Comprensión del control de acceso basado en TrustSec con FirePower e ISE

Contenido

Introducción

Cisco TrustSec utiliza etiquetado y asignación de tramas Ethernet de capa 2 para segregar el tráfico sin afectar a la infraestructura IP existente. El tráfico etiquetado se puede tratar con medidas de seguridad con mayor granularidad.

La integración entre Identity Services Engine (ISE) y Firepower Management Center (FMC) permite que el etiquetado TrustSec se comunique desde la autorización del cliente, que puede utilizar Firepower para aplicar políticas de control de acceso basadas en la etiqueta de grupo de seguridad del cliente. Este documento describe los pasos para integrar ISE con la tecnología Cisco Firepower.

Componentes Utilizados

Este documento utiliza los siguientes componentes en la configuración de ejemplo:

- Identity Services Engine (ISE) versión 2.1
- Firepower Management Center (FMC) versión 6.x
- Cisco Adaptive Security Appliance (ASA) 5506-X versión 9.6.2
- Módulo Cisco Adaptive Security Appliance (ASA) 5506-X Firepower, versión 6.1

Overview

Hay dos maneras para que un dispositivo de sensor detecte la Security Group Tag (SGT) asignada al tráfico:

1. Mediante asignación de IP de usuario
2. A través del etiquetado SGT en línea

El método de asignación de IP de usuario

Para garantizar que la información de TrustSec se utiliza para el control de acceso, la integración de ISE con un FMC se realiza a través de los siguientes pasos:

Paso 1: FMC recupera una lista de los grupos de seguridad de ISE.

Paso 2: Las políticas de control de acceso se crean en FMC que incluye grupos de seguridad como condición.

Paso 3: Cuando los terminales se autentican y autorizan con ISE, los datos de la sesión se publican en FMC.

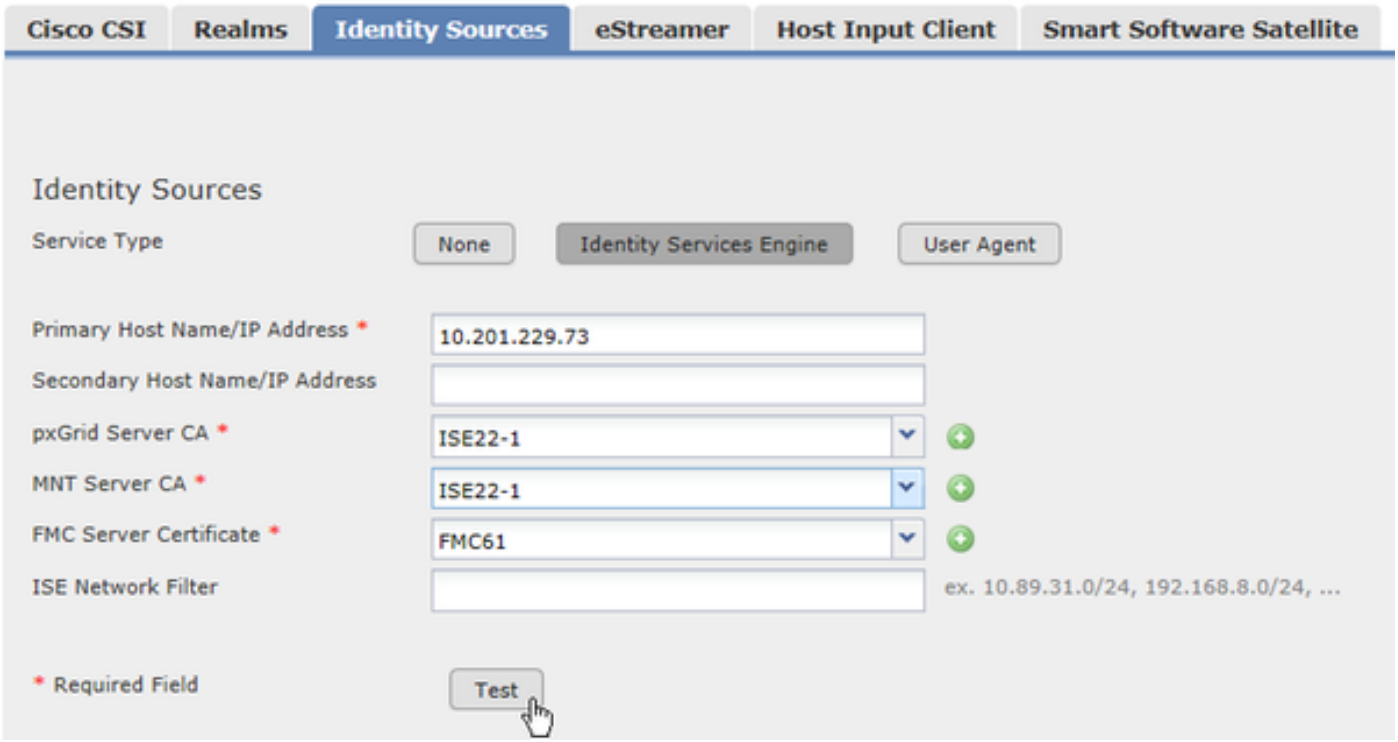
Paso 4: FMC crea un archivo de asignación User-IP-SGT y lo envía al sensor.

Paso 5: La dirección IP de origen del tráfico se utiliza para hacer coincidir el grupo de seguridad mediante los datos de sesión de la asignación IP de usuario.

Paso 6: Si el grupo de seguridad del origen de tráfico coincide con la condición de la política de control de acceso, el sensor toma las medidas correspondientes.

Un FMC recupera una lista SGT completa cuando la configuración para la integración de ISE se guarda en **System > Integration > Identity Sources > Identity Services Engine**.

> **Nota:** Al hacer clic en el botón **Prueba** (como se muestra a continuación), FMC no se activa para recuperar datos SGT.



La comunicación entre FMC e ISE se ve facilitada por ADI (Interfaz de directorio abstracto), que es un proceso único (sólo puede haber una instancia) que se ejecuta en FMC. Otros procesos en FMC se suscriben a ADI y solicitan información. Actualmente, el único componente que se suscribe a ADI es el correlador de datos.

FMC guarda la SGT en una base de datos local. La base de datos contiene tanto el nombre como el número de SGT, pero actualmente FMC utiliza un identificador único (ID de etiqueta segura) como identificador al procesar los datos de SGT. Esta base de datos también se propaga a los sensores.

Si se cambian los grupos de seguridad de ISE, como la eliminación o adición de grupos, ISE envía una notificación pxGrid a FMC para actualizar la base de datos SGT local.

Cuando un usuario se autentica con ISE y se autoriza con una etiqueta de grupo de seguridad, ISE notifica a FMC a través de pxGrid, proporcionando el conocimiento de que el usuario X del rango Y ha iniciado sesión con SGT Z. FMC toma la información e inserta en el archivo de asignación de IP de usuario. FMC utiliza un algoritmo para determinar el tiempo necesario para enviar la asignación adquirida a los sensores, en función de la carga de red presente.

> **Nota:** FMC no envía todas las entradas de asignación de IP de usuario a los sensores. Para que FMC impulse la asignación, primero debe tener conocimiento del usuario a través del rango. Si el usuario de la sesión no forma parte del rango, los sensores no aprenderán la información de asignación de este usuario. Se considera el soporte para usuarios que no son de rango para futuras versiones.

Firepower System versión 6.0 sólo admite asignación de IP-User-SGT. No se utilizan las etiquetas reales en el tráfico o la asignación SGT-IP aprendida de SXP en un ASA. Cuando el sensor capta el tráfico entrante, el proceso Snort toma la IP de origen y busca la correspondencia User-IP (que es impulsada por el módulo Firepower al proceso Snort), y encuentra la ID de etiqueta segura. Si coincide con la ID de SGT (no con el número de SGT) configurada en la política de control de acceso, la política se aplica al tráfico.

El método de etiquetado en línea

A partir de ASA versión 9.6.2 y ASA Firepower módulo 6.1, se soporta el etiquetado SGT en línea. Esto significa que el módulo Firepower ahora es capaz de extraer el número SGT directamente de los paquetes sin depender de la correspondencia User-IP proporcionada por FMC. Esto proporciona una solución alternativa para el control de acceso basado en TrustSec cuando el usuario no forma parte del rango (por ejemplo, dispositivos que no pueden autenticarse en 802.1x).

Con el método de etiquetado en línea, los sensores todavía responden en FMC para recuperar grupos SGT de ISE y empujar la base de datos SGT hacia abajo. Cuando el tráfico etiquetado con el número de grupo de seguridad alcanza el ASA, si el ASA se configura para confiar en el SGT entrante, la etiqueta se pasará al módulo Firepower a través del plano de datos. El módulo Firepower toma la etiqueta de los paquetes y la utiliza directamente para evaluar las políticas de control de acceso.

ASA debe tener una configuración TrustSec adecuada en la interfaz para recibir el tráfico etiquetado:

```
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
```

> **Nota:** Solo ASA versión 9.6.2 y posterior admite etiquetado en línea. Las versiones anteriores de un ASA no pasan la etiqueta de seguridad a través del plano de datos al módulo Firepower. Si un sensor admite etiquetado en línea, primero intentará extraer etiquetas del tráfico. Si el tráfico no está etiquetado, el sensor vuelve al método de asignación User-IP.

Resolución de problemas

Desde el shell restringido de un dispositivo Firepower

Para mostrar la política de control de acceso enviada desde FMC:

```
> 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
```

> **Nota:** Las etiquetas del grupo de seguridad especifican dos números: [7:6]. En este conjunto de números, "7" es el identificador único de la base de datos SGT local, que sólo es conocida por FMC y sensor. "6" es el número SGT real conocido por todas las partes.

Para ver los registros generados cuando SFR procesa el tráfico entrante y evalúa la política de acceso:

```
> 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
```

Ejemplo de firewall-engine-debug para el tráfico entrante con etiquetado en línea:

```
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
```

Desde el modo experto de un dispositivo Firepower

> **Precaución:** La siguiente instrucción puede afectar al rendimiento del sistema. Ejecute el comando sólo para solucionar problemas o cuando un ingeniero de soporte de Cisco solicite estos datos.

El módulo Firepower envía la asignación de IP de usuario al proceso de Snort local. Para verificar qué sabe Snort sobre la asignación, puede utilizar el siguiente comando para enviar la consulta a Snort:

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

Successfully commanded snort.
```

Para ver los datos, ingrese al modo experto:

```
> expert

admin@firepower:~$
```

Snort crea un archivo de volcado bajo el directorio /var/sf/detection_Engines/GUID/instance-x. El nombre del archivo de volcado es 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
-------------------
~
```

La salida anterior muestra que Snort conoce una dirección IP 10.201.229.94 que está asignada a la SGT ID 7, que es el número SGT 6 (Invitados).

Desde Firepower Management Center

Puede revisar los registros de ADI para verificar la comunicación entre FMC e ISE. Para encontrar los registros del componente adi, verifique el archivo /var/log/messages en FMC. Observará registros como los siguientes:

```
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
.
.
```