Big Data-Powered DDoS Protection with A10 Networks & Kentik

Gain Greater Detection Accuracy, Deeper Analytics Plus Support for A10 Networks Dynamic Mitigation

Challenge:

The rising volume and severity of DDoS attacks are overwhelming the capabilities of traditional out-of-band detection schemes.

Solution:

A10 Networks and Kentik offer a powerful combination of big data-powered detection and analytics with the industry's most powerful and intelligent DDoS protection and mitigation solution.

Benefits:

- Ensure business continuity in the face of rising DDoS threats
- Significantly increase the accuracy of detecting and stopping DDoS attacks
- Gain service assurance visibility with big data traffic and BGP analytics on months of network data
- Mitigate DDoS attacks up to 300 Gbps of throughput capacity (2.4 Tbps in synchronization cluster)

With the advent of global IoT-powered botnets, DDoS is a serious threat that is escalating to new levels of sophistication, volume and payload. As organizations develop Internet-dependent digital lines of business, and move large portions of infrastructure and applications to the cloud, the need to prevent devastating network outages caused by DDoS attacks is increasingly critical.

Traditional out-of-band DDoS detection approaches, based on scale-up appliances or single-server software, can no longer cope with the threat. Built with compute, memory and storage constraints from a pre-cloud era, these legacy solutions suffer from numerous false negatives — or missed attacks — that wreak havoc with customer experiences, revenues and brand equity.

Further, traditional DDoS detection appliances don't offer the analytics that network engineers and security pros need to maintain situational awareness.

A next-generation DDoS detection capability, powered by big data, offers significant improvements in both attack detection accuracy and deep, exploratory traffic and BGP-peering analytics. Integration and automated triggering of high-powered mitigation technology closes the loop, providing an end-to-end solution with cloud-scale power to meet and defeat today's DDoS threats.

The Challenge

DDoS attacks are on the rise in volume and severity, creating greater risks for enterprises, service providers, online platforms and other digital businesses. Attacks that eclipse 10 or even 100 Gbps are the new normal, with even terabit attacks already a reality.

Meanwhile, the wide commercialization of lower-level DDoS cyberattack tools — available to launch for a fraction of a bitcoin — means that attacks are becoming an ever-present factor that need to be dealt with proactively and efficiently.

Unfortunately, traditional out-of-band means of detecting attacks are prone to inaccuracy due to the severe limitations of single-server solutions and the computational compromises they must make. As a result, online businesses — and the service providers that connect them — are increasingly falling victim to DDoS attacks.

The A10 Thunder TPS and Kentik Detect Solution

Increase the robustness and depth of your DDoS defenses by deploying an end-to-end solution from A10 Networks and Kentik.

Kentik Detect is the industry's first purpose-built big data platform for real-time network operations and DDoS detection, and is integrated with A10 Networks Thunder TPS. Users of Kentik Detect's network-wide data-scanning and learning algorithm-based anomaly detection have experienced a 30 percent increase in attack detection accuracy over traditional appliances.

Kentik Detect automatically triggers mitigation in A10 Thunder TPS, and provides ad hoc, big data analytics that returns reports across billions of rows of data in seconds.

A10 Thunder TPS, powered by the ACOS platform, offers dynamic mitigation policies, where traffic may be escalated to progressively increasing levels of scrutiny and scrubbing. A10 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.

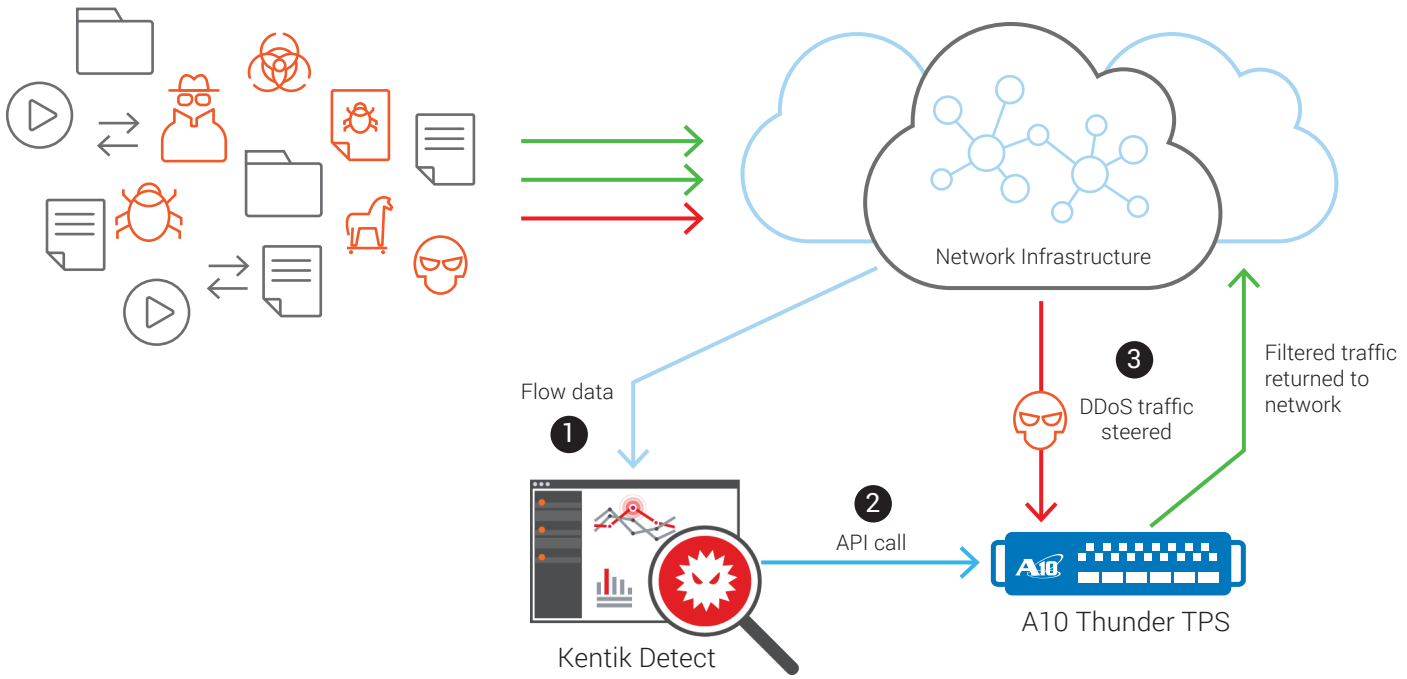
Solution Components

A10 Networks and Kentik provide a highly scalable DDoS protection and analytics solution. Featuring Kentik Detect's real-time, automated triggering of A10 Thunder TPS mitigation, the A10 and Kentik solution keeps online business traffic flowing and stops DDoS in its tracks.

1. Kentik Detect receives and unifies NetFlow, sFlow, IPFIX, BGP, SNMP and GeoIP data, applying auto-learning baselines and anomaly measurement policies to watch for DDoS attacks.
2. When attacks are detected, Kentik Detect signals A10 Thunder TPS through A10's RESTful API, called aXAPI, with information about the attack.
3. A10 Thunder TPS signals the network to redirect the suspect traffic, applies dynamic mitigation with progressively increasingly levels of scrubbing, then returns the filtered traffic to the customer network.

Features and Benefits

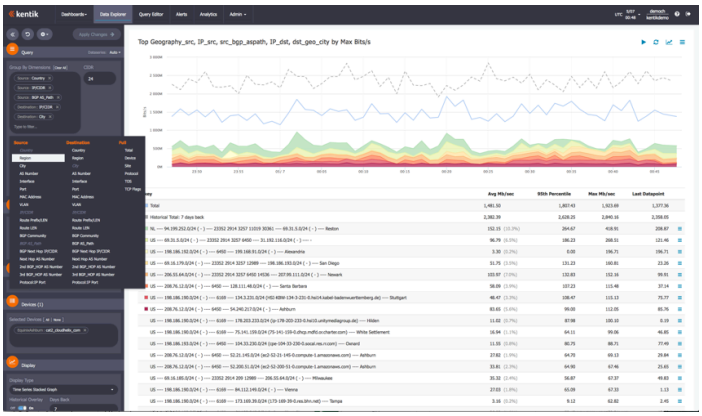
- Big data-powered detection with adaptive, learning algorithm baselining
- Automated triggering of mitigation via A10 Thunder TPS
- Support for remote-triggered black hole (RTBH) as additional emergency mitigation option
- Reduced manual configuration and maintenance
- 30 percent more accurate DDoS detection versus legacy technologies
- Powerful DDoS mitigation throughput capacity, ranging from 1 to 300 Gbps (2.4 Tbps in synchronization cluster), ensures that the largest multi-vector DDoS attacks can be mitigated effectively



Big Data Network Traffic & BGP Analysis

Kentik Detect provides the industry's most powerful network traffic analytics. Kentik Detect retains months of ingested NetFlow, sFlow, IPFIX and other traffic flow data details and fuses them with real-time BGP data gained from live routing peerings, plus geolocation, network performance metrics and SNMP interface data.

The Kentik Detect portal and REST API offer multi-dimensional, ad-hoc analytics on billions of data records with query response in a few seconds. Kentik Detect provides deep insights that aid real-time operational troubleshooting, forensic analysis, network-performance monitoring, peering analytics and capacity planning.



Increase DDoS Protection Accuracy and Visibility

Together, A10 Networks and Kentik offer improved accuracy and efficiency of DDoS protection, combined with unprecedented visibility into network traffic and performance.

A10 Thunder TPS provides the industry's most scalable and advanced solution for protecting against multi-vector DDoS attacks, while Kentik Detect offers the industry's most accurate out-of-band DDoS detection along with the industry's only big data platform for network visibility.

Next Steps

To learn more about the A10 Thunder TPS and Kentik Detect DDoS protection solution, 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-19171-EN-01
Jan 2017

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.