Présentation du contrôle d'accès basé sur TrustSec avec FirePower et ISE

Contenu

Introduction

Cisco TrustSec utilise le marquage et le mappage des trames Ethernet de couche 2 pour séparer le trafic sans affecter l'infrastructure IP existante. Le trafic étiqueté peut être traité avec des mesures de sécurité plus précises.

L'intégration entre Identity Services Engine (ISE) et Firepower Management Center (FMC) permet de communiquer le balisage TrustSec à partir de l'autorisation du client, qui peut être utilisé par Firepower pour appliquer des stratégies de contrôle d'accès basées sur la balise Security Group du client. Ce document décrit les étapes à suivre pour intégrer ISE à la technologie Cisco Firepower.

Components Used

Ce document utilise les composants suivants dans l'exemple de configuration :

- Identity Services Engine (ISE) version 2.1
- Firepower Management Center (FMC) version 6.x
- Appareil de sécurité adaptatif Cisco (ASA) 5506-X version 9.6.2
- Module Cisco Adaptive Security Appliance (ASA) 5506-X Firepower, version 6.1

Aperçu

Il existe deux façons pour un périphérique capteur de détecter la balise SGT (Security Group Tag) attribuée au trafic :

1. Par le mappage des adresses IP des utilisateurs
2. Par marquage SGT en ligne

Méthode de mappage utilisateur-IP

Pour s'assurer que les informations TrustSec sont utilisées pour le contrôle d'accès, l'intégration d'ISE à une FMC passe par les étapes suivantes :

Étape 1 : FMC récupère une liste des groupes de sécurité dans ISE.

Étape 2 : Les stratégies de contrôle d'accès sont créées sur FMC qui inclut les groupes de sécurité comme condition.

Étape 3 : Lorsque les terminaux s'authentifient et autorisent avec ISE, les données de session sont publiées sur FMC.

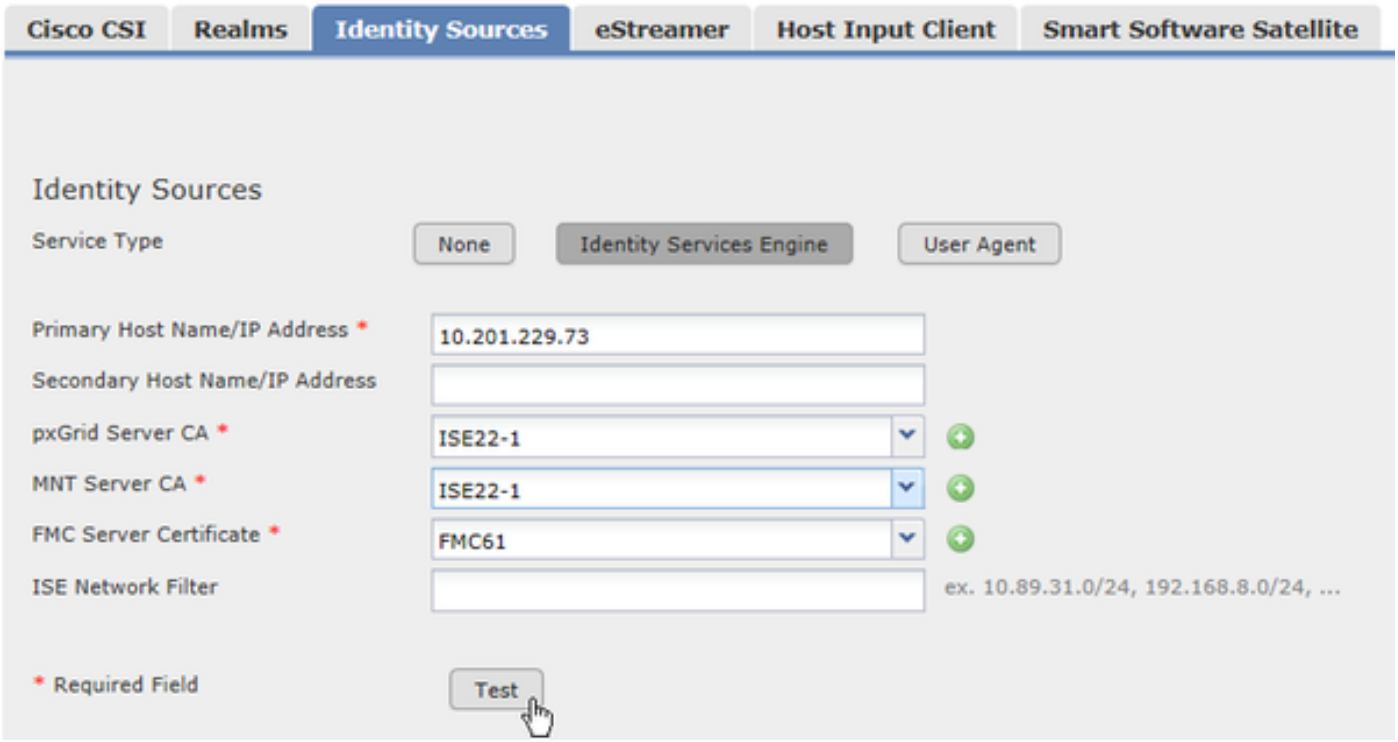
Étape 4 : FMC crée un fichier de mappage User-IP-SGT et le pousse au capteur.

Étape 5 : L'adresse IP source du trafic est utilisée pour faire correspondre le groupe de sécurité à l'aide des données de session du mappage User-IP.

Étape 6 : Si le groupe de sécurité de la source de trafic correspond à la condition de la stratégie de contrôle d'accès, l'action est effectuée par le capteur en conséquence.

Une FMC récupère une liste SGT complète lorsque la configuration pour l'intégration ISE est enregistrée sous **System > Integration > Identity Sources > Identity Services Engine**.

> **Note**: Le fait de cliquer sur le bouton **Test** (comme illustré ci-dessous) ne déclenche pas FMC pour récupérer les données SGT.



La communication entre FMC et ISE est facilitée par ADI (Abstract Directory Interface), qui est un processus unique (il ne peut y avoir qu'une seule instance) exécuté sur FMC. D'autres processus sur FMC s'abonnent à ADI et demandent des informations. Actuellement, le seul composant qui s'abonne à ADI est le corrélateur de données.

FMC enregistre le SGT dans une base de données locale. La base de données contient à la fois le nom et le numéro SGT, mais actuellement FMC utilise un identificateur unique (ID de balise sécurisée) comme handle lors du traitement des données SGT. Cette base de données est également propagée aux capteurs.

Si des groupes de sécurité ISE sont modifiés, tels que la suppression ou l'ajout de groupes, ISE envoie une notification pxGrid à FMC pour mettre à jour la base de données SGT locale.

Lorsqu'un utilisateur s'authentifie avec ISE et autorise avec une balise de groupe de sécurité, ISE informe FMC via pxGrid, en indiquant que l'utilisateur X du domaine Y s'est connecté avec SGT Z. FMC prend les informations et les insère dans le fichier de mappage utilisateur-IP. FMC utilise un algorithme pour déterminer la durée de transmission du mappage acquis aux capteurs, selon la charge réseau présente.

> **Note**: FMC n'envoie pas toutes les entrées de mappage utilisateur-IP aux capteurs. Pour que FMC puisse pousser le mappage, il doit d'abord avoir connaissance de l'utilisateur via le domaine. Si l'utilisateur de la session ne fait pas partie du domaine, les capteurs n'apprendront pas les informations de mappage de cet utilisateur. La prise en charge des utilisateurs autres que Realm est envisagée pour les versions futures.

Firepower System Version 6.0 prend uniquement en charge le mappage IP-User-SGT. Les balises réelles dans le trafic ou le mappage SGT-IP appris de SXP sur un ASA ne sont pas utilisés. Lorsque le capteur récupère le trafic entrant, le processus Snort prend l'adresse IP source et recherche le mappage User-IP (qui est poussé par le module Firepower au processus Snort), et trouve l'ID de balise sécurisée. S'il correspond à l'ID SGT (et non au numéro SGT) configuré dans la stratégie de contrôle d'accès, la stratégie est appliquée au trafic.

Méthode d'étiquetage en ligne

Depuis ASA version 9.6.2 et ASA Firepower module 6.1, l'étiquetage SGT en ligne est pris en charge. Cela signifie que le module Firepower est désormais capable d'extraire le numéro SGT directement des paquets sans compter sur le mappage User-IP fourni par FMC. Cela fournit une solution alternative pour le contrôle d'accès basé sur TrustSec lorsque l'utilisateur ne fait pas partie du domaine (comme les périphériques ne prenant pas en charge l'authentification 802.1x).

Avec la méthode d'étiquetage en ligne, les capteurs répondent toujours sur FMC pour récupérer les groupes SGT à partir d'ISE et pousser la base de données SGT vers le bas. Lorsque le trafic étiqueté avec le numéro de groupe de sécurité atteint l'ASA, si l'ASA est configuré pour faire confiance à la SGT entrante, la balise sera transmise au module Firepower via le plan de données. Le module Firepower prend la balise des paquets et l'utilise directement pour évaluer les stratégies de contrôle d'accès.

ASA doit avoir une configuration TrustSec appropriée sur l'interface pour recevoir le trafic étiqueté :

```
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
```

Note: Seul ASA version 9.6.2 et ultérieure prend en charge le marquage en ligne. Les versions antérieures d'un ASA ne transmettent pas le Security Tag par le plan de données au module Firepower. Si un capteur prend en charge le marquage en ligne, il tente d'abord d'extraire la balise du trafic. Si le trafic n'est pas étiqueté, le capteur revient à la méthode de mappage User-IP.

Dépannage

Àpartir de l'interpréteur de commandes restreint d'un périphérique Firepower

Pour afficher la stratégie de contrôle d'accès à partir de 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
```

Note: Les balises de groupe de sécurité indiquent deux numéros : [7:6]. Dans cet ensemble de nombres, "7" est l'ID unique de la base de données SGT locale, qui est connue seulement de FMC et du capteur. "6" est le numéro SGT réel connu de toutes les parties.

Pour afficher les journaux générés lorsque SFR traite le trafic entrant et évalue la stratégie d'accès :

```
> 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
```

Exemple de firewall-engine-debug pour le trafic entrant avec marquage en ligne :

```
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
```

En mode Expert d'un périphérique Firepower

> **Attention** : Les instructions suivantes peuvent affecter les performances du système. Exécutez la commande uniquement à des fins de dépannage ou lorsqu'un ingénieur d'assistance Cisco demande ces données.

Le module Firepower transfère le mappage utilisateur-IP au processus Snort local. Pour vérifier ce que Snort sait sur le mappage, vous pouvez utiliser la commande suivante pour envoyer une requête à Snort :

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

Successfully commanded snort.
```

Pour afficher les données, passez en mode expert :

```
> expert

admin@firepower:~$
```

Snort crée un fichier de vidage sous le répertoire /var/sf/detection_engine/GUID/instance-x. Le nom du fichier de vidage est 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
-------------------
~
```

Le résultat ci-dessus montre que Snort connaît une adresse IP 10.201.229.94 qui est mappée à l'ID SGT 7, qui est le numéro SGT 6 (Invités).

Depuis Firepower Management Center

Vous pouvez consulter les journaux ADI pour vérifier la communication entre FMC et ISE. Pour rechercher les journaux du composant adi, consultez le fichier /var/log/messages sur FMC. Vous remarquerez les journaux comme ci-dessous :

```
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
.
.
```