

# 了解基于TrustSec的FirePower和ISE访问控制

## 目录

[简介](#)

[使用的组件](#)

[概述](#)

[用户IP映射方法](#)

[内联标记方法](#)

[故障排除](#)

[从Firepower设备的受限外壳](#)

[从Firepower设备的专家模式](#)

[从Firepower管理中心](#)

## 简介

Cisco TrustSec利用第2层以太网帧的标记和映射来隔离流量，而不影响现有IP基础设施。标记流量可以采用更精细的安全措施进行处理。

身份服务引擎(ISE)和Firepower管理中心(FMC)之间的集成允许从客户端授权传递TrustSec标记，Firepower可使用此授权根据客户端的安全组标记应用访问控制策略。本文档讨论将ISE与Cisco Firepower技术集成的步骤。

## 使用的组件

本文档在示例设置中使用以下组件：

- 身份服务引擎(ISE)版本2.1
- Firepower管理中心(FMC)版本6.x
- 思科自适应安全设备(ASA)5506-X版本9.6.2
- 思科自适应安全设备(ASA)5506-X Firepower模块，版本6.1

## 概述

传感器设备有两种方法可检测分配给流量的安全组标记(SGT):

1. 通过用户IP映射
2. 通过内联SGT标记

## 用户IP映射方法

为确保TrustSec信息用于访问控制，ISE与FMC的集成将完成以下步骤：

**步骤 1：** FMC从ISE检索安全组列表。

**步骤 2：** 访问控制策略在FMC上创建，其中将安全组作为条件。

**步骤 3：** 当终端使用ISE进行身份验证和授权时，会话数据会发布到FMC。

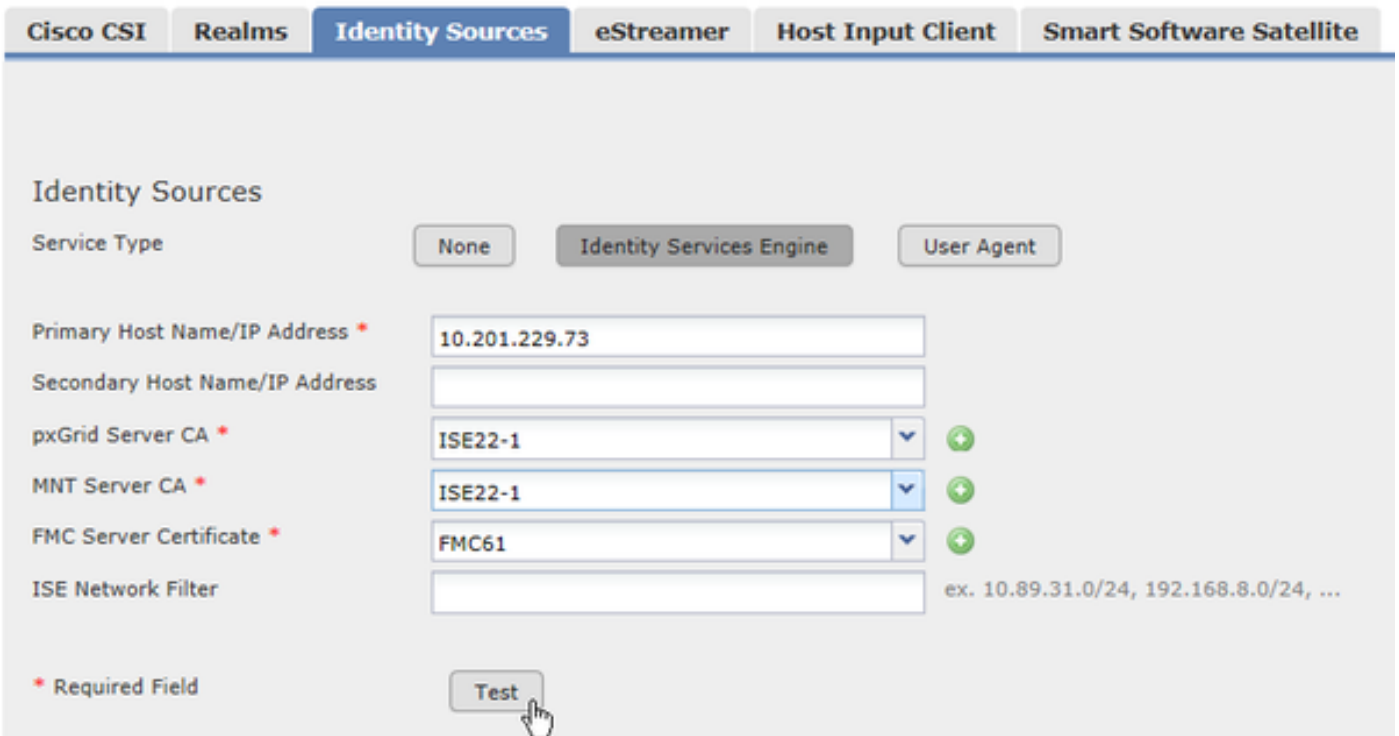
**步骤 4：** FMC构建用户IP-SGT映射文件，并将其推送到传感器。

**步骤 5：** 流量的源IP地址用于使用来自用户IP映射的会话数据匹配安全组。

**步骤 6：** 如果流量源的安全组与访问控制策略中的条件匹配，则传感器将相应地采取操作。

当ISE集成的配置保存在System > Integration > Identity Sources > Identity Services Engine下时，FMC将检索完整的SGT列表。

**注意：** 单击Test按钮（如下所示）不会触发FMC检索SGT数据。



The screenshot shows the 'Identity Sources' configuration page in FMC. The 'Service Type' is set to 'Identity Services Engine'. The 'Primary Host Name/IP Address' is '10.201.229.73'. The 'Secondary Host Name/IP Address' is empty. The 'pxGrid Server CA', 'MNT Server CA', and 'FMC Server Certificate' are all set to 'ISE22-1', 'ISE22-1', and 'FMC61' respectively. The 'ISE Network Filter' is empty. A 'Test' button is visible at the bottom.

FMC和ISE之间的通信由ADI（抽象目录接口）实现，ADI是在FMC上运行的唯一进程（只能有一个实例）。FMC上的其他进程订用ADI并请求信息。目前，唯一订用ADI的组件是数据相关器。

FMC将SGT保存在本地数据库中。数据库包含SGT名称和编号，但当前FMC在处理SGT数据时使用唯一标识符（安全标记ID）作为句柄。此数据库也传播到传感器。

如果ISE安全组发生更改（如删除或添加组），ISE会将pxGrid通知推送到FMC以更新本地SGT数据库。

当用户使用ISE进行身份验证并使用安全组标记进行授权时，ISE通过pxGrid通知FMC，提供领域Y中的用户X已使用SGT Z登录的信息。FMC获取信息并插入用户IP映射文件。FMC使用算法确定将获取的映射推送到传感器的时间，具体取决于存在多少网络负载。

**注意：** FMC不会将所有用户IP映射条目推送到传感器。FMC要推送映射，首先必须通过领域

了解用户。如果会话中的用户不属于领域，传感器将不会获取此用户的映射信息。未来版本将考虑对非领域用户的支持。

Firepower系统版本6.0仅支持IP — 用户 — SGT映射。流量中的实际标记或从ASA上的SXP获知的SGT-IP映射不会使用。当传感器拾取传入流量时，Snort进程将获取源IP并查找用户 — IP映射(由Firepower模块推送到Snort进程)，并查找安全标记ID。如果它与访问控制策略中配置的SGT ID (而非SGT编号) 匹配，则策略将应用于流量。

## 内联标记方法

从ASA 9.6.2版和ASA Firepower模块6.1版开始，支持内联SGT标记。这意味着Firepower模块现在能够直接从数据包中提取SGT编号，而不依赖于FMC提供的用户 — IP映射。当用户不属于领域 (例如不支持802.1x身份验证的设备) 时，这为基于TrustSec的访问控制提供了替代解决方案。

使用Inline Tagging方法时，传感器仍在FMC上回复，从ISE检索SGT组并向下推送SGT数据库。当标有安全组编号的流量到达ASA时，如果ASA配置为信任传入的SGT，则标记将通过数据平面传递到Firepower模块。Firepower模块从数据包中获取标记，并直接使用它来评估访问控制策略。

ASA必须在接口上配置正确的TrustSec才能接收已标记的流量：

```
interface GigabitEthernet1/1
 nameif inside
 cts manual
 policy static sgt 6 trusted
 security-level 100
 ip address 10.201.229.81 255.255.255.224
```

**注意：**只有ASA 9.6.2及更高版本支持内联标记。ASA的早期版本不会通过数据平面将安全标记传递到Firepower模块。如果传感器支持内联标记，它将首先尝试从流量中提取标记。如果流量未标记，则传感器将回退到用户IP映射方法。

## 故障排除

### 从Firepower设备的受限外壳

要显示从FMC推送的访问控制策略，请执行以下操作：

```
> show access-control-config
.
.
.
.
. =====[ Rule Set: (User) ]===== [ Rule: DenyGambling ]-----
----- Action : Block ISE Metadata : Security Group Tags: [7:6]

Destination Ports      : HTTP (protocol 6, port 80)
                        : HTTPS (protocol 6, port 443)
URLs
  Category              : Gambling
  Category              : Streaming Media
  Category              : Hacking
```

```
Category           : Malware Sites
Category           : Peer to Peer
Logging Configuration
DC                 : Enabled
Beginning          : Enabled
End                : Disabled
Files              : Disabled
Safe Search        : No
Rule Hits          : 3
Variable Set       : Default-Set
```

**注意：**安全组标记指定两个数字：[7:6]。在这组数字中，“7”是本地SGT数据库的唯一ID，仅FMC和传感器知道此ID。“6”是所有各方已知的实际SGT编号。

要查看SFR处理传入流量并评估访问策略时生成的日志，请执行以下操作：

```
> system support firewall-engine-debug
```

```
Please specify an IP protocol:
Please specify a client IP address: 10.201.229.88
Please specify a client port:
Please specify a server IP address:
Please specify a server port:
Monitoring firewall engine debug messages
```

带内联标记的传入流量的firewall-engine-debug示例：

```
10.201.229.88-52243 > 104.28.4.103-80 6 AS 0 I 1 Starting with minimum 0, id 0 and IPProto first
with zones -1 -> -1,
geo 0(0) -> 0, vlan 0, sgt tag: 6, svc 676, payload 0, client 686, misc 0, user 9999999, url
http://www.poker.com/, xff
10.201.229.88-52243 > 104.28.4.103-80 6 AS 0 I 1: DataMessaging_GetURLData: Returning URL_BCTYPE
for www.poker.com
10.201.229.88-52243 > 104.28.4.103-80 6 AS 0 I 1 rule order 1, 'DenyGambling', URL Lookup
Success: http://www.poker.com/ waited: 0ms
10.201.229.88-52243 > 104.28.4.103-80 6 AS 0 I 1 rule order 1, 'DenyGambling', URL
http://www.poker.com/ Matched Category: 27:96 waited: 0ms
10.201.229.88-52243 > 104.28.4.103-80 6 AS 0 I 1 match rule order 1, 'DenyGambling', action
Block
10.201.229.88-52243 > 104.28.4.103-80 6 AS 0 I 1 sending block response of 474 bytes
```

## 从Firepower设备的专家模式

**警告：**以下指令可能会影响系统性能。仅为故障排除目的或思科支持工程师请求此数据时运行该命令。

Firepower模块将用户 — IP映射推送到本地Snort进程。要验证Snort对映射的了解，可以使用以下命令将查询发送到Snort:

```
> system support firewall-engine-dump-user-identity-data
```

```
Successfully commanded snort.
```

要查看数据，请进入专家模式：

```
> expert
```

```
admin@firepower:~$
```

Snort在/var/sf/detection\_engines/GUID/instance-x目录下创建转储文件。转储文件的名称为user\_identity.dump。

```
admin@firepower:/var/sf/detection_engines/7eed8b44-707f-11e6-9d7d-e9a0c4d67697/instance-1$ sudo
cat user_identity.dump
Password:
```

```
----- IP:USER ----- Host ::ffff:10.201.229.88 -----
----- ::ffff:10.201.229.88: sgt 7, device_type 313, location_ip ::ffff:10.201.229.94
::ffff:10.201.229.88:47 realm 3 type 1 user_pat_start 0

-----
USER:GROUPS
-----
~
```

以上输出显示，Snort知道IP地址10.201.229.94映射到SGT ID 7，即SGT编号6（访客）。

## 从Firepower管理中心

您可以查看ADI日志以验证FMC和ISE之间的通信。要查找adi组件的日志，请检查FMC上的/var/log/messages文件。您会注意到如下日志：

```
ADI_ISE_Test_Help:adi.ISEConnection [INFO] Preparing ISE Connection objects...
ADI_ISE_Test_Help:adi.ISEConnection [INFO] Preparing subscription objects...
ADI_ISE_Test_Help:adi.ISEConnection [INFO] subscribed successfully to
EndpointProfileMetaDataCapability
ADI_ISE_Test_Help:adi.ISEConnection [INFO] registered callback for capability
EndpointProfileMetaDataCapability
ADI_ISE_Test_Help:adi.ISEConnection [INFO] subscribed successfully to
TrustSecMetaDataCapability
ADI_ISE_Test_Help:adi.ISEConnection [INFO] registered callback for capability
TrustSecMetaDataCapability
ADI_ISE_Test_Help:adi.ISEConnection [INFO] subscribed successfully to
SessionDirectoryCapability
ADI_ISE_Test_Help:adi.ISEConnection [INFO] registered callback for capability
SessionDirectoryCapability
ADI_ISE_Test_Help:adi.ISEConnection [INFO] Connecting to ISE server...
ADI_ISE_Test_Help:adi.ISEConnection [INFO] Beginning to connect to ISE server...
.
.
.
.
ADI_ISE_Test_Help:adi.ISEConnection [INFO] ...successfully connected to ISE server.
ADI_ISE_Test_Help:adi.ISEConnection [INFO] Starting bulk download
.
.
```