Министерство образования Российской Федерации

НГТУ

Кафедра программных систем и баз данных

РЕФЕРАТ
на тему: “Технология виртуальных частных сетей VPN ”

Новосибирск 2002

Введение.

За последние несколько десятилетий количество накопленных человечеством знаний, и без того внушительное, достигло совершенно неимоверных размеров. Этот, казалось бы, замечательный факт поначалу породил большие проблемы, а затем науку информатику и различные способы, методы и технические приспособления для работы с информацией. Безусловно, самым значительным и приведшим к поистине революционным изменениям в мире явилось «такое техническое приспособление», как компьютер. В связи со стремительным развитием сетевых технологий в последние годы, компьютер, и так задействованный во многих отраслях человеческой деятельности, взял на себя также большую часть функций по коммуникации, связи, передачи самой различной информации во всевозможные точки планеты. Огромную роль в жизни человечества играет такое явление, как Всемирная Сеть Интернет, широко распространены на сегодняшний день и локальные сети различных конфигураций. В контексте темы данного реферата следует сказать, что значительная доля передаваемой по сетям информации носит служебный характер и используется сотрудниками различных организаций, корпораций и т.д. Разумеется, очень остро стоит вопрос о защите такого рода информации как от «случайных искажений», так и от преднамеренного искажения или несанкционированного копирования, да и просто ознакомления. Рассматриваемая в данном реферате технология виртуальных частных сетей VPN направлена как раз на защиту от подобных воздействий.

Что такое VPN.

Технологию VPN можно определить, как "комплекс мероприятий по передаче данных из одной точки сети в другую безопасным образом". Это, на первый взгляд, достаточно расплывчатое определение, охватывает все возможные технологии построения VPN.

Суть VPN состоит в следующем:

- На все компьютеры, имеющие выход в Интернет, устанавливается средство, реализующее VPN (VPN-агент, программное, или программно-аппаратное средство).
- VPN-агенты автоматически шифруют всю исходящую информацию (и соответственно, расшифровывают всю входящую). Они также следят за ее целостностью с помощью ЭЦП или «имитоприставок» (криптографическая контрольная сумма, рассчитанная с использованием ключа шифрования).

Поскольку информация, циркулирующая в Интернете, представляет собой множество пакетов протокола IP, VPN-агенты работают именно с ними.

Перед отправкой IP-пакета VPN-агент действует следующим образом:

- Определяет и добавляет в пакет ЭЦП отправителя или имитоприставку.
- Шифрует пакет (целиком, включая заголовок).
- Проводит инкапсуляцию, т.е. формирует новый заголовок, где указывается адрес вовсе не получателя, а его VPN-агента. Эта полезная дополнительная функция позволяет представить обмен между двумя сетями как обмен между двумя компьютерами. Полезная для целей предполагаемого злоумышленника информация, например, внутренние IP-адреса, ему уже недоступна.

При получении IP-пакета выполняются обратные действия:

- Заголовок содержит сведения о VPN-агенте отправителя. Если таковой не входит в список разрешенных в настройках, то информация просто отбрасывается. То же самое происходит при приеме пакета с намеренно или случайно поврежденным заголовком.
- Согласно настройкам выбираются алгоритмы шифрования и ЭЦП, а также необходимые криптографические ключи.
- Пакет расшифровывается, затем проверяется его целостность. Если ЭЦП неверна, то он выбрасывается.
- И, наконец, пакет в его исходном виде отправляется настоящему адресату по внутренней сети.

Все операции выполняются автоматически. Сложной в технологии VPN является только настройка VPN-агентов, которая, впрочем, вполне по силам опытному пользователю (хотя это зависит и от конкретной реализации VPN-системы).

VPN-агент может находиться непосредственно на защищаемом ПК, что полезно для мобильных пользователей, подключающихся к Интеренту где попало. В этом случае он обезопасит обмен данными только того компьютера, на котором установлен.

Возможно совмещение VPN-агента с маршрутизатором IP-пакетов. Ведущие мировые производители в последнее время выпускают маршрутизаторы со встроенной поддержкой VPN, например Express VPN от Intel.

Как видно из описания, VPN-агенты создают каналы в Интернет между защищаемыми сетями, которые обычно называют «туннелями». Циркулирующая в них информация спрятана от посторонних.

Кроме того, все пакеты «фильтруются» в соответствии с настройками. Таким образом, все действия VPN-агентов можно свести к двум механизмам: созданию туннелей и фильтрации проходящих пакетов.

Зачем использовать именно VPN.

Итак, VPN обеспечивает надежную защиту трафика. Важно, что VPN делает это совершенно прозрачно для всех приложений, не вмешиваясь в их работу.

VPN можно воспринимать как:

- защиту трафика, основанную на криптографии;
- средство коммуникации; возможность получить защищенный доступ к вашим внутренним ресурсам из любой точки мира;
- средство влияния на стратегию развития коммуникационных систем фирмы: вместо расходования огромных средств на строительство собственных выделенных линий возможно получить надежно защищенные каналы связи от коммуникационных провайдеров.

При правильном выборе VPN:

- компания получает защищенные собственные каналы и защищенный трафик отдельных приложений по цене доступа в Интернет, что на несколько порядков дешевле владения собственными линиями;
- при установке VPN не требуется изменять топологию сетей, переписывать приложения, обучать пользователей, т.е. тратить дополнительные ресурсы;
- обеспечивается масштабируемость: VPN не создаст проблем роста, что сохранит инвестиции в инфраструктуру безопасности.

Заключение

На сегодняшний день в мире информация играет такую же важную роль, как воздух, которым мы дышим. Мир не мыслит себя без Интернета и повсеместно развитых коммуникационных сетей (телефонных, телеграфных, теле-, радио-, мобильной связи). Наиболее требовательными к качеству связи в принципе, и в частности к ее защищенности, являются, пожалуй, различные коммерческие структуры, фирмы, корпорации.

Технология VPN появилась на свет как объективный результат наличия потребности в защищенной и удобной связи между локальными информационными центрами (локальными сетями), либо удаленного доступа тех же характеристик к подобным центрам. Эта технология предоставляет достаточно удобное и функциональное средство для решения описанных задач коммуникации. Причем, что немаловажно, реализация VPN значительно дешевле, чем реализация пожалуй единственной достойной альтернативы – построения системы собственных выделенных линий связи. Это достигается тем, что VPN эффективно использует широко развитую систему предоставления услуг доступа в Интернет, распространенную буквально во всем мире.

Вполне естественно, что основными потребителями VPN видимо станут средние и крупные коммерческие организации и фирмы, которые, активно развиваясь, будут нуждаться в эффективном решении задач коммуникации между своими филиалами, офисами, а также задач удаленного доступа к своим локальным сетям собственных сотрудников.

Безусловно, никакая технология, и VPN в том числе, не обеспечит идеальной защиты информации. В конце концов, кроме атак на криптографические алгоритмы, ключи, операционные системы и т.д. существуют еще и так называемые атаки на пользователей. Не стоит забывать, что с VPN работают люди, и человеческий фактор в системе безопасности также важен. Так пользователь может потерять дискету с секретными ключами, или записать свой пароль на бумаге, и оставить ее на своем рабочем столе, или даже просто выбрать для пароля легко угадываемое осмысленное слово/фразу.

Подводя итог, можно сказать, что VPN на сегодняшний день – самое выгодное по соотношению цена/качество средство защищенного обмена информацией между двумя сетями или сетью и удаленным пользователем.

Список литературы

1. Виртуальные частные сети и другие способы защиты информации.//Мир ПК. – 2002. - №4. – с. 92
2. VPN – Старые песни о главном.//КомпьютерПресс. – 2001. - №5. (статья взята с сайта http://www.infosec.ru)
3. Виртуальные частные сети.//PC Magazine.– 2000. - №6. (статья взята с сайта http://www.pcmag.ru)
4. http://www.infosec.ru - статья «Атаки на VPN». – 2002
5. http://www.crnep.ru