當收到惡意URL情資時，如何加強UTM設定

近日，調查局資安工作站釋出一份情資，內容為其在偵辦的案件中追蹤到之駭客使用的惡意網域&IP位址，由於同時受駭的單位不少，因此提供各機關企業自我檢查並封鎖相關網域和網址。相信不少企業在看到這類消息時都會不知所措，該從哪項功能開始下手？有哪些功能是可以用來加強防護的？是不是有漏掉很重要的設定？等問題，本解決方案可協助使用者，完成所有設定防護流程。

首先，當我們接收到這類的資訊時，先將已知的黑名單加入設定中。

STEP 1.到【管理目標>URL管理>黑白名單設定】點選新增

（可選擇是否要啟用進階URL資料庫，NU系列皆內建一年授權。）

台中總公司 04-2705-0888
台中市西屯區西屯路二段256巷6號3F-6

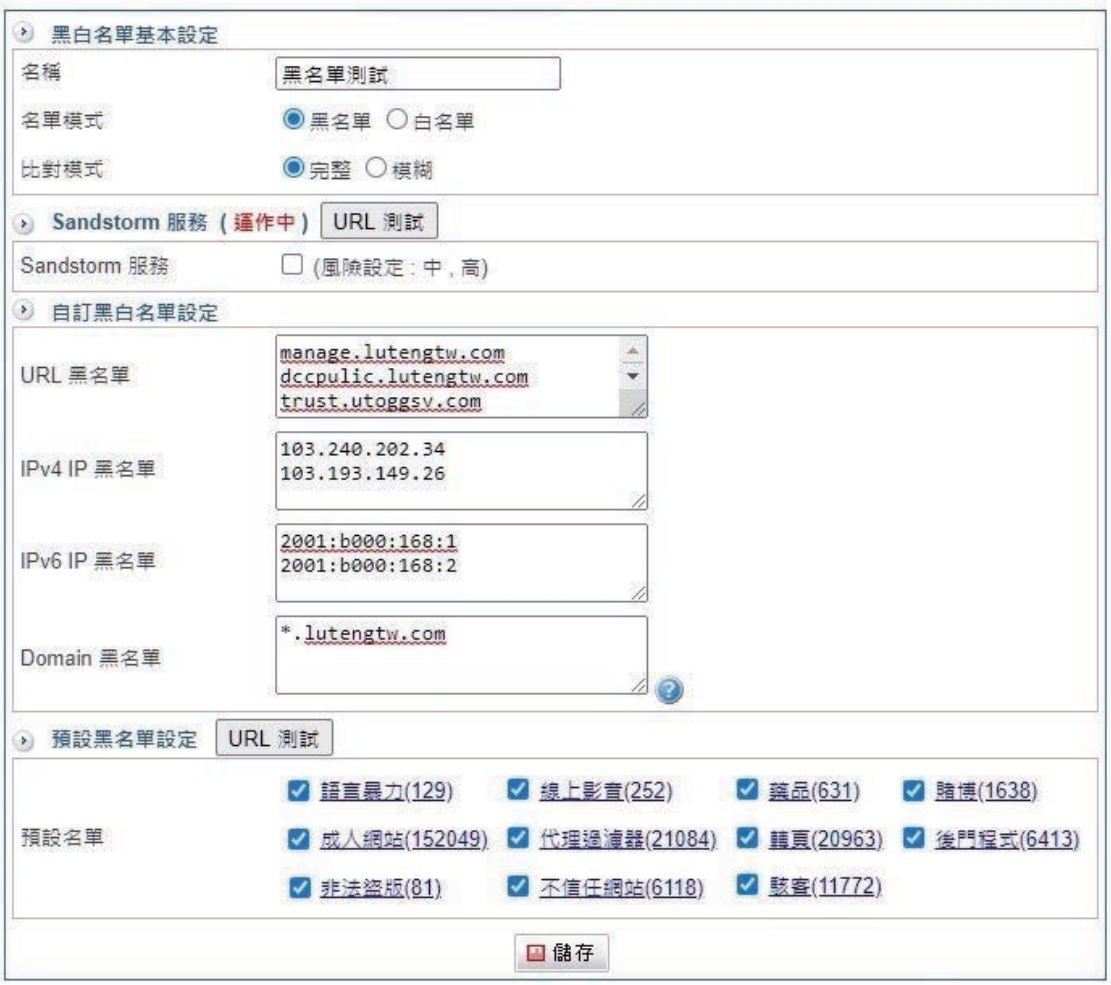
台北分公司 02-2501-1185
台北市中山區松江路129號6F-2

高雄分公司 07-229-8788
高雄市新興區民權一路251號8F-6

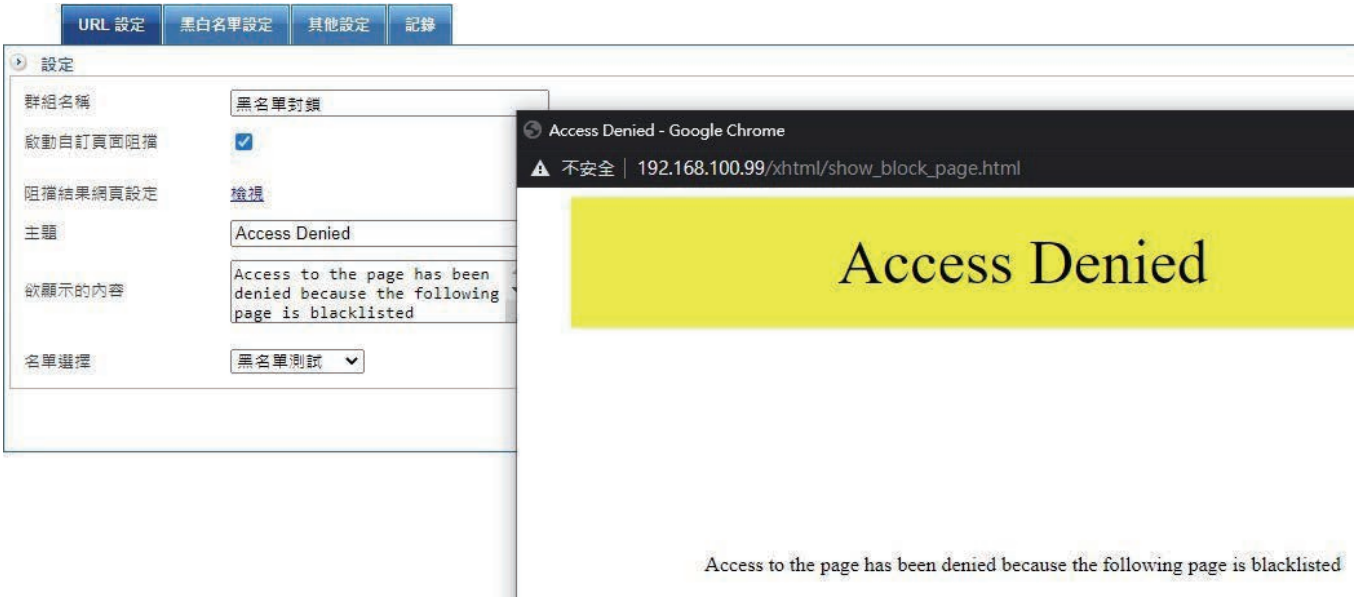
免付費專線 0800-666-188

官方網站 | www.sharetech.com.tw
銷售諮詢 | sales@sharetech.com.tw
技術支援 | help@sharetech.com.tw

STEP 2. 選擇需比對的【名單】與【模式】後，可手動輸入已知的惡意URL也可勾選內建的資料庫來使用。



STEP 3. 切換到分頁【URL設定】並套用剛才的設定；另外也可以自訂阻擋頁面，當觸發時就會出現以下的阻擋視窗畫面。



STEP 4. 最後到【管制條例>管制規則】中套用該設定即可。

其次，除了上述的黑名單設定外，眾至UTM也提供像是**IPS入侵偵測、防火牆功能、Sandstorm、WAF網頁防護、內網防護**等機制都可以幫助企業加強網路安全。（WAF網頁防護和內網防護在官網皆有更詳盡的文件解說，可至「客服專區>解決方案下載>UTM」中下載。）

IPS入侵偵測

能夠即時中斷或隔離具有傷害性的網路資料傳輸行為，針對Layer4-7的深層封包進行檢測； IPS管制設定分成基本&進階模式，兩種模式都將風險由低至高分成三類，企業只需要根據自身需求設定即可。此外，眾至提供特徵碼的定期免費更新。

IPS管制設定畫面

當收到惡意URL情資時，如何加強UTM設定

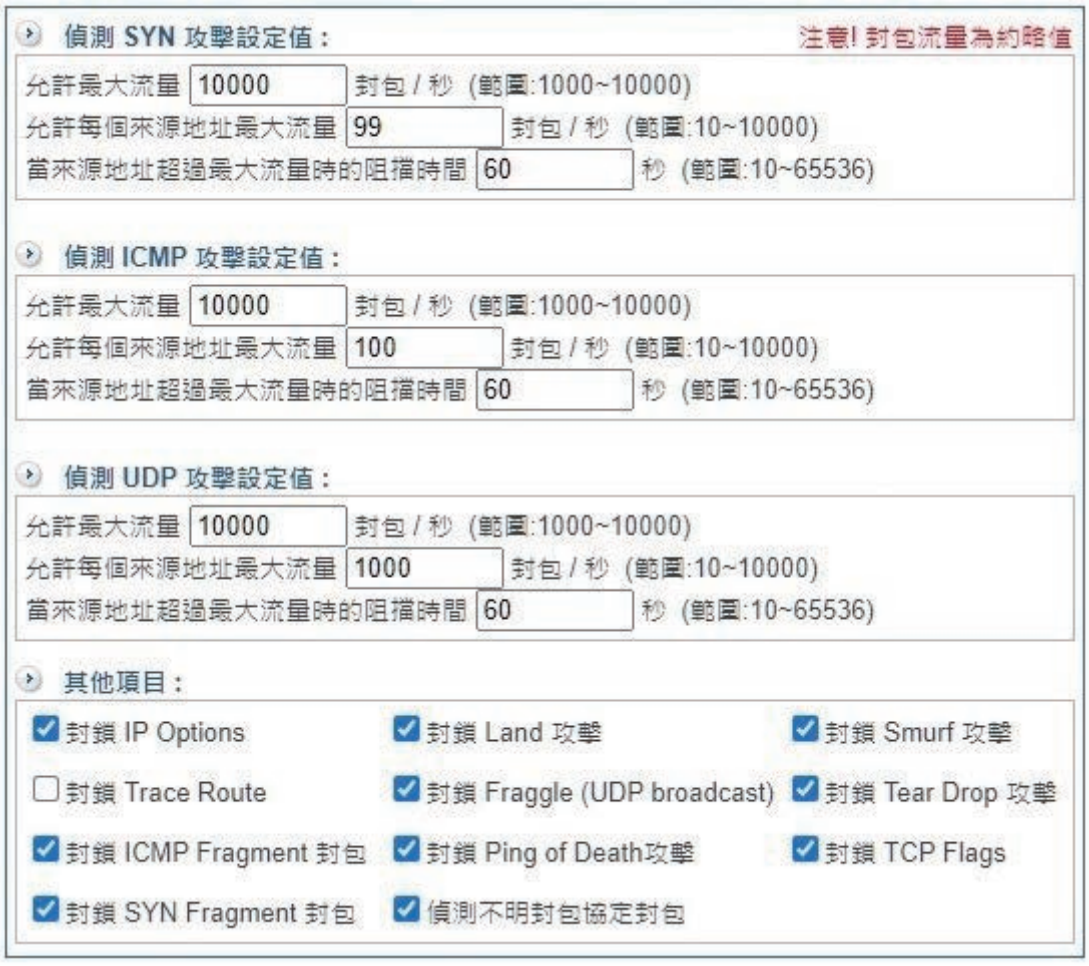
DNS filter

提供使用者的上網保護。當使用者查詢在DNS filter上設定的域名時，系統會代理回應0.0.0.0給使用者，如此一來使用者就無法進入，可避免誤觸網址。通常會搭配Sandstorm來做相關保護，因為Sandstorm上面的網址通常是惡意網站。

DNS filter設定畫面

防火牆功能

透過套用合理流量及連線數的概念，我們認為一台電腦不會同時產生過多的連線數，若超過合理的流量及連線數時，防火牆就會阻擋多餘的連線，並可主動攔截、阻擋駭客攻擊。調整SYN、ICMP&UDP協定的設定值後可在項目中設定是否封鎖其他常見的阻斷服務攻擊。



防火牆功能設定畫面

當收到惡意URL情資時，如何加強UTM設定

Sandstorm

Sandstorm有-- FILE Hash、Web URL& Domain可以分別做設定，並提供兩種類型的木馬程式掃描--檔案類型和網址類型。每一項目版本後面的括弧表示目前的木馬數量，和IPS一樣也歸類成高、中、低三種風險，如果怕誤擋，可以取消低風險的阻擋。

Sandstorm設定畫面