Интеграция OpenVPN со службой каталога ALD Pro

06/10/2025

Содержание

OpenVPN является серверным приложением, позволяющим обеспечить доступ удаленных сотрудников к локальной сети предприятия по технологии виртуальной частной сети (VPN) с использованием шифрованных каналов.

В настоящей инструкции описана процедура интеграции OpenVPN со службой каталога ALD Pro. Данная интеграция позволяет пользователям устанавливать защищенные VPN-соединения с использованием доменных учетных записей. Пароль на VPN-сервер предоставляется в открытом виде, проверка выполняется через службу SSSD по протоколу Kerberos V5, как при интерактивном входе в систему.

1 Описание стенда

ALSE 1.7.4 - операционная система на всех компьютерах.

ALD.LAN – имя домена.

astravpn.ald.lan - сервер OpenVPN (**версия 2.4.7**) введен в домен **ALD.LAN**

2 Настройка аутентификации на сервере и клиенте OpenVPN

В OpenVPN, начиная с версии 2.0, включена функция, которая позволяет серверу OpenVPN безопасно получать имя пользователя и пароль от подключаемого клиента, чтобы использовать их для аутентификации.

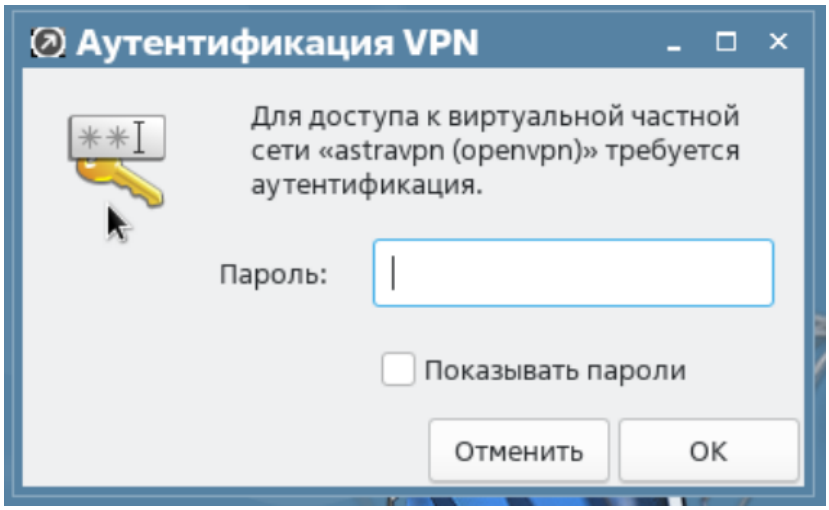
Для активации метода аутентификации необходимо добавить в конфигурацию клиента следующую опцию:

auth-user-pass

Она позволит выводить у клиента OpenVPN окно ввода имени пользователя и пароля для дальнейшей передачи на сервер OpenVPN по защищенному каналу TLS.

На заметку

После настройки клиента VPN на пользовательском рабочем месте, например, используя NetworkManager, клиент VPN запросит только пароль, а в качестве пользователя будет использоваться имя пользователя вашей текущей сессии.



Следующим шагом будет настройка сервера OpenVPN для использования плагина аутентификации. Плагин аутентификации загружается при запуске сервера OpenVPN и будет вызываться каждый раз когда клиент VPN пытается подключиться, передавая имя пользователя и пароль, введенные пользователем. Плагин аутентификации может контролировать разрешено ли подключение, возвращая значение success (0), если разрешено, или failure (1), если запрещено.

Для активации плагина необходимо добавить в конфигурационный файл сервера OpenVPN /etc/openvpn/server.conf следующую строчку:

```
plugin /usr/lib/x86_64-linux-gnu/openvpn/plugins/openvpn-plugin-auth-pam.so openvpn
```

Эта опция сообщит серверу OpenVPN валидировать имя пользователя и пароль, введенные клиентом, используя PAM-модуль **openvpn**.

На заметку

В момент подключения пользователя к VPN-серверу со стороны PAM-службы происходит неудачная попытка обращения к несуществующему файлу конфигурации /etc/pam.d/openvpn, что можно увидеть через системные вызовы с помощью утилиты STRACE. При отсутствии указанного файла PAM-служба обратится к файлу /etc/pam.d/other, в котором определяются настройки по умолчанию. В файле other подключаются все базовые файлы конфигурации для выполнения аутентификации пользователей:

- common-auth,
- common-account,
- common-password,
- common-session.

За детальной информацией о плагине можно обратиться на сайт:

https://github.com/OpenVPN/openvpn/blob/master/src/plugins/auth-pam/README.auth-pam

По умолчанию при подключении клиента к сервер OpenVPN и ввода имени пользователя и пароля в качестве имени пользователя серверу OpenVPN отправится значение Common Name из пользовательского сертификата. В случае, если оно не совпадает с реальным именем пользователя, то аутентификация не пройдет. Для изменения такого поведения необходимо добавить в конфигурационный файл сервера OpenVPN /etc/openvpn/server.conf следующую строку:

```
username-as-common-name
```

После применения данной опции в качестве имени пользователя будет отправляться имя пользователя, под которым запущена текущая сессия.

3 Настройка авторизации на основе HBAC-правил

В случае если у вас развернута инфраструктура ALD Pro и в политиках доступа к узлу используются правила HBAC по умолчанию, то доступ к сервису OpenVPN будет у всех пользователей. Связано это с тем, что во время установки ALD Pro создается правило HBAC **allow_all**, которое разрешает доступ «всех ко всему».

Поэтому для управления авторизацией к сервису OpenVPN на уровне HBAC нужно сначала ограничить область применения правила **allow_all**, например, только группой администраторов.

Внести указанные настройки можно через веб-портал на странице «Групповые политики > Политики доступа к узлу > allow_all > Пользователи» (рис. 1).

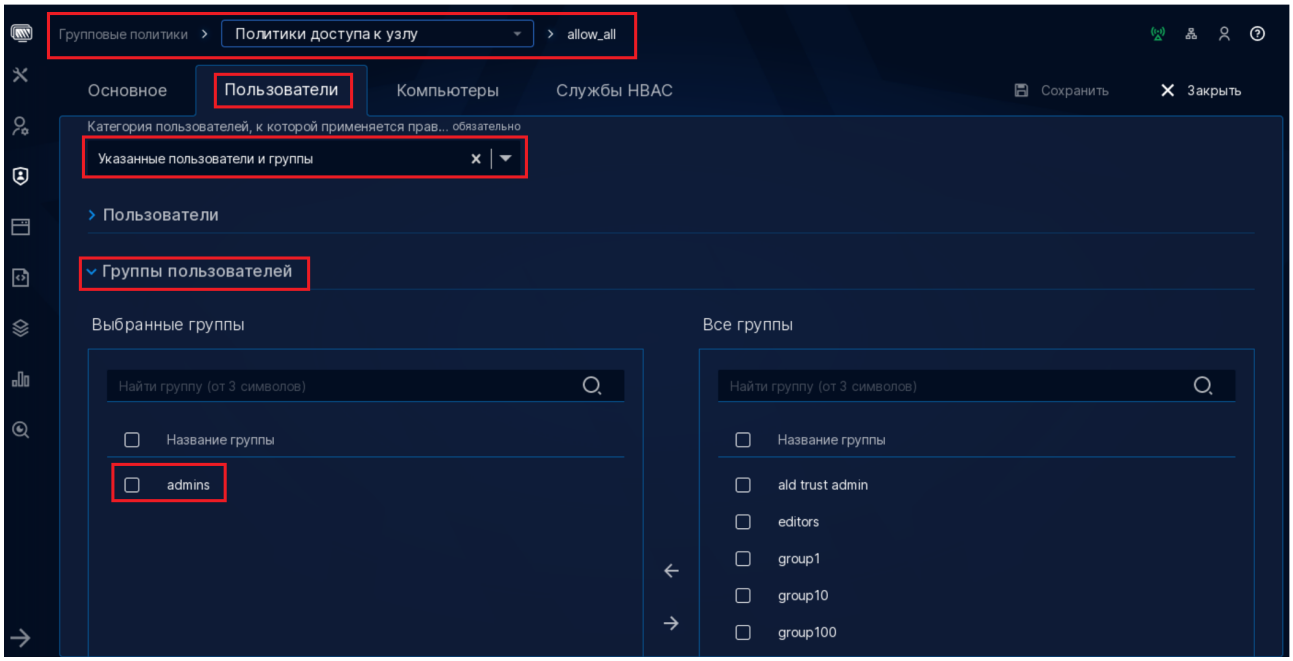


Рисунок 1 - Настройка политики доступа к узлу allow_all

или из командной строки:

```
# kinit admin
# ipa hbacrule-mod allow_all --usercat=''
# ipa hbacrule-mod allow_all --desc='Разрешает администраторам доступ к любому хосту
в домене'
# ipa hbacrule-add-user allow_all --group admins
# ipa hbacrule-show allow_all
```

, где

- kinit admin — аутентификация в системе под учетной записью admin;
- hbacrule-mod — команда, с помощью которой можно модифицировать настройки существующей группы;
- allow_all — имя правила, которое мы хотим модифицировать;
- usercat — ключ, который позволяет изменить категорию для области применения в части пользователей. Может принимать одно из возможных значений: 'all' (все) или '' (пустая строка);
- hbacrule-add-user — команда, с помощью которой можно расширить область применения правила в части пользователей;

- allow_all — имя правила, которое мы хотим модифицировать;
- group — ключ, который позволяет добавить группу пользователей в область применения HBAC-правила;
- admins — имя группы, которая будет добавлена в область применения правила;
- hbacrule-show — команда, с помощью которой можно получить информацию о существующем HBAC-правиле;
- allow_all — имя правила, по которому мы хотим получить информацию.

На заметку

Если из-за неправильной настройки HBAC-правил доступ к хостам будет все же заблокирован, вы сможете подключиться к порталу управления с любого другого компьютера, который не находится в домене, либо зайти на доменную машину под локальным пользователем (если не запрещено политиками), чтобы исправить ошибку. Доступ к порталу управления не регулируется через механизм HBAC.

Если ограничить область действия правила **allow_all** группой администраторов, то для остальных сотрудников компании нужно будет создать правило **allow_computers**, которое предоставит им право входа на обычные компьютеры в домене.

Создадим это правило с использованием веб-интерфейса:

1. Создадим группу хостов **computers**. Откройте страницу «Пользователи и компьютеры > Группы компьютеров» и нажмите кнопку «Новая группа». Введите имя группы, ее описание и нажмите кнопку «Сохранить» (рис. 2).

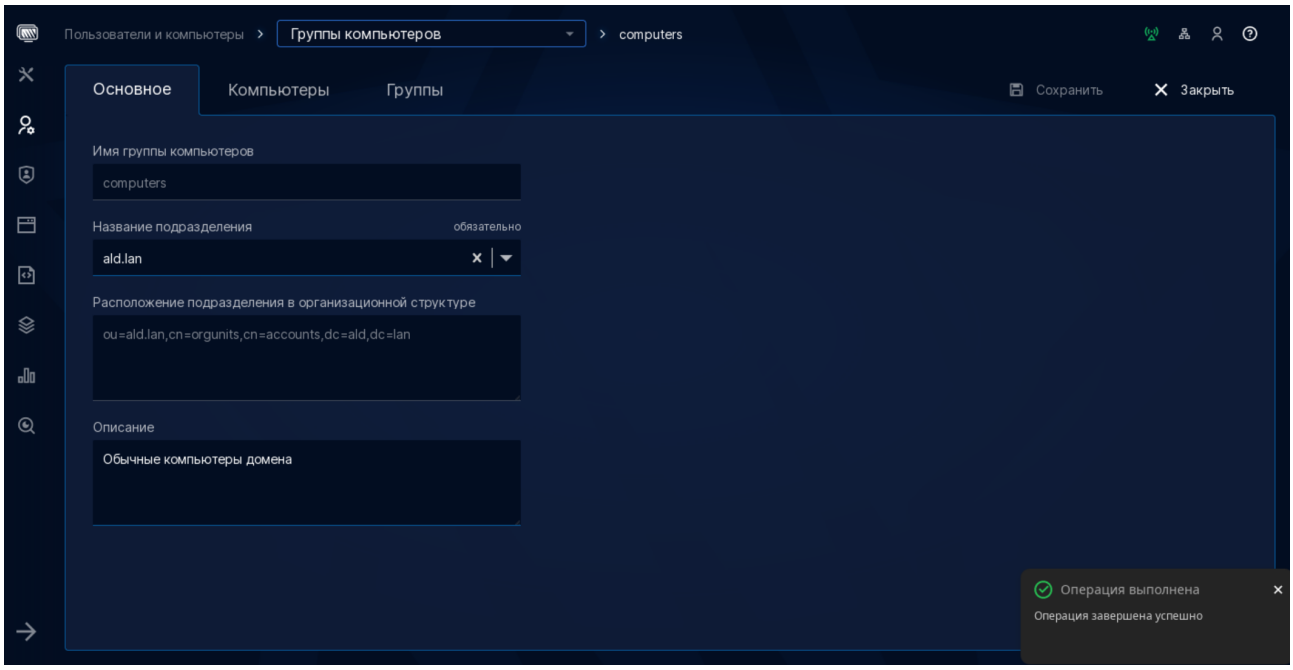


Рисунок 2 - Создание группы хостов **computers**

2. На вкладке «Компьютеры» внесите рабочие станции в список участников группы (рис. 3).

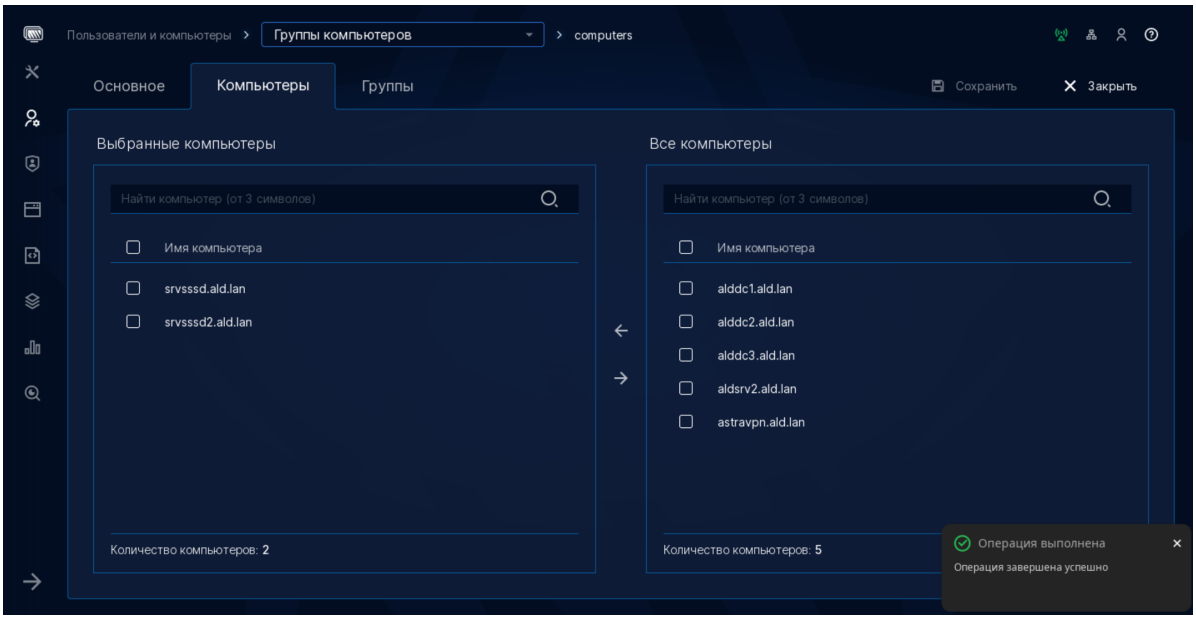
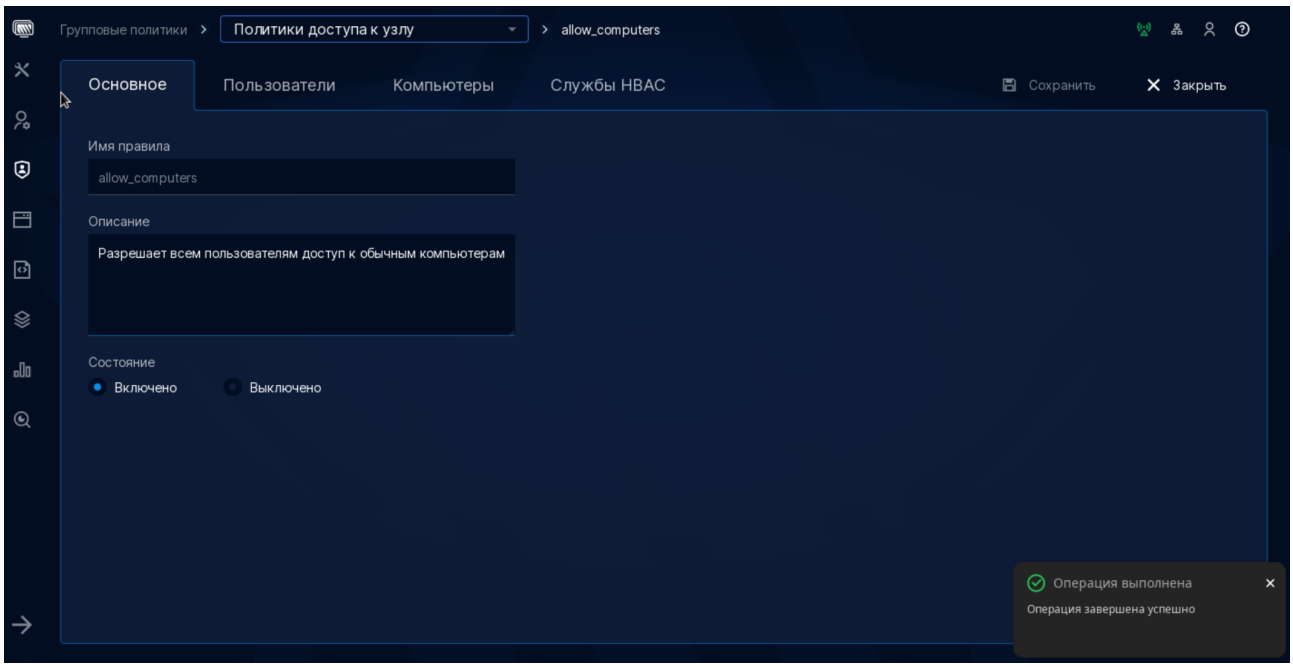


Рисунок 3 — Внесение рабочих станций

3. Создадим HBAC-правило (рис. 4). Откройте страницу «Групповые политики > Политики доступа к узлу > Правила HBAC» и нажмите кнопку «Новое правило». Введите имя правила **allow_computers** и сохраните его. Для созданного правила определите следующую область действия:

- пользователи — любой пользователь;
- хосты — указанные компьютеры и группы, группа computers;
- службы — любая служба.



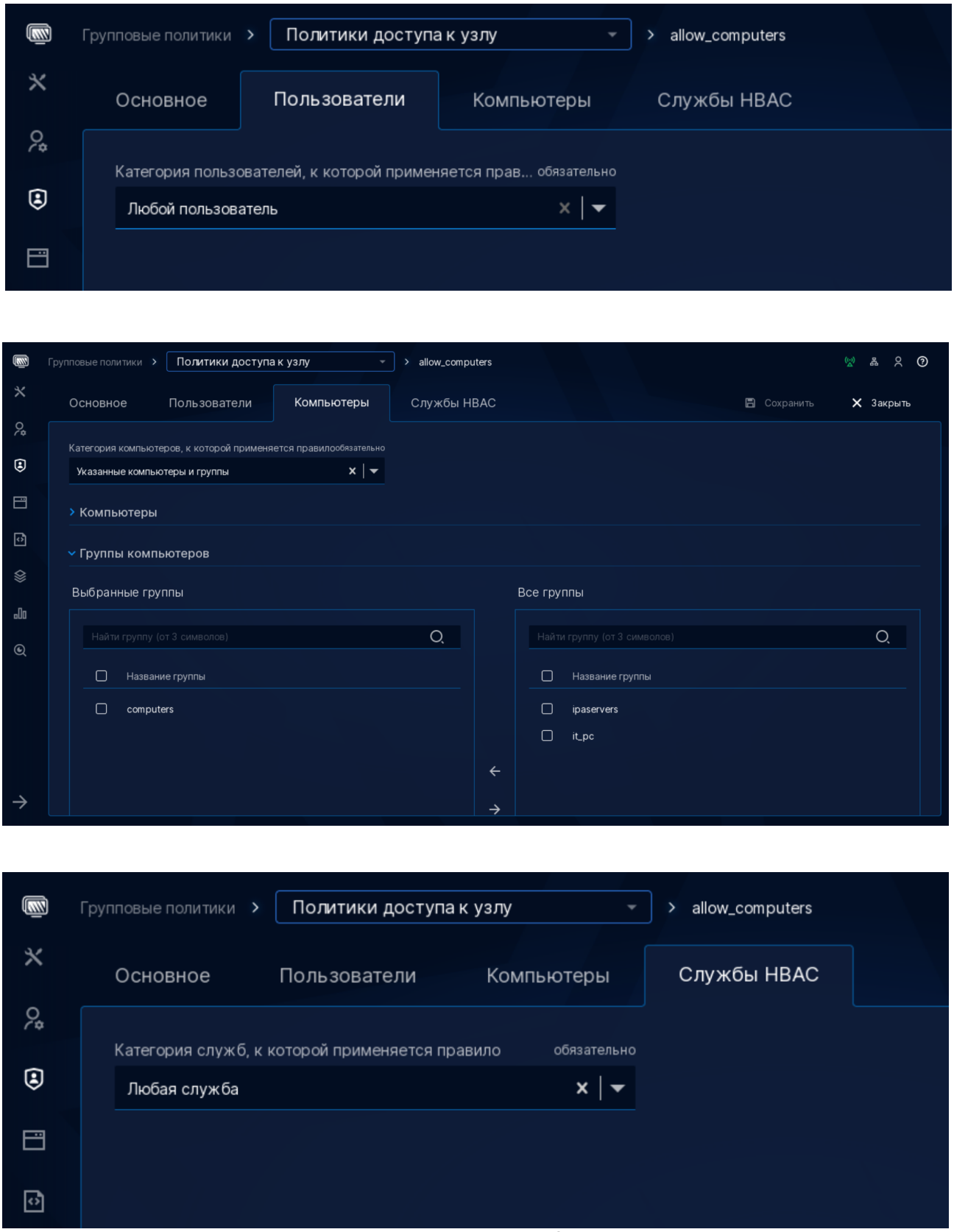


Рисунок 4 — Создание HBAC-правила

Если вы хотите внести в систему те же настройки из командной строки, то выполните следующие команды:

```
# ipa hostgroup-add computers
```

```
# ipa hostgroup-mod computers --desc='Обычные компьютеры домена'
# ipa hostgroup-add-member computers --hosts srvsssd --hosts srvsssd2


# ipa hbacrule-add allow_computers
# ipa hbacrule-mod allow_computers --desc='Разрешает всем пользователям доступ к
обычным компьютерам'
# ipa hbacrule-mod allow_computers --usercat=all
# ipa hbacrule-mod allow_computers --servicecat=all
# ipa hbacrule-add-host allow_computers --hostgroup computers
```

Ограничив доступ пользователей только к обычным компьютерам, можно переходить к настройке доступа к сервису OpenVPN. Делать это будем через правила HBAC.

Нам нужно предоставить возможность пользователям из группы **vpn_access** подключаться к сервису **openvpn** на сервере **astravpn**.

Первым делом создадим группу пользователей **vpn_access** и добавим туда тех, кому разрешено пользоваться сервисом **openvpn** (рис. 5,6)**.** Сделаем это через веб-интерфейс.

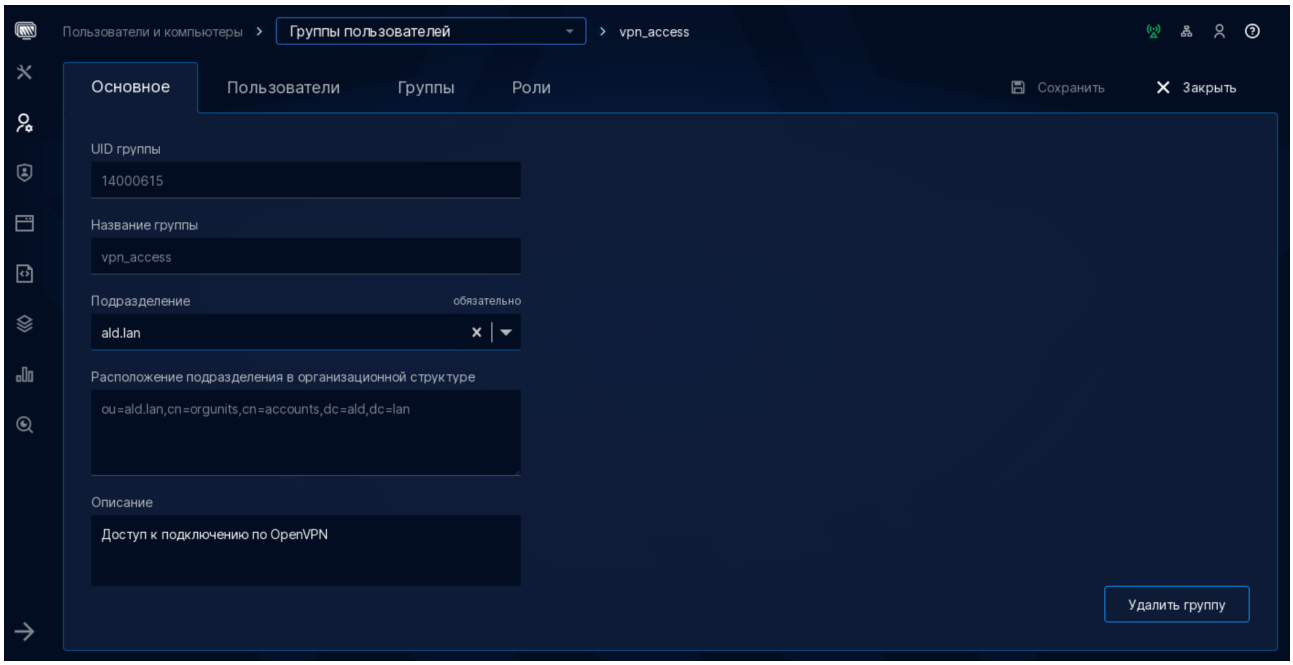


Рисунок 5 — Создание группы

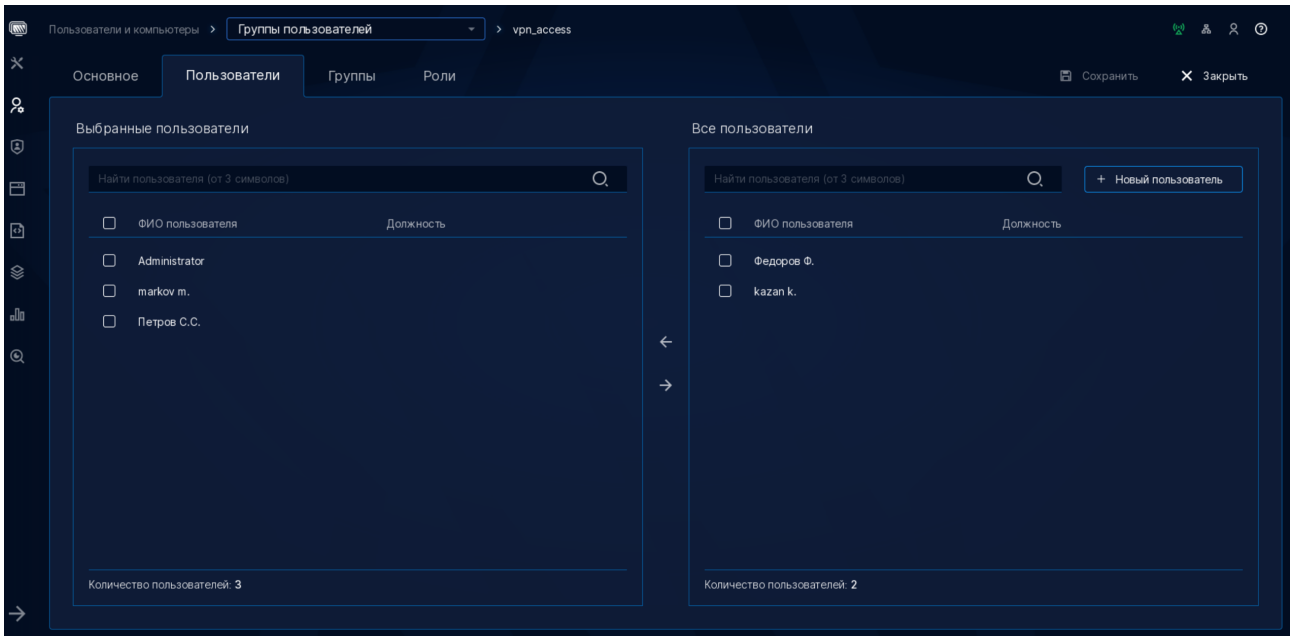


Рисунок 6 — Добавление пользователей

Если хотите сделать это из командной строки, то она будет выглядеть следующим образом:

```
# ipa group-add vpn_access
# ipa group-add-member vpn_access --users=admin --users=mark
```

Теперь создадим службу **openvpn** в службах HBAC. Сделать это можно будет через веб-интерфейс на странице «Групповые политики > Политики доступа к узлу > Службы HBAC > кнопка Новая служба» (рис. 7).

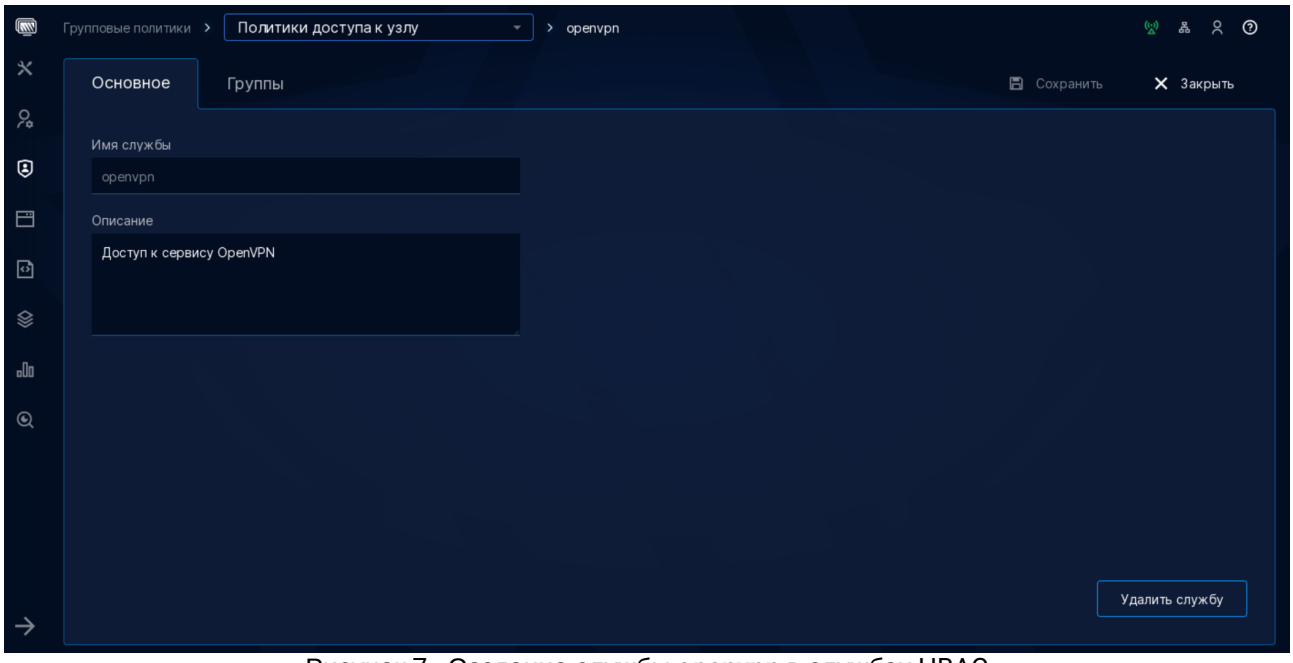


Рисунок 7 - Создание службы **openvpn** в службах HBAC

То же самое можно сделать из командной строки:

```
# ipa hbacsvc-add 'openvpn'
# ipa hbacsvc-mod 'openvpn' --desc='Доступ к сервису OpenVPN'
```

Следующим шагом создадим правило HBAC **openvpn_access**. Это можно сделать как через портал управления ALD Pro, так и из командной строки.

С использованием веб-интерфейса делается это следующим образом:

1. Создайте HBAC-правило. Для этого откройте страницу «Групповые политики > Политики доступа к узлу > Правила HBAC» и нажмите кнопку «Новое правило». Введите имя правила **openvpn_access** и нажмите кнопку «Сохранить» (рис. 8). Пока вы не сохраните правило, остальные вкладки с настройками будут недоступны.

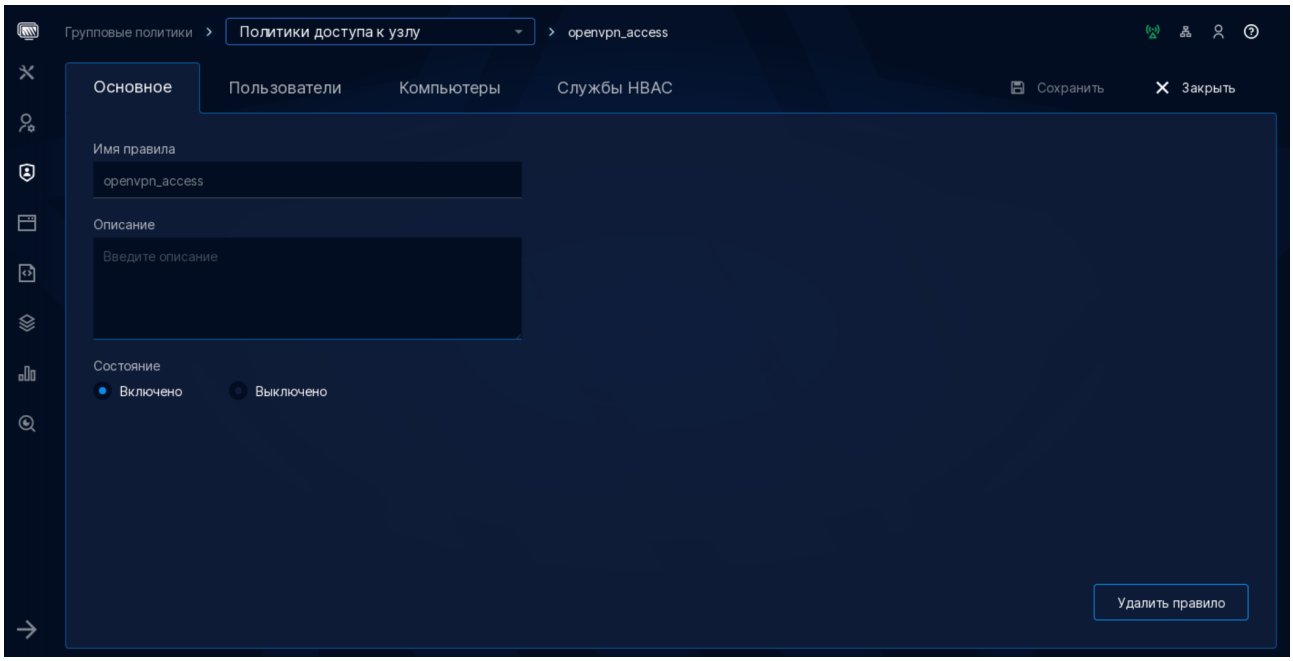


Рисунок 8 — Создание нового правила HBAC

2. Настройте область применения правила в части пользователей, выберите категорию «Указанные пользователи и группы» и добавьте группу **vpn_access** (рис.9). В части компьютеров добавьте компьютер **astravpn.ald.lan** (рис. 10). Не забудьте нажать кнопку «Сохранить» в правом верхнем углу, прежде чем переходить к следующей вкладке.

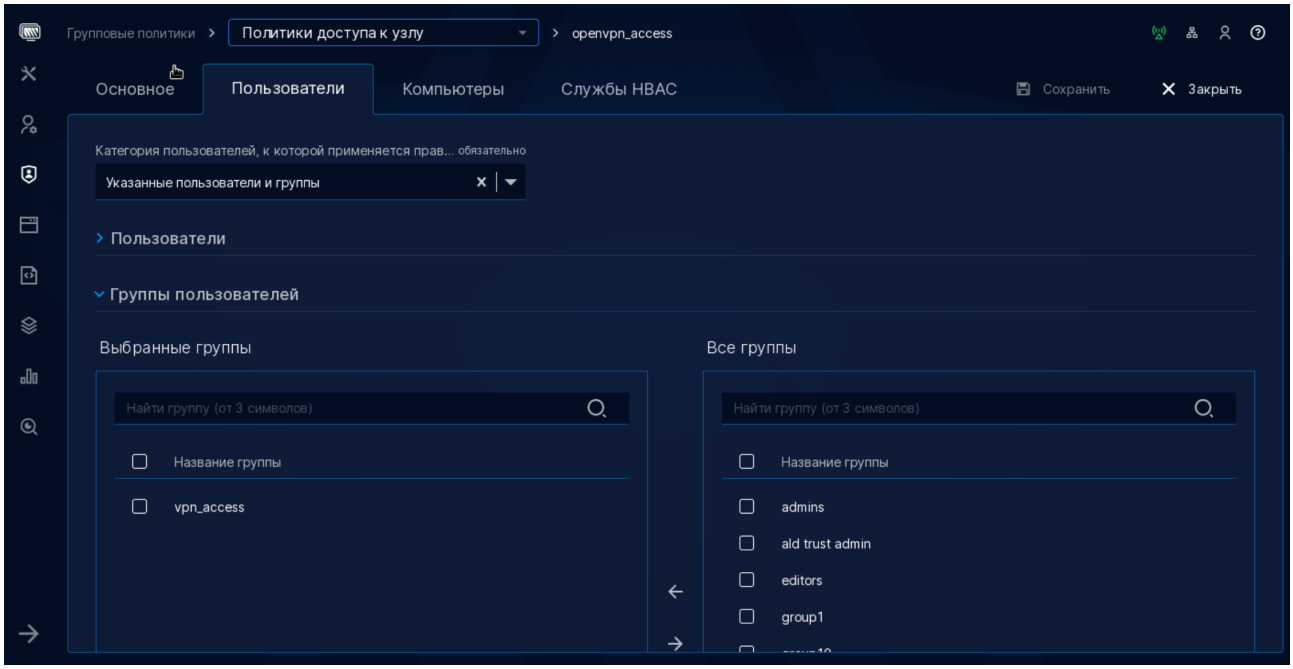


Рисунок 9 — Добавление группы **vpn_access**

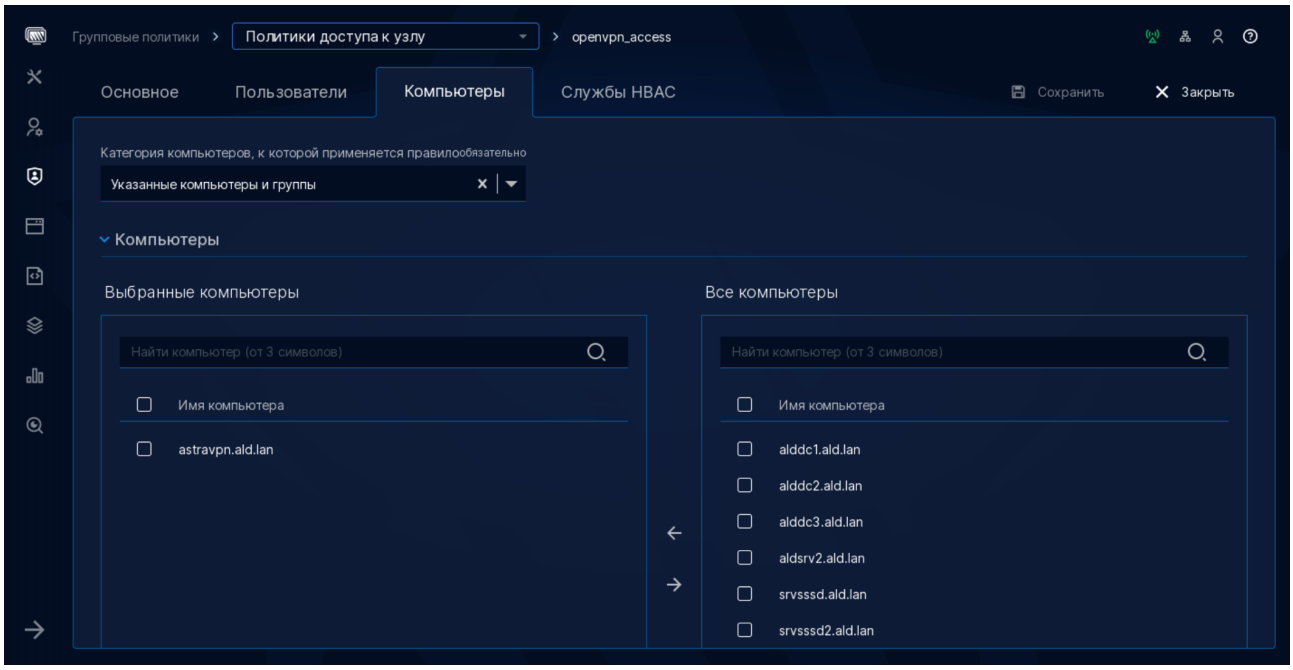


Рисунок 10 - Добавление компьютера **astravpn.ald.lan**

3. Настройте область применения правила в части служб, добавьте **openvpn** (рис. 11).

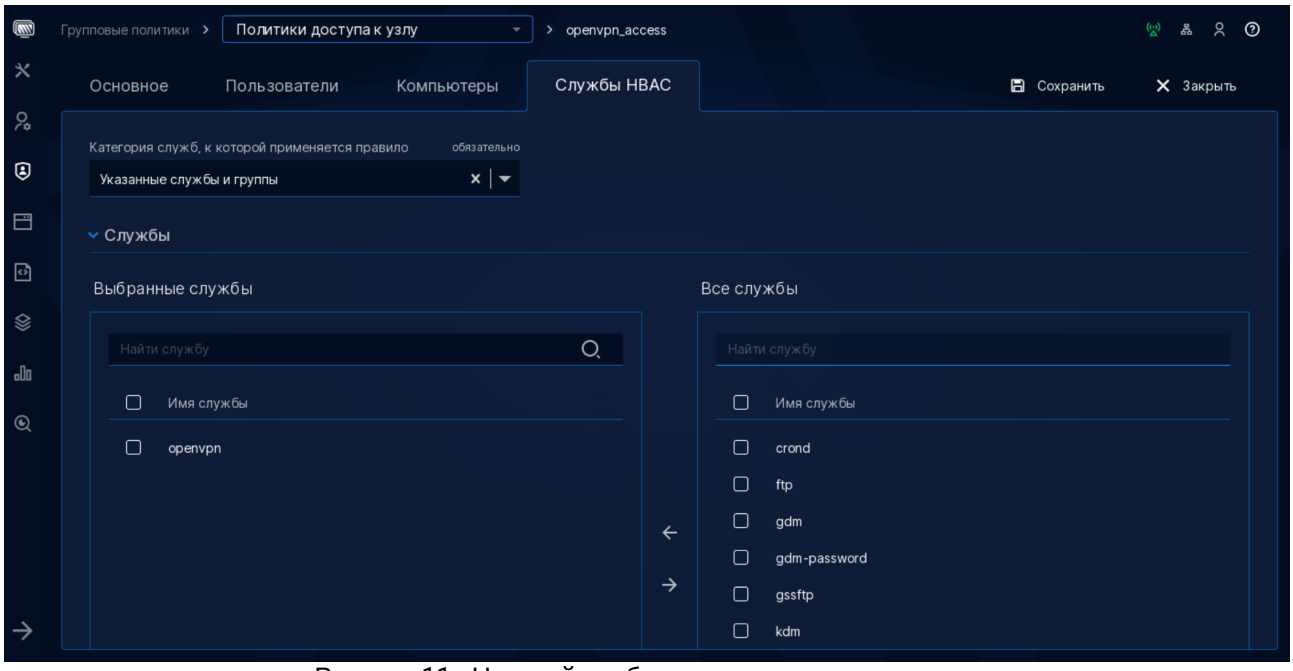


Рисунок 11 - Настройка области применения правила

В командной строке такое правило можно создать следующим образом:

```
# ipa hbacrule-add openvpn_access
# ipa hbacrule-add-user openvpn_access --groups vpn_access
# ipa hbacrule-add-host openvpn_access --hosts astravpn
# ipa hbacrule-add-service openvpn_access --hbacsvcs openvpn
```

, где

- hbacrule-add — команда для создания HBAC-правила;
- команды hbacrule-add-user, hbacrule-add-host и hbacrule-add-service позволяют определить область применения правила;

- ключ groups позволяет указать группу пользователей;
- ключ hosts позволяет указать хост;
- ключ hbacsvcs позволяет указать идентификатор PAM службы.

Теперь, если вы хотите разрешить новому пользователю подключаться к VPN, вам нужно добавить его в группу пользователей **vpn_access**.