

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

當收到惡意URL情資時，如何加強UTM設定

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。

The screenshot shows the 'Blacklist Basic Settings' (黑白名單基本設定) section. The name is 'Blacklist Test' (黑名單測試). The list mode is 'Blacklist' (黑名單) and the comparison mode is 'Exact' (完整). The Sandstorm service is currently disabled. Under 'Custom Blacklist Settings' (自訂黑白名單設定), there are four input fields: 'URL Blacklist' (URL 黑名單) containing 'manage.lutengtw.com', 'dcccpublic.lutengtw.com', and 'trust.utoggsv.com'; 'IPv4 IP Blacklist' (IPv4 IP 黑名單) containing '103.240.202.34' and '103.193.149.26'; 'IPv6 IP Blacklist' (IPv6 IP 黑名單) containing '2001:b000:168:1' and '2001:b000:168:2'; and 'Domain Blacklist' (Domain 黑名單) containing '*.lutengtw.com'. The 'Predefined Blacklist Settings' (預設黑名單設定) section shows a grid of checkboxes for various categories, all of which are checked: 'Language Violence (129)', 'Online Scams (252)', 'Drugs (631)', 'Gambling (1638)', 'Adult Websites (152049)', 'Proxy Filters (21084)', 'Porn (20963)', 'Backdoors (6413)', 'Illegal Copies (81)', 'Untrusted Websites (6118)', and 'Spammers (11772)'. A 'Save' (儲存) button is at the bottom.

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。

The screenshot shows the 'URL Settings' (URL 設定) tab in the configuration interface. The 'Group Name' (群組名稱) is 'Blacklist Lock' (黑名單封鎖). The 'Enable Custom Page Blocking' (啟動自訂頁面阻擋) checkbox is checked. The 'Blocking Result Page Setting' (阻擋結果網頁設定) is 'Custom' (自訂). The 'Theme' (主題) is 'Access Denied'. The 'Content to Display' (欲顯示的內容) is 'Access to the page has been denied because the following page is blacklisted'. The 'List Selection' (名單選擇) is 'Blacklist Test' (黑名單測試). To the right, a browser window shows the 'Access Denied' page with a yellow background and the text 'Access Denied'. Below the browser window, the text 'Access to the page has been denied because the following page is blacklisted' is visible.

當收到惡意URL情資時，如何加強UTM設定

STEP 4. 最後到【管制條例>管制規則】中套用該設定即可。



進階設定

時間表	None ▾
頻寬管理	None ▾
應用程式管制	None ▾
每個來源IP能使用的最大連線數	0
上網認證	None ▾
電子白板	None ▾
URL 管制 ?	黑名單封鎖 ▾
IPS	None
DNS Filter	新增
	黑名單封鎖

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過濾設定

新增 IPS

群組名稱: Test

模式: 初階模式 進階模式

風險程度	記錄	阻擋
<input checked="" type="checkbox"/> High Risk (16496)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Medium Risk (1910)	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> Low Risk (652)	<input type="checkbox"/>	<input type="checkbox"/>

儲存

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 管制記錄

新增 DNS Filter :

群組名稱: DNS查詢惡意網站封鎖

Sandstorm 服務(運作中) (風險設定: 中,高)

完整比對: [Empty Input Field]

模糊比對: [Empty Input Field]

+ 新增

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。



偵測 SYN 攻擊設定值: 注意! 封包流量為約略值

允許最大流量: 10000 封包 / 秒 (範圍:1000~10000)

允許每個來源地址最大流量: 99 封包 / 秒 (範圍:10~10000)

當來源地址超過最大流量時的阻擋時間: 60 秒 (範圍:10~65536)

偵測 ICMP 攻擊設定值:

允許最大流量: 10000 封包 / 秒 (範圍:1000~10000)

允許每個來源地址最大流量: 100 封包 / 秒 (範圍:10~10000)

當來源地址超過最大流量時的阻擋時間: 60 秒 (範圍:10~65536)

偵測 UDP 攻擊設定值:

允許最大流量: 10000 封包 / 秒 (範圍:1000~10000)

允許每個來源地址最大流量: 1000 封包 / 秒 (範圍:10~10000)

當來源地址超過最大流量時的阻擋時間: 60 秒 (範圍:10~65536)

其他項目:

- 封鎖 IP Options
- 封鎖 Land 攻擊
- 封鎖 Smurf 攻擊
- 封鎖 Trace Route
- 封鎖 Fraggle (UDP broadcast)
- 封鎖 Tear Drop 攻擊
- 封鎖 ICMP Fragment 封包
- 封鎖 Ping of Death 攻擊
- 封鎖 TCP Flags
- 封鎖 SYN Fragment 封包
- 偵測不明封包協定封包

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。

The screenshot displays the Sandstorm configuration interface, organized into four main sections:

- Sandstorm (Main):** Includes a '雲端測試' (Cloud Test) button. Settings include: '啟動' (Enabled) checked; '啟用功能' (Enabled Features) with 'File Hash', 'Web URL', and 'Domain' all checked; '最後更新時間' (Last Update Time) as 2020-09-18 11:00:28.
- Domain (Domain測試):** Includes a 'Domain測試' (Domain Test) button. Settings include: '版本' (Version) 4.2009.1806 (69349); '風險程度' (Risk Level) with '低' (Low) unchecked and '中' (Medium) and '高' (High) checked; 'DNS' link pointing to '管理目標 > DNS Filter > DNS Filter'.
- File Hash (File Hash):** Settings include: '版本' (Version) 1.2009.1805 (240098); '風險程度' (Risk Level) with '低' (Low) unchecked and '中' (Medium) and '高' (High) checked; 'Web服務' (Web Services) link pointing to '網路服務 > WEB 服務'; '郵件服務' (Mail Services) link pointing to '郵件管理 > 郵件掃毒'.
- Web URL (Url測試):** Includes a 'Url測試' (Url Test) button. Settings include: '版本' (Version) 2.2009.1806 (760924); '風險程度' (Risk Level) with '低' (Low) unchecked and '中' (Medium) and '高' (High) checked; 'WEB 服務' (Web Services) link pointing to '管理目標 > URL 管理 > 黑白名單設定'; '郵件管理' (Mail Management) link pointing to '郵件管理 > 垃圾郵件過濾 > 郵件內文過濾'.

Sandstorm設定畫面