Securing My Home Network with OPNsense

Objective

To enhance the security, visibility, and control of the home network by deploying an open-source firewall solution.

Hardware and Virtualization Setup

- Hardware Specs: Intel Core i3-2120 @ 3.30GHz, 8 GB RAM
- Host OS: Proxmox VE
- Guest VM: OPNsense Firewall

Network Architecture

- Router: Set to Bridge Mode to disable NAT and pass traffic directly to OPNsense.
- OPNsense VM: Serves as the main firewall and gateway.
- LAN Devices: Connected via a switch and Wi-Fi access point, behind the OPNsense VM.

Implemented Features and Benefits

- Traffic Routing and Monitoring: Full visibility into all internet traffic.
- Malware Protection: Uses Suricata IDS/IPS for real-time packet inspection.
- Content Filtering: With Sensei plugin, blocks malicious domains, ads, and tracking scripts.
- Per-Device Usage Monitoring: Bandwidth tracking, website visits, and connection attempts.
- DNS Query Forwarding: Enforces use of family-safe DNS servers (e.g., OpenDNS: 208.67.220.123).
- Network-wide IDS with Suricata: Applies rules to all devices.

Custom Blocking Rules (Suricata)

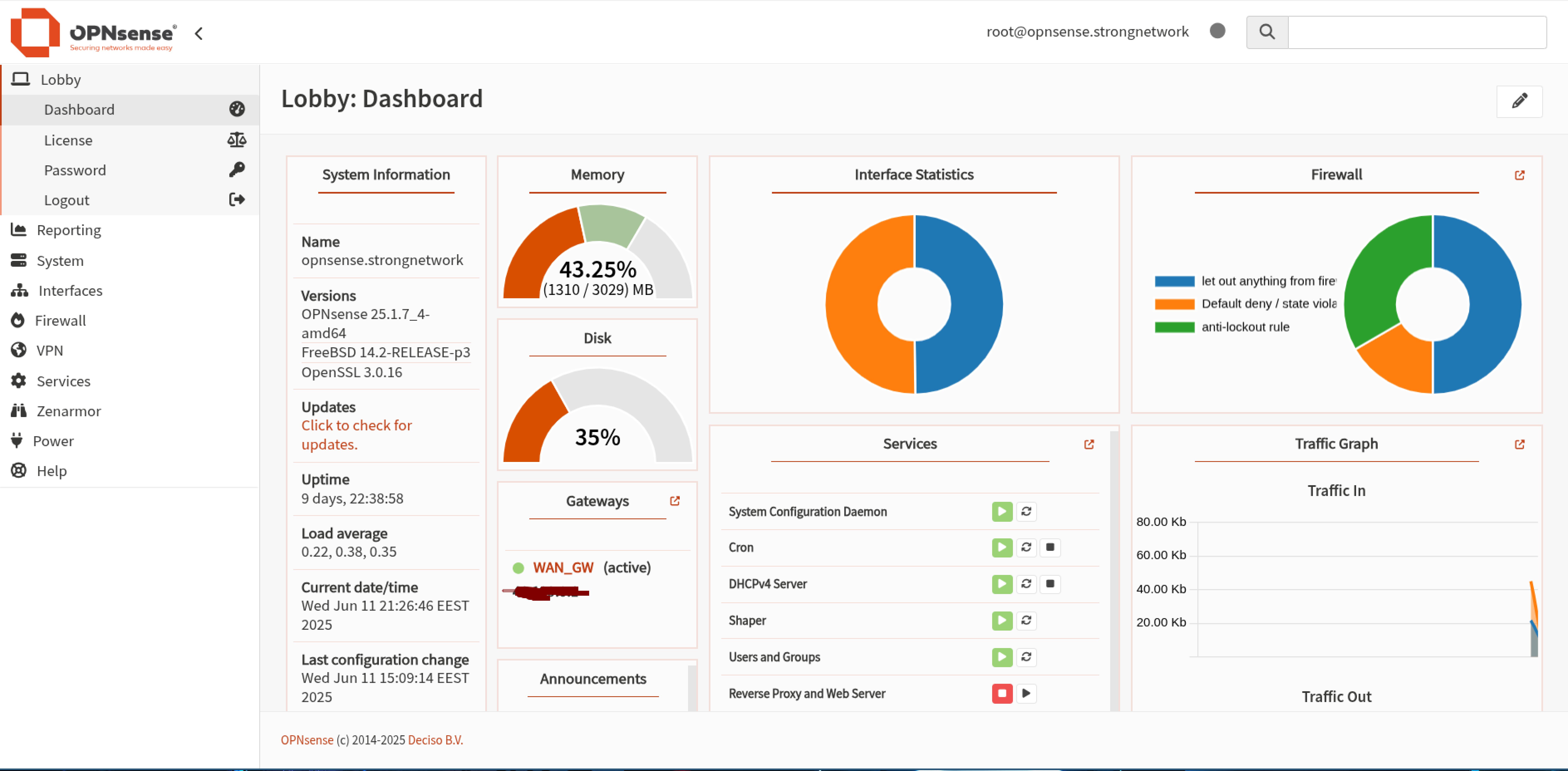
```
drop dns $HOME_NET any -> any any (msg:"Block vpn-super-8e2b5.firebaseio.com"; content:"vpn-super-8e2b5.firebaseio.com"; nocase; sid:1000003;)
drop dns $HOME_NET any -> any any (msg:"Block account.getsuperulimited.com"; content:"account.getsuperulimited.com"; nocase; sid:1000004;)
```

Zenarmor (Sensei) Integration

- Real-time detection of threats
- Dashboard showing blocked threats, top hosts, apps, and traffic sessions
- Optional cloud reporting with Zenconsole

Conclusion

Deploying OPNsense on a Proxmox VM enables enterprise-grade network management at minimal cost. The configuration offers robust control, visibility, and filtering across all devices, enhancing overall home network security and performance.



OPNsense® Securing networks made easy

root@opnsense.strongnetwork

- Lobby
  - Dashboard
  - License
  - Password
  - Logout
- Reporting
- System
- Interfaces
- Firewall
- VPN
- Services
- Zenarmor
- Power
- Help

Lobby: Dashboard

System Information

Name
opnsense.strongnetwork

Versions
OPNsense 25.1.7_4-amd64
FreeBSD 14.2-RELEASE-p3
OpenSSL 3.0.16

Updates
Click to check for updates.

Uptime
9 days, 22:38:58

Load average
0.22, 0.38, 0.35

Current date/time
Wed Jun 11 21:26:46 EEST 2025

Last configuration change
Wed Jun 11 15:09:14 EEST 2025

Memory

43.25%
(1310 / 3029) MB

Disk

35%

Gateways

● WAN_GW (active)
[redacted]

Announcements

Interface Statistics

Firewall

Services

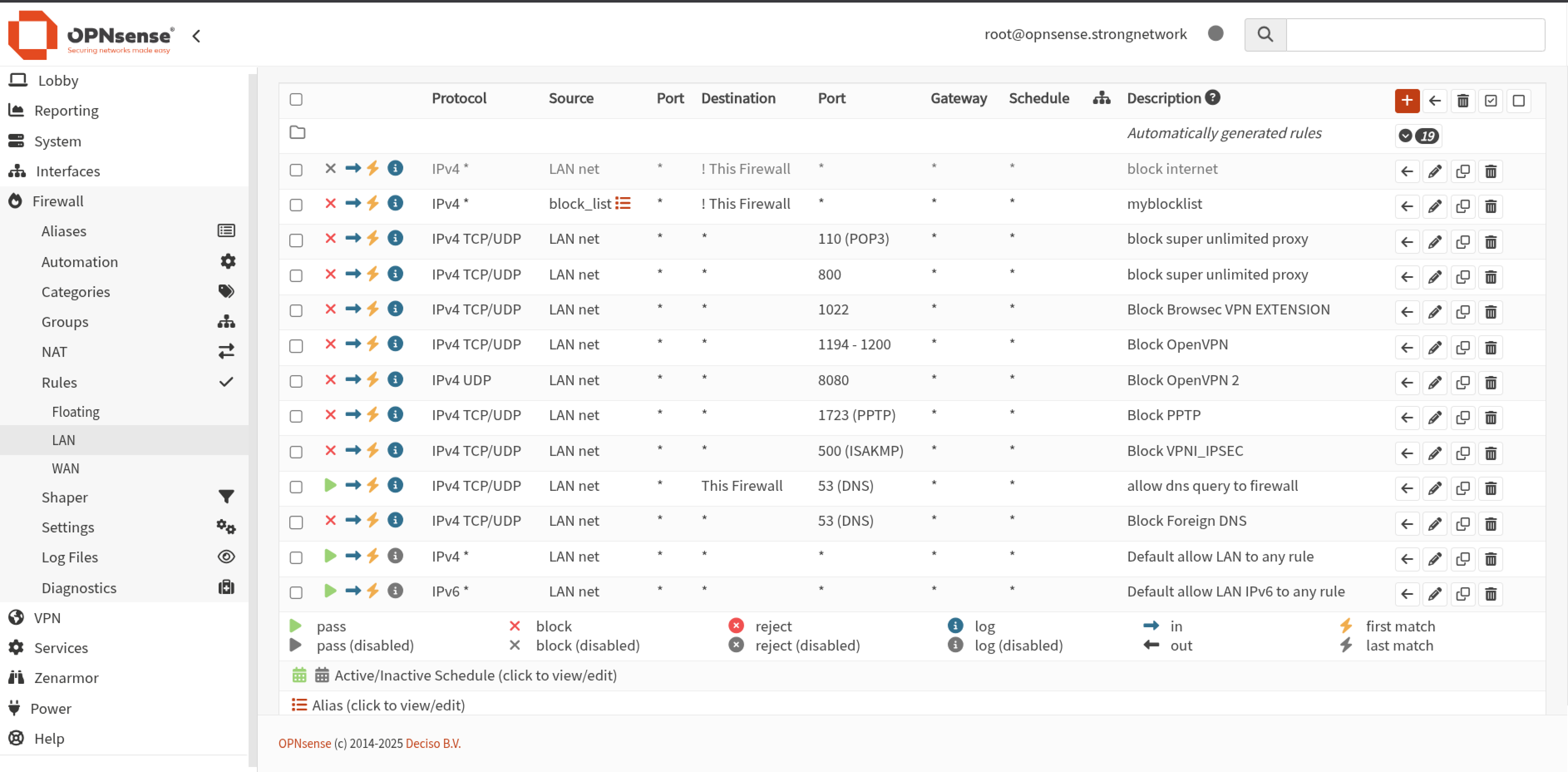
System Configuration Daemon	▶ ↻
Cron	▶ ↻ ■
DHCPv4 Server	▶ ↻ ■
Shaper	▶ ↻
Users and Groups	▶ ↻
Reverse Proxy and Web Server	■ ▶

Traffic Graph

Traffic In

Traffic Out

OPNsense (c) 2014-2025 Deciso B.V.



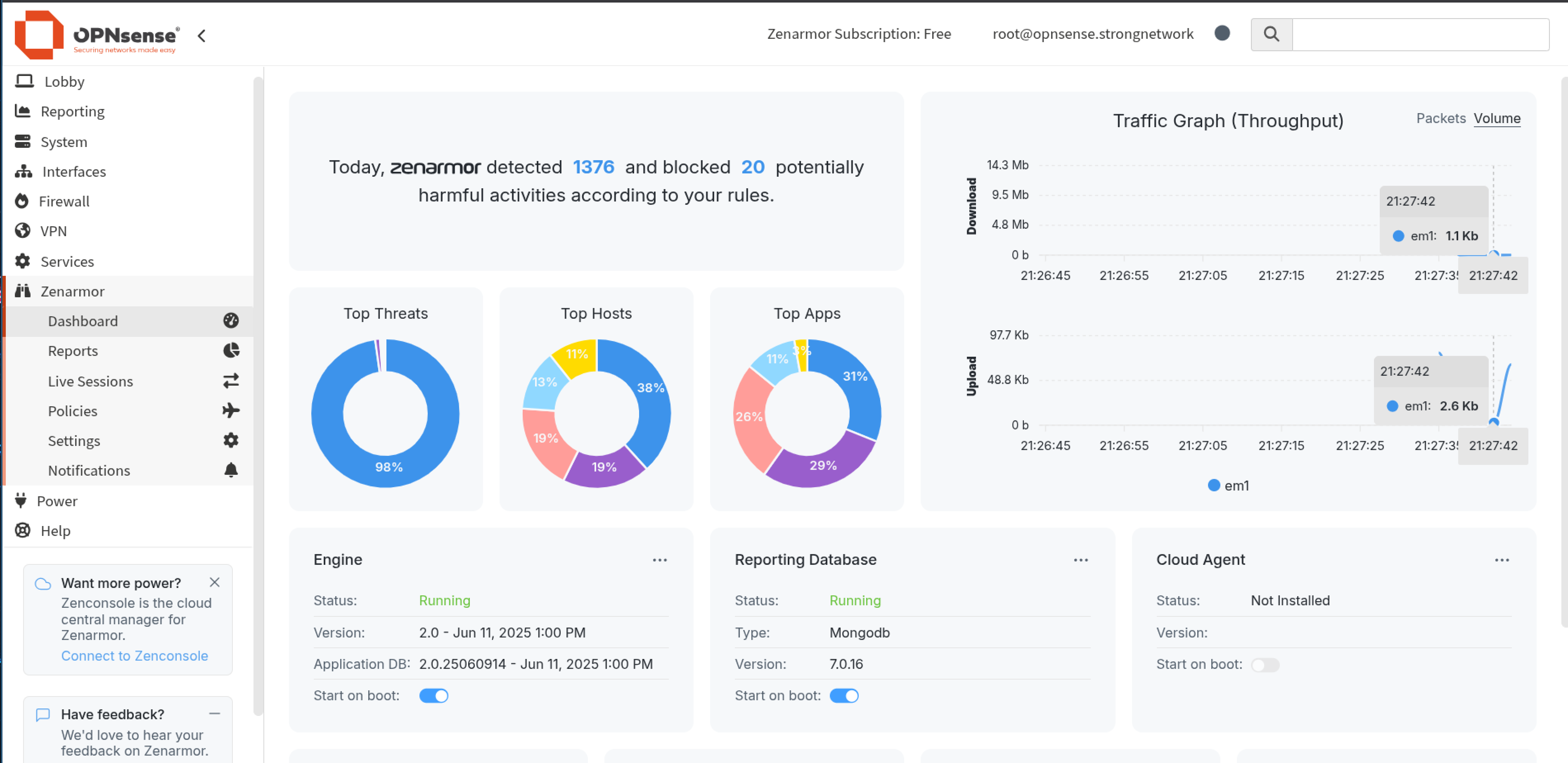
□		Protocol	Source	Port	Destination	Port	Gateway	Schedule		Description
										Automatically generated rules 19
□	✕ → ⚡ ℹ	IPv4 *	LAN net	*	! This Firewall	*	*	*		block internet
□	✕ → ⚡ ℹ	IPv4 *	block_list ☰	*	! This Firewall	*	*	*		myblocklist
□	✕ → ⚡ ℹ	IPv4 TCP/UDP	LAN net	*	*	110 (POP3)	*	*		block super unlimited proxy
□	✕ → ⚡ ℹ	IPv4 TCP/UDP	LAN net	*	*	800	*	*		block super unlimited proxy
□	✕ → ⚡ ℹ	IPv4 TCP/UDP	LAN net	*	*	1022	*	*		Block Browsec VPN EXTENSION
□	✕ → ⚡ ℹ	IPv4 TCP/UDP	LAN net	*	*	1194 - 1200	*	*		Block OpenVPN
□	✕ → ⚡ ℹ	IPv4 UDP	LAN net	*	*	8080	*	*		Block OpenVPN 2
□	✕ → ⚡ ℹ	IPv4 TCP/UDP	LAN net	*	*	1723 (PPTP)	*	*		Block PPTP
□	✕ → ⚡ ℹ	IPv4 TCP/UDP	LAN net	*	*	500 (ISAKMP)	*	*		Block VPNI_IPSEC
□	▶ → ⚡ ℹ	IPv4 TCP/UDP	LAN net	*	This Firewall	53 (DNS)	*	*		allow dns query to firewall
□	✕ → ⚡ ℹ	IPv4 TCP/UDP	LAN net	*	*	53 (DNS)	*	*		Block Foreign DNS
□	▶ → ⚡ ℹ	IPv4 *	LAN net	*	*	*	*	*		Default allow LAN to any rule
□	▶ → ⚡ ℹ	IPv6 *	LAN net	*	*	*	*	*		Default allow LAN IPv6 to any rule

▶ pass ✕ block ⊗ reject ℹ log → in ⚡ first match
▶ pass (disabled) ✕ block (disabled) ⊗ reject (disabled) ℹ log (disabled) ← out ⚡ last match

Active/Inactive Schedule (click to view/edit)

☰ Alias (click to view/edit)

OPNsense (c) 2014-2025 Deciso B.V.



Zenarmor Subscription: Free   root@opnsense.strongnetwork

Today, zenarmor detected 1376 and blocked 20 potentially harmful activities according to your rules.

Want more power?
Zenconsole is the cloud central manager for Zenarmor.
Connect to Zenconsole

Have feedback?
We'd love to hear your feedback on Zenarmor.

Engine

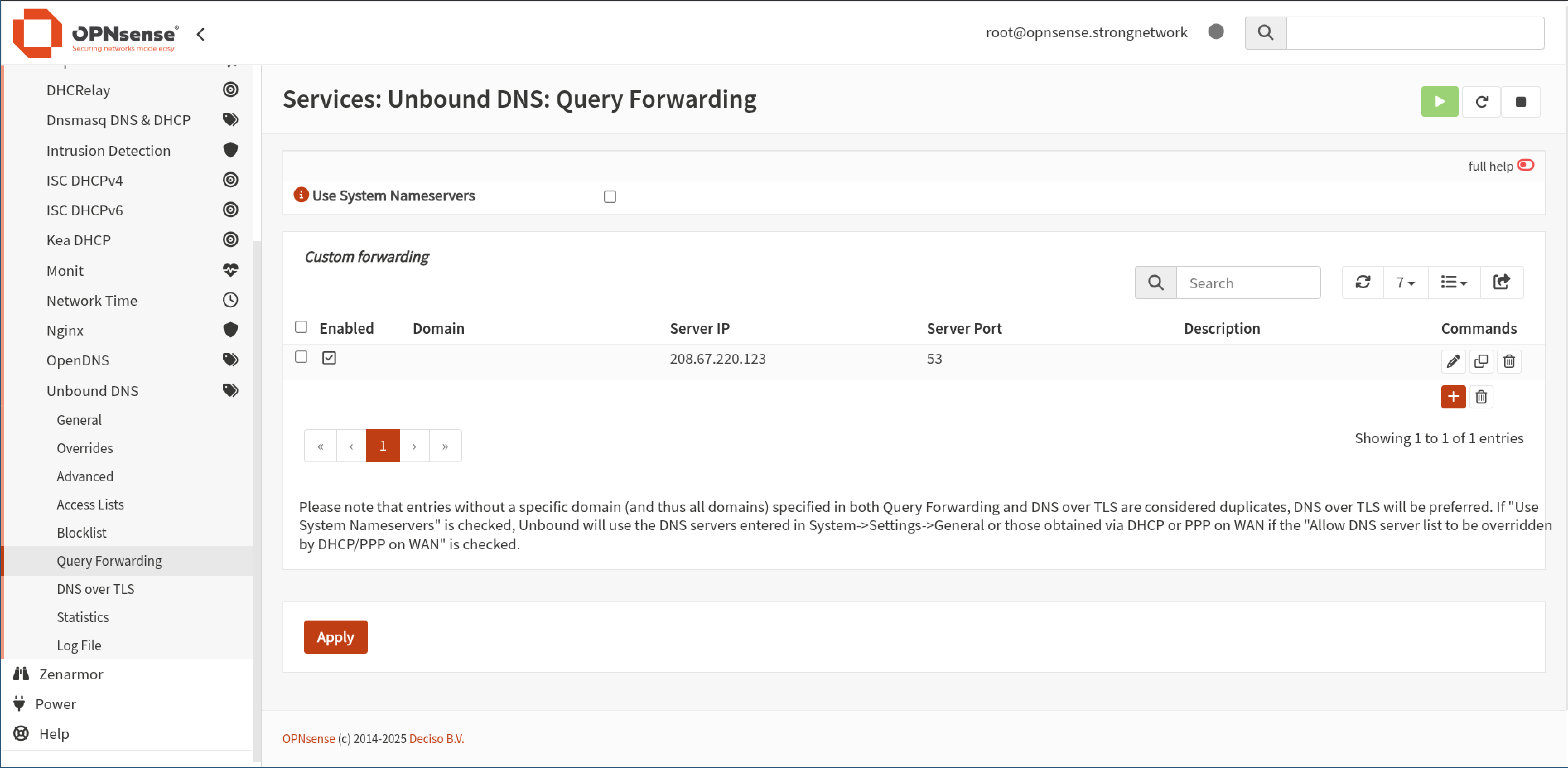
Status:	Running
Version:	2.0 - Jun 11, 2025 1:00 PM
Application DB:	2.0.25060914 - Jun 11, 2025 1:00 PM
Start on boot:	●

Reporting Database

Status:	Running
Type:	Mongodb
Version:	7.0.16
Start on boot:	●

Cloud Agent

Status:	Not Installed
Version:	
Start on boot:	○



Services: Unbound DNS: Query Forwarding

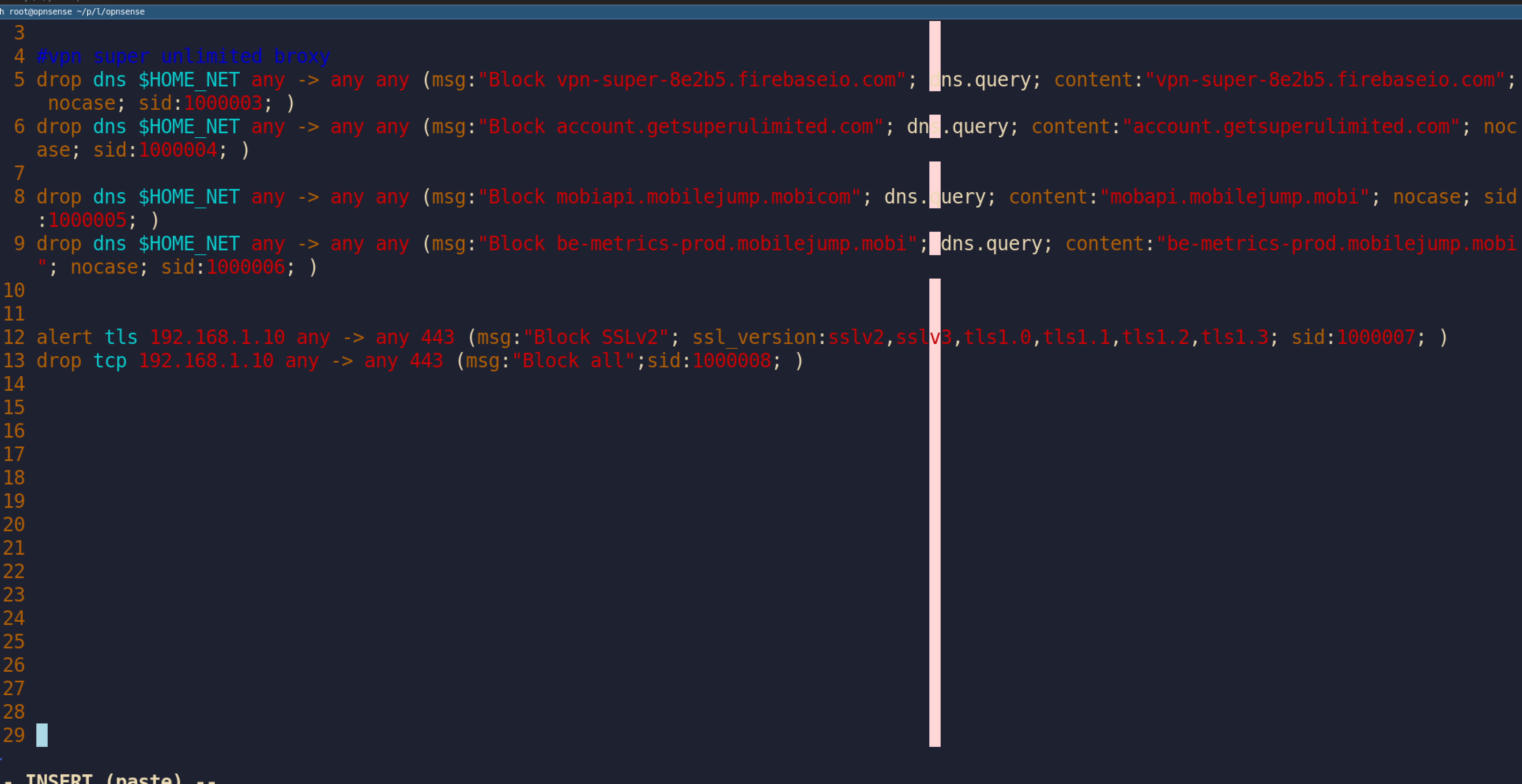
Use System Nameservers □

Custom forwarding

□	Enabled	Domain	Server IP	Server Port	Description	Commands
□	☑		208.67.220.123	53		

Showing 1 to 1 of 1 entries

Please note that entries without a specific domain (and thus all domains) specified in both Query Forwarding and DNS over TLS are considered duplicates, DNS over TLS will be preferred. If "Use System Nameservers" is checked, Unbound will use the DNS servers entered in System->Settings->General or those obtained via DHCP or PPP on WAN if the "Allow DNS server list to be overridden by DHCP/PPP on WAN" is checked.



```
h root@opnsense ~/p/l/opnsense

#vpn super unlimited broxy
drop dns $HOME_NET any -> any any (msg:"Block vpn-super-8e2b5.firebaseio.com"; dns.query; content:"vpn-super-8e2b5.firebaseio.com"; nocase; sid:1000003; )
drop dns $HOME_NET any -> any any (msg:"Block account.getsuperulimited.com"; dns.query; content:"account.getsuperulimited.com"; nocase; sid:1000004; )

drop dns $HOME_NET any -> any any (msg:"Block mobiapi.mobilejump.mobicom"; dns.query; content:"mobapi.mobilejump.mobi"; nocase; sid:1000005; )
drop dns $HOME_NET any -> any any (msg:"Block be-metrics-prod.mobilejump.mobi"; dns.query; content:"be-metrics-prod.mobilejump.mobi"; nocase; sid:1000006; )


alert tls 192.168.1.10 any -> any 443 (msg:"Block SSLv2"; ssl_version:sslv2,sslv3,tls1.0,tls1.1,tls1.2,tls1.3; sid:1000007; )
drop tcp 192.168.1.10 any -> any 443 (msg:"Block all";sid:1000008; )

-- INSERT (paste) --
```