11-16-2021

Arbor Edge Defense (AED) Sales Training

Michael J. Wetherbee
University of Massachusetts Boston

A final project presented to the faculty of the

Instructional Design Master's Degree Program

University of Massachusetts at Boston

Arbor Edge Defense (AED) Sales Training

Submitted by

Michael J Wetherbee

in partial fulfillment for the requirement of the degree

MASTER OF EDUCATION

11/16/21

Approved by Dr. Domenic Screnci, Faculty

Abstract:

Due to a change in revenue policy, an organization that sells products in the DDoS attack solution space embarked on a journey to fundamentally change the strategy they employed to sell their DDoS solution. The offering from the organization was a combination of two products that provided a comprehensive DDoS solution. The solution was made up of a cloud solution combined with an on-premises appliance.

Because most of the cloud portion was owned by another organization and the profit margins were small, they decided to sell their portion to the other organization. Once sold, they decided to change the sales strategy to lead an opportunity with the on-premises appliance and augment with the cloud solution even though the typical strategy previously was vice versa. Sales behavior required change simply because the previous approach to lead with the cloud solution was easier to sell.

This training will be designed to help the sales stakeholders in understanding the value for customers in the adoption of the on-premises appliance first with augmentation from the cloud solution as a secondary priority. This training will provide the knowledge to support the new strategy and the assets for the sales stakeholders to test that knowledge to ensure full adoption.

Keywords: Corporate, Sales, Enablement, Strategy, Behavior

Table of Contents:

Instructional Design

Background Information:

NETSCOUT is an organization that is in the Distributed Denial of Service (DDoS) Security space. They sell solutions to identify and mitigate DDoS attacks against an organization's networks. These solutions initially included a Cloud Solution called Arbor Cloud and an on-premises appliance called Arbor Edge Defense or AED. DDoS attacks are designed to flood a network and overwhelm access to services and applications for customers and employees. The requested training relates to changing the message on how the organization's sales stakeholders approach an opportunity. The typical approach was to lead with the organization's cloud solution and bring in the on-premises appliance to augment the cloud solution. Cloud solutions are easier to sell because there is no installation on a customer's network, and it is easier to configure. That said, it is understood in the industry that eventually you need both types of protection to provide a comprehensive protection strategy.

Organizational Problem:

Unfortunately, the organization recently sold the cloud solution and changed the sales strategy due to the newly created discrepancy in profit margins between products after the sale. Because of this, the sales stakeholders are required to lead with the on-premises appliance because of its higher margins and then bring in a cloud solution to augment the on-premises piece to achieve the recommended and recognized best practice hybrid DDoS protection strategy.

When an organization changes the strategic direction on messaging around selling a product based on changes to the product mix, sales stakeholders like Business Development Representatives (BDRs), Account Executives (AEs), and Sales Engineers (SEs) need to be brought up to speed on how to sell with the new strategy. This can be accomplished by

highlighting use cases of the on-premises appliance that provide value to the customer but cannot be accomplished as effectively with a cloud solution, essentially providing value differentiator's that sales can use in their executive presentations.

The enablement team will be required to create a training program that will assist the sales stakeholders in meeting the new goals set by the executives to support the new strategy.

Learning Objectives:

Prior to making decisions on an Analysis plan and an instructional strategy, the desired outcome needs to be defined to drive the analysis and strategy toward that goal.

The overall program goal for all sales stakeholders is to be able to demonstrate within 1 month in the field, the ability to execute customer executive conversations and manage sales opportunities with an on-premises (AED) first approach as a foundation for DDoS protection and implementation of the recommended hybrid DDoS protection strategy. Each sales stakeholder's learning objectives are as follows based on what they will be measured on after they have completed the training.

Business Development Representatives (BDRs):

After completing the BDR learning module, BDRs will demonstrate the knowledge to secure qualified meetings on AED as a primary DDoS mitigation solution.

Account Representatives (AEs):

After completing the AE learning module, AEs will exhibit the ability to generate opportunities with AED as a customer's primary DDoS mitigation solution.

Sales Engineers (SEs):

After completing the SE learning module, SEs will be able to perform product demonstrations displaying the value AED provides as a primary DDoS mitigation solution.

Analysis Plan:

To understand the needs of each sales stakeholder in achieving the desired change in the selling strategy, the enablement team will employ a survey to the following number of constituents within each stakeholder category:

- Business Development Representatives - 6
- Account Executives - 10
- Sales Engineers - 10

The survey will focus on the areas of enablement that are usually a part of an on-boarding or ever-boarding sales program but are focused on the new strategy. This survey will provide guidance into what will be required to ensure training outcomes that learners will transfer to the field.

To further enhance this training, there were a couple of areas of focus that will be explored to determine where the training program can be improved.

One area of focus will be combining a multiple disciplinary approach so that learners can begin to understand customer's problems but also be able to discern the value of an increase in productivity or increase in costs that the problem is creating. "Third, many programs are not successful at effectively integrating multiple functional disciplines into the decision-making and problem-solving processes. This deficit begs curriculum designers and course developers to create deliberate linkages between quantitative analysis and critical thinking, create learning that is integrated across all courses, and links multiple disciplinary perspectives." (Bossche, Gijselaers & Milter, 2011, p.57)

To achieve an understanding of a customers challenges in any sales scenario and determine the increase in costs or decrease in productivity that the challenge is presenting, the salesperson

should be able to ask probing questions effectively. The training will have an interactive activity (Role Play or Surreal Play Experience) to help the learners in how to ask the right questions. "Since professional sales is a skill-oriented career, the best way to train students is using methods that emphasize on actively practicing those skills in the classroom similar to the way they will be used in the real-life job circumstances" (Saavedra & Rawal, 2021, p.2)

Since the target audience for this training will contain a wide range of ages, the design of the training should not focus on a younger audience versus an older one. The training will be valuable to all sales stakeholders no matter their age or experience simply because it is a change in strategy and messaging. "Low investment in training is particularly related to the stereotype that older workers are resistant to change, with lower learning abilities and development potential than their younger colleagues." (Lazazzara, Karpinska & Henkens, 2013 p.4)

Analysis Report:

The target audience for the Analysis Plan and the survey is the frontline sales stakeholders including BDRs, AEs and SEs. The BDR Role is an entry-level role and is typically made up of male and female learners between 20 and 25 years old. The AE group is also made up of men and women, but the ages will range from 25 to 60. Finally, the SE group is made up of men and women and slightly older due to the time required to gain the technical expertise needed for the role, usually between 30 and 60 but leaning more on the high level of that scale.

The gender breakdown of the survey participants is equal at the BDR level (3 Males, 3 Females). However, at the AE level the gender difference turns slightly in favor of males (6 Males, 4 Females). For the Sales Engineers, it is even heavier in favor of the males (8 males, 2 females). The age range in each of the stakeholder categories is typical across most sales organizations due mainly to the need to gain the required experience to execute on the job. The breakdown in

genders as you move up in experience especially technical experience, is most likely due to the higher participation rates of males to females over the past couple of decades in Science Technical Engineering and Math (STEM) programs. But since there have been efforts over the last couple of years put into getting more females involved in STEM programs earlier may be the underlying reason for the even gender participation ratio in the younger BDR group.

The survey answers tell an interesting story about the difference in-field performance of sales when leading with a cloud solution and the desired strategy to lead with the on-premises appliance. The first three questions in the survey were focused on this topic. Generally, the field prefers to lead with a cloud solution since that is how they have found success over the past five years besides the fact that it is also perceived as an easier sale. Here are a couple of example answers that display this mindset:

- Why is selling a cloud solution easier than selling an on-premises appliance?
    - *It does not need anything installed on the customer's network and takes very little configuration. We can also easily set up a proof of concept which sells itself.*
- Do customers understand the value of a hybrid solution? (Cloud & On-Premises)
    - *They do to some degree. We need to educate them on the value of the on-premises appliance and why they do not get that value from the cloud solution.*
- Have you experienced selling an on-premises appliance first or selling on-premises with cloud solution together successfully?
    - *I personally have not but have heard of a couple of people in other offices being successful at it.*

Some additional example answers are in the Appendix. I can provide a link to all 26 Survey results on Survey Monkey if required.

Instructional Strategy: The instructional strategy of the training will be an experiential strategy. It will touch on a variety of types of experiential learning including:

- Interactive Role Playing
- Experiential Success Stories
- Mentoring
- Question and Answer Activities

The approach to implementing this training will be slightly different for each sales stakeholder role participating in the training. Details for each are below:

Business Development Representative Training Module:

- Complete self-paced eLearning module on sales strategy change
- Complete the self-paced eLearning on using the sales strategy quick reference guide (QRG) which includes how to Employ Success Stories
- Participate in the QRG question and answer phone activity employing the AED Drill Down Qualifying Conversation Prompter.

Account Executive Training Module:

- Complete self-paced eLearning module on sales strategy change
- Complete the self-paced eLearning on using the executive presentation deck with differentiator use cases
- Participate in executive presentation role-play activity employing AED Drill Down Qualifying Conversation Prompter

Sales Engineer Training Module:

- Complete self-paced eLearning module on sales strategy change

- Complete self-paced eLearning module on demonstrating differentiator use cases and why they augment a cloud solution
- Participate in technical demonstration role play activity employing AED Drill Down Qualifying Conversation Prompter

Development of Instructional Materials

Introduction:

The instructional materials for the three modules have been developed over the past 6 months as part of the preparation for the sales strategy change. Everyone will take the initial eLearning to gain the overall knowledge to execute on managing conversations around the value of a hybrid and comprehensive DDoS mitigation. The remaining materials are designed to help each of the identified stakeholders in understanding what they must execute in the field to reach their specific goals

Instructional Materials:

1. Self-Paced eLearning Module PowerPoint Deck

   Employed as the basis for the eLearning module that all sales stakeholders are required to take as part of their training module. For an example see appendixes.

2. Executive Presentation Deck

   Employed during customer executive meetings to highlight reasons for on-premises appliance as foundation of DDoS protection strategy. Talking points and scripting for this deck to participate in presentation role play are embedded in the slide notes. For an example see appendixes.

3. Product Quick Reference Guide

A guide to understanding customers' challenges and roles at the customers site, objections they may have and solution we can provide during sales calls. For an example see appendixes.

4. Stopping Encrypted Traffic Attacks Use Case

Differentiator Use Case to give to customers that supports the position that on-premises appliance is the foundation of DDoS protection strategy. For an example, see appendixes.

5. Protecting Stateful Devices Use Case

Differentiator Use Case to give to customers that supports the position that on-premises appliance is the foundation of DDoS protection strategy. For an example, see appendixes.

6. Stopping Encrypted Traffic Attacks Demo Deck

Demonstration deck with slides to display how Stopping Encrypted Traffic Attacks appears in the product user interface and how it supports the position that on-premises appliance is the foundation of DDoS protection strategy. Talking points and scripting for this deck to participate in demonstration role play are embedded in the slide notes. For an example, see appendixes.

7. Protecting Stateful Devices Demo Deck

Demonstration deck with slides to display how Protecting Stateful Devices appears in the product user interface and how it supports the position that on-premises appliance is the foundation of DDoS protection strategy. Talking points and scripting for this deck to participate in demonstration role play are embedded in the slide notes. For an example, see appendixes.

Evaluation Plan:

For this training, Kirkpatrick's evaluation model was selected. This evaluation model contains two items that are very important in the corporate training world, the first is, did business metrics improve? "Many businesses are only beginning to witness the dramatic cost savings in transitioning from traditional training to e-learning, yet a few forward-thinking companies already know this is old news. They have started ambitious measurement programs to prove e-learning's positive impact on customer service, productivity, and sales." (Berry, 2000, p.2)

The second is, do they work better? Or, in other words did the training transfer to the field. "Return on expectation (ROE) is a strategic measure that best illustrates the power of reasonable evidence as opposed to proof. ROE is simply the percentage estimate of the extent to which learning's impact is met." (Berry, 2000, p.2)

Kirkpatrick's model of learning evaluation has been used for more than 50 years. The model encourages us to evaluate learning on four levels:

- Reaction – Did they enjoy the training?
- Learning – Did they pass the assessment?
- Behavior – Do they work better?
- Results – Did business metrics improve?

The most important level in Kirkpatrick's model based on my experience is, Reaction -Did they enjoy the training? This is very important in the corporate world, especially with sales folks. If you throw a prerecorded PowerPoint driven sales training out there, no one will take it or more importantly, absorb it. But if you design training based on the learner's needs that provides a salesperson with quantifiable value for their bottom line and put in some competitive interactive exercises to keep their interest, they will eat it up.

The details on activities that will make up the evaluation process and achieve the desired goals for this program are as follows:

- Interactive Role Playing
- Mentoring
- Question and Answer Activities

The approach to implementing this evaluation will be slightly different for each sales stakeholder role participating in the training. Details for each are below:

Business Development Representative Evaluation:

- Complete a QRG question and answer phone activity employing the AED Drill Down Qualifying Conversation Prompter with a mentor or manager.

Account Executive Evaluation:

- Complete an executive presentation role play activity while employing AED Drill Down Qualifying Conversation Prompter and differentiator use cases with a mentor or manager.

Sales Engineer Training Evaluation:

- Complete a technical demonstration role play activity while employing AED Drill Down Qualifying Conversation Prompter with a mentor or manager.

Once the learners have participated in these evaluation activities, further metrics will be employed to understand the effect the training has on job performance.

Business Development Representative Metric: (To be gathered in CRM)

- Qualified Meetings Scheduled with On-Premises Mitigation as Lead Product.

Account Executive Metric:

- Opportunities Closed with On-Premises Mitigation as Lead Product (To be gathered in CRM)

Sales Engineer Metric:

- Product Demonstrations with On-Premises Mitigation as Lead Product (To be gathered in CRM)

Summary:

Although this program has not been launched yet, the design has been employed successfully before. In fact, many of the facets of this program have been hailed by participants of past training through post-training surveys. We will continue post-training surveys to help identify further areas of improvement. This training program will be launched in January of 2022 and surveys will be collected in February. Ideally those responses will again help to improve further programs.

References:

Bossche, P. V. den, Gijselaers, W., & Milter, R. G. (2011). Building Learning Experiences in a Changing World / edited by Piet Van den Bossche, Wim H. Gijselaers, Richard G. Milter. (1st ed. 2011.). Springer Netherlands. https://doi.org/10.1007/978-94-007-0802-0 *1*, P 7.

Saavedra Torres, J., & Rawal, M. (2021). SURREAL PLAY EXPERIENCE FOR TEACHING SALES: LEARNING HOW TO ASK THE RIGHT QUESTIONS. Marketing Education Review, 1–11. https://doi.org/10.1080/10528008.2021.1871848

Lazazzara, A., Karpinska, K., & Henkens, K. (2013). What factors influence training opportunities for older workers? Three factorial surveys exploring the attitudes of HR professionals. International Journal of Human Resource Management, 24(11), 2154–2172. https://doi.org/10.1080/09585192.2012.725077

Martins, B. R., Jorge, J. A., & Zorzal, E. R. (2021). Towards augmented reality for corporate training. Interactive Learning Environments, 1–19. https://doi.org/10.1080/10494820.2021.1879872

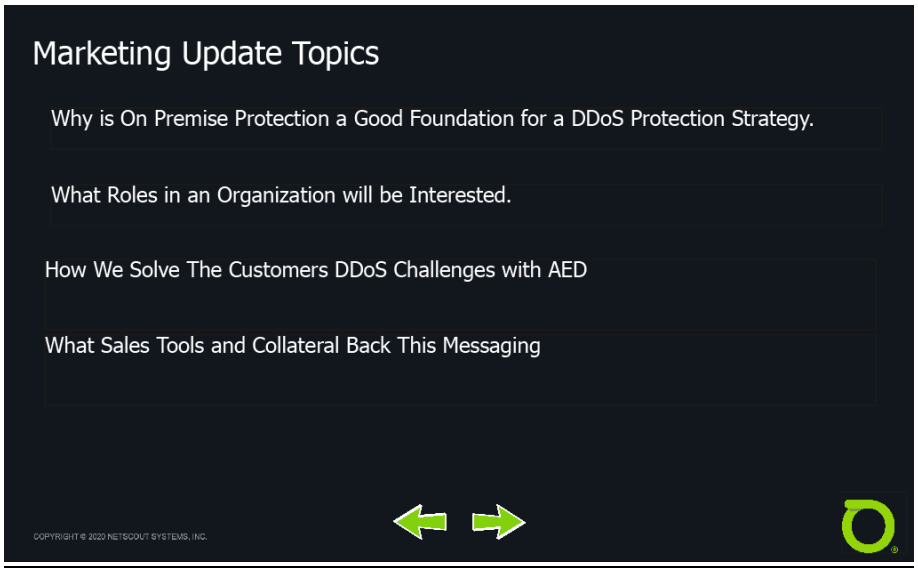
Cavalieri, S., Gaiardelli, P., & Ierace, S. (2007). Aligning strategic profiles with operational metrics in after-sales service. International Journal of Productivity and Performance Management, 56(5/6), 436–455. https://doi.org/10.1108/17410400710757132

Fergurson, J. R. (2020). The paradox of diminishing returns: Measurement and metrics for valuation of B2C sales professionals. Journal of Marketing Channels, 26(2), 141–146. https://doi.org/10.1080/1046669X.2020.1747280

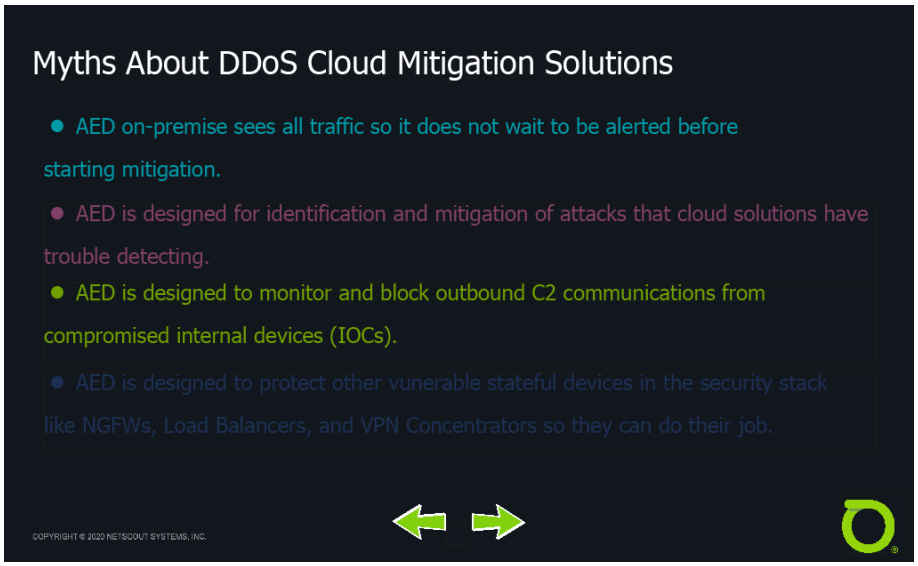
Berry, J. (2000). CORPORATE TRAINING -- THE E-LEARNING CENTER -- Companies are using metrics to justify e-learning's impact on strategic business goals. Internet Week (Manhasset, N.Y.), 61–.

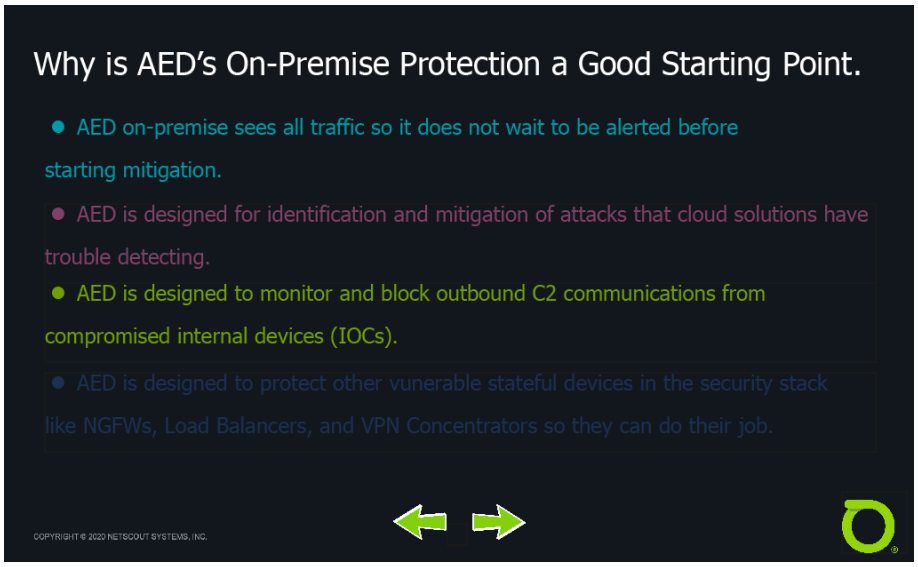
Appendixes:

1. Self-Paced eLearning Module PowerPoint Deck Example

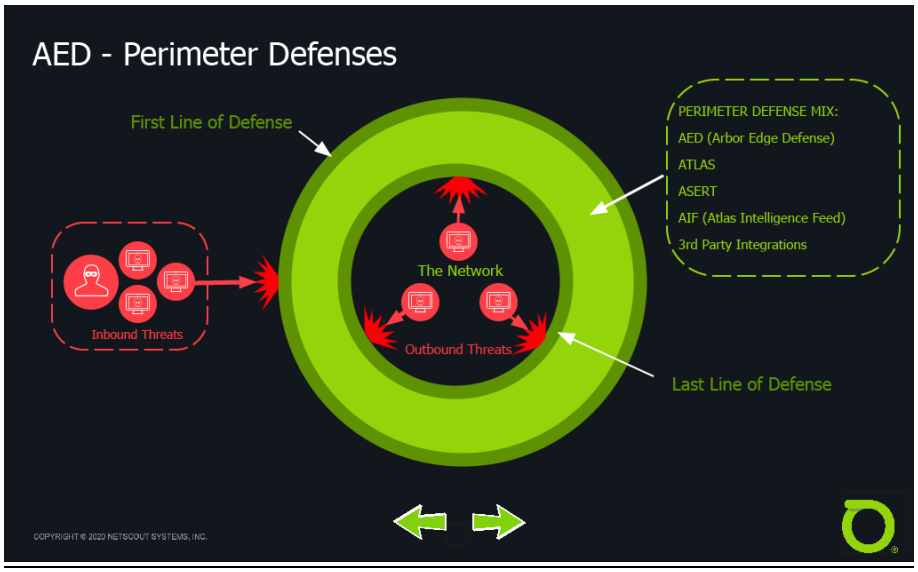

Marketing Update Topics
Why is On Premise Protection a Good Foundation for a DDoS Protection Strategy.
What Roles in an Organization will be Interested.
How We Solve The Customers DDoS Challenges with AED
What Sales Tools and Collateral Back This Messaging
COPYRIGHT © 2020 NETSCOUT SYSTEMS, INC.

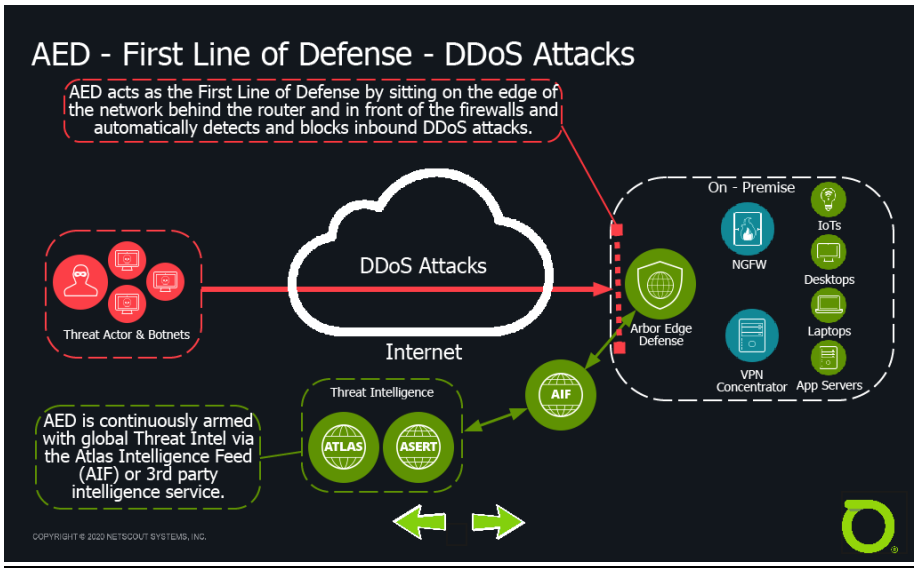

DDoS Attacks are Getting Worse.
There were 5,351,930 attacks identified in the 1H of 2021.
Attack size has see an increase of 169% over the same time last year.
One ransomware group collected $100,000,000 in the 1H of 2021.
Multivector attacks are up 230% year over year from 2020 to 2021.
COPYRIGHT © 2020 NETSCOUT SYSTEMS, INC.

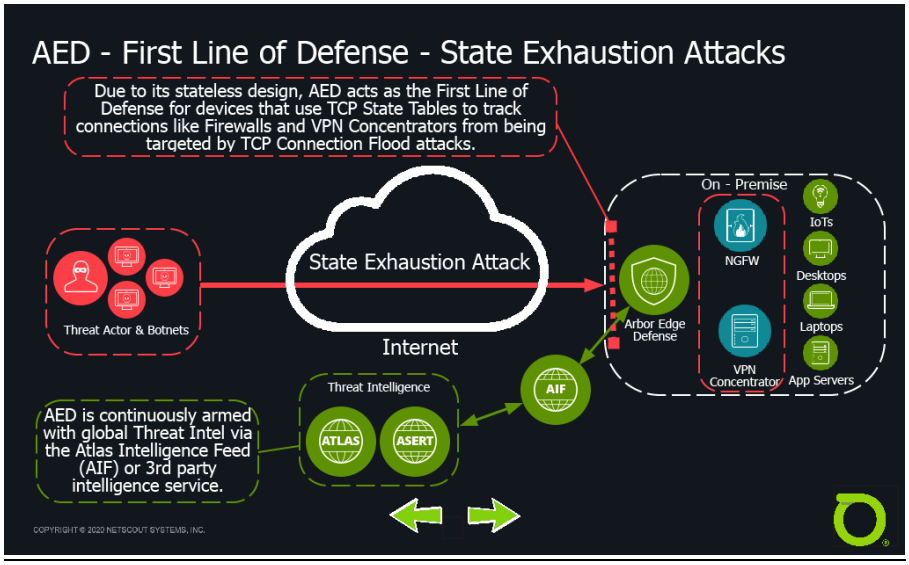

Myths About DDoS Cloud Mitigation Solutions
AED on-premise sees all traffic so it does not wait to be alerted before starting mitigation.
AED is designed for identification and mitigation of attacks that cloud solutions have trouble detecting.
AED is designed to monitor and block outbound C2 communications from compromised internal devices (IOCs).
AED is designed to protect other vunerable stateful devices in the security stack like NGFWs, Load Balancers, and VPN Concentrators so they can do their job.
COPYRIGHT © 2020 NETSCOUT SYSTEMS, INC.

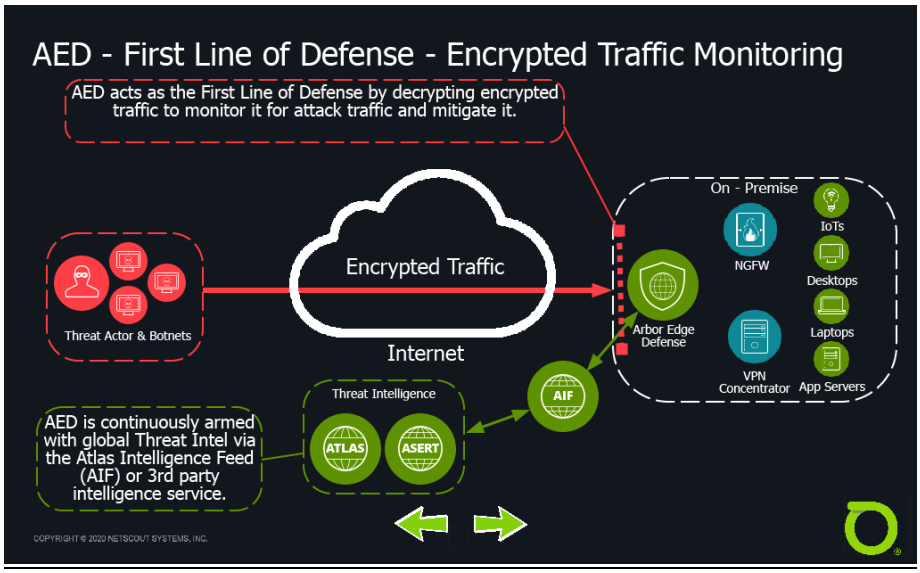

Why is AED's On-Premise Protection a Good Starting Point.
AED on-premise sees all traffic so it does not wait to be alerted before starting mitigation.
AED is designed for identification and mitigation of attacks that cloud solutions have trouble detecting.
AED is designed to monitor and block outbound C2 communications from compromised internal devices (IOCs).
AED is designed to protect other vunerable stateful devices in the security stack like NGFWs, Load Balancers, and VPN Concentrators so they can do their job.
COPYRIGHT © 2020 NETSCOUT SYSTEMS, INC.

2. Executive Presentation Deck Example




AED - First Line of Defense - DDoS Attacks
AED acts as the First Line of Defense by sitting on the edge of the network behind the router and in front of the firewalls and automatically detects and blocks inbound DDoS attacks.
Threat Actor & Botnets
DDoS Attacks
Internet
On - Premise
NGFW
IoTs
Desktops
Laptops
Arbor Edge Defense
VPN Concentrator
App Servers
Threat Intelligence
ATLAS
ASERT
AIF
AED is continuously armed with global Threat Intel via the Atlas Intelligence Feed (AIF) or 3rd party intelligence service.
COPYRIGHT © 2020 NETSCOUT SYSTEMS, INC.


AED - First Line of Defense - State Exhaustion Attacks
Due to its stateless design, AED acts as the First Line of Defense for devices that use TCP State Tables to track connections like Firewalls and VPN Concentrators from being targeted by TCP Connection Flood attacks.
Threat Actor & Botnets
State Exhaustion Attack
Internet
On - Premise
NGFW
IoTs
Desktops
Laptops
Arbor Edge Defense
VPN Concentrator
App Servers
Threat Intelligence
ATLAS
ASERT
AIF
AED is continuously armed with global Threat Intel via the Atlas Intelligence Feed (AIF) or 3rd party intelligence service.
COPYRIGHT © 2020 NETSCOUT SYSTEMS, INC.


AED - First Line of Defense - Encrypted Traffic Monitoring
AED acts as the First Line of Defense by decrypting encrypted traffic to monitor it for attack traffic and mitigate it.
Threat Actor & Botnets
Encrypted Traffic
Internet
On - Premise
NGFW
IoTs
Desktops
Laptops
VPN Concentrator
App Servers
Arbor Edge Defense
Threat Intelligence
ATLAS
ASERT
AIF
AED is continuously armed with global Threat Intel via the Atlas Intelligence Feed (AIF) or 3rd party intelligence service.
COPYRIGHT © 2020 NETSCOUT SYSTEMS, INC.

3. Sales Strategy Quick Reference Guide Example

NETSCOUT

I QUICK REFERENCE GUIDE I

Arbor Edge Defense (AED)

Top Persona's to Call Into:

1. Network Teams: Director/Manager of Network Operations, Network Engineer/Architect, Director/Manager Network Infrastructure.

2. Security Teams: Director/Manager of Security Operations, Security Analyst, Security Architect, Threat Intelligence Researcher.

3. Channels and Partners: Chief Information Security Officer (CISO), Chief Technology Officer (CTO), Vice President of IT.

Differentiators

Deployed at the network perimeter in between firewall and internet router; and using stateless packet processing technology, NETSCOUT® AED provides a first and last line of smart, automated defense.

First Line of Defense:

- Inbound DDoS Attacks: NETSCOUT AED provides best of breed, DDoS attack protection.
- NETSCOUT AED can stop inbound volumetric DDoS attacks,application layer attacks, and TCP-state exhaustion attacks that target stateful devices such as firewalls. AED's Cloud Signaling feature can automatically reroute large attack traffic to one of NETSCOUT Arbor Cloud (or a MSSP's) scrubbing centers for cloud-based mitigation.
- Inbound Indicators of Compromise (IOCs): Armed with potentially millions of reputation-based IoCs from NETSCOUT ATLAS Intelligence Feed or 3rd parties (via support for STIX/TAXII), NETSCOUT AED can stop inbound IOCs in bulk --> which takes pressure off stateful security devices such as NGFWs.

Last Line of Defense:

- Missed by existing security stack, NETSCOUT AED blocks outbound communication from compromised internal devices to known bad IP addresses, domains, URLs, geographies --> helps stop the further proliferation of malware within an organization and ultimately avoid a data breach from occurring.

Integration with Existing Security Stack:

- REST API, support for Syslog, CEF, LEEF and STIX/TAXII, enable NETSCOUT AED to be a fully integrated component of an organization's existing security stack and processes --> reduces complexity and allows security teams to enforce their threat intelligence at the network perimeter.

COMPETITORS	COMPETITOR LIMITATIONS	ARBOR DIFFERENCE
Radware (DefensePro)	• DefensePro (Radware's on premise device) touts their BDoS (Behavioral DoS) technology which completely relies on users to configure the correct initial baselines, which is difficult to do and produces many false positives.	• AED does not rely upon baselines and has attack automated out-of-box, attack mitigation capabilities. • AED and Arbor Cloud provide an automated, hybrid DDoS attack protection solution protection.
Akamai	• Akamai is a cloud-only solution that will miss application layer attacks. • Time to-mitigation can take upwards of 20+ minutes to address even the smallest attacks.	• AED is an on-premise solution that can stop all types of DDoS attacks. In the event of a large attack, AED's Cloud Signaling feature automatically reroutes attack traffic to one of Arbor Cloud's global scrubbing centers. for mitigation. • Real-time on-premise protection and off-premise mitigation in seconds.
F5	• High false-positive performance tested by NSS Labs with 7.3% impact to legitimate traffic. • ADC architecture inherently stateful, thus vulnerable to state-exhaustion and require symmetric traffic paths.	• Lowest false positives among solutions tested by NSS Labs with only 0.4% impact to traffic. • Stateless architecture immune to state exhausting DDoS attacks, plus ideal for asymmetric traffic.

Qualifying Questions

- Have you recently experienced a DDoS attack?
- What is your current strategy to protect and mitigate against DDoS attacks?
- What impact would your company suffer if your web-based application/service went offline (lost revenue, customer confidence)?
- Has your firewall ever been impacted by a DDoS attack?
- How would you know if you were suffering an application-layer DDoS attack?
- Is your firewall struggling to stop Indicators of Compromise (IOCs) and other advanced threats?
- Do you consume multiple sources of cyber threat intelligence or use a Threat Intelligence Platform (TIP)?
- Are you enforcing your cyber threat intelligence ad the network perimeter?

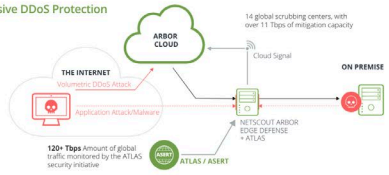
330+ Arbor Service Provider Customers throughout the world

Recognized as one of the 5 most amazing technologies DARPA helped invent

---

MYTH	REALITY
My firewall and IPS will stop DDoS attacks.	Perimeter solutions such as firewalls and IDS/IPS are vital part of a security posture. However, they are susceptible to some types of attacks due to their stateful inspection of network connections. You need a dedicated, on-premise, stateless solution like AED; which is deployed in front of firewalls/IPS to protect them from DDoS attacks.
My ISP will stop any DDoS attacks.	Today's attacker uses a dynamic combination of volumetric, TCP-state exhaustion and application layer attack vectors. Best practice advises a hybrid approach to DDoS protection. That is, the best place to stop small, more stealthy application-layer attacks is on premise. The best place to stop large attacks in in the cloud. AED and Arbor cloud provide intelligently integrated hybrid DDoS protection.
DDoS attacks are low risk for me.	There are plenty of motivations: from hacktivism, to competitive take out, to nation state sponsored attacks. Attacks can be used for extortion or as a smoke screen for an advanced threat campaign. The combination of "ease of use" and "motivations" is causing a dramatic increase in the number of DDoS attacks against all organizations, industries, and geographies. AED is continuously armed with global threat intelligence from ATLAS.
Advanced threats are a greater concern.	Sophisticated attackers are using a combination of different attack tools and techniques (e.g., phishing, social engineering, and DDoS attacks) to penetrate organizations and steal confidential data. 26% saw DDoS attacks used in advanced threat campaigns as a diversion to cover up exfiltration of data. AED has the ability to act as a first and last line of defense stopping not only DDoS attacks but all communication to known bad sites.

Comprehensive DDoS Protection



Key Data Points from 14th Annual Worldwide Infrastructure Security Report

- Globally, the number of DDoS attacks was flat year over year, with 6.13 million. But that's still 16,794 attacks/day and 699 attacks/hour.
- Largest DDoS attack reported was 1.7Tbps. Average DDoS attack sizes are now above 1Gbps - capable of saturating the Internet connectivity of many enterprises.
- Ratio of DDoS attack types = Volumetric (42%), Application layer (17%) and TCP sate Exhaustion (31%, which grew 2x more than prior year, 54% of respondents reported their firewalls failing).
- 67% of the enterprises observed a multi-vector DDoS attack.
- Attacker has low bar to entry due to readily available and cheap (less than $5/hr) DDoS attack tools and services.
- For 2018, the average cost of downtime associated with internet service outages caused by DDoS attacks was $221,836.80.

Key Product Specs

- AED comes in a variety of form factors (e.g. 2U appliance, virtual) and pricing options (e.g. perpetual appliance, perpetual software only, software subscription).
- AED mitigation capacities range from sub 100Mbps to 40 Gbps.
- AED has an option SSL decryption module which can be added to appliance.
- AED can be offered as the on-premise component of Arbor Cloud DDoS Protection Services which has over 14 scrubbing centers with over 11 Tbps of mitigation capacity.
- AED can consume and enforce up to 3+ Million IoCs from ATLAS or 3rd party (via STIX/TAXII) threat intelligence sources.
- AED's use of open standards such as Syslog (CEF, LEEF), REST API and support for STIX/TAXII enable it to integrate into security stack and process.

NETSCOUT

Corporate Headquarters
NETSCOUT Systems, Inc.
Westford, MA 01886-4105
Phone: +1 978-614-4000
www.netscout.com

Sales Information
Toll Free US: 800-309-4804
(International numbers below)

Product Support
Toll Free US: 888-357-7667
(International numbers below)

4. Stopping Encrypted Traffic Attacks Use Case Example

NETSCOUT

| USE CASE |

Stopping Attacks in Encrypted Traffic

Encryption is one of the most basic necessities in the security arsenal. It's what makes it possible for banks to offer online banking and funds transfers, or for consumers to make purchases online using their credit or debit cards. It's what protects the public's online interaction with government agencies or health care providers. Such services enable access to a wealth of personal, confidential, and financial data. So it should surprise no one that encrypted services are prime targets of DDoS attacks. Identity thieves and cyber criminals can have a field day if they succeed in breaking web service encryption.

Threat

According to NETSCOUT® Arbor's 13th Annual Worldwide Infrastructure Security Report (WISR), attacks targeting encrypted web services have become increasingly common in recent years. Among enterprise, government, and education (EGE) respondents, 53% of detected attacks targeted encrypted services at the application layer. And 42% of respondents experienced attacks targeting the TLS/SSL (Transport Layer Security/Secure Socket Layer) protocol governing client-server authentication and secure communications.

One helpful statistic coming out of the 13th WISR though, is that enterprises are recognizing that traditional firewalls and intrusion prevention systems are insufficient in confronting sophisticated DDoS attacks – particularly encrypted attacks targeting encrypted services. Encryption is essential but cannot be relied upon on its own to thwart determined and sophisticated attackers. Given the critical nature of most encrypted applications and services, a single successful attack can have devastating consequences.

Risk

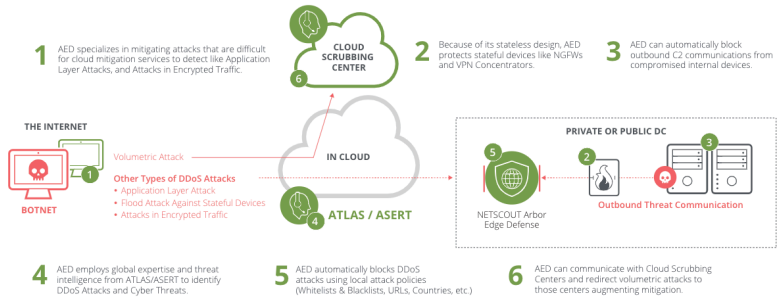
Reputational and brand damage are frequently cited as the worst consequences of a DDoS attack. Additionally, nothing could be more damaging to an organization's reputation than to compromise the secure services like banking or online purchases that consumers have come to trust and rely upon every day with hardly a second thought. Institutions need to take measures that go beyond encryption to ensure the integrity and availability of their most critical services and continued credibility of their reputation and brand.

Investigation

DDoS attacks targeting encrypted services tend to fall into four categories:

- Attacks that target the SSL/TLS negotiation, commonly known as the "handshake," which determines how two parties to an internet connection will encrypt their communications.
- Protocol or connection attacks against SSL service ports, which seek to exploit SSL vulnerabilities.
- Volumetric attacks targeting SSL/TLS service ports, which overwhelm port capacity with high-volume traffic floods.
- Application-layer attacks against underlying service running over SSL/TLS.

I USE CASE I Stopping Attacks in Encrypted Traffic



Attackers are unrelenting in their assaults on high-value encrypted targets. To make matters worse, attackers often use SSL/TLS encryption themselves to hide nefarious activity. The high volumes of encrypted internet traffic that traverse networks without being inspected, make it easy for malicious actors to hide among legitimate traffic, all while preparing to unleash attacks on secure HTTPS services. A key component of a security arsenal, therefore, is the ability to decrypt and inspect encrypted traffic securely and attest to its authenticity without slowing, disrupting or compromising legitimate traffic.

Another area of concern regarding decrypting and scanning packets is where their decryption is executed. Many organizations do not want their traffic being decrypted off site or by a cloud service because it may require sharing private certificates with the cloud provider, which is a security risk that many Enterprises aren't willing to take. In some situations, cloud providers themselves don't want to have to be responsible for managing private keys and the associated liability risks if the keys are leaked or exposed from their systems.

While decryption is not always necessary for successful mitigation, there is clearly a growing need for scalable solutions for decrypting packets that will expose malicious traffic.

Mitigation

Operators and hosts of secure web services increasingly recognize the need for purpose-built on-premise DDoS Mitigation Systems as the only effective option for mitigating DDoS attacks on encrypted traffic. NETSCOUT Arbor Edge Defense® (AED) allows the Enterprise to segment the decryption and application-layer mitigation (which often is done at lower volume) from the cloud while still having the cloud service for coverage against volumetric attacks. AED's decryption capabilities, include support for Perfect Forward Secrecy (PFS) through an active TLS Proxy, dedicated hardware-based decryption, and support for many different cipher suites.

Summary

Understanding the impact a DDoS attack against secure encrypted services could have on your organization's reputation and brand should be enough to drive an initiative to find a solution. Having the knowledge that decrypting traffic for inspection in the cloud could lead to potential degradation of the security of the organization's private keys should bolster the need to execute decryption, inspection, and re-encryption with an on-premise, purpose-built DDoS-mitigation solution like AED.

NETSCOUT.

Corporate Headquarters
NETSCOUT Systems, Inc.
Westford, MA 01886-4105
Phone: +1 978-614-4000
www.netscout.com

Sales Information
Toll Free US: 800-309-4804
(International numbers below)

Product Support
Toll Free US: 888-357-7667
(International numbers below)

NETSCOUT offers sales, support, and services in over 32 countries. Global addresses, and international numbers are listed on the NETSCOUT website at: www.netscout.com/company/contact-us

5. Protecting Stateful Devices Use Case Example

NETSCOUT

I USE CASE I

Protecting Your Stateful Devices

DDoS attacks are rising so much that for the first time in history, the annual number of observed DDoS attacks crossed the 10 million attack threshold, with NETSCOUT's ATLAS Security Engineering and Response Team (ASERT) seeing 10,089,687 attacks over the course of the last year. Furthermore, as the pandemic lockdown took effect last spring, cybercriminals launched 929,000 DDoS attacks in May, the single largest number of monthly attacks we've ever seen. These attacks targeted critical work/learn-from-home stateful infrastructure such as firewalls and Virtual Private Network (VPN) concentrators.

Challenge

The attackers are not only increasing their frequency, but they are also increasing the complexity. 58% of Worldwide Infrastructure Security Survey (WISR) enterprise respondents are now reporting multi-vector attacks, which is up from 38% a year earlier. There was an attack recorded in the 2nd half of 2020 that employed 26 attack vectors in a single attack, which is a new record. These complex attacks are a dynamic mixture of state-exhaustion, volumetric and application-layer attacks. An attacker will run multiple attack types at the same time or alternately, which makes it hard to defend.

Increases in how networks are accessed by users and other devices during the rise in work-from-home populations due to the pandemic, are also a contributing factor to the breakdown of business continuity. The cybercriminals know corporations are more exposed while employees are working remotely and that's all the motivation they need to launch targeted attacks, which can crash servers and burden systems of any size. Some of the typical targets for the bad guys are stateful devices like firewalls and VPN devices. In fact, 83% of WISR enterprise respondents reported DDoS attacks in which overloaded firewalls and/or VPN devices contributed to an outage, which is up 21% from 2019.

Threat

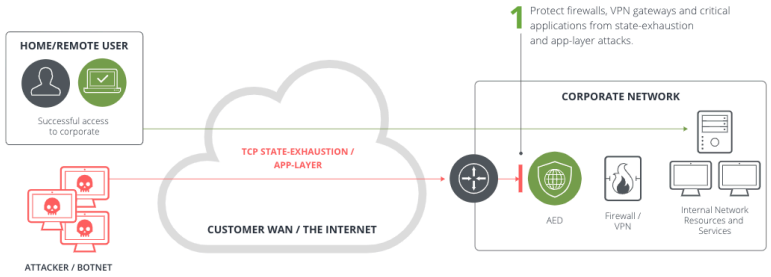
Firewalls, VPNs and other security products are essential elements of a layered-defense strategy, but they are designed to solve security problems that are fundamentally different from dedicated DDoS detection and mitigation products. The problem is that Firewalls and VPNs are typically stateful devices. Being stateful means they are using tables to collect connection details like IP addresses, ports and timestamps. The memory for these tables is limited, and even high-performance devices capable of handling millions of connections are vulnerable to flood type attacks that are designed to overwhelm these systems, which means they are vulnerable to DDoS attacks and often become the targets themselves. Since many stateful devices are also targets or partial targets of multi-layered attacks, they also require protection. Even a low-volume attack can exhaust resources on VPN concentrators and firewalls. Crafted attack volumes as low as a couple of Mbps can bring network firewalls to a point where they can't handle any newer connections.

To have adequate protection against DDoS, you need a solution that can protect against all types of attacks and guard your stateful devices.

Risk

The availability of business-critical services is essential — and not just to avoid loss of revenue. Availability of services also strengthens the company's reputation in a market and contributes to sustainable business success. Cyber resilience refers to an entity's ability to continuously deliver an intended outcome, despite adverse cyber events. Adverse cyber events are those that negatively impact the availability of networked IT systems plus associated information and services.

I USE CASE I Protecting Your Stateful Devices



VPNs

Historically, VPNs weren't in constant use, but they've become the backbone of business during the COVID-19 pandemic. This means companies are far exceeding standard capacities and straining access to critical applications and resources. Now more than ever, a relatively minor DDoS attack could bring down a VPN gateway, causing the business to shut down for remote, home-based users. As pandemic lockdowns get lifted and society comes back to normal, many organizations will still offer at least a hyrbid, work-from-home environment thus maintaining the importance of protecting the VPN gateway.

Firewalls

Firewalls act as policy enforcers to prevent unauthorized access to data. While such security products effectively address "network integrity and confidentiality," they fail to address a fundamental concern regarding DDoS attacks—"network availability." A Next-Generation Firewall (NGFW) is a cybersecurity solution to protect network fronts with capabilities that extend beyond traditional firewalls. While traditional firewalls detect suspicious traffic and block network access based on a predefined blacklist, NGFWs include additional features such as intrusion prevention and deep-packet inspection. That said, even NGFWs do not provide adequate protection at this point, and they are often themselves the target.

Mitigation

Arbor Edge Defense® (AED) is an on-premise, always-on, stateless, DDoS-specific, mitigation solution. AED can identify and mitigate attacks up to 40 Gbps, and because of its stateless design, it is not susceptible to state-exhaustion attacks that target stateful devices such as VPN gateways, firewalls or load balancers. AED is designed to sit on the edge of the network between the Internet and your network's stateful devices and protect them from the very attacks designed to take them down. In the event of a large volumetric attack that's designed to saturate the Internet circuit, AED's cloud signaling feature will automatically route traffic to a cloud-based, DDoS-protection like NETSCOUT Arbor Cloud or one from your ISP.

In general, AED can eliminate the DDoS threat and the danger to your stateful devices all while assisting your organization in continued efforts to maintain availability to business-critical applications and services.

Summary

DDoS attacks are obviously increasing in frequency and complexity when measured by the amount and variety of vectors involved in each attack. And now that more employees are working from home due to the pandemic, attackers are taking advantage of the increased threat surface provided by VPN devices and firewalls. In fact, even though these devices are an integral part of the security stack and the network protection strategy, outages have increased around targeting of these stateful devices. If it has not already, this increase in attacks will degrade the availability of your services for your end users or customers, which will affect your bottom line. The best practice for DDoS protection is a hybrid approach, which includes a cloud-based and on-premise, in-line, stateless, DDoS-protection solution like AED to protect your stateful devices from further attacks.

NETSCOUT.

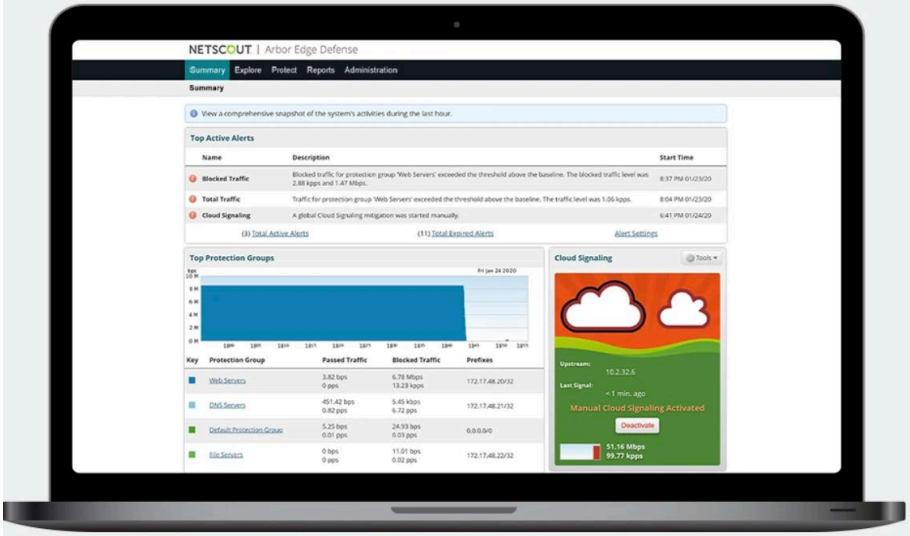
Corporate Headquarters
NETSCOUT Systems, Inc.
Westford, MA 01886-4105
Phone: +1 978-614-4000
www.netscout.com

Sales Information
Toll Free US: 800-309-4804
(International numbers below)

Product Support
Toll Free US: 888-357-7667
(International numbers below)

NETSCOUT offers sales, support, and services in over 32 countries. Global addresses, and international numbers are listed on the NETSCOUT website at: www.netscout.com/company/contact-us

6. Stopping Encrypted Traffic Attacks Demo and Script Example



Stopping Encrypted Traffic Attacks

Display how AED decrypts scans and re-encrypts traffic for embedded attacks.

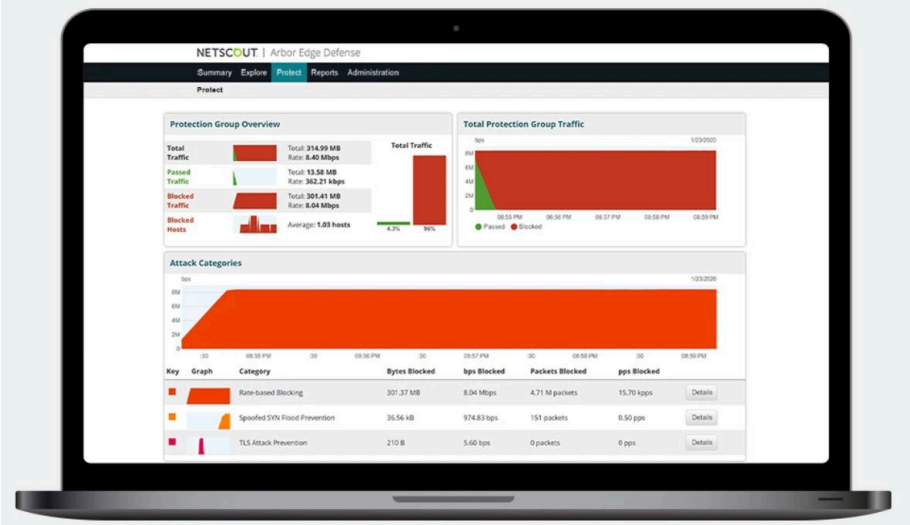
Overview/Summary

First log into AED. Display the AED Summary page first and show how you get immediate understanding of where traffic is coming from (Internet) and where it is going to within the network. This is also the point where we talk about the various other aspects of the AED. Its ability to be actively blocking or just monitoring traffic from a system wide perspective as well as individual Protection groups (PG). Easy escalation during attacks from a "normal" Low mode to an "aggressive" High mode. NOTE: STIX are either enabled or disabled on the PG. Visibility into AIF and TIG functions (ATLAS) Inbound/Outbound and STIX blocking right on the summary page.

Encrypted Traffic Monitoring

From the summary page pick the Web Servers PG. Show the attack categories and from the ATLAS Threat Categories choose the drop down circle and choose Blocked hosts selection. You will be taken directly to the blocked hosts search page showing several entries. Look for the entry where the source/destination is **See Table 1 below** and click details. A pop up will show the host(s) being blocked and the traffic blocked. At the bottom of the pop up you will see an entry labeled Threats. Show that the threat is **See Table 1 below** and note the threat and the time it was blocked.

7. Protecting Stateful Devices Demo and Script Example



Demonstrating Protection of Stateful Devices

Show how we identify and identify attacks against system stateful devices.

Overview/Summary

First log into AED. Display the AED Summary page first and show how you get immediate understanding of where traffic is coming from (Internet) and where it is going to within the network. This is also the point where we talk about the various other aspects of the AED. Its ability to be actively blocking or just monitoring traffic from a system wide perspective as well as individual Protection groups (PG). Easy escalation during attacks from a "normal" Low mode to an "aggressive" High mode. NOTE: STIX are either enabled or disabled on the PG. Visibility into AIF and TIG functions (ATLAS) Inbound/Outbound and STIX blocking right on the summary page.

Stateful Devices

From the summary page pick the Web Servers PG. Show the attack categories and from the ATLAS Threat Categories choose the drop down circle and choose Blocked hosts selection. You will be taken directly to the blocked hosts search page showing several entries. Look for the entry where the source/destination is **See Table 1 below** and click details. A pop up will show the host(s) being blocked and the traffic blocked. At the bottom of the pop up you will see an entry labeled Threats. Show that the threat is **See Table 1 below** and note the threat and the time it was blocked.

8. AED Drill Down Qualifying Conversation Prompter

AED Drill Down Qualifying Conversation Prompter:

This question guide is designed to assist you in how to ask the list of qualifying questions and generate follow up questions to get the most information possible in a short period of time while also encouraging the customer to admit the problem they are experiencing and the impact it is having.

Question Drill Down Structure:

1- Ask one of the Sample Questions

2- Summarize the answer given and the ask another open-ended question. This can be specific to a part of the answer or for the whole answer.

   a. Example:

      i. Question: Have you recently experienced a DDoS attack?

      ii. Answer: We are not completely sure but it seemed we had an outage of an application server last week for no reason.

      iii. Some Example Replies: (Do not be afraid to act confused, See Columbo TV Series)

         1. So, you are not sure that there was an attack, how do you monitor your traffic to identify an attack?
         2. So, you know that you had an outage, what else could have caused that?
         3. So, you know you experienced an attack, what DDoS protection do you employ?

3- Continue this question-and-answer methodology until you have captured all relevant information for the question.

AED Drill Down Qualifying Conversation Prompter:

This question guide is designed to assist you in how to ask the list of qualifying questions and generate follow up questions to get the most information possible in a short period of time while also encouraging the customer to admit the problem they are experiencing and the impact it is having.

Question Drill Down Structure:

1- Ask one of the Sample Questions

2- Summarize the answer given and the ask another open-ended question. This can be specific to a part of the answer or for the whole answer.

   a. Example:

      i. Question: Have you recently experienced a DDoS attack?

      ii. Answer: We are not completely sure but it seemed we had an outage of an application server last week for no reason.

      iii. Some Example Replies: (Do not be afraid to act confused, See Columbo TV Series)

         1. So, you are not sure that there was an attack, how do you monitor your traffic to identify an attack?
         2. So, you know that you had an outage, what else could have caused that?
         3. So, you know you experienced an attack, what DDoS protection do you employ?

3- Continue this question-and-answer methodology until you have captured all relevant information for the question.