FireSIGHT系統上的URL過濾配置示例

目錄

簡介

本文檔介紹在FireSIGHT系統上配置URL過濾的步驟。FireSIGHT管理中心的URL過濾功能允許您在訪問控制規則中寫入條件，以便根據受監控主機的非加密URL請求確定穿越網路的流量。

必要條件

需求

本檔案對URL過濾授權和連線埠有一些特定需求。

URL過濾許可證的要求

FireSIGHT管理中心需要URL過濾許可證，以便定期與雲聯絡以更新URL資訊。您可以新增基於類別和信譽的URL條件到沒有URL過濾許可證的訪問控制規則；但是，在向FireSIGHT管理中心新增URL過濾許可證，然後在策略所針對的裝置上啟用該許可證之前，無法應用訪問控制策略。

如果URL過濾許可證過期，具有基於類別和基於信譽的URL條件的訪問控制規則將停止篩選URL，並且FireSIGHT管理中心不再聯絡雲服務。如果沒有URL過濾許可證，可以將單個URL或URL組設定為允許或阻止，但無法使用URL類別或信譽資料來過濾網路流量。

連線埠需求

FireSIGHT系統使用埠443/HTTPS和80/HTTP與雲服務通訊。埠443/HTTPS必須雙向開啟，並且必須在FireSIGHT管理中心上允許對埠80/HTTP的入站訪問。

採用元件

本檔案中的資訊是根據以下硬體和軟體版本：

- FirePOWER裝置：7000系列、8000系列
- 新世代入侵防禦系統(NGIPS)虛擬裝置
- 調適型安全裝置(ASA)FirePOWER
- Sourcefire軟體版本5.2或更新版本

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。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

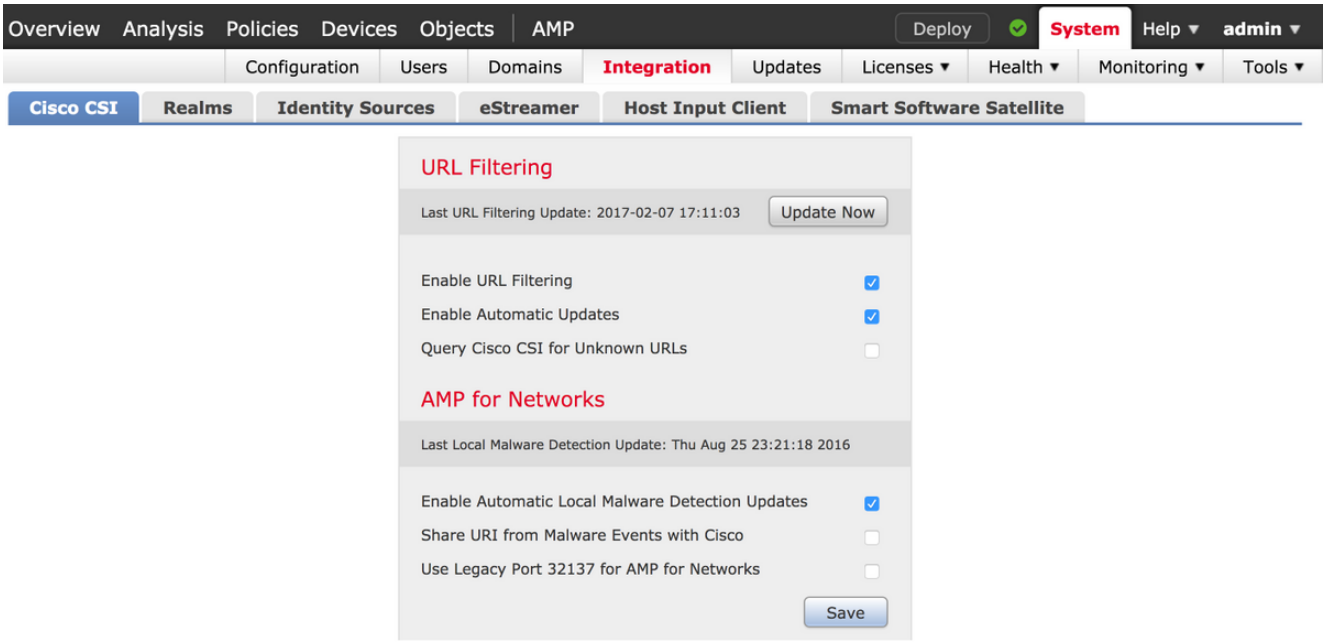
設定

在FireSIGHT管理中心上啟用URL篩選

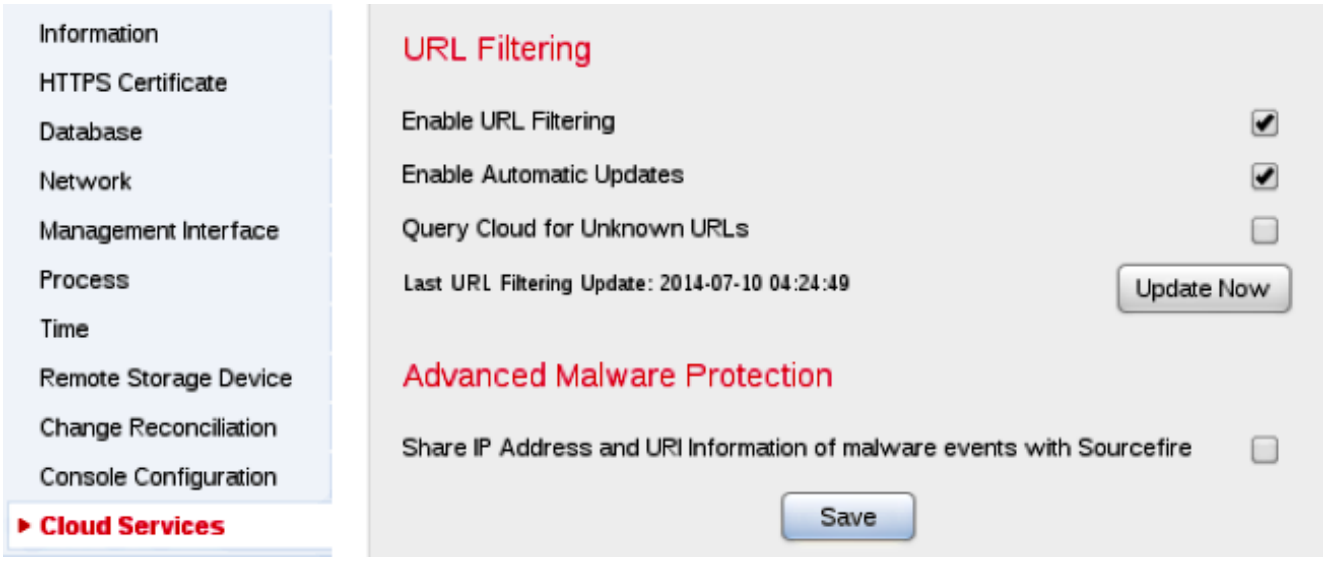
若要啟用URL篩選，請完成以下步驟：

1. 登入到FireSIGHT管理中心的Web使用者介面。
2. 根據您執行的軟體版本，導航方式會有所不同：

   在6.1.x版本上，選擇**System > Integration > Cisco CSI**。



   在5.x版本上，選擇**System > Local > Configuration**。選擇**Cloud Services**。



3. 勾選「**Enable URL Filtering**」覈取方塊以啟用URL篩選。
4. 或者，選中**Enable Automatic Updates**覈取方塊以啟用自動更新。此選項允許系統定期與雲服務聯絡，以獲取裝置本地資料集中URL資料的更新。

   附註：雖然雲服務通常每天更新一次資料，但如果您啟用自動更新，則會強制FireSIGHT管理中心每30分鐘檢查一次以確保資訊始終保持最新。雖然每日更新量通常較小，但如果自上次更新後超過5天，則下載新URL過濾資料可能需要長達20分鐘。下載更新後，執行更新本身可能需要30分鐘。

5. 或者，選中**Query Cloud for Unknown URLs**覈取方塊，以便針對未知URL查詢雲服務。當受監控網路上的某人嘗試瀏覽到不在本地資料集中的URL時，此選項允許系統查詢Sourcefire雲。如果雲不知道URL的類別或信譽，或者如果FireSIGHT管理中心無法聯絡雲，則URL與基於類別或信譽的URL條件不匹配訪問控制規則。

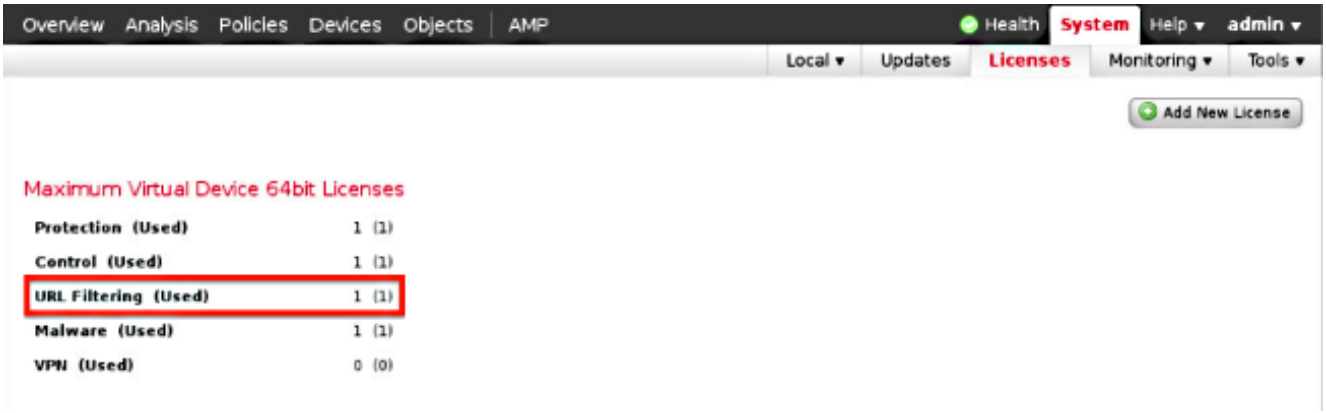
   附註：不能手動為URL分配類別或信譽。如果您不希望未分類的URL由Sourcefire雲分類（例如，出於隱私原因），請禁用此選項。

6. 按一下「**Save**」。URL過濾設定已儲存。

   附註：根據上次啟用URL過濾後的時間長度，或者如果這是第一次啟用URL過濾，FireSIGHT管理中心將從雲服務檢索URL過濾資料。

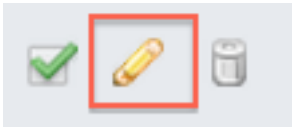
在受管裝置上應用URL過濾許可證

1. 檢查FireSIGHT管理中心上是否安裝了URL過濾許可證。若要尋找授權清單，請前往**System > Licenses**頁面。

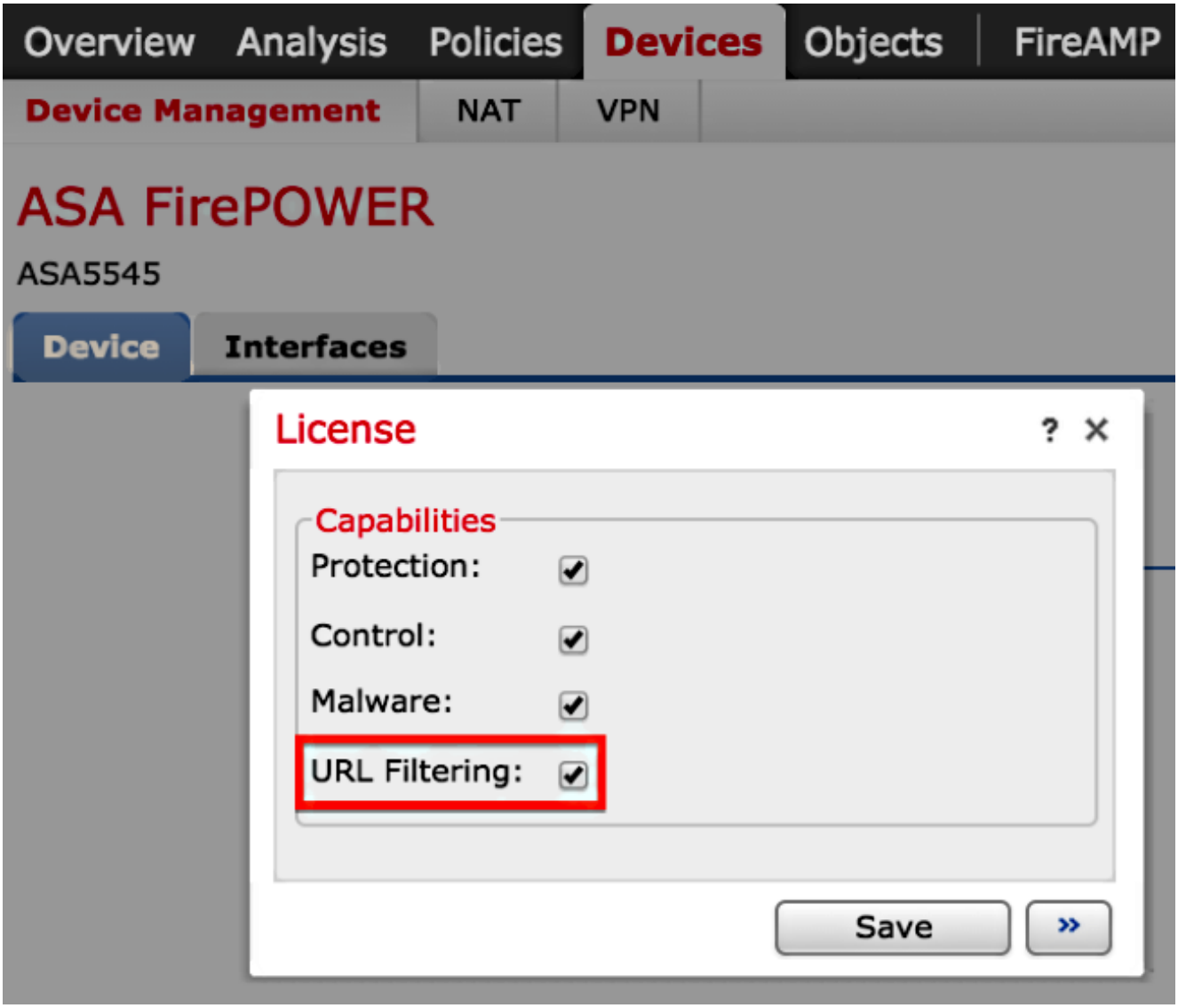


2. 轉到**Devices > Device Management**頁面，驗證在監控流量的裝置上是否應用了URL過濾許可證。

3. 如果未在裝置上應用URL過濾許可證，請按一下**鉛筆**圖示以編輯設定。圖示位於裝置名稱旁邊。



4. 您可以從**Devices**頁籤在裝置上啟用URL過濾許可證。



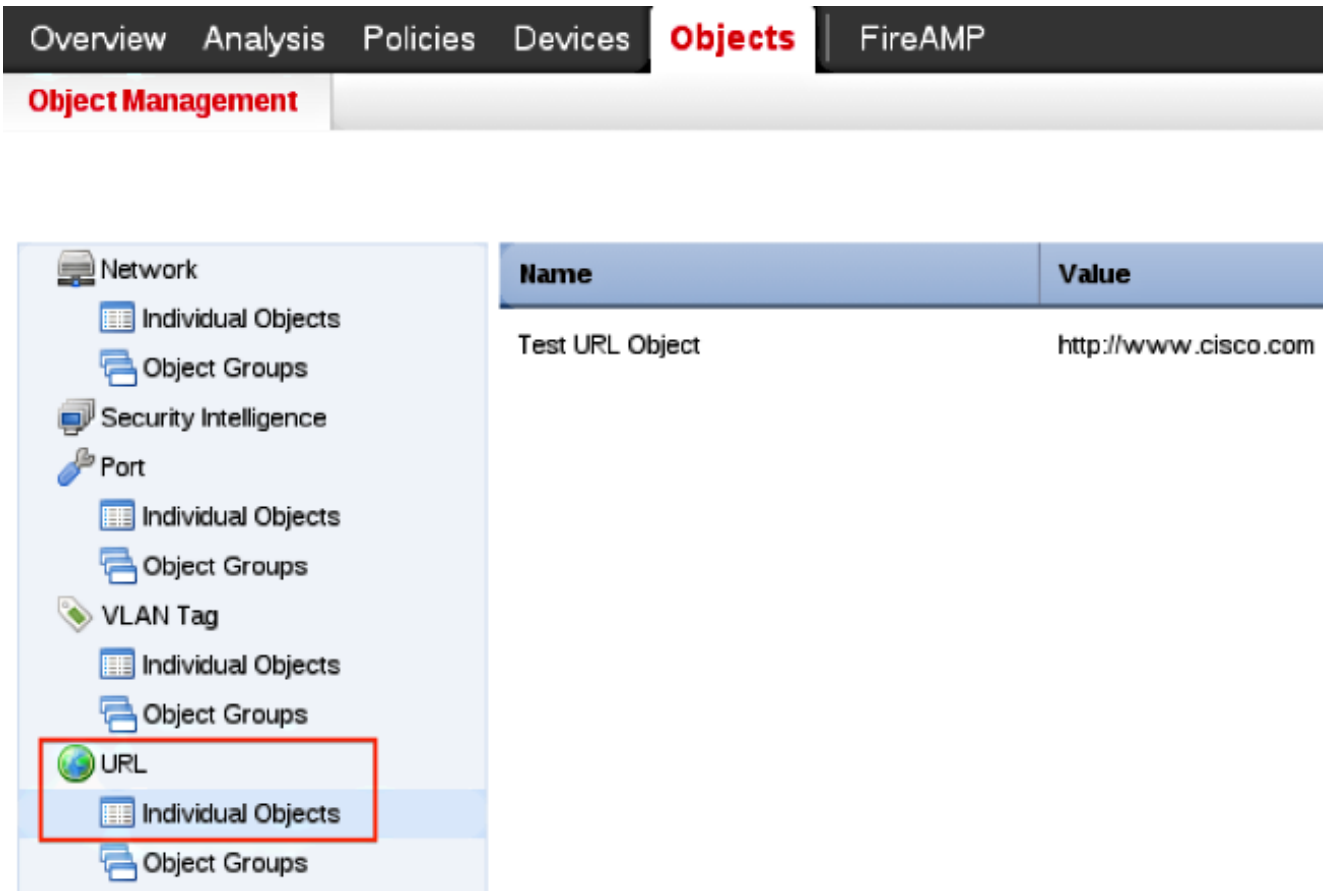
5. 啟用許可證並儲存更改後，還必須按一下**Apply Changes**以在受管裝置上應用許可證。

從阻止的URL類別中排除特定站點

FireSIGHT管理中心不允許您擁有本地的URL評級，該評級會覆蓋預設的Sourcefire提供的類別評級。為了完成此任務，必須使用訪問控制策略。以下說明介紹了如何在訪問控制規則中使用URL對象來從塊類別中排除特定站點。

1. 轉到**Objects > Object Management**頁。

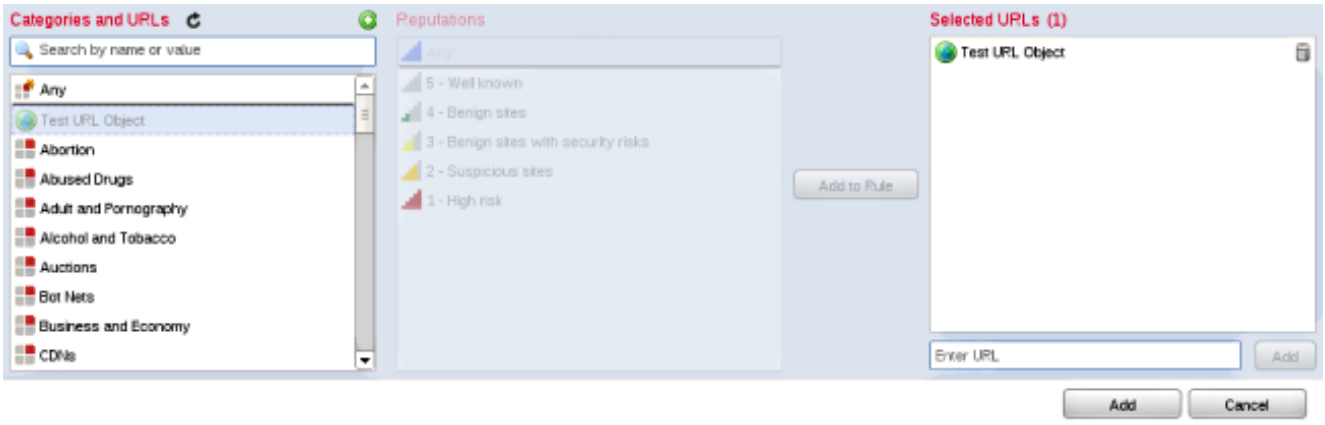
2. **選擇URL的**單個對象，然後單**擊Add URL按**鈕。出現「**URL Objects**」視窗。



3. 儲存更改後，選擇**Policies > Access Control**，然後按一下**鉛筆**圖示以編輯訪問控制策略。

4. 按一下「**Add Rule**」。

5. 使用**Allow**操作將URL對象新增到規則，並將其置於URL Category規則上方，以便首先評估其規則操作。



6. 新增規則後，按一下**儲存並應用**。它儲存新更改並將訪問控制策略應用於受控裝置。

驗證

有關「Verify or Troubleshoot information（驗證或故障排除）」的資訊，請參閱「Related Information（相關資訊）」部分中連結的**Troubleshoot Issue with URL Filtering on FireSIGHT System**（對FireSIGHT系統上的URL過濾進行故障排除）」文章。

疑難排解

有關驗證或故障排除資訊，請參閱 **疑難排解FireSIGHT系統上的URL過濾問題** 連結在「相關資訊」部分中的文章。

相關資訊

- **疑難排解FireSIGHT系統上的URL過濾問題**
- **技術支援與文件 - Cisco Systems**

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）。