

Anleitung zur Konfiguration von Policy based Rules zur Einrichtung folgender Anforderung

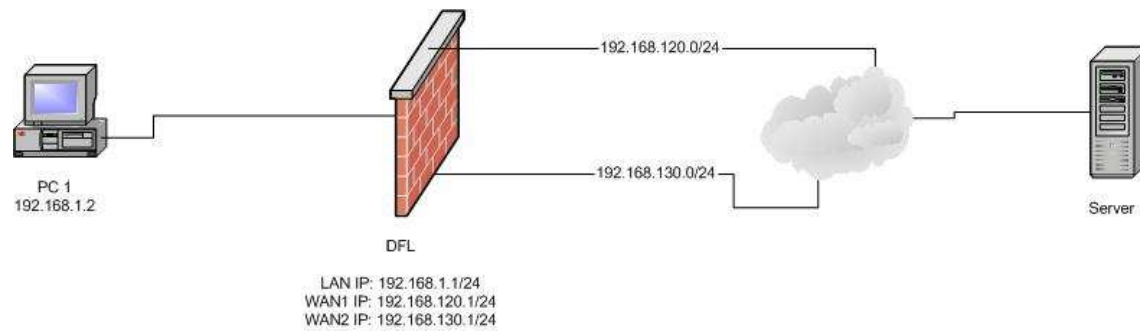
**Ausgehender Datenverkehr der an Port 80 adressiert ist (http), soll immer über WAN2
geführt werden, während Telnet über WAN1 geleitet werden sollen.**

Um diese Anleitung nutzen zu können werden Kenntnisse über Routing, TCP, UDP und Paketfilterung
vorausgesetzt.

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



Testumgebung:



Ausgehender Traffic:

WAN1 -> telnet

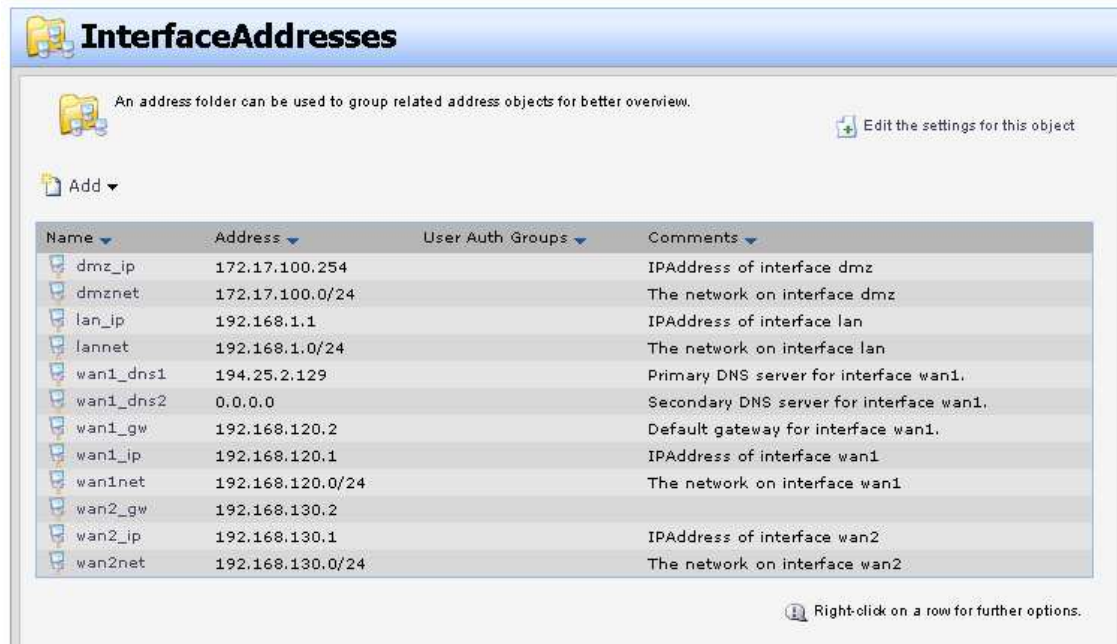
WAN2 -> http

Ziel der Konfiguration:

Aus dem LAN Netz ausgehender Datenverkehr mit dem Zielpport 23 soll über WAN1 geleitet werden, während Datenverkehr an Port 80 ausschließlich über WAN 2 geleitet werden soll.

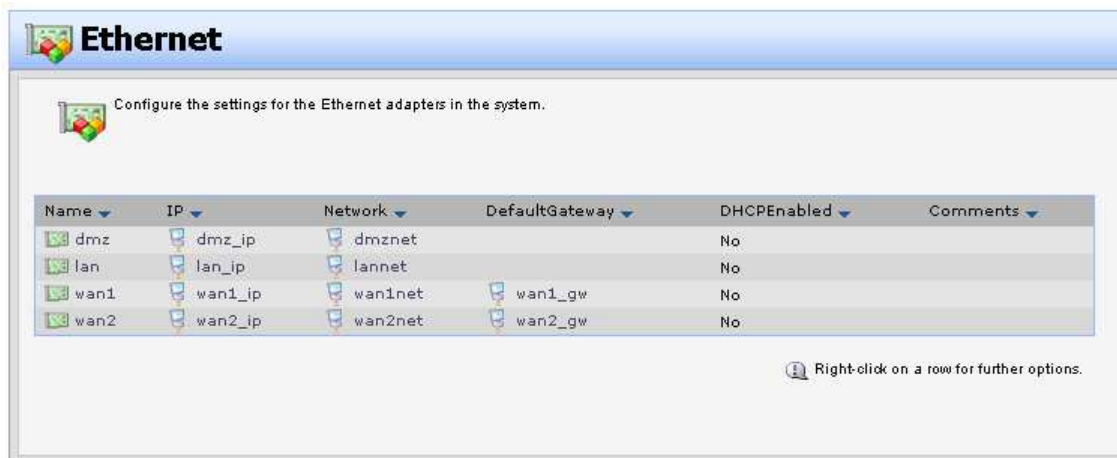
Anmerkung: Die Wolke wurde durch einen L3 Switch ersetzt. Für den Rückweg sind Routen erforderlich.

Zunächst wurden unter „Objects-Address Book-InterfaceAddresses“ die IP Adressen der Firewall an die Netzwerkumgebung angepasst:



Name	Address	User Auth	Groups	Comments
dmz_ip	172.17.100.254			IPAddress of interface dmz
dmznet	172.17.100.0/24			The network on interface dmz
lan_ip	192.168.1.1			IPAddress of interface lan
lannet	192.168.1.0/24			The network on interface lan
wan1_dns1	194.25.2.129			Primary DNS server for interface wan1.
wan1_dns2	0.0.0.0			Secondary DNS server for interface wan1.
wan1_gw	192.168.120.2			Default gateway for interface wan1.
wan1_ip	192.168.120.1			IPAddress of interface wan1
wan1net	192.168.120.0/24			The network on interface wan1
wan2_gw	192.168.130.2			
wan2_ip	192.168.130.1			IPAddress of interface wan2
wan2net	192.168.130.0/24			The network on interface wan2

Danach erfolgt die Zuweisung der WAN Gateways im Menü Interfaces Ethernet. (Hier die Übersicht des Menüs „Interfaces-Ethernet“.)



Name	IP	Network	DefaultGateway	DHCPEnabled	Comments
dmz	dmz_ip	dmznet		No	
lan	lan_ip	lannet		No	
wan1	wan1_ip	wan1net	wan1_gw	No	
wan2	wan2_ip	wan2net	wan2_gw	No	

Nachdem die Interfaces und ihre Adressen definiert sind, müssen die nötigen Routing Informationen angelegt werden. Dazu zunächst ein Blick auf die im Auslieferungszustand angelegte Main Routing Table:

main (read-only)

The system has a predefined main routing table. Alternate routing tables can be defined by the user. [Edit the settings for this object](#)

Add ▾

Type ▾	Interface ▾	Network ▾	Gateway ▾	LocalIP ▾	Metric ▾	RouteMonitor ▾	Comments ▾
Route	wan1	wan1net			100	No	Direct route for network wan1net over interface wan1.
Route	wan1	all-nets	wan1_gw		100	No	Default route over interface wan1.
Route	dmz	dmznet			100	No	Direct route for network dmznet over interface dmz.
Route	lan	lanet			100	No	Direct route for network lanet over interface lan.
Route	wan2	wan2net			100	No	Direct route for network wan2net over interface wan2.
Route	wan2	all-nets	wan2_gw		100	No	Default route over interface wan2.

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

Parallel zu der Main Routing Table wird eine weitere Routing Table für die neue http über WAN2 Route erstellt. Die Table trägt in unserem Beispiel die Bezeichnung „route_wan2_http“ und beinhaltet eine Route.

route_wan2_http

The system has a predefined main routing table. Alternate routing tables can be defined by the user. [Edit the settings for this object](#)

Add ▾

Type ▾	Interface ▾	Network ▾	Gateway ▾	LocalIP ▾	Metric ▾	RouteMonitor ▾	Comments ▾
Route	wan2	all-nets	wan2_gw		100	No	

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

Hier sehen Sie die oben angelegte Route im Detail. Diese Route definiert, dass über Interface wan2 mit dem Gateway „wan2_gw“ auf „all-net“ zugegriffen werden kann.

Route

General Proxy ARP Monitor

General

A route defines what interface and gateway to use in order to reach a specified network.

Interface: wan2

Network: all-nets

Gateway: wan2_gw

Local IP Address: (None)

Metric: 100

Comments

Comments:

OK Cancel

Hier sehen Sie die beiden Routing Tables nach Abschluss der Routing Konfiguration. Bitte achten Sie dabei darauf die zweite Routing Table „route_wan2_http“ mit dem „Ordering“ „First“ zu versehen, damit sichergestellt ist, dass diese Routing Table zuerst Verwendung findet.

Routing Tables

Configure the routing tables of the system. The system has a predefined main routing table. Alternate routing tables can be defined by the user.

Add

Name	Ordering	RemoveInterfaceIPRoutes	Comments
main	Only	No	The main routing table of the system.
route_wan2_http	First	Yes	

Right-click on a row for further options.

Nun erfolgt die Konfiguration der eigentlichen Routing Policy. Unter dem Menüpunkt „Routing-Routing Rules“ wird eine Rule angelegt, welche besagt das Pakete vom Interface „lan“ in das Internet (über Interface „wan1“) die Route „route_wan2_http“ für ausgehende Verbindungen nutzen müssen. Eingehende Pakete werden dann über die Routing Tabelle „main“ zurückgeleitet. (Dies wird benötigt um einen Weg in das lannet zu finden).

pbr_http_wan2

General

A Routing Rule forces the use of a routing table in the forward and/or return direction of traffic on a connection. The ordering parameter of the routing table determines if it is consulted before or after the main routing table.

Name: pbr_http_wan2

Forward Table: route_wan2_http

Return Table: main

Service: http

Schedule: (None)

Address Filter

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

	Source	Destination
Interface:	lan	wan1
Network:	lannet	all-nets

Hier die angelegte Policy noch einmal nach Abschluss der Konfiguration.

Routing Rules

Configure a policy for what routing tables are to be used for what network traffic.

Add

#	Name	SourceInterface	SourceNetwork	DestinationInterface	DestinationNetwork	Service	Comments
1	pbr_http_wan2	lan	lannet	wan1	all-nets	http	

Right-click on a row for further options.

Zuletzt legen Sie bitte noch die benötigten „IP Rules“ unter „Rules-IP Rules“ an. (Anleitungen zur Konfiguration von Port Weiterleitungen finden Sie unter http://ftp.dlink.de/dfi/dfi-800/documentation/DFL-800_Howto_de_Video_portfreigabe-LAN1-LAN2.zip.)

IP Rules

IP Rules are used to filter IP-based network traffic. In addition, they provide means for address translation as well as Server Load Balancing.

Add

#	Name	Action	SourceInterface	SourceNetwork	DestinationInterface	DestinationNetwork	Service
1	ping_fw	Allow	lan	lannet	core	lan_ip	ping-inbound
2	lan_to_wan1						
3	lan_to_wan2						

Right-click on a row for further options.

lan_to_wan1

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 object

Add

#	Name	Action	SourceInterface	SourceNetwork	DestinationInterface	DestinationNetwork	Service
1	drop_smb-all	Drop	lan	lannet	wan1	all-nets	smb-all
2	allow_ping-outbound	NAT	lan	lannet	wan1	all-nets	ping-out
3	allow_ftp-passthrough	NAT	lan	lannet	wan1	all-nets	ftp-pass
4	allow_standard	NAT	lan	lannet	wan1	all-nets	all_tcpuc

Right-click on a row for further options.

lan_to_wan2

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 object

Add

#	Name	Action	SourceInterface	SourceNetwork	DestinationInterface	DestinationNetwork	Service
1	http_to_wan2	Allow	lan	lannet	wan2	all-nets	http
2	dns_to_wan2	Allow	lan	lannet	wan2	all-nets	dns-all

Right-click on a row for further options.

