OPNsense®
Securing networks made easy

White paper

A full feature overview of OPNsense® including high-end features such as high availability, traffic shaping, intrusion detection and easy OpenVPN client setup.

OPNsense is a Deciso® brand.

OPNsense® is an open-source, user-friendly firewall and routing platform that combines the extensive features of commercial products, ranging from a stateful firewall to web application control and integrated inline intrusion detection and prevention. Based on FreeBSD for long-term support, OPNsense's focus on security brings unique features such as an easy to use one time password authentication for various components. Through its modular design and – the in house developed – Model View Controller framework the product is extendible, and API functionality is readily available.

The robust and reliable update mechanism gives OPNsense® the ability to provide important security updates in a timely fashion.

Table of contents

Categorized List of OPNsense Features

1. Firewall and Security

Feature	Description	Remark
Stateful Firewall	Supports stateful packet inspection for filtering traffic based on rules and policies.	
Firewall Aliases	Simplifies management of firewall rules using aliases for IP addresses, networks, ports, MACs, GeoIP and BGP ASN, etc.	
Time-based Firewall Rules	Allows firewall rules to be active only during specified times or schedules.	
Port Forwarding and NAT	Configures Network Address Translation for inbound and outbound traffic.	
Traffic Shaping	Manages bandwidth and prioritizes traffic using queues and schedules.	
Policy-Based Routing	Routes traffic based on defined policies and criteria (Source Routing).	
Static Routing	Configure static routes and manually control the path that traffic takes through the network.	
Bridging	Create a layer-2 bridge. Can be configured with (Rapid) Spanning Tree Protocol (RSTP/RTP).	
Anti DDOS	DDoS protection using SYN cookies.	
Static ARP & NDP	Staticly configure Adress Resolution Protocol (ARP) and Neighbor Discovery Protocol (NDP) and control to which (physical) machine an IP address is connected.	
GeoIP Blocking	Blocks or allows traffic based on geographical location using MaxMind GeoLite2 databases.	*Business Edition (or plugin for CE)*
Bogon Network Blocking	Blocks traffic from bogon (unallocated or private) IP address spaces.	
Intrusion Detection and Prevention	Network-based intrusion detection and prevention using Suricata.	
Packet Capture and Analysis	Captures and analyzes network traffic at the packet level for troubleshooting and security analysis.	
Traffic Normalization	Protects internal machines against inconsistencies in Internet protocols and implementations.	
Granular State Table Control	Granular control over state table size, rule bases limitations (connections, connection per second, timeout, state type) and optimization options (Normal, High latency, etc.)	
802.1Q VLAN	Support upto 4096 vlans per interface and addtionally QinQ 802.1ad is supported by stacking a vlan on top of a vlan.	
VXLAN	Support for Virtual eXtensible Local Area Networks (VXLANs)	
GIF/GRE	Both Generic Routing Encapsulation as wel as Generic Tunnel Interfaces are supported.	
Loopback	Logical virtual interfaces which emulate real interfaces and can be used for different setup scenario's, which require always-on interfaces	
Vritual IP configuration	Add extra addresses to already defined interfaces using virtual IPs.	
Advanced Routing	Supports dynamic routing protocols like BGP, IS-IS, LDP, OSPF, PIM and RIP via the FRR plugin.	*Plugin*
Policy Organization	Support Interface Groups and Rule Categorization	

2. VPN and Remote Access

Feature	Description	Remark
OpenVPN Support	Provides site-to-site and remote access VPN using OpenVPN protocol with SSL/TLS encryption. Includes easy to use client export.	
IPsec VPN	Supports IPsec VPN for secure site-to-site and remote access connections.	
WireGuard VPN	Lightweight and high-performance VPN protocol support. Includes an easy to use QR code generator for client configuration.	
Other VPN options	Openconnect, Stunnel, Tinc, ZeroTier (SDWAN/commercial)	*Plugin*
Dynamic DNS Integration	Keeps VPN endpoints reachable with dynamic IP addresses by updating DNS records automatically.	
Multi-Factor Authentication	Enhances VPN security with additional authentication methods like TOTP (Time-based OTP).	
VPN Road Warrior Setup	Allows mobile clients to connect securely from remote locations.	

3. Web and Email Security

Feature	Description	Remark
Web Application Firewall	Easily protect webservices against all sort of injection attacks and provides encryption for traffic to and from the outside world.	*Business Edition*
Web Proxy (Squid)	Caches web content and enforces access control policies for HTTP/HTTPS traffic.	*Plugin*
URL Filtering	Controls access to websites based on URLs, domains, and categories using blacklists.	*Plugin*
Transparent Proxy Mode	Redirects traffic without configuring client browsers.	*Plugin*
ICAP Support	Integrates with external content adaptation services for advanced filtering.	*Plugin*
DNS Filtering and Security	Protects against DNS-based threats using DNS over TLS and blocking malicious domains.	
Fine grained DNS filtering	Configure DNS blocking policies in a more fine-grained manner by specifying networks on which the blocklists should apply.	*Business Edition*
Web Filtering and Control	Filters web content using Squid proxy and URL filtering with blacklists and whitelists.	*Plugin*
Antivirus Integration	Provides antivirus scanning for web traffic passing through the proxy (ClamAV).	*Plugin*
SSL Inspection	Decrypts and inspects SSL/TLS traffic using Squid proxy with SSL bumping capabilities.	*Plugin*
SMTP Proxy	Filters and routes email traffic to protect against spam and malware.	*Plugin*
Email Antivirus and Antispam	Scans email for viruses and spam using integrated tools like ClamAV and SpamAssassin.	*Plugin*
Let's Encrypt Integration	Automates SSL/TLS certificate issuance and renewal for secure web access.	*Plugin & Business Edition*

4. Management and Reporting

Feature	Description	Remark
Console administration	Console access is available via serial & SSH. Several features can be controlled from a text based menu including basic setup and firmware upgrade.	
User Identity and Group Management	Manages users and groups locally or integrates with LDAP/RADIUS for authentication and policy enforcement.	*Plugin*
Role-Based Administration	Defines administrative roles with specific permissions for multi-user management.	
Two-Factor Authentication	Enhances login security using methods like TOTP or hardware tokens.	
Firmware Management	Automatic updates and easy firmware management via web interface or console.	
Configuration Backup and Restore	Allows backing up and restoring configurations locally or to cloud services like Google Drive, Git & NextCloud	*Local: Integrated / External: Plugin*
Snapshots	Space-efficient and easy to manage full system snapshot.	
Dashboard and Reporting	Web-based dashboard with customizable widgets and detailed reporting tools.	
Netflow Reporting (Insight)	Flexible and fast Netflow Analyzer with drill down and export functionality.	
NetFlow Exporter	Exports network flow data for traffic analysis using external collectors.	
Live Traffic Monitoring	Streaming live traffic graph with both egress and ingress traffic. Selectable interfaces, update timing. Shows both total bandwidth per interfaces as well as per host.Also includes a Top Talkers overview in a tabular form.	
System Health	Monitors system performance and generates graphical statistics over time.	
Logging and Diagnostics	Comprehensive logging facilities with search and filtering capabilities.	
Remote Logging	Comprehensive remote logging with application adn level selection. Supports UDP & TCP & Encypted TLS via IPv4 and IPv6.	
Monit Service Monitoring	Monitors services and system resources, and sends alerts based on defined conditions.	
APIs and Automation	Provides REST API for automating configuration and management tasks.	

5. High Availability and Clustering

Feature	Description	Remark
CARP Failover	Provides failover and redundancy using Common Address Redundancy Protocol (CARP).	
pfsync State Synchronization	Synchronizes firewall states between clustered firewalls for seamless failover.	
High Availability Sync	Synchronizes configuration between primary and secondary firewalls in a high availability setup.	
Load Balancing	Distributes incoming network traffic across multiple servers. Sevral option are availbe including relayd and Web Application Firewall (Business Edition)	*Plugin*
Multi-WAN Load Balancing	Balances outbound traffic across multiple WAN connections for redundancy and bandwidth.	
Gateway Quality Monitoring	Gateway monitoring includes RTT(d) and Loss.	
Link Aggregation (LAGG)	Combines multiple network interfaces for increased bandwidth and redundancy.	

6. Cloud and Virtualization

Feature	Description	Remark
Virtualization Support	Runs on various hypervisors like VMware, Hyper-V, Proxmox, and VirtualBox.	
Open Virtual Appliance	The official OPNsense Open Vritual Appliance image an be deployed in various virtualization products (e.g. VMWare, Virtualbox).	*Business Edition*
Cloud Deployment	Can be deployed on cloud platforms like AWS and Azure (Marketplace)	
VMware & Xen Integration	Supports open-vm-tools & xen guest utilities for better integration with Vmware and Xen environments.	*Plugin*

7. Authentication and Access Control

Feature	Description	Remark
Local User and Group Management	Manages users and groups locally for authentication and access control.	
LDAP and Active Directory Support	Integrates with external directory services for authentication.	
RADIUS Authentication	Supports RADIUS servers for centralized authentication.	
Captive Portal	Provides a web portal for authenticating users before granting network access.	
Certificate Management	Manages SSL/TLS certificates for authentication and encrypted connection. The trust manager includes Certificate Authority's (CA) and Certificate Revocayion Lists (CRL).	
Single Sign-On (SSO)	Limited SSO capabilities through integration with directory services.	
802.1X Authentication	Supports network access control for wired and wireless clients using RADIUS authentication.	*Plugin*
Authentication Logging	Logs authentication events for auditing and compliance purposes.	

8. Network Services

Feature	Description	Remark
DHCP Server and Relay	Provides DHCP services and can relay DHCP requests to external servers.	
DNS Server and Forwarder	Offers DNS resolution services using Unbound or Dnsmasq, supports DNS over TLS.	
Dynamic DNS Client	Updates dynamic DNS services with current IP addresses.	*Plugin*
NTP Server	Synchronizes time across network devices using Network Time Protocol.	
SNMP	Simple Network Management Protocol (SNMP) is a widely used protocol for monitoring the health and welfare of network equipment. Support IPv4 and IPv6 / SNMP v1, v2c and v3.	*Plugin*
IPv6 Support	Full support for IPv6 addressing and routing.	

9. Central Management & Automation

Feature	Description	Remark
REST API	REST API with ACL support for many parts of the system.	
Scheduled Job Configuration	Schedule jobs to be executed periodically using a Cron deamon. Jobs are registered in the backend to prevent command injection and privilege escalation.	
Central Management	A flexible and power central management enviroment to manage many OPNsense firewalls centrally.	*Business Edition*
Multi Tenancy	Create multy tenancy setups using host groups with user access controls.	*Business Edition*
Central Backups	Centralize automatic configuration backup of all configured hosts.	*Business Edition*
Provisioning	Provision Users & Groups, Aliases, Firewall rules & categories and NAT.	*Business Edition*
Firmeware status & control	Report local firmware version and remotely upgrade.	*Business Edition*
Remote control services	Monitor local services and conrol them (start/stop)	*Business Edition*
Monitoring	Central monitoring of resource usage, such as CPU, Memory, state table, aliases as wel as bandwidth.	*Business Edition*
Automatic Login	Use the configured trust to login on the remote hosts WebGUI with a single click.	*Business Edition*

10. Diagnostics & Troubleshooting

Feature	Description	Remark
System Health	Provides detailed graphs and statistics on system performance metrics like CPU usage, memory, disk I/O, and network throughput over time.	
Logging	Comprehensive logging for system events, firewall actions, VPN connections, and services, accessible via the web interface.	
System Logs (Settings)	Configures log settings, such as log retention times and remote syslog servers, for better log management and analysis.	
Logs (General)	Accesses logs for various services like DHCP, VPN, IPSec, PPPoE, and more, facilitating troubleshooting of specific services.	
PPP Log	Shows logs specific to Point-to-Point Protocol connections, useful for troubleshooting WAN links like PPPoE or L2TP.	
Firmware Update Logs	Provides logs related to firmware updates, useful for diagnosing issues during updates.	
Unbound DNS Logs	Shows logs for the Unbound DNS resolver service, helping troubleshoot DNS resolution problems.	
VPN Status and Logs	Provides status and logs for VPN connections (OpenVPN, IPsec, WireGuard), aiding in troubleshooting connectivity issues.	
Cron Logs	Shows logs related to scheduled tasks configured in the Cron daemon, aiding in troubleshooting automation scripts.	
Monit Service Monitoring Logs	Provides logs from Monit, which monitors services and system resources, helping diagnose service failures or resource issues.	
Dynamic DNS Logs	Shows logs related to Dynamic DNS updates, helping diagnose issues with hostname updates.	*Plugin*
Proxy Server Logs	Displays access and error logs for the proxy server (Squid), useful for diagnosing web access issues.	*Plugin*

Feature (Continued)	Description	Remark
Intrusion Detection Alerts	Displays alerts generated by the IDS/IPS system (Suricata), including details about detected threats and actions taken.	
High Availability Sync Logs	Displays logs related to configuration synchronization between primary and secondary nodes in high-availability setups.	
ACME Client Logs	Shows logs from the ACME client used for obtaining SSL/TLS certificates from Let's Encrypt, helping diagnose certificate issuance issues.	*Plugin*
DNSCrypt-Proxy Logs	If using DNSCrypt, displays logs related to encrypted DNS queries and responses, aiding in DNS troubleshooting.	*Plugin*
Firewall Log View	Displays real-time and historical firewall logs, allowing you to filter and search for specific entries based on criteria like interface, source, destination, and port.	
Firewall Live View	Offers a live view of firewall logs with auto-refresh and color- coded entries for easier analysis of ongoing network activity.	
Packet Capture	Allows capturing network packets on selected interfaces with options to filter by protocol, host, or port; captures can be downloaded for analysis in tools like Wireshark.	
Traffic Graphs	Visualizes real-time network traffic on interfaces, showing bandwidth usage and packet rates.	
Interfaces Statistics	Provides detailed statistics for each network interface, including errors, collisions, and packet counts.	
Ping Utility	Enables you to send ICMP echo requests to test connectivity to a host; supports IPv4 and IPv6.	
Traceroute Utility	Traces the route packets take to reach a destination host, helping identify network path issues; supports IPv4 and IPv6.	
DNS Lookup	Resolves domain names to IP addresses and vice versa, useful for testing DNS functionality.	
NDP Table	Displays the IPv6 Neighbor Discovery Protocol table, showing IPv6 addresses and their corresponding MAC addresses.	
ARP Table	Shows the Address Resolution Protocol table, mapping IP addresses to MAC addresses for IPv4.	
State Table	Lists all active connection states maintained by the firewall, including source, destination, protocol, and interface.	
States Summary	Provides a summarized view of the state table, showing counts of states per protocol, source, and destination.	
Test Port Utility	Checks the connectivity to a specified port on a remote host, useful for testing whether services are reachable.	
Routing Table	Displays the current routing table, showing destination networks, gateways, and interface associations.	
System Activity (Top)	Shows real-time system processes and their CPU and memory usage, similar to the Unix top command.	
NetFlow Exporter	Exports NetFlow data for detailed traffic analysis; can be used with external collectors for in-depth traffic monitoring.	
Firmware Audit	Checks the integrity and versions of installed packages and plugins, ensuring system components are up-to-date and not corrupted.	
Backup & Restore	Allows you to backup the current configuration and restore previous configurations, useful for recovering from misconfigurations.	
Configuration History	Tracks changes made to the system configuration, allowing you to view and revert to previous configurations.	

Feature (Continued)	Description	Remark
DHCP Leases	Displays current DHCP leases, both active and expired, showing IP addresses, MAC addresses, and lease times.	
Sessions (Diagnostics)	Shows currently logged-in users and their session details, including login time and IP address.	
CARP (Status)	Displays Common Address Redundancy Protocol status, useful in high-availability setups to monitor master and backup states.	
Gateway Status	Monitors the status of network gateways, showing latency and packet loss statistics; useful for identifying WAN issues.	
NTP Status	Displays Network Time Protocol synchronization status, including peers and offsets, crucial for time-sensitive operations.	
Services Status	Lists the status of all services running on the firewall, allowing you to start, stop, or restart services as needed.	
Aliases (Diagnostics)	**Resolves and lists the current content of aliases, which can be hostnames, networks, or ports used in firewall rules.**	
Traffic Shaper Status	Shows the status of traffic shaping queues and their usage, helpful for diagnosing traffic prioritization problems.	
IPsec SAD and SPD	Displays Security Association Database (SAD) and Security Policy Database (SPD) for IPsec VPN connections, essential for VPN troubleshooting.	
Captive Portal Sessions	Displays active captive portal sessions, including user information and session duration.	
User Authentication Tester	Allows testing of user authentication against configured authentication servers like LDAP, RADIUS, or local database.	
Mail Queue Viewer	Displays the status of the mail queue if the firewall is configured to send emails, aiding in troubleshooting email notifications.	*Plugin*
DHCPv6 Leases	Lists current DHCPv6 leases, similar to DHCP leases but for IPv6 addresses.	
Route Lookup Tool	Determines which gateway or interface traffic to a specific IP address will use, aiding in routing troubleshooting.	
CARP Diagnostics	Provides tools and logs specific to CARP, including pfsync and synchronization status in high-availability setups.	
Wireless Survey	Scans for available wireless networks and displays signal strength and channel usage, useful for wireless network planning and troubleshooting.	
Disks Health and Usage	Monitors disk space usage and health, alerting when thresholds are exceeded to prevent system issues due to disk space exhaustion.	*Plugin*
Syslog Export	Configures and monitors the export of syslog data to external servers for centralized logging and analysis.	
System Patches	Allows for applying and managing system patches, which can be necessary for fixing specific issues or applying custom changes.	*CLI / Console base tools*

11. Documentation & Support

Feature	Description	Remark
E-Book (English & German)	The complete 4th Edition of Practical OPNsense® by Markus Stubbig	*Business Edition*
E-learning	Hands-On Labs for Beginners	*Business Edition*
Online Documentation	Fully serachble online documentation with example setups.	
Online Forum	Online User Forum	
Commercial Support	Commercial support for configration and trouble shooting.	*Business Edition (preferred)*

12. Compliance

Feature	Description	Remark
LINCE compliance testing	Extrenal / 3rd party LINCE compliance tetsing (jtsec)	*Business Edition*

OPNsense is a Deciso® brand.

White paper

A full feature overview of OPNsense® including high-end features such as high availability, traffic shaping, intrusion detection and easy OpenVPN client setup.

OPNsense®

Securing networks made easy