Настройте Unified Wireless Network для Аутентификации Против eDirectory Базы данных Novell

Содержание

Введение

В образовательном пространстве K-12 была увеличивающаяся потребность аутентифицировать пользователей беспроводной связи через учетные записи, созданные в eDirectory Novell. Из-за распределенного характера среды K-12, отдельные школы не могли бы иметь ресурсов для размещения сервера RADIUS на каждом узле, и при этом они не желают дополнительных издержек настройки этих серверов RADIUS. Единственный способ выполнить это при помощи LDAP для передачи между Контроллером беспроводной локальной сети (WLC) и Сервером LDAP. Контроллеры беспроводной локальной сети Cisco поддерживают Локальную EAP-аутентификацию против внешних баз данных LDAP, таких как Microsoft Active Directory. Это Описание технологических решений документирует WLC Cisco, настроенный для Локальной EAP-аутентификации против eDirectory Novell, включенного как полнофункциональный Сервер LDAP. Одно предупреждение обратить внимание – протестированные клиенты использовало утилиту Cisco Aironet Desktop Utility для выполнения аутентификации 802.1x. Novell в настоящее время не поддерживает 802.1x с их клиентом в это время. В результате в зависимости от клиента, двухэтапный процесс регистрации в системе мог произойти. Обратите внимание на эти ссылки:

Оператор 802.1x Novell

"В настоящее время они должны войти дважды. Когда Клиент novell установлен, пользователь должен войти в использование флажка Workstation Only на диалоговом окне первоначального входа в систему для разрешения проверки подлинности пользователя 802.1x, когда рабочий стол инициализируется, и затем они должны войти к Сети Novell с помощью "красного N" утилита входа в систему. Это упоминается как двухэтапный вход в систему".

Альтернатива "рабочей станции только входит", должен настроить Клиента novell для использования "Novell Начальной буквы Лоджин=офф" в Усовершенствованных параметрах настройки Входа в систему (по умолчанию является "Login=On Novell Начальной буквы"). Для получения дополнительной информации обратитесь к Аутентификации 802.1x и Клиенту novell для Windows.

Клиенты третьей стороны, такие как Meetinghouse Клиент Aeigs (Cisco Secure Services Client) Партнер по технологии Novell могут не потребовать двойного входа в систему. Для получения дополнительной информации обратитесь к AEGIS SecureConnect.

Другой жизнеспособный обходной путь для Клиента novell должен иметь машину (или пользователь) аутентифицируют (802.1x) на WLAN до GINA Novell быть выполняемым.

Тестирование решения для Единой точки входа с Клиентом novell и 802.1x выходит за рамки этого Описания технологических решений.

Протестированная топология

Протестированное решение

- Контроллер беспроводной локальной сети Cisco с 6.0.188.0 программными обеспечениями
- AP LWAPP Cisco Aironet 1242AG
- Windows XP с утилитой Cisco Aironet Desktop Utility 4.4
- Windows Server 2003 с eDirectory 8.8,5 Novell
- ConsoleOne 1.3.6 h Novell (eDirectory программа для управления)

Топология сети

Рисунок 1

Устройство	IP-адрес	Маска подсети	Шлюз по умолчанию
eDirectory Novell	192.168.3.3	255.255.255.0	192.168.3.254
Коммутатор уровня 3	192.168.3.254	255.255.255.0	-
AP	Назначенный через DHCP от Коммутатора L3	255.255.255.0	192.168.3.254
Интерфейс диспетчера точки доступа WLC интерфейса управления WLC	192.168.3.253 192.168.3.252	255.255.255.0	192.168.3.254

!--- конфигурацию

eDirectory Конфигурация Novell

eDirectory установка и конфигурация полного Novell выходят за рамки этого Описания технологических решений. eDirectory Novell должен быть установлен, а также соответствующие компоненты LDAP.

Ключевые требуемые параметры конфигурации - то, что Простой пароль должен быть включен для учетных записей пользователя, и Аутентифицируемый LDAP должен быть настроен. Использование TLS для LDAP поддерживалось в предыдущих версиях кода (4.2) WLC; однако, Безопасный LDAP больше не поддерживается на программном обеспечении контроллера беспроводной локальной сети Cisco.

1. При настройке части Сервера LDAP eDirectory удостоверьтесь, что включены Незашифрованные порты LDAP (389). Посмотрите рисунок 2 из iManager приложения Novell.**Рис. 2**
2. Во время eDirectory установки это попросит у вас Древовидной структуры или Доменного имени и т.д. Если eDirectory уже установлен, ConsoleOne Novell (рисунок 3) является легким программным средством, которым можно просмотреть eDirectory структуру. Важно найти то, что соответствующие схемы при попытке установить связь к WLC. Необходимо было также создать учетную запись, которая позволит, что WLC для выполнения Аутентифицируемого Связывает с Сервером LDAP. Для простоты, в этом случае, eDirecotry Учетная запись администратора Novell используется для Аутентифицируемого, Связывают.**Рис. 3**
3. Используйте ConsoleOne, чтобы проверить, что группа LDAP позволяет **Незашифрованные пароли**.**Рис. 4**
4. Проверьте, что под OU, Параметры безопасности, которые включен **Простой пароль**.**Рис. 5**

Другой полезный инструмент, которым можно просмотреть eDirectory структуру Novell, является браузером, включенным с установкой по умолчанию.

Рис. 6

Настройка WLC

См. рисунок 1 для физической топологии тестовой сети. WLC, используемый в этом тесте, был настроен согласно стандартной практике и с AP - диспетчером и с Интерфейсами управления в той же подсети и без меток с точки зрения VLAN.

Рисунок 7

1. Настройте Локальную EAP-аутентификацию: **Безопасность> Локальный EAP> Общий**.Стандартные настройки по умолчанию не были изменены.**Рис. 8**
2. Создайте нового Локального EAP Profile: **Безопасность> Локальный EAP> Профили**.Для этого контрольного примера Локальное выбранное название EAP profile было eDirectory. Выбранные методы аутентификации были LEAP, EAP-FAST и PEAP; однако, только PEAP был протестирован в этом документе.**Рис. 9** При настройке Локальной EAP-аутентификации для PEAP необходимо было установить сертификат на WLC. В этом случае, для тестирования, установленный сертификат Cisco фабрики использовался; однако, настроенный сертификат клиента может также быть установлен. Сертификаты стороны клиента не требуются для использования PEAP-GTC, но им можно включить для Внутреннего метода PEAP при необходимости.**Рис. 10**

3. Установите Приоритет аутентификации для LDAP: **Безопасность> Локальный EAP> Приоритет аутентификации**.**Рис. 1-1**
4. Добавьте Сервер LDAP к WLC: **Безопасность> AAA> LDAP**.**Рисунок 12**
5. Настройте WLC для использования Романа eDirecotry (см. рисунок 13):Выберите **Authenticated** для Простого Связывают метод.Введите Связывать Имя пользователя. Это - учетная запись, которая была создана к в eDirectory, который будет использоваться для WLC для привязки с eDirectory.**Примечание:** Удостоверьтесь, что вы вводите атрибуты верного каталога для имени пользователя. Для этого контрольного примера, "использовался cn=Admin, o=ZION".Введите Связывать Пароль. Это - пароль для Связывать учетной записи пользователя.Введите DN Пользовательской базы. Это - Доменное имя, где пользователь беспроводной связи считает, расположены. В контрольном примере пользователи были расположены в root DN (o=Zion). Если они вложены в других группах/организациях, объединяют их в цепочку вместе с запятой (например, "o=ZION, o=WLCUser").Введите Атрибут пользователя. Это - Общее имя (CN) (см. рисунок 6).Тип Объекта пользователя – Это установлено в *пользователя*.**Рисунок 13**
6. Создайте WLAN, который вы хотите, чтобы eDirectory клиенты Novell использовали. Для этого контрольного примера Имя профиля WLAN является *eDirectory*, и SSID является *Novell* (см. рисунок 14).**Рисунок 14**
7. Включите WLAN и примените соответствующую радио-политику и интерфейс. Для этого контрольного примера SSID Novell был только включен для 802.11a сеть и был связан к интерфейсу управления.**Рисунок 15**
8. Настройте соответствующие параметры настройки безопасности уровня 2. Для этого контрольного примера были выбраны Безопасность WPA+WPA2, политика WPA2, шифрование AES и 802.1x для Управления ключами.**Рисунок 16**
9. Для завершения конфигурации Локальной EAP-аутентификации настройте WLAN для Локальной EAP-аутентификации с помощью Сервера LDAP:Выберите **Local EAP Authentication Enabled** и примените созданного EAP Profile **(eDirectory)**.Под Серверами LDAP выберите IP Address настроенного eDirectory сервера **(192.168.3.3)**.**Рисунок 17**

Конфигурация клиента

PEAP-GTC является текущим требованием проверки подлинности для большинства школ K-12. WLC не поддерживает MSCHAPv2 для Локальной EAP-аутентификации. В результате необходимо выбрать GTC для типа Аутентификации eap на клиенте.

Следующие рисунки являются пошаговой демонстрацией конфигурации утилиты Cisco Aironet Desktop Utility для PEAP-GTC для подключения с SSID WLAN Novell. Подобные конфигурации достигнуты с собственным клиентом Microsoft с поддержкой PEAP-GTC.

1. Настройте клиентское имя профиля и SSID (Novell).**Рисунок 18**
2. Выберите **WPA/WPA2/CCKM for Security** и **PEAP (EAP-GTC)** для типа EAP.**Рисунок 19**
3. Настройте PEAP-GTC:Выберите **Validate Server Identity** и **Static Password**.Введите имя пользователя и пароль для учетной записи, или соискатель вызовет для учетных данных при входе в систему.Не входите в **<ANY>** схема каталогов Novell, поскольку это не требуется.**Рис. 20**
4. Как только профиль заполнен, активируйте его, и процесс проверки подлинности должен начаться.**Рис. 21**

Рисунок 22 изображает успешную Ассоциацию и Аутентификацию через PEAP-GTC.

Рисунок 22

Отладка

Чтобы проверить, что вы в состоянии выполнить аутентифицируемый BIND, а также проверку подлинности пользователя, включите эти опции трассировки для eDirectory:

- **Authentication**
- **LDAP**
- **NMAS**

Рисунок 23

Как показано в отладке, успешный ответ проверки подлинности LDAP отправлен Контроллеру беспроводной локальной сети в 192.168.3.253:

```
LDAP   : (192.168.3.253:36802)(0x0020:0x63) DoSearch on connection
    0x34367d0
LDAP   : (192.168.3.253:36802)(0x0020:0x63) Search request:
      base: "o=ZION"
      scope:2  dereference:0  sizelimit:0  timelimit:5  attrsonly:0
      filter: "(&(objectclass=user)(cn=sorr))"
      attribute: "dn"
      attribute: "userPassword"
Auth   : Starting SEV calculation for conn 23, entry .sorr.ZION.ZION..
Auth   : 1 GlobalGetSEV.
Auth   : 4 GlobalGetSEV succeeded.
Auth   : SEV calculation complete for conn 23, (0:0 s:ms).
LDAP   : (192.168.3.253:36802)(0x0020:0x63) Sending search result entry
    "cn=sorr,o=ZION" to connection 0x34367d0
LDAP   : (192.168.3.253:36802)(0x0020:0x63) Sending operation result 0:"":"" to
    connection 0x34367d0
LDAP   : (192.168.3.253:36802)(0x0021:0x63) DoSearch on connection 0x34367d0
LDAP   : (192.168.3.253:36802)(0x0021:0x63) Search request:
      base: "o=ZION"
      scope:2  dereference:0  sizelimit:0  timelimit:5  attrsonly:0
      filter: "(&(objectclass=user)(cn=sorr))"
      attribute: "dn"
      attribute: "userPassword"
LDAP   : (192.168.3.253:36802)(0x0021:0x63) Sending search result entry
    "cn=sorr,o=ZION" to connection 0x34367d0
LDAP   : (192.168.3.253:36802)(0x0021:0x63) Sending operation result 0:"":"" to
    connection 0x34367d0
LDAP   : (192.168.3.253:36802)(0x0022:0x60) DoBind on connection 0x34367d0
LDAP   : (192.168.3.253:36802)(0x0022:0x60) Bind name:cn=sorr,o=ZION, version:3,
    authentication:simple
Auth   : [0000804d] <.sorr.ZION.ZION.> LocalLoginRequest. Error success, conn:
    22.
LDAP   : (192.168.3.253:36802)(0x0022:0x60) Sending operation result 0:"":"" to
    connection 0x34367d0
Auth   : UpdateLoginAttributesThread page 1 processed 1 login in 0 milliseconds
```

Примечание: Некоторые линии в выходных данных отладки были обернуты из-за пространственных ограничений.

Чтобы гарантировать, что WLC выполняет запрос успешной аутентификации к eDirectory серверу, выполните эти **команды отладки** на WLC:

debug aaa ldap enable

debug aaa local-auth eap method events enable

debug aaa local-auth db enable

Пример выходных данных от успешной аутентификации:

```
*Dec 23 16:57:04.267: LOCAL_AUTH: (EAP) Sending password verify request profile
    'sorr' to LDAP
*Dec 23 16:57:04.267: AuthenticationRequest: 0xcdb6d54
*Dec 23 16:57:04.267:   Callback.....................................0x84cab60
*Dec 23 16:57:04.267:   protocolType.................................0x00100002
*Dec 23 16:57:04.267:   proxyState.................................
    00:40:96:A6:D6:CB-00:00
*Dec 23 16:57:04.267:   Packet contains 3 AVPs (not shown)
*Dec 23 16:57:04.267: EAP-AUTH-EVENT: Waiting for asynchronous reply from LL
*Dec 23 16:57:04.267: EAP-AUTH-EVENT: Waiting for asynchronous reply from LL
*Dec 23 16:57:04.267: EAP-AUTH-EVENT: Waiting for asynchronous reply from method
*Dec 23 16:57:04.267: ldapTask [1] received msg 'REQUEST' (2) in state
    'CONNECTED' (3)
*Dec 23 16:57:04.267: disabled LDAP_OPT_REFERRALS
*Dec 23 16:57:04.267: LDAP_CLIENT: UID Search (base=o=ZION,
    pattern=(&(objectclass=user)(cn=sorr)))
*Dec 23 16:57:04.269: LDAP_CLIENT: ldap_search_ext_s returns 0 85
*Dec 23 16:57:04.269: LDAP_CLIENT: Returned 2 msgs including 0 references
*Dec 23 16:57:04.269: LDAP_CLIENT: Returned msg 1 type 0x64
*Dec 23 16:57:04.269: LDAP_CLIENT: Received 1 attributes in search entry msg
*Dec 23 16:57:04.269: LDAP_CLIENT: Returned msg 2 type 0x65
*Dec 23 16:57:04.269: LDAP_CLIENT : No matched DN
*Dec 23 16:57:04.269: LDAP_CLIENT : Check result error 0 rc 1013
*Dec 23 16:57:04.269: LDAP_CLIENT: Received no referrals in search result msg
*Dec 23 16:57:04.269: ldapAuthRequest [1] called lcapi_query base="o=ZION"
    type="user" attr="cn" user="sorr" (rc = 0 - Success)
*Dec 23 16:57:04.269: Attempting user bind with username cn=sorr,o=ZION
*Dec 23 16:57:04.273: LDAP ATTR> dn = cn=sorr,o=ZION (size 14)
*Dec 23 16:57:04.273: Handling LDAP response Success
*Dec 23 16:57:04.274: LOCAL_AUTH: Found context matching MAC address - 448
*Dec 23 16:57:04.274: LOCAL_AUTH: (EAP:448) Password verify credential callback
    invoked
*Dec 23 16:57:04.274: eap_gtc.c-TX-AUTH-PAK:
*Dec 23 16:57:04.274: eap_core.c:1484: Code:SUCCESS  ID:0x 8  Length:0x0004
    Type:GTC
*Dec 23 16:57:04.274: EAP-EVENT: Received event 'EAP_METHOD_REPLY' on handle
    0xBB000075
*Dec 23 16:57:04.274: EAP-AUTH-EVENT: Handling asynchronous method response for
    context 0xBB000075
*Dec 23 16:57:04.274: EAP-AUTH-EVENT: EAP method state: Done
*Dec 23 16:57:04.274: EAP-AUTH-EVENT: EAP method decision: Unconditional Success
*Dec 23 16:57:04.274: EAP-EVENT: Sending method directive 'Free Context' on
    handle 0xBB000075
*Dec 23 16:57:04.274: eap_gtc.c-EVENT: Free context
*Dec 23 16:57:04.274: id_manager.c-AUTH-SM: Entry deleted fine id 68000002 -
    id_delete
*Dec 23 16:57:04.274: EAP-EVENT: Sending lower layer event 'EAP_SUCCESS' on
    handle 0xBB000075
*Dec 23 16:57:04.274: peap_inner_method.c-AUTH-EVENT: EAP_SUCCESS from inner
    method GTC
*Dec 23 16:57:04.278: LOCAL_AUTH: EAP: Received an auth request
*Dec 23 16:57:04.278: LOCAL_AUTH: Found context matching MAC address - 448
*Dec 23 16:57:04.278: LOCAL_AUTH: (EAP:448) Sending the Rxd EAP packet (id 9) to
    EAP subsys
*Dec 23 16:57:04.280: LOCAL_AUTH: Found matching context for id - 448
*Dec 23 16:57:04.280: LOCAL_AUTH: (EAP:448) ---> [KEY AVAIL] send_len 64,
```

```
    recv_len 64
*Dec 23 16:57:04.280: LOCAL_AUTH: (EAP:448) received keys waiting for success
*Dec 23 16:57:04.280: EAP-EVENT: Sending lower layer event 'EAP_SUCCESS' on
    handle 0xEE000074
*Dec 23 16:57:04.281: LOCAL_AUTH: Found matching context for id - 448
*Dec 23 16:57:04.281: LOCAL_AUTH: (EAP:448) Received success event
*Dec 23 16:57:04.281: LOCAL_AUTH: (EAP:448) Processing keys success
*Dec 23 16:57:04.281: 00:40:96:a6:d6:cb [BE-resp] AAA response 'Success'
*Dec 23 16:57:04.281: 00:40:96:a6:d6:cb [BE-resp] Returning AAA response
*Dec 23 16:57:04.281: 00:40:96:a6:d6:cb AAA Message 'Success' received for
    mobile 00:40:96:a6:d6:cb
```

Примечание: Некоторые линии в выходных данных были обернуты из-за пространственных ограничений.

Поскольку больше школ K-12 принимает архитектуру WLAN Cisco, будет увеличивающаяся потребность поддержать аутентификацию пользователя беспроводной связи к eDirectory Novell. Эта бумага проверила, что WLC Cisco может аутентифицировать пользователей против eDirectory базы данных LDAP Novell, когда настроено для Локальной EAP-аутентификации. Подобная конфигурация может также быть реализована с пользователями аутентификации Cisco Secure ACS к eDirectory Novell. Дополнительное исследование должно быть сделано для Единой точки входа с другими клиентами WLAN, такими как Cisco Secure Services Client и Нулевая конфигурация Microsoft Windows.

Дополнительные сведения

- Пример конфигурации локальной проверки подлинности EAP на контроллере беспроводных LAN с EAP-FAST и сервером LDAP
- Пример конфигурации локального сервера EAP Unified Wireless Network
- Пример конфигурации проверки подлинности EAP-FAST с контроллерами беспроводной сети и внешним сервером RADIUS
- Cisco Systems – техническая поддержка и документация