**AAA and VPNs:**

AAA and VPNs:

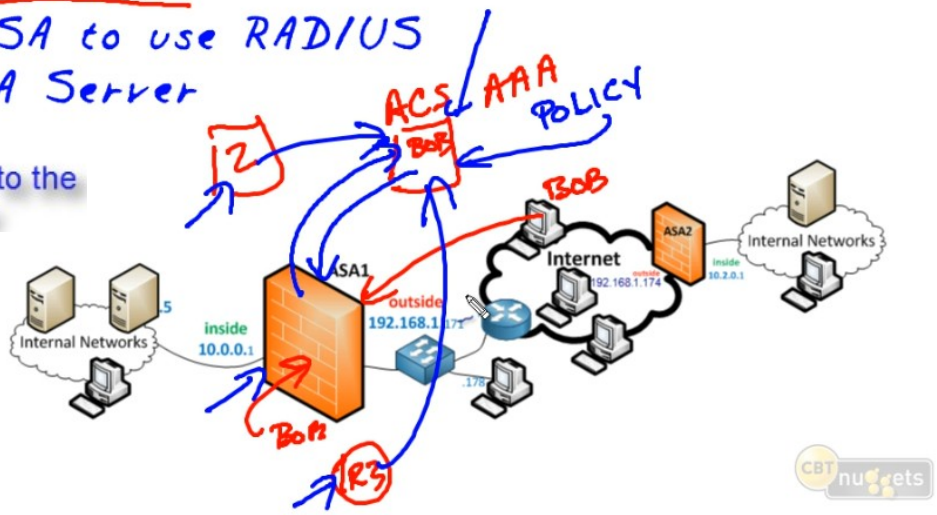
Using RADIUS for AAA VPN policy

---

- LOCAL vs Centralized

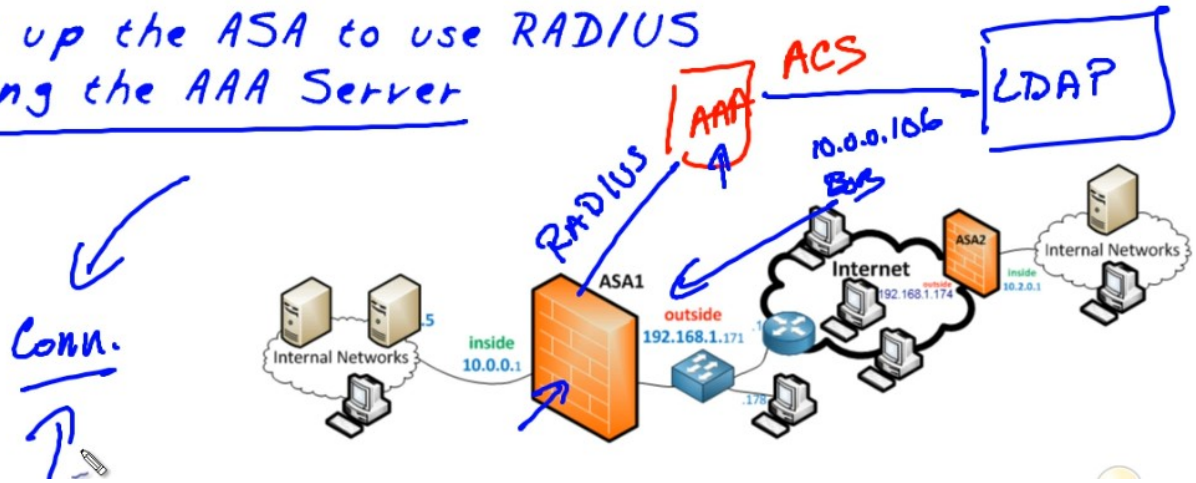
Set up the ASA to use RADIUS Using the AAA Server

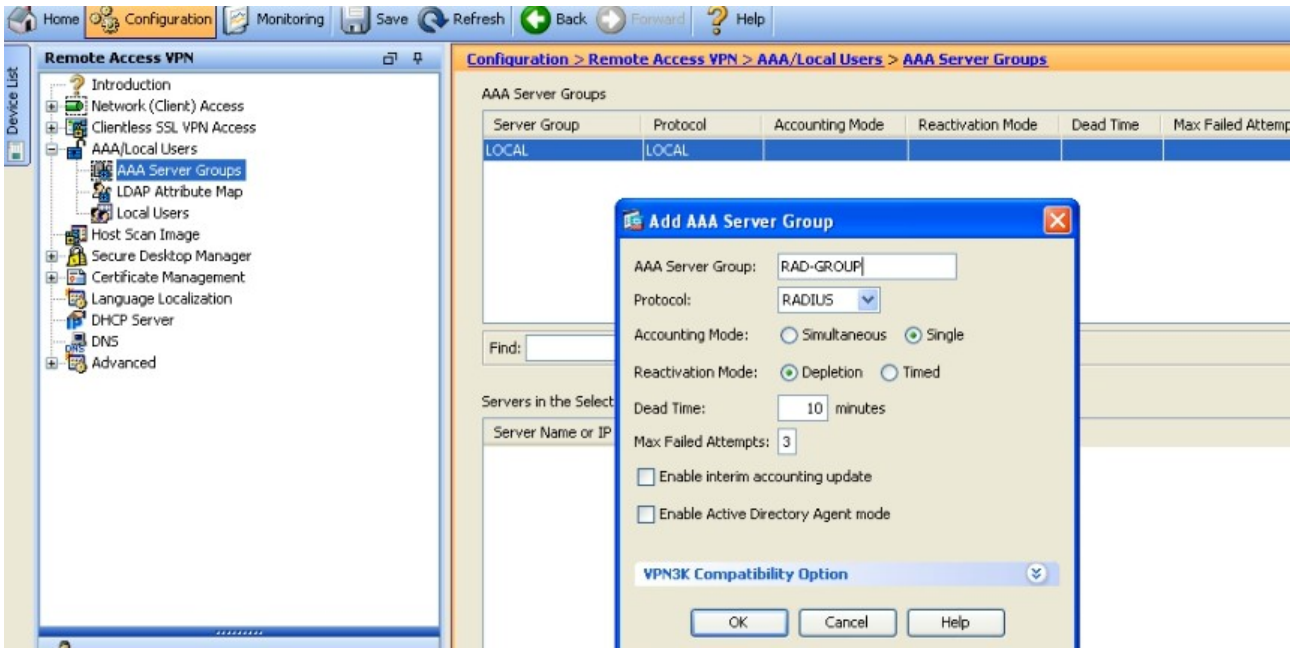
The ASA is a "client" to the ACS AAA server

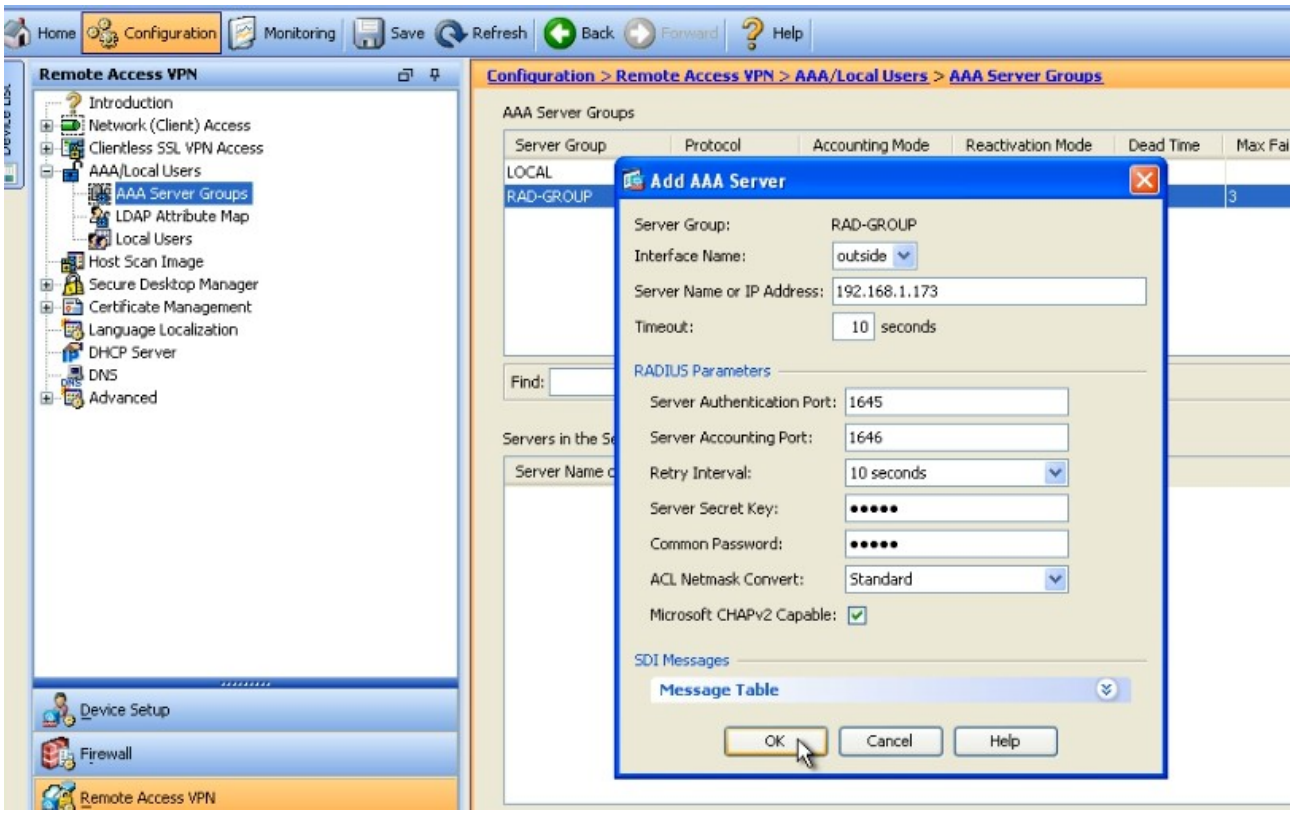



LOCAL vs Centralized

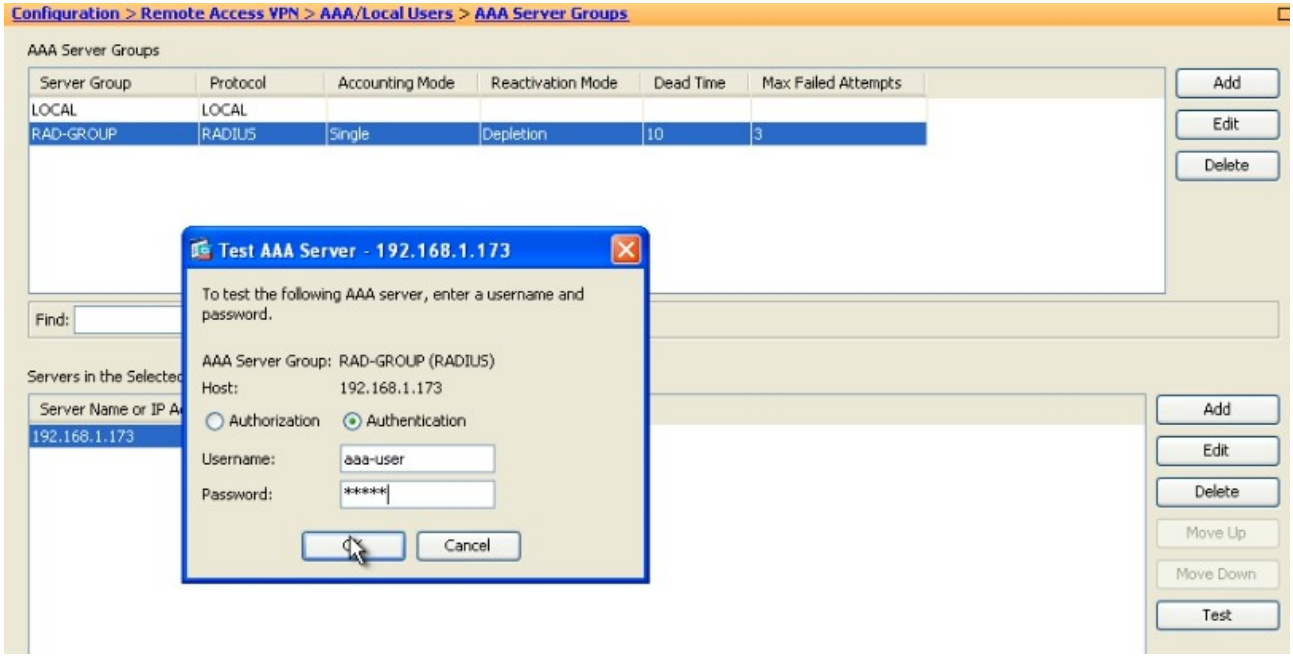
Set up the ASA to use RADIUS Using the AAA Server





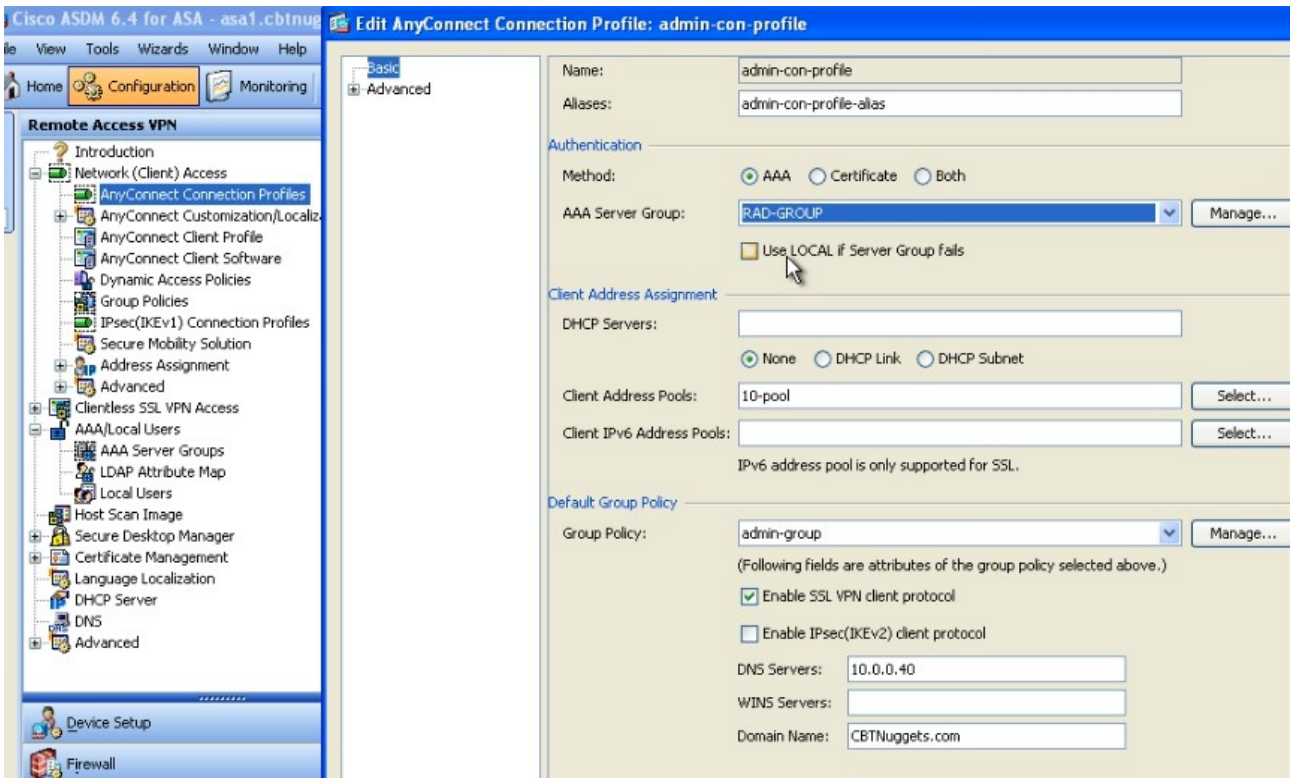




Good to do a test once server is configured.



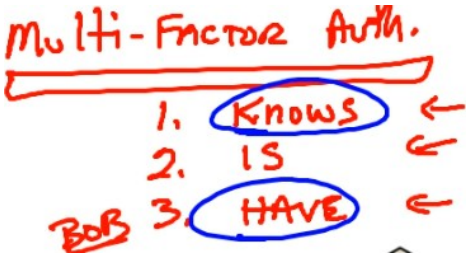

```
ASA1# test aaa-server ?

  ad-agent        Test connectivity to the AD agent server
  authentication  Test connectivity to the authentication server
  authorization   Test connectivity to the authorization server
ASA1# test aaa-server
```

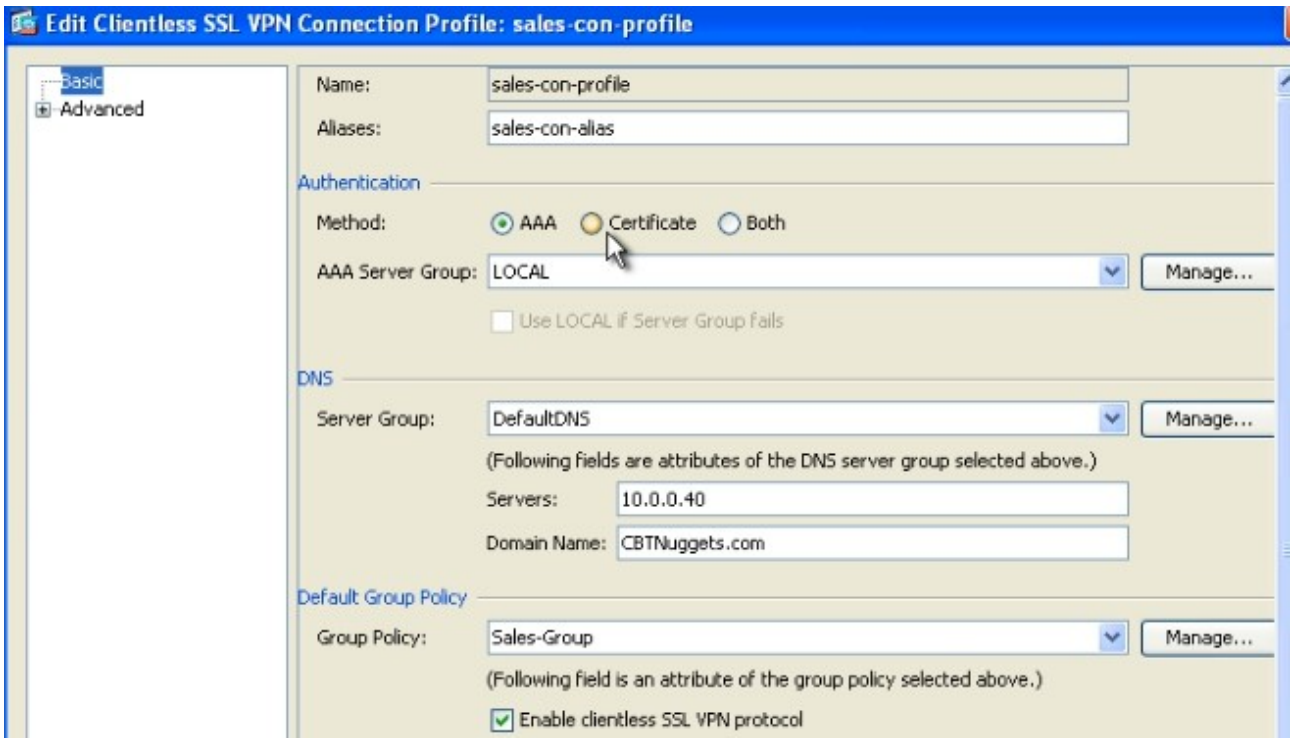


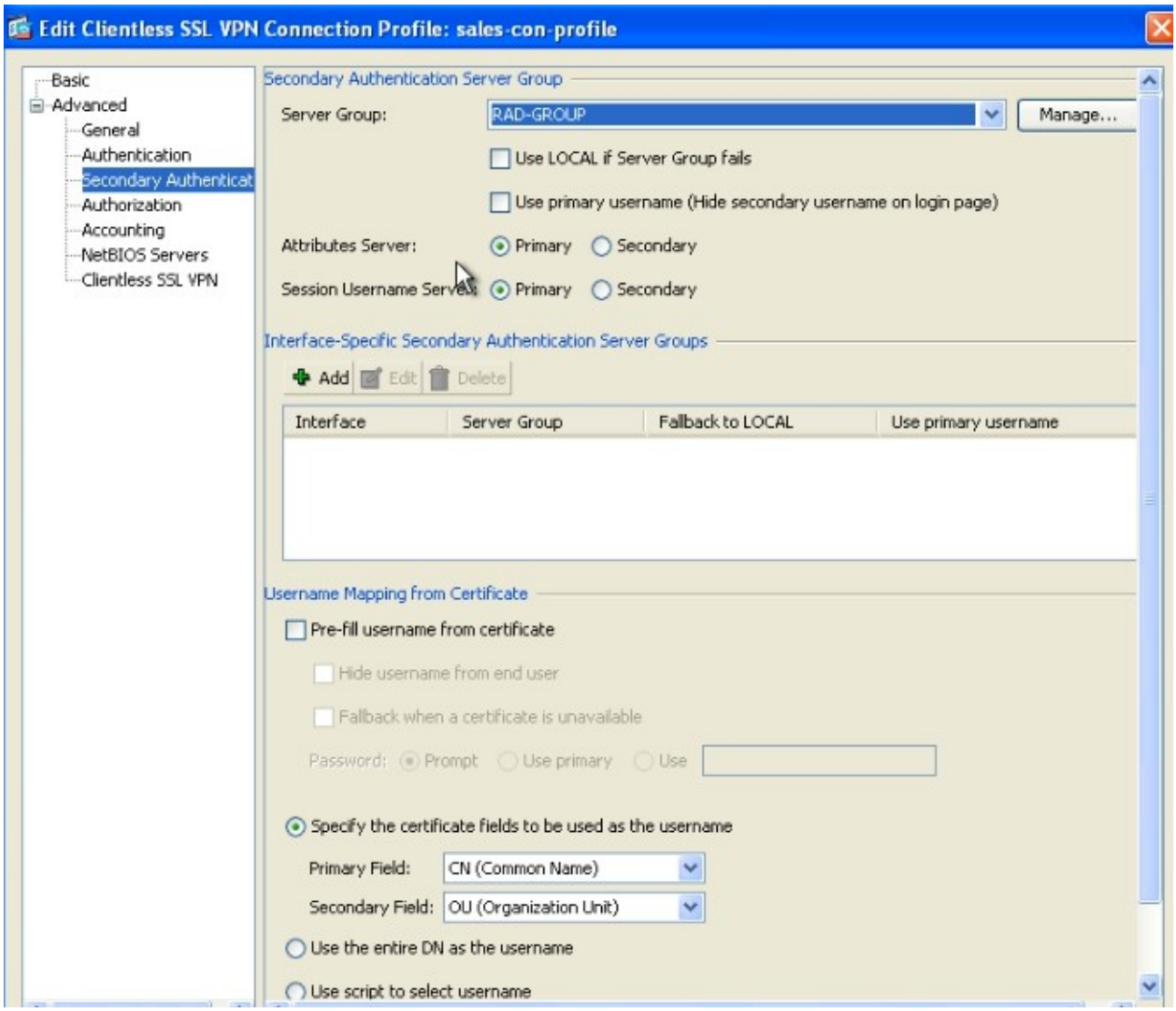

aaa-user is on the ACS and not on the local database of the ASA.

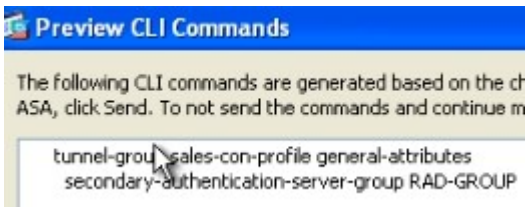





ASA can be a facilitator of Multi Factor authenticaion:
e.g. Safenet tokens that are proviosioned to the users and generate OTP (One Time Password) every 60 seconds.
user knows(username/password) and user have (OTP from the token)
tokens can be software or hardware (e.g. safenet or even google authenticator)


Edit Clientless SSL VPN Connection Profile: sales-con-profile
Basic
Advanced
Name:
sales-con-profile
Aliases:
sales-con-alias
Authentication
Method:
AAA
Certificate
Both
AAA Server Group:
LOCAL
Manage...
Use LOCAL if Server Group fails
DNS
Server Group:
DefaultDNS
Manage...
(Following fields are attributes of the DNS server group selected above.)
Servers:
10.0.0.40
Domain Name:
CBTNuggets.com
Default Group Policy
Group Policy:
Sales-Group
Manage...
(Following field is an attribute of the group policy selected above.)
Enable clientless SSL VPN protocol


Edit Clientless SSL VPN Connection Profile: sales-con-profile
Basic
Advanced
General
Authentication
Secondary Authenticat
Authorization
Accounting
NetBIOS Servers
Clientless SSL VPN
Secondary Authentication Server Group
Server Group:
RAD-GROUP
Manage...
Use LOCAL if Server Group fails
Use primary username (Hide secondary username on login page)
Attributes Server:
Primary
Secondary
Session Username Server:
Primary
Secondary
Interface-Specific Secondary Authentication Server Groups
Add
Edit
Delete
Interface
Server Group
Fallback to LOCAL
Use primary username
Username Mapping from Certificate
Pre-fill username from certificate
Hide username from end user
Fallback when a certificate is unavailable
Password:
Prompt
Use primary
Use
Specify the certificate fields to be used as the username
Primary Field:
CN (Common Name)
Secondary Field:
OU (Organization Unit)
Use the entire DN as the username
Use script to select username


Preview CLI Commands
The following CLI commands are generated based on the ch
ASA, click Send. To not send the commands and continue m
tunnel-grou sales-con-profile general-attributes
secondary-authentication-server-group RAD-GROUP


Address
https://asa1.cbtnuggets.com/+CSCOE+/logon.html?reason=12&gmsg=666E7972662D
Go


Logon
Group
sales-con-alias
Username
sales-user
Password
2nd Username
aaa-user
2nd Password
Logon


Edit AnyConnect Connection Profile: sales-con-profile
Basic
Advanced
General
Client Addressing
Authentication
Secondary Authenticat
Authorization
Accounting
Group Alias/Group URL
Authorization Server Group
Server Group:
RAD-GROUP
Manage...
Users must exist in the authorization database to connect
Interface-specific Authorization Server Groups
Add
Edit
Delete
Interface
Server Group


Edit AnyConnect Connection Profile: sales-con-profile
Basic
Advanced
General
Client Addressing
Authentication
Secondary Authenticat
Authorization
Accounting
Group Alias/Group URL
Server Group:
RAD-GROUP
Manage...