Hybrid Multi-Vector DDoS Protection with A10 Networks & Verisign

Protect Organizations with Limited Bandwidth from Advanced Volumetric & Application-Layer DDoS Attacks

Challenge:

Organizations with limited bandwidth are falling victim to advanced multi-vector DDoS attacks.

Solution:

A10 Networks and Verisign deliver a hybrid multi-vector DDoS protection solution to leverage both on-premise and cloud-based infrastructure to seamlessly defeat advanced volumetric attacks.

Benefits:

- Ensure business operation in the face of advanced multi-vector DDoS attacks
- Bridge on-premise and cloud-based solutions for appropriate control, security and scalability
- Seamlessly mitigate high-bandwidth attacks that surpass an organization's capacity

VERISIGN

DDoS attacks — growing in size, frequency and sophistication — jeopardize an organization's online revenue streams. Multi-vector distributed denial of service (DDoS) attacks are particularly hard to mitigate. They consist of simultaneous attack vectors, ranging from attacks on the infrastructure to more sophisticated application attacks.

In addition, application-layer attacks, including "slow-and-low attacks," tend to avoid detection by traditional security controls. In contrast, volumetric attacks deploy large amounts of data against an organization's network — seemingly from random or spoofed source locations — with the goal of saturating bandwidth to deny legitimate traffic.

A hybrid on-premise and cloud approach helps solve capacity limitations. An on-premise solution can inspect traffic and mitigate DDoS attacks locally, up to the point where the DDoS traffic starts to reach an organization's available bandwidth capacity. From this point, a cloud-based solution can mitigate larger volumetric attacks.

The Challenge

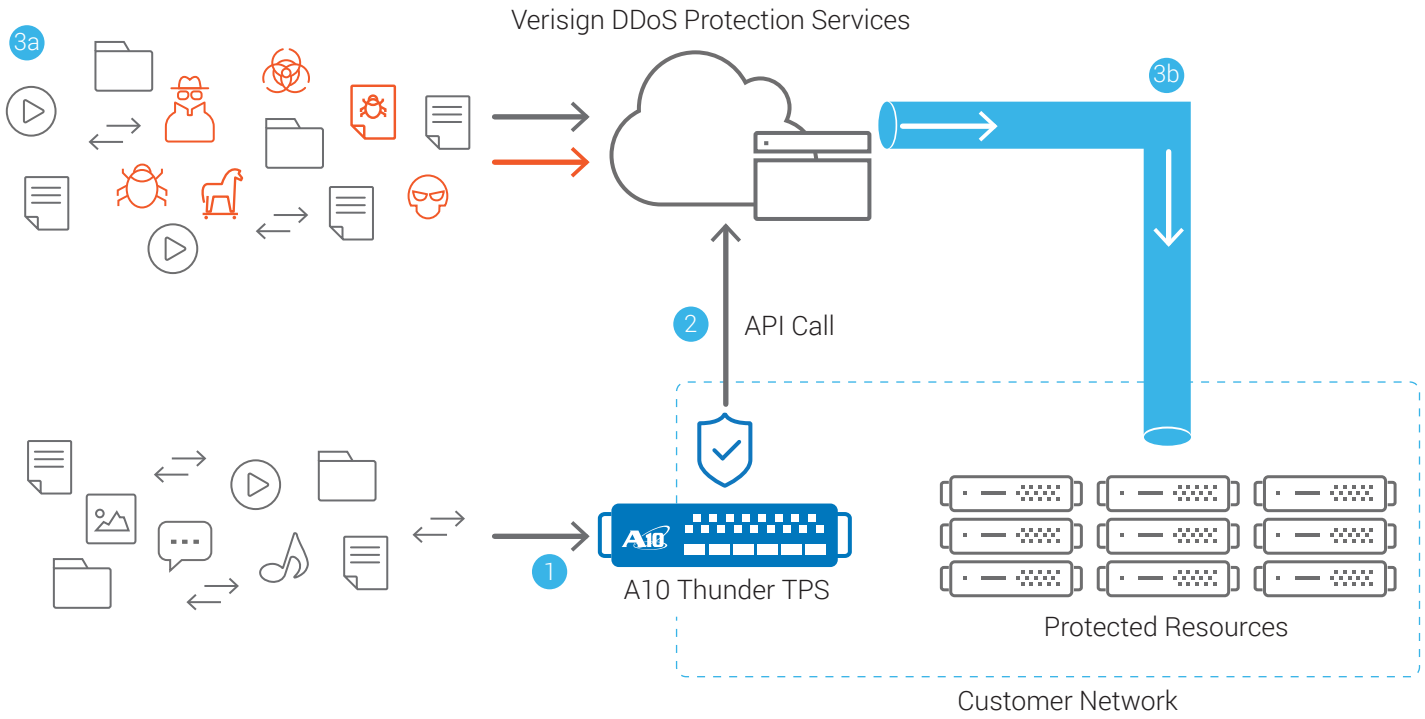
DDoS attacks are increasingly sophisticated by strategically combining volumetric and application-layer attacks on network bandwidth, server sockets, Web server resources and CPU utilization.

Many security experts manage DDoS protection through an on-premise solution. While this approach provides a level of control to enforce security policies and reduce potential latency during mitigation, the solution is limited to an organization's expensive Internet uplink capacity. On-premise solutions can only mitigate an attack up to the amount of bandwidth it has at its disposal.

A10 Networks Thunder TPS and Verisign DDoS Protection Service

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

A10 Networks Thunder TPS, powered by the ACOS Harmony platform, inspects network traffic and helps users set a baseline for their service's traffic patterns. When anomalies are suspected, the traffic may be escalated to progressively increasing levels of scrutiny. Thunder TPS validates whether a source is actively communicating with the protected service or if it is simply distributing traffic to overwhelm resources and render the service unavailable.



Thunder TPS Integration with Verisign DDoS Protection Service

Solution Components

A10 provides a highly scalable and configurable DDoS mitigation solution. Featuring real-time integration with the Verisign DDoS Protection Service, Thunder TPS can ensure organizations can defeat advanced DDoS attacks and keep online services and applications operational.

1. Thunder TPS analyzes incoming traffic and protects against DDoS attacks
2. When the bandwidth threshold is reached or exceeded, Thunder TPS sends an alert to Verisign through the Verisign OpenHybrid API with information about the attack which may indicate to Verisign that traffic redirection may be required
3. Once traffic has been redirected (3a), Verisign will apply layered filters to the redirect traffic and return the filtered traffic back to the customer network (3b)

Thunder TPS can signal to the Verisign DDoS Protection Service when traffic rates reach or exceed an organization's Internet bandwidth or other pre-defined resource utilization thresholds. The Verisign DDoS Protection Service can then mitigate both volumetric and application-layer attacks.

How it Works

During a DDoS attack, Thunder TPS sends signals to Verisign through the Verisign OpenHybrid API once pre-defined thresholds are reached. The signals provide critical information about the attack target, source and types to Verisign's 24x7 Technical Support Service (TSS) team.

Verisign TSS will continuously monitor these signals and implement the necessary steps to mitigate the DDoS attack, if required. The Verisign DDoS Protection Service leverages its global scrubbing centers and proprietary Athena mitigation platform to actively defeat some of the largest and complex DDoS attacks.

Customers may choose to redirect its traffic to the Verisign DDoS Protection sites through BGP or DNS-based swings. Once traffic is redirected to the Verisign DDoS Protection sites, Verisign will apply layered filters to the traffic and return the filtered traffic back to the customer's network.

Features and Benefits

- Full control of data flows on-premise
- Manage complex attacks on-premise
- Progressively escalate inspection levels of suspect traffic with Thunder TPS
- Hybrid solution for both complex and large volumetric DDoS attacks
- Escalate to Verisign's cloud-based DDoS Protection Service when Thunder TPS identifies the attack is reaching pre-defined threasholds
- BGP- or DNS-based traffic redirection

Protect Online Services Against Large DDoS Attacks

Together, A10 Networks and Verisign can help protect your online services against large DDoS attacks. Thunder TPS provides the best on-premise solution for protecting against multi-vector DDoS attacks while the Verisign DDoS Protection Service is a cloud-based solution that can mitigate against volumetric and complex application layer attacks.

Next Steps

To learn more about the A10 Networks Thunder TPS and Verisign DDoS Protection Service, 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-19161-EN-01
Aug 2016

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 discover how A10 Networks products will enhance, accelerate and secure your business, contact us at **a10networks.com/contact** or call to speak with an A10 sales representative.