Infoblox
CONTROL YOUR NETWORK

白皮書

您已經完全準備好對抗 DNS 攻擊了嗎?

強化關鍵的 DNS 基礎結構

Infoblox 代理商 docutek 達友科技

服務專線: 02-2658-8970 | http://www.docutek.com.tw

您已經完全準備好對抗 DNS 攻擊了嗎?

強化關鍵的 DNS 基礎結構

自 2012 年第 1 季起，目標為「網域名稱系統」(DNS) 的基礎結構攻擊數目增加了 200%[1]。為什麼？因為 DNS 的本質就是容易遭受惡意探索。

- 大部分的企業防火牆是設定為允許連接埠 53 流量以允許提供 DNS 服務，這讓攻擊者能輕鬆規避您現有的防禦系統。
- 因為 DNS 查詢是不對稱的，所以產生的回應數目可能是查詢數目的數倍之多，這表示您的 DNS 系統本身會使得攻擊被放大。攻擊者只需要傳送一個資料封包就可能讓 DNS 系統產生數倍之多的回應，導致您的業務停擺。
- 攻擊者可以輕鬆地掩飾其身分，因為 DNS 是一種無狀態的通訊協定。

大型 IT 組織與服務提供者並沒有太多選擇，而只能盡量補強這些弱點，因為在網際網路時代，DNS 服務對於幾乎所有關鍵現代化業務功能而言都是不可或缺的。若沒有能正確運作的 DNS，智慧型手機將無法運作、企業將無法從事網路業務、團隊成員將無法有效溝通、生產力會降低、客戶滿意度會降低、營收會降低，而且公司的商譽也會受影響。

此白皮書的內容旨在說明如何解決 DNS 所面臨的安全威脅問題。我們將簡要說明 DNS 通訊協定的功能、分類並說明各種 DNS 型態攻擊以協助您釐清安全威脅，以及闡述並解釋可用的最佳解決方案：Infoblox Advanced DNS Protection，這是市面上第一個可進行自我保護並補強整體安全性結構的 DNS 設備。

DNS 的功能與其運作方式

在開始說明安全威脅與防護方式之前，讓我們先了解一下 DNS 的基礎概念。DNS 是記載網際網路上每個目的地的通訊錄。它負責將網域名稱 (例如 infoblox.com) 轉換為 IP 位址 (例如 54.235.223.101)。這表示 DNS 會決定通訊與要求是否能送達正確的位址。企業與服務提供者需要快速且精確的 DNS 服務，才能解析連入與連出流量的目的地以從事線上業務。與供應商、客戶及分公司之間的通訊形式包括電子郵件、網站與 HTTP 檔案傳輸。DNS 處理方式的潛在問題是：DNS 伺服器就如同購物中心的大門，對於小偷與客戶都一視同仁的都允許可以經由大門進入。

DNS 名稱伺服器有兩種型態：「權威名稱伺服器」與「遞迴名稱伺服器」。

- 權威 DNS 伺服器是公司服務的進入點。它們只會回應已設定的網域名稱查詢與特定區域集合中的名稱查詢。連線到網際網路的 DNS 伺服器通常是設定為權威模式，而此類型的伺服器是外部攻擊 (例如放大攻擊、反射與惡意探索) 的目標。
- 遞迴 DNS 伺服器 (亦稱為「快取伺服器」) 則會透過向其他名稱伺服器查詢以回應查詢要求。有時它們會從快取提取回應，這是「快取伺服器」這個名稱的由來。若遞迴伺服器在快取中找不到查詢目標，它會向網際網路的主要根源名稱主機重複該查詢並依循來自權威伺服器的轉介進行詢問，直到找到能回應查詢的名稱伺服器。換句話說，遞迴名稱伺服器仰賴於權威名稱伺服器。遞迴名稱伺服器通常部署於企業內部，為內部使用者提供服務。此類名稱伺服器容易遭受源自於企業內部使用者的攻擊。

DNS 安全威脅分類

在本文撰寫時，潛在安全威脅的種類極其繁多。我們在此處予以列出並簡短描述。

直接 DNS 放大攻擊的目標是癱瘓 DNS 伺服器的連外頻寬。此類攻擊的發動方式是傳送大量精心變造的 DNS 查詢，企圖使 DNS 伺服器產生非常大量的回應 (回應大小甚至可高達要求大小的 70 倍)。因為 DNS 仰賴「使用者資料包通訊協定」(UDP)，攻擊者可以使用小量的連外流量來使得 DNS 伺服器產生大量的回應，導致 DNS 伺服器的上傳頻寬耗盡，甚至最後演變成阻斷服務 (DoS)。

反射攻擊會使用網際網路上的第三方 DNS 伺服器 (通常是開放式遞迴名稱伺服器) 來遂行 DoS 或 DDoS 攻擊，方式是傳送查詢給該遞迴伺服器。遞迴伺服器將處理來自任何 IP 位址的查詢並傳回回應。攻擊者會將受害者的 IP 位址包含在查詢的來源 IP 中並送出此變造的 DNS 查詢，讓查詢中包含的是受害者的伺服器資訊，而非攻擊者的伺服器資訊。這樣一來，當遞迴名稱伺服器收到要求時，它會將所有回應傳送到受害者的 IP 位址。大量的此類「反射」流量會導致受害者的網站無法正確運作。

分散式反射 DoS (DrDoS) 攻擊結合了反射與放大效果，會大幅增加初始查詢的回應大小，並大幅提高受害者的伺服器因為負載過重而當機的機率。諷刺的是，設計目的是透過加密來保護 DNS 回應安全並提供快取毒害防護的「DNS 安全性延伸規格」(DNSSEC) 卻會造成此類型攻擊的危害更大，因為 DNSSEC 使用的加密編譯簽章會導致產生更大的 DNS 訊息。放大效果可能高達 100 倍，而且攻擊者可以使用殭屍網路 (通常由數以千計的伺服器所組成) 來大幅增加傳送的查詢數目。

這是危害程度極其嚴重且非常難以對抗的安全威脅。網際網路上大約有 3,300 萬部開放式遞迴 DNS 伺服器[2]，而其中有 2,800 萬部沒有制定存取控制機制 (ACL)，因此它們可能成為 DrDoS 攻擊的幫兇。

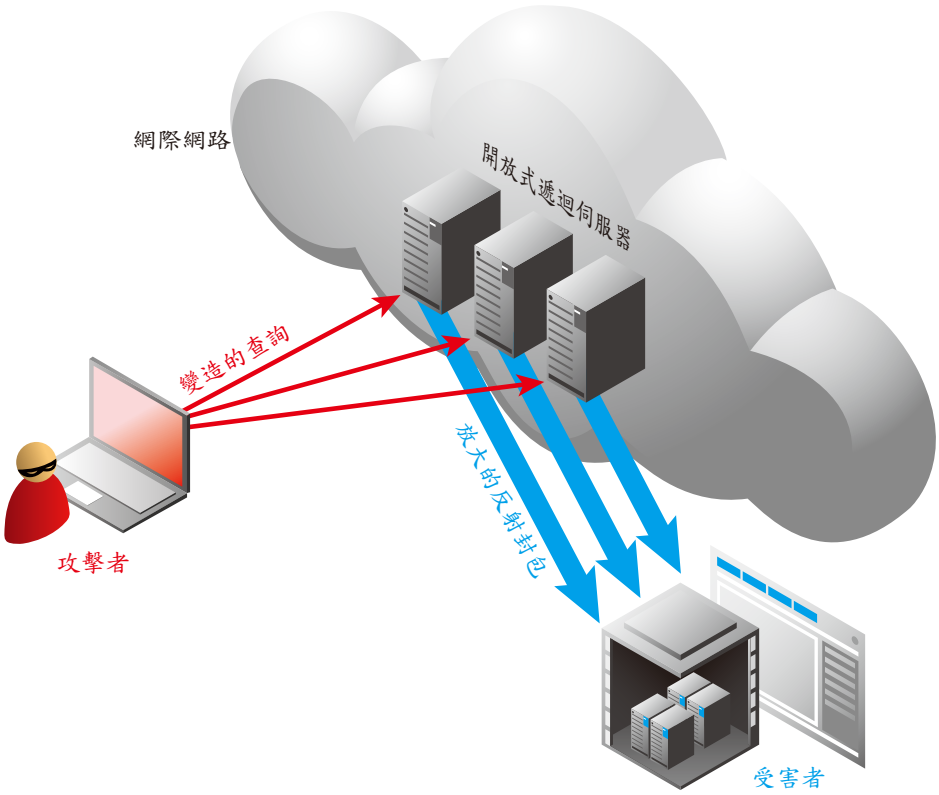

圖 1：分散式反射 DoS 攻擊

TCP/UDP/ICMP 洪水攻擊是一種利用大量封包造成網路頻寬與資源耗盡的攻擊類型。此類攻擊會利用「傳輸控制通訊協定」(TCP)、「使用者資料包通訊協定」(UDP) 與「網際網路控制訊息通訊協定」(ICMP)。

UDP 洪水攻擊會傳送大量 UDP 封包至遠端伺服器上的隨機連接埠，造成伺服器資源因為檢查聆聽特定連接埠的應用程式而耗盡 (因為並沒有那麼多應用程式在聆聽那些連接埠)。接著，遠端伺服器會被迫傳回大量「ICMP 無法與目的地取得連線」封包給攻擊者，說明無法連線到該目的地。攻擊者也能變造傳回 IP 位址，讓伺服器的回應不會傳送到攻擊者的伺服器。傳送回應會耗盡受害者的伺服器資源，並導致伺服器無法處理其他要求。

TCP SYN 洪水攻擊是由大量的半開放式 TCP 連線所組成，它會造成伺服器停止回應用戶端開啟新連線的其他要求。此類型的攻擊是利用 TCP 連線建立方式來遂行。每次用戶端 (例如瀏覽器) 嘗試開啟連線時，資訊便會儲存在伺服器上。因為此資訊會佔用記憶體與作業系統資源，所以允許的處理中連線數目有所限制 (通常少於 10 個)。接著，伺服器會傳送回應給用戶端，然後用戶端會傳回接收通知，然後彼此就可以建立連線。此時，系統會釋放已排入佇列的資源，以準備用於接受其他連線。

在攻擊期間，發動攻擊的軟體會產生變造的封包，讓伺服器將它視為有效的新連線。這些封包會進入佇列中，但連線建立程序卻永遠不會完成—連線建立要求會被保留在佇列中，直到逾時。受攻擊的系統會停止回應新連線建立要求，直到攻擊停止。

ICMP 攻擊會使用網路裝置 (例如路由器) 在要求的服務無法使用或無法連線到遠端伺服器時傳送錯誤訊息。ICMP 攻擊的範例包括 Ping 洪水攻擊、Ping-of-Death 攻擊與 Smurf 攻擊。

Ping *洪水攻擊*會快速傳送 ICMP 封包而完全不等候回應，此類攻擊會造成受害者產生大量待傳回的 ICMP 回應回覆封包。

Ping-of-Death 攻擊是以片段形式傳送的超大型 ICMP 封包。當目標伺服器重組這些片段時，組合後的封包大小會超過允許的大小上限，導致伺服器因為記憶體緩衝區溢位而當機。

Smurf *攻擊*涉及以受害者的來源位址變造 ICMP 封包並以廣播方式傳送到電腦網路中。網路上的所有裝置都會回應這些封包，而回應訊息會塞爆受害者的伺服器。

DNS 型態惡意探索會利用 DNS 伺服器軟體的通訊協定剖析與處理實作錯誤 (Bug) 來探索弱點並遂行攻擊。透過傳送格式不正確的 DNS 封包至目標 DNS 伺服器，攻擊者可以導致伺服器停止回應或當機。

DNS 快取毒害涉及將攻擊者指定的網際網路網域位址記錄插入到 DNS 查詢中。若 DNS 伺服器接受該記錄，該網域位址的後續要求將由攻擊者所控制的伺服器位址負責回應。只要該變造的項目存在於快取中，連入網頁要求與電子郵件就會被傳送到攻擊者的位址。新的快取毒害攻擊 (例如「生日悖論」) 同時使用暴力攻擊、DNS 洪水攻擊回應與查詢，企圖取得符合的回應並在快取中「下毒」。

通訊協定異常封包傳送會傳送格式不正確的 DNS 封包 (包含未預期的標頭與承載值) 至目標伺服器，導致伺服器因為伺服器執行緒中發生無窮迴圈而停止回應或當機。這些攻擊有時會以模擬身分的形式遂行。

偵察探測是在發動大型 DDoS 或其他類型攻擊前嘗試取得網路環境資訊的動作。所使用的技術包括連接埠掃描及尋找 DNS 版本與組態資訊。這些攻擊會顯現異常行為模式，若識別出模式便可提供早期預警。

DNS 通道穿越涉及透過 DNS 連接埠 53 來傳送其他通訊協定的資料 (若防火牆是設定為允許通過此連接埠的流量攜帶非 DNS 流量)。有一個用於透過 DNS 伺服器轉送 IPv4 流量的免費 ISC 授權通道處理應用程式被廣泛用於遂行此類型的攻擊。

現有安全防護解決方案的不足之處

某些安全防護解決方案宣稱能保護 DNS，但事實上卻或多或少都有其限制。它們大部分都是屬於「拼湊而成」的外部解決方案，而非從底層建置的解決方案，因此在抵禦 DNS 攻擊的有效性方面明顯不如後者。這些解決方案使用諸如過度佈建、深度封包檢測、泛型 DDoS 安全防護、簡單的速率限制與雲端式解決方案等方式。

方式 1：過度佈建

透過諸如負載平衡器的技術增加網路處理能力以因應 DDoS 攻擊，希冀攻擊能在某個時間點停止。這種方式無法跟上迅速增加的 DDoS 攻擊封包大小與數目，再者，它無法用來監控無效或格式不正確的 DNS 流量。

方式 2：深度封包檢測

新一代的防火牆與 IPS 裝置對於常見弱點與基本的第 3 層 DDoS 攻擊有某種程度的防禦能力。但是，它們沒有能力可偵測或減輕 DNS 特定通訊協定異常封包或 DNS 型態攻擊造成的影響。它們需要超高的運算效能才能精確地偵測 DNS 型態攻擊，因此從成本與所需分布點數目的觀點來看，深度檢測是一種不切實際的方式。

方式 3：泛型 DDoS 安全防護

這些解決方案雖可抵禦許多種 DDoS 攻擊，但對於 DNS 型態攻擊卻沒有有效的處理方式。

方式 4：雲端式解決方案

雲端解決方案只著重在因應大量的攻擊，但對於格式不正確的 DNS 與其他類型的攻擊卻毫無抵抗能力。此類解決方案也有隱私權方面的隱憂[3]、可輕易被繞過[4]，而且會導致延遲問題。

方式 5：簡單的回應速率限制 (RRL)

不具智慧型功能的簡單 RRL 是一種企圖「大小通吃」的方式，設定不適當的閾值會導致合法流量被捨棄。針對不同來源的 DNS 流量必須有不同的處理方式。例如，相較於正常電腦來源，下游 DNS 快取伺服器可會產生 100 倍的流量，而這些流量可能都是合法的。如 HTTP 或電子郵件 Proxy 伺服器會產生較高的 DNS 流量模式。因此，簡單的速率限制將產生太多假警報，這表示員工與客戶在伺服器遭受 DDoS 攻擊期間可能無法存取所需資源。

透過 Infoblox 的全方位安全防護解決方案防堵可能的漏洞

目前只有一個有效的方式可以處理這些 DNS 安全威脅以保護您網路的安全，那就是直接從 DNS 伺服器內部著手。Infoblox 可協助您達成此目標，因為我們對 DNS 通訊協定相當熟悉，而且我們的伺服器就是負責回應 DNS 要求的伺服器。

Infoblox AdvancedDNS Protection 提供獨特的防護方式來抵禦 DNS 型態攻擊。它會以智慧型方式分辨合法流量與攻擊流量，然後自動捨棄惡意 DNS 流量並回應合法流量。此外，AdvancedDNS Protection 會根據安全威脅分析與研究接收自動更新，以協助您抵禦新型攻擊與演化的攻擊。以下說明此解決方案的功能。

強化的 DNS 伺服器—最佳的 DNS 型態攻擊防護解決方案

「Infoblox 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，以抵禦外部或內部攻擊。「進階設備」使用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。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

AdvancedDNS Protection 會持續監控、偵測及捨棄 DNS 型態攻擊 (包括放大攻擊、反射、洪水攻擊、惡意探索、通道穿越、快取毒害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。這能讓您的 DNS 服務即使面臨攻擊仍能正確運作。此外，系統也會接收以安全威脅分析與研究為基礎的自動更新，協助您在新型與演化的 DNS 攻擊出現時即予以偵測並消除。

集中化的攻擊分析報告

AdvancedDNS Protection 透過詳盡的報告為您提供您網路的集中化攻擊分析檢視，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

每一間企業有不同的 DNS 流量模式，而且流量模式在每個季度、每天的不同時間或不同的地理位置可能會不一樣。例如，相較於小型銀行，線上零售網站預期在「網購星期一」與聖誕節購物季會有比平常日高出許多的 DNS 流量。因此，零售網站可接受的速率限制對於銀行而言可能就是不尋常的速率限制。AdvancedDNS 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。

Infoblox Advanced DNS Protection 有效性深入剖析

沒有一種單一方式可抵禦各種用於對 DNS 伺服器進行惡意探索的手段，因此 Infoblox AdvancedDNS Protection 結合了數種特定技術性回應。

- 智慧型速率閾值可以緩和 DNS DDoS 與洪水攻擊，使服務不會無法處理合法使用者的要求。智慧型速率閾值使用 AdvancedDNS Protection 功能來區別不同的查詢類型與關聯的速率。例如，相較於正常電腦來源，下游 DNS 快取伺服器可會產生 100 倍的流量，而這些流量可能都是合法的。如 HTTP 或電子郵件 Proxy 伺服器會產生較高的 DNS 流量需求，而這些流量可能都是合法流量。
  - 以來源為基礎的節流處理會依來源偵測異常查詢，讓暴力攻擊方式失敗。
  - 以目的地為基礎的節流處理會依目標網域分組來偵測流量異常增加的情況。
- 新一代的可程式化處理器提供高效率的流量過濾功能，讓系統可以捨棄惡意流量並回應合法查詢。
- 偵測偵察探測活動並回報可協助識別攻擊，並讓網路團隊能在攻擊發起前即予以識別並封鎖。
- 分析封包以偵測以特定弱點為目標的惡意探索模式讓您可以在某些攻擊流量到達 DNS 軟體之前即予以封鎖。

- 集中化的報告檢視可讓網路團隊識別網路中不同位置發生的攻擊。此功能會提供全局檢視，並提供攻擊範圍與嚴重性資訊，讓您可以採取適當的動作。
- 透過自動更新從 Infoblox 取得最新的安全威脅資料以維持最新的安全防護狀態可確保 AdvancedDNS Protection 能應付各種最新的安全威脅。
- Advanced DNS Protection 是 DNS 伺服器，它不會處理有問題的流量，不像市面上其他安全防護裝置因為並沒有智慧型功能而無法正確地判斷 DNS 流量的合法與否。

由於這些技術，我們的解決方案讓您的 DNS 服務即使在遭受攻擊時仍能正確運作。

是時候該防堵您網路中的DNS安全性漏洞了！

此白皮書的目的是在喚起您對 DNS 弱點的注意，並說明網路的健康情況在相當程度上取決於您採用 DNS 特定解決方案來防堵所有安全漏洞的速度。

從底層開始建置的安全防護解決方案優於拼湊而成的解決方案。從 DNS 伺服器內部防禦 DNS 惡意探索攻擊是最佳位置，因為 DNS 伺服器是此類型攻擊的直接目標。以這些事實考量為基礎而設計的唯一解決方案就是 Infoblox AdvancedDNS Protection。請立即與我們連絡，了解這個解決方案如何協助您抵禦您的網路所面臨的各種危險的安全威脅。

關於 Infoblox

Infoblox (紐約證交所代號：BLOX) 旨在協助客戶控制其網路。Infoblox 解決方案可協助企業將複雜的網路控制功能自動化，以降低成本、提高安全性並將服務運作時間最大化。我們的技術不僅可讓您實現自動探索、即時設定與變更管理，還能協助您確保安全性設定符合網路基礎結構要求。此外，還針對應用程式與端點裝置提供關鍵網路控制功能，例如 DNS、DHCP 與「IP 位址管理」(IPAM)。Infoblox 解決方案協助遍及全球 25 個國家 7,100 家以上的企業與服務提供者控制其網路。

---

1 Prolexic 每季全球 DDoS 攻擊報告 (Prolexic Quarterly Global DDoS Attack Report)，2013 年第 1 季
2 http://openresolverproject.org/
3 http://www.renesys.com/2013/10/google-dns-departs-brazil-ahead-new-law/
4 http://www.crn.com/news/security/240159295/cloud-based-ddos-protection-is-easily-bypassed-says-researcher.htm

Infoblox 代理商 docutek 達友科技

服務專線：02-2658-8970 | http://www.docutek.com.tw

公司總部：
+1.408.986.4000
+1.866.463.6256
(美加地區免付費)
info@infoblox.com
www.infoblox.com

歐洲、中東與非洲總部：
+32.3.259.04.30
info-emea@infoblox.com

亞太地區總部：
+852.3793.3428
sales-apac@infoblox.com

台灣辦公室：
地址：台北市信義路四段6號13樓之6
電話：+886-2-2700-6277 ext 33
電子郵件：sales-tw@infoblox.com