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
Logs
DHCP Leases
IPsec
Ping/Traceroute
ARP Table
Firewall states
Reset state
Backup/Restore
Factory Defaults
Reboot system

Firewall: Rules: Edit

Action
Block
Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded. Reject only works when the protocol is set to either TCP or UDP (but not "TCP/UDP") below.

Disabled
☐ **Disable this rule**
Set this option to disable this rule without removing it from the list.

Interface
LAN
Choose on which interface packets must come in to match this rule.

Protocol
TCP
Choose which IP protocol this rule should match.
Hint: in most cases, you should specify *TCP* here.

ICMP type
any
If you selected ICMP for the protocol above, you may specify an ICMP type here.

Source
☑ **not**
Use this option to invert the sense of the match.

Type: Single host or alias
Address: 192.168.1.3 / 31

Source port range
from: any
to: any

Specify the port or port range for the source of the packet for this rule. This is usually not equal to the destination port range (and is often "any").
Hint: you can leave the *'to'* field empty if you only want to filter a single port

Destination
☐ **not**
Use this option to invert the sense of the match.

Type: any
Address: / 31

Destination port range
from: SMTP
to: SMTP

Specify the port or port range for the destination of the packet for this rule.
Hint: you can leave the *'to'* field empty if you only want to filter a single port

Fragments
☐ **Allow fragmented packets**
Hint: this option puts additional load on the firewall and may make it vulnerable to DoS attacks. In most cases, it is not needed. Try enabling it if you have troubles connecting to certain sites.

Log
☑ **Log packets that are handled by this rule**
Hint: the firewall has limited local log space. Don't turn on logging for everything. If you want to do a lot of logging, consider using a remote syslog server (see the Diagnostics: System logs: Settings page).

Description
LAN -> Block SMTP Exept From Server
You may enter a description here for your reference (not parsed).

Save