ENSURING THE GAME IS ALWAYS "ON"

High-performance, Highly Granular and Versatile DDoS Mitigation for Gaming Providers

Challenge:

Gaming providers need to ensure service uptime under all circumstances, as degraded availability leads to revenue and reputation loss. The gaming industry accounts for more than a third of all DDoS attacks, while the attacks themselves continue to increase in frequency, persistence, size and sophistication.

Solution:

Thunder TPS provides a high-performance, versatile and highly configurable DDoS solution that delivers automated threat detection and mitigation, and enforces granular service protection policies.

Benefits:

- Hardware acceleration to combat multi-vector attacks effectively
- High-performance live traffic tracking to analyze traffic patterns and detect anomalies
- Highly scalable and configurable to continuously inspect and mitigate sophisticated attacks
- Flexible deployment to support easy integration into custom systems through open standards and a RESTful aXAPI

The online gaming industry is constantly combating Distributed Denial of Service (DDoS) attacks, and the media provides many examples of "hacker" groups claiming responsibility for taking down many online games. The motives for deploying such attacks vary from extortion and competitive, to retaliation and boasting.

Online services known as "booters" or "stress testers" or even DDoS-as-a-Service (DDoSaaS) are readily available. Anyone can go online, anonymously pay through bitcoin and have their victim of choice booted off the Net.

Online video games are now mostly hosted by the software companies that create the gaming software, or the gaming platform. This centralized position unfortunately creates a focal point for DDoS attacks, whereas gamer-to-gamer attacks are a problem on the Internet Service Provider (ISP) level. Together with government and ISPs, gaming providers (both video games and gambling) stand out as the most likely DDoS targets, accounting for more than a third of all DDoS attacks. And combating them is critically important to these businesses, as the availability of online gaming services directly relates to an organization's revenue, as well as its reputation.

The Challenge

Gaming providers require their services to be available at all times, as the online services are the major revenue source. Loss of uptime leads to loss in revenue in the short run, and can also impair a provider's reputation for being reliable, causing gamers to choose to use services from the competition.

Just in late 2014, high volume attacks were aimed at gaming networks such as Sony's Play Station Network (PSN), successfully impairing those services. A group naming itself Lizard Squad claimed responsibility for taking down the services for Destiny and Call of Duty, using Twitter to brag about it. Subsequent attacks during the Christmas holiday week, a prime time for gaming traffic, were promised and successfully executed. The group's focus was to market its online DDoS-for-hire services.

Gaming providers need to ensure service uptime under all circumstances, as degraded availability leads to revenue and reputation loss. As the most likely target of any DDoS attack, gaming providers need continuous protection to preserve their online presence. Traditional security solutions are not always up to the task of combating DDoS attacks due to their stateful nature. Introducing new solutions in the path of traffic can introduce new problems, such as latency. Low latency in the online service is key; gaming lag is one of the most important metrics gamers look at when choosing a medium to play on. A fast, always-on DDoS protection solution protects the entire network from the impact of DDoS attacks.
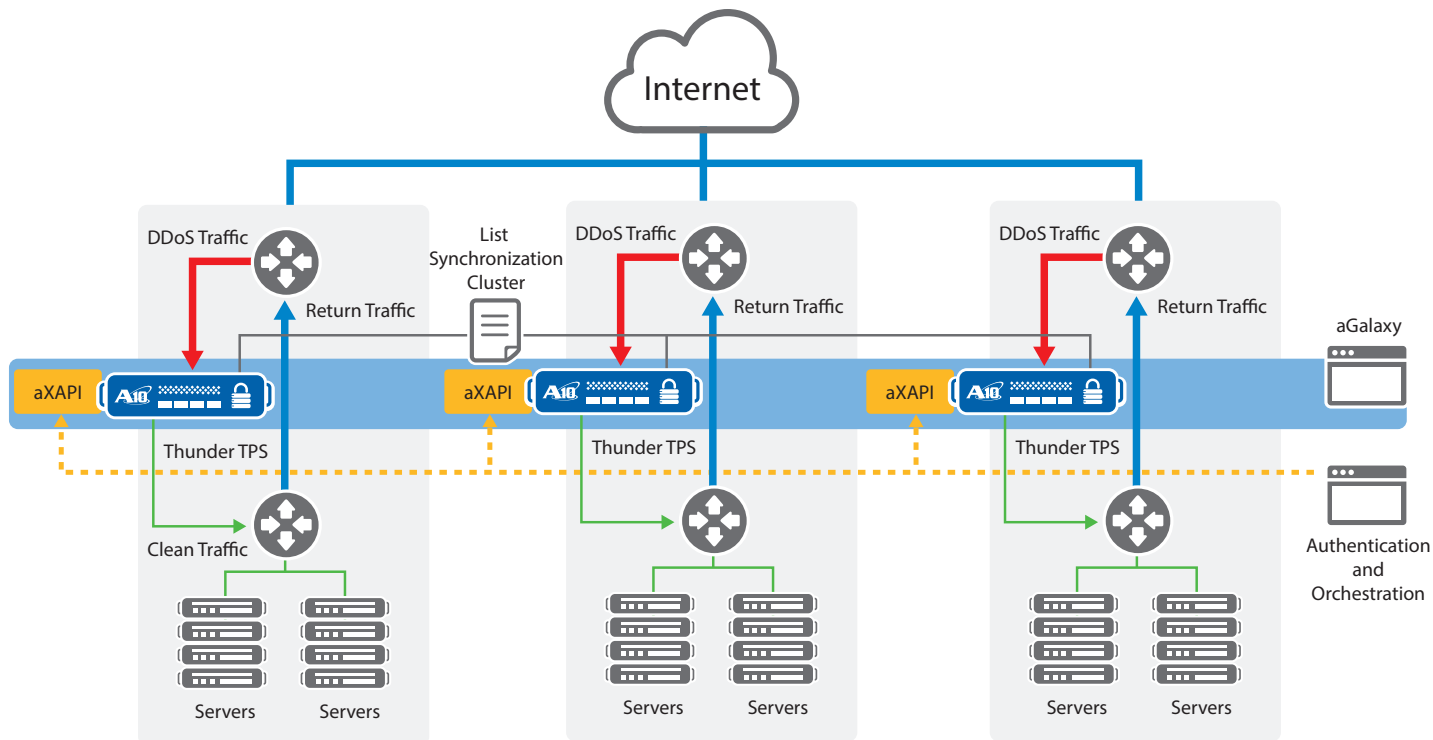
Figure 1: Thunder TPS providing always-on service availability, with aXAPI for dynamic provisioning

Since the providers cater to gamers all over the world, their network capacity is substantial. Their infrastructure needs to be able to scale along with the surges of new gamers coming online, such as after work or school hours, or because of traffic surges due to new launches that are trending in gaming community forums. Volumetric DDoS attacks have similar traffic characteristics but are more extreme and damaging. Whatever the reason for a sudden traffic increase, DDoS protection infrastructures have to be able to scale along with the connections per second tsunamis, as well as the accompanying bandwidth.

A10 Networks Thunder TPS

To combat the relentless DDoS attacks, a scalable, high-performance solution is required. Since gaming providers are under attack almost constantly, an always-on solution which is fast in both detection and mitigation is key.

A10 Networks® Thunder™ TPS line of Threat Protection Systems provides high-performance, network-wide protection against DDoS attacks, and enables service availability against a variety of volumetric, as well as more sophisticated application attacks.

A10 Thunder TPS is designed to deliver the highest performance in terms of bandwidth, packet-per-second throughput and connections-per-second capacity to ensure that the infrastructure has enough headroom to deal with fast data growth due to popularity surges, as well as DDoS attacks and anomalies that happen on a daily basis.

Thunder TPS is the right choice for defending against multi-vector DDoS attacks, where simple infrastructure attacks (for example, SYN floods) are combined with more sophisticated application-layer attacks (low-and-slow, for example). The majority of high volume traffic can

be mitigated by specialized hardware such as a Field Programmable Gate Array (FPGA), preserving the powerful CPUs for intensive deep packet inspection (DPI) tasks. This combination allows the Thunder TPS solution to stand strong in the face of increasingly popular multi-vector attacks.

Because network designs and their policies are different everywhere, there are many ways to deploy and integrate Thunder TPS into a gaming provider's network. Through its A10 Networks aXAPI® REST-based API, third-party systems can dynamically apply specific policies. Authentication systems can quickly update the Thunder TPS white lists, leveraging the BGP protocol to announce authenticated sources.

Network security administrators can choose how the Thunder TPS system enforces network protection. Fully automatic learning and mitigation are available but DevOps staff will appreciate the programmatic environment that Thunder TPS provides. TCL-based A10 Networks aFleX® Deep Packet Inspection (DPI) Scripting Technology is available, as well as regular expressions and Berkeley packet filter (BPF), which can be used for pattern matching.

There are also many deployment modes that can be used to integrate Thunder TPS in the network, but proactively managing ingress traffic in an asymmetric deployment is the recommended model for most gaming providers, as their networks are under almost constant attack. This architecture provides continuous traffic analysis and the fastest detection and mitigation times.

Volumetric attacks that exceed your network's capacity can be dealt with by Verisign's DDoS Protection Services. The Verisign DDoS Protection Service is backed by 75 global points of presence and over 2 Tbps of global capacity.

Features and Benefits

Thunder TPS provides:

- **Hardware-based mitigation of common infrastructure attack types:** Thunder TPS can detect and mitigate up to 60 common attack vectors in hardware, offloading its ultra-powerful CPUs for more complex application-layer attack detection and mitigation.

- **Low latency:** Thunder TPS provides ultra-low latency to minimize "gaming lag," along with sub-second mitigation times.

- **Always-on protection and policy enforcement:** With Thunder TPS, there are no external detection systems required.

- **Scale out:** Easily scale out with black/white list synchronization between different Thunder TPS systems and centrally manage through the A10 Networks aGalaxy® Centralized Management System.

- **Highly granular bandwidth rate enforcement:** Thunder TPS is uniquely able to track the traffic rates per outside session. Unlike total bandwidth utilization to a service, per-session traffic patterns are fairly predictable so anomalies are easily spotted and mitigated, eliminating impact to other gamers.

- **Comprehensive detection and statistics:** With access to over 400 global, destination-specific and behavioral counters, network and security staff can quickly spot and analyze network anomalies. Automated traffic baselining is also available. The enhanced, easy-to-use GUI provides a dashboard, with incident and rich report views, which can be used to improve DDoS protection strategies. Mitigation can be done manually or automatically.

- **Programmatic policy enforcement:** Leverage system states and statistics within the TCL based aFleX environment, to customize enforcement of advanced security policies. Regular Expressions (regex), as well as Berkeley Packet Filter (BPF) statements can be used for advanced pattern matching.

- **Third party integration:** Network and service functions can grow very diverse and tight integration is required. Many custom systems exist and Thunder TPS can integrate easily by leveraging its API, or by leveraging BGP Blackhole signals from other systems to redirect suspect traffic through Thunder TPS.

- **False positive protection:** Authentication systems can easily distribute authenticated client IP addresses to the Thunder TPS white list using the BGP networking protocol. This provides a fast and dynamic solution to update security systems of IPs that demand less scrutiny.

- **IPv6 feature parity:** With gamers connecting from anywhere on the Internet and the adoption of IPv6 increasing at a rapid rate, gaming providers want to be sure that their security infrastructure is ready for any attack type, whether launched over IPv4 or IPv6.

Summary – Versatile Thunder TPS DDoS Mitigation for Gaming Providers

A10 provides a highly scalable, highly configurable DDoS mitigation solution for gaming providers who are constantly exposed to increasingly sophisticated DDoS attacks. Thunder TPS provides comprehensive tools to ensure that gaming platforms are always available, and the game is always "on."

Next Steps

For more information, please contact your A10 representative and visit: www.a10networks.com/products/thunder-series/thunder-tps-ddos-protection.

About A10 Networks

A10 Networks is a leader in application networking, 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, California, and serves customers globally with offices worldwide. For more information, visit: **www.a10networks.com**

Corporate Headquarters

A10 Networks, Inc
3 West Plumeria Ave.
San Jose, CA 95134 USA
Tel: +1 408 325-8668
Fax: +1 408 325-8666
www.a10networks.com

Worldwide Offices

North America
sales@a10networks.com
Europe
emea_sales@a10networks.com
South America
latam_sales@a10networks.com
Japan
jinfo@a10networks.com
China
china_sales@a10networks.com

Hong Kong
HongKong@a10networks.com
Taiwan
taiwan@a10networks.com
Korea
korea@a10networks.com
South Asia
SouthAsia@a10networks.com
Australia/New Zealand
anz_sales@a10networks.com

To learn more about the A10 Thunder Application Service Gateways and how it can enhance your business, contact A10 Networks at: **www.a10networks.com/contact** or call to talk to an A10 sales representative.