

家庭與個人工作室 應用範例

■ 家庭及工作室資安解決方案

描述

防止來自網際網路的攻擊，分成2個部份，一個是系統內建的駭客防護部份，另一個是管制條例的規則設定。

眾至解決方案

1.駭客入侵

只要啟動下列選項，內部網路就自動獲得多功能防火牆的保護，甚至連殺手病毒、疾風病毒等都可以防護，一般駭客的攻擊手法是用大量ICMP、UDP、SYN等通訊協定，造成目標主機無法對外連線或是提供服務，達到癱瘓對方的目的。

ShareTech 多功能防火牆將這些防範的功能做在每一台設備上，只要勾選就具有這樣的防護效果。

DoS / Anti-Attack 設定	
<input checked="" type="checkbox"/> 阻擋殺手病毒	<input checked="" type="checkbox"/> 阻擋疾風病毒
<input checked="" type="checkbox"/> 阻擋紅色警戒病毒	<input checked="" type="checkbox"/> 阻擋 Nimda 病毒
<input checked="" type="checkbox"/> 偵測 SYN 攻擊	允許 SYN 最大流量 <input type="text" value="200"/> 封包/秒 (範圍: 0 - 9999)
	允許每個來源位址 SYN 最大流量 <input type="text" value="50"/> 封包/秒 (範圍: 0 - 9999)
	當來源位址超過 SYN 最大流量時的阻擋時間 <input type="text" value="60"/> 秒 (範圍: 0 - 9999)
<input checked="" type="checkbox"/> 偵測 ICMP 流量	允許 ICMP 最大流量 <input type="text" value="1000"/> 封包/秒 (範圍: 0 - 9999)
	允許每個來源位址 ICMP 最大流量 <input type="text" value="300"/> 封包/秒 (範圍: 0 - 9999)
	當來源位址超過 ICMP 最大流量時的阻擋時間 <input type="text" value="60"/> 秒 (範圍: 0 - 9999)
<input checked="" type="checkbox"/> 偵測 UDP 流量	允許 UDP 最大流量 <input type="text" value="1000"/> 封包/秒 (範圍: 0 - 9999)
	允許每個來源位址 UDP 最大流量 <input type="text" value="300"/> 封包/秒 (範圍: 0 - 9999)
	當來源位址超過 UDP 最大流量時的阻擋時間 <input type="text" value="60"/> 秒 (範圍: 0 - 9999)
<input checked="" type="checkbox"/> 偵測 Ping of Death 攻擊	<input type="checkbox"/> 偵測 Tear Drop 攻擊
<input type="checkbox"/> 偵測 IP Spoofing 攻擊	<input type="checkbox"/> 過濾 IP Route 選擇
<input checked="" type="checkbox"/> 偵測 Port Scan 攻擊	<input type="checkbox"/> 偵測 Land 攻擊

家庭與個人工作室 應用範例

你
·
簡
單
用
網
路
·
複
雜
問
題
我
們
處
理
!

2.管制條例外到內

在管制條例的外部到內部的規則中，如果沒有設定代表不能從網際網路進來內部，如果內部有架設郵件伺服器、WWW或者是ERP伺服器等，就要像下圖的紅色框框的設定規則在管制條例上，一般的定義如下，從網際網路的哪個來源IP位址，可以到內部伺服器作哪件事情(Port)。

來源網路	目的網路	服務名稱	動作	監控功能	變更	移動
Outside_Any	Inside_Any(Routing)	ANY			修改 刪除 暫停	To 1 <input type="button" value="v"/>
*CHINA_TELECOM	Inside_Any(Routing)	ANY			修改 刪除 暫停	To 2 <input type="button" value="v"/>

[新增](#)