How to Set Up an IPsec Connection with RADIUS Authentication (with 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: IPSec connections with RADIUS authentication

Connections with a road warrior require X.509 certificates.

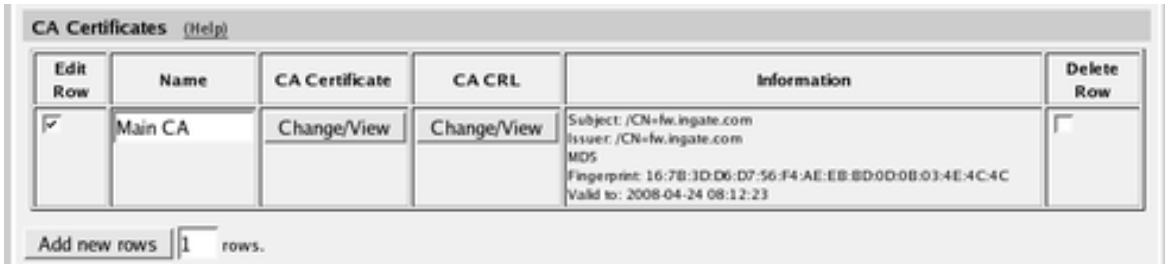
If you want to make the connection even more secure, you can require that the VPN users also authenticate to a local RADIUS server before they can use the IPsec connection.

This is how to set up an IPSec VPN connection with RADIUS authentication to the Firewall/SIParator.

Certificates

If you have many road warriors connecting to the Firewall/SIParator and you don't want to upload every client X.509 certificate separately, you can choose to trust certificates signed by a certain CA. For this, the Firewall/SIParator requires the CA certificate instead. You upload the CA certificate on the **Certificates** page.

Enter a name for the CA certificate. The name is only used internally in the Firewall/SIParator.



To authenticate itself, the Firewall/SIParator needs an X.509 certificate. This is created on the same page.

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.

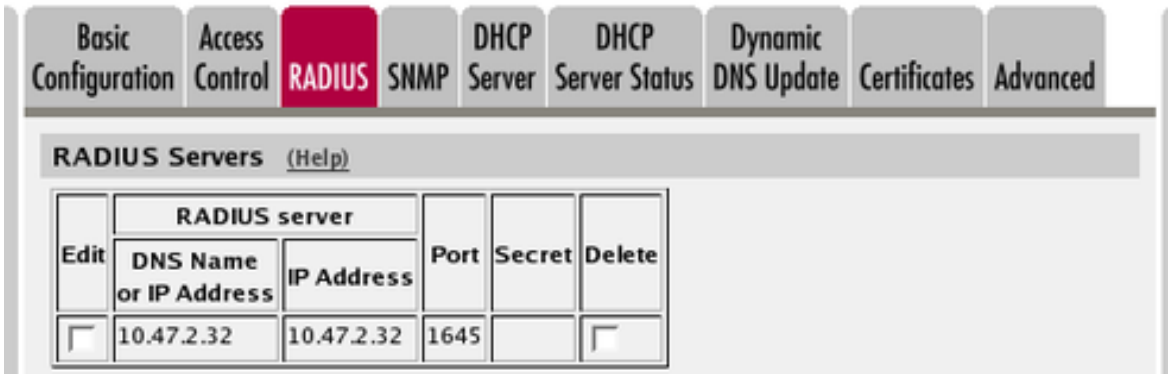
You can select to let the Firewall/SIParator sign its own certificate (this is the simple way) or create a certificate request and make a CA sign it for you. If you use an outside CA, the signed certificate must be uploaded to the Firewall/SIParator.

You have now created the certificate that should be used when the Firewall/SIParator authenticates itself to the connecting IPsec client.

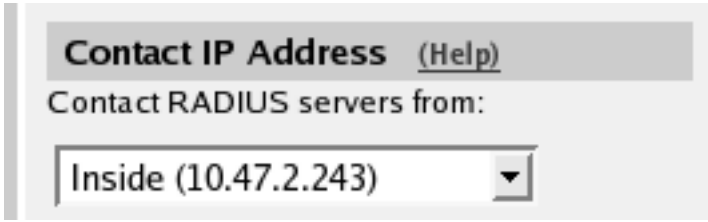
The Firewall/SIParator also needs a certificate to authenticate itself for the connecting web browser when performing the RADIUS authentication. You can use the same certificate for both purposes, or create separate certificates.

RADIUS

When RADIUS authentication is used, the Firewall/SIParator must know which RADIUS server to contact. Go to the **RADIUS** page under **Basic Configuration** and enter the RADIUS server to use.



You must also select which IP address the Firewall/SIParator should use when contacting the RADIUS server.

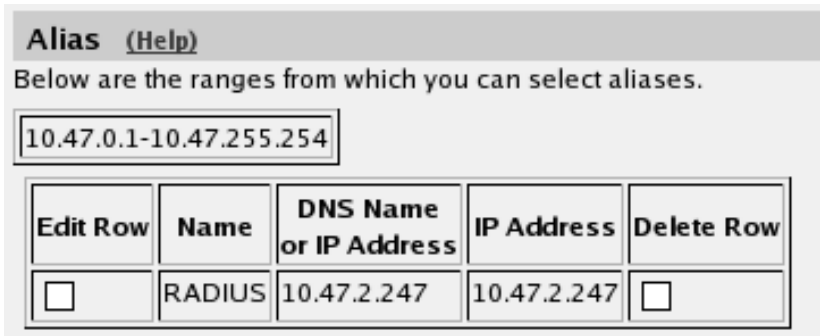


Interface

When the IPsec user wants to use the IPsec connection, she will need to connect to an IP address on the Firewall/SIParator itself, to make the RADIUS authentication. This connection is made in a web browser over https.

You must select an IP address of the Firewall/SIParator to which the user can connect. This IP address must be one that can be accessed by the user via the IPsec connection. Usually, this means that you need an IP address on the LAN.

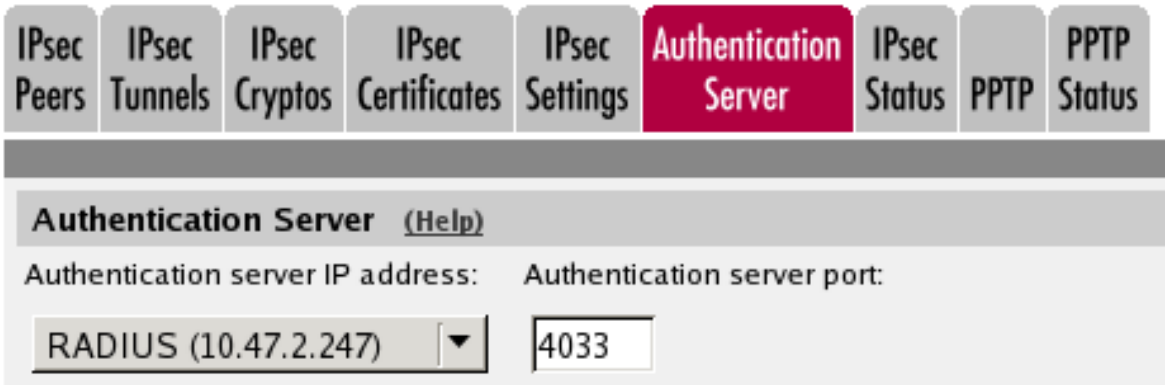
You can either use the Firewall/SIParator's main IP address (as defined in the **Directly Connected Networks** table), or create an **Alias** to use for this purpose. This is done on the **Interface** pages.



Authentication Server

If RADIUS is used to authenticate the user, the Firewall/SIParator must have an SSL certificate for its authentication server.

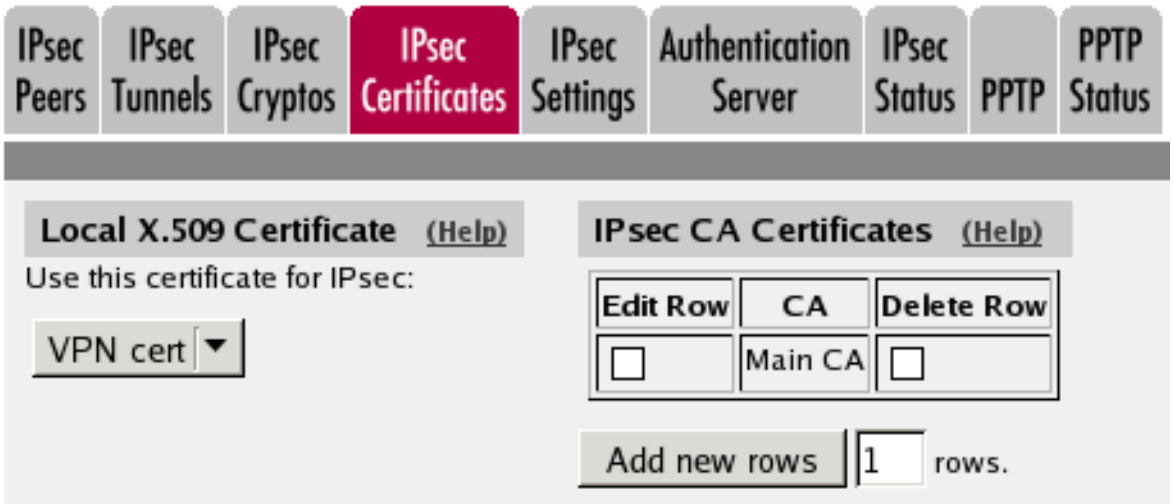
Go to the **Authentication Server** page and select a public IP address and port of the Firewall/SIParator. This is the IP address and port which the user should connect to when opening the IPsec connection.



You must also select which certificate the authentication server of the Firewall/SIParator should use to identify itself to the connecting client.

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.



IPsec Peers

Go to the **IPsec Peers** page under **Virtual Private Networks** to 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.

Select On under **Status**. Under **Authentication:Type**, select the authentication method. Road warriors must use X.509 certificates, and you can select to upload the client's certificate or trust the CA which signed the client certificate. To use X.509 certificates, you must have access to a CA server (or purchase signings) 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**, upload the client certificate or enter the CA/DN, depending on the authentication type selected above. N.B.: The X.509 certificate you upload here is the client certificate, not the Firewall/SIParator's own one.

Under **Local side**, select a public IP address of the Firewall/SIParator, and enter a "*" under **Remote side**. This means that the peer is a road warrior.

Enter a lifetime for the ISAKMP (IKE) keys. The lifetime must be the same on both VPN peers.

Select "On" under **RADIUS** to activate RADIUS authentication for this peer.

Note that when RADIUS authentication is used, the peer name must be the same as the user's RADIUS username. This means that you have to create one row per IPsec user.

IPsec Peers | IPsec Tunnels | IPsec Cryptos | IPsec Certificates | IPsec Settings | Authentication Server | IPsec Status | PPTP | PPTP Status

IPsec Peers (Help)

These settings are called "Phase 1 settings" in some other IPsec products.

Edit Row	Name	Subgroup	Active	Local Side	Remote Side			RADIUS	Blacklist
					DNS Name or IP Address	Dynamic	IP Address		
☐	+ Martin	-	Yes	Internet (193.12.253.113)	*	No	*	Yes	*

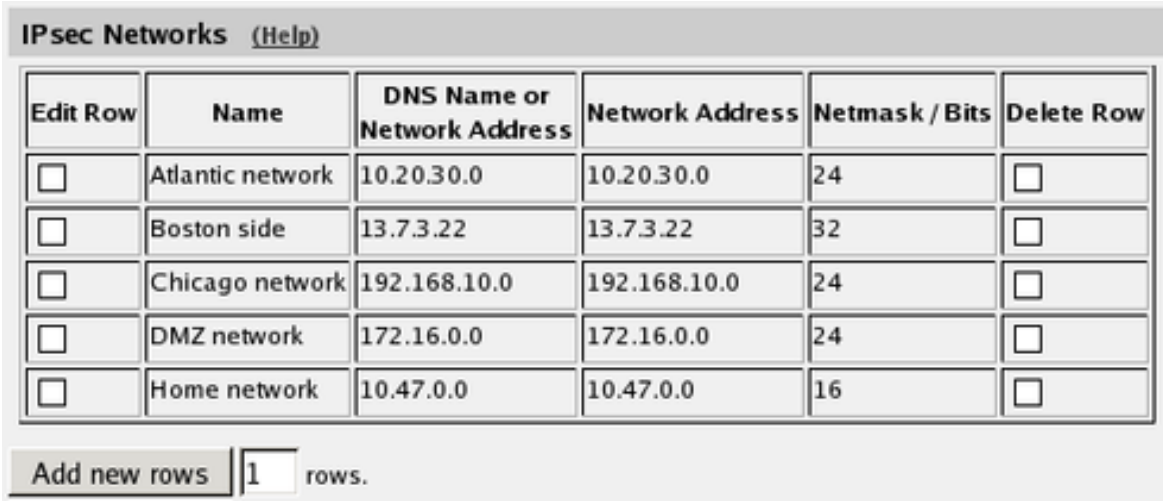
ISAKMP Key Lifetime (seconds)	Initiate Re-keying	Encryption	Authentication		Delete Row
			Type	Info	
3600	Yes	AES/3DES	Trusted CA, with DN	/CN=ingate /O=Ingate	☐

IPsec Tunnels

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

In the **IPsec Networks** table, define the local office network that will be used through the VPN tunnel.

You must also enter the IP address of the authentication server here, either as a part of the office network or as a separate network.



IPsec Networks (Help)

Edit Row	Name	DNS Name or Network Address	Network Address	Netmask / Bits	Delete Row
☐	Atlantic network	10.20.30.0	10.20.30.0	24	☐
☐	Boston side	13.7.3.22	13.7.3.22	32	☐
☐	Chicago network	192.168.10.0	192.168.10.0	24	☐
☐	DMZ network	172.16.0.0	172.16.0.0	24	☐
☐	Home network	10.47.0.0	10.47.0.0	16	☐

Add new rows 1 rows.

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 **IPsec Networks**.

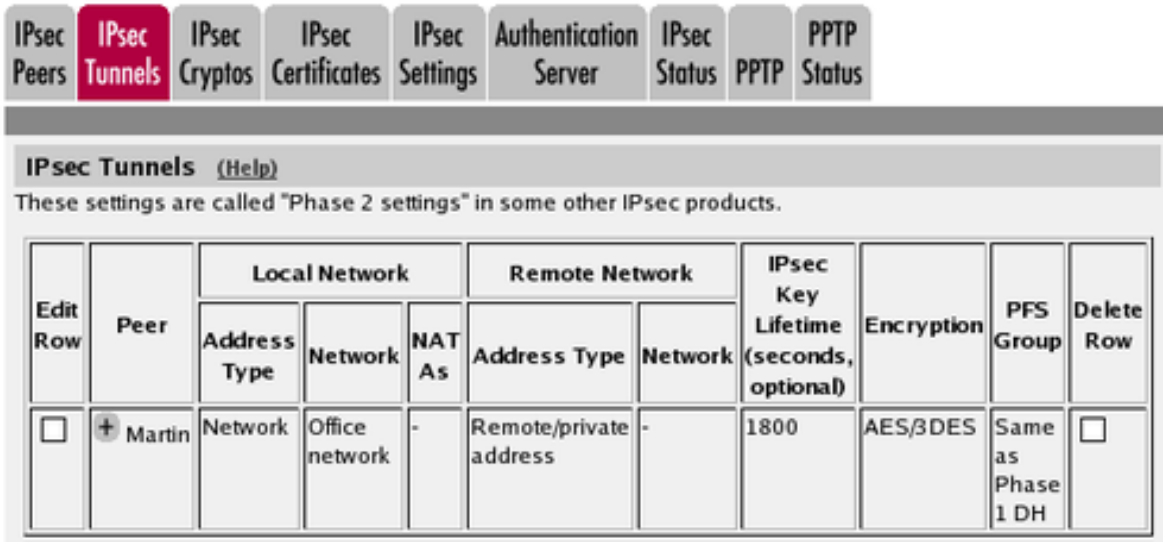
Under **Remote network**, you have the following options:

- The road warrior has a public IP address on the Internet. Select Remote side address under **Address type**. This means "the same IP address as on the IPsec Peers page".
- The road warrior is located behind a NAT:ing device, and you know which IP network it belongs to. Enter that network in the **IPsec Networks** table. In the **IPsec Tunnels** table, select Network, allow subset under **Address type** and select the network you just created under **Network**.
- Usually, you won't know the private IP address of the road warrior in advance, or it will change a lot. You might not even know if the client is NAT:ed or not.

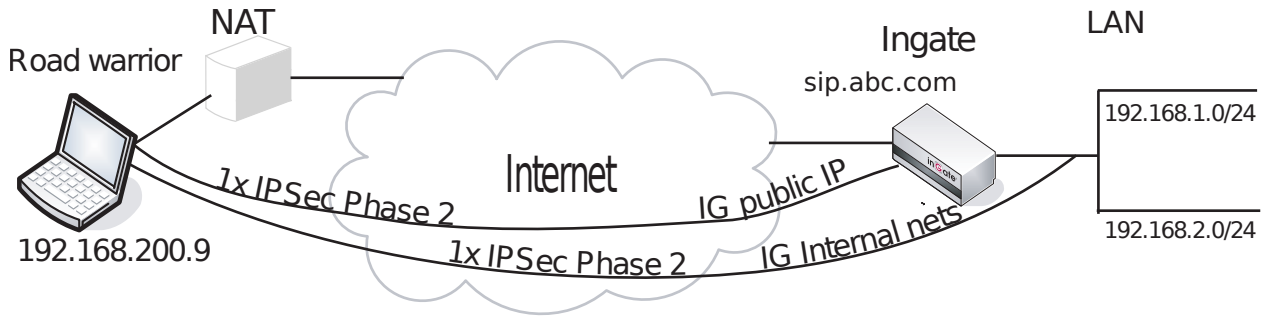
  Select Remote/private address as the **Address type**. This will allow all private IP addresses as well as the public address presented by the client at the negotiation.

When **Network** or **Network, allow subset** was selected, there must be a line for every pair of networks that should be able to communicate with each other through the VPN connection.

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



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.

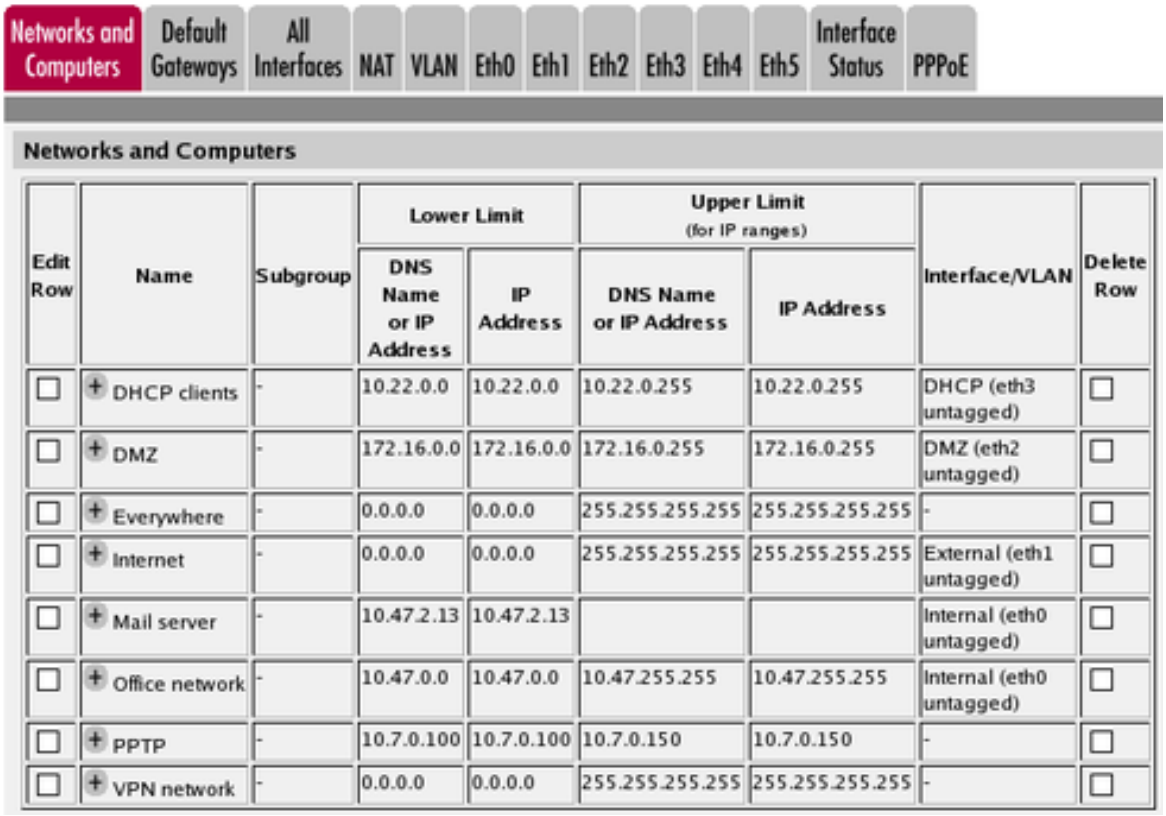
Ensure that:

- 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**.

Networks and Computers

Go to the **Networks and Computers** page under **Network** and make sure that there are groups for all networks that will use the VPN tunnel. These are used for building rules for the VPN traffic. You don't need a network for the authentication server.

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

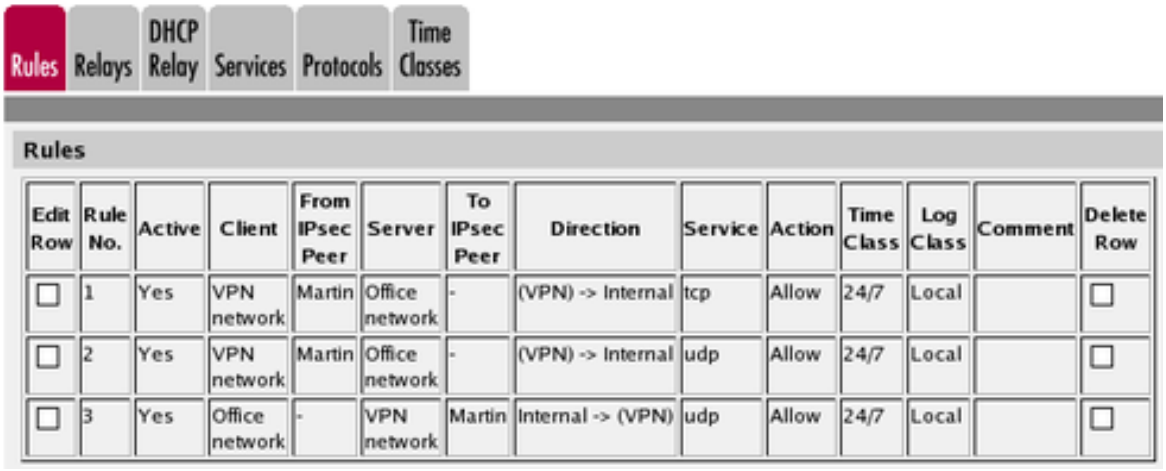


Edit Row	Name	Subgroup	Lower Limit		Upper Limit (for IP ranges)		Interface/VLAN	Delete Row
			DNS Name or IP Address	IP Address	DNS Name or IP Address	IP Address		
☐	DHCP clients	-	10.22.0.0	10.22.0.0	10.22.0.255	10.22.0.255	DHCP (eth3 untagged)	☐
☐	DMZ	-	172.16.0.0	172.16.0.0	172.16.0.255	172.16.0.255	DMZ (eth2 untagged)	☐
☐	Everywhere	-	0.0.0.0	0.0.0.0	255.255.255.255	255.255.255.255	-	☐
☐	Internet	-	0.0.0.0	0.0.0.0	255.255.255.255	255.255.255.255	External (eth1 untagged)	☐
☐	Mail server	-	10.47.2.13	10.47.2.13			Internal (eth0 untagged)	☐
☐	Office network	-	10.47.0.0	10.47.0.0	10.47.255.255	10.47.255.255	Internal (eth0 untagged)	☐
☐	PPTP	-	10.7.0.100	10.7.0.100	10.7.0.150	10.7.0.150	-	☐
☐	VPN network	-	0.0.0.0	0.0.0.0	255.255.255.255	255.255.255.255	-	☐

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.

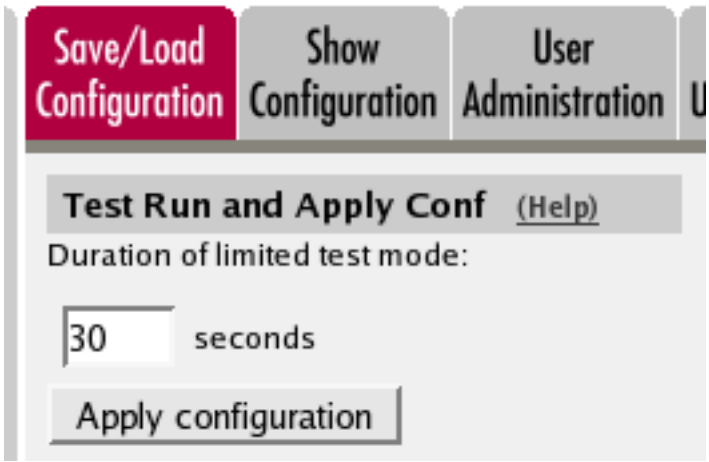
Select the VPN tunnel under **From VPN** if the **Client** network is the road warrior network. Select the VPN tunnel under **To VPN** if the **Server** network is the road warrior network.



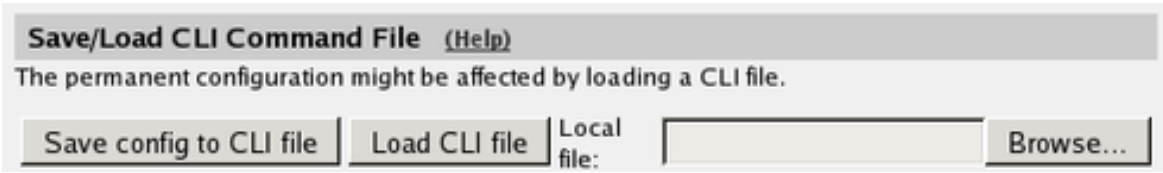
Edit Row	Rule No.	Active	Client	From IPsec Peer	Server	To IPsec Peer	Direction	Service	Action	Time Class	Log Class	Comment	Delete Row
☐	1	Yes	VPN network	Martin	Office network	-	(VPN) -> Internal	tcp	Allow	24/7	Local		☐
☐	2	Yes	VPN network	Martin	Office network	-	(VPN) -> Internal	udp	Allow	24/7	Local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



Configuring the RADIUS Server

Add the Firewall/SIParator as a client in the RADIUS server. Make sure that the shared secret here is the same as in the Firewall/SIParator.

The Firewall/SIParator checks the permissions for a user by looking at its RADIUS attribute *Service-Type*.

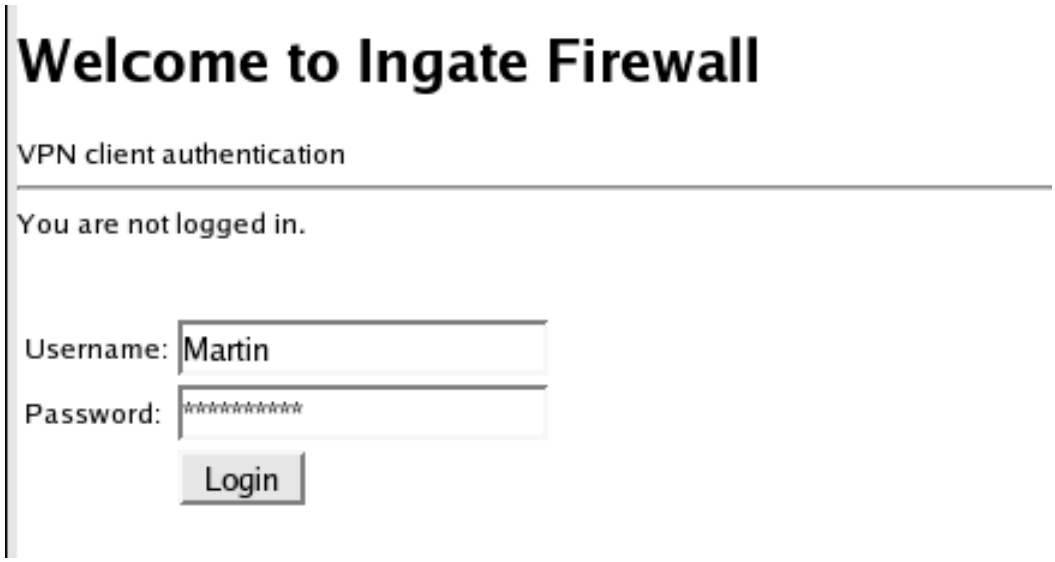
If the value is *Framed (2)*, the user is allowed to connect via VPN.

Configuring the Client

The road warrior itself must also be configured. The exact moves for this is of course dependant of what client software you use. See http://www.ingate.com/Interaction.php for configuration instructions for several VPN clients.

When the user wants to use the IPsec connection, she starts with directing her web browser to the IP address selected under **Authentication Server**. Note that https must be used!

This will present a RADIUS login page where the user enters her RADIUS username and password/PIN code.



When the username and password/PIN code has been verified by the RADIUS server, the connection is set up for the user.