HIOB Messenger Kochbuch

HIOB Messenger Kochbuch

Inhaltsverzeichnis

1.Kochbuch....1
1.1. Firewall absichern und administrierbar machen 2
1.1.1.Skizze....2
1.1.2.Konfigurationsziel....3
1.1.3.Objekte....3
1.1.4.Regeln....4
1.1.5.Download....5
1.2. NAT-Gateway und Internet-Zugriff: http, https, pop3, imap 5
1.2.1.Skizze....5
1.2.2.Konfigurationsziel....6
1.2.3.Objekte....6
1.2.4.Regeln....6
1.2.5.Download....7
1.3. FTP über 'ftp-proxy' 7
1.3.1.Skizze....7
1.3.2.Konfigurationsziel....8
1.3.3.Objekte....8
1.3.4.Regeln....8
1.3.5.Download....9
1.4. DMZ mit Web- und Mailserver 9
1.4.1.Skizze....10
1.4.2.Konfigurationsziel....10
1.4.3.Objekte....10
1.4.4.Regeln....11
1.4.5.Download....12
1.5. VPN-Tunnel zwischen 'roaming client' und Intranet 12
1.5.1.Skizze....13
1.5.2.Konfigurationsziel....14
1.5.3.Objekte....14
1.5.4.Regeln....15
1.5.5.Download....16
1.6. VPN-Tunnel zwischen 2 Netzen 16
1.6.1.Skizze....17
1.6.2.Konfigurationsziel....17
1.6.3.Objekte....17
1.6.4.Regeln....18
1.6.5.Download....19
1.7. Firewall-Redundanz (carp + pfsync) 19
1.7.1.Skizze....19
1.7.2.Konfigurationsziel....20
1.7.3.Objekte....20
1.7.4.Regeln....26
1.7.5.Download....27
1.8. NAT vor dem VPN-Tunnel 27
1.8.1.Skizze....27
1.8.2.Konfigurationsziel....28
1.8.3.Objekte....28
1.8.4.Regeln....35
1.8.5.Download....37

Kapitel 1. Kochbuch

Sie haben Ihr HIOB Gateway angeschlossen und auf einem Rechner HIOB MP installiert. Was müssen Sie nun tun, um Ihre Netzwerk-Konfiguration über HIOB MP abzubilden und abzusichern?

Dieses 'Kochbuch' enthält Rezepte zur Erstellung von Firewall/VPN-Konfigurationen für häufig zu findende Netzwerk-Szenarien. Es soll Ihnen dabei helfen, Ihre Netzwerk-Konfiguration über HIOB MP abzubilden und abzusichern. Die einzelnen Konfigurationen bauen teilweise aufeinander auf. Sie können in Form von Policy-Dateien hier [../download/index.html] heruntergeladen, in ein Policy-Verzeichnis kopiert und dann mit *HIOB MP* bearbeitet werden.

Benennung der Policy-Dateien

Die bereitgestellten Policy-Dateien haben die Dateinamen `rezept-1.xml` bis `rezept-8.xml`. Wenn Sie eine Datei heruntergeladen haben, benennen Sie diese bitte um. HIOB MP benutzt Dateinamen der Form `00001`

Zunächst sichern wir die Firewall ab und konfigurieren den Administratorzugriff. Dann aktivieren wir NAT und schalten den Zugriff von Intern (Intranet) ins Internet frei (http, https, pop3, imap). Die Anwender können nun surfen und mailen, die Administratoren sich direkt an der Firewall anmelden. Anschliessend wird FTP freigeschaltet.

Um selbst abgesicherte Web- und Mail-Dienste zur Verfügung stellen zu können, wird eine DMZ eingerichtet und der Zugriff auf die darin befindlichen Server erlaubt.

Als nächstes wird die Firewall als VPN-Gateway konfiguriert und sowohl die Anbindung eines 'roaming client' als auch eines anderen Netzes über VPN erklärt.

Rezept 7 beschreibt die Ausfallsicherheit/Verfügbarkeit der Firewall mit Hilfe von 'CARP' und 'pfsync' (siehe PF: Firewall-Redundanz mit CARP und pfsync [http://www.openbsd.com/faq/pf/de/carp.html]).

Zum Schluß geht es um NAT vor dem VPN-Tunnel. Pakete aus dem lokalen Subnetz der einen Tunnelseite erscheinen der anderen Tunnelseite mit einer anderen Absenderadresse.

Hier noch ein paar Dinge, die bei der Erstellung der Regeln beachtet werden sollten:

- bei der Generierung der 'pf.conf' werden 2 Filterregeln automatisch erzeugt:
  - Pakete über das 'Loopback-Interface' dürfen passieren
  - IPv6-Pakete werden geblockt
- alle erzeugten Filterregeln sind 'quick'-Regeln, d.h. die erste passende Regel wird auf das Paket angewendet, danach ist die Regelverarbeitung für dieses Paket beendet. Das bedeutet u.a., daß die Reihenfolge der Regeln wichtig ist:
  - am Anfang sollten die Regeln stehen, die den Zugang zur Firewall regeln. Dieser Regelblock sollte dann von einer Regel abgeschlossen werden, die jeden weiteren Verkehr zur Firewall blockt.
  - Weitere Regelblöcke mit jeweils einer abschließenden Block-Regel ('Drop') sollten dann den Zugang zu den Netzen - in der Reihenfolge ihrer Wichtigkeit - festlegen. Im Allgemeinen also:
    - interne(s) Netz(e)
    - DMZ(s)
    - externe(s) Netz(e)
- wenn für ein 'gateway'-Objekt das Default-Gateway gesetzt ist, bezeichnet 'world' alle Adressen, die über das Default-Gateway erreichbar sind.

- 'any' bezeichnet wirklich 'alle' Adressen, d.h. eine Regel wie 'FROM int TO any SERVICE ssh ACTION pass' würde Verbindungen in alle Netze und auf die Firewall selbst erlauben.

Ein Rezept besteht aus:

- einer einfachen Netzwerk-Skizze,
- der Beschreibung des Konfigurationziels,
- der Liste der zu erstellenden Objekte,
- einer grafischen Darstellung der NAT- und Filterregeln und
- dem Verweis zur Download-Seite

Folgende IP-Adressen (privater Adreßbereich!) werden in den Beispielen benutzt:

- Firewall extern: 192.168.10.79/24
- Firewall-Default-Gateway: 192.168.10.1/24
- Firewall intern: 10.5.0.1/20
- Firewall DMZ: 192.168.11.1/24

Weitere Netzwerkobjekte und IP-Adressen werden in den jeweiligen Rezepten explizit aufgeführt.

Für folgende Konfigurationen existieren Rezepte:

- Firewall absichern und administrierbar machen [#Rezept-1]
- NAT-Gateway und Internet-Zugriff: http, https, pop3, imap [#Rezept-2]
- FTP über 'ftp-proxy' [#Rezept-3]
- DMZ mit Web- und Mailserver [#Rezept-4]
- VPN-Tunnel zwischen 'roaming client' und Intranet [#Rezept-5]
- VPN-Tunnel zwischen 2 Netzen [#Rezept-6]
- Firewall-Redundanz (carp + pfsync) [#Rezept-7]
- NAT vor dem VPN-Tunnel [#Rezept-8]

1.1. Firewall absichern und administrierbar machen

Administratoren sollen sich per 'ssh' vom Intranet her an der Firewall anmelden können. Ebenfalls soll der Zugriff auf die HIOB Gateway Statusseite ('WEB Status View') per 'https' möglich sein. Jeder andere eingehende Verkehr wird geblockt, nur auf der Firewall selbst erzeugter Verkehr und Antworten darauf dürfen passieren.

1.1.1. Skizze

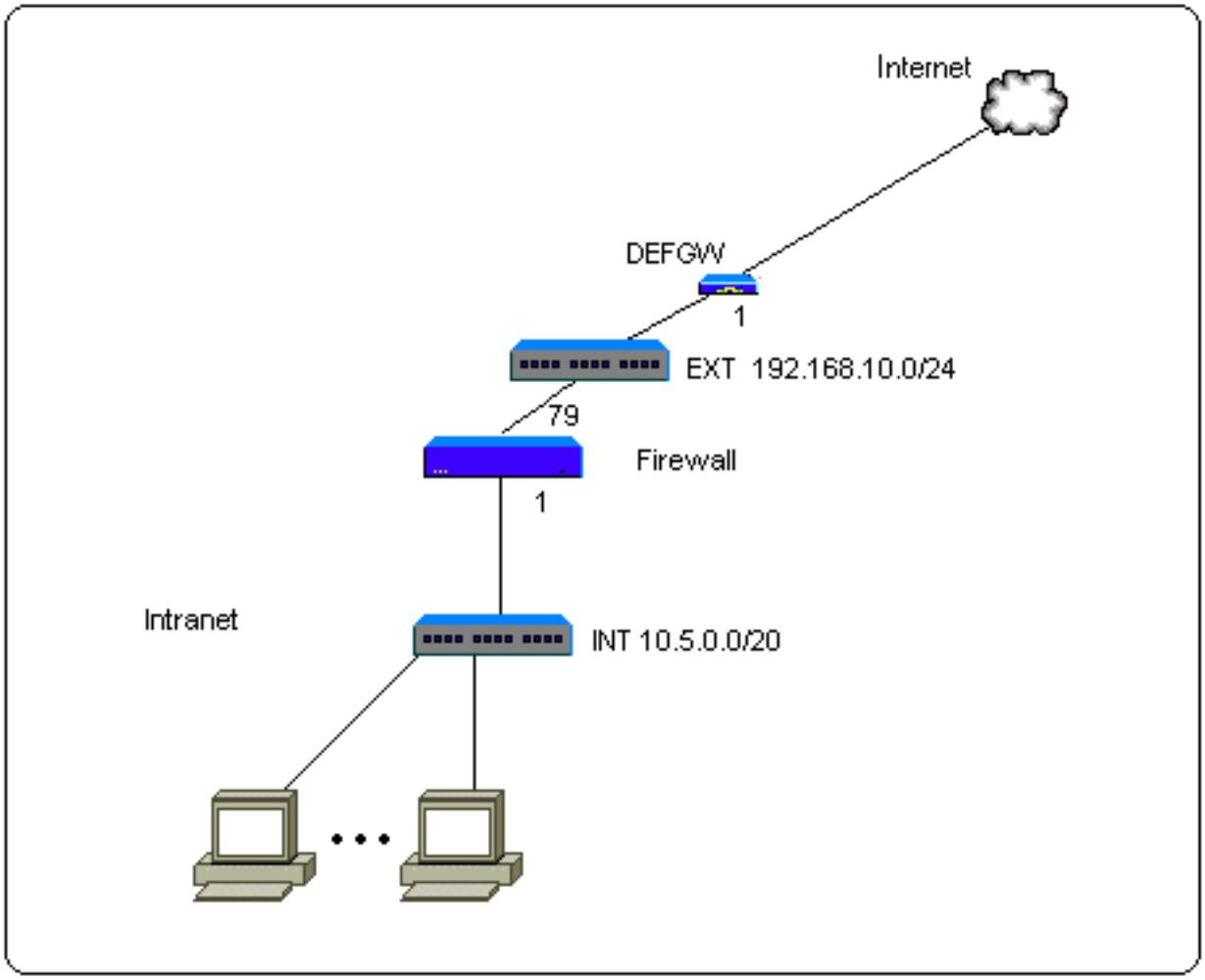


Bild 1.1 Firewall absichern und administrierbar machen

1.1.2. Konfigurationsziel

- zur Firewall eingehenden Verkehr verbieten, außer 'ssh' und 'https'
- alles, was nicht explizit erlaubt ist verbieten ('default deny')

1.1.3. Objekte

- 'Gateway'-Objekt 'firewall' mit Interface 'ext' (192.168.10.79/24) und 'int' (10.5.0.1/20)
- 'firewall' zugewiesene Objekte (Bild 1.2):
  - für Interface 'ext' mit IP 192.168.10.79/24: EXT-IP/offset 0, EXT/offset 0, DEFGW/offset -78
  - für Interface 'int' mit IP 10.5.0.1/20: INT-IP/offset 0, INT/offset 0
- 'Object Group'-Objekt 'Firewall-IP', in dem alle Interfaces/IP-Adressen der Firewall zusammengefasst werden.

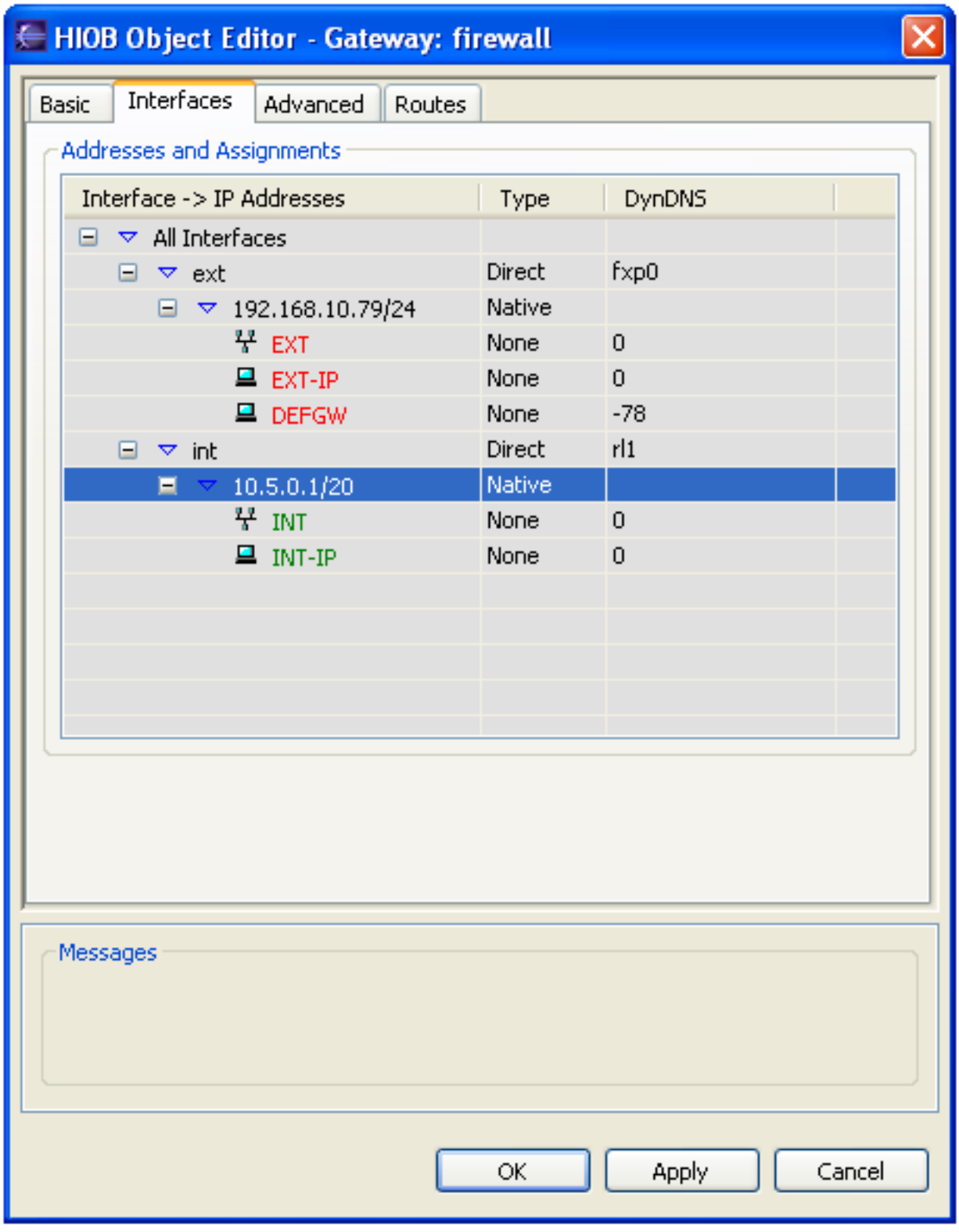


Bild 1.2 'firewall' zugewiesene Objekte

1.1.4. Regeln

NAT

NAT-Regeln werden hier noch nicht benötigt. Die Filterregeln haben folgende Bedeutung:

Filter

- Regel 1 erlaubt die Verbindung vom Intranet zur Firewall über 'ssh' und 'https'
- Regel 2 blockt jeglichen weiteren Verkehr zur Firewall
- Regel 3 blockt alles, was nicht explizit erlaubt ist. Regel 2 wäre also im Moment nicht notwendig, aber da später noch weitere Regeln hinter Regel 2 eingefügt werden, tragen wir sie jetzt schon ein

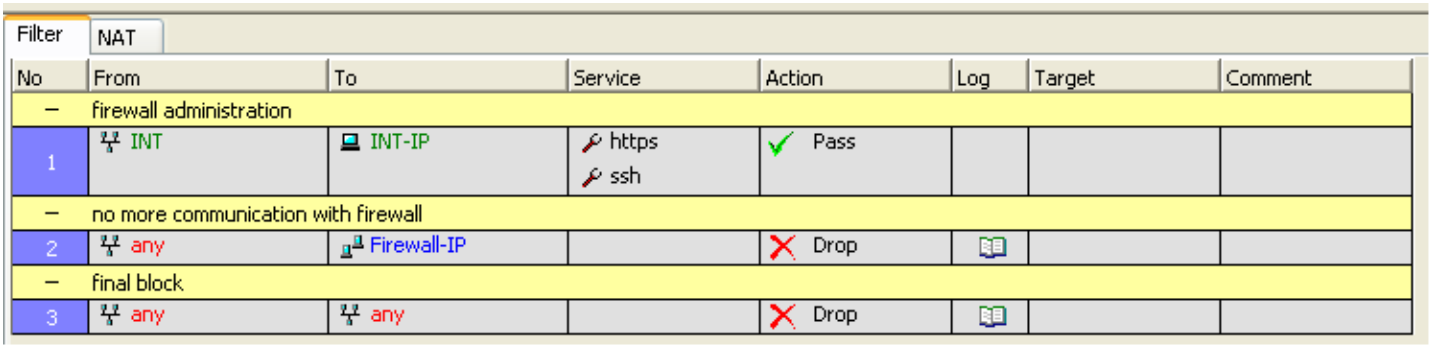


Bild 1.3 - Rezept-1-Filter-Regeln

1.1.5. Download

rezept-1 [../download/rezept-1.xml]

1.2. NAT-Gateway und Internet-Zugriff: http, https, pop3, imap

Der Zugriff auf die Firewall ist freigeschaltet, jetzt soll vom Intranet aus Zugriff auf das Internet ermöglicht werden. Zunächst werden per NAT die internen, privaten IP-Adressen auf die externe IP-Adresse der Firewall abgebildet, dann die Dienste freigeschaltet.

1.2.1. Skizze

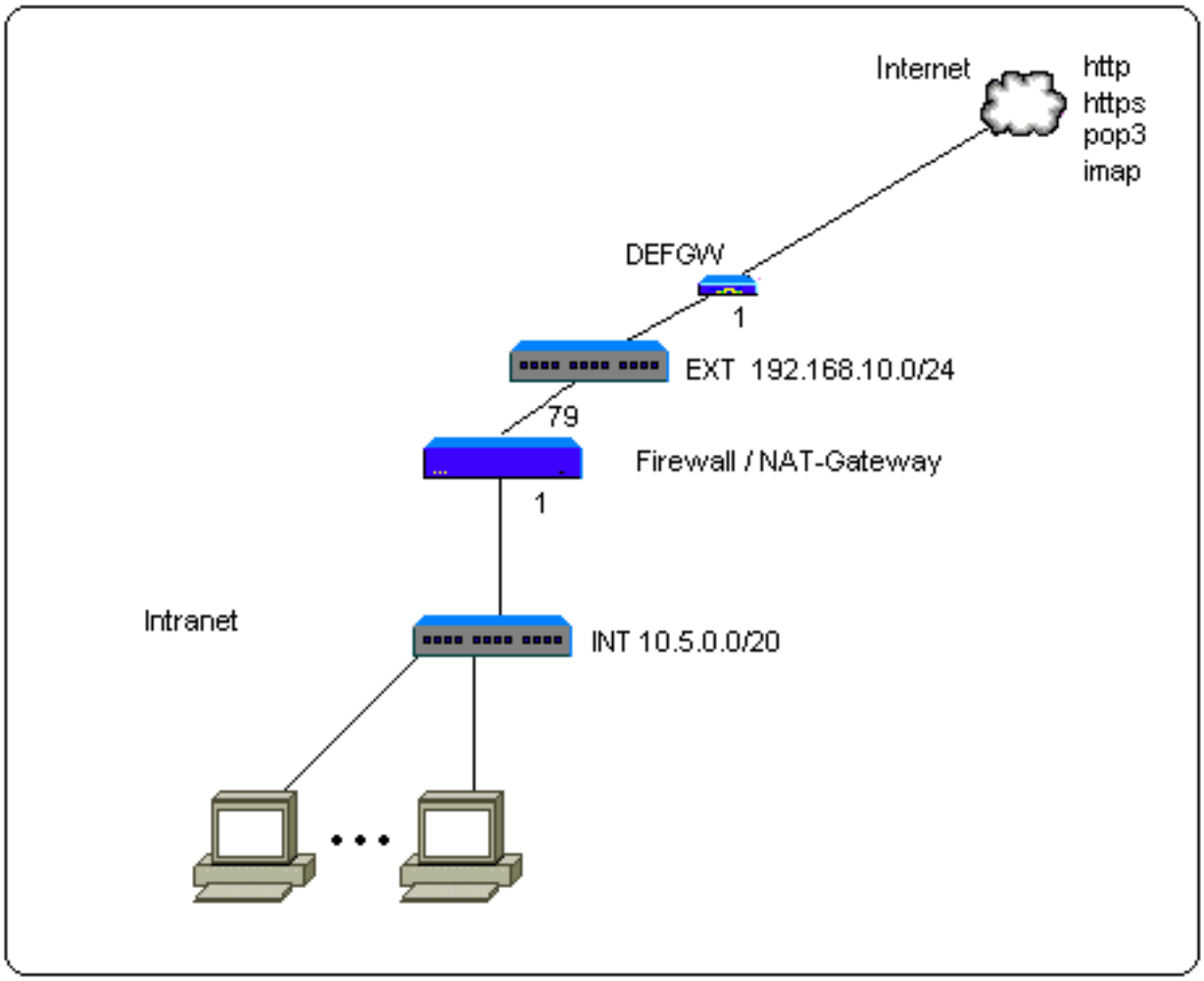


Bild 2.1 NAT-Gateway und Internet-Zugriff: http, https, pop3, imap

1.2.2. Konfigurationsziel

- wie in Firewall absichern und administrierbar machen [#Rezept-1], zusätzlich:
- interne, private IP-Adressen (Intranet) auf die externe IP-Adresse der Firewall abbilden
- vom Intranet ausgehenden Verkehr (http, https, pop3, imap) erlauben, 'stateful'

1.2.3. Objekte

- wie in Firewall absichern und administrierbar machen [#Rezept-1]

1.2.4. Regeln

NAT

NAT-Regel 1 bildet alle internen, privaten IP-Adressen (Intranet) auf die externe IP-Adresse der Firewall ab.

Filter | NAT

No	From	To	Service	Action	Target	Comment
–	nat for internal net					
1	INT	world	any-stateful	Hide A → EXT-IP		

Bild 2.2 - Rezept-2-NAT-Regeln

Filter

Filterregel 4 schaltet die angegebenen Dienste für alle Verbindungen frei, die aus dem Intranet über das Default-Gateway gehen. Da Pakete, auf die NAT-Regel 1 zutrifft, mit Absenderadresse EXT-IP weitergeleitet werden, wird in Filter-Regel 3 in Spalte 'From' 'EXT-IP'eingetragen.

Filter | NAT

No	From	To	Service	Action	Log	Target	Comment
–	firewall administration						
1	INT	INT-IP	https ssh	Pass			
–	no more communication with firewall						
2	any	Firewall-IP		Drop			
–	from inside to outside						
3	EXT-IP	world	any-stateful	Pass			
4	INT	world	http https imap pop3	Pass			
–	final block						
5	any	any		Drop			

Bild 2.3 - Rezept-2-Filter-Regeln

1.2.5. Download

rezept-2 [../download/rezept-2.xml]

1.3. FTP über 'ftp-proxy'

Bei der Freischaltung von 'ftp' muß ein etwas größerer Aufwand betrieben werden, als z.B. bei der Freischaltung von 'http', da FTP auf zwei unterschiedliche Arten (aktiv und passiv) betrieben werden kann und zwei Verbindungen per FTP-Session benötigt. Die Probleme, die FTP im Zusammenhang mit NAT und Firewall bereitet (siehe PF: Probleme mit FTP [http://www.openbsd.org/faq/pf/de/ftp.html]), werden durch die Benutzung des FTP-Proxyservers 'ftp-proxy' gelöst. 'ftp-proxy' wird durch die Benutzung entsprechender Filter-/ und NAT-Regeln auf der Firewall automatisch gestartet.

1.3.1. Skizze

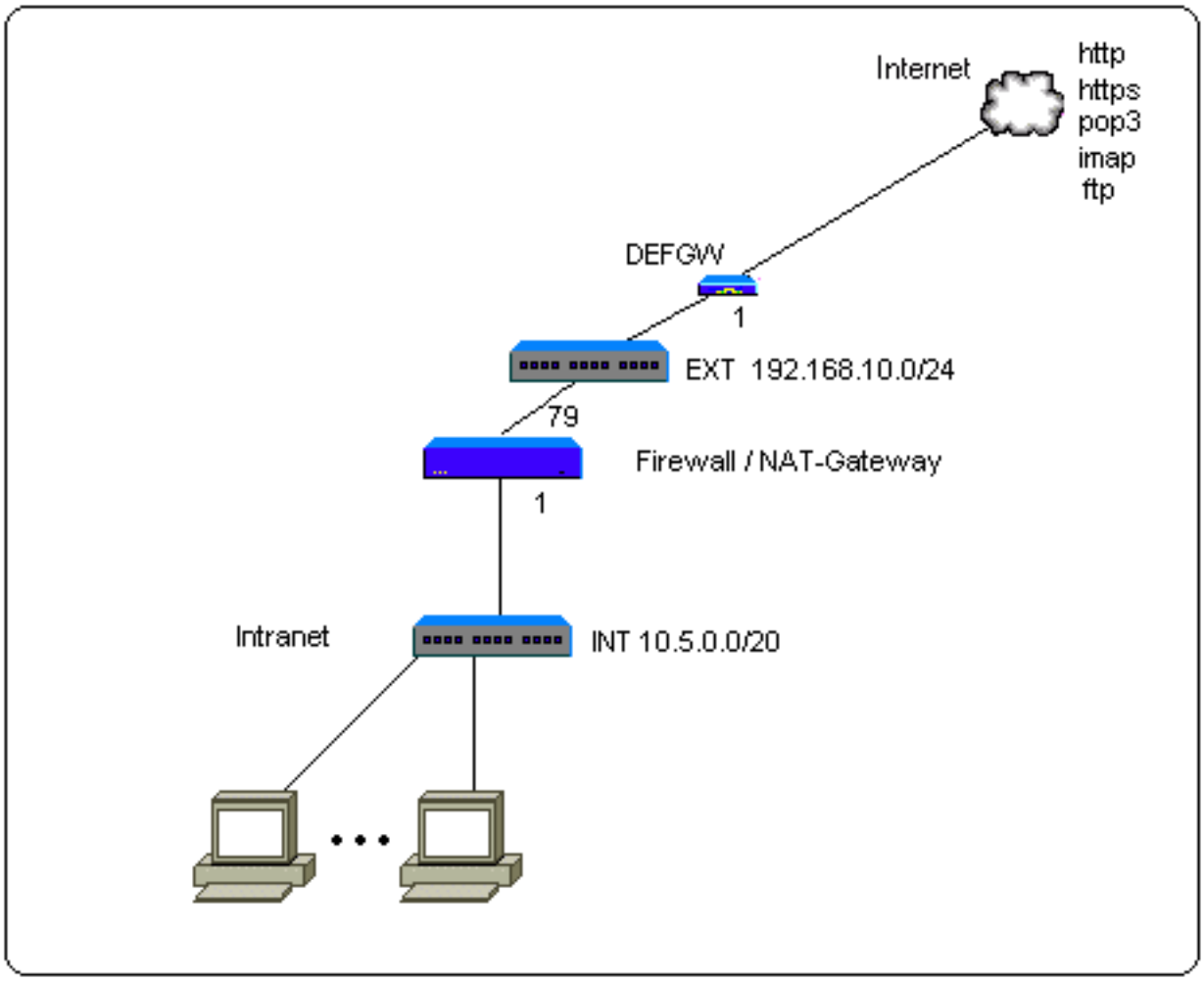


Bild 3.1 - FTP über 'ftp-proxy'

1.3.2. Konfigurationsziel

- wie in NAT-Gateway und Internet-Zugriff: http, https, pop3, imap [#Rezept-2], zusätzlich:
- FTP erlauben

1.3.3. Objekte

- wie in NAT-Gateway und Internet-Zugriff: http, https, pop3, imap [#Rezept-2]

1.3.4. Regeln

NAT

Regel 2 sorgt dafür, daß FTP-Verbindungen vom Intranet ins Internet über den 'ftp-proxy' laufen.

Filter | NAT

No	From	To	Service	Action	Target	Comment
–	nat for internal net					
1	INT	world	any-stateful	Hide A → EXT-IP		
–	ftp-proxy					
2	INT	world	ftp-control	Redirect A → localhost S → ftp-proxy		

Bild 3.2 - Rezept-3-NAT-Regeln

Filter

Der in Filterregel 4 in der Spalte 'Service' hinzugefügte Eintrag 'ftp-proxy' schaltet für das Intranet den FTP-Zugriff auf das Internet frei.

Filter | NAT

No	From	To	Service	Action	Log	Target	Comment
–	firewall administration						
1	INT	INT-IP	https ssh	Pass			
–	no more communication with firewall						
2	any	Firewall-IP		Drop			
–	from inside to outside						
3	EXT-IP	world	any-stateful	Pass			
4	INT	world	ftp-proxy http https imap pop3 smtp	Pass			
–	final block						
5	any	any		Drop			

Bild 3.3 - Rezept-3-Filter-Regeln

1.3.5. Download

rezept-3 [../download/rezept-3.xml]

1.4. DMZ mit Web- und Mailserver

Es gibt mehrere Möglichkeiten, von Extern (Internet) auf die Server in der DMZ zuzugreifen:

- Haben sie wie die Firewall eine öffentliche IP-Adresse, dann werden per NAT Verbindungen zu dieser öffentlichen IP auf deren interne IP umgeleitet
- Haben sie nur eine private IP-Adresse, dann werden Verbindungen zur externen Firewall-IP-Adresse auf Port 'http' bzw. 'smtp' per NAT zu der internen IP-Adresse des entsprechenden Servers umgeleitet

Von Intern kann auf die beiden Server über ihre interne IP (DMZ) zugegriffen werden. Dafür muß keine NAT-Regeln erstellt werden.

Wir vergeben den beiden Servern jeweils eine interne und externe IP und legen entsprechende Objekte und Regeln an.

1.4.1. Skizze

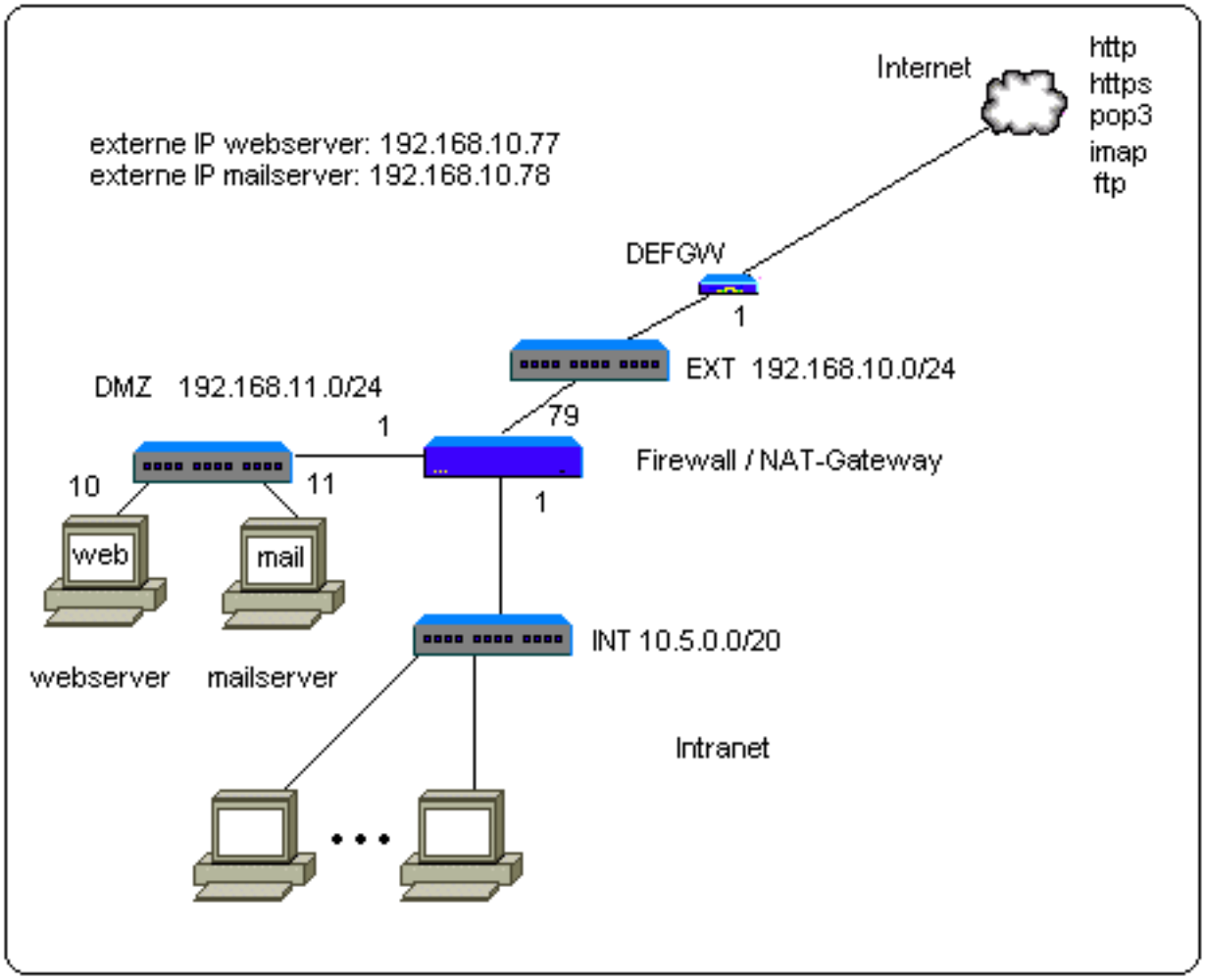


Bild 4.1 - DMZ mit Web- und Mailserver

1.4.2. Konfigurationsziel

- wie in FTP über 'ftp-proxy' [#Rezept-3], zusätzlich:
- Zugriff auf Web- und Mailserver in DMZ (von intern und extern)

1.4.3. Objekte

- 'Gateway'-Objekt 'firewall' mit Interfaces 'ext' (192.168.10.79/24), 'int' (10.5.0.1/20) und 'dmz' (192.168.11.1/24)
- 4 globale 'host'-Objekte 'mail-dmz', 'mail-extern', 'web-dmz', 'web-extern'. Diese bekommen ihre IP-Adresse über 'firewall' zugewiesen
- 'firewall' zugewiesene Objekte:

- für 192.168.10.79/24: EXT-IP/offset 0, EXT/offset 0, DEFGW/offset -78, mail-extern/offset -1, web-extern/offset -2
- für 10.5.0.1/20: INT/offset 0, INT-IP/offset 0
- für 192.168.11.1/24: DMZ/offset 0, DMZ-IP/offset 0, mail-dmz/offset 10, web-dmz/offset 9

1.4.4. Regeln

NAT

Regel 1 erzeugt eine 'eins zu eins'-Abbildung der internen IP-Adresse des Mailservers zu seiner externen IP-Adresse. Verbindungen aus dem Internet auf die externe Adresse werden auf die interne Adresse umgeleitet, bei Verbindungen vom Mailserver ins Internet wird die interne Adresse durch die externe Adresse ersetzt. Regel 2 sorgt dafür, daß Verbindungen vom Internet zur externen IP-Adresse des Webservers auf seine interne IP-Adresse umgeleitet werden. Da der Webserver in unserem Beispiel keine Verbindungen ins Internet aufbauen muß, reicht hier eine 'redirect'-Regel.

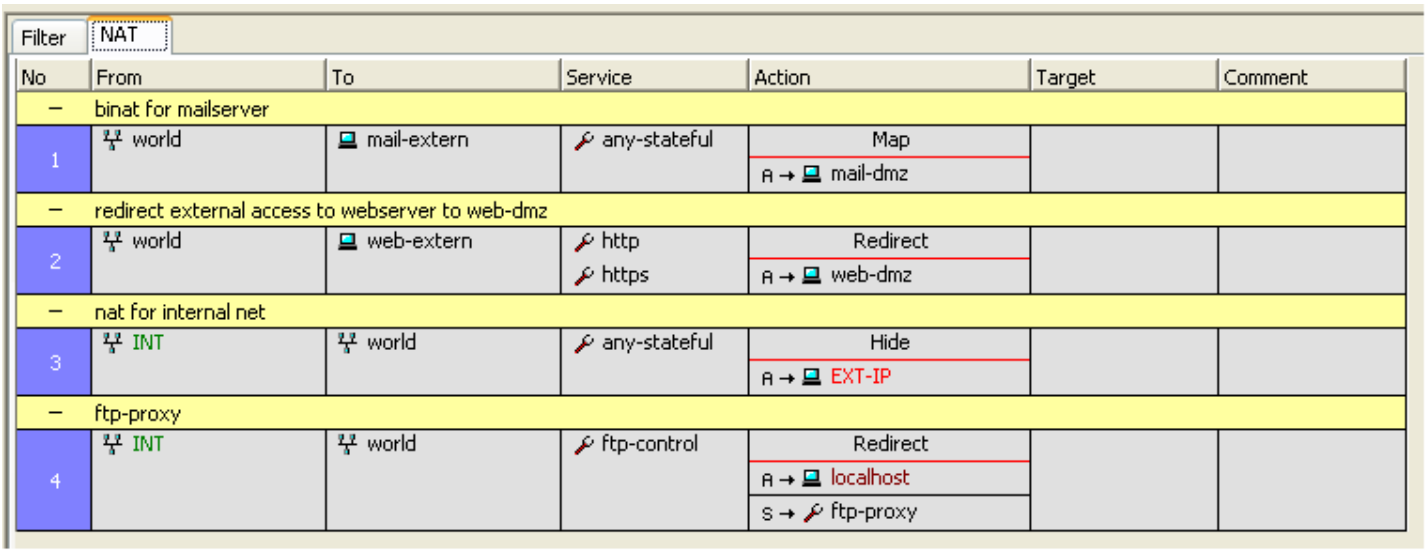


Bild 4.2 - Rezept-4-NAT-Regeln

Filter

Zunächst fügen wir eine Block-Regel ein, die den Zugriff auf das Intranet explizit sperrt (Regel 3) (wenn zukünftig Regeln zum Zugriff auf das Intranet hinzugefügt werden sollen, müssen diese vor diese Block-Regel eingefügt werden). Dann schalten wir für das Intranet und das Internet den Zugriff auf die beiden Server in der DMZ frei (Regeln 4 und 5) und blocken danach explizit jeden weiteren Zugriff auf die DMZ (Regel 6). Schließlich erlauben wir dem Mailserver - zwecks Mailversand - den Aufbau von Verbindungen ins Internet (Regel 9).

Die klare Gliederung der Regeln in einzelne Abschnitte und das Einfügen expliziter Block-Regeln am Ende jedes Abschnitts machen die Regelmenge übersichtlich. So ist außerdem gewährleistet, daß durch das Hinzufügen weiterer Regeln keine unbeabsichtigten Freischaltungen erzeugt werden.

Filter | NAT

No	From	To	Service	Action	Log	Target	Comment
–	firewall administration						
1	INT	INT-IP	https ssh	Pass			
–	no more communication to firewall						
2	any	Firewall-IP		Drop			
–	protect internal net						
3	any	INT		Drop			
–	access to mail-server in DMZ						
4	INT world	mail-dmz	imap pop3 smtp	Pass			
–	access to web-server in DMZ						
5	INT world	web-dmz	http https	Pass			
–	no more communication to DMZ						
6	any	DMZ		Drop			
–	from inside to outside						
7	EXT-IP	world	any-stateful	Pass			
8	INT	world	ftp-proxy http https imap pop3	Pass			
–	allow mailserver out						
9	mail-extern	world	smtp	Pass			
–	final block						
10	any	any		Drop			

Bild 4.3 - Rezept-4-Filter-Regeln

1.4.5. Download

rezept-4 [../download/rezept-4.xml]

1.5. VPN-Tunnel zwischen 'roaming client' und Intranet

Der 'roaming client' ist in unserem Fall ein Laptop mit der VPN-Client-Software 'NCP Secure Entry Client' von NCP [http://www.ncp.de/]. Nach dem Herstellen einer Internetverbindung und dem anschließenden Aufbau einer VPN-Verbindung ist der 'roaming client' ins Intranet eingebunden.

Die VPN-Client-Software wird in unserem Beispiel mit folgenden Parametern konfiguriert:

- IP-Adresse: 10.5.0.100/20
- VPN IPNetz: 10.5.0.0/20
- Nameserver: 192.168.11.10 (Webserver in DMZ bietet diesen Dienst)
- IPsec Gateway: 192.168.10.79

- IKE Policy:
  - Authentisierung: Preshared Key
  - Verschlüsselung: 3DES
  - Hash: SHA
  - DH-Gruppe: 2
- IPSec Policy:
  - Protokoll: ESP
  - Verschlüsselung: AES 128 Bit
  - Authentisierung: SHA
  - DH-Gruppe: 2
- IKE Phase 1: Aggressive mode
- Identität:
  - Typ: Fully Qualified Username
  - ID: user@default.org
- Preshared Key: j9qQFvGXkxE2VNw5iErPm4TyCmFlJgrL2anXzKZGLreFlZMS

1.5.1. Skizze

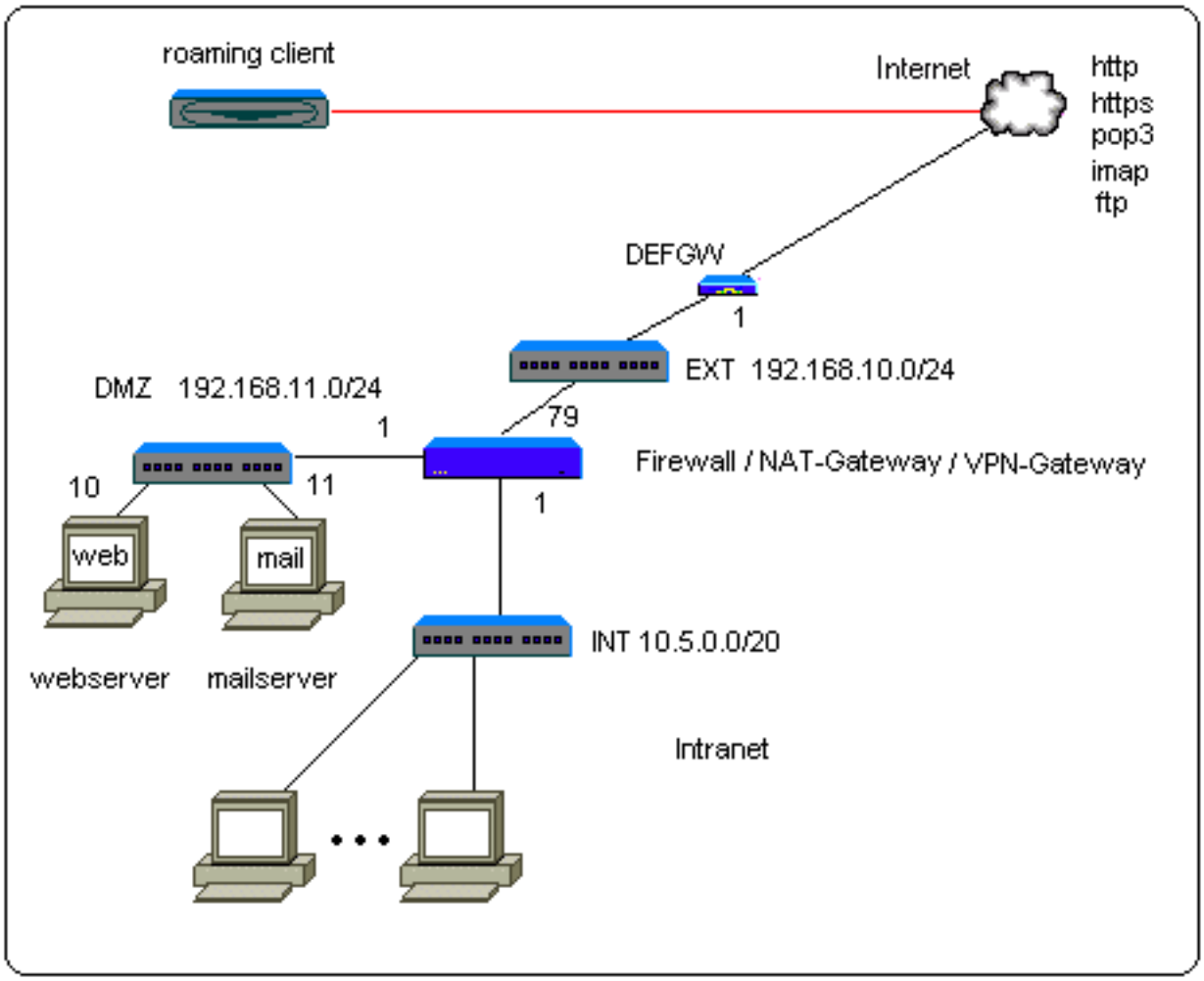


Bild 5.1 - VPN-Tunnel zwischen 'roaming client' und Intranet

1.5.2. Konfigurationsziel

- wie in DMZ mit Web- und Mailserver [#Rezept-4], zusätzlich:
- Webserver bietet auch DNS
- 'roaming client' wird über VPN ins Intranet eingebunden

1.5.3. Objekte

- wie in DMZ mit Web- und Mailserver [#Rezept-4]
- 'mobile tunnel'-Objekt 'mobileTunnel'; ihm werden nachfolgende Objekte zugewiesen:
  - lokales 'network'-Objekt 'EXT-IP'; repräsentiert im 'mobile tunnel'-Objekt den linken Endpunkt (VPN-Gateway) des Tunnels
  - lokales 'network'-Objekt 'INT'; repräsentiert im 'mobile tunnel'-Objekt das interne Netz (Intranet) der Firewall
  - globales 'host'-Objekt 'web-dmz'; repräsentiert im 'mobile tunnel'-Objekt den DNS-Server, der dem 'roaming client' bei der Einwahl zugewiesen wird

- 'Id'-Objekt 'roaming-client-id'; repräsentiert im 'mobile tunnel'-Objekt die IP-Adresse und die Identität des rechten Endpunkts ('roaming client') des Tunnels
- 'key'-Objekt 'roaming-client-key'; repräsentiert im 'mobile tunnel'-Objekt den 'preshared key'

1.5.4. Regeln

NAT

Neue NAT-Regeln werden nicht benötigt, da sich der 'roaming client' nach der Einwahl wie ein Rechner im Intranet verhält.

Filter

Die Regeln 2 und 3 erlauben Aufbau und Verwaltung eines VPN-Tunnels und die damit zusammenhängenden Protokolle (UDP/500 (IKE), UDP/4500 (NAT traversal), esp, ipencap). In Regeln 8 wird DNS freigschaltet. Der eigentliche Datenverkehr zwischen 'roaming client' und Intranet wird durch Regel 5 freigeschaltet. Die Regeln 7 und 8 aus Rezept 4 sind zu einer einzigen Regel 10 zusammengefasst.

Filter | NAT

No	From	To	Service	Action	Log	Target	Comment
–	firewall administration						
1	INT	INT-IP	https ssh	Pass			
–	VPN: allow roaming clients						
2	EXT-IP	world	ipsec	Pass			
3	world	EXT-IP	ipsec	Pass			
–	no more communication to firewall						
4	any	Firewall-IP		Drop			
–	VPN: allow vpn traffic						
5	roaming-client-id	INT	any-stateful	Pass			
–	protect internal net						
6	any	INT		Drop			
–	access to mail-server in DMZ						
7	INT world	mail-dmz	imap pop3 smtp	Pass			
–	access to web-server in DMZ						
8	INT world	web-dmz	dns http https	Pass			
–	no more communication to DMZ						
9	any	DMZ		Drop			
–	from inside to outside						
10	INT EXT-IP	world	ftp-proxy http https imap pop3	Pass			
–	allow mailserver out						
11	mail-extern	world	smtp	Pass			
–	final block						
12	any	any		Drop			

Bild 5.2 - Rezept-5-Filter-Regeln

1.5.5. Download

rezept-5 [../download/rezept-5.xml]

1.6. VPN-Tunnel zwischen 2 Netzen

In unserer bisherigen Konfiguration benennen wir das Objekt 'firewall' in 'Firewall-A' um. Das zweite Netz, welches wir über einen VPN-Tunnel anbinden werden, wird über 'Firewall-B' verwaltet. Die folgenden IP-Adressen werden dafür benutzt:

- 'Firewall-B' extern: 192.168.99.2/24
- 'Firewall-B'-Default-Gateway: 192.168.99.1/24
- 'Firewall-B' intern: 10.6.0.1/20

1.6.1. Skizze

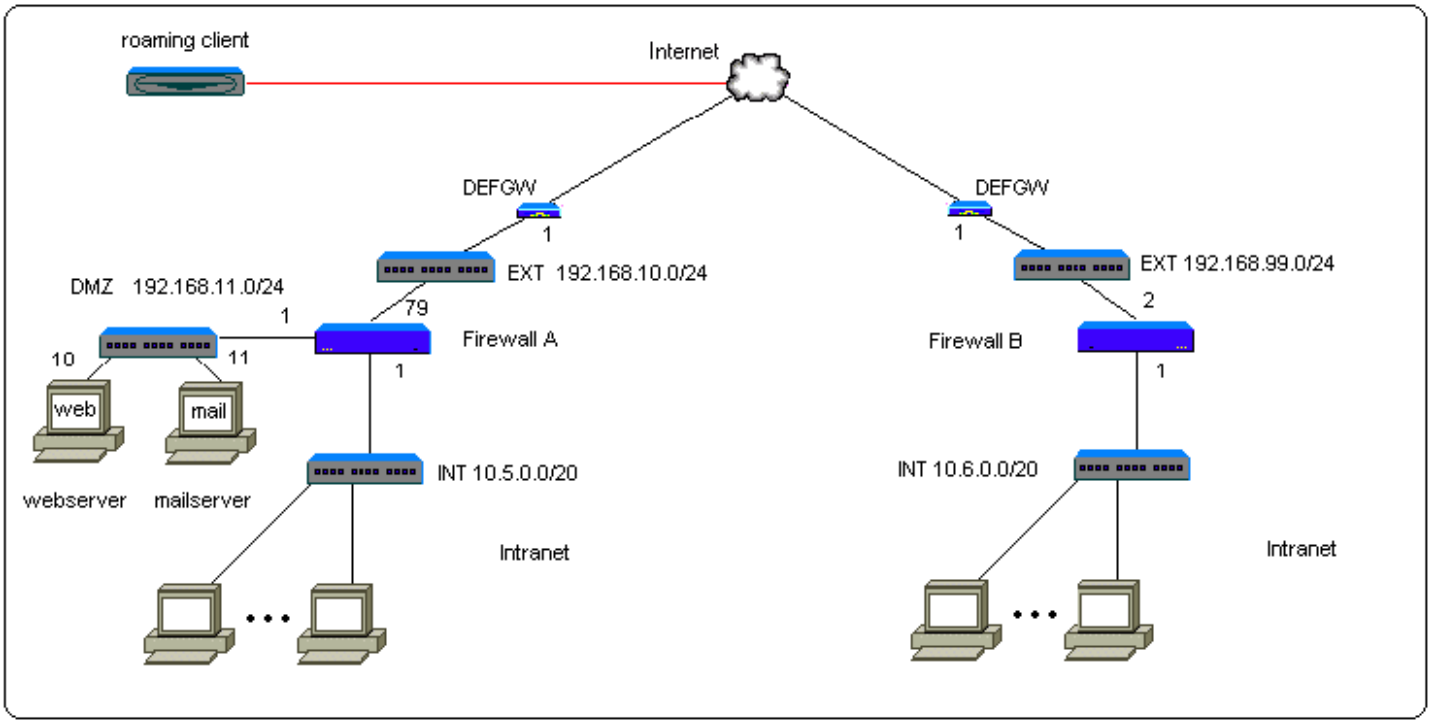


Bild 6.1 - VPN-Tunnel zwischen 2 Netzen

1.6.2. Konfigurationsziel

- wie in VPN-Tunnel zwischen 'roaming client' und Intranet [#Rezept-5], zusätzlich:
- Zweites Netz über VPN-Tunnel anbinden

1.6.3. Objekte

- wie in VPN-Tunnel zwischen 'roaming client' und Intranet [#Rezept-5]
- 'Gateway'-Objekt 'Firewall-A' werden zusätzlich zwei globale Objekte zugewiesen:
  - für 192.168.10.79/24: vpn-gw-A/offset 0
  - für 10.5.0.1/20: vpn-gateway-int/offset 0
- 'Gateway'-Objekt 'Firewall-B' mit Interfaces 'ext' (192.168.99.2/24) und 'int' (10.6.0.1/20) wird angelegt und folgende Objekte werden zugewiesen:
  - für 192.168.99.2/24: EXT-IP/offset 0, EXT/offset 0, DEFGW/offset -1
  - für 10.6.0.1/20: INT/offset 0, INT-IP/offset 0
- für 'Gateway'-Objekt 'Firewall-B' werden zwei statische Objekte angelegt:
  - statisches 'host'-Objekt 'vpn-gw-B', IP 192.168.99.1

    - statisches 'network'-Objekt 'B-int-net', IP 10.6.0.0/20
- 'tunnel'-Objekt 'A-B-Tunnel' wird angelegt; ihm werden nachfolgende Objekte zugewiesen:
    - 'Firewall-A"; repräsentiert im 'tunnel'-Objekt das linke VPN-Gateway
    - 'Firewall-B"; repräsentiert im 'tunnel'-Objekt das rechte VPN-Gateway
    - 'vpn-gw-A'; repräsentiert im 'tunnel'-Objekt die IP-Adresse des linken Endpunkts des Tunnels
    - 'vpn-gw-B'; repräsentiert im 'tunnel'-Objekt die IP-Adresse des rechten Endpunkts des Tunnels
    - 'vpn-gateway-int'; repräsentiert im 'tunnel'-Objekt das interne Netz von 'Firewall-A'
    - 'B-int-net'; repräsentiert im 'tunnel'-Objekt das interne Netz von 'Firewall-B'
    - 'key'-Objekt 'A-B-key'; repräsentiert im 'tunnel'-Objekt den 'preshared key'

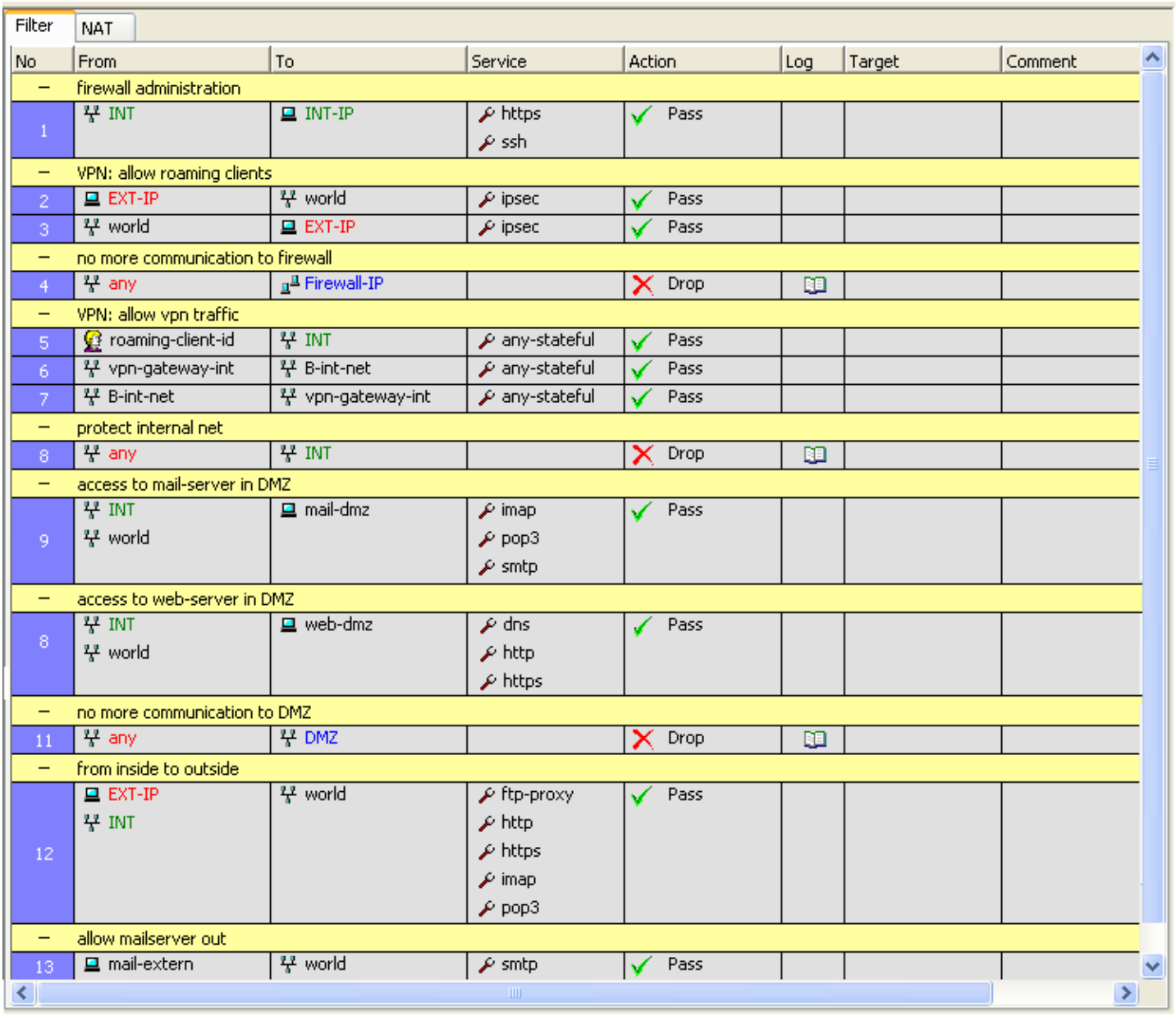
1.6.4. Regeln

NAT

Neue NAT-Regeln werden nicht benötigt. Nach dem Tunnelaufbau kann von beiden 'Intranets' aus aufeinander zugegriffen werden.

Filter

Aufbau und Verwaltung des VPN-Tunnels zu Netz B wird bereits über die Regeln 2 und 3 erlaubt ('world'). Der eigentliche Datenverkehr zwischen den beiden Netzen wird durch die Regeln 6 und 7 freigeschaltet.



Filter | NAT

No	From	To	Service	Action	Log	Target	Comment
–	firewall administration						
1	INT	INT-IP	https ssh	Pass			
–	VPN: allow roaming clients						
2	EXT-IP	world	ipsec	Pass			
3	world	EXT-IP	ipsec	Pass			
–	no more communication to firewall						
4	any	Firewall-IP		Drop			
–	VPN: allow vpn traffic						
5	roaming-client-id	INT	any-stateful	Pass			
6	vpn-gateway-int	B-int-net	any-stateful	Pass			
7	B-int-net	vpn-gateway-int	any-stateful	Pass			
–	protect internal net						
8	any	INT		Drop			
–	access to mail-server in DMZ						
9	INT world	mail-dmz	imap pop3 smtp	Pass			
–	access to web-server in DMZ						
8	INT world	web-dmz	dns http https	Pass			
–	no more communication to DMZ						
11	any	DMZ		Drop			
–	from inside to outside						
12	EXT-IP INT	world	ftp-proxy http https imap pop3	Pass			
–	allow mailserver out						
13	mail-extern	world	smtp	Pass			

Bild 6.2 - Rezept-6-Filter-Regeln

1.6.5. Download

rezept-6 [../download/rezept-6.xml]

1.7. Firewall-Redundanz (carp + pfsync)

In den bisherigen Beispielen ist die Firewall ein 'single point of failure'. Dies kann durch Parallelschaltung mehrerer Firewalls verhindert werden. Mit dem CARP-Protokoll wird ein 'Cluster' (hier aus 2 Maschinen) aufgebaut, mit dem 'pfsync'-Interface werden 'state table updates' übertragen.

Der gesamte Verkehr geht in unserem Beispiel durch 'Firewall-A' (Master); fällt sie aus, übernimmt 'Firewall-B' (Backup) ihre Funktion. Existierende Verbindungen werden beibehalten und der Netzwerkverkehr fließt weiter, als wäre nichts geschehen. Ist 'Firewall-A' wieder aktiv, übernimmt sie wieder die 'Master'-Rolle.

1.7.1. Skizze

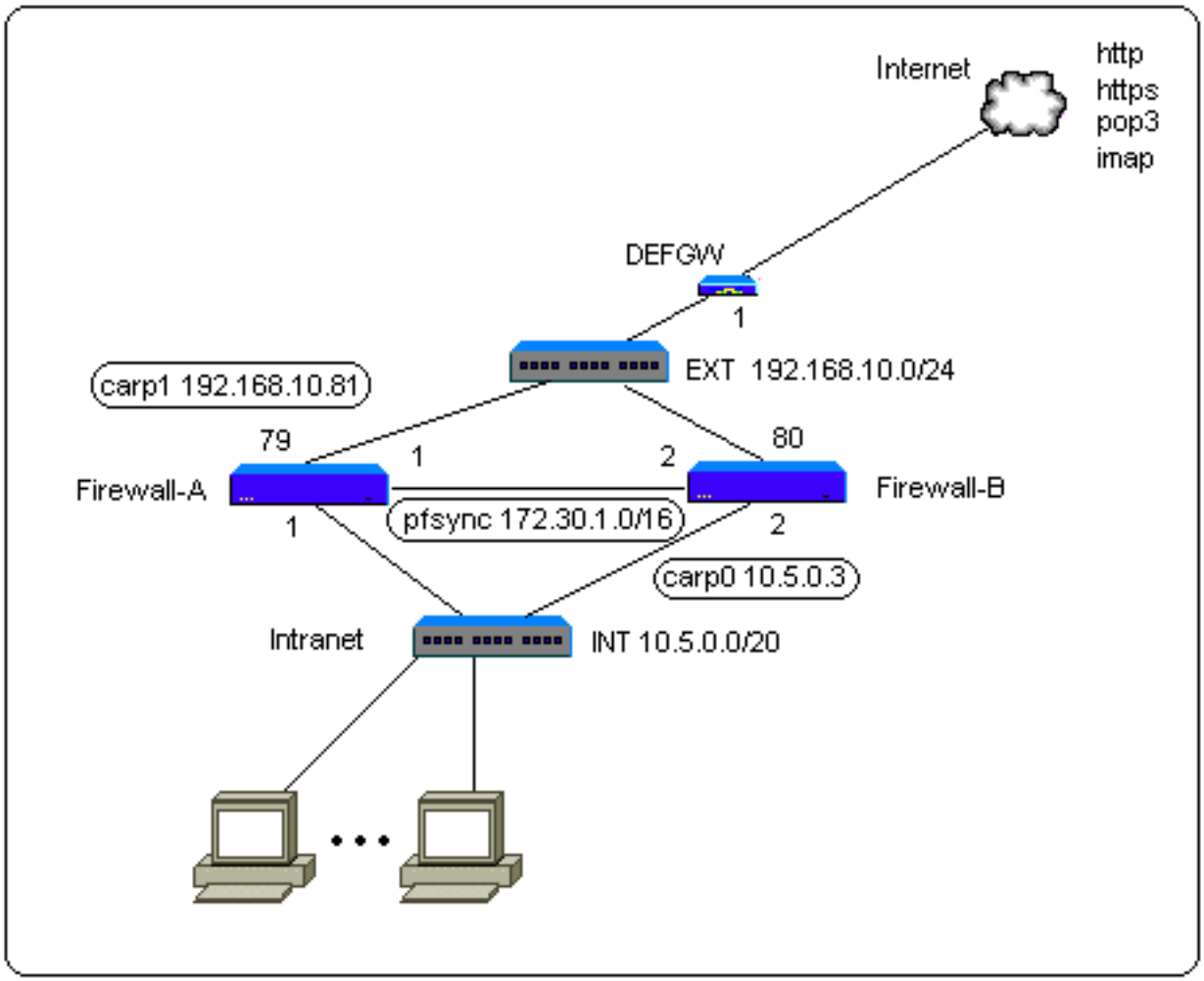


Bild 7.1 Firewall-Cluster

1.7.2. Konfigurationsziel

- wie in NAT-Gateway und Internet-Zugriff: http, https, pop3, imap [#Rezept-2], zusätzlich:
- Firewall-Redundanz durch Cluster mit 2 Maschinen

1.7.3. Objekte

Den externen und internen Interfaces beider Firewalls wird jeweils eine zweite IP-Adresse zugewiesen (ext 192.168.10.81/24, int 10.5.0.3/20) und als Typ carp1 bzw. carp0 eingestellt. Zusätzlich wird für beide Firewalls jeweils ein drittes Interface ('sync') angelegt. Um den Zugriff auf die Interfaces zu regeln, werden folgende lokale Objekte angelegt:

- EXT-CARP-IP: IP-Adresse des externen CARP-Interface
- INT-CARP-IP: IP-Adresse des internen CARP-Interface
- SYNC-IP: IP-Adresse des pfsync-Interface

- SYNC: IP-Adresse des pfsync-Netzes

In die Gruppe 'Firewall-IP' werden die zusätzlichen Objekte EXT-CARP-IP, INT-CARP-IP und SYNC-IP eingetragen. Dann werden die Interfaces der beiden Firewalls entsprechend konfiguriert:

- 'Gateway'-Objekt 'Firewall-A' mit Interface 'ext' (192.168.10.79/24 + 192.168.10.81/24), 'int' (10.5.0.1/20 + 10.5.0.3/20) und 'sync' (172.30.1.1/16)
- 'Firewall-A' zugewiesene Objekte (Bild 7.2):
  - für Interface 'ext' mit IP 192.168.10.79/24: EXT-IP/offset 0, EXT/offset 0, DEFGW/offset -78
  - für Interface 'ext' mit IP 192.168.10.81/24 ('carp1'): EXT-CARP-IP/offset 0
  - für Interface 'int' mit IP 10.5.0.1/20: INT-IP/offset 0, INT/offset 0
  - für Interface 'int' mit IP 10.5.0.3/20 ('carp0'): INT-CARP-IP/offset 0
  - für Interface 'sync' mit IP 172.30.1.1/16 ('pfsync'): SYNC-IP/offset 0, SYNC/offset 0
- 'Gateway'-Objekt 'Firewall-B' mit Interface 'ext' (192.168.10.80/24 + 192.168.10.81/24), 'int' (10.5.0.2/20 + 10.5.0.3/20) und 'sync' (172.30.1.2/16)
- 'Firewall-B' zugewiesene Objekte (Bild 7.3):
  - für Interface 'ext' mit IP 192.168.10.80/24: EXT-IP/offset 0, EXT/offset 0, DEFGW/offset -79
  - für Interface 'ext' mit IP 192.168.10.81/24 ('carp1'): EXT-CARP-IP/offset 0
  - für Interface 'int' mit IP 10.5.0.2/20: INT-IP/offset 0, INT/offset 0
  - für Interface 'int' mit IP 10.5.0.3/20 ('carp0'): INT-CARP-IP/offset 0
  - für Interface 'sync' mit IP 172.30.1.2/16 ('pfsync'): SYNC-IP/offset 0, SYNC/offset 0
- 'Object Group'-Objekt 'Firewall-IP', in dem alle Interfaces/IP-Adressen der Firewall zusammengefasst werden.

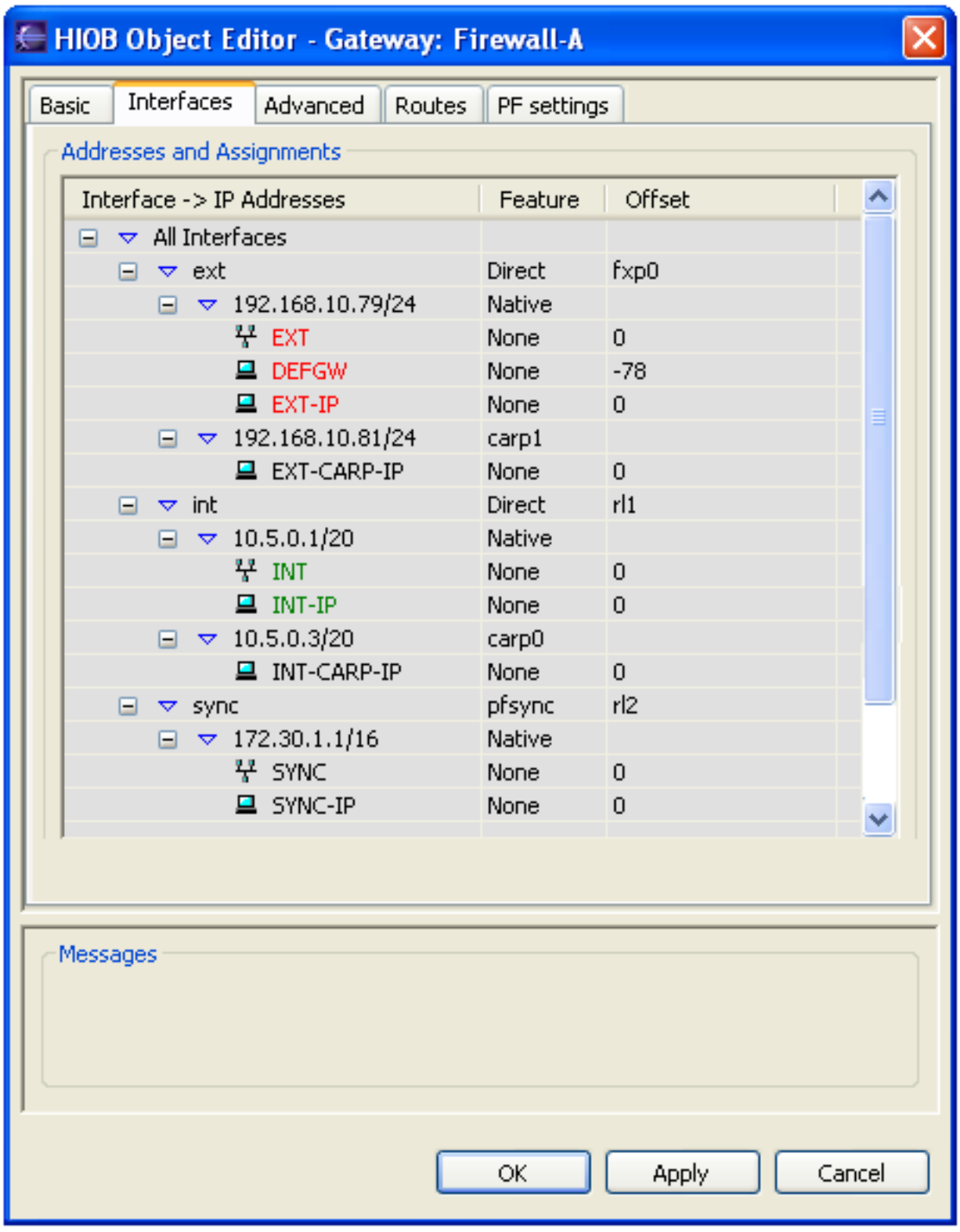


Bild 7.2 'Firewall-A' zugewiesene Objekte

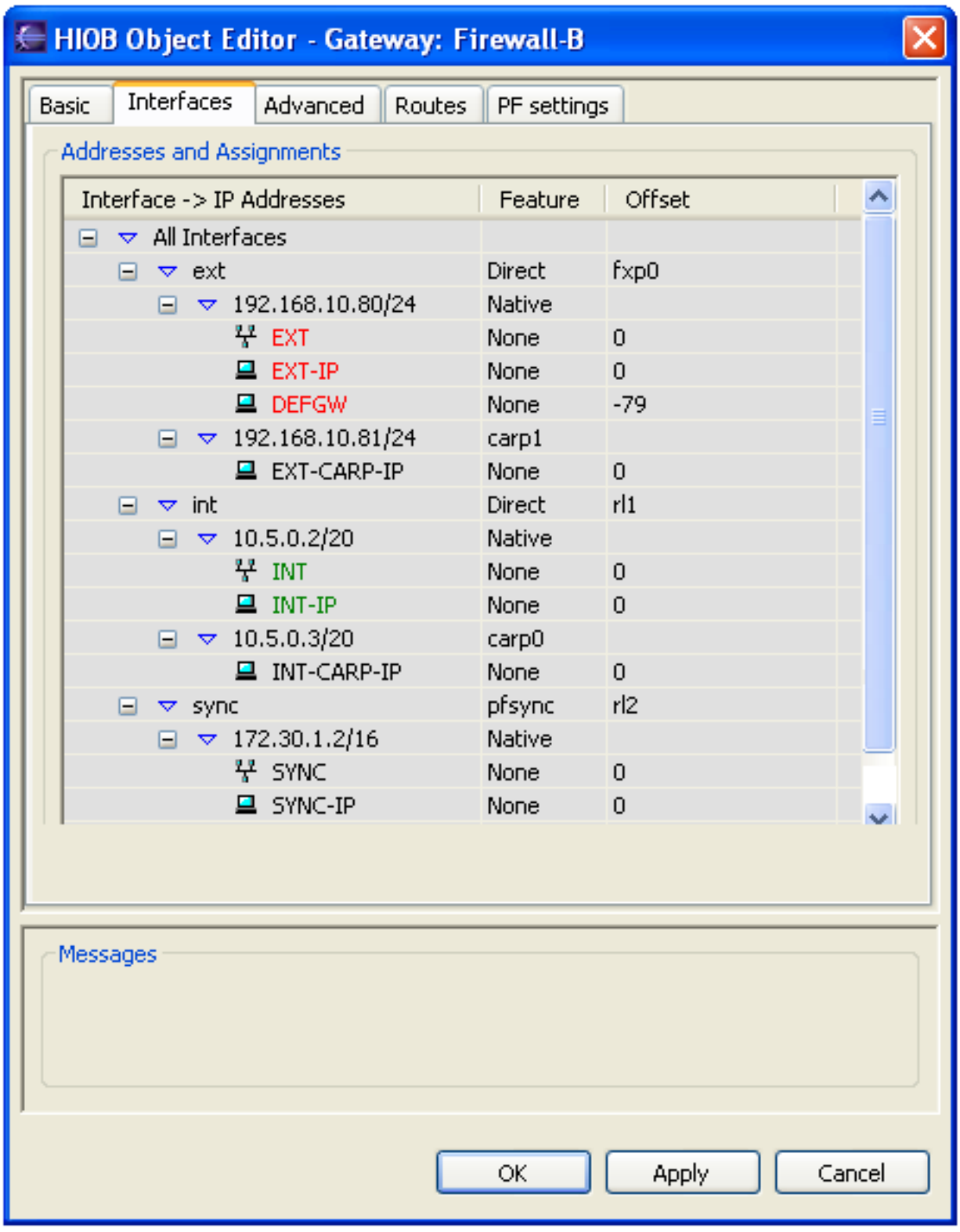


Bild 7.3 'Firewall-B' zugewiesene Objekte

Einige der default-Einstellungen für CARP müssen jetzt noch geändert werden (Bild 7.4 + 7.5):

- für carp0/Firewall-A: VHID:11 Base:1 Skew:10

- für carp1/Firewall-A: VHID:10 Base:1 Skew:10
- für carp0/Firewall-B: VHID:11 Base:1 Skew:100
- für carp1/Firewall-B: VHID:10 Base:1 Skew:100

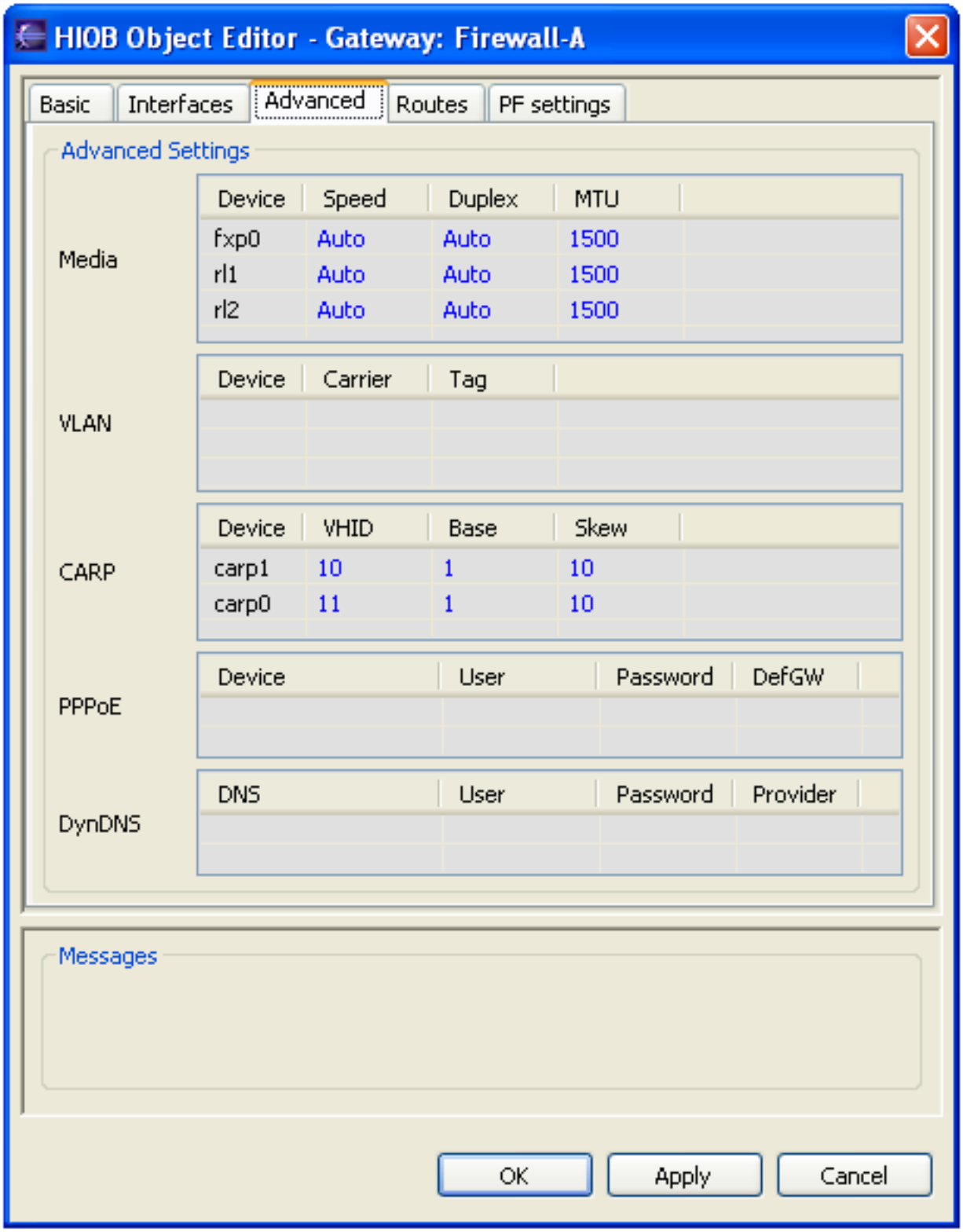


Bild 7.4 'Firewall-A' CARP-Parameter

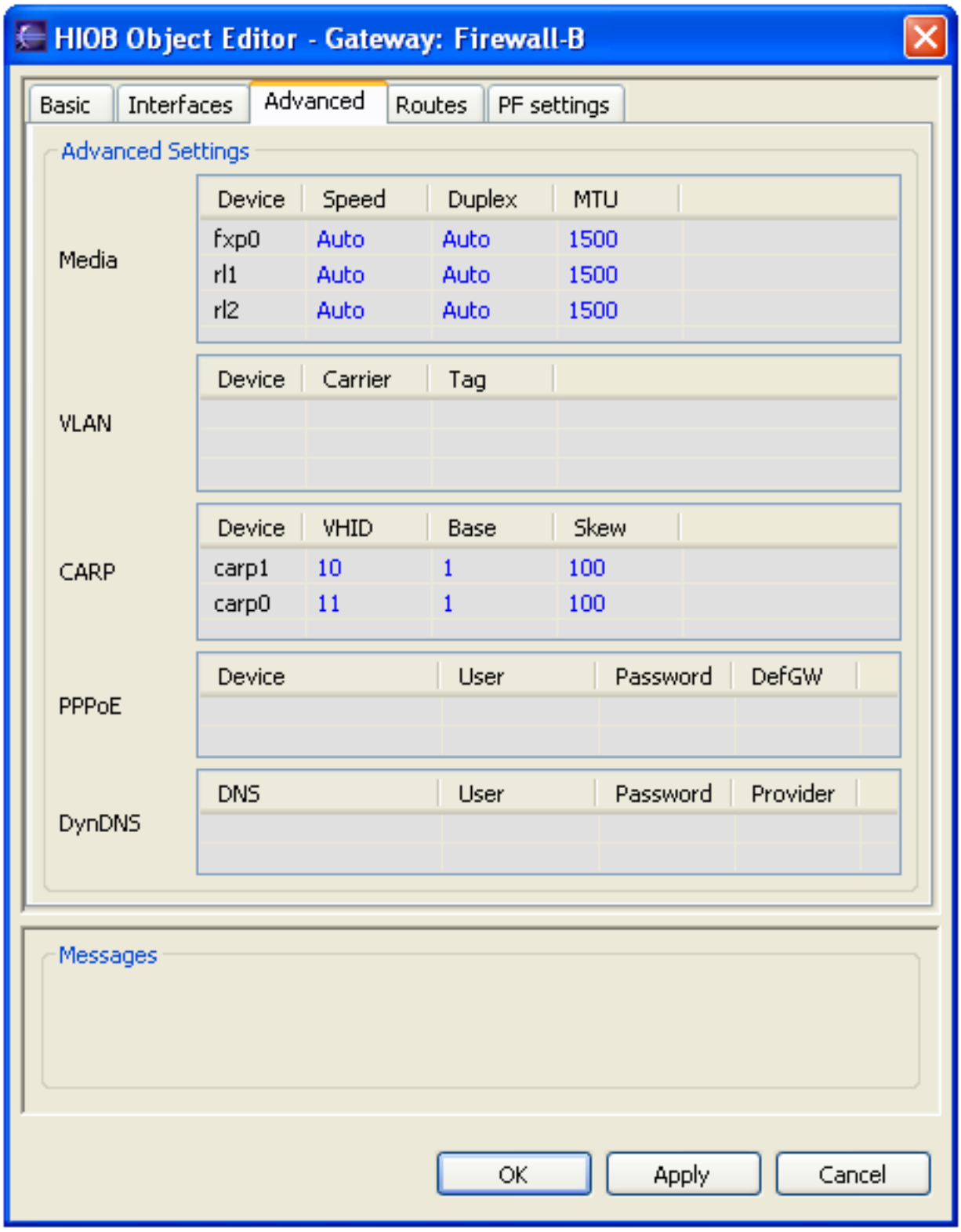


Bild 7.5 'Firewall-B' CARP-Parameter

Die Ausführung von 'Preview Configuration' für Firewall-A sollte unter 'Files' jetzt u.a. folgende Einträge zeigen:

```
...
------------------ myname
Firewall-A

------------------ hostname.fxp0
#@MNE:ext
inet 192.168.10.79 255.255.255.0 NONE

------------------ hostname.carp1
!ifconfig fxp0 up
inet 192.168.10.81 255.255.255.0 192.168.10.255 vhid 10 advbase 1 advskew 10 pass _zZz_10_xXx_

------------------ hostname.rl1
#@MNE:int
inet 10.5.0.1 255.255.240.0 NONE

------------------ hostname.carp0
!ifconfig rl1 up
inet 10.5.0.3 255.255.240.0 10.5.15.255 vhid 11 advbase 1 advskew 10 pass _zZz_11_xXx_ carpdev

------------------ hostname.pfsync0
up syncdev rl2
...
```

1.7.4. Regeln

NAT

NAT-Regel 1 bildet alle internen, privaten IP-Adressen (Intranet) auf die externe IP-Adresse der Firewall ab, in diesem Fall die IP-Adresse des externen CARP-Interface.

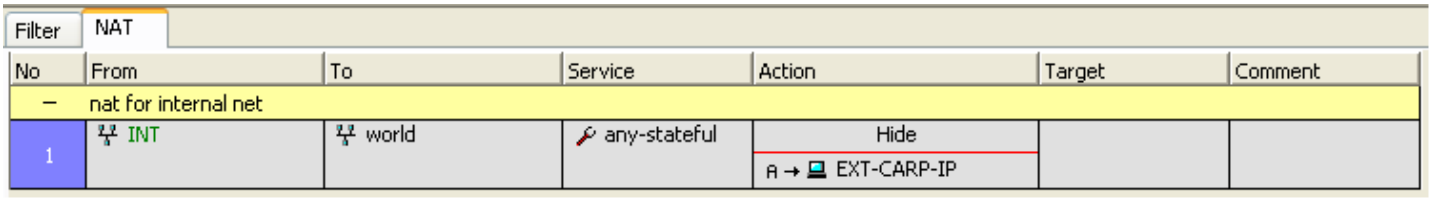


Bild 7.6 - Rezept-7-NAT-Regeln

Filter

Die neue Filterregel 2 schaltet 'pfsync' frei. In Regel 4 wird zusätzlich der Dienst 'carp' eingetragen. Da Pakete, auf die NAT-Regel 1 zutrifft, mit Absenderadresse EXT-CARP-IP weitergeleitet werden, wird in Regel 4 in Spalte 'From' 'EXT-CARP-IP'eingetragen.

Filter | NAT

No	From	To	Service	Action	Log	Target	Comment
–	firewall administration						
1	INT	INT-CARP-IP INT-IP	https ssh	Pass			
–	pfsync						
2	SYNC	SYNC-IP	pfsync	Pass			
–	no more communication with firewall						
3	any	Firewall-IP		Drop			
–	from inside to outside						
4	EXT-CARP-IP INT	world	carp http https imap pop3	Pass			
–	final block						
5	any	any		Drop			

Bild 7.7 - Rezept-7-Filter-Regeln

1.7.5. Download

rezept-7 [../download/rezept-7.xml]

1.8. NAT vor dem VPN-Tunnel

In manchen Netzwerk-Topologien ist es erforderlich, NAT auf den Datenverkehr anzuwenden, bevor er in den Tunnel eintritt. Am anderen Ende des Tunnels erscheint der Datenverkehr dann mit den entsprechend geänderten Quell-Adressen.

1.8.1. Skizze

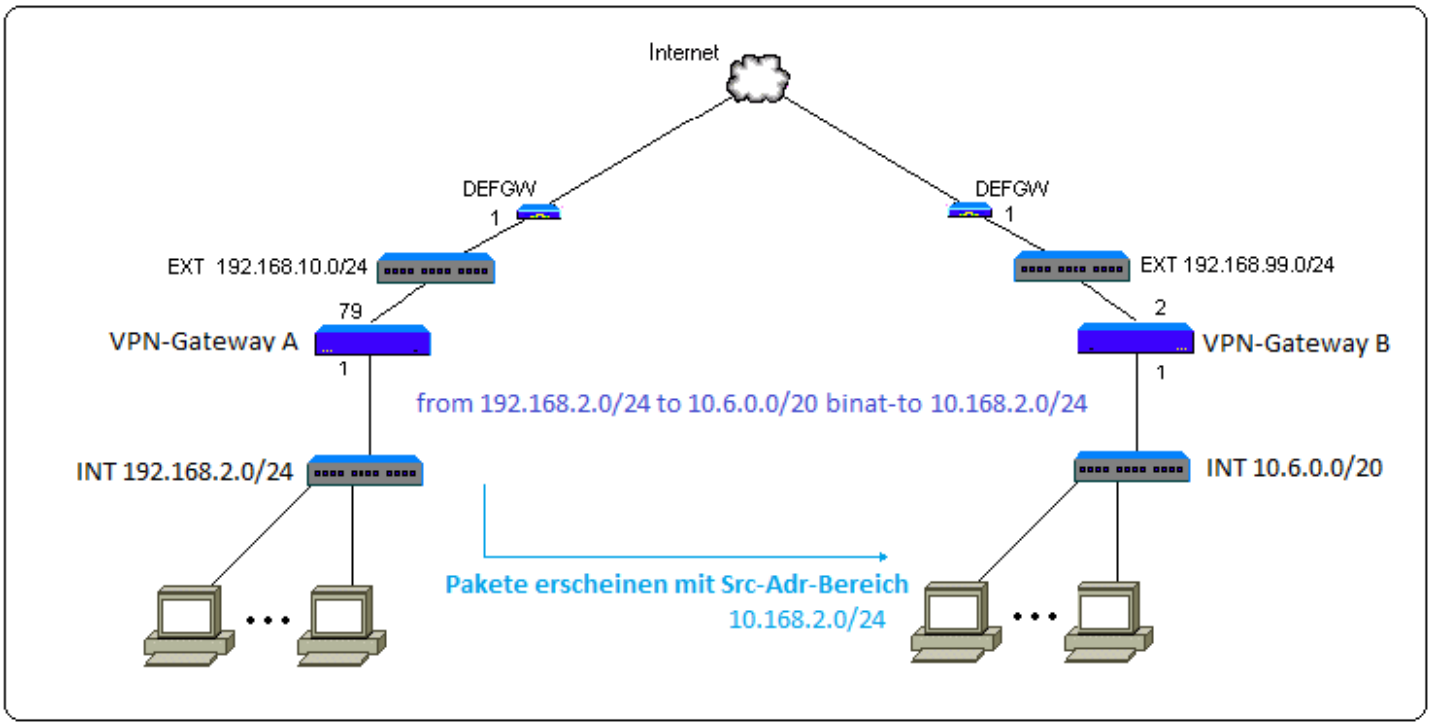


Bild 8.1 NAT vor dem VPN-Tunnel

1.8.2. Konfigurationsziel

- NAT vor dem VPN-Tunnel

In dem folgenden Rezept hat das lokale Subnetz von 'VPN-Gateway A' die Adresse 192.168.2.0/24, aber der gesamte Verkehr von A nach B soll im lokalen Subnetz von 'VPN-Gateway B' (10.6.0.0/20) so aussehen, als würde er von 10.168.2.0/24 kommen (siehe OpenBSD/ipsec.conf, Abschnitt 'OUTGOING NETWORK ADDRESS TRANSLATION '" [http://www.openbsd.org/cgi-bin/man.cgi?query=ipsec.conf&sektion=5&arch=i386&apropos=0&manpath=OpenBSD+Current]).

1.8.3. Objekte

Zunächst werden vier globale Objekte erzeugt. Sie erhalten ihre Adressen durch das entsprechende 'Gateway'-Objekt. Das Objekt 'internal-gateA-nat' wird im 'VPN-Gateway A' dem 'ipsec'-Interface zugeordnet und erhält damit die übersetzte (NAT)-Adresse.

- gateA: 'Host'-Objekt als Tunnelendpunkt im VPN-Gateway A
- gateB: 'Host'-Objekt als Tunnelendpunkt im VPN-Gateway B
- internal-gateA-nat: 'Network'-Objekt; repräsentiert das interne Netz von VPN-Gateway A
- internal-gateB: 'Network'-Objekt; repräsentiert das interne Netz von VPN-Gateway B

Dann wird ein statisches 'Network'-Objekt erzeugt. Ihm wird explizit die NAT-Adresse zugewiesen (10.168.2.0/24).

- internal-gateA-ipsec: 'Network'-Objekt; repräsentiert das interne Netz von VPN-Gateway A

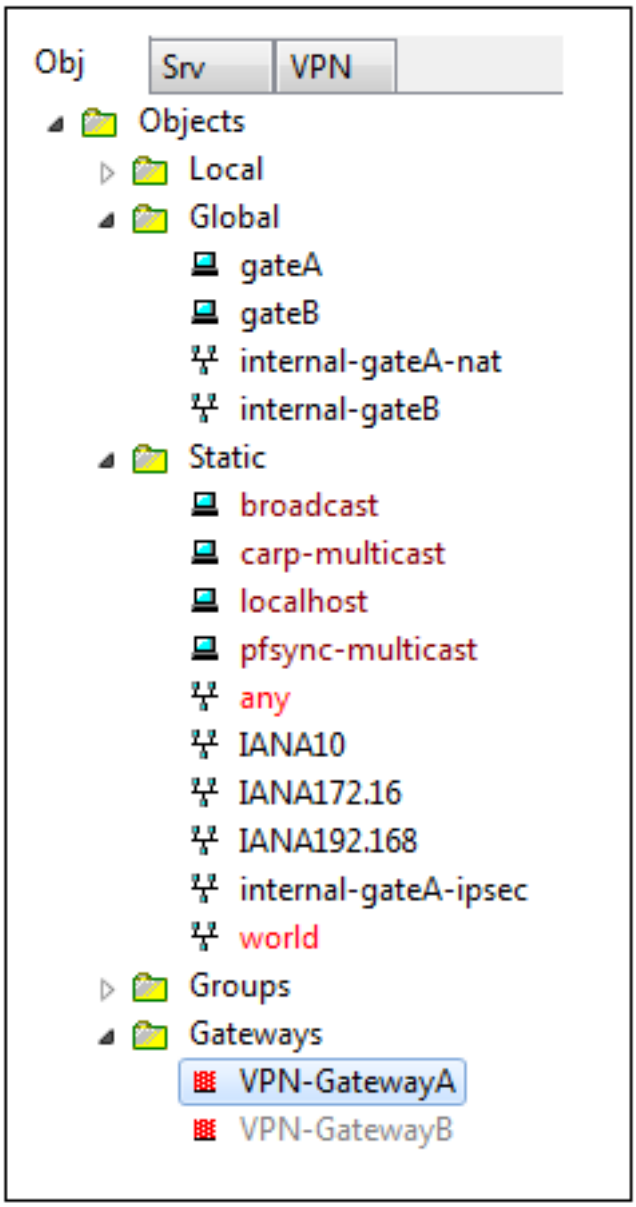


Bild 8.2 'Host'- und 'Network'-Objekte

Jetzt werden die beiden 'Gateway'-Objekte erstellt und ihnen die obigen 'Host'- und 'Network'-Objekte zugewiesen (Bild 8.3/8.4).

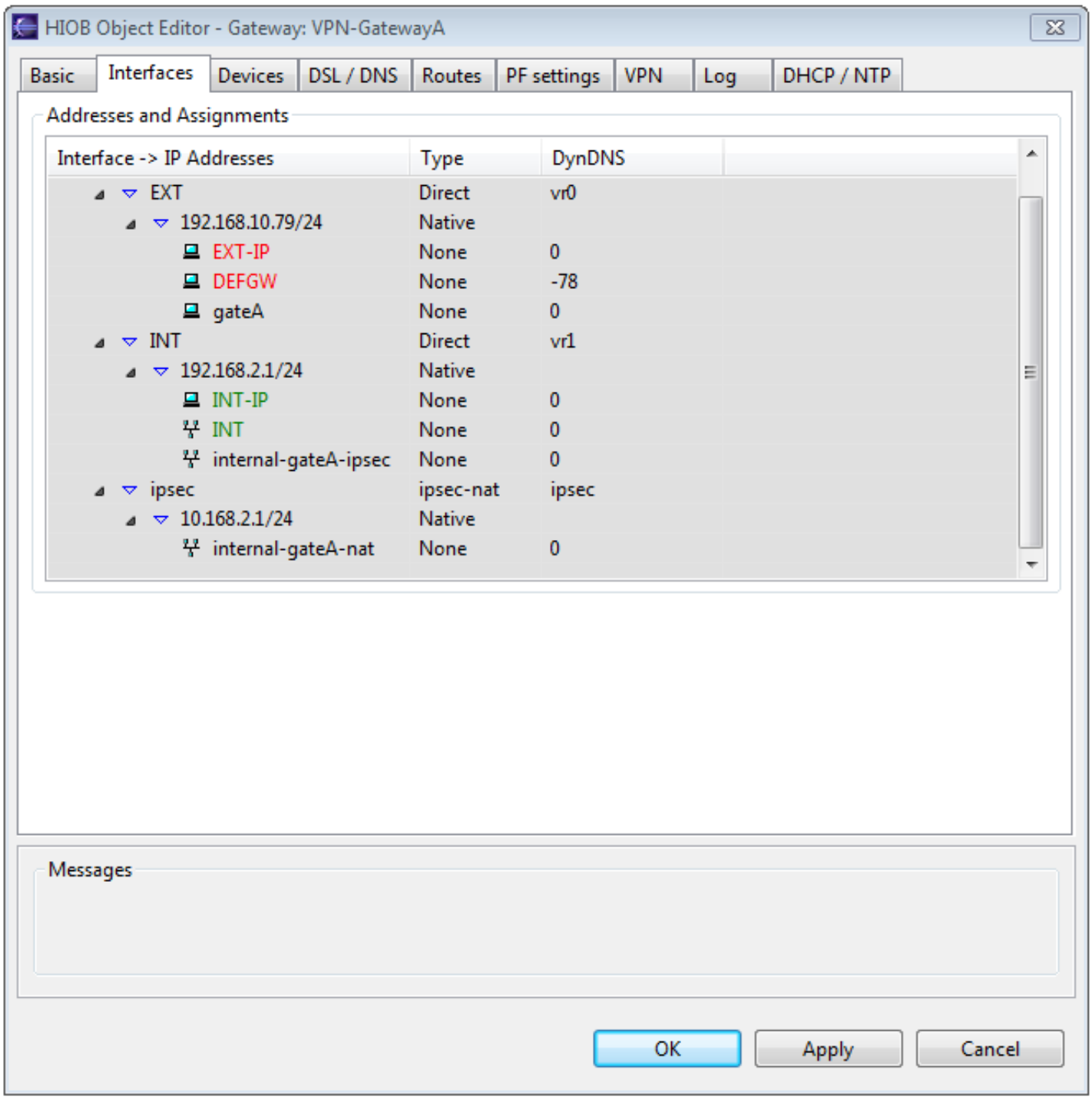


Bild 8.3 VPN-GatewayA

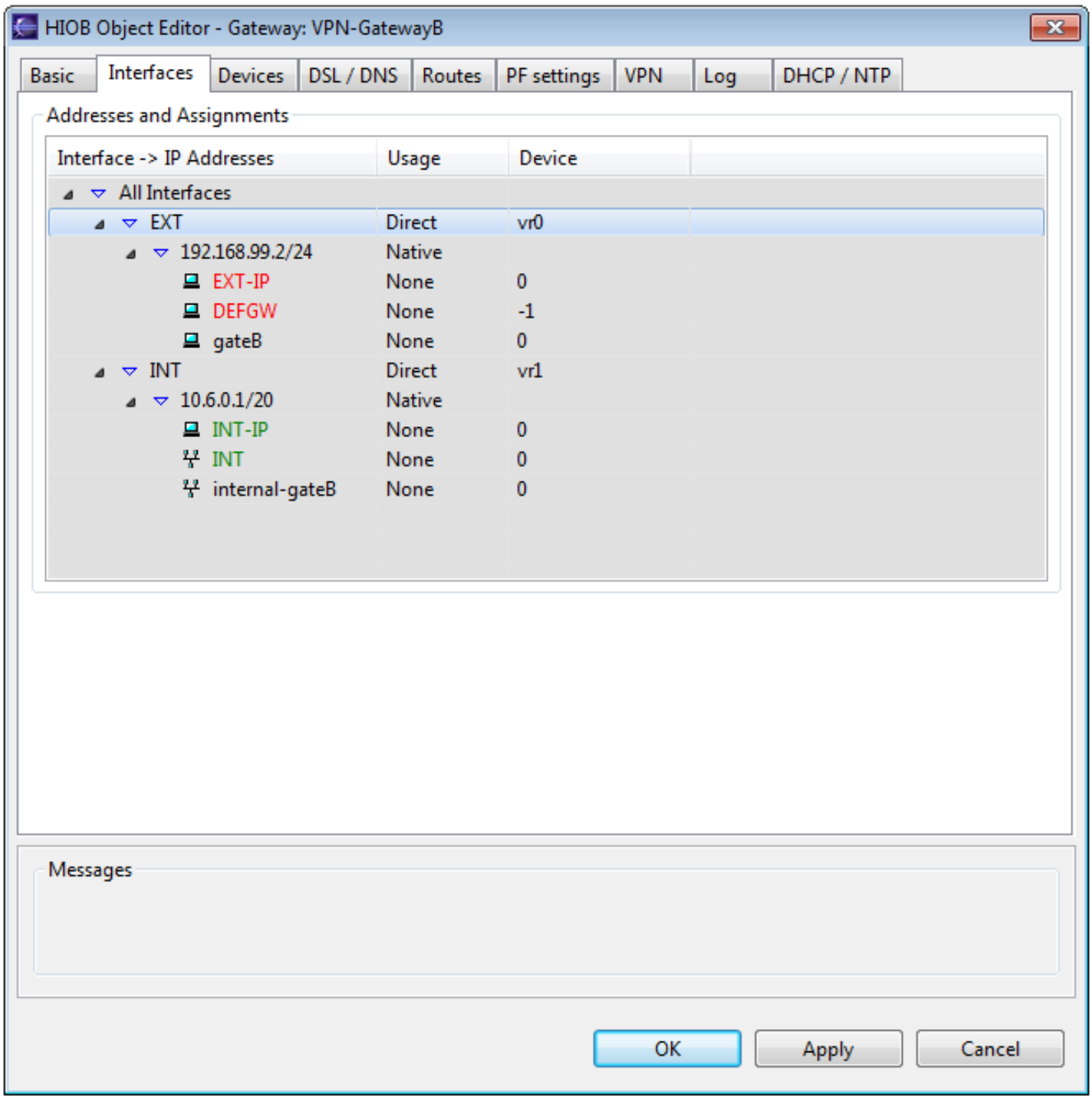


Bild 8.4 VPN-GatewayB

Zum Schluss wird das 'Tunnel'-Objekt erstellt und konfiguriert. Ein 'Keys'-Objekt ('gateA-gateB-key') wird dafür benötigt und muss natürlich auch erstellt werden (Bilder 8.5/8.6/8.7/8.8).

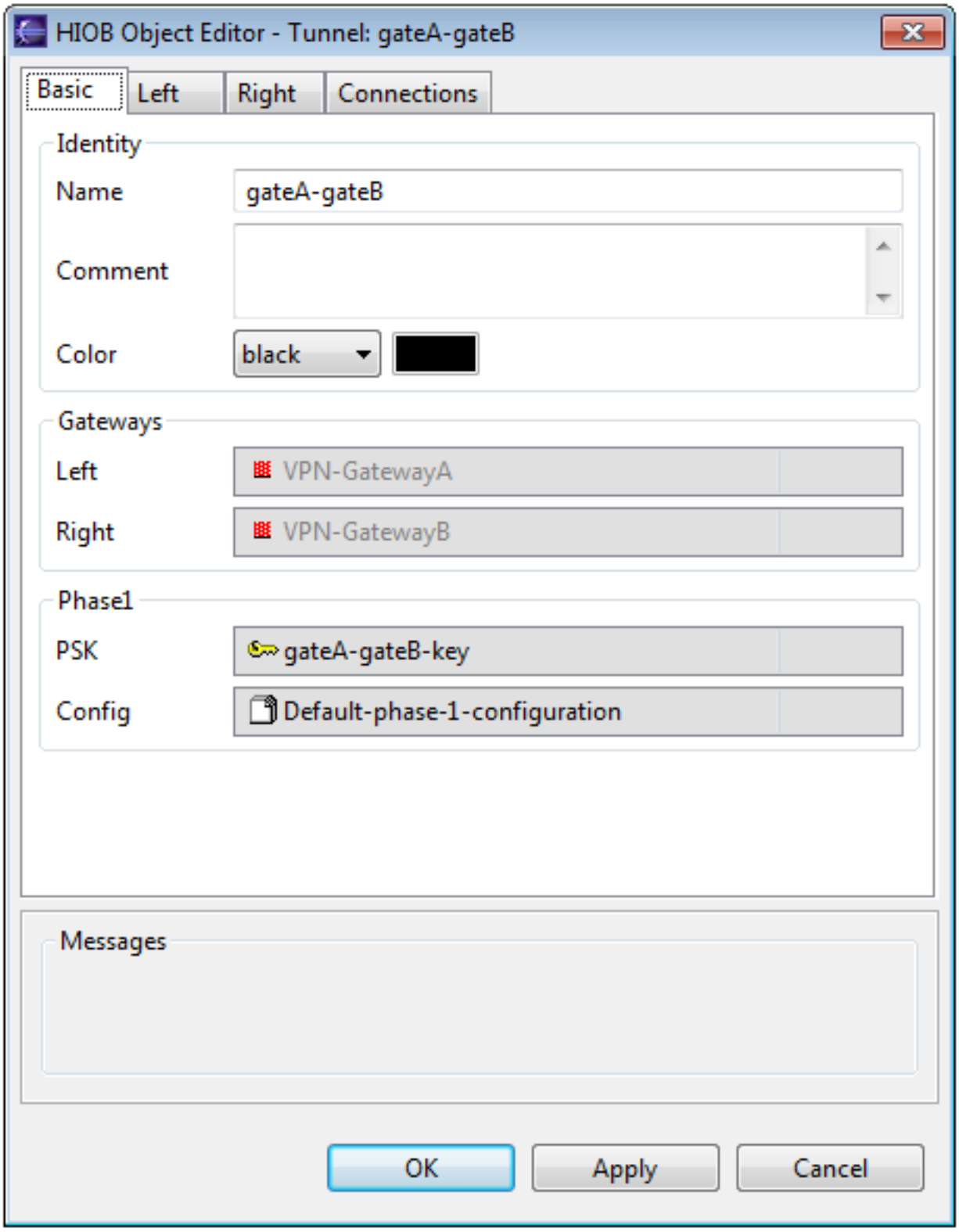


Bild 8.5 Tunnel, Basic

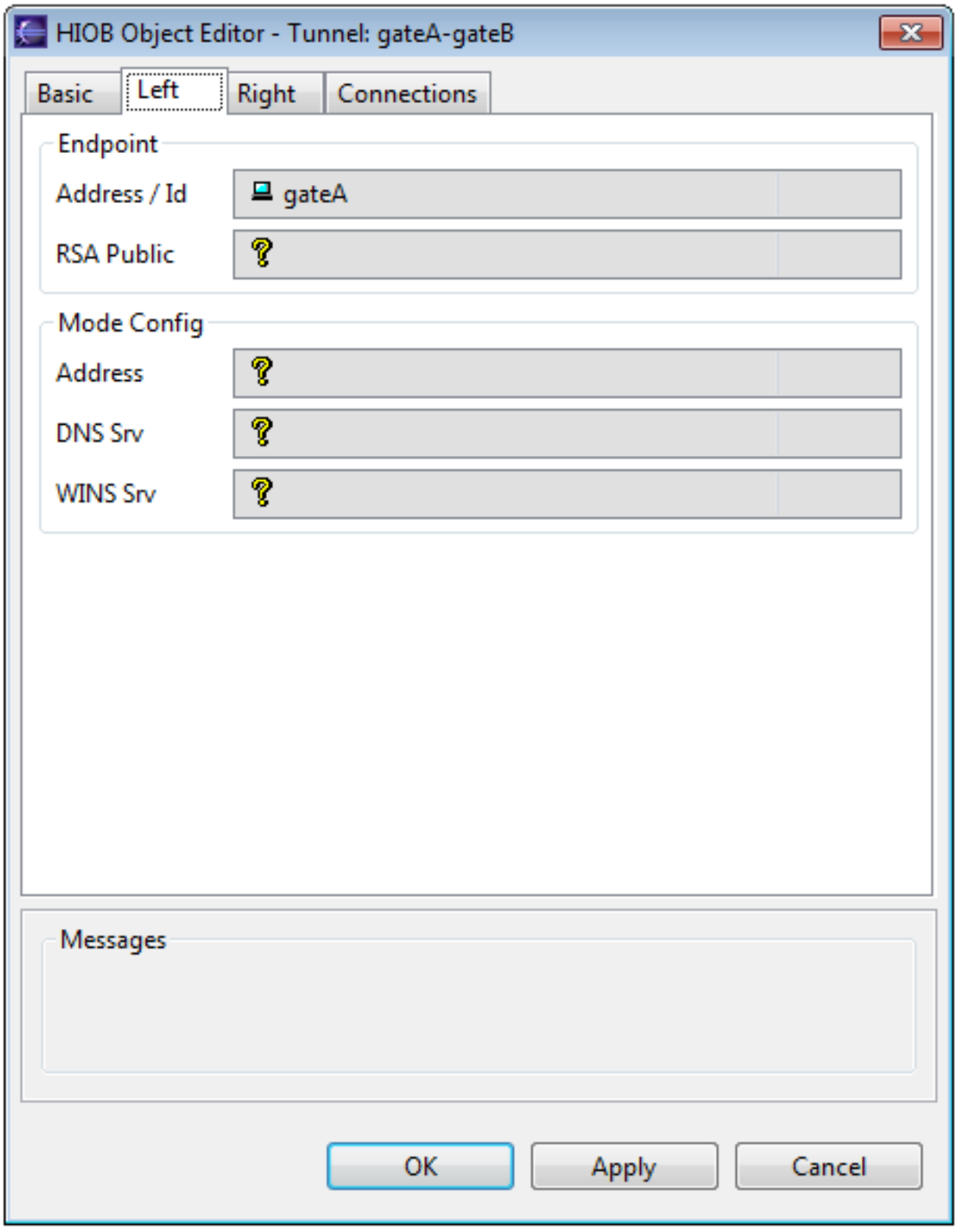


Bild 8.6 Tunnel, Left

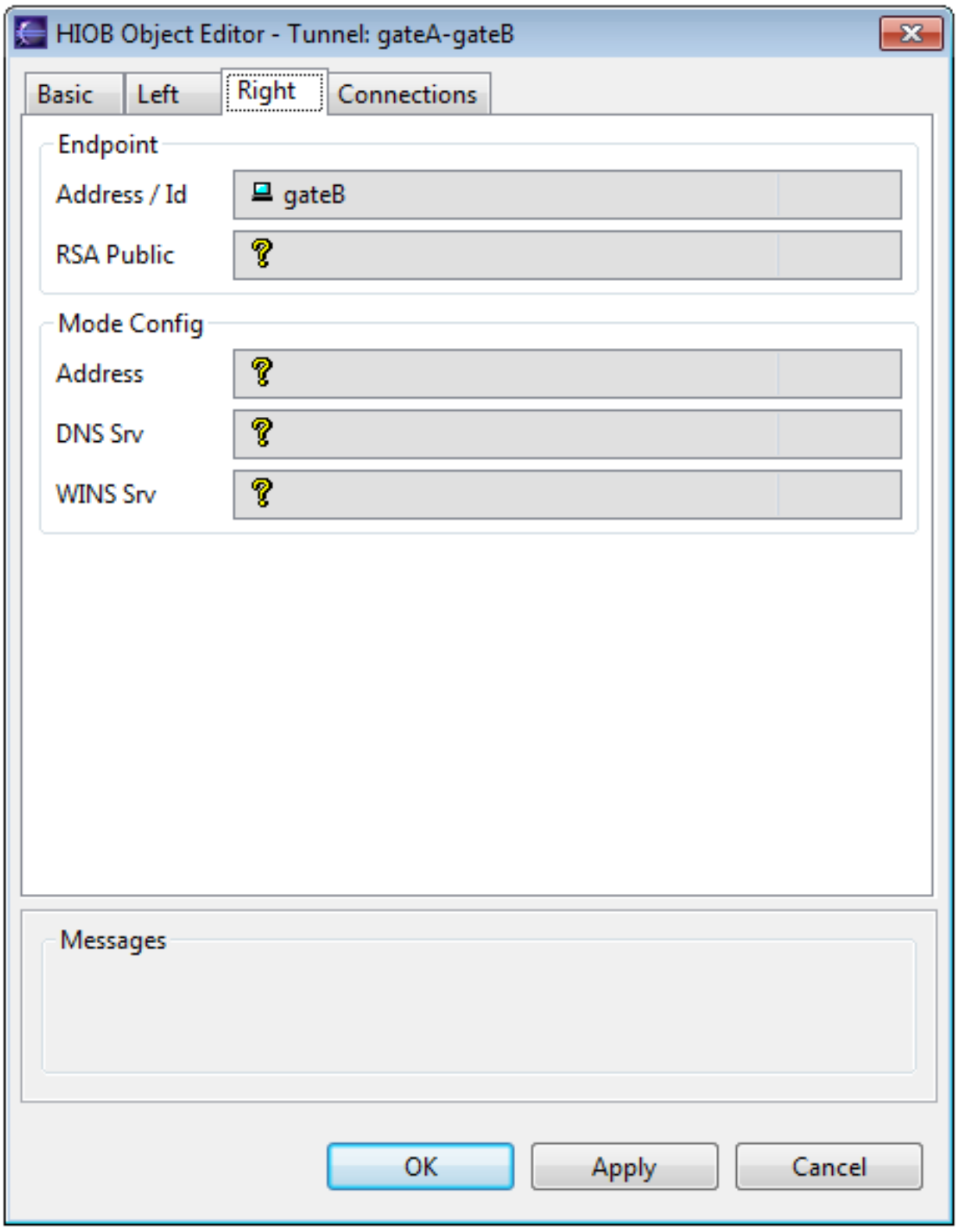


Bild 8.7 Tunnel, Right

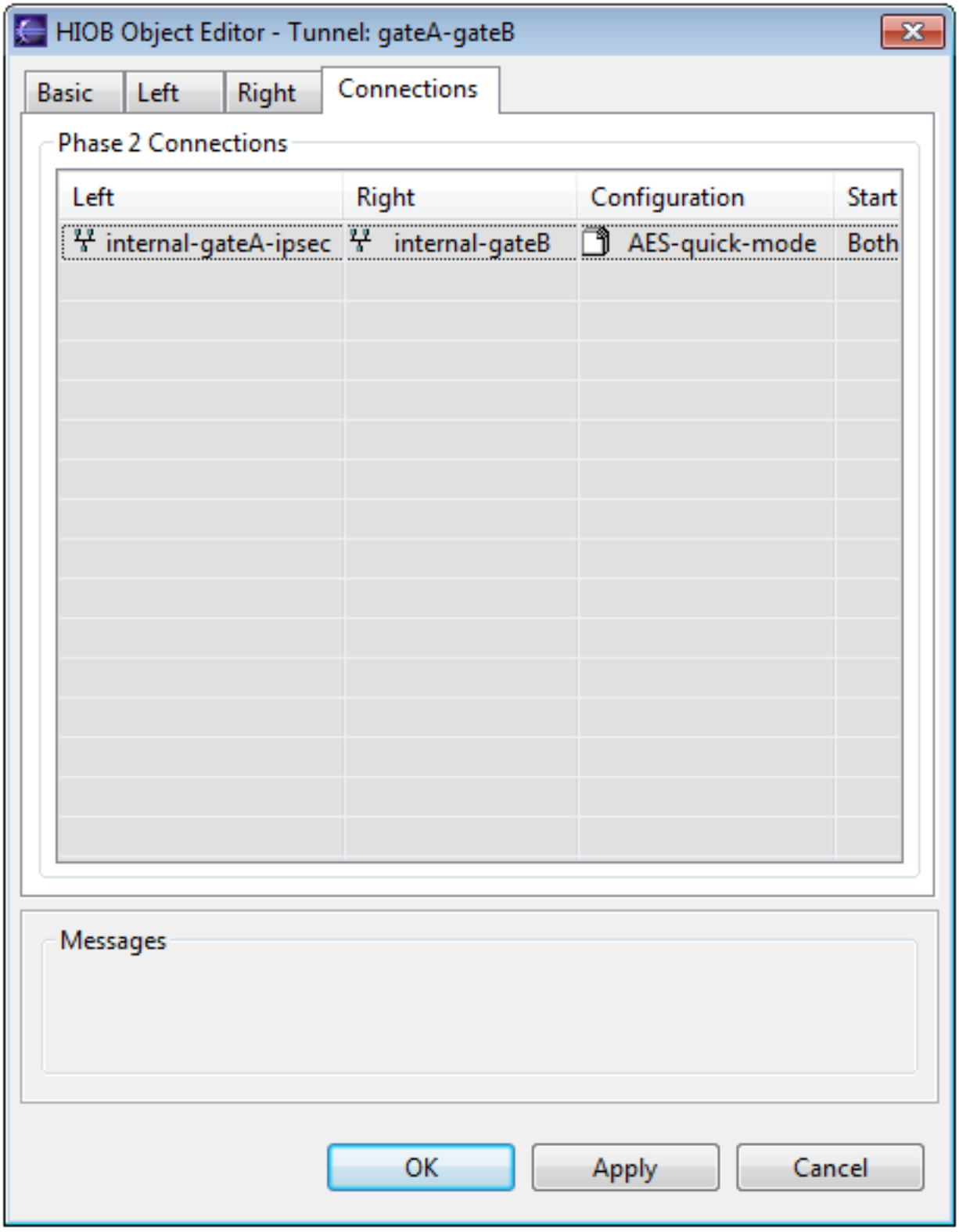
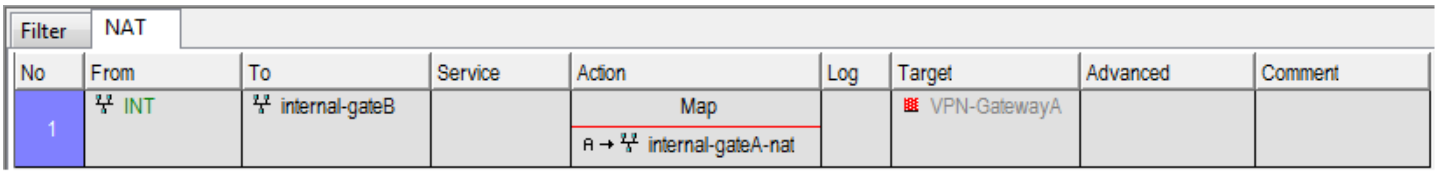


Bild 8.8 Tunnel, Connections

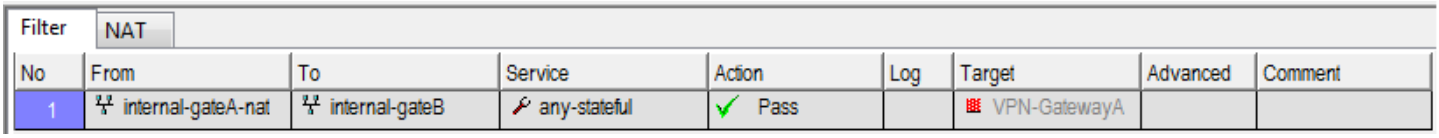
1.8.4. Regeln

Es werden nur die Filter- und NAT-Regeln angezeigt, die für 'NAT vor dem Tunnel' erforderlich sind.



No	From	To	Service	Action	Log	Target	Advanced	Comment
1	INT	internal-gateB		Map internal-gateA-nat		VPN-GatewayA		

Bild 8.9 - Rezept-8-NAT-Regeln



No	From	To	Service	Action	Log	Target	Advanced	Comment
1	internal-gateA-nat	internal-gateB	any-stateful	Pass		VPN-GatewayA		

Bild 8.10 - Rezept-8-Filter-Regeln

Die Ausführung von 'Preview Configuration' für Firewall-A sollte unter 'Files' jetzt u.a. folgende Einträge zeigen:

```
...
------------------ isakmpd.conf
[General]
Retransmits= 5
Exchange-max-time= 120
Listen-on= 192.168.10.79

[Phase 1]
192.168.99.2= gateB

[Phase 2]
Connections=\
        VPN-GatewayA-gateB-0

[internal-gateA-ipsec-REAL-1-ID]
ID-type= IPV4_ADDR_SUBNET
Network= 10.168.2.0
Netmask= 255.255.255.0

[internal-gateA-ipsec-ID]
ID-type= IPV4_ADDR_SUBNET
Network= 192.168.2.0
Netmask= 255.255.255.0

[internal-gateB-ID]
ID-type= IPV4_ADDR_SUBNET
Network= 10.6.0.0
Netmask= 255.255.240.0

# IKE: gateB
[gateB]
Phase=          1
Transport= udp
Local-address= 192.168.10.79
Address= 192.168.99.2
Authentication=
Configuration= Default-phase-1-configuration

# IPSEC: gateB
[VPN-GatewayA-gateB-0]
Phase=          2
ISAKMP-peer= gateB
Configuration= AES-quick-mode
Local-ID= internal-gateA-ipsec-REAL-1-ID
NAT-ID= internal-gateA-ipsec-ID
Remote-ID= internal-gateB-ID

[Default-phase-1-configuration]
```

```
DOI=          IPSEC
EXCHANGE_TYPE= ID_PROT
Transforms= AES-SHA,3DES-SHA

[AES-quick-mode]
DOI=          IPSEC
EXCHANGE_TYPE= QUICK_MODE
Suites=          QM-ESP-AES-SHA-PFS-SUITE
...
```

1.8.5. Download

rezept-8 [../download/rezept-8.xml]