URL Filtering

阻止網路釣魚、憑證濫用以及命令與控制

網路本身就是最常見的網路攻擊來源

惡意網頁使員工在網路釣魚和憑證竊取、惡意軟體感染和勒索軟體的之間暴露。攻擊者使用自動化每天動態產生數千個新的惡意 URL，使獨立 Proxy 或網路篩選工具等傳統保護措施難以負荷。在識別、分類和防禦惡意網站所需的數分鐘內，感染可能已快速傳播而導致整個企業面臨風險。單點產品未與安全堆疊的其他部分相整合，這表示需要管理更多的政策集，而這可能會造成您無法迅速採用新的商業應用程式，同時需要額外的資源來進行維護。

商業優勢

- **消除安全隔閡，確保使用者安全。**作為新世代防火牆的原生元件，URL Filtering 為校園、分公司，或是行動使用者 (無論身在何處) 提供絕佳的網路安全性，藉以消除難以管理的傳統解決方案。
- **大幅減少營運支出。**URL Filtering 功能直接部署在您現有的網路流量政策中、簡化規則集，並精簡安全團隊的管理。
- **封鎖新的惡意網站。**URL Filtering 可以在數毫秒內對前所未見的惡意 URL 進行分類和封鎖，以防感染您的網路和最終使用者。
- **防禦已知的惡意網站。**保護企業免於遭受已知的網路型威脅，包括網路釣魚、惡意軟體、入侵套件和命令與控制 (C2)。
- **防止網路釣魚。**藉由即時阻止憑證網路釣魚的能力，多個層級的防禦措施可以保護企業免於遭受已知和全新網路釣魚網站的侵害。
- **支援合規性和可接受的使用。**確保企業遵守內部、業界和政府法規政策的合規性。

透過整合式防護支援安全網路存取

啟用安全的網頁存取需要原生整合的做法，透過可自動偵測、防禦和控制威脅且易於設定的網路控制，延伸您的新世代防火牆政策。除了直接允許及封鎖網站之外，Palo Alto Networks URL Filtering 也使用機器學習來識別和防禦內嵌的未知新攻擊，因此在使用者甚至尚未接觸威脅之前就予以封鎖。

該服務會分析 URL，並且將 URL 區分為良性或惡意，讓您可以在新世代防火牆政策中輕鬆地建立這些類別，全面掌控網路流量。這些類別可以觸發整個新世代防火牆平台的互補功能，因而實現附加層級的防護，例如目標 SSL 解密和進階日誌記錄。除了自身分析之外，URL Filtering 也使用 WildFire® 惡意軟體防禦服務和其他來源提供的共用威脅資訊，自動更新對於惡意網站的防護。

主要功能

機器學習式防禦

URL Filtering 訂閱能夠在使用者甚至尚未接觸新威脅之前就予以阻止。直接在您的機器學習式新世代防火牆上啟用機器學習功能，可以阻止前所未見的網路釣魚和內嵌的 JavaScript 攻擊，避免將這些威脅散播到企業中。這可以在惡意 URL 伺機感染企業之前立即識別並阻止惡意 URL。

全面控制網路內容

網路政策是防火牆政策的延伸。新世代防火牆使用 URL Filtering 識別 URL 類別、分配風險等級，並套用一致的政策。可以將多種 URL 類別和風險等級組合到更細緻的政策中，精確執行例外排除、簡化管理，並透過單一政策表精細控制網路流量。您可以封鎖可能在網路釣魚攻擊、入侵套件傳遞或 C2 中使用的危險網站，同時仍允許員工自由存取基於業務目所需的網路資源。

選擇性網路流量解密

針對性解密有助於您進一步降低風險。您可以建立政策，選擇將 TLS/SSL 加密網路流量解密，充分掌握潛在威脅，同時遵循數據隱私法規。特定 URL 類別 (例如社交網路，網路型電子郵件或內容傳遞網路) 可以指定為解密，而與其他類型網站 (例如政府、金融機構或醫療保健供應商) 之間進行的交易則可指定為維持加密。您可以實施簡易的政策，針對具有高度或中度風險等級的適用內容類別啟用解密。選擇性解密能夠維持最佳的安全狀況，同時遵守公司政策或外部法規設定的機密流量參數。

憑證網路釣魚防禦

即時保護使用者登入名稱和密碼。URL Filtering 會分析潛在的憑證網路釣魚頁面，識別這些頁面並阻止任何人透過「網路釣魚」URL 類別進行存取。URL Filtering 是一款業界首創的產品，能夠偵測並阻止進行中的網路釣魚攻擊，透過控制使用者可以依據網站的 URL 類別提交公司憑證的網站，藉以防禦憑證遭竊，完全達到零誤判的成效。您可以藉此阻止使用者向不受信任的網站提交憑證，同時仍然可以向公司網站和已獲批准的網站提交憑證。

可自訂類別

依據企業需求調整類別和政策。雖然 URL Filtering 會運用一組已定義的類別，但不同企業對於風險承受能力、合規性、規範或可接受的使用政策可能會有不同需求。為了符合企業需求並微調安全政策，管理員可結合多個現有的類別來建立各種新的自訂類別。例如，您可以結合「高風險」、「金融服務」和「新註冊的網域」類別來建立強大的新類別，當有任何網站符合這些條件時就能立即制定相關政策。

快取結果分析和翻譯網站篩選

持續加強控制常見政策迴避策略。即使攻擊使用了常見的迴避策略，例如快取結果和語言翻譯網站，仍可強制實施 URL Filtering 政策。這將透過以下程序完成：

- **搜尋引擎快取結果防禦：**當最終使用者嘗試檢視網路搜尋和網際網路封存的快取結果時，將套用 URL Filtering 政策。
- **翻譯網站篩選：**URL Filtering 政策將套用於在語言翻譯網站 (例如 Google Translate) 中作為規避政策輸入的 URL。

安全搜尋強制

為了嚴格控制搜尋結果，安全搜尋強制可防禦不當內容出現在使用者的搜尋結果中。此功能啟用時，僅允許安全搜尋選項設定為最嚴格的 Google、Yandex、Yahoo 或 Bing 搜尋，而其他所有搜尋均可封鎖。

可自訂的最終使用者通知

根據政策和相關的 URL Filtering 設定檔，對於如何通知使用者他們正嘗試造訪遭封鎖的網頁，每個企業採取不同的方法。管理員可透過自訂封鎖頁面通知使用者違規行為，包含使用者名稱和 IP 位址參考，以及使用者嘗試存取的 URL 和頁面的 URL 類別，並加上管理員的自訂訊息。

若要讓使用者重新取回網路活動的所有權，使用者嘗試存取有風險的頁面時，管理員有兩個選項：

- **繼續**顯示有「繼續」按鈕的自訂警告頁面。可以趁此時讓使用者瞭解其所要求的網站會造成的風險，並且讓使用者在認為可接受風險的情況下繼續進行。
- **覆蓋**會要求使用者正確輸入可設定的密碼，以便建立政策例外並繼續進行。這能夠讓使用者在獲得管理員核准的情況下存取可能重要的網站。

Palo Alto Networks 安全訂閱的功能

適用於網路安全性的進階防禦

如今，網路攻擊已利用進階技術規避網路安全裝置和工具，因此數量和複雜度日漸提升。企業需要在不增加安全團隊的工作負載且不影響業務生產力的情況下保護網路，這對於企業是一項挑戰。

我們的雲端交付安全訂閱與業界領先的新世代防火牆平台無縫整合，可協調情報並防範所有攻擊途徑，不僅提供絕佳的功能，而且消除不同的網路安全工具造成的涵蓋範圍落差。運用領先市場的功能和一致的平台體驗，使企業即使遭受最先進的迴避式攻擊也能獲得保護。

從 URL Filtering 或我們的任何安全訂閱中獲益：

- **Threat Prevention：**超越傳統的入侵防禦系統 (IPS)，可自動針對單一通道的所有流量防禦所有已知的威脅。
- **WildFire：**透過業界領先的雲端式分析，自動偵測及防禦未知的惡意軟體以確保檔案安全無虞。
- **DNS Security：**阻斷使用 DNS 進行 C2 或數據竊取的攻擊，而不需要變更任何基礎結構。
- **IoT Security：**藉由業界首款統包式物聯網安全解決方案，保護整個企業的物聯網 (IoT) 和 OT 裝置。
- **適用於端點的 GlobalProtect™ 網路安全性：**將新世代防火牆延伸至遠端使用者，可讓您在環境中的任何角落提供一致的 SaaS 安全性。

營運優勢

URL Filtering 訂閱可讓您：

- **情報共享的優點。**利用基於應用程式和使用者的易用政策，以及與 Threat Prevention 和 WildFire 的緊密整合，運用絕佳的網路安全性。
- **保持對網路流量的全面控制。**使用 URL 類別自動觸發進階安全操作，例如對可疑網站的選擇性 TLS/SSL 解密。
- **自動化您的安全性。**政策自動套用於 URL 類別，完全不需要分析人員介入。
- **瞭解使用者和 URL 活動。**IT 部門可透過一組預先定義或完全自訂的 URL Filtering 報告，取得 URL Filtering 和相關網路活動的可視性。

	URL Filtering	進階 URL Filtering
URL 篩選數據庫	✓	✓
機器學習式網路分類	✓	✓
信譽/風險等級	✓	✓
網域歷史記錄分析	✓	✓
多類別支援	✓	✓
準則比對	✓	✓
多種語言支援	✓	✓
所有新世代防火牆的自動更新	✓	✓
內嵌機器學習式 URL 分析	—	✓
對於惡意 URL 的內嵌即時防禦	—	✓
自我提升的 AI	—	✓
防迴避措施	—	✓

表 1：根據 URL 類別建立政策*	
政策	**描述**
選擇性 SSL	根據 URL 類別啟動 SSL 解密
憑證竊取	表明哪些網站可接收企業憑證，並封鎖、允許或警告使用者將憑證提交至未經授權的網站
封鎖高風險檔案類型	防止上傳/下載可執行檔或具潛在危險的檔案類型
更為嚴格的 IPS 設定檔	自動針對特定 URL 類別採用嚴格的弱點和反間諜軟體設定檔以封鎖網路釣魚套件、入侵套件以及伺服器和用戶端弱點
基於使用者的政策	允許企業中的特定群組存取某些 URL 類別，同時針對其他人封鎖這些類別

*除了簡單的封鎖惡意網站之外，您也可以使用 URL 類別來啟用精細安全政策以保護使用者，不致減緩其業務發展。

表 2：隱私權和授權摘要	
URL Filtering 訂閱的隱私權	
信任與隱私權	Palo Alto Networks 擁有嚴格的隱私權與安全性控制措施，以防止在未獲授權情況下存取機密或個人身分識別資訊。我們會套用業界標準的最佳實務提供安全性和機密性。您可在我們的隱私權型錄中找到進一步的資訊。
授權和要求	
要求	若要使用 Palo Alto Networks URL Filtering 訂閱，您需要： • 執行 PAN-OS 8.1 或更高版本的 Palo Alto Networks 新世代防火牆 • Palo Alto Networks Threat Prevention 授權
建議的環境	Palo Alto Networks 新世代防火牆部署在任何面向網際網路的位置，因為涉及網路釣魚、憑證竊取和 C2 的威脅需要外部連線。
URL Filtering 授權	URL Filtering 需要獨立的授權，並以整合的雲端式訂閱形式提供給 Palo Alto Networks 新世代防火牆。這也可以作為 Palo Alto Networks 訂閱 ELA、VM-Series ELA 或 Prisma Access 的一部分使用。

諮詢熱線：0800666326
網址：www.paloaltonetworks.tw
郵箱：contact_salesAPAC@paloaltonetworks.com

Palo Alto Networks 台灣代表處
11073 台北市信義區松仁路 100 號台北南山廣場 34 樓

parent_ds_url-filtering_051021