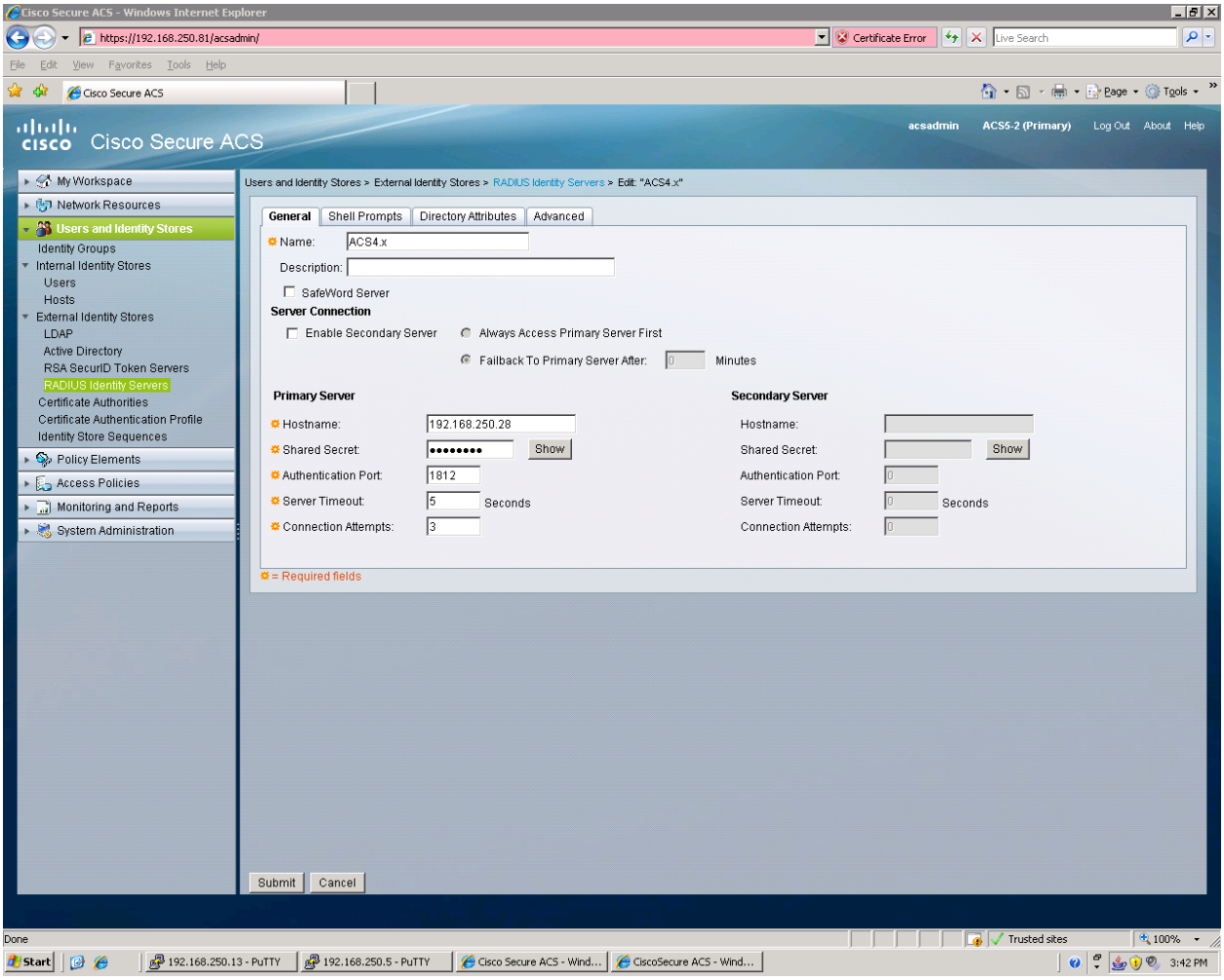
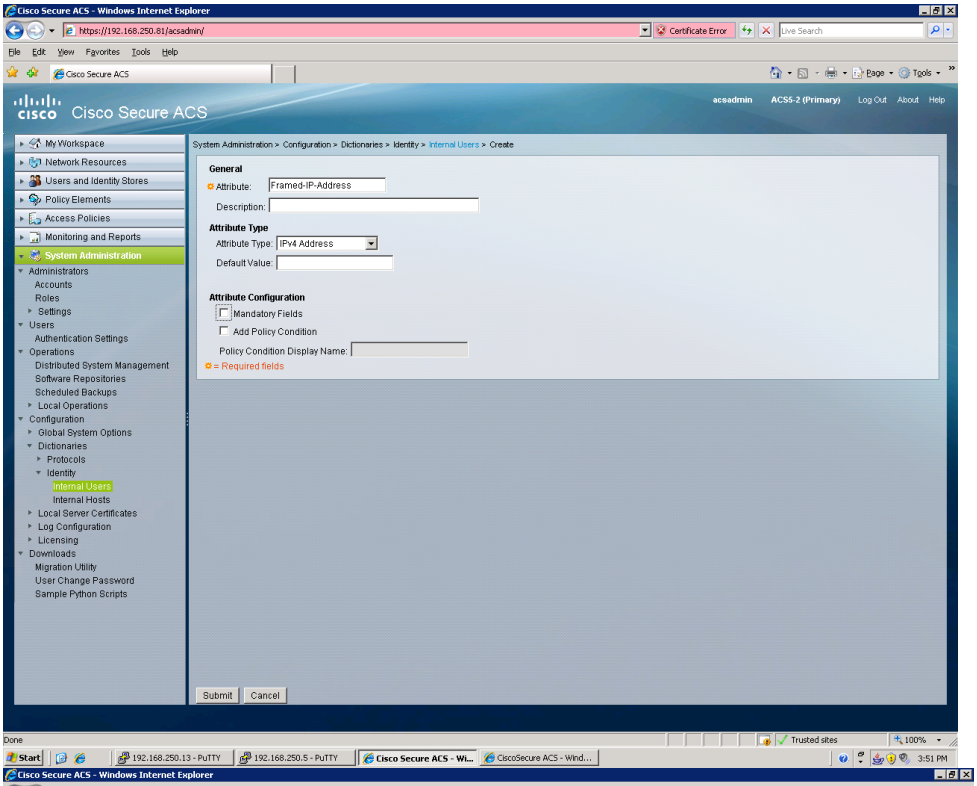
IP assignment for VPN users using an External server on ACS 5.x

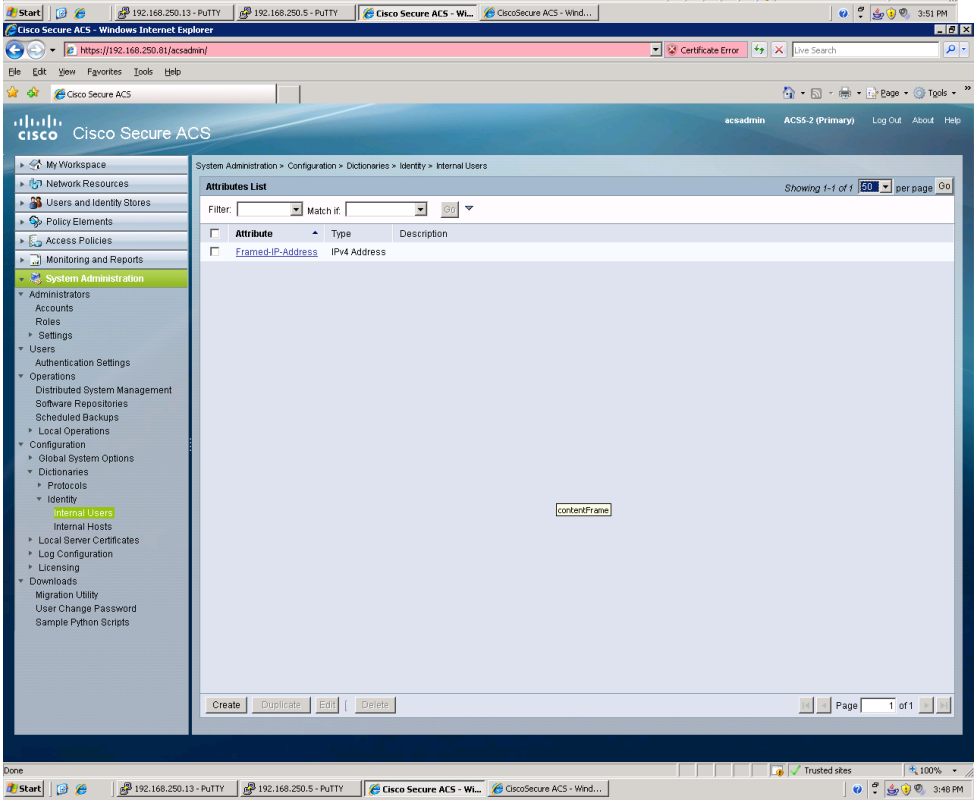
On this example I am using Radius Identity Server for the authentication and the Internal database for the Authorization to add the IP information.

Step 1: Create the Radius Identity server that will handle the user information for the authentication.

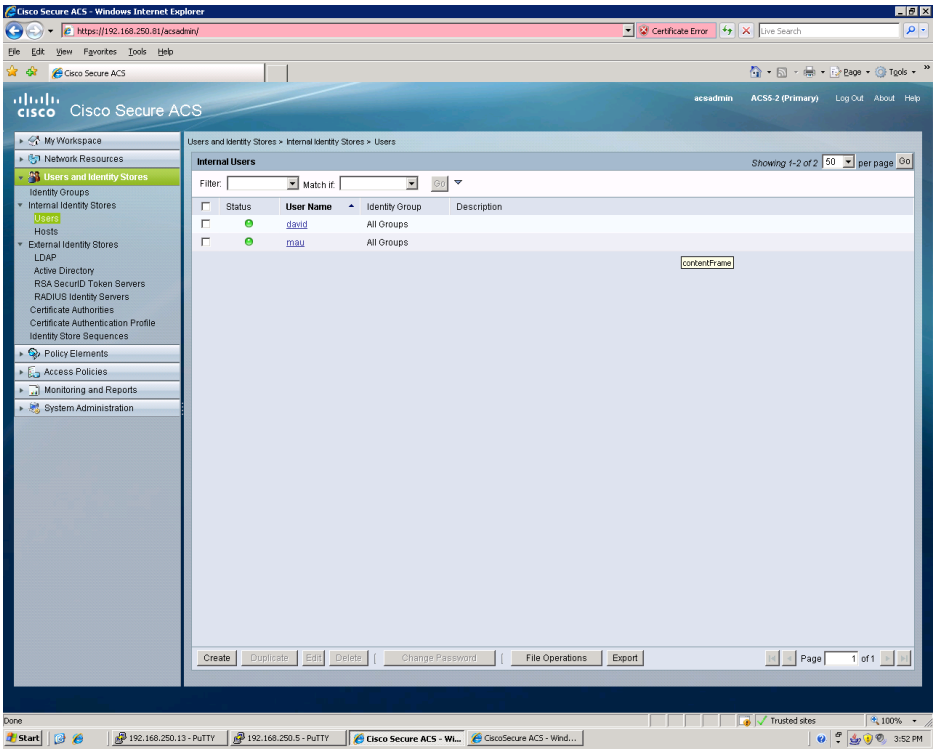


Step 2: Create a new value for the user entries that include the IP address value “IPv4 address”. This configuration is done under “System Administration” / “Configuration”/ “Dictionaries” /”Identity”/”Internal Users”

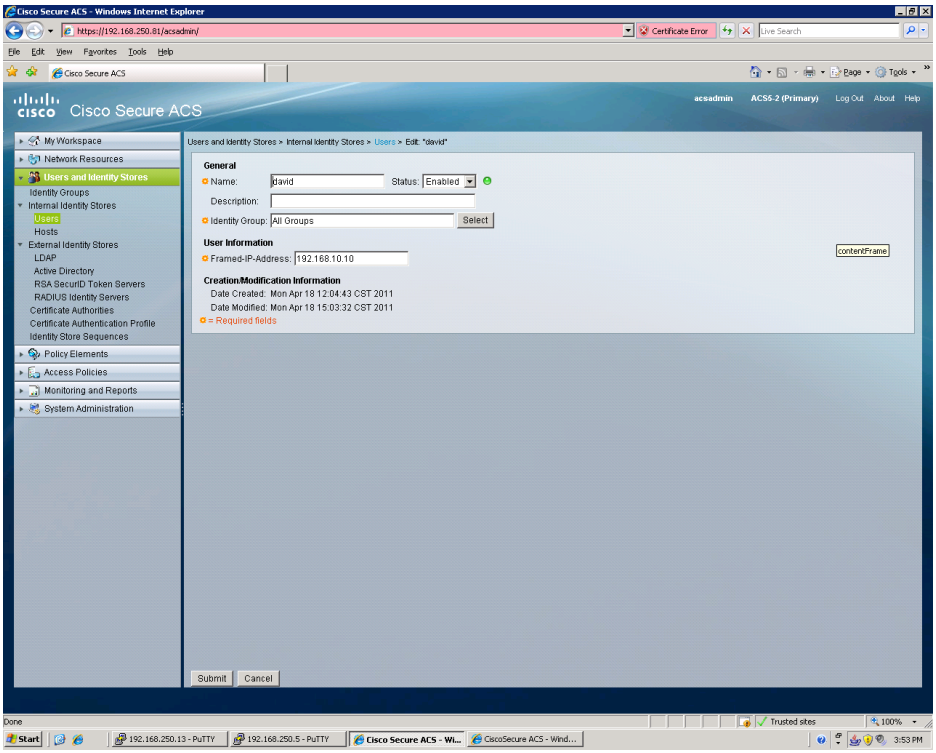




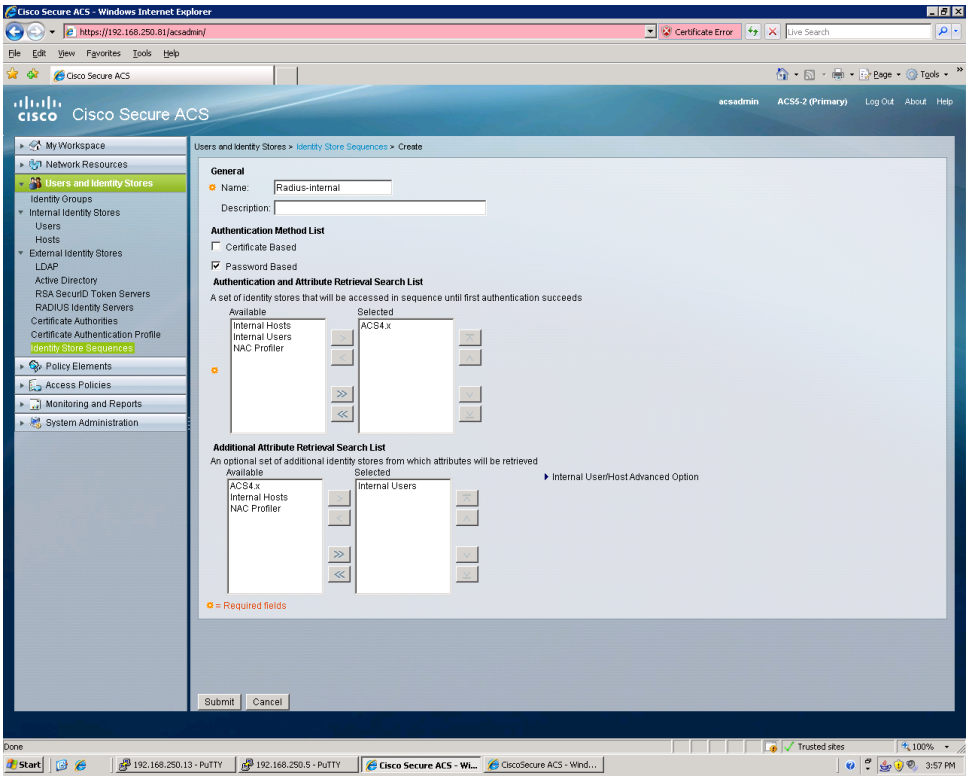
Step 3: Make sure that the user on the Radius Identity server also exist on the internal database. On this example I created two account called “David” and “Mau”

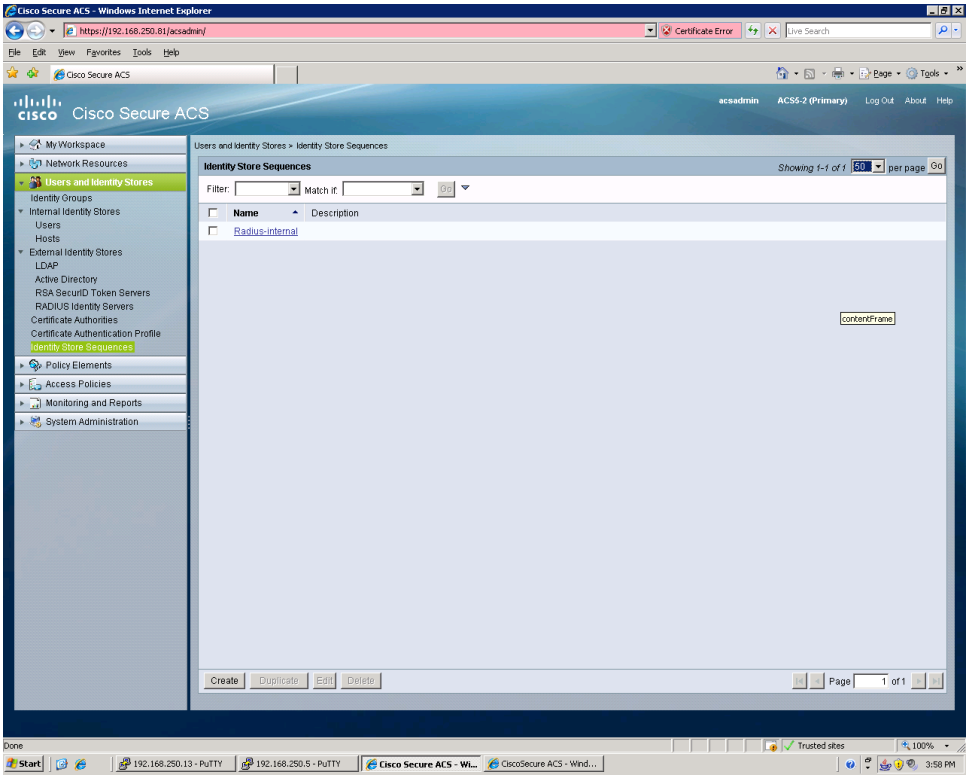


Step 4: Assign the IP address to the specific user

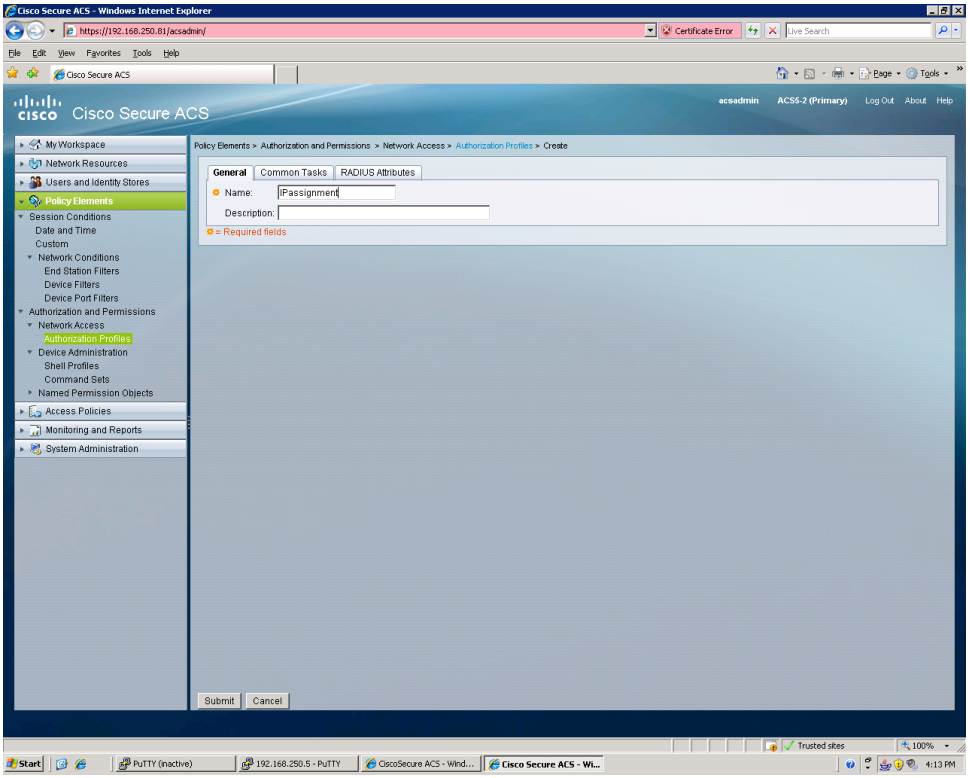


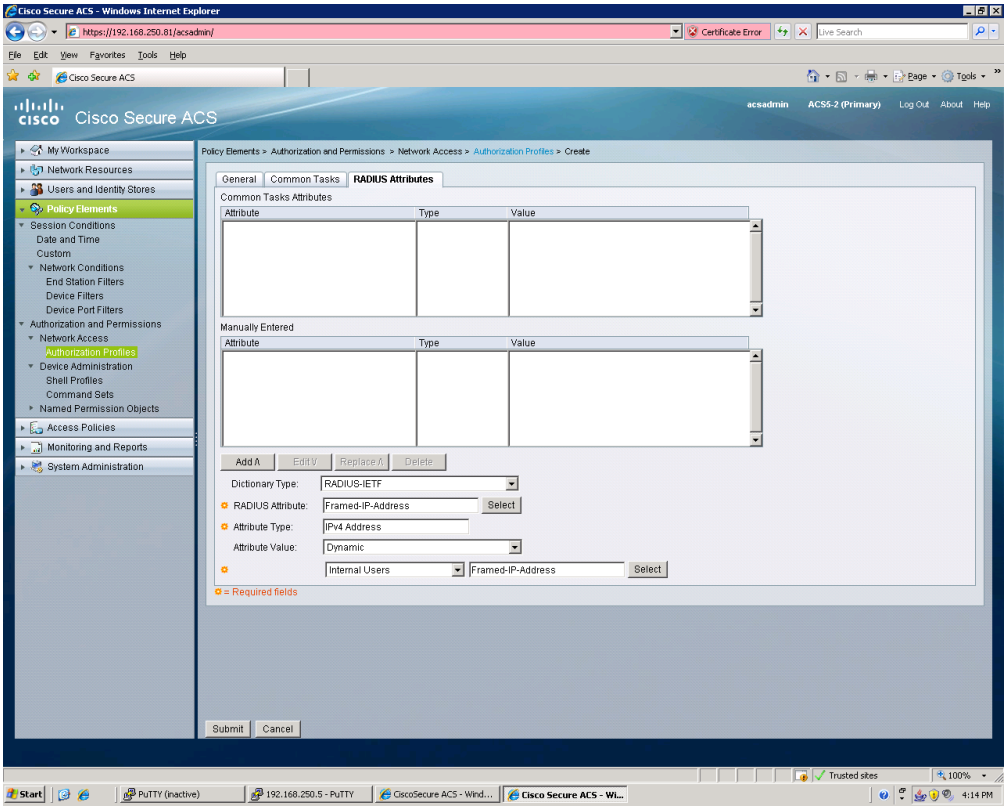
Step 5: Create a Identity Store Sequence in order to force the authentication to be done through the Radius Identity server and the additional attribute retrieval that contains the IP address created on the user against the Internal User database.





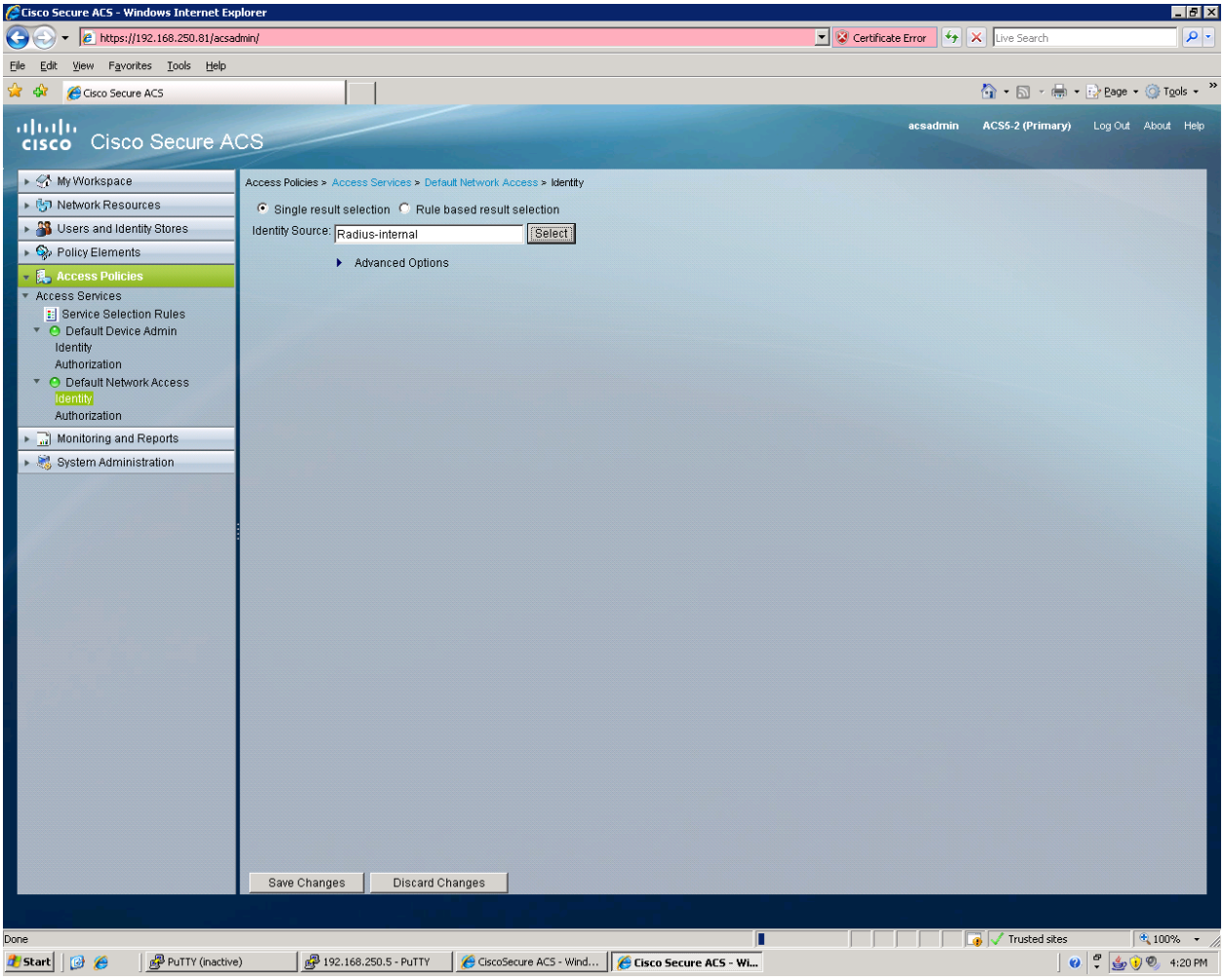
Step 6: Go into the Policy Elements / Network Access/ Authorization Profile and create a new rule



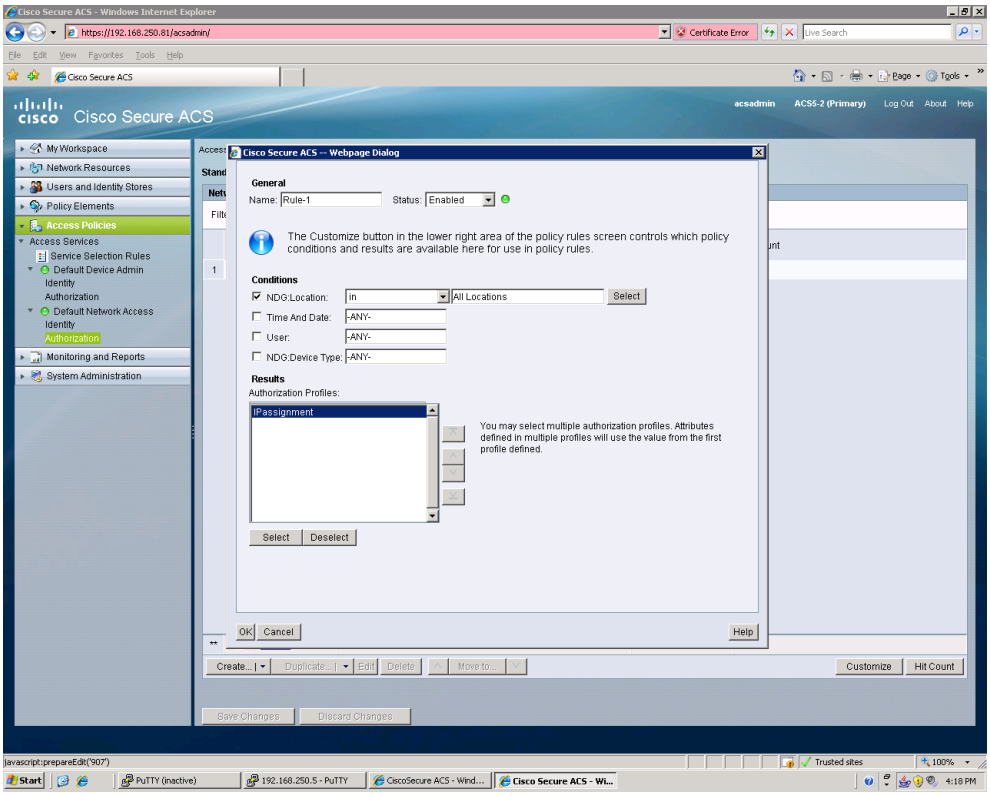


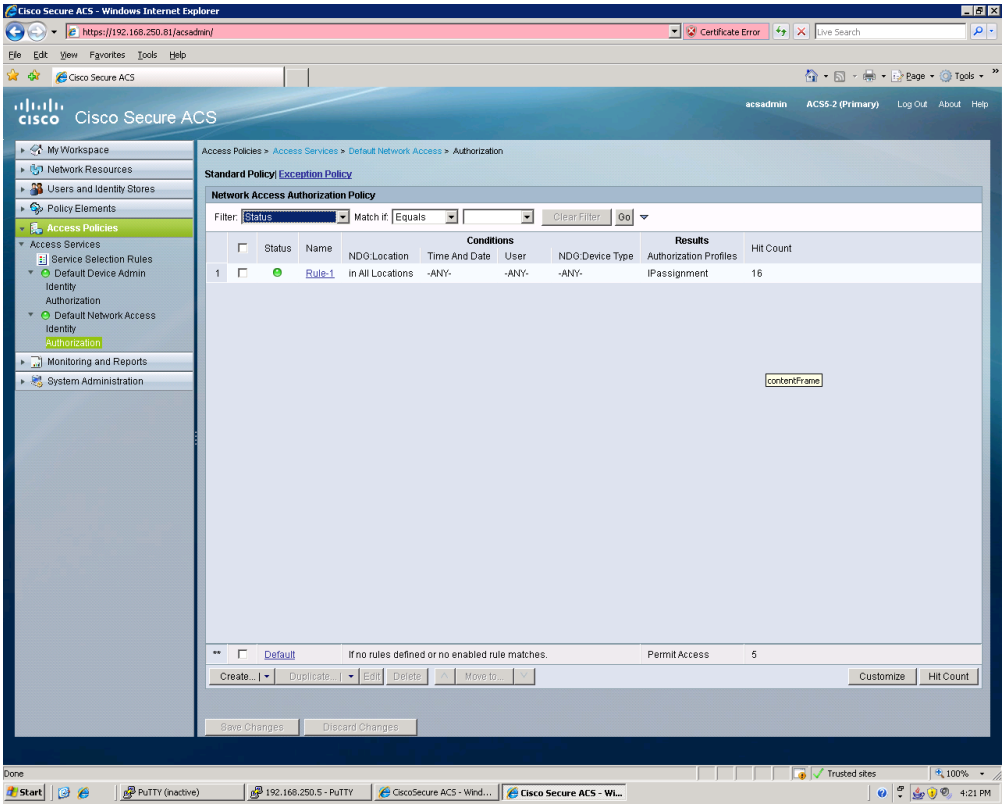
NOTE: Make sure that the new profile is using the Directory called “Radius IETF” with the attribute “Framed-IP-Address” and select the value as Dynamic using the Internal Users values and finally select the name of the attribute that was created under Step 2. On this example the name was Framed-IP-Address.

Step 7: Apply the identity store sequence into the Access Policy for the Radius Authentication so we can retrieve the authentication with the external Radius server and the authorization from the internal users.



Step 8: Create a new rule under the Authorization section of the Default Network Access or the specific Access Service that you are using and as a result apply the Authorization Profile.





Troubleshooting:

a) On the ASA or VPN Server you can enable the Radius debugs to verify if the Framed IP address attribute is being sent by the ACS.

Debug aaa authentication

Debug radius

Term monitor

Example of the log:

Parsed packet data.....
Radius: Code = 2 (0x02)
Radius: Identifier = 15 (0x0F)
Radius: Length = 56 (0x0038)
Radius: Vector: 5D9D606E796D7D9690EB931F08BDAF99
Radius: Type = 1 (0x01) User-Name
Radius: Length = 5 (0x05)
Radius: Value (String) =
6d 61 75 | mau
Radius: Type = 8 (0x08) Framed-IP-Address
Radius: Length = 6 (0x06)
Radius: Value (IP Address) = 192.168.20.120 (0xC0A81478)
Radius: Type = 25 (0x19) Class
Radius: Length = 25 (0x19)
Radius: Value (String) =
43 41 43 53 3a 41 43 53 35 2d 32 2f 39 32 35 33 | CACS:ACS5-2/9253
32 37 36 38 2f 31 36 | 2768/16
rad_procpkt: ACCEPT
RADIUS_ACCESS_ACCEPT: normal termination
RADIUS_DELETE
remove_req 0xd8381bd0 session 0x113 id 15
free_rip 0xd8381bd0
radius: send queue empty
INFO: Authentication Successful

b) Verify the ACS reports to verify if the Authorization Profile is being assigned.