

NETSCOUT AED (Arbor Edge Defense)

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 ATLAS® global 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, 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 Threat Communication Detection and Blocking

AED's ATLAS derived, reputation based threat intelligence allow it to detect and block outbound communication from internal compromised hosts; helping to stop further proliferation of malware or data breach.

Support for Virtual & Hybrid-Cloud Environments

VAED is a virtual version of the AED appliance that can be run in your private virtual environment like Amazon Web Services, providing unified protection for your hybrid-cloud environments.

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

Security teams need best of breed cyber security solutions that can detect and stop all types of cyber threats - both inbound threats and outbound malicious communication from compromised internal devices. 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 AED (Arbor Edge Defense) 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 feed enable it to automatically detect and stop both inbound threats and outbound communication from internal compromised hosts – essentially acting as the first and last line of defense for organizations.

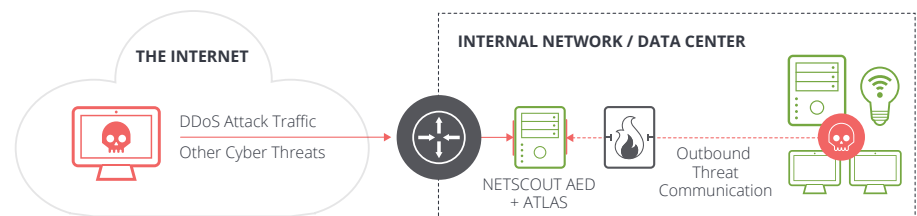


Figure 1: AED's unique location on network edge + stateless packet processing engine + ATLAS Global Threat Intelligence = First and Last Line of Defense from advanced cyber threats.

Benefits of Arbor Edge Defense:

- **First Line of Defense:** Deployed at the network perimeter, using stateless technology and armed with millions of IoCs, AED detects and blocks inbound commodity cyber threats thus taking pressure off of stateful devices such as Next Gen Firewalls.
- **Last Line of Defense:** Missed by existing security stack, AED can detect and block outbound communication to known bad IP addresses, domains, URLs, geographies; thus helping stop the further proliferation of malware within an organization and avoid a data breach.
- **Contextual Threat Intelligence:** When an IoC is blocked, AED leverages the global threat intelligence of NETSCOUT ATLAS to provide more context related to the IoC thus helping security teams determine risk and/or give them more information to proactively hunt using their other security tools.
- **Best of Breed DDoS Protection:** AED can automatically detect and stop inbound application layer, TCP-state exhaustion and DDoS attacks as large as 40 Gbps. In the event of even larger DDoS attacks, Cloud Signaling automatically reroutes traffic to Arbor Cloud or a MSSP's cloud-based mitigation center.
- **Integration:** AED's robust REST API, support for STIX/TAXII enable AED to integrate into existing security stack and processes.

NETSCOUT AED Appliances

Features	2600	2800
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)	
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	
Hard Drives	2 x 120 GB SSD in RAID 1 Configuration	2 x 240 GB SSD in RAID 1 Configuration
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%	
Memory	32 GB	64 GB
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
Operating System	Our proprietary, embedded 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
Protection Interface	<ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> 4 x 10 GigE (SR or LR mixed fiber) 8 x 10 GigE (SR or LR or mixed fiber) 8 x 10 GigE (SR or LR or mixed fiber) + 4 x 1 GigE (SX or LX fiber, or copper)
Traffic Bypass Options	Integrated hardware bypass; Internal “software” bypass to pass traffic without inspection	
Latency	Less than 80 microseconds	
Availability	Inline bypass, dual power supplies, solid-state hard drive RAID cluster	
MTBF	44,000 hours	
Regulatory Compliance	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)	

DDoS & Advanced Cyber Threat Protection

Features	2600	2800
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
Maximum DDoS Flood Prevention Rate	Up to 15 Mpps	Up to 28.80 Mpps
Simultaneous Connections	Not applicable: AED does not track connections	
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
SSL Decryption Options	Inspected Throughput: Options for 750 Mbps and 5 Gbps HTTPS Connections: Up to 7,500 (750M HSM) or 45,000 (5G HSM) Concurrent Sessions: Up to 150,000	Inspected Throughput: Up to 5 Gbps HTTPS Connections: Up to 45,000 Concurrent Sessions: Up to 150,000
	Supported encryption protocols: SSL 3.0, TLS 1.0, 1.1 and 1.2; Supported Cypher Suites: RSA, ECDH, ECDHE; FIPS 140-2 Level 2 and 3 support; Separate “Trusted-Path” Administration for FIPS 140-2 Level 3; Secure tamper-proof enclosure; Keys cleared if enclosure breached	
Maximum Number of Keys/Certificate Pairs	1998	
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, 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	Internet Explorer v10-11, Firefox ESR v31, Firefox v40, Chrome v44, Safari v6
Maximum IoCs	3+ Million
loc Types	IP address, fully qualified domain names, URLs

NETSCOUT AED Console

Supported Platforms	Arbor Appliance; Virtual Machine
Max Number AED Managed	50
Virtual AED Console Requirements	VMware vSphere 5.5+; 2 CPUs; 100 GB hard disk space; 4 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	Internet Explorer v10-11, Firefox ESR v31, Firefox v40, Chrome v44, Safari v6

NETSCOUT AED Console 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	
Support for Amazon AWS	Yes, Amazon EC2	
Minimum Virtual Machine Requirements	vCPUs: 2; NICs: 1 to 10; Memory: 6 GB; Storage: 100 GB	
Supported Hypervisors	VMware vSphere 5.5+	KVM kernel 3.19 QEMU 2.0
Inspection Throughput/Instance	1 Gbps	1 Gbps
Maximum DDoS Flood Rate/Instance	910 Mbps	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 Hypervisors	VMware vSphere 5.5+
Virtual Machine Requirements	4 CPUs; 300 GB hard disk space; 24 GB RAM
Supported Browsers	Chrome v70 and Edge v42



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