OPNsense

Your next open source firewall

www.rhinolabsinc.com

About OPNsense

Highlights

Businesses

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 you voice over ip above other traffic. Backup your configuration to the cloud automatically, no need for manual backups anymore!

School Networks

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. Its easy to setup as no additional plugins nor packages are required. Teach about security or use our development documentation to show how an Model Viewer Controller works. You and your students are invited to join the effort and OPNsense community!

About OPNsense

Highlights

Hotels and Camping

On The Road

Remote Offices & SOHO

Hotels & Campings

Hotels and campings usually utilise a captive portal to allow guests (paid) access to internet for a limited duration. Guests need to login using a voucher that they can either buy or obtain for free at the reception. OPNsense has a built-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**. The **easy client exporter** make 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.

About OPNsense

Highlights

Alias Support

Granular State Table Control

Transparent layer 2 firewall capable

Disable Packet Filtering

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.

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

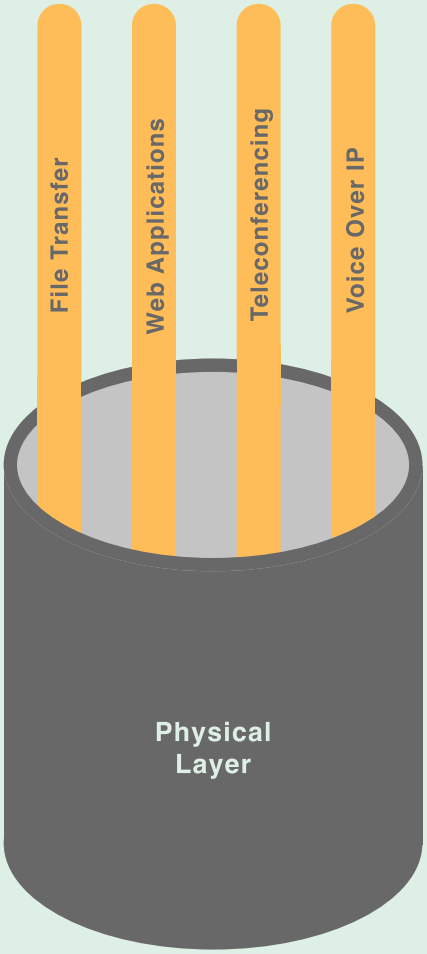
Transparent Layer 2 Firewall Capable

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

Disable Packet Filtering

This option can be used to turn the system in to a pure router

Traffic Shaping



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).

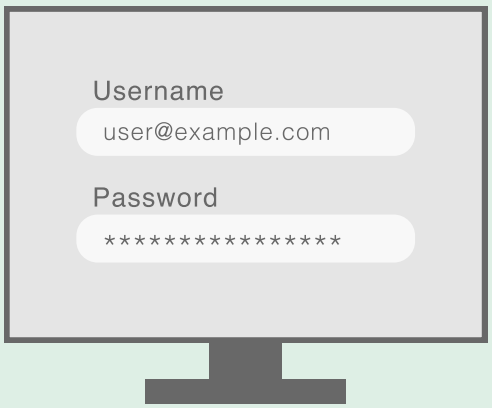
Bandwidth Sharing

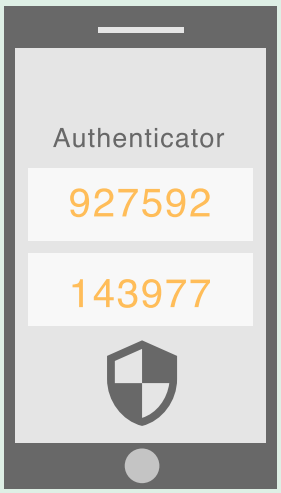
The available bandwidth can be shared evenly over all users, this allows for optimum performance at all times.

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.

Two-Factor Authentication





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 very simple to setup using OPNsense.

Supported 2FA Services

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

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

Easy Setup

Configuring Two-Factor authentication is very simple using Google's Authenticator. Integrated in OPNsense's unified authentication system
Automatic Seed Generation
Token activation by Barcode Scanning

Captive Portal

Typical Applications

- ✓ Guest Network
- ✓ Hotel and Capming WiFi Access
- ✓ Bring Your Own Device (BYOD)

Template Management

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 Management

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.

Captive Portal

Authentication

Secure authentication ia 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
- ✓ Voucher/Tickets
- ✓ Two-Factor One-Time-Password
- ✓ No authentication (Splash screen only)
- ✓ Multiple (a combination of above)

Voucher Manager

OPNsense's Captive Portal has an easy voucher creation system that exports the vouchers to a csv file for use with you 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.

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.

Captive Portal

Bandwidth Management

The built-in traffic shaper can be used to:

- ✓ Share bandwidth evenly
- ✓ Give priority to protocols port numbers and/or ip addresses

Portal Bypass

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

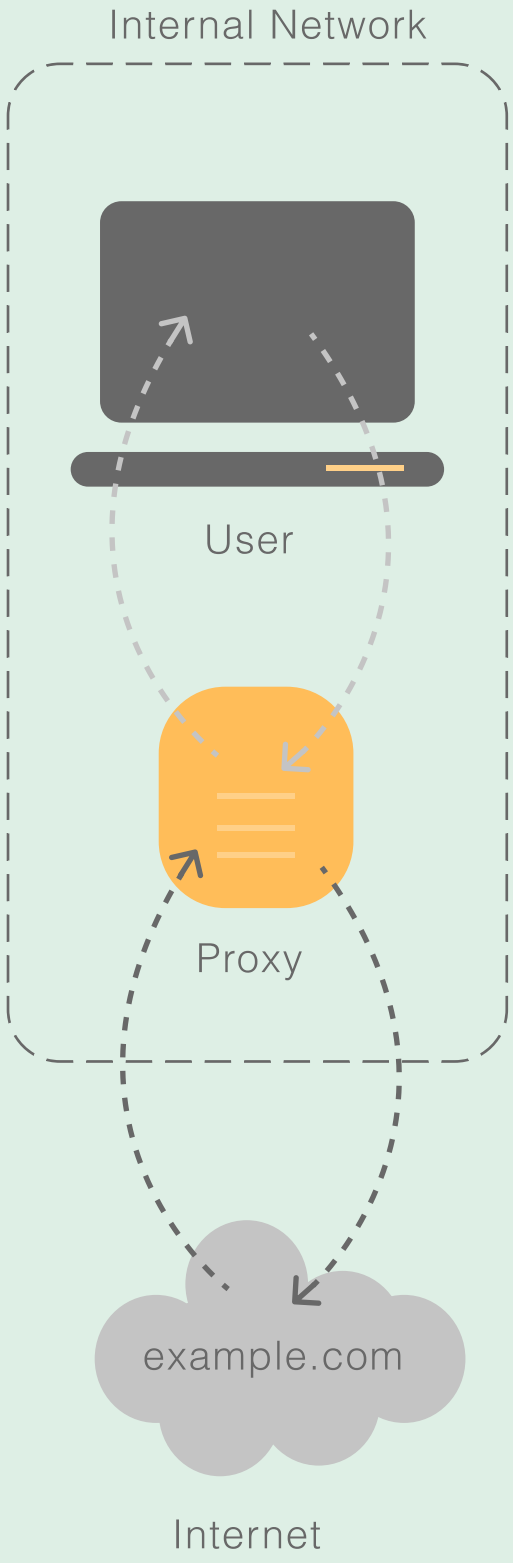
IPsec allows connectivity with any device supporting standard IPsec. This is most commonly used for site to site connectivity to other OPNsense installations, other open source firewalls, and most commercial firewall solutions (Cisco, Juniper, etc.). It can also be used for mobile client connectivity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

Supported VPN Clients

The built-in traffic shaper can be used to:

- ✓ Viscosity (Mac OSx & Windows)
- ✓ OpenVPN for Android
- ✓ OpenVPN Connect (iOS)

Catching Proxy



Multi Interface

Proxy can run at multiple interfaces

Traffic Management

The proxy can be combined with traffic shaper and take full advantage of its shaping features.

Transparent Proxy

The proxy can be configured as transparent proxy.

FTP proxy

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

ICAP

Supports external processing including 3rd party virus scanning engine.

Authenticators

- ✓ LDAP (Microsoft Active Directory)
- ✓ Radius
- ✓ Local User Manager
- ✓ Voucher/Tickets
- ✓ Two-Factor One-Time-Password
- ✓ No authentication (Splash screen only)
- ✓ Multiple (a combination of above)

Catching Proxy

Access Control

Fine grained access control includes:

- ✓ Subnets
- ✓ Ports
- ✓ MIME types
- ✓ Banned IPs
- ✓ Whitelists
- ✓ Blacklists
- ✓ Browser/User Agents

Category Based Web Filter

OPNsense has build-in category based web filter support. Main features include:

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

Inline Intrusion Prevention System

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

Finger Printing

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

Inline Intrusion Prevention System

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.

Netflow Export & Analyses - Insight

Netflow is a monitoring feature, invented by Cisco, it is implemented in the FreeBSD kernel with ng_netflow (Netgraph). Since Netgraph is a kernel implementation it is very fast with little overhead compared to softflowd or pfflowd.

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.

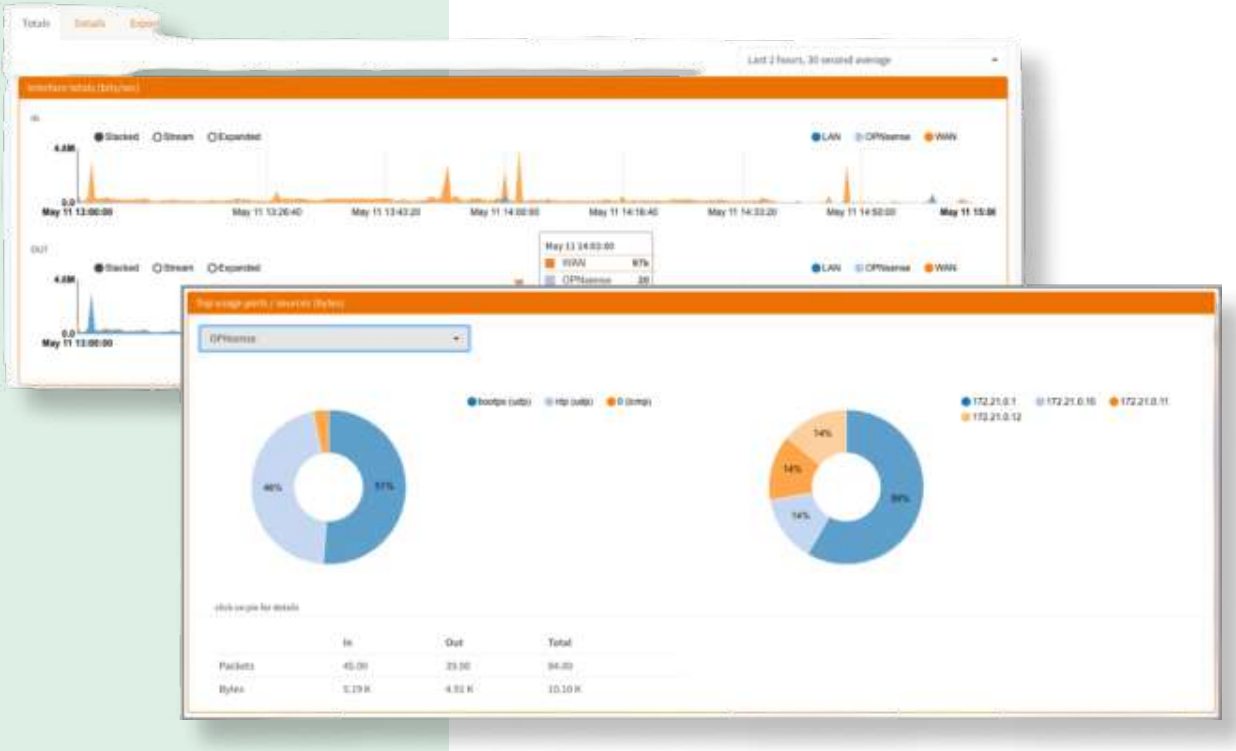
OPNsense offers full support for exporting Netflow data to external collectors as well as a comprehensive Analyser called Insight for on-the-box analysis and live monitoring.

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

Netflow Export & Analyses - Insight

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

Netflow Export & Analyses - Insight

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

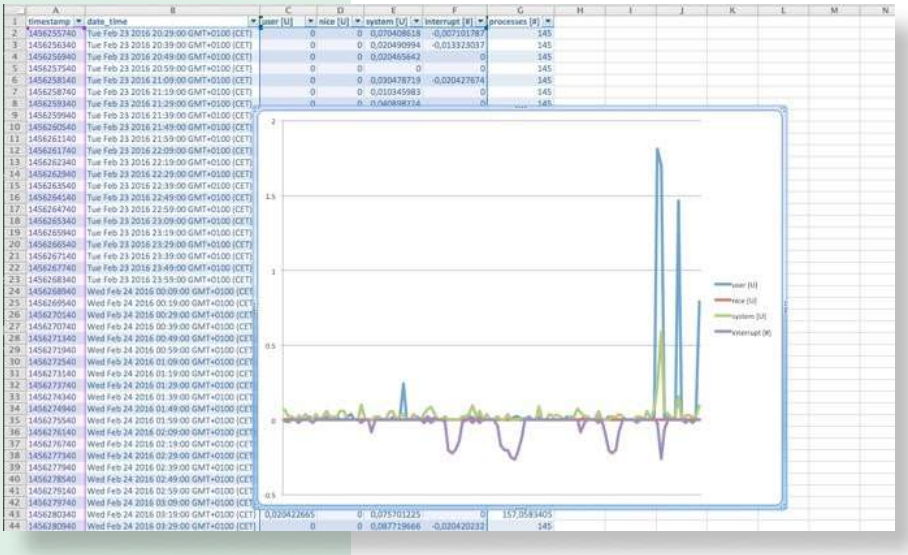
System Health & Information

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.

System Health & Information

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.

System Health & Information

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.

Traffic

Shows traffic graphs for each interface including vpn (ipsec).

Table View & Exporting

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

Modern Bootstrap-Based 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. Work is already in progress to support German, French, Japanese, Chinese & Mongolian.

Build-in help

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

Modern Bootstrap-Based User Interface

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 trough two-factor authentication using Googles Authenticator or other TOTP tokens.

Backup & Restore

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

History

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

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.

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.

Firmware & Plugins

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

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

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

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 and the customer can choose to cancel the upgrade procedure.

Feature List

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

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
- Agressive
- Conservative

2-Factor Authentication Supports TOTP

Google Authenticator
Support services:
- Captive Portal
- Proxy
- VPN
- GUI

802.1Q VLAN support

max 4096 VLAN's

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

Feature List

•Port
•Direction

IGMP Proxy

For multicast routing

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

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 & Camping Wifi Access
•Template Management
•Multiple Zones
Authenticators
•LDAP
•Radius
•Local User Manager
•Vouchers / Tickets
•Multiple
•None (Splash Screen Only) ⊙Voucher Manager

Feature List

- 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

PPTP (Legacy)
LT2P (Legacy)

High Availability

Automatic hardware failover
Synchronised state table
Configuration synchronisation

Caching Proxy

Multi interface
Transparent Mode

Access Control Lists
Blacklists
Category Based Web-filter
Traffic Management
Auto sync for remote blacklists
ICAP (supports virus scan engine)

System Health

Round Robin Data Selection & Zoom
- Exportable

Backup & Restore

History & Diff support
File Backup - Cloud Backup

SNMP

Monitor & Traps

Diagnostics

Filter reload status
Firewall Info (pfInfo)
Top Users (pfTop)
Firewall Tables
Current Open Sockets
Show All States

Feature List

State Reset
State Summary

Wake on LAN
ARP Table
DNS Lookup
NDP Table
Ping
Packet Capture
Test Port
Trace route
Traffic Graph

Network Monitoring
Netflow Exporter
Network Flow Analyser
- Fully Integrated
- CVS Exporter

Firmware

Easy Upgrade
- Reboot warning for base upgrades

SSL selectable

- OpenSSL
- LibreSSL

REST API

- ACL support

Rhino Labs Inc.,
3240 Scott Blvd.,
Santa Clara, CA
95054

(408) 207 0400

info@rhinolabsinc.com

www.rhinolabsinc.com