23.03.20г.

Дисциплина: Организация, принципы построения и функционирования компьютерных сетей

Тема: Сети VPN

Технология виртуальных частных сетей (VPN - Virtual Private Network) является одним из эффективных механизмов обеспечения информационной безопасности при передаче данных в распределенных вычислительных сетях.

Виртуальные частные сети являются комбинацией нескольких самостоятельных сервисов (механизмов) безопасности:

· шифрования (с использование инфраструктуры криптосистем) на выделенных шлюзах (шлюз обеспечивает обмен данными между вычислительными сетями, функционирующими по разным протоколам);

· экранирования (с использованием межсетевых экранов);

· туннелирования.

Сущность технологии VPN заключается в следующем (рис. 11):

· На все компьютеры, имеющие выход в Интернет (вместо Интернета может быть и любая другая сеть общего пользования), устанавливается VPN-агенты, которые обрабатывают IP-пакеты, передаваемые по вычислительным сетям.

· Перед отправкой IP-пакета VPN-агент выполняет следующие операции:

· анализируется IP-адрес получателя пакета, в зависимости от этого адреса выбирается алгоритм защиты данного пакета (VPN-агенты могут, поддерживать одновременно несколько алгоритмов шифрования и контроля целостности). Пакет может и вовсе быть отброшен, если в настройках VPN-агента такой получатель не значится;

· вычисляется и добавляется в пакет его имитоприставка, обеспечивающая контроль целостности передаваемых данных;

· пакет шифруется (целиком, включая заголовок IP-пакета, содержащий служебную информацию);

· формируется новый заголовок пакета, где вместо адреса получателя указывается адрес его VPN-агента (эта процедура называется инкапсуляцией пакета).

В результате этого обмен данными между двумя локальными сетями снаружи представляется как обмен между двумя компьютерами, на которых установлены VPN-агенты. Всякая полезная для внешней атаки информация, например, внутренние IP-адреса сети, в этом случае недоступна.

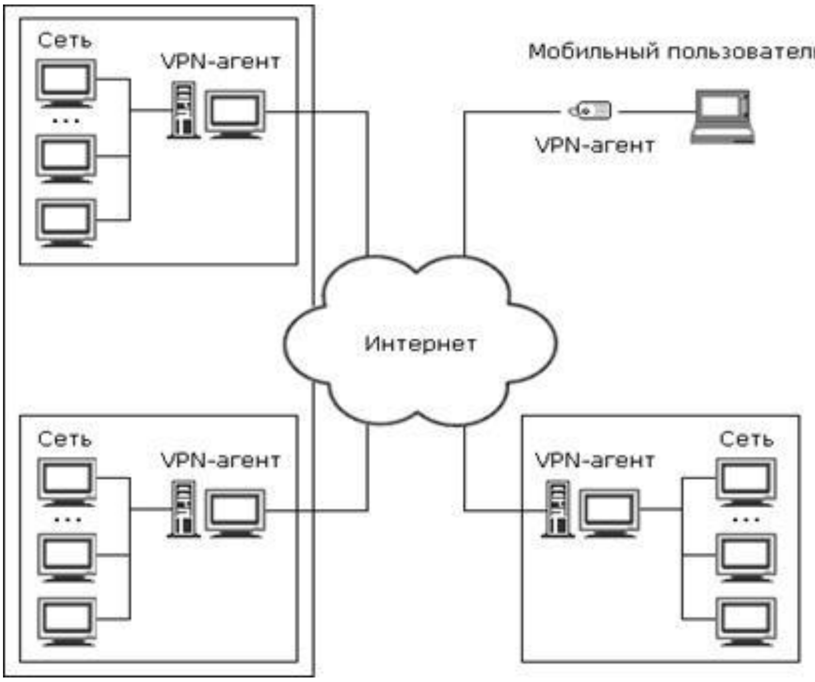

Рисунок 1.1.- Схема технологии VPN

· При получении IP-пакета выполняются обратные действия:

· из заголовка пакета извлекается информация о VPN-агенте отправителя пакета, если такой отправитель не входит в число разрешенных, то пакет отбрасывается (то же самое происходит при приеме пакета с намеренно или случайно поврежденным заголовком);

· согласно настройкам выбираются криптографические алгоритмы и ключи, после чего пакет расшифровывается и проверяется его целостность (пакеты с нарушенной целостностью также отбрасываются);

· после всех обратных преобразований пакет в его исходном виде отправляется настоящему адресату по локальной сети.

Все перечисленные операции выполняются автоматически, работа VPN-агентов является незаметной для пользователей. Сложной является только настройка VPN-агентов, которая может быть выполнена только очень опытным пользователем. VPN-агент может находиться непосредственно на защищаемом компьютере (что особенно полезно для мобильных пользователей). В этом случае он защищает обмен данными только одного компьютера, на котором он установлен.

Понятие "туннеля" при передаче данных в сетях

Для передачи данных VPN-агенты создают виртуальные каналы между защищаемыми локальными сетями или компьютерами (такой канал называется "туннелем", а технология его создания называется "туннелированием"). Вся информация передается по туннелю в зашифрованном виде.

Рисунок 1.2. – Организация туннеля в VPN.

Одной из обязательных функций VPN-агентов является фильтрация пакетов. Фильтрация пакетов реализуется в соответствии с настройками VPN-агента, совокупность которых образует политику безопасности виртуальной частной сети. Для повышения защищенности виртуальных частных сетей на концах туннелей целесообразно располагать межсетевые экраны.

Выводы по теме

· Виртуальные частные сети являются комбинацией нескольких самостоятельных сервисов (механизмов) безопасности:

· шифрования (с использование инфраструктуры криптосистем);

· экранирования (с использованием межсетевых экранов);

· туннелирования.

· При реализации технологии виртуальных частных сетей на все компьютеры, имеющие выход в Интернет (вместо Интернета может быть и любая другая сеть общего пользования), устанавливаются VPN-агенты, которые обрабатывают IP-пакеты, передаваемые по вычислительным сетям.

· В виртуальной частной сети обмен данными между двумя локальными сетями снаружи представляется как обмен между двумя компьютерами, на которых установлены VPN-агенты. Всякая полезная для внешней атаки информация, например, внутренние IP-адреса сети, в этом случае недоступна.

· Для передачи данных VPN-агенты создают виртуальные каналы между защищаемыми локальными сетями или компьютерами (такой канал называется "туннелем", а технология его создания называется "туннелированием").

· Одной из обязательных функций VPN-агентов является фильтрация пакетов.

· Фильтрация пакетов реализуется в соответствии с настройками VPN-агента, совокупность которых образует политику безопасности виртуальной частной сети.

· Для повышения защищенности виртуальных частных сетей на концах туннелей целесообразно располагать межсетевые экраны.