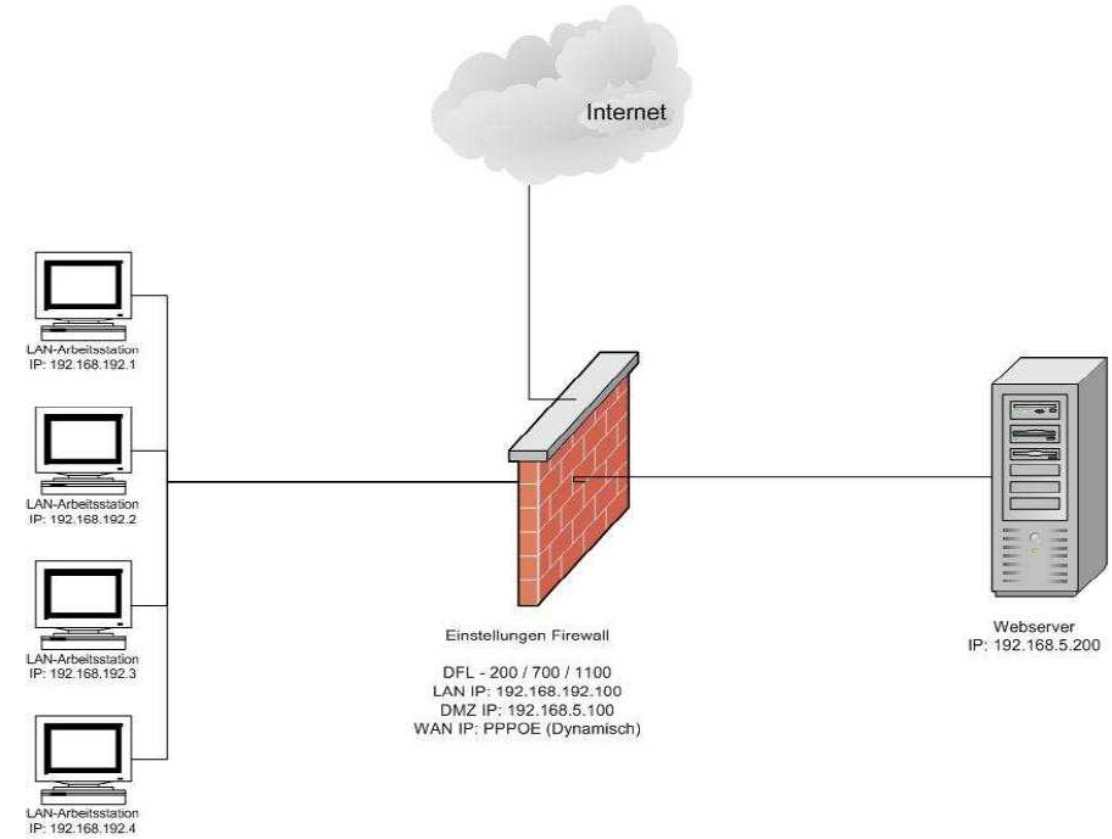
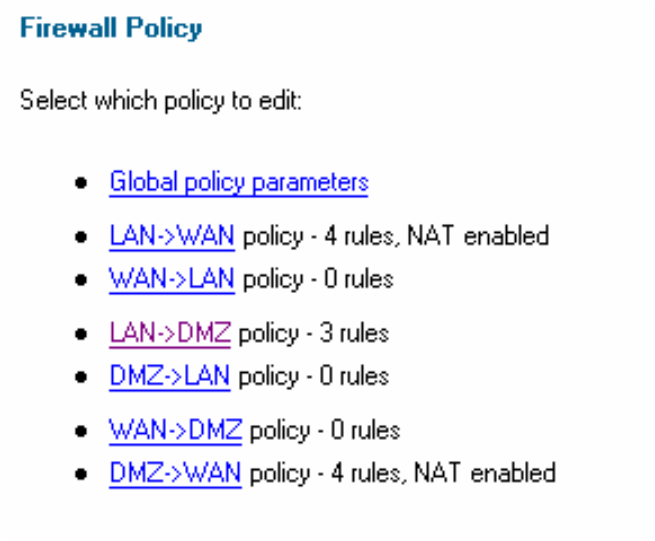
Port-Freigaben und Port-Weiterleitungen

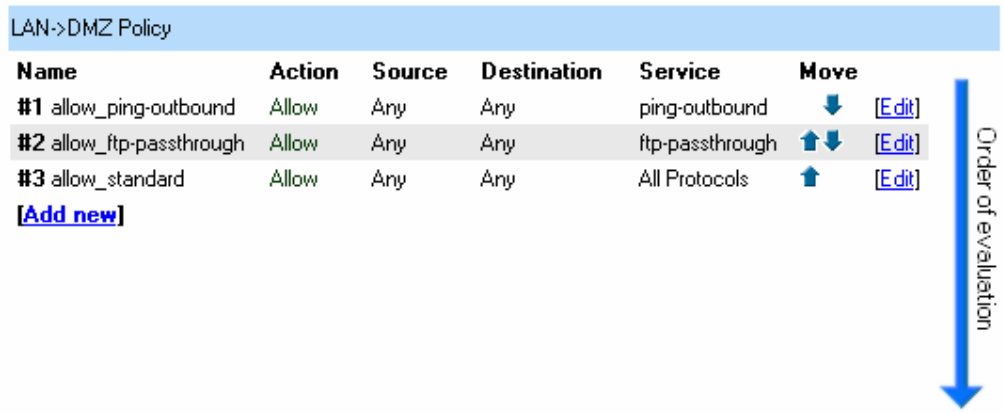
Testaufbau:



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

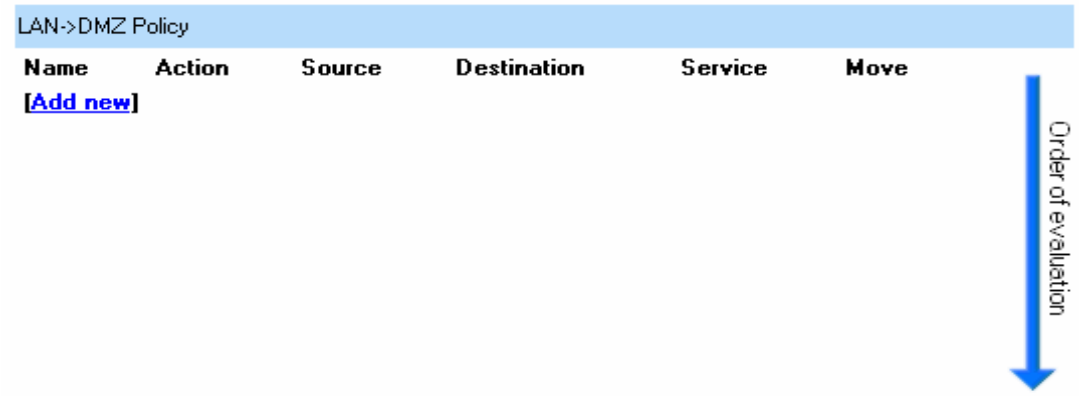


2. Wählen Sie die bereits vorhandenen Regeln nacheinander über „edit“ aus.



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

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



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“.

6. Die Anzeige sollte nun wie folgt aussehen.

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

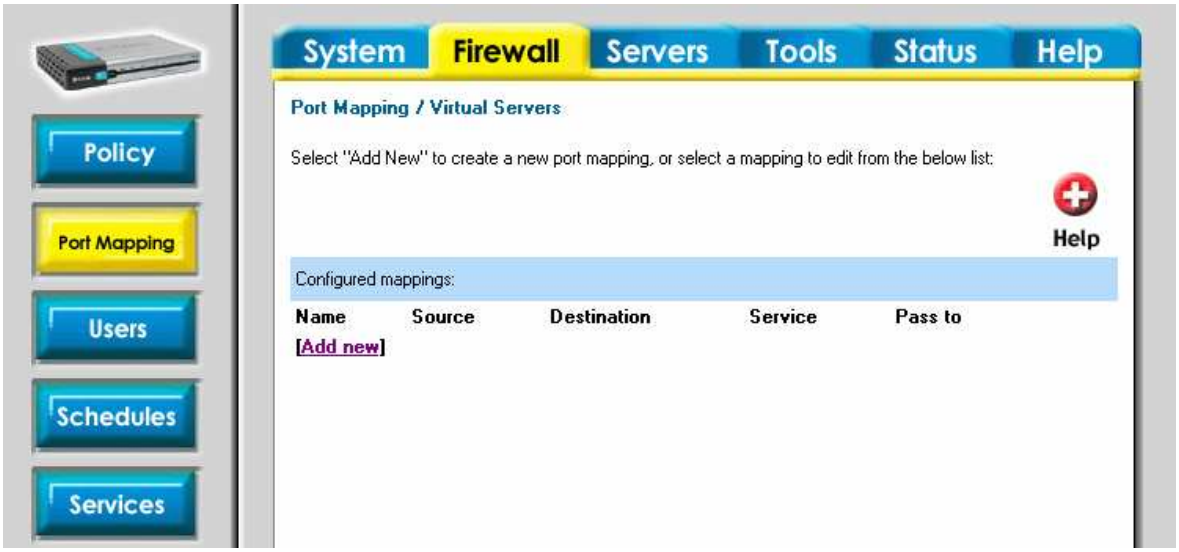
8. Nun können Sie auf die Webseite eines Servers im Netz der DMZ zugreifen. In unserem Beispiel wurde ein Webserver auf der IP-Adresse 192.168.5.200 eingerichtet.

Webserver

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

Port-Weiterleitung zwischen WAN und DMZ

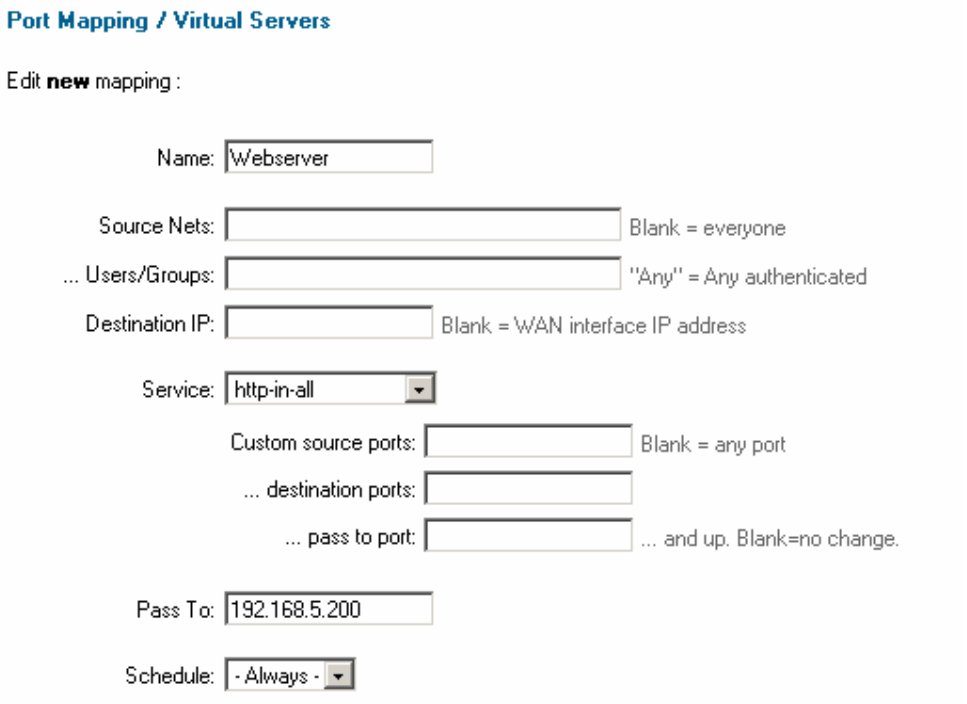
1. Klicken Sie auf „/Firewall/Port Mapping/“ und „Add new“



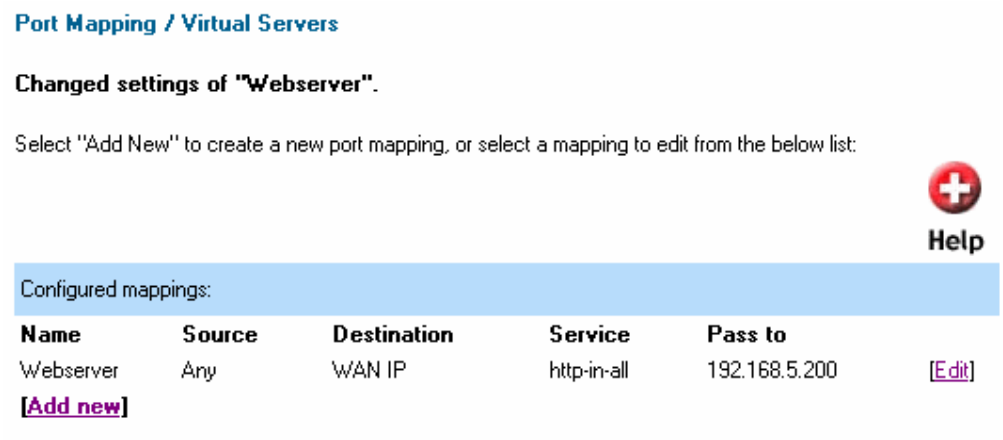
2. Tragen Sie die folgenden Daten in die Maske ein.

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

   Bestätigen Sie die Eingabe durch die Auswahl von „Apply“



3. Die Anzeige sollte nun wie folgt aussehen.



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.