

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 datapowered 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 cloudscale 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.

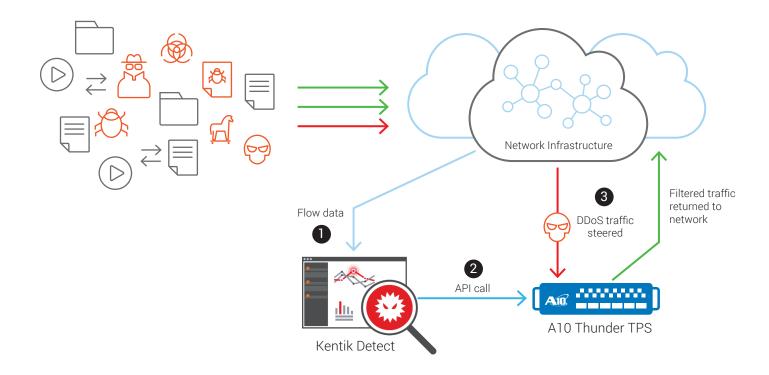
Solution Components

A10 Networks and Kentik provide a highly scalable DDoS protection and analytics solution. Featuring Kentik Detect's realtime, 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 realtime 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, networkperformance monitoring, peering analytics and capacity planning.

0 •• 949	Apply Durips:	Top Geography_sr	rc, IP_src, src_bgp_asp	path, IP_dst, dst_geo_city	by Max Bits/s					► 0 E	
a ly Dimensioni (dae al louros Daelly 3) louros 19(004 3) louros 19(7 40, 148 3) louros 19(7 40, 148 3) lourostor 19(004 3) loutostor (dy 1 4) pelo film ,	N	2 500M 2 500M									
Courty Region Ory Al Number Stantes Part			23 30 23 31	0/7 8645	0533	0015 0020	0025 0038	90.33	0.45	0.41	
PUT NACAMINI	HICABERS TO						Avg Mb/sec 9	Sth Percentile	Max Hb/sec	Last Datapoint	
648		7064					1,481.50	1,817.40	1,923.69	1,377.36	
Route Prefact.EN	Route Prefacture	Il Hatorical Total: 7 da	ke peck				2,382.39	2,628.25	2,040.15	2,358.05	
		I N 94.199.252.0	(24 (-) 23352 2914 3257 110	019 30361 69.31.5.0/24 (·) Re	nale		152.15 (13.3%)	254.67	418.91	208.87	
KP Cannudy	BGP Community BCP AL INFO	US 68.31.5.0/24	(-) 23352 2914 3257 6450 -				96.79 (L.SN)	196.23	268.51	121.46	=
		US	2/24 (-) 6450 199.168.9	11.0/24 (-) Alexandria			3.30 (0.2%)	6.00	196.71	196.71	
Not Hip AS Number Ind HOP HOP AS Number	Not Np AS Number and BCP INCP AS Number	US 68.16.179.00	24 (-) 23352 2914 3257 1298	89 196.386.183.0/24 (·) San C	lego		\$1.75 (1.5%)	131.23	160.81	23.26	-
H BOP, HOP AS Number	34107_107 #1 Survey	US 206.55.64.0/	24 (-) 23352 2914 3257 6450	0 14536 207.99.111.0/24 (-) 5	imark		123.57 (2.0%)	132.83	152.36	99.51	
Potocit/P Port	Protocol IP Port	US 208.76.12.0/	24 (-) 6450 128.111.48.0	Q24 (-) — Serta Berbera			58.09 (3.9%)	107.23	115.48	37.14	
		. US 198.186.190	.0/24 (-) 6368 134.3.231	L0/24 (H5) KBM 134-3-235-0.3654 Aub	d badenwuertenberg.de) Stu	fige1	46.47 (3.3%)	108.47	115.13	75.77	
		US 200.76.32.07	24 (-) 5450 54,240,217.0	1/24 (-) Autourn			83.65 (5.0%)	95.00	112.05	85.75	
		US 198.186.190	J/24 (·) ···· 6168 ···· 178.203.2	133.0/24 (p-178-200-233-0.hei03.unityr	rediagroup.de) Hiden		11.62 (0.7%)	87.98	100.30	0.19	
		US 198.195.190	0/24(-)	19.0/24 (75-141-199-0 dhca.mdtd.ox.cha	tecon) White Settlement		16.94 (1.1%)	94.11	99.06	46.85	
		US 198.185.153	-3/24 (·) ···· 6450 ···· 104.33.23	0.0/24 (spe 104-33-230-0.socal.res.rco	wi) Owend		11.55 (1.0%)	86.75	88.71	77.49	
		US 208.76.12.02	24 (-) 5450 52,21,145,0	(24 (ec2 52-21-145-0 compute-1 amon	naws.com) Ashburn		27.62 (1.9%)	64.20	69.13	29.64	
	Display			/24 (er2-52-300-51 0.compute-1.amazo			33.81 (2.3%)	64.90	62.46	25.65	
Dapley							25.32 (2.4%)	56.67	62.37	49.40	
			24 (-) 23352 2914 209 1298								
Display 19 7cps • Inter Nation Grad		US 68.16.185.0/	24 (-) 23352 2954 209 1298 3/24 (-) 6368 84.112.14		•		2248 (1.8%)	65.09	62.33	1.13	

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 <u>www.a10networks.com</u>.

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

Worldwide Offices

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 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.

©2017 A10 Networks, Inc. All rights reserved. A10 Networks, the A10 Networks logo, ACOS, Thunder and SSL Insight are trademarks or registered trademarks of A10 Networks, Inc. in the United States and other countries. All other trademarks are property of their respective owners. A10 Networks assumes no responsibility for any inaccuracies in this document. A10 Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice. For the full list of trademarks, visit: www.a10networks.com/a10-trademarks.