L7 Networks
Secure Networks at Layer-7

雲世代入侵防禦系統

InstantDefend

管理、備份、側錄、過濾

結合威脅情報中心抵擋網站威脅!

內部/外部威脅，都愛藏在https加密通道中!

Malware Patrol 勒索情報網

TALOS CISCO 威脅情報網

NCCST 國家資通安全會報技術服務中心

FireHOL 惡意IP情報網

ABUSE.ch 威脅情報網

■ 雲世代的隱憂：防禦外敵 or 內外兼顧?

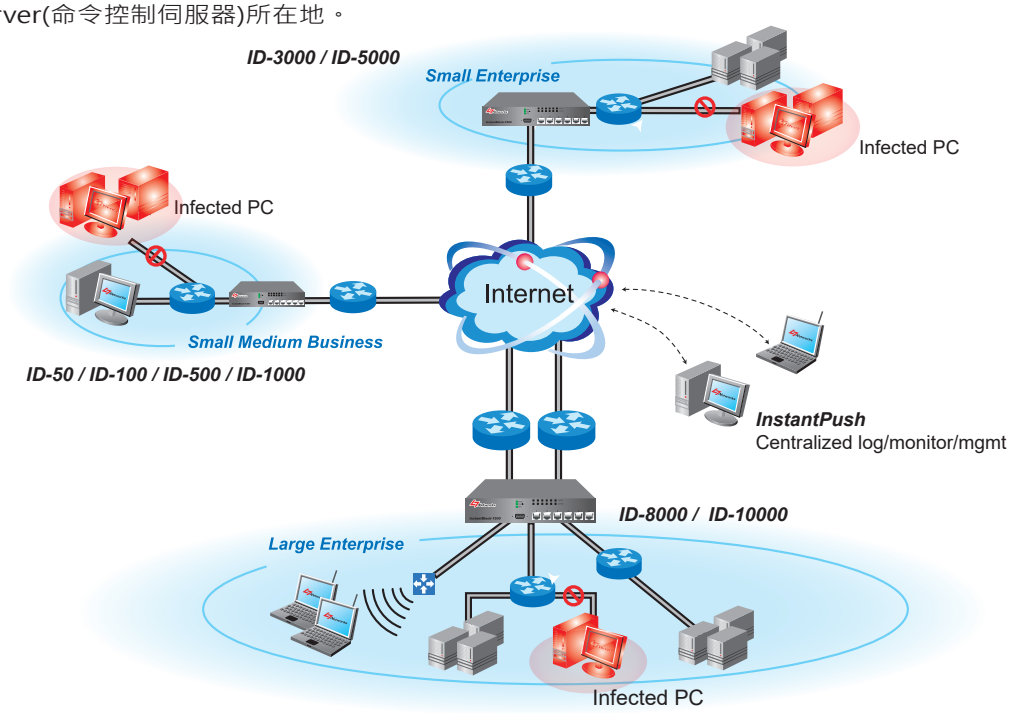
傳統 IDS/IPS無法結合國際威脅情資來確保特徵碼的廣度，InstantDefend 是一套可以彈性佈署在各種位置的IPS，具備inline/sniffer模式可以分析惡意的入侵流程，並判斷是否存在可疑的攻擊行為，協助機關阻擋針對網站應用程式的各種攻擊，必結合國際八大威脅情報中心，提供更安全的防護機制。

■ 雲世代IPS: 過濾/記錄/辨識內網https加密行為

以雲端惡意程式分析技術，收集全球各式惡意程式，建立完整特徵資料庫。經由惡意網址過濾及入侵防禦、防毒，保護使用者；並可攔阻Botnet對外連線，避免DDoS攻擊及資料外洩。不僅防禦入侵(Intrusion)，更具備外洩偵測(Extrusion)，一次達成雙重保護。加強變形攻擊的偵測能力與防禦能力，透過正向行為檢視與負向行為剖析的自我學習安全模式，建立先進之變形攻擊過濾分析機制。可以針對 HTTPS 加密資訊解密並偵測惡意攻擊。提供智慧型的阻絕能力，降低誤判率並減少檢視網路封包造成的延遲封包重新切割傳送。

■ 內建MalwarePatrol/Talos/FireHOL/Abuse惡意網站庫 & 國家資通安全會報

URL過濾與AV模組，整合了後端雲端全球情報網聯合防禦服務，與國家資通安全會報(俗稱技服)中繼站黑名單，以零時差處理不斷變化的網站內容。尤其對當代以的社交工程為主的APT攻擊，例如透過假冒Facebook / Email好友而散佈的危險超連結，或感染Malware / Spyware而成僵屍網路(Botnet)，能達到立即阻斷的效果，抓出病原，甚至追溯到幕後C&C Server(命令控制伺服器)所在地。



L7 Networks
Secure Networks at Layer-7

InstantDefend

雲世代
入侵防禦系統

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

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' 1U或2U	19' 1U或2U	19' 1U或2U
記憶體	2GB	2GB	4GB	4GB	4GB	8GB	8GB	8GB
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
光纖旁路(擴充)	-	-	-	Silicom	Silicom	Silicom	Silicom	Silicom
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(CCC/CE/FCC/ROHS)，具備RJ-45主控台console介面							
設備性能								
同時上線IP(超出則不控管)	70	250	500	1000	3000	5000	8000	20000
政策上限	512	512	1024	1024	2048	4192	10K	20K
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

攻擊防禦	
入侵偵測防禦	包括針對用戶端/服務器端系統弱點保護 、蠕蟲擴散防禦、後門程式/木馬程式防禦、緩衝溢位攻擊防禦、Shellcode以及惡意軟體偵測防禦，另外也對所有攻擊流量進行威脅分析(威脅程度按照5級分類)，並可即時查看。
異常行為偵測與防護	針對異常行為進行狀態檢查、通訊協定異常偵測、IP位址/通訊埠掃瞄偵測 、異常行為分析、DoS/DDoS攻擊防禦 、流量異常偵測，完善的偵測防護作業，有效保護用戶安全。
偵測入侵閃避攻擊	有效偵測近10種入侵及惡意攻擊，包括重複傳送(Retransmission) 、內容重疊偽裝(Overlapping)、Whisker (URL%編碼/目錄遊走)、Back Orifice 、URL混淆攻擊(URL obfuscation) 、破碎封包(Packet Fragmentation)、串流片段(Stream Segmentation)、FTP Bounce /內含Telnet OP Code之FTP指令(FTP evasion)及IP/TCP/SUNRPC/SMB/MSRPC碎片(Fragments)等等。
偵測入侵反應模式	入侵行為發生時所採取的反應模式包括: 中斷連線(TCP Reset) 、記錄攻擊事件(Log)、即時畫面顯示(Monitor) 、電子郵件警告(E-mail Alert)、丟棄封包 (Drop)
使用者自訂攻擊特徵碼	領先業界提供全GUI介面供自訂攻擊特徵碼，且能夠指定Layer 7之比對內容，另外可針對特徵碼觸發次數、來源IP觸發特徵碼次數、目的IP觸發特徵碼次數、 IP Pair觸發特徵碼次數，來制訂觸發條件。 可制訂第3層至第7層之詳細內容，包括IP/TCP/UDP/ICMP/IGMP等Header欄位，並提供比對位移、比對長度機制，可跨封包比對特徵碼內容。
殭屍木馬偵測防禦	支援Botnet C&C伺服器檢測防禦/Botnet IP位址黑名單檢測防禦/Botnet域名黑名單檢測防禦 且能夠偵測並切斷惡意APT連線，提供業界最完整的大中華地區惡意連線資料庫，在地化網路威脅防禦最佳。
安裝監控	
安裝模式	支援以透明橋接(Inline)模式安裝，或以旁聽(Sniff)模式安裝，監聽交換器端口鏡像(port mirror)流量，並可以tcpdump擷取複製封包
身分辨識(User-ID)	透過網頁登入AD / LDAP / RADIUS / POP3(S) / IMAP(S)方式，或自動AD認證或agent達成單次登入(Single Sign On)
即時流量監控	能以3~60秒為更新週期，即時以樹狀圖逐層列出其下各子網或各應用的總流量與連線細節(方向/傳輸量/封包數/頻寬/通道)，並可按欄位排序
第七層應用(20類3000種以上)	
即時通訊(Chat)類	Line/QQ/AliWangWang/Fetion/Dushow/Popo/SinaUC/Skype/Yahoo/AOL/ICQ/Jabber/LavaLava/Gadu/GoogleHangout...
點對點下載(P2P)類	Xunlei/Thunder/WebThunder/FlashGet/BT/eDonkey/eD2K/eMule/Overnet/EzPeer/Kuro/ClubBox/Poco/Fs2You/KaZaA/Vagga /GoBoogy /Ares /iMesh/Gnutella/WinMX/Bearshare/Shareaza/Morpheus/Gnucleus/Kugoo/Pigo/dc++/100bao
網路電話(VoIP)類	Skype/Polycom/RTP/RTCP/SkypeOut/Eyeballchat/SIP/TelTel/H.323/MsnVoice/NetMeeting/...
地道軟體(Tunnel)類	Hopster/YourFreedom/Garden/Gpass/Tor/HttpTunnel/JAP/RealTunnel/Vnn/SoftEther/FreeGate/Wujie/...
串流媒體(Streaming)類	QQTV /UUsee /PPfilm /PPlive /PPstream /RealPlayer /QuickTime /KKBox /Shoutcast /Winamp /Live365 /Radio365/PPTV/TVants/FastTV /SSTV /MeteorNetTV /3TV /PhoenixTV /YahooMusic /MMS /SeeTV /QQlive /QQmusic /JetAudio /Jetcast
企業應用(Enterprise)類	Citrix /MySQL /Notes /Oracle /MSSQL /RDP /VNC /UltraVNC /Win /PcAnywhere /Telnet /SSH /TeamViewer /Logmein
網路硬碟(File Transfer)類	SkypeFile / LineFile / SMB / FTP / OneDrive / GoogleDriveUp / Dropbox / AsusWebStorage / Aspera / ...
炒股軟體(Stock)類	HuaTai/Tazihuei/TungHuaShuen/TienI/FenShiChia/StockStar/ZaoZang/AnShin/SkyNet
線上遊戲(Game)類	Diablo3/LoL/CounterStrike/DaHuaShiYo/Dance/WarCraft/MoYu/CadinCar/MiracleWorld/Fight/WenDao/Lineage/...
http(s)上網安全管理	
支援各種http(s)流量	除了一般標準埠號80/443外，能針對自動辨識出的非標準80/443的http(s)或Proxy流量進行過濾，包括http(s) get/post/connect指令
內建URL資料庫	內建70種以上網站類別，包括色情/廣告/賭博/暴力/股市/新聞/遊戲/動漫/聊天室/笑話/駭客/釣魚/間諜/...，並可自訂URL關鍵字類別
雲端URL資料庫	支援雲端URL資料庫，有效阻斷快速變動的色情/惡意網址，針對內建網址庫不足的部分能即時送回雲端掃瞄網頁內容判斷出網頁類別
條列式政策管理	可對內建的URL資料庫類別或自定的URL關鍵字類別，搭配內網地址/網段/AD-User/Group、VLAN-ID、第七層應用(App-ID)執行QoS政策
自訂違規警告畫面	可以html自訂阻擋畫面，內容包括用戶名、來源IP、阻擋理由(網址分類)，亦可設定特權瀏覽，讓特權人員可按下繼續按鈕後能繼續違規網頁
依網站行為阻擋	可阻擋Java/ActiveX/Cookies等網頁物件、過濾http/https檔案上傳行為，並可依據自訂關鍵字過濾POST內容
頻寬管理	
雙向頻寬獨立切割	針對進出流量可設定頻寬總量，並自定各方向的子通道，樹狀子通道內能以IP、網段、連線作為單位公平分配通道內頻寬，避免佔用
自動排程切換	支援依時間排程自動切換不同之頻寬通道方案，例如P2P在不同時間段有不同的頻寬設定，彈性分配頻寬
頻寬租借/保證/預留	支援動態頻寬租借（最大頻寬）、頻寬通道（保證頻寬）、通道內連線/IP數控制（頻寬預留），具備PostACK專利技術精確控制TCP頻寬
流量限速/配額/限連線數	支援以IP或以用戶名為基礎的應用限流措施，提供公佈欄供用戶查詢，以了解目前已傳輸多少量、是否已被鎖定等狀態
兩段式懲罰設計	支援以網頁警告用戶即將用光配額、尚餘配額，實際用完配額時亦能以網頁警告，告知進入第二階段限流（受限的流速/連線數）
威脅管理	
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NCCST同步	可自動更新來自【NCCST國家資通安全會報技服中心】的惡意中繼站名單，包括URL與IP網段列表
支援F-ISAC同步	可自動更新來自【F-ISAC金融資安資訊分享與分析中心】的惡意中繼站名單，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
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

L7 Networks
Secure Networks at Layer-7

CE FC

L7 Networks Inc.
11494台北市內湖區新湖二路128號5樓之2
30043新竹市民族路25號10樓(SOGO斜對面)
Tel: +886-2-27936053
+886-3-5225946
Fax: +886-3-5240632
http://www.L7-Networks.com