THUNDER TPS
Next-generation DDoS Protection

A10 Thunder™ TPS product line of Threat Protection Systems provides high-performance, network-wide protection against distributed denial of service (DDoS) attacks, and enables service availability against a variety of volumetric, protocol, resource and other sophisticated application attacks.

The Thunder TPS product line is built upon our Advanced Core Operating System (ACOS) platform, with our A10’s Symmetric Scalable Multi-Core Processing (SSMP) software architecture that delivers high performance and leverages a shared memory architecture to provide efficient tracking of network flows, as well as accurate DDoS protection enforcement for service providers, Web site operators and enterprises.

- **Multi-level DDoS protection for service availability:** Organizations are increasingly dependent on the availability of their services, and on their ability to connect to the Internet. Downtime results in immediate revenue loss. Thunder TPS protects against multiple classes of attack vectors, including volumetric, protocol, resource and advanced application-layer attacks, which are detected and mitigated to prevent a service from becoming unavailable. In addition, customized actions can be taken against advanced application-layer (L7) attacks as needed with our aFleX deep packet inspection (DPI) scripting technology.

- **Performance scalability meets growing attack scale:** The networking industry as well as business analysts are seeing an increasing trend in DDoS attacks. Attacks are not only occurring more frequently, but with greater volumes and increased sophistication. With DDoS mitigation capacity ranging from 38 to 155 Gbps, (and up to 1.2 Tbps in a list synchronization cluster), Thunder TPS ensures that the largest DDoS attacks can be handled effectively.

- **Broad deployment flexibility enables integration:** To easily integrate in various networking architectures, a vendor neutral, flexible DDoS mitigation solution is required. With flexible deployment models for in- and out-of-band operations, and routed or transparent operation modes, Thunder TPS can easily be integrated into any network architecture, of any size. And with our aXAPI open RESTful API, Thunder TPS enables integration to your custom or third-party detection solutions.

Each Thunder TPS model is equipped with high-performance Field Programmable Gate Array (FPGA)-based Flexible Traffic Acceleration (FTA) technology, to immediately detect and mitigate over 30 common attack vectors in hardware, without impact to the core system general-purpose CPUs. More complex application-layer (L7) attacks (HTTP, SSL, DNS and more) are processed by the latest Intel Xeon CPUs, so performance scaling can be maintained by distributing multi-vector detection and mitigation functions across optimal system resources.

A10 Thunder TPS devices protects critical services in the most efficient hardware form factors, which enables your data center resources are used productively. The combination of high performance in a small form factor results in lower OPEX through significantly lower power usage, reduced rack space and lowered cooling requirements.
### Architecture and Key Components

**Asymmetric mode**

For on-demand, or permanent (proactive) volumetric mitigation, triggered manually or by flow analytical systems.

**Inline mode**

Provides continuous, comprehensive detection and mitigation, with more application-level attack mitigation options.

**Out-of-band mode**

For detailed telemetry analysis, define threshold violations, and synchronize white/black lists master to in-band Thunder TPS units.

### Features and Benefits

The Thunder TPS Series product line provides many features to detect and mitigate multi-vector DDoS attacks with unprecedented performance scalability and deployment flexibility.

**Multi-level DDoS protection for service availability:**

A10's Thunder TPS Series is able to detect and mitigate any level of attack, even if multiple attacks hit the network simultaneously.

- **Complete multi-vector attack protection:** Service availability is realized by detecting and mitigating DDoS attacks of all types, whether they are pure volumetric, protocol or resource attacks, or even application-level attacks:
  - Volumetric attacks, such as SYN Floods and DNS amplification attacks, are aimed to flood and saturate a victim's network connection, thus rendering services unavailable. Thunder TPS implements multi-protocol rate limiting to prevent sudden surges of illegitimate traffic from overwhelming network and server resources.
  - Protocol attacks, such as ping of death and IP anomalies, are aimed at exhausting a victim's protocol stack so it cannot respond to legitimate traffic. Thunder TPS detects and mitigates over 30 anomaly attacks in hardware to stop them before system CPUs have to be involved.
  - Resource attacks, such as fragmentation attacks or HTTP Slowloris, are aimed at exhausting a victim's network or application resources. A resource attack renders a victim's services unusable, with minimal bandwidth usage. Thunder TPS recognizes many resource attacks and can deny malicious client access.
  - Application attacks such as HTTP GET floods are specifically exploiting a weakness in an application's function or trying to make it unavailable. With A10's aFleX feature, Thunder TPS is able to perform deep packet inspection (DPI) on incoming packets and take defined actions to protect the application.

- **Hitless redirect (aka action on ACK):** When deployed in asymmetric mode, Thunder TPS can perform TCP authentication on established sessions. This means that for legitimate clients, the session will not be broken.

**Performance and scale to address the largest attacks:**

Over the last years, DDoS attacks have rapidly proliferated in terms of bandwidth (Gbps) and packets per second (PPS). Thunder TPS is equipped with high-performance FPGA hardware and the latest, most powerful Intel Xeon CPUs to mitigate any scale of attack.

- **Performance to address the largest attacks:** Mitigation capacity ranging from 38 to 155 Gbps (or 1.2 Tbps in a list synchronization cluster) of throughput ensures that the largest DDoS attacks can be handled effectively. Each Thunder TPS model is equipped with high-performance FPGA-based FTA technology to detect and mitigate over 30 common attack vectors immediately, before the Intel CPUs are involved. More
complex application-layer (L7) attacks (HTTP, SSL, DNS, etc.) are processed by the latest Intel Xeon CPUs, so that high-performance system scaling is maintained even for multi-vector attacks. The FPGA FTA technology can address over 30 attack vectors without involving the high-performance CPUs. Network connectivity is provided by 16 x 10 Gbps interfaces, and 4 x 40 Gbps interfaces.

- **Large threat intelligence class lists**: Eight individual lists, each containing up to 16 million list entries, can be defined. This allows a user to utilize data from IP reputation databases, in addition to the dynamically generated entries of black/white lists.

- **Simultaneous protected objects**: To protect entire networks with many connected users and services, the Thunder TPS Series is able to simultaneously monitor 64,000 hosts or subnets.

**Flexible deployment for ease of integration:**

For network operators, it is critical that a DDoS mitigation solution can easily be inserted into the existing network architecture, so that the network remains prepared for imminent DDoS threats.

- **Easy network integration**: With multiple performance options and flexible deployment models for inline and out-of-band operations, including both routed and transparent operation modes, Thunder TPS can be integrated into any network architecture, of any size. And, with aXAPI, our open RESTful API, Thunder TPS can easily be integrated into third-party detection solutions.

The unprecedented capacity of Thunder TPS allows a device to be deployed in inline mode and out-of-band mode simultaneously. In this deployment model, the Thunder TPS unit can analyze traffic from other network segments and apply this knowledge to its configuration.

**Product Description**

The Thunder TPS product line is a family of high-performance appliances that detect and mitigate multi-vector DDoS attacks at the network edge, functioning as a first line of defense for a network infrastructure.

Our Thunder TPS line of hardware appliances protects large networks with entry-level models starting at 38 Gbps and moving up to a 155 Gbps high-performance appliance for your most demanding requirements. All models feature dual power supplies, solid-state drives (SSDs), and have no inaccessible moving parts for high availability. All models benefit from our FPGA-based FTA technology, featuring FPGA for hardware optimized packet processing to provide highly scalable flow distribution and DDoS protection capabilities. The FPGA-based FTA detects 30 common attack vectors in hardware without impacting the performance of the general-purpose CPUs that are used for processing more complex application-layer attacks.

Switching and routing processors provide high-performance network processing. Each appliance offers the best performance per rack unit, and the highest level “80 PLUS™ Platinum” certification for power supplies to ensure a green solution and reduce power consumption costs. High density 1/10 Gbps and 40 Gbps port options are available to meet the highest networking bandwidth demands. Each of our high-performance appliances is an efficient 1 RU form factor, and up to eight Thunder TPS models can be clustered for even higher capacity and efficient list synchronization.

**Appliance Summary/Specifications Table**

<table>
<thead>
<tr>
<th>Model</th>
<th>Thunder 4435 TPS</th>
<th>Thunder 4435S TPS</th>
<th>Thunder 5435 TPS</th>
<th>Thunder 5435S TPS</th>
<th>Thunder 6435 TPS</th>
<th>Thunder 6435S TPS</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Throughput</strong></td>
<td>38 Gbps</td>
<td>38 Gbps</td>
<td>77 Gbps</td>
<td>77 Gbps</td>
<td>155 Gbps</td>
<td>155 Gbps</td>
</tr>
<tr>
<td>TCP SYN Auth/sec (PPS)*</td>
<td>35 million</td>
<td>35 million</td>
<td>40 million</td>
<td>40 million</td>
<td>65 million</td>
<td>65 million</td>
</tr>
<tr>
<td>SYN Cookie/sec (PPS)*</td>
<td>50 million</td>
<td>50 million</td>
<td>100 million</td>
<td>100 million</td>
<td>200 million</td>
<td>200 million</td>
</tr>
<tr>
<td><strong>Network Interface</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1/10 GE Fiber (SFP+)</td>
<td>16</td>
<td>16</td>
<td>16</td>
<td>16</td>
<td>16</td>
<td>16</td>
</tr>
<tr>
<td>40 GE Fiber (QSFP+)</td>
<td>0</td>
<td>0</td>
<td>4</td>
<td>4</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td><strong>Management Interface</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Lights Out Management</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Console Port</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Solid-state Drive (SSD)</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Processor</strong></td>
<td>Intel Xeon Deca-core</td>
<td>Intel Xeon Deca-core</td>
<td>Intel Xeon Deca-core</td>
<td>Intel Xeon Deca-core</td>
<td>2 x Intel Xeon Deca-core</td>
<td>2 x Intel Xeon Deca-core</td>
</tr>
<tr>
<td><strong>Memory (ECC RAM)</strong></td>
<td>64 GB</td>
<td>64 GB</td>
<td>64 GB</td>
<td>64 GB</td>
<td>128 GB</td>
<td>128 GB</td>
</tr>
</tbody>
</table>
### Appliance Summary/Specifications Table (continued)

<table>
<thead>
<tr>
<th>Hardware Acceleration</th>
<th>Thunder 4435 TPS</th>
<th>Thunder 4435S TPS</th>
<th>Thunder 5435 TPS</th>
<th>Thunder 5435S TPS</th>
<th>Thunder 6435 TPS</th>
<th>Thunder 6435S TPS</th>
</tr>
</thead>
<tbody>
<tr>
<td>64-bit Linear Decoupled Architecture</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Flexible Traffic Acceleration</td>
<td>1 x FTA-3+ FPGA</td>
<td>1 x FTA-3+ FPGA</td>
<td>2 x FTA-3+ FPGA</td>
<td>2 x FTA-3+ FPGA</td>
<td>4 x FTA-3+ FPGA</td>
<td>4 x FTA-3+ FPGA</td>
</tr>
<tr>
<td>Switching/Routing</td>
<td>Hardware No</td>
<td>Hardware Dual</td>
<td>Hardware No</td>
<td>Hardware Dual</td>
<td>Hardware No</td>
<td>Hardware Quad</td>
</tr>
<tr>
<td>SSL Security Processor</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>(Typical/Max)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Heat in BTU/hr</td>
<td>1,195 / 1,433</td>
<td>1,365 / 1,638</td>
<td>1,365 / 1,638</td>
<td>1,535 / 1,877</td>
<td>2,013 / 2,320</td>
<td>2,320 / 2,661</td>
</tr>
<tr>
<td>(Typical/Max)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Power Supply</td>
<td>Dual 1100W RPS</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(DC option available)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cooling Fan</td>
<td>80 Plus &quot;Platinum&quot; efficiency, 100 - 240 VAC, Frequency 50 – 60 Hz</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dimensions</td>
<td>1.75 in (H), 17.5 in (W), 30 in (D)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rack Units</td>
<td>1U</td>
<td>1U</td>
<td>1U</td>
<td>1U</td>
<td>1U</td>
<td>1U</td>
</tr>
<tr>
<td>Unit Weight</td>
<td>34.5 lbs</td>
<td>34.5 lbs</td>
<td>35.5 lbs</td>
<td>35.5 lbs</td>
<td>39 lbs</td>
<td>39 lbs</td>
</tr>
<tr>
<td>Operating Ranges</td>
<td>Temperature 0° - 40° C, Humidity 5% - 95%</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Regulatory Certifications</td>
<td>FCC Class A‡, UL‡, CE‡, TUV‡, CB‡, VCCI‡</td>
<td>China CCC‡, BSMI‡, RCM (replace C-Tick)‡, GOST-R‡, FAC‡, KCC‡, NEBS‡</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Standard Warranty</td>
<td>90-day Hardware and Software</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

1Certification in progress

* Packets per second. Performance varies with deployment mode and configuration

---

### Detailed Feature List

#### High Performance, Scalable Platform

- ACOS Operating System
  - Multi-core, Multi-CPU support
  - Linear Application Scaling
  - Linux on control plane
  - ACOS on data plane

#### Networking

- Asymmetric, Inline, Out-of-band (Transparent Mode/Routed Mode)
- Routing: Static Routes, BGP4+
- VLAN (802.1Q)
- Trunking (802.1AX), LACP
- Access Control Lists (ACLs)

---

### Management

- Dedicated management interface (Console, SSH, Telnet)
- Industry-standard Command Line Interface (CLI)
- SNMP, Syslog, Email Alerts
- Port mirroring
- REST-style XML API (aXAPI)
- LDAP, TACACS+, RADIUS Support

### Flood Attack Protection

- SYN Cookies
- SYN Authentication
- TCP/UDP/ICMP Flood
- DNS Authentication

---

Customer Driven Innovation
Flood Attack Protection (continued)

- DNS Flood
- HTTP Authentication
- HTTP Flood

Protocol Attack Protection

- Invalid Packets
- Anomalous TCP Flag Combinations (No Flag, SYN/FIN, SYN Frag, LAND attack)
- IP Options
- Packet size validation (Ping of Death)
- HTTP Protocol Compliance
- HTTP Anomalies

Resource Attack Protection

- Fragmentation
- Slowloris
- Slow GET/POST
- Long Form Submission
- SSL Renegotiation

Application Attack Protection

- Application Layer (L7) Scripting (aFleX)
- HTTP GET Flood

Protected Objects

- Source/Destination IP Address
- Source/Destination IP Pair
- Source/Destination Port
- Subnet
- Protocol (HTTP,DNS,TCP,UDP,CMP)
- DNS Query Type
- URI
- List

Actions

- Drop
- TCP Reset
- Add to Black List
- Add to White List
- Log
- Limit Concurrent Connections
- Limit Connection Rate
- Limit Rate

Telemetry

- sFlow v5 with Host, HTTP, and Custom Counter Blocks
- High Speed Logging

Redirection

- BGP Route Injection
- IPinIP (source and terminate)
- GRE Tunnel Termination

Detection

- Manual Thresholds
- Protocol Anomaly Detection
- Inspection within IPinIP
- Black/White Lists
- IP/Port Scanning

Carrier-grade Hardware

- Advanced hardware architecture
- Redundant Power Supplies (AC or DC)
- Smart Fans (hot swap)
- Solid-state drive (SSD) and Compact Flash
- 1/10 GE ports, 40 GE ports
- Tamper Detection
- Lights Out Management (LOM/IPMI)

About A10 Networks

A10 Networks is a leader in application networking, providing a range of high-performance application networking solutions that help organizations ensure that their data center applications and networks remain highly available, accelerated and secure. Founded in 2004, A10 Networks is based in San Jose, California, and serves customers globally with offices worldwide. For more information, visit: www.a10networks.com

©2014 A10 Networks, Inc. All rights reserved. A10 Networks, the A10 Networks logo, A10 Thunder, Thunder, vThunder, aCloud, ACOS, and aGalaxy are trademarks or registered trademarks of A10 Networks, Inc. in the United States and in other countries. All other trademarks are property of their respective owners. A10 Networks assumes no responsibility for any inaccuracies in this document. A10 Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.