ASA 8.0：为 WebVPN 用户配置 LDAP 身份验证

目录

简介

本文档说明如何配置 Cisco 自适应安全设备 (ASA) 以使用 LDAP 服务器来对 WebVPN 用户进行身份验证。本示例中的 LDAP 服务器为 Microsoft Active Directory。此配置用可适应安全设备管理器(ASDM)执行运行软件版本8.0(2)的6.0(2)在ASA。

注意： 在此示例轻量级目录访问协议(LDAP)验证为WebVPN用户配置，但是此配置可以用于远程访问客户端的其他类型。只需将 AAA 服务器组分配给所需的连接配置文件（隧道组）即可，如下所示。

先决条件

需要进行基本 VPN 配置。本示例中使用 WebVPN。

背景信息

在本示例中，ASA 与 LDAP 服务器进行核对，以验证要进行身份验证的用户的身份。此进程不工作类似一传统远程验证拨入用户服务(RADIUS)或终端访问控制器访问控制系统加上(TACACS+)交换。这些步骤从高层面上说明了 ASA 如何使用 LDAP 服务器检查用户凭据。

1. 用户发起到 ASA 的连接。
2. ASA配置验证该用户用Microsoft Active Directory (AD) /LDAP服务器。
3. ASA 使用在 ASA 上配置的凭据（本例中为 admin）绑定到 LDAP 服务器，并查找所提供的用户名。**admin 用户**也获得适当的凭据，以将内容列于 Active Directory 中。有关如何授予 LDAP 查询权限的详细信息，请参阅 http://support.microsoft.com/?id=320528 。**注意**

：Microsoft 网站 http://support.microsoft.com/?id=320528 由第三方提供商管理。 Cisco 对其内容概不负责。

4. 如果找到用户名，则 ASA 尝试使用用户登录时提供的凭据绑定到 LDAP 服务器。
5. 如果第二次绑定成功，则身份验证成功，ASA 处理用户的属性。**注意：** 在本示例中，属性没有任何作用。请参阅 ASA/PIX：通过 LDAP 将 VPN 客户端映射到 VPN 组策略配置示例，以查看 ASA 如何才能处理 LDAP 属性的示例。

配置 LDAP 验证

本部分提供有关如何配置 ASA 以使用 LDAP 服务器对 WebVPN 客户端进行身份验证的信息。

ASDM

在 ASDM 中完成以下步骤，以将 ASA 配置为与 LDAP 服务器通信并对 WebVPN 客户端进行身份验证。

1. 导航到“Configuration”>“Remote Access VPN”>“AAA Setup”>“AAA Server Groups”。
2. 单击“AAA Server Groups”旁边的 **Add**
3. 指定新 AAA 服务器组的名称，然后选择 **LDAP** 作为协议。
4. 请确保在顶部窗格中选择了新组，并在“Selected Group”窗格中单击“Servers”旁边的 **Add**。
5. 为您的 LDAP 服务器提供配置信息。随后的屏幕截图显示了一个配置示例。下面对其中的多个配置选项进行了解释：**Interface Name**—ASA 用于连接 LDAP 服务器的接口**Server Name or IP address**—ASA 用于连接 LDAP 服务器的地址**Server Type**—LDAP 服务器的类型，如Microsoft**Base DN**—服务器在 LDAP 层次结构中进行搜索的起始位置**Scope**—服务器在 LDAP 层次结构中进行搜索的搜索范围**Naming Attribute**—一个（或多个）唯一标识 LDAP 服务器上的条目的相对可分辨名称属性。**sAMAccountName** 为 Microsoft Active Directory 中的默认属性。其他常用属性包括 CN、UID 和 userPrincipalName。**Login DN**—具有足够权限以便能够在 LDAP 服务器中搜索/读取/查找用户的 DN**Login Password**—DN 帐户的口令**LDAP Attribute Map**—要与来自此服务器的响应一起使用的 LDAP 属性映射。请参阅 ASA/PIX：通过 LDAP 将 VPN 客户端映射到 VPN 组策略配置示例，以了解如何配置 LDAP 属性映射。
6. 配置了 AAA 服务器组并向其中添加了服务器之后，必须将您的连接配置文件（隧道组）配置为使用新的 AAA 配置。导航到“Configuration”>“Remote Access VPN”>“Clientless SSL VPN Access”>“Connection Profiles”。
7. 选择要配置 AAA 的连接配置文件（隧道组），并单击 **Edit**
8. 在 **Authentication** 下，选择之前创建的 LDAP 服务器组。

命令行界面

完成在命令行界面(CLI)的这些步骤为了配置ASA用LDAP服务器通信和验证WebVPN客户端。

```
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
ciscoasa(config-aaa-server-host)#ldap-scope subtree ciscoasa(config-aaa-server-host)#server-type
microsoft ciscoasa(config-aaa-server-host)#exit !--- 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
```

执行多域搜索（可选）

可选。当前，ASA 不支持使用 LDAP referal 机制进行多域搜索 (Cisco Bug ID CSCsj32153)。支持在“全局编录服务器”模式下使用 AD 进行多域搜索。要执行多域搜索，请将 AD 服务器设置为“全局编录服务器”模式，在 ASA 中，通常为 LDAP 服务器条目使用以下关键参数。关键是所使用的 ldap-name-attribute 在目录树间必须是唯一的。

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

验证

使用本部分可确认配置能否正常运行。

使用 ASDM 测试

使用“AAA Server Groups”配置屏幕上的 **Test** 按钮可验证您的 LDAP 配置。提供用户名和口令后，使用此按钮可向 LDAP 服务器发送测试身份验证请求。

1. 导航到“Configuration”>“Remote Access VPN”>“AAA Setup”>“AAA Server Groups”。
2. 在顶部窗格中选择所需的 AAA 服务器组。
3. 在下部窗格中选择要测试的 AAA 服务器。
4. 单击下部窗格右侧的 **Test** 按钮。
5. 在显示的窗口中，单击 **Authentication** 单选按钮，并提供要用来进行测试的凭据。完成后单击 **OK**。
6. 在 ASA 与 LDAP 服务器联系后，将显示成功或失败消息。

使用 CLI 测试

可以在命令行中使用 **test** 命令测试您的 AAA 设置。向 AAA 服务器发送测试请求，并在命令行中显示结果。

```
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
```

故障排除

如果不确定当前要使用的 DN 字符串，可在 Windows Active Driectory 服务器上从命令提示窗口发出 **dsquery** 命令，以验证用户对象的适当 DN 字符串。

```
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"
```

debug ldap 255 命令可帮助您对此方案中的身份验证问题进行故障排除。此命令启用 LDAP 调试并允许您查看 ASA 用于连接到 LDAP 服务器的过程。此输出显示 ASA 连接到 LDAP 服务器，如本文档的背景信息部分所述。

以下调试显示成功的身份验证：

```
ciscoasa#debug ldap 255 [7] Session Start [7] New request Session, context 0xd4b11730, reqType =
1 [7] Fiber started [7] Creating LDAP context with uri=ldap://192.168.1.2:389 [7] Connect to
```

LDAP server: ldap://192.168.1.2:389, status = Successful [7] defaultNamingContext: value = DC=ftwsecurity,DC=cisco,DC=com [7] supportedLDAPVersion: value = 3 [7] supportedLDAPVersion: value = 2 [7] supportedSASLMechanisms: value = GSSAPI [7] supportedSASLMechanisms: value = GSS-SPNEGO [7] supportedSASLMechanisms: value = EXTERNAL [7] supportedSASLMechanisms: value = DIGEST-MD5 *!--- The ASA connects to the LDAP server as admin to search for kate.* **[7] Binding as administrator [7] Performing Simple authentication for admin to 192.168.1.2 [7] LDAP Search: Base DN = [dc=ftwsecurity, dc=cisco, dc=com] Filter = [sAMAccountName=kate] Scope = [SUBTREE] [7] User DN = [CN=Kate Austen,CN=Users,DC=ftwsecurity,DC=cisco,DC=com]** [7] Talking to Active Directory server 192.168.1.2 [7] Reading password policy for kate, dn:CN=Kate Austen,CN=Users, DC=ftwsecurity,DC=cisco,DC=com [7] Read bad password count 1 *!--- The ASA binds to the LDAP server as kate to test the password.* **[7] Binding as user [7] Performing Simple authentication for kate to 192.168.1.2 [7] Checking password policy for user kate [7] Binding as administrator [7] Performing Simple authentication for admin to 192.168.1.2 [7] Authentication successful for kate to 192.168.1.2 [7] Retrieving user attributes from server 192.168.1.2** [7] Retrieved Attributes: [7] objectClass: value = top [7] objectClass: value = person [7] objectClass: value = organizationalPerson [7] objectClass: value = user [7] cn: value = Kate Austen [7] sn: value = Austen [7] givenName: value = Kate [7] distinguishedName: value = CN=Kate Austen,CN=Users,DC=ftwsecurity, DC=cisco,DC=com [7] instanceType: value = 4 [7] whenCreated: value = 20070815155224.0Z [7] whenChanged: value = 20070815195813.0Z [7] displayName: value = Kate Austen [7] uSNCreated: value = 16430 [7] memberOf: value = CN=Castaways,CN=Users,DC=ftwsecurity,DC=cisco,DC=com [7] memberOf: value = CN=Employees,CN=Users,DC=ftwsecurity,DC=cisco,DC=com [7] uSNChanged: value = 20500 [7] name: value = Kate Austen [7] objectGUID: value = ..z...yC.q0..... [7] userAccountControl: value = 66048 [7] badPwdCount: value = 1 [7] codePage: value = 0 [7] countryCode: value = 0 [7] badPasswordTime: value = 128321799570937500 [7] lastLogoff: value = 0 [7] lastLogon: value = 128321798130468750 [7] pwdLastSet: value = 128316667442656250 [7] primaryGroupID: value = 513 [7] objectSid: value = ...Q..p..*.p?E.Z... [7] accountExpires: value = 9223372036854775807 [7] logonCount: value = 0 [7] sAMAccountName: value = kate [7] sAMAccountType: value = 805306368 [7] userPrincipalName: value = kate@ftwsecurity.cisco.com [7] objectCategory: value = CN=Person,CN=Schema,CN=Configuration, DC=ftwsecurity,DC=cisco,DC=com [7] dSCorePropagationData: value = 20070815195237.0Z [7] dSCorePropagationData: value = 20070815195237.0Z [7] dSCorePropagationData: value = 20070815195237.0Z [7] dSCorePropagationData: value = 16010108151056.0Z [7] Fiber exit Tx=685 bytes Rx=2690 bytes, status=1 [7] Session End

以下调试显示由于口令错误而失败的身份验证：

ciscoasa#**debug ldap 255** [8] Session Start [8] New request Session, context 0xd4b11730, reqType = 1 [8] Fiber started [8] Creating LDAP context with uri=ldap://192.168.1.2:389 [8] Connect to LDAP server: ldap://192.168.1.2:389, status = Successful [8] defaultNamingContext: value = DC=ftwsecurity,DC=cisco,DC=com [8] supportedLDAPVersion: value = 3 [8] supportedLDAPVersion: value = 2 [8] supportedSASLMechanisms: value = GSSAPI [8] supportedSASLMechanisms: value = GSS-SPNEGO [8] supportedSASLMechanisms: value = EXTERNAL [8] supportedSASLMechanisms: value = DIGEST-MD5 *!--- The ASA connects to the LDAP server as admin to search for kate.* **[8] Binding as administrator [8] Performing Simple authentication for admin to 192.168.1.2 [8] LDAP Search: Base DN = [dc=ftwsecurity, dc=cisco, dc=com] Filter = [sAMAccountName=kate] Scope = [SUBTREE] [8] User DN = [CN=Kate Austen,CN=Users,DC=ftwsecurity,DC=cisco,DC=com]** [8] Talking to Active Directory server 192.168.1.2 [8] Reading password policy for kate, dn:CN=Kate Austen,CN=Users, DC=ftwsecurity,DC=cisco,DC=com [8] Read bad password count 1 *!--- The ASA attempts to bind as kate, but the password is incorrect.* **[8] Binding as user [8] Performing Simple authentication for kate to 192.168.1.2 [8] Simple authentication for kate returned code (49) Invalid credentials** [8] Binding as administrator [8] Performing Simple authentication for admin to 192.168.1.2 [8] Reading bad password count for kate, dn: CN=Kate Austen,CN=Users, DC=ftwsecurity,DC=cisco,DC=com [8] Received badPwdCount=1 for user kate [8] badPwdCount=1 before, badPwdCount=1 after for kate [8] now: Tue, 28 Aug 2007 15:33:05 GMT, lastset: Wed, 15 Aug 2007 15:52:24 GMT, delta=1122041, maxage=3710851 secs [8] Invalid password for kate [8] Fiber exit Tx=788 bytes Rx=2904 bytes, status=-1 [8] Session End

以下调试显示由于在 LDAP 服务器上找不到该用户而失败的身份验证：

ciscoasa#**debug ldap 255** [9] Session Start [9] New request Session, context 0xd4b11730, reqType = 1 [9] Fiber started [9] Creating LDAP context with uri=ldap://192.168.1.2:389 [9] Connect to LDAP server: ldap://192.168.1.2:389, status = Successful [9] defaultNamingContext: value = DC=ftwsecurity,DC=cisco,DC=com [9] supportedLDAPVersion: value = 3 [9] supportedLDAPVersion: value = 2 [9] supportedSASLMechanisms: value = GSSAPI [9] supportedSASLMechanisms: value = GSS-

```
SPNEGO [9] supportedSASLMechanisms: value = EXTERNAL [9] supportedSASLMechanisms: value =
DIGEST-MD5 !--- The user mikhail is not found. [9] Binding as administrator [9] Performing
Simple authentication for admin to 192.168.1.2 [9] LDAP Search: Base DN = [dc=ftwsecurity,
dc=cisco, dc=com] Filter = [sAMAccountName=mikhail] Scope = [SUBTREE] [9] Requested attributes
not found [9] Fiber exit Tx=256 bytes Rx=607 bytes, status=-1 [9] Session End
```

当ASA和LDAP认证服务器之间的连接不工作时，调试表示此错误消息：

```
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.
```

相关信息

- 技术支持和文档 - Cisco Systems