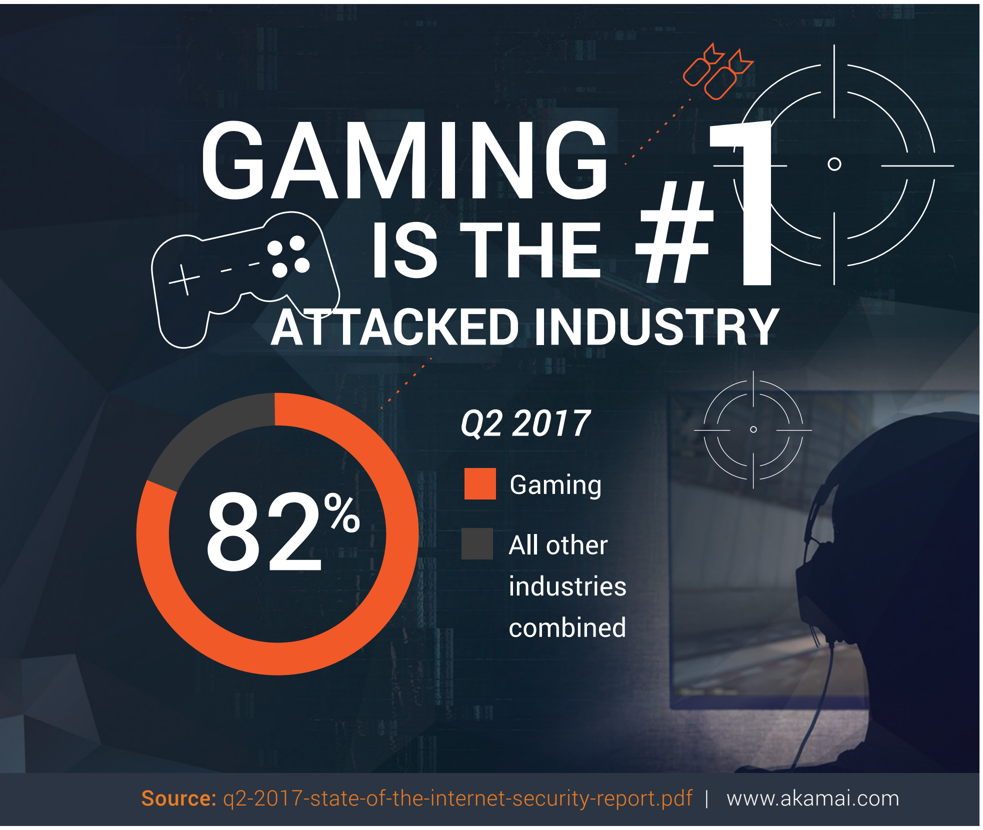
SOLUTION BRIEF

DDOS DESTRUCTION: DEFENDING ONLINE GAMING NETWORKS

PROTECT YOUR REAL-TIME GAMING EXPERIENCE, AND YOUR INFRASTRUCTURE

Online gaming DDoS defenders, you have it rough. Your industry is the most frequently targeted by DDoS attacks, and often you're attacked by your own users! As part of this industry, you know just how important availability is, and that downtime equates to lost revenue, and possibly social media rants that damage your company's reputation, and affronts new players.



Source: q2-2017-state-of-the-internet-security-report.pdf | www.akamai.com

Figure 1: In Q2 2017, online gaming was the No. 1 frequently attacked industry with 82% of total attacks aimed at gaming providers.

CHALLENGE

The frequency, intensity and sophistication of DDoS attacks – and attackers –threaten the most crucial aspect of running an online gaming enterprise: 24/7 availability. You need comprehensive, cost-effective defenses to ensure real-time gameplay is uninterrupted.

SOLUTION

A10 Thunder TPS offers surgical multi-vector DDoS protection to ensure the availability of business services at scale. Available in various form factors, Thunder TPS delivers online gaming enterprises cost-effective resilience against crushing DDoS attacks, while protecting legitimate user accesses.

BENEFITS

- Full-spectrum, multi-vector DDoS protection
- Surgical, precise detection and mitigation minimize false events
- Source-based mitigation prevents collateral damage to legitimate users when under attack
- Up to 128 million concurrent 5-tuple sessions are tracked, with rate enforcement

The increasing frequency, intensity and sophistication of attacks - and attackers - make DDoS resilience a critical requirement. Defending your online gaming infrastructure requires your focus to be on user experience. After all, it's the users who play your games, drive your business and create value for your company.

A10 Networks has created an ideal solution for gaming defenses. Legacy DDoS products jump to heavy-handed service rate limiting to defend infrastructure. A10 Thunder TPS® (Threat Protection System), by contrast, is a complete DDoS detection and mitigation solution that uses source-based mitigation to surgically distinguish legitimate users from attacking agents.

Thunder TPS delivers advanced and modern strategies to make your defenses invisible to your users and make solid economic sense.

3 OUT OF THE 5 TOP GAMING COMPANIES IN THE WORLD TRUST A10 DDOS DEFENSE TO PROTECT THEIR CRITICAL SERVICES.

SURGICAL PRECISION TO PROTECT GAMING EXPERIENCE

By nature, DDoS attacks are largely brute-force.

Therefore, effective DDoS defenses must be precise, with the ability to intelligently distinguish legitimate users, in this case gamers, from the attacking bots. Strategies like Remote Triggered Black Hole (RTBH), and service rate limiting should be the last courses of action, as these strategies are indiscriminate and unintentionally achieve the attacker's goals of blocking service availability to legitimate users.

SOURCE-BASED MITIGATION

Thunder TPS is unique in the DDoS protection market, and is especially relevant for the gaming industry. Online gaming companies must keep their networks and games on and running smoothly, even when experiencing DDoS attacks. Thunder TPS tracks every access to the network and can therefore distinguish between legitimate users and attackers. Thunder TPS initiates source-based authentication challenges and applies limits only to policy violators that deviate from learned, peacetime behavior. Even if a sophisticated bot can validate the challenge, Thunder TPS tracks 28 behavioral indicators to catch bot-based deviations.

If an attacking bot or misbehaving user breaks a defined policy, that misbehaving agent is blocked without creating collateral damage against legitimate users. Thunder TPS does this at an astounding scale of up to 128 million concurrent sessions – thereby helping to keep networks online and available.

5-TUPLE SESSION LEVEL GRANULARITY

Competitive multi-player gaming is a social experience. Gamers accessing popular titles can be globally distributed, but in many cases are clustered locally. In congested localities like university campuses or cities, gamers and attackers access the internet through network address translation (NAT) as it exits their host networks. NAT gateways translate private IPs to a public IP address at a scale of up to 64,512:1 (toward a destination). Each of the translated IP addresses is assigned an unreserved TCP or UDP source port so returning messages can be translated back to the original host. If there are offending attackers behind the NAT IP address and DDoS defenses don't track individual sessions, the entire pool of users are blocked or passed. Legacy DDoS defense systems don't have the granularity to track the state of sessions and, as a result, create collateral damage to your legitimate users behind NAT IP. Conversely, Thunder TPS can:

- Execute traffic limits on each 5-tuple session
- Track up to 128 million concurrent sessions

FAST INTERVAL MITIGATION ENSURES RESPONSIVE REAL-TIME EXPERIENCE

Adrenaline-fueled games count on low latency, real-time experiences. Attackers use microburst DDoS attacks to cause sluggish responses from game servers to gain an advantage over their competitors. Humans can detect irregularities down to 200 milliseconds, while legacy DDoS defenses may take tens of seconds or even minutes to respond. If this describes your gaming network, then you're at risk of alienating your real-time gamers.

- Thunder TPS is fast, with a traffic rate enforcement interval down to 100 milliseconds

IMPROVE FRONTLINE DEFENDER EFFECTIVENESS WITH AUTOMATED POLICY-BASED ESCALATION

Have you ever tried to manage pure chaos? That's what DDoS attacks feel like from the inside. Organizations typically only have a few trained personnel available during an attack, and they often have more to contend with than they can handle. To maximize personnel effectiveness, Thunder TPS supports five levels of programmatic mitigation escalation. Peacetime scenarios are learned and baselined for each protected zone. Administrators create custom policies for each protected service and Thunder TPS automatically applies the required mitigation at each escalation level. This removes the need for frontline personnel to make time-consuming manual changes, and improves response times during attacks. However, administrators retain the option to manually intervene at any stage of an attack.

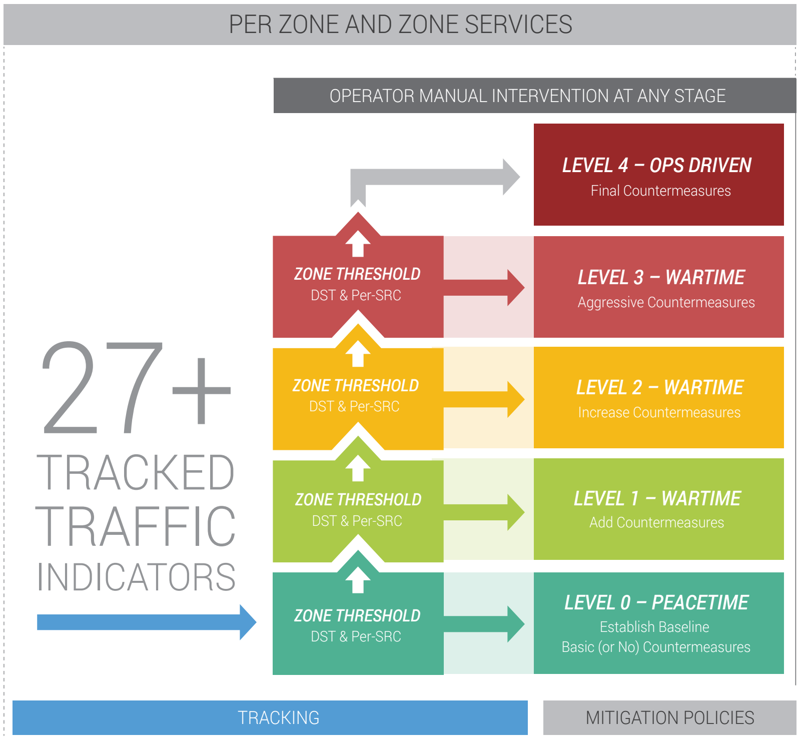


Figure 2: Policy-based automatic mitigation escalation

HIGH PERFORMANCE AND COST-EFFECTIVE SCALING

PERFORMANCE BY DESIGN

Thunder TPS was designed to deliver high performance and surgical precision to increase the effectiveness of DDoS defenses. It is available in a wide range of form factors that make economic sense for gaming infrastructures of all sizes. Thunder TPS offers unrivaled scale, so fewer units are needed, which dramatically improves TCO and overall reliability.

Thunder TPS can scale to 2.4 Tbps in a Class-list synchronized cluster.

THUNDER 14045 TPS

Throughput	300 Gbps
Packets Per Second (Legitimate traffic)	440 Mpps

SCALABLE PROTECTION FOR INCREASINGLY DISTRIBUTED DDOS ATTACKS

Successful gaming titles can have millions of users, and botnet herders are weaponizing millions of vulnerable IoT devices as DDoS attack agents. The combination of this good and bad traffic to gaming infrastructure requires rethinking scale to add breadth. Thunder TPS is enabled with A10 Networks' Advanced Core Operating System (ACOS®) data processing engine that provides the compute parallelism at internet scale.

Figure 3: Thunder 14045 TPS, the industry's highest performance appliance

SOURCE TRACKING BREADTH	MAXIMUM UNITS	NOTES
Monitored concurrent sessions	128,000,000	High resolution, zero sampling
Block known bad actors **Pass known good users**	96 million entries with 16 million entries per Class-list	Administrator specified A10 Threat Intelligence feed

24% | 24 hrs

ON AVERAGE, 24% OF THE IPS AND DOMAINS IN OUR THREAT INTEL ENGINE CHANGES EVERY 24 HOURS

A10 Threat Intelligence Service: current, accurate, powered by ThreatStop

MORE PERFORMANCE, LESS REAL ESTATE

Space is a premium at Internet Exchange Points (IXP). Gaming architects depend on these IXPs to build geographically distributed networks that minimize network delay and jitter so gamers' experiences are fast and responsive.

A10 DDoS protection solutions deliver the most performance per appliance, especially when compared to performance levels from other vendors.

vTHUNDER TPS
VMWare ESXI
Microsoft Hyper-V

THUNDER 840 TPS
2 Gbps

THUNDER 6435 TPS
152 Gbps

Figure 4: Thunder TPS virtual and space saving 1RU hardware appliances

HOW IT WORKS

A10's DDoS protection solutions have two critical components: Thunder TPS and aGalaxy® Central Management System. These components can be modularly deployed to scale to meet the demands of any gaming 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, OSPF, IS-IS protocols
- Fast 100ms traffic rate enforcement interval

AGALAXY CENTRAL MANAGEMENT SYSTEM

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

FEATURES AND BENEFITS

- Surgical precision protects users and infrastructure against volumetric and sophisticated attacks
- Cost-effective, full-spectrum, multi-vector DDoS protection
- Frontline defenders are more effective with precise detection and automated mitigation escalation
- Fast response, down to 100ms detection and mitigation intervals for your time-sensitive applications
- 100 percent API-programmable policy engine for easy automated orchestration integration

SUMMARY

New threat vectors have changed the breadth, intensity and complexity of options available to attackers putting online gaming enterprises and their real-time services in jeopardy. Established solutions that rely on ineffective, signature-based IPS or traffic rate limiting are no longer adequate to defend a gaming enterprise's most important assets: 24/7 availability and value-creating subscriber experiences.

Unlike outdated DDoS products, Thunder TPS is built on A10's market-proven ACOS platform, which delivers scalable form factors that make economic sense with a full spectrum DDoS detection, mitigation and reporting.

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.

ABOUT A10 NETWORKS

A10 Networks (NYSE: ATEN) is a Secure Application Services™ company, providing a range of high-performance application networking solutions that help organizations ensure that their data center applications and networks remain highly available, accelerated and secure. 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.

NEXT STEPS

To learn more about the A10 Thunder TPS DDoS protection solution, please contact your A10 representative or visit a10networks.com/tps.

LEARN MORE

ABOUT A10 NETWORKS

CONTACT US

a10networks.com/contact

Part Number: A10-SB-19188-EN-02 MAR 2018