How To Guide

VPN between Ingate <-> Intertex Devices using X509: International edition

23 October 2009

Tested versions: Ingate Firewall version(s): 4.8.0
Intertex IX78 version(s): 5.11F6

Tested versions: Ingate Firewall version(s): 4.8.1
Intertex IX78 version(s): 5.20

Revision History:

Revision	Date	Author	Comments
1.00	23/10/09	Paul Donald	First Public Release
1.01	27/10/09	Paul Donald	Minor updates and logging
1.02	30/10/09	Paul Donald	Minor updates
1.03	25/01/10	Paul Donald	Minor updates, v4.8.1, trunks on IX

Information forthwith is provided as-is and is not warranted for any purpose other than use with Ingate and Intertex units. For errors and omissions, please contact support@ingate.com quoting this document.

Prerequisites

- Ingate with VPN module installed
- The Ingate unit installed, and connected to the Internet with a public IP address
- The Intertex unit installed, and connected to the Internet with a public IP address
- Neither unit has any VPN configurations
- You can securely access the web interfaces of both your Ingate and Intertex.

Assumptions

- Trunks are/will be configured on the Ingate
- IG is synonymous to Ingate
- IX is synonymous to Intertex.

Specifics

Throughout this howto, you will see the following IP addresses;

IX78 public IP: 10.50.11.78

IX78 private subnet: 192.168.3.0

IG public IP: 10.50.11.77

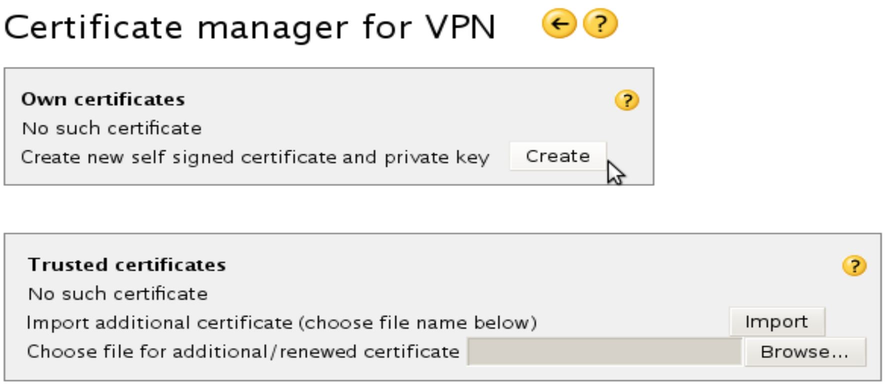
IG private subnet: 192.168.1.0

There were no other simulated NAT, routers or gateways between the IX and IG.

Step 01 - X509 Certificate representing the IX

Create a self-signed certificate to represent the ID of the IX78.

- On your IX78, go to Configurations -> VPN -> Certificates.



Certificate manager for VPN

Own certificates

No such certificate

Create new self signed certificate and private key

Trusted certificates

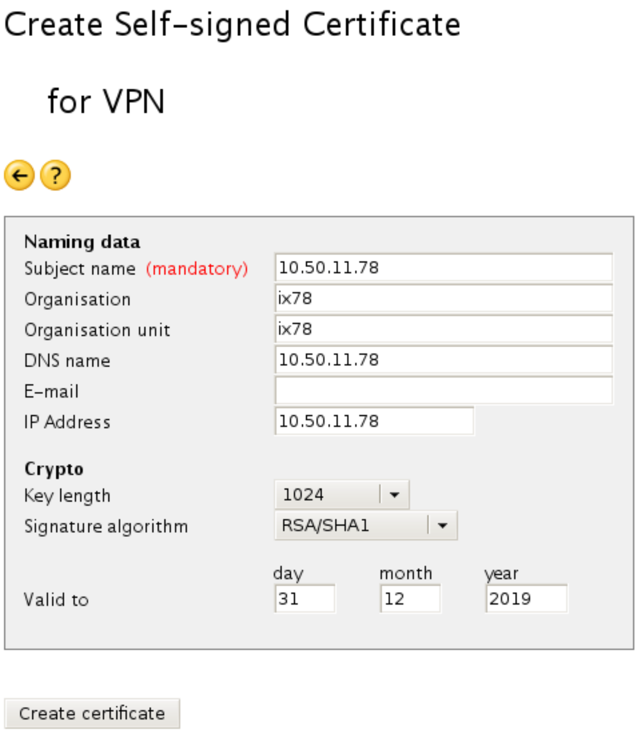
No such certificate

Import additional certificate (choose file name below)

Choose file for additional/renewed certificate

- Ensure the “Subject name” (This is the CN, or Common Name) field matches the public IP or domain name that resolves to the public IP of the IX78.
    - If it is dynamic, use a dynamic DNS service and enter that hostname here.

- Change the “valid to” to something within the next 10 years.
    - The default valid to “2099” year could pose problems for other VPN Servers with older IPsec implementations connecting, that think the certificate is too far in the future.



Create Self-signed Certificate

for VPN

Naming data

Subject name (mandatory)	10.50.11.78
Organisation	ix78
Organisation unit	ix78
DNS name	10.50.11.78
E-mail	
IP Address	10.50.11.78

Crypto

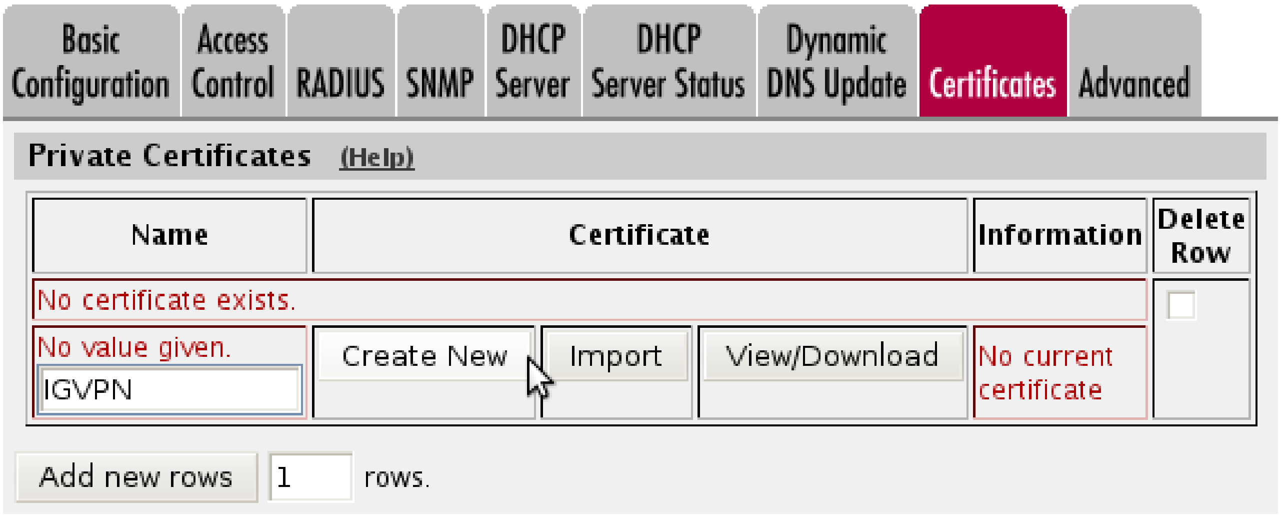
Key length	1024
Signature algorithm	RSA/SHA1

	day	month	year
Valid to	31	12	2019

Step 02 - X509 Certificate representing the IG

Now, create a self-signed certificate to represent the ID of the Ingate.

- On your Ingate, go to Basic Configuration -> Certificates.
- Add 1 new row. Name it. Click Create New.

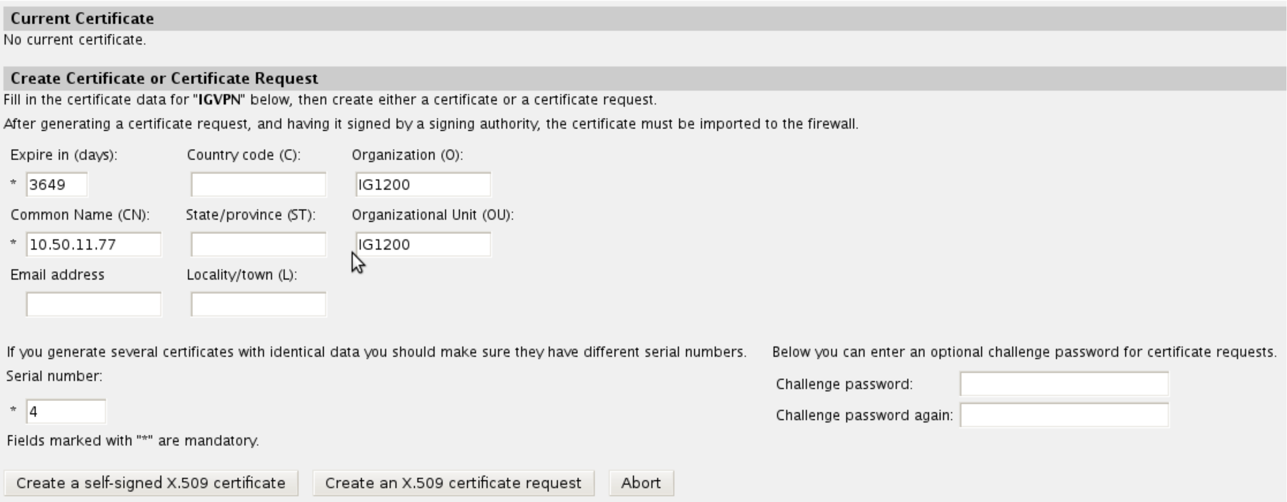


Private Certificates (Help)

Name	Certificate			Information	Delete Row
No certificate exists.					□
No value given. IGVPN	Create New	Import	View/Download	No current certificate	

Add new rows 1 rows.

You will be presented with the following page:



Current Certificate

No current certificate.

Create Certificate or Certificate Request

Fill in the certificate data for "**IGVPN**" 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): * 3649

Country code (C):

Organization (O): IG1200

Common Name (CN): * 10.50.11.77

State/province (ST):

Organizational Unit (OU): IG1200

Email address

Locality/town (L):

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

Serial number: * 4

Fields marked with "*" are mandatory.

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

Challenge password:

Challenge password again:

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

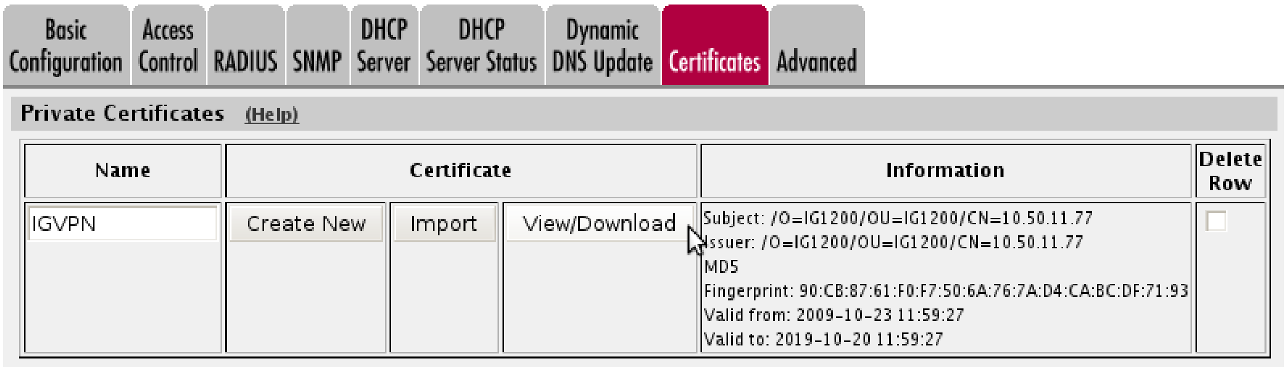
Expire in 3649 days is roughly 10 years into the future.

- The "Common Name (CN)" field needs to be set to the public IP address of the Ingate. If it is dynamic, use a dynamic DNS service and enter that hostname here.
- Click on "create self-signed".

Once created, you will see a message similar to this:

```
Self signed certificate created:


   * Subject: /O=IG1200/OU=IG1200/CN=10.50.11.77
```

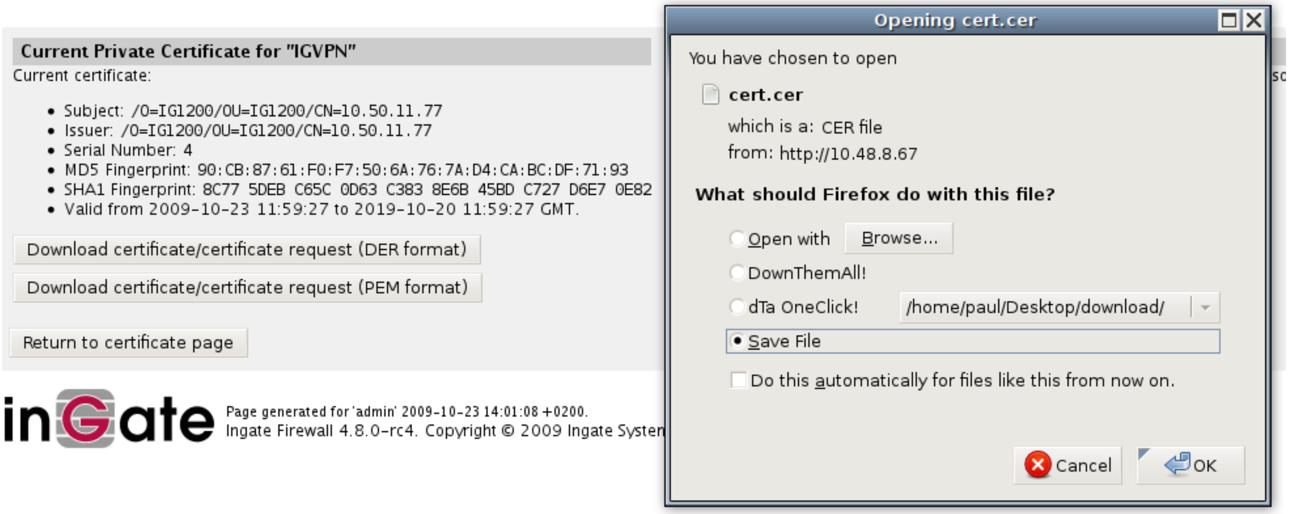
```
    * Issuer: /O=IG1200/OU=IG1200/CN=10.50.11.77
    * Serial Number: 4
    * MD5 Fingerprint: 90:CB:87:61:F0:F7:50:6A:76:7A:D4:CA:BC:DF:71:93
    * SHA1 Fingerprint: 8C77 5DEB C65C 0D63 C383 8E6B 45BD C727 D6E7 0E82
    * Valid from 2009-10-23 11:59:27 to 2019-10-20 11:59:27 GMT.
```



Private Certificates

Name	Certificate			Information	Delete Row
IGVPN	Create New	Import	View/Download	Subject: /O=IG1200/OU=IG1200/CN=10.50.11.77 Issuer: /O=IG1200/OU=IG1200/CN=10.50.11.77 MD5 Fingerprint: 90:CB:87:61:F0:F7:50:6A:76:7A:D4:CA:BC:DF:71:93 Valid from: 2009-10-23 11:59:27 Valid to: 2019-10-20 11:59:27	□

Click “view/download”



Current Private Certificate for "IGVPN"

Current certificate:

- Subject: /O=IG1200/OU=IG1200/CN=10.50.11.77
- Issuer: /O=IG1200/OU=IG1200/CN=10.50.11.77
- Serial Number: 4
- MD5 Fingerprint: 90:CB:87:61:F0:F7:50:6A:76:7A:D4:CA:BC:DF:71:93
- SHA1 Fingerprint: 8C77 5DEB C65C 0D63 C383 8E6B 45BD C727 D6E7 0E82
- Valid from 2009-10-23 11:59:27 to 2019-10-20 11:59:27 GMT.

Download certificate/certificate request (DER format)
Download certificate/certificate request (PEM format)
Return to certificate page
inGate

Page generated for 'admin' 2009-10-23 14:01:08 +0200.
Ingate Firewall 4.8.0-rc4. Copyright © 2009 Ingate Systen

Opening cert.cer

You have chosen to open

cert.cer

which is a: CER file

from: http://10.48.8.67

What should Firefox do with this file?

○ Open with

○ DownThemAll!

○ dTa OneClick! /home/paul/Desktop/download/

● Save File

□ Do this automatically for files like this from now on.

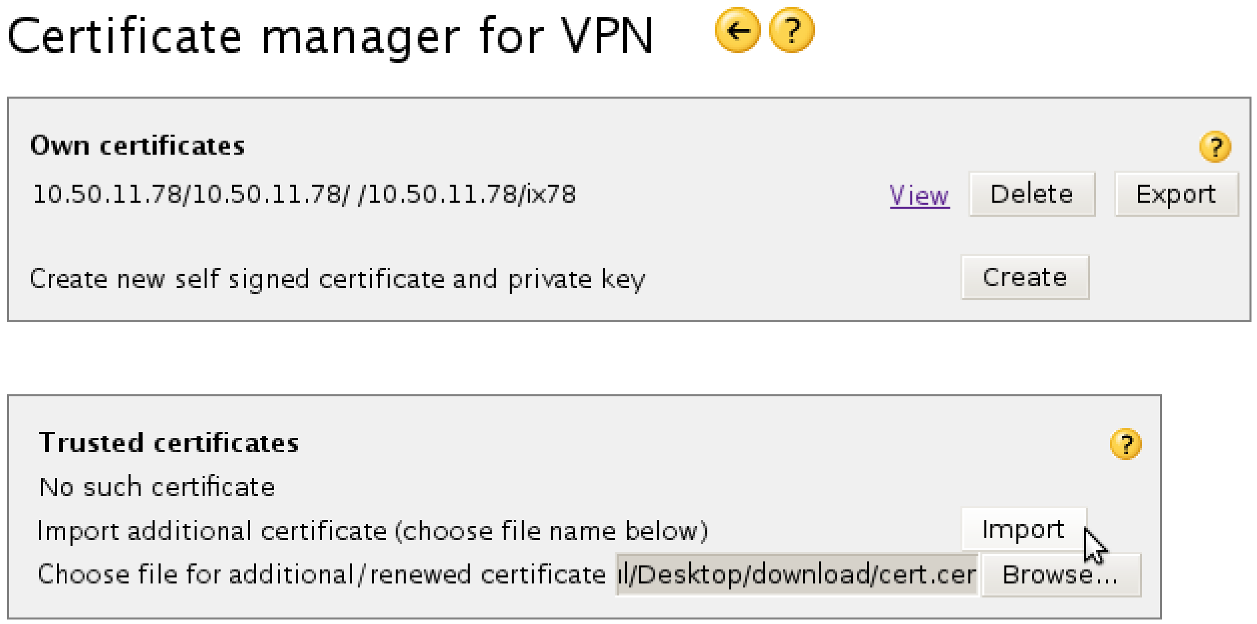
Download in PEM. Save locally.

PEM is ASCII compatible and looks similar to this:

```
-----BEGIN CERTIFICATE-----
MIIDfjCCAmagAwIBAgIBBDANBgkqhkiG9w0BAQQFADA4MQ8wDQYDVQQKEwZJRzEy
MD...
-----END CERTIFICATE-----
```

Step 03 – IG X509 Certificate on the IX

- On your IX78, go to Configurations -> VPN -> Certificates.
- Under Trusted certificates, browse for the cert.cer file you just downloaded from the Ingate. Select, open. Click on Import



Certificate manager for VPN

Own certificates

10.50.11.78/10.50.11.78/ /10.50.11.78/ix78 View Delete Export

Create new self signed certificate and private key Create

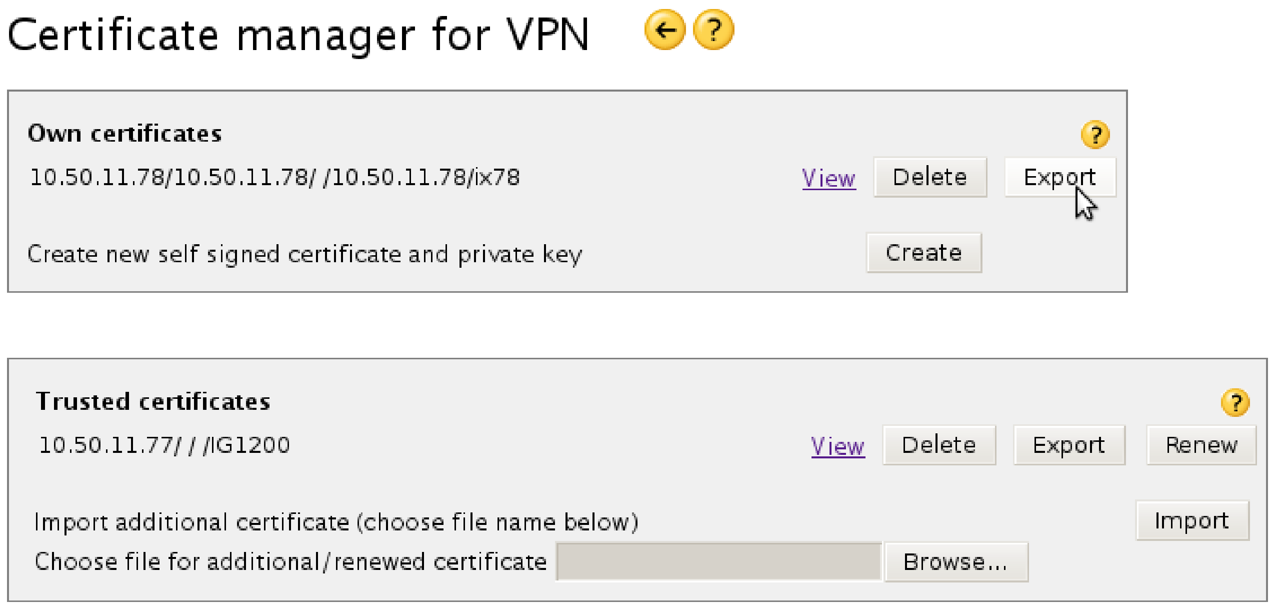
Trusted certificates

No such certificate

Import additional certificate (choose file name below) Import

Choose file for additional/renewed certificate l/Desktop/download/cert.cer Browse...

My IX78 Certificates page will now look like so – yours should be similar:



Certificate manager for VPN

Own certificates

10.50.11.78/10.50.11.78/ /10.50.11.78/ix78 View Delete Export

Create new self signed certificate and private key Create

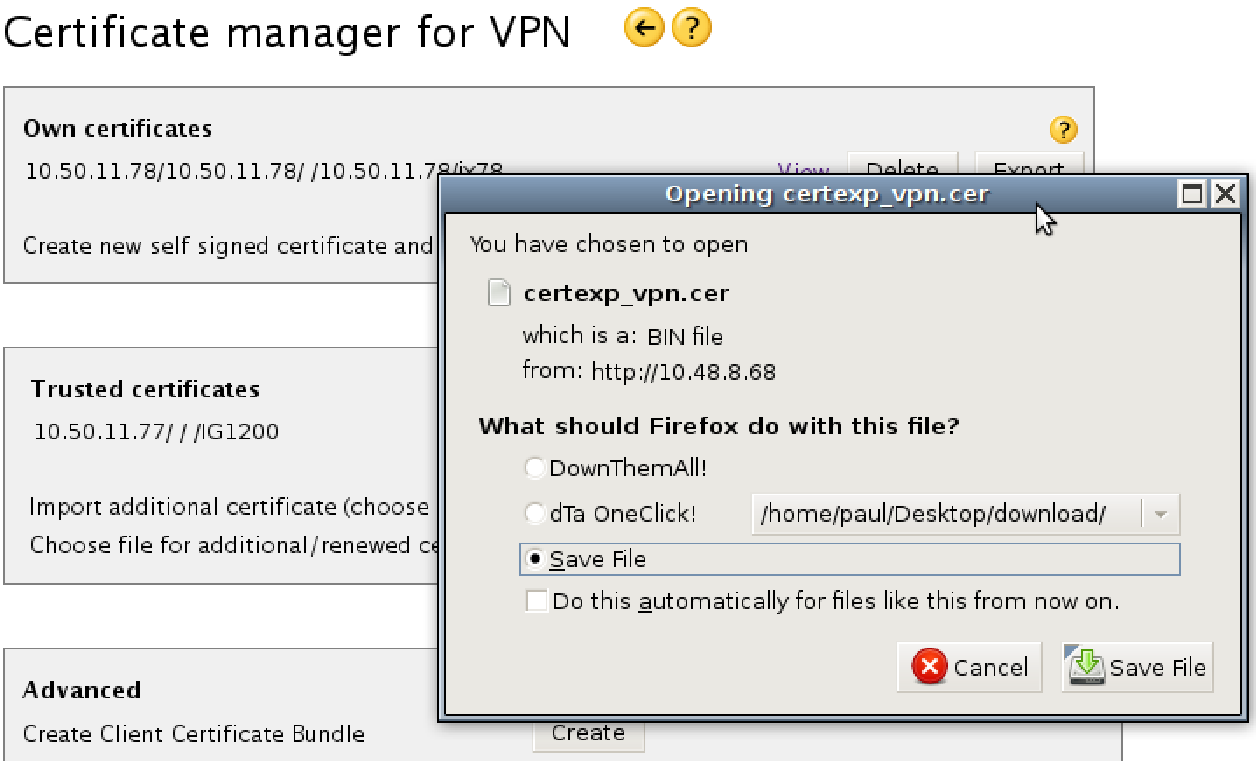
Trusted certificates

10.50.11.77/ / /IG1200 View Delete Export Renew

Import additional certificate (choose file name below) Import

Choose file for additional/renewed certificate Browse...

- Click Export under "Own certificates" on the IX78. Save this file locally.



Certificate manager for VPN

Own certificates

10.50.11.78/10.50.11.78/ /10.50.11.78/ix78

Create new self signed certificate and

Trusted certificates

10.50.11.77/ / /IG1200

Import additional certificate (choose

Choose file for additional/renewed ce

Advanced

Create Client Certificate Bundle

Opening certexp_vpn.cer

You have chosen to open

certexp_vpn.cer

which is a: BIN file

from: http://10.48.8.68

What should Firefox do with this file?

○ DownThemAll!

○ dTa OneClick! /home/paul/Desktop/download/

● Save File

□ Do this automatically for files like this from now on.

Step 04a – Phase 1 on the Ingate ...

- On your Ingate, go to VPN-> Ipsec Peers.
- Add 1 new row:

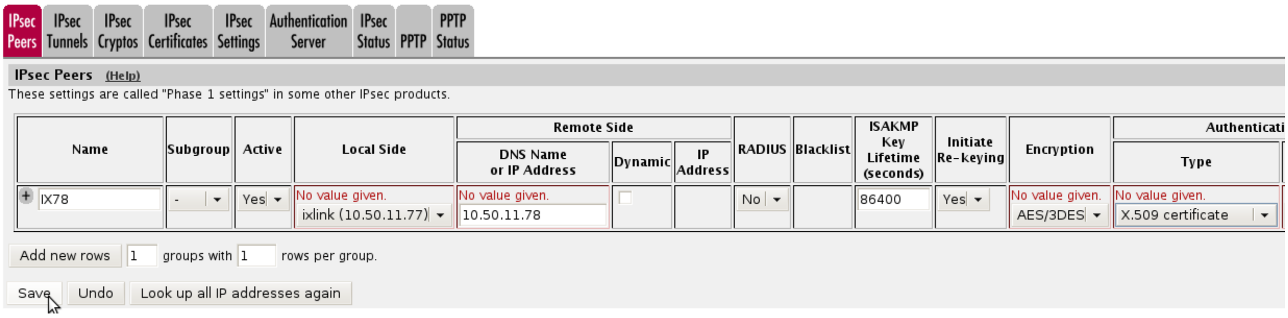
Name: IX78. Local Side: Ingate public IP. Remote Side: IX78 public IP.

ISAKMP Key Lifetime (set to the IX78 default): 86400

Encryption: The default AES/3DES installed will auto-negoatiate a Phase 1 protocol overlap with IX78.

Authentication: X.509 Certificate.

Click Save.



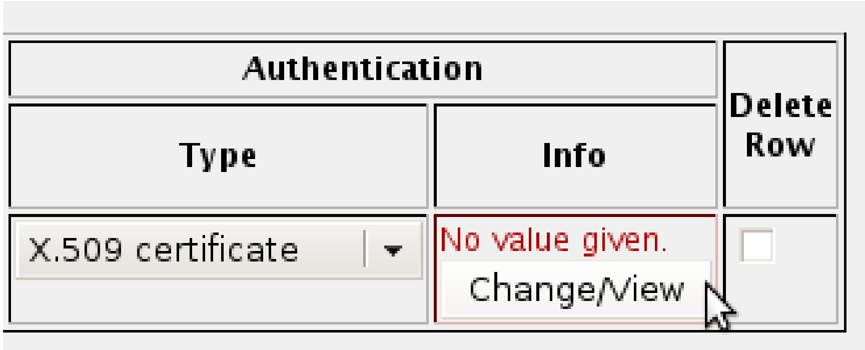
IPsec Peers (Help)

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

Name	Subgroup	Active	Local Side	Remote Side			RADIUS	Blacklist	ISAKMP Key Lifetime (seconds)	Initiate Re-keying	Encryption	Authenticati
				DNS Name or IP Address	Dynamic	IP Address						Type
IX78	-	Yes	No value given. ixlink (10.50.11.77)	No value given. 10.50.11.78	□		No		86400	Yes	No value given. AES/3DES	No value given. X.509 certificate

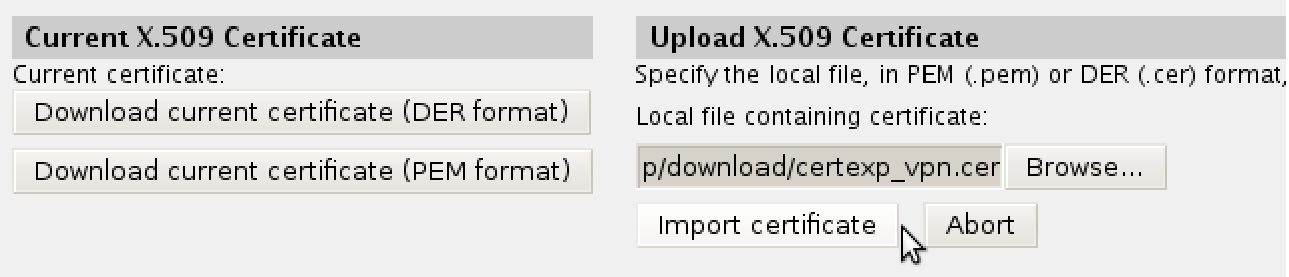
Add new rows 1 groups with 1 rows per group.

Step 04b – IX certificate on the IG



Authentication		Delete Row
Type	Info	
X.509 certificate	No value given. Change/View	□

- Click "Change/View"



Current X.509 Certificate

Current certificate:

Download current certificate (DER format)
Download current certificate (PEM format)

Upload X.509 Certificate

Specify the local file, in PEM (.pem) or DER (.cer) format,

Local file containing certificate: p/download/certexp_vpn.cer

Browse...
Import certificate
Abort

- Browse to the local copy of the IX78 certificate – this is the certificate you downloaded from the IX78 in Step 03. Click "Import Certificate"

Once imported, you will see a message similar to this:

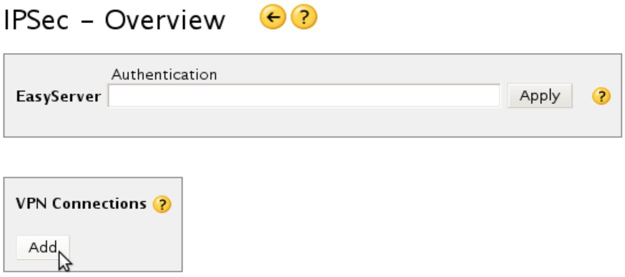
```
Certificate imported:
    * Subject: /CN=10.50.11.78/O=ix78/OU=ix78
    * Issuer: /CN=10.50.11.78/O=ix78/OU=ix78
    * Serial Number: 371401
    * MD5 Fingerprint: 92:40:5C:FA:F2:75:AE:34:38:3A:63:D5:D2:15:76:E1
    * SHA1 Fingerprint: 12A3 A784 3A60 988A 0979 7F30 35AF F954 686C 49EF
    * Valid from 2003-01-01 00:00:00 to 2019-12-31 00:00:00 GMT.
```

In the unlikely event that this step fails – check your certificate, create a new one, or export to a different format (DER).

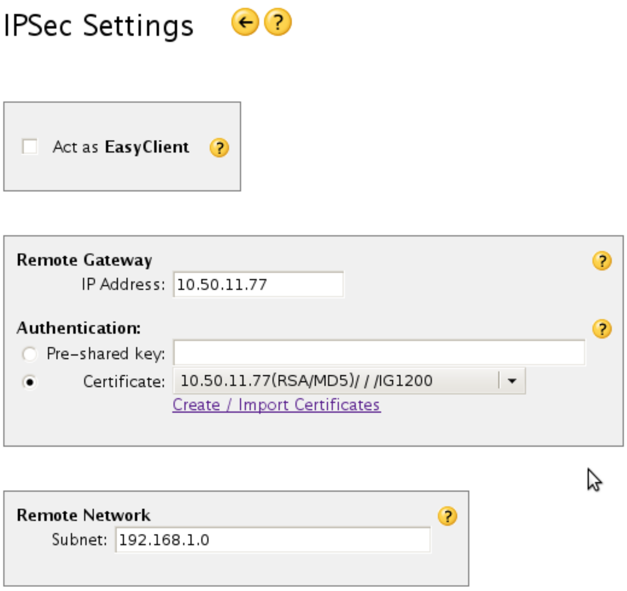
Step 05 – Phase 1 on the IX (+ first Phase 2)

It's time to create Phase 1 and 2 connections.

- On your IX78, go to Configurations->VPN.
- Click on “Add”



- Set “Remote Gateway” to the public IP of the Ingate.
- Set “Certificate” to the copy of the Ingates Certificate uploaded previously.
- Set “Remote Network” to the private subnet behind the Ingate.



IPSec Settings

□ Act as **EasyClient**

Remote Gateway
IP Address: 10.50.11.77

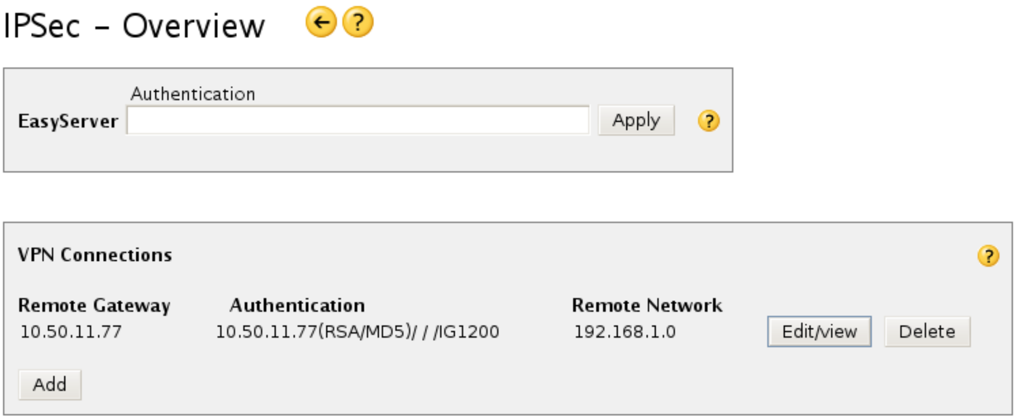
Authentication:
○ Pre-shared key:
● Certificate: 10.50.11.77(RSA/MD5)/ / /IG1200

Create / Import Certificates

Remote Network
Subnet: 192.168.1.0

- Click “Apply”.

This just created a Phase 1 connection between the IG+IX public IPs and a Phase 2 connection and route between IG 192.168.1.0 and IX 192.168.3.0 on the Intertex.



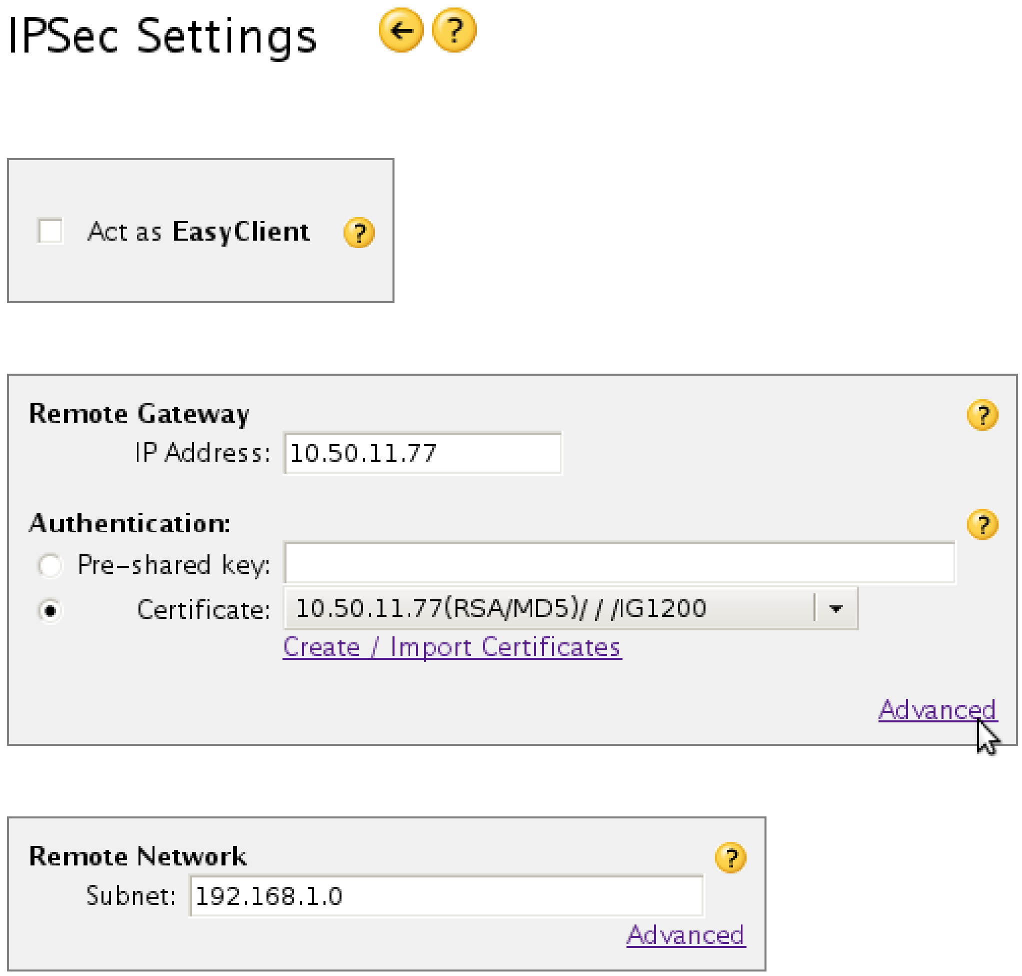
IPSec – Overview

EasyServer Authentication

VPN Connections

Remote Gateway	Authentication	Remote Network
10.50.11.77	10.50.11.77(RSA/MD5)/ / /IG1200	192.168.1.0

- Click on “Edit/View” under VPN Connections:



IPSec Settings

□ Act as **EasyClient**

Remote Gateway

IP Address: 10.50.11.77

Authentication:

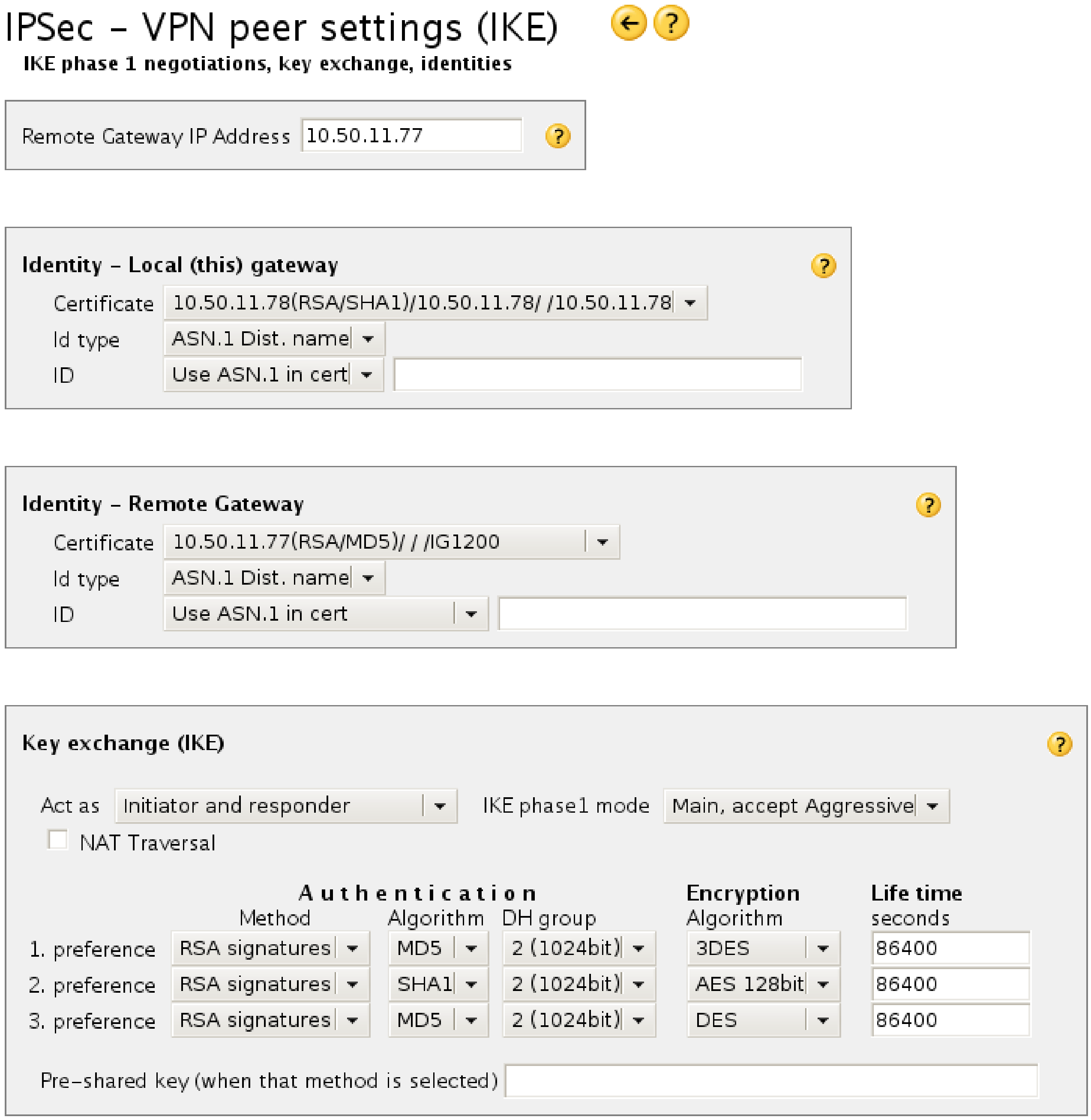
○ Pre-shared key:

● Certificate: 10.50.11.77(RSA/MD5)/ / /IG1200

Remote Network

Subnet: 192.168.1.0

- Click on "Advanced" under Authentication – these are the Phase 1 settings.



IPSec – VPN peer settings (IKE)

IKE phase 1 negotiations, key exchange, identities

Remote Gateway IP Address 10.50.11.77

Identity – Local (this) gateway

Certificate	10.50.11.78(RSA/SHA1)/10.50.11.78/ /10.50.11.78	
Id type	ASN.1 Dist. name	
ID	Use ASN.1 in cert	

Identity – Remote Gateway

Certificate	10.50.11.77(RSA/MD5)/ / /IG1200	
Id type	ASN.1 Dist. name	
ID	Use ASN.1 in cert	

Key exchange (IKE)

Act as Initiator and responder   IKE phase1 mode Main, accept Aggressive

□ NAT Traversal

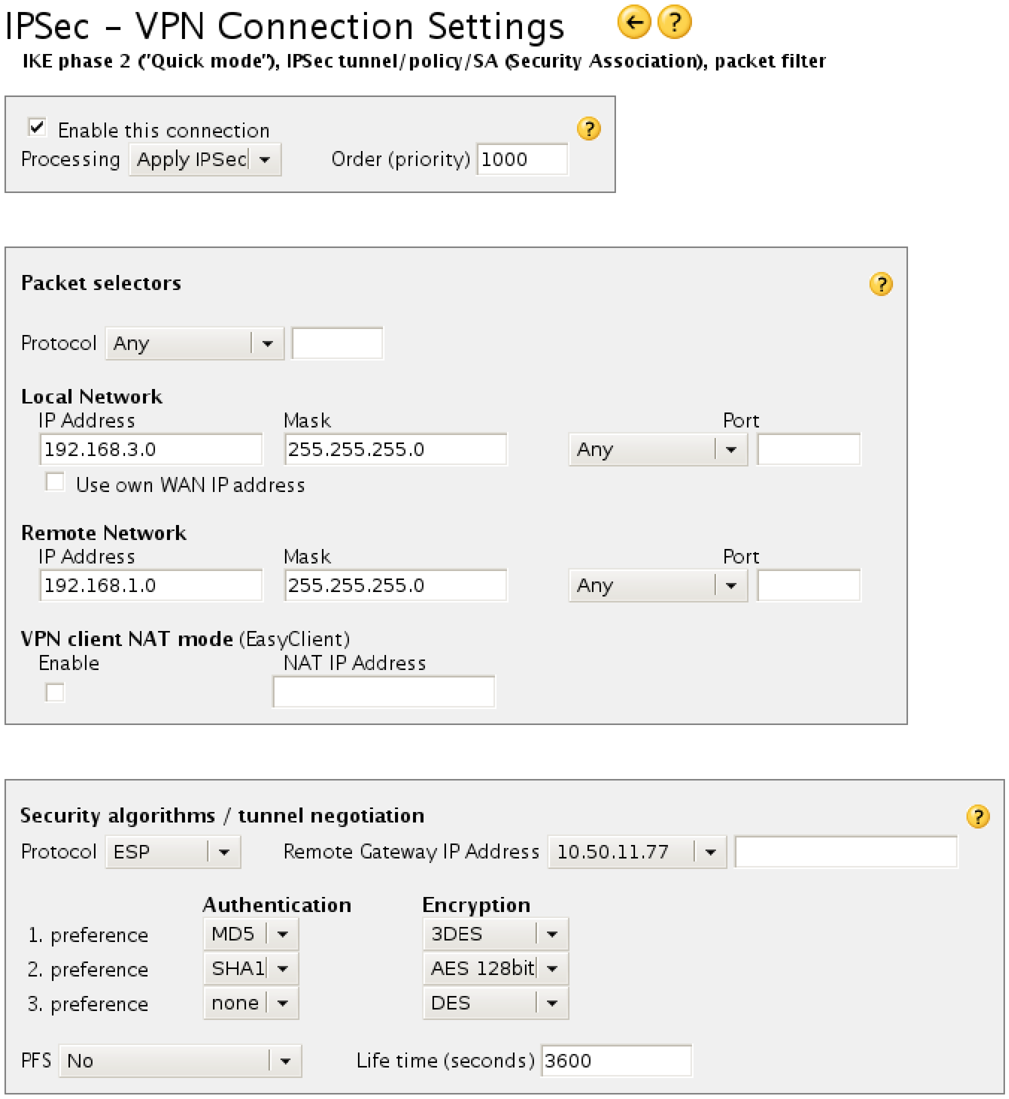
	Authentication			Encryption	Life time
	Method	Algorithm	DH group	Algorithm	seconds
1. preference	RSA signatures	MD5	2 (1024bit)	3DES	86400
2. preference	RSA signatures	SHA1	2 (1024bit)	AES 128bit	86400
3. preference	RSA signatures	MD5	2 (1024bit)	DES	86400

Pre-shared key (when that method is selected)

This is the ESP conversation between the public IP of the IX78 and the public IP of the Ingate. This means the two units are now aware of each other and can begin to build secure private networks between each other i.e. link the private networks via the public IPs.

- Note the IKE Lifetime (here 86400). It should look like the above. This should be the same as the ISAKMP value from the Ingate that we entered earlier.

- Go back and now view the “Advanced” under Remote Network. These are the Phase 2 settings:



IPSec – VPN Connection Settings

IKE phase 2 ('Quick mode'), IPSec tunnel/policy/SA (Security Association), packet filter

☑ Enable this connection

Processing: Apply IPSec ▾   Order (priority): 1000

Packet selectors

Protocol: Any ▾

Local Network

IP Address: 192.168.3.0   Mask: 255.255.255.0   Port: Any ▾

□ Use own WAN IP address

Remote Network

IP Address: 192.168.1.0   Mask: 255.255.255.0   Port: Any ▾

VPN client NAT mode (EasyClient)

Enable: □   NAT IP Address:

Security algorithms / tunnel negotiation

Protocol: ESP ▾   Remote Gateway IP Address: 10.50.11.77 ▾

	Authentication	Encryption
1. preference	MD5	3DES
2. preference	SHA1	AES 128bit
3. preference	none	DES

PFS: No ▾   Life time (seconds): 3600

Note that on the IX78 by default, PFS is NO. Lifetime is 3600 seconds.

Note the Local & Remote Network & Netmask.

We just created a Phase 2 connection between the private nets :

IG 192.168.1.0 and IX 192.168.3.0

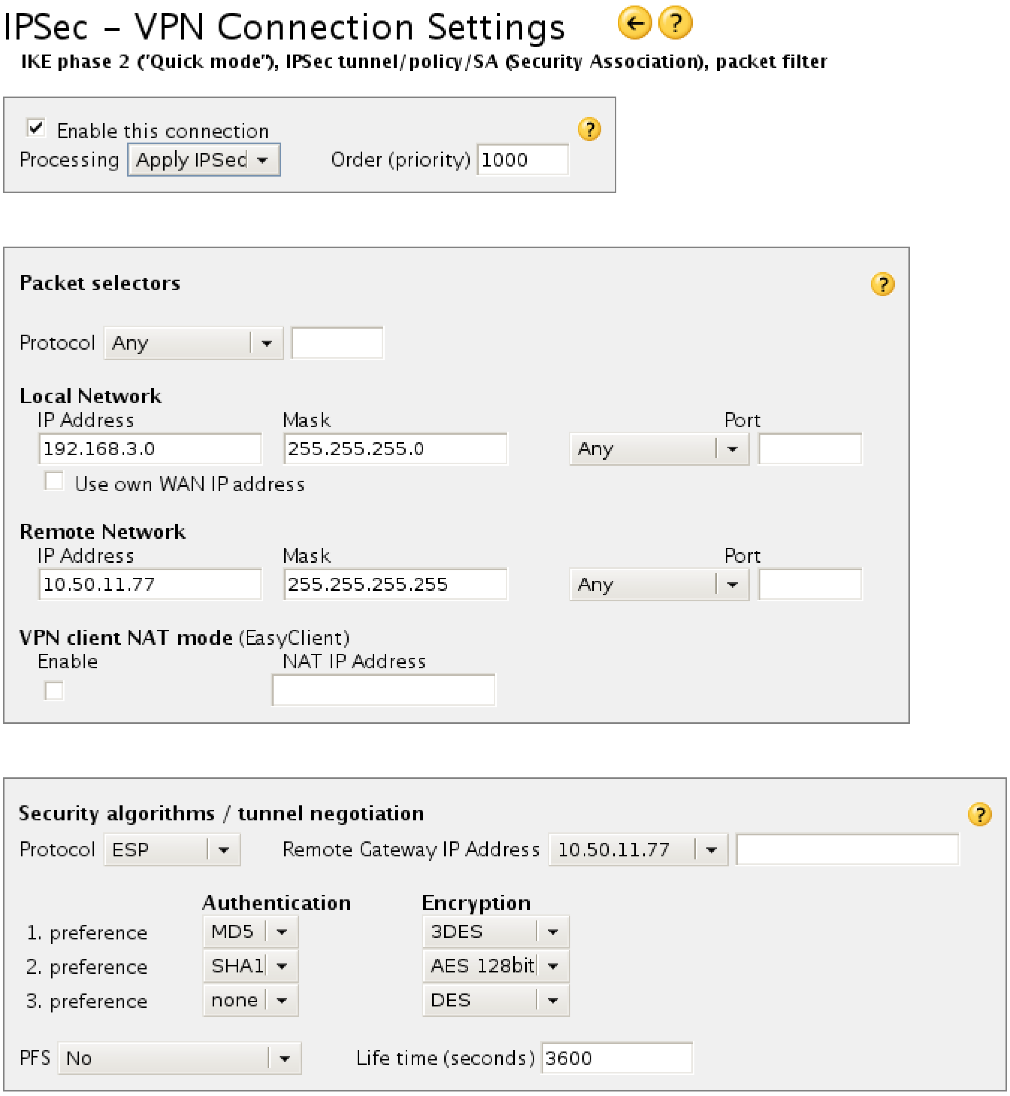
i.e. the tunnels can route between any IP in the subnet 192.168.1.0 and any IP on the subnet 192.168.3.0

Step 06 – Phase 2 on the IX for the B2BUAs

This step is *important* for sending SIP through an IPsec tunnel between Ingate and Intertex – and in general, proxies with SIP b2buas in them. The SIP b2buas communicate with each other using public IPs.

Add 1 more VPN Connection (Phase 2) in the same way toward the Ingate's public IP.

- Set the Remote Network to the public IP of the Ingate. Netmask to 255.255.255.255



IPSec – VPN Connection Settings

IKE phase 2 ("Quick mode"), IPSec tunnel/policy/SA (Security Association), packet filter

☑ Enable this connection

Processing: Apply IPSec Order (priority): 1000

Packet selectors

Protocol: Any

Local Network

IP Address	Mask		Port
192.168.3.0	255.255.255.0	Any	

□ Use own WAN IP address

Remote Network

IP Address	Mask		Port
10.50.11.77	255.255.255.255	Any	

VPN client NAT mode (EasyClient)

Enable □ NAT IP Address:

Security algorithms / tunnel negotiation

Protocol: ESP Remote Gateway IP Address: 10.50.11.77

	Authentication	Encryption
1. preference	MD5	3DES
2. preference	SHA1	AES 128bit
3. preference	none	DES

PFS: No Life time (seconds): 3600

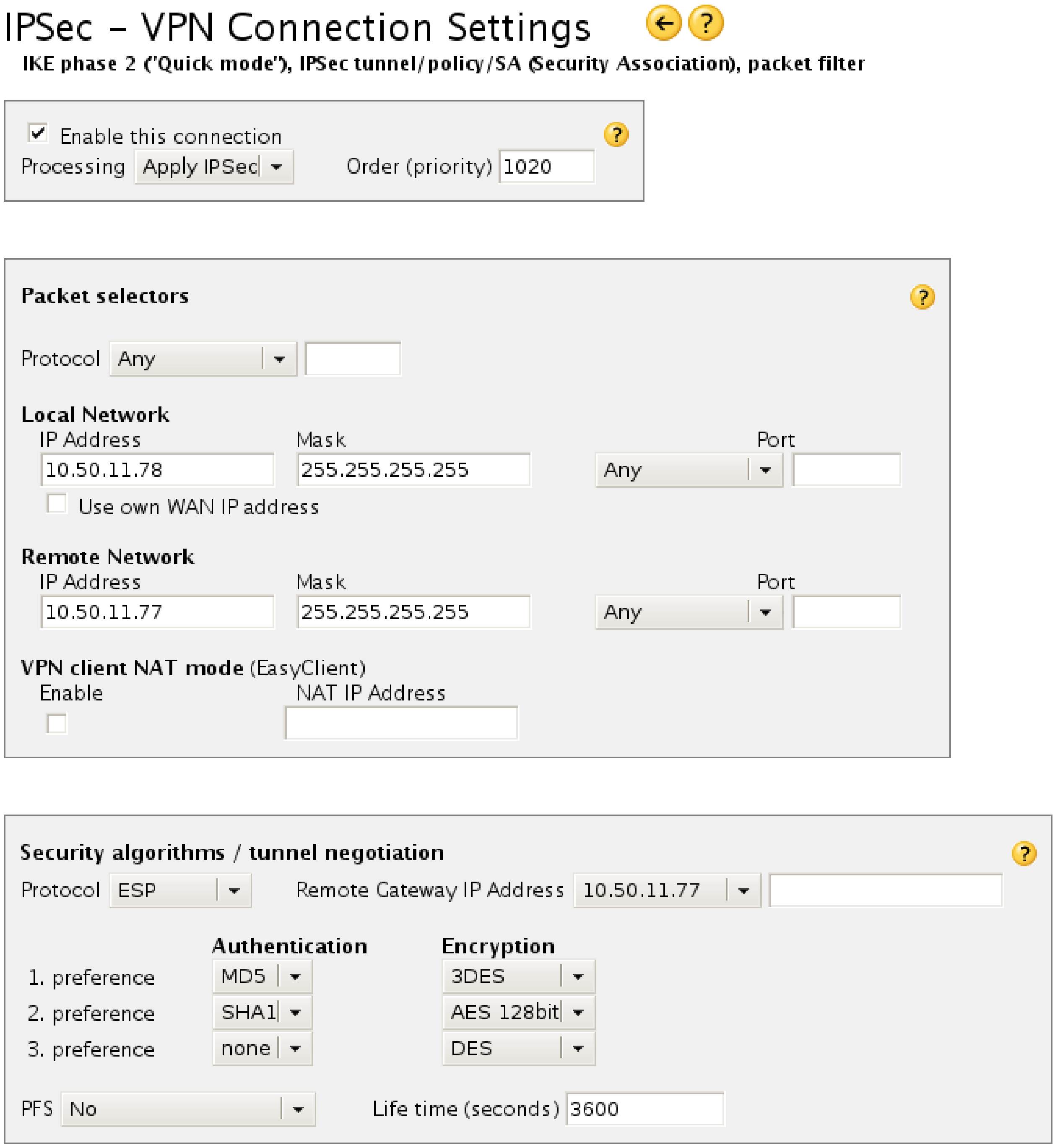
This will allow the Ingate to ping the public IP of the IX78 from the Logging and Tools menu.

This also allows any proxied SIP signalling from the Ingate to enter the IX78 private network and vice-versa, i.e. signalling between the private net 192.168.3.0 on the Intertex and the public IP of the Ingate.

Step 07 – Phase 2 on the IX

Add 1 more VPN Connection in the same way toward the Ingates public IP.

- Set the Remote Network to the public IP of the Ingate. Netmask to 255.255.255.255
- Set the Local Network to the public IP of the IX78. Netmask to 255.255.255.255



IPSec – VPN Connection Settings

IKE phase 2 ('Quick mode'), IPSec tunnel/policy/SA (Security Association), packet filter

☑ Enable this connection

Processing: Apply IPSec

Order (priority): 1020

Packet selectors

Protocol: Any

Local Network

IP Address	Mask	Port	
10.50.11.78	255.255.255.255	Any	

□ Use own WAN IP address

Remote Network

IP Address	Mask	Port	
10.50.11.77	255.255.255.255	Any	

VPN client NAT mode (EasyClient)

Enable	NAT IP Address
□	

Security algorithms / tunnel negotiation

Protocol: ESP

Remote Gateway IP Address: 10.50.11.77

	Authentication	Encryption
1. preference	MD5	3DES
2. preference	SHA1	AES 128bit
3. preference	none	DES

PFS: No

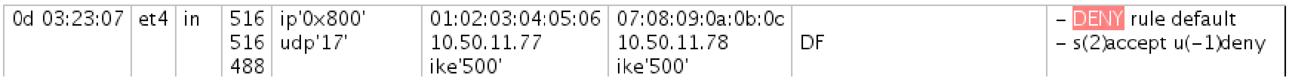
Life time (seconds): 3600

This allows proxied SIP signalling between the public IP of the IX78 and the public IP of the Ingate.

Step 08 – check the IX traffic rules

In some situations FIREWALL RULES are not auto-created to allow incoming IPsec ESP traffic (specifically where two public IPs have no gateway, or the same gateway between them). You will know this is the case if you look in the IX78 Firewall logs (which is set to Show all packets, verbosity level 3) and see DENY for traffic on port 500:

```
--- deny ---
0d 01:43:06 et4    in     516
516
488    ip'0x800'
udp'17'
      01:02:03:04:05:06
10.50.11.77
ike'500'     07:08:09:0a:0b:0c
10.50.11.78
ike'500'
DF
      - DENY rule default
- s(2)accept u(-1)deny
-----------
```

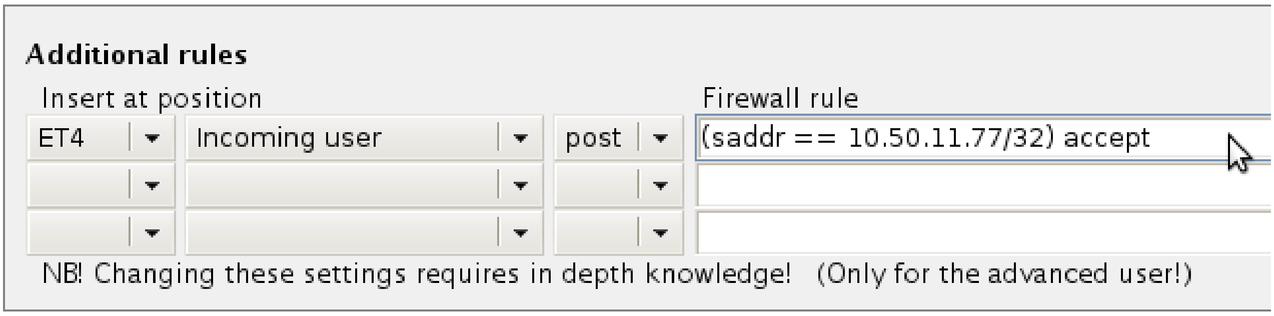


0d 03:23:07	et4	in	516 516 488	ip'0x800' udp'17'	01:02:03:04:05:06 10.50.11.77 ike'500'	07:08:09:0a:0b:0c 10.50.11.78 ike'500'	DF	– DENY rule default – s(2)accept u(–1)deny

- On the IX78, go to Status -> Firewall Rules

Search for the public IP of the Ingate. If you don't find it, you need to add a rule manually.

- On the IX78, go to Configurations -> Security/[active profile]
- Go to the section “Additional Rules”:



Additional rules

Insert at position			Firewall rule
ET4	Incoming user	post	(saddr == 10.50.11.77/32) accept

NB! Changing these settings requires in depth knowledge! (Only for the advanced user!)

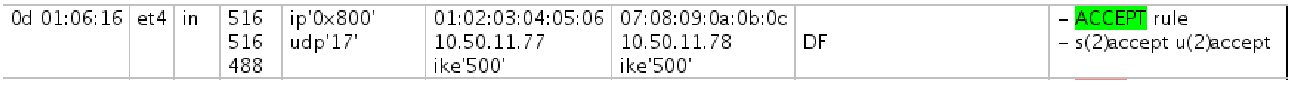
The formula is: `(saddr == remote.ipsec.peer.ip-address/32) accept`

A more specific rule for the IX78 for the IPsec traffic would be (the following is what is normally auto-generated on the IX78):

```
(dport == ipsec-nat-t'4500' || dport == ike'500') && saddr == 5.6.7.8/32 &&
proto == udp accept #IPSec
saddr == 5.6.7.8/32 && (proto == esp || proto == ah) accept #IPSec
```

Once added, check the Firewall rules and you should see green text that says ACCEPT.

```
--- acc ---

0d 01:06:26 et4   in    516

516

488   ip'0x800'

udp'17'

      01:02:03:04:05:06

10.50.11.77

ike'500'    07:08:09:0a:0b:0c

10.50.11.78

ike'500'

DF

      - ACCEPT rule

- s(2)accept u(2)accept

-----------
```

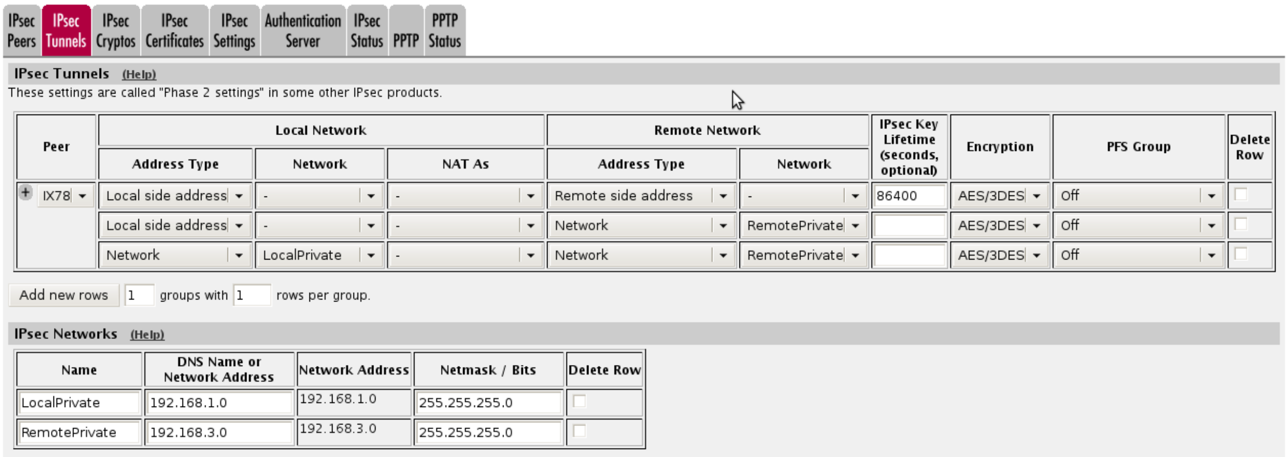


0d 01:06:16	et4	in	516 516 488	ip'0x800' udp'17'	01:02:03:04:05:06 10.50.11.77 ike'500'	07:08:09:0a:0b:0c 10.50.11.78 ike'500'	DF	– ACCEPT rule – s(2)accept u(2)accept

Step 09 – Phase 2 on the Ingate

- Go to your Ingate. VPN-> Ipsec Tunnels.
- Add 2 IPsec Networks. These are the local (to Ingate) 192.168.1.0 and remote (from Ingate) 192.168.3.0 subnets
- Add a new row under Tunnels (a.k.a. IPsec Phase 2 connections), select the IX78 Peer (a.k.a. the IPsec Phase 1 connection) created earlier. Click + twice. Set the 3 rows like so:

```
Local side address <-> Remote side address
Local side address <-> Network [Ix78 Remote private subnet]
Network [Ingate local private subnet] <-> Network [Ix78 Remote private subnet]
```



IPsec Tunnels (Help)

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

Peer	Local Network			Remote Network		IPsec Key Lifetime (seconds, optional)	Encryption	PFS Group	Delete Row
	Address Type	Network	NAT As	Address Type	Network				
+ IX78	Local side address	-	-	Remote side address	-	86400	AES/3DES	Off	□
	Local side address	-	-	Network	RemotePrivate		AES/3DES	Off	□
	Network	LocalPrivate	-	Network	RemotePrivate		AES/3DES	Off	□

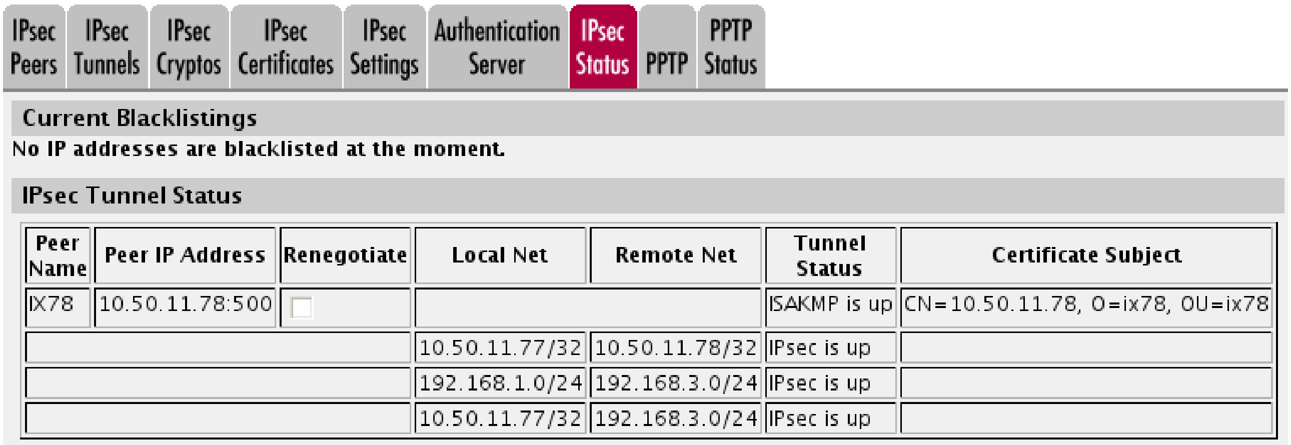
Add new rows 1 groups with 1 rows per group.

IPsec Networks (Help)

Name	DNS Name or Network Address	Network Address	Netmask / Bits	Delete Row
LocalPrivate	192.168.1.0	192.168.1.0	255.255.255.0	□
RemotePrivate	192.168.3.0	192.168.3.0	255.255.255.0	□

Set `PFS Group to Off`, as set in the IX78. (Ingate sets PFS to ON by default)

Save and apply your configuration. Your IPsec Status will look like so when working correctly:



Current Blacklistings

No IP addresses are blacklisted at the moment.

IPsec Tunnel Status

Peer Name	Peer IP Address	Renegotiate	Local Net	Remote Net	Tunnel Status	Certificate Subject
IX78	10.50.11.78:500	□			ISAKMP is up	CN=10.50.11.78, O=ix78, OU=ix78
			10.50.11.77/32	10.50.11.78/32	IPsec is up	
			192.168.1.0/24	192.168.3.0/24	IPsec is up	
			10.50.11.77/32	192.168.3.0/24	IPsec is up	

Step 10 – trunks on the IX

For completeness – you can add a further Phase 2 which covers all SIP routing scenarios between the 4 “networks” i.e. this enables trunks on the Intertex IX78 instead of/as well as the Ingate:

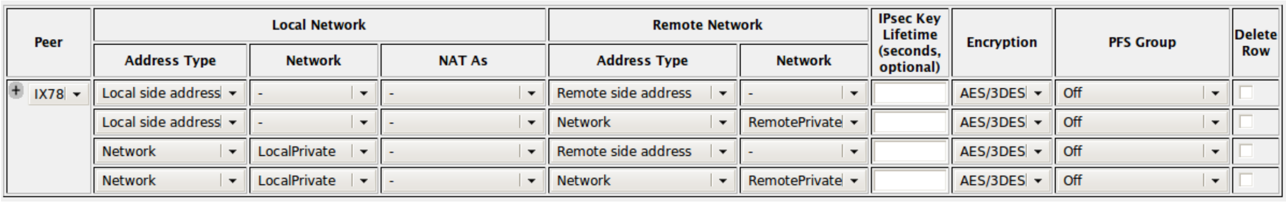
Under Tunnels (a.k.a. IPsec Phase 2 connections), click + once. Set the 1 additional row like so:

Network [Ingate local private subnet] <-> Remote side address

resulting in 4 total Phase 2s that look like:

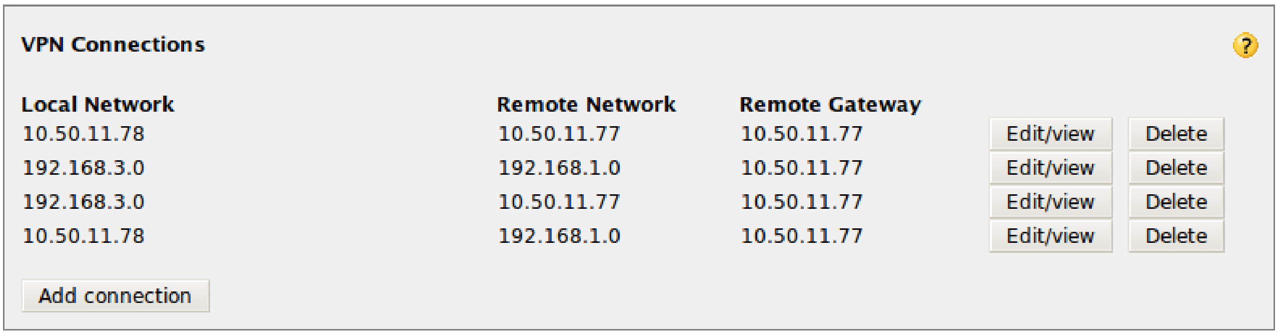
```
Local side address <-> Remote side address
Local side address <-> Network [Ix78 Remote private subnet]
Network [Ingate local private subnet] <-> Remote side address
Network [Ingate local private subnet] <-> Network [Ix78 Remote private subnet]
```

On the IG



Peer	Local Network			Remote Network		IPsec Key Lifetime (seconds, optional)	Encryption	PFS Group	Delete Row
	Address Type	Network	NAT As	Address Type	Network				
+ IX78	Local side address	-	-	Remote side address	-		AES/3DES	Off	□
	Local side address	-	-	Network	RemotePrivate		AES/3DES	Off	□
	Network	LocalPrivate	-	Remote side address	-		AES/3DES	Off	□
	Network	LocalPrivate	-	Network	RemotePrivate		AES/3DES	Off	□

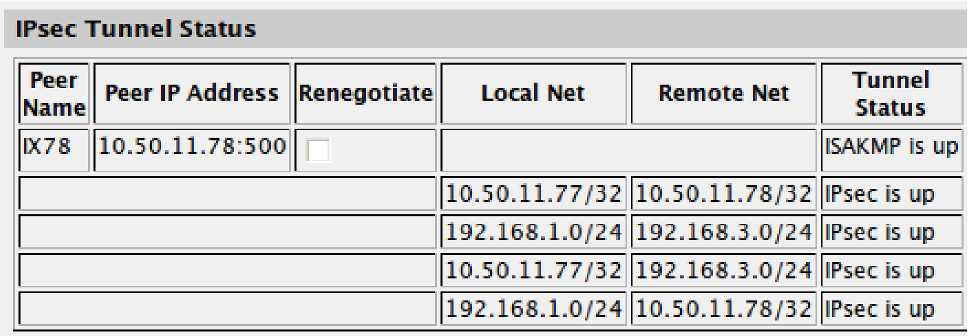
This corresponding Phase 2 connection must also be added to the Intertex IX78 configuration, this is similar to Step 06. On the IX



VPN Connections

Local Network	Remote Network	Remote Gateway		
10.50.11.78	10.50.11.77	10.50.11.77	Edit/view	Delete
192.168.3.0	192.168.1.0	10.50.11.77	Edit/view	Delete
192.168.3.0	10.50.11.77	10.50.11.77	Edit/view	Delete
10.50.11.78	192.168.1.0	10.50.11.77	Edit/view	Delete

The IPsec status on the IG will look like so if all Phase 2 connections are working:



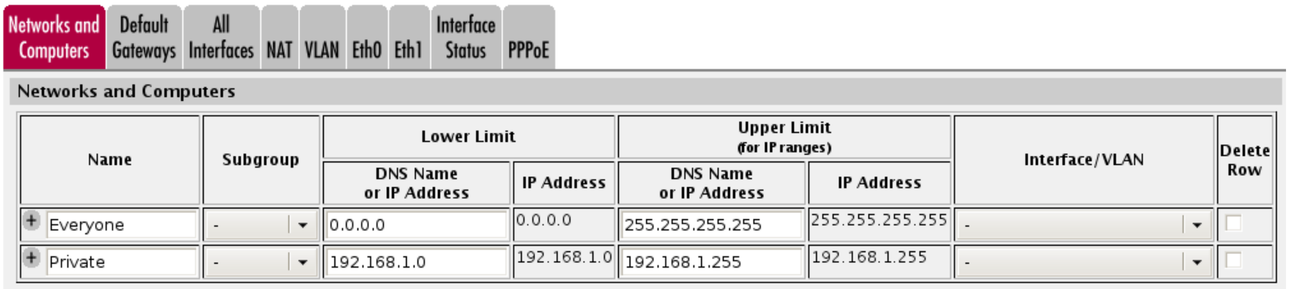
IPsec Tunnel Status

Peer Name	Peer IP Address	Renegotiate	Local Net	Remote Net	Tunnel Status
IX78	10.50.11.78:500	□			ISAKMP is up
			10.50.11.77/32	10.50.11.78/32	IPsec is up
			192.168.1.0/24	192.168.3.0/24	IPsec is up
			10.50.11.77/32	192.168.3.0/24	IPsec is up
			192.168.1.0/24	10.50.11.78/32	IPsec is up

Step 11 – traffic through the VPN

To be able to send and receive non-SIP traffic (i.e. ping, FTP etc) between the private subnets, you need to define which IP addresses are allowed to do so, and add a rule to the Ingate under Rules & Relays to permit them to do so. Note that only 1 rule is needed to cover sending and receiving of the traffic. It stands to reason that if you send through an interface, you will also want to receive replies through it.

- Go to Ingate, Network -> Networks and Computers:

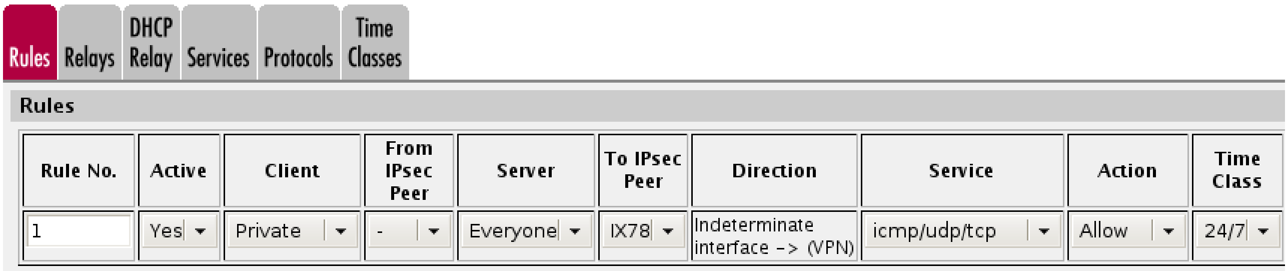


Networks and Computers

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		
Everyone	-	0.0.0.0	0.0.0.0	255.255.255.255	255.255.255.255	-	☐
Private	-	192.168.1.0	192.168.1.0	192.168.1.255	192.168.1.255	-	☐

Above, “Private” is the private subnet local to the Ingate, 192.168.1.0. Note: no interface attached, where Interface is “ - ”, simply means that any IP in the subnet range, can be on any interface.

- Go to Ingate, Rules & Relays -> Rules:



Rules

Rule No.	Active	Client	From IPsec Peer	Server	To IPsec Peer	Direction	Service	Action	Time Class
1	Yes	Private	-	Everyone	IX78	Indeterminate interface -> (VPN)	icmp/udp/tcp	Allow	24/7

Client: “Private” (added in networks and computers)

Server can be any private IP on the “other side”.

To IPsec Peer: the IX78 Peer created earlier.

Service:“icmp/udp/tcp” (available by default on the Ingate)

Action: Allow

The above rule specifics are fairly general, and should permit most traffic types to flow.

Errors and Troubleshooting in the logs - IX

You may see errors in the IX78 VPN Log. The following means that Phase 2 networks set in the Ingate aren't ready or correctly set in the IX78:

```
0d 00:27:32    iked     info     respond new phase 2 negotiation: 10.50.11.78[0]<=>10.50.11.77[0]
0d 00:27:32    iked     error    no policy found: 192.168.1.0/24[0] 192.168.3.0/24[0] proto=any dir=in ifIndex=3
0d 00:27:32    iked     error    failed to get proposal for responder.
0d 00:27:32    iked     error    failed to pre-process packet.
0d 00:27:32    iked     info     respond new phase 2 negotiation: 10.50.11.78[0]<=>10.50.11.77[0]
0d 00:27:32    iked     error    no policy found: 10.50.11.77/32[0] 10.50.11.78/32[0] proto=any dir=in ifIndex=3
0d 00:27:32    iked     error    failed to get proposal for responder.
0d 00:27:32    iked     error    failed to pre-process packet.
0d 00:28:12    iked     info     respond new phase 2 negotiation: 10.50.11.78[0]<=>10.50.11.77[0]
0d 00:28:12    iked     error    no policy found: 10.50.11.77/32[0] 10.50.11.78/32[0] proto=any dir=in ifIndex=3
0d 00:28:12    iked     error    failed to get proposal for responder.
0d 00:28:12    iked     error    failed to pre-process packet.
0d 00:28:12    iked     info     respond new phase 2 negotiation: 10.50.11.78[0]<=>10.50.11.77[0]
0d 00:28:12    iked     error    no policy found: 192.168.1.0/24[0] 192.168.3.0/24[0] proto=any dir=in ifIndex=3
0d 00:28:12    iked     error    failed to get proposal for responder.
0d 00:28:12    iked     error    failed to pre-process packet.
```

The following means that Phase 2 networks set in the Ingate are correctly set in the IX78:

```
0d 00:28:22    iked     info     respond new phase 2 negotiation: 10.50.11.78[0]<=>10.50.11.77[0]
0d 00:28:22    iked     info     suitable SP found:192.168.3.0/24[0] 192.168.1.0/24[0] proto=any dir=out ifIndex=3
0d 00:28:22    iplocal  info     Pfkey_Parse: *** Received getspi message of length 80 from IKED ***
0d 00:28:22    iplocal  info     Pfkey_Parse: Parsing successful, calling message handling routine for getspi message
0d 00:28:22    iplocal  info     IPv4 Address : 10.50.11.77
0d 00:28:22    iplocal  info     IPv4 Address : 10.50.11.78
```

The following means that the certificate uploaded to the IX78 could be in a bad format (DER) – regenerate the key on the Ingate under the certificates page and export it as PEM.

```
0d 00:53:00ikedinfoAES with key length 128.
0d 00:53:00ikederrorfailed to get peers CERT.
```

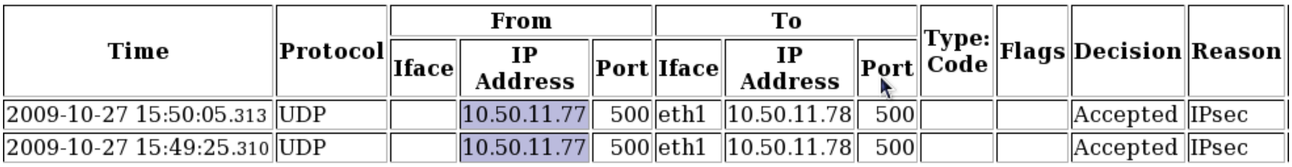
Regenerate the key on the Ingate under the certificates page and export it as PEM.

Errors and Troubleshooting in the logs – IG

Examining the Ingate logs is a good way to determine what is happening on the Ingate side also:

With “IP packets as selected” under the “Show This” section, display the log.

```
2009-10-27 15:50:05.313 UDP         10.50.11.77  500   eth1  10.50.11.78  500
             Accepted    IPsec
```



Time	Protocol	From			To			Type: Code	Flags	Decision	Reason
		Iface	IP Address	Port	Iface	IP Address	Port				
2009-10-27 15:50:05.313	UDP		10.50.11.77	500	eth1	10.50.11.78	500			Accepted	IPsec
2009-10-27 15:49:25.310	UDP		10.50.11.77	500	eth1	10.50.11.78	500			Accepted	IPsec

The above is the actual traffic. Not the content of the traffic. To see what's happening in IPsec, check the IPsec boxes especially the debug one, under “Show This”. Display the logs.

```
>>> Debug: IPsec: | ******emit ISAKMP Oakley attribute:
```

Lots of these mean that the two end-points are trying to negotiate a common encryption method.

```
>>> Debug: IPsec: | emitting length of ISAKMP Transform Payload (ISAKMP): 36
>>> Debug: IPsec: | emitting length of ISAKMP Proposal Payload: 312
>>> Debug: IPsec: | emitting length of ISAKMP Security Association Payload: 324
```

These mean they end points are trying to make a connection now.

```
>>> Debug: IPsec: | emitting 16 raw bytes of V_ID into ISAKMP Vendor ID Payload
>>> Debug: IPsec: | V_ID  4a 13 1c 81  07 03 58 45  5c 57 28 f2  0e 95 45 2f
>>> Debug: IPsec: | emitting length of ISAKMP Vendor ID Payload: 20
>>> Debug: IPsec: | out_vendorid(): sending [draft-ietf-ipsec-nat-t-ike-03]
```

These mean it's still attempting to build a tunnel.

```
>>> Debug: IPsec: |    next payload type: ISAKMP_NEXT_NONE
```

These mean the IG doesn't think it has found the right handshake for Phase 1 yet.:

```
>>> Notice: IPsec: "IX78-01.01" #1: max number of retransmissions (20) reached
STATE_MAIN_I1.  No response (or no acceptable response) to our first IKE message
```

This is bad. Something is wrong in the IG or IX configuration. Usually certificates.

These mean the IX and IG have correct certificates and can make a Phase 1 Tunnel:

```
>>> Notice: IPsec: "IX78-02.01" #25: transition from state STATE_QUICK_I1 to state STATE_QUICK_I2

>>> Notice: IPsec: "IX78-02.01" #25: STATE_QUICK_I2: sent QI2, IPsec SA established {ESP=>0x204734d2 <0x6fa0cf63 xfrm=AES_128-
HMAC_SHA1 NATD=none DPD=none}
```