Понимание находящегося в TrustSec управления доступом с FirePower и ISE

Содержание

Введение

Cisco TrustSec использует маркировку и сопоставление Фреймов Ethernet Уровня 2 для разделения трафика, не влияя на существующую Инфраструктуру IP. Помеченный трафик может рассматриваться с измерениями безопасности с большей глубиной детализации.

Интеграция между платформой Identity Services Engine (ISE) и Центр управления огневой мощи (FMC) позволяет маркировке TrustSec быть переданной из клиентской авторизации, которая может использоваться Огневой мощью для применения политики контроля доступа на основе Метки Группы безопасности клиента. Этот документ обсуждает шаги для интеграции ISE с технологией Огневой мощи Cisco.

Используемые компоненты

Использование этого документа после компонентов в настройке в качестве примера:

- Версия 2.1 платформы Identity Services Engine (ISE)
- Центр управления огневой мощи (FMC) версия 6. x
- Устройство адаптивной защиты Cisco (ASA) 5506-X версия 9.6.2
- Устройство адаптивной защиты Cisco (ASA) 5506-X модуль огневой мощи, версия 6.1

Обзор

Существует два пути к датчику для обнаружения тега группы безопасности (SGT), назначенного на трафик:

1. Посредством сопоставления Пользовательского IP
2. Посредством Встроенной маркировки SGT

Метод сопоставления пользовательского IP

Гарантировать информацию о TrustSec используется для управления доступом, интеграция ISE с FMC проходит следующие шаги:

Шаг 1: FMC получает список Групп безопасности от ISE.

Шаг 2: Политика контроля доступа создана на FMC, который включает Группы безопасности как условие.

Шаг 3: Когда оконечные точки аутентифицируют и авторизуют с ISE, данные сеанса публикованы в FMC.

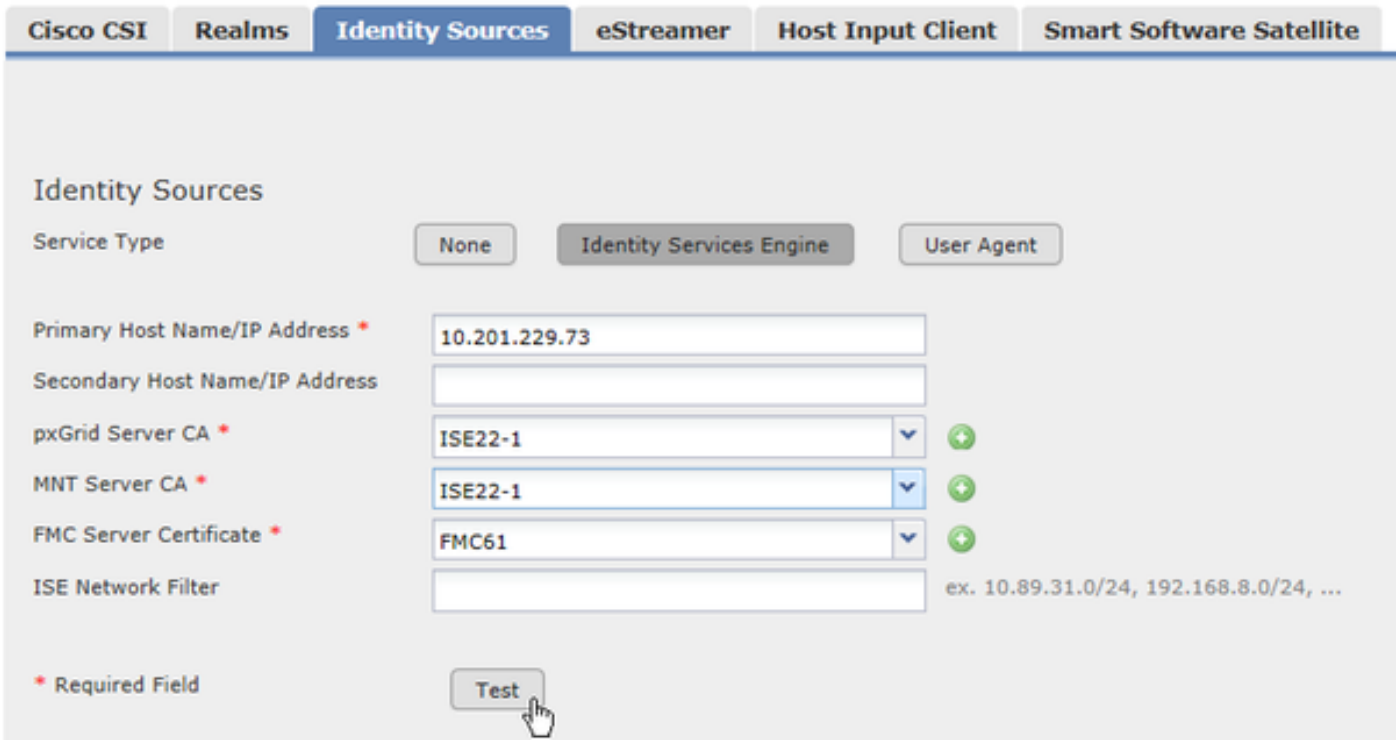
Шаг 4. : FMC создает файл сопоставления ПОЛЬЗОВАТЕЛЬСКОГО SGT IP и выдвигает его к датчику.

Шаг 5. : IP - адрес источника трафика используется для соответствия с Группой безопасности с помощью данных сеанса от сопоставления Пользовательского IP.

Шаг 6: Если Группа безопасности источника трафика совпадает с условием в политике контроля доступа, меры приняты датчиком соответственно.

Когда конфигурация для интеграции ISE сохранена под **Системой> Интеграция> Идентификационные Источники> платформа Identity Services Engine,** FMC получает завершенный список SGT.

> **Примечание:** Нажатие **кнопки Test** (как показано ниже) не инициирует FMC для получения данных SGT.



Связь между FMC и ISE упрощена ADI (Абстрактный Интерфейс Каталога), который является уникальным процессом (может только быть один экземпляр), работающий на FMC. Другие процессы на FMC подписываются на ADI и запрашивают информацию. В настоящее

время единственный компонент, который подписывается на ADI, является коррелятором данных.

FMC сохраняет SGT в локальной базе данных. База данных содержит обоих имя и номер SGT, но в настоящее время FMC использует уникальный идентификатор (Безопасный ID Метки) как маркер при обработке данных SGT. Эта база данных также распространяется к датчикам.

Если Группы безопасности ISE изменены, такие как удаление или добавление групп, ISE выдвигает pxGrid уведомление FMC обновлять локальную базу данных SGT.

Когда пользователь аутентифицируется с ISE и авторизует с Меткой Группы безопасности, ISE уведомляет FMC через pxGrid, предоставляя знание, что пользователь X от области Y вошел с SGT Z. FMC берет информацию и вставки в файл сопоставления пользовательского IP. FMC использует алгоритм для определения времени для продвижения полученного сопоставления с датчиками, в зависимости от того, сколько сетевой нагрузки присутствует.

> **Примечание:** FMC не выдвигает все записи сопоставления Пользовательского IP в датчики. Для FMC для продвижения сопоставления это должно сначала ознакомиться с пользователем через именованную область (Realm). Если пользователь на сеансе не будет частью именованной области (Realm), то датчики не изучат данные сопоставления этого пользователя. Поддержку пользователей неименованной области (Realm) рассматривают для будущих версий.

Версия системы Огневой мощи 6.0 только поддержки сопоставление ПОЛЬЗОВАТЕЛЬСКОГО SGT IP. Фактические метки в трафике или сопоставление IP SGT, изученное из SXP на ASA, не используются. Когда датчик берет входящий трафик, процесс Фырканья берет source IP и ищет сопоставление Пользовательского IP (который выдвинут модулем Огневой мощи к процессу Фырканья), и находит Безопасный ID Метки. Если это совпадает с ID SGT (не номер SGT) настроенный в политике контроля доступа, то политика применена к трафику.

Встроенный метод маркировки

При начале с версии ASA 9.6.2 и модуля 6.1 Огневой мощи ASA, поддерживается Встроенная маркировка SGT. Это означает, что модуль Огневой мощи теперь способен к извлечению номера SGT непосредственно от пакетов, не полагаясь на сопоставление Пользовательского IP, предоставленное FMC. Когда пользователь не является частью именованной области (Realm) (такой как устройства, не способные к аутентификации 802.1x), это предоставляет альтернативное решение для находящегося в TrustSec управления доступом.

Со Встроенным Методом Маркировки датчики все еще отвечают на FMC, чтобы получить группы SGT из ISE и оттолкнуть базу данных SGT. Когда трафик, помеченный с номером Группы безопасности, достигает ASA, если ASA будет настроен для доверия входящему SGT, то метку передадут к модулю Огневой мощи через dataplane. Модуль Огневой мощи берет метку от пакетов и использует ее непосредственно для оценки политики контроля доступа.

ASA должен иметь надлежащую конфигурацию TrustSec на интерфейсе для

получения помеченного трафика:

```
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
```

Примечание: Только версия ASA 9.6.2 и более высокие поддержки Встроенная Маркировка. Более ранние версии ASA не передают Метку Безопасности через dataplane к модулю Огневой мощи. Если датчик поддержит Встроенную Маркировку, то он сначала попытается извлечь метку из трафика. Если трафик не помечен, датчик переключается на метод сопоставления Пользовательского IP.

Устранение неисправностей

От ограниченного Shell устройства огневой мощи

Отображать политику контроля доступа, выдвинутую от FMC:

```
> 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
```

Примечание: Метки Группы безопасности задают два номера: `[7:6]`. В этом наборе номеров, "`7`" уникальный идентификатор локальной базы данных SGT, которая только известна FMC и датчику. "`6`" фактический номер SGT, известный всем сторонам.

Просмотреть журналы, генерируемые, когда SFR обрабатывает политика доступа оценки и входящий трафик:

```
> 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
```

Пример `отладки механизма межсетевого экрана` для входящего трафика со встроенной маркировкой:

```
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
```

От экспертного режима устройства огневой мощи

> **Внимание. :** Следующие инструкции могут повлиять на производительность системы. Выполните команду только для цели устранения проблем, или когда специалист службы технической поддержки Cisco запросит на эти данные.

Модуль огневой мощи выдвигает сопоставление Пользовательского IP с локальным процессом Фырканья. Для проверки, что Фырканье знает о сопоставлении можно использовать следующую команду для передачи запроса для Фырканья:

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

Successfully commanded snort.
```

Для просмотра данных войдите к экспертному режиму:

```
> expert

admin@firepower:~$
```

Фырканье создает файл дампа в `/var/sf/detection_engines/GUID/instance-x` каталоге. Название файла дампа является `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
-------------------
~
```

Выходные данные выше показов, что Фырканье знает о IP-адресе 10.201.229.94, который сопоставлен с ID 7 SGT, который является SGT номер 6 (Гости).

От центра управления огневой мощи

Можно рассмотреть журналы ADI для проверки связи между FMC и ISE. Для обнаружения журналов `adi` компонента проверьте`/var/log/messages` файл на FMC. Вы заметите журналы как ниже:

```
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>
```