A10 Thunder TPS® (Threat Protection System) is the world’s highest-performance DDoS protection solution, leading the industry in precision, intelligent automation, scalability, and performance.

SURGICAL MULTI-VECTOR DDoS PROTECTION

Ensuring availability of business services requires organizations to rethink how to build scalable DDoS defenses that can surgically distinguish an attacker from a legitimate user.

New threat vectors have changed the breadth, intensity, and complexity of options available to attackers. Today’s attacks have evolved, and now include DDoS toolkits, weaponized IoT devices, online DDoS services, and more. Established solutions, which rely on ineffective signature-based IPS or only traffic rate-limiting, are no longer adequate.

Thunder TPS scales to defend against the DDoS of Things and traditional zombie botnets and detects DDoS attacks through high-resolution packets or flow record analysis from edge routers and switches. Unlike outdated DDoS defense products, A10 Networks’ defenses include detection capabilities across key networks elements including A10 Thunder® ADC, CGN and CFW. These capabilities provide the context, packet level granularity and visibility needed to thwart today’s sophisticated attacks.

The One-DDoS Protection detectors work in concert with A10 Networks aGalaxy® Centralized Management System and Thunder TPS for centralized mitigation that delivers fast and cost-effective DDoS resilience.

When attacks grow beyond an organization’s bandwidth capacity, traffic can be diverted to the A10 DDoS Protection Cloud service to defend against volumetric attacks.

A10 Networks is available when you need help most. A10 support provides 24x7x365 services, including the A10 DSIRT (DDoS Security Incident Response Team) to help you understand and respond to DDoS incidents and orchestrate cloud scrubbing. A10 Threat Intelligence Service leverages global knowledge to proactively stop bad actors.
MAINTAIN SERVICE AVAILABILITY
Downtime results in immediate productivity and revenue loss for any business. Thunder TPS ensures service availability by automatically spotting anomalies across the traffic spectrum and mitigating multi-vector DDoS attacks.

DEFEAT GROWING ATTACKS
Thunder TPS protects the largest, most-demanding network environments. Thunder TPS offloads common attack vectors to specialized hardware, allowing its powerful multicore CPUs to distinguish legitimate users from attacking botnets and complex application-layer attacks that require resource-intensive deep packet inspection (DPI).

SCALABLE PROTECTION
Select Thunder TPS hardware models benefit from our Security and Policy Engine (SPE) hardware acceleration, leveraging FPGA-based FTA technology and other hardware-optimized packet-processing for highly scalable flow distribution and hardware DDoS protection capabilities.

DEPLOY WARTIME SUPPORT
No organization has unlimited trained personnel or resources during real-time DDoS attacks. Thunder TPS supports five levels of programmatic mitigation escalation and de-escalation per protected zone. Remove the need for frontline personnel to make time-consuming manual changes to escalating mitigation strategies and improve response times during attacks. Administrators have the option to manually intervene and coordinate with A10's DDoS Security Incident Response Team (DSIRT) at any stage of an attack.

REDUCE SECURITY OPEX
Thunder TPS is extremely efficient. It delivers high performance in a small form factor to reduce OPEX with significantly lower power usage, rack space, and cooling requirements.
REFERENCE ARCHITECTURES

PROACTIVE MODE
(ASYMMETRIC OR SYMMETRIC)

Proactive mode provides continuous, comprehensive detection and fast mitigation. This mode is most useful for real-time environments where the user experience is critical, and for protection against application-layer attacks. TPS supports L2 or L3 inpath deployments. A10 DDoS Protection Cloud provides protection against volumetric attacks that exceed an organization’s internet bandwidth.

REACTIVE MODE

Larger networks benefit from on-demand mitigation, triggered manually or by flow analytical systems. TPS fits in any network configuration with integrated BGP and other routing protocols. This eliminates the need for any additional diversion and re-injection routers. A10 Networks partners with the industry’s leading visibility and DDoS detection companies to provide additional flexibility for creating best-of-class solutions for each customer’s unique business needs. The flow-detection partner companies leverage Thunder TPS’ open RESTful API (aXAPI® and aGAPI®), to create tightly integrated monitoring solutions that include visibility, detection and reporting.

REACTIVE DEPLOYMENT WITH THUNDER TPS DETECTOR

Thunder TPS Detector is available as a standalone appliance or integrated with aGalaxy 5000. The flow-based DDoS detector supports tightly integrated interworking with aGalaxy management and Thunder TPS mitigation for a complete reactive DDoS defense solution.
Distributed Detection with One-DDoS Protection

One-DDoS Protection provides full spectrum DDoS protection by placing detection capabilities across key networks elements including A10’s Thunder ADC, CGN and CFW. These capabilities provide the context, packet level granularity and visibility needed to thwart today’s sophisticated targeted attacks. The distributed DDoS detectors work in concert with aGalaxy and Thunder TPS for centralized mitigation that delivers fast and cost effective DDoS resilience.

OUT-OF-BAND (TAP) MODE

The out-of-band mode is used when packet-based DDoS detection and monitoring are required.
A10 Thunder TPS is the world’s highest-performance DDoS protection solution. It detects and mitigates multi-vector DDoS attacks with surgical precision while providing unprecedented performance, scalability, and deployment flexibility.

**FULL SPECTRUM DDoS PROTECTION FOR SERVICE AVAILABILITY**

A10 Thunder TPS detects and mitigates broad levels of attacks, even if multiple attacks hit the network simultaneously.

**COMPLETE SOLUTION FOR FLEXIBLE DEPLOYMENTS**

Thunder TPS DDoS solutions provide a complete solution for DDoS defenses in proactive always-on or on-demand reactive modes to meet their business objectives. Thunder TPS can be deployed in L2 or L3 inpath modes with full IPv4 and IPv6 support. On-demand reactive DDoS detection is facilitated with the collection and analysis of exported flow data records from routers and switches. The Thunder TPS detector applies always-on adaptive learning to build peacetime profiles for protected servers and services, based on 17 flow record traffic indicators to spot anomalous behavior. When an attack is detected, aGalaxy instructs Thunder TPS to initiate a BGP route redirection for the suspicious traffic. Then TPS applies the appropriate countermeasures using a progressive auto mitigation level escalation technique before delivering the clean traffic to the intended destination.

**MULTI-VECTOR ATTACK PROTECTION**

Detect and mitigate DDoS attacks of many types, including volumetric, protocol, or resource attacks; application-level attacks; or IoT-based attacks. Hardware acceleration offloads the CPUs and makes Thunder TPS particularly adept to deal with simultaneous multi-vector attacks.

**ZAP ZERO-DAY AUTOMATED PROTECTION**

The ZAP engine utilizes heuristic and machine learning automatically discover mitigation filters without advanced configuration or manual intervention. ZAP speeds the response time against increasingly sophisticated multi-vector attacks while minimizing downtime and errors and lower operating costs.

**HYBRID DDoS PROTECTION**

Thunder TPS on-premise protection works in concert with the A10 DDoS Protection Cloud service to provide full-spectrum protection against attacks of any type. The service is backed by purpose-built, globally distributed scrubbing centers scaled to handle the largest known DDoS volumetric attacks, all orchestrated by A10 DSIRT.

**NON-STOP DNS AUTHORITATIVE DNS CACHE**

A10 Thunder TPS can be configured as a high-performance DNS authoritative cache, enabling Thunder TPS’ Non-stop DNS operational mode to cache common DNS records and respond to queries at rates of up to 35M queries per second. Non-stop DNS can also work in conjunction with Thunder TPS DDoS defenses to create a highly resilient DNS service.
HIGH PERFORMANCE AND EFFICIENCY TO MEET GROWING ATTACK SCALE

Thunder TPS provides solutions to protect organizations from attacks of all sizes, from 1 to 300 Gbps (or 2.4 Tbps in a list synchronization cluster).

ONE-DDOS PROTECTION

Layered, Distributed Detection

One-DDoS Protection provides the freshest approach to full-spectrum DDoS defense, placing detection capabilities across key network elements closest to the targeted elements of the infrastructure. This provides the context, packet level granularity, and visibility needed to thwart today’s sophisticated targeted attacks.

A10 Thunder ADC, CGN, and CFW with integrated DDoS detectors work in concert with Thunder TPS’ edge flow-based detection and centralized mitigation to enable full spectrum DDoS resilience.

A10 DDOS THREAT INTELLIGENCE

Threat intelligence data from more than three dozen security intelligence sources, including DShield and Shadowserver, is included with support, enabling Thunder TPS to instantly recognize and block traffic to and from known malicious sources. The service includes millions of current and accurate IP addresses of DDoS weapons used regularly in reflected amplification attacks and crippling IoT botnet attacks.

HIGH PERFORMANCE PROTECTION

Select Thunder TPS models have high-performance FPGA-based Flexible Traffic Acceleration (FTA) technology to immediately detect and mitigate up to 60 common attack vectors in hardware – before data CPUs are involved. Thunder TPS supports protocol and packet anomaly check and forwarding of up to 440 million packets per second (Mpps). Thunder TPS enforces highly granular traffic rates up to 100 ms intervals.

SIMULTANEOUS PROTECTED OBJECTS

To protect entire networks, applications, and services, Thunder TPS simultaneously mitigates up to 3,000 Zones with individual protection policies that include thousands of hosts, subnets, and services per zone. The scale of simultaneous mitigation helps organizations apply granular controls to protected objects and create profitable DDoS scrubbing services.
LARGE THREAT INTELLIGENCE CLASS LISTS

Eight lists, each containing up to 16 million entries, may be defined to utilize data from intelligence sources, such as the A10 Threat Intelligence Service, in addition to dynamically generated entries of actionable black/white lists.

ZERO-DAY ATTACK PROTECTION

DDoS attackers continue to innovate their multi-vector attack arsenals with new attack strategies. Thunder TPS ZAP engine automatically recognizes DDoS attack characteristics and dynamically applies mitigation filters without advanced configuration or manual intervention.

FULL CONTROL AND SMART AUTOMATION FOR AGILE PROTECTION

For network operators, it is critical that a DDoS mitigation solution integrates easily into many network architectures.

EFFICIENT INTELLIGENT AUTOMATION

No organization has unlimited resources or the time for manual interventions. A10 provides the industry’s most advanced intelligent automation capabilities, powered by machine learning throughout the entire protection lifecycle.

Operators define the networks to protect, and A10 defenses do the rest based on the operator’s pre-defined policies, including individual learned detection threshold per monitored entity, automatic traffic redirection orchestration, start of mitigation and escalation, and extract and apply attack pattern filters. When the attack subsides, the network and defenses are returned to peacetime posture and detailed reports are generated for future analysis.

EASY NETWORK INTEGRATION

With multiple performance options and flexible deployment models, Thunder TPS may be integrated into any network architecture of any size, including MPLS. And with aXAPI, A10’s 100-percent programmable RESTful API, Thunder TPS easily integrates into third-party detection solutions and into agile SecOps workflows.

Leveraging open standards like BGP Blackhole and Flowspec functionality, Thunder TPS mitigation integrates easily with any DDoS detection solution. Open APIs and networking standards enable tight integration with other devices, including A10 threat detection partners, SDN controllers, and other security products.
EFFECTIVE MANAGEMENT

Thunder TPS supports an industry-standard CLI, on-box GUI, and the aGalaxy management system. The CLI allows sophisticated operators easy troubleshooting and debugging. The intuitive on-box GUI enables ease of use and basic graphical reporting. aGalaxy offers a comprehensive dashboard with advanced reporting, mitigation console, and policy enforcement for multiple TPS devices.

aGalaxy is available with an optional integrated Thunder TPS detector that supports tightly integrated interworking of Thunder TPS DDoS mitigation, flow-based DDoS detection, system-wide management, and robust reporting.

THUNDER

BY THE NUMBERS

14045 TPS

500 Gbps
HW Blocking

300 Gbps
Throughput

2.4 Tbps
Cluster

8x16M
Threat Class Lists

100 GbE
Ports

440 Mpps

60 Hardware Mitigations

64K Protected Objects
## THUNDER TPS PHYSICAL APPLIANCE

### PERFORMANCE

<table>
<thead>
<tr>
<th></th>
<th>THUNDER 1040 TPS</th>
<th>THUNDER 1040 TPS HARDWARE BYPASS</th>
<th>THUNDER 3040 TPS</th>
<th>THUNDER 4435 TPS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Throughput (Software Scrubbing)(^1)</td>
<td>5 Gbps</td>
<td>5 Gbps</td>
<td>10 Gbps</td>
<td>38 Gbps</td>
</tr>
<tr>
<td>Packets Rate (pps)(^1)</td>
<td>2.5 Million</td>
<td>2.5 Million</td>
<td>4.5 Million</td>
<td>20 Million</td>
</tr>
<tr>
<td>Software-based - SYN Authentication (pps)</td>
<td>2.5 Million</td>
<td>2.5 Million</td>
<td>4.5 Million</td>
<td>20 Million</td>
</tr>
<tr>
<td>Hardware-based - Anomaly Flood Blocking (pps)</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>55 Million</td>
</tr>
<tr>
<td>Maximum Concurrent Sessions (Asymmetric Deployment)</td>
<td>8 Million</td>
<td>8 Million</td>
<td>8 Million</td>
<td>32 Million</td>
</tr>
<tr>
<td>Average Latency</td>
<td>10 µs</td>
<td>10 µs</td>
<td>10 µs</td>
<td>35 µs</td>
</tr>
<tr>
<td>Minimum Rate Enforcement Interval</td>
<td></td>
<td></td>
<td>100 ms</td>
<td></td>
</tr>
</tbody>
</table>

### FLOW DETECTION PERFORMANCE

<table>
<thead>
<tr>
<th></th>
<th>N/A</th>
<th>N/A</th>
<th>1 Million</th>
<th>3 Million</th>
</tr>
</thead>
</table>

### NETWORK INTERFACE

<table>
<thead>
<tr>
<th></th>
<th>1 GE Copper</th>
<th>1 GE Fiber (SFP)</th>
<th>1/10 GE Fiber (SFP+)</th>
<th>1/10 GE Fiber (Fixed)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Flows Per Second (fps)</td>
<td>5</td>
<td>1 + 4 (Bypass)</td>
<td>6</td>
<td>0</td>
</tr>
<tr>
<td>Management Ports</td>
<td>1 x Ethernet Management Port, 1 x RJ-45 Console Port</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### HARDWARE SPECIFICATIONS

<table>
<thead>
<tr>
<th>Processor</th>
<th>Intel Communications Processor</th>
<th>Intel Communications Processor</th>
<th>Intel Xeon 4-core</th>
<th>Intel Xeon 10-core</th>
</tr>
</thead>
<tbody>
<tr>
<td>Memory (ECC RAM)</td>
<td>16 GB</td>
<td>16 GB</td>
<td>16 GB</td>
<td>64 GB</td>
</tr>
<tr>
<td>Storage</td>
<td>SSD</td>
<td>SSD</td>
<td>SSD</td>
<td>SSD</td>
</tr>
<tr>
<td>Hardware Acceleration</td>
<td>Software</td>
<td>Software</td>
<td>Software</td>
<td>FTA-3, SPE</td>
</tr>
<tr>
<td>Dimensions (Inches)</td>
<td>1.75(H) x 17.5(W) x 17.25(D)</td>
<td>1.75(H) x 17.5(W) x 17.45(D)</td>
<td>1.75(H) x 17.5(W) x 30(D)</td>
<td></td>
</tr>
<tr>
<td>Rack Units (Mountable)</td>
<td>1U</td>
<td>1U</td>
<td>1U</td>
<td>1U</td>
</tr>
<tr>
<td>Unit Weight</td>
<td>14 lbs 16 lbs (RPS)</td>
<td>15 lbs 17 lbs (RPS)</td>
<td>20.6 lbs</td>
<td>34.5 lbs</td>
</tr>
<tr>
<td>Power Supply (DC option available)</td>
<td>Single 750W(^*)</td>
<td>Single 750W(^*)</td>
<td>Dual 600W RPS</td>
<td>Dual 1100W RPS</td>
</tr>
<tr>
<td>Power Consumption (Typical/Max)(^2)</td>
<td>80W / 110W</td>
<td>80W / 110W</td>
<td>180W / 240W</td>
<td>350W / 420W</td>
</tr>
<tr>
<td>Heat in BTU/Hour (Typical/Max)(^2)</td>
<td>273 / 376</td>
<td>273 / 376</td>
<td>615 / 819</td>
<td>1,195 / 1,433</td>
</tr>
<tr>
<td>Cooling Fan</td>
<td>Removable Fans</td>
<td>Removable Fans</td>
<td>Hot Swap Smart Fans</td>
<td></td>
</tr>
<tr>
<td>Operating Ranges</td>
<td>Temperature 0(^\circ) - 40(^\circ) C</td>
<td>Humidity 5% - 95%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Regulatory Certifications</td>
<td>FCC Class A, UL, CE, TUV, CB, VCCI, CCC, BSMI, RCM</td>
<td>FCC Class A, UL, CE, TUV, CB, VCCI, CCC, BSMI, RCM</td>
<td>FCC Class A, UL, CE, GS, CB, VCCI, CCC, KCC, BSMI, RCM</td>
<td>FCC Class A, UL, CE, TUV, CB, VCCI, CCC, MSIP, BSMI, RCM, EAC, NEBS, CCC EAL2+, RoHS</td>
</tr>
<tr>
<td>Standard Warranty</td>
<td>90-Day Hardware and Software</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Thunder TPS Physical Appliance Specifications (Cont.)

### PERFORMANCE

<table>
<thead>
<tr>
<th></th>
<th>THUNDER 5845 TPS</th>
<th>THUNDER 7445 TPS</th>
<th>THUNDER 14045 TPS SINGLE MODULE</th>
<th>THUNDER 14045 TPS DUAL MODULE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Throughput (Software Scrubbing)*1</td>
<td>100 Gbps</td>
<td>220 Gbps</td>
<td>150 Gbps</td>
<td>300 Gbps</td>
</tr>
<tr>
<td>Hardware Blocking</td>
<td>N/A</td>
<td>500 Gbps</td>
<td>500 Gbps</td>
<td>500 Gbps</td>
</tr>
<tr>
<td>Packets Rate (pps)*3</td>
<td>28 Million</td>
<td>60 Million</td>
<td>60 Million</td>
<td>120 Million</td>
</tr>
<tr>
<td>Software-based - SYN Authentication (pps)</td>
<td>28 Million</td>
<td>60 Million</td>
<td>60 Million</td>
<td>120 Million</td>
</tr>
<tr>
<td>Hardware-based - Anomaly Flood Blocking (pps)</td>
<td>125 Million</td>
<td>250 Million</td>
<td>220 Million</td>
<td>440 Million</td>
</tr>
<tr>
<td>Maximum Concurrent Sessions (Asymmetric Deployment)</td>
<td>48 Million</td>
<td>64 Million</td>
<td>128 Million</td>
<td>256 Million</td>
</tr>
<tr>
<td>Average Latency</td>
<td>50 µs</td>
<td>50 µs</td>
<td>60 µs</td>
<td>60 µs</td>
</tr>
<tr>
<td>Minimum Rate Enforcement Interval</td>
<td>N/A</td>
<td>50 µs</td>
<td>100 µs</td>
<td>100 ms</td>
</tr>
</tbody>
</table>

### FLOW DETECTION PERFORMANCE

<table>
<thead>
<tr>
<th>Flows Per Second (fps)</th>
<th>THUNDER 5845 TPS</th>
<th>THUNDER 7445 TPS</th>
<th>THUNDER 14045 TPS SINGLE MODULE</th>
<th>THUNDER 14045 TPS DUAL MODULE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Flows Per Second (fps)</td>
<td>3 Million</td>
<td>6 Million</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>

### DNS AUTHORITATIVE CACHE PERFORMANCE

<table>
<thead>
<tr>
<th>DNS Queries Per Second (pps)</th>
<th>THUNDER 5845 TPS</th>
<th>THUNDER 7445 TPS</th>
<th>THUNDER 14045 TPS SINGLE MODULE</th>
<th>THUNDER 14045 TPS DUAL MODULE</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNS Queries Per Second (pps)</td>
<td>N/A</td>
<td>35 Million</td>
<td>35 Million</td>
<td>N/A</td>
</tr>
</tbody>
</table>

### NETWORK INTERFACE

<table>
<thead>
<tr>
<th>Network Interface</th>
<th>THUNDER 5845 TPS</th>
<th>THUNDER 7445 TPS</th>
<th>THUNDER 14045 TPS SINGLE MODULE</th>
<th>THUNDER 14045 TPS DUAL MODULE</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/10 GE Fiber (SFP+)</td>
<td>48</td>
<td>48</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>40 GE Fiber (QSFP+)</td>
<td>0</td>
<td>0</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>100 GE Fiber</td>
<td>4 (QSFP28)</td>
<td>4 (QSFP28)</td>
<td>4 (CFP2 or QSFP28)</td>
<td>4 (CFP2 or QSFP28)</td>
</tr>
<tr>
<td>Management Ports</td>
<td>1 x Ethernet Management Port, 1 x RJ-45 Console Port*</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### HARDWARE SPECIFICATIONS

<table>
<thead>
<tr>
<th>Hardware Specification</th>
<th>THUNDER 5845 TPS</th>
<th>THUNDER 7445 TPS</th>
<th>THUNDER 14045 TPS SINGLE MODULE</th>
<th>THUNDER 14045 TPS DUAL MODULE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processor</td>
<td>Intel Xeon 18-core</td>
<td>2 x Intel Xeon 18-core</td>
<td>2 x Intel Xeon 18-core</td>
<td>4 x Intel Xeon 18-core</td>
</tr>
<tr>
<td>Memory (ECC RAM)</td>
<td>64 GB</td>
<td>128 GB</td>
<td>256 GB</td>
<td>512 GB</td>
</tr>
<tr>
<td>Storage</td>
<td>SSD</td>
<td>SSD</td>
<td>SSD</td>
<td>SSD</td>
</tr>
<tr>
<td>Hardware Acceleration</td>
<td>2 x FTA-4, SPE</td>
<td>3 x FTA-4, SPE</td>
<td>4 x FTA-3, SPE</td>
<td>8 x FTA-3, SPE</td>
</tr>
<tr>
<td>Dimensions (Inches)</td>
<td>1.75’h x 17.5(W)x30(D)</td>
<td>1.75’h x 17.5(W)x30(D)</td>
<td>5.3’h x 169(W)x30(D)</td>
<td>5.3’h x 169(W)x30(D)</td>
</tr>
<tr>
<td>Rack Units (Mountable)</td>
<td>1U</td>
<td>1U</td>
<td>3U</td>
<td>3U</td>
</tr>
<tr>
<td>Unit Weight</td>
<td>34.3 lbs</td>
<td>35.7 lbs</td>
<td>80 lbs</td>
<td>102 lbs</td>
</tr>
<tr>
<td>Power Supply (DC option available)</td>
<td>Dual 1500W RPS</td>
<td>Dual 1500W RPS</td>
<td>2+2 1100W RPS</td>
<td>2+2 1100W RPS</td>
</tr>
<tr>
<td>Power Consumption (Typical/Max)*2</td>
<td>585W / 921W</td>
<td>784W / 1,078W</td>
<td>1,000W / 1,200W</td>
<td>1,700W / 2,000W</td>
</tr>
<tr>
<td>Heat in BTU/ Hour (Typical/Max)*3</td>
<td>1,997 / 3,143</td>
<td>2,676 / 3,679</td>
<td>3,412 / 4,095</td>
<td>5,801 / 6,825</td>
</tr>
<tr>
<td>Cooling Fan</td>
<td>Hot Swap Smart Fans</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Operating Ranges</td>
<td>Temperature 0°C - 40°C</td>
<td>Humidity 5% - 95%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Regulatory Certifications</td>
<td>FCC Class A, UL, CE, GS, CB, VCCI, CCC, BSMI, RCM</td>
<td>FCC Class A, UL, CE, GS, CB, VCCI, CCC, BSMI, RCM</td>
<td>FCC Class A, UL, CE, GS, CB, VCCI, CCC, BSMI, RCM</td>
<td>FCC Class A, UL, CE, GS, CB, VCCI, CCC, BSMI, RCM</td>
</tr>
<tr>
<td>Standard Warranty</td>
<td>90-Day Hardware and Software</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The specifications and performance numbers are subject to change without notice, and vary depending on configuration and environmental conditions. As for network interface, it’s highly recommended to use A10 Networks qualified optics/transceivers to ensure network reliability and stability.

*1 Throughput performances are traffic-forwarding capacity and measured with legitimate traffic with DDoS protection enabled.

*2 With base model. The value may vary with SSL options.

*3 Available in Q4 2019. *4 Optional RPS available | *5 Fixed SFP+ optical ports with dual rate (10GBASE-SR and 1000BASE-SX) | *6 Available in Q4 2019 | *7 Certification in process | *8 Thunder 14045 comes with a splitter cable for console to provide access to both modules.
vTHUNDER TPS VIRTUAL APPLIANCE

vTHUNDER TPS

| Supported Hypervisors | VMware ESXi 5.5 or higher  
Microsoft Hyper-V on Windows Server 2008 R2 or higher |
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Hardware Requirements</td>
<td>See Installation Guide</td>
</tr>
<tr>
<td>Standard Warranty</td>
<td>90-Day Software</td>
</tr>
<tr>
<td>Bandwidth Licenses</td>
<td>1 Gbps</td>
</tr>
<tr>
<td>VMware ESXi</td>
<td>●</td>
</tr>
<tr>
<td>Microsoft Hyper-V</td>
<td>●</td>
</tr>
</tbody>
</table>

Lab license is also available | * 5 Gbps license not recommended for Microsoft Hyper-V

DETAILED FEATURE LIST
Features may vary by appliance.

Detection/Analysis
- In-line packet-based DDoS detection
- Out-of-band flow-based DDoS detection
- Distributed detection
- Individual detection policies for more than 256K servers and services
- Continuous behavioral learning
- Manual and learned thresholds
- Protocol anomaly detection
- Inspection within IPinIP (e.g., networking, encapsulation)
- Black/white lists
- Traffic indicator and top talkers
- Mitigation console
- Packet debugger tool

DDoS Threat Intelligence Service
- Dynamically updated threat intelligence feed
- IP addresses of reflected amplification weapons
- IP addresses of DDoS botnets

Zero-Day Automated Protection
- Dynamically discover and apply attack pattern filters
- Prevent zero-day attacks
- No pre-configuration or manual intervention
- Fast, automated response

Resource Attack Protection
- Fragmentation attack
- Slowloris
- Slow GET/POST
- Long form submission
- SSL renegotiation

Application Attack Protection
- Application-aware filter
- Regular expression filter (TCP/UDP/HTTP/SIP)
- HTTP request rate limit (per URI)
- DNS request rate limit (per type)
- SIP request limit (per type)
- Application request malformed check (DNS/HTTP/SIP)
- DNS domain-list
- HTTP/HTTPS protocol compliance
- Application (DNS/HTTP/SIP) flood protection
- Signature-based IPS
Detailed Feature Lists (Cont.)

**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)
- POODLE attack
- TCP/UDP/ICMP flood protection
- Per-connection traffic control

**Challenge-based Authentication**

- TCP SYN cookies, SYN authentication
- ACK authentication
- Spoof detection
- SSL authentication*
- DNS authentication
- HTTP challenge

**Telemetry**

- Rich traffic and DDoS statistics counters
- sFlow v5
- NetFlow (e.g., v9, IPFIX)
- Custom counter blocks for flow-based export
- High-speed logging
- CEF logging

**Protected Objects**

- Protected zones for automated detection and mitigation
- Source/destination IP address/subnet
- Source and destination IP pair
- Destination port
- Source port
- Protocol (e.g., HTTP, DNS, SIP, TCP, UDP, ICMP and others)
- Class list/geolocation
- Passive mode

**Actions**

- Capture packet
- Run script
- Drop
- TCP reset
- Dynamic authentication
- Add to black list
- Add to white list
- Log
- Limit concurrent connections
- Limit connection rate
- Limit traffic rate (pps/bps)
- Forward to other device
- Remote-Triggered Black Hole (RTBH)

**Management**

- Dedicated on-box management interface (GUI, CLI, SSH, Telnet)
- aGalaxy for comprehensive management**
- SNMP, syslog, email alerts
- REST API (aXAPI) or SDK
- LDAP, TACACS+, RADIUS support
- Configurable control CPUs

**Networking and Deployment**

- Proactive, Reactive, Asymmetric, Symmetric, Out-of-Band (TAP)
- Transparent (L2), routed (L3)
- Routing: static routes, BGP4+, OSPF, OSPFv3, IS-IS
- Bidirectional Forwarding Detection (BFD)
- VLAN (802.1Q)
- Trunking (802.1AX), LACP
- Access control lists (ACLs)
- Network Address Translation (NAT)
- MPLS traffic protection
- BGP route injection, FlowSpec
- IPinIP (source and terminate)
- GRE tunnel interface
- VXLAN

**High-Performance, Scalable Platform**

- Advanced Core Operating System (ACOS)
  - Linear application scaling
  - ACOS on data plane
- Linux on control plane
- IPv6 feature parity

---

* Features may vary by appliance
** aGalaxy is an optional product

©2019 A10 Networks, Inc. All rights reserved. A10 Networks, the A10 Networks logo, ACOS, A10 Thunder, Thunder TPS, A10 Lightning, A10 Harmony, and SSL Insight are trademarks or registered trademarks of A10 Networks, Inc. in the United States and 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. For the full list of trademarks, visit: www.a10networks.com/a10-trademarks.