在安全網路裝置中阻止流量

目錄

簡介

本文檔介紹在安全網路裝置(SWA)中阻止流量的步驟。

必要條件

需求

思科建議您瞭解以下主題：

- SWA管理。

思科建議您：

- 已安裝物理或虛擬SWA。
- 對SWA圖形使用者介面(GUI)的管理訪問。

採用元件

本文件所述內容不限於特定軟體和硬體版本。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

阻塞流量

在SWA中阻止流量是確保網路安全、保持對內部策略的遵守以及防範惡意活動的關鍵步驟。以下是封鎖流量的一些常見原因：

按源阻止的原因

- 單個或多個使用者泛洪：當一個或多個使用者生成過多的流量時，網路可能會被淹沒，從而導致效能下降和潛在的服務中斷。
- 應用程式（使用者代理程式）的未信任資源存取：某些應用程式可能會嘗試存取未信任或可能有害的資源。阻止這些使用者代理有助於防止安全漏洞和資料洩漏。
- 限制特定IP範圍的Internet訪問：某些IP地址或範圍由於安全策略或為了防止未經授權的使用而可能需要限制其訪問Internet。
- 可疑的流量行為：必須阻止表現出異常模式或行為可能表明惡意活動或安全威脅的流量，以保護網路。

按目標阻止的原因

- 遵守公司內部政策：組織通常有限制訪問某些網站或線上資源的政策，以確保工作效率和遵守法律或法規要求。
- 不受信任的站點：阻止訪問被認為不可信或可能有害的網站，有助於保護使用者免受網路釣魚、惡意軟體和其他線上威脅的侵害。
- 惡意行為：必須阻止已知託管惡意內容或從事有害活動的網站，以防止安全事故和資料洩露。

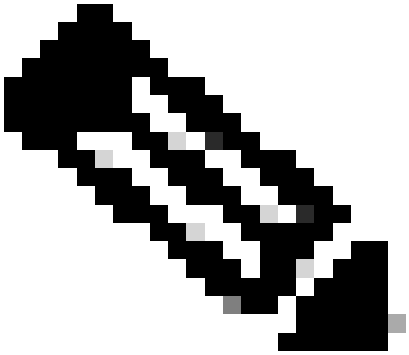
.

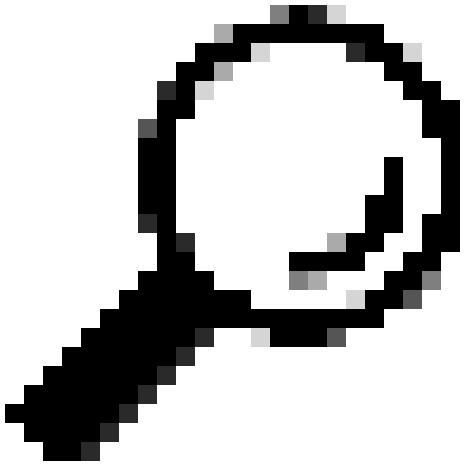
阻止流量的步驟

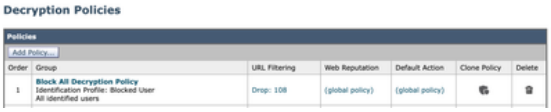
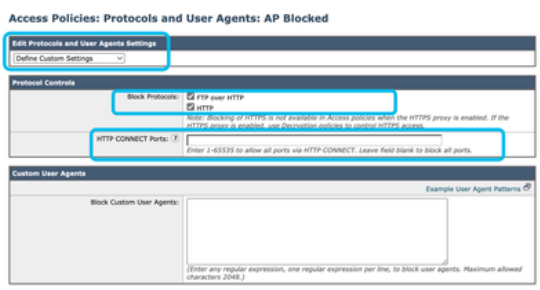
一般而言，在SWA中阻止流量需要三個主要階段：

- 為使用者建立標識配置檔案。
- 在解密策略中阻止HTTPS流量。
- 在Access Policy中阻止HTTP流量。

階段	阻止特定使用者訪問任何網站	阻止特定使用者訪問某些網站
自訂URL類別	不適用。	為您計畫阻止訪問的站點建立自定義URL類別。 有關詳情，請訪問： 在安全Web裝置中配置自定義URL類別-思科

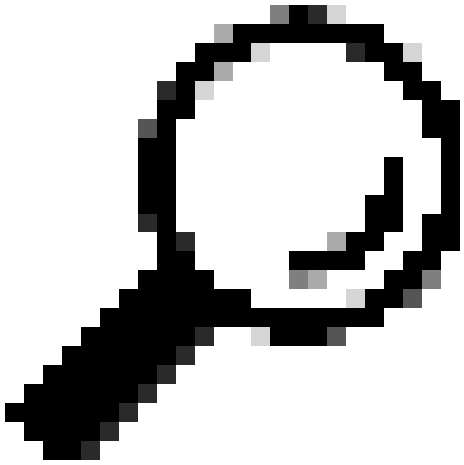
標識配置檔案	步驟 1.在GUI中，選擇網路安全管理器，然後按一下標識配置檔案。 步驟 2.按一下Add Profile以增加配置檔案。 步驟 3.使用Enable Identification Profile覈取方塊可啟用此配置檔案，或者快速停用此配置檔案而不刪除它。 步驟 4.指定唯一的設定檔名稱。 步驟5.（可選）增加說明。 步驟 6.從Insert Above下拉選單中，選擇此配置檔案在表中的顯示位置。 步驟 7. 在User Identification Method部分中，選擇Exempt from authentication/identication。 步驟 8.在Define Members by Subnet中，輸入此標識配置檔案必須應用的IP地址或子網。您可以使用IP地址、無類域間路由(CIDR)塊和子網。	 注意：要阻止所有使用者訪問某些網站，不需要建立單獨的ID配置檔案。這可以透過全局解密/訪問策略進行有效管理。 步驟 1.在GUI中，選擇網路安全管理器，然後按一下標識配置檔案。 步驟 2.按一下Add Profile以增加配置檔案。 步驟 3.使用Enable Identification Profile覈取方塊可啟用此配置檔案，或者快速停用此配置檔案而不刪除它。 步驟 4.指定唯一的設定檔名稱。 步驟5.（可選）增加說明。 步驟 6.從Insert Above下拉選單中，選擇此配置檔案在表中的顯示位置。 步驟 7. 在User Identification Method部分中，選擇Exempt from authentication/identication。 步驟 8.在Define Members by Subnet中，輸入此標識配置檔案必須應用的IP地址或子網。您可以使用IP地址、無類域間路由(CIDR)塊和子網。 步驟 9. 按一下高級，然後增加您要阻止訪問的URL類別。
解密策略	步驟 1.在GUI中，選擇Web Security Manager，然後按一下Decryption Policy。 步驟 2. 按一下Add Policy以增加解密策	步驟 1.在GUI中，選擇Web Security Manager，然後按一下Decryption Policy。 步驟 2. 按一下Add Policy以增加解密策

	略。 步驟 3.使用Enable Policy覈取方塊啟用此策略。 步驟 4.分配唯一的策略名稱。 步驟5.（可選）增加說明。 步驟 6.從Insert Above Policy下拉選單中，選擇第一個Policy。 步驟 7.從Identification Profiles and Users中，選擇您在前面的步驟中建立的標識配置檔案。 步驟 8.提交。 步驟 9.在解密策略頁的URL過濾下，按一下與此新解密策略關聯的連結。	略。 步驟 3.使用Enable Policy覈取方塊啟用此策略。 步驟 4.分配唯一的策略名稱。 步驟5.（可選）增加說明。 步驟 6.從Insert Above Policy下拉選單中，選擇第一個Policy。 步驟 7.從Identification Profiles and Users中，選擇您在前面的步驟中建立的標識配置檔案。 步驟 8.提交。 步驟 9. 在Decryption Policies 頁面的URL Filtering下，點選與此新解密策略關聯的連結。 步驟 10.選擇Drop作為為阻止的網站建立的自定義URL類別的操作。 步驟 11.按一下Submit。  影象-阻止解密策略中的某些URL
	 提示：假設您正在阻止所有URL類別，可以透過刪除自定義URL類別並僅使用預定義的URL類別來最佳化策略。這透過避免將URL與自定義URL類別進行匹配的額外步驟來減少SWA的處理負載。	
	步驟 10.選擇Drop作為每個URL類別的操作。 步驟 11. 在同一頁中，向下滾動到Unclassified URLs，並從下拉選單中選擇Drop。 步驟 12.提交。	

	 影象-用於阻止特定使用者的所有網站的解密策略	
訪問策略	步驟 1.在GUI中選擇網路安全管理器，然後按一下訪問策略。 步驟 2. 按一下Add Policy以增加訪問策略。 步驟 3.使用Enable Policy覈取方塊啟用此策略。 步驟 4.分配唯一的策略名稱。 步驟5.（可選）增加說明。 步驟 6.從Insert Above Policy下拉選單中，選擇第一個Policy。 步驟 7.從Identification Profiles and Users中，選擇您在前面的步驟中建立的標識配置檔案。 步驟 8.提交。 步驟 9.在訪問策略頁的協定和使用者代理下，按一下與此新訪問策略相關聯的連結。 步驟 10. 在Edit Protocols and User Agents Settings 下拉選單中選擇Define Custom Settings。 步驟 11.在 Block Protocols選擇 兩個核取方塊 FTP over HTTP和HTTP。 步驟 12.在 HTTP連線埠，刪除每個埠號以阻塞所有埠。  映像-訪問策略中的阻塞協定和連線埠	步驟 1.在GUI中選擇網路安全管理器，然後按一下訪問策略。 步驟 2. 按一下Add Policy以增加訪問策略。 步驟 3.使用Enable Policy覈取方塊啟用此策略。 步驟 4.分配唯一的策略名稱。 步驟5.（可選）增加說明。 步驟 6.從Insert Above Policy下拉選單中，選擇第一個Policy。 步驟 7.從Identification Profiles and Users中，選擇您在前面的步驟中建立的標識配置檔案。 步驟 8.提交。 步驟 9. 在訪問策略頁的URL過濾下，點選與此新訪問策略關聯的連結 第10步：選擇阻止作為為阻止的網站建立的自定義URL類別的操作。 步驟 11.提交。 步驟 12.提交更改。  圖-在訪問策略中阻止某些URL

步驟 13.提交。

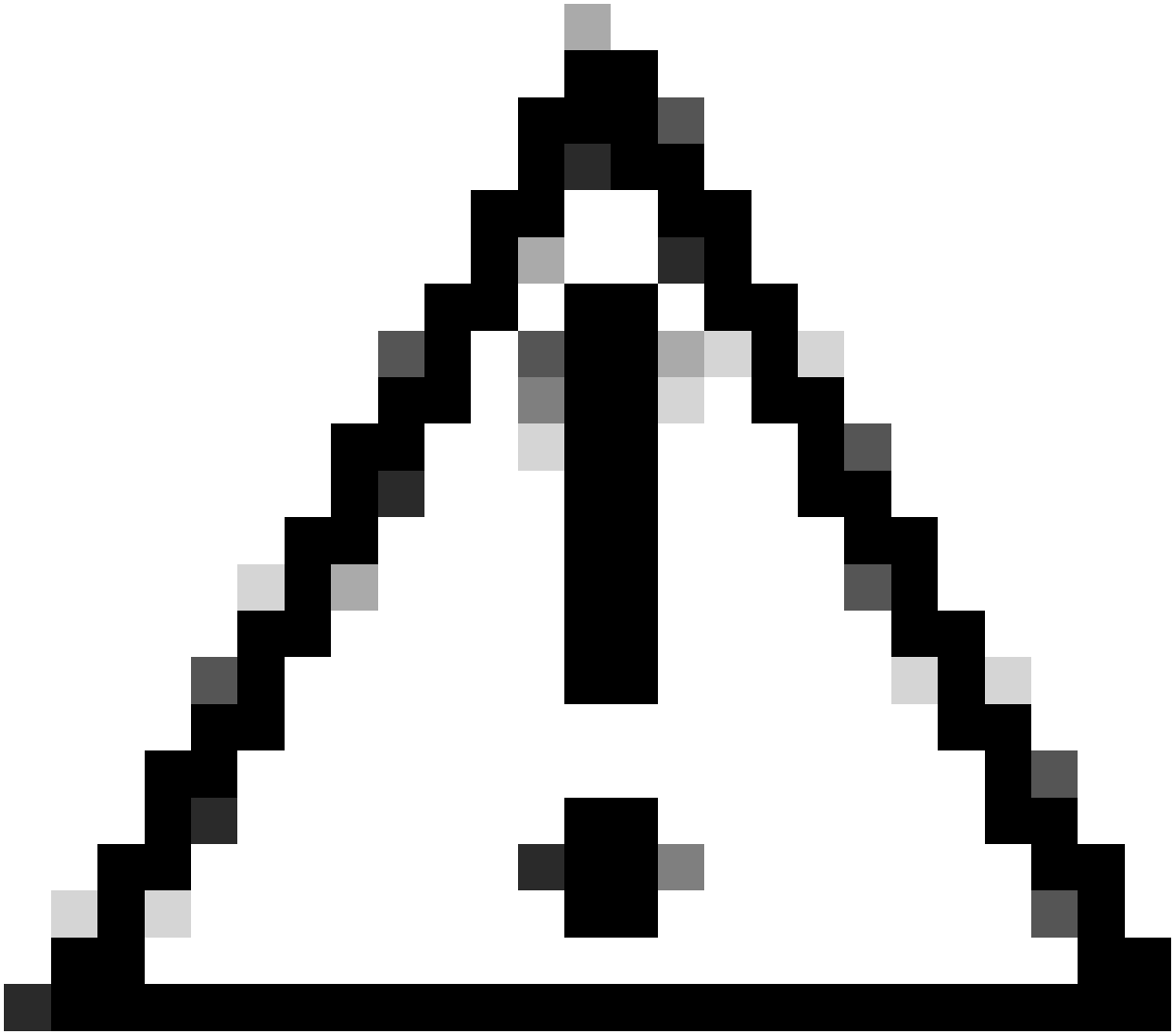
步驟14.（可選）在訪問策略頁的URL過濾下，點選與此新訪問策略關聯的連結，然後 選擇Block作為每個URL類別的操作，並且 未分類的URL，然後提交。



提示：假設您正在阻止所有URL類別，可以透過刪除自定義URL類別並僅使用預定義的URL類別來最佳化策略。這透過避免將URL與自定義URL類別進行匹配的額外步驟來減少SWA的處理負載。

步驟 16.提交更改。

映像-用於阻止所有站點的訪問策略



注意：在透明代理部署中，SWA無法讀取HTTPS流量的使用者代理或完整URL，除非流量被解密。因此，如果使用使用者代理配置標識配置檔案，或使用正規表示式配置自定義URL類別，此流量將無法與標識配置檔案匹配。

在透明代理部署中使用正規表示式阻止站點

在透明代理部署中，如果要阻止具有正規表示式條件的自定義URL類別（例如，阻止訪問某些YouTube頻道），可以使用以下步驟：

步驟 1.為主站點建立自定義URL類別。(在本示例中：YouTube.com)。

步驟 2.建立解密策略，分配此自定義URL類別，並將操作設定為解密。

步驟 3.建立訪問策略，將自定義URL類別指定為正規表示式（在本示例中，為YouTube通道指定自定義URL類別），並將操作設定為「阻止」。

相關資訊

- AsyncOS 15.0 for Cisco Secure Web Appliance使用手冊- GD（常規部署）-對終端使用者進行策略應用分類[Cisco Secure Web Appliance] -思科
- 在安全Web裝置中配置自定義URL類別-思科
- 如何在思科網路安全裝置(WSA)上免除Office 365流量身份驗證和解密-思科

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。