

## System

General setup  
Static routes  
Firmware  
Advanced  
User manager

## Interfaces (assign)

LAN  
WAN  
OPT1

## Firewall

Rules  
NAT  
Traffic shaper  
Aliases

## Services

DNS forwarder  
Dynamic DNS  
DHCP server  
DHCP relay  
SNMP  
Proxy ARP  
Captive portal  
Wake on LAN

## VPN

IPsec  
PPTP

## Status

System  
Interfaces  
Traffic graph  
Wireless

## Diagnosics

## Firewall: Rules



The changes have been applied successfully.

LAN

WAN

OPT1



Proto	Source	Port	Destination	Port	Description
*	LAN net	*	*	*	Default LAN -> any



pass



block



reject



log



pass (disabled)



block (disabled)



reject (disabled)



log (disabled)

### Hint:

Rules are evaluated on a first-match basis (i.e. the action of the first rule to match a packet will be executed). This means that if you use block rules, you'll have to pay attention to the rule order. Everything that isn't explicitly passed is blocked by default.

## System

General setup  
Static routes  
Firmware  
Advanced  
User manager

## Interfaces (assign)

LAN  
WAN  
OPT1

## Firewall

Rules  
NAT  
Traffic shaper  
Aliases

## Services

DNS forwarder  
Dynamic DNS  
DHCP server  
DHCP relay  
SNMP  
Proxy ARP  
Captive portal  
Wake on LAN

## VPN

IPsec  
PPTP

## Status

System  
Interfaces  
Traffic graph  
Wireless

## ► Diagnostics

## Firewall: Rules

LAN WAN OPT1

		Proto	Source	Port	Destination	Port	Description	
	✗	*	RFC 1918 networks	*	*	*	Block private networks	⬅️ Ⓜ️ ╕
<input type="checkbox"/>	⬆️	TCP	*	*	192.168.	25 (SMTP)	NAT Allow SMTP traffic	⬅️ Ⓜ️ ╕
<input type="checkbox"/>	⬆️	TCP/UDP	*	*	192.168.	80 (HTTP)	NAT Allow HTTP traffic	⬅️ Ⓜ️ ╕
<input type="checkbox"/>	⬆️	TCP/UDP	*	*	192.168.	443 (HTTPS)	NAT Allow HTTPS traffic	⬅️ Ⓜ️ ╕
<input type="checkbox"/>	⬆️	TCP/UDP	*	*	192.168.	3389	NAT Allow RDP to server	⬅️ Ⓜ️ ╕

⬆️ pass      ✗ block      ✗ reject      📄 log  
 ⬆️ pass (disabled)      ✗ block (disabled)      ✗ reject (disabled)      📄 log (disabled)

### Hint:

Rules are evaluated on a first-match basis (i.e. the action of the first rule to match a packet will be executed). This means that if you use block rules, you'll have to pay attention to the rule order. Everything that isn't explicitly passed is blocked by default.

## System

General setup  
Static routes  
Firmware  
Advanced  
User manager

## Interfaces (assign)

LAN  
WAN  
OPT1

## Firewall

Rules  
NAT  
Traffic shaper  
Aliases

## Services

DNS forwarder  
Dynamic DNS  
DHCP server  
DHCP relay  
SNMP  
Proxy ARP  
Captive portal  
Wake on LAN

## VPN

IPsec  
PPTP










## Status

System  
Interfaces  
Traffic graph  
Wireless

## ► Diagnostics

## Firewall: NAT: Inbound

**Inbound** Server NAT 1:1 Outbound

If	Proto	Ext. port range	NAT IP	Int. port range	Description	
WAN	TCP/UDP	25 (SMTP)	192.168.	25 (SMTP)	Allow SMTP traffic	 
WAN	TCP/UDP	80 (HTTP)	192.168.	80 (HTTP)	Allow HTTP traffic	 
WAN	TCP/UDP	443 (HTTPS)	192.168.	443 (HTTPS)	Allow HTTPS traffic	 
WAN	TCP/UDP	3389	192.168.	3389	Allow RDP to server	 
						

### Note:

It is not possible to access NATed services using the WAN IP address from within LAN (or an optional network).