|  |
| --- |
| Aston Technologies Inc. |
| Cisco TrustSec –Inline Wired |
| An Aston training document explaining how to deploy inline wired TrustSec |

Contents

[Contents 2](#_Toc37948797)

[Lab Diagram 3](#_Toc37948798)

[Configure Core-SW 4](#_Toc37948799)

[Configure Access Switch 8](#_Toc37948800)

[Testing with PC-2 10](#_Toc37948801)

[Conclusion 14](#_Toc37948802)

Lab Diagram



Configure Core-SW

For these labs connect to the external Core and Access Switches Management interfaces. We are going to be bringing down the interfaces to configure the inline connection which will affect connectivity to the devices.

Connect the Core Switch’s mgmt. IP. We’ll remove the SXP connection to the Access-SW since we’ll be configuring inline.

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

Conf t

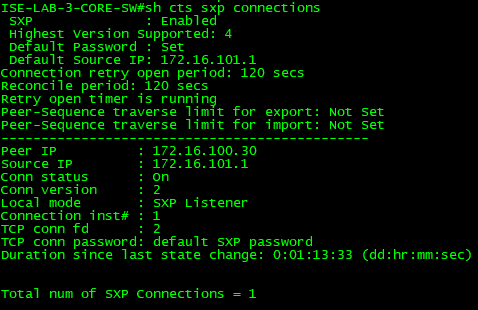
!

no cts sxp connection peer 172.16.101.2 password default mode local listener

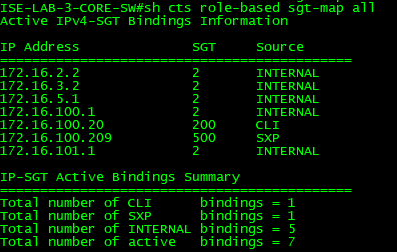
!

end

Check the SXP connections on the switch. We should only have the WLC now.



Also, we can check the mappings to see what they look like. You should have only the internal IPs, our AD server and possibly the host that is connected to our corporate wireless network.



In this lab we’re also going to configure Netflow on these interfaces so we can see if the SGTs are working without having to look at pcaps. Run the following commands on Core-SW.

Conf t

!

flow record FLEX\_NET\_REC

match ipv4 protocol

match ipv4 source address

match ipv4 destination address

match transport source-port

match transport destination-port

match flow cts source group-tag

match flow cts destination group-tag

collect counter bytes long

collect counter packets long

!

flow monitor NETFLOW

cache timeout active 120

record FLEX\_NET\_REC

!

Interface range g1/0/23 – 24

shutdown

no channel-group 10 mode on

cts manual

policy static sgt 2 trusted

channel-group 10 mode on

ip flow monitor NETFLOW input

ip flow monitor NETFLOW output

no shutdown

!

end

Now we are going to configure the interfaces for inline and apply the netflow configuration. Apply the following commands:

Conf t

!

Interface range g1/0/23 – 24

shutdown

no channel-group 10 mode on

cts manual

policy static sgt 2 trusted

channel-group 10 mode on

ip flow monitor NETFLOW input

ip flow monitor NETFLOW output

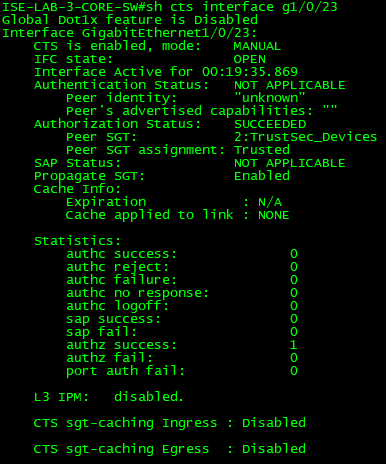
no shutdown

!

end

!

We can check the interfaces cts status by running the command **show cts interface g1/0/x**.



Configure Access Switch

Log into the Access-SW from the MGMT IP. We are going to remove the SXP configuration and apply the netflow and inline configurations.

Conf t

!

no aaa authorization config-commands

!

no cts sxp enable

no cts sxp default source-ip 172.16.101.2

no cts sxp default password cisco123

no cts sxp connection peer 172.16.101.1

!

flow record FLEX\_NET\_REC

match ipv4 protocol

match ipv4 source address

match ipv4 destination address

match transport source-port

match transport destination-port

match flow cts source group-tag

match flow cts destination group-tag

collect counter bytes long

collect counter packets long

!

!

flow monitor NETFLOW

cache timeout active 120

record FLEX\_NET\_REC

!

Interface range g1/0/23 – 24

shutdown

no channel-group 10 mode on

cts manual

policy static sgt 2 trusted

channel-group 10 mode on

ip flow monitor NETFLOW input

ip flow monitor NETFLOW output

no shutdown

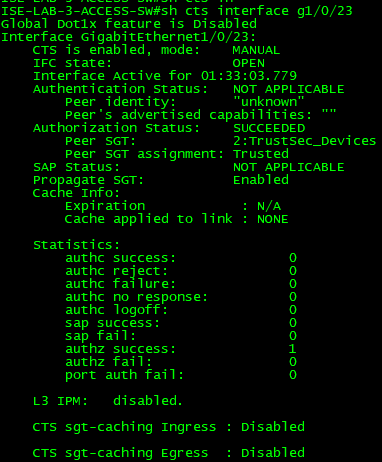
!

aaa authorization config-commands

!

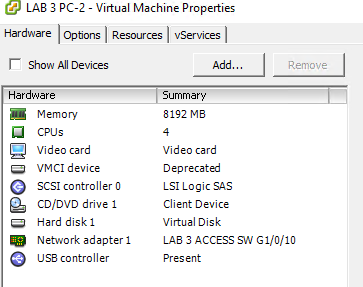
end

Let’s check the interfaces cts status by running the command **show cts interface g1/0/x.**

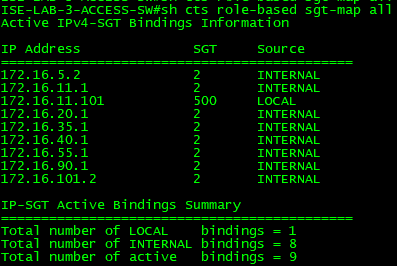


Testing with PC-2

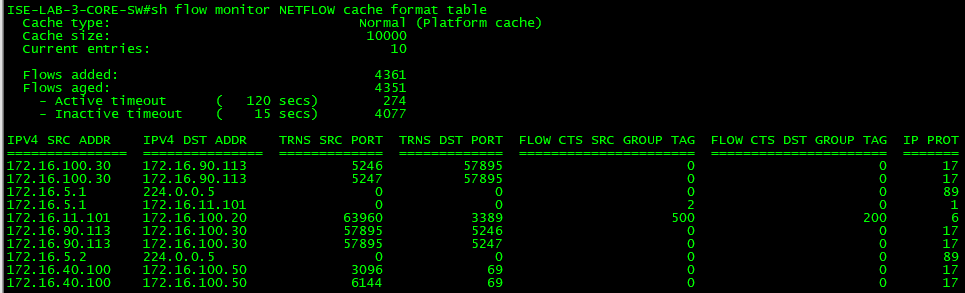
Remove the wireless USB adaptor from PC-2 and reconnect the ethernet adaptor.



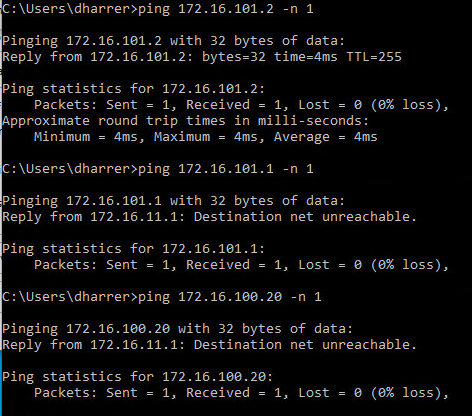
After the device has authenticated check to see if we have our mapping with the **show cts role-based sgt-map all** command.



Try RDP’ing to the AD server. This should fail according to our policy. If we check the netflow data on the core-sw we can see that the traffic from SGT 500 to 200 is there on port 3389. The Command for that is **show flow monitor NETFLOW cache format table**.



Now test by ping the access-sw(172.16.101.2), core-sw(172.16.101.1) and the AD server.



Notice that only the ping to the access-sw worked. That’s not what we want according to policy we created. We should be able to ping the access-sw, core-sw and AD and nothing else.

If you remember back to the wired SXP lab we couldn’t ping the AD server either because we don’t have the AD mapping on the access-sw. We could correct that by simply configuring the mapping on the access switch. That’s what we would have to do in this scenario for SXP but with inline we can move the enforcement point to the core-sw.

On the access-sw configure the following:

Conf t

!

Interface range g1/0/23 – 24

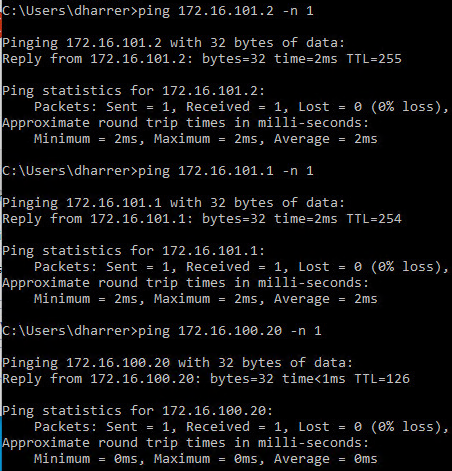
no channel-group 10 mode on

no cts role-based enforcement

channel-group 10 mode on

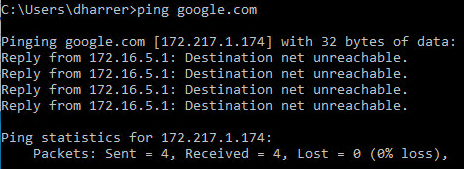
!

Now let’s try pinging everything again.



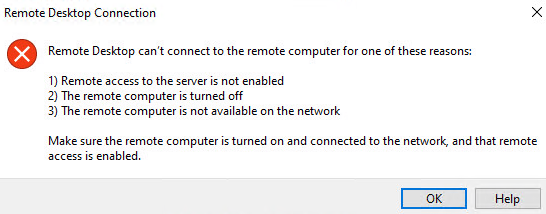
Now all the pings to the access-sw, core-sw and AD work.

Try pinging the internet.



Notice the reply is from the core-sw.

Now try to RDP to the AD server again. This should still fail.



These TrustSec labs are just a very basic example of function. I suggest that you spend some time to play around with this. Create new rules, SGTs, SGACLs and combine wired with wireless devices to really get an understanding of behavior.

Conclusion

In this lab, we have:

* Configured our Switches for native TrustSec (inline)
* Configured Netflow for testing visibility
* Tested our SGTs are being applied to the traffic and enforcement.