How to configure virtual private network using a IPsec in a lan-to-lan tunnel

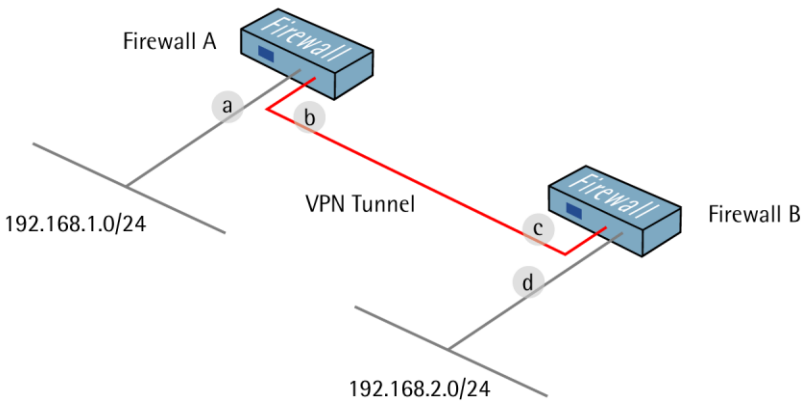
Create one lan-to-lan IPsec VPN tunnel between firewall A and B.

a IP: 192.168.1.1

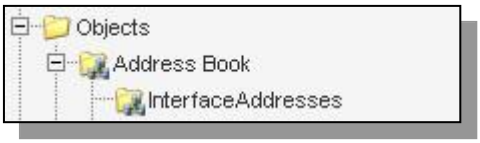
b IP: 192.168.110.1
Mask: 255.255.255.0
Gateway: 192.168.110.2

c IP: 192.168.110.2
Mask: 255.255.255.0
Gateway: 192.168.110.1

d IP: 192.168.2.1



1. Firewall A - Addresses



Go to *Objects -> Address book -> InterfaceAddresses*.
Edit the following items:
Change **lan_ip** to **192.168.1.1**
Change **lannet** to **192.168.1.0/24**

Change **wan1_ip** to **192.168.110.1**
Change **wan1net** to **192.168.110.0/24**

Go to *Objects -> Address book*.

Add a new Address Folder called **RemoteHosts**.

In the new folder, add a new IP address:
Name: **fwB-remotenet**
IP Address: **192.168.2.0/24**

Click Ok

In the same folder, add a new IP address:
Name: **fwB-remotegw**
IP Address: **192.168.110.2**

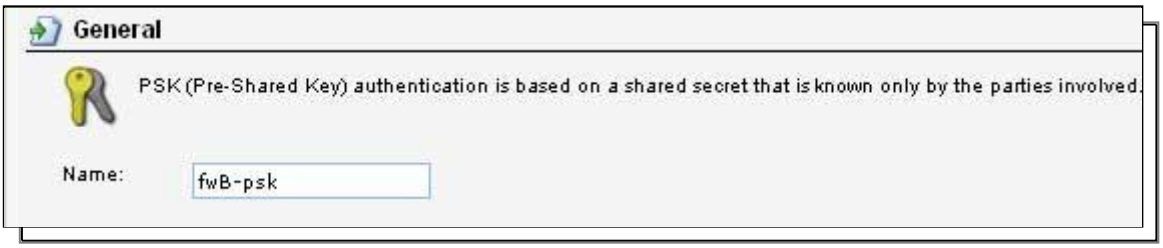
Click Ok

2. Firewall A - Pre-shared keys

Go to *Objects -> Authentication Objects*

Add a new Pre-Shared Key.

General:



Name: **fwB-psk**

Shared secret:

Select Passphrase and enter a shared secret

Click Ok.

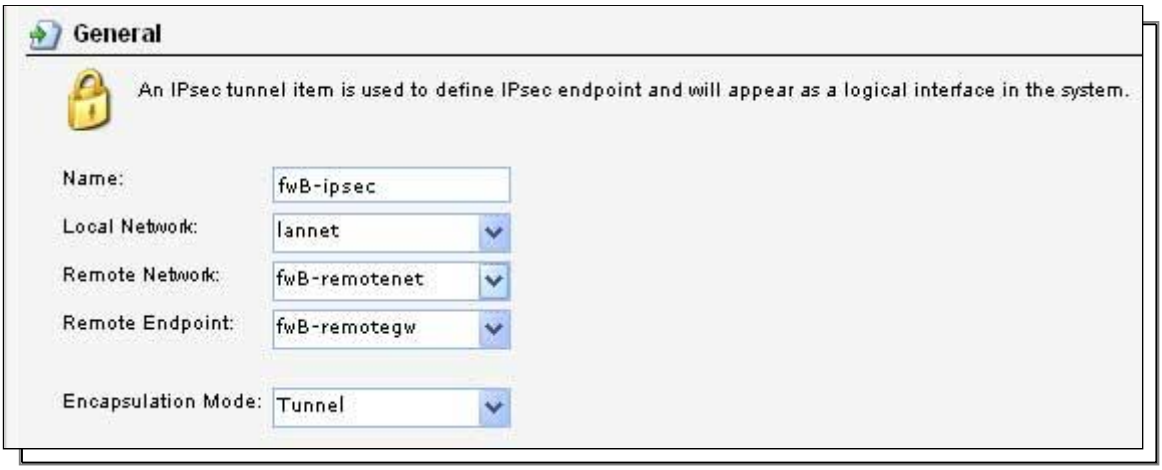
3. Firewall A - IPsec interface

Go to *Interfaces -> IPsec*.

Add a new IPsec Tunnel.

In the General tab:

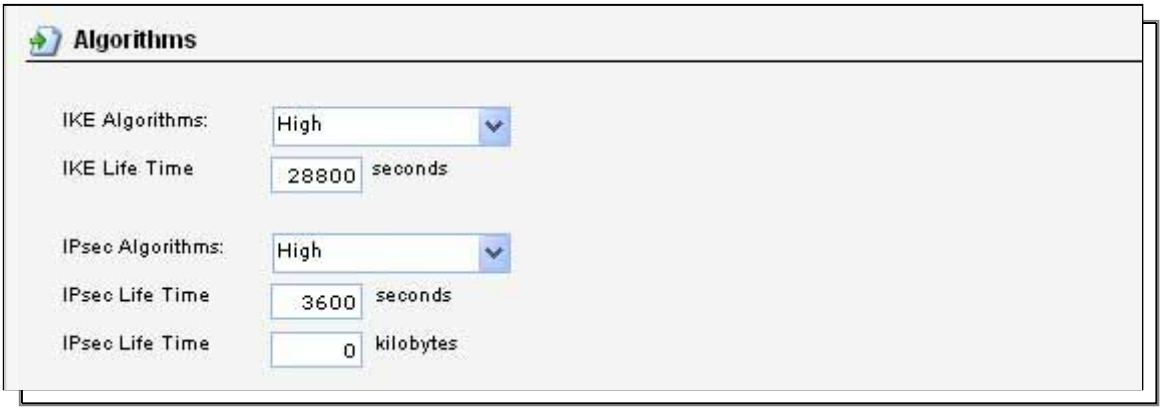
General:



Name: **`fwB-ipsec`**
Local Network: **`lannet`**
Remote Network: **`fwB-remotenet`**
Remote Endpoint: **`fwB-remotegw`**

Encapsulation Mode: **`Tunnel`**

Algorithms:



IKE Algorithms: **High**
IKE Life Time: **28800**
IPsec Algorithms: **High**
IPsec Life Time: **3600**
IPsec Life Time: **0**

In the Authentication tab:

Authentication:

Select **Pre-Shared Key** and **fwB-psk.**

Click Ok.

4. Firewall A - Rules

Go to *Rules -> IP Rules.*

Create a new IP Rules Folder called **lan_to_fwB-ipsec**

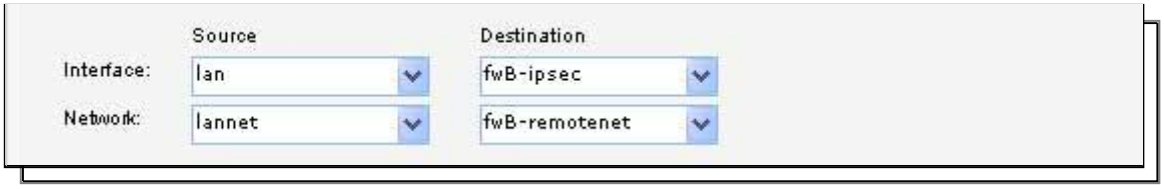
In the new folder, create a new IP Rule.

In the General tab:

General:

Name: **allow_all**
Action: **Allow**
Service: **all_services**

Address Filter:



Source Interface: **lan**
Source Network: **lannet**
Destination Interface: **fwB-ipsec**
Destination Network: **fwB-remotenet**

Click Ok.

Create a second rule in the same folder.

In the General tab:

General:

Name: **allow_all**
Action: **Allow**
Service: **all_services**

Address Filter:

Source Interface: **fwB-ipsec**
Source Network: **fwB-remotenet**
Destination Interface: **lan**
Destination Network: **lannet**

Click Ok.

Save and activate the configuration on firewall A.

5. Firewall B - Addresses

Go to *Objects -> Address book -> InterfaceAddresses*.
Edit the following items:
Change **lan_ip** to **192.168.2.1**
Change **lannet** to **192.168.2.0/24**

Change **wan1_ip** to **192.168.110.2**
Change **wan1net** to **192.168.110.0/24**

Go to *Objects -> Address book*.

Add a new Address Folder called **RemoteHosts**.

In the new folder, add a new IP4 address:
Name: **fwA-remotenet**
IP Address: **192.168.1.0/24**

Click Ok

In the same folder, add a new IP4 address:
Name: **fwA-remotegw**
IP Address: **192.168.110.1**

Click Ok

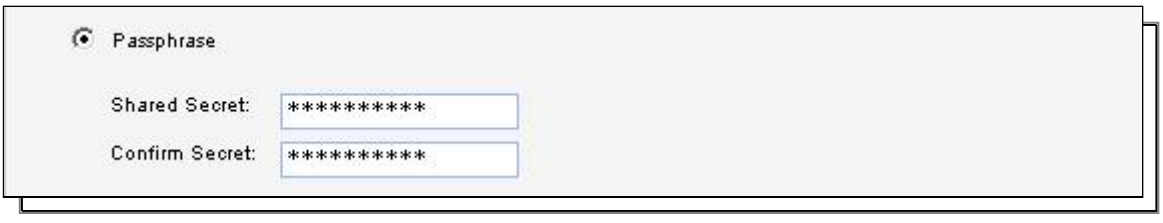
6. Firewall B - Pre-shared keys

Go to *Objects -> Authentication Objects*.

Add a new Pre-Shared Key.

General:
Name: **fwA-psk**

Shared secret:



Select Passphrase and enter a shared secret

Click Ok.

7. Firewall B - IPsec interface

Go to *Interfaces -> IPsec*.

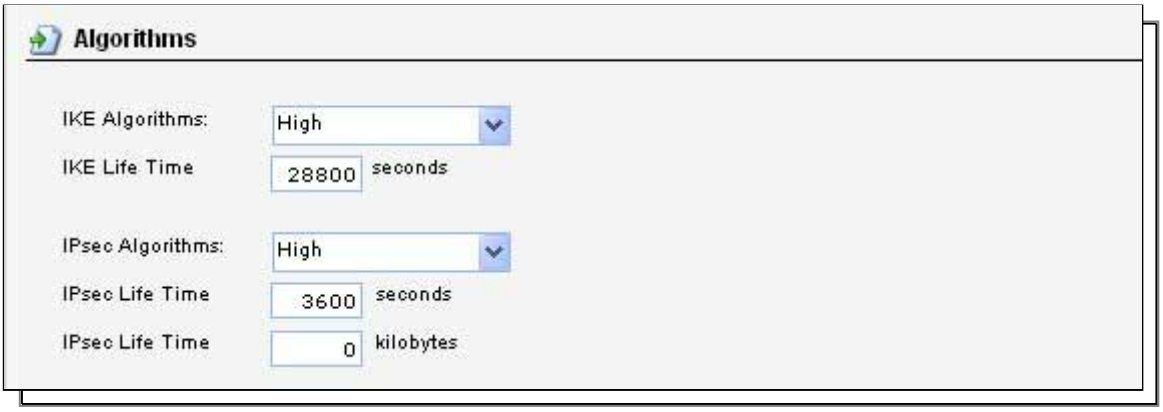
Add a new IPsec Tunnel.

In the General tab:

General:
Name: **fwA-ipsec**
Local Network: **lannet**
Remote Network: **fwA-remotenet**
Remote Endpoint: **fwA-remotegw**

Encapsulation Mode: **Tunnel**

Algorithms:



IKE Algorithms: **High**
IKE Life Time: **28800**
IPsec Algorithms: **High**
IPsec Life Time: **3600**
IPsec Life Time: **0**

In the Authentication tab:

Authentication:
Select **Pre-Shared Key** and **fwA-psk.**

Click Ok.

8. Firewall B - Rules

Go to *Rules -> IP Rules*.

Create a new IP Rules Folder called **lan_to_fwA-ipsec**

In the new folder, create a new IP Rule.

In the General tab:

General:

Name: **allow_all**
Action: **Allow**
Service: **all_services**

Address Filter:
Source Interface: **lan**
Source Network: **lannet**
Destination Interface: **fwA-ipsec**
Destination Network: **fwA-remotenet**

Click Ok.

Create a second rule in the same folder.

In the General tab:

General:
Name: **allow_all**
Action: **Allow**
Service: **all_services**

Address Filter:
Source Interface: **fwA-ipsec**
Source Network: **fwA-remotenet**
Destination Interface: **lan**
Destination Network: **lannet**

Click Ok.

Save and activate the configuration on firewall B.