24.03.20

Дисциплина: Организация, принципы построения и функционирования компьютерных сетей

Тема: Основы сетей VPN

При подключении корпоративной локальной сети к открытой сети возникают угрозы безопасности двух основных типов:

• НСД к внутренним ресурсам корпоративной локальной сети, получаемый злоумышленником в результате несанкционированного входа в эту сеть;

• НСД к корпоративным данным в процессе их передачи по открытой сети.

Обеспечение безопасности информационного взаимодействия локальных сетей и отдельных компьютеров через открытые сети, в частности через сеть Интернет, возможно путем эффективного решения следующих задач:

• защита подключенных к открытым каналам связи локальных сетей и отдельных компьютеров от несанкционированных действий со стороны внешней среды;

• защита информации в процессе ее передачи по открытым каналам связи.

Как уже отмечалось выше, для защиты локальных сетей и отдельных компьютеров от несанкционированных действий со стороны внешней среды обычно используют МЭ, поддерживающие безопасность информационного взаимодействия путем фильтрации двустороннего потока сообщений, а также выполнения функций посредничества при обмене информацией. МЭ располагают на стыке между локальной и открытой сетью. Для защиты отдельного удаленного компьютера, подключенного к открытой сети, на этом компьютере устанавливают ПО сетевого экрана, и такой сетевой экран называется персональным.

Защита информации в процессе ее передачи по открытым каналам основана на использовании виртуальных защищенных сетей VPN. Виртуальной защищенной сетью VPN (Virtual Private Network) называют объединение локальных сетей и отдельных компьютеров через открытую внешнюю среду передачи информации в единую виртуальную корпоративную сеть, обеспечивающую безопасность циркулирующих данных. Виртуальная защищенная сетьVPN формируется путем построения виртуальных защищенных каналов связи, создаваемых на базе открытых каналов связи общедоступной сети. Эти виртуальные защищенные каналы связи называются туннелями VPN. Сеть VPN позволяет с помощью туннелей VPN соединить центральный офис, офисы филиалов, офисы бизнес-партнеров и удаленных пользователей и безопасно передавать информацию через Интернет.

Туннель VPN представляет собой соединение, проведенное через открытую сеть, по которому передаются криптографически защищенные пакеты сообщений виртуальной сети. Защита информации в процессе ее передачи по туннелю VPN основана:

- на аутентификации взаимодействующих сторон;
- криптографическом закрытии (шифровании) передаваемых данных;
- проверке подлинности и целостности доставляемой информации.

Для этих функций характерна взаимосвязь друг с другом. При их реализации используются криптографические методы защиты информации. Эффективность такой защиты обеспечивается за счет совместного использования симметричных и асимметричных криптографических систем. ТуннельVPN, формируемый устройствами VPN, обладает свойствами защищенной выделенной линии, которая развертывается в рамках общедоступной сети, например Интернета. Устройства VPN могут играть в виртуальных частных сетях роль VPN-клиента, VPN-сервера или шлюза безопасности VPN.

VPN-клиент представляет собой программный или программно-аппаратный комплекс, выполняемый обычно на базе персонального компьютера. Его сетевое ПО модифицируется для выполнения шифрования и аутентификации трафика, которым это устройство обменивается с другими VPN-клиентами,VPN-серверами или шлюзами безопасности VPN. Обычно реализация VPN-клиента представляет собой программное решение, дополняющее стандартную ОС — Windows NT/2000/XP или Unix.

VPN-сервер представляет собой программный или программно-аппаратный комплекс, устанавливаемый на компьютере, выполняющем функции сервера.VPN-сервер обеспечивает защиту серверов от НСД из внешних сетей, а также организацию защищенных соединений (ассоциаций) с отдельными компьютерами и с компьютерами из сегментов локальных сетей, защищенных соответствующими VPN-продуктами. VPN-сервер является функциональным аналогом продукта VPN-клиент для серверных платформ. Он отличается прежде всего расширенными ресурсами для поддержания множественных соединений с VPN-клиентами. VPN-сервер может поддерживать защищенные соединения с мобильными пользователями.

Шлюз безопасности VPN (security gateway) — это сетевое устройство, подключаемое к двум сетям и выполняющее функции шифрования и аутентификации для многочисленных хостов, расположенных за ним. Размещен шлюз безопасности VPN так, чтобы через него проходил весь трафик, предназначенный для внутренней корпоративной сети. Сетевое соединение шлюза VPN прозрачно для пользователей позади шлюза, и представляется им выделенной линией, хотя на самом деле прокладывается

через открытую сеть с коммутацией пакетов. Адрес шлюза безопасности VPN указывается как внешний адрес входящего тунне-лируемого пакета, а внутренний адрес пакета является адресом конкретного хоста позади шлюза. Шлюз безопасности VPNможет быть реализован в виде отдельного программного решения, отдельного аппаратного устройства, а также в виде маршрутизатора или МЭ, дополненных функциями VPN.

Открытая внешняя среда передачи информации включает как каналы скоростной передачи данных, в качестве которой используется сеть Интернет, так и более медленные общедоступные каналы связи, в качестве которых обычно применяются каналы телефонной сети. Эффективность виртуальной частной сети VPN определяется степенью защищенности информации, циркулирующей по открытым каналам связи. Для безопасной передачи данных через открытые сети широко используют инкапсуляцию и туннелирование. С помощью методики туннелиро-вания пакеты данных передаются через общедоступную сеть, как по обычному двухточечному соединению. Между каждой парой «отправитель — получатель данных» устанавливается своеобразный туннель — логическое соединение, позволяющее инкапсулировать данные одного протокола в пакеты другого.

Суть туннелирования состоит в том, чтобы инкапсулировать, т. е. «упаковать», передаваемую порцию данных, вместе со служебными полями, в новый «конверт». При этом пакет протокола более низкого уровня помещается в поле данных пакета протокола более высокого или такого же уровня. Следует отметить, что туннелирование само по себе не защищает данные от НСД или искажения, но благодаря туннелированию появляется возможность полной криптографической защиты инкапсулируемых исходных пакетов. Чтобы обеспечить конфиденциальность передаваемых данных, отправитель шифрует исходные пакеты, упаковывает их во внешний пакет с новым IP-заголовком и отправляет по транзитной сети.