ASA 8.0: Configure LDAP Authentication for WebVPN Users

Contents

Introduction
Prerequisites
Background Information
Configure LDAP Authentication
ASDM
Command Line Interface
Perform Multi-Domain Searches (Optional)
Verify
Test with ASDM
Test with CLI
Troubleshoot
Related Information

Introduction

This document demonstrates how to configure the Cisco Adaptive Security Appliance (ASA) to use an LDAP server for authentication of WebVPN users. The LDAP server in this example is Microsoft Active Directory. This configuration is performed with Adaptive Security Device Manager (ASDM) 6.0(2) on an ASA that runs software version 8.0(2).

Note: In this example Lightweight Directory Access Protocol (LDAP) authentication is configured for WebVPN users, but this configuration can be used for all other types of remote access clients as well. Simply assign the AAA server group to the desired connection profile (tunnel group), as shown.

Prerequisites

A basic VPN configuration is required. In this example WebVPN is used.

Background Information

In this example, the ASA checks with an LDAP server in order to verify the identity of users that it authenticates. This process does not work like a traditional Remote Authentication Dial-In User Service (RADIUS) or Terminal Access Controller Access-Control System Plus (TACACS+) exchange. These steps explain, at a high level, how the ASA uses an LDAP server in order to check user credentials.
1. The user initiates a connection to the ASA.
2. The ASA is configured to authenticate that user with the Microsoft Active Directory (AD)/LDAP server.
3. The ASA binds to the LDAP server with the credentials configured on the ASA (admin in this case), and looks up the provided username. The admin user also obtains the appropriate credentials to list contents within Active Directory. Refer to [http://support.microsoft.com/?id=320528](http://support.microsoft.com/?id=320528) for more information about how to grant LDAP query privileges. **Note:** The Microsoft website at [http://support.microsoft.com/?id=320528](http://support.microsoft.com/?id=320528) is managed by a third party provider. Cisco is not responsible for its content.
4. If the username is found, the ASA attempts to bind to the LDAP server with the credentials that the user provided at login.
5. If the second bind is successful, authentication succeeds and the ASA processes the attributes of the user. **Note:** In this example the attributes are not used for anything. Refer to [ASA/PIX: Mapping VPN Clients to VPN Group Policies Through LDAP Configuration Example](http://www.cisco.com/c/dam/en/us/td/docs/security/asa/asa/ldap/concepts/asa_ldap_concepts.html) in order to see an example of how the ASA can process LDAP attributes.

**Configure LDAP Authentication**

In this section, you are presented with the information to configure the ASA to use an LDAP server for the authentication of WebVPN clients.

**ASDM**

Complete these steps in the ASDM in order to configure the ASA to communicate with the LDAP server and authenticate WebVPN clients.

2. Click **Add** next to AAA Server Groups.
3. Specify a name for the new AAA Server group, and choose **LDAP** as the protocol.
4. Be sure that your new group is selected in the top pane, and click **Add** next to the **Servers** in
5. Provide the configuration information for your LDAP server. The subsequent screenshot illustrates an example configuration. This is an explanation of many of the configuration options:

- **Interface Name**—the interface that the ASA uses in order to reach the LDAP server
- **Server Name or IP address**—the address that the ASA uses in order to reach the LDAP server
- **Server Type**—the type of LDAP server, such as Microsoft
- **Base DN**—the location in the LDAP hierarchy where the server must begin to search
- **Scope**—the extent of the search in the LDAP hierarchy that the server must make
- **Naming Attribute**—the Relative Distinguished Name attribute (or attributes) that uniquely identifies an entry on the LDAP server. **sAMAccountName** is the default attribute in the Microsoft Active Directory. Other commonly used attributes are **CN**, **UID**, and **userPrincipalName**.
- **Login DN**—the DN with enough privileges in order to be able to search/read/lookup users in the LDAP server
- **Login Password**—the password for the DN account
- **LDAP Attribute Map**—an LDAP attribute map to be used with responses from this server. Refer to [ASA/PIX: Mapping VPN Clients to VPN Group Policies Through LDAP Configuration Example](#) for more information on how to configure LDAP attribute
6. Once you have configured the AAA server group and added a server to it, it is necessary to configure your connection profile (tunnel group) to use the new AAA configuration. Navigate to Configuration > Remote Access VPN > Clientless SSL VPN Access > Connection Profiles.  
7. Choose the connection profile (tunnel group) for which you want to configure AAA, and click **Edit**.  
8. Under **Authentication**, choose the LDAP server group that you created earlier.
Complete these steps in the command line interface (CLI) in order to configure the ASA to communicate with the LDAP server and authenticate WebVPN clients.

```bash
ciscoasa#configure terminal
--- Configure the AAA Server group.
ciscoasa(config)#aaa-server LDAP_SRV_GRP protocol ldap
--- Configure the AAA Server.
ciscoasa(config-aaa-server-group)#aaa-server LDAP_SRV_GRP (inside) host 192.168.1.2
ciscoasa(config-aaa-server-host)#ldap-base-dn dc=ftwsecurity, dc=cisco, dc=com
ciscoasa(config-aaa-server-host)#ldap-login-dn cn=admin, cn=users, dc=ftwsecurity, dc=cisco, dc=com
ciscoasa(config-aaa-server-host)#ldap-login-password **********
ciscoasa(config-aaa-server-host)#ldap-naming-attribute sAMAccountName
--- Configure the tunnel group to use the new AAA setup.
ciscoasa(config)#tunnel-group ExampleGroup2
general-att ciscoasa(config-tunnel-general)#authentication-server-group LDAP_SRV_GRP
```

**Perform Multi-Domain Searches (Optional)**

**Optional.** The ASA currently does not support the LDAP referral mechanism for multi-domain searches (Cisco bug ID CSCsj32153). Multi-domain searches are supported with the AD in Global Catalog Server mode. In order to perform multi-domain searches, setup up the AD server for Global Catalog Server mode, usually with the these key parameters for the LDAP server entry in the ASA. The key is to use an ldap-name-attribute that must be unique across the directory tree.

```bash
server-port 3268
ldap-scope subtree
ldap-naming-attribute userPrincipalName
```
Verify

Use this section in order to confirm that your configuration works properly.

Test with ASDM

Verify your LDAP configuration with the **Test** button on the AAA Server Groups configuration screen. Once you supply a username and password, this button allows you to send a test authentication request to the LDAP server.

2. Select your desired AAA Server group in the top pane.
3. Select the AAA server that you want to test in the lower pane.
4. Click the **Test** button to the right of the lower pane.
5. In the window that appears, click the **Authentication** radio button, and supply the credentials with which you want to test. Click **OK** when finished.

6. After the ASA contacts the LDAP server, a success or failure message
Test with CLI

You can use the test command on the command line in order to test your AAA setup. A test request is sent to the AAA server, and the result appears on the command line.

```
ciscoasa# test aaa-server authentication LDAP_SRV_GRP host 192.168.1.2 username kate password cisco123 INFO: Attempting Authentication test to IP address <192.168.1.2> (timeout: 12 seconds) INFO: Authentication Successful
```

Troubleshoot

If unsure of the current DN string to use, you can issue the dsquery command on a Windows Active Directory server from a command prompt in order to verify the appropriate DN String of a user object.

```
C:\Documents and Settings\Administrator>dsquery user -samid kate !--- Queries Active Directory for samid id "kate" "CN=Kate Austen,CN=Users,DC=ftwsecurity,DC=cisco,DC=com"
```

The debug ldap 255 command can help to troubleshoot authentication problems in this scenario. This command enables LDAP debugging and allows you to watch the process that the ASA uses to connect to the LDAP server. This outputs show the ASA connect to the LDAP server as outlined in the Background Information section of this document.

This debug shows a successful authentication:

```
```
attributes from server 192.168.1.2 [7]


This debug shows an authentication that fails due to an incorrect password:


This debug shows an authentication that fails because the user can not be found on the LDAP server:

The debugs show this error message when the connectivity between the ASA and the LDAP authentication server does not work:

```
ciscoasa# debug webvpn 255
INFO: debug webvpn enabled at level 255.
ciscoasa# webvpn_portal.c:ewaFormSubmit_webvpn_login[2162]
ewaFormSubmit_webvpn_login: tgCookie = NULL
ewaFormSubmit_webvpn_login: cookie = 1
ewaFormSubmit_webvpn_login: tgCookieSet = 0
ewaFormSubmit_webvpn_login: tgroup = NULL
....not resuming [2587]
webvpn_portal.c:http_webvpn_kill_cookie[787]
webvpn_auth.c:http_webvpn_pre_authentication[2327]
WebVPN: calling AAA with ewsContext (-847917520) and nh (-851696992)!
webvpn_auth.c:webvpn_add_auth_handle[5118]
WebVPN: started user authentication...
webvpn_auth.c:webvpn_aaa_callback[5158] WebVPN: AAA status = (ERROR)
webvpn_portal.c:ewaFormSubmit_webvpn_login[2162] ewaFormSubmit_webvpn_login: tgCookie = NULL
ewaFormSubmit_webvpn_login: cookie = 1
ewaFormSubmit_webvpn_login: tgCookieSet = 0
ewaFormSubmit_webvpn_login: tgroup = NULL ....resuming [2564]
webvpn_auth.c:http_webvpn_post_authentication[1506] WebVPN: user: (utrcd01) auth error.
```

**Related Information**

- [Technical Support & Documentation - Cisco Systems](#)