NETSCOUT Arbor Edge Defense

企業級別的DDoS防禦系統

重要的功能與優勢

第一道與最後一道防線

Netscout DDoS 防禦系統位於網路的獨特位置，其無狀態處理引擎，讓它可阻止來自受危害主機的攻擊威脅和對外通訊。

與安全堆疊整合

RESTFUL 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 NETSCOUT DDOS 防禦系統 能夠整合至現有的安全環境與流程中。

智慧型自動化與混合 DDoS 防護

透過雲端清洗服務 Arbor Cloud 及本地端設備的智慧型自動化組合，並結合威脅情報；提供最全面的防護，免於當今的 DDoS 攻擊。

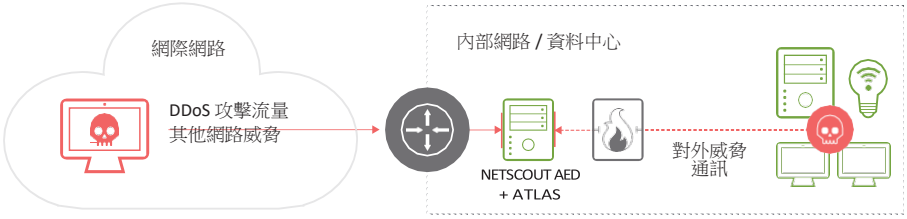
對外威脅通訊的偵測與阻止

NETSCOUT DDOS 防禦系統 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。

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DDoS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(Arbor Edge Defense) 就是這樣的解決方案。NETSCOUT DDOS 防禦系統 在網路邊緣（即路由器和防火牆之間）的獨特位置，其無狀態處理引擎以及從 NETSCOUT 的 ATLAS 所收到的威脅情報，使其能夠自動偵測並阻止DDoS威脅和來自內部受危害主機的對外通訊－這就是組織的第一道和最後一道防線。



Arbor Edge Defense 的優勢：

- 第一道防線：NETSCOUT DDOS 防禦系統 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，從而減輕狀態設備的壓力。
- 最後一道防線：NETSCOUT DDOS 防禦系統 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，NETSCOUT DDOS 防禦系統 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：NETSCOUT DDOS 防禦系統 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：NETSCOUT DDOS 防禦系統 強大的 REST API 以及對 STIX/TAXII 的支援，使 NETSCOUT DDOS 防禦系統 能夠整合至現有的安全堆疊與程序中。

DDoS 網路威脅防護

濾後效能	授權 100 Mbps、250 Mbps、500 Mbps、1 Gbps、2 Gbps、5 Gbps、10 Gbps、15 Gbps、20 Gbps
最大 DDoS 洪水攻擊防禦率	15 Mpps
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
SSL 解密選項	處理效能：在2,048-bit key的加密等級下， 每秒加密連線數為1500
	支援的加密協議：SSL 3.0、TLS 1.0,1.1 ,1.2 ,1.3； 支援的 Cypher 套件：RSA、ECDH、ECDHE
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；
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 (監測、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、Chro□e 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