How to Set Up an IPsec Connection Between Two Ingate Firewalls/SIParators® (including SIP)

Lisa Hallingström

Paul Donald

Bogdan Musat

Adnan Khalid

Per Johnsson

Rickard Nilsson

Table of Contents

Ingate Firewall/SIParator® version: > 4.6.2

Document version: 1.1

How to configure Ingate Firewall/SIParator® for IPsec connections

With a VPN connection between two Firewall/SIParators or other VPN gateways, several offices can share servers and other resources without exposing the traffic openly on the Internet.

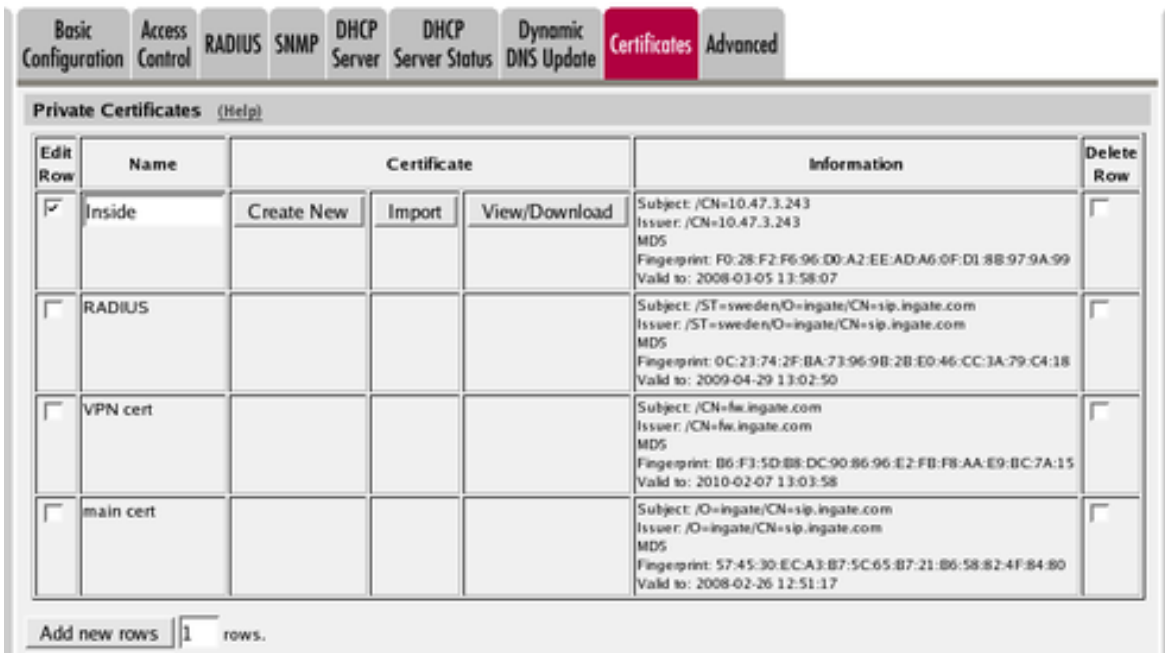
This is how to set up an IPsec VPN connection to the Firewall/SIParator.

Certificates

If the Firewall/SIParators should authenticate using X.509 certificates, the Firewall/SIParator needs a certificate of its own. All local certificates for the Firewall/SIParator are created on the **Certificates** page under **Basic Configuration**.

Make a new row in the **Private Certificates** table, press **Create new**, and fill in the form. The password fields are only relevant if you want to be able to revoke the certificate.

You can select to let the Firewall/SIParator sign its own certificate (this is the simple way) or create a certificate request and make a CA sign it for you. If you use an outside CA, the signed certificate must be uploaded to the Firewall/SIParator.



IPsec Peers

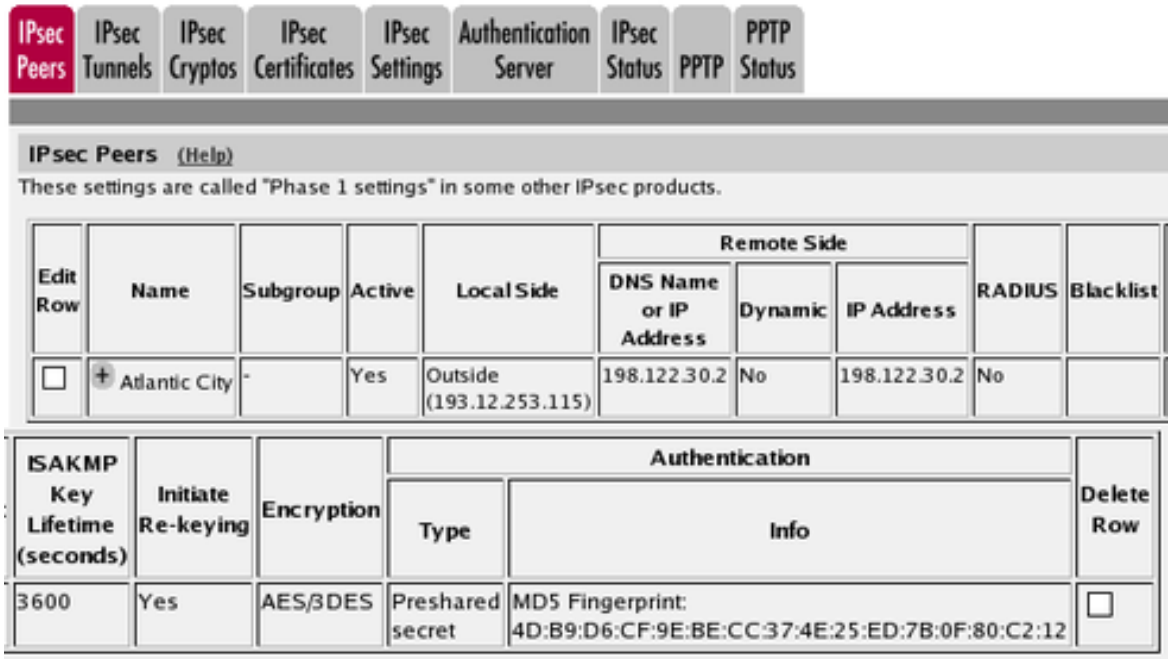
Start on the **IPsec Peers** page under **Virtual Private Networks**, where you define the IP addresses between which the VPN connection should be established. You also define how the VPN peers should authenticate themselves to each other.

Under **Authentication:Type**, select authentication with a Preshared secret or X.509 certificates. To use X.509 certificates, either both units must be able to sign their own certificates, or you must have access to a CA server which will sign certificate requests. If you have your own CA server, you can upload its certificate to the Firewall/SIParator and then trust all certificates signed by that CA (select Trusted CA).

Under **Info**, enter the secret or upload the certificate that should be used for authentication. If you use certificates, you should upload the other unit's certificate here, not the Firewall/SIParator's own one.

Under **Local side**, select a public IP address of the Firewall/SIParator, and enter a public IP address of the other VPN gateway under **Remote side**.

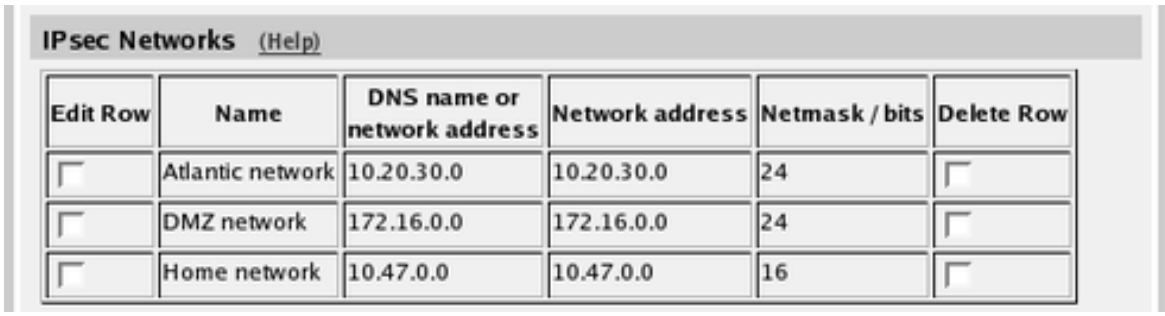
Select On under **Status**, select Off under **RADIUS**, and enter a lifetime for the ISAKMP (IKE) keys. The lifetime must be the same on both VPN peers.



IPsec Tunnels

Next, go to the **IPsec Tunnels** page and enter the networks which will use the IPsec tunnel.

In the **IPsec Networks** table, define the networks that will connect through the IPsec tunnel. You must define the local office network as well as the network behind the other Firewall/SIParator.



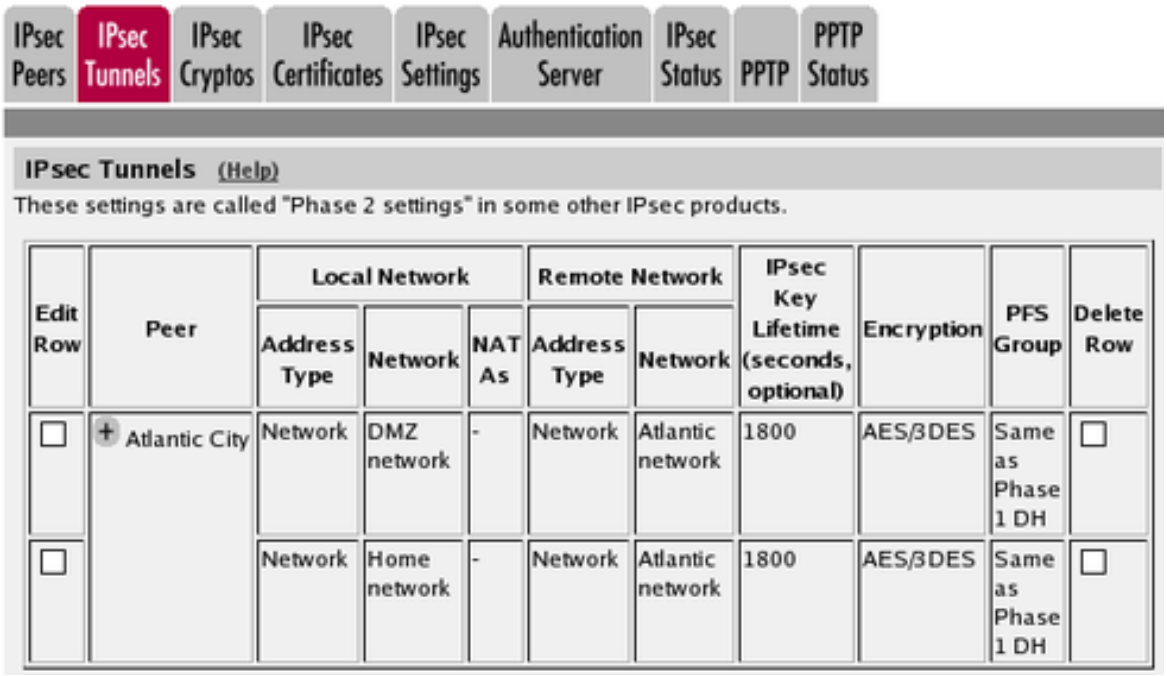
Then, create a new row in the **IPsec Tunnels** table. Under **Peer**, select the newly created VPN tunnel.

Under **Local network**, select Network as the **Address type** and the local network (connected to the Firewall/SIParator) that you defined below under **Network**.

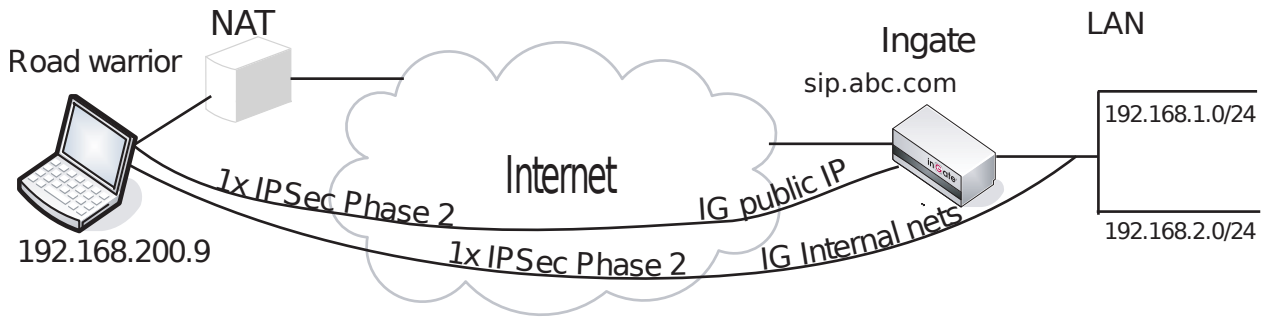
Under **Remote network**, select Network and the network defined below, which is connected to the remote Firewall/SIParator.

The IPSec key lifetime is optional, but if you enter a lifetime, it must be the same on both IPsec peers.

Select AES/3DES as encryption algorithm.



SIP through IPsec



Additionally, for SIP to work over your IPsec connections, you require a tunnel under **IPsec tunnels** between the client and the **public** IP address of the Firewall/SIParator, i.e. the Local side address under **IPsec Peers**. This requires a Phase 2 connection in the client (The Greenbow) also.

Example: if your DNS record sip.abc.com points to the WAN IP of the Firewall/SIParator then you must have a tunnel between the client and this IP address.

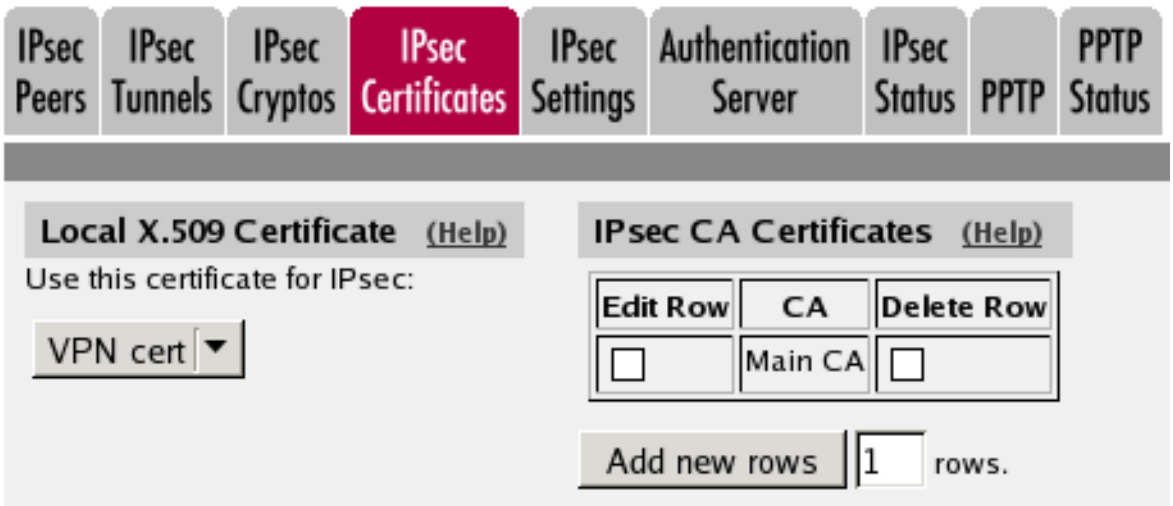
This is so that all SIP and RTP media through the b2bua or proxy is permitted.

Ensure that:

- The remote (road warrior) client also has a tunnel/Phase2 to the external IP of the Firewall/SIParator. This means "the same IP address as on the IPsec Peers page". Optionally, a tunnel to a network or subnet that includes the external IP of the Firewall/SIParator, i.e. to a DMZ range.
- The external IP (or DMZ range) of the Firewall/SIParator is a network in the **IPsec Networks** table. In the **IPsec Tunnels** table, select Network under **Address type** and select the network you just created under **IPsec Networks**.

IPsec Certificates

Go to the **IPsec Certificates** page under **Virtual Private Networks** and select which certificate the Firewall/SIParator should use for VPN connections. Also add all CA servers which have signed certificates for the VPN clients.



Networks and Computers

Go to **Networks and Computers** under **Network** to create network groups for the networks that will use the VPN tunnel. These are used for building rules for the VPN traffic.

The network on the other side of the VPN tunnel (see *Atlantic network* in the example) must have "-" selected under **Interface**.

Networks and Computers | Default Gateways | All Interfaces | NAT | VLAN | Eth0 | Eth1 | Eth2 | Eth3 | Eth4 | Eth5 | Interface Status | PPPoE

Networks and Computers

Edit Row	Name	Subgroup	Lower Limit		Upper Limit (for IP ranges)		Interface/VLAN	Delete Row
			DNS Name or IP Address	IP Address	DNS Name or IP Address	IP Address		
☐	+ All	-	0.0.0.0	0.0.0.0	255.255.255.255	255.255.255.255	-	☐
☐	+ Atlantic VPN	-	10.20.30.0	10.20.30.0	10.20.30.255	10.20.30.255	-	☐
☐	+ DHCP clients	-	10.5.1.0	10.5.1.0	10.5.1.255	10.5.1.255	DHCP clients (eth3 untagged)	☐
☐	+ DNS server	-	172.16.0.3	172.16.0.3			Ext2 (eth2 untagged)	☐
☐	+ Internet	-	0.0.0.0	0.0.0.0	255.255.255.255	255.255.255.255	External (eth1 untagged)	☐
☐	+ Office network	-	10.10.0.0	10.10.0.0	10.10.0.255	10.10.0.255	Internal (eth0 untagged)	☐
☐		-	10.47.0.0	10.47.0.0	10.47.255.255	10.47.255.255	Internal (eth0 untagged)	☐

Rules

Go to the **Rules** page and create rules to let traffic through the VPN tunnel. If there are no rules, no traffic will be let through, even if the tunnel is established.

Select the VPN tunnel under **From IPsec peer** if the **Client** network is located behind the VPN peer. Select the VPN tunnel under **To IPsec peer** if the **Server** network is located behind the VPN peer.

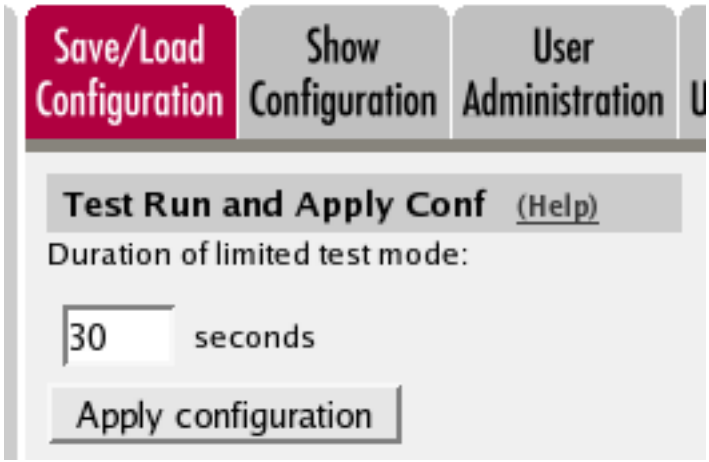
Rules | Relays | DHCP Relay | Services | Protocols | Time Classes

Rules

Edit Row	Rule No.	Active	Client	From IPsec Peer	Server	To IPsec Peer	Direction	Service	Action	Time Class	Log Class	Comment	Delete Row
☐	1	Yes	Atlantic VPN	Atlantic City	Office network	-	(VPN) -> Internal	icmp/udp/tcp	Allow	24/7	Local		☐
☐	2	Yes	Office network	-	Atlantic VPN	Atlantic City	Internal -> (VPN)	icmp/udp/tcp	Allow	24/7	Local		☐

Save/Load Configuration

Finally, go to the **Save/Load Configuration** page under **Administration** and apply the new settings by pressing **Apply configuration**.



When the configuration has been applied, you should save a backup to file. Press **Save config to CLI file** to save the configuration.