SOLUTION BRIEF

ONE-DDOS PROTECTION

FULL-SPECTRUM DDOS PROTECTION FOR FLEXIBLE REACTIVE DEPLOYMENT WITH LAYERED DISTRIBUTED DETECTION

Service providers need to protect their infrastructures and subscribers against today's colossal DDoS attacks. Modern attacks exploit vulnerabilities in IoT devices, so they can scale to a magnitude legacy systems simply can't match. Older systems, many of which are still marketed today, can't discern between a legitimate user and a bot—bots have become too sophisticated to be detected by systems that weren't purpose-built to recognize them.

To protect assets and customers, service providers need a DDoS defense that's effective, scalable, and affordable. A10 One-DDoS Protection provides the freshest approach to full spectrum DDoS defense, placing layered distributed detection closer to the targeted elements of the infrastructure. This provides the context and visibility needed to thwart today's sophisticated targeted attacks. This matters to service providers as they monetize infrastructure investments with services that rely on compelling applications and clean pipe services to appeal to subscribers.

Service Providers' Legacy DDoS Defense Challenges

CHALLENGE

Building defenses that scale to thwart all categories of attacks against the infrastructure, critical application services, and downstream business customers is challenging.

SOLUTION

A10 Networks' comprehensive strategy applies layered distributed detection capabilities across key networks elements. A10's Thunder ADC, CGN, and CFW work in concert with Thunder TPS' edge flow-based detection and centralized mitigation to enable service providers to achieve full spectrum DDoS resilience.

BENEFITS

- Full-spectrum protection against multi-vector attacks
- Machine learning enhances DDoS detection and defense effectiveness
- Intelligent automation speeds detection and response times
- Individual policies for clean pipe services protect elements at scale
- The industry's highest-performance flow-based detection and mitigation appliances reduce complexity

THE CHALLENGE

Traditional edge flow-based detection with centralized scrubbing pools is effective against volumetric attacks but leaves network elements and business-critical applications exposed to targeted attacks. Since legacy solutions don't provide visibility into all attack types, service providers are blindsided when an attack occurs.

In many service provider environments, hundreds of thousands of individual policies are needed to achieve full-spectrum DDoS resilience over sprawling infrastructures and to provide business subscribers with clean pipe services in a profitable manner. Legacy defenses don't scale to support these requirements without consuming racks and racks of datacenter space.

THE A10 NETWORKS SOLUTION

A10 One-DDoS Protection includes the industry's highest performance detection and mitigation appliances, providing a layered approach for full-spectrum volumetric, network and application DDoS protection. The Thunder ADC, CGN, and CFW product lines offer detection-in-depth works in concert with Thunder TPS to provide automated mitigation.

A10 Networks One-DDoS Protection utilizes machine learning to automate the challenges of protected service discovery, peacetime traffic learning, detection threshold setting, and fast mitigation response.

These capabilities give service providers a cost-effective reactive DDoS defense topology with flow-based detection at the edge of the network. High resolution packet-based detection is enabled closer to the targeted critical services and applications where Thunder ADC, CFW or CGN are placed. This allows context to be applied, so service providers can thwart sophisticated network and application assaults against critical applications and services.

Distributed detection helps organizations achieve the common goal of protecting services while overcoming organizational silo ownership issues. For example, application teams and CGN teams can provision and manage server load balancing and CGNAT systems as usual without needing any training on DDoS attacks or mitigation procedures. A10 One-DDoS Protection works transparently in the background, so when DDoS attacks are identified signals are automatically enabled and DDoS defenses are intelligently evoked. The DDoS defense system and protection policies remain under the ownership of the security team, where the required DDoS expertise already reside.

A10 One-DDoS Protection Capabilities

Modern Approach to Service Provider DDoS Defenses

Layered, detection-in-depth

- Full spectrum protection
- Cost effective reactive mode

Intelligent automation with machine learning

- Auto discover, learn, detect, respond

Scales to 100Ks of protected entities with individual policies

- Scale profitable clean pipe services

Overcomes organizational silo ownership issues

- Leverage common resources and talents

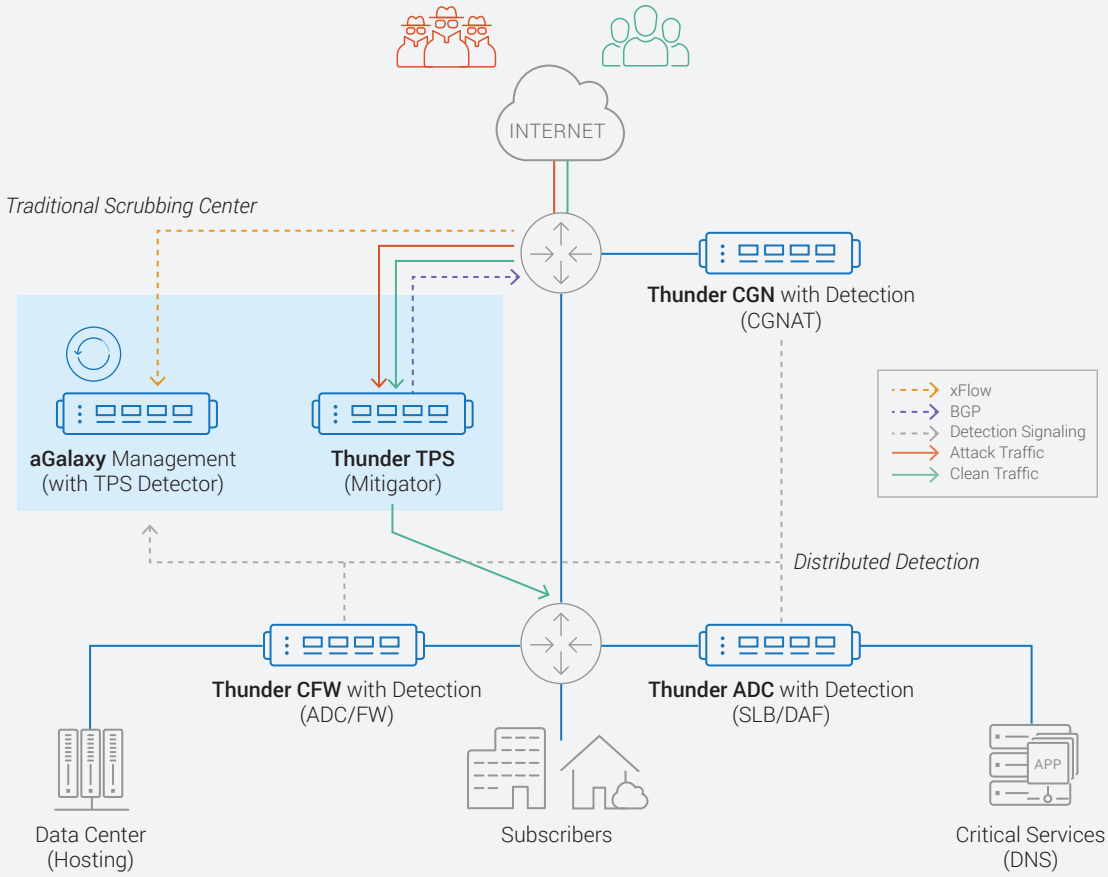

Figure 1: Layered full spectrum DDoS protection

SOLUTION COMPONENTS

One-DDoS Protection protects against attacks by integrating detection and intelligent automation across a hierarchy of A10 Networks solutions with centralized orchestrated reactive scrubbing

- Thunder TPS Detector
- Thunder ADC
- Thunder CFW
- Thunder CGN
- Thunder TPS
- aGalaxy TPS

FEATURES AND BENEFITS

DISTRIBUTED DETECTION WITH COST-EFFECTIVE CENTRALIZED SCRUBBING POOLS

Reactive deployments provide easy integration into existing environments and cost effective oversubscribed shared mitigation pools that are non-intrusive at peacetime. Layered detection in A10's network elements adds packet-based precision to defend against devastating network and application layer attacks close to targeted infrastructure.

INTELLIGENT AUTOMATION THROUGH MACHINE LEARNING

A10 Networks One-DDoS Protection utilizes machine learning to automatically learn about and understand downstream infrastructure and services. This speeds detection and response times by eliminating slow, labor-intensive manual interventions. The result is a highly scalable, cost-effective model for serving subscribers.

SCALES TO 100KS OF PROTECTED ENTITIES WITH INDIVIDUAL POLICIES

Clean pipe DDoS defenses for business subscribers have become an important revenue stream for service providers. These services require granular controls for each individual subscriber and must scale to tens of thousands or even millions of businesses. Legacy systems require service providers to purchase expensive and complicated arrays of appliances. A10 Networks solutions scale to hundreds of thousands of monitored entities with a single appliance straight out of the box.

SUMMARY

ONE-DDOS PROTECTION THWARTS MULTI-VECTOR DDOS ATTACKS

Up till recently, DDoS attacks have targeted service providers and their subscribers with request floods that bombard and overwhelm infrastructure. Now, targeted attacks against the network or application layer are on the rise. These sophisticated tactics are generally not detected until well into the attack progression, so threat actors have a better chance of blocking availability or even completing a data breach. Service providers can achieve full DDoS resilience and improve security by using a layered approach for detecting and mitigating attacks of all types and sizes before attackers take down their targets.

NEXT STEPS

For more information, please contact your A10 representative and visit: a10networks.com/TPS

ABOUT A10 NETWORKS

A10 Networks (NYSE: ATEN) provides Reliable Security Always™ through a range of high-performance solutions that enable intelligent automation with deep machine learning to ensure business critical applications are protected, reliable and always available. Founded in 2004, A10 Networks is based in San Jose, Calif., and serves customers globally with offices worldwide.

For more information, visit: a10networks.com or tweet @a10Networks

LEARN MORE

ABOUT A10 NETWORKS

CONTACT US

a10networks.com/contact

Part Number: A10-SB-19190-EN-01 APR 2018