DATA SHEET

A10 Defend Orchestrator

DDoS Defense Monitoring, Orchestration and Management

A10 Defend Orchestrator (formerly aGalaxy® management system), a part of A10 Defend suite, integrates with A10 Defend Detector and Mitigator (formerly Thunder TPS®) for intelligent and automated DDoS protection, providing a centralized point of control for seamless DDoS defense management and execution.

Real-time Global DDoS Defense Management

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 centralized management component. This centralized management console is needed to help customers understand and manage the new complexities that come with modern DDoS attacks and modern DDoS protection appliances.

The A10 Defend DDoS protection suite empowers enterprises, data center and service providers to surgically distinguish DDoS attackers from valid users and block unwanted traffic.

The solution's industry-leading scalability ensures an organization's frontline security personnel are more effective with optimized wartime workflows.

A10 Defend Orchestrator enables organizations to gain a global view of their environments to rapidly identify and remediate attacks and ensure that DDoS protection policies are consistently enforced from a central point. Administrators can configure and comprehensively monitor network activity using telemetry data from their Defend Detector and Defend Mitigator, observe DDoS attacks in real time, and drill down to see the details of the DDoS attack incident.

Defend Orchestrator scales to manage multiple Detector and Mitigator deployments — across geographic locations — to streamline operations and lower IT operating costs.

Platforms

Virtual Appliance

Related Products & Services

A10 Defend Detector

A10 Defend Mitigator

A10 Defend Threat Control

DSIRT Support

Talk with A10

A10Networks.com/a10-defend

Benefits

Automate

DDoS Defense for Stronger Protection

As a central point of the DDoS protection architecture, A10 Defend Orchestrator enables intelligent automated DDoS defense by working in concert with A10 Defend Detector and Mitigator when a DDoS attack occurs. This includes DDoS detection, alerting, suspicious traffic diversion, DDoS traffic scrubbing, and attack mitigation with a multi-modal approach along with continuous analysis until the attack subsides. This will drastically reduce the burden of manual operation which is time-consuming and prone to errors.

Once the DDoS incident is over, Defend Orchestrator automatically generates a DDoS incident report that can be sent via email. Security operators can be assured of the intelligent, automated DDoS defense from provisioning, wartime operation to the incident reporting workflows.

Accelerate

Wartime Response

No organization has unlimited trained personnel or resources during real-time DDoS attacks. Within the A10 Defend suite, A10 Defend Detector performs flow analytics on the live traffic to monitor DDoS attacks and detect any traffic anomalies toward the protected services and victim IP hosts based on the dynamically learned detection thresholds.

In case of a DDoS attack, security operators can monitor the incident status in real time through a live dashboard called Mitigation Console on the Defend Orchestrator, and can control and manage DDoS defense policies as needed. A10 Defend Mitigator enforces a multi-modal protection approach including DDoS threat intelligence list and attack filter list-based mitigation, five-level adaptive protection with automatic mitigation escalation and de-escalation, and automated zero-day attack pattern recognition powered by machine learning technology. This drastically improves the response time and minimizes the need for time-consuming manual changes and reevaluation of mitigation strategies during attacks.

Maximize

IT Agility and Security

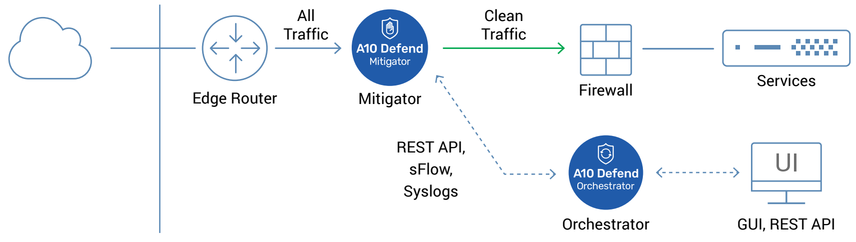
As network operators embrace web scale and SecOps/DevOps practices, they need to quickly provision changes, identify issues and roll back configurations when necessary. A10 Defend Orchestrator makes it easy to assess and learn the network traffic patterns using A10 Defend Detector, and to update mitigation policies on multiple A10 Defend Mitigators at once from a central point using a graphical user interface or over the REST API (aGAPI). A10 Defend Orchestrator also supports easy integration with existing third-party DDoS detection systems, external SIEM and/or syslog servers for consolidated security operation.

Reduce

Security OPEX

A10 Defend DDoS protection is extremely efficient. A10 Defend Detector and Mitigator appliances deliver high performance in a small form factor to reduce OPEX with significantly lower power usage, rack space, and cooling requirements. A10 Defend Orchestrator enables intelligent and automated DDoS defense that helps further reduce operational complexity and associated costs.

Reference Architectures

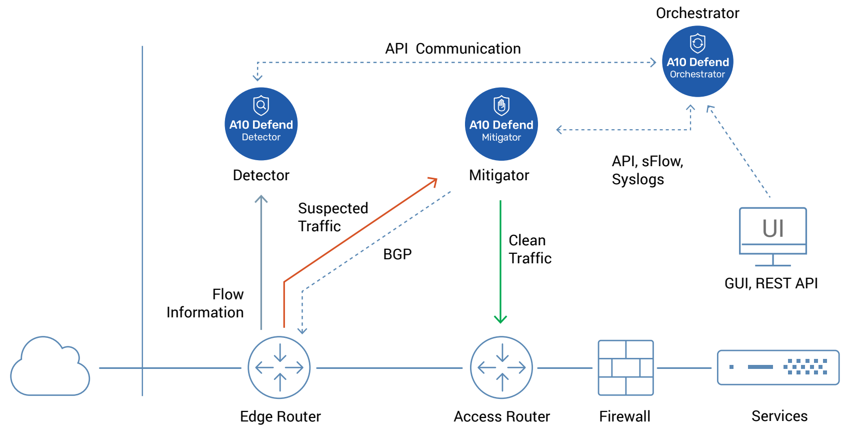


Proactive Deployment

(Asymmetric or Symmetric)

Deploying A10 Defend Mitigator in proactive mode provides continuous, comprehensive detection and fast mitigation. This mode is most useful for real-time services such as gaming and DNS where the user experience is critical, and for protection against application-layer attacks.

A10 Defend Orchestrator provides traffic visibility and wartime DDoS mitigation dashboard and console.



Reactive Deployment

Larger networks benefit from on-demand mitigation, triggered manually or by flow analytical systems. A10 Defend Orchestrator seamlessly integrates with globally deployed A10 Defend Detector and Mitigator, and enables automated DDoS protection upon detecting traffic anomalies to protect victims from the DDoS attacks.

The A10 Defend suite also works with third-party detection solution using A10's open API and/or BGP FlowSpec to protect your investment and augment your DDoS defense infrastructure.

Features

Intelligent Automation Across the Full Protection Cycle

Simplified

Automated Operation

A10 Defend 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 Defend Orchestrator does the rest based on the operator's pre-defined detection and mitigation strategies, including individual learned detection thresholds, automatic traffic redirection orchestration, start of mitigation and escalation, and applying adaptive protection policies, then extracting and applying attack pattern filters. When the attack subsides, the network and defenses are returned to peacetime posture and detailed incident reports are generated for future analysis.

Single Pane

of Glass Management

Featuring an intuitive interface, the A10 Defend Orchestrator enables organizations to manage global DDoS defense deployments across geographic locations and gain a global view of their network and DDoS incidents. Operators can run health checks, backup, update, modify configurations, apply mitigation templates and generate reports across all managed A10 Defend appliances from a central point.

Easy

and Flexible Integration

A10 Defend Orchestrator integrates seamlessly with existing third-party DDoS detection systems to automatically recognize the signs of a DDoS attack (e.g., protocol anomalies, sudden surge in traffic, large numbers of requests from known bots). Once detected, a DDoS attack incident can be created dynamically using REST API (aGAPI). Incident management not only tracks key information (e.g., attack duration and type), but also allows operators to directly mitigate an attack based on incident data.

Wartime Operation and Reporting

Real-time

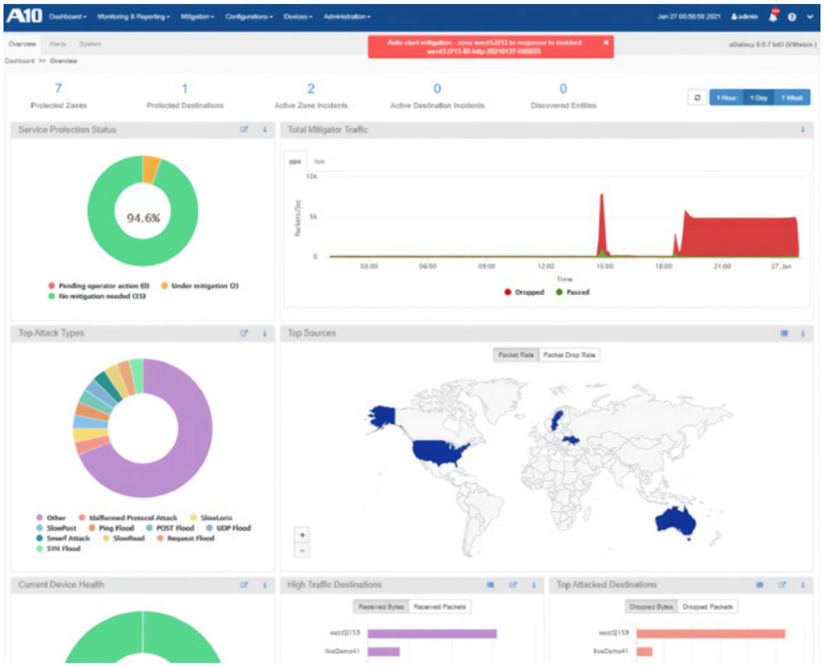
Mitigation Console

From the A10 Defend Orchestrator mitigation console, security operators can monitor incidents in real time through a live dashboard. The DDoS defense-oriented dashboard provides real-time suspicious traffic statistics, applied countermeasures, incident details including mitigation escalation levels, top-k information, and activity logs. To help further incident investigation, it enables packet capture and debugger remotely and creates custom countermeasures instantly, as needed.

Robust

Reporting

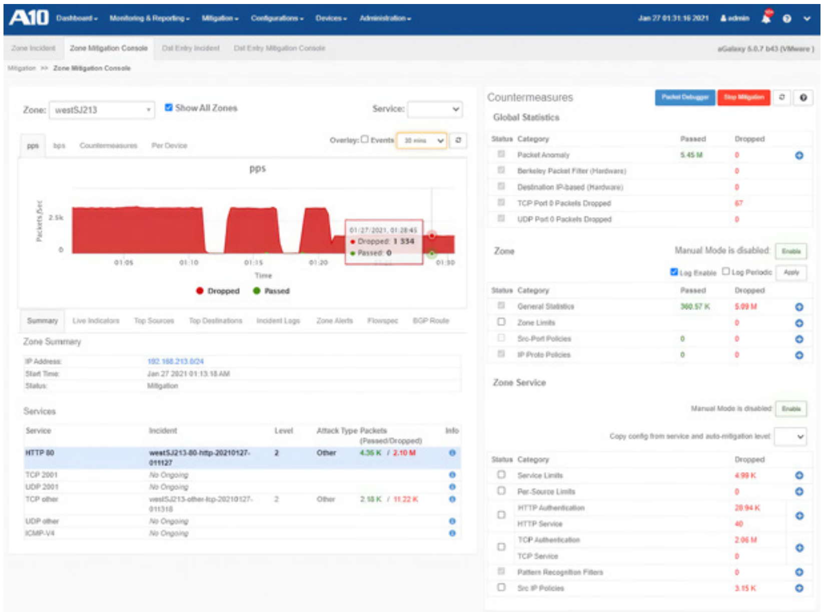
A10 Defend Orchestrator collects all the required data from the managed A10 Defend Detector and Mitigator devices to generate simple-to-read incident reports that can be exported in PDF or CSV formats, and emailed immediately or scheduled at recurring intervals or as one-time notifications. Once a DDoS attack incident is over, a detailed incident report with a rich set of telemetry, counters, graphs, and event logs is automatically generated and can be shared with all stakeholders via email.



Auto start mitigation - zone westSJ213 in response to incident westSJ213-80-http-20210127-006850

A10 Defend Orchestrator Dashboard

The DDoS defense-oriented dashboard provides real-time suspicious traffic statistics and a variety of summaries of DDoS incidents that enable organizations to track security events, identify attack trends and address compliance risk.



Zone: westSJ213 ☑ Show All Zones Service:

Overlay: □ Events 30 mins

Zone Summary

IP Address:	192.168.213.0/24
Start Time:	Jan 27 2021 01:13:18 AM
Status:	Mitigation

Services

Service	Incident	Level	Attack Type	Packets (Passed/Dropped)	Info
HTTP 80	westSJ213-80-http-20210127-011127	2	Other	4.36 K / 2.10 M	●
TCP 2001	*No Ongoing*				●
UDP 2001	*No Ongoing*				●
TCP other	westSJ213-other-tcp-20210127-011318	2	Other	2.18 K / 11.22 K	●
UDP other	*No Ongoing*				●
ICMP-V4	*No Ongoing*				●

Countermeasures

Global Statistics

Status	Category	Passed	Dropped
☑	Packet Anomaly	5.45 M	0
☑	Berkeley Packet Filter (Hardware)		0
☑	Destination IP-based (Hardware)		0
☑	TCP Port 0 Packets Dropped		67
☑	UDP Port 0 Packets Dropped		0

Zone

Manual Mode is disabled: Enable

☑ Log Enable □ Log Periodic Apply

Status	Category	Passed	Dropped
☑	General Statistics	360.57 K	5.09 M
□	Zone Limits		0
□	Src-Port Policies	0	0
☑	IP Proto Policies	0	0

Zone Service

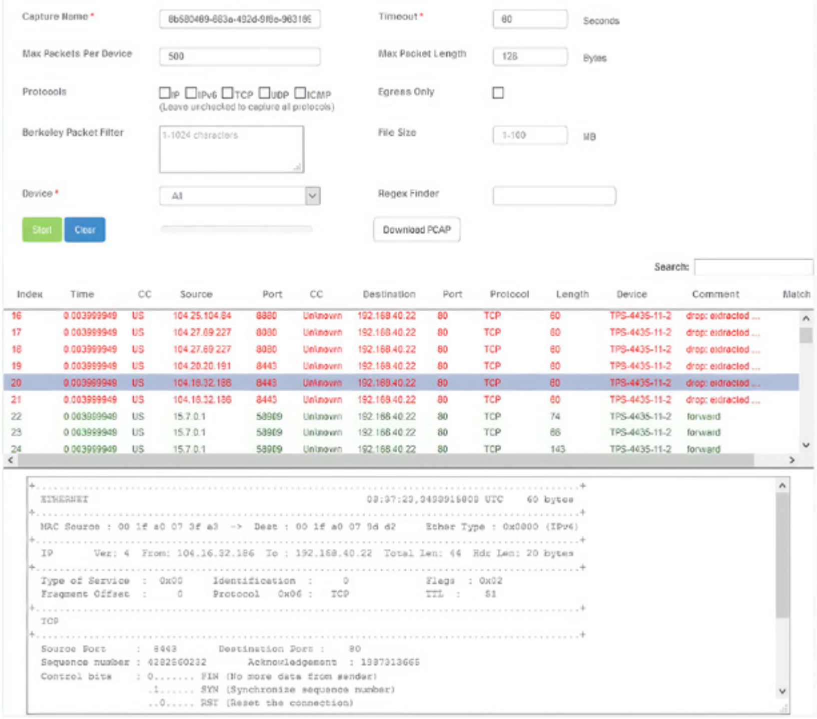
Manual Mode is disabled: Enable

Copy config from service and auto-mitigation level:

Status	Category	Dropped
□	Service Limits	4.99 K
□	Per-Source Limits	0
□	HTTP Authentication	28.94 K
	HTTP Service	40
□	TCP Authentication	2.06 M
	TCP Service	0
☑	Pattern Recognition Filters	0
□	Src IP Policies	3.15 K

Real-time DDoS Mitigation Console

From the mitigation console, security operators can view a live dashboard of attacks, check mitigation status, and instantly apply any advanced countermeasures when needed. The mitigation console offers real-time statistics and incident details including mitigation escalation levels, top-k information, and activity logs.



Capture Name *	8b580489-883a-492d-9f8e-983189	Timeout *	80	Seconds
Max Packets Per Device	500	Max Packet Length	128	Bytes
Protocols	□IP □IPv6 □TCP □UDP □ICMP (Leave unchecked to capture all protocols)	Egress Only	□	
Berkeley Packet Filter	1-1024 characters	File Size	1-100	MB
Device *	All	Regex Finder		

Index	Time	CC	Source	Port	CC	Destination	Port	Protocol	Length	Device	Comment	Match
16	0.003999949	US	104.25.104.84	8880	Unknown	192.168.40.22	80	TCP	60	TPS-4435-11-2	drop: extracted ...	
17	0.003999949	US	104.27.69.227	8080	Unknown	192.168.40.22	80	TCP	60	TPS-4435-11-2	drop: extracted ...	
18	0.003999949	US	104.27.69.227	8080	Unknown	192.168.40.22	80	TCP	60	TPS-4435-11-2	drop: extracted ...	
19	0.003999949	US	104.20.20.191	8443	Unknown	192.168.40.22	80	TCP	60	TPS-4435-11-2	drop: extracted ...	
20	0.003999949	US	104.16.32.186	8443	Unknown	192.168.40.22	80	TCP	60	TPS-4435-11-2	drop: extracted ...	
21	0.003999949	US	104.16.32.186	8443	Unknown	192.168.40.22	80	TCP	60	TPS-4435-11-2	drop: extracted ...	
22	0.003999949	US	15.7.0.1	58909	Unknown	192.168.40.22	80	TCP	74	TPS-4435-11-2	forward	
23	0.003999949	US	15.7.0.1	58909	Unknown	192.168.40.22	80	TCP	66	TPS-4435-11-2	forward	
24	0.003999949	US	15.7.0.1	58909	Unknown	192.168.40.22	80	TCP	143	TPS-4435-11-2	forward	

```
+.....................................................................+
 ETHERNET                                09:37:23,0499915008 UTC    60 bytes
+.....................................................................+
 MAC Source : 00 1f a0 07 3f a3  ->  Dest : 00 1f a0 07 9d d2     Ether Type : 0x0800 (IPv4)
+.....................................................................+
 IP       Ver: 4  From: 104.16.32.186  To : 192.168.40.22  Total Len: 44  Hdr Len: 20 bytes
+.....................................................................+
 Type of Service  :  0x00     Identification  :      0              Flags  : 0x02
 Fragment Offset  :     0     Protocol   0x06 :   TCP               TTL  :    51
+.....................................................................+
 TCP
+.....................................................................+
 Source Port      :  8443       Destination Port :     80
 Sequence number : 4282560232        Acknowledgement  : 1987313665
 Control bits     : 0....... FIN (No more data from sender)
                    .1...... SYN (Synchronize sequence number)
                    ..0..... RST (Reset the connection)
```

Remote Packet Capture and Debugger Tool

In order to help further incident investigation after or during the attack, A10 Defend Orchestrator enables packet capture and debugger remotely which helps create custom countermeasures or filters, as needed.

A10 Defend Orchestrator Specifications

A10 Defend Orchestrator Virtual Appliance	
Supported Hypervisors	VMware ESXi, KVM QEMU
Hardware Requirements	See installation guide
Standard Warranty	90-day software

Virtual Appliance Sizing Recommendations

Deployment Scale	100 zones/1,000 services	1,000 zones/8,000 services	3,000 zones/15,000 services
vCPU	8	12	16
vRAM	24 GB	40 GB	96 GB
vDisk	500 GB	1 TB	1.5 TB

Detailed Feature List

Simplified DDoS Defense Management

- Central DDoS defense operation console for provisioning, wartime operation and incident reporting
- Centralized management for A10 Defend Detector and Mitigator appliances
- Real-time DDoS protection dashboard and console
- Centralized management for configuration, backup, restore, upgrade image repository
- Centralized device management for reboot, shutdown, and upgrade
- Health monitoring for managed devices
- Predefined mitigation policies and configuration profiles in customizable template
- Remote packet capture and debugger during wartime
- Searchable managed devices and A10 Defend Orchestrator audit logs
- On-box management GUI
- REST API (aGAPI)

Event Management and Reporting

- Attack visualization and geolocation tracking
- Dashboard provides continuous monitoring of most attacked services
- Data consolidation across multiple appliances into real-time dashboard
- Wartime real-time mitigation console
- Fully automated attack detection and mitigation with minimal operator intervention
- Customizable event alerts/alarms
- Centralized packet capture from all managed A10 Defend Mitigators
- On-demand and scheduled reports
- Automatic DDoS incident report via email

Access Management

- Role-based access control management
- External authentication that supports RADIUS and TACACS+

* Features may vary by licensed options.
Options include base device management and A10 Defend (previously Thunder TPS) device management pack.

Learn More

About A10 Networks

Contact Us

A10networks.com/contact

Part Number: A10-DS-15137-EN-01 Feb 2024