|  |
| --- |
| Aston Technologies Inc. |
| Cisco Identity Services Engine (ISE) Remote Access VPN |
| An Aston training document explaining how to deploy Remote Access VPN |

Contents

[Contents 2](#_Toc496877437)

[Lab Diagram 3](#_Toc496877438)

[ASA Configuration 4](#_Toc496877439)

[VPN Address Pool 4](#_Toc496877440)

[NAT Configuration 5](#_Toc496877441)

[Add AAA Server 6](#_Toc496877442)

[Tunnel Group Configuration (AKA Connection Profiles) 7](#_Toc496877443)

[Split Tunneling Policy 10](#_Toc496877444)

[Group Policy 10](#_Toc496877445)

[AnyConnect Client Profile 11](#_Toc496877446)

[ISE Configuration 13](#_Toc496877447)

[Downloadable ACLs 13](#_Toc496877448)

[Authorization Profiles 14](#_Toc496877449)

[Policy Set 15](#_Toc496877450)

[Testing VPN Access 16](#_Toc496877451)

[Conclusion 23](#_Toc496877452)

Lab Diagram

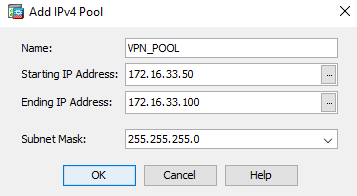


ASA Configuration

VPN Address Pool

For our users to have access to our internal network we need to give them an IP address that is routable internally. There are a number of ways to do this 1) configure the ASA to use our internal DHCP server 2) configure an address pool on the ASA for Remote Access users. There are more less prevalent ways to accomplish this but these two are the most common. We are going to use number 2 which is probably the most commonly deployed method.

Navigate to **Configuration > Remote Access VPN > Network (Client) Access > Address Assignment > Address Pools**. Click **Add** and name it **VPN\_POOL** and give it the following IP addressing:

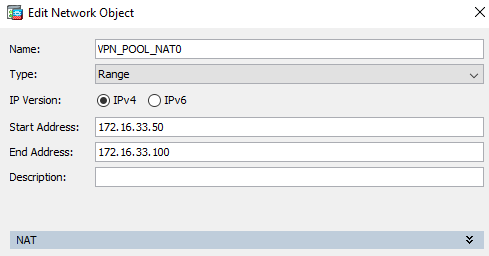


Then hit **Apply**.

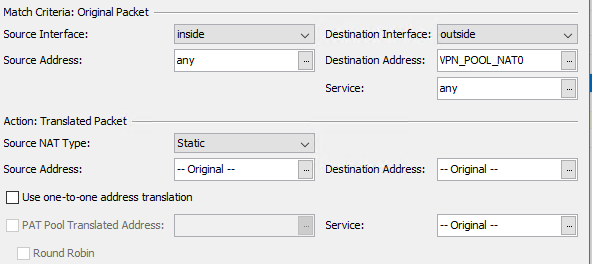
NAT Configuration

We need to create a NAT rule so our VPN users return traffic doesn’t get NAT’d.

Go to **Configuration > Firewall > NAT Rule**s and hit **Add**. In the Original Packet section click on **Destination Addres**s box. Click **Add** to create a network object. Name it **VPN\_POOL\_NAT0** and configure the following:



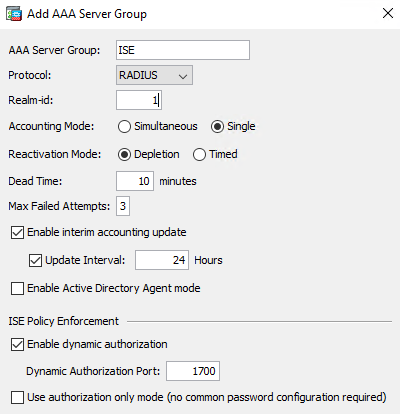
Configure the NAT rule as follows:



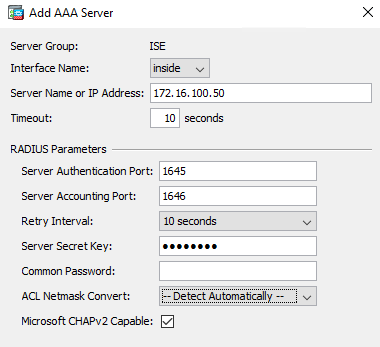
Hit **OK** and **Apply**.

Add AAA Server

Next, let’s add a server group for ISE like we did for TACACS except we are going to use RADIUS this time. Navigate to **Configuration > Device Management > Users/AAA > AAA Server Groups**. Click **Add**, give it a name of **ISE** and configure the following:



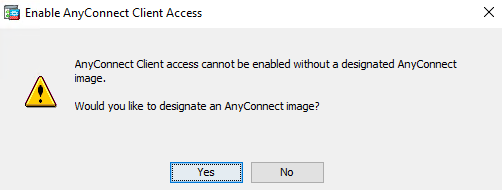
Now let’s add a server to the group. Click the **Add** button on the bottom section and configure the following (Secret Key – cisco123):



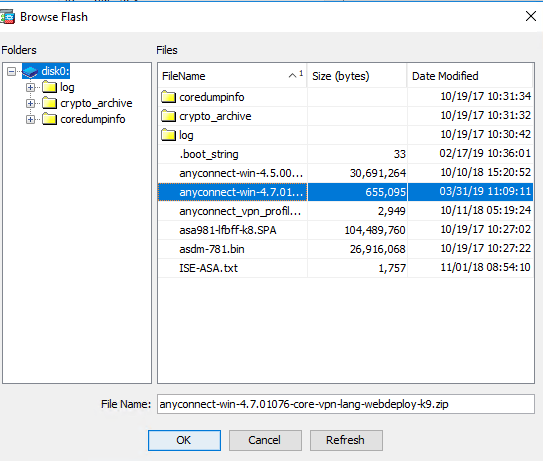
Hit **Apply** and test **Authentication**.

Tunnel Group Configuration (AKA Connection Profiles)

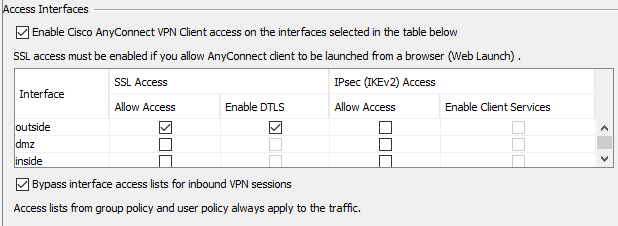
Navigate to **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles** and click the checkbox to **Enable Cisco AnyConnect VPN Client Access**. Hit **Yes** on the popup to designate an AnyConnect image.



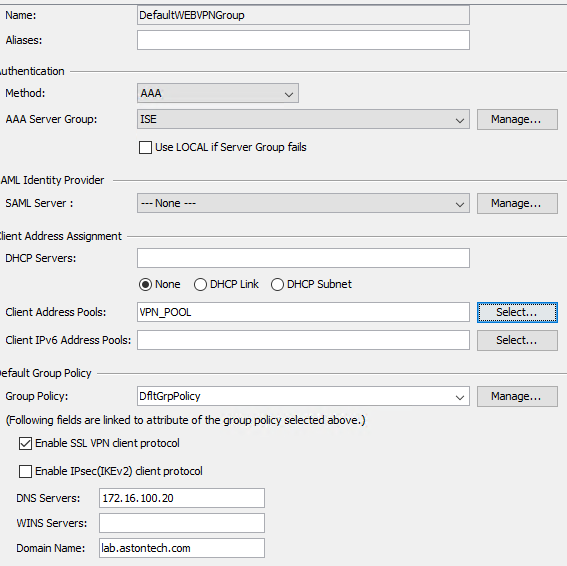
Hit Browse Flash and select the anyconnect-win-4-x.xxxxx-webdeploy-k9-pkg image and hit **OK**.



Allow access on the **outside** interface as shown below:



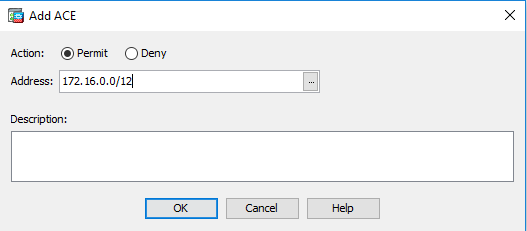
We are going to use ISE to control what Group Policy our users get based on their Active Directory group membership. By default, if you don’t allow users to select a connection profile (tunnel group) upon login they will be directed to the DefaultWEBVPNGroup. Let’s edit that profile to fit our needs. Click on the **DefaultWEBVPNGroup** and select **Edit**. Configure the following on the Basic tab and hit **OK** then **Apply**:



Split Tunneling Policy

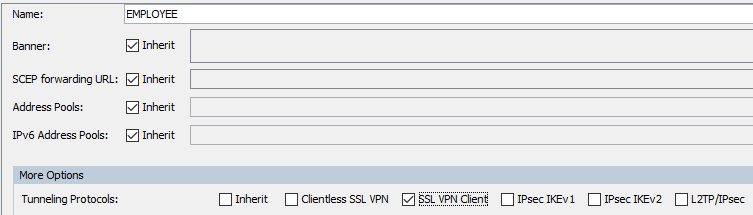
Split Tunneling allows you to specify what you want or don’t want to be sent through the tunnel. In our case, we only want to send traffic to our internal network through the tunnel and allow the user to browse the internet etc. locally.

We are going to create a Standard ACL to tell the ASA or the AnyConnect client what IP addresses to send through the tunnel. Navigate to **Configuration > Firewall > Advanced > Standard ACL**. Click **Add ACL** and name it **SPLIT-TUNNEL-ACL**. Then **Add ACE** and give it the address of **172.16.0.0/12**. Hit **Ok** then **Apply**.

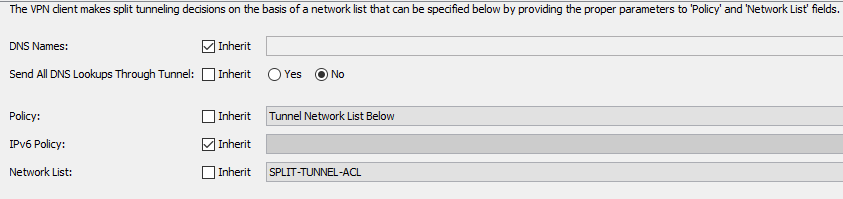


Group Policy

We are going to create one group policy and use ISE to allow for differentiated access to the network. Navigate to **Configuration > Remote Access VPN > Network (Client) Access > Group Policies** and click **Add**. Name it **EMPLOYE**E then click **More Options**, uncheck **Inherit** on the Tunneling Protocols and check **SSL VPN Client**. Everything else on this page can stay default.



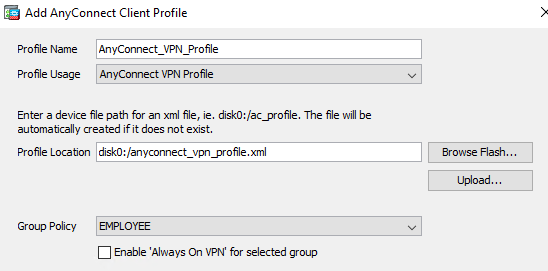
Expand the Advanced tab and select **Split Tunneling**. For **Policy,** we want to **Tunnel Network List Below** and for the **Network List** we want to use the **SPLIT-TUNNEL-ACL** we created earlier.



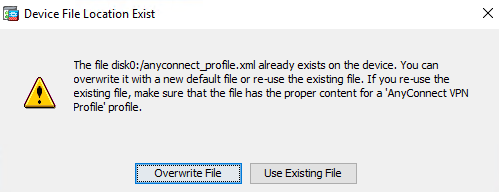
Hit **OK** and **Apply**.

AnyConnect Client Profile

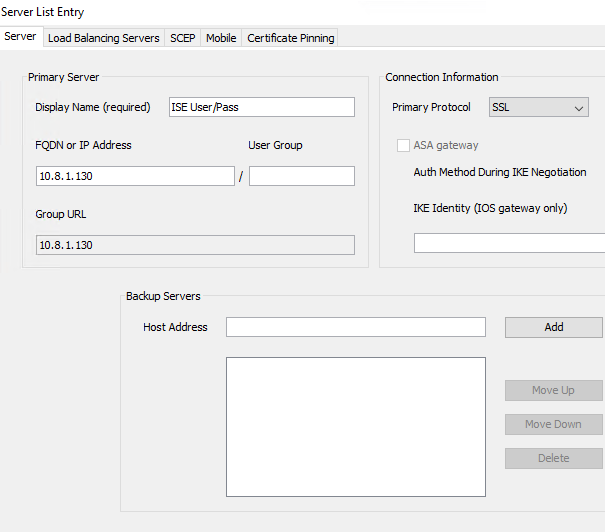
Last thing we’ll do on the ASA is create an AnyConnect Client Profile. Navigate to **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Profile** and click **Add**. Name it **AnyConnect\_VPN\_PROFILE** and apply our **EMPLOYEE** group policy. Then hit **OK**.



If you get a message saying it already exists hit **Overwrite File**.



Click on our newly created policy and hit **Edit**. Go to the **Server List** tab and hit **Add**. Configure your ASA outside IP address:



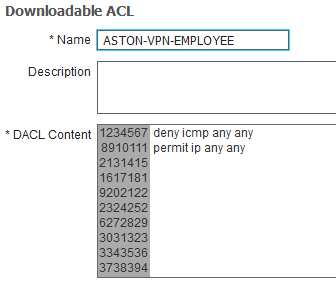
Then hit **OK** and **Apply**.

ISE Configuration

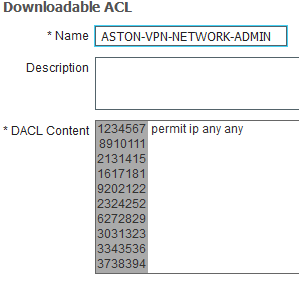
Downloadable ACLs

We already have added the ASA into ISE as a network device, so we are ready to start creating policy. Log into ISE and navigate to **Work Centers > Network Access > Policy Elements > Results > Downloadable ACLs**.

We are going to add ACLs for our Employees and for Network Admins. Click **Add** and name it **ASTON-VPN-EMPLOYEE**. For this one we are going to deny ICMP and permit everything else.



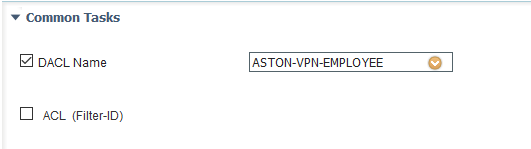
Add another one and name it **ASTON-VPN-NETWORK-ADMIN**. We are going to just do a permit any on this one.



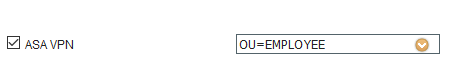
Authorization Profiles

Now we need to create our authorization profiles for our two groups. We need to do two things here one is apply the dACL and the other is to send the class attribute equal to the group policy we want to apply to the user.

Go to Authorization Profiles and click Add. Name it **ASTON-VPN-EMPLOYEE**. In the Common Tasks check DACL Name and give it ASTON-VPN-EMPLOYEE.



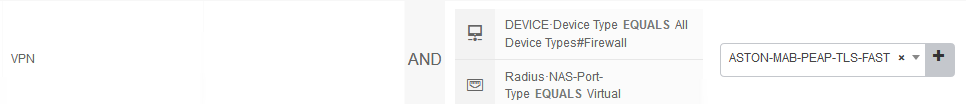
Then Scroll down in the Common Tasks down to **ASA VPN**. We want to add our Group Policy exactly like it is configured on the ASA. Click the checkbox and input **OU=EMPLOYEE**. Then hit **Save**.



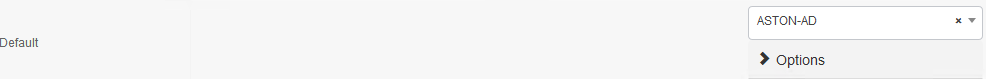
Add another name it **ASTON-VPN-NETWORK-ADMIN**. This is going to be the same except the ACL is going to be **ASTON-VPN-NETWORK-ADMIN**.

Policy Set

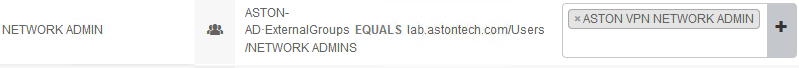
We are going to add a new Policy Set for VPN. Click Add and create a new Policy Set. Name it VPN and for the conditions we are going to match **on DEVICE:Device Type EQUALS Device Type#All Device Types#Firewall** AND **Radius:NAS-Port-Type EQUALS Virtual**.



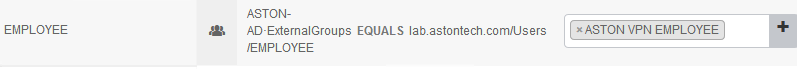
For the Authentication Policy, we are going to just edit the default. Change the Identity Source to **ASTON-AD**.



Now we need to create our Authorization Policies. Create a new rule and name it **NETWORK ADMIN**. We want to match **on ASTON-AD:ExternalGroups EQUALS Network Admins** then give it **ASTON-VPN-NETWORK-ADMIN** for permissions.

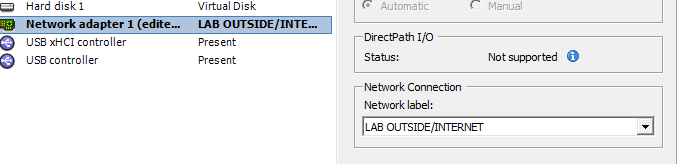


Duplicate below and name it **EMPLOYEE**. Change the AD group to **Employee** and the permissions to **ASTON-VPN-EMPLOYEE**. Then **Save**.



Testing VPN Access

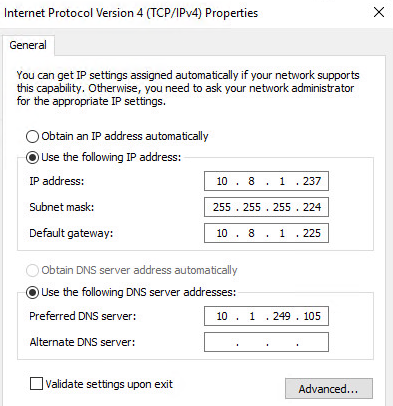
Log into vCenter, open a console window to LAB-PC-2 and log in. Change the Network Adaptor to **LAB OUTSIDE/INTERNET**.



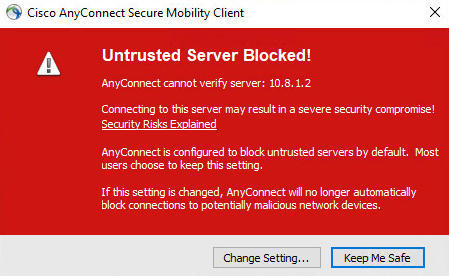
We don’t currently have a DHCP server for this subnet. Statically Assign an IP appropriately as shown below -

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 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 |

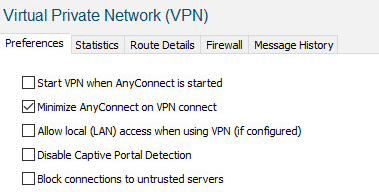
Lab 4 example -



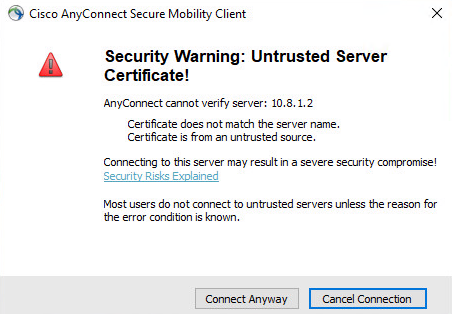
Open the AnyConnect client and connect to your VPN gateway. Hit **Change Setting** on the popup.



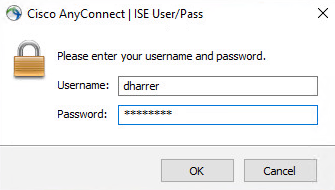
Uncheck the **Block connections to untrusted servers**.



Try your connection again. Click **Connect Anyway** on the popup.

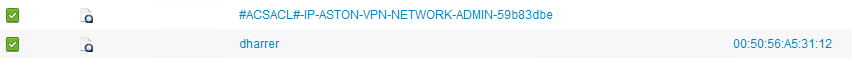


Input your creds and hit **OK**.



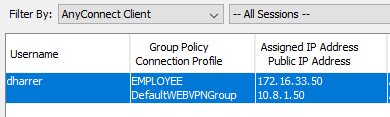
Now you should be connected and have full access to the ISE lab. Try pinging some devices and going to ISE in a web browser.

If we check the Live Logs in ISE we passed, and the ACL was downloaded.

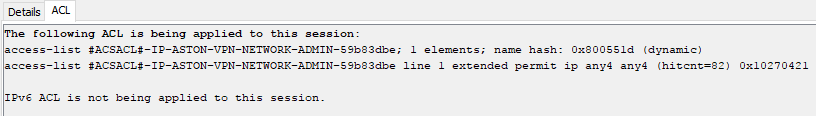


Dive into the details and take a closer look.

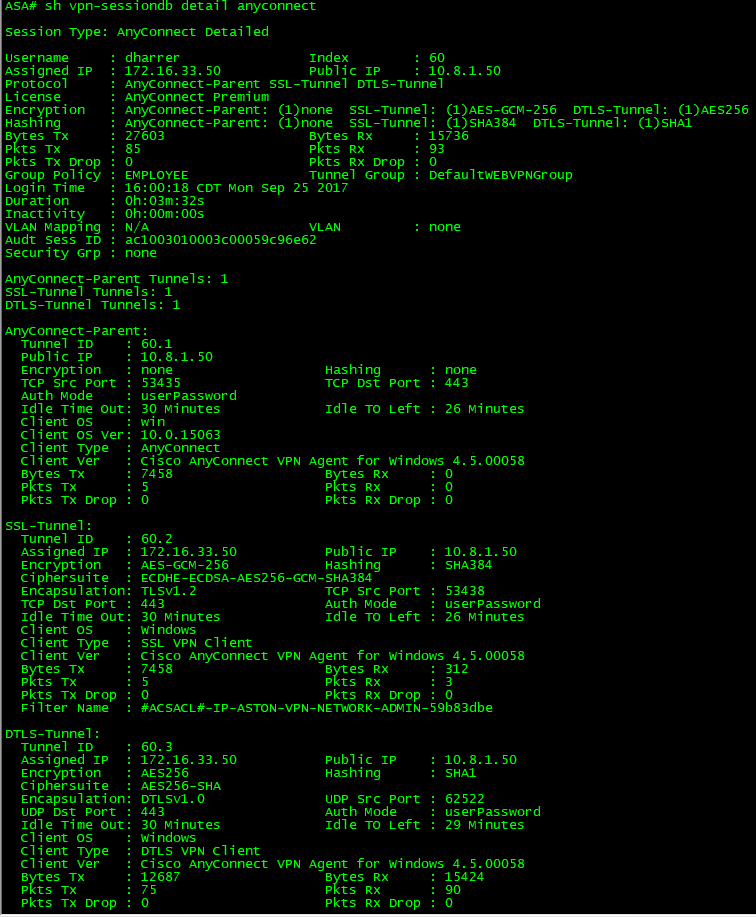
If we look from the ASA side in ASDM by going to **Monitoring > VPN > VPN Statistics > Sessions** then filtering on AnyConnect Client you can see we are getting the EMPLOYEE Group Policy.



Click the Details button you’ll get more information on the tunnel. If you hit the ACL tab you can see the ACL and ACEs that are applied to the session.



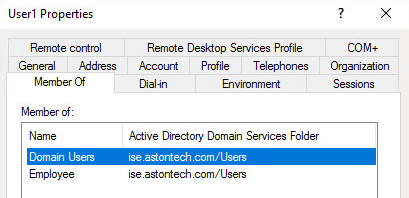
You can see the same information in the ASA CLI. Log into the ASA CLI and run the command **show vpn-sessiondb detail anyconnect**.



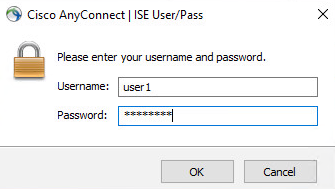
Same as with a switch you can see what’s in the access-list by doing a **show access-list <name>.**



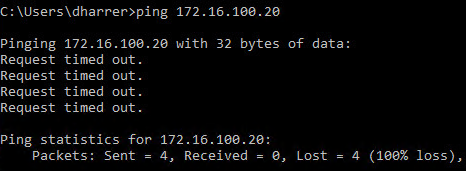
Now let’s test the regular employee account. Log into **LAB-AD-DC** and add **User1** to the **Employee** group.

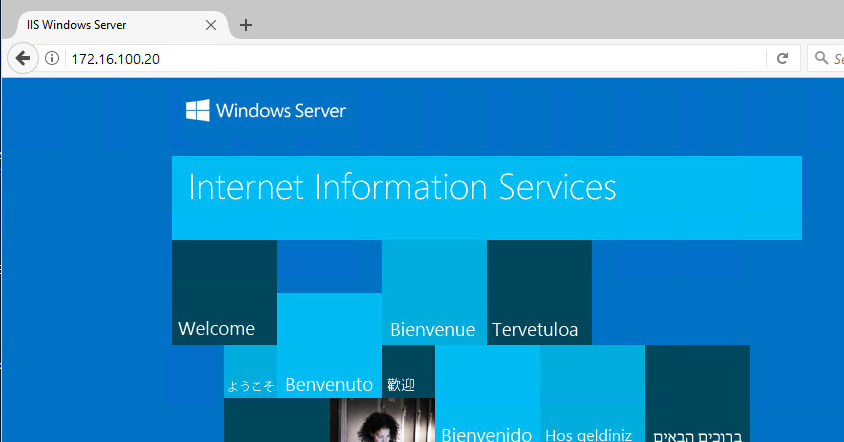


Back to ISE-PC-2 and Disconnect the current VPN session. Reconnect and use the User1 account.



Try pinging our AD server or ISE. This should fail but you should be able to access the AD server or ISE via a web browser.





Check the Live Logs in ISE and the ASA and make sure everything is as expected.

Conclusion

In this lab, we have:

* Configured the ASA to support RA VPN with the AnyConnect client
* Added ISE to use as the backend AAA server for RA VPN
* Configured dACLs for each group in our use case in ISE
* Created Authorization Profiles for our RA VPN groups
* Configured a new Policy Set for VPN access in ISE
* Tested both types of accounts access to the internal network

In the next lab, we are going to go a step further and use certificates to authenticate to the VPN. We’ll use the ISE CA for our non-domain machines and our internal CA for our domain machines.