your future life

Firewall

繁體中文使用手冊

九、防火牆配置

本章節介紹防火牆設定的選項，以及網路存取控制的設定，保證網路的安全性。

9.1 基本設置

從防火牆功能的一般設定選項當中， 您可以控制開啟或是關閉這些選項功能。出廠預設值是將防火牆開

啟，並關閉不必要的回應。

防火牆功能： 此為選擇開啟或關閉防火牆功能。預設啟用。

SPI 封包檢測: 此為封包主動偵測檢驗技術，防火牆主要運作在網路層，但是藉由執行對每個連結的動態檢驗，也擁有應用程式的警示功能。同時，封包檢驗型防火牆可以拒絕非標準的通訊協定所使用的連結。預設啟用。

防止 DoS 攻擊功能: 此為保護 DoS 攻擊，如 SYN Flooding， Smurf， LAND， Ping of Death， IP Spoofing 等。預設啟用。

關閉廣域網回應功能: 若是選擇啟用的話，則 VPN 防火牆會關閉對外的 ICMP 與不正常連線的封包回應，所以若是您從外部去 ping 此台 VPN 防火牆的 WAN IP 是無法 ping 通的，預設值為開啟拒絕對外回應的功能。

遠距管理: 遠端管理功能，若您要通過遠端網路 直接連線進入 VPN 防火牆的設定視窗，必需將此功能開啟，並於遠端於流覽器網址填入 VPN 防火牆的外部合法 IP 位址(WAN IP)，並加上預設可修改的控制埠。

Http 模式：預設為 8080，可更改為 80 或者是 1024 以上的埠口號。

Https 模式：預設為 443，可更改為 1024 以上的埠口號。

本地管理： 管控內部網路(LAN)電腦連線到 VPN 防火牆的設定視窗的連線埠口號。

Http 模式：預設為 8080，可更改為 80 或者是 1024 以上的埠口號。

Https 模式：預設為 443，可更改為 1024 以上的埠口號。

允許 Multicast 封包穿透: 網路上有許多影音串流媒體，使用廣播方式可以讓用戶端接收此類封包訊息格式。預設為關閉

防止 ARP 病毒攻擊： 此功能為防止內網遭受 ARP 欺騙攻擊而造成電腦無法上網，此 ARP 病毒欺騙大多在網咖環境發生，會讓所有上網電腦一瞬間掉線或部份電腦無法上網。開啟此功能可以避免此種病毒攻擊。

高級設定

封包類型: VPN 防火牆提供三種資料封包傳輸類型，包括 TCP-SYN-Flood、UDP-Flood 以及 ICMP-Flood。

廣域網限定值設定：防止來自外部網路的攻擊。設定"所有封包限定值"（即外部攻擊的所有封包資料），當其達到一個最大值（預設 15000pakets/Sec），VPN 防火牆將只允許通過所設定最大值的封包數。

當單一 IP 的封包限定值（外部單一一個 IP 位址攻擊的封包資料）達到一個最大值（預設 2000pakets/Sec），就會阻擋此 IP 上網 5 分鐘（預設是 5 分鐘），禁止其訪問伺服器，限制其流量和連接數，從而有效保證網路的安全。這裏您可以根據需要調整你的限定值以及阻擋時間來達到對外網攻擊的有效防護，建議其限定值從大到小來調節，避免限定值過小影響正常網路的運行。

區域網限定值設定：防止來自內部網路的攻擊。同樣，當所有封包限定值（即外部攻擊的所有封包資料）達到一個最大值（預設 15000pakets/Sec），VPN 防火牆將只允許通過所設定最大值的封包數。

當單一封包限定值（內部單一一個 IP 位址攻擊的封包資料）達到一個最大值（預設 2000pakets/Sec），就會阻擋此 IP 上網 5 分鐘（預設是 5 分鐘），禁止其訪問伺服器，限制其流量和連接數，從而有效保證網路的安全。您可以根據需要調整你的閥值以及阻擋時間來達到對內網攻擊的有效防護，建議其閥值從大到小來調節，避免閥值過小影響正常網路的運行。

不受限制的來源IP位址: 輸入不要被 DOS 防禦設定限定值所限制的區域網來源 IP 位址或是範圍

不受限制的目的IP位址: 輸入不要被 DOS 防禦設定限定值所限制的目的 IP 位址

(從區域網發出的封包)

顯示被阻擋的 IP：

顯示被 DOS 防禦功能所阻擋的 IP 位址，以及該 IP 位址還剩餘多少時間解除阻擋

禁止特殊應用： VPN 防火牆支援封鎖下列幾種的方式連結：Java，Cookies，Active X，HTTP 代理伺服器存取。

不受限制的信任網域名稱: 若啟用這項功能，使用者可以將信任的網站或者 IP 位址加入可信任的網域中，則 VPN 防火牆就不會去阻擋可信任網域的網頁中所帶有的 Java/ActiveX/Cookies 等。

確定: 點選此按鈕"確定"即會儲存剛才所變動的修改設定內容參數。

取消: 點擊此按鈕"取消"即會清除剛才所變動的修改設置內容參數，此操作必須於"確定"存儲動作之前才會有效。