

Configuration Aid To Ingate Firewall/SIParator - How to Set Up an IPsec Connection Between Two Ingate Firewalls/SIParators

Lisa Hallingström
Ingate Systems AB



Table of Contents

How to configure Ingate Firewall/SIParator for IPsec connections	3
Certificates	3
IPsec Peers	3
IPsec Tunnels	4
X.509 Certificates	5
Networks and Computers.....	5
Rules	6
Save/Load Configuration	6

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.

Edit Row	Name	Certificate			Information	Delete Row
<input checked="" type="checkbox"/>	Inside	Create New	Import	View/Download	Subject: /CN=10.47.3.243 Issuer: /CN=10.47.3.243 MD5 Fingerprint: F0:28:F2:F6:96:D0:A2:EE:AD:A6:0F:D1:8B:97:9A:99 Valid to: 2008-03-05 13:58:07	<input type="checkbox"/>
<input type="checkbox"/>	RADIUS				Subject: /ST=sweden/O=ingate/CN=sip.ingate.com Issuer: /ST=sweden/O=ingate/CN=sip.ingate.com MD5 Fingerprint: 0C:23:74:2F:BA:73:96:9B:2B:E0:46:CC:3A:79:C4:18 Valid to: 2009-04-29 13:02:50	<input type="checkbox"/>
<input type="checkbox"/>	VPN cert				Subject: /CN=fw.ingate.com Issuer: /CN=fw.ingate.com MD5 Fingerprint: B6:F3:5D:B8:DC:90:86:96:E2:FB:F8:AA:E9:BC:7A:15 Valid to: 2010-02-07 13:03:58	<input type="checkbox"/>
<input type="checkbox"/>	main cert				Subject: /O=ingate/CN=sip.ingate.com Issuer: /O=ingate/CN=sip.ingate.com MD5 Fingerprint: 57:45:30:EC:A3:B7:5C:65:B7:21:B6:58:82:4F:84:80 Valid to: 2008-02-26 12:51:17	<input type="checkbox"/>

Add new rows rows.

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.

*Configuration Aid To Ingate Firewall/SIParator - How to Set Up an IPsec Connection
Between Two Ingate Firewalls/SIParators*

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 Peers

Please define the tunnels between this Ingate Firewall and the remote IPsec peers.
For a Road Warrior setup, where the IP address of the remote IPsec peer isn't known or may vary, please enter "*" as the remote side IP address.

Edit Row	Name	Subgroup	Status	Local side	Remote side			RADIUS	Blacklist	ISAKMP key lifetime (seconds)
					DNS name or IP address	Dynamic	IP address			
<input type="checkbox"/>	Atlantic City		On	Outside (193.12.253.115)	198.122.30.2		198.122.30.2	Off		3600

Authentication		Delete Row
Type	Info	
Preshared secret	MD5 Fingerprint: 4D:B9:D6:CF:9E:BE:CC:37:4E:25:ED:7B:0F:80:C2:12	<input type="checkbox"/>

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 networks that will connect through the VPN tunnel. You must define the local office network as well as the network behind the other firewall/SIParator.

IPsec Networks (Help)

Edit Row	Name	DNS name or network address	Network address	Netmask / bits	Delete Row
<input type="checkbox"/>	Atlantic network	10.20.30.0	10.20.30.0	24	<input type="checkbox"/>
<input type="checkbox"/>	DMZ network	172.16.0.0	172.16.0.0	24	<input type="checkbox"/>
<input type="checkbox"/>	Home network	10.47.0.0	10.47.0.0	16	<input type="checkbox"/>

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.

Edit Row	Peer	Local network			Remote network		IPsec key lifetime (seconds, optional)	Encryption	Delete Row
		Address type	Network	NAT as	Address type	Network			
<input type="checkbox"/>	+ Atlantic City	Network	DMZ network	-	Network	Atlantic network	1800	AES/3DES	<input type="checkbox"/>
<input type="checkbox"/>		Network	Home network	-	Network	Atlantic network	1800	AES/3DES	<input type="checkbox"/>

X.509 Certificates

Go to the **X.509 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.

Local X.509 Certificate [\(Help\)](#)
Use this certificate for IPsec:

CA Certificates [\(Help\)](#)
Certificates are not used for PPTP.

Edit row	CA	Delete row
<input type="checkbox"/>	Main CA	<input type="checkbox"/>

Add new rows rows.

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									
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			
<input type="checkbox"/>	+ All	-	0.0.0.0	0.0.0.0	255.255.255.255	255.255.255.255	-	<input type="checkbox"/>	
<input type="checkbox"/>	+ Atlantic VPN	-	10.20.30.0	10.20.30.0	10.20.30.255	10.20.30.255	-	<input type="checkbox"/>	
<input type="checkbox"/>	+ DHCP clients	-	10.5.1.0	10.5.1.0	10.5.1.255	10.5.1.255	DHCP clients (eth3 untagged)	<input type="checkbox"/>	
<input type="checkbox"/>	+ DNS server	-	172.16.0.3	172.16.0.3			Ext2 (eth2 untagged)	<input type="checkbox"/>	
<input type="checkbox"/>	+ Internet	-	0.0.0.0	0.0.0.0	255.255.255.255	255.255.255.255	External (eth1 untagged)	<input type="checkbox"/>	
<input type="checkbox"/>	+ Office network	-	10.47.0.0	10.47.0.0	10.47.255.255	10.47.255.255	Internal (eth0 untagged)	<input type="checkbox"/>	
<input type="checkbox"/>		-	10.10.0.0	10.10.0.0	10.10.0.255	10.10.0.255	Internal (eth0 untagged)	<input type="checkbox"/>	

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.

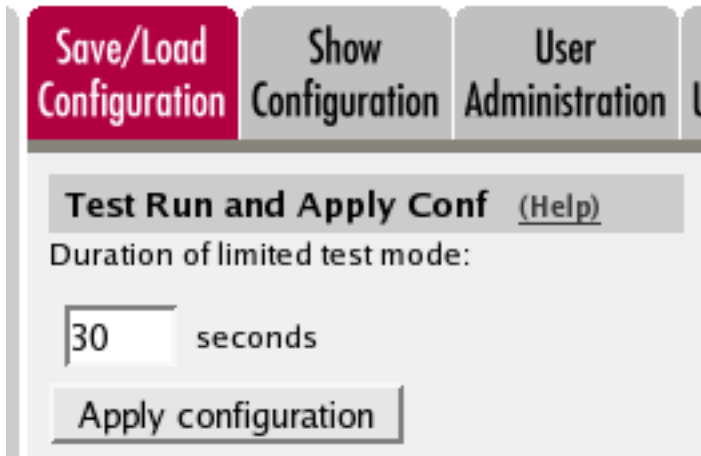
Select the VPN tunnel under **From IPsec peer** if the **Client** network is located behind the VPN peer. Select the VPN tunnel under **To IPsec peer** if the **Server** network is located behind the VPN peer.

Rules													
Edit Row	Rule no.	Rule State	Client	From IPsec peer	Server	To IPsec peer	Direction	Service	Action	Time class	Log class	Comment	Delete Row
<input type="checkbox"/>	1	On	Atlantic VPN	Atlantic City	Office network	-	(VPN) -> Internal	icmp/udp/tcp	Allow	24/7	Local		<input type="checkbox"/>
<input type="checkbox"/>	2	On	Office network	-	Atlantic VPN	Atlantic City	Internal -> (VPN)	icmp/udp/tcp	Allow	24/7	Local		<input type="checkbox"/>

Save/Load Configuration

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

*Configuration Aid To Ingate Firewall/SIParator - How to Set Up an IPsec Connection
Between Two Ingate Firewalls/SIParators*



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

