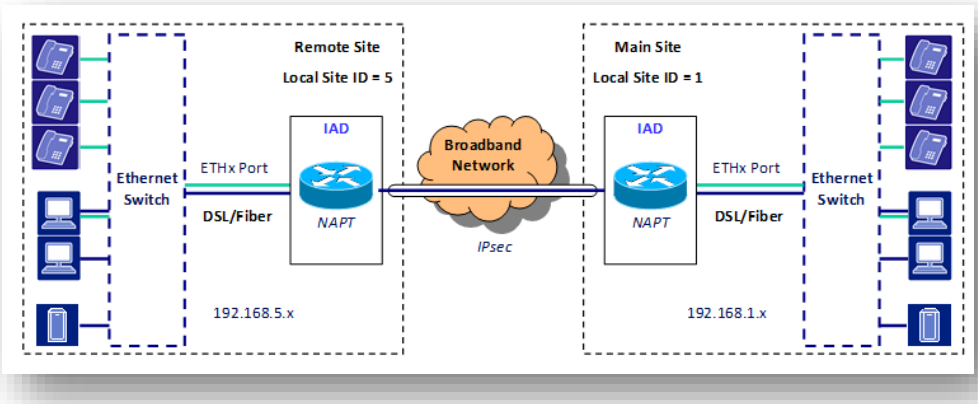
Requirements:

- Swisscom Contract: My SME Office, Business Internet Services, Enterprise Connect XS, Business Internet Light
- Centro Business 2.0 with current firmware version. You can find the firmware on the official Centro Business help page under Update Firmware
- Access to the router portal is established
- Availability: Min. 1 fixed IP address or dynDNS account

Limitations:

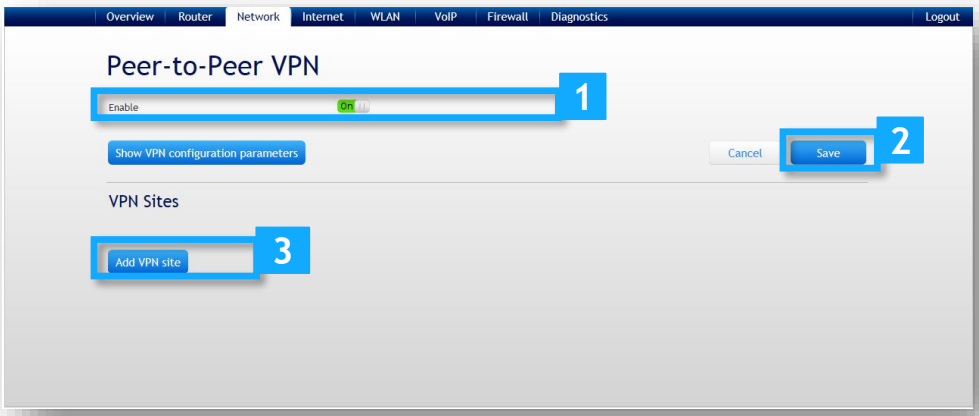
- PPPoE Passthrough may not be activated.
- The 192.168.11.0/24 and 192.168.13.0/24 subnets cannot be used at the VPN sites.
- QoS or a fixed bandwith reservation on the IPsec VPN tunnel is not supported. A network link for VoIP is not recommended.
- The service was tested with Zyxel 2802, Zywall and Fortigate.

## 1.4 Illustration



## 1.5 How to set up the VPN for Centro Business

In the router menu, select **Network > Peer-to-Peer VPN**. Set “Enable” to “On”. Store your preferences by pressing **Save.** By selecting **Add VPN site,** you can now configure one additional VPN site.



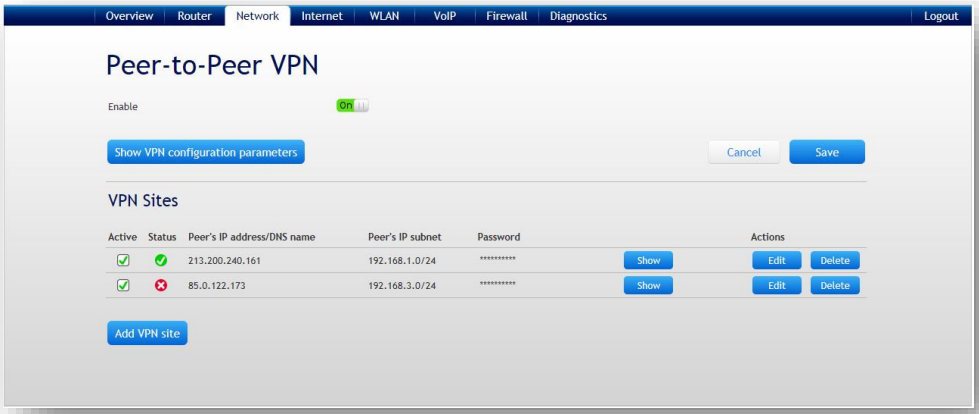

In the **Add VPN Site** section, under **Peer’s IP address/DNS name,** enter the WAN IP address or the DNS name for the new site. Add the LAN IP address of the new VPN site in the **Peer’s IP subnet** field. Use, for example, the 192.168.N.0/24 format to make an entry, whereby N is recommended as a value for 1 to 10. Remember that each site requires a unique LAN address. You may set your own password for every VPN tunnel. Note that you will need to enter the same password at the remote site. Finalise the process by pressing **Add.** Repeat this process for each remote site that you want to add.

## 1.6 Monitoring the connection status

**Remote sites** will provide you with a list of all the VPN sites you have added. Each site can be individually deactivated and activated. The operating status of every VPN tunnel is represented by a colour.

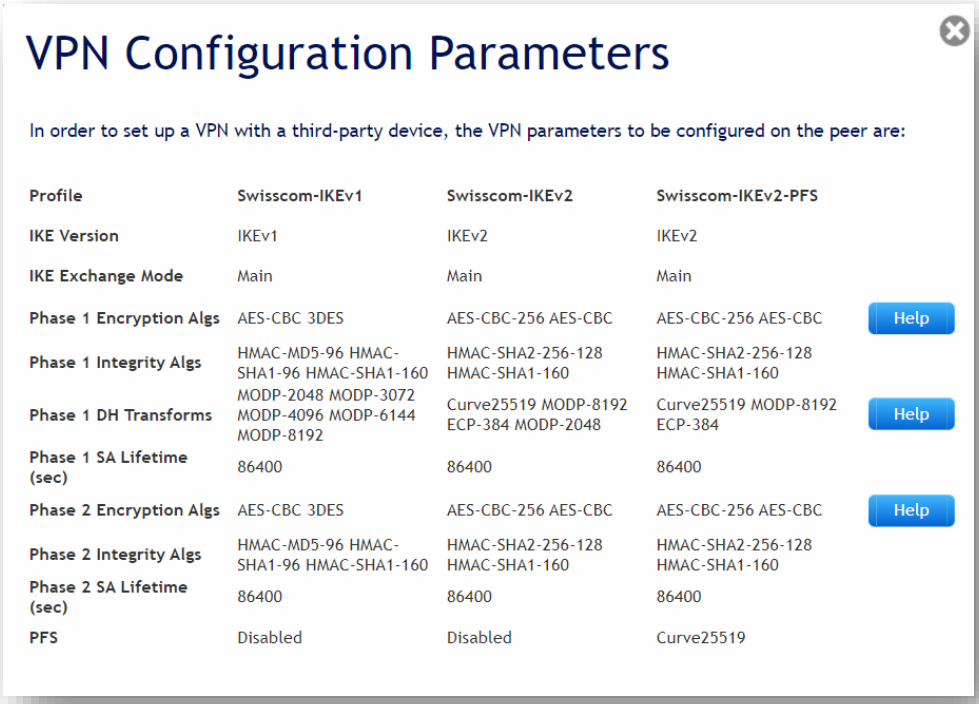
- Grey: DNS name cannot be resolved.
- Green: The tunnel is active.
- Red: The tunnel is off-line - there is no traffic or the tunnel could not be set up.

Attention! The status of the newly set up VPN tunnel is only activated when traffic runs over the connection. Therefore, please test the VPN connection with a ping.




## 1.7 Display VPN parameters

In the **Peer to Peer VPN** menu, you can see the correct parameters by pressing "Display the VPN configuration parameters" and thus enter your VPN client.



# VPN Configuration Parameters

In order to set up a VPN with a third-party device, the VPN parameters to be configured on the peer are:

| 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 | Help |
| 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 | Help |
| 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 | Help |
| 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 | Disabled | Disabled | Curve25519 | |