About me

Nathan Ritchey

Network Engineer - YMCA Enterprise Shared Services (YESS)

Information Security Officer, Network & Telephony Engineer - Global Call Center Solutions

Network & Technical Consultant - Southern Colorado Computer Solutions

OPNsense®

Securing networks made easy

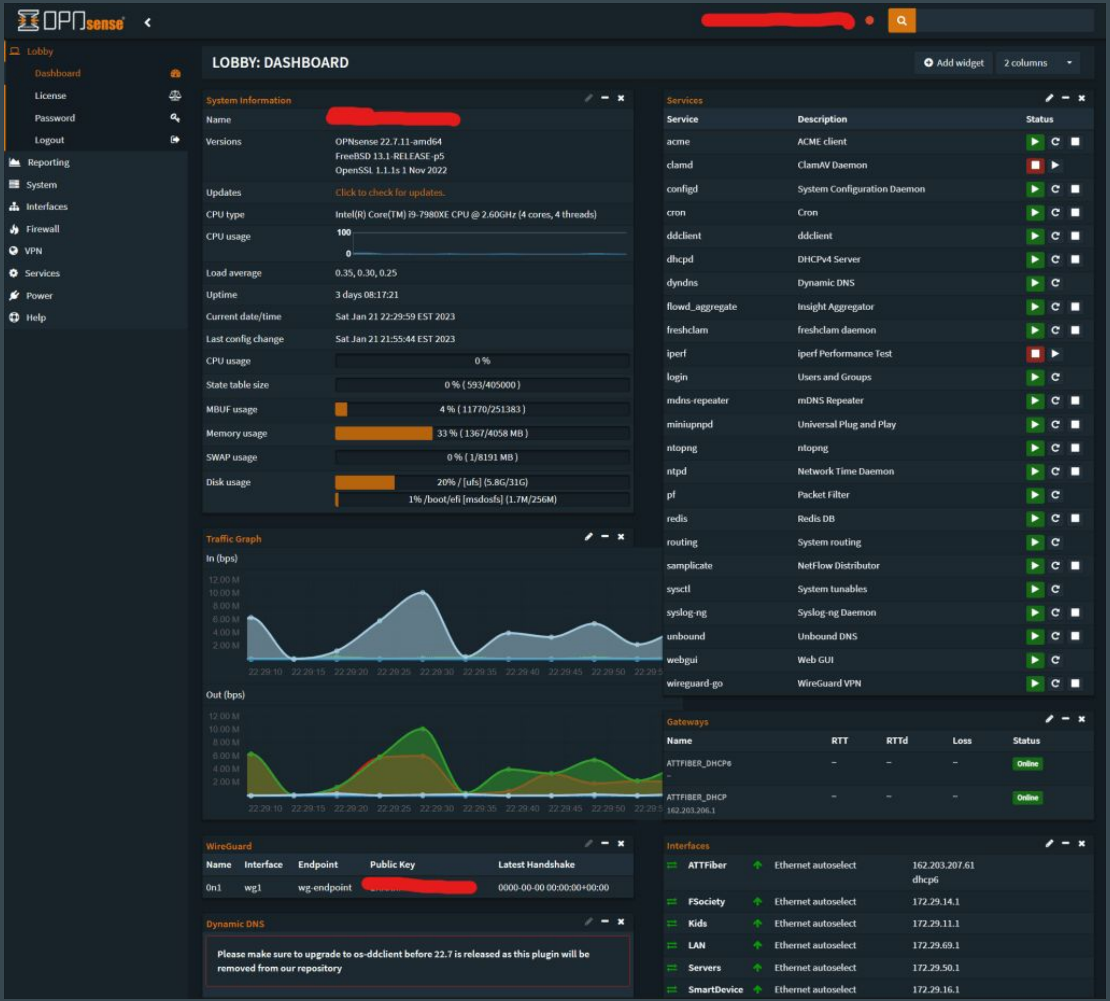
What is OPNsense?

- OPNsense is a router and security appliance forked from pfSense, based on FreeBSD.
- Open-source based on the BSD license.
- Powerful Web based GUI.
- Modular plugins.
- Enterprise features.
- Flexible hardware options.
- Frequent community updates.
- Developed by Deciso B.V. with many community based contributions.

Why OPNsense?

- Flexible hardware support - low cost barrier to entry
- Incredibly useful tool for learning enterprise networking at home
- Highly customizable
- Highly secure
- Highly stable
- Far more secure and stable than an off the shelf router, or your ISPs provided gateway
- More affordable than enterprise firewalls

What it looks like



LOBBY: DASHBOARD

System Information

Name	[redacted]
Versions	OPNsense 22.7.11-amd64 FreeBSD 13.1-RELEASE-p5 OpenSSL 1.1.1s 1 Nov 2022
Updates	Click to check for updates.
CPU type	Intel(R) Core(TM) i9-7980XE CPU @ 2.60GHz (4 cores, 4 threads)
CPU usage	100 0
Load average	0.35, 0.30, 0.25
Uptime	3 days 08:17:21
Current date/time	Sat Jan 21 22:29:59 EST 2023
Last config change	Sat Jan 21 21:55:44 EST 2023
CPU usage	0 %
State table size	0 % (593/405000)
MBUF usage	4 % (11770/251383)
Memory usage	33 % (1367/4058 MB)
SWAP usage	0 % (1/8191 MB)
Disk usage	20% / [ufs] (5.8G/31G) 1% /boot/efi [msdosfs] (1.7M/256M)

Traffic Graph

WireGuard

Name	Interface	Endpoint	Public Key	Latest Handshake
0n1	wg1	wg-endpoint	[redacted]	0000-00-00 00:00:00+00:00

Dynamic DNS

Please make sure to upgrade to os-ddclient before 22.7 is released as this plugin will be removed from our repository

Services

Service	Description	Status
acme	ACME client	▶ ⟳ ■
clamd	ClamAV Daemon	■ ▶
configd	System Configuration Daemon	▶ ⟳ ■
cron	Cron	▶ ⟳ ■
ddclient	ddclient	▶ ⟳ ■
dhcpd	DHCPv4 Server	▶ ⟳ ■
dyndns	Dynamic DNS	▶ ⟳
flowd_aggregate	Insight Aggregator	▶ ⟳ ■
freshclam	freshclam daemon	▶ ⟳ ■
iperf	iperf Performance Test	■ ▶
login	Users and Groups	▶ ⟳
mdns-repeater	mDNS Repeater	▶ ⟳ ■
miniupnpd	Universal Plug and Play	▶ ⟳ ■
ntopng	ntopng	▶ ⟳ ■
ntpd	Network Time Daemon	▶ ⟳ ■
pf	Packet Filter	▶ ⟳
redis	Redis DB	▶ ⟳ ■
routing	System routing	▶ ⟳
samplicate	NetFlow Distributor	▶ ⟳ ■
sysctl	System tunables	▶ ⟳
syslog-ng	Syslog-ng Daemon	▶ ⟳ ■
unbound	Unbound DNS	▶ ⟳ ■
webgui	Web GUI	▶ ⟳
wireguard-go	WireGuard VPN	▶ ⟳ ■

Gateways

Name	RTT	RTTd	Loss	Status
ATTFIBER_DHCP6 ~	~	~	~	Online
ATTFIBER_DHCP 162.203.206.1	~	~	~	Online

Interfaces

⇄	ATTFiber	↑	Ethernet autoselect	162.203.207.61 dhcp6
⇄	FSociety	↑	Ethernet autoselect	172.29.14.1
⇄	Kids	↑	Ethernet autoselect	172.29.11.1
⇄	LAN	↑	Ethernet autoselect	172.29.69.1
⇄	Servers	↑	Ethernet autoselect	172.29.50.1
⇄	SmartDevice	↑	Ethernet autoselect	172.29.16.1

Security Features

- Robust firewall with intentionally restrictive default block rules and stateful packet filtering, per-rule logging, direction, scheduling, and advanced options.
- NAT (forwarding & 1:1)- Full control over inbound and outbound NAT.
- Aliases - Group IPs, ports, URLs, etc. for cleaner firewall rules.
- GeoIP Blocking
- Two-Factor Authentication (2FA)- Built-in support for TOTP and remote auth via LDAP, Radius, etc.
- Two-Factor Authentication (2FA)
- Built-in support for TOTP and remote auth via LDAP, Radius, etc.
- Traffic Shaper - Limit or prioritize traffic based on IP, port, or protocol.

Network Features

- VLAN Support - Configure VLAN interfaces for network segmentation.
- Dynamic DNS (DDNS) - Supports major providers out of the box—great for remote access on dynamic IPs.
- DHCP Server & Static Mappings - Per-interface DHCP server with static lease assignment.
- DNS Resolver (Unbound) - Built-in caching resolver with override, forwarding, and DNSBL options. Also support for DNS over TLS and DNS over HTTPS.
- PPPoE, IPsec, L2TP, GRE, and OpenVPN Support out of the box.

Additional Plugins

- Zenarmor - Next-gen firewall plugin with advanced analytics, application control, and TLS inspection.
- Wireguard - Lightweight, fast VPN support for remote access and site-to-site tunnels.
- HAproxy-High-performance TCP/HTTP load balancer and reverse proxy. Great for self-hosted services.
- Unbound plus - Enhanced Unbound DNS resolver with better control and DNS blocklists.
- AdguardHome - Runs AdGuard Home directly in OpnSense.
- ZeroTier - Bridge your ZeroTier network into your network directly in OPNsense.
- Many, many more.

IDS/IPS

- IDS - Intrusion Detection System - Detects suspicious traffic based on a ruleset.
- IPS - Intrusion Protection System - Blocks suspicious traffic based on a ruleset.
- Suricata is the detection engine used in OPNsense.
- Emerging Threats, Proofpoint ET Pro, and Snort rulesets can be used with Suricata.
- Suricata uses TLS handshake metadata, DNS data, IP, port and protocol patterns, flow anomalies and unencrypted traffic to match traffic to patterns in the rulesets.
- SSL inspection can also be used, but setup is difficult in a non-enterprise environment. This requires installing a trusted CA cert on all client devices.

Ruleset tuning

- A well tuned ruleset is critical for efficient performance when using IDS/IPS
- Using too many rules will greatly degrade network performance.
- Using too aggressive of a ruleset will give you many false-positives.
- Avoid enabling too many rulesets at once, enable a few and test.
- Do not enable rulesets for services you are not running on your network, e.g. webserver or samba. Only cover the services you are running.
- If running IPS, be careful to test rulesets carefully for false-positives - this can break many services.

Suggested starting rulesets

- ET Open/emerging-trojan - Detects Trojan and C2 communication
- ET Open/emerging-malware - Detects known malware signatures
- ET Open/emerging-mobile_malware - Detects malware targeting mobile devices
- ET Open/emerging-current_events - Detects ongoing major threats (e.g. 0-days)
- ET Open/emerging-user_agents - Detects suspicious user-agent strings
- ET Open/emerging-dns - Detects DNS tunneling, fast flux detection
- ET Open/emerging-web_client - Detects threats from web browser activity
- ET Open/emerging-policy - Detects suspicious or unwanted protocols (e.g. tor, etc)
- ET Open/emerging-scan - Detects port scans and probing

Hardware for OPNsense

- OPNsense is an x86/64 software appliance - is not hardware dependent
- Run on cheap upcycled hardware
- Run in a Virtual Machine
- Dedicated hardware appliances

Build your own OPNsense Router!

Time to ditch that off the shelf router full of CVEs...

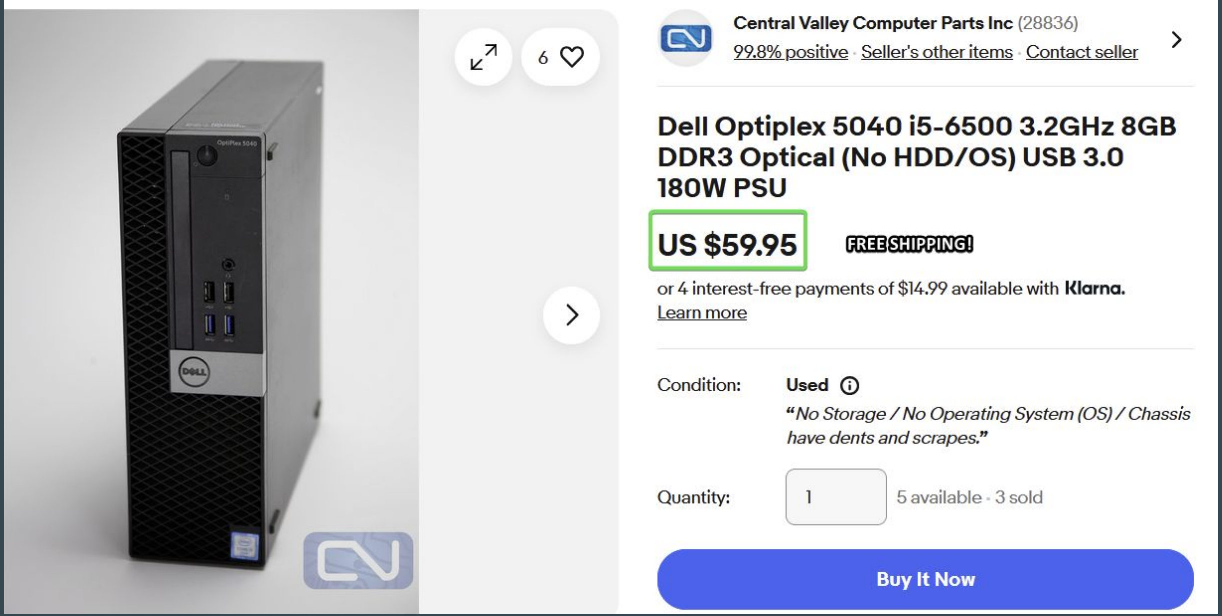
LETS GO!

Basic hardware guidelines

- Old enterprise desktops; Dell Optiplex, ThinClients, SFF PCs, reused old desktop
- PCIe interface is highly recommended.
- Dual gigabit network card.
- 8Gb RAM for basic setup, 16GB for IPS.
- Dual Core CPU.
- Cheap 64GB or 128GB SSD.
- Intel NIC recommended - Avoid Broadcom/Realtek at all costs!
- Gigabit Network Switch and WiFi Access Points

Base system

- Cheap Dell enterprise desktop.
- More than enough CPU power for IDS/IPS
- Available PCIe slots for NIC
- Not super efficient (25-35 watts idle, 45-65 watts under load)



Central Valley Computer Parts Inc (28836)

99.8% positive · Seller's other items · Contact seller

Dell Optiplex 5040 i5-6500 3.2GHz 8GB DDR3 Optical (No HDD/OS) USB 3.0 180W PSU

US $59.95 FREE SHIPPING!

or 4 interest-free payments of $14.99 available with Klarna. Learn more

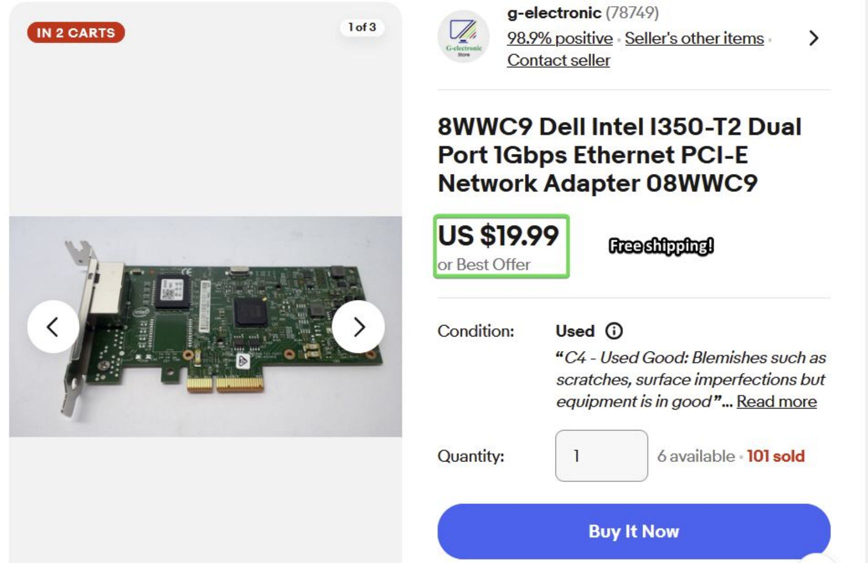
Condition: **Used**

"No Storage / No Operating System (OS) / Chassis have dents and scrapes."

Quantity: 1 5 available · 3 sold

Network card

- Reliable enterprise grade Dual Gigabit Network card.
- Look for Intel based card.
- Cheap!
- One port for WAN, one port for LAN.
- Quad port cards don’t cost much more, and allow for more advanced setups if needed. ($30)
- Dual SPF+ 10G cards for >1Gbps ($45)
- AVOID BROADCOM or REALTEK!



g-electronic (78749)
98.9% positive · Seller's other items · Contact seller

8WWC9 Dell Intel I350-T2 Dual Port 1Gbps Ethernet PCI-E Network Adapter 08WWC9

US $19.99
or Best Offer

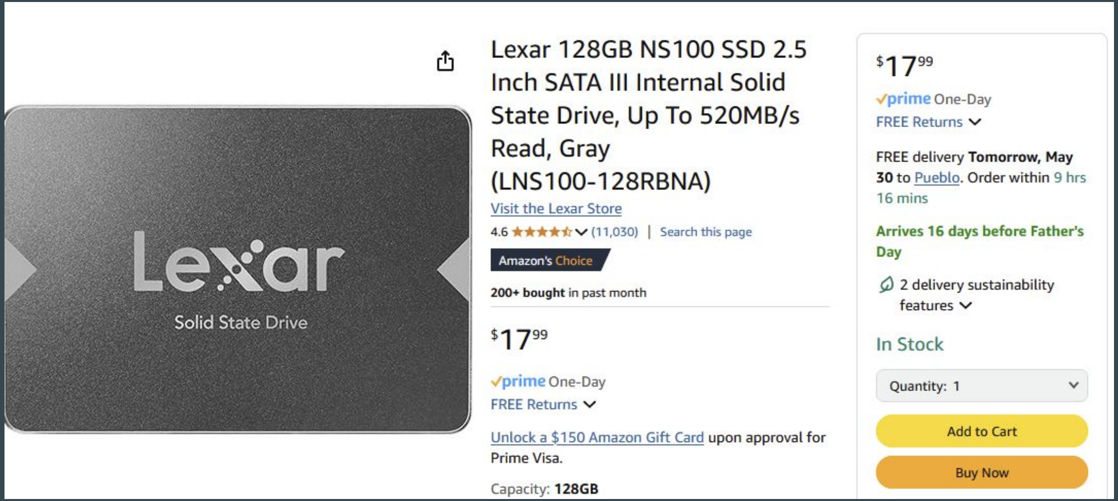
Free shipping!

Condition: **Used**
“C4 - Used Good: Blemishes such as scratches, surface imperfections but equipment is in good”... Read more

Quantity: 1 6 available · 101 sold

Cheap basic setup

- 128GB SATA SSD ($18)
- Plenty of space for IDS rule sets and logging.
- You can run two SSDs on this system for drive mirroring.
- OPNsense Supports ZFS Mirror (RAID1) out of the box.
- Allows for redundancy in case of drive failure.



Lexar 128GB NS100 SSD 2.5 Inch SATA III Internal Solid State Drive, Up To 520MB/s Read, Gray (LNS100-128RBNA)

Visit the Lexar Store

4.6 ★★★★☆ (11,030) | Search this page

Amazon's Choice

200+ bought in past month

$17.99

✓prime One-Day

FREE Returns

Unlock a $150 Amazon Gift Card upon approval for Prime Visa.

Capacity: **128GB**

$17.99

✓prime One-Day

FREE Returns

FREE delivery **Tomorrow, May 30** to Pueblo. Order within 9 hrs 16 mins

Arrives 16 days before Father's Day

2 delivery sustainability features

In Stock

Quantity: 1

Additional Network Gear

- Network switch for your LAN
  - CHEAP used Gigabit switches - $20 - $50 (craigslist, FB marketplace, ebay, ask around)
  - MikroTik Switches - $100+
  - Unifi Switches -$200+
- Wireless Access Points for Wi-Fi
  - Mikrotik HAPs - $30+
  - Unifi APs - $60+
  - Trendnet, TP-Link Etc...
- Repurpose your old router! - FREE
  - Disable DHCP and routing features to turn it into a switch and AP
  - Install DD-WRT/Opnwrt to give extra functionality/stability.

Total cost

- Old desktop PC - $60
- Network card - $20
- SSD - $20
- Used switch $20
- MikroTik HAP $20

Total $140

Comparable off shelf routers are $150+!!!

This one is $700 and can’t even do half of what OPNsense can! ---------------->

Installing OPNsense

- Get your system ready - Install SSD and network card.
- Download installer ISO from https://opnsense.org/download/ and write iso to USB flash drive with Rufus or dd.
- Set your PC to boot from USB, and boot the installer.
- Once installer finishes, reboot and sign into the CLI (root/opnsesne is default)
- Assign network interfaces to WAN and LAN.
- Sign into web interface (https://192.168.1.1 is the default)
- Reset root password
- Install updates

(If you are using an ISP provided gateway/router, don’t forget to put it in bridge mode)

Additional Resources

Your Router Sucks. Build Your Own Instead!
2.1M views • 2 years ago
Linus Tech Tips
Did you know that you can build your own router that can perform better th...
4K CC
Matching chapter 4:01 Installing and configuring...

LTT - How to build an OPNsense router

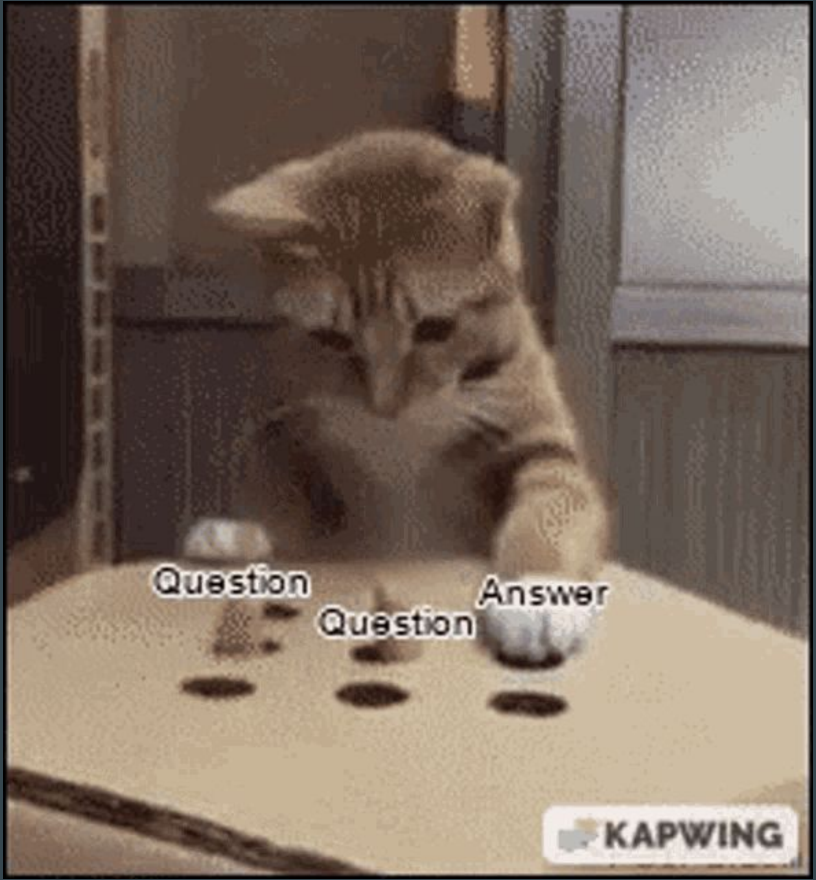
A pretty great Homelab firewall in a tiny package - The Lenovo M720q with SFP+ for...
147K views • 8 months ago
KTZ Systems
In this video I break down a recent build of a Lenovo M720q box that has d...
4K CC
10 chapters Intro | Temporary desk setup | Software...

Powerful OPNsense build

Official OPNsense Documentation

Questions?

Comments?



Access this presentation