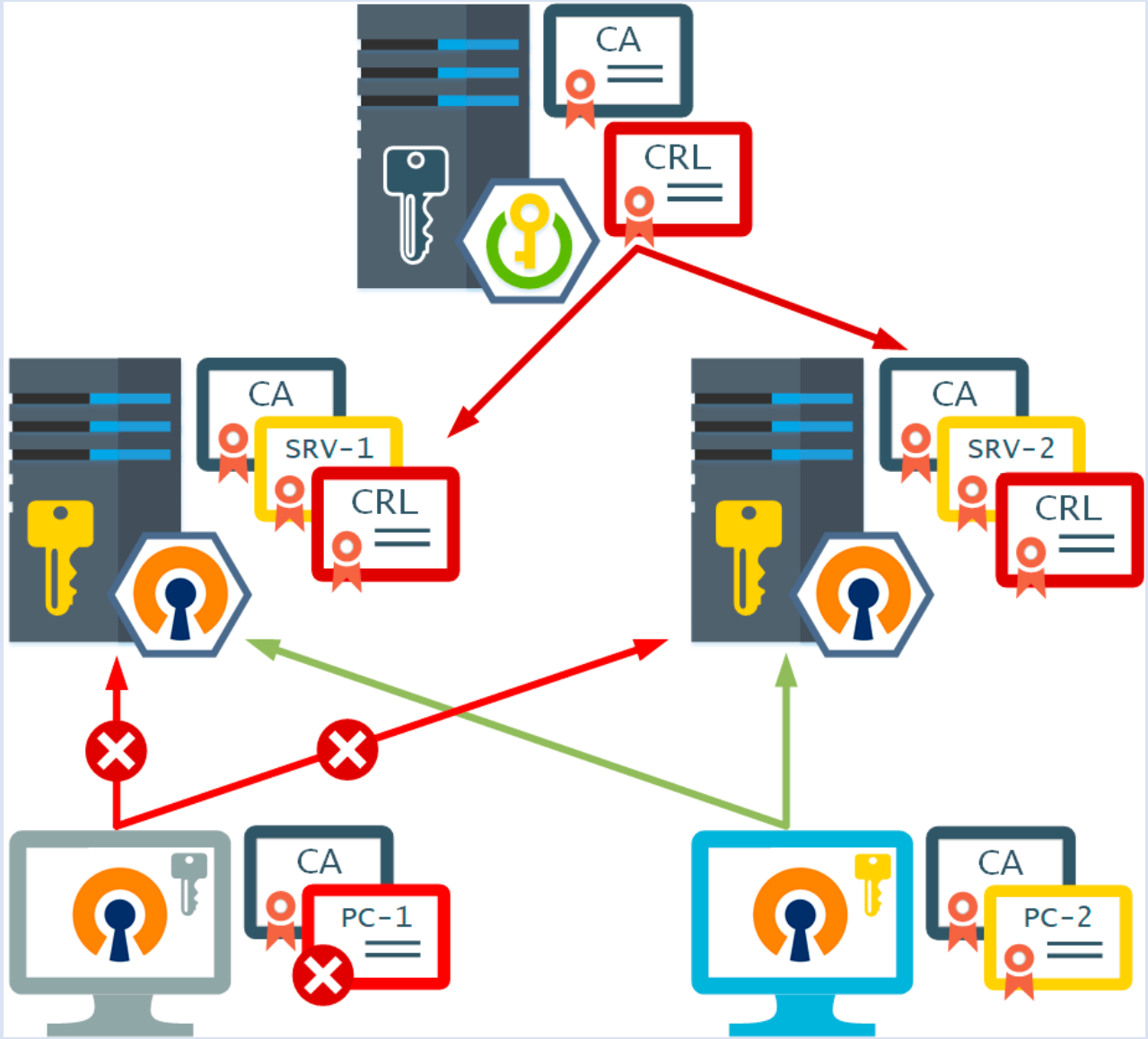
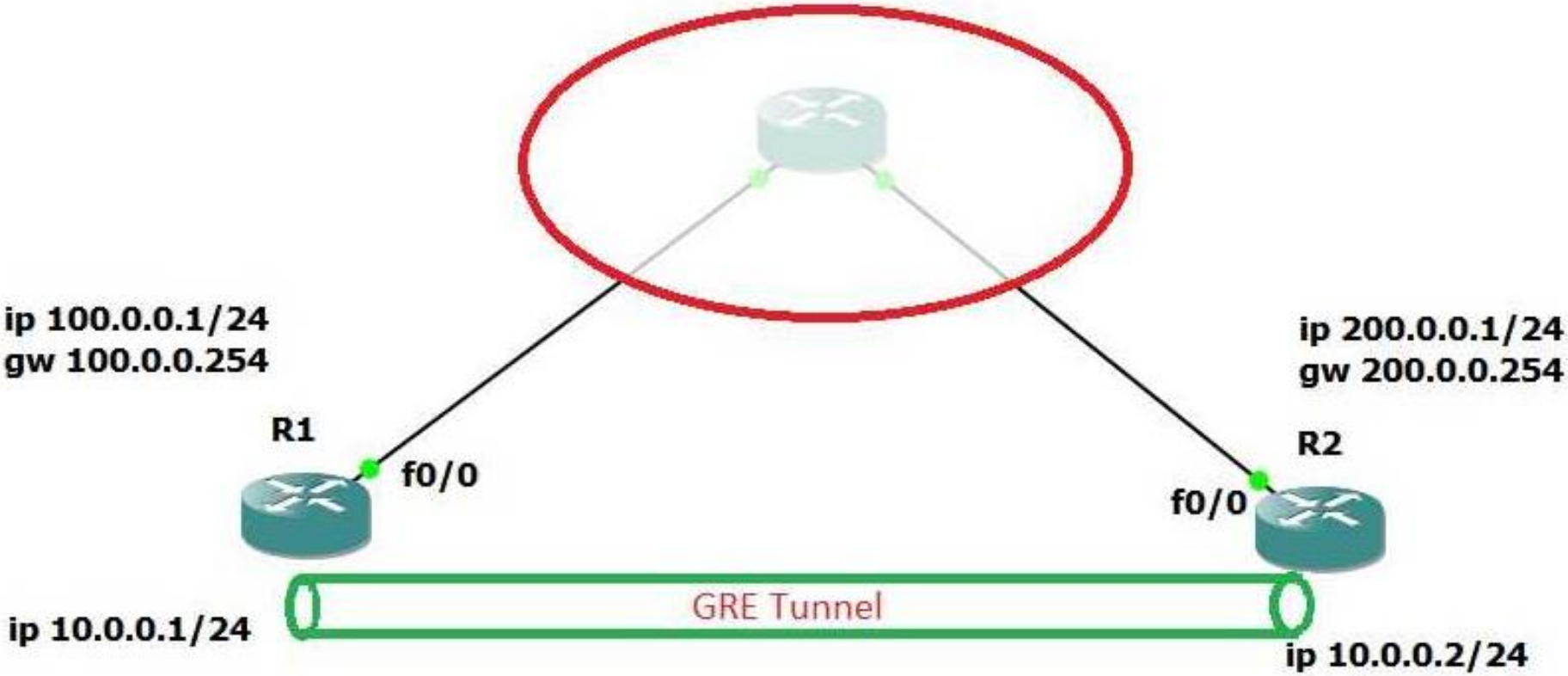
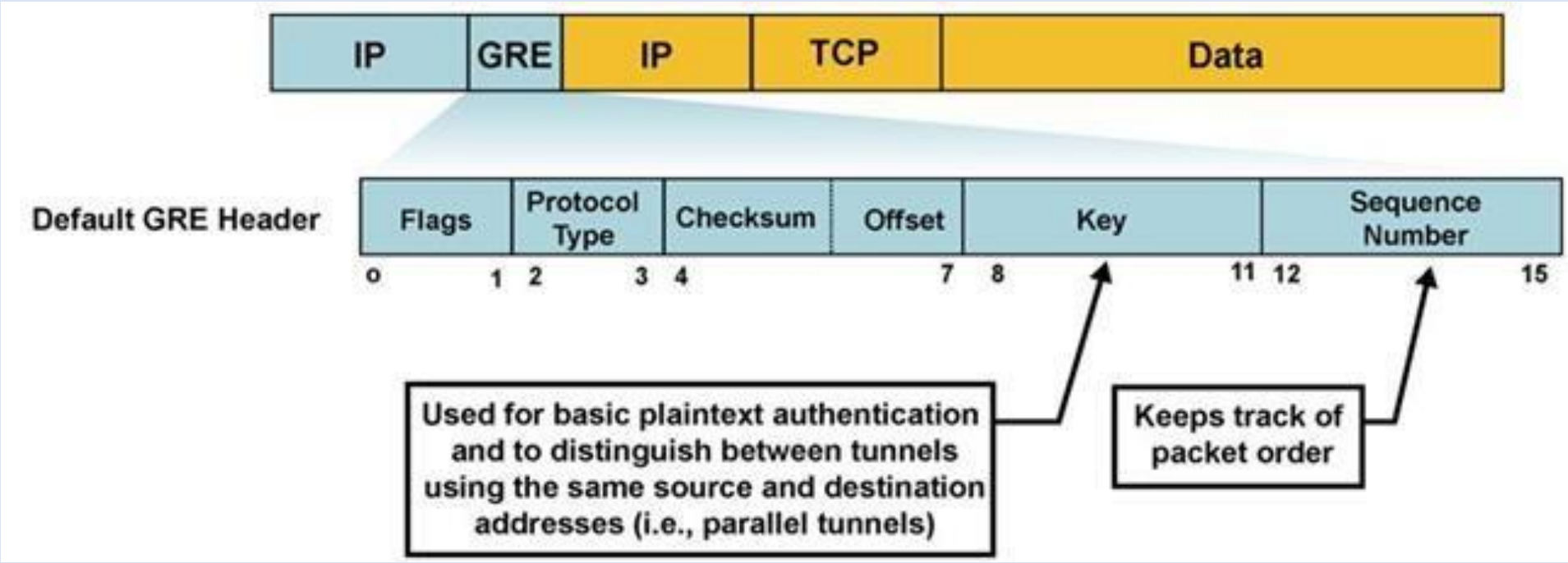
Тема:
Основные сервисы на Linux .
PKI и Openvpn.



План занятия:

1. Основы PKI (Public Key Infrastructure).
2. OpenVPN.


ip 100.0.0.1/24
gw 100.0.0.254
R1
f0/0
ip 200.0.0.1/24
gw 200.0.0.254
R2
f0/0
GRE Tunnel
ip 10.0.0.1/24
ip 10.0.0.2/24


IP
GRE
IP
TCP
Data
Default GRE Header
Flags
Protocol Type
Checksum
Offset
Key
Sequence Number
0
1
2
3
4
7
8
11
12
15
Used for basic plaintext authentication and to distinguish between tunnels using the same source and destination addresses (i.e., parallel tunnels)
Keeps track of packet order

Методы шифрования

Симметричное шифрование – один ключ

Асимметричное шифрование – пара ключей: открытый и личный

Алгоритм Диффи-Хеллмана

Пользователь А	Открытый канал	Пользователь Б
1. Выбрать случайное число x	g, n – большие простые числа, открытые параметры	1. Выбрать случайное число y
2. Вычислить $X = \mathrm{mod}(g^x, n)$		2. Вычислить $Y = \mathrm{mod}(g^y, n)$
3. Передать X пользователю Б	X →	3. Передать Y пользователю А
4. Получить Y. Вычислить $K2 = \mathrm{mod}(Y^x, n)$	← Y	4. Получить X. Вычислить $K1 = \mathrm{mod}(X^y, n)$

Ключ $K1 = K2 = \mathrm{mod}(g^{x \cdot y}, n)$ используется в симметричном алгоритме

1. Основы PKI (Public Key Infrastructure).

Инфраструктура открытых ключей (PKI - Public Key Infrastructure) — набор средств (технических, материальных, людских и т. д.), распределённых служб и компонентов, в совокупности используемых для поддержки криптозадач на основе шифрования с открытым ключом.

Основными компоненты PKI:

1.Центр сертификации (CA, Certificate Authority) является доверенным органом, который выпускает и подписывает цифровые сертификаты. Он удостоверяет подлинность открытых ключей и связь между открытыми ключами и субъектами (пользователями, устройствами или серверами).

2.Регистрационный авторитет (RA, Registration Authority) отвечает за аутентификацию и проверку подлинности пользователей и устройств перед выдачей сертификатов Центром сертификации. RA может собирать и верифицировать информацию о субъекте. RA обычно работает вместе с CA

3.Цифровые сертификаты (Digital Certificates) содержат открытый ключ и информацию о субъекте, такую как имя, адрес электронной почты и другие атрибуты. Сертификаты подписываются Центром сертификации, что делает их доверенными.

4.Закрытые ключи (Private Keys) и **открытые ключи** (Public Keys). Пары ключей используются в криптографии с открытым ключом.

5.Списки отзыва сертификатов (CRL, Certificate Revocation Lists): Списки отзыва сертификатов содержат информацию о сертификатах, которые были отозваны до истечения срока действия.

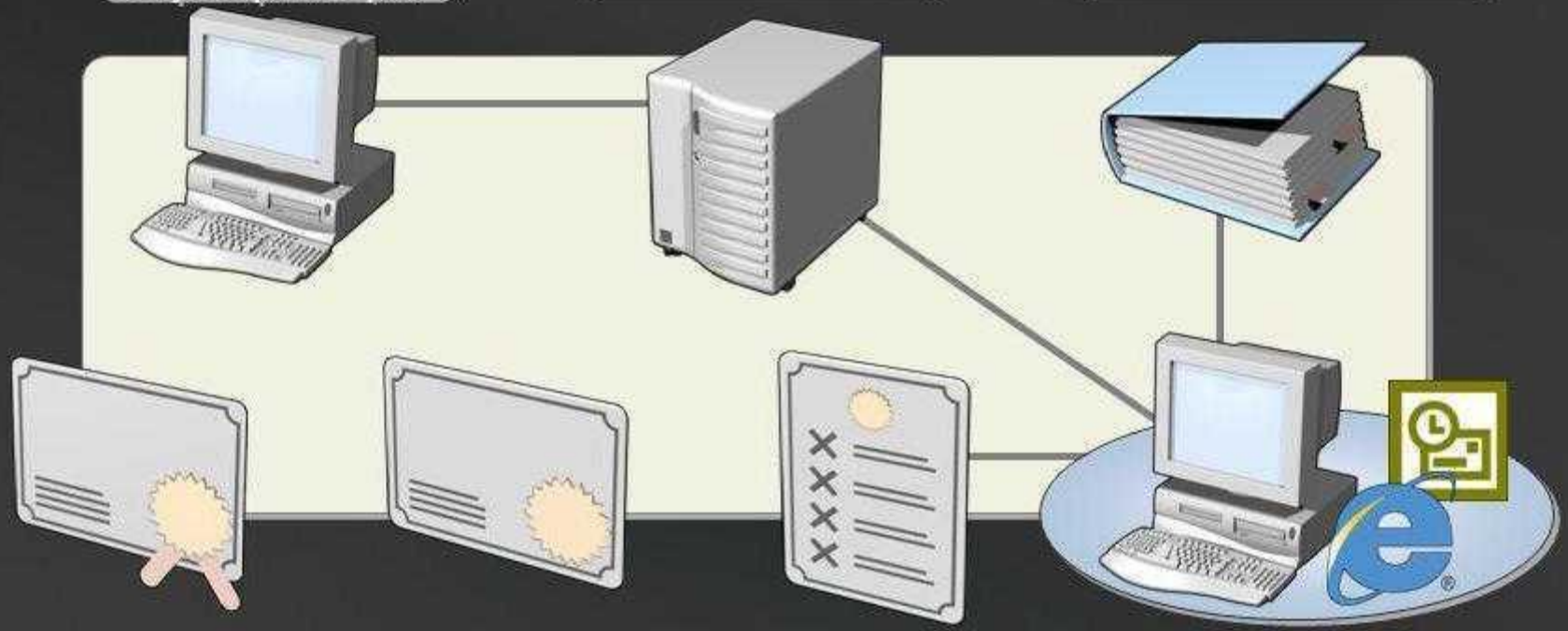
6.Протоколы и стандарты для обеспечения безопасности, такие как X.509 для формата сертификатов, SSL/TLS для защищенной передачи данных и протоколы аутентификации, такие как Kerberos.

Компоненты PKI

Инструменты управления центром сертификации

Центр сертификации

Сертификаты, точки отзывов и распространения



Шаблоны сертификатов

Цифровой сертификат

Список отозванных сертификатов

PKI Приложения и службы

Механизм работы PKI :

1.Генерация ключей: Пользователь или организация, намеревающиеся использовать PKI, генерируют пару ключей - публичный и приватный ключи. Приватный ключ является секретным и должен храниться в безопасности, а публичный ключ распространяется и связывается с соответствующим субъектом.

2.Запрос на сертификат: Субъект, имеющий публичный ключ, отправляет запрос на цифровой сертификат в Центр сертификации (CA) или его регистрационный центр (RA). Запрос на сертификат содержит информацию о субъекте, включая его публичный ключ.

3.Проверка и аутентификация: CA или RA проверяют подлинность идентификационных данных субъекта, представленных в запросе на сертификат. Это может включать проверку удостоверяющих документов или других методов аутентификации. Если субъект успешно проходит проверку, CA выпускает цифровой сертификат.

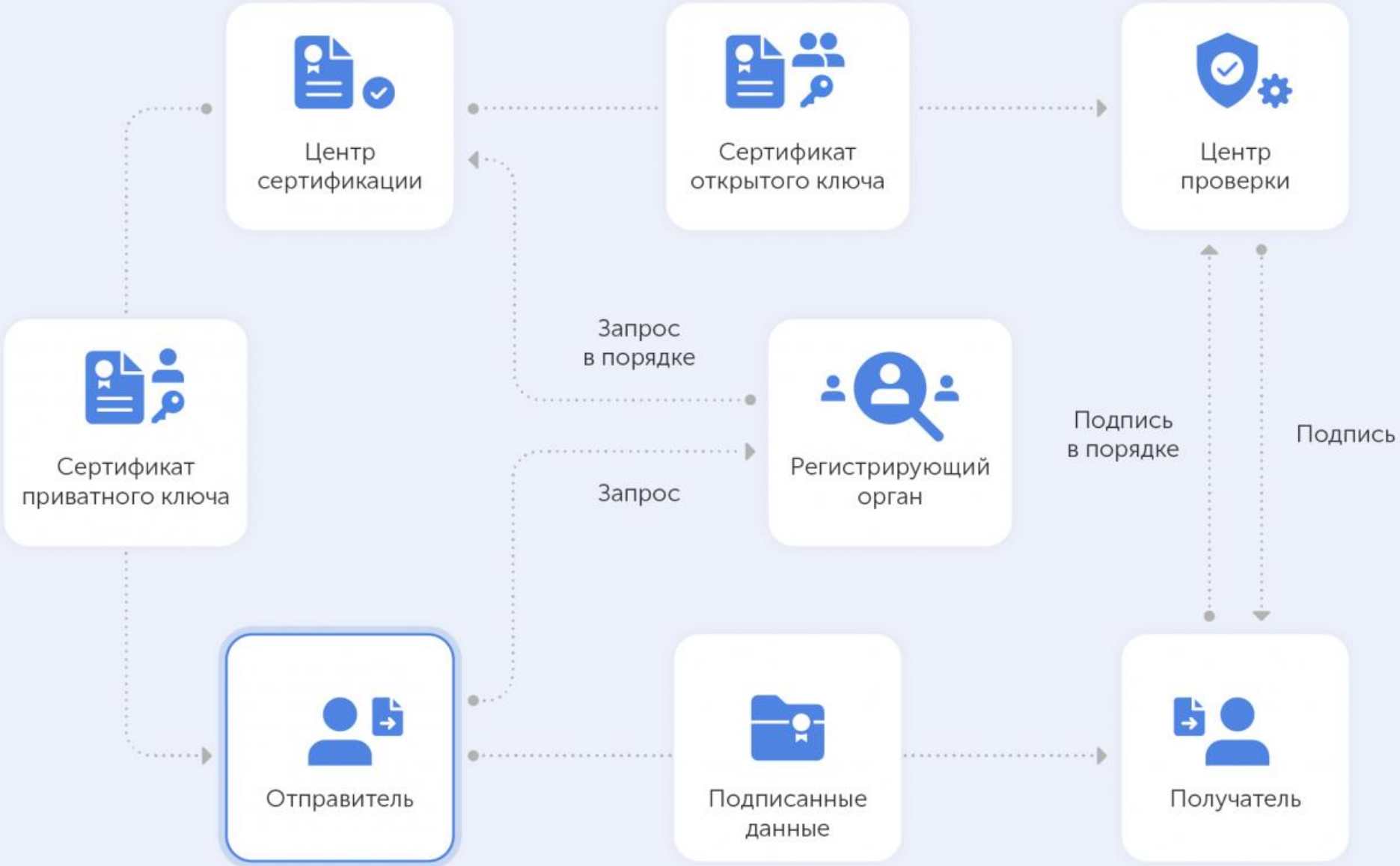
4.Выпуск сертификата: Центр сертификации создает цифровой сертификат, который содержит информацию о субъекте, его публичный ключ и подпись CA. Подпись CA гарантирует подлинность и целостность сертификата. Цифровой сертификат является электронным документом, который может быть распространен и использован другими участниками системы PKI.

5.Распространение сертификатов: Выпущенные цифровые сертификаты распространяются посредством различных методов. Они могут быть размещены в общедоступных каталогах, отправлены по электронной почте или доступны через онлайн-протоколы проверки статуса сертификатов (OCSP).

6.Проверка подлинности: При необходимости другие пользователи или приложения могут проверить подлинность цифрового сертификата, используя публичный ключ CA. Они могут также проверить статус сертификата, используя список отзыва сертификатов (CRL) или онлайн-протокол проверки статуса сертификатов (OCSP).

7.Шифрование и аутентификация: При взаимодействии между субъектами, использующими PKI, они могут использовать публичные ключи друг друга для шифрования информации и проверки подлинности. Публичный ключ субъекта может быть использован для шифрования данных, которые затем могут быть расшифрованы только с использованием соответствующего приватного ключа.

8.Обновление и отзыв сертификатов: Центр сертификации может выполнять обновление сертификатов при истечении срока их действия или в случае изменения данных субъекта. Кроме того, в случае компрометации приватного ключа или других проблем безопасности, сертификат может быть отозван Центром отзыва сертификатов, и его статус будет отражен в списках отзыва сертификатов (CRL) или онлайн-протоколе проверки статуса сертификатов (OCSP).


Центр сертификации
Сертификат открытого ключа
Центр проверки
Запрос в порядке
Сертификат приватного ключа
Регистрирующий орган
Подпись в порядке
Подпись
Запрос
Отправитель
Подписанные данные
Получатель

2. OpenVPN

VPN (Virtual Private Network) - это технология, которая создает зашифрованное и безопасное соединение между вашим устройством (клиентом) и удаленной сетью (сервером) через общедоступную сеть, такую как интернет.

Вот основные принципы работы VPN:

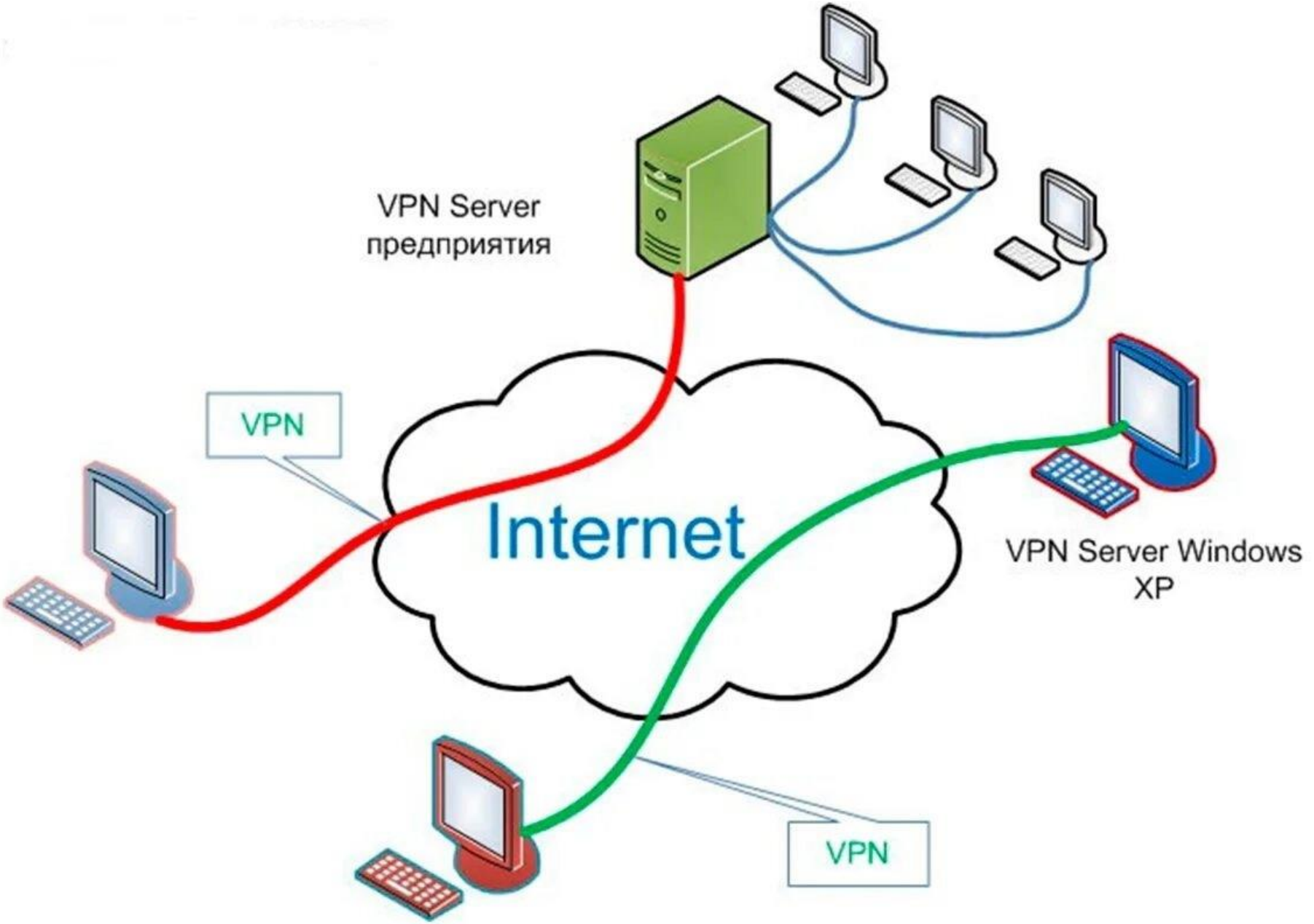
1. **Шифрование данных**: VPN использует мощные алгоритмы шифрования для защиты данных во время их передачи через общедоступные сети

2. **Туннелирование**: VPN устанавливает зашифрованный "туннель" через общедоступные сети между вашим устройством и удаленной сетью.

3. **Сокрытие IP-адреса**: VPN скрывает ваш реальный IP-адрес и заменяет его IP-адресом сервера VPN.

4. **Удаленный доступ** к ресурсам сети: VPN позволяет удаленным пользователям получать доступ к ресурсам корпоративной сети или домашнего компьютера, как если бы они находились внутри этой сети.

5. **Безопасная передача данных**: VPN защищает данные от перехвата и манипуляции вредоносными лицами, обеспечивая конфиденциальность и целостность информации во время ее передачи.


VPN Server
предприятия
VPN
Internet
VPN Server Windows
XP
VPN

Программные решения для создания VPN (виртуальных частных сетей):

IPsec (Internet Protocol Security): IPsec - это протокол безопасности, который используется для обеспечения безопасного и защищенного VPN-соединения на уровне IP. Он предоставляет методы аутентификации, шифрования и целостности данных.

WireGuard - это современный протокол VPN с открытым исходным кодом, который обеспечивает быструю и безопасную передачу данных. Он характеризуется простотой в настройке и высокой производительностью.

L2TP/IPsec (Layer 2 Tunneling Protocol / Internet Protocol Security): L2TP/IPsec - это комбинированный протокол, который объединяет L2TP для создания туннеля и IPsec для обеспечения безопасности данных внутри туннеля. Он широко используется в корпоративных сетях и маршрутизаторах.

PPTP (Point-to-Point Tunneling Protocol): PPTP - это старый протокол VPN, который обеспечивает простую настройку и высокую совместимость с различными операционными системами. Однако его безопасность подвергается сомнению, и его использование сейчас не рекомендуется из-за известных уязвимостей.

IKEv2 (Internet Key Exchange version 2): IKEv2 - это протокол обмена ключами, который обеспечивает аутентификацию и установку безопасного VPN-туннеля. Он часто используется в мобильных устройствах и сетях с мобильными клиентами.

OpenVPN — это программное обеспечение для создания виртуальной частной сети (VPN), которая обеспечивает безопасное соединение между удаленными пользователями или сетями через незащищенные сети, такие как интернет. Оно основано на технологии SSL/TLS для шифрования и аутентификации данных, обеспечивая тем самым конфиденциальность, целостность и аутентификацию.

Основные особенности и компоненты OpenVPN:

1. **Протоколы**: OpenVPN поддерживает различные протоколы, включая UDP (User Datagram Protocol) и TCP (Transmission Control Protocol), что делает его гибким в использовании в различных сценариях сетевой связи.

2. **Шифрование**: OpenVPN использует сильные алгоритмы шифрования для защиты данных, такие как AES (Advanced Encryption Standard) с ключами длиной до 256 бит.

3. **Аутентификация**: OpenVPN обеспечивает аутентификацию пользователей и устройств с помощью сертификатов или логинов/паролей, используя TLS (Transport Layer Security) протокол.

4. **Множество операционных систем**: OpenVPN доступен для различных операционных систем, включая Windows, macOS, Linux и многие другие, что обеспечивает широкий спектр совместимости и возможность использования на различных устройствах.
5. **Гибкая конфигурация**: OpenVPN предлагает широкие возможности конфигурации, включая настройку сетевых параметров, маршрутизацию, управление доступом и многое другое.
6. **Масштабируемость**: OpenVPN поддерживает масштабирование, что позволяет создавать сложные сети с большим количеством клиентов и серверов.
7. **Открытый исходный код**: OpenVPN является проектом с открытым исходным кодом, что позволяет разработчикам и администраторам проверять его безопасность, а также вносить свои вклады в его развитие и улучшение.

Основные компоненты OpenVPN:

1.Сервер OpenVPN: Сервер OpenVPN - это устройство или программное обеспечение, которое устанавливает VPN-сервер и обрабатывает входящие подключения от клиентов. Он управляет аутентификацией, шифрованием и маршрутизацией данных.

2.Клиент OpenVPN: Клиент OpenVPN - это устройство или программное обеспечение, которое устанавливает VPN-клиент и подключается к серверу OpenVPN. Он управляет установкой безопасного канала связи с сервером и обеспечивает защищенную передачу данных через общедоступные сети.

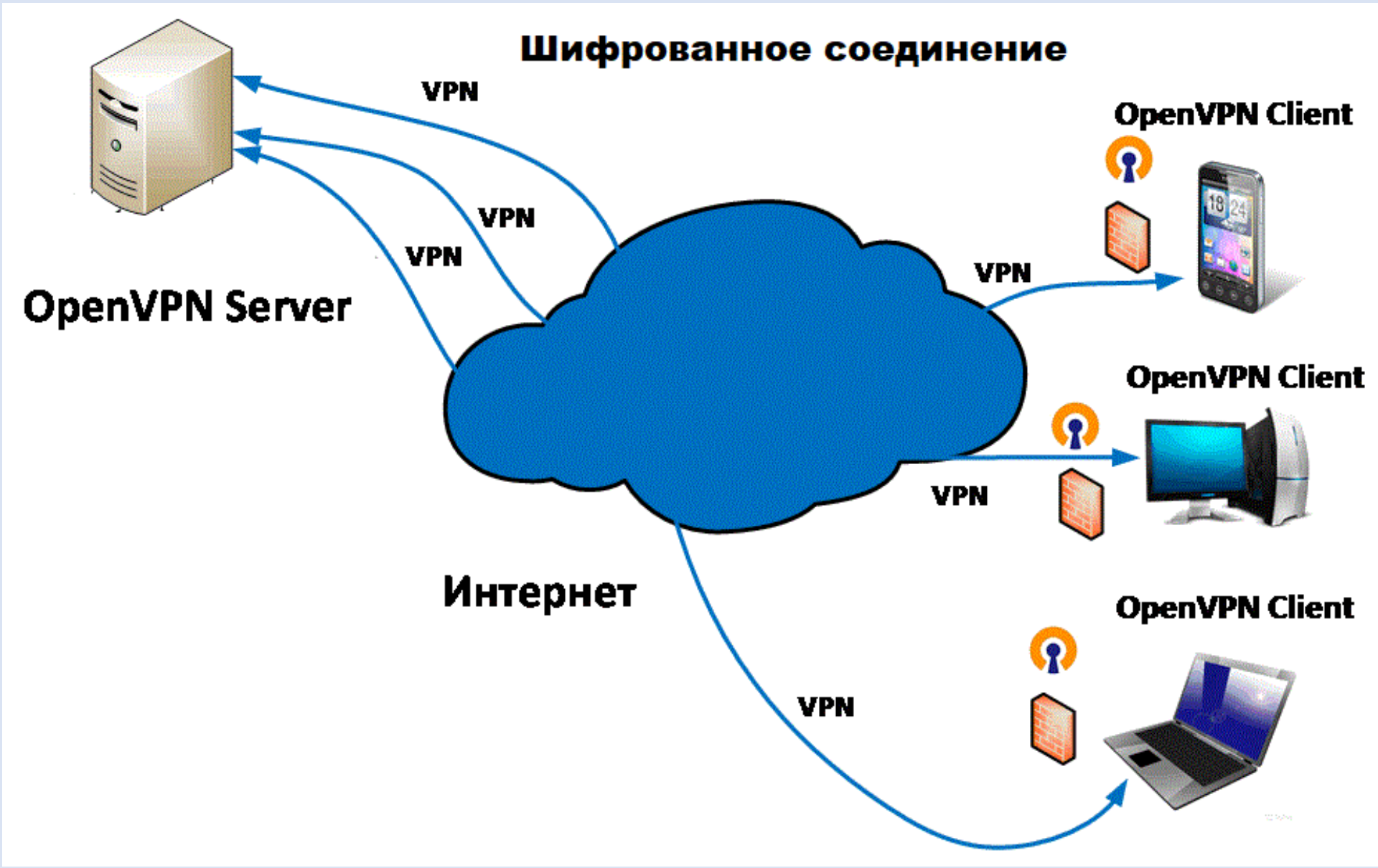
3.Конфигурационные файлы: OpenVPN использует конфигурационные файлы для определения параметров соединения, таких как адрес сервера, порт, протокол, аутентификационные данные и настройки безопасности. Эти файлы настраиваются на сервере и клиенте для правильной настройки соединения.

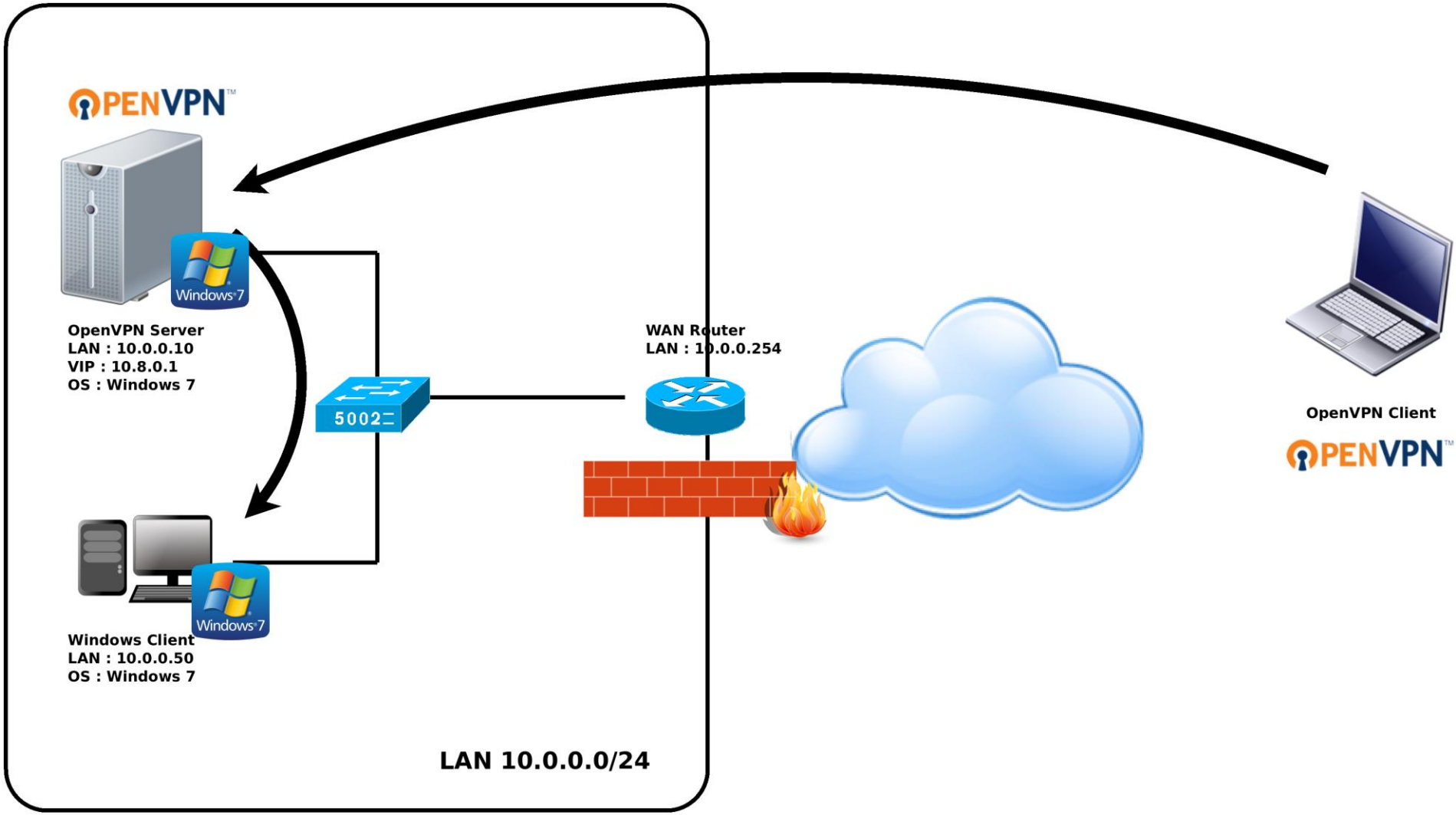
4.Сертификаты и ключи: OpenVPN использует сертификаты и ключи для аутентификации и обеспечения безопасности соединения. Сервер и клиент обычно имеют свои собственные сертификаты и ключи, которые используются для взаимной аутентификации.

5.Файлы хранения данных (Data Storage Files): OpenVPN использует файлы хранения данных для временного хранения информации о текущем состоянии соединения, сессионных ключах и других параметрах, необходимых для обмена данными между сервером и клиентами.

6.**Протоколы и шифрование**: OpenVPN поддерживает различные протоколы, включая UDP (User Datagram Protocol) и TCP (Transmission Control Protocol), а также различные алгоритмы шифрования, такие как AES (Advanced Encryption Standard) и RSA (Rivest-Shamir-Adleman).

Эти компоненты взаимодействуют друг с другом для создания безопасного и надежного VPN-соединения между сервером и клиентами. Они позволяют защищать данные от несанкционированного доступа и обеспечивать конфиденциальность и целостность коммуникации в сети.


Шифрованное соединение
VPN
VPN
VPN
OpenVPN Server
Интернет
VPN
OpenVPN Client
VPN
OpenVPN Client
VPN
OpenVPN Client


OPENVPN
Windows 7
OpenVPN Server
LAN : 10.0.0.10
VIP : 10.8.0.1
OS : Windows 7
5002
WAN Router
LAN : 10.0.0.254
OpenVPN Client
OPENVPN
Windows 7
Windows Client
LAN : 10.0.0.50
OS : Windows 7
LAN 10.0.0.0/24

Настройка openvpn на linux.

Установка OpenVPN. Установите пакеты OpenVPN на вашем сервере и клиентском устройстве. В большинстве дистрибутивов Linux это можно сделать через менеджер пакетов.

Создание сертификатов и ключей. Создайте сертификаты и ключи для сервера и клиента. Это включает в себя генерацию ключей шифрования и подписывания, а также самоподписанный сертификат для сервера. Для этого можно использовать утилиту Easy-RSA, входящую в пакет OpenVPN.

Настройка сервера OpenVPN. Создайте конфигурационный файл для сервера OpenVPN, указав параметры сети, аутентификации, шифрования и другие настройки. Обычно конфигурационный файл сервера располагается в каталоге /etc/openvpn/. Настройте файлы сертификатов и ключей в конфигурационном файле.

Настройка клиента OpenVPN. Создайте конфигурационный файл для клиента OpenVPN, указав параметры подключения к серверу, аутентификации, шифрования и другие настройки. Обычно конфигурационный файл клиента имеет расширение .conf. Скопируйте файлы сертификатов и ключей клиента на клиентское устройство.

Настройка брандмауэра. Убедитесь, что брандмауэр на сервере и клиентском устройстве разрешает трафик через порты, используемые OpenVPN. По умолчанию, это порт 1194/UDP.

Запуск и тестирование. Запустите службу OpenVPN на сервере и клиентском устройстве, используя соответствующие команды. Проверьте соединение между сервером и клиентом, убедившись, что клиент успешно подключается к серверу и может передавать данные через VPN.

Дополнительная настройка. При необходимости выполните дополнительные настройки, такие как настройка маршрутизации, перенаправления трафика или настройка DNS.

После завершения этих шагов ваш сервер OpenVPN должен быть готов к использованию, и клиенты смогут подключаться к нему через безопасный VPN-туннель. Убедитесь, что вы обеспечиваете безопасность ваших сертификатов и ключей, так как они предоставляют доступ к вашей защищенной сети.

Домашнее задание:

1. Изучить дополнительные материалы.