План:

1. Как подключить сеть к интернету

1.1) Два метода подключения

1.2) Учёт трафика

1.3) Безопасность подключения к Интернету

1. Организация доступа в интернет через мобильные сети
2. Какой провайдер выбрать (см. таблицу)

**Как подключить корпоративную сеть к интернету**

В наше время всем предприятиям требуется доступ в интернет. За работу канала доступа обычно отвечает Интернет-провайдер, но и системному администратору компьютерной сети предприятия, даже небольшого, нужно решать ряд организационных и технологических задач.

Существует два основных метода предоставления пользователям корпоративной сети доступа к Web- и ftp- сервисам: посредством маршрутизации (трансляции) или через прокси-сервер.

В первом случае доступ предоставляется по IP-адресу компьютера, на котором работает сотрудник. Такую схему можно полностью реализовать на базе программного решения - шлюза и брандмауэра. Кроме того, существуют комплексные специализированные аппаратно-программные шлюзы. Для терминальных рабочих мест организация доступа по IP-адресам технически невозможна, так как все они используют один IP-адрес терминального сервера. Для сопряжения рабочих станций пользователей с каналом Интернета используется шлюз в виде х86-сервера с установленными на нем операционной системой, программой, обеспечивающей трансляцию внутренних IP-адресов в реальный IP-адрес сервера и обратно, включенной маршрутизацией и двумя сетевыми интерфейсами: один из них "смотрит" в сторону локальной сети, другой подключен к провайдеру. На каждой клиентской машине в свойствах протокола TCP/IP сетевой карты необходимо прописать IP-адрес шлюза.

Во втором случае происходит авторизация пользователя по имени доступа (login) и паролю, выделенному сотруднику. Этот вариант, в частности, можно реализовать при помощи прокси-сервера и системы аутентификаци. Рассмотрим типовую схему, где прокси сервер установлен на шлюзе сети: сервер "смотрит" одним интерфейсом в локальную сеть, а другим подключен к Интернет-каналу. При такой установке прокси сервера для работы в Интернете (по HTTP, FTP и DNS) на машинах в локальной сети не требуется маршрутизации, поскольку все запросы к ресурсам Интернета прокси сервер отправляет "от себя" - с IP-адресом внешнего интерфейса шлюза. Службу DNS на компьютерах клиентов можно отключить, поскольку сам прокси сервер обращается к DNS. Как правило, в корпоративной сети используется электронная почта, и для ее работы маршрутизация на шлюзе все равно понадобится, но для Web-почты, работающей по протоколу HTTP, достаточно прокси-сервера.

Скачанные из Интернета данные прокси сервер передает пользователю и сохраняет в своем кэше. При повторном запросе эти данные извлекаются уже из кэша (если, конечно, Web-страница допускает кэширование), что происходит гораздо быстрее и не занимает к тому же канал доступа. Кроме более эффективного использования пропускной способности канала, получается экономия и на объеме трафика . Данные в кэше могут обновляться в зависимости от настройки самого прокси-сервера. При нажатии кнопки "Обновить" на панели управления браузера прокси-сервер принудительно копирует данные с Web-сервера, даже если они есть у него в кэше и не устарели (а заодно и обновляет их в кэше). Но некоторые страницы на Web-сайтах специально помечаются как некэшируемые, например, для целей повышенной актуальности. Кроме собственно доступа, системному администратору необходимо еще решить проблемы авторизации доступа, учета трафика и времени работы пользователей в Интернете, обеспечения безопасности локальной сети предприятия. Необходимо также определить правила распределения пропускной способности Интернет-канала между пользователями сети и правила доступа к ресурсам Интернета; возможно, потребуется установить и другие ограничения для пользователей. Все эти процедуры, в зависимости от принятого типа доступа (по IP-адресу или через прокси-сервер), имеют свои особенности.

**Учёт трафика**

Учет трафика по IP-адресам рабочих станций ведется средствами программного брандмауэра, встроенного в операционную систему. Для достоверного учета трафика по пользователям при такой схеме доступа сотрудники должны выходить в Интернет только с закрепленных за ними рабочих мест, что, естественно, ограничивает гибкость и мобильность их работы.

При использовании прокси-сервера учет трафика ведется по протоколу HTTP, и объем таких данных меньше, чем величина IP-трафика. Но при аутентификации по пользователям прокси сервер заносит все данные о запросах (DNS-адреса сайтов, время получения запроса, объем скачанных файлов, источник - кэш прокси сервера или Интернет) в журнал по каждому пользователю, вне зависимости от IP-адреса клиентской машины.

**Безопасность подключения к Интернету**

Подключение физического канала Интернет напрямую в корпоративную сеть равносильно вынесению рабочих мест своего предприятия на людную площадь. Как правило, информация, циркулирующая в локальной сети, критически важна для деятельности предприятия, и вредоносное воздействие вирусов (например, почтовых), атака извне или утечка данных изнутри могут полностью нарушить его работу.  
  
Вредоносное воздействие вирусов трудно недооценить, но решение этой проблемы на 90% зависит от осведомленности пользователей - не запустит ли кто вложенный в письмо вирус. Вирусные атаки можно блокировать и отражать антивирусными программами на почтовых серверах (Dr.Web, "Антивирус Касперского" и т. д.) и на компьютерах пользователей (Norton Antivirus, Comodo Internet Security, соответствующие продукты "Лаборатории Касперского" и т. д.). Главное при этом - своевременное обновление антивирусных баз.  
  
Атаки извне, в зависимости от того, как организовано подключение, блокируются грамотной настройкой шлюза, применением прокси-сервера на шлюзе без NAT и маршрутизации, а также вынесением прокси-сервера, почтового и Web-сервера в "демилитаризованную зону" (DMZ, подсеть корпоративной сети, доступная из Интернета).  
  
Утечки корпоративных данных имеют в основном организационную природу и составляют самую сложную проблему для службы безопасности предприятия. Существуют технические решения, минимизирующие возможность этого: в частности, закрытие всех TCP/UDP-портов на интерфейсе шлюза, "смотрящем" в локальную сеть (остается только порт прокси-сервера). Должна быть отключена маршрутизация и преобразование адресов (NAT) между Интернетом и внутренними ("серыми") IP-адресами сети предприятия.  
  
Перечисленные меры используются, когда прокси-сервер установлен на шлюзе, но более защищенной считается система с прокси-сервером, вынесенным в DMZ.  
  
Наиболее полную защиту обеспечивает физическое разделение локальной корпоративной сети и Интернета. В этом случае на предприятии организуется компьютерная сеть для работы в Интернете, не связанная с локальной сетью каналами передачи информации. Данные, которые необходимо отправить по электронной почте, переносятся на сменных носителях или хранятся в облачных хранилищах, которые проверяются службой безопасности и шифруются, например, с помощью PGP - бесплатной программы шифрования почтовых сообщений и файлов.  
  
**Распределение пропускной способности канала**

Для IP-схемы доступа разделение пропускной способности канала между пользователями можно реализовать средствами брандмауэра, а в случае прокси-сервера - использовать его механизм delay\_pools.  
  
Сервер определяет размер файла, запрошенного пользователем, и если этот размер не превышает установленной величины, то файл загружается на максимально возможной скорости. В случае более объемного файла он передается с заданной ограниченной скоростью. Данный механизм применяется не ко всем пользователям, а лишь к перечисленным в списках ACL (Access Control List - именованная группа объектов, к которым могут применяться различные ограничения), что позволяет очень гибко настраивать приоритеты работы различных групп пользователей.

### **Доступ к ресурсам и другие ограничения**

Для IP-схемы возможны ограничения только по IP-адресам серверов и по TCP/UDP-портам. Это вызывает неудобства, поскольку сегодня распространен механизм Virtual Hosts Web-сервера, когда один Web-сервер с одним IP-адресом обслуживает множество сайтов с разными DNS-именами.

Прокси сервер, наоборот, предоставляет очень гибкие механизмы администрирования доступа пользователей к ресурсам Интернета с помощью списков ACL. Это может быть, например, доступ в определенное время, день недели, месяц; разрешение/запрет на копирование определенных типов файлов, разрешение/запрет на обращение к ресурсу, в имени которого содержится некоторое ключевое слово.

В то же время, если в данный момент работает только один пользователь, к нему все равно будут применяться ограничения по скорости при загрузке больших файлов. Брандмауэр, в отличие от delay\_pools у прокси сервера, позволяет реализовать динамическое деление канала.

**Организация доступа в интернет через мобильные сети**

Для малых предприятий возможна организация доступа в интернет через мобильные сети т.к это является более дешевым решением и позволяет создать альтернативную организацию доступа в интернет для локальной сети.