|  |
| --- |
| Aston Technologies Inc. |
| Cisco Identity Services Engine (ISE) Posture Assessment via VPN |
| An Aston training document explaining how to deploy ISE Posturing over VPN |

Contents

[Contents 2](#_Toc41500684)

[Lab Diagram 3](#_Toc41500685)

[ASA Configuration 4](#_Toc41500686)

[Adding ACLs 4](#_Toc41500687)

[Edit Group Policy 5](#_Toc41500688)

[ISE Configuration 6](#_Toc41500689)

[Client Provisioning 6](#_Toc41500690)

[Policy Elements 6](#_Toc41500691)

[Posture Policy 10](#_Toc41500692)

[Policy Set 10](#_Toc41500693)

[Testing 11](#_Toc41500694)

[Network Admin Account 11](#_Toc41500695)

[Employee Account 19](#_Toc41500696)

[Conclusion 23](#_Toc41500697)

Lab Diagram



ASA Configuration

Adding ACLs

Like what we did with the wired posture we need to create a redirect ACL for the posture module to get to ISE.

Log into the ASA either CLI or ASDM and add the following access-list:

access-list REDIRECT\_ACL extended deny udp any any eq domain

access-list REDIRECT\_ACL extended permit tcp any host 72.163.1.80 eq www

We are going to add an IP to our split-tunneling ACL. One of the discovery methods of the ISE Posture module is to send a http request to enroll.cisco.com which resolves to 72.163.1.80. We want that to go through the tunnel and hit the REDIRECT\_ACL we just created.

access-list SPLIT-TUNNEL-ACL standard permit host 72.163.1.80

Edit Group Policy

Since we are running split tunneling on our VPN we are going to push the ISE posture module to anyone connecting to the Employee Group Policy. Rather than having them connect and going to an internal web site to force a redirect to the provisioning portal.

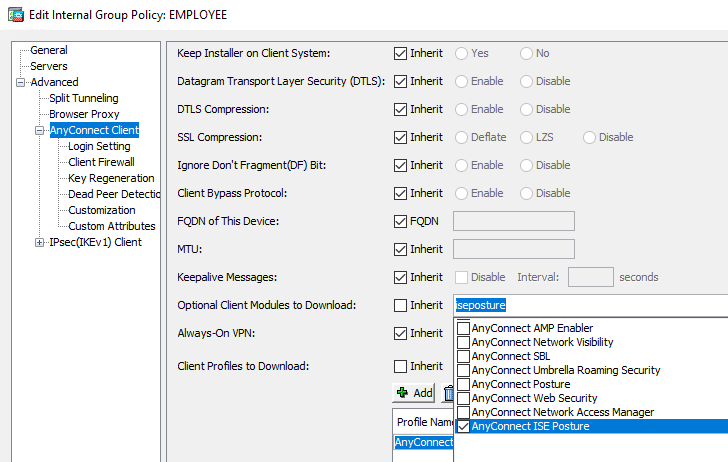
Commands for that via CLI:

group-policy EMPLOYEE attributes

webvpn

anyconnect modules value iseposture

In ASDM go to **Configuration > Remote Access VPN > Network (Client) Access > Group Policies** then select **EMPLOYEE** and hit **Edit**. Expand the **Advanced** tab and click on **AnyConnect Client**. Uncheck the **Optional Client Modules to Download** checkbox and select **AnyConnect ISE Posture**.

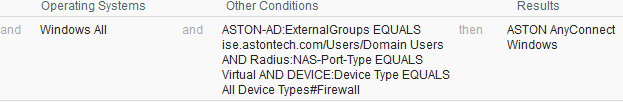


ISE Configuration

Client Provisioning

We have the AnyConnect ISE Posture module install covered for anyone who doesn’t have it installed already with the ASA but we still need to push the Compliance module and the profile out. We’ll need to configure a new Client Provisioning Policy that will match the conditions of users connecting via VPN.

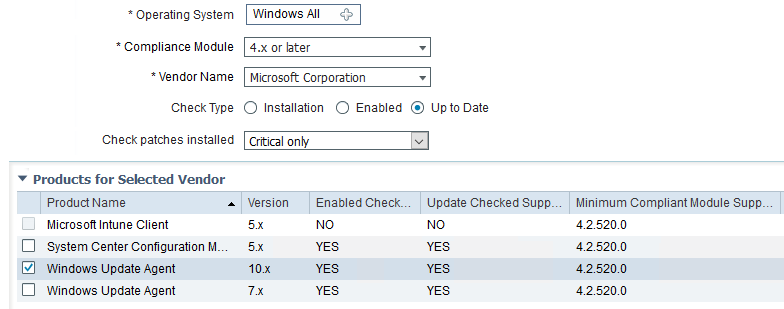
Log into ISE and navigate to **Work Centers > Posture > Client Provisioning > Client Provisioning Policy**. Insert a new policy and name it **ASTON VPN POSTURE WIN**. Operating System will be **Windows All**. For conditions **ASTON-AD:ExternalGroups EQUALS Domain Users AND Radius:NAS-Port-Type EQUALS Virtual AND DEVICE:Device Type EQUALS Device Type#All Device Types#Firewall**. Then give it **ASTON AnyConnect Windows**. Then hit **Save**.



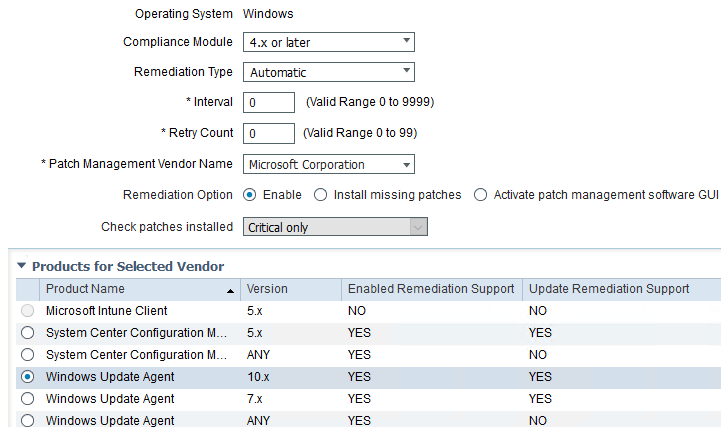
Policy Elements

We already have our 3 posture checks we configured previously but for VPN let’s add another. These VPN users are road warriors and aren’t in the office often. We want to make sure that they are getting updates from Microsoft.

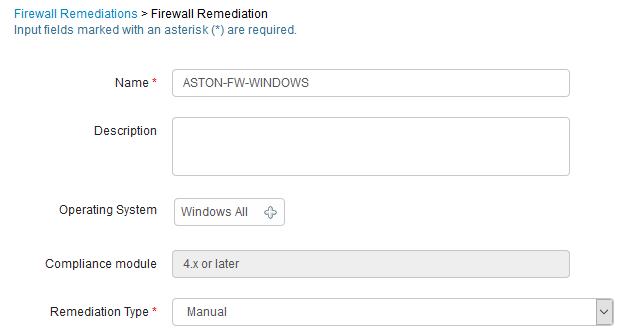
Navigate to **Policy Elements > Conditions > Patch Management**. Hit **Add** name it **ASTON-PM-UP-TO-DATE** and configure the following:



Navigate down to **Remediations > Patch Management**. Hit **Add** and name it **ASTON-PM-REM** and configure the following:



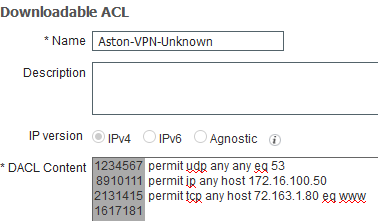
Now just so we can test our non-compliant policy later let’s change our **Firewall Remediation** back to manual for **Remediation Type**.



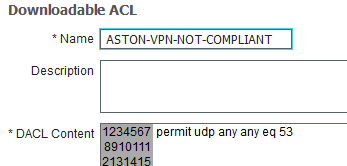
Navigate to Requirements and Insert a new requirement. Name it **ASTON PM UPDATE WIN**. Operating system will be **Window All** and the compliance module will be **4.x or later**. Conditions will be **ASTON-PM-UP-TO-DATE** and Remediation Actions **ASTON-PM-REM**. Then hit **Save**.



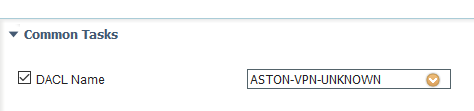
Now we need to add a few dACLs. Navigate to **Downloadable ACLs** and hit **Add**. Name it **ASTON-VPN-UNKNOWN** and configure the following:



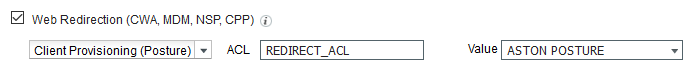
**Add** another and name it **ASTON-VPN-NOT-COMPLIANT**. Add a permit for **DNS only**.



Let’s add our Authorization Profiles. Click on the **ASTON-VPN-NETWORK-ADMIN** checkbox and **Duplicate** it. Change the name to **ASTON-VPN-UNKNOWN**. Change the dACLs to **ASTON-VPN-UNKNOWN**.



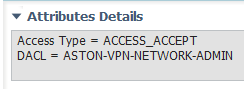
Now we need to add our **Web Redirection** like we did with our wired policy. Configure the following then **Save**:



Add another one and name it **ASTON-VPN-NOT-COMPLIANT**. Give it the **ASTON-VPN-NOT-COMPLIANT** dACL and hit Save.

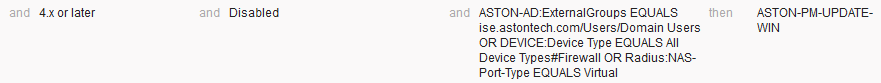


For both **ASTON-VPN-NETWORK-ADMIN** and **ASTON-VPN-EMPLOYEE** **Edit** them and uncheck the **ASA VPN** checkbox. They should only be sending an access accept and the dACL now.



Posture Policy

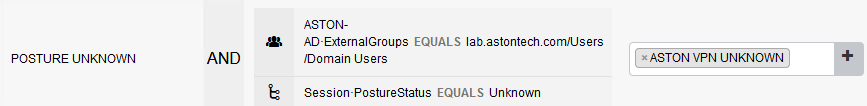
We need to add our new posture check for our VPN users. Navigate to **Posture Policy** and **Insert a new policy**. Name it **VPN WINDOWS**. The conditions will be the same as the Client Provisioning Policy we created. Then we’ll give it a **Requirement** of **ASTON-PM-UPDATE-WIN**.



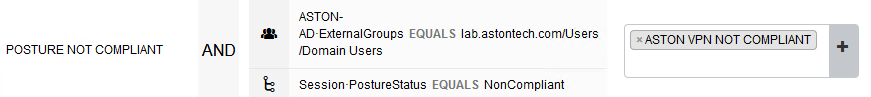


Policy Set

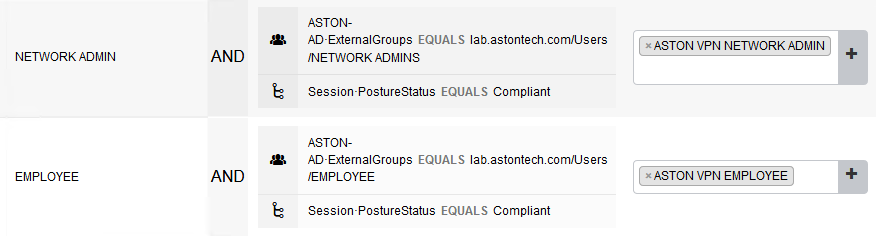
Navigate to **Policy Sets > VPN**. **Duplicate** the **NETWORK ADMIN** policy **above**. Name it **POSTURE UNKNOWN**, change the **AD Group** to **Domain Users** add **Session:PostureStatus Equals Unknown**. Change the permission to **ASTON-VPN-UNKOWN**.



**Duplicate below** the **POSTURE UNKNOWN** policy. Name it **POSTURE NOT-COMPLIANT** and change the Posture Status to Equals **NonCompliant**. Then give it **ASTON-VPN-NOT-COMPLIANT**.



Add **Session:PostureStatus EQUALS COMPLIANT** for both **NETWORK ADMIN** and **EMPLOYEE** policies then hit **Save**.



Testing

Network Admin Account

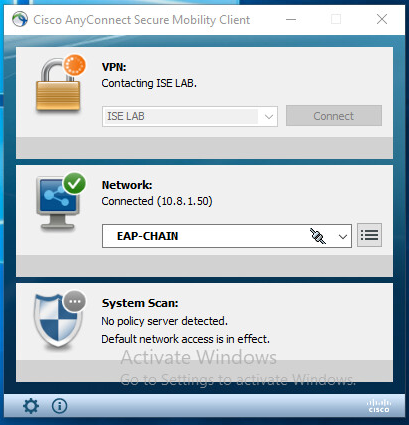
Open a console window for **PC-2** and log in. Change the Network Adaptor to **LAB OUTSIDE/INTERNET**.



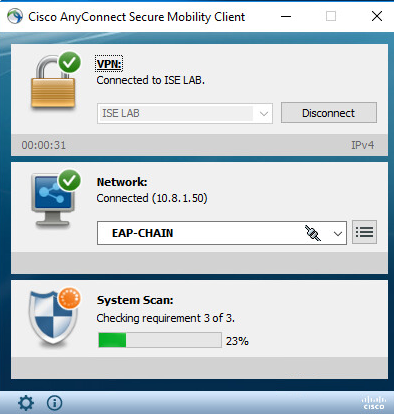
Configure your **IP** address appropriately:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Gateway | Lab 1 | Lab 2 | Lab 3 | Lab 4 |
| 10.8.1.225/27 | 10.8.1.226 – 228 | 10.8.1.229 – 232 | 10.8.1.233 – 236 | 10.8.1.237 – 240 |

Open **AnyConnect** and connect to the VPN.



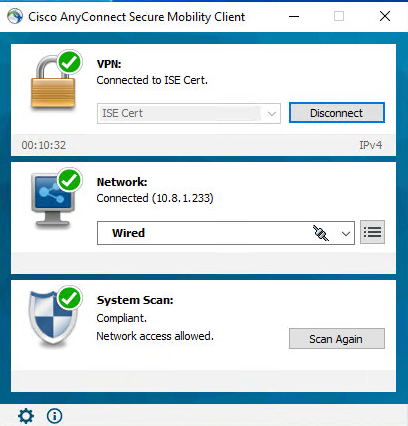
Here you can see its checking 3 requirements, two that we set up for all employees and the additional one for VPN users.

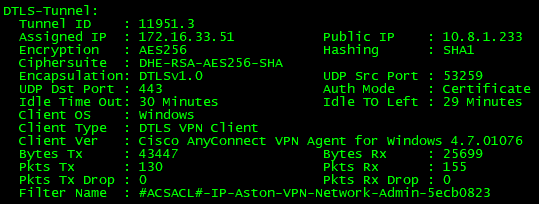


Quick look at the ASA to see the dACL, Redirect URL and ACL is being applied.

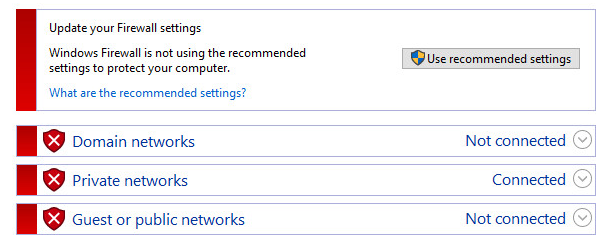


Now posture has completed, and I have full access.

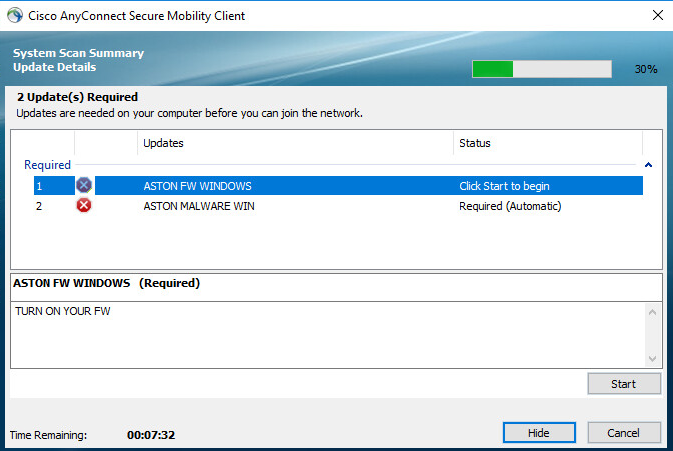




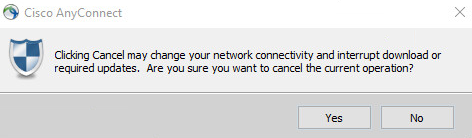
Let’s test the not-compliant policies. Turn off all the **Windows Firewalls**.



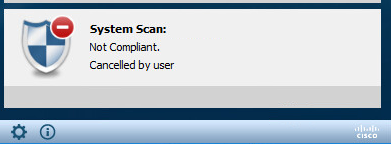
I failed. Looks like my Windows Defender definition is behind ISE as well. We could hit Start here and it would turn the Windows Firewall on and update Windows defender but we want to test the not-compliant policy. Hit **Cancel**.



Hit **Yes** to cancel.



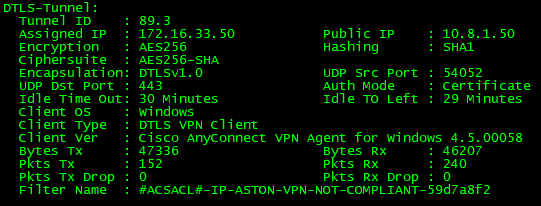
There we go, not compliant. Try pinging or accessing anything internally. You should have no access.



Live Logs show what we expect.

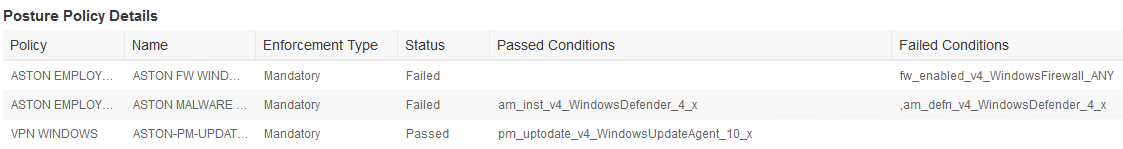


Same with the ASA.

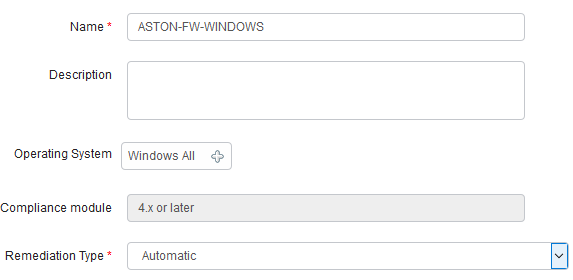


Now if we check the Posture Reports we can see the failure and the Posture Policy checks.

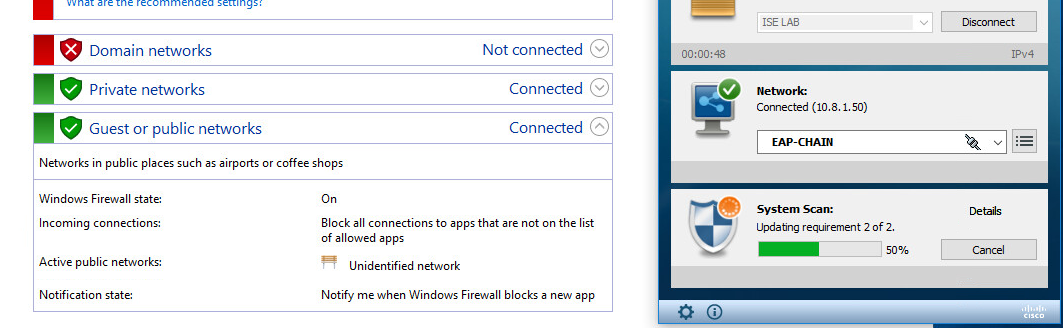




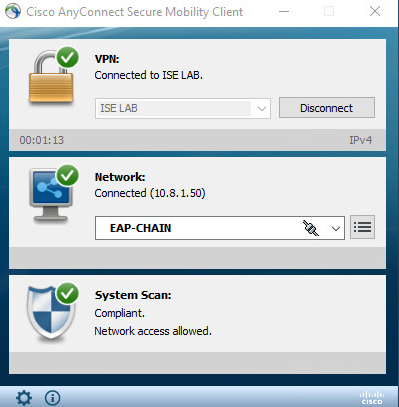
Let’s quick change the **ASTON-FW-WINDOWS** Remediation back to **Automatic** and disconnect and reconnect to the VPN and see if it will fix my two issues.



It turned my Firewall on and is downloading the Windows Defender update now.



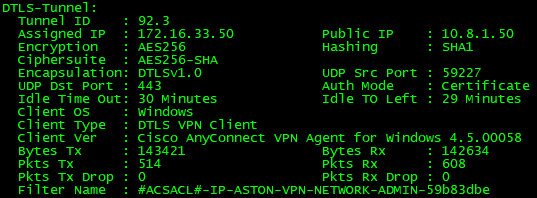
It’s done. Now I’m Compliant again.



Live Logs show the correct dACL.

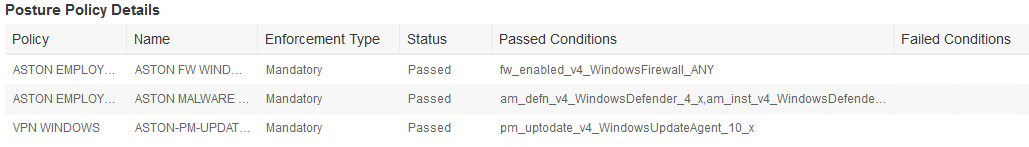


ASA looks good too.



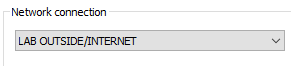
Posture Report shows everything passed this time.





Employee Account

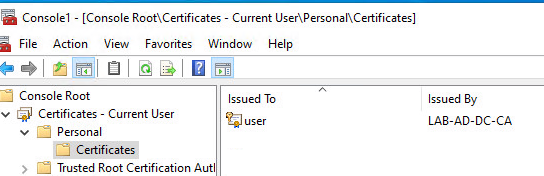
Open a console window to **PC-1** and log in with your **user** account. Let’s test the ISE Posture module provisioning. Change the network adaptor to **LAB OUTSIDE/INTERNET**.



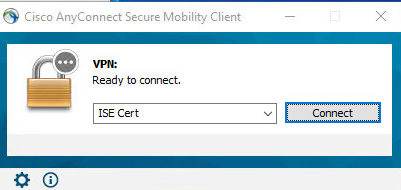
Apply IP addressing appropriately:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Gateway | Lab 1 | Lab 2 | Lab 3 | Lab 4 |
| 10.8.1.225/27 | 10.8.1.226 – 228 | 10.8.1.229 – 232 | 10.8.1.233 – 236 | 10.8.1.237 – 240 |

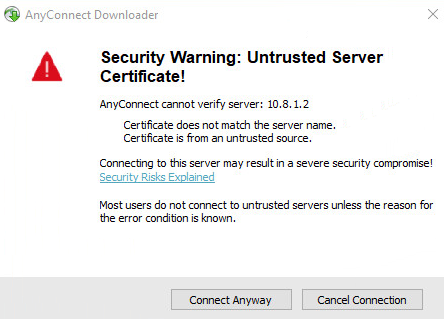
We also want to test the other VPN policy we have for **EMPLOYEE**. Open a **MMC** window and double check to make sure you have a certificate.



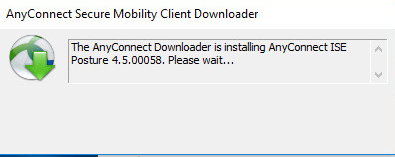
Open **AnyConnect** and select **ISE Cert** and hit **Connect**.



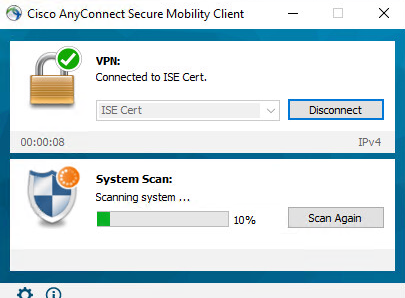
Hit **Connect Anyway**.



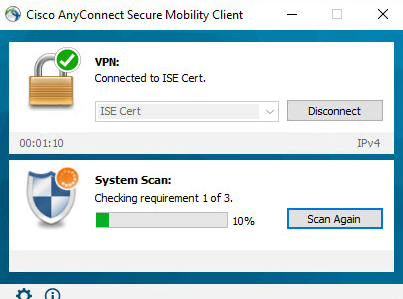
Profile, Posture and compliance module is installing.



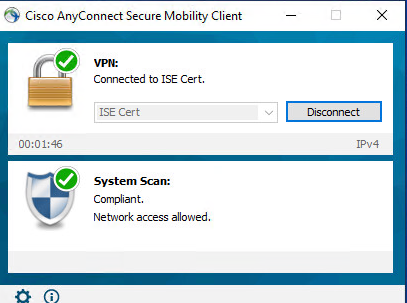
Automatically scanning the system.



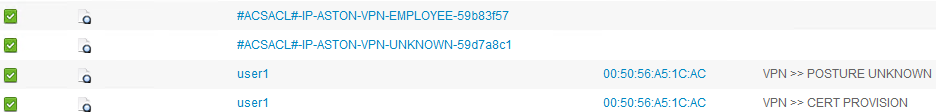
Checking our 3 requirements.



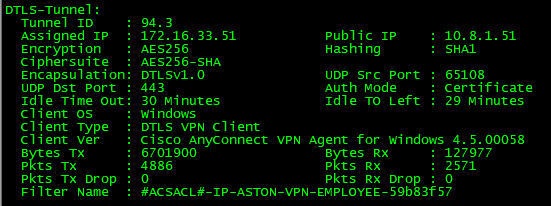
All good.



Live logs show we got the EMPLOYEE ACL. You should have access to everything internally except pings should fail.

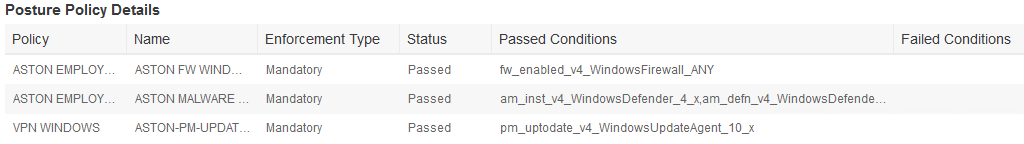


ASA shows the same.



Posture Report shows everything passed.





Conclusion

In this lab, we have:

* Configured a Redirect ACL and added to our Split-Tunneling policy on the ASA
* Configured our Client Provisioning Policy on ISE
* Added a new Posture check for VPN users
* Configured our Policy Elements
  + Added two dACLs
  + Configured our Authorization Profiles
* Configured a Posture Policy for VPN users
* Configured our VPN Policy Set
* Tested our posture policies for compliant and non-compliant and client provisioning