FirePower 및 ISE로 TrustSec 기반 액세스 제어 이해

목차

소개

Cisco TrustSec은 Layer 2 이더넷 프레임의 태깅 및 매핑을 활용하여 기존 IP 인프라에 영향을 주지 않고 트래픽을 분리합니다.태그가 지정된 트래픽은 더욱 세분화된 보안 측정으로 처리할 수 있습니다.

ISE(Identity Services Engine)와 FMC(Firepower Management Center) 간의 통합으로 클라이언트 권한 부여에서 TrustSec 태깅을 전달할 수 있으며, 클라이언트의 보안 그룹 태그에 따라 액세스 제어 정책을 적용하는 데 Firepower에서 사용할 수 있습니다.이 문서에서는 ISE를 Cisco Firepower 기술과 통합하는 단계에 대해 설명합니다.

사용되는 구성 요소

이 문서에서는 예제 설정에서 다음 구성 요소를 사용합니다.

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

개요

센서 디바이스에서 트래픽에 할당된 SGT(Security Group Tag)를 탐지하는 방법에는 두 가지가 있습니다.

1. 사용자-IP 매핑을 통해
2. 인라인 SGT 태깅을 통해

사용자-IP 매핑 방법

액세스 제어에 TrustSec 정보가 사용되도록 하기 위해 ISE와 FMC를 통합하려면 다음 단계를 수행합니다.

1단계:FMC는 ISE에서 보안 그룹 목록을 검색합니다.

2단계:액세스 제어 정책은 보안 그룹을 조건으로 포함하는 FMC에서 생성됩니다.

3단계:엔드포인트가 ISE를 인증하고 권한을 부여할 때 세션 데이터가 FMC에 게시됩니다.

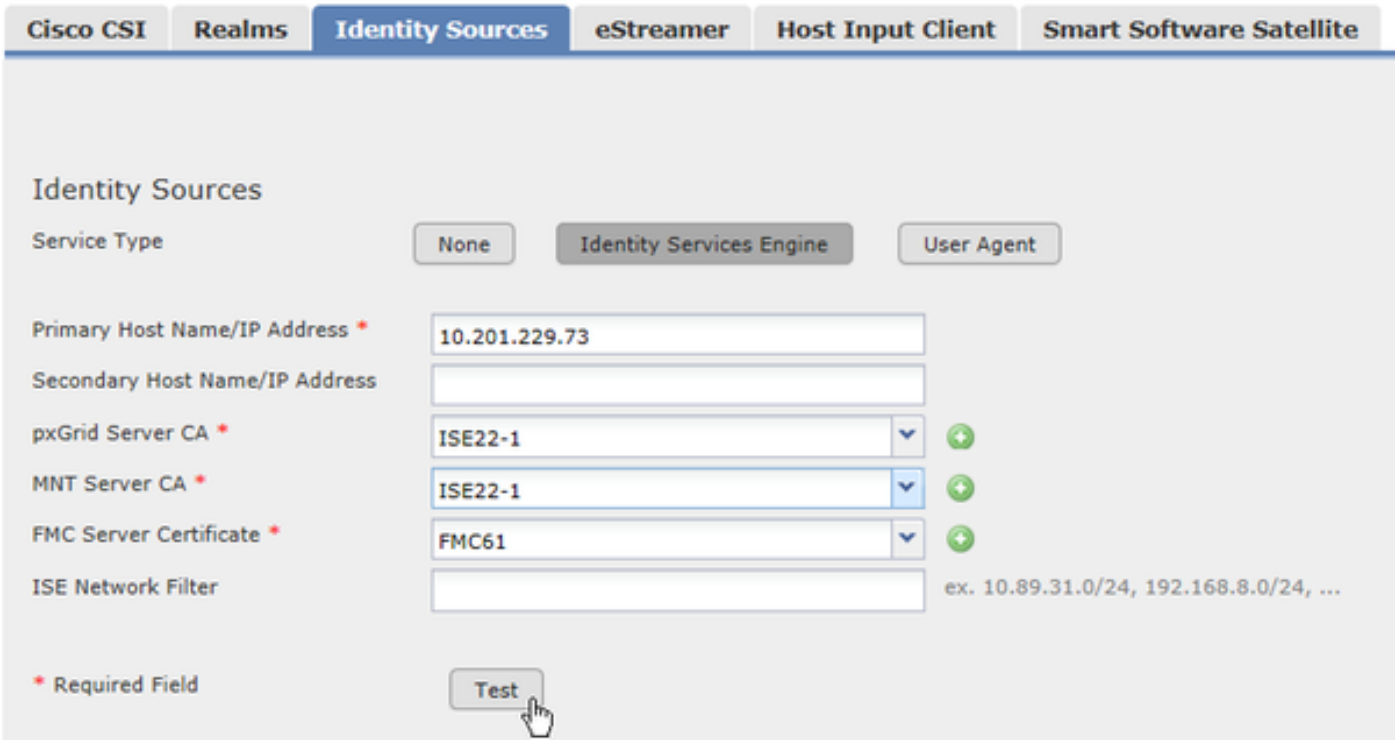
4단계:FMC는 User-IP-SGT 매핑 파일을 작성하여 센서에 푸시합니다.

5단계:트래픽의 소스 IP 주소는 User-IP 매핑의 세션 데이터를 사용하여 보안 그룹과 일치시키는 데 사용됩니다.

6단계:트래픽 소스의 보안 그룹이 액세스 제어 정책의 조건과 일치하면 센서에서 그에 따라 조치를 취합니다.

ISE 통합에 대한 컨피그레이션이 **System > Integration > Identity Sources > Identity Services Engine**에 저장되면 FMC는 전체 SGT 목록**을 검색합니다**.

> **참고:**테스트 버튼(아래 표시)을 클릭해도 SGT 데이터를 검색하도록 FMC가 트리거되지 않습니다.



FMC와 ISE 간의 통신은 ADI(Abstract Directory Interface)를 통해 이루어지며, 이는 FMC에서 실행되는 고유한 프로세스(하나의 인스턴스만 있을 수 있음)입니다.FMC에서 ADI에 가입하고 정보를 요청하는 기타 프로세스.현재 ADI에 가입한 유일한 구성품은 데이터 상관자입니다.

FMC는 SGT를 로컬 데이터베이스에 저장합니다.데이터베이스에는 SGT 이름과 번호가 모두 포함되어 있지만, 현재 FMC는 SGT 데이터를 처리할 때 고유한 식별자(Secure Tag ID)를 핸들로 사용합니다.이 데이터베이스는 센서에도 전파됩니다.

그룹 제거 또는 추가 등 ISE 보안 그룹이 변경되면 ISE는 pxGrid 알림을 FMC에 푸시하여 로컬 SGT 데이터베이스를 업데이트합니다.

사용자가 ISE를 사용하여 인증하고 보안 그룹 태그를 사용하여 권한을 부여하면 ISE는 pxGrid를 통해 FMC에 통지하여 영역 Y의 사용자 X가 SGT Z로 로그인했다는 정보를 제공합니다. FMC는 정보를 가져와 사용자-IP 매핑 파일에 삽입합니다.FMC는 네트워크 로드 양에 따라 알고리즘을 사용하여 센서에 가져온 매핑을 푸시할 시간을 결정합니다.

> **참고:**FMC는 모든 사용자-IP 매핑 항목을 센서로 푸시하지 않습니다.FMC가 매핑을 푸시하려면 먼저 영역을 통해 사용자에 대한 지식을 가져야 합니다.세션의 사용자가 영역에 속하지 않을 경우 센서는 이 사용자의 매핑 정보를 학습하지 않습니다.비영역 사용자에 대한 지원은 향후 릴리스에서 고려됩니다.

Firepower System 버전 6.0은 IP-User-SGT 매핑만 지원합니다.트래픽의 실제 태그 또는 ASA의 SXP에서 학습된 SGT-IP 매핑은 사용되지 않습니다.센서가 수신 트래픽을 포착하면 Snort 프로세스는 소스 IP를 가져와 FirePOWER 모듈에서 Snort 프로세스로 푸시되는 User-IP 매핑을 조회하고 Secure Tag ID를 찾습니다.액세스 제어 정책에 구성된 SGT ID(SGT 번호 아님)와 일치하면 정책이 트래픽에 적용됩니다.

인라인 태깅 방법

ASA 버전 9.6.2 및 ASA Firepower 모듈 6.1부터 인라인 SGT 태깅이 지원됩니다.이는 Firepower 모듈이 FMC에서 제공하는 User-IP 매핑에 의존하지 않고 패킷에서 직접 SGT 번호를 추출할 수 있음을 의미합니다.사용자가 영역에 속하지 않는 경우(예: 802.1x 인증을 지원하지 않는 디바이스) TrustSec 기반 액세스 제어를 위한 대체 솔루션을 제공합니다.

Inline Tagging Method(인라인 태깅 방법)를 사용해도 센서는 FMC에 응답하여 ISE에서 SGT 그룹을 검색하고 SGT 데이터베이스를 아래로 누릅니다.보안 그룹 번호로 태그가 지정된 트래픽이 ASA에 도달할 때, ASA가 수신 SGT를 신뢰하도록 구성된 경우, 태그는 데이터 플레인을 통해 Firepower 모듈에 전달됩니다.Firepower 모듈은 패킷에서 태그를 가져와 직접 사용하여 액세스 제어 정책을 평가합니다.

태그가 지정된 트래픽을 수신하려면 ASA에 인터페이스에 적절한 TrustSec 컨피그레이션이 있어야 합니다.

```
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
```

> **참고:**ASA 버전 9.6.2 이상만 인라인 태깅을 지원합니다.이전 버전의 ASA는 데이터 플레인을 통해 Security Tag를 Firepower 모듈로 전달하지 않습니다.센서가 인라인 태깅을 지원하는 경우, 먼저 트래픽에서 태그를 추출하려고 시도합니다.트래픽에 태그가 지정되지 않으면 센서가 사용자-IP 매핑 방법으로 돌아갑니다.

문제 해결

Firepower 디바이스의 제한된 셸에서

FMC에서 푸시된 액세스 제어 정책을 표시하려면

```
> 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
```

참고: Security Group Tags(보안 그룹 태그)는 두 개의 숫자를 지정합니다.[7:6].이 숫자 집합에서 "7"은 FMC 및 센서로만 알려진 로컬 SGT 데이터베이스의 고유 ID입니다."6"은 모든 당사자가 알고 있는 실제 SGT 번호입니다.

SFR에서 수신 트래픽을 처리하고 액세스 정책을 평가할 때 생성된 로그를 보려면

```
> 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
```

인라인 태깅을 사용하는 수신 트래픽에 대한 firewall-engine-debug의 예:

```
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
```

Firepower 디바이스의 Expert 모드에서

> **주의:**다음 명령은 시스템 성능에 영향을 미칠 수 있습니다.트러블슈팅을 위해 또는 Cisco 지원 엔지니어가 이 데이터를 요청할 때만 명령을 실행합니다.

Firepower 모듈은 User-IP 매핑을 로컬 Snort 프로세스에 푸시합니다.Snort가 매핑에 대해 알고 있는 내용을 확인하려면 다음 명령을 사용하여 Snort에 쿼리를 보낼 수 있습니다.

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

Successfully commanded snort.
```

데이터를 보려면 expert 모드로 들어갑니다.

```
> expert

admin@firepower:~$
```

Snort는 /var/sf/detection_engines/GUID/instance-x 디렉토리 아래에 덤프 파일을 생성합니다.덤프 파일의 이름은 user_identity.dump입니다.

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

위의 출력에서는 Snort가 SGT ID 7에 매핑된 IP 주소 10.201.229.94을 인식하며, 이는 SGT 번호 6(게스트)입니다.

Firepower Management Center에서

ADI 로그를 검토하여 FMC와 ISE 간의 통신을 확인할 수 있습니다.adi 구성 요소의 로그를 찾으려면 FMC에서 /var/log/messages 파일을 확인합니다.다음과 같은 로그가 표시됩니다.

```
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
.
.
```