DATA SHEET

aGALAXY FOR THUNDER TPS

DDOS DEFENSE MONITORING, OCHESTRATION AND MANAGEMENT

The A10 aGalaxy® management system integrates with One-DDoS Protection detectors and Thunder TPS® (Threat Protection System) for effective automated DDoS protection. Centralize management, ochestration, monitoring, alerting, reporting and detecting of global DDoS attacks and defenses.

REAL-TIME GLOBAL DDOS DEFENSE MANAGEMENT

A10's DDoS detection and mitigation solutions empower enterprises and service providers to surgically distinguish DDoS attackers from valid users. The solution's industry-leading scalability ensures an organization's frontline security personnel are more effective with optimized wartime workflows.

A10 Networks aGalaxy for Thunder TPS enables organizations to gain a global view of their environments to rapidly identify and remediate attacks, and ensure that policies are consistently enforced from a central point.

Administrators can configure, monitor and comprehensively analyze their Thunder TPS and One-DDoS detector deployments to view DDoS attacks in real time, and drill down to see the details of connections handled by an individual protected service.

aGalaxy scales to manage multiple Thunder TPS deployments — across geographic locations — to streamline operations and lower IT operating costs.

aGalaxy is available with an optional integrated Thunder TPS detector module that supports tightly integrated interworking of Thunder TPS DDoS mitigation, flow-based DDoS detection, system-wide management and robust reporting.

PLATFORMS

aGALAXY
Physical Appliance

aGALAXY
Virtual Appliance

SOLUTIONS

THUNDER TPS
Physical Appliance

vTHUNDER TPS
Virtual Appliance

Thunder ADC, CGN, CFW Integrated One-DDoS detector

TALK WITH A10

WEB
a10networks.com/aGalaxy

CONTACT US
a10networks.com/contact

BENEFITS

STOP DDOS ATTACKS
WITH SURGICAL PRECISION

Security administrators have unique challenges. They must swiftly detect and mitigate DDoS attacks to prevent downtime — often in diverse geographic locations.

The aGalaxy centralized management system aggregates data from all managed Thunder TPS deployments, providing a rich set of telemetry data to monitor and defeat DDoS attacks.

From the aGalaxy mitigation console, security administrators can view a live dashboard of attacks and apply all the advanced Thunder TPS features through mitigation templates or create custom countermeasures instantly.

With a myriad of policies and thresholds at their fingertips, administrators can granularly regulate traffic and block suspicious activity. Within seconds of applying policies, verify whether policies mitigated the attack and adjust countermeasures, as needed.

DDOS DEFENSE MANAGEMENT

- Lower operating costs by consolidating management tasks
- Monitor incidents in real time through a live dashboard
- Receive consolidated DDoS incident alerts and mitigate attacks rapidly
- Scale to manage multiple Thunder TPS appliances

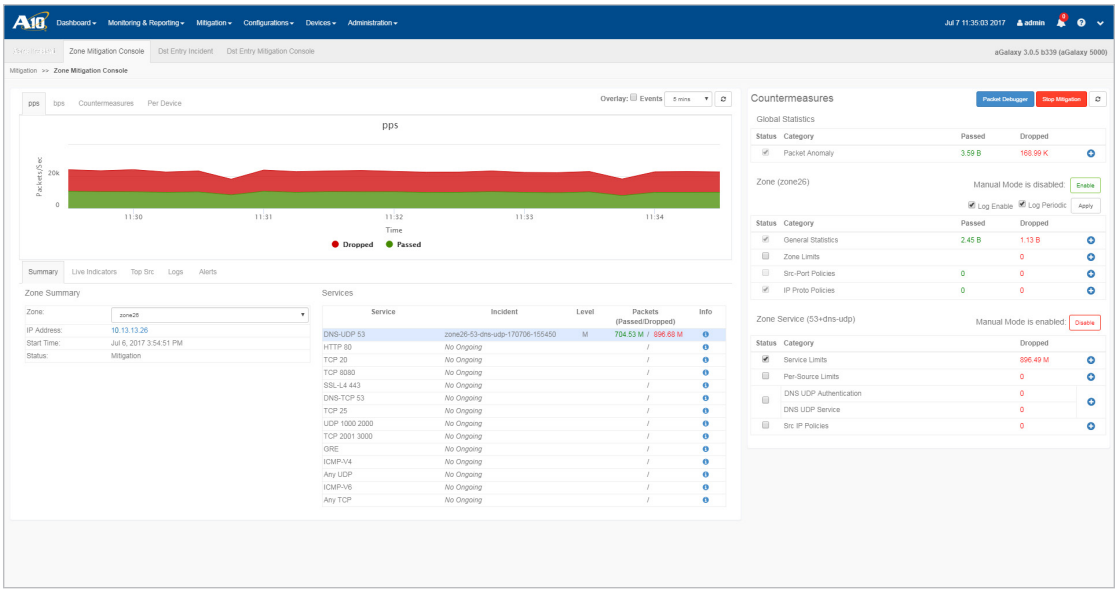


Figure 1: View network activity, apply surgical mitigation policies and quickly verify whether policies have neutralized a DDoS attack.

SIMPLIFY MANAGEMENT

OF THUNDER TPS

Managing multiple appliances can be challenging. A10 streamlines device management, even for organizations with multiple Thunder TPS appliances. Upgrade software, manage SSL certificates, and backup and restore configuration files for all of your appliances. aGalaxy consolidates all management tasks in one location, making it easy for administrators to apply consistent policies across all devices.

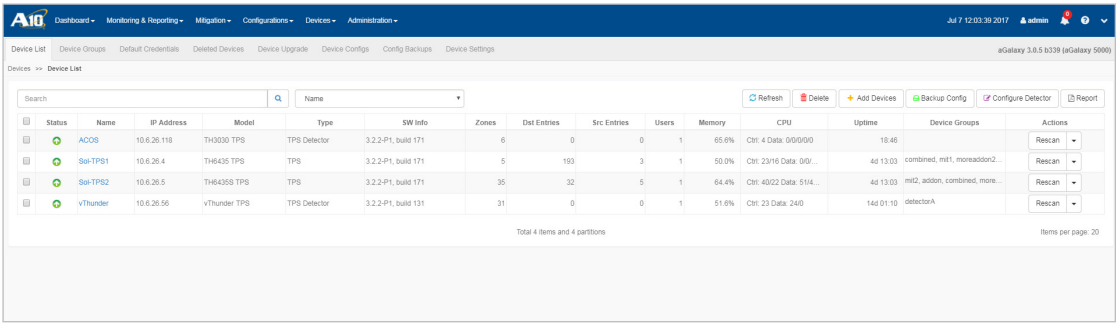


Figure 2: View all devices under management and backup configuration settings via the aGalaxy management system.

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. aGalaxy makes it easy to assess the environment and push policies to multiple Thunder TPS appliances at once from the graphical user interface or over the aGAPI REST API.

REPORT ON ATTACKS

AND NETWORK ACTIVITY

aGalaxy offers a variety of summaries, detailed incident reports and real-time dashboards that enable organizations to track security events, identify attack trends and address compliance risk. aGalaxy provides a rich set of reports that illustrate overall traffic and blocked attacks by protocol. All reports can be exported, viewed, emailed or printed (e.g., PDF), enabling all stakeholders to analyze security events.

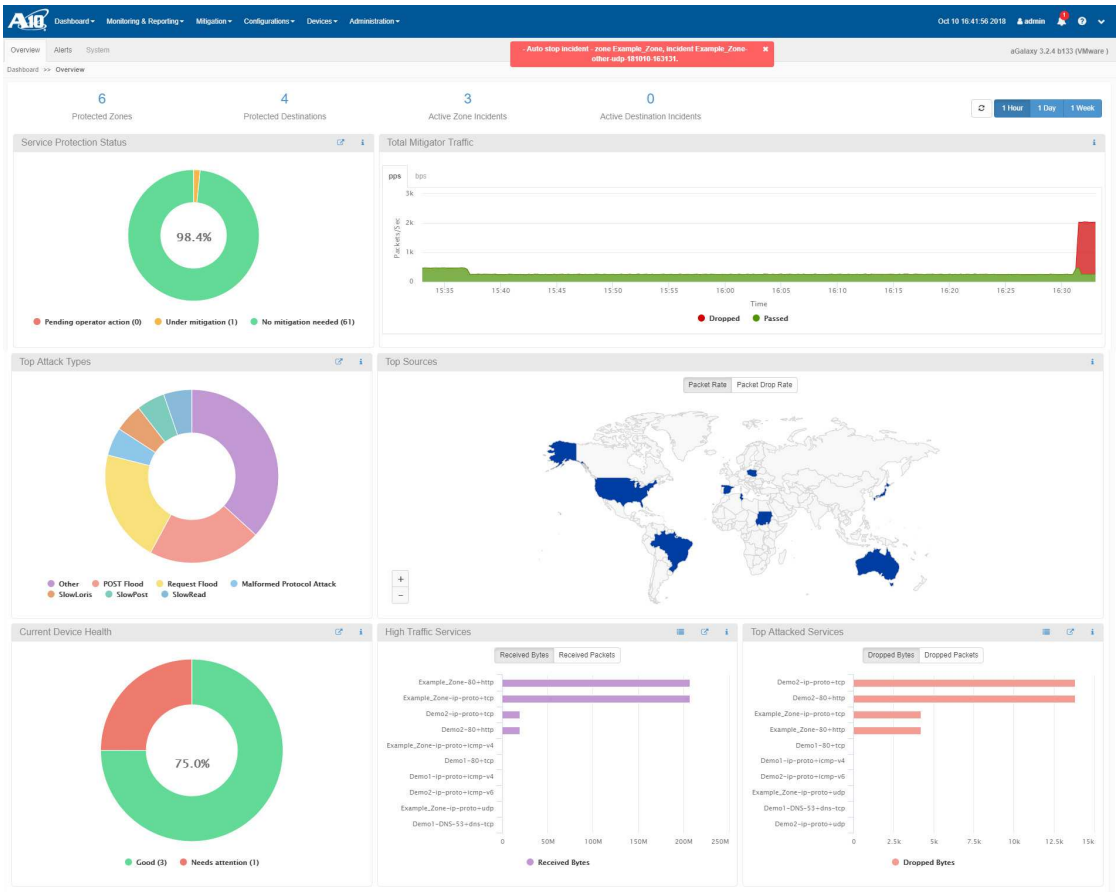
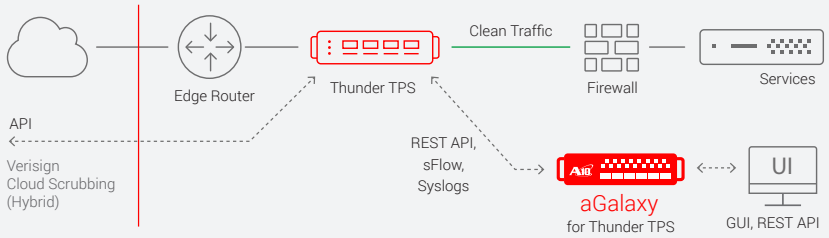


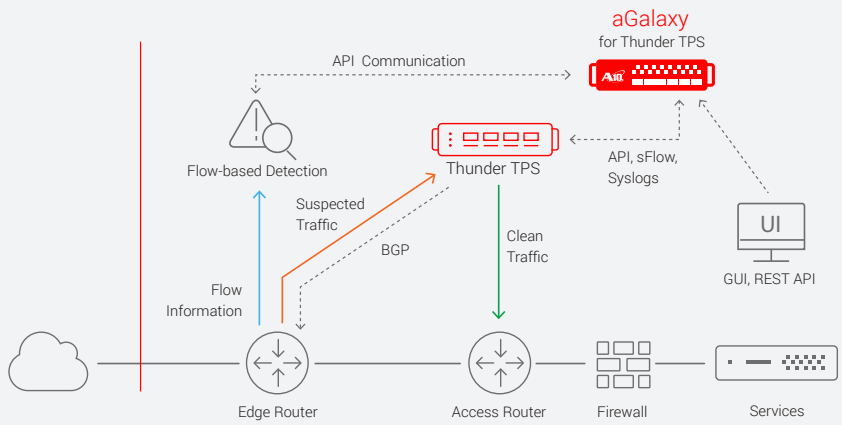
Figure 3: Intuitive dashboards deliver network activity, reporting and blocked attacks over time.

REFERENCE ARCHITECTURES



PROACTIVE DEPLOYMENT
(ASYMMETRIC OR SYMMETRIC)

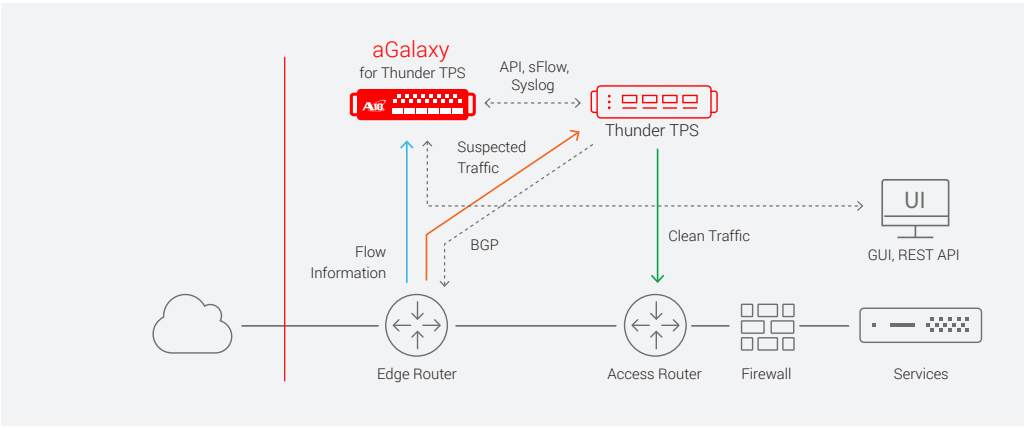
aGalaxy provides full management controls over multiple Thunder TPS deployed in proactive mode. Proactive mode provides continuous, comprehensive detection and faster mitigation. This mode is most useful for real-time environments where the user experience is critical. Thunder TPS supports L2 or L3 inpath deployments.



REACTIVE DEPLOYMENT

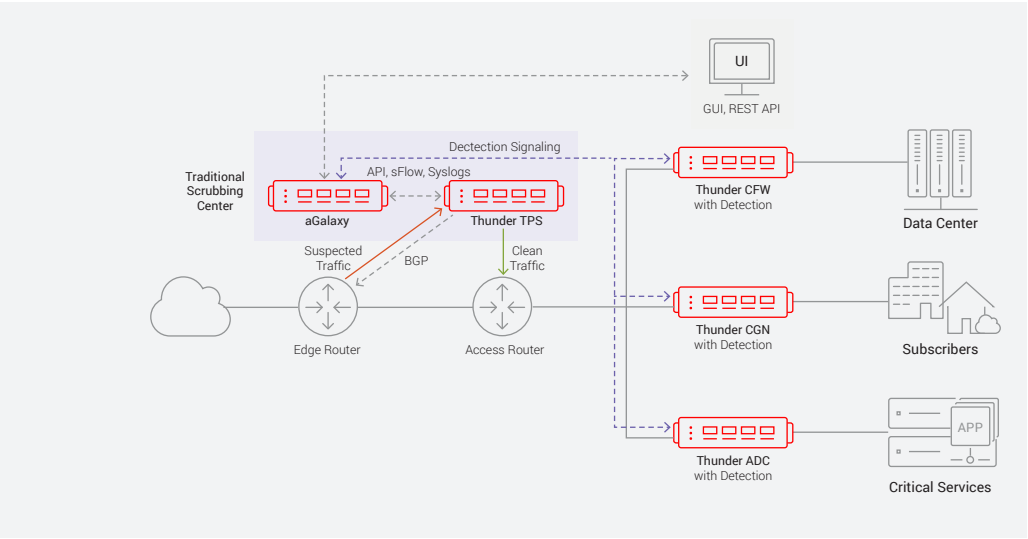
Larger networks benefit from on-demand mitigation, triggered manually or by flow analytical systems. aGalaxy orchestrates globally deployed Thunder TPS that fit any network configurations with integrated BGP and other routing protocols. This eliminates the need for any additional diversion and re-injection routers. A10's open API integrates seamlessly with third-party detection solutions.

REFERENCE ARCHITECTURES



REACTIVE DEPLOYMENT WITH INTEGRATED DDOS DETECTOR

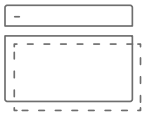
aGalaxy is optionally available with an integrated flow-based DDoS detector module to support tightly integrated interworking for reactive deployments.



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.

FEATURES



SINGLE PANE OF GLASS

MANAGEMENT

Featuring an intuitive interface, the aGalaxy centralized management system is a robust network monitoring and management solution that performs and automates a variety of essential tasks. Run health checks, modify configurations, backup, update, apply mitigation templates and generate reports across all managed Thunder TPS appliances.

ROBUST REPORTING

aGalaxy collects all the required data from the managed Thunder TPS devices to create simple-to-read reports that can be saved in PDF or CSV formats, which can be emailed immediately or scheduled at recurring intervals or one-time notifications.

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 aGalaxy centralized mitigation to enable full spectrum DDoS resilience.

REAL-TIME DASHBOARDS

Easy-to-follow dashboards help administrators monitor system health, respond to alerts and view active incidents against protected objects and zone services.

AUTOMATION AND INTEGRATION

aGalaxy integrates with third-party DDoS detection systems that 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 administrators to directly mitigate an attack based on incident data.

INTEGRATED

FLOW-BASED DDOS DETECTOR

(available on specific models)

Reactive DDoS detection is facilitated through the collection and analysis of exported flow data records from routers and switches for IPv4 and IPv6 traffic. The flow-based DDoS detector module enters traffic behavioral-learning mode to build a peacetime profile for protected zones. Once in monitoring mode, the flow-based detector tracks up to 17 flow data traffic indictors to spot anomalous behavior for inbound or bi-directional traffic.

When an attack is detected, the flow-based DDoS detector alerts aGalaxy to instruct Thunder TPS to apply appropriate mitigation templates and initiate a BGP route change of the suspicious traffic for DDoS scrubbing before delivering the clean traffic to the intended destination.

aGALAXY PHYSICAL APPLIANCE

aGALAXY 5000 CENTRALIZED MANAGEMENT SYSTEM

Recommended Devices Managed	20 Thunder TPS Devices
Network Interfaces	4x 1GE Copper + 4x 10GE SFP+, Management , Console
Processor	2 x Intel Xeon 10-core
Memory	128 GB ECC RAM
ACOS Versions Supported	Thunder TPS: 3.2.2 or Higher
Supported Browser	Internet Explorer 8.x and Firefox 9.x or Above
Dimensions	3.5 in (H), 17.5 in (W), 25.0 in (D)
Rack Units (Mountable)	2U
Operating Ranges	Temperature 0° - 40° C | Humidity 5% - 95%
Standard Warranty	90-Day Software or Hardware Warranty
Regulatory Certifications	FCC Class A, UL, CE, TUV, CB, VCCI | RoHS

aGALAXY VIRTUAL APPLIANCE

aGALAXY CENTRALIZED MANAGEMENT SYSTEM

Recommended Devices	20 Thunder TPS Devices
Supported Hypervisor	VMware ESXi 5.0 or Higher KVM version 0.14 (qemu-kvm-0.14.0) or Higher
Hardware Requirements	See Installation Guide
Standard Warranty	90-Day Software

FLOW-BASED DETECTION SYSTEM

Max Flow Analysis Capabilities	500K Flows Per Second
Max Thunder TPS Managed	4
Max Protected Zones	250

Flow-Based Detection is an optional configuration shipped with specific aGalaxy hardware appliance.

DETAILED FEATURE LIST

Simplified Thunder TPS Device Management

- Wizard-based system configuration
- Real-time and centralized management
- Configuration, backup and restore
- Uptime status
- Centralized management for managed device upgrades and image upgrade repository
- Reboot and shutdown features for managed devices
- Managed Thunder TPS health monitoring
- Configuration deployment and comparison
- Centralized sFlow collector
- Searchable managed devices and aGalaxy audit logs
- On-box management GUI
- aGAPI REST API

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 Thunder TPS
- On-demand and scheduled reports
- Automatic DDoS incident report via e-mail

Flow-based DDoS Detector

(available on specific models)

- Supports sFlow, NetFlow v5/v9, IPFIX/NetFlow v10
- Capable of profiling and detecting attacks in IPv4/IPv6 traffic
- Always-on adaptive peacetime learning
- Tracks 17 behavioral indicators to detect DDoS attacks
- Capable of identifying anomalies in bi-directional traffic
- Fast three-second detection time
- aGalaxy configuration controls

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 Thunder TPS device management pack.

LEARN MORE

ABOUT A10 NETWORKS

CONTACT US

a10networks.com/contact

©2018 A10 Networks, Inc. All rights reserved. A10 Networks, the A10 Networks logo, ACOS, Thunder and SSL Insight are trademarks or registered trademarks of A10 Networks, Inc. in the United States and other countries. All other trademarks are property of their respective owners. A10 Networks assumes no responsibility for any inaccuracies in this document. A10 Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice. For the full list of trademarks, visit: www.a10networks.com/a10-trademarks.

Part Number: A10-DS-15125-EN-02 OCT 2018