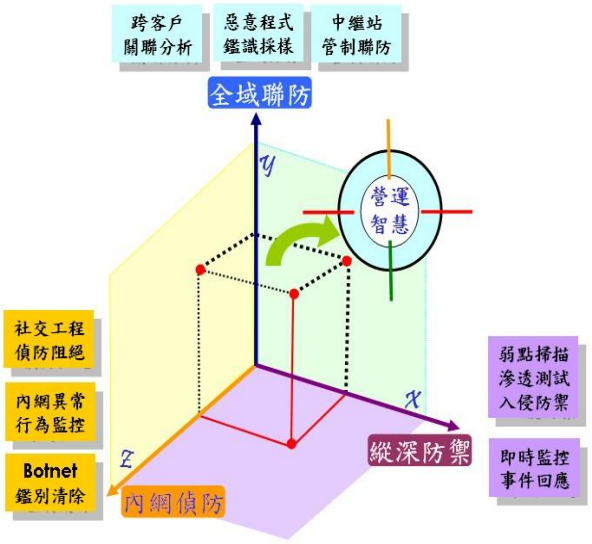
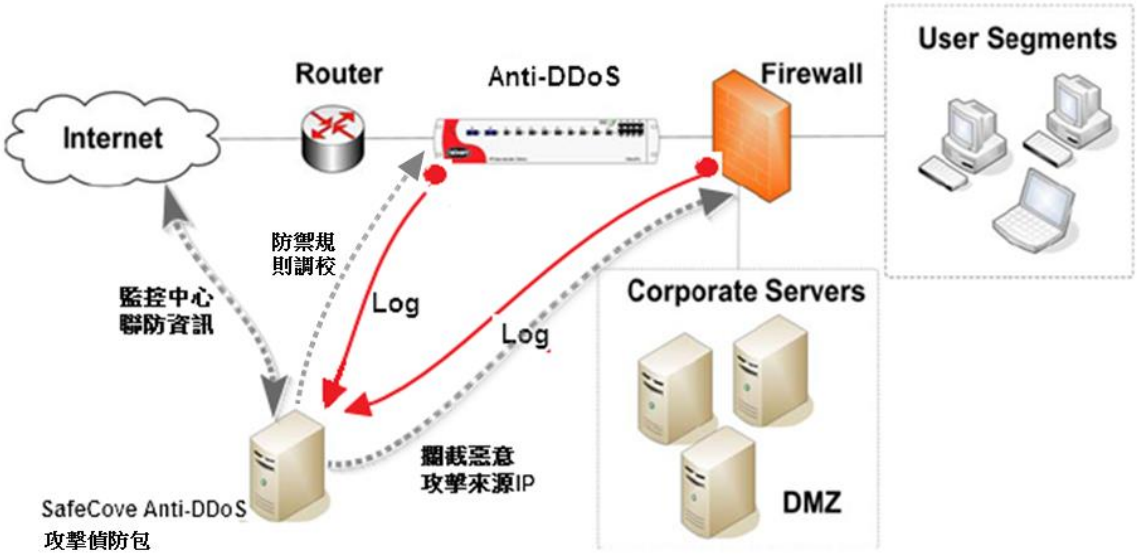
SafeCove DoS/DDoS 攻擊偵防包

產品簡介

近年來 DoS/DDoS 攻擊方式手法已經不僅限於以發動大量的網路攻擊流量來進行摧毀式的攻擊，取而代之的是更容易複製與實現的低頻率、慢速的攻擊手法來進行滲透與攻擊，再加上其多變的入侵行為與手法，即使是宣稱能防範 DoS/DDoS 攻擊的資安設備，也很容易因防禦規則過嚴或過鬆而導致常有誤判情勢，甚至影響軟件系統的正常運作。這些現象顯現 DoS/DDoS 攻擊手法的難以防範與破壞能力。事實證明，現有防火牆與入侵防禦設備皆難以防護這類型的攻擊。



SafeCove DoS/DDoS 攻擊偵防包，可以針對 Microsoft IIS 網站伺服器、Anti-DDoS 防護設備之日誌記錄與事件進行關聯規則分析，以系統化的方式進行相關存取日誌與事件收集、關連分析後，對快攻、慢打等多種攻擊行為進行事件電子郵件通報預警，可提升對於 DoS/DDoS 防禦、HTTP Flood 防禦、伺服器防護的有效性，提供給政府



機關作為因應網路安全與資訊安全的管理依據。

產品功能說明

項目	內容說明
產品功能	
DoS/DDoS 攻擊偵防功能	1.可對以下 DoS/DDoS 攻擊進行自動告警 1).TCP SYN floods 2).TCP SYN+ACK floods 3).TCP FIN floods 4).TCP RESET floods 5).TCP Fragment floods 6).UDP floods 7).ICMP floods 8).IGMP floods 9).Packet Anomalies 10).HTTP Flood 11).Zero-minute Malware spread 12).Application resource misuse A.Brute force attacks B.Web application scanning C.HTTP page floods D.SIP Scans E.SIP Floods 13).HTTP DoS page floods 14).HTTP bandwidth consumption attacks 15).頻寬流量異常等
跨設備聯防	1. 針對異常連線或攻擊來源之攻擊行為自動彙整分析 2. 針對異常連線或攻擊來源 IP，驅動防火牆進行聯防 3. 針對異常連線或攻擊來源 IP，驅動入侵防禦設備進行 4. 單一連線每秒最小傳輸量低於定義基準傳輸量(*註) 5. 大量連結固定網頁頁面(*註) 6. 時間(time-taken)超過定義基準秒數及事件筆數超過定義基準筆數(*註) 7. 同一用戶端(來源端)IP 觸發前項規則(*註)

項目	內容說明
	8. 使用 POST 方法傳送資料至根目錄發生 HTTP status code 500(* 註) 註：此項目需搭配選購監控 IIS 網頁伺服器、防火牆、入侵防禦設備或 WAF。
產品技術支援	
產品諮詢	1.5x8 線上（電話／電子郵件）客服 2.客服電話：0800-286-009

產品授權

產品名稱	授權數量
SafeCove DoS/DDoS 攻擊偵防包	一個設備授權(IIS 主機、防火牆或 Anti-DDoS 設備)（一年授權）

產品售價

- SafeCove DoS/DDoS 攻擊偵防包一套（1 個設備授權）NT$95 萬(未稅)

交付項目

- SafeCove DoS/DDoS 攻擊偵防包使用授權書

系統需求

- CPU ： Intel 4 核心 2.0 GHz 以上
- 記 憶 體： 4 GB 以上
- 硬碟空間： 500 GB 以上
- 作業系統： Microsoft Windows 2003 Server 標準版 或 Linux 以上

預期效益

- 獲得即時資安事件自動通報，強化資安防護能力
- 提升 DoS/DDoS 攻擊監控自動預警機制

聯絡窗口：	
公司：安碁資訊股份有限公司	地址：台北市忠孝東路四段 563 號 8 樓
聯絡人：張文棟	電話：(02)8979-6186 轉 6712
傳真：(02)2784-1092	手機：0956-260-588