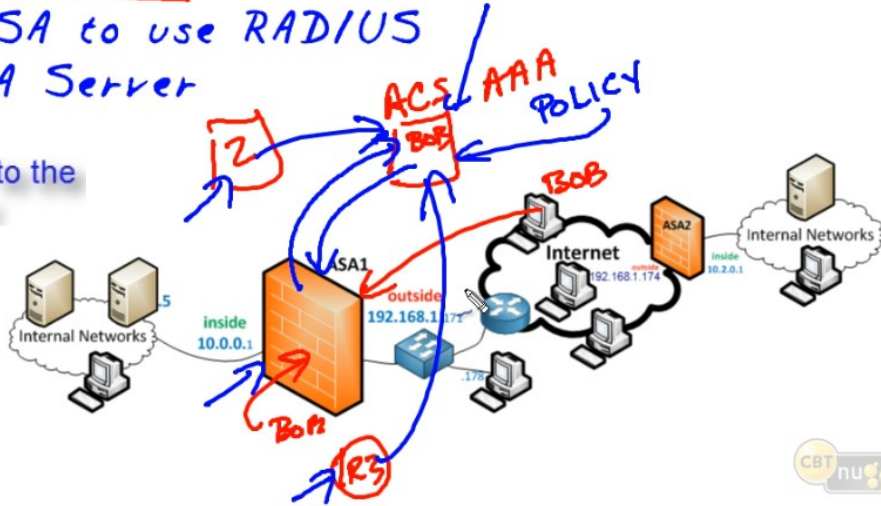


AAA and VPNs:
 AAA and VPNs:

Using RADIUS for AAA VPN policy

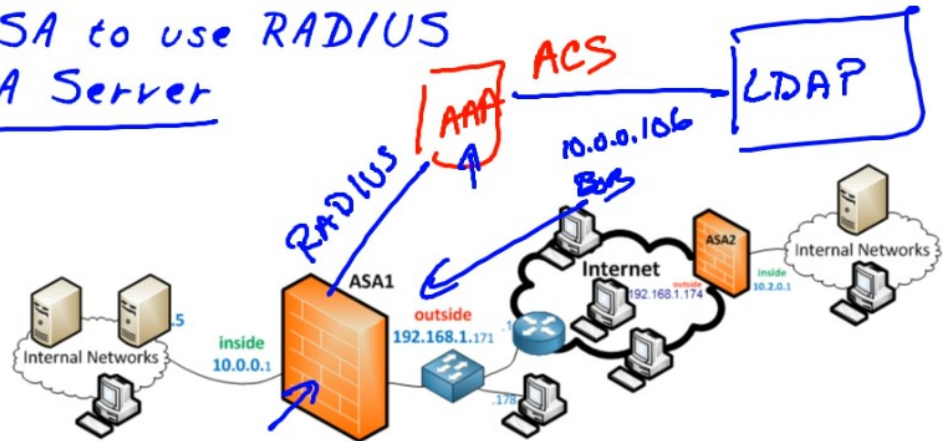
- LOCAL vs Centralized
 Set up the ASA to use RADIUS
 Using the AAA Server

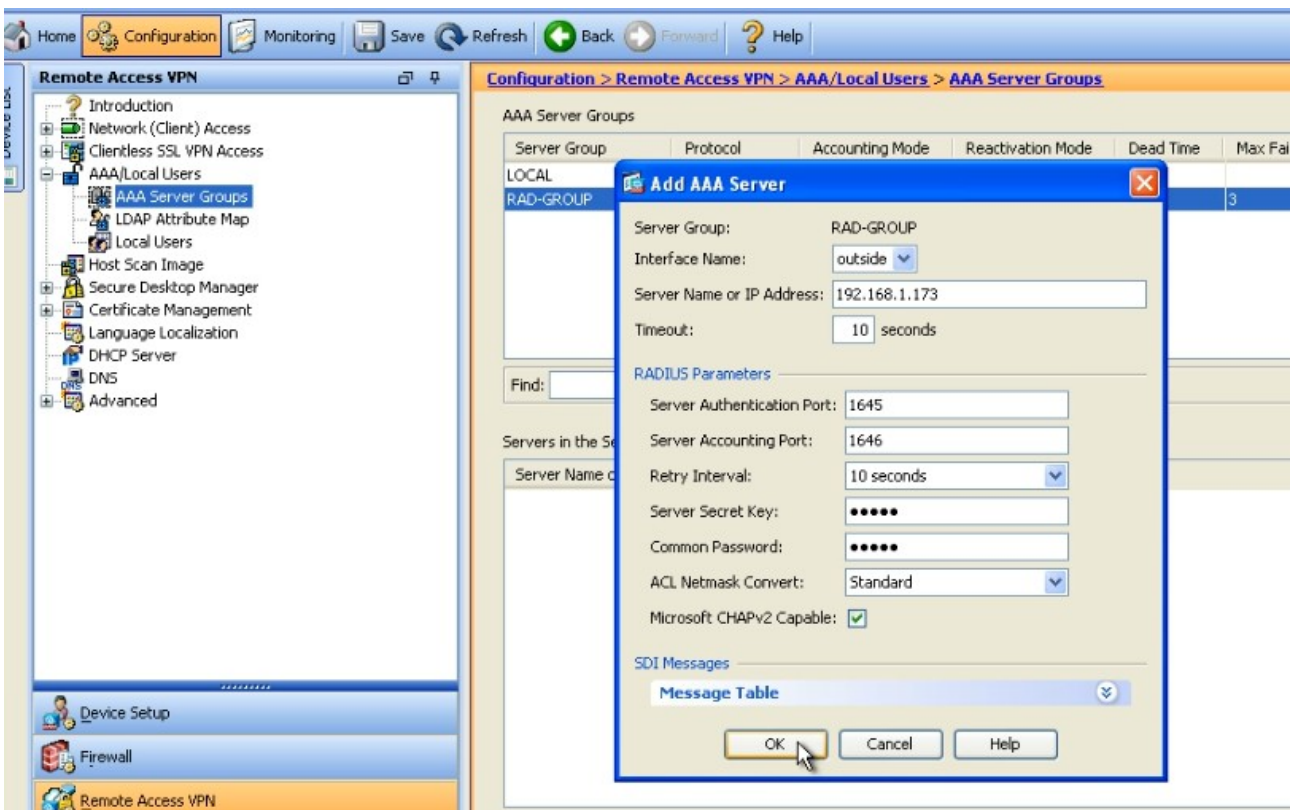
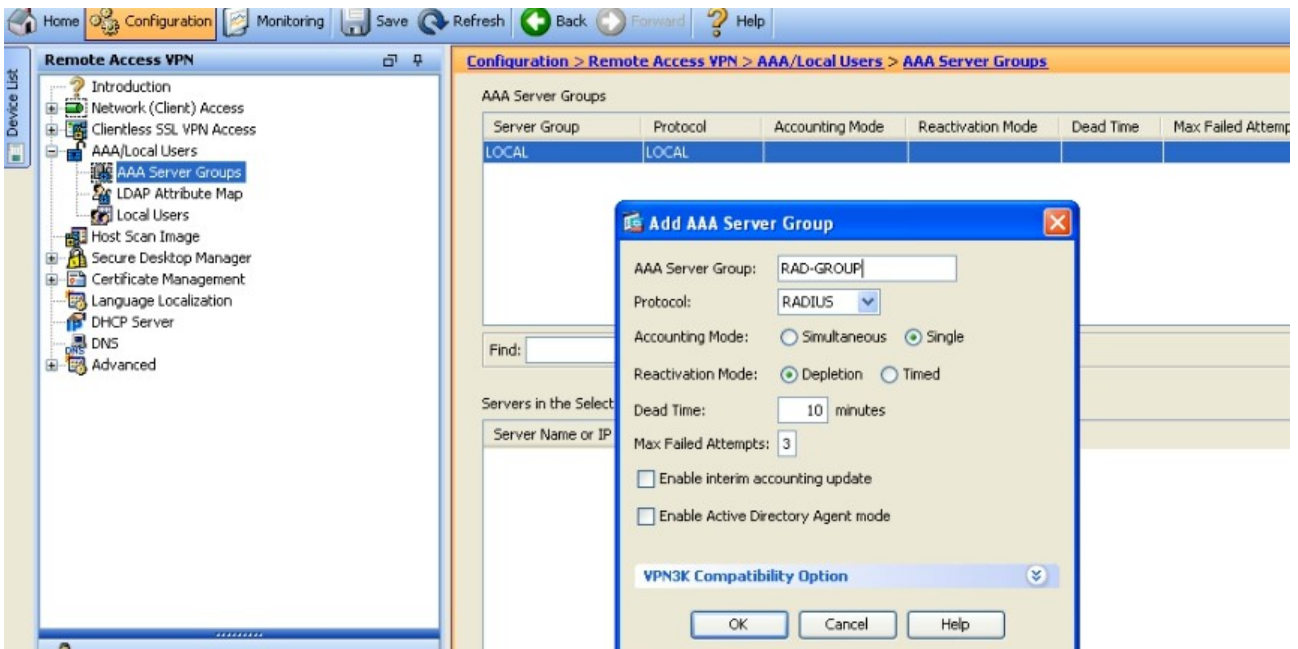
The ASA is a "client" to the ACS AAA server



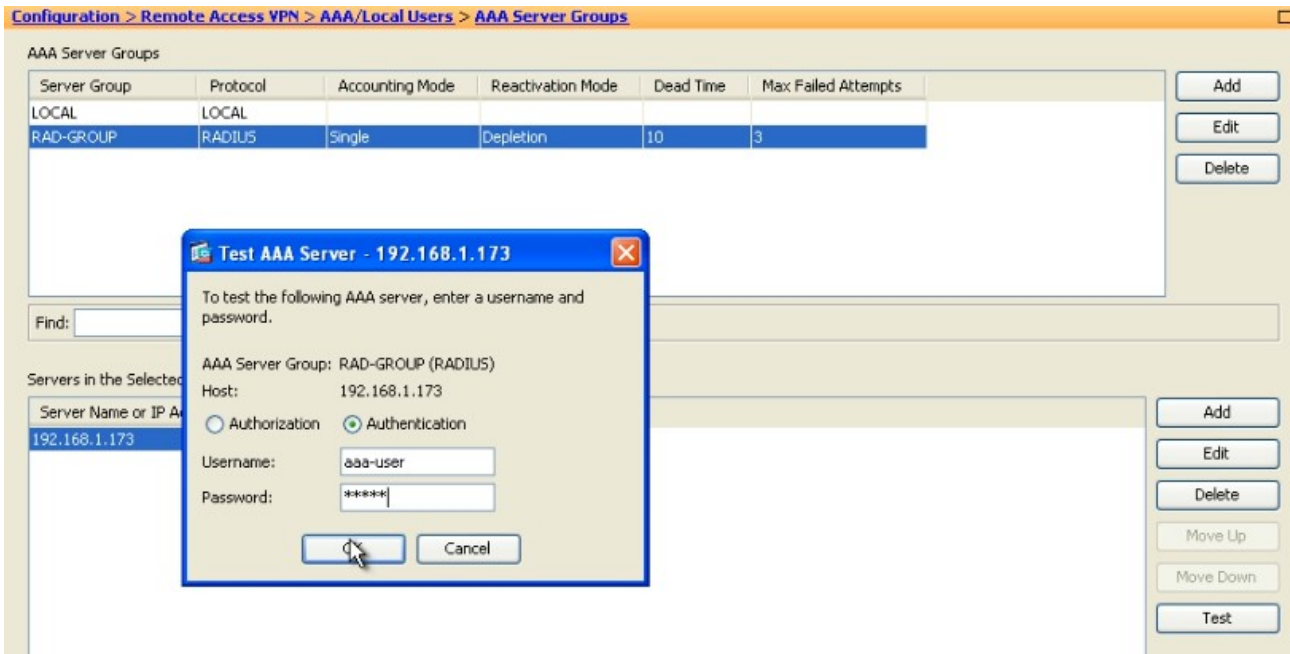
- LOCAL vs Centralized
 Set up the ASA to use RADIUS
 Using the AAA Server

Conn.
 ↑

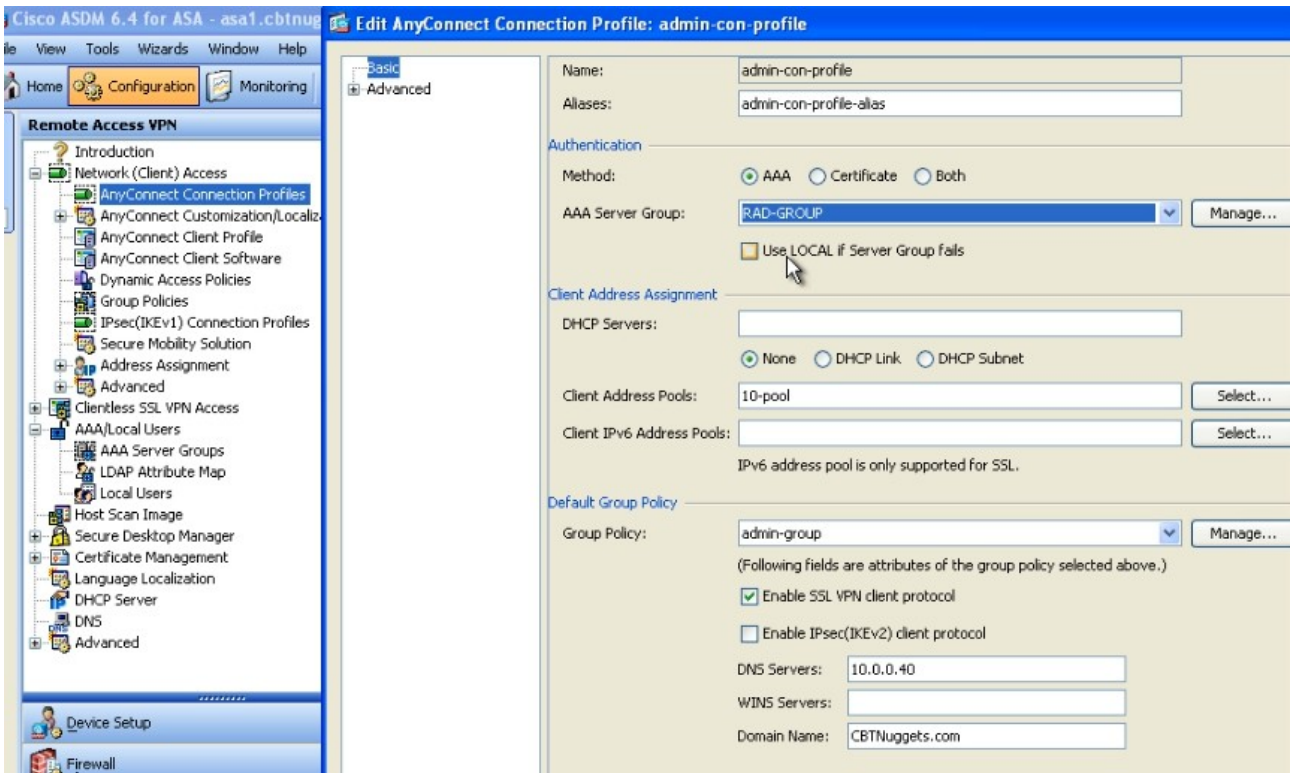




Good to do a test once server is configured.



```
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.

Configuration > Remote Access VPN > AAA/Local Users > Local Users

Create entries in the ASA local user database.
 Command authorization must be enabled in order for the user account privileges to be enforced. To enable command authorization, go to [Authorization](#).
 AAA authentication console commands must be enabled in order for certain access restrictions to be enforced. To enable AAA authentication command go to Authentication.

Username	Privilege Level (Role)	Access Restrictions	VPN Group Policy	VPN Group Lock
sales-user	2	No ASDM/CLI	Sales-Group	sales-con-profile
bob1	2	Full	GroupPolicy1	-- Inherit Group Policy --
admin-user	15	Full	admin-group	-- Inherit Group Policy --
ipsec-user	0	No ASDM/CLI	ipsec-group	-- Inherit Group Policy --
enable_15	15	Full	N/A	N/A



Multi-Factor Auth.

1. KNOWS ←
2. IS ←
- BOB 3. HAVE ←

ASA can be a facilitator of Multi Factor authentication:

e.g. Safenet tokens that are provisioned 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)

Configuration > Remote Access VPN > AAA/Local Users > Local Users

Create entries in the ASA local user database.
 Command authorization must be enabled in order for the user account privileges to be enforced. To enable command authorization, go to [Authorization](#).
 AAA authentication console commands must be enabled in order for certain access restrictions to be enforced. To enable AAA authentication command go to Authentication.

Username	Privilege Level (Role)	Access Restrictions	VPN Group Policy	VPN Group Lock
sales-user	2	No ASDM/CLI	Sales-Group	sales-con-profile
bob1	2	Full	GroupPolicy1	-- Inherit Group Policy --
admin-user	15	Full	admin-group	-- Inherit Group Policy --
ipsec-user	0	No ASDM/CLI	ipsec-group	-- Inherit Group Policy --
enable_15	15	Full	N/A	N/A

Edit Clientless SSL VPN Connection Profile: sales-con-profile

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

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 E Edit D 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 configuration of the ASA. To not send the commands and continue in the configuration mode, click Send. To not send the commands and continue in the configuration mode, click Send.

```
tunnel-group sales-con-profile general-attributes  
secondary-authentication-server-group RAD-GROUP
```

Address <https://asa1.cbttuggets.com/+CSCOE+/logon.html?reason=12&msg=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 Authentication
 - 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 Authentication
 - Authorization
 - Accounting
 - Group Alias/Group URL

Server Group: RAD-GROUP Manage...