

中小企業商務應用 應用範例

■ 常遭受到外部網路攻擊，怎麼辦？

IDP(入侵偵測與即時防禦 (Intrusion Detection and Prevention)，它和IDS(入侵偵測系統)不同的是，對於偵測到的攻擊和掃描的行為，具有主動和自動的阻擋功能，並且在阻擋完成後，會告訴系統管理者有人曾經試圖對你的系統進行掃描和攻擊，但是已經被IDP阻擋了。它跟防火牆最大的不同是防火牆只管到Layer 3 TCP/IP 層，IDP則會管制Layer 3~7 資料層。

眾至解決方案

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 的特徵值資料庫：

AW目前最多約有 2696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，預設值都是刪除這類的網路封包，目前資料庫中有313 種木馬程式，這些木馬程式屬於高危險程度的特徵值，一但通過AW IDP 系列的閘道器，馬上就會被AW的IDP攔截，並將封包丟棄。

中小企業商務應用 應用範例

你
·
簡
單
用
網
路
·
複
雜
問
題
我
們
處
理
!

Rservices (13)					修改
Scan (17)					修改
Shellcode (21)					修改
SMTP (59)					修改
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

對於中、低危險程度的封包處理，就由管理者決定，以BitTorrent 這個P2P為例，他是不是個危險行爲，每個人的觀點都不一樣，在AW的IDP中就可以定義是否要讓他通行或阻擋。

P2P (18)					修改
[P2P] napster login	M	⊗	v		修改
[P2P] napster new user login	M	⊗	v		修改
[P2P] napster download attempt	M	⊗	v		修改
[P2P] napster upload request	M	⊗	v		修改
[P2P] GNUTella client request	M	⊗	v		修改
[P2P] Outbound GNUTella client request	M	⊗	v		修改
[P2P] GNUTella client request	M	⊗	v		修改
[P2P] Napster Client Data	M	⊗	v		修改

這個功能在沒有IDP功能的設備IM/P2P內管管制中也有，但是2者還是有些不同，在Content Blocking 的設定會針對這個軟體做開放或關閉的動作，但是IDP中的P2P管理更可以針對這個P2P軟體的細項功能做開放或關閉的動作，例如可以看到BitTorrent的更新資料，但是卻不能傳檔。所以IDP是比原來的【內容管制】有更多的管理機制。

中小企業商務應用 應用範例

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

新增自訂特徵	
特徵名稱	jean_test (最多30個字元, ex: external_mounted_access)
通訊協定	<input checked="" type="radio"/> TCP <input 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	138:112 (範圍: 1 - 65535, ex: 111:112)
風險	高
動作	通行 <input type="checkbox"/> 記錄 <input type="checkbox"/> 警示
內容	報價單 (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	

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)。

最重要的是[Content]這個欄位，例如可以填入 [報價單]三個字，意味只要傳遞的內容有這三個字，IDP就會執行將網路封包丟掉、紀錄或是警告這些動作。

中小企業商務應用 應用範例

你，簡單用網路，複雜問題我們處理！

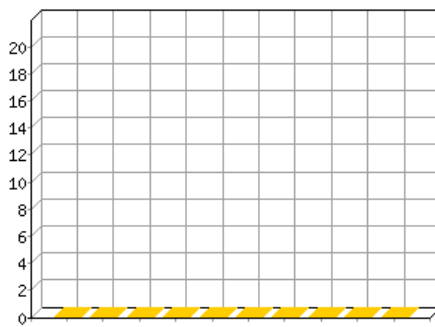
IDP Report

除了實際的阻擋之外，AW IDP 也有完整的報表制度，搭配實際的攻防紀錄，讓管理者更清楚地知道網路安全狀況。

年 月 週 日

期間	2009-08-12 00:00:00 ~ 2009-08-12 09:36:41				
事件種類	0	事件總數	0	TCP	0
首次事件	---	最近事件	---	UDP	0
攻擊位址總數	0	被攻擊位址總數	0	ICMP	0
攻擊介面	LAN	WAN1	WAN2	WAN3	DMZ
攻擊次數	0	0	0	0	0

前10名事件排行



前5名介面排行

