Что такое VPN?

VPN, или **Virtual Private Network**, создаёт зашифрованный туннель между вашим устройством и удалённым сервером. Всё, что вы отправляете через этот туннель, скрыто от вашей сети, провайдера и любых, кто следит за вами в **public WiFi**.

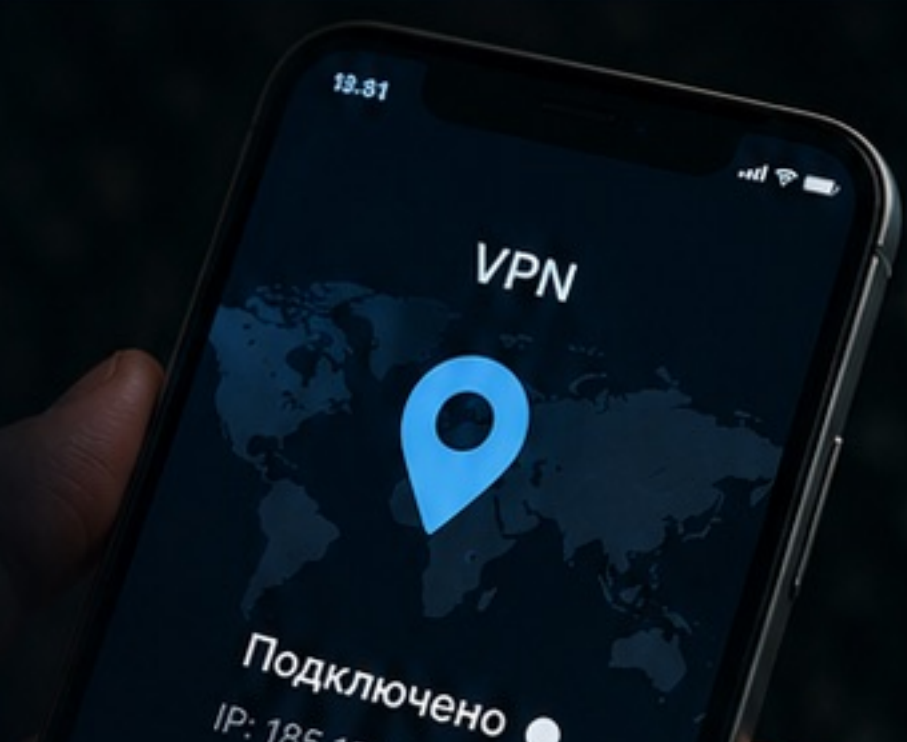
Скрывает ваш трафик

Данные перемешиваются и шифруются, поэтому посторонние видят только бессмысленный **шум** вместо ваших действий.



Маскирует ваше местоположение

Сайты видят **IP**-адрес **VPN**-сервера, а не ваш реальный IP.



Защищает открытые сети

Public и общие **WiFi** становятся безопаснее, потому что туннель защищает каждый пакет данных.



Совет: Используйте VPN, чтобы сохранить приватность, обойти ограничения и защитить своё соединение.

Что такое VPN protocol?

Если VPN — это туннель, то protocol — это план, по которому он строится и защищается. Он определяет три вещи.

VPN = транспорт. **Protocol** = движок.

Аутентификация

Как каждая сторона доказывает, кто она, используя ключи, сертификаты или пароли.



Шифрование

Какой шифр перемешивает ваши данные, чтобы их могли прочитать только два конца туннеля.



Транспорт

Как пакеты на самом деле передаются по интернету через UDP или TCP.



Совет: Понимание VPN protocol помогает выбрать лучший баланс между скоростью, безопасностью и совместимостью.

Пирамида компромиссов

Ни один protocol не выигрывает по всем пунктам. Каждый балансирует между четырьмя силами: одна усиливается, другая — уступает. Поэтому лучший выбор зависит от того, что вам действительно нужно.

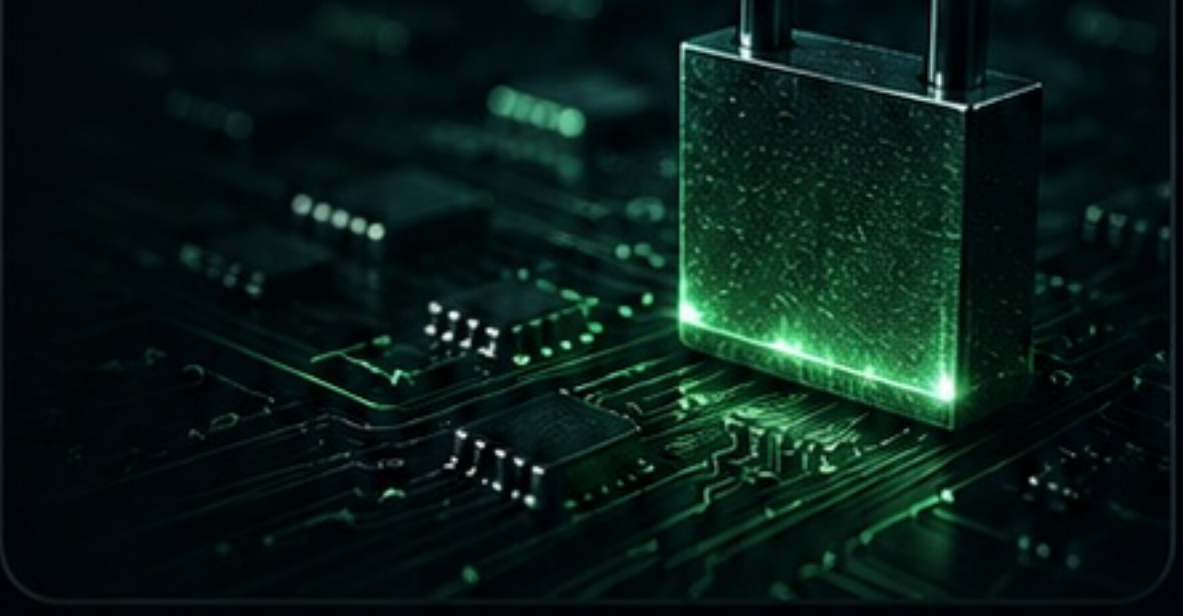
Speed
Скорость

Насколько быстро туннель передаёт данные.



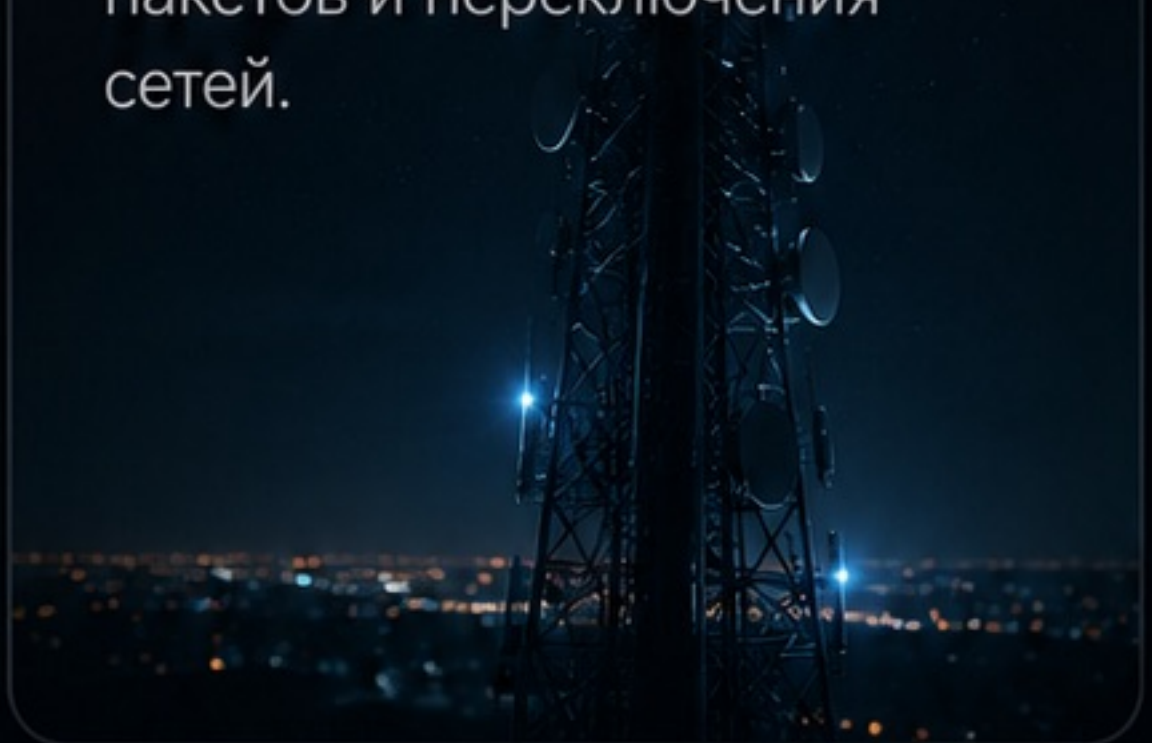
Security
Безопасность

Насколько сильное шифрование используется.



Stability
Стабильность

Насколько хорошо выдерживает потери пакетов и переключения сетей.



Compatibility
Совместимость

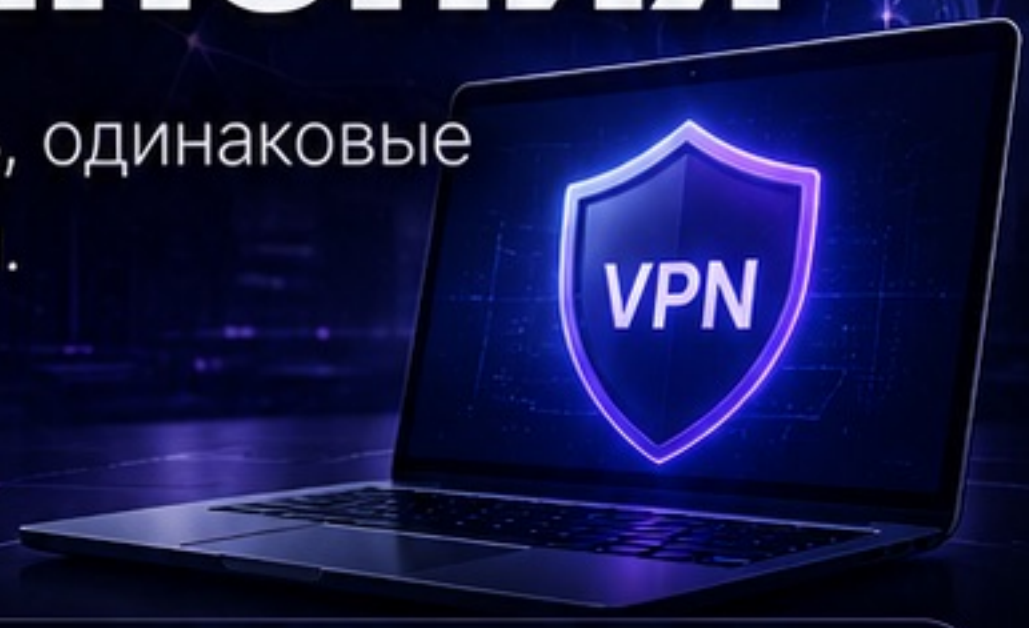
Сколько устройств поддерживают его «из коробки».



Совет: Определите, что для вас важнее всего — и выбирайте protocol под эту задачу.

Анатомия VPN-соединения

Каждый раз, когда вы подключаетесь, одинаковые **5 шагов** происходят за доли секунды.



1 Рукопожатие

Ваше устройство и VPN-сервер соглашаются на правила и создают **ключи**.



2 Аутентификация

Обе стороны подтверждают свою личность с помощью **сертификатов** или **ключей**.



3 Шифрование

Новый **сессионный ключ** перемешивает (шифрует) все ваши дальнейшие данные.

4 Туннель

Создаётся зашифрованный **канал**, который оборачивает каждый пакет данных.



5 Транспорт

Данные передаются через **UDP** для скорости или **TCP** для надёжности.

Совет: Понимая, как работает VPN, вы лучше выбираете protocol под свои задачи — скорость, безопасность и стабильность.

OpenVPN

THE VERSATILE VETERAN

Open-source и проверенный в боях, OpenVPN работает почти где угодно. Использует сильное **AES-256** шифрование и может передавать данные через **TCP** или **UDP**, проходя через строгие **firewall** так, что выглядит как обычный **secure web traffic**.



Преимущества

- **Проверенный, зрелый и надёжный**
- **Гибкие порты:** легко проходит через **firewall**
- Очень сильное шифрование **(AES-256)**

Обратите внимание

- Тяжелее на вашем устройстве
- Может быть медленнее, чем новые **protocol**
- Требует больше настроек



SPEED	SECURITY	STABILITY
●●●○○	●●●●●	●●●●●
Средняя	Отличная	Отличная

PROTOCOL 02

07/15

WireGuard

СОВРЕМЕННЫЙ СПРИНТЕР

Лёгкий и современный **protocol** с крошечной кодовой базой (~4 000 строк), поэтому его легко проверить и доверять. Использует быстрое **ChaCha20** шифрование, подключается почти мгновенно и экономит заряд батареи — идеален для телефонов.



Преимущества

Молниеносная скорость

Минимальные задержки, высокая пропускная способность.



Крошечная кодовая база

Всего ~4 000 строк — легко аудитить.



Отличная автономность

Почти не расходует батарею на мобильных устройствах.



На что обратить внимание

UDP-only

Работает только через UDP по задумке.



Новее и менее универсален

Поддерживается не везде, чем старые protocol.



Чувствителен к смене IP

Может потребовать переподключения при нестабильной сети.





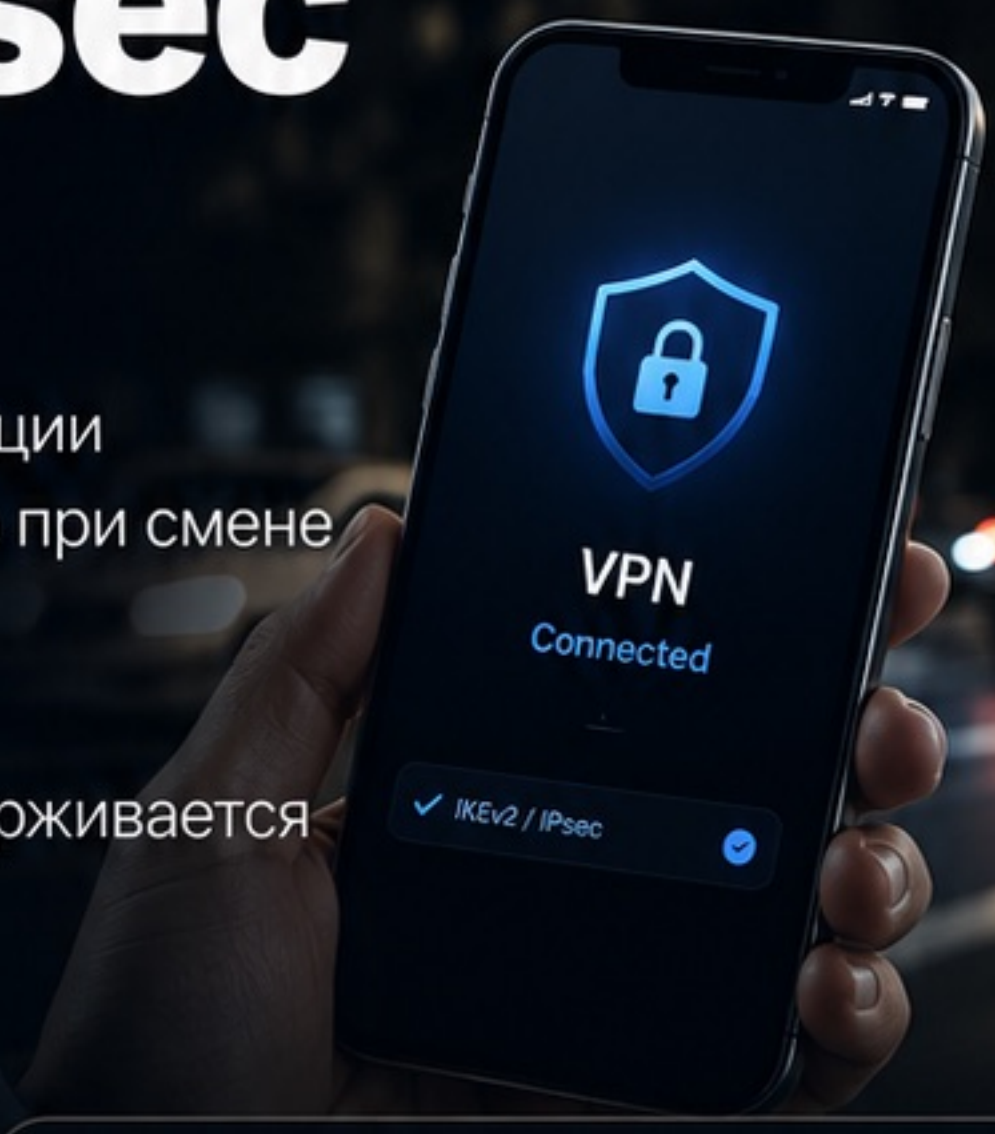
Быстро. Безопасно. Просто.

Speed	Security	Stability
●●●●●	●●●●●	●●●●○
Отличная	Отличная	Хорошая

IKEv2 / IPsec

THE MOBILE CHAMPION

Создан для движения. Благодаря функции MOBIKE, переподключается мгновенно при смене WiFi на cellular, поэтому туннель остается живым.
Быстрый, стабильный и нативно поддерживается на большинстве phones.



Преимущества

Мгновенные переподключения
Переключайтесь между WiFi и cellular без разрывов.

Быстрый и стабильный
Стабильная скорость и надежная связь.

Нативная поддержка на большинстве phones
Работает «из коробки» на iOS, Android и др.

Обратите внимание

Фиксированные UDP-порты
Могут быть заблокированы некоторыми сетями.

Менее открыт, чем другие
Не такой универсальный, как некоторые протоколы.

Меньше настроек
Меньше опций для тонкой настройки.

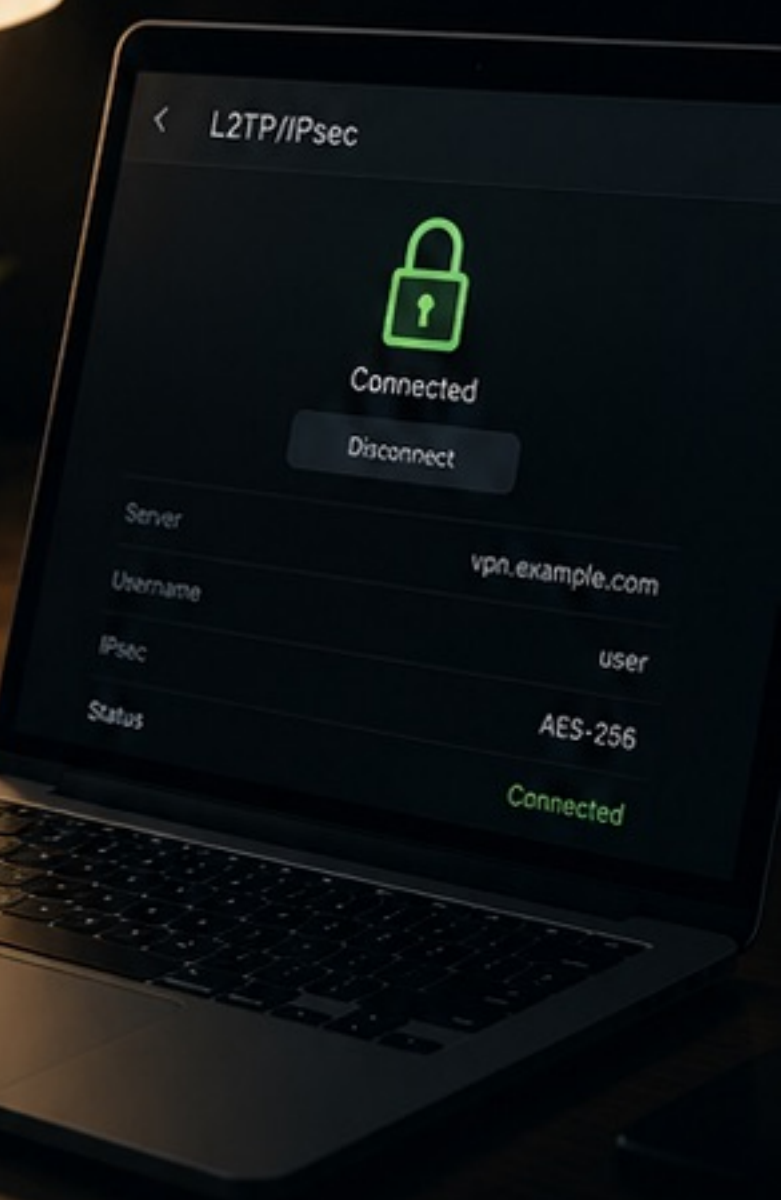


Всегда на связи. Всегда защищен.

SPEED	SECURITY	STABILITY
●●●●○	●●●●●	●●●●●
Хорошая	Отличная	Отличная

L2TP / IPsec

THE OLD RELIABLE



L2TP создаёт туннель, а **IPsec** добавляет шифрование сверху, поэтому данные упакованы дважды. Это широко поддерживается и просто настраивается, но двойная упаковка делает его медленнее альтернатив.

Преимущества

Широкая поддержка
Работает на большинстве устройств и ОС.

Простая настройка
Легко настроить даже новичку.

Надёжная безопасность
Проверенный временем и безопасный.

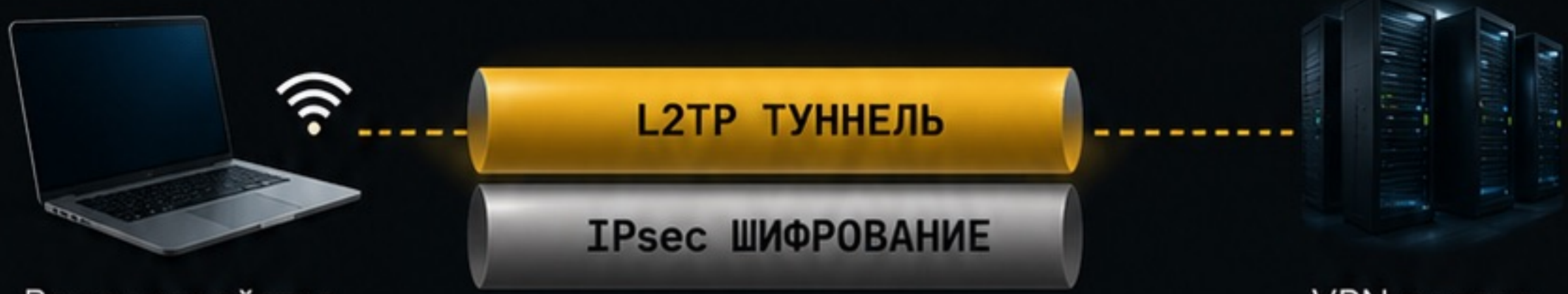
На что обратить внимание

Медленнее из-за двойной упаковки
Данные шифруются дважды.

Фиксированные порты
Легко могут быть заблокированы.

Менее скрытен
Легче обнаруживается файрволами.

Двойная защита, но больше накладных расходов



SPEED	SECURITY	STABILITY
●●●○○	●●●●○	●●●●○
Средняя	Отличная	Отличная

SSTP

THE FIREWALL BYPASSER

SSTP оборачивает ваш туннель в **TLS** и отправляет его через порт **443** — тот же порт, что и обычные **HTTPS**-сайты. Для **firewall** это выглядит как обычный **secure web traffic**, поэтому обнаружить и заблокировать его крайне сложно.



Преимущества

Обходит строгие firewalls
Легко проходит через жёсткие ограничения.

Сильное TLS шифрование
Данные защищены на уровне TLS.

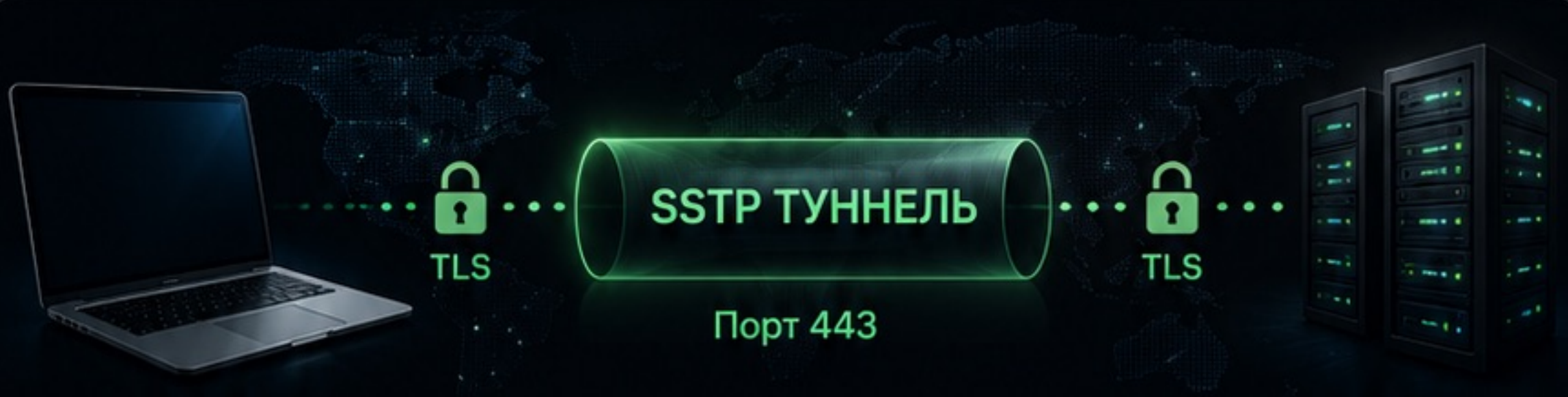
Похоже на обычный HTTPS
Не выделяется среди другого трафика.

На что обратить внимание

Привязан к одной экосистеме
Работает в основном в среде Microsoft.

Закрытый исходный код, меньше аудита
Меньше проверок со стороны сообщества.

Ограниченная поддержка платформ
Доступен не на всех устройствах и ОС.



Выглядит как **HTTPS**. Работает как **VPN**.

SPEED	SECURITY	STABILITY
●●●●○	●●●●○	●●●●○
Хорошая	Отличная	Отличная

PPTP

FAST BUT BROKEN

Самый старый протокол здесь. Быстрый и простой, потому что его **шифрование слабое** последующее взлом был давно. Современный атакующий может взломать его за часы, поэтому он устарел и небезопасен для приватности.



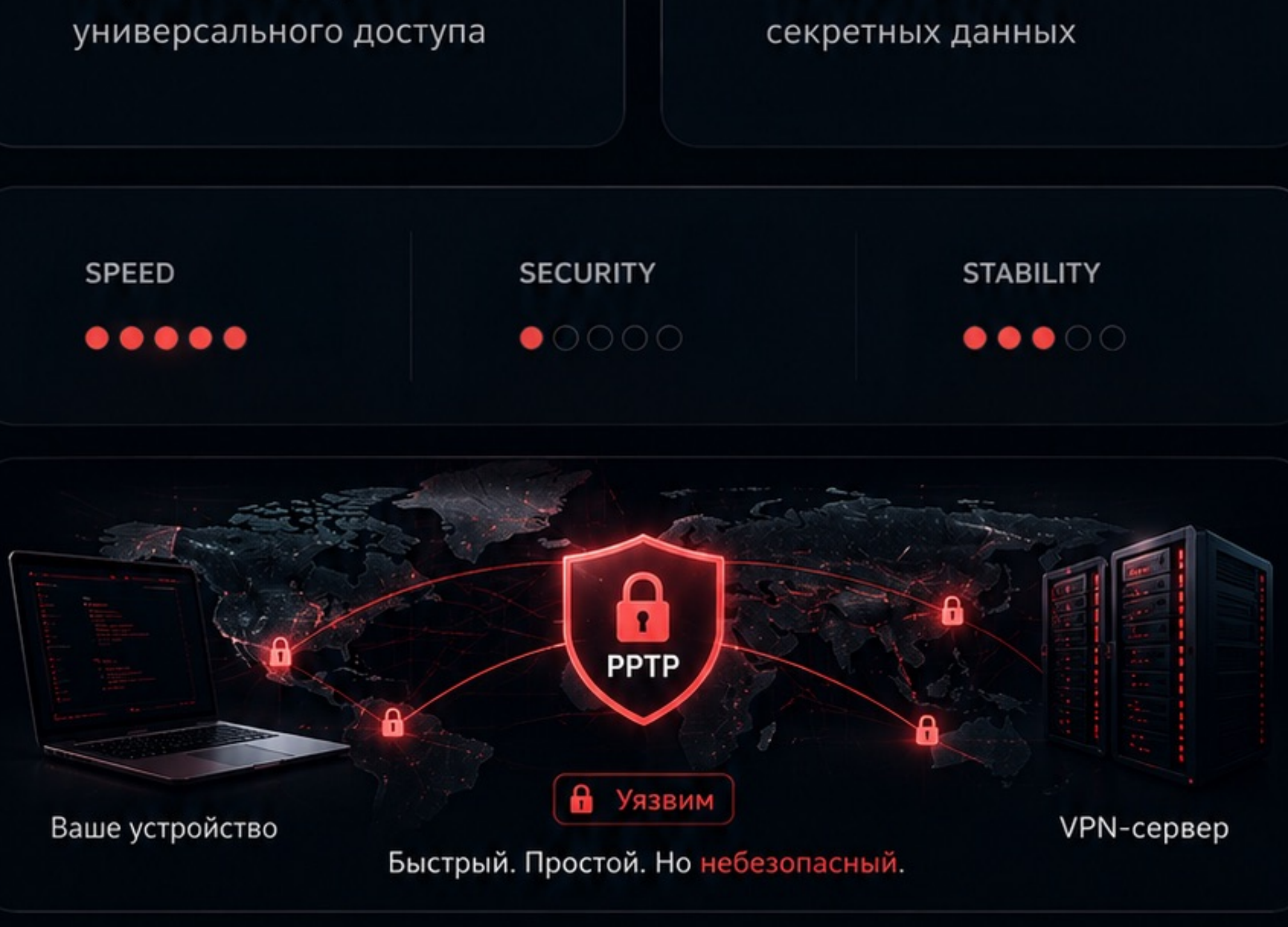
Преимущества

- Очень быстро
- Работает в старых системах
- Широкая поддержка универсального доступа

Недостатки

- Шифрование слабое
- Нет реальной конфиденциальности
- Небезопасно для секретных данных

SPEED	SECURITY	STABILITY
●●●●●	●○○○○	●●●○○



Быстрый. Простой. Но **небезопасный**.

Encryption, decoded



Сложные термины на этих слайдах не так страшны.
Вот что они означают простыми словами.

AES-256

Симметричный шифр стандарта gold.
256-битный ключ даёт миллиарды комбинаций — взлом практически невозможен.



ChaCha20-Poly1305

Быстрый современный шифр, который остаётся быстрым даже на телефонах без специального железа.



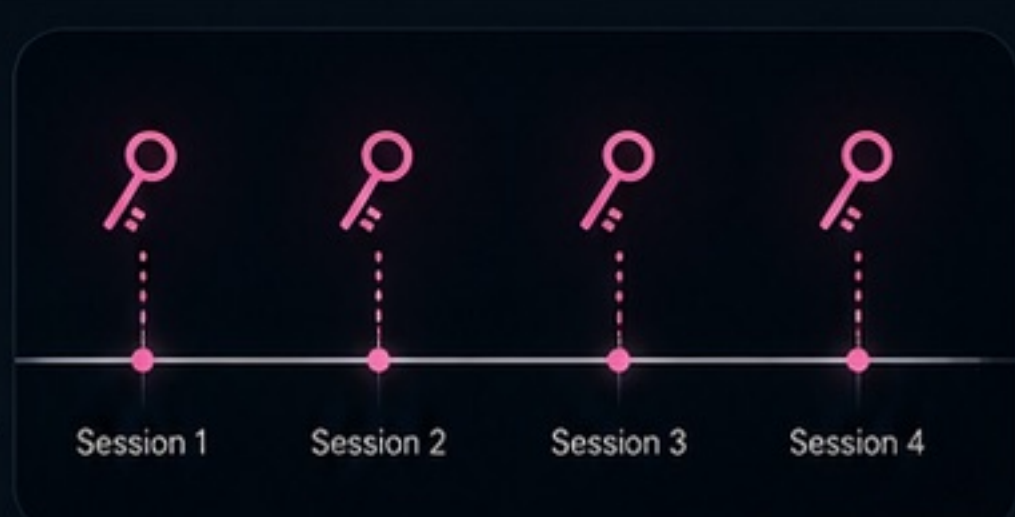
Key exchange

Как обе стороны тайно договариваются о ключе по открытому, но защищённому каналу.



Perfect Forward Secrecy

Новый ключ для каждой сессии, поэтому украденный ключ не откроет ваш прошлый трафик.



Сильное шифрование + Безопасный обмен + Защита сессий = Ваша приватность в безопасности

Side-by-side

Один экран, шесть протоколов.
Сохраните для следующей настройки VPN.



PROTOCOL	SPEED Скорость	SECURITY Безопасность	BEST FOR Лучше всего для
OpenVPN	●●●○○	●●●●●	All-round Универсальный
WireGuard	●●●●●	●●●●●	Speed Максимальная скорость
IKEv2	●●●●○	●●●●●	Mobile Мобильные устройства
L2TP	●●●○○	●●●●○	Compatibility Совместимость с устройствами
SSTP	●●●○○	●●●●○	Firewalls Обход строгих сетей
PPTP	●●●●●	●○○○○	Avoid Избегать (небезопасно)

Выбирайте протокол под свои задачи:
Speed, Security, Compatibility или обход Firewalls.



Какой выбрать?

Выбор зависит от ваших задач.
Каждый протокол — для своего случая.



Лучший выбор на все случаи

OpenVPN или WireGuard

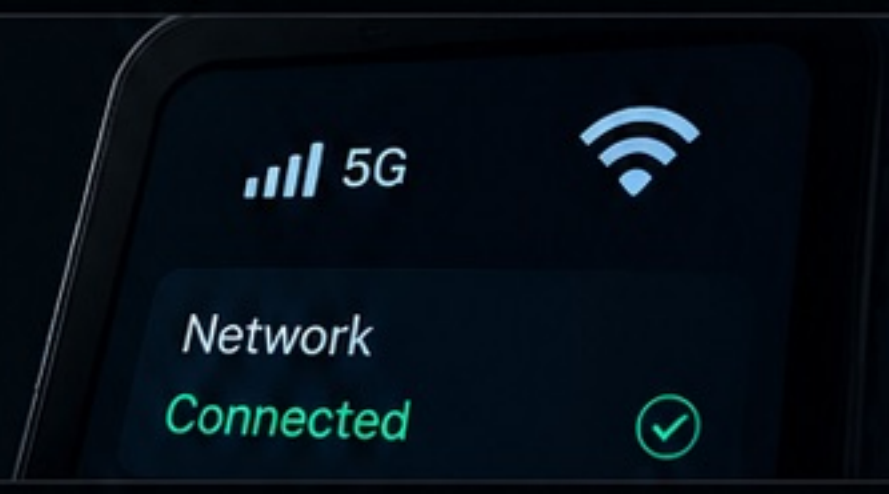
Самый быстрый

WireGuard



Для мобильных устройств
и смены сетей

IKEv2 / IPsec



Максимальная поддержка
устройств

L2TP / IPsec



За строгим firewall

**SSTP или OpenVPN
через порт 443**



Не для приватности

PPTP

Нет универсального решения.
Выбирайте под свои приоритеты:
Speed, Security, Compatibility или обход Firewalls.