DATA SHEET

A10 Defend Detector

Precise, Highly Scalable Network-wide Anomaly Detection

A10 Defend Detector (formerly Thunder TPS), a part of A10 Defend suite, is the high-performance flow-based network anomaly detection that provides precise and faster DDoS detection with automated traffic behavior profiling. With A10 Defend Orchestrator and Mitigator, it enables intelligent automated DDoS defense suited for network-wide protection.

Detecting Modern DDoS Attacks

In today's hyper-connected world, service providers and large enterprises face a constant barrage of threats. Among them, distributed denial-of-service (DDoS) attacks stand out for their sheer power and potential to disrupt critical service and infrastructure. DDoS attacks flood victims' networks with a large volume of malicious traffic, aiming to take down services, disrupt operations, and ultimately damage reputation.

Modern DDoS attacks present immense challenges to organizations. Attackers have an arsenal of tools at their disposal, from DDoS toolkits, online services (DDoS-as-a-service) and weaponized IoT devices to DDoS botnets. They often exploit vulnerabilities in open internet servers, launching reflection-amplification attacks that magnify the attack volume and hide their true source. To further complicate matters, they might employ carpet bombing attacks, spreading the attack across multiple targets — a range of IP addresses — potentially triggering many alerts and exhausting DDoS scrubbing capacity. This combination of techniques makes DDoS defense incredibly challenging.

Platforms

Physical Appliances

Virtual Appliance

Related Products & Services

A10 Defend Mitigator

A10 Defend Orchestrator

A10 Defend Threat Control

DSIRT Support

Talk with A10

A10Networks.com/a10-defend

Precision Matters

While simple volumetric attacks might be detectable by monitoring traffic volume, this approach may not be effective against today's sophisticated threats. Traditional solutions struggle with high false positives, delayed detection, and resource-draining mitigation. This leaves the service network vulnerable and wastes precious resources and time during critical moments.

Due to the increasing volume and complexity of modern-day DDoS attacks, DDoS protection has also evolved. A holistic DDoS protection suite is needed. A10 Defend Detector, part of the holistic A10 Defend suite, is a high-performance network-wide DDoS detection solution with higher precision and intelligence.

A10 Defend Detector is a standalone network flow-based traffic anomaly detection technology that collects network flows information via NetFlow or IPFIX from routers, tracks the traffic behavior and patterns and creates a baseline profile using unique indicators. It supports continuous traffic-pattern learning, eliminating tedious and time-consuming work while ensuring dynamic thresholds for precise anomaly detection and faster mitigation.

It offers unmatched performance and capacity that allows organizations to have fewer flow-based detectors and simplifies the deployment. Combined with A10 Defend Orchestrator and Mitigator, a whole DDoS protection cycle is streamlined and can be seamlessly executed with intelligent automation, from detection, traffic diversion to scrubbing center, as well as mitigation and reporting after the incident.

The A10 Defend suite, consisting of A10 Defend Detector, Mitigator, Orchestrator, and Threat Control, helps organizations enable more effective DDoS protection and/or create profitable DDoS scrubbing services for their customers. A10 Networks is available when you need help most. A10 Networks 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.

A10 Defend Suite

A10 Defend Detector

High-performance NetFlow, sFlow, IPFIX-based DDoS detector to easily manage the scale and heterogenous nature of SP networks, resulting in a unified DDoS protection solution.

A10 Defend Mitigator

High precision, automated, scalable, and intelligent DDoS mitigation solution is delivered as hardware or virtual appliances ranging from 1 Gbps to over 1 Tbps.

A10 Defend Orchestrator

Enables organizations to gain a global view of their environments to rapidly identify and remediate DDoS attacks and ensure that policies are consistently enforced from a central point.

A10 Defend Threat Control

Standalone SaaS platform proactively establishes a robust first layer of defense by offering actionable analytics and blocklists.

Benefits

Maximize

Service Availability

Downtime results in immediate productivity and revenue loss for any business. It's critical for organizations to protect their network infrastructure, mission-critical applications, and their subscribers and tenants from today's evolving DDoS attacks. A10 Defend Detector provides precise traffic anomaly detection by leveraging unique behavioral traffic indicators and continuous learning, which helps organization take appropriate actions and remedies before the DDoS attack impacts their networks and customers' services.

Defeat

Modern Attacks

Modern DDoS attacks have evolved far beyond simple volumetric flooding. They are now sophisticated, multi-layered, and often leverage several techniques to evade detection. For example, a reflection-amplification attack is a commonly used technique that typically exploits vulnerabilities in internet servers to amplify the attack traffic, making it harder to identify the true source. A carpet-bombing attack is another technique to spread attack destinations to a wide range of IP addresses, making it harder to identify the target and possibly generating an unmanageable number of alerts. Sometimes these techniques can be combined. A10 Defend Detector has multiple detection mechanisms and can precisely detect such complex targeted volumetric attacks.

Simplify

Deployment and Operation

DDoS protection deployment and operation can be a very complicated process and no organization has unlimited trained personnel or resources available as SecOps teams typically take care of many other security concerns and issues. The A10 Defend suite offers a complete solution from automated traffic profiling and monitoring, precise DDoS detection, minimizing false negatives and positives, along with seamless orchestration and traffic diversion, multi-modal mitigation with intelligent automation and auto-generating incident reporting. In addition, A10's DSIRT is available to work live with SecOps team at any stage of an DDoS attack incident.

Reduce

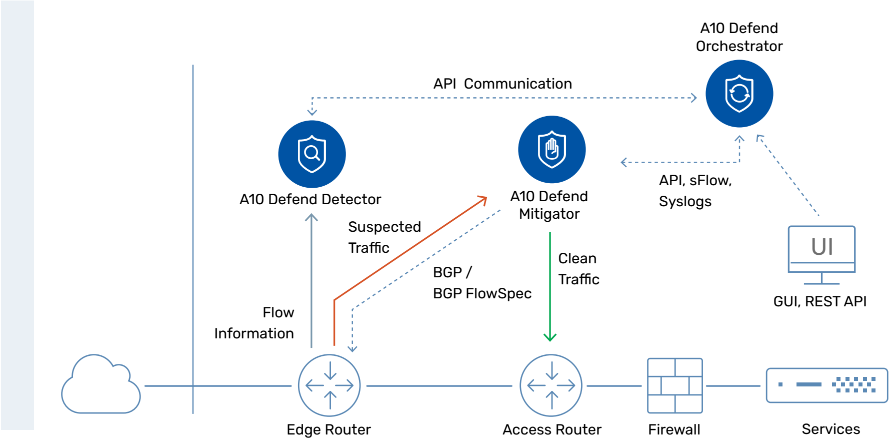
Security OPEX

When monitoring network-wide and large traffic volumes, network flow-based DDoS detection is the right choice for operational and cost effectiveness.

A10 Defend Detector is extremely efficient. It delivers unmatched high performance in a small form factor, up to 6 million flows per second in 1 RU, that allows coverage of a wide area of the network (or consolidation of dozen of legacy flow-based detectors into one). This results in a reduction of OPEX with significantly lower power usage, rack space, and cooling requirements.

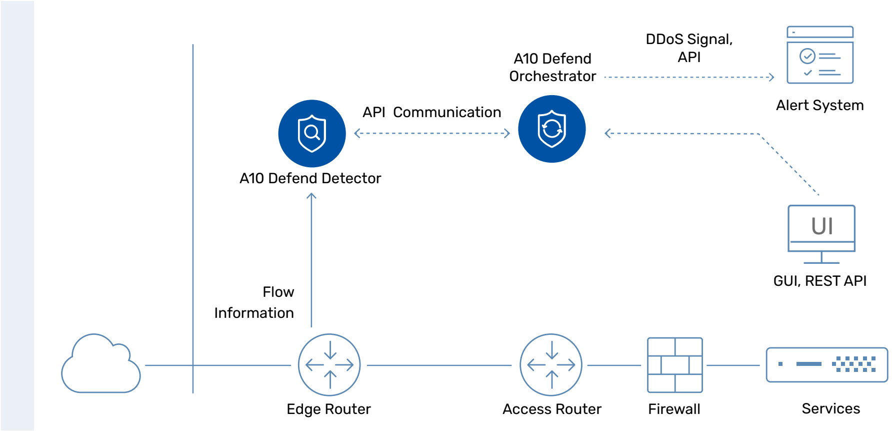
A10 Defend Detector's scale and intelligent automation orchestrated by A10 Defend Orchestrator, simplifies the full DDoS protection workflow and lifecycle from detection and mitigation to reporting, while strengthening the security posture. The A10 Defend solution maximizes effectiveness of the SecOps team and reduces operational costs, resulting in better ROI.

Reference Architectures



Reactive Deployment

Larger networks benefit from on-demand mitigation, triggered manually or by flow analytical systems. A10 Defend Detector is available as a standalone appliance (hardware or virtual). The flow-based DDoS detector is tightly integrated with A10 Defend Orchestrator and Mitigator for a intelligent and automated DDoS defense solution. A10 Defend Mitigator is capable of sending BGP FlowSpec for better collaborating with upstream routers.



Detection-only Deployment

To build a DDoS protection strategy and milestone, it's recommended to get a good understanding of network traffic and anomalous activities. The A10 Defend suite can be deployed in detection-only mode using A10 Defend Detector and Orchestrator to provide insights into network traffic for the monitored entity and make the organization aware of real DDoS activities based on collected network-flow information. In the case where A10 Defend Detector has detected a DDoS attack, the detailed information is available in Orchestrator, or the alert can be forwarded to organization's alert system.

Features

High Performance

Detection

A10 Defend Detector provides unmatched performance for network flow collection and DDoS detection, processing up to 6 million flows per second (fps) on a hardware appliance and up to 1.5 million fps on a virtual appliance. A10 Defend Detector can allow monitoring of up to 3,000 protected objects with zone configuration or covering hundreds of class-B or thousands of class-C network subnets in a network object configuration with unique automated network discovery technology. This enables fewer devices to manage and simplifies deployment and management as 10 or more legacy flow-based DDoS detection systems can be consolidated into one A10 Defend Detector.

Smart

Victim Identification

A10 Defend Detector's network region object uses the victim identification technology that is suitable for service providers who need an automated DDoS defense solution to protect their enterprise subscribers and network and service infrastructure against volumetric DDoS attacks as well as carpet-bombing attacks. It uses intelligent automation to adaptively slice the monitored network entities and hierarchically profile each entity of active subnet or IP based on real-time traffic distribution. Narrowing down the scope of the victim helps conserve DDoS scrubbing center resources and enables efficient operations. When it comes to detection strategy, it uses advanced baselining using a characteristic histogram in parallel with automatic baselining using volume-centric traffic indicators, ensuring high-precision DDoS detection.

Precise

Behavioral Anomaly Detection

No organization can afford service downtime; thus, DDoS detection plays a crucial role for minimizing the impact from imminent DDoS attacks. A10 Defend Detector tracks the network traffic pattern using unique traffic and behavioral indicators, not only packet rate (pps) or volume (bps), but also protocol or behavior-based rate such as TCP empty ACK rate and SYN/FIN ratio, and automatically learns and builds behavioral traffic profiles for each service defined under the zone object. This technique provides precise detection by reducing false negatives and enabling faster time-to-detect operation.

Automatic

Baselining and Profiling

Baselining traffic patterns is the foundation of effective DDoS detection. Traditionally, baselining network traffic was a manual burden, hindering agility and accuracy. A10 Defend Detector provides automated baselining that continuously learns traffic patterns and adapts using various and unique traffic indicators. This eliminates tedious work while ensuring dynamic thresholds. Whether facing seasonal spikes or emerging threats, real-time adjustments help ensure precise anomaly detection and faster mitigation. Automation delivers speed and efficiency as well as flexibility and granular control. Customized baselines and thresholds can be leveraged for specific subscribers, services, or even individual servers for pinpoint precision for simple and faster detection. Through automated baselining for streamlined defense, an organization can focus on what matters most — protecting their network and business.

Intelligent

Automation

The A10 Defend suite provides a complete and automated DDoS protection solution for service providers and large enterprises who are securing services and subscribers from DDoS attacks. A10 Defend Detector works in concert with A10 Defend Mitigator and Orchestrator in a reactive or on-demand deployment. When an attack is detected and reported by a Detector, Orchestrator instructs Mitigator to initiate the mitigation along with sending a BGP notification for redirecting the suspicious traffic. Then Mitigator applies adaptive countermeasures including five levels of progressive mitigation policies with auto-escalation and machine learning powered automated zero-day attack pattern recognition before delivering the clean traffic to the intended destination.

A10 Defend Detector Physical Appliance Specifications

Defend Detector	Thunder 3350-E	Thunder 5845-40G	Thunder 5845	Thunder 7445
Flow Detection Performance				
Flows Per Second (fps)	1 Million	3 Million[*3]	3 Million	6 Million
Network Interface				
1 GE Copper	6	0	0	0
1 GE Fiber (SFP)	2	0	0	0
1/10 GE Fiber (SFP+)	8+4[*1]	48	48	48
1/10 GE Fiber (Fixed)	0	0	0	0
40 GE Fiber (QSFP+)	0	0	0	0
100 GE Fiber	0	4 (QSFP28)	4 (QSFP28)	4 (QSFP28)
Management Ports	Ethernet mgmt. port, RJ-45 console port			
Hardware Specifications				
Processor	Intel Xeon 8-core	Intel Xeon 18-core[*3]	Intel Xeon 18-core	2 x Intel Xeon 18-core
Memory (ECC RAM)	16 GB	64 GB [*3]	64 GB	128 GB
Storage	SSD	SSD	SSD	SSD
Hardware Acceleration	Software	2 x FTA-4, SPE	2 x FTA-4, SPE	3 x FTA-4, SPE
Dimensions (inches)	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)	1.75 (H) x 17.5 (W) x 30 (D)
Rack Units (mountable)	1U	1U	1U	1U
Unit Weight	18 lbs	34.3 lbs	34.3 lbs	35.7 lbs
Power Supply (DC option available)	Dual 750W RPS	Dual 1500W RPS	Dual 1500W RPS	Dual 1500W RPS
	80 Plus Platinum efficiency, 100-240 VAC, 50-60 Hz			
Power Consumption (typical/max)[*2]	151W / 205W	585W / 921W	585W / 921W	784W / 1,078W
Heat in BTU/Hour (typical/max)[*2]	516 / 700	1,997 / 3,143	1,997 / 3,143	2,676 / 3,679
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 | RoHS	FCC Class A, UL, CE, CB, VCCI, KCC, BSMI, RCM | RoHS	FCC Class A, UL, CE, UKCA, CB, VCCI, KCC, BSMI, RCM | RoHS	FCC Class A, UL, CE, CB, VCCI, BSMI, 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 10Gbps speed only | *2 With base model |
*3 The number of flows per second (fps), and the number of active CPU core counts and memory size may vary depending on the module license .| ^ Certification in process

A10 Defend Detector Virtual Appliance Specifications

A10 Defend Detector Virtual Appliance	
Supported Hypervisors	VMware ESXi 6.7 or higher (SR-IOV)
Hardware Requirements	See installation guide
Standard Warranty	90-day software

Virtual Appliance License and Sizing Recommendations*

Zone Object Configuration			
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

Network Object Configuration			
Flows Per Second (fps)	150K	500K	1.5M
vCPU	6	8	24
vRAM	16 GB	32 GB	64 GB
vDisk	40 GB	40 GB	40 GB

* Using A10 Defend Detector (formerly Thunder TPS) standalone Detector image.

Detailed Feature List

Features may vary by appliance.

Detection/Analysis

- Network flow-based anomaly detection
- Individual detection policies for more than 256K servers and services
- Continuous behavioral learning and profiling
- Automated adaptive thresholds
- Custom thresholds
- Behavioral traffic indicators and top talkers
- Inbound and outbound detection
- Service discovery
- Victim network/host dentification

Protected Objects

- Protected zone for per-service level monitoring
- Protected zone for per-IP level monitoring
- Network object for subnet and IP level monitoring

Actions

- Anomaly notification signal (start / stop)
- Reporting and visibility
- Fully automated mitigation using A10 Defend Orchestrator and Mitigator
- Manual mitigation using A10 Defend Orchestrator and Mitigator

Management

- Dedicated on-box management interface (GUI, CLI, SSH, Telnet)
- A10 Defend Orchestrator for comprehensive management
- SNMP, syslog, email alerts
- REST API (aXAPI)
- LDAP, TACACS+, RADIUS support
- Configurable control CPUs

Telemetry

- Rich traffic and DDoS statistics counters
- sFlow**
- NetFlow v5**, v9, IPFIX
- Custom counter blocks for flow-based export
- High-speed logging
- CEF logging
- REST API (aXAPI)

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
- 40 GbE and 100 GbE ports

Security and Capability Assurance Certifications*

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

* Features and certifications may vary by appliance.

** Available for zone-based detection. For network object detection, to be supported in 1H 2024.

Learn More

About A10 Networks

Contact Us

A10networks.com/contact

Part Number: A10-DS-15138-EN-01 Mar 2024