了解FirePOWER设备上的规则扩展

目录

简介

本文档介绍从Firepower管理中心(FMC)部署时，访问控制规则到传感器的转换。

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 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 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：

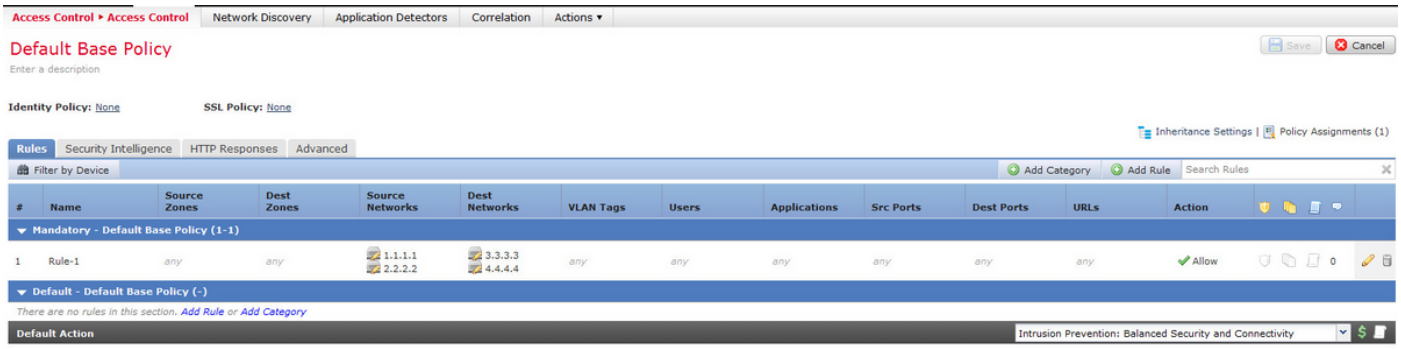
- IP地址（源和目标）
- 端口（源和目标）
- URL（系统提供的类别和自定义URL）
- 应用检测器
- VLAN
- 区域

根据访问规则中使用的参数组合，规则扩展在传感器上会发生变化。本文档重点介绍FMC上规则的各种组合以及传感器上各自关联的扩展。

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：



这是管理中心上的单个规则。但是，将其部署到传感器后，它将扩展**为四**个规则，如图所示：

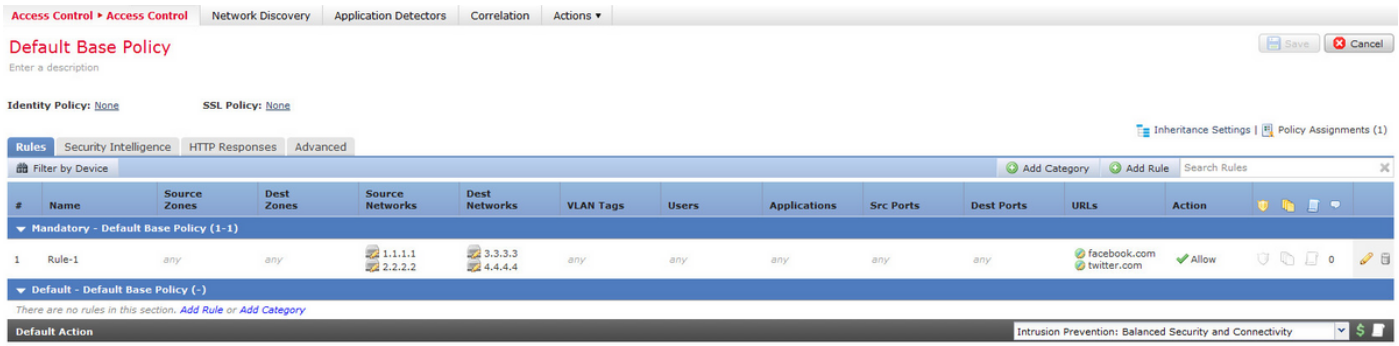
```
268436480 allow any 1.1.1.1 32 any any 3.3.3.3 32 any any any  (log dcforward flowstart)
268436480 allow any 1.1.1.1 32 any any 4.4.4.4 32 any any any  (log dcforward flowstart)
268436480 allow any 2.2.2.2 32 any any 3.3.3.3 32 any any any  (log dcforward flowstart)
268436480 allow any 2.2.2.2 32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

当部署一个规则时，该规则将两个子网配置为源，两个主机配置为目标地址，该规则将扩展为传感器上的四个规则。

注意：如果要求根据目的网络阻止访问，则更好的方法是使用安全情报下黑名单的功能。

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：



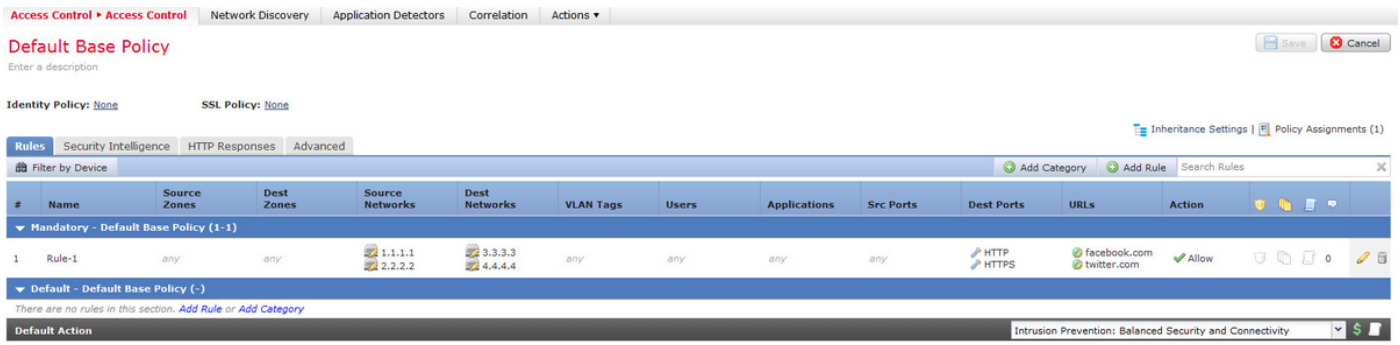
这是管理中心上的单个规则。但是，将其部署到传感器后，将其扩展为八个规则，如图所示：

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

当在管理中心的单个规则中部署具有两个配置为源的子网、两个配置为目标地址的主机和两个自定义URL对象的规则时，此规则将扩展为传感器上的八个规则。这意味着，对于每个自定义URL类别，都有源IP/端口范围和目标IP/端口范围的组合，这些范围是配置和创建的。

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：



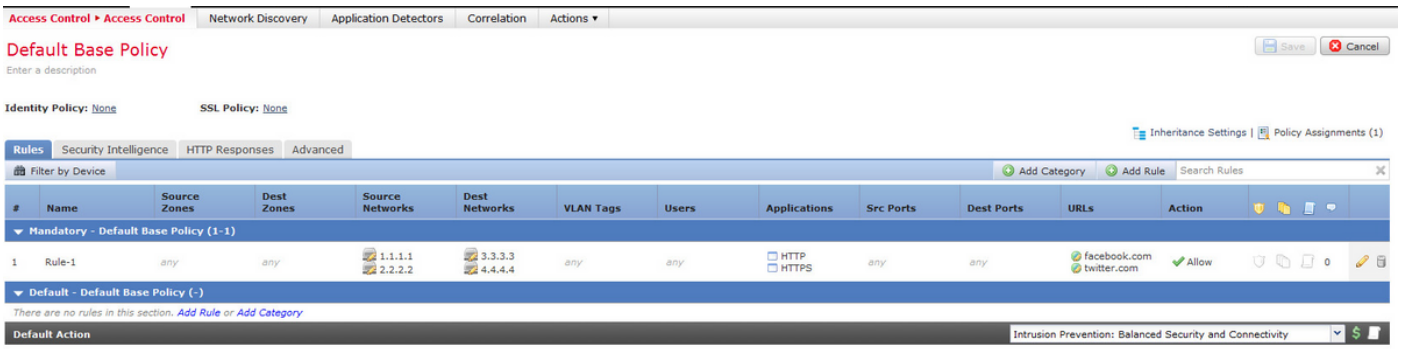
这是管理中心上的单个规则。但是，将其部署到传感器后，将其扩展为十六条规则，如图所示：

```
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.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)
```

当部署一个规则时，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对象发往两个端口，该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**用程**序检测器。这有助于以高效的方式扩展规则。

考虑从FMC配置访问规则，如图所示：



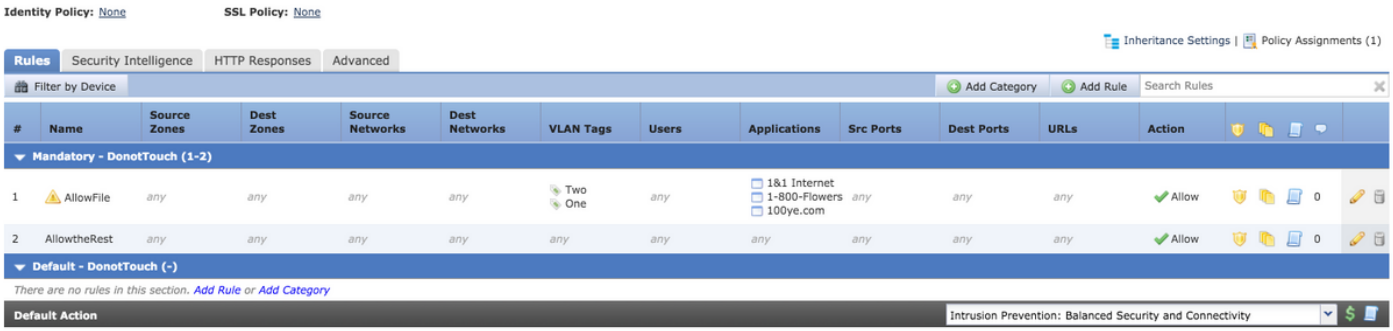
使用应用检测器而不是端口时，扩展规则的数量从十六个减少到八个，如图所示：

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



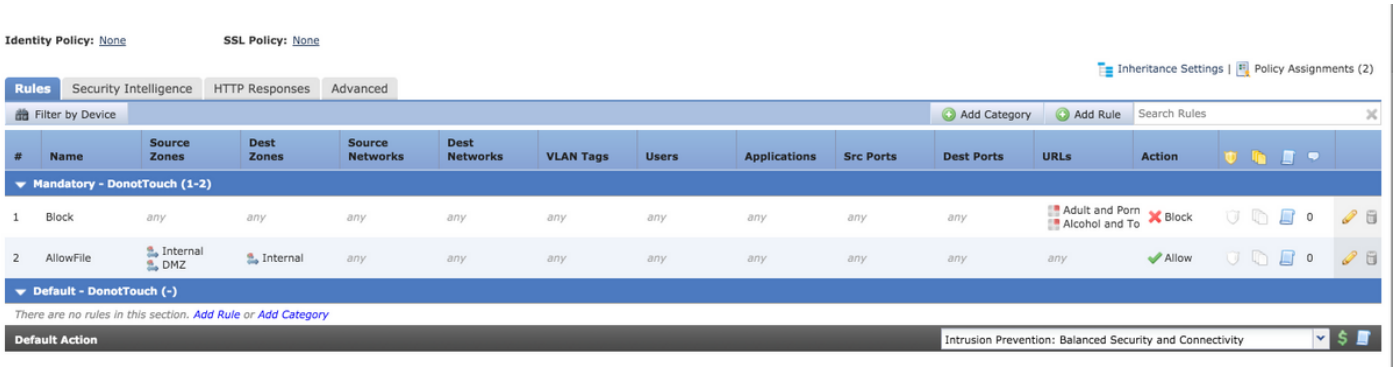
规则AllowFile有一行，该行与两个VLAN ID匹配，其中包含一些应用检测器、入侵策略和文件策略。规则AllowFile将扩展为两个规则。

```
268436480 allow any any any any any any 1 any (log dcforward flowstart) (ipspolicy 5)
(filepolicy 1 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策略和文件策略对于每个访问控制规则都是唯一的，但多个应用检测器在同一规则中引用，因此不参与扩展。当您考虑一个包含两个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。

扩展基于IP的规则和URL类别

考虑从FMC配置访问规则，如图所示：



阻止规则阻止**成人和色情**信誉**和酒精和烟草信誉1-3的URL类别。这是管理中心的单一规则，但当您将其部署到传感器时，它将扩展为两个规则，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)
```

当部署一个规则，其中两个子网配置为源，两个主机配置为目标地址，两个自定义URL对象以两个URL类别为目标的两个端口为目标时，此规则将扩展到传感器上的32个规则。

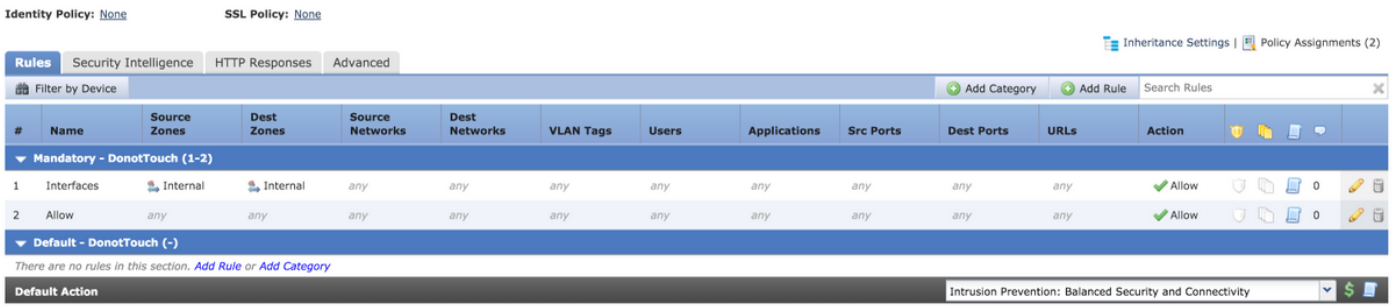
扩展基于IP的规则（带区域）

区域是分配的编号，在策略中引用。

如果某个区域在策略中引用，但该区域未分配到要向其推送策略的设备上的任何接口，则该区域被视为**any**，且**any**不会导致规则扩展。

如果源区域和目标区域在规则中相同，则区域因子被视为**any**，并且只添加一个规则，因为ANY不会导致规则扩展。

考虑从FMC配置访问规则，如图所示：



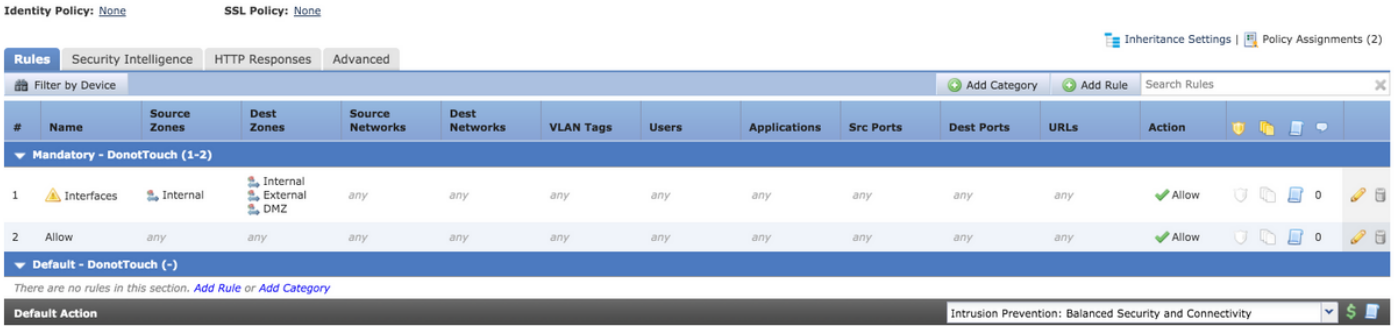
有两条规则。一条规则配置了Zones，但源区域和目标区域相同。另一条规则没有特定配置。在本例中，接口访**问规**则不会转换为规则。

```
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)<-------
---Default Intrusion Prevention Rule
```

在传感器上，由于涉及相同接口的基于区域的控制不会导致扩展，因此两个规则显示相同。

当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：



规则接口涉及基于区域的规则，源区域为内部区域，目标区域为内部区域、外部区域和DMZ区域。在此规则中，接口上配置了内部和DMZ接口区域，而设备上不存在外部区域。这是相同的扩展：

```
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)<-------Default Intrusion Prevention: Balanced Security over Connectivity
```

为特定接口对创建规则，该接口对为“内部”**>“DMZ”，**且区域规范明确，**且不创建“**内部”>“内部”规则。

展开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比例，这**包括**相同的源区域和目标区域规则。

> **注意**：在策略部署期间，FMC中禁用的规则不会传播，也不会扩展到传感器。

规则展开的通式

传感器规则数=（源子网或主机数）*（目标S数）*（源端口数）*（目标端口数）*（目标端口数）*（自定义URL数）*（VLAN标记数）*（URL类别数）*（有效源和目标区域对数）

> **注意**：对于计算，**字段**中的任何值都被1替换。规则组合中**的**任何值都被视为1，并且不会增加或扩展规则。

排除由于规则扩展导致的部署故障

在添加访问规则后出现部署故障时，请按照以下步骤处理已达到规则扩展限制的情况

检查/var/log/action.queue.log中是否包含以下关键字：

错误 — 规则太多 — 正在写入规则28，最大规则9094

上述消息表示正在扩展的规则数量有问题。检查FMC上的配置，以根据上述场景优化规则。

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