

3. Ретранслятор gits-relay

Ретранслятор ставится в удалённом или изолированном сегменте. Агенты сегмента подключаются к нему, а он к ядру. На межсетевом экране достаточно одного правила на сегмент: «ретранслятор → ядро:8443».

Что делает ретранслятор:

- проверяет сертификаты агентов (mTLS) и передаёт ядру их идентичность;
- буферизует события на диске, пока ядро недоступно (`spool_max_mb` , по умолчанию 2 ГБ);
- кэширует пакеты обновлений агентов;
- выполняет push-установку агентов на hosts своего сегмента.

Ретранслятору не нужны права root. Секретов ядра он не хранит: подписи команд и конфигураций проверяют сами агенты.

1. Установка пакета

```
# Debian / Astra
apt install ./gits-relay_<ver>-1_amd64.deb
# RHEL и совместимые
dnf install ./gits-relay-<ver>-1.x86_64.rpm
```

Пакет создаёт системного пользователя `gits-relay` и раскладывает файлы:

Путь	Содержимое
<code>/usr/bin/gits-relay</code>	исполняемый файл
<code>/etc/gits-relay/relay.yaml.example</code>	пример конфигурации
<code>/var/lib/gits-relay</code> (0700)	сертификат, ключ, буфер событий, кэш пакетов
<code>/lib/systemd/system/gits-relay.service</code>	юнит: <code>User=gits-relay</code> , <code>ProtectSystem=strict</code> , <code>CAP_NET_BIND_SERVICE</code>

Пока ретранслятор не зарегистрирован, служба не включается.

2. Конфигурация

```
cp /etc/gits-relay/relay.yaml.example /etc/gits-relay/relay.yaml
cp ca.crt /etc/gits-relay/ca.pem # /var/lib/gits/ca/ca.crt с узла ядра
chown root:gits-relay /etc/gits-relay/relay.yaml /etc/gits-relay/ca.pem
chmod 0640 /etc/gits-relay/relay.yaml /etc/gits-relay/ca.pem
```

Параметр	Значение
<code>name</code>	имя в консоли (по умолчанию — имя хоста)
<code>listen</code>	адрес для агентов, по умолчанию <code>:8443</code>
<code>core</code>	адреса шлюза ядра по порядку предпочтения: <code>["gits.bank.local:8443"]</code>
<code>core_server_name</code>	имя в сертификате ядра, если оно отличается от адреса в <code>core</code>
<code>ca_file</code>	корневой сертификат СКР

Параметр	Значение
<code>state_dir</code>	<code>/var/lib/gits-relay</code>
<code>dns_names</code> , <code>ip_addresses</code>	имена и адреса, по которым к ретранслятору обращаются агенты. Попадают в сертификат ретранслятора; нужно хотя бы одно значение
<code>spool_max_mb</code>	размер буфера событий, МБ

3. Регистрация

1. Выпустите токен вида `relay`: в консоли «Агенты и токены» → «Выдать токен регистрации» (вид «ретранслятор») или на узле ядра:

```
bash gctl create-token -kind relay -name relay-seg1 -uses 1 -ttl 24h
```

2. Зарегистрируйте ретранслятор и запустите службу:

```
bash sudo -u gits-relay gits-relay enroll -config /etc/gits-relay/relay.yaml -token '<токен>'
systemctl enable --now gits-relay journalctl -u gits-relay -n 20 -o cat
```

При регистрации ретранслятор создаёт ключ и получает от ядра сертификат на 1 год с именами из `dns_names` / `ip_addresses`. Сертификат и идентификатор сохраняются в `state_dir`.

3. Ретранслятор появится в консоли, раздел «Ретрансляторы», в состоянии «на связи».

4. Перевод агентов сегмента на ретранслятор

В карточке ИС («Информационные системы») укажите в «Адресах подключения агентов» адрес ретранслятора, например `relay-seg1.bank.local:8443`. Агенты хостов этой ИС получают новый список адресов в подписанной конфигурации и переподключаются сами. Для новых агентов этот адрес попадёт в установочные комплекты.

Межсетевой экран: хосты сегмента → ретранслятор TCP 8443; ретранслятор → ядро TCP 8443.

5. Ограничения

- Сертификат ретранслятора действует 1 год и автоматически **не продлевается**. До истечения срока перерегистрируйте ретранслятор новым токеном: остановите службу, выполните `enroll` (§3) и запустите службу. Если после этого в разделе «Ретрансляторы» осталась прежняя запись без связи, отзовите её. Срок действия сертификата показан там же, в поле «Сертификат до».
- На Windows ретранслятор ставится как служба: `gits-relay.exe service install -config relay.yaml`, затем `service start`.