Einrichtung eines IPSec-Konzentrator

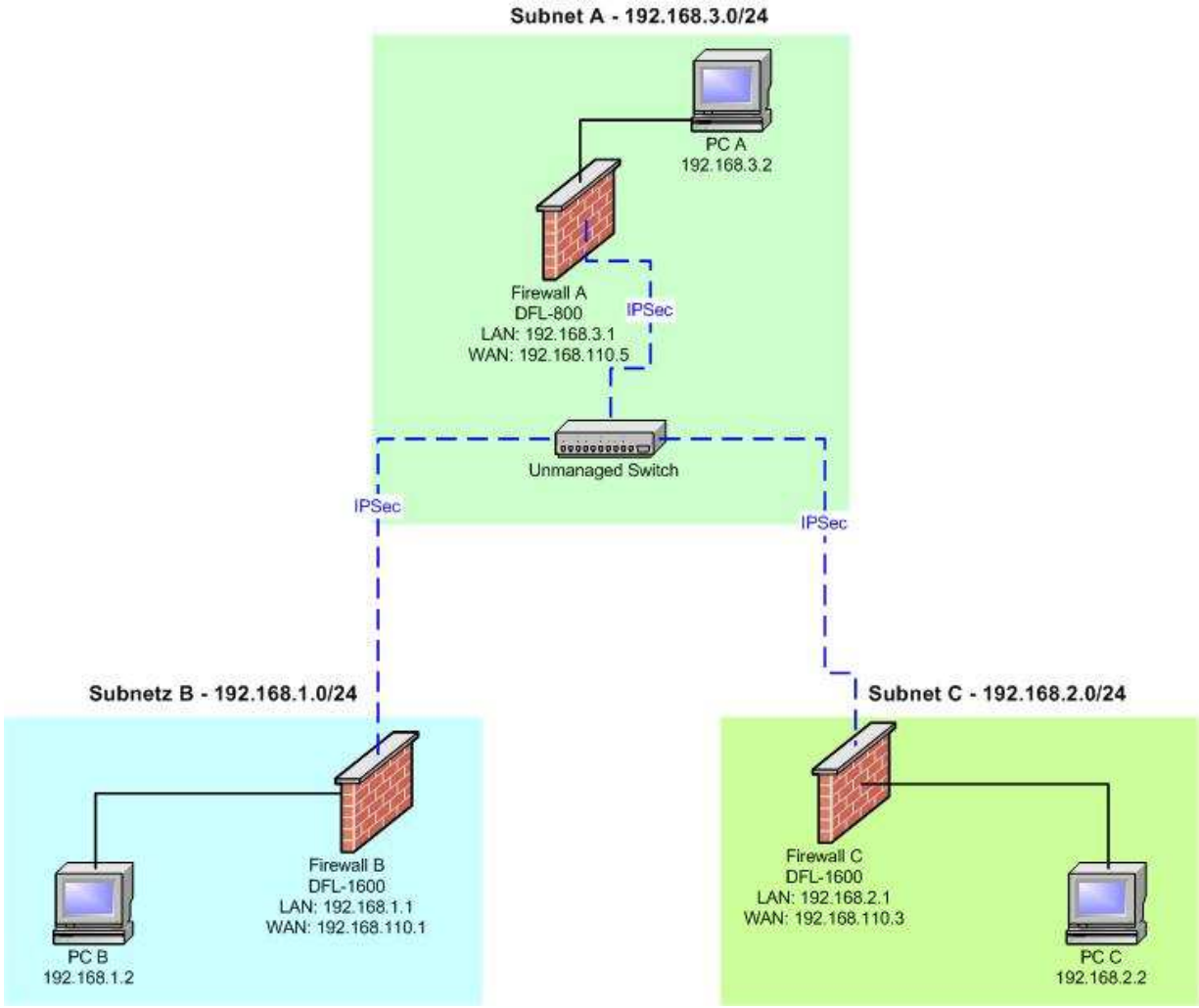
(Hub and Spoke)

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.

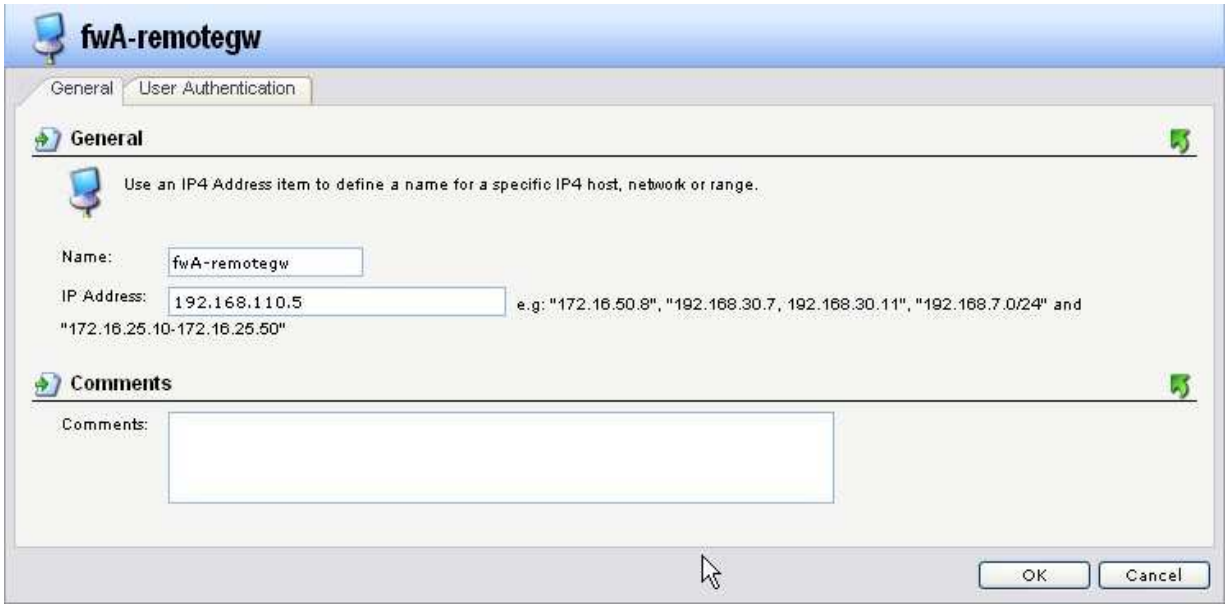
Viele dieser Informationen finden Sie beispielsweise unter: http://de.wikipedia.org/wiki/

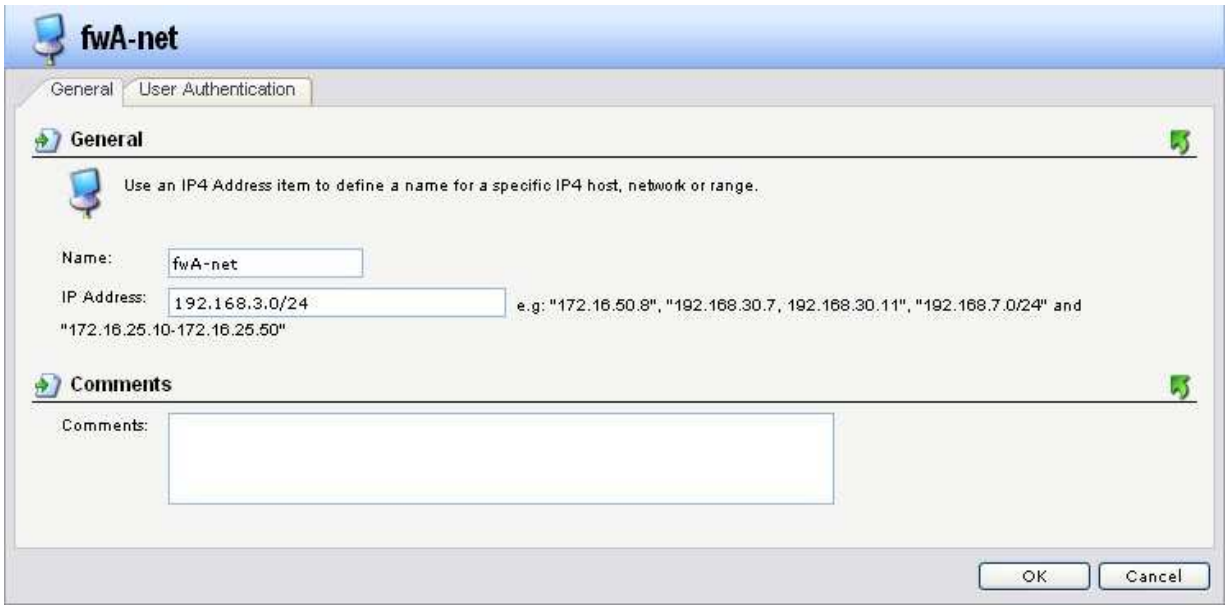
Testumgebung:



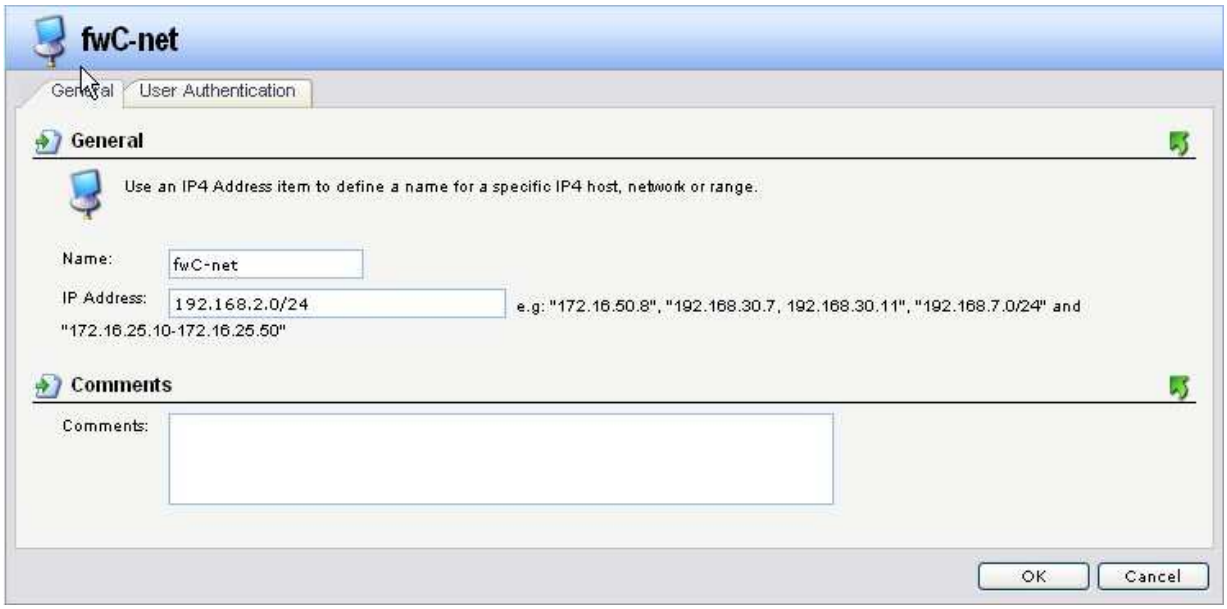
Konfiguration auf Firewall B:

Zuerst wurden die folgenden Objekte auf Firewall B angelegt: [1]

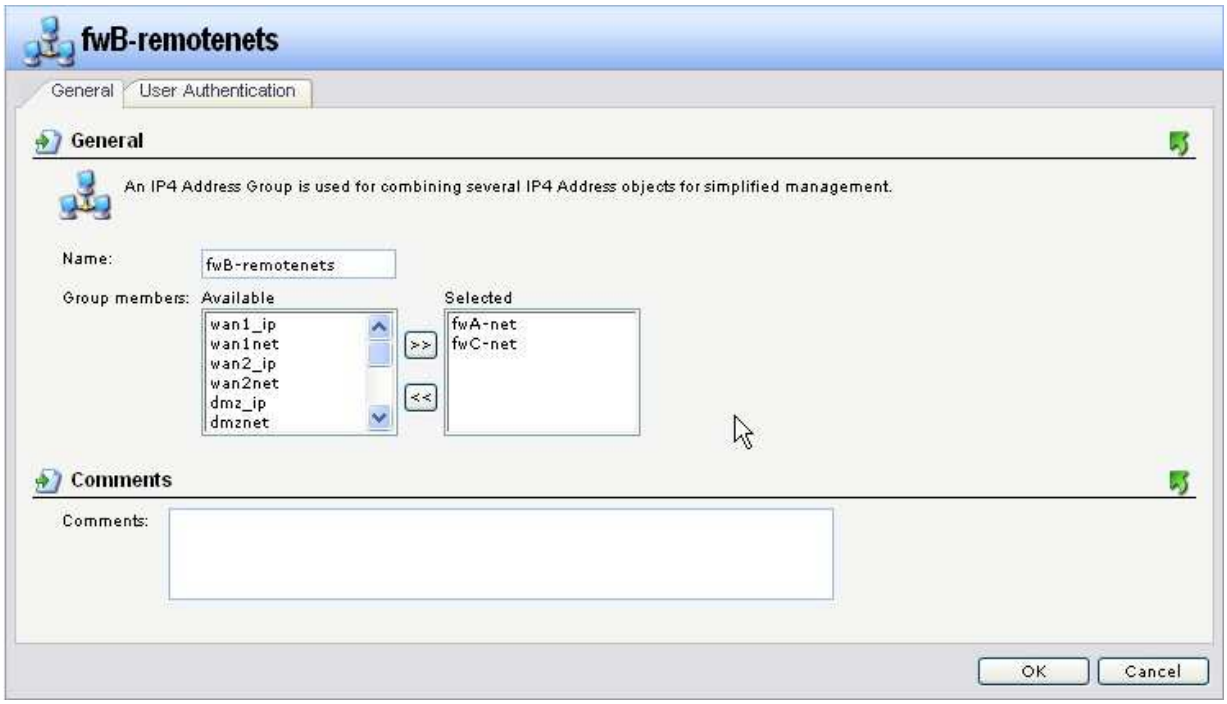




[1] Diese Einstellung finden Sie unter folgendem Menüpunkt: / Objects / Address Book / Add / IP4 Host/Network /



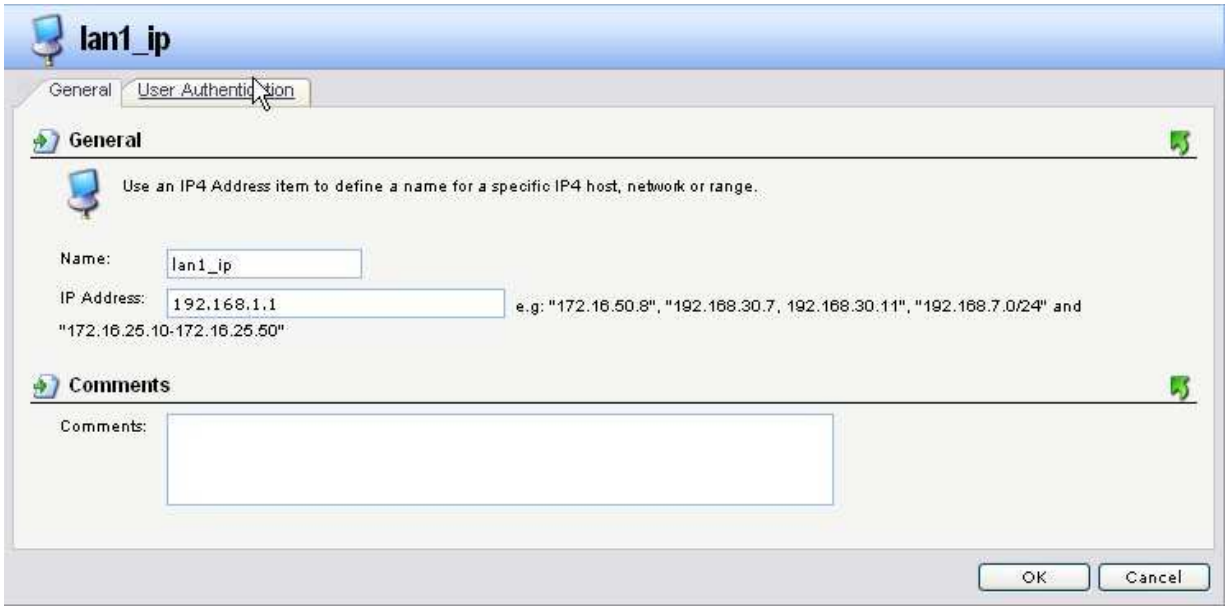
Nun muss weiterhin eine neue IP-Gruppe angelegt werden: [2]



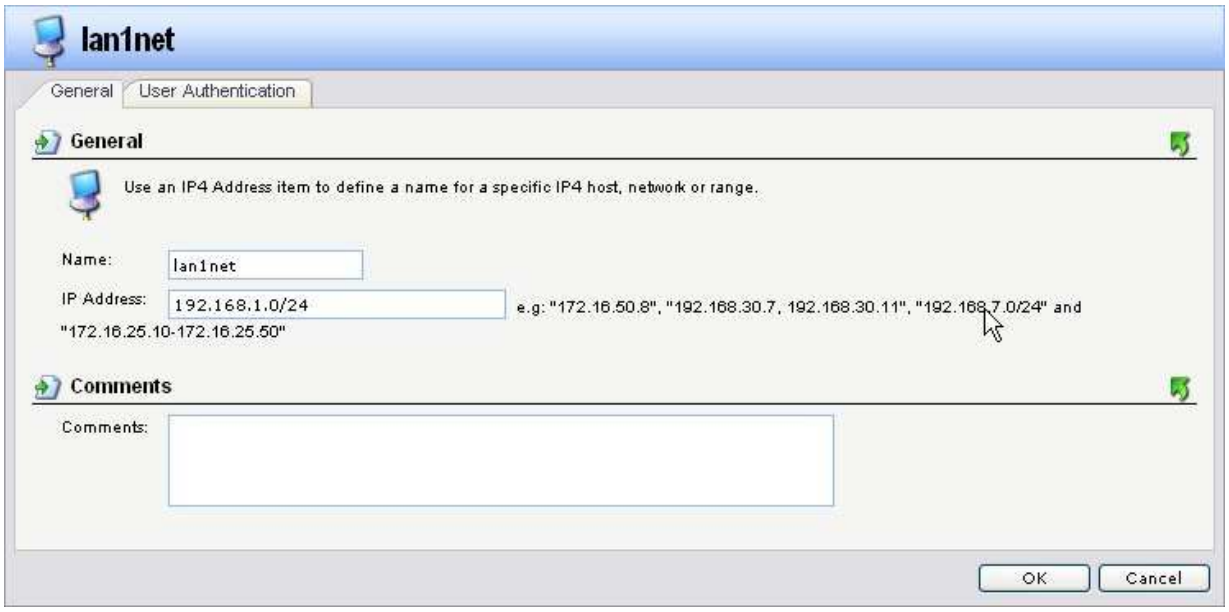
[2] Diese Einstellung finden Sie unter folgendem Menüpunkt: / Objects / Address Book / Add / IP4 Address Group /

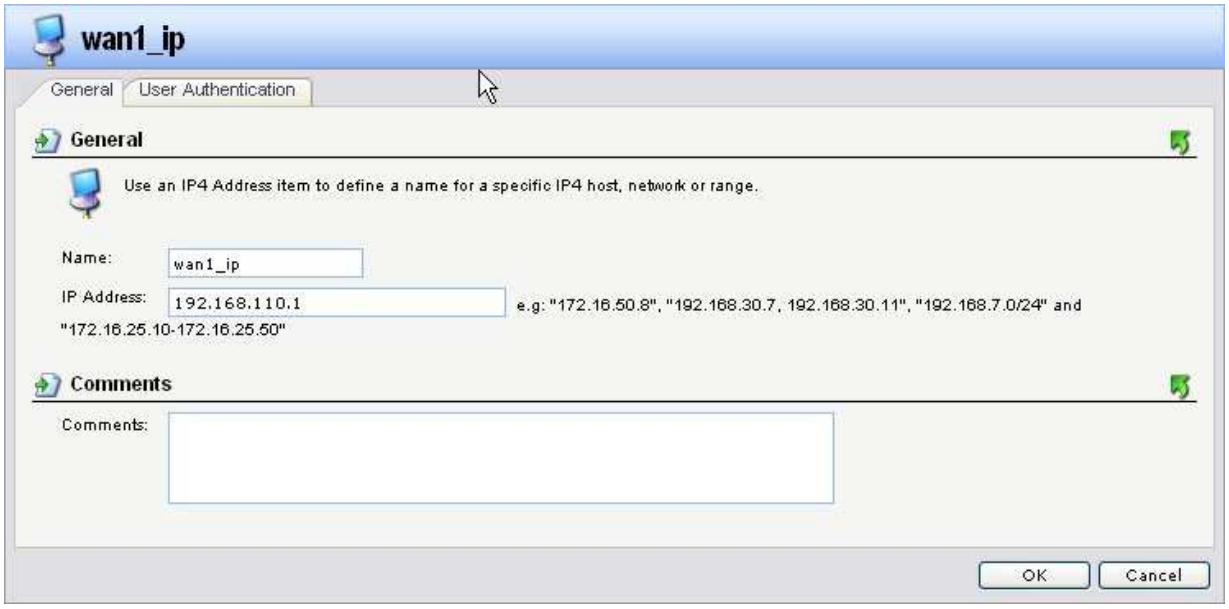
In der Übersicht sieht dies wie folgt aus:

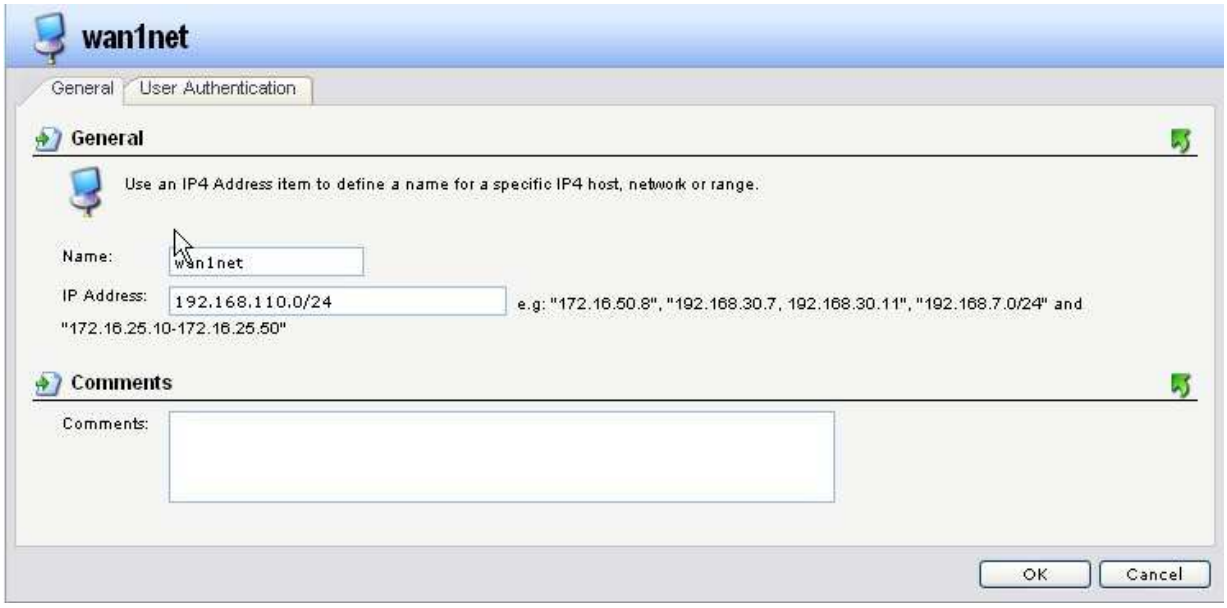
Ändern Sie nun gegebenenfalls die bestehenden Objekte für LAN und WAN Interface:[3]



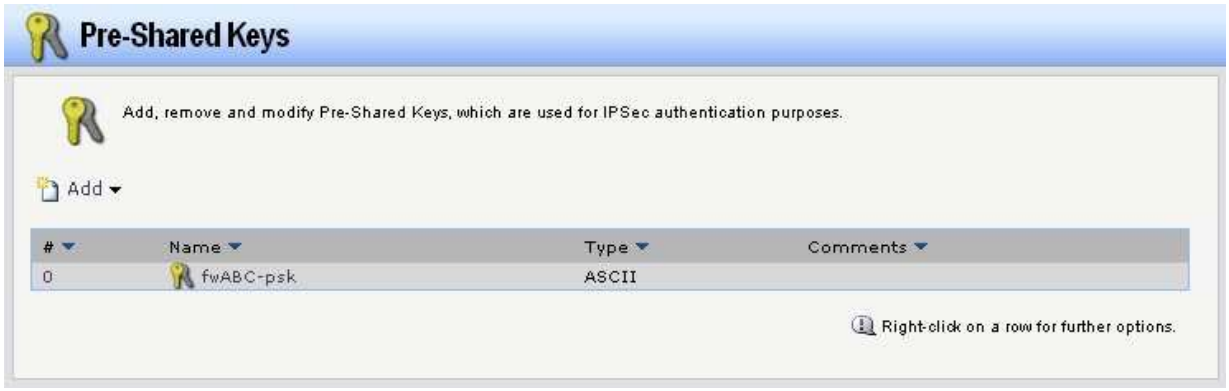
[3] Diese Einstellung finden Sie unter folgendem Menüpunkt: / Objects / Address Book /


lan1net
General
User Authentication
General
Use an IP4 Address item to define a name for a specific IP4 host, network or range.
Name:
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
General
User 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

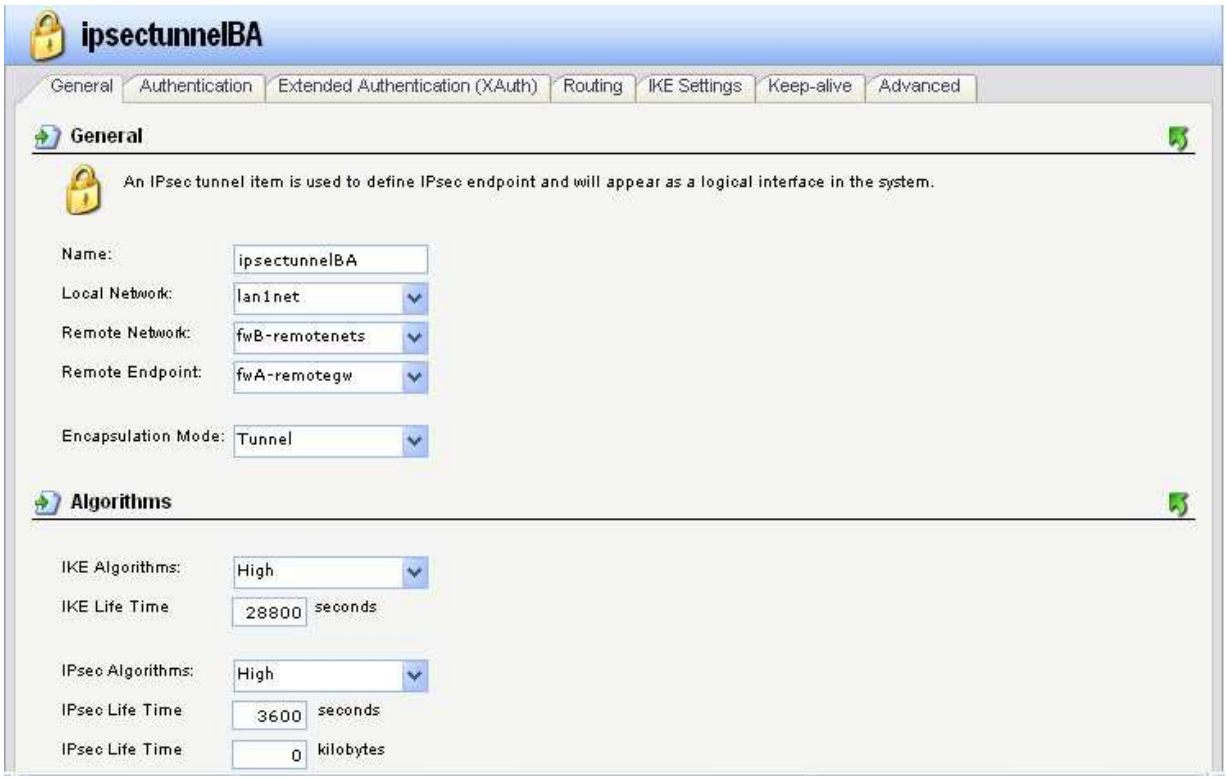


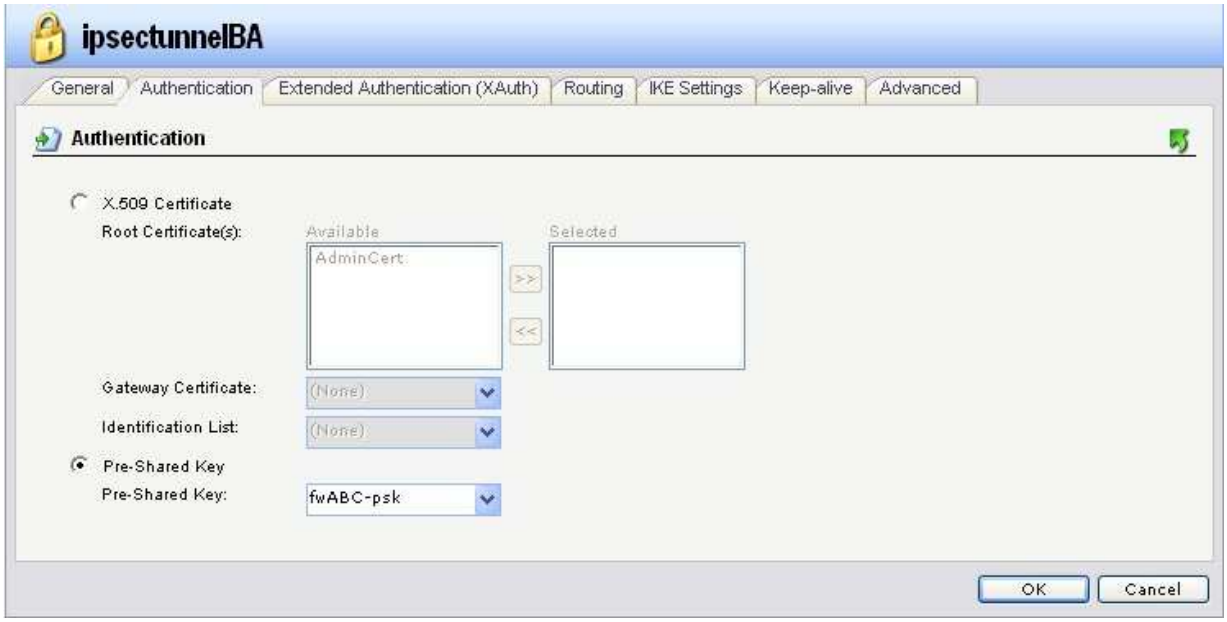
Legen Sie nun den Pre-Shared Key an: [4]



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

Legen Sie nun einen IPSec-Tunnel an: [5]

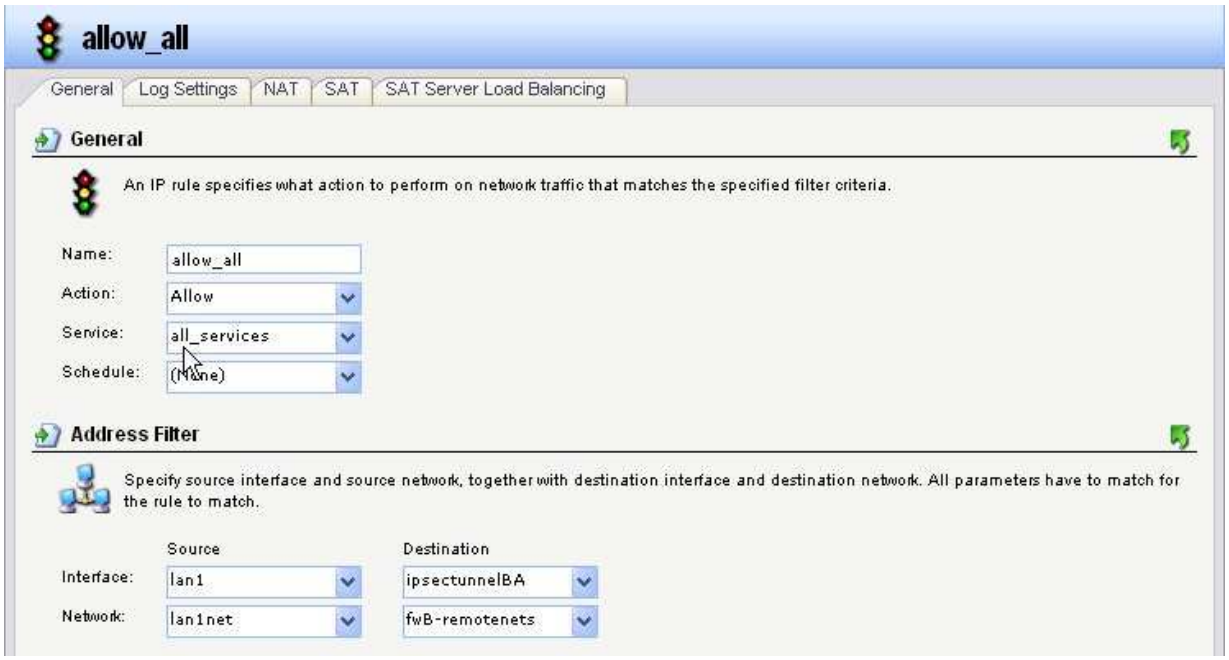




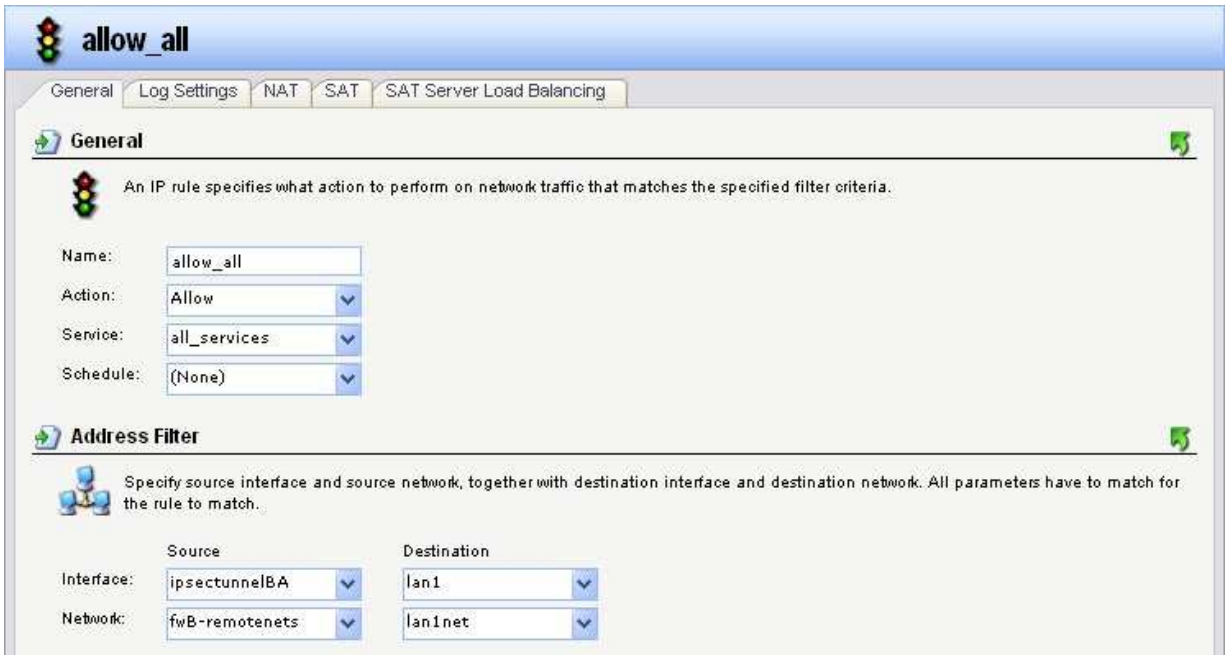
[5] Diese Einstellung finden Sie unter folgendem Menüpunkt: / Interfaces / IPSec Tunnels /

In der Übersicht sieht dies wie folgt aus:

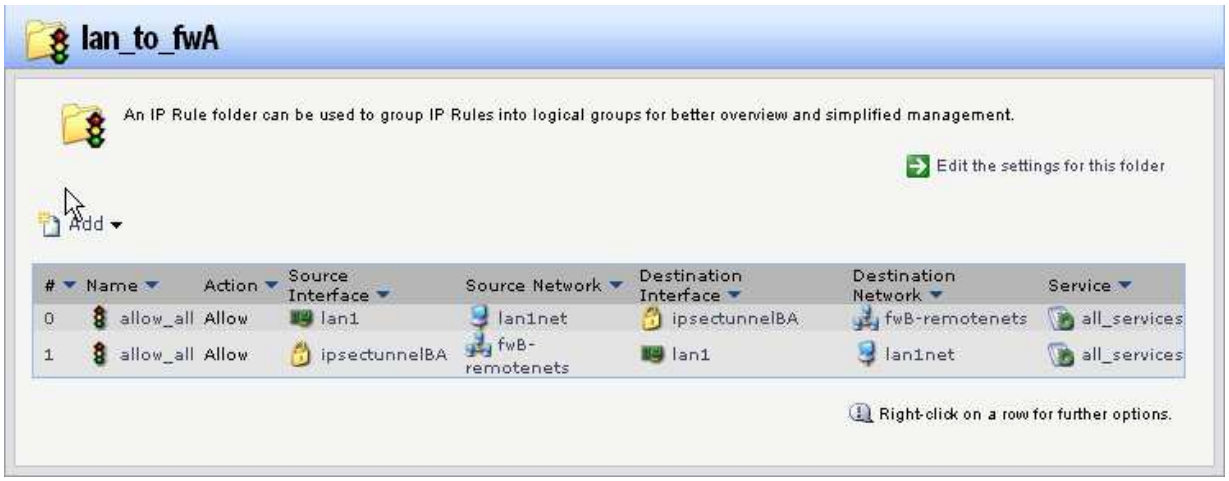
Richten Sie nun die Access-Rules ein: [6]



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

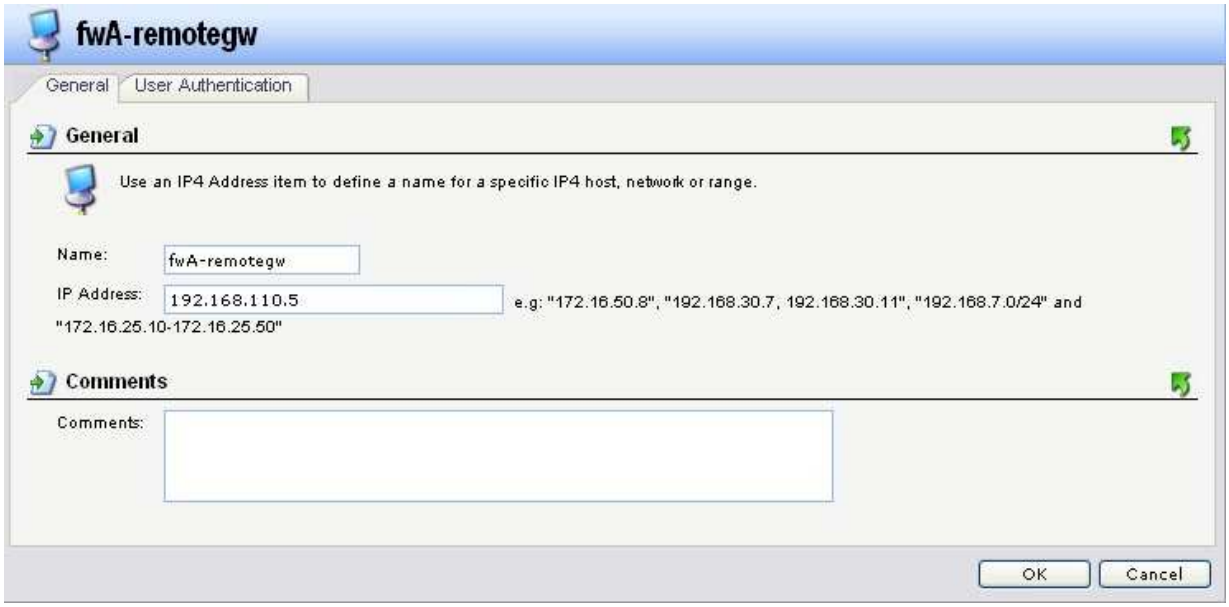


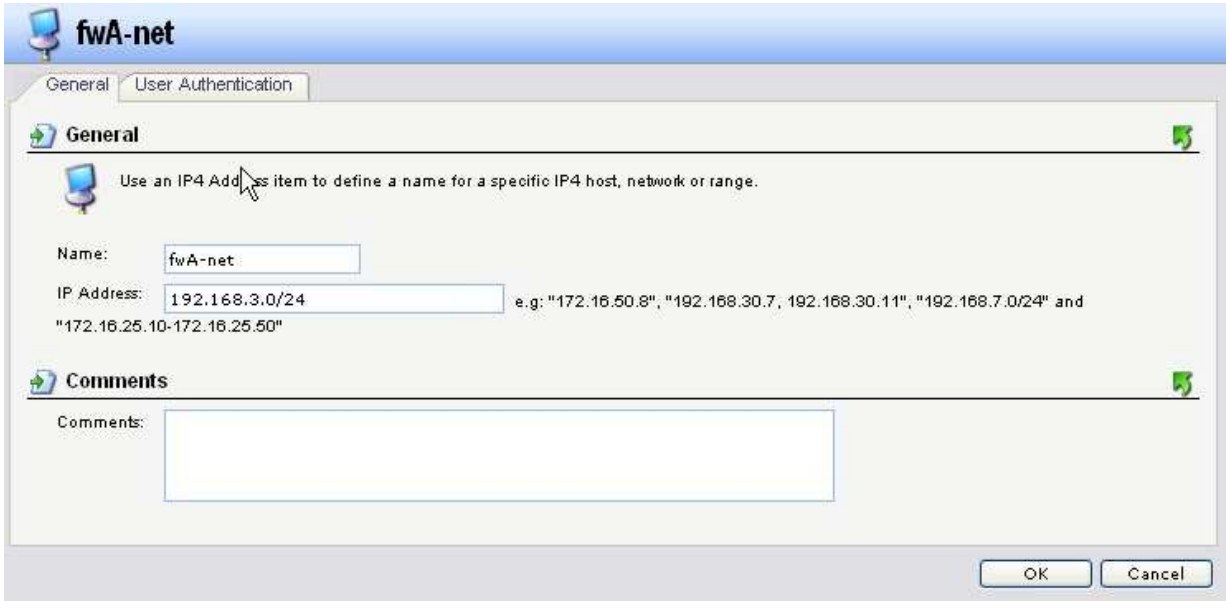
In der Übersicht sieht dies wie folgt aus:



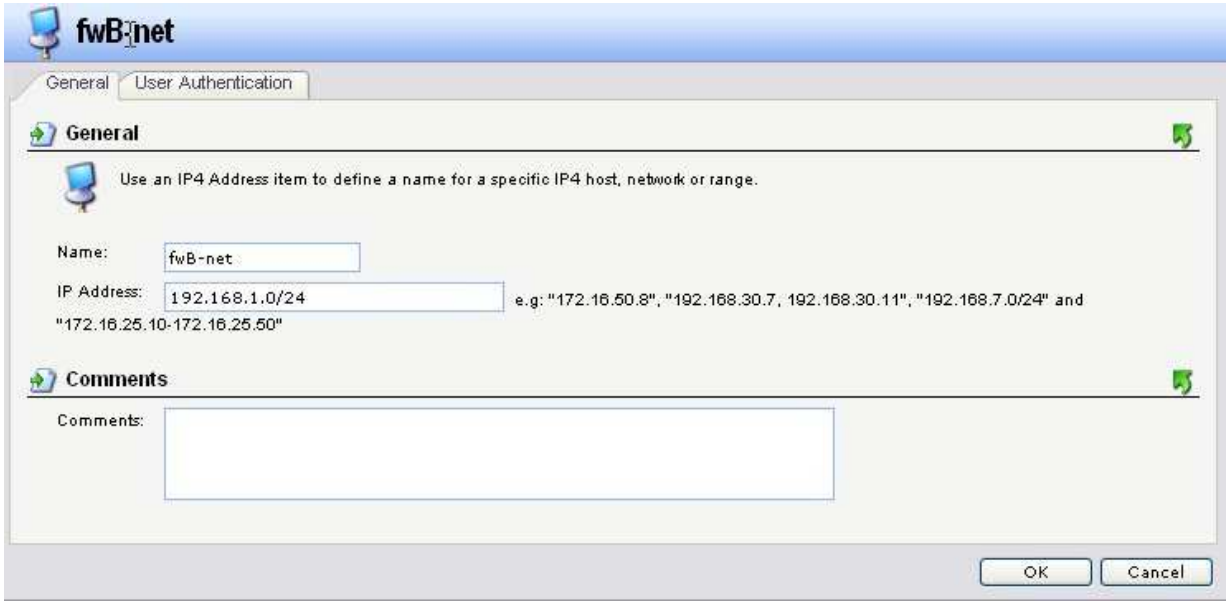
Konfiguration auf Firewall C:

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

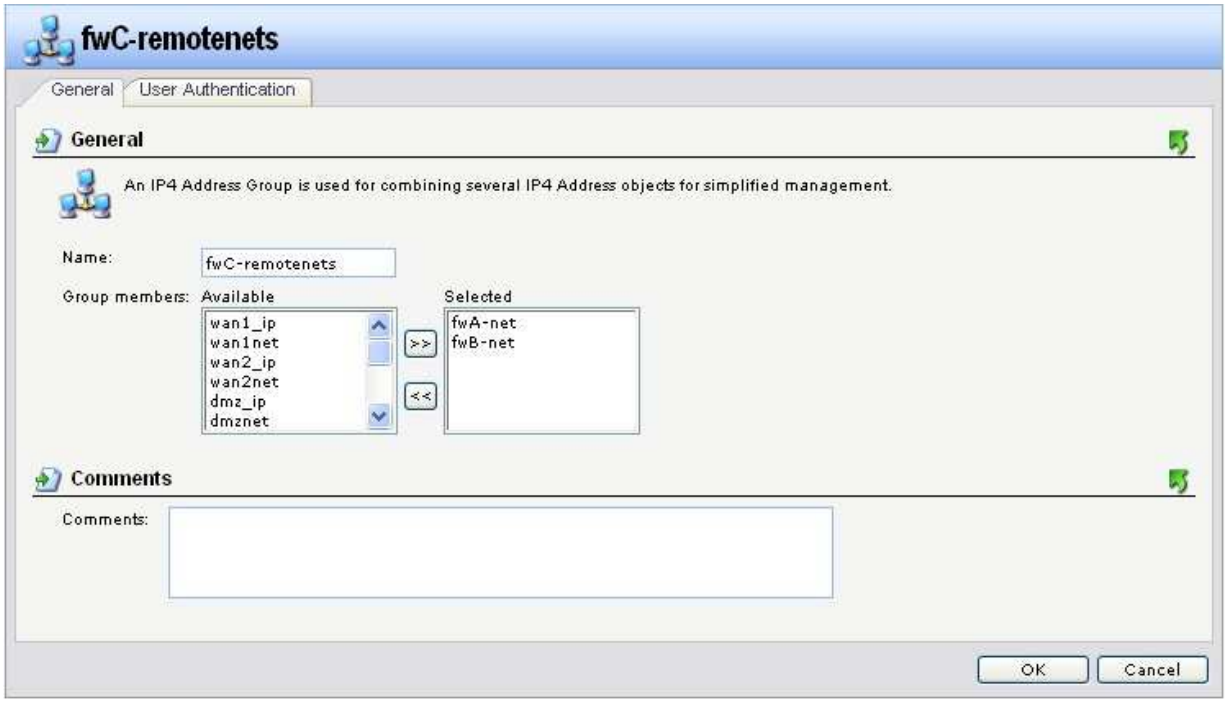




[7] Diese Einstellung finden Sie unter folgendem Menüpunkt: Objects / Address Book / Add / IP4 Host/Network /



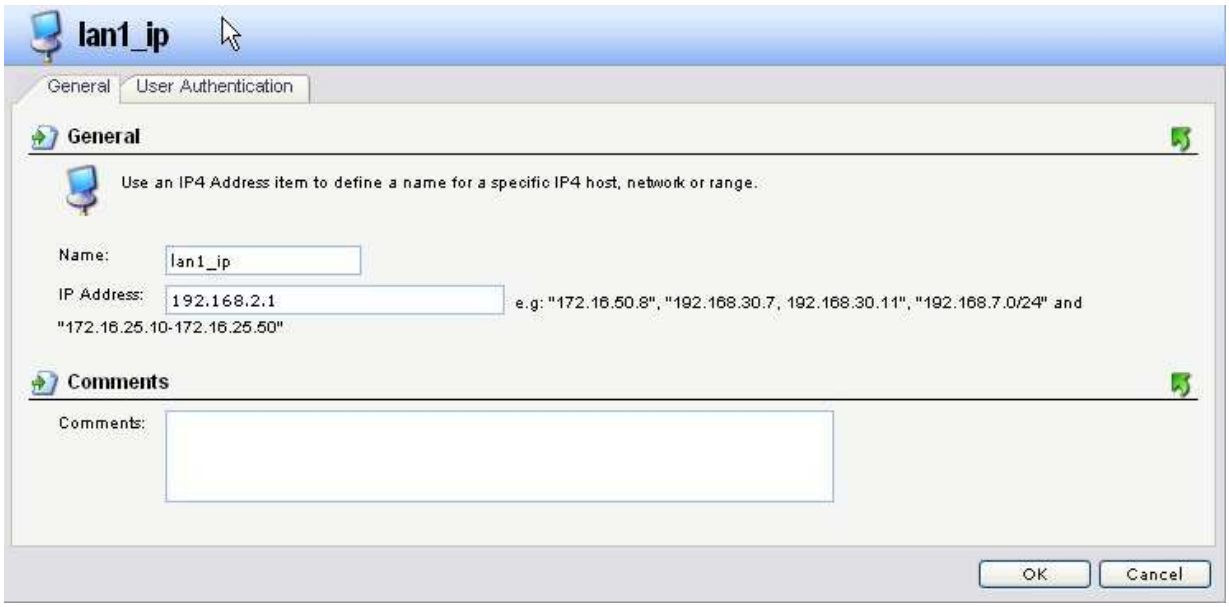
Nun muss weiterhin eine neue IP-Gruppe angelegt werden:[8]



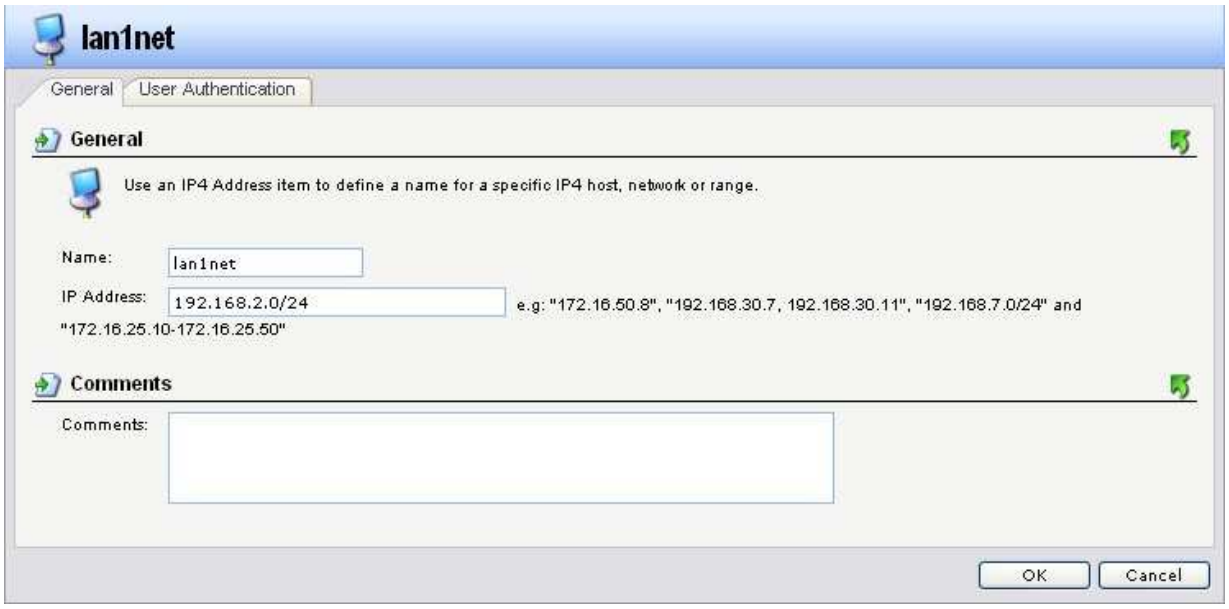
[8] Diese Einstellung finden Sie unter folgendem Menüpunkt: / Objects / Address Book / Add / IP4 Address Group /

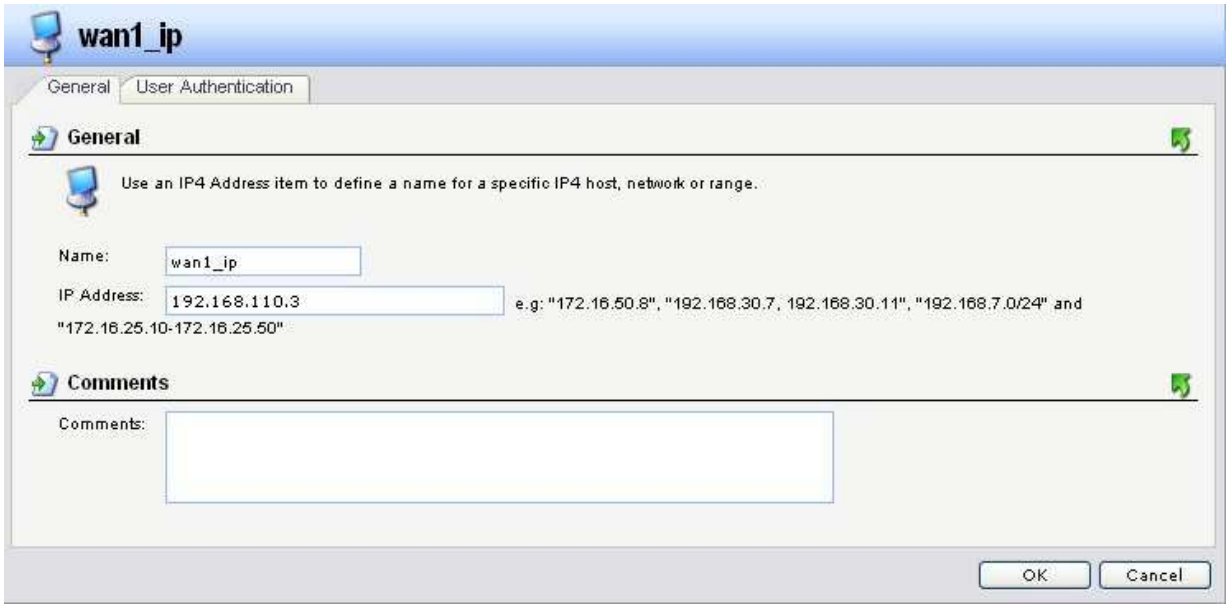
In der Übersicht sieht dies wie folgt aus:

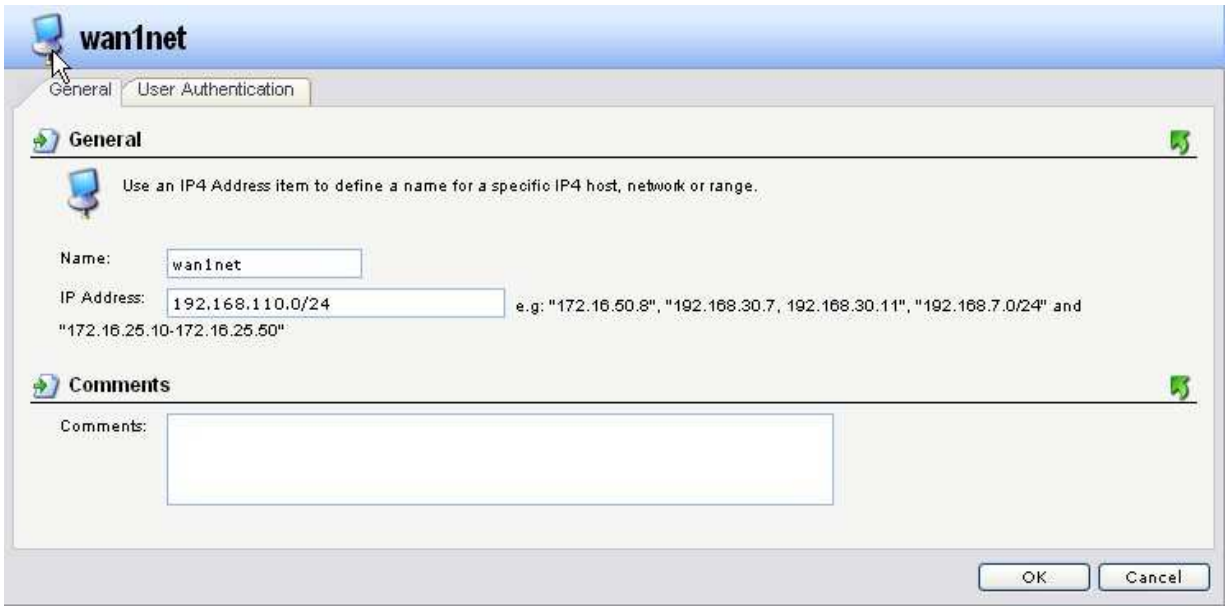
Ändern Sie nun gegebenenfalls die bestehenden Objekt für LAN und WAN Interface:[9]



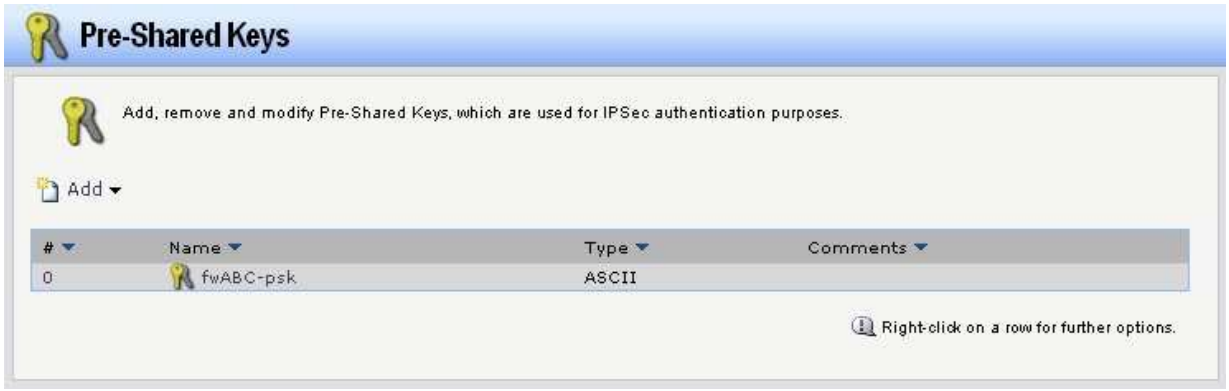
[9] Diese Einstellung finden Sie unter folgendem Menüpunkt: / Objects / Address Book /


lan1net
General
User Authentication
General
Use an IP4 Address item to define a name for a specific IP4 host, network or range.
Name:
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
General
User 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

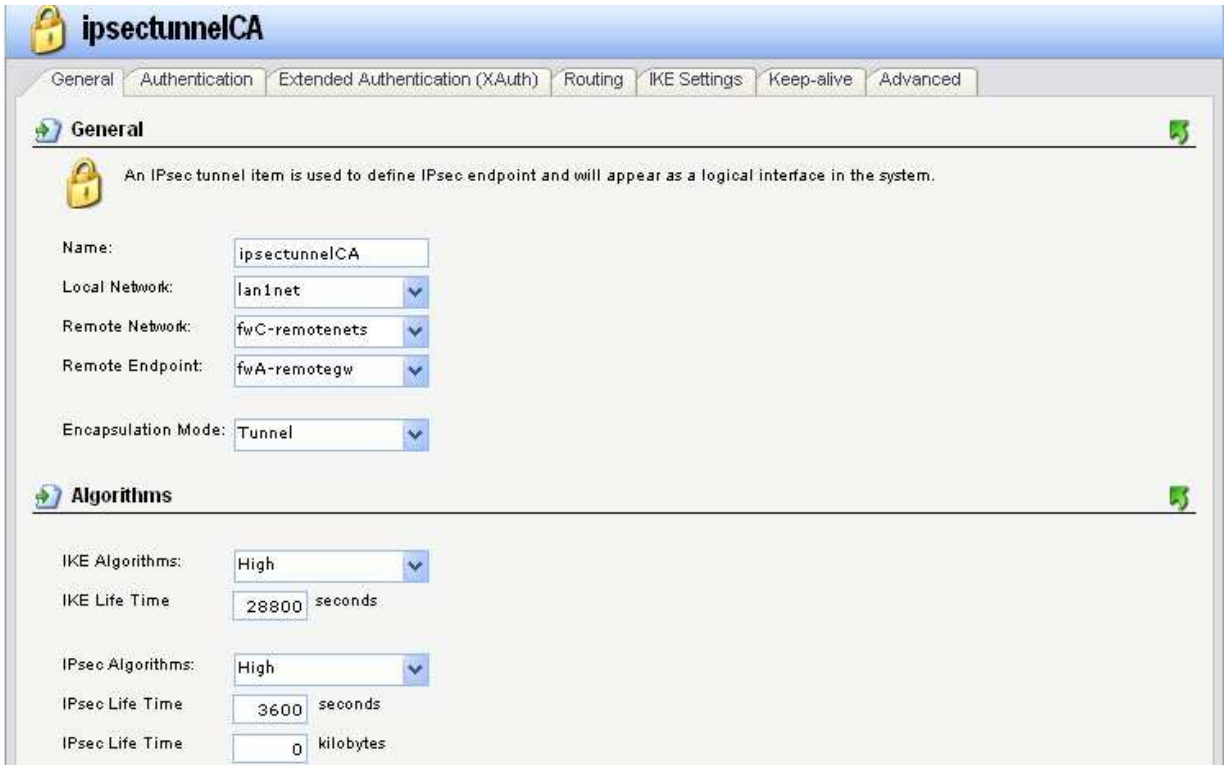


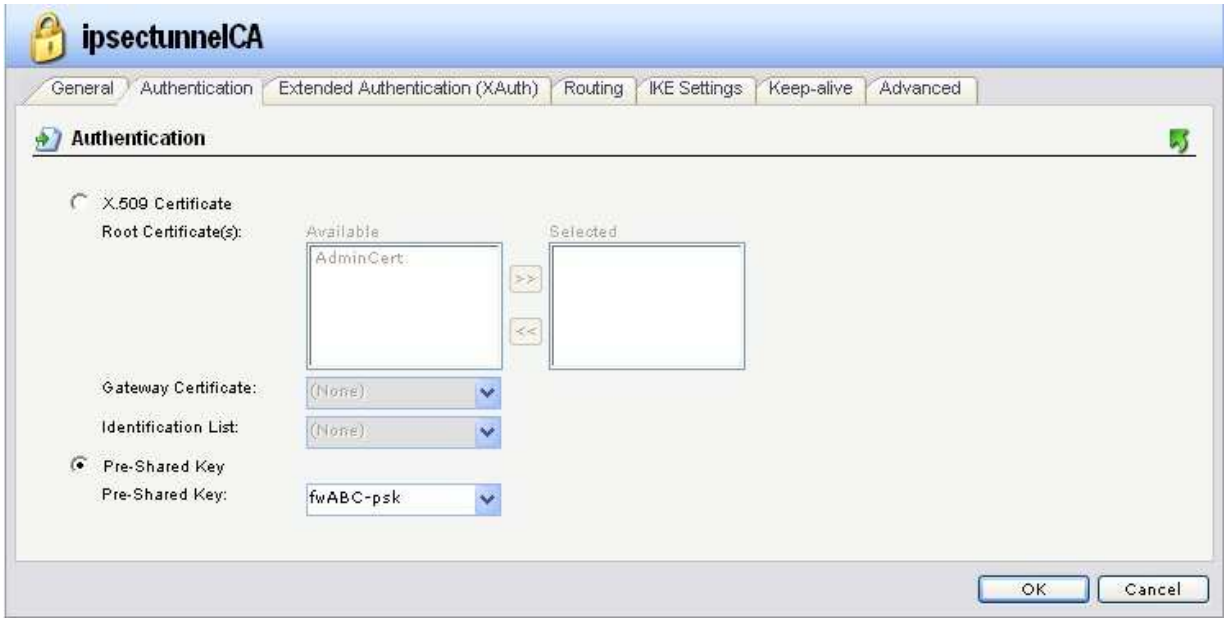
Legen Sie nun den Pre-Shared Key an: [10]



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

Legen Sie nun einen IPSec-Tunnel an: [11]

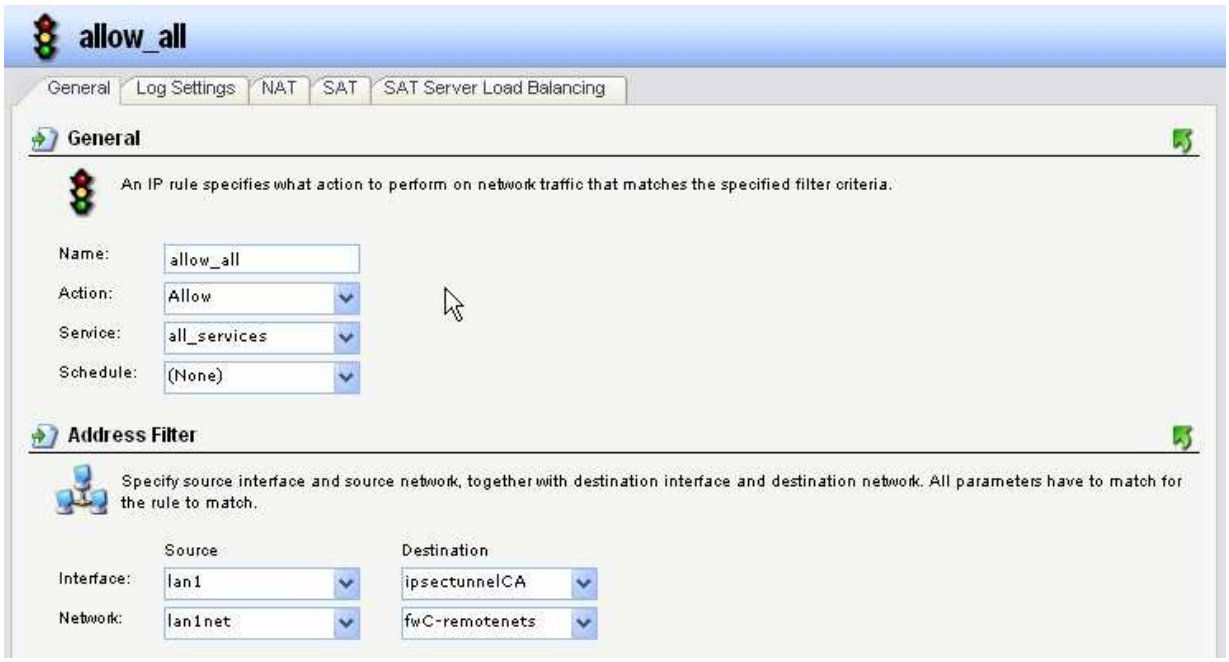




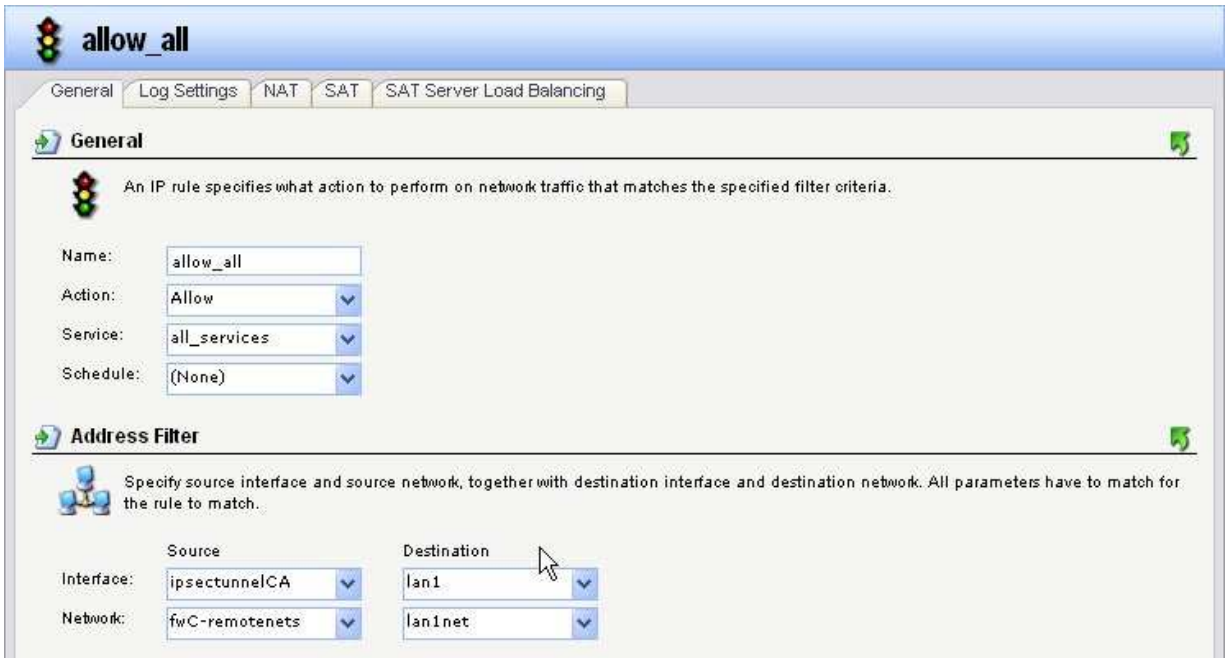
[11] Diese Einstellung finden Sie unter folgendem Menüpunkt: / Interfaces / IPSec Tunnels /

In der Übersicht sieht dies wie folgt aus:

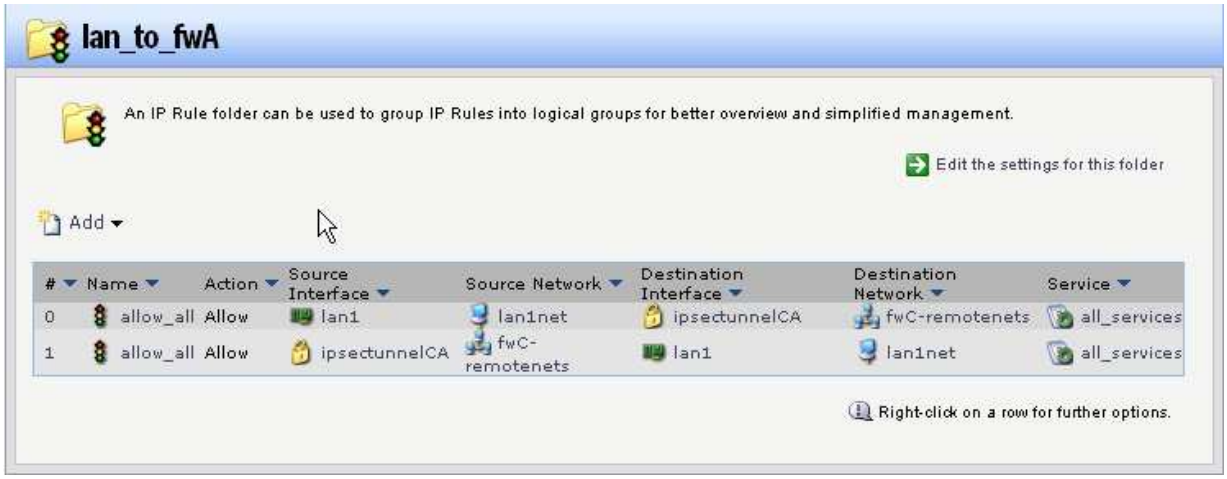
Richten Sie nun die Access-Rules ein: [12]



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

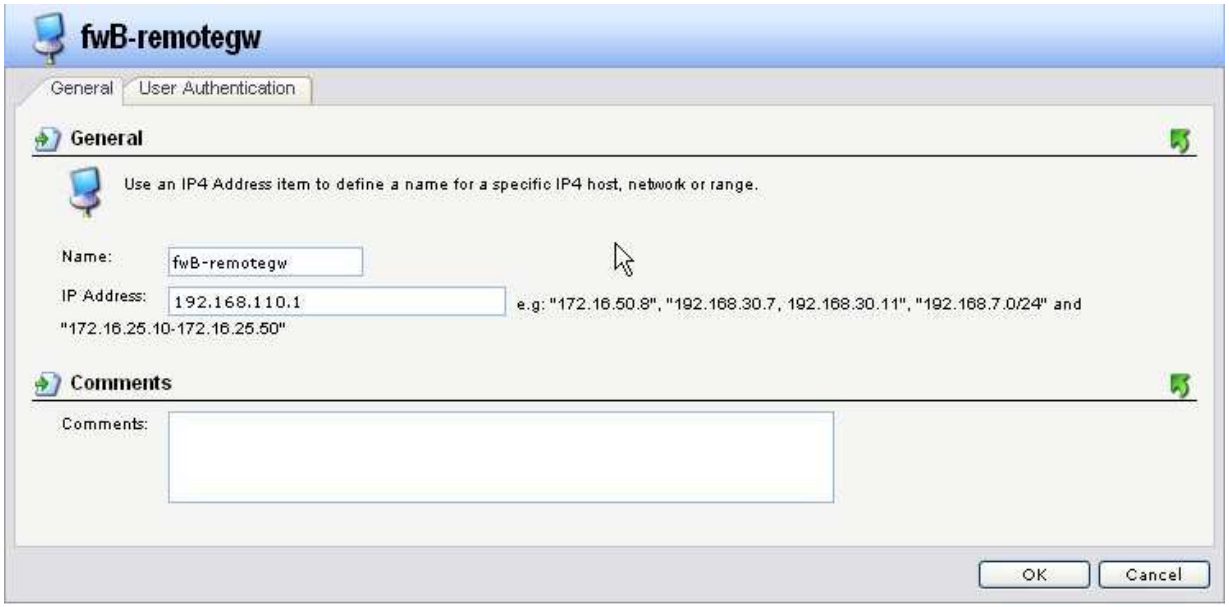


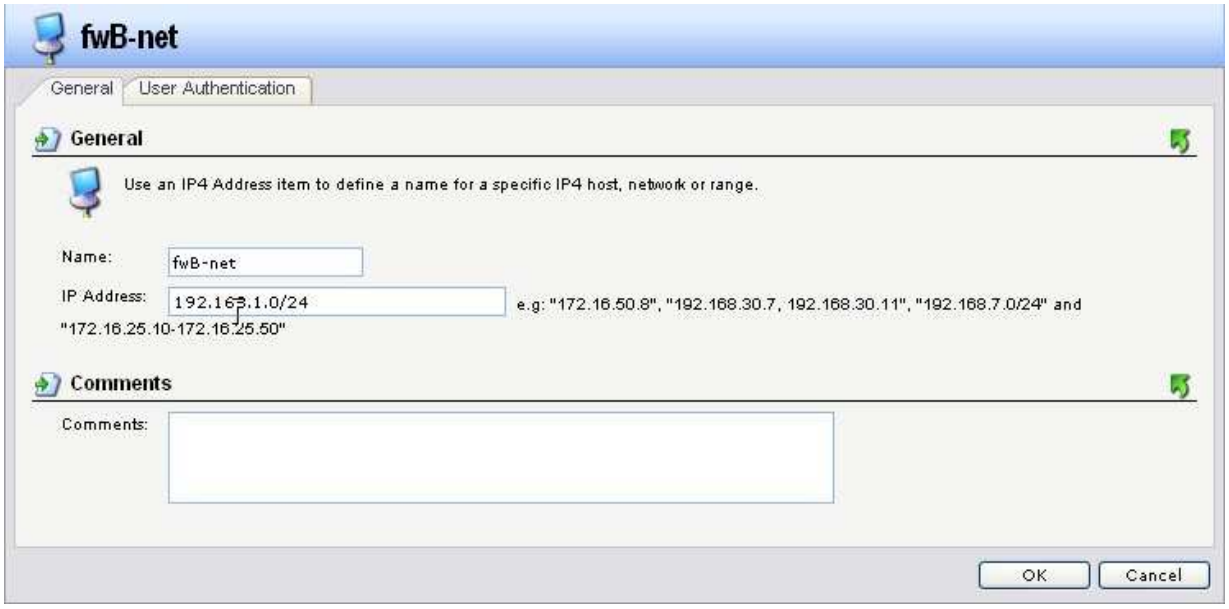
In der Übersicht sieht dies wie folgt aus:



Konfiguration auf Firewall A:

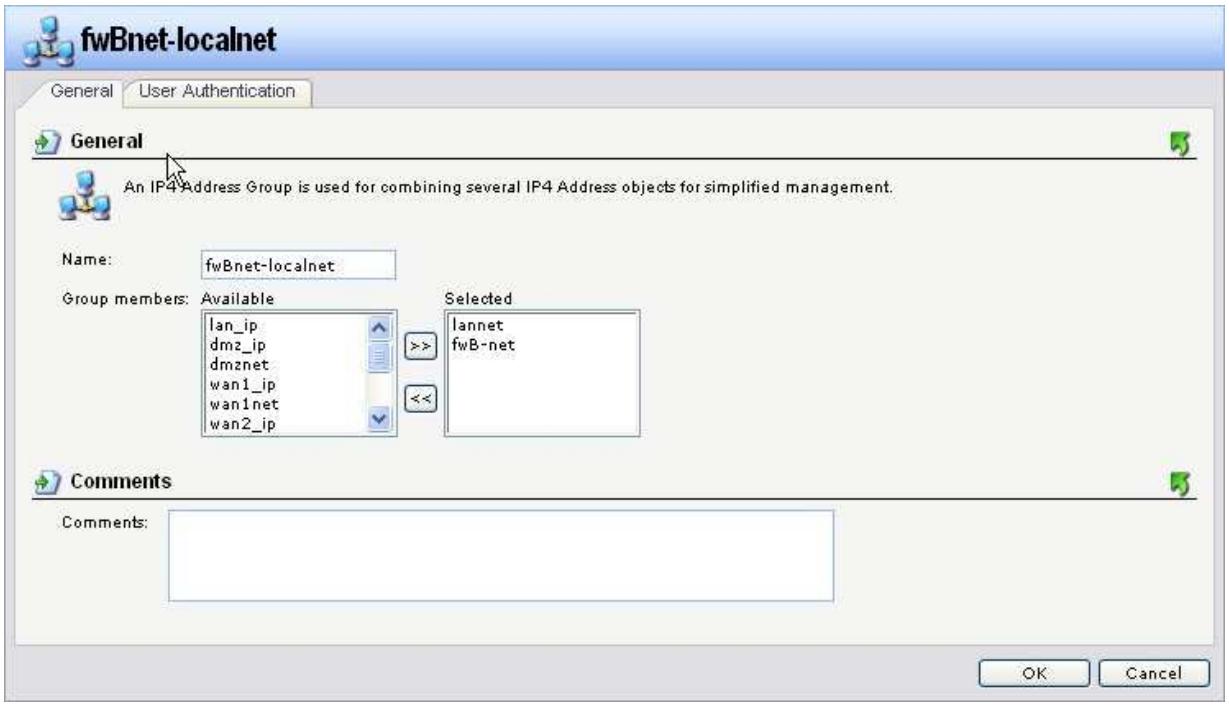
Zuerst wurden die folgenden Objekte auf Firewall A angelegt: [13]



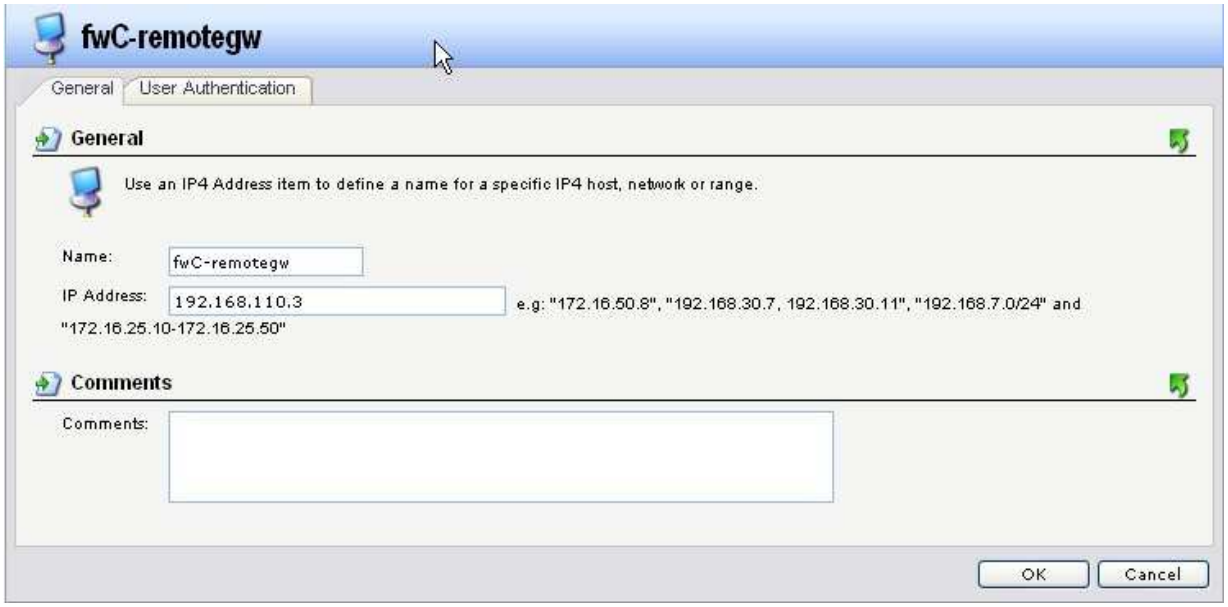


[13] Diese Einstellung finden Sie unter folgendem Menüpunkt: / Objects / Address Book / Add / IP4 Host/Network /

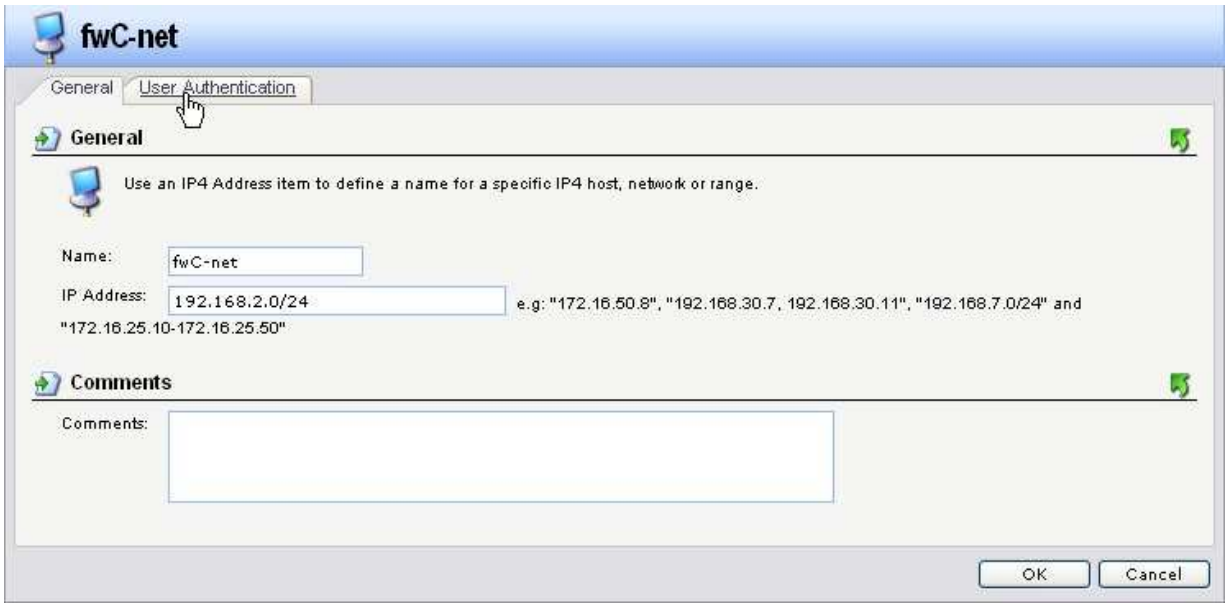
Nun muss weiterhin eine neue IP-Gruppe angelegt werden: [14]



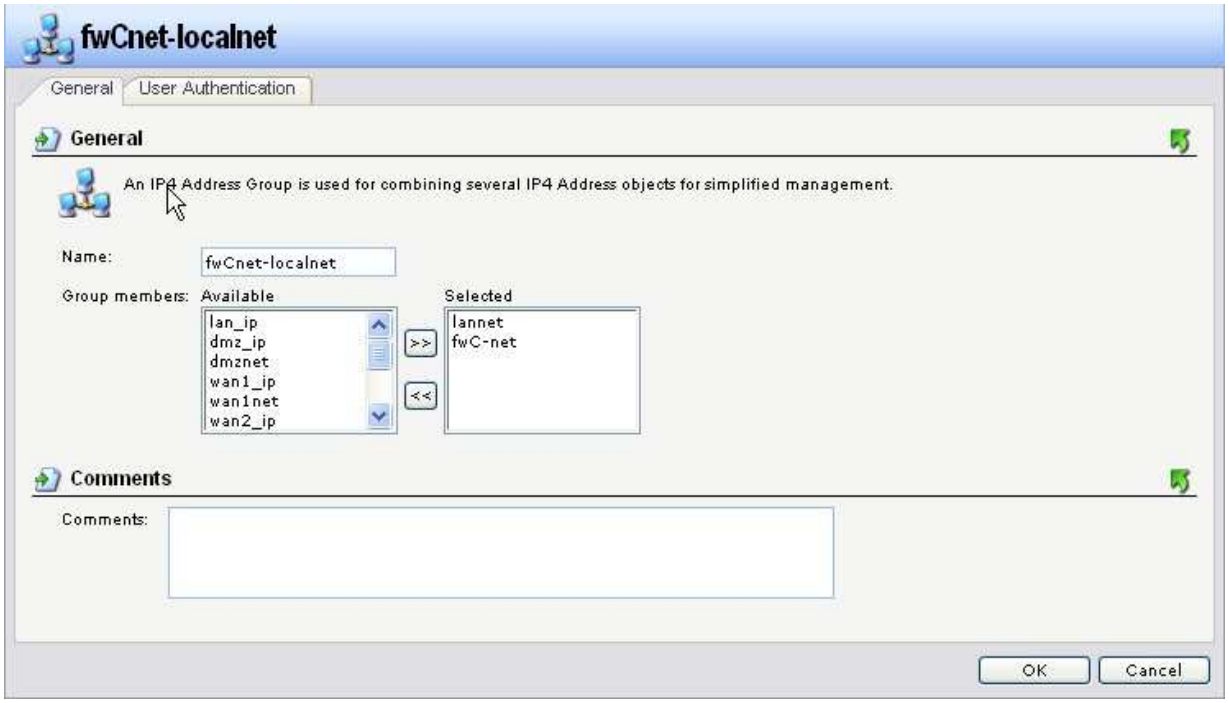
Legen Sie nun weitere Objekte an: [15]:



[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 /



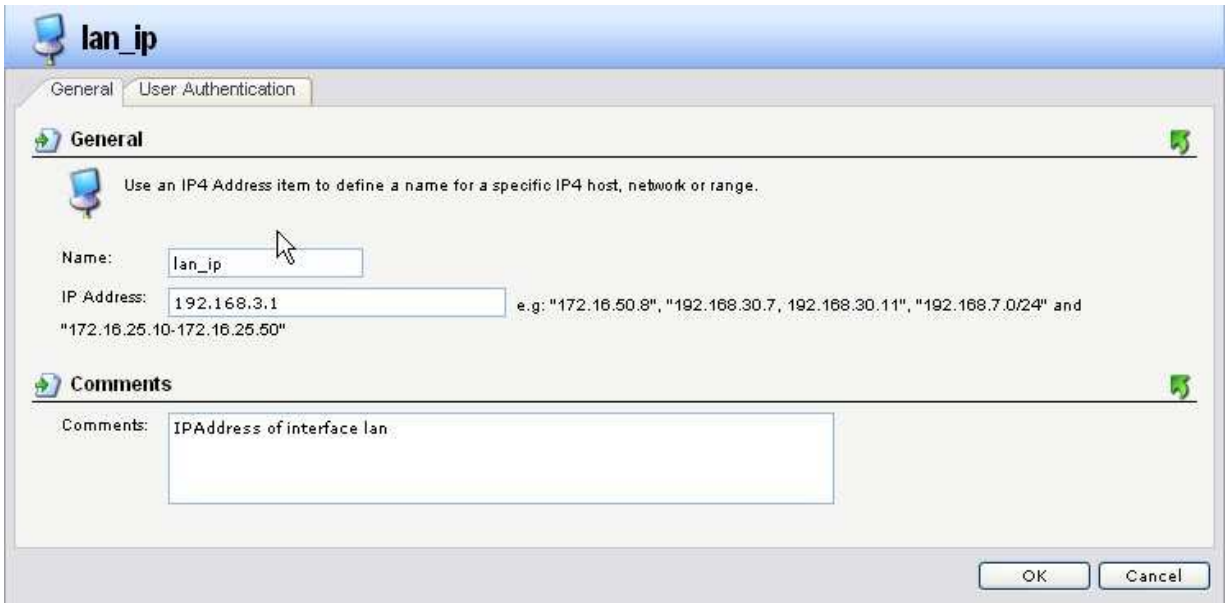
Nun muss weiterhin eine neue IP-Gruppe angelegt werden: [16]



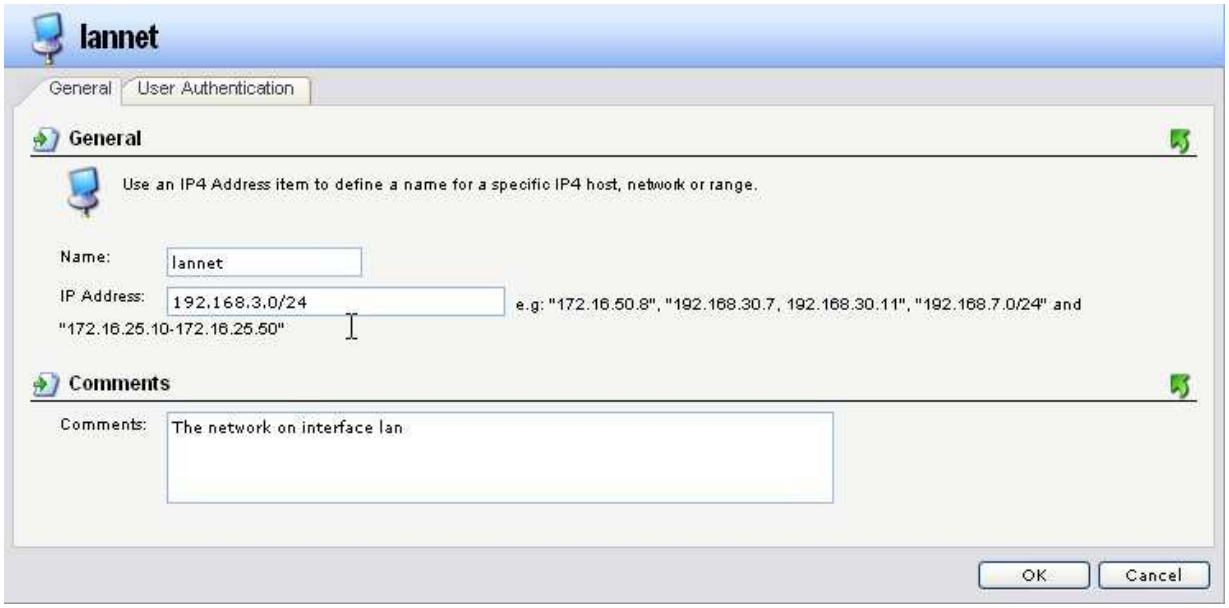
[16] Diese Einstellung finden Sie unter folgendem Menüpunkt: / Objects / Address Book / Add / IP4 Address Group /

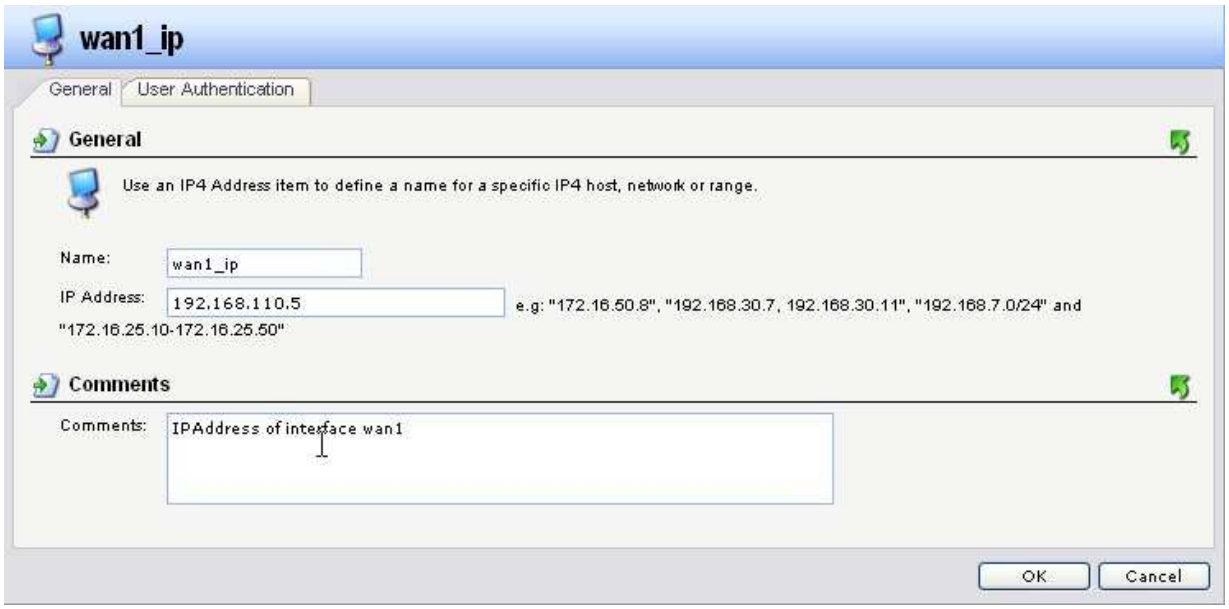
In der Übersicht sieht dies wie folgt aus:

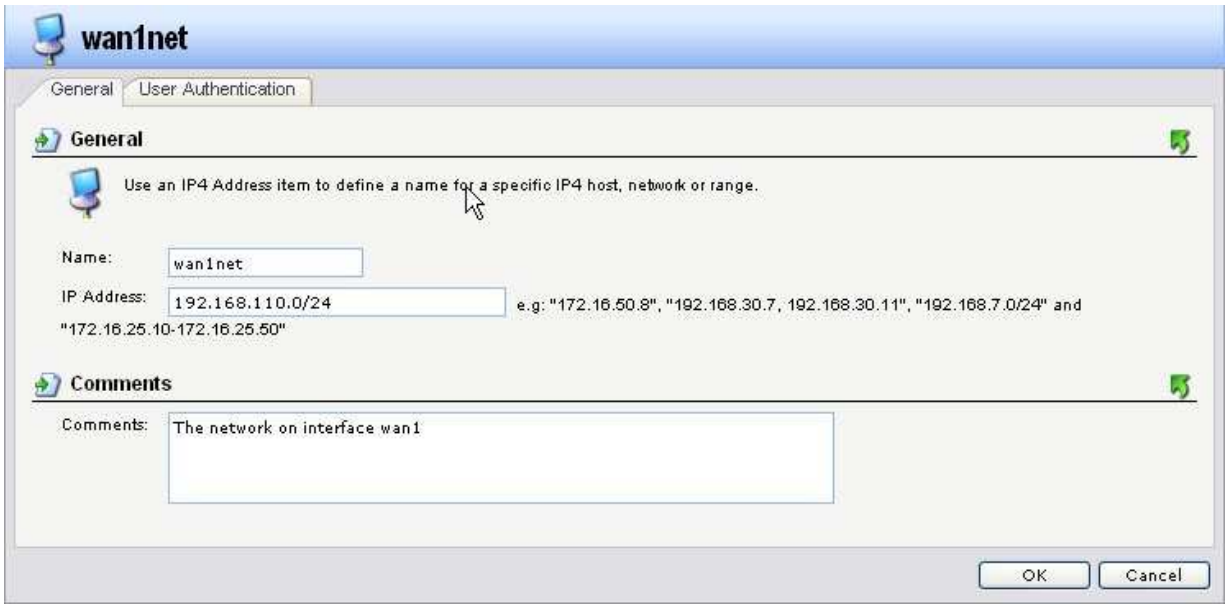
Ändern Sie nun gegebenenfalls die bestehenden Objekte für LAN und WAN Interface: [17]



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

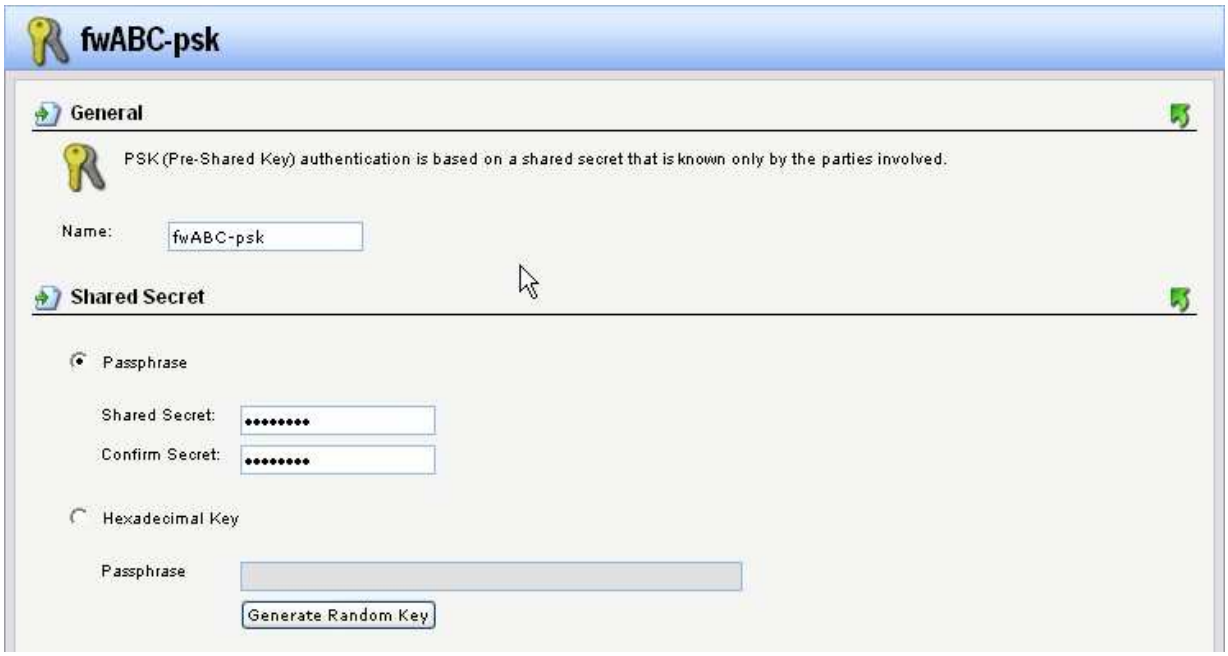

lannet
General
User Authentication
General
Use an IP4 Address item to define a name for a specific IP4 host, network or range.
Name:
lannet
IP Address:
192.168.3.0/24
e.g: "172.16.50.8", "192.168.30.7, 192.168.30.11", "192.168.7.0/24" and "172.16.25.10-172.16.25.50"
Comments
Comments:
The network on interface lan
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:
wan1_ip
IP Address:
192.168.110.5
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:
IPAddress of interface wan1
OK
Cancel

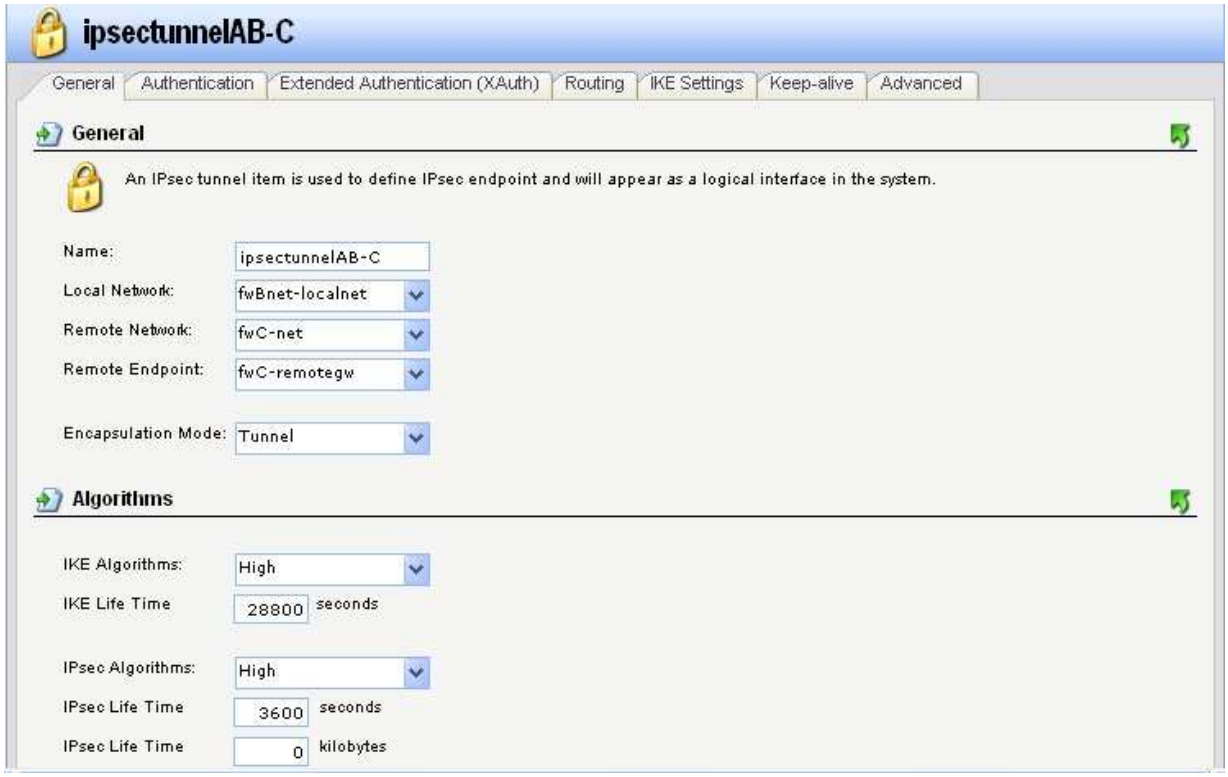


In der Übersicht sieht dies wie folgt aus:

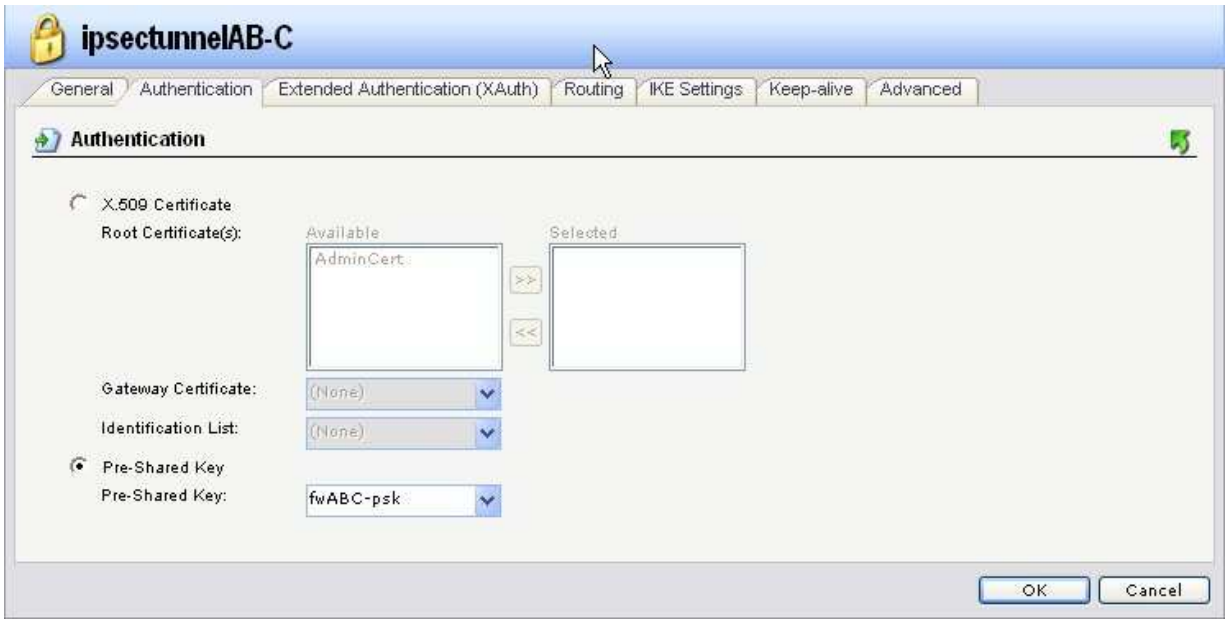
Legen Sie nun den Pre-Shared Key an: [18]

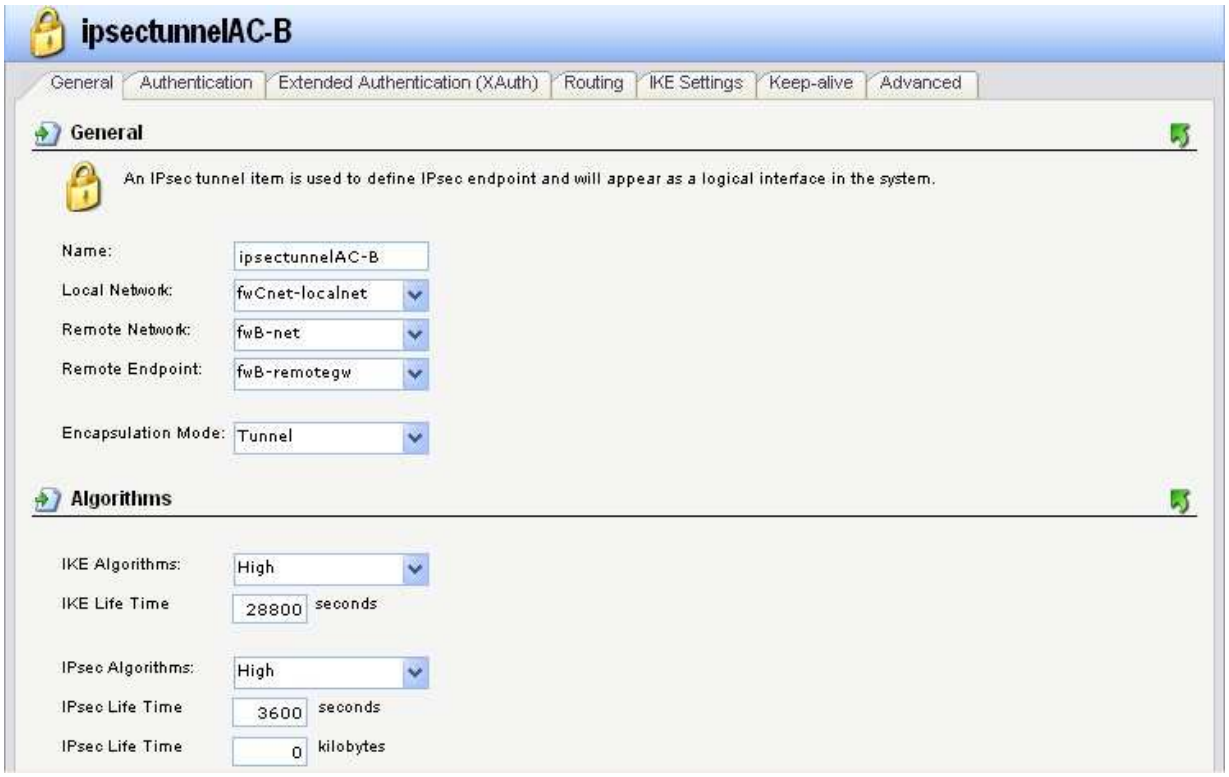


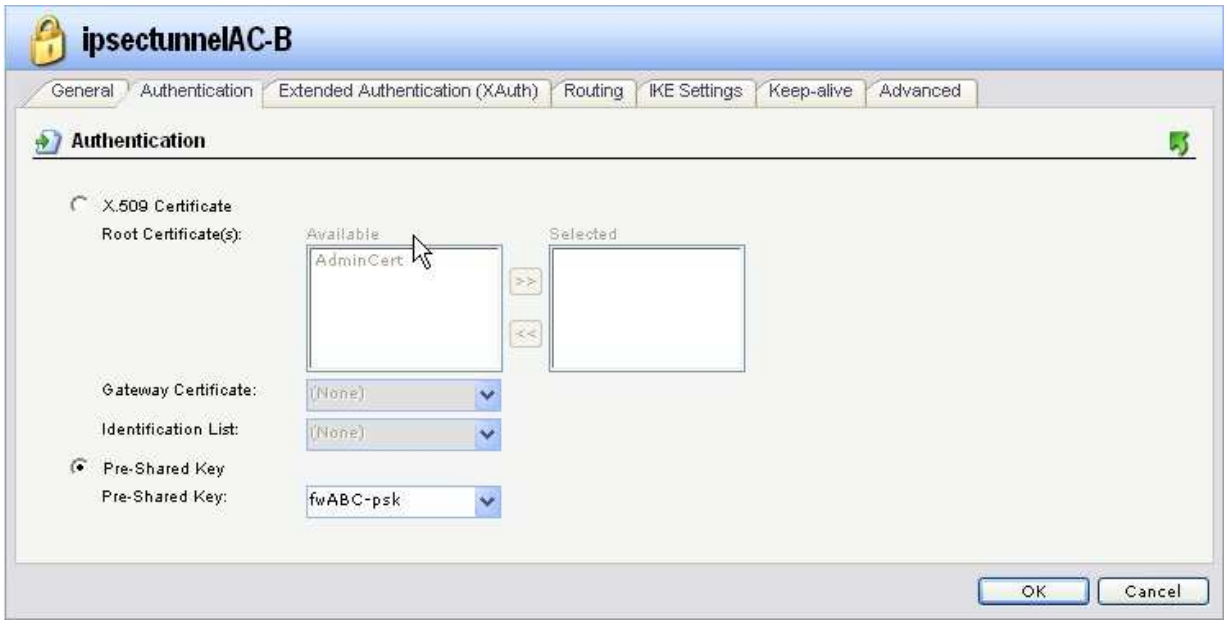
Legen Sie nun zwei IPSec Tunnel an: [19]



[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 /

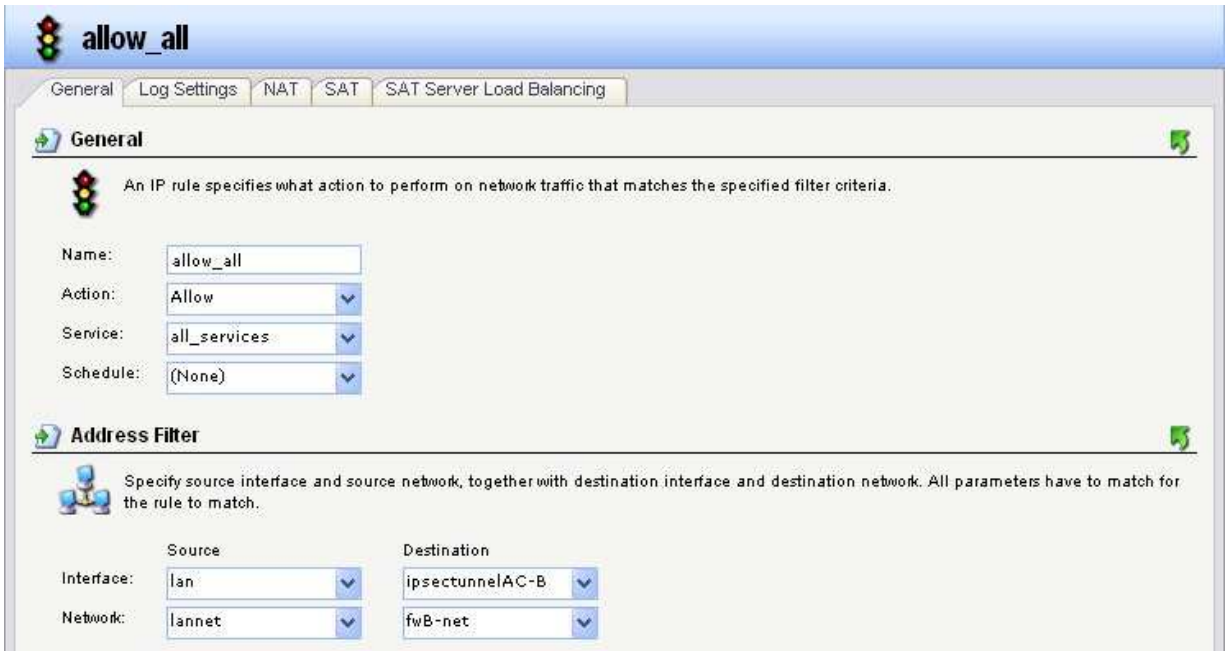

ipsectunnelAB-C
General
Authentication
Extended Authentication (XAuth)
Routing
IKE Settings
Keep-alive
Advanced
Authentication
X.509 Certificate
Root Certificate(s):
Available
Selected
AdminCert
>>
<<
Gateway Certificate:
(None)
Identification List:
(None)
Pre-Shared Key
Pre-Shared Key:
fwABC-psk
OK
Cancel

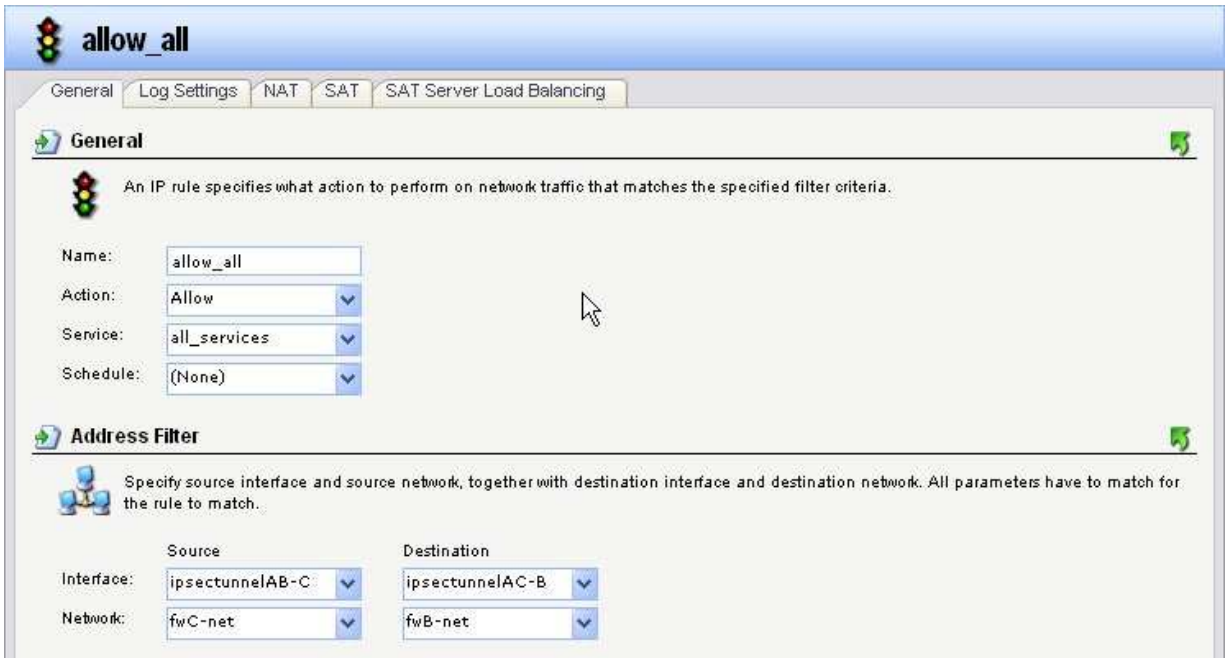

ipsectunnelAC-B
General
Authentication
Extended Authentication (XAuth)
Routing
IKE Settings
Keep-alive
Advanced
General
An IPsec tunnel item is used to define IPsec endpoint and will appear as a logical interface in the system.
Name:
ipsectunnelAC-B
Local Network:
fwCnet-localnet
Remote Network:
fwB-net
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



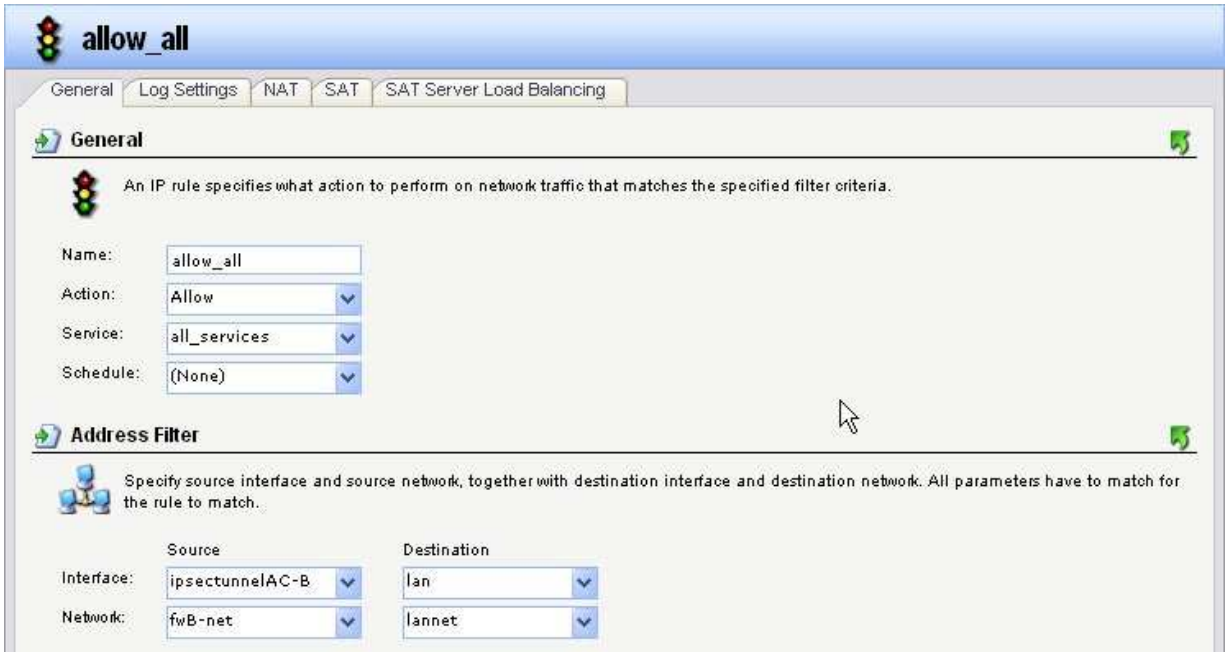
In der Übersicht sieht dies wie folgt aus:

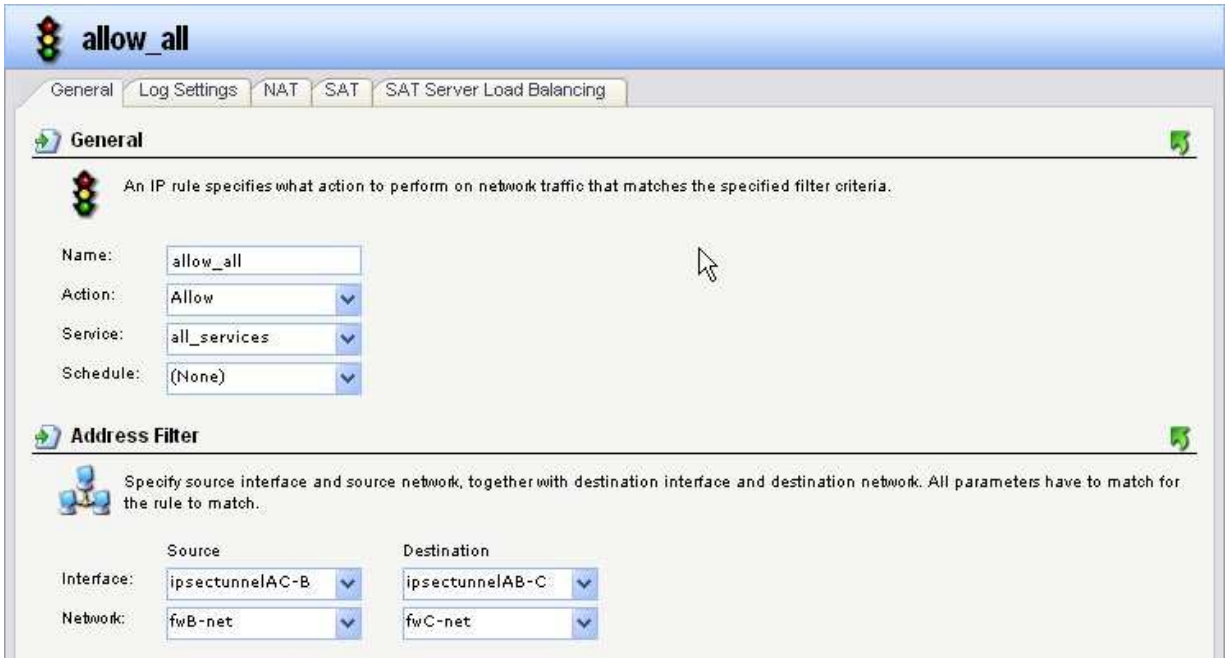
Richten Sie nun die Access-Rules ein: [20]

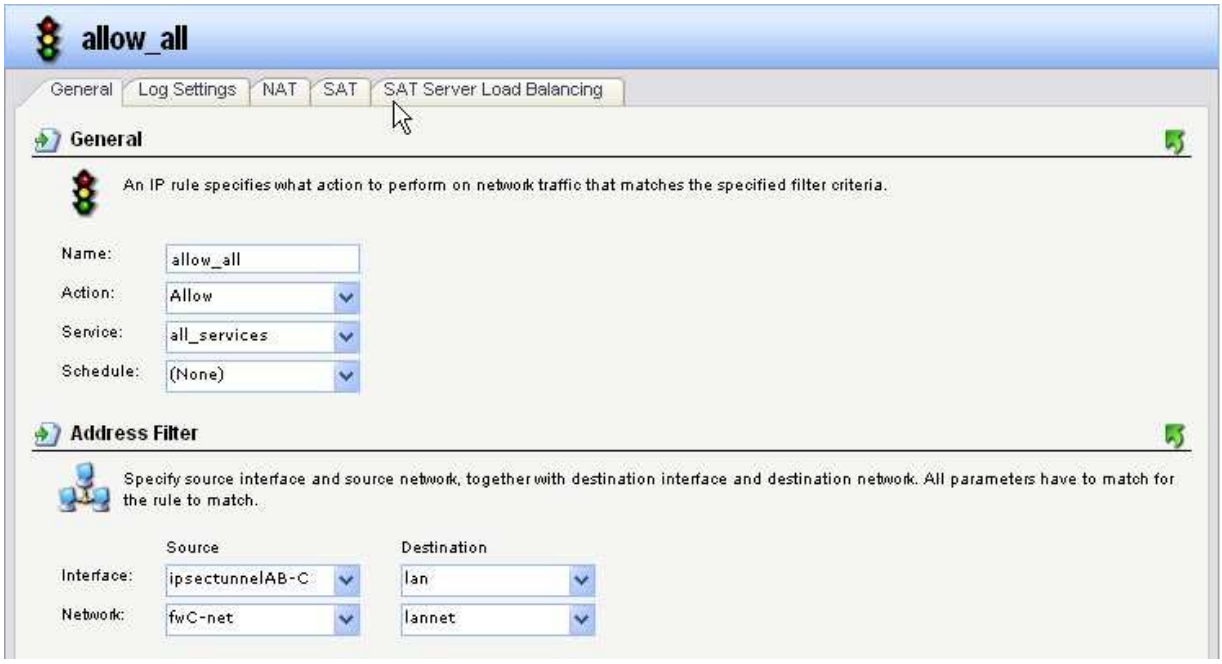


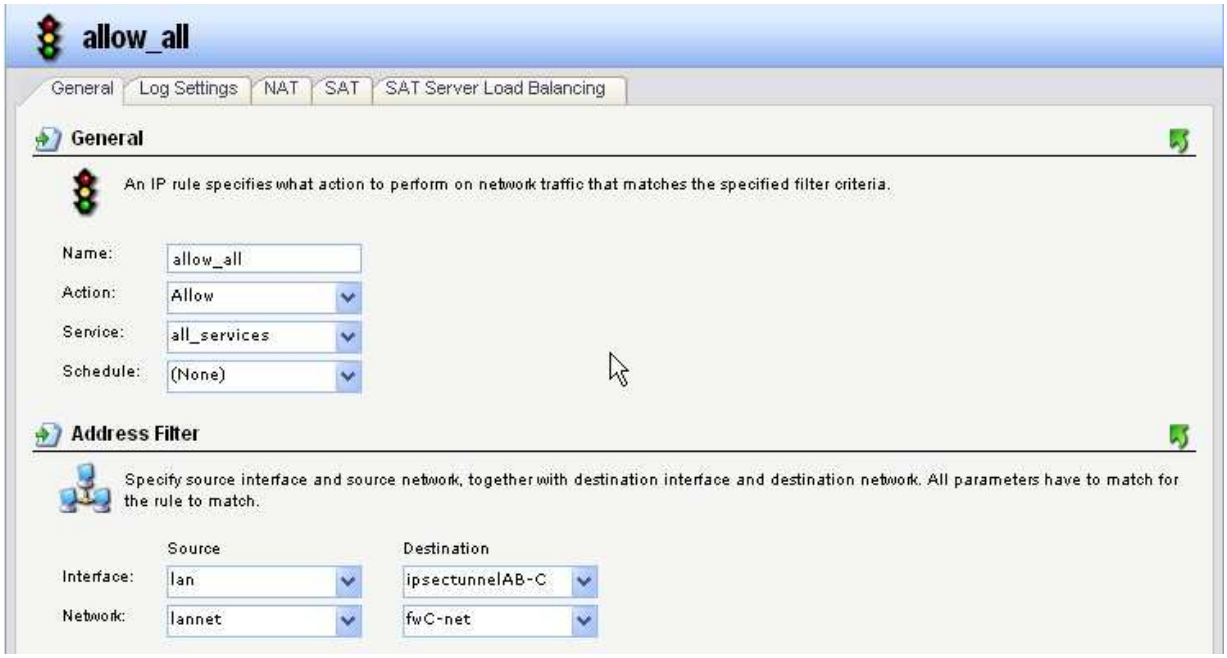


[20] Diese Einstellung finden Sie unter folgendem Menüpunkt: / Rules / IP Rules /

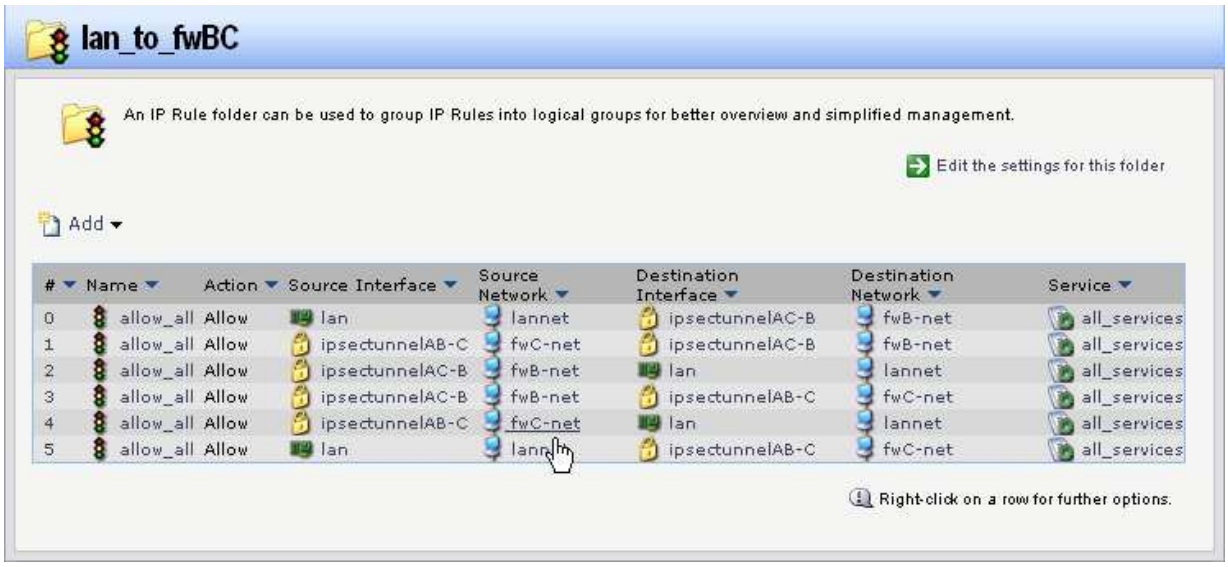

allow_all
General
Log Settings
NAT
SAT
SAT Server Load Balancing
General
An IP rule specifies what action to perform on network traffic that matches the specified filter criteria.
Name:
allow_all
Action:
Allow
Service:
all_services
Schedule:
(None)
Address Filter
Specify source interface and source network, together with destination interface and destination network. All parameters have to match for the rule to match.
Source
Destination
Interface:
ipsectunnelAC-B
lan
Network:
fwB-net
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:
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
Destination
Interface:
ipsectunnelAC-B
ipsectunnelAB-C
Network:
fwB-net
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:
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
Destination
Interface:
ipsectunnelAB-C
lan
Network:
fwC-net
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:
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
Destination
Interface:
lan
ipsectunnelAB-C
Network:
lannet
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.