

整合連接埠控管機制的UTM設備

FortiGate 224B對於LAN埠提供嚴謹、動態兩種管理模式，檢查用戶端電腦是否合乎設備的管理規則，否則便予以隔離

整合L2交換器功能的FortiGate 224B，是一臺具備24組10/100埠、2組GbE埠，共計26組LAN埠的UTM設備。除了交換器的功能之外，FortiGate 224B的LAN埠也提供網路隔離的安全機制，管理者可以在設備的Web介面中將LAN埠設定成嚴謹（Strict），或是動態（Dynamic）兩種模式，並且制定管理規則，從中檢查連接設備的用戶端電腦是否有依照規定安裝防毒軟體、個人防火牆、修補程式，以及通過設備的流量當中是否帶有病毒之類的資安風險。對於未能符合規則要求的電腦，設備會自動將所連接的LAN埠隔離到另外一個預設好的VLAN，直到問題解決才准予放行，以免將可能存在的資安威脅透過區域網路散布到周圍的其它電腦。

預設狀態下，FortiGate 224B對於各個LAN埠皆完整開放存取網路的權限，剛才所提到的網路隔離機制，在預設值當中並未開啟，這時設備對於用戶端電腦的防護，主要是利用UTM所定義的各項功能，過濾掉流量當中不被允許，或者是帶有資安風險的內容。

彈性管理網路存取權限

登入Web介面之後，我們可以在Switch→Port Quarantine的路徑下，將LAN埠個別設定為嚴謹或是動態模式。

設定為嚴謹模式的LAN埠，對於所連接的用戶端電腦，一開始皆是隔離到設備所預設好的VLAN網段



在嚴謹、動態模式下，未能符合管理規則的電腦將會隔離到設備預先設定好的VLAN，並透過瀏覽器畫面告知有那些項目不合乎管理規則的要求。

(quaran_vlan)，待設備確認用戶端電腦的安全性合乎管理規則的要求，才會給予正常存取網路的權限，此時開啟瀏覽器，FortiGate 224B會自動把畫面導引到位於10.255.100.254的入口網站。若是用戶端電腦的安全性與管理規則完全相符，那麼瀏覽器畫面將會出現訊息告知使用者已經取得存取網路的權限，設備對於未能符合規定的電腦，則將繼續隔離，並透過瀏覽器畫面告知目前還有那些項目未能合乎管理規則的要求。

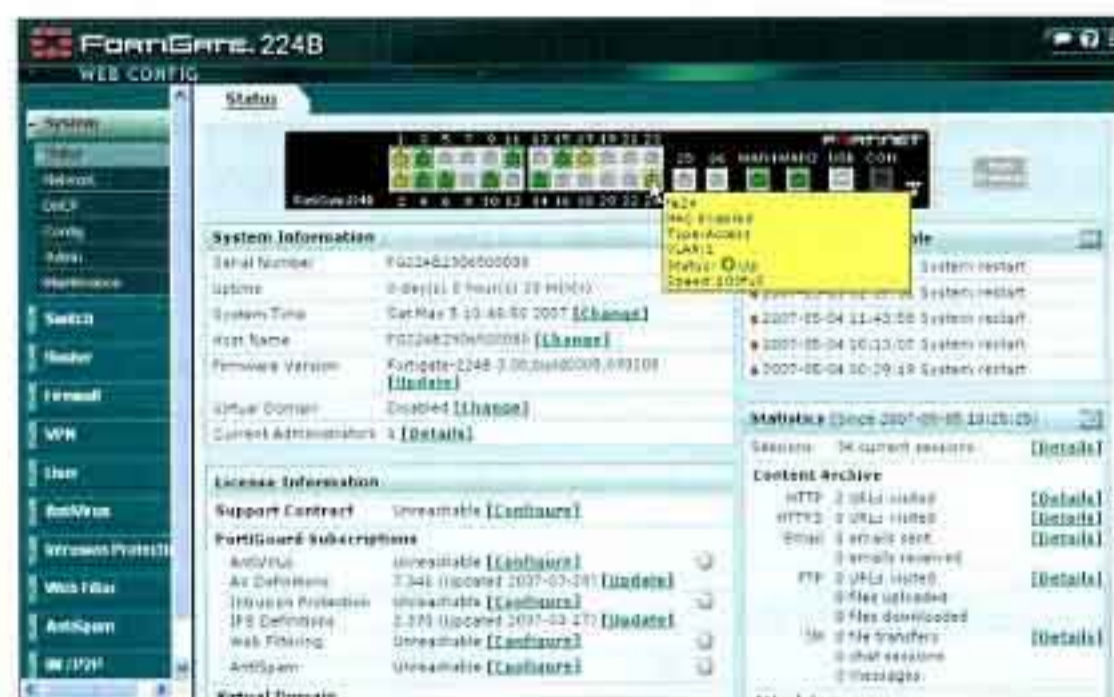
相對於前者，動態模式對於用戶端電腦的管理就比較寬鬆，對於所有相連接的電腦均給予正常存取網路的權限，直到發現電腦未能符合管理規則的要求才會予以隔離。設備的管理者可以視實際需求以兩種不同模式設定各個LAN埠，以提升設備管理的靈活程度。

以VLAN、安全埠強化區網控管

像是會議室這類經常有訪客電腦連接的公共區域，我們也可以透過FortiGate 224B將所在的網路環境予以隔離，僅提供存取外部網路的權限，保護企業內部電腦不會從區域網路接收來自這些電腦所帶來的資安威脅。

由於FortiGate 224B本身也是一臺L2等級的交換器，因此可以透過切割VLAN的方式達到這個目的。預設情況下，設備會將所有的LAN埠畫分在一個叫做Native的VLAN區域，之後管理者可以視需求，將Native下的LAN埠指派到其它的VLAN，以便達到隔離網路環境的目的。

除此之外，也可以將LAN埠個別設定成所謂的Secure Port，被指定成Secure Port的LAN埠，在狀態上和這臺設備上其它的LAN埠完全隔離。和VLAN相比，這項功能的設定方式相當容易，只要在Web介面勾選這項功能，就直接可以啟用。



FortiGate 224B的Web介面上方，有一個模擬出來的連接埠面板，藉由不同色塊的區隔，可以清楚了解各連接埠的使用狀態，例如設置在嚴謹、動態模式下的LAN埠以黃色表示，遭到隔離的LAN埠所使用的是紅色，至於未受到管理，且正常使用中的LAN埠，則用綠色來做表示。



以兩種設定檔檢查電腦是否安全無虞

前述兩種模式檢查用戶端電腦是否合乎要求的依據，主要是透過Client Profile（在Port Quarantine當中設定），以及Protection Profile兩種設定檔對用戶端電腦進行檢查，其中Client Profile的功能類似於NAC（Network Access Control），不過用戶端電腦並不需要安裝代理程式，負責收集資訊，管理者只要在Web介面當中選取想要檢查的項目，就可以透過Client Profile檢查用戶端電腦是否有依照規定安裝所需的防護軟體，或者是系統修補程式。

除了Fortinet自家的Forti Client、Forti Firewall之外，FortiGate 224B也支援第三方廠商所推出的防護軟體，比方說，像是Sophos、趨勢等7家廠商的防毒軟體，以及Panda、F-Secure等6家廠商所推出的個人防火牆。

修補程式的部份以Service Pack為主，Windows 95之外的各種Windows版本，FortiGate 224B皆有支援，管理者可以在Client Profile的設定當中，限定只允許特定版本的Windows才能透過FortiGate 224B存取網路，否則便予以隔離，以防止網路上的安全威脅透過系統漏洞入侵到用戶端電腦。

至於Protection Profile則是FortiGate系列設備所一貫採用的安全設定檔，透過這項機制，可以因時制宜地使用不同的UTM功能，對用戶端提供安全防護。而在嚴謹和動態兩種模式的設定當中，我們也能將之前所設定好的Protection Profile匯入其中，過濾流量

當中的不當內容。

以虛擬連接埠面板顯示LAN埠使用狀態

如同大多數的FortiGate系列設備，在FortiGate 224B的Web介面的上方有一個模擬出來的連接埠面板，透過連接埠所顯示的顏色不同，讓管理者可以快速理解LAN埠目前的使用狀態，舉例來說，設置為嚴謹、動態模式的LAN埠以黃色表示，遭到隔離的LAN埠所使用的是紅色，至於未受到管理，且正常使用中的LAN埠，則用綠色來做表示。

在測試的過程之中，我們發現，雖然FortiGate 224B有提供正體中文的設定介面，不過當我們把選單切換成繁體中文之後，左側的Switch選項，以及下方的子選項，卻全部變成了null，文字顯示上並不正確，雖然還是可以點選進入，不過在使用上仍是稍嫌不便，關於這個問題，Fortinet表示，新版軟體目前已在製作當中，預計在第二季推出，屆時就會針對這個問題有所修正。

設置方式不同於一般的UTM設備

由於FortiGate 224B是一臺針對LAN埠實施控管的UTM設備，因此在設置上並不適合採取一般UTM設備的做法，也就是在後方串接交換器以延伸LAN埠的數量，原則上，一個LAN埠就只提供給一臺電腦上網使用，否則當其中一臺電腦因為違反設備的管理規則而遭到隔離，那麼連接在該臺交換器上的所有電腦也會一併遭到封鎖而無法存取網路。文◎楊啟倫



嚴謹與動態兩種模式也可以和VLAN、Secure Port混合使用，強化功能的使用彈性。

Fortinet FortiGate 224B	
建議售價：	599,500元
Fortinet	(02)2796-1666
尺寸	1U，19吋機架式
處理器	FortiASIC
軟體版本	FortiOS 3.0
網路介面	WAN埠：10/100×2，LAN埠：GbE×2、10/100×24，管理埠：10/100×1
防火牆效能	150Mbps
保固方式	隨機提供1年硬體、90天軟體保固