

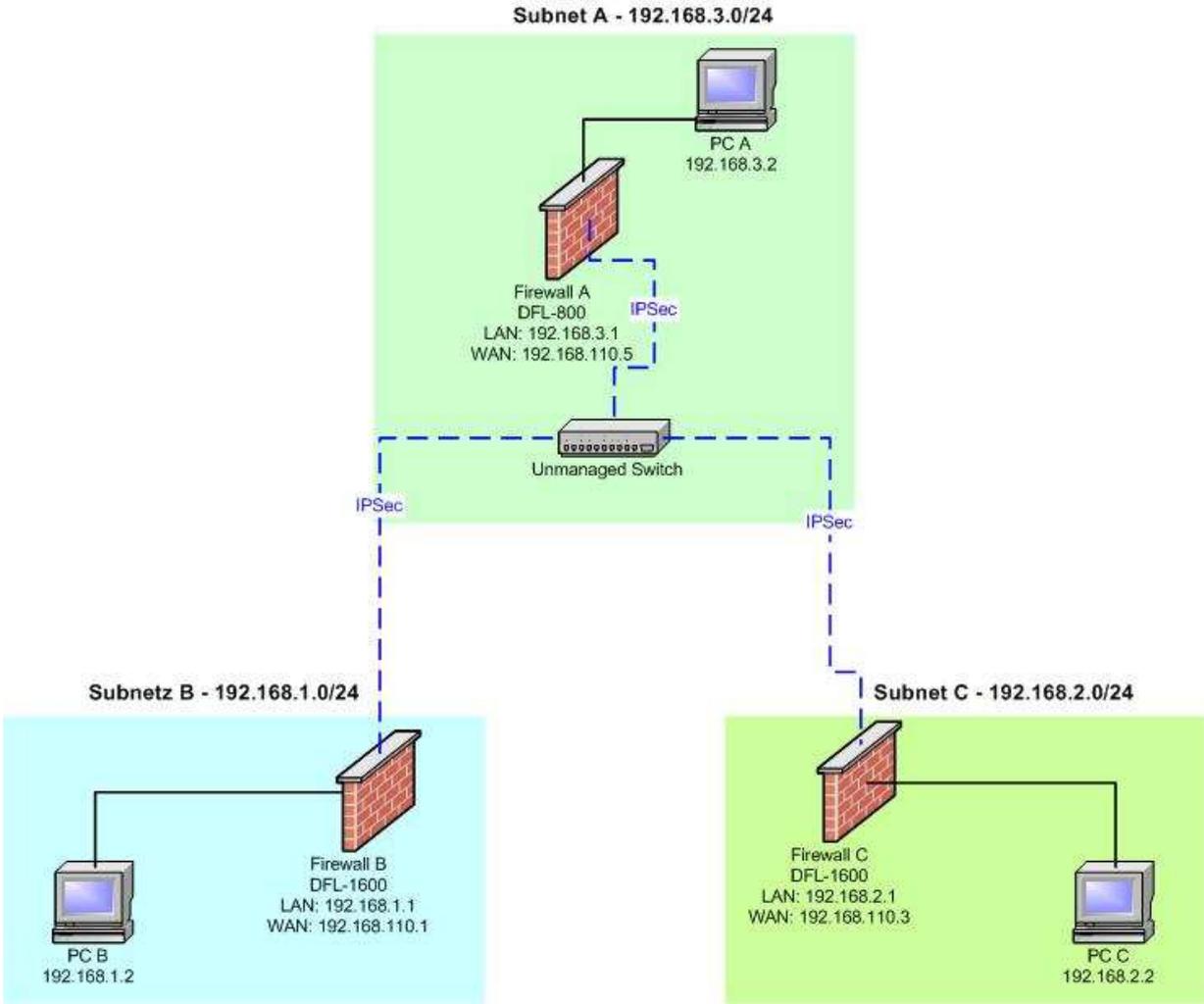
Einrichtung eines IPSec-Konzentrator *(Hub and Spoke)*

auf der DFL-800, DFL-1600 und DFL-2500

Um diese Anleitung nutzen zu können werden folgende Kenntnisse vorausgesetzt:
IPSec, Routing, TCP, UDP, ICMP, Paketfilterung.

Viele dieser Informationen finden Sie beispielsweise unter: <http://de.wikipedia.org/wiki/>

Testumgebung:



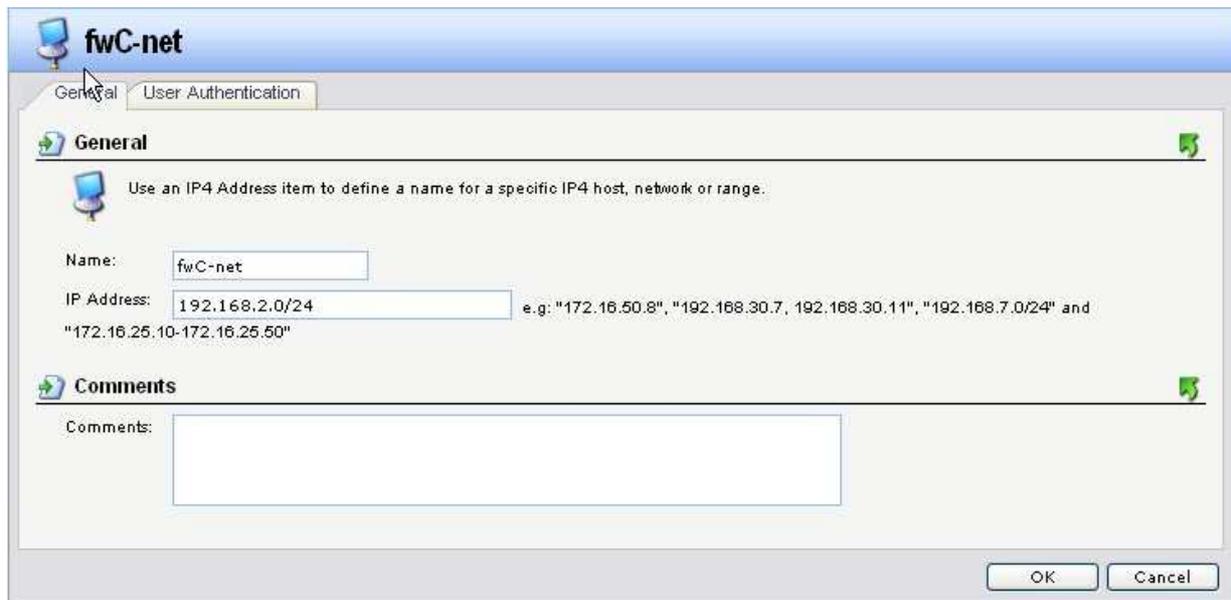
Konfiguration auf Firewall B:

Zuerst wurden die folgenden Objekte auf Firewall B angelegt: ¹

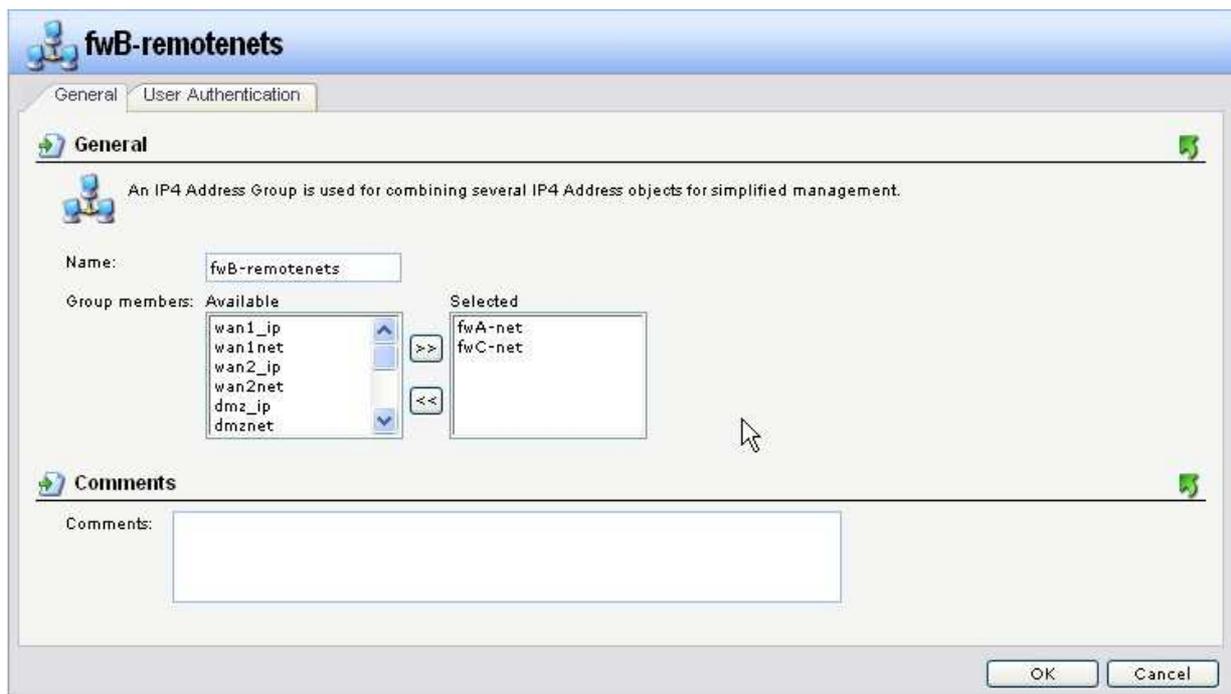
The screenshot shows the configuration window for 'fwA-remotegw'. It has two tabs: 'General' (selected) and 'User Authentication'. The 'General' tab contains a 'General' section with a help icon and a description: 'Use an IP4 Address item to define a name for a specific IP4 host, network or range.' Below this, there are two input fields: 'Name:' with the value 'fwA-remotegw' and 'IP Address:' with the value '192.168.110.5'. To the right of the IP Address field, there is a list of examples: '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"'. Below the IP Address field is a 'Comments:' section with an empty text area. At the bottom right, there are 'OK' and 'Cancel' buttons.

The screenshot shows the configuration window for 'fwA-net'. It has two tabs: 'General' (selected) and 'User Authentication'. The 'General' tab contains a 'General' section with a help icon and a description: 'Use an IP4 Address item to define a name for a specific IP4 host, network or range.' Below this, there are two input fields: 'Name:' with the value 'fwA-net' and 'IP Address:' with the value '192.168.3.0/24'. To the right of the IP Address field, there is a list of examples: '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"'. Below the IP Address field is a 'Comments:' section with an empty text area. At the bottom right, there are 'OK' and 'Cancel' buttons.

¹ Diese Einstellung finden Sie unter folgendem Menüpunkt: / Objects / Address Book / Add / IP4 Host/Network /

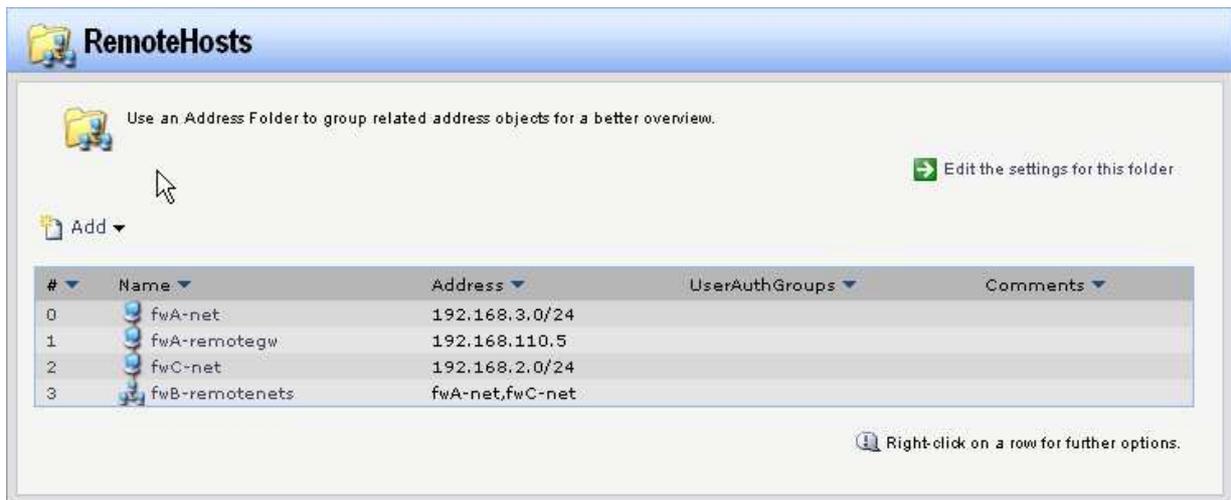


Nun muss weiterhin eine neue IP-Gruppe angelegt werden:²

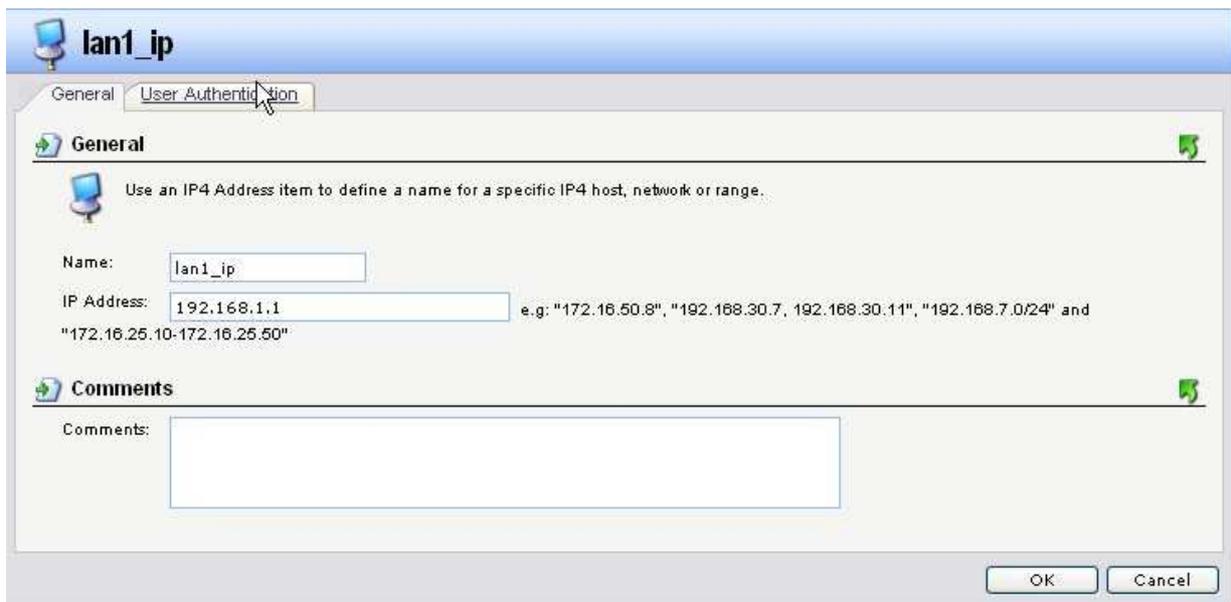


² Diese Einstellung finden Sie unter folgendem Menüpunkt: / Objects / Address Book / Add / IP4 Address Group /

In der Übersicht sieht dies wie folgt aus:



Ändern Sie nun gegebenenfalls die bestehenden Objekte für LAN und WAN Interface:³



³ Diese Einstellung finden Sie unter folgendem Menüpunkt: / Objects / Address Book /

lan1net

General | User Authentication

General

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

Name:

IP Address: 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:

OK Cancel

wan1_ip

General | User Authentication

General

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

Name:

IP Address: 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:

OK Cancel

wan1net

General User Authentication

General

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

Name:

IP Address: 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:

OK Cancel

Legen Sie nun den Pre-Shared Key an:⁴

Pre-Shared Keys

Add, remove and modify Pre-Shared Keys, which are used for IPSec authentication purposes.

Add ▾

#	Name	Type	Comments
0	 fwABC-psk	ASCII	

 Right-click on a row for further options.

⁴ Diese Einstellung finden Sie unter folgendem Menüpunkt: / Objects / VPN-Objects / Pre-Shared-Keys /

Legen Sie nun einen IPSec-Tunnel an: ⁵

The screenshot shows the configuration window for an IPsec tunnel named 'ipsectunnelBA'. The 'General' tab is active. The configuration includes:

- Name:** ipsectunnelBA
- Local Network:** lan1net
- Remote Network:** fwB-remotenets
- Remote Endpoint:** fwA-remotegw
- Encapsulation Mode:** Tunnel

Under the 'Algorithms' section:

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

The screenshot shows the 'Authentication' tab of the 'ipsectunnelBA' configuration window. The 'Pre-Shared Key' option is selected.

- X.509 Certificate:** Unselected. Root Certificate(s): AdminCert (Available).
- Gateway Certificate:** (None)
- Identification List:** (None)
- Pre-Shared Key:** Selected. Pre-Shared Key: fwABC-psk

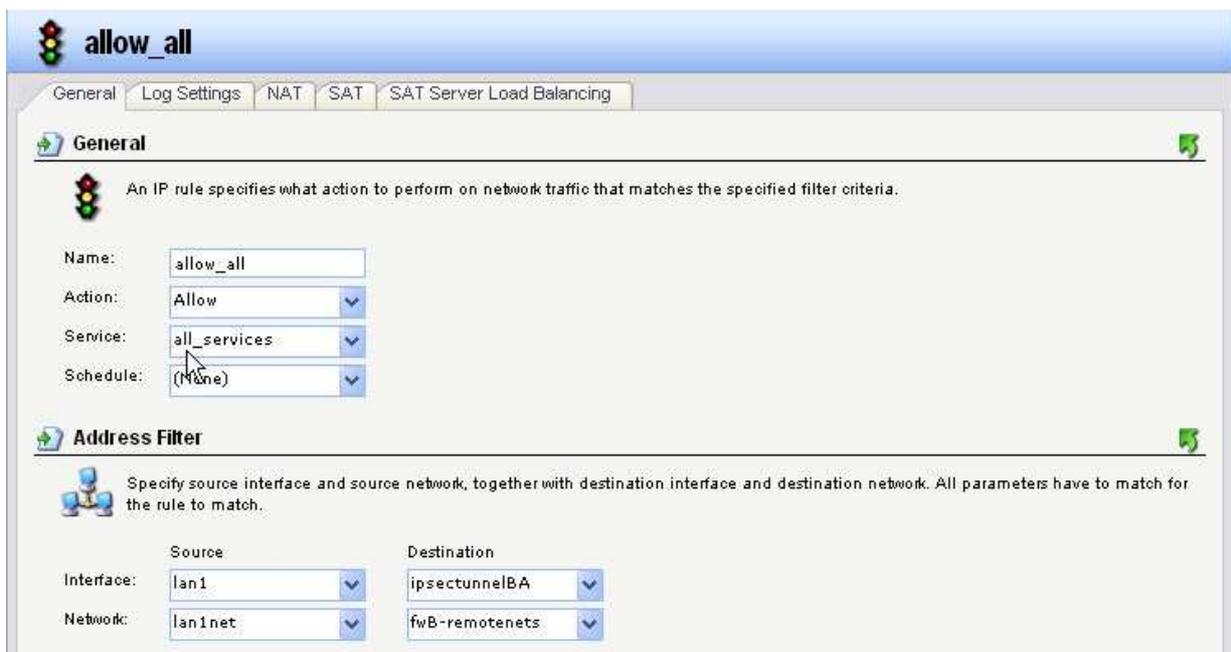
Buttons: OK, Cancel

⁵ Diese Einstellung finden Sie unter folgendem Menüpunkt: / Interfaces / IPSec Tunnels /

In der Übersicht sieht dies wie folgt aus:



Richten Sie nun die Access-Rules ein:⁶



⁶ Diese Einstellung finden Sie unter folgendem Menüpunkt: / Rules / IP Rules /

allow_all

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:

Action:

Service:

Schedule:

Address Filter

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

Source Destination

Interface:

Network:

In der Übersicht sieht dies wie folgt aus:

lan_to_fwA

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

[Edit the settings for this folder](#)

[Add](#)

#	Name	Action	Source Interface	Source Network	Destination Interface	Destination Network	Service
0	allow_all	Allow	lan1	lan1net	ipsectunnelBA	fwB-remotenets	all_services
1	allow_all	Allow	ipsectunnelBA	fwB-remotenets	lan1	lan1net	all_services

[Right-click on a row for further options.](#)

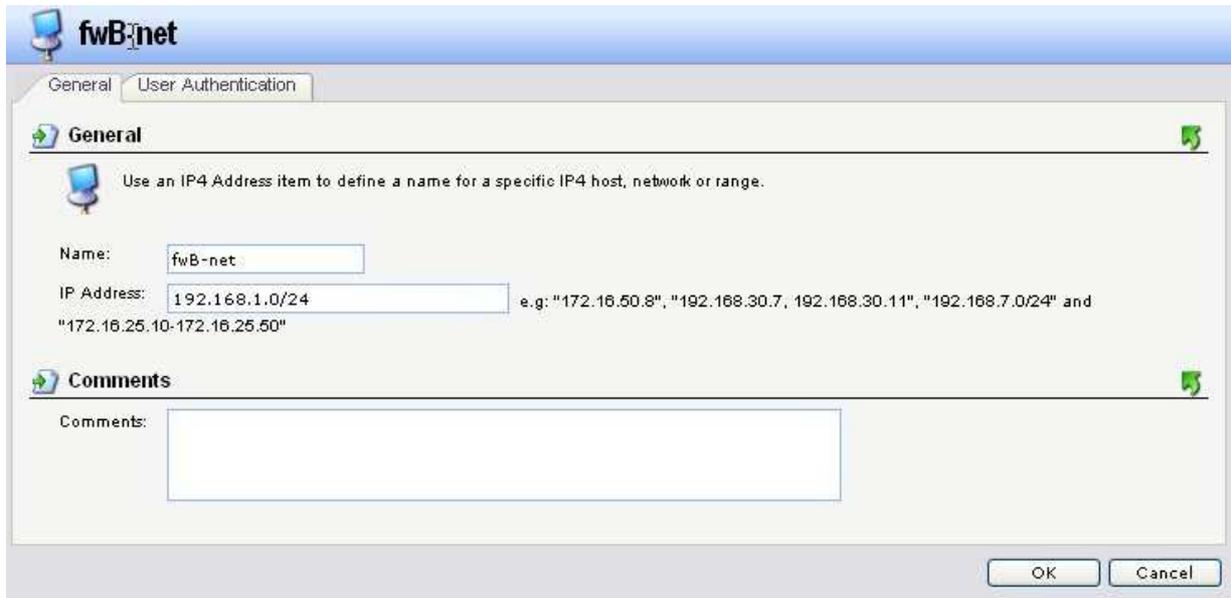
Konfiguration auf Firewall C:

Zuerst wurden die folgenden Objekte auf Firewall C angelegt: ⁷:

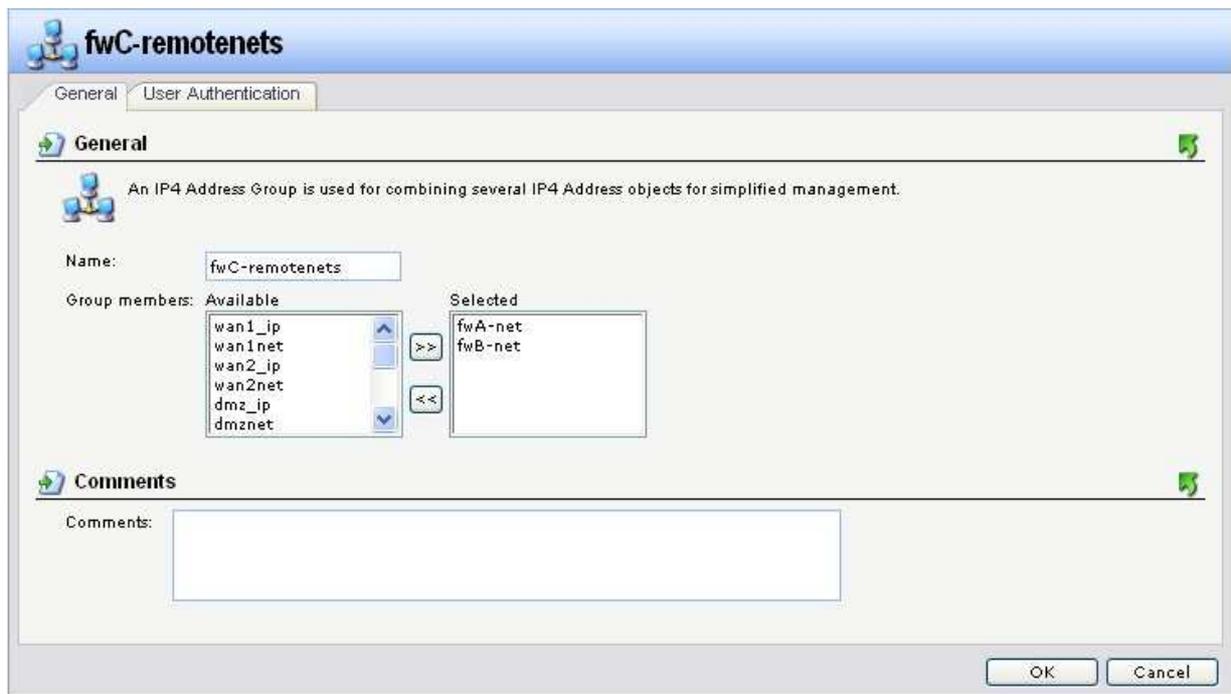
The screenshot shows the configuration window for 'fwA-remotegw'. The 'General' tab is active. The 'Name' field contains 'fwA-remotegw'. The 'IP Address' field contains '192.168.110.5'. Below the IP address field, there is a list of examples: 'e.g. "172.16.50.8", "192.168.30.7", "192.168.30.11", "192.168.7.0/24" and "172.16.25.10-172.16.25.50"'. The 'Comments' field is empty. At the bottom right, there are 'OK' and 'Cancel' buttons.

The screenshot shows the configuration window for 'fwA-net'. The 'General' tab is active. The 'Name' field contains 'fwA-net'. The 'IP Address' field contains '192.168.3.0/24'. Below the IP address field, there is a list of examples: '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"'. The 'Comments' field is empty. At the bottom right, there are 'OK' and 'Cancel' buttons.

⁷ Diese Einstellung finden Sie unter folgendem Menüpunkt: Objects / Address Book / Add / IP4 Host/Network /

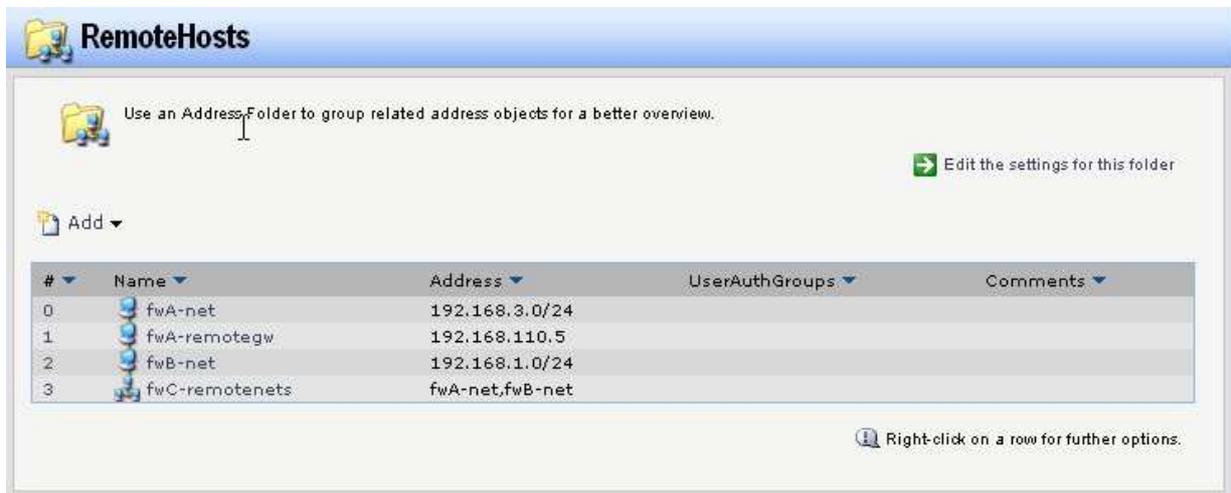


Nun muss weiterhin eine neue IP-Gruppe angelegt werden:⁸

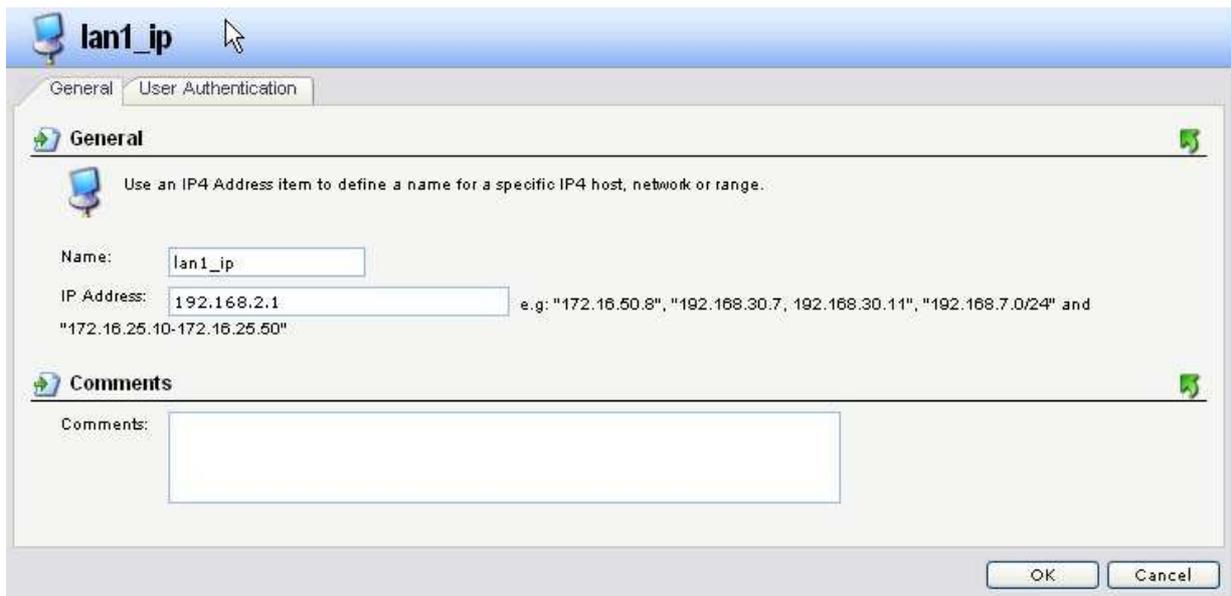


⁸ Diese Einstellung finden Sie unter folgendem Menüpunkt: / Objects / Address Book / Add / IP4 Address Group /

In der Übersicht sieht dies wie folgt aus:



Ändern Sie nun gegebenenfalls die bestehenden Objekte für LAN und WAN Interface:⁹



⁹ Diese Einstellung finden Sie unter folgendem Menüpunkt: / Objects / Address Book /

lan1net

General | User Authentication

General

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

Name:

IP Address: 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:

OK Cancel

wan1_ip

General | User Authentication

General

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

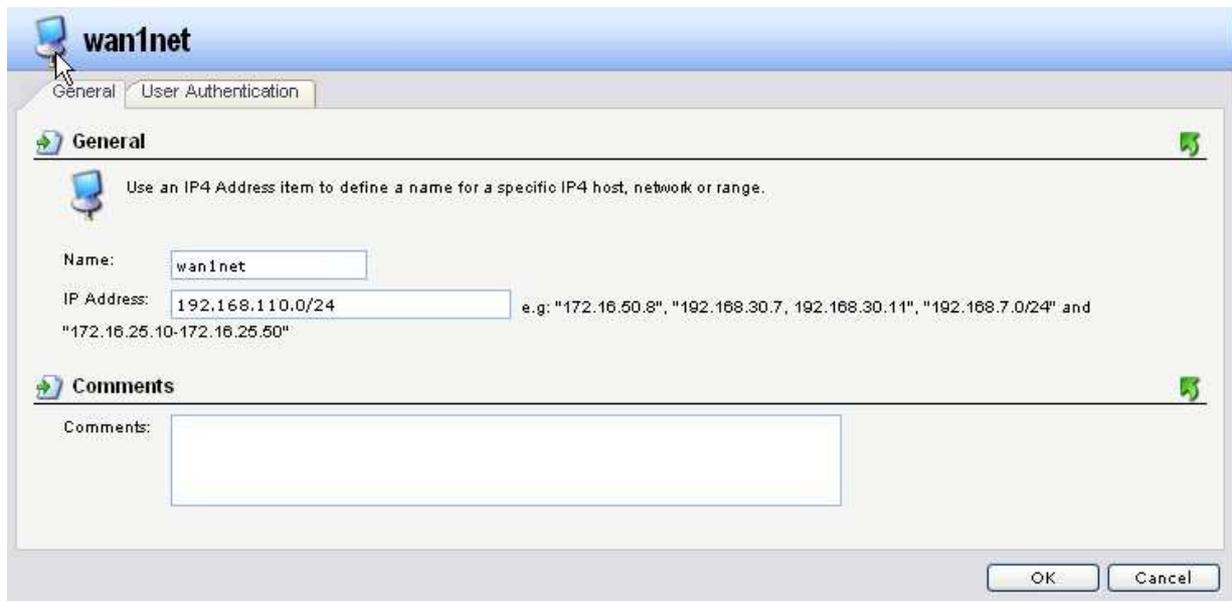
Name:

IP Address: 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"

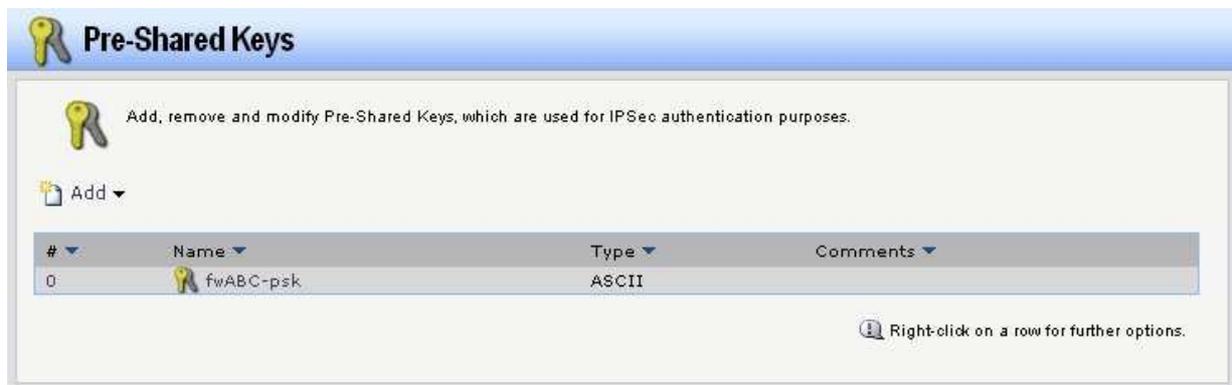
Comments

Comments:

OK Cancel



Legen Sie nun den Pre-Shared Key an: ¹⁰



¹⁰ Diese Einstellung finden Sie unter folgendem Menüpunkt: / Objects / VPN-Objects / Pre-Shared-Keys /

Legen Sie nun einen IPSec-Tunnel an: ¹¹

The screenshot shows the 'ipsectunnelCA' configuration window with the 'General' tab selected. The window title is 'ipsectunnelCA'. The tabs are: General, Authentication, Extended Authentication (XAuth), Routing, IKE Settings, Keep-alive, and Advanced. The 'General' section contains the following fields:

- Name: ipsectunnelCA
- Local Network: lan1net
- Remote Network: fwC-remotenets
- Remote Endpoint: fwA-remotegw
- Encapsulation Mode: Tunnel

The 'Algorithms' section contains the following fields:

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

The screenshot shows the 'ipsectunnelCA' configuration window with the 'Authentication' tab selected. The window title is 'ipsectunnelCA'. The tabs are: General, Authentication, Extended Authentication (XAuth), Routing, IKE Settings, Keep-alive, and Advanced. The 'Authentication' section contains the following fields:

- X.509 Certificate
- Root Certificate(s): Available (AdminCert) and Selected (empty)
- Gateway Certificate: (None)
- Identification List: (None)
- Pre-Shared Key
- Pre-Shared Key: fwABC-psk

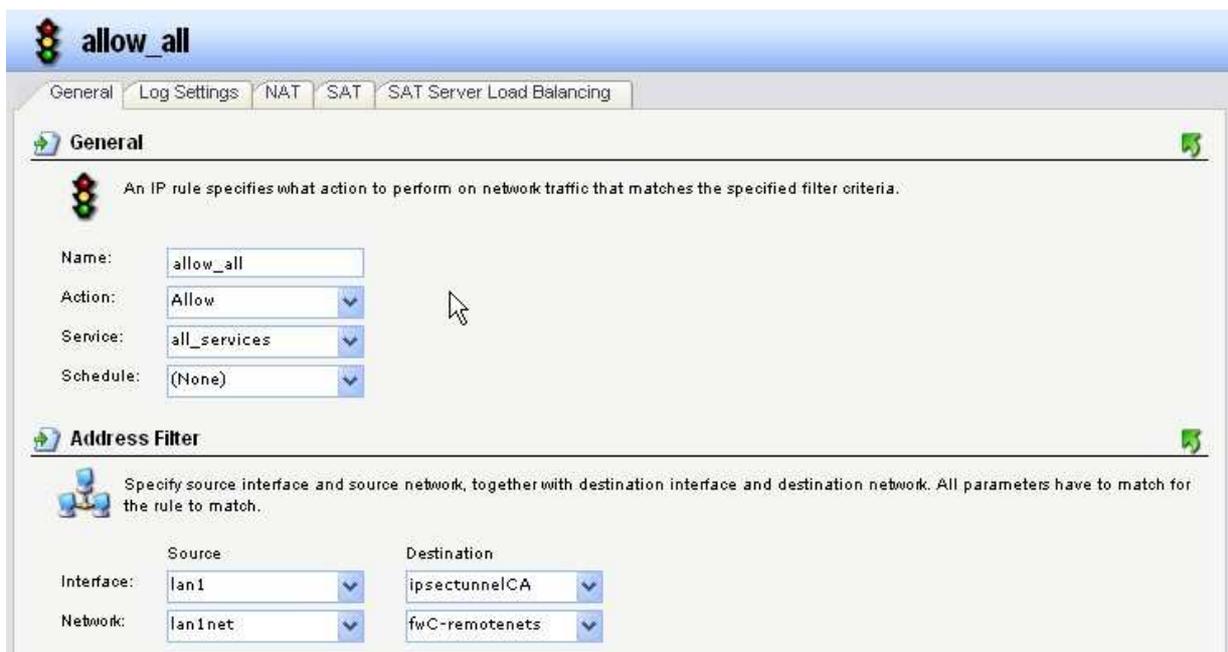
At the bottom right, there are 'OK' and 'Cancel' buttons.

¹¹ Diese Einstellung finden Sie unter folgendem Menüpunkt: / Interfaces / IPSec Tunnels /

In der Übersicht sieht dies wie folgt aus:



Richten Sie nun die Access-Rules ein: ¹²



¹² Diese Einstellung finden Sie unter folgendem Menüpunkt: / Rules / IP Rules /

allow_all

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:

Action:

Service:

Schedule:

Address Filter

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

Interface: Source Destination

Network:

In der Übersicht sieht dies wie folgt aus:

lan_to_fwA

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

[Edit the settings for this folder](#)

Add

#	Name	Action	Source Interface	Source Network	Destination Interface	Destination Network	Service
0	allow_all	Allow	lan1	lan1net	ipsectunnelCA	fwC-remotenets	all_services
1	allow_all	Allow	ipsectunnelCA	fwC-remotenets	lan1	lan1net	all_services

[Right-click on a row for further options.](#)

Konfiguration auf Firewall A:

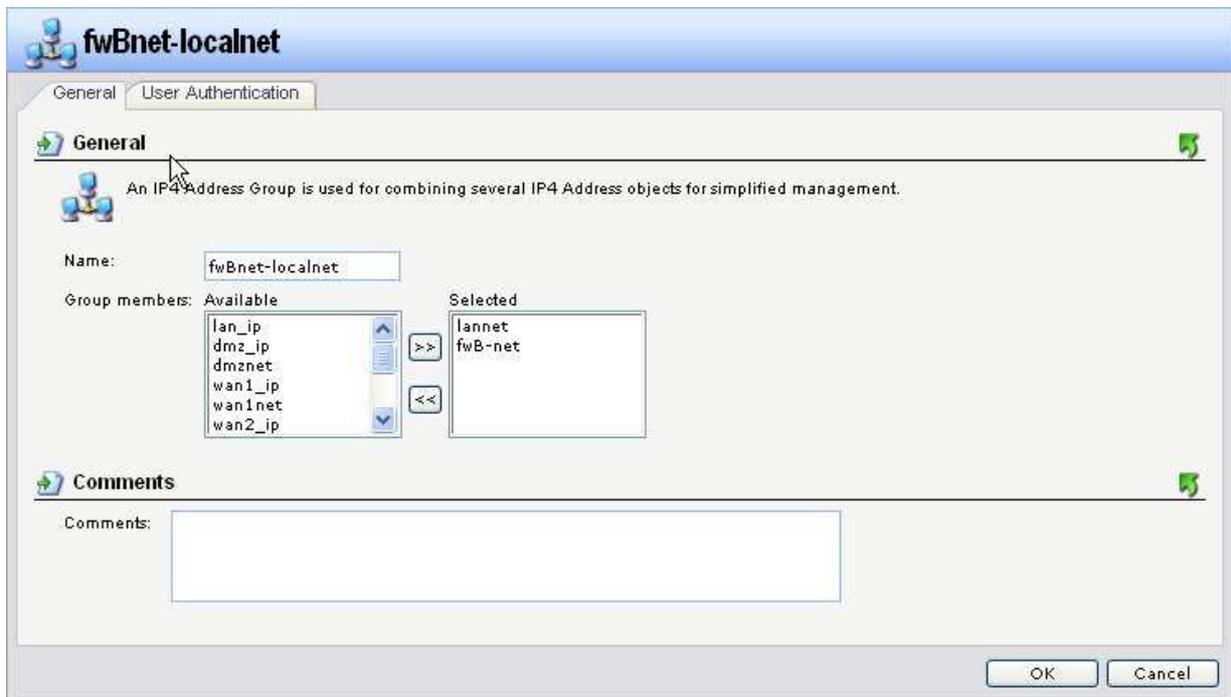
Zuerst wurden die folgenden Objekte auf Firewall A angelegt: ¹³

The screenshot shows the configuration window for 'fwB-remotegw'. The window has a blue header with the title 'fwB-remotegw'. Below the header, there are two tabs: 'General' (selected) and 'User Authentication'. The 'General' tab contains a section titled 'General' with a green plus icon and a refresh icon. Below this, there is a text box for 'Name' containing 'fwB-remotegw'. Underneath, there is a text box for 'IP Address' containing '192.168.110.1'. To the right of the IP address field, there is a small text box with the example text: '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"'. Below the IP address field, there is a larger text box for 'Comments'. At the bottom right of the window, there are two buttons: 'OK' and 'Cancel'.

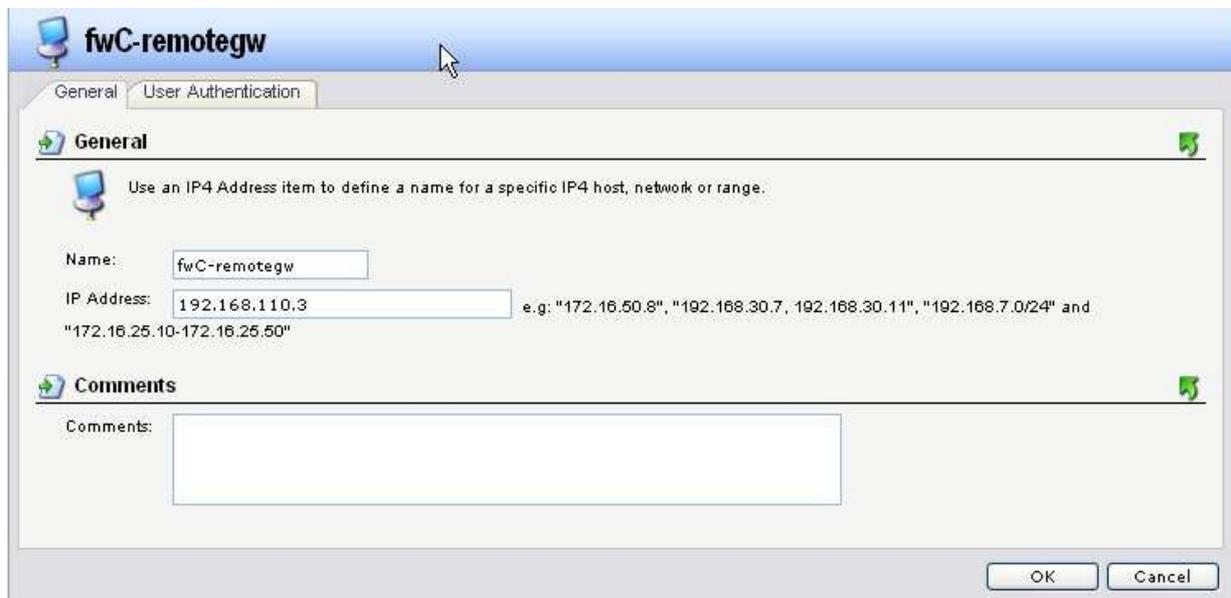
The screenshot shows the configuration window for 'fwB-net'. The window has a blue header with the title 'fwB-net'. Below the header, there are two tabs: 'General' (selected) and 'User Authentication'. The 'General' tab contains a section titled 'General' with a green plus icon and a refresh icon. Below this, there is a text box for 'Name' containing 'fwB-net'. Underneath, there is a text box for 'IP Address' containing '192.168.1.0/24'. To the right of the IP address field, there is a small text box with the example text: '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"'. Below the IP address field, there is a larger text box for 'Comments'. At the bottom right of the window, there are two buttons: 'OK' and 'Cancel'.

¹³ Diese Einstellung finden Sie unter folgendem Menüpunkt: / Objects / Address Book / Add / IP4 Host/Network /

Nun muss weiterhin eine neue IP-Gruppe angelegt werden: ¹⁴

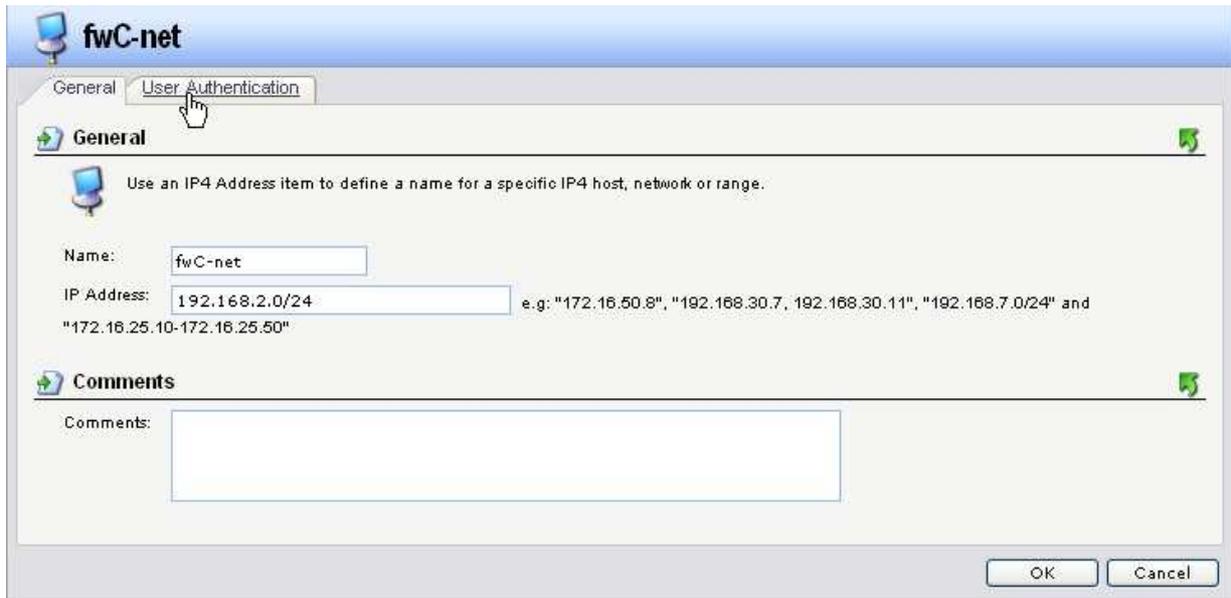


Legen Sie nun weitere Objekte an: ¹⁵

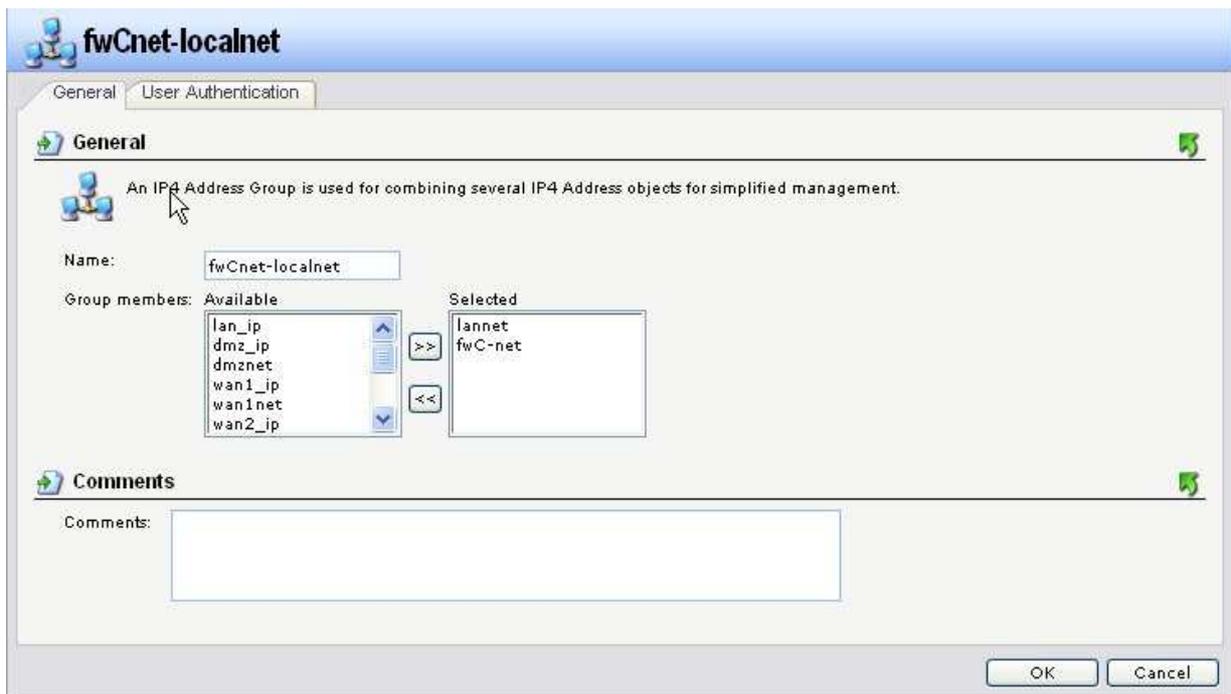


¹⁴ Diese Einstellung finden Sie unter folgendem Menüpunkt: / Objects / Address Book / Add / IP4 Address Group /

¹⁵ Diese Einstellung finden Sie unter folgendem Menüpunkt: Objects / Address Book / Add / IP4 Host/Network /



Nun muss weiterhin eine neue IP-Gruppe angelegt werden: ¹⁶

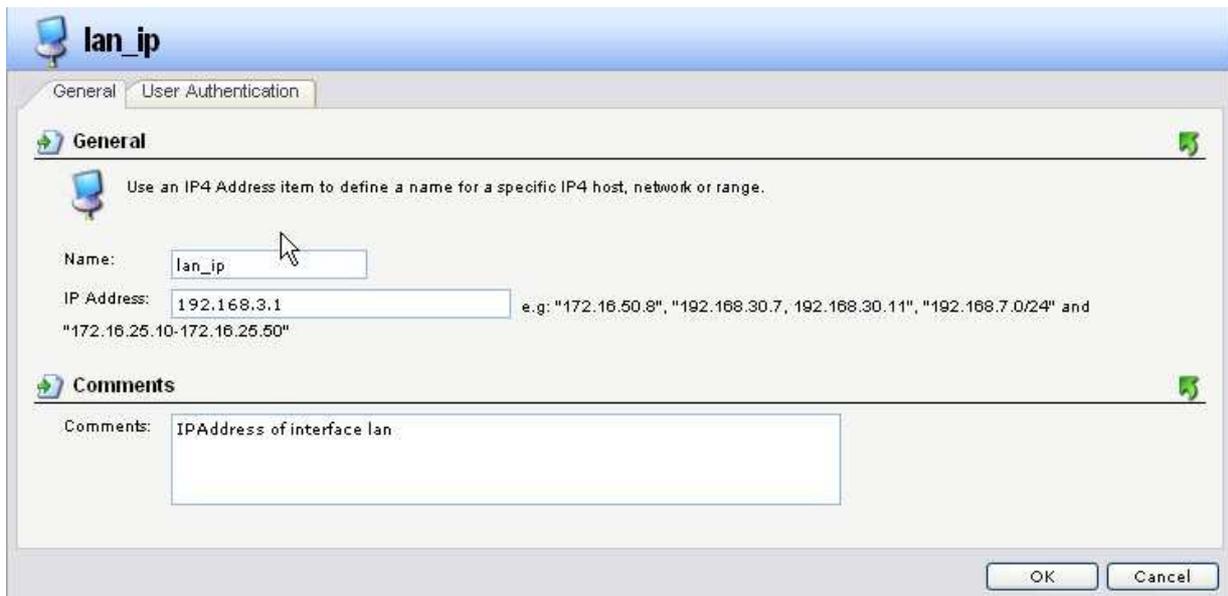


¹⁶ Diese Einstellung finden Sie unter folgendem Menüpunkt: / Objects / Address Book / Add / IP4 Address Group /

In der Übersicht sieht dies wie folgt aus:



Ändern Sie nun gegebenenfalls die bestehenden Objekte für LAN und WAN Interface: ¹⁷



¹⁷ Diese Einstellung finden Sie unter folgendem Menüpunkt: / Objects / Address Book /

lannet

General User Authentication

General

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

Name:

IP Address: 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:

OK Cancel

wan1_ip

General User Authentication

General

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

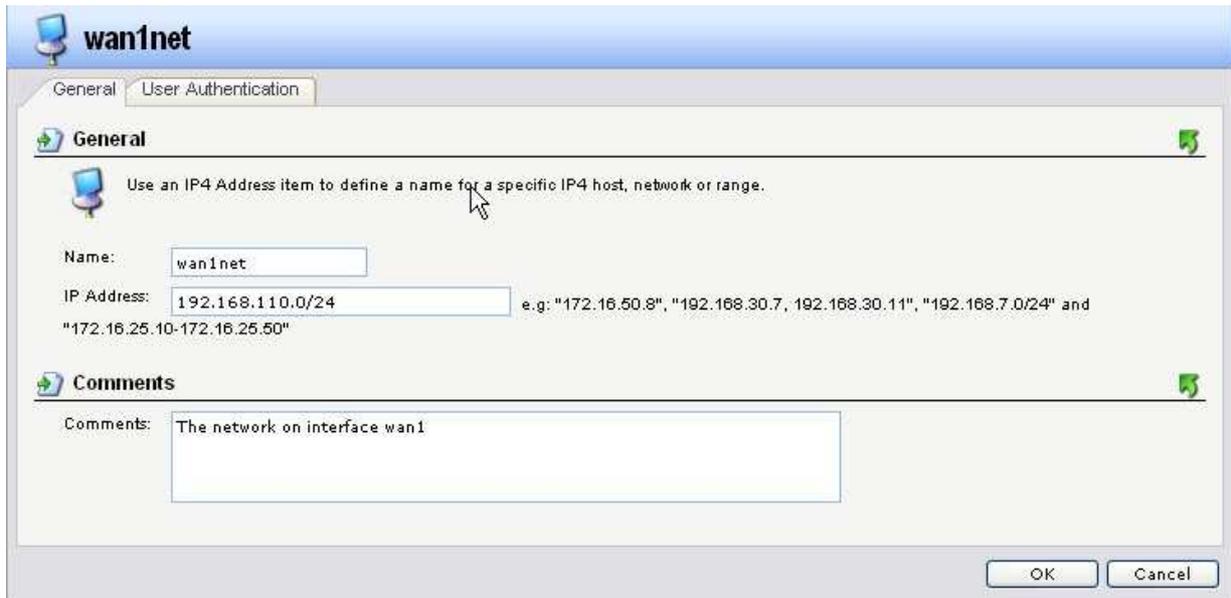
Name:

IP Address: 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:

OK Cancel



In der Übersicht sieht dies wie folgt aus:



Legen Sie nun den Pre-Shared Key an: ¹⁸

The screenshot shows the configuration page for a Pre-Shared Key (PSK) named 'fwABC-psk'. The page is titled 'fwABC-psk' and has a 'General' tab selected. Below the title, there is a key icon and a description: 'PSK (Pre-Shared Key) authentication is based on a shared secret that is known only by the parties involved.' The 'Name' field contains 'fwABC-psk'. Below this is the 'Shared Secret' section, which has two radio buttons: 'Passphrase' (selected) and 'Hexadecimal Key'. Under 'Passphrase', there are two input fields for 'Shared Secret' and 'Confirm Secret', both containing seven dots. There is also a 'Passphrase' input field and a 'Generate Random Key' button.

Legen Sie nun zwei IPSec Tunnel an: ¹⁹

The screenshot shows the configuration page for an IPSec tunnel named 'ipsectunnelAB-C'. The page is titled 'ipsectunnelAB-C' and has a 'General' tab selected. Below the title, there is a lock icon and a description: 'An IPSec tunnel item is used to define IPSec endpoint and will appear as a logical interface in the system.' The 'Name' field contains 'ipsectunnelAB-C'. Below this are four dropdown menus: 'Local Network' (fwBnet-localnet), 'Remote Network' (fwC-net), 'Remote Endpoint' (fwC-remotegw), and 'Encapsulation Mode' (Tunnel). Below these is the 'Algorithms' section, which has four fields: 'IKE Algorithms' (High), 'IKE Life Time' (28800 seconds), 'IPsec Algorithms' (High), and 'IPsec Life Time' (3600 seconds). There is also a field for 'IPsec Life Time' (0 kilobytes).

¹⁸ Diese Einstellung finden Sie unter folgendem Menüpunkt: / Objects / VPN-Objects / Pre-Shared-Keys /

¹⁹ Diese Einstellung finden Sie unter folgendem Menüpunkt: / Interfaces / IPSec Tunnels /

ipsectunnelAB-C

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

Authentication

X.509 Certificate

Root Certificate(s):

Available	Selected
AdminCert	

Gateway Certificate: (None)

Identification List: (None)

Pre-Shared Key

Pre-Shared Key: fwABC-psk

OK Cancel

ipsectunnelAC-B

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

General

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

Name: ipsectunnelAC-B

Local Network: fwCnet-localnet

Remote Network: fwB-net

Remote Endpoint: fwB-remotegw

Encapsulation Mode: Tunnel

Algorithms

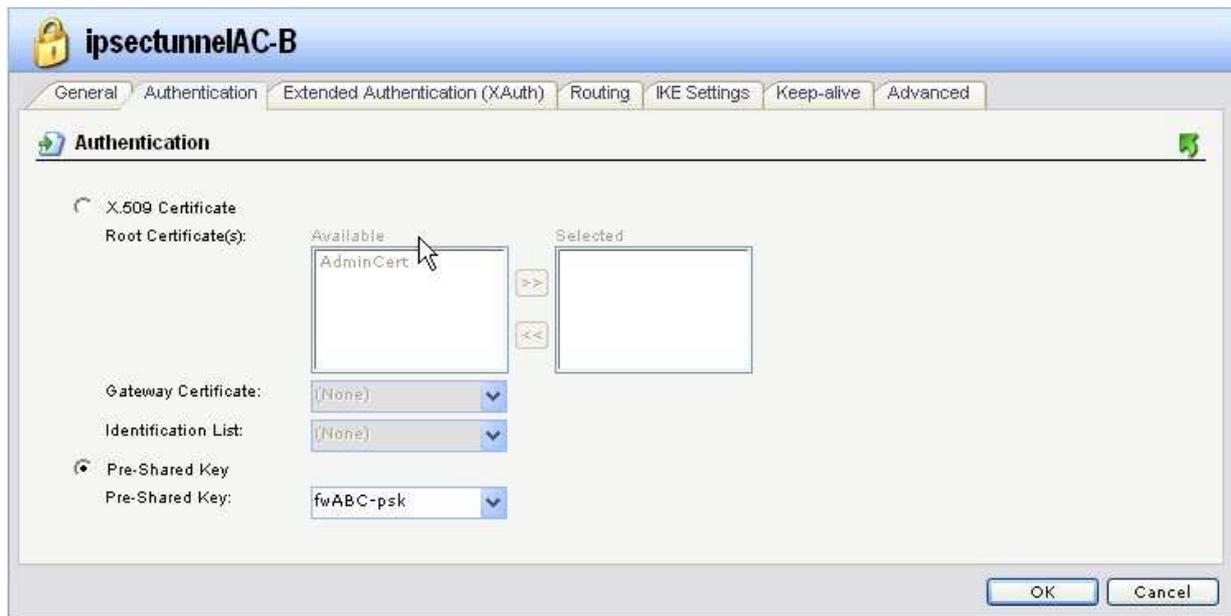
IKE Algorithms: High

IKE Life Time: 28800 seconds

IPsec Algorithms: High

IPsec Life Time: 3600 seconds

IPsec Life Time: 0 kilobytes



In der Übersicht sieht dies wie folgt aus:



Richten Sie nun die Access-Rules ein:²⁰

The screenshot shows the Mikrotik WinBox interface for configuring an IP rule. The title bar reads "allow_all". Below the title bar are tabs for "General", "Log Settings", "NAT", "SAT", and "SAT Server Load Balancing". The "General" tab is active. A green arrow icon is in the top right corner. Below the tab bar is a section titled "General" with a green arrow icon on the right. A traffic light icon is on the left, followed by the text: "An IP rule specifies what action to perform on network traffic that matches the specified filter criteria." Below this text are four fields: "Name:" with the value "allow_all", "Action:" with a dropdown menu showing "Allow", "Service:" with a dropdown menu showing "all_services", and "Schedule:" with a dropdown menu showing "(None)". Below the "General" section is another section titled "Address Filter" with a green arrow icon on the right. A traffic light icon is on the left, followed by the text: "Specify source interface and source network, together with destination interface and destination network. All parameters have to match for the rule to match." Below this text are two columns of fields. The "Source" column has "Interface:" with a dropdown menu showing "lan" and "Network:" with a dropdown menu showing "lanet". The "Destination" column has "Interface:" with a dropdown menu showing "ipsectunnelAC-B" and "Network:" with a dropdown menu showing "fwB-net".

The screenshot shows the Mikrotik WinBox interface for configuring an IP rule. The title bar reads "allow_all". Below the title bar are tabs for "General", "Log Settings", "NAT", "SAT", and "SAT Server Load Balancing". The "General" tab is active. A green arrow icon is in the top right corner. Below the tab bar is a section titled "General" with a green arrow icon on the right. A traffic light icon is on the left, followed by the text: "An IP rule specifies what action to perform on network traffic that matches the specified filter criteria." Below this text are four fields: "Name:" with the value "allow_all", "Action:" with a dropdown menu showing "Allow", "Service:" with a dropdown menu showing "all_services", and "Schedule:" with a dropdown menu showing "(None)". Below the "General" section is another section titled "Address Filter" with a green arrow icon on the right. A traffic light icon is on the left, followed by the text: "Specify source interface and source network, together with destination interface and destination network. All parameters have to match for the rule to match." Below this text are two columns of fields. The "Source" column has "Interface:" with a dropdown menu showing "ipsectunnelAB-C" and "Network:" with a dropdown menu showing "fwC-net". The "Destination" column has "Interface:" with a dropdown menu showing "ipsectunnelAC-B" and "Network:" with a dropdown menu showing "fwB-net". A mouse cursor is visible over the "Action:" dropdown menu.

²⁰ Diese Einstellung finden Sie unter folgendem Menüpunkt: / Rules / IP Rules /

allow_all

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:

Action:

Service:

Schedule:

Address Filter

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

	Source	Destination
Interface:	<input type="text" value="ipsectunnelAC-B"/>	<input type="text" value="lan"/>
Network:	<input type="text" value="fwB-net"/>	<input type="text" value="lannet"/>

allow_all

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:

Action:

Service:

Schedule:

Address Filter

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

	Source	Destination
Interface:	<input type="text" value="ipsectunnelAC-B"/>	<input type="text" value="ipsectunnelAB-C"/>
Network:	<input type="text" value="fwB-net"/>	<input type="text" value="fwC-net"/>

allow_all

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:

Action:

Service:

Schedule:

Address Filter

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

	Source	Destination
Interface:	<input type="text" value="ipsectunnelAB-C"/>	<input type="text" value="lan"/>
Network:	<input type="text" value="fwC-net"/>	<input type="text" value="lannet"/>

allow_all

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:

Action:

Service:

Schedule:

Address Filter

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

	Source	Destination
Interface:	<input type="text" value="lan"/>	<input type="text" value="ipsectunnelAB-C"/>
Network:	<input type="text" value="lannet"/>	<input type="text" value="fwC-net"/>

In der Übersicht sieht dies wie folgt aus:

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

Edit the settings for this folder

Add

#	Name	Action	Source Interface	Source Network	Destination Interface	Destination Network	Service
0	allow_all	Allow	lan	lannet	ipsectunnelAC-B	fwB-net	all_services
1	allow_all	Allow	ipsectunnelAB-C	fwC-net	ipsectunnelAC-B	fwB-net	all_services
2	allow_all	Allow	ipsectunnelAC-B	fwB-net	lan	lannet	all_services
3	allow_all	Allow	ipsectunnelAC-B	fwB-net	ipsectunnelAB-C	fwC-net	all_services
4	allow_all	Allow	ipsectunnelAB-C	fwC-net	lan	lannet	all_services
5	allow_all	Allow	lan	lannet	ipsectunnelAB-C	fwC-net	all_services

Right-click on a row for further options.

Nun kann eine Kommunikation zwischen PC B und PC C hergestellt werden.

Hierbei ist die Firewall A für den Verbindungsaufbau zwischen IPSec Tunnel zwischen Fw B – Fw A und Fw A – Fw C verantwortlich.