# DDoS 攻擊手法與防護策略重點摘要

國家資通安全會報 技術服務中心彙整

1. DDoS 攻擊

分散式阻斷服務攻擊（Distributed Denial of Service， DDoS）即是利用網路上已被攻陷的電腦作為「殭屍」，向某一特定的目標電腦發動密集式的「拒絕服務」式攻擊，藉以把目標電腦的網路資源與系統資源耗盡，使之無法向真正正常請求的使用者提供服務。常見的攻擊手法可分為針對頻寬與資源兩種類型的消耗攻擊。

- 頻寬消耗型攻擊
  - Internet Control Message Protocol (ICMP) flood (Ping flood、Ping of death)
    透過發送 Ping 指令或 ICMP 廣播等大量的封包進而造成系統或服務的癱瘓。
  - User Datagram Protocol (UDP) flood
    因為 UDP 協定的封包不須經過三向交握，利用此特點進行大量 UDP 封包發送。
  - Teardrop attacks
    每個資料要傳送前，該封包都會經過切割，每個小切割都會記錄位移的資訊，以便重組，但此攻擊模式則利用捏造位移資訊，造成重組時發生問題，造成錯誤。
- 資源消耗型攻擊
  - SYN flood
    利用網路 TCP 三向交握特點持續進行 SYN 請求封包發送，並且不帶 ACK 確認封包，讓伺服器無止盡暫存 SYN 封包，進而達到阻斷服務的目的。
  - Application-level floods
    主要是針對應用軟體層，以大量消耗系統資源為目的，透過向網路應用程式伺服器提出無節制的資源申請，阻斷正常的網路服務。
  - 弱點攻擊型
    針對受害單位提供服務的弱點進行攻擊。此類攻擊的特性是攻擊者使用小量特製的封包或操作就可以癱瘓整個服務，在所利用之弱點尚未被公開前相當難以預防，但是在安裝修補程式後就可以完全免疫。

2. 防護手法

阻斷式服務攻擊的防禦通常涵蓋攻擊偵測、流量分類以及回應工具的組合使用，目的在阻擋非法的流量與允許合法且正常的流量封包。防禦與回應工具如下：

- 防火牆 (Firewall)

  防火牆可以可以設定簡單規則來允許或阻擋特定通訊協定、埠號以及 IP 位址。複雜且混合式的攻擊方式將無法透過簡單的防火牆規則來做防禦，過程中可能阻擋正常合法的封包流量進而影響服務的可用性。

  防火牆常見的有啟用網路層防禦功能，包含 ICMP Flood、UDP Flood、SYN Flood；啟用 DOS 防禦功能，包含 Ping of Death Attack、Teardrop Attack、ICMP Fragment、ICMP Ping ID Zero、Large Size ICMP Packet、Block Fragment Traffic、Land Attack Protection、SYN-ACK-ACK Proxy；啟動通訊協定異常防護，分為 IP Option 異常與 TCP/IP 異常。
- 交換器 (Switch)

  大多數的交換器有一定的速率限制與 ACL 能力。有些交換器提供了 Automatic and/or system-wide rate limiting、Traffic shaping、Delayed binding、Deep packet inspection 和 Bogon filtering (bogus IP filtering)以偵測和修復 DDoS 攻擊。
- 路由器 (Router)

  路由器具備速率限制與 ACL 能力。大多數的路由器很容易於 DDoS 攻擊下不堪負荷。可利用路由器或防火牆上啟動入口過濾 (Ingress filtering)。路由器或防火牆上啟動入口過濾 (Ingress filtering) 防止路由器傳送來源地址跟收到介面不符的封包。但無法阻止在相同網路上的機器發起欺騙攻擊，可防止機器對外部網路發起欺騙攻擊 。
- 應用程式前端硬體 (Application front end hardware)

  應用程式前端硬體為一種智能型硬體設備，它置放於流量達到應用程式伺服器之前，且可與網路上的路由器與交換器結合。藉此來分析所有進入應用程式伺服器之前的封包流量。

  此防禦手法對於特定型態攻擊模式相當有效，如小規模的 SYN flooding，或針對特定系統弱點的攻擊。但對於大流量的攻擊幾無抵抗能力，可依網路或應用服務協定做總量管制。除防禦功能外，另可提供監控警示作用。
- 入侵防禦系統 (IPS based prevention)

  入侵防禦系統 (Intrusion-prevention systems，IPS) 對於特徵明顯攻擊是可以有效防禦的。但是攻擊趨勢已轉向為以合法流量掩飾非法行為的攻擊方式，對於此類的攻擊 IPS 的防禦顯得不足。
- 阻斷服務防禦系統 (DDS based defense)

  阻斷服務防禦系統 (DoS Defense System，DDS)相較於入侵防禦系統更專注問題於 DDoS 攻擊之上，具備阻擋以連線方式形成的 DDoS 攻擊。DDS 也能夠辨識來自通訊協定式 (例如 Teardrop 與 Ping of death) 與頻率式 (Rate-based) 的攻擊。
- 黑洞與水坑 (Blackholing and sinkholing)

透過 Blackholing 將所有送往被攻擊的 DNS 或 IP 流量導進到黑洞之中(通常是 Null 接口或者是不存在的伺服器)；而 Sinkholing 則是將流量導進有效 IP 位址來進行分析。相較之下，Blackholing 可能會降低服務可用性；而 Sinkholing 面對滿頻的攻擊則效率降低。

以 ISP (Internet Service Provider) 業者來說可於國際端 Border Router 使用 Blackhole 阻檔受害網站所有國際流量；於 ISP 骨幹 Router 使用 Blackhole 阻檔非 ISP 網段所有流量，但此種方式阻擋流量方式不區分合法與非法流量，全數流量皆被丟棄，故將影響網站可用度。

- 清洗管線 (Clean pipes)

將所有的流量導進「清洗中心 (cleaning center)」或「洗滌中心 (scrubbing center)」，並透過透 Proxies、Tunnels 等方式將非法與正常合法流量區分出來。

像是 ISP 業者提供清洗中心，過濾非法流量後，將合法正常流量導回用戶網站。而且 ISP 業者具有骨幹級頻寬與大型資安防護設備配合 Sinkholing，將可有效應付滿頻攻擊。

3. 結論

DDoS 攻擊種類眾多，其防禦方法不可寄望於單一方案，必須先行研判其種類選擇合適方式才能有效處理。關於其他防禦的考量重點尚有：

- 多層次過濾防護
- 提昇 DNS 服務安全
- 落實業務永續規劃及災難復原演練(異地/服務備援、Hot/Warm Sites 規劃設計)
- 多重網路出口(雙資料中心、第二 ISP、雲端備援)
- 上游 ISP 業者建立緊急連繫管道
- 確實執行弱點補強作業及系統效能調校
- 安全監控及緊急應變程序。

DDoS 防護以恢復受害者之正常服務為目標，如何於防禦與提供正常服務之間取得平衡，判斷被攻擊之原則也需經嚴謹審慎評估。

資料來源：資安技術交流會議宏碁、中華電信、趨勢科技、關貿網路及數聯資安提供資料彙整而成