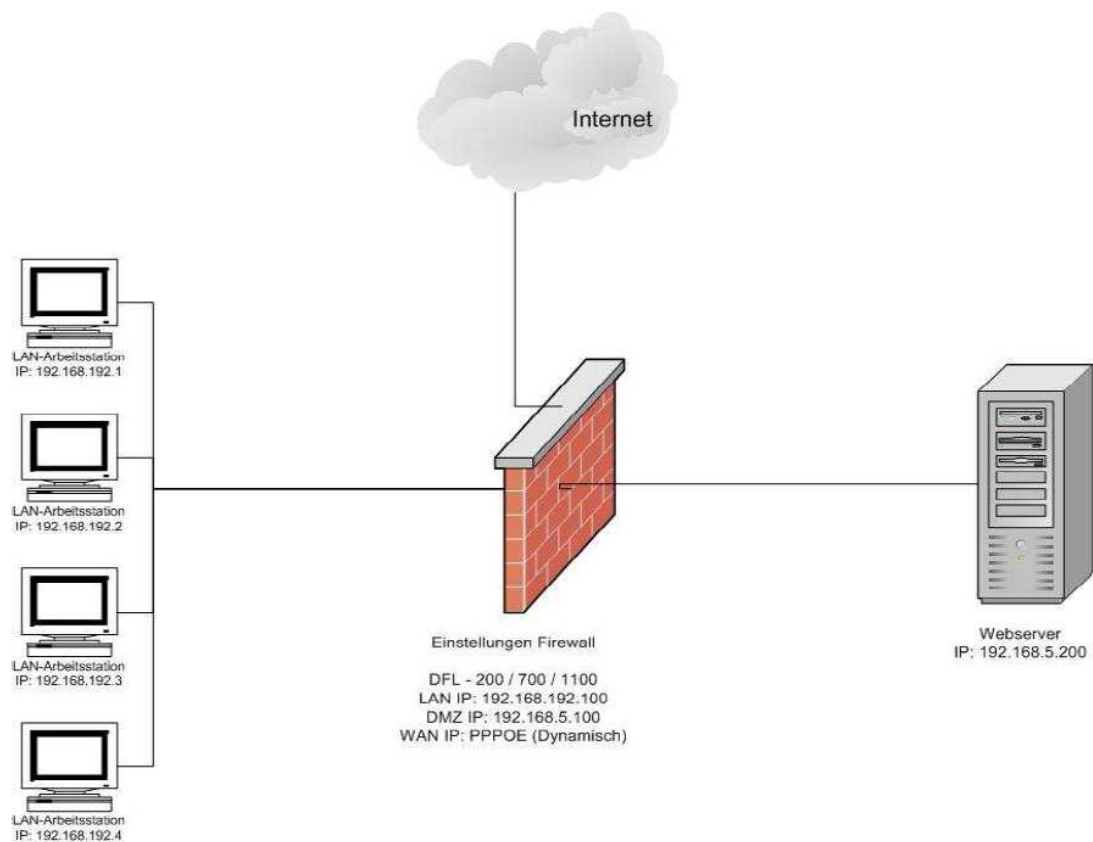


Port-Freigaben und Port-Weiterleitungen

Testaufbau:



Port-Freigaben zwischen LAN und DMZ

1. Klicken Sie auf „Firewall/Policy“ und auf „LAN -> DMZ“.

Firewall Policy

Select which policy to edit:

- [Global policy parameters](#)
- [LAN->WAN](#) policy - 4 rules, NAT enabled
- [WAN->LAN](#) policy - 0 rules
- [LAN->DMZ](#) policy - 3 rules
- [DMZ->LAN](#) policy - 0 rules
- [WAN->DMZ](#) policy - 0 rules
- [DMZ->WAN](#) policy - 4 rules, NAT enabled

2. Wählen Sie die bereits vorhandenen Regeln nacheinander über „edit“ aus.

LAN->DMZ Policy

Name	Action	Source	Destination	Service	Move
#1 allow_ping-outbound	Allow	Any	Any	ping-outbound	↓ [Edit]
#2 allow_ftp-passthrough	Allow	Any	Any	ftp-passthrough	↑↓ [Edit]
#3 allow_standard	Allow	Any	Any	All Protocols	↑ [Edit]

[Add new]

Order of evaluation ↓

3. Löschen Sie die Regeln danach durch die Auswahl von „Delete this rule“.

Delete this rule



4. Danach wählen Sie bitte „add new“ aus.

LAN->DMZ Policy					
Name	Action	Source	Destination	Service	Move
[Add new]					

↓
Order of evaluation

5. Tragen Sie die folgenden Daten in diese Maske ein.

Somit können alle Geräte im Subnet 192.168.192.0/24 auf die IP-Adresse 192.168.5.200 über Port 80 (http) zugreifen.

Bestätigen Sie die Eingabe durch die Auswahl „Apply“.

Name:

Position: Moves before given position. Blank = last.

Action:

Source Nets:

... Users/Groups: "Any" = Any authenticated

Destination Nets:

... Users/Groups: "Any" = Any authenticated

Leave source and/or destination blank to match everything.

Service:

Custom source ports: Blank = any port

... destination ports:

Schedule:

Intrusion Detection / Prevention:

Mode:

Alerting: Enable IDS/IDP alerting via email for this rule



6. Die Anzeige sollte nun wie folgt aussehen.

LAN->DMZ Policy						
Name	Action	Source	Destination	Service	Move	
#1 DMZ_Webserver	Allow	192.168.192.0/24	192.168.5.200	http-in-all	[Edit]	Order of evaluation ↓
[Add new]						

7. Speichern Sie die kompletten Einstellungen durch Auswahl von „Changes: Activate“



8. Nun können Sie auf die Webseite eines Servers im Netz der DMZ zugreifen. In unserem Beispiel wurde ein Webserver auf der IP-Adresse 192.168.5.200 eingerichtet.



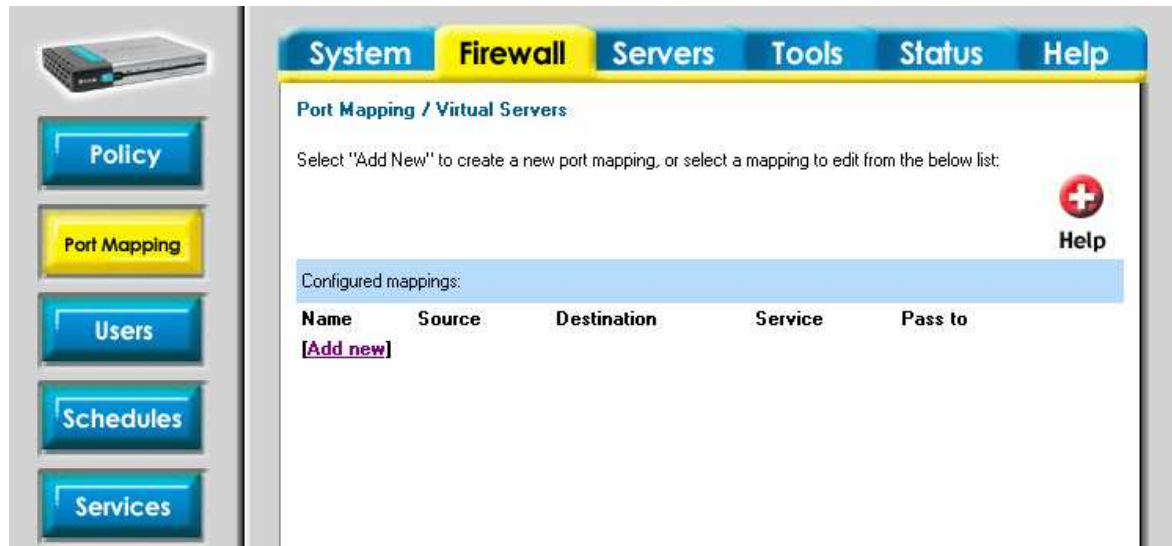
Webserver

D-Link DFL-200, DFL-700, DFL-100



Port-Weiterleitung zwischen WAN und DMZ

1. Klicken Sie auf „/Firewall/Port Mapping/“ und „Add new“



2. Tragen Sie die folgenden Daten in die Maske ein.

Somit werden alle Anfragen vom WAN-Interface auf den Zielport 80 (http) direkt an die angegebene IP-Adresse des Webserver weitergeleitet.

Bestätigen Sie die Eingabe durch die Auswahl von „Apply“

Port Mapping / Virtual Servers

Edit **new** mapping :

Name:

Source Nets: Blank = everyone

... Users/Groups: "Any" = Any authenticated

Destination IP: Blank = WAN interface IP address

Service:

Custom source ports: Blank = any port

... destination ports:

... pass to port: ... and up. Blank=no change.

Pass To:

Schedule:



3. Die Anzeige sollte nun wie folgt aussehen.

Port Mapping / Virtual Servers

Changed settings of "Webserver".

Select "Add New" to create a new port mapping, or select a mapping to edit from the below list:



Configured mappings:

Name	Source	Destination	Service	Pass to	
Webserver	Any	WAN IP	http-in-all	192.168.5.200	[Edit]
[Add new]					

4. Speichern Sie die kompletten Einstellungen durch Auswahl von „Changes: Activate“



Der Webserver ist jetzt über das Internet erreichbar.



Häufige Fehlerquellen:

- Kein oder falsches Gateway auf den Netzwerkgeräten
- Gleiche Subnetze in LAN und DMZ
- Administrative WAN-Konfigurationsfreigabe über http oder https und ein zuzügliches Port-Mapping des http-Ports auf einen Webserver.

