



如何做好

網站、Script、檔案下載、上傳 管制與防範

網路的發達，雖然讓資訊傳輸更加方便與迅速，但是相對的也衍生不少資安問題。例如：企業員工常常藉由上班時間瀏覽非法網站或是擷取公司網路頻寬下載影音檔案。企業老闆對員工這些行為，總是想不出一套完善的管制措施，想全部阻擋員工上網又怕影響企業營運狀況，最後通常只能睜一眼閉一眼，當作沒看見。

眾至提供一系列有效解決方案，利用 UTM 設備或防火牆設備「內容管制」功能，來做到對「網站」、「Script」、「檔案下載」與「檔案上傳」管制，讓公司網路可以有效充分利用。

範例一

如果想限定公司聯外網頁只開放 Google 可以連線，其他網頁都不能連線，該怎麼做呢？

步驟 1：眾至防火牆或 UTM 產品設備中有一項「內容管制」的功能，可以從「網站管制」設定。例如：

第一條：~google 或 ~tw.google.com

第二條：*

【符號說明：~ 表示開放 * 表示萬用字元】

這樣就只開放使用者只能上 Google 的網站，其他的網站都不能連線上去。

步驟 2：設定好條例之後，在到「管制條例」—「內部至外部設定」中新增一條管制條例，並套用至內容管制，則使用者只能連上 Google 網站。

註解：	(最多64個字元)
變更管制條例	
來源網路位址	Inside_Any
目的網路位址	Outside_Any
服務名稱	ANY
自動排程	None
認證名稱	None
VPN Trunk	None
管制動作_外部網路埠	<input checked="" type="checkbox"/> 允許,所有外部網路埠 <input type="checkbox"/> 拒絕,所有外部網路埠 <input type="checkbox"/> 外部網路埠1 <input type="checkbox"/> 外部網路埠2 <input type="checkbox"/> 外部網路埠3
流量監控	<input type="checkbox"/> 開啓
流量統計	<input type="checkbox"/> 開啓
IDP	<input type="checkbox"/> 開啓
內容管制	<input checked="" type="checkbox"/> URL <input type="checkbox"/> Script <input type="checkbox"/> Download <input type="checkbox"/> Upload
M / P2P 管制	None
病毒偵測	<input type="checkbox"/> HTTP / WebMail <input type="checkbox"/> FTP
頻寬管理	None
每個來源IP最大頻寬	下載頻寬 <input type="text" value="0"/> Kbps 上傳頻寬 <input type="text" value="0"/> Kbps (0: 表示不限制)
每個來源IP最多連線數	<input type="text" value="0"/> (範圍: 1 - 99999, 0: 表示不限制)
最多連線數	<input type="text" value="0"/> (範圍: 1 - 99999, 0: 表示不限制)
Quota Per Session	<input type="text" value="0"/> KBytes (範圍: 0 - 999999)
Quota Per Day	<input type="text" value="0"/> MBytes (範圍: 0 - 999999)

【新增 URL 管制條例】

範例二：

員工利用上班時間瀏覽股票交易，並利用網路下單，該如何管制？

利用眾至防火牆設備，將特定網站上的功能(如 java、cookie..)加以禁止，則使用者就無法瀏覽證券交易網站。

步驟 1：於防火牆設備中，「內容管制」功能中，勾選 Popup、ActiveX、Java、Cookie



【Popup、ActiveX、Java、Cookie 管制勾選】

步驟 2：在到【管制條例】之【內部至外部】功能中新增一條管制條例，並套用【內容管制】，就完成限制內部使用者透過管制條例存取網站之 Script 資料。



註解	(最多64個字元)
變更管制條例	
來源網路位址	Inside_Any
目的網路位址	Outside_Any
服務名稱	ANY
自動排程	None
認證名稱	None
VPN Trunk	None
管制動作,外部網路埠	<input checked="" type="checkbox"/> 允許,所有外部網路埠 <input type="checkbox"/> 拒絕,所有外部網路埠 <input type="checkbox"/> 外部網路埠1 <input type="checkbox"/> 外部網路埠2 <input type="checkbox"/> 外部網路埠3
流量監控	<input type="checkbox"/> 開啓
流量統計	<input type="checkbox"/> 開啓
IDP	<input type="checkbox"/> 開啓
內容管制	<input type="checkbox"/> URL <input checked="" type="checkbox"/> Script <input type="checkbox"/> Download <input type="checkbox"/> Upload
IM / P2P 管制	None
病毒偵測	<input type="checkbox"/> HTTP / WebMail <input type="checkbox"/> FTP
頻寬管理	None
每個來源IP最大頻寬	下載頻寬 0 Kbps 上傳頻寬 0 Kbps (0: 表示不限制)
每個來源IP最多連線數	0 (範圍: 1 - 99999, 0: 表示不限制)
最多連線數	0 (範圍: 1 - 99999, 0: 表示不限制)
Quota Per Session	0 KBytes (範圍: 0 - 999999)
Quota Per Day	0 MBytes (範圍: 0 - 999999)

【新增 Script 管制條例】

範例三：

企業員工利用公司網路頻寬，藉由 http、ftp 方式下載、上傳影片或歌曲，對於這些上傳下載行為該怎麼防範呢？

可以限制內部影音和特定副檔名，讓使用者無法藉由 http 或 ftp 方式下載。

步驟 1：不管是檔案下載或者是檔案上傳，只要在「內容管制」中，針對要管制影音與影像類型作選取。並於【管制條例】之【內部至外部】功能中新增一條管制條例，並套用之即可。

檔案下載

全部類型
 語音與影像類型

副檔名

<input type="checkbox"/> .exe	<input type="checkbox"/> .zip	<input type="checkbox"/> .rar
<input type="checkbox"/> .iso	<input type="checkbox"/> .bin	<input type="checkbox"/> .rpm
<input type="checkbox"/> .doc	<input type="checkbox"/> .xl?	<input type="checkbox"/> .ppt
<input type="checkbox"/> .pdf	<input type="checkbox"/> .tgz	<input type="checkbox"/> .gz
<input type="checkbox"/> .bat	<input type="checkbox"/> .dll	<input type="checkbox"/> .hta
<input type="checkbox"/> .scr	<input type="checkbox"/> .vb?	<input type="checkbox"/> .wps
<input type="checkbox"/> .pif	<input type="checkbox"/> .msi	<input type="checkbox"/> .com
<input type="checkbox"/> .reg	<input type="checkbox"/> .mp3	<input type="checkbox"/> .mpeg
<input type="checkbox"/> .mpg	<input type="checkbox"/> .wma	<input type="checkbox"/> .rmvb
<input type="checkbox"/> .rm	<input type="checkbox"/> .avi	<input type="checkbox"/> .wmv
<input type="checkbox"/> .3gp	<input type="checkbox"/> .mov	<input type="checkbox"/> .asf
<input type="checkbox"/> .mp4	<input type="checkbox"/> .amv	<input type="checkbox"/> .ram

確定 取消

【新增檔案下載管制功能選項】