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

Contents

[Contents 2](#_Toc37933117)

[Lab Diagram 3](#_Toc37933118)

[ISE Configuration 4](#_Toc37933119)

[Authorization Policy 4](#_Toc37933120)

[NAD Configuration 5](#_Toc37933121)

[Configure WLC SXP Connection 5](#_Toc37933122)

[Configure Core Switch SXP Connection 6](#_Toc37933123)

[Testing with PC-2 7](#_Toc37933124)

[Conclusion 11](#_Toc37933125)

Lab Diagram

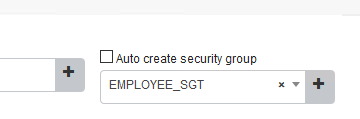


ISE Configuration

Authorization Policy

This lab should be reatlivy quick we have already configured our TrustSec configuration on ISE we will just need to add the configuration on the NADs.

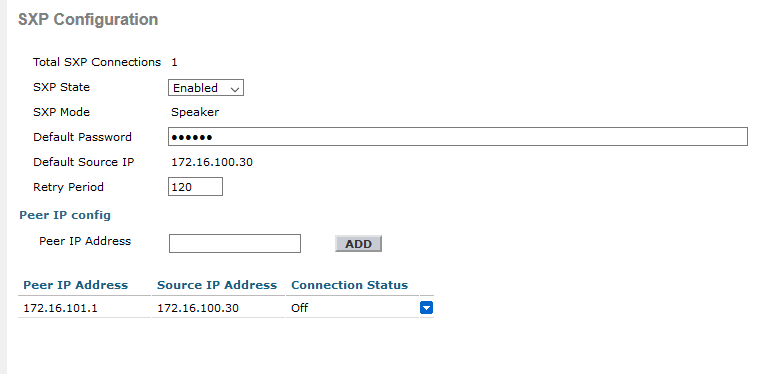
Before we start, navigate to the Wireless policy set and make sure the tag was added to the Employee Compliant rule we created. This should have been done in the previous lab.



NAD Configuration

Configure WLC SXP Connection

We need to configure the WLC SXP connection in order to share IP to SGT bindings. WE are going to configure the Core-SW to receive bindings from the WLC. Log into the WLC and navigate to **Security > TrustSec > SXP Config**. Configure the **default password** (cisco123) and hit **Apply**. Then **enable SXP** and configure the **Peer address** as seen below:



Then hit **Apply** again.

Configure Core Switch SXP Connection

We’ll need to configure the SXP connection from the WLC in order to share IP to SGT bindings. Log into the Core-SW and apply these commands.

Conf t

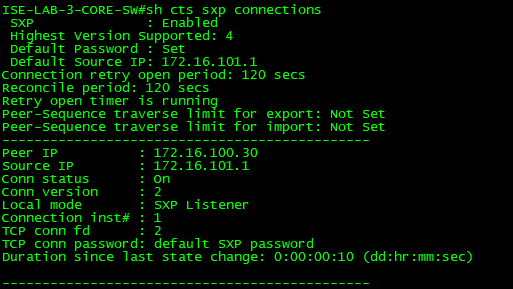
!

cts sxp connection peer 172.16.100.30 password default mode local listener

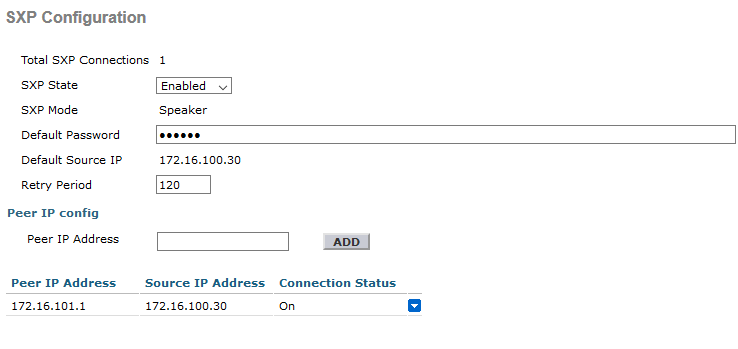
!

end

If we check the connection on the switch, we should see that it is now on.



And on the WLC side if we check back, we should see a connection status of On.



Testing with PC-2

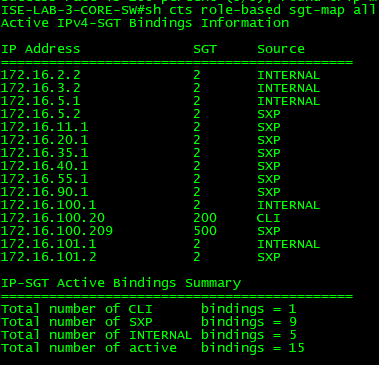
Connect PC-2 to the wireless network by adding the Wireless USB to the host and connect to the wireless network. Once authenticated we should have our SGT of 500 applied to the session. We can check this in a few places.

First on ISE in the live logs, then we can also check the WLC and switch.

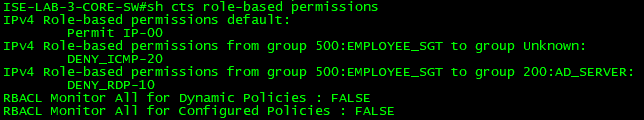
On the WLC go to **Monitor > Clients** then click on the client’s MAC address. If you scroll down about halfway you should see our SGT applied.



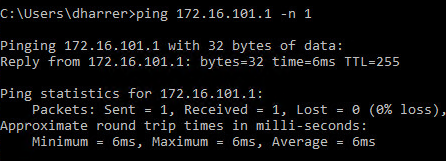
Then on the Core-SW if we run the command show cts role-based sgt-map all. We should see our mapping applied.

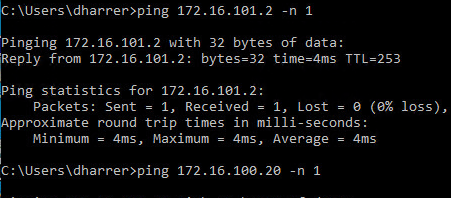


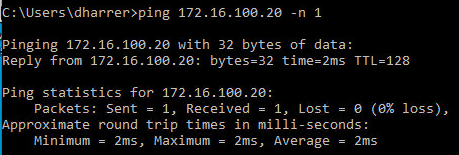
Now on the Core-sw just double check let’s look at the permissions to make sure that match expectations. You should see something like the following:

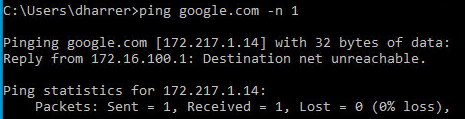


Now let’s start testing by pinging the switches, AD server and anything else on the internet. You should find that you can ping the switches and AD but nothing else should work.

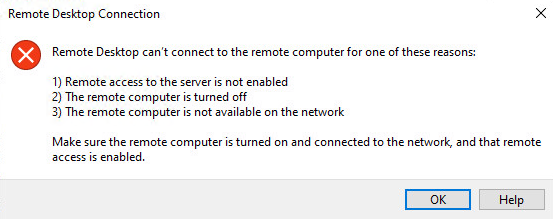




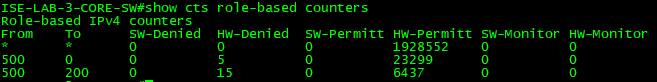




Try to RDP to the AD server. This should fail since we have the mapping configured on the Core-SW.



You can check the counters to see the Hardware denied and permitted counts.



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 the WLC for SXP
* Configured our Core Switch for the WLC SXP connection TrustSec
* Tested our SGTs are being applied to the traffic and the SGACL are enforced.

In the next lab, we will continue on with configuring inline on the wired side.