

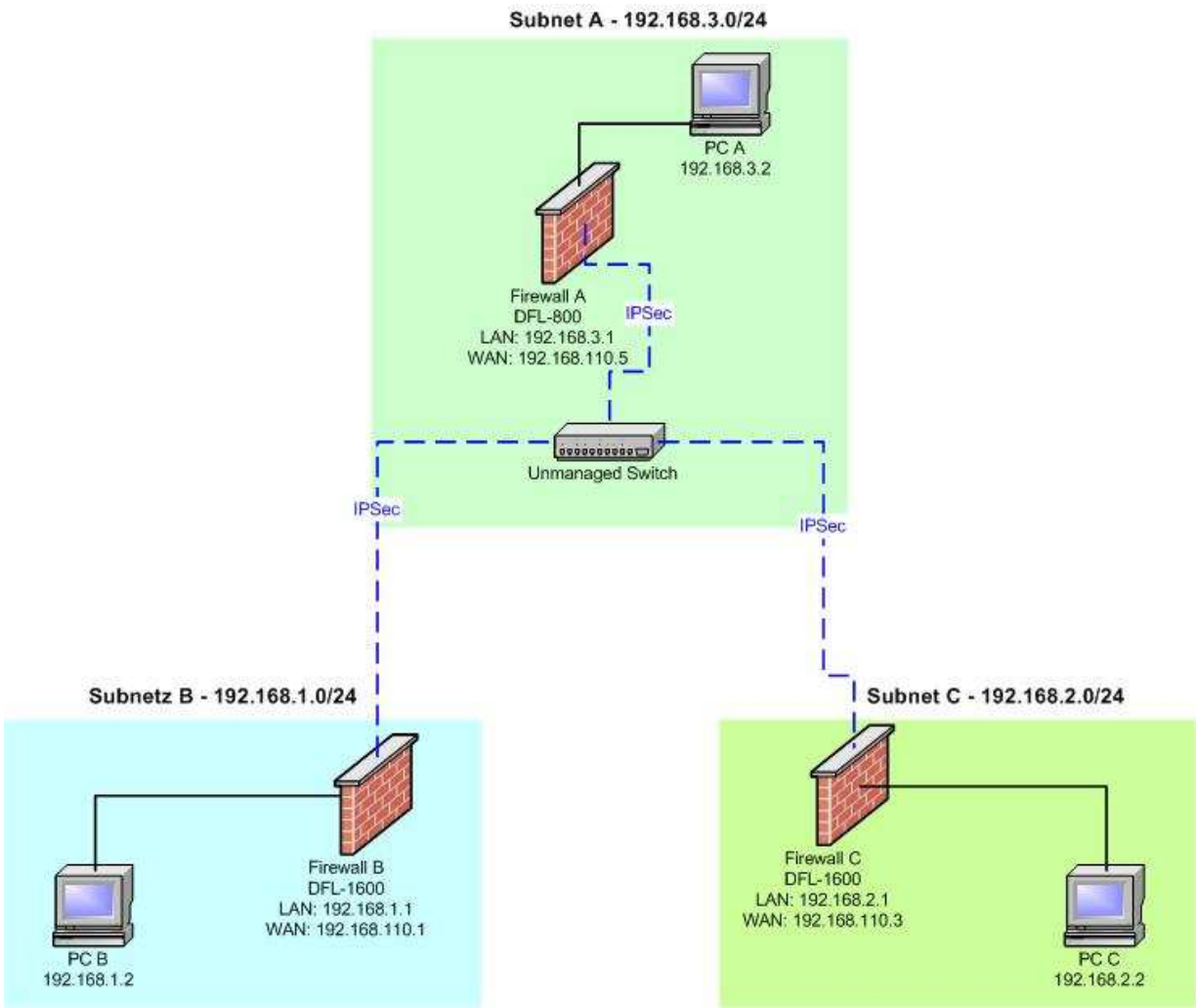
Einrichtung eines IPSec-Konzentrator *(Hub and Spoke)*

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 an object named 'fwA-remotegw'. The window has a title bar with a computer icon and the text 'fwA-remotegw'. Below the title bar are two tabs: 'General' (selected) and 'User Authentication'. The 'General' tab contains a section titled 'General' with a green arrow icon on the right. Below this is a text box with a computer icon and the instruction: 'Use an IP4 Address item to define a name for a specific IP4 host, network or range.' 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 is a text string: '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 large empty text box labeled 'Comments:'. At the bottom right are 'OK' and 'Cancel' buttons.

The screenshot shows the configuration window for an object named 'fwA-net'. The window has a title bar with a computer icon and the text 'fwA-net'. Below the title bar are two tabs: 'General' (selected) and 'User Authentication'. The 'General' tab contains a section titled 'General' with a green arrow icon on the right. Below this is a text box with a computer icon and the instruction: 'Use an IP4 Address item to define a name for a specific IP4 host, network or range.' 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 is a text string: '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 large empty text box labeled 'Comments:'. At the bottom right are 'OK' and 'Cancel' buttons.

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

fwC-net

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

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

fwB-remotenets

General User Authentication

General

An IP4 Address Group is used for combining several IP4 Address objects for simplified management.

Name:

Group members:

Available		Selected
wan1_ip	>>	fwA-net
wan1net	<<	fwC-net
wan2_ip		
wan2net		
dmz_ip		
dmznet		

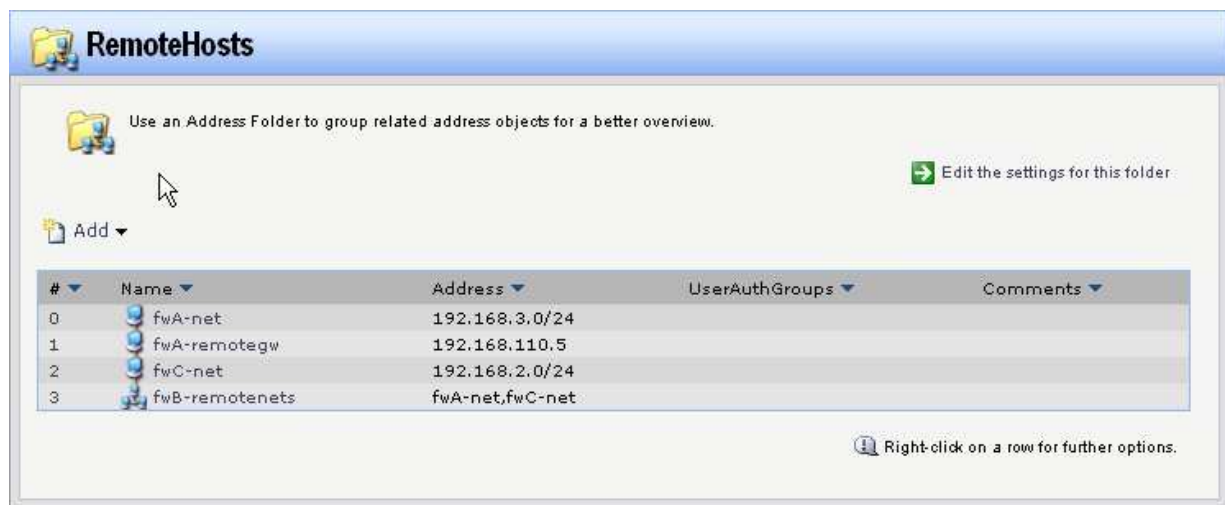
Comments

Comments:

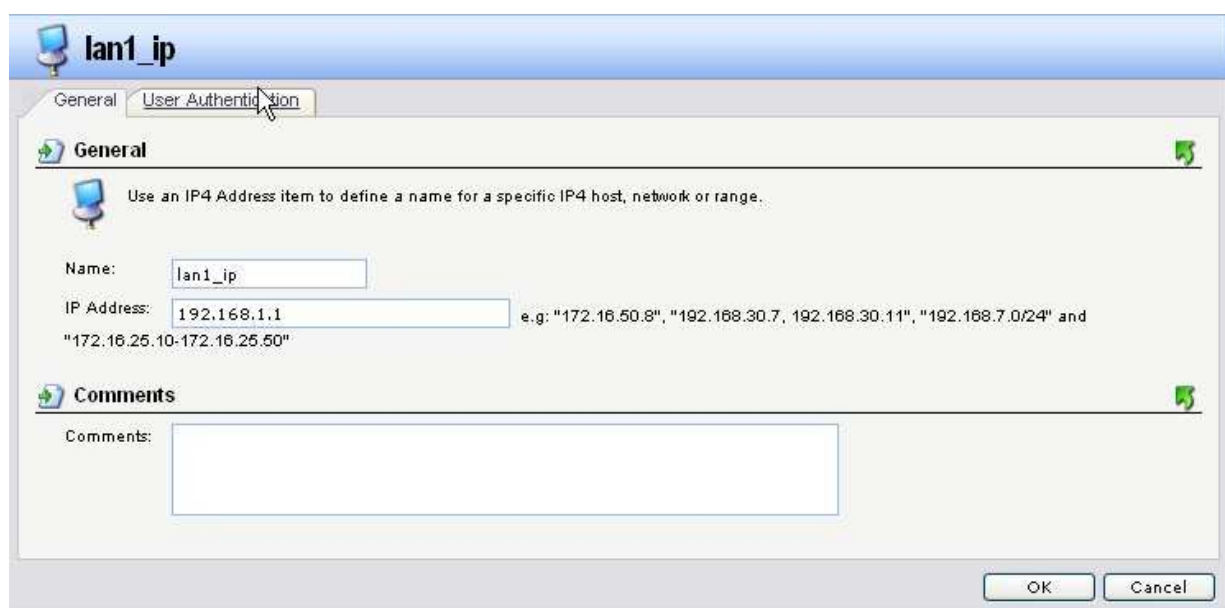
OK Cancel

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

GeneralUser Authentication

General





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


Name:


lan1net

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




Comments:


OK


Cancel

wan1_ip

GeneralUser Authentication

General





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


Name:


wan1_ip

IP Address:

192.168.110.1

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"

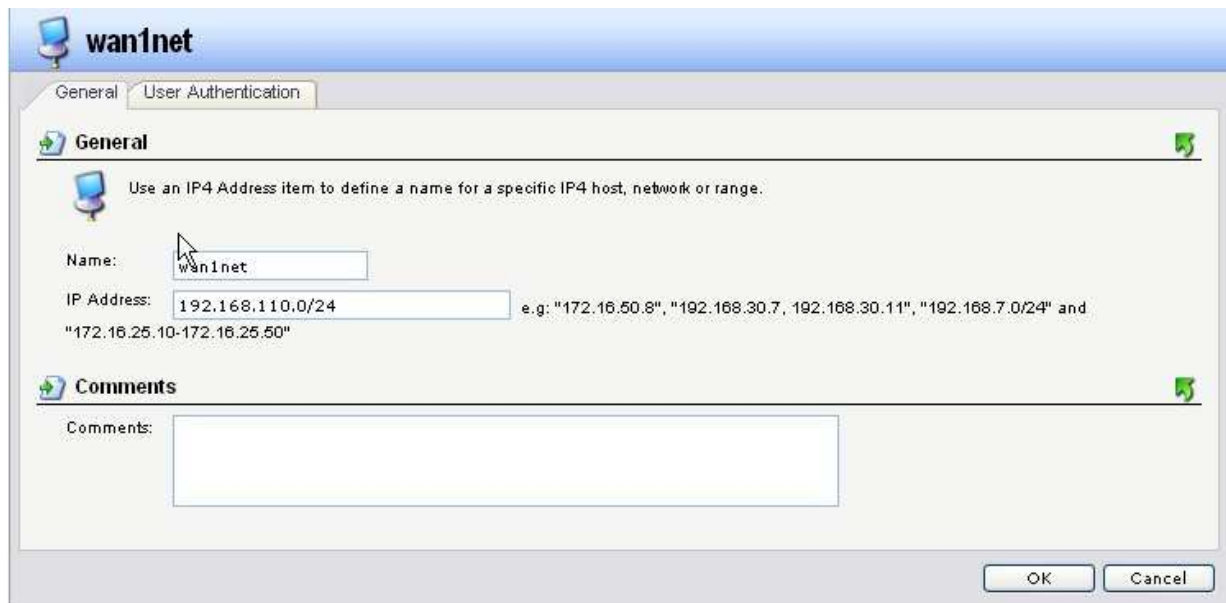
Comments



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 'ipsectunnelBA' configuration window with the 'General' tab selected. The window has a title bar with a lock icon and the text 'ipsectunnelBA'. Below the title bar are tabs: 'General', 'Authentication', 'Extended Authentication (XAuth)', 'Routing', 'IKE Settings', 'Keep-alive', and 'Advanced'. The 'General' tab is active, showing a description: 'An IPsec tunnel item is used to define IPsec endpoint and will appear as a logical interface in the system.' Below this are several fields: 'Name' (ipsectunnelBA), 'Local Network' (lan1net), 'Remote Network' (fwB-remotenets), 'Remote Endpoint' (fwA-remotegw), and 'Encapsulation Mode' (Tunnel). Below these fields is the 'Algorithms' section, which includes 'IKE Algorithms' (High), 'IKE Life Time' (28800 seconds), 'IPsec Algorithms' (High), 'IPsec Life Time' (3600 seconds), and 'IPsec Life Time' (0 kilobytes).

ipsectunnelBA

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: ipsectunnelBA

Local Network: lan1net

Remote Network: fwB-remotenets

Remote Endpoint: fwA-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

The screenshot shows the 'ipsectunnelBA' configuration window with the 'Authentication' tab selected. The window has a title bar with a lock icon and the text 'ipsectunnelBA'. Below the title bar are tabs: 'General', 'Authentication', 'Extended Authentication (XAuth)', 'Routing', 'IKE Settings', 'Keep-alive', and 'Advanced'. The 'Authentication' tab is active, showing two radio buttons: 'X.509 Certificate' (selected) and 'Pre-Shared Key'. Below the 'X.509 Certificate' radio button are two lists: 'Available' (AdminCert) and 'Selected'. Below these lists are three dropdown menus: 'Gateway Certificate' (None), 'Identification List' (None), and 'Pre-Shared Key' (fwABC-psk). At the bottom right are 'OK' and 'Cancel' buttons.

ipsectunnelBA

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

Authentication

☐ X.509 Certificate

Root Certificate(s):

Available: AdminCert

Selected:

Gateway Certificate: (None)

Identification List: (None)

☒ Pre-Shared Key

Pre-Shared Key: fwABC-psk

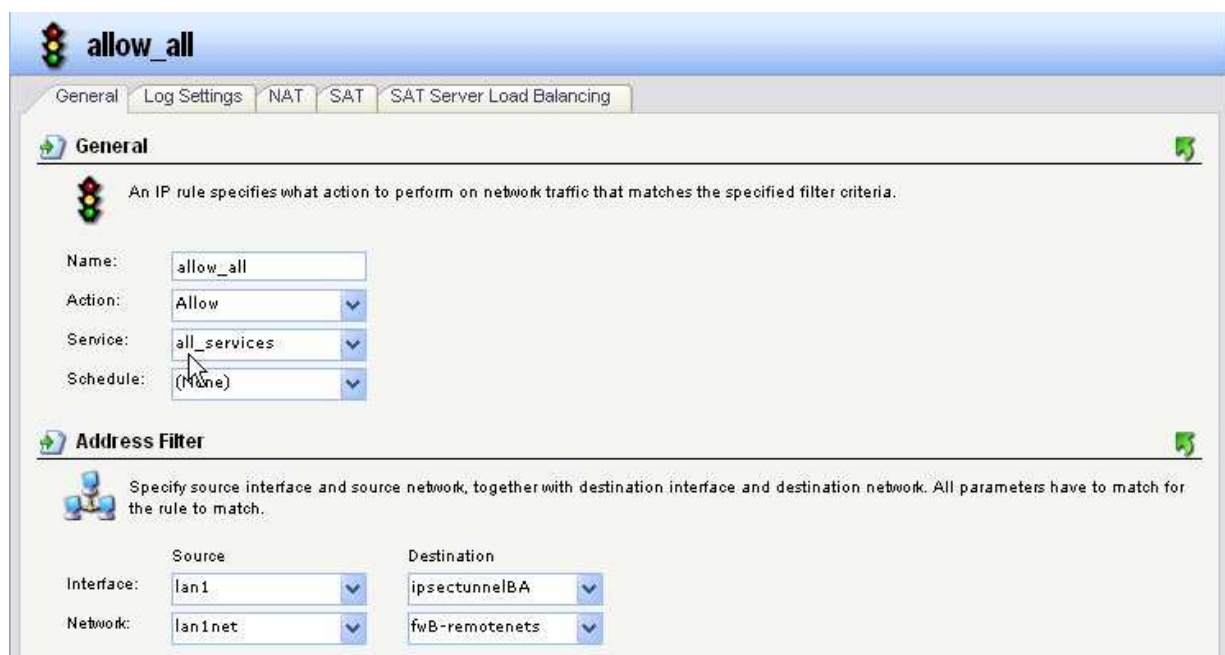
OK Cancel

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:	<input type="text" value="ipsectunnelBA"/>	<input type="text" value="lan1"/>
Network:	<input type="text" value="fwB-remotenets"/>	<input type="text" value="lan1net"/>

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 'fwA-remotegw' configuration window. It has two tabs: 'General' and 'User Authentication'. The 'General' tab is active. Below the tab bar, there is a section titled 'General' with a green plus icon and a green minus icon. Below this, there is a text box with the instruction: 'Use an IP4 Address item to define a name for a specific IP4 host, network or range.' Below this instruction, 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 text string: '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 input fields, there is a section titled 'Comments' with a green plus icon and a green minus icon. Below this, there is a text box with the label 'Comments:'. At the bottom right of the window, there are two buttons: 'OK' and 'Cancel'.

The screenshot shows the 'fwA-net' configuration window. It has two tabs: 'General' and 'User Authentication'. The 'General' tab is active. Below the tab bar, there is a section titled 'General' with a green plus icon and a green minus icon. Below this, there is a text box with the instruction: 'Use an IP4 Address item to define a name for a specific IP4 host, network or range.' Below this instruction, 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 text string: '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 input fields, there is a section titled 'Comments' with a green plus icon and a green minus icon. Below this, there is a text box with the label 'Comments:'. At the bottom right of the window, there are two buttons: 'OK' and 'Cancel'.

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

fwB-net

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

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

fwC-remotenets

General User Authentication

General

An IP4 Address Group is used for combining several IP4 Address objects for simplified management.

Name:

Group members:

Available		Selected
wan1_ip	>>	fwA-net
wan1net		fwB-net
wan2_ip	<<	
wan2net		
dmz_ip		
dmznet		

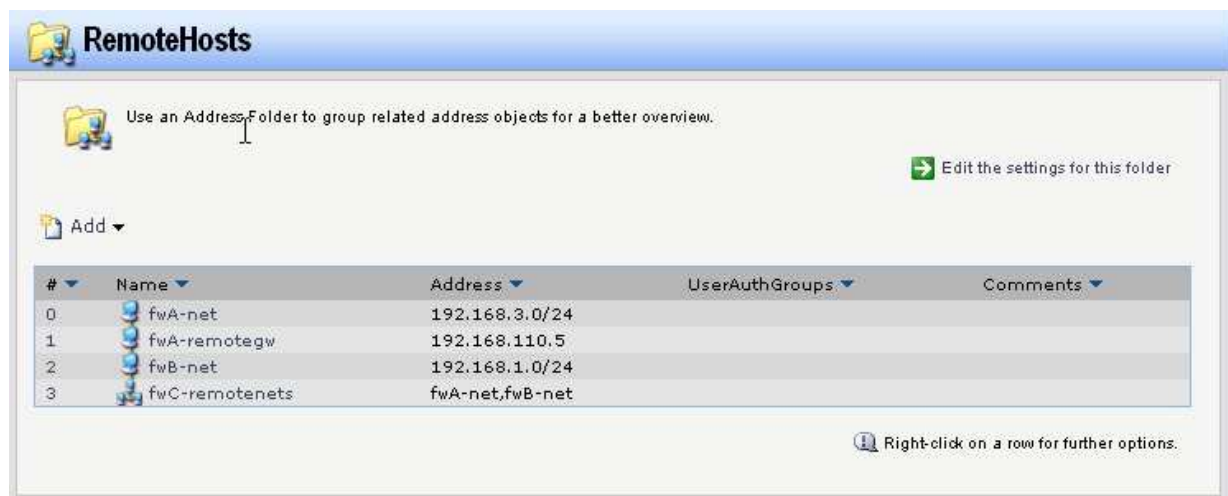
Comments

Comments:

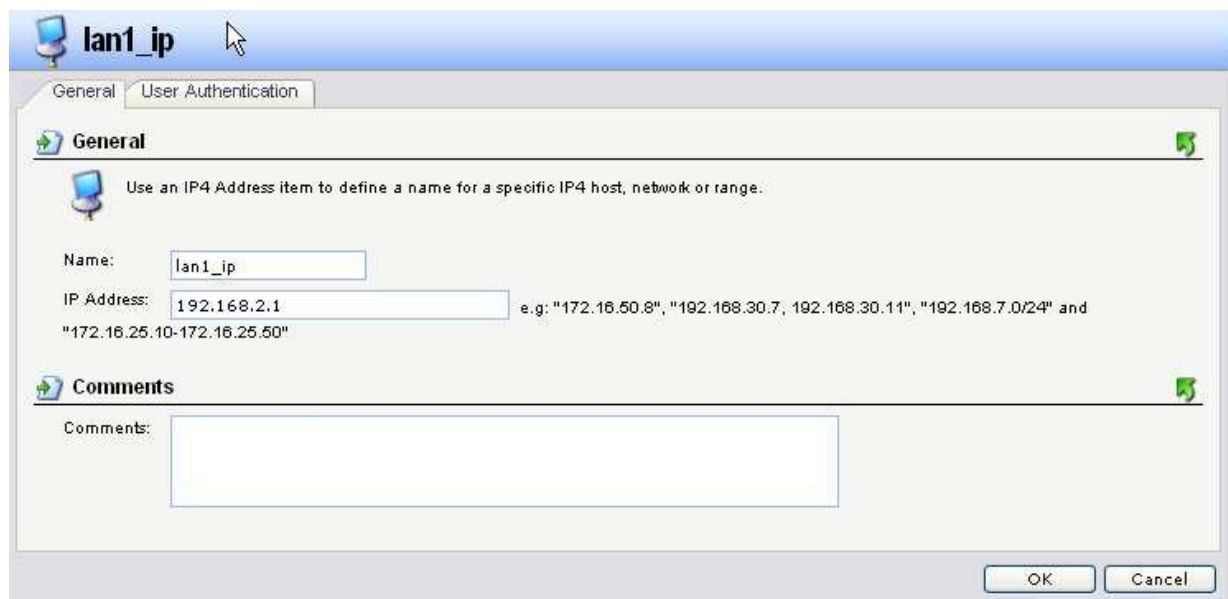
OK Cancel

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 Objekt für LAN und WAN Interface:⁹





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

lan1net

GeneralUser Authentication

General





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


Name:


lan1net

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:


OK


Cancel

wan1_ip

GeneralUser Authentication

General





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


Name:


wan1_ip

IP Address:

192.168.110.3

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"

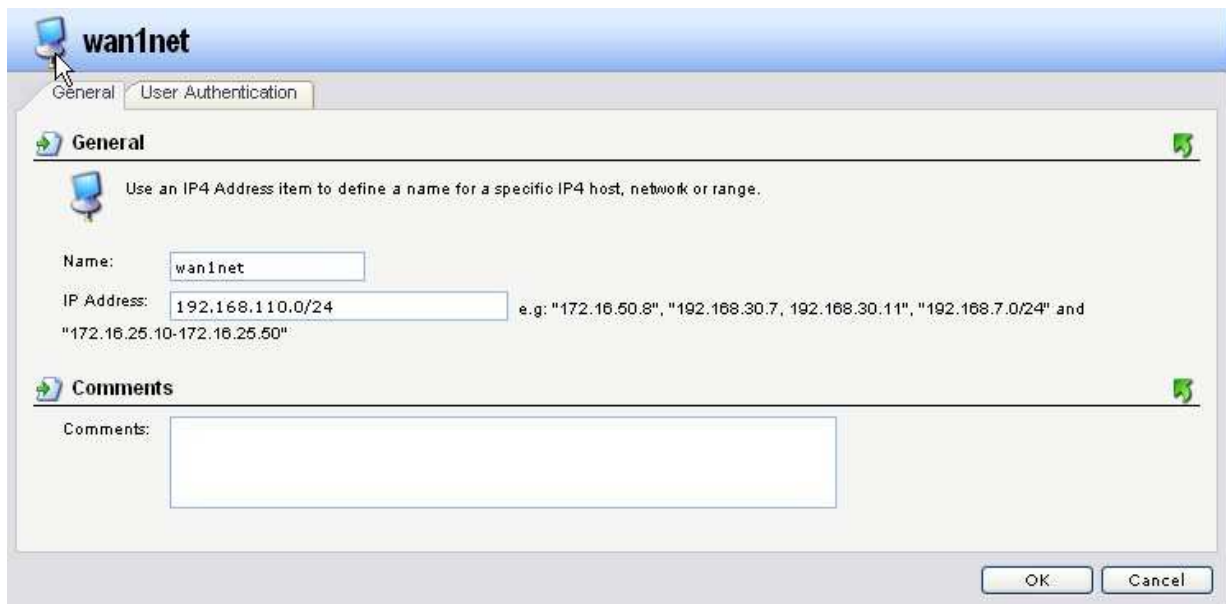
Comments



Comments:

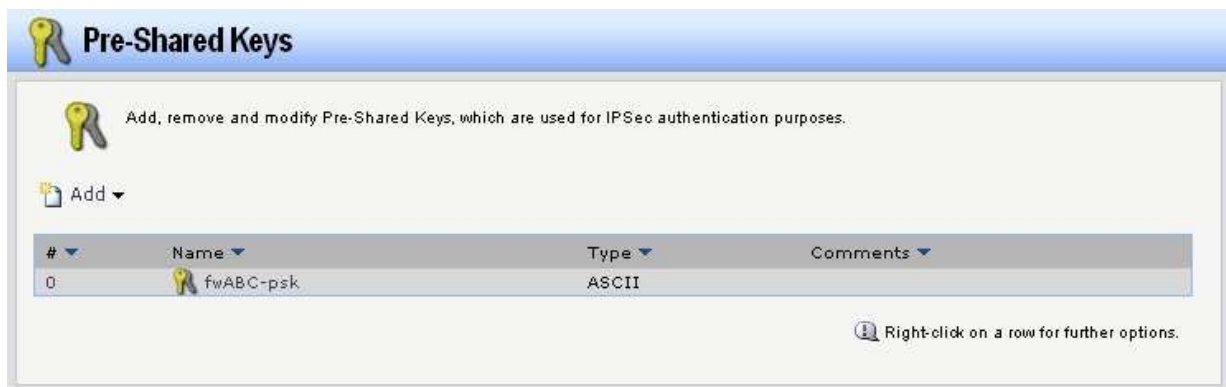
OK

Cancel



The image shows a software window titled "wan1net" with a blue header bar. Below the header, there are two tabs: "General" (selected) and "User Authentication". The "General" tab contains a section with a computer icon and the text "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 "wan1net" and "IP Address:" with the value "192.168.110.0/24". To the right of the IP Address field, there is a text string: "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 "Comments:" label followed by a large empty text box. At the bottom right of the window, there are "OK" and "Cancel" buttons.

Legen Sie nun den Pre-Shared Key an: ¹⁰



The image shows a software window titled "Pre-Shared Keys" with a blue header bar. Below the header, there is a section with a key icon and the text "Add, remove and modify Pre-Shared Keys, which are used for IPSec authentication purposes." Below this, there is an "Add" button with a dropdown arrow. Below the button, there is a table with the following columns: "#", "Name", "Type", and "Comments". The table contains one row with the index "0", the name "fwABC-psk" (preceded by a key icon), the type "ASCII", and an empty comments field. Below the table, there is a message icon and the text "Right-click on a row for further options."

#	Name	Type	Comments
0	fwABC-psk	ASCII	

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 has a title bar with a lock icon and the text 'ipsectunnelCA'. Below the title bar are tabs: 'General', 'Authentication', 'Extended Authentication (XAuth)', 'Routing', 'IKE Settings', 'Keep-alive', and 'Advanced'. The 'General' tab is active, showing a description: 'An IPsec tunnel item is used to define IPsec endpoint and will appear as a logical interface in the system.' Below this are several configuration fields: 'Name' (ipsectunnelCA), 'Local Network' (lan1net), 'Remote Network' (fwC-remotenets), 'Remote Endpoint' (fwA-remotegw), and 'Encapsulation Mode' (Tunnel). Below these fields is the 'Algorithms' section, which includes 'IKE Algorithms' (High), 'IKE Life Time' (28800 seconds), 'IPsec Algorithms' (High), 'IPsec Life Time' (3600 seconds), and 'IPsec Life Time' (0 kilobytes).

ipsectunnelCA

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: ipsectunnelCA

Local Network: lan1net

Remote Network: fwC-remotenets

Remote Endpoint: fwA-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

The screenshot shows the 'ipsectunnelCA' configuration window with the 'Authentication' tab selected. The window has a title bar with a lock icon and the text 'ipsectunnelCA'. Below the title bar are tabs: 'General', 'Authentication', 'Extended Authentication (XAuth)', 'Routing', 'IKE Settings', 'Keep-alive', and 'Advanced'. The 'Authentication' tab is active, showing the 'X.509 Certificate' section. It includes a 'Root Certificate(s)' section with 'Available' and 'Selected' lists. The 'Available' list contains 'AdminCert:'. Below this are 'Gateway Certificate' (None) and 'Identification List' (None). The 'Pre-Shared Key' section is selected, showing 'Pre-Shared Key' (fwABC-psk). At the bottom right are 'OK' and 'Cancel' buttons.

ipsectunnelCA

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

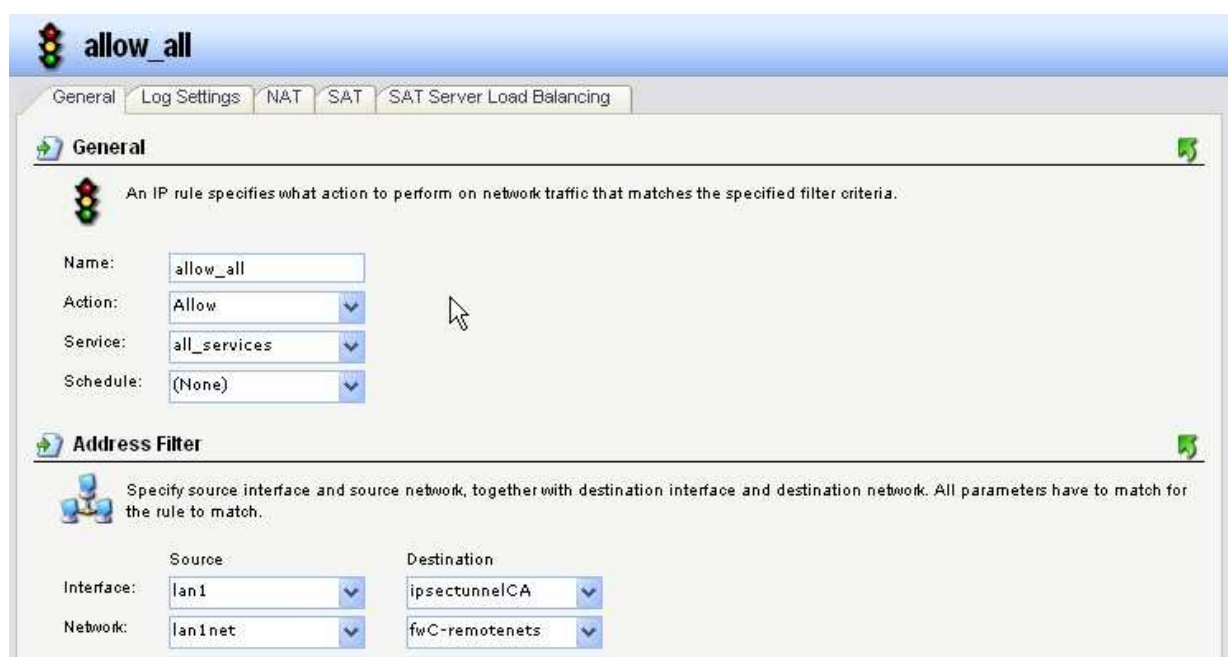
OK Cancel

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.

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	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:

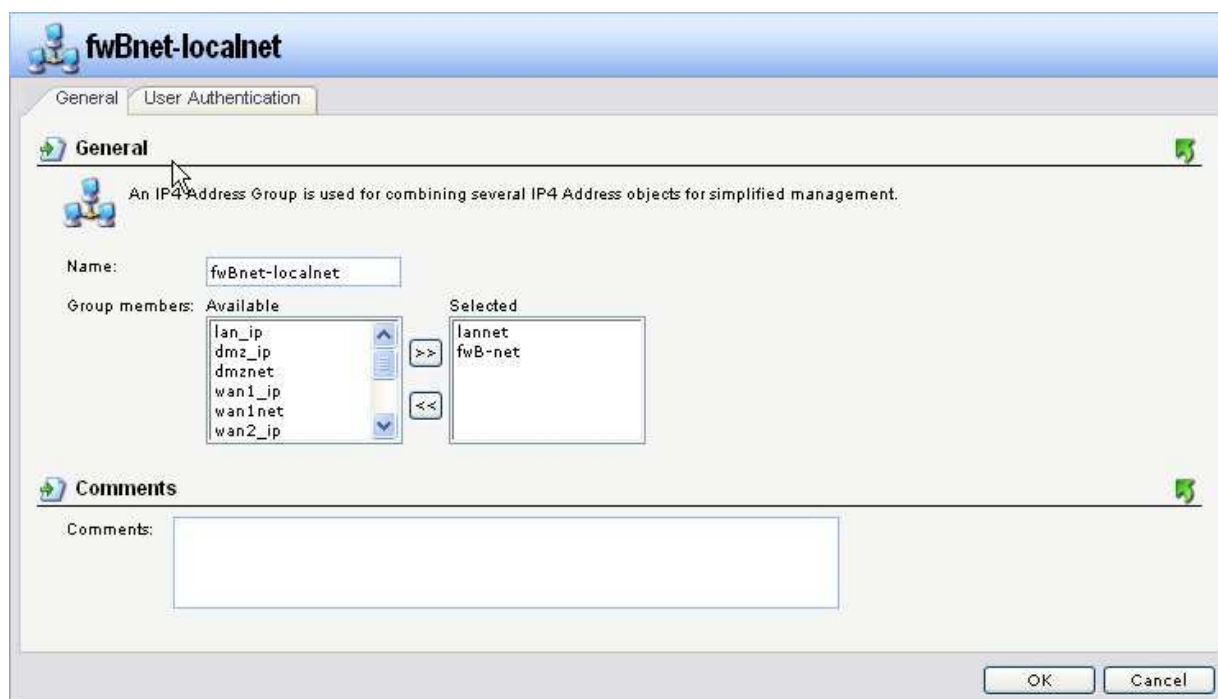
Zuerst wurden die folgenden Objekte auf Firewall A angelegt:¹³

The screenshot shows a configuration window titled 'fwB-remotegw'. It has two tabs: 'General' (selected) and 'User Authentication'. The 'General' tab contains a 'General' section with 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 'fwB-remotegw' and 'IP Address:' with the value '192.168.110.1'. To the right of the IP Address field, there is a list of example IP addresses: '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 a large empty text area. At the bottom right, there are 'OK' and 'Cancel' buttons.

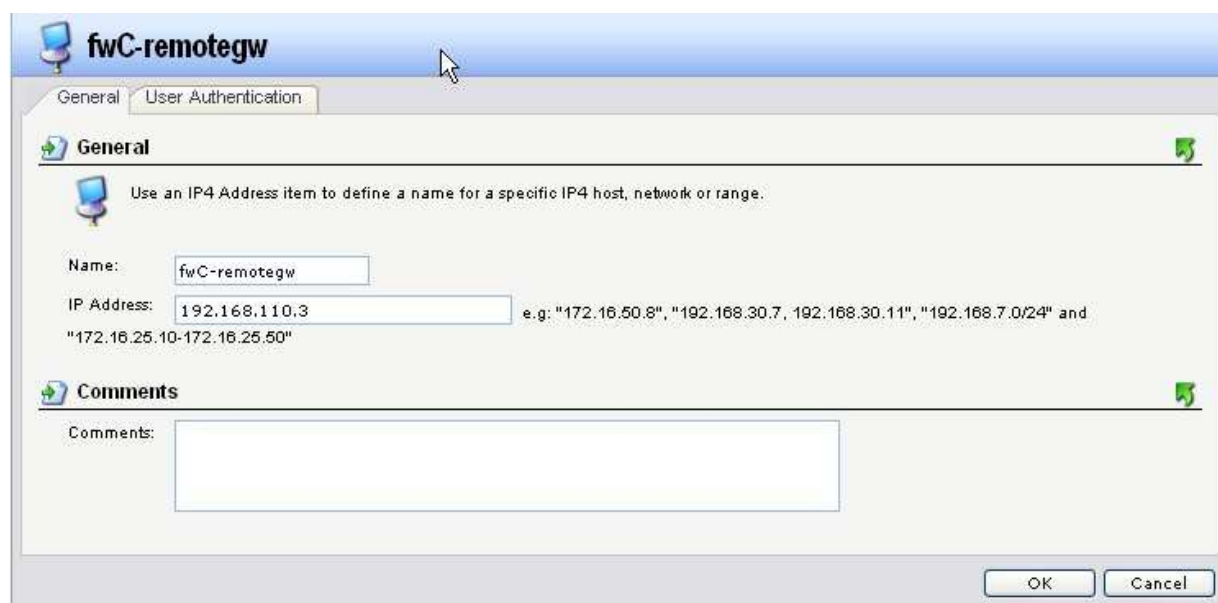
The screenshot shows a configuration window titled 'fwB-net'. It has two tabs: 'General' (selected) and 'User Authentication'. The 'General' tab contains a 'General' section with a description: 'Use an IP4 Address item to define a name for a specific IP4 host, network or range.' Below this, there are two input fields: 'Name:' with the value 'fwB-net' and 'IP Address:' with the value '192.168.1.0/24'. To the right of the IP Address field, there is a list of example IP addresses: '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 a large empty text area. At the bottom right, there are 'OK' and 'Cancel' buttons.

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

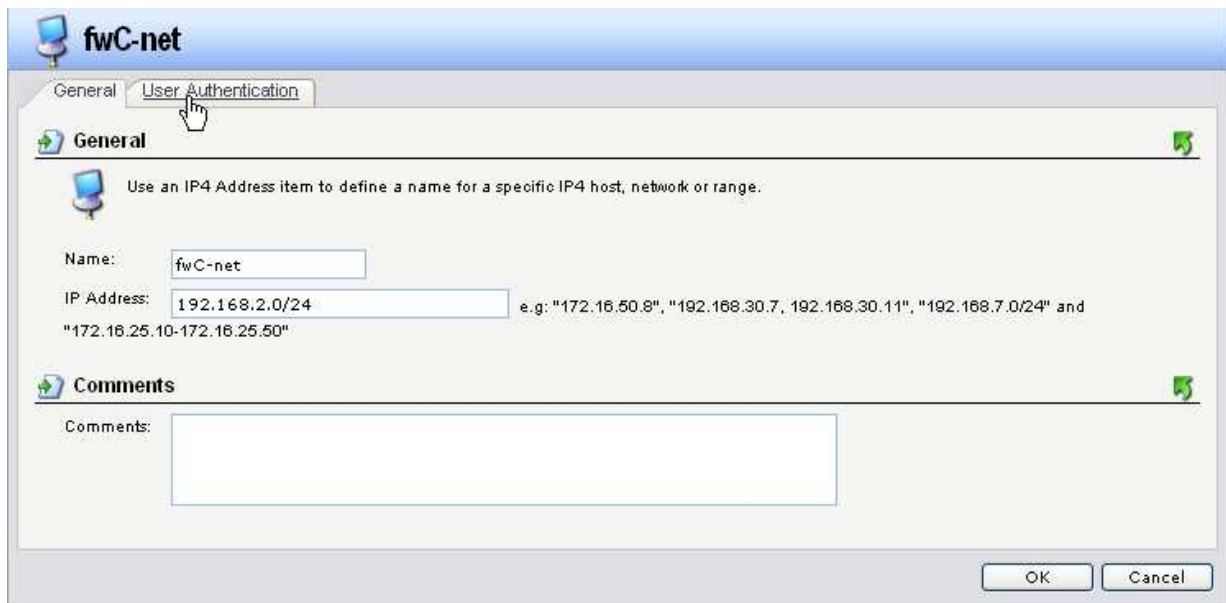


Legen Sie nun weitere Objekte an: ¹⁵

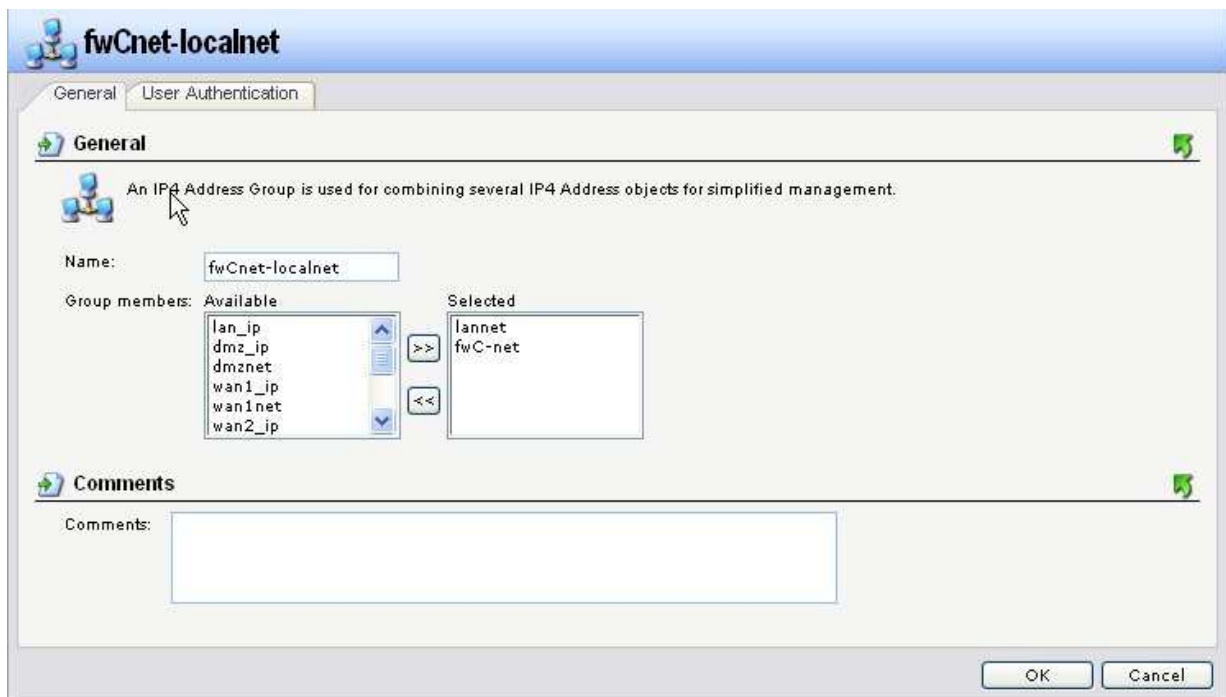


¹⁴ Diese Einstellung finden Sie unter folgendem Menüpunkt: / Objects / Address Book / Add / IP4 Address Group /

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

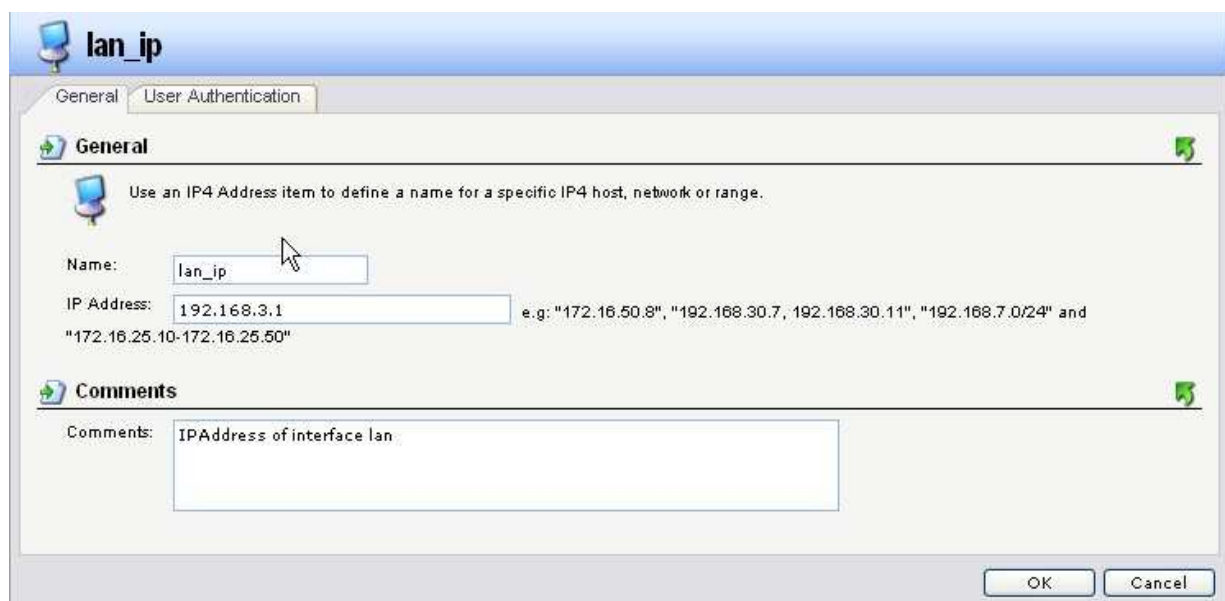


¹⁶ Diese Einstellung finden Sie unter folgendem Menüpunkt: / Objects / Address Book / Add / IP4 Address Group /


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

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

In der Übersicht sieht dies wie folgt aus:

InterfaceAddresses

Use an Address Folder to group related address objects for a better overview.

Edit the settings for this folder

Add

#	Name	Address	UserAuthGroups	Comments
0	lan_ip	192.168.3.1		IPAddress of interface lan
1	lan1net	192.168.3.0/24		The network on interface lan
2	dmz_ip	172.17.100.254		IPAddress of interface dmz
3	dmznet	172.17.100.0/24		The network on interface dmz
4	wan1_ip	192.168.110.5		IPAddress of interface wan1
5	wan1net	192.168.110.0/24		The network on interface wan1
6	wan2_ip	192.168.120.254		IPAddress of interface wan2
7	wan2net	192.168.120.0/24		The network on interface wan2

Right-click on a row for further options.

Legen Sie nun den Pre-Shared Key an: ¹⁸

fwABC-psk

General

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

Name:

Shared Secret

☒ Passphrase

Shared Secret:

Confirm Secret:

☐ Hexadecimal Key

Passphrase:

Legen Sie nun zwei IPSec Tunnel an: ¹⁹

ipsectunnelAB-C

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:

Local Network:

Remote Network:

Remote Endpoint:

Encapsulation Mode:

Algorithms

IKE Algorithms:

IKE Life Time: seconds


IPsec Algorithms:

IPsec Life Time: seconds

IPsec Life Time: 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

AdminCert

>>

<<

Selected

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

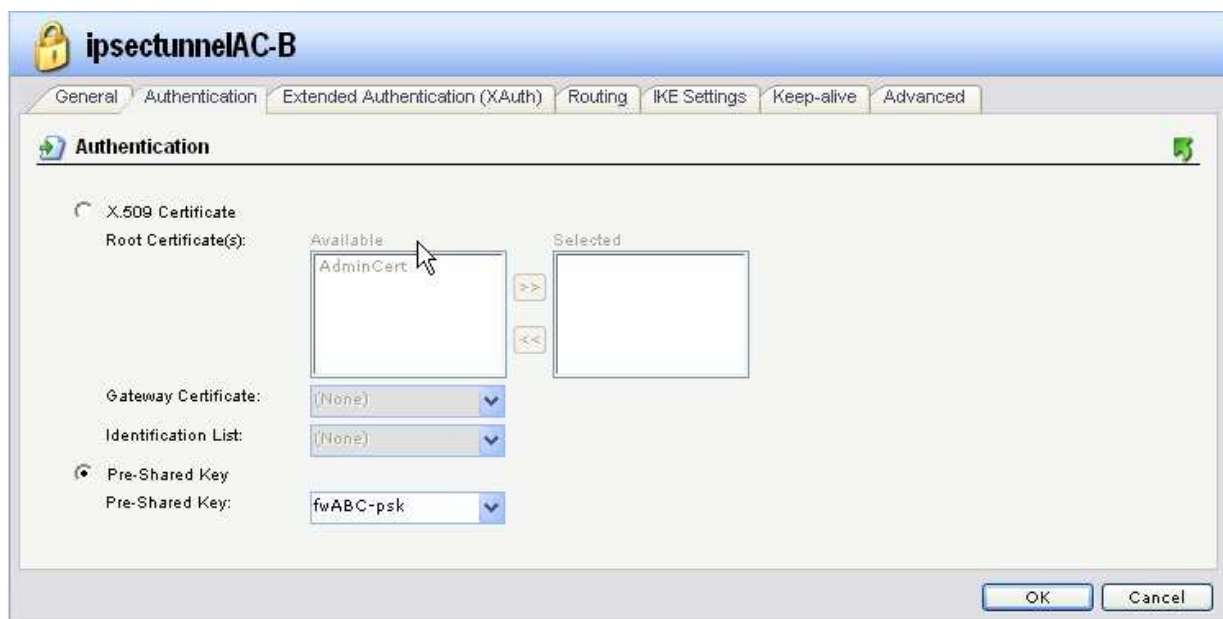
3600

 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 is 'allow_all'. The 'General' tab is selected. The 'General' section contains the following fields:

- Name: allow_all
- Action: Allow
- Service: all_services
- Schedule: (None)

The 'Address Filter' section is also visible, with the following fields:

- Source Interface: lan
- Source Network: lan-net
- Destination Interface: ipsectunnelAC-B
- Destination Network: fwB-net


The screenshot shows the Mikrotik WinBox interface for configuring an IP rule. The title bar is 'allow_all'. The 'General' tab is selected. The 'General' section contains the following fields:

- Name: allow_all
- Action: Allow
- Service: all_services
- Schedule: (None)


The 'Address Filter' section is also visible, with the following fields:


- Source Interface: ipsectunnelAB-C
- Source Network: fwC-net
- Destination Interface: ipsectunnelAC-B
- Destination Network: fwB-net

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

 **allow_all**

GeneralLog SettingsNATSATSAT Server Load Balancing

 **General**


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


Name:allow_all

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 to match for the rule to match.

Source


Interface:ipsectunnelAC-B

Network:fwB-net


Destination


Interface:lan

Network:lannet

 **allow_all**

GeneralLog SettingsNATSATSAT Server Load Balancing

 **General**


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


Name:allow_all

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 to match for the rule to match.

Source


Interface:ipsectunnelAC-B

Network:fwB-net


Destination


Interface:ipsectunnelAB-C

Network:fwC-net

 **allow_all**

GeneralLog SettingsNATSATSAT Server Load Balancing

 **General**


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


Name:allow_all

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 to match for the rule to match.

Source


Interface:ipsectunnelAB-C

Network:fwC-net


Destination


Interface:lan

Network:lannet

 **allow_all**

GeneralLog SettingsNATSATSAT Server Load Balancing

 **General**


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


Name:allow_all

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 to match for the rule to match.

Source

Interface:lan

Network:lannet

Destination

Interface:ipsectunnelAB-C

Network:fwC-net

In der Übersicht sieht dies wie folgt aus:



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.