A10

Building Profitable DDoS Scrubbing Services

Scale, Automation, and Flexibility that Drive Profits

Overview

The scourge of DDoS attacks affects every category of communications service providers and data center/colocation providers. Your response to this growing menace can be an opportunity to increase stickiness with your customers, as well as a source of profits.

To build effective and profitable scrubbing services, you need a DDoS defense platform that can scale to protect thousands of customers with individual protection policies and advanced automation that can be managed by your already oversubscribed staff.

The Challenge

Colocation, data center and other service providers are finding that the strategies that worked for protecting their own infrastructures may not meet the challenges of scaling protection policies per customer or deliver the responsiveness that businesses demand.

The A10 Networks DDoS Scrubbing Service Solution

A10's DDoS defense solutions are built for performance and scale. The solution is ideally suited for DDoS scrubbing services with the ability to protect thousands of customers with individual protection policies. Unlike legacy products, the A10 solution is powered by intelligent automation that offers a policy-based, automated defense that is required for multi-tenant environments.

Challenge

Building and operating profitable DDoS scrubbing services that can scale with a small staff presents many challenges to internet, mobile, cloud, data center, colocation and web hosting service providers.

Solution

A10's DDoS defense solutions scale to hundreds of thousands of protected services with individual protection policies that drive profits and instill customer loyalty. Our solution is powered by intelligent automation to speed up response and make your staff and operations more effective.

Benefits

- Increase your profits by scaling your DDoS scrubbing services to thousands of protected customers
- Speed response time with a policy-based fully automated defense
- Provide differentiated services to match the demands of each customer's needs

The A10 solutions enables data center providers to

- serve thousands of customers with their own protection policies
- minimize hiring additional staff with intelligent automated defenses
- offer differentiated services to meet customer's budget and risk tolerance.

Features and Benefits

Scale for Profits

The number of paying customers drives the top line profits of the DDoS scrubbing service. However, each customer in the scrubbing service has unique network and application characteristics that require custom defense policies. A10's solutions automatically discover peacetime profiles and set policies for more han 256K servers and services per detector appliance. When an attack is detected, Thunder TPS is able to mitigate up to 3,000 protected zones simultaneously on a single appliance.

Intelligent Automation

DDoS attackers have evolved and now use multi-vector attack techniques tuned for their victims. Multiply this by tens, hundreds or thousands of simultaneous attacks against your customers and the result is chaos. The A10 defenses are fully automated solutions that leverage machine learning with intelligent automation of protection workflow to stop such DDoS attacks with no manual intervention.

- **Always-on adaptive learning** - Continuous machine learning provides real-time adaptive traffic learning versus limited peacetime, operator-initiated learning.
- **Progressive automatic five-level mitigation escalation** - Apply the right level of mitigation to prevents collateral damage against legitimate users.
- **Dynamic Zero-day Attack Pattern Recognition (ZAPR)** - ML/AI based attack learning, to identify and thwart zero-day attacks.
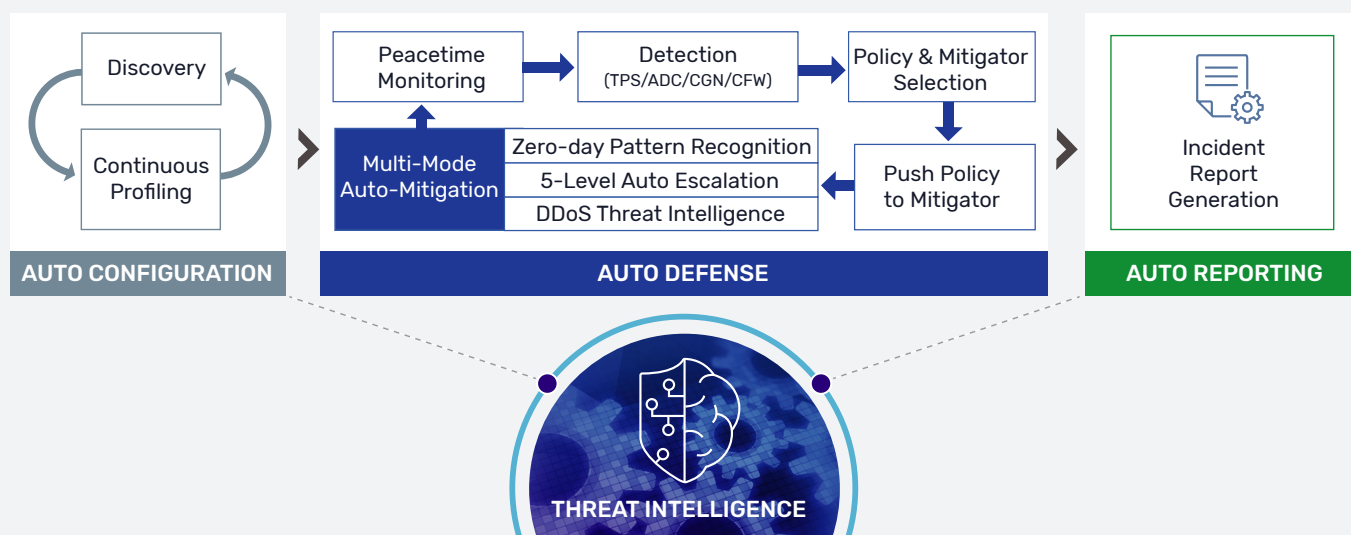

Figure 1: Full protection lifecycle intelligent automation capabilities

Differentiated Services

Each scrubbing service customer has different budgets and acceptable exposure criteria that drive their decisions. To satisfy every customer's needs, the scrubbing service operator must provide differentiated services at varying subscription levels. A10 solutions provides the protection scaling and operational flexibility to support differentiated services.

Type of Service	Orchestration and Data Path	Customer Cost
Basic service	Volumetric defense, no policy	No cost, best effort
On-demand	Manual reactive protection with predefined mitigation policies	$
Monitored with automatic mitigation	Automated reactive protection with predefined detection and mitigation policies	$$
Always-on	Proactive protection for fast full-spectrum protection	$$$

Solution Components

How it Works

A10 DDoS defenses are comprised by these key components: Thunder TPS, Thunder TPS detector, and aGalaxy® Centralized Management System. These components can be deployed modularly to scale to meet the demands of any network environment, including large, complex service provider networks.

Thunder TPS Detector

- High precision flow-based DDoS detector for network wide protection
- Continuous peacetime learning
- Up to 6M fps flow-based detection

One-DDoS Protection Distributed Detector

- High precision packet-based detection distributed closest to targeted infrastructure
- Integrated on Thunder CFW
- Attack detection signaling to aGalaxy for intelligent automation

Thunder TPS

- Flexible proactive or reactive deployment with integrated BGP, OSPF, IS-IS protocols
- Industry's only 5-level adaptive policy escalation that minimizes damage
- Machine learning powered zero-day attack protection
- Precise traffic control with fast 100ms mitigation interval and per-source based rate control

aGalaxy

- Managed and automated orchestration across the full attack lifecycle
- Simple, unified dashboard and reporting
- DDoS defense focused workflow

The ability to automate and scale the delivery of differentiated services could have a major impact on the quality and economics of DDoS scrubbing services.

— Bart van der Sloot, Managing Director of Leaseweb Network

Summary

DDoS Scrubbing Solutions that Drive Profits and Instill Customer Loyalty

Delight your customers with an effective scrubbing service that is powered by a DDoS protection platform that enables you to scale profits and has low operating costs.

Thunder TPS is powered by intelligent automation that scales to match each of your customers unique security and budget needs.

A10 provides 24x7x365 support and includes the A10 DDoS Security Incident Response Team (DSIRT) to help you analyze and respond to DDoS incidents and attacks. The A10 Threat Intelligence Service leverages global knowledge to proactively stop known bad actors.

Next Steps

For more information, visit: a10networks.com/TPS

About A10 Networks

A10 Networks (NYSE: ATEN) provides secure application services for on-premises, multi-cloud and edge-cloud environments at hyperscale. Our mission is to enable service providers and enterprises to deliver business-critical applications that are secure, available and efficient for multi-cloud transformation and 5G readiness. We deliver better business outcomes that support investment protection, new business models and help future-proof infrastructures, empowering our customers to provide the most secure and available digital experience. Founded in 2004, A10 Networks is based in San Jose, Calif. and serves customers globally. For more information, visit A10networks.com and follow us @A10Networks.

Learn More
About A10 Networks

Contact Us
A10networks.com/contact