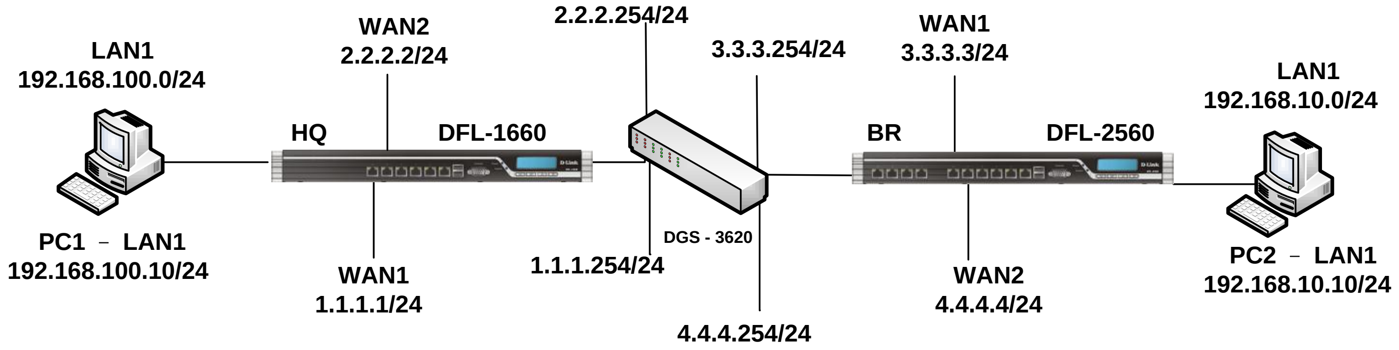
How to set up two IPsec tunnel failover with DFL model

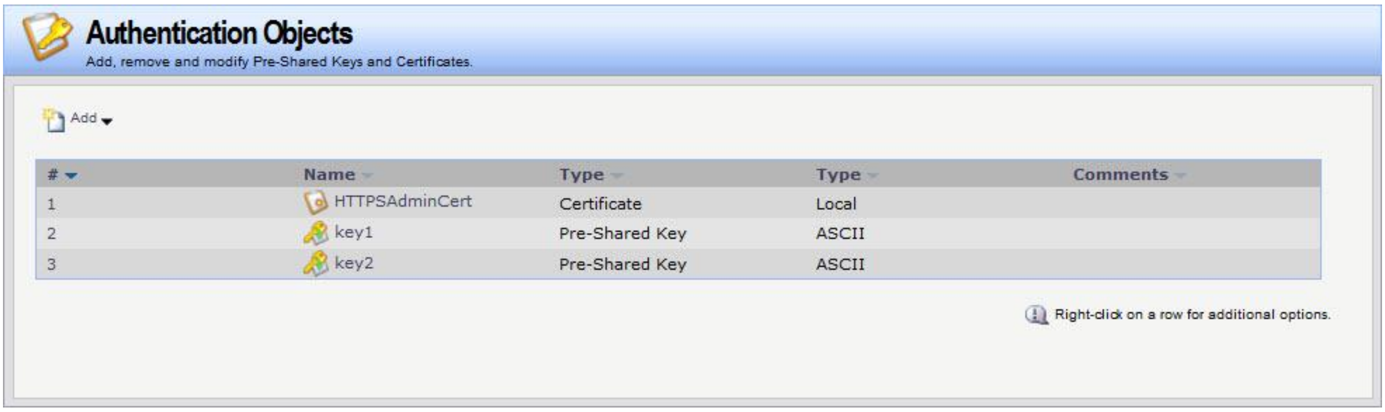
[Topology]



[HQ-DFL-1660 Setup]

1. Objects > Authentications Objects > Add

   Add two of Pre-Shared Keys. Both side keys must set up the same shared secret.



Authentication Objects

Add, remove and modify Pre-Shared Keys and Certificates.

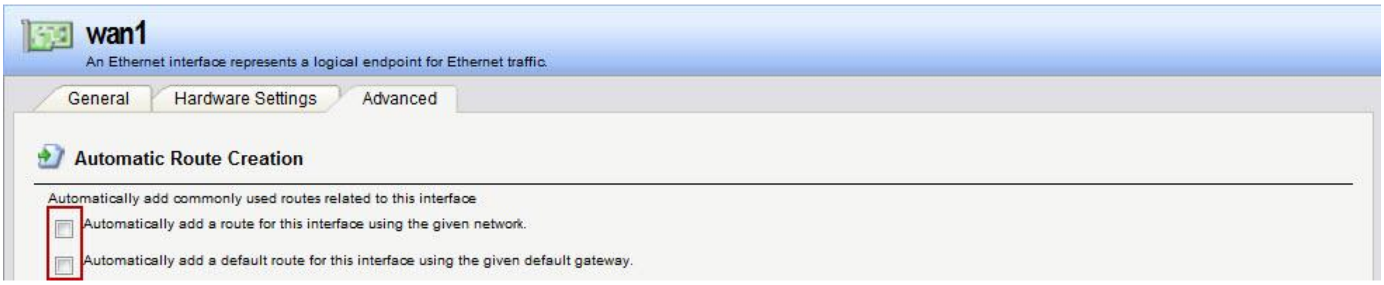
Add

#	Name	Type	Type	Comments
1	HTTPSAdminCert	Certificate	Local	
2	key1	Pre-Shared Key	ASCII	
3	key2	Pre-Shared Key	ASCII	

Right-click on a row for additional options.

2. Interfaces > Ethernet

   Disable WAN1 and WAN2 automatic route.



wan1

An Ethernet interface represents a logical endpoint for Ethernet traffic.

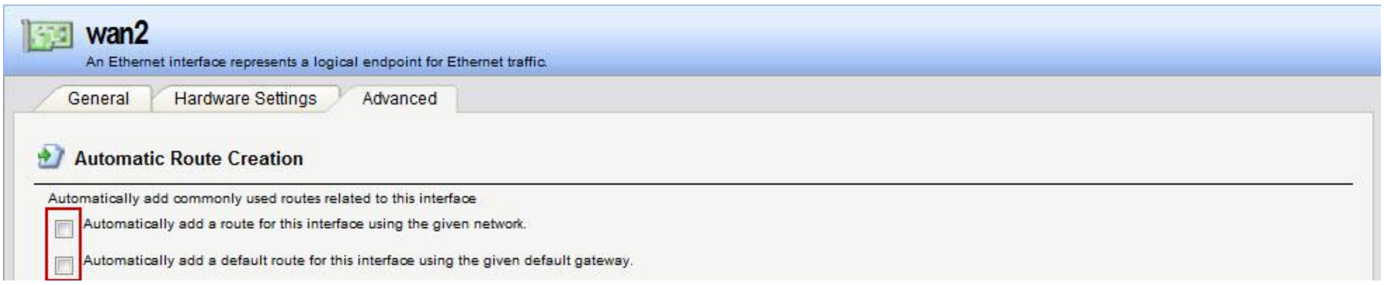
General | Hardware Settings | Advanced

Automatic Route Creation

Automatically add commonly used routes related to this interface

☐ Automatically add a route for this interface using the given network.

☐ Automatically add a default route for this interface using the given default gateway.



wan2

An Ethernet interface represents a logical endpoint for Ethernet traffic.

General | Hardware Settings | Advanced

Automatic Route Creation

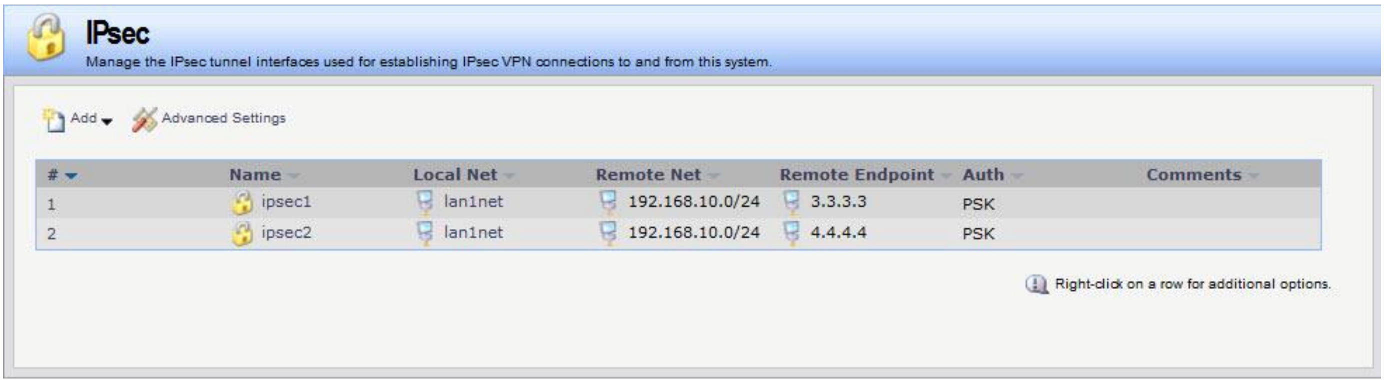
Automatically add commonly used routes related to this interface

☐ Automatically add a route for this interface using the given network.

☐ Automatically add a default route for this interface using the given default gateway.

3. Interfaces > IPsec

   Make two of IPsec tunnel for different key and remote endpoint.

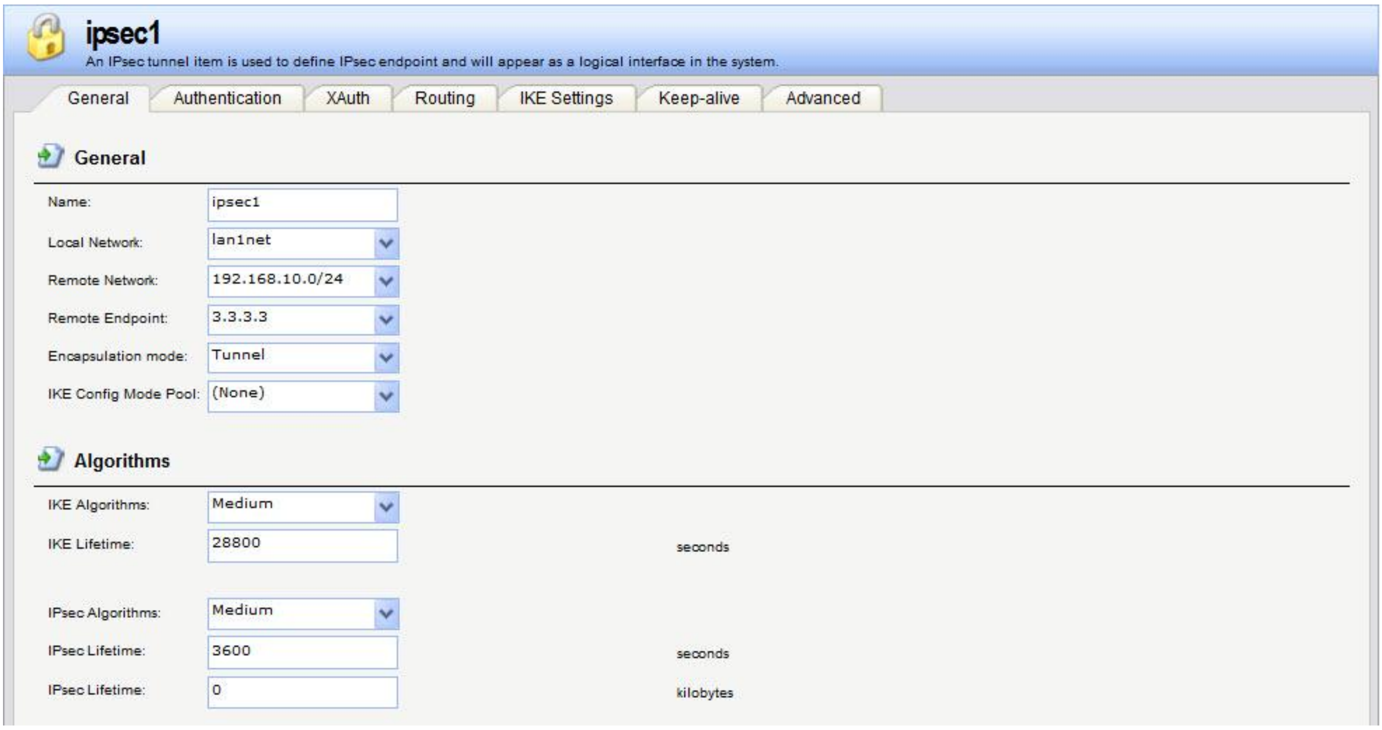


IPsec

Manage the IPsec tunnel interfaces used for establishing IPsec VPN connections to and from this system.

#	Name	Local Net	Remote Net	Remote Endpoint	Auth	Comments
1	ipsec1	lan1net	192.168.10.0/24	3.3.3.3	PSK	
2	ipsec2	lan1net	192.168.10.0/24	4.4.4.4	PSK	

Right-click on a row for additional options.



ipsec1

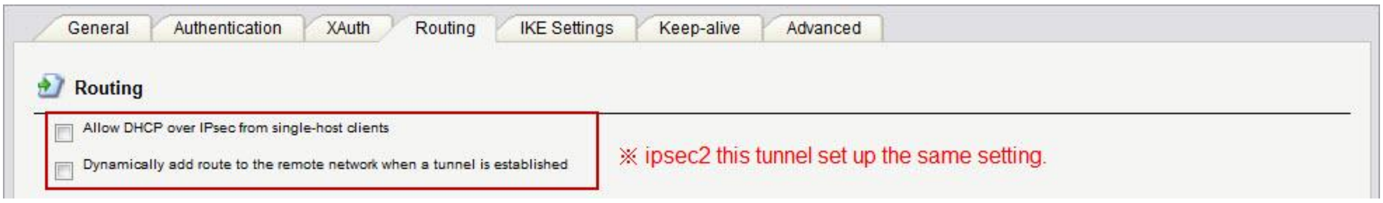
An IPsec tunnel item is used to define IPsec endpoint and will appear as a logical interface in the system.

General

Name:	ipsec1
Local Network:	lan1net
Remote Network:	192.168.10.0/24
Remote Endpoint:	3.3.3.3
Encapsulation mode:	Tunnel
IKE Config Mode Pool:	(None)

Algorithms

IKE Algorithms:	Medium	
IKE Lifetime:	28800	seconds
IPsec Algorithms:	Medium	
IPsec Lifetime:	3600	seconds
IPsec Lifetime:	0	kilobytes

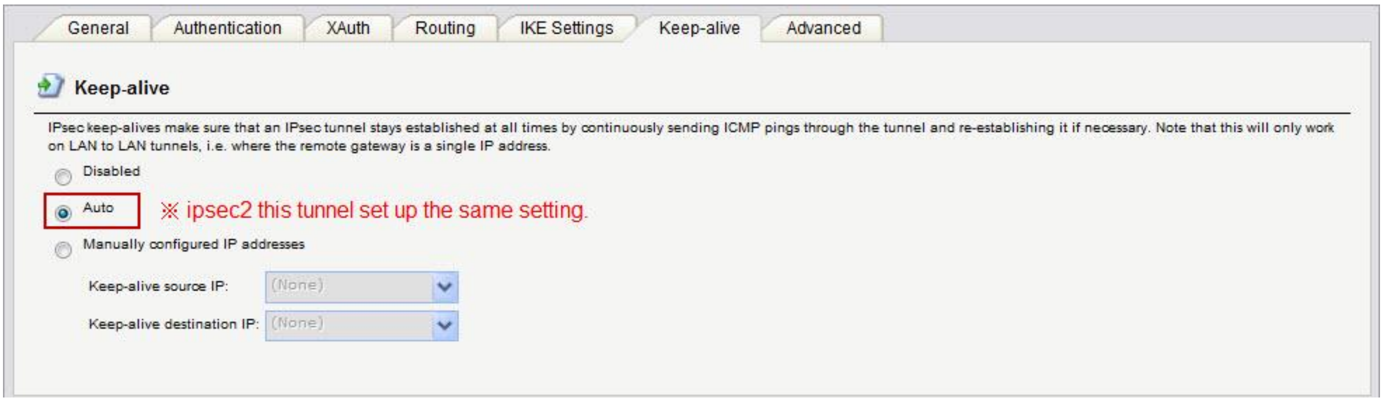


Routing

□ Allow DHCP over IPsec from single-host clients

□ Dynamically add route to the remote network when a tunnel is established

※ ipsec2 this tunnel set up the same setting.



Keep-alive

IPsec keep-alives make 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.

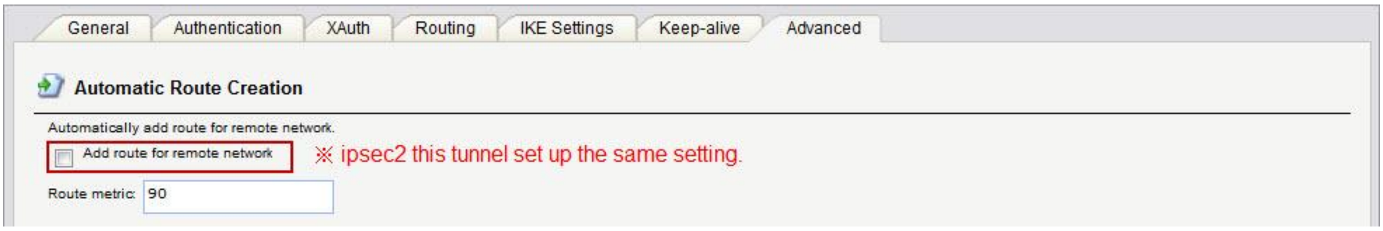
○ Disabled

● Auto ※ ipsec2 this tunnel set up the same setting.

○ Manually configured IP addresses

Keep-alive source IP: (None)

Keep-alive destination IP: (None)

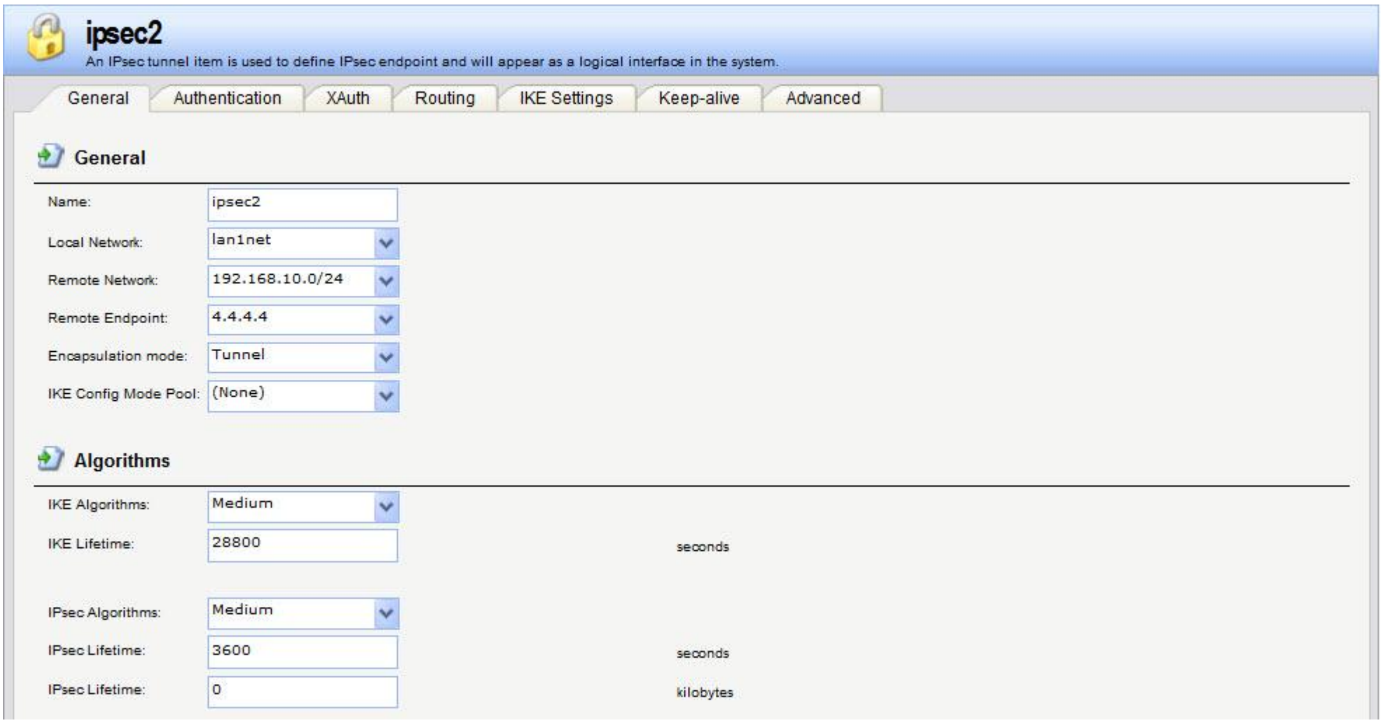


Automatic Route Creation

Automatically add route for remote network.

□ Add route for remote network ※ ipsec2 this tunnel set up the same setting.

Route metric: 90



ipsec2

An IPsec tunnel item is used to define IPsec endpoint and will appear as a logical interface in the system.

General

Name: ipsec2

Local Network: lan1net

Remote Network: 192.168.10.0/24

Remote Endpoint: 4.4.4.4

Encapsulation mode: Tunnel

IKE Config Mode Pool: (None)

Algorithms

IKE Algorithms: Medium

IKE Lifetime: 28800 seconds

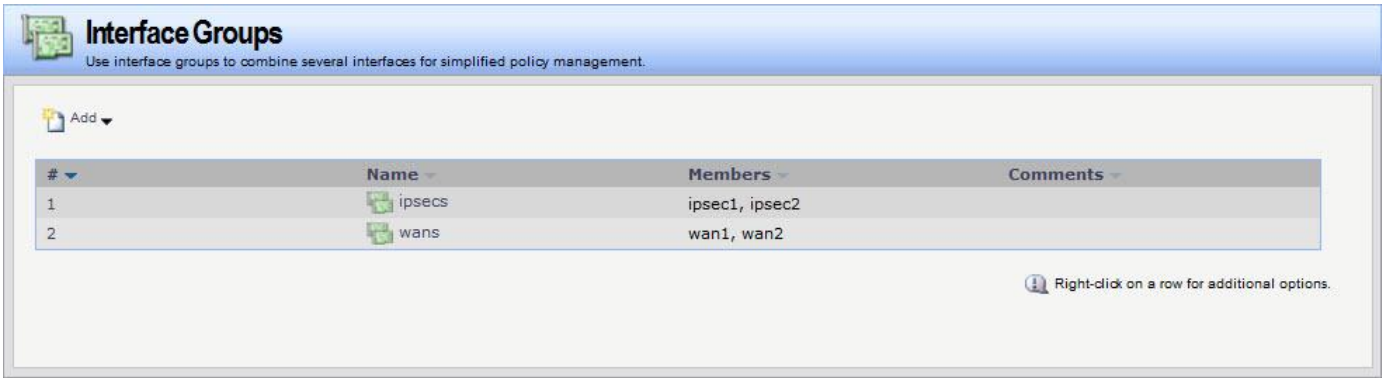
IPsec Algorithms: Medium

IPsec Lifetime: 3600 seconds

IPsec Lifetime: 0 kilobytes

4. Interfaces > Interfaces Groups

   Setup interfaces groups for IP rules.



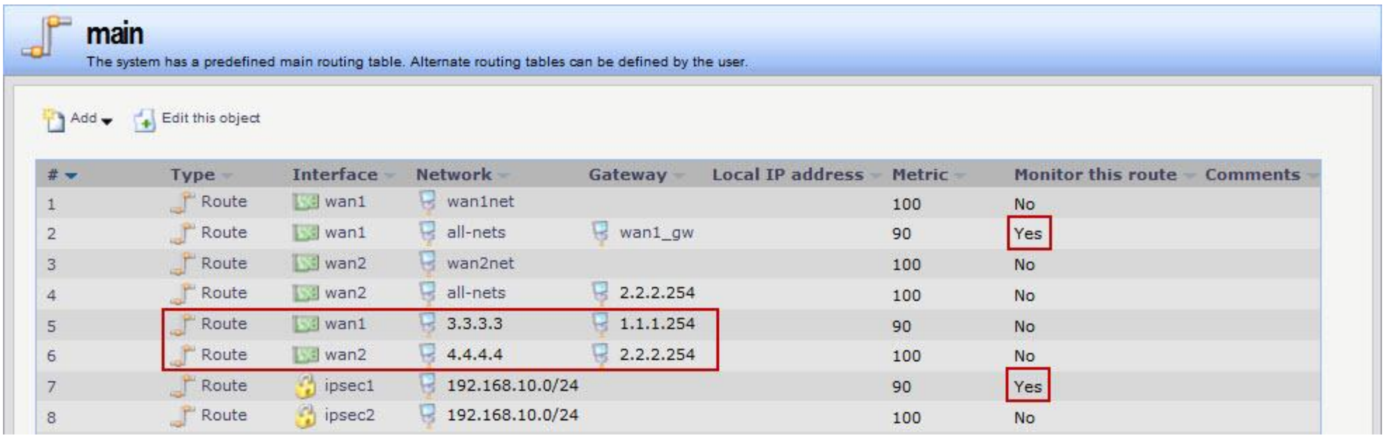
Interface Groups

Use interface groups to combine several interfaces for simplified policy management.

#	Name	Members	Comments
1	ipsecs	ipsec1, ipsec2	
2	wans	wan1, wan2	

Right-click on a row for additional options.

5. Routing > Routing Tables > Main



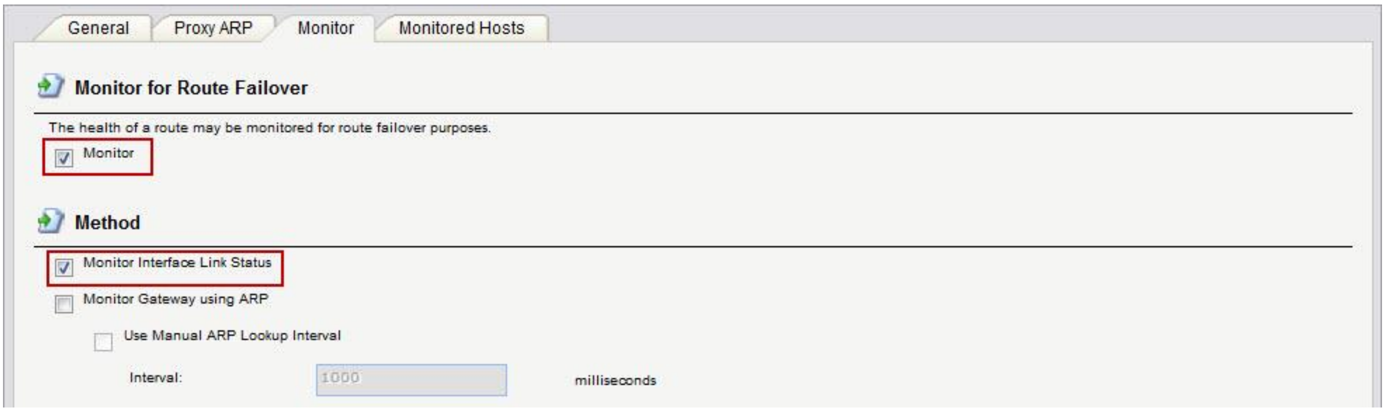
main

The system has a predefined main routing table. Alternate routing tables can be defined by the user.

#	Type	Interface	Network	Gateway	Local IP address	Metric	Monitor this route	Comments
1	Route	wan1	wan1net			100	No	
2	Route	wan1	all-nets	wan1_gw		90	Yes	
3	Route	wan2	wan2net			100	No	
4	Route	wan2	all-nets	2.2.2.254		100	No	
5	Route	wan1	3.3.3.3	1.1.1.254		90	No	
6	Route	wan2	4.4.4.4	2.2.2.254		100	No	
7	Route	ipsec1	192.168.10.0/24			90	Yes	
8	Route	ipsec2	192.168.10.0/24			100	No	

We have some of very important parts on routing rules setup.

1. Only monitor two of routing rules. (Index 2 & 7)
2. Index 5 & 6 must setup remote endpoint and local interface gateway.
3. The monitor set up only need to use interface link status.
4. Index 2 & 5 & 7 metric must law than the partner rules.



Monitor for Route Failover

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

☑ Monitor

Method

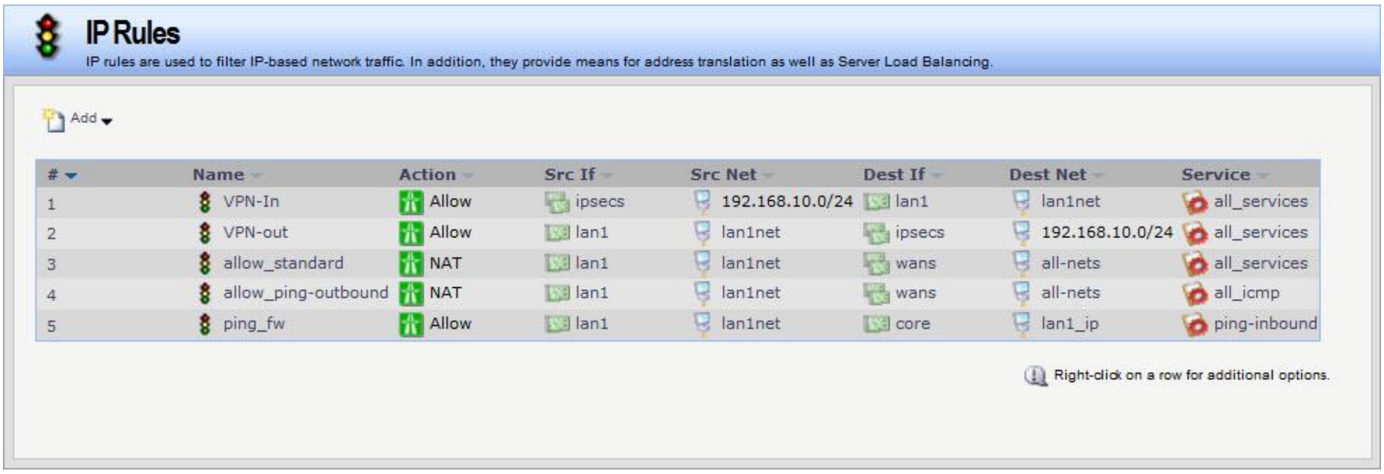
☑ Monitor Interface Link Status

□ Monitor Gateway using ARP

□ Use Manual ARP Lookup Interval

Interval: 1000 milliseconds

6. Rules > IP Rules



IP Rules

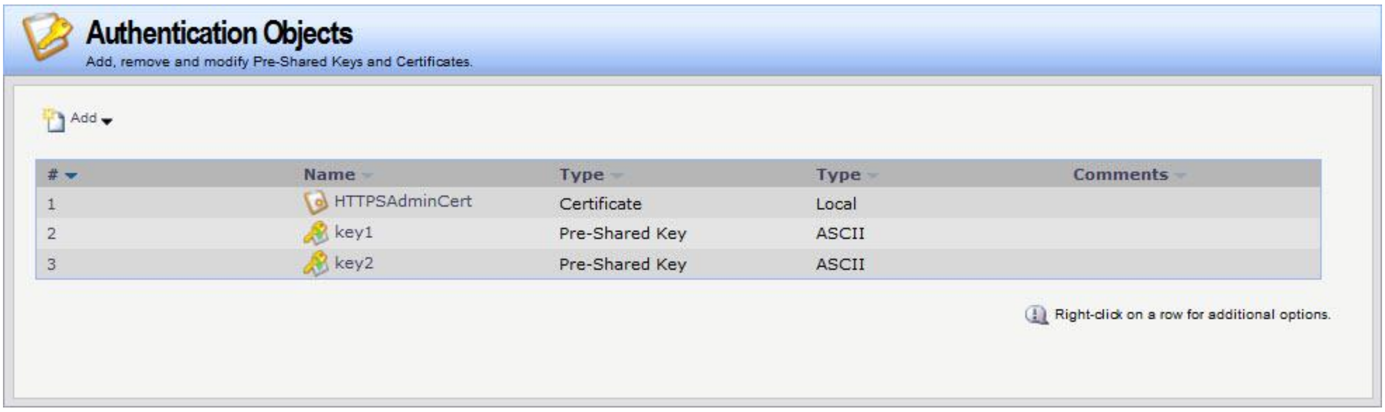
IP rules are used to filter IP-based network traffic. In addition, they provide means for address translation as well as Server Load Balancing.

#	Name	Action	Src If	Src Net	Dest If	Dest Net	Service
1	VPN-In	Allow	ipsecs	192.168.10.0/24	lan1	lan1net	all_services
2	VPN-out	Allow	lan1	lan1net	ipsecs	192.168.10.0/24	all_services
3	allow_standard	NAT	lan1	lan1net	wans	all-nets	all_services
4	allow_ping-outbound	NAT	lan1	lan1net	wans	all-nets	all_icmp
5	ping_fw	Allow	lan1	lan1net	core	lan1_ip	ping-inbound

Right-click on a row for additional options.

[BR-DFL-2560 Setup]

1. Objects > Authentications Objects > Add
   Add two of Pre-Shared Keys. Both side keys must set up the same shared secret.



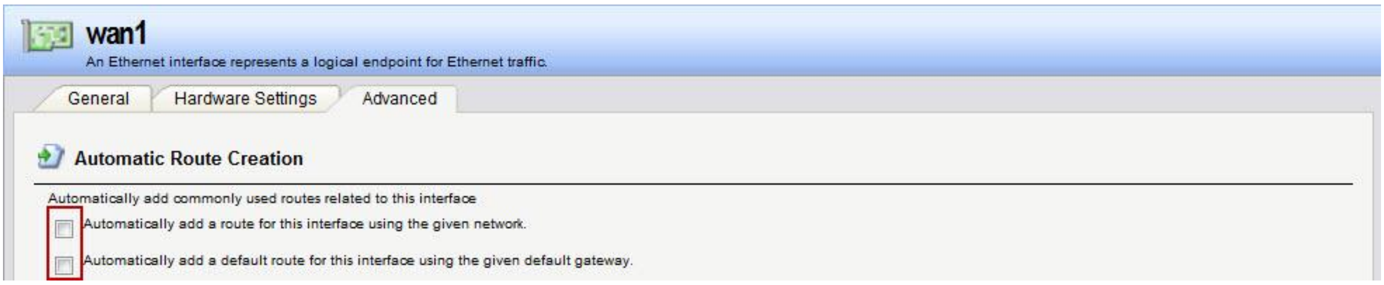
Authentication Objects

Add, remove and modify Pre-Shared Keys and Certificates.

#	Name	Type	Type	Comments
1	HTTPSAdminCert	Certificate	Local	
2	key1	Pre-Shared Key	ASCII	
3	key2	Pre-Shared Key	ASCII	

Right-click on a row for additional options.

2. Interfaces > Ethernet
   Disable WAN1 and WAN2 automatic route.



wan1

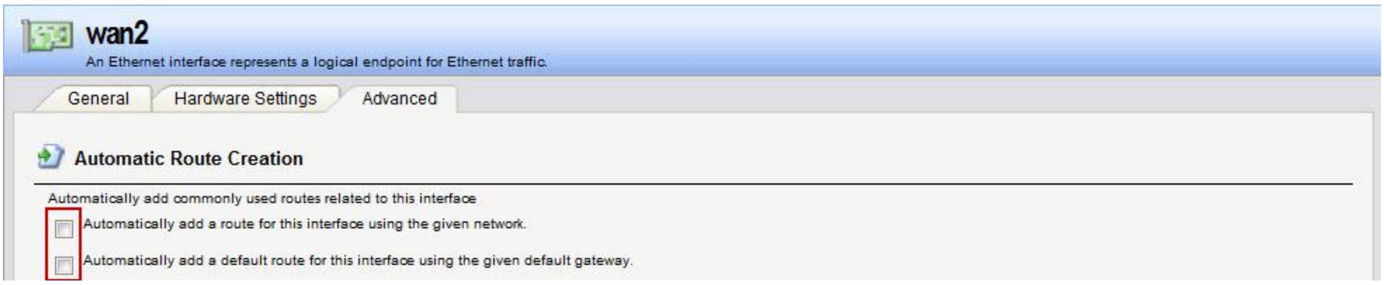
An Ethernet interface represents a logical endpoint for Ethernet traffic.

Automatic Route Creation

Automatically add commonly used routes related to this interface

□ Automatically add a route for this interface using the given network.

□ Automatically add a default route for this interface using the given default gateway.



wan2

An Ethernet interface represents a logical endpoint for Ethernet traffic.

Automatic Route Creation

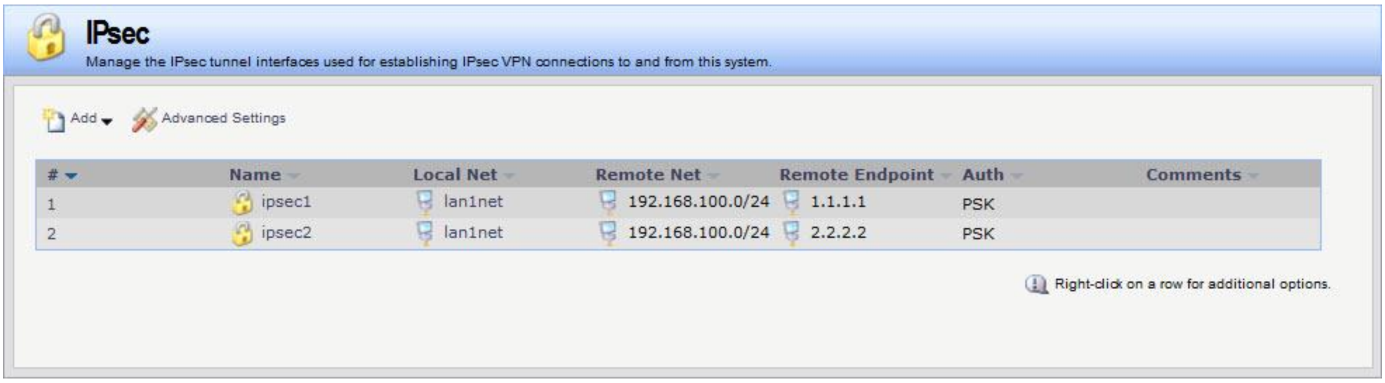
Automatically add commonly used routes related to this interface

□ Automatically add a route for this interface using the given network.

□ Automatically add a default route for this interface using the given default gateway.

3. Interfaces > IPsec

   Make two of IPsec tunnel for different key and remote endpoint.

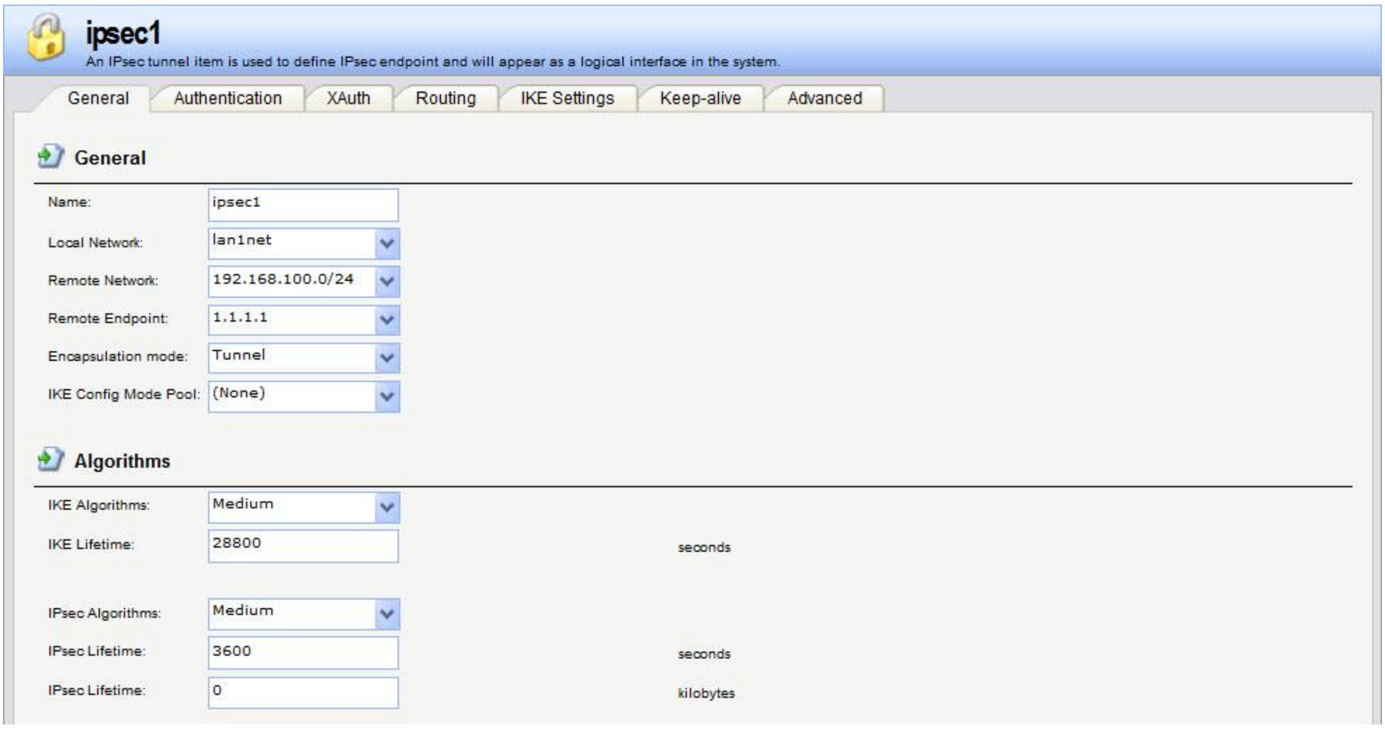


IPsec

Manage the IPsec tunnel interfaces used for establishing IPsec VPN connections to and from this system.

#	Name	Local Net	Remote Net	Remote Endpoint	Auth	Comments
1	ipsec1	lan1net	192.168.100.0/24	1.1.1.1	PSK	
2	ipsec2	lan1net	192.168.100.0/24	2.2.2.2	PSK	

Right-click on a row for additional options.



ipsec1

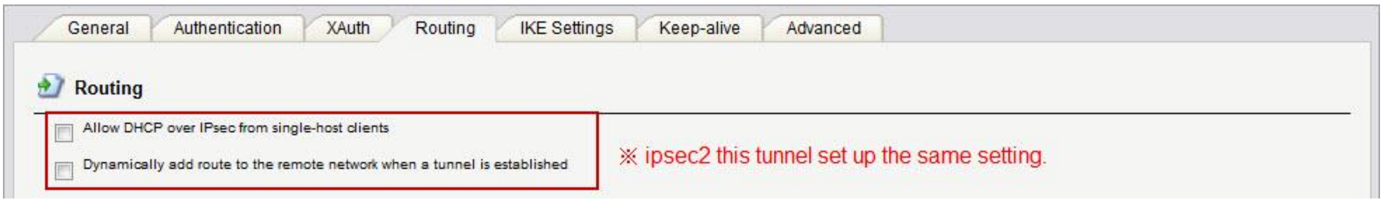
An IPsec tunnel item is used to define IPsec endpoint and will appear as a logical interface in the system.

General

Name:	ipsec1
Local Network:	lan1net
Remote Network:	192.168.100.0/24
Remote Endpoint:	1.1.1.1
Encapsulation mode:	Tunnel
IKE Config Mode Pool:	(None)

Algorithms

IKE Algorithms:	Medium	
IKE Lifetime:	28800	seconds
IPsec Algorithms:	Medium	
IPsec Lifetime:	3600	seconds
IPsec Lifetime:	0	kilobytes

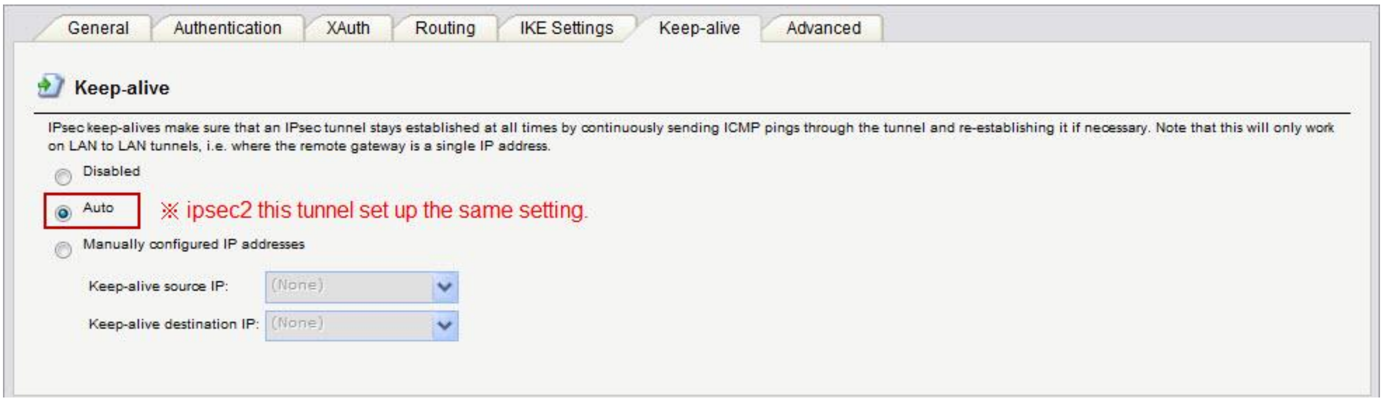


Routing

□ Allow DHCP over IPsec from single-host clients

□ Dynamically add route to the remote network when a tunnel is established

※ ipsec2 this tunnel set up the same setting.



Keep-alive

IPsec keep-alives make 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.

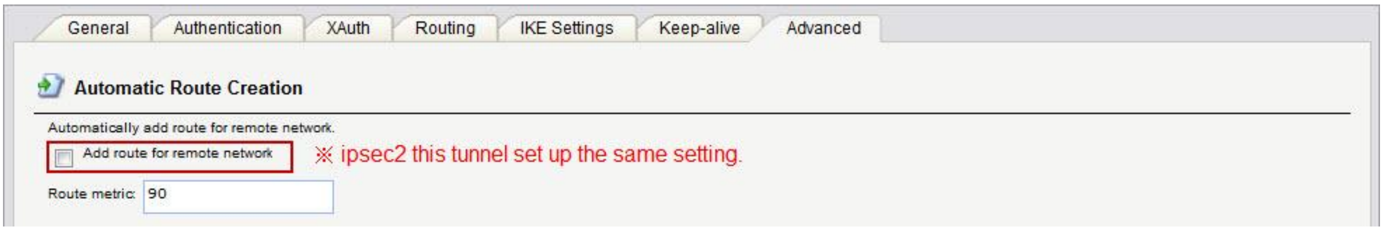
○ Disabled

● Auto ※ ipsec2 this tunnel set up the same setting.

○ Manually configured IP addresses

Keep-alive source IP: (None)

Keep-alive destination IP: (None)

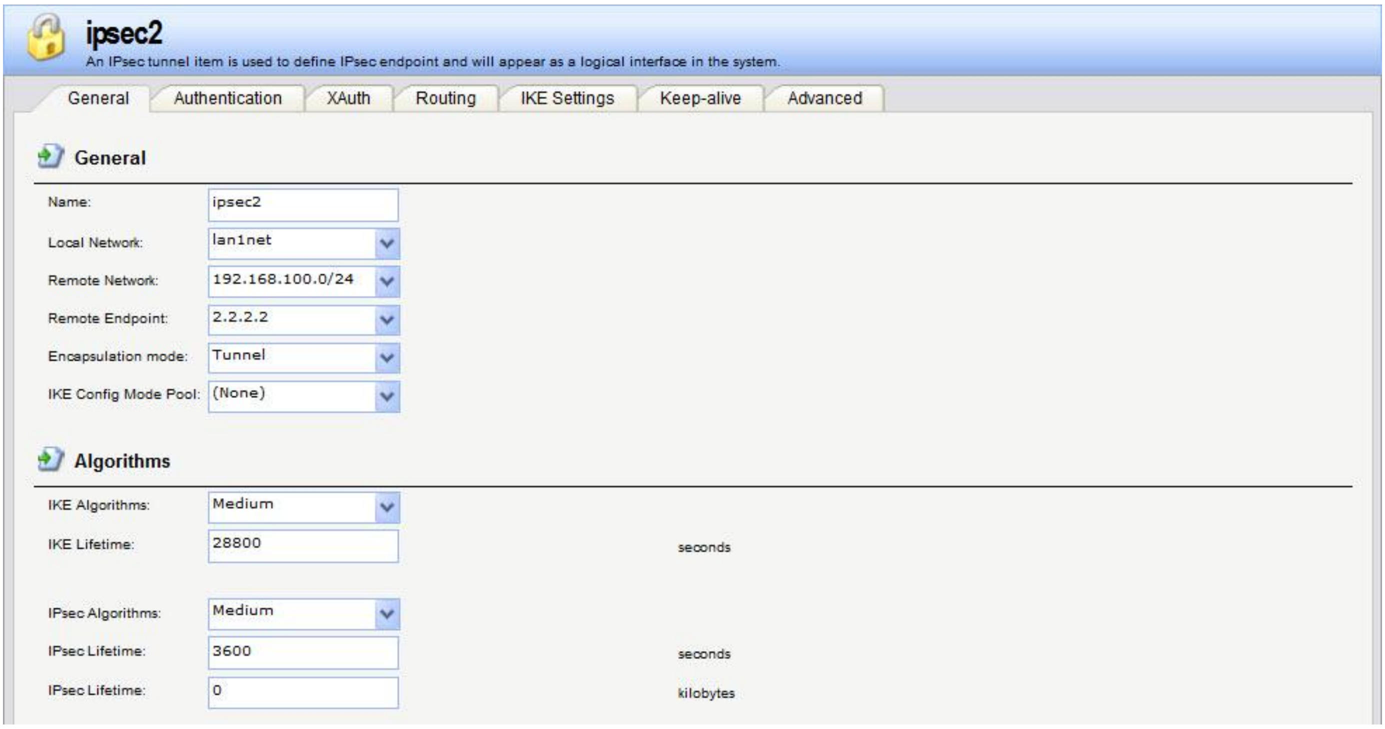


Automatic Route Creation

Automatically add route for remote network.

□ Add route for remote network ※ ipsec2 this tunnel set up the same setting.

Route metric: 90


ipsec2

An IPsec tunnel item is used to define IPsec endpoint and will appear as a logical interface in the system.

General

Name: ipsec2

Local Network: lan1net

Remote Network: 192.168.100.0/24

Remote Endpoint: 2.2.2.2

Encapsulation mode: Tunnel

IKE Config Mode Pool: (None)

Algorithms

IKE Algorithms: Medium

IKE Lifetime: 28800 seconds

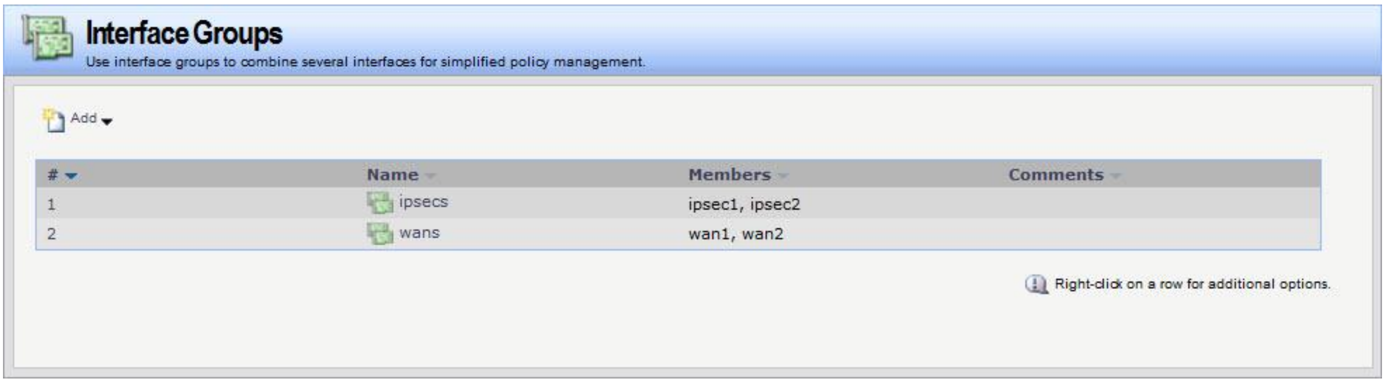
IPsec Algorithms: Medium

IPsec Lifetime: 3600 seconds

IPsec Lifetime: 0 kilobytes

4. Interfaces > Interfaces Groups

   Setup interfaces groups for IP rules.

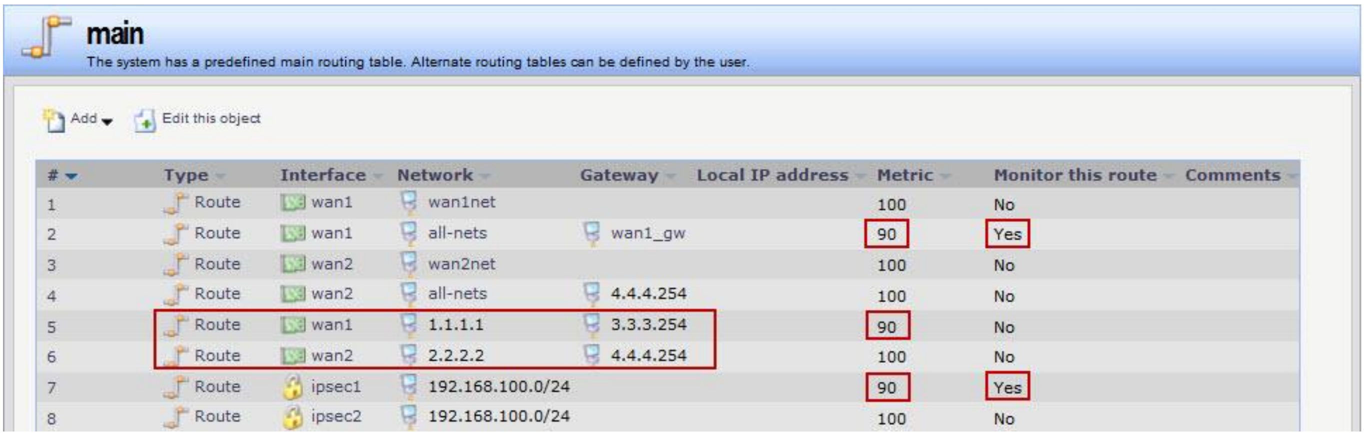

Interface Groups

Use interface groups to combine several interfaces for simplified policy management.

#	Name	Members	Comments
1	ipsecs	ipsec1, ipsec2	
2	wans	wan1, wan2	

Right-click on a row for additional options.

5. Routing > Routing Tables > Main



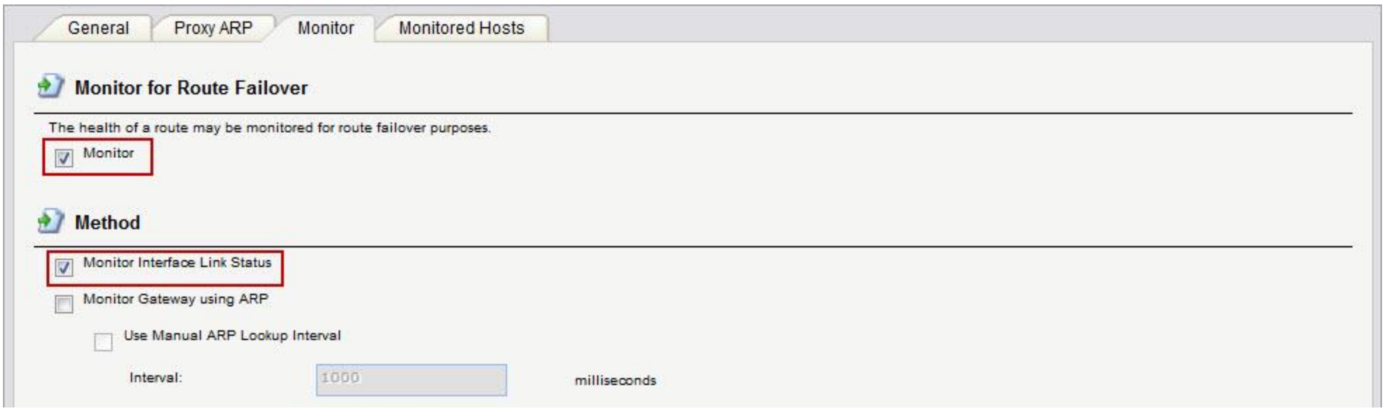
main

The system has a predefined main routing table. Alternate routing tables can be defined by the user.

#	Type	Interface	Network	Gateway	Local IP address	Metric	Monitor this route	Comments
1	Route	wan1	wan1net			100	No	
2	Route	wan1	all-nets	wan1_gw		90	Yes	
3	Route	wan2	wan2net			100	No	
4	Route	wan2	all-nets	4.4.4.254		100	No	
5	Route	wan1	1.1.1.1	3.3.3.254		90	No	
6	Route	wan2	2.2.2.2	4.4.4.254		100	No	
7	Route	ipsec1	192.168.100.0/24			90	Yes	
8	Route	ipsec2	192.168.100.0/24			100	No	

We have some of very important parts on routing rules setup.

1. Only monitor two of routing rules. (Index 2 & 7)
2. Index 5 & 6 must setup remote endpoint and local interface gateway.
3. The monitor set up only need to use interface link status.
4. Index 2 & 5 & 7 metric must law than the partner rules.



Monitor for Route Failover

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

☑ Monitor

Method

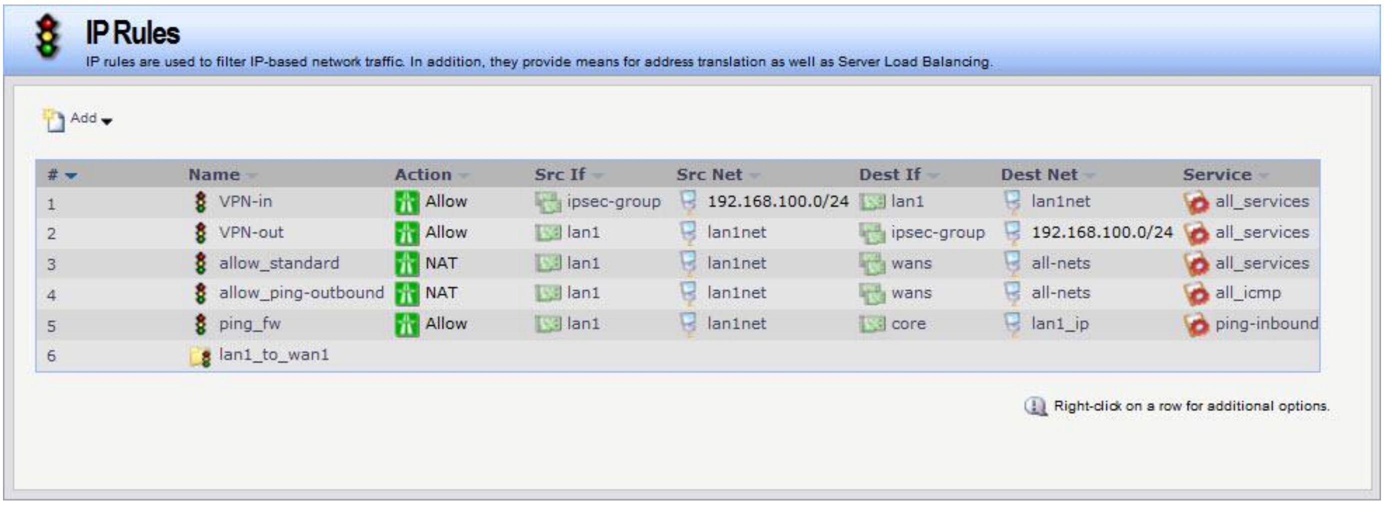
☑ Monitor Interface Link Status

□ Monitor Gateway using ARP

□ Use Manual ARP Lookup Interval

Interval: 1000 milliseconds

6. Rules > IP Rules



IP Rules

IP rules are used to filter IP-based network traffic. In addition, they provide means for address translation as well as Server Load Balancing.

#	Name	Action	Src If	Src Net	Dest If	Dest Net	Service
1	VPN-in	Allow	ipsec-group	192.168.100.0/24	lan1	lan1net	all_services
2	VPN-out	Allow	lan1	lan1net	ipsec-group	192.168.100.0/24	all_services
3	allow_standard	NAT	lan1	lan1net	wans	all-nets	all_services
4	allow_ping-outbound	NAT	lan1	lan1net	wans	all-nets	all_icmp
5	ping_fw	Allow	lan1	lan1net	core	lan1_ip	ping-inbound
6	lan1_to_wan1						

Right-click on a row for additional options.

END