Configuration examples for the D-Link NetDefend Firewall series

Scenario: How to configure IPSec VPN Failover

Platform Compatibility: All NetDefend Firewall Series

Last update: 2008-03-07

Overview

In this document, the notation *Objects->Address book* means that in the tree on the left side of the screen **Objects** first should be clicked (expanded) and then **Address Book**.

Most of the examples in this document are adapted for the DFL-800. The same settings can easily be used for all other models in the series. The only difference is the names of the interfaces. Since the DFL-1600 and DFL-2500 has more than one lan interface, the lan interfaces are named lan1, lan2 and lan3 not just lan.

The screenshots in this document is from firmware version 2.11.02. If you are using an earlier version of the firmware, the screenshots may not be identical to what you see on your browser.

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.

Note:

In this scenario, it supposed all of Wan ports to be using static IP address. Please make sure the DHCP client is uncheck on Ethernet/Wan interface page for both firewalls.

a IP: 192.168.1.1

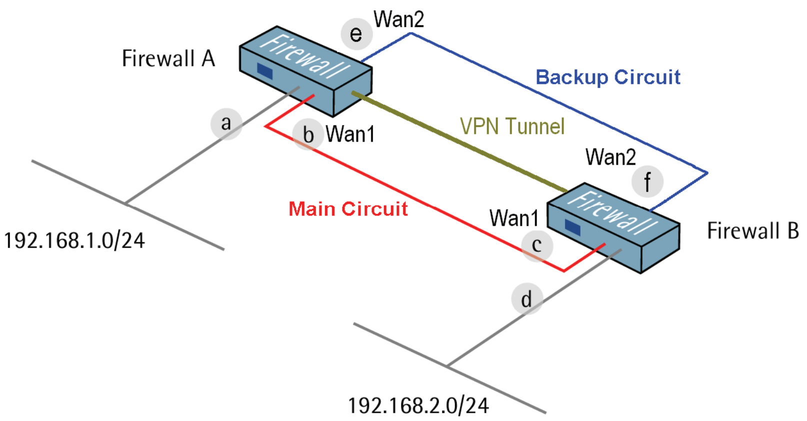
b IP: 192.168.110.1
Mask: 255.255.255.0
Gateway: 192.168.110.254

c IP: 192.168.110.254
Mask: 255.255.255.0
Gateway: 192.168.110.1

d IP: 192.168.2.1

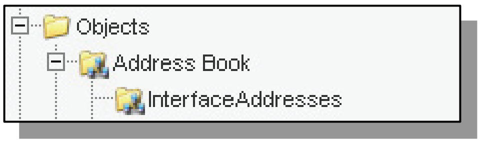
e IP: 192.168.120.1
Mask: 255.255.255.0
Gateway: 192.168.210.254

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 **lannet** to **192.168.1.0/24**

Change **wan1_ip** to **192.168.110.1**
Change **wan1net** to **192.168.110.0/24**
Change **Wan1_gw** to **192.168.110.254** (If this object does not exist, create a new one)

Change **wan2_ip** to **192.168.120.1**
Change **wan2net** to **192.168.120.0/24**
Change **Wan2_gw** to **192.168.120.254** (If this object does not exist, create a new one)

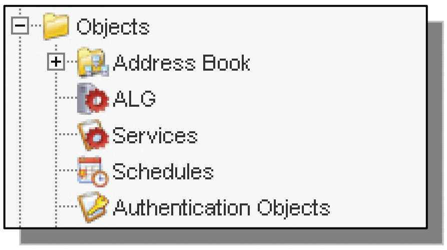
Add a new Address Folder called RemoteHosts.

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**

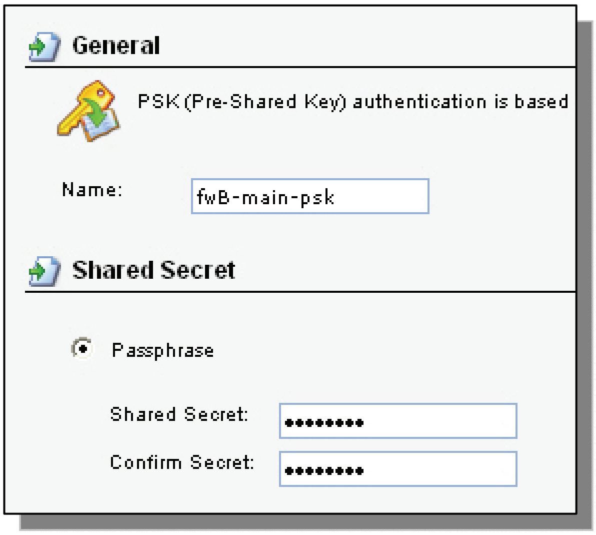
Click OK.



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

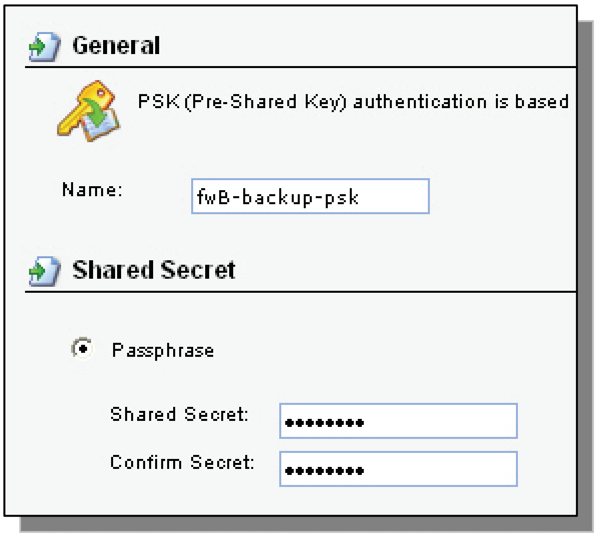
Name: fwB-main-psk

Shared Secret

● Passphrase

Shared Secret: •••••••••

Confirm Secret: •••••••••



General

PSK (Pre-Shared Key) authentication is based

Name: fwB-backup-psk

Shared Secret

● Passphrase

Shared Secret: •••••••••

Confirm Secret: •••••••••

General:

Name: **fwB-main-psk**
Name: **fwB-backup-psk**

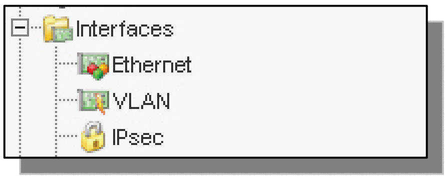
Shared secret:
Select Passphrase and enter a shared secret in above Pre-shared key objects

Click Ok.

3. Firewall A - Main IPsec interface

Create a Main IPSec Tunnel:

Go to *Interfaces -> IPsec*.

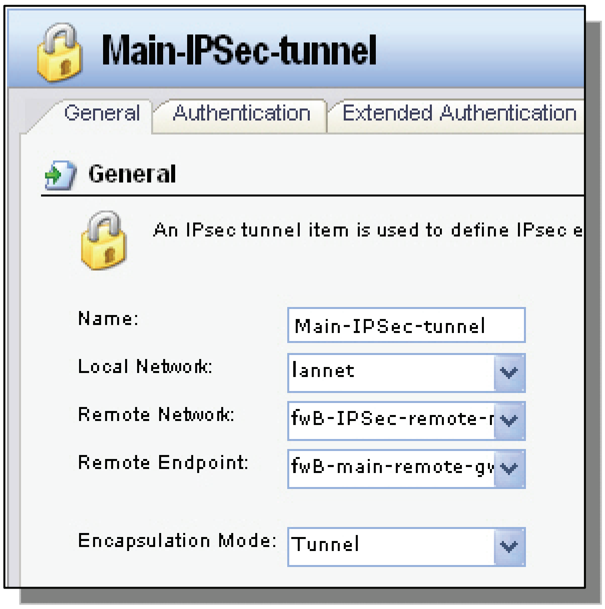


Add a new IPsec Tunnel `for Main WAN link`.

In the General tab:

General:
Name: ***Main-IPSec-tunnel***
Local Network: **lannet**
Remote Network: **fwB-IPSec-remote-net**
Remote Endpoint: **fwB-main-remote-gw**

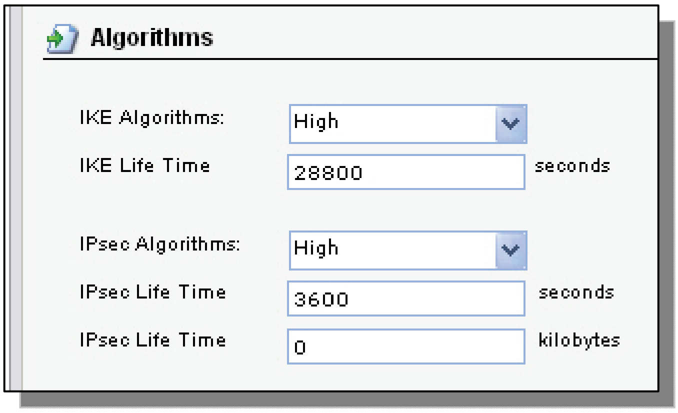
Encapsulation Mode: **Tunnel**



An IPsec tunnel item is used to define IPsec e

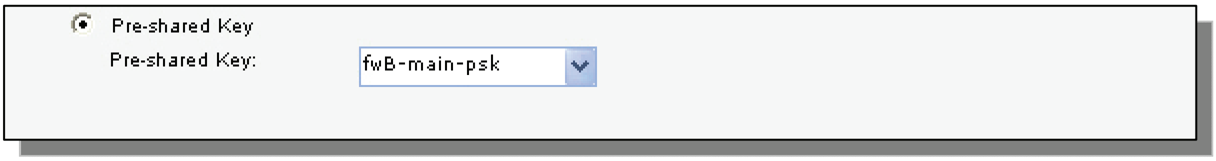
Name: Main-IPSec-tunnel
Local Network: lannet
Remote Network: fwB-IPSec-remote-r
Remote Endpoint: fwB-main-remote-gv
Encapsulation Mode: Tunnel

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



IKE Algorithms: High
IKE Life Time 28800 seconds
IPsec Algorithms: High
IPsec Life Time 3600 seconds
IPsec Life Time 0 kilobytes

Authentication:

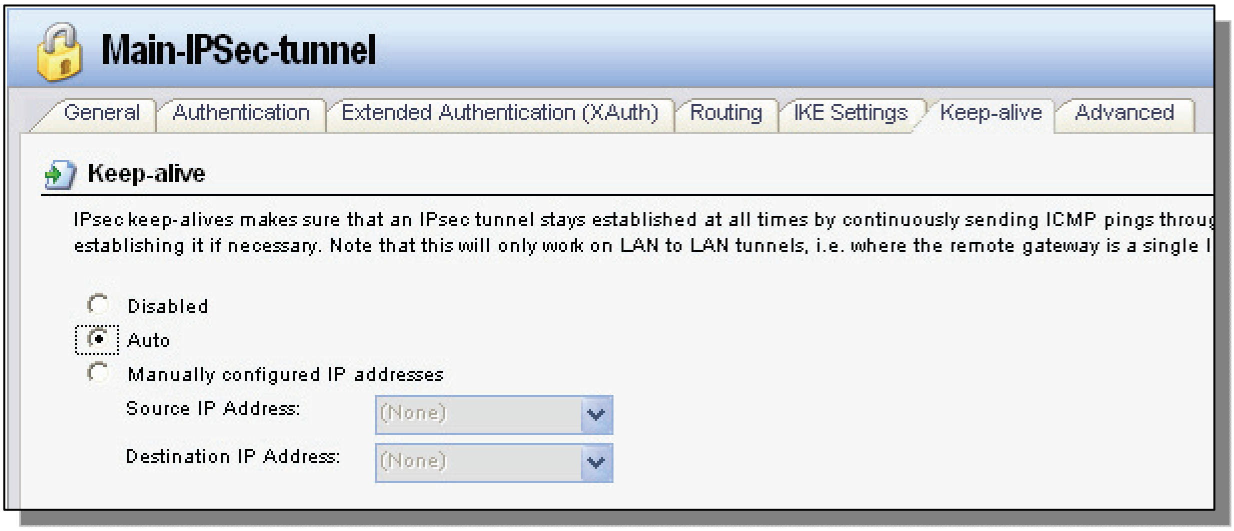


● Pre-shared Key

Pre-shared Key: fwB-main-psk

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

Keep-alive:



Keep-alive

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

○ Disabled

● Auto

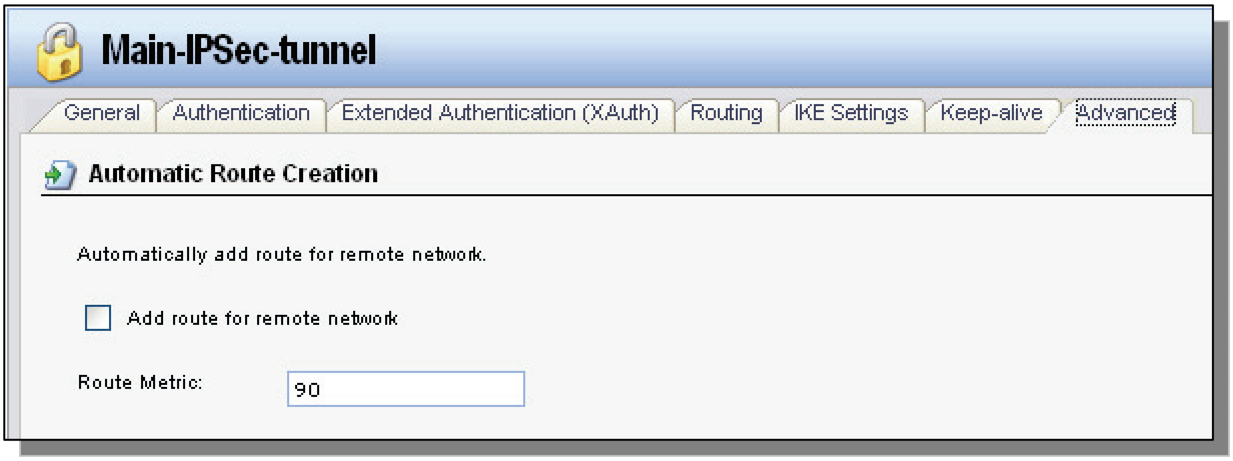
○ Manually configured IP addresses

Source IP Address: (None)

Destination IP Address: (None)

Select **Auto**.

Advanced:



Automatic Route Creation

Automatically add route for remote network.

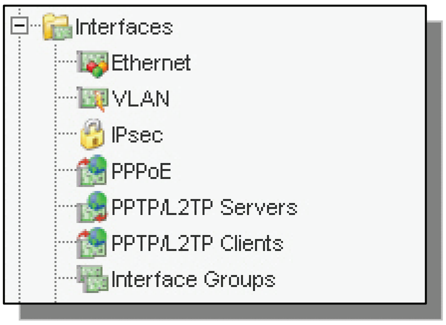
□ Add route for remote network

Route Metric: 90

Make sure the "**Add route for remote network**" option is uncheck since this route without Monitoring feature.

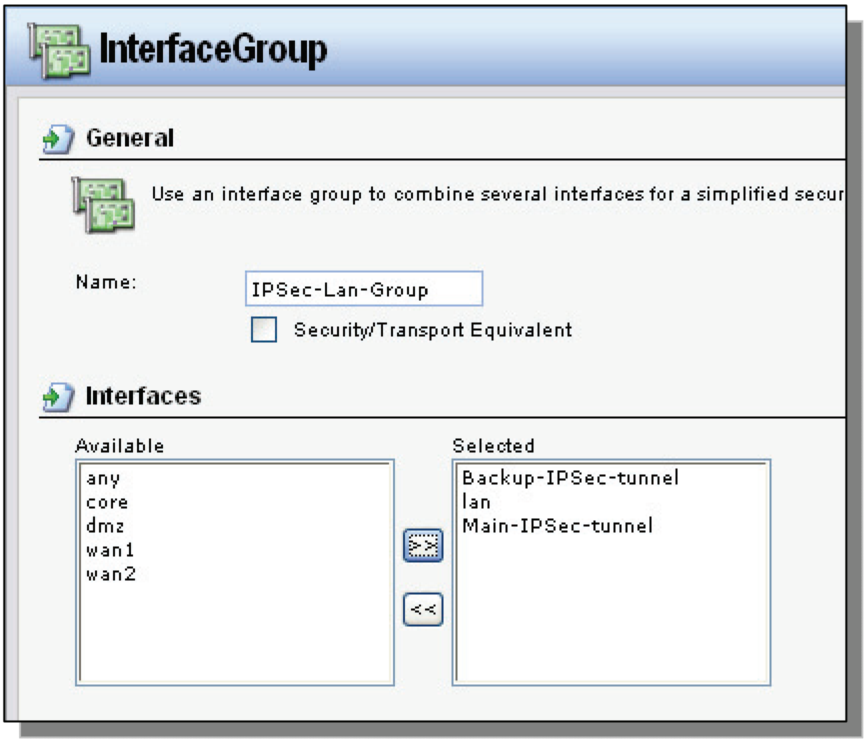
Click Ok.

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 secur

Name: IPSec-Lan-Group

□ Security/Transport Equivalent

Interfaces

Available: any, core, dmz, wan1, wan2

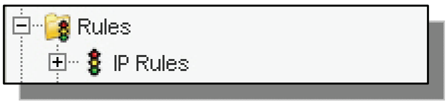
Selected: Backup-IPSec-tunnel, lan, Main-IPSec-tunnel

Name: **`IPSec-Lan-Group`**
Selected Interface:

  `Backup-IPSec-tunnel`
  `Main-IPSec-tunnel`
  `Lan`

Click Ok.

5. Firewall A - Rules



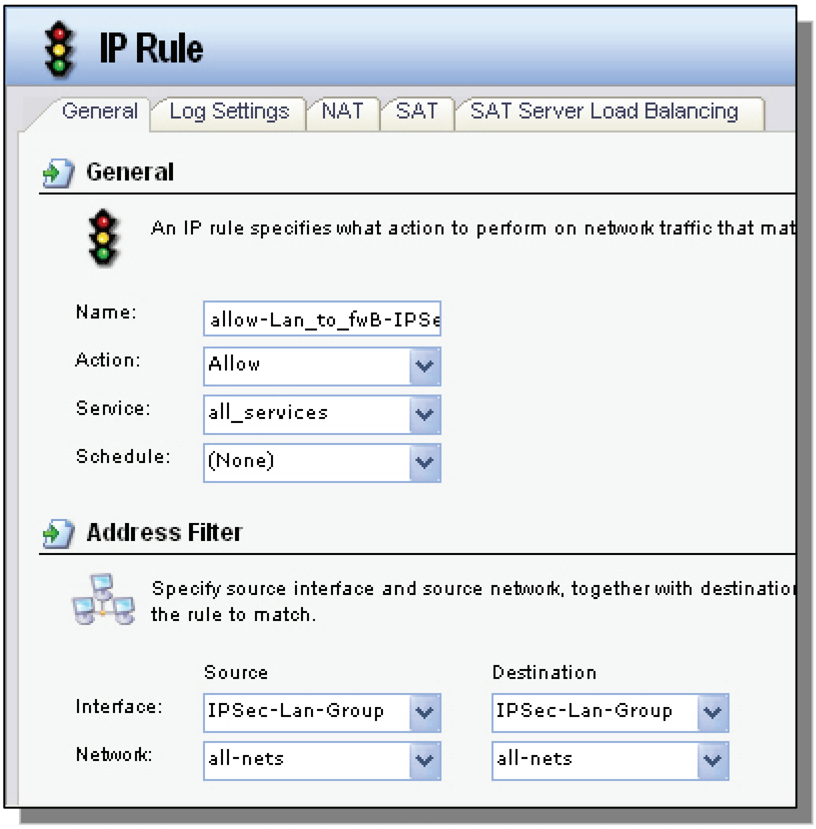
Go to *Rules* -> *IP Rules*.

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:



General

An IP rule specifies what action to perform on network traffic that mat

Name: allow-Lan_to_fwB-IPSe
Action: Allow
Service: all_services
Schedule: (None)

Address Filter

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

	Source	Destination
Interface:	IPSec-Lan-Group	IPSec-Lan-Group
Network:	all-nets	all-nets

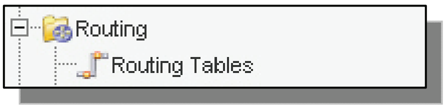
Name: **`allow_Lan_to_fwB-IPSec`**
Action: **`Allow`**
Service: **`all_services`**

Source Interface: **`IPSec-Lan-Group`**
Source Network: **`all-nets`**
Destination Interface: **`IPSec-Lan-Group`**
Destination Network: **`all-nets`**

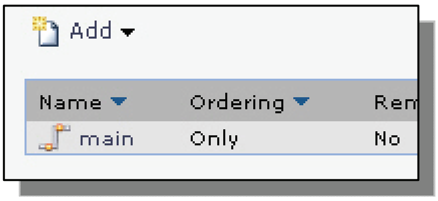
Click Ok.

6. Firewall A - Manually add route for interface monitoring

Go to *Routing -> Routing Tables*.

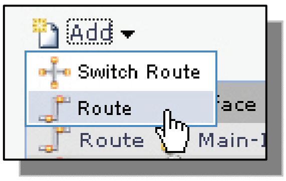


Click main routing table

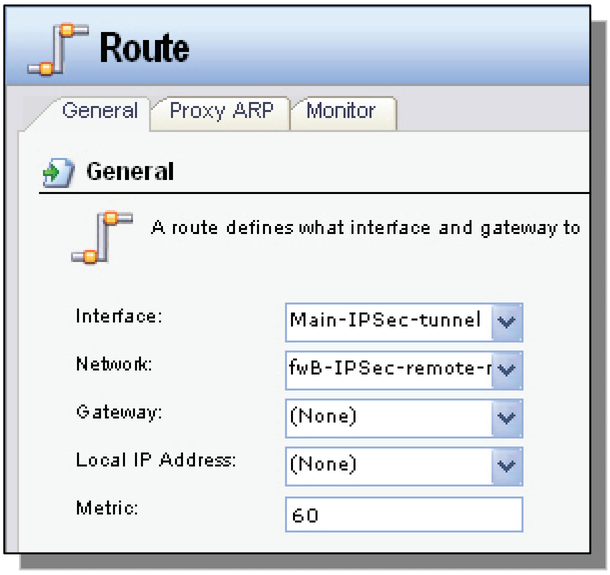


Name	Ordering	Rem
main	Only	No

Add a new Route for main IPSec tunnel



In the General tab:
General:



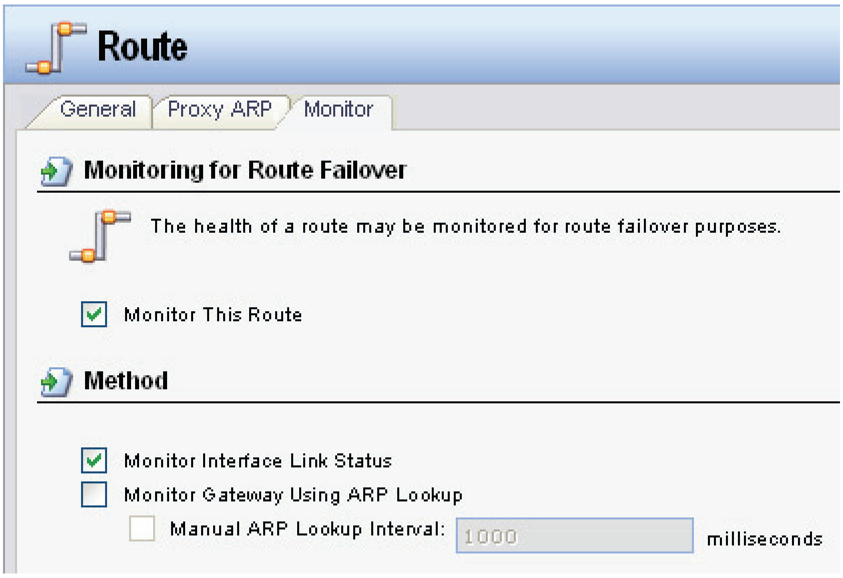
General

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:



Monitoring for Route Failover

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

☑ Monitor This Route

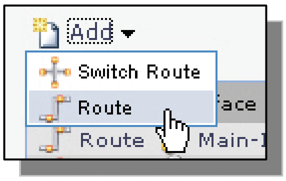
Method

☑ 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.

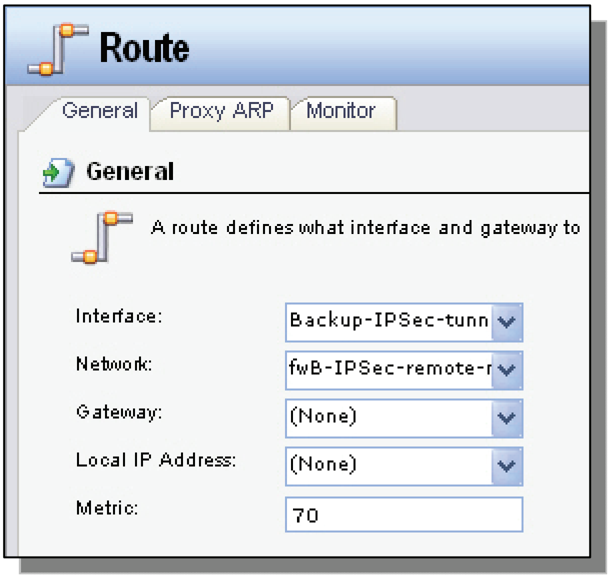
Click Ok.

Create a second Route for backup IPSec tunnel



In the General tab:

General:



A route defines what interface and gateway to

Interface: Backup-IPSec-tunn

Network: fwB-IPSec-remote-r

Gateway: (None)

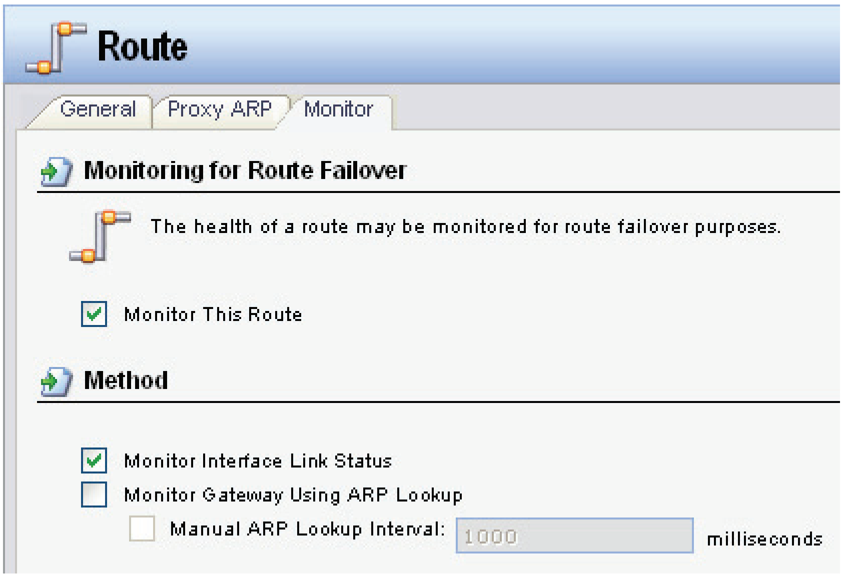
Local IP Address: (None)

Metric: 70

Interface: **Backup-IPSec-tunnel**
Network: **fwB-IPSec-remote-net**
Metric: **70**

In the Monitor tab:

Monitor:



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

☑ Monitor This Route

☑ Monitor Interface Link Status

☐ Monitor Gateway Using ARP Lookup

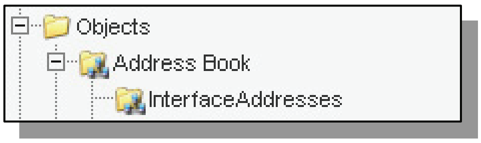
☐ Manual ARP Lookup Interval: 1000 milliseconds

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

Click Ok.

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 **lannet** to **192.168.2.0/24**

Change **wan1_ip** to **192.168.110.254**
Change **wan1net** to **192.168.110.0/24**
Change **Wan1_gw** to **192.168.110.1** (If this object does not exist, create a new one)

Change **wan2_ip** to **192.168.120.254**
Change **wan2net** to **192.168.120.0/24**
Change **Wan2_gw** to **192.168.120.1** (If this object does not exist, create a new one)

Add a new Address Folder called RemoteHosts.

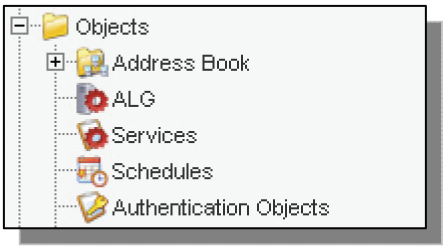
In the new folder, add following new IP Address objects
Name: **fwA-IPSec-remote-net**
IP Address: **192.168.1.0/24**

Name: **fwA-main-remote-gw**
IP Address: **192.168.110.1**

Name: **fwA-backup-remote-gw**
IP Address: **192.168.120.1**

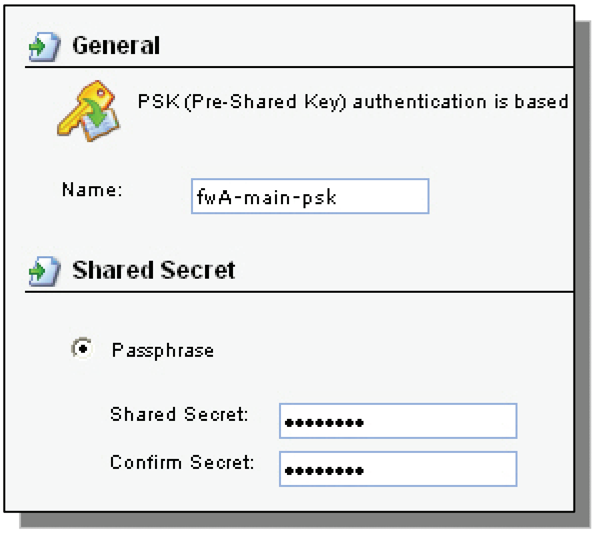
Click OK.

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

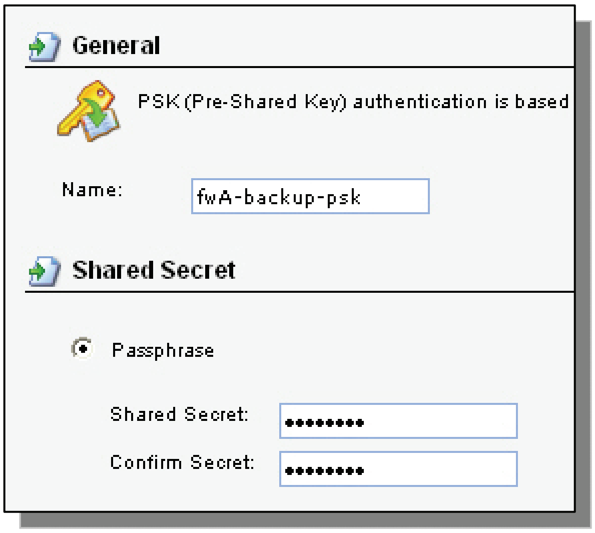
Name: fwA-main-psk

Shared Secret

● Passphrase

Shared Secret: ••••••••

Confirm Secret: ••••••••


General

PSK (Pre-Shared Key) authentication is based

Name: fwA-backup-psk

Shared Secret

● Passphrase

Shared Secret: ••••••••

Confirm Secret: ••••••••

General:

Name: **fwA-main-psk**
Name: **fwA-backup-psk**

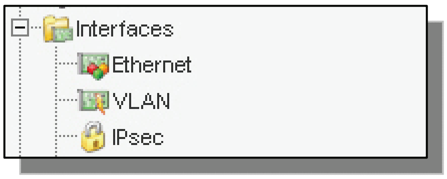
Shared secret:
Select Passphrase and enter a shared secret in above Pre-shared key objects

Click Ok.

9. Firewall B - Main IPsec interface

Create a Main IPSec Tunnel:

Go to *Interfaces -> IPsec*.

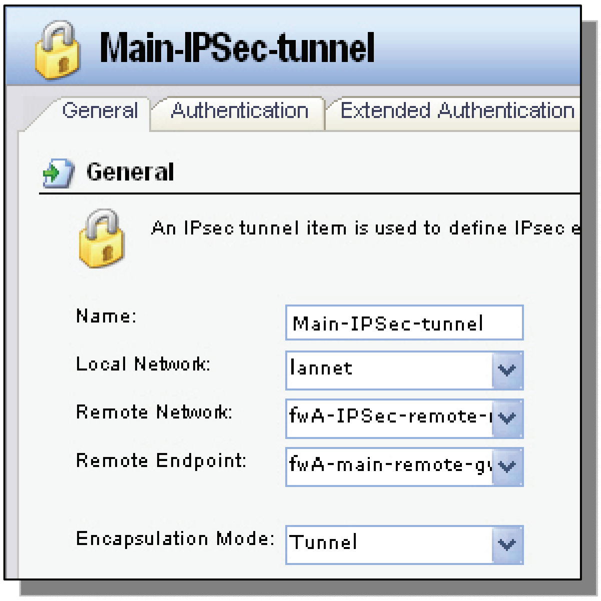


Add a new IPsec Tunnel for Main WAN link.

In the General tab:

General:
Name: ***Main-IPSec-tunnel***
Local Network: **lannet**
Remote Network: **fwA-IPSec-remote-net**
Remote Endpoint: **fwA-main-remote-gw**

Encapsulation Mode: **Tunnel**



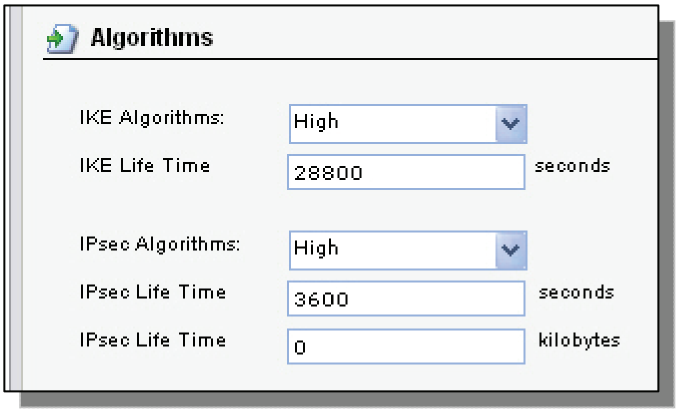
Main-IPSec-tunnel

General

An IPsec tunnel item is used to define IPsec e

Name: Main-IPSec-tunnel
Local Network: lannet
Remote Network: fwA-IPSec-remote-r
Remote Endpoint: fwA-main-remote-gv
Encapsulation Mode: Tunnel

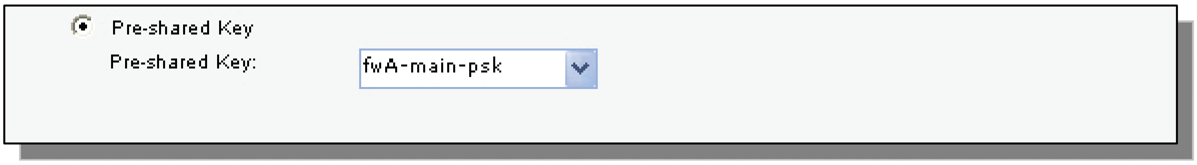
Algorithms:
IKE Algorithms: **High**
IKE Life Time: **28800**
IPsec Algorithms: **High**
IPsec Life Time: **3600**
IPsec Life Time: **0**



Algorithms

IKE Algorithms: High
IKE Life Time 28800 seconds
IPsec Algorithms: High
IPsec Life Time 3600 seconds
IPsec Life Time 0 kilobytes

Authentication:

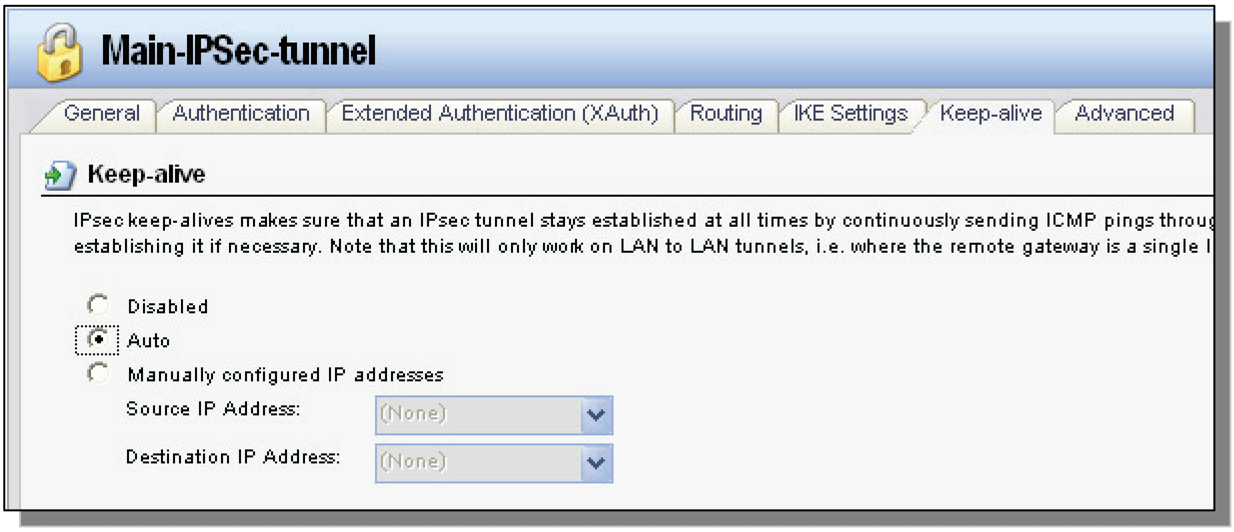


● Pre-shared Key

Pre-shared Key: fwA-main-psk

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

Keep-alive:



Keep-alive

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

○ Disabled

● Auto

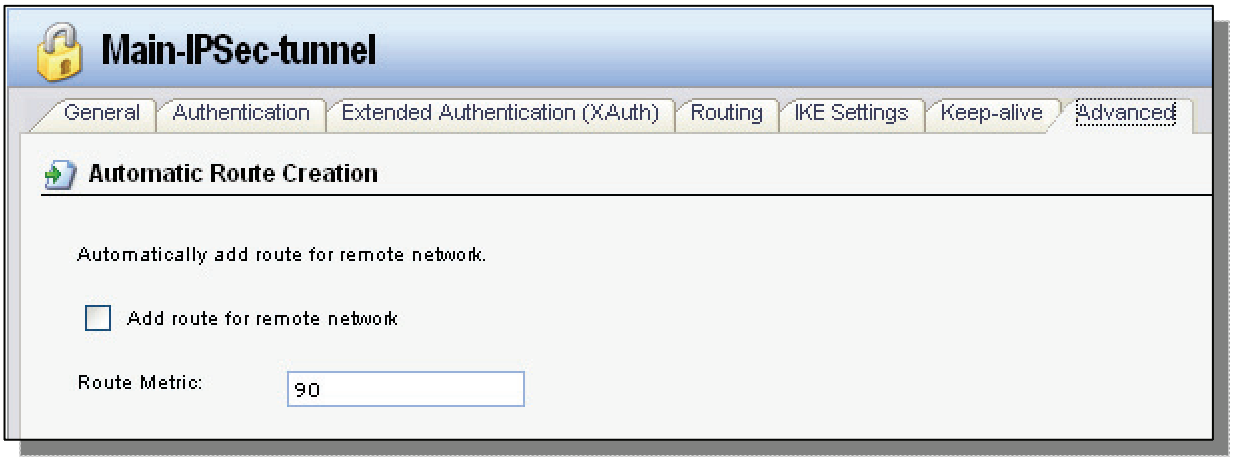
○ Manually configured IP addresses

Source IP Address: (None)

Destination IP Address: (None)

Select **`Auto`**.

Advanced:



Automatic Route Creation

Automatically add route for remote network.

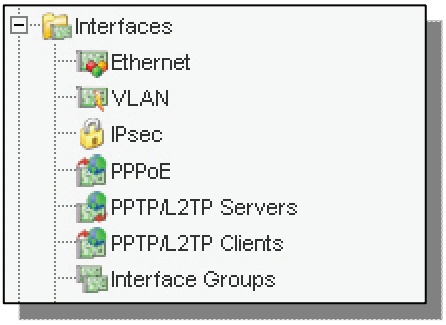
☐ Add route for remote network

Route Metric: 90

Make sure the "**`Add route for remote network`**" option is uncheck since this route without Monitoring feature.

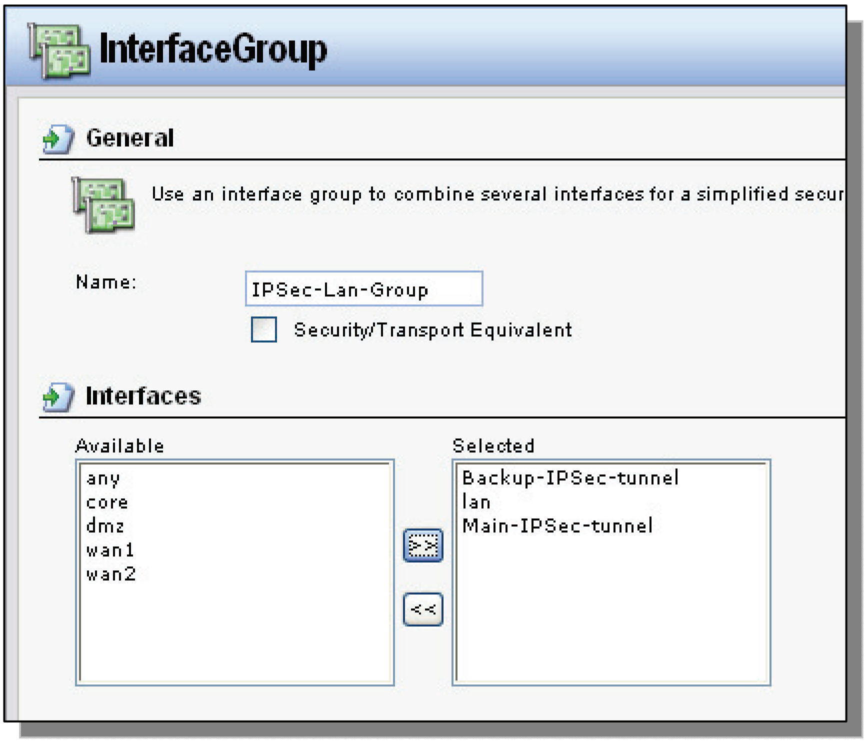
Click Ok.

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 secur

Name: IPSec-Lan-Group

□ Security/Transport Equivalent

Interfaces

Available: any, core, dmz, wan1, wan2

Selected: Backup-IPSec-tunnel, lan, Main-IPSec-tunnel

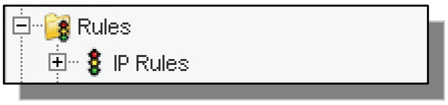
Name: **IPSec-Lan-Group**

Selected Interface:

Backup-IPSec-tunnel
Main-IPSec-tunnel
Lan

Click Ok.

11. Firewall B - Rules



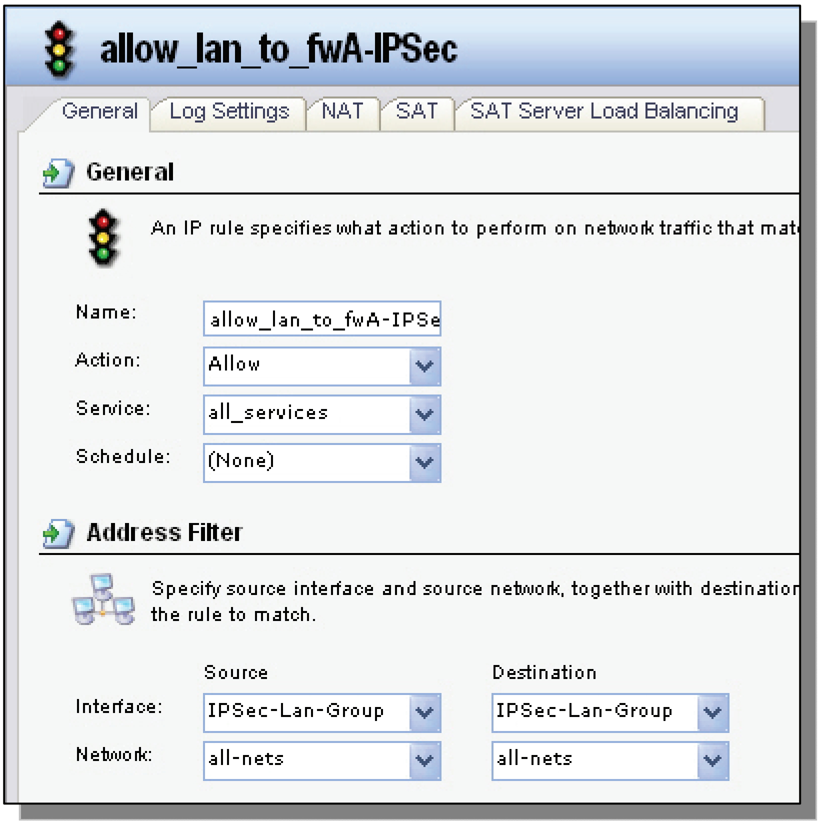
Go to *Rules* -> *IP Rules*.

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:



allow_lan_to_fwA-IPSec

General | Log Settings | NAT | SAT | SAT Server Load Balancing

General

An IP rule specifies what action to perform on network traffic that mat

Name: allow_lan_to_fwA-IPSe
Action: Allow
Service: all_services
Schedule: (None)

Address Filter

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

	Source	Destination
Interface:	IPSec-Lan-Group	IPSec-Lan-Group
Network:	all-nets	all-nets

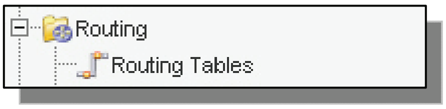
Name: **`allow_Lan_to_fwA-IPSec`**
Action: **`Allow`**
Service: **`all_services`**

Source Interface: **`IPSec-Lan-Group`**
Source Network: **`all-nets`**
Destination Interface: **`IPSec-Lan-Group`**
Destination Network: **`all-nets`**

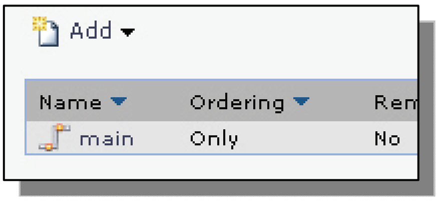
Click Ok.

12. Firewall B - Manually add route for interface monitoring

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

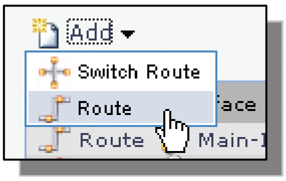


Click main routing table



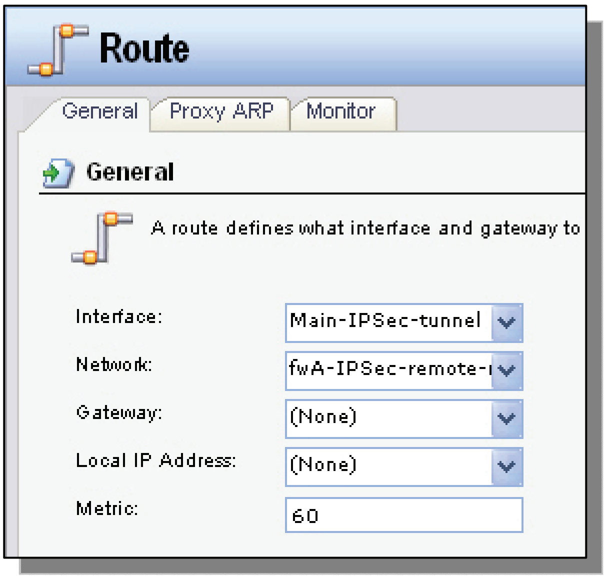
Name	Ordering	Rem
main	Only	No

Add a new Route for main IPSec tunnel



In the General tab:

General:



General

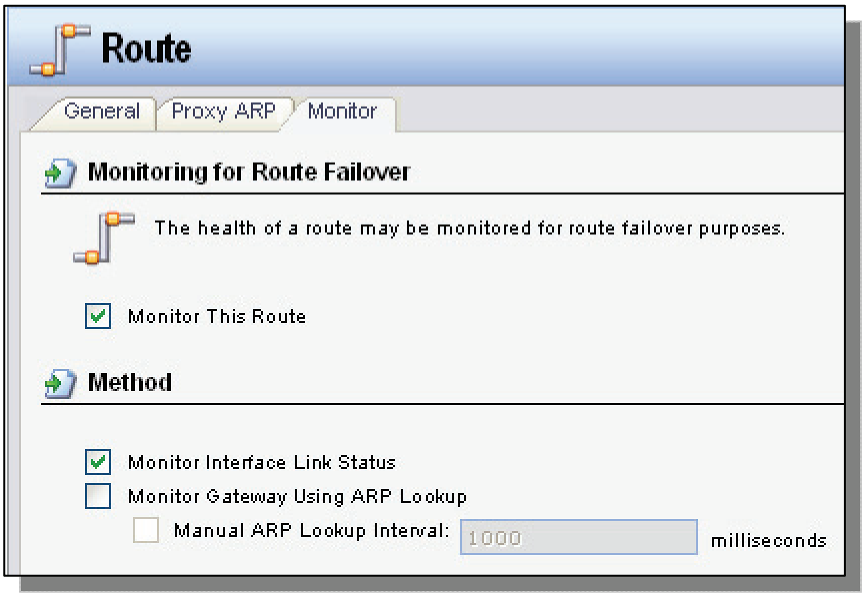
A route defines what interface and gateway to

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

Interface: **`Main-IPSec-tunnel`**
Network: **`fwA-IPSec-remote-net`**
Metric: **60**

In the Monitor tab:

Monitor:



Monitoring for Route Failover

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

☑ Monitor This Route

Method

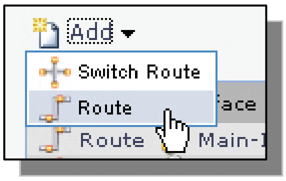
☑ Monitor Interface Link Status

☐ Monitor Gateway Using ARP Lookup

☐ Manual ARP Lookup Interval: 1000 milliseconds

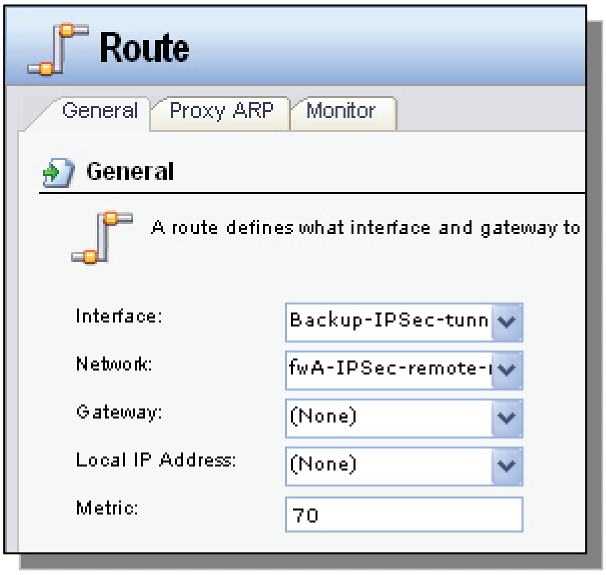
Make sure the “Monitor This Route” and “Monitor Interface Link Status” option is enabled.
Click Ok.

Create a second Route for backup IPSec tunnel



In the General tab:

General:



A route defines what interface and gateway to

Interface: Backup-IPSec-tunn

Network: fwA-IPSec-remote-r

Gateway: (None)

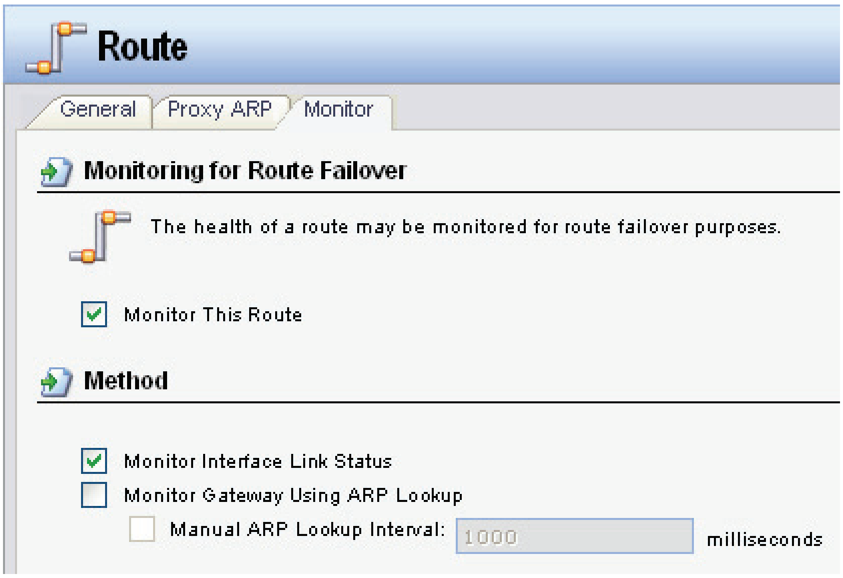
Local IP Address: (None)

Metric: 70

Interface: **Backup-IPSec-tunnel**
Network: **fwA-IPSec-remote-net**
Metric: **70**

In the Monitor tab:

Monitor:



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

☑ 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.

Save and activate the configuration on firewall B.