How to Set Up an IPsec Connection with NAT (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 configure Ingate Firewall/SIParator® for IPsec connections with NAT

You might want to NAT the traffic through an IPsec tunnel. A reason for wanting this could be that the networks on each side of the tunnel clash, thus making routing decisions tricky.

In this example we assume that computers on one side (client side) wants to contact servers on the other side of the tunnel (server side). The configuration needed for this is presented here.

NB! If the IPsec peer is not an Ingate unit, some settings might differ from what is shown here. The primary setting which will not look the same is which networks are involved in the IPsec negotiation. The local networks (sharing the same IP interval) will never be used in the negotiation; only the IP addresses used to NAT the traffic.

Client Side

On the client side, the IPsec connection must be defined, and rules to allow traffic going through the tunnel to the server side.

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 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		
☐	+ Boston	-	Yes	Outside (193.12.253.115)	13.7.3.22	No	13.7.3.22	No	

ISAKMP Key Lifetime (seconds)	Initiate Re-keying	Encryption	Authentication		Delete Row
			Type	Info	
3600	Yes	AES/3DES	Preshared secret	MD5 Fingerprint: C9:97:87:1F:9E:BF:7C:38:BE:25:85:D6:04:84:2F:F6	☐

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 IP address or addresses used by the IPsec peer for NATing traffic for its local network.

As the two networks clash, you can't define the remote network directly here. Instead, the local computers need to contact an IP address on the peer outside. The peer then forwards the traffic to the server.

IPsec Networks (Help)

Edit Row	Name	DNS name or network address	Network address	Netmask / bits	Delete Row
☐	Boston side	13.7.3.22	13.7.3.22	32	☐
☐	Home network	10.47.0.0	10.47.0.0	16	☐

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

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 consists of the IP address(es) connected to the remote Firewall/SIParator.
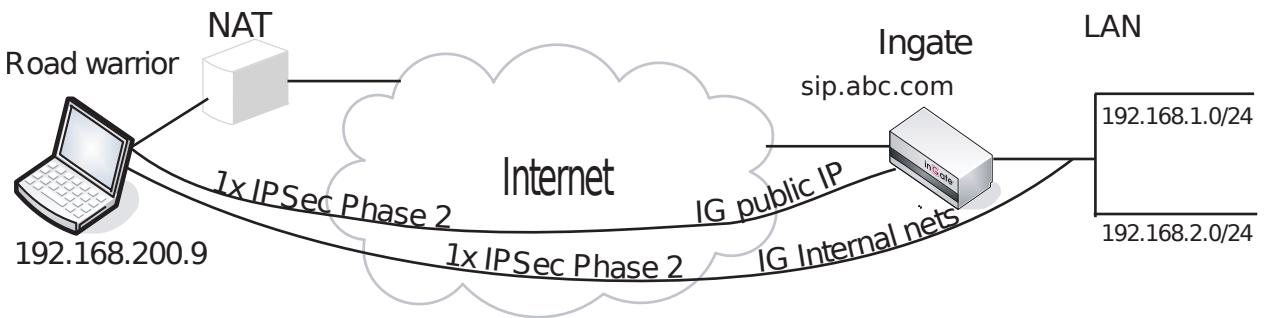
Select to NAT as the outside IP address (the one selected on the **IPsec Peers** page.

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.

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

IPsec Tunnels (Help)

These settings are called "Phase 2 settings" in some other IPsec products.

Edit Row	Peer	Local Network			Remote Network		IPsec Key Lifetime (seconds, optional)	Encryption	PFS Group	Delete Row
		Address Type	Network	NAT As	Address Type	Network				
☐	+ Boston	Network	Home network	Outside (193.12.253.115)	Network	Boston side	1800	AES/3DES	Same as Phase 1 DH	☐

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

The network on the server side of the IPsec tunnel must consist of the IP address(es) that are used to NAT the traffic on that side. This network must have "-" selected under **Interface/VLAN**.

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		
☐	⊞ Boston VPN endpoint	-	13.7.3.22	13.7.3.22			-	☐
☐	⊞ Internet	-	0.0.0.0	0.0.0.0	255.255.255.255	255.255.255.255	External (eth1 untagged)	☐
☐	⊞ Office network	-	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 IPsec tunnel. If there are no rules, no traffic will be let through, even if the tunnel is established.

Select the local network under **Client**. Select the IPsec peer under **To IPsec peer** and the peer's network under **Server**. Create rules like this for the services that should be allowed to the server side.

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	Office network	-	Boston VPN endpoint	Boston	Internal -> (VPN)	www	Allow	24/7	Local		☐
☐	2	Yes	Office network	-	Boston VPN endpoint	Boston	Internal -> (VPN)	ftp	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**.
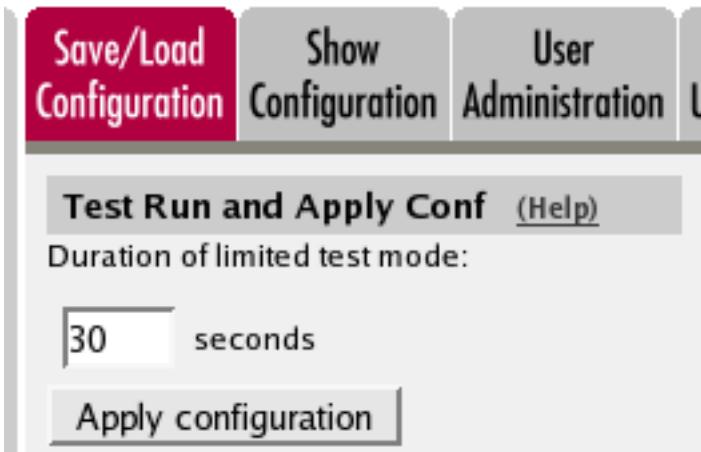
When the configuration has been applied, you should save a backup to file. Press **Save config to CLI file** to save the configuration.
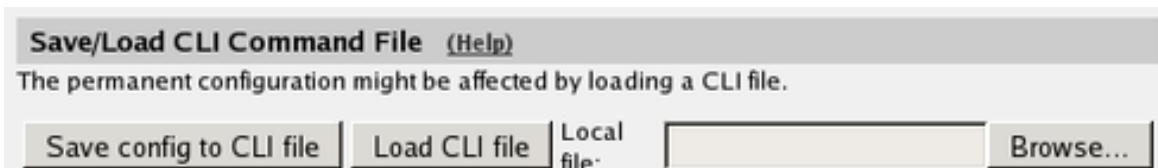
Server Side

On the server side, the IPsec connection must be defined, and relays to forward the received traffic to the servers on the inside.

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 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		
☐	+ Seattle	-	Yes	Outside (13.7.3.22)	193.12.253.115	No	193.12.253.115	No	

ISAKMP Key Lifetime (seconds)	Initiate Re-keying	Encryption	Authentication		Delete Row
			Type	Info	
3600	Yes	AES/3DES	Preshared secret	MD5 Fingerprint: C9:97:87:1F:9E:BF:7C:38:BE:25:85:D6:04:84:2F:F6	☐

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 IP address or addresses used by the IPsec peer for NATing traffic from its local network.

As the two networks clash, you can't define the remote network directly here. Instead, use the IP address from which the traffic seems to be sent.

IPsec Networks (Help)

Edit Row	Name	DNS name or network address	Network address	Netmask / bits	Delete Row
☐	Home network	10.47.0.0	10.47.0.0	16	☐
☐	Seattle side	193.12.253.115	193.12.253.115	32	☐

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

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 consists of the IP address(es) connected to the remote Firewall/SIParator.
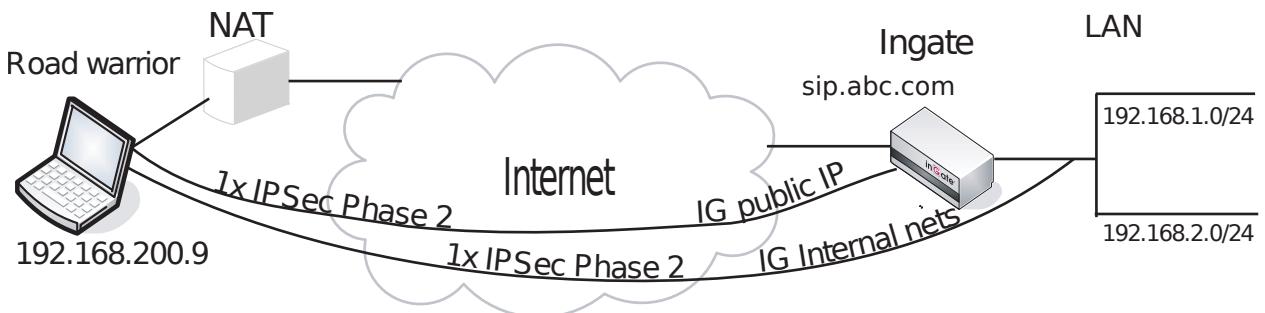
Select to NAT as the outside IP address (the one selected on the **IPsec Peers** page.

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	PFS Group	Delete Row
		Address Type	Network	NAT As	Address Type	Network				
☐	+ Seattle	Network	Home network	Outside (13.7.3.22)	Network	Seattle side		AES/3DES	Same as Phase 1 DH	☐

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 **Networks and Computers** under **Network** to create a network group for the remote network that will use the IPsec tunnel. This will be used to define which computers can use the relay that will forward traffic to the inside servers.

The network on the client side of the IPsec tunnel must consist of the IP address(es) that are used to NAT the traffic on that side. This network must have "-" selected under **Interface/VLAN**.

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		
☐	⊞ Internet	-	0.0.0.0	0.0.0.0	255.255.255.255	255.255.255.255	External (eth1 untagged)	☐
☐	⊞ Office network	-	10.47.0.0	10.47.0.0	10.47.255.255	10.47.255.255	Internal (eth0 untagged)	☐
☐	⊞ Seattle VPN endpoint	-	193.12.253.115	193.12.253.115			-	☐

Relays

Go to the **Relays** page and create relays to forward traffic from the IPsec tunnel to the inside servers.

Select to Listen to an IP address on the outside. This IP address must be listed among the IP addresses for which the client side makes the IPsec negotiation.

Enter the IP address and port for the server under **Relay to** and select the appropriate relay type. Select the IPsec peer under **IPsec peer** and the client network under **Network**.

Rules	Relays	DHCP Relay	Services	Protocols	Time Classes

Relays

Edit Row	Listen to ...		Relay to ...			Relay type	Allow access from ...		Time class	Log class	Delete Row
	IP address	Port	DNS name or IP address	IP address	Port		Network	IPsec peer			
☐	Outside (13.7.3.22)	80	10.47.4.38	10.47.4.38	80	TCP relay	Seattle VPN endpoint	Seattle	24/7	Local	☐
☐	Outside (13.7.3.22)	21	10.47.4.75	10.47.4.75	21	FTP relay	Seattle VPN endpoint	Seattle	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**.
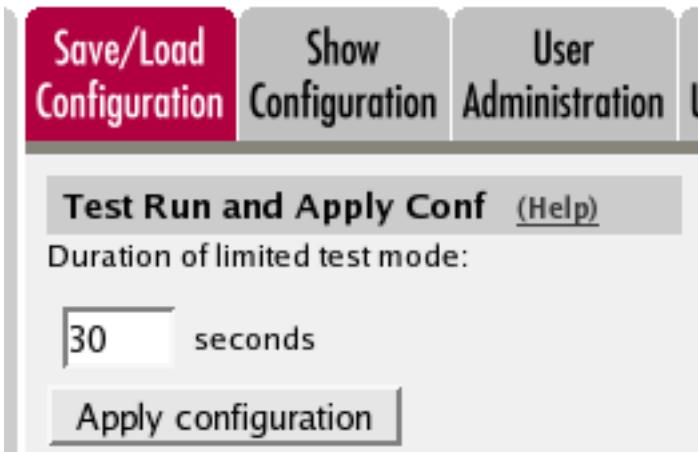
When the configuration has been applied, you should save a backup to file. Press **Save config to CLI file** to save the configuration.
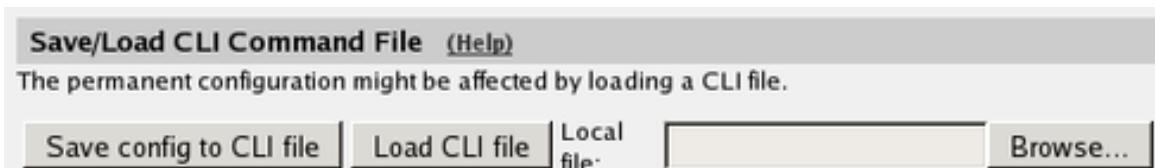
IPsec Connection With NAT, Client Side has a Dynamic IP Address

You might want to NAT the traffic through an IPsec tunnel. A reason for wanting this could be that the networks on each side of the tunnel clash, thus making routing decisions tricky.

In this example we assume that computers on one side (client side) wants to contact servers on the other side of the tunnel (server side), and that the IPsec peer of the client side has a dynamic IP address. The configuration needed for this is presented here.

NB! If the IPsec peer is not an Ingate unit, some settings might differ from what is shown here. The primary setting which will not look the same is which networks are involved in the IPsec negotiation. The local networks (sharing the same IP interval) will never be used in the negotiation; only the IP addresses used to NAT the traffic.

Client Side

On the client side, the IPsec connection must be defined, and rules to allow traffic going through the tunnel to the server side.

Certificates

As one of the IPsec peers has a dynamic IP address, the IPsec authentication must be performed with X.509 certificates. Create a certificate on the **Certificates** page.

Add a new row to the **Private Certificates** table and enter a name for this certificate. Press **Create new**.

Enter information about the Firewall/SIParator in the form, and press **Create a self-signed X.509 certificate**.

When the certificate has been created, download it as a PEM or DER certificate. This certificate should then be uploaded on the **IPsec Peers** page of the other unit.

IPsec Certificates

Go to **IPsec Certificates** under **Virtual Private Networks** and select that the Firewall/SIParator should use the newly created certificate for IPsec negotiations.

IPsec Peers

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

Under **Authentication:Type**, select X.509 certificates.

Under **Info**, upload the *other* unit's certificate.

Under **Local side**, select the interface with the dynamic IP address, and enter a public IP address of the other IPsec 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 IPsec peers.

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		
☐	⊕ Main office	-	Yes	Internet (eth1)	88.131.69.205	No	88.131.69.205	No	

ISAKMP Key Lifetime (seconds)	Initiate Re-keying	Encryption	Authentication		Delete Row
			Type	Info	
3600	Yes	AES/3DES	X.509 certificate	Subject: /CN=vpn.ingate.com Issuer: /CN=vpn.ingate.com MD5 Fingerprint: A1:D7:A3:07:43:6C:07:7D:F0:C6:61:7A:CA:88:48:C9 Valid to: 2009-07-24 11:47:47	☐

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 IP address or addresses used by the IPsec peer for NATing traffic for its local network.

As the two networks clash, you can't define the remote network directly here. Instead, the local computers need to contact an IP address on the peer outside. The peer then forwards the traffic to the server.

IPsec Networks (Help)

Edit	Name	DNS Name or Network Address	Network Address	Netmask / Bits	Delete
☐	LAN	192.168.0.0	192.168.0.0	24	☐
☐	Remote side	88.131.69.205	88.131.69.205	32	☐

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

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 consists of the IP address(es) connected to the remote Firewall/SIParator.

Select to NAT as the outside IP address (the one selected on the **IPsec Peers** page.

The IPSec key lifetime is optional, but if you enter a lifetime, it must be the same on both IPsec peers.
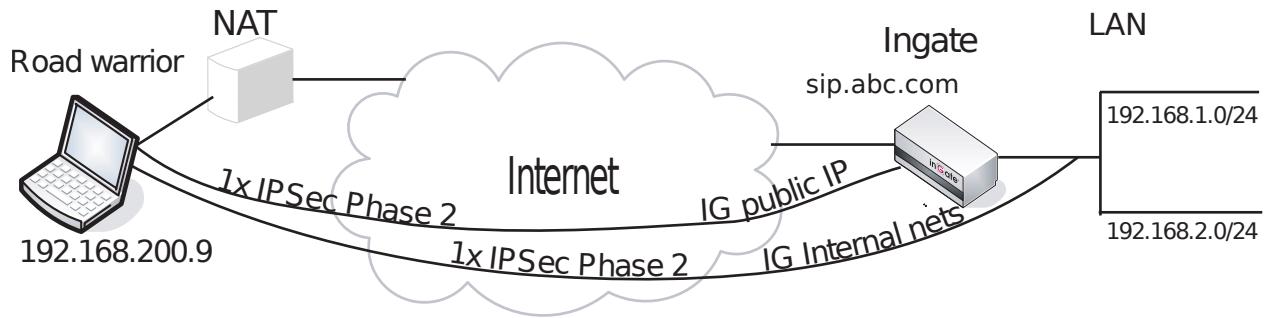
Select AES/3DES as encryption algorithm.

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

IPsec Tunnels (Help)

These settings are called "Phase 2 settings" in some other IPsec products.

Edit Row	Peer	Local Network			Remote Network		IPsec Key Lifetime (seconds, optional)	Encryption	PFS Group	Delete Row
		Address Type	Network	NAT As	Address Type	Network				
☐	+ Main office	Network	LAN	Internet (eth1)	Network	Remote side		AES/3DES	Same as Phase 1 DH	☐

14

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

The network on the server side of the IPsec tunnel must consist of the IP address(es) that are used to NAT the traffic on that side. This network must have "-" selected under **Interface/VLAN**.

			Lower Limit		Upper Limit (for IP ranges)			
Edit Row	Name	Subgroup	DNS Name or IP Address	IP Address	DNS Name or IP Address	IP Address	Interface/VLAN	Delete Row
☐	⊞ LAN	-	192.168.0.0	192.168.0.0	192.168.0.255	192.168.0.255	Ethernet2 (eth2 untagged)	☐
☐	⊞ Remote VPN	-	88.131.69.205	88.131.69.205			-	☐

Rules

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

Select the local network under **Client**. Select the IPsec peer under **To IPsec peer** and the peer's network under **Server**. Create rules like this for the services that should be allowed to the server side.

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	LAN	-	Remote VPN	Main office	Ethernet2 -> (VPN)	pop3	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.

Server Side

On the server side, the IPsec connection must be defined, and relays to forward the received traffic to the servers on the inside.

Certificates

As one of the IPsec peers has a dynamic IP address, the IPsec authentication must be performed with X.509 certificates. Create a certificate on the **Certificates** page.

Add a new row to the **Private Certificates** table and enter a name for this certificate. Press **Create new**.

Enter information about the Firewall/SIParator in the form, and press **Create a self-signed X.509 certificate**.

When the certificate has been created, download it as a PEM or DER certificate. This certificate should then be uploaded on the **IPsec Peers** page of the other unit.

IPsec Certificates

Go to **IPsec Certificates** under **Virtual Private Networks** and select that the Firewall/SIParator should use the newly created certificate for IPsec negotiations.

IPsec Peers

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

Under **Authentication:Type**, select X.509 certificates.

Under **Info**, upload the *other* unit's certificate.

Under **Local side**, select the interface with the public IP address. Under **Remote side**, enter '*', which means that the peer has a dynamic IP address..

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 IPsec peers.

IPsec Tunnels

On the **IPsec Tunnels** page, create a new row in the **IPsec Tunnels** table. Under **Peer**, select the newly created IPsec peer.

Under **Local network**, select Local side address as the **Address type**.

Under **Remote network**, select Remote side address.

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.

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

IPsec Tunnels   (Help)

These settings are called "Phase 2 settings" in some other IPsec products.

Edit Row	Peer	Local Network			Remote Network		IPsec Key Lifetime (seconds, optional)	Encryption	PFS Group	Delete Row
		Address Type	Network	NAT As	Address Type	Network				
☐	⊞ Branch office	Local side address	-	-	Remote side address	-		AES/3DES	Same as Phase 1 DH	☐

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 **Networks and Computers** under **Network** to create a network group for the remote network that will use the VPN tunnel. This will be used to define which computers can use the relay that will forward traffic to the inside servers.

The network on the client side of the VPN tunnel must consist of the IP address that is used to NAT the traffic on that side. As this IP address is dynamic, all IP addresses need to be included in the network.

Select "-" under **Interface/VLAN**.

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	-	☐

Relays

Go to the **Relays** page and create relays to forward traffic from the IPsec tunnel to the inside servers.

Select to Listen to an IP address on the outside. This IP address must be listed among the IP addresses for which the client side makes the IPsec negotiation.

Enter the IP address and port for the server under **Relay to** and select the appropriate relay type. Select the IPsec peer under **IPsec peer** and the client network under **Network**.

Edit	Listen To ...		Relay To ...			Relay Type	Allow Access From ...		Certificate for TLS/SSL	Time Class	Log Class	Delete
	IP Address	Port	DNS Name or IP Address	IP Address	Port		Network	IPsec Peer				
☐	Internet (88.131.69.205)	110	192.168.0.33	192.168.0.33	110	TCP port forwarding	All	Branch office	-	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.

IPsec Connection With NAT, Server Side has a Dynamic IP Address

You might want to NAT the traffic through an IPsec tunnel. A reason for wanting this could be that the networks on each side of the tunnel clash, thus making routing decisions tricky.

In this example we assume that computers on one side (client side) wants to contact servers on the other side of the tunnel (server side), and that the IPsec peer of the server side has a dynamic IP address. The configuration needed for this is presented here.

NB! If the IPsec peer is not an Ingate unit, some settings might differ from what is shown here. The primary setting which will not look the same is which networks are involved in the IPsec negotiation. The local networks (sharing the same IP interval) will never be used in the negotiation; instead the IP addresses used to NAT the traffic are used.

Server Side

On the server side, the IPsec connection must be defined, and relays to forward the received traffic to the servers on the inside.

As the server side has a dynamic public IP address, it is not possible to make the client side use this address when contacting servers. Instead, you need to set up an extra IP network on the inside, just for forwarding traffic to the inside servers.

In this example, the common network for both sides is 192.168.0.0/24, and the extra IP network on the server side is 172.16.20.0/24.

Interface

Go to **Interface** and create a new network for the traffic forwarding in the **Directly Connected Networks** table.

Directly Connected Networks (Help)

Edit Row	Name	Address Type	DNS Name or IP Address	IP Address	Netmask / Bits	Network Address	Broadcast Address	VLAN Id	VLAN Name	Delete Row
☐	LAN	Static	192.168.0.1	192.168.0.1	24	192.168.0.0	192.168.0.255		-	☐
☐	Relay Net	Static	172.16.20.1	172.16.20.1	24	172.16.20.0	172.16.20.255		-	☐

In the **Alias** table, add alias IP addresses for the server that should be reachable over the IPsec connection.

Alias (Help)

Below are the ranges from which you can select aliases.

172.16.20.1-172.16.20.254

192.168.0.1-192.168.0.254

Edit Row	Name	DNS Name or IP Address	IP Address	Delete Row
☐	FTP Server	172.16.20.34	172.16.20.34	☐
☐	pop3 Server	172.16.20.33	172.16.20.33	☐

Certificates

As one of the IPsec peers has a dynamic IP address, the IPsec authentication must be performed with X.509 certificates. Create a certificate on the **Certificates** page.

Add a new row to the **Private Certificates** table and enter a name for this certificate. Press **Create new**.

Private Certificates _(Help)_					
Name	**Certificate**			**Information**	**Delete**
VPN cert	Create New	Import	View/Download	Subject: /CN=home.ingate.com Issuer: /CN=home.ingate.com MD5 Fingerprint: CD:6F:19:99:1C:4E:3C:94:C0:9B:F8:37:AD:5B:41:E0 Valid to: 2009-07-24 11:53:57	☐

Enter information about the Firewall/SIParator in the form, and press **Create a self-signed X.509 certificate**.

Create Certificate or Certificate Request

Fill in the certificate data for "**VPN cert**" below, then create either a certificate or a certificate request.

After generating a certificate request, and having it signed by a signing authority, the certificate must be imported to the firewall.

Expire in (days): * 365
Country code (C):
Organization (O):

Common Name (CN): * ome.ingate.com
State/province (ST):
Organizational Unit (OU):

Email address
Locality/town (L):

If you generate several certificates with identical data you should make sure they have different serial numbers.

Serial number: * 0

Below you can enter an optional challenge password for certificate requests.

Challenge password:
Challenge password again:

Fields marked with "*" are mandatory.

[Create a self-signed X.509 certificate] [Create an X.509 certificate request] [Abort]

When the certificate has been created, download it as a PEM or DER certificate. This certificate should then be uploaded on the **IPsec Peers** page of the other unit.

IPsec Certificates

Go to **IPsec Certificates** under **Virtual Private Networks** and select that the Firewall/SIParator should use the newly created certificate for IPsec negotiations.

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

Local X.509 Certificate (Help)
Use this certificate for IPsec:

VPN cert ▼

IPsec CA Certificates (Help)

[Edit Row] [CA] [Delete Row]

[Add new rows] 1 rows.

IPsec Peers

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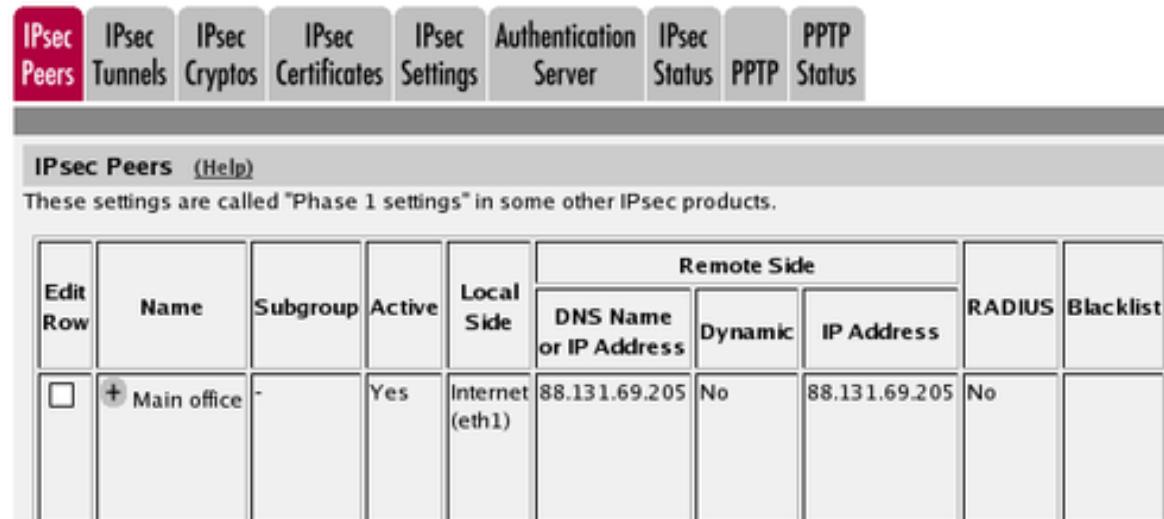
the IPsec peers should authenticate themselves to each other.

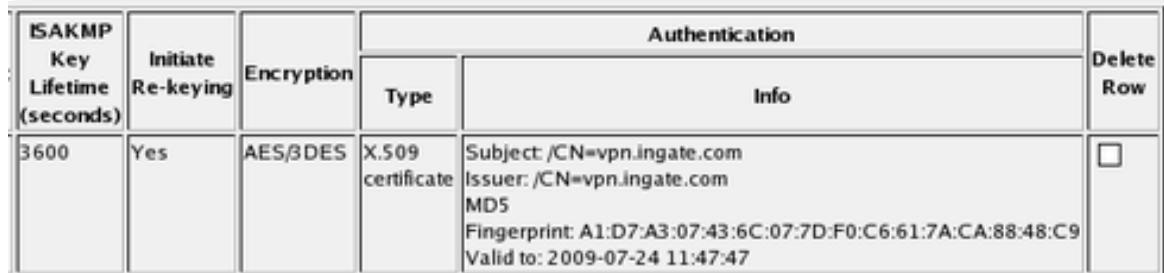Under **Authentication:Type**, select X.509 certificates.

Under **Info**, upload the *other* unit's certificate.

Under **Local side**, select the interface with the dynamic IP address, and enter a public IP address of the other IPsec 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 IPsec peers.

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		
☐	⊞ Main office	-	Yes	Internet (eth1)	88.131.69.205	No	88.131.69.205	No	

ISAKMP Key Lifetime (seconds)	Initiate Re-keying	Encryption	Authentication		Delete Row
			Type	Info	
3600	Yes	AES/3DES	X.509 certificate	Subject: /CN=vpn.ingate.com Issuer: /CN=vpn.ingate.com MD5 Fingerprint: A1:D7:A3:07:43:6C:07:7D:F0:C6:61:7A:CA:88:48:C9 Valid to: 2009-07-24 11:47:47	☐

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. Define the extra network that was created for the servers.

As the two office networks clash, you can't define the remote network directly here. Instead, the IP address from which the traffic seems to be sent will be used directly in the **IPsec Tunnels** table.
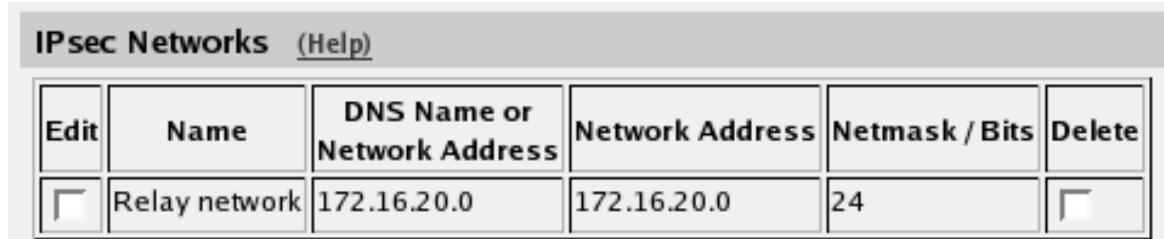
IPsec Networks (Help)

Edit	Name	DNS Name or Network Address	Network Address	Netmask / Bits	Delete
☐	Relay network	172.16.20.0	172.16.20.0	24	☐

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

Under **Local network**, select Network as the **Address type** and the server network that you defined below under **Network**.

Under **Remote network**, select Remote side address.

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.

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

IPsec Tunnels (Help)

These settings are called "Phase 2 settings" in some other IPsec products.

Edit Row	Peer	Local Network			Remote Network		IPsec Key Lifetime (seconds, optional)	Encryption	PFS Group	Delete Row
		Address Type	Network	NAT As	Address Type	Network				
☐	⊞ Main office	Network	Relay network	-	Remote side address	-		AES/3DES	Same as Phase 1 DH	☐

Networks and Computers

Go to **Networks and Computers** under **Network** to create a network group for the remote network that will use the IPsec tunnel. This will be used to define which computers can use the relay that will forward traffic to the inside servers.

The network on the client side of the IPsec tunnel must consist of the IP address(es) that are used to NAT the traffic on that side. This network must have "-" selected under **Interface/VLAN**.

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		
☐	⊞ LAN	-	192.168.0.0	192.168.0.0	192.168.0.255	192.168.0.255	Ethernet2 (eth2 untagged)	☐
☐	⊞ Remote IP	-	88.131.69.205	88.131.69.205			-	☐

Relays

Go to the **Relays** page and create relays to forward traffic from the IPsec tunnel to the inside servers.

Select to Listen to an IP address on the server network. This IP address must be listed among the IP addresses for which the client side makes the IPsec negotiation.

Enter the IP address and port for the server under **Relay to** and select the appropriate relay type. Select the IPsec peer under **IPsec peer** and the client network under **Network**.

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.

Client Side

On the client side, the IPsec connection must be defined, and rules to allow traffic going through the tunnel to the server side.

Certificates;

As one of the IPsec peers has a dynamic IP address, the IPsec authentication must be performed with X.509 certificates. Create a certificate on the **Certificates** page.

Add a new row to the **Private Certificates** table and enter a name for this certificate. Press **Create new**.

Enter information about the Firewall/SIParator in the form, and press **Create a self-signed X.509 certificate**.

When the certificate has been created, download it as a PEM or DER certificate. This certificate should then be uploaded on the **IPsec Peers** page of the other unit.

IPsec Certificates

Go to **IPsec Certificates** under **Virtual Private Networks** and select that the Firewall/SIParator should use the newly created certificate for IPsec negotiations.

IPsec Peers

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

Under **Authentication:Type**, select X.509 certificates.

Under **Info**, upload the *other* unit's certificate.

Under **Local side**, select the interface with the public IP address. Under **Remote side**, enter '*', which means that the peer has a dynamic IP address..

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 IPsec peers.

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		
☐	⊞ Branch office	-	Yes	Internet (88.131.69.205)	*	No	*	No	*

ISAKMP Key Lifetime (seconds)	Initiate Re-keying	Encryption	Authentication		Delete Row
			Type	Info	
3600	Yes	AES/3DES	X.509 certificate	Subject: /CN=vpn.ingate.com Issuer: /CN=vpn.ingate.com MD5 Fingerprint: A1:D7:A3:07:43:6C:07:7D:F0:C6:61:7A:CA:88:48:C9 Valid to: 2009-07-24 11:47:47	☐

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 remote server network.

IPsec Networks (Help)

Edit	Name	DNS Name or Network Address	Network Address	Netmask / Bits	Delete
☐	LAN	192.168.0.0	192.168.0.0	24	☐
☐	Servers	172.16.20.0	172.16.20.0	24	☐

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

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 consists of the IP address(es) 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.

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

IPsec Tunnels (Help)

These settings are called "Phase 2 settings" in some other IPsec products.

Edit Row	Peer	Local Network			Remote Network		IPsec Key Lifetime (seconds, optional)	Encryption	PFS Group	Delete Row
		Address Type	Network	NAT As	Address Type	Network				
☐	⊕ Branch office	Network	LAN	Internet (88.131.69.205)	Network	Servers		AES/3DES	Same as Phase 1 DH	☐

Networks and Computers

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

The network on the server side of the IPsec tunnel must be the extra server network. This network must have "-" selected under **Interface/VLAN**.

			Lower Limit		Upper Limit (for IP ranges)			
Edit Row	Name	Subgroup	DNS Name or IP Address	IP Address	DNS Name or IP Address	IP Address	Interface/VLAN	Delete Row
☐	⊞ LAN	-	192.168.0.0	192.168.0.0	192.168.0.255	192.168.0.255	Ethernet0 (eth0 untagged)	☐
☐	⊞ Server network	-	172.16.20.0	172.16.20.0	172.16.20.255	172.16.20.255	-	☐

Rules

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

Select the local network under **Client**. Select the IPsec peer under **To IPsec peer** and the peer's network under **Server**. Create rules like this for the services that should be allowed to the server side.

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	LAN	-	Server network	Branch office	Ethernet0 -> (VPN)	pop3	Allow	24/7	Local		☐
☐	2	Yes	LAN	-	Server network	Branch office	Ethernet0 -> (VPN)	ftp	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.