De betekenis van op vertrouwen gebaseerde toegangscontrole met FirePower en ISE

Inhoud

Inleiding

Cisco TrustSec gebruikt het taggen en in kaart brengen van Layer 2 Ethernet frames om verkeer te segregeren zonder bestaande IP infrastructuur te beïnvloeden. Gevorderd verkeer kan worden behandeld met beveiligingsmaatregelen met een grotere granulariteit.

Dankzij de integratie tussen de Identity Services Engine (ISE) en het Firepower Management Center (FMC) kan Trustsec-identificatie worden doorgegeven vanaf de autorisatie van de cliënt, die door Firepower kan worden gebruikt voor de toepassing van toegangscontrolemaatregelen op basis van de veiligheidsgroepsmarkering van de klant. Dit document beschrijft de stappen om ISE te integreren met de Cisco Firepower technologie.

Gebruikte componenten

Dit document gebruikt de volgende onderdelen in de voorbeeldinstelling:

- Identity Services Engine (ISE) versie 2.1
- Firepower Management Center (FMC) versie 6.x
- Cisco adaptieve security applicatie (ASA) 5506-X versie 9.6.2
- Cisco adaptieve security applicatie (ASA) 5506-X FirePOWER Module, versie 6.1

Overzicht

Er zijn twee manieren voor een sensor apparaat om de Security Group Tag (SGT) toegewezen aan het verkeer te detecteren:

1. Door gebruiker-IP-omzetting
2. Via inline SGT-markering

De gebruiker-IP-toerekeningsmethode

Om er zeker van te zijn dat vertrouwensinformatie voor toegangscontrole wordt gebruikt, volgt de integratie van ISE met een VCC de volgende stappen:

Stap 1: FMC ontvangt een lijst met beveiligingsgroepen van ISE.

Stap 2: Toegangsbeheer wordt ingesteld op FMC, dat Beveiligingsgroepen als voorwaarde omvat.

Stap 3: Wanneer endpoints authentiek zijn en ISE machtigen, worden de sessiegegevens aan FMC gepubliceerd.

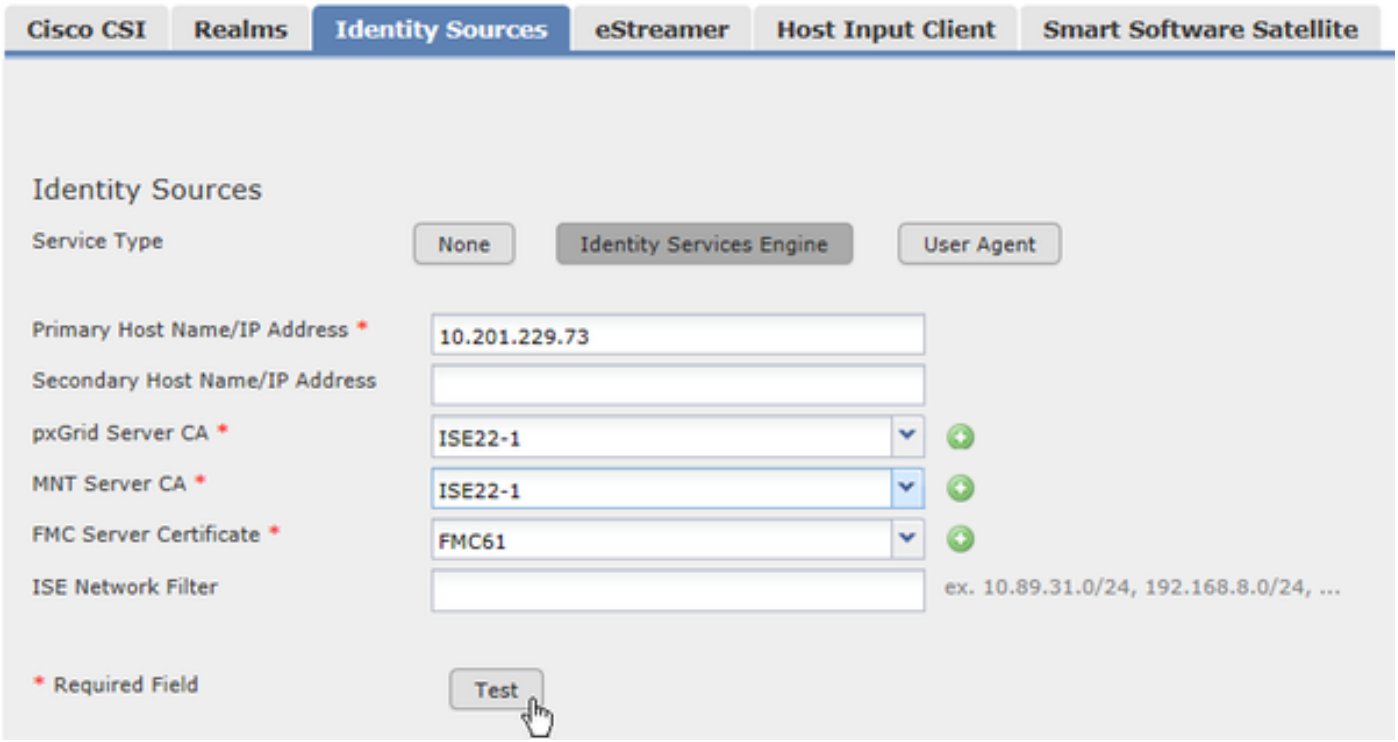
Stap 4: FMC bouwt een User-IP-SGT kaartbestand en duwt het naar de sensor.

Stap 5: Het bron IP-adres van het verkeer wordt gebruikt om beveiligingsgroep aan te passen met behulp van sessiegegevens van de User-IP-afbeelding.

Stap 6: Als de veiligheidsgroep van de verkeersbron de voorwaarde van het toegangscontrolemiddel aanpast, wordt actie door de sensor dienovereenkomstig ondernomen.

Een FMC haalt een volledige SGT-lijst op wanneer de configuratie voor ISE-integratie is opgeslagen onder **System > Integration > Identity Services Engine**.

> Opmerking: Als u op de **Test-**knop klikt (zoals hieronder wordt getoond), wordt FMC niet geactiveerd om SGT-gegevens terug te halen.



De communicatie tussen FMC en ISE wordt vergemakkelijkt door ADI (Abstract Directory Interface), een uniek proces (er kan maar één instantie zijn) dat op FMC loopt. Andere processen op FMC abonneren zich op ADI en vragen om informatie. Op dit moment is de enige component die zich abonneert op ADI de datacorrelator.

FMC slaat de SGT op in een lokale database. De database bevat zowel de SGT-naam als het

SGT-nummer, maar momenteel gebruikt FMC een unieke identificator (Secure Tag ID) als handle bij het verwerken van SGT-gegevens. Deze database wordt ook verspreid naar de sensoren.

Als ISE Security Group gewijzigd is, zoals verwijdering of toevoeging van groepen, drukt ISE een pxGrid-melding aan FMC om de lokale SGT-database bij te werken.

Wanneer een gebruiker zich authentiek verklaart met ISE en met een Markering van de Veiligheidsgroep goedkeurt, waarschuwt ISE FMC door pxGrid, die de kennis verstrekt die gebruiker X van gebied Y met SGT Z heeft ingelogd. FMC neemt de informatie en voegt de informatie toe in het user-IP mapping bestand. FMC gebruikt een algoritme om de tijd te bepalen om de verworven mapping naar de sensoren te duwen, afhankelijk van hoeveel netwerkbelasting er aanwezig is.

> Opmerking: FMC duwt niet alle User-IP mapping ingangen naar sensoren. Om FMC in kaart te kunnen brengen, moet de FMC eerst kennis hebben van de gebruiker via het Realm. Als de gebruiker in de sessie geen deel uitmaakt van het programma, zullen sensoren de mapping informatie van deze gebruiker niet leren. Ondersteuning voor gebruikers die geen banden hebben met het Realm wordt overwogen voor toekomstige releases.

Het Firepower System versie 6.0 ondersteunt alleen IP-User-SGT mapping. Feitelijke tags in het verkeer, of SGT-IP mapping die van SXP op een ASA is geleerd, worden niet gebruikt. Wanneer de sensor inkomend verkeer oppakt, neemt het proces van de Snort de bron IP en kijkt naar de User-IP mapping (die door Firepower module naar het SNIJproces wordt geduwd) en vindt de Secure Tag-ID. Als het overeenkomt met het SGT-ID (geen SGT-nummer) dat is ingesteld in het toegangscontrolebeleid, dan wordt het beleid toegepast op het verkeer.

De methode van inline tagging

Vanaf ASA versie 9.6.2 en ASA Firepower module 6.1 wordt de labeling van inline SGT ondersteund. Dit betekent dat de Firepower module nu in staat is om SGT nummer direct uit de pakketten te halen zonder te vertrouwen op User-IP mapping die door het FMC wordt geleverd. Dit biedt een alternatieve oplossing voor op TrustSec gebaseerde toegangscontrole wanneer de gebruiker geen deel uitmaakt van het Realm (zoals apparaten die geen 802.1x authenticatie in staat zijn).

Met de inline Tagging-methode reageren de sensoren nog steeds op FMC om SGT-groepen van ISE te herstellen en de SGT-database omlaag te duwen. Wanneer het verkeer met het nummer van de Security Group de ASA bereikt, als de ASA is geconfigureerd om de inkomende SGT te vertrouwen, wordt de tag via de dataplane doorgegeven aan de Firepower module. De module Firepower neemt de tag van de pakketten en gebruikt deze direct om het toegangscontrolebeleid te evalueren.

ASA moet een geschikte TrustSec configuratie op de interface hebben om het gelabelde verkeer te ontvangen:

```
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
```

Opmerking: Alleen ASA versie 9.6.2 en hoger ondersteunt inline tagging. De eerdere versies van een ASA passen niet op de Security Tag via de dataplane bij de Firepower module. Als een sensor het afstemmen van inline-tags ondersteunt, zal hij eerst proberen om tag uit het verkeer te halen. Als het verkeer niet is getagd, valt de sensor terug naar de User-IP mapping methode.

Probleemoplossing

Van de beperkte Shell van een FirePOWER-apparaat

U kunt als volgt het toegangsbeheerbeleid van FMC weergeven:

```
> 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
```

Opmerking: De tags van de Security Group geven twee getallen aan: [7:6]. In deze reeks getallen is "7" de unieke ID van de lokale SGT-database, die alleen bekend is bij FMC en sensor. "6" is het aan alle partijen bekende SGT-nummer.

U kunt logboeken weergeven die zijn gegenereerd wanneer SFR inkomend verkeer verwerkt en het toegangsbeleid beoordeelt:

```
> 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
```

Voorbeeld van firewall-motor-debug voor inkomend verkeer met 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
```

Vanaf de Expert-modus van een FirePOWER-apparaat

> **Voorzichtig:** De volgende instructie kan van invloed zijn op de systeemprestaties. Start de opdracht alleen voor de probleemoplossing of wanneer een Cisco Support Engineer om deze gegevens vraagt.

De module van de Firepower drukt Gebruiker-IP mapping naar een lokaal SNIJproces. Om te verifiëren wat Snort over de mapping weet, kunt u de volgende opdracht gebruiken om query naar Snort te verzenden:

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

Successfully commanded snort.
```

U kunt de gegevens als volgt weergeven in de deskundigenmodus:

```
> expert

admin@firepower:~$
```

Snort maakt een dumpbestand onder /var/sf/detectie_engine/ô/Instance-x-folder. De naam van het dumpbestand is user_Identity.dumpen.

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

De bovenstaande output toont dat Snort op de hoogte is van een IP-adres van 10.201.229.94 dat in kaart is gebracht aan SGT ID 7, dat SGT nummer 6 (Guests) is.

Van het FireSIGHT Management Center

U kunt de ADI-bestanden bekijken om de communicatie tussen FMC en ISE te controleren. Om de logbestanden van de adi-component te vinden, controleert u het bestand/var/log/berichten op de FMC. U ziet blogs als volgt:

```
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
.
.
```