SOLUTION BRIEF

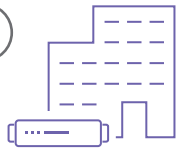
ENSURE ENTERPRISE DDOS RESILIENCE

TWO-PRONGED DDOS DEFENSE FOR COMPLETE ATTACK COVERAGE

The focus of enterprise DDoS defense should always be on users. After all, they drive your business and create value for your company. When services are blocked or down, users don't care why. They're not concerned with what DDoS strategies attackers take. Without access to critical services, workers opt to go home or use unsecured methods. Worse yet, customers get frustrated and go elsewhere.

Full-coverage DDoS defense ensures uninterrupted service availability. Without it, you're left with lost revenue, brand damage and unproductive workers.

For true DDoS resilience, enterprises require a two-pronged DDoS defense approach:

1. 

   Deploy A10 Networks' always-on, proactive, on-premise A10 Thunder TPS® to surgically detect and mitigate all types of DDoS attacks at your network edge

2. 

   Gain the benefits of cloud scrubbing for volumetric attacks that go beyond your internet pipe's capacity

CHALLENGE

The frequency, intensity and sophistication of DDoS attacks threaten the most important thing to an enterprise: 24/7 availability. Enterprises need comprehensive, cost-effective defense to ensure services are available and users are protected.

SOLUTION

A10 DDoS defense offers a combination of a surgically precise on-premises appliance with on-demand cloud scrubbing to ensure enterprises are resilient against crushing volumetric, network protocol and application layer DDoS attacks.

BENEFITS

- The most cost-effective approach to full spectrum DDoS resilience
- Precise on-premise detection and mitigation minimizes false events and protects legitimate users
- Orchestrated cloud escalation
- Scalability to defend the most challenging enterprise environments

CLOUD VS. ON-PREMISE OR CLOUD WITH ON-PREMISE

Cloud scrubbing is an important part of enterprise DDoS defense when attack volume grows beyond the capacity of a business' internet pipes. But cloud scrubbing is not a panacea. Cloud only scrubbing has inherent limitations due to how it works, diminishing its effectiveness.

Enterprises need to complement cloud solutions with surgical precision and context-aware controls not available in cloud defense.

According to the IDG report commissioned by A10 Networks (DDoS: Strategies For Dealing With a Growing Threat, 2017) only 25 percent of observed attacks were volumetric. In fact, 75 percent of the attacks were against infrastructure like DNS, and network components like firewalls, or against applications and servers. These types of attacks require proactive on-premise defense.

75% *OF DDOS ATTACK ARE NOT VOLUMETRIC*

Other considerations for cloud-only strategies:

- Cost may be attack bandwidth-based
- Can be expensive for frequently attacked business sectors
- Response time can be slow due to DNS convergence
- Services are largely a black box with limited controls for the subscriber

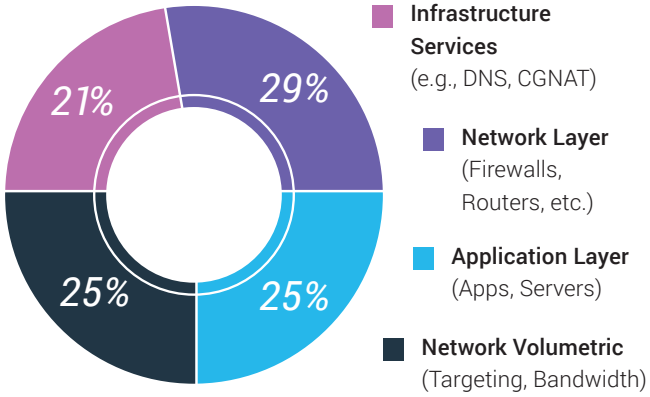


Figure 1: Multi-vector DDoS attack type breakdown

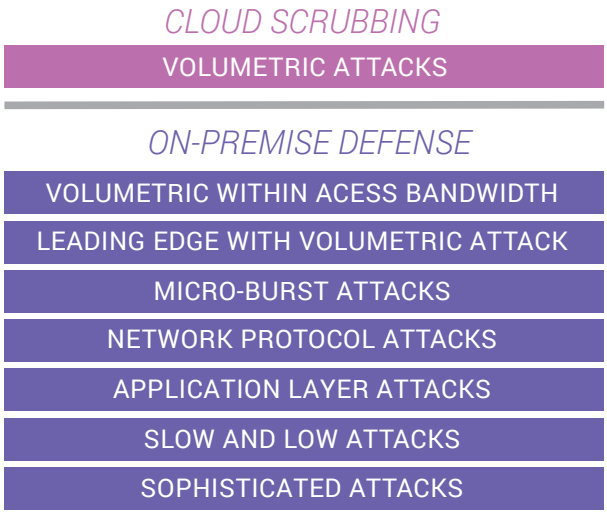


Figure 2: Cloud alone defense is only a partial solution for enterprises

ON-PREMISE DEFENSE MAKES SENSE FOR MOST ATTACK SIZES AND ALL ATTACK TYPES

News outlets only report on colossal DDoS attacks and massive defensive failures. As a result, organizations focus their attention on the next mega attack. However, according to Verisign's DDoS Trend report (Q1, 2017), 77 percent of attacks peak at less than 10 Gbps, and nearly half of all attack volumes are less than 1 Gbps. These statistics, in conjunction with the IDG report, indicate enterprises should focus on on-premise DDoS defense to handle the increasing attacker sophistication and the numerous lower-bandwidth attacks that fall below their internet pipe's capacity.

77% *OF ATTACKS PEAK LESS THAN 10 GBPS*

41% *LESS THAN 1 GBPS*

Verisign's DDoS Trend report (Q1, 2017)

A10 Networks' proactive on-premise defense provides precision and saves TCO by minimizing the number of times cloud scrubbing services are invoked.

- Proactive on-premise defense detects and mitigates all classes of DDoS attacks
- Fast detection and mitigation intervals down to 100 ms
- On-premise defense defends networks during DNS and BGP convergence
- On-premise defense blocks attacks undetectable by cloud scrubbing, like low-slow application attacks

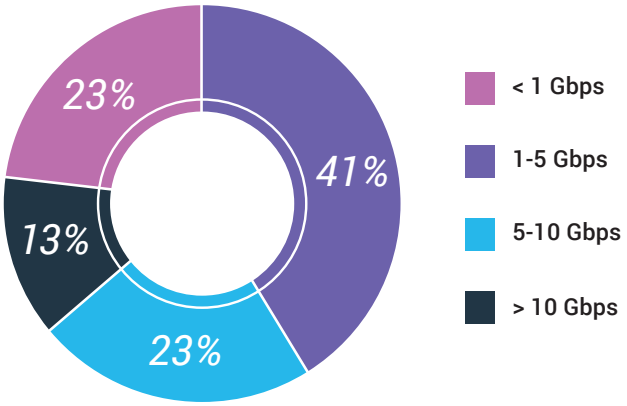


Figure 3: Q1 mitigation peaks

A10 NETWORKS HYBRID DDOS DEFENSE

Our full spectrum enterprise hybrid protection defends against DDoS attacks that threaten your network, revenue and reputation. We combine powerful on-demand cloud DDoS scrubbing with surgically precise on-premise A10 Thunder TPS for protection against large volumetric, application and slow-and-low attacks. The result: complete hybrid DDoS defense.

SURGICAL PRECISION TO PROTECT YOUR USERS FROM ATTACKING BOTS

Although DDoS attacks are largely brute-force, DDoS defense must be surgical and intelligently distinguish legitimate users from attacking bots. Strategies like Remote Triggered Black Hole (RTBH) and service rate limiting should be the last courses of action, not the first, because these strategies are indiscriminate and, in effect, achieve the attacker's goal of blocking service availability to legitimate users.

Thunder TPS focuses on legitimate users, which makes it different from other DDoS defense products and critically important for meeting enterprise business goals. Thunder TPS tracks every session coming into your environment to distinguish if the session is originated by a legitimate user or an attacking bot. For example, it initiates source-based authentication challenges and applies limits only to policy violators that deviate from learned, normal behavior. Even if a sophisticated bot is able to validate the challenge, Thunder TPS tracks more than 27 behavioral traffic indicators to catch deviation from normal behavior. If a session breaks a defined policy, only that session is blocked without creating collateral damage against legitimate users. Thunder TPS does this at an astounding scale of up to 128 million concurrent sessions.

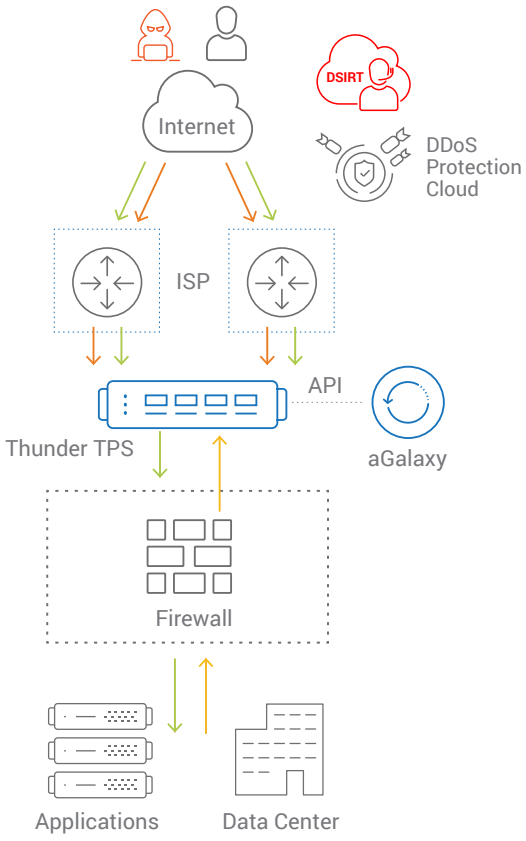


Figure 4: Multi-vector DDoS attack type breakdown

AUTOMATION TO REDUCE MANUAL INTERVENTION AND FALSE POSITIVES DAMAGE

Thunder TPS's five-stage automated mitigation escalation lets administrators create policies for each protected service and Thunder TPS automatically applies the required mitigations at each escalation level. This removes the need for time-strapped frontline personnel to make cumbersome manual changes, reduces collateral damage from false positives and improves response times during attacks.

Thunder TPS includes many strategies for surgical detection and mitigation, including:

- Automatic peacetime traffic behavioral learning and anomalous threshold setting
- Tracking more than 27 behavioral indicators to spot malicious behavior against applications or services
- Blocking L3-L4 packet anomalies and protocol and application anomalies
- Deflect spoofed attacks
- Initiating authentication challenges at L4-L7
- Limiting traffic and query rates by source and source IP sessions
- Current, accurate threat intelligence to stop known bad actors

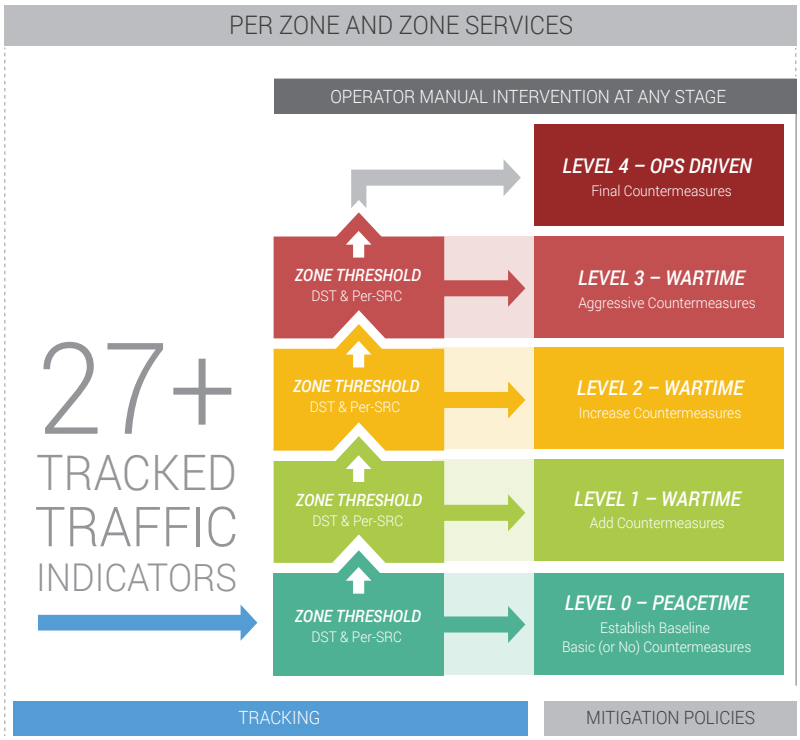


Figure 5: Policy-based automatic mitigation escalation

A10 DDOS PROTECTION CLOUD

The A10 DDoS Protection Cloud helps organizations reduce the risk of a catastrophic DDoS when attack volume grows beyond the capacity of an enterprise's internet pipe.

Unlike other scrubbing services, DDoS Protection Cloud service is built to protect your legitimate traffic, not for the amount of traffic that attacks apply against you. You are only charged for the protected traffic and the number of times cloud-scale scrubbing is required. Because Thunder TPS is deflecting all attacks that fall under your internet bandwidth, A10's two-pronged defense is the most surgically effective and economical full spectrum DDoS solution.

HOW IT WORKS

A10's two-pronged hybrid DDoS defense comprises three key components: A10 Thunder TPS, A10 DDoS Protection Cloud and A10 Networks aGalaxy® Central Management System. These components can be modularly deployed to scale to the demands of any network environment.

THUNDER TPS

- Always-on proactive surgical detection and mitigation
- Hardware or virtual appliance
- Deployed in-line L2 or in-path L3 with integrated BGP, OSPIF, IS-IS protocols
- Fast 100 ms detection and mitigation intervals

AGALAXY

- Manage and orchestrate Thunder TPS
- Unified dashboard and reporting
- Real-time mitigation console
- Packet capture

DDOS PROTECTION CLOUD

- 24/7 cloud redirection orchestration by A10 DSIRT
- On-demand volumetric defense
- Globally distributed scrubbing centers
- BGP and DNS traffic redirection

FEATURES AND BENEFITS

- Cost-effective, full spectrum multi-vector DDoS protection
- Cloud scrubbing for volumetric attack protection
- Surgical precision to protect users and infrastructure against sophisticated attacks
- Precise detection and automated mitigation escalation to make frontline defenders more effective
- Fast response, down to 100 ms detection and mitigation intervals, for time-sensitive applications
- Space saving one RU form factor from 2 Gbps through 152 Gbps throughput

SUMMARY

Our hybrid DDoS solution protects the most demanding network environments. Thunder TPS offloads common attack vectors to specialized hardware, allowing its powerful, multicore CPUs to distinguish legitimate users from attacking botnets and complex application-layer attacks that require resource-intensive deep packet inspection (DPI). When attacks grow past an organization's internet bandwidth capacity, A10 DDoS Security Incident Response Team (DSIRT) orchestrates traffic redirection to DDoS Protection Cloud for traffic scrubbing.

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

NEXT STEPS

To learn more about the A10 Thunder TPS DDoS protection solution, please contact your A10 representative or 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-19184-EN-01 MAR 2018