Arbor Edge Defense (AED)

How It Works and Where It Lives in the Network

First and Last Line of Defense

Organizations are under constant threat from all types of advanced cyber threats, those can be DDoS attacks, ransomware, phishing attempts or compromised BYOD and IoT devices.

By sitting between the router and the firewall, NETSCOUT® Arbor Edge Defense (AED) has been built to stop inbound threats and outbound communication from compromised hosts. In other words, while other security devices focus on integrity and confidentiality, AED focuses on availability threats.

In order to help security teams by providing best of breed cybersecurity solutions AED, has been designed with a stateless packet processing engine (in addition to stateful FWs), RESTAPI and STICS/TAXII capabilities (to be integrated in customers security stacks). AED is also capable of processing and exploiting reputation-based threat intelligence received from NETSCOUT's ATLAS® Threat Intelligence or 3rd parties.

Focus on the Customer Edge

AED protects enterprises from both incoming and outgoing threats, it can then help to maintain connectivity towards customers premises. That is key for applications and services available on site but also for all remote and cloud-based tools mandatory for enterprises to guarantee the continuity of their business.

Two options can be offered, physical and virtual appliance with inspection capabilities from 100Mbps up to 40Gbps (up to 28Mpps). AED solution can also enable decryption of SSL and TLS for security inspection by addition of hardware security and cryptographic acceleration modules.

Each AED comes with a local GUI, however multiple instances can be put in a put in network to be managed by an AED manager to use config templates and centralize management and administration. In addition, AED propose different type of usages and associated strategies depending on expertise and engagement level of each end user. AED is able to run automatic protection services so the user can limit his duty to monitoring that's hands-off interaction. Another option is to customize security setting over time in reaction to received attacks. Finally, more advanced users can plan the organization's protection policies.

NETSCOUT Arbor Edge Defense is then suitable for all types of customer locations, Data Centers, HQ and branch offices. The solution offers the capacity to protect end users from both incoming and outgoing threats and can be integrated with SEIM and centralized management system to facilitate day to day security operations.

AED can be installed in monitoring mode only (inactive) to collect info but not act on the traffic. It is configurable to enable hardware and/or software bypass (fail open) or disconnect (fail close).

BENEFITS AND POSSIBILITIES

AED functionalities and possibilities can be gathered into four main topics

1. **Define protection setting:** Automatically protect against behavior based, or signature-based threats. Create custom protection settings for a specific group of hosts. Configure automatic actions for protection groups associated with thresholds, those are TCP authentication or HTTP authentication to prevent Spoofed SYN Flood and protection level modification.
2. **Attack countermeasures:** Actions can be taken manually or configured to start automatically while an attack is detected. Traffic mitigation (traffic cleaning) is the most common, AED allows also to automatically change the protection level, signal to a cloud service provider mitigation system to deal with volumetric attacks.
3. **Monitoring and visibility:** AED monitors the system's operations (interfaces, synchronization, health...) and detected attacks are reported by alerts. Network traffic graphs are available globally and per protection groups (number of hosts). There is also a possibility to capture traffic (both incoming and outgoing) per protection group or per interface to allow packet analysis and more accurate troubleshooting.
4. **Management and security stack integration:** AED can be polled by third party monitoring system. The solution can also be integrated with a TIP/SEIM (using STICS/TAXII for example). The system functionalities can also be enhanced via REST/API available interface. AED's also interact with cloud mitigation platform and ATLAS Threat Intelligence. AED is manageable using local GUI or AED management system for centralization and harmonization purposes. AED can also be configured using CLI where this tool is more commonly used for installation and upgrades.

Robust to State Exhaustion

Unlike firewalls or load-balancers which keep connection information as long as the session is up, AED perform real-time Layer 3 to Layer 7 packet and event countermeasures without keeping session table entry during session lifetime. In this way, memory and CPU are not affected by state exhaustion attacks and AED can protect customer network and handle this kind of threats.

...while other security devices focus on integrity and confidentiality, AED focuses on availability threats.

vAED

vAED is the virtual machine version of AED that runs on a hypervisor. vAED contains all of the AED software packages and configurations (including software bypass in case of failure)

The following orchestrators are supported: Cloud-Init v0.7.6, Openstack Kilo and Mitaka series, OpenStack Heat, OpenStack Tacker, Ansible, Nokia Cloudband, Cisco NSO/ESC, Cisco NFVIS, Amdocs, Netcracker and other ONAP or ETSI NFV management and orchestration technologies

vAED is compatible with VMware vSphere 5.5+ and VM kemel 3.19 QEMU 2.0 hypervisors.

vAED requires a minimum of 2 vCPUs; 6GB of memory: 6 GB and 100 GB of storage space. The virtual appliance can deliver up to 1Gbps (or 910 Kpps) inspected traffic per appliance.

Arbor Enterprise Manager

AEM is a management tool which allows central management and configuration of up to 50 AED's. Common configurations and specific ones (protection groups, blacklists/whitelists, outbound threat filter) are propagated to AED's. AEM also gives the possibility to view aggregated and specific graphs and alerts. It's also possible to launch protection actions (mitigation, protection level modification ...) in response to an attack.

ATLAS Intelligence Feed

AIF contains information about the latest advanced threats, botnets, and web crawlers that our Active Threat Level Analysis System (ATLAS) has identified. AED can use this information to detect threats (malformed/invalid DNS or SIP requests, HTTP messages and Botnet packets), block attacks, and allow legitimate search engine web crawlers to access your network. Updates can be done automatically or upon request on the GUI.

AED protects enterprises from both incoming and outgoing threats, it can then help to maintain connectivity towards customers premises.

STICS/TAXII

AED can accept the IOCs in STIX 2.0 feeds that are sent from TAXII 2.0 clients in order to identify and block any traffic that matches the STIX IOCs in the TAXII collections.

Protection Level

AED proposes Three protection levels and associated setting and behavior (rate-based threshold, specific countermeasures like filters). Those levels apply globally or per protection group (set of hosts):

- **Low (under normal conditions):** there is no tolerance for false positives.
- **Medium (during significant attack):** The protection settings are stricter. Clean traffic that is unusual might be blocked.
- **High (during heavy attack):** This level provides the most aggressive protection but it carries risks. Blocking some clean traffic is acceptable as long as most of the hosts are protected.

Protection Groups and Server Types

In order to protect a set of hosts, user should define a protection group containing the IPs and identify the server type of the machines (ex. Web, DNS, FTP, VPN ….) so predefined protection setting can be applied. Server type determines application-specific data to be collected and displayed by AED for that group. Note that custom server type can be created, and settings customized. AED supports a maximum of 100 protection groups. Protection level (low, med, high) and mode (active/inactive) can be configured per protection group.

Traffic Profiling and Rate-Based Protection

AED can simplify the configuration of certain rate-based protection settings by learning typical network behaviors and suggesting values that are appropriate for your network. AED can then suggest values to block traffic over some thresholds like Bits/packets per Second, DNS Query/ NXDomain Rate Limit, HTTP Request Limit, maximum bps for UDP/ICMP, SIP Source Limit, maximum bps/pps for fragmented packets.

Regular Expressions Filtering

To identify malicious traffic, AED offers the possibility to look into the packet or application header and payload, therefore regular expression are tracked in HTTP, DNS header or requests, PCAP filters (filter lists) can also be setup to allow or block traffic (source port, destination, port, IPs, checksum….).

TCP Flood Attacks Prevention

A SYN flood attack exploits the TCP three-way handshake, which establishes a connection between a client and a server. By forcing all TCP clients to authenticate that they are valid, Spoofed SYN Flood Prevention can protect against highly distributed attacks (AED replies to the client's initial SYN with an ACK that imitates an existing, half-open TCP connection. If the client sends a reset, then AED authenticates the client, and the client opens a new TCP connection to the protected host).

EAD proposes also the possibility to block TCP connections/reset/idle when thresholds are exceeded (number of TCP connections per host, idle timeout).

HTTP Authentication

To ensure that the client is a legitimate browser, AED can use one the following methods to authenticate the client

- EAD answers with an HTTP redirect to force the browser to a request to the redirected URL
- HTTP soft reset while EAD asks the client to resend the request
- HTTP JavaScript: AED sends a small amount of JavaScript to the client. If the client responds with a redirect, then AED authenticates the client.

UDP Flood Detection

This feature protects against attacks that send an excessive number of UDP packets to a server to exhaust its resources.

AED solution can also enable decryption of SSL and TLS for security inspection by addition of hardware security and cryptographic acceleration modules.

AED is able to run automatic protection services so the user can limit his duty to monitoring that's hands-off interaction.

Blacklist and Whitelist

AED offers the possibility to blacklist countries or hosts (globally or per protection group). That can be done for both inbound and outbound traffic, this mechanism can also be automatically activated while the system identifies an attack for a particular target or source. To avoid any critical traffic to be affected, users can whitelist sources when those are, for example, belonging to a trusted network (remote sites, partners, providers or customers).

TLS/SSL Traffic Protection

The TLS Attack Prevention settings enforce correct protocol usage and block malformed SSL and TLS requests. These settings also block clients that attempt to exploit the protocols to exhaust server resources.

With the appropriate module (CAM: Cryptographic Acceleration Module and HSM : Hardware Security Module) and the import of keys and certificate on it, AED can decrypt and TLS/SSL traffic and applies the HTTP-related protections. Processing capacity goes up to 97K connections/second.

Mitigation

The focus of AED is on the automatic detection and mitigation of attacks. When AED is in active mode, it continually blocks any malicious traffic that it detects. However, additional solutions are available to help monitoring the system and blocking attacks which do not fit configured protection settings, or which is not detectable by AED (ex. affecting upstream equipment).

Following actions can be taken to mitigate an attack:

- Raise protection level on AED to apply stricter setting (thresholds, filter lists...)
- Identify and block malicious traffic: blacklist IPs, setup FCAP filters....
- Use Cloud signaling: if available, AED can ask for cloud-based mitigation for volumetric attacks to avoid overloading of uplink connectivity.

Cloud Signaling

When Cloud Signaling is activated, AED signals to the cloud service provider that mitigation help is needed. When the service provider begins the mitigation process, the attack that is congesting the upstream links is redirected to the cloud service provider who mitigates the attack, and then routes the cleaned traffic back to customer site (using GRE tunnel for example). Cloud signaling can be setup towards Cloud mitigation infrastructure of the service provider or towards Arbor Cloud DDoS Protection service which is built to handle the high-bandwidth, volumetric attacks that are too large to mitigate at the data center's premises. By rerouting the traffic away from service provider infrastructure, the Arbor Cloud DDoS Protection service can defuse the attack, thereby limiting downtime and maintaining availability. Redirection to Arbor Cloud can be done by changing DNS records of affected hosts or by modifying BGP announcements (Arbor Cloud service announces the BGP routes for the affected prefixes).

Unlike firewalls or load-balancers which keep connection information as long as the session is up, AED perform real-time Layer 3 to Layer 7 packet and event countermeasures without keeping session table entry during session lifetime.

Packet Capture

AED offers the possibility to sample the packets that AED inspects, and capture information about the packets in real time. Users can save the packet information (PCAP files for example) to use it to explore payload and define regular expressions to be used to filter traffic (TCP/UPD ports, IP headers…).

Graphs and Traffic Data

AED provides traffic forensics in real time, graphs for global, per protection group, per target, source, top countries, blocked and passed, matched countermeasure category, top URL, top protocols and top service traffic are displayed as well as Outbound Threat Activity.

Alerting

Bandwidth alerts can be set up globally and per protection group. Alerts raise when defined threshold are exceeded for total, blocked and botnet traffic.

Alerts are also raised when a system issue is detected to allow user to take appropriate actions (ex. Interface down, CPU, HW…).

Notifications

E-mails, syslog messages and SNMP traps can be configured to be sent when a configured event happens (bandwidth, system health, Cloud signaling event, protection level, change logs …).

CDN and Proxy Support Settings

When traffic is routed through a CDN or proxy, the source IP address is that of the last CDN or proxy device. Therefore, the protection settings that block an attacker's IP address might block all traffic from the CDN or proxy. To avoid that, CDN and Proxy Support can be enabled, AED relies on the protection categories that block malicious traffic but do not block the attacker's IP address. The clean traffic from the CDN or proxy is passed.

LEARN MORE

For more information about NETSCOUT Arbor Edge Defense (AED) visit:

https://www.netscout.com/product/netscout-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

SECJTF_001_EN-2001 05/2020