Установка с использованием XMLAPI

Создание роли SSO

Для того, чтобы создать роль SSO в МСЭ PaloAlto, необходимо выполнить следующие шаги:

Шаг 1. В веб-интерфейсе МСЭ перейдите в раздел **Device → Admin Roles** и нажмите **+Add**.

Шаг 2. Создайте роль с именем **SSO_Role** и активируйте все параметры на вкладке XML API, подтвердите их нажатием кнопки **OK**.

Создание учетной записи в PAN-OS

После того, как роль создана, необходимо создать пользователя, который будет ассоциироваться с этой ролью. Для этого выполните следующие действия:

Шаг 1. Перейдите в раздел **Device → Administrators** и нажмите **+Add**.

Шаг 2. Во всплывающем окне заполните поля следующим образом:

- **Name:** xmluser;
- **Authentication Profile:** None;
- **Password:** xmluser;
- **Role:** Role Based;
- **Profile:** SSO_Role (профиль, созданный в предыдущей секции);
- **Password Profile:** None.

Получение XML-ключа

Для того, чтобы получить XML-ключ, перейдите по ссылке: https://@IP-АДРЕС_ВАШЕГО_МСЭ/api/?type=keygen&user=xmluser&password=xmluser.

В окне должно отобразиться:

<response status="success">
<result>
<key>
LUFRPT1jeFV6SHd1QnJHaU55dnYvRlFNSkJNeTR6Uzg9TDgzNVlj0=
</key>
</result>
</response>

Конфигурация SSO в AxelNAC

Для настройки интеграции с МСЭ PaloAlto, выполните следующие действия в веб-интерфейсе AxelNAC:

Шаг 1. Перейдите в раздел **Конфигурация → Интеграция → SSO через межсетевой экран (МСЭ)** , нажмите **Новый межсетевой экран** и в выпадающем списке выберите **PaloAlto**.

Шаг 2. В открывшемся окне заполните поля следующим образом:

- **Имя хоста или IP-адрес:** IP-адрес PaloAlto;
- **Транспорт:** HTTP;
- **Секретная фраза или ключ:** используйте ранее сгенерированный ключ;
- **Порт для обслуживания:** 443;
- **Роли:** выберите роли, для которых информация будет транслироваться в МСЭ.

Процесс верификации

Для проверки интеграции:

Шаг 1. Проверьте, что AxelNAC отправляет информацию при регистрации пользователя на портале. Если процесс прошел успешно, в базе данных PaloAlto появится запись.

Шаг 2. Подключитесь к МСЭ по протоколу SSH и выполните следующую команду:

show user ip-user-mapping all

В случае правильной конфигурации будет получен ответ:

admin@PA-VM> show user ip-user-mapping all
IP Vsys From User IdleTimeout(s)
MaxTimeout(s)

---------- ------ ------- ---------- ----------

192.168.100.10 vsys1 XMLAPI domain\user1 Never
Never

Установка с использованием syslog

Данный режим установки не рекомендуется, если SSO не используется для ознакомительного доступа. AxelNAC будет использовать легко поддающиеся подделке UDP-пакеты для связи с МСЭ PaloAlto. Если же требуется шифрование и проверка происхождения сообщений SSO, используйте XML API.

Создание фильтра

Шаг 1. Создайте фильтр для синтаксического анализа строки SSO, которую будет отправлять AxelNAC. Это можно сделать в разделе **User Identification → User Mapping → Syslog Filters** :

- **Syslog Parse File:** ANAC;
- **Type:** Field Identifier;
- **Event String:** Group <axelnac>;
- **Username Prefix:** User <;
- **Username Delimiter:** >;
- **Addres Prefix:** Address <;
- **Address Delimiter:** >.

Шаг 2. Настройте фильтр для использования в приемнике syslog на Palo Alto. Для этого перейдите в раздел **User Identification → User Mapping** и настройте отправителя syslog:

- **Name:** anac.acme.com;
- **Enabled:** Да;
- **Type:** Syslog Sender;
- **Connection Type:** UDP;
- **Filter:** укажите фильтр, созданный в предыдущем шаге.

Конфигурация SSO в AxelNAC

Для настройки интеграции с МСЭ PaloAlto, выполните следующие действия в веб-интерфейсе AxelNAC:

Шаг 1. Перейдите в раздел **Конфигурация → Интеграция → SSO через межсетевой экран (МСЭ)** , нажмите **Новый межсетевой экран** и в выпадающем списке выберите **PaloAlto**.

Шаг 2. В открывшемся окне заполните поля следующим образом:

- **Имя хоста или IP-адрес:** IP-адрес PaloAlto;
- **Транспорт:** Syslog;
- **Роли:** выберите роли, для которых информация будет транслироваться в МСЭ.

Процесс верификации

Для проверки интеграции:

Шаг 1. Проверьте, что AxelNAC отправляет информацию при регистрации пользователя на портале. Если процесс прошел успешно, в базе данных PaloAlto появится запись.

Шаг 2. Подключитесь к МСЭ по протоколу SSH и выполните следующую команду:

show user ip-user-mapping all

В случае правильной конфигурации будет получен ответ:

admin@PA-VM> show user ip-user-mapping all
IP Vsys From User IdleTimeout(s)
MaxTimeout(s)
---------- ------ ------- ---------- ----------

192.168.100.10 vsys1 syslog domain\user1 Never
Never

Если процесс не работает и выдается ошибка **Usage: Socket::inet_ntoa(ip_address_sv)**, убедитесь, что имя хоста сервера AxelNAC правильно разрешено на самом сервере. Если это не так, убедитесь, что файл hosts или DNS-сервер настроены корректно.

ID статьи: 86
Последнее обновление: 24 июл., 2024
Обновлено от: Егоров В.

Ревизия: 3
База знаний AxelNAC -> Документация -> Система контроля доступа к сети «AxelNAC». Версия 1.0.0 -> AxelNAC. Руководство администратора -> Реализация SSO через межсетевой экран (МСЭ) -> МСЭ PaloAlto
https://docs.axel.pro/entry/86/