ISE со статическим перенаправлением для отдельного примера конфигурации гостевых сетей

Содержание

Введение

Этот документ описывает, как настроить платформу Cisco Identity Services Engine (ISE) со статическим перенаправлением для отдельных гостевых сетей для поддержания резервирования. Это также описывает, как настроить узел политики так, чтобы клиентам не предлагали с предупреждением сертификата неподдающимся проверке.

Предварительные условия

Требования

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- Центральная веб-аутентификация (CWA) Cisco ISE и все связанные компоненты
- Проверка браузера Достоверности сертификата
- Версия 1.2.0.899 Cisco ISE или позже
- Контроллер беспроводной локальной сети Cisco (WLC) Версия 7.2.110.0 или позже (Версия 7.4.100.0 или позже предпочтен),

Примечание: CWA описан в Центральной веб-аутентификации на статье WLC и ISE Configuration Example Cisco.

Используемые компоненты

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

- Версия 1.2.0.899 Cisco ISE
- Cisco действительный WLC (vWLC) версия 7.4.110.0
- Устройство адаптивной защиты Cisco (ASA) версия 8.2.5

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.

Общие сведения

Во многих средах BYOD гостевая сеть полностью изолирована от внутренней сети в De-Militarized Zone (DMZ). Часто, DHCP в гостевом DMZ предлагает Систему Названия общественного достояния (DNS) серверы гостям, потому что единственная услуга, которая предложена, является доступом в Интернет.

Это делает гостевое перенаправление на ISE трудным до Версии 1.2, потому что ISE перенаправляет клиентов к Полному доменному имени (FQDN) для web-аутентификации. Однако с Версиями ISE 1.2 и позже, администраторы могут перенаправить гостей к статическому IP - адресу или имени хоста.

Настройка

Схема сети

Это - логическая диаграмма.

> **Примечание:** Физически, существует контроллер беспроводной локальной сети во внутренней сети, точки доступа (AP) находятся на внутренней сети, и Идентификация Набора сервисов (SSID) привязана на контроллере DMZ. См. документацию для WLC Cisco для получения дополнительной информации.

!--- конфигурацию

Конфигурация на WLC остается неизменной от обычной конфигурации CWA. SSID настроен для разрешения фильтрации по MAC-адресам с Проверкой подлинности RADIUS и точек учета RADIUS к двум или больше узлам политики ISE.

Этот документ фокусируется на конфигурации ISE.

Примечание: В этом примере конфигурации узлы политики являются **jesse-dunkel** (172.18.124.20) и **jesse-maibock** (172.18.124.21).

Когда WLC отправляет запрос Обхода проверки подлинности MAC (MAB) RADIUS к ISE, поток CWA начинается. ISE отвечает с URL перенаправления на контроллер для перенаправления трафика HTTP к ISE. Важно, чтобы RADIUS и трафик HTTP перешли к тому же Узлу Policy Services (PSN), потому что сеанс поддержан на одиночном PSN. Это обычно выполняется с одиночным правилом, и PSN вставляет свое собственное имя хоста в URL CWA. Однако со статическим перенаправлением, необходимо создать правило для каждого PSN, чтобы гарантировать, что RADIUS и трафик HTTP передаются тому же PSN.

Выполните эти шаги для настройки ISE:

1. Установите два правила для перенаправления клиента к IP-адресу PSN. Перейдите к **Политике> Элементы Политики> Результаты> Авторизация> Профили Авторизации**.

   Эти образы показывают информацию для имени профиля **DunkelGuestWireless**:

   Эти образы показывают информацию для имени профиля **MaibockGuestWireless**:

   Примечание: УСЛОВИЕМ ACL является Контрольный список локального доступа (ACL), который настроен на WLC, чтобы позволить клиенту связываться с ISE на аутентификацию. См. Центральную веб-аутентификацию на статье WLC и ISE Configuration Example Cisco для получения дополнительной информации.
2. Настройте полицейских авторизации так, чтобы они совпали на **Сетевом Имени хоста Access:ISE**, приписывают и предоставляют соответствующий профиль авторизации:

   Теперь, когда клиент перенаправлен к IP-адресу, пользователи получают предупреждения сертификата, потому что URL не совпадает с информацией в сертификате. Например, FQDN в сертификате является **jesse-dunkel.rtpaaa.local**, но URL **172.18.124.20**. Вот сертификат в качестве примера, который позволяет браузеру проверять сертификат с IP-адресом:

С использованием записей альтернативного имени субъекта (SAN) браузер может проверить URL, который включает IP-адрес **172.18.124.20**. Три SAN записи должны быть созданы для адресации к различным клиентским несовместимостям.

3. Создайте SAN запись для имени DNS и гарантируйте, что оно совпадает **с CN =** запись от Поля Тема.

4. Создайте две записи, чтобы позволить клиентам проверять IP-адрес; это для обоих имя DNS IP-адреса, а также IP-адреса, который появляется в атрибуте IP-адреса. Некоторые клиенты только обращаются к имени DNS. Другие не принимают IP-адрес в атрибуте имени DNS, но вместо этого ссылаются на атрибут IP-адреса.

   Примечание: Для получения дополнительной информации о генерации сертификата, обратитесь к **Руководству по установке оборудования платформы Cisco Identity Services Engine, Выпуску 1.2**.

Проверка

Выполните эти шаги, чтобы подтвердить, что ваша конфигурация работает должным образом:

1. Чтобы проверить, что оба из правил функциональны, вручную установите порядок PSN ISE, которые настроены на WLAN:

2. Войдите в гостевой SSID, перейдите к **Операции> Аутентификации** в ISE и проверьте, что поражены корректные правила авторизации:

   Начальная аутентификация MAB дана профилю авторизации **DunkelGuestWireless**. Это - правило, которое в частности перенаправляет к **jesse-dunkel**, который является первым узлом ISE. После **gguest01** входов пользователя в систему в даны корректные заключительные разрешения **GuestPermit**.

3. Для очистки сеансов аутентификации от WLC разъедините устройство клиента от беспроводной сети, перейдите для **Мониторинга> Клиенты** на WLC и удалите сеанс из выходных данных. WLC проводит пустой сеанс в течение пяти минут по умолчанию, поэтому для выполнения допустимого теста, необходимо начать снова.

4. Инвертируйте заказ PSN ISE под гостевой конфигурацией WLAN:

5. Войдите в гостевой SSID, перейдите к **Операции> Аутентификации** в ISE и проверьте,

что поражены корректные правила авторизации:

Для второй попытки профиль авторизации **MaibockGuestWireless** правильно поражен для начальной аутентификации MAB. Подобный первой попытке к **jesse-dunkel** (Шаг 2), аутентификация к **jesse-maibock** правильно поражает **GuestPermit** для заключительной авторизации. Поскольку нет никакой специфичной для PSN информации в профиле авторизации **GuestPermit**, одиночное правило может использоваться для аутентификации к любому PSN.

Устранение неполадок

Окно Authentication Details является мощным представлением, которое отображает каждый шаг аутентификации/процесса авторизации. Для доступа к нему перейдите к **Операциям> Аутентификации** и нажмите значок лупы под столбцом Details. Используйте это окно, чтобы проверить, что условия аутентификации/правила авторизации настроены должным образом.

В этом случае поле Policy Server является основной областью фокуса. Это поле содержит имя хоста PSN ISE, которым обслуживается аутентификация:

Сравните запись Сервера политик в условие правила и гарантируйте, что два совпадают (это значение учитывает регистр):

Примечание: Важно помнить, что необходимо разъединить от SSID и очистить запись клиента от WLC между тестами.