

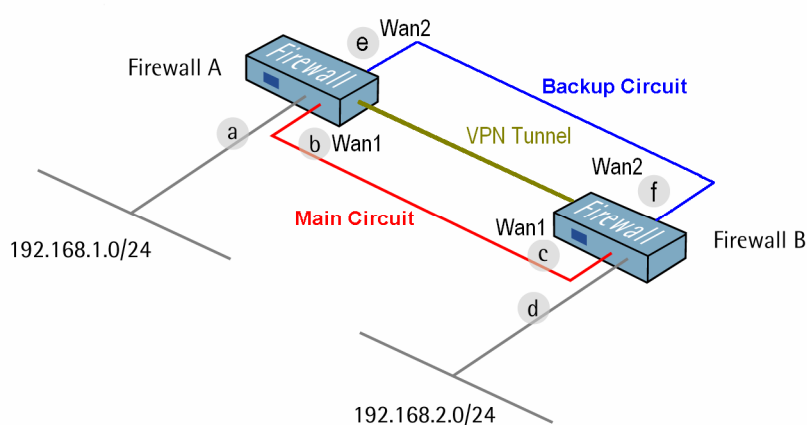
How to configure IPSec VPN failover

This scenario shows how both firewalls can be configured IPSec VPN failover between two WAN links. Either of WAN links is broken, all VPN traffic will be on-line redirected to other backup circuit. When the failed circuit returns to normal, these services will come back to original WAN circuit.

Detail for this scenario:

- Both firewalls are all built two WAN links for failover mechanism. One is **main circuit** and another one is **backup circuit**.
- All Traffic between **Firewall A** and **Firewall B** will be via an IPSec VPN tunnel.

- a IP: 192.168.1.1
- b IP: 192.168.110.1
Mask: 255.255.255.0
Gateway: 192.168.110.254
- c IP: 192.168.110.254
Mask: 255.255.255.0
Gateway: 192.168.110.1
- d IP: 192.168.2.1
- e IP: 192.168.120.1
Mask: 255.255.255.0
Gateway: 192.168.210.254
- f IP: 192.168.120.254
Mask: 255.255.255.0
Gateway: 192.168.120.1



1. Firewall A - Address.

Go to *Objects ->Address book -> InterfaceAddresses*:



Edit the following items:

Change **lan_ip** to **192.168.1.1**

Change **lanet** to **192.168.1.0/24**

Change **wan1_ip** to **192.168.110.1**

Change **wan1net** to **192.168.110.0/24**

Change **wan2_ip** to **192.168.120.1**

Change **wan2net** to **192.168.120.0/24**

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

In the new folder, add following new IP Address objects

Name: **fwB-IPSec-remote-net**

IP Address: **192.168.2.0/24**

Name: **fwB-main-remote-gw**

IP Address: **192.168.110.254**

Name: **fwB-backup-remote-gw**

IP Address: **192.168.120.254**

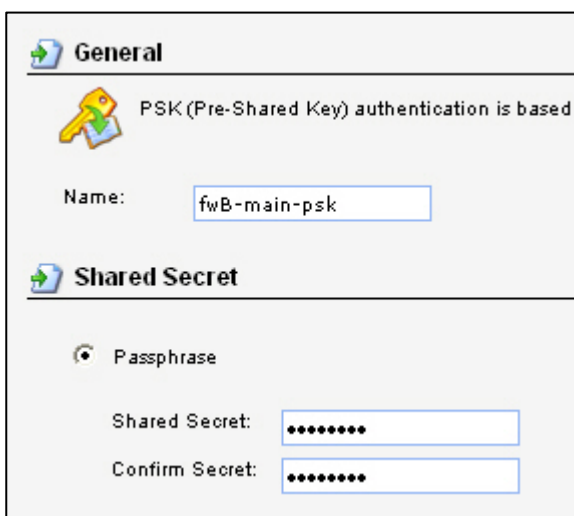
Click **OK**.



2. Firewall A - Pre-shared keys

Go to *Objects -> Authentication Objects -> Pre-Shared keys*.

Add following new Pre-Shared Key for both IPSec tunnels.



General

PSK (Pre-Shared Key) authentication is based

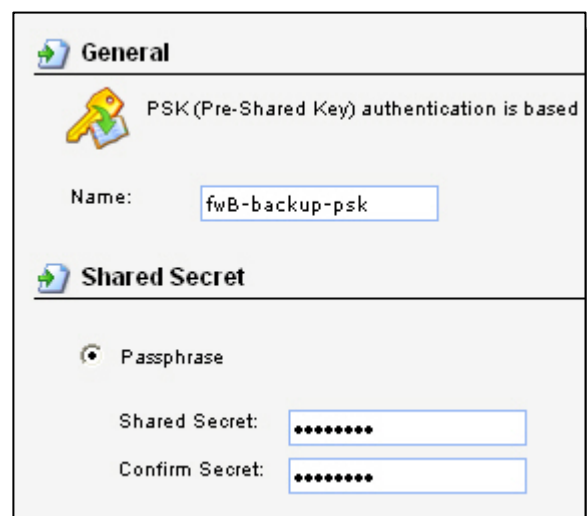
Name:

Shared Secret

Passphrase

Shared Secret:

Confirm Secret:



General

PSK (Pre-Shared Key) authentication is based

Name:

Shared Secret

Passphrase

Shared Secret:

Confirm Secret:

General:

Name: **fwB-main-psk**

Name: **fwB-backup-psk**

Shared secret:

Select **Passphrase** and enter a shared secret in above Pre-shared key objects

Click **Ok**.

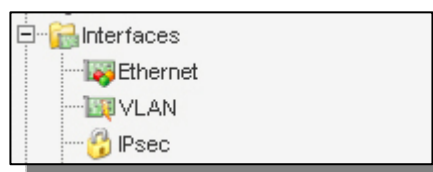
3. Firewall A - Main IPsec interface

Create a Main IPsec Tunnel:

Go to **Interfaces -> IPsec**.

Add a new **IPsec Tunnel** for Main WAN link.

In the **General** tab:



General:

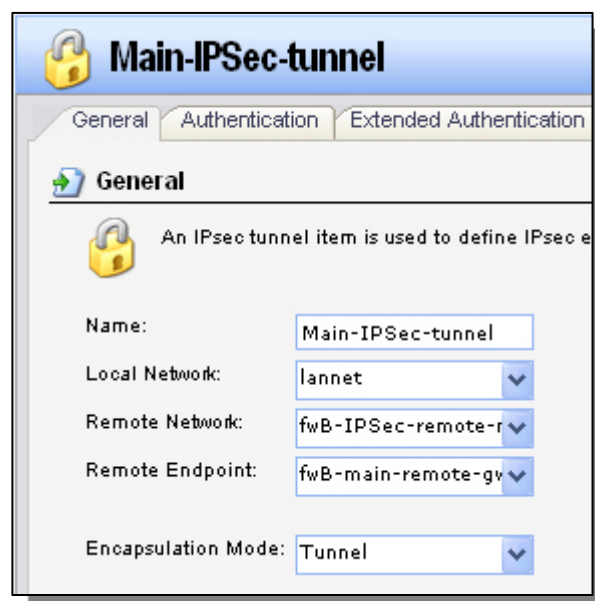
Name: *Main-IPSec-tunnel*

Local Network: *lanet*

Remote Network: *fwB-IPSec-remote-net*

Remote Endpoint: *fwB-main-remote-gw*

Encapsulation Mode: **Tunnel**



Algorithms:

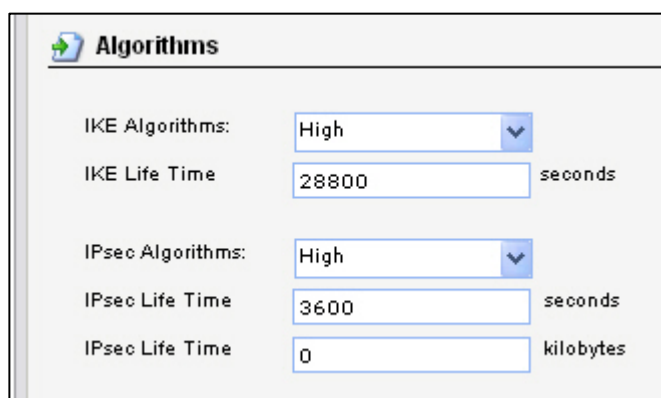
IKE Algorithms: **High**

IKE Life Time: **28800**

IPsec Algorithms: **High**

IPsec Life Time: **3600**

IPsec Life Time: **0**



Authentication:

Pre-shared Key
Pre-shared Key:

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

Keep-alive:

Main-IPSec-tunnel

General Authentication Extended Authentication (XAuth) Routing IKE Settings Keep-alive Advanced

Keep-alive

IPsec keep-alives makes sure that an IPsec tunnel stays established at all times by continuously sending ICMP pings through establishing it if necessary. Note that this will only work on LAN to LAN tunnels, i.e. where the remote gateway is a single IP.

Disabled
 Auto
 Manually configured IP addresses

Source IP Address:
Destination IP Address:

Select **Auto**.

Advanced:

Main-IPSec-tunnel

General Authentication Extended Authentication (XAuth) Routing IKE Settings Keep-alive Advanced

Automatic Route Creation

Automatically add route for remote network.

Add route for remote network

Route Metric:

Make sure the “**Add route for remote network**” option is unchecked since this route without Monitoring feature.

Click **Ok**.

4. Firewall A - Combine IPSec and Lan interfaces

Go to *Interfaces* -> *Interface Groups*.

Add a new InterfaceGroup :

InterfaceGroup

General

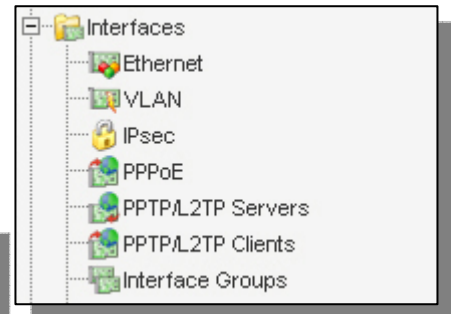
Use an interface group to combine several interfaces for a simplified security configuration.

Name:

Security/Transport Equivalent

Interfaces

Available	Selected
any	Backup-IPSec-tunnel
core	lan
dmz	Main-IPSec-tunnel
wan1	
wan2	



Name: IPSec-Lan-Group

Selected Interface:

Backup-IPSec-tunnel

Main-IPSec-tunnel

Lan

Click Ok.

5. 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:



IP Rule

General Log Settings NAT SAT SAT Server Load Balancing

General

An IP rule specifies what action to perform on network traffic that matches the rule.

Name:

Action:

Service:

Schedule:

Address Filter

Specify source interface and source network, together with destination interface and destination network, for the rule to match.

	Source	Destination
Interface:	<input type="text" value="IPSec-Lan-Group"/>	<input type="text" value="IPSec-Lan-Group"/>
Network:	<input type="text" value="all-nets"/>	<input type="text" value="all-nets"/>

Name: **allow_Lan_to_fwB-IPSec**

Action: **Allow**

Service: **all_services**

Source Interface: **IPSec-Lan-Group**

Source Network: **all-nets**

Destination Interface: **IPSec-Lan-Group**

Destination Network: **all-nets**

Click Ok.

6. Firewall A - Manually add route for interface monitoring

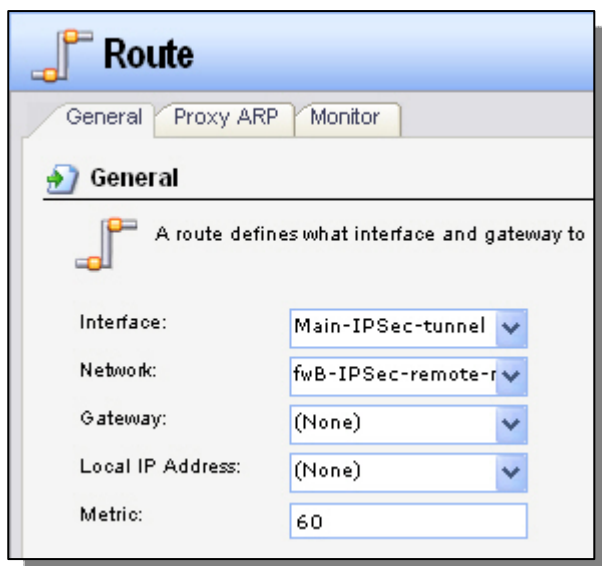
Go to *Routing* -> *Routing Tables*.

Click main routing table

Add a new Route for main IPsec tunnel

In the *General* tab:

General:



Route

General Proxy ARP Monitor

General

A route defines what interface and gateway to

Interface: Main-IPSec-tunnel

Network: fwB-IPSec-remote-r

Gateway: (None)

Local IP Address: (None)

Metric: 60

Interface: Main-IPSec-tunnel

Network: fwB-IPSec-remote-net

Metric: 60

In the *Monitor* tab:

Monitor:



Route

General Proxy ARP Monitor

Monitoring for Route Failover

The health of a route may be monitored for route failover purposes.

Monitor This Route

Method

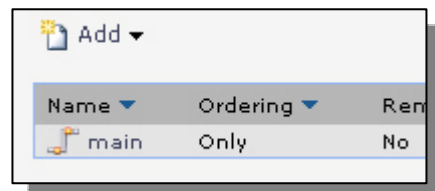
Monitor Interface Link Status

Monitor Gateway Using ARP Lookup

Manual ARP Lookup Interval: 1000 milliseconds

Make sure the “Monitor This Route” and “Monitor Interface Link Status” option is enabled.

Click **Ok**.

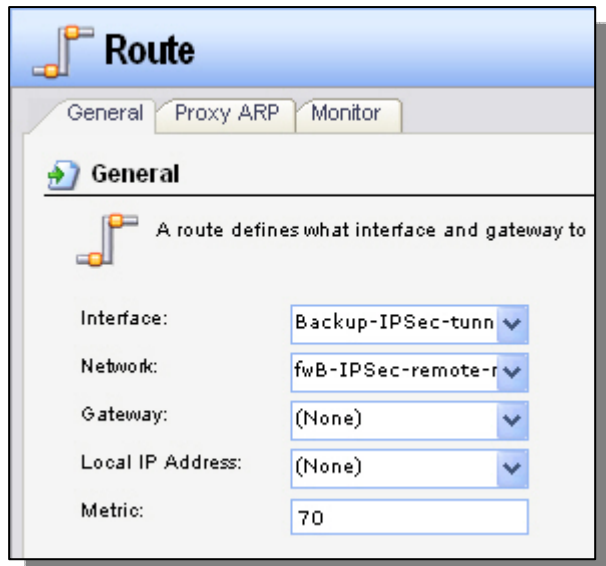


Create a second Route for backup IPSec tunnel



In the General tab:

General:



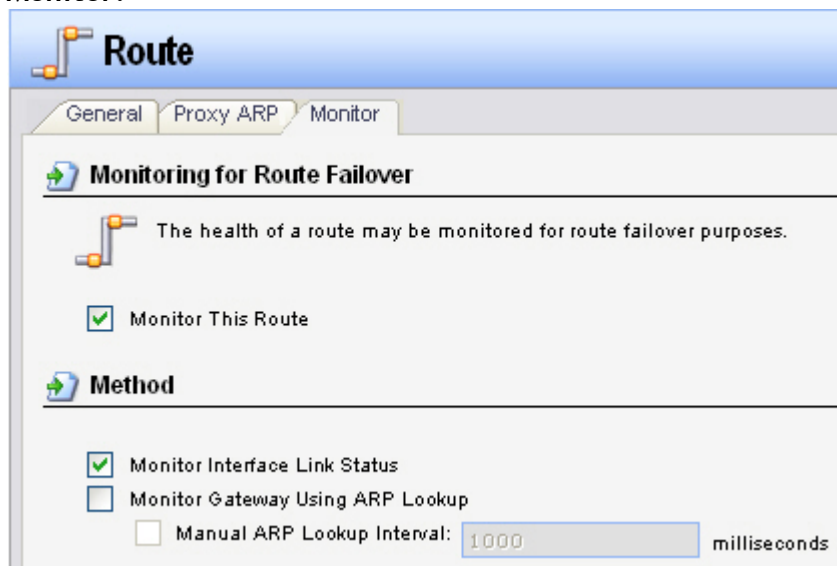
Interface: **Backup-IPSec-tunnel**

Network: **fwB-IPSec-remote-net**

Metric: **70**

In the Monitor tab:

Monitor:



Make sure the “**Monitor This Route**” and “**Monitor Interface Link Status**” option is enabled.

Click Ok.

Save and activate the configuration on firewall A.

7. Firewall B - Address.

Go to *Objects ->Address book -> InterfaceAddresses*:



Edit the following items:

Change **lan_ip** to **192.168.2.1**

Change **lanet** to **192.168.2.0/24**

Change **wan1_ip** to **192.168.110.254**

Change **wan1net** to **192.168.110.0/24**

Change **wan2_ip** to **192.168.120.254**

Change **wan2net** to **192.168.120.0/24**

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

In the new folder, add following new IP Address objects

Name: **fwA-IPSec-remote-net**

IP Address: **192.168.1.0/24**

Name: **fwA-main-remote-gw**

IP Address: **192.168.110.1**

Name: **fwA-backup-remote-gw**

IP Address: **192.168.120.1**

Click **OK**.



8. Firewall B - Pre-shared keys

Go to *Objects -> Authentication Objects -> Pre-Shared keys*.

Add following new Pre-Shared Key for both IPSec tunnels.

General

PSK (Pre-Shared Key) authentication is based

Name:

Shared Secret

Passphrase

Shared Secret:

Confirm Secret:

General

PSK (Pre-Shared Key) authentication is based

Name:

Shared Secret

Passphrase

Shared Secret:

Confirm Secret:

General:

Name: **fwA-main-psk**

Name: **fwA-backup-psk**

Shared secret:

Select **Passphrase** and enter a shared secret in above Pre-shared key objects

Click **Ok**.

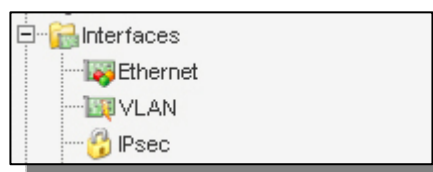
9. Firewall B - Main IPsec interface

Create a Main IPsec Tunnel:

Go to **Interfaces** -> **IPsec**.

Add a new **IPsec Tunnel** for Main WAN link.

In the **General** tab:



General:

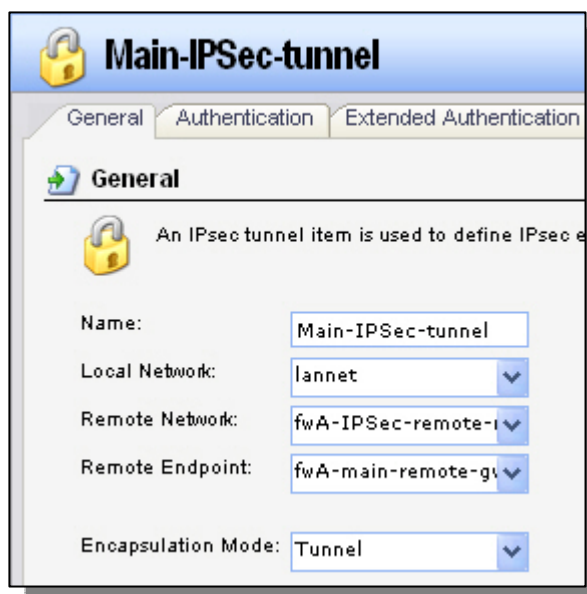
Name: *Main-IPSec-tunnel*

Local Network: *lanet*

Remote Network: *fwA-IPSec-remote-net*

Remote Endpoint: *fwA-main-remote-gw*

Encapsulation Mode: *Tunnel*



Algorithms:

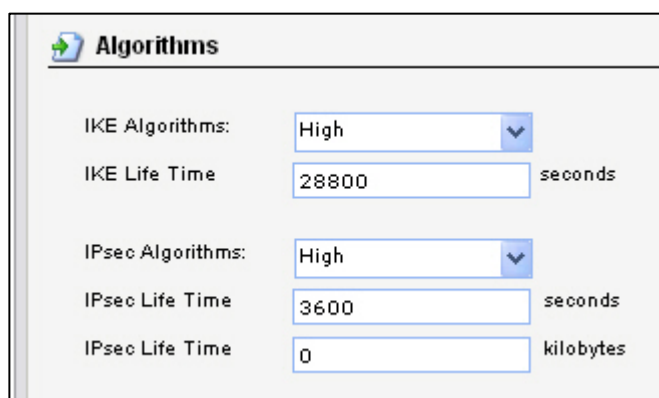
IKE Algorithms: *High*

IKE Life Time: *28800*

IPsec Algorithms: *High*

IPsec Life Time: *3600*

IPsec Life Time: *0*



Authentication:

Pre-shared Key
Pre-shared Key:

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

Keep-alive:

Main-IPSec-tunnel

General Authentication Extended Authentication (XAuth) Routing IKE Settings Keep-alive Advanced

Keep-alive

IPsec keep-alives makes sure that an IPsec tunnel stays established at all times by continuously sending ICMP pings through the tunnel and re-establishing it if necessary. Note that this will only work on LAN to LAN tunnels, i.e. where the remote gateway is a single IP address.

Disabled
 Auto
 Manually configured IP addresses

Source IP Address:
Destination IP Address:

Select **Auto**.

Advanced:

Main-IPSec-tunnel

General Authentication Extended Authentication (XAuth) Routing IKE Settings Keep-alive Advanced

Automatic Route Creation

Automatically add route for remote network.

Add route for remote network

Route Metric:

Make sure the “**Add route for remote network**” option is unchecked since this route without Monitoring feature.

Click **Ok**.

10. Firewall B - Combine IPSec and Lan interfaces

Go to *Interfaces* -> *Interface Groups*.

Add a new InterfaceGroup :

InterfaceGroup

General

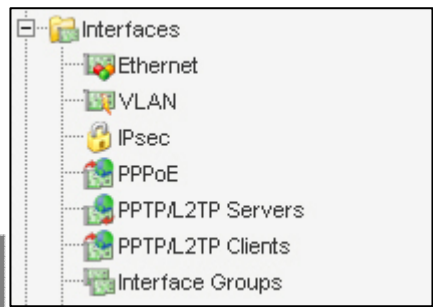
Use an interface group to combine several interfaces for a simplified security configuration.

Name:

Security/Transport Equivalent

Interfaces

Available	Selected
any	Backup-IPSec-tunnel
core	lan
dmz	Main-IPSec-tunnel
wan1	
wan2	



Name: **IPSec-Lan-Group**

Selected Interface:

Backup-IPSec-tunnel

Main-IPSec-tunnel

Lan

Click Ok.

11. Firewall B - Rules

Go to *Rules* -> *IP Rules*.

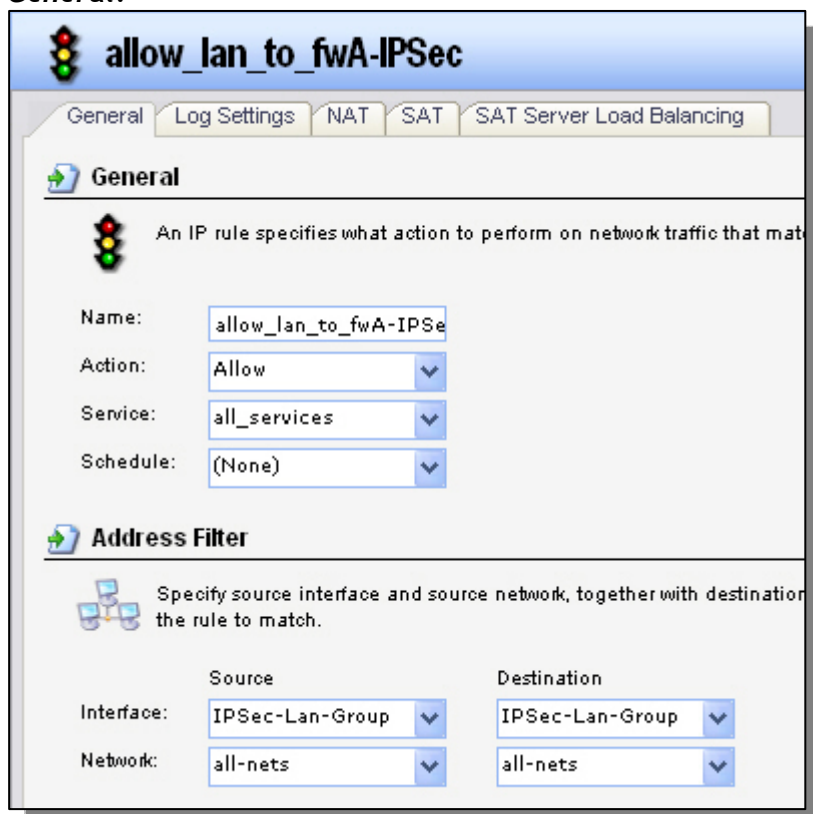


Create a new IP Rules Folder called `lan_to_fwA-IPSec`

In the new folder, create a new IP Rule.

In the **General** tab:

General:



The screenshot shows the configuration window for a new IP rule named 'allow_lan_to_fwA-IPSec'. The 'General' tab is selected, and the configuration is as follows:

Field	Value
Name	allow_lan_to_fwA-IPSec
Action	Allow
Service	all_services
Schedule	(None)

Address Filter	
Interface	IPSec-Lan-Group
Network	all-nets
Destination Interface	IPSec-Lan-Group
Destination Network	all-nets

Name: `allow_Lan_to_fwA-IPSec`

Action: **Allow**

Service: `all_services`

Source Interface: `IPSec-Lan-Group`

Source Network: `all-nets`

Destination Interface: `IPSec-Lan-Group`

Destination Network: `all-nets`

Click Ok.

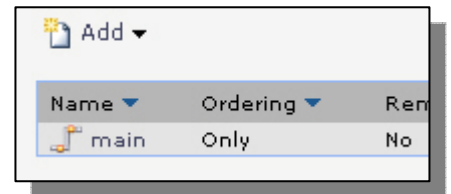
12. Firewall B - Manually add route for interface monitoring

Go to *Routing* -> *Routing Tables*.

Click main routing table



Add a new Route for main IPsec tunnel

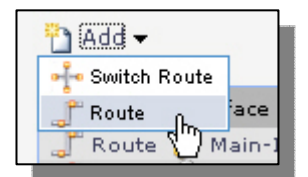


In the *General* tab:

General:

The 'Route' configuration page, General tab. The interface shows the following settings:

- Interface: Main-IPSec-tunnel
- Network: fwA-IPSec-remote-net
- Gateway: (None)
- Local IP Address: (None)
- Metric: 60



Interface: Main-IPSec-tunnel

Network: fwA-IPSec-remote-net

Metric: 60

In the *Monitor* tab:

Monitor:

The 'Route' configuration page, Monitor tab. The interface shows the following settings:

- Monitor This Route
- Monitor Interface Link Status
- Monitor Gateway Using ARP Lookup
- Manual ARP Lookup Interval: 1000 milliseconds

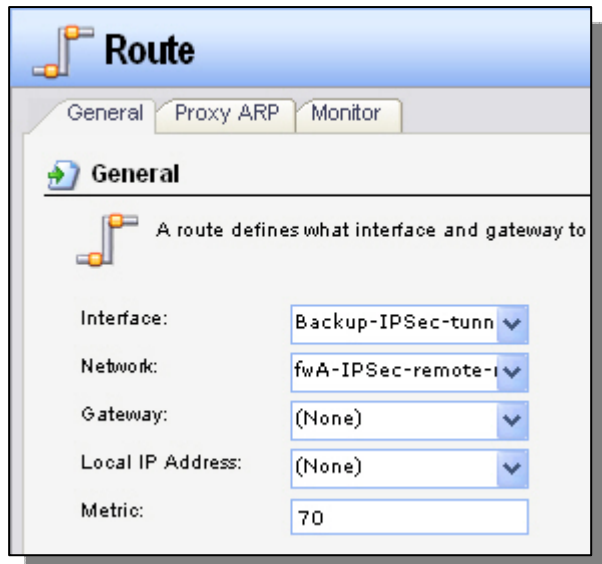
Make sure the "Monitor This Route" and "Monitor Interface Link Status" option is enabled. Click **Ok**.

Create a second Route for backup IPSec tunnel



In the General tab:

General:



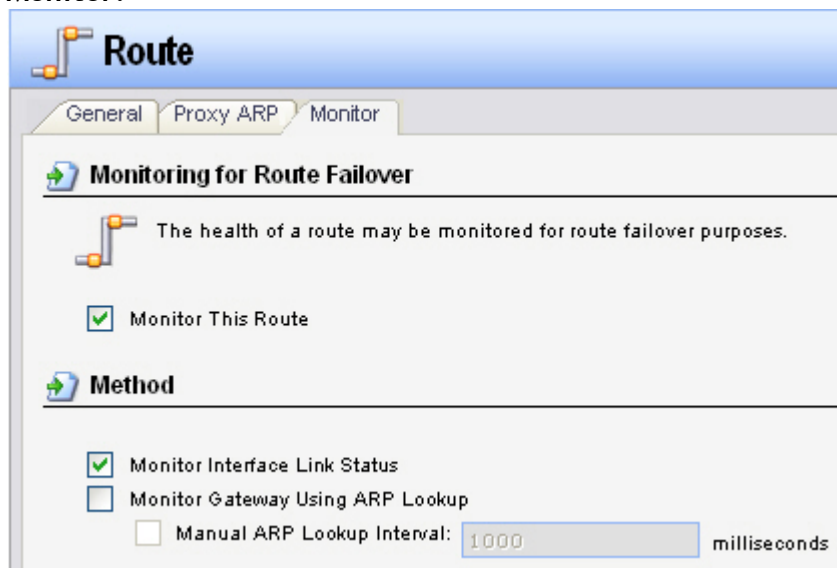
Interface: **Backup-IPSec-tunnel**

Network: **fwA-IPSec-remote-net**

Metric: **70**

In the Monitor tab:

Monitor:



Make sure the “Monitor This Route” and “Monitor Interface Link Status” option is enabled.

Click Ok.

Save and activate the configuration on firewall B.