Cisco ASA VPN

Cisco ASA VPN (https://www.cisco.com/) - это частная виртуальная сеть с высоким уровнем защиты.

Подключение Cisco ASA VPN к Blitz Identity Provider выполняется по протоколу SAML и состоит из двух этапов:

- Этап 1. Настройки на стороне Cisco ASA VPN
- Этап 2. Настройки на стороне Blitz Identity Provider

Важно:

В инструкции для примера указано, что Blitz IDP установлен на домене `https://login.company.com`, а Cisco ASA расположен на домене `https://vpn-gw1.company.com`. Уточните ваши адреса перед применением инструкции.

Этап 1. Настройки на стороне Cisco ASA VPN

Примечание:

Только следующие версии Cisco ASA поддерживают SAML: 9.7.1.24, 9.8.2.28, 9.9.2.1 и выше в данных релизах, а также 9.10 и позднее.

1. Для добавления сертификата перейдите на `https://login.company.com/blitz/saml/profile/Metadata/SAML` и **Скопируйте** сертификат.
2. В CLI Cisco ASA выполните следующие команды:

```
crypto ca trustpoint Blitz-IDP
no ca-check
enrollment terminal
no id-usage
exit
crypto ca authenticate Blitz-IDP
<paste in the IdP-certificate in Base64-format>
-----BEGIN CERTIFICATE-----
```

```
.............................TEXT SHORTENED.............................

-----END CERTIFICATE-----
quit
yes
```

3. Для настройки SAML в CLI Cisco ASA выполните следующие команды:

```
saml idp https://login.company.com/blitz/saml
url sign-in https://login.company.com/blitz/saml/profile/SAML2/Redirect/SSO
url sign-out https://login.company.com/blitz/saml/profile/SAML2/Redirect/SLO
base-url https://vpn-gw1.company.com/
trustpoint idp Blitz-IDP
trustpoint sp <asa_saml_sp_certificate_name>
no signature
no force re-authentication
clock-skew 15 #Настройка ошибки по времени
tunnel-group-list enable
tunnel-group-preference group-url
cache
disable
```

4. Для настройки AAA сервера только на авторизацию в CLI Cisco ASA выполните следующие команды:

```
aaa-server ISE(Authorization) protocol radius
 authorize-only
aaa-server ISE(Authorization) (inside) host <fqdn-radius-server-1>
 timeout 30
 key *****
aaa-server ISE(Authorization) (inside) host <fqdn-radius-server-2>
 key *****
```

5. Для настройки туннельной группы в CLI Cisco ASA выполните следующие команды:

```
tunnel-group <Group-Name> type remote-access
tunnel-group <Group-Name> general-attributes
address-pool vpn-pool.pmh
authentication-server-group ISE(Authorization)
authorization-server-group ISE(Authorization)
```

```
accounting-server-group ISE(Authorization)
default-group-policy <Group-Policy>
dhcp-server <DHCP-SRV1>
dhcp-server <DHCP-SRV2>
tunnel-group <Group-Name> webvpn-attributes
authentication saml
group-url https://vpn-gw1.company.com/<Group-Name> enable
group-url https://<fqdn-group-balancing>/<Group-Name> enable
saml identity-provider <Blitz entityID>
```

Особенность Cisco ASA:

При изменении настроек SAML в Cisco ASA требуется отключить и заново назначить конфигурацию для туннельной группы.

6. В CLI Cisco ASA выполните следующие команды:

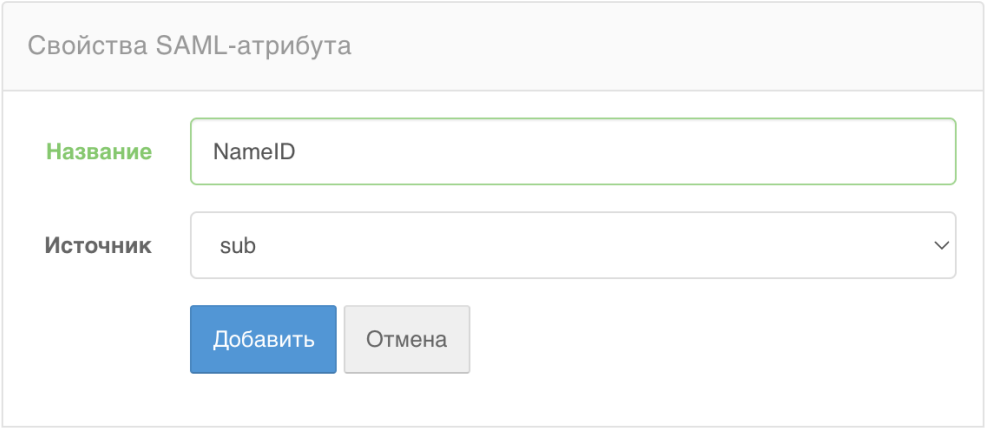
```
tunnel-group <Group-Name> webvpn-attributes
no saml identity-provider <Blitz entityID>
saml identity-provider <Blitz entityID>
```

Также возможно выполнить в интерфейсе администратора ASDM: Connection Profile > Basic > смените SAML Identity Provider на “None” > нажмите OK и Apply, вернитесь назад и повторно выберите SAML-server в выпадающем списке и нажмите OK и Apply снова.

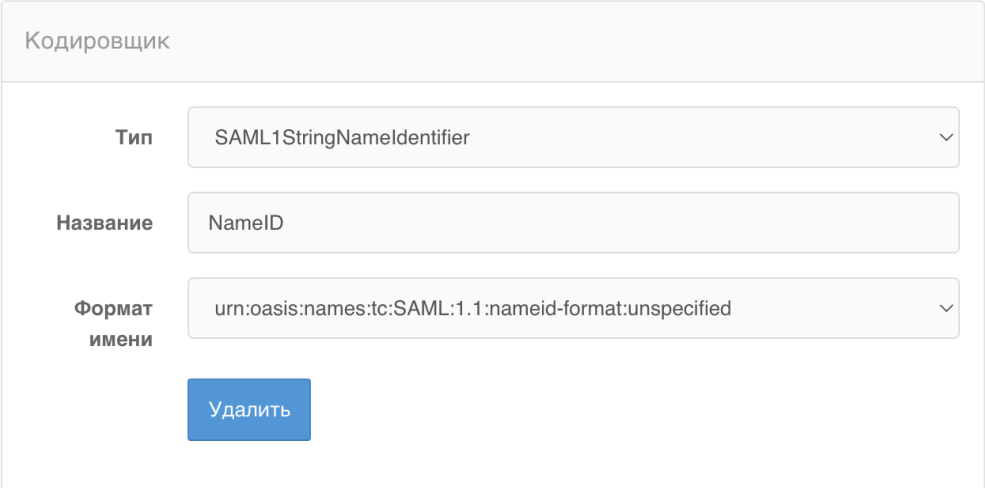
Этап 2. Настройки на стороне Blitz Identity Provider

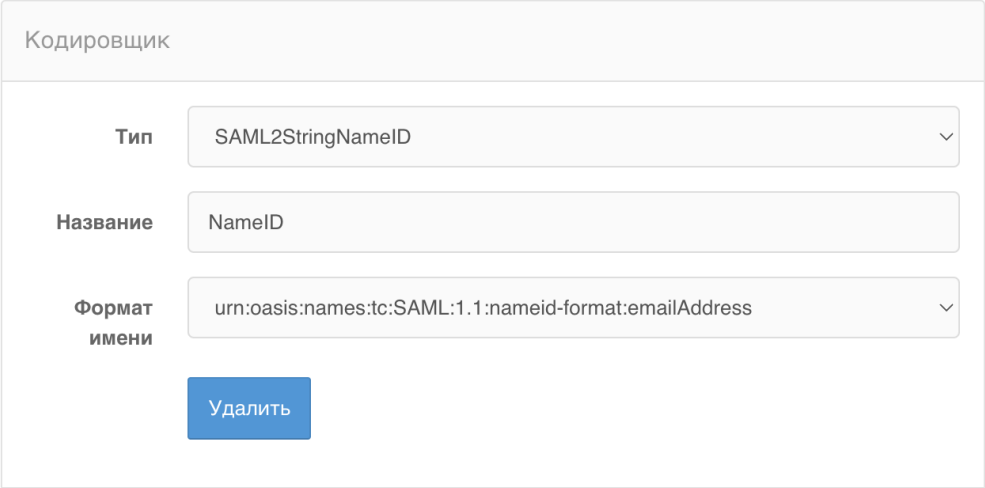
В консоли управления Blitz Identity Provider перейдите в раздел **SAML** и выполните следующие действия:

1. Нажмите **Добавить новый SAML-атрибут**.
2. Укажите название атрибута и его источник в хранилище. В данном случае источник `sub`. Выберите его из выпадающего списка.
3. После заполнения свойств атрибута нажмите **Добавить**.



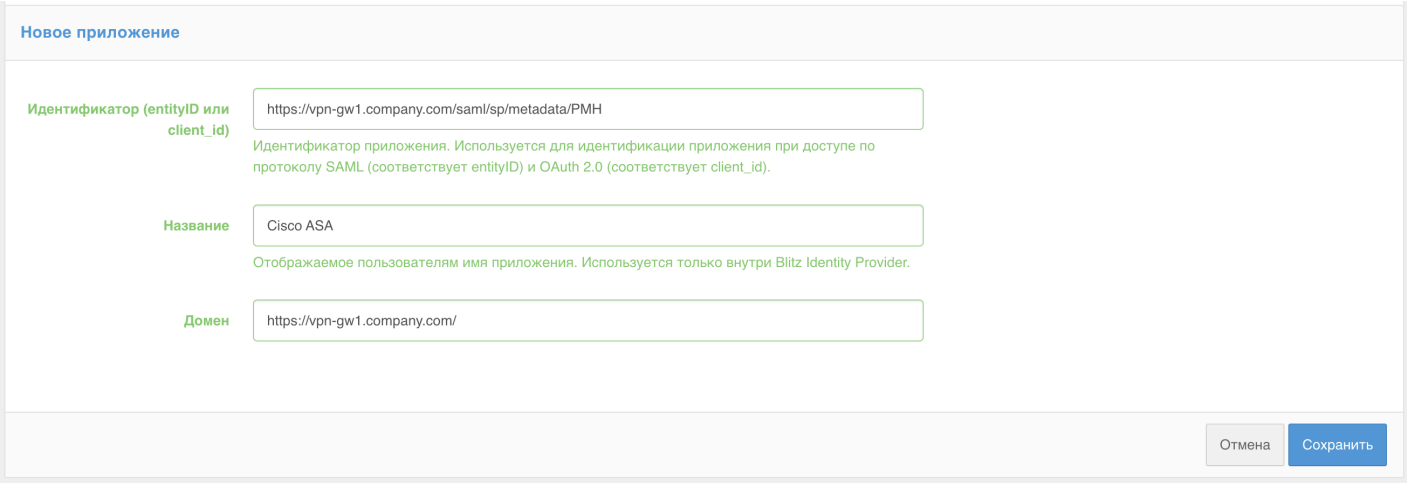
4. Далее добавьте кодировщик для атрибута. Для этого выберите атрибут и нажмите **Добавить кодировщик**.
5. Для атрибута добавьте кодировщики `SAML1StringNameIdentifier` и `SAML2StringNameID`. Каждому кодировщику присваивается название `NameID`.
6. Задайте настройки кодировщика по аналогии с приведенным ниже примером:





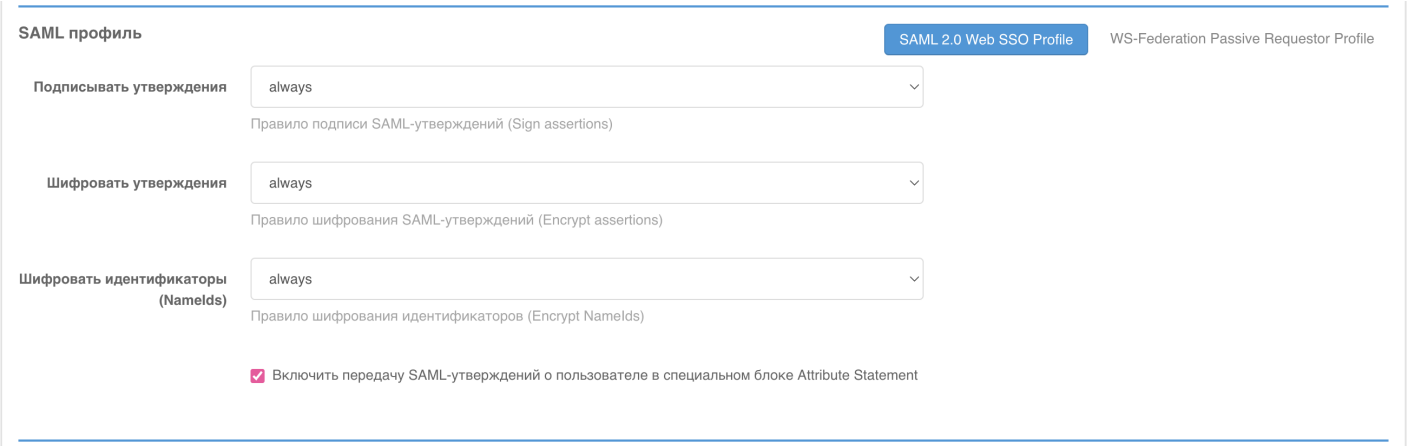
7. Нажмите **Сохранить** после каждого создания кодировщика.
8. Далее необходимо получить метаданные Cisco ASA. Для этого перейдите по ссылке `https://<fqdn-node-x>/saml/sp/metadata/<Group-Name>`.
9. В консоли управления *Blitz Identity Provider* перейдите в раздел **Приложения**.
10. Создайте новое приложение, задав его базовые настройки:

- **Идентификатор (entityID или client_id)**: введите значение entityID из метаданных Cisco ASA.
- **Название**: укажите название приложения, которое видно только внутри Blitz. Например, `Cisco ASA`.
- **Домен**: `https://vpn-gw1.company.com/`

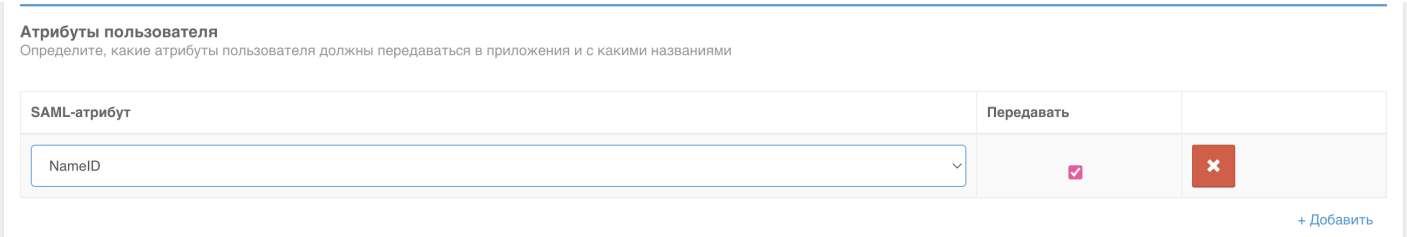


11. Нажмите **Сохранить**.
12. Далее нажмите кнопку **Параметры** у предложения Cisco ASA и отредактируйте параметры приложения:

- **Протоколы**: выберите `SAML` и нажмите **Сконфигурировать**
- Выберите **SAML 2.0 Web SSO Profile** и нажмите **Сконфигурировать**. Установите следующие настройки:
  - **Подписывать утверждения**: `always`
  - **Шифровать утверждения**: `never`
  - **Шифровать идентификаторы (NameIds)**: `never`
  - **Включить передачу SAML-утверждений о пользователе в специальном блоке AttributeStatement**: установить флажок.



13. В разделе **Атрибуты пользователя** настройте передачу в Cisco ASA SAML-атрибута, созданного на первом этапе.



14. Нажмите **Сохранить**.
15. Далее в разделе **Метаданные** нажмите **Изменить**. Скопируйте и вставьте метаданные Cisco ASA из пункта 9.
16. Нажмите **Сохранить**.

Совет:

После прохождения всех шагов рекомендуем проверить корректность входа в Cisco ASA: https://vpn-gw1.company.com/

Версия #5
Admin создал 16 сентября 2024 14:57:33
Superadmin обновил 2 апреля 2025 10:31:36