Гостевой доступ с использованием электронной почты

В данной статье описано, как разрешить пользователям-гостям регистрировать свои устройства, используя адрес электронной почты. При таком методе аутентификации, на указанный адрес электронной почты будет отправлен PIN-код для доступа к сети.

Добавление источника аутентификации по электронной почте

Для того, чтобы добавить источник аутентификации, выполните следующие действия:

Шаг 1. Перейдите в раздел **Конфигурация → Политики и контроль доступа → Источники аутентификации** и нажмите **Новый внешний источник**, после чего в выпадающем списке выберите **Email**.

Шаг 2. В полях **Имя** и **Описание** укажите значение **email-source**. Также доступны следующие **опциональные** параметры:

- **Список запрещенных доменов** — список доменов (разделенный запятыми), которые запрещены для регистрации с помощью электронной почты. Запрещенные домены проверяются перед разрешенными доменами.
- **Список разрешенных доменов** — список доменов (разделенный запятыми), которые разрешены для регистрации с помощью электронной почты. Разрешенные домены проверяются после запрещенных доменов.
- **Таймаут ссылки активации** — задержка, предоставляемая гостю, который зарегистрировался с подтверждением по электронной почте для входа в свою почту и перехода по ссылке активации;
- **Разрешить локальный домен** — разрешение на принятие самостоятельной регистрации с адреса электронной почты в пределах локального домена;
- **Заменить хост в ссылке активации** — активация этого параметра разрешает изменение имени хоста в ссылке валидации. Для применения изменений будет необходимо перезапустить службу **haproxy**.

Шаг 3. Нажмите **Добавить правило** в строке **Правила аутентификации** и назовите его **catchall**. В качестве действий установите следующие параметры:

- **Роль** — guest;
- **Срок предоставления доступа** — 12 часов.

Сохраните новый источник аутентификации, нажав **Создать**.

Настройка профиля подключения

После того, как вы создали источник аутентификации, необходимо добавить его в профиль подключения. Выполните следующие действия:

Шаг 1. Перейдите в раздел **Конфигурация → Политики и контроль доступа → Профили подключения** и кликните по профилю, который вы хотите использовать, либо создайте новый нажав **Новый профиль подключения**.

Шаг 2. Настройте профиль подключения под свои предпочтения и политики сетевой безопасности.

Шаг 3. В строке Источники нажмите **Добавить источник** и выберите источник, созданный в предыдущем разделе, из выпадающего списка.

Шаг 4. Сохраните профиль подключения.

Captive-портал, связанный с профилем подключения, можно просмотреть в любой момент. Для этого нажмите **Предпросмотр** рядом с названием подключения.

Проверка работы подключения

Для того чтобы проверить работу подключения, выполните следующие действия:

Шаг 1. Отключите и снимите с регистрации клиентское устройство.

Шаг 2. Снова подключите клиентское устройство к сети. При правильной конфигурации, должен появиться Captive-портал с новой опцией регистрации по электронной почте.

Шаг 3. Пройдите регистрацию с помощью электронной почты и убедитесь, что на указанную почту пришло письмо с учетными данными.

Шаг 4. Введите полученные учетные данные на Captive-портале и убедитесь, что вы получили доступ к сети.

ID статьи: 545
Последнее обновление: 3 июл., 2024
Обновлено от: Егоров В.
Ревизия: 4

https://docs.axel.pro/entry/545/