Command Authorization on PIX/ASA 7.x

[1] Configuration on PIX/ASA 7.x :

!—Local user account for fallback purpose

username <username> password <password> privilege 15
username enable_15 password <enable-password> privilege 15

aaa-server TACACS+ protocol tacacs+
aaa-server TACACS+ host <ACS-ip-addr> <Shared-Key>

aaa authentication telnet console TACACS+ LOCAL
aaa authentication ssh console TACACS+ LOCAL
aaa authentication serial console TACACS+ LOCAL
aaa authentication http console TACACS+ LOCAL

aaa authentication enable console TACACS+ LOCAL

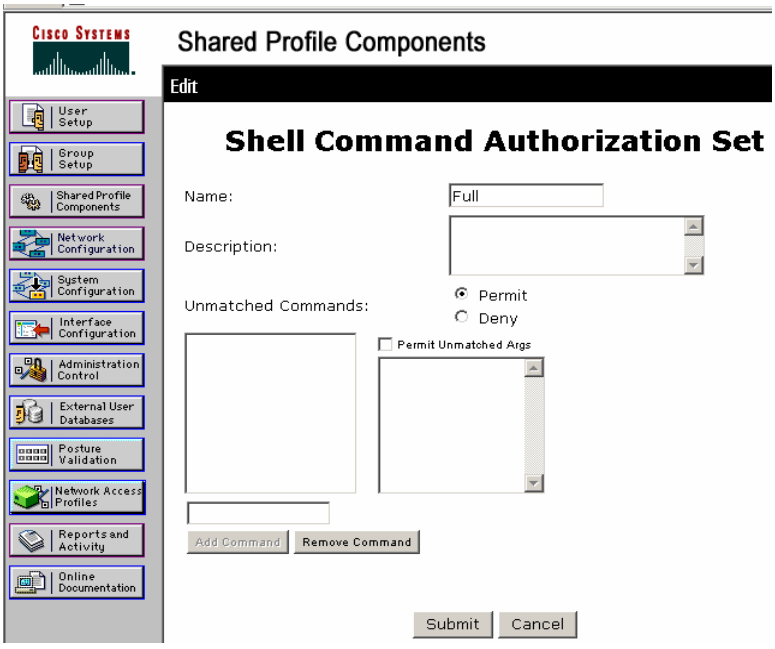
aaa authorization command TACACS+ LOCAL

aaa accounting telnet console TACACS+
aaa accounting ssh console TACACS+
aaa accounting serial console TACACS+
aaa accounting enable console TACACS+
aaa accounting command TACACS+

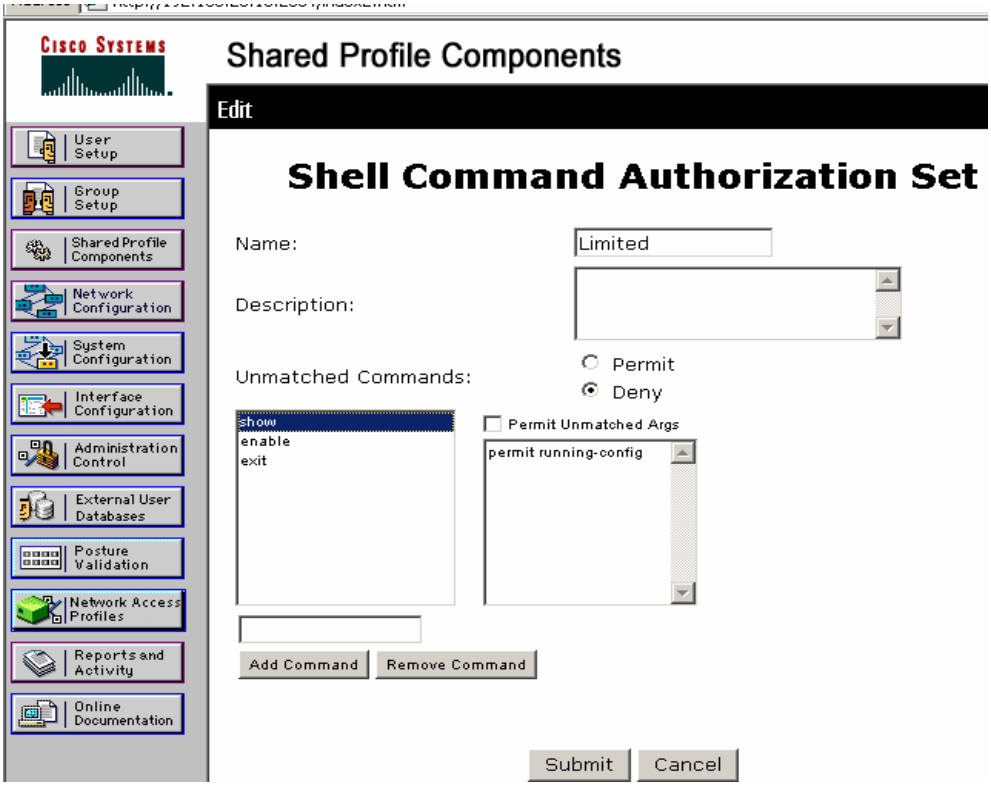
[2] Configuration on ACS:

[a] Create Shell Command authorization Set :

[b] One for Full Access:

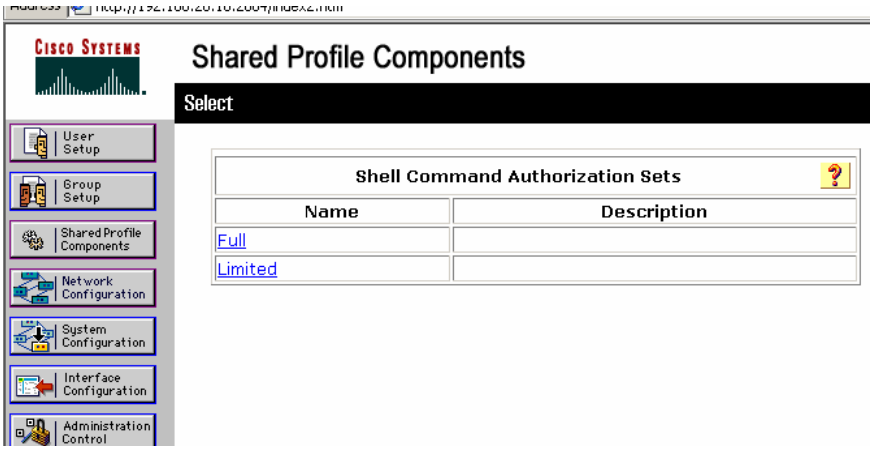


[c] One for Limited Access:



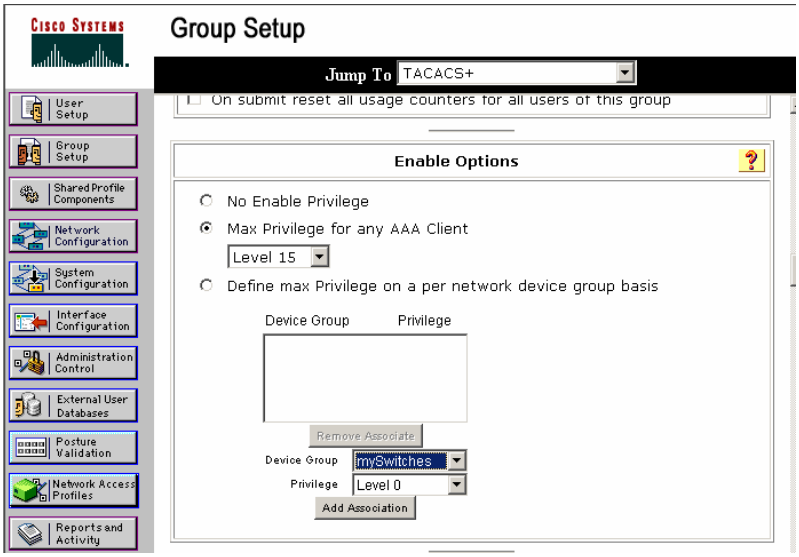
For detail on how to specify command, please refer to link provided below

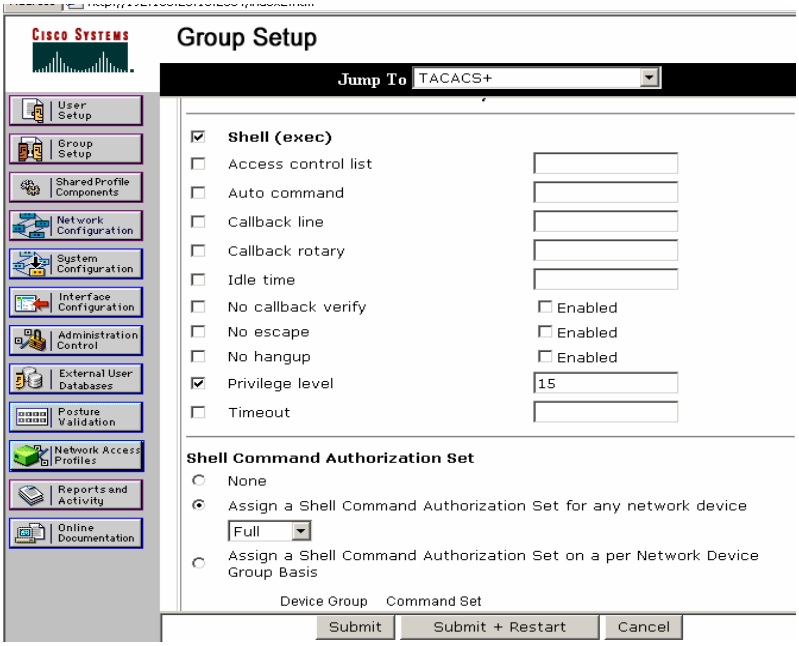
http://www.cisco.com/univercd/cc/td/doc/product/multisec/asa_sw/v_7_2/conf_gd/sysadmin/mgaccess.htm#wp1042042



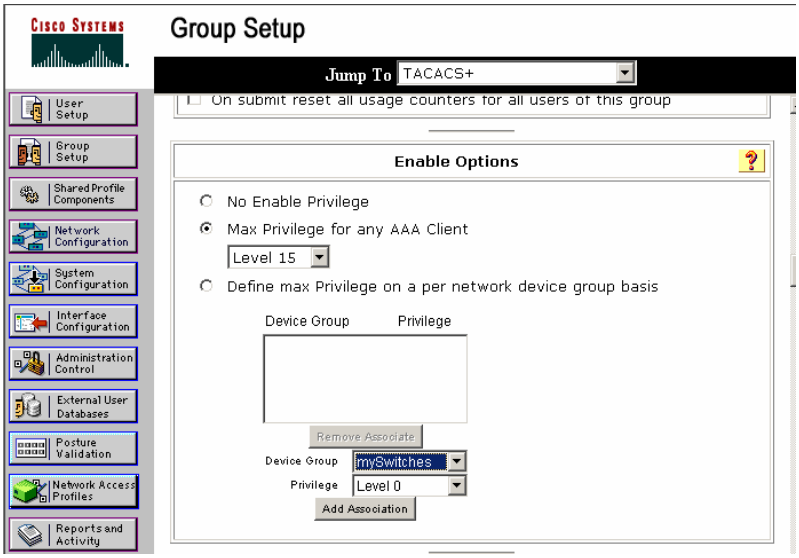
[d] Create two users and two groups on ACS from User Setup:

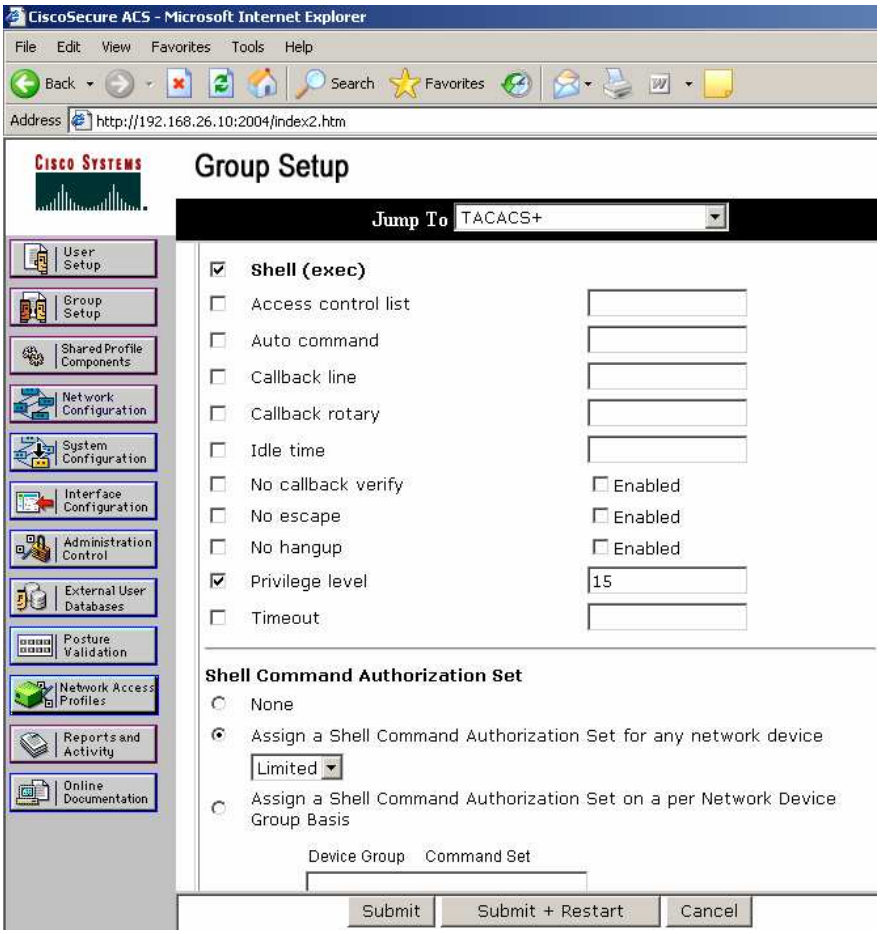
--A group for Full Access:





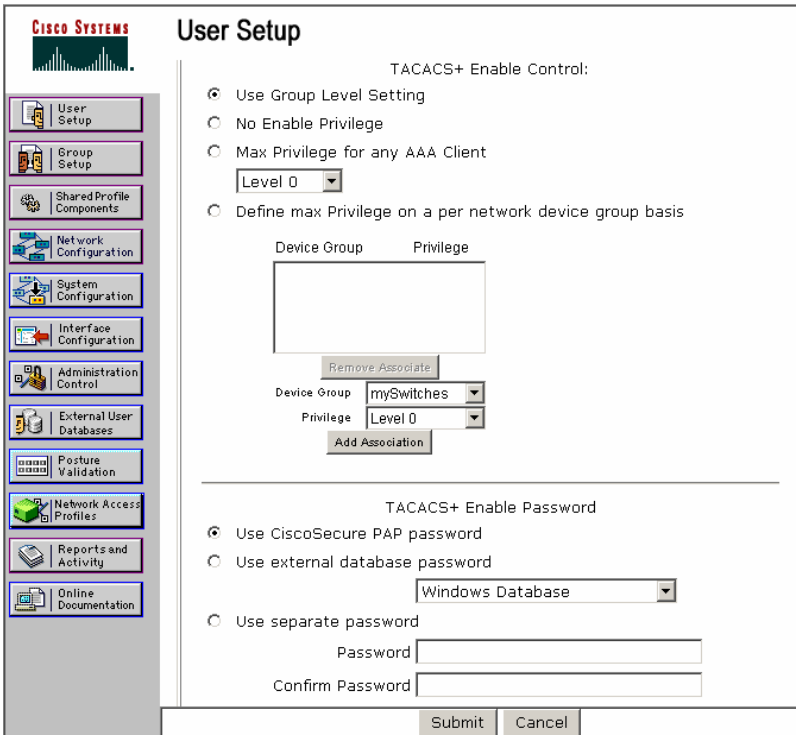
--A group for Limited Access:





--A User for account:

By default a user doesn't have Enable Privileges, and as user setting over takes group setting, so either we can specify the enable privilege per user, of check "Use Group Level Setting". Also, by default for a user, "Use separate password" is checked, and the field is empty. To log in to enable mode, we can choose password of our choice, as in example, the user account is a local user so we have selected same password for enable password.



Please go through following link, before applying command authorization :

http://www.cisco.com/univercd/cc/td/doc/product/multisec/asa_sw/v_7_2/conf_gd/sysadmin/mgaccess.htm#wp1042042

Please be aware that ASA will not log for show command :

http://www.cisco.com/univercd/cc/td/doc/product/multisec/asa_sw/v_7_2/conf_gd/sysadmin/mgaccess.htm#wp1059882

-pbanga@cisco.com