SOLUTION BRIEF

DATA CENTER DDOS PROTECTION

HIGH-PERFORMANCE AND VERSATILE DDOS MITIGATION FOR COLOCATION AND DATA CENTER PROVIDERS

Enterprises use provider data centers because they want operational predictability, a higher ROI than going in-house and greater security. Data centers hold their most valued corporate assets, so protecting their integrity and guarding against service interruptions should be the highest priority.

The leading causes of data center down times, as reported by the Ponemon Institute's latest report, are: UPS system failure, human error, Distributed Denial of Service (DDoS) cyber crime, weather, climate control, generator failure and IT equipment failure. Whereas two years earlier it was at the bottom of the list, DDoS has skyrocketed to third place and is now the cause of one in five outages.

Greater ease of launch, coupled with lower costs and more impact, has contributed to an increase in DDoS attacks in all industry segments. However, data centers are a particularly rich target, since the shared resources and multi-tenant nature of these environments aggregate the individual tenant risks to all involved. DDoS attacks not only impact the targeted customer but they take down other tenants, not to mention the data center itself, by way of collateral damage.

Downtime leads to lost revenue and unsatisfied customers, which increases customer churn, operational expenses and the marketing costs required to retain and attract new customers. Most importantly, however, it damages the data center's brand and reputation.

Downtimes also lead to significant customer costs. Ponemon estimates that DDoS-spurred outages cost an average of $822,000 to mitigate, second only to the $959,000 it costs to fix outages caused by IT equipment failure.

To prevent extra costs to the data center and its tenants' data, security must be addressed at every level of a data center's service. Most data centers have high levels of data security and defenses in place for viruses and malware, but most have inadequate DDoS protection – an oversight with potentially devastating consequences.

CHALLENGE

Due to collateral damage, the risk of a DDoS attack for each tenant in a data center equals the aggregate of the risk to every tenant. DDoS is now the third leading cause of data center downtime and rising, so defending against it has never been more important.

SOLUTION

A10 Thunder TPS provides a high-performance, versatile and highly configurable DDoS mitigation solution to provide automated threat detection and mitigation and granular service protection policies.

BENEFITS

- Hardware acceleration to combat multi-vector attacks effectively
- Smart traffic baselining for automated threat detection and mitigation
- Highly scalable and configurable to inspect and mitigate sophisticated attacks
- Flexible deployment; easily integrates into custom systems through open standards and a RESTful aXAPI

THE CHALLENGE

DDoS attacks are becoming increasingly sophisticated through the combined use of volumetric and application-layer attacks on network bandwidth, server sockets, web server threads and CPU utilization. Volumetric attacks saturate primary carrier links into the data center, knocking out access to all applications and services hosted behind them. Application attacks target specific hosts by overloading application resources and therefore are isolated by nature.

DDoS attacks have become easier and less expensive to launch, while at the same time increasing in volume, velocity, duration and complexity. Internet Service Providers (ISPs) should be the first line of defense against volumetric attacks but they can't be relied on. And while firewalls, Intrusion Prevention Systems (IPS) and load balancers are effective tools for network integrity, they're susceptible to state exhaustion attacks and are often simply inadequate to detect and mitigate layer 7 attacks. To defend themselves, data center operators must implement dedicated DDoS solutions to withstand and mitigate volumetric and application-layer attacks launched against their network infrastructure.

Surprisingly, only a minority of data centers sell their customers security services beyond firewalls, SSL certificates, antivirus, VPNs and alerts. But data centers that employ dedicated DDoS solutions can also make available managed, state-of-the-art DDoS attack protection services for their tenants, differentiating themselves and increasing revenue.

THE A10 NETWORKS THUNDER TPS SOLUTION

Avoid downtime by deploying a scalable, high-performance solution at the data center's edge to protect customers' lower speed downstream links and servers.

DDoS attacks cause significant customer costs and lead to higher churn and damage to brand and reputation. A10 Networks® Thunder TPS™ line of Threat Protection Systems mitigates these risks by providing high-performance, network-wide protection against DDoS attacks. It also enables service availability against a variety of volumetric and more sophisticated application attacks.

Thunder TPS is designed to deliver the highest performance in terms of bandwidth, packet-per-second throughput, as well as connections-per-second and black/white list capacity to ensure that the infrastructure has enough headroom to deal with DDoS attacks and other security anomalies that happen on an almost daily basis.

Because network designs and their policies are different, there are many options for the deployment and integration of Thunder TPS. Through its A10 Networks aXAPI® REST-based API, third-party analytics systems can instruct specific traffic to be redirected for cleaning when deemed necessary. Simlarly, orchestration solutions can provision the Thunder TPS systems in a data center with individual policies for select end users.

The A10 Networks aGalaxy® Centralized Management System unifies the management of several Thunder TPS devices, improving operational efficiency and cost. It consolidates all management tasks in one location, making it easy for administrators to apply consistent policies across all devices. From the aGalaxy web user interface, administrators can view the status of virtual servers or, for Thunder TPS management, TPS protected objects.

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.

Leading data centers deploy A10 Thunder TPS to maintain availability to their services and increase revenue by providing managed DDoS security solutions to their customers.

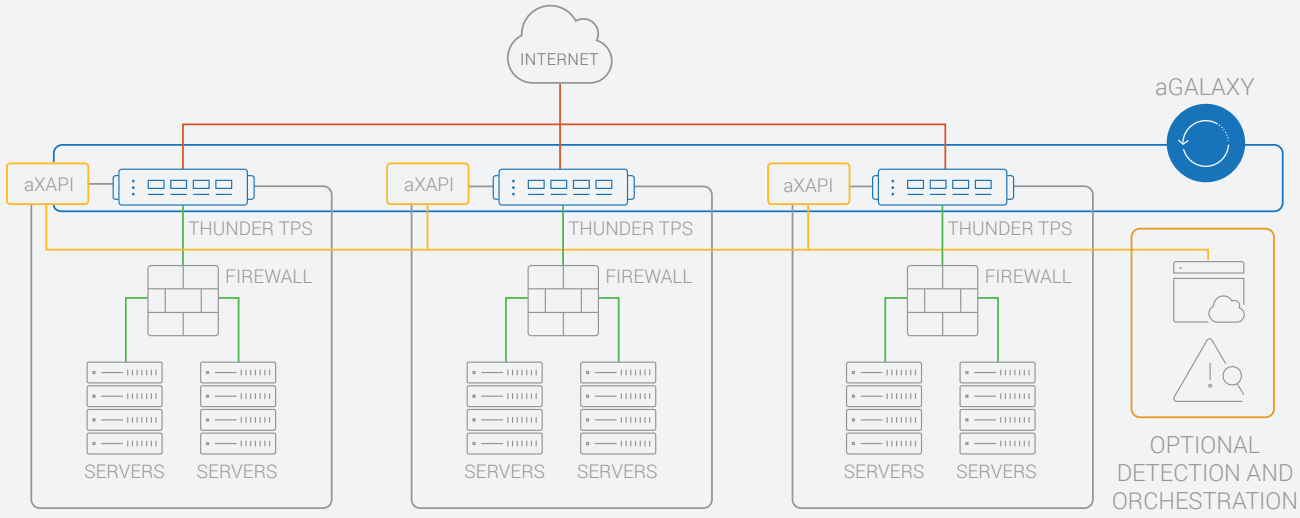

Figure 1: Thunder TPS protecting multiple datacenters, controlled by aGalaxy. Third-party inspection and orchestration solutions can leverage aXAPI for full control and select policy enforcement.

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, reserving its ultra-powerful CPUs for more complex application-layer attack detection and mitigation.
- **Smart threat detection and mitigation:** The system has access to a rich set of multi-protocol counters and behavioral indicators to learn peacetime network conditions, enabling precise detection of anomalies. Dynamic mitigation policies escalate suspect traffic through progressively tougher countermeasures to minimize legitimate traffic drops. DevOps can leverage event triggered scripts for increased operational agility.
- **Highly granular bandwidth rate enforcement:** Thunder TPS is uniquely able to track the traffic rates per outside connection. These traffic patterns are fairly predictable so anomalies are easily spotted and mitigated, eliminating impact to other customers.
- **Programmable policy engine:** Along with access to system states and statistics, Thunder TPS simplifies enforcement of advanced application and security policies. Regular Expressions (regex) and Berkeley Packet Filter (BPF) are the preferred tools for pattern matching.
- **A10 Threat Intelligence Service powered by ThreatSTOP.** This service combines and enhances reputation data from over three dozen security intelligence sources, including DShield and Shadowserver, to enable Thunder TPS to instantly recognize and block traffic to and from known malicious sources. A10's Threat Intelligence Service provides the following benefits:
  - Protects networks from future threats
  - Blocks non-DDoS related threats such as spam and phishing
  - Increases Thunder TPS efficiency

  With a threat intelligence network that continuously charts potential intruders on the Internet, customers can leverage global knowledge to block traffic from malicious Internet locations and offload Thunder TPS from identifying known bots and attack sources.
- **Programmatic integration**: Networks can grow very complex so tight integration is required. Many custom systems exist and Thunder TPS can integrate easily by leveraging open networking protocol standards and its aXAPI API.
- **IPv6 feature parity**: With the adoption of IPv6 increasing at a rapid rate, data center providers can be assured that their security infrastructure is ready for any attack type, whether launched over IPv4 or over IPv6.

SUMMARY

HIGH-PERFORMANCE, VERSATILE DDOS MITIGATION FOR DATA CENTER OPERATORS

A10 provides a highly scalable, highly configurable DDoS mitigation solution for data center operators trying to maintain the integrity of their facility by fending off attacks that can lead to collateral damage. Thunder TPS line of Threat Protection Systems helps to analyze traffic with ultra-low latency and provides comprehensive tools that minimize outages.

NEXT STEPS

To learn more about the A10 Thunder TPS, please contact your A10 representative or visit: a10networks.com/products/thunder-series/ddosdetection-protection-mitigation

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

LEARN MORE

ABOUT A10 NETWORKS

CONTACT US

a10networks.com/contact

Part Number: A10-SB-19140-EN-03 OCT 2017