IP地址被Cisco FireSIGHT系統的安全情報阻止或列入黑名單

目錄

簡介

安全情報功能允許您根據源或目標IP地址指定可以穿越網路的流量。如果要在訪問控制規則對流量進行分析之前將特定的IP地址列入黑名單（拒絕來往流量），這尤其有用。本檔案介紹如何處理Cisco FireSIGHT系統封鎖或將IP位址列入黑名單的情境。

必要條件

需求

思科建議您瞭解Cisco FireSIGHT管理中心。

採用元件

本檔案中的資訊是根據以下硬體和軟體版本：

- Cisco FireSIGHT管理中心
- Cisco Firepower裝置
- 具備Firepower(SFR)模組的Cisco ASA
- 軟體版本5.2或更高版本

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。

情報源與情報清單之間的區別

在FireSIGHT系統中使用安全情報功能的方法有兩種：

安全情報源

安全情報源是防禦中心從HTTP或HTTPS伺服器下載的IP地址的動態集合。為了幫助您構建黑名單，思科提供了*安全情報源*，它代表漏洞研究團隊(VRT)確定為信譽不佳的IP地址。

安全情報清單

與源相比，安全情報清單是手動上傳到FireSIGHT管理中心的簡單IP地址靜態清單。

合法IP地址被阻止或被列入黑名單

驗證IP地址是否在安全情報源中

如果IP地址被安全情報源黑名單阻止，您可以按照以下步驟進行驗證：

第1步：訪問Firepower裝置或服務模組的CLI。

第2步：運行以下命令。將<IP_Address>替換為要搜尋的IP地址：

```
admin@Firepower:~$ grep
```

例如，如果要搜尋IP地址198.51.100.1，請運行以下命令：

```
admin@Firepower:~$ grep 198.51.100.1 /var/sf/iprep_download/*.blf
```

如果此命令返回您提供的IP地址的任何匹配項，則表示該IP地址存在於安全情報源黑名單中。

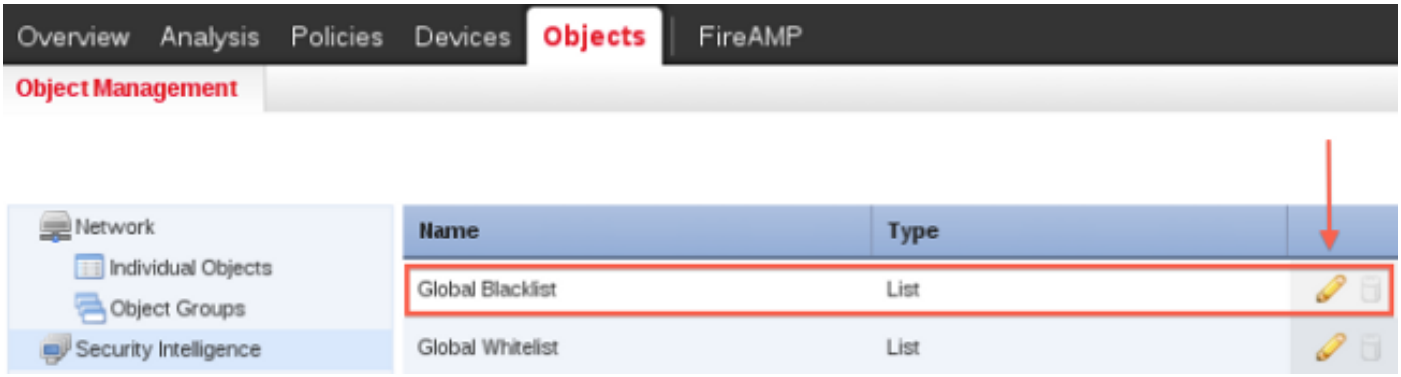
檢查黑名單

要查詢可能列入黑名單的IP地址清單，請執行以下步驟：

第1步：訪問FireSIGHT管理中心的網路介面。

第2步：導航到**對象>對象管理>安全情報**。

步驟3:按一下鉛筆圖示*以開啟*或編輯「全域性黑名單」(Global Blacklist)。系統將顯示一個彈出視窗，其中包含IP地址清單。



使用被阻止或列入黑名單的IP地址

如果特定IP地址被Security Intelligence Feed阻止或列入黑名單，則可以考慮使用以下任何選項來允許它。

選項1:安全情報白名單

可以將安全情報列入黑名單的IP地址列入白名單。白名單會覆蓋其黑名單。FireSIGHT系統使用訪問控制規則評估具有列入白名單的源IP地址或目標IP地址的流量，即使一個IP地址也被列入黑名單。因此，當黑名單仍然有用，但範圍過廣，並且錯誤地阻止要檢查的流量時，可以使用白名單。

例如，如果信譽良好的源錯誤地阻止了您對重要資源的訪問，但總體上對您的組織很有用，則您可以僅將不適當分類的IP地址列入白名單，而不用從黑名單中刪除整個源。

> **注意**：對訪問控制策略進行任何更改後，必須將策略重新應用於受管裝置。

選項2:按安全區域實施安全情報過濾器

為了增加粒度，您可以根據連線中的源IP地址或目標IP地址是否位於特定安全區域來實施安全情報過濾。

要擴展上述白名單示例，您可以將分類不當的IP地址列入白名單，然後使用您的組織中需要訪問這些IP地址的人員使用的安全區域限制白名單對象。這樣，只有有業務需要的使用者才能訪問列入白名單的IP地址。另一個示例是，您可能希望使用第三方垃圾郵件源將電子郵件伺服器安全區域上的流量列入黑名單。

選項3:監控，而不是黑名單

如果您不確定要將特定IP地址或一組地址列入黑名單，可以使用「僅監控」設定，該設定允許系統向訪問控制規則傳遞匹配的連線，但也會將匹配項記錄到黑名單。請注意，無法將全域性黑名單設定為僅監控

請考慮以下情況：在使用該源實施阻止之前要測試第三方源。將饋送設定為僅監控時，系統允許系統進一步分析原本會阻塞的連線，但也會記錄每個連線的記錄以供評估。

使用「僅監控」設定配置安全情報的步驟：

1. 在訪問控制策略的**Security Intelligence**頁籤上，按一下日誌記錄圖示。系統將顯示Blacklist Options對話方塊。

2. 選中Log Connections覈取方塊以在流量滿足安全情報條件時記錄連線開始事件。
3. 指定傳送連線事件的位置。
4. 按一下OK以設定日誌記錄選項。系統將再次顯示Security Intelligence頁籤。
5. 按一下「Save」。您必須應用訪問控制策略才能使更改生效。

選項4:聯絡思科技術支援中心

在以下情況下，您可以隨時聯絡思科技術支援中心：

- 您對上述選項1、2或3有問題。
- 您希望對安全情報列入黑名單的IP地址進行進一步研究和分析。
- 您需要解釋IP地址為何被安全情報列入黑名單。