# Compreendendo o controle de acesso TrustSec-baseado com potência de fogo e ISE

## Índice



## Introdução

Cisco TrustSec utiliza a colocação de etiquetas e o traço de frames da Ethernet da camada 2 para segregar o tráfego sem afetar infraestrutura de IP existente. O tráfego rotulado pode ser tratado com as medidas de segurança com maior granularidade.

A integração entre o Identity Services Engine (ISE) e o centro de gerenciamento da potência de fogo (FMC) permite TrustSec que etiqueta para ser comunicado da autorização do cliente, que pode ser usada pela potência de fogo para aplicar as políticas do controle de acesso baseadas na etiqueta do grupo de segurança do cliente. Este documento discute as etapas para integrar o ISE com a tecnologia da potência de fogo de Cisco.

## Componentes Utilizados

Este documento usa-se depois dos componentes no exemplo setup:

- Versão 2.1 do Identity Services Engine (ISE)
- Versão 6.x do centro de gerenciamento da potência de fogo (FMC)
- Versão 9.6.2 5506-X adaptável da ferramenta de segurança de Cisco (ASA)
- Módulo adaptável da potência de fogo 5506-X da ferramenta de segurança de Cisco (ASA), versão 6.1

## Visão geral

Há duas maneiras para que um dispositivo de sensor detecte a etiqueta do grupo de segurança (SGT) atribuída ao tráfego:

1. Através do mapeamento USER-IP
2. Com da colocação de etiquetas Inline SGT

## O método do mapeamento USER-IP

Para assegurar a informação de TrustSec é usado para o controle de acesso, a integração do ISE com um FMC atravessa as seguintes etapas:

**Passo 1:** FMC recupera uma lista dos grupos de segurança do ISE.

**Passo 2:** As políticas do controle de acesso são criadas em FMC que inclui grupos de segurança como a circunstância.

**Passo 3:** Quando os valores-limite autenticam e autorizam com ISE, os dados de sessão estão publicados a FMC.

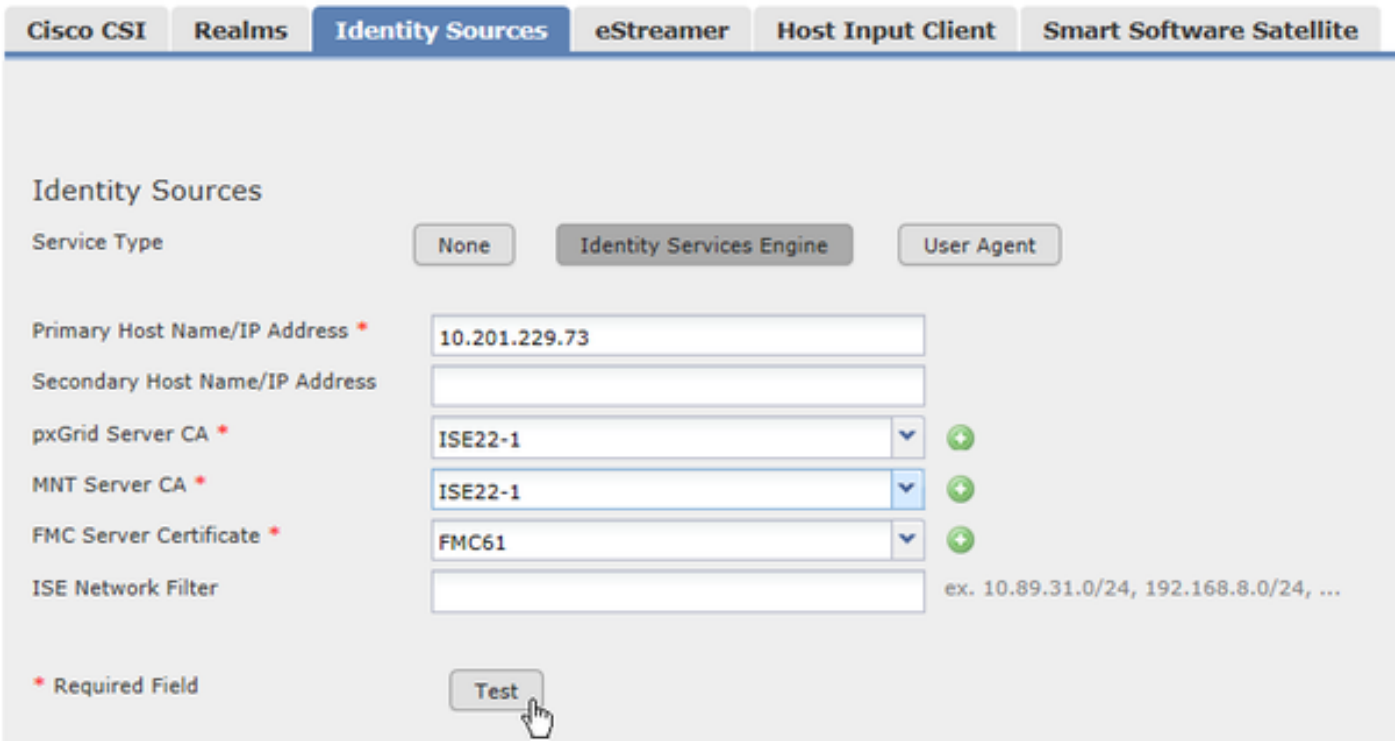
**Passo 4:** FMC constrói um arquivo do mapeamento USER-IP-SGT, e empurra-o para o sensor.

**Passo 5:** O endereço IP de origem do tráfego é usado para combinar o grupo de segurança que usa dados de sessão do mapeamento USER-IP.

**Passo 6:** Se o grupo de segurança do origem de tráfego combina a condição na política do controle de acesso, a ação está tomada pelo sensor em conformidade.

Um FMC recupera uma lista completa SGT quando a configuração para a integração ISE salvar sob o **sistema > a integração > as fontes > o Identity Services Engine da identidade**.

> Nota: **O botão Test Button de** clique (como mostrado abaixo) não provoca FMC para recuperar dados SGT.




A comunicação entre FMC e ISE é facilitada pelo ADI (relação abstrata do diretório), que é um processo original (pode somente haver um exemplo) que é executado em FMC. Outros processos

em FMC subscrevem ao ADI e pedem a informação. Atualmente o único componente que subscreve ao ADI é o correlator dos dados.

FMC salvar o SGT em um base de dados local. O base de dados contém o nome e o número SGT, mas atualmente FMC usa um identificador exclusivo (etiqueta segura ID) como o punho ao processar dados SGT. Este base de dados é propagado igualmente aos sensores.

Se os grupos de segurança ISE estão mudados, como a remoção ou a adição de grupos, ISE empurra uma notificação do pxGrid para FMC para atualizar o base de dados local SGT.

Quando um usuário autentica com ISE e autoriza com uma etiqueta do grupo de segurança, o ISE notifica FMC através do pxGrid, fornecendo o conhecimento que o usuário que X do reino Y entraram com SGT Z. FMC toma a informação e as inserções no mapeamento USER-IP arquivam. FMC usa um algoritmo para determinar o momento de empurrar o mapeamento adquirido para os sensores, segundo quanto a carga de rede esta presente.

> Nota: FMC não empurra todas as entradas do mapeamento USER-IP para sensores. Para que FMC empurre o mapeamento, deve primeiramente ter o conhecimento do usuário com o reino. Se o usuário na sessão não é parte do reino, os sensores não aprenderão a informação de mapeamento deste usuário. O apoio para usuários do NON-reino é considerado para as liberações futuras.

A versão do sistema 6.0 da potência de fogo apoia somente o mapeamento IP-USER-SGT. As etiquetas reais no tráfego, ou o traço SGT-IP aprendido de SXP em um ASA não são usados. Quando o sensor pegara o tráfego de entrada, o processo do Snort toma o IP da fonte e olha acima o mapeamento USER-IP (que é empurrado pelo módulo da potência de fogo ao processo do Snort), e encontra a etiqueta segura ID. Se combina o SGT ID (não número SGT) configurado na política do controle de acesso, a seguir a política está aplicada ao tráfego.

## O método de colocação de etiquetas Inline

Partindo do módulo 6.1 da versão ASA 9.6.2 e da potência de fogo ASA, a colocação de etiquetas Inline SGT é apoiada. Isto significa que o módulo da potência de fogo é agora capaz de extrair o número SGT diretamente dos pacotes sem confiar no mapeamento USER-IP fornecido por FMC. Isto fornece uma solução alternativa para o controle de acesso TrustSec-baseado quando o usuário não é parte do reino (tal como os dispositivos não capazes da autenticação do 802.1x).

Com o método de colocação de etiquetas Inline, os sensores ainda respondem em FMC para recuperar grupos SGT do ISE e para abaixar o base de dados SGT. Quando o tráfego etiquetado com o número de grupo de segurança alcança o ASA, se o ASA está configurado para confiar o SGT entrante, a etiqueta estará passada ao módulo da potência de fogo através do dataplane. O módulo da potência de fogo toma a etiqueta dos pacotes e usa-a diretamente para avaliar políticas do controle de acesso.

O ASA deve ter a configuração apropriada de TrustSec na relação a fim receber o tráfego rotulado:

```
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
```

Nota: Somente versão ASA 9.6.2 e colocação de etiquetas Inline dos apoios mais altos. As versões anterior de um ASA não passam a etiqueta da Segurança através do dataplane ao módulo da potência de fogo. Se um sensor apoia Inline a colocação de etiquetas, tentará primeiramente extrair a etiqueta do tráfego. Se o tráfego não é etiquetado, o sensor cai de volta ao método do mapeamento USER-IP.

# Troubleshooting

## Do shell restrito de um dispositivo da potência de fogo

Para indicar o Policy Pushed do controle de acesso de 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
```

Nota: As etiquetas do grupo de segurança especificam dois números: `[7:6]`. Neste conjunto de número, "`7`" é o ID exclusivo do base de dados local SGT, que é sabido somente a FMC e a sensor. "`6`" é o número real SGT conhecido a todos os partidos.

Para ver os logs gerados quando SFR processar o tráfego de entrada e a política de acesso de avaliação:

```
> 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
```

O exemplo de Firewall-motor-`debuga` para o tráfego de entrada com inline colocação de etiquetas:

```
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
```

## Do modo de especialista de um dispositivo da potência de fogo

> Cuidado: A seguinte instrução pode impactar o desempenho de sistema. Execute o comando somente para o propósito de Troubleshooting, ou quando pedidos de um engenheiro de suporte da Cisco para estes dados.

O módulo da potência de fogo empurra o USER-IP que traça ao processo local do Snort. Para verificar que Snort sabe sobre o mapeamento, você pode usar o comando seguinte enviar a pergunta para roncar:

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

Successfully commanded snort.
```

Para ver os dados, entre ao modo de especialista:

```
> expert

admin@firepower:~$
```

O Snort cria um arquivo da descarga sob o diretório de `/var/sf/detection_engines/GUID/instance-x`. O nome do arquivo da descarga é `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
-------------------
~
```

A saída acima mostra que o Snort está ciente de um endereço IP 10.201.229.94 qual é traçado a SGT ID 7, que é o número 6 SGT (convidados).

## Do centro de gerenciamento da potência de fogo

Você pode rever os logs ADI para verificar uma comunicação entre FMC e ISE. Para encontrar os logs do componente `DDA`, verifique o arquivo de `/var/log/messages em` FMC. Você observará logs como abaixo:

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>*