3COM Tippingpoint IPS的產品介紹

3COM TippingPoint介紹

TippingPoint 是唯一榮獲資安專業測試機構**--NSS Group** 頒發 **Gold Award** 獎項的設備

2006 年 **TippingPoint** 通過 **ICSA IPS** 認證**,**並且是唯一一家能處理 **3Gbps** 流量的 **IPS** 產品 美國軍方與政府單位所認可的 **Common Criteria(EAL)**認證。

TippingPoint 是在三年內的測試廠商中唯一榮獲 **NSS Gold Award** 的廠商。沒有任何 IDS 的廠商曾經得過這個獎，而 NSS 也是第一次 頒發這個獎給 IPS 廠商。NSS Group 運用了超過 750 種的測試方法與工具來做綜合性的測試，分為效能特徵、安全準確性與使用性三大類進行測試。

(備註：NSS Group 是世界知名的網路與安全測試機構，發佈了一份綜合性的 IPS 安全與效能測試報告，參與測試的產品包括 Cisco、ISS、Juniper/NetScreen、McAfee、TippingPoint 與 TopLayer。)

- **TippingPoint** 在本次的測試中，**NSS Group** 給予下列的結論
  - 在 1GB 流量的環境下，唯一擁有 100%正確性的設備
  - 最快最優異的攻擊辨識能力
  - 最好的 SYN Flood 防護能力
  - 最好的全面性管理機制與安全政策編輯
  - 最好的價格效能比

Test	UnityOne Results
Attack Recognition	100%
Resistance to False Positives	100%
Evasion Baselines	100%
Packet Fragmentation and Stream Segmentation	100%
URL Obfuscation	100%
Miscellaneous Evasion Techniques	100%
Stateless Attack Relays (Mid flows)	100%
Simultaneous Open Connections (Default setings)	100%
Simultaneous Open Connections (After tuning)	100%
UDP Traffic to Random Valid Ports	100%
HTTP "maximum stress" traffic with no transaction delays	100%
HTTP "maximum stress" traffic with transaction delays	100%
Protocol Mix Traffic	100%
"Real World" Traffic	100%
Latency	Exceptional (<116 µs)
User Response Times	Exceptional (<1ms)
Stability and Reliability	PASS
Management Interface	PASS

為何需要IPS

TippingPoint IPS 效能與功能滿分，頻頻榮獲全球各大專業測試機構最高評價的肯定
在資安防護技術的演進歷史中，過去扮演要角的防火牆因為只能管制 IP 與 Port#，對於 新一代透過 Port# 80 或是 Random Port#傳遞的攻擊封包已經束手無策。傳統的入侵偵測系統(IDS)產品由於只能偵測惡意與非法的網路流量卻不能在第一時間阻擋，對使用者的實質幫助不大，更何況誤判情況嚴重、過多而雜亂無序的 Alert 反而增加使用者的工作負擔。面對日益嚴重的網路威脅，入侵偵測防禦系統(IPS)不但可以早一步偵測到駭客的攻擊，更可以直接將有害的流量阻擋於網路之外。

TippingPoint IPS 真正採用硬體架構的設計，處理效能業界第一

TippingPoint IPS 擁有客製化的 Xilinx Vertex FPGA (For Layer 7 Packet Inspection/ Block/ Rate-limit)以及 ASIC 架構的 NPU 晶片(For Layer 4)，來建構 IPS 的核心--TSE 威脅防禦引擎（Threat Suppression Engine），不像其他採用軟體架構的 IPS，由於處理效能會隨著 Filter 啟動越多而受到嚴重影響，Latency 往往高達數秒甚至數十秒之多。

優異的硬體效能讓 TippingPoint IPS 即使建置在 Gigabit 流量的網路環境中也可以輕鬆處理包括表現於下列性能：

- IP De-fragmentation
- Flow Reassembly
- 第七層封包解析比對
- 攻擊行為統計分析
- 流量限速
- 惡意封包阻擋
- DoS/DDoS 攻擊防禦
- Spyware 防護
- 異常流量狀態追蹤和超過 170 種的應用層網路通訊協定檢查工作
- 僅有微秒的延遲 (Latency under Microsecond)發生，並具有高度的準確性
- TippingPoint IPS 運用 TSE 突破性的擴充性與高效能技術來辨識異常的通訊協定與網路流量，保護網路不會遭受 DDoS 攻擊，並阻擋或限制未經授權的應用程式的頻寬(例如 P2P)。
- TSE 重組與檢視封包的內容並分析至網路的應用層。當每一個新的封包隨著資料流到達 TSE 時，資料流會被重新檢視是否含有有害的內容，如果封包被檢查出有害，那麼這個封包 以及隨後而來附屬於這個資料流的封包將會被阻擋。這可以保證攻擊不會毫無阻欄的到達目的地。

TippingPoint 擁有優質安全技術團隊，攻擊防禦機制更新最迅速最確實

TippingPoint 的安全技術團隊與全球知名的資安通報中心 SANS、CERT 等協同工作，可以同步的針對新型態攻擊與新發布的漏洞製作出防禦 Filter，載入數位疫苗（Digital Vaccines）中。數位疫苗不只針對特定的攻擊 製作 Filter，還包括變種的攻擊與零時差的威 脅。為了擁有最大的安全涵蓋範圍，數位疫苗 除了每週定時更新 Filter 資料庫外，當隨時有 新的威脅嚴重漏洞或威脅產生，數位疫苗也會 自動的透過 Akamai 佈建於全球 56 個國家超過 9,700 台的伺服器同步下載至客戶端。 TippingPoint 的數位疫苗擁有業界最快速的更新，零時差的為您阻擋入侵過濾有害封包，即使系統漏洞未能即時修補也不用擔心。

TippingPoint 的安全專家是被世界公認的，全球超過二十五萬個安全管理者及專家都訂閱了 TippingPoint 所編輯的 SAN @RISK 分析報告。相同的分析也運用到數位疫苗的開發上，優先製作出保護 TippingPoint 客戶的最佳 Filter

TippingPoint在網路安全管理中可用的功能有那些：

- 加強管制 **MSN、Yahoo Messenger、QQ、Skype、P2P**
  IM(MSN、Yahoo Messenger、ICQ、QQ….) 與各種P2P服務大舉進佔企業網路， 頻寬即使加得再多都感覺到網路壅塞不順,更別提不當使用這些軟體所帶來的災難，如：木馬進駐、蠕蟲亂竄、資料外洩….等。越來越多的單位開始採取行動--加強管制 IM、Skype、P2P….等，TippingPoint可做以下的安全等級管理：
  - 阻擋 IM(MSN、Yahoo Messenger、ICQ、QQ….)的使用
  - 讓 IM 只能傳遞文字訊息不允許傳檔
  - 阻擋 Skype
  - 針對P2P流量做使用頻寬的限制
- 作業系統常常公佈新漏洞，公司裡的電腦又一大堆，管理人員**Patch** 上到手抽筋
  TippingPoint可以解決以下的難題：
  - 對於企業單位裡的每一台伺服器、每一台電腦都隨時下載最新的 Patch 檔嗎？
  - 有多少員工帶進來的 Notebook 藏身於企業內部？
  - 是否得要常常祈求老天保佑這些外來設備都是乾淨而且安全的嗎？
  - 辛苦的 MIS 工作者對於層出不窮的網路攻擊事件是否感到維運網路的負擔越來越沉重？

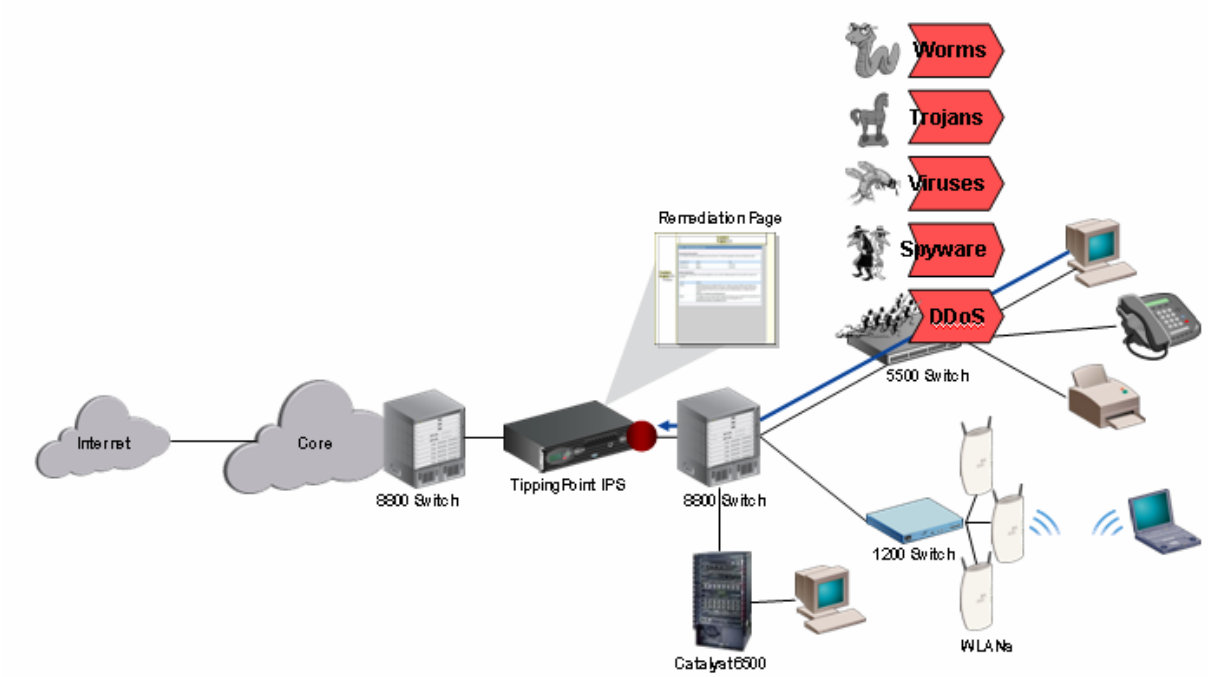
最寬廣、最深入資安保護設計--TippingPoint IPS 的三大入侵防禦功能

TippingPoint IPS 擁有業界最寬廣也最深入的入侵防禦設計，將 TippingPoint IPS 放置在網路最重要的節點上(例如 Internet 出入口、Server Farm 出入口、學校宿網出入口、企業 外點 VPN 入口處等…),可以有效阻絕惡意封包,提供您涵蓋 PC、Server、Switch、Firewall、 Router 等設備的入侵保護，並藉由對 P2P、IM、間諜程式(Spyware)以及 DDoS 攻擊的頻寬管制或是阻攔，確保網路傳輸效能始終保持在最佳狀態。

Tippingpoint IPS 應用範例（一）

隔離功能**(Qurantine)**

從閘道端防護擴展到端點防護的新技術



在現在的網路環境中最常見到的情況就是：一台電腦因為使用不慎遭植入惡意程式，當 使用者操作這台電腦連結網路的同時，惡意程式也在運作，因此這台電腦有好的連線行為(例如瀏覽網站、寄送 Email)；也有壞的連線行為(例如惡意程式發送攻擊封包)。

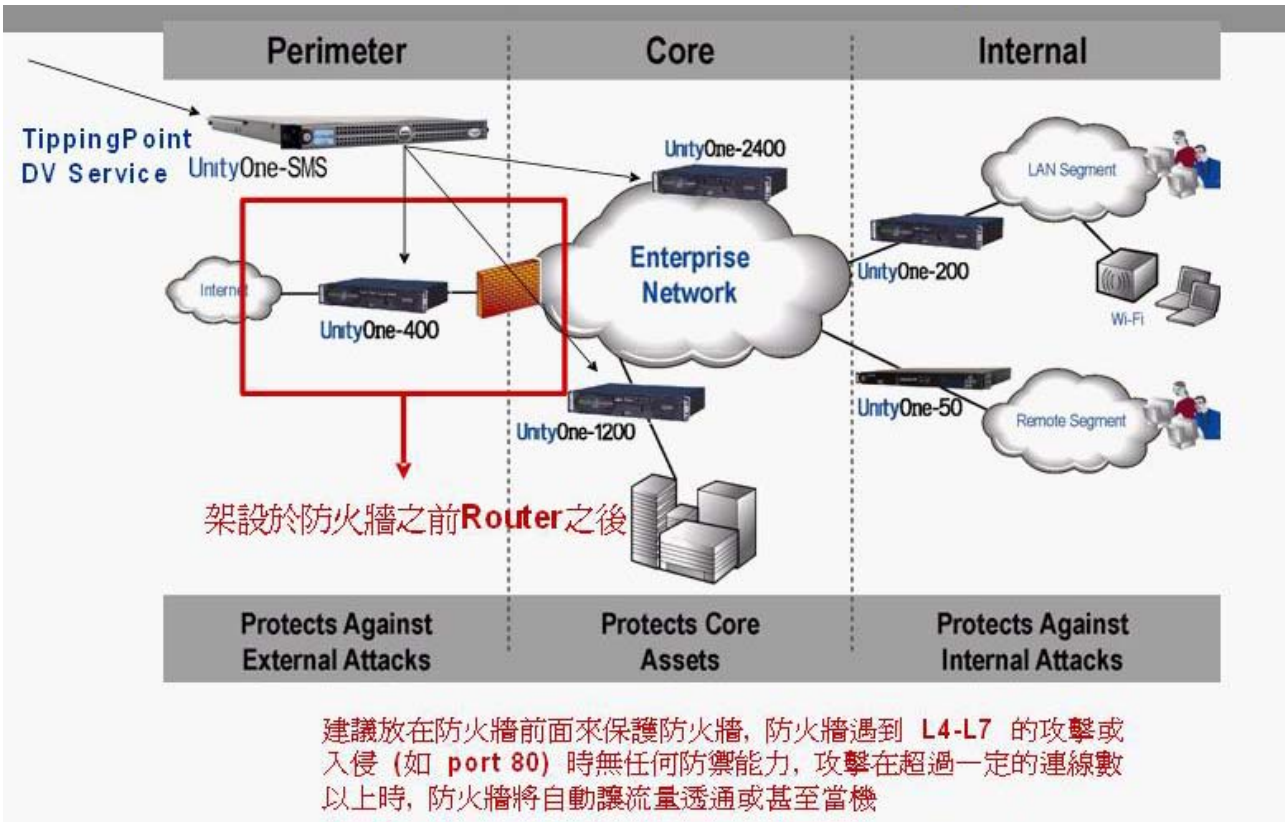
不同於防火牆只能把 IP Deny 的作法，IPS 的優點就在於：僅針對惡意的流量或是攻擊封包攔阻，允許正常的網路使用行為通過。只是這樣的優點尚有不足的地方，包括使用者並不知自己的電腦有問題正在散撥蠕蟲或是攻擊別人；以及這台電腦倘若攻擊鄰近的設備，閘道型 IPS 將無法防護。

為了改善上述的問題，TippingPoint 發展出實用的隔離技術(Qurantine)讓原本只是閘道端防護的 IPS 也可以做到端點防護(End-to-End Security)。TippingPoint IPS 具備下述幾種隔離作法：

- 不讓遭隔離的電腦瀏覽網站--攔截使用者瀏覽網站的頁面，改成預先配置好的告警畫面
- 不允許遭隔離的電腦繼續連結網際網路--阻斷 Email 的寄送以及其他一切連網服務(例如 IM 以及 P2P),**Disable** 遭隔離的電腦的 **Switch Port**將遭隔離的電腦切換到一個隔離的 **VLAN**--例如：該 VLAN 不允許連結內部網路但是可以連上網際網路

Tippingpoint IPS 應用範例（二）

企業環境內部與外部流量兼具的保護



Tinpingpoint IPS在企業的網路環境中，不但對於想要保護的Server，有完善的安全防護機制，像是一般常見DDoS阻斷式的攻擊手法，或是利用微軟系統的漏洞而產生的零時差攻擊手法，或像是其他的木馬，間諜程式都有優秀的防護能力，以確保Server不會遭受到被入侵，或是重要的資料被竊取，遭他人竄改，甚至被破壞；同時，也提升了整個網路的品質，因為減少了許多不必要的封包流量，而使得網路中都是真正需要被傳遞的資訊。

TippingPoint IPS 可以逐一檢查網路中的封包內容，透過辨識間諜程式的方式來保護網路不受其危害。使用者可以針對TippingPoint IPS 中關於間諜程式的過慮器(Filter)設定成阻擋(Block)模式，就可以輕鬆防止間諜程式的危害，同時還會防止資料傳輸出去。對於已經安裝病毒成為殭屍軍團一員的電腦，TippingPoint IPS 會阻斷其與外界控制端的連線，管理者只需從Report 中就可以得知哪些電腦已經遭到入侵成為殭屍軍團，方便管理者清除病毒。

另一方面，TippingPoint IPS提供使用者可以針對Protocol(TCP/UDP/ICMP/other IP protocol)或是Application(某個特定的Port#)做臨界值(Threshold)的設定。使用者可以根據平時觀察出的正常流量設定臨界值，當異常暴增的流量發生時，TippingPoint IPS會遵照使用者預先的設定將該Protocol或是Application 限制在一定的頻寬之內(Bandwidth Control)，確保網路的效能不受到影響。也可以保護企業內部中的網路設備，因為許多不必要，甚至是惡意的封包都先被Tippingpoint IPS阻擋下來，而減少過多的封包造成其他二層、三層的設備的負載，同時，也會增快了二層、三層設備處理網路封包的速度，進而提升企業在資訊傳遞上的時效性。

Tippingpoint IPS 應用範例（三）

IPS 與身份解析A10 IDsentrie企業環境的應用

A10 IDsentrie的事件管理引擎通過對網路中的防火牆、IDS/IPS 等安全設備以及網路設備的日誌進行綜合分析，並與用戶身份和認證訊息進行相互關聯，能夠準確地追蹤網路資源的使用情況和重要的用戶行爲。可以基于用戶身份進行實時監視、查看以往的歷史記錄、提供基于身份的報表、日誌以及預警功能，使得用戶的網路行爲具有較深層次的可視性。網路行爲監視及事件管理能夠快速地指出某個用戶、在什麼時間、通過哪個防火牆做了哪些事情，這樣對快速解決問題和預防網路異常發揮了積極的作用。