瞭解FirePOWER裝置上的規則擴展

目錄

[簡介](#)
[必要條件](#)
[需求](#)
[採用元件](#)
[背景資訊](#)
[瞭解規則擴展](#)
[擴展基於IP的規則](#)
[使用自定義URL擴展基於IP的規則](#)
[使用埠擴展基於IP的規則](#)
[使用VLAN擴展基於IP的規則](#)
[擴展具有URL類別的基於IP的規則](#)
[擴展帶區域的IP規則](#)
[規則展開的一般公式](#)
[排除由於規則擴展導致的部署故障](#)
[相關資訊](#)

簡介

本文檔介紹從Firepower管理中心(FMC)部署訪問控制規則到感測器的轉換。

必要條件

需求

思科建議您瞭解以下主題：

- Firepower技術知識
- 有關在FMC上配置訪問控制策略的知識

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Firepower管理中心版本6.0.0及更高版本
- 運行軟體版本6.0.1及更高版本的ASA Firepower防禦映像(ASA 5515-X、ASA 5525-X、ASA 5545-X、ASA 5555-X、ASA 5585-X)
- 運行軟體版本6.0.0及更高版本的ASA Firepower SFR映像(ASA 5515-X、ASA 5525-X、ASA 5545-X、ASA 5555-X、ASA 5585-X)

- Firepower 7000/8000系列感測器6.0.0版及更高版本

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。

背景資訊

使用以下引數的一個或多個組合建立訪問控制規則：

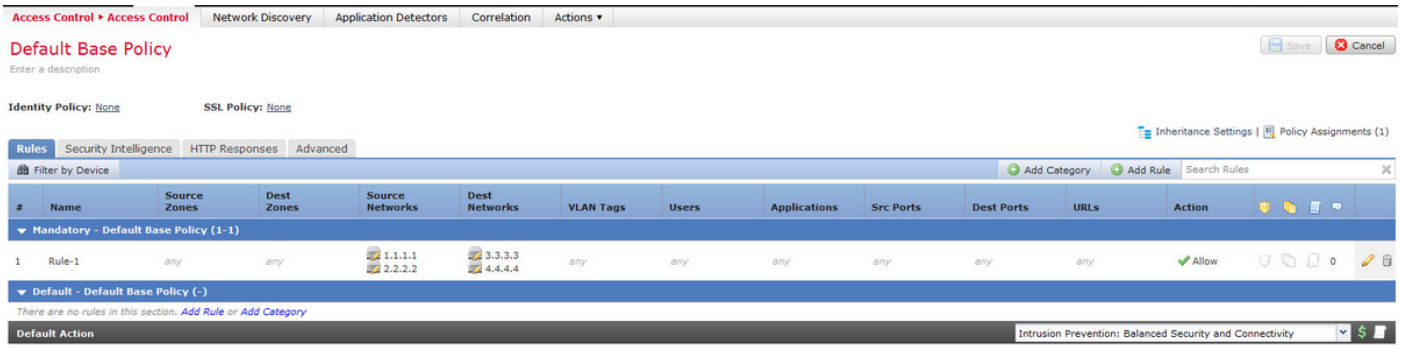
- IP地址（源和目標）
- 連線埠（來源和目的地）
- URL（系統提供的類別和自定義URL）
- 應用檢測器
- VLAN
- 區域

根據訪問規則中使用的參陣列合，感測器上的規則擴展將發生變化。本文檔重點介紹了FMC上的各種規則組合以及感測器上各自的關聯擴展。

瞭解規則擴展

擴展基於IP的規則

考慮從FMC配置訪問規則，如下圖所示：



這是管理中心上的一個規則。但是，將其部署到感測器後，它將擴展為**四個**規則，如下圖所示：

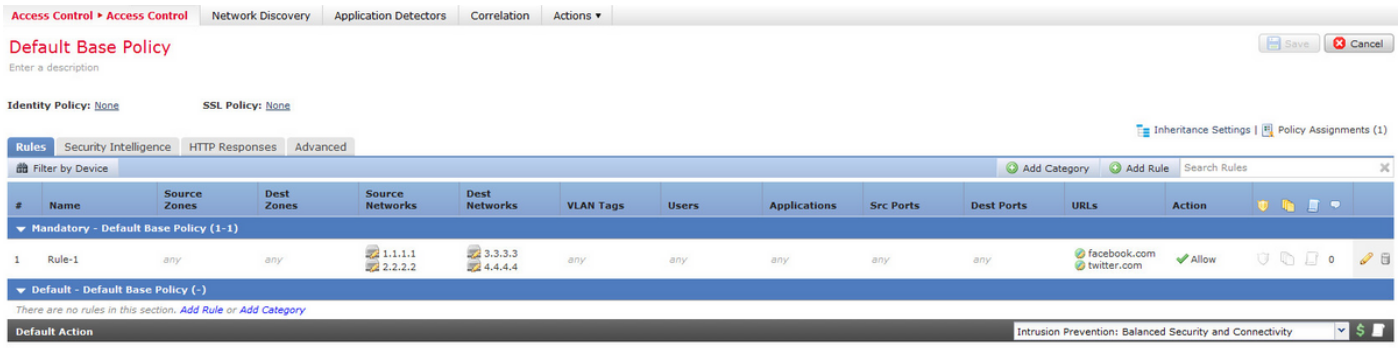
```
268436480 allow any 1.1.1.1 32 any any 3.3.3.3 32 any any any  (log dcforward flowstart)
268436480 allow any 1.1.1.1 32 any any 4.4.4.4 32 any any any  (log dcforward flowstart)
268436480 allow any 2.2.2.2 32 any any 3.3.3.3 32 any any any  (log dcforward flowstart)
268436480 allow any 2.2.2.2 32 any any 4.4.4.4 32 any any any  (log dcforward flowstart)
268435456 allow any any  any any any  any any any  (ipspolicy 2)
```

部署一個規則時，將兩個子網配置為源，兩個主機配置為目標地址，此規則將擴展為感測器上的四個規則。

> **附註**：如果要求基於目標網路阻止訪問，則執行此操作的更好方法是使用安全情報下的黑名單功能。

使用自定義URL擴展基於IP的規則

考慮從FMC配置訪問規則，如下圖所示：



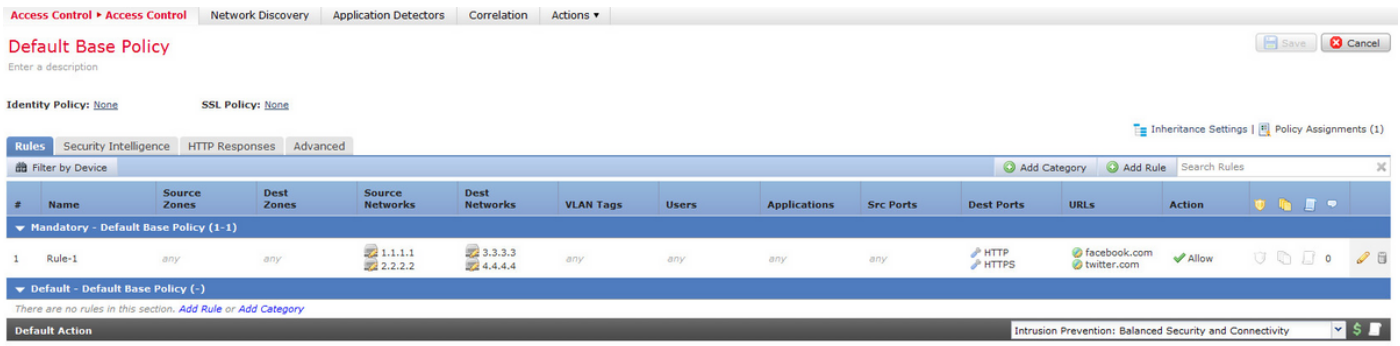
這是管理中心上的一個規則。但是，將其部署到感測器後，將擴展為八個規則，如下圖所示：

```
268436480 allow any 1.1.1.1 32 any any 3.3.3.3 32 any any any  (log dcforward flowstart) (url
"facebook.com")
268436480 allow any 1.1.1.1 32 any any 3.3.3.3 32 any any any  (log dcforward flowstart) (url
"twitter.com")
268436480 allow any 1.1.1.1 32 any any 4.4.4.4 32 any any any  (log dcforward flowstart) (url
"facebook.com")
268436480 allow any 1.1.1.1 32 any any 4.4.4.4 32 any any any  (log dcforward flowstart) (url
"twitter.com")
268436480 allow any 2.2.2.2 32 any any 3.3.3.3 32 any any any  (log dcforward flowstart) (url
"facebook.com")
268436480 allow any 2.2.2.2 32 any any 3.3.3.3 32 any any any  (log dcforward flowstart) (url
"twitter.com")
268436480 allow any 2.2.2.2 32 any any 4.4.4.4 32 any any any  (log dcforward flowstart) (url
"facebook.com")
268436480 allow any 2.2.2.2 32 any any 4.4.4.4 32 any any any  (log dcforward flowstart) (url
"twitter.com")
268435456 allow any any  any any any  any any any  (ipspolicy 2)
```

部署一個規則時，如果兩個子網配置為源，兩個主機配置為目標地址，兩個自定義URL對象位於管理中心的單個規則中，則此規則將擴展到感測器上的八個規則。這表示每個自訂URL類別都有一個來源和目的地IP/連線埠範圍的組合，會設定和建立。

使用埠擴展基於IP的規則

考慮從FMC配置訪問規則，如下圖所示：



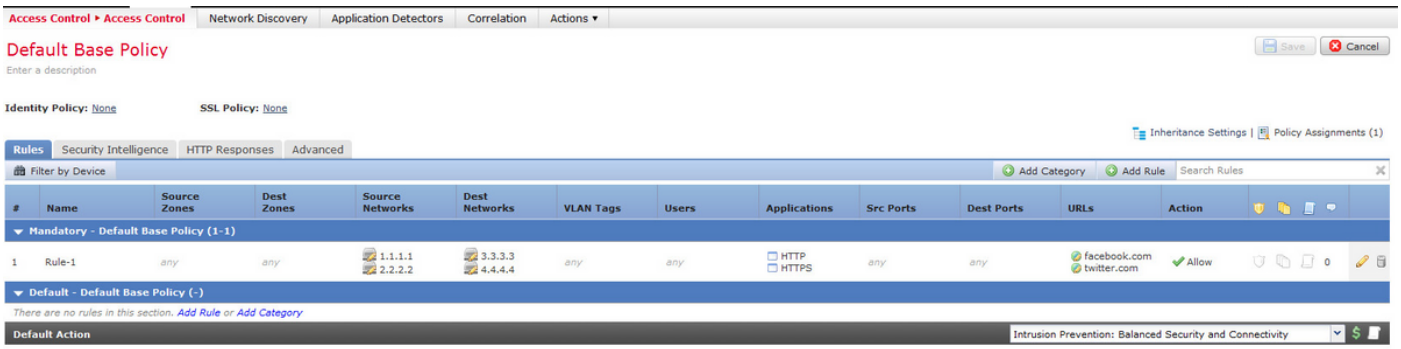
這是管理中心上的一個規則。但是，將其部署到感測器後，將擴展為十六個規則，如下圖所示：

```
268436480 allow any 1.1.1.1 32 any any 3.3.3.3 32 80 any 6 (log dcforward flowstart) (url
"facebook.com")
268436480 allow any 1.1.1.1 32 any any 3.3.3.3 32 80 any 6 (log dcforward flowstart) (url
"twitter.com")
268436480 allow any 1.1.1.1 32 any any 3.3.3.3 32 443 any 6 (log dcforward flowstart) (url
"facebook.com")
268436480 allow any 1.1.1.1 32 any any 3.3.3.3 32 443 any 6 (log dcforward flowstart) (url
"twitter.com")
268436480 allow any 1.1.1.1 32 any any 4.4.4.4 32 80 any 6 (log dcforward flowstart) (url
"facebook.com")
268436480 allow any 1.1.1.1 32 any any 4.4.4.4 32 80 any 6 (log dcforward flowstart) (url
"twitter.com")
268436480 allow any 1.1.1.1 32 any any 4.4.4.4 32 443 any 6 (log dcforward flowstart) (url
"facebook.com")
268436480 allow any 1.1.1.1 32 any any 4.4.4.4 32 443 any 6 (log dcforward flowstart) (url
"twitter.com")
268436480 allow any 2.2.2.2 32 any any 3.3.3.3 32 80 any 6 (log dcforward flowstart) (url
"facebook.com")
268436480 allow any 2.2.2.2 32 any any 3.3.3.3 32 80 any 6 (log dcforward flowstart) (url
"twitter.com")
268436480 allow any 2.2.2.2 32 any any 3.3.3.3 32 443 any 6 (log dcforward flowstart) (url
"facebook.com")
268436480 allow any 2.2.2.2 32 any any 3.3.3.3 32 443 any 6 (log dcforward flowstart) (url
"twitter.com")
268436480 allow any 2.2.2.2 32 any any 4.4.4.4 32 80 any 6 (log dcforward flowstart) (url
"facebook.com")
268436480 allow any 2.2.2.2 32 any any 4.4.4.4 32 80 any 6 (log dcforward flowstart) (url
"twitter.com")
268436480 allow any 2.2.2.2 32 any any 4.4.4.4 32 443 any 6 (log dcforward flowstart) (url
"facebook.com")
268436480 allow any 2.2.2.2 32 any any 4.4.4.4 32 443 any 6 (log dcforward flowstart) (url
"twitter.com")
268435456 allow any any any any any any any any (ipspolicy 2)
```

部署一個規則時，將兩個子網配置為源，兩個主機配置為目標地址，兩個自定義URL對象以兩個埠為目標，此規則將擴展為感測器上的16個規則。

> **注意**：如果要求使用訪問規則中的埠，請使用標準應**用中**存在的應用檢測器。這有助於以高效的方式實現規則擴展。

考慮從FMC配置訪問規則，如下圖所示：



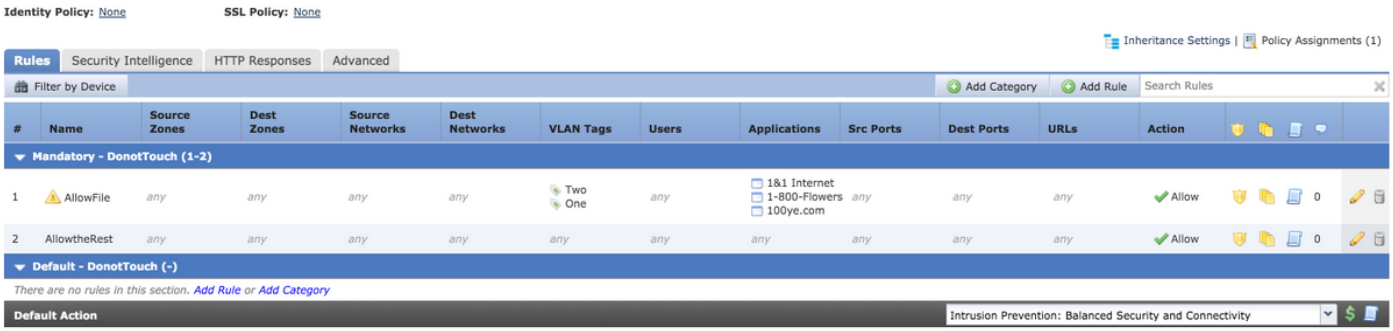
使用應用檢測器而不是埠時，擴展規則的數量從16個減少到8個，如下圖所示：

```
268436480 allow any 1.1.1.1 32 any any 3.3.3.3 32 any any any (log dcforward flowstart) (appid
676:1, 1122:1) (url "facebook.com")
```

```
268436480 allow any 1.1.1.1 32 any any 3.3.3.3 32 any any any (log dcforward flowstart) (appid
676:1, 1122:1) (url "twitter.com")
268436480 allow any 1.1.1.1 32 any any 4.4.4.4 32 any any any (log dcforward flowstart) (appid
676:1, 1122:1) (url "facebook.com")
268436480 allow any 1.1.1.1 32 any any 4.4.4.4 32 any any any (log dcforward flowstart) (appid
676:1, 1122:1) (url "twitter.com")
268436480 allow any 2.2.2.2 32 any any 3.3.3.3 32 any any any (log dcforward flowstart) (appid
676:1, 1122:1) (url "facebook.com")
268436480 allow any 2.2.2.2 32 any any 3.3.3.3 32 any any any (log dcforward flowstart) (appid
676:1, 1122:1) (url "twitter.com")
268436480 allow any 2.2.2.2 32 any any 4.4.4.4 32 any any any (log dcforward flowstart) (appid
676:1, 1122:1) (url "facebook.com")
268436480 allow any 2.2.2.2 32 any any 4.4.4.4 32 any any any (log dcforward flowstart) (appid
676:1, 1122:1) (url "twitter.com")
```

使用VLAN擴展基於IP的規則

考慮從FMC配置訪問規則，如下圖所示：



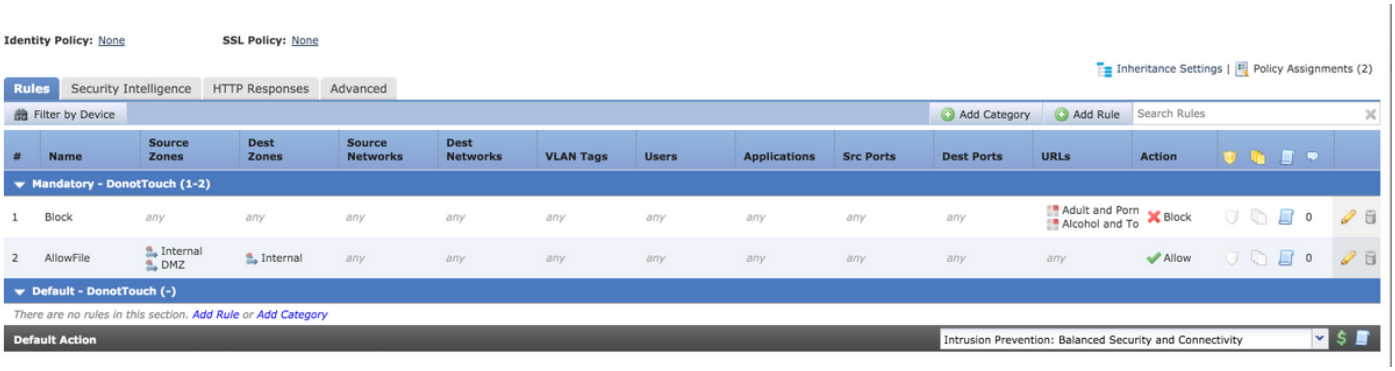
規則**AllowFile**有一行與兩個VLAN ID匹配，其中包含一些應用程式檢測器、入侵策略和檔案策略。規則AllowFile將擴展為兩個規則。

```
268436480 allow any any any any any any 1 any (log dcforward flowstart) (ipspolicy 5)
(filepolicy 1 enable) (appid 535:4, 1553:4, 3791:4)
268436480 allow any any any any any any 2 any (log dcforward flowstart) (ipspolicy 5)
(filepolicy 1 enable) (appid 535:4, 1553:4, 3791:4)
```

IPS策略和檔案策略對於每個訪問控制規則都是唯一的，但多個應用檢測器在同一規則中引用，因此不參與擴展。當您考慮具有兩個VLAN ID和三個應用檢測器的規則時，只有兩個規則，每個VLAN一個。

擴展具有URL類別的基於IP的規則

考慮從FMC配置訪問規則，如下圖所示：



阻止規則阻止**成人和色情網站**Any Reputation和Alcohol and Tobacco Reputations 1-3的URL類別。這是管理中心上的一個規則，但將其部署到感測器時，將擴展為如下所示的兩個規則：

```
268438530 deny any any  any any any  any any any  (log dcforward flowstart) (urlcat 11)
268438530 deny any any  any any any  any any any  (log dcforward flowstart) (urlcat 76) (urlrep
le 60)
```

部署單個規則時，將兩個子網配置為源，兩個主機配置為目標地址，並將兩個自定義URL對象配置為兩個埠（兩個URL類別），該規則將擴展到感測器上的三十二個規則。

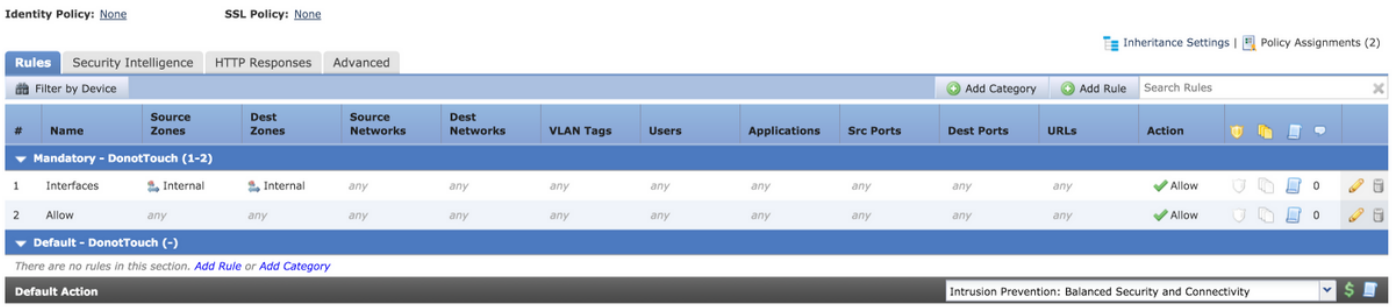
擴展帶區域的IP規則

區域是策略中引用的已分配號碼。

如果在策略中引用了某個區域，但該區域未分配給要向其推送該策略的裝置上的任何介面，則該區域將被視為**any**，並且**any不會導致任何規則擴展。**

如果規則中的源區域和目標區域相同，則區域因子被視為**any**，並且只新增一個規則，因為ANY不會導致規則的任何擴展。

考慮從FMC配置訪問規則，如下圖所示：



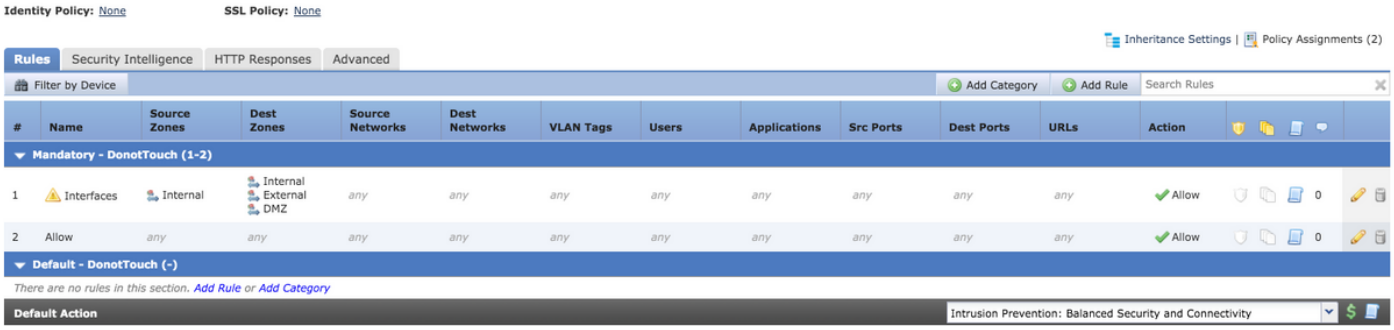
有兩種規則。一個規則配置了區域，但源區域和目標區域相同。另一個規則沒有特定配置。在本例中， **Interfaces**訪問規則不會轉換為規則。

```
268438531 allow any any any any any any any any (log dcforward flowstart)<-----Allow Access Rule
268434432 allow any any any any any any any any (log dcforward flowstart) (ipspolicy 17)<-------
---Default Intrusion Prevention Rule
```

在感測器上，兩個規則都顯示相同，因為涉及相同介面的基於區域的控制不會導致擴展。

基於區域的訪問控制規則訪問的規則擴展在將規則中引用的區域分配給裝置上的介面時發生。

考慮從FMC配置訪問規則，如下所示：



規則介面涉及基於區域的規則，源區域為內部，目標區域為內部、外部和DMZ。在此規則中，介面上配置了Internal和DMZ介面區域，裝置上不存在External。這是同一區域的擴展：

```
268436480 allow 0 any any 2 any any any any (log dcforward flowstart) <------Rule for Internal to DMZ)
268438531 allow any any any any any any any any (log dcforward flowstart)<--------Allow Access rule
268434432 allow any any any any any any any any (log dcforward flowstart) (ipspolicy 17)<-------Default Intrusion Prevention: Balanced Security over Connectivity
```

為特定介面對建立規則，該介面對為**Internal > DMZ**，具有清除區域規範，並且未建立**Internal > Internal**規則。

擴展的規則數與可為有效關聯區域建立的區域源和目標對數成正比，這包括相同的源和目標區域規則。

> **附註**：在策略部署期間，不會傳播FMC中禁用的規則，也不會將其擴展到感測器。

規則展開的一般公式

感測器上的規則數=（源子網或主機數）*（目標埠數）*（目標埠數）*（目標埠數）*（自定義URL數）*（VLAN標籤數）*（URL類別數）*（有效源和目標區域對數）

> **附註**：對於計算，欄位中的任何值都用1替換。規則組合中的**any**值將被視為1，它不會增加或擴展規則。

排除由於規則擴展導致的部署故障

如果對訪問規則進行新增後發生部署故障，則對於已達到規則擴展限制的情況，請按照下列步驟操作

在**/var/log/action.queue.log**中查詢包含以下關鍵字的消息：

錯誤 — 規則太多 — 正在編寫規則28，最大規則9094

上面的消息表明正在擴展的規則數量有問題。檢查FMC上的配置，以基於上述方案最佳化規則。

相關資訊

- Firepower管理中心配置指南6.0版
- 技術支援與文件 - Cisco Systems