Policy Group Assignment for AnyConnect Clients That Use LDAP on Cisco IOS Headends Configuration Example

Document ID: 118695

Contributed by Atri Basu and Heather Dashnau, Cisco TAC Engineers.
Jan 07, 2015

Contents

Introduction

This document describes how to configure Lightweight Directory Access Protocol (LDAP) attribute maps to automatically assign the correct VPN policy to a user based on their credentials.

Note: Support for LDAP authentication for Secure Sockets Layer VPN (SSL VPN) users that connect to a Cisco IOS® headend is tracked by the Cisco bug ID CSCuj20940. Until support is officially added, LDAP support is the best effort.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- SSL VPN on Cisco IOS
- LDAP authentication on Cisco IOS
- Directory Services

Components Used

The information in this document is based on these software and hardware versions:

- CISCO881−SEC−K9
- Cisco IOS Software, C880 Software (C880DATA−UNIVERSALK9−M), Version 15.1(4)M, RELEASE SOFTWARE (fc1)

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, make sure that you understand the potential impact of any command.

Background Information

The LDAP is an open, vendor−neutral, industry standard application protocol to access and maintain distributed directory information services over an Internet Protocol (IP) network. Directory services play an important role in the development of intranet and Internet applications as they allow the sharing of information about users, systems, networks, services, and applications throughout the network.

Frequently, administrators want to provide VPN users with different access permissions or WebVPN content. This can be completed with the configuration of different VPN policies on the VPN server and assignment of these policy−sets to each user dependent upon their credentials. While this can be completed manually, it is more efficient to automate the process with Directory Services. In order to use LDAP to assign a group policy to a user, you need to configure a map that maps an LDAP attribute such as the Active Directory (AD) attribute "memberOf" to an attribute that is understood by the VPN headend.

On the Adaptive Security Appliance (ASA) this is regularly achieved through the assignment of different group policies to different users with an LDAP attribute map as shown in ASA Use of LDAP Attribute Maps Configuration Example.

On the Cisco IOS the same thing can be achieved with the configuration of different policy groups under the WebVPN context and the use of LDAP attribute maps in order to determine which policy group the user will be assigned. On Cisco IOS headends, the "memberOf" AD attribute is mapped to the Authentication, Authorization, and Accounting (AAA) attribute supplicant−group. For more details on the default attribute mappings, see LDAP on IOS Devices Using Dynamic Attribute Maps Configuration Example. However for SSL VPN, there are two relevant AAA attribute mappings:

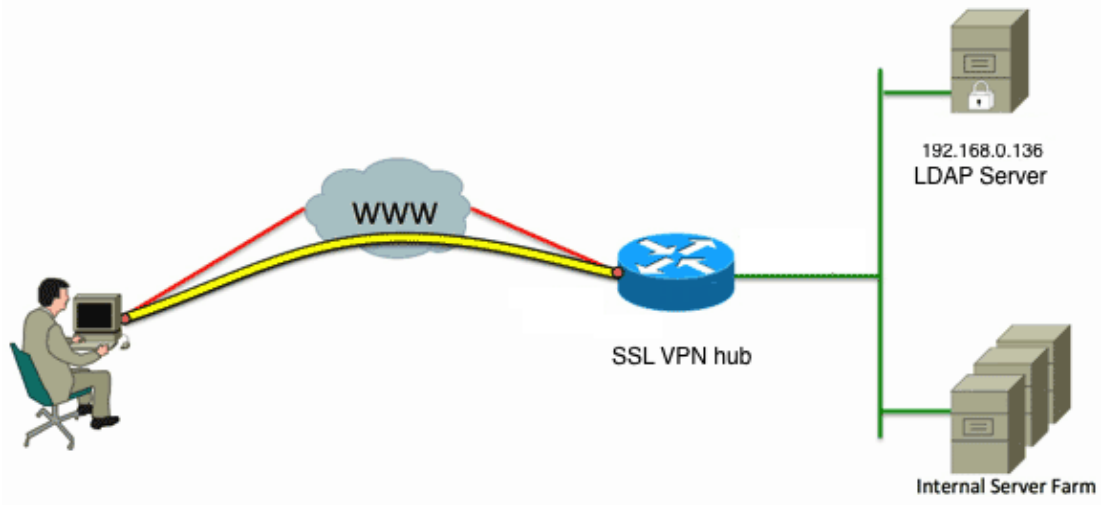
AAA Attribute Name	***SSL VPN Relevance***
user−vpn−group	maps to the policy group defined under the WebVPN context
webvpn−context	maps to the actual WebVPN context itself

Therefore the LDAP attribute map needs to map the relevant LDAP attribute to either one of these two AAA attributes.

Configure

Note: Use the Command Lookup Tool (registered customers only) in order to obtain more information on the commands used in this section.

Network Diagram



This configuration uses an LDAP attribute map in order to map the "memberOf" LDAP attribute to the AAA attribute user−vpn−group.

1. Configure the authentication method and the AAA server group.

```
aaa new-model
!
!
aaa group server ldap AD
 server DC1
!
aaa authentication login default local
aaa authentication login vpn local
aaa authentication login AD group ldap local
aaa authorization exec default local
```

2. Configure an LDAP attribute map.

```
ldap attribute-map ADMAP
 map type memberOf user-vpn-group
```

3. Configure the LDAP server which references the previous LDAP attribute map.

```
ldap server DC1
 ipv4 192.168.0.136
 attribute map ADMAP
 bind authenticate root-dn CN=Cisco Systems,OU=Service Accounts,DC=chillsthrills,
DC=local password 7 <removed>
 base-dn DC=chillsthrills,DC=local
```

4. Configure the router to act as a WebVPN server. In this example, since the "memberOf" attribute will be mapped to the "user−vpn−group" attribute, a single WebVPN context is configured with multiple policy groups which include a "NOACCESS" policy. This policy group is for users who do not have a matching "memberOf" value.

```
ip local pool vpnpool 192.168.200.200 192.168.200.250
!
webvpn gateway gateway_1
 hostname vpn
 ip address 173.11.196.220 port 443
 http-redirect port 80
 ssl trustpoint TP-self-signed-2564112419
 logging enable
 inservice
 !
webvpn install svc flash:/webvpn/anyconnect-win-2.5.2019-k9.pkg sequence 1
 !
```

```
webvpn install csd flash:/webvpn/sdesktop.pkg
 !
webvpn context VPNACCESS
 secondary-color white
 title-color #669999
 text-color black
 ssl authenticate verify all
 !
 policy group NOACCESS
   banner "Access denied per user group restrictions in Active Directory.
 Please contact your system administrator or manager to request access."
   hide-url-bar
   timeout idle 60
   timeout session 1
 !
 !
 policy group CN=T,OU=MyBusiness,DC=chillsthrills,DC=local
   functions svc-enabled
   banner "special access-granted"
   svc address-pool "vpnpool"
   svc default-domain "cisco.com"
   svc keep-client-installed
   svc rekey method new-tunnel
   svc split dns "cisco.com"
   svc split include 192.168.0.0 255.255.255.0
   svc split include 10.10.10.0 255.255.255.0
   svc split include 172.16.254.0 255.255.255.0
   svc dns-server primary 192.168.0.136
 default-group-policy NOACCESS
 aaa authentication list AD
 gateway gateway_1
 inservice
!
end
```

Caveats

1. If the user is a "memberOf" multiple groups, the first "memberOf" value is used by the router.
2. What is odd in this configuration is that the name of the policy group has to be an exact match for the ***complete*** string pushed by the LDAP server for the "memberOf value". Usually administrators use shorter and more relevant names for the policy group, such as VPNACCESS, but apart from the cosmetic issue this can lead to a bigger problem. It is not uncommon for the "memberOf" attribute string to be considerably larger than what has been used in this example. For example, consider this debug message:

   ```
   004090: Aug 23 08:26:57.235 PCTime: %SSLVPN-6-INVALID_RADIUS_CONFIGURATION:
    Radius configured group policy "CN=VPNACCESS,OU=SecurityGroups,OU=MyBusiness,
   DC=chillsthrills,DC=local" does not exist
   ```

   It clearly shows that the string received from AD is:

   ```
   "CN=VPNACCESS,OU=SecurityGroups,OU=MyBusiness,DC=chillsthrills,DC=local"
   ```

   However, since there is no such policy group defined, if the administrator tries to configure such a group policy it results in an error because Cisco IOS has a limit on the number of characters in the policy group name:

   ```
   HOURTR1(config-webvpn-context)#webvpn context VPNACCESS
   HOURTR1(config-webvpn-context)# policy group "CN=VPNACCESS,OU=Security Groups,
   OU=MyBusiness,DC=chillsthrills,DC=local"
   Error: group policy name cannot exceed 63 characters
   ```

In such situations there are two possible workarounds:

1. Use a different LDAP attribute, such as "department".

   Consider this LDAP attribute map:

   ```
   ldap attribute-map ADMAP
    map type department user-vpn-group
   ```

   In this case the value of the department attribute for a user can be set to a value such as VPNACCESS and the WebVPN configuration is a bit simpler:

   ```
   webvpn context VPNACCESS
    secondary-color white
    title-color #669999
    text-color black
    ssl authenticate verify all
    !
    policy group NOACCESS
      banner "Access denied per user group restrictions in Active Directory.
    Please contact your system administrator or manager to request access."
    !
    policy group VPNACCESS
      functions svc-enabled
      banner "access-granted"
      svc address-pool "vpnpool"
      svc default-domain "cisco.com"
      svc keep-client-installed
      svc rekey method new-tunnel
      svc split dns "cisco.com"
      svc split include 192.168.0.0 255.255.255.0
      svc split include 10.10.10.0 255.255.255.0
      svc split include 172.16.254.0 255.255.255.0
      svc dns-server primary 192.168.0.136
    default-group-policy NOACCESS
    aaa authentication list AD
    gateway gateway_1
    inservice
   !
   end
   ```

2. Use the DN-to-string keyword in the LDAP attribute map.

   If the previous workaround is not suitable then the administrator can use the dn-to-string keyword in the LDAP attribute map in order to extract just the Common Name (CN) value from the "memberOf" string. In this scenario the LDAP attribute map would be:

   ```
   ldap attribute-map ADMAP
    map type memberOf user-vpn-group format dn-to-string
   ```

   And the WebVPN configuration would be:

   ```
   webvpn context VPNACCESS
    secondary-color white
    title-color #669999
    text-color black
    ssl authenticate verify all
    !
    policy group NOACCESS
      banner "Access denied per user group restrictions in Active Directory.
    Please contact your system administrator or manager to request access."
    !
    policy group VPNACCESS
   ```

```
   functions svc-enabled
   banner "access-granted"
   svc address-pool "vpnpool"
   svc default-domain "cisco.com"
   svc keep-client-installed
   svc rekey method new-tunnel
   svc split dns "cisco.com"
   svc split include 192.168.0.0 255.255.255.0
   svc split include 10.10.10.0 255.255.255.0
   svc split include 172.16.254.0 255.255.255.0
   svc dns-server primary 192.168.0.136
 default-group-policy NOACCESS
 aaa authentication list AD
 gateway gateway_1
 inservice
!
end
```

Note: Unlike in ASAs where you can use the ***map value*** command under an attribute map in order to match the value received from the LDAP server to some other locally significant value, Cisco IOS headends do not have this option and are therefore not as flexible. Cisco bug ID CSCts31840 has been filed in order to address this.

Verify

Use this section to confirm that your configuration works properly.

The Output Interpreter Tool (registered customers only) supports certain ***show*** commands. Use the Output Interpreter Tool in order to view an analysis of ***show*** command output.

- ***show ldap attributes***
- ***show ldap server all***

Troubleshoot

This section provides information you can use in order to troubleshoot your configuration.

Note: Refer to Important Information on Debug Commands before you use ***debug*** commands.

In order to troubleshoot the LDAP attribute mapping, enable these debugs:

- ***debug ldap all***
- ***debug ldap event***
- ***debug aaa authentication***
- ***debug aaa authorization***

Updated: Jan 07, 2015 Document ID: 118695