Generate A CSR In Cisco ASA SSL VPN/Firewall:

1. From the Cisco Adaptive Security Device Manager (ASDM), select "Configuration" and then "Device Management."
2. Expand "Certificate Management," then select "Identity Certificates," and then "Add."
3. Select the button to "Add a new identity certificate" and click the "New..." link for the Key Pair.
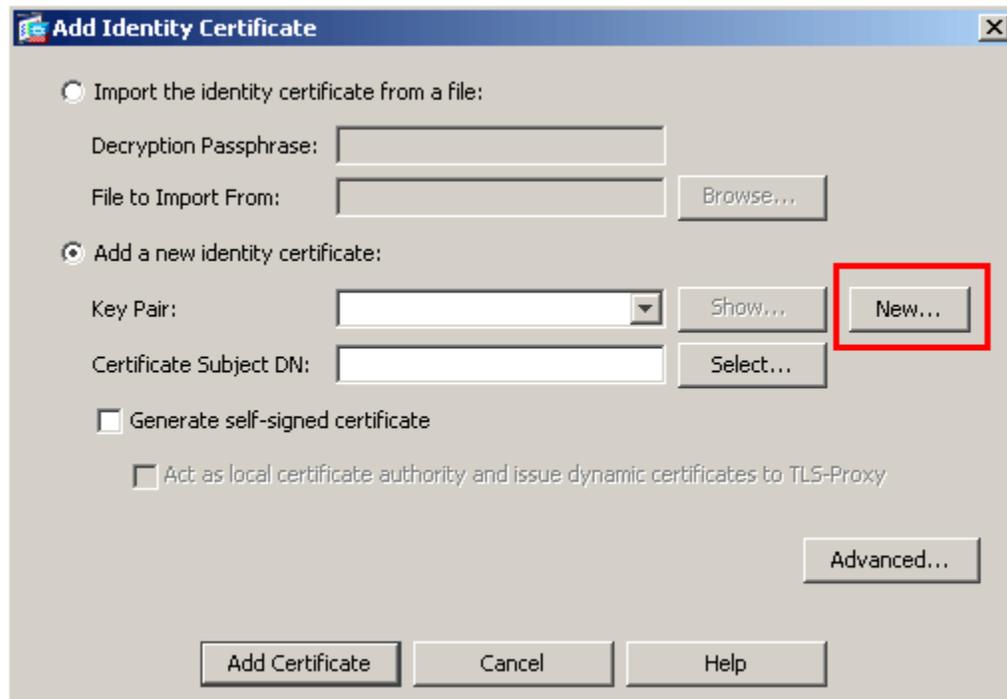
4. Select the option to "Enter new key pair name" and enter a name (any name) for the key pair. Next, click the "Generate Now" button to create your key pair.

Change the key size to 2048 and leave Usage on General purpose.
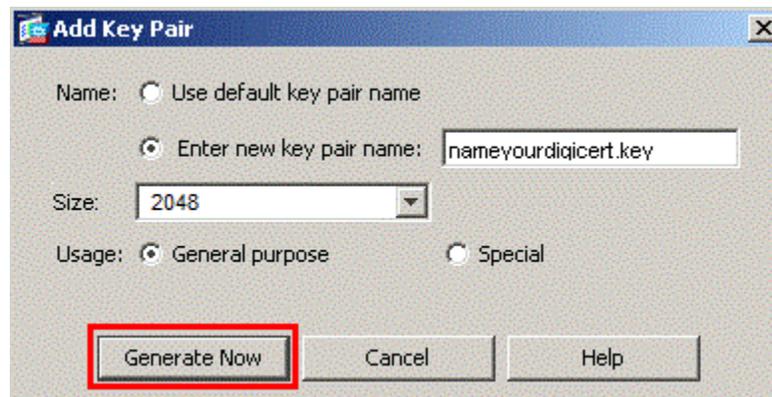
5. Next you will define the "Certificate Subject DN" by clicking the Select button to the right of that field. In the Certificate Subject DN window, configure the following values by selecting each from the "Attribute" drop-down list, entering the appropriate value, and clicking "Add."

CN - The name through which the firewall will be accessed (usually the fully qualified domain name, e.g., vpn.domain.com).

OU - The name of your department within the organization (frequently this entry will be listed as "IT," "Web Security," or is simply left blank).

O - The legally registered name of your organization/company.

C - If you do not know your country's two-digit code, IN

ST - The state in which your organization is located.

L - The city in which your organization is located.
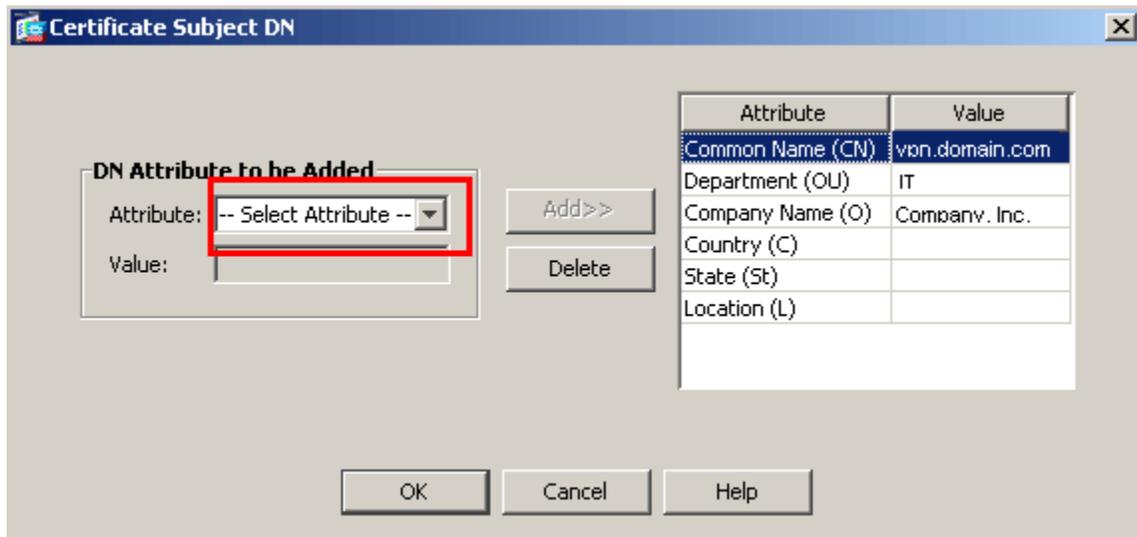
6. Next, click "Advanced" in the "Add Identity Certificate" window.
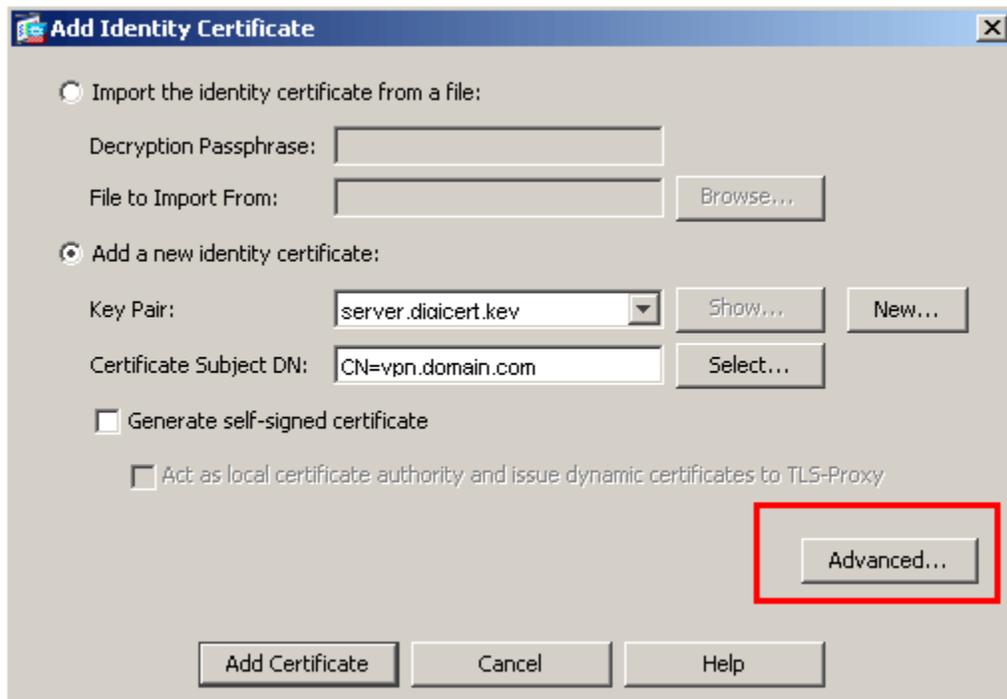
7. In the FQDN field, type in the fully qualified domain name through which the device will be accessed externally, e.g., vpn.domain.com (or the same name as was entered in the CN value in step 5).
8. Click "OK" and then "Add Certificate." You will then be prompted to save your newly created CSR information as a text file (.txt extension).

Remember the filename that you choose and the location to which you save it. You will need to open this file as a text file and copy the entire body of it (including the Begin and End Certificate Request tags) into the online order process when prompted.