Центральная веб-аутентификация с коммутатором и примером конфигурации платформы Identity Services Engine

Содержание

Введение

Этот документ описывает, как настроить центральную веб-аутентификацию с проводными клиентами, связанными с коммутаторами с помощью платформы Identity Services Engine (ISE).

Понятие центральной веб-аутентификации настроено против локальной web-аутентификации, которая является обычной web-аутентификацией на самом коммутаторе. В той системе, после сбоя dot1x/mab, коммутатор будет аварийное переключение к профилю webauth и перенаправит трафик клиента к веб-странице на коммутаторе.

Центральная веб-аутентификация предлагает возможность иметь центральное устройство, которое действует как веб-портал (в th, пример, ISE). Основное различие по сравнению с обычной локальной web-аутентификацией - то, что она смещена к Уровню 2 наряду с аутентификацией mac/dot1x. Понятие также отличается по этому, сервер RADIUS (ISE в данном примере) возвращает специальные атрибуты, которые указывают к коммутатору, что должно произойти веб-перенаправление. Это решение имеет преимущество для устранения любой задержки, которая была необходима для web-аутентификации для удара.

Глобально, если MAC-адрес станции клиента не известен сервером RADIUS (но другие критерии могут также использоваться), сервер возвращает атрибуты перенаправления, и коммутатор авторизует станцию (через Обход проверки подлинности MAC [MAB]), но размещает список доступа для перенаправления веба - трафика к порталу. Однажды входы пользователя в систему в на гостевом портале, возможно через CoA (Изменение Авторизации) возвратиться порт коммутатора так, чтобы произошла новая аутентификация MAB Уровня 2. ISE может тогда помнить, что это был webauth пользователь, и примените атрибуты Уровня 2 (как динамическое присвоение VAN) пользователю. Компонент ActiveX может также вынудить клиентский компьютер обновить свой IP-адрес.

Предварительные условия

Требования

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- Платформа Identity Services Engine (ISE)
- Конфигурация коммутатора Cisco IOS®

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

- Платформа Cisco Identity Services Engine (ISE), выпуск 1.1.1
- Коммутатор Cisco Catalyst серии 3560, который работает под управлением ПО версии 12.2.55SE3

  Примечание: Процедура подобна или идентична для других Моделей коммутатора Catalyst. Можно использовать эти шаги во все Cisco IOS Software Release для Catalyst, если не указано иное.

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Настройка

Обзор

Конфигурация ISE составлена из этих пяти шагов:

1. Создайте загружаемый список контроля доступа (ACL).
2. Создайте профиль авторизации.
3. Создайте опознавательное правило.
4. Создайте правило авторизации.
5. Включите (дополнительное) обновление IP.

Создайте загружаемый список ACL

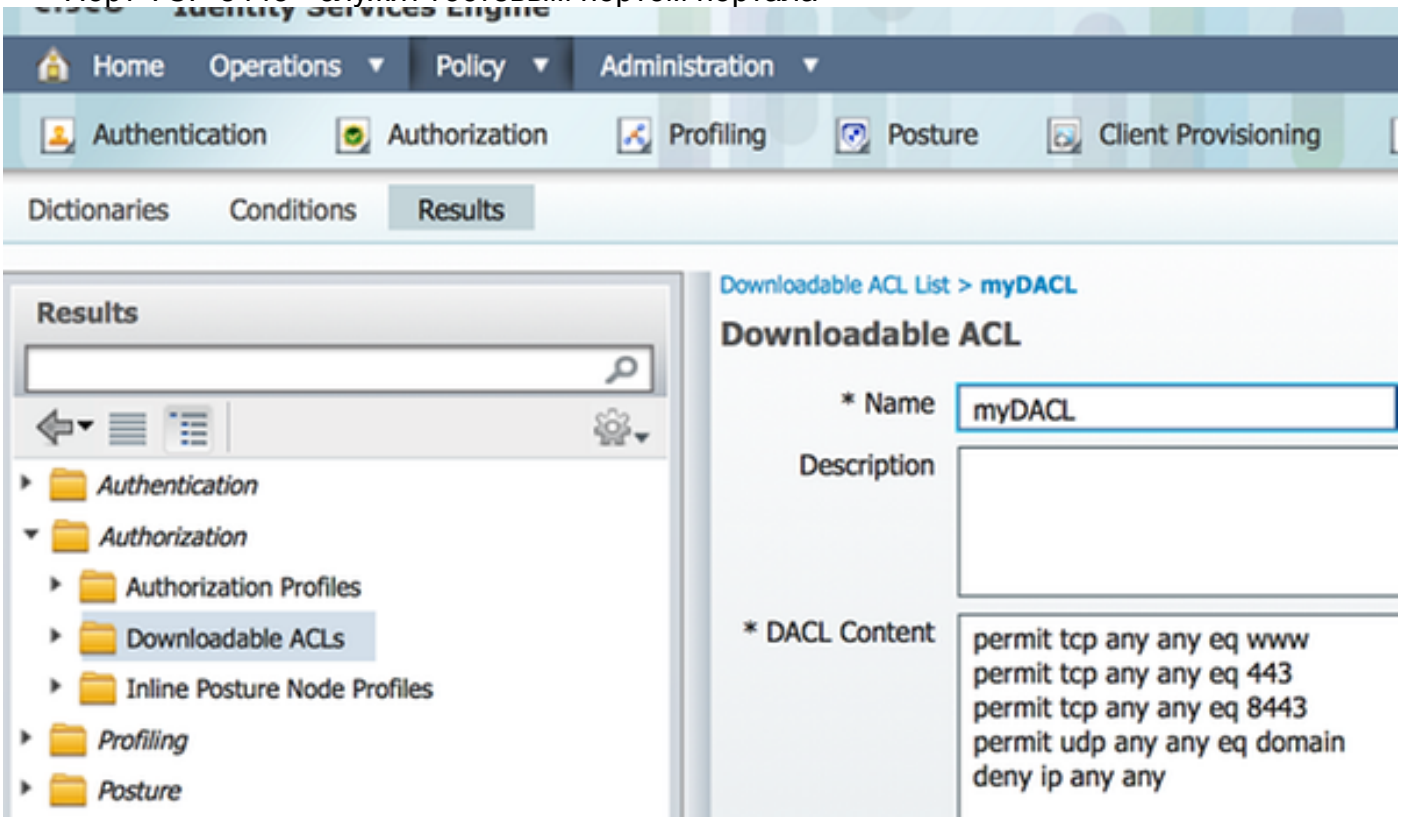
Это не обязательный шаг. ACL перенаправления, переданный обратно с центральным профилем webauth, определяет, какой трафик (HTTP или HTTPS) перенаправлен к ISE. Загружаемый список ACL позволяет вам определять то, какой трафик позволен. Необходимо, как правило, обеспечивать DNS, HTTP (S), и 8443 и запрещать остальных. В противном случае коммутатор перенаправляет трафик HTTP, но позволяет другие протоколы.

Выполните эти шаги для создания загружаемого списка ACL:

1. Нажмите **Policy** и нажмите **Policy Elements**.
2. Нажмите **Results**.
3. Разверните **Авторизацию** и нажмите **Downloadable ACLs**.
4. Нажмите **кнопку Add** для создания нового загружаемого списка ACL.
5. В **Поле имени** введите имя для DACL. Данный пример использует *myDACL*.

Этот образ показывает типичное содержание DACL, которое позволяет:

- DNS - решает имя хоста портала ISE
- HTTP и HTTPS - позволяют перенаправление
- Порт TCP 8443 - служит гостевым портом портала



Создайте профиль авторизации

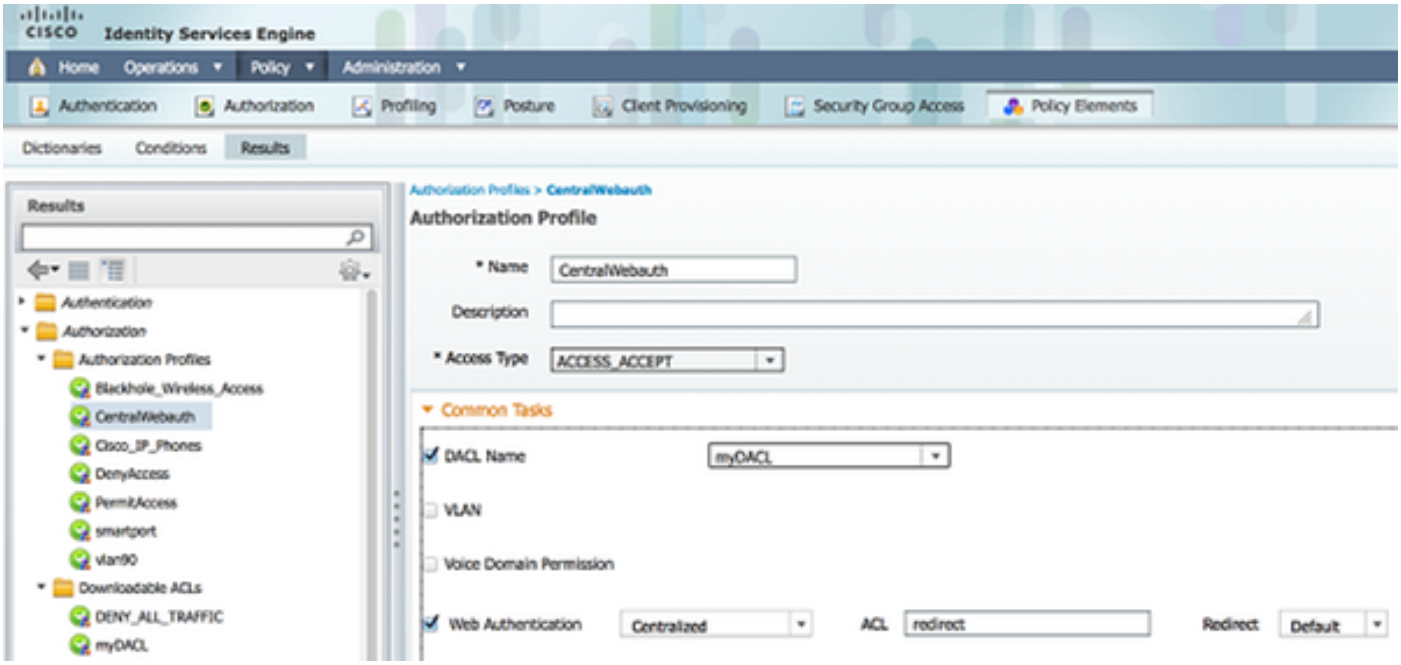
Выполните эти шаги для создания профиля авторизации:

1. Нажмите **Policy** и нажмите **Policy Elements**.
2. Нажмите **Results**.
3. Разверните **Авторизацию** и нажмите **профиль Authorization**.
4. Нажмите **кнопку Add** для создания нового профиля авторизации для центрального

webauth.

5. В **Поле имени** введите имя для профиля. Данный пример использует *CentralWebauth*.
6. Выберите **ACCESS_ACCEPT** из выпадающего списка Типа доступа.
7. Проверьте флажок **Web Authentication** и выберите **Centralized** из выпадающего списка.
8. В поле ACL введите имя ACL на коммутаторе, который определяет трафик, который будет перенаправлен. Данные примеры используют *перенаправление*.
9. Выберите **Default** из выпадающего списка Перенаправления.
10. Проверьте флажок **DACL Name** и выберите **myDACL** из выпадающего lsit, если вы решаете использовать DACL вместо ACL статического порта на коммутаторе.

Атрибут Перенаправления определяет, видит ли ISE портал веб-страницы по умолчанию или пользовательский веб-портал, который создал admin ISE. Например, ACL *перенаправления* в данном примере инициирует перенаправление после трафика HTTP или Трафика HTTPS от клиента к где угодно. ACL определен на коммутаторе позже в этом примере конфигурации.

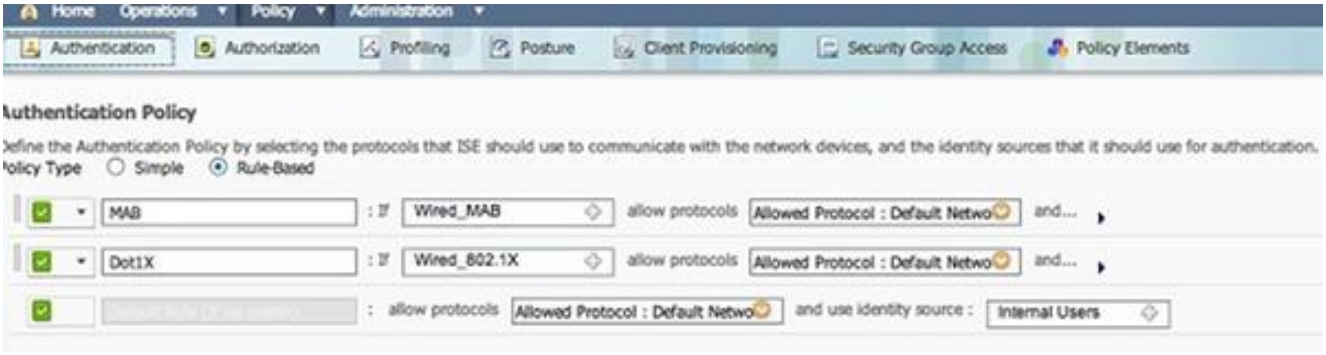


Создайте опознавательное правило

Выполните эти шаги для использования опознавательного профиля для создания опознавательного правила:

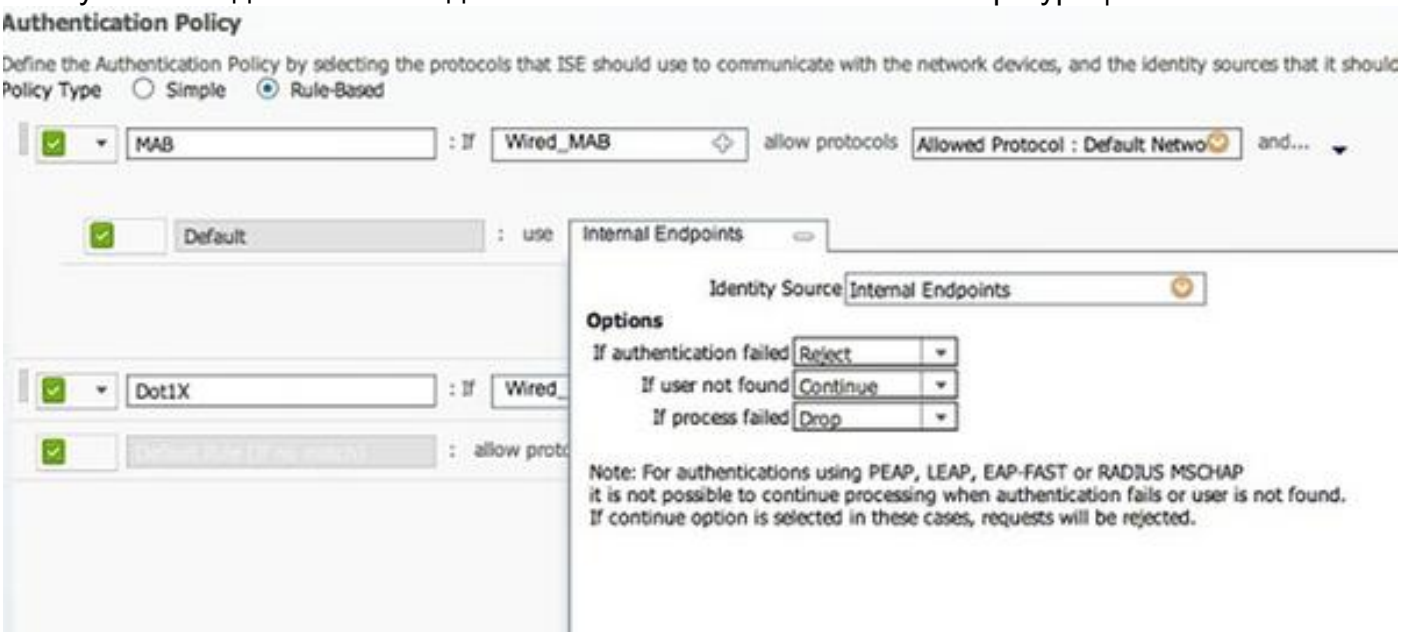
1. В соответствии с меню Policy, нажмите **Authentication**.

   Этот образ показывает пример того, как настроить правило политики аутентификации. В данном примере правило настроено, что триггеры, когда обнаружен MAB.



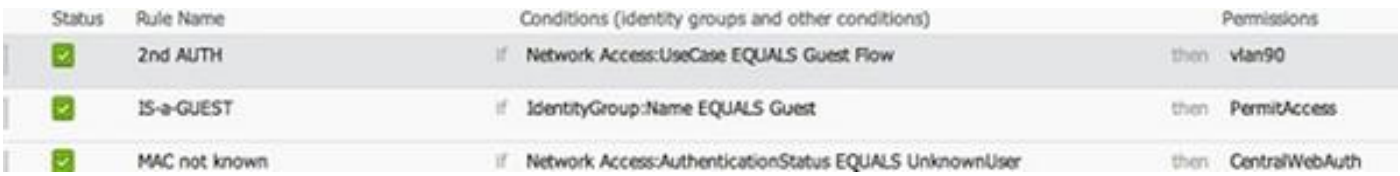
2. Введите имя для своего опознавательного правила. Данный пример использует *MAB*.
3. Выберите плюс **(+)** значок в Если поле условия.
4. Выберите **условие Compound** и выберите **Wired_MAB**.
5. Нажмите стрелку, расположенную рядом с **и...** для расширения правила далее.
6. Нажмите **+** значок в поле Identity Source и выберите **Internal endpoints**.
7. Выберите **Continue** из 'Если пользователь, не найденный' выпадающий список.

   Эта опция позволяет устройству аутентифицироваться (через webauth), даже если не известен его MAC-адрес. Клиенты Dot1x могут все еще аутентифицироваться с их учетными данными и не должны быть обеспокоены этой конфигурацией.



Создайте правило авторизации

Существует теперь несколько правил настроить в политике авторизации. Когда ПК включен, он проходит MAB; предполагается, что MAC-адрес не известен, таким образом, возвращены webauth и ACL. Этот *MAC не известное* правило показывают в этом образе и настраивают в этом разделе:



Выполните эти шаги для создания правила авторизации:

1. Создайте новое правило и введите имя. Данный пример использует *MAC, не*

известный.
2. Нажмите плюс **(+)** значок в поле условия и примите решение создать новое условие.
3. Разверните выпадающий список **выражения**.
4. Выберите **Network Access** и разверните его.
5. Нажмите **AuthenticationStatus** и выберите оператора **Equals**.
6. Выберите **UnknownUser** в правом поле.
7. На странице General Authorization выберите **CentralWebauth** (Authorization Profile) в поле направо от слова *тогда*.

   Этот шаг позволяет ISE продолжаться даже при том, что не известен пользователь (или MAC).

   Неизвестным пользователям теперь предоставляют Страницу входа. Однако, как только они вводят свои учетные данные, они представлены снова с запросом аутентификации на ISE; поэтому, другое правило должно быть настроено с условием, которое соблюдают, если пользователь является гостем. В данном примере, *Если UseridentityGroup равняется Гостю*, используется, и предполагается, что все гости принадлежат этой группе.
8. Нажмите кнопку действий, расположенную в конце *MAC не известное* правило, и примите решение вставить новое правило выше.

   Примечание: Очень важно, чтобы это новое правило появилось перед *MAC не известное* правило.
9. Введите имя для нового правила. Данный пример использует *ГОСТЕВОЙ IS*.
10. Выберите условие, которое совпадает с вашими гостями.

    InternalUser:IdentityGroup использования данного примера *Равняется Гостю*, потому что все гости связаны с *Гостевой* группой (или другая группа, которую вы настроили в своих параметрах настройки спонсора).
11. Выберите **PermitAccess** в коробке результата (расположенный направо от слова *тогда*).

    Когда пользователь авторизуется на Странице входа, ISE перезапускает аутентификацию Уровня 2 на порте коммутатора, и происходит новый MAB. В этом сценарии различие - то, что невидимый флаг собирается для ISE помнить, что это был гость-проверенный пользователь. Это правило является *2-м AUTH*, и условие является *Сетевым, Access:UseCase Равняется GuestFlow*. Это условие соблюдают, когда пользователь аутентифицируется через webauth, и порт коммутатора установлен снова для нового MAB. Можно назначить любые атрибуты, которые вы любите. Данный пример назначает профиль *vlan90* так, чтобы пользователю назначили VLAN 90 на его второй аутентификации MAB.
12. Нажмите **Actions** (расположенный в конце правила ГОСТЕВОГО IS) и выберите **Insert новое правило выше**.
13. Введите **2-й AUTH** в поле имени.
14. В поле условия нажмите плюс **(+)** значок и примите решение создать новое условие.
15. Выберите **Network Access** и нажмите **UseCase**.
16. Выберите **Equals** в качестве оператора.
17. Выберите **GuestFlow** в качестве правильного операнда.

18. На странице авторизации нажмите плюс **(+)** значок (расположенный рядом с *тогда*) для выбора результата для правила.

    В данном примере назначен предварительно сконфигурированный профиль (vlan90); эту конфигурацию не показывают в этом документе.

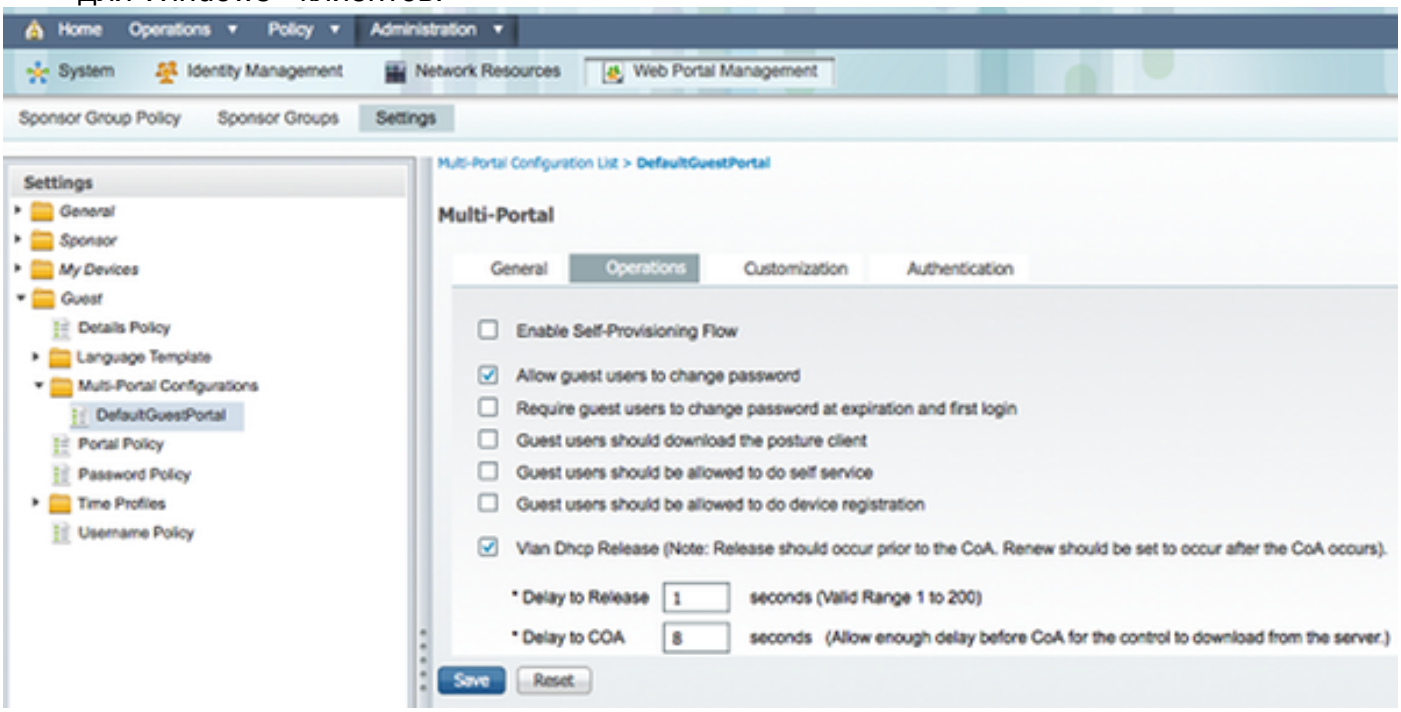
    Можно выбрать опцию **Permit Access** или создать пользовательский профиль для возврата VLAN или атрибутов, которые вы любите.

Включите обновление IP (Необязательно)

При присвоении VLAN заключительный шаг для клиентского компьютера для возобновления его IP-адреса. Этот шаг достигнут гостевым порталом для Windows - клиентов. Если вы сделали "not set", VLAN для *2-го AUTH* управляет ранее, можно пропустить этот шаг.

При присвоении VLAN выполните эти шаги для включения обновления IP:

1. Нажмите **Administration** и нажмите **Guest Management**.
2. Нажмите **Settings**.
3. Разверните **Гостя** и разверните **Мультипортала Конфигурацию**.
4. Нажмите **DefaultGuestPortal** или название пользовательского портала, который вы, возможно, создали.
5. Нажмите коробку **Vlan DHCP Releasecheck**. **Примечание:** Эта опция работает только для Windows - клиентов.



Конфигурация коммутатора (выборка)

Этот раздел предоставляет выборку конфигурации коммутатора. Посмотрите Конфигурацию коммутатора (Полную) для полной конфигурации.

Эта выборка показывает простую конфигурацию MAB.

```
interface GigabitEthernet1/0/12
description ISE1 - dot1x clients - UCS Eth0
switchport access vlan 100
switchport mode access
ip access-group webauth in
authentication order mab
authentication priority mab
authentication port-control auto
mab
spanning-tree portfast
end
```

VLAN 100 является VLAN, которая предоставляет полное сетевое подключение. ACL порта по умолчанию (названный *webauth*) применен и определен как показано здесь:

```
ip access-list extended webauth
permit ip any any
```

Даже если пользователь не аутентифицируется, этот пример конфигурации дает полный доступ к сети; поэтому, вы могли бы хотеть ограничить доступ к не прошедшим поверку подлинности пользователям.

В этой конфигурации, HTTP и просмотре HTTPS не работает без аутентификации (на другой ACL), так как ISE настроен для использования ACL перенаправления (названный *перенаправлением*). Вот определение на коммутаторе:

```
ip access-list extended redirect
deny ip any host <ISE ip address>
permit TCP any any eq www
permit TCP any any eq 443
```

Этот список доступа должен быть определен на коммутаторе для определения, на котором торгуют коммутатором, выполнит перенаправление. (Это совпадает на *разрешении*.) В данном примере, любом трафике HTTP или Трафике HTTPS, что клиент передает триггерам веб-перенаправление. Данный пример также запрещает IP-адрес ISE, таким образом, трафик к ISE переходит к ISE и не перенаправляет в петле. (В этом сценарии запретите, не блокирует трафик; это просто не перенаправляет трафик.) При использовании необычных портов HTTP или прокси можно добавить другие порты.

Другая возможность состоит в том, чтобы предоставить доступ HTTP к некоторым веб-сайтам и перенаправить другие веб-сайты. Например, если бы вы определяете в ACL разрешение для внутренних веб-серверов только, клиенты могли бы просмотреть веб-сайты, не аутентифицируясь, но встретились бы с перенаправлением, если они пытаются обратиться к внутреннему веб-серверу.

Последний шаг должен разрешить CoA на коммутаторе. В противном случае ISE не может вынудить коммутатор повторно аутентифицировать клиента.

```
aaa server radius dynamic-author
client <ISE ip address> server-key <radius shared secret>
```

Эта команда требуется для коммутатора перенаправить на основе трафика HTTP:

```
ip http server
```

Эта команда требуется, чтобы перенаправлять на основе Трафика HTTPS:

```
ip http secure-server
```

Эти команды также важны:

```
radius-server vsa send authentication
```

```
radius-server vsa send accounting
```

Если пользователь еще не аутентифицируется, **интервал сеанса show authentication <интерфейсная цифра>** возвращает эти выходные данные:

```
01-SW3750-access#show auth sess int gi1/0/12
Interface: GigabitEthernet1/0/12
MAC Address: 000f.b049.5c4b
          IP Address: 192.168.33.201
           User-Name: 00-0F-B0-49-5C-4B
              Status: Authz Success
              Domain: DATA
     Security Policy: Should Secure
     Security Status: Unsecure
      Oper host mode: single-host
    Oper control dir: both
       Authorized By: Authentication Server
         Vlan Policy: N/A
             ACS ACL: xACSACLx-IP-myDACL-51519b43
    URL Redirect ACL: redirect
        URL Redirect: https://ISE2.wlaaan.com:8443/guestportal/gateway?
sessionId=C0A82102000002D8489E0E84&action=cwa
     Session timeout: N/A
        Idle timeout: N/A
   Common Session ID: C0A82102000002D8489E0E84
     Acct Session ID: 0x000002FA
              Handle: 0xF60002D9

Runnable methods list:

      Method  State
      mab     Authc Success
```

Примечание: Несмотря на успешную аутентификацию MAB, ACL перенаправления размещен, так как MAC-адрес не был известен ISE.

(Полная) конфигурация коммутатора

Этот раздел перечисляет полную конфигурацию коммутатора. Были опущены некоторые ненужные интерфейсы и командные строки; поэтому, этот пример конфигурации должен использоваться для ссылки только и не должен быть скопирован.

```
Building configuration...

Current configuration : 6885 bytes
!
version 15.0
no service pad
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
no service password-encryption
!
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$xqtx$VPsZHbpGmLyH/EOObPpla.
!
aaa new-model
!
!
```

```
aaa group server radius newGroup
!
aaa authentication login default local
aaa authentication dot1x default group radius
aaa authorization exec default none
aaa authorization network default group radius
!
!
!
!
aaa server radius dynamic-author
client 192.168.131.1 server-key cisco
!
aaa session-id common
clock timezone CET 2 0
system mtu routing 1500
vtp interface Vlan61
udld enable

nmsp enable
ip routing
ip dhcp binding cleanup interval 600
!
!
ip dhcp snooping
ip device tracking
!
!
crypto pki trustpoint TP-self-signed-1351605760
enrollment selfsigned
subject-name cn=IOS-Self-Signed-Certificate-1351605760
revocation-check none
rsakeypair TP-self-signed-1351605760
!
!
crypto pki certificate chain TP-self-signed-1351605760
certificate self-signed 01
30820245 308201AE A0030201 02020101 300D0609 2A864886 F70D0101 04050030
31312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D 43657274
69666963 6174652D 31333531 36303537 3630301E 170D3933 30333031 30303033
35385A17 0D323030 31303130 30303030 305A3031 312F302D 06035504 03132649
4F532D53 656C662D 5369676E 65642D43 65727469 66696361 74652D31 33353136
30353736 3030819F 300D0609 2A864886 F70D0101 01050003 818D0030 81890281
8100B068 86D31732 E73D2FAD 05795D6D 402CE60A B93D4A88 C98C3F54 0982911D
D211EC23 77734A5B 7D7E5684 388AD095 67354C95 92FD05E3 F3385391 8AB9A866
B5925E04 A846F740 1C9AC0D9 6C829511 D9C5308F 13C4EA86 AF96A94E CD57B565
92317B2E 75D6AB18 04AC7E14 3923D3AC 0F19BC6A 816E6FA4 5F08CDA5 B95D334F
DA410203 010001A3 6D306B30 0F060355 1D130101 FF040530 030101FF 30180603
551D1104 11300F82 0D69696C 796E6173 2D333536 302E301F 0603551D 23041830
16801457 D1216AF3 F0841465 3DDDD4C9 D08E06C5 9890D530 1D060355 1D0E0416
041457D1 216AF3F0 8414653D DDD4C9D0 8E06C598 90D5300D 06092A86 4886F70D
01010405 00038181 0014DC5C 2D19D7E9 CB3E8ECE F7CF2185 32D8FE70 405CAA03

dot1x system-auth-control
dot1x critical eapol
!
!
!
errdisable recovery cause bpduguard
errdisable recovery interval 60
!
spanning-tree mode pvst
spanning-tree logging
spanning-tree portfast bpduguard default
```

```
spanning-tree extend system-id
spanning-tree vlan 1-200 priority 24576
!
vlan internal allocation policy ascending
lldp run
!
!
!
!
!
!
interface FastEthernet0/2
switchport access vlan 33
switchport mode access
authentication order mab
authentication priority mab
authentication port-control auto
mab
spanning-tree portfast
!
interface Vlan33
ip address 192.168.33.2 255.255.255.0
!
ip default-gateway 192.168.33.1
ip http server
ip http secure-server
!
ip route 0.0.0.0 0.0.0.0 192.168.33.1
!
ip access-list extended MY_TEST
permit ip any any
ip access-list extended redirect
deny ip any host 192.168.131.1
permit tcp any any eq www
permit tcp any any eq 443
ip access-list extended webAuthList
permit ip any any
!
ip sla enable reaction-alerts
logging esm config
logging trap warnings
logging facility auth
logging 10.48.76.31
snmp-server community c3560public RO
snmp-server community c3560private RW
snmp-server community private RO
radius-server host 192.168.131.1 auth-port 1812 acct-port 1813 key cisco
radius-server vsa send authentication
radius-server vsa send accounting
!
!
!
privilege exec level 15 configure terminal
privilege exec level 15 configure
privilege exec level 2 debug radius
privilege exec level 2 debug aaa
privilege exec level 2 debug
!
line con 0
line vty 0 4
exec-timeout 0 0
password Cisco123
authorization commands 1 MyTacacs
authorization commands 2 MyTacacs
```

```
authorization commands 15 MyTacacs
authorization exec MyTacacs
login authentication MyTacacs
line vty 5 15
!
ntp server 10.48.76.33
end
```

Конфигурация HTTP прокси

При использовании HTTP прокси для клиентов это означает что клиенты:

- Используйте нетрадиционный порт для HTTP - протокола
- Передайте весь их трафик к тому прокси

Для имения коммутатора, слушают на нетрадиционном порту (например, 8080), используют эти команды:

```
ip http port 8080
ip port-map http port 8080
```

Также необходимо настроить всех клиентов, чтобы продолжать использовать их прокси, но не использовать прокси для IP-адреса ISE. Все браузеры включают функцию, которая позволяет вам вводить имена хоста или IP-адреса, которые не должны использовать прокси. Если вы не добавляете исключение для ISE, вы встречаетесь со страницей аутентификации петли.

Также необходимо модифицировать ACL перенаправления для разрешения на прокси - порте (8080 в данном примере).

Важное замечание о SVI коммутатора

В это время коммутатору нужен виртуальный интерфейс коммутатора (SVI), чтобы ответить клиенту и передать перенаправление веб-портала клиенту. Этот SVI должен не обязательно быть на подсети клиента / VLAN. Однако, если коммутатор не имеет никакого SVI в подсети клиента / VLAN, это должно использовать любой из других SVI и передать трафик, как определено в клиентской таблице маршрутизации. Это, как правило, означает, что трафик передается другому шлюзу в ядре сети; этот трафик возвращается к коммутатору доступа в подсети клиента.

Межсетевые экраны, как правило, блокируют трафик от и до того же коммутатора, как в этом сценарии, таким образом, перенаправление не могло бы работать должным образом. Обходные пути должны позволить это поведение на межсетевом экране или создать SVI на коммутаторе доступа в подсети клиента.

Важное замечание о перенаправлении HTTPS

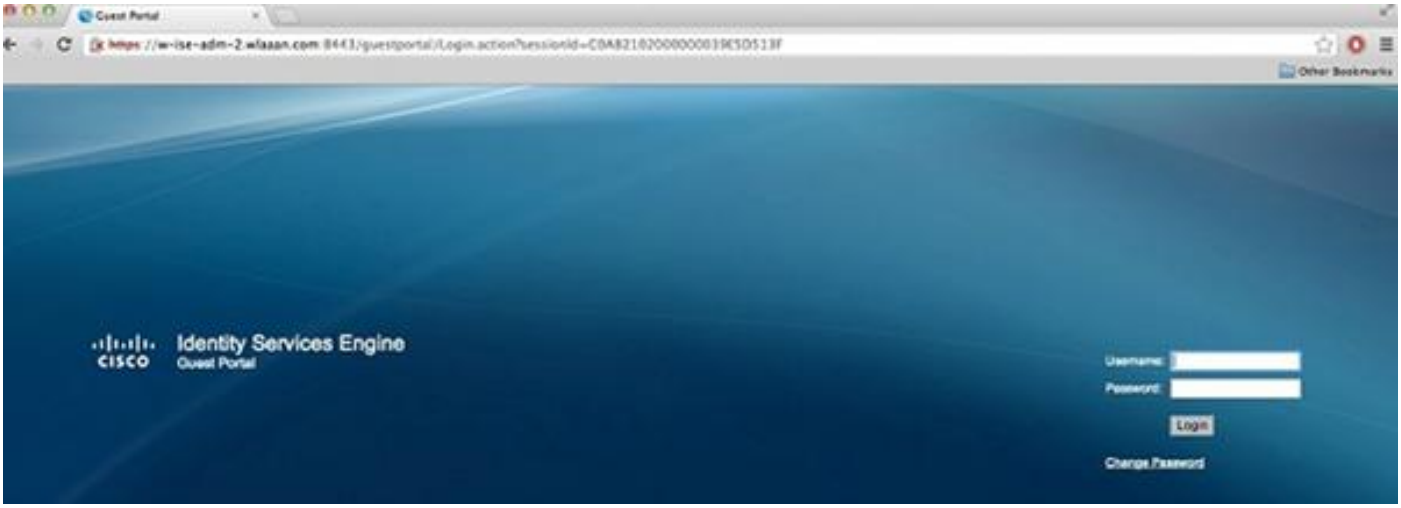
Коммутаторы в состоянии перенаправить Трафик HTTPS. Таким образом, если у гостевого клиента есть домашняя страница в HTTPS, перенаправление происходит правильно.

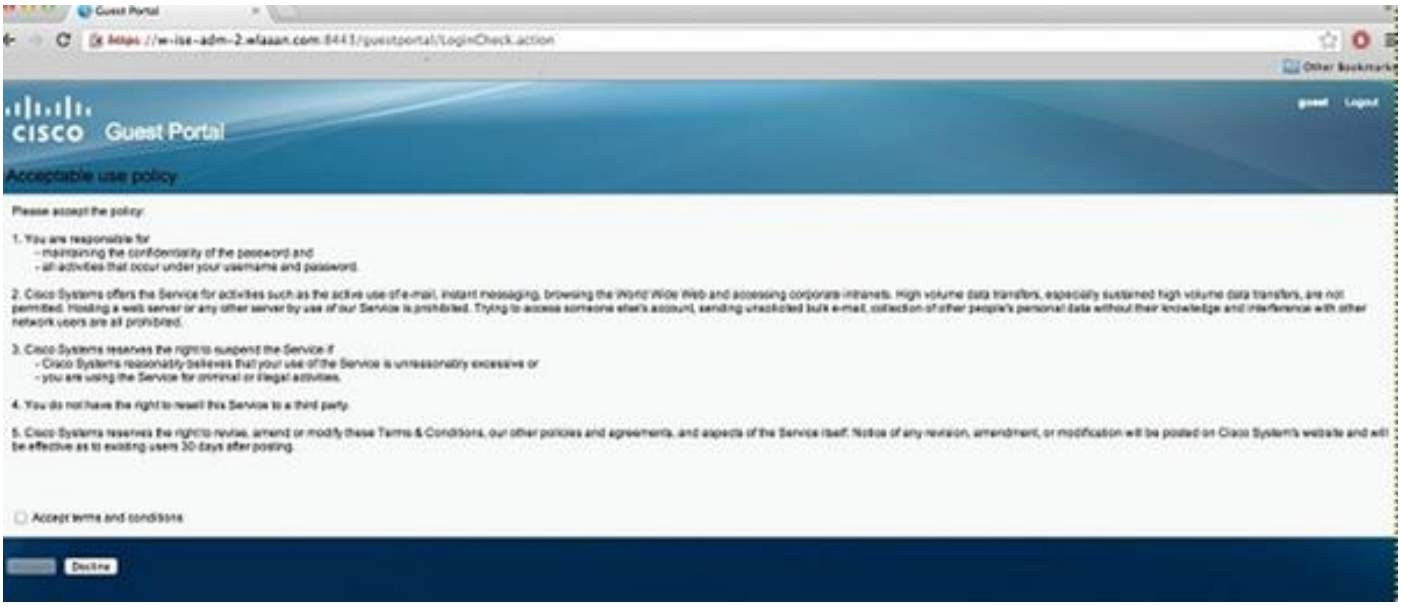
Целое понятие перенаправления основано на факте, что устройство (в этом случае, коммутатор) имитирует IP-адрес веб-сайта. Однако основная проблема возникает, когда точки пересечения коммутатора и перенаправляют Трафик HTTPS, потому что коммутатор может представить только свой собственный сертификат в квитировании Transport Layer Security (TLS). Так как это не тот же сертификат как веб-сайт, который первоначально

запрашивают, большинство браузеров выполняет основные предупреждения. Браузеры правильно обрабатывают перенаправление и представление другого сертификата как проблема безопасности. Нет никакого обходного пути для этого, и нет никакого пути к коммутатору для спуфинга исходного сертификата веб-сайта.

Окончательный результат

Клиентский компьютер включает и выполняет MAB. MAC-адрес не известен, таким образом, ISE выдвигает атрибуты перенаправления назад к коммутатору. Пользователь пытается перейти к веб-сайту и перенаправлен.





Когда аутентификация Страницы входа успешна, ISE возвращается порт коммутатора через Изменение Авторизации, которая начинает снова аутентификацию MAB Уровня 2.

Однако ISE знает, что это - бывший webauth клиент и авторизует клиента на основе webauth учетных данных (невзирая на то, что это - аутентификация Уровня 2).

В журналах аутентификации ISE аутентификация MAB появляется у основания журнала. Несмотря на то, что это неизвестно, MAC-адрес аутентифицировался и представлялся, и атрибуты webauth были возвращены. Затем, аутентификация происходит с именем пользователя пользователя (т.е. пользователь вводит свои учетные данные в Странице входа). Сразу после аутентификации, новая аутентификация Уровня 2 происходит с именем

пользователя как учетные данные; этот опознавательный шаг состоит в том, куда можно возвратиться, приписывает такую динамическую LAN.

Проверка

В настоящее время для этой конфигурации нет процедуры проверки.

Устранение неполадок

Для этой конфигурации в настоящее время нет сведений об устранении проблем.

Дополнительные сведения

- Cisco Identity Services Engine
- Справочник по командам платформы Cisco Identity Services Engine
- Интеграция ISE (платформа Identity Services Engine) с WLC Cisco (контроллер беспроводной локальной сети)
- Запросы комментариев (RFC)
- Cisco Systems – техническая поддержка и документация