# 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 N	VAT3
Client Side	3
Server Side	7
IPsec Connection With NAT, Client Side has a Dynamic IP Address	
Client Side	
Server Side	17
IPsec Connection With NAT, Server Side has a Dynamic IP Address	
Server Side	
Client Side	

```
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	IPs Tunr	ec I iels Cr	Psec yptos	IP Certi	sec ficates	IPsec Settings	Authentico Server	ntion IPse Stat	ec us PPTP	PPTP Status		
IRco	c Do	ore //	Hele)									
These	setti	ngs are	e calle	ed "Ph	ase 1	settings" in	some oth	er IPsec p	roducts.			
								F	Remote S	ide		
Edit Rov	Edit Row Na		ame Subgroup		Activ	ve Local Side		DNS Name or IP Address	Dynam	ic IP Address	RADIUS	Blacklist
	÷	Boston	-		Yes	Outside (193.12	.253.115)	13.7.3.22	No	13.7.3.22	No	
EAV								Authe	ntication			
ISAKMP Key Initiate Lifetime Re-keying (seconds)							Delete Row					
3600		Yes		AES/3	DES	Preshared secret	MD5 Fing C9:97:87	gerprint: ':1F:9E:BF	:7C:38:B	E:25:85:D6:	04:84:2F:F	6

#### **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	Delete Row							
Γ	Boston side	13.7.3.22	13.7.3.22	32	Γ						
Г	Home network	10.47.0.0	10.47.0.0	16	Г						

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**.

Ne (	twork ompi	is and Default Iters Gateways Inte	All rfaces	NAT V	LAN EthO	Eth1 Et	h2 Et	h3	Eth4 E	h5	Interface Status P	PPoE		
N	Networks and Computers													
					Lowe	ver Limit (for IP ranges)								
	Ediit Row	Name	Sı	ubgroup	DNS Name or IP Address	IP Addres	or	IP A	Name ddress		IP Address		Interface/VLAN	Delete Row
		+ Boston VPN endpoint			13.7.3.22	13.7.3.2	2					-		
		🖲 Internet			0.0.0.0	0.0.0.0	255	.255	.255.25	5 2	255.255.255.	255	External (eth1 untagged)	
		Office network	-		10.47.0.0	10.47.0.	0 10.4	7.25	5.255	1	10.47.255.25	5	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.



Rule	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	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.

Save/Load CLI Comman	d File (Help)	
The permanent configuration	might be affected by loading a CLI file.	
Save config to CLI file	Load CLI file file:	Browse

### **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	IPse Tunn	ec I els Cr	Psec yptos	IP Certi	sec ficates	IPsec A Settings	Authentication Server	IPsec Status	PPTP	PPTP Status			
IP se These	c Pee	e <b>rs</b> <u>(</u> ngs are	<u>Help)</u> e calle	d "Ph	ase 1 se	ettings" in :	some other IP	sec pro	ducts.				
Edit Rov	Edit Row Name Subgroup Acti		Active	Local Sic	le DNS Nat	Re me ress	emote S Dynami	ide c IP Ada	dress	RADIUS	Blacklist		
	€ s	eattle	-		Yes	Outside (13.7.3.2	2) 193.12.25	3.115	No	193.12.2	253.115	No	
БАК	MP							Auth	nenticat	tion			
Ke Lifeti (seco	y ime nds)	Initi Re-ke	ate :ying	Encr	yption	Туре	Info						Delete Row
3600 Yes AES/3DES Preshared MD5 Fingerprint: secret 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						
Г	Home network	10.47.0.0	10.47.0.0	16	Γ						
Г	Seattle side	193.12.253.115	193.12.253.115	32	Г						

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 A Settings	Authentication Server	IPsec Status	PPTP	PPTP Status				
IP se These	IPsec Tunnels (Help) These settings are called "Phase 2 settings" in some other IPsec products.											
Edi			Local Ne	twork	Remote	Network	IP K	sec ley		DEE	Delete	
Rov	v Peer	Addr Tyj	ess Netwo	k NATA	s Address Type	Network	Life (sec opt	time onds, ional)	Encryption	Group	Row	

#### **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**.

Network Comp	ks and Default d uters Gateways Inter	ul faces NAT	VLAN EthO Eth1	Eth2 Eth3 Eth4	Eth5 Interface Status	PPPoE						
Networks and Computers												
Edit			Lowe	r Limit	Uppe (for IP	r Limit ranges)		Delete				
Row	Name	Subgroup	DNS Name or IP Address	IP Address	DNS Name or IP Address	IP Address	Interface/vLAN	Row				
	Internet	-	0.0.0	0.0.0.0	255.255.255.255	255.255.255.255	External (eth1 untagged)					
	• Office network	etwork - 10.47.0.0 10.47.0.0		10.47.255.255	10.47.255.255	Internal (eth0 untagged)						
	🗄 Seattle VPN endpo	int -	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**.

ules	Relays	DHCF Relay	Ser	vices	Proto	cols	Time Cl	asses						
Rela	ys													
	List	en to			Re	lay to	o			Allow a from	ccess			
Edit Row	addre	ess	Port	Di na or add	NS me IP ress	add	IP Iress	Port	Relay type	Network	IPsec peer	Time class	Log class	Delete Row
Г	Outsid (13.7.3	e 3.22)	80	10.47	7.4.38	10.4	7.4.38	80	TCP relay	Seattle VPN endpoint	Seattle	24/7	Local	Г
	Outsid (13.7.3	e 3.22)	21	10.47	7.4.75	10.4	7.4.75	21	FTP relay	Seattle VPN endpoint	Seattle	24/7	Local	Г

#### 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.

Save/Load CLI Command File (Help)									
The permanent configuration might be affected by loading a CLI file.									
Save config to CLI file	Load CLI file Local		Browse						

# 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**.

Private Certificates (Help)											
Name		Certificat	le	Information	Delete						
VPN cert	Create New	Import	View/Download	Subject: /CN=home.ingate.com Issuer: /CN=home.ingate.com MDS Fingerprint: CD:6F:19:99:1C:4E:3C:94:C0:98:F8:37:AD:58:41:E0 Valid to: 2009-07-24 11:53:57	Г						

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, t	hen create either a certificate or a	a certificate request.
After generating a certific	ate request, and havin	g 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 of they have different serial	ertificates with identica I numbers.	l data you should make sure	Below you can enter an optional challenge password for certificate requests.
Serial number:			Challenge password:
* 0			Challenge password again:
Fields marked with "" ar	re mandatory.		
Create a self-signed	X.509 certificate	Create an X.509 certificate rec	uest 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
Loc	al X.509	Certific	ate (Help)	IPs	ec CA Certific	ates (	(Help)	
Use t	his certifi	cate for IF	sec:	Edi	t Row CA Dele	ete Row	7	
VP	N cert 🔽						1	
				Ad	d new rows	1 rov	ws.	

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

IPsec Peers (Help)

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

							R	emote Sid	le		
	Row		Name	Subgroup	Active	Side	DNS Name or IP Address	Dynamic	IP Address	RADIUS	Blacklist
		ŧ	Main office	-	Yes	Internet (eth1)	88.131.69.205	No	88.131.69.205	No	
ſ	ISAKM	Р					Auth	entication			
	Key Lifetim (second	e is)	Initiate Re-keying	Encryption	Туре			Info			Row
	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.

IPse	c Networks	(Help)			
Edit	Name	DNS Name or Network Address	Network Address	Netmask / Bits	Delete
Γ	LAN	192.168.0.0	192.168.0.0	24	
Γ	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.

<b>IPsec</b>	IPsec	IPsec	IPsec	IPsec	Authentication	IPsec		PPTP
Peers	Tunnels	Cryptos	Certificates	Settings	Server	Status	PPTP	Status

#### IPsec Tunnels (Help)

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

		Local Network			Remote	Network	IPsec Key			
Row	Peer	Address Type	Network	NAT As	Address Type	Network	Lifetime (seconds, optional)	Encryption	PFS Group	Delete Row
	Main office	Network	LAN	Internet (eth1)	Network	Remote 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 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**.

Net C	twork ompi	ks and uters	Default Gateways	All Interfaces	NAT	VLAN	EthO	Eth 1	Eth2	Eth3	Eth4	Eth 5	Interface Status	PPPoE		
N	etw	orks a	nd Comp	uters												1
E	Edit		Eukaraum		Lower Limit			Upper Limit (for IP ranges)					Delete			
F	tow		ame	Subgroup	DNS or IP	5 Name Addres	s II	P Addro	ess	DNS or IP	5 Nam Addre	e ss	IP Address		nace/vDAN	Row
[		+ LAN	4	-	192.1	68.0.0	19	2.168.0	0.0	192.1	68.0.2	55 1	92.168.0.25	5 Ethe unta	ernet2 (eth2 igged)	
[		+ Rer	note VPN		88.13	1.69.20	5 88	.131.69	9.205					-		

#### 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.

		DHCP			Time
Rules	Relays	Relay	Services	Protocols	Classes

Rule	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	-	Remote VPN	Main office	Ethernet2 -> (VPN)	рор3	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.

Save/Load CLI Comman The permanent configuration	<b>d File</b> ( <u>Help</u> ) might be affected by loadi	ng a CLI file.	
Save config to CLI file	Load CLI file file:		Browse

### **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**.

Priva	rivate Certificates (Help)											
Edit	Name		Certificat	e	Information							
4	VPN cert	Create New	Import	View/Download	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	Г						

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, t	hen create either a certificate or a	certificate request.
After generating a certific	cate request, and havin	g 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):	State/province (ST):	Organizational Unit (OU):	
Email address	Locality/town (L):		
If you generate several of they have different seria	certificates with identica I numbers.	I data you should make sure	Below you can enter an optional challenge password for certificate requests.
Serial number:			Challenge password:
* 0			Challenge password again:
Fields marked with "" a	re mandatory.		
Create a self-signed	X.509 certificate	Create an X.509 certificate rec	uest 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**

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	IP: Tun	sec I nels Cr	Psec yptos	IPsec Certificat	IPsec tes Setting	Authentication gs Server	IPsec Status	PPTP	PPTP Status	;			
I														
	IPse	c Pe	eers (	Help)										
	These	e sett	ings are	e calle	d "Phase	1 settings	" in some other IP	sec prod	ucts.					
													_	_
									Rem	ote Sid	le			
	Edi Rov	dit ow Name Subg		Subgro	up Active Local Side		DNS Name or IP Address	Dyi	namic	IP Address			Blacklist	
		Ð	Branch	office	-	Yes	Internet (88.131.69.205)	a	No		e.	No	a.	
ľ	ISAK	MP						Authentik	cation	1				
	Ke Lifeti (seco	y me nds)	Initiat Re-key	e ing En	cryption	Туре			Info	,			D e	elete tow
	3600		Yes	AE	S/3DES	X.509 certificate	Subject: /CN=vpn.i Issuer: /CN=vpn.in MD5 Fingerprint: A1:D7: Valid to: 2009-07-2	ngate.com gate.com :A3:07:43: !4 11:47:4	6C:07	7:7D:F0	:C6:61:7A:	CA:88:48:0	:9	]

#### **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	Aut	nentication Server	ntication IPsec rver Status F		TP Status				
IP se The se	IPsec Tunnels (Help) These settings are called "Phase 2 settings" in some other IPsec products.												
Edit Row	Pe	er	Loca Address Type	l Network Network	NAT As	Remote Address Type	Network Networ	k (sec	rsec (ey etime conds, ional)	Encryption	PFS Group	Delete Row	
	🕈 Bran	ich 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.

Networ Comp	ks and uters	Default Gateways	All Interfaces	NAT VI	AN Eth	0 Eth1	Eth2	Eth3	Eth4	Eth5	Interface Status	PPP	PoE
Netw	orks a	nd Compu	iters										
			Lower	r Limit		Upper Limit (for IP ranges)							
Edit Row	Name	Subgroup	DNS Name or IP Address	IP Addres	DN or IF	S Name Addres	:	IP Ad	dress	1	nterface/VL	AN	Delete Row
	🕀 All	-	0.0.0.0	0.0.0.0	255.2	55.255.2	255 2	\$5.255	.255.2	55 -			

```
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**.

Rela	Relays (Help)											
	Listen To		Relay To			Balay	Allow Access From		Certificate	Time		
Edit	IP Address	Port	DNS Name or IP Address	IP Address	Port	Relay Type	Network	IPsec Peer	for TLS/SSL	Class	Class	Delete
Г	Internet (88.131.69.205)	110	192.168.0.33	192.168.0.33	110	TCP port forwarding	All	Branch office	-	24/7	Local	Г

### 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.

Direc	Irectly 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 Certificat	rivate Certificates (Help)											
Name		Certificat	e	Information								
VPN cert	Create New	Import	View/Download	Subject: /CN=home.ingate.com Issuer: /CN=home.ingate.com MDS 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	Γ							

# 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, t	hen create either a certificate or a	a certificate request.
After generating a certific	ate request, and havin	g 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):	State/province (ST):	Organizational Unit (OU):	
* ome.ingate.com			
Email address	Locality/town (L):		
If you generate several of they have different seria	certificates with identica I numbers.	il data you should make sure	Below you can enter an optional challenge password for certificate requests.
Serial number:			Challenge password
* 0			Challenge password again:
Fields marked with "" a	re mandatory.		
Create a self-signed	X.509 certificate	Create an X.509 certificate re	auest 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				
Loc	al X.509	Certific	ate <u>(Help)</u>	IPs	ec CA Certific	ates	(Help)					
Use t	his certifi	cate for IF	sec:	Edi	Edit Row CA Delete Row							
VP	N cert 🔽											
		-		Ad	d new rows	1 ro	ws.					

#### **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	IP: Tun	sec IPs nels Cryp	ec IPsec tos Certifica	IPse tes Settin	ec Aut Igs	hentication Server	IPse State	ic us PPTP	PPTP Status		
	IPse These	c Pe	e <b>ers</b> <u>(He</u> ings are c	l <u>ø)</u> alled "Phase	1 setting	s" in sor	ne other IP:	sec p	roducts.			
		Γ						R	emote S	ide		
	Edit Row	/	Name	Subgroup	Active	Local Side	DNS Nai or IP Addr	ne ess	Dynamie	IP Address	RADIUS	Blacklist
		÷	Main offic	e -	Yes	Internet (eth1)	88.131.69	.205	No	88.131.69.205	No	
ï	ISAK	MP						Auth	enticatio	1		
	Key Lifetir (secor	/ ne ids)	Initiate Re-keying	Encryption	Туре				Info	,		Row
	3600		Yes	AES/3DES	X.509 certificate	Subject Issuer: MD5 Finger Valid to	t /CN=vpn.i /CN=vpn.in print: A1:D7: p: 2009-07-2	ngate gate.c A3:07 4 11:	.com :om ?:43:6C:07 47:47	7:7D:F0:C6:61:7A:	CA:88:48:C	:9

#### **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
Γ	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 Certifica	IPse tes Settin	c Ai igs	uthenticatio Server	on IPsec Status	PPTP	PPTP Status			
IPsec Tunnels (Help) These settings are called "Phase 2 settings" in some other IPsec products.												
Edit Row	dit ow Peer Address Network AS				Remote Address Type	Network Network	IPse Key Lifetir (secor	c / ne Er nds,	ncryption	PFS Group	Delete Row	
								option				

#### **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**.

Networl Comp	ks and Defau uters Gatewo	lt All ays Interfac	ces NAT	VLAN	Eth0	Eth1	Eth2	Eth3	Eth4	Eth5	Interface Status	PPPoE	
Netw	Networks and Computers												
Edit	Name			Lower Limit				Upper Limit (for IP ranges)				luterforce All AM	Delete
Row	Mame	Subgroup	DNS Na or IP Add	ame dress	IP A	ddres	5	DNS N r IP Ad	lame Idress	IP.	Address	internace/vEAN	Row
	1 LAN	-	192.168.	0.0	192.1	168.0.0	1	92.168	3.0.255	192.	168.0.255	Ethernet2 (eth2 untagged)	
	🖲 Remote IP	-	88.131.6	9.205	88.13	1.69.2	05					-	

#### 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**.



Relay	Relays (Help)												
	Listen To .		Relay To				Allow Access From		Certificate	_			
Row	IP Address	Port	DNS Name or IP Address	IP Address	Port	Relay Type	Network	IPsec Peer	for TLS/SSL	Time Class	Log Class	Row	
	FTP Server (172.16.20.34)	21	192.168.0.34	192.168.0.34	21	FTP relay	Remote IP	Main office	-	24/7	Local		
	pop3 Server (172.16.20.33)	110	192.168.0.33	192.168.0.33	110	TCP port forwarding	Remote IP	Main 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**.

Save/Load Configuration	Show Configuration	User Administration									
Test Run and Apply Conf (Help) Duration of limited test mode:											
30 sec	conds										
Apply conf	figuration										

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

Save/Load CLI Command File (Help)										
The permanent configuration might be affected by loading a CLI file.										
Save config to CLI file	Load CLI file Local file:		Browse							

## **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**.

Priva	te Certificates	Help)				
Edit	Name		Certificat	e	Information	Delete
4	VPN cert	Create New	Import	View/Download	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	Г

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, th	ien create either a certificate or a	certificate request.
After generating a certific	ate request, and having	g 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):  vpn.ingate.com	State/province (ST):	Organizational Unit (OU):	
Email address	Locality/town (L):		
If you generate several of they have different serial	ertificates with identica I numbers.	l data you should make sure	Below you can enter an optional challenge password for certificate requests.
Serial number:			Challenge password:
* 0			Challenge password again:
Fields marked with "" ar	e mandatory.		
Create a self-signed	X.509 certificate	Create an X.509 certificate req	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**

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.

	lPsec Peers	IP: Tun	sec IPs nels Cryp	ec tos	IPsec Certifica	IPsec tes Setting	Authentication gs Server	IPsec Status	PPTP	PPTP Status			
I													
	IPse	c Pe	eers (He	lp)									
	These	sett	ings are c	alle	d "Phase	1 settings	in some other IP	sec prod	ucts.				
		-		_			·						
									Rem	ote Sid	e		
	Edit Rov	v	Name Subgr		Subgro	up Active	Local Side	DNS Name or IP Address	Dyi	namic	IP Address	RADIUS	Blacklist
		Ð	Branch o	h office		Yes	Internet (88.131.69.205)	ż	No		e.	No	ė.
ï	ISAK	MP		Г				Authenti	cation	1			
	Key Lifetir (secor	ne nds)	Initiate Re-keying	En	cryption	Туре			Info	,			Delete Row
	3600		Yes	AE	S/3DES	X.509 certificate	Subject: /CN=vpn.i Issuer: /CN=vpn.in MD5 Fingerprint: A1:D7: Valid to: 2009-07-2	ingate.com igate.com :A3:07:43:6C:07:7D:F0:C6:61:7A:CA:88:48:C9 24:11:47:47					:9

#### **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	Γ						
	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.



#### **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**.

Netwo Comj	rks and puters	Default Gateways	All Interfaces	NAT VLAP	Eth0	Eth1	Eth2	Eth3	Eth4	Eth 5	Interface Status	PPPoE	
Netv	Networks and Computers												
Edit		Name	Subgroup	Lower Limit				Upper Limit (for IP ranges)					Dalata
Row	'			DNS Na or IP Addres	ne IP s	Addres	s	DNS N IP Ad	ame dress	IP A	Address	Interface/VLAN	Row
	+ LAN	N	-	192.168	0.0 19	2.168.0	.0 19	92.168	.0.255	192.3	168.0.255	Ethernet0 (eth0 untagged)	
	🖲 Ser	ver network	-	172.16.2	0.0 17	2.16.20	.0 17	2.16.2	0.255	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.

Rule	85	Relays	DHCP Relay	Service	es Prot	ocols Cla	ime isses							
R	ules	5												
E R	dit ow	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)	рор3	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**.

Save/Load Configuration	Show Configuration	User Administration	U		
Test Run and Apply Conf (Help) Duration of limited test mode:					
30 sec	conds				
Apply cont	figuration				

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

Save/Load CLI Command File (Help)				
The permanent configuration might be affected by loading a CLI file.				
Save config to CLI file	Load CLI file		Browse	