Networks
Secure Networks at Layer-7

雲世代上網安全管理(VM版)

InstantCheck

管理、備份、
側錄、過濾

雲世代早已來臨，面對事實吧!

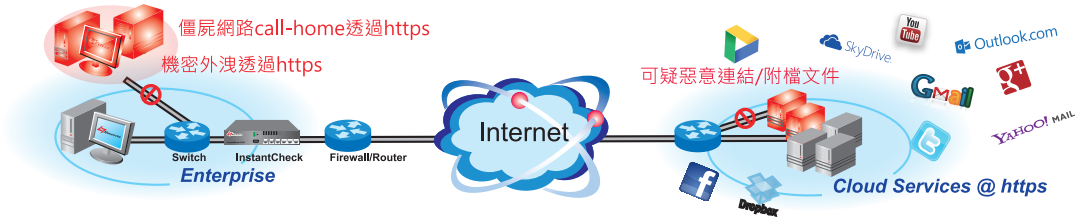
內部/外部威脅，都愛藏在https加密通道中!

■ 過濾https中的內部/外部威脅

當代雲端服務與駭客連線幾乎都是加密的https，導致傳統資安設備無法過濾內容，包括駭客雲(Botnet C&C / APT)網頁郵件雲(Gmail / Outlook / Yahoo Mail)、社群雲 (Facebook / Twitter / Google Plus)、網路硬碟雲 (Dropbox / Google Drive / One Drive)、即時通訊雲(Line / Skype / Google Chat / Facebook Chat)等。研究報告指出，已有40%以上的流量都藏匿於https裡，稽核與過濾網頁內容不再簡單，現在該是面對事實的時候了!

■ 勒索綁架、竊取機密、威脅不斷

近期電腦被勒索綁架的事件頻傳不斷，顯示防毒軟體早已跟不上駭客攻擊漏洞的速度。能有效掌握殭屍網路回報的路徑，與沙箱惡意程式分析，已成為企業最後防線。InstantCheck®內建了InstantGuard®授權，能自動更新【國家資通安全會報】中繼站黑名單，切斷內網中毒者與網軍中繼站的連繫；InstantCheck®從https解密出的可疑檔案能送往外掛的InstantTrace®沙箱惡意程式分析，進行動態模擬與靜態分析。



■ 落實個資法「適當安全維護措施」，備好無過失舉證

各行業都有各自的法規遵循，例如台灣的個資法、美國的沙賓法案、PCI-DSS, HIPAA, SEC, FINRA, FSA, IIROC, FERC, NERC, CFTC, NFA。他們都要求電子通訊必須要記錄並存檔多年供稽核使用。針對https的數位鑑識有其必要性，因為目前犯罪行為都偏向藏匿至加密的https通道中。

■ 數位鑑識不費力，務求無痛導入

無痛導入極為重要，InstantCheck®以透明或代理模式安裝於網路出口，不改網路架構，對用戶幾乎是完全無感。目前能解析一般最主流的https網頁郵件（Gmail / Outlook / Hotmail / YahooMail /...）、最主流的網頁硬碟（Dropbox / One Drive / Google Drive / ...）、最主流的聊天軟體（Line / WeChat / Facebook Chat / Gmail Chat /....）。

■ 豐富的專業外掛模組

為稽核https通道中的內容，InstantCheck®另外配備了以下應用：
(1)內建AegisLab®雲端網址庫: 專業惡意網址資料庫，杜絕已知綁架/間諜軟體入侵
(2)內建InstantGuard®惡意中繼站黑名單: 含【國家資通安全會報】黑名單阻擋僵屍網路
(3)選購InstantAudit®端點稽核: 可記錄PC版Line/Skype/QQ傳送的訊息與檔案
(4)選購InstantTrace®沙箱惡意程式分析: 專業Sandbox杜絕未知惡意APT
(5)選購OCR Lab®資料辨識引擎: 用以偵測檔案、訊息中的個資外洩

駭客雲

惡意中繼站、殭屍連線、
社交工程攻擊、勒索軟體

郵件雲

登入、寄信、寄信夾檔
讀信、讀信夾檔

社群雲

登入、塗鴉牆、留言、
張貼照片、動態消息

即時通訊雲

登入、傳訊息、傳檔

網路硬碟雲

登入、檔案上傳、檔案下載

L7 Networks
Secure Networks at Layer-7

雲世代上網行為管理器(VM版)

InstantCheck

管理、備份、側錄、過濾

授權型號	IC-50VM	IC-100VM	IC-500VM	IC-1000VM	IC-3000VM	IC-5000VM	IC-8000VM	IC-10000VM
處理器需求	雙核心	雙核心	四核心	四核心	八核心	八核心	八核心	八核心
記憶體需求	8GB	8GB	8GB	8GB	8GB	16GB	16GB	32GB
運行作業系統								
VMware ESXi	支援	支援	支援	支援	支援	支援	支援	支援
KVM	支援	支援	支援	支援	支援	支援	支援	支援
管理伺服器								
Windows XP / 7 / 10	支援	支援	支援	支援	支援	支援	支援	支援
Server 2008/2012/2016	支援	支援	支援	支援	支援	支援	支援	支援
Linux CentOS	支援	支援	支援	支援	支援	支援	支援	支援
授權容量								
同時上線IP(可擴充)	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	20K/秒	30K/秒	40K/秒
同時併發連線數	20K	200K	300K	1M	2M	4M	8M	12M
雙向效能	80Mbps	160Mbps	300Mbps	600Mbps	1.2Gbps	2Gbps	4Gbps	6Gbps
基本規格								
安裝模式	獨立主機搭配專屬作業系統，支援以代理(Proxy)與透明橋接(Inline)安裝，支援IPv4與IPv6與LACP鍊路聚合(802.1ax)以執行頻寬合併							
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	能以三秒為即時更新週期，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，包括方向/傳輸量/封包數/頻寬/通道，並可按欄位排序							
聯合防禦	可將解密後內容以ICAP導至第三方進行病毒、沙箱檢測、機密外洩防護等外掛模組或產品，進行深度聯合防禦							
https內容記錄/過濾								
網頁(Web)	能記錄、過濾HTTPS Get之URL與下載檔案名稱/內容、HTTPS Post上傳之各欄位參數、檔案名稱/內容、檔案上傳行為							
網頁郵件(WebMail)	能記錄、過濾https網頁郵箱之寄件/收件內容（含附件），包括Gmail / Outlook / YahooMail / Hinet WebMail / 163 / 126 /...							
網頁硬碟(WebHD)	能記錄、過濾https網頁硬碟之上傳/下載文件進行記錄，包括Dropbox / Google Drive / OneDrive / ...							
社群網站(WebSocial)	能記錄、過濾https社群網站之瀏覽頁面、分享照片、上傳分享文件，包括Facebook / LinkedIn / Twitter / Weibo /...							
網頁即時通(WebIM)	針對瀏覽器https的即時通交談內容進行記錄，包括FacebookChat / Gmail Chat (Google Hangout) / WeChat網頁版 / ...							
傳統內容記錄								
Telnet/FTP	支援Telnet屏幕重組還原（支援彩色ANSI碼）、FTP行為控管(依附檔名、上傳/下載等)與檔案內容記錄							
Email	支援SMTP、POP3、IMAP行為控管（收/送、夾檔等）與內容還原，包括寄件/收件夾檔內容還原							
端點內容記錄 (選購)								
聊天內容記錄	能記錄電腦版Skype/Line/WeChat的一般聊天、群組聊天的訊息內容，以樹狀圖顯示內網人交談對象							
傳檔內容記錄	能記錄透過Skype傳出、接收的檔案名稱與內容							
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	支援70種以上類別，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							
依網站類別作QoS	可針對Content-ID例如內建的URL資料庫類別或自定的URL關鍵字類別，搭配內網地址/AD(User-ID)、第七層應用(App-ID)執行QoS政策							
依網站類別阻擋或警告	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							
威脅防護InstantGuard								
惡意網址/中繼站阻斷	自動更新包括【國家資通安全會報】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							
Google惡意網址庫	自動更新Google Safe Browsing惡意網址庫，阻擋釣魚、詐騙、綁架等惡意連結與下載							
BYOD管理								
行動裝置偵測	支援辨識PC/Android/iOS/WindowsPhone/BlackBerry裝置，並可以策略進行管理							
USB控管	支援以Windows用戶端程式關閉USB大量儲存裝置，並維持其他USB周邊設備運作							
手持裝置單次登入	提供Android/iOS應用程式安裝至手機/平板，以利其單次登入AD網域後，供管理者辨識身分與裝置型態							
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，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)							
流量限速/配額/限連線數	支援以IP或以用戶名為基礎的限流措施，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）							
第七層應用辨識								
即時通訊(Chat)	Line/QQ/AliWangWang/Fetion/Dushow/Popo/SinaUC/Skype/Yahoo/AOL/ICQ/Jabber/LavaLava/Gadu/GoogleHangout...							
點對點下載(P2P)	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)	Skype/Polycom/RTP/RTCP/SkypeOut/Eyeballchat/SIP/TelTel/H.323/MsnVoice/NetMeeting/...							
地道軟體(Tunnel)	Hopster/YourFreedom/Garden/Gpass/Tor/HttpTunnel/JAP/RealTunnel/Vnn/SoftEther/FreeGate/Wujie/...							
串流媒體(Streaming)	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)	Citrix /MySQL /Notes /Oracle /MSSQL /RDP /VNC /UltraVNC /Win /PcAnywhere /Telnet /SSH /TeamViewer /Logmein							
網路硬碟(File Transfer)	SkypeFile / LineFile / SMB / FTP / OneDrive / GoogleDriveUp / Dropbox / AsusWebStorage / Aspera / ...							
線上遊戲(Game)	Diablo3/LoL/CounterStrike/DaHuaShiYo/Dance/WarCraft/MoYu/CadinCar/MiracleWorld/Fight/WenDao/Lineage/...							
特徵碼客製化服務	維護合約期間，可透過內建的tcpdump指令紀錄特定IP的封包至pcap檔案(<200MB)，交由原廠專業服務團隊訂製特徵碼							
http(s)資料外洩防護(選購)	**(Powered by OCR Lab Inc.)**							
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							
網頁快取&代理								
快取演算法	採LRU法則淘汰快取資料，或對特定型態設定TTL，可快取各種類型檔案，包括主流Streaming平台視訊流量							
支援代理協議	支援IPv4/v6的Http(s)/FTP/DNS/RTSP/MMS/Telnet/SOCKS，加密https支援TLS 1.0/1.1/1.2/1.3							
基本過濾功能	可自訂關鍵字/正規表達式，以比對Http(s)要求/回應中的字串，包括文件內容、檔名、附檔名、30種以上資料類型，進行允許或阻擋的政策							
管理與設定								
管理帳號分權管理	支援中文報表、設備集中管理，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，syslog記錄可自訂欄位定時排程上傳至外部伺服器							
報表資料管理	可針對連線細節分析，包括內網IP地址/AD用戶名/外網IP/應用/協議/網址分類/URL/進出流量，並即時或定期依照自訂條件產生							
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							
系統監控	具備硬體健康狀態監測(CPU/記憶體/網路介面/磁碟機/溫度/風扇/電壓等)，與軟體模組健康狀態(Http(s)/FTP/ICAP等服務)							

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 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
Tel: +886-2-27936053
+886-3-5225946
Fax: +886-3-5240632
http://www.L7-Networks.com