



OPNsense® Open Source Security

High-end security made easy™

OPNsense is a fully featured security platform that secures your network with high-end features such as inline intrusion prevention, virtual private networking, two factor authentication, captive portal and filtering web proxy. The optional high availability setup ensures stable network performance with automatic failover and synchronised states, minimising disruption. **Keep your network secure and the good packets flowing.**



Stateful Inspection Firewall



Inline Intrusion Prevention & SSL Finger Printing



Fast Filtering
The Traffic Shaper eliminates buffer bloat and lower latency.



Virtual Private Networking
Hardware Assisted Encryption



Guard Web Access
Filtering (SSL) Proxy
Captive Portal with Voucher support



On system Logging & Reporting including Netflow analyser (Insight)



System wide two-factor authentication.
Compatible with Google Authenticator.

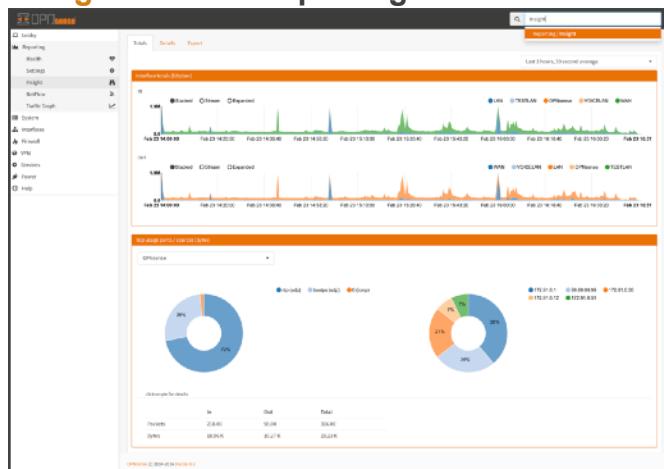
Securing Networks



INTRODUCING OPNsense®

VERSATILE - OPEN SOURCE - FULLY FEATURED

Insight Netflow Reporting



High-end Security Made Easy™

OPNsense® is **Deciso's** fast growing open source firewall and security platform released under an Open Source Initiative approved license. It's rich feature set is combined with the benefits of open and verifiable sources.

All features can be used from within the easy to use graphical interface, equipped with a build-in search feature for quick navigation. Protecting your network has never been this easy, utilise the integrated intrusion prevention capable of blacklisting based on SSL fingerprints and the two-factor authentication for safely connecting mobile users.

Keep full insight on the traffic flowing through your firewall at all times, with its advanced Netflow capture, aggregate & reporting tool 'Insight'.



Businesses

Protect your business network and secure your connections. From the stateful inspection firewall to the inline intrusion detection & prevention system everything is included for free. Use the traffic shaper to enhance network performance and prioritise your voice over IP above other traffic. Backup your configuration to the cloud automatically, no need for manual backups.



School networks

Limit and share available bandwidth evenly amongst students and utilise the category based web filtering to filter unwanted traffic such as adult content and malicious websites. It's easy to setup as no additional plugins nor packages are required.



Hotels

Hotels usually utilise a captive portal to allow guests (paid) access to internet for a limited duration. Guests need to login using a voucher they can either buy or obtain for free at the reception. OPNsense has a build-in captive portal with voucher support and can easily create them on the fly.



On the road

Even on the road OPNsense is a great asset to your business as it offers OpenVPN and IPsec VPN solution with road warrior support and two-factor authentication. The easy client exporter makes configuring your OpenVPN SSL client setup a breeze.



Remote Offices & SOHO

Utilise the integrated site to site VPN (IPsec or SSL VPN) to create a secure network connection to and from your remote offices. Enjoy the easy configuration and online searchable documentation with simple how-to type of articles to get you started, quickly.

Professional support for Businesses, Integrators & Resellers



Supported

Securing Networks



STATEFUL INSPECTION FIREWALL

“A stateful firewall is a firewall that keeps track of the state of network connections (such as TCP streams, UDP communication) traveling across it. The firewall is programmed to distinguish legitimate packets for different types of connections. Only packets matching a known active connection will be allowed by the firewall; others will be rejected.”

source: en.wikipedia.org



Filtering

The firewall can filter traffic on source, destination and protocol as well as port on number (TCP/UDP).

Operating System Fingerprinting (OSFP)

Advanced passive OS fingerprinting technology can be used to allow or block traffic based by the Operating System initiating the connection.

Log matching firewall traffic on a per rule bases

Each rule can be set to log a match, this also allows for easy add of a block or pass rule through the firewall rule log module.

Policy based routing by per rule gateway option

With policy based routing it is possible to add a gateway to a rule and effectively change the standard routing of matching traffic.

Alias support for grouping and naming IPs, networks and ports

Aliases help to keep your firewall ruleset clean and easy to understand, in environments with multiple public IPs and numerous servers.

Rule organisation

Besides interface grouping, where rules are managed for several interfaces at once, firewall rules can also be organised per category to bundle rules that otherwise have no apparent relation to each other.

Transparent layer 2 firewall capable

Bridge interfaces and filter traffic between them, even allowing for an IP-less firewall.

Granular state table control

Adjustable state table size, ability to limit traffic per rule based on simultaneous connections, states per host & new connections per second as well as define state timeout and state type.

Pure routing

Disable the packet filtering to turn the system in to a pure router.



TRAFFIC SHAPING

Traffic shaping (also known as “packet shaping”) is the control of computer network traffic in order to optimise or guarantee performance, lower latency, and/or increase usable bandwidth by delaying packets that meet certain criteria. More specifically, traffic shaping is any action on a set of packets (often called a stream or a flow), which imposes additional delay on those packets such that they conform to some predetermined constraint (a contract or traffic profile).



Easy and flexible

Traffic shaping within OPNsense is very flexible and is organised around pipes, queues and corresponding rules. The pipes define the allowed bandwidth, the queues can be used to set a weight within the pipe and finally the rules are used to apply the shaping to a certain package flow. The shaping rules are handled independently from the firewall rules and other settings.

Limit bandwidth

Bandwidth limitations can be defined based upon the interface(s), ip source & destination, direction of traffic (in/out) and port numbers (application).

Bandwidth sharing

The available bandwidth can be shared evenly over all users, this allows for optimum performance at all times.

Prioritise

Traffic can be prioritised by adding queues and defining weights. Applications with a higher weight can consume more bandwidth than others when the total available bandwidth is limited.



Securing Networks



CAPTIVE PORTAL

Captive Portal allows you to force authentication, or redirection to a click through page for network access. This is commonly used on hot spot networks, but is also widely used in corporate networks for an additional layer of security on wireless or Internet access.



✓ Guest Network ✓ Hotel Wifi Access ✓ Bring Your Own Device (BYOD)

Template Manager

OPNsense's unique template manager makes setting up your own login page an easy task. At the same time it offers additional functionalities, such as:

- ✓ URL redirection
- ✓ Option for your own Pop-up
- ✓ Custom Splash page

Zone Manager

Different zones can be setup on each interface or multiple interfaces can share one zone setup. Each Zone can use a different Captive Portal Template or share it with another zone.

Voucher Manager

OPNsense's Captive Portal has an easy voucher creation system that exports the vouchers to a csv file for use with your favourite application. The export allows you to print vouchers by merging them with your word or open office template and create a good looking handout with your logo and company style.



Authentication

Secure authentication via HTTPS or splash-only portal with URL redirection to a given page. Different sources can be used to authenticate a user in a zone:

- ✓ LDAP [Microsoft Active Directory]
- ✓ Radius
- ✓ Local user manager
- ✓ Vouchers / Tickets
- ✓ Two-Factor One Time Password (2FA)
- ✓ No authentication (Splash Screen Only)
- ✓ Multiple (a combination of above)

Bandwidth Management

The integrated traffic shaper can be utilised to:

- ✓ Share bandwidth evenly
- ✓ Prioritise protocols port numbers and/or ip addresses

Portal bypass

MAC and IP addresses can be white listed to bypass the portal.

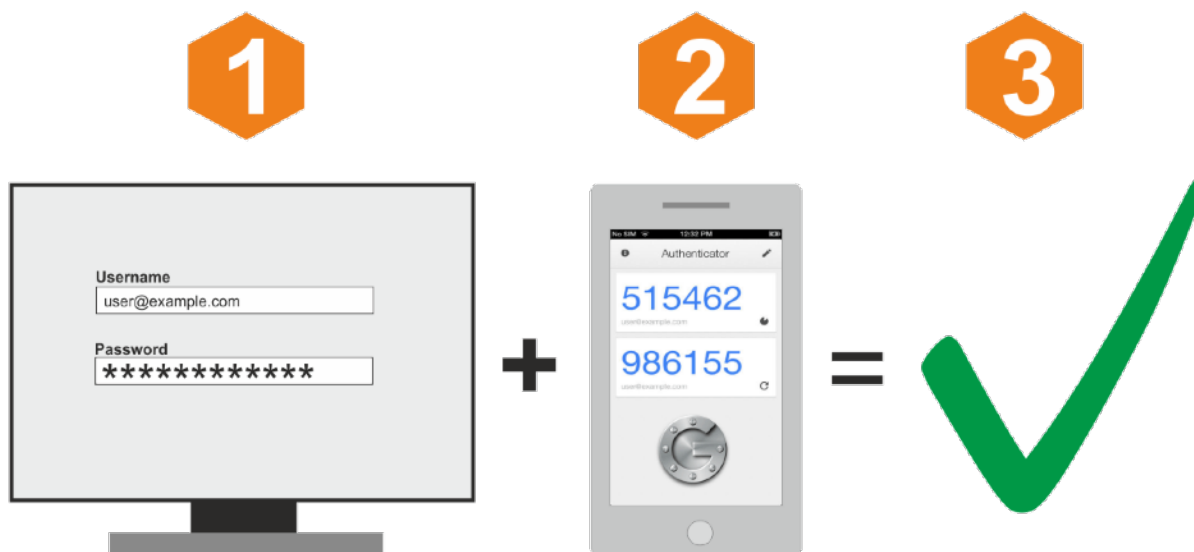
Timeouts & Welcome Back

Connection can be terminated after the user has been idle for a certain amount of time (idle timeout) and/or force a disconnect when a number of minutes have passed even if the user is still active (hard timeout). In case a user reconnect within the idle timeout and/or hard timeout no login is required and the user can resume its active session.



TWO-FACTOR AUTHENTICATION

Two-Factor Authentication also known as 2FA or 2-Step Verification is an authentication method that requires two components, such as a pin/password + a token. OPNsense offers support for Two-factor authentication throughout the entire system.



Time-based One-time Password

TOTP is an algorithm (RFC 6238) that computes a one-time password from a shared secret key and the current time. OPNsense supports RFC 6238.

Google Authenticator

OPNsense fully supports the use of Google's Authenticator application. This application can generate tokens on Android, iOS and BlackBerry OS. The usage of this application is free and it simple to setup.

Supported 2FA services

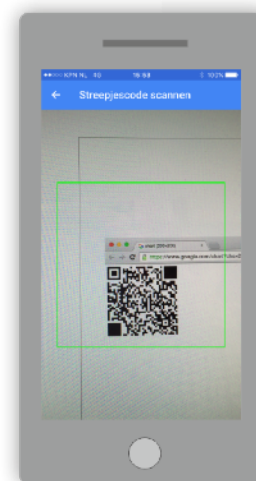
OPNsense supports two-factor authentication throughout the entire system for the following services:

- ✓ OPNsense Graphical User Interface
- ✓ SSH & Console Access
- ✓ Captive Portal
- ✓ Virtual Private Networking - OpenVPN & IPsec
- ✓ Caching Proxy

Easy setup

Configuring Two-Factor authentication is easy using Google's Authenticator.

- ✓ Integrated in OPNsense's unified authentication system
- ✓ Automatic Seed Generation
- ✓ Token activation by Barcode Scanning



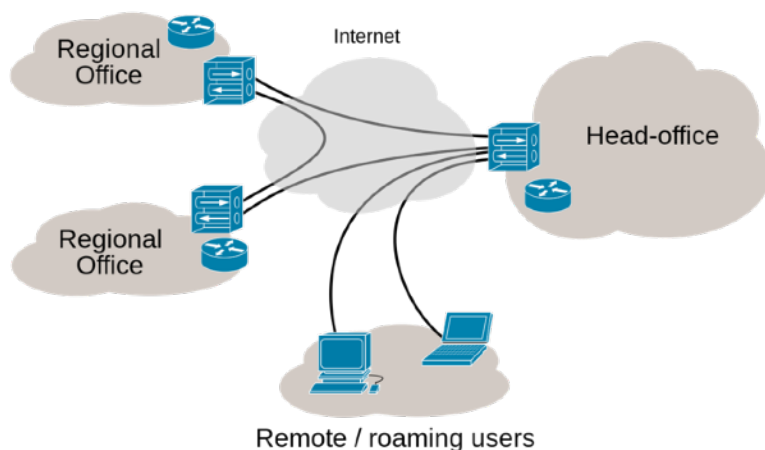
Securing Networks



VIRTUAL PRIVATE NETWORK

A virtual private network (VPN) extends a private network across a public network, such as the Internet. It enables a computer to send and receive data across shared or public networks as if it is directly connected to the private network, while benefiting from the functionality, security and management policies of the private network.

Internet VPN



Supported VPN technologies

OPNsense offers a wide range of VPN technologies ranging from modern SSL VPN's or even full mesh VPN routing using Tinc to well known IPsec as well as older (now considered insecure) legacy options such as L2TP and PPTP.

OpenVPN

A powerful SSL VPN solution supporting a wide range of client operating systems including mobile (Android / IOS).

Tinc

Tinc is a mesh based VPN solution that can be used to build a secure, encrypted pseudo-VLAN over the the public internet.

Legacy Support

OPNsense has legacy support for L2TP and PPTP, just in case you need it.

IPsec

IPsec allows connectivity with any device supporting standard IPsec. This is most commonly used for site to site connectivity to other OPNsense installations, other open source firewalls, and most commercial firewall solutions (Cisco, Juniper, etc.). It can also be used for mobile client connectivity (road warrior).



Supported Clients

✓ Viscosity (Mac OSX & Windows) ✓ OpenVPN for Android ✓ OpenVPN Connect (IOS)

Two-Factor Authentication

- ✓ Supports TOTP Tokens
- ✓ Integrated Support for Google Authenticator
- ✓ Easy Setup



Google Authenticator

Free Token Generation, supports:

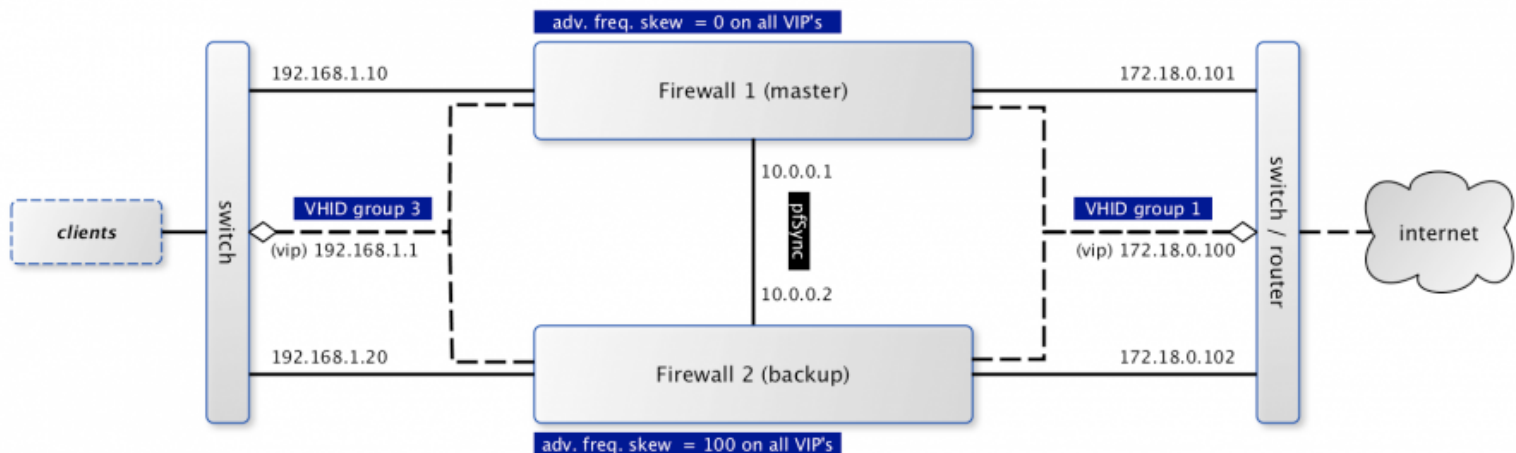
- ✓ Android
- ✓ iOS
- ✓ Blackberry

Securing Networks



HIGH AVAILABILITY / HARDWARE FAILOVER

The Common Address Redundancy Protocol or CARP allows for hardware failover. Two or more firewalls can be configured as a failover group. If one interface fails on the primary or the primary goes offline entirely, the secondary becomes active.



Overview

OPNsense utilises the Common Address Redundancy Protocol or CARP for hardware failover. Two or more firewalls can be configured as a failover group. If one interface fails on the primary or the primary goes offline entirely, the secondary becomes active.

Utilising this powerful feature of OPNsense creates a fully redundant firewall with automatic and seamless fail-over. While switching to the backup network connections will stay active with minimal interruption for the users.

Automatic failover

If the primary firewall becomes unavailable, the secondary firewall will take over without user intervention.

Synchronised state tables

The firewall's state table is replicated to all failover configured firewalls. This means the existing connections will be maintained in case of a failure, which is important to prevent network disruptions.

Configuration synchronisation

OPNsense includes configuration synchronisation capabilities. Configuration changes made on the primary system are automatically synchronised to the secondary firewall.

Service Status Overview & Restart

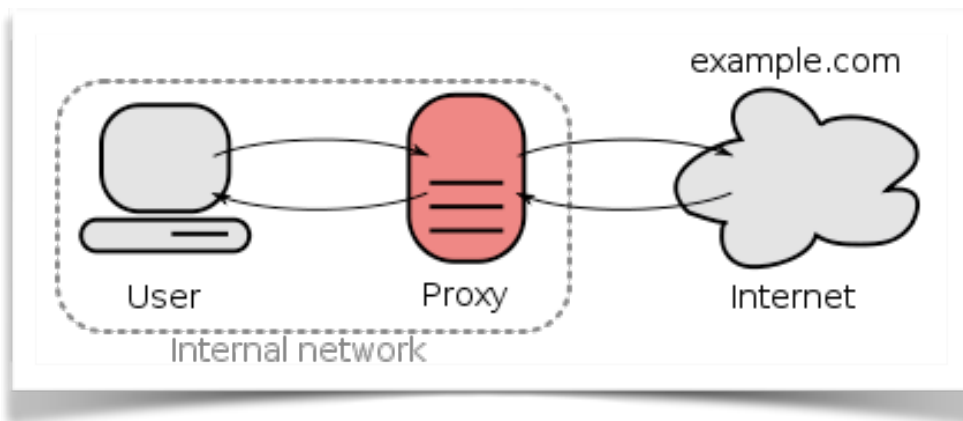
An overview of running services on the Backup device can be viewed and restarted per service or all at once right from the Masters User Interface.



CACHING PROXY

Squid is a caching proxy for the Web supporting HTTP, HTTPS, FTP, and more. It reduces bandwidth and improves response times by caching and reusing frequently-requested web pages. Squid has extensive access controls and makes a great server accelerator.

source - www.squid-cache.org



Multi Interface

Proxy can run at multiple interfaces.

Transparent Proxy

The proxy can be configured as transparent proxy.

Authenticators

- ✓ LDAP (incl. Microsoft Active Directory)
- ✓ Radius
- ✓ Local user manager
- ✓ Two-Factor One Time Password (OTP 2FA)
- ✓ No authentication

FTP proxy

Integrated FTP proxy that makes use of the same Access Control Lists.

Access Control

Fine grained access control, includes:

- ✓ Subnets
- ✓ Ports
- ✓ MIME types
- ✓ Banned IP's
- ✓ Whitelists
- ✓ Blacklists
- ✓ Browser/User Agents
- ✓ Support for blacklists

ICAP

Supports external processing including 3rd party virus scanning engine.

Category Based Web Filter

OPNsense offers category based web filter support. Main features include:

- ✓ Fetch from a remote URL
- ✓ Supports flat file & category based compressed lists
- ✓ Automatically convert category based blacklists to squid ACL's
- ✓ Keep up to date with the integrated scheduler
- ✓ Compatible with most popular blacklist



INTRUSION DETECTION & PREVENTION

The inline IPS system of OPNsense is based on Suricata and utilises Netmap to enhance performance and minimise cpu utilisation. This deep packet inspection system is very powerful and can be used to mitigate security threats at high speed.



Rulesets

All available rule categories can easily be selected and applied with their defaults or custom setting.

Alerts

The alerts are searchable within the user interface. Full details about the alert can be displayed.

Emerging Threats ETOpen Ruleset

OPNsense has integrated support for ET Open rules. The ETOpen Ruleset is an excellent anti-malware IDS/IPS ruleset that enables users with cost constraints to significantly enhance their existing network-based malware detection.

Abuse.ch

Abuse.ch offer several blacklist for protecting against fraudulent networks.

OPNsense has integrated support for SSL Blacklist (SSLBL), a project maintained by abuse.ch. The goal is to provide a list of “bad” SSL certificates identified by abuse.ch to be associated with malware or botnet activities. SSLBL relies on SHA1 fingerprints of malicious SSL certificates and offers various blacklists.

Feodo Tracker

Feodo (also known as Cridex or Bugat) is a Trojan used to commit ebanking fraud and steal sensitive information from the victims computer, such as credit card details or credentials. At the moment, Feodo Tracker is tracking four versions of Feodo.

Maxmind GeoLite2 Country

OPNsense has integrated GeoLite2 Country database support. GeoLite2 databases are free IP geolocation databases comparable to, but less accurate than, MaxMind’s GeoIP2 databases. GeoLite2 databases are updated on the first Tuesday of each month.

Finger Printing

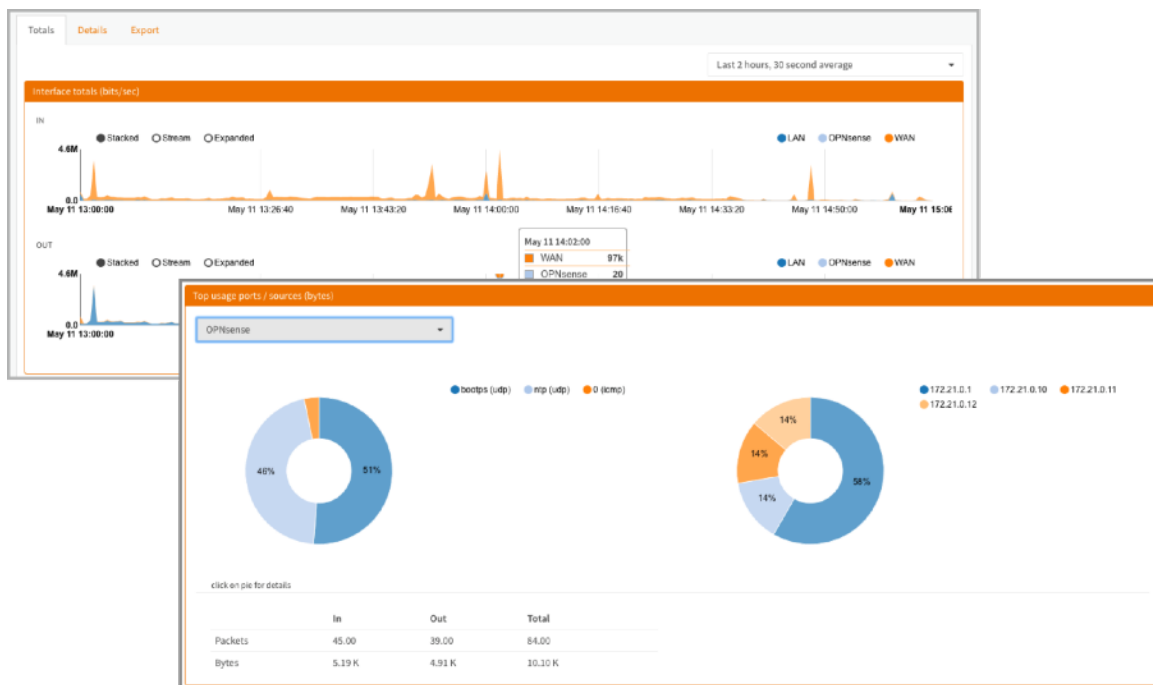
OPNsense includes a very polished solution to block protected sites based on their SSL fingerprint.

Securing Networks



NETFLOW EXPORT & ANALYSIS - INSIGHT

Netflow is a **monitoring** feature, invented by Cisco, it is implemented in the kernel. Since it is a kernel implementation it is very fast with little overhead. While many monitoring solutions such as Nagios, Cacti and vnstat only capture traffic statistics, Netflow captures complete packet flows including source, destination ip and port number. OPNsense offers full support for exporting Netflow data to external collectors as well as a comprehensive Analyser called **Insight** for on-the-box analysis and live monitoring.



OPNsense® is the only open source solution with a built-in Netflow analyser integrated into it's Graphical User Interface.

Netflow Analyser - Insight

OPNsense offers a full Netflow Analyser with the following features:

- ✓ Captures 5 detail levels
- ✓ Graphical representation of flows (stacked, stream and expanded)
- ✓ Top usage per interface, both IP's and ports.
- ✓ Full in/out traffic in packets and bytes
- ✓ Detailed view with date selection and port/ip filter (up to 2 months)
- ✓ Data export to CSV for offline analysis
 - ✓ Selectable Detail Level
 - ✓ Selectable Resolution
 - ✓ Selectable Date range

Netflow Exporter

OPNsense Netflow Exporter supports multiple interfaces, filtering of ingress flows and multiple destinations including local capture for analysis by Insight (OPNsense Netflow Analyser).

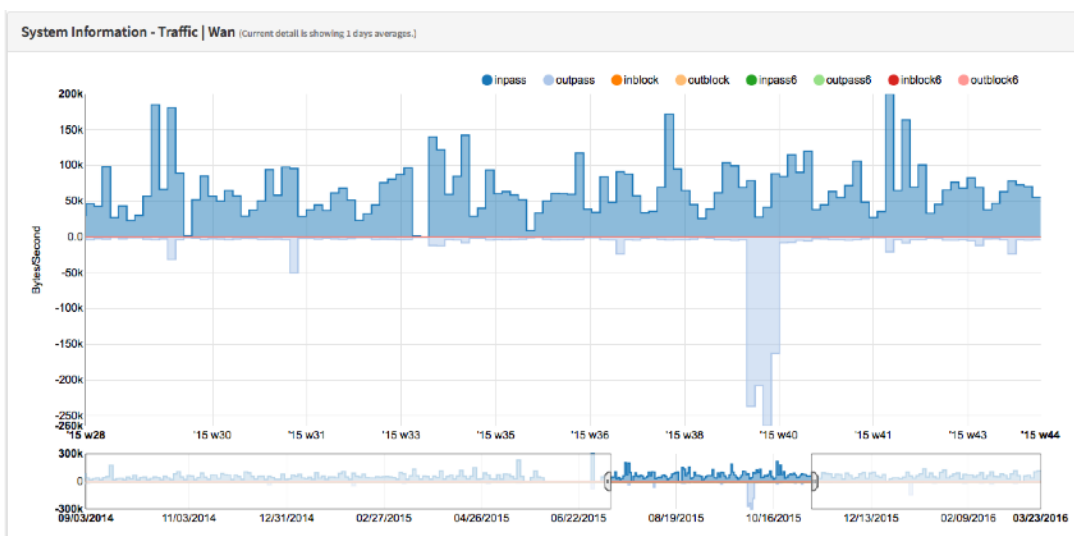
Supported Versions

OPNsense supports both Netflow version 5 (IPv4) and version 9 (IPv4 & IPv6).



SYSTEM HEALTH & INFORMATION

The fastest way to analyse your systems health with our dynamic view on Round Robin Data



System Health offers a dynamic view on RRD data gathered by the system. It allows you to dive into different statistics that show the overall health and performance of the system over time.

The system health module will enable you to track down issues faster and easier than traditional static RRD graphs and it allows you to zoom in.

Primary Data Collectors

System Health offers data collectors for most parts of the system. depending on the features in use there may be more or less graphs available. The primary collectors are:

Packets

Packets show the number of packets per second traveling to and from a certain interface.

Quality

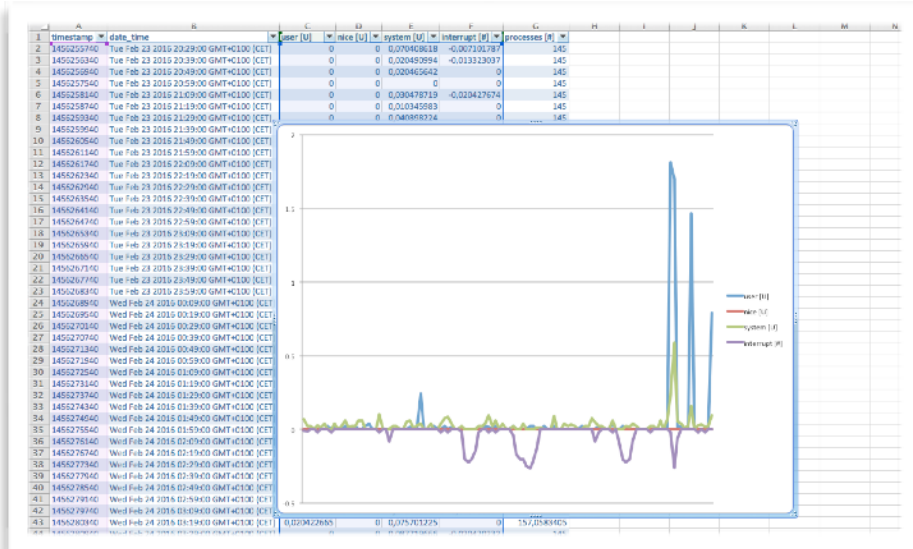
Quality show latency and packet loss of the monitored gateways (ip).

System

The system section is used for sensor data regarding the system utilisation, such as memory usage, mbufs, states, processes and (when available) cpu temperature.

Table View & Exporting

Data can be viewed as a table and exported for further analysis in Excel or any other csv compatible spreadsheet.

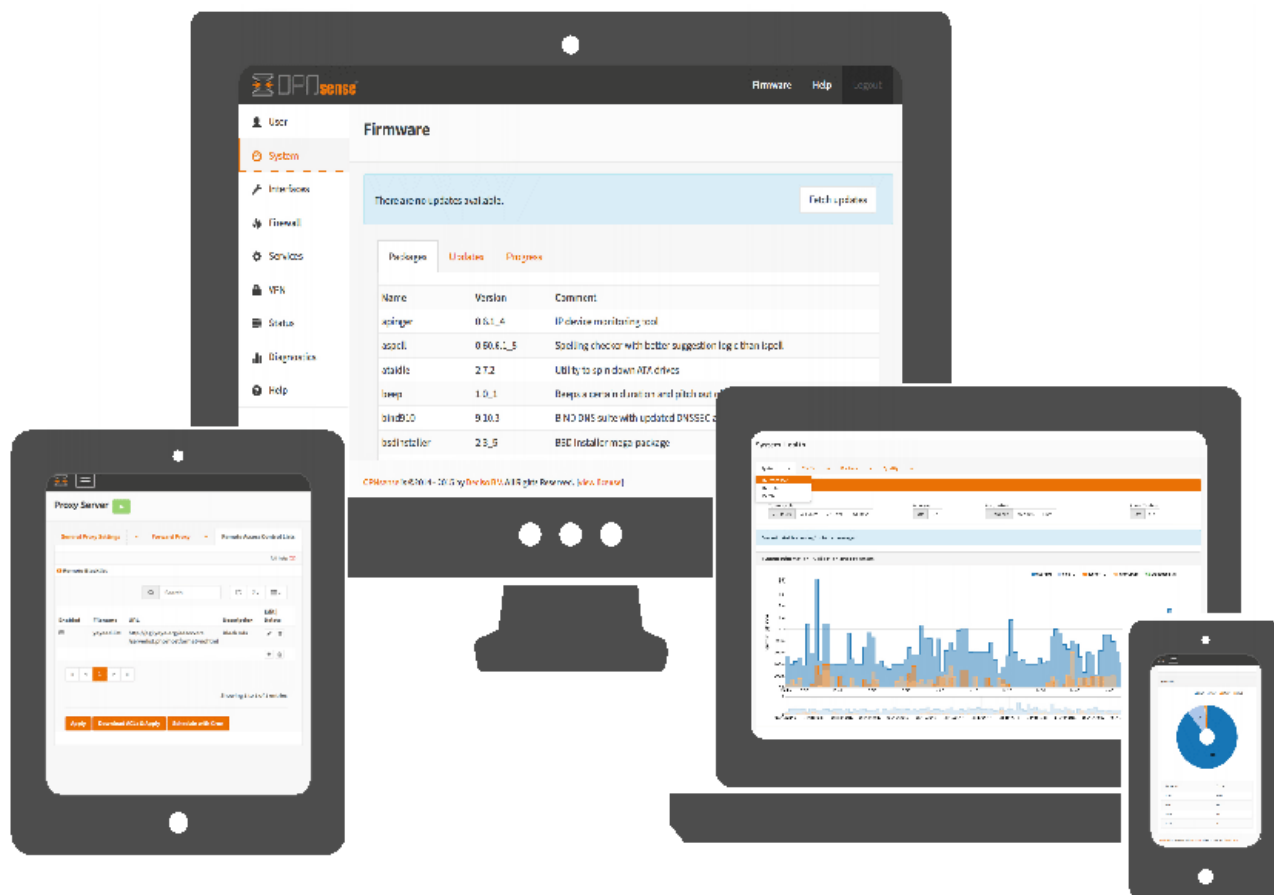


Securing Networks



MODERN USER INTERFACE

Easy to use responsive design, accessible from a desktop pc, tablet and smart phone.



Everything included

All features offered by OPNsense are configurable through the responsive user interface.

Multi language

The user interface is built with multi language support in mind and currently offers English, Czech, Chinese, French, German, Italian, Japanese, Portuguese (Brazil & Portugal) and Russian.

Built-in help

Many options have an info icon with built-in help to get you started quickly.

Advanced mode

More complex features such as proxy, traffic shaping and IDPS have advanced options that can be shown or hidden.

Sane defaults

Many features have usable defaults to allow easy, fast and simple configuration.

Two Factor Authentication

OPNsense's User Interface support authentication through two-factor authentication using Google's Authenticator or other TOTP tokens.

Securing Networks



BACKUP & RESTORE

Better safe than sorry, always keep an up to date backup of your configuration. It's easy with OPNsense.

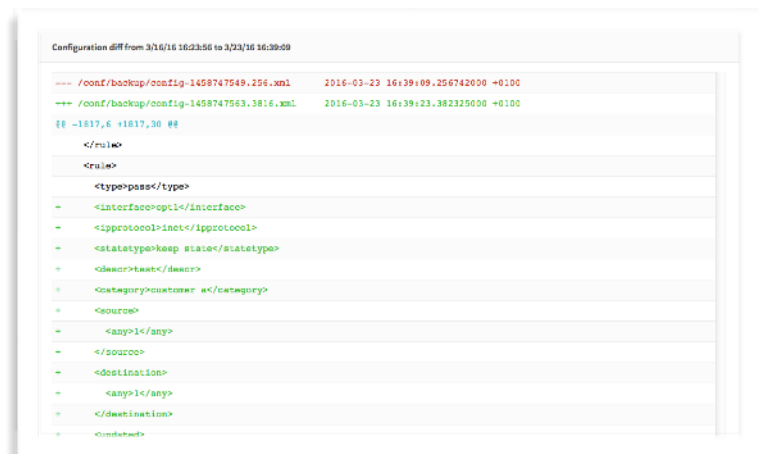


Backup

Easily download a backup from within the GUI and store on a safe place.
Encrypt the backup with a strong password and make plain text unreadable for unauthorised persons.

Restore

Upload your configuration backup file and restore it with ease.



History

Automatic backups of configuration changes make it possible to review history and restore previous settings.

Cloud Backup

OPNsense supports encrypted cloud backup of your configuration with the option to keep backups of older files (history). For this purpose Google drive support has been integrated into the user interface.



Google Drive

Securing Networks



FIRMWARE & PLUGINS

Robust firmware upgrade path to react on emerging threats in a fashionable time.

Packages	Plugins	Updates	Progress
Name	Version	Size	Comment
GeoIP	1.6.9	808KiB	Find the country that any IP address or hostname originates from
apinger	0.6.1_4	86.3KiB	IP device monitoring tool
aspell	0.60.6.1_5	3.68MiB	Spelling checker with better suggestion logic than ispell
ataidle	2.7.2	21.4KiB	Utility to spin down ATA drives
beep	1.0_1	8.28KiB	Beeeps a certain duration and pitch out of the PC Speaker
bind910	9.10.3P4	46.8MiB	BIND DNS suite with updated DNSSEC and DNS64
bsdinstaller	2.3_5	1.48MiB	BSD Installer mega-package
bsnmp-regex	0.6_1	63.5KiB	bsnmpd module allowing creation of counters from log files

OPNsense is equipped with a reliable and secure update mechanism to provide frequent security updates.

A plugin mechanism can be used to install additional packages and customisations.

Release schedule

OPNsense offers two major releases annually; in January and July. Smaller incremental (security) updates are provided weekly. Minor updates are not required, but provide an extra safety layer by incorporating security fixes fast. Customers can choose to skip versions and upgrade on their own timeframe.

Minimise downtime and keep up to date

The upgrade mechanism is simple and easy to use and proven to be safe. Upgrading can be done from within the User Interface or trough the console (CLI). For most minor upgrades rebooting is not required and services will continue to function uninterrupted. In case a reboot is required the system will notify this before the actual upgrade

Plugins

OPNsense is highly extensible with plugins to add customisations or additional features.

Standard plugins include:

- ✓ Let's Encrypt,
- ✓ HAProxy,
- ✓ BGP (Quagga),
- ✓ Monit,
- ✓ vmware-tools,
- ✓ Xen-tools.





SOFTWARE FEATURE OVERVIEW

Stateful firewall

- Filter by
 - Source
 - Destination
 - Protocol
 - Port
 - OS (OSFP)
- Limit simultaneous connections on a per rule base
- Log matching traffic on a per rule bases
- Policy Based Routing
- Packet Normalisation
- Option to disable filter for pure router mode

Policy organisation

- Alias Support
 - IP addresses
 - Port ranges
 - Domain names (FQDN)
- Interface Groups
 - Create security zones with equal rules
- Rule Category
 - Easy access rule sets

Granular control state table

- Adjustable state table size
- On a per rule bases
 - Limit simultaneous client connection
 - Limit states per host
 - Limit new connections per second
 - Define state timeout
 - Define state type
- State types
 - Keep
 - Sloppy
 - Modulate
 - Synproxy
 - None
- Optimisation options
 - Normal
 - High latency
 - Aggressive
 - Conservative

2-Factor Authentication

- Supports TOTP
- Google Authenticator
- Support services:
 - Captive Portal
 - Proxy
 - VPN
 - GUI
 - SSH / Console

802.1Q VLAN support

- max 4096 VLAN's

Link Aggregation & Failover

- Failover
- Load Balance
- Round Robin
- Cisco Ether Channel (FEC)
- 802.3ad LACP

Border Gateway Protocol

Other Interface types

- Bridged interfaces
- Generic Tunnel Interface (GIF)
- Generic Routing Encapsulation
- 802.1ad QinQ

Network Address Translation

- Port forwarding
- 1:1 of ip's & subnets
- Outbound NAT
- NAT Reflection

Traffic Shaping

- Limit bandwidth
- Share bandwidth
- Prioritise traffic
- Rule based matching
 - Protocol
 - Source
 - Destination
 - Port
 - Direction

IGMP Proxy

- For multicast routing

Universal Plug & Play

- Fully supported

Dynamic DNS

- Selectable form a list
- Custom
- RFC 2136 support

DNS Forwarder

- Host Overrides
- Domain Overrides

DNS Server

- Host Overrides
 - A records
 - MX records

- Access Lists

DNS Filter

- Supports OpenDNS

DHCP Server

- IPv4 & IPv6
- Relay Support
- BOOTP options

Multi WAN

- Load balancing
- Failover
- Aliases

Load Balancer

- Balance incoming traffic over multiple servers

Network Time Server

- Hardware devices
 - GPS
 - Pulse Per Second

Intrusion Detection & Prevention

- Inline Prevention
- Integrated rulesets
 - SSL Blacklists
 - Feodo Tracker
 - Geolite2 Country IP
 - Emerging Threats ETOpen
- SSL Fingerprinting
- Auto rule update using configurable cron

Captive Portal

- Typical Applications

- Guest Network
- Bring Your Own Device (BYOD)
- Hotel Wifi Access
- Template Management
- Multiple Zones

- Authenticators

- LDAP
- Radius
- Local User Manager
- Vouchers / Tickets
- Multiple
- None (Splash Screen Only)

- Voucher Manager

- Multiple Voucher Databases
- Export vouchers to CSV

- Timeouts & Welcome Back

- Bandwidth Management

- Share evenly
- Prioritise
- Protocols
- Ports
- IP

- Portal bypass

- MAC and IP whitelisting

- Real Time Reporting

- Live top IP bandwidth usage
- Active Sessions
- Time left
- Rest API

Virtual Private Networks

- IPsec

- Site to Site
- Road Warrior

- OpenVPN

- Site to Site
- Road Warrior
- Easy client configuration exporter

- Tinc (Plugin)

- Full mesh routing

- PPTP (Legacy)

- LT2P (Legacy)

High Availability

- Automatic hardware failover

- Synchronised state table

- Configuration synchronisation

Caching Proxy

- Multi interface
- Transparent Mode
- Support SSL Bump
- SSL Domain only (easy filtering)
- Access Control Lists
- Blacklists
- Category Based Web-filter
- Traffic Management
- Auto sync for remote blacklists
- ICAP (supports virus scan engine)

Backup & Restore

- History & Diff support
- File Backup
- Cloud Backup

SNMP

- Monitor & Traps

Diagnostics

- Filter reload status

- Firewall Info (pfInfo)

- Top Users (pfTop)

- Firewall Tables

- Aliases
- Bogons

- Current Open Sockets

- Show All States

- State Reset

- State Summary

- Wake on LAN

- ARP Table

- DNS Lookup

- NDP Table

- Ping

- Packet Capture

- Test Port

- Trace route

Enhanced Reporting

- Network Flow Analyser 'Insight'

- Fully Integrated
- Detailed Aggregation
- Graphical Representation
- Clickable and Searchable
- CVS Exporter

- System Health

- Round Robin Data
- Selection & Zoom
- Exportable

- Traffic Graph

- Live Traffic Monitoring

Network Monitoring

- Netflow Exporter

- Version 5 & version 9
- Local for 'Insight'

Firmware

- Easy Upgrade

- Reboot warning for base upgrades

- SSL Flavour selectable

- OpenSSL
- LibreSSL

- Selectable Package Mirror

- Reinstall Single Package

- Lock Package (prevents upgrade)

- Audit Feature

- Check installed packages for known security vulnerabilities

- Plugin Support

- VMware tools
- Xen tools
- Tinc
- HAProxy -Load balancer
- Let's Encrypt

REST API

- ACL support

Online Documentation

- Free & Searchable

Securing Networks