Компьютерные сети

Протоколы туннелирования и VPN-технологии

Поломошнов И.С.

преп. каф. ИБ, ИМФКН, БГУ

Вопрос:

- Зачем нужны туннели и VPN?

- В современных сетях данные часто передаются через недоверенные каналы (Интернет).
- Чтобы обеспечить конфиденциальность, целостность и аутентификацию, используют виртуальные частные сети (VPN) и протоколы туннелирования.

Основные задачи:

- Защита трафика от прослушивания (шифрование)
- Сокрытие IP-адреса и местоположения
- Объединение удаленных офисов в единую сеть
- Безопасный доступ к корпоративным ресурсам
- Обход географических блокировок и цензуры (может преследоваться по закону)
- > Туннелирование — это инкапсуляция одного сетевого протокола в пакеты другого. Например, пакет IPv4 внутри пакета UDP.

Классификация

- Протоколы можно разделить на несколько поколений и подходов:

Категория	Примеры
Старые, небезопасные	PPTP
Транспортный уровень	IPsec (ESP/AH), L2TP
Прикладной уровень	OpenVPN, SSH, SSTP, XRay
Туннелирование L2	PPPoE, L2TP
Современные стандарты	WireGuard, XRay

> Важно: Некоторые протоколы работают в паре: L2TP + IPsec, IKEv2 + IPsec, PPPoE + PPP.

Описание основных протоколов

PPTP (Point-to-Point Tunneling Protocol)
Год создания: 1996 (Microsoft)
Порт: TCP 1723 + GRE (протокол 47)
Шифрование: MPPE (до 128 бит), RC4
Аутентификация: MS-CHAPv2, PAP, CHAP
Безопасность: Критически уязвим. MS-CHAPv2 взломан (2012). Возможны атаки "Man-in-the-Middle".
Применение: Полностью устарел. Использовать категорически не рекомендуется ни при каких условиях.
Особенности работы: Создает PPP-сессию внутри GRE-туннеля. Заголовок GRE не шифруется, что позволяет анализировать трафик.

L2TP (Layer 2 Tunneling Protocol) + IPsec
Год создания: 1999 (IETF)
Порты: UDP 500 (IKE), UDP 4500 (NAT-T), UDP 1701 (L2TP)
Шифрование: Сам L2TP не шифрует. В паре с IPsec дает шифрование (AES-256, AES-128, 3DES)
Аутентификация: IPSec IKE (PSK или сертификаты) + PPP-аутентификация (PAP, CHAP, EAP)
Безопасность: Средняя. Уязвим к некоторым DoS-атакам, но в целом надежен при правильной настройке.
Применение: Встроен во все ОС (Windows, macOS, iOS, Android, Linux). Часто используется на роутерах.
Особенности работы: L2TP инкапсулирует PPP-кадры в UDP, затем IPsec шифрует весь пакет. Двойная инкапсуляция создает дополнительный overhead (до 32 байт), что снижает MTU до ~1300 байт.

IPsec (Internet Protocol Security)
Год создания: 1995 (IETF, постоянно обновляется)
Режимы: Транспортный (шифрует только payload, оставляя IP-заголовок открытым) и туннельный (шифрует весь пакет целиком)
Протоколы внутри: AH (Authentication Header — только целостность), ESP (Encapsulating Security Payload — шифрование + целостность)
Порты: UDP 500 (IKE), UDP 4500 (NAT-T), протоколы ESP (50) и AH (51)
Аутентификация: PSK (Pre-Shared Key) или сертификаты X.509
Безопасность: Хорошая. Проходит независимые аудиты.
Применение: Site-to-Site VPN, корпоративные сети, защита маршрутизаторов.
Особенности работы: IKE (Internet Key Exchange) версии 1 и 2 управляют ключами. При прохождении через NAT ESP ломается, поэтому используется NAT-T (NAT Traversal), инкапсулирующий ESP в UDP 4500

IKEv2 (Internet Key Exchange version 2) — подвид IPsec
Год создания: 2014 (IETF)
Порт: UDP 500, UDP 4500
Шифрование: AES-256-GCM, ChaCha20-Poly1305 (через IPsec ESP)
Аутентификация: EAP (логин/пароль), сертификаты, PSK
Безопасность: Хорошая. Используется в Windows, iOS, Android как стандартный VPN-клиент.
Применение: Мобильные устройства, быстрые переключения между сетями (WiFi → LTE без разрыва VPN).
Особенности работы: Использует MOBIKE (Mobility and Multihoming) — клиент может сменить IP-адрес без переустановки туннеля. Встроен в большинство ОС нативно.

PPPoE (Point-to-Point Protocol over Ethernet)
Год создания: 1999 (IETF)
Порт: Неприменимо (работает напрямую с Ethernet-кадрами)
Шифрование: Нет (в спецификации). Теоретически может работать с MPPE поверх PPP, но практически не используется.
Аутентификация: PAP, CHAP, MS-CHAPv2
Безопасность: Нет. Пароль может передаваться в открытом виде (PAP). Шифрование отсутствует.
Применение: Исключительно для доступа провайдера (DSL, FTTB, Ethernet-вход в квартиру). Не является VPN в классическом смысле.
Особенности работы: Инкапсулирует PPP-кадры в Ethernet-кадры с полями Destination/Source MAC.

OpenVPN
Год создания: 2002 (Джеймс Йонан)
Порт: UDP 1194 (по умолчанию) или TCP 443 (для маскировки под HTTPS)
Шифрование: OpenSSL/BoringSSL (AES-256-GCM, AES-128-CBC, ChaCha20-Poly1305)
Аутентификация: TLS (сертификаты клиента и сервера) + опционально логин/пароль + двухфакторная аутентификация
Безопасность: Отличная. Проходит аудиты, используется правительствами и банками.
Применение: Корпоративные VPN, удаленный доступ, обход блокировок, P2P-сети.
Особенности работы: Работает в userspace (не в ядре), что дает гибкость, но снижает скорость. Использует TLS-рукопожатие перед передачей данных.

SSTP (Secure Socket Tunneling Protocol)
Год создания: 2007 (Microsoft)
Порт: TCP 443 (HTTPS)
Шифрование: SSL/TLS (AES-256, 3DES, RC4 — зависит от версии SSL)
Аутентификация: MS-CHAPv2, EAP (TLS, MSCHAPv2), PAP, CHAP
Безопасность: Хорошая. Использование HTTPS делает трафик неотличимым от обычного веб-трафика.
Применение: Windows-среды, обход блокировок (почти невозможно отфильтровать без полного DPI).
Особенности работы: Инкапсулирует PPP-кадры в HTTPS (TCP 443). Только Microsoft имеет полноценную реализацию.

SSH (Secure Shell) туннелирование
Год создания: 1995 (Tatu Ylönen)
Порт: TCP 22
Режимы: Dynamic (SOCKS5-прокси), Local, Remote (удаленный порт → локальный хост)
Шифрование: ChaCha20-Poly1305, AES-128/256-GCM, AES-128/256-CBC, 3DES
Аутентификация: Пароль, публичный ключ, GSSAPI (Kerberos)
Безопасность: Хорошая. Стандарт де-факто для удаленного управления серверами.
Применение: Проброс портов, безопасный доступ к одному серверу, временный SOCKS-прокси.
Особенности работы: Не создает полноценный VPN-интерфейс. Низкая скорость из-за перекодирования потоков и работы в userspace.

WireGuard
Год создания: 2018 (Джейсон Доненфельд, вошел в ядро Linux 5.6)
Порт: UDP 51820 (по умолчанию, можно изменить)
Шифрование: ChaCha20 для шифрования, Poly1305 для аутентификации
Ключи: Curve25519 для DH (Diffie-Hellman), BLAKE2s для хеширования
Аутентификация: Криптографическая
Безопасность: Отличная. Кодовая база ~4000 строк (для сравнения: OpenVPN — ~70 000 строк). Прошел несколько аудитов (Cure53, OSTIF). Считается безопасным по умолчанию.
Применение: Все современные сценарии: Site-to-Site, клиент-сервер, mesh-сети (Tailscale, Netmaker), провайдерские VPN (Mullvad, IVPN), домашние роутеры.
Особенности работы: Нет TCP over TCP: В отличие от OpenVPN, WireGuard использует только UDP.

XRay (Project X / V2Ray core)
Год создания: 2018 (как форк V2Ray, который появился в 2015)
Порты: Любые: TCP, UDP, WebSocket (80/443), HTTP/2, gRPC, QUIC, KCP
Протоколы внутри: VMess, VLESS, Trojan, Shadowsocks, SOCKS, HTTP, Dokodemo-door
Шифрование: AES-128-GCM, ChaCha20-Poly1305, None (не рекомендуется)
Аутентификация: UUID для VMess/VLESS, пароль для Shadowsocks, сертификаты для TLS
Безопасность: Средняя. Решение не стандартизировано IETF, не проходило крупных независимых аудитов.
Применение: Исключительно для обхода Deep Packet Inspection. Не предназначен для корпоративной безопасности.
Особенности работы: XRay — это платформа прокси с поддержкой маскировки трафика. Может прятать VPN-трафик внутри WebSocket поверх TLS, имитируя реальный HTTPS-сеанс.

Сравнительная таблица

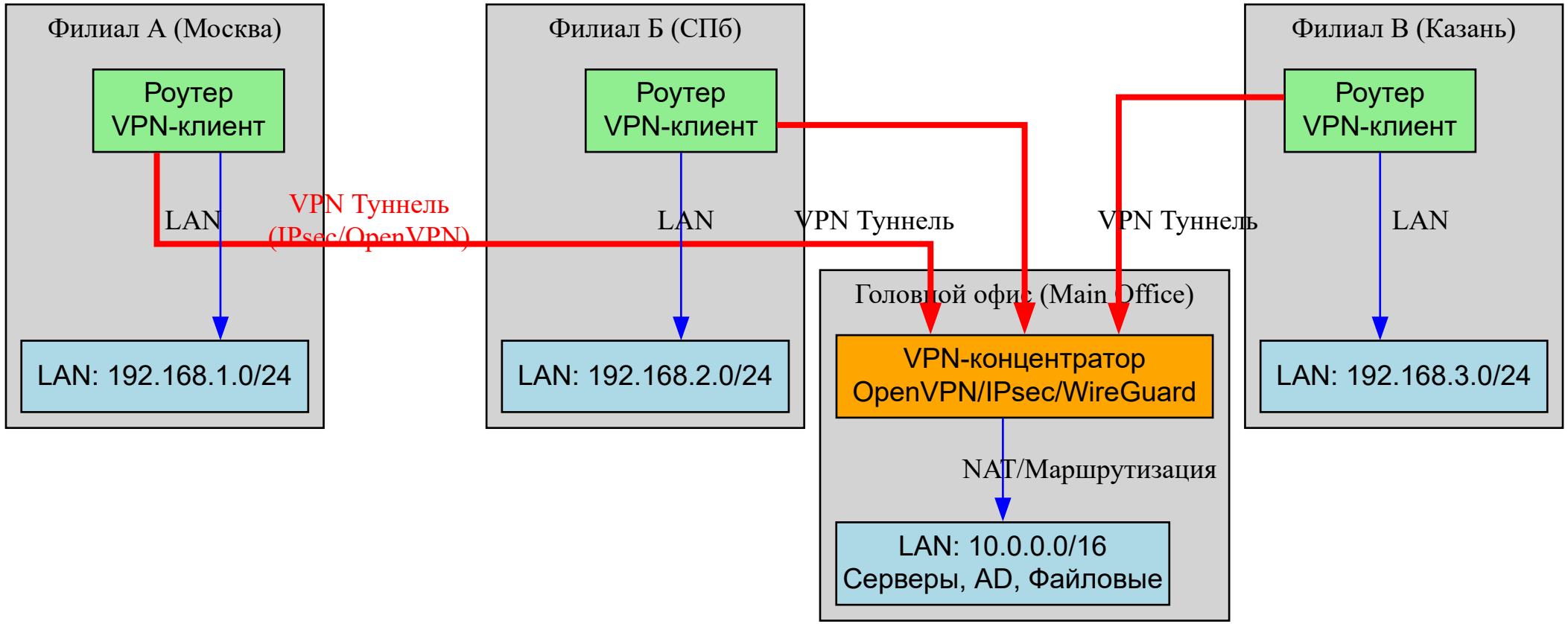
Протокол	ОС по умолч.	Шифрование	Порт(ы)	Скорость	Без-ть	Сложность
PPTP	Все (устар.)	MPPE (RC4)	TCP 1723 + GRE	Средняя	Критич.	Низкая
L2TP/IPsec	Все	AES, 3DES (через IPsec)	UDP 500,4500,1701	Низкая	Средняя	Средняя
IPsec/IKEv2	Все (совр.)	AES-256	UDP 500,4500, ESP	Высокая	Хорошая	Средняя
PPPoE	PC/ роутеры	Нет (редко MPPE)	Ethernet (broadcast)	Высокая	Нет	Низкая
OpenVPN	Все (доп. ПО)	AES-256-GCM, ChaCha20	UDP 1194 / TCP 443	Средняя	Отличная	Высокая

Общий вывод

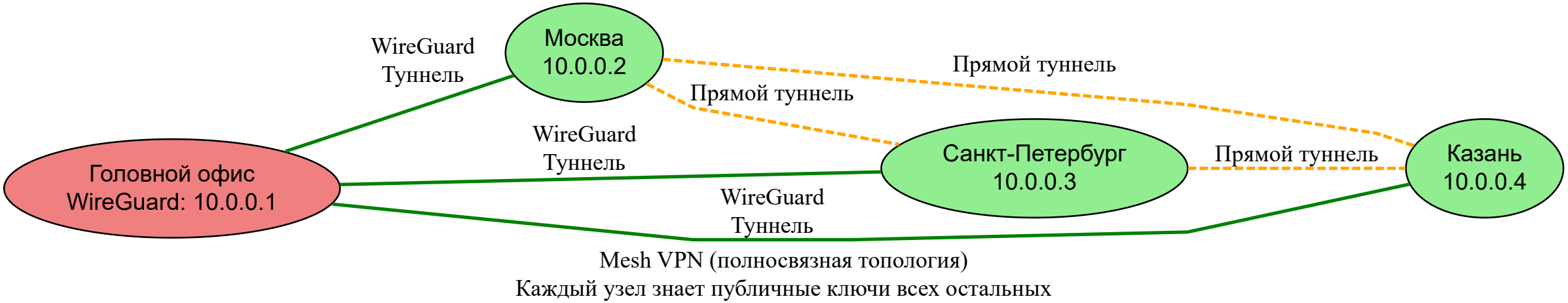
- PPTP — исторический артефакт, не должен использоваться в защищенных сетях.
- PPPoE — не VPN, а технология доступа провайдера.
- L2TP/IPsec — совместимый, но медленный компромисс.
- IKEv2 — современный стандарт для мобильных устройств.
- OpenVPN — золотая середина по безопасности и обходу блокировок, но сложен в настройке.
- SSTP — отличный выбор, если весь клиентский парк — Windows.
- SSH — инструмент администратора, но не для полноценного VPN.
- XRay (V2Ray) — узкоспециализированное решение, сложное, но очень эффективное в руках эксперта.

> Главный принцип безопасности: никогда не используйте устаревшие протоколы (PPTP, L2TP без IPsec). Всегда включайте аутентификацию по сертификатам и PFS (Perfect Forward Secrecy).

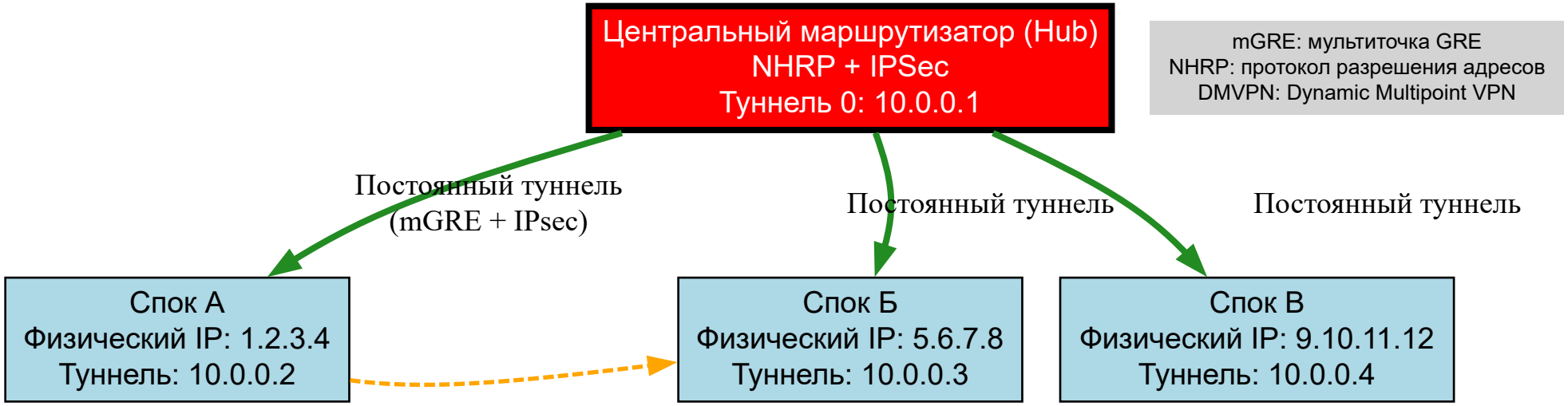
Site-to-Site VPN (классика с центральным офисом)



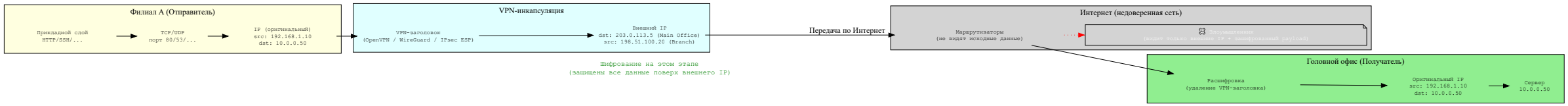
Mesh VPN (WireGuard / Tinc / Nebula)



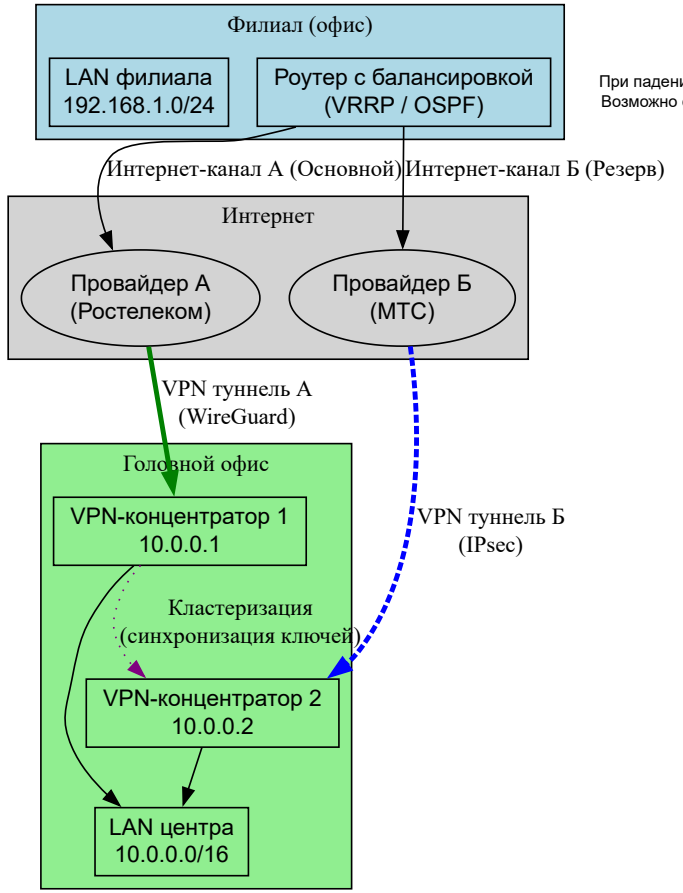
Hub-and-Spoke с резервированием (DMVPN)



Защищенный туннель через Интернет (слои инкапсуляции)



Резервирование каналов (Active-Backup + VPN)



При падении основного канала трафик автоматически переключается на резервный
Возможно объединение каналов (bonding) для увеличения пропускной способности

Проблема MTU и фрагментации в VPN

- Что такое MTU?
- MTU (Maximum Transmission Unit) — максимальный размер пакета, который может пройти через сетевое устройство без фрагментации. Стандарт для Ethernet — 1500 байт.

Как VPN убивает MTU

VPN добавляет свои заголовки к каждому пакету:

```
Оригинальный пакет:          [IP-заголовок (20) + TCP (20) + Payload (1460)] = 1500 байт
После VPN-инкапсуляции:      [Внешний IP (20) + VPN-заголовок (x) + оригинальный пакет (1500)] = 1500+x байт → ФРАГМЕНТАЦИЯ!
```

Реальный overhead популярных протоколов

Протокол	Дополнительные байты	Рекомендуемый MTU туннеля
WireGuard	32-64 байта	1420-1440
OpenVPN (UDP)	40-80 байт	1400-1420
OpenVPN (TCP)	60-100 байт	1350-1400
IPsec (ESP)	50-80 байт	1380-1420
L2TP/IPsec	70-110 байт	1300-1350
PPTP	20-40 байт	1450

Признаки проблем с MTU

- Некоторые сайты открываются, некоторые нет
- SSH подключается, но зависает при вводе команд
- Email-клиент работает, но не отправляет вложения
- curl зависает на больших ответах

Типичные ошибки и их диагностика

Ошибка	Симптомы	Диагностика	Решение
MTU mismatch	Сайты грузятся частично	ping -M do -s 1472 <host>	Уменьшить MTU туннеля
NAT Traversal проблемы	Клиент подключается, нет трафика	tcpdump -i eth0 port 500 or 4500	Включить NAT-T, пробросить порты
Clock skew	Ошибка TLS handshake	date на сервере и клиенте	Синхронизировать NTP
Routing loop	Трафик не доходит, высокий ping	traceroute, ip route	Проверить AllowedIPs, метрики
Kill switch не работает	Трафик утекает при падении VPN	curl ifconfig.me	Настроить policy routing

Глоссарий терминов

Термин	Расшифровка	Простое объяснение
DPI	Deep Packet Inspection	Просмотр содержимого пакетов для блокировки
NAT	Network Address Translation	Один внешний IP для многих устройств в LAN
NAT-T	NAT Traversal	Технология, позволяющая VPN работать через NAT
PFS	Perfect Forward Secrecy	При компрометации ключа прошлые сессии не расшифровать
mGRE	Multipoint GRE	Один туннель для многих точек (DMVPN)
NHRP	Next Hop Resolution Protocol	Узнает IP другого филиала в DMVPN
ROA	Routing on Authentication	Маршрутизация на основе сертификата (WireGuard)

Глоссарий терминов

Термин	Расшифровка	Простое объяснение
Handshake	-	Обмен ключами при установке соединения
Roaming	-	Смена IP без разрыва туннеля
Kill switch	-	Блокировка интернета при падении VPN

Контрольные вопросы

- Чем отличается транспортный режим IPsec от туннельного?
- Почему PPTP признан небезопасным?
- Зачем L2TP нужен IPsec?
- Как злоумышленник может определить, что вы используете WireGuard?
- Какой протокол автоматически переподключается при смене сети (WiFi → LTE)?

«Контрольные» ответы

- Чем отличается транспортный режим IPsec от туннельного?
- - *Ответ: В транспортном шифруется только payload, а IP-заголовок остается открытым; в туннельном — весь исходный пакет целиком помещается в новый IP-пакет.*
- Почему PPTP признан небезопасным?
- - *Ответ: Из-за критических уязвимостей в протоколе аутентификации MS-CHAPv2.*
- Зачем L2TP нужен IPsec?
- - *Ответ: L2TP не предоставляет шифрования, а только инкапсуляцию, и без IPsec весь трафик идет открытым текстом.*
- Как злоумышленник может определить, что вы используете WireGuard?
- - *Ответ: по характерным размерам пакетов handshake*
- Какой протокол автоматически переподключается при смене сети (WiFi → LTE)?
- - *Ответ: IKEv2 (благодаря MOBIKE) и WireGuard (благодаря встроенному роумингу).*

Спасибо за внимание

Вопросы?