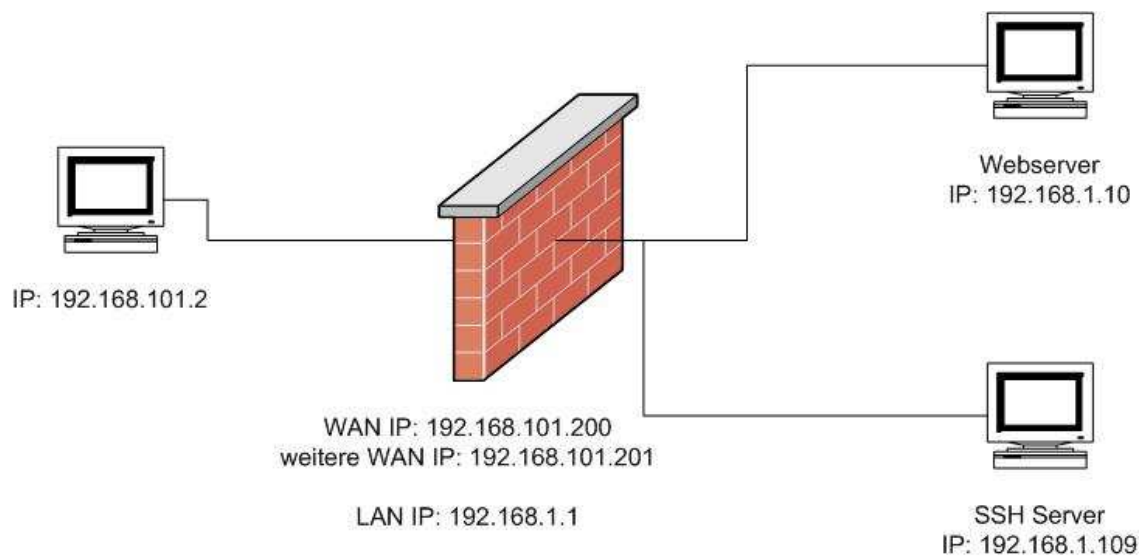


# Benutzung mehrerer IP Adressen am

## WAN - Interface

## Testumgebung:



Realisiert werden soll:

192.168.101.200 -> 192.168.1.109 SSH  
192.168.101.201 -> 192.168.1.10 Webserver

1.) Tragen Sie die zusätzliche IP Adresse unter „System/Routing“ durch „Add new“ ein.

### Routing Table

Edit **192.168.101.201/255.255.255.255** route:

Interface:

Network:

Subnet Mask:

Gateway:  Network is behind remote gateway


Proxy ARP:  Publish network on all other interfaces via Proxy ARP

Additional IP:  Additional firewall IP address that hosts can use as gateway:

Delete this route

2.) So sollte dieser Eintrag aussehen.

Routing table				
Interface	Network	Gateway	Additional IP	Proxy ARP
LAN	192.168.1.0/24			<a href="#">[Edit]</a>
WAN	192.168.101.0/24			<a href="#">[Edit]</a>
WAN	0.0.0.0/0	192.168.101.254		<a href="#">[Edit]</a>
DMZ	127.0.0.0/24			<a href="#">[Edit]</a>
LAN	192.168.101.201/32			Yes <a href="#">[Edit]</a>
<a href="#">[Add new]</a>				



3.) Richten Sie die Weiterleitung für die IP Adressen unter „Firewall/Port Mapping“ ein.

In diesem Fall werden SSH Pakete vom WAN Interface (192.168.101.200) auf die IP 192.168.1.109 weitergeleitet. Das Feld „Destination IP“ ist leer, da diese somit mit der WAN IP genutzt wird. Es wäre auch möglich gewesen, die WAN-IP direkt einzutragen.

### Port Mapping / Virtual Servers

Edit **SSH\_1\_109** 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:

**Intrusion Detection / Prevention:**

Mode:

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

4.) In diesem Fall werden Pakete an den Webserver (Port 80) vom WAN Interface (192.168.101.200) auf die IP 192.168.1.109 weitergeleitet. Die Ziel-IP ist in diesem Fall die zusätzliche IP Adresse.

### Port Mapping / Virtual Servers

Edit **Web\_1\_10** 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:

**Intrusion Detection / Prevention:**

5.) So sollte die Weiterleitung aussehen.

[help](#)

Configured mappings:					
Name	Source	Destination	Service	Pass to	
SSH_1_109	Any	WAN IP	ssh	192.168.1.109	<a href="#">[Edit]</a>
Web_1_10	Any	192.168.101.201	http-in	192.168.1.10	<a href="#">[Edit]</a>

[\[Add new\]](#)

6.) Nun werden alle Webserver-Anfragen an die IP Adresse 192.168.101.200 zum Webserver unter 192.168.1.109 weitergeleitet. Anfragen an den SSH-Port werden an die IP 192.168.1.10 gesendet.