Data Sheet

Thunder TPS

DDoS Detection, Mitigation & Cloud Protection

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 Unlike outdated DDoS defense products, A10 Networks' defenses include detection capabilities across key networks elements including A10 Thunder® ADC, CGN and CFW.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.

Platforms and Services

Thunder TPS
Physical Appliance

Thunder TPS
Virtual Appliance

DDoS Protection
Cloud

Management

aGALAXY
Management

Talk With A10

Web
a10networks.com/tps

Benefits

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

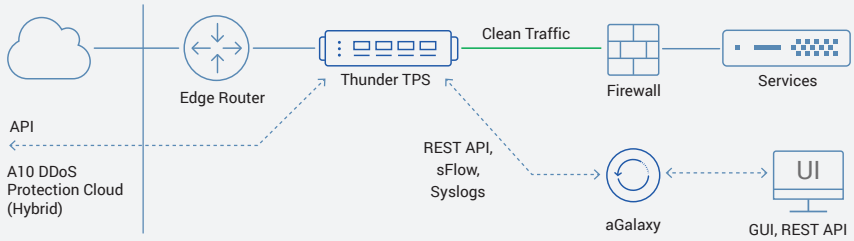
No organization has unlimited trained personnel or resources during real-time DDoS attacks. Thunder TPS supports five levels of programmatic mitigation escalation and de-escalation per protected zone. Remove the need for frontline personnel to make time-consuming manual changes to escalating mitigation 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

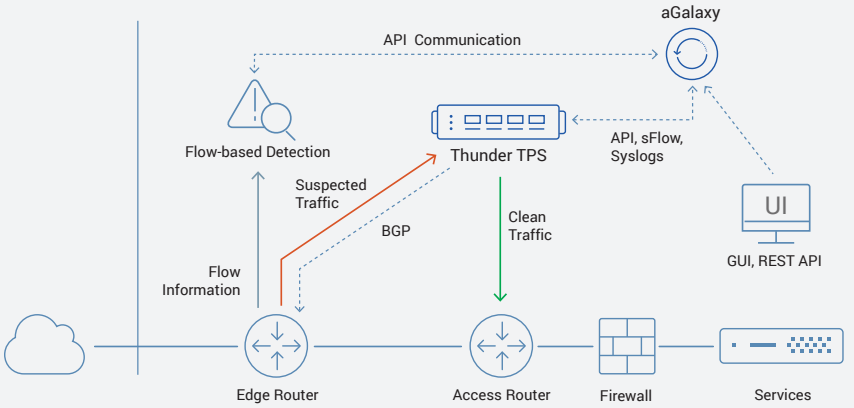
Thunder TPS is extremely efficient. It delivers high performance in a small form factor to reduce OPEX with significantly lower power usage, rack space, and cooling requirements.

Reference Architectures



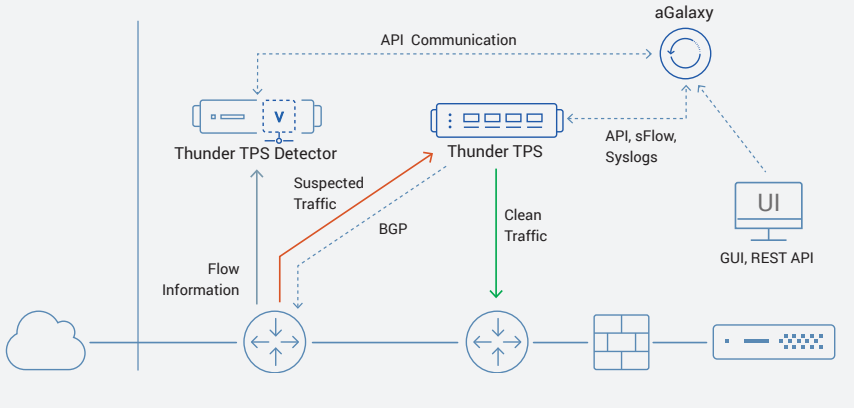
Proactive Mode
(Asymmetric or Symmetric)

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

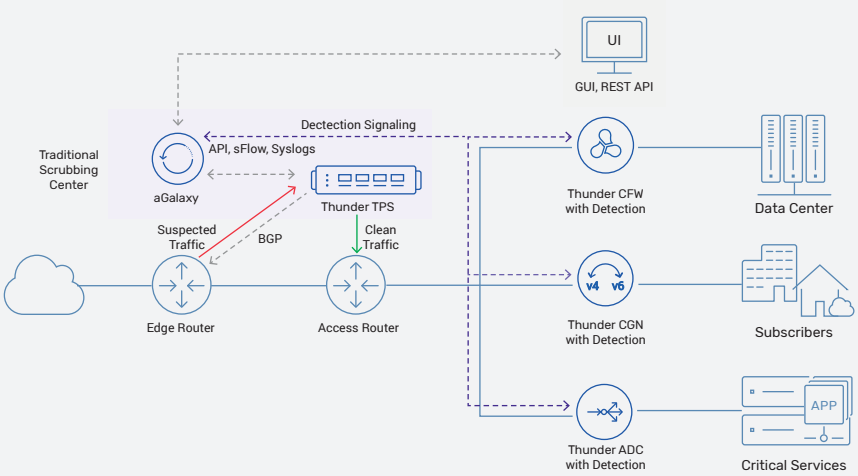
Larger networks benefit from on-demand mitigation, triggered manually or by flow analytical systems. TPS fits in any network configuration with integrated BGP and other routing protocols. This eliminates the need for any additional diversion and re-injection routers. A10 Networks partners with the industry's 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

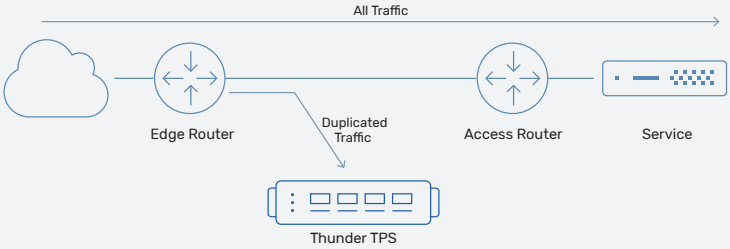
Thunder TPS Detector is available as a standalone appliance or integrated with aGalaxy 5000. The flow-based DDoS detector supports tightly integrated interworking with aGalaxy management and Thunder TPS mitigation for a complete reactive DDoS defense solution.

Reference Architectures



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 provides 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.

Features

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 provides 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 IoTbased 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 70 million queries per second. Non-stop DNS can also work in conjunction with Thunder TPS DDoS defenses to create a highly resilient DNS service.

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

Aggregated and correlated DDoS weapons intelligence from over 40 reputable data sources, 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 and Efficiency to Meet Growing Attack Scale

Thunder TPS provides solutions to protect organizations from attacks of all sizes, from 1 to 380 Gbps (or 3 Tbps in a list synchronization cluster).

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 blocking of up to 500 million packets per second (Mpps). Thunder TPS enforces highly granular traffic rates up to 100 ms intervals. The enhanced vThunder TPS running on KVM hypervisor provides 100 Gbps throughput in a single virtual appliance and can be expanded to 800 Gbps with eight-way clustering.

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.

Complex

Attack Mitigation at Scale

Thunder TPS tracks more than 27 traffic and behavioral indicators and can apply escalating protocol challenges to surgically differentiate attackers from valid users for appropriate mitigation of up to 256 million concurrent tracked sessions.

Complex application attacks (e.g., HTTP, DNS, etc.) are mitigated with advanced parallel processing across a large number of CPU cores to maintain high-performance system scaling, even for multi-vector attacks.

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 DDoS Weapons 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

7655 TPS

By the Numbers

1.2 Tbps HW Blocking	380 Gbps Throughput	3 Tbps Throughput in Cluster	8x16M Threat Class Lists
100 GbE Ports	500 Mpps	60 Hardware Mitigations	64K Protected Objects

Thunder TPS Physical Appliance Specifications

Performance	Thunder 1040 TPS	Thunder 3040 TPS	Thunder 4435 TPS	Thunder 5845 TPS
Throughput (Software Scrubbing)*1	5 Gbps	10 Gbps	38 Gbps	100 Gbps
Hardware Blocking	N/A	N/A	N/A	250 Gbps
Packets Rate (pps)*1	2.5 Million	4.5 Million	20 Million	28 Million
Software-based - SYN Authentication (pps)	2.5 Million	4.5 Million	20 Milloin	28 Million
Hardware-based - Anomaly Flood Blocking (pps)	N/A	N/A	55 Million	125 Million
Maximum Concurrent Sessions (Asymmetric Deployment)	8 Million	10 µs	32 Million	48 Million
Average Latency	10 µs	10 µs	35 µs	50 µs
Minimum Rate Enforcement Interval	100 ms			

Flow Detection Performance				
Flows Per Second (fps)	N/A	1 Million	3 Million	3 Million

Network Interface		Hardware Bypass Model			
1 GE Copper	5	1 + 4 (Bypass)	6	0	0
1 GE Fiber (SFP)	0	0	2	0	0
1/10 GE Fiber (SFP+)	4*3	4*3	4	16	48
1/10 GE Fiber (Fixed)	0	2 (Optical Bypass)*5	0	0	0
100 GE Fiber	0	0	0	0	4 (QSFP28)
Management Ports	Ethernet Management Port, RJ-45 Console Port				

Hardware Specifications				
Processor	Intel Communications Processor	Intel Xeon 4-core	Intel Xeon 10-core	Intel Xeon 18-core
Memory (ECC RAM)	16 GB	16 GB	64 GB	64 GB
Storage	SSD	SSD	SSD	SSD
Hardware Acceleration	Software	Software	FTA-3, SPE	2 x FTA-4, SPE
Dimensions (Inches)	1.75 (H) x 17.5 (W) x 17.25 (D)	1.75 (H) x 17.5 (W) x 17.45 (D)	1.75 (H) x 17.5 (W) x 30 (D)	1.75 (H) x 17.5 (W) x 30 (D)
Rack Units (Mountable)	1U	1U	1U	1U
Unit Weight	14 lbs | 16 lbs (RPS)	20.6 lbs	34.5 lbs	34.3 lbs
Power Supply (DC option available)	Single 750W*4	Dual 600W RPS	Dual 1100W RPS	Dual 1500W RPS
	80 Plus Platinum efficiency, 100-240 VAC, 50-60 Hz			
Power Consumption (Typical/Max)*2	80W / 110W	180W / 240W	350W / 420W	585W / 921W
Heat in BTU/Hour (Typical/Max)*2	273 / 376	615 / 819	1,195 / 1,433	1,997 / 3,143
Cooling Fan	Removable Fans	Hot Swap Smart Fans		
Operating Ranges	Temperature 0° - 40° C | Humidity 5% - 95%			
Regulatory Certifications	FCC Class A, UL, CE, TUV, CB, VCCI, CCC^, BSMI^, RCM^ | RoHS	FCC Class A, UL, CE, GS, CB, VCCI, CCC, KCC, BSMI, RCM | RoHS	FCC Class A, UL, CE, TUV, CB, VCCI, CCC, MSIP, BSMI, RCM, EAC, NEBS | CC EAL2+, RoHS	FCC Class A, UL, CE, GS, CB, VCCI, CCC^, BSMI, RCM | RoHS^
Standard Warranty	90-Day Hardware and Software			

Thunder TPS Physical Appliance Specifications (Cont.)

Performance	Thunder 7445 TPS	Thunder 14045 TPS Single-Module	Thunder 14045 TPS Dual-Module	Thunder 7655 TPS‡
Throughput (Software Scrubbing)*1	220 Gbps	150 Gbps	300 Gbps	380 Gbps
Hardware Blocking	500 Gbps	500 Gbps	500 Gbps	1.2 Tbps
Packets Rate (pps)*1	60 Million	60 Million	110 Million	110 Million
Software-based - SYN Authentication (pps)	60 Million	60 Million	110 Million	110 Million
Hardware-based - Anomaly Flood Blocking (pps)	250 Million	220 Million	440 Million	500 Million
Maximum Concurrent Sessions (Asymmetric Deployment)	64 Million	128 Million	256 Million	256 Million
Average Latency	50 µs	60 µs	60 µs	70 µs
Minimum Rate Enforcement Interval	100 ms			
Flow Detection Performance				
Flows Per Second (fps)	6 Million	N/A	N/A	N/A
DNS Authoritative Cache Performance				
DNS Queries Per Second (qps)	35 Million	35 Million	N/A	70 Million
Network Interface				
1/10 GE Fiber (SFP+)	48	0	0	0
40 GE Fiber (QSFP+)	0	4	4	0
100 GE Fiber	4 (QSFP28)	4 (CFP2 or QSFP28)	4 (CFP2 or QSFP28)	16 (QSFP28)
Management Ports	Ethernet Management Port, RJ-45 Console Port+			
Hardware Specifications				
Processor	2 x Intel Xeon 18-core	2 x Intel Xeon 18-core	4 x Intel Xeon 18-core	2 x Intel Xeon 24-core
Memory (ECC RAM)	128 GB	256 GB	512 GB	384 GB
Storage	SSD	SSD	SSD	SSD
Hardware Acceleration	3 x FTA-4, SPE	4 x FTA-3, SPE	8 x FTA-3, SPE	2 x FTA-5, SPE
Dimensions (Inches)	1.75 (H) x 17.5 (W) x 30 (D)	5.3 (H) x 16.9 (W) x 30 (D)	5.3 (H) x 16.9 (W) x 30 (D)	2.625 (H) x 17.5 (W) x 30 (D)
Rack Units (Mountable)	1U	3U	3U	1.5U
Unit Weight	35.7 lbs	80 lb	102 lbs	44.2 lbs
Power Supply (DC option available)	Dual 1500W RPS	2+2 1100W RPS	2+2 1100W RPS	Dual 1500W RPS
	80 Plus Platinum efficiency, 100-240 VAC, 50-60 Hz			
Power Consumption (Typical/Max)*2	784W / 1,078W	1,000W / 1,200W	1,700W / 2,000W	965W / 1,222W
Heat in BTU/Hour (Typical/Max)*2	2,676 / 3,679	3,412 / 4,095	5,801 / 6,825	3,293 / 4,170
Cooling Fan	Hot Swap Smart Fans			
Operating Ranges	Temperature 0° - 40° C | Humidity 5% - 95%			
Regulatory Certifications	FCC Class A, UL, CE, GS, CB, VCCI, CCC^, BSMI, RCM | RoHS^	FCC Class A, UL, CE, GS, CB, VCCI, CQC, CCC^, KCC, BSMI, RCM | RoHS	FCC Class A, UL, CE, GS, CB, VCCI, CQC, CCC^, KCC, BSMI, RCM | RoHS	FCC Class A^, UL^, CE^, GS^, CB^, VCCI^, CCC^, BSMI^, RCM^ | RoHS^
Standard Warranty	90-Day Hardware and Software			

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 | *3 10Gbps speed only | *4 Optional RPS available | *5 Fixed SFP+ optical ports with dual rate (10GBASE-SR and 1000BASE-SX)
^ Certification in process | + Thunder 14045 comes with a splitter cable for console to provide access to both modules | ‡ Available in Q3 2020

Thunder TPS Virtual Appliance Specifications

vThunder TPS

Supported Hypervisors	VMware ESXi 5.5 or higher KVM QEMU 2.5 or higher (SR-IOV) Microsoft Hyper-V on Windows Server 2008 R2 or higher
Hardware Requirements	See Installation Guide
Standard Warranty	90-Day Software

Bandwidth Licenses	1 Gbps	2 Gbps	5 Gbps	FlexPool (40Gbps/100Gbps)
KVM	●	●	●	●
VMware ESXi	●	●	●	●
Microsoft Hyper-V	●	●	●*	●

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

vThunder TPS Sizing Recommendations

Performance License	1/2/5 Gbps	40 Gbps^	100 Gbps^
vCPU	6	8	24
vRAM	16 GB	16 GB	64 GB
vDisk	60 GB	60 GB	100 GB

^Available in Q3 2020. Requires vThunder TPS running on KVM with SR-IOV enabled. For 100 Gbps, Mellanox Connect X-5 NIC is recommended.

vThunder TPS Detector Flow Detection Performance*

Flows per Second (fps)	150K	500K	1.5M
vCPU	2	3	5
vRAM	16 GB	32 GB	64 GB
vDisk	40 GB	40 GB	40 GB

*Using vThunder TPS Standalone Detector image.

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

- Machine Learning powered attack pattern recognition and filtering
- 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/S protocol compliance
- Application (DNS/HTTP/SIP) flood protection
- Signature-based IPS
- QUIC version control and malformed header check

Protocol Attack Protection

- Invalid packets
- Anomalous TCP flag combinations (no flag, SYN-FIN, SYN frag, LAND attack)
- SYN-ACK amplification attack protection
- 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
- 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
- Outbound mitigation (destination policy)

Detailed Features List (Cont.)

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

Learn More

About A10 Networks

Contact Us

a10networks.com/contact

Part Number: A10-DS-15101-EN-29 MAY 2020