Infoblox Advanced DNS Protection

主要功能

- DNS 安全威脅防護：
  持續監控、偵測並捨棄 DNS 型態攻擊 (包括 DDoS、惡意探索、放大攻擊與反射) 封包。
- 自動更新：
  使用安全威脅分析與研究機制，偵測並消除新型與演化的安全威脅。
- 集中化的檢視：
  掌握您網路面臨的攻擊類型與模式。
- 可調整的流量閾值：
  微調安全防護參數。
- 強化的處理功能：
  透過新一代的可程式化處理器，提供抵禦安全威脅所需的專屬運算能力。
- 完整的強化設備產品線：
  選擇適合您網路環境的設備。
- 已取得專利的 Infoblox Grid™：
  將所有設備的設定與更新程序自動化，讓您以自動化的方式快速將安全性原則散發給所有 Infoblox 進階設備。

為關鍵 DNS 服務提供嚴密的安全防護

DNS 伺服器—經常遭受DDoS 與其他攻擊類型的目標

攻擊者通常會搜尋安全防護強度最弱的連結與壓力點，企圖透過受害企業資源遂行不法活動，而「網域名稱系統」(DNS) 通訊協定在本質上便是容易遭受惡意探索的一個環節。因此，外部與內部 DNS 攻擊一直是一種日益增多的攻擊類型。DNS 分散式阻斷服務 (DDoS) 攻擊的目標是使 DNS 伺服器無法運作並耗用網路頻寬，進而使關鍵 IT 應用程式 (例如電子郵件、網站、VoIP 與軟體即服務 (SaaS)) 無法運作。

單單在去年，DNS 攻擊數目就增加了 200% 以上。在過去 12 個月內，美國與英國的中型與大型企業中就有 31% 的企業面臨至少一次 DDoS 攻擊。有多家服務提供者與 DNS 主機服務提供者的 DNS 伺服器遭受 DDoS 攻擊而癱瘓，使得客戶無法存取其網站且代管的數百萬個網站無法運作。這些事件所造成損害的成本非常高—根據弗雷斯特研究公司 (Forrester Research) 預估，24 小時無法運作的平均財務損失高達 2,700 萬美元。此類攻擊的受害者可能會面臨營收降低、客戶流失與品牌價值受損等結果。

透過 Infoblox Advanced DNS Protection 減輕此問題的影響

Infoblox Advanced DNS Protection 提供獨特的防護方式來抵禦 DNS 型態攻擊。不像依賴於過度佈建之基礎結構或簡單的回應速率限制 (限制全部或全不限制) 的方式，Advanced DNS Protection 會以智慧型方式偵測 DNS 攻擊並自動捨棄惡意 DNS 流量，同時提供穩定安全的 DNS 服務。

Advanced DNS Protection 解決方案由下列元件組成：

- Infoblox 進階設備：以安全為設計考量的 DNS 伺服器
- Infoblox Advanced DNS Protection 服務：此軟體加上自動更新功能可提供嚴密的安全防護，協助您抵禦現有與新型的 DNS 伺服器安全威脅

強化的 DNS 伺服器—最佳的 DNS 型態攻擊防護解決方案

「進階設備」是以安全為設計考量的強化型 DNS 伺服器。您可以將它設定為外部權威伺服器或 DNS 遞迴伺服器，以協助您抵禦攻擊。沒有任何方式比使用 DNS 伺服器來協助保護網路並抵禦 DNS 型態攻擊來得更有效。

獨特的偵測與損害減輕機制

Advanced DNS Protection 會持續監控、偵測及捨棄 DNS 型態攻擊 (包括 DDoS、惡意探索與通訊協定異常封包傳送) 封包並減輕此類攻擊對您的環境造成的影響，同時回應合法流量。以安全威脅分析與研究為基礎的自動更新有助於在新型與演化的 DNS 相關攻擊出現時即予以偵測並消除。

Infoblox Advanced DNS Protection

Infoblox CONTROL YOUR NETWORK

優點

- 快速識別 DNS 型態攻擊並予以回應，以達成穩定安全的 DNS 服務。
- 維持企業營運不中斷與網路可靠性。
- 在新型與演化的 DNS 相關攻擊出現時即予以偵測並消除。
- 保護您的企業，讓您免於因為網路停機造成的營收降低與品牌價值受損等情況。
- 檢視您網路所面臨的所有攻擊，並根據我們提供的詳細資訊採取因應措施。
- 根據您企業的特殊 DNS 流量模式需求設定 DNS 安全防護參數。
- 讓您的 DNS 服務即使面臨攻擊仍能正確運作。

集中化的攻擊分析報告

Advanced DNS Protection 透過詳盡的報告以集中化檢視為您提供網路攻擊分析，並提供可協助您採取因應措施的資訊。這些報告包括諸如依類別、規則、嚴重性、成員趨勢分析與時間型分析排序的事件數目等詳細資料。您可以透過「Infoblox 報告伺服器」存取這些報告。

可根據您的特殊需求而調整

每家企業的 DNS 流量模式都不盡相同，而各個流量模式在每個季度、每天的不同時間或不同的地理位置也會有所差異。Advanced DNS Protection 提供可調整的流量閾值供您設定，讓您可以根據您的特殊 DNS 流量模式來微調安全防護參數。這樣讓您可以回應正常流量，同時封鎖或捨棄惡意流量。

Advanced DNS Protection 所抵禦的攻擊類型摘要*

* 此表格只是 Advanced DNS Protection 解決方案所抵禦的攻擊分類概觀，並非完整清單。

提供選項

DNS 反射/DrDoS 攻擊	使用第三方 DNS 伺服器 (開放式解析) 來遂行DOS 或 DDOS 攻擊
DNS 放大攻擊	使用精心變造的查詢來建立放大的回應，讓受害者飽受洪水流量的攻擊
DNS 型態惡意探索	惡意探索 DNS 軟體弱點的攻擊
TCP/UDP/ICMP 洪水攻擊	以洪水流量攻擊網路或服務，造成網路層級第 3 層的阻斷服務，使該網路或服務無法正常運作
DNS 快取毒害	以非法惡意的網際網路地址汙染 DNS 快取資料
通訊協定異常封包傳送	傳送格式不正確的封包與查詢，讓伺服器當機
偵察探測	攻擊者在發動大型 DDoS 或其他類型攻擊前，嘗試取得網路環境資訊的動作
DNS 通道穿越	透過 DNS 通道傳輸其他通訊協定類型的資料，以突破封鎖

Infoblox Advanced DNS Protection

Infoblox
CONTROL YOUR NETWORK

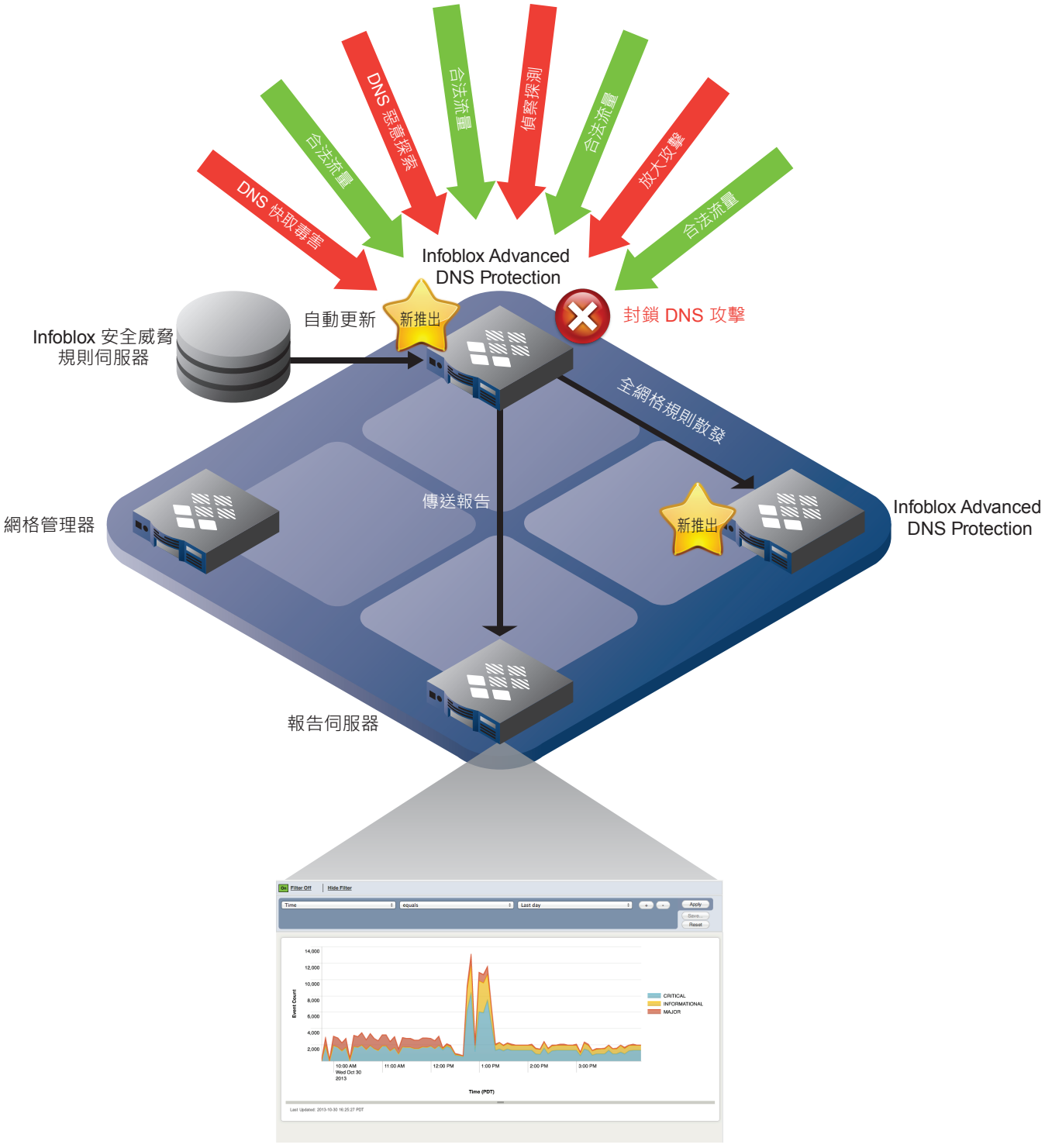


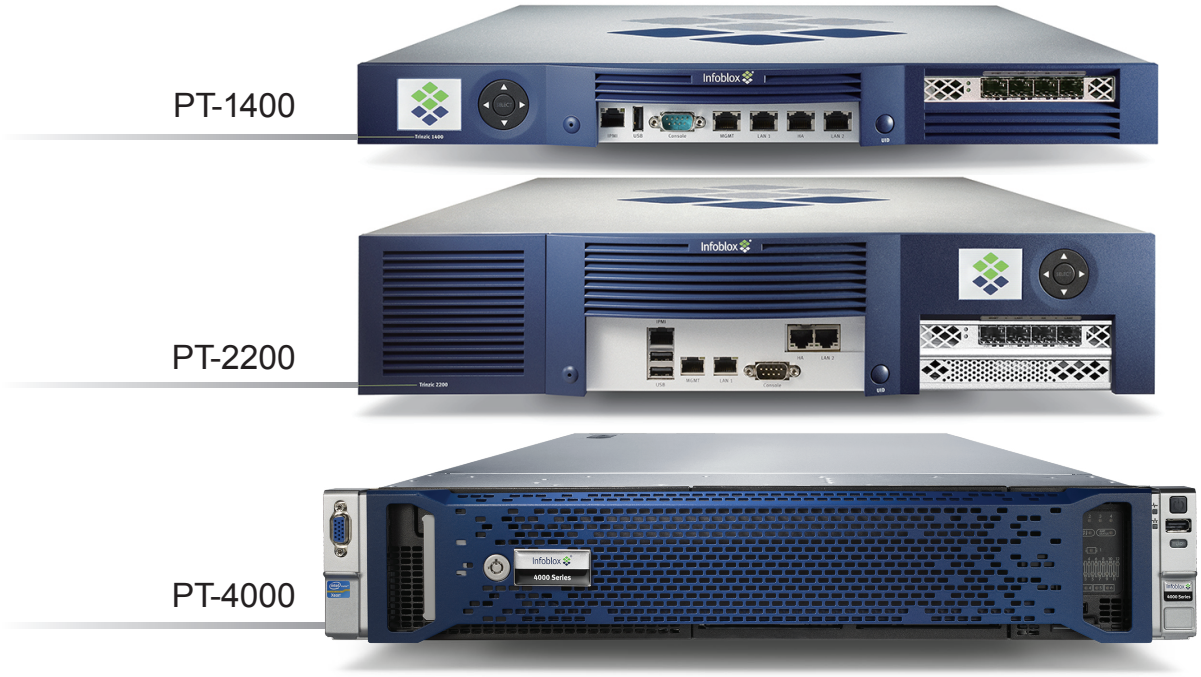
圖 1：Infoblox Advanced DNS Protection 提供獨特的防護方式來抵禦 DNS 型態攻擊。

Infoblox Advanced DNS Protection

Infoblox CONTROL YOUR NETWORK

進階設備以三種實體平台提供。

「進階設備」具備新一代的可程式化處理器，可提供抵禦安全威脅所需的專屬運算能力。設備同時提供 AC 交流電與 DC 直流電電源供應器選購項目。



關於Infoblox

Infoblox (NYSE:BLOX)是自動化網路控制解決方案的領導廠商，許多全球最大的企業都採用我們的整合式強化設備型軟體來進行業務持續性、可用性和合規性。我們提供整合式的 DNS、DHCP、IP 位址管理 (IPAM)，以及網路自動化 (Network Automation) 產品方案，它們是一種可將終端使用者、設備和網路連接起來的基礎技術。這些解決方案已經成功幫助全球6,500家大型企業和電信服務提供商能夠轉型和調整複雜的網路。Infoblox可幫助IT管理人員從複雜的網路控制負擔中解放出來，降低成本並提高準確性和快速執行時間。Infoblox總部位於加州聖塔克拉拉，在全球25個國家營運。

sales-tw@infoblox.com | www.infoblox.com.cn | www.infoblox.com

Infoblox 代理商 docutek達友科技 服務專線：02-2658-8970 | www.infoblox.com | http://www.docutek.com.tw