УДК 004.716

VPN И ЕГО ПРИМЕНЕНИЕ

Д.Д. МОРОЗОВ
(Представлено: канд. физ.-мат. наук, доц. О.В. ГОЛУБЕВА)

В статье рассказывается, что такое виртуальная частная сеть и для чего она используется в различных сферах.

Ключевые слова: виртуальная частная сеть, VPN-сети, защита трафика.

VPN сейчас актуален, как никогда прежде. Даже в домашних роутерах стали появляться не просто VPN-серверы, а еще и с аппаратным ускорением шифрования. Что же такое VPN и для чего он вообще нужен?

Что такое VPN?

Аббревиатура VPN расшифровывается как Virtual Private Network, то есть виртуальная частная сеть. Что такое «сеть» — на примитивном уровне это объединение двух и более узлов каким-либо видом связи для того, чтобы они могли обмениваться информацией. Естественно, наиболее удобным способом и с поддержкой всех необходимых сервисов.

Что такое «частная» — не публичная, поэтому и частная. То есть такая, в которой только дозволенные узлы. Именно эта составляющая VPN и является самой главной, так как она определяет ряд требований к этой самой «частности».

Во-первых, надо как-то маркировать участников этой сети и ту информацию, которой они обмениваются, чтобы она не смешивалась с чужой. Во-вторых, определенно полезно эту информацию защитить от посторонних глаз. Ну хотя бы зашифровать, что снова накладывает следующий круг ограничений, связанных со стойкостью этого шифрования.

В-третьих, надо сохранять целостность такого способа передачи информации — не пускать посторонних в частную сеть, проверять источник передаваемых сообщений и следить за тем, чтобы информация нигде не просачивалась в «голом виде».

Понятие «виртуальная» значит, что такая сеть абстрагирована от физической составляющей — ей не важно, по каким и скольким каналам связи она проложена, так как для участников этой сети она работает прозрачно. Или же, с другой стороны, физическая сеть чаще всего просто не принадлежит пользователю виртуальной.

Например, в серьезных организациях сотрудников при подсоединении рабочего ноутбука к любым проводным или беспроводным сетям, находящимся за пределами стен этой самой организации, обязуют сразу же задействовать VPN-подключение до офисной сети. При этом не важно, через какие именно сети будет установлено это соединение, но можно не сомневаться, что пойдет оно по публичным, чужим сетям связи. Такое соединение принято называть туннелем, впоследствии этот термин нам встретится еще не раз.

Для чего нужен VPN?

Приведенный выше пример подключения удаленного пользователя к корпоративной сети — один из наиболее типичных сценариев использования VPN. Злоумышленник не сможет просто так узнать, чем конкретно занят этот пользователь, какие данные он передает и получает. Более того, в компаниях, озабоченных собственной безопасностью, на всех используемых работниками устройствах принудительно включается обязательное использование VPN-подключений где бы то ни было. Даже использование Интернета в таком случае идет сквозь корпоративную сеть и под строгим надзором службы безопасности.

Второй по распространенности вариант использования схож с первым, только подключаются к корпоративной сети не отдельные пользователи, а целые офисы или здания. Цель та же — надежно и безопасно объединить географически удаленные элементы одной организации в единую сеть.

Это могут быть как крупные представительства корпораций в разных странах или даже просто камеры, сигнализации и прочие охранные системы. При такой простоте создания VPN виртуальные частные сети могут создавать и внутри компаний для объединения и изоляции тех или иных отделов или систем.

Не менее часто организовываются VPN-сети и между серверами или целыми вычислительными кластерами для поддержания их доступности и дублирования данных. Частота их использования напрямую связана с ростом популярности облачных технологий. Причем все вышеперечисленное — это не какие-то временные решения: такие подключения могут поддерживаться (и поддерживаются) годами.

У России свой путь применения VPN на практике. Когда-то крупные ISP строили свои сети на основе простых неуправляемых коммутаторов — очевидно, в целях экономии. Для разделения трафика клиентов стали использовать различные варианты VPN-подключений к серверу провайдера, через который и выдавали доступ в Интернет.

Такой метод используется до сих пор, а производители домашних роутеров для российского региона все еще вынуждены добавлять поддержку таких подключений в прошивку своих устройств. Так что, в каком-то смысле, Россия была лидером по числу одновременных VPN-подключений среди пользователей Сети.

Контрпример таких постоянных VPN-соединений — это сессионные подключения. Они нередко используются при предоставлении клиентского доступа к различным сервисам, которые, как правило, связаны с обработкой очень чувствительной информации в области финансов, здравоохранения, юриспруденции.

Впрочем, для обычного пользователя гораздо важнее другой вариант практического использования VPN. В советах по безопасности Android и iOS настоятельно рекомендуется применять защищенное VPN-соединение до надежного узла (будь то домашний роутер или специальный VPN-провайдер) при подключении к любым публичным сетям, чтобы защитить свой трафик от возможного вмешательства злоумышленников.

Наконец, последний вариант применения VPN в частном порядке — это обход разнообразных сетевых ограничений. Например, для получения доступа к ресурсам, которые заблокированы или не предоставляют свои услуги на определенной территории. Согласно отчету GlobalWebIndex, только в 2014 году для доступа к социальным сетям VPN использовали около 166 млн. человек.

ЛИТЕРАТУРА

1. A Framework for IP Based Virtual Private Networks [Электронный документ] / B. Gleeson, A. Lin, J. Heinanen. — http://www.ietf.org/rfc/rfc2764.txt.
2. VPN и IPSec на пальцах [Электронный документ] / Dru Lavigne. — http://www.nestor.minsk.by/sr/2005/03/050315.html.
3. Сергей Петренко Защищённая виртуальная частная сеть: современный взгляд на защиту конфиденциальных данных // Мир Internet. – 2001. – № 2.
4. Маркус Файльнер Виртуальные частные сети нового поколения // LAN. – 2005. – № 11.