ASA 8. 0: Настройка проверки подлинности LDAP для пользователей WebVPN

Содержание

Введение
Предварительные условия
Общие сведения
Настройка аутентификации LDAP
ASDM
Интерфейс командной строки
Мультидоменный поиск (дополнительно)
Проверка
Проверка в ASDM
Проверка в интерфейсе командной строки
Устранение неполадок
Дополнительные сведения

Введение

Этот документ иллюстрирует порядок настройки устройств адаптивной защиты Cisco (ASA) для использования сервера LDAP при аутентификации пользователей WebVPN. Сервер LDAP в этом примере — Microsoft Active Directory. Настройка выполняется посредством Менеджера устройств адаптивной защиты (ASDM) 6.0(2) на устройстве ASA, работающем под управлением версии ПО 8.0(2).

Примечание: В данном примере аутентификация Протокола LDAP настроена для пользователей WebVPN, но эта конфигурация может использоваться для всех других типов клиентов удаленного доступа также. Достаточно назначить группу сервера AAA требуемому профилю подключения (группе туннелей), как это будет продемонстрировано.

Предварительные условия

Требуется базовая конфигурация VPN. В данном примере используется WebVPN.

Общие сведения

В этом примере ASA обращается к серверу LDAP для проверки идентификационных данных пользователей, аутентификация которых производится. Это протокол работает иным образом, чем традиционный обмен данными со службой аутентификации RADIUS или TACACS+. Приведенная последовательность действий иллюстрирует общий порядок использования сервера LDAP устройством ASA для проверки реквизитов учетной записи

пользователя.

1. Пользователь инициирует подключение к устройству ASA.
2. Устройство ASA настроено на аутентификацию пользователя посредством сервера Microsoft Active Directory (AD)/LDAP.
3. ASA связывается с сервером LDAP с учетными данными (в данном случае admin), настроенными на ASA, и ищет предоставленное имя пользователя. **Пользователь admin также получает соответствующие реквизиты для просмотра содержимого Active Directory.** См. http://support.microsoft.com/? id=320528 для получения дополнительной информации о том, как предоставить LDAP, сделали запрос привилегий.**Примечание:** Веб-узел Microsoft в http://support.microsoft.com/? id=320528 управляет поставщик третьей стороны. Компания Cisco не несет ответственности за его содержимое.
4. Если имя пользователя найдено, ASA предпринимает попытку связаться с сервером LDAP с использованием указанных пользователем учетных данных при входе.
5. При успешном выполнении второй привязки аутентификация считается пройденной, и ASA обрабатывает атрибуты пользователя.**Примечание:** В данном примере атрибуты не используются ни для чего. В документе ASA/PIX: Пример конфигурации для назначения клиентов VPN групповым политикам VPN посредством LDAP подробно описана обработка атрибутов LDAP устройством ASA.

Настройка аутентификации LDAP

В этом разделе приведены сведения, позволяющие настроить устройство ASA для использования сервера LDAP при аутентификации клиентов WebVPN.

ASDM

Чтобы настроить устройство ASA для взаимодействия с сервером LDAP и выполнения аутентификации клиентов WebVPN, выполните следующие шаги в ASDM.

1. Выберите Configuration > Remote Access VPN > AAA Setup > AAA Server Groups (Конфигурация > VPN для удаленного доступа > Настройка AAA > Группы серверов AAA).
2. **Рядом со списком AAA Server Groups (Группы серверов AAA) выберите Add (Добавить)**
3. **Укажите имя новой группы серверов AAA и в качестве протокола выберите LDAP.**
4. **Убедитесь, что новая группа выбрана в верхней области, и нажмите кнопку Add (Добавить) рядом с областью Servers in the Selected Group (Серверы в выбранной группе).**
5. Укажите сведения о конфигурации сервера LDAP. Последующий снимок экрана иллюстрирует пример конфигурации. Ниже поясняются многие параметры конфигурации:**Interface Name (Имя интерфейса) — интерфейс, который устройство ASA должно использовать для обращения к серверу LDAPServer Name or IP address (Имя или IP-адрес сервера) — адрес, который устройство ASA должно использовать для обращения к серверу LDAPServer Type (Тип сервера) — тип сервера LDAP, например MicrosoftBase DN (Базовое отличительное имя) — местоположение в иерархии LDAP, с которого должен начинать поиск серверScope (Рамки) — рамки поиска в иерархии LDAP, выполняемого серверомNaming Attribute (Атрибут именования) — атрибут (или атрибуты) относительного отличительного имени,**

однозначно определяющий запись на сервере LDAP. атрибут по умолчанию в Microsoft Active Directory —sAMAccountName. Другие часто используемые атрибуты: CN, UID и userPrincipalName.**Login DN (Отличительное имя входа) — отличительное имя с достаточными привилегиями для поиска, чтения и указания пользователей на сервере LDAPLogin Password (Пароль для входа) — пароль учетной записи отличительного имениLDAP Attribute Map (Карта атрибутов LDAP) — карта, используемая для ответов от этого сервера.** В документе ASA/PIX: Пример конфигурации для назначения клиентов VPN групповым политикам VPN посредством LDAP более подробно описана настройка карт атрибутов LDAP.

6. После настройки группы серверов AAA и добавления в нее сервера необходимо настроить профиль подключения (группу туннелирования) для использования новой конфигурации AAA. Выберите Configuration > Remote Access VPN > Clientless SSL VPN Access > Connection Profiles (Конфигурация > VPN для удаленного доступа > Доступ по бесклиентской сети VPN на основе SSL > Профили подключений).
7. **Выберите профиль подключения (группу туннелирования), для которого необходимо настроить AAA, и нажмите Edit (Изменить)**
8. **В разделе Authentication (Аутентификация) выберите группу серверов LDAP, созданную ранее.**

Интерфейс командной строки

Чтобы настроить устройство ASA для взаимодействия с сервером LDAP и выполнения аутентификации клиентов WebVPN, выполните следующие шаги в интерфейсе командной строки.

```
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
```

Мультидоменный поиск (дополнительно)

Дополнительно. ASA в настоящее время не поддерживает механизм перенаправления LDAP для мультидоменного поиска (идентификатор ошибки Cisco CSCsj32153). Мультидоменный поиск поддерживается с AD в режиме сервера глобального каталога. Для выполнения мультидоменного поиска нужно настроить сервер AD в режиме сервера глобального каталога. Обычно при этом используются следующие ключевые параметры записи сервера LDAP в ASA. Принципиально важно использовать значение ldap-name-attribute, уникальное в пределах дерева каталогов.

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

Проверка

Воспользуйтесь данным разделом для проверки правильности функционирования вашей

конфигурации.

Проверка в ASDM

Проверьте конфигурацию LDAP кнопкой Test (Проверка) на экране настройки групп серверов AAA. Эта кнопка позволяет после указания имени пользователя и пароля отправить проверочный запрос аутентификации на сервер LDAP.

1. Выберите Configuration > Remote Access VPN > AAA Setup > AAA Server Groups (Конфигурация > VPN для удаленного доступа > Настройка AAA > Группы серверов AAA).
2. Выберите требуемую группу серверов AAA в верхней области.
3. В нижней области выберите сервер AAA, который необходимо проверить.
4. **Справа от нее нажмите кнопку Test (Проверить).**
5. **В появившемся окне выберите переключатель Authentication (Аутентификация) и укажите реквизиты аутентификации, которые необходимо проверить. По окончании нажмите OK.**
6. После того, как устройство ASA обратится к серверу LDAP, появится сообщение об успешном выполнении операции или ошибке.

Проверка в интерфейсе командной строки

Для проверки настроек AAA можно использовать команду test в интерфейсе командной строки. На сервер AAA направляется проверочный запрос, а результат появляется в командной строке.

```
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
```

Устранение неполадок

В случае сомнений относительно текущей используемой строки отличительного имени (DN) можно проверить соответствующую строку DN пользовательского объекта, введя команду dsquery на сервере Windows Active Directory из приглашения командной строки.

```
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"
```

Команда debug ldap 255 помогает диагностировать проблемы аутентификации в этом сценарии. Эта команда позволяет выполнять отладку LDAP и следить за процессом подключения ASA к серверу LDAP. В выходных данных показано подключение ASA к серверу LDAP в соответствии с общим описанием в разделе Общие сведения настоящего документа.

Этот журнал отладки показывает успешную аутентификацию:

```
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

Этот журнал отладки показывает ошибку аутентификации из-за неверного пароля:

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

Этот журнал отладки показывает ошибку аутентификации из-за отсутствия пользователя на сервере LDAP:

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

Когда подключение между ASA и сервером проверки подлинности LDAP не работает, отладки показывают это сообщение об ошибках:

```
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.
```

Дополнительные сведения

- Cisco Systems – техническая поддержка и документация