THUNDER TPS

Next-generation DDoS Protection

A10 Networks® 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, and more sophisticated application attacks.

The Thunder TPS product line is built upon our Advanced Core Operating System (ACOS®) platform, with A10's Symmetric Scalable Multi-Core Processing (SSMP) software architecture which 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 provides deep traffic visibility to spot anomalies across the traffic spectrum, and protects against multiple classes of attack vectors, including volumetric, protocol and sophisticated application-layer attacks, which are detected and mitigated to prevent a service from becoming unavailable. The system has access to a rich set of protocol and application checks and a wide range of authentication methods to verify if client communications are valid, or if the traffic is scripted botnet traffic. In addition, customized actions can be taken as needed with our programmatic policy engine.
- **High performance to meet 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 10 to 155 Gbps, (and up to 1.2 Tbps in a list synchronization cluster), or up to 223 million packets per second (pps). Thunder TPS ensures that the largest DDoS attacks can be handled effectively. Select Thunder TPS models are equipped with a hardware-assisted Security and Policy Engine (SPE) to enforce security policies at high speed. The Field Programmable Gate Array (FPGA) hardware is leveraged to immediately detect and mitigate over 50 common infrastructure attack vectors. SSL processors make the system even more efficient at detecting and mitigating SSL-based attacks. More complex application-layer (L7) attacks (HTTP, 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.
- **Flexibility for customization and broad network integration:** To easily integrate in various networking architectures, a vendor neutral, flexible DDoS mitigation solution is required. Various network deployment models for in- and out-of-band operations are available and with our RESTful API, aXAPI, Thunder TPS enables integration to your custom or third-party detection solutions. Information such as logs and network statistics can be shared at high speeds, using common standards. The programmatic

Supported Platforms

Thunder TPS
physical appliance

Overview

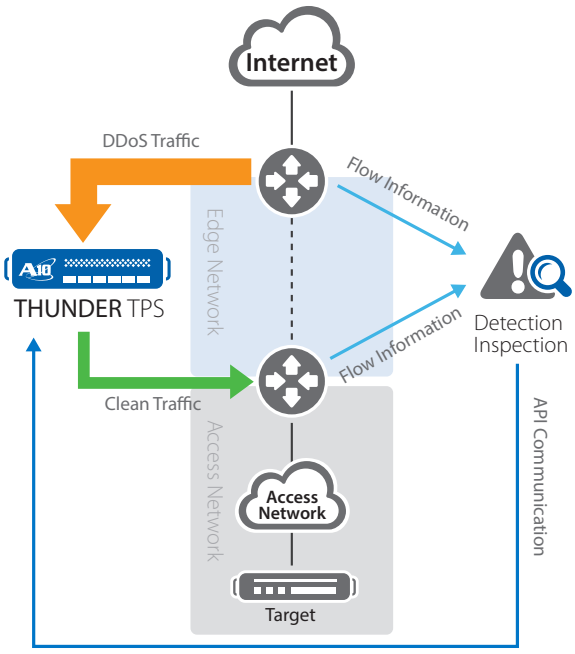
The Thunder TPS product line is a family of high-performance appliances that detect and mitigate multi-vector DDoS attacks at the network edge, functioning as a first line of defense for your network infrastructure.

policy engine allows for fully customized detection and mitigation using TCL-based aFleX® scripting technology, or leveraging regular expressions (regex) and Berkeley Packet Filter (BPF) pattern matching filters to perform deep packet inspection (DPI).

A10 Thunder TPS devices protect 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 significant lower power usage, reduced rack space and lowered cooling requirements.

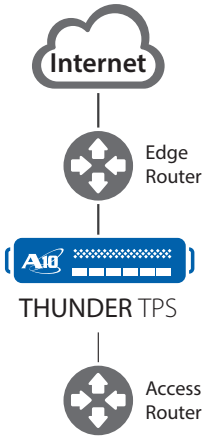
Architecture and Key Components

Asymmetric mode



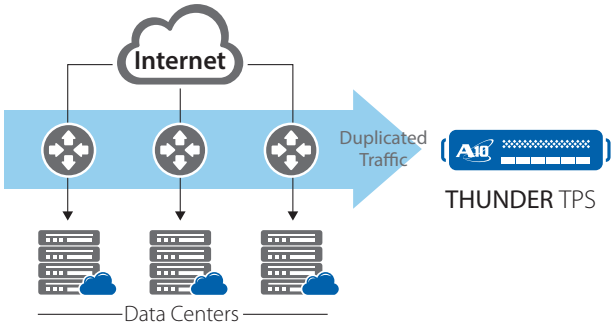
For on-demand, or permanent (proactive) mitigation, triggered manually or by flow analytical systems

Symmetric (Inline) mode



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

Out-of-band (TAP) 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 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. The system provides a vast set of features to validate, block or rate-limit the traffic entering the network.

- **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 DNS or NTP amplification attacks, are aimed to flood and saturate a victim's Internet connection, thus rendering services unavailable. Thunder TPS offers a variety of authentication techniques, amplification and flood attack mitigation, and filter spoofed traffic or apply highly granular, multi-protocol rate limiting to prevent sudden surges of illegitimate traffic to overwhelm network and server resources. It is possible to apply limits per connection, defined by bandwidth or packet rate.
  - Protocol attacks, such as SYN floods, 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 50 anomaly attacks in hardware to stop them before the system CPUs have to be involved. For example, SYN requests can be validated, or other features to manage out of sequence segments, TCP/UDP port scanning and many more are available.
  - Application attacks such as slowloris, HTTP GET flood or SSL-based attacks are specifically exploiting a weakness in an application's function or trying to make it unavailable. Thunder TPS provides many application checks and request rate limit control. With A10's programmatic aFleX feature, Thunder TPS is able to perform deep packet inspection (DPI)

on incoming packets and take defined actions to protect the application. For example, the system can enforce limits on various DNS query types, or apply security checks in many portions of the HTTP header.

High performance to meet growing attack scale:

Over the last years, DDoS attacks have rapidly proliferated in terms of bandwidth (Gbps) and packets per second (pps). Thunder TPS can leverage high-performance, specialized hardware as well as the latest, most powerful Intel Xeon CPUs to mitigate the largest and most sophisticated attacks.

- **High performance platform:** With mitigation throughput capacity ranging from 10 to 155 Gbps (or 1.2 Tbps in a list synchronization cluster) ensures that the largest DDoS attacks can be handled effectively. Select Thunder TPS models are equipped with high-performance FPGA-based FTA technology to detect and mitigate over 50 common attack vectors immediately, before the data CPUs are involved. SYN cookies can be generated to validate client connection requests, at a rate of up to 223 Mpps. The Security and Policy Engine (SPE) hardware enforces highly granular traffic rates; as fine as 100 ms interval. SSL security processors are leveraged for detecting and mitigating SSL-based attacks, including the recent POODLE vulnerability. More complex application-layer (L7) attacks (HTTP, DNS, etc.) are processed by the latest Intel Xeon CPUs, so that high-performance system scaling is maintained even for multi-vector attacks. Network connectivity is provided with 1, 10 and 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 for 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 user-defined hosts and/or subnets.

Flexibility for customization and broad network 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.

- **Programmatic Policy Engine:** a fully programmable centralized configuration and management engine along with access to system states and statistics to simplify enforcement of advanced application and security policies. The detection and mitigation capabilities are extremely customizable, using the aFleX TCL-based language, or regular expression (regex) and Berkeley Packet Filter (BPF) for high-speed pattern matching in policies.
- **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 including MPLS inspection, Thunder TPS can be integrated into any network architecture, of any size. And, with aXAPI, our RESTful API, Thunder TPS can easily be integrated into third-party detection solutions. The common event format (CEF) open log management standard, increases cross-platform support.

The unprecedented capacity of Thunder TPS allows a device to be deployed in asymmetric 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 10 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. Select models benefit from our Security and Policy Engine (SPE) hardware acceleration, leveraging FPGA-based FTA technology among other hardware optimized packet processing to provide highly scalable flow distribution and DDoS protection capabilities. The FPGA detects and mitigates more than 50 common attack vectors in hardware without impacting the performance of the data 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 with 1, 10 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 devices can be clustered for even higher capacity and efficient list synchronization.

Appliance Summary/Specifications Table

	Thunder 3030S TPS	Thunder 4435(S) TPS	Thunder 5435(S) TPS	Thunder 6435(S) TPS
Throughput	10 Gbps	38 Gbps	77 Gbps	155 Gbps
TCP SYN Auth/sec*	6.5 million	35 million	35 million	70 million
SYN Cookie/sec*	6.5 million	55 million	112 million	223 million
Network Interface				
1 GE Copper	6	0	0	0
1 GE Fiber (SFP)	2	0	0	0
1/10 GE Fiber (SFP+)	4	16	16	16
40 GE Fiber (QSFP+)	0	0	4	4
Management Interface	Yes	Yes	Yes	Yes
Lights Out Management	Yes	Yes	Yes	Yes
Console Port	Yes	Yes	Yes	Yes
Solid-state Drive (SSD)	Yes	Yes	Yes	Yes
Processor (Intel Xeon)	4-core	10-core	10-core	Dual 12-core
Memory (ECC RAM)	16 GB	64 GB	64 GB	128 GB
Hardware Acceleration				
64-bit Linear Decoupled Architecture	Yes	Yes	Yes	Yes
Flexible Traffic Acceleration	Software	1 x FTA-3+ FPGA	2 x FTA-3+ FPGA	4 x FTA-3+ FPGA
Switching/Routing	Software	Hardware	Hardware	Hardware
SSL Security Processor ('S' Models)	Single	Dual	Dual	Quad
Power Consumption (Typical/Max)^	131W / 139W	350W / 420W	400W / 480W	620W / 710W
Heat in BTU/hour (Typical/Max)^	447 / 474	1,195 / 1,433	1,365 / 1,638	2,116 / 2,423
Power Supply (DC option available)	Dual 600W RPS	Dual 1100W RPS	Dual 1100W RPS	Dual 1100W RPS
	80 Plus "Platinum" efficiency, 100 - 240 VAC, Frequency 50 – 60 Hz			
Cooling Fan	Hot Swap Smart Fans			
Dimensions	1.75 in (H), 17.5 in (W), 17.45 in (D)	1.75 in (H), 17.5 in (W), 30 in (D)	1.75 in (H), 17.5 in (W), 30 in (D)	1.75 in (H), 17.5 in (W), 30 in (D)
Rack Units (Mountable)	1U	1U	1U	1U
Unit Weight	20.1 lbs	34.5 lbs	35.5 lbs	39 lbs
Operating Ranges	Temperature 0° C - 40° C | Humidity 5% - 95%			
Regulatory Certifications	FCC Class A‡, UL‡, CE‡, TUV‡, CB‡, VCCI‡, China CCC‡, BSMI‡, RCM (replace C-Tick) ‡, KCC‡‡, GOST-R‡‡, FAC‡‡, NEBS‡‡‡, RoHS | FIPS 140-2^^			
Standard Warranty	90-day Hardware and Software			

* Packets per second. Performance varies with deployment mode and configuration
^ With base model. The value may vary with SSL options | ^^ Certification in process and FIPS model must be purchased
‡ Except Thunder 3030S that is in process | ‡‡ In process for Thunder 3030S | ‡‡‡ Except Thunder 3030S


Thunder 3030S


Thunder 4435(S) TPS


Thunder 5435(S) TPS


Thunder 6435(S) TPS

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
- IPv6 feature parity

Networking

- Asymmetric, Symmetric, Out-of-band (TAP)
- Transparent (L2), Routed (L3)
- Routing: Static Routes, BGP4+
- VLAN (802.1Q)
- Trunking (802.1AX), LACP
- Access Control Lists (ACLs)
- Network Address Translation (NAT)
- MPLS traffic protection

Management

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

Flood Attack Protection

- SYN Cookies
- SYN Authentication
- ACK Authentication
- Spoof detection
- SSL Authentication
- DNS Authentication
- HTTP Challenge
- TCP/UDP/ICMP Flood protection
- Application (DNS/HTTP) Flood protection
- Amplification Attack Protection

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

Resource Attack Protection

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

Application Attack Protection

- Application Layer (L7) Scripting (aFleX)
- Regular Expression filter (TCP/UDP/HTTP)
- HTTP Request Rate Limit
- DNS Request Rate Limit
- DNS Query Check
- HTTP Protocol Compliance
- HTTP Anomalies

Protected Objects

- Source/Destination IP Address/Subnet
- Source and Destination IP Pair
- Destination Port
- Source Port
- Protocol (HTTP, DNS, TCP, UDP, ICMP and others)
- DNS Query Type
- URI
- Class List/Geo Location
- Passive Mode

Actions

- 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)

Telemetry

- Rich traffic and DDoS statistics counters
- sFlow v5
- netFlow (v9, IPFIX)
- Custom counter blocks for flow based export
- High Speed Logging
- CEF Logging

Redirection

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

Detection/Analysis

- Manual Thresholds
- Protocol Anomaly Detection
- Inspection within IPinIP
- Black/White Lists
- IP/Port Scanning Detection
- Traffic indicator and Top-talkers
- Mitigation Console (GUI)
- Packet Debugger Tool (GUI)

Carrier-grade Hardware

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

*Features may vary by appliance.

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**

Corporate Headquarters

A10 Networks, Inc
3 West Plumeria Ave.
San Jose, CA 95134 USA
Tel: +1 408 325-8668
Fax: +1 408 325-8666
www.a10networks.com

Part Number: A10-DS-15101-EN-06
Jan 2015

Worldwide Offices

North America
sales@a10networks.com
Europe
emea_sales@a10networks.com
South America
latam_sales@a10networks.com
Japan
jinfo@a10networks.com
China
china_sales@a10networks.com
Taiwan
taiwan@a10networks.com
Korea
korea@a10networks.com
Hong Kong
HongKong@a10networks.com
South Asia
SouthAsia@a10networks.com
Australia/New Zealand
anz_sales@a10networks.com

To learn more about the A10 Thunder Application Service Gateways and how it can enhance your business, contact A10 Networks at: **www.a10networks.com/contact** or call to talk to an A10 sales representative.