LTRSEC-2002
ISE integration with Firepower using pxGrid protocol

Vibhor Amrodia
Designated Support Manager
Cisco Systems.

Aditya Ganjoo
High Touch Technical Support
Cisco Systems.

YOUR TIME IS NOW
to
SECURE YOUR NETWORK ACCESS
Task 1: Getting Access to the LAB from the Computer ................................................................. 8
   Step 1: Accessing the Admin Client PC to Manage the ASAv, FMC and ISE
   Step 2: IP assignment for devices
   Step 3: Access DNS/AD server to create test users
   Step 4: Permissions on AD Server

Task 2: Configuring ASAv (Firewall) ............................................................................................. 13
   Step 1: Accessing the ASAv via ASDM
   Step 2: Generating Identity certificate on ASAv
   Step 3: Enabling TCP state bypass on ASAv and split-tunnel on ASAv
   Step 4: Adding Radius Server on ASAv
   Step 5: Configuring Anyconnect on ASAv

Task 3: Configuring Identity Services Engine (ISE) and pxGrid ...................................................... 26
   Step 1: Accessing the Identity Services Engine (ISE)
   Step 2: Adding ASAv as a AAA client
   Step 3: ISE AD integration
   Step 4: ISE MnT and pxGrid Certificate Installation
   Step 5: Enabling pxGrid services on ISE
   Step 6: Authorization Policy on ISE
   Step 7: Configuring Anyconnect on ASAv

Task 4: Configuring FMC .................................................................................................................... 34
   Step 1: Configuration for FTD in Inline Mode (Registration)
   Step 2: Assigning Interfaces and Inline Sets on FMC
   Step 3: Generate Identity certificate for FMC
   Step 4: Creating Access Policies on FMC
   Step 5: FMC integration with ISE

Task 5: Testing AnyConnect Client for Network Access ................................................................. 4
   Step 1: Accessing the Test Client PC
   Step 2: Testing the Anyconnect Client
   Step 3: Generate Identity certificate for FMC
   Step 4: Creating Access Policies on FMC
   Step 5: FMC integration with ISE
Verify/Test the traffic ................................................................................................................................. 47
   Step 1: Test 1 ICMP test
   Step 2: Test 2 TFTP test
   Step 3: CheckFMC logs
   Step 4: Check ISE logs
   Step 5: Check ASAv logs

Summary................................................................................................................................................... 54
Related Sessions at Ciscolive......................................................................................................................... 55
Introduction/Learning Objectives

Upon completion of this lab, you will be able to:

- Understand the role of ISE, pxGrid and Firepower in Network Infrastructure.
- Implement Firepower with ISE using pxGrid to make your network secure and compliant.
- Verify/Troubleshoot the common issues while implementation.
Prerequisites

The information in this document is based on these software version

- Microsoft Windows 7
- Microsoft Windows 2012 Certificate Authority (CA)
- Cisco ASAV Version 9.8
- Cisco ISE software Versions 2.1 patch 3
- Cisco AnyConnect Secure Mobility Client Versions 4.4
- Cisco FirePower Management Center (FMC) Version 6.2.0.2
- Cisco FirePower NGIPS Version 6.2.0.2

Disclaimer

This training document is to familiarize with Identity Service Engine and FMC as a product. Although the lab design and configuration examples could be used as a reference, it’s not a real design, thus not all recommended features are used, or enabled optimally. For the design, related questions please contact your representative at Cisco, or a Cisco partner. Else feel free to reach out to us. We will be glad to answer.

Scenario

In this lab activity, you will learn how to configure and test Cisco ISE, FMC with pxGrid integration. Configuration with respect to devices:

- **ISE:**
  - ISE integration with Active directory (AD).
  - Adding ASAv as a radius client.
  - Creating authorization rules in ISE with authorization policy for
  - Certificate installation for MnT and pxGrid services.
  - Enable pxGrid

- **ASAv:**
  - Configuring the ASAV for RADIUS authentication with ISE
  - Configuring AnyConnect.
  - Certificate installation on ASAV.
- **Firepower and FTD:**
  - Integration of FTD on FMC.
  - Certificate installation on FMC.
  - Configuring Access policies on Firepower.
  - Configuring the AD realm.

## Pre-Configuration

Due to limited duration of this lab, we have some pre-configuration, already configured to save your time. Please find the details:

- Active Directory setup.
- Certificate Authority setup.
- DNS setup.
- ASAv configuration:
  - Interface Configuration
  - SSH, HTTPS configuration
  - Default route
  - NTP configuration
  - Dynamic PAT for ISE to reach the NTP server
  - Hostname configuration: ASAv

- Configuring the network on ESXI server.
- FMC configuration:
  - Management IP configuration using configure-network command
  - Hostname: vFMC
  - Patch upgrade

- FTD configuration:
  - Management IP
  - Hostname: vFTD
  - `Configure manager add command cisco123` --- Used for FMC registration.
Network Diagram
Task 1: Getting Access to the LAB from the Computer

Step 1.1 Accessing the Admin Client PC to Manage the ASAv, FMC and ISE

- Click on Anyconnect and enter the IP "72.163.218.175". Enter the credentials ciscolive1/ciscolive1 to get connected to the LAB network.
- Open a RDP session and enter the following details to RDP to the Management PC:
  o Connect: 192.168.x.100 (x being the VLAN assigned to your POD)
  o If you get any warning, please click on "Continue".
  o Login using the below credentials:
    - Username: Windows-Cisco-Live
    - Password: cisco123

Step 1.2 IP assignment for devices

- Assignment of IP's for the devices:
  - ASAv – 10.0.0.10 (Internal)
  - ASAv – 192.168.x.220 (External)
  - FMC - 10.0.0.20
  - ISE - 10.0.0.30
  - AD/DNS/CA server – 10.0.0.40
  - FTD – 10.0.0.60
  - Management PC – 192.168.x.100
  - Anyconnect PC – 192.168.x.150

  - x being the VLAN assigned to your POD

Step 1.3 Access DNS/AD server to create test users

- You need to create two users for accessing the management and Anyconnect VM's that are a part of ciscolive.com domain.
  - RDP to the DNS/AD machine from the management VM with IP 10.0.0.40
  - Enter credentials: Username: Ciscolive\Administrator
  - Password: Admin@123
  - Click Start, point to Programs, point to Administrative Tools, and then click Active Directory Users and Computers.
In the Active Directory Users and Computers window, expand `<domain name>.com`.

- Right-click **Users**, point to **New**, and then click **User**.
- In the **New Object - User** dialog box, do the following:
  - First name: Type a first name for the account.
  - User logon name: Type the appropriate account name from the previous list.
  - In the **Password** box, type a password for the account, and then in the **Confirm password** box, type the password again.
  - Select **User cannot change password** and **Password never expires**, and then click **Next**.
  - Click **Finish**.

## Step 1.4 Permissions on AD Server

### Audit Policies

- Ensure that the "Audit Policy" (part of the "Group Policy Management" settings) allows successful logons to generate the necessary events in the Windows Security Log of that AD domain controller machine (this is the default Windows setting, but you must explicitly ensure that this setting is correct). Run `gpedit.msc` > *Local Computer Policy* > *Computer Configuration* > *Windows Setting* > *Security Setting* > *Advanced Security Setting* > *System Audit Policies* > *Logon*. Here make sure Audit Logon are set to Success.
Permissions on registry

Permissions Required when an Active Directory User is a Member of the Domain Admin Group

For Windows 2008 R2, Windows 2012, and Windows 2012 R2, the Domain Admin group does not have full control on certain registry keys in the Windows operating system by default. In order to get the ISE to add the AD as a Domain Controller, Active Directory admin must give the Active Directory User Full Control permissions on the following registry keys:

```
HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}
HKEY_LOCAL_MACHINE\Software\Classes\Wow6432Node\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}
```

In order to grant full control, the Active Directory admin must first take ownership of the key. To do this:

Type Regedit.exe in Run
Right Click on the Key and go to permissions.
Select Advanced and then navigate to the permissions TAB.

- Change the owner to the user that is going to be used to join the node.
- Click OK twice.
Permissions to Use DCOM on the Domain Controller

The Active Directory user must have permissions to use DCOM (remote COM) on the Domain Controller. You can do this by using the dcomcnfg tool.

- Run the dcomcnfg tool from the command line.
- Expand Component Services.
- Expand Computers and click on My Computer.
- Select Action from the menu bar, click on properties OR Right Click on My Computer and click on COM Security.

- Make sure that account for both Access and Launch has Allow permissions. The Active Directory user should be added to all the four options (Edit Limits and Edit Default for both Access Permissions and Launch and Activation Permissions).
- Allow all Local and Remote access for both Access Permissions and Launch and Activation Permissions.

WMI management
Permissions to the WMI Root\CIMv2 Name Space
The Active Directory users do not have the Execute Methods and Remote Enable permissions by default. These can be granted by using the wmic.msc MMC console.

- Click Start > Run and type wmic.msc.
- Right-click WMI Control and click Properties.
- Under the Security tab expand Root and choose CIMV2.
Click Security.

- Find the Active Directory user and check for the required permissions (Execute Methods, Enable Account, Remote Enable)

**Task 2: Configuring ASAv (Firewall)**

**Step 2.1 Accessing the ASAv via ASDM**

- Double click the "ASDM" launcher icon on the desktop and login with the following details:
  - Device IP Address: 10.0.0.10
    - Username: cisco
    - Password: cisco
  - Click “Continue” on the certificate security warning to trust the certificate.

**Step 2.2 Generating Identity certificate on ASAv**

- Open ASDM and navigate to Configuration > Device Management > Certificate management
  - Click on the Identity certificate tab and add an Identity certificate
    - Add a Trustpoint name and generate a new key-pair of 2048 bits.
- You need to add the Certificate Subject DN information as 
  `CN=asav.ciscolive.com`
- Click on add certificate and save it on desktop:
Download certificate from Certificate server:

- Access the Certificate Authority GUI by entering `http://10.0.0.40/certsrv`.
- Open the CSR file and copy and paste the CSR file content on the CA dashboard and click submit:
Download the certificate in base64 format and install the certificate on ASDM and click the apply button at the bottom:
Step 2.3  Enabling TCP state bypass and split-tunnel on ASAv

- Due to the topology, we are using we need to enable TCP state bypass on ASAv since the default gateways of the Anyconnect VM and Management VM are different resulting in asymmetric routing. >>>>> This is not recommended as this would bypass all the ASAv checks. This has been configured to get the RDP access of the Anyconnect VM.

- Click on the putty tab on the management VM and enter the ASAv IP 10.0.0.10.
  - Credentials: cisco/cisco

- Create an access-list to permit TCP state bypass for Anyconnect VM and the management VM. It is a bi-direction Access-list. Enter into the config terminal mode:

  access-list TCP-BYPASS extended permit ip 192.168.100.0 255.255.255.0 host 192.168.x.150
  access-list TCP-BYPASS extended permit ip host 192.168.x.150 192.168.100.0 255.255.255.0

- Create a class-map to match the access-list:

  class-map BYPASS
  match access-list TCP-BYPASS
Create a policy-map to match the class-map and set the tcp-state-bypass for this traffic:

```
asav(config)# policy-map global_policy
asav(config-pmap)# class BYPASS
asav(config-pmap-c)# set connection advanced-options tcp-state-bypass
```

**Split Tunnel Configuration (Required for RDP access of the Anyconnect VM)**

- Log into the ASA CLI and create a standard ACL for the network:
  ```
  access-list split standard permit 192.168.100.0 255.255.255.0
  ```

- Add this split tunnel under the group-policy of the Anyconnect profile:
  ```
  asav(config)#group-policy <> internal
  asav(config)#group-policy <> attributes
  asav(config-group-policy)#split-tunnel-policy tunnelspecified
  asav(config-group-policy)#split-tunnel-network-list value split
  ```

**Step 2.4 Adding Radius Server on ASAv**

- On ASDM, navigate to Configuration > Device Management > Users/AAA > AAA server groups
  - Click on Add > Add AAA Server Groups and add the AAA server group information:
  - Add the sever name and Realm-id. Put 1 in the realm-id field.
Make the similar changes as shown in this image:
Click on **Add > (servers in the selected group) Server Name or IP address tab** and add the AAA server group information as shown in the snapshot and click on apply:
Step 2.5 Configuring Anyconnect on ASAv

- On ASDM, navigate to:
  a. Wizards > VPN Wizards > Anyconnect VPN Wizard
b. Give a name to the Anyconnect Connection Profile:

```
Connection Profile Name: Anyconnect VPN
```

c. Select the protocols that you would like to use for the Anyconnect VPN connection:

```
IPSec (IKEv1) Remote Access VPN Wizard
IPSec (IKEv2) Remote Access VPN Wizard
```

d. Select the Anyconnect Client Image. If you don’t have one already on the flash, upload one from the Local Machine which should be under the Files folder created on the desktop:

![Add AnyConnect Client Image](image1.png)

![AnyConnect VPN Connection Setup Wizard](image2.png)

e. Select the Authentication Server for the VPN connections(ISE):
f. Select the VPN address pool for the assigned IP’s for the VPN connections:

- Add 10.0.1.1 as starting address and 10.0.1.100 as the end address with 255.255.255.0 mask.


g. Select the other settings for the VPN configuration (DNS, WINS etc.):

- DNS IP should be configured as 10.0.0.40
h. Create a NAT exempt for this VPN traffic:

![NAT Exempt](image1)

i. This is an informational screen showing the deployment types for the Anyconnect VPN:

![Deployment Types](image2)
j. This would show you the summary of all the changes which would be pushed to the ASA device:

k. Save the configuration on the device by clicking save button tab shown on ASDM.

l. After doing these changes Navigate to Configuration > Network Client Access > Anyconnect Profiles

  - Add the accounting server information by editing the profile and go to Accounting section > Add the server group info and save the configuration.
  - Also, create an Anyconnect Client Profile for the RDP access since we are using Anyconnect from a remote VM machine.
  - Navigate to Configuration > Network Client Access > Anyconnect Client profile
  - Add a new profile and then edit it.
  - Go to Preferences Part 1 and select Allow Remote Users under Windows VPN Establishment as shown in the image.
LTRSEC-2002 ISE integration with Firepower using pxGrid protocol
LTRSEC-2002 ISE integration with Firepower using pxGrid protocol
Task 3: Configuring Identity Services Engine (ISE) and pxGrid

Step 3.1 Accessing the Identity Services Engine (ISE)

- Double click the “Mozilla Firefox” browser icon on the desktop and navigate to https://10.0.0.30
- Use the following credentials to login:
  - Username: admin
  - Password: Adm!n123

Step 3.2 Adding ASA as a AAA client

- Navigate to tab ISE GUI > Administration > Network Resources > Network Devices.
- Click on ‘Add’. Fill the below mentioned mandatory fields:
  - Name: ASA
  - IP Address: 10.0.0.10 (Where, ‘x’ is the number written on your lab slip)
- Check the ‘RADIUS Authentication Settings’ and configure below mentioned shared secret:
  - Shared Secret: cisco
- Click on ‘Submit’
Step 3.3  ISE AD integration

- Navigate to tab ISE GUI > Administration > External Identity Sources > Active Directory.
  - Click on ‘Join’. Fill the below mentioned mandatory fields:
    - AD username: admin
    - Password: Admin@123
  - Click on Save button and the click on Test User tab for testing the AD connectivity.
Step 3.4  ISE MnT and pxGrid Certificate Installation

- Navigate to ISE GUI > Administration > Certificates > Certificate Management > Certificate Signing Requests
  - Usage type should be set to Multi-use
  - Enter the CN name as ise.ciscolive.com
  - Generate the CSR and export the request on the desktop
Navigate to the browser and enter the CA server IP (same that we used before) and get the certificate signed.
Microsoft Active Directory Certificate Services -- example-WIN-CA

Submit a Certificate Request or Renewal Request

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

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

Certificate Template:

ISE-pxgrid

Additional Attributes:

Attributes:

Submit >

- Verify the certificate installation on ISE node:
LTRSEC-2002 ISE integration with Firepower using pxGrid protocol

Step 3.5 Enabling pxGrid services on ISE

- Navigate to ISE GUI > Administration > Deployment > Edit node list > Check pxGrid service
  - Save the settings

With the correct certificates pxGrid role for specific node must be enabled, as shown in this image:
Navigate to ISE GUI > Administration > pxGrid Services to check the clients enabled for pxGrid communication:

And automatic approval must be set to enabled:

**Step 3.6 Authorization Policy on ISE**

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 ASAv-VPN and belonging to Active Directory Group Administrators - for those users SGT tag Auditors is returned:

- Navigate to ISE GUI > Policy > Policy Sets and click on Policy > Policy Elements > Authorization >Simple Conditions and create two policies for AD-GROUP and ASA-Device as shown:
Navigate to ISE GUI > Policy > Policy Sets

- Click on the ‘Default’ policy set in the left pane and expand ‘Authorization Policy’:
  - Configure the rule as per the following details:
    - Rule Name: ASAVPN (In place of ‘Standard Rule 1’)
    - Click on the ‘+’ sign next to ‘Condition(s)’:
      - Click on ‘Select condition from Library’.
      - Click on ‘+’ sign next to ‘Select Attribute’.
      - Under Description, click on ‘simple condition drop down menu and select AD-GROUP
      - Add another simple condition for ASA-Device
    - Permissions/Authorization Profile:
      - Click on the drop down and select Security Group and Auditors
      - Click on the ‘+’ sign and select Standard and PermitAccess.
      - Click on ‘Done’ on the right.
  - Click on the ‘Save’ button at the bottom of the page.
Task 4: Configuring FMC

Step 4.1 Configuration for FTD in Inline Mode (Registration)

Navigate to FMC GUI:

- Device IP Address: 10.0.0.20 (You should see a bookmark on Firefox)

- Click on Device > Device Management > Add > Add Device and enter the FTD details:
  - Host: 10.0.0.60
  - Display Name: vFTD
  - Registration key: cisco123
  - Group: None
  - Access Control Policy: Initial-Policy
Once you click on Register, it will start the registration and once it is completed, you should see the tasks as below:

![Tasks](image)

Also, device would show as online on the Registration Screen:

![Device](image)
Step 4.2 Assigning Interfaces and Inline Sets on FMC

➢ Navigate to FMC GUI:

   o Click on Devices > Device Management
   o Click on FTD-V now and go to Interfaces section:
     • Click on Edit interface (right side button) for GigabitEthernet0/0
     • Assign the name as ASAv-Interface and check the enabled button
     • Click on OK.
     • Repeat the same procedure for GigabitEthernet0/1 and name it as VM-Interface
     • Save the changes and click on deploy

➢ Creating Inline Sets

➢ Navigate to FMC GUI:

   o Click on Devices > Device Management
   o Click on FTD-V now and go to Inline Sets tab section:
Click on the add Inline Set tab and assign a name
Click on the available interface pairs and add it under the selected interface pair
Click on OK.
Save the changes and click on deploy

**Step 4.3 Generate Identity certificate for FMC**

- Navigate to **FMC GUI > System > Configuration > HTTPS certificate** and click on **Generate New CSR**:

  ![Generate Certificate Signing Request](image)

- Upload the contents on the certificate server as you did for ASA v and download the certificate.
- Import the HTTPS Server Certificate and verify:
Step 4.4   Creating Access Policies on FMC

➢ Navigate to FMC GUI > Policies > Access Control:

  o You need to click on the Default-policy that should be already there.
  o Click on the edit button and click on the Add Rule button.
- Navigate to Users tab and add the AD server users.
- Go to applications tab and type TFTP and ICMP and select them:

![Editing Rule - SGT-Block](image1)

- Navigate to SGT/ISE attributes and select Security Group tag.
- Select Metadata as Auditors and add it.

![Editing Rule - SGT-Block](image2)

- Go to the logging tab on the right side and select the log at beginning of connection.
Select the Action as Permit/Block as per the requirement and hit the save button.

Ensure that policy is assigned to the NGIPS and all the changes are deployed:
Verification of the rules:
Step 4.5  FMC integration with ISE

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

Use the imported CA for both pxGrid and Mn 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:
LTRSEC-2002 ISE integration with Firepower using pxGrid protocol
Task 5: Testing AnyConnect Client for Network Access

### Step 5.1 Accessing the Test Client PC

- RDP on the Anyconnect VM and enter the following details:
  - Remote Host: 192.168.195.4x
    (Where, ‘x’ is the number written on your lab slip)
  - Click on "Connect".

### Step 5.2 Testing AnyConnect Client

- On Client PC which is external to the network (RDP to 192.168.x.150):
  - Open the Mozilla Firefox browser from the task bar.
  - Navigate to [https://asav.ciscolive.com](https://asav.ciscolive.com) (ASAv-IP)
  - Welcome to SSL VPN Service page. Please login with the user credentials, we created on the ISE:
    - Group: Anyconnect
    - USERNAME: Anyconnect >>> Created by you on the AD server
    - PASSWORD: Admin@123
  - Click “Anyconnect VPN” on the following popup to run the AnyConnect Secure Mobility client without any restriction:
After the Anyconnect is downloaded, browse it from Start Panel and click on it.

In the address bar enter asav.ciscoclive.com

Hit the connect button and enter the same credentials
- Group: Anyconnect
- USERNAME: Anyconnect
LTRSEC-2002 ISE integration with Firepower using pxGrid protocol

- PASSWORD: Admin@123

Now, the VPN connection is being established.

- We are connected to the VPN now.
Task 6: Verify/Test the traffic

- After the Anyconnect is connected open the command line on the machine.

### Step 6.1  Test 1: ICMP test

- Ping the management VM IP (192.168.x.100) from the cmd.
- It should be denied as per the policy.
Step 6.2  Test 2: TFTP test

- Initiate a TFTP file transfer from the Anyconnect VM to Management VM.

- Use the following command to test the TFTP application:

  `tftp -i 192.168.x.100 GET test.txt` (where x is the VLAN no.) and test.txt is a file on the server

- It should be denied as per the policy.
| host       | transfers the file to a remote host. |
| GET        | specifies the file destination on the remote host. |
| PUT        | transfers the file source on the local host to the file destination on the remote host. |
| source     | specifies the file to transfer. |
| destination| specifies where to transfer the file. |

C:\Users\Myconnect-UM\Desktop>ftp LOCAL PUT CA.cer 192.168.168.100
ftp: don't know host 'LOCAL'
C:\Users\Myconnect-UM\Desktop>ftp local PUT CA.cer 192.168.168.100
ftp: don't know host 'local'
C:\Users\Myconnect-UM\Desktop>ftp -i 192.168.168.100 GET CA
Timeout occurred
C:\Users\Myconnect-UM\Desktop>ftp -i 192.168.168.100 GET CA
Connect request failed
C:\Users\Myconnect-UM\Desktop>ftp -i 192.168.168.100 GET Ch
Connect request failed
C:\Users\Myconnect-UM\Desktop>ftp -i 192.168.168.100 GET Ch.cer
Transfer successful: 1286 bytes in 1 second(s), 1286 bytes/s
C:\Users\Myconnect-UM\Desktop>ftp -i 192.168.168.100 GET Ch.cer
ftp: can't write to local file 'Ch.cer'
C:\Users\Myconnect-UM\Desktop>ftp -i 192.168.168.100 GET PMc-Lags
Transfer successful: 2866824 bytes in 304 second(s), 9430 bytes/s
C:\Users\Myconnect-UM\Desktop>ftp -i 192.168.168.100 GET PMc-Lags
Connect request failed
C:\Users\Myconnect-UM\Desktop>ftp -i 192.168.168.100 GET PMc-Lags
Connect request failed
C:\Users\Myconnect-UM\Desktop>ftp -i 192.168.168.100 GET PMc-Lags
Connect request failed
C:\Users\Myconnect-UM\Desktop>ftp -i 192.168.168.100 GET PMc-Lags
Connect request failed
C:\Users\Myconnect-UM\Desktop>
Step 6.3  Check FMC logs

➢ Navigate to FMC GUI:

Check under Analysis > Connections > Events for block events as shown below
TFTP application is getting blocked on the basis of SGT tags.

- Navigate to FMC GUI > Analysis > Users and we should be able to see the AD users:

Step 6.4 Check ISE logs

- Navigate to ISE GUI > Administration > pxGrid Services > Live Log:
- From the logs you can also confirm that FMC has subscribed for TrustSecMetaData (SGT tags) service - got all the tags and unsubscribed.
• Navigate to ISE GUI > Operations > Radius Livelog

• Please notice that ASA does see any SGT tag returned for this authentication. ASA is not configured for Trust Sec - so that information is skipped anyway. ISE is also reporting successful authorization
Step 6.5 Check ASAv logs

```
ash# sh vpn-sessiondb anyconnect

Session Type: AnyConnect

Username : anyconnect            Index    : 11419
Assigned IP : 10.0.1.1            Public IP : 192.168.168.150
Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License : AnyConnect Premium
Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-256 DTLS-Tunnel: (1)AES256
Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA384 DTLS-Tunnel: (1)SHA1
Bytes Tx : 15020            Bytes Rx    : 1441
Group Policy : GroupPolicy_Anyconnect Tunnel Group : Anyconnect
Login Time : 18:11:24 UTC Wed Jun 21 2017
Duration : 0h:01m:53s
Inactivity : 0h:00m:00s
VLAN Mapping : N/A            VLAN : none
Audit Sess ID : 0a000000a02c9b000594ab6cc
Security Grp : 9
```

Summary

This is to familiarize you with the initial configuration and testing of deploying Firepower with ISE using pxGrid. Deployment also allows you to understand the packet flow and understand basic troubleshooting steps. This is the first critical step in the process of securing your endpoints.

End: Please Inform the Proctor that you have completed the lab.

Thank You! Have a Wonderful Day 😊

Related Sessions at CiscoLive

You can search CiscoLive Las Vegas content catalog link below with “Firepower” and “FTD” keywords. We have some useful sessions.

https://www.ciscolive.com/us/learn/sessions/session-catalog/?search=firepower&showEnrolled=false

Dissecting Firepower-NGFW(FTD) "Installation & Troubleshooting
Session ID: BRKSEC-3455
Veronika Klauzova, Firepower TAC Team Lead, Cisco

Firepower NGFW Internet Edge Deployment Scenarios
Session ID: BRKSEC-2050
Jeff Fanelli, Principal Systems Engineer, Cisco
Implementing Cisco Firepower NGFW/NGIPS and AMP
Session ID: LTRCRT-2200
Jagdeep Kang, Engineer Content, Cisco
Patrick Lao, Content Engineer, Cisco

Vulnerability Prioritization and Mitigation with Cisco ISE and Firepower
Session ID: VILSEC-1007

Firepower Threat Defense (FTD) Deployment Hands-on Lab
Session ID: LTRSEC-1000
Patrick Gilkey, Technical Solutions Architect, Cisco
Dax Mickelson, Project Consultant, Cisco