Comprensión del control de acceso TrustSec-basado con la potencia de fuego y el ISE

Contenido

Introducción

Cisco TrustSec utiliza marcar con etiqueta y asociar de las tramas Ethernet de la capa 2 para segregar el tráfico sin afectar a la infraestructura IP existente. El tráfico con Tag se puede tratar con las medidas de seguridad con el mayor granularity.

La integración entre el Identity Services Engine (ISE) y el centro de administración de la potencia de fuego (FMC) permite TrustSec que marca con etiqueta para ser comunicado de la autorización del cliente, que se puede utilizar por la potencia de fuego para aplicar las directivas del control de acceso basadas en la etiqueta del grupo de seguridad del cliente. Este documento discute los pasos para integrar el ISE con la tecnología de la potencia de fuego de Cisco.

Componentes Utilizados

Este documento utiliza después de los componentes en el ejemplo puesto:

- Versión 2.1 del Identity Services Engine (ISE)
- Versión 6.x del centro de administración de la potencia de fuego (FMC)
- Versión 9.6.2 adaptante 5506-X del dispositivo de seguridad de Cisco (ASA)
- Módulo adaptante de la potencia de fuego 5506-X del dispositivo de seguridad de Cisco (ASA), versión 6.1

Información general

Hay dos maneras para que un dispositivo sensor detecte la etiqueta del grupo de seguridad (SGT) asignada al tráfico:

1. A través de la asignación Usuario-IP
2. Con marcar con etiqueta en línea SGT

El método de la asignación Usuario-IP

Para asegurar la información de TrustSec se utiliza para el control de acceso, la integración del ISE con un FMC pasa con los pasos siguientes:

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

Paso 2: Las directivas del control de acceso se crean en FMC que incluya a los grupos de seguridad como condición.

Paso 3: Cuando los puntos finales autentican y autorizan con el ISE, los datos de la sesión se publican a FMC.

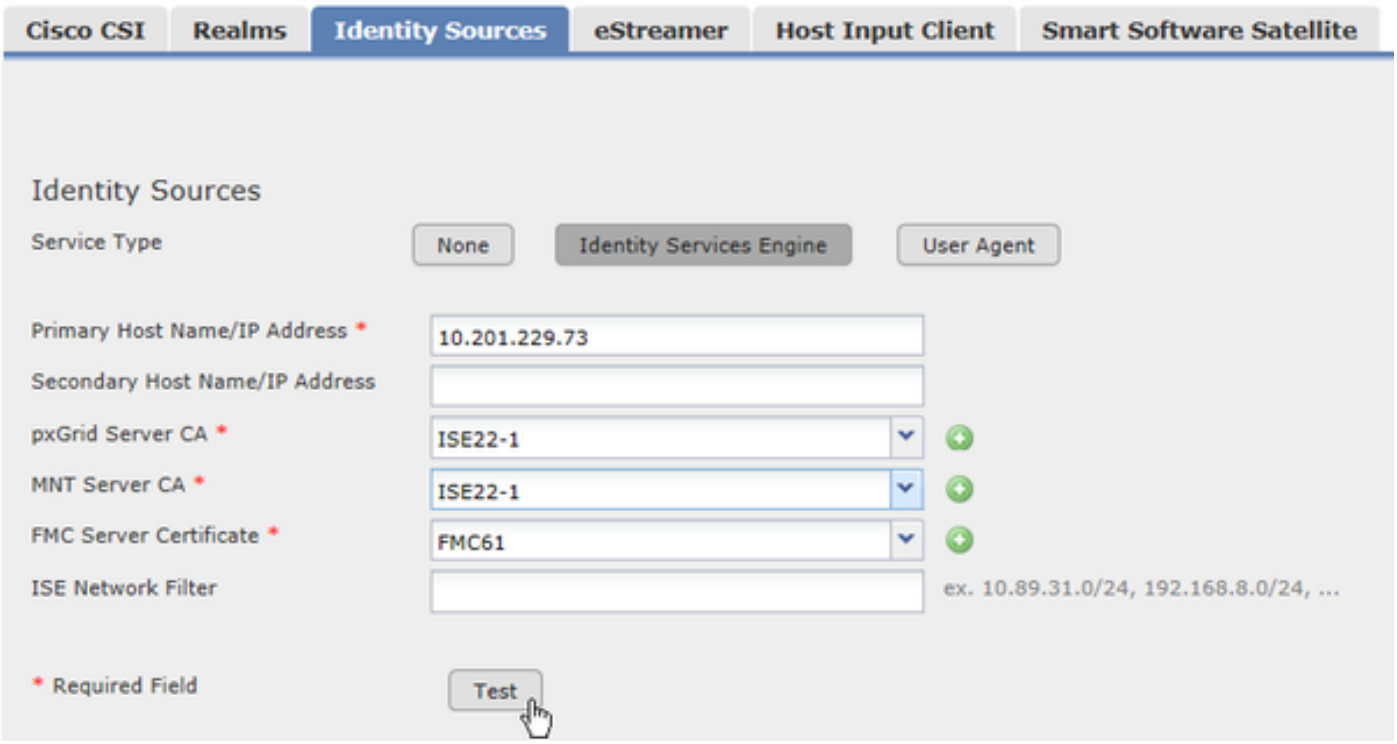
Paso 4: FMC construye un archivo de asignación Usuario-IP-SGT, y lo avanza al sensor.

Paso 5: La dirección IP de origen del tráfico se utiliza para hacer juego al grupo de seguridad que usa los datos de la sesión de la asignación Usuario-IP.

Paso 6: Si el grupo de seguridad de la fuente del tráfico hace juego la condición en la directiva del control de acceso, medidas son tomadas por el sensor por consiguiente.

Un FMC extrae una lista completa SGT cuando la configuración para la integración ISE se guarda bajo el **sistema > la integración > las fuentes > el Identity Services Engine de la identidad**.

> Nota: **El botón Test Button** que hace clic (como se muestra abajo) no acciona FMC para extraer los datos SGT.



La comunicación entre FMC y el ISE es facilitada por el ADI (interfaz abstracta del directorio), que es un proceso único (puede solamente haber un caso) que se ejecuta en FMC. Otros procesos en

FMC inscriben al ADI y piden la información. El único componente que inscribe al ADI es actualmente el correlador de los datos.

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

Si los grupos de seguridad ISE se cambian, por ejemplo el retiro o la adición de grupos, ISE avanza una notificación del pxGrid a FMC para poner al día la base de datos local SGT.

Cuando un usuario autentica con el ISE y autoriza con una etiqueta del grupo de seguridad, el ISE notifica FMC a través del pxGrid, proporcionando al conocimiento que el usuario que X del reino Y ha abierto una sesión con SGT Z. FMC toma la información y los separadores de millares en el archivo de asignación usuario-IP. FMC utiliza un algoritmo para determinar la época de avanzar asociar adquirido a los sensores, dependiendo de cuánta carga de la red está presente.

> Nota: FMC no avanza todas las entradas de la asignación Usuario-IP a los sensores. Para que FMC avance la asignación, debe primero tener conocimiento del usuario con el reino. Si el usuario en la sesión no es parte del reino, los sensores no aprenderán la información de mapeo de este usuario. El soporte para los usuarios del NON-reino se considera para las futuras versiones.

La versión del sistema 6.0 de la potencia de fuego soporta solamente la asignación del IP-usuario-SGT. Las etiquetas reales en el tráfico, o el asociar SGT-IP aprendido de SXP en un ASA no se utilizan. Cuando el sensor coge el tráfico entrante, el proceso del Snort toma el IP de la fuente y mira para arriba la asignación Usuario-IP (que es avanzada por el módulo de la potencia de fuego al proceso del Snort), y encuentra la etiqueta segura ID. Si hace juego el SGT ID (no número SGT) configurado en la directiva del control de acceso, después la directiva se aplica al tráfico.

El método que marca con etiqueta en línea

A partir del módulo 6.1 de la Versión de ASA 9.6.2 y de la potencia de fuego ASA, se soporta el marcar con etiqueta en línea SGT. Esto significa que el módulo de la potencia de fuego es capaz ahora de extraer el número SGT directamente de los paquetes sin la confianza en la asignación Usuario-IP proporcionada por FMC. Esto proporciona una solución alternativa para el control de acceso TrustSec-basado cuando el usuario no es parte del reino (tal como dispositivos no capaces de la autenticación del 802.1x).

Con el método que marca con etiqueta en línea, los sensores todavía contestan en FMC para extraer a los grupos SGT del ISE y para empujar la base de datos SGT hacia abajo. Cuando el tráfico marcado con etiqueta con el número de grupo de seguridad alcanza el ASA, si el ASA se configura para confiar en el SGT entrante, la etiqueta será pasada al módulo de la potencia de fuego a través del dataplane. El módulo de la potencia de fuego toma la etiqueta de los paquetes y la utiliza directamente para evaluar las directivas del control de acceso.

El ASA debe tener configuración apropiada de TrustSec en la interfaz para recibir el tráfico con Tag:

```
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: Solamente Versión de ASA 9.6.2 y el marcar con etiqueta en línea de soportes más altos. Las versiones anteriores de un ASA no pasan la etiqueta de la Seguridad a través del dataplane al módulo de la potencia de fuego. Si un sensor soporta en línea marcar con etiqueta, primero intentará extraer la etiqueta del tráfico. Si el tráfico no se marca con etiqueta, el sensor recurre al método de la asignación Usuario-IP.

Resolución de problemas

Del shell restricto de un dispositivo de la potencia de fuego

Para visualizar el Policy Pushed del control de acceso de FMC:

```
> 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
```

Nota: Las etiquetas del grupo de seguridad especifican dos números: `[7:6]`. En este conjunto de números, el "`7`" es el ID único de la base de datos local SGT, que se sabe solamente a FMC y al sensor. el "`6`" es el número real SGT sabido a todos los partidos.

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

```
> 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 del Firewall-motor-`debug` para el tráfico entrante con en línea marcar con etiqueta:

```
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
```

Del Modo experto de un dispositivo de la potencia de fuego

> Precaución: La instrucción siguiente puede afectar el rendimiento del sistema. Funcione con el comando solamente para el propósito de Troubleshooting, o cuando las peticiones de un ingeniero de soporte de Cisco estos datos.

El módulo de la potencia de fuego avanza el Usuario-IP que asocia al proceso local del Snort. Para verificar qué Snort sabe sobre la asignación, usted puede utilizar el siguiente comando de enviar la interrogación para resoplar:

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

Successfully commanded snort.
```

Para ver los datos, ingrese al Modo experto:

```
> expert

admin@firepower:~$
```

El Snort crea un archivo de volcado bajo directorio de `/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 antedicha muestra que el Snort es consciente de una dirección IP 10.201.229.94 cuál se asocia a SGT ID 7, que es SGT número 6 (invitados).

Del centro de administración de la potencia de fuego

Usted puede revisar los registros ADI para verificar la comunicación entre FMC y el ISE. Para encontrar los registros del componente `adi`, marque el archivo de `/var/log/messages` en FMC. Usted notará los registros como abajo:

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>