NETSCOUT AED (Arbor Edge Defense)

第一道與最後一道 - 智慧型邊界防禦系統

重要的功能與優勢

第一道與最後一道防線

AED 位於網絡邊緣的獨特位置，其無狀態數據包處理引擎和 ATLAS® 全球威脅情報，讓它可阻止來自受危害主機的入埠威脅和對外通訊。

與安全堆疊整合

REST API、對 STIX/TAXII 的支援以及 ATLAS 所支持的情境威脅情報 (Contextual Threat Intelligence)，皆使 AED 能夠整合至現有的安全堆疊與流程中。

智慧型自動化與混合 DDoS 防護

透過雲端服務 Arbor Cloud 及 AED 本地端設備的智慧型自動化組合，並結合 ATLAS 全球威脅情報；提供最全面的防護，免於當今的 DDoS 攻擊。

對外威脅通訊的偵測與阻止

AED 透過 ATLAS 所取得的威脅情報，讓它能偵測並阻止來自內部受危害主機的對外通訊，協助阻止惡意軟體或資料外洩的進一步擴散。

支援虛擬與混合雲環境

vAED 是 AED 設備的虛擬版本，可在您的私有虛擬環境 (**如亞馬遜雲端服務** Amazon Web Services) 中運作，為您的混合雲環境提供統一防護。

讓我們面對現實。*沒有所謂的和平時期*。無論是否是新形式的 DDoS 攻擊、勒索軟體或網絡釣魚皆嘗試入侵 BYOD 和物聯網設備，組織都持續面臨著各種類型的進階網路威脅。為處理這些不斷演變的威脅，現代安全性堆疊變得越來越大，越來越複雜，但遺憾的是，每天都有資料外洩和停機報告出現，證明這種作法仍是失敗的。

安全團隊需要最佳的網路安全解決方案，可以偵測並阻止所有類型的網路威脅，包括從 Internet 至企業內部的外對內威脅和已被入侵的內部主機其對外惡意通訊。同樣重要的是，這些解決方案亦必須能夠整合到企業現行的網路及安全架構中以降低成本、複雜性和風險。

NETSCOUT 的 AED (Arbor Edge Defense) 就是這樣的解決方案。AED 在網路邊緣 (即路由器和防火牆之間) 的獨特位置，其無狀態數據包處理引擎以及從 NETSCOUT 的 ATLAS Threat Intelligence 饋送所收到之連續根據評價的威脅情報，使其能夠自動偵測並阻止入埠威脅和來自內部受危害主機的對外通訊 - 基本上是組織的第一道和最後一道防線。

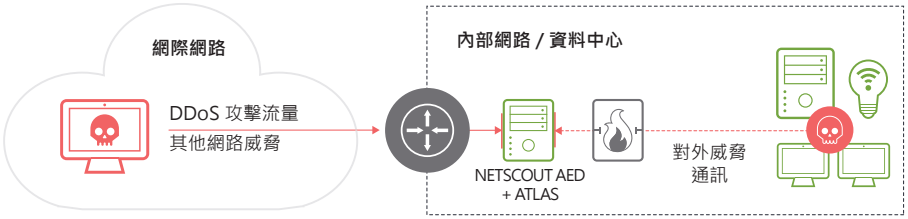

圖 1：AED 在網路邊緣上的獨特位置 + 無狀態封包處理引擎 + ATLAS 全球威脅情報 = 進階網路威脅的第一道和最後一道防線。

Arbor Edge Defense 的優勢：

- **第一道防線：**AED 部署在網路外圍，採用無狀態技術並配備數百萬個入侵指標 (IoC)，可偵測並阻止傳入的網路威脅，從而減輕狀態設備 (如下一代防火牆) 的壓力。
- **最後一道防線：**AED 可以偵測並阻擋對已知的錯誤 IP 地址、網域、URL、地理位置的對外通訊，從而協助阻止組織內惡意軟體進一步擴散，避免數據洩露。
- **情境威脅情報：**當入侵指標被阻擋時，AED 利用 NETSCOUT ATLAS 的全球威脅情報提供更多與 IoC 相關的上下文情境，從而協助安全團隊確認風險及 / 或為安全團隊提供更多訊息，以利主動使用其他安全工具進行搜索。
- **最佳 DDoS 防護：**AED 可以自動偵測並阻止傳入應用層、TCP 狀態耗盡和最大 40 Gbps 的 DDoS 攻擊。如果發生較大規模的 DDoS 攻擊，雲端傳訊會自動將流量重新繞行到 Arbor Cloud 或 MSSP 的雲端緩解中心。
- **整合：**AED 強大的 REST API 以及對 STIX/TAXII 的支援，使 AED 能夠整合至現有的安全堆疊與程序中。

NETSCOUT AED 設備

特性	2600	2800
外型尺寸	**機箱：**2U 機架高度；**高度：**3.45 英寸 (8.67 公分)； **寬度：**17.4 英寸 (43.53 公分)； **深度：**20 英寸 (50.8 公分)；**重量：**36.95 磅 (17.76 公斤)	
電源選項	**DC：**2 個直流備援、熱交換電源供應器；**DC 電源額定功率：**-40 至 -72 Vdc，最大值 28/14 A(每個直流輸入)；**AC：**2 個交流備援，熱交換電源供應器； **交流電源額定功率：**100 至 240 VAC，50 至 60 Hz，最大 12/6 A；**Watts：**一般 315 瓦，最高 375 瓦	
硬碟	2 x 120 GB SSD，RAID 1 組態	2 x 240 GB SSD，RAID 1 組態
環境	**操作：**溫度：41°至 104° F (5°至 40° C)，濕度 5 - 85%；**非操作：**溫度 -40°至 158° F (-40°至 70° C)，濕度 95%	
記憶體	32 GB	64 GB
處理器	2 x Intel Xeon E5-2608L v3(6 核)2 GHz	2 x Intel Xeon E5-2648L v3 (12 核) 1.8Ghz
作業系統	專屬嵌入式 ArbOS® 作業系統	
管理介面	2 x 10/100/1000 BaseT 銅纜；RJ-45 序列控制台連接埠	2 x 10/100/1000 BaseT 銅纜；RJ-45 序列控制台連接埠
防護介面	• 4、8 或 12 1G 旁路連接埠 (銅纜、SX 光纖、LX 光纖) • 4 x 10 G 旁路連接埠加上 0、4 或 8、1 G 旁路連接埠	• 4 x 10 GigE (SR 或 LR 光纖) • 8 x 10 GigE (SR 或 LR 光纖) • 8 x 10 GigE (SR 或 LR 光纖) + 4 x 1 GigE (SX 或 LX 光纖，或銅纜)
流量旁路選項	整合硬體旁路；內部「軟體」旁路流量而不經過檢查	
延遲	低於 80 微秒	
可用性	內嵌旁路，雙電源供應器，固態硬碟 RAID 叢集	
平均無故障時間 (MTBF)	44,000 小時	
法規遵循	UL60950-1/CSA 60950-1 (美國 / 加拿大)；EN60950-1 (歐洲)；IEC60950-1 (國際)，包括所有國際偏差的 CB 證書與報告；GS 證書 (德國)；EAC-R 許可 (俄羅斯)；CE — 低電壓指令 73/23/EEE (歐洲)；BSMI CNS 13436 (台灣)；KCC (南韓)；RoHS 指令 2002/95/EC (歐洲)	

DDoS 與進階網路威脅防護

特性	2600	2800
濾後效能	授權 100 Mbps、250 Mbps、500 Mbps、1 Gbps、2 Gbps、5 Gbps、10 Gbps、15 Gbps、20 Gbps	授權 10 Gbps、20 Gbps、30 Gbps、40 Gbps；軟體可升級
最大 DDoS 洪水攻擊防禦率	高達 15 Mpps	高達 28.80 Mpps
同時連線數	不適用：AED 不追蹤連線	
每秒 HTTP(s) 連線數	368 K 在建議的保護等級；613 K 僅限篩選清單保護	1,351 K 在建議的保護等級；1,497 K 僅限篩選清單保護
SSL 解密選項	**處理效能：**750 Mbps 和 5 Gbps 選項 **HTTPS 連線數：**最高 7,500 (750 M HSM) 或 45,000 (5 G HSM) **並行工作階段：**高達 150,000	**處理效能：**高達 5 Gbps **HTTPS 連線數：**高達 45,000 **並行工作階段：**高達 150,000
	支援的加密協議：SSL 3.0、TLS 1.0,1.1 和 1.2；支援的 Cypher 套件：RSA、ECDH、ECDHE；支援 2 級和 3 級 FIPS 140-2；3 級 FIPS 140-2 單獨「可信路徑」管理；安全防篡改外殼；如果外殼遭破壞，會清除金鑰	
最大金鑰數 / 憑證對數	1998	
受保護的端點	無限制	
驗證	本機資料庫，RADIUS；TACACS	

管理	SNMP GET v1 與 v2c；SNMP TRAP v1、v2c、v3；CLI；網頁 UI；HTTPS；SSH 可自訂，基於角色的管理；AED 控制台可以管理高達 50 個 AED(設備和 / 或執行 KVM 管理程序的虛擬 AED)；託管 AED 必須至少能執行 v5.11；vAED 控制台可以在 VM 管理程序上執行。
保護群組數	100
報告和鑑識	即時和歷史的 IPV4 和 IPV6 流量報告、依據保護群組和封鎖主機的廣泛下探分析，包括總流量、通過 / 封鎖、主要目的地 URL/ 服務 / 網域、攻擊類型、封鎖來源、根據 IP 位置的主要來源。即時封包可視性。
DDoS 防護	TCP/UDP/HTTP(S) 洪水攻擊、殭屍網路防護、激進駭客攻擊防護、主機行為防護、反偽裝、可設定流量運算式過濾、根據荷載運算式過濾、永久和動態黑名單 / 白名單、流量成形、HTTP、DNS 和 SIP 的多重保護、TCP 連線限制、片段攻擊、連線攻擊。
模式	Inline active, Inline Inactive (分檔、不阻擋), SPAN 旁路監控
通知	SNMP TRAP、syslog、電子郵件
雲端傳訊	是 (與服務供應商或 Arbor Cloud 協作進行 DDoS 攻擊緩解)
網頁式 GUI	支援多語系使用者介面
支援的瀏覽器	Internet Explorer v10 - 11、Firefox ESR v31、Firefox v40、Chrome v44、Safari v6
最大 IoC	300 萬以上
Ioc 類型	IP 位址、完全限定的網域名稱、URL

NETSCOUT AED 控制台

支援平台	Arbor 設備；虛擬機
最大數量 AED 管理	50
虛擬 AED 控制台需求	VMware vSphere 5.5+；2 個 CPU; 100 GB 硬碟空間；4 GB RAM；1 個管理界面 (第二個管理界面為選配)
管理選項	配置或視圖 (個別和 / 或所有 AED) : 硬體和軟體健康 ; 系統和安全警報 ; 被封鎖的主機 ; ATLAS 威脅摘要 ; 伺服器類型，防護組 (IPV4/6)；黑名單 / 白名單；執行管理報告
支援的瀏覽器	Internet Explorer v10 - 11、Firefox ESR v31、Firefox v40、Chrome v44、Safari v6

NETSCOUT AED 控制台 7000 設備

記憶體	128G (8x16G DIMMs)
處理器	Intel Xeon (12 核) - ES-2648Lv3 - 1.8GHz - 20M 快取
電源需求	備援、負載均衡及自動感應的 850 W 雙電源供應器；AC：100-240 VAC、50/60 Hz、12/6 A；DC；-40 至 -72 V、最大 28/14 A
外型尺寸	**機箱：**2U 機架高度 ; **高度：**3.45 英寸 (8.67 公分) ; **寬度：**17.4 英寸 (43.53 公分) **深度：**20 英寸 (50.8 公分) ; **重量：**36.95 磅 (17.76 公斤) ；標準 19 和 23 英寸機架式安裝
硬碟	6 個 RAID 5 配置的 480 GB 固態硬碟
網路介面	2 x 1 GigE(適用於 Copper、GigE SX 或 GigE LX 的 SFP)
環境	**操作：**溫度 41°至 104° F (5°至 40° C)；濕度 95%；**非操作：**溫度 73°至 104° F (23°至 40° C)
作業系統	專屬嵌入式 ArbOS® 作業系統
法規遵循	UL60950-1/CSA 60950-1；EN60950-1；IEC60950-1； 加入所有國家偏差的 CB 證書與報告；SONCAP；EAC Mark；CE —低電壓指令 2014/35/EU；KCC Mark、RoHS 2011/65/EU；Telcordia GR-63；ETSI EN 300 019；NEBS ; ETSI EN 300 753 ; cULus 標誌 ; IC ICES-003 甲類 ; 符合 EMC 指令 2014/30/EU 的 CE 標誌 ; EN55022 甲類 ; EN55024；EN61000-3-2；EN61000-3-3；CISPR 22 甲類、CISPR 24 抗擾度；FCC 47 CFR Parts 15 甲類

虛擬 AED

虛擬網路功能 (VNF) 編排	Cloud-Init v0.7.6、Openstack Kilo 與 Mitaka 系列、OpenStack Heat、OpenStack Tacker、Ansible、Nokia Cloudband、Cisco NSO/ESC、Cisco NFVIS、Amdocs、Netcracker 以及其他 ONAP 或 ETSI NFV 管理和編排技術	
支援亞馬遜 AWS	支援亞馬遜 EC2	
最低虛擬機器需求	vCPUs：2；NIC：1 至 10；記憶體：6 GB；儲存容量：100 GB	
支援的管理程序	VMware vSphere 5.5+	KVM kemel 3.19 QEMU 2.0
檢查輸送量 / 執行個體	1 Gbps	1 Gbps
最大 DDoS 洪水攻擊防禦率 / 執行個體	910 Mbps	600 Kpps
保護群組數	10; 50 配有 4 vCPUs 與 12 GB RAM	10; 50 配有 4 vCPUs 與 12 GB RAM

NETSCOUT

企業總部
NETSCOUT Systems, Inc.
Westford, MA 01886-4105
電話：+1 978-614-4000
www.netscout.com

銷售資訊
美國免付費專線：800-309-4804
(下列為國際電話號碼)

產品支援
美國免付費專線：888-357-7667
(下列為國際電話號碼)

NETSCOUT 在超過 32 個國家提供銷售、支援和服務。全球地址與國際電話號碼請參考 NETSCOUT 網站：
www.netscout.com/company/contact-us

SECPDS_013_EN-1801 2018 年 7 月