Аутентификация по протоколу SAML

Настройка источника SAML-аутентификации

AxelNAC поддерживает совместную работу SAML-аутентификации в Captive-портале с другими внутренними источниками для определения уровня авторизации пользователя.

Для того, чтобы настроить источник SAML-аутентификации, выполните следующие действия:

Шаг 1. Создайте новый источник аутентификации SAML в AxelNAC. Для этого в разделе **Конфигурация → Политики и контроль доступа → Источники аутентификации** нажмите **Новый внутренний источник** и выберите SAML в выпадающем списке.

Шаг 2. На открывшейся странице заполните обязательные поля:

- **Имя** — имя источника аутентификации;
- **Описание** — описание источника аутентификации, которое будет отображаться в списке существующих источников аутентификации;
- **Идентификатор провайдера услуг** — идентификатор провайдера услуг (AxelNAC). Убедитесь, что он соответствует конфигурации провайдера идентификационных данных;
- **Ключ провайдера услуг (x509)** — поле для загрузки закрытого ключа, который будет использоваться AxelNAC для подписи своих сообщений провайдеру идентификационных данных;
- **Сертификат провайдера услуг (x509)** — поле для загрузки сертификата, связанного с указанным выше ключом;
- **Идентификатор провайдера идентификационных данных** — идентификатор провайдера идентификационных данных;
- **Метаданные провайдера идентификационных данных** — поле для загрузки файла метаданных;
- **Сертификат провайдера идентификационных данных (x509)** — поле для загрузки сертификата провайдера идентификации;
- **Сертификат CA провайдера идентификационных данных** — поле для загрузки сертификата CA провайдера идентификации;
- **Атрибут имени пользователя** — атрибут, который содержит имя пользователя в выражении SAML, который возвращает провайдер идентификационных данных. По умолчанию должно подходить значение **SimpleSAMLphp**;
- **Источник авторизации** — источник, который будет использоваться для сопоставления имени пользователя с определенными в нем правилами. Это позволяет задать роль и продолжительность доступа пользователя.

Файлы сертификатов, ключей и метаданных могут быть загружены напрямую из веб-интерфейса. Для этого нажмите на значок загрузки файла слева от поля.

Шаг 3. Сохраните метаданные провайдера услуг (эти данные понадобятся в шаге 4), нажав **Просмотреть метаданные провайдера услуг** после создания источника аутентификации.

Шаг 4. Настройте провайдера идентификационных данных в соответствии со сгенерированными метаданными, чтобы завершить процесс установления доверия между AxelNAC и провайдером идентификационных данных.

В качестве примера рассмотрим конфигурацию **SimpleSAMLPHP**, которая находится в файле **metadata/saml20-spremote.php**:

```
$metadata ['ID_СУЩНОСТИ_ANAC'] = array (
'AssertionConsumerService' => 'http://ИМЯ_ХОСТА_ПОРТАЛА/saml/assertion',
'SingleLogoutService' => 'http://ИМЯ_ХОСТА_ПОРТАЛА/saml/logoff',
);
```

AxelNAC не поддерживает выход из системы провайдера идентификационных данных SAML. Можно по прежнему указывать URL-адрес в метаданных, но он использоваться не будет.

Passthrough

Чтобы пользователи могли получить доступ к странице входа в систему провайдера идентификационных данных, необходимо активировать Passthrough и добавить домен провайдера в список разрешенных Passthrough. Для этого:

Шаг 1. Перейдите в раздел **Конфигурация → Сетевое взаимодействие → Сети → Фенсинг** .

Шаг 2. Активируйте параметр **Passthrough**.

Шаг 3. Добавьте имя домена провайдера идентификационных данных в список **Домены для Passthrough**.

Шаг 4. Перезапустите службы **iptables** и **pfdns**, чтобы применить изменения.

ID статьи: 549
Последнее обновление: 3 окт., 2024

Обновлено от: Егоров В.
Ревизия: 5

https://docs.axel.pro/entry/549/