Example of the Radius Profile configured to pass the group information:



Example of Spiderman assigned to the “Recruiting VPN Client Access” group:



Example of the Authentication Agent for Radius:



Example of the Link Identity Source to System – Still have Internal Database running as well as ActiveDirectory-Email:



Example of the Operations Console Identity Source – connections tab:



Example of the ActiveDirectory-Email Map tab:



**Palo Alto Configurations**

The GlobalProtect Gateway must have the authentication profile configured to use a Radius ‘Authentication Profile’. You can name the authentication profile whatever you’d like – in our case it’s called Radius\_VPN. Also, the GlobalProtect Gateway should have all of the IP addresses that will be used for client based VPN. The permissions will be defined by the group they’re associated with – not by IP address – hence the IP address for the client is irrelevant. In our case we have an entire class C assigned for those connecting via VPN Client.

***\*\*\* The following examples are provided, but the locations in Active Directory, Server name, and IP Addresses need to be modified if the intent is to create a document for RSA or Palo Alto – For Security Reasons.***

Authentication Profile:

Defines the allow list of what groups can authenticate. This must match exactly what is referenced in RSA / Radius configurations. RSA / Radius passes the group information over to Palo Alto after successful authentication. That information is compared to this list and the user is allowed in. This list MUST match the group that the user is added to in Active Directory.



The key is to get the attribute from the group in Active Directory, add it in here and then add it into the Group you create in RSA. Do it all with Copy/Paste and you’ll know they match up.

You also MUST have LDAP configured in Palo Alto so the user groups can be retrieved. Make sure your Bind DN to LDAP is done by email address. See the example on the next page.

LDAP Server Profile – changed information I could type over, but the Server names / addresses should be changed if you want to use this screen shot.

LDAP is how the groups associated with the users get imported. I will show you a backend example of how Palo Alto interprets the username for radius that’s entered (email address).



Radius Server Profile (how Palo Alto and Radius communicate):



Example of what the verbose log file looks like for Spiderman authenticating through RSA, which utilizes Radius to pass the group information, which then takes the group and compares it to the users and the user’s assigned groups from LDAP to compare against the allowed lists in the GlobalProtect Gateway to allow the users access with the assigned permissions. So it all makes sense, here’s an example of a policy from Palo Alto defining what user group can access what when authenticating to the VPN Client – there will be screen shots of 7 tabs to complete the entire policy:













