OPNsense A10 Quad Core Rack Series
DEC2640

The OPNsense A10 Quad Core Rack 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.

- **3.800Mbps Throughput**
- **550,000 Packets per Second**

- **487Mbps Inline High Speed Intrusion Prevention & SSL Finger Printing**

- **Fast Filtering**
  - 45,000 new connections per second (10 second burst)
  - Low Latency ~137µS

- **Hardware Assisted Encryption**
  - 950Mbps IPsec (AES256GCM16)

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

- **128GB SSD**
- Offering Sufficient Space for Logging & Reporting

- **8GB RAM**
- for demanding applications and plugins

- **System wide two-factor authentication.**
- Compatible with Google Authenticator.
DEC2640

POWER SW/LED 3  CONSOLE 5  POWER (C14)
USB 4  RJ45 GbE 6  GROUND

Securing Networks
SOFTWARE
VERSATILE - OPEN SOURCE - FULLY FEATURED

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 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 and two-factor authentication. 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.

Securing Networks
### SOFTWARE

#### FEATURE OVERVIEW

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stateful firewall</td>
<td>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</td>
</tr>
<tr>
<td>Policy organisation</td>
<td>Alias Support IP addresses Port ranges Domain names (FQDN) Geolite2 Country IP Interface Groups Create security zones with equal rules Rule Category Easy access rule sets</td>
</tr>
<tr>
<td>Granular control state table</td>
<td>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 Module Sympoxy None Optimisation options Normal High latency Agressive Conservative</td>
</tr>
</tbody>
</table>
### DEC2640 Hardware Specifications

- **GbE RJ45 Ports [10/100/1000Mbps]**: 4
- **USB Ports**: 1
- **Console Port**: 1
- **Internal Storage**: 128GB
- **Memory**: 8GB DDR3
- **CPU Cores**: 4 (2.0Ghz)
- **Virtual Interfaces (802.1q VLANS)**: 4093

#### System Performance

<table>
<thead>
<tr>
<th>Specification</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total Firewall Throughput (physical limit)</td>
<td>6600 Mbps (3800Mbps)</td>
</tr>
<tr>
<td>Firewall Packets Per Second</td>
<td>550000</td>
</tr>
<tr>
<td>Firewall Port to Port Throughput</td>
<td>950 Mbps</td>
</tr>
<tr>
<td>Firewall Port to Port Packets Per Second</td>
<td>340000</td>
</tr>
<tr>
<td>Concurrent Sessions</td>
<td>7000000</td>
</tr>
<tr>
<td>New Connections Per Second</td>
<td>450000</td>
</tr>
<tr>
<td>Firewall Latency</td>
<td>~137 uSec</td>
</tr>
<tr>
<td>Firewall Policies (Recommended Maximum)</td>
<td>10000</td>
</tr>
<tr>
<td>IPsec VPN Throughput (single tunnel)</td>
<td>950 Mbps</td>
</tr>
<tr>
<td>IPsec VPN Packets Per Second</td>
<td>300000</td>
</tr>
<tr>
<td>SSL VPN Throughput (single tunnel)</td>
<td>240 Mbps</td>
</tr>
<tr>
<td>SSL VPN Packets Per Second</td>
<td>200000</td>
</tr>
<tr>
<td>Threat Protection Throughput (IPS)</td>
<td>487Mbps</td>
</tr>
<tr>
<td>High Availability with State Synchronisation</td>
<td>Requires Two</td>
</tr>
</tbody>
</table>

#### Dimensions

- **Height x Width x Length (mm)**: 44 x 485 x 335
- **Height x Width x Length (inches)**: 1.74 x 19 x 13.2
- **Form Factor**: Rack Mount 1U
- **Weight (Kg)**: 3.75

#### Environment

- **Power Requirements**: 100-240VAC, 50-60Hz
- **Maximum Current**: 0.8A
- **Power Consumption (Typical)**: 30W
- **Heat Dissipation**: 85 BTU/hr
- **Operating Temperature**: 0 to +45°C
- **Storage Temperature**: -20 to +70°C
- **Humidity**: 10-90% non-condensing

#### Regulatory Compliance

- **FCC part 15 Class A, CE, RoHs**

---

1 The user interface is designed for normal business usage, large rulesets, high number of users or interface assignments may be less practical.

Firewall Throughput is the maximum theoretical throughput and is defined as the maximum packets per second under test multiplied with a standard package size of 1.514 bytes. The maximum packets per second is measured using stateless traffic and an internet mix profile (IMIX) with an average packet size of 360 bytes. The maximum port to port traffic with UDP packets of 256bytes after 60 seconds of activity. Connections per second is measured by generating a 10 second burst of TCP connects from simulated clients. The value recorded is the maximum where no connections where dropped. Concurrent sessions are based upon memory available, where one state consumes 1KB of memory and 1GB of memory is reserved for system tasks.

IPS performance is measured using ETPro Telemetry ruleset of march 14th 2019, with all rules enabled and a realistic traffic profile (EMIX) containing stateful traffic, test duration is 100 seconds, average package size after full test is ~700bytes.

IPsec packets per second is measured using AES256GCM16 and the throughput is defined as the maximum packets per second under test multiplied with a standard package size of 1.514 bytes. SSL VPN is measured using AES256CBC.

OPNsense version used for performance tests was 19.1.4.