Политика ISE на основе примеров конфигурации SSID

Содержание

Введение

Этот документ описывает, как настроить политику авторизации в платформе Cisco Identity Services Engine (ISE) для различения другие идентификаторы наборов сервисов (SSIDs). Организации очень свойственно иметь множественный SSIDs в их беспроводной сети в различных целях. Одна из наиболее распространенных целей состоит в том, чтобы иметь корпоративный SSID для сотрудников и гостевой SSID для посетителей организации.

Это руководство предполагает что:

1. Контроллер беспроводной локальной сети (WLC) установлен и работает для всего включенного SSIDs.
2. Аутентификация работает на весь SSIDs, включенный против ISE.

Другие Документы в этой Серии

- Центральная веб-аутентификация с коммутатором и примером конфигурации платформы Identity Services Engine
- Центральная веб-аутентификация на WLC и примере конфигурации ISE
- Гость ISE Объясняет Пример Конфигурации аутентификации RADIUS/802.1x
- VPN Встроенное Положение с помощью iPEP ISE и ASA

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

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

- Выпуск 7.3.101.0 контроллера беспроводной локальной сети
- Выпуск 1.1.2.145 платформы Identity Services Engine

Более ранние версии также имеют обе из этих функций.

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.

Условные обозначения

Более подробную информацию о применяемых в документе обозначениях см. в описании условных обозначений, используемых в технической документации Cisco.

Настройка

В этом разделе содержатся сведения о настройке функций, описанных в этом документе.

Примечание: Используйте инструмент Command Lookup (только для зарегистрированных пользователей) для того, чтобы получить более подробную информацию о командах, использованных в этом разделе.

Конфигурации

Эти конфигурации используются в данном документе:

- Способ 1: Airespace-Wlan-Id
- Способ 2: Вызванный Station-ID

Только один метод задания конфигурации должен использоваться за один раз. Если и конфигурации внедрены одновременно, сумма, обработанная увеличениями ISE и влиянием, управляет удобочитаемостью. Этот документ рассматривает преимущества и недостатки каждого метода задания конфигурации.

Способ 1: Airespace-Wlan-Id

Каждый Wireless Local Area Network (WLAN), созданный на WLC, имеет ИДЕНТИФИКАТОР WLAN. ИДЕНТИФИКАТОР WLAN отображен на сводной странице WLAN.

Когда клиент соединяется с SSID, Запрос RADIUS к ISE содержит атрибут ИДЕНТИФИКАТОРА WLAN AIRESPACE. Этот простой атрибут используется для создания решений о применении политики в ISE. То, если ИДЕНТИФИКАТОР WLAN не совпадает на распространении SSID через несколька контроллеров, один недостаток к этому атрибуту. Если это описывает ваши развертывания, продолжите к Методу 2.

В этом случае Airespace-Wlan-Id используется в качестве условия. Это может

использоваться в качестве простого условия (отдельно) или в составном условии (в сочетании с другим атрибутом) для достижения нужного результата. Этот документ покрывает оба варианта использования. С двумя SSIDs выше, могут быть созданы эти два правила.

A) Гости должны войти к Гостевому SSID.

B) Корпоративные пользователи должны быть в группе Active Directory (AD) "Пользователями домена" и должны войти к Корпоративному SSID.

Правило A

Правило A имеет всего одно требование, таким образом, можно создать простое условие (на основе значений выше):

1. В ISE перейдите **к Политике> Элементы Политики> Условия> Авторизация> Простые Условия** и создайте новое условие.
2. В Поле имени введите имя условия
3. В Поле описания введите (дополнительное) описание.
4. От выпадающего списка Атрибута выберите **Airespace> Airespace-Wlan-Id - [1]**.
5. От выпадающего списка Оператора выберите **Equals.**
6. От Раскрывающегося списка значенего выберите **2**.
7. **Нажмите Save.**

Правило B

Правило B имеет два требования, таким образом, можно создать составное условие (на основе значений выше):

1. В ISE перейдите **к Политике> Элементы Политики> Условия> Авторизация> Составные Условия** и создайте новое условие.
2. В Поле имени введите имя условия.
3. В Поле описания введите (дополнительное) описание.
4. Выберите **Create New Condition (Advance Option)**.
5. От выпадающего списка Атрибута выберите **Airespace> Airespace-Wlan-Id - [1]**.
6. От выпадающего списка Оператора выберите **Equals.**
7. От Раскрывающегося списка значенего выберите **1**.
8. Нажмите механизм вправо и выберите **Add Attribute/Value**.
9. От выпадающего списка Атрибута выберите **AD1> External Groups**.
10. От выпадающего списка Оператора выберите **Equals.**
11. От Раскрывающегося списка значенего выберите требуемую группу. В данном примере это установлено в Пользователей домена.
12. **Нажмите Save.**

Примечание: Всюду по этому документу мы используем простые Профили Авторизации, настроенные под Политикой> Элементы Политики> Результаты> Авторизация> Профили Авторизации. Они собираются Разрешить Доступ, но могут быть адаптированы для адаптации потребностям развертываний.

Теперь, когда у нас есть условия, мы можем применить их к Политике авторизации. Перейдите **к Политике> Авторизация**. Определите, где вставить правило в список или отредактировать ваше существующее правило.

Гостевое правило

1. Нажмите стрелку вниз направо от существующего правила и выберите **Insert новое правило**.
2. Введите имя для своего гостя, управляют и оставляют идентификационный полевой набор групп Любому.
3. При Условиях нажмите плюс и нажмите **Select Existing Condition from Library**.
4. Под Названием Условия выберите **Simple Condition> GuestSSID**.
5. В соответствии с Разрешениями, выберите соответствующий Профиль Авторизации для своих Гостей.
6. **Нажмите "Готово".**

Корпоративное правило

1. Нажмите стрелку вниз направо от существующего правила и выберите **Insert новое правило**.
2. Введите имя для своего корпоративного правила и оставьте идентификационный полевой набор групп Любому.
3. При Условиях нажмите плюс и нажмите **Select Existing Condition from Library**.
4. Под Названием Условия выберите **Compound Condition> CorporateSSID**.
5. В соответствии с Разрешениями, выберите соответствующий Профиль Авторизации для своих Корпоративных пользователей.
6. **Нажмите "Готово".**

Примечание: Пока вы не нажмете Save в нижней части Списка Политики, никакие изменения, внесенные на этом экране, не будут применены к вашим развертываниям.

Способ 2: Вызванный Station-ID

WLC может быть настроен для передачи названия SSID в атрибуте Вызванного Station-ID RADIUS, который в свою очередь может использоваться в качестве условия на ISE. Преимущество этого атрибута состоит в том, что он может использоваться независимо от того, во что установлен ИДЕНТИФИКАТОР WLAN на WLC. По умолчанию WLC не передает SSID в атрибуте Вызванного Station-ID. Для активации этой опции на WLC перейдите **к Безопасности> AAA> RADIUS> Аутентификация** и установите Тип Идентификатора станции Вызова в MAC AP Address:SSID. Это устанавливает формат Вызванного Station-ID к *<MAC AP, который пользователь подключает с>: <Name> SSID*.

Вы видите, какое Название SSID будет передаваемым от сводной страницы WLAN.

Так как атрибут Вызванного идентификатора станции также содержит MAC-адрес AP, Регулярное выражение (REGEX) используется для соответствия с названием SSID в политике ISE. Оператор 'Соответствия' в конфигурации условия может считать REGEX из Поля значения.

Примеры REGEX

'Запускается с' — например, используйте значение REGEX **^ (Acme).*** — это условие настроено, поскольку CERTIFICATE:Organization СОВПАДАЕТ с 'Acme' (любое соответствие с условием, которое запускается с "Acme").

'Концы с' — например, используйте значение REGEX.*** (mktg) $** — это условие настроено, поскольку CERTIFICATE:Organization СОВПАДАЕТ с 'mktg' (любое соответствие с условием,

которое заканчивается "mktg").

'Содержит' — например, используйте значение REGEX. *** (1234).*** — это условие настроено, поскольку CERTIFICATE:Organization СОВПАДАЕТ '1234' (любое соответствие с условием, которое содержит "1234", такие как Eng1234, 1234Dev, и Corp1234Mktg).

'Не запускается с' — например, используют значение REGEX **^ (?! LDAP).*** — это условие настроено, поскольку CERTIFICATE:Organization СОВПАДАЕТ с 'LDAP' (любое соответствие с условием, которое не запускается с "LDAP", такого как usLDAP или CorpLDAPmktg).

Концы вызванного Station-ID с названием SSID, таким образом, REGEX для использования в данном примере**.* (: <NAME> SSID) $**. Помните это, поскольку вы проходите конфигурацию.

С двумя SSIDs выше, можно создать два правила с этими требованиями:

A) Гости должны войти к Гостевому SSID.

B) Корпоративные пользователи должны быть в AD группе "Пользователями домена" и должны войти к Корпоративному SSID.

Правило A

Правило A имеет всего одно требование, таким образом, можно создать простое условие (на основе значений выше):

1. В ISE перейдите **к Политике> Элементы Политики> Условия> Авторизация> Простые Условия** и создайте новое условие.
2. В Поле имени введите имя условия.
3. В Поле описания введите (дополнительное) описание.
4. От выпадающего списка Атрибута выберите **Radius-> Called-Station-ID - [30]**.
5. От выпадающего списка Оператора выберите **Matches.**
6. От Раскрывающегося списка значенего выбрать.*** (:Guest) $**. Необходимо учитывать регистр.
7. **Нажмите Save.**

Правило B

Правило B имеет два требования, таким образом, можно создать составное условие (на основе значений выше):

1. В ISE перейдите **к Политике> Элементы Политики> Условия> Авторизация> Составные Условия** и создайте новое условие.
2. В Поле имени введите имя условия.
3. В Поле описания введите (дополнительное) описание.
4. Выберите **Create New Condition (Advance Option)**.
5. От выпадающего списка Атрибута выберите **Radius-> Called-Station-Id - [30]**.
6. От выпадающего списка Оператора выберите **Matches.**
7. От Раскрывающегося списка значенего выбрать**.* (:Corporate) $**. Необходимо учитывать регистр.
8. Нажмите механизм вправо и выберите **Add Attribute/Value**.
9. От выпадающего списка Атрибута выберите **AD1> External Groups**.

10. От выпадающего списка Оператора выберите **Equals.**
11. От Раскрывающегося списка значенего выберите требуемую группу. В данном примере это установлено в Пользователей домена.
12. **Нажмите Save.**

Примечание: Всюду по этому документу мы используем простые Профили Авторизации, настроенные под Политикой> Элементы Политики> Результаты> Авторизация> Профили Авторизации. Они собираются Разрешить Доступ, но могут быть адаптированы для адаптации потребностям развертываний.

Теперь, когда условия настроены, применяют их к Политике авторизации. Перейдите **к Политике> Авторизация**. Вставьте правило в список в соответствующем местоположении или отредактируйте существующее правило.

Гостевое правило

1. Нажмите стрелку вниз направо от существующего правила и выберите **Insert новое правило**.
2. Введите имя для своего гостя, управляют и оставляют идентификационный полевой набор групп Любому.
3. При Условиях нажмите плюс и нажмите **Select Existing Condition from Library**.
4. Под Названием Условия выберите **Simple Condition> GuestSSID**
5. В соответствии с Разрешениями, выберите соответствующий Профиль Авторизации для своих Гостей.
6. **Нажмите "Готово".**

Корпоративное правило

1. Нажмите стрелку вниз направо от существующего правила и выберите **Insert новое правило**.
2. Введите имя для своего корпоративного правила и оставьте идентификационный полевой набор групп Любому.
3. При Условиях нажмите плюс и нажмите **Select Existing Condition from Library**.
4. Под Названием Условия выберите **Compound Condition> CorporateSSID**.
5. В соответствии с Разрешениями, выберите соответствующий Профиль Авторизации для своих Корпоративных пользователей.
6. **Нажмите "Готово".**
7. Нажмите **Save** в нижней части списка Политики.

Примечание: Пока вы не нажмете Save в нижней части Списка Политики, никакие изменения, внесенные на этом экране, не будут применены к вашим развертываниям.

Проверка

В настоящее время для этой конфигурации нет процедуры проверки.

Устранение неполадок

В этом разделе описывается процесс устранения неполадок конфигурации.

Чтобы узнать, была ли политика создана должным образом и удостоверяться, ISE получает

надлежащие атрибуты, рассмотрите подробный опознавательный отчёт или для переданного или для ошибки проверки подлинности для пользователя. Выберите **Operations> Authentications** и затем нажмите **Подробный** значок для аутентификации.

Во-первых, проверьте Опознавательную Сводку. Это показывает основы аутентификации, которые включают, какой Профиль Авторизации был предоставлен пользователю.

Если политика будет неправильной, то Опознавательные Подробные данные покажут, какой Airespace-Wlan-Id и какой Вызванный идентификатор станции передавался от WLC. Отрегулируйте свои правила соответственно. Правило Политики авторизации, с которым Совпадают, подтверждает, совпадает ли аутентификация с вашим намеченным правилом.

Эти правила обычно неправильно конфигурируются. Для раскрытия проблемы конфигурации совпадите с правилом против того, что замечено в опознавательных подробных данных. Если вы не видите атрибутов в поле Other Attributes, удостоверьтесь, что должным образом настроен WLC.

Дополнительные сведения

- Cisco Systems – техническая поддержка и документация