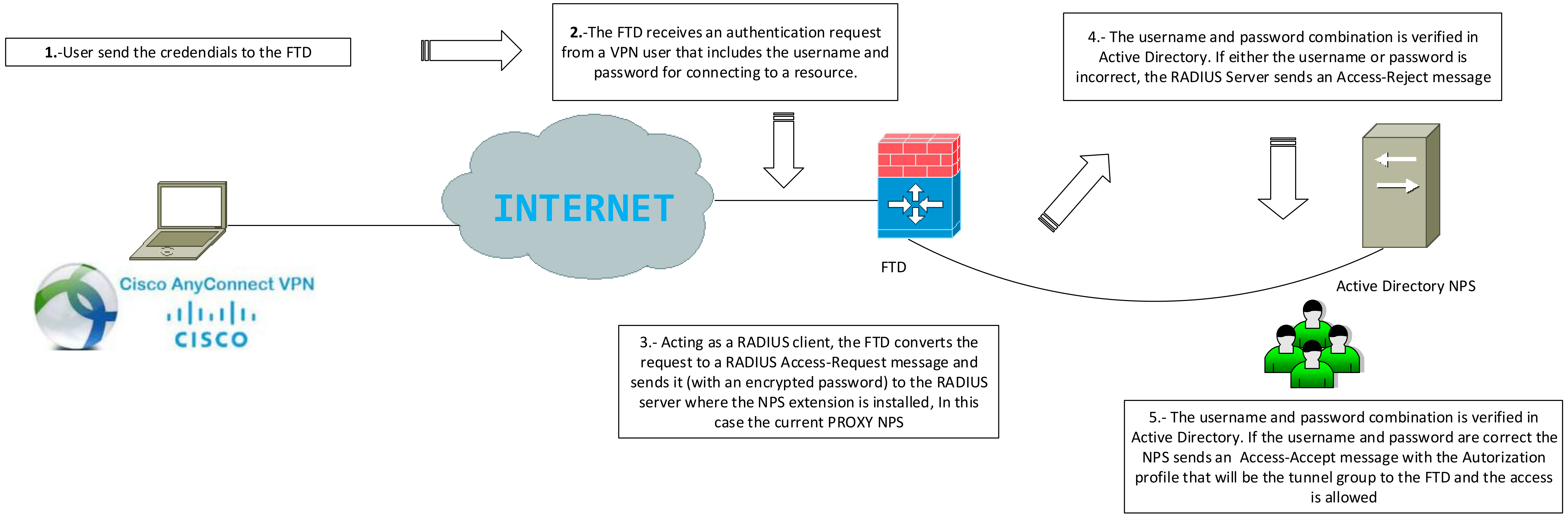


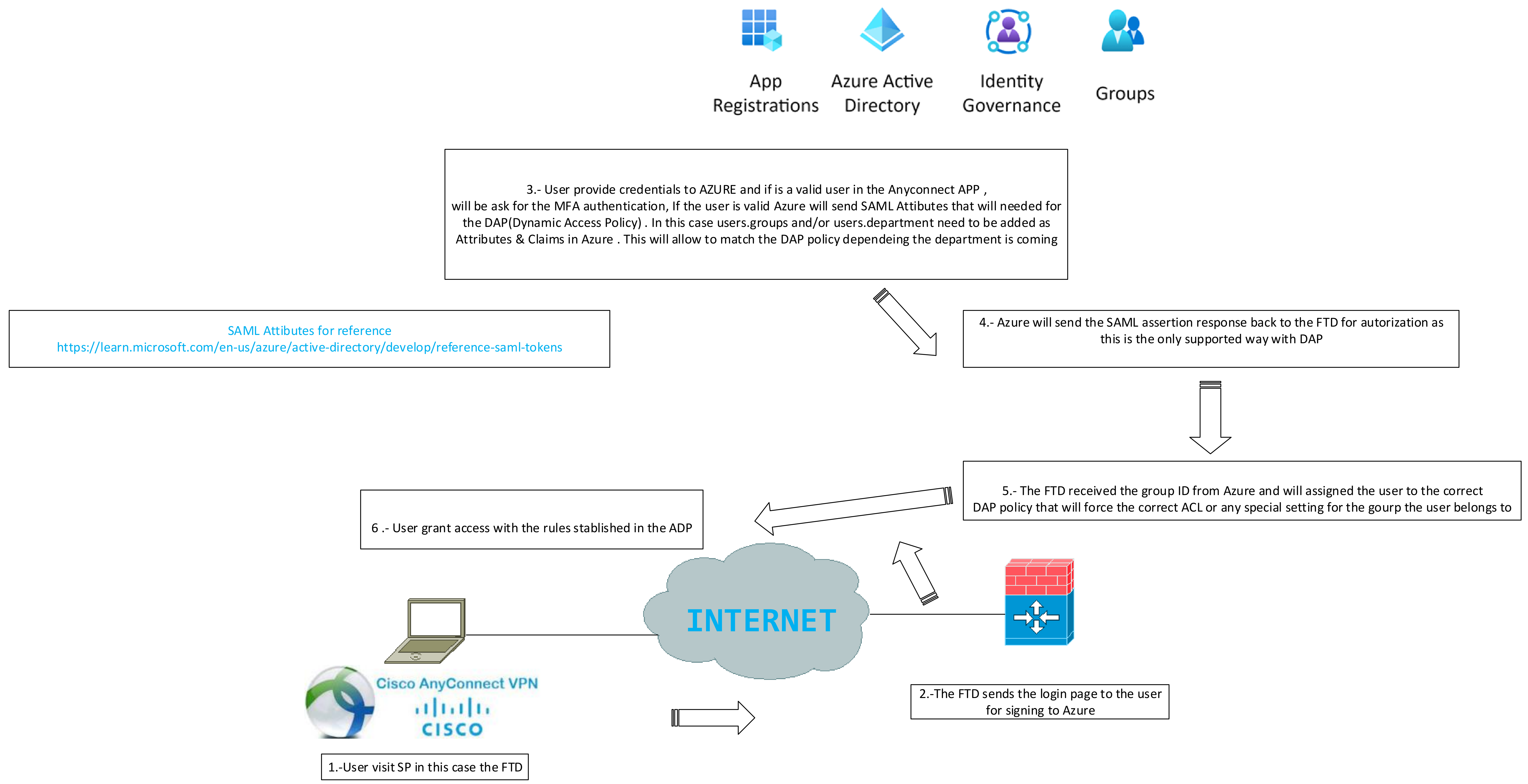
1.-User send the credendials to the FTD

2.-The FTD receives an authentication request from a VPN user that includes the username and password for connecting to a resource.

3.- Acting as a RADIUS client, the FTD converts the request to a RADIUS Access-Request message and sends it (with an encrypted password) to the RADIUS server where the NPS extension is installed, In this case the current PROXY NPS

4.- The username and password combination is verified in Active Directory. If either the username or password is incorrect, the RADIUS Server sends an Access-Reject message

5.- The username and password combination is verified in Active Directory. If the username and password are correct the NPS sends an Access-Accept message with the Autorization profile that will be the tunnel group to the FTD and the access is allowed



3.- User provide credentials to AZURE and if is a valid user in the Anyconnect APP ,
will be ask for the MFA authentication, If the user is valid Azure will send SAML Attibutes that will needed for the DAP(Dynamic Access Policy) . In this case users.groups and/or users.department need to be added as Attributes & Claims in Azure . This will allow to match the DAP policy dependeing the department is coming

SAML Attibutes for reference
https://learn.microsoft.com/en-us/azure/active-directory/develop/reference-saml-tokens

4.- Azure will send the SAML assertion response back to the FTD for autorization as this is the only supported way with DAP

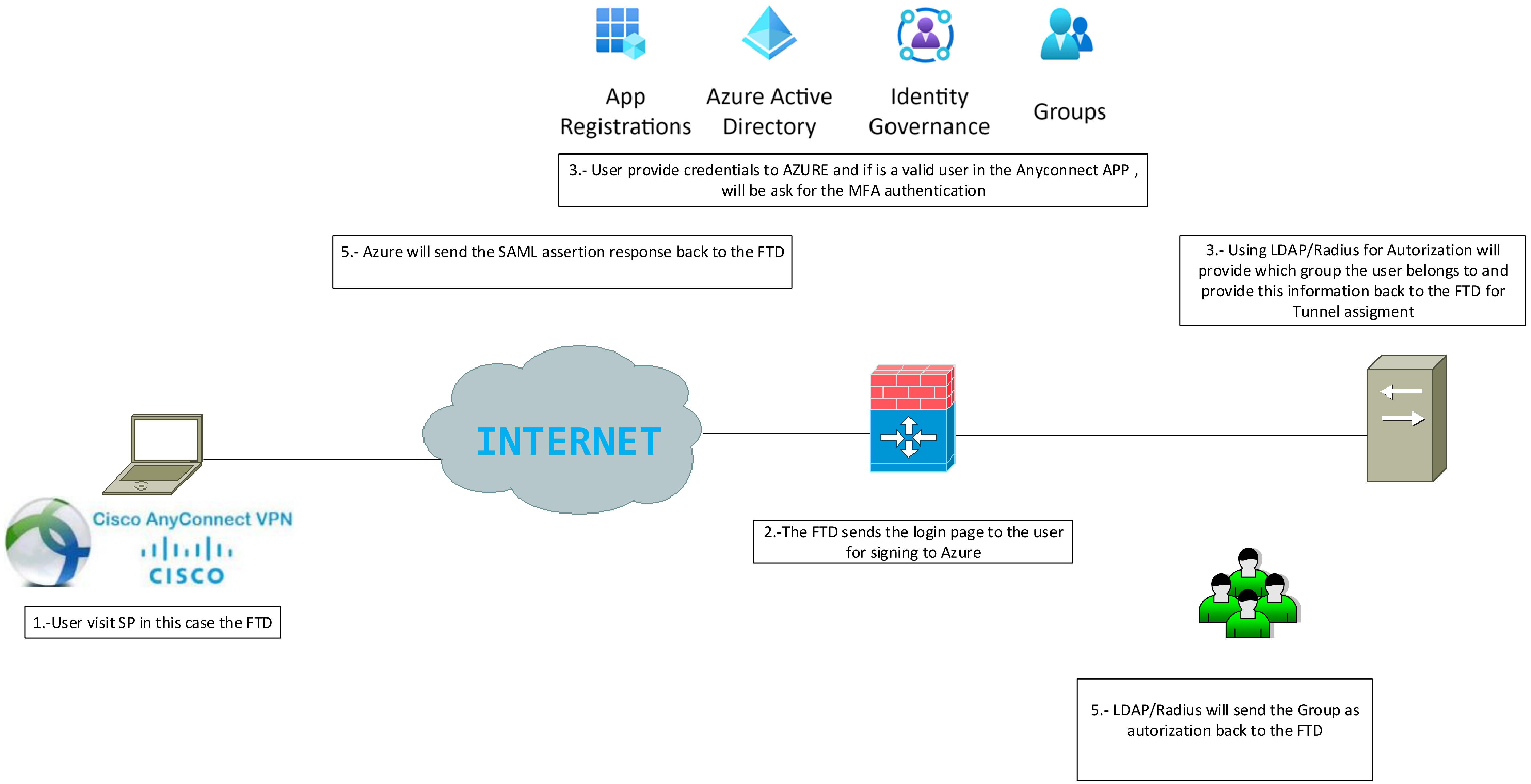
5.- The FTD received the group ID from Azure and will assigned the user to the correct DAP policy that will force the correct ACL or any special setting for the gourp the user belongs to

6 .- User grant access with the rules stablished in the ADP

2.-The FTD sends the login page to the user for signing to Azure

1.-User visit SP in this case the FTD

https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/216268-configure-anyconnect-with-saml-authentic.html



3.- User provide credentials to AZURE and if is a valid user in the Anyconnect APP , will be ask for the MFA authentication

5.- Azure will send the SAML assertion response back to the FTD

3.- Using LDAP/Radius for Autorization will provide which group the user belongs to and provide this information back to the FTD for Tunnel assigment

2.-The FTD sends the login page to the user for signing to Azure

1.-User visit SP in this case the FTD

5.- LDAP/Radius will send the Group as autorization back to the FTD