Firewall

As Firewall I use IPFire . https://www.ipfire.org

This document is valid as per December 2023. Revisions will be made as changes in below occurs.

Please refer to the Topology page for a visual graphic.

IPFire Network denominations

RED incoming ISP connection	Used
GREEN interconnected wired Lan	Used
BLUE wireless connections	Used
ORANGE that has a standard DMZ setup	Not used

IPFire is a custom Linux distribution installed on my SuperMicro server with a network card having 4 1GBit ports. It is a bare-metal setup, no hypervisor or anything virtual on it's server. Server specifications here.

Firewall settings

It is not obvious what method to use to document my current firewall and all it's settings. I have tried to avoid complex rules and configurations and trying to find a general documented approach that is based on what the network and its monitoring components need to work as safely as possible.

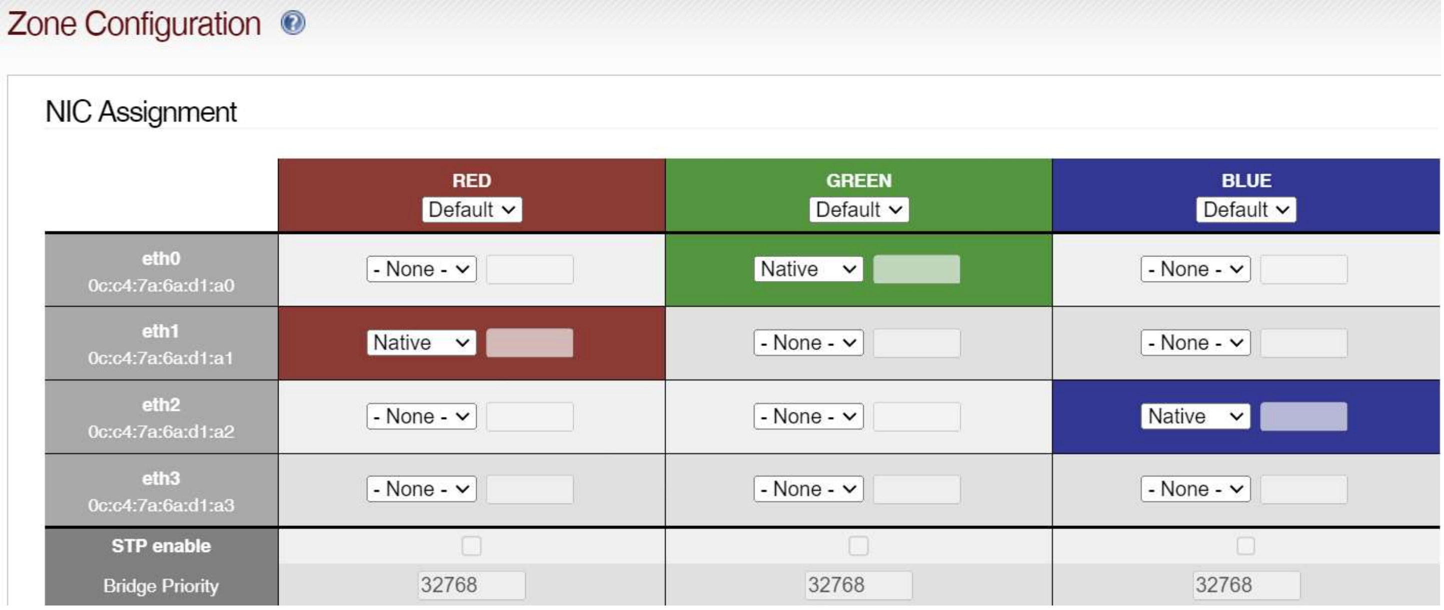
As mentioned above the original configuration of the firewall is based on default networks: Known network Zones .

RED is DHCP towards ISP. GREEN has been defined as 192.168.1.1/24, BLUE as 192.168.10.1/24.

Essential parts of the configuration

As you use the menu you will see these pages in below order. The screenshots indicate current configuration.

Current Firewall rules comes last.

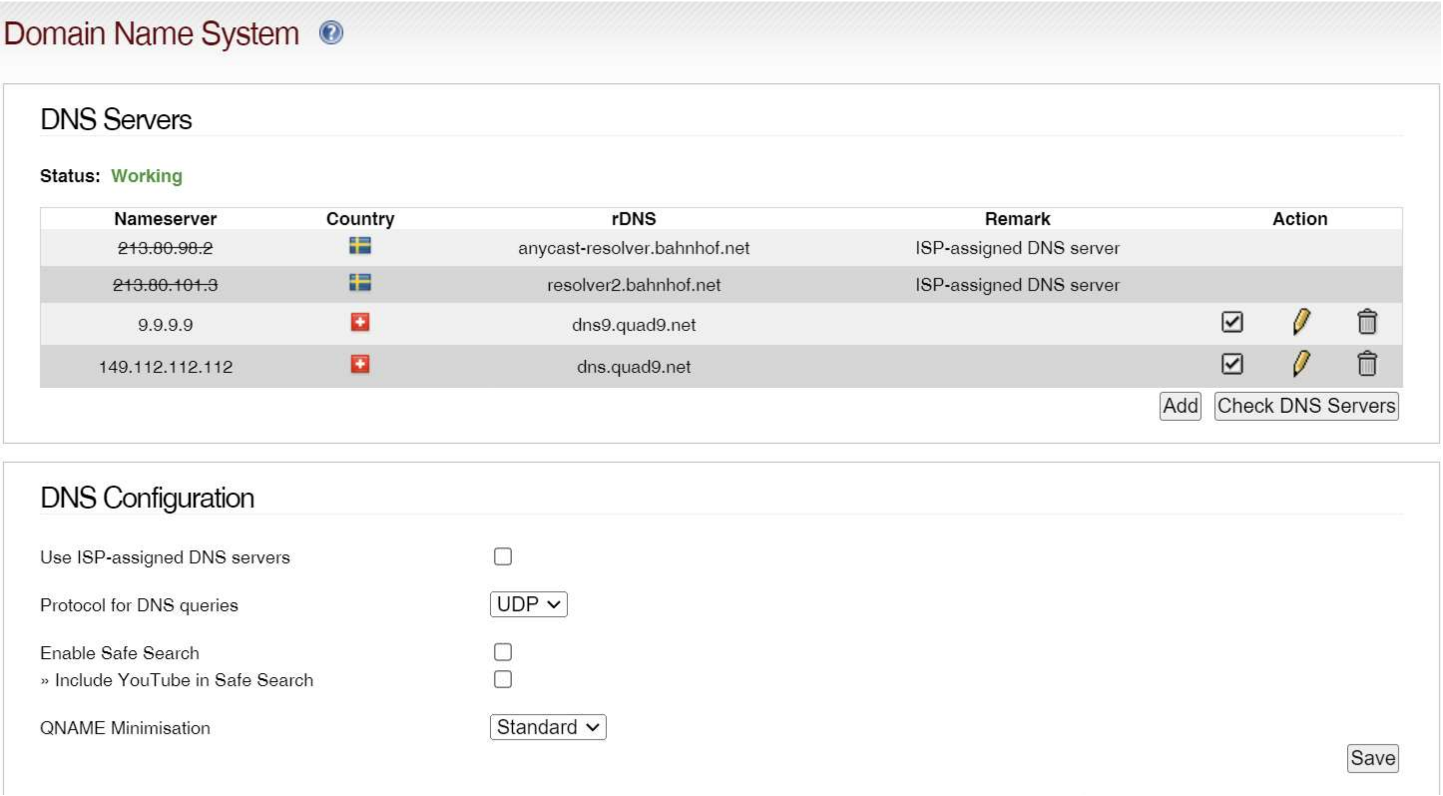


Zone Configuration

NIC Assignment

	RED Default	GREEN Default	BLUE Default
eth0 0c:c4:7a:6a:d1:a0	- None -	Native	- None -
eth1 0c:c4:7a:6a:d1:a1	Native	- None -	- None -
eth2 0c:c4:7a:6a:d1:a2	- None -	- None -	Native
eth3 0c:c4:7a:6a:d1:a3	- None -	- None -	- None -
STP enable	□	□	□
Bridge Priority	32768	32768	32768

> **As you can see by above image, it is extremely important to connect cables to the correct network port.**



Domain Name System

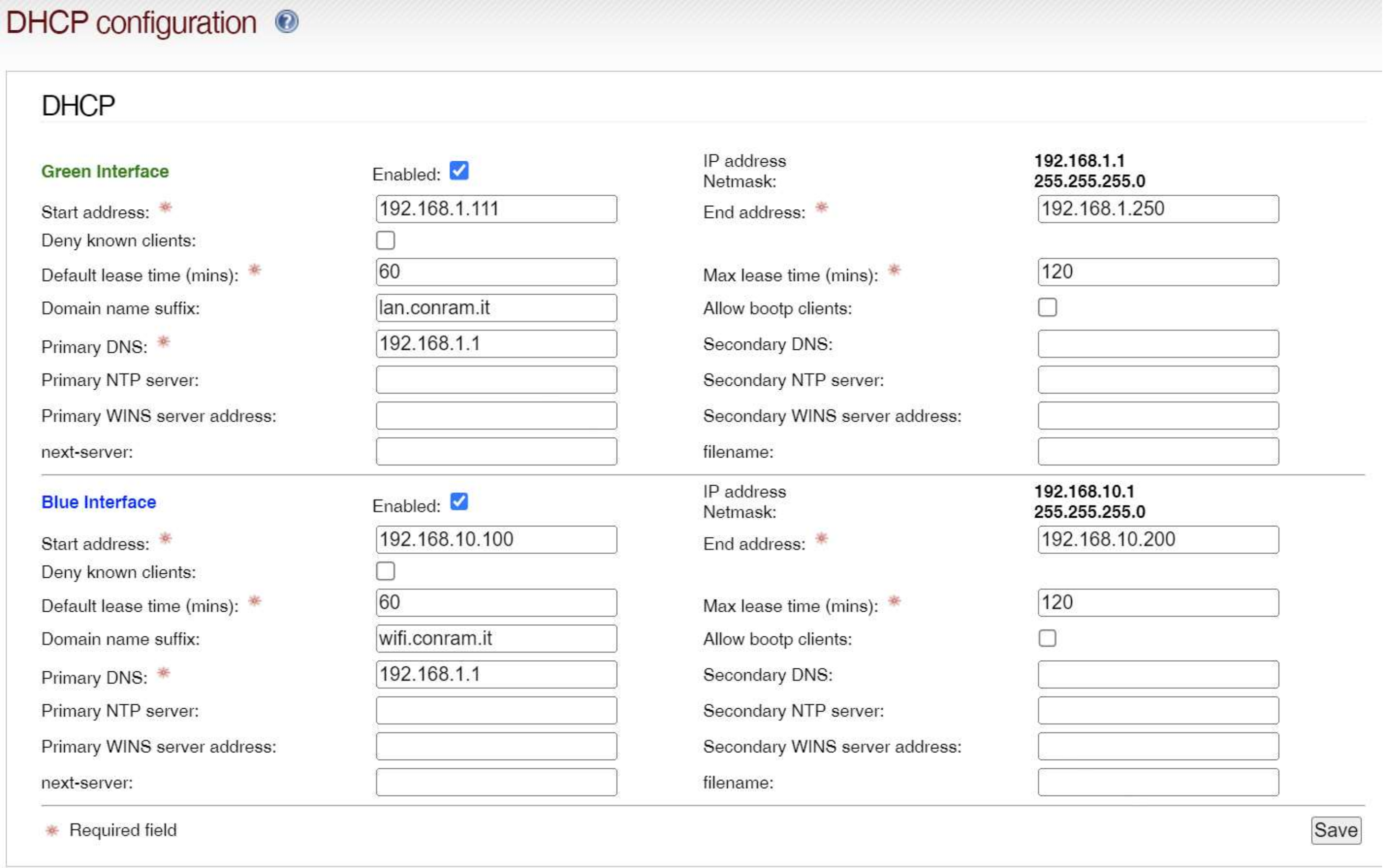
DNS Servers

Status: Working

Nameserver	Country	rDNS	Remark	Action
~~213.80.98.2~~	🇸🇪	anycast-resolver.bahnhof.net	ISP-assigned DNS server	
~~213.80.101.3~~	🇸🇪	resolver2.bahnhof.net	ISP-assigned DNS server	
9.9.9.9	🇨🇭	dns9.quad9.net		☑ ✎ 🗑
149.112.112.112	🇨🇭	dns.quad9.net		☑ ✎ 🗑

DNS Configuration

Use ISP-assigned DNS servers	□
Protocol for DNS queries	UDP
Enable Safe Search	□
» Include YouTube in Safe Search	□
QNAME Minimisation	Standard

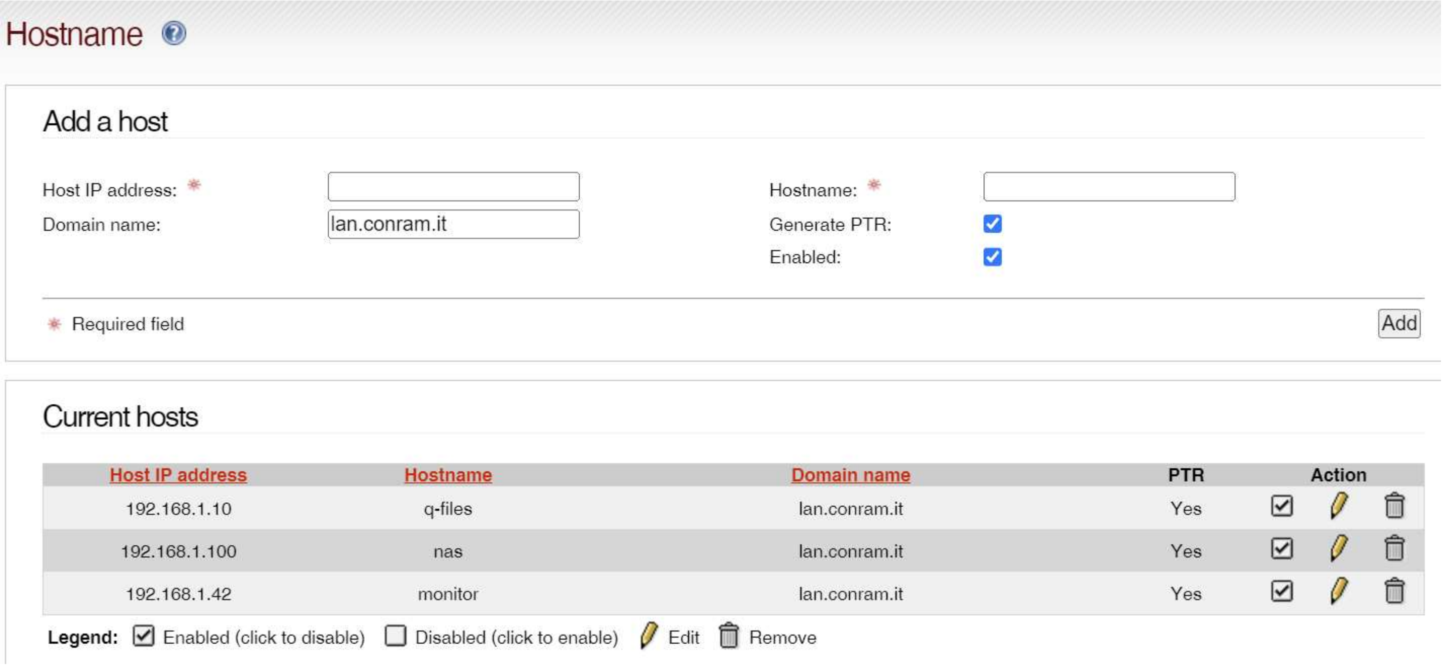


DHCP configuration

DHCP

Green Interface	Enabled: ☑	IP address Netmask:	**192.168.1.1** **255.255.255.0**
Start address: *	192.168.1.111	End address: *	192.168.1.250
Deny known clients:	☐		
Default lease time (mins): *	60	Max lease time (mins): *	120
Domain name suffix:	lan.conram.it	Allow bootp clients:	☐
Primary DNS: *	192.168.1.1	Secondary DNS:	
Primary NTP server:		Secondary NTP server:	
Primary WINS server address:		Secondary WINS server address:	
next-server:		filename:	
Blue Interface	Enabled: ☑	IP address Netmask:	**192.168.10.1** **255.255.255.0**
Start address: *	192.168.10.100	End address: *	192.168.10.200
Deny known clients:	☐		
Default lease time (mins): *	60	Max lease time (mins): *	120
Domain name suffix:	wifi.conram.it	Allow bootp clients:	☐
Primary DNS: *	192.168.1.1	Secondary DNS:	
Primary NTP server:		Secondary NTP server:	
Primary WINS server address:		Secondary WINS server address:	
next-server:		filename:	

* Required field



Hostname

Add a host

Host IP address: *		Hostname: *	
Domain name:	lan.conram.it	Generate PTR:	☑
		Enabled:	☑

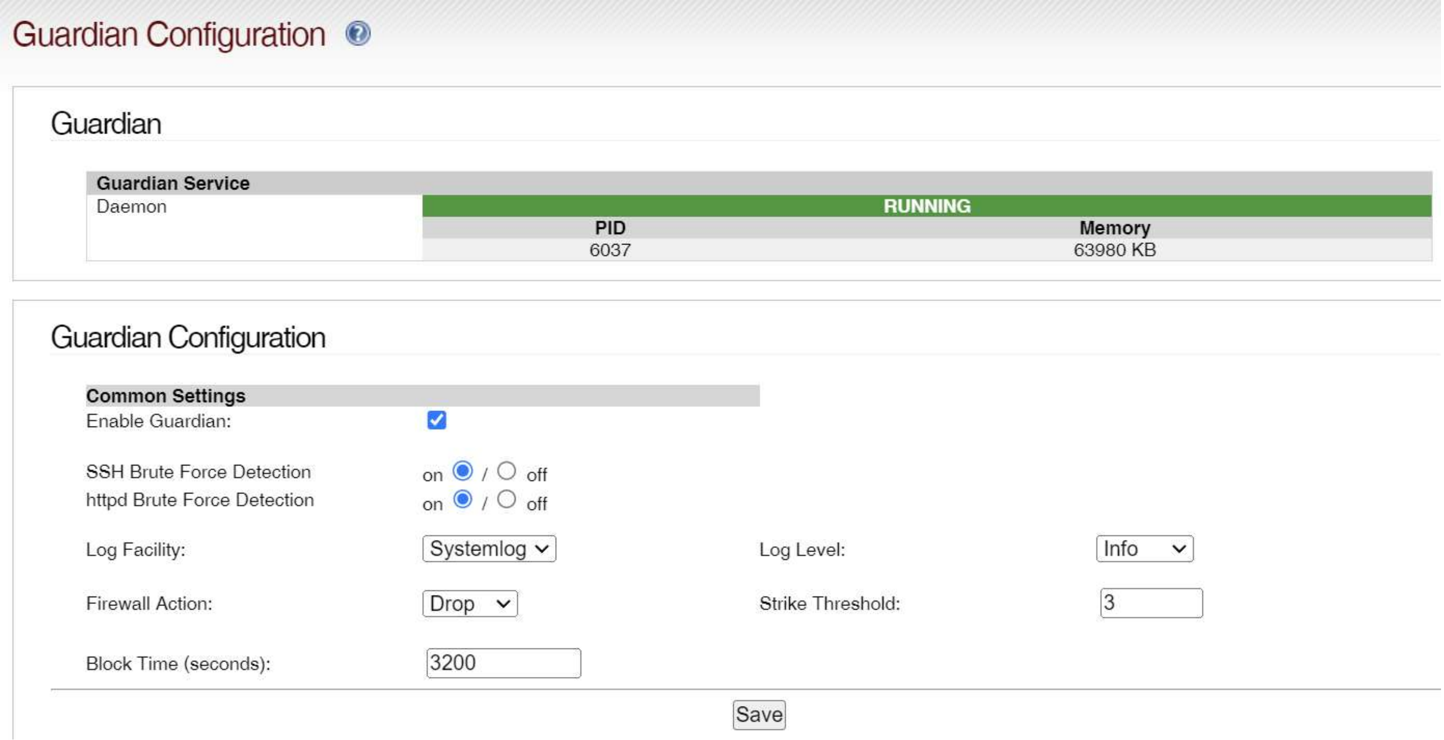
* Required field

Current hosts

Host IP address	Hostname	Domain name	PTR	Action
192.168.1.10	q-files	lan.conram.it	Yes	☑ ✏ 🗑
192.168.1.100	nas	lan.conram.it	Yes	☑ ✏ 🗑
192.168.1.42	monitor	lan.conram.it	Yes	☑ ✏ 🗑

Legend: ☑ Enabled (click to disable) ☐ Disabled (click to enable) ✏ Edit 🗑 Remove

Guardian is a Plugin to the Firewall:



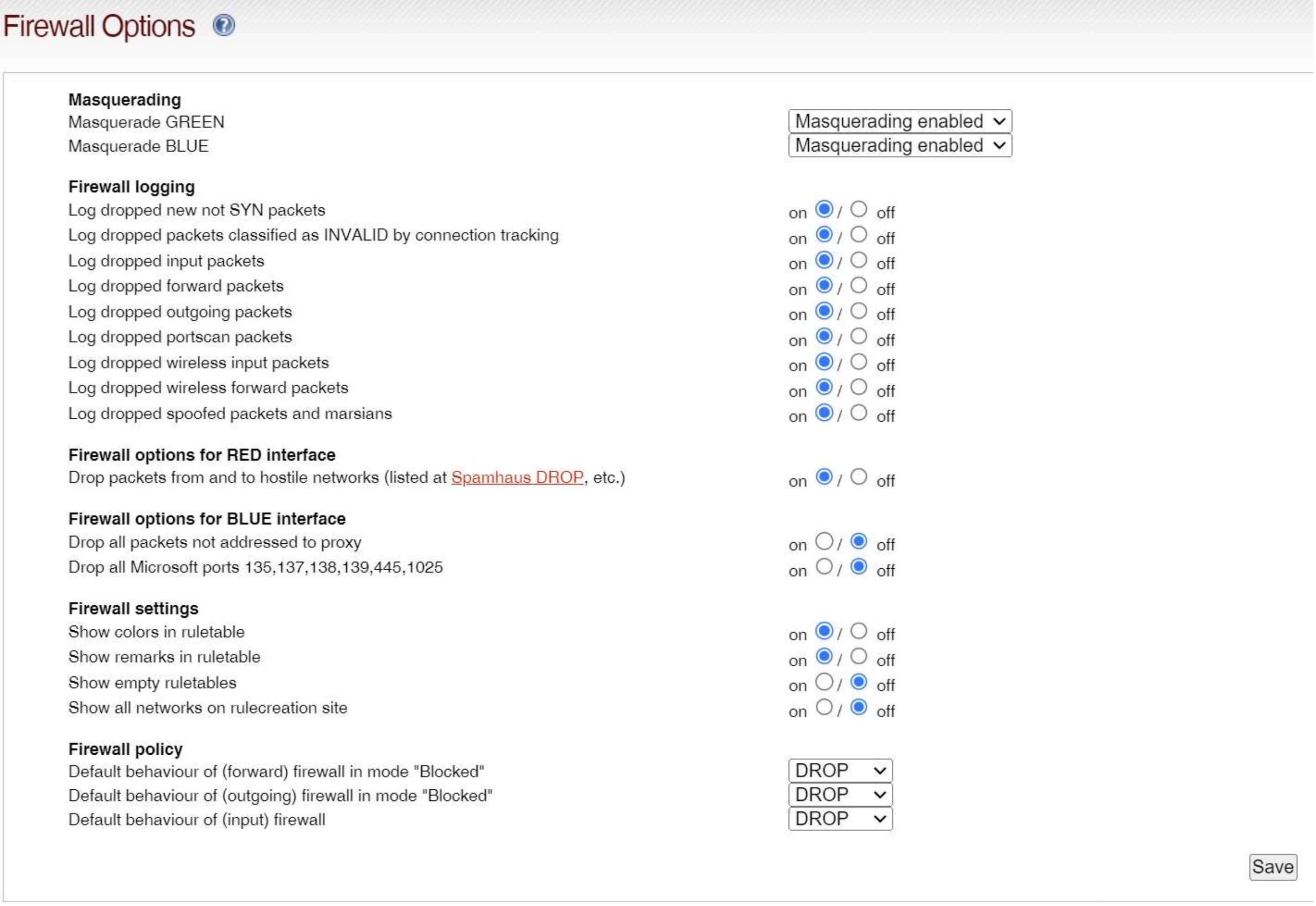
Guardian Configuration

Guardian

Guardian Service		
Daemon	RUNNING	
	PID	Memory
	6037	63980 KB

Guardian Configuration

Common Settings			
Enable Guardian:	☑		
SSH Brute Force Detection	on ● / ○ off		
httpd Brute Force Detection	on ● / ○ off		
Log Facility:	Systemlog	Log Level:	Info
Firewall Action:	Drop	Strike Threshold:	3
Block Time (seconds):	3200		



Firewall Options

Masquerading

Masquerade GREEN	Masquerading enabled
Masquerade BLUE	Masquerading enabled

Firewall logging

Log dropped new not SYN packets	on ● / ○ off
Log dropped packets classified as INVALID by connection tracking	on ● / ○ off
Log dropped input packets	on ● / ○ off
Log dropped forward packets	on ● / ○ off
Log dropped outgoing packets	on ● / ○ off
Log dropped portscan packets	on ● / ○ off
Log dropped wireless input packets	on ● / ○ off
Log dropped wireless forward packets	on ● / ○ off
Log dropped spoofed packets and marsians	on ● / ○ off

Firewall options for RED interface

Drop packets from and to hostile networks (listed at Spamhaus DROP, etc.)	on ● / ○ off

Firewall options for BLUE interface

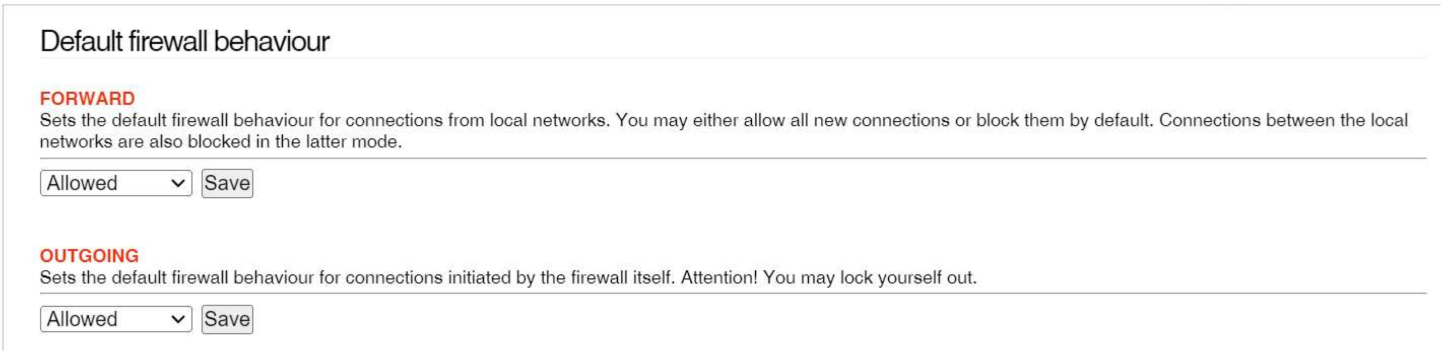
Drop all packets not addressed to proxy	on ○ / ● off
Drop all Microsoft ports 135,137,138,139,445,1025	on ○ / ● off

Firewall settings

Show colors in ruletable	on ● / ○ off
Show remarks in ruletable	on ● / ○ off
Show empty ruletables	on ○ / ● off
Show all networks on rulecreation site	on ○ / ● off

Firewall policy

Default behaviour of (forward) firewall in mode "Blocked"	DROP
Default behaviour of (outgoing) firewall in mode "Blocked"	DROP
Default behaviour of (input) firewall	DROP



Default firewall behaviour

FORWARD

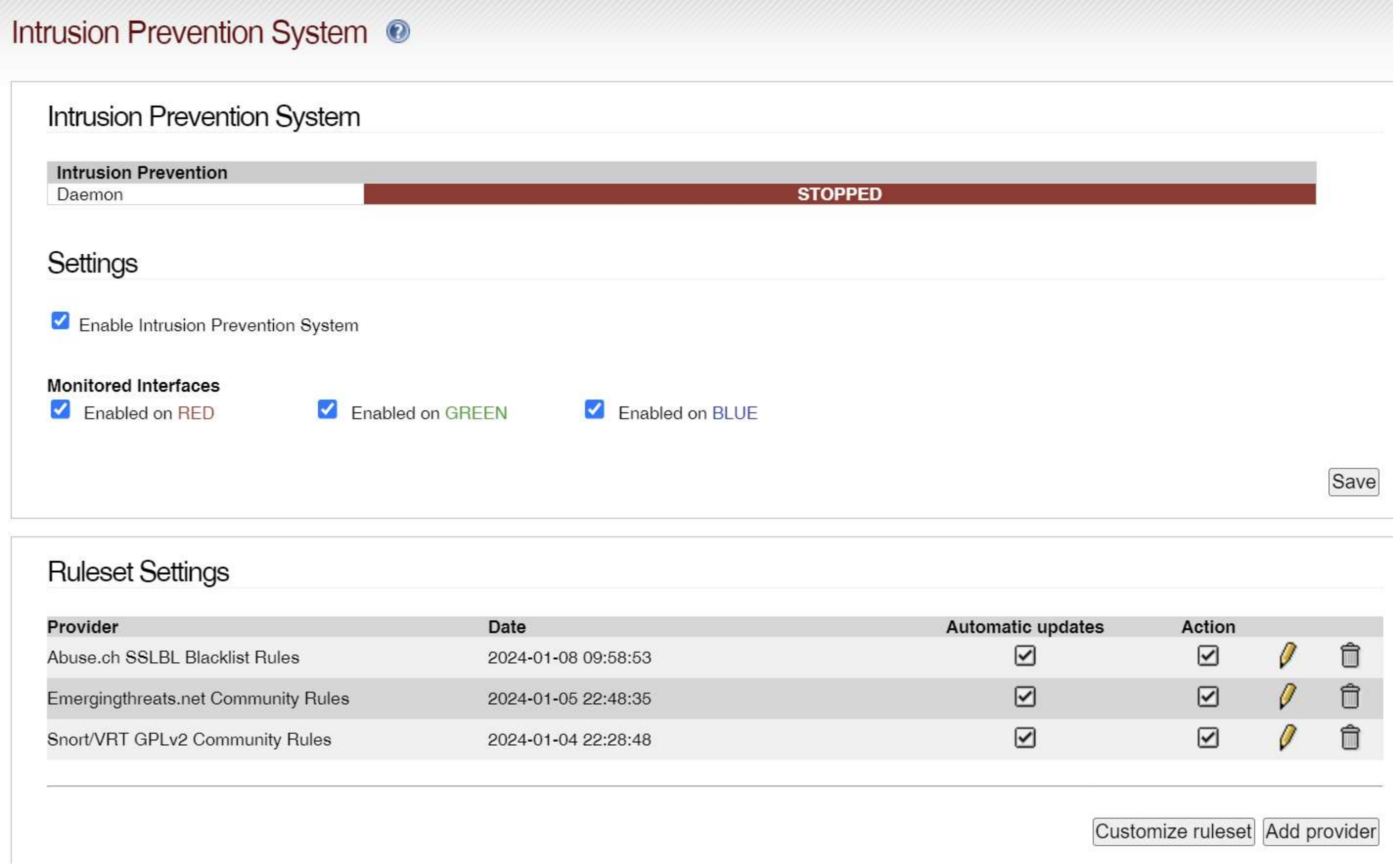
Sets the default firewall behaviour for connections from local networks. You may either allow all new connections or block them by default. Connections between the local networks are also blocked in the latter mode.

Allowed

OUTGOING

Sets the default firewall behaviour for connections initiated by the firewall itself. Attention! You may lock yourself out.

Allowed



Intrusion Prevention System

Intrusion Prevention System

Intrusion Prevention	
Daemon	STOPPED

Settings

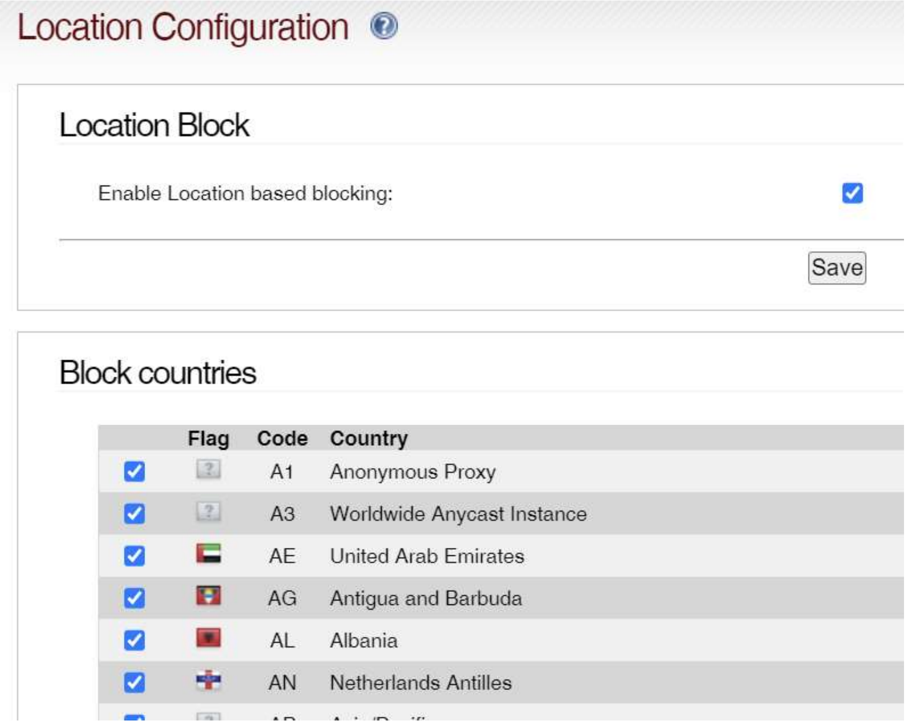
☑ Enable Intrusion Prevention System

Monitored Interfaces

☑ Enabled on RED ☑ Enabled on GREEN ☑ Enabled on BLUE

Ruleset Settings

Provider	Date	Automatic updates	Action		
Abuse.ch SSLBL Blacklist Rules	2024-01-08 09:58:53	☑	☑	✎	🗑
Emergingthreats.net Community Rules	2024-01-05 22:48:35	☑	☑	✎	🗑
Snort/VRT GPLv2 Community Rules	2024-01-04 22:28:48	☑	☑	✎	🗑



Location Configuration

Location Block

Enable Location based blocking: ☑

Block countries

	Flag	Code	Country
☑		A1	Anonymous Proxy
☑		A3	Worldwide Anycast Instance
☑		AE	United Arab Emirates
☑		AG	Antigua and Barbuda
☑		AL	Albania
☑		AN	Netherlands Antilles

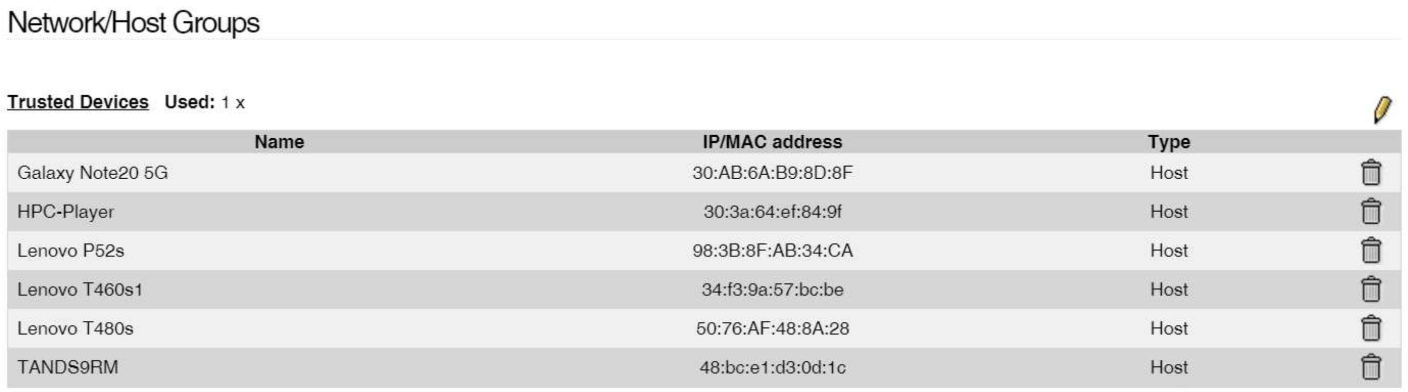
Everything in Location Block is blocked.

All countries, all locations.

Specific Firewall rules

Firewall groups - Trusted devices

in order to grant some WIFI devices access to resources on the LAN connected network one must add the devices to a group:

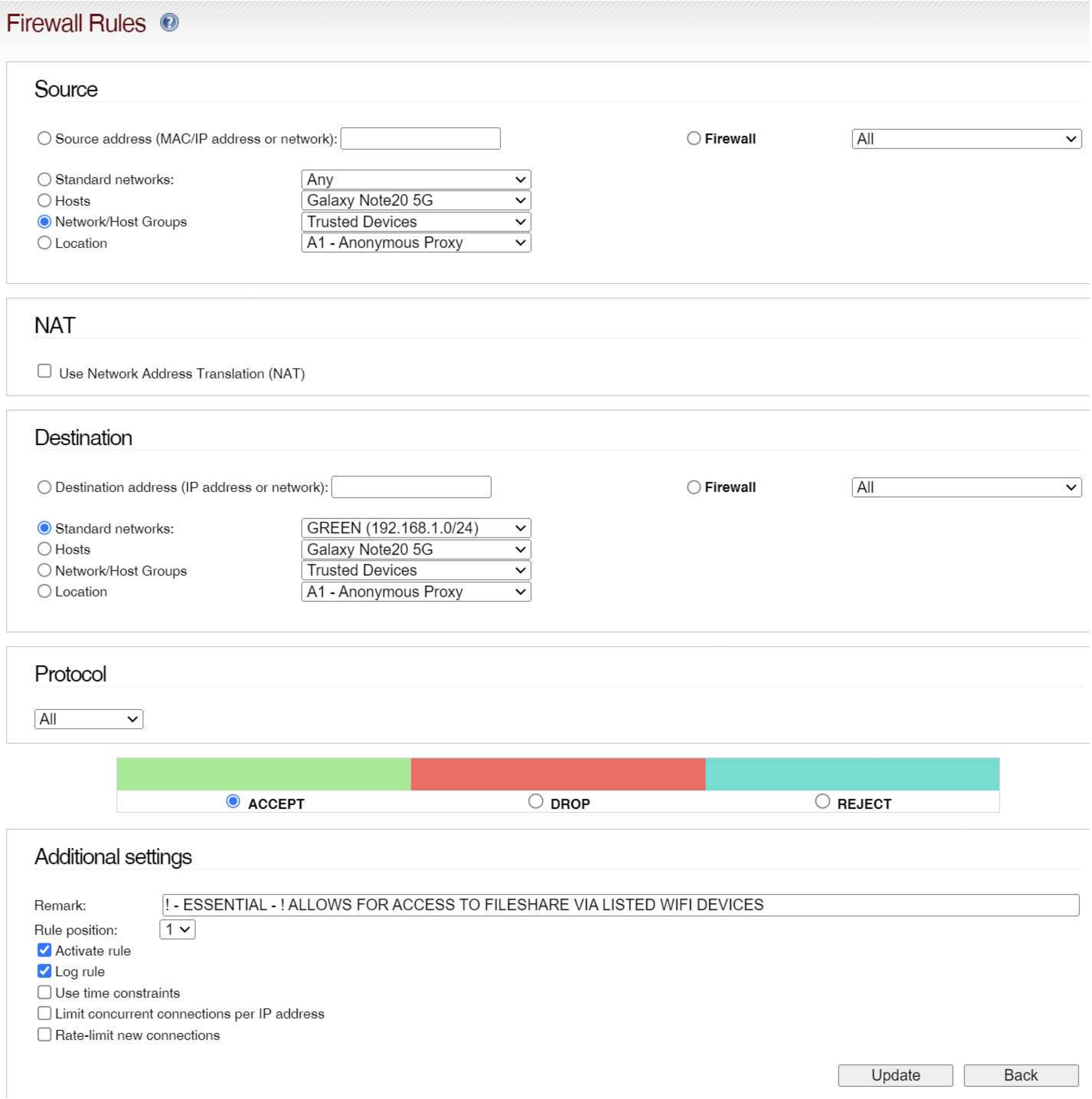


Network/Host Groups

Trusted Devices **Used:** 1 x

Name	IP/MAC address	Type
Galaxy Note20 5G	30:AB:6A:B9:8D:8F	Host
HPC-Player	30:3a:64:ef:84:9f	Host
Lenovo P52s	98:3B:8F:AB:34:CA	Host
Lenovo T460s1	34:f3:9a:57:bc:be	Host
Lenovo T480s	50:76:AF:48:8A:28	Host
TANDS9RM	48:bc:e1:d3:0d:1c	Host

Then add that group to a firewall rule:



Firewall Rules

Source

○ Source address (MAC/IP address or network): ○ **Firewall** All

○ Standard networks:	Any
○ Hosts	Galaxy Note20 5G
● Network/Host Groups	Trusted Devices
○ Location	A1 - Anonymous Proxy

NAT

□ Use Network Address Translation (NAT)

Destination

○ Destination address (IP address or network): ○ **Firewall** All

● Standard networks:	GREEN (192.168.1.0/24)
○ Hosts	Galaxy Note20 5G
○ Network/Host Groups	Trusted Devices
○ Location	A1 - Anonymous Proxy

Protocol

All

● **ACCEPT** ○ **DROP** ○ **REJECT**

Additional settings

Remark: ! - ESSENTIAL - ! ALLOWS FOR ACCESS TO FILESHARE VIA LISTED WIFI DEVICES

Rule position: 1

☑ Activate rule

☑ Log rule

□ Use time constraints

□ Limit concurrent connections per IP address

□ Rate-limit new connections