了解FirePOWER设备上的规则扩展

目录

[简介](#)

[先决条件](#)

- [要求](#)
- [使用的组件](#)

[背景信息](#)

[了解规则扩展](#)

- [扩展基于IP的规则](#)
- [使用自定义URL扩展基于IP的规则](#)
- [使用端口扩展基于IP的规则](#)
- [使用VLAN扩展基于IP的规则](#)
- [使用URL类别扩展基于IP的规则](#)
- [扩展带有区域的基于IP的规则](#)

[规则扩展的一般公式](#)

[排除规则扩展引起的部署故障](#)

[相关信息](#)

简介

本文档介绍从Firepower管理中心(FMC)部署访问控制规则时，如何将其转换为传感器。

先决条件

要求

Cisco 建议您了解以下主题：

- Firepower技术知识
- 有关在FMC上配置访问控制策略的知识

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Firepower管理中心6.0.0版及更高版本
- 运行软件版本6.0.1及更高版本的ASA Firepower防御映像(ASA 5515-X、ASA 5525-X、ASA 5545-X、ASA 5555-X、ASA 5585-X)
- 运行软件版本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系列传感器6.0.0版及更高版本

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

背景信息

使用以下参数的一个或多个组合创建访问控制规则：

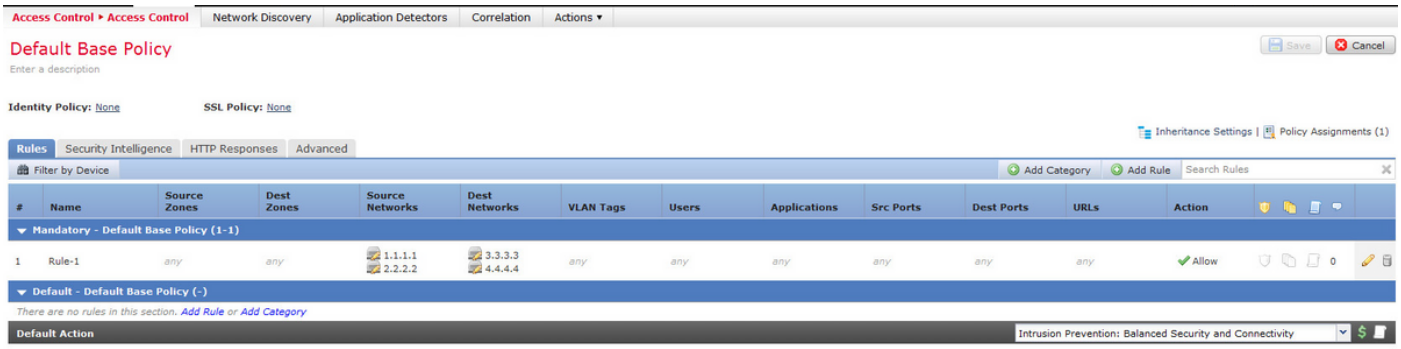
- IP地址（源和目标）
- 端口（源和目标）
- URL（系统提供的类别和自定义URL）
- 应用检测器
- VLAN
- 区域

根据访问规则中使用的参数组合，传感器上的规则扩展将会改变。本文档重点介绍FMC上的各种规则组合以及传感器上各自的关联扩展。

了解规则扩展

扩展基于IP的规则

考虑从FMC配置访问规则，如图所示：



这是管理中心的单一规则。但是，将其部署到传感器后，它会扩展为四个规则，如图所示：

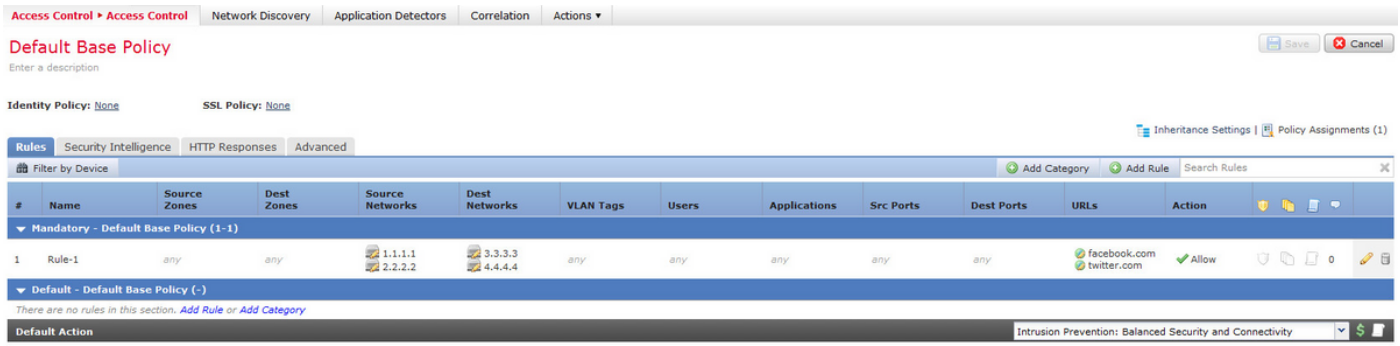
```
268436480 allow any 1.1.1.1 32 any any 3.3.3.3 32 any any any  (log dcforward flowstart)
268436480 allow any 1.1.1.1 32 any any 4.4.4.4 32 any any any  (log dcforward flowstart)
268436480 allow any 2.2.2.2 32 any any 3.3.3.3 32 any any any  (log dcforward flowstart)
268436480 allow any 2.2.2.2 32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

部署一个规则时，如果两个子网配置为源地址，两个主机配置为目标地址，则此规则将扩展为传感器上的四个规则。

注意：如果要求基于目标网络阻止访问，则执行此操作的更好方法是使用安全情报下的黑名单功能。

使用自定义URL扩展基于IP的规则

考虑从FMC配置访问规则，如图所示：



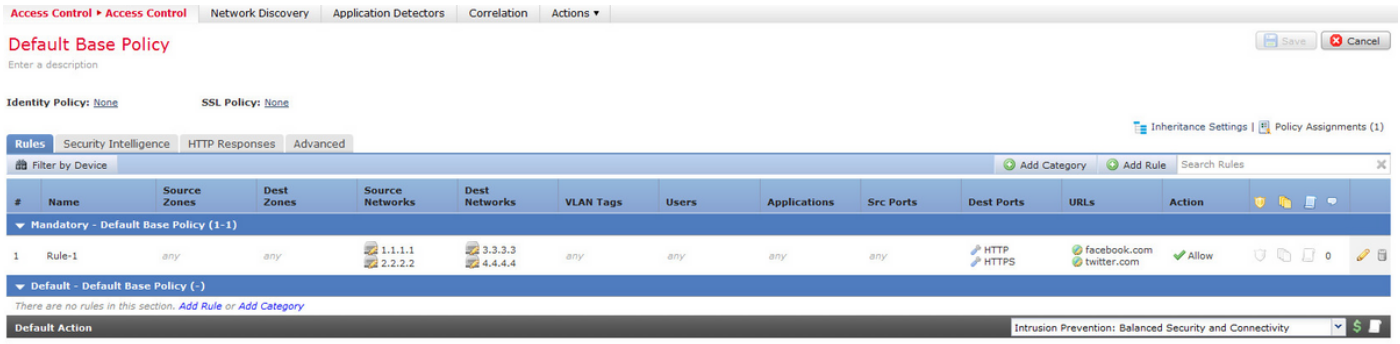
这是管理中心的单一规则。但是，将其部署到传感器后，会扩展为八条规则，如图所示：

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

部署一个规则时，该规则将传感器上的两个子网配置为Source，两个主机配置为目标地址，两个自定义URL对象合并到单个规则中，此规则将扩展为八个规则。这意味着对于每个自定义URL类别，都存在配置和创建的源和目标IP/端口范围的组合。

使用端口扩展基于IP的规则

考虑从FMC配置访问规则，如图所示：



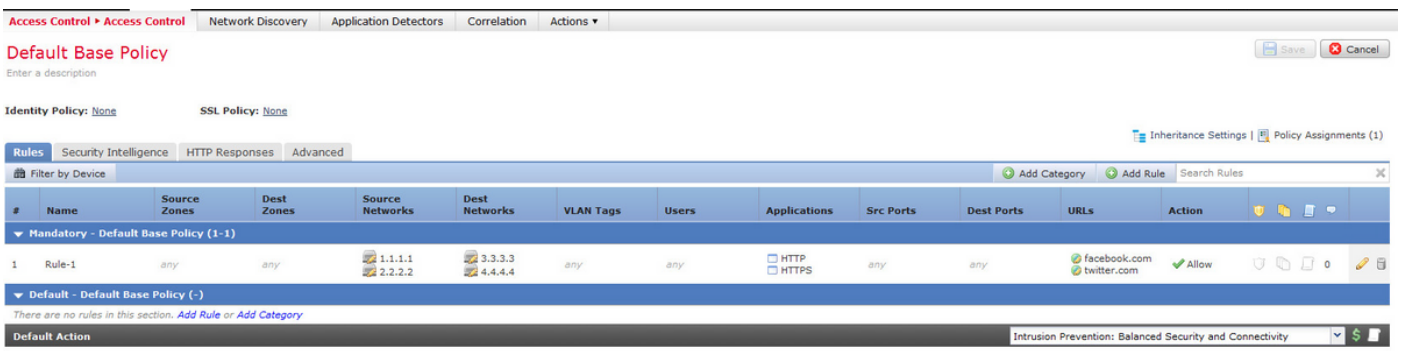
这是管理中心的单一规则。但是，将其部署到传感器后，会扩展为十六条规则，如图所示：

```
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.co
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.co
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.co
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.co
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 (ipspolicy 2)
```

当您部署一个规则时，该规则将两个子网配置为源，两个主机配置为目标地址，两个自定义URL对象指定到两个端口，此规则将扩展为传感器上的16个规则。

> 注意：如果需要使用访问规则中的端口，请使用标准应用的应用检测器。这有助于以高效的方式实现规则扩展。

考虑从FMC配置访问规则，如图所示：

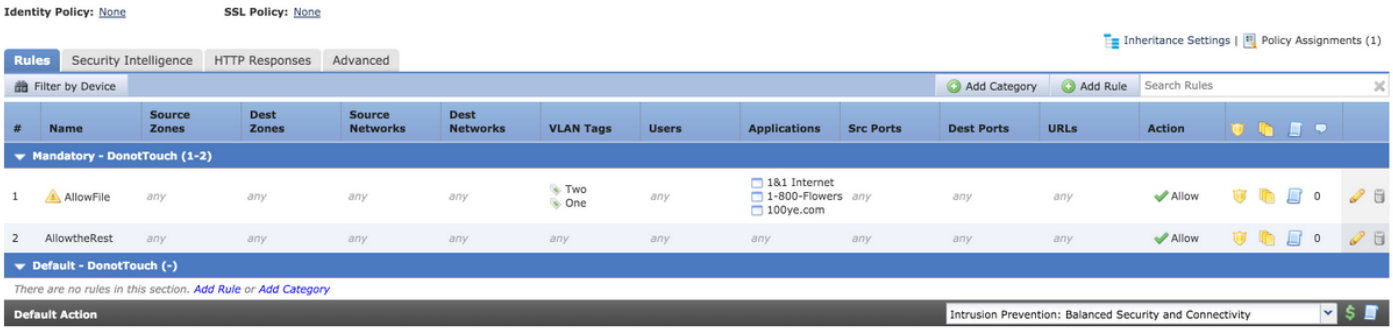


使用应用检测器而不是端口时，扩展规则的数量从十六个减少到八个，如图所示：

```
268436480 allow any 1.1.1.1 32 any any 3.3.3.3 32 any any any (log dcforward flowstart) (appid 676:1, 1
268436480 allow any 1.1.1.1 32 any any 3.3.3.3 32 any any any (log dcforward flowstart) (appid 676:1, 1
268436480 allow any 1.1.1.1 32 any any 4.4.4.4 32 any any any (log dcforward flowstart) (appid 676:1, 1
268436480 allow any 1.1.1.1 32 any any 4.4.4.4 32 any any any (log dcforward flowstart) (appid 676:1, 1
268436480 allow any 2.2.2.2 32 any any 3.3.3.3 32 any any any (log dcforward flowstart) (appid 676:1, 1
268436480 allow any 2.2.2.2 32 any any 3.3.3.3 32 any any any (log dcforward flowstart) (appid 676:1, 1
268436480 allow any 2.2.2.2 32 any any 4.4.4.4 32 any any any (log dcforward flowstart) (appid 676:1, 1
268436480 allow any 2.2.2.2 32 any any 4.4.4.4 32 any any any (log dcforward flowstart) (appid 676:1, 1
```

使用VLAN扩展基于IP的规则

考虑从FMC配置访问规则，如图所示：



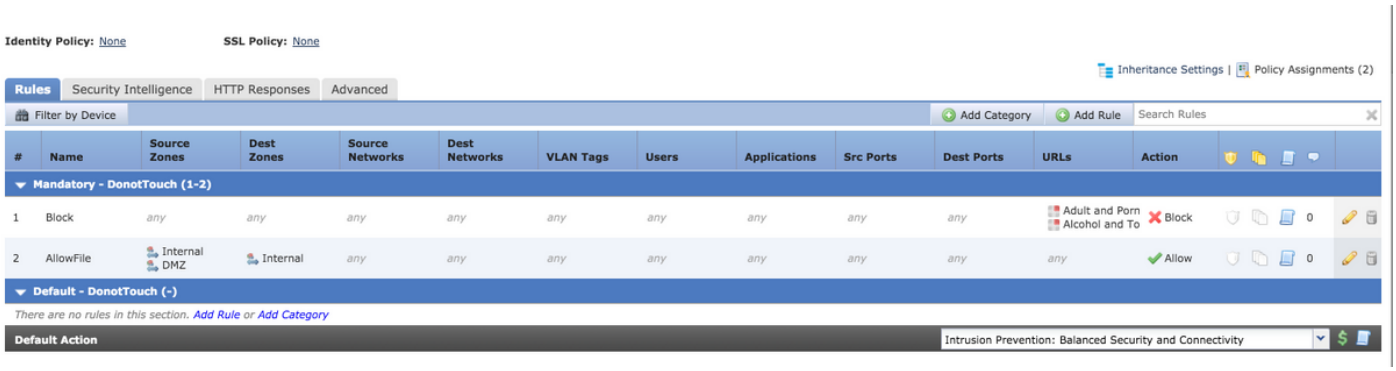
规则AllowFile具有匹配两个VLAN ID的单行，此两个VLAN ID带有一些应用检测器、入侵策略和文件策略。 规则AllowFile将扩展为两个规则。

```
268436480 allow any any any any any any 1 any (log dcforward flowstart) (ipspolicy 5) (filepolicy 1 ena
268436480 allow any any any any any any 2 any (log dcforward flowstart) (ipspolicy 5) (filepolicy 1 ena
```

IPS策略和文件策略对于每个访问控制规则都是唯一的，但同一规则中引用多个应用检测器，因此不参与扩展。当考虑具有两个VLAN ID和三个应用检测器的规则时，只有两个规则，每个VLAN一个。

使用URL类别扩展基于IP的规则

考虑从FMC配置访问规则，如图所示：



阻止规则阻止成人与色情网站的URL类别任何信誉和酒精与烟草信誉1-3。这是管理中心上的一个规则，但将其部署到传感器时，该规则将扩展为两个规则，如下所示：

```
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)
```

部署单个规则时，如果两个子网配置为源，两个主机配置为目标地址，并且两个自定义URL对象指向具有两个URL类别的两个端口，则此规则将扩展为传感器上的32个规则。

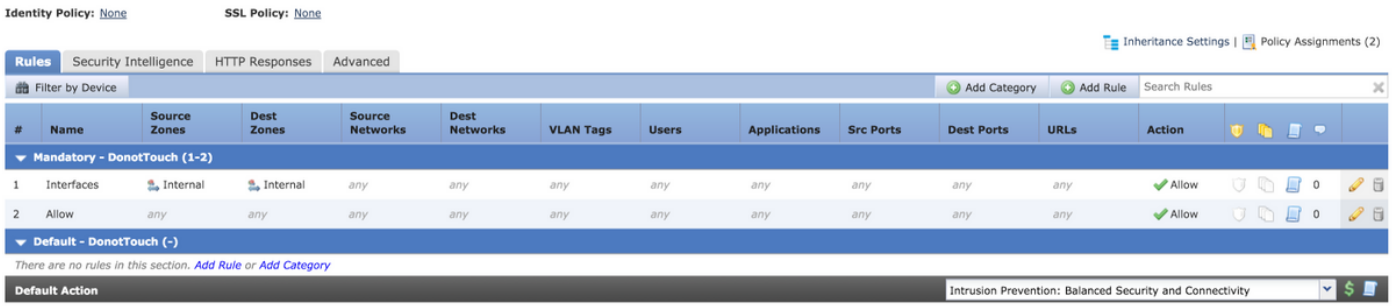
扩展带有区域的基于IP的规则

区域是分配给在策略中引用的编号。

如果在策略中引用了某个区域，但是未将该区域分配给正在向其推送策略的设备上的任何接口，则将该区域视为any，并且any不会导致任何规则扩展。

如果规则中的源区域和目标区域相同，则区域系数被视为any，并且只添加一个规则，因为ANY不会导致规则的任何扩展。

考虑从FMC配置访问规则，如图所示：



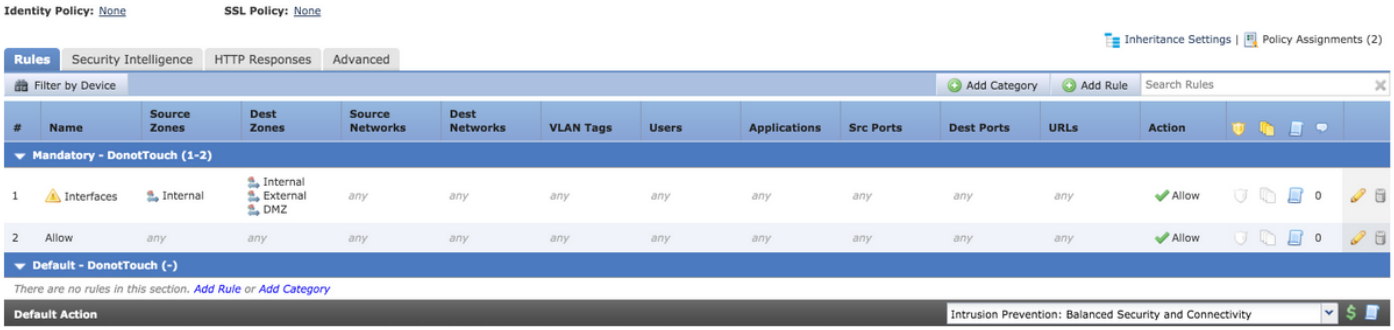
有两个规则。一条规则配置了区域，但源和目标区域相同。另一个规则没有特定配置。在本示例中，Interfaces 访问规则不转换为规则。

```
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)<----------Defa
```

在传感器上，两个规则看起来相同，因为涉及相同接口的区域控制不会导致扩展。

将规则中引用的区域分配给设备上的接口时，会扩展基于区域的访问控制规则访问的规则。

考虑从FMC配置访问规则，如下所示：



规则Interfaces涉及基于区域的规则，其中源区域为Internal，目标区域为Internal、External和DMZ。在此规则中，接口上配置了Internal和DMZ接口区域，而设备上不存在External。这是同一规则的扩展：

```
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)<--------Defaul
```

为特定接口对创建规则，即带有明确区域规范的Internal > DMZ，但不会创建Internal > Internal规则。

扩展的规则数量与可以为有效关联区域创建的区域源和目标对的数量成正比，这包括相同的源和目标区域规则。

注意：在策略部署期间，不会传播FMC中已禁用的规则，也不会将其扩展至传感器。

规则扩展的一般公式

传感器上的规则数量=（源子网或主机数量）*（目标数量）*（源端口数量）*（目标端口数量）*（自定义URL数量）*（VLAN标记数量）*（URL类别数量）*（有效源区域对和目标区域对数量）

注：在计算中，字段中的任何值将替换为1。规则组合中的any值将被视为1，它不会增加或扩展规则。

排除规则扩展引起的部署故障

添加访问规则后，如果部署失败，请按照下述步骤处理已达到规则扩展限制的情况

有关包含以下关键字的消息，请查看/var/log/action.queue.log：

错误-规则太多-写入规则28，最大规则9094

上述消息表明正在扩展的规则数量存在问题。检查FMC上的配置，以基于上述场景优化规则。

相关信息

- Firepower管理中心配置指南，版本6.0
- 技术支持和文档 - Cisco Systems

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。