Configure LDAP Attribute Mapping on ASA for Secure Client VPN

Contents

Introduction

This document describes configuring LDAP attribute mapping on Cisco ASA to assign VPN group policies based on Active Directory groups.

Requirements

Cisco ASA Requirements

- Cisco ASA running a supported software version.
- Administrative access to the ASA device.

Network Requirements

- Active Directory (AD) domain accessible to the ASA.
- LDAP over SSL (LDAPS) configured on the AD server (default port 636).

Client Requirements

- Secure Client installed on client devices.

Components Used

The information in this document is not restricted to specific software and hardware versions.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Configuration Steps

Step 1. Define Group Policies

Group policies determine the permissions and restrictions for VPN users. Create the necessary group policies that align with the access requirements of your organization.

Create a Group Policy for Authorized Users

```
 group-policy VPN_User_Policy internal
 group-policy VPN_User_Policy attributes
   vpn-simultaneous-logins 3
   split-tunnel-policy tunnelspecified
   split-tunnel-network-list value SPLIT_TUNNEL_ACL
```

Create a Default Group Policy to Deny Access.

```
group-policy No_Access_Policy internal
 group-policy No_Access_Policy attributes
   vpn-simultaneous-logins 0
```

Step 2. Configure the LDAP Attribute Map

The attribute map translates LDAP attributes to ASA attributes, enabling the ASA to assign users to the correct group policy based on their LDAP group memberships.

```
ldap attribute-map VPN_Access_Map
   map-name  memberOf Group-Policy
   map-value memberOf "CN=VPN_Users,OU=Groups,DC=example,DC=com" VPN_User_Policy
```

Note: The distinguished name (DN) of the LDAP group must always be enclosed in double quotes (""). This ensures that the ASA correctly interprets spaces and special characters in the DN.

Step 3. Configure the LDAP AAA Server

Set up the ASA to communicate with the AD server for authentication and group mapping.

```
aaa-server AD_LDAP_Server protocol ldap
aaa-server AD_LDAP_Server (inside) host 192.168.1.10
  ldap-base-dn dc=example,dc=com
  ldap-scope subtree
  ldap-naming-attribute sAMAccountName
  ldap-login-password ********
  ldap-login-dn CN=ldap_bind_user,OU=Service Accounts,DC=example,DC=com
  ldap-over-ssl enable
  ldap-attribute-map VPN_Access_Map
```

Step 4. Define the Tunnel Group

The tunnel group defines the VPN parameters and ties the authentication to the LDAP server.

```
tunnel-group VPN_Tunnel type remote-access
tunnel-group VPN_Tunnel general-attributes
  address-pool VPN_Pool
  authentication-server-group AD_LDAP_Server
  default-group-policy No_Access_Policy

tunnel-group VPN_Tunnel webvpn-attributes
  group-alias VPN_Tunnel enable
```

Note: The default-group-policy is set to No_Access_Policy, denying access to users not matching any LDAP attribute map criteria.

Verify

After completing the setup, verify that users are correctly authenticated and assigned the appropriate group policies.

Verify VPN Session Assignment

```
show vpn-sessiondb anyconnect filter name <username>
```

Replace **<username>** with the actual test account.

Troubleshoot

Use this section to troubleshoot your configuration.

Enable LDAP Debugging

If users are not receiving the expected group policies, enable debugging to identify issues.

```
debug ldap 255
debug aaa common 255
debug aaa shim 255
```

Initiate a VPN Connection

Have a test user attempt to connect using **Cisco Secure Client**.

Review Debug Output

Check the Cisco ASA logs to ensure the user is mapped to the correct group policy based on their Active Directory (AD) group membership.

Disable Debugging After Verification

```
undebug all
```

Common Issues

LDAP attribute mappings are case-sensitive. Ensure that the **AD** group names in the map-value statements match exactly, including case sensitivity.

Verify that users are **direct members** of the specified **AD** groups. Nested group memberships are not always recognized, leading to authorization issues.

Users not matching any map-value criteria receive the default-group-policy (No_Access_Policy in this case), preventing access.