AhnLab DPS

Alliance 一通科技股份有限公司 ALLIANCE TECHNOLOGY CO., LTD.

DDoS Protection System (DPS)

符合企業需求提供大規模、混合及進階的DDoS攻擊防禦

大容量　精準　自主學習　即時處理

分散式阻斷服務攻擊（DDoS）透過傳送大量封包或連線需求使得網路或伺服器無法運作而中斷服務，使客戶不知所措而導致企業鉅額的損失。最初，DDoS攻擊目標主要為網路，但就像其他攻擊行為一樣，在駭客主義的運作下，DDoS攻擊的質量也日益成長。

舉例來說，原本以小型封包使網站或資料庫伺服器無法運作的攻擊模式，在混合式攻擊中，攻擊網站或資料庫伺服器的小型封包會被隱藏於攻擊網路的大型封包裡。這類進化後的攻擊形式，使得企業必須尋求更進一步有效率的解決方案，不僅僅是偵測DDoS的封包，還必須提供詳細的分析。

AhnLab DPS正是為此類型DDoS攻擊模式提供專業分析及檢測惡意程式所設計的產品。在安全層級上偵測混合式DDoS攻擊並同時有效地處理急速上升流量的安全層面，確保企業不中斷營運。

DDoS攻擊手法

- 利用殭屍電腦
- 智慧型攻擊技術
- 組織型態攻擊

企業營運中斷危機

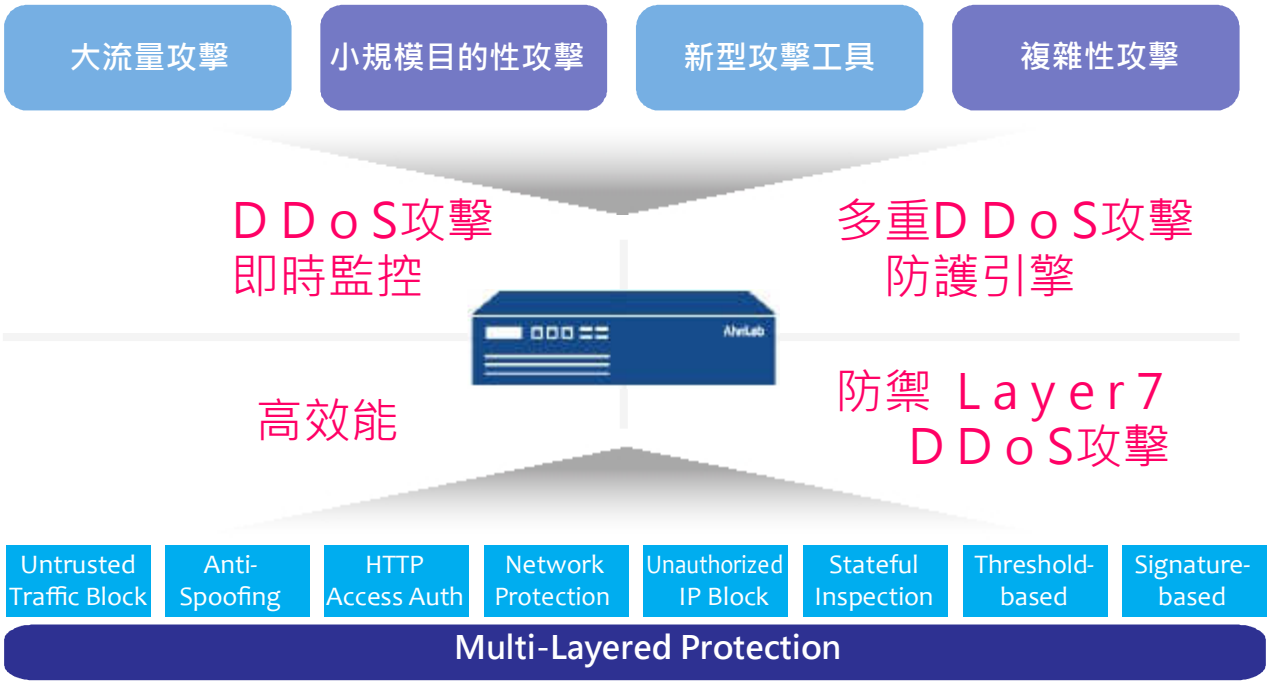
- 線上購物、電子商務、線上遊戲、入口網站 → 營運中斷 減少銷售?!
- 銀行、證券、保險業 → 無法使用匯款、查詢、繳款、交易等服務 導致客戶信心下降?!
- 企業與公共機關網站與網路 → 系統超載、通訊故障 業務中斷?!

AhnLab 能為您做什麼？

- 企業營運不中斷：降低損失風險及避免企業評價受損。
- 減少後續處理負擔：DPS可立即回應偵測到新型攻擊模式或方法。
- 降低人力資源成本：具備多層（multi-layered）過濾與自主學習能力。
- 持續性監控服務：可自行動裝置存取顯示網路流量與篩選狀況，包含系統資源使用率及網路埠的連接。

Why DPS ?

傳統DDoS攻擊解決方案無法真正防禦混合式DDoS攻擊，這類的解決方案經常觸發誤報會導致不必要的網路中斷並浪費企業資源。由於DPS精準的偵測惡意TCP和HTTP requests，相對來說能夠大幅降低誤報產生的服務中斷。此外，DPS能防護系統受到目標式、小型HTTP攻擊，而這類攻擊常在傳統DDoS攻擊解決方案中無法偵測出來。



AhnLab DPS：完整解決方案

近來DDoS攻擊使用各類型流量，但DPS能夠全方位阻擋今日複雜的攻擊行為。

- 即時流量監控與自主學習
- 從網路到應用程式（HTTP）防護
- 基於來源IP的防護及防止偽裝IP
  -TCP Flooding : SYN, SYN-ACK, ACK, Fin, PSH, RST, URG, XMAS
  -Other : UDP, ICMP, IP, Fragments, DNS Query
- TCP連線防護：TCP Multi-Connection, TCP Established Attack, Low Bandwidth TCP Session Flooding
- HTTP防護：HTTP Get Flooding, HTTP Null Page Flooding, HTTP CC Attack, HTTP Redirect Bypass Flooding, SQL Query Based HTTP Attack
- 可防護如同RUDY或Slowloris的新型進階攻擊

AhnLab DPS 產品規格

機型	DPS 6000	DPS 10000
效能	6 Gbps Max 10 Gbps	10 Gbps Max 20 Gbps
CPU	Exclusive multi-core	Exclusive multi-core
記憶體	8 GB	16 GB
Flash	2 GB(含)以上	2 GB(含)以上
OS	AhnLab 專屬作業系統	AhnLab 專屬作業系統
介面： 1G Copper 1G Fiber (SFP)	2 EA (管理) 4 EA (Max 6 EA) Max 6 EA	2 EA (管理) 2 EA (管理) 4 EA (Max 8 EA)
電源	Redundant dual sources	Redundant dual sources
認證	CC EAL4	CC EAL4

Pato Huang
TEL:02-7708-2013#318
Cell:+886-918-672-361
E-MAIL: pato@atc.com.tw