NETSCOUT AED and AEM

Adaptive DDoS Protection Solution that Adapts to Dynamically Changing DDoS Attacks To Provide Effective First and Last Line of Automated Perimeter Defense

DDoS attacks are evolving, the new preferred flavor of DDoS attack, is a multi-vector dynamic direct path attack that adjusts vectors and methodologies to continually evade existing DDoS defenses. Add to this the ransomware, phishing attempts, and compromised IoT devices and you can see how organizations are under constant risk from all types of advanced cyber threats. To address these evolving threats, security teams need solutions that can dynamically adapt to the changing attacks - both entering or leaving their networks. Just 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.

KEY FEATURES & BENEFITS

Adaptive DDoS Protection

Effectively detect and mitigate ever-changing DDoS attacks without impacting legitimate services by automatically detecting new attack techniques and providing targeted mitigation. Enabled by dynamic traffic analysis technology, global attack visibility, adaptive intelligence and decades of DDoS domain expertise.

Enterprise Scale and Multi-Layer Defense in-Depth

Centralized and scalable visibility for management of all deployed AEDs from a single pane of glass through Arbor Enterprise Manager. Intelligently integrates with Arbor Cloud for comprehensive, hybrid DDoS attack protection.

Protect Assets in AWS

Deploy virtual AED in AWS to detect and mitigate attacks targeting assets in AWS, both from outside of AWS cloud and inside the cloud between VPCs.

First & Last Line of Defense

Automatically and surgically block unwanted inbound and outbound malicious traffic including malware, scanning and phishing attempts at the network edge with unparalleled threat intelligence and embedded security analysis expertise.

Integration with Existing Security Stack and Process

NETSCOUT AED's 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 process.

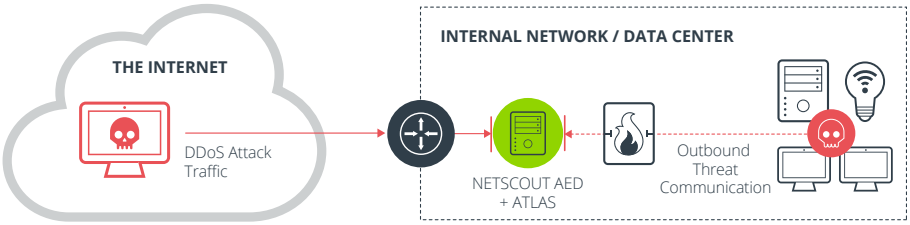

Figure 1: AED's unique location on network edge + stateless packet processing engine + ATLAS Global Threat Intelligence = First and Last Line of Defense from advanced cyber threats.

NETSCOUT Arbor Edge Defense (AED) is uniquely positioned on the network edge (i.e., between the internet router and the firewall) to provide an inline, always-on, first and last line of defense. Using stateless packet processing, continuous global threat intelligence, decades of DDoS mitigation expertise, and adaptive DDoS defense technology, AED can automatically stop inbound, dynamically changing DDoS attacks and outbound communication from internal compromised devices communicating with threat actor command and control (C2) infrastructure. Arbor Enterprise Manager provides a centralized and scalable single-pane-of-glass console for managing all AEDs.

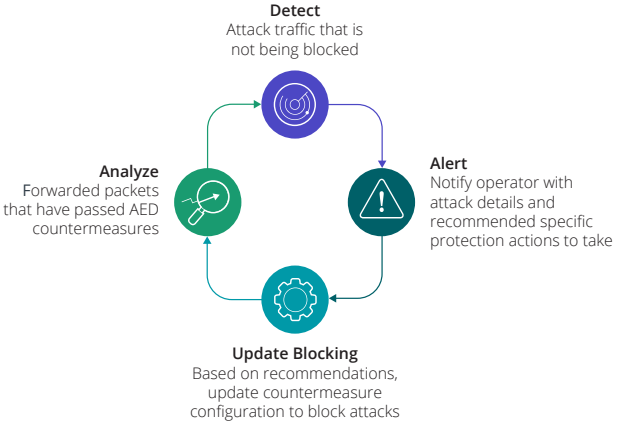

Figure 2: Arbor Adaptive DDoS Protection is driven by this simple efficient workflow.

NOTE: Adaptive DDoS Protection is only supported with AED-8100 and AEM

NETSCOUT AED Appliances

Features	8100	8100-CI	HD1000
Physical Dimensions	**Chassis:** 2RU rack height; **Height:** 3.45 inches (8.67 cm); **Width:** 17.14 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; Both AC and DC power options are 850-watt.		**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 Vdc, 44 A (x2)
Hard Drives	2 x 240GB SSD in RAID 1 Configuration		2 x 480GB SSD drives, RAID 1
Environmental	**Operating:** Temperature: 41ºF to 104ºF (5º to 40ºC) Humidity: 5–85%; **Non-Operating:** Temperature -40º to 158ºF (-40º to 70ºC); Humidity 95%		**Operating temperature:** 39.2º to 104ºF (-4º to 40ºC) **Relative humidity (operating):** 5 to 93%, non-condensing
Operating System	Our proprietary ArbOS® operating system		
Management Interfaces	2 x 1G or 2 x 10G Copper, RJ-45 serial console support		4 x 1G Copper, RJ-45 serial console port
Protection Interfaces	• 4 x 1 GigE bypass ports (LX, SX or copper) • 8 x 1 GigE bypass ports (LX, SX, copper or mixed) • 12 x 1 GigE bypass ports (LX, SX, copper or mixed) • 4 x 10 GigE bypass ports (LR or SR) • 8 x 10 GigE bypass ports (LR, SR, or mixed) • 4 x 10 GigE bypass ports (LR or SR) plus 4 x 1GigE bypass ports (LX, SX or copper) • 4 x 10 GigE bypass ports (LR or SR) plus 8 x 1GigE bypass ports (LX, SX or copper) • 8 x 10 GigE bypass ports (LR or SR) plus 4 x 1GigE bypass ports (LX, SX or copper) • 2 x 40 GigE bypass ports (LR or SR) • 4 x 40 GigE bypass ports (LR or SR) • 2 x 40 GigE bypass ports (LR or SR) plus 4 x 10 GigE bypass ports (LR or SR) • 2 x 40 GigE bypass ports (LR or SR) plus 8 x 10 GigE bypass ports (LR or SR)		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		
Availability	Inline bypass, dual power supplies, solid-state hard drive RAID cluster		External bypass, dual power supplies

Features	8100	8100-CI	HD1000
Regulatory Compliance	UL/cUL/EN/IEC 62368-1; EN 55032; EN 55035; CISPR 32, 35; ETSI EN 300 386; cULus Mark; IC ICES-003 Class A; EN 61000-3-2; EN 61000-3-3; EMC Directive 2014/30/EU; Low Voltage Directive 2014/35/EU; UL 60950-1 2nd edition/CSA C22.2 No.60950-1-07 2nd Edition; FCC 47 CFR Parts 15, Class A; CB Certificate & Report including all international deviations; RoHS 2011/65/EU; Moroccan Conformity Mark; VCCI (Japan); BIS (India); CCC (China); RCM (Australia/ New Zealand); KCC (South Korea); EAC-R Approval (Russia); South Africa LoA; Mexico (UL-CoC for Mexico); NEBS-ready	EN60950-1 (Europe); IEC60950-1 (International), CB Certificate & Report including all international deviations, EAC-R Approval (Russia), FCC 47CFR Parts 15, CE—Low Voltage Directive 73/23/EEE (Europe), RCM (Australia/ New Zealand), KCC (South Korea), RoHS Directive 2002/95/EC (Europe), VCCI (Japan), BIS (India), CCC (China)	RoHS 6/6, IEC/EN/UL/ CSA 60950-1, FCC Part 15 Subpart BClass A, ETSI EN 300 386, CE Mark, RCM Mark, KCC Mark, EAC Mark, BIS, CCC Mark, CB Certificate and Report to IEC62368-1 andIEC60950-1, 2nd edition and all international deviations, EMC Directive 2014/30/EU, Low Voltage Directive 2014/35/EU

Features	2600 (End of Sale)	2800 (End of Sale)
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 240GB 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%	
Operating System	Our proprietary ArbOS® operating system	
Management Interfaces	2 x 10/100/1000 BaseT Copper; RJ-45 serial console port	
Protection Interfaces	• 4 x 1 GigE bypass ports (LX, SX, or copper) • 8 x 1 GigE bypass ports (LX, SX, copper or mixed) • 12 x 1 GigE bypass ports (LX, SX, copper or mixed) • 4 x 10 GigE bypass ports (LR or SR) • 4 x 10 GigE bypass ports (LR or SR) plus 8 x 1 GigE bypass ports (LX, SX, copper or mixed) • 4 x 10 GigE bypass ports (LR or SR) plus 4 x 1 GigE bypass ports (LX, SX, or copper)	• 4 x 10 GigE bypass ports (LR or SR) • 8 x 10 GigE bypass ports (LR, SR or mixed • 8 x 10 GigE bypass ports (LR, SR or mixed) plus 4 x 1 GigE bypass ports (LX, SX or copper) • 2 x 40 GbE bypass ports (LR or SR) • 4 x 40 GbE bypass ports (LR, SR or mixed) • 2 x 40 GbE bypass ports (LR or SR) plus 8 x 10 GbE bypass ports (LR, SR or mixed) • 2 x 40 GbE bypass ports (LR or SR) plus 4 x 10 GbE bypass ports (LR or SR)
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	

Features	2600 (End of Sale)	2800 (End of Sale)
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, EAC-R Approval (Russia), FCC 47CFR Parts 15, CE—Low Voltage Directive 73/23/EEE (Europe), RCM (Australia/New Zealand), KCC (South Korea), RoHS Directive 2002/95/EC (Europe), VCCI (Japan), BIS (India), CCC (China)	

DDoS & Advanced Cyber Threat Protection

Features	8100	8100-CI	HD1000
Inspected Throughput	Licenses for 100 Mbps, 250 Mbps, 500 Mbps,1 Gbps, 2 Gbps, 5 Gbps, 10 Gbps, 20 Gbps, 30 Gbps, 40 Gbps; software upgradeable		Licenses for 25 Gbps, 50 Gbps, 75 Gbps, 100 Gbps, 125 Gbps, 150 Gbps, 175 Gbps and 200 Gbps; **Hardware Mitigation Capacity:** determined by the number of PPMs with 25G per PPM. Up to 8.7M PPS (Packet Per Second) per PPM. **Note:** Licensed Inspected Throughput should not go above the Hardware Mitigation Capacity.
Maximum DDoS Flood Prevention Rate	Up to 38.92 Mpps		Up to 289.17 Mpps
Protected Endpoints	Unlimited		
Authentication	On device, RADIUS; TACACS		
SSL/TLS Traffic Support Capabilities	TLS, and CAM support can be found in the Decryption Capabilities table on page 8		Not Supported
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 v.6.0 (v AED), v6.4 (HD1000), or v.6.6 (8100).		
Protection Groups	100		200
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, 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 83, Mozilla Firefox 77, 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		

Features	2600 (End of Sale)	2800 (End of Sale)
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
HTTP Connections per 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	
SSL/TLS Traffic Support Capabilities	TLS, and CAM support can be found in the Decryption Capabilities table on page 8	TLS, and CAM support can be found in the Decryption Capabilities table on page 8
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; v AED 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 83, Mozilla Firefox 77, 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

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)
Supported Browsers	Google Chrome 80, Mozilla Firefox 74, Internet Explorer 11

Virtual Arbor Enterprise Manager (vAEM) Configurations

Configuration	Base vAEM with 2 Devices	Each Additional Device
Disk Space	250GB	70GB
Cores	4	0.25
Memory	16GB	1GB
Management Interface	1 management interface required; a second management interface is optional	
Hypervisor Requirements Contents	VMware vSphere Hypervisor™ version 6.7 or later; VMware vSphere Client software, version 6.7 or later	

Arbor Enterprise Manager 8000 Appliance

Features	8000	8000-CI
Power Requirements	Dual redundant, load-sharing, auto-sensing 850 Watt power supplies **AC:** 100-240 VAC, 50/60 Hz, 10/5 A **DC:** -40 Vdc to -72 Vdc, 25/12.5 A	
Physical Dimensions	**Chassis:** 2U rack height; **Height:** 3.45 inches (8.67 cm); **Width:** 17.14 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	Minimum: Six 480GB solid state drives configured for RAID 5	
Network Interfaces	2 x 10G RJ45 onboard, 4 x 10G pluggable ports via installed PCI card	
Environmental	**Operating:** 41° – 104°F (5° – 40°C), 5-85% humidty **Non-Operating:** -40°F – 158°F (-40°C – 70°C), 95% non-condensing humidity	
Operating System	Our proprietary, embedded ArbOS operating system, based on Linux	
Regulatory Compliance	UL 60950-1 2nd edition/CSA C22.2 No.60950-1-07 2nd Edition, EMC Directive 2014/30/EU, Low Voltage Directive 2014/35/EU, CB Certificate and Report to IEC62368-1 and IEC60950-1, 2nd edition and all international deviations, CE, FCC 47CFR Parts 15, Verified Class A limit, ICES-003 Class A Limit, VCCI Class A ITE, RoHS (recast) Directive 2011/65/EU, Moroccan Conformity Mark, KC (Korea) Approval, RCM (Australia/New Zealand) Approval, EAC (Russia)	EN60950-1 (Europe); IEC60950-1 (International), CB Certificate & Report including all international deviations, EAC-R Approval (Russia), FCC 47CFR Parts 15, CE—Low Voltage Directive 73/23/EEE (Europe), RCM (Australia/New Zealand), KCC (South Korea), RoHS Directive 2002/95/EC (Europe), VCCI (Japan), BIS (India), CCC (China)

Arbor Enterprise Manager 7000 Appliance (End of Sale)

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 480GB 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

Features	VMware	KVM
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; Memory: 6GB; Storage: 100GB	vCPUs: 2; Memory: 6GB; Storage: 100GB; SR-IOV Support
Supported Hypervisors	VMware vSphere 5.5 or newer	KVM kernel 3.19 or newer, QEMU 2.0
Maximum Inspected Throughput / Instance	1 Gbps	10 Gbps
Maximum DDoS Flood Rate / Instance	910 Kpps	12 Mpps
Number of Protection Groups	10 (2 vCPUs); 50 (>=4 vCPUs)	10 (2 vCPUs); 50 (>=4 vCPUs)

Decryption Capabilities

- Supports Perfect Forward Secrecy (PFS) through TLS Proxy.
- Performance data are measured with 2048-bit key.

Performance	TLS Proxy	Cryptographic Acceleration Module (CAM)
Connections/Sec.	• Each AED 2800 & 8100 appliance supports up to 2700 connection/sec. • Each AED 2600 appliance supports up to 1500 connections/sec.	• Each AED 2600, 2800 & 8100 appliance supports up to 97K connection/sec.
Inbound Inspected Throughput	• Each AED 2600, 2800 & 8100 appliance support up to 1.8 Gbps.	• AED 2800 & 8100 provide up to 18 Gbps. • AED 2600 provides up to 18 Gbps.

✓ Supported
✖ Unsupported
❶ Supported for TLS 1.3
❷ Supported for TLS 1.2
❸ Unsupported in FIPS mode

Supported Cipher Suites

IANA Name	TLS Proxy	CAM
TLS_AES_256_GCM_SHA384	✓ ❶	x
TLS_AES_128_GCM_SHA256	✓ ❶	x
TLS_CHACHA20_POLY1305_SHA256	✓ ❶	x
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	✓	x
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	✓	x
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	✓	x
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	✓	x
TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256	✓	x
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256	✓	x
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	✓	x
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	✓	x
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA	✓	x
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	✓	x
TLS_RSA_WITH_AES_128_GCM_SHA256	✓	x
TLS_RSA_WITH_AES_256_GCM_SHA384	✓	x
TLS_RSA_WITH_AES_128_CBC_SHA	✓	✓ ❷
TLS_RSA_WITH_AES_256_CBC_SHA	✓	✓ ❷
TLS_RSA_WITH_3DES_EDE_CBC_SHA	✓	✓ ❷
SSL_RSA_WITH_3DES_EDE_CBC_SHA	x	✓ ❷
TLS_RSA_WITH_AES_128_CBC_SHA256	x	✓
TLS_RSA_WITH_AES_256_CBC_SHA256	x	✓
TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256	x	✓

IANA Name	TLS Proxy	CAM
TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256	x	✓
TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384	x	✓
TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384	x	✓
TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256	x	✓
TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256	x	✓
TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384	x	✓
TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384	x	✓
TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA	x	✓ ❷
TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA	x	✓ ❷
TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA	x	✓ ❷
TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA	x	✓ ❷
TLS_ECDH_RSA_WITH_AES_128_CBC_SHA	x	✓ ❷
TLS_ECDH_RSA_WITH_AES_256_CBC_SHA	x	✓ ❷
TLS_RSA_WITH_RC4_128_SHA	x	x
TLS_RSA_WITH_RC4_128_MD5	x	x
TLS_RSA_WITH_DES_CBC_SHA	x	x
SSL_RSA_WITH_DES_CBC_SHA	x	x

Note: Unlike the passive decryption capabilities provided by CAM, the TLS proxy plays an active role in cipher suite negotiation. This active role allows the TLS proxy to select the most modern, secure cipher suites, which eliminates the need to support a larger set of older, less secure cipher suites.

If the client and server support a cipher suite that the TLS proxy supports, then the client can connect and the TLS proxy can decrypt traffic. In this case, the cipher suite that AED uses with the TLS proxy might be different than the cipher suite that AED uses when the TLS proxy is not present.

For more information about the cipher suites and their security efficacy, refer to the SSL Labs web site at https://www.ssllabs.com/

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-2303 05/2023