TrustSec-basierte Zugriffskontrolle mit FirePower und ISE

Inhalt

Einführung

Cisco TrustSec nutzt Tagging und Mapping von Layer-2-Ethernet-Frames, um den Datenverkehr zu trennen, ohne die vorhandene IP-Infrastruktur zu beeinträchtigen. Markierter Datenverkehr kann mit Sicherheitsmaßnahmen mit größerer Genauigkeit behandelt werden.

Die Integration zwischen der Identity Services Engine (ISE) und dem FirePOWER Management Center (FMC) ermöglicht die Kommunikation von TrustSec-Tagging über die Client-Autorisierung, die von FirePOWER zur Anwendung von Zugriffskontrollrichtlinien auf Basis der Security Group Tag des Kunden verwendet werden kann. In diesem Dokument werden die Schritte zur Integration der ISE in die Cisco FirePOWER-Technologie erläutert.

Verwendete Komponenten

In diesem Dokument werden die folgenden Komponenten in der Beispieleinrichtung verwendet:

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

Übersicht

Es gibt zwei Möglichkeiten, wie ein Sensorgerät die dem Datenverkehr zugewiesene Security Group Tag (SGT) erkennt:

1. Über die Benutzer-IP-Zuordnung
2. Durch Inline-SGT-Tagging

Die Benutzer-IP-Zuordnungsmethode

Um sicherzustellen, dass die TrustSec-Informationen für die Zugriffskontrolle verwendet werden, wird die Integration der ISE mit einem FMC wie folgt durchgeführt:

Schritt 1: FMC ruft eine Liste der Sicherheitsgruppen von der ISE ab.

Schritt 2: Zugriffskontrollrichtlinien werden auf dem FMC erstellt, das Sicherheitsgruppen als Bedingung enthält.

Schritt 3: Bei der Authentifizierung und Autorisierung von Endpunkten mit der ISE werden Sitzungsdaten an das FMC veröffentlicht.

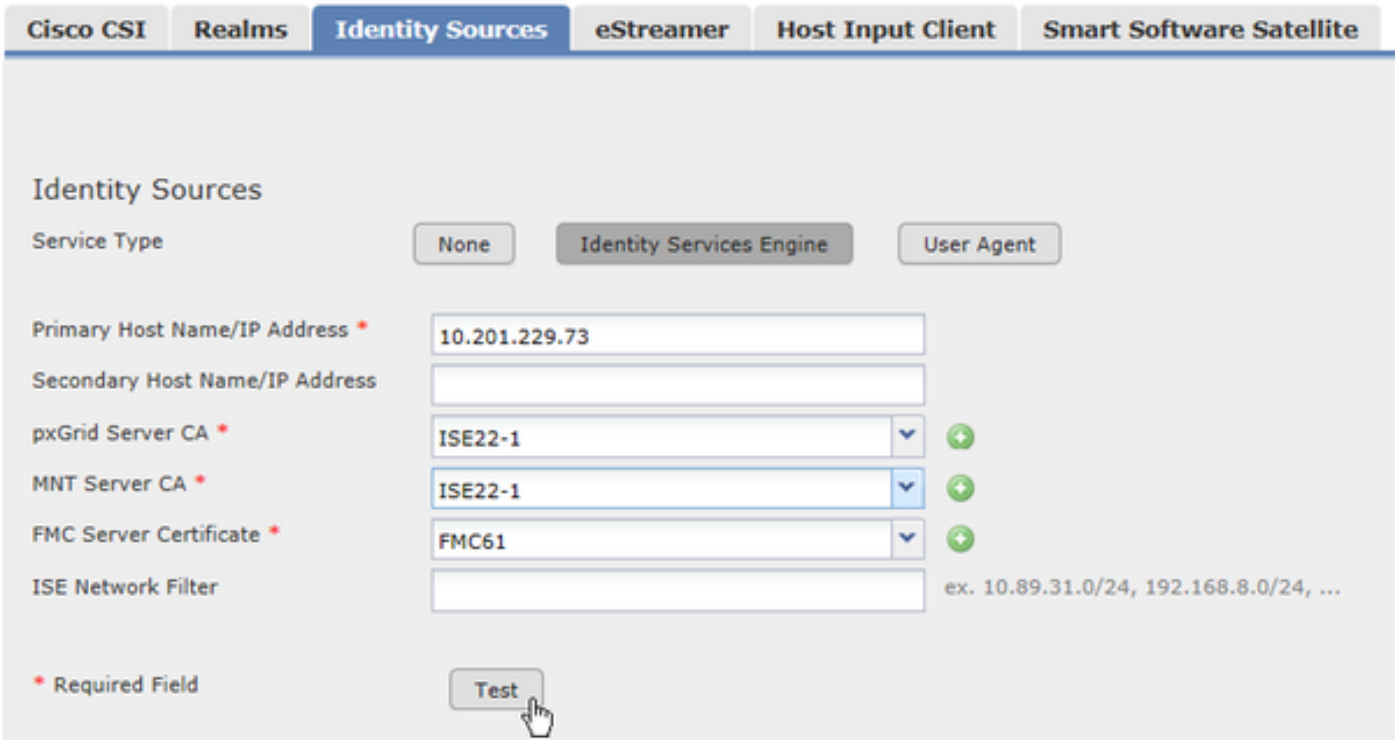
Schritt 4: FMC erstellt eine Benutzer-IP-SGT-Zuordnungsdatei und überträgt diese an den Sensor.

Schritt 5: Die Quell-IP-Adresse des Datenverkehrs wird verwendet, um die Security Group mithilfe von Sitzungsdaten aus der Benutzer-IP-Zuordnung abzugleichen.

Schritt 6: Wenn die Sicherheitsgruppe der Datenverkehrsquelle mit dem Zustand in der Zugriffskontrollrichtlinie übereinstimmt, wird vom Sensor entsprechend gehandelt.

Ein FMC ruft eine vollständige SGT-Liste ab, wenn die Konfiguration für die ISE-Integration unter **System > Integration > Identity Sources > Identity Services Engine** gespeichert wird.

> **Hinweis**: Durch Klicken auf die **Test**-Schaltfläche (wie unten gezeigt) wird die FMC nicht zum Abrufen von SGT-Daten ausgelöst.



Die Kommunikation zwischen FMC und ISE wird durch ADI (Abstract Directory Interface) ermöglicht, ein einzigartiger Prozess (es kann nur eine Instanz geben), der auf FMC ausgeführt wird. Andere Prozesse auf dem FMC abonnieren die ADI und fordern Informationen an. Derzeit ist der Datenkorrelator die einzige Komponente, die ADI abonniert.

FMC speichert das SGT in einer lokalen Datenbank. Die Datenbank enthält sowohl den SGT-Namen als auch die SGT-Nummer. Derzeit verwendet die FMC jedoch bei der Verarbeitung der SGT-Daten eine eindeutige ID (Secure Tag ID). Diese Datenbank wird auch an die Sensoren weitergeleitet.

Wenn ISE-Sicherheitsgruppen geändert werden, z. B. das Entfernen oder Hinzufügen von Gruppen, sendet die ISE eine pxGrid-Benachrichtigung an das FMC, um die lokale SGT-Datenbank zu aktualisieren.

Wenn sich ein Benutzer bei der ISE authentifiziert und eine Sicherheitsgruppen-Tag-Nummer erhält, benachrichtigt die ISE die FMC über pxGrid und gibt die Erkenntnis an, dass sich Benutzer X aus Bereich Y bei SGT Z angemeldet hat. FMC übernimmt die Informationen und fügt sie in die Benutzer-IP-Zuordnungsdatei ein. FMC verwendet einen Algorithmus, um die Zeit zu bestimmen, in der die erfasste Zuordnung an die Sensoren übertragen wird, abhängig davon, wie viel Netzwerkauslastung vorhanden ist.

> **Hinweis**: FMC überträgt nicht alle Benutzer-IP-Zuordnungseinträge an Sensoren. Damit FMC Push-Mapping durchführen kann, muss es zunächst über den Bereich mit dem Benutzer vertraut sein. Wenn der Benutzer in der Sitzung nicht Teil des Bereichs ist, werden die Zuordnungsinformationen dieses Benutzers von den Sensoren nicht erfasst. Unterstützung für Nicht-Realm-Benutzer wird für zukünftige Versionen in Betracht gezogen.

Das FirePOWER-System Version 6.0 unterstützt nur die IP-Benutzer-SGT-Zuordnung. Tatsächliche Tags im Datenverkehr oder SGT-IP-Zuordnung, die von SXP auf einer ASA gelernt wurde, werden nicht verwendet. Wenn der Sensor eingehenden Datenverkehr übernimmt, übernimmt der Snort-Prozess die Quell-IP-Zuordnung (die vom FirePOWER-Modul an den Snort-Prozess übertragen wird) und sucht nach der Secure Tag-ID. Wenn sie der in der Zugriffskontrollrichtlinie konfigurierten SGT-ID (nicht der SGT-Nummer) entspricht, wird die Richtlinie auf den Datenverkehr angewendet.

Die Inline-Tagging-Methode

Ab ASA Version 9.6.2 und ASA FirePOWER-Modul 6.1 wird Inline-SGT-Tagging unterstützt. Das bedeutet, dass das FirePOWER-Modul jetzt in der Lage ist, die SGT-Nummer direkt aus den Paketen zu extrahieren, ohne auf die vom FMC bereitgestellte Benutzer-IP-Zuordnung angewiesen zu sein. Dies bietet eine alternative Lösung für die TrustSec-basierte Zugriffskontrolle, wenn der Benutzer nicht Teil des Bereichs ist (z. B. Geräte, die nicht für die 802.1x-Authentifizierung geeignet sind).

Bei der Inline-Tagging-Methode antworten die Sensoren auf der FMC-Ebene immer noch darauf, SGT-Gruppen von der ISE abzurufen und die SGT-Datenbank nach unten zu schieben. Wenn der mit der Security Group Number getaggte Datenverkehr die ASA erreicht und die ASA so konfiguriert ist, dass sie dem eingehenden SGT vertraut ist, wird der Tag über die Datenspur an das FirePOWER-Modul übergeben. Das FirePOWER-Modul nimmt das Tag aus den Paketen und verwendet es direkt, um Zugriffskontrollrichtlinien zu evaluieren.

Die ASA muss über eine geeignete TrustSec-Konfiguration auf der Schnittstelle verfügen, um getaggten Datenverkehr empfangen zu können:

```
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
```

Hinweis: Inline-Tagging wird nur von ASA Version 9.6.2 und höher unterstützt. Die früheren Versionen einer ASA übergeben die Sicherheits-Tag-Nummer nicht über die Datenebene an das FirePOWER-Modul. Wenn ein Sensor Inline-Tagging unterstützt, versucht er zunächst, Tags aus dem Datenverkehr zu extrahieren. Wenn der Datenverkehr nicht markiert ist, kehrt der Sensor zur Benutzer-IP-Zuordnungsmethode zurück.

Fehlerbehebung

Über die eingeschränkte Shell eines FirePOWER-Geräts

So zeigen Sie die von FMC gesendete Zugriffskontrollrichtlinie an:

```
> 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
```

Hinweis: Die Sicherheitsgruppentags geben zwei Zahlen an: [7:6]. In diesem Nummernsatz ist "7" die eindeutige ID der lokalen SGT-Datenbank, die nur für FMC und Sensor bekannt ist. "6" ist die tatsächliche SGT-Nummer, die allen Parteien bekannt ist.

So zeigen Sie Protokolle an, die beim Verarbeiten des eingehenden Datenverkehrs durch SFR generiert werden, und werten die Zugriffsrichtlinie aus:

```
> 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
```

Beispiel für Firewall-Engine-Debugging für eingehenden Datenverkehr mit Inline-Tagging:

```
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
```

Im Expertenmodus eines FirePOWER-Geräts

> Vorsicht: Die folgende Anweisung kann sich auf die Systemleistung auswirken. Führen Sie den Befehl nur zu Fehlerbehebungszwecken oder auf Anforderung eines Cisco Support Engineers für diese Daten aus.

Das FirePOWER-Modul überträgt die Benutzer-IP-Zuordnung an den lokalen Snort-Prozess. Um zu überprüfen, was Snort über die Zuordnung weiß, können Sie den folgenden Befehl verwenden, um eine Abfrage an Snort zu senden:

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

Successfully commanded snort.
```

Um die Daten anzuzeigen, wechseln Sie in den Expertenmodus:

```
> expert

admin@firepower:~$
```

Snort erstellt eine Dump-Datei im Verzeichnis /var/sf/detect_engines/GUID/instance-x. Der Name der Dump-Datei lautet 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
```

```
------------------
~
```

Die obige Ausgabe zeigt, dass Snort von der IP-Adresse 10.201.229.94 Kenntnis erhält, die der SGT-ID 7 zugeordnet ist, also der SGT-Nummer 6 (Gäste).

Im FirePOWER Management Center

Sie können die ADI-Protokolle überprüfen, um die Kommunikation zwischen FMC und ISE zu überprüfen. Um die Protokolle der adi-Komponente zu finden, überprüfen Sie die Datei /var/log/messages im FMC. Protokolle werden wie folgt angezeigt:

```
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
.
.
```