CARRIER GRADE DDOS PROTECTION

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

Challenge:

DDoS attacks are on the rise, increasing in volume, velocity, duration and complexity, and so too are customer expectations. Maintaining five nines service, for example, means no more than five minutes of downtime per year. Meeting SLA obligations has never been more challenging for ISPs.

Solution:

A10 Thunder TPS provides a high-performance, versatile and highly configurable DDoS mitigation solution to empower network traffic insight and granular DDoS mitigation.

Benefits:

- Hardware acceleration to combat multi-vector attacks effectively
- High-performance live tracking to analyze traffic patterns and anomalies
- Highly scalable and configurable solution to automatically inspect and mitigate sophisticated attacks
- Flexible deployment; easily integrates into custom systems through open standards and a RESTful aXAPI

Distributed Denial of Service (DDoS) attacks have become more numerous and diversified, threatening the availability and performance of the service provider's network. To maintain service availability and keep their downstream customers up and running, Internet Service Providers (ISPs) must be able to detect, analyze and mitigate DDoS threats in real time before they develop into costly service availability outages.

Enterprises choose their ISP based on reliability, responsiveness and the expected consequence for not meeting those objectives. Five nines service availability translates into no more than five minutes of downtime per year. So when an ISP's network is attacked, response must be quick and effective.

When a DDoS attack brings down an ISP's network, businesses face lost revenue, dissatisfied or lost customers, damage to their brand and reputation and, in some regulated industries, possible fines. If downtime is higher than the obligations set in the Service Level Agreement (SLA), customers may be due credits, reimbursements and the option to terminate their contract.

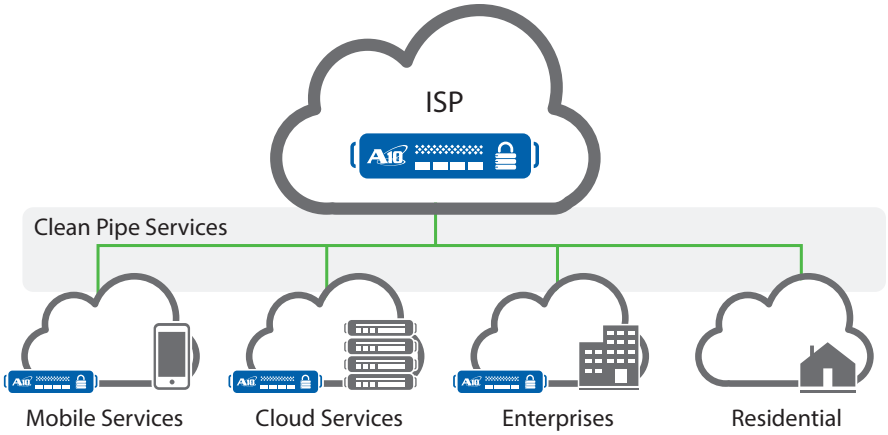
In short, the blowback from a successful DDoS attack affects both ISPs and their customers.

The Challenge

Multi-vector DDoS attacks bring a tough challenge 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, knocking out access for all customers 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. Firewalls, Intrusion Prevention Systems (IPS), and load-balancing devices are all effective tools for network integrity but they're susceptible to state exhaustion attacks and are simply inadequate to detect and mitigate layer 7 attacks.

DDoS attacks cause significant customer costs and lead to higher churn and damage to brand and reputation. To defend themselves, service providers must deploy dedicated DDoS solutions to withstand and mitigate volumetric and application-layer attacks against their infrastructure. Maintaining a competitive edge in the marketplace requires that they differentiate themselves from other providers. An effective way of doing this is by offering customers "clean pipes" through cost-effective, value-added DDoS attack protection security services.



The A10 Networks Thunder TPS Solution

Avoid downtime by deploying a scalable, high-performance solution at the perimeter of the provider network to protect customers' lower speed downstream links. A10 Networks® Thunder™ TPS line of Threat Protection Systems mitigates 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 and packet-per-second throughput capacity to ensure that service providers (fixed, mobile, cloud infrastructure) have enough headroom to deal with multi-vector DDoS attacks and other security anomalies that happen on an almost daily basis.

Because network designs and their policies are different, there are different options for the deployment and integration of Thunder TPS. Through its A10 Networks aXAPI® REST-based API, Thunder TPS easily integrates into custom systems, and third-party analytics can instruct specific traffic to be redirected for cleaning when deemed necessary.

Leading service providers deploy A10 Thunder TPS to maintain availability to their services and increase revenue by providing value-added DDoS security services to their customers.

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.
- **Low latency:** Thunder TPS provides ultra-low latency to minimize mean time to mitigation, which maximizes effectiveness against volumetric attacks.
- **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.
- **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. The enhanced, easy-to-use GUI provides a dashboard, with incident and rich report views, which can be used to improve DDoS protection strategies.
- **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.
- **Programmatic integration:** Networks can grow very complex so tight integration is required. Many custom systems exist and Thunder TPS can integrate easily by leveraging BGP Blackhole signals or its aXAPI API.
- **IPv6 feature parity:** With the adoption of IPv6 increasing at a rapid rate, service 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 ISPs

A10 provides a highly scalable, highly configurable DDoS mitigation solution for service providers trying to meet the obligations of their SLA contracts. Thunder TPS provides hardware-based mitigation of common infrastructure attack types with ultra-low latency. It leverages A10's aXAPI API to tightly integrate with custom systems. It provides an easy-to-use dashboard with rich reporting. And it helps to analyze traffic and provides comprehensive tools that minimize down time.

Next Steps

To learn more about A10 Networks products and solutions, please contact your A10 representative or visit www.a10networks.com.

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

Part Number: A10-SB-19141-EN-02
Dec 2015

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.