Беспроводной BYOD с платформой Identity Services Engine

Содержание

Введение

Платформа Cisco Identity Services Engine (ISE) является сервером политик Cisco следующего поколения, который предоставляет инфраструктуру проверки подлинности и авторизация решению Cisco TrustSec. Это также предоставляет два других важных сервиса:

- Первый сервис должен предоставить способ представить тип оконечного устройства автоматически на основе атрибутов, которые Cisco ISE получает от различных источников информации. Этот сервис (названный Профилировщиком) предоставляет эквивалентные функции тому, что Cisco ранее предложила с устройством Cisco NAC Profiler.
- Другой важный сервис, который предоставляет Cisco ISE, должен просмотреть совместимость оконечной точки; например, установка программного обеспечения AV/AS и ее законность файла определения (известный как Положение). Cisco ранее предоставляла эту точную функцию положения только устройством Cisco NAC.

Cisco ISE предоставляет эквивалентный уровень функциональности, и это интегрировано с механизмами аутентификации 802.1X.

Cisco ISE, интегрированный с контроллерами беспроводной локальной сети (WLC), может предоставить копировальные механизмы мобильных устройств, такие как продукты компании Apple Apple (iPhone, iPad и iPod), смартфоны на базе Android и другие. Для пользователей 802.1X Cisco ISE может предоставить тот же уровень сервисов, таких как сканирование положения и профилирование. Гостевые сервисы на Cisco ISE могут также быть интегрированы с WLC Cisco путем перенаправления запросов web-аутентификации к Cisco ISE для аутентификации.

Этот документ представляет беспроводное решение для BYOD, такого как обеспечение дифференцируемого доступа на основе известных оконечных точек и пользовательской политики. Этот документ не предоставляет полное решение BYOD, но служит для демонстрации простого варианта использования динамического доступа. Другие примеры конфигурации включают использование портала спонсора ISE, где привилегированный пользователь может спонсировать гостя для инициализации беспроводного гостевого доступа.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

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

- Контроллер беспроводной локальной сети Cisco 2504 или 2106 с версией программного обеспечения 7.2.103
- Catalyst 3560 – 8 портов
- WLC 2504
- Платформа Identity Services Engine 1.0MR (версия образа сервера VMware)
- Windows 2008 Server (образ VMware) — 512M, диск на 20 ГБActive DirectoryDNSDHCPСервисы сертификации

Топология

Условные обозначения

Дополнительные сведения об условных обозначениях см. в документе Условные обозначения технических терминов Cisco.

NAC RADIUS контроллера беспроводной локальной сети и обзор CoA

Эта установка позволяет WLC искать пары значение-атрибут перенаправления URL, прибывающие из сервера RADIUS ISE. Это находится только на WLAN, который связан к интерфейсу с включенным значением NAC RADIUS. Когда AV-пара Cisco для Перенаправления URL получена, клиент помещен в состояние POSTURE_REQD. Это - в основном то же как состояние WEBAUTH_REQD внутренне в контроллере.

Когда сервер RADIUS ISE считает, Клиент является Posture_Compliant, он выполняет CoA ReAuth. Session_ID используется для связывания его. С этим новым AuthC (переаутентификация) это не передает пары значение-атрибут URL-Redirec. Поскольку нет никаких пар значение-атрибут Перенаправления URL, WLC знает, что клиент не требует Положения больше.

Если значение NAC RADIUS не включено, WLC игнорирует VSA Перенаправления URL.

CoA-ReAuth: Это включено со Значением RFC 3576. Возможность ReAuth была добавлена к существующим командам CoA, которые поддерживались ранее.

Значение NAC RADIUS является взаимоисключающим от этой возможности, невзирая на то, что это требуется для CoA работать.

ACL перед положением: Когда клиент находится в состоянии POSTURE_REQ, поведение по умолчанию WLC должно заблокировать весь трафик кроме DHCP/DNS. ACL Перед положением (которым это вызывают в паре значение-атрибут acl перенаправления URL) применен к клиенту, и что разрешено в том ACL, то, чего может достигнуть клиент.

Предподлинный ACL по сравнению с Заменой VLAN: Карантин или AuthC VLAN, который отличается от VLAN Доступа, не поддерживаются в 7.0MR1. При установке VLAN от Сервера политик это будет VLAN для всего сеанса. Никакие изменения VLAN не необходимы после первого AuthZ.

NAC RADIUS контроллера беспроводной локальной сети и поток функции CoA

Когда клиент аутентифицируется на подтверждении состояния NAC и конечном сервере, ниже рисунка предоставляет подробную информацию обмена сообщениями.

1. Клиент аутентифицирует аутентификацию dot1x использования.
2. ДОСТУП К СЕРВЕРУ RADIUS Признает, что переносы перенаправили URL для порта 80 и предподлинных ACL, который включает IP-адреса разрешения и порты или карантинную VLAN.
3. Клиент будет перенаправлен к URL, предоставленному на доступе, принимают и помещают в новое состояние, пока не сделано подтверждение состояния. Клиент в этом состоянии говорит с сервером ISE, и проверьте себя против политики, настроенной на сервере NAC ISE.
4. Агент NAC на клиенте инициирует подтверждение состояния (трафик к порту 80): Агент передает запрос на обнаружение HTTP к порту 80, который принимают перенаправления контроллера к URL, предоставленному на доступе. ISE знает, что клиент, пытающийся достигнуть и, непосредственно отвечает клиенту. Таким образом, клиент учится о IP - сервере ISE и с этого времени, говорит клиент непосредственно с сервером ISE.
5. WLC позволяет этот трафик, потому что ACL настроен для разрешения этого трафика. В случае замены VLAN соединен трафик так, чтобы это достигло сервера ISE.
6. Как только клиент ISE завершает оценку, CoA-Req RADIUS с reauth сервисом передается WLC. Это инициирует повторную проверку подлинности клиента (передачей, ЗАПУСКАЮТСЯ EAP). Как только повторная проверка подлинности успешно выполняется, ISE передает доступ, принимают с новым ACL (если таковые имеются) и никакое перенаправление URL или VLAN доступа.
7. WLC имеет поддержку CoA-Req и Req Разъединения согласно RFC 3576. WLC должен поддержать CoA-Req для переподлинного сервиса согласно RFC 5176.
8. Вместо загружаемых списков ACL предварительно сконфигурированные ACL используются на WLC. Сервер ISE просто передает название ACL, которое уже настроено в контроллере.
9. Этот дизайн должен работать и для VLAN и для случаев ACL. В случае замены VLAN мы просто перенаправляем порт 80, перенаправлен и позволяет (соединяют) отдых трафика на карантинной VLAN. Для ACL предподлинный ACL, полученный на доступе, принимает, применен.

Этот рисунок предоставляет визуальное отображение этого потока функции:

Обзор профилирования ISE

Сервис профилировщика Cisco ISE предоставляет функциональность в обнаружении, определении местоположения и определении возможностей всех подключенных оконечных

точек в вашей сети, независимо от их типов устройства, чтобы гарантировать и поддержать соответствующий доступ к вашей корпоративной сети. Это прежде всего собирает атрибут или ряд атрибутов всех оконечных точек в вашей сети и классифицирует их согласно их профилям.

Профилировщик состоит из этих компонентов:

- Датчик содержит много зондов. Зонды перехватывают сетевые пакеты путем запроса устройств доступа к сети и передают атрибуты и их значения атрибута, которые собраны с оконечных точек на анализатор.
- Анализатор оценивает оконечные точки с помощью настроенной политики и идентификационных групп для соответствия с атрибутами и их собранными значениями атрибута, который классифицирует оконечные точки указанной группе и хранит оконечные точки профилем, с которым совпадают, в базе данных Cisco ISE.

Для обнаружения мобильного устройства это, рекомендуют использовать комбинацию этих зондов для надлежащей идентификации устройства:

- RADIUS (Calling-Station-ID): предоставляет MAC-адрес (OUI)
- DHCP (имя хоста): Имя хоста – имя хоста по умолчанию может включать тип устройства; пример: iPad jsmith
- DNS (инвертируют поиск IP): FQDN - имя хоста по умолчанию может включать тип устройства
- HTTP (User-Agent): Подробные данные об определенном типе мобильного устройства

В данном примере iPad профилировщик перехватывает информацию о web-браузере от атрибута User-Agent, а также других атрибутов HTTP из сообщений запроса, и добавляет их к списку атрибутов оконечной точки.

Создайте внутренних идентификационных пользователей

Active Directory (AD) MS не требуется для простого тестового. ISE может использоваться в качестве единственного идентификационного хранилища, которое включает дифференцирующийся пользовательский доступ для доступа и гранулированного правила управления политиками.

При выпуске ISE 1.0, с помощью AD интеграции, ISE может использовать AD группы в политике авторизации. Если хранилище внутреннего пользователя ISE используется (никакая AD интеграция), группы не могут использоваться в политике в сочетании с идентификационными группами устройства (определенный дефект, который будет решен в ISE 1.1). Поэтому только отдельные пользователи могут дифференцироваться, такие как сотрудники или подрядчики, когда используется в дополнение к идентификационным группам устройства.

Выполните следующие действия:

1. Откройте окно браузера для https://адрес ISEip.
2. Перейдите к **администрированию> Управление идентификацией> Личности**.
3. Выберите **Users**, затем **нажмите Add** (Пользователь Доступа к сети). Введите эти пользовательские значения и назначьте на группу Сотрудника:Name: сотрудникPassword: XXXX

4. **Нажмите кнопку Submit (Отправить).**Name: подрядчикPassword: XXXX
5. Подтвердите, что созданы обе учетных записи.

Добавьте контроллер беспроводной локальной сети к ISE

Любое устройство, которое инициирует Запросы RADIUS к ISE, должно иметь определение в ISE. Эти сетевые устройства определены на основе их IP-адреса. Определения сетевого устройства ISE могут задать Диапазоны IP-адресов, таким образом позволяющие определение представлять множественные существующие устройства.

Вне какого требуется для связи RADIUS, определения сетевого устройства ISE содержат параметры настройки для другой связи ISE/устройства, такие как SNMP и SSH.

Другой важный аспект определения сетевого устройства соответственно группирует устройства так, чтобы эта группировка могла быть усилена в политике доступа к сети.

В этом осуществлении настроены определения устройства, требуемые для вашей лабораторной работы.

Выполните следующие действия:

1. От ISE переходят **к администрированию> Сетевые ресурсы> Сетевые устройства**.
2. От Сетевых устройств **нажмите Add**. Введите IP-адрес, параметр аутентификации проверки маски, затем введите 'Cisco' для общего секретного ключа.
3. Сохраните запись WLC и подтвердите контроллер в списке.

Настройте ISE для беспроводной аутентификации

ISE должен быть настроен для аутентификации беспроводных клиентов 802.1x и использовать Active Directory в качестве идентификационного хранилища.

Выполните следующие действия:

1. От ISE перешли к **Политике> Аутентификация**.
2. Нажмите для расширения Dot1x> Wired_802.1X (-).
3. Щелкните по значку механизма для **Добавления Условия от Библиотеки**.
4. От выпадающего выбора условия выберите **Compound Condition> Wireless_802.1X**.
5. Установите условие Экспресса к **OR**.
6. Расширьтесь после того, как позволят опцию протоколов и примут Внутренних пользователей по умолчанию (по умолчанию).
7. Оставьте все остальное в по умолчанию. Нажмите **Save** для выполнения шагов.

Контроллер беспроводной локальной сети начальной загрузки

Соединение WLC к сети

Руководство по развертыванию Контроллера беспроводной локальной сети Cisco 2500 также доступно в Руководстве по развертыванию контроллера беспроводной сети Cisco серии 2500.

Настройте контроллер Использование мастера запуска

```
(Cisco Controller)
 Welcome to the Cisco Wizard Configuration Tool Use the '-' character to backup
 Would you like to terminate autoinstall? [yes]: yes AUTO-INSTALL: process terminated
-- no configuration loaded System Name [Cisco_d9:24:44] (31 characters max):
   ISE-Podx Enter Administrative User Name (24 characters max): admin
   Enter Administrative Password
   (3 to 24 characters): Cisco123
   Re-enter Administrative Password: Cisco123
Management Interface IP Address: 10.10.10.5
Management Interface Netmask: 255.255.255.0
Management Interface Default Router: 10.10.10.1
Management Interface VLAN Identifier (0 = untagged): 0
Management Interface Port Num [1 to 4]: 1
Management Interface DHCP Server IP Address: 10.10.10.10
 Virtual Gateway IP Address: 1.1.1.1
Mobility/RF Group Name: ISE
 Network Name (SSID): PODx
Configure DHCP Bridging Mode [yes][NO]: no
Allow Static IP Addresses [YES][no]: no
 Configure a RADIUS Server now? [YES][no]: no
Warning! The default WLAN security policy requires a RADIUS server.
Please see documentation for more details.
 Enter Country Code list (enter 'help' for a list of countries) [US]: US

Enable 802.11b Network [YES][no]: yes
Enable 802.11a Network [YES][no]: yes
Enable 802.11g Network [YES][no]: yes
Enable Auto-RF [YES][no]: yes
 Configure a NTP server now? [YES][no]: no
Configure the ntp system time now? [YES][no]: yes
Enter the date in MM/DD/YY format: mm/dd/yy
Enter the time in HH:MM:SS format: hh:mm:ss
Configuration correct? If yes, system will save it and reset. [yes][NO]: yes
 Configuration saved!
 Resetting system with new configuration...
Restarting system.
```

Конфигурация соседнего коммутатора

Контроллер подключен к Порту Ethernet на соседнем коммутаторе (Fast Ethernet 1). Порт соседнего коммутатора настроен как магистраль "802.1q" и позволяет все VLAN на транке. Собственный VLAN 10 позволяет интерфейсу управления WLC быть связанным.

Конфигурация портов коммутатора 802.1Q следующие:

```
switchport
switchport trunk encapsulation dot1q
switchport trunk native VLAN 10
switchport mode trunk
end
```

Добавьте серверы проверки подлинности (ISE) к WLC

ISE должен быть добавлен к WLC для включения 802.1X и функции CoA беспроводных оконечных точек.

Выполните следующие действия:

1. Откройте браузер, затем соединитесь с WLC переходной приставки (использующий безопасный HTTP)> https://wlc.
2. Перейдите к **Security> Authentication> Новый**.
3. Введите эти значения:IP-адрес сервера: 10.10.10.70 (проверяют присвоение),Общий secret: ciscoПоддержка RFC 3576 (CoA): включенный (по умолчанию)Все остальное: По умолчанию
4. Нажмите **Apply** для продолжения.
5. Выберите **RADIUS Accounting>, добавляет NEW**.
6. Введите эти значения:IP-адрес сервера: 10.10.10.70Общий secret: ciscoВсе остальное: По умолчанию
7. Нажмите **Apply**, затем сохраните Конфигурацию на WLC.

Создайте динамический интерфейс сотрудника WLC

Выполните эти шаги, чтобы добавить новый динамический интерфейс для WLC и сопоставить его с VLAN Сотрудника:

1. От WLC перейдите к **Контроллеру> Интерфейсы**. Затем нажмите **New**.
2. От WLC перейдите к **Контроллеру> Интерфейсы**. Введите следующее:Имя интерфейса: сотрудникИдентификатор VLAN: 11
3. Введите придерживающееся для интерфейса Сотрудника:Port number: 1Идентификатор VLAN: 11IP-адрес: 10.10.11.5Маска подсети: 255.255.255.0Шлюз: 10.10.11.1DHCP: 10.10.10.10
4. Подтвердите, что создан новый динамический интерфейс сотрудника.

Создайте гостевой динамический интерфейс WLC

Выполните эти шаги, чтобы добавить новый динамический интерфейс для WLC и сопоставить его с Гостевым VLAN:

1. От WLC перейдите к **Контроллеру> Интерфейсы**. Затем нажмите **New**.
2. От WLC перейдите к **Контроллеру> Интерфейсы**. Введите следующее:Имя интерфейса: гостьИдентификатор VLAN: 12
3. Введите их для Гостевого интерфейса:Port number: 1Идентификатор VLAN: 12IP-адрес: 10.10.12.5Маска подсети: 255.255.255.0Шлюз: 10.10.12.1DHCP: 10.10.10.10
4. Подтвердите, что был добавлен гостевой интерфейс.

Добавьте WLAN 802.1x

От начальной начальной загрузки WLC, возможно, был созданный WLAN по умолчанию. Если так, модифицируйте его или создайте новый WLAN для поддержки беспроводной аутентификации 802.1X, как проинструктировано в руководстве.

Выполните следующие действия:

1. От WLC перейдите к **WLAN>, Создают Новый**.
2. Для WLAN введите придерживающееся:Имя профиля: pod1xSSID: то же
3. Для параметров настройки WLAN> Вкладка Общие, используйте придерживающееся:Radio Policy: ВсеИнтерфейс/Группа: управлениеВсе остальное: по умолчанию
4. Для вкладки> Security WLAN> Уровень 2, набор придерживающееся:Уровень 2 Security:WPA+WPA2Политика WPA2 / Шифрование: Включенный / AESПодлинный ключевой Mgmt: 802.1x
5. Для вкладки> Security WLAN> AAA-серверы, набор придерживающееся:Радио-интерфейс перезаписи сервера: отключенныйАутентификация/Учетные серверы: ВключенныйСервер 1: 10.10.10.70
6. Для WLAN> Вкладка Дополнительно, набор придерживающееся:Позвольте замену AAA: включенныйСостояние NAC: NAC радиуса (выбран)
7. Назад к WLAN> Вкладка Общие> Включают WLAN (флажок).

Тестовые динамические интерфейсы WLC

Необходимо осуществить быструю проверку для допустимых интерфейсов сотрудника и гостя. Используйте любое устройство для соединения к WLAN, затем измените присвоение интерфейса WLAN.

1. От WLC перейдите к **WLAN> WLAN**. Нажмите для редактирования безопасного SSID, созданного в более раннем осуществлении.
2. Измените Интерфейс/Интерфейсную группу на **Сотрудника**, затем нажмите **Apply**.
3. Если настроено должным образом, устройство получает IP-адрес от VLAN сотрудника (10.10.11.0/24). Данный пример показывает устройство на iOS, которое получает новый IP-адрес.
4. Как только предыдущий интерфейс был подтвержден, изменяет присвоение интерфейса WLAN на **Гостя**, затем нажимает **Apply**.
5. Если настроено должным образом, устройство получает IP-адрес от гостевого VLAN (10.10.12.0/24). Данный пример показывает устройство на iOS, которое получает новый IP-адрес.
6. **Важно:** Возвратите Интерфейсное присвоение на исходное управление.
7. Нажмите **Apply** и сохраните Конфигурацию на WLC.

Беспроводная Аутентификация для iOS (iPhone/iPad)

Партнер к WLC через аутентифицируемый SSID ВНУТРЕННИЙ ПОЛЬЗОВАТЕЛЬ (или интегрированный, AD Пользователь) использование устройства на iOS, такого как iPhone, iPad или iPod. Пропустите эти шаги если не применимый.

1. На устройстве на iOS перейдите к параметрам настройки WLAN. Включите WIFI, затем выберите включенный SSID 802.1X, созданный в предыдущем разделе.
2. Предоставьте эту информацию для соединения:Username: сотрудник (внутренний – Сотрудник) или подрядчик (внутренний – Подрядчик)Password: XXXX
3. Нажмите для принятия сертификата ISE.
4. Подтвердите, что устройство на iOS получает IP-адрес от управления (VLAN10)

интерфейс.
5. На WLC> Монитор> Клиенты, проверьте информацию об оконечной точке включая использование, состояние и тип EAP.
6. Точно так же сведения о клиенте могут быть предоставлены ISE> Монитор> Страница аутентификации.
7. Нажмите **Подробный** значок для развертки к сеансу для всесторонней информации сеанса.

Добавьте ACL перенаправления положения к WLC

ACL перенаправления положения настроен на WLC, где ISE будет использовать для ограничения клиента для положения. Эффективно и как минимум ACL разрешает трафик между ISE. Дополнительные правила могут быть добавлены в этом ACL в случае необходимости.

1. Перейдите к**> Security WLC> Списки контроля доступа> Списки контроля доступа**. **Щелкните New.**
2. Предоставьте название (REDIRECT POSTURE ACL) для ACL.
3. **Нажмите add new rule** для нового ACL. Установите следующие значения в последовательность ACL #1. Нажмите **Apply** по окончании.Источник: ЛюбойDestination: IP-адрес 10.10.10.70, 255.255.255.255Протокол: любойДействие: Разрешение
4. Подтвердите, что была добавлена последовательность.
5. **Нажать add new rule**. Установите следующие значения в последовательность ACL #2. Нажмите **Apply** по окончании.Источник: IP-адрес 10.10.10.70, 255.255.255.255Destination: ЛюбойПротокол: любойДействие: Разрешение
6. Подтвердите, что была добавлена последовательность.
7. Установите следующие значения в последовательность ACL #3. Нажмите **Apply** по окончании.Источник: ЛюбойDestination: ЛюбойПротокол: UDPИсходный порт: DNSНомер порта: ЛюбойДействие: Разрешение
8. Подтвердите, что была добавлена последовательность.
9. **Нажать add new rule**. Установите следующие значения в последовательность ACL #4. Нажмите **Apply** по окончании.Источник: ЛюбойDestination: ЛюбойПротокол: UDPИсходный порт: ЛюбойНомер порта: DNSДействие: Разрешение
10. Подтвердите, что была добавлена последовательность.
11. Сохраните текущую конфигурацию WLC.

Позвольте представить зонды на ISE

ISE должен быть настроен как зонды для эффективного профилирования оконечных точек. По умолчанию эти опции отключены. Этот раздел показывает, как настроить ISE, чтобы быть зондами.

1. От управления ISE перейдите к **администрированию> Система> Развертывания**.
2. Выберите **ISE**. Нажмите **хост Edit ISE**.
3. От страницы Edit Node выберите Profiling Configuration и настройте придерживающееся:DHCP: Включенный, Все (или по умолчанию)DHCPSPAN: Включенный, Все (или по умолчанию)HTTP: Включенный, Все (или по

умолчанию)RADIUS: включенный, Н/ДDNS: включенный, Н/Д
4. Повторно привяжите устройства (iPhone/iPad/Droid/Mac, и т.д.).
5. Подтвердите личности оконечной точки ISE. Перейдите к **администрированию> Управление идентификацией> Личности**. Щелкните по Endpoints для распечатки то, что было представлено.**Примечание:** Начальное профилирование от зондов RADIUS.

Включите политику профиля ISE для устройств

Из коробки ISE предоставляет библиотеку различных профилей оконечной точки. Выполните эти шаги для включения профилей для устройств:

1. От ISE перейдите к **Политике> Профилирование**.
2. От левой панели разверните **Копировальную Политику**.
3. Нажмите **Apple Device> Apple iPad** и установите придерживающееся:Политика включила: включенныйCreate Matching Identity Group: выбранный
4. Нажмите **Apple Device> iPhone Apple**, установите придерживающееся:Политика включила: включенныйCreate Matching Identity Group: выбранный
5. Нажмите **Android**, установите придерживающееся:Политика включила: включенныйCreate Matching Identity Group: выбранный

Профиль авторизации ISE для перенаправления обнаружения положения

Выполните эти шаги для настройки перенаправления положения политики авторизации, позволяет новым устройствам быть перенаправленными к ISE для правильного обнаружения и профилирования:

1. От ISE перейдите к **Политике> Элементы Политики> Результаты**.
2. Разверните **Авторизацию**. Нажмите **Authorization Profiles** (левая панель) и **нажмите Add**.
3. Создайте профиль авторизации с придерживающимся:Name: Posture_RemediationТип доступа: Access_AcceptСтандартные средства:Обнаружение положения, включенноеОбнаружение положения, ACL REDIRECT POSTURE ACL
4. Нажмите **Submit** для выполнения этой задачи.
5. Подтвердите, что добавлен новый профиль авторизации.

Создайте профиль авторизации ISE для сотрудника

Добавление профиля авторизации для сотрудника позволяет ISE авторизовать и разрешать доступ с назначенными атрибутами. VLAN 11 сотрудника назначен в этом случае.

Выполните следующие действия:

1. От ISE перейдите к **Политике> Результаты**. Разверните **Авторизацию**, затем нажмите **Authorization Profiles** и **нажмите Add**.
2. Введите придерживающееся для профиля авторизации Сотрудника:Name: Employee_WirelessОбщие задачи:VLAN, включеннаяVLAN, sub оценивают 11
3. Нажмите **Submit** для выполнения этой задачи.

4. Подтвердите, что был создан новый профиль авторизации сотрудника.

Создайте профиль авторизации ISE для подрядчика

Добавление профиля авторизации для подрядчика позволяет ISE авторизовать и разрешать доступ с назначенными атрибутами. VLAN 12 подрядчика назначен в этом случае.

Выполните следующие действия:

1. От ISE перейдите к **Политике> Результаты**. Разверните **Авторизацию**, затем нажмите **Authorization Profiles** и **нажмите Add**.
2. Введите придерживающееся для профиля авторизации Сотрудника:Name: Employee_WirelessОбщие задачи:VLAN, включеннаяVLAN, sub оценивают 12
3. Нажмите **Submit** для выполнения этой задачи.
4. Подтвердите, что был создан профиль авторизации Подрядчика.

Политика авторизации для положения/Профилирования устройства

Мало информации известно о новом устройстве, когда она сначала прибудет на сеть, администратор создаст соответствующую политику, чтобы позволить неизвестным оконечным точкам быть определенными прежде, чем разрешить доступ. В этом осуществлении будет создана политика авторизации так, чтобы новое устройство было перенаправлено к ISE для оценки положения (для мобильных устройств, являются бессубъектными, поэтому только профилирование релевантно); оконечные точки будут перенаправлены к присоединенному порталу ISE и определены.

Выполните следующие действия:

1. От ISE перейдите к **Политике> Авторизация**.
2. Существует политика для Представленных Cisco IP Phone. Это вне коробки. Отредактируйте это как политику положения.
3. Введите следующие значения для этой политики:Имя правила: Posture_RemediationIdentity Groups: любойДругие Условия> Создают Новый: (Усовершенствованный) Сеанс> PostureStatusPostureStatus> Равняется: Неизвестный
4. Установите придерживающееся для разрешений:Разрешения> Стандарт: Posture_Remediation
5. **Нажмите Save.Примечание:** Альтернативно пользовательские элементы политики могут быть созданы для добавления простоты использования.

Тестирование политики исправления положения

К простой демонстрации может быть выполнен, чтобы показать, что ISE должным образом представляет новое устройство на основе политики положения.

1. От ISE перейдите к **администрированию> Управление идентификацией> Личности**.

2. Нажмите **Endpoints**. Привяжите и подключите устройство (iPhone в данном примере).
3. Обновите список Оконечных точек. Наблюдайте то, какая информация дана.
4. От оконечного устройства перейдите к:Url : http://www (или 10.10.10.10)Устройство перенаправлено. Примите любое приглашение для сертификатов.
5. После того, как мобильное устройство полностью перенаправило от обновления ISE список Оконечных точек снова. Наблюдайте то, что изменилось. Предыдущая оконечная точка (например, Устройство Apple) должна была измениться на 'Apple-iPhone'etc. Причина состоит в том, что Проверка HTTP эффективно получает информацию о user-agent как часть процесса того, чтобы быть перенаправленным к присоединенному порталу.

Политика авторизации для дифференцируемого доступа

После успешного тестирования авторизации положения продолжите создавать политику для поддержки дифференцируемого доступа для Сотрудника и Подрядчика с известными устройствами и другим назначением VLAN, определенным для роли пользователя (в этом сценарии, Сотруднике и Подрядчике).

Выполните следующие действия:

1. Перейдите к **ISE> Политика> Авторизация**.
2. Добавьте/Вставьте новое правило выше политики/линии Исправления Положения.
3. Введите следующие значения для этой политики:Имя правила: СотрудникIdentity Groups (расширяется): Endpoint Identity GroupsEndpoint Identity Groups: представленныйПредставленный: Android, Apple iPad или iPhone Apple
4. Для определения дополнительных типов устройства нажмите **+** и добавьте больше устройств (в случае необходимости):Endpoint Identity Groups: представленныйПредставленный: Android, Apple iPad или iPhone Apple
5. Задайте значения следующих Разрешений для этой политики:Другие условия (расширяются): создайте новое условие (расширенная настройка)Условие> Выражение (из списка): InternalUser> НазваниеInternalUser> Название: сотрудник
6. Добавьте условие для Совместимого сеанса положения:Разрешения> Профили> Стандарт: Employee_Wireless
7. **Нажмите Save.** Подтвердите, что политика была добавлена должным образом.
8. Продолжите путем добавления политики Подрядчика. В этом документе предыдущая политика дублирована для ускорения процесса (или, можно вручную настроить для полезного приема).От политики Сотрудника> Действия, нажмите **Duplicate Below**.
9. Отредактируйте следующие поля для этой политики (дубликат):Имя правила: ПодрядчикДругие Условия> InternalUser> Название: подрядчикРазрешения: Contractor_Wireless
10. **Нажмите Save.** Подтвердите, что предыдущая дублированная копия (или новая политика) настроена должным образом.
11. Для предварительного просмотра политики нажмите **Policy-at-a-Glance**.Политика с первого взгляда просматривает, предоставляет объединенное, суммированное и легкое видеть политику.

Тестирование CoA для дифференцируемого доступа

С профилями авторизации и политикой, подготовленной к дифференциации доступа, пора протестировать. Защищая сингл WLAN, сотруднику назначат, VLAN сотрудника и подрядчик будут для VLAN подрядчика. iPhone/iPad Apple используется в следующих примерах.

Выполните следующие действия:

1. Соединитесь с защищенным WLAN (POD1x) с мобильным устройством и используйте эти учетные данные:Username: сотрудникPassword: XXXXX
2. Нажмите **Join**. Подтвердите, что сотрудник является назначенным VLAN 11 (VLAN Сотрудника).
3. Нажмите **Forget эта Сеть**. Подтвердите путем нажатия **Forget**.
4. Перейдите к WLC и удалите существующие клиентские соединения (если то же использовалось в предыдущих шагах). Перейдите, чтобы **Контролировать> Клиенты> MAC-адрес**, затем нажать **Remove**.
5. Другой верный способ очистить предыдущие сеансы клиента состоит в том, чтобы отключить/разрешить WLAN.Перейдите **к WLC> WLAN> WLAN**, затем нажмите WLAN для редактирования.Анчек **Включил>, Применяются** (для отключения).Установите флажок для **Включенного>, Применяются** (для реактивирования).
6. Вернитесь к мобильному устройству. Соединитесь снова с тем же WLAN с этими учетными данными:Username: подрядчикPassword: XXXX
7. Нажмите **Join**. Подтвердите, что пользователь подрядчика является назначенным VLAN 12 (Подрядчик/гостевой VLAN).
8. Можно посмотреть на ISE регистрационное представление в реальном времени в **ISE> Монитор> Авторизации**. Необходимо видеть, что отдельные пользователи (сотрудник, подрядчик) получают дифференцируемые профили авторизации (Employee_WirelessvsContractor_Wireless) в других VLAN.

Гостевой WLAN WLC

Выполните эти шаги для добавления гостевого WLAN, чтобы позволить гостям обращаться к Гостевому Порталу Спонсора ISE:

1. От WLC перейдите к **WLAN>, WLAN> добавляют Новый**.
2. Введите придерживающееся для нового гостевого WLAN:Имя профиля: pod1guestSSID: pod1guest
3. **Щелкните "Применить".**
4. Введите придерживающееся под гостевым WLAN> Вкладка Общие:Статус: ОтключенныйИнтерфейс/Интерфейсная группа: Гость
5. Перейдите к гостевому**> Security WLAN> Layer2** и введите придерживающееся:Безопасность уровня 2: Нет
6. Перейдите к гостевому**> Security WLAN>** вкладка **Layer3** и введите придерживающееся:Безопасность уровня 3: НетВеб-политика: включенныйВеб-Политика sub значение: AuthenticationACL предварительной проверки подлинности: REDIRECT POSTURE ACLВеб-Подлинный тип: Внешний (Перенаправление к внешнему серверу)Url : https://10.10.10.70:8443/guestportal/Login. действие
7. **Щелкните "Применить".**
8. Удостоверьтесь, что **сохранили Конфигурацию WLC**.

Тестирование гостевого WLAN и гостевого портала

Теперь, можно протестировать конфигурацию гостевого WLAN. Это должно перенаправить гостей к гостевому порталу ISE.

Выполните следующие действия:

1. От устройства на iOS, такого как iPhone, перейдите к **сетям Wi-Fi>, Включают**. Затем выберите гостевую сеть POD.
2. Ваше устройство на iOS должно показать действительный IP - адрес от гостевого VLAN (10.10.12.0/24).
3. Откройте браузер Safari и соединитесь с:Url : http://10.10.10.10Перенаправление Web-аутентификации появляется.
4. Нажмите **Continue**, пока вы не поступили в Гостевую Страницу портала ISE.Следующий типовой снимок экрана показывает устройство на iOS на Гостевом Входе в систему Портала. Это подтверждает, что корректная настройка для WLAN и Гостевого Портала ISE активна.

Беспроводные сети ISE спонсируемый гостевой доступ

ISE может быть настроен, чтобы позволить гостям спонсироваться. В этом случае вы настроите гостевую политику ISE, чтобы позволить или Внутреннему или AD домену (если интегрировано) пользователи спонсировать гостевой доступ. Вы также настроите ISE, чтобы позволить спонсорам просматривать (дополнительный) пароль гостевого пользователя, который полезен этой лабораторной работе.

Выполните следующие действия:

1. Добавьте пользователя сотрудника к группе SponsorAllAccount. Существуют другие способы сделать это: пойдите непосредственно к группе, или отредактируйте пользователя и назначьте группу. Для данного примера перейдите к **администрированию> Управление идентификацией> Группы> User Identity Groups**. Затем нажмите **SponsorAllAccount** и добавьте пользователя сотрудника.
2. Перейдите к **администрированию> Гостевой менеджмент> Sponsor Groups**.
3. Нажмите **Edit**, затем выберите **SponsorAllAccounts**.
4. Выберите Authorization Levels и установите придерживающееся:Обзорный пароль гостевого пользователя: Да
5. Нажмите **Save** для выполнения этой задачи.

Поддержка гостя

Ранее, вы настроили соответствующую гостевую политику и группы, чтобы позволить AD пользователю домена спонсировать временных гостей. Затем, вы обратитесь к Порталу Спонсора и создадите временный гостевой доступ.

Выполните следующие действия:

1. От браузера перейдите к любому из этих URL: http://<ip ise>:8080/sponsorportal/**или**

https://<ip ise>:8443/sponsorportal/. Затем войдите с придерживающимся:Username: aduser (Active Directory), сотрудник (Внутренний пользователь)Password: XXXX
2. От страницы Sponsor нажмите **Create Single Guest User Account**.
3. Для временного гостя добавьте придерживающееся:Имя: Требуемый (например, Сэм)*Фамилия: Требуемый (например, Джонс)Роль группы: гостьПрофиль времени: DefaultOneHourTime Zone (Часовой пояс): Любой/По умолчанию
4. **Нажмите кнопку Submit (Отправить).**
5. Гостевая учетная запись создана на основе вашей предыдущей записи. Обратите внимание на то, что пароль видим (от предыдущего осуществления) в противоположность хэшу ***.
6. Оставьте это окно открытым показом Имени пользователя и пароля для гостя. Вы будете использовать их для тестирования Гостевого Входа в систему Портала (затем).

Тестирование гостевого портального доступа

С новой гостевой учетной записью, созданной AD пользователем/спонсором, пора протестировать гостевой портал и доступ.

Выполните следующие действия:

1. На предпочтительном устройстве (в этом случае iOS Apple / iPad), соединитесь с Гостевым SSID Переходной приставки и проверьте IP-адрес / подключение.
2. Используйте браузер и попытайтесь перейти к http://www.Вы перенаправлены к Гостевой Странице входа Портала.
3. Войдите в использование гостевой учетной записи, созданной в предыдущем осуществлении.Если успешный, страница политики допустимого использования появляется.
4. Проверка **Принимает условия использования**, затем **нажимает кнопку Принять**.Исходный URL завершен, и оконечная точка является доступом разрешен как гостем.

Конфигурация сертификата

Для обеспечения связи с ISE определите, является ли связь отнесенной аутентификацией или для управления ISE. Например, для конфигурации с помощью веб-UI ISE, сертификаты X.509 и цепочки доверия сертификата должны быть настроены для включения асимметричного шифрования.

Выполните следующие действия:

1. От вашего проводного связанного ПК откройте окно браузера для https://AD/certsrv.**Примечание:** Используйте безопасный HTTP.**Примечание:** Используйте Mozilla Firefox или Internet Explorer MS для доступа к ISE.
2. Войдите как администратор/Cisco123.
3. Нажмите **Download a CA certificate, цепочку сертификатов или CRL**.
4. Нажмите **Download CA certificate** и сохраните его (обратите внимание на местоположение сохранения).

5. Откройте окно браузера для https://<ISE переходной приставки>.
6. Перейдите **к администрированию> Система> Сертификаты> Сертификаты полномочий Сертификатов**.
7. Выберите операцию **Certificate Authority Certificates** и перейдите к ранее загруженному свидетельству CA.
8. Выберите **Trust для клиента с EAP-TLS**, затем подвергнитесь.
9. Подтвердите, что CA был добавлен доверяемый как узел CA.
10. От браузера перейдите **к администрированию> Система> Сертификаты> Сертификаты полномочий Сертификатов**.
11. **Нажмите Add**, затем **Генерируйте Запрос подписи сертификата**.
12. Отправьте эти значения:Предмет сертификата: CN=ise.corp.rf-demo.comДлина ключа: 2048
13. Приглашения ISE, что CSR доступен на странице CSR. **Нажмите кнопку OK.**
14. Выберите CSR от страницы ISE CSR и нажмите **Export**.
15. Сохраните файл к любому местоположению (например, Загрузки, и т.д.)
16. Файл будет сохранен как *.pem.
17. Найдите файл CSR и отредактируйте с любым Notepad/Wordpad/TextEdit.
18. Скопируйте содержание (Выберите все> Копия).
19. Откройте окно браузера для https://<AD переходной приставки>/certsrv.
20. Нажмите **Request сертификат**.
21. Нажмите для отправки **усовершенствованного запроса сертификата**.
22. Вставьте содержание CSR в Поле Сохраненного запроса.
23. Выберите **Web Server** как Шаблон сертификата, затем нажмите **Submit**.
24. Выберите **закодированный DER**, затем нажмите **сертификат Download**.
25. Сохраните файл к известному местоположению (например, Загрузки)
26. Перейдите **к администрированию> Система> Сертификаты> Сертификаты полномочий Сертификатов**.
27. **Нажмите Add>, Связывают Сертификат CA**.
28. Перейдите к, ранее загрузил сертификат CA.
29. Выберите **Protocol EAP** и **Management Interface**, затем нажмите **Submit**.
30. Подтвердите, что CA был добавлен доверяемый как узел CA.

Windows 2008 Active Directory Integration

ISE может связаться непосредственно с Active Directory (AD) для пользователя/аутентификации компьютера или для получения атрибутов пользователя сведений авторизации. Для передачи с AD к ISE нужно 'присоединиться' к AD домену. В этом осуществлении вы соедините ISE с AD доменом и подтвердите, что AD связь работает правильно.

Выполните следующие действия:

1. Для соединения ISE с AD доменом, от ISE переходят **к администрированию> Управление идентификацией> Внешние Идентификационные Источники**.
2. От левой панели (Внешние Идентификационные Источники), выберите **Active Directory**.
3. На правой стороне выберите вкладку **Connection** и введите придерживающееся:Имя домена: corp.rf-demo.comИдентификационное название магазина: AD1
4. Нажмите **Test Connection**. Введите AD имя пользователя (aduser/Cisco123), затем

нажмите **OK**.
5. Подтвердите, что Состояние проверки показывает **Следовавший Тест**.
6. Выберите Show Detailed Log и наблюдайте подробные данные, полезные для устранения проблем. **Для продолжения нажмите кнопку OK.**
7. Нажмите **Save Configuration**.
8. Нажмите **Join**. Введите AD пользователя (администратор/Cisco123), затем нажмите **OK**.
9. Подтвердите, что Состояние работы Соединения показывает **Следовавший**, затем нажмите **OK** для продолжения.Статус Подключения к серверу показывает **СВЯЗАННЫЙ**. Если это Изменения статуса когда-либо, Тестовое подключение поможет решать проблемы с AD операциями.

Добавьте группы Active Directory

Когда AD группы добавлены, более тонкая настройка позволена по политике ISE. Например, AD группы могут дифференцироваться функциональными ролями, такими как Сотрудник или группы Подрядчика, без связанного дефекта, являющегося опытным в предыдущих упражнениях ISE 1.0, где политика была ограничена только пользователями.

В этой лабораторной работе только используются Пользователи домена и/или группа Сотрудника.

Выполните следующие действия:

1. От ISE перейдите **к администрированию> Управление идентификацией> Внешние Идентификационные Источники**.
2. Выберите вкладку **Active Directory> Groups**.
3. Нажмите **+Add**, затем **Select Groups Из Каталога**.
4. В последующем окне (Выбирают Группы каталогов), примите настройки по умолчанию для домена (corp-rf-demo.com) и Фильтр (*). Затем нажмите **Retrieve Groups**.
5. Выберите коробки для групп **Сотрудника** и **Пользователей домена**. **По окончании нажмите OK.**
6. Подтвердите, что группы были добавлены к списку.

Добавьте идентификационную исходную последовательность

По умолчанию ISE собирается использовать Внутренних пользователей для опознавательного хранилища. Если AD добавлен, порядок приоритетов последовательности может быть создан для включения AD, который ISE будет использовать для проверки для аутентификации.

Выполните следующие действия:

1. От ISE перейдите к **администрированию> Управление идентификацией> Идентификационные Исходные Последовательности**.
2. Нажмите **+Add** для добавления новой последовательности.
3. Введите новое имя: **AD_Internal**. Добавьте все доступные источники к полю Selected. Затем переупорядочивание по мере необходимости так, чтобы AD1 был перемещен в

вершину списка. **Нажмите кнопку Submit (Отправить).**
4. Подтвердите, что последовательность была добавлена к списку.

Беспроводные сети ISE спонсируемый гостевой доступ с интегрированным AD

ISE может быть настроен, чтобы позволить гостям спонсироваться с политикой, чтобы позволить AD пользователям домена спонсировать гостевой доступ.

Выполните следующие действия:

1. От ISE перейдите к **администрированию> Гостевой менеджмент> Параметры настройки**.
2. Разверните **Спонсора** и нажмите **Authentication Source**. Затем выберите **AD_Internal** как Последовательность хранилища идентификаторов.
3. Подтвердите AD_Internal как последовательность хранилища идентификаторов. **Нажмите Save.**
4. Перейдите к **администрированию> Гостевой менеджмент> Групповая политика Спонсора**.
5. Вставьте Новую Политику Выше первого правила (нажмите значок **Действий** от права).
6. Для новой Групповой политики Спонсора создайте придерживающееся:Имя правила: Пользователи доменаIdentity Groups: любойДругие Условия: (Создайте Новый / Усовершенствованный),> AD1AD1: внешние группыВнешние группы AD1> Равняются> corp.rf-demo.com/Users/Domain Пользователи
7. В Sponsor Groups, набор придерживающееся:Sponsor Groups: SponsorAllAccounts
8. Перейдите к **администрированию> Гостевой менеджмент> Sponsor Groups**.
9. Выберите для Редактирования> **SponsorAllAccounts**.
10. Выберите Authorization Levels и установите придерживающееся:Обзорный пароль гостевого пользователя: Да

Настройте SPAN на коммутаторе

Настройте SPAN - интерфейс mgt/зонда ISE L2 смежный с интерфейсом управления WLC. Коммутатор может быть настроен к SPAN и другим интерфейсам, таким как гостевой interface vlan и сотрудник.

```
Podswitch(config)#monitor session 1 source vlan10 , 11 , 12
Podswitch(config)#monitor session 1 destination interface Fa0/8
ISE virtual probe interface.
```

Ссылка: Беспроводная аутентификация для Apple Mac OS X

Партнер к WLC через аутентифицируемый SSID как ВНУТРЕННИЙ ПОЛЬЗОВАТЕЛЬ (или интегрированный, AD Пользователь) использование Apple Mac OS X беспроводных портативных ПК. Пропустите если не применимый.

1. На Mac перейдите к параметрам настройки WLAN. Включите WIFI, затем выберите и соединитесь с включенным SSID POD 802.1X, созданным в предыдущем

осуществлении.
2. Предоставьте следующую информацию для соединения:Username: aduser (при использовании AD), сотрудник (внутренний – Сотрудник), подрядчик (внутренний – Подрядчик)Password: XXXX802.1x: АвтоматическийСертификат TLS: НетВ это время портативный ПК не мог бы соединиться. Кроме того, ISE может бросить отказавшее событие следующим образом:`Authentication failed :12514 EAP-TLS failed SSL/TLS handshake because of an unknown CA in the client certificates chain`
3. Перейдите **к Системному Предпочтению> Сеть> Аэропорт>** значение **802.1X** и установите новый SSID POD / Аутентификация профиля WPA как:TLS: отключенныйPEAP: включенныйTTLS: отключенныйEAP-FAST: отключенный
4. Нажмите **OK**, чтобы продолжить и позволить установке быть сохраненной.
5. На экране Network выберите соответствующий SSID + профиль WPA 802.1X и нажмите **Connect**.
6. Система могла бы вызвать для имени пользователя и пароля. Введите AD пользователя и пароль (aduser/XXXX), затем нажмите **OK**.Клиент должен показать **Связанный** через PEAP с действительным IP - адресом.

Ссылка: Беспроводная аутентификация для Microsoft Windows XP

Партнер к WLC через аутентифицируемый SSID как ВНУТРЕННИЙ ПОЛЬЗОВАТЕЛЬ (или интегрированный, AD Пользователь) использование портативного ПК радио Windows XP. Пропустите если не применимый.

Выполните следующие действия:

1. На портативном ПК перейдите к параметрам настройки WLAN. Включите WIFI и соединитесь с включенным SSID POD 802.1X, созданным в предыдущем осуществлении.
2. Обратитесь к свойствам сети для интерфейса WIFI.
3. Перейдите к вкладке **Wireless Networks**. Выберите свойства сети SSID переходной приставки> вкладка Authentication> тип EAP = Защищенный EAP (PEAP).
4. Нажмите EAP Properties.
5. Установите придерживающееся:Проверьте серверный сертификат: ОтключенныйAuthentication method: Защищенный пароль (MSCHAP EAP v2)
6. Нажмите **OK** на всех окнах для завершения этой задачи конфигурации.
7. Клиент Windows XP вызывает для имени пользователя и пароля. В данном примере это - aduser/XXXX.
8. Подтвердите сетевое подключение, IP-адресация (v4).

Ссылка: Беспроводная аутентификация для Microsoft Windows 7

Партнер к WLC через аутентифицируемый SSID как ВНУТРЕННИЙ ПОЛЬЗОВАТЕЛЬ (или интегрированный, AD Пользователь) использование портативного ПК радио Windows 7.

1. На портативном ПК перейдите к параметрам настройки WLAN. Включите WIFI и соединитесь с включенным SSID POD 802.1X, созданным в предыдущем осуществлении.
2. Обратитесь к беспроводному Менеджеру и измените новый беспроводной профиль POD.
3. Установите придерживающееся:Authentication method: PEAPПомните мои учетные данные …: ОтключенныйПроверьте серверный сертификат (расширенная настройка): ОтключенныйМетод аутентификации (реклама. Установка): MSCHAP EAP v2Автоматически используйте мой вход в систему Windows …: Отключенный

Дополнительные сведения

- Cisco Systems – техническая поддержка и документация