

Firewalling co-located servers with RouterOS

MUM Amsterdam 2016

Stephan Szarafinski

stephan@szarafinski.net

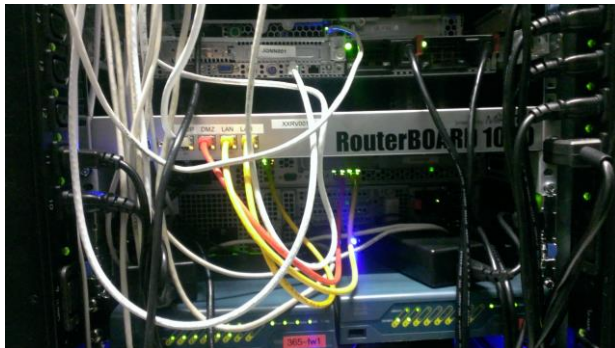
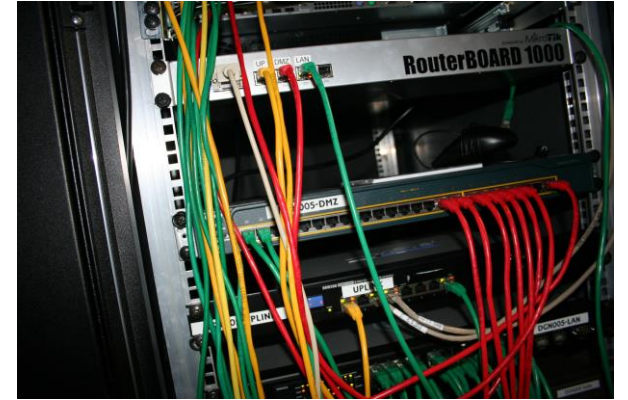
Introductie

- Stephan Szarafinski
- RouterOS gebruiker sinds 2003
- MTCNA sinds 2011



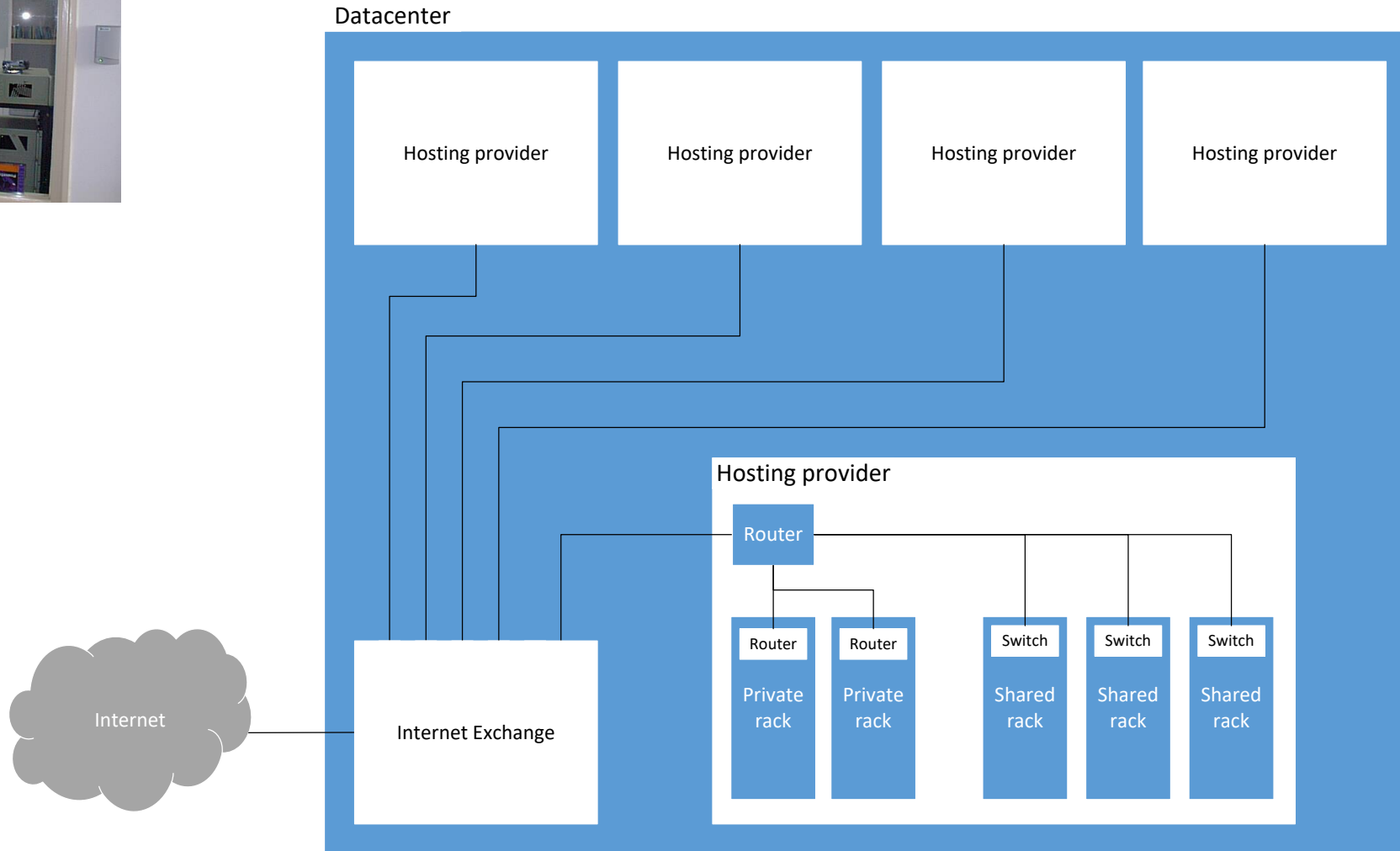
RouterOS / RouterBoard

- Routing
- Firewalling
- WiFi
- Networking
- Tunneling

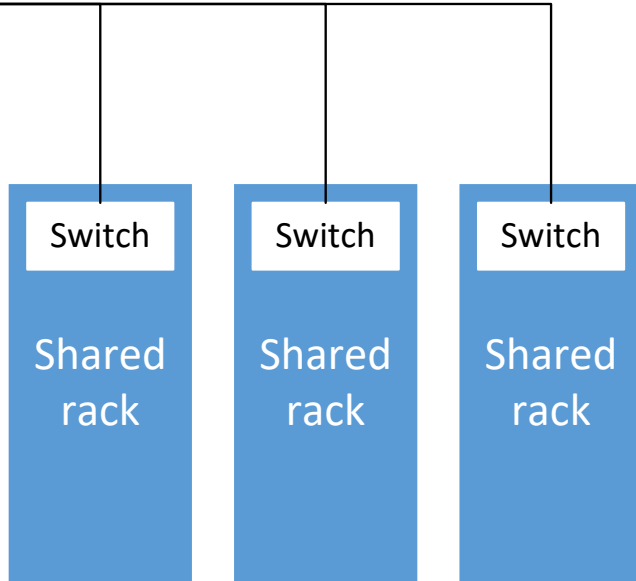




Co-location?

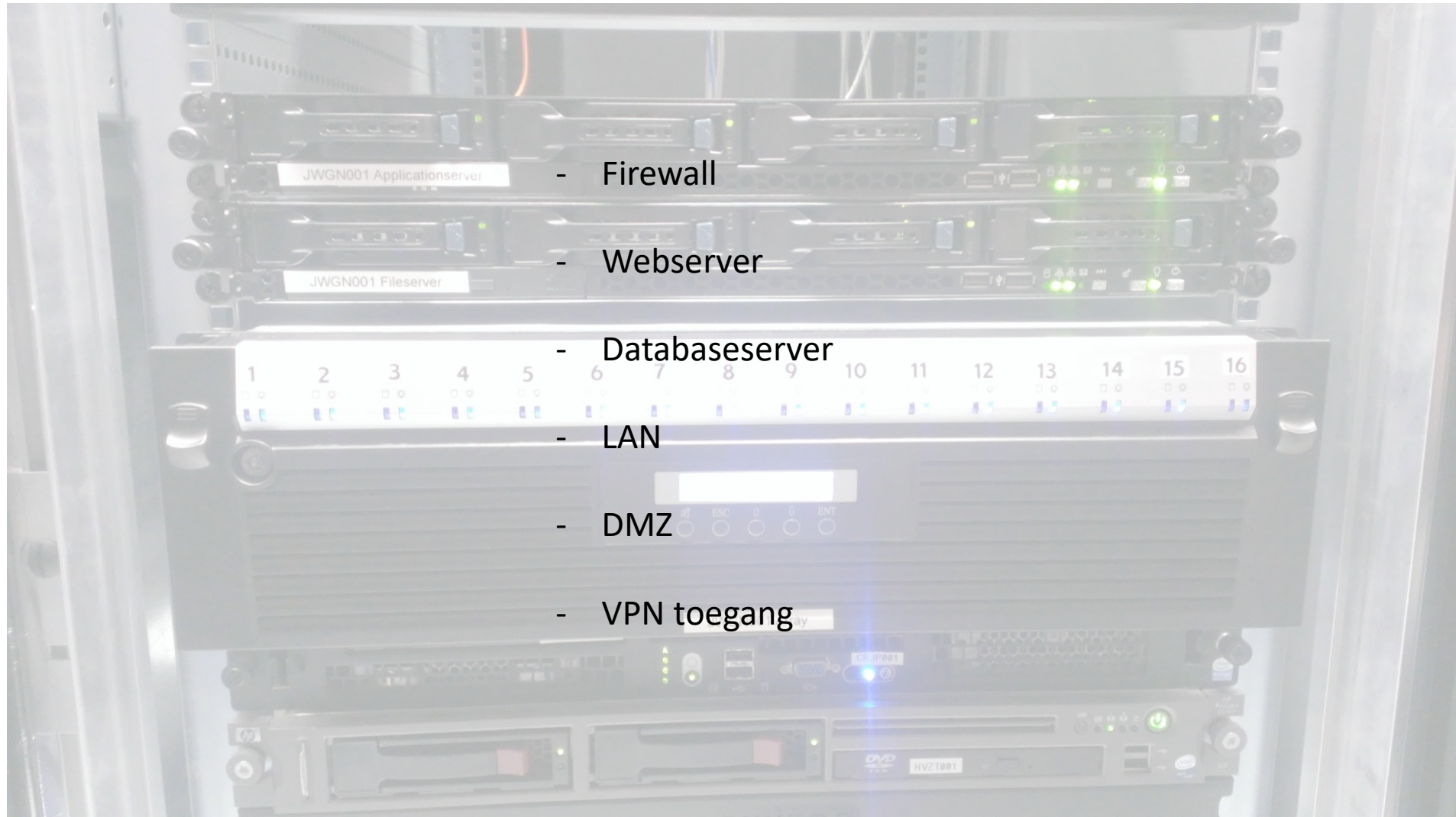


Co-location



- Servers van verschillende klanten in 1 rack
- 1 switchpoort ter beschikking
- Vlan met klein aantal IP adressen
- Gateway IP is de router van de provider
- Firewall in OS op servers

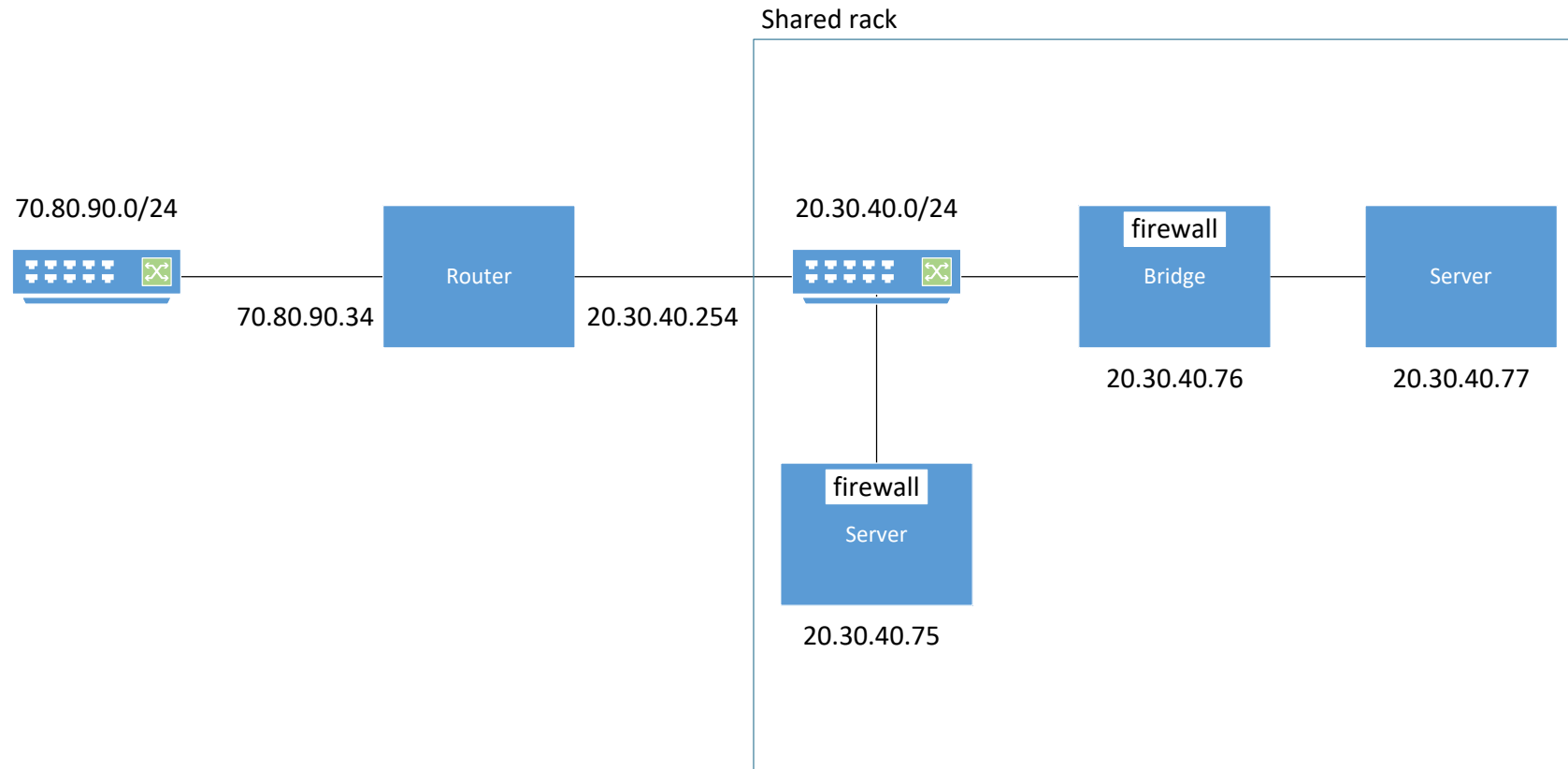
Ik wil meer...



Het probleem

- Weinig ruimte beschikbaar
- Niet teveel stroom gebruiken
- IP reeks is gedeeld
- Firewalling kan niet in de router, want die is van de hosting provider

Bridge met firewall

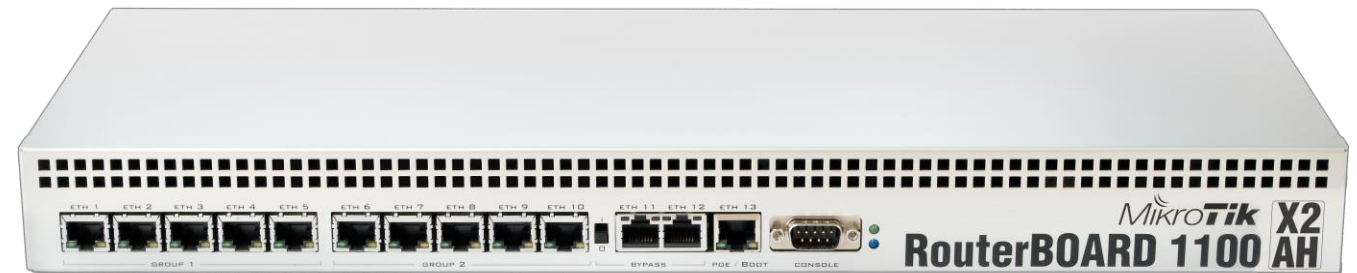


RouterBoard alles in 1 oplossingen

- Kleine behuizing
- Low power
- Twee switchchips met wirespeed transfer
- Genoeg ethernet poorten



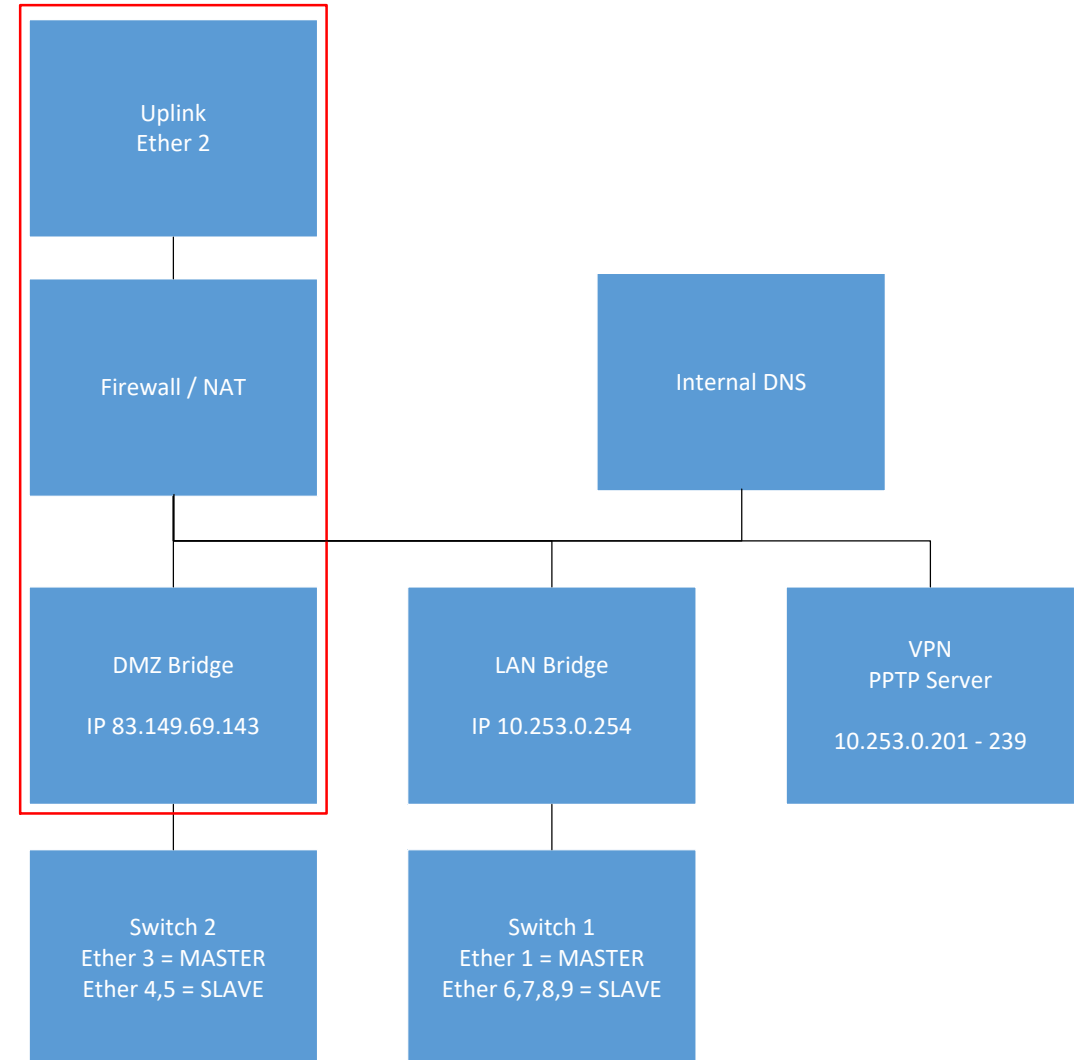
RB3011



RB1100

Configuratie

- RB493G
- IP reeks van Provider
 - 83.149.69.128/26
 - Gateway 83.149.69.190
- Toegewezen IP adressen
 - 83.149.69.143, 144, 145, 146, 147
- LAN IP reeks
 - 10.253.0.0/24
- 1x Uplink, 3x DMZ en 5x LAN



Winbox

admin@10.7.0.242:8290 (JWGN001 Router) - WinBox v6.35.2 on RB493G (mipsbe)

Session Settings Dashboard

Session: 10.7.0.242:8290

Quick Set
Interfaces
Bridge
PPP
Switch
Mesh
IP
System
Queues
Files
Log
Radius
Tools
New Terminal
MetaROUTER
Partition
Make Supout.nf
Manual
New WinBox
Exit

Interface List

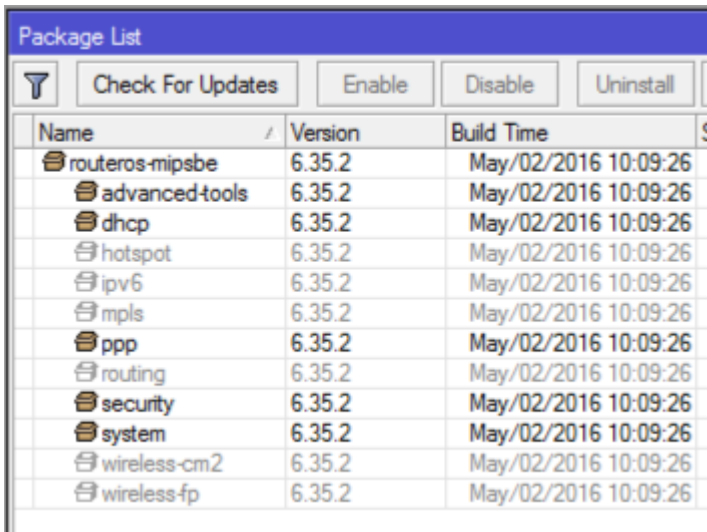
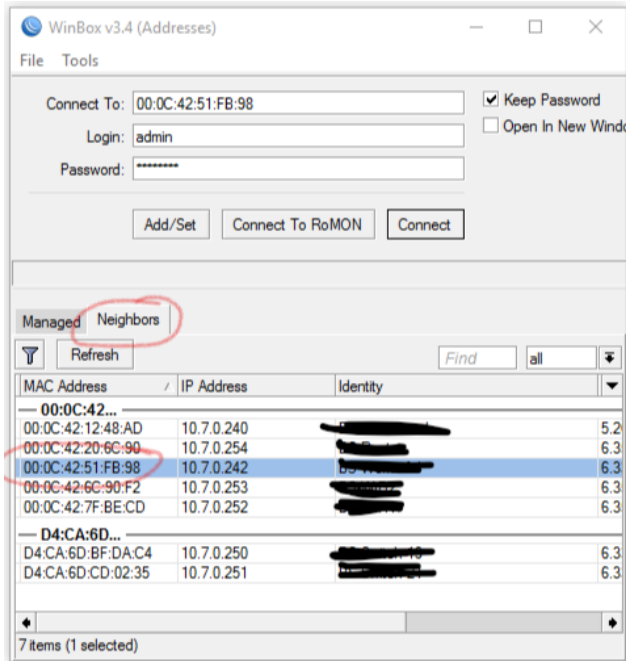
Interface Ethernet EoIP Tunnel IP Tunnel GRE Tunnel VLAN VRRP Bonding LTE

Find

	Name	Type	L2 MTU	Tx	Rx	Tx Packet (p/s)	Rx Packet (p/s)
RS	(01)LAN	Ethernet	1520	0 bps	0 bps	0	0
S	(02)JWGN001	Ethernet	1520	0 bps	0 bps	0	0
S	(03)DMZ	Ethernet	1520	0 bps	0 bps	0	0
S	(04)DMZ-SLAVE	Ethernet	1520	0 bps	0 bps	0	0
S	(05)DMZ-SLAVE	Ethernet	1520	0 bps	0 bps	0	0
S	(06)LAN-SLAVE	Ethernet	1520	0 bps	0 bps	0	0
S	(07)LAN-SLAVE	Ethernet	1520	0 bps	0 bps	0	0
S	(08)LAN-SLAVE	Ethernet	1520	0 bps	0 bps	0	0
RS	(09)LAN-SLAVE	Ethernet	1520	103.4 kbps	2.0 kbps	9	3
R	brDMZ	Bridge	1520	0 bps	0 bps	0	0
R	brLAN	Bridge	1520	103.1 kbps	1856 bps	9	4
	pptp-in-harski	PPTP Server Binding		0 bps	0 bps	0	0
	pptp-in-jm	PPTP Server Binding		0 bps	0 bps	0	0
	pptp-out-xxrv001	PPTP Client		0 bps	0 bps	0	0

14 items

Vorbereidingen



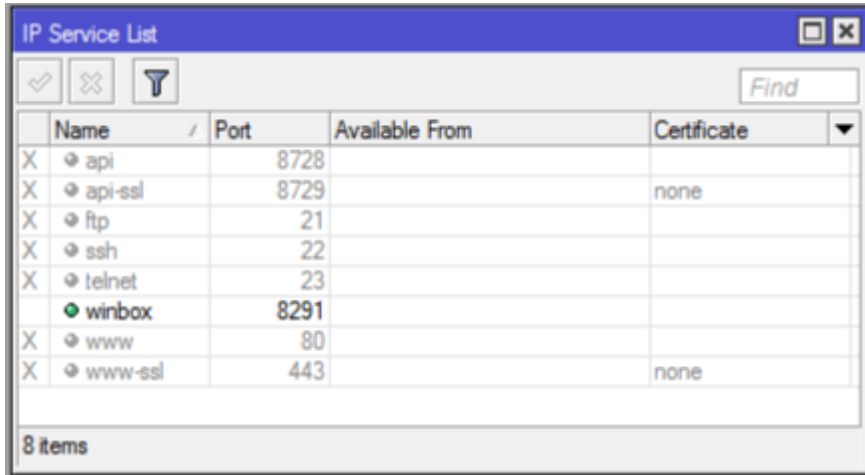
- Maak verbinding via MAC adres
- Upgrade naar laatste stable RouterOS versie
- Firmware update indien nodig
- Disable packages die niet nodig zijn, reboot
- Reset configuratie

```
/system reset-configuration keep-user=no no-defaults=yes skip-backup=yes
```

Systeem instellingen

```
/system clock set time-zone-autodetect=no time-zone-name=Europe/Amsterdam  
  
/system identity set name="JWGN001 Router"  
  
/system ntp client set enabled=yes primary-ntp=10.254.0.12  
  
/tool bandwidth-server set enabled=no  
  
/ip dns  
set allow-remote-requests=yes servers=85.17.150.123,62.212.64.122
```


Systeem instellingen



	Name	Port	Available From	Certificate
X	api	8728		
X	api-ssl	8729		none
X	ftp	21		
X	ssh	22		
X	telnet	23		
	winbox	8291		
X	www	80		
X	www-ssl	443		none

8 items

```
/ip service
set telnet disabled=yes
set ftp disabled=yes
set www disabled=yes
set ssh disabled=yes
set api disabled=yes
set api-ssl disabled=yes
```

Interfaces

Interface List		
Interface Ethernet EoIP Tunnel IP Tunnel		
✓ ✗ 📁 📏 Power Cycle		
	Name	Type
RS	(01)LAN	Ethernet
S	(02)JWGN001	Ethernet
S	(03)DMZ	Ethernet
S	(04)DMZ-SLAVE	Ethernet
S	(05)DMZ-SLAVE	Ethernet
S	(06)LAN-SLAVE	Ethernet
S	(07)LAN-SLAVE	Ethernet
S	(08)LAN-SLAVE	Ethernet
RS	(09)LAN-SLAVE	Ethernet

Switch			
Switch Port Host VLAN Rule			
📏			
	Name	Type	Mirror
	(switch1)LAN	Atheros 8316	
	(switch2)DMZ	Atheros 8316	

Interface <(04)DMZ-SLAVE>

General Ethernet Overall Stats Rx Stats Tx Stats ...

Name: (04)DMZ-SLAVE

Type: Ethernet

MTU: 1500

L2 MTU: 1520

Max L2 MTU: 1520

MAC Address: 00:0C:42:A9:96:9F

ARP: enabled

Master Port: (03)DMZ

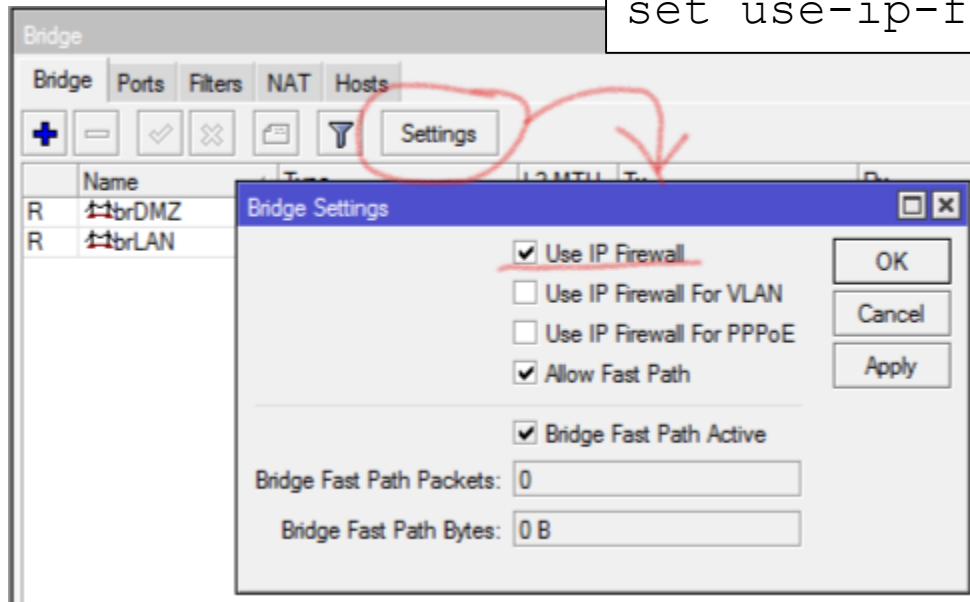
Bandwidth (Rx/Tx): unlimited / unlimited

Switch: (switch2)DMZ

```
/interface ethernet
set ether1 name="(01) LAN"
set ether2 name="(02) JWGN001"
set ether3 name="(03) DMZ"
set ether4 master-port="(03) DMZ" name="(04) DMZ-SLAVE"
set ether5 master-port="(03) DMZ" name="(05) DMZ-SLAVE"
set ether6 master-port="(01) LAN" name="(06) LAN-SLAVE"
set ether7 master-port="(01) LAN" name="(07) LAN-SLAVE"
set ether8 master-port="(01) LAN" name="(08) LAN-SLAVE"
set ether9 master-port="(01) LAN" name="(09) LAN-SLAVE"
```

Bridge

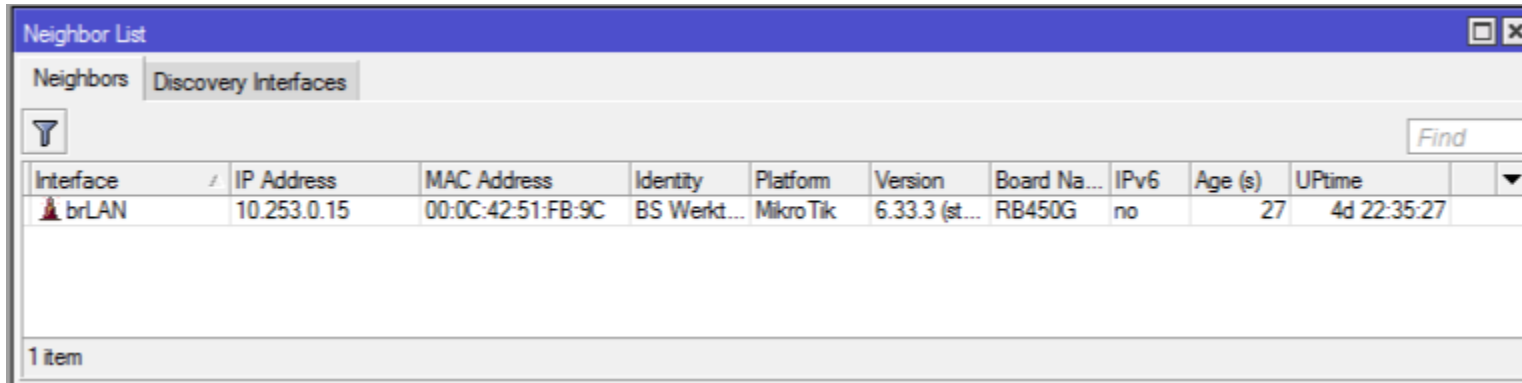
```
/interface bridge
add mtu=1500 name=brDMZ protocol-mode=none
add arp=proxy-arp mtu=1500 name=brLAN protocol-mode=none
/interface bridge port
add bridge=brLAN interface="(01) LAN"
add bridge=brDMZ interface="(02) JWGN001"
add bridge=brDMZ interface="(03) DMZ"
/interface bridge settings
set use-ip-firewall=yes
```



- LAN bridge nu niet perse nodig, maar handig voor later
- Proxy-arp op LAN bridge voor VPN verbindingen
- Al het bridge verkeer moet door de firewall

Neighbours

```
/ip neighbor discovery
set "(02)JWGN001" discover=no
set "(03)DMZ" discover=no
set "(04)DMZ-SLAVE" discover=no
set "(05)DMZ-SLAVE" discover=no
set brDMZ discover=no
```

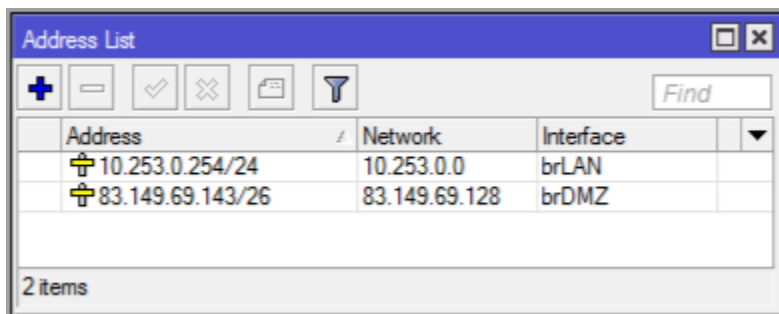


Interface	IP Address	MAC Address	Identity	Platform	Version	Board Na...	IPv6	Age (s)	Uptime
brLAN	10.253.0.15	00:0C:42:51:FB:9C	BS Werk...	MikroTik	6.33.3 (st...	RB450G	no	27	4d 22:35:27

1 item

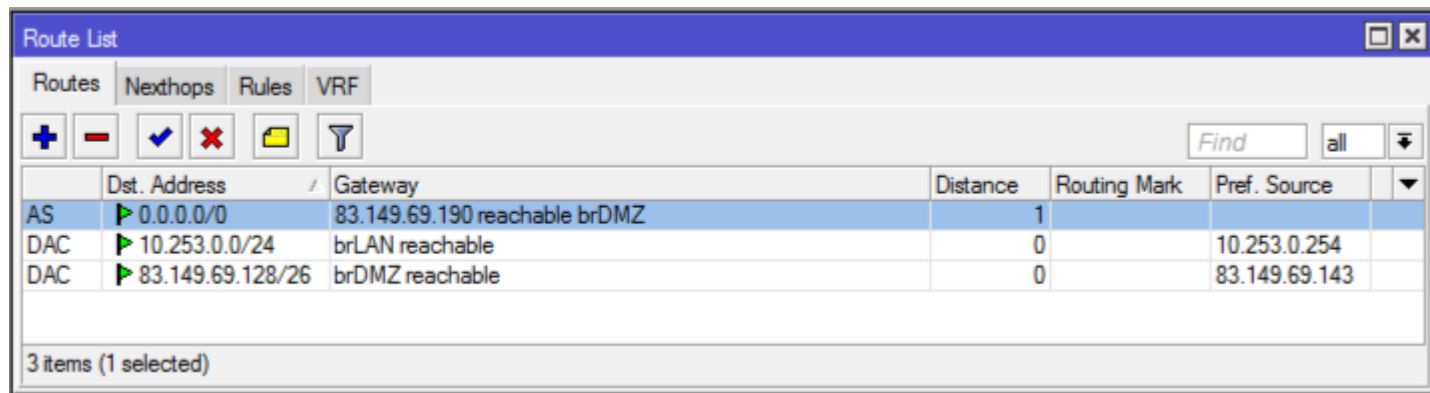
IP adressen en gateway

```
/ip address  
add address=10.253.0.254/24 interface=brLAN network=10.253.0.0  
add address=83.149.69.143/26 interface=brDMZ network=83.149.69.128  
  
/ip route  
add distance=1 gateway=83.149.69.190
```



Address	Network	Interface
10.253.0.254/24	10.253.0.0	brLAN
83.149.69.143/26	83.149.69.128	brDMZ

2 items



	Dst. Address	Gateway	Distance	Routing Mark	Pref. Source
AS	0.0.0.0/0	83.149.69.190 reachable brDMZ	1		
DAC	10.253.0.0/24	brLAN reachable	0		10.253.0.254
DAC	83.149.69.128/26	brDMZ reachable	0		83.149.69.143

3 items (1 selected)

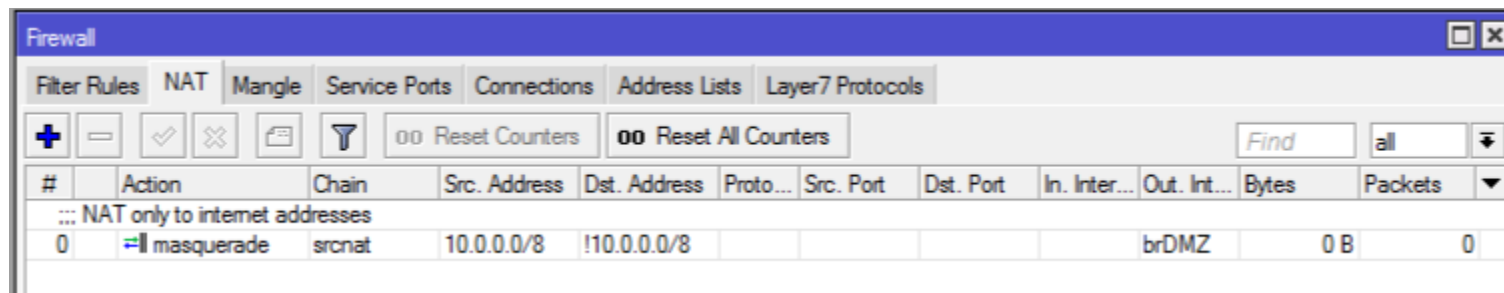
VPN

```
/ip pool
add name=pool-VPN next-pool=pool-VPN ranges=10.253.0.201-10.253.0.239
/interface pptp-server server
set enabled=yes
/ppp profile
set default-encryption local-address=10.253.0.200 only-one=\
    yes remote-address=pool-VPN
/ppp secret
add name=harski password="jlkjdsf7343ij4889" profile=default-encryption routes=\
    10.12.0.0/24 service=pptp
add name=jm password="789kjhd6532jljflk8o32" profile=\
    default-encryption routes=10.12.1.0/24 service=pptp
/interface pptp-server
add name=pptp-in-harski user=harski
add name=pptp-in-jm user=jm
```


Connection tracking en NAT

```
/ip settings
set tcp-syncookies=yes

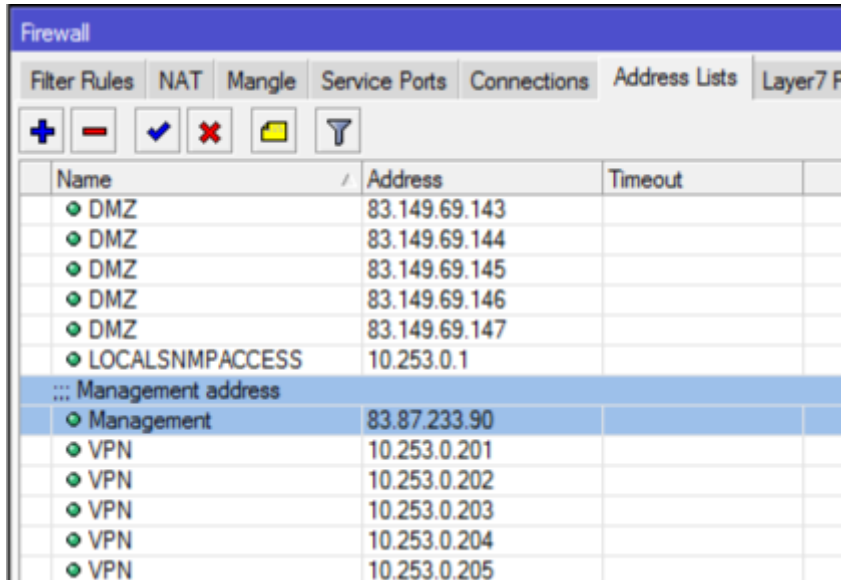
/ip firewall nat
add action=masquerade chain=srcnat \
    dst-address=!10.0.0.0/8 out-interface=brDMZ src-address=10.0.0.0/8
```



The screenshot shows the Mikrotik WinBox Firewall configuration window. The 'NAT' tab is selected. The rule list shows a single rule with the following configuration:

#	Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port	Dst. Port	In. Inter...	Out. Int...	Bytes	Packets
0	masquerade	srcnat	10.0.0.0/8	!10.0.0.0/8					brDMZ	0 B	0

Address lists



Name	Address	Timeout
DMZ	83.149.69.143	
DMZ	83.149.69.144	
DMZ	83.149.69.145	
DMZ	83.149.69.146	
DMZ	83.149.69.147	
LOCALSNMPACCESS	10.253.0.1	
... Management address		
Management	83.87.233.90	
VPN	10.253.0.201	
VPN	10.253.0.202	
VPN	10.253.0.203	
VPN	10.253.0.204	
VPN	10.253.0.205	

```
/ip firewall address-list
add address=83.149.69.143 list=DMZ
add address=83.149.69.144 list=DMZ
add address=83.149.69.145 list=DMZ
add address=83.149.69.146 list=DMZ
add address=83.149.69.147 list=DMZ
add address=10.253.0.1 list=LOCALSNMPACCESS
add address=83.87.233.90 list=Management
add address=85.17.150.123 list=trusted-ISP-DNS
add address=62.212.64.122 list=trusted-ISP-DNS
add address=10.253.0.201 list=VPN
add address=10.253.0.202 list=VPN
add address=10.253.0.203 list=VPN
. . . . .
add address=10.253.0.238 list=VPN
add address=10.253.0.239 list=VPN
add address=10.253.0.240 list=VPN
```

Firewall - Input

```
/ip firewall filter
add chain=input dst-port=8291 protocol=tcp src-address-list=Management
add action=drop chain=input in-interface=brDMZ src-address=10.0.0.0/8
add action=drop chain=input comment="Drop blacklist" src-address-list=black
add action=drop chain=input comment="Drop greylist" src-address-list=grey
add action=drop chain=input comment="Drop invalid connections" \
    connection-state=invalid
add chain=input comment="Accept established connections" connection-state=\
    established
add chain=input comment="Accept related connections" connection-state=related
add chain=input comment="Accept ICMP traffic" protocol=icmp
add chain=input comment="Accept winbox traffic from LAN" dst-port=8291 \
    in-interface=brLAN protocol=tcp
add chain=input comment="Accept replies from ISP DNS" in-interface=brDMZ \
    protocol=tcp src-address-list=trusted-ISP-DNS src-port=53
add chain=input comment="Accept replies from ISP DNS" in-interface=brDMZ \
    protocol=udp src-address-list=trusted-ISP-DNS src-port=53
add chain=input comment="Accept DNS requests from LAN" dst-port=53 \
    in-interface=brLAN protocol=tcp
```

Firewall - Input

```
add chain=input comment="Accept DNS requests from LAN" dst-port=53 \
    in-interface=brLAN protocol=udp
add action=add-src-to-address-list address-list=grey address-list-timeout=5m \
    chain=input comment="Winbox protection grey" connection-state=new \
    dst-port=8291 protocol=tcp src-address-list=winbox_darkgrey
add action=add-src-to-address-list address-list=winbox_darkgrey \
    address-list-timeout=30s chain=input comment="Winbox protection darkgrey" \
    connection-state=new dst-port=8291 protocol=tcp src-address-list=\
    winbox_lightgrey
add action=add-src-to-address-list address-list=winbox_lightgrey \
    address-list-timeout=30s chain=input comment=\
    "Winbox protection lightgrey" connection-state=new dst-port=8291 \
    protocol=tcp
add chain=input comment="Accept winbox traffic" dst-port=8291 protocol=tcp
add chain=input comment="Accept broadcasts" dst-address-type=broadcast \
    in-interface=brDMZ
add chain=input comment="Accept PPTP traffic from DMZ" dst-port=1723 \
    in-interface=brDMZ protocol=tcp
```

Firewall - Input

```
add chain=input comment="Accept PPTP traffic from DMZ" in-interface=brDMZ \
    protocol=tcp src-port=1723
add chain=input comment="Accept SSTP traffic from DMZ" disabled=yes dst-port=\
    443 in-interface=brDMZ protocol=tcp
add chain=input comment="Accept EOIP/PPTP/SSTP traffic from DMZ" \
    in-interface=brDMZ protocol=gre
add chain=input comment="Accept SNMP traffic" dst-port=161 in-interface=brLAN \
    protocol=udp src-address-list=LOCALSNMPACCESS
add chain=input comment="Accept neighbour traffic from LAN" dst-port=5678 \
    in-interface=brLAN protocol=udp
add action=add-src-to-address-list address-list=grey address-list-timeout=5m \
    chain=input comment="Port scan to grey list" psd=21,3s,3,1
add action=log chain=input
add action=drop chain=input comment=Default
```

Firewall - Input

Firewall

Filter Rules NAT Mangle Service Ports Connections Address Lists Layer7 Protocols

00 Reset Counters00 Reset All Counters

Find

#	Action	Chain	Src. Address	Dst. Address	Protocol	Src. Port	Dst. Port	In. Inter...	Out. Int...	Connection State	Src. Address List	Dst. Address List	Out. Bridge Port	In. Bridge
0	✓ accept	input			6 (tcp)		8291				Management			
1	✗ drop	input	10.0.0.0/8					brDMZ						
... Drop blacklist														
2	✗ drop	input									black			
... Drop greylist														
3	✗ drop	input									grey			
... Drop invalid connections														
4	✗ drop	input								invalid				
... Accept established connections														
5	✓ accept	input								established				
... Accept related connections														
6	✓ accept	input								related				
... Accept ICMP traffic														
7	✓ accept	input			1 (icmp)									
... Accept winbox traffic from LAN														
8	✓ accept	input			6 (tcp)		8291	brLAN						
... Accept replies from ISP DNS														
9	✓ accept	input			6 (tcp)	53		brDMZ			trusted-ISP-DNS			
... Accept replies from ISP DNS														
10	✓ accept	input			17 (udp)	53		brDMZ			trusted-ISP-DNS			
... Accept DNS requests from LAN														
11	✓ accept	input			6 (tcp)		53	brLAN						
... Accept DNS requests from LAN														
12	✓ accept	input			17 (udp)		53	brLAN						

Firewall - Input

::: Winbox protection grey												
13		add src to address list	input			6 (tcp)		8291			new	winbox_darkgrey
::: Winbox protection darkgrey												
14		add src to address list	input			6 (tcp)		8291			new	winbox_lightgrey
::: Winbox protection lightgrey												
15		add src to address list	input			6 (tcp)		8291			new	
::: Accept winbox traffic												
16		accept	input			6 (tcp)		8291				
::: Accept broadcasts												
17		accept	input							brDMZ		
::: Accept PPTP traffic from DMZ												
18		accept	input			6 (tcp)		1723		brDMZ		
::: Accept PPTP traffic from DMZ												
19		accept	input			6 (tcp)		1723		brDMZ		
::: Accept EOIP/PPTP/SSTP traffic from DMZ												
20		accept	input			47 (gre)				brDMZ		
::: Accept SNMP traffic												
21		accept	input			17 (udp)		161		brLAN		LOCALSNMPACCESS
::: Accept neighbour traffic from LAN												
22		accept	input			17 (udp)		5678		brLAN		
::: Port scan to grey list												
23		add src to address list	input									
24		log	input									
::: Default												
25		drop	input									

Firewall - Output

```
/ip firewall filter
add chain=output dst-address-list=Management protocol=tcp src-port=8291
add action=drop chain=output dst-address=10.0.0.0/8 out-interface=brDMZ
add action=drop chain=output comment="Drop blacklist" dst-address-list=black
add action=drop chain=output comment="Drop greylist" dst-address-list=grey
add action=drop chain=output comment="Drop invalid connections" \
    connection-state=invalid
add chain=output comment="Accept established connections" connection-state=\
    established
add chain=output comment="Accept related connections" connection-state=\
    related
add chain=output comment="Accept ICMP traffic" protocol=icmp
add chain=output comment="Accept winbox traffic" protocol=tcp src-port=8291
add chain=output comment="Accept requests to ISP DNS" dst-address-list=\
    trusted-ISP-DNS dst-port=53 out-interface=brDMZ protocol=tcp
add chain=output comment="Accept requests to ISP DNS" dst-address-list=\
    trusted-ISP-DNS dst-port=53 out-interface=brDMZ protocol=udp
add chain=output comment="Accept DNS replies to LAN" out-interface=brLAN \
    protocol=tcp src-port=53
```


Firewall - Output

```
add chain=output comment="Accept DNS replies to LAN" out-interface=brLAN \
    protocol=udp src-port=53
add chain=output comment="Accept broadcasts" dst-address-type=broadcast \
    out-interface=brDMZ
add chain=output comment="Accept PPTP traffic to DMZ" out-interface=brDMZ \
    protocol=tcp src-port=1723
add chain=output comment="Accept PPTP traffic to DMZ" dst-port=1723 \
    out-interface=brDMZ protocol=tcp
add chain=output comment="Accept SSTP traffic to DMZ" disabled=yes \
    out-interface=brDMZ protocol=tcp src-port=443
add chain=output comment="Accept EOIP/PPTP/SSTP traffic to DMZ" \
    out-interface=brDMZ protocol=gre
add chain=output comment="Time server access" dst-address=10.254.0.12 \
    dst-port=123 protocol=udp
add chain=output comment="Accept SNMP traffic" dst-address-list=\
    LOCALSNMPACCESS out-interface=brLAN protocol=udp src-port=161
add chain=output comment="Accept neighbour traffic to LAN" dst-port=5678 \
    out-interface=brLAN protocol=udp
```

Firewall - Output

```
add chain=output comment="Accept SYSLOG traffic" dst-address-list=\
    LOCALSNMPACCESS out-interface=brLAN protocol=udp src-port=514
add action=log chain=output
add action=drop chain=output comment=Default
```

Firewall - Output

Firewall														
Filter Rules NAT Mangle Service Ports Connections Address Lists Layer7 Protocols														
00 Reset Counters 00 Reset All Counters Find output														
#	Action	Chain	Src. Address	Dst. Address	Protocol	Src. Port	Dst. Port	In. Inter...	Out. Int...	Connection State	Src. Address List	Dst. Address List	Out. Bridge Port	In. Bridge
26	✓ accept	output			6 (tcp)	8291						Management		
27	✗ drop	output		10.0.0.0/8					brDMZ					
... Drop blacklist														
28	✗ drop	output										black		
... Drop greylist														
29	✗ drop	output										grey		
... Drop invalid connections														
30	✗ drop	output								invalid				
... Accept established connections														
31	✓ accept	output								established				
... Accept related connections														
32	✓ accept	output								related				
... Accept ICMP traffic														
33	✓ accept	output			1 (icmp)									
... Accept winbox traffic														
34	✓ accept	output			6 (tcp)	8291								
... Accept requests to ISP DNS														
35	✓ accept	output			6 (tcp)		53		brDMZ			trusted-ISP-DNS		
... Accept requests to ISP DNS														
36	✓ accept	output			17 (udp)		53		brDMZ			trusted-ISP-DNS		

Firewall - Output

... Accept DNS replies to LAN													
37	✓	accept	output			6 (tcp)	53			brLAN			
... Accept DNS replies to LAN													
38	✓	accept	output			17 (udp)	53			brLAN			
... Accept broadcasts													
39	✓	accept	output							brDMZ			
... Accept PPTP traffic to DMZ													
40	✓	accept	output			6 (tcp)	1723			brDMZ			
... Accept PPTP traffic to DMZ													
41	✓	accept	output			6 (tcp)		1723		brDMZ			
... Accept SSTP traffic to DMZ													
42	X	✗ accept	output			6 (tcp)	443			brDMZ			
... Accept EOIP/PPTP/SSTP traffic to DMZ													
43	✓	accept	output			47 (gre)				brDMZ			
... Time server access													
44	✓	accept	output		10.254.0.12	17 (udp)		123					
... Accept SNMP traffic													
45	✓	accept	output			17 (udp)	161			brLAN		LOCALSNMPACC...	
... Accept neighbour traffic to LAN													
46	✓	accept	output			17 (udp)		5678		brLAN			
... Accept SYSLOG traffic													
47	✓	accept	output			17 (udp)	514			brLAN		LOCALSNMPACC...	
48		log	output										
... Default													
49	✗	drop	output										

Firewall - Forward

The screenshot shows the 'Firewall Rule' configuration window in WinBox, specifically the 'Forward' tab. The 'General' tab is selected. The configuration includes:

- Src. Address List:** A dropdown menu with 'DMZ' selected.
- Dst. Address List:** An empty dropdown menu.
- Layer7 Protocol:** An empty dropdown menu.
- Content:** An empty dropdown menu.
- Connection Bytes:** An empty dropdown menu.
- Connection Rate:** An empty dropdown menu.
- Per Connection Classifier:** An empty dropdown menu.
- Src. MAC Address:** An empty dropdown menu.
- Out. Bridge Port:** A dropdown menu with '(02)VWGN001' selected.
- In. Bridge Port:** A dropdown menu with '(02)VWGN001' selected.

- Gebruik out bridge port en in bridge port
- Voor de snelheid worden accepted en related packets meteen geaccepteerd
- DMZ verkeer gaat naar DMZ-IN en DMZ-OUT
- Firewalling gaat per service, de IP adressen van de servers gaan per service in een address list

Firewall - Forward

```
/ip firewall filter
add action=drop chain=forward comment=\
    "Internal source address not allowed from DMZ" in-interface=brDMZ \
    src-address=10.0.0.0/8
add action=log chain=forward comment=\
    "Internal destination address not allowed to DMZ" dst-address=10.0.0.0/8 \
    out-interface=brDMZ
add action=drop chain=forward comment=\
    "Internal destination address not allowed to DMZ" dst-address=10.0.0.0/8 \
    out-interface=brDMZ
add action=drop chain=forward comment=\
    "VPN source address not allowed from LAN" in-interface=brLAN \
    src-address-list=VPN
add action=drop chain=forward comment=\
    "VPN destination address not allowed to LAN" dst-address-list=VPN \
    out-interface=brLAN
add action=drop chain=forward comment="Drop blacklist" src-address-list=black
add action=drop chain=forward comment="Drop blacklist" dst-address-list=black
add action=drop chain=forward comment="Drop greylist" src-address-list=grey
```

Firewall - Forward

```
add action=drop chain=forward comment="Drop greylist" dst-address-list=grey
add action=drop chain=forward comment="Drop invalid connections" \
    connection-state=invalid
add action=jump chain=forward comment="Accept established connections" \
    connection-state=established jump-target=ConnectionExceptions
add action=jump chain=forward comment="Accept related connections" \
    connection-state=related jump-target=ConnectionExceptions
add action=jump chain=forward comment=\
    "Accept traffic from DMZ to JWGN001 uplink" in-bridge-port="!(02)JWGN001" \
    jump-target=DMZ-OUT out-bridge-port="(02)JWGN001" src-address-list=DMZ
add action=drop chain=forward comment=\
    "Drop other traffic from DMZ to JWGN001 uplink" in-bridge-port=\
    "!(02)JWGN001" out-bridge-port="(02)JWGN001"
add action=jump chain=forward comment=\
    "Accept traffic from JWGN001 uplink to DMZ" dst-address-list=DMZ \
    in-bridge-port="(02)JWGN001" jump-target=DMZ-IN out-bridge-port=\
    "!(02)JWGN001"
add action=drop chain=forward comment=\
    "Drop other traffic from JWGN001 uplink to DMZ" in-bridge-port=\
    "(02)JWGN001" out-bridge-port="!(02)JWGN001"
```

Firewall - Forward

```
add chain=forward comment="Traffic from LAN via NAT to DMZ" dst-address=\
    !10.0.0.0/8 in-interface=brLAN out-interface=brDMZ src-address=10.0.0.0/8
add chain=forward comment="Traffic from DMZ via NAT to LAN" dst-address=\
    10.0.0.0/8 in-interface=brDMZ out-interface=brLAN src-address=!10.0.0.0/8
add chain=forward comment=xxrv001 dst-address=10.253.0.0/24 in-interface=\
    pptp-out-xxrv001 src-address=10.0.0.0/8
add action=jump chain=forward comment="Accept traffic from VPN" jump-target=\
    VPN-IN src-address-list=VPN
add action=jump chain=forward comment=harski in-interface=pptp-in-harski \
    jump-target=VPN-IN src-address=10.12.0.0/24
add action=jump chain=forward comment=jm in-interface=pptp-in-jm jump-target=\
    VPN-IN src-address=10.12.1.0/24
add action=jump chain=forward comment="Accept traffic from VPN" \
    dst-address-list=VPN jump-target=VPN-OUT
add action=jump chain=forward comment=harski dst-address=10.12.0.0/24 \
    jump-target=VPN-OUT out-interface=pptp-in-harski
add action=jump chain=forward comment=jm dst-address=10.12.1.0/24 \
    jump-target=VPN-OUT out-interface=pptp-in-jm
add action=log chain=forward
add action=drop chain=forward comment=Default
```


Firewall - Forward

Firewall														
Filter Rules NAT Mangle Service Ports Connections Address Lists Layer7 Protocols														
00 Reset Counters 00 Reset All Counters Find forward														
#	Action	Chain	Src. Address	Dst. Address	Protocol	Src. Port	Dst. Port	In. Inter...	Out. Int...	Connection State	Src. Address List	Dst. Address List	Out. Bridge Port	In. Bridge Port
... Internal source address not allowed from DMZ														
50	drop	forward	10.0.0.0/8					brDMZ						
... Internal destination address not allowed to DMZ														
51	log	forward		10.0.0.0/8				brDMZ						
... Internal destination address not allowed to DMZ														
52	drop	forward		10.0.0.0/8				brDMZ						
... VPN source address not allowed from LAN														
53	drop	forward						brLAN			VPN			
... VPN destination address not allowed to LAN														
54	drop	forward						brLAN				VPN		
... Drop blacklist														
55	drop	forward									black			
... Drop blacklist														
56	drop	forward										black		
... Drop greylist														
57	drop	forward									grey			
... Drop greylist														
58	drop	forward										grey		
... Drop invalid connections														
59	drop	forward								invalid				
... Accept established connections														
60	jump	forward								established				
... Accept related connections														
61	jump	forward								related				

Firewall - Forward

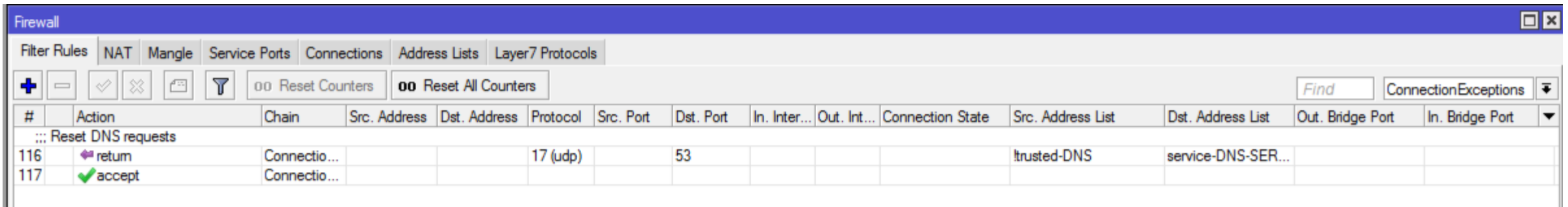
... Accept traffic from DMZ to JWGN001 uplink													
62		jump	forward								DMZ	(02)JWGN001	!(02)JWGN001
... Drop other traffic from DMZ to JWGN001 uplink													
63		drop	forward									(02)JWGN001	!(02)JWGN001
... Accept traffic from JWGN001 uplink to DMZ													
64		jump	forward								DMZ	!(02)JWGN001	(02)JWGN001
... Drop other traffic from JWGN001 uplink to DMZ													
65		drop	forward									!(02)JWGN001	(02)JWGN001
... Traffic from LAN via NAT to DMZ													
66		accept	forward	10.0.0.0/8	!10.0.0.0/8					brLAN	brDMZ		
... Traffic from DMZ via NAT to LAN													
67		accept	forward	!10.0.0.0/8	10.0.0.0/8					brDMZ	brLAN		

Firewall - Forward

... Accept traffic from VPN													
68		jump	forward									VPN	
... harski													
-- ptp-in-harski not ready													
69		jump	forward	10.12.0.0/24						ptp-in-...			
... jm													
-- ptp-in-jm not ready													
70		jump	forward	10.12.1.0/24						ptp-in-jm			
... Accept traffic from VPN													
71		jump	forward									VPN	
... harski													
-- ptp-in-harski not ready													
72		jump	forward	10.12.0.0/24						ptp-in-...			
... jm													
-- ptp-in-jm not ready													
73		jump	forward	10.12.1.0/24						ptp-in-jm			
74		log	forward										
... Default													
75		drop	forward										

Firewall Forward

```
add action=return chain=ConnectionExceptions comment="Reset DNS requests" \
    dst-address-list=service-DNS-SERVERS dst-port=53 protocol=udp \
    src-address-list=!trusted-DNS
add chain=ConnectionExceptions
```



#	Action	Chain	Src. Address	Dst. Address	Protocol	Src. Port	Dst. Port	In. Inter...	Out. Int...	Connection State	Src. Address List	Dst. Address List	Out. Bridge Port	In. Bridge Port
::: Reset DNS requests														
116	return	Connection...			17 (udp)		53				!trusted-DNS	service-DNS-SER...		
117	accept	Connectio...												

- Sommige accepted connections wil je kunnen weigeren of beperken

Firewall – DMZ-IN

```
/ip firewall filter
add action=add-src-to-address-list address-list=grey address-list-timeout=5m \
    chain=DMZ-IN comment="Port scan to grey list" psd=21,3s,3,1
add chain=DMZ-IN comment="From Gateway" protocol=icmp src-address=85.17.3.190
add chain=DMZ-IN comment="PASSTROUGH list" dst-address-list=\
    service-PASSTROUGH
add chain=DMZ-IN comment="DNS servers list port 53" dst-address-list=\
    service-DNS-SERVERS dst-port=53 protocol=tcp
add chain=DMZ-IN comment="DNS servers list port 53" dst-address-list=\
    service-DNS-SERVERS dst-limit=1,5,src-address dst-port=53 protocol=udp
add action=drop chain=DMZ-IN comment="DNS servers list port 53 limited" \
    dst-address-list=service-DNS-SERVERS dst-port=53 protocol=udp
add chain=DMZ-IN comment="VOIP list" dst-address-list=service-VOIP-SERVERS \
    dst-port=5004-5060 protocol=udp src-address-list=service-VOIP-CARRIERS
add chain=DMZ-IN comment="VOIP list" dst-address-list=service-VOIP-SERVERS \
    dst-port=5060 protocol=udp src-address-list=service-VOIP-USERS
add chain=DMZ-IN comment="WEB list port 80" dst-address-list=\
    service-WEB-SERVERS dst-port=80 protocol=tcp
```

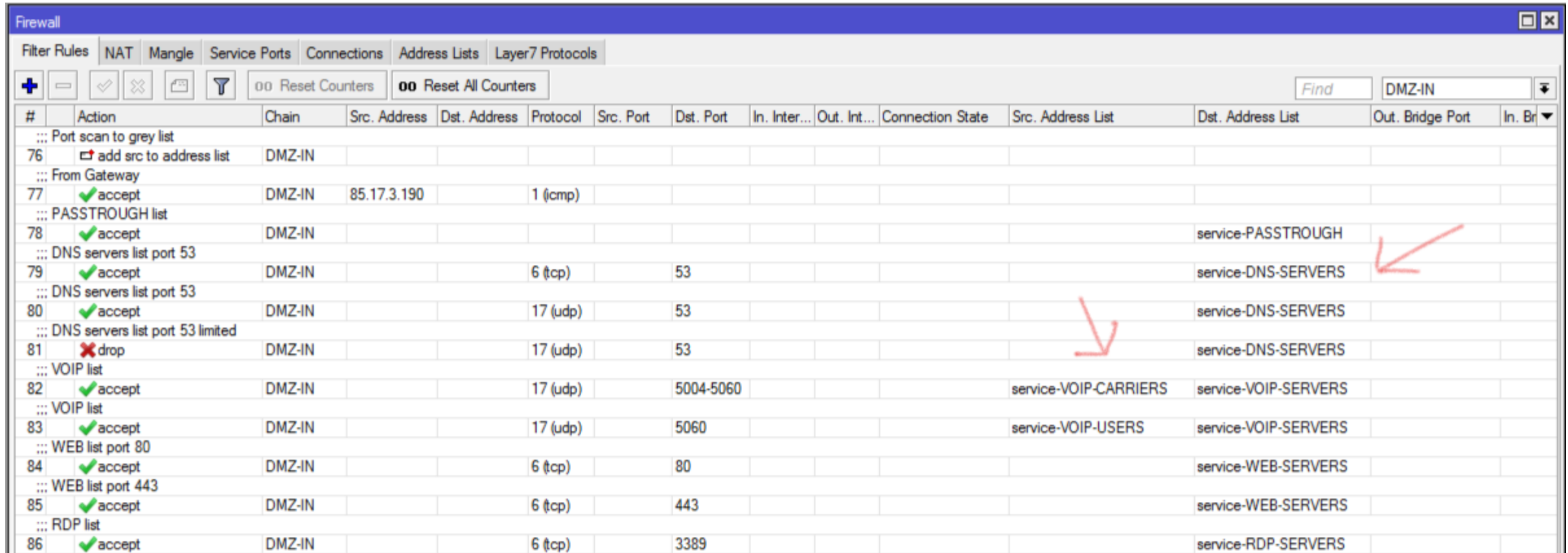
Firewall – DMZ-IN

```
add chain=DMZ-IN comment="WEB list port 443" dst-address-list=\
    service-WEB-SERVERS dst-port=443 protocol=tcp
add chain=DMZ-IN comment="RDP list" dst-address-list=service-RDP-SERVERS \
    dst-port=3389 protocol=tcp
add chain=DMZ-IN comment="SSL list port 22" dst-address-list=service-SSL \
    dst-port=22 protocol=tcp
add chain=DMZ-IN comment="MAIL list port 25" dst-address-list=\
    service-MAIL-SERVERS dst-port=25 protocol=tcp
add chain=DMZ-IN comment="MAIL list port 587" dst-address-list=\
    service-MAIL-SERVERS dst-port=587 protocol=tcp
add chain=DMZ-IN comment="MAIL list port 110" dst-address-list=\
    service-MAIL-SERVERS dst-port=110 protocol=tcp
add chain=DMZ-IN comment="MAIL list port 995" dst-address-list=\
    service-MAIL-SERVERS dst-port=995 protocol=tcp
add chain=DMZ-IN comment="MAIL list port 143" dst-address-list=\
    service-MAIL-SERVERS dst-port=143 protocol=tcp
add chain=DMZ-IN comment="MAIL list port 993" dst-address-list=\
    service-MAIL-SERVERS dst-port=993 protocol=tcp
```

Firewall – DMZ-IN

```
add chain=DMZ-IN comment="FTP list port 20" dst-address-list=\
    service-FTP-SERVERS dst-port=20 protocol=tcp
add chain=DMZ-IN comment="FTP list port 21" dst-address-list=\
    service-FTP-SERVERS dst-port=21 protocol=tcp
add chain=DMZ-IN comment="FTP list port 40000-50000" dst-address-list=\
    service-FTP-SERVERS dst-port=40000-50000 protocol=tcp
add action=drop chain=DMZ-IN comment=Default
```

Firewall – DMZ-IN



#	Action	Chain	Src. Address	Dst. Address	Protocol	Src. Port	Dst. Port	In. Inter...	Out. Int...	Connection State	Src. Address List	Dst. Address List	Out. Bridge Port	In. Br
...	Port scan to grey list													
76	add src to address list	DMZ-IN												
...	From Gateway													
77	accept	DMZ-IN	85.17.3.190		1 (icmp)									
...	PASSTROUGH list													
78	accept	DMZ-IN										service-PASSTROUGH		
...	DNS servers list port 53													
79	accept	DMZ-IN			6 (tcp)		53					service-DNS-SERVERS		
...	DNS servers list port 53													
80	accept	DMZ-IN			17 (udp)		53					service-DNS-SERVERS		
...	DNS servers list port 53 limited													
81	drop	DMZ-IN			17 (udp)		53					service-DNS-SERVERS		
...	VOIP list													
82	accept	DMZ-IN			17 (udp)		5004-5060				service-VOIP-CARRIERS	service-VOIP-SERVERS		
...	VOIP list													
83	accept	DMZ-IN			17 (udp)		5060				service-VOIP-USERS	service-VOIP-SERVERS		
...	WEB list port 80													
84	accept	DMZ-IN			6 (tcp)		80					service-WEB-SERVERS		
...	WEB list port 443													
85	accept	DMZ-IN			6 (tcp)		443					service-WEB-SERVERS		
...	RDP list													
86	accept	DMZ-IN			6 (tcp)		3389					service-RDP-SERVERS		

Firewall – DMZ-IN

... SSL list port 22												
87	✓ accept	DMZ-IN		6 (tcp)	22						service-SSL	
... MAIL list port 25												
88	✓ accept	DMZ-IN		6 (tcp)	25						service-MAIL-SERVERS	
... MAIL list port 587												
89	✓ accept	DMZ-IN		6 (tcp)	587						service-MAIL-SERVERS	
... MAIL list port 110												
90	✓ accept	DMZ-IN		6 (tcp)	110						service-MAIL-SERVERS	
... MAIL list port 995												
91	✓ accept	DMZ-IN		6 (tcp)	995						service-MAIL-SERVERS	
... MAIL list port 143												
92	✓ accept	DMZ-IN		6 (tcp)	143						service-MAIL-SERVERS	
... MAIL list port 993												
93	✓ accept	DMZ-IN		6 (tcp)	993						service-MAIL-SERVERS	
... FTP list port 20												
94	✓ accept	DMZ-IN		6 (tcp)	20						service-FTP-SERVERS	
... FTP list port 21												
95	✓ accept	DMZ-IN		6 (tcp)	21						service-FTP-SERVERS	
... FTP list port 40000-50000												
96	✓ accept	DMZ-IN		6 (tcp)	40000-50...						service-FTP-SERVERS	
... Default												
97	✗ drop	DMZ-IN										

Firewall – DMZ-OUT

```
/ip firewall filter
add chain=DMZ-OUT comment="To Gateway" dst-address=85.17.3.190 protocol=icmp
add chain=DMZ-OUT comment="PASSTROUGH list" src-address-list=\
    service-PASSTROUGH
add chain=DMZ-OUT comment="DNS servers list port 53" dst-port=53 protocol=tcp \
    src-address-list=service-DNS-SERVERS
add chain=DMZ-OUT comment="DNS servers list port 53" dst-port=53 protocol=udp \
    src-address-list=service-DNS-SERVERS
add chain=DMZ-OUT comment="DNS users list port 53" dst-port=53 protocol=udp \
    src-address-list=service-DNS-CLIENTS
add chain=DMZ-OUT comment="TIME users list port 123" dst-port=123 protocol=\
    udp src-address-list=service-TIME-CLIENTS
add chain=DMZ-OUT comment="VOIP list" dst-address-list=service-VOIP-CARRIERS \
    dst-port=5060 protocol=udp src-address-list=service-VOIP-SERVERS
add chain=DMZ-OUT comment="VOIP list" dst-address-list=service-VOIP-USERS \
    dst-port=5004-5060 protocol=udp src-address-list=service-VOIP-SERVERS
add chain=DMZ-OUT comment="MAIL list port 25" dst-port=25 protocol=tcp \
    src-address-list=service-MAIL-SERVERS
```

Firewall – DMZ-OUT

```
add chain=DMZ-OUT comment="MAIL list port 25" dst-port=25 protocol=tcp \
    src-address-list=service-MAIL-CLIENTS
add chain=DMZ-OUT comment="WEB Clients port 80" dst-port=80 protocol=tcp \
    src-address-list=service-WEB-CLIENTS
add chain=DMZ-OUT comment="WEB Clients port 443" dst-port=443 protocol=tcp \
    src-address-list=service-WEB-CLIENTS
add action=drop chain=DMZ-OUT comment=Default
```

Firewall – DMZ-OUT

Firewall														
Filter Rules														
NATMangleService PortsConnectionsAddress ListsLayer7 Protocols														
+ - ✓ ✕ ⌂ ⚙ 00 Reset Counters 00 Reset All Counters Find DMZ-OUT														
#	Action	Chain	Src. Address	Dst. Address	Protocol	Src. Port	Dst. Port	In. Inter...	Out. Int...	Connection State	Src. Address List	Dst. Address List	Out. Bridge Port	In. Br
... To Gateway														
98	✓ accept	DMZ-OUT		85.17.3.190	1 (icmp)									
... PASSTROUGH list														
99	✓ accept	DMZ-OUT									service-PASSTROUGH			
... DNS servers list port 53														
100	✓ accept	DMZ-OUT			6 (tcp)		53				service-DNS-SERVERS			
... DNS servers list port 53														
101	✓ accept	DMZ-OUT			17 (udp)		53				service-DNS-SERVERS			
... DNS users list port 53														
102	✓ accept	DMZ-OUT			17 (udp)		53				service-DNS-CLIENTS			
... TIME users list port 123														
103	✓ accept	DMZ-OUT			17 (udp)		123				service-TIME-CLIENTS			
... VOIP list														
104	✓ accept	DMZ-OUT			17 (udp)		5060				service-VOIP-SERVERS	service-VOIP-CARRIERS		
... VOIP list														
105	✓ accept	DMZ-OUT			17 (udp)		5004-5060				service-VOIP-SERVERS	service-VOIP-USERS		
... MAIL list port 25														
106	✓ accept	DMZ-OUT			6 (tcp)		25				service-MAIL-SERVERS			
... MAIL list port 25														
107	✓ accept	DMZ-OUT			6 (tcp)		25				service-MAIL-CLIENTS			
... WEB Clients port 80														
108	✓ accept	DMZ-OUT			6 (tcp)		80				service-WEB-CLIENTS			
... WEB Clients port 443														
109	✓ accept	DMZ-OUT			6 (tcp)		443				service-WEB-CLIENTS			
... Default														
110	✗ drop	DMZ-OUT												

Firewall – VPN-IN

```
/ip firewall filter
add chain=VPN-IN comment="Accept VPN connections traffic to LAN" dst-address=\
10.253.0.0/24
add chain=VPN-IN comment="Accept VPN connections traffic to LAN" dst-address=\
10.0.0.0/8 src-address-list=VPN
add chain=VPN-IN comment=jm dst-address=10.0.0.0/8 src-address=\
10.12.1.0/24
add chain=VPN-IN comment=harski dst-address=10.0.0.0/8 src-address=\
10.12.0.0/24
add action=drop chain=VPN-IN comment=Default
```

#	Action	Chain	Src. Address	Dst. Address	Protocol	Src. Port	Dst. Port	In. Inter...	Out. Int...	Connection State	Src. Address List	Dst. Address List	Out. Bridge Port	In. Br
...	Accept VPN connections traffic to LAN													
113	✓ accept	VPN-IN		10.253.0.0/...										
...	Accept VPN connections traffic to LAN													
114	✓ accept	VPN-IN		10.0.0.0/8							VPN			
...	jm													
115	✓ accept	VPN-IN	10.12.1.0/24	10.0.0.0/8										
...	harski													
116	✓ accept	VPN-IN	10.12.0.0/24	10.0.0.0/8										
...	Default													
117	✗ drop	VPN-IN												

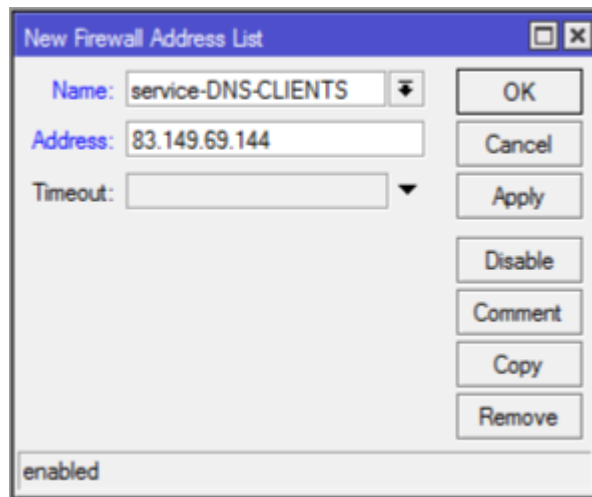
Firewall – VPN-OUT

```
/ip firewall filter
add chain=VPN-OUT comment="Accept VPN connections traffic from LAN" \
src-address=10.253.0.0/24
add chain=VPN-OUT comment="Accept VPN connections traffic from LAN" \
dst-address-list=VPN src-address=10.0.0.0/8
add chain=VPN-OUT comment=jm dst-address=10.12.1.0/24 src-address=\
10.0.0.0/8
add chain=VPN-OUT comment=harski dst-address=10.12.0.0/24 src-address=\
10.0.0.0/8
add action=drop chain=VPN-OUT comment=default
```

#	Action	Chain	Src. Address	Dst. Address	Protocol	Src. Port	Dst. Port	In. Inter...	Out. Int...	Connection State	Src. Address List	Dst. Address List	Out. Bridge Port	In. Br
...	Accept VPN connections traffic from LAN													
118	✓ accept	VPN-OUT	10.253.0.0/...											
...	Accept VPN connections traffic from LAN													
119	✓ accept	VPN-OUT	10.0.0.0/8									VPN		
...	jm													
120	✓ accept	VPN-OUT	10.0.0.0/8	10.12.1.0/24										
...	harski													
121	✓ accept	VPN-OUT	10.0.0.0/8	10.12.0.0/24										
...	default													
122	✗ drop	VPN-OUT												

Toestaan van verkeer naar en van een server

- Op 83.149.69.144 zit een webserver
- Toevoegen aan address list 'service-WEB-SERVERS'
- Meestal heeft een server ook een DNS-CLIENT en een WEB-CLIENT



VPN	10.253.0.255
VPN	10.253.0.240
service-DNS-CLIENTS	83.149.69.144
service-WEB-CLIENTS	83.149.69.144
service-WEB-SERVERS	83.149.69.144
trusted-ISP-DNS	85.17.150.123
trusted-ISP-DNS	62.212.64.122

Afsluiting

- Vragen?
- U kunt altijd mailen naar stephan@szarafinski.net voor meer info en advies.
- Bedankt voor uw aandacht!