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

How to configure Ingate Firewall/SIParator® for IPsec connections with NAT ............3
  Client Side......................................................................................................................3
  Server Side ...................................................................................................................7

IPsec Connection With NAT, Client Side has a Dynamic IP Address.........................11
  Client Side ....................................................................................................................11
  Server Side ...................................................................................................................17

IPsec Connection With NAT, Server Side has a Dynamic IP Address.........................21
  Server Side ...................................................................................................................21
  Client Side ....................................................................................................................26
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 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.

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.

**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**.

![Networks and Computers](image)

### 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](image)
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 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.

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.
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.

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.
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 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.
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.
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**.
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.

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 Tunnels Table](image)

**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.

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.
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.

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

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](image)

**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](image)
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.

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.
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 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 Table]

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.

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.
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.

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.