Refer to **sk172909**

Configure the firewall as per:

https://dl3.checkpoint.com/paid/d9/d99fd83a9b0028e2e6ecb42ac23c840b/CP_R80.40_and_R81_Jumbo_Hotfix_SAML_For_VPN_RA.pdf?HashKey=1648637502_1bbd79fea971181d656bc2dcbc6760af&xtn=.pdf

Pg 19 – Step 6 (optional) – turns out to be critical, rather than optional! You must complete this step. Here are some additional notes to put more flesh on the bones….

(Step 6, A)

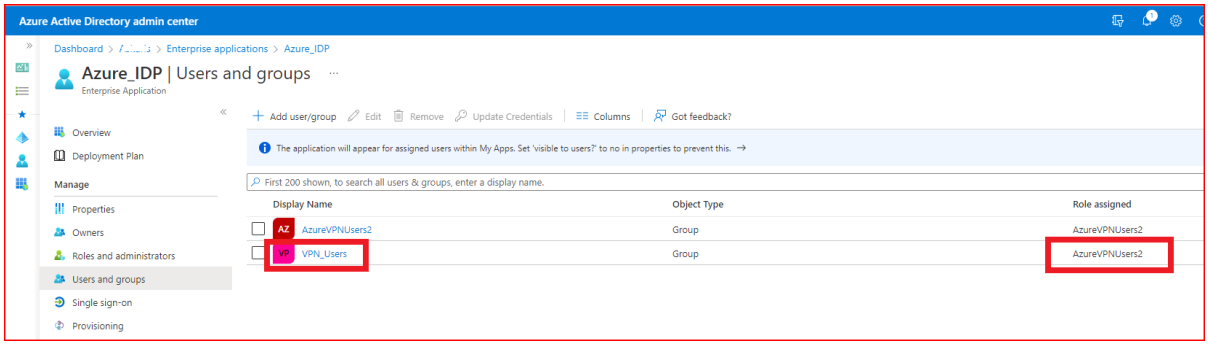
Create user groups. Add members.

https://portal.azure.com/#blade/Microsoft_AAD_IAM/GroupsManagementMenuBlade/AllGroups

Enterprise Applications:

https://portal.azure.com/#blade/Microsoft_AAD_IAM/StartboardApplicationsMenuBlade/AppAppsPreview/menuId/

When you add user groups to the Enterprise App they may have the wrong role assigned. For example…

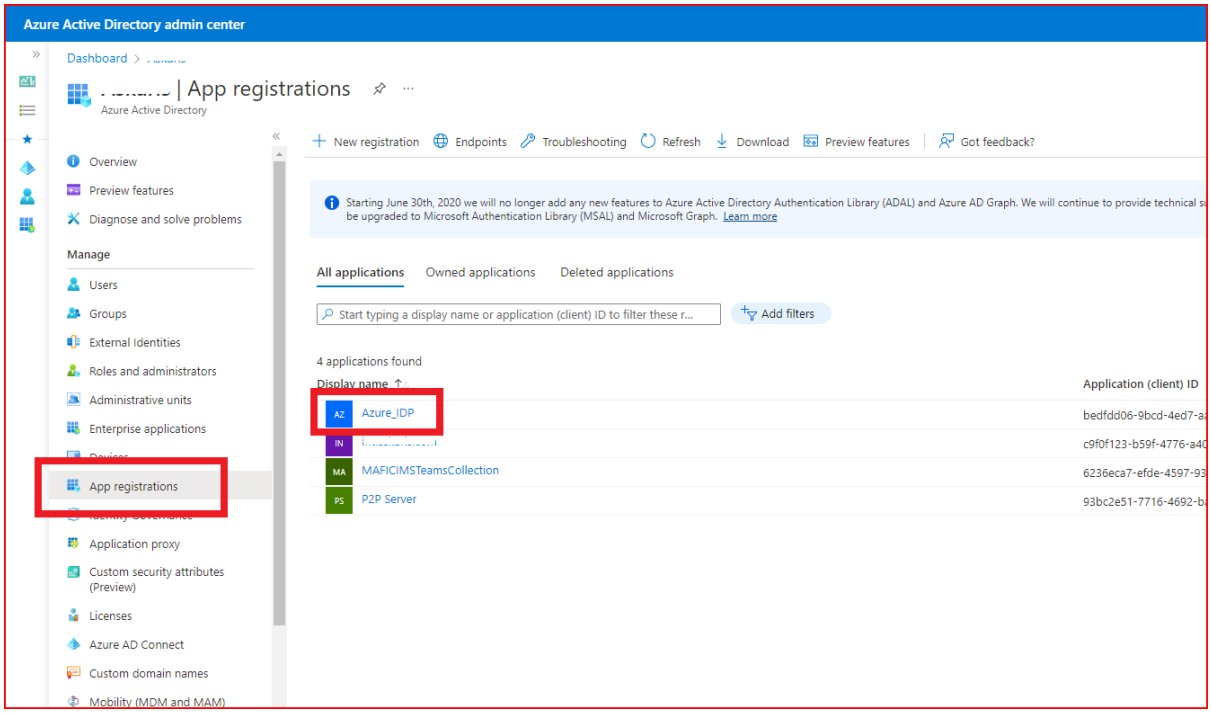


This means the "VPN_Users" group will **not** be included in the App Manifest, and will **not** apply to the Access Role in the rulebase. This needs to be updated.

Check Point Access Roles need to reference the Azure Group names – BUT - If you continue in the state shown above, then any users in the **VPN_Users** group will actually match the **AzureVPNUsers2**

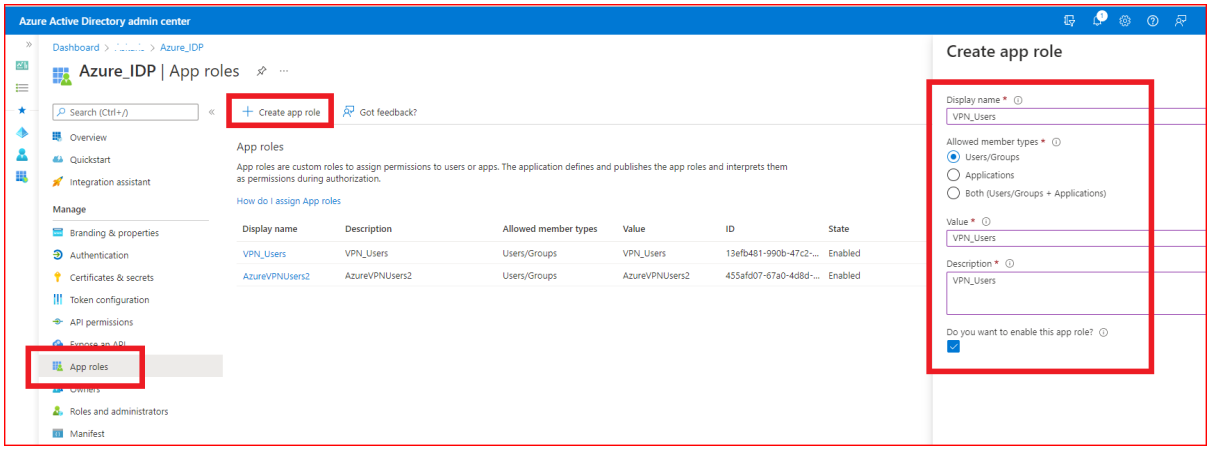
group rules on the Check Point firewall. Therefore, it is crucial to follow these steps to change the group role within the Enterprise App (not fully documented in Step 6 of the instructions).

Go to Home > App Registrations > find your app….



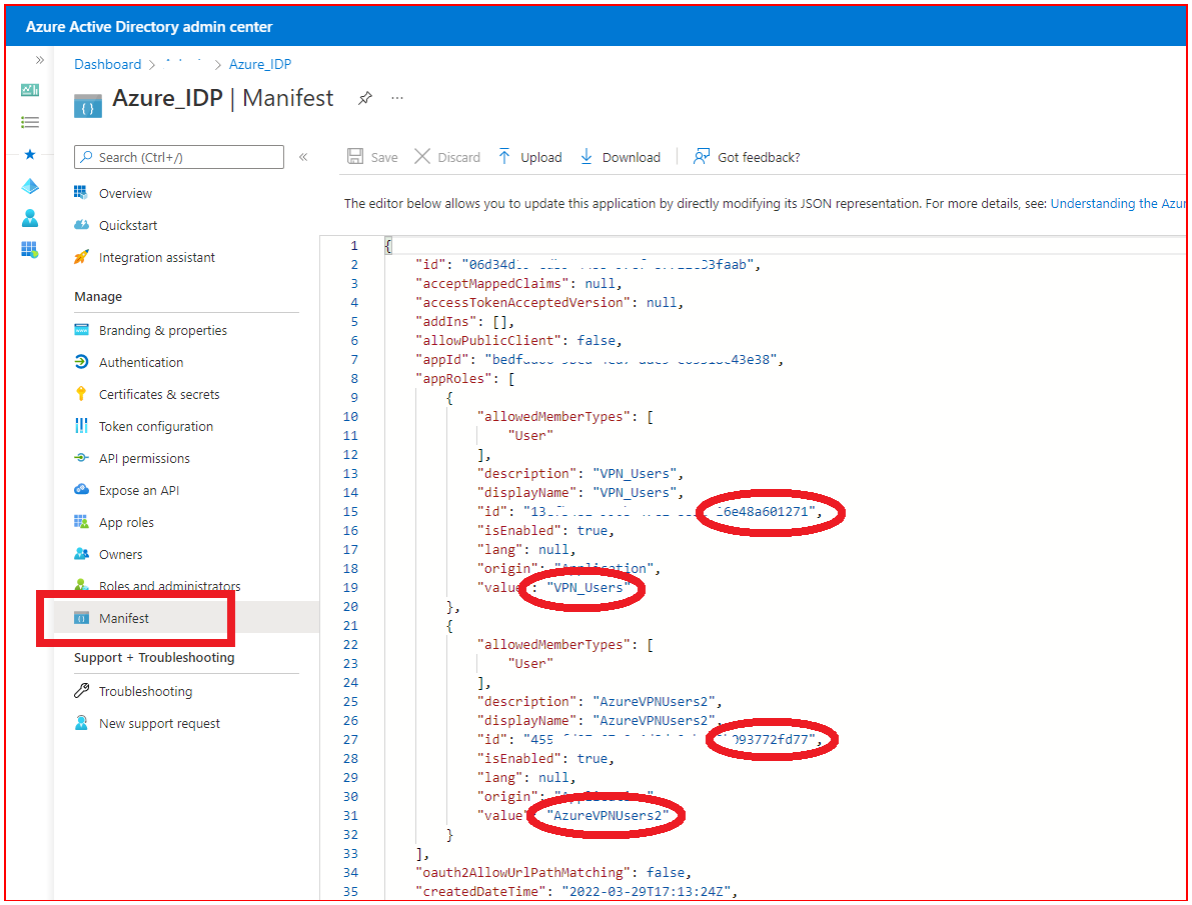
Then, App Roles > Create App Role. Create a new role for the new User Group. Make sure the “enabled” box is ticked.

Repeat this to create a new role for each User Group you need to use for VPN access.



Next, open the **Manifest** page.

Check that the manifest contains each of the roles you have created, as demonstrated below. The description, Display Name and Value should contain the role name. Check that the ID exactly matches the Object ID for the role. There should be a section for each user group. E.g:



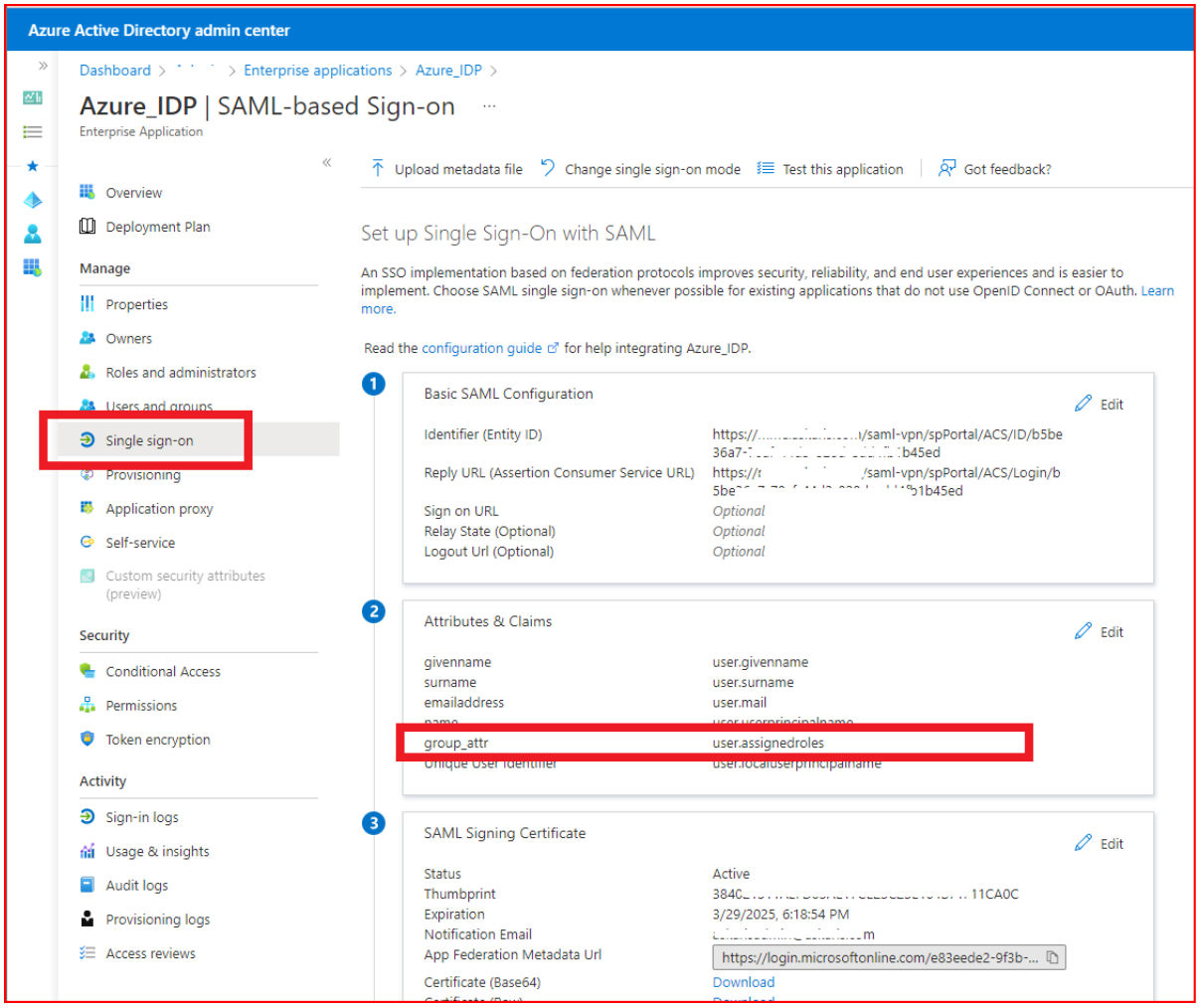
(Step 6, B)

Next, go back to Azure Home > Enterprise Apps. Find your App.

https://portal.azure.com/#blade/Microsoft_AAD_IAM/StartboardApplicationsMenuBlade/AppAppsPreview

Single Sign-On.

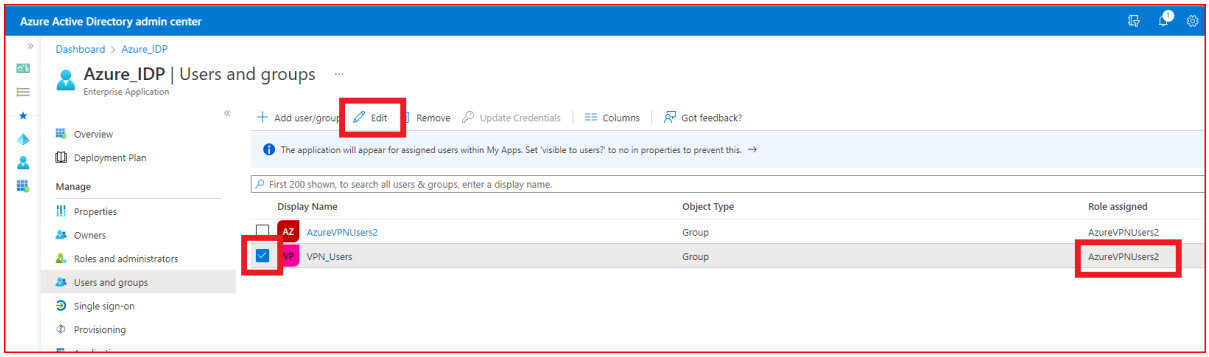
Add the **group_attr**

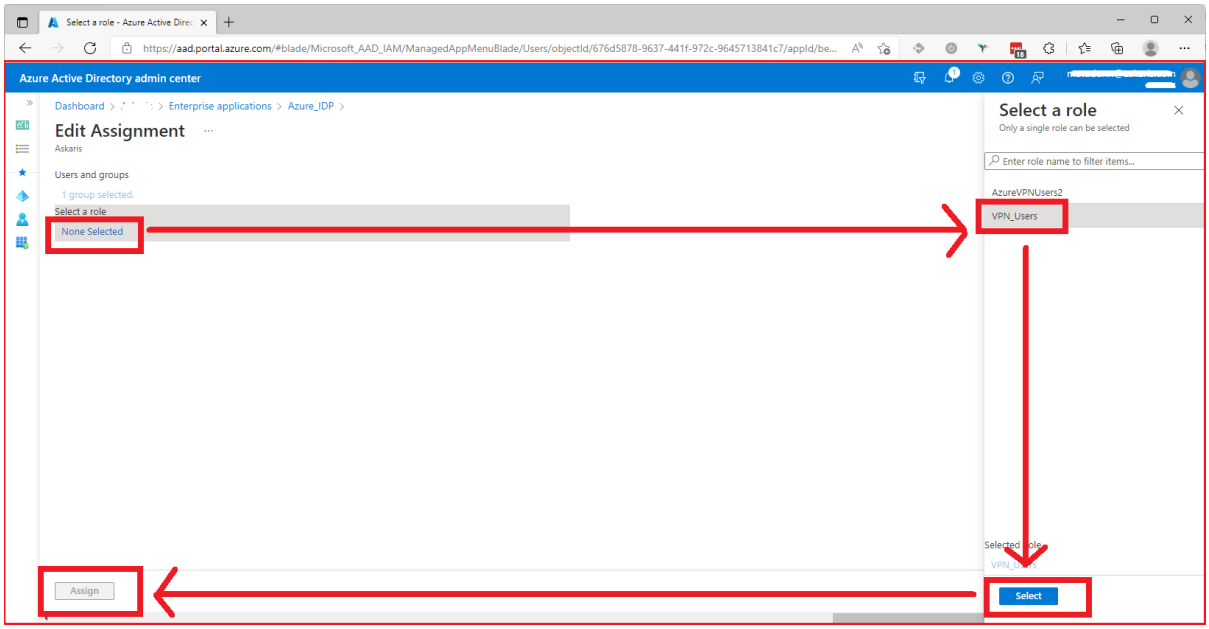


Undocumented step – **CRUCIAL**

Go back to the Enterprise App > Users & Groups. We need to change the user group **Role Assigned** to ensure that each group has its own Role assigned (rather than all having the same role assigned, as shown previously).

Tick the box next to the role you need to change. Edit. Select the relevant role and click **Assign**.





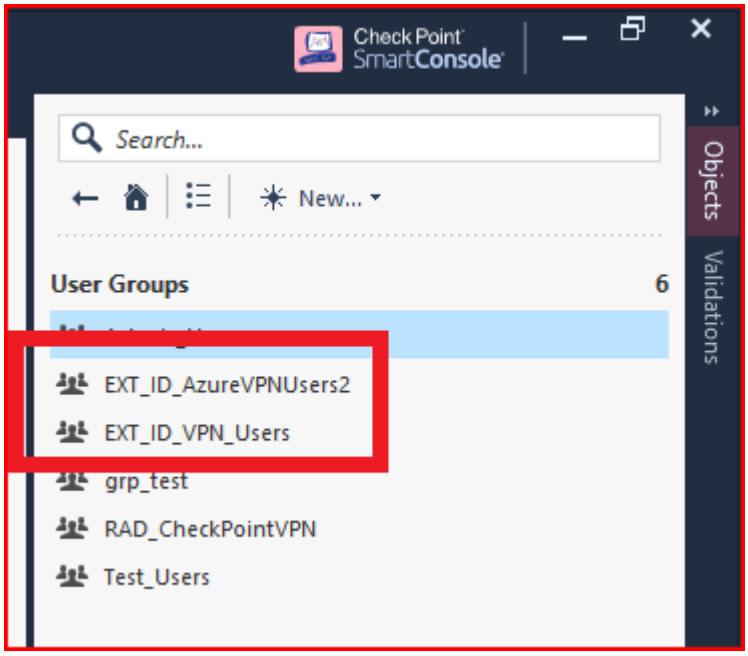
(Step 6, C)

Next, open SmartConsole.

Create legacy User Groups for each of the Azure groups you wish to reference. These group names must start with **EXT_ID_** then exactly match the Azure group case – including the exact upper/lower case. In this example we need two groups named:

EXT_ID_AzureVPNUsers2

EXT_ID_VPN_Users

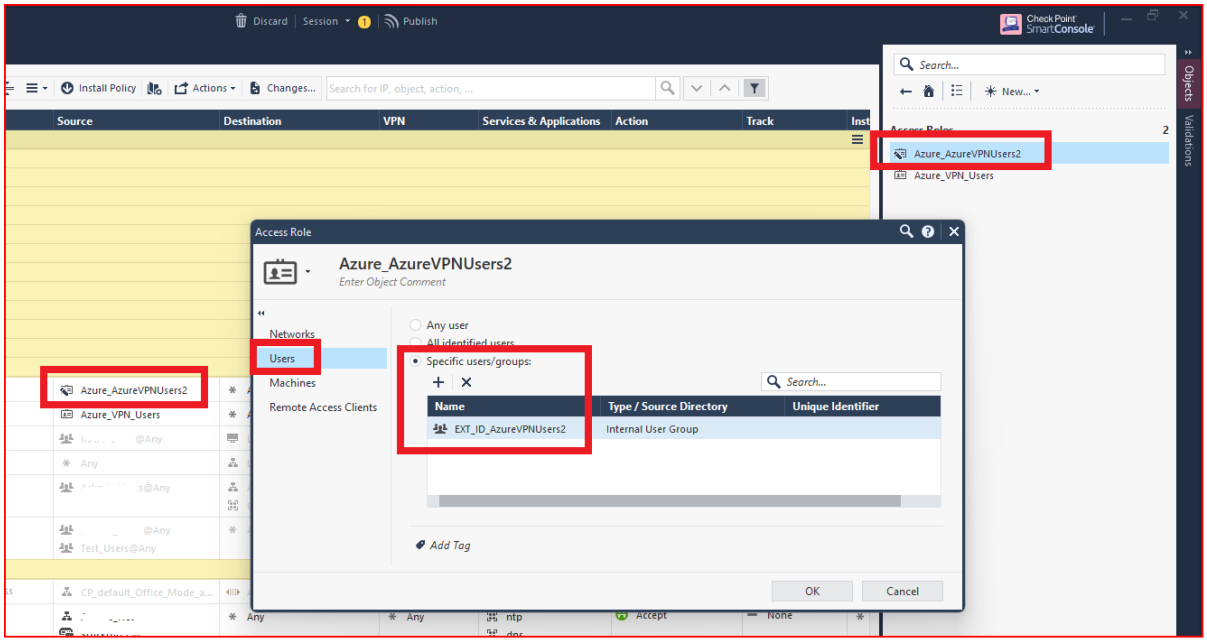


These groups should be empty. Check Point simply uses the group names as a way to reference what is in Azure.

Finally, create new Access Roles for each VPN user group. Give the Access Role a unique name.

Within the Users section, select the relevant legacy User Group created in the previous step.

Use the Access Role in your security rules as normal.



Log into VPN using your Azure credentials.

Thoroughly test that users are being applied to the correct Group/Access Role when they log in. This should be done be confirming the traffic rule # in the logs, and also using #pdp monitor, e.g:

```
#pdp monitor user matt.dunn
```