Networks
Secure Networks at Layer-7

雲世代網站應用防火牆

InstantWAF

隨插即用免停機
清洗+過濾+稽核

阻擋OWASP十大攻擊已不足
結合國際威脅情資，定位威脅來源

■ 雲世代的隱憂: 阻擋OWASP十大攻擊已不足

美國聯邦眾議院議長裴洛西率領美國眾議院國會訪問團來台訪問時，引發對岸高度不滿，不只進行軍演，網路攻擊更是持續長達9天。這些攻擊手法大致可區分為: 分散式阻斷服務(DDoS)攻擊、內容置換(Deface)，以及幾可亂真的假訊息等。

■ 雲世代WAF: 結合國際情資單位聯合防禦

網頁遭置換或竄改(Web Defacement)的攻擊手法，主要是系統遭駭客入侵後，取得系統管理者權限，以進行更換網頁的手法，通常網站會遭受駭客上傳惡意程式(Web Shell)。漏洞通常是網站頁面提供了上傳功能，例如大頭貼、檔案等等，駭客透過僵屍網路，利用經過偽裝附檔名的惡意程式，騙取系統的認證，待順利將僵惡意程式上傳至系統內部時，即遠端將惡意程式呼叫出來，進而取得系統管理員權限的帳號，以達控制系統的目的。當今OWASP的前十大攻擊類型之外，仍有許多漏洞可被殭屍網路滲透。

Malware Patrol 勒索情報網

TALOS 威脅情報網

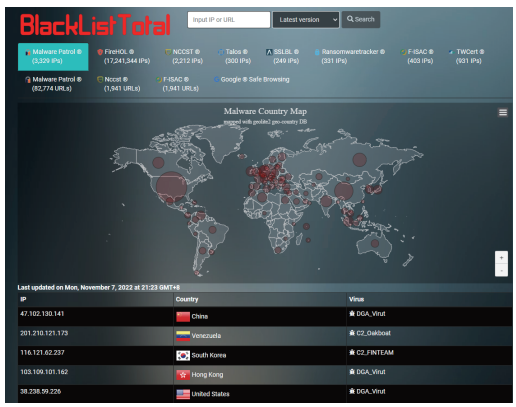
國內各大情資網 (政府/金融/ 園區/企業)

FireHOL 惡意IP情報網

ABUSE.ch 威脅情報網

■ 內建BlacklistTotal整合MalwarePatrol / FireHOL / 等國內外情資

WAF內建國際情資，有如台海作為第一島鏈，能收到各國的最新情報，把附近的飛行器快速判斷出是敵方還是我方的客機、戰鬥機、飛彈、無人機，才可以快速清洗流量，避免WAF花太多力氣進行無謂的判斷，提升整體的性能。本地政府的情資能針對常對本地活動的惡意IP阻斷，國外情資單位能把常被做為跳板的IP擋住，甚至病毒的名稱。

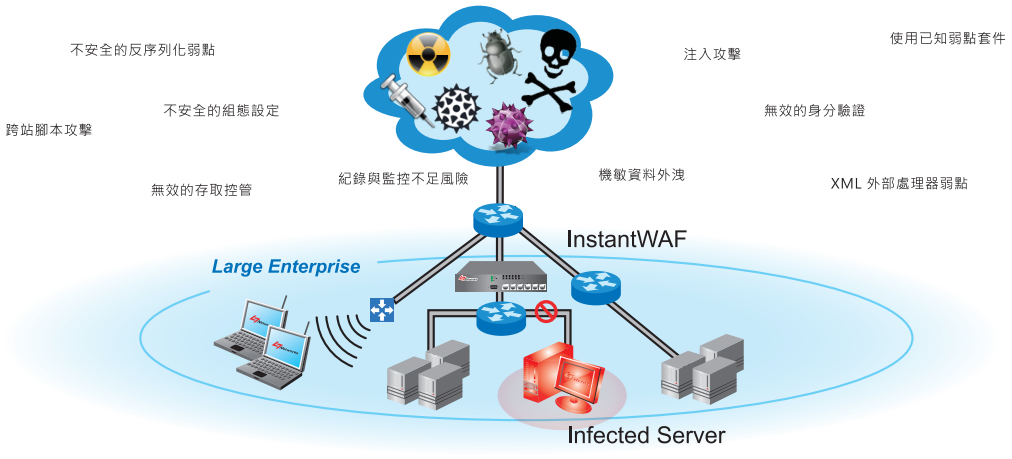


■ 高抗擊力Anti-DDoS清洗流量

新一代Syn代理能準確清洗無效的TCP連線，避免伺服器被耗盡資源；每一個服務可設定單一外網IP最大連線數、最大每秒新建連線數；對各服務可提供頻寬切割、保證、限制，確保服務能有效提供且不會互相影響。

■ 具備自動阻斷境外勢力入境能力

情況緊急時可觸發安全等級升級，將境外IP來訪連線依照國家地區IP阻斷，讓境內來訪IP能正常存取，快速恢復服務。



InstantWAF

雲世代網站應用防火牆

設備型號	50型	100型	500型	1000型	3000型	5000型	8000型	10000型
尺寸	19' 1U	19' 1U	19' 1U	19' 1U或2U	19' 1U或2U	19' 2U或3U	19' 2U或3U	19' 2U或3U
記憶體	8GB	8GB	8GB	16GB	16GB	16GB	32GB	32GB
流量介面(UTP)	GEx4	GEx4	GEx4	GEx6	GEx6	GEx6	GEx6	GEx6
SFP介面	-	-	-	SFPx2	SFPx2	SFPx2	max:16	max:16
可擴充10G介面	-	-	-	max:2	max:2	max:2	max:4	max:4
管理介面	GEx1	GEx1	GEx1	GEx1	GEx1	GEx1	GEx1	GEx1
硬體旁路(內建)	GEx4	GEx4	GEx4	GEx4	GEx4	GEx4	GEx6	GEx6
硬體加速(擴充)	-	-	-	-	-	Xilinx U25	Xilinx U25	Xilinx U25
電源(100-240v,50/60Hz)	單電源	單電源	單電源	單或雙電源	單或雙電源	單或雙電源	熱插拔雙電源	熱插拔雙電源
其他	符合安規認證(BSMI / CCC / CE / FCC / ROHS)，具備RJ-45或RS-232主控台console介面							
設備性能								
同時訪客IP(超出則不控管)	70	250	500	1000	3000	5000	8000	20000
每秒新建連線數	1000/秒	1850/秒	3000/秒	5150/秒	10K/秒	50K/秒	100K/秒	200K/秒
同時併發連線數	20K	200K	300K	1M	2M	4M	8M	12M
設備雙向效能(in+out)	80M	200M	300M	600M	1.2G	2Gbps	6Gbps	12Gbps
授權WAN頻寬(in+out)	20/40/80M	100/200M	200/300M	400/600M	600M/1.2G	1.2G/2G	2G/3G/4G	4G/8G/12G

基本規格	
安裝模式	支援以透明橋接(Inline)模式、代理(proxy)模式安裝，IPv4或v6皆可保留原始Client IP地址，或加上XFF表頭讓網站伺服器解析原本IP
匯入網站憑證	針對要解密https並進行WAF保護的網站，可匯入該網站的憑證

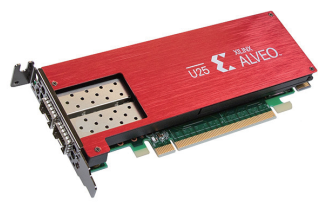
OWASP前10名攻擊防禦	
1. 注入攻擊	嚴密檢查輸入值，過濾非法字元，阻止竊取者讀取資料庫，造成洩漏機敏資料或進而發生作業系統漏洞，執行系統指令，甚至讓主機被接管
2. 無效的身分驗證	強制登入加密，避免Session 無控管 Cookie 為保護，杜絕帳號 / 身分盜用或身分認證機制無效化
3. 機敏資料外洩	防止駭客取得金融資訊、個人資料，以進行偽造 / 竊取身分，或進行其他的犯罪行為
4. XML 外部處理器弱點	阻止攻擊者以外部讀取的XML為基礎，讓系統讀取後，進行文件的共享、監聽內部網路、執行遠端程式，進而導致資料外洩或系統被駭客接管
5. 無效的存取控管	阻止攻擊者透過網址或 HTML 頁面繞過存取控制，將自己的權限提升自管理者，進而攻破公司系統
6. 不安全的組態設定	確保只開啟相關的帳號、頁面、服務、port並杜絕預設密碼，確保各項服務升級到最新版
7. 跨站腳本攻擊	阻止將來自使用者的執行請求送回瀏覽器執行，避免駭客擷取使用者的 Cookie假冒身分為合法用戶，或將用戶轉到惡意網站或執行惡意腳本
8. 不安全的反序列化弱點	阻止駭客將竄改後的惡意物件進行反序列化，導致應用程式或 API 出現不安全的風險
9. 使用已知弱點套件	阻止駭客利用系統外部元件或函式庫尚未更新至最新版，且該元件或函式庫已具有弱點，進行弱點攻擊
10.紀錄與監控不足風險	強制紀錄足夠的訊息，遇到可疑活動時可照SOP查看紀錄以立即解決，不讓駭客進一步攻擊系統、非法竄改、存取或銷毀系統的資料
攻擊事件報表	紀錄各類攻擊事件，並分析排行外網攻擊IP與內網被攻擊server IP
整合全球威脅情報	
自動更新同步惡意情資	能每天自動更新BlacklistTotal所整合的中繼站黑名單，阻擋網軍的殭屍網路回報到駭客中繼站下載惡意程式，有效阻絕勒索軟體等駭客行為
支援台灣情資同步	可自動更新來自國家政府組織定期推出的惡意情資名單，包括URL與IP網段列表
支援金融情資同步	可自動更新來自國家金融單位定期推出的惡意情資名單，包括URL與IP網段列表
支援Malware Patrol同步	可自動更新來自【Malware Patrol】的威脅情資，專注於勒索病毒的惡意IP，包括DGA (網域產生演算法)於定點定時爆發即消失的惡意網域
支援FireHOL同步	可自動更新來自【FireHOL】的駭客地圖，包括C&C控制站、惡意中繼站、勒索病毒、RBL
支援ABUSE.CH/Talos同步	可自動更新來自【ABUSE.CH】與Cisco【Talos】公布的惡意情資，包括不受信任的SSL憑證的IP網段列表、駭客活動區域
防阻斷式攻擊(Anti-DDoS)	
支援Syn Proxy防Flooding	針對TCP連線進行3-way handshake代理，確定是真的連線才允許連往內部server，有效清洗駭客偽造IP狂發Syn耗盡server連線空間上限
外網訪客單IP限制	可設定連到同一個內部網站的外網來訪IP，每個IP的連線數上限、每秒新建連線數上限、頻寬上限，避免單一IP耗盡某內部網站資源
頻寬租借/保證/預留	支援依時間排程自動切換不同之頻寬通道方案，例如下載行為在不同時間段有不同的頻寬設定，彈性分配頻寬
智慧型自動阻斷境外勢力	情況緊急時(可自訂條件)可觸發提升安全等級，將境外IP來訪連線依照國家地區IP阻斷，讓境內來訪IP能正常存取，快速恢復服務
攻擊事件報表	可觀察攻擊次數的長期趨勢，與外網攻擊IP的排行分布、內網被攻擊server的排行分布
防止機敏資料外洩(外掛選購)	
偵測格式	支援掃瞄pdf/doc(x)/xls(x)/ppt(x)/txt/eml等格式以多次zip/tgz/7z/rar/tar/gz壓縮，即使更改檔名也無法規避過濾
內建個資法欄位	內建台灣個資法定義的欄位(姓名/電話/身分證號/銀行帳號/護照號碼/電子郵件/學歷/住址/...)，對外洩檔案進行統計各欄位出現的次數
外洩筆數設定	能設定政策，以特定數個欄位偵測到的次數，經過【且】/【或】等邏輯運算結果，決定是否阻擋，有效降低誤判事件
惡意程式辨識與阻擋	
防止殭屍伺服器外連	可辨識偽裝連線，例如走port 443的SSH，避免被攻占的殭屍伺服器偽裝成正常連線與駭客溝通
阻止惡意程式橫向感染	支援常見的惡意程式辨識，避免中毒受害的伺服器成為跳板，橫向感染其他主機

管理與設定	
中央集中控管	支援中文報表、中央集中管理設備與集中報表，分admin/manager/audit分權控制各設備、功能讀寫權限，並詳細紀錄存取設備紀錄
違規/用量排名報表	支援樹狀圖動態展示各式日/週/月/季/年報表，能照搜尋條件的順序動態顯示排行，記錄能匯出並支援關鍵字全文檢索
報表資料管理	可針對行為/IP地址/用戶名/分類/URL/QoS通道等連線細節欄位分析，並即時或定期依照自訂條件產生記錄檔
郵件通知/警告	可自訂日/週/月/季/年報表 (pdf/html/xls格式)，或訂立個資 (姓名/信用卡號/身份證號/護照號/電話等) 外洩條件，即時警告
資料備份與還原	報表資料能透過網路備份至異地磁碟，亦可透過網路讀取舊有備份報表資料，無需將資料倒回系統，能直接調閱查詢之前備份出去的資料
異常頻寬或行為告警	可建立異常頻寬通報閾值，超過閾值後能自動通報並啟動特定政策

關於L7 Networks Inc.
L7 Networks成立於2002年，
由資深研發團隊組成，
已成功推出多款整合式防火牆，
代工銷售於多家上市公司，
產品遍及全球。

自2005年後，
以全球領先的第七層網路技術:
1. 應用辨識與頻寬控管
2. 雲端內容過濾與記錄
3. SSL資料外洩防禦

提供頂尖的網管解決方案



L7 is officially supported and
powered by Xilinx U25 FPGA

L7 Networks Inc.
11494台北市內湖區新湖二路219號4樓
30043新竹市民族路25號10樓
Tel: +886-2-27936053
+886-3-5225946
Fax: +886-3-5240632
http://www.L7-Networks.com