Firepower および ISE の TrustSec ベースのアクセスコントロールの概要

目次

概要

Cisco TrustSec は既存の IP インフラストラクチャに影響を与えないでトラフィックを分離するのにレイヤ2 イーサネットフレームのタギングおよびマッピングを利用します。 タグ付きトラフィックはより優れた精度のセキュリティ対策と処理することができます。

クライアントのセキュリティグループ タグに基づいてアクセスコントロール ポリシーを適用するのに Firepower によって使用することができるクライアント 許可から通信されるためにタグ付けする Identity Services Engine （ ISE ）および Firepower Management Center （ FMC ）割り当て間の統合 TrustSec。 この資料は Cisco Firepower テクノロジーと ISE を統合ためにステップを説明します。

使用するコンポーネント

この資料は設定される例でコンポーネントの後で使用します:

- Identity Services Engine （ ISE ）バージョン 2.1
- Firepower Management Center （ FMC ）バージョン 6.x
- Cisco 適応型セキュリティ アプライアンス (ASA) ソフトウェア (ASA) 5506-X バージョン 9.6.2
- Cisco 適応型セキュリティ アプライアンス (ASA) ソフトウェア (ASA) 5506-X Firepower モジュール、バージョン 6.1

概要

トラフィックに割り当てられるセキュリティグループ タグ (SGT) を検出する センサ デバイスのための 2 つの方法があります:

1. ユーザ IP マッピングを通して
2. インライン SGT タギングによって

ユーザ IP マッピング方式

TrustSec 情報を確認することは次のステップを FMC とアクセスコントロールのために、ISE の統合通過します使用されます:

ステップ 1： FMC は ISE からセキュリティグループのリストを取得します。

ステップ 2： アクセスコントロール ポリシーは状態としてセキュリティグループを含む FMC で作成されます。

ステップ 3： エンドポイントが ISE と認証し、承認するとき、セッションデータは FMC に送達されます。

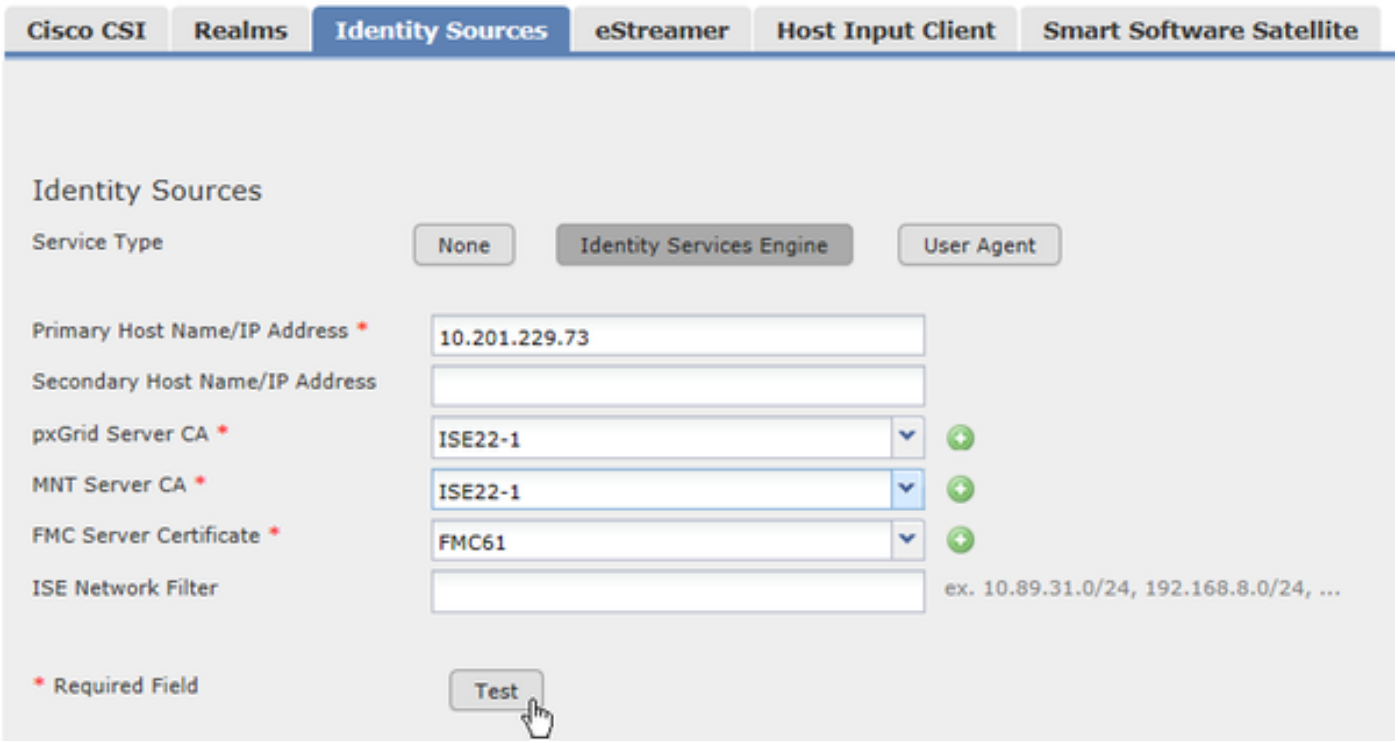
ステップ 4： FMC はユーザ IPSGT マッピング ファイルを構築し、センサーに押します。

ステップ 5： トラフィックのソース IP アドレスがユーザ IP マッピングからのセッションデータを使用しているセキュリティグループを一致するのに使用されています。

ステップ 6： トラフィックソースのセキュリティグループがアクセスコントロール ポリシーの条件と一致する場合、処置はセンサーによってそれに応じてとられます。

FMC は ISE 統合のための設定が**システム > 統合 > 識別**の下で**ソースをたどる > Identity Services Engine** 保存されるとき完全な SGT リストを取得します。

> **注:** ボタンを（ ）下記に示されているように『Test』 をクリック することは引き起こしません SGT データを取得するために FMC を。



FMC と ISE 間の通信は FMC で動作するユニークなプロセス（1 つの例があるただ場合もあります）である ADI（抽象的なディレクトリ インターフェイス）によって促進されます。 FMC の他

のプロセスは ADI および要求された情報を定期講読します。 現在唯一のコンポーネントは ADI を定期講読するデータ コリレータです。

FMC はローカルデータベースの SGT を保存します。 データベースは両方の SGT 名前および数が含まれていますが、SGT データを処理するとき現在 FMC はハンドルとして固有の識別番号（セキュア タグ ID）を使用します。 このデータベースはまたセンサーに伝搬します。

ISE セキュリティグループが削除のような、変更されるかまたはローカル SGT データベースをアップデートするためにグループの付加が FMC に、ISE pxGrid 通知を押せば。

ユーザが ISE と認証を受け、セキュリティグループ タグと承認するとき、ISE は X つが SGT Z. FMC とレルム Y からログオンしたユーザがユーザ IP マッピング ファイルに情報および挿入を運ぶというナレッジを提供する pxGrid を通して FMC を知らせます。 FMC は押すネットワーク負荷があるかどの位によってアルゴリズムをセンサーに得られたマッピングを、時期を判別するのに使用します。

> **注:** FMC はセンサーにすべてのユーザ IP マッピング エントリを押しません。 マッピングを押す FMC に関してはレルムを通して最初にユーザのナレッジを持たなければなりません。 セッションのユーザがレルムの一部ではない場合、センサーはこのユーザのマッピング情報を学びません。 非レルム ユーザ向けのサポートは将来のリリースのために考慮されます。

Firepower システムバージョン 6.0 は IP ユーザSGT マッピングしかサポートしません。 トラフィックの実際のタグ、か ASA の SXP から学ばれる SGT-IP マッピング することは使用されません。 センサーが着信トラフィックを取るとき、Snort プロセスは出典 IP を奪取 し、（Snort プロセスへの Firepower モジュールによって押される）ユーザ IP マッピング調べ、セキュア タグ ID を見つけます。 それがアクセスコントロール ポリシーで設定される SGT ID （ない SGT 数）と一致する場合ポリシーはトラフィックに適用されます。

インライン タギング 方式

ASA バージョン 9.6.2 および ASA Firepower モジュール 6.1 から始まって、インライン SGT タギングはサポートされます。 これは Firepower モジュールが FMC ことをによって提供されるユーザ IP マッピングに頼らないでパケットから SGT 数を直接得る現在ことができることを意味します。 これは TrustSec ベースのアクセスコントロールにユーザがレルムの一部のとき代替案を提供します（802.1X 認証が可能ではないデバイスのような）。

インライン タギング 方式によって SGT グループを ISE から取得し、SGT データベースを押下げるために、センサーはまだ FMC で答えます。 セキュリティグループ数によってタグ付けされるトラフィックが ASA に達する場合、ASA が着信 SGT を信頼するために設定される場合タグは dataplane を通して Firepower モジュールに通じます。 Firepower モジュールはパケットからのタグを奪取 し、それをアクセスコントロール ポリシーを評価するのに直接使用します。

ASA はタグ付きトラフィックを受信するためにインターフェイスの適切な TrustSec 設定がなければなりません:

```
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
```

> **注:** ASA バージョン 9.6.2 および それ 以上だけインライン タギングをサポートします。

ASA の以前のバージョンは Firepower モジュールに dataplane を通してセキュリティ タグを渡しません。 センサーがインライン タギングをサポートする場合、最初にトラフィックからタグを得ることを試みます。 トラフィックがタグ付けされていない場合、センサーはユーザ IP マッピング方式に戻って落ちます。

トラブルシューティング

Firepower デバイスの制限シェルから

FMC からのアクセスコントロール Policy Pushed を表示するため:

```
> 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
```

注: セキュリティグループ タグは 2 つの数を規定 します: [7:6]. この数字の組合せでは、「7" FMC およびセンサーにだけ知られている ローカル SGT データベースのユニークな ID です。「6" すべてのパーティに知られている実際の SGT 数です。

SFR が着信トラフィックおよび評価アクセスポリシーを処理する時生成される ログを調べるため:

```
> 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
```

インライン タギングの着信トラフィックのためのファイアウォール エンジン の例:

```
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
```

Firepower デバイスの巧妙なモードから

> **注意**：次の手順はシステムパフォーマンスに影響を与えるかもしれません。トラブルシューティングする 目的でだけコマンドを、または時このデータのための Ciscoサポート エンジニア 要求実行して下さい。

ローカル Snort プロセスにマッピング する Firepower モジュール プッシュ ユーザ IP。どんな Snort がマッピングについて確認するか確認するために、鼻を鳴らすためにクエリを送信するのに次のコマンドを使用できます:

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

Successfully commanded snort.
```

データを表示するために、巧妙なモードになって下さい:

```
> expert

admin@firepower:~$
```

Snort は `/var/sf/detection_engines/GUID/instance-x` ディレクトリの下でダンプする ファイルを作成します。ダンプする ファイルの名前は `user_identity.dump` です

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

上記の出力はマッピング されるかどれが SGT 第 6（ゲスト）である SGT ID 7 に Snort が IP アドレス 10.201.229.94 に気づいていることを示したものです。

Firepower Management Center から

FMC と ISE 間の通信を確認するために ADI ログを見ることができます。`adi` コンポーネントのログを見つけるために、FMC の `/var/log/messages` ファイルをチェックして下さい。下記にのような口グに注意します:

```
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>
```