Introduction

This document describes how to configure and troubleshoot TrustSec aware policies on Cisco Next Generation Intrusion Prevention System (NGIPS).

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:
Cisco Adaptive Security Appliance (ASA) VPN configuration
- Cisco AnyConnect Secure Mobility Client configuration
- Cisco FirePower Management Center basic configuration
- Cisco ISE configuration
- Cisco TrustSec solutions

Components Used

The information in this document is based on these software and hardware versions:

- Microsoft Windows 7
- Microsoft Windows 2012 Certificate Authority (CA)
- Cisco ASA Version 9.3
- Cisco ISE software Versions 1.4
- Cisco AnyConnect Secure Mobility Client Versions 4.2
- Cisco FirePower Management Center (FMC) Version 6.0
- Cisco FirePower NGIPS Version 6.0

Configure

FirePower Management Center (FMC) is the management platform for FirePower. There are two types of functionalities related to ISE integration:

- Remediation - allows FMC to quarantine the attacker via ISE, which is dynamically changing authorization status on access device providing limited network access. There are two generations of this solution:
  1. Legacy perl script using Endpoint Protection Service (EPS) API call to ISE.
  2. Newer module using pxGrid protocol call to ISE (this module is supported only in version 5.4 - not supported in 6.0, native support planned in 6.1).

- Policy - allows FMC to configure policies based on TrustSec Security Group Tags (SGT).

This article focuses on the second functionality. For Remediation example please read references section

Network Diagram
FMC is configured with Access Control Policy containing two rules:

- Deny for HTTP traffic with custom URL (attack-url)
- Allow for HTTP traffic with custom URL (attack-url) but only if the user is assigned to Audit (9) SGT tag by ISE

ISE decides to assign Audit tag to all Active Directory users that belongs to Administrator group and uses ASA-VPN device for network access.

User accesses network via VPN connection on the ASA. The user then tries to access Audited server using URL attack-url - but fails because he has not been assigned to Audit SGT group. Once that is fixed, the connection is successful.

ISE

Active Directory

AD integration must be configured and the correct groups must be fetched (Administrators group is used for authorization rule condition):

Network Access Device

ASA is added as a network device. Custom group ASA-VPN-Audit is used, as shown in this image:
Certificates for pxGrid and MnT

FMC uses both services on ISE:

- pxGrid for SGT and profiling data query
- Monitoring and Reporting (MnT) for bulk session download

MnT availability is very important since this way FMC is being informed what is the IP address of authenticated session, also its username and SGT tag. Based on that, the correct policies can be applied. Please notice NGIPS does not support natively SGT tags (inline tagging) like the ASA. But in contrary to ASA, it supports SGT names instead of numbers only.

Because of those requirements both ISE and FMC needs to trust each other service (certificate). MnT uses just server side certificate, pxGrid uses both client and server side certificate.

Microsoft CA is used to sign all the certificates.

For MnT (Admin role) ISE must generate certificate signing request (CSR), as shown in this image:

After being signed by Microsoft CA it must be imported via **Bind Certificate** option. Similar process must be followed for pxGrid service. **Certificate(s) will be used for** option must have pxGrid selected.

Since there can not be two certificates with identical Subject Name it is fully acceptable to add different value for OU or O section (for example pxGrid).

**Note:** Please make sure that for every Fully Qualified Domain Name (FQDN) for both ISE
and FMC, the correct DNS record is configured on DNS server.

The only difference between Admin and pxGrid certificate is with signing process. Since pxGrid certificates must have Extended Key Usage options for both Client and Server authentication custom template on Microsoft CA can be used for that:

How to use Microsoft Web service to sign pxGrid CSR is shown in this image:

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded

Saved Request:

```
A824ikCi+VGuqYCd1s1jficXG3ejph2h2mdy/i123
FlbaaEM0X14ayq6G6KX1elLslaXZV8s1IVMFZJ3
zbes2F9d2G535zeyXCCOTh4Wd3E/Naokc/7EexuKV
6G6dakjo0HfTbQfjacr1SklmO6c/XQ2S60Q2A12j
pg+/OQtj3dkW
-----END CERTIFICATE REQUEST-----
```

Certificate Template:

ISE-pxgrid

Additional Attributes:

Attributes:

Submit >
At the end ISE must have Admin and pxGrid certificates signed by the trusted CA (Microsoft) as shown in this image:

pxGrid service

With the correct certificates pxGrid role for specific node must be enabled, as shown in this image:

And automatic approval must be set to enabled:
Authorization Policy

Default authentication policy is used (AD lookup is performed if local user is not found).

Authorization policy has been configured to provide full network access (Permission: PermitAccess) for users authenticating via ASA-VPN and belonging to Active Directory group Administrators - for those users SGT tag Auditors is returned:

FMC

Active Directory Realm

Realm configuration is required in order to work with ISE integration (to use Identity Policies and retrieve group membership for passively authenticated users). Realm can be configured for Active Directory or Lightweight Directory Access Protocol (LDAP). In this example AD is being used. From **System > Integration > Realm**:

AD-Realm

Enter a description
Standard directory settings are used:

And some of the AD groups are retrieved (to be used as additional condition in Access Control rules):

Certificates for Admin and pxGrid

Although not required, its a good practice to generate CSR for admin access. Sign that CSR using trusted AD, import back the signed certificate, as shown in this image:
CA certificate needs to be added to a trusted store:

The last step is to generate pxGrid certificate used by FMC to authorize to ISE pxGrid service. To generate CSR CLI needs to be used (or any other external machine with openssl tool).

```
admin@firepower:~$ sudo su -
Password:
root@firepower:~#
root@firepower:~#
openssl genrsa -des3 -out fire.key 4096
Generating RSA private key, 4096 bit long modulus
..........
..............
e is 65537 (0x10001)
Enter pass phrase for fire.key:
Verifying - Enter pass phrase for fire.key:
root@firepower:~#
root@firepower:~#
openssl req -new -key fire.key -out fire.csr
You are about to be asked to enter information that will be incorporated into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank For some fields there will be a default value, If you enter ".", the field will be left blank.
-----
Country Code [-]:PL
State or Province Name [-]:
Locality Name [-]:
Organization Name [-]:Cisco
Organizational Unit Name [-]:TAC
Common Name [-]:firepower.example.com
Email Address [-]:
root@firepower:~#
```

Once generated fire.csr, sign it using Microsoft CA (pxGrid template). Import back private key (fire.key) and signed certificate (fire.pem) to FMC Internal Certificate store. For private key use the password set up during generation of the key (openssl genrsa command):
ISE Integration

Once all the certificates are installed configure ISE integration from **System > Integration:**

Use the imported CA for both pxGrid and MnT services certificates validation. For Management Console (MC) use Internal certificate generated for pxGrid.

Identity Policy

Configure Identity Policy which is utilizing previously configured AD Realm for Passive Authentication:
Access Control Policy

For this example the custom URL has been created:

And the two rules in the custom Access Control Policy:

PermitPrivileged-HTTP rule allows all users belonging to AD Administrators group who have been assigned SGT tag. Auditors to execute HTTP attack on all targets.
DenyUnprivileged-HTTP denies that action to all other users.

Also notice that previously created Identity Policy has been assigned to this Access Control Policy. On this tab its not possible to see SGT tags, but those are visible while creating or editing specific rule:

Ensure that policy is assigned to the NGIPS and all the changes are deployed:
Verify

After everything is configured correctly ISE should see pxGrid client subscribing for a Session Service (status Online).

From the logs you can also confirm that FMC has subscribed for TrustSecMetaData (SGT tags) service - got all the tags and unsubscribed.

VPN session establishment

The first test is performed for a scenario when authorization on ISE does not return the correct SGT tag (NGIPS does not allow for Audit tests).

Once VPN session is UP AnyConnect User Interface (UI) can provide more details:
ASA can confirm the session is established:

```
asav# show vpn-sessiondb anyconnect
```

**Session Type:** AnyConnect

<table>
<thead>
<tr>
<th>Username</th>
<th>Assigned IP</th>
<th>Protocol</th>
<th>License</th>
<th>Encryption</th>
<th>Hashing</th>
<th>Bytes Tx</th>
<th>Bytes Rx</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrator</td>
<td>172.16.50.50</td>
<td>AnyConnect-Parent SSL-Tunnel DTLS-Tunnel</td>
<td>AnyConnect Essentials</td>
<td>AnyConnect-Parent: (1)none SSL-Tunnel: (1)RC4 DTLS-Tunnel: (1)AES128</td>
<td>AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA1 DTLS-Tunnel: (1)SHA1</td>
<td>11428</td>
<td>24604</td>
</tr>
</tbody>
</table>

**Group Policy:** POLICY

** Tunnel Group:** SSLVPN

**Login Time:** 12:22:59 UTC Wed Dec 2 2015

**Duration:** 0h:01m:49s

**Inactivity:** 0h:00m:00s

**VLAN Mapping:** N/A

Please notice that ASA does see any SGT tag returned for this authentication. ASA is not configured for TrustSec - so that information is skipped anyway.

ISE is also reporting successful authorization (the log at 23:36:19) - no SGT tag returned:

**FMC getting session data from MnT**

At that stage FMC in /var/log/messages reports a new session (received as a subscriber for pxGrid service) for Administrator username and perform AD lookup for group membership:

```
firepower SF-IMS[3554]: [17768] ADI:adi.LdapRealm [INFO] search '(((sAMAccountName=Administrator))' has the following DN:
```
Unprivileged and Privileged network access

When at that stage user tries to open web browser and access audited server, the connection will be terminated:

```
It can be confirmed by the packet captures taken from the client (TCP RST send as per FMC configuration):
```

```
Once ISE is configured to return, the audit tag ASA session reports:
```

```
asav# show vpn-sessiondb anyconnect
```

Session Type: AnyConnect

<table>
<thead>
<tr>
<th>Username</th>
<th>Index</th>
<th>Assigned IP</th>
<th>Public IP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrator</td>
<td>1</td>
<td>172.16.50.50</td>
<td>192.168.10.67</td>
</tr>
</tbody>
</table>
Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License : AnyConnect Essentials
Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)RC4 DTLS-Tunnel: (1)AES128
Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA1 DTLS-Tunnel: (1)SHA1
Bytes Tx : 11428
Bytes Rx : 24604
Group Policy : POLICY Tunnel Group : SSLVPN
Duration : 0h:01m:49s
Inactivity : 0h:00m:00s
VLAN Mapping : N/A VLAN : none
Audt Sess ID : ac101f6400001000565ee2a3
Security Grp : 9
ISE is also reports a successful authorization (the log at 23:37:26) - SGT tag Auditor is returned:

And the user can access mentioned service:
FMC logging access

This activity can be confirmed by Connection Event report:

First, the user had no SGT tag assigned and was hitting DenyUnprivileged-HTTP rule. Once the auditor's tag has been assigned by ISE (and retrieved by FMC) rule, PermitPrivileged-HTTP is used and access is allowed.

Also notice that to have the display, multiple columns have been removed because normally Access Control Rule and Security Group Tag are displayed as one of the last columns (and horizontal scroll bar needs to be used). That customized view can be saved and reused in the future.

Troubleshoot

FMC debugging

To check the logs of adi component responsible for identity services check /var/log/messages file:

[23509] ADI_ISE_Test_Help:ADI_ISE_Test_Help [INFO] Parsing command line arguments...
[23509] ADI_ISE_Test_Help:adi.ISEConnection [INFO] Preparing ISE Connection objects...

[23509] ADI_ISE_Test_Help:adi.ISEConnection [INFO] Preparing subscription objects...
[23509] ADI_ISE_Test_Help:adi.ISEConnection [INFO] subscribed successfully to EndpointProfileMetaDataCapability
[23509] ADI_ISE_Test_Help:adi.ISEConnection [INFO] registered callback for capability EndpointProfileMetaDataCapability
[23509] ADI_ISE_Test_Help:adi.ISEConnection [INFO] subscribed successfully to TrustSecMetaDataCapability
[23509] ADI_ISE_Test_Help:adi.ISEConnection [INFO] registered callback for capability TrustSecMetaDataCapability
[23509] ADI_ISE_Test_Help:adi.ISEConnection [INFO] Connecting to ISE server...
[23509] ADI_ISE_Test_Help:adi.ISEConnection [INFO] Beginning to connect to ISE server...

connecting to host lise20.example.com .......
stream opened
EXTERNAL authentication complete
authenticated successfully (sasl mechanism: EXTERNAL)
message repeated 2 times
Successfully subscribed
hostnames:lise20.example.com:8910
...successfully connected to ISE server.
Starting bulk download

https://lise20.example.com:8910/pxgrid/mnt/sd/getSessionListByTime

* Trying 172.16.31.210...
Connected to lise20.example.com (172.16.31.210) port 8910 (0)
SSL connection using TLSv1.2 / DHE-RSA-AES256-SHA256
Server certificate: CN=lise20.example.com
start date: 2015-11-21 14:40:36 GMT
expire date: 2017-11-20 14:40:36 GMT
common name: lise20.example.com (matched)

^I issuer: DC=com; DC=example; CN=example-WIN-CA
^I SSL certificate verify ok.

POST /pxgrid/mnt/sd/getSessionListByTime
HTTP/1.1

Host: lise20.example.com:8910
Accept: */*
Content-Type: application/xml
user: firesightisetest-firepower.example.com-0739edea820cc7e04cc7c424200f6f61e9xgrid.cisco.com
Content-Length: 269

Upload completely sent off: 269 out of 269 bytes

< HTTP/1.1 200 OK
< Date: Tue, 01 Dec 2015 23:10:45 GMT
< Content-Type: application/xml
< Content-Length: 1287
< Server: "M"
< "M"
< Connection #0 to host lise20.example.com left intact

bulk download processed 0 entries.
disconnecting pxgrid

Starting reconnection stop
_reconnection_thread exited
stream closed; err_dom=(null) 2015-12-01T23:10:45
destroying client object
INFO]: pxgrid connection shutdown done successfully
[23509] ADI_ISE_Test_HELP:adi.ISEConnection [INFO] destroying pxgrid reconnection
[23509] ADI_ISE_Test_HELP:adi.ISEConnection [INFO] destroying underlying pxgrid connection
[23509] ADI_ISE_Test_HELP:adi.ISEConnection [INFO] destroying pxgrid config
[23509] ADI_ISE_Test_HELP:ADI_ISE_Test_HELP [INFO] ISE identity feed destructor called

[23509] ADI_ISE_Test_HELP:ADI_ISE_Test_HELP [/usr/local/sf/bin/adi_iTestHelp cleanly exits.
[23509] ADI_ISE_Test_HELP:adi.ISEConnection [INFO] Captured Jabberwerx log:2015-12-01T23:10:45 [INFO]: pxgrid library has been uninitialized
[8893] ADI:ADI [INFO] Parent done waiting, child completed with integer status 0
To get more detailed debugs it's possible to kill adi process (from root after sudo) and run it with debug argument:

root@firepower:/var/log# ps ax | grep adi
24047 ? Sl 0:00 /usr/local/sf/bin/adi
24090 pts/0 S+ 0:00 grep adi
root@firepower:/var/log# kill -9 24047
root@firepower:/var/log# /usr/local/sf/bin/adi --debug
</debug>
SGT query via pxGrid
The operation is executed when the Test button is clicked in ISE Integration section or when SGT list is refreshed, while adding rule in Access Control Policy.

For a better view xml content from that log can be copied to xml file and opened by a web browser. You can confirm that specific SGT (audit) is being received as well as all other SGT defined on ISE:
Session query via REST API to MnT

That is also a part of Test operation (please notice that MnT hostname and port is passed via pxGrid). Bulk session download is used:

And parsed result (1 active session received):

 gid = ac101f6400007000565d597f, timestamp = 2015-12-01T23:37:31.191+01:00, state = Started, session_id = 91200007, nas_ip = 172.16.31.100, mac_addr = 08:00:27:23:E6:F2, ip = 172.16.50.50, user_name = Administrator, sgt = Auditors, domain = example.com, device_name = Windows7-Workstation

At that stage NGIPS is tries to correlate that username (and domain) with Realm-AD username:

LDAP is used to find a user and group membership:

Dec 01 23:14:39 firepower SF-IMS[24106]: [24142] ADI:adi.LdapRealm [INFO] adi.cpp:322:HandleLog(): search '(|(|sAMAccountName=Administrator))' has the following DN: 'CN=Administrator,CN=Users,DC=example,DC=com'.

ISE debugs

After enabling TRACE level debug for pxGrid component its possible to check every operation (but without payload/data like on FMC).

Example with SGT tag retrieval:

2015-12-02 00:05:39,352 DEBUG [pool-1-thread-14]{} cisco.pxgrid.controller.query.CoreAuthorizationManager -::: checking core authorization (topic=TrustSecMetaData, user=firesightisetest-firepower.example.com)...
2015-12-02 00:05:39,358 TRACE [pool-1-thread-14]{} cisco.pxgrid.controller.common.LogAdvice -:::::: args: [TrustSecMetaData, subscribe, firesightisetest-firepower.example.com-0739eade820cc77e04cc7c44200f661e@xgrid.cisco.com]
2015-12-02 00:05:39,359 DEBUG [pool-1-thread-14]{} cisco.pxgrid.controller.persistence.XgridDaoImpl -::: groups [Any, Session] found for client firesightisetest-firepower.example.com-0739eade820cc77e04cc7c44200f661e@xgrid.cisco.com
2015-12-02 00:05:39,360 DEBUG [pool-1-thread-14]{} cisco.pxgrid.controller.persistence.XgridDaoImpl -::: permitted rule found for Session TrustSecMetaData subscribe.
total rules found 1

Bugs

CSCuv32295 - ISE may send domain information in username fields
References

- Configure Remediation Services with ISE and FirePower Integration
- Configuring pxGrid in a Distributed ISE Environment
- How-To Deploying Certificates with Cisco pxGrid: Configuring CA-Signed ISE pxGrid Node and CA-Signed pxGrid client
- ISE Version 1.3 pxGrid Integration with IPS pxLog Application
- Cisco Identity Services Engine Administrator Guide, Release 2.0
- Cisco Identity Services Engine API Reference Guide, Release 1.2 – Introduction to External RESTful S...
- Cisco Identity Services Engine API Reference Guide, Release 1.2 – Introduction to the Monitoring RES...
- Cisco Identity Services Engine Administrator Guide, Release 1.3
- Technical Support & Documentation – Cisco Systems