排除FireSIGHT系統上的URL過濾問題

目錄

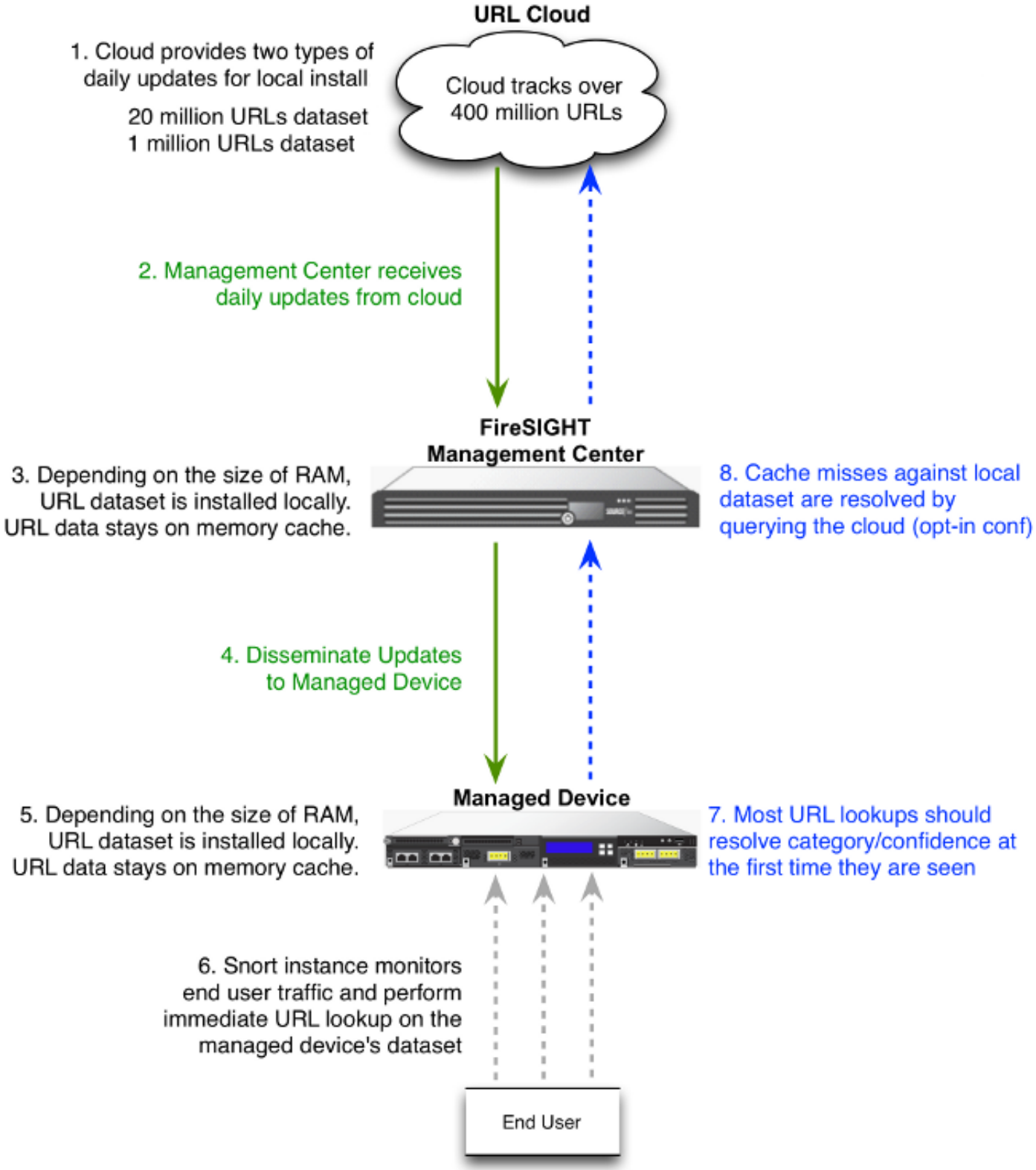
簡介

本檔案將說明URL過濾的常見問題。FireSIGHT管理中心的URL過濾功能可對受監控主機的流量進行分類，並允許您根據信譽在訪問控制規則中寫入條件。

URL過濾查詢過程

為了加速URL查詢過程，URL過濾提供本地安裝在Firepower系統上的資料集。根據裝置上可用的記憶體(RAM)量，有兩種型別的資料集：

資料集型別	記憶體要求 5.3版	在5.4或更高版本上
2000萬個URL資料集	>2GB	>3.4 GB
100萬個URL資料集	<= 2GB	<= 3.4 GB



雲連線問題

第1步：檢查許可證

是否安裝了許可證？

您可以在沒有URL過濾許可證的情況下將類別和基於信譽的URL條件新增到訪問控制規則，但是，在首先將URL過濾許可證新增到FireSIGHT管理中心，然後在策略所針對的裝置上啟用該許可證之前，不能應用訪問控制策略。

許可證是否已過期？

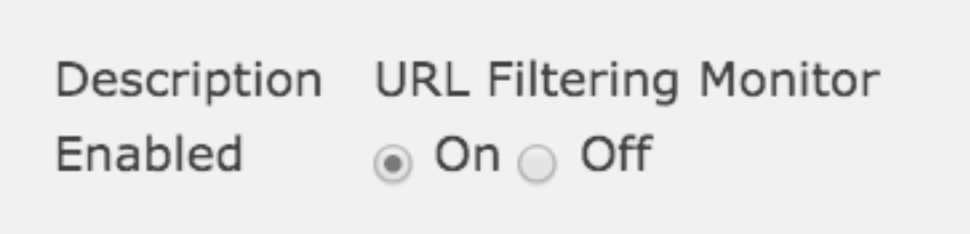
如果URL過濾許可證過期，具有基於類別和基於信譽的URL條件的訪問控制規則將停止篩選URL，並且FireSIGHT管理中心不再聯絡雲服務。

> **提示：**閱讀FireSIGHT系統上的URL過濾配置示例，以瞭解如何在FireSIGHT系統上啟用URL過濾功能並在受管裝置上應用URL過濾許可證。

第2步：檢查運行狀況警報

URL過濾監控模組跟蹤FireSIGHT管理中心與思科雲之間的通訊，在該雲中，系統獲取常見訪問URL的URL過濾（類別和信譽）資料。URL過濾監視器模組還跟蹤FireSIGHT管理中心與您已啟用URL過濾的任何受管裝置之間的通訊。

要啟用URL過濾監視器模組，請轉到**運行狀況策略配置**頁面，選擇**URL過濾監視器**。按一下**Enabled**選項的**On**單選按鈕，以便允許使用模組進行運行狀況測試。如果要使設定生效，必須將運行狀況策略應用到FireSIGHT管理中心。



- **嚴重警報**：如果FireSIGHT管理中心未能與雲成功通訊或從雲中檢索更新，則該模組的狀態分類將更改為*嚴重*。
- **警告警報**:如果FireSIGHT管理中心成功與雲通訊，如果管理中心無法將新的URL過濾資料推送到其受管裝置，則模組狀態將更改為*警告*。

步驟3:檢查DNS設定

FireSIGHT管理中心在雲查詢期間與這些伺服器通訊：

```
database.brightcloud.com
service.brightcloud.com
```

確保防火牆上允許兩台伺服器後，在FireSIGHT管理中心運行以下命令，並驗證管理中心是否能夠解析名稱：

```
admin@FireSIGHT:~$ sudo nslookup database.brightcloud.com

admin@FireSIGHT:~$ sudo nslookup service.brightcloud.com
```

第4步：檢查與所需埠的連線

FireSIGHT系統使用埠443/HTTPS和80/HTTP與雲服務通訊。

確認管理中心能夠成功執行nslookup後，使用telnet檢驗到埠80和埠443的連線。URL資料庫通過database.brightcloud.com（埠443）下載，而未知URL查詢通過service.brightcloud.com（埠

80）完成。

```
telnet database.brightcloud.com 443
telnet service.brightcloud.com 80
```

以下輸出是一個成功連線到database.brightcloud.com的telnet連線示例。

```
Connected to database.brightcloud.com.
Escape character is '^]'.
```

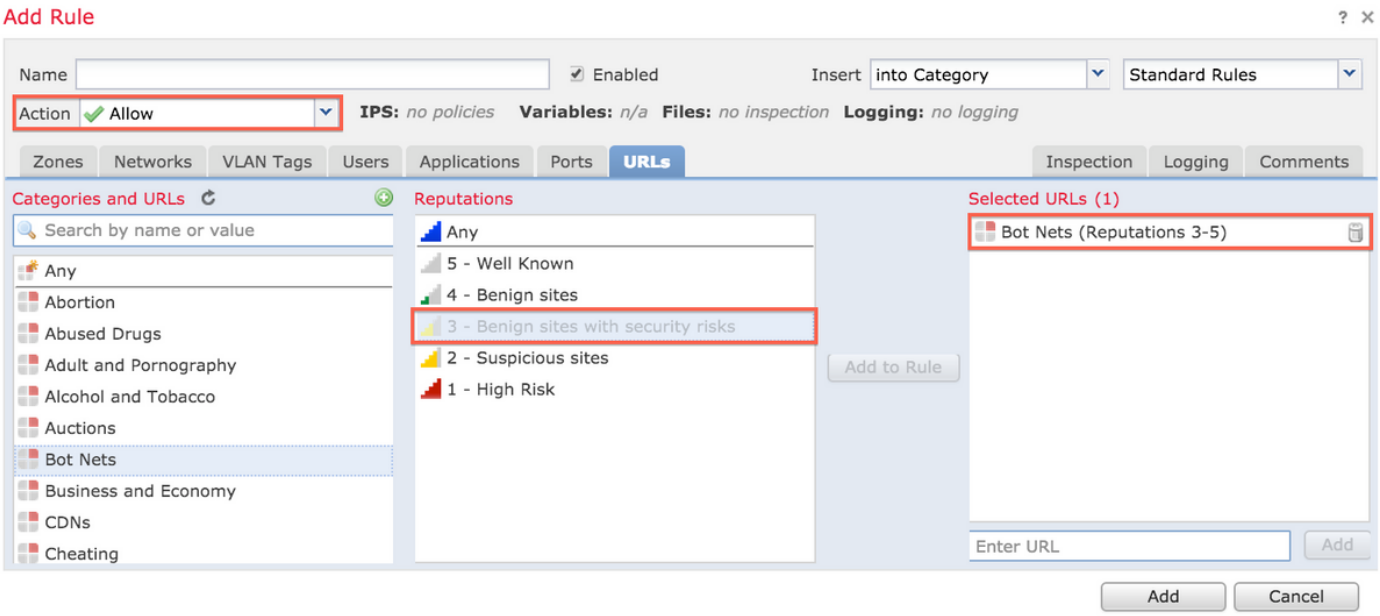
存取控制與錯誤分類問題

問題1:允許/阻止具有未選擇信譽級別的URL

如果您注意到某個URL被允許或阻止，但您沒有在訪問控制規則中選擇該URL的信譽級別，請閱讀本節以瞭解URL過濾規則的工作原理。

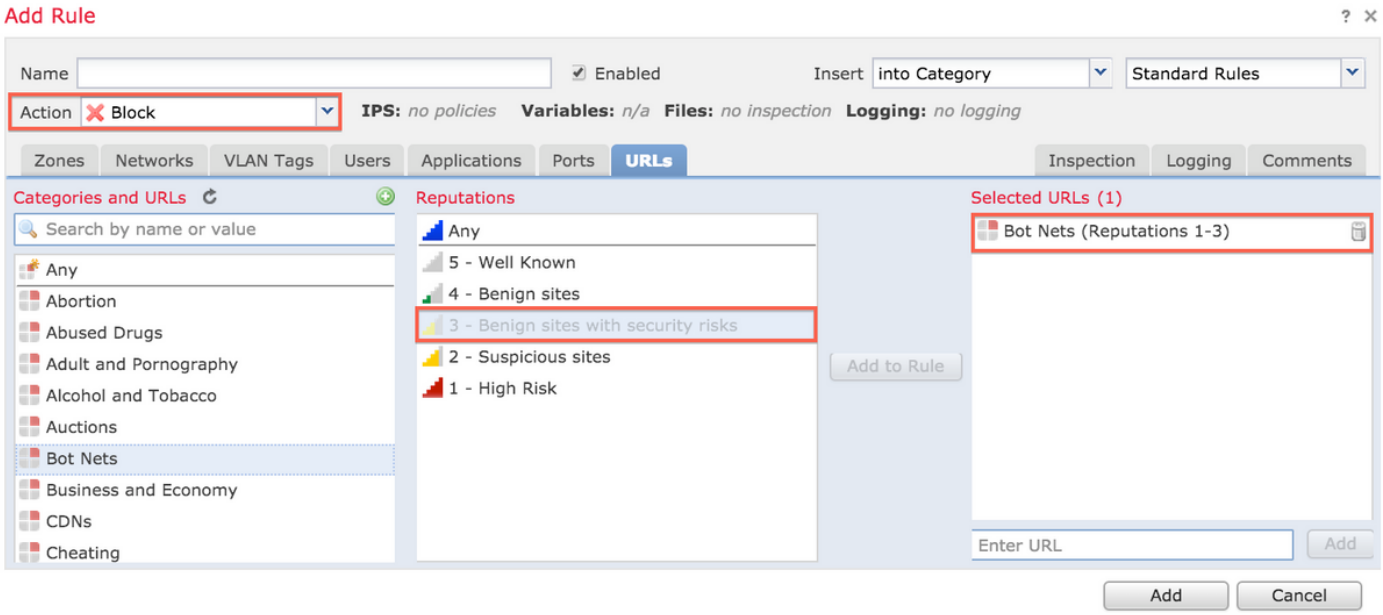
Rule Action is Allow

當您建立規則以**Allow** traffic based on a reputation level時，選擇信譽級別還會選擇所有比您最初選擇的級別更不安全的信譽級別。例如，如果將規則配置為允許*Benign sites with security risks*(level 3)，它也會自動允許*Benign sites*(level 4)和*Known*(level 5)站點。



規則操作為阻止

當您根據信譽級別建立規則**Block**流量時，選擇信譽級別還會選擇比最初選擇的級別更嚴重的所有信譽級別。例如，如果將規則配置為阻止存在安全風險(第3級)的*Benign Sites，則它也會自動阻止Suspicious sites*（第2級）和*High risk*（第1級）站點。



URL選擇矩陣

所選信譽級別

1 — 高風險
2 — 可疑站點
3 — 存在安全風險的良性站點
4 — 良性站點
5 — 已知

所選規則操作
高風險 可疑站點 有安全風險的良性站點 良性站點 廣為人知

問題2:萬用字元在訪問控制規則中不起作用

FireSIGHT系統不支援在URL條件中指定萬用字元。此情況可能無法在cisco.com上發出警報。

```
*cisco*.com
```

此外，不完整的URL可能會與其他流量匹配，從而導致意外結果。在URL條件中指定單個URL時，必須仔細考慮可能受影響的其他流量。例如，請考慮想要明確封鎖cisco.com的情境。但是，子字串匹配意味著阻止cisco.com也會阻止sanfrancisco.com，這可能不是您的本意。

輸入URL時，輸入域名並忽略子域資訊。例如，輸入cisco.com而不是 www.cisco.com。在 Allow規則中使用 cisco.com時，使用者可以瀏覽到以下任何URL:

```
http://cisco.com
http://cisco.com/newcisco
http://www.cisco.com
```

問題3:URL類別和信譽未填充

如果URL不在本地資料庫中，並且它是第一次在流量中看到該URL，則可能無法填充類別或信譽。這表示首次看到未知URL時，它與AC規則不匹配。 有時，在第一次看到URL時，針對常訪問的URL的URL查詢可能無法解析。此問題已在版本5.3.0.3、5.3.1.2和5.4.0.2、5.4.1.1中修正。

相關資訊

- FireSIGHT系統上的URL過濾配置
- 技術支援與文件 - Cisco Systems