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

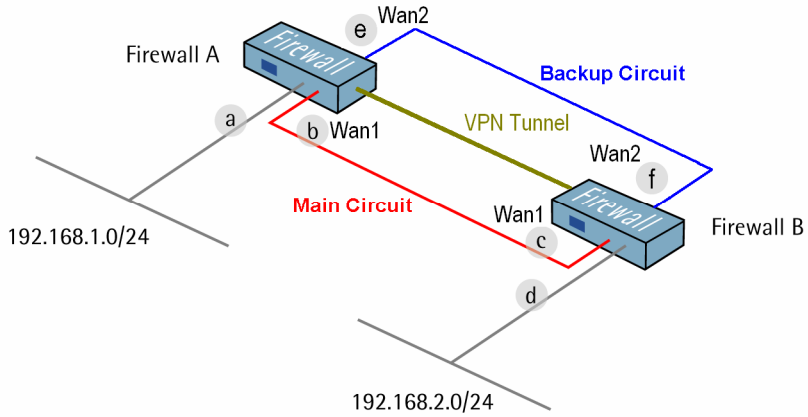
b IP: 192.168.110.1
Mask: 255.255.255.0
Gateway: 192.168.110.254

c IP: 192.168.110.254
Mask: 255.255.255.0
Gateway: 192.168.110.1

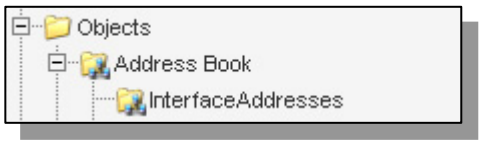
d IP: 192.168.2.1

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 **lannet** 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**

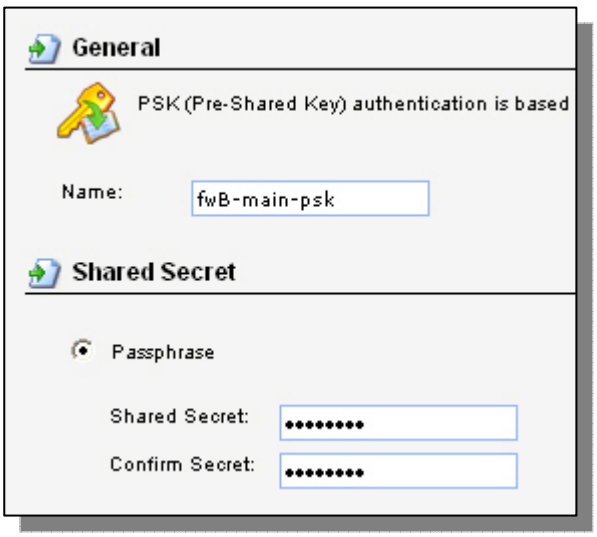
Name: **fwB-backup-remote-gw**
IP Address: **192.168.120.254**

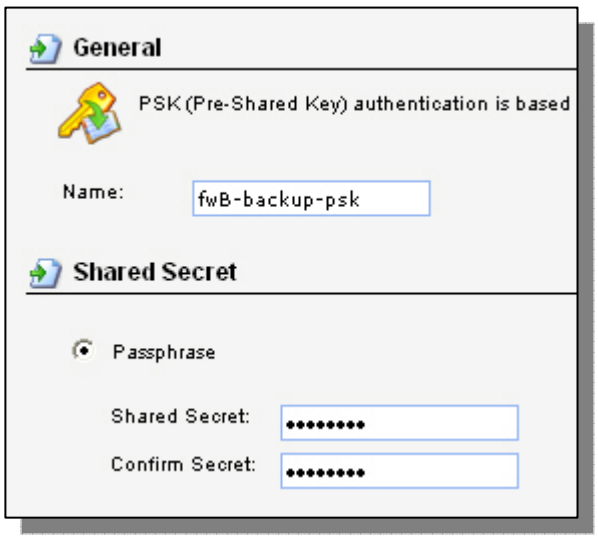
Click OK.

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

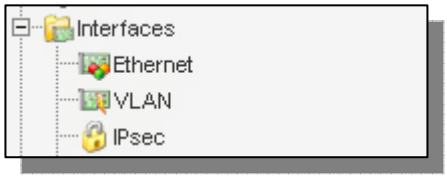
Shared secret:
Select Passphrase and enter a shared secret in above Pre-shared key objects

Click Ok.

3. Firewall A – Main IPsec interface

Create a Main IPSec Tunnel:

Go to *Interfaces -> IPsec*.

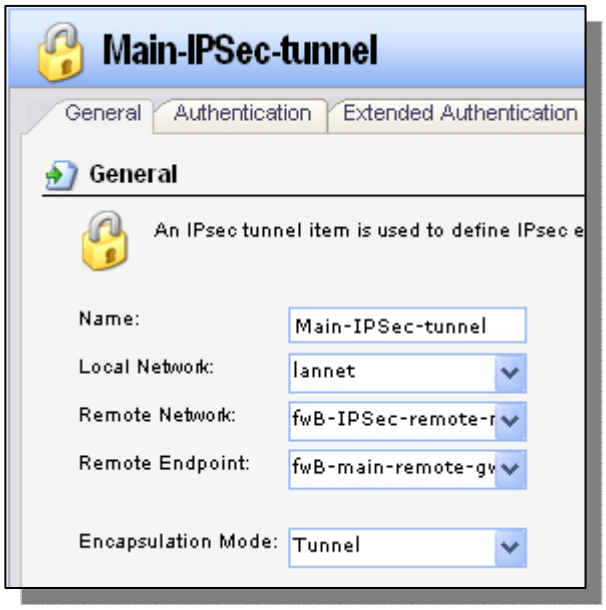


Add a new IPsec Tunnel `for Main WAN link`.

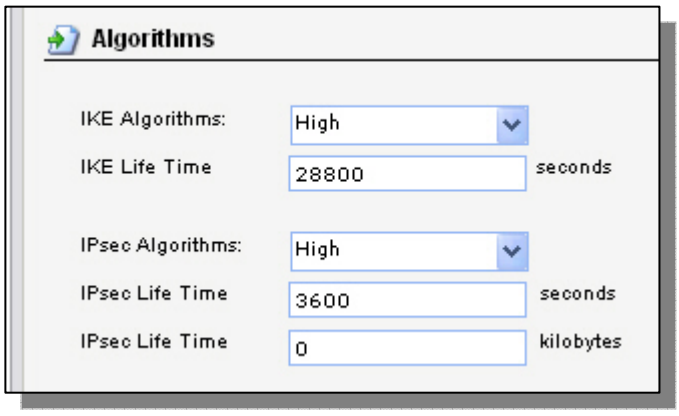
In the General tab:

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

Encapsulation Mode: **`Tunnel`**



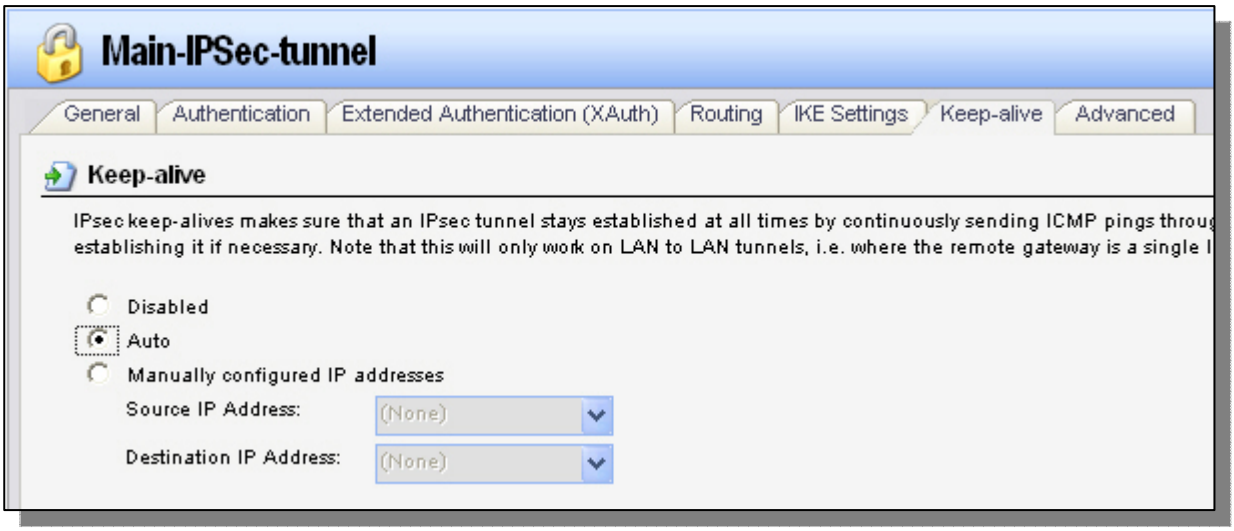
Algorithms:
IKE Algorithms: **`High`**
IKE Life Time: **`28800`**
IPsec Algorithms: **`High`**
IPsec Life Time: **`3600`**
IPsec Life Time: **`0`**



Authentication:

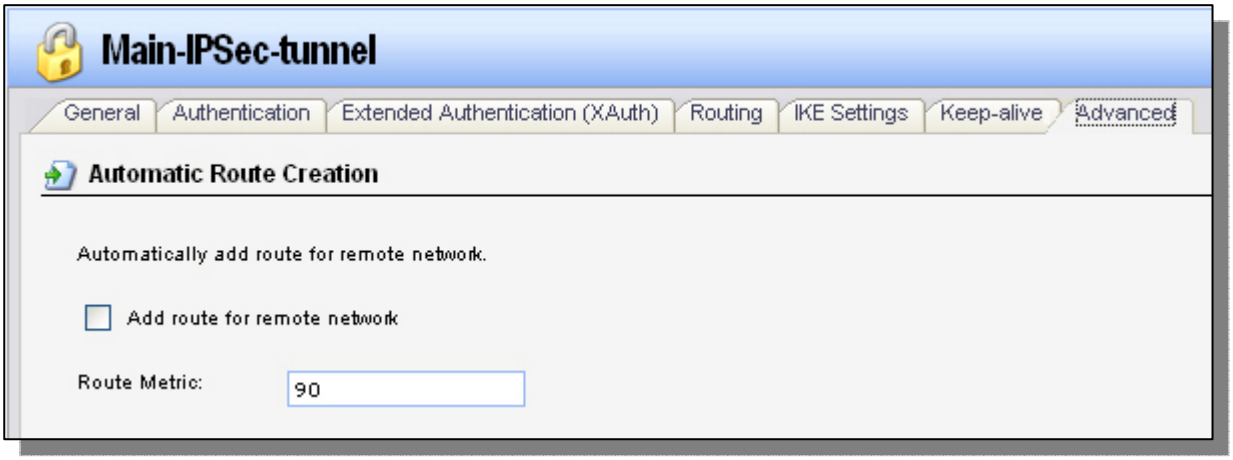
Select **`Pre-Shared Key`** and **`fwB-psk`**.

Keep-alive:



Select **`Auto`**.

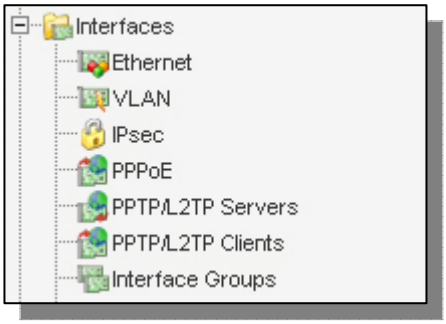
Advanced:



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

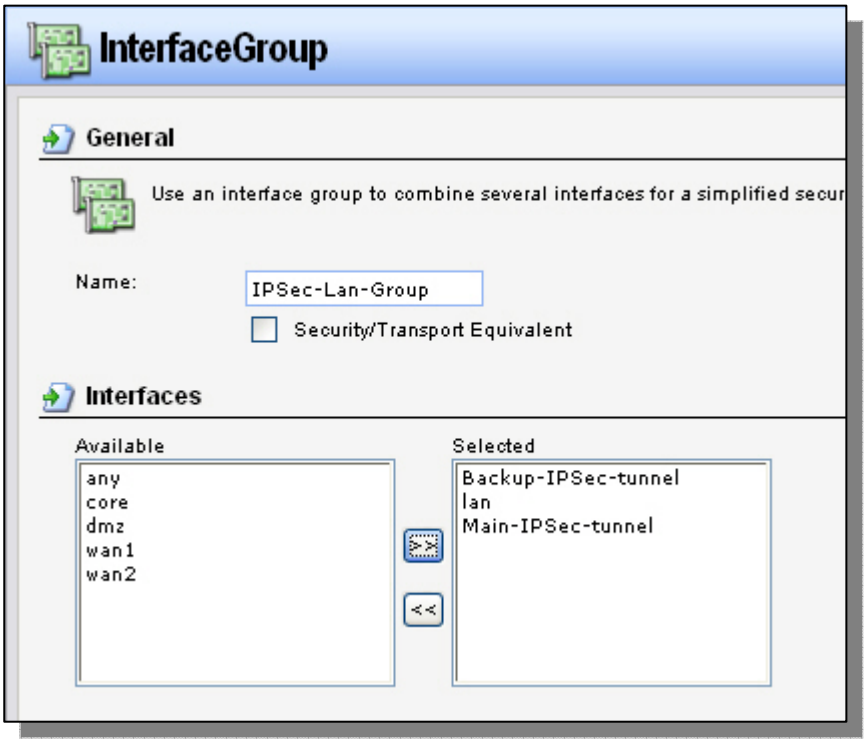
Click Ok.

4. Firewall A - Combine IPSec and Lan interfaces



Go to *Interfaces -> Interface Groups*.

Add a new InterfaceGroup :



Name: **IPSec-Lan-Group**
Selected Interface:
Backup-IPSec-tunnel
Main-IPSec-tunnel
Lan

Click Ok.

5. Firewall A - Rules

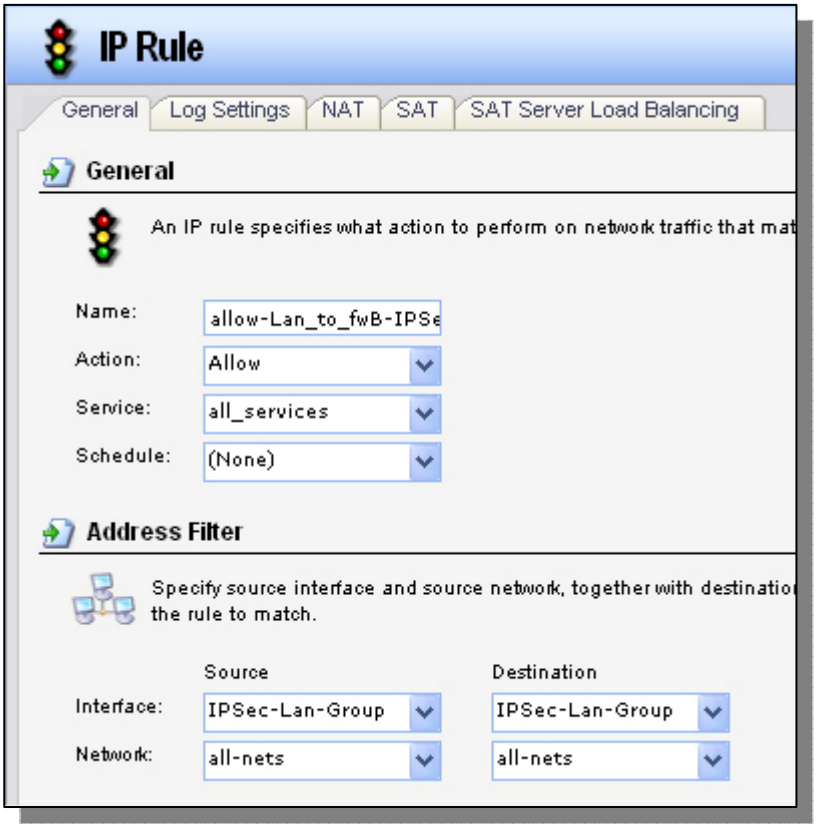
Go to *Rules -> IP Rules*.

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:



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`**

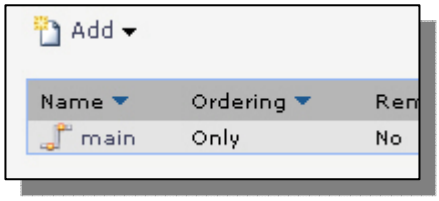
Click Ok.

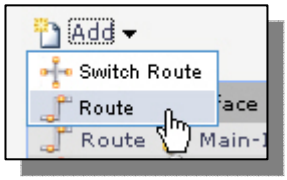
6. Firewall A - Manually add route for interface monitoring

Go to *Routing -> Routing Tables*.

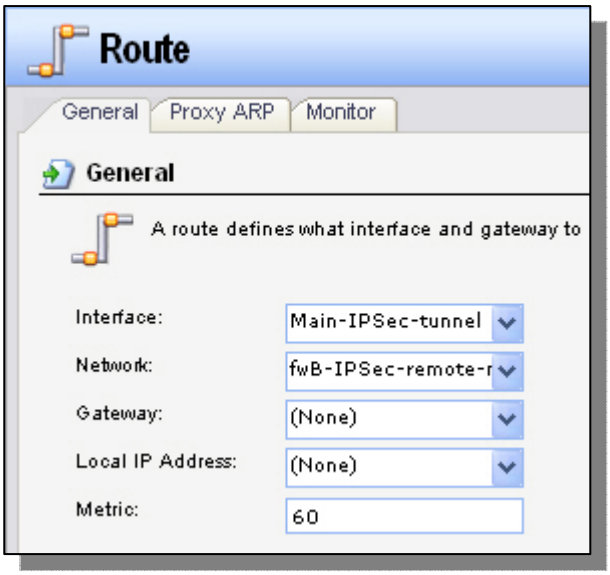
Click main routing table

Add a new Route for main IPSec tunnel



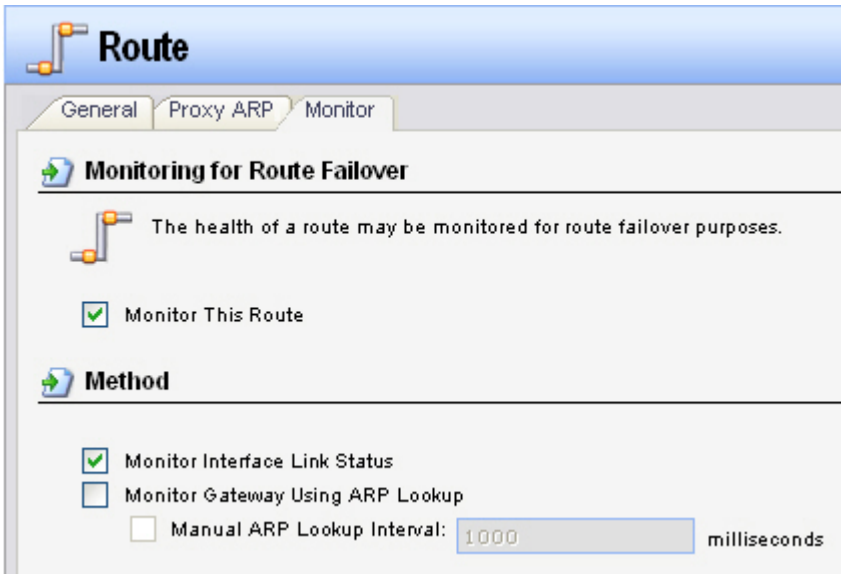


In the General tab:
General:



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

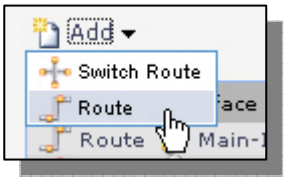
In the Monitor tab:
Monitor:



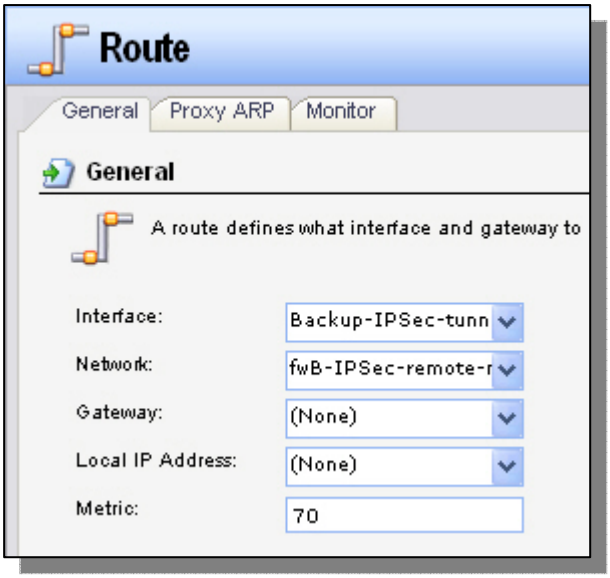
Make sure the “Monitor This Route” and “Monitor Interface Link Status” option is enabled.

Click Ok.

Create a second Route for backup IPSec tunnel

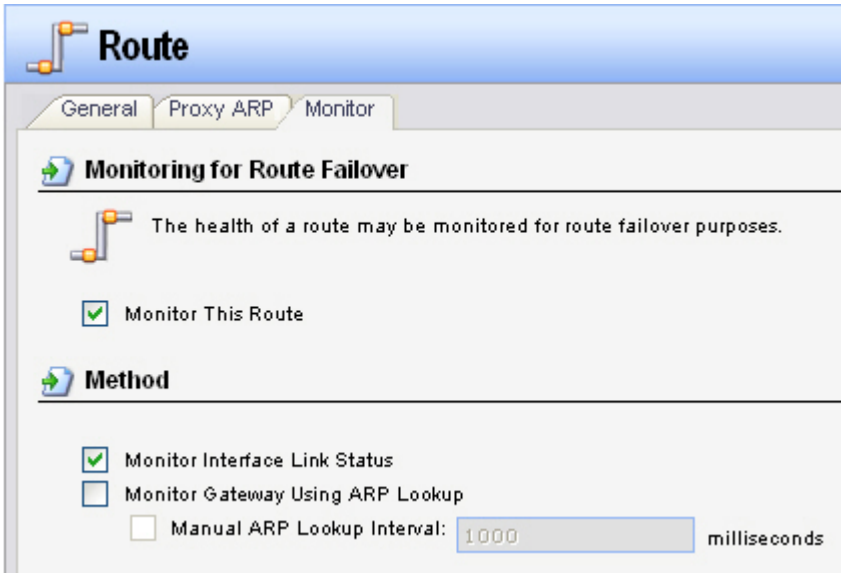


In the General tab:
General:



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

In the Monitor tab:
Monitor:

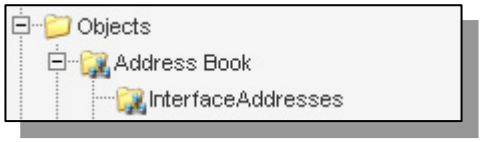


Make sure the "**Monitor This Route**" and "**Monitor Interface Link Status**" option is enabled.

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 **lannet** 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**

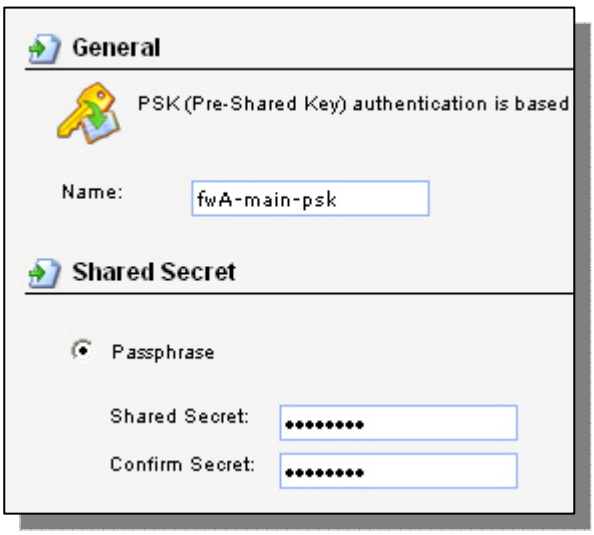
Name: **fwA-backup-remote-gw**
IP Address: **192.168.120.1**

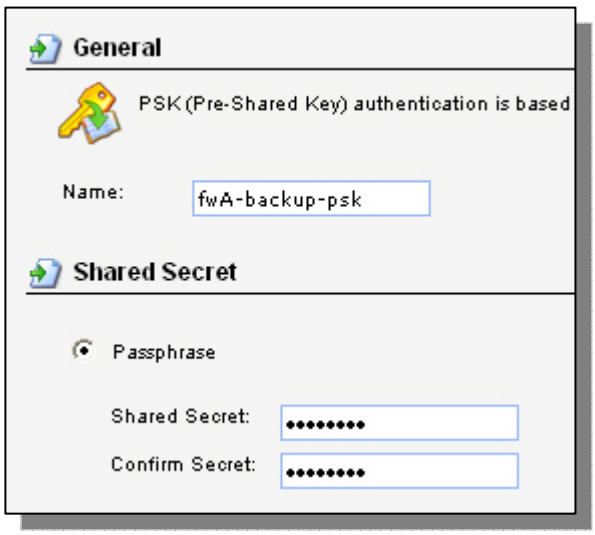
Click OK.

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

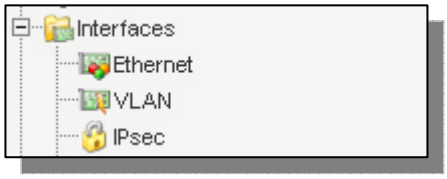
Shared secret:
Select Passphrase and enter a shared secret in above Pre-shared key objects

Click Ok.

9. Firewall B - Main IPsec interface

Create a Main IPSec Tunnel:

Go to *Interfaces -> IPsec*.

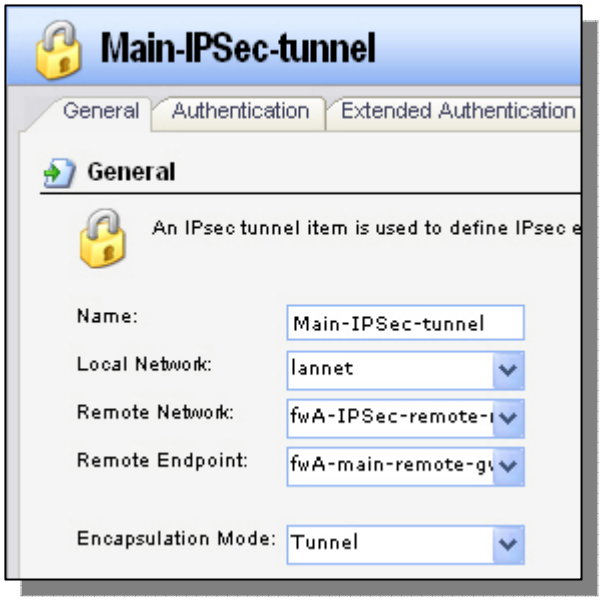


Add a new IPsec Tunnel `for Main WAN link`.

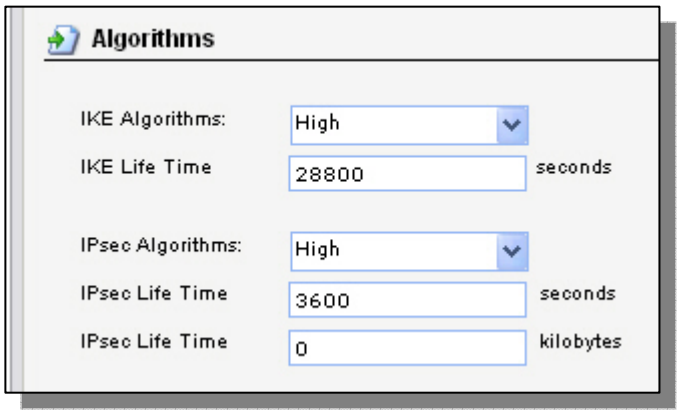
In the General tab:

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

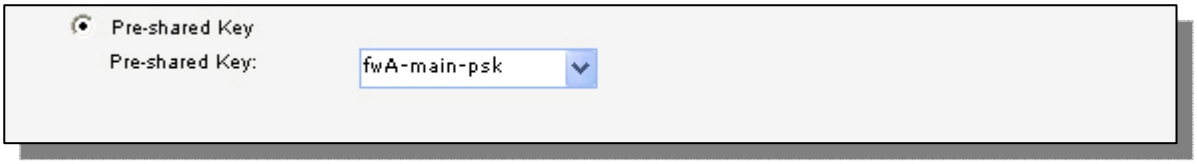
Encapsulation Mode: **`Tunnel`**



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

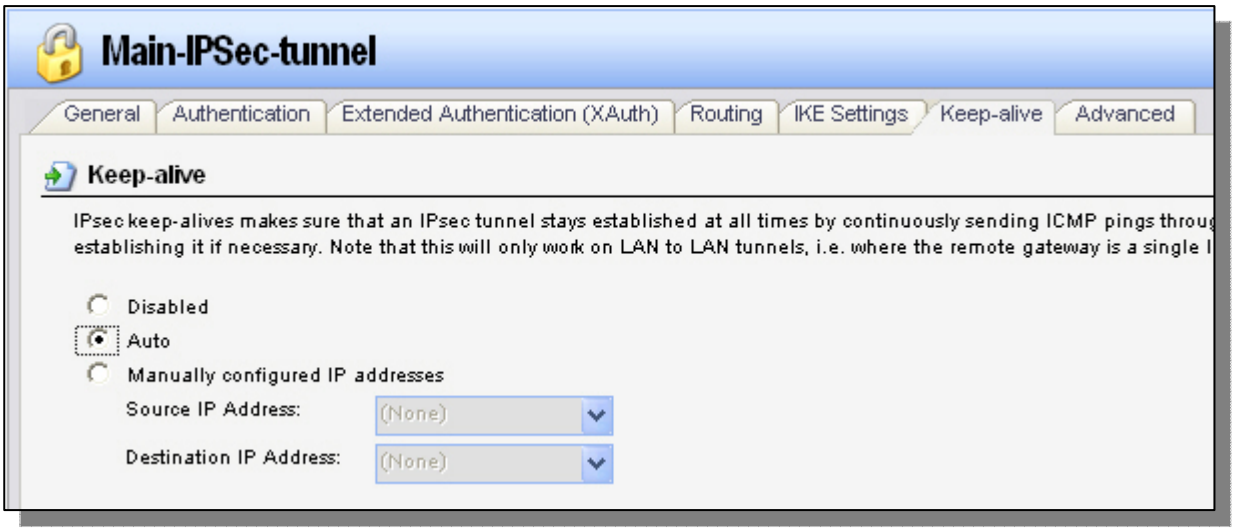


Authentication:



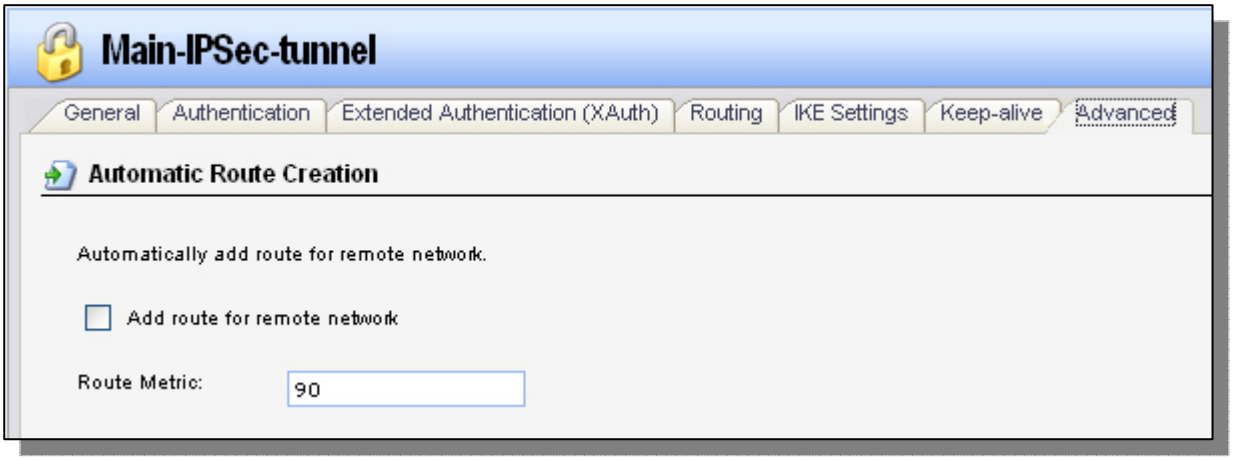
Select **`Pre-Shared Key`** and **`fwA-psk`**.

Keep-alive:



Select **`Auto`**.

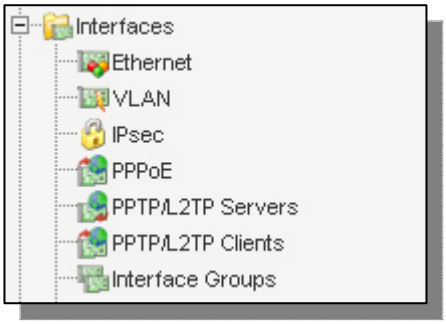
Advanced:



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

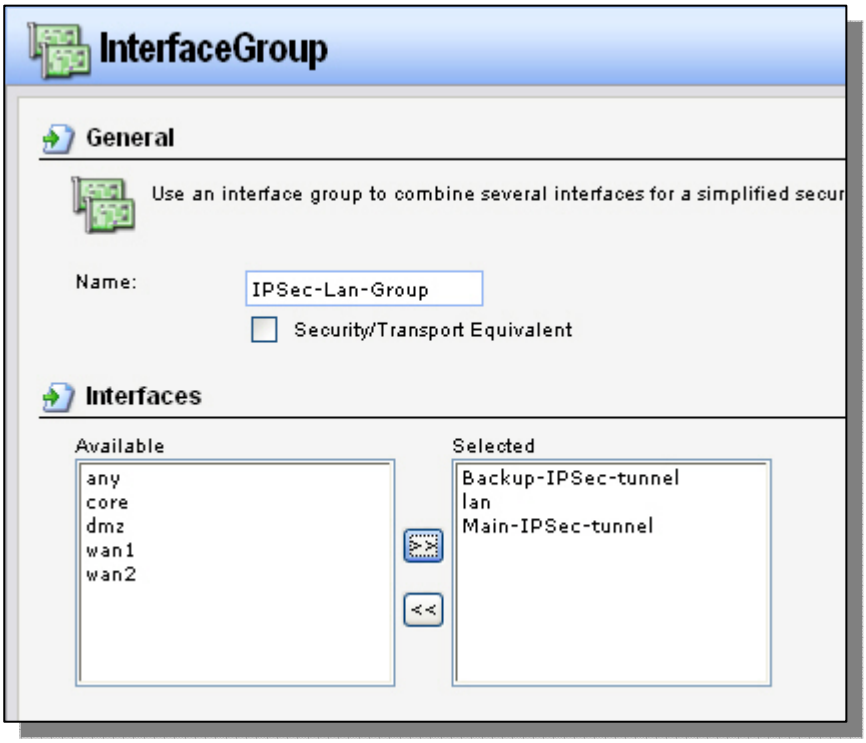
Click Ok.

10. Firewall B - Combine IPSec and Lan interfaces



Go to *Interfaces -> Interface Groups*.

Add a new InterfaceGroup :



Name: **IPSec-Lan-Group**
Selected Interface:
Backup-IPSec-tunnel
Main-IPSec-tunnel
Lan

Click Ok.

11. Firewall B - Rules

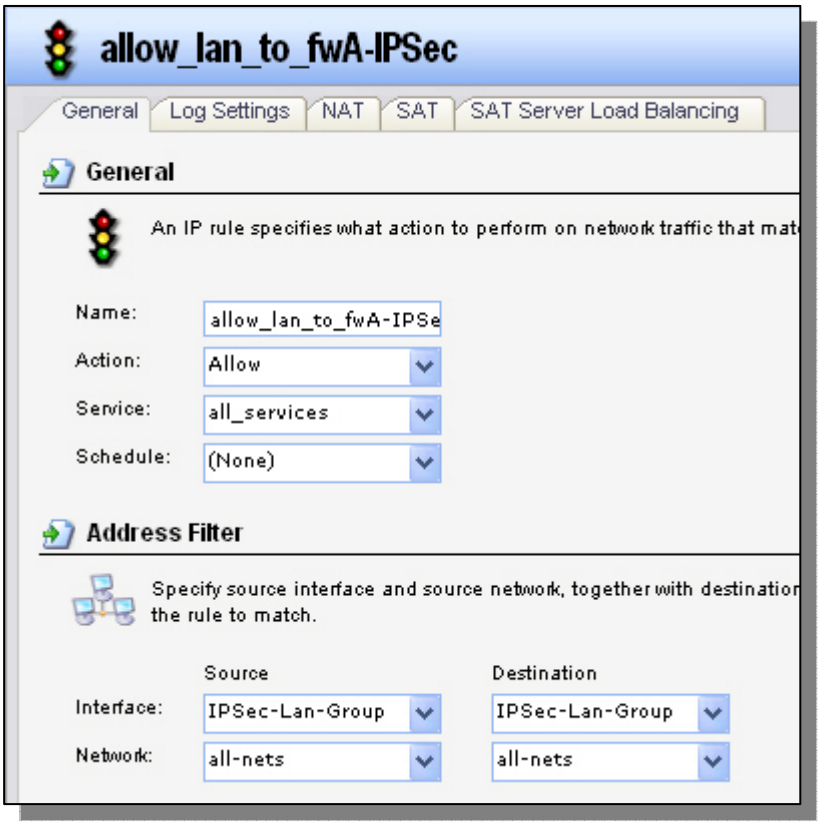
Go to *Rules -> IP Rules*.

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:



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`**

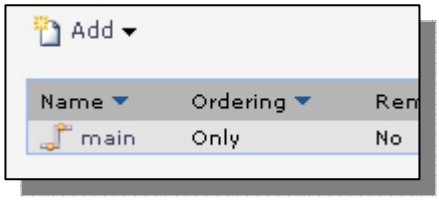
Click Ok.

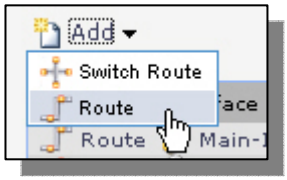
12. Firewall B - Manually add route for interface monitoring

Go to *Routing -> Routing Tables*.

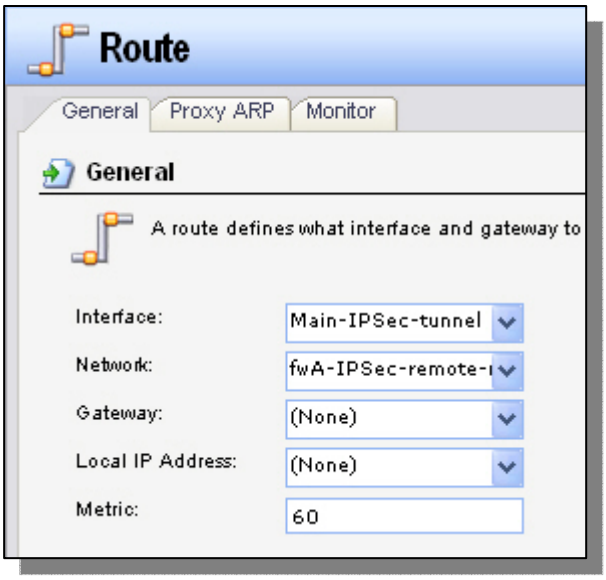
Click main routing table

Add a new Route for main IPSec tunnel



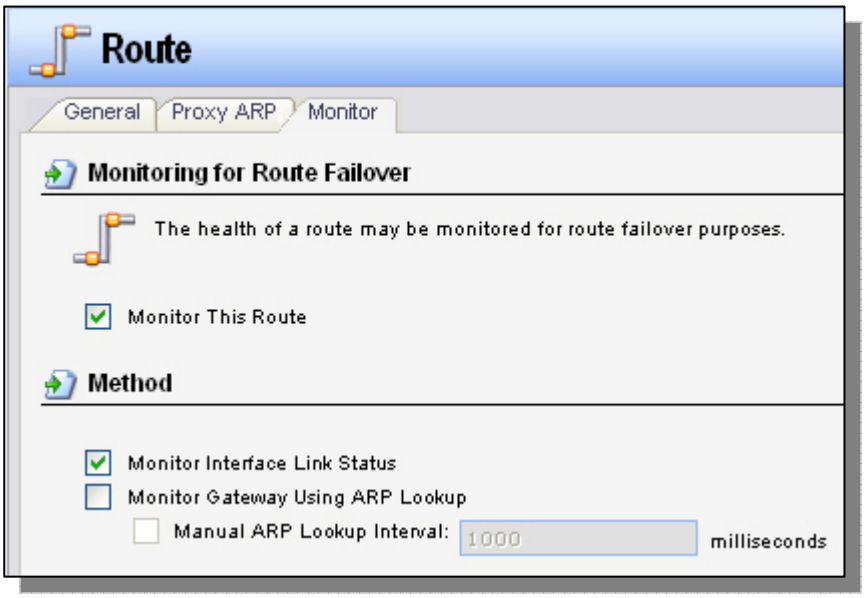


In the General tab:
General:



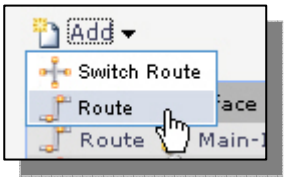
Interface: **`Main-IPSec-tunnel`**
Network: **`fwA-IPSec-remote-net`**
Metric: **`60`**

In the Monitor tab:
Monitor:

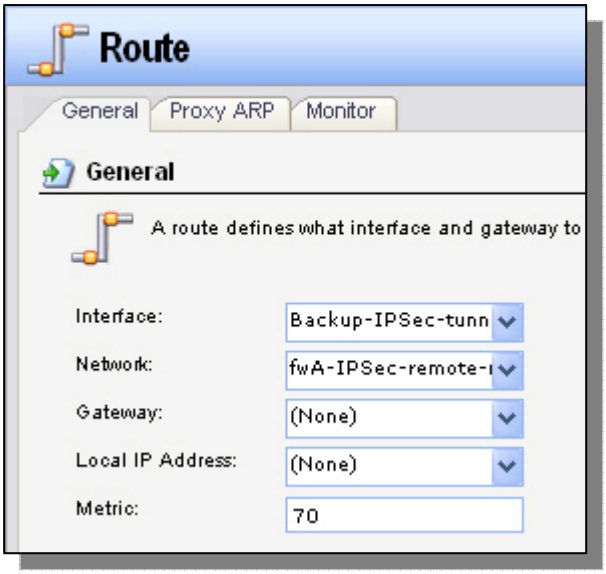


Make sure the “Monitor This Route” and “Monitor Interface Link Status” option is enabled.
Click Ok.

Create a second Route for backup IPSec tunnel

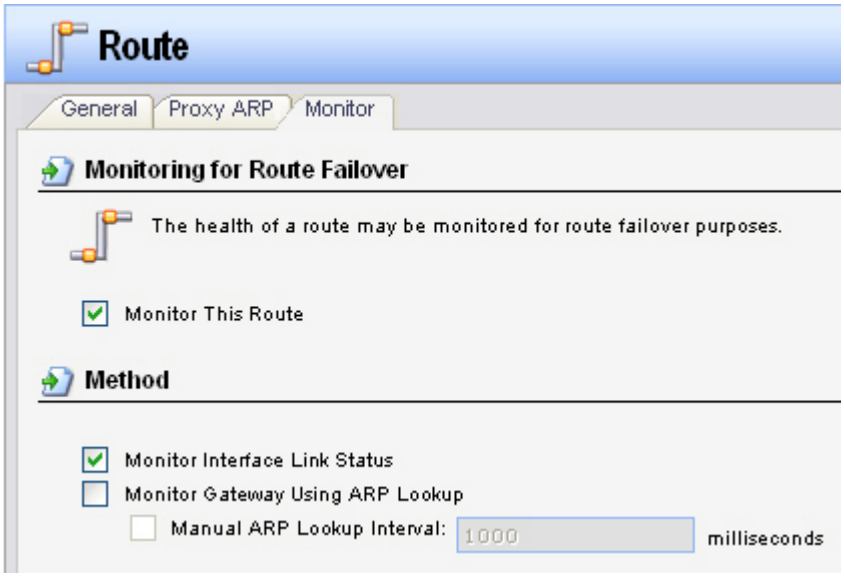


In the General tab:
General:



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.