Informazioni sul controllo degli accessi basato su TrustSec con FirePower e ISE

Sommario

Introduzione

Cisco TrustSec utilizza la codifica e la mappatura dei frame Ethernet di layer 2 per segregare il traffico senza influire sull'infrastruttura IP esistente. Il traffico contrassegnato può essere gestito con misure di sicurezza più dettagliate.

L'integrazione tra Identity Services Engine (ISE) e Firepower Management Center (FMC) consente la comunicazione dei tag TrustSec dall'autorizzazione del client, che può essere utilizzata da Firepower per applicare i criteri di controllo dell'accesso in base al tag del gruppo di sicurezza del client. In questo documento viene descritto come integrare ISE con la tecnologia Cisco Firepower.

Componenti usati

In questo documento vengono utilizzati i seguenti componenti nell'impostazione di esempio:

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

Panoramica

Un dispositivo sensore può rilevare in due modi il codice SGT (Security Group Tag) assegnato al traffico:

1. Tramite mapping utente-IP
2. Tramite tagging SGT inline

Metodo di mapping utente-IP

Per garantire che le informazioni TrustSec vengano utilizzate per il controllo degli accessi, l'integrazione di ISE con un FMC prevede le seguenti fasi:

Passaggio 1: FMC recupera un elenco dei gruppi di sicurezza da ISE.

Passaggio 2: I criteri di controllo di accesso vengono creati in FMC che include i gruppi di sicurezza come condizione.

Passaggio 3: Quando gli endpoint vengono autenticati e autorizzati con ISE, i dati della sessione vengono pubblicati in FMC.

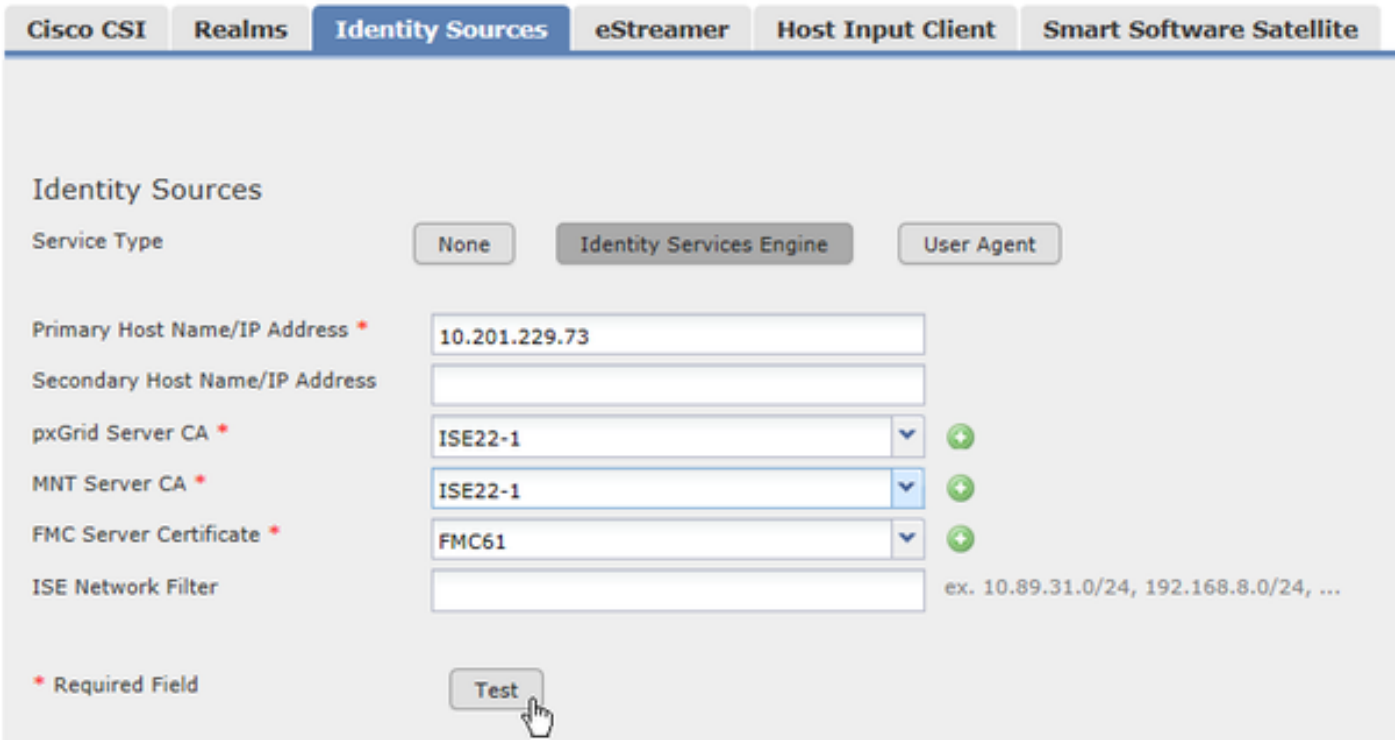
Passaggio 4: FMC crea un file di mappatura User-IP-SGT e lo invia al sensore.

Passaggio 5: L'indirizzo IP di origine del traffico viene utilizzato per creare una corrispondenza con il gruppo di sicurezza utilizzando i dati della sessione del mapping User-IP.

Passaggio 6: Se il gruppo di sicurezza dell'origine del traffico soddisfa la condizione specificata nei criteri di controllo di accesso, l'azione verrà eseguita dal sensore di conseguenza.

Un FMC recupera un elenco SGT completo quando la configurazione per l'integrazione ISE viene salvata in **Sistema > Integrazione > Origini identità > Identity Services Engine**.

> **Nota:** Se si fa clic sul pulsante **Test** (come illustrato di seguito), FMC non viene attivato per recuperare i dati SGT.



La comunicazione tra FMC e ISE è facilitata dall'interfaccia ADI (Abstract Directory Interface), che è un processo unico (può esistere una sola istanza) in esecuzione su FMC. Altri processi del CCP sottoscrivono ADI e richiedono informazioni. Attualmente l'unico componente che sottoscrive ADI è il correlatore dati.

FMC salva il SGT in un database locale. Il database contiene sia il nome che il numero SGT, ma attualmente FMC utilizza un identificatore univoco (Secure Tag ID) come handle durante l'elaborazione dei dati SGT. Questo database viene anche propagato ai sensori.

Se i gruppi di sicurezza ISE vengono modificati, ad esempio la rimozione o l'aggiunta di gruppi, ISE invia una notifica pxGrid a FMC per aggiornare il database SGT locale.

Quando un utente esegue l'autenticazione con ISE e dispone di un tag per il gruppo di sicurezza, ISE avvisa FMC tramite pxGrid, comunicando che l'utente X dell'area di autenticazione Y ha eseguito l'accesso con SGT Z. FMC accetta le informazioni e le inserisce nel file di mapping IP dell'utente. FMC utilizza un algoritmo per determinare il tempo necessario per inviare il mapping acquisito ai sensori, a seconda del carico di rete presente.

> **Nota:** FMC non esegue il push di tutte le voci di mapping User-IP nei sensori. Per eseguire il push della mappatura da parte di FMC, è necessario innanzitutto conoscere l'utente tramite il realm. Se l'utente nella sessione non fa parte del realm, i sensori non apprenderanno le informazioni di mappatura di questo utente. Il supporto per utenti non appartenenti al realm è previsto per le versioni future.

Firepower System versione 6.0 supporta solo il mapping IP-User-SGT. Non vengono usati i tag effettivi nel traffico o il mapping SGT-IP appreso da SXP su un'appliance ASA. Quando il sensore rileva il traffico in entrata, il processo Snort rileva l'IP di origine e cerca la mappatura User-IP (che viene spinta dal modulo Firepower al processo Snort) e trova l'ID del tag sicuro. Se corrisponde all'ID SGT (non al numero SGT) configurato nei criteri di controllo di accesso, i criteri vengono applicati al traffico.

Metodo di tag in linea

A partire dalla versione 9.6.2 di ASA e dal modulo Firepower 6.1 di ASA, è supportata la codifica Inline SGT. Ciò significa che il modulo Firepower è ora in grado di estrarre il numero SGT direttamente dai pacchetti senza affidarsi alla mappatura User-IP fornita da FMC. In questo modo viene fornita una soluzione alternativa per il controllo degli accessi basato su TrustSec quando l'utente non fa parte del realm (ad esempio, dispositivi che non supportano l'autenticazione 802.1x).

Con il metodo Inline Tagging, i sensori rispondono ancora su FMC per recuperare i gruppi SGT da ISE e spingere il database SGT verso il basso. Quando il traffico contrassegnato con il numero del gruppo di sicurezza raggiunge l'ASA, se l'ASA è configurata in modo da considerare attendibile il SGT in arrivo, il tag viene passato al modulo Firepower attraverso il dataplane. Il modulo Firepower preleva il tag dai pacchetti e lo utilizza direttamente per valutare le policy di controllo dell'accesso.

Per ricevere il traffico contrassegnato, l'ASA deve avere una configurazione TrustSec corretta sull'interfaccia:

```
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 le appliance ASA versione 9.6.2 e successive supportano l'assegnazione di tag in linea. Le versioni precedenti di un'ASA non passano il tag di sicurezza attraverso la corsia dati al modulo Firepower. Se un sensore supporta l'applicazione di tag in linea, tenterà prima di estrarre il tag dal traffico. Se il traffico non è contrassegnato, il sensore torna al metodo di mappatura User-IP.

Risoluzione dei problemi

Dalla shell limitata di un dispositivo Firepower

Per visualizzare i criteri di controllo di accesso inviati da 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: Le etichette del gruppo di sicurezza specificano due numeri: [7:6]. In questa serie di numeri, "7" è l'ID univoco del database SGT locale, che è noto solo a FMC e sensore. "6" è il numero SGT effettivo noto a tutte le parti.

Per visualizzare i log generati quando SFR elabora il traffico in entrata e valuta i criteri di accesso:

```
> 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
```

Esempio di firewall-engine-debug per il traffico in entrata con tag in linea:

```
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
```

Dalla modalità Expert di una periferica Firepower

> **Attenzione:** Le istruzioni seguenti possono influire sulle prestazioni del sistema. Eseguire il comando solo per risolvere i problemi o quando richiesto da un tecnico dell'assistenza Cisco.

Il modulo Firepower invia il mapping User-IP al processo Snort locale. Per verificare le informazioni di Snort sul mapping, è possibile utilizzare il comando seguente per inviare una query a Snort:

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

Successfully commanded snort.
```

Per visualizzare i dati, accedere alla modalità Expert:

```
> expert

admin@firepower:~$
```

Snort crea un file dump nella directory /var/sf/detection_engine/GUID/instance-x. Il nome del file di dump è 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
-------------------
~
```

L'output precedente mostra che Snort è a conoscenza di un indirizzo IP 10.201.229.94 mappato

all'ID SGT 7, che è il numero SGT 6 (Guests).

Da Firepower Management Center

Èpossibile esaminare i registri ADI per verificare la comunicazione tra FMC e ISE. Per trovare i registri del componente adi, controllare il file /var/log/messages su FMC. Si noteranno registri come di seguito:

```
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
.
.
```