Contents

Introduction

Cisco TrustSec utilizes tagging and mapping of Layer 2 Ethernet frames to segregate traffic without affecting existing IP infrastructure. Tagged traffic can be treated with security measures with greater granularity.

Integration between the Identity Services Engine (ISE) and Firepower Management Center (FMC) allows TrustSec tagging to be communicated from the client authorization, which can be used by Firepower to apply access control policies based on the client's Security Group Tag. This document discusses the steps to integrate ISE with the Cisco Firepower technology.

Components Used

This document uses following components in the example setup:

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

Overview

There are two ways for a sensor device to detect the Security Group Tag (SGT) assigned to the traffic:

1. Through User-IP mapping
2. Through Inline SGT tagging

The User-IP Mapping Method

To ensure TrustSec information is used for access control, the integration of ISE with an FMC goes through the following steps:

Step 1: FMC retrieves a list of the Security Groups from ISE.

Step 2: Access control policies are created on FMC that includes Security Groups as condition.

Step 3: When endpoints authenticate and authorize with ISE, session data is published to FMC.

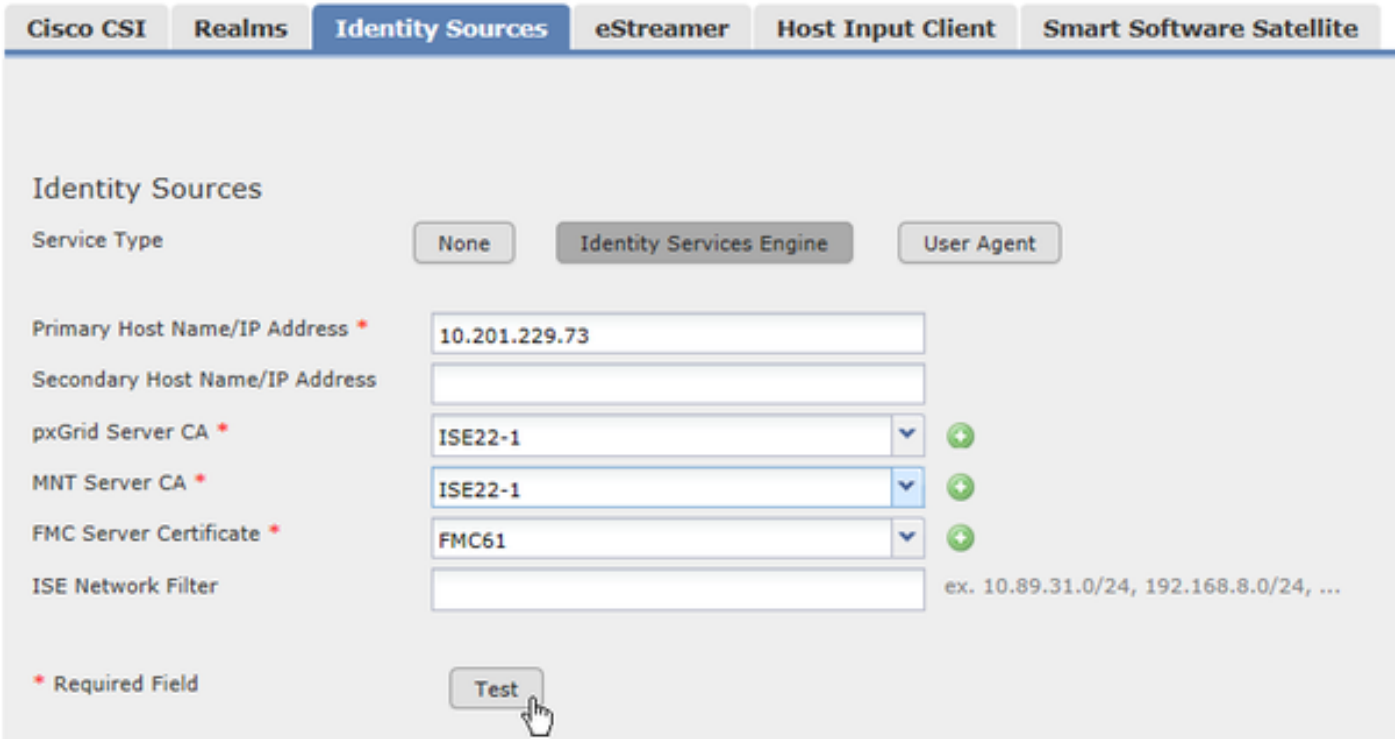
Step 4: FMC builds a User-IP-SGT mapping file, and pushes it to the sensor.

Step 5: The source IP address of the traffic is used to match Security Group using session data from the User-IP mapping.

Step 6: If the Security Group of the traffic source matches the condition in the access control policy, action is taken by sensor accordingly.

An FMC retrieves a complete SGT list when the configuration for ISE integration is saved under **System > Integration > Identity Sources > Identity Services Engine**.

Note: Clicking **Test** button (as shown below) does not trigger FMC to retrieve SGT data.



The communication between FMC and ISE is facilitated by ADI (Abstract Directory Interface), which is a unique process (there can only be one instance) running on FMC. Other processes on FMC subscribe to ADI and request information. Currently the only component that subscribes to ADI is the data correlator.

FMC saves the SGT in a local database. The database contains both the SGT name and number, but currently FMC uses a unique identifier (Secure Tag ID) as handle when processing SGT data. This database is also propagated to the sensors.

If ISE Security Groups are changed, such as removal or addition of groups, ISE pushes a pxGrid notification to FMC to update the local SGT database.

When a user authenticates with ISE and authorizes with a Security Group Tag, ISE notifies FMC

through pxGrid, providing the knowledge that user X from realm Y has logged in with SGT Z. FMC takes the information and inserts into the user-IP mapping file. FMC uses an algorithm to determine the time to push the acquired mapping to the sensors, depending on how much network load is present.

> **Note**: FMC does not push all User-IP mapping entries to sensors. For FMC to push mapping, it must first have knowledge of the user through the Realm. If the user in the session is not part of the Realm, sensors will not learn the mapping information of this user. Support for non-Realm users is considered for future releases.

The Firepower System Version 6.0 only supports IP-User-SGT mapping. Actual tags in the traffic, or SGT-IP mapping learned from SXP on an ASA are not used. When the sensor picks up incoming traffic, the Snort process takes the source IP and looks up the User-IP mapping (which is pushed by Firepower module to the Snort process), and finds the Secure Tag ID. If it matches the SGT ID (not SGT number) configured in the access control policy, then the policy is applied to the traffic.

The Inline Tagging Method

Starting from ASA version 9.6.2 and ASA Firepower module 6.1, Inline SGT tagging is supported. This means the Firepower module is now capable of extracting SGT number directly from the packets without relying on User-IP mapping provided by FMC. This provides an alternative solution for TrustSec-based access control when the user is not part of the Realm (such as devices not capable of 802.1x authentication).

With the Inline Tagging Method, the sensors still replies on FMC to retrieve SGT groups from ISE and push the SGT database down. When traffic tagged with the Security Group number reaches the ASA, if the ASA is configured to trust the incoming SGT, the tag will be passed to the Firepower module through the dataplane. The Firepower module takes the tag from the packets and uses it directly to evaluate access control policies.

ASA must have proper TrustSec configuration on the interface in order to receive the tagged traffic:

```
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
```

> **Note**: Only ASA version 9.6.2 and higher supports Inline Tagging. The earlier versions of an ASA do not pass the Security Tag through the dataplane to the Firepower module. If a sensor supports Inline Tagging, it will first try to extract tag from traffic. If the traffic is not tagged, the sensor falls back to the User-IP mapping method.

Troubleshooting

From the Restricted Shell of a Firepower Device

To display access control policy pushed from 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
```

> **Note**: The Security Group Tags specifies two numbers: `[7:6]`. In this set of numbers, "7" is the unique ID of the local SGT database, which is only known to FMC and sensor. "6" is the actual SGT number known to all parties.

To view logs generated when SFR processes incoming traffic and evaluating access policy:

```
> 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
```

Example of `firewall-engine-debug` for incoming traffic with inline tagging:

```
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
```

From the Expert Mode of a Firepower Device

> **Caution**: The following instruction may impact the system performance. Run the command only for troubleshooting purpose, or when a Cisco Support Engineer requests for this data.

Firepower module pushes User-IP mapping to local Snort process. To verify what Snort knows about the mapping, you can use the following command to send query to Snort:

```
> system support firewall-engine-dump-user-identity-data Successfully commanded snort.
```

To view the data, enter to the expert mode:

```
> expert

admin@firepower:~$
```

Snort creates a dump file under `/var/sf/detection_engines/GUID/instance-x` directory. The name of the dump file is `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 --------
----------- ~
```

The output above shows that Snort is aware of an IP address 10.201.229.94 which is mapped to SGT ID 7, which is SGT number 6 (Guests).

From the Firepower Management Center

You can review the ADI logs to verify communication between FMC and ISE. To find the logs of `adi` component, check the `/var/log/messages` file on FMC. You will notice logs like below:

```
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>
```