Способы защиты информации

Основы сетей. Прокси-сервер. Межсетевые экраны. VPN.

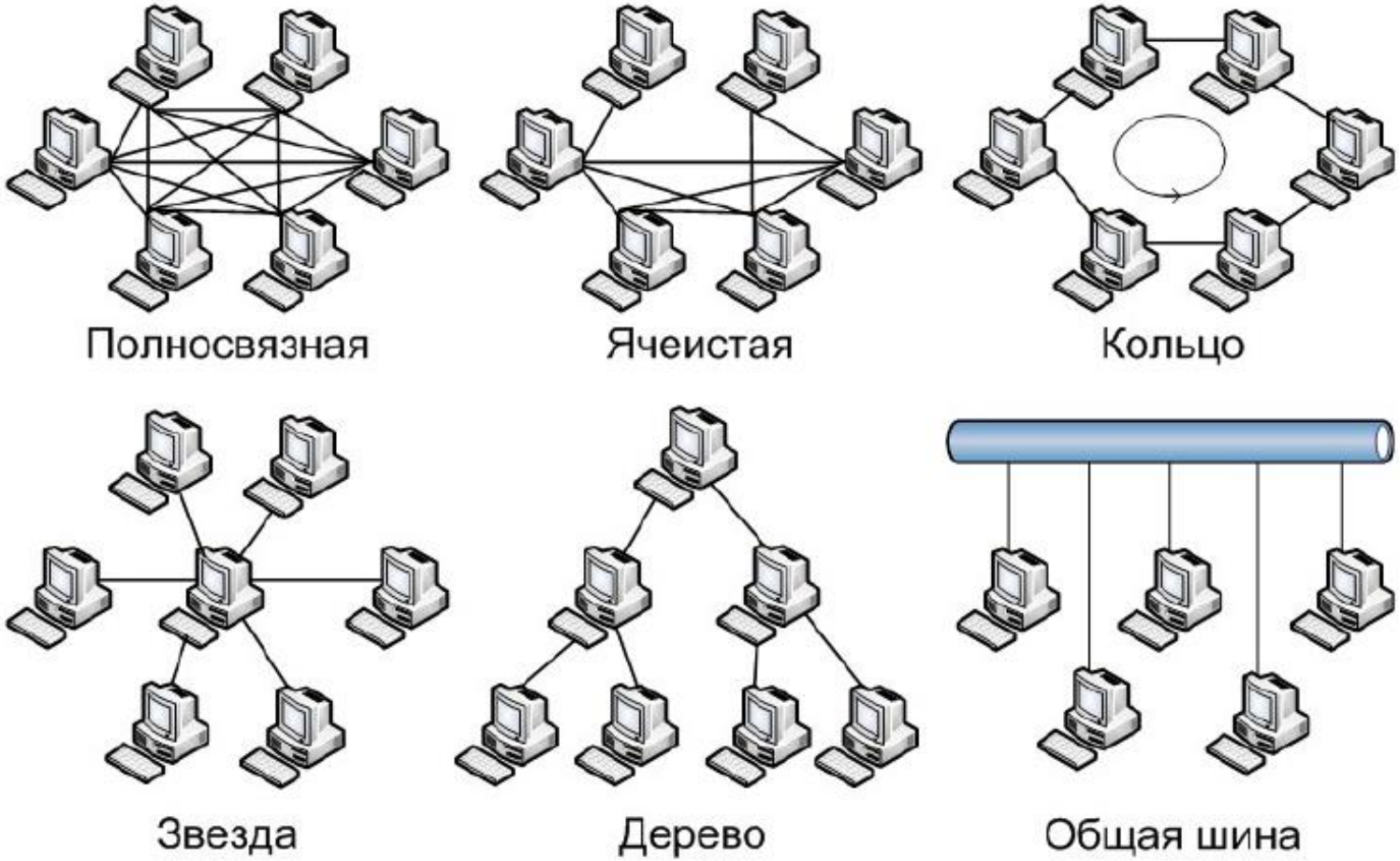
Сеть передачи данных – это совокупность устройств и систем, которые подключены друг к другу (логически или физически) и общающихся между собой (совокупность устройств и каналов связи между ними).

Узел сети (хост) — это устройство, соединённое с другими устройствами как часть компьютерной сети.

Сетевой протокол – это совокупность правил, методов, стандартов и реализующих их аппаратных и программных средств, совместно обеспечивающих взаимодействие компьютеров в компьютерной сети.

Маршрутизация – это процесс выбора маршрута от одного узла к другому внутри сети.

Топология сетей



OSI (Open Systems Interconnection - взаимодействие открытых систем) - это название соответствующего стандарта, рекомендуемого в качестве эталона всем разработчикам новых сетевых протоколов.

ISO (International Standard Organization - международная организация по стандартам) - это название организации, разработавшей указанный стандарт.

7	Прикладной уровень (application layer)
6	Уровень представления (presentation layer)
5	Сеансовый уровень (session layer)
4	Транспортный уровень (transport layer)
3	Сетевой уровень (network layer)
2	Канальный уровень (data link layer)
1	Физический уровень (physical layer)

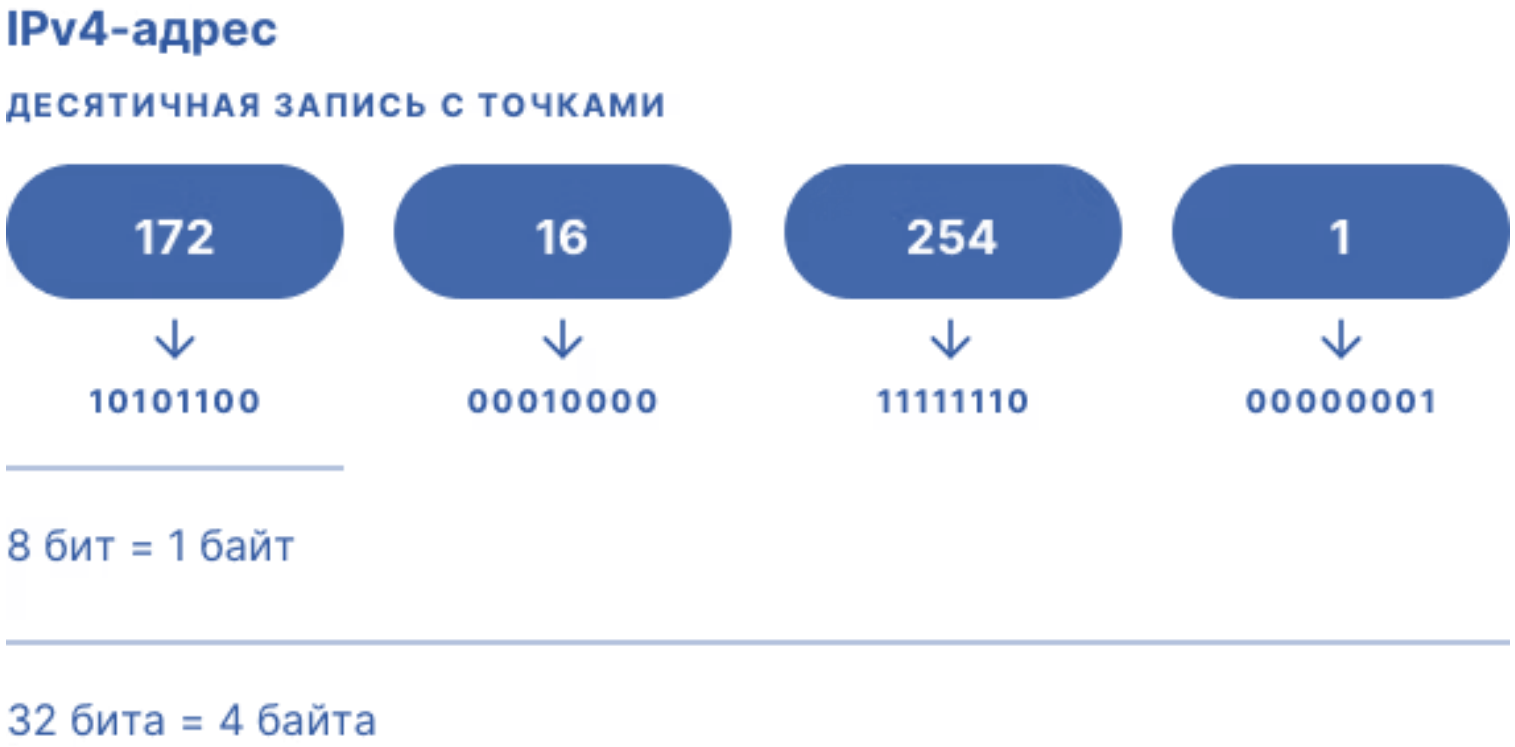
Данные	**Прикладной** (доступ к сетевым службам)	Осуществляет взаимодействие между пользователем и сетью. Взаимодействует с приложениями на стороне клиента.	HTTP, FTP, Telnet, SSH, SNMP
Данные	**Представления** (представление и кодирование данных)	Осуществляет преобразование данных в нужную форму, шифрование/кодирование, сжатие.	MIME, SSL
Данные	**Сеансовый** (управление сеансом связи)	Управляет созданием/поддержанием/завершением сеанса связи.	L2TP, RTCP
Блоки	**Транспортный** (безопасное и надежное соединение точка-точка)	Предназначен для доставки данных без ошибок, потерь и дублирования в той последовательности, как они были переданы. Выполняет сквозной контроль передачи данных от отправителя до получателя.	TCP, UDP
Пакеты	**Сетевой** определение пути и IP (логическая адресация)	Его основными задачами являются маршрутизация – определение оптимального пути передачи данных, логическая адресация узлов. Кроме того, на этот уровень могут быть возложены задачи по поиску неполадок в сети (протокол ICMP). Сетевой уровень работает с пакетами.	IP, ICMP, IGMP, BGP, OSPF
Кадры	**Канальный** MAC и LLC (физическая адресация)	Отвечает за доступ к среде передачи, исправление ошибок, надежную передачу данных. *На приеме* полученные с физического уровня данные упаковываются в кадры после чего проверяется их целостность. Если ошибок нет, то данные передаются на сетевой уровень. Если ошибки есть, то кадр отбрасывается и формируется запрос на повторную передачу. Канальный уровень подразделяется на два подуровня: **MAC (Media Access Control)** и **LLC (Locical Link Control)**. MAC регулирует доступ к разделяемой физической среде. LLC обеспечивает обслуживание сетевого уровня. На канальном уровне работают коммутаторы.	IEEE 802.3, IEEE 802.11, PPP, DHCP, ARP
Биты	**Физический** (кабель, сигналы, бинарная передача данных)	Определяет вид среды передачи данных, физические и электрические характеристики интерфейсов, вид сигнала. Этот уровень имеет дело с битами информации.	IEEE 802.11, ISDN

IP-адрес - Это идентификационный номер устройства в сети, который присваивается при подключении к Интернету.

Маска подсети – это битовая маска, позволяющая разделить IP-адрес на адрес подсети и адрес узла (хоста, компьютера, устройства) внутри этой подсети.

Префикс маски – это короткая запись сетевой маски, определяет количество бит порции сети.

IP адрес узла



Маска подсети и префикс

Маска подсети	32-битный адрес	Длина префикса
255.0.0.0	11111111.00000000.00000000.00000000	/8
255.255.0.0	11111111.11111111.00000000.00000000	/16
255.255.255.0	11111111.11111111.11111111.00000000	/24
255.255.255.128	11111111.11111111.11111111.10000000	/25
255.255.255.192	11111111.11111111.11111111.11000000	/26
255.255.255.224	11111111.11111111.11111111.11100000	/27
255.255.255.240	11111111.11111111.11111111.11110000	/28
255.255.255.248	11111111.11111111.11111111.11111000	/29
255.255.255.252	11111111.11111111.11111111.11111100	/30

Расчет адреса сети по адресу узла и маске

IP адрес узла (10):	192.	168.	0.	123	
IP адрес узла (2):	11000000.	10101000.	00000000.	01111011	
Маска подсети:	11111111.	11111111.	11111111.	00000000	^ (конъюнкция)
Адрес сети (2):	11000000.	10101000.	00000000.	00000000	
Адрес сети (10):	192.	168.	0.	0	
Min адрес(2):	11000000.	10101000.	00000000.	00000001	
Min адрес(10):	192.	168.	0.	1	
Max адрес(2):	11000000.	10101000.	00000000.	11111111	
Max адрес(10):	192.	168.	0.	255	

Расчет адреса сети по адресу узла и маске

IP адрес узла (10):	192.	168.	123.	123
IP адрес узла (2):	11000000.	10101000.	01111011.	01111011
Маска подсети:	11111111.	11111111.	11100000.	00000000
	———	———	———	———
Адрес сети (2):	11000000.	10101000.	01100000.	00000000
Адрес сети (10):	192.	168.	96.	0
Min адрес(2):	11000000.	10101000.	00000000.	00000001
Min адрес(10):	192.	168.	96.	1
Max адрес(2):	11000000.	10101000.	00000000.	11111111
Max адрес(10):	192.	168.	127.	255

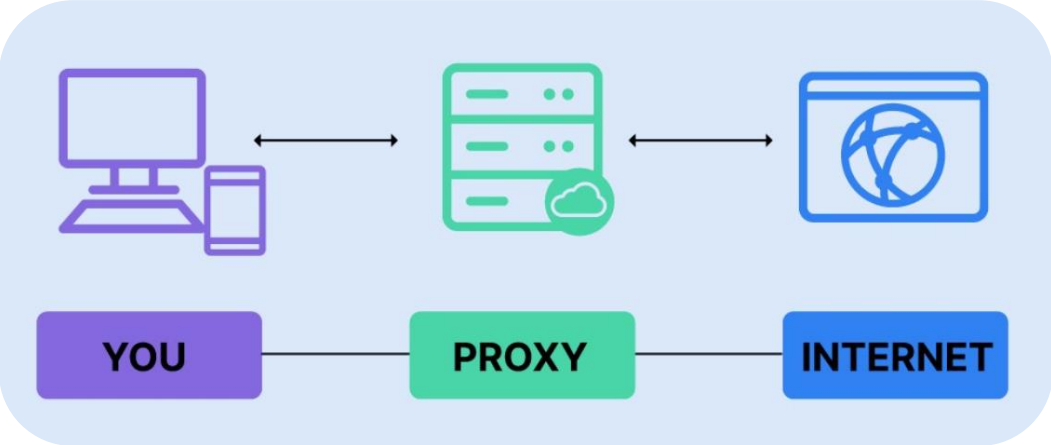
^
(конъюнкция)

Расчет маски сети по адресам узла и сети

IP адрес узла (10):	192.	168.	123.	123	
IP адрес узла (2):	11000000.	10101000.	01111011.	01111011	
Адрес сети (2):	11000000.	10101000.	01100000.	00000000	~ (эквивалентность)
Адрес сети (10):	192.	168.	96.	0	
Маска подсети:	11111111.	11111111.	11100000.	00000000	

Прокси-сервер – это дополнительный шлюз, участвующий в интернет-соединении.

Proxy используется как посредник между клиентом и сайтом, на который он хочет перейти. При подключении через proxy-server происходит замена IP-адреса, что позволяет ускорить интернет-соединение, обойти блокировку какого-либо ресурса и другое.



Зачем нужен прокси-сервер?

- отслеживать трафик
- увеличивать итоговую скорость загрузки за счет предварительного кэширования данных
- посещать сайты в режиме полного инкогнито за счет постоянной смены IP-адреса
- посещать территориально или регионально заблокированные ресурсы за счет перенаправления трафика через IP с местоположением, отличным от реального
- устанавливать запрет на посещение определенных сайтов по их IP-адресу.

Классификация прокси-серверов

Прозрачные

Их используют как дополнительные точки сети. При таком подключении от конечного сервера не скрывается IP клиента, а администратор ресурса может следить за соединением через встраиваемый шлюз.

Анонимные

Их используют, чтобы скрыть данные об изначальном пользователе. При таком подключении от конечного сервера не скрывается факт соединения через прокси, но в отличие от «прозрачного» варианта также и не раскрывается информация об изначальном пользователе.

Искажающие

Их применяют для подмены данных об изначальном пользователе. Такой вариант подключения позволяет получить доступ к веб-ресурсу, который территориально заблокирован для посещения, например, пользователям из конкретной страны.

Приватные

Их используют для полной защиты трафика.

Proxy vs. VPN

Обе технологии позволяют скрыть IP-адрес, защитить свои данные или получить доступ к территориально заблокированным сайтам. Однако в этом прокси выигрывает, поскольку его легче настроить: в сети можно найти бесплатные быстрые точки доступа в то время, когда скоростных VPN, которые распространялись бы на безвозмездной основе, практически не существует.

Главное отличие в том, что при соединении через прокси-сервер трафик только перенаправляется через него, а VPN полностью шифрует соединение и делает его анонимным. По этой причине прокси-сервер чаще используют для перераспределения кэшированных данных (например, для увеличения скорости соединения), а VPN – для обеспечения конфиденциальности подключения.

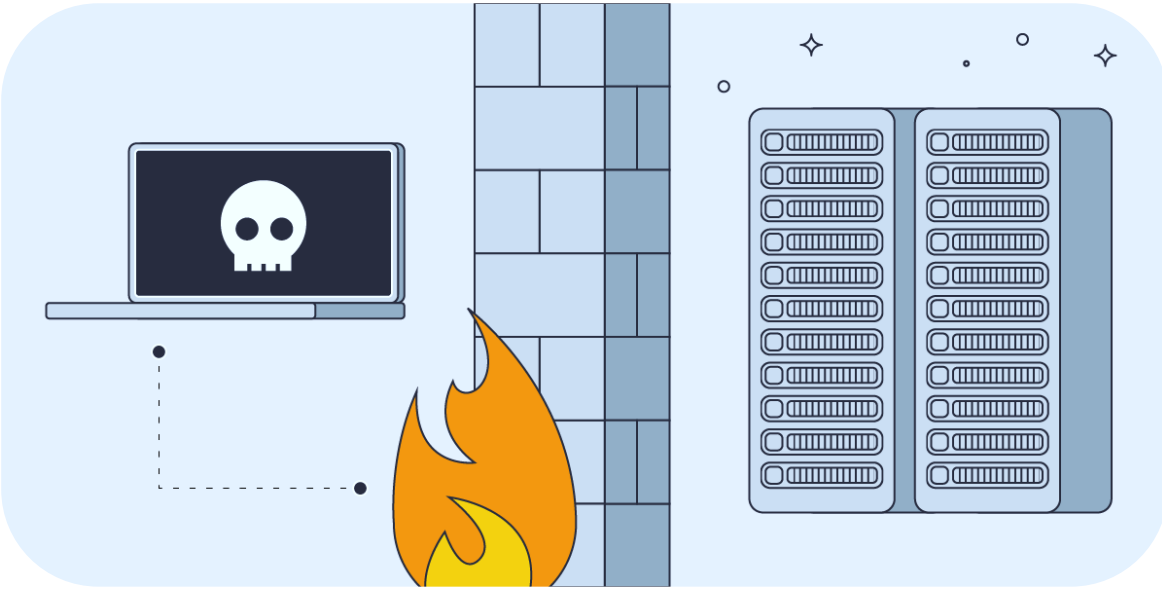
Межсетевой экран (файрвол, брандмауэр) — программный или программно-аппаратный элемент компьютерной сети, осуществляющий контроль и фильтрацию входящего, исходящего и внутрисетевого трафика в соответствии с заданными правилами.

Зачем нужен межсетевой экран?

- контроль доступа
- предотвращение атак
- защита от вредоносных программ
- управление доступом к ресурсам
- отчетность и мониторинг

Основные функции межсетевого экрана

- ✓ Проверка входящего и исходящего трафика
- ✓ Блокировка нежелательных соединений
- ✓ Применение правил доступа
- ✓ Контроль трафика
- ✓ Управление пропускной способностью
- ✓ Предотвращение атак
- ✓ Виртуальные частные сети (VPN)
- ✓ Прокси-серверы



Типы межсетевых экранов

Программный
Он устанавливается на компьютер как обычная программа, его легко настроить и установить на множество машин сразу.

Аппаратный
Это устройство, специально разработанное для сканирования трафика в сети.

Облачный
Может быть как программным, так и аппаратным. Компания-провайдер облака может предоставлять услуги защиты с помощью любого из этих способов.

Пассивный
Проверяет пакеты данных на основе правил, основанных на IP-адресах, портах, протоколах. Они просты в настройке и стоят недорого, но не могут защитить от атак, использующих легальные протоколы и порты.

Активный
Отслеживает состояния соединений и проверяют пакеты данных на соответствие этим состояниям. Они обеспечивают более надежную защиту, чем пассивные, но более сложные в настройке.

Межсетевые экраны vs Прокси-сервер

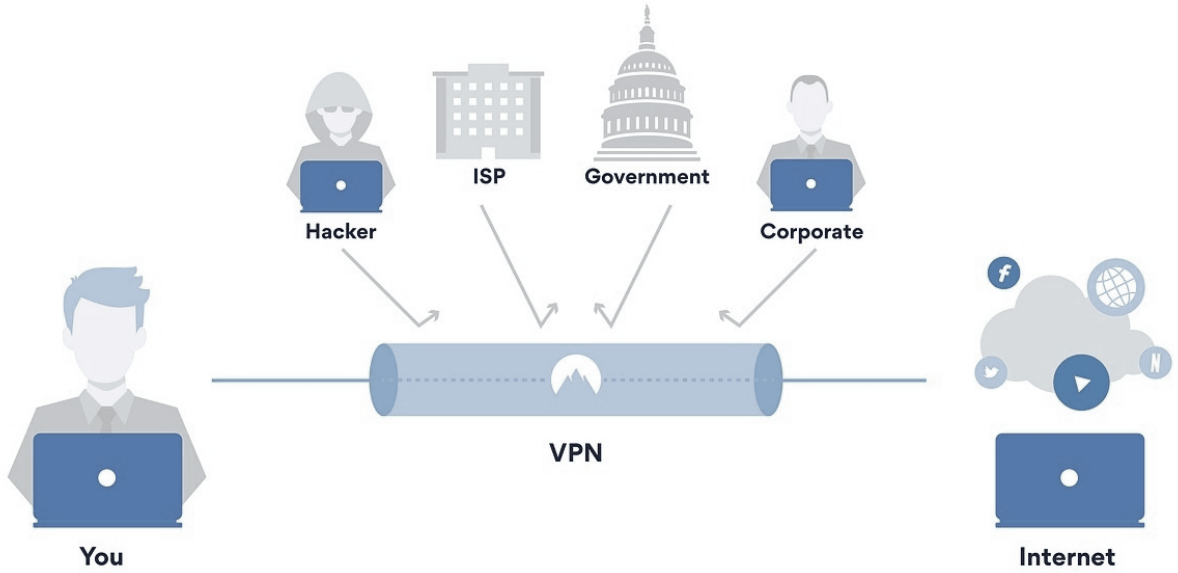
Основное сходство заключается в том, что прокси-серверы предназначены для управления сетевым трафиком и повышения анонимности.

Межсетевые экраны предназначены для защиты сетей от атак и несанкционированного доступа. Хотя прокси-серверы могут имитировать некоторые функции файрвол, они не обеспечивают такой же уровень защиты, как специализированные файрволы.

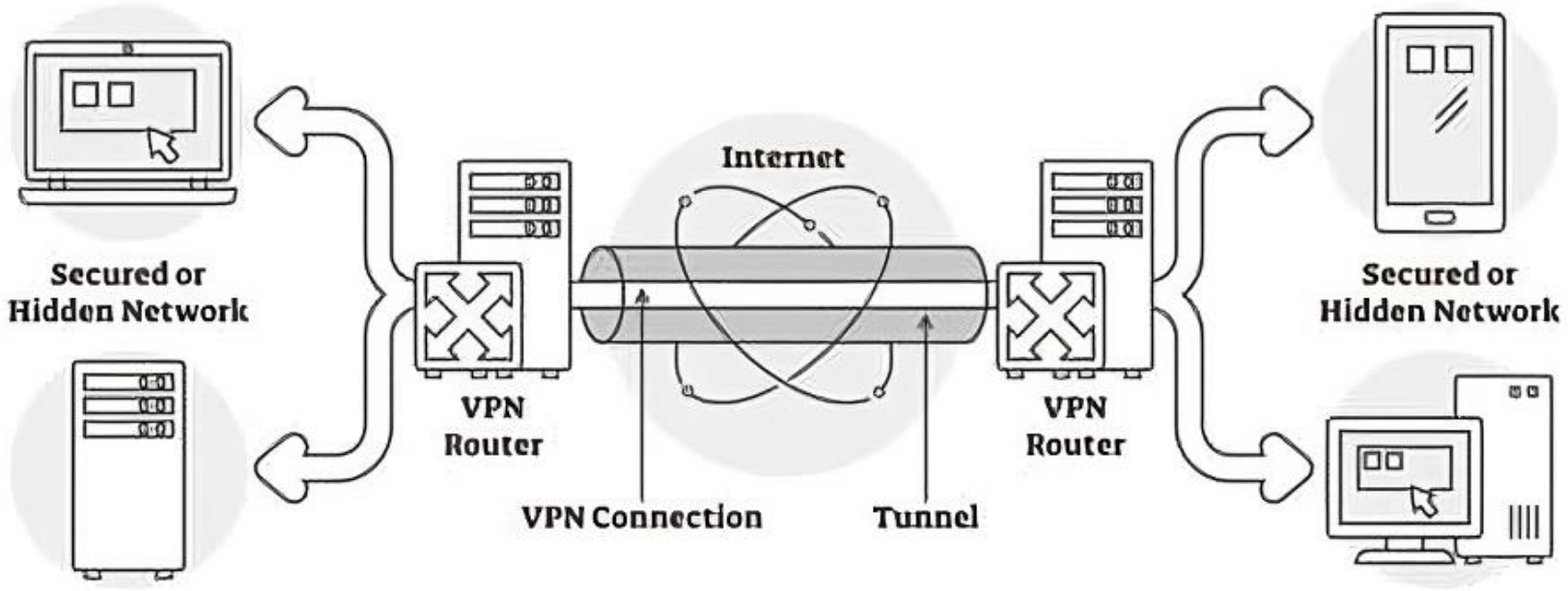
VPN (virtual private network — «виртуальная частная сеть») — обобщённое название технологий, позволяющих обеспечить одно или несколько сетевых соединений поверх чьей-либо другой сети.

Зачем нужен VPN?

- Удаленное подключение к сети
- Скрытие цепочки действий в интернете
- Защита данных при использовании интернета в общественных местах
- Избежание ограничения пропускной способности
- Экономия денег при совершении покупок в интернете



Как это работает?
Соединение маскирует IP-адрес, перенаправляя его через специально настроенный удаленный сервер, которым управляет отдельный провайдер. VPN действует как фильтр, превращая всю отправляемую и получаемую информацию в бессмыслицу. Даже если она попадёт в руки преступников, они не смогут ею воспользоваться.



Протоколы VPN

Протокол	Описание
OpenVPN	Открытый исходный код. Считается безопасным и совместим практически со всеми устройствами с поддержкой VPN.
WireGuard	Подойдет пользователям мобильных VPN. Не так хорош в обходе брандмауэров, как другие протоколы VPN.
IKEv2/IPsec	Протокол с закрытым исходным кодом, который подходит, если вы используете VPN на своем мобильном телефоне и регулярно переключаетесь между WiFi и, например, 3G/4G.
L2TP/IPsec	Более медленный протокол. Не рекомендуется выбирать его, если вы раскрываете личную информацию или используете VPN, которая публично делится своими ключами шифрования в интернете.
SSTP	Хорошо взаимодействует с брандмауэрами, но имеет закрытый исходный код и потенциально уязвим для атак.
PPTP	PPTP работает быстро, потому что не защищает ваши данные. Устаревший, небезопасный протокол, который рекомендуют избегать.

Плюсы и минусы VPN

Основные преимущества:

+ Возможность построения сети с узлами, которые могут находиться в разных точках мира
+ Маскировка IP-адреса, чтобы скрыть или изменить ваше местоположение от посещаемых веб-сайтов.
+ Шифрование веб-трафика для защиты данных при использовании незащищенного Wi-Fi.
+ Предотвращение мониторинга вашей интернет-активности от интернет-провайдера и других третьих лиц.

Основные недостатки:

- VPN не обеспечит полную анонимность.
- Безопасный VPN с высоким рейтингом стоит денег.
- Некачественный VPN может допустить утечку личной информации, например, раскрыть истинный IP-адрес или DNS-запросы.
- VPN почти всегда замедляет скорость интернета.
- Использование VPN на мобильных устройствах увеличивает трафик.
- Некоторые онлайн-сервисы пытаются запретить клиентам использовать VPN.