NETSCOUT Arbor Edge Defense (AED)

First and Last Line of Smart, Automated Perimeter Defense

KEY FEATURES & BENEFITS

First & Last Line of Defense

AED's unique location on the network edge, its stateless packet processing engine and enforcement of ATLAS® or 3rd party threat intelligence feed allow it to stop inbound threats and outbound communication from compromised hosts.

Integration with Security Stack

REST API, support for STIX/TAXII, Syslog (CEF, LEEF) and Contextual Threat Intelligence fueled by ATLAS enable AED to integrate into existing security stack and processes.

Intelligently Automated, Hybrid DDoS Protection

The intelligently automated, fully managed combination of in-cloud (via Arbor Cloud) and on-premises (via AED) is continuously armed with ATLAS global threat intelligence; offers the most comprehensive form of protection from the modern-day DDoS attack.

Outbound Enforcement of Threat Intelligence

AED can enforcement reputation-based threat intelligence from NETSCOUT's ATLAS or 3rd parties (via STIX/TAXII)'s to block outbound communication from internal compromised hosts; helping to stop further proliferation of malware or data breach.

Let's face it. *There is no peace time.* Whether it be new forms of DDoS attacks, ransomware, phishing attempts or compromised BYOD and IoT devices; organizations are under constant threat from all types of advanced cyber threats. To address these evolving threats, the modern-day security stack has become larger and more complex. And unfortunately, as evidenced by the daily reports of data breaches and downtime – is still failing.

Security teams need best of breed cybersecurity solutions that can detect and stop all types of cyber threats - both entering or leaving their networks. As importantly, these solutions must also be able to integrate into an organization's existing security stack and/or consolidate functionality to reduce cost, complexity and risk.

NETSCOUT® Arbor Edge Defense (AED) is such a solution. AED's unique position on the network edge (i.e. between the router and the firewall), its stateless packet processing engine and the continuous reputation based threat intelligence it receives from NETSCOUT's ATLAS Threat Intelligence or 3rd parties, enable it to automatically stop both inbound threats such as DDoS attacks, and outbound communication from internal compromised threat actor command and control (C2) infrastructure – essentially acting as the first and last line of defense for organizations.

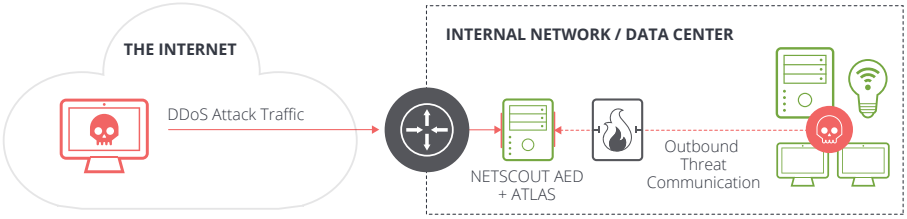

Figure 1: AED's unique location on network edge + stateless packet processing engine + ATLAS Global Threat Intelligence = First and Last Line of Defense from advanced cyber threats.

- **Benefits of Arbor Edge Defense** – First Line of Defense: AED stops all types of inbound DDoS attacks (e.g. volumetric, TCP-state exhaustion, application-layer) to protect the availability of an organization's network, services and stateful devices (e.g. NGFWs). Fully integrated with Arbor Cloud (a global, cloud-based, DDoS protection service with over 11 Tbps of mitigation capacity), AED is the on-premise component of NETSCOUT's industry leading, hybrid DDoS protection solution.
- **Last Line of Defense** – Armed with potentially millions of reputation-based IOCs and other threat intelligence from NETSCOUT ATLAS or 3rd parties (via STIX/TAXII), AED can stop outbound communication from compromised internal devices to threat actor command and control (C2); to help stop the proliferation of malware or attacker within an organization and avoid a data breach.
- **Integration** – AED's ability to act as a first and last line of defense, use of a REST API, support for standards such as STIX/TAXII, SYSLOG (CEF, LEEF) and additional context provided by ATLAS allow AED to integrate into an organizations existing security stack and processes.

NETSCOUT AED Appliances

Features	2600	2800	HD1000
Physical Dimensions	**Chassis:** 2U rack height; **Height:** 3.45 inches (8.67 cm); **Width:** 17.4 inches (43.53 cm); **Depth:** 20 inches (50.8 cm); **Weight:** 36.95 lbs. (17.76 kg)		**Chassis:** 2U rack height **Weight:** 45.2 lbs (20.5 kg) with 1 PPM, add 1.6 lb (.73 kg) per PPM (up to eight) **Height:** 3.5 in (8.89 cm) **Width:** 17.6 in (44.70 cm) **Depth:** 21 in (53.34 cm)
Power Options	**DC:** 2 x DC redundant, hot swap capable power supplies; **DC Power Ratings:** -40 to -72 Vdc, 28/14 A max (per DC input); **AC:** 2 x AC redundant, hot swap capable power supplies; **AC Power Ratings:** 100 to 240 VAC, 50 to 60 Hz, 12/6 A max; **Watts:** 315 typical, 375 max		**AC:** Two 1500-watt redundant power supplies; 100-240V AC, 15-10 A, 50-60 Hz (x2); **DC:** Two 1500-watt redundant power supplies; -48 to -60 V dc, 44 A (x2)
Hard Drives	2 x 240 GB SSD in RAID 1 Configuration	2 x 240 GB SSD in RAID 1 Configuration	2 x 480 GB SSD drives, RAID 1
Environmental	**Operating:** Temperature : 41°F to 104°F (5° to 40°C) Humidity: 5–85%; **Non-Operating:** Temperature -40° to 158°F (-40° to 70°C); Humidity 95%		**Operating temperature:** 39.2° to 104°F (-4° to 40°C) **Relative humidity (operating):** 5 to 93%, non-condensing
Memory	32 GB	64 GB	128GB per PPM, 8 PPMs per AED-HD1000
Processor	2 x Intel Xeon E5-2608L v3 (6 cores) 2 GHz; Watts: 315 typical, 375 max	Dual Intel Xeon (12-core) E5–2648L v3 –1.80GHz	(1) MM, (5) fans, (2) QSFP+, (4) QSFP28; (x1) PPM: @ 327 Watts, 1116 BTU/ hr; (x4) PPM: @ 569 Watts, 1940 BTU/ hr ; (x8) PPM: @ 932 Watts, 3180 BTU/ hr
Operating System	Our proprietary ArbOS® operating system		
Management Interfaces	2 x 10/100/1000 BaseT Copper; RJ-45 serial console port	2 x 10/100/1000 BaseT Copper; RJ-45 serial console port	4 x 1G Copper, RJ-45 serial console port
Protection Interface	• 4, 8 or 12 1G bypass ports (copper, sx fiber, lx fiber) • 4 x 10 G bypass ports plus 0, 4 or 8, 1 G bypass ports	• 4x10 GigE bypass ports (SR or LR mixed fiber) • 8x10 GigE bypass ports (SR or LR mixed fiber) • 8x10 GigE bypass ports (SR or LR mixed fiber) plus 4x1 GigE bypass ports (SR or LR fiber or copper) • 2x40 GbE bypass ports	4 x 100 GigE + 8 x 10 GigE = One to four 100 GbE QSFP28 (LR) optical transceivers + One or two 4 x 10 GbE QSFP+ (SR or LR Lite) optical transceivers with one 4 x 10 GbE breakout cable on each transceiver
Traffic Bypass Options	Integrated hardware bypass; Internal "software" bypass to pass traffic without inspection		External hardware bypass via 3296 Inline Bypass Switch
Latency	Less than 80 microseconds		< 2ms
Availability	Inline bypass, dual power supplies, solid-state hard drive RAID cluster		External bypass, dual power supplies
Regulatory Compliance	FIPS 140-2 Level 1 UL60950-1/CSA 60950-1 (USA/Canada); EN60950-1 (Europe); IEC60950-1 (International), CB Certificate & Report including all international deviations; GS Certificate (Germany); EAC-R Approval (Russia); CE—Low Voltage Directive 73/23/EEE (Europe); BSMI CNS 13436 (Taiwan); KCC (South Korea); RoHS Directive 2002/95/EC (Europe)		RoHS 6/6, IEC/EN/UL/ CSA 60950-1, FCC Part 15 Subpart B Class A, EN 55022, EN55024, ETSI EN 300 386, cCSAus Mark, CE Mark, KN22, KN24, RCM Mark, KCC Mark, EAC Mark, BIS, CCC Mark (pending)

DDoS & Advanced Cyber Threat Protection

Features	2600	2800	HD1000
Inspected Throughput	Licenses for 100 Mbps, 250 Mbps, 500 Mbps, 1 Gbps, 2 Gbps, 5 Gbps, 10 Gbps, 15 Gbps, 20 Gbps	Licenses for 10 Gbps, 20 Gbps, 30 Gbps, 40 Gbps; software upgradeable	Licenses for 25Gbps, 50Gbps, 75Gbps, 100Gbps, 125Gbps, 150Gbps, 175Gbps and 200Gbps; 70M PPS (Packet Per Second); **Hardware Mitigation Capacity:** Up to eight Packet Processing Modules (PPMs) with 50Gbps of mitigation capacity per PPM
Maximum DDoS Flood Prevention Rate	Up to 15 Mpps	Up to 28.80 Mpps	
HTTP(s) Connections/SEC	368K at recommended protection level; 613K filter list only protection	1,351K at recommended protection level; 1,497K filter list only protection	
Protected Endpoints	Unlimited		
Authentication	On device, RADIUS; TACACS		
Management	SNMP gets v1, v2c; SNMP traps v1, v2c, v3; CLI; Web UI; HTTPS; SSH customizable, role-based management; Up to 50 AED (appliances and/or virtual AED running KVM hypervisor) can be managed by the AED Console; managed AED must at least be running v5.11; vAED Console can run on VM hypervisor.		
Protection Groups	100		
Reporting and Forensics	Real-time and historical IPV4 and IPV6 traffic reporting, extensive drill-down by protection group and blocked host including total traffic, passed/blocked,top destination URLs/services/domains, attack types, blocked sources, top sources by IP location. Packet visibility in real-time.		
DDoS Protection	TCP/UDP/HTTP(S) flood attacks, botnet protection, hacktivist protection, host behavioral protection, anti-spoofing, configurable flow expression filtering, payload expression-based filtering, permanent and dynamic blacklists/whitelists, traffic shaping, multiple protections for HTTP, DNS and SIP, TCP connection limiting, fragmentation attacks, connection attacks.		
Modes	Inline active; inline inactive (reporting, no blocking); SPAN port monitor		
Notifications	SNMP trap, Syslog (CEF,LEEF); email		
Cloud Signaling	Yes (collaborative DDoS attack mitigation with service provider or Arbor Cloud)		
Web-Based GUI	Supports multi-language translated user interfaces		
Supported Browsers	Google Chrome, Mozilla Firefox, Internet Explorer 11		
Maximum IoCs	3+ Million		
Ioc Types & Formats	IP address, fully qualified domain names, URLs . Formats: Proprietary ATLAS Intelligence Feed format, STIX, and TAXII		

Arbor Enterprise Manager Console

Supported Platforms	Arbor Appliance; Virtual Machine
Max Number AED / APS Managed	50. (Note: The Arbor Enterprise Manager Console can managed both APS and AED devices)
Virtual AED Console Requirements	VMware vSphere Hypervisor™ version 5.5 or later; VMware vSphere Client software, version 5.5 or later; vAEM image file (ova); 4 CPUs; 100 GB hard disk space; 12 GB RAM; 1 management interface (a second management interface is optional)
Management Options	Configuration or Views into (individual and/or all AED): Hardware and Software health; System and Security alerts; Blocked Hosts; ATLAS Threat Summary; Server Types, Protection groups (IPV4/6); Blacklist/Whitelist; Executive Management Reports.
Supported Browsers	Google Chrome 80, Mozilla Firefox 74, Internet Explorer 11

Arbor Enterprise Manager 7000 Appliance

Memory	128G (8x16G DIMMs)
Processor	Intel Xeon (12-Core) – ES-2648Lv3 – 1.8GHz – 20M Cache – 9.60 GT/sec – 75W
Power Requirements	Redundant, load sharing and auto-sensing 850W dual power supplies; AC: 100-240 VAC, 50/60 Hz, 12/6 A; DC: -40 to -72 V, 28/14 A max
Physical Dimensions	**Chassis:** 2U rack height; **Height:** 3.45 inches (8.67 cm); **Width:** 17.4 inches (43.53 cm) **Depth:** 20 inches (50.8 cm); **Weight:** 36.95 lbs. (17.76 kg); Standard 19 and 23 inches rack mountable
Hard Drives	Six 480 GB solid state drives configured for RAID 5
Network Interfaces	2 x 1 GigE (SFP for Copper, GigE SX, or GigE LX)
Environmental	**Operating:** Temperature 41° to 104°F (5° to 40°C); Humidity 95%; **Non-Operating:** Temperature 73° to 104°F (23° to 40°C)
Operating System	Our proprietary, embedded ArbOS operating system, based on Linux
Regulatory Compliance	UL60950-1/CSA 60950-1; EN60950-1; IEC60950-1, CB Certificate & Report including all international deviations; SONCAP; EAC Mark; CE—Low Voltage Directive 2014/35/EU; KCC Mark; RoHS 2011/65/EU; Telcordia GR-63; ETSI EN 300 019; NEBS; ETSI EN 300 753; cULus Mark; IC ICES-003 Class A; CE Mark to EMC Directive, 2014/30/EU; EN55022, Class A; EN55024; EN61000-3-2; EN61000-3-3, CISPR22, Class A, CISPR 24 Immunity; FCC 47 CFR Parts 15, Class A

Virtual AED

Virtual Network Function (VNF) Orchestration	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	
Minimum Virtual Machine Requirements	vCPUs: 2; NICs: 1 to 10; Memory: 6 GB; Storage: 100 GB	
Supported Hypervisors	VMware vSphere 5.5+	KVM kemel 3.19 QEMU 2.0
Inspection Throughput/Instance	1 Gbps	1 Gbps
Maximum DDoS Flood Rate/Instance	910 Kpps	600 Kpps
Protection Groups	10; 50 with 4 vCPUs and 12 GB RAM	10; 50 with 4 vCPUs and 12 GB RAM

Edge Defense Manager Virtual Appliance

Max Number AED Supported	12
Supported Hyper Visors	VMware vSphere 5.5+
Virtual Machine Requirements	4 CPUs; 300 GB hard disk space; 24 GB RAM
Supported Browsers	Chrome v70 and Edge v42

Decryption Capabilities

For 2600 and 2800 Appliances Only	Hardware Security Module (HSM)"	Hardware Security Module (HSM) FIPS Mode	Cryptographic Acceleration Module (CAM)	Cryptographic Acceleration Module (CAM)
FIPS Support	N/A	140-2 Level 2 and Level 3. Separate "Trusted-Path" Administration for FIPS 140-2 Level 3	N/A	N/A
Connections/second, Throughput	HSM 750M: 1.4K connections/sec, HSM 5G: 8K connections/sec		CAM 2048: 97K connections/sec	
Supported SSL/TLS protocol versions	TLS 1.0, 1.1, 1.2 SSL 3.0"	TLS 1.0, 1.1, 1.2 SSL 3.0"	TLS 1.0, 1.1	TLS 1.2
Supported Cipher Suites				
TLS_RSA_WITH_RC4_128_SHA	✓	×	×	×
TLS_RSA_WITH_RC4_128_MD5	✓	×	×	×
TLS_RSA_WITH_DES_CBC_SHA	✓	×	×	×
SSL_RSA_WITH_DES_CBC_SHA	✓	×	×	×
TLS_RSA_WITH_3DES_EDE_CBC_SHA	✓	✓	✓	×
SSL_RSA_WITH_3DES_EDE_CBC_SHA	✓	✓	✓	×
TLS_RSA_WITH_AES_128_CBC_SHA	✓	✓	✓	×
TLS_RSA_WITH_AES_128_CBC_SHA256	✓	✓	✓	✓
TLS_RSA_WITH_AES_256_CBC_SHA	✓	✓	✓	×
TLS_RSA_WITH_AES_256_CBC_SHA256	✓	✓	✓	✓
TLS_RSA_WITH_AES_128_GCM_SHA256	✓	✓	✓	✓
TLS_RSA_WITH_AES_256_GCM_SHA384	✓	✓	✓	✓
TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256	✓	✓	✓	✓
TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384	✓	✓	✓	✓
TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384	✓	✓	✓	✓
TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256	✓	✓	✓	✓
TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256	✓	✓	✓	✓
TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384	✓	✓	✓	✓
TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384	✓	✓	✓	✓
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	✓	✓	✓	✓
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	✓	✓	✓	✓
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384	✓	✓	✓	✓
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	✓	✓	✓	✓
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	✓	✓	✓	✓
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	✓	✓	✓	✓
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	✓	✓	✓	✓
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	✓	✓	✓	✓

For 2600 and 2800 Appliances Only	Hardware Security Module (HSM)"	Hardware Security Module (HSM) FIPS Mode	Cryptographic Acceleration Module (CAM)	Cryptographic Acceleration Module (CAM)
TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA	✓	✓	✓	×
TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA	✓	✓	✓	×
TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA	✓	✓	✓	×
TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA	✓	✓	✓	×
TLS_ECDH_RSA_WITH_AES_128_CBC_SHA	✓	✓	✓	×
TLS_ECDH_RSA_WITH_AES_256_CBC_SHA	✓	✓	✓	×
TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA	✓	✓	✓	×
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	✓	✓	✓	×
Maximum number of keys/ certificate pairs	1998			

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

SECPDS_013_EN-2001 06/2020