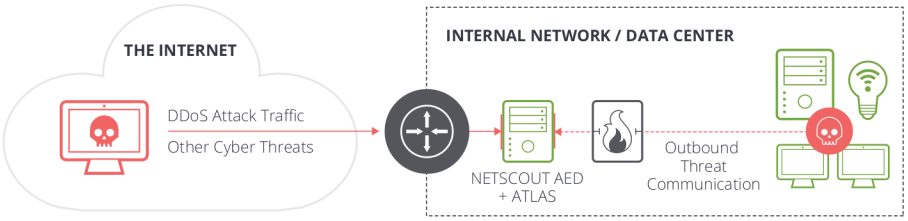
NETSCOUT AED (Arbor Edge Defense)

Pierwsza i Ostatnia Linia Inteligentnej, Automatycznej Ochrony na Styku Sieci

Spójrzmy prawdzie w oczy. Nie żyjemy w czasach pokoju. Czy to nowe formy ataków DDoS, ransomware, phishing, ataki na urządzenia BYOD czy IOT, nad organizacjami nieustannie wisi widmo różnego rodzaju zagrożeń. Aby zaadresować te ewoluujące zagrożenia, nowoczesny stack bezpieczeństwa stał się większy i bardziej skomplikowany – jednak jak pokazują najnowsze raporty o atakach i wyciekach danych, jest to wciąż za mało.

Zespoły bezpieczeństwa potrzebują najlepszych w swojej klasie rozwiązań cyberbezpieczeństwa, które umożliwią wykrywanie i blokowanie wszystkich typów zagrożeń – zarówno w ruchu przychodzącym, jak i w komunikacji wychodzącej, pochodzącej z zainfekowanych urządzeń w sieci. Niemniej istotna jest też możliwość integracji tych rozwiązań z już istniejącym zestawem rozwiązań bezpieczeństwa w organizacji w celu konsolidacji funkcjonalności oraz redukcji kosztów, stopnia skomplikowania i ryzyka.

NETSCOUT AED (Arbor Edge Defense) jest takim właśnie rozwiązaniem. Unikalne umiejscowienie AED na styku sieci (pomiędzy routerem a firewallem), bezstanowy silnik procesujący pakiety oraz ciągły stream danych o najnowszych zagrożeniach płynący z platformy ATLAS umożliwia rozwiązaniu AED automatyczne wykrywanie i blokowanie podejrzanej komunikacji, zarówno przychodzącej jak i wychodzącej. W ten sposób AED przejmuje rolę pierwszej i ostatniej linii ochrony.



Rysunek 1: Unikalne umiejscowienie AED na styku sieci + bezstanowy silnik procesujący pakiety + ciągły stream danych o najnowszych zagrożeniach płynący z platformy ATLAS = Pierwsza i ostatnia linia ochrony przed zaawansowanymi zagrożeniami.

Korzyści Arbor Edge Defense:

Pierwsza linia obrony: Wdrożony na styku sieci, wykorzystując technologię bezstanowego procesowania pakietów i wyposażony w miliony IoC, AED wykrywa zagrożenia w komunikacji przychodzącej, tym samym odciążając urządzenia stanowe takie jak NGFW.

Ostatnia linia obrony: AED umożliwia wykrywanie wychodzącej komunikacji do znanych adresów IP, domen, URL, lokalizacji powiązanych z zagrożeniami, a przeoczonej przez istniejące rozwiązania bezpieczeństwa; tym samym przyśpiesza proces wykrycia malware w sieci zanim zdoła się rozpropagować.

Kontekstowe Dane o Zagrożeniach: Kiedy IoC zostaje zablokowane, AED wykorzystuje dane płynące z platformy ATLAS aby dostarczyć więcej kontekstu związanego z danym IoC, umożliwiając tym samym zespołom security oszacowanie ryzyka i/lub podjęcie działań proaktywnych.

Najlepsza w klasie ochrona DDoS: AED automatycznie wykrywa i blokuje ataki aplikacyjne, wysycenia stanu TCP i wolumetryczne do 40Gbps. W przypadku wystąpienia większego ataku, funkcja Cloud Signalling automatycznie wysyła prośbę o pomoc do ISP/MSSP.

Integracja: REST API, wsparcie dla STIX/TAXII, Syslog, CEF, LEEF umożliwia zintegrowanie AED z istniejącymi rozwiązaniami bezpieczeństwa.

NAJWAŻNIEJSZE FUNKCJONALNOŚCI

Pierwsza i ostatnia linia obrony

Unikalne umiejscowienie AED na styku sieci (pomiędzy routerem a firewallem), bezstanowy silnik procesujący pakiety oraz ciągły stream danych o najnowszych zagrożeniach z platformy ATLAS umożliwia rozwiązaniu AED automatycznie wykrywać i blokować podejrzaną przychodzącą i wychodząca komunikację.

Integracja

REST API, wsparcie dla STIX/TAXII, Syslog, CEF, LEEF oraz kontekstowe Threat Intelligence płynące z ATLAS umożliwia zintegrowanie AED z istniejącymi rozwiązaniami bezpieczeństwa.

Inteligentnie zautomatyzowana, hybrydowa ochrona DDoS

Inteligentnie zautomatyzowana i w pełni zarządzalna kombinacja ochrony w chmurze (via Arbor Cloud) oraz na styku sieci (via AED), w trybie ciągłym zasilana najnowszymi danymi o zagrożeniach, stanowi najbardziej kompleksową formę ochrony przed dzisiejszymi atakami DDoS.

Wykrywanie i blokowanie podejrzanej komunikacji wychodzącej

Pochodzące z ATLAS oparte o reputacje najnowsze dane o zagrożeniach, umożliwiają platformie AED wykrywać i blokować komunikację wychodzącą od zainfekowanych hostów w sieci, tym samym wspierając zespoły bezpieczeństwa w szybszej reakcji na incydenty.

Wsparcie dla środowisk wirtualnych i chmurowych

vAED jest wersją wirtualną rozwiązania AED i może być wdrażany w środowisku wirtualnym Twojej organizacji, takim jak Amazon Web Services, dostarczając kompleksowej ochrony dla hybrydowych infrastruktur.

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	
Ioc Types	IP address, fully qualified domain names, URLs	

4Sync Solutions sp. z o.o. –SKA
ul. Instalatorow 17, 02-237 Warszawa

tel.: 22 299 17 00
Dział Handlowy: sales@4sync.pl
Wsparcie techniczne: support@4sync.pl