**Что такое VPN?**

***VPN*** (англ. *Virtual Private Network* — виртуальная частная сеть) — логическая сеть, создаваемая поверх другой сети, например Интернет. Несмотря на то, что коммуникации осуществляются по публичным сетям с использованием небезопасных протоколов, за счёт шифрования создаются закрытые от посторонних каналы обмена информацией. *VPN* позволяет объединить, например, несколько офисов организации в единую сеть с использованием для связи между ними неподконтрольных каналов.

Пользователи Microsoft Windows обозначают термином «*VPN*» одну из реализаций виртуальной сети — *PPTP*, причём используемую зачастую не для создания частных сетей. Чаще всего для создания виртуальной сети используется инкапсуляция протокола *PPP* в какой-нибудь другой протокол — *IP* (такой способ использует реализация *PPTP* —*Point-to-Point Tunneling Protocol*) или *Ethernet (PPPoE)* (хотя и они имеют различия).

Технология *VPN* в последнее время используется не только для создания собственно частных сетей, но и некоторыми провайдерами «последней мили» для предоставления выхода в Интернет.

При должном уровне реализации и использовании специального программного обеспечения сеть *VPN*может обеспечить высокий уровень шифрования передаваемой информации. При правильной настройке всех компонентов технология *VPN* обеспечивает анонимность в Сети.

**Структура *VPN***

*VPN* состоит из двух частей: «внутренняя» (подконтрольная) сеть, которых может быть несколько, и «внешняя» сеть, по которой проходит инкапсулированное соединение (обычно используется Интернет). Возможно также подключение к виртуальной сети отдельного компьютера. Подключение удалённого пользователя к *VPN*производится посредством сервера доступа, который подключён как к внутренней, так и к внешней (общедоступной) сети. При подключении удалённого пользователя (либо при установке соединения с другой защищённой сетью) сервер доступа требует прохождения процесса идентификации, а затем процесса аутентификации. После успешного прохождения обоих процессов, удалённый пользователь (удаленная сеть) наделяется полномочиями для работы в сети, то есть происходит процесс авторизации.

**Классификация *VPN***

Классифицировать *VPN* решения можно по нескольким основным параметрам:

**1. По типу используемой среды**
**Защищённые**

Наиболее распространённый вариант виртуальных частных сетей. C его помощью возможно создать надежную и защищенную подсеть на основе ненадёжной сети, как правило, Интернета. Примером защищённых *VPN* являются:*IPSec, OpenVPN* и *PPTP*.

**Доверительные**

Используются в случаях, когда передающую среду можно считать надёжной и необходимо решить лишь задачу создания виртуальной подсети в рамках большей сети. Вопросы обеспечения безопасности становятся неактуальными. Примерами подобных *VPN* решении являются:*Multi-protocol label switching (MPLS)* и *L2TP (Layer 2 Tunnelling Protocol)*. (точнее сказать, что эти протоколы перекладывают задачу обеспечения безопасности на другие, например *L2TP*, как правило, используется в паре с *IPSec*).

**2. По способу реализации**
**В виде специального программно-аппаратного обеспечения**

Реализация *VPN* сети осуществляется при помощи специального комплекса программно-аппаратных средств. Такая реализация обеспечивает высокую производительность и, как правило, высокую степень защищённости.
**В виде программного решения**

Используют персональный компьютер со специальным программным обеспечением, обеспечивающим функциональность *VPN*.
**Интегрированное решение**

Функциональность *VPN* обеспечивает комплекс, решающий также задачи фильтрации сетевого трафика, организации сетевого экрана и обеспечения качества обслуживания.

**3. По назначению**
***Intranet VPN***

Используют для объединения в единую защищённую сеть нескольких распределённых филиалов одной организации, обменивающихся данными по открытым каналам связи.
***Remote Access VPN***

Используют для создания защищённого канала между сегментом корпоративной сети (центральным офисом или филиалом) и одиночным пользователем, который, работая дома, подключается к корпоративным ресурсам с домашнего компьютера или, находясь в командировке, подключается к корпоративным ресурсам при помощи ноутбука.

***Extranet VPN***

Используют для сетей, к которым подключаются «внешние» пользователи (например, заказчики или клиенты). Уровень доверия к ним намного ниже, чем к сотрудникам компании, поэтому требуется обеспечение специальных «рубежей» защиты, предотвращающих или ограничивающих доступ последних к особо ценной, конфиденциальной информации.

**4. По типу протокола**

Существуют реализации виртуальных частных сетей под *TCP/IP, IPX* и *AppleTalk*. Но на сегодняшний день наблюдается тенденция к всеобщему переходу на протокол *TCP/IP*, и абсолютное большинство *VPN* решений поддерживает именно его.

**5. По уровню сетевого протокола**

По уровню сетевого протокола на основе сопоставления с уровнями эталонной сетевой модели *ISO/OSI*.

**Примеры *VPN****IPSec (IP security)* — часто используется поверх *IPv4*.
*PPTP (point-to-point tunneling protocol)* — разрабатывался совместными усилиями нескольких компаний, включая*Microsoft*.
*L2TP (Layer 2 Tunnelling Protocol)* — используется в продуктах компаний *Microsoft* и *Cisco*.
*L2TPv3 (Layer 2 Tunnelling Protocol version 3).*

**История**

Исторически, проблему организации надёжного канала для передачи данных решали при помощи прокладки прямого кабеля, физически защищённого от перехвата данных, например за счёт расположения его в труднодоступных местах или установки датчиков объёма, контролирующих доступ к нему. Но стоимость подобных решений была слишком высока даже для соединения близкорасположенных объектов, а в случае соединения объектов из разных частей страны или разных стран стоимость приближалась к астрономическим цифрам. Поэтому такие коммуникации могли себе позволить лишь военные организации и крупные корпорации.

С другой стороны, конец XX века был отмечен лавинообразным распространением Интернета: в геометрической прогрессии росли скорости доступа, охватывались все новые и новые территории, практически между любыми двумя точками в мире можно было установить быструю связь через Интернет. Но передача информации не была безопасной, злоумышленники могли перехватить, украсть, изменить её. В это время стала набирать популярность идея организации надёжного канала, который для связи будет использовать общедоступные коммуникации, но за счёт применения криптографических методов защитит передаваемые данные. Стоимость организации такого канала была во много раз меньше стоимости прокладки и поддержания выделенного физического канала, таким образом организация защищённого канала связи становилась доступной средним и малым предприятиям, и даже частным лицам.

На заре своего развития идея организации частных приватных сетей была чрезвычайно популярна, и многие серьёзные участники *IT* рынка и энтузиасты-любители пытались воплотить абстрактные идеи в реальный программный продукт. Серьёзные компании создали множество решений, обеспечивающих функциональность частных приватных сетей, как на программном, так и на аппаратном уровне. Свою реализацию *VPN* предлагало большинство известных *IT* компаний:

*Cisco — L2F (Layer 2 Forwarding), L2TP (Layer 2 Tunnelling Protocol), L2TPV3 (Layer 2 Tunnelling Protocol version 3)
Microsoft — PPTP (Point-To-Point Tunnelling Protocol)
Check Point Software Technologies — VPN-1
Redcreek Communications — Ravlin
Intel — Landrover VPN Express*

и многие другие….

Количество программных реализаций *VPN* от энтузиастов-любителей очень и очень велико. Большинство из них содержали в себе ряд серьёзных уязвимостей, зачастую в них был достаточно посредственно проработан вопрос шифрования — использовались достаточно слабые криптоалгоритмы, ни о какой многоплатформенности нельзя было и говорить. Но, несмотря на то, что большинство умирало на уровне альфа-бета версий, некоторые семена выросли в достаточно серьёзные решения, например, *OpenVPN*. Первые создаваемые реализации *VPN*обеспечивали лишь создание защищённого канала точка-точка между двумя серверами, по которому передавались все виды трафика. Со временем функциональность *VPN* расширялась, стали поддерживать более сложные, чем точка-точка, конфигурации сети: extranet *VPN*, *intranet VPN*, *remote access VPN* и *VPN* смешанных типов. Следствием этого явилось увеличение числа пользователей в виртуальных частных сетях, и на передний план вышли проблемы управления акаунтами, ассоциации с ними необходимых прав доступа, оперативное изменение прав в рамках всей создаваемой сети. Затем, в связи с увеличением числа пользователей стали повышаться требования к масштабируемости и расширяемости. Последние в свою очередь, сначала, включали требования поддержки различных протоколов и служб (*web, ftp, samba*, …), а со временем стали включать и требования поддержки разных операционных систем, платформ и даже различных дополнительных устройств, например мобильных телефонов и сетевых маршрутизаторов. Помимо постоянного увеличения числа пользователей изменился контент и объём передаваемых данных. Если на заре *VPN* по сетям в основном передавались текстовые данные, то на сегодняшний день эти сети часто используются для передачи медиа данных, на основе виртуальных частных сетей нередко устраивают видеоконференции и обеспечивают голосовую связь. Подобный «взрыв» объёмов трафика стал создавать огромные нагрузки на виртуальные частные сети, часто важная информация стала доходить со значительным запозданием из-за загрузки сетей. Это поставило перед разработчиками *VPN* решений новую проблему — проблему обеспечения качества обслуживания (*QoS*), которая на сегодняшний день наиболее актуальна.