

在Cisco Firepower系統上配置通過規則

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[設定](#)

[建立通行規則](#)

[啟用通行規則](#)

[驗證](#)

[疑難排解](#)

簡介

本文檔介紹通過規則、如何建立該規則以及如何在入侵策略中啟用該規則。

您可以建立傳遞規則以防止符合傳遞規則中定義的條件的資料包在特定情況下觸發警報規則，而不是禁用警報規則。預設情況下，通過規則覆蓋警報規則。Firepower系統將資料包與每個規則中指定的條件進行比較，如果資料包資料與規則中指定的所有條件匹配，則觸發規則。如果規則是警報規則，則會生成入侵事件。如果是通行規則，則會忽略流量。

例如，您可能希望將查詢以使用者「anonymous」身份登入FTP伺服器的嘗試的規則保持活動狀態。但是，如果您的網路有一個或多個合法的匿名FTP伺服器，則可以編寫並啟用通行規則，指定對於這些特定伺服器，匿名使用者不會觸發原始規則。

注意：當傳遞規則基於的原始規則收到修訂時，傳遞規則不會自動更新。因此，通行證規則可能難以維護。

附註：如果為規則啟用「抑制」功能，則它會抑制該規則的事件通知。但是，仍然會評估規則。例如，如果抑制丟棄規則，則匹配該規則的資料包將被靜默丟棄。

必要條件

需求

本文件沒有特定需求。

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。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

設定

建立通行規則

1. 導航到 **Objects > Intrusion Rules**。系統將顯示規則類別清單。
2. 查詢與要篩選的規則關聯的規則類別。使用箭頭圖示從類別清單中展開規則類別，並查詢要為其建立傳遞規則的規則。或者，您可以使用規則搜尋框。
3. 找到所需規則後，按一下其旁邊的鉛筆圖示以編輯規則。
4. 編輯規則時，請完成以下步驟：點選與規則對應的 **Edit** 按鈕。在「操作」(Action) 下拉選單中，選擇 **pass**。將 Source IPs 欄位和 Destination IPs 欄位更改為不希望規則發出警報的主機或網路。按一下「**Save As New**」。

Edit Rule 3:13921:5 [\(View Documentation, Rule Comment\)](#)

Message:

Classification: [Edit Classifications](#)

Action: (circled in red)

Protocol:

Direction:

Source IPs: Source Port:

Destination IPs: Destination Port:

Detection Options


reference

reference

reference

metadata

5. 記下新規則的ID號。例如1000000。

 **Success** ✕
Successfully created new rule "IMAP Altrium Software MERCUR IMAPD NTLMSSP command handling memory corruption attempt"

Edit Rule 3:1000000:1 [\(View Documentation, Rule Comment\)](#)

Message:

Classification: ▼
[Edit Classifications](#)

Action: ▼

Protocol: ▼

Direction: ▼

Source IPs: Source Port:

Destination IPs: Destination Port:

Detection Options

reference

reference

reference

metadata

▼

啟用通行規則

您需要在相應的入侵策略中啟用新規則，以便在指定的源或目標地址上傳遞流量。按照以下步驟啟用通過規則：

1. 修改活動入侵策略：導航到**Policies > Access Control > Intrusion**。點選活動入侵策略旁邊的**Edit**。
2. 將新規則新增到規則清單：按一下左側窗格中的**Rules**。在過濾器框中輸入您之前註明的Rule ID。選中Rules覈取方塊，並將Rule State更改為**Generate Events**。按一下左側窗格中的**Policy Information**。按一下**Commit Changes**。

3. 按一下**Deploy**以在裝置上部署更改。

驗證

您應該監視新事件一段時間，以確保沒有為定義的源IP地址或目標IP地址的此特定規則生成事件。

疑難排解

目前尚無適用於此組態的具體疑難排解資訊。