

防火牆與 IDP 的差異

傳統防火牆可以檢視對應 OSI 模型第 2 到第 4 層通訊協定的內容，防火牆最常檢查及管理的就是 Source IP Address (**來源 IP 位址**)、Destination IP Address (**目的 IP 位址**)、Source Port Number (**來源埠號**)、Destination Port Number (**目的埠號**)、以及 **Flag Fields**，**Flag Fields** 僅位於 TCP 表頭中。

以 HTTP 為例，它預設使用的 Port 為 TCP 80，如果公司的 WEB 伺服器允許外界利用 80 Port 存取服務，則防火牆會將這樣的封包轉給內部的伺服器，除了 Port 80 的要求外，對其他的要求通通都拒絕，這樣就達成一個基本的防護效果。

這一切似乎都很美好，但是如此傳統的防禦機制已無法遏止日新月異的攻擊手法，以剛剛的 WEB 需求為例，如果在 TCP 80 Port 中傳遞的是有惡意的木馬、病毒等攻擊程式碼，因為在防火牆的規則中它是屬於合理的使用行為，所以不會阻擋，往往使用者的電腦就因此而癱瘓、中毒，這樣的事件層出不窮，但是 IDP 卻可以做到更完美的阻擋。

防火牆僅能就網路封包做到 2 到 4 層的檢測，就來源位址、埠號以及目的地址、服務進行控管。而 **IDP 可以做到 4 到 7 層(也就是應用層)的檢測**。因此 IDP 可以發覺包藏在應用層裏的惡意攻擊碼(譬如蠕蟲攻擊、緩衝溢位攻擊便藏匿於此)，並予以狙擊。

IDP 內建龐大的攻擊特徵資料庫，可以有效阻絕已知的攻擊，IDP 也透過「異常協定偵測」的方式，即時檢查並將不符合 RFC 規範的網路封包丟棄。所以在「攻擊防禦」方面，IDP 遠勝於防火牆之上。

IDP 可以防止蠕蟲由外入侵至企業網路內部，而如果防火牆要防止蠕蟲攻擊，僅能消極地關閉某些 Port。但一般的檔案型病毒，則不在 IDP 及防火牆的防護範圍內。因此資安的最後一層防護網便是在使用者端安裝防毒軟體。

前面已經說明 IDP 跟 FireWall 的差別就是 IDP 會做內容或行為檢查，所以 IDP 的優劣就在於特徵值資料庫的多寡及更新速度，也就是說 IDP 的資料庫有越多的特徵值，意味它能辨識越多不正常的內容或網路行為，但是事情總不是如此完美，越多的檢查就需要越強的運算能力，否則好處沒嘗到，反而付出網路速度緩慢的後果。

一般而言，IDP 的特徵值資料庫會依照危險程度分成高、中、低三種，再讓管理者決定放行或阻擋，考量客戶端的實際網路環境及機器的運算能力，在中小型的網路架構的 IDP 設備只需要有完整的危險程度高、中(例如，病毒、木馬程式)的特徵值資料庫就足夠，其他屬於警告或通知性質的檢查沒必要處理。

IDP 的設定及特徵值更新

打開 IDP 功能選項的頁面如下圖：



入侵偵測防禦設定

最近查詢時間：08/04/07 11:09:39 (每 120 分鐘自動查詢特徵定義檔)

特徵定義檔版本：1.1.1 (Signature definitions updated at 08/04/06 17:09:12)

立即更新特徵定義檔 (使用 TCP 埠號：80 和 UDP 埠號：53) [立即更新](#) [輔助測試](#)

啟動病毒偵測 (for P2P, IM, NetBIOS...)

開啓 NetBIOS 警訊通知

管理員 IP 位址

啟動遠端記錄 必須先完成 Syslog 設定。 [監控報告 -> 監控記錄 -> 設定]

[確定](#) [取消](#)

目前 IDP 會每 30 分鐘到 IDP 伺服器更新特徵值資料庫，它使用 TCP 80 及 UDP 53 Port 跟伺服器溝通，同時管理者可以決定要不要啟動 P2P、IM、NetBIOS 的防毒。

剛剛所說的危險程度分成高、中、低三種，再讓管理者決定通行或阻擋的設定就在同一個畫面的下方，如下圖：

設定所有預設特徵的動作				
高風險	<input type="button" value="阻擋"/>	<input checked="" type="checkbox"/> 記錄	<input checked="" type="checkbox"/> 警示	(建議使用 [通行])
中風險	<input type="button" value="通行"/>	<input checked="" type="checkbox"/> 記錄	<input checked="" type="checkbox"/> 警示	(建議使用 [通行])
低風險	<input type="button" value="通行"/>	<input checked="" type="checkbox"/> 記錄	<input checked="" type="checkbox"/> 警示	(建議使用 [通行])

只要將高危險程度的封包設為 Drop (丟棄)，滿足大部分的資訊安全機制。

IDP 的特徵值資料庫

再高階的機種目前約有 2913 個特徵值，分布在數十種的類別中，以木馬程式分類為例，大部分都會被歸類在高危險類，目前資料庫中有 313 種木馬程式，如下圖：

SNMP (17)	修改
Spyware (313)	修改
[SPYWARE] 180solutions Update Engine	H → v 修改
[SPYWARE] 2020search Update Engine	H → v 修改
[SPYWARE] 2nd-thought (W32.Daqa.C) Download	H → v 修改
[SPYWARE] Abox Install Report	H → v 修改
[SPYWARE] Unknown Advertising.com Agent	H → v 修改
[SPYWARE] Unknown Advertising.com Data Post	H → v 修改
[SPYWARE] Unknown Advertising.com Data Post	H → v 修改
[SPYWARE] A-d-w-a-r-e.com Activity	H → v 修改
[SPYWARE] A-d-w-a-r-e.com Activity	H → v 修改
[SPYWARE] Adwave Agent Access	H → v 修改
[SPYWARE] Wintools Download/Configure	H → v 修改
[SPYWARE] Aitnet PeerPoints Manager Start	H → v 修改
[SPYWARE] Aitnet PeerPoints Manager Data Submission	H → v 修改
[SPYWARE] Aitnet PeerPoints Manager Settings Download	H → v 修改
[SPYWARE] Aitnet PeerPoints Manager Traffic	H → v 修改
[SPYWARE] Amex.lpsrime.com Unknown Malware Download	H → v 修改

自訂特徵值資料庫

除了靠 IDP 伺服器的特徵值資料庫外，管理者可以依自己網路的行為特性制定自己的特徵資料庫，它建立的範例如下：

新增自訂特徵	
特徵名稱	sharetech_TEST (最多30個字元, ex: external_mounted_access)
通訊協定	<input type="radio"/> TCP <input checked="" type="radio"/> UDP <input type="radio"/> ICMP <input type="radio"/> IP
來源埠	0:65535 (範圍: 1 - 65535, ex: 80 or 80:80)
目的埠	138:139 (範圍: 1 - 65535, ex: 111:112)
風險	高
動作	阻擋 <input type="checkbox"/> 記錄 <input type="checkbox"/> 警示
內容	File keyword (最多50個字元, ex: mount or \x6d\x6f\x75\x6e\x74)
進階選項	
<input checked="" type="checkbox"/> 無方向性	
<input type="checkbox"/> 不區分大小寫	
<input type="button" value="確定"/> <input type="button" value="取消"/>	

Name：這個特徵值它的命名。

Protocol：通訊協定是 TCP、UDP、ICMP 或只是 IP。

Source Port：來源位址，0:65535 代表外部任何 Port。

Destination Port：目的位址，如果防止的攻擊來自外面，就是內部伺服器的 Port。

Risk：區分高、中、低三種危險程度。

Action：放行或阻擋。

Content：封包內容是否有含有特定字元，可以是文字模式或編碼模式(例如特定的 MAC Address)。