Compréhension du contrôle d'accès basé sur TrustSec avec la puissance de feu et l'ISE

Contenu

Introduction

Le Cisco TrustSec utilise l'étiquetage et la cartographie des trames Ethernet de la couche 2 pour isoler le trafic sans affecter l'infrastructure IP existante. Le trafic étiqueté peut être traité avec des mesures de sécurité avec une plus grande finesse.

L'intégration entre le Cisco Identity Services Engine (ISE) et le centre de Gestion de puissance de feu (FMC) permet TrustSec étiquetant pour être communiqué de l'autorisation de client, qui peut être utilisée par puissance de feu pour appliquer des stratégies de contrôle d'accès basées sur la balise du groupe de sécurité du client. Ce document discute les étapes pour intégrer ISE avec la technologie de puissance de feu de Cisco.

Composants utilisés

Ce document utilise les composants suivants dans l'exemple installé :

- Version 2.1 du Cisco Identity Services Engine (ISE)
- Version 6.x du centre de Gestion de puissance de feu (FMC)
- Version 9.6.2 5506-X de l'appliance de sécurité adaptable Cisco (ASA)
- Module de la puissance de feu 5506-X de l'appliance de sécurité adaptable Cisco (ASA), version 6.1

Aperçu

Il y a deux manières pour qu'un périphérique de capteur détecte la balise de groupe de sécurité (SGT) assignée au trafic :

1. Par le mappage Utilisateur-IP
2. Par l'étiquetage de l'en ligne SGT

La méthode du mappage Utilisateur-IP

Pour assurer les informations de TrustSec est utilisé pour le contrôle d'accès, l'intégration d'ISE avec un FMC passe par les étapes suivantes :

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

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

Étape 3 : Quand les points finaux authentifient et autorisent avec ISE, des données de session sont éditées à FMC.

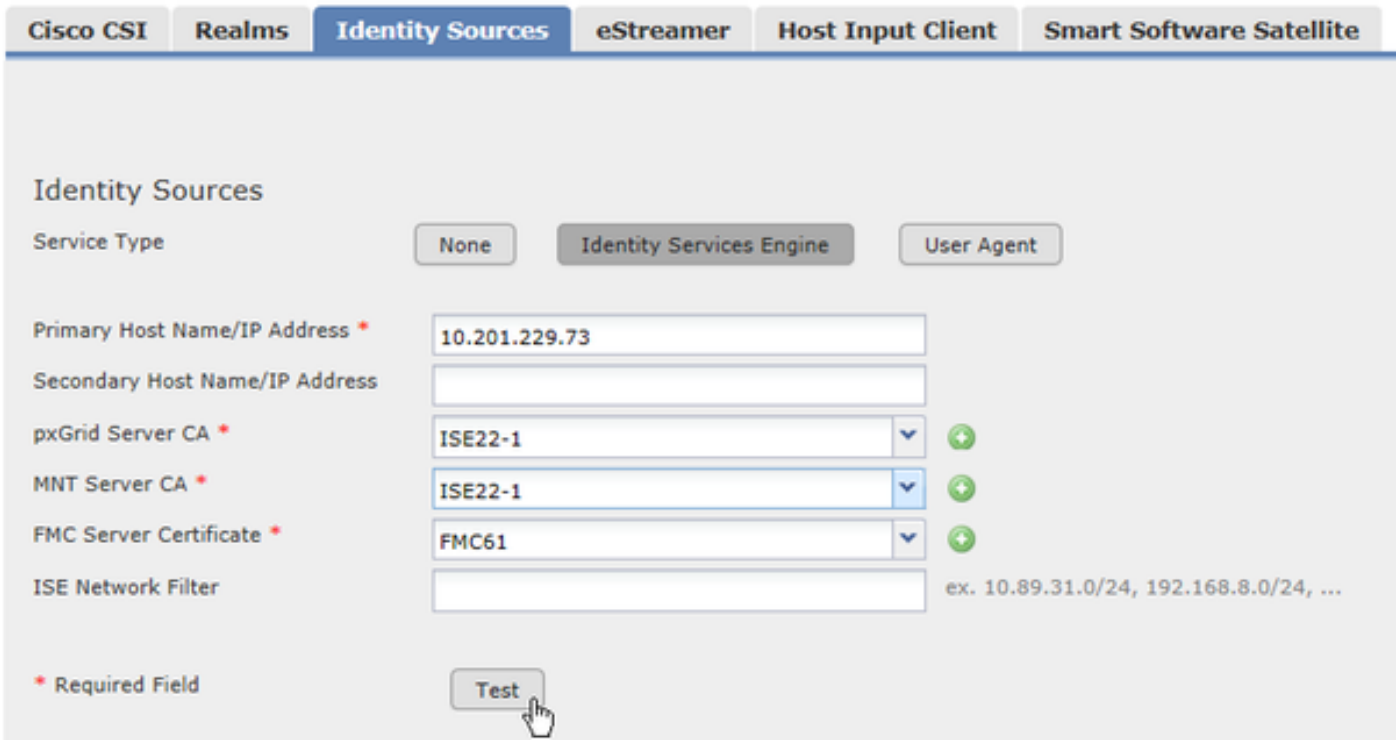
Étape 4 : FMC établit un fichier du mappage Utilisateur-IP-SGT, et le pousse au capteur.

Étape 5 : L'adresse IP source du trafic est utilisée pour concurrencer le groupe de sécurité utilisant des données de session du mappage Utilisateur-IP.

Étape 6 : Si le groupe de sécurité de la source de trafic apparie la condition dans la stratégie de contrôle d'accès, une mesure est prise par le capteur en conséquence.

Un FMC récupère une liste complète SGT quand la configuration pour l'intégration ISE est enregistrée sous le **système > l'intégration > les sources > le Cisco Identity Services Engine d'identité**.

> Remarque: Cliquer sur la touche "TEST" (comme affiché ci-dessous) ne déclenche pas FMC pour récupérer des données SGT.



La transmission entre FMC et ISE est facilitée par l'ADI (interface abstraite de répertoire), qui est

une seule (il peut seulement y avoir un exemple) exécution de processus sur FMC. D'autres processus sur FMC s'abonnent à l'ADI et demandent les informations. Actuellement le seul composant qui s'abonne à l'ADI est le corrélateur de données.

FMC enregistre le SGT dans une base de données locale. La base de données contient le les deux le nom et le nombre SGT, mais actuellement FMC utilise un identifiant unique (ID sécurisé de balise) en tant que traitement en traitant des données SGT. Cette base de données est également propagée aux capteurs.

Si des groupes de sécurité ISE sont changés, comme la suppression ou l'ajout des groupes, ISE pousse une notification de pxGrid à FMC pour mettre à jour la base de données des gens du pays SGT.

Quand un utilisateur authentifie avec ISE et autorise avec une balise de groupe de sécurité, ISE informe FMC par le pxGrid, fournissant la connaissance que l'utilisateur que X du royaume Y a ouvert une session avec SGT Z. FMC prend les informations et les insertions dans le mappage utilisateur-IP classent. FMC emploie un algorithme pour déterminer l'heure de pousser le mappage saisi aux capteurs, selon combien charge du réseau coûte présente.

> Remarque: FMC ne pousse pas toutes les entrées du mappage Utilisateur-IP aux capteurs. Pour que FMC pousse le mappage, il doit d'abord avoir la connaissance de l'utilisateur par le royaume. Si l'utilisateur en session n'est pas une partie du royaume, les capteurs n'apprendront pas les informations de mappage de cet utilisateur. Le soutien des utilisateurs de non-royaume est considéré pour des versions futures.

La version 6.0 de système de puissance de feu prend en charge seulement la cartographie d'IP-utilisateur-SGT. Des balises d'effectif dans le trafic, ou le mappage SGT-IP appris de SXP sur une ASA ne sont pas utilisés. Quand le capteur prend le trafic entrant, le processus de renifler jette le source ip et les consultations le mappage Utilisateur-IP (qui est poussé par le module de puissance de feu au processus de renifler), et trouve l'ID sécurisé de balise. S'il apparie l'ID SGT (pas nombre SGT) configuré dans la stratégie de contrôle d'accès, alors la stratégie est appliquée au trafic.

La méthode d'étiquetage intégrée

Àpartir du module 6.1 de version 9.6.2 ASA et de puissance de feu ASA, l'étiquetage de l'en ligne SGT est pris en charge. Ceci signifie que le module de puissance de feu est maintenant capable d'extraire le nombre SGT directement des paquets sans compter sur le mappage Utilisateur-IP fourni par FMC. Ceci fournit une solution alternative pour le contrôle d'accès basé sur TrustSec quand l'utilisateur n'est pas une partie du royaume (tel que des périphériques non capables de l'authentification de 802.1x).

Avec la méthode d'étiquetage intégrée, les capteurs répond toujours sur FMC pour récupérer des groupes SGT d'ISE et pour abaisser la base de données SGT. Quand le trafic étiqueté avec le nombre de groupe de sécurité atteint l'ASA, si l'ASA est configurée pour faire confiance au SGT entrant, la balise sera passée au module de puissance de feu par le dataplane. Le module de puissance de feu prend la balise des paquets et l'emploie directement pour évaluer des stratégies de contrôle d'accès.

L'ASA doit avoir la configuration appropriée de TrustSec sur l'interface afin de 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
```

Remarque: Seulement la version 9.6.2 et ultérieures ASA prend en charge l'étiquetage intégré. Les versions antérieures d'une ASA ne passent pas la balise de Sécurité par le dataplane au module de puissance de feu. Si un capteur prend en charge l'étiquetage intégré, il essayera d'abord d'extraire la balise du trafic. Si le trafic n'est pas étiqueté, le capteur retombe à la méthode du mappage Utilisateur-IP.

Dépannage

Du shell restreint d'un périphérique de puissance de feu

Pour afficher la stratégie de contrôle d'accès poussée 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
```

Remarque: Les balises de groupe de sécurité spécifie deux nombres : `[7:6]`. Dans cet ensemble de nombres, « `7`" est l'identificateur unique de la base de données des gens du pays SGT, qui est seulement connue à FMC et à capteur. « `6`" est le nombre de l'effectif SGT connu de tous les interlocuteurs.

Pour visualiser des logs générés quand le trafic entrant de processus SFR et stratégie de évaluation 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 Pare-feu-engine-`debug` pour le trafic entrant avec l'étiquetage d'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
```

Du mode expert d'un périphérique de puissance de feu

> **Attention** : L'instruction suivante peut affecter la performance du système. Exécutez la commande seulement pour dépannage du but, ou quand des demandes d'un ingénieur d'assistance technique de Cisco de ces données.

L'Utilisateur-IP de poussers de module de puissance de feu traçant aux gens du pays reniflent le processus. Pour vérifier ce qui reniflent sait le mappage, vous peut utiliser la commande suivante d'envoyer la requête pour renifler :

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

Successfully commanded snort.
```

Pour visualiser les données, entrez au mode expert :

```
> expert

admin@firepower:~$
```

Reniflez crée un fichier de vidage mémoire sous le répertoire de `/var/sf/detection_engines/GUID/instance-x`. Le nom du fichier de vidage mémoire 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
-------------------
~
```

La sortie ci-dessus prouve que Snort se rend compte d'une adresse IP 10.201.229.94 ce qui est tracé à l'ID 7 SGT, qui est SGT le numéro 6 (invités).

Du centre de Gestion de puissance de feu

Vous pouvez passer en revue les logs ADI pour vérifier la transmission entre FMC et ISE. Pour trouver les logs du composant `ADI`, vérifiez le fichier de `/var/log/messages` sur FMC. Vous noterez des logs 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...
.
.
<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>
```