VPN своими руками

Всё чаще компьютеры объединяются в локальные сети, которые подключаются к глобальной сети Интернет. На первое место выходит сохранность, идентичность и конфиденциальность данных при передаче через незащищённые от перехвата участки сети.

В локальной сети с парой-другой коммутаторов достаточно ограничить к ним физический доступ и правильно настроить политику безопасности для портов - будь то статические MAC адреса или 801.1x авторизация. При объединении нескольких локальных сетей в распределенную корпоративную сеть, как правило, используются либо арендованные каналы, либо Интернет. В обоих случаях нет никакой гарантии, что данные при передаче не будут перехвачены или даже изменены. Один из способов быть уверенным в защищенности ценной информации при ее передаче - построить VPN.

Технология VPN – Virtual Private Network – позволяет создавать шифрованные туннели с опциональной поддержкой проверки идентичности пакетов через слабо или в принципе незащищенные сети. Два VPN шлюза (это могут быть специально предназначенные для этого устройства или обычные PC) устанавливают соединение через IP сеть, по которому данные передаются в зашифрованном виде. Перед началом сеанса передачи VPN шлюзы „договариваются" о ключах для шифрования, порядке и частоте их замены. Для авторизации соединений наиболее часто используются либо пароли (preshared key), либо сертификаты (RSA, x509). Существует множество реализаций данной технологии, как коммерческих, построенных на проприетарных алгоритмах - Intel shiva и другие, так и open source реализаций - openvpn, cipe и так далее. Однако, официально признанным стандартом является протокол IPSec - именно этот протокол поддерживается наибольшим количеством производителей программного обеспечения и оборудования - даже в последних версия OS от Microsoft этот протокол включен по умолчанию. Подавляющее большинство оборудования работающего с коммерческими протоколами, кроме того поддерживают работу и с IPSec.

Можно выделить три базовых подхода в построении распределенной корпоративной сети на базе VPN.

Во-первых, можно выбрать готовое решение VPN, предлагаемое поставщиками услуг передачи данных. Наверное, самое известное и доступное на латвийском рынке это услуга VBT (Vienotais Biznesa Tīkls), продвигаемая Латтелеком. Практически каждый крупный игрок на рынке предлагает нечто подобное. Плюсом такого пути является то, что от заказчика требуется только заплатить (немного) денег - специально обученные люди все настроят и даже объяснят, как это работает. Минус - заказчик должен полностью доверять фирме, обещающей конфиденциальность передаваемых данных и работоспособность решения. Еще пару лет назад автор своими глазами видел, как VBT решение Латтелекома временами пускало внутренний трафик напрямую в Интернет. VITA, позиционирующаяся как сеть государственного значения, арендует каналы данных у того же Латтелеком и некоторые государственные структуры вынуждены строить свои VPN сети внутри сети VITA для обеспечения конфиденциальной передачи данных.

Во-вторых, можно использовать программные решения VPN, которые устанавливаются непосредственно на компьютер пользователя. Как уже упоминалось выше, WindowsXP имеет встроенную поддержку IPSec. На рынке много платных и бесплатных программных продуктов для рабочих станций, позволяющих безопасно обмениваться данными. Плюсом данного решения является низкая, либо нулевая стоимость. Минусом - сложность управления. Каждую рабочую станцию приходится настраивать соответствующим образом и постоянно следить за корректным функционированием, персонал необходимо обучать. Политика безопасности требует также серьезной разработки - один разглашенный пароль может привести к компрометации всей системы. Чем больше людей и компьютеров, тем труднее поддерживать подобную систему.

Третий путь подходит компаниям, имеющим в штате IT профессионала или собственный IT отдел. Данное решение предусматривает использование выделенных аппаратных VPN шлюзов, которые устанавливаются на границе включения локальных сетей в сети общего пользования и прозрачно шифруют внутренний трафик при передаче через Интернет. Вся конфигурация производится на VPN шлюзах - это даёт полный контроль над происходящим, что определенно понравится параноидальным админам. Минусом является необходимость иметь в штате профессионала, способного построить и поддерживать в работе подобную систему.

Как пример можно рассмотреть следующий проект. Имеется фирма с центральным офисом и 3-4 филиалами. Необходимо создать корпоративную компьютерную сеть и обеспечить конфиденциальность передаваемых между офисами данных.

В первом варианте у провайдера заказывается решение по объединению локальных сетей.

Во втором варианте сначала необходимо подключить все офисы к Интернет (или любой другой общей сети). Следующий шаг это установка программных VPN клиентов (и возможно сервера) на рабочие станции. Заключительным этапом можно считать обучающие курсы для персонала.

Третий вариант стоит рассмотреть подробнее - возможны довольно интересные варианты реализации.

Итак, есть центральный офис с широкополосным подключением к Интернет со скоростью > 1Mbps. Это может быть ultraDSL, кабельное подключение или радиолинк. С другой стороны имеются 3 и более филиалов с дешевым подключением типа pilsētas/mājasDSL – 10Ls в месяц вполне адекватная цена для постоянного подключения 4-5 компьютеров. Первым делом необходимо определится с внутренней адресацией - корпоративная сеть может иметь общее адресное пространство, используя частный диапазон IP адресов (к примеру - 192.168.x.x). Во-вторых, надо выбрать технологию VPN - например, IPSec как наиболее распространенную. IPSec требует для корректной работы „реальные” IP адреса и отсутствие фильтрации протокола ESP.

Шлюзом центрального офиса может быть выделенный компьютер работающий под OS Linux. Такой шлюз, помимо трансляции адресов (NAT) и функций брандмауэра, может выполнять еще и функции VPN концентратора. В случае использования ядра linux серии 2.4 необходимо установить и настроить (листинг.1) openswan - продукт, реализующий поддержку IPSec и x509 сертификатов.

```
# File /etc/ipsec.conf
config setup
        interfaces="ipsec0=eth0"
        klipsdebug=none
        plutodebug=none
        plutoload=%search
        plutostart=%search
        plutowait=no
        uniqueids=yes
        forwardcontrol=yes
conn %default
        pfs=no
        keyingtries=2
        keylife=8h
        ikelifetime=30m
        disablearrivalcheck=no
        rekey=no
        leftid=@vpn.company.lv
        leftcert=certs/ipsec.pem
        left=XXX.XXX.XXX.XXX
        leftsubnet=192.168.0.0/24
        rightrsasigkey=%cert
        right=%any
        authby=rsasig
        auto=add
conn office1
        rightid=@office1.vpn
        rightsubnet=192.168.1.0/24
conn office2
        rightid=@office2.vpn
        rightsubnet=192.168.2.0/24
conn office3
        rightid=@office3.vpn
        rightsubnet=192.168.3.0/24
```

Листинг.1

В роли шлюза для филиалов может выступать VPN роутер уровня SOHO с поддержкой IPSec. Цена на такие устройства составляет от 50$ до 100$. Такой шлюз кроме поддержки NAT, firewall и IPSec обычно имеет функции DHCP клиента - способен получать IP адрес от провайдера - и DHCP сервера - сам может раздавать IP адреса подключенным к нему компьютерам. Через руки автора прошло несколько различных подобных устройств - поделки фирмы EUSSO были откровенно „сырыми”, устройства другой фирмы намертво „вешали” коммутатор после нескольких дней работы. Удачным можно назвать решения Linksys (подразделение Cisco). А выбор стоит остановить на

изделии фирмы TrendNet - единственное из дешевых и доступных с поддержкой RSA сертификатов для авторизации IPSec. Использование сертификатов позволяет аутентифицировать разные подключения с динамических адресов. Для этого необходимо создать (листинг.2) и установить сертификаты для каждого устройства.

В схеме, показанной на рисунке.1, шлюзы получают IP адрес по DHCP и инициируют установку шифрованного туннеля с головным офисом. Компьютеры получают IP адреса динамически от шлюза. При обращении к корпоративным ресурсам трафик маршрутизируется через защищённый туннель, в обратном случае после трансляции адресов шлюзом попадает в Интернет.

Схема построения корпоративной сети на базе VPN

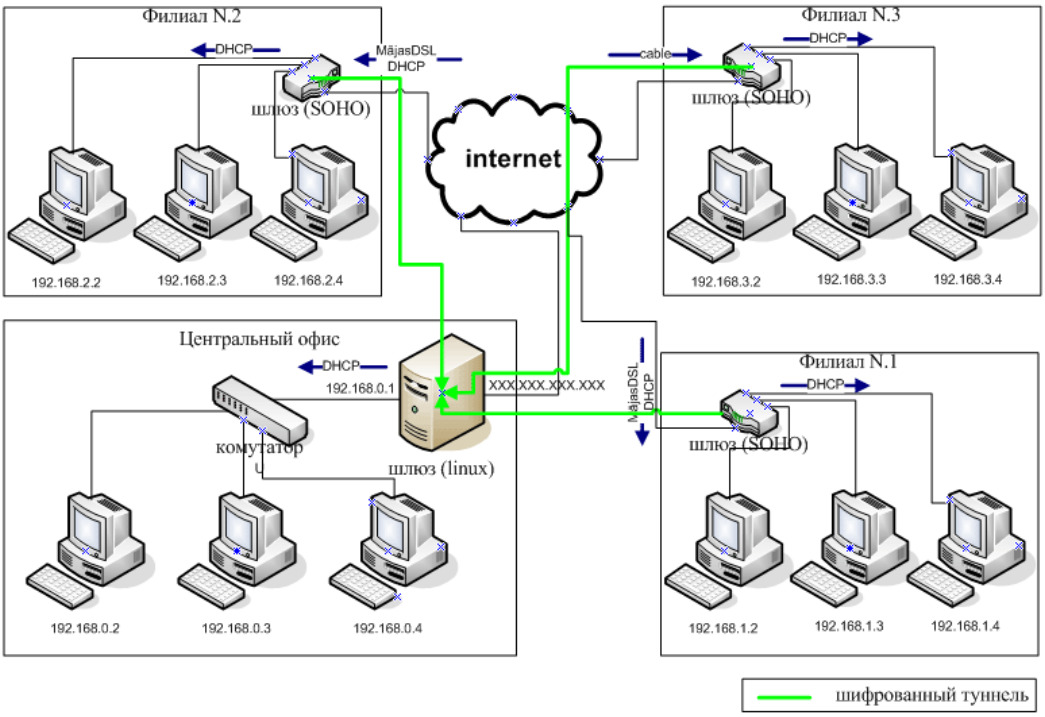

Рисунок 1

Таким образом, каждый может выбрать VPN решение на свой вкус и кошелёк - одни готовы платить за сервис и не беспокоится о том, как это работает, другие ищут решения подешевле, а некоторые пытаются придумать и сделать что-то своими руками из подручных материалов :)

```
# Самоподписанный CA:
openssl genrsa -des3 -out ca.key 1024
openssl req -new -x509 -days 3650 -key ca.key -out ca.crt
# Сертификат для VPN концентратора
openssl genrsa -out ipsec.key 1024
openssl req -new -key ipsec.key -out ipsec.csr
# Подпись сертификата для VPN концентратора
# Файл 509.txt должен состоять из строки 'subjectAltName = DNS:vpn.company.lv'
openssl ca -config openssl.cnf -cert ca.crt -keyfile ca.key \
        -in ipsec.csr -out ipsec.pem -days 365 -extfile 509.txt
# Подпись сертификатов для филиала
# Файл 509.txt должен состоять из строки 'subjectAltName = DNS:office1.vpn'
openssl ca -config openssl.cnf -cert ca.crt -keyfile ca.key \
        -in office1.csr -out office1.pem -days 365 -extfile 509.txt
```

Листинг.2