3.2 SSL-Based VPN Configuration on Cisco ASA

SSL Based is the newest VPN type on ASA firewalls. It is used only for Remote Access implementations and provides flexibility and lower administration overhead since no IPSEC Client software is required to be installed manually on user's computers.

3.2.1 Anyconnect SSL Web VPN

The Anyconnect SSL VPN implementation is the most powerful option since it provides full network access to remote users. This is similar with the IPSEC VPN client software which also provides full network access remotely. The newest Anyconnect product from Cisco is called now "**Cisco Anyconnect Secure Mobility Client**". From Anyconnect Client version 3.x and above both SSL and IKEv2/IPSEC protocols are supported.

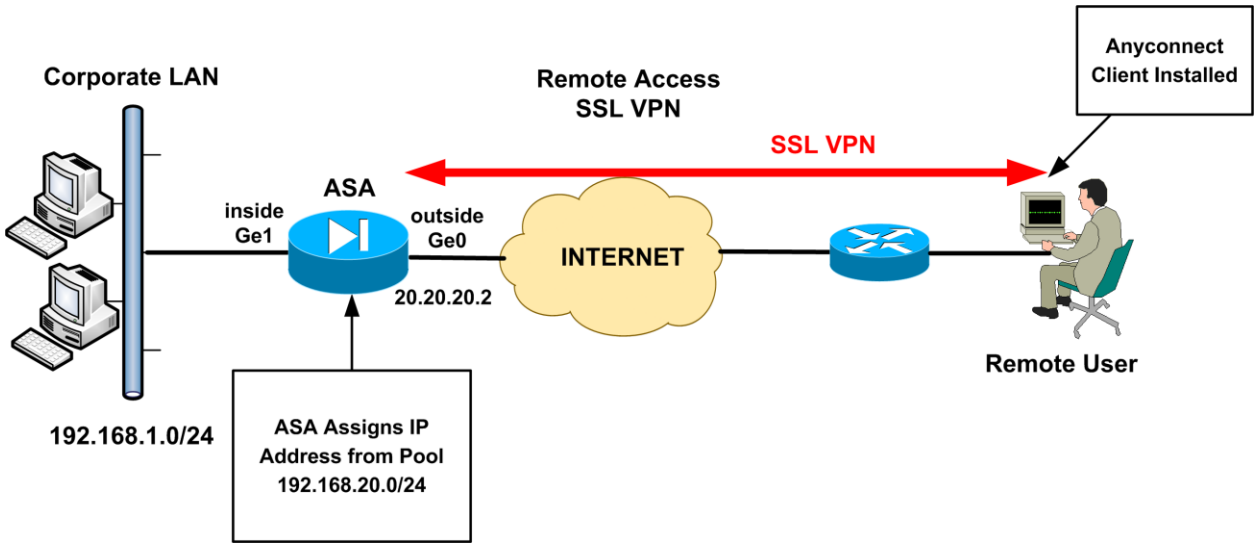
There are two Initial Installation options for AnyConnect client:

- Using clientless WebVPN portal.
- Manual installation by the user or administrator

Using the clientless Web portal, the user first connects and authenticates securely to the ASA with a web browser and the Java Anyconnect client is automatically downloaded and installed on the user's computer (the user can also click the "AnyConnect" Tab on the WebVPN portal to download the client). This necessitates that the Java client (**.pkg extension**) must be already stored on the ASA flash memory by the administrator. After the Anyconnect client is downloaded and installed upon the first connection, the user from now on can start the Anyconnect client directly from his/her computer and connect remotely without using a web browser. This is the preferred method in my opinion because it automates the distribution of the client to the remote users.

With the manual installation method, the network administrator must download the appropriate Anyconnect client software (Microsoft package or one of the other OS versions) from Cisco site and provide the file to the users for manual installation on their laptop. With this method, the user does not need to log in via clientless mode to start the SSL VPN tunnel. Instead, the users can start up the AnyConnect client manually from their desktop and provide their authentication credentials.

Let's see how to configure a Cisco ASA for Anyconnect SSL VPN based on the diagram below.



ASA:

- **STEP 1: Copy Anyconnect Software to ASA Flash**

As we've said before, we need to transfer the Anyconnect package file to the flash of the ASA. First you need to download one of the **.pkg** files from Cisco website. An example Windows client file has the format "**anyconnect-win-x.x.xxxx-k9.pkg**".

To copy the PKG file to ASA flash:
ASA# copy {tftp|ftp|scp}://*[ip address]/anyconnect-win-x.x.xxxx-k9.pkg* **disk0:**

Assume we have downloaded the Anyconnect client file on our computer with IP address 192.168.1.1. We will use a TFTP server on our PC to transfer the file to ASA.

ASA# copy tftp://192.168.1.1/anyconnect-win-2.4.1012-k9.pkg disk0:

Address or name of remote host [192.168.1.1]?

Source filename [anyconnect-win-2.4.1012-k9.pkg]?

Destination filename [anyconnect-win-2.4.1012-k9.pkg]?

Accessing tftp://192.168.1.1/anyconnect-win-2.4.1012-k9.pkg...!!!!!!

- **STEP 2: Tell the ASA where to find the Anyconnect software on Flash**

Then we need to identify the PKG image file on flash by telling the ASA where the image file is located. Also, enable the webvpn Anyconnect service on the outside ASA interface.

ASA# configure terminal
ASA(config)# webvpn
ASA(config-webvpn)# anyconnect image disk0:/anyconnect-win-2.4.1012-k9.pkg 1
ASA(config-webvpn)# enable outside ← enable ssl webvpn on outside interface
ASA(config-webvpn)# anyconnect enable ← enable anyconnect service
ASA(config-webvpn)# exit

Note: The number **1** at the end of the package file is the file order. It is used when you have more than one images stored on the ASA flash (e.g Anyconnect client images for Windows and MAC).

- **STEP 3: Configure VPN Pool to assign IP addresses**

Create an IP address pool from which the ASA will assign addresses to remote users. From the diagram above we see that after the remote user gets authenticated, the ASA assigns an IP address to the remote user from a predefined pool 192.168.20.0/24

ASA(config)# ip local pool vpnpool 192.168.20.1-192.168.20.254 mask 255.255.255.0

- **STEP 4: Configure NAT Exemption**

Create a NAT exemption for traffic between the corporate LAN network behind the ASA (192.168.1.0/24) and the remote user's address pool (192.168.20.0/24).

ASA(config)# object network obj-local
ASA(config-network-object)# subnet 192.168.1.0 255.255.255.0
ASA(config-network-object)# exit

ASA(config)# object network obj-vpnpool
ASA(config-network-object)# subnet 192.168.20.0 255.255.255.0
ASA(config-network-object)# exit

ASA(config)# nat (inside,outside) source static obj-local obj-local destination static obj-vpnpool obj-vpnpool no-proxy-arp route-lookup

- **STEP 5: Configure Split-Tunneling (Optional)**

Similar with the IPSEC VPN client configuration, if you want to allow users to access the Internet and also access the Corporate LAN network at the same time, you must configure a Split-Tunnel Access Control List.

ASA(config)# access-list split-tunnel standard permit 192.168.1.0 255.255.255.0

Traffic from the remote users towards the network specified in the split-tunnel ACL (192.168.1.0/24) will pass through the SSL VPN tunnel. All other traffic from the remote user will go to the Internet.

- **STEP 6: Configure VPN Group Policy**

Create a Group Policy for the AnyConnect WebVPN users. The Group Policy allows you to separate different remote access users into groups with different attributes. The Group Policy attributes that can be configured include DNS server addresses, split-tunneling settings, how the client will be downloaded (automatically or after prompting the user), if the client software will remain permanently on the user's computer etc.

The command format is as following:

ASA(config)# group-policy *"policy name"* **internal**
ASA(config)# group-policy *"policy name"* **attributes**
ASA(config-group-policy)# vpn-tunnel-protocol {[ikev1] [ikev2][l2tp-ipsec][ssl-client]}
ASA(config-group-policy)# split-tunnel-policy {tunnelspecified | tunnelall}
ASA(config-group-policy)# split-tunnel-network-list value *"acl-for-split-tunnel"*
ASA(config-group-policy)# webvpn
ASA(config-group-webvpn)# anyconnect keep-installer {installed | none}
ASA(config-group-webvpn)# anyconnect ask {none | enable [default {webvpn | anyconnect} timeout *value*]}

Let's clarify some of the Group Policy commands shown above:

vpn-tunnel-protocol {[ikev1] [ikev2][l2tp-ipsec][ssl-client]} ← **Select the type of VPN tunnel protocol. For SSL VPN you must select "ssl-client"**

split-tunnel-policy {tunnelspecified | tunnelall} ← **Specify whether only selected traffic will pass through the tunnel ("tunnelspecified") or whether ALL remote traffic will pass through the tunnel ("tunnelall").**
split-tunnel-network-list value *"acl-for-split-tunnel"* ← **Specify the Access List for split-tunnel (see Step 5 above)**

anyconnect keep-installer {installed | none} ← **"installed" means that the client remains installed permanently on the user's computer even after disconnection. The default is that the client gets uninstalled after the user disconnects from the Anyconnect session.**

anyconnect ask {none | enable [default {webvpn | anyconnect } timeout *value*]} ← **This command has to do with how AnyConnect client will be downloaded to user's computer.**

- anyconnect ask none default webvpn ← The ASA immediately displays the WebPortal. This is the default configuration.
- anyconnect ask none default anyconnect ← Download the AnyConnect client automatically.
- anyconnect ask enable default anyconnect timeout 20 ← The user will get a prompt to install the AnyConnect client. If nothing is done within 20 seconds, the client will be downloaded and installed automatically.

anyconnect dpd-interval {[gateway {*seconds* | none*}]* | [client {*seconds* | none*}]*} ← **This enables Dead Peer Detection (DPD) mechanism which ensures that the ASA (gateway) or the client can quickly detect a condition where the peer is not responding and the connection has failed.**

Let's see the actual configuration commands of group-policy for our specific scenario:

EXAMPLE:

ASA(config)# group-policy SSLVPNpolicy internal

ASA(config)# group-policy SSLVPNpolicy attributes

ASA(config-group-policy)# vpn-tunnel-protocol ssl-client

ASA(config-group-policy)# split-tunnel-policy tunnelspecified

ASA(config-group-policy)# split-tunnel-network-list value split-tunnel

ASA(config-group-policy)# webvpn

ASA(config-group-webvpn)# anyconnect keep-installer installed

ASA(config-group-webvpn)# anyconnect ask enable default anyconnect timeout 10

ASA(config-group-webvpn)# anyconnect dpd-interval client 20 ← The client will check for Dead Peer Detection every 20 seconds.

- **STEP 7: Configure a Tunnel Group**

Create a Tunnel Group. The tunnel group must incorporate the Group Policy configured above. It also binds the Group Policy with the IP address pool that we have already configured for remote users.

The command format is as following:

ASA(config)# tunnel-group *"tunnel name"* **type remote-access**

ASA(config)# tunnel-group *"tunnel name"* **general-attributes**

ASA(config-tunnel-general)# default-group-policy *"group policy name"* **←Assign the Group Policy configured in Step6 above.**

ASA(config-tunnel-general)# address-pool *"IP Pool for VPN"* **← Assign the IP address pool configured in Step3 above.**

ASA(config-tunnel-general)# exit

ASA(config)# tunnel-group *"tunnel name"* **webvpn-attributes**

ASA(config-tunnel-webvpn)# group-alias "*group_name_alias"* **enable ← Create an alias name for the tunnel group which will be listed on the log-in screen of the Anyconnect client.**

ASA(config-tunnel-webvpn)# exit

ASA(config)# webvpn

ASA(config-webvpn)# tunnel-group-list enable ← Enable the listing of the alias name on the log-in screen of the AnyConnect client.

Let's see the actual configuration commands of tunnel-group for our specific scenario:

EXAMPLE:

ASA(config)# tunnel-group SSLVPNprofile type remote-access
ASA(config)# tunnel-group SSLVPNprofile general-attributes
ASA(config-tunnel-general)# default-group-policy SSLVPNpolicy
ASA(config-tunnel-general)# address-pool vpnpool
ASA(config-tunnel-general)# exit
ASA(config)# tunnel-group SSLVPNprofile webvpn-attributes
ASA(config-tunnel-webvpn)# group-alias SSL_USERS enable ← This name will be shown to the log-in screen of Anyconnect.
ASA(config-tunnel-webvpn)# exit
ASA(config)# webvpn
ASA(config-webvpn)# tunnel-group-list enable ← Allow users to select which tunnel group to connect (useful if you have multiple tunnel groups)

- **STEP 8: Configure Local User(s) for Authentication**

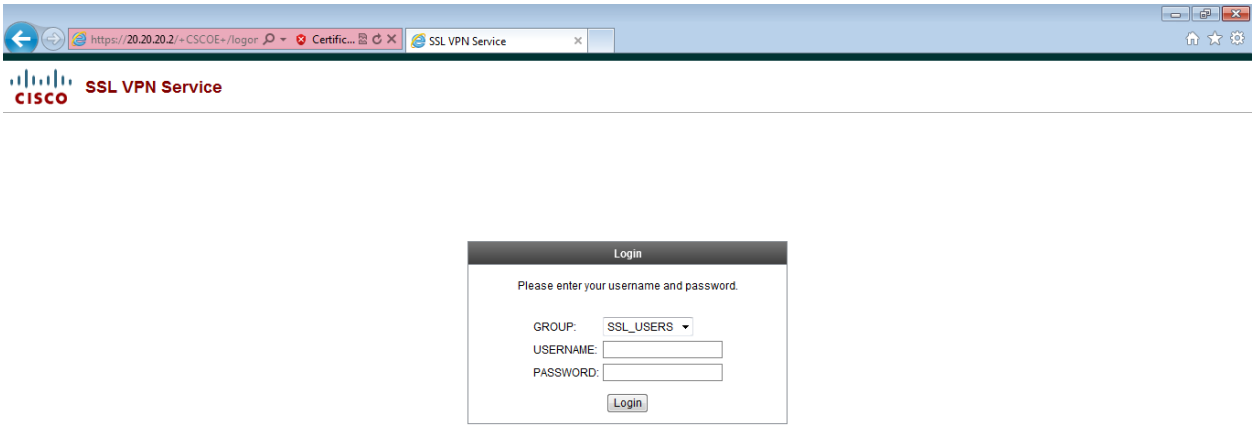
Create a local user on ASA which will be used for AnyConnect authentication. This user will be allowed to have remote network access.

ASA(config)# username sslvpnuser password test123
ASA(config)# username sslvpnuser attributes ← OPTIONAL
ASA(config-username)# service-type remote-access ← OPTIONAL

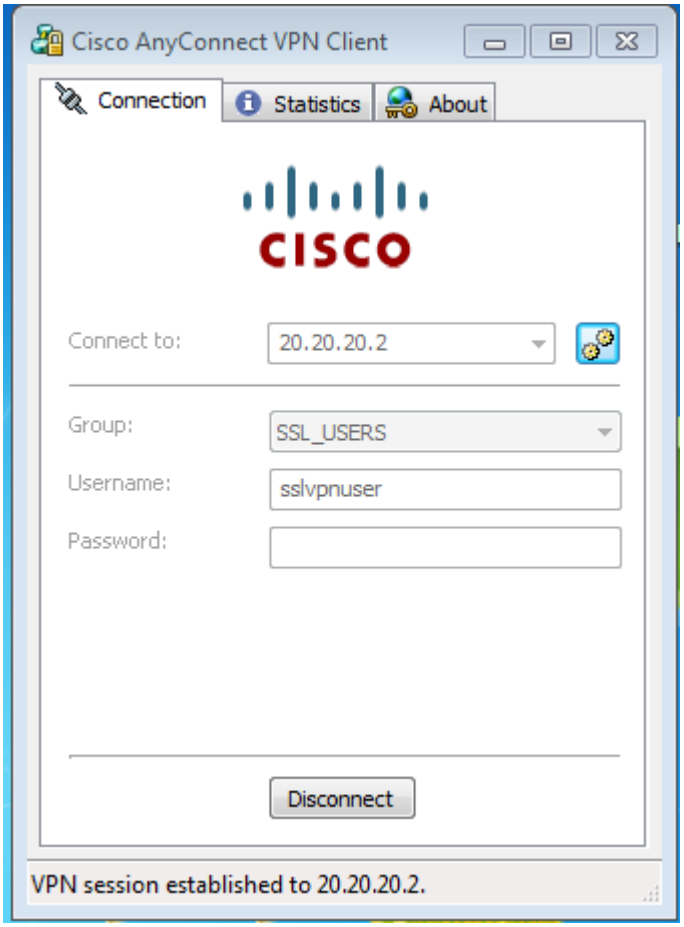
- **STEP 9: Verification**

Let's see some screenshots and ASA log output for verification.

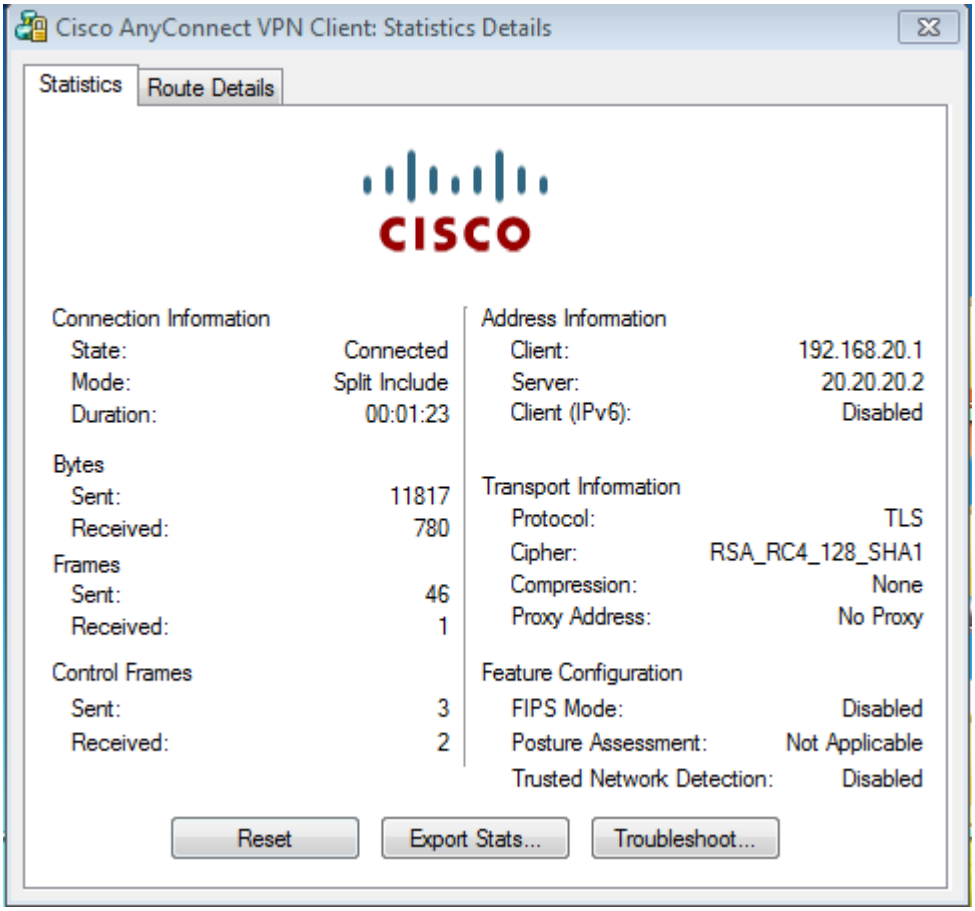
1. Connect to ASA on its public outside address: **https://[outside ASA Address]**
You might have to accept some certificate messages. Then, you will get the following log-in screen:



2. Enter your username and password (sslvpnuser). Also, choose your respective group from the drop down list as shown. Note that the group name in the drop down is the group-alias name configured in Step7 (**SSL_USERS**). After successful authentication you can see that a VPN Session is established with 20.20.20.2 (Public IP of ASA).



3. Clicking on the “Statistics” Tab you can see various important stats and parameters as shown below:



The statistics tab above shows that the Anyconnect remote user received an IP address 192.168.20.1 from the ASA.

4. Let's see also some output from the ASA:

ASA# show webvpn anyconnect

```
1. disk0:/anyconnect-win-2.4.1012-k9.pkg 1 dyn-regex=/Windows NT/
 CISCO STC win2k+
 2,4,1012
 Thu 12/17/2009 15:47:55.45

1 AnyConnect Client(s) installed
```

ASA# show ip local pool vpnpool

```
Begin        End          Mask          Free    Held    In use
192.168.20.1   192.168.20.254  255.255.255.0    253      0      1

In Use Addresses:
192.168.20.1
```

The above verifies that there is one Anyconnect user connected who received an IP 192.168.20.1

You can find a complete configuration of the scenario above in Chapter 4, Section 4.2.9.

3.3 VPN Authentication using External Server

In all of our scenarios we have seen so far, the authentication of remote access users was implemented using local device username/password credentials. That is, local user credentials were created on the device (ASA or Router) which were used to authenticate remote access users (either for IPSEC VPN or for Anyconnect SSL VPN). However, if you have a large number of remote users, it's not manageable to create local device credentials for all of them. The best option for such a case is to use an external authentication server which will hold all remote users' credentials for authentication. We will see three popular options for External Server authentication: Using **Microsoft Active Directory**, using a **AAA Radius/Tacacs** server (such as as the Cisco Secure ACS Server), and finally using an **RSA Server** for two-factor authentication.

3.3.1 VPN Authentication using Microsoft Active Directory

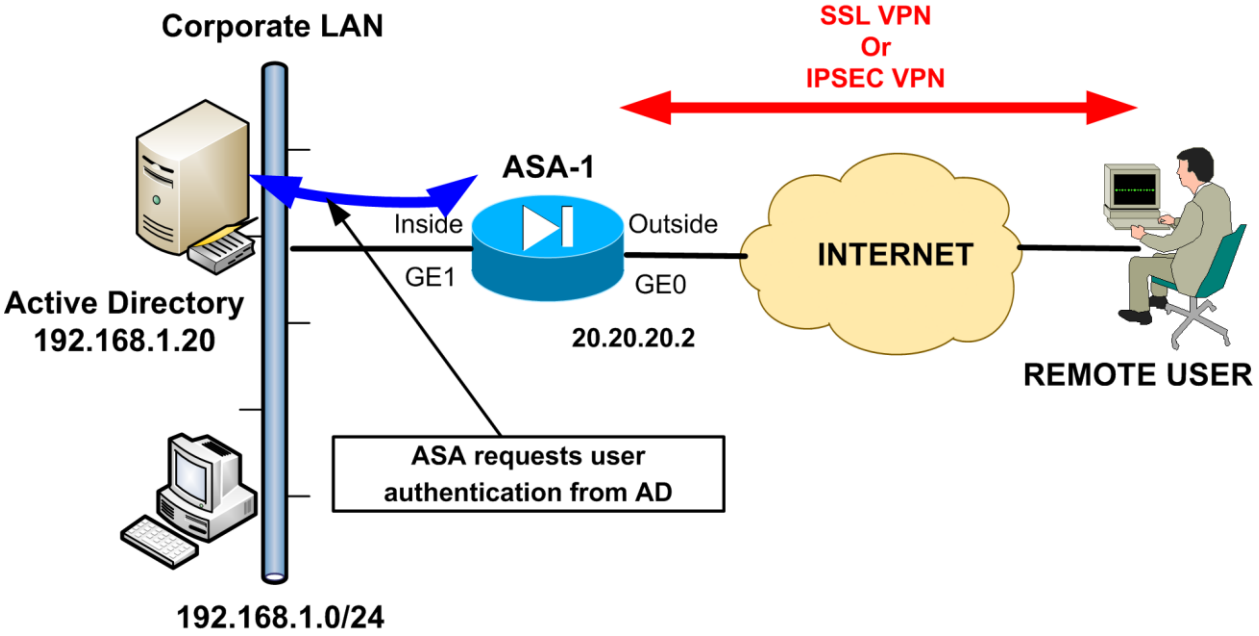
In this section we will describe how to implement user VPN authentication on ASA devices via a Microsoft Active Directory. This is very useful in cases where there are a large number of remote users who require VPN access to network resources via an ASA firewall, and these users already have Active Directory accounts. Therefore, administrators won't need to create and maintain extra account credentials on the ASA device.

With the addition of LDAP support on Cisco ASA firewalls, it is possible now to use a Microsoft Active Directory (AD) server to authenticate remote access users. As we know, AD supports the LDAP protocol.

There are two general steps to configure AD authentication of remote access users on Cisco ASA:

1. First configure a AAA server group which will be using the LDAP protocol. Under this group, define the parameters of the Active Directory server (IP address, distinguished names, AD login username/password etc).
2. After proper configuration of the AAA server group above, assign this group to the desired connection profile ("**Tunnel Group**") of the remote access users.

Let's see the steps above in more details. We will be using the network diagram below:



Assume we have remote access users which are connected either via the traditional IPSEC VPN client or via the Anyconnect SSL VPN method. An internal Active Directory Server (192.168.1.20) will be used by the ASA device to send the authentication requests from remote users.

- **STEP 1: Configure AAA Server Group and LDAP parameters**

ASA-1(config)# aaa-server AD-SERVER protocol ldap← The name "AD-SERVER" will be used later under a Tunnel Group profile. This server uses the "ldap" protocol.
ASA-1(config-aaa-server-group)# exit
ASA-1(config)# aaa-server AD-SERVER (inside) host 192.168.1.20 ← The specific "AD-SERVER" is reachable via the "inside" interface on IP 192.168.1.20
ASA-1(config-aaa-server-host)# server-type microsoft ← This AAA server is "Microsoft"
ASA-1(config-aaa-server-host)# ldap-base-dn dc=mycompany, dc=com← See below
ASA-1(config-aaa-server-host)# ldap-login-dn cn=admin, cn=users, dc=mycompany, dc=com← See below

ASA-1(config-aaa-server-host)# ldap-login-password *cisco123*← See below
ASA-1(config-aaa-server-host)# ldap-naming-attribute sAMAccountName← See below
ASA-1(config-aaa-server-host)# ldap-scope subtree← See below

The configuration parameters in red above are explained below:

- **ldap-base-dn** : Specifies the location in the LDAP hierarchy where the server should begin searching when it receives an authentication request from ASA.
- **ldap-login-dn** : Specifies the Distinguished Name (DN) for the admin account or any account on the Active Directory which has the privileges to login, search and retrieve account information from the AD. Here we used the username "**admin**" as an example. You must use a proper username which has enough privileges to be able to search/read/lookup users in the LDAP server.
- **ldap-login-password** : Specifies the password of the "admin" account used in "ldap-login-dn" parameter above.
- **ldap-naming-attribute** : Specifies the Relative Distinguished Name (DN) attribute that uniquely identifies an entry on the LDAP server. **sAMAccountName** is the default attribute in the Microsoft Active Directory.
- **ldap-scope** : This specifies whether ASA will look at the base DN level or go below the Base DN level to search for the user accounts. In our case we want to go below the Base DN level, so we use the "**subtree**" value.

The above concludes the mandatory configuration parameters required for properly specifying an Active Directory (LDAP) server to be used by the ASA for user authentication. Next we will see how

to apply the AAA Server Group above to a VPN connection profile (Tunnel-Group) in order to be used for authentication.

- **STEP 2: Assign the above AAA Server Group to a VPN Tunnel-Group**

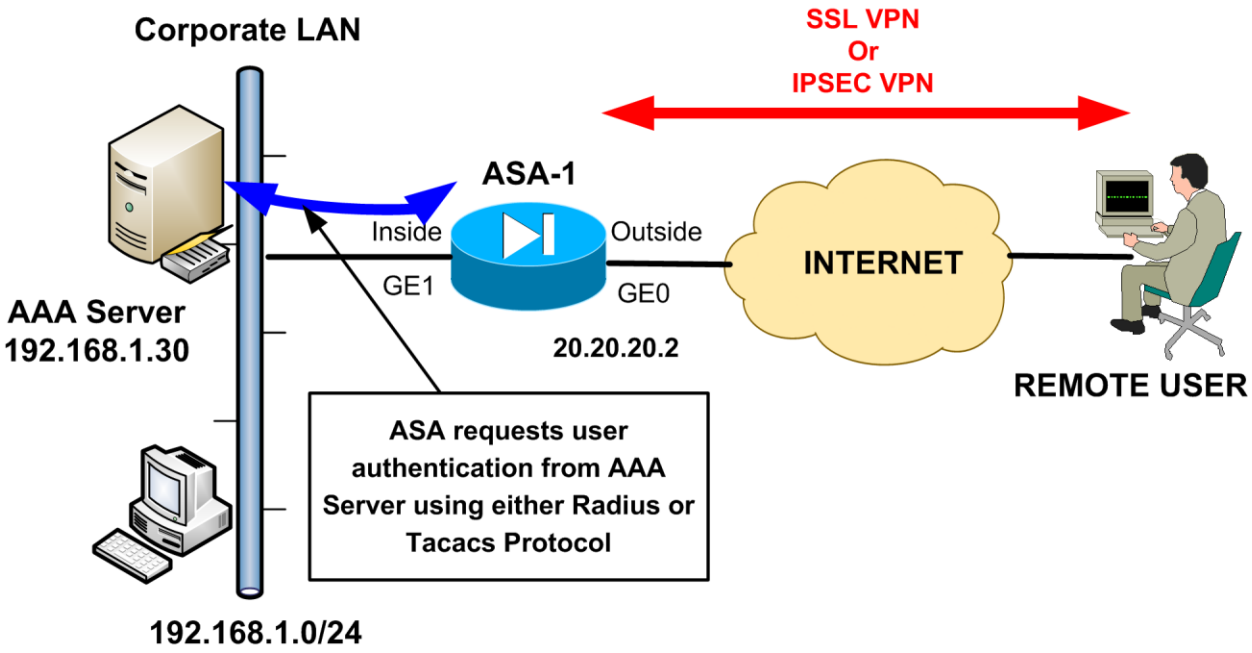
When we discussed the remote access scenarios for both IPSEC VPN and Anyconnect VPN (sections 3.1.4 and 3.2.1) we have seen that one of the required elements to configure is a "**tunnel-group**". In order to use the AAA Server Group configured above for authentication via AD, we must assign it under the Tunnel-Group profile.

ASA-1(config)# tunnel-group remotevpn type remote-access
ASA-1(config)# tunnel-group remotevpn general-attributes
ASA-1(config-tunnel-general)# authentication-server-group AD-SERVER ← Assign the AAA Server Group from Step 1 above. Anyone using the "remotevpn" group for remote access, will be authenticated via the "AD-SERVER" using Active Directory.

3.3.2 VPN Authentication using RADIUS or TACACS

Another popular method for authentication of remote VPN users is with an external AAA Server which uses the RADIUS or TACACS protocol. For example, the Cisco Secure Access Control System (CS-ACS) supports both RADIUS and TACACS+ protocols, so you can use it in conjunction with a Cisco ASA to authenticate remote access VPN users. Furthermore, the Cisco ACS server can communicate with a two-factor authentication server (such as RSA) to provide two-factor authentication of remote access VPN users (e.g providing One-Time-Passwords with a token), as we will see later.

The general configuration steps are the same as with Active Directory above. You need to define a AAA Server Group and then attach it to a VPN connection profile ("Tunnel Group"). Let's see the configuration steps based on the diagram below:



- **STEP 1: Configure AAA Server Group**

ASA-1(config)# aaa-server AAA-SERVER protocol [radius|tacacs+] ← **The name "AAA-SERVER" will be used later under a Tunnel Group profile. This server will use either "radius" or "tacacs+" protocol.**
ASA-1(config-aaa-server-group)# exit
ASA-1(config)# aaa-server AAA-SERVER (inside) host 192.168.1.30 ← **The specific "AAA-SERVER" is reachable via the "inside" interface on IP 192.168.1.30**
ASA-1(config-aaa-server-host)# key *strongkey* ← **Authentication password between ASA and External AAA Server**

- **STEP 2: Assign the above AAA Server Group to a VPN Tunnel-Group**

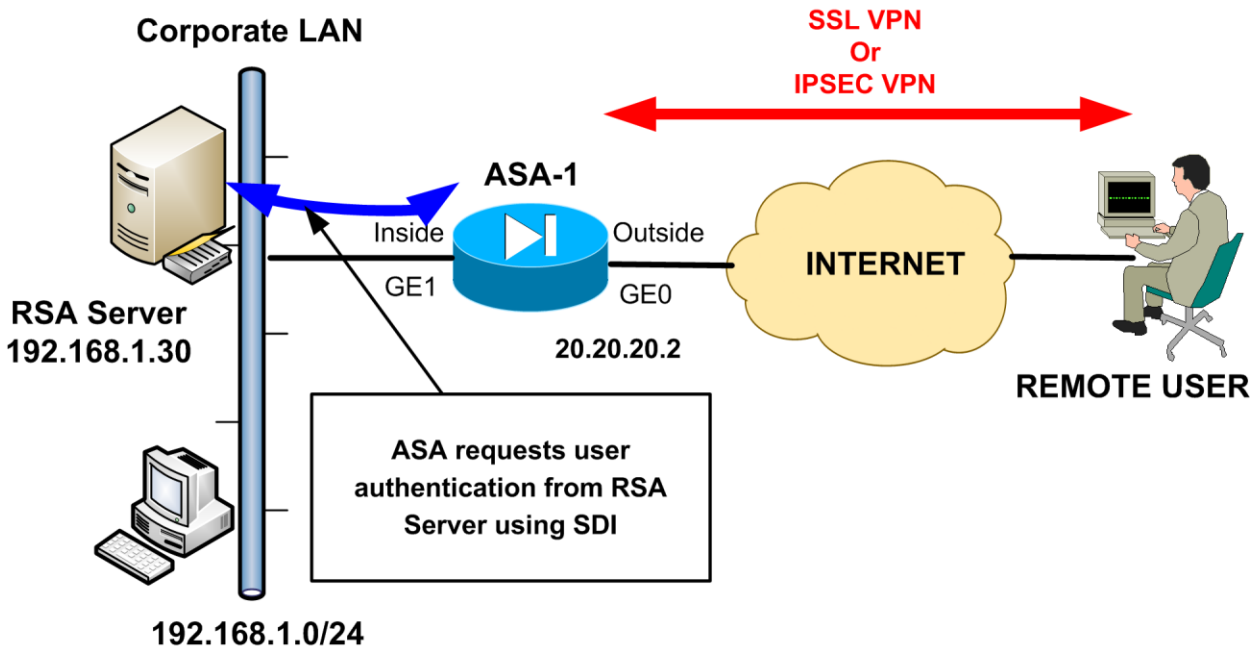
ASA-1(config)# tunnel-group remotevpn type remote-access
ASA-1(config)# tunnel-group remotevpn general-attributes
ASA-1(config-tunnel-general)# authentication-server-group AAA-SERVER ← **Assign the AAA Server Group from Step 1 above. Anyone using the "remotevpn" group for remote access, will be authenticated via the "AAA-SERVER".**

3.3.3 VPN Authentication using RSA

RSA is popular for providing two-factor authentication for remote access users. Using either a hardware or software token on the user side, the RSA server can issue One-Time Passwords to remote users. It's not in the scope of this book to describe the details of configuring the RSA server itself. However, we will see the configuration on the ASA to communicate with an RSA server for authentication.

There are two authentication options to use with ASA and RSA.

1. ASA communicates with a RADIUS server (usually a Cisco Secure ACS Server) for authentication (just like Section 3.3.2 above) and the RADIUS communicates with the RSA server for One-Time Passwords.
2. ASA communicates with RSA Server directly. This is what we will see below.



- **STEP 1: Configure AAA Server Group**

ASA-1(config)# aaa-server RSA-SERVER protocol sdi ← Use "SDI" as protocol
ASA-1(config-aaa-server-group)# exit
ASA-1(config)# aaa-server RSA-SERVER (inside) host 192.168.1.30 ← The specific "RSA-SERVER" is reachable via the "inside" interface on IP 192.168.1.30