How do I configure an IPSec LAN-to-LAN tunnel between two locations (Office A and Office B)?

Note: *This FAQ will demonstrate setting up a Lan-to-Lan IPSec VPN tunnel between firewall A and B.*

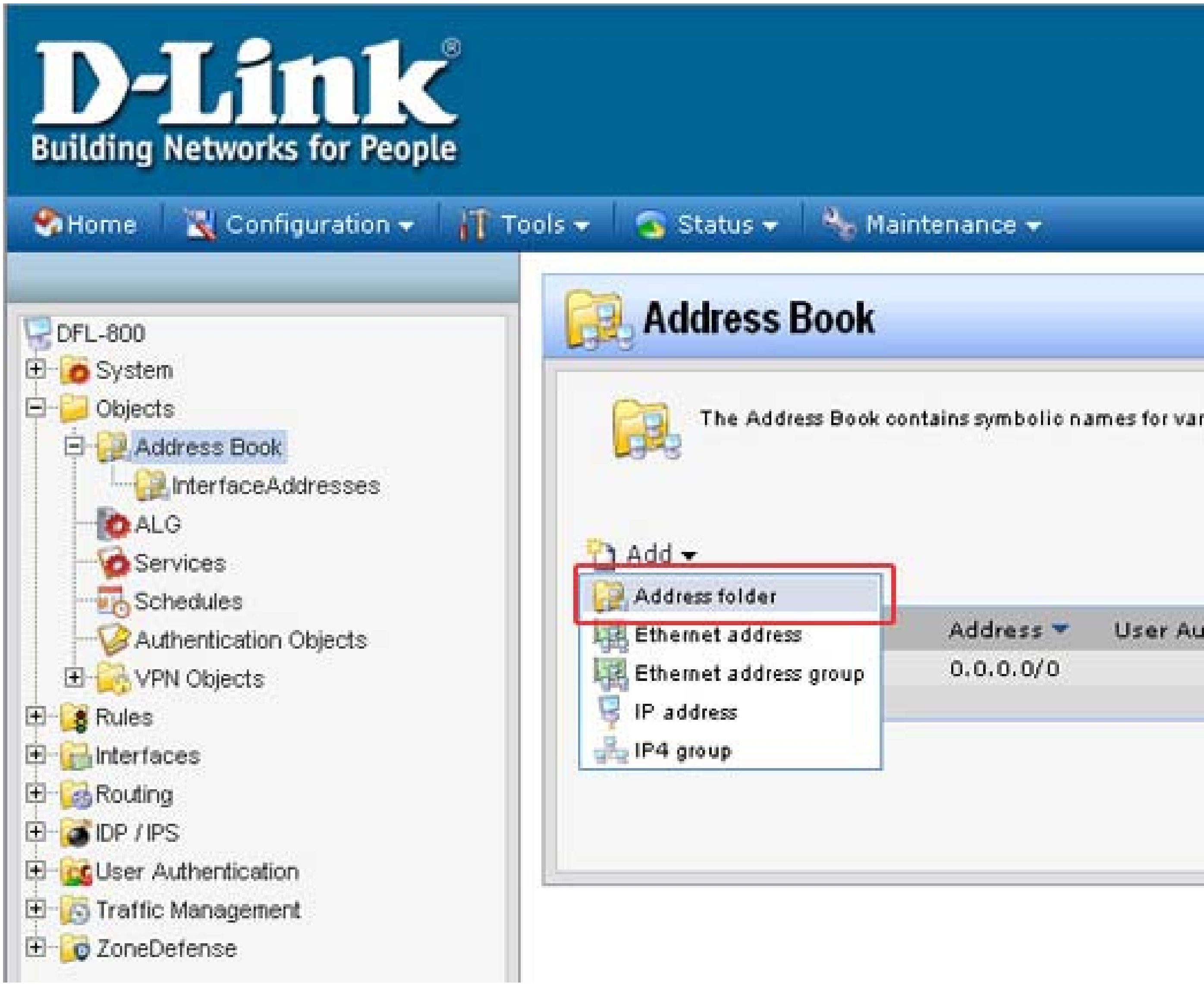
In this example:
Firewall A *is on* ***192.168.1.0/24 network***
Firewall B *is on* ***192.168.2.0/24 network***

Configuration of Firewall A

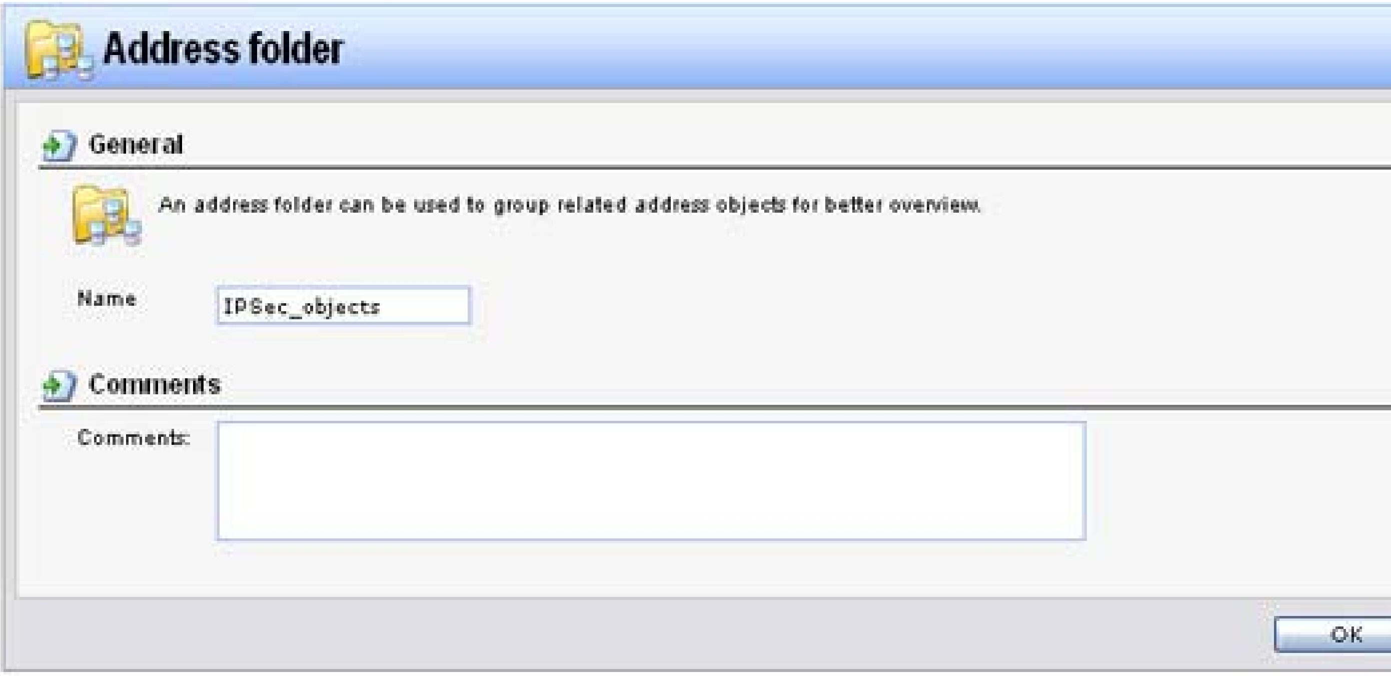
Step 1: Open your web browser and type in the IP address of the Firewall (*192.168.1.1* by default). Enter the username (*admin* by default) and password (*admin* by default), and then click **OK**.

Step 2: Click the plus sign next to **Objects** and select **Address Book**.

Step 3: Click **Add** and select **Address Folder** from the dropdown menu.



Step 4: Enter a name for the folder and click **OK**.



Address folder

General

An address folder can be used to group related address objects for better overview.

Name: IPSec_objects

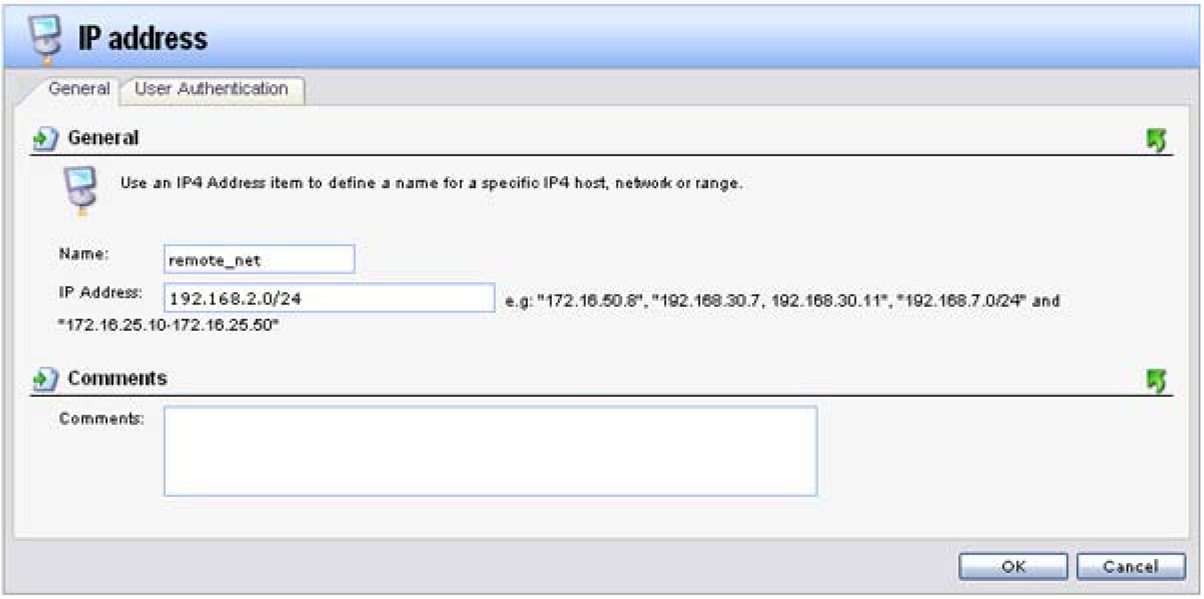
Comments

Comments:

Step 5: Click **Add** and select **IP address** from the dropdown menu and configure as followed:

- **Name:** enter a name as desired (*remote_net* in this example)
- **IP Address:** enter the remote subnet of the remote firewall (*192.168.2.0/24* in this example)

Click **OK**.



IP address

General

Use an IP4 Address item to define a name for a specific IP4 host, network or range.

Name: remote_net

IP Address: 192.168.2.0/24 e.g: "172.16.50.8", "192.168.30.7, 192.168.30.11", "192.168.7.0/24" and "172.16.25.10-172.16.25.50"

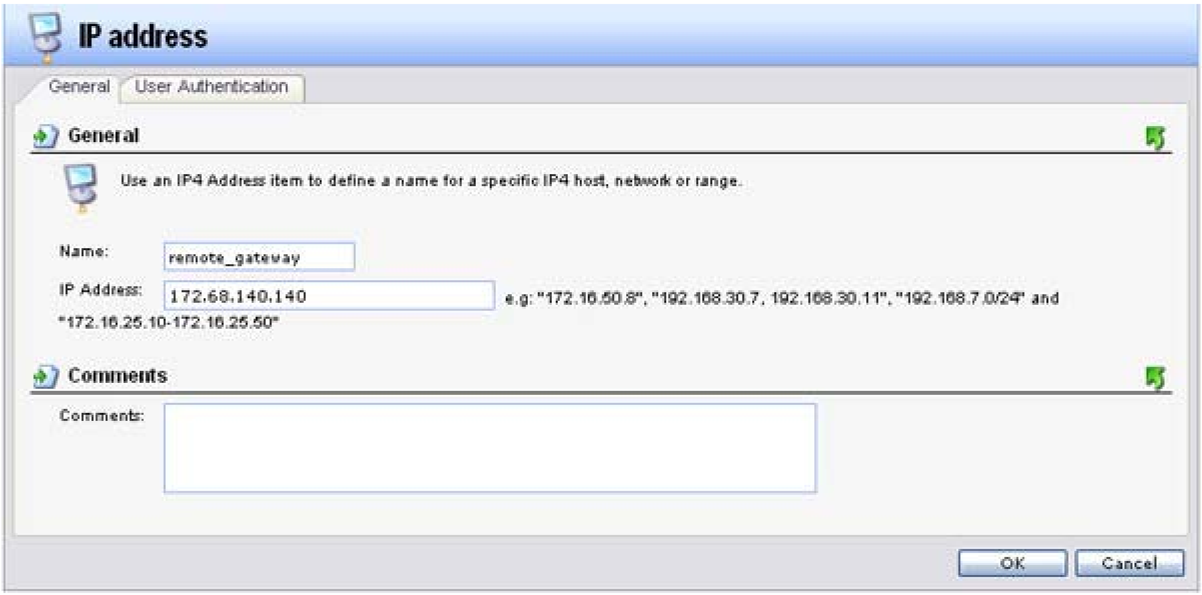
Comments

Comments:

Step 6: Click **Add** and select IP address from the dropdown menu and configure as followed:

- **Name:** enter a name as desired (*remote_gateway* in this example)
- **IP Address:** enter the gateway of the remote location

Click **OK**.



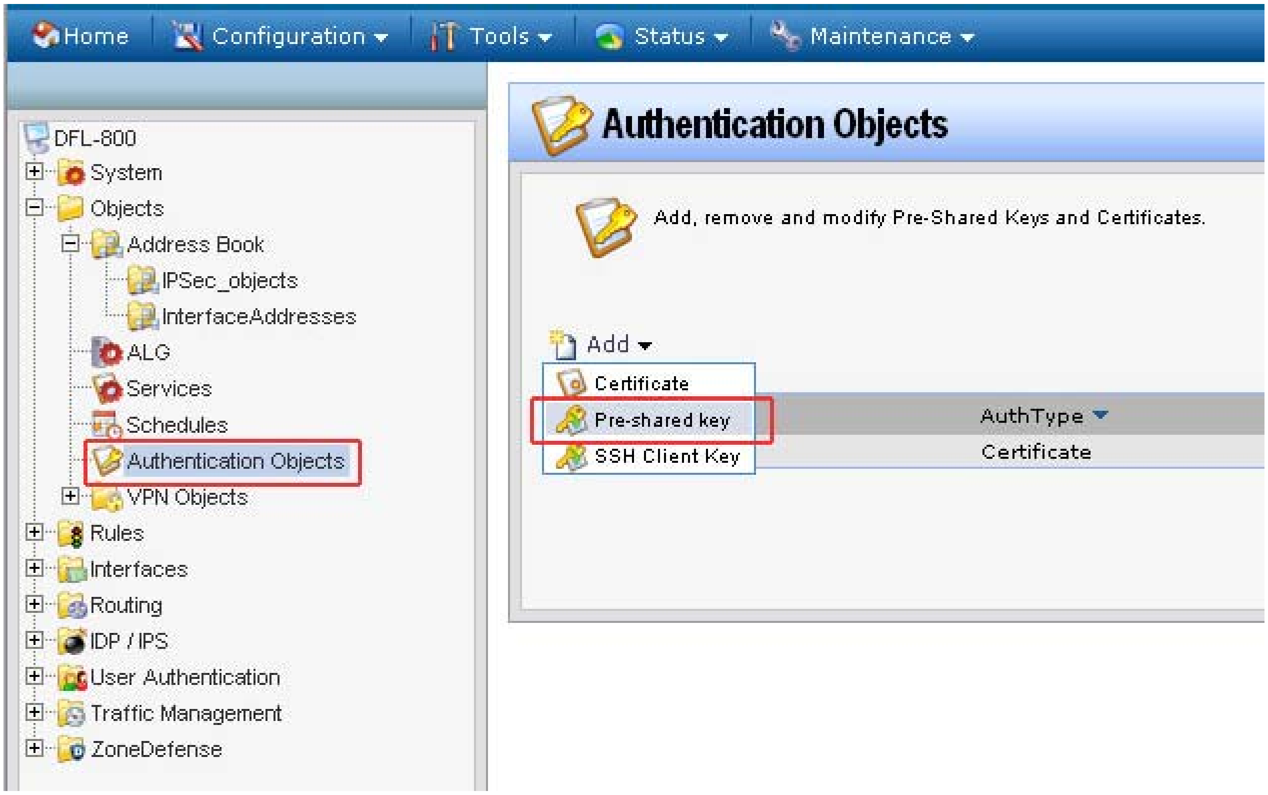
Use an IP4 Address item to define a name for a specific IP4 host, network or range.

Name: remote_gateway

IP Address: 172.68.140.140 e.g: "172.16.50.8", "192.168.30.7, 192.168.30.11", "192.168.7.0/24" and "172.16.25.10-172.16.25.50"

Comments:

Step 7: Click on **Authentication Objects**, click on **Add** and select **Pre-shared key** from the dropdown menu to add a *Pre-shared key*.



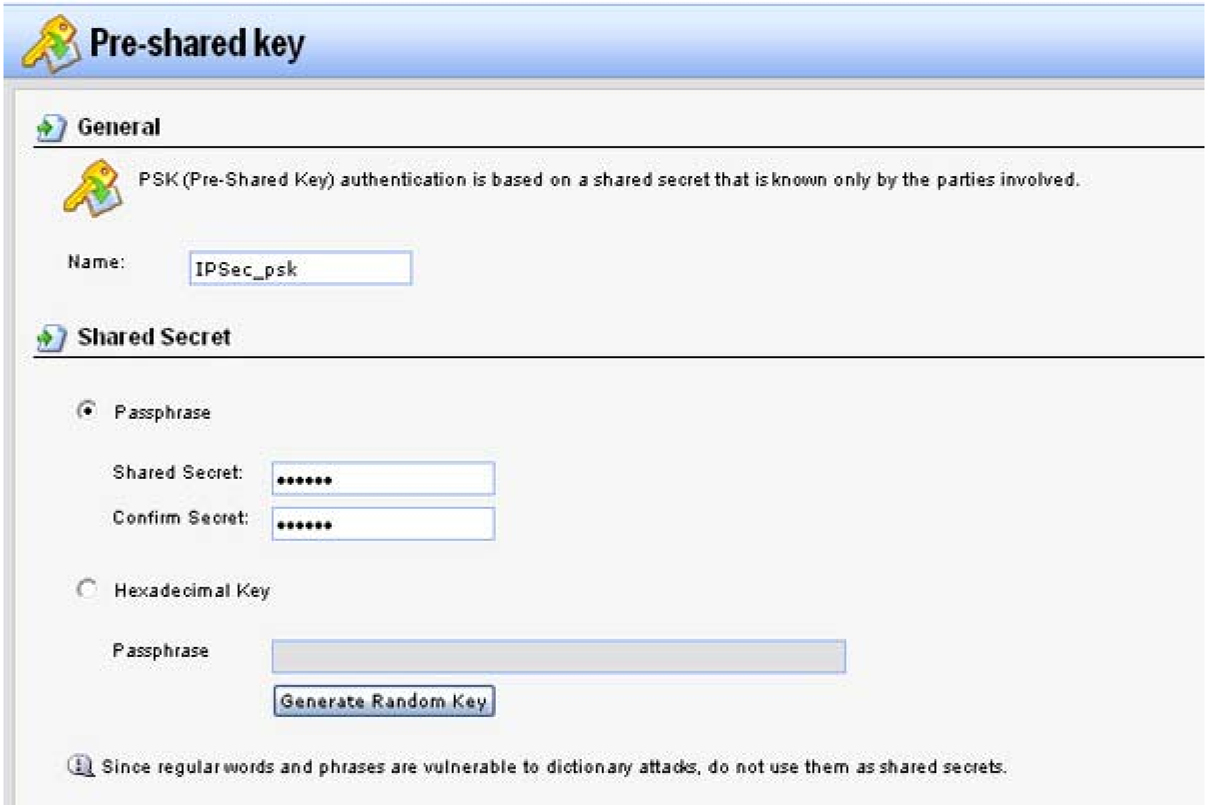
Step 8: Configure the *Pre-shared key* as followed:

- **Name:** enter a name as desired (IPSec_psk in this example)

Passphrase

- **Shared Secret:** enter a desired key
- **Confirm Secret:** re-enter the key

Click **OK**.



Pre-shared key

General

PSK (Pre-Shared Key) authentication is based on a shared secret that is known only by the parties involved.

Name: IPSec_psk

Shared Secret

● Passphrase

Shared Secret: ••••••

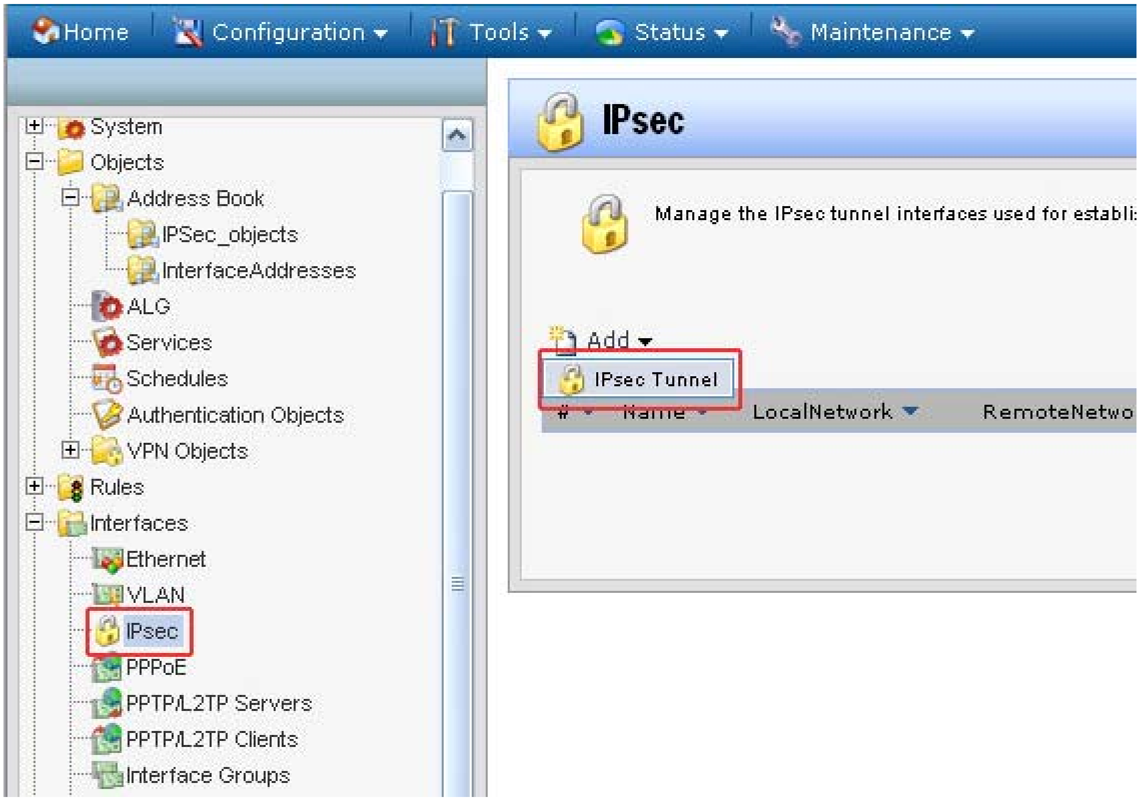
Confirm Secret: ••••••

○ Hexadecimal Key

Passphrase

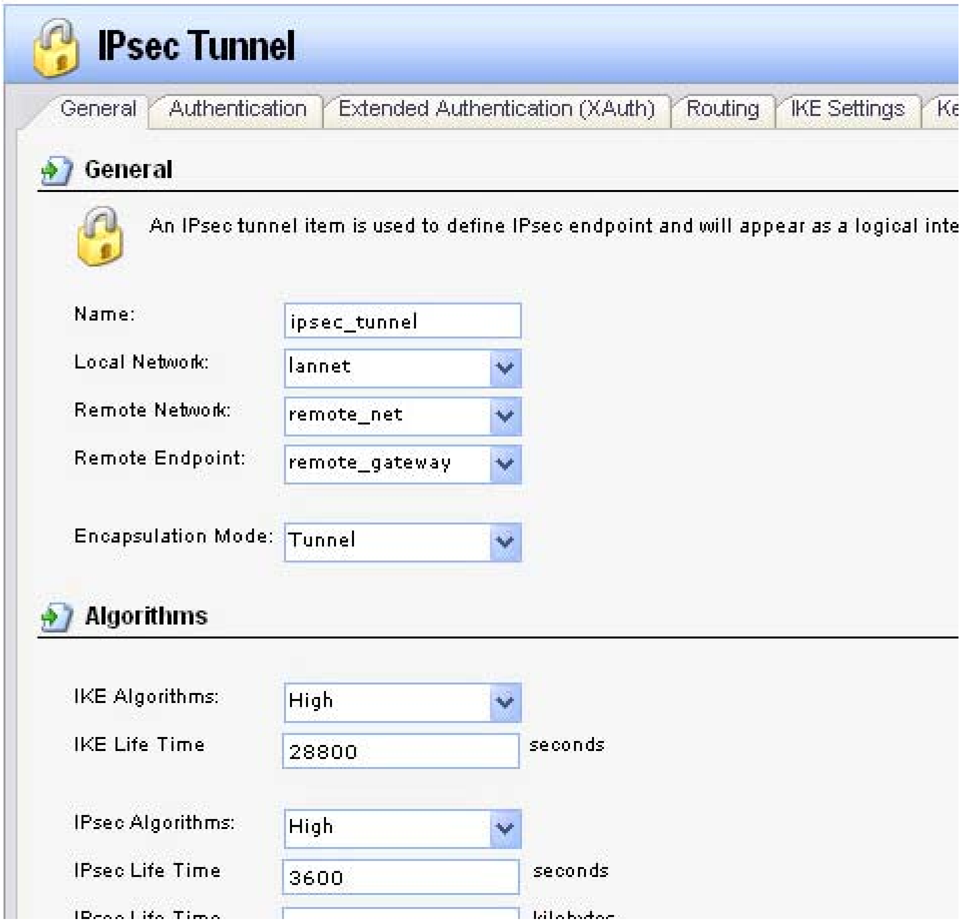
Since regular words and phrases are vulnerable to dictionary attacks, do not use them as shared secrets.

Step 9: Click the plus sign next to **Interfaces** and select **IPsec**. Click **Add** and select **IPsec Tunnel** from the dropdown menu.



Step 10: Configure the *IPsec Tunnel* as followed:

- **Name:** enter a name as desired (*ipsec_tunnel* in this example)
- **Local Network:** lannet
- **Remote Network:** remote_net (created in *step 5*)
- **Remote Endpoint:** remote_gateway (created in *step 6*)
- **Encapsulation Mode:** Tunnel
- **IKE Algorithms:** High
- **IKE Life Time:** 28800 secs
- **IPsec Algorithms:** High
- **IPsec Life Time:** 3600 secs



General

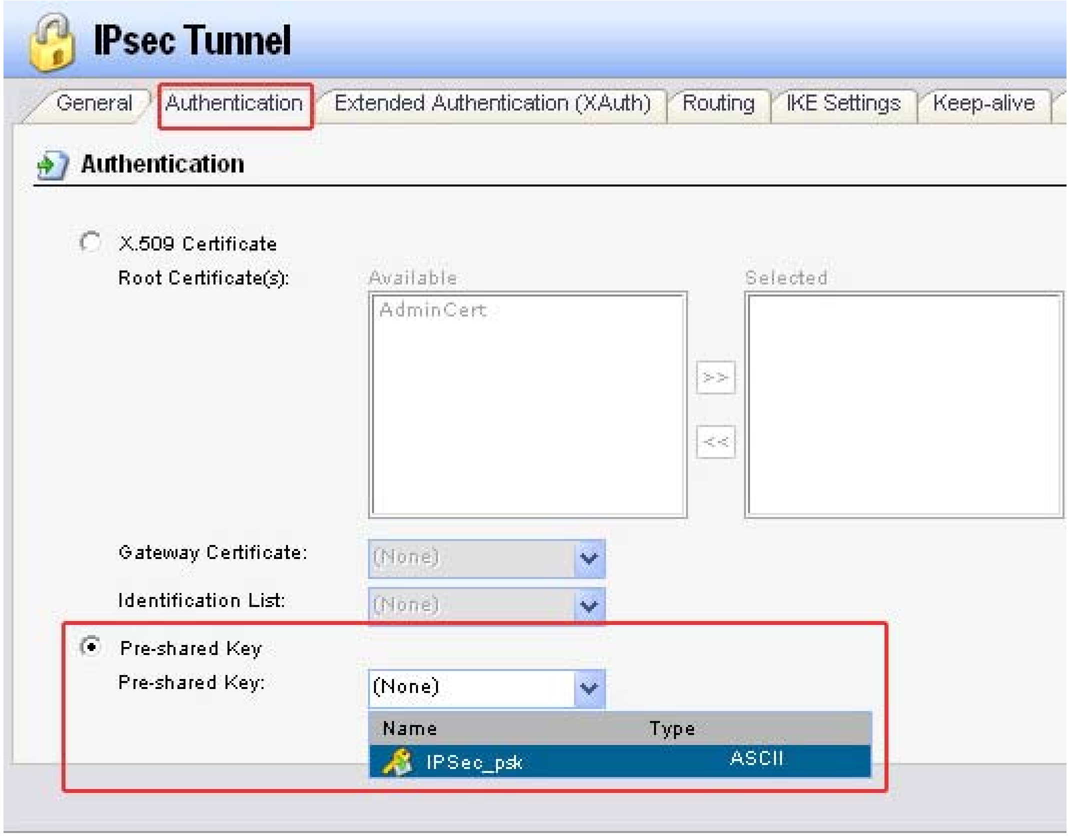
An IPsec tunnel item is used to define IPsec endpoint and will appear as a logical inte

Name:	ipsec_tunnel
Local Network:	lannet
Remote Network:	remote_net
Remote Endpoint:	remote_gateway
Encapsulation Mode:	Tunnel

Algorithms

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

Step 11: Click on the **Authentication** tab and select the *pre-shared key* (created in *step 8*) from the **Pre-Shared Key** dropdown menu.



Authentication

○ X.509 Certificate

Root Certificate(s): Available: AdminCert | Selected:

Gateway Certificate: (None)

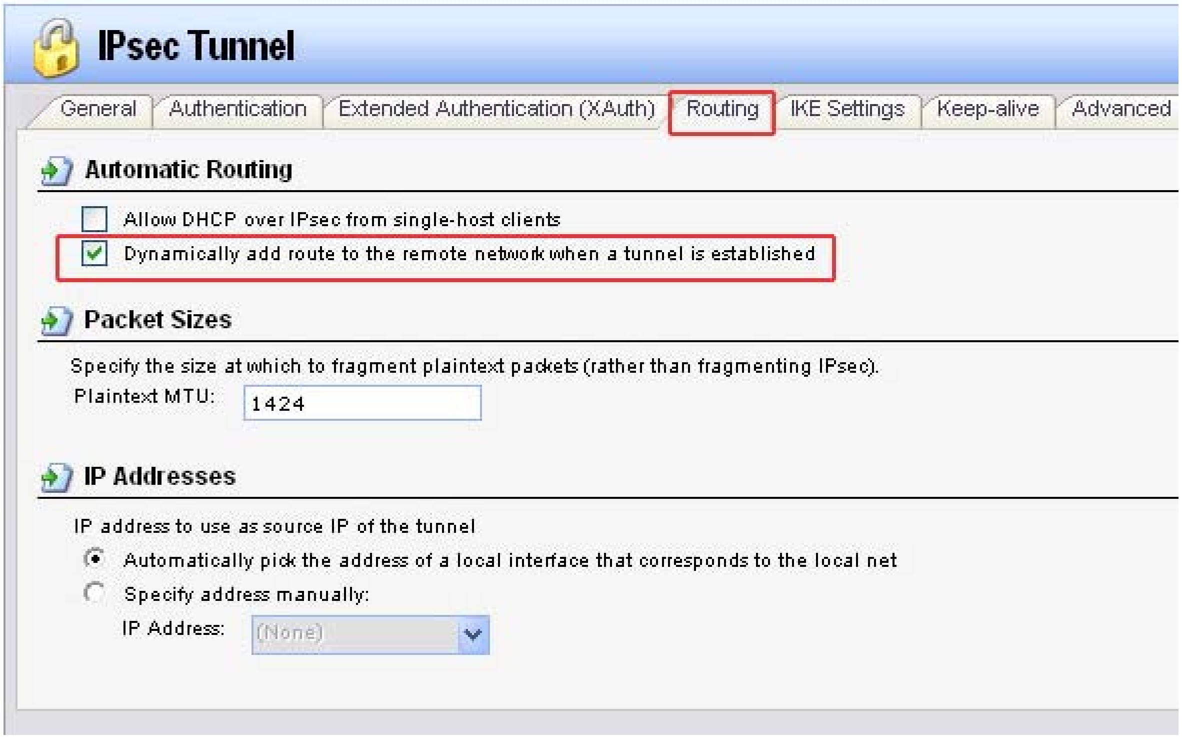
Identification List: (None)

● Pre-shared Key

Pre-shared Key: (None)

Name	Type
IPSec_psk	ASCII

Step 12: Click on the **Routing** tab and check the box labeled **Dynamically add route to the remote network when a tunnel is established**.



Automatic Routing

□ Allow DHCP over IPsec from single-host clients

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

Packet Sizes

Specify the size at which to fragment plaintext packets (rather than fragmenting IPsec).

Plaintext MTU: 1424

IP Addresses

IP address to use as source IP of the tunnel

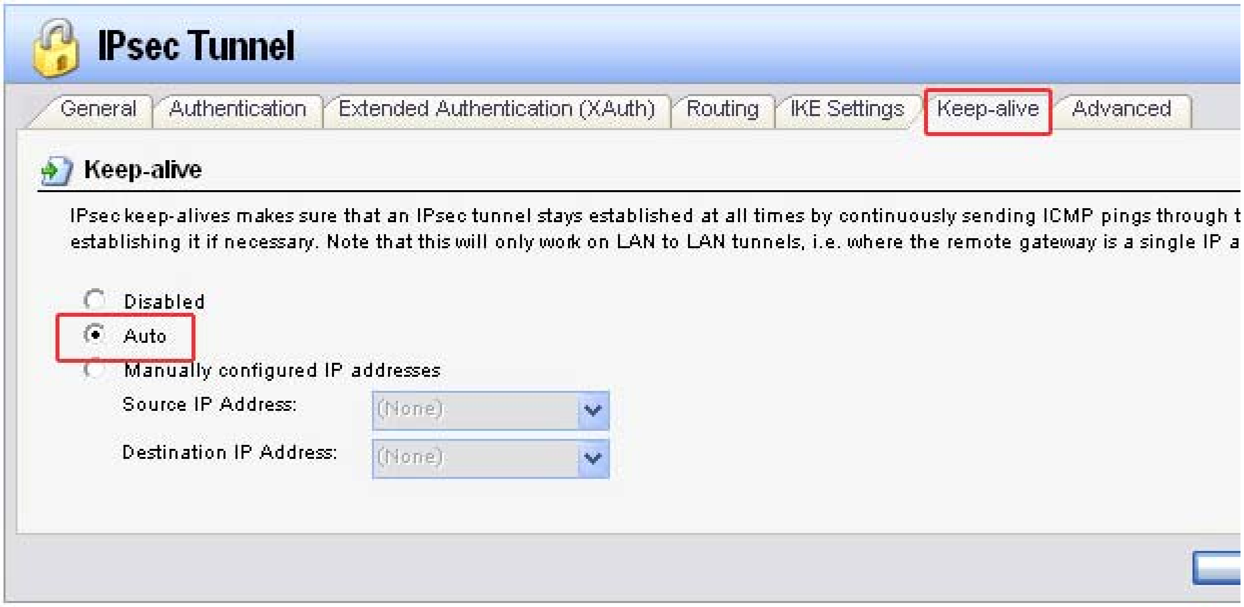
● Automatically pick the address of a local interface that corresponds to the local net

○ Specify address manually:

IP Address: (None)

Step 13: Click on the **Keep-alive** tab and select **Auto**.

Click **OK**.



Keep-alive

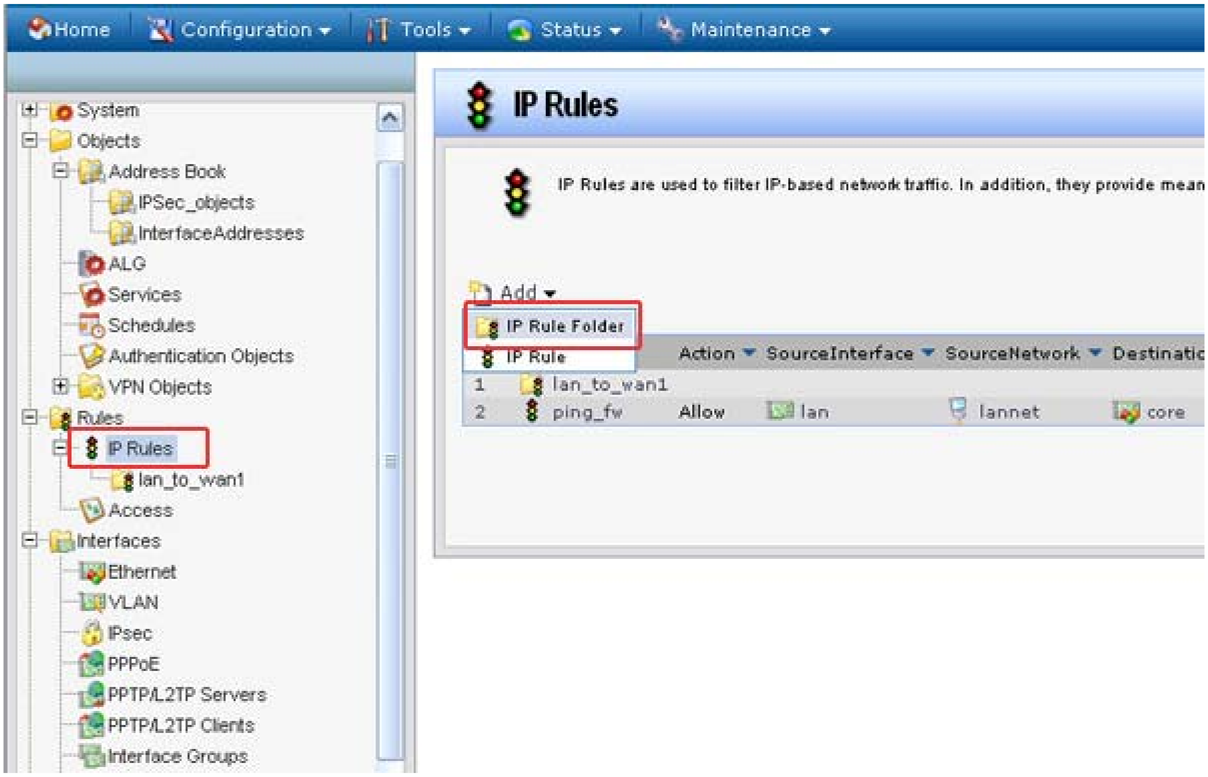
IPsec keep-alives makes sure that an IPsec tunnel stays established at all times by continuously sending ICMP pings through t
establishing it if necessary. Note that this will only work on LAN to LAN tunnels, i.e. where the remote gateway is a single IP a

○ Disabled
● Auto
○ Manually configured IP addresses

Source IP Address: (None)

Destination IP Address: (None)

Step 14: Click the plus sign next to **Rules** and select **IP Rules**. Click **Add** and select **IP Rule Folder**.

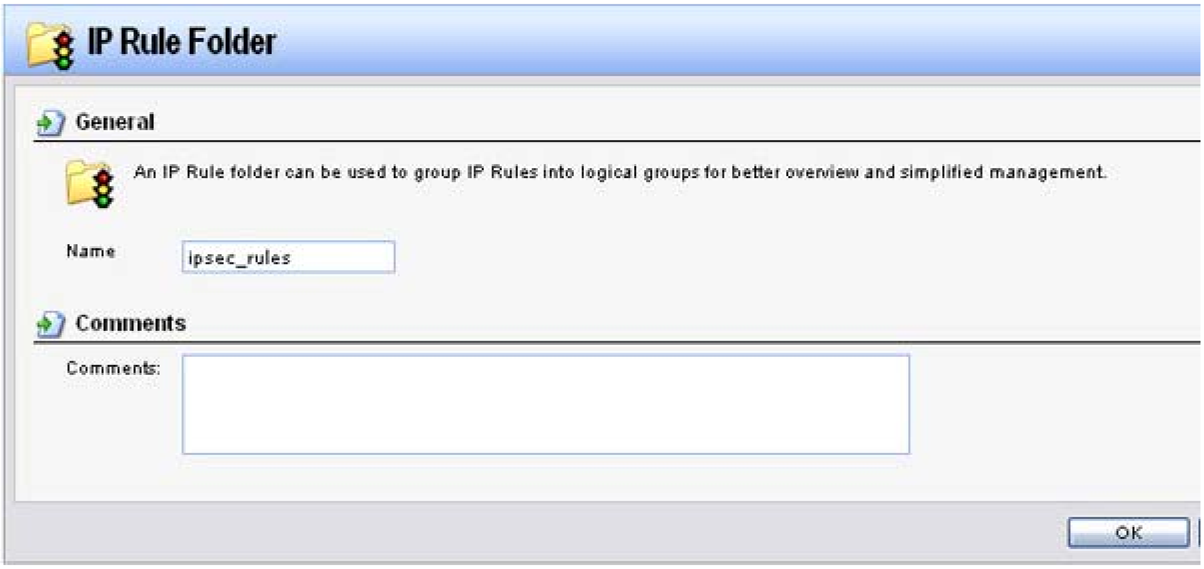


IP Rules

IP Rules are used to filter IP-based network traffic. In addition, they provide mean

		Action	SourceInterface	SourceNetwork	Destinatio
1	lan_to_wan1				
2	ping_fw	Allow	lan	lannet	core

Step 15: Enter a name for the folder and click **OK**.



IP Rule Folder

General

An IP Rule folder can be used to group IP Rules into logical groups for better overview and simplified management.

Name: ipsec_rules

Comments

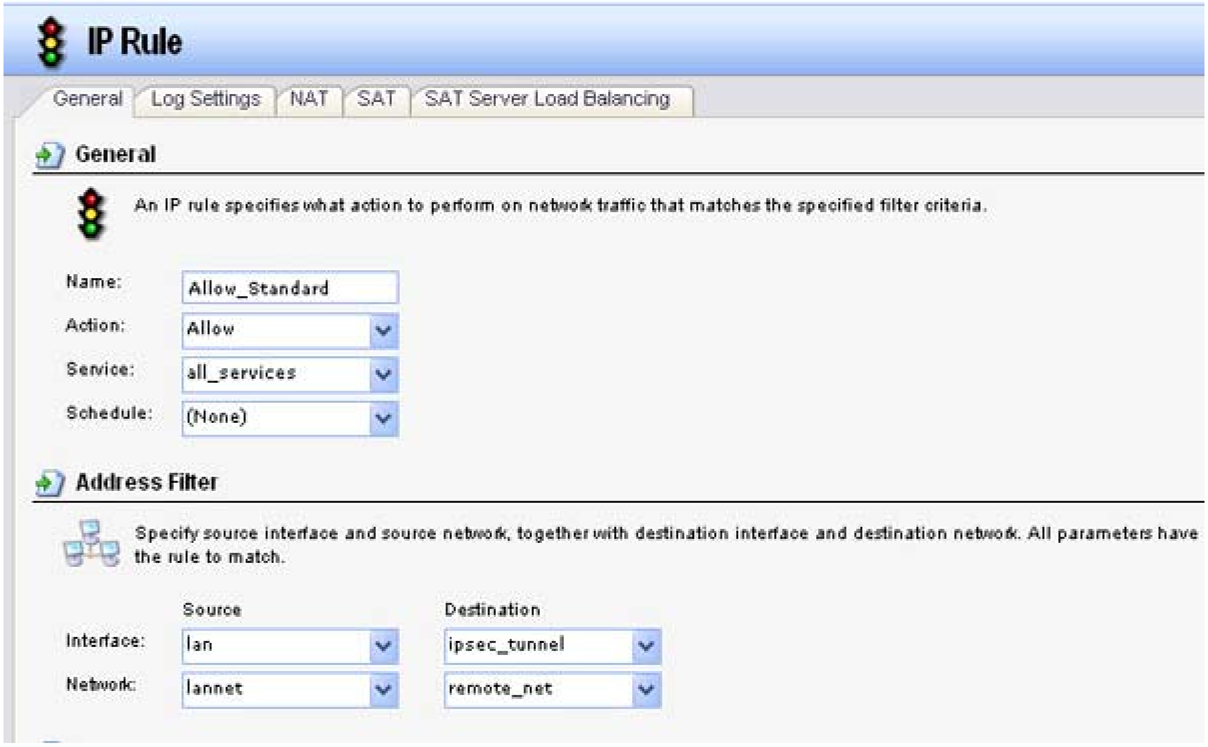
Comments:

Step 16: Click **Add** and select **IP Rule**. Configure the *IP Rule* as followed:

- **Name:** enter a name as desired
- **Action:** Allow
- **Service:** all_services

- **Schedule:** None
- **Source interface:** lan
- **Source network:** lannet
- **Destination interface:** ipsec_tunnel (created in *step 10*)
- **Destination network:** remote_net (created in *step 5*)

Click **OK**.



IP Rule

General

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

Name:	Allow_Standard
Action:	Allow
Service:	all_services
Schedule:	(None)

Address Filter

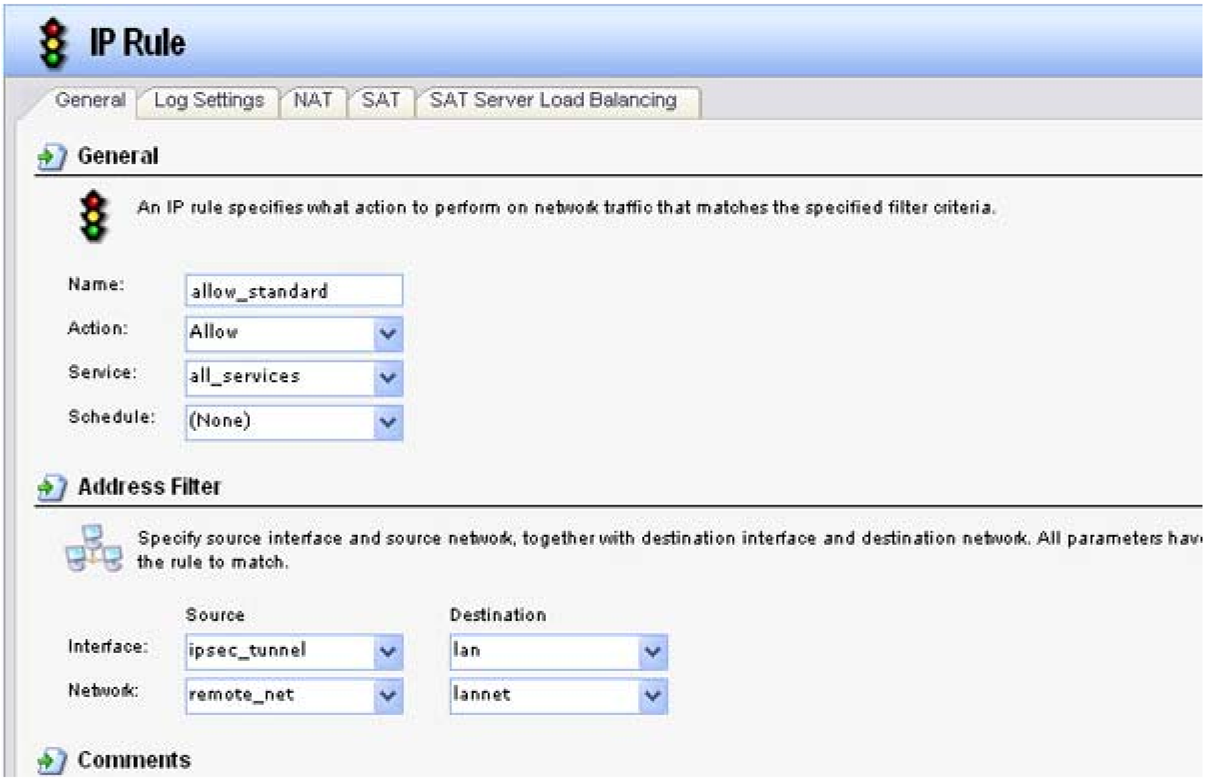
Specify source interface and source network, together with destination interface and destination network. All parameters have the rule to match.

	Source	Destination
Interface:	lan	ipsec_tunnel
Network:	lannet	remote_net

Step 17: Click **Add** and select **IP Rule**. Configure the *IP Rule* as followed:

- **Name:** enter a name as desired
- **Action:** Allow
- **Service:** all_services
- **Schedule:** None
- **Source interface:** ipsec_tunnel (created in *step 10*)
- **Source network:** remote_net (created in *step 5*)
- **Destination interface:** lan
- **Destination network:** lannet

Click **OK**.



General

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

Name: allow_standard

Action: Allow

Service: all_services

Schedule: (None)

Address Filter

Specify source interface and source network, together with destination interface and destination network. All parameters hav the rule to match.

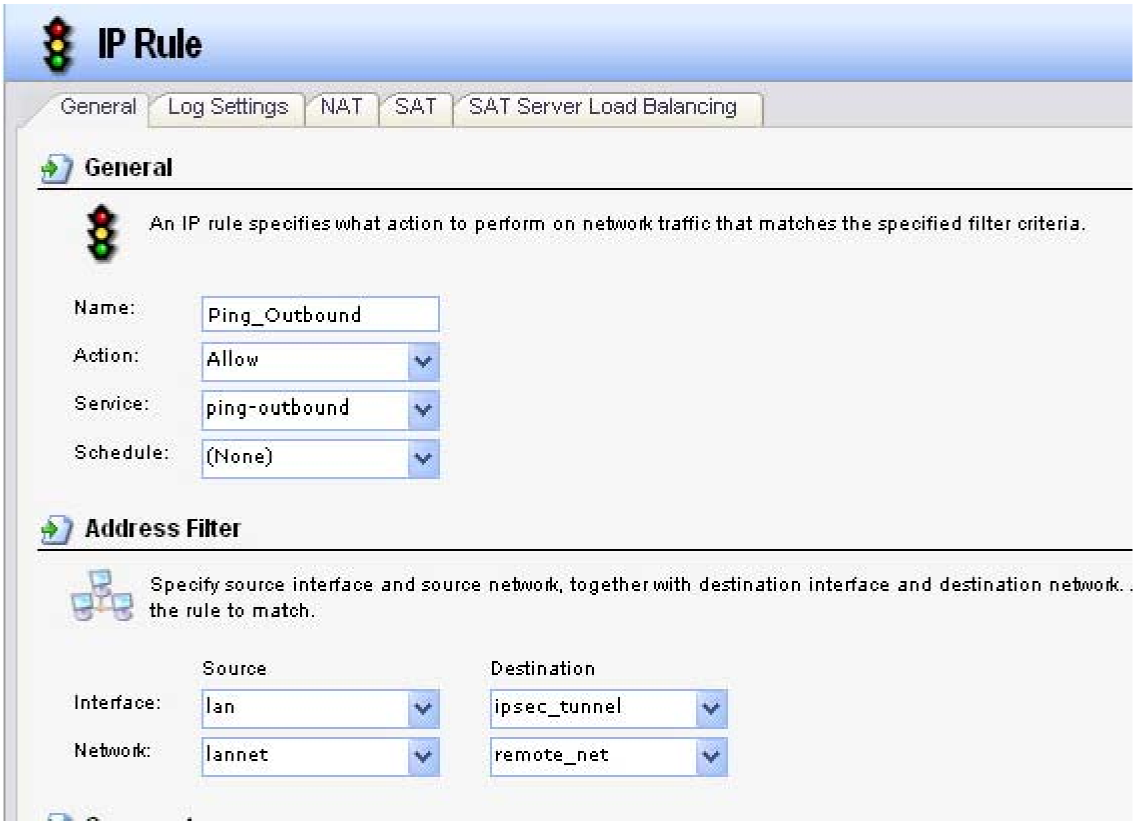
	Source	Destination
Interface:	ipsec_tunnel	lan
Network:	remote_net	lannet

Comments

Step 18: Click **Add** and select **IP Rule**. Configure the *IP Rule* as followed:

- **Name:** enter a name as desired
- **Action:** Allow
- **Service:** ping-outbound
- **Schedule:** None
- **Source interface:** lan
- **Source network:** lannet
- **Destination interface:** ipsec_tunnel (created in *step 10*)
- **Destination network:** remote_net (created in *step 5*)

Click **OK**.



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

Name: Ping_Outbound

Action: Allow

Service: ping-outbound

Schedule: (None)

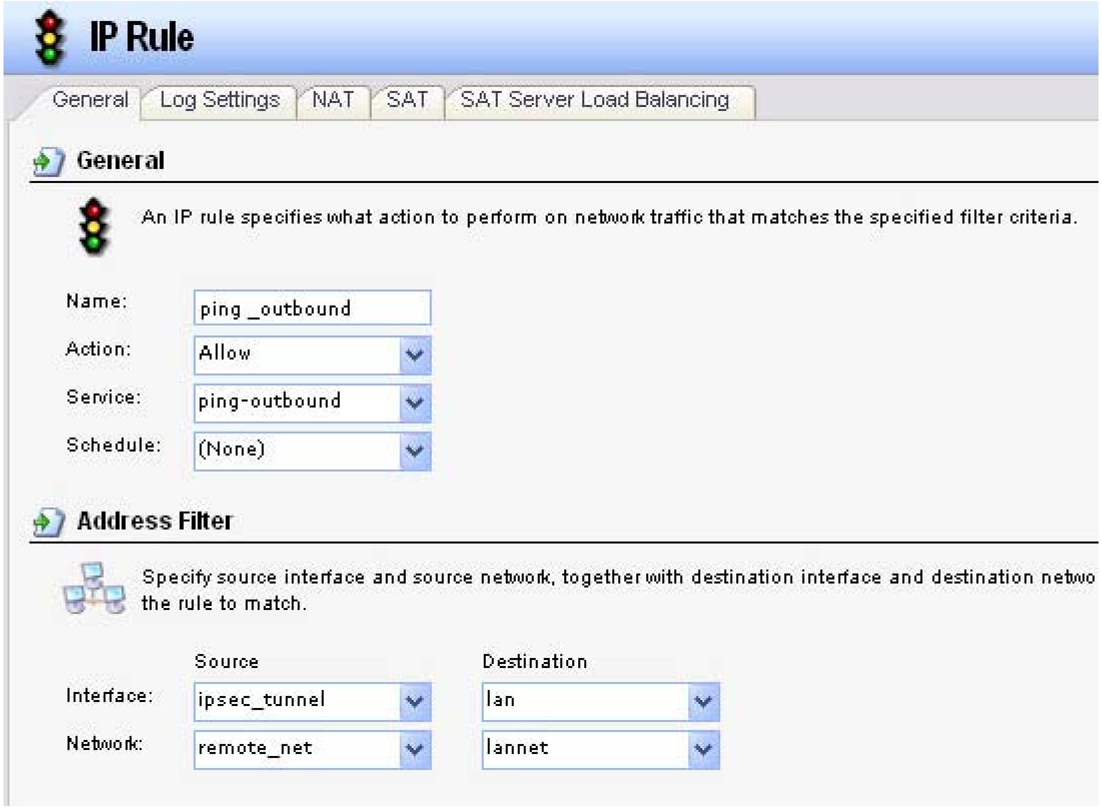
Specify source interface and source network, together with destination interface and destination network. . the rule to match.

	Source	Destination
Interface:	lan	ipsec_tunnel
Network:	lannet	remote_net

Step 19: Click **Add** and select **IP Rule**. Configure the *IP Rule* as followed:

- **Name:** enter a name as desired
- **Action:** Allow
- **Service:** ping-outbound
- **Schedule:** None
- **Source interface:** ipsec_tunnel (created in *step 10*)
- **Source network:** remote_net (created in *step 5*)
- **Destination interface:** lan
- **Destination network:** lannet

Click **OK**.



General

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

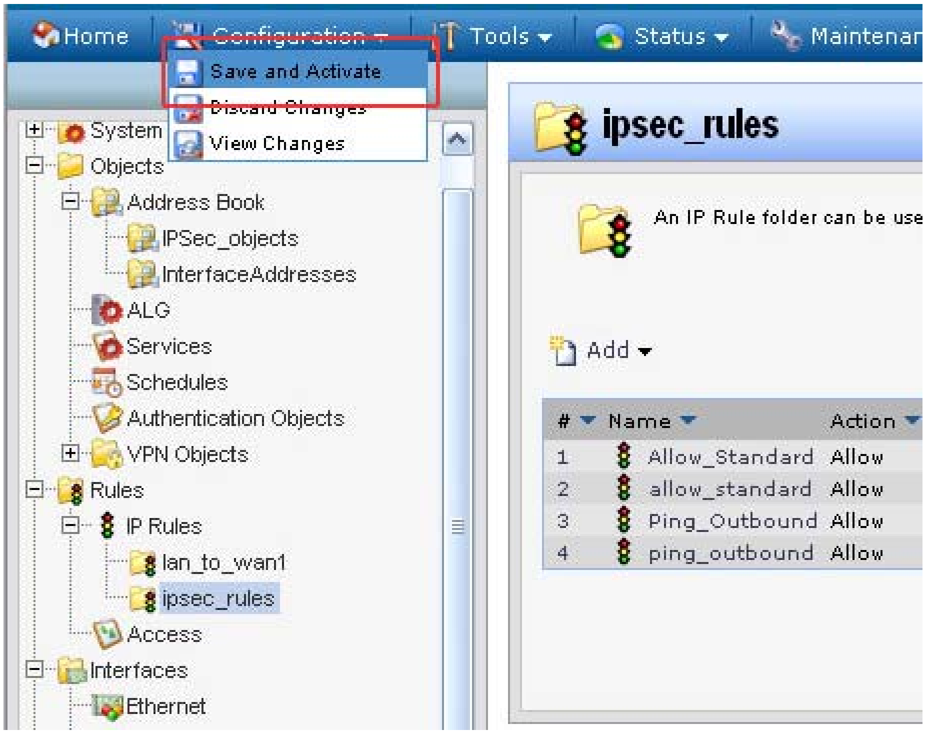
Name:	ping _outbound
Action:	Allow
Service:	ping-outbound
Schedule:	(None)

Address Filter

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

	Source	Destination
Interface:	ipsec_tunnel	lan
Network:	remote_net	lannet

Step 20: Click **Configuration** and select **Save and Activate**. Click **OK** to activate changes.



An IP Rule folder can be use

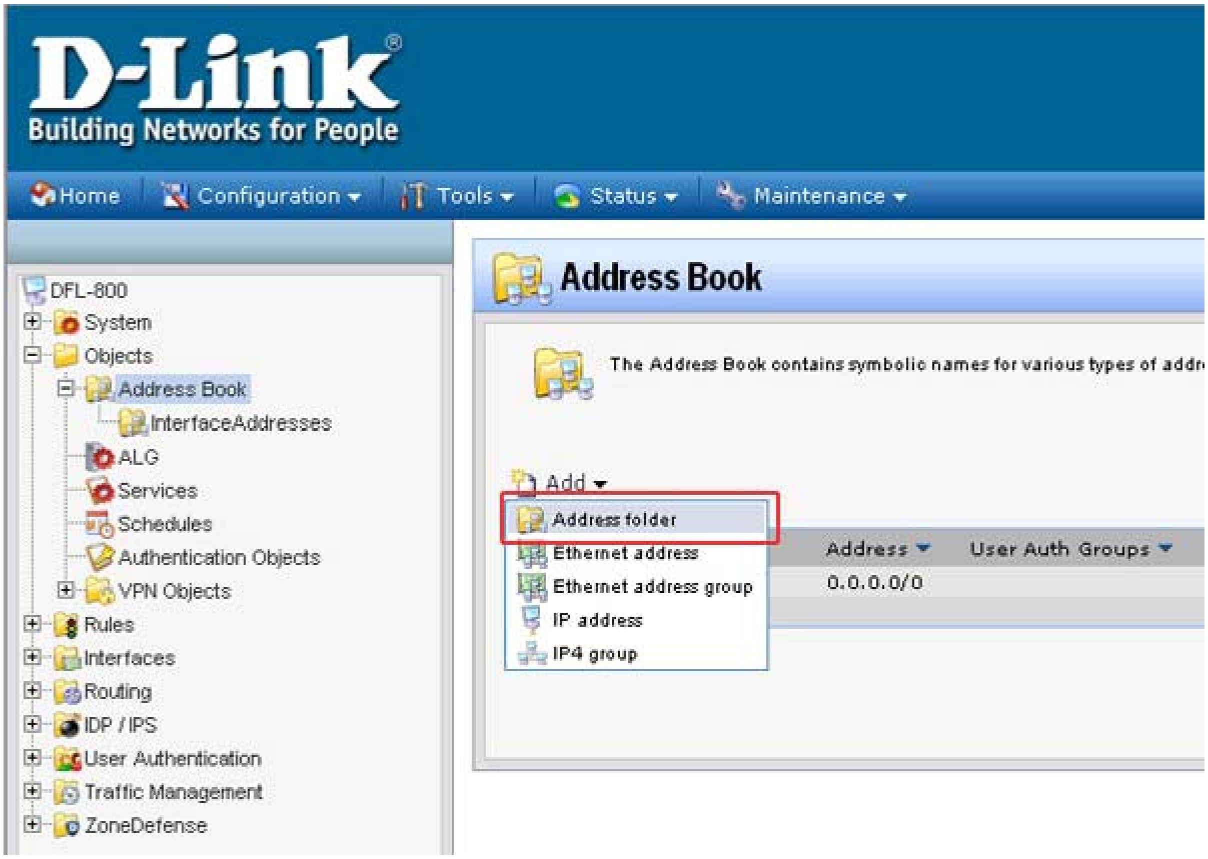
#	Name	Action
1	Allow_Standard	Allow
2	allow_standard	Allow
3	Ping_Outbound	Allow
4	ping_outbound	Allow

Configuration of Firewall B

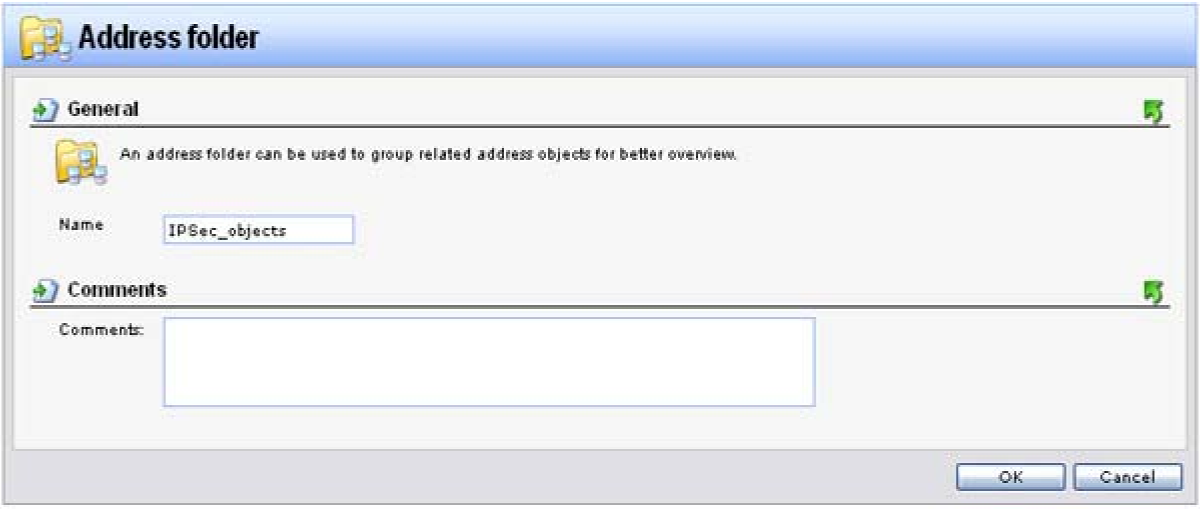
Step 1: Open your web browser and type in the IP address of the Firewall (*192.168.1.1* by default). Enter the username (*admin* by default) and password (*admin* by default), and then click **OK**.

Step 2: Click the plus sign next to **Objects** and select **Address Book**.

Step 3: Click **Add** and select **Address Folder** from the dropdown menu.



Step 4: Enter a name for the folder and click **OK**.



An address folder can be used to group related address objects for better overview.

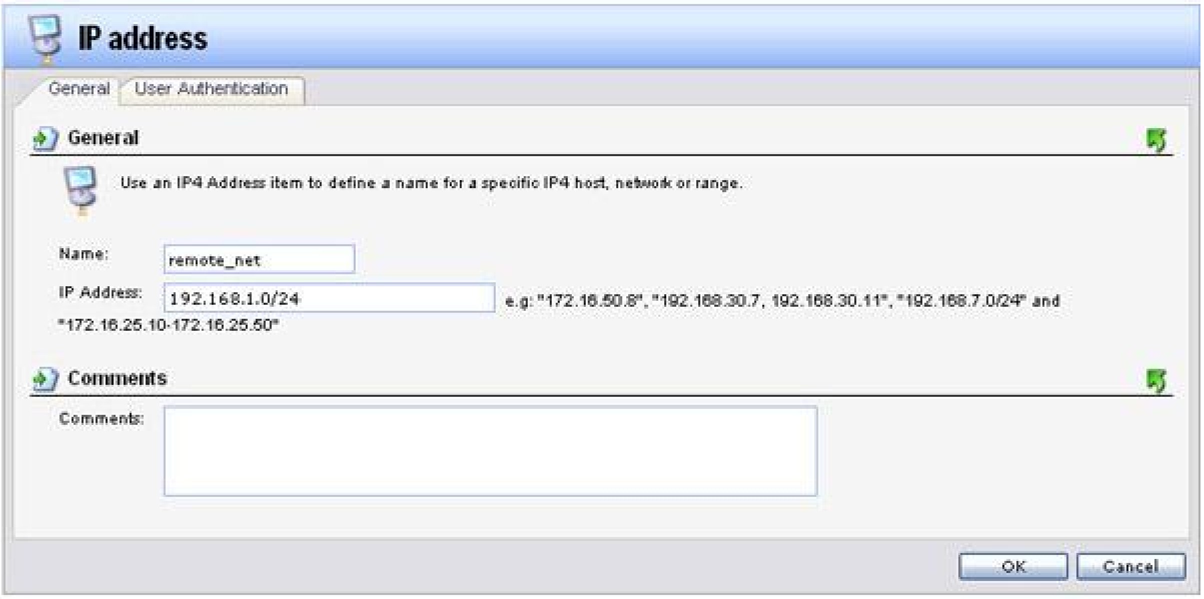
Name: IPSec_objects

Comments:

Step 5: Click **Add** and select **IP address** from the dropdown menu and configure as followed:

- **Name:** enter a name as desired (*remote_net* in this example)
- **IP Address:** enter the remote subnet of the remote firewall (*192.168.1.0/24* in this example)

Click **OK**.



Use an IP4 Address item to define a name for a specific IP4 host, network or range.

Name: remote_net

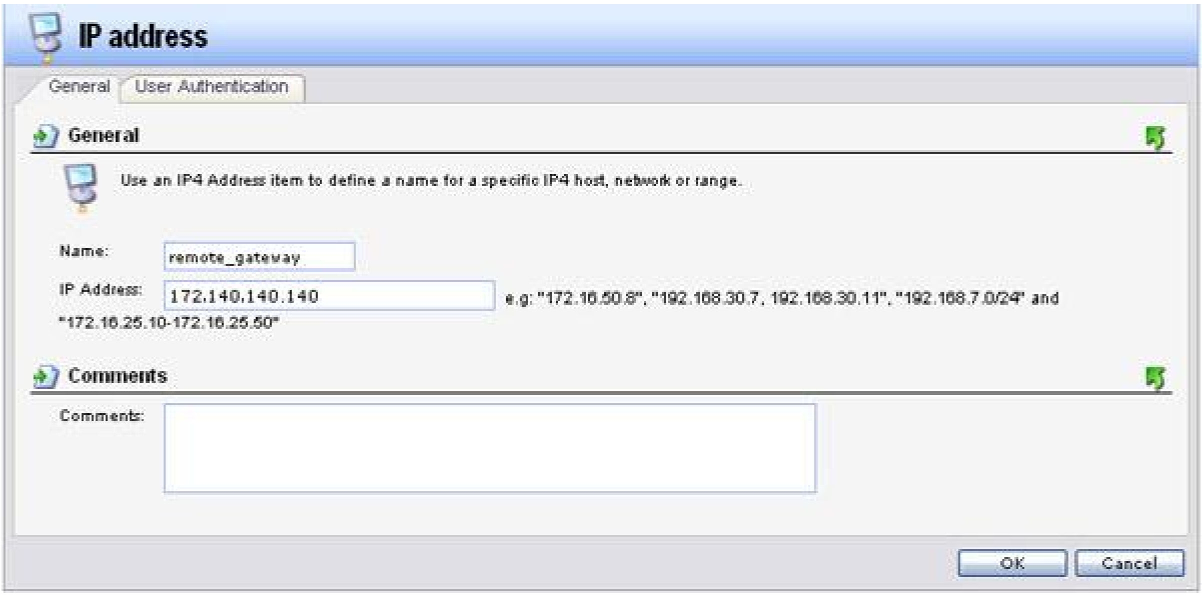
IP Address: 192.168.1.0/24 e.g: "172.16.50.8", "192.168.30.7, 192.168.30.11", "192.168.7.0/24" and "172.16.25.10-172.16.25.50"

Comments:

Step 6: Click **Add** and select IP address from the dropdown menu and configure as followed:

- **Name:** enter a name as desired (*remote_gateway* in this example)
- **IP Address:** enter the gateway of the remote location

Click **OK**.



IP address

General

Use an IP4 Address item to define a name for a specific IP4 host, network or range.

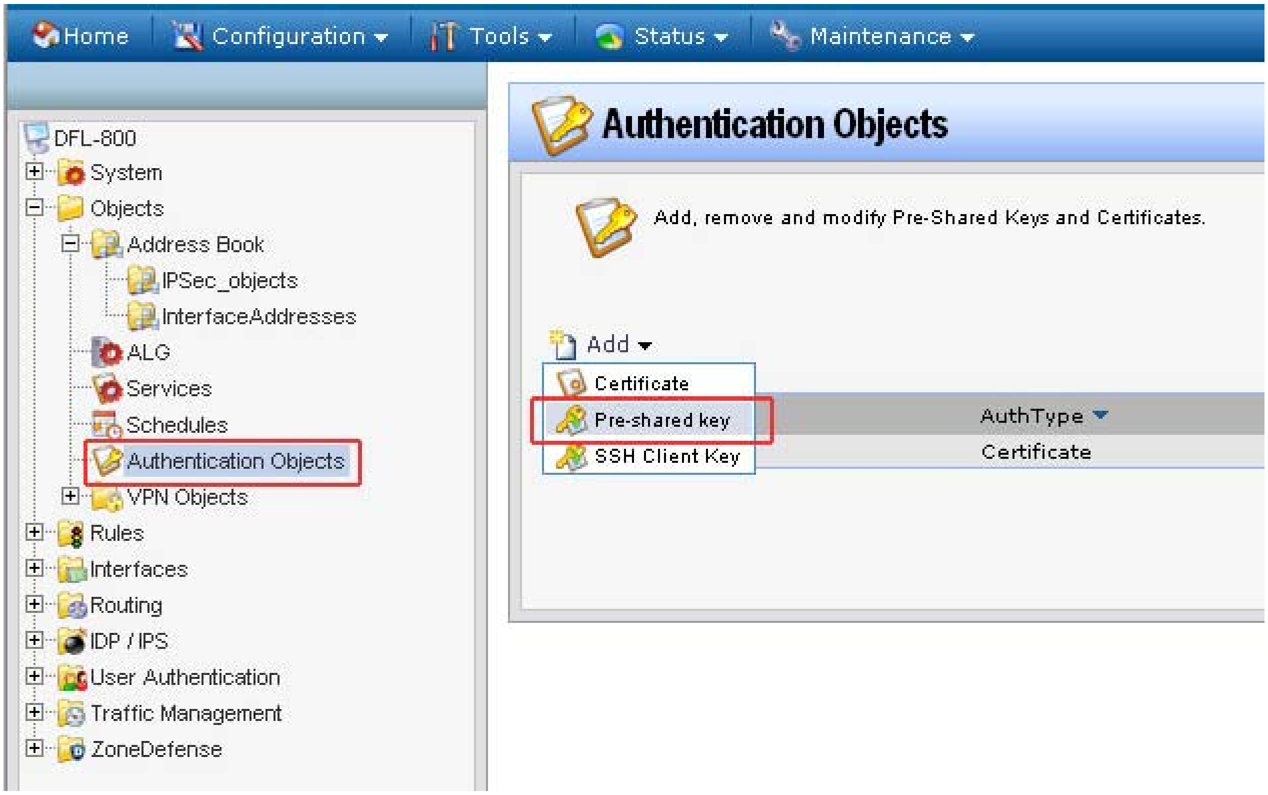
Name: remote_gateway

IP Address: 172.140.140.140 e.g: "172.16.50.8", "192.168.30.7, 192.168.30.11", "192.168.7.0/24" and "172.16.25.10-172.16.25.50"

Comments

Comments:

Step 7: Click on **Authentication Objects**, click on **Add** and select **Pre-shared key** from the dropdown menu to add a *Pre-shared key*.



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

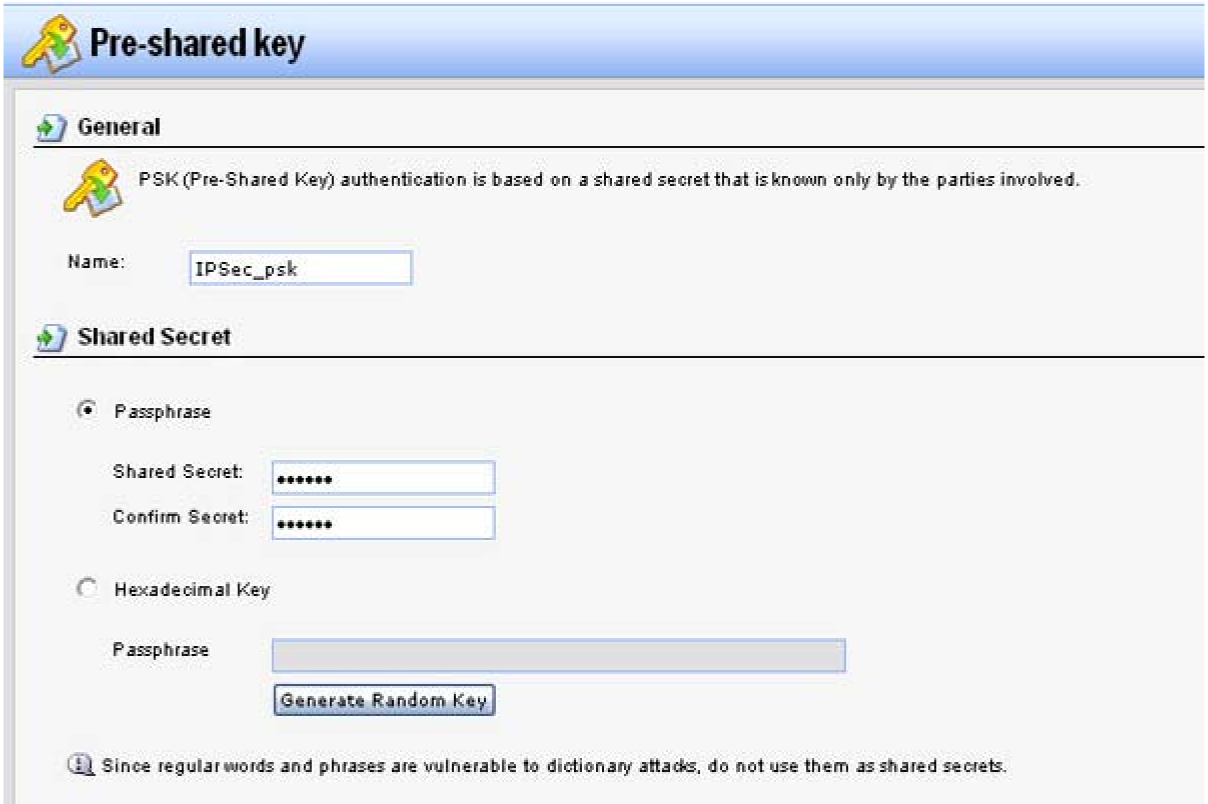
Step 8: Configure the *Pre-shared key* as followed:

- **Name:** enter a name as desired (IPSec_psk in this example)

Passphrase

- **Shared Secret:** enter a desired key
- **Confirm Secret:** re-enter the key

Click **OK**.



Pre-shared key

General

PSK (Pre-Shared Key) authentication is based on a shared secret that is known only by the parties involved.

Name: IPSec_psk

Shared Secret

● Passphrase

Shared Secret: ••••••

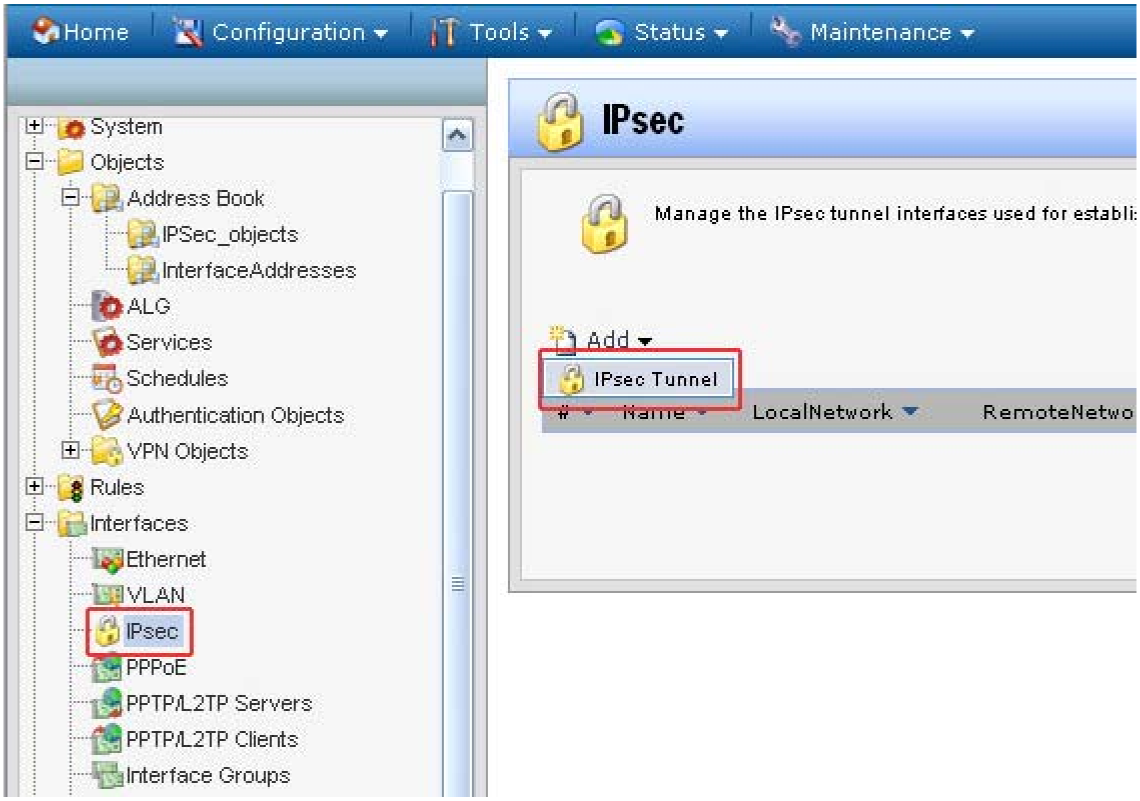
Confirm Secret: ••••••

○ Hexadecimal Key

Passphrase

Since regular words and phrases are vulnerable to dictionary attacks, do not use them as shared secrets.

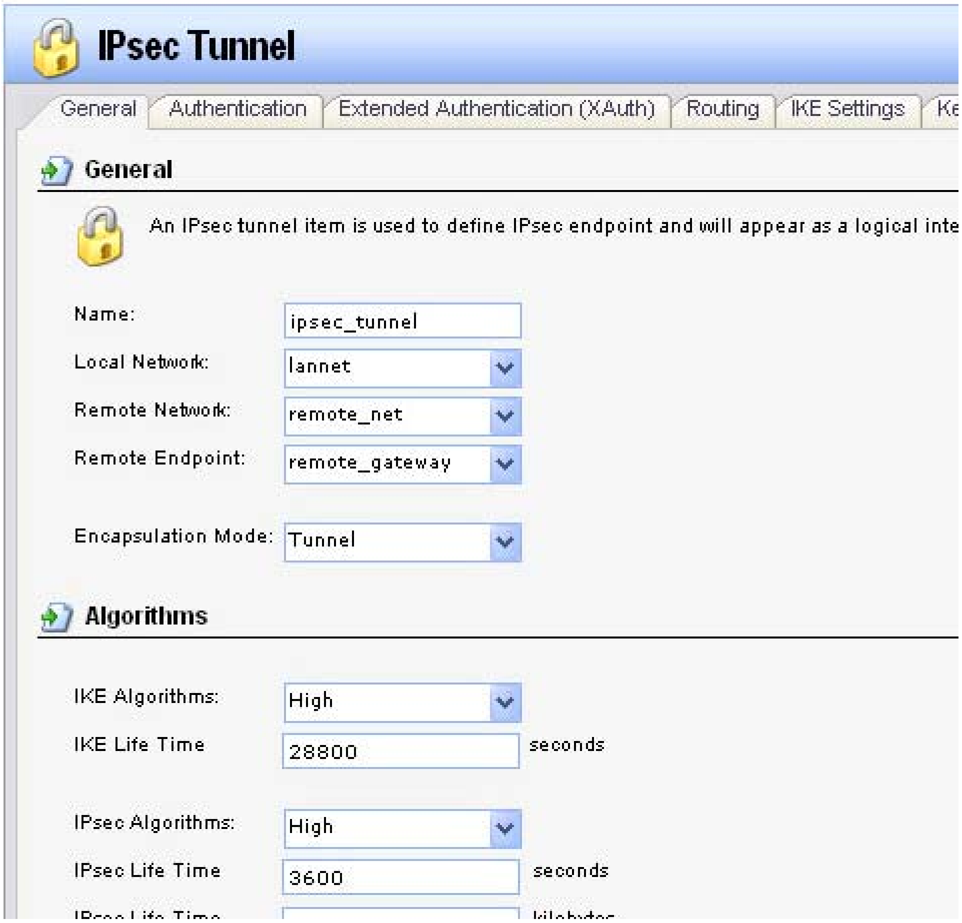
Step 9: Click the plus sign next to **Interfaces** and select **IPsec**. Click **Add** and select **IPsec Tunnel** from the dropdown menu.



Manage the IPsec tunnel interfaces used for establi

Step 10: Configure the *IPsec Tunnel* as followed:

- **Name:** enter a name as desired (*ipsec_tunnel* in this example)
- **Local Network:** lannet
- **Remote Network:** remote_net (created in *step 5*)
- **Remote Endpoint:** remote_gateway (created in *step 6*)
- **Encapsulation Mode:** Tunnel
- **IKE Algorithms:** High
- **IKE Life Time:** 28800 secs
- **IPsec Algorithms:** High
- **IPsec Life Time:** 3600 secs



IPsec Tunnel

General

An IPsec tunnel item is used to define IPsec endpoint and will appear as a logical inte

Name: ipsec_tunnel

Local Network: lannet

Remote Network: remote_net

Remote Endpoint: remote_gateway

Encapsulation Mode: Tunnel

Algorithms

IKE Algorithms: High

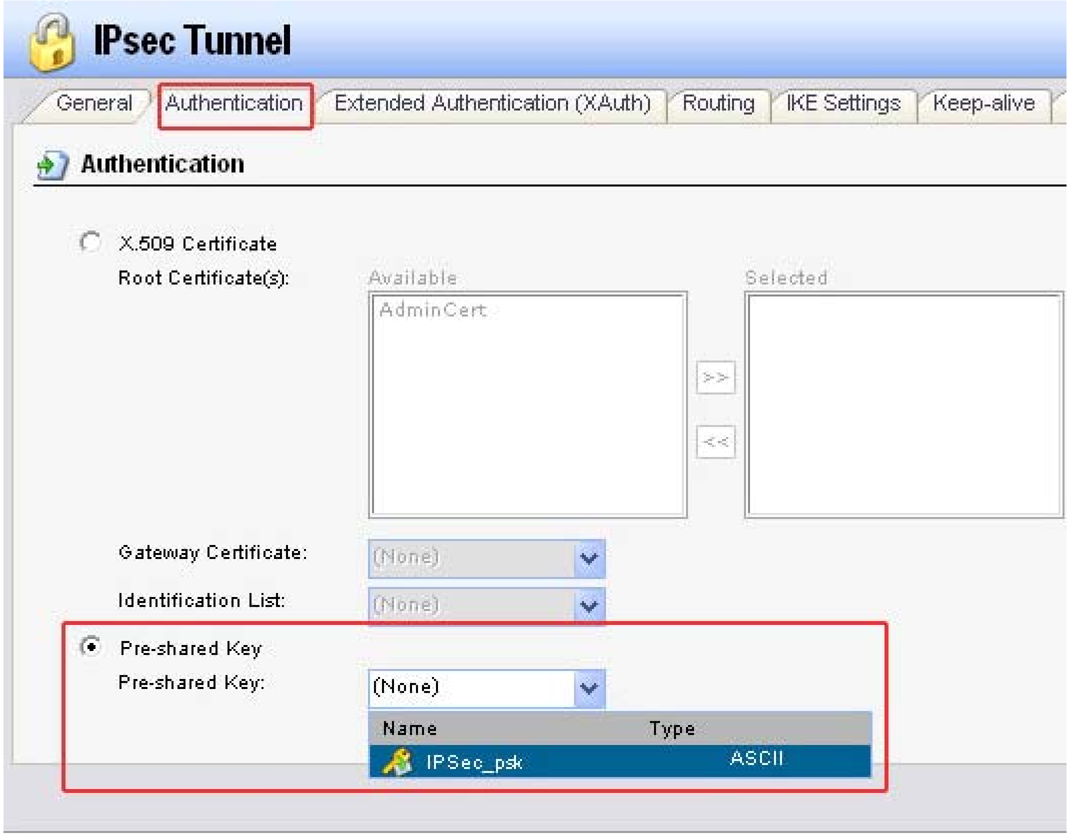
IKE Life Time 28800 seconds

IPsec Algorithms: High

IPsec Life Time 3600 seconds

IPsec Life Time kilobytes

Step 11: Click on the **Authentication** tab and select the *pre-shared key* (created in *step 8*) from the **Pre-Shared Key** dropdown menu.



Authentication

○ X.509 Certificate

Root Certificate(s): Available: AdminCert; Selected: (empty)

Gateway Certificate: (None)

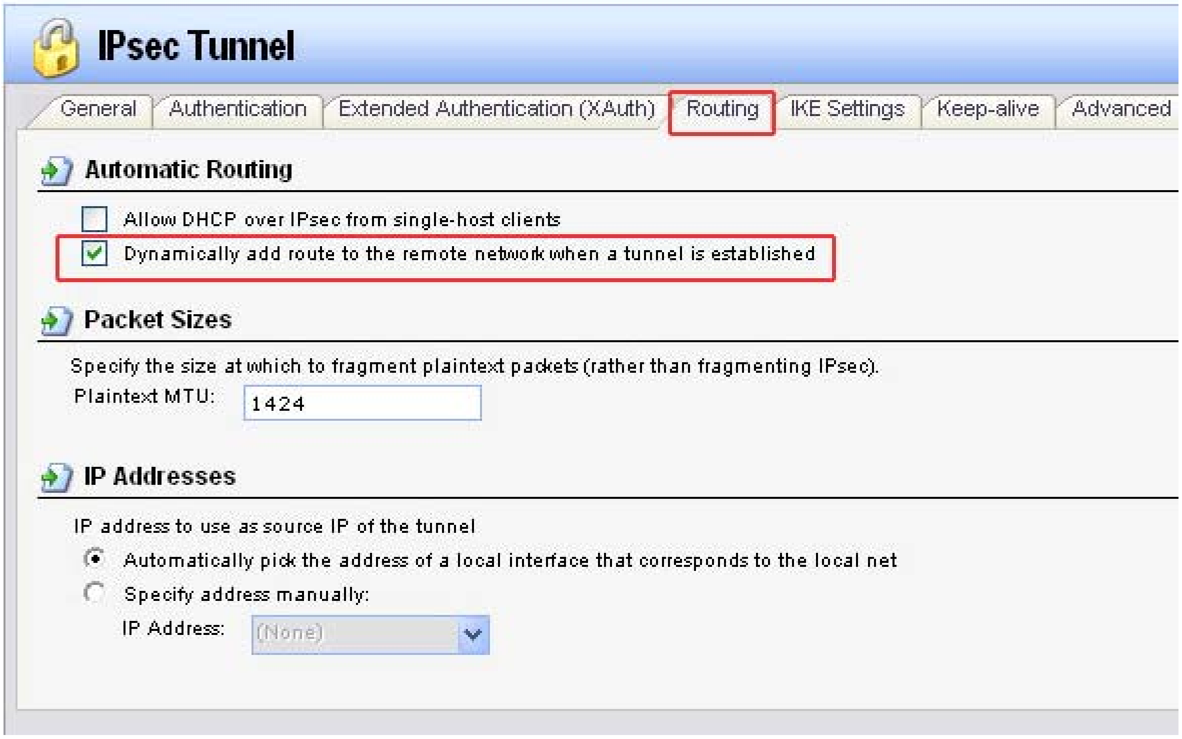
Identification List: (None)

● Pre-shared Key

Pre-shared Key: (None)

Name	Type
IPSec_psk	ASCII

Step 12: Click on the **Routing** tab and check the box labeled **Dynamically add route to the remote network when a tunnel is established**.



Automatic Routing

□ Allow DHCP over IPsec from single-host clients

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

Packet Sizes

Specify the size at which to fragment plaintext packets (rather than fragmenting IPsec).

Plaintext MTU: 1424

IP Addresses

IP address to use as source IP of the tunnel

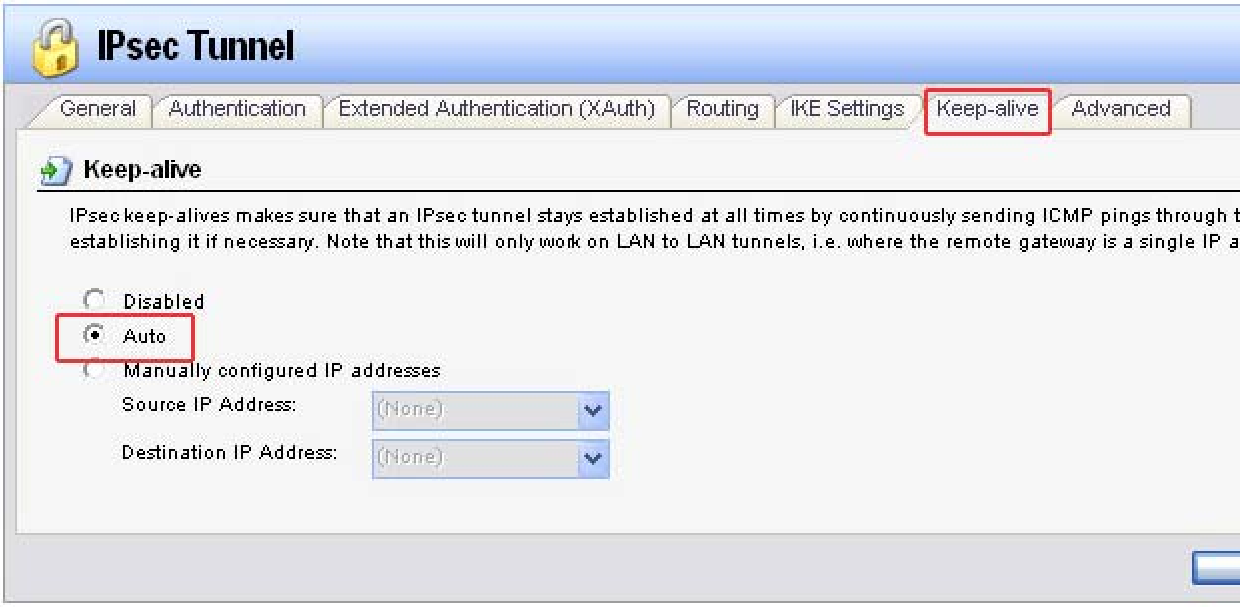
● Automatically pick the address of a local interface that corresponds to the local net

○ Specify address manually:

IP Address: (None)

Step 13: Click on the **Keep-alive** tab and select **Auto**.

Click **OK**.



Keep-alive

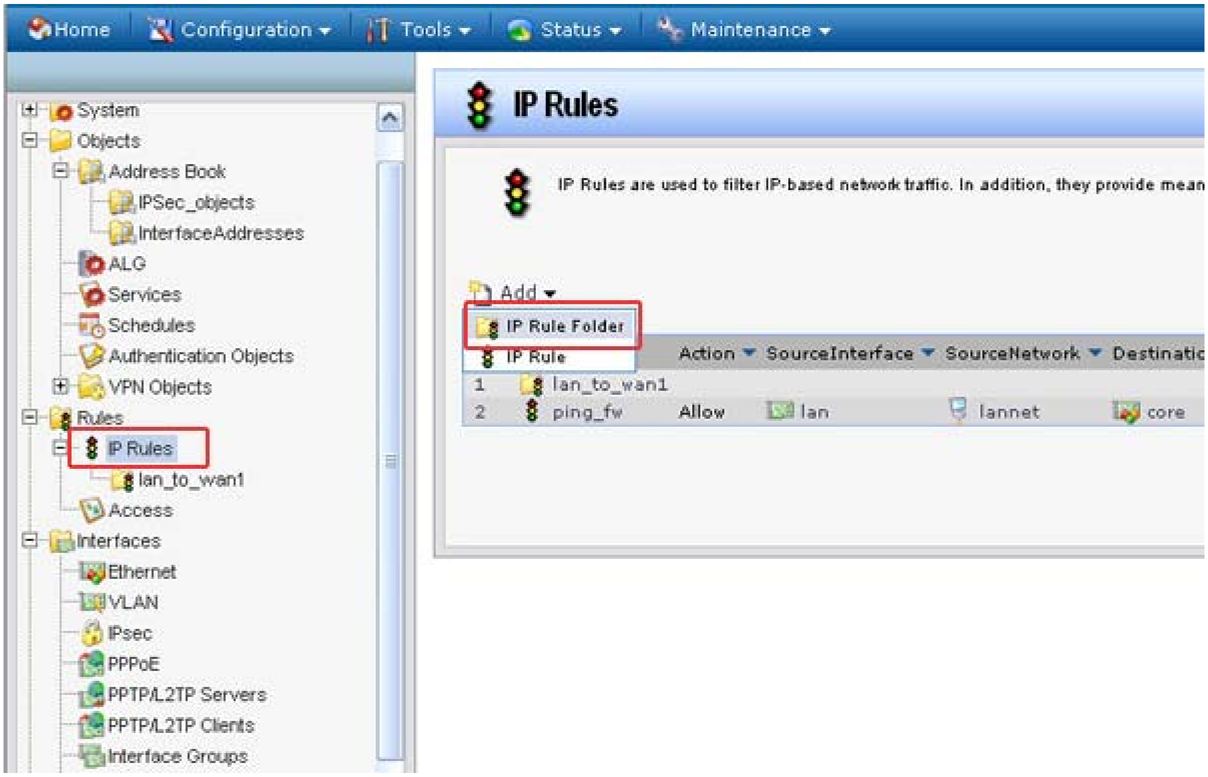
IPsec keep-alives makes sure that an IPsec tunnel stays established at all times by continuously sending ICMP pings through t
establishing it if necessary. Note that this will only work on LAN to LAN tunnels, i.e. where the remote gateway is a single IP a

○ Disabled
● Auto
○ Manually configured IP addresses

Source IP Address: (None)

Destination IP Address: (None)

Step 14: Click the plus sign next to **Rules** and select **IP Rules**. Click **Add** and select **IP Rule Folder**.

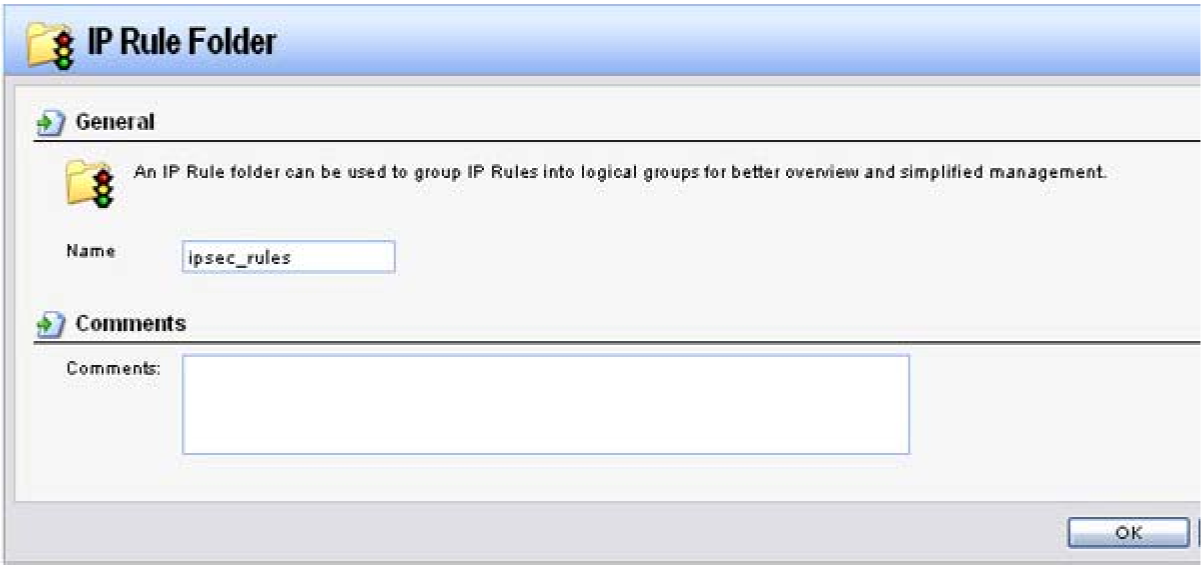


IP Rules

IP Rules are used to filter IP-based network traffic. In addition, they provide mean

		Action	SourceInterface	SourceNetwork	Destinatio
1	lan_to_wan1				
2	ping_fw	Allow	lan	lannet	core

Step 15: Enter a name for the folder and click **OK**.



IP Rule Folder

General

An IP Rule folder can be used to group IP Rules into logical groups for better overview and simplified management.

Name ipsec_rules

Comments

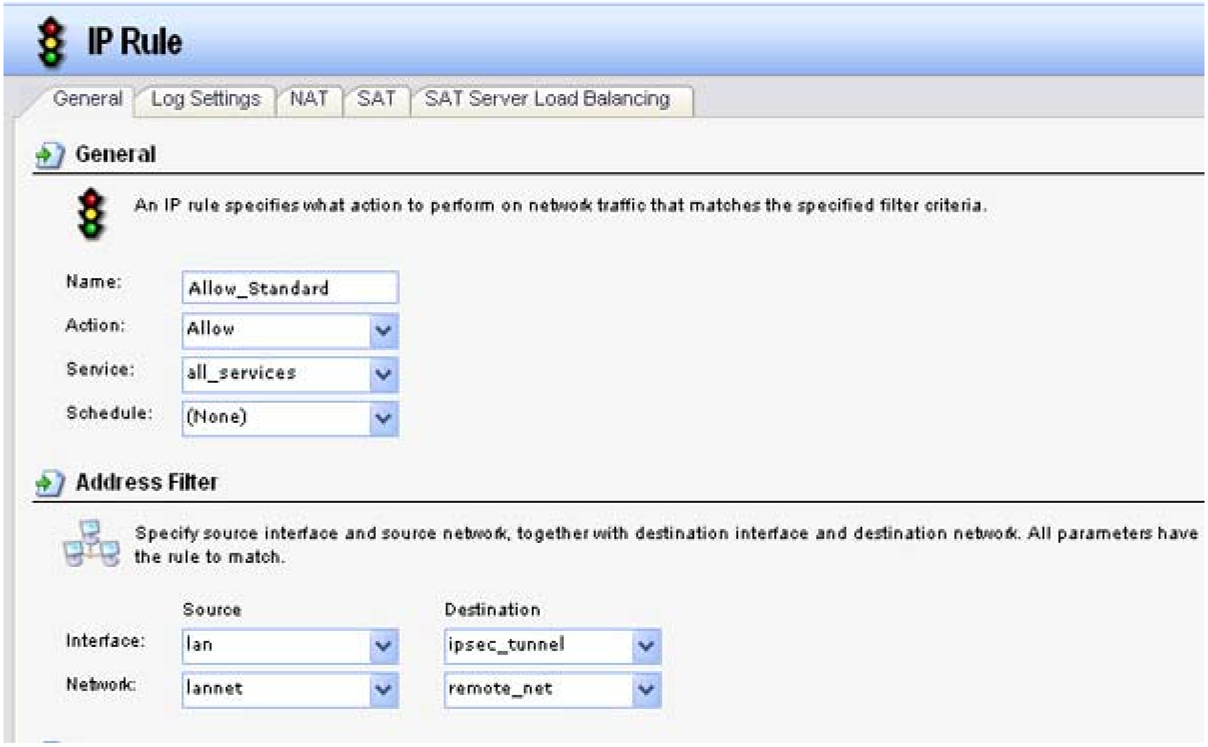
Comments:

Step 16: Click **Add** and select **IP Rule**. Configure the *IP Rule* as followed:

- **Name:** enter a name as desired
- **Action:** Allow
- **Service:** all_services

- **Schedule:** None
- **Source interface:** lan
- **Source network:** lannet
- **Destination interface:** ipsec_tunnel (created in *step 10*)
- **Destination network:** remote_net (created in *step 5*)

Click **OK**.



General

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

Name:	Allow_Standard
Action:	Allow
Service:	all_services
Schedule:	(None)

Address Filter

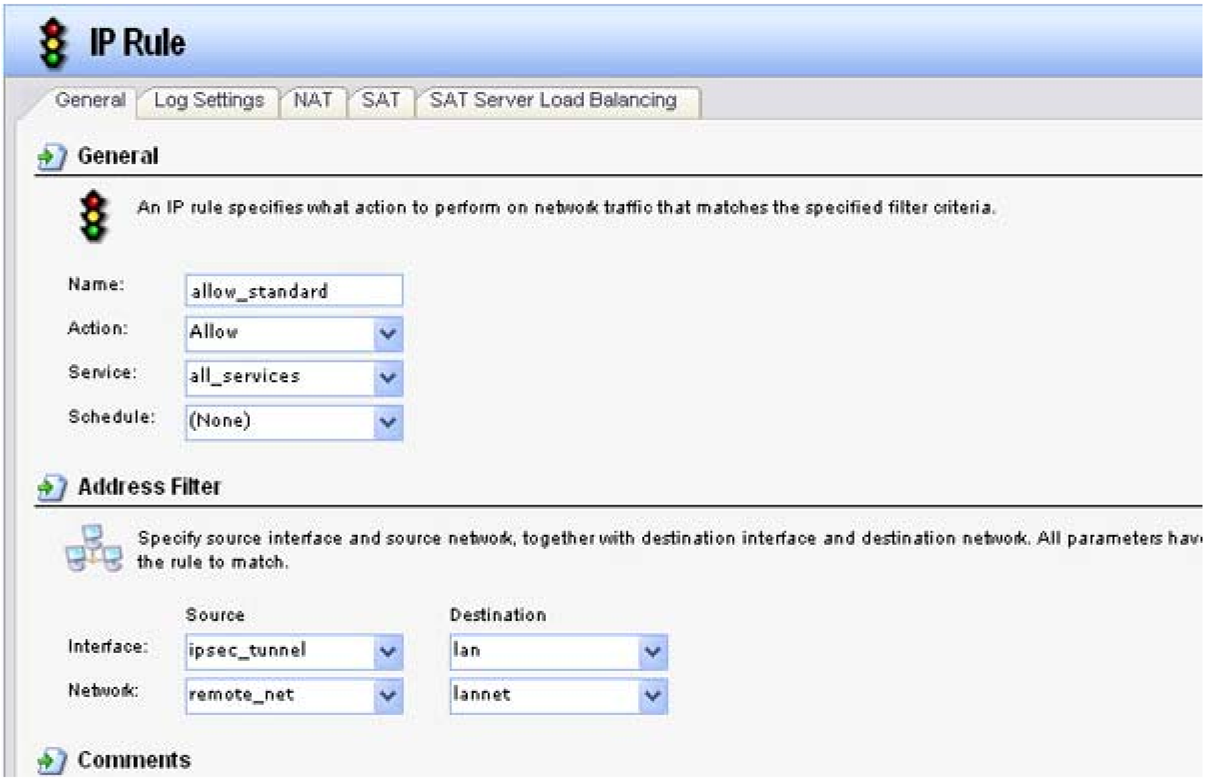
Specify source interface and source network, together with destination interface and destination network. All parameters have the rule to match.

	Source	Destination
Interface:	lan	ipsec_tunnel
Network:	lannet	remote_net

Step 17: Click **Add** and select **IP Rule**. Configure the *IP Rule* as followed:

- **Name:** enter a name as desired
- **Action:** Allow
- **Service:** all_services
- **Schedule:** None
- **Source interface:** ipsec_tunnel (created in *step 10*)
- **Source network:** remote_net (created in *step 5*)
- **Destination interface:** lan
- **Destination network:** lannet

Click **OK**.



IP Rule

General

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

Name: allow_standard
Action: Allow
Service: all_services
Schedule: (None)

Address Filter

Specify source interface and source network, together with destination interface and destination network. All parameters hav
the rule to match.

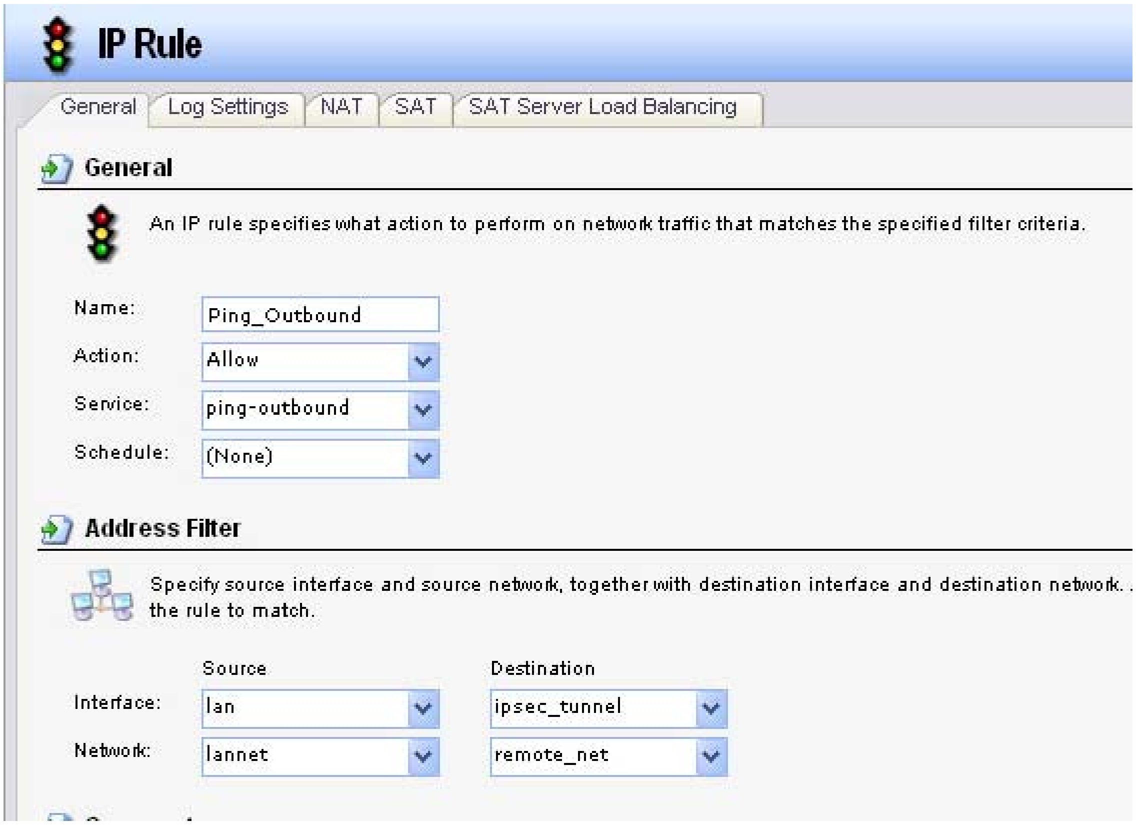
	Source	Destination
Interface:	ipsec_tunnel	lan
Network:	remote_net	lannet

Comments

Step 18: Click **Add** and select **IP Rule**. Configure the *IP Rule* as followed:

- **Name:** enter a name as desired
- **Action:** Allow
- **Service:** ping-outbound
- **Schedule:** None
- **Source interface:** lan
- **Source network:** lannet
- **Destination interface:** ipsec_tunnel (created in *step 10*)
- **Destination network:** remote_net (created in *step 5*)

Click **OK**.



General

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

Name: Ping_Outbound
Action: Allow
Service: ping-outbound
Schedule: (None)

Address Filter

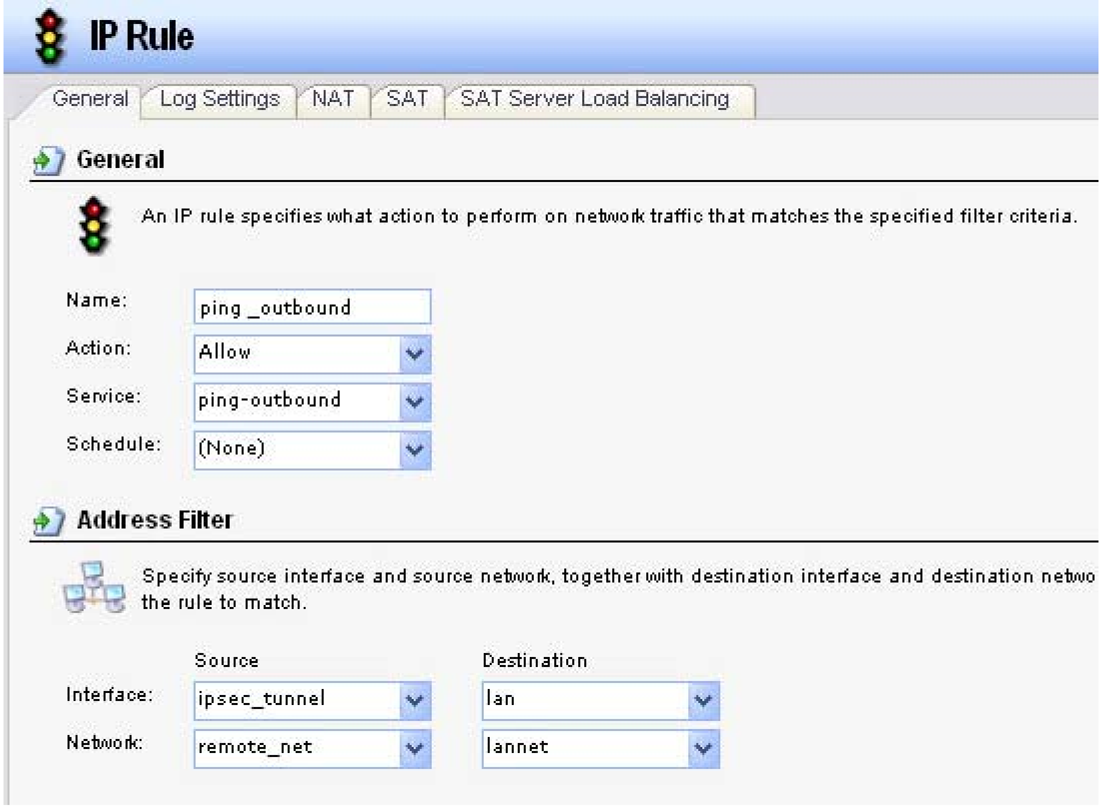
Specify source interface and source network, together with destination interface and destination network. . the rule to match.

	Source	Destination
Interface:	lan	ipsec_tunnel
Network:	lannet	remote_net

Step 19: Click **Add** and select **IP Rule**. Configure the *IP Rule* as followed:

- **Name:** enter a name as desired
- **Action:** Allow
- **Service:** ping-outbound
- **Schedule:** None
- **Source interface:** ipsec_tunnel (created in *step 10*)
- **Source network:** remote_net (created in *step 5*)
- **Destination interface:** lan
- **Destination network:** lannet

Click **OK**.



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 specified filter criteria.

Name: ping _outbound

Action: Allow

Service: ping-outbound

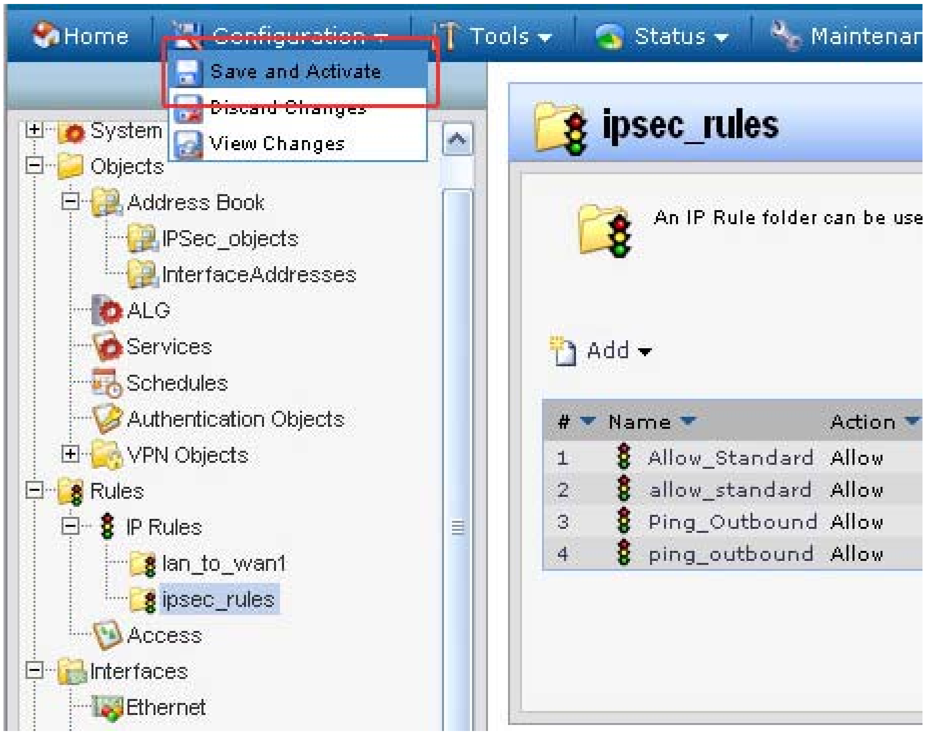
Schedule: (None)

Address Filter

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

	Source	Destination
Interface:	ipsec_tunnel	lan
Network:	remote_net	lannet

Step 20: Click **Configuration** and select **Save and Activate**. Click **OK** to activate changes.



ipsec_rules

An IP Rule folder can be use

#	Name	Action
1	Allow_Standard	Allow
2	allow_standard	Allow
3	Ping_Outbound	Allow
4	ping_outbound	Allow