|  |
| --- |
| Aston Technologies Inc. |
| Cisco TrustSec – Wired SXP |
| An Aston training document explaining how to deploy SXP for wired devices |

Contents

[Contents 2](#_Toc37926480)

[Lab Diagram 3](#_Toc37926481)

[Add User to AD 4](#_Toc37926482)

[ISE Configuration 5](#_Toc37926483)

[General Settings 5](#_Toc37926484)

[Security Group Tags (SGT) 6](#_Toc37926485)

[TrustSec NDA 8](#_Toc37926486)

[Security Group Tags 8](#_Toc37926487)

[Security Group ACLs 11](#_Toc37926488)

[TrustSec Policy 12](#_Toc37926489)

[Switch Configuration 13](#_Toc37926490)

[Provision Core-SW 13](#_Toc37926491)

[Provision Access Switch 15](#_Toc37926492)

[Configure Core Switch SXP Connection 16](#_Toc37926493)

[Configure Access Switch SXP Connection 16](#_Toc37926494)

[Testing with PC-2 19](#_Toc37926495)

[Conclusion 21](#_Toc37926496)

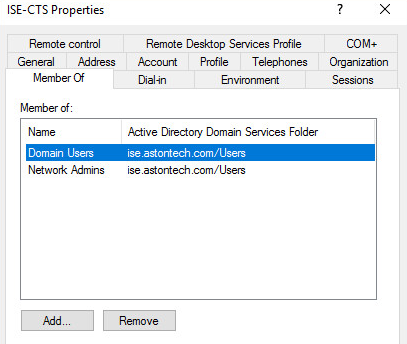
Lab Diagram



Add User to AD

In upcoming labs ISE will need to open a SSH session to the NADs. Since we are using ISE as a TACACS server with AD as the backend authentication the easiest thing to do is add a service account for ISE in Ad.

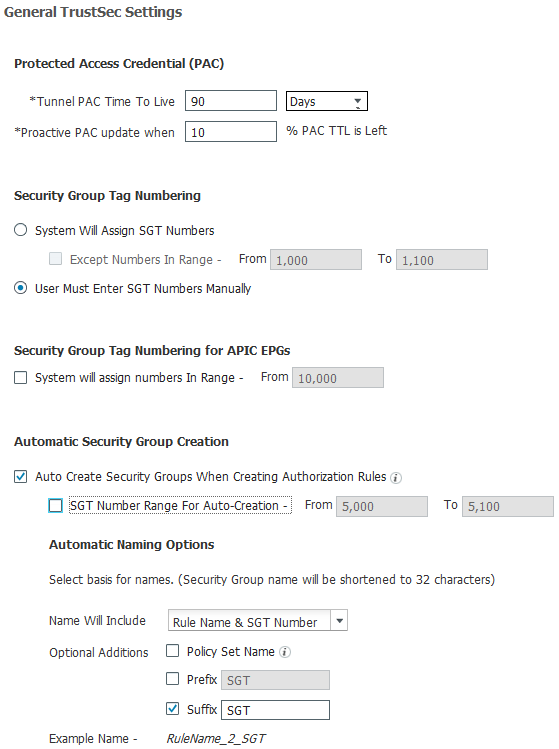
Open a console window to ISE-AD-DC and add a user. Name it **ISE-CTS**, give it a password of **cisco** and make it a member of **Network Admins**.



ISE Configuration

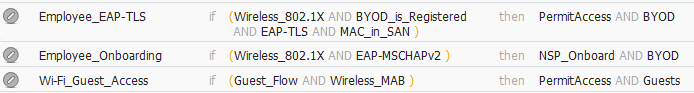
General Settings

Log into ISE and navigate to **Work Centers > TrustSec > Settings > General TrustSec Settings**. Configure the following:

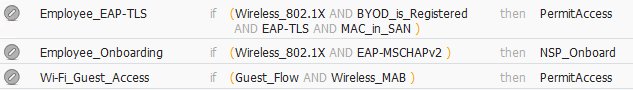


Security Group Tags (SGT)

We are going to edit the default SGTs but first we need to remove the ones Cisco has applied in the Default Policy Set. Navigate to **Policy Sets > Default** and remove the **BYOD** and **Guest** Permissions.



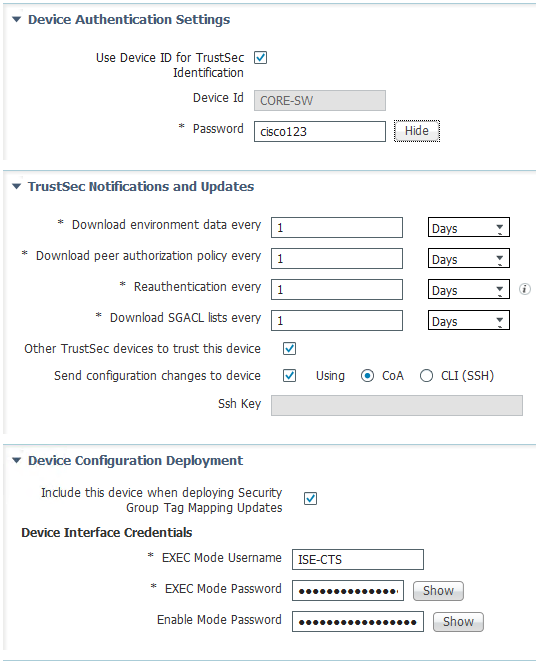
After.



Navigate to **Components > Security Groups**. Delete all the tags except **TrustSec\_Devices** and **Unknown**.



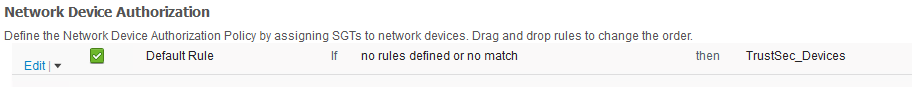
Go down to **Network Devices**. We need to add **TrustSec** to the **Acces-SW** and **Core-SW**. Click into the Core-SW and check the **Advanced** **TrustSec Settings** box and configure the following:



**Device Configuration Deployment** Section is the user you created for ISE in AD which is only needed on the Core-SW for this lab. Now do the same for the other switch except for enabling Device Configuration Deployment.

TrustSec NDA

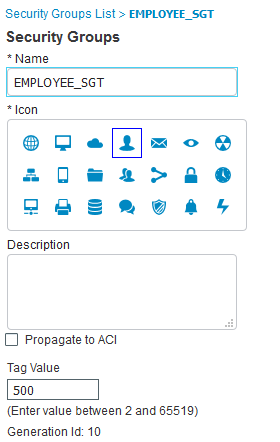
Navigate to **TrustSec Policy > Network Device Authorization** and **Edit the Default Rule**. Change from Unknown to TrustSec\_Devices.



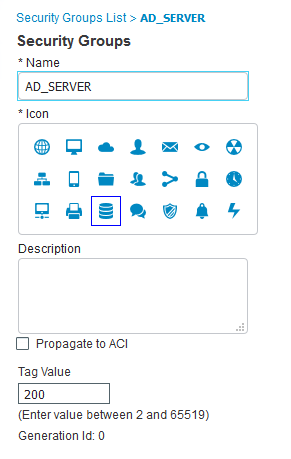
Security Group Tags

Let’s create our Security Group tags that we will apply to the endpoints.

Navigate to **Work Centers > TrustSec > Components > Secuirty Groups**. We are going to add some new ones. Click Add, change the name to **EMPLOYEE\_SGT** and the icon to a **user icon**.

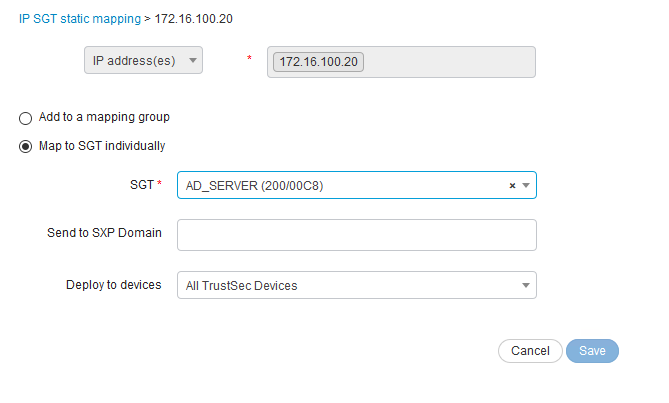


Create a new one and name it **AD\_SERVER** and give it a tag value of **200**.



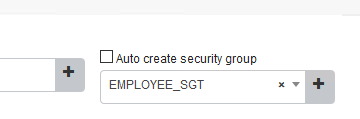
Since the AD server isn’t being authenticated to the network via ISE. We’ll need to create a static mapping. We can configure the mapping locally on the device via CLI or push the mapping out to the device from ISE. We’ll do the latter.

Navigate down to **IP SGT Static Mapping** and click **Add**. Configure the following:



Click **Save**.

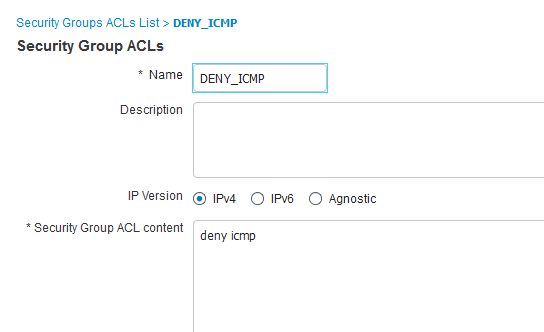
Now that we have the SGT created. Let’s apply them to the authorization policy. Navigate to **Wired** and **Wireless** policy sets and add the tag to the Employee Compliant rule we created.



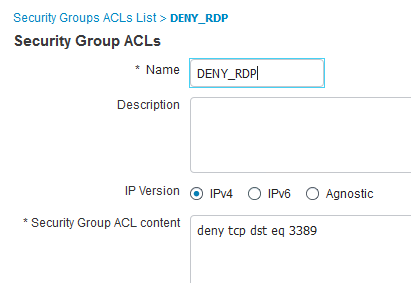
Security Group ACLs

Let’s keep it simple and only add a couple SGACLs. Navigate to **Security Group ACLs** and Click **Add**. SGACLs have a slightly different syntax then your typical ACL, there are no IP addresses or Security group tags referenced.

The first one we are going to create is a rule to **DENY\_ICMP**.



**Add** a second one to deny RDP:



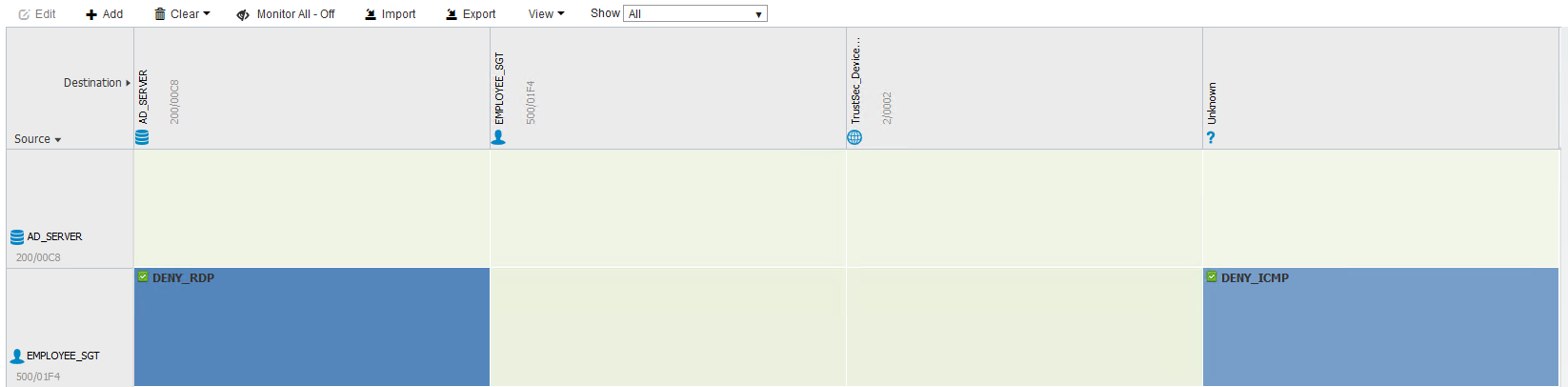
TrustSec Policy

Now it’s almost time to put this all together on the ISE side and start making this work.

In ISE navigate to **Work Centers > TrustSec > TrustSec Policy**. There are 3 ways you can configure policy. You can use the matrix, Source tree and Destination tree. We are going to use the matrix for this after we create the policy go into the source and destination tree and see what’s there.

Let’s just keep it simple, starting with the EMPLOYEE\_SGT group click on the box that is a source of **EMPLOYEE\_SGT** and destination of **AD\_SERVER**. We are going to **DENY\_RDP** then permit everything else.

Next click on the box that is a source of **EMPLOYEE\_SGT** and destination of **UNKNOWN**. We are going to **DENY\_ICMP.**



Switch Configuration

Provision Core-SW

We’ll need to configure the Core-Sw for RADIUS so it can talk to ISE.

Log into the Core-SW and apply the following configuration:

ISE-CORE-SW#cts credentials id CORE-SW password cisco123

!

Conf t

!

aaa group server radius ISE

server name ISE

!

radius server ISE

address ipv4 172.16.100.50 auth-port 1812 acct-port 1813

pac key cisco123

!

aaa authentication dot1x default group ISE

aaa authorization network CTS-LIST group ISE

aaa accounting dot1x default start-stop group ISE

!

cts authorization list CTS-LIST

!

ip radius source-interface Loopback0

!

radius-server vsa send authentication

!

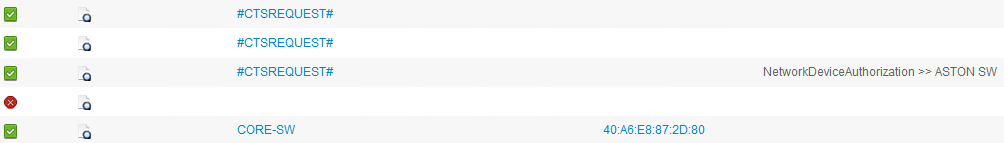
aaa server radius dynamic-author

client 172.16.100.50 server-key cisco123

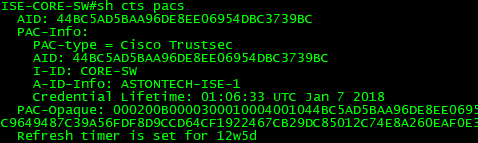
!

dot1x system-auth-control

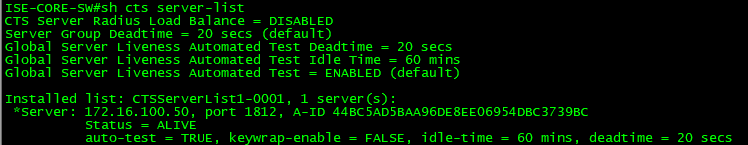
Now if you check the Live Logs you should see some activity from the core switch. Look at the details and see what’s been sent.



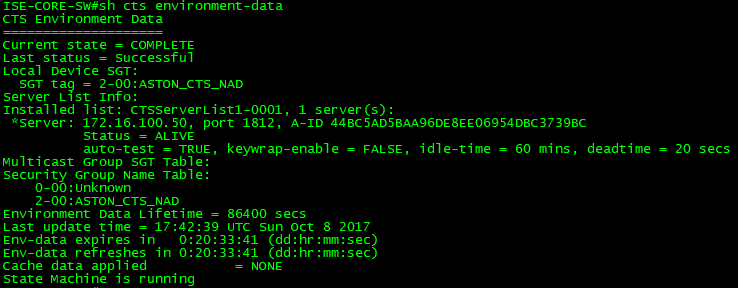
Let’s look at what sent down on switch. We should have downloaded a pac from ISE. Run **Show cts pacs**.



**Show cts server-list**.



**Show cts environment-data**.



Provision Access Switch

Log into the Access-SW and apply these commands.

ISE-ACCESS-SW#cts credentials id Access-SW password cisco123

!

Conf t

!

aaa authorization network CTS-LIST group ISE-GROUP

!

cts authorization list CTS-LIST

!

no radius server ISE

!

radius server ISE

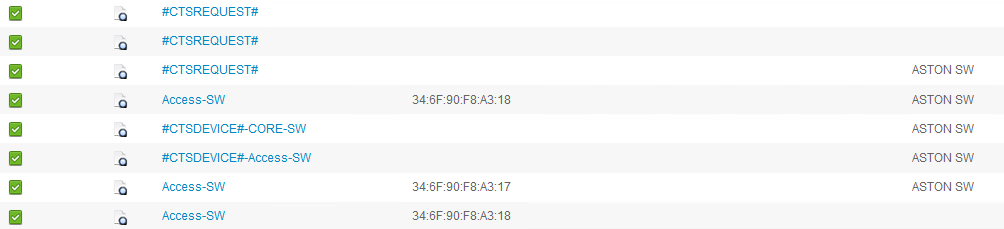
address ipv4 172.16.100.50 auth-port 1812 acct-port 1813

pac key cisco123

!

end

Once the interfaces come back up you should see some activity in ISE. Look into the details on these.



Run the show commands we ran on the core-sw – **show cts pacs, show cts server-list, show cts environment-data**.

Configure Core Switch SXP Connection

We need to configure the switches SXP connection in order to share IP to SGT bindings. WE are going to configure the Core-SW to receive bindings from the Access-Sw. Log into the Core-SW and apply these commands.

Conf t

!

cts sxp enable

!

cts sxp default source-ip 172.16.101.1

!

cts sxp default password cisco123

!

cts sxp connection peer 172.16.101.2 password default mode local listener

!

end

Configure Access Switch SXP Connection

On the Access-Sw configure it to send the bindings to the Core-Sw. Log into the Access-SW and apply these commands.

Conf t

!

cts sxp enable

!

cts sxp default source-ip 172.16.101.2

!

cts sxp default password cisco123

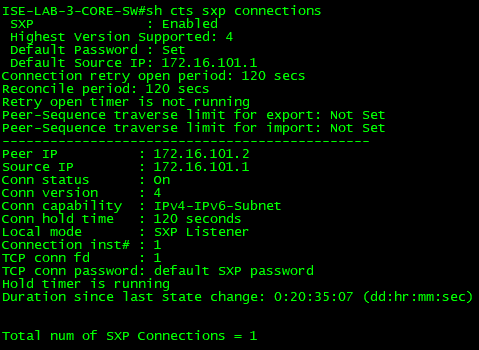
!

cts sxp connection peer 172.16.101.1 password default mode local speaker

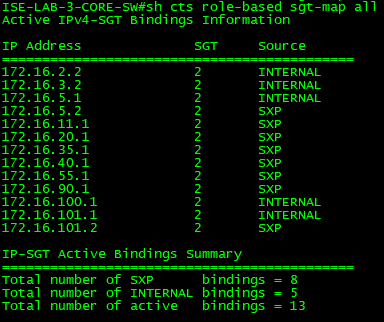
!

end

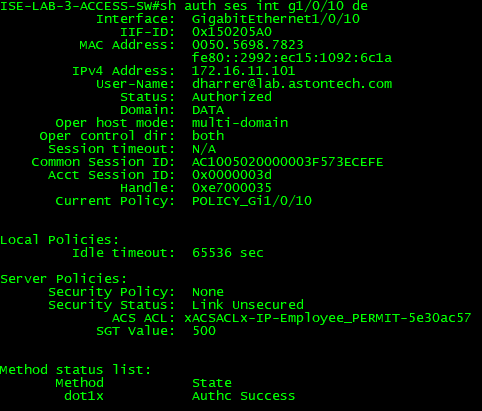
Run the command **show cts sxp connections**. Here we can see info on the SXP connections take note that the status is On, which means the connection has been established.



If we run the command **show cts role-based sgt-map all** on the Core-Sw we can see the SXP mappings being learned from the Access-SW. It is advertising all its internal IP addresses with the tag of 2 (the TrustSec\_Devices tag).



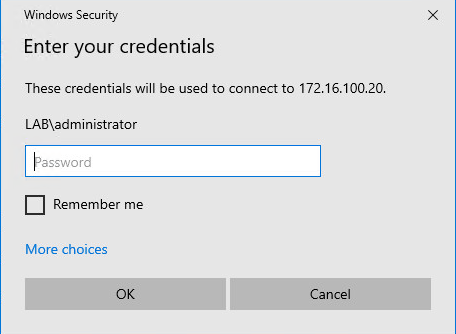
Now connect Lab PC-2 to access-sw interface g1/0/10 and force an authentication. We should now see that our SGT is applied to the session.



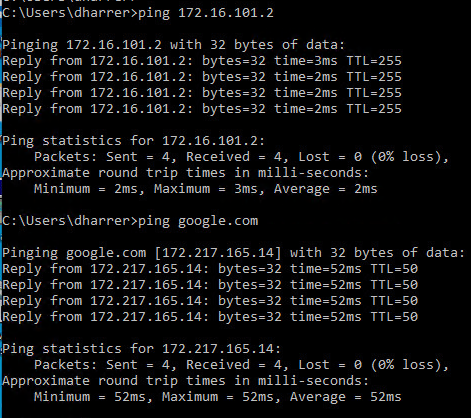
Testing with PC-2

Now we have ISE configured, the switches provisioned, and our SGT applied to the endpoint. However, we haven’t enabled enforcement on the switches yet. Before we do let’s start by testing base access.

From PC-2 test to make sure you can RDP to the AD server. This should work at this point if it doesn’t make sure that Remote Desktop is Enabled on the AD server.



You should also be able to ping anything. Try pinging the access-sw, AD server and something on the internet.



Now let’s enable enforcement on the Access-SW. Configure the following commands:

Conf t

!

cts role-based enforcement

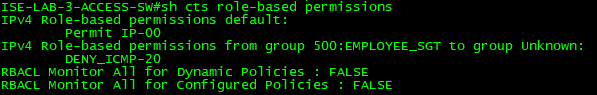
!

cts role-based enforcement vlan-list all

!

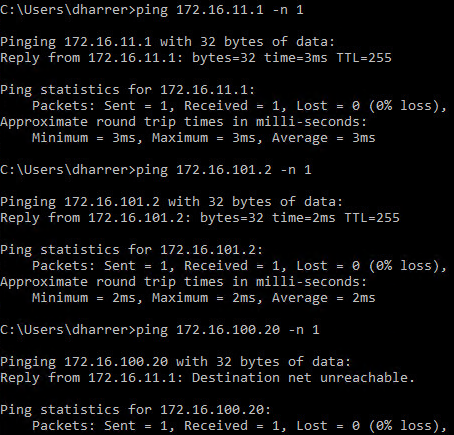
end

You should have now downloaded the policies down from ISE. We can check this with the command **show cts role-based permissions**:



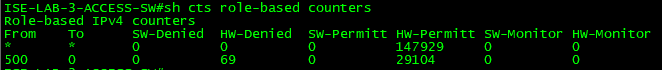
If you don’t see the correct polices you can force a download by running the command **cts refresh policy** in exec mode.

Now test the policy. Try pinging the IPs on the Acces-Sw from PC-2, these should succeed but pinging anything else should fail.

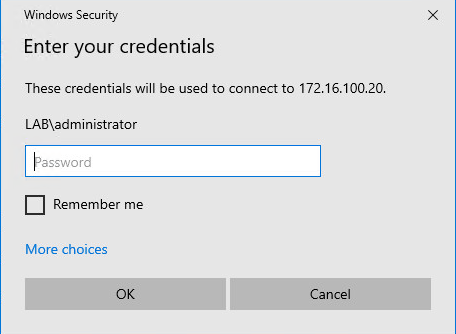


As you can see here we can ping PC-2’s GW and the loopback on the switch but a ping to the AD server fails since the Access-Sw doesn’t have a binding for anything that’s not local to the switch we hit our deny icmp policy.

With the **show cts role-based counters** command you can see the how packets have been allowed and denied.



Try to RDP to the AD server. This should still work.



Now let’s enable enforcement on the Core-SW. This should now block RDP access to the AD server. On the Core-SW type the following commands:

Conf t

!

cts role-based enforcement

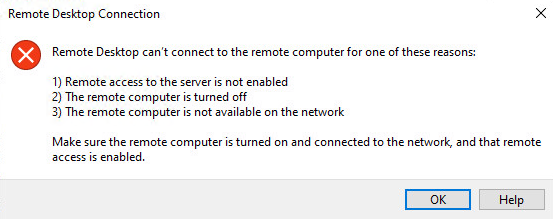
!

cts role-based enforcement vlan-list all

!

end

Try to RDP to the AD server again. This should now fail since we have the mapping configured on the Core-SW.



Feel free to play around with the TrustSec policy to create rules etc. to get a good grip on how it functions. Next we’ll move on to adding in wireless.

Conclusion

In this lab, we have:

* Configured a server user for ISE in AD
* Configured SGTs and added TrustSec support for the NADs in ISE
* Configured our Switches for TrustSec
  + Added RADIUS configuration
  + Configured our uplink interfaces for DOT1X
* Tested our SGTs are being applied to the traffic.

In the next lab, we will continue on with configuring SXP on the wireless side.