SkyDNS

Невидимые туннели Интернета

Как атаки годами живут в тени DNS

SkyDNS

Павел Евтихов

руководитель отдела внедрения

SkyDNS — это

Большой опыт на рынке

Мы уже 15 лет на российском рынке информационной безопасности

Отечественная разработка

Весь наш софт зарегистрирован в реестре российского ПО

Скорость ракеты

Мы самый быстрый публичный DNS-резолвер в России

Передовые технологии

Под капотом собственные технологии фильтрации контента и ML-модели

Высокая производительность

Ежедневно обрабатываем миллиарды DNS-запросов — 15 млн пользователей под защитой

Подтвержденная надежность

Наш сервис входит в мировой ТОП-3 по устойчивости DNS-резолверов — нам доверяют миллионы юзеров

Злоумышленники могут оставаться незамеченными годами

51 мин

Средняя продолжительность кибератаки на российские компании в 2024 году

«Информзащита», 2024

249 дней

В среднем злоумышленники находятся в инфраструктуре компании-жертвы до их обнаружения

IBM Data Breach Report, 2025

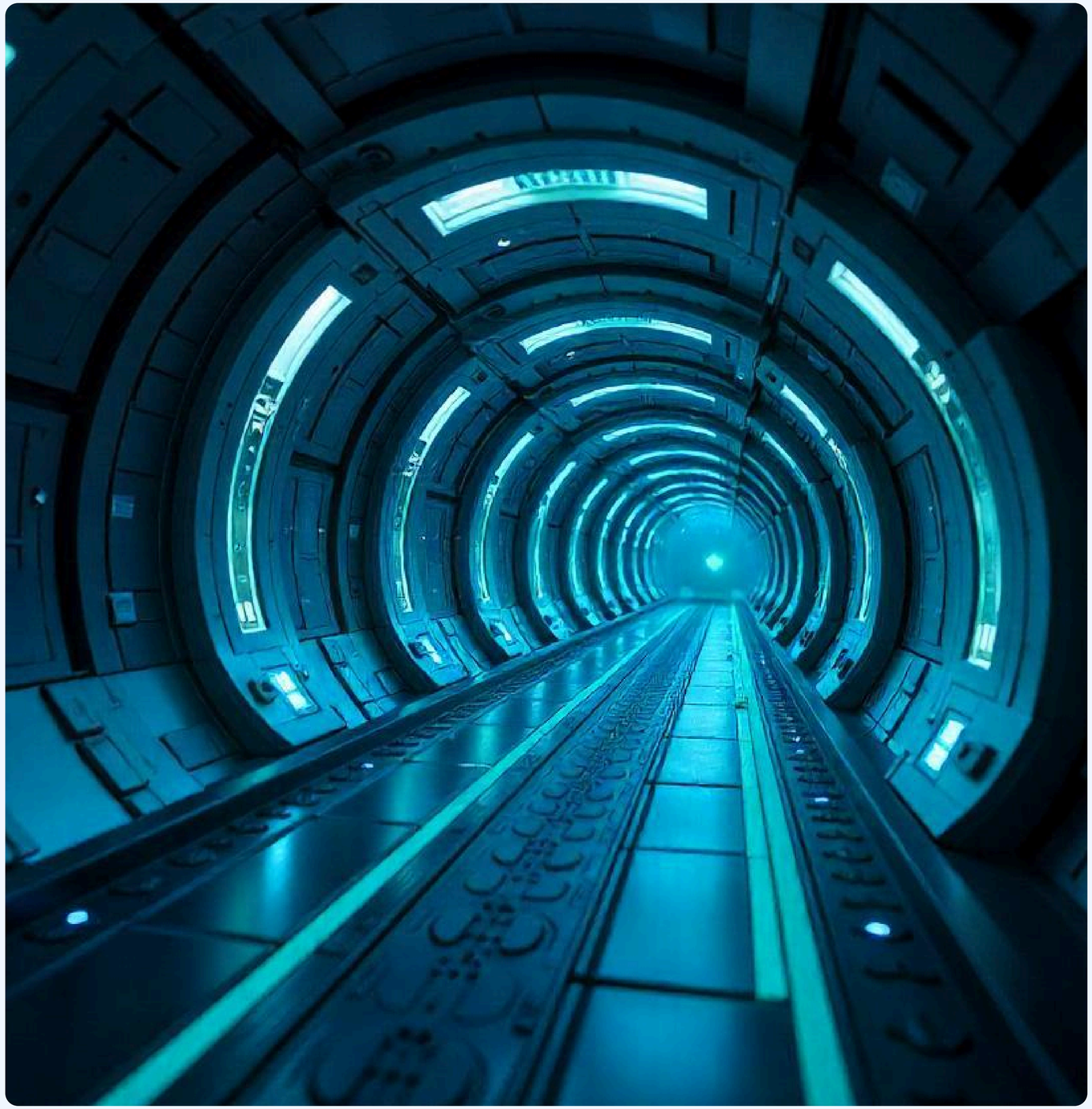
3 года

Длилось самое долгое пребывание злоумышленников в инфраструктуре

Отчет Positive Technologies, 2023

DNS-туннель

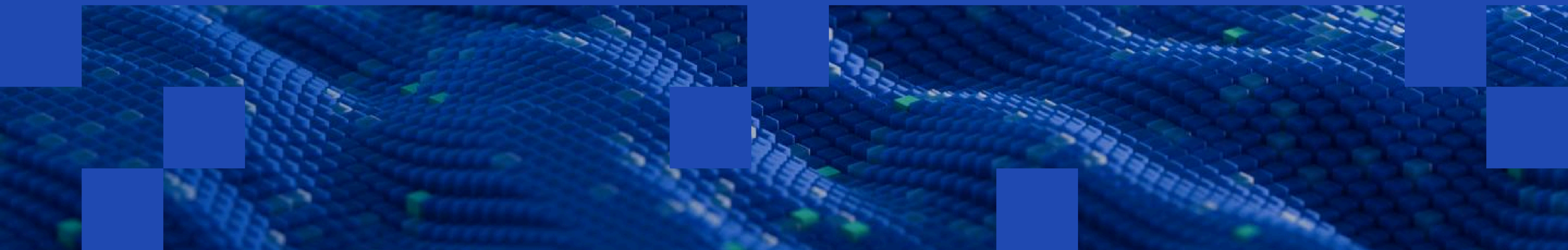
Метод передачи данных между двумя точками, например, между компьютером и сервером, через протокол DNS



Для чего используется DNS-туннель?

Для передачи управляющих команд

Для передачи файлов



Почему опасен DNS-туннель?

Внедрить легко

Существует множество готовых open-source решений

Обнаружить сложно

Маскируется под легитимный трафик и сливается с фоновым «шумом» сети

Заблокировать ещё сложнее

100% компаний, которые обращались к нам, не имели возможности блокировать DNS-туннели на лету

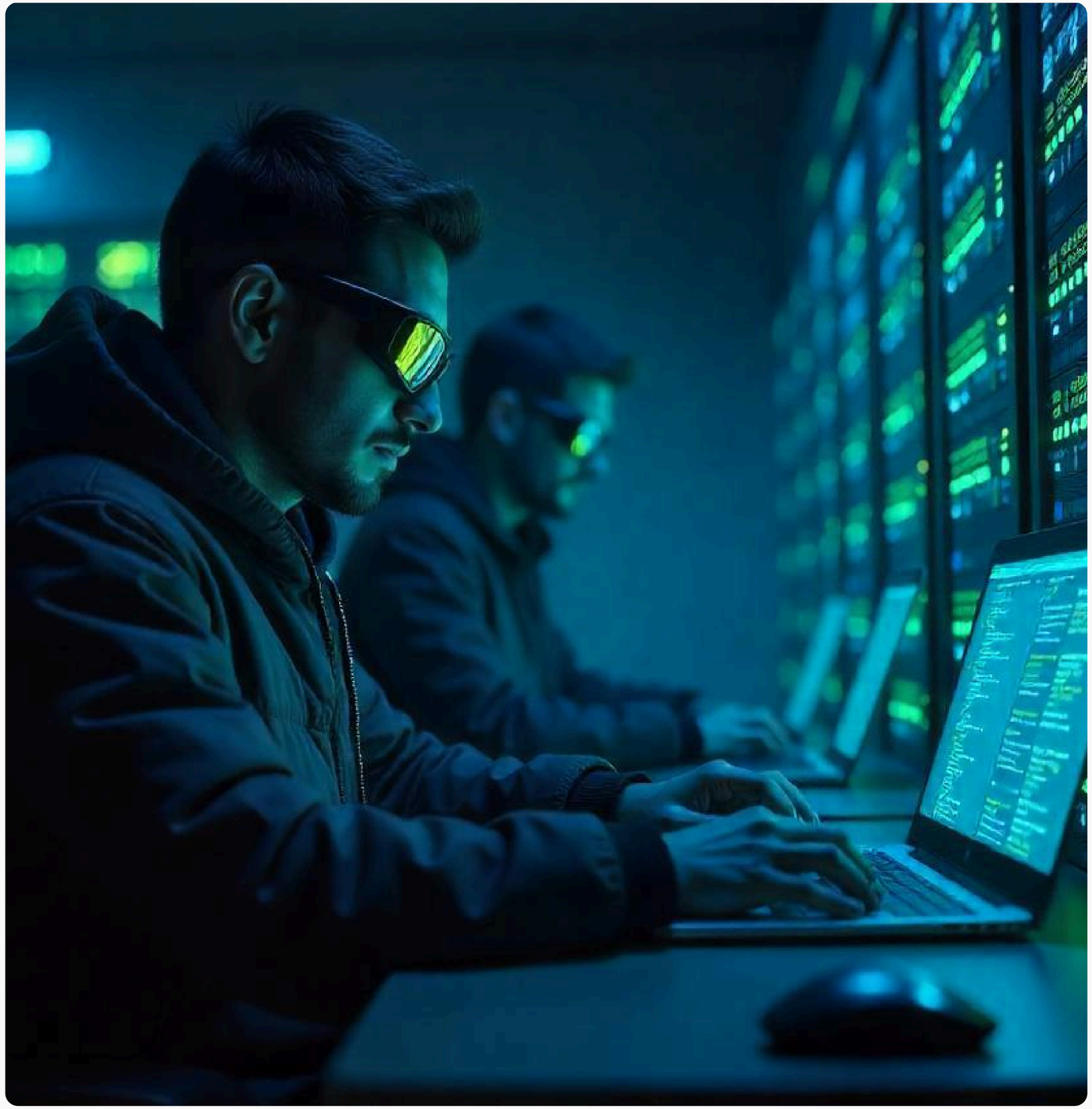


Схема DNS-трафика

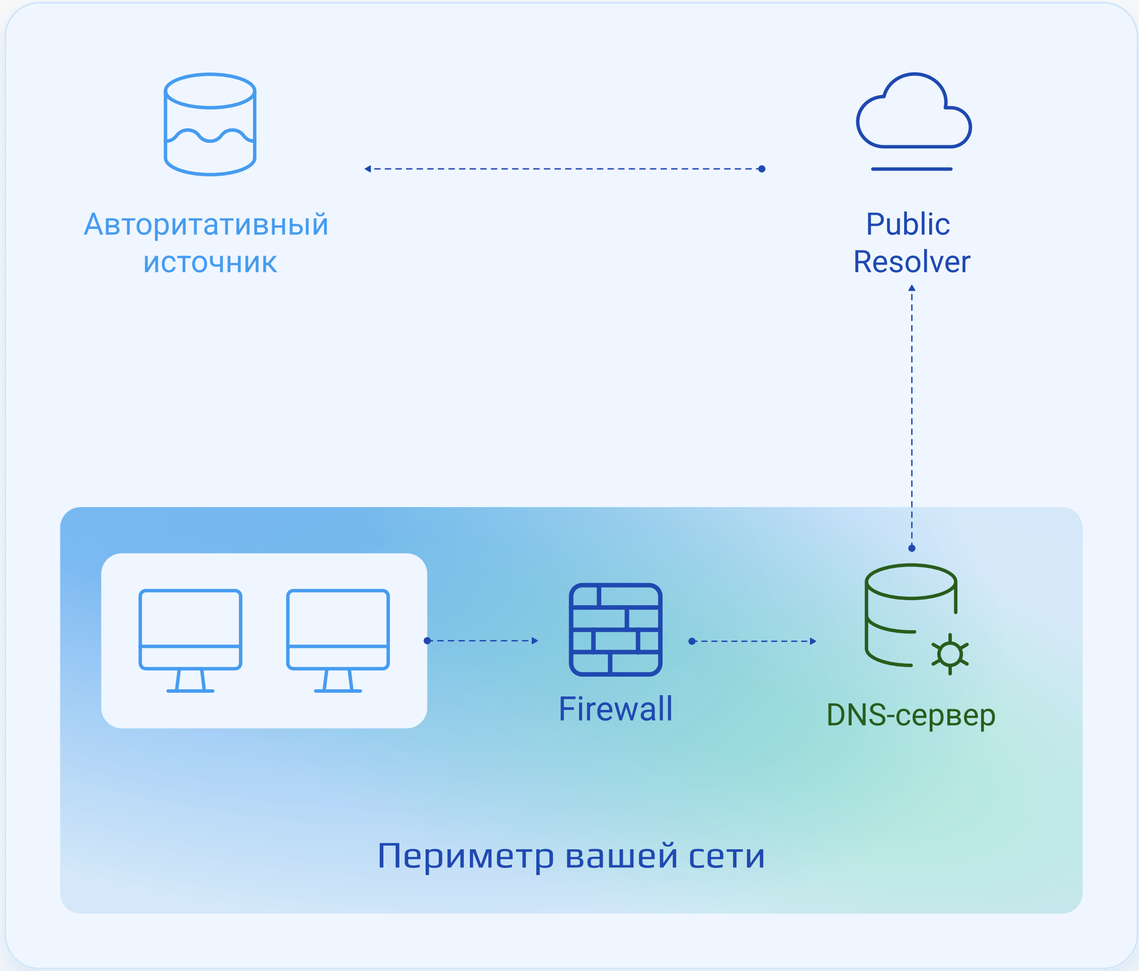


Схема DNS-туннеля

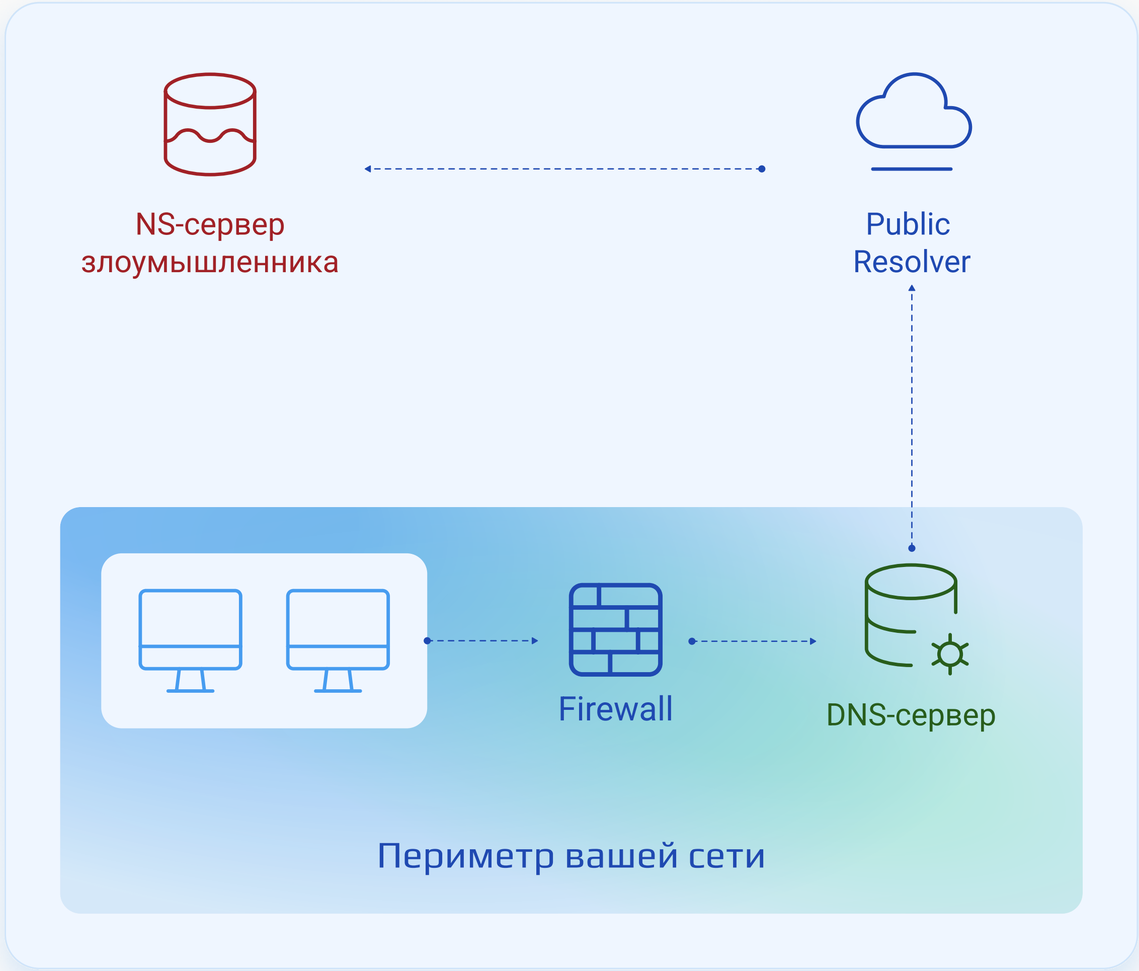
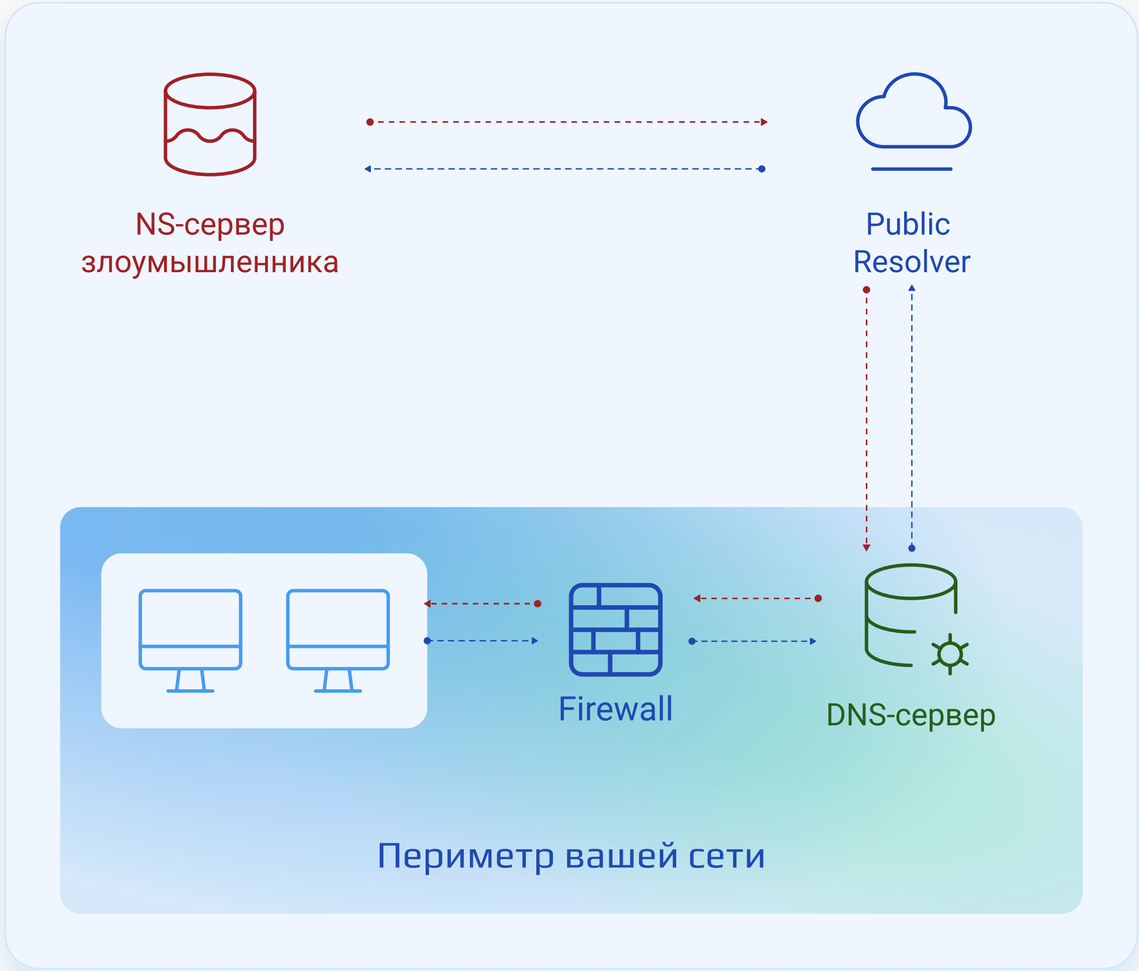
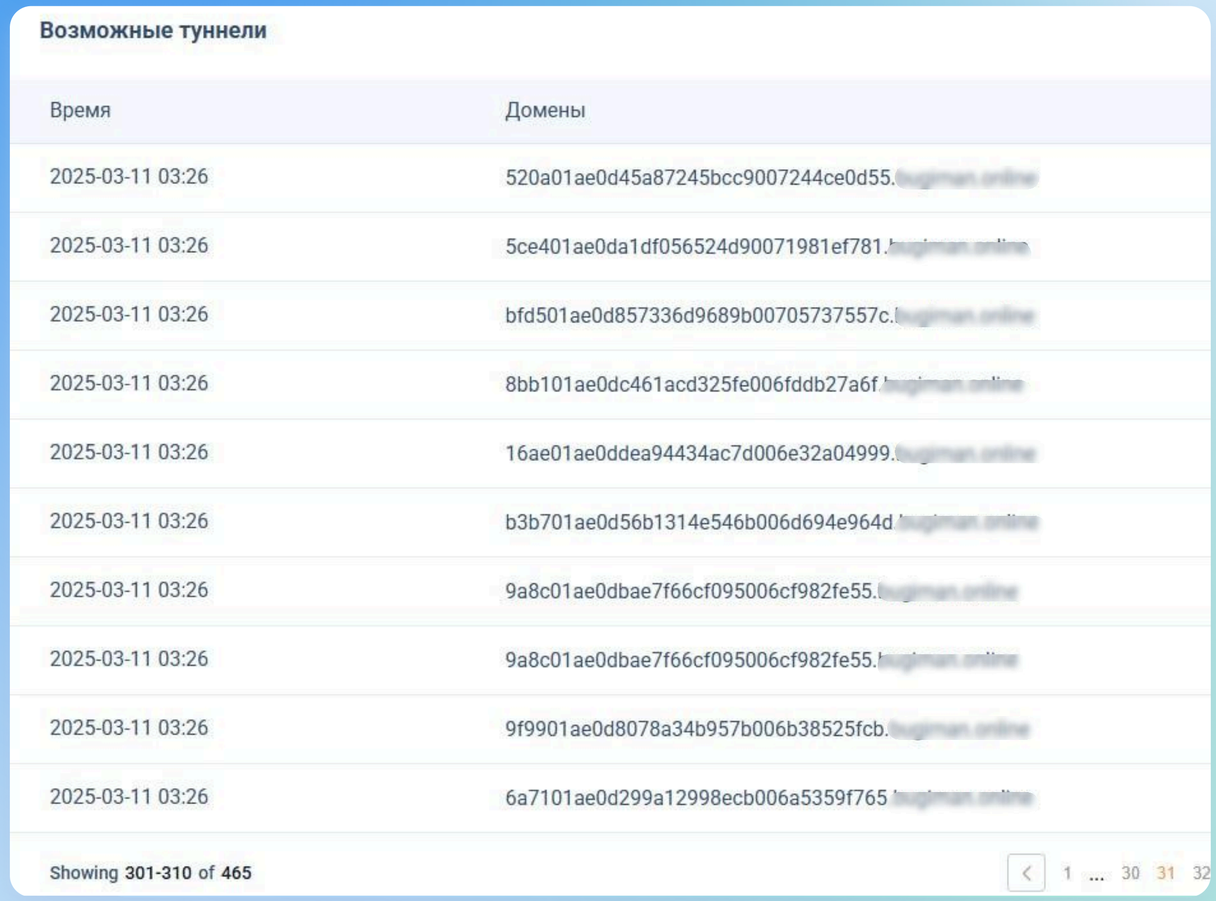


Схема DNS-туннеля



Как передается полезная нагрузка

Любая полезная нагрузка может быть передана прямо в самом домене в виде текста



```
Autodetecting DNS query type (use -T to override).iodine: Received unsupported encoding
.iodine: Received unsupported encoding
.....iodine: Received unsupported encoding
.iodine: Received unsupported encoding
....iodine: Received unsupported encoding
.iodine: Received unsupported encoding
```

Iodine проверяет какие типы DNS-пакетов вообще подходят для полезной нагрузки

Проверяем максимально возможный размер полезной нагрузки в пакете

```
Autoprobing max downstream fragment size... (skip with -m fragsize)
768 not ok.. 384 not ok.. 192 ok.. 288 not ok.. 240 not ok.. 216 not ok.. 204 ok.. 210 ok.. 213 ok.. 214 ok.. will use 214-2=212
Setting downstream fragment size to max 212...
```

```
root@[redacted]:~# wget http://[redacted].ru/test.csv
--2025-02-02 17:18:45--  http://[redacted].ru/test.csv
Resolving [redacted].ru ([redacted].ru)... [redacted].52.251
Connecting to [redacted].ru ([redacted].ru)|[redacted].52.251|:80... connected.
HTTP request sent, awaiting response... 301 Moved Permanently
Location: https://[redacted].ru/test.csv [following]
--2025-02-02 17:18:46--  https://[redacted].ru/test.csv
Connecting to [redacted].ru ([redacted].ru)|[redacted].52.251|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 10535496 (10M) [application/octet-stream]
Saving to: ‘test.csv.2’

test.csv.2                          100%[=============================================================================>]  10.05M  10.0MB/s    in 1.0s
```

Передали файл 10Мб за 1 секунду

В случае если мы на файрволе заблокировали абсолютно все неизвестные исходящие DNS-подключения, скорость значительно снижается, но туннель продолжает работать

```
Saving to: ‘test.pdf.5’

test.pdf.5                          100%[=============================================================================>]  96.84K  12.8KB/s    in 67s

2025-02-14 13:17:23 (1.44 KB/s) - ‘test.pdf.5’ saved [99162/99162]
```

Бесплатные лайфхаки для замедления DNS-туннелей

1

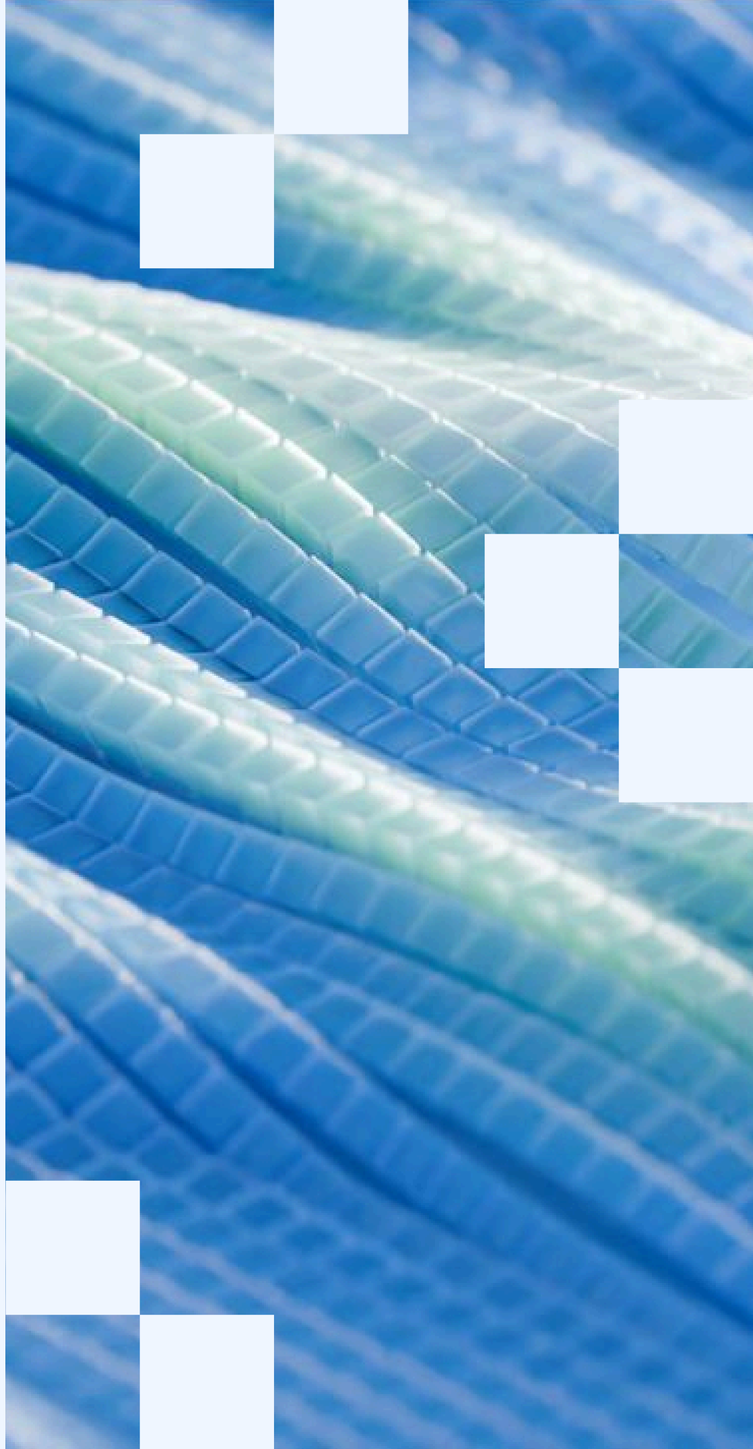
Можно закрыть 53 порт

Скорость передачи информации уменьшится в 1000 раз

2

Анализируйте DNS-трафик

Поможет лучше понять, что происходит в сети



«DNS-туннели не смогут нас коснуться»

Убеждение подавляющего большинства компаний.
Некоторые убеждены, что они защищены по белым спискам

ТОП блокировок по категориям за 2025

Оставьте мне контакты,
и я свяжусь с вами