DATA SHEET

A10 Defend DDoS Mitigator

DDoS Mitigation with Intelligent Automation

A10 Defend DDoS Mitigator (formerly Thunder TPS), a part of A10 Defend suite, is the scalable and automated DDoS protection solution powered by advanced machine learning, leading the industry in precision, 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.

Due to the increasing complexity and volume of modern-day DDoS attacks, DDoS protection has also evolved. A holistic DDoS protection suite is needed. Part of that holistic A10 Defend suite is the high precision, intelligent, scalable and automated DDoS mitigation.

A10 Defend DDoS Mitigator scales to defend against the "DDoS of Things" and traditional zombie botnets, and precisely screens out multi-vector DDoS attacks including reflection and zero-day attacks to minimize collateral damage to users. It's built with a unique multi-modal and source-based protection posture with intelligent automation in mind, including an auto-updated threat intelligent list at a scale, five-level adaptive mitigation policies, and automated zero-day attack pattern recognition powered by machine learning technologies, to name a few.

Mitigator's scale and zero-touch intelligent automation architecture with A10 Defend DDoS Orchestrator maximize effectiveness of limited staff and reduce operational cost, resulting in better ROI. Thus, A10 Defend DDoS Protection suite consisting of Detector, Mitigator, Orchestrator, and Threat Control helps organizations enable more effective DDoS protection or create profitable DDoS scrubbing services for their customers.

A10 Networks is available when you need help most. A10 support provides 24x7x365 services, including emergency assistance from the A10 DDoS Security Incident Response Team (DSIRT) to immediately help you understand and respond to DDoS incidents.

Platforms

Physical and SPE Appliances

Virtual Appliance

Cloud

Related Products & Services

A10 Defend DDoS Detector

A10 Defend DDoS Orchestrator (A10 Control)

A10 Defend Threat Control

DSIRT Support

Learn More

A10Networks.com/a10-defend

Benefits

Maintain

Service Availability

Downtime results in immediate productivity and revenue loss for any business. Mitigator ensures service availability by automatically spotting anomalies across the traffic spectrum and mitigating multi-vector DDoS attacks.

Defeat

Growing Attacks

Mitigator protects the largest, most-demanding network environments. Mitigator 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 Mitigator hardware models benefit from our Security and Policy Engine (SPE) hardware acceleration, leveraging FPGA-based FTA technology and other hardware-optimized security checks for highly scalable packet processing and hardware DDoS protection capabilities. Mitigator appliances can scale up to eight times the mitigation capacity, regardless of form factor, either hardware or virtual appliance, by the clustering and synchronization technology.

Deploy

Wartime Support

No organization has unlimited trained personnel or resources during real-time DDoS attacks. Mitigator 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 DSIRT at any stage of an attack.

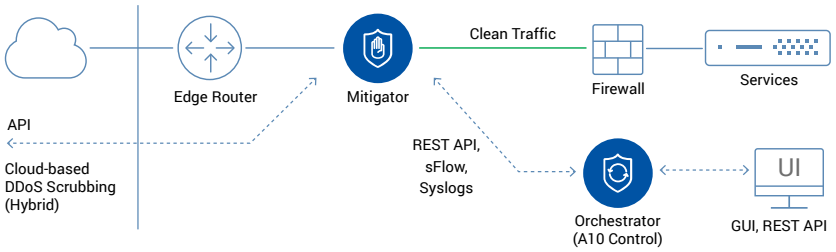
Reduce

Security OPEX

Mitigator 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. Mitigator's scale and intelligent automated mitigation architecture, along Orchestrator, simplifies the full DDoS protection workflow and lifecycle from detection, mitigation to reporting, while strengthening security posture.

The A10 Defend DDoS Protection solution maximizes effectiveness of the SecOps team and reduces operational cost, resulting in better ROI.

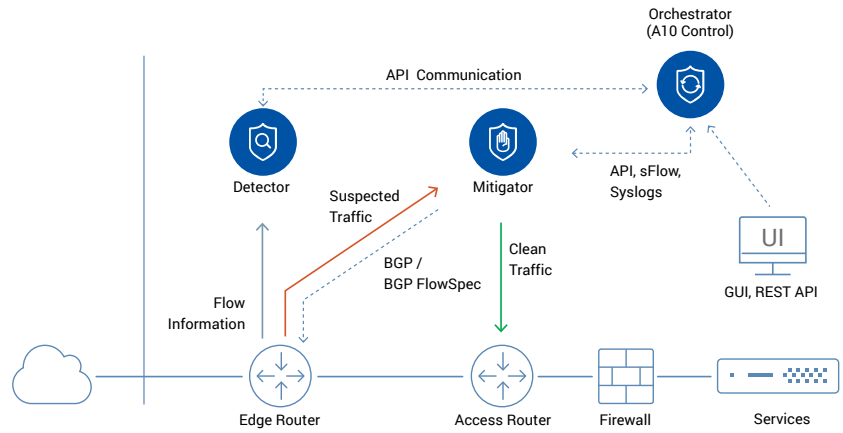
Reference Architectures



Proactive Deployment

(Asymmetric or Symmetric)

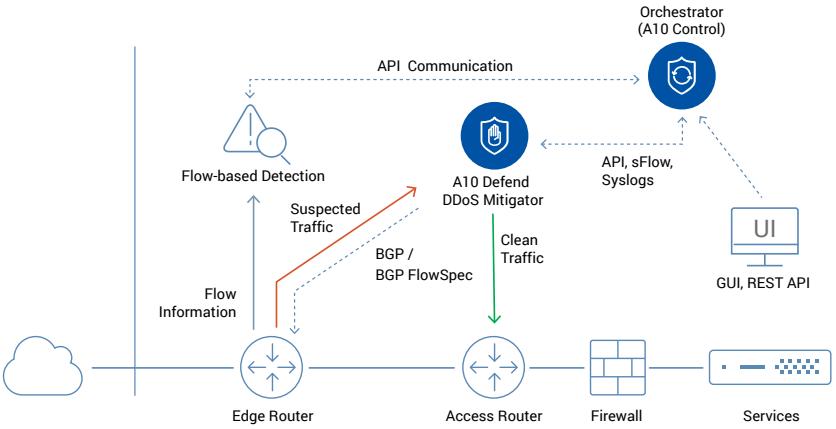
Deploying A10 Defend DDoS Mitigator inline or in-path of the services network provides continuous, comprehensive detection and fast mitigation. This mode is most useful for real-time services such as gaming and VoIP where the user experience is critical, and for enterprise DDoS protection use cases. DDoS Mitigator supports L2 or L3 in-path deployments.



Reactive Deployment

Larger networks benefit from on-demand mitigation, triggered manually or by flow analytical systems. Detector is available as a standalone appliance (hardware or virtual). The flow-based Detector is tightly integrated with Orchestrator and Mitigator for a intelligent and automated DDoS defense solution. Mitigator is capable of sending BGP FlowSpec for better collaborating with upstream routers.

Reference Architectures



Reactive Deployment with Third-party Flow Detector

A10 Defend DDoS Mitigator 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 network monitoring and DDoS detection companies to provide additional flexibility for creating best-of-class solutions for each customer's unique business needs. The third-party DDoS detection can leverage API, syslog, or BGP Flowspec, to create tightly integrated DDoS protection solutions.

Features

Full Spectrum DDoS Protection for Service Availability

Complete Solution

For Flexible Deployments

Mitigator provides a complete solution for DDoS defenses in proactive always-on or on-demand reactive modes to meet customers' business objectives. Mitigator can be deployed with inline mode in L2 or L3 with full IPv4 and IPv6 support, where the proactive mode is ideal for critical and real-time services such as gaming, voice and DNS. In reactive mode, Mitigator works in concert with Detector and Orchestrator, and becomes active only when needed. When an attack is detected by a Detector, Orchestrator instructs Mitigator to initiate a BGP route redirection for the suspicious traffic. Then Mitigator 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

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 Mitigator particularly adept to deal with simultaneous multi-vector attacks.

ZAP

Zero-day Automated Protection

The Zero-day Automated Protection (ZAP) utilizes heuristics and machine learning to 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.

Non-stop DNS

Authoritative DNS Cache

Mitigator can be configured as a high-performance authoritative DNS cache, enabling Mitigator's non-stop DNS operational mode to cache up to 240 million DNS records using zone transfer and respond to queries at rates of up to 35 million queries per second. Non-stop DNS can also work in conjunction with typical DNS DDoS protection using Mitigator to create a highly resilient DNS service.

A10 DDoS Threat Intelligence

Aggregated and correlated DDoS weapons intelligence from over 40 reputable data sources, is included with support contract enabling Mitigator 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

High Performance
Protection

Select Mitigator models have high-performance FPGA-based Flexible Traffic Acceleration (FTA) technology to immediately mitigate up to 60 common attack vectors including packet and protocol anomalies in hardware, up to 500 million packets per second (Mpps), before data CPUs are involved. Mitigator enforces highly granular traffic rates as low as 100 ms intervals.

Simultaneous
Protected Objects

To protect entire networks, applications, and services, Mitigator 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.

Scalability
Leading Mitigation Capacity

Mitigator provides solutions to protect organizations from attacks of all sizes, from 5 to 550 Gbps in power-efficient and small form factor hardware. It's also available as a virtual appliance with a feature parity and provides 100 Gbps throughput.

The Mitigator can easily scale its mitigation capacity by clustering up to 8 appliances (e.g., 4.4 Tbps in hardware, 800 Gbps in a virtual appliance) with a list synchronization technology.

Precise
Attack Mitigation at Scale

Mitigator 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 350 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.

A10 Defend DDoS Mitigator

8665S

by the Numbers

4.8 Tbps HW Blocking	550 Gbps Throughput	4.4 Tbps Throughput in Cluster	8x16M Threat Class Lists
400 GE Ports	820 Mpps Anomaly Drop (HW assisted)	60 Hardware Mitigations	64K Protected Objects

Large Threat

Intelligence Class Lists

Eight lists, each containing up to 16 million entries, may be defined to utilize data from DDoS threat intelligence sources, such as A10 Defend Threat Control. Such class lists, along with own custom black/white lists, can be configured as IP block lists or used for source IP-based mitigation policy as needed.

Zero-day

Attack Pattern Recognition

DDoS attackers continue to innovate their multi-vector attack arsenals with new strategies. The Mitigator Zero-day Attack Pattern Recognition (ZAPR) engine automatically identifies DDoS attack characteristics and dynamically applies mitigation filters without advanced configuration or manual intervention.

Full Control and Smart Automation for Agile Protection

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 thresholds per monitored entity, automatic traffic redirection orchestration, start of mitigation and escalation, and then 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, Mitigator may be integrated into any network architecture of any size, including MPLS and BGP. And with aXAPI, A10's 100-percent programmable RESTful API, Mitigator easily integrates into third-party detection solutions and into agile SecOps workflows.

Leveraging open standards like BGP blackhole and Flowspec functionality, Mitigator integrates easily with any DDoS detection and DDoS mitigation capable BGP routers 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

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

A10 Defend DDoS Mitigator Physical Appliance Specifications

DDoS Mitigator	Thunder 1060S*4	Thunder 3350-E	Thunder 5845-40G	Thunder 5845
Mitigation Performance				
Throughput (software scrubbing)*1	5/10/20 Gbps	10 Gbps	40 Gbps	100 Gbps
Hardware Blocking	N/A	N/A	250 Gbps	250 Gbps
Packets Rate (pps)*1	2.5/5/8 Million	6 Million	12 Million	25 Million
Software-based - SYN Authentication (pps)	2.5/5/8 Million	6 Million	12 Million	25 Million
Hardware-based - Anomaly Flood Blocking (pps)	N/A	N/A	125 Million	125 Million
Maximum Concurrent Sessions (asymmetric deployment)	8/10/16 Million	8 Million	32 Million	48 Million
Average Latency	15 µs	20 µs	50 µs	50 µs
Minimum Rate Enforcement Interval	100 ms	100 ms	100 ms	100 ms
DNS Authoritative Cache Performance				
DNS Queries Per Second (qps)	N/A	N/A	10 Million	18 Million
Network Interface				
1 GE (BASE-T)	7	6	0	0
1 GE Fiber (SFP)	0	2	0	0
10/1 GE Fiber (SFP+/SFP)	4	8 + 4*3	48	48
25/10 GE Fiber (SFP28/SFP+)	2	0	0	0
40 GE Fiber (QSFP+)	0	0	0	0
100/40 GE Fiber (QSFP28/QSFP+)	0	0	4	4
400 GE Fiber (QSFP-DD)	0	0	0	0
Management Ports	Ethernet mgmt. port, RJ-45 console port			
Hardware Specifications				
Processor	Intel communications processor 20-core*5	Intel Xeon 8-core	Intel Xeon 18-core*5	Intel Xeon 18-core
Memory (ECC RAM)	32 GB	16 GB	64 GB	64 GB
Storage	SSD	SSD	SSD	SSD
Hardware Acceleration	Software	Software	2 x FTA-4, SPE	2 x FTA-4, SPE
Dimensions (inches)	1.75 (H) x 17.5 (W) x 17(D)	1.75 (H) x 17.5 (W) x 18(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	12 lbs	18 lbs	34.3 lbs	34.3 lbs
Power Supply (DC option available)	Dual 300W RPS	Dual 750W RPS	Dual 1500W RPS	Dual 1500W RPS
	80 Plus Gold efficiency, 100 - 240 VAC, 50 – 60 Hz	80 Plus Platinum efficiency, 100-240 VAC, 50-60 Hz		
Power Consumption (typical/max)*2	112W / 127W	151W / 205W	585W / 921W	585W / 921W
Heat in BTU/Hour (typical/max)*2	383 / 434	516 / 700	1,997 / 3,143	1,997 / 3,143
Cooling Fan (front-to-back airflow)	Removable fans	Hot swap smart fans		
Operating Ranges	Temperature 0° - 40° C | Humidity 5% - 95%			
Regulatory Certifications	FCC Class A, UL^, ICES, CE, UKCA, CB^, VCCI, BSMI^, RCM | RoHS	FCC Class A, UL, CE, UKCA, CB, VCCI, BSMI, RCM, MTCTE^ | RoHS	FCC Class A, UL, CE, UKCA, CB, VCCI, KCC, BSMI, RCM, MTCTE^ | RoHS	FCC Class A, UL, CE, UKCA, CB, VCCI, KCC, BSMI, RCM, MTCTE^ | RoHS
Standard Warranty	90-day hardware and software			

A10 Defend DDoS Mitigator Physical Appliance (cont.)

DDoS Mitigator	Thunder 7465		
Modular License	40 Gbps	100 Gbps	270 Gbps
Mitigation Performance			
Throughput (software scrubbing)*1	40 Gbps	100 Gbps	270 Gbps
Hardware Blocking	800 Gbps	800 Gbps	1 Tbps
Packets Rate (pps)*1	13 Million	28 Million	60 Million
Software-based - SYN Authentication (pps)	13 Million	28 Million	60 Million
Hardware-based - Anomaly Flood Blocking (pps)	550 Million	550 Million	550 Million
Maximum Concurrent Sessions (asymmetric deployment)	32 Million	64 Million	128 Million
Average Latency	40 µs	40 µs	40 µs
Minimum Rate Enforcement Interval	100 ms	100 ms	100 ms
DNS Authoritative Cache Performance			
DNS Queries Per Second (qps)	N/A	N/A	N/A
Network Interface			
1 GE (BASE-T)	0		
1 GE Fiber (SFP)	0		
10/1 GE Fiber (SFP+/SFP)	0		
25/10 GE Fiber (SFP28/SFP+)	24		
40 GE Fiber (QSFP+)	0		
100/40 GE Fiber (QSFP28/QSFP+)	8		
400 GE Fiber (QSFP-DD)	0		
Management Ports	Ethernet mgmt. port, RJ-45 console port		
Hardware Specifications			
Processor	Intel Xeon 36-core*5		
Memory (ECC RAM)	256 GB		
Storage	SSD		
Hardware Acceleration	1 x FTA-6, SPE		
Dimensions (inches)	1.75 (H) x 17.5 (W) x 30 (D)		
Rack Units (mountable)	1U		
Unit Weight	38.5 lbs		
Power Supply (DC option available)	Dual 1500W RPS 80 Plus Platinum efficiency, 100-240 VAC, 50-60 Hz		
Power Consumption (typical/max)*2	680W / 770W		
Heat in BTU/Hour (typical/max)*2	2,321 / 2,628		
Cooling Fan (front-to-back airflow)	Hot swap smart fans		
Operating Ranges	Temperature 0° - 40° C | Humidity 5% - 95%		
Regulatory Certifications	FCC Class A, UL, CE, UKCA, CB, VCCI, KCC, BSMIˆ, RCM, MTCTEˆ, ANATELˆ | RoHS		
Standard Warranty	90-day hardware and software		

A10 Defend DDoS Mitigator Physical Appliance (cont.)

DDoS Mitigator	Thunder 7445	Thunder 7655S	Thunder 8665S
Mitigation Performance			
Throughput (software scrubbing)*1	220 Gbps	380 Gbps	550 Gbps
Hardware Blocking	500 Gbps	1.2 Tbps	4.8 Tbps
Packets Rate (pps)*1	50 Million	100 Million	120 Million
Software-based - SYN Authentication (pps)	50 Million	100 Million	110 Million
Hardware-based - Anomaly Flood Blocking (pps)	250 Million	500 Million	820 Million
Maximum Concurrent Sessions (asymmetric deployment)	64 Million	256 Million	350 Million
Average Latency	60 µs	40 µs	40 µs
Minimum Rate Enforcement Interval	100 ms	100 ms	100 ms
DNS Authoritative Cache Performance			
DNS Queries Per Second (qps)	35 Million	N/A	N/A
Network Interface			
1 GE (BASE-T)	0	0	0
1 GE Fiber (SFP)	0	0	0
10/1 GE Fiber (SFP+/SFP)	48	0	0
25/10 GE Fiber (SFP28/SFP+)	0	0	0
40 GE Fiber (QSFP+)	0	0	0
100/40 GE Fiber (QSFP28/QSFP+)	4	16	0
400 GE Fiber (QSFP-DD)	0	0	12
Management Ports	Ethernet mgmt. port, RJ-45 console port		2 x Ethernet mgmt. port, RJ-45 console port
Hardware Specifications			
Processor	2 x Intel Xeon 18-core	2 x Intel Xeon 28-core	2 x Intel Xeon 36-core
Memory (ECC RAM)	128 GB	384 GB	512 GB
Storage	SSD	SSD	SSD
Hardware Acceleration	3 x FTA-4, SPE	2 x FTA-5, SPE	3 x FTA-6, SPE
Dimensions (inches)	1.75 (H) x 17.5 (W) x 30 (D)	2.625 (H) x 17.5 (W) x 30 (D)	2.625 (H) x 17.5 (W) x 30 (D)
Rack Units (mountable)	1U	1.5U	1.5U
Unit Weight	35.7 lbs	44.2 lbs	44.9 lbs
Power Supply (DC option available)	Dual 1500W RPS	Dual 1500W RPS	Dual 2500W RPS
	80 Plus Platinum efficiency, 100-240 VAC, 50-60 Hz		
Power Consumption (typical/max)*2	784W / 1,078W	1,121W / 1,300W	1,491W / 1,720W
Heat in BTU/Hour (typical/max)*2	2,676 / 3,679	3,826 / 4,436	5,088 / 5,869
Cooling Fan (front-to-back airflow)	Hot swap smart fans		
Operating Ranges	Temperature 0° - 40° C | Humidity 5% - 95%		
Regulatory Certifications	FCC Class A, UL, CE, UKCA, CB, VCCI, BSMI, RCM, MTCTE^ | RoHS	FCC Class A, UL, CE, UKCA, CB, VCCI, BSMI, RCM, MTCTE^ | RoHS	FCC Class A, UL, CE, UKCA, CB, VCCI, RCM | RoHS
Standard Warranty	90-day hardware and software		

Hardware specifications and performance numbers are subject to change without notice, and may 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 Available in different capacity with modular license. Specifications and numbers vary based on the modular license tier
*5 Active CPU core counts may vary depending on the modular license | ^ Certification in process

A10 Defend DDoS Mitigator Software Specifications

A10 Defend DDoS Mitigator Virtual Appliance	
Supported Hypervisors	VMware ESXi 7.0 or higher (SR-IOV, DirectPath I/O), KVM QEMU (SR-IOV, PCI Passthrough)
Hardware Requirements	See installation guide
Standard Warranty	90-day software

Virtual Appliance License and Sizing Recommendations

Throughput	Lab/1/2/5 Gbps	50 Gbps*1	100 Gbps*1
vCPU	8	16	32
vRAM	16 GB	32 GB	64 GB
vDisk	128 GB	256 GB	384 GB
Licence Types	Bandwidth license (per instance)	FlexPool	FlexPool
Hypervisors	ESXi, KVM	ESXi, KVM	ESXi, KVM

*1 Supported in ACOS 6.0 and above for ESXi and ACOS 7.0.2 and above for KVM, and tested with with NVIDIA Mellanox ConnectX-6 NIC.

A10 Defend DDoS Mitigator for Cloud	Microsoft Azure
Throughput per instance	Up to 5 Gbps
Image Format	Microsoft VHD
Licenses	30-day trial license | BYOL FlexPool license

Detailed Feature List

Features may vary by appliance.

Detection/Analysis

- In-line packet-based DDoS detection
- Individual detection policies for more than 256K servers and services
- 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
- Top-k insights (source, destination)
- Outbound detection
- Victim IP Identification

DDoS Threat Intelligence List

- Large capacity class lists for proactive blocking of toxic IP addresses as a first layer of protection
- Up to 96 million active entries - maximum 8 lists with each containing up to 16M
- Action or mitigation policies can be defined for each list
- Support various types of DDoS threat intelligence feed including ThreatSTOP and IP block list from A10 Defend Threat Control

Zero-day Automated Protection

- ZAPR: Machine learning powered attack pattern recognition and filtering
- TCP progression tracking
- 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, FQDN, label count)
- 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
- QUIC version control and malformed header check
- Packet watermarking (UDP) for gaming traffic
- Encrypted flood attack protection

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/SSL/ICMP flood protection
- Per-connection traffic control

Challenge-based Authentication

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

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 symmetric deployment

Non-stop DNS Solution

- Act as authoritative DNS cache
- Seamless layered protection with A10 Defend Mitigator in scrubbing center
- DNS water torture (random subdomain) attack protection
- Selective and customizable action (response/ forward/ drop)

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)
- BGP Flowspec

Management

- Dedicated on-box management interface (GUI, CLI, SSH, Telnet)
- A10 Defend DDoS Orchestrator (ADO) app, running on A10 Control, for comprehensive management and operation
- 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)
- Virtual wire
- 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,
- BGP FlowSpec
- IPinIP (source and terminate)
- GRE tunnel interface
- VXLAN

Detailed Feature List (Cont.)

Telemetry

- Rich traffic and DDoS statistics counters
- sFlow v5
- Custom counter blocks for flow-based export
- High-speed logging
- CEF logging

High-performance, Scalable Platform

- Advanced Core Operating System (ACOS)
- Linear application scaling
- ACOS on data plane
- Linux on control plane
- IPv6 feature parity
- Security policy engine (SPE) enabling hardware acceleration for policy enforcement*
- High-performance hardware blocking*

Carrier-grade Hardware*

- Advanced hardware architecture
- Hot-swap redundant power supplies (AC and DC)
- Smart fans (hot swap)
- Solid-state drive (SSD)
- Tamper detection
- 25GE, 40GE, 100GE and 400GE interfaces

Security and Capability Assurance Certifications*

- Common Criteria EAL 2+
- FIPS 140-1 Level 1 Compliance (all)

* Features and certifications may vary by appliance.

About A10

A10Networks.com

Contact Us

A10Networks.com/contact

Part Number: A10-DS-15136-EN-06 January 2026