通過FirePower和ISE瞭解基於TrustSec的訪問控制

目錄

簡介

Cisco TrustSec利用第2層乙太網幀的標籤和對映來隔離流量，而不會影響現有的IP基礎設施。可以使用更精細的安全措施處理已標籤的流量。

身份服務引擎(ISE)和Firepower管理中心(FMC)之間的整合允許通過客戶端授權傳遞TrustSec標籤，Firepower可使用此標籤基於客戶端的安全組標籤應用訪問控制策略。本文檔討論將ISE與思科Firepower技術整合的步驟。

採用元件

本文檔在示例設定中使用以下元件：

- 身分識別服務引擎 (ISE) 2.1 版
- Firepower管理中心(FMC)版本6.x
- Cisco調適型安全裝置(ASA)5506-X版本9.6.2
- 思科調適型安全裝置(ASA)5506-X Firepower模組，版本6.1

概觀

感測器裝置檢測分配給通訊量的安全組標籤(SGT)有兩種方法：

1. 通過使用者IP對映
2. 通過內聯SGT標籤

使用者 — IP對映方法

為確保TrustSec資訊用於訪問控制，ISE與FMC的整合需執行以下步驟：

第1步：FMC從ISE檢索安全組清單。

第2步：訪問控制策略是在FMC上建立的，包括作為條件的安全組。

步驟3:當終端通過ISE進行身份驗證和授權時，會話資料將發佈到FMC。

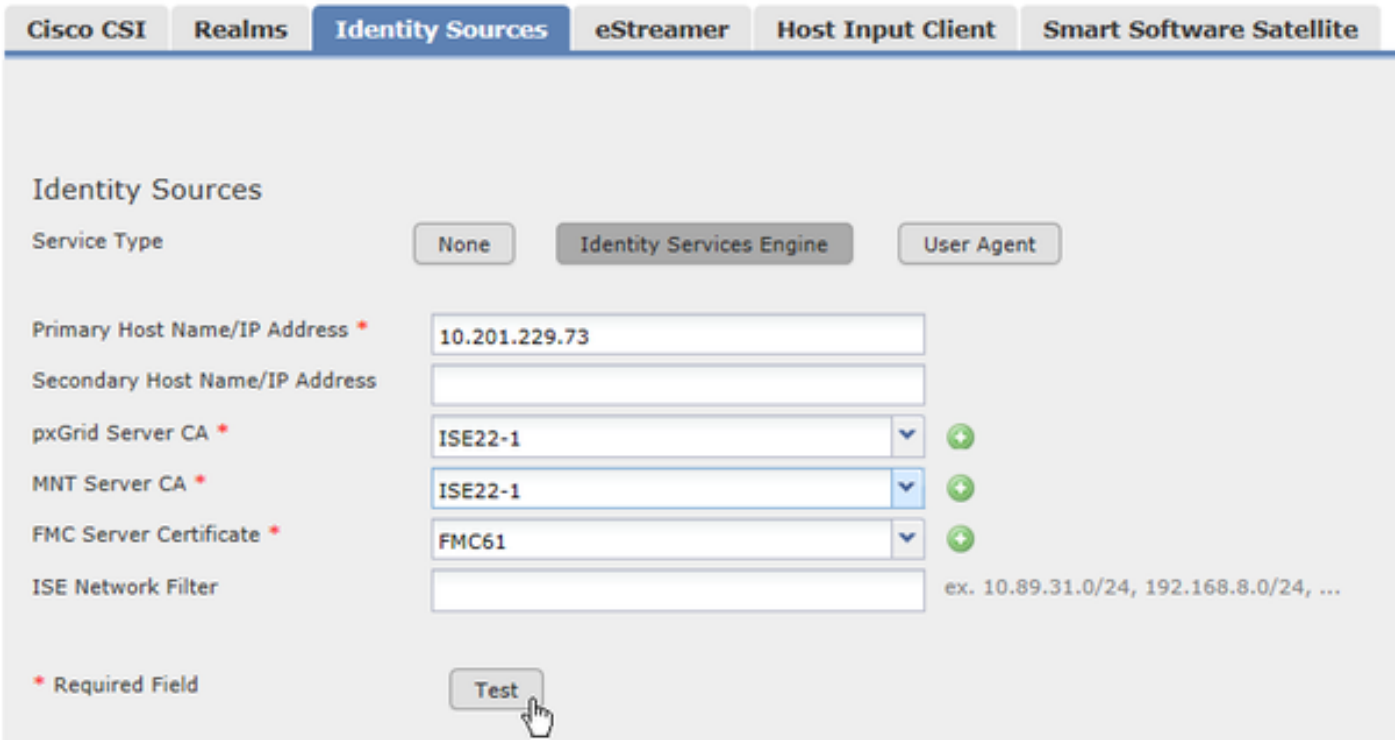
第4步：FMC構建使用者 — IP-SGT對映檔案，並將其推送到感測器。

第5步：流量的源IP地址用於使用使用者 — IP對映中的會話資料匹配安全組。

第6步：如果通訊量源的安全組與訪問控制策略中的條件相匹配，則感測器將採取相應的操作。

當ISE整合的配置儲存在**System > Integration > Identity Sources > Identity Services Engine**下時，FMC會檢索完整的SGT清單。

> **附註**：按一下**Test**按鈕（如下所示）不會觸發FMC檢索SGT資料。



FMC和ISE之間的通訊通過ADI（抽象目錄介面）實現，這是一個在FMC上運行的唯一進程（只能有一個例項）。FMC上的其他流程可訂購ADI並請求獲得資訊。目前唯一訂閱ADI的元件是資料相關器。

FMC將SGT儲存在本地資料庫中。資料庫包含SGT名稱和編號，但當前FMC在處理SGT資料時使用唯一識別符號（安全標籤ID）作為控制代碼。此資料庫也會傳播到感測器。

如果ISE安全組發生更改，例如刪除或新增組，ISE會向FMC推送pxGrid通知以更新本地SGT資料庫。

當使用者使用ISE進行身份驗證並授權使用安全組標籤時，ISE通過pxGrid通知FMC，提供來自領域Y的使用者X已使用SGT Z登入的資訊。FMC獲取資訊並插入使用者 — IP對映檔案。FMC使用一種演算法來確定將獲取的對映推送到感測器的時間，具體取決於網路負載的大小。

附註：FMC不會將所有使用者IP對映條目推送到感測器。FMC要推送對映，必須首先通過領域瞭解使用者。如果會話中的使用者不是領域的一部分，感測器將不會獲知此使用者的對映資訊。未來版本會考慮對非領域使用者的支援。

Firepower系統版本6.0僅支援IP-User-SGT對映。不會使用流量中的實際標籤，或者從ASA上的SXP學習的SGT-IP對映。當感測器拾取傳入通訊量時，Snort進程獲取源IP並查詢使用者 — IP對映(由Firepower模組推送到Snort進程)，然後查詢安全標籤ID。如果它與訪問控制策略中配置的SGT ID（而不是SGT編號）匹配，則此策略將應用於流量。

內嵌標籤方法

從ASA 9.6.2版和ASA Firepower模塊6.1開始，支援內聯SGT標籤。這表示Firepower模組現在可以直接從封包中擷取SGT編號，而無需依賴FMC提供的使用者 — IP對應。當使用者不屬於領域（例如裝置不支援802.1x身份驗證）時，這為基於TrustSec的訪問控制提供了替代解決方案。

使用Inline Tagging Method，感測器仍然在FMC上回覆以從ISE檢索SGT組，並下推SGT資料庫。當使用安全組編號標籤的流量到達ASA時，如果ASA配置為信任傳入的SGT，則標籤將通過資料平面傳遞到Firepower模組。Firepower模組從資料包獲取標籤，並直接使用該標籤評估訪問控制策略。

ASA必須在介面上具有正確的TrustSec配置才能接收標籤的流量：

```
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
```

附註：只有ASA 9.6.2及更高版本支援內聯標籤。早期版本的ASA不會將安全標籤通過資料平面傳遞到Firepower模組。如果感測器支援Inline Tagging，它會首先嘗試從通訊量中提取標籤。如果通訊量未標籤，感測器將回退到使用者IP對映方法。

疑難排解

從Firepower裝置的受限外殼

要顯示從FMC推送的訪問控制策略，請執行以下操作：

```
> 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
```

附註：安全組標籤指定兩個數字：[7:6]。在這一組數字中，「7」是本地SGT資料庫的唯一ID，只有FMC和感測器知道。「6」是各方已知的實際SGT編號。

檢視SFR處理傳入流量和評估訪問策略時生成的日誌：

```
> 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
```

使用內嵌標籤傳入流量的firewall-engine-debug範例：

```
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
```

從Firepower裝置的專家模式

注意：以下指令可能會影響系統效能。僅在進行故障排除時或在思科支援工程師請求提供此資料時運行命令。

Firepower模塊將使用者 — IP對映推送到本地Snort進程。要驗證Snort對對映的瞭解，您可以使用以下命令將查詢傳送到Snort:

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

```
Successfully commanded snort.
```

要檢視資料，請進入專家模式：

```
> expert

admin@firepower:~$
```

Snort在/var/sf/detection_engine/GUID/instance-x目錄下建立轉儲文件。轉儲檔案的名稱為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
-------------------
~
```

上面的輸出顯示，Snort知道對映到SGT ID 7的IP地址10.201.229.94，即SGT編號6（訪客）。

從Firepower管理中心

您可以檢視ADI日誌以驗證FMC和ISE之間的通訊。要查詢adi元件的日誌，請檢查FMC上的/var/log/messages檔案。您將注意到以下日誌：

```
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
.
.
```