了解有Firepower和ISE的基于TrustSec的访问控制

目录

简介

思科TrustSec使用Layer2以太网帧标记和映射分离流量，无需影响现有IP基础设施。标记的数据流可以处理与与更加极大的粒度的安全措施。

在身份服务引擎(ISE)和Firepower管理中心(FMC)之间的集成允许标记的TrustSec从客户端授权通信，可以由Firepower用于运用根据客户端的安全组标记的访问控制策略。本文讨论步骤集成与思科Firepower技术的ISE。

使用的组件

本文使用根据组件在设置的示例：

- 身份服务引擎(ISE)版本2.1
- Firepower管理中心(FMC)版本6.x
- Cisco可适应安全工具(ASA) 5506-X版本9.6.2
- Cisco可适应安全工具(ASA) 5506-X Firepower模块，版本6.1

概述

有传感器设备的两种方式能检测安全组标记(SGT)分配到流量：

1. 通过用户IP映射
2. 通过轴向SGT标记

用户IP映射方法

要保证TrustSec信息使用访问控制， ISE的集成与FMC通过以下步骤：

步骤 1：FMC从ISE获取安全组的列表。

步骤 2：访问控制策略在包括安全组作为情况的FMC创建。

步骤 3：当终端验证并且授权与ISE时，会话数据发布对FMC。

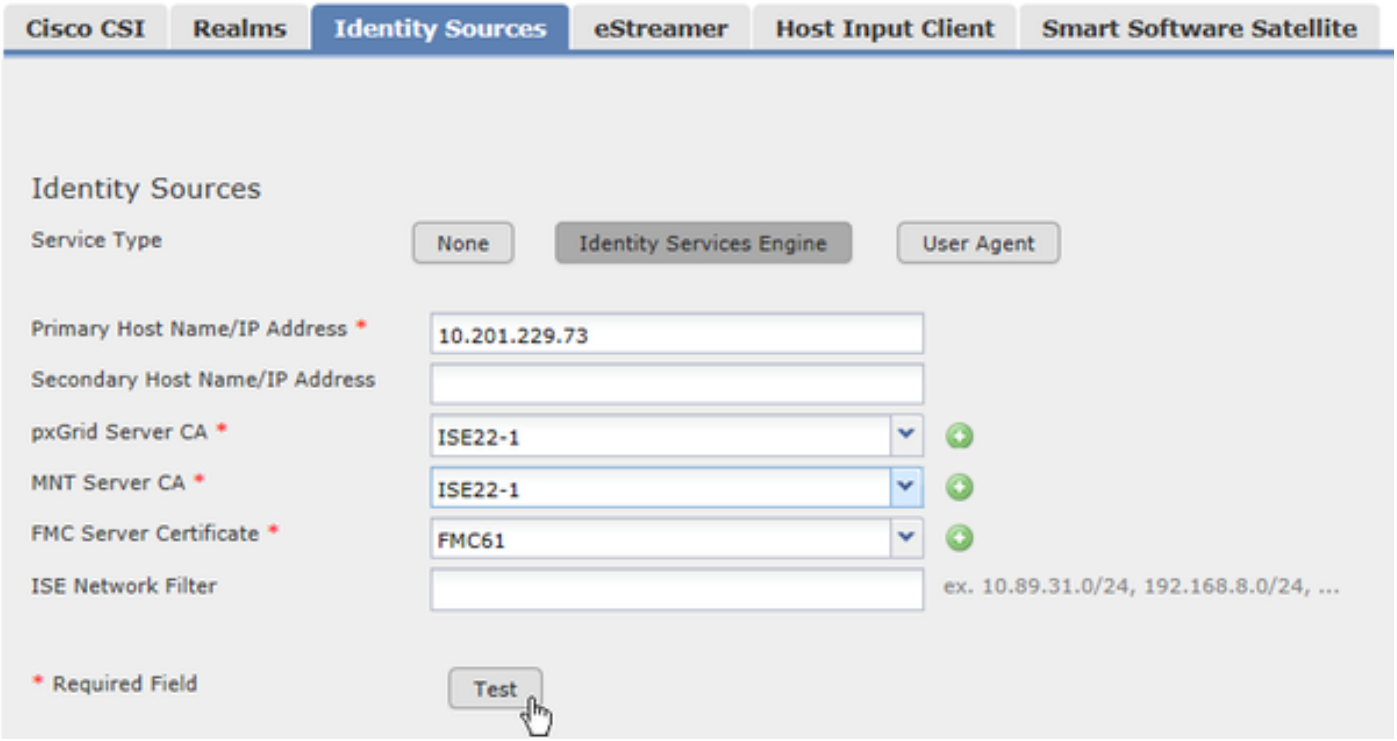
步骤 4：FMC创建用户IPSGT映射文件，并且推送它到传感器。

步骤 5：流量的源IP地址用于匹配使用从用户IP映射的安全组会话数据。

步骤 6：如果数据流源的安全组匹配在访问控制策略的条件，行动由传感器相应地采取。

当ISE集成的配置保存在**系统>集成>标识下来源>身份服务引擎时，** FMC获取一完整SGT列表。

注意：单击**Test按钮**(如下所示)不触发FMC获取SGT数据。



FMC和ISE之间的通信由ADI (抽象目录接口)实现，是一唯一进程(可以只有一个实例)运行在FMC。在FMC的其他进程订阅对ADI和请求数据。目前订阅对ADI的唯一的组件是数据相关器。

FMC保存在本地数据库的SGT。数据库包含两SGT名称和编号，但是FMC当前使用一个唯一标识符(安全标记ID)作为把柄，当处理SGT数据时。此数据库也被传播到传感器。

如果ISE安全组更改，例如删除或组的新增内容， ISE推送pxGrid通知对FMC更新本地SGT数据库。

当用户验证与ISE并且授权与安全组标记时， ISE通过pxGrid通知FMC，提供知识x从领域Y登陆与SGT Z. FMC的用户采取信息和插入到用户IP映射文件。FMC使用一种算法确定时候推送获取的映射到传感器，根据多少网络负载存在。

注意：FMC不推送所有用户IP映射条目到传感器。为了使推送的FMC映射，必须通过领域首先有用户的知识。如果用户在会话上不作为领域的部分，传感器不会学习此用户映射信息。非领域用户的支持为将来版本考虑。

Firepower系统版本6.0仅支持IP用户SGT映射。没有使用在流量的实际标记或者从在ASA的SXP了解的SGT-IP映射。当传感器拾起流入的数据流时，喷鼻息进程采取来源IP并且查寻由对喷鼻息进程的Firepower模块推送)的用户IP映射(并且查找安全标记ID。如果它匹配在访问控制策略(不是SGT编号)配置的SGT ID，则策略应用对流量。

轴向标记方法

从ASA版本9.6.2和ASA Firepower模块6.1开始，支持轴向SGT标记。这意味着Firepower模块当前能够解压缩SGT编号直接地从数据包，无需取决于在用户IP FMC提供的映射。这为基于TrustSec的访问控制提供一其它方案，当用户不作为领域的部分时(例如设备没有能力在802.1x验证上)。

使用轴向标记方法，传感器在FMC仍然回复从ISE检索SGT组和增加SGT数据库。当用安全组组编号标记的流量到达ASA，如果ASA配置委托流入SGT，标记将通过到Firepower模块通过dataplane。Firepower模块采取从数据包的标记并且直接地使用它评估访问控制策略。

ASA必须有在接口的适当的TrustSec配置为了收到标记的数据流：

```
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：仅ASA版本9.6.2和以上支持轴向标记。ASA的更早版本不通过安全标记dataplane到Firepower模块。如果传感器支持轴向标记，首先将设法解压缩从流量的标记。如果流量不是标记为的，传感器落回到用户IP映射方法。

排除故障

从Firepower设备的限制Shell

显示从FMC的访问控制推行的策略：

```
> show access-control-config .
.
<Output Omitted>
.
. ===============[ 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编号：[7:6].在此一组数字，“7"是本地SGT数据库的唯一的ID，只为FMC和传感器所知。“6"是实际SGT编号为所有当事人所知。

查看生成的日志，当SFR处理流入的数据流和评估的访问策略：

```
> 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
```

示例流入的数据流的与轴向标记：

```
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：**以下说明可能影响系统性能。运行仅命令故障排除目的，或者，当Cisco技术支持工程师要求此数据。

Firepower模块映射对本地喷鼻息进程的推进用户IP。要验证什么喷鼻息知道关于映射，您能使用以下命令发送查询打鼾：

```
> system support firewall-engine-dump-user-identity-data Successfully commanded snort.
```

查看数据，回车到专家模式：

```
> expert

admin@firepower:~$
```

喷鼻息创建转储文件在/var/sf/detection_engines/GUID/instance-x目录下。转储文件的名称是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 --------
----------- ~
```

以上输出显示喷鼻息知道IP地址10.201.229.94哪些被映射对SGT ID 7，是SGT第6 (访客)。

从Firepower管理中心

您能检查ADI日志验证FMC和ISE之间的通信。要查找adi组件日志，请检查在FMC的/var/log/messages文件。您将注意日志类似如下：

```
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...
.
.
<Output Omitted>
.
.
ADI_ISE_Test_Help:adi.ISEConnection [INFO] ...successfully connected to ISE server.
ADI_ISE_Test_Help:adi.ISEConnection [INFO] Starting bulk download
.
.
<Output Omitted>
```