Интеграция Squid Proxy со службой каталога ALD Pro

01/26/2026

Содержание

1 Введение

Squid — это кэширующий прокси-сервер с открытым исходным кодом, разработанный для оптимизации HTTP- и HTTPS-трафика.

Данная интеграция позволяет прокси-серверу Squid предоставлять пользователям доступ с аутентификацией по протоколу Kerberos, а также настраивать прокси-сервер для браузера Firefox на всех доменных компьютерах при помощи дополнительных параметров групповых политик.

2 Описание стенда

Контроллер домена - **dc-1.ald.company.lan**

Доменный компьютер – **client.ald.company.lan**

Прокси-сервер – **squid.ald.company.lan**

3 Регистрация Kerberos-службы для сервера Squid

1. Для регистрации Kerberos-службы требуется, чтобы на контроллере домена существовала DNS-запись. Если прокси-сервер не введен в домен, то необходимо добавить A-запись следующей командой:

ipa dnsrecord-add ald.company.lan squid --a-rec 10.0.2.100

, где

- **ald.company.lan** – имя зоны,
- **squid** - имя A-записи,
- **10.0.2.100** – IP-адрес, который должен возвращаться при обращении к данной записи.

Примечание!

Если у вас несколько прокси-серверов, то кроме основной DNS-записи сервера вы можете создать общую DNS-запись, включающую в себя A-записи всех прокси-серверов. Это позволит обеспечить балансировку нагрузки, так как DNS-сервер по умолчанию будет отдавать записи в случайном порядке, а клиент будет использовать их по кругу (Round Robin). Несколько прокси-серверов гарантируют также надежную работу функции проксирования в том случае, если клиенту будет доступен хотя бы один из них.

---

2. Добавить Kerberos-службу при помощи указанной команды:

```
ipa service-add http/squid.ald.company.lan –skip-host-check
```

3. Загрузить Kerberos-ключ:

```
sudo ipa-getkeytab -p http/squid.ald.company.lan -k /etc/squid/squid.keytab
```

4. Установить права для загруженного ключа:

```
chown root:proxy /etc/squid/squid.keytab

chmod 640 /etc/squid/squid.keytab
```

4 Конфигурация прокси-сервера Squid

В конфигурационном файле **/etc/squid/squid.conf** добавить следующие параметры:

```
auth_param negotiate program /usr/lib/squid/negotiate_kerberos_auth -k /etc/squid/
squid.keytab -s HTTP/squid.ald.company.lan@ALD.COMPANY.LAN

auth_param negotiate children 20

auth_param negotiate keep_alive on

acl authenticated proxy_auth REQUIRED

http_access allow authenticated

http_access deny all
```

Рассмотрим настройку данных директив.

- **auth_param negotiate program** - указывает способ аутентификации через библиотеку **negotiate_kerberos_auth** с переданным ей Kerberos-ключом, который ранее был сгенерирован и загружен на прокси-сервер.
- **auth_param negotiate children –** определяет максимальное количество дочерних процессов для обработки аутентификации. В официальной документации отсутствует информация о необходимом количестве процессов по отношению к пользователям, поэтому при больших нагрузках рекомендуется увеличивать количество серверов.
- **auth_param negotiate keep_alive on -** при включенной настройке оставляет процессы для обработки аутентификации активными в течение всего времени работы сервера, что увеличивает скорость обработки аутентификации при большом количестве пользователей. В противном случае процессы будут завершаться каждый раз, когда заканчивается сессия аутентификации.
- **acl authenticated proxy_auth REQUIRED –** создает запись в списке правил контроля доступа с именем **authenticated,** действие которой распространяется на пользователей, прошедших аутентификацию.
- **http_access allow authenticated –** разрешает доступ по правилу authenticated**.**
- **http_access deny all –** запрещает доступ всем остальным пользователям.

5 Создание доп. параметра групповой политики

Большим преимуществом ALD Pro является возможность создавать собственные доп. параметры групповых политик. В данной интеграции использование такого доп. параметра групповой политики используется для настройки браузера Firefox для всех компьютеров в выбранном подразделении. Для этого нужно в веб-портале ALD Pro в разделе «Управление доменом» выбрать пункт «Доп. параметры групповых политик», как показано на рисунке 1.

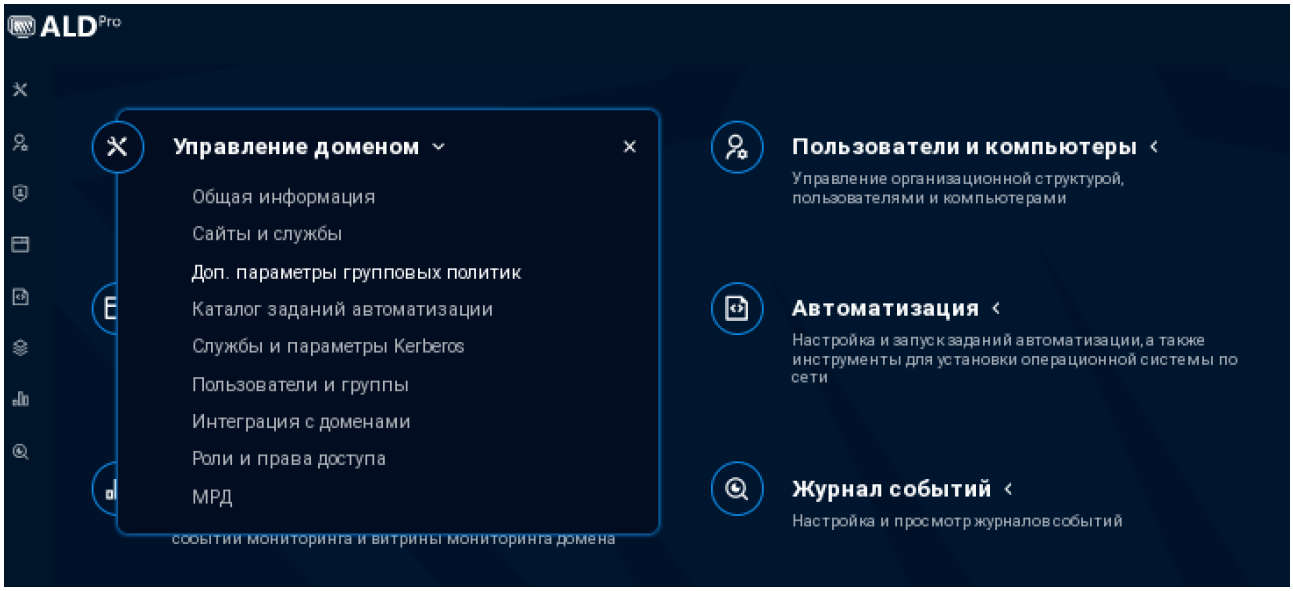

Рисунок 1 – Демонстрация раздела «Управление доменом» в веб-портале ALD Pro

Далее нужно нажать на кнопку «Новый параметр», после чего заполнить информацию о данном параметре, как показано на рисунке 2.

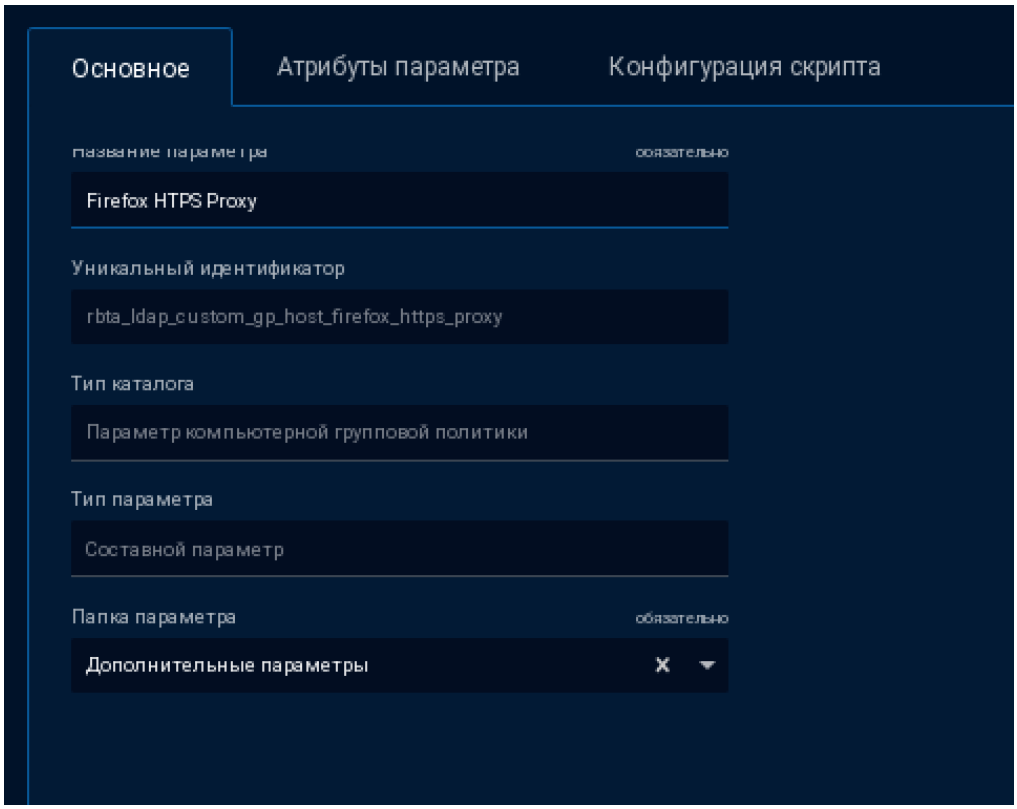

Рисунок 2 – Раздел создания доп. параметра групповой политики

Назначение полей формы:

- **Название параметра** – имя доп. параметра, которое вы будете видеть в веб-портале управления.
- **Уникальный идентификатор** – имя параметра, который используется для идентификации данного доп. параметра в salt-скриптах.
- **Тип каталога** – неизменяемое значение.
- **Тип параметра** –выбрать «Составной параметр».
- **Папка параметра** – если вы храните доп. параметры в определенной структуре папок, для соблюдения порядка выберите конкретную папку, где будет храниться созданный параметр.

Важно!

В данной инструкции для уникального идентификатора используется имя

rbta_ldap_custom_gp_host_firefox_https_proxy. Если вы будете использовать другое имя параметра, то в дальнейшем вам нужно будет соответствующим образом скорректировать текст salt-скрипта.

В разделе «Атрибуты параметра» добавить атрибуты из таблицы 1.

Таблица 1

Атрибут	Идентификатор

Адрес прокси-сервера	proxy_address
Сетевой порт прокси-сервера	proxy_port

Созданные атрибуты изображены на рисунке 3.

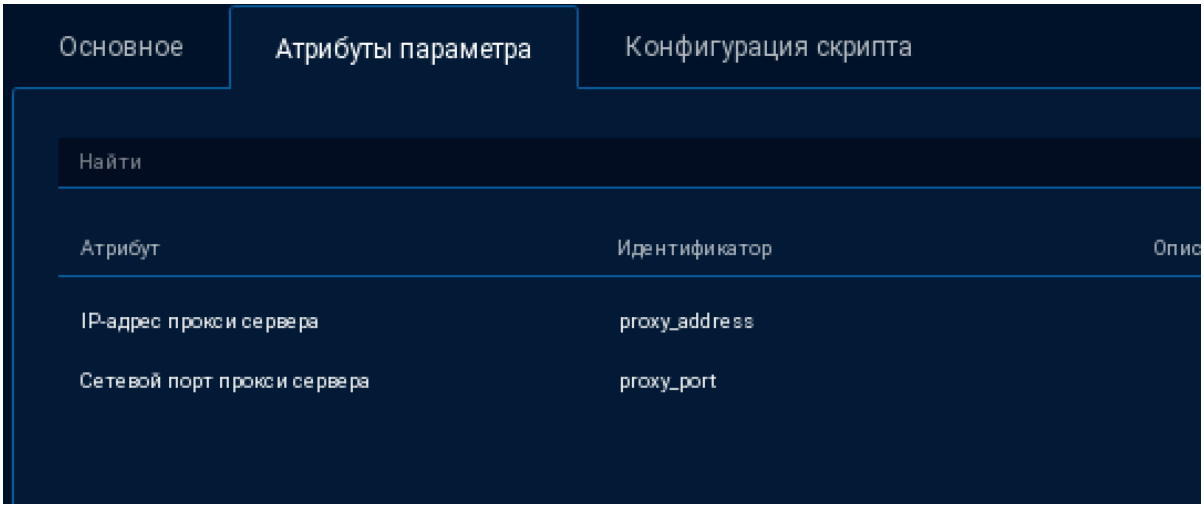

Рисунок 3 – Раздел «Атрибуты параметра»

В разделе «Конфигурация скрипта» нужно вставить текст скрипта.
После копирования проверьте, что структура yaml не нарушена.

```
{% set id = 'rbta_ldap_custom_gp_host_firefox_https_proxy' %}

{% set node = salt['grains.get']('nodename') %}

{% set gpo = salt['pillar.get']('aldpro-hosts:' + node + ':' + id) %}


{% if gpo %}

{% set sls_proxy_address = gpo[0].get('proxy_address') %}

{% set sls_proxy_port = gpo[0].get('proxy_port') %}


{{ id }}:

file.serialize:

- name: /usr/lib/firefox/distribution/policies.json

- formatter: json

- makedirs: True

- merge_if_exists: True

- user: root
```

```
- group: root

- mode: '0644'

- dataset:

policies:

Proxy:

Mode: "manual"

SSLProxy: "{{ sls_proxy_address }}:{{ sls_proxy_port }}"

{% endif %}
```

Данный скрипт извлечет значения переданных ему атрибутов **proxy_address** и **proxy_port** (сами значения будут указаны далее при создании групповой политики) и добавит в файл **/usr/lib/firefox/distribution/policies.json** директивы, включающие передачу запросов через прокси-сервер, полученный из ранее обозначенных атрибутов.

6 Создание групповой политики

В разделе «Групповые политики» нажать на кнопку «Новая групповая политика». Указать имя политики, как показано на рисунке 4:

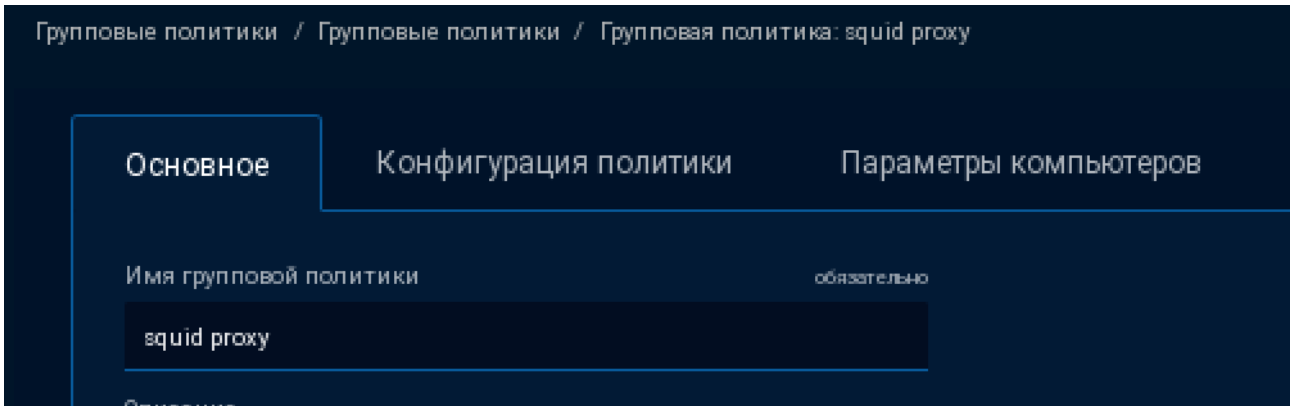

Рисунок 4 — Создание групповой политики

После указания имени откроется возможность перейти в раздел «Параметры компьютеров». В этом разделе нужно выбрать «Дополнительные параметры» и найти ранее созданный доп. параметр групповой политики, после чего указать атрибуты прокси-сервера Squid.

В демонстрационном примере, изображенном на рисунке 5, указаны:

- доменное имя — squid.ald.company.lan,
- порт – 3128.

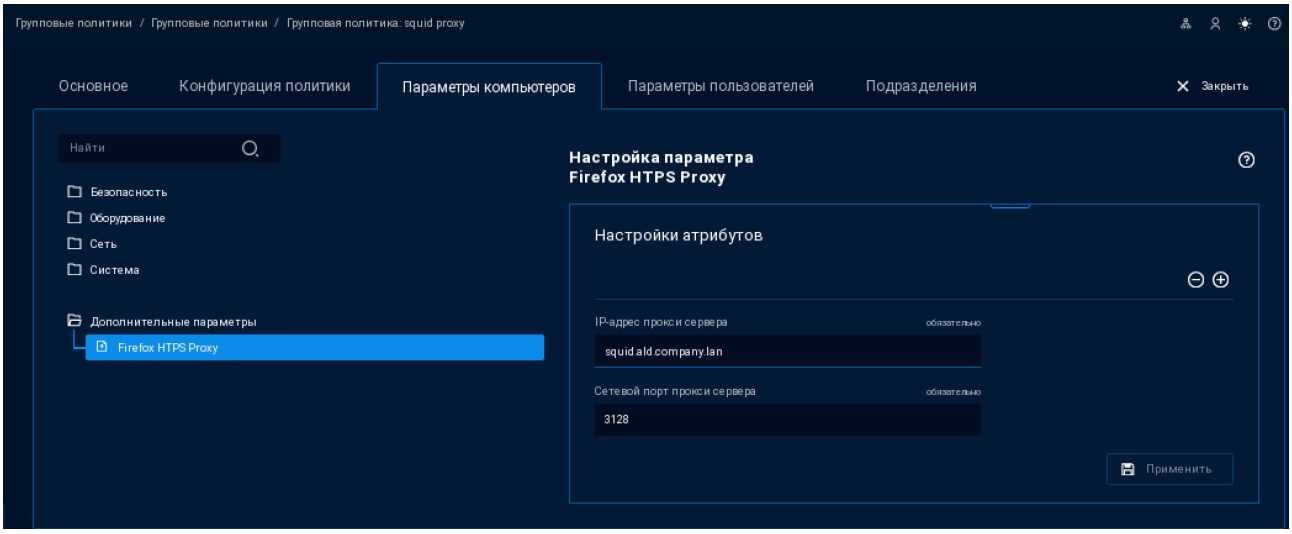

Рисунок 5 — Указание доп. параметров групповой политики

В разделе «Подразделение» можно указать область действия создаваемой политики (рис. 6):

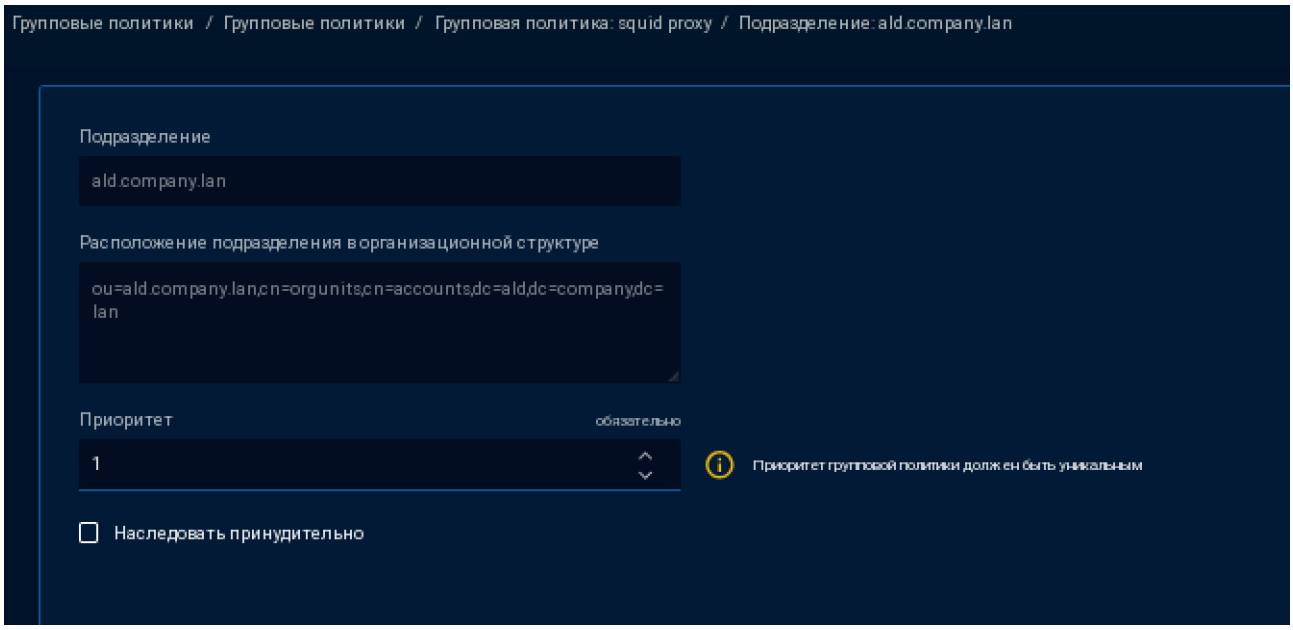

Рисунок 6 — Раздел «Подразделения»