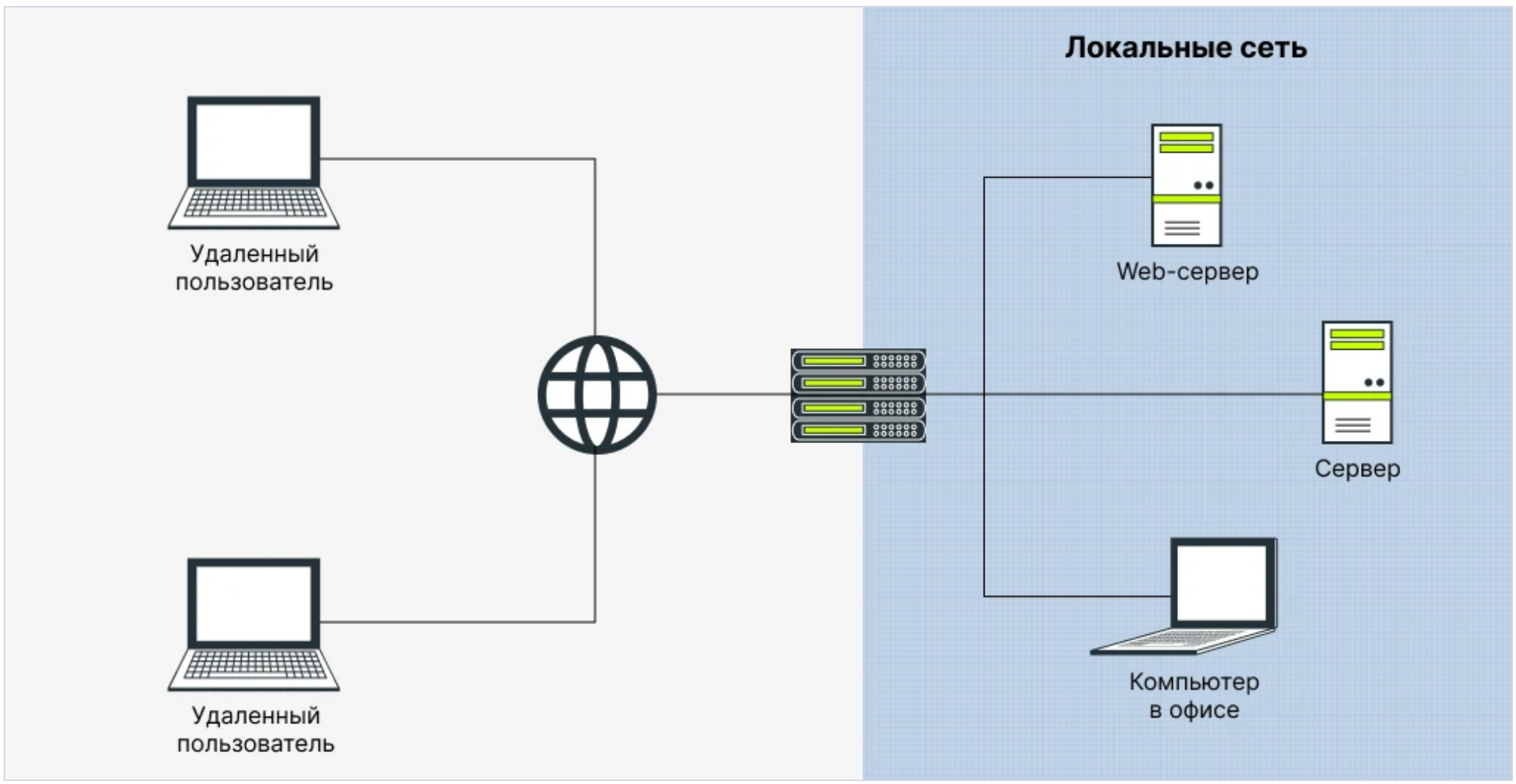
VPN

JSP & Servlets
8 уровень, 5 лекция

ОТКРЫТА

6.1 Знакомство с VPN

Virtual Private Network или **VPN** – это дословно виртуальная частная сеть. Скорее всего, ты часто слышал слово VPN, когда хотели подменить страну в браузере телефона или компьютера. Запустил VPN, выбрал страну и готово.



Хотя VPN к странам, собственно говоря, никакого отношения не имеет. Дело обстоит немного по-другому.

Представь, что ты работаешь в офисе на компьютере, и в этом офисе есть различное компьютерное оборудование с доступом по сети: компьютеры, сервера, принтеры, оборудование для видеоконференций.

Ситуация 1: твой офис вырос, ты решил переехать на соседний этаж. Ты взял свой компьютер, перенес его в другую комнату, подключил в другую сетевую розетку и доступ ко всем серверам и компьютерам компании у тебя сохранился.

Скорее всего, твой компьютер обращается теперь к другому роутеру, но все роутеры вашей компании знают, как общаться друг с другом и обеспечивают тебе все преимущества нахождения в одной локальной сети. У тебя нет проблем с доступом к любому оборудованию в корпоративной сети.

Ситуация 2: началась пандемия и ты решил работать из дома. Ты забрал рабочий компьютер домой, но вот незадача, доступа к офисным серверам дома нет. Вроде бы логично, ведь они остались на офисе в другом конце города. С другой стороны, возникает вопрос: когда ты перенес компьютер в первом случае, то доступ к офисным компьютерам у тебя сохранился. Когда ты перенес компьютер во втором случае, то доступа нет. Что поменялось?

В первом случае все компьютеры в твоем офисе (даже расположенные на разных этажах) находились в одной локальной сети. А во втором случае – нет. Твой компьютер дома не подключен к офисной локальной сети. Соответственно, у тебя нет доступа к внутренним ресурсам офисной сети.

В качестве устранения этой проблемы было предложено решение – **виртуальная локальная сеть** (VPN). У тебя в офисе на каждом этаже стояло по роутеру, которые пересылали между собой данные и обеспечивали работу локальной сети.

Нам нужно создать два **виртуальных роутера** (в виде программ), один у тебя в офисе, второй – дома, которые так же будут пересылать между собой данные по интернету в зашифрованном виде. И такие программы есть: одна из них называется **VPN-сервер**, а вторая – **VPN-клиент**.

VPN-сервер настраивает системный администратор в офисе, а VPN-клиент сейчас есть в каждом компьютере и/или телефоне.

Ты запускаешь у себя на компьютере VPN-клиент и конектишься с его помощью к VPN-серверу, таким образом компьютер теперь думает, что он находится внутри локальной сети, в которой расположен VPN-сервер.

Если ты теперь запустишь у себя браузер, то все данные от твоего браузера пойдут в твой локальный виртуальный роутер (VPN-клиент), из него в виртуальный роутер компании (VPN-сервер), а затем уже дальше в мир через интернет-шлюз офиса твоей компании.

Внешний IP-адрес твоего компьютера теперь будет совпадать с публичным IP-адресом твоего офиса. И если этот офис был, например, в Германии, то сервер, к которому обращался твой браузер, будет уверен, что ты в офисе в Германии.

6.2 Типы VPN

Сети VPN делятся по их целевым функциям. Можно выделить много разных, но вот список типовых вариантов VPN-решений:

Intranet VPN

Используется для объединения в единую защищенную сеть нескольких распределенных филиалов одной организации, обменивающихся данными по открытым каналам связи. Это первый вариант, с которого все и началось.

Remote-access VPN

Используется для создания защищенного канала между сегментом корпоративной сети (центральным офисом или филиалом) и одиночным пользователем, который, работая дома, подключается к корпоративным ресурсам с домашнего компьютера, корпоративного ноутбука, смартфона или интернет-киоска. Именно этот вариант у тебя, если ты работаешь из дома и подключаешься к офису через VPN.

Extranet VPN

Используется для сетей, к которым подключаются “внешние” пользователи (например, заказчики или клиенты). Уровень доверия к ним намного ниже, чем к сотрудникам компании, поэтому требуется обеспечение специальных “рубежей” защиты, предотвращающих или ограничивающих доступ последних к особо ценной, конфиденциальной информации.

Internet VPN

Используется провайдерами для предоставления доступа к интернету, обычно если по одному физическому каналу подключаются несколько пользователей. Протокол PPPoE стал стандартом в ADSL-подключениях.

L2TP был широко распространен в середине 2000-х годов в домовых сетях: в те времена внутрисетевой трафик не оплачивался, а внешний стоил дорого. Это давало возможность контролировать расходы: когда VPN-соединение выключено, пользователь ничего не платит.

В настоящее время проводной интернет дешевый или безлимитный, а на стороне пользователя зачастую есть маршрутизатор, на котором включать-выключать интернет не так удобно, как на компьютере. Поэтому L2TP-доступ отходит в прошлое.

Client/server VPN

Тоже популярный вариант. Он обеспечивает защиту передаваемых данных между двумя узлами (не сетями) корпоративной сети. Особенность данного варианта в том, что VPN строится между узлами, находящимися, как правило, в одном сегменте сети, например, между рабочей станцией и сервером. Такая необходимость очень часто возникает в тех случаях, когда в одной физической сети необходимо создать несколько логических сетей.

Например, когда надо разделить трафик между финансовым департаментом и отделом кадров, обращающихся к серверам, находящимся в одном физическом сегменте. Этот вариант похож на технологию VLAN, но вместо разделения трафика используется его шифрование.

6.3 OpenVPN

Помните, мы говорили про виртуальный роутер на стороне офиса, к которому можно конектиться с помощью VPN-клиентов? Так вот, есть одно очень популярное решение, о котором вам полезно будет узнать. Это OpenVPN.

OpenVPN — это бесплатная программа, которая реализует технологию виртуальной частной сети (VPN). Она поддерживает два популярных режима работы: клиент-сервер и точка-точка, когда нужно объединить две большие сети.

Она поддерживает хороший уровень шифрования трафика между своими участниками, а также позволяет устанавливать соединения между компьютерами, находящимися за NAT и сетевым экраном, без необходимости изменения их настроек.

Для обеспечения безопасности управляющего канала и потока данных OpenVPN использует библиотеку **OpenSSL**. Это позволяет задействовать весь набор алгоритмов шифрования, доступных в данной библиотеке.

Также может использоваться пакетная аутентификация **HMAC** для обеспечения большей безопасности и аппаратное ускорение для улучшения производительности шифрования. Эта библиотека использует OpenSSL, а точнее, протоколы **SSLv3/TLSv1.2**.

Есть реализации этой программы под все популярные операционные системы: Solaris, OpenBSD, FreeBSD, NetBSD, GNU/Linux, Apple Mac OS X, QNX, Microsoft Windows, Android, iOS.

OpenVPN предлагает пользователю **несколько видов аутентификации**:

- **Предустановленный ключ** — самый простой метод.
- **Сертификатная аутентификация** — наиболее гибкий в настройках метод.
- С помощью **логина** и **пароля** — может использоваться без создания клиентского сертификата (серверный сертификат все равно нужен).

Техническая информация

OpenVPN проводит все сетевые операции через TCP- или UDP-транспорт. В общем случае предпочтительным является UDP, потому что через туннель проходит трафик сетевого уровня и выше по OSI, если используется TUN-соединение, или трафик канального уровня и выше, если используется TAP.

Это значит, что OpenVPN для клиента выступает протоколом канального или даже физического уровня, а значит, надежность передачи данных может обеспечиваться вышестоящими по OSI уровнями, если это необходимо.

С учетом того, что мы хорошо разобрали модель OSI, вы должны понимать, о чем тут говорится.

Именно поэтому протокол UDP по своей концепции наиболее близок к OpenVPN, так как он, как и протоколы канального и физического уровней, не обеспечивает надежности соединения, передавая эту инициативу более высоким уровням. Если же настроить туннель на работу по TCP, сервер в типичном случае будет получать TCP-сегменты OpenVPN, которые содержат другие TCP-сегменты от клиента.

Также, что не маловажно, OpenVPN может работать через большую часть прокси-серверов, включая HTTP, SOCKS, через NAT и сетевые фильтры. Сервер может быть настроен на назначение сетевых настроек клиенту. Например, IP-адрес, настройки маршрутизации и параметры соединения.

‹ Предыдущая лекция

Следующая лекция ›

+12

Комментарии (3) популярные новые старые

JavaCoder

Введите текст комментария

Mixon Older Уровень 21 — 19 июня, 19:25

Как свой впн сделать?

Ответить +2

Andrey Panchenko Моет полы в **Яндекс** — 16 сентября, 19:18

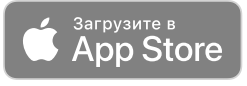
Вот, не благодари

Ответить +8

Mixon Older Уровень 21 — 17 сентября, 09:54

Это идеальное решение!!!
просто уровня бог))))

Ответить 0



"Программистами не рождаются" © 2022 JavaRush