

Сеть и сетевые протоколы: VPN

Александр Гришин
Эксперт в области системного администрирования



Александр Гришин

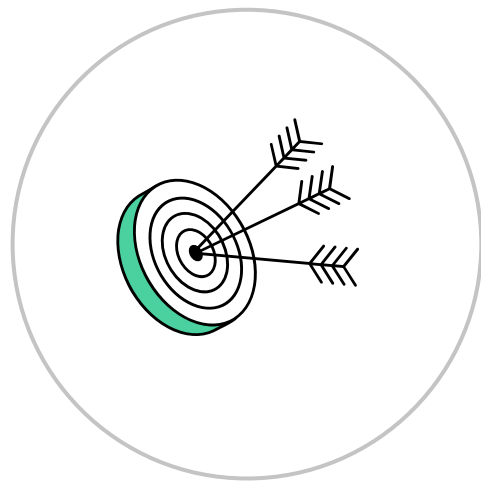
О спикере:

- Инженер в компании YADRO



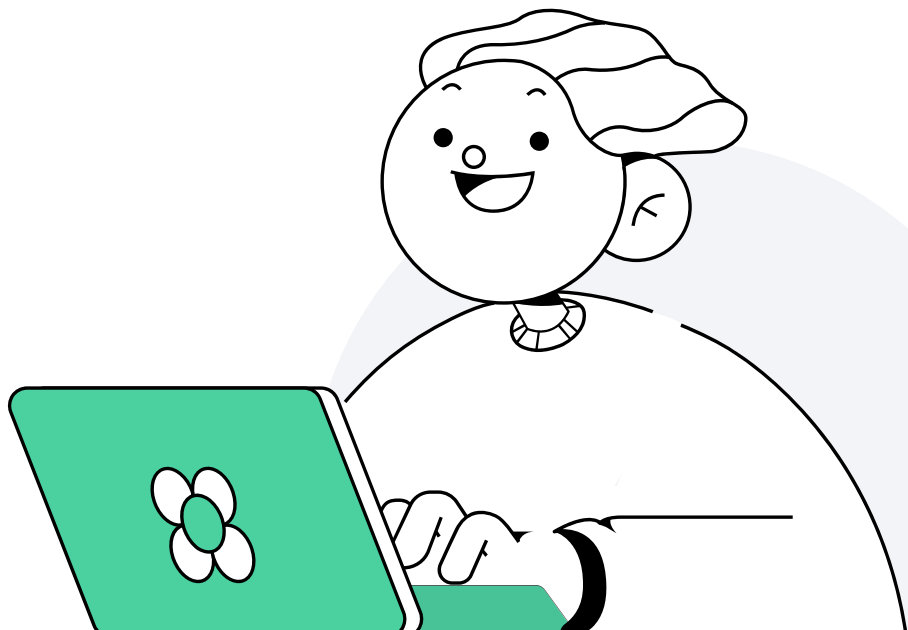
Цели занятия

- Познакомиться с технологией VPN, особенностями архитектуры и применения
- Разобраться с различными протоколами VPN, их преимуществами и недостатками
- Понять принцип работы шифрования и туннелирования на примере работы протокола IPSec

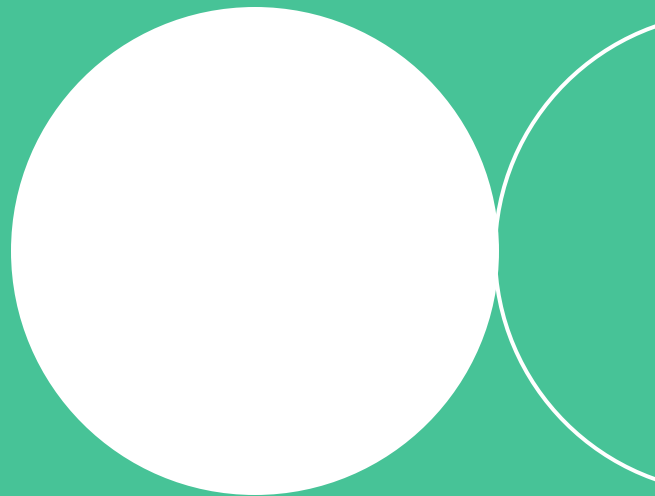


План занятия

- 1 [Знакомство с VPN](#)
- 2 [VPN Point-to-Point](#)
- 3 [VPN Remote access](#)
- 4 [VPN Site-to-Site](#)
- 5 [VPN протоколы](#)
- 6 [IPSec](#)
- 7 [VPN сервисы](#)
- 8 [Домашнее задание](#)

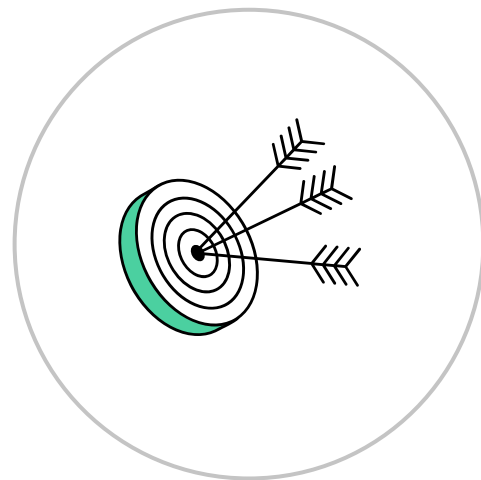


Знакомство с VPN



Цели темы

- Провести краткий обзор технологии VPN
- Узнать об истории возникновения и особенностях применения VPN
- Познакомиться с различными видами архитектуры VPN



VPN



Check Point
SOFTWARE TECHNOLOGIES LTD.

infotecs
ViPNet



КОД
безопасности
Континент 4



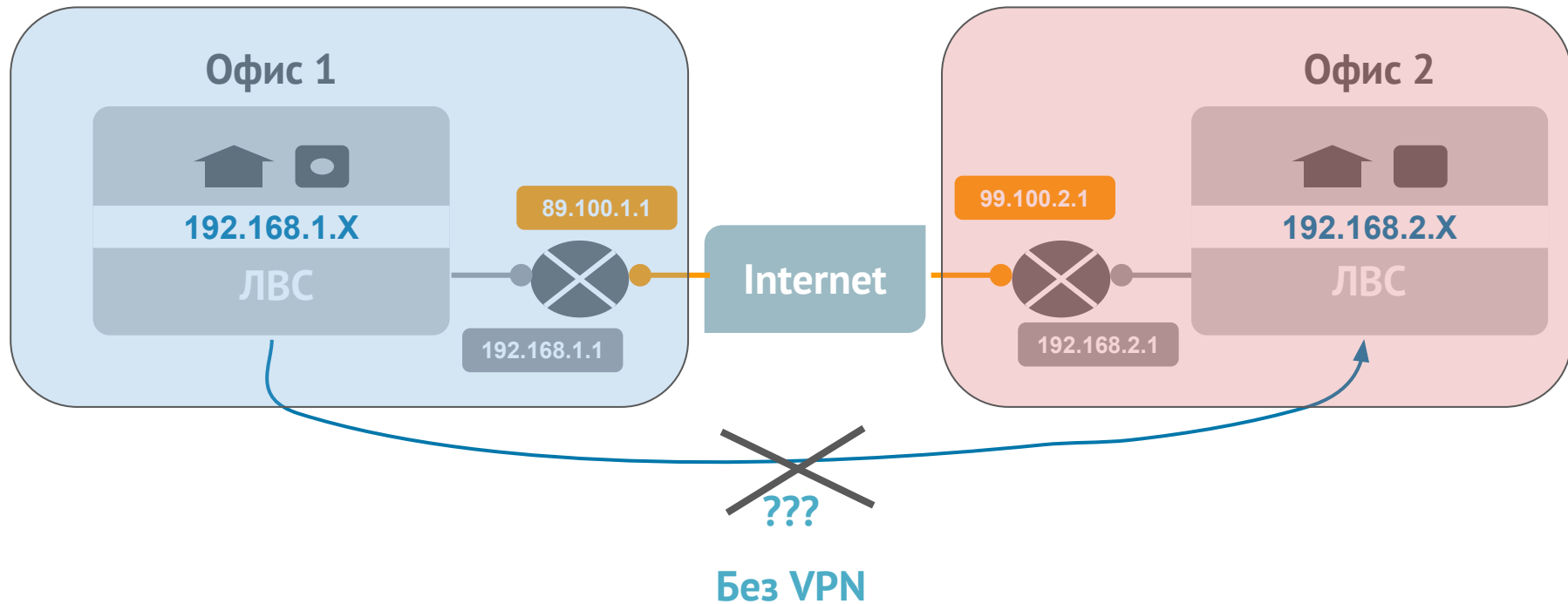
Частный IP-адрес



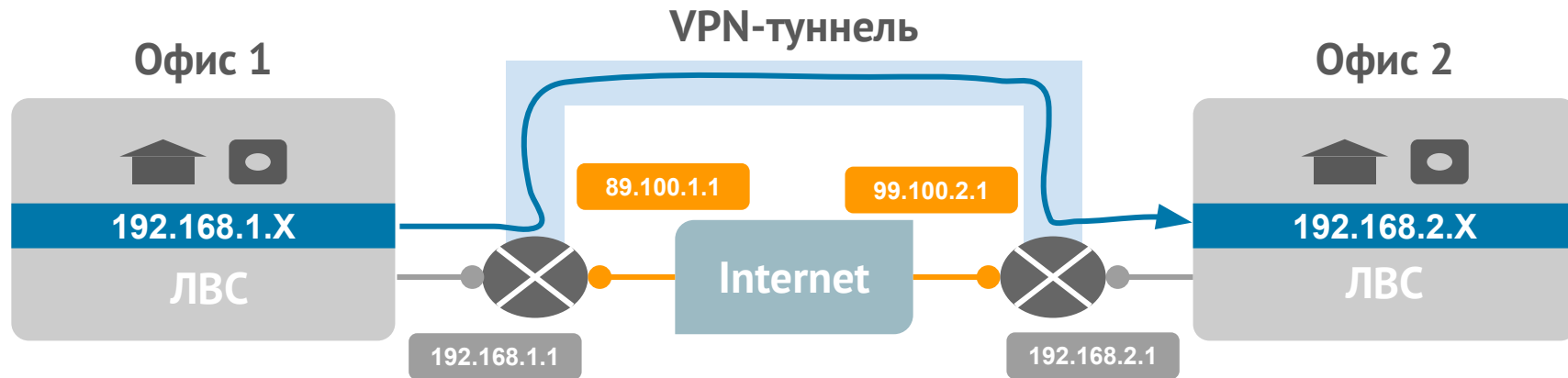


Как объединить несколько частных адресов в одну сеть, используя только сети общего доступа?

Без использования VPN



При использовании VPN



Дословный перевод VPN

Virtual Private Network

Виртуальная частная
сеть



VPN

механизм, позволяющий настроить подключение устройств через сети общего доступа, так, как если бы они находились в одной (частной) сети



Зачем нужен VPN для компаний?

1

Полный контроль сети (private)

Задать жесткое соответствие
между IP адресом и
пользователем/устройством

2

Шифрование

Передавать данные в
зашифрованном виде, повышая
безопасность передаваемых
данных

Зачем нужен VPN для компаний?

3

Единая адресация, разграничение доступа

Разграничить доступ к
внутренним ресурсам
основываясь только на
L3 адресах

4

Контроль действий сотрудников

На основе адресов можно вести
статистику запросов с привязкой
к пользователю

Зачем нужен VPN для компаний?

5

Соккрытие / маскировка реального IP-адреса

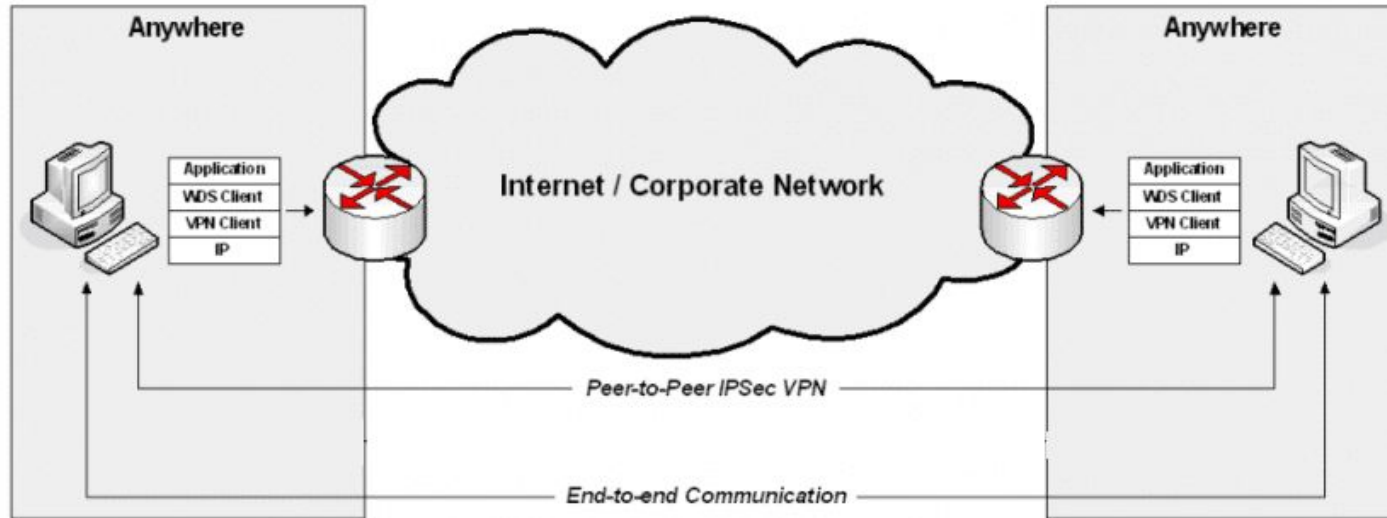
Анонимность запросов,
обезличивание как защита от
неправомерных действий через
социальную инженерию

6

Доступ к заблокированным ресурсам

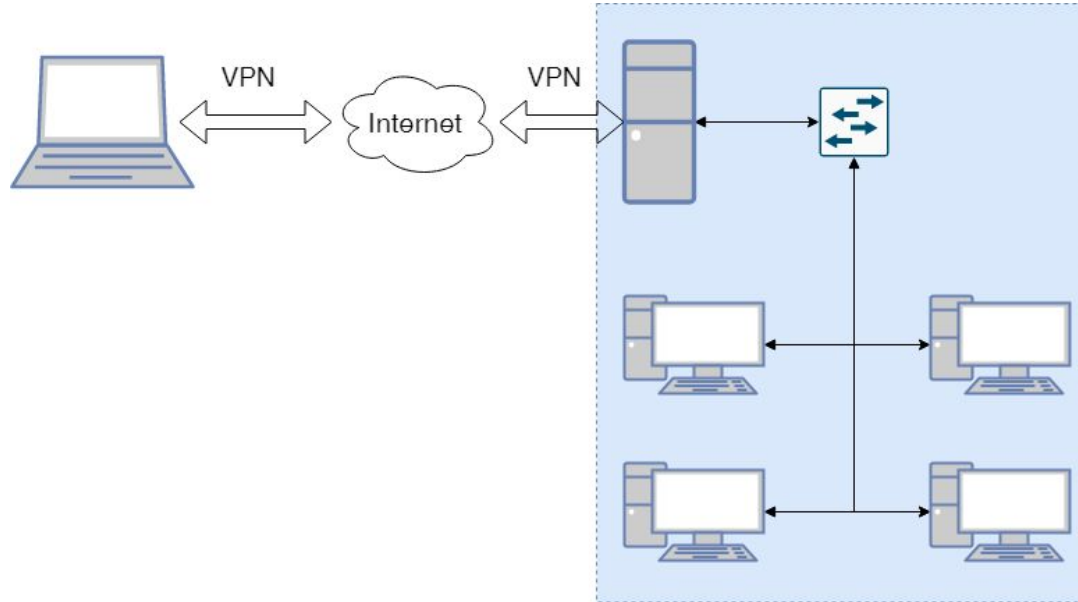
Обеспечить доступ к недоступным
по региональному признаку
ресурсу

Виды VPN: Точка - точка (Point-to-Point)



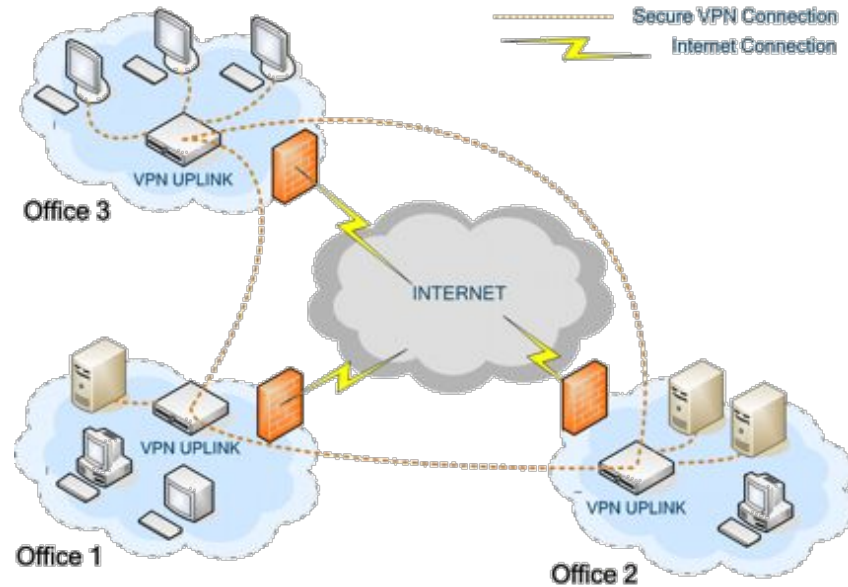
Объединение 2-х серверов

Виды VPN: Точка - Сеть (Remote Access)



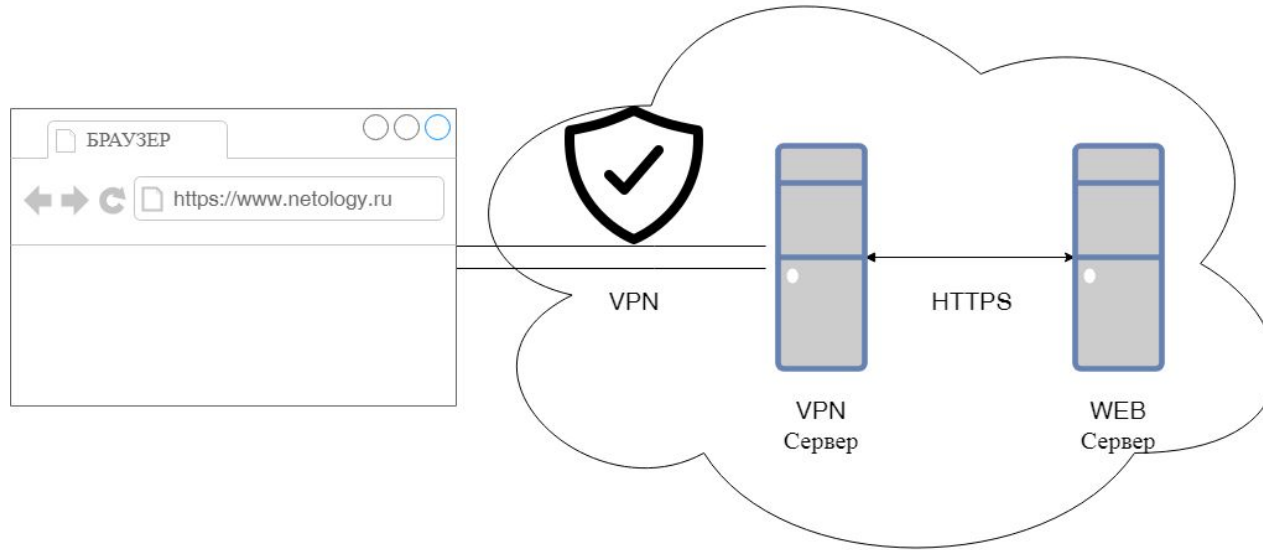
Подключение из дома к рабочей сети

Виды VPN: Сеть - сеть (Site-to-Site)



Объединение нескольких офисов в одну сеть

Виды VPN: VPN-сервис в браузере



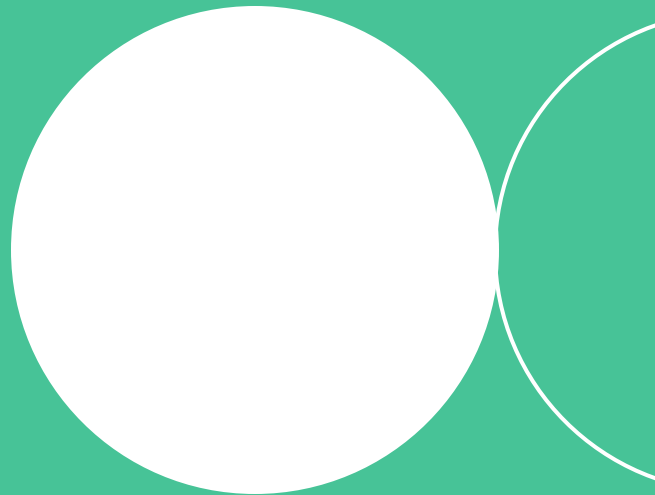
Маскировка IP-адреса

Итоги темы

- 1 Технология VPN появилась во второй половине 90-х гг. и с тех пор активно совершенствуется и развивается
- 2 Для компаний использование VPN помимо связи с удаленными сотрудниками, позволяет также упростить контроль за всеми пользователями
- 3 Для подключения удаленных сотрудников чаще используется Peer-to-Site (по другому Remote Access). Для подключения филиальных сетей – Site-to-Site

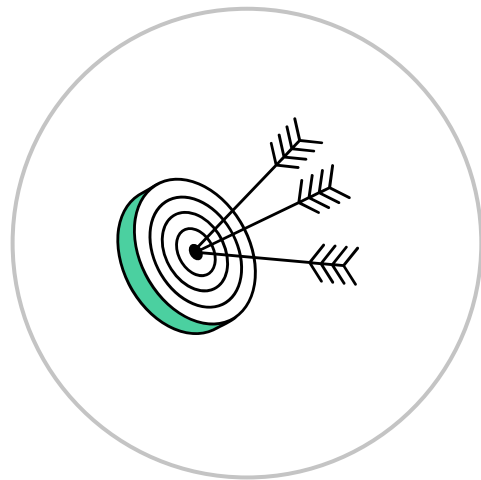


VPN Point-to-Point



Цели темы

- Познакомиться с видом соединения VPN точка-точка
- Понять для чего применяется такое соединение
- Узнать об особенностях реализации такого VPN



Все названия VPN Point-to-Point



point-to-point

p2p

точка-точка

VPN Point-to-Point

**используются для соединения
между собой двух устройств**

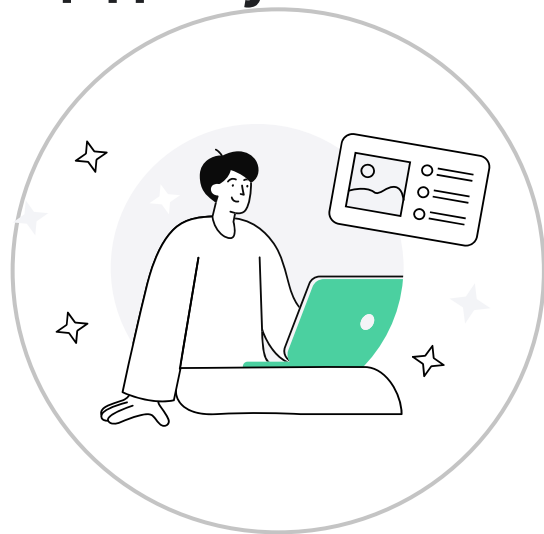
Пример





VPN-туннель

зашифрованное подключение между двумя точками,
VPN клиентом и VPN сервером, через общедоступные
сети



Пример VPN Point-to-Point



Для защиты информации на всех уровнях от целенаправленной компрометации со стороны сотрудников

Настройки VPN Point-to-Point

На одном устройстве настроить серверную часть VPN, другое устройство в роли клиента

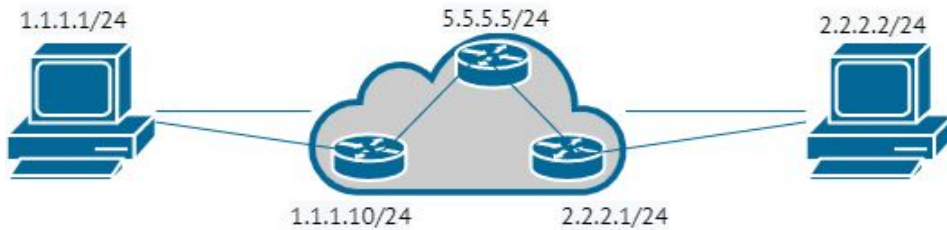
Настройки должны выполняться с повышенными правами, так как в процессе добавляется виртуальный сетевой интерфейс, через который будет происходить взаимодействие

При взаимодействии все реальные промежуточные узлы будут скрыты

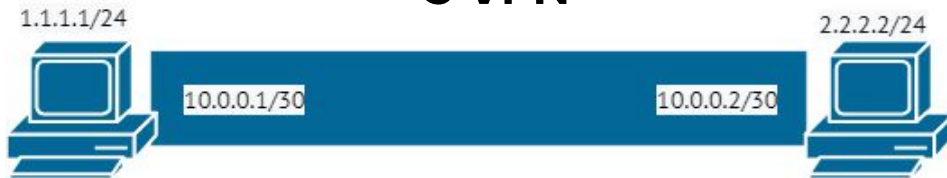
VPN Point-to-Point

При взаимодействии все реальные промежуточные узлы будут скрыты

Без VPN



С VPN

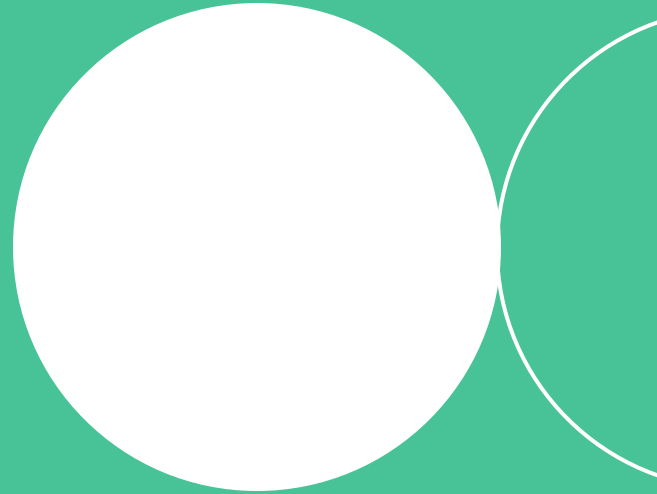


Итоги темы

- 1 Соединение точка-точка применимо когда вы хотите передавать обезличенную зашифрованную информацию между двумя адресами в общедоступных или локальных сетях
- 2 Создание туннеля требует наличие повышенных прав на обеих машинах
- 3 С точки зрения обеих машин они будут соединены напрямую, без промежуточных узлов

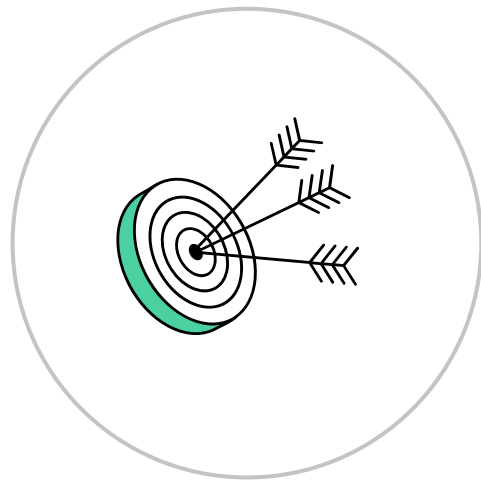


VPN Remote access

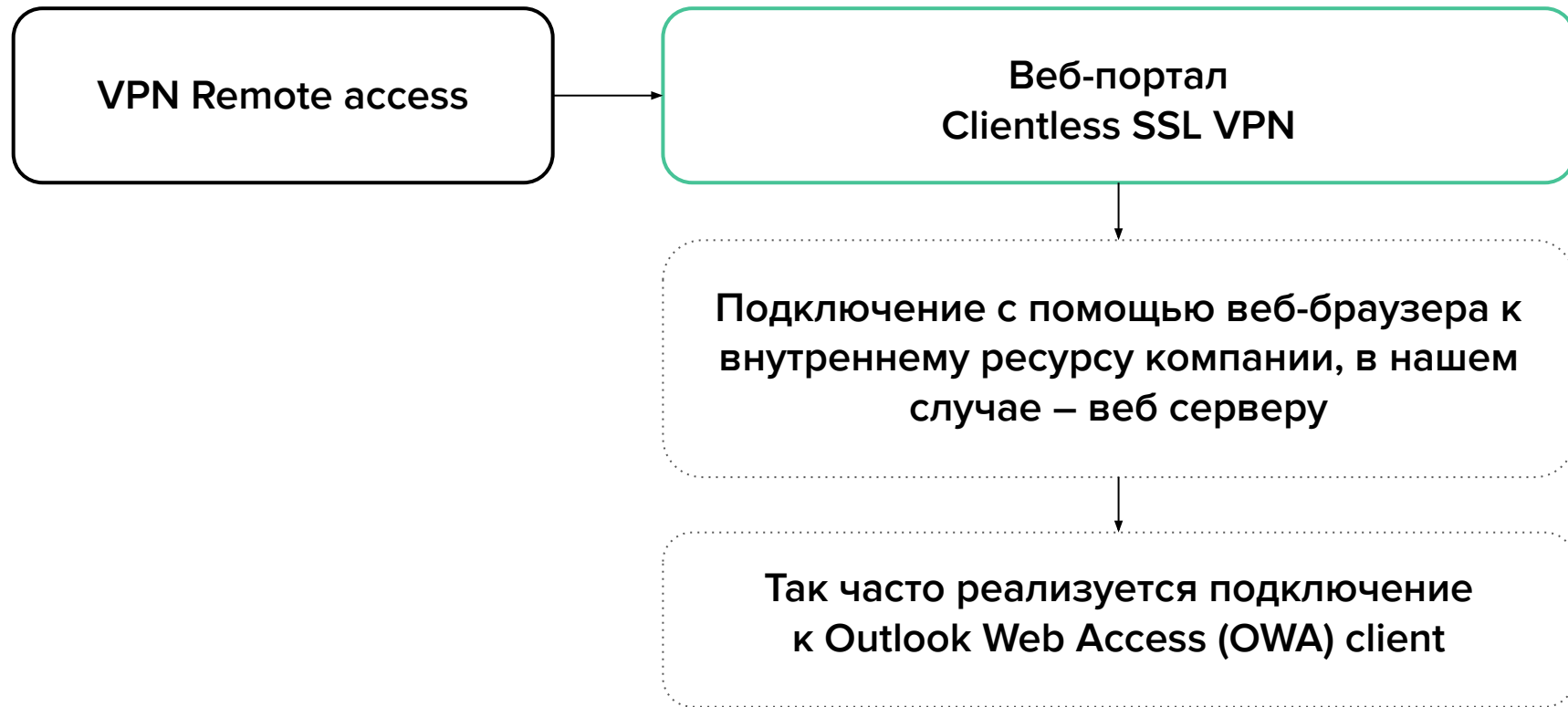


Цели темы

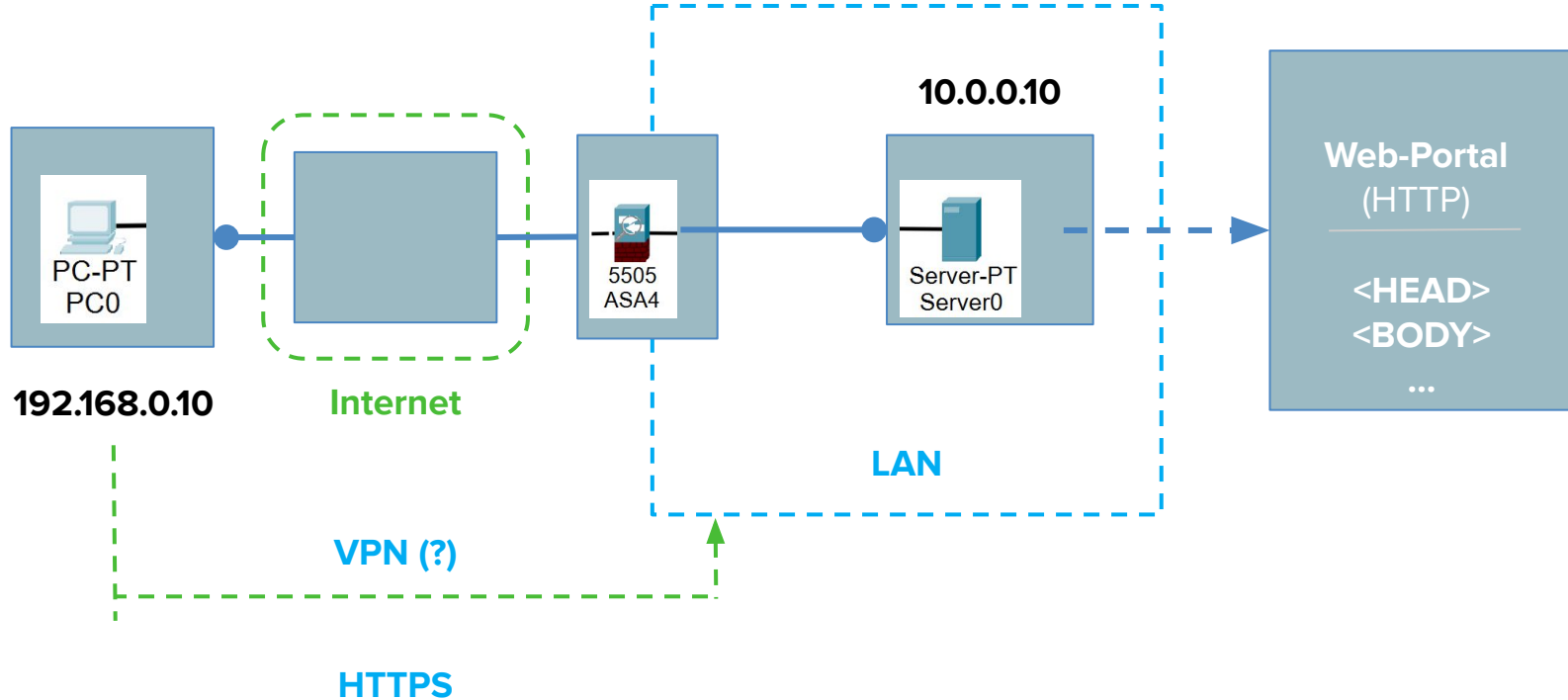
- Узнать о виде соединения VPN точка-сеть (Remote Access)
- Научиться определять ситуации, когда применима такая архитектура
- Разобраться с особенностями реализации соединения



Простой вид VPN Remote access



Clientless SSL VPN





Clientless SSL VPN

веб-портал позволяет предоставить доступ к внутренним веб-ресурсам, терминальным и SSH-серверам компании для удаленных или мобильных пользователей, используя защищенное HTTPS-соединение веб-браузера



Требования для Clientless SSL VPN

Специальное
оборудование,
поддерживающее
данный режим

либо

Настройка
отдельного сервера

Вендоры Clientless SSL VPN



Cisco

Palo Alto

UserGate

и другие

Настройка Clientless SSL VPN

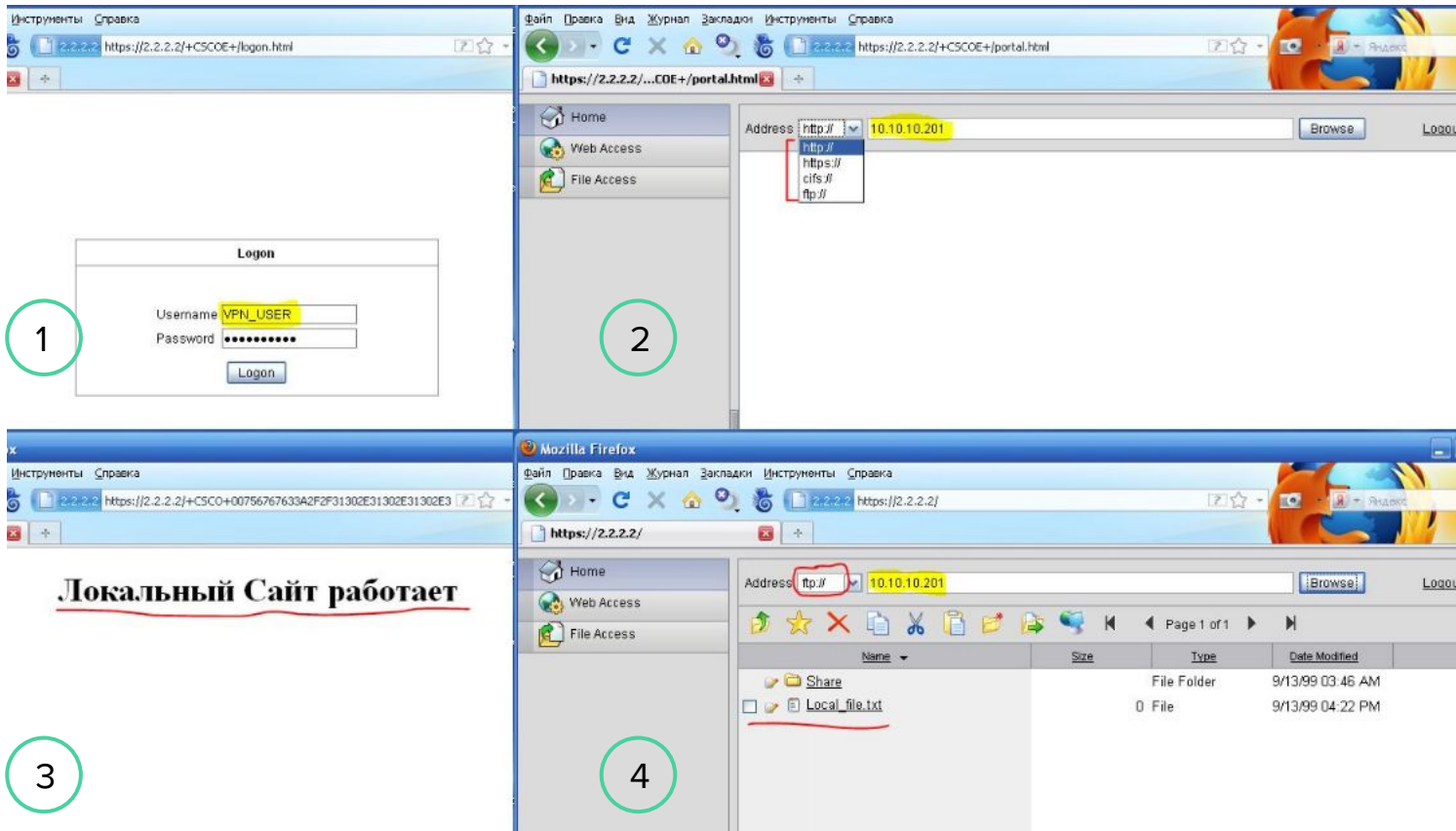
Создать
профиль
подключения
(пользователя,
группы, методы
авторизации,
пароли и т.д)

Указать при
необходимости
варианты 2-
факторной
авторизации
(OTP/SMS/Email)

Указать
доступные
ресурсы
локальной сети

Настроить
портал
(указать DNS
имя, порт, SSL
сертификат)

Clientless SSL VPN



Популярный корпоративный VPN клиент

The logo for Cisco Anyconnect VPN is centered within a white rounded rectangle with a thin black border. The text "Cisco Anyconnect" is in a teal color, and "VPN" is in a darker teal color below it.

Cisco Anyconnect
VPN

Подключение с помощью специального
ПО (VPN клиента) к VPN серверу
компании с использованием
шифрования и авторизации

Авторизация VPN клиентов



The diagram consists of two large, empty circles with black outlines, positioned side-by-side. Each circle contains text in a teal color. Below each circle is a block of black text describing the authentication method.

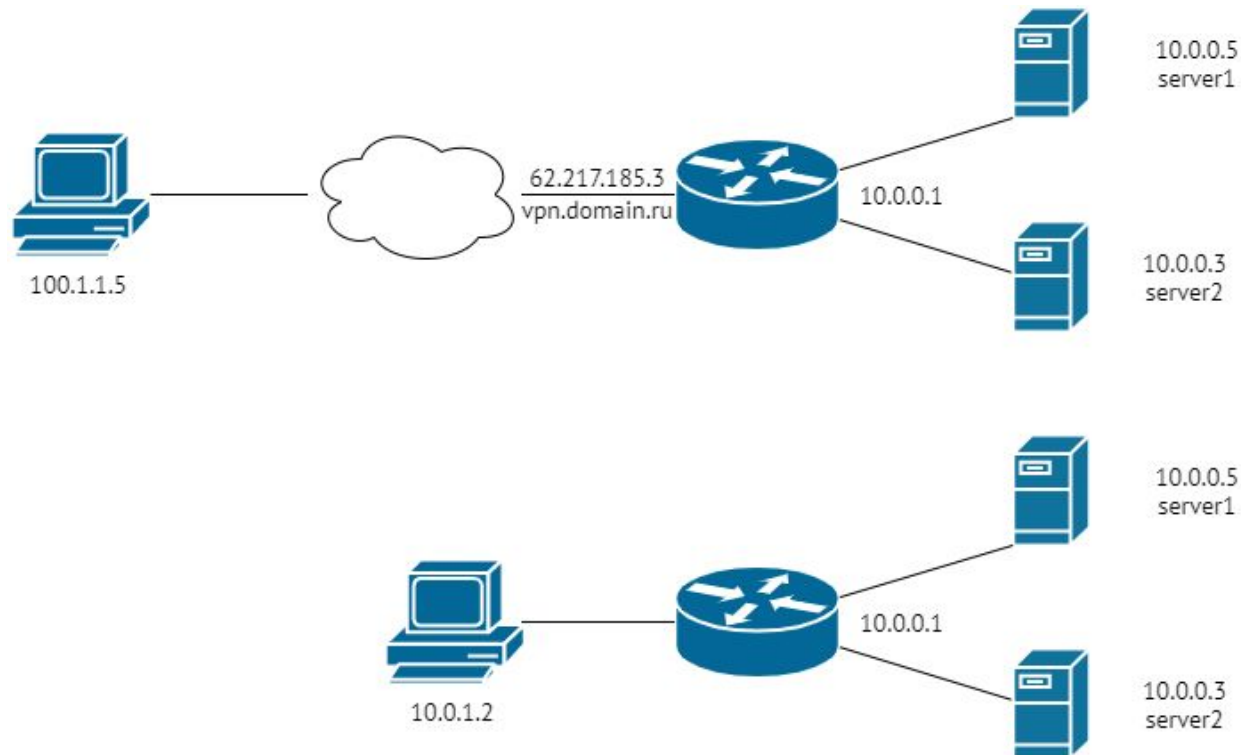
**Clientless SSL
VPN**

Использование одного
логина/пароля для авторизации
во все системы внутри сети

**Cisco Anyconnect
VPN**

Использование двухфакторной
аутентификации , с одноразовым
кодом для входа

SSL VPN Client

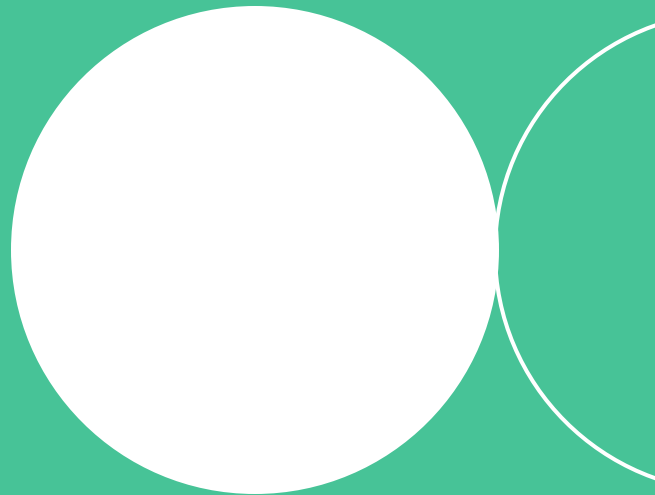


Итоги темы

- 1 Удаленный доступ отдельного хоста к локальной сети через VPN Remote access можно организовать двумя способами: без или с использованием специального клиента
- 2 Clientless VPN удобен тем, что не требует наличия специальной настройки или программы у подключающегося, но требует поддержки на серверной стороне и ограничивает доступные сервисы сети
- 3 При использовании специальных клиентских приложений достигается полное включение удаленного хоста в локальную сеть со всей доступностью сервисов

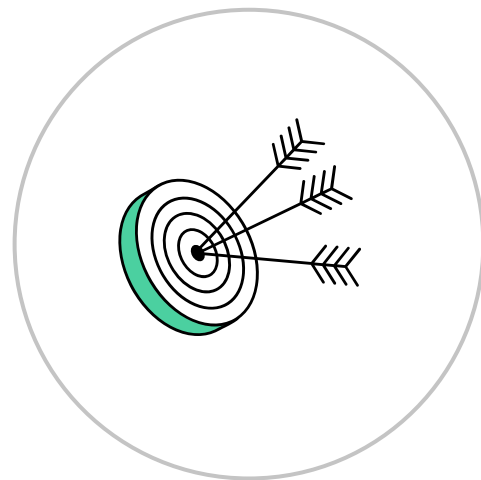


VPN Site-to-Site



Цели темы

- Познакомиться с соединением VPN сеть-сеть (Site to site)
- Узнать об особенностях применения
- Рассказать о видах “Провайдерского VPN”



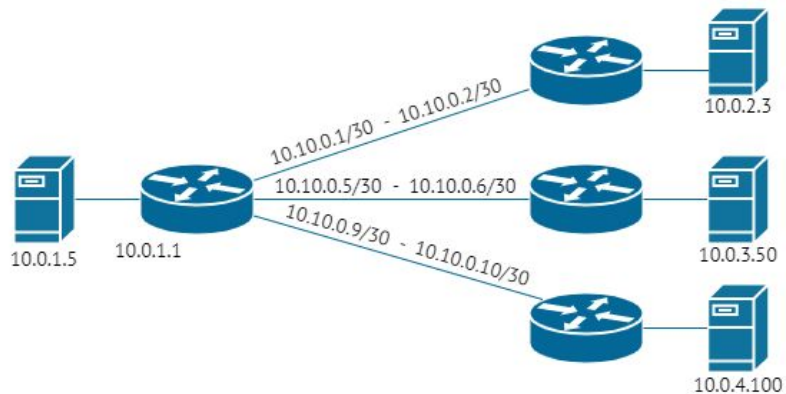
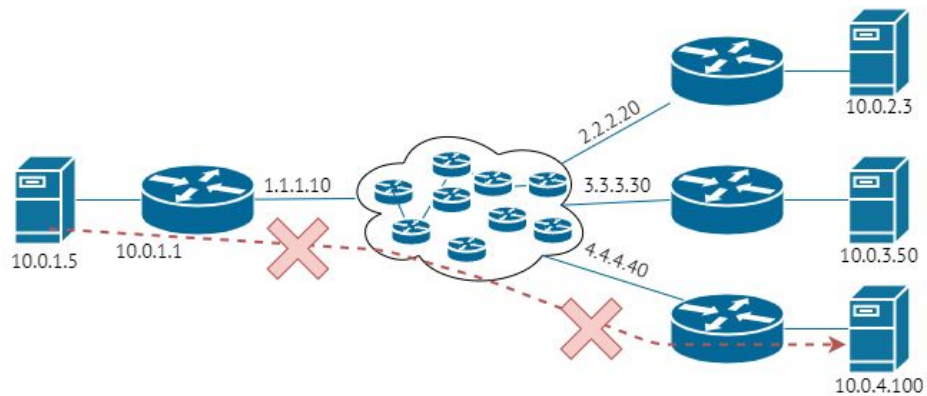
VPN Site-to-Site

**используются для объединения
удалённых офисов через
публичную сеть интернет**



Для конечных пользователей VPN выглядит прозрачным, при трассировке никаких «белых» IP-адресов никто не увидит

VPN Site-to-Site





**В чем разница между
L2 VPN и L3 VPN?**

Провайдерские VPN

1

L2 VPN

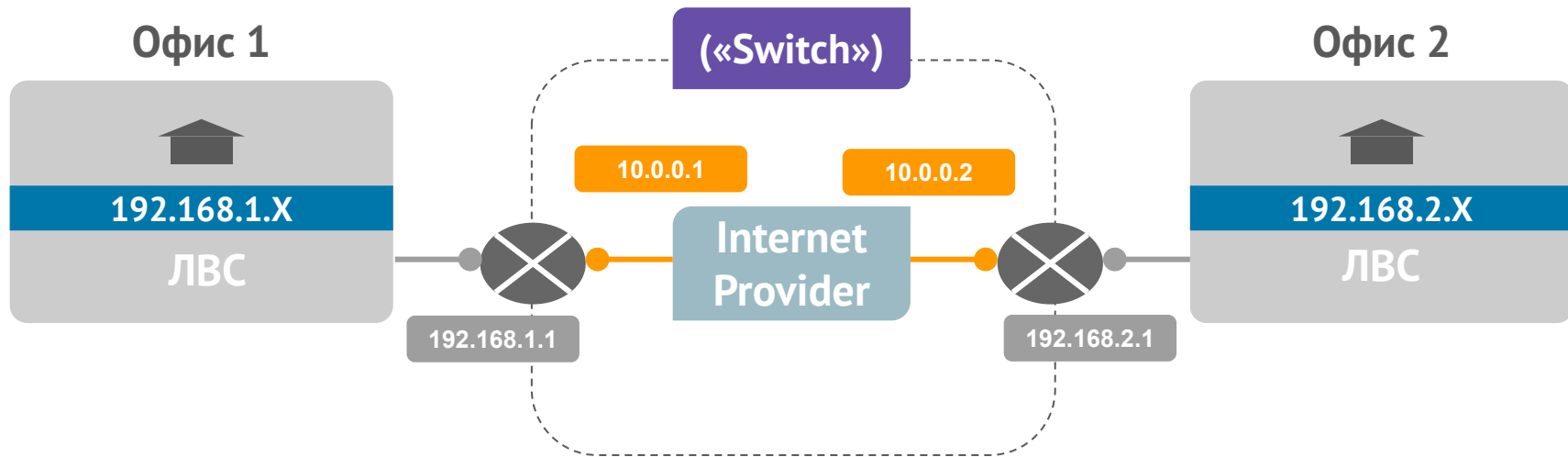
Провайдер предоставляет
«как-будто» коммутатор

2

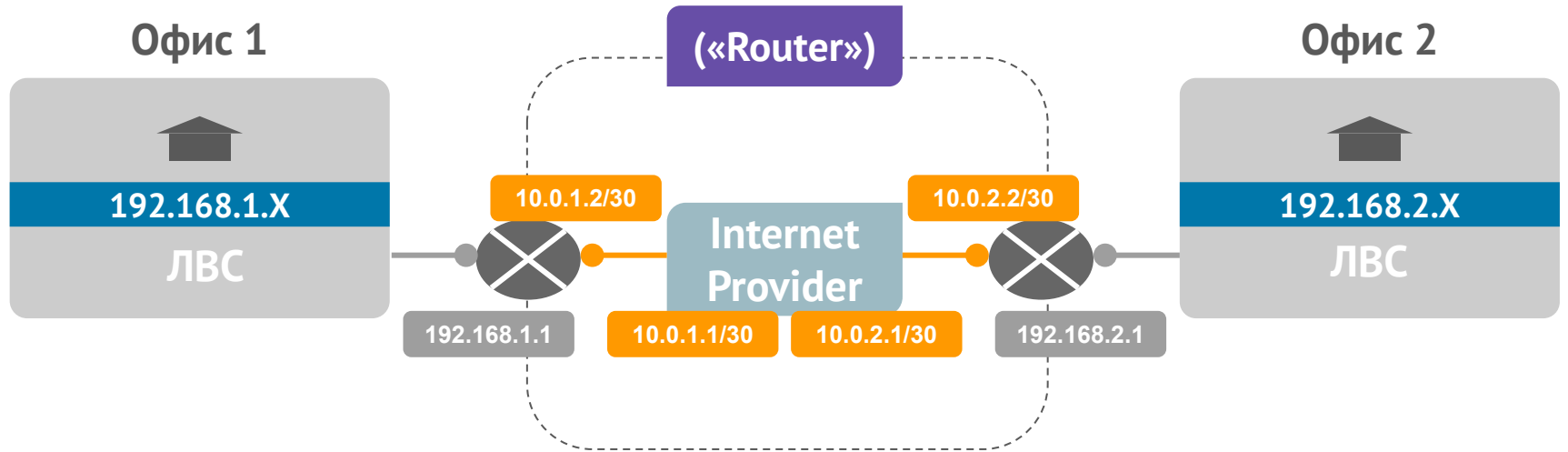
L3 VPN

Провайдер предоставляет
«как-будто» маршрутизатор

L2 VPN



L3 VPN

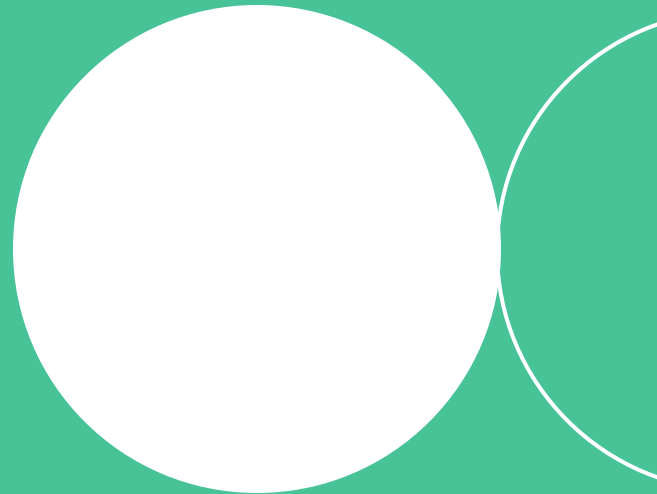


Итоги темы

- 1 Соединение VPN Site-to-Site используется для объединения в одну сеть территориально разнесенных подразделений
- 2 Основной принцип остается неизменным: виртуальный тоннель устанавливается между двумя точками, которые выполняют роль шлюзов для своих сегментов сети
- 3 Услуги объединения офисов может предлагать и провайдер с помощью L2 и L3 VPN. Даже в таком случае рекомендуется передавать данные между сетями в зашифрованном виде по VPN туннелю

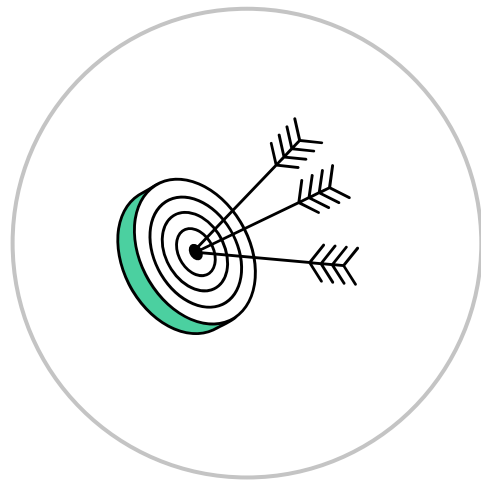


VPN протоколы



Цели темы

- Обзорно узнать о различных VPN протоколах
- Познакомиться с особенностями работы и реализации этих протоколов
- Научиться понимать какой протокол необходим в тех или иных случаях



VPN протоколы

PPTP

**Point-to-Point
Tunneling Protocol**

L2TP / IPSec

**Layer 2 Tunneling
Protocol /
IP Security**

SSTP

**Secure Socket
Tunneling Protocol**

WireGuard

OpenVPN




PPTR


туннельный протокол типа точка-точка, позволяющий компьютеру устанавливать защищённое соединение с сервером за счёт создания специального туннеля в стандартной, незащищённой сети



RTP



**Работает на
L4 уровне,
поверх TCP**



**Предоставляет
сервисы L2
уровня**

Как работает PPTP?



Какие особенности PPTP?

Несмотря на относительно высокую скорость, PPTP не слишком надежен: после обрыва соединения он не восстанавливается так же быстро, как, например, OpenVPN

В настоящее время PPTP по существу устарел и Microsoft советует пользоваться другими VPN решениями, так как обладает серьёзными уязвимостями

Мы также не советуем выбирать PPTP, если для вас важна безопасность и конфиденциальность



L2TP

**протокол туннелирования второго уровня,
используется для поддержки виртуальных частных
сетей**



L2TP



**Работает на
L4 уровне,
поверх UDP**

**Предоставляет
сервисы L2
уровня**

Протокол L2TP

**при передачи данных по
туннелю L2TP кадр L2TP
помещается в дейтаграмму
UDP и пересылается
конечной точке**

Какие особенности L2TP?

L2TP / IPsec считается безопасным и не имеет серьезных выявленных проблем (гораздо безопаснее, чем PPTP)

L2TP / IPsec может использовать шифрование 3DES или AES, хотя, учитывая, что 3DES в настоящее время считается слабым шифром, он используется редко

У протокола L2TP иногда возникают проблемы из-за использования по умолчанию UDP-порта 500, который иногда блокируется брандмауэрами

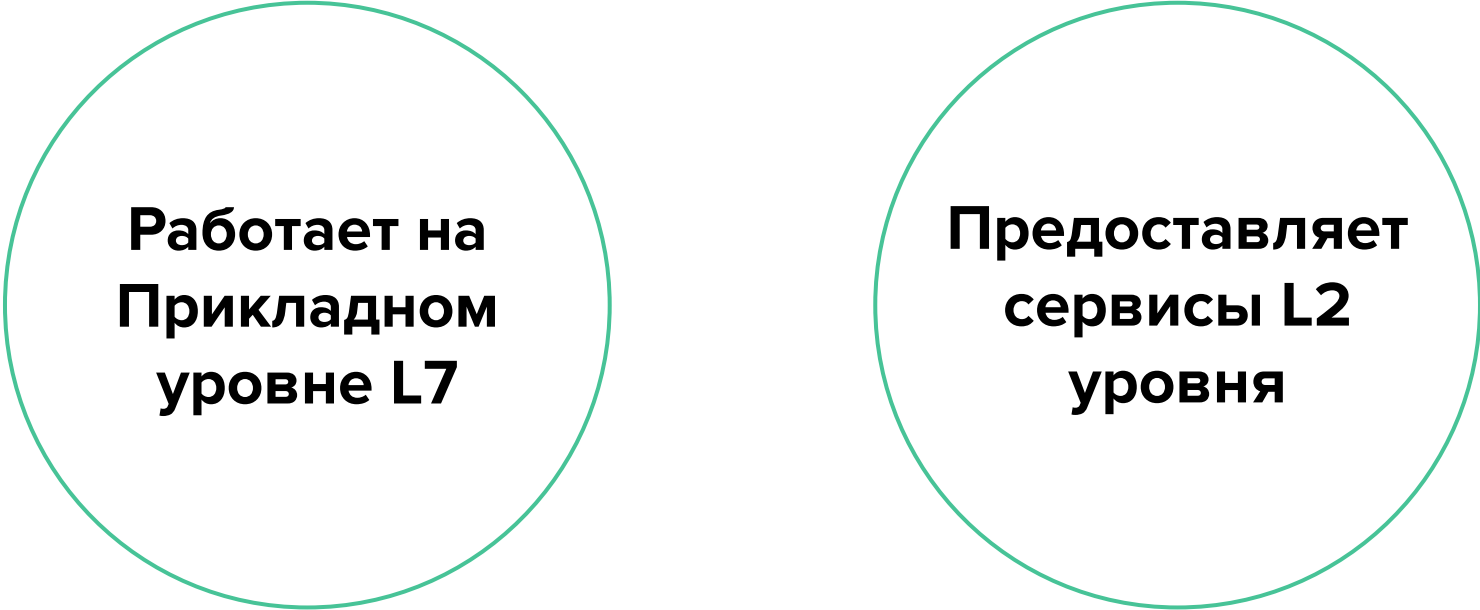


SSTP

**безопасный протокол туннелирования сокетов,
проприетарный продукт от Microsoft**



SSTP



**Работает на
Прикладном
уровне L7**

**Предоставляет
сервисы L2
уровня**



Протокол SSTP
отправляет трафик по SSL
через TCP-порт 443

Какие особенности SSTP?

Как и PPTP не очень широко используется в VPN, но, в отличие от PPTP, у него не диагностированы серьезные проблемы с безопасностью

SSTP удобен для использования в ограниченных сетевых ситуациях, например, если вам нужен VPN для Китая

Несмотря на то, что SSTP также доступен и на Linux, RouterOS и SEIL, по большей части он все равно используется Windows-системами



WireGuard


коммуникационный протокол и бесплатное программное обеспечение с открытым исходным кодом, который реализует зашифрованные виртуальные частные сети



WireGuard



**Работает
поверх L4
(UDP)**



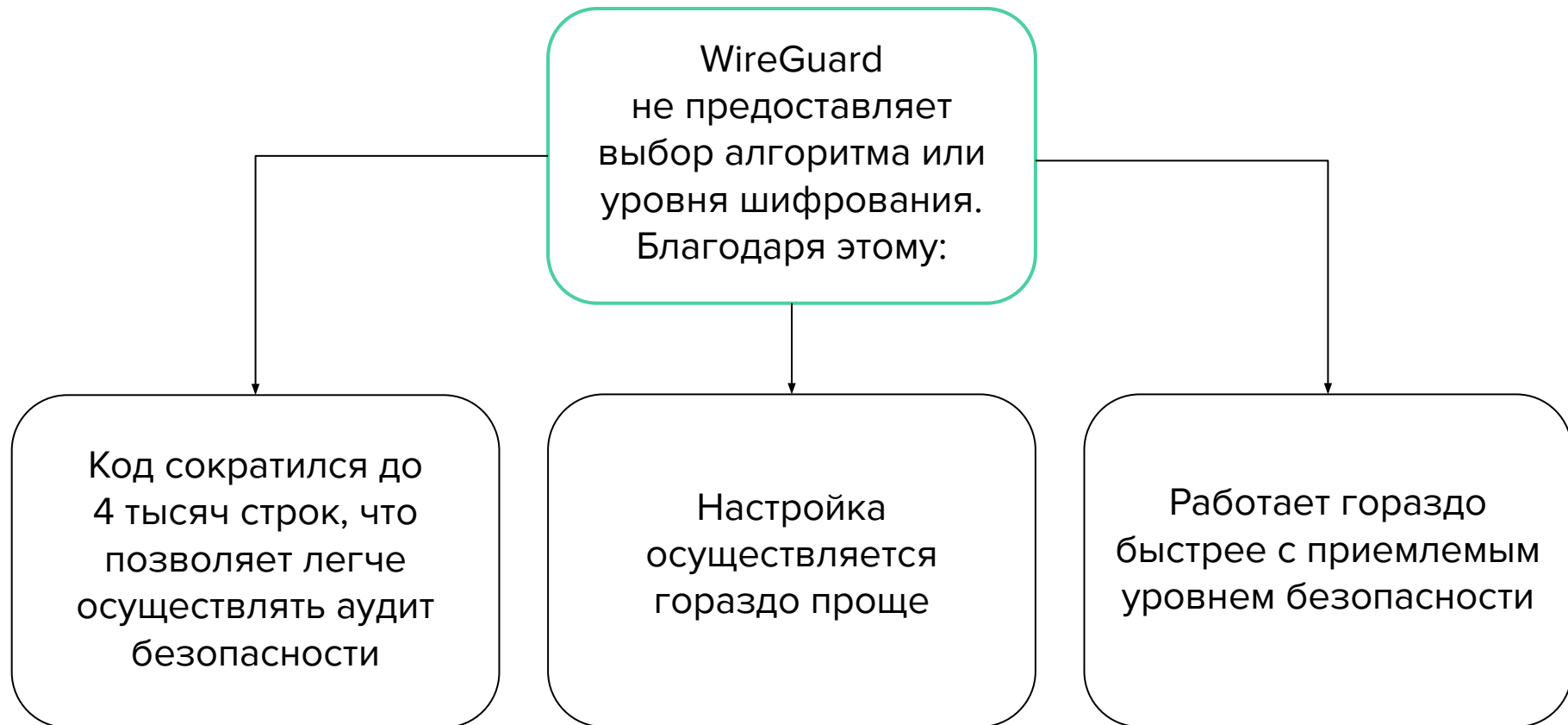
**Предоставляет
сервисы L2
уровня**

The logo for WireGuard, featuring the word "WireGuard" in a green, sans-serif font. The background of the slide consists of three large, light gray circles that overlap each other, creating a pattern of lens shapes.

WireGuard

**один из новейших VPN
протоколов, распространяется
по GNU GPL**

Какие особенности WireGuard?



Какие особенности WireGuard?

В Linux системах реализован в виде модуля ядра, что дополнительно увеличивает производительность

Протокол может работать на любом из портов UDP, существуют клиенты под все основные платформы: Windows, Mac OS, Linux, Apple iOS, Android




OpenVPN

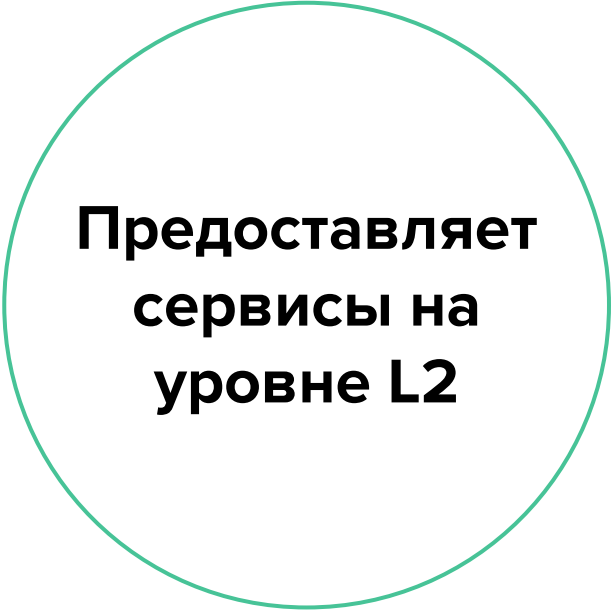
универсальный протокол VPN с открытым исходным кодом, разработанный компанией
OpenVPN Technologies



OpenVPN



**Работает на L4
уровне, поверх
TCP и UDP**



**Предоставляет
сервисы на
уровне L2**

OpenVPN

**самый популярный протокол
VPN. Будучи открытым
стандартом, он прошел не одну
независимую экспертизу
безопасности**



OpenVPN использует библиотеку OpenSSL для шифрования и аутентификации, большинство VPN-сервисов создают свои приложения для работы с OpenVPN, которые можно использовать в разных операционных системах и устройствах

Какие особенности OpenVPN?

Для работы OpenVPN
нужно специальное
клиентское
программное
обеспечение

OpenVPN является
альтернативой IPsec
тогда, когда провайдер
блокирует некоторые
протоколы VPN

Протокол может
работать на любом из
портов TCP и UDP и
может использоваться
на всех основных
платформах через
сторонние клиенты:
Windows, Mac OS, Linux,
Apple iOS, Android

Как настроить OpenVPN?



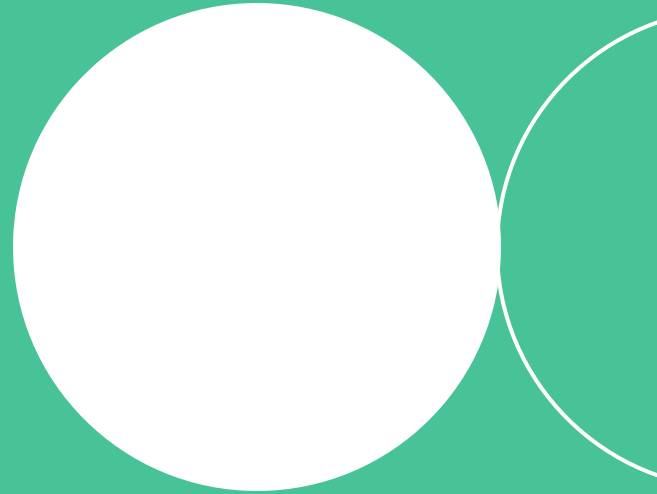
Пример
настройки
OpenVPN

Итоги темы

- 1 Старейшим протоколом VPN является PPTP, в настоящее время не используется из-за ненадежности соединения и большого количества уязвимостей
- 2 Большинство современных протоколов (OpenVPN, WireGuard) могут работать на любом порту UDP (и TCP для OpenVPN).
- 3 Протокол SSTP работает на 443 порту TCP, который используется так же для HTTPS соединений

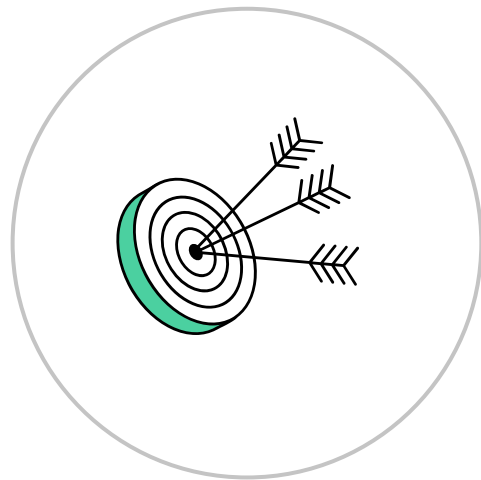


IPsec



Цели темы

- Познакомиться с протоколом IPSec
- Разобраться с режимами работы, особенностями реализации протокола
- Понять алгоритм работы протокола





IPSec

стек сетевых протоколов для защищенной передачи данных через IP-сети



IPsec обеспечивает

Аутентификацию

Шифрование

Проверку целостности
передаваемых данных

IPsec

Описание стека IPsec
занимает 12 документов RFC



[RFC 2401 – RFC 2412](#)

Режимы IPsec

1

Транспортный режим

Работает поверх протокола IP и шифрует содержимое IP-пакета (payload)

2

Туннельный режим

Создает новый IP-пакет, полностью шифруя исходный

Особенности режимов IPsec

Транспортный режим

↓

Адреса отправителя и получателя не шифруются, поэтому можно проанализировать адреса и объем переданной информации

Туннельный режим

↓

Использование туннельного режима сильно затрудняет анализ перехваченного трафика

Где используют режимы IPsec?

Транспортный режим



Чаще всего используется для
соединения между хостами

Туннельный режим



Чаще всего используется для
передачи данных через
Интернет



Туннелирование (tunneling)

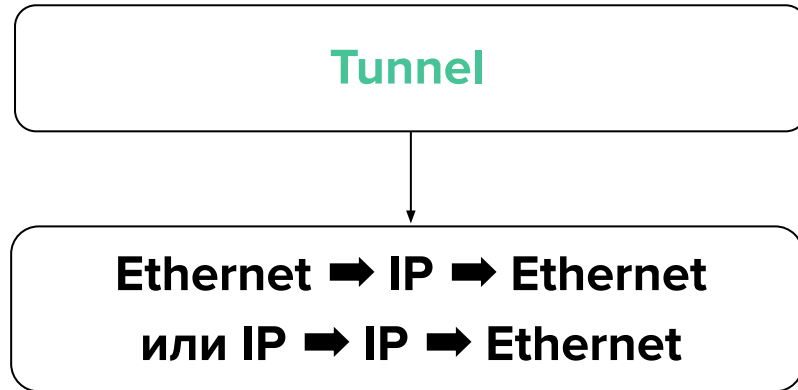
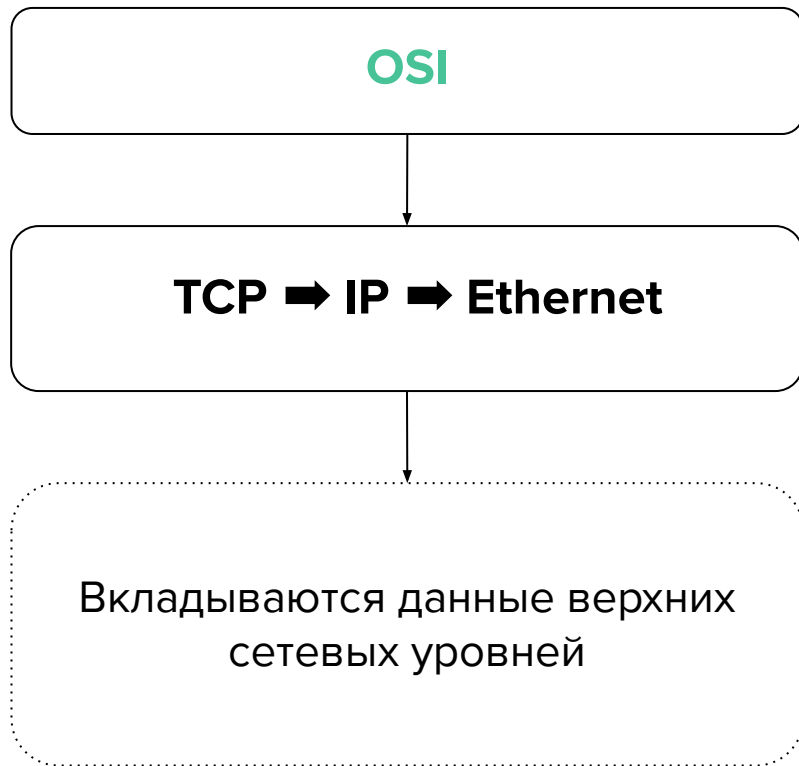
метод, используемый для передачи полезной нагрузки (кадра или пакета) одного протокола с использованием межсетевой инфраструктуры другого протокола



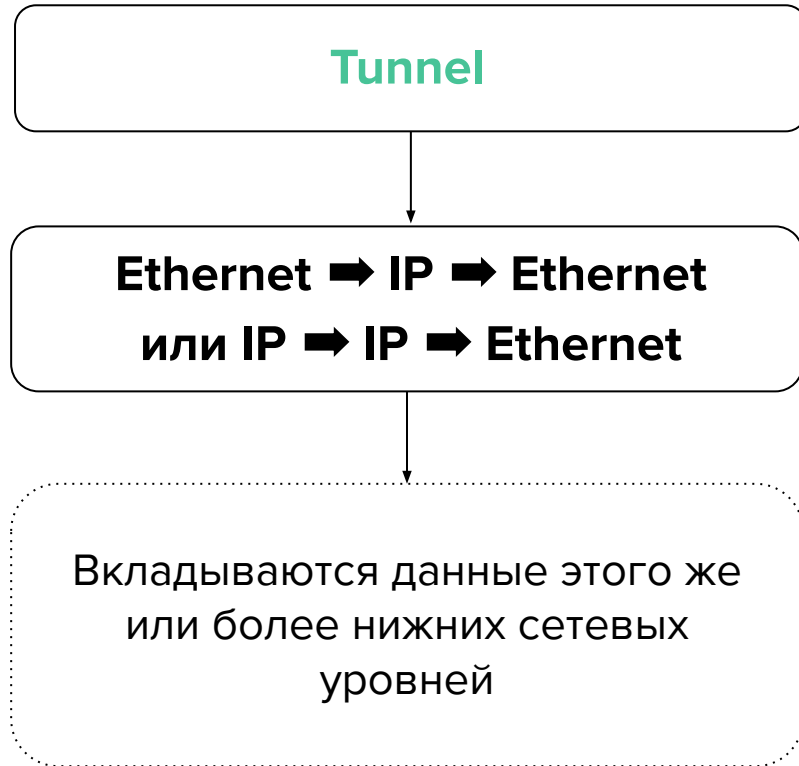
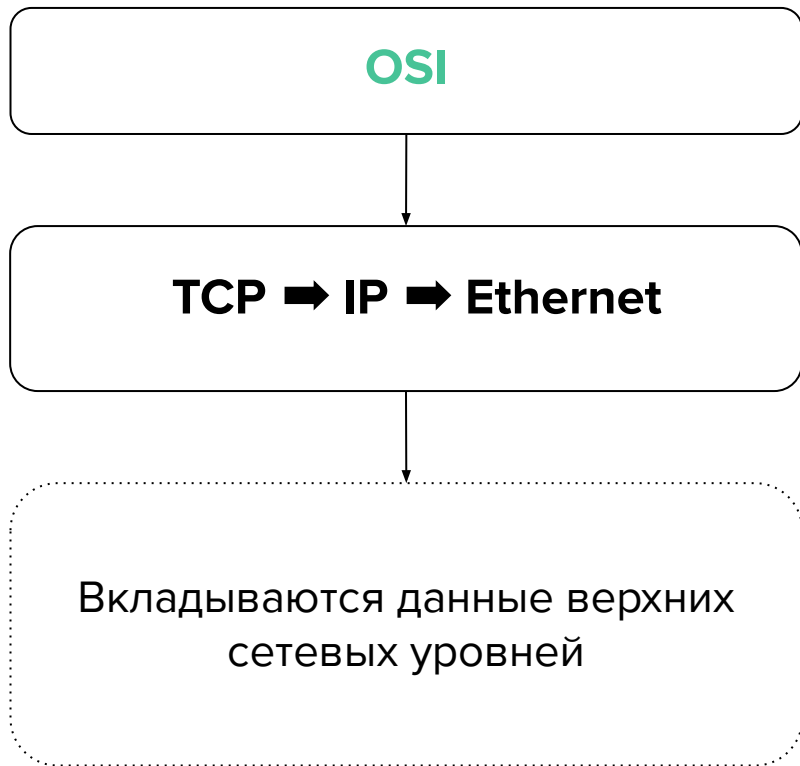


**Инкапсуляция в
Tunnel и в Model OSI,
в чём разница?**

Инкапсуляция в Tunnel и в Model OSI



Инкапсуляция в Tunnel и в Model OSI



Дословный перевод SA

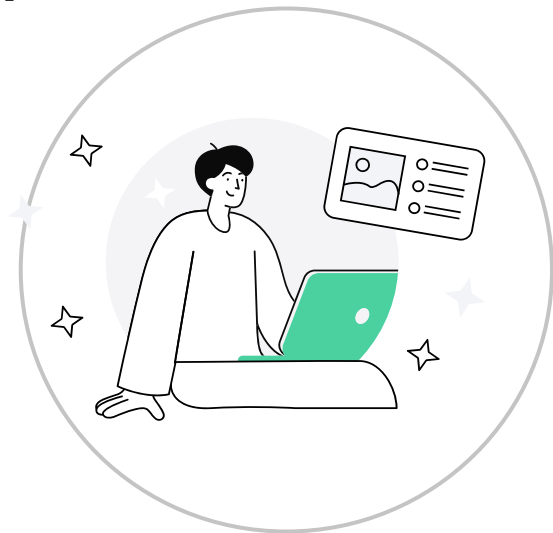
Security Association

Ассоциация
безопасности



Security Association

базовое понятие IPsec. Включает в себя информацию о криптографических протоколах и алгоритмах, ключах шифрования, определяет какие данные будут проходить через туннель



Security Association

Для создания SA
используется

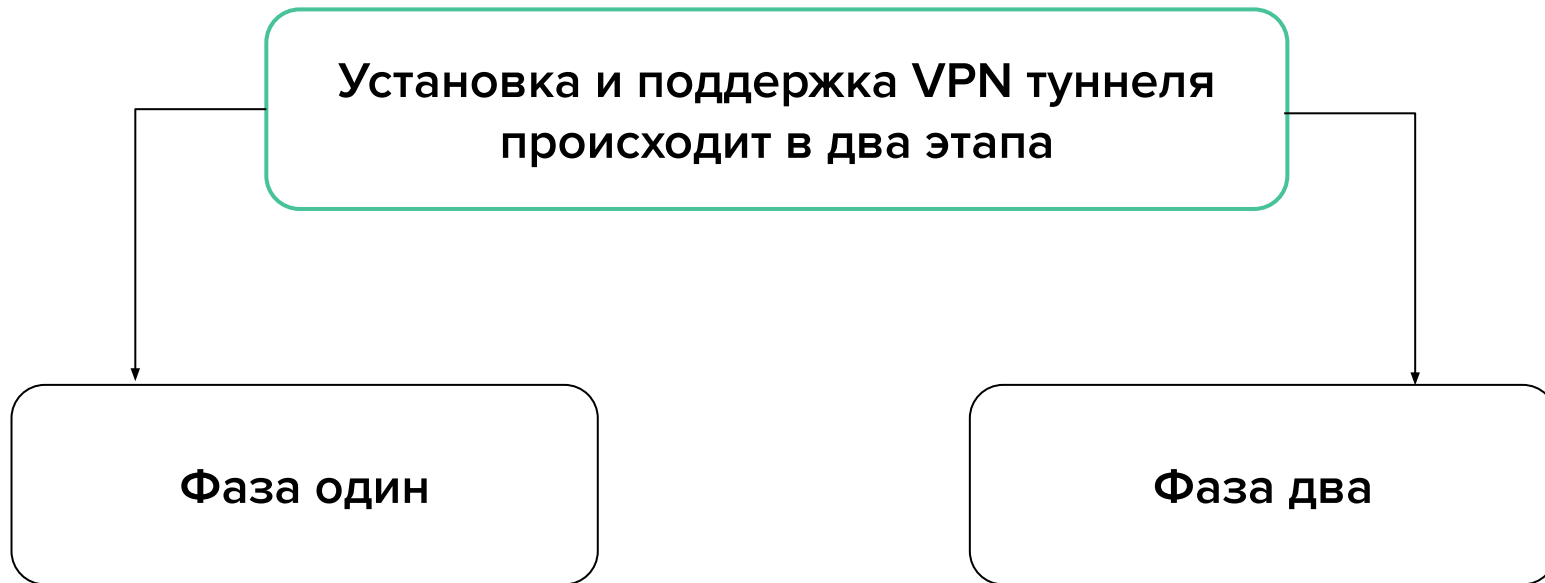
Internet Security Association and Key
Management Protocol (ISAKMP)

Для работы
с ключами

Протокол Internet Key Exchange (IKE)



Алгоритм работы IPsec



В фазе один, узлы договариваются о:

Методе идентификации

Алгоритме шифрования

Хэш алгоритме

Группе Diffie Hellman

Также происходит взаимная идентификация

**Если шаги в первой фазе
завершились успешно, то
создаётся SA первой Фазы
(Phase 1 SA или IKE SA)
и процесс переходит
к фазе два**

Алгоритм работы фазы два

В этой фазе генерируются ключи и узлы договариваются
об используемой политике

**Если вторая фаза
выполняется успешно,
то создается Phase 2 SA или
IPSec SA.**

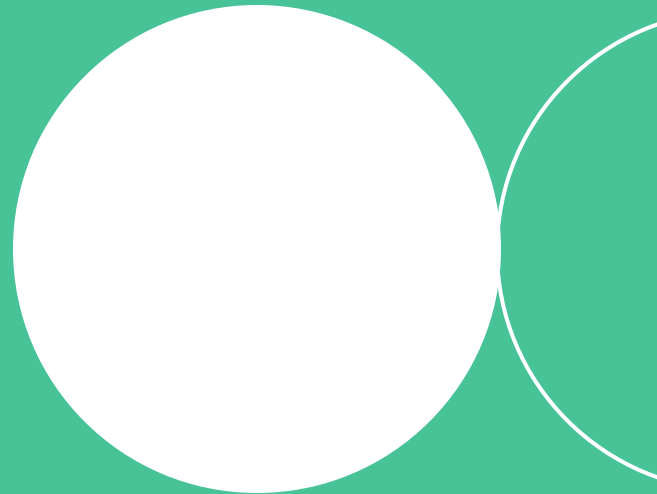
**На этом установка туннеля
считается завершенной**

Итоги темы

- 1 IPsec разработан IETF и включает 18 спецификаций RFC и позволяет осуществлять подтверждение подлинности, проверку целостности IP-пакетов, защищённый обмен ключами
- 2 IPsec работает на L3 уровне модели OSI и может работать в двух режимах: транспортном и туннельном
- 3 Установка туннеля происходит в две фазы: идентификация и согласование; генерация ключей и создание SA

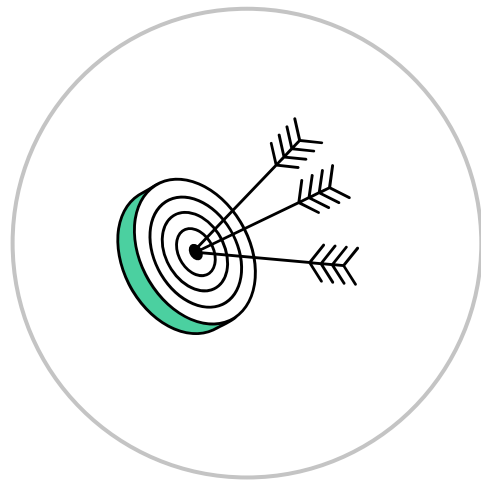


VPN сервисы



Цели темы

- Разобраться с различными существующими VPN сервисами
- Узнать об их особенностях и применении
- Понять риски информационной безопасности при их использовании



VPN сервисы

**Серверная часть не требует контроля
и предоставляется в качестве сервиса**

Реализация сервисов VPN

**На базе какого-либо
браузера
(плагин, аддон)**

или

**Быть отдельным клиентом,
влияя на сетевое
подключение**

Браузеры для безопасной и анонимной работы в сети Интернет



Opera

Epic Privacy
Browser

Google Chrome +
Browsec addon

TOR

Отдельные продукты VPN сервисов

Hotspot Shield

Betternet

(есть реклама, но бесплатная
версия работает хорошо)

**Kaspersky Secure
Connection**

Hola VPN

(много рекламы,
не рекомендуется к установке)

Вопросы безопасности VPN сервисов

- Установка клиента всегда требует повышенных привилегий, которые вы передаёте стороннему приложению
- У вас снижается контроль над потоком принимаемой или передаваемой информацией
- Некоторые сервисы могут критически снижать уровень безопасности. Так, например, в апреле 2022 года у 6 популярных VPN сервисов (Surfshark, Atlas VPN, VyprVPN, VPN Proxy Master, Sumrando VPN и Turbo VPN) была выявлена проблема установки доверенных корневых сертификатов
- Поддержание всякой VPN инфраструктуры, способной работать с большими нагрузками сопряжена с финансовыми затратами. Если же вам неочевидна схема заработка сервиса, то не стоит доверять им критически важную информацию

Итоги темы

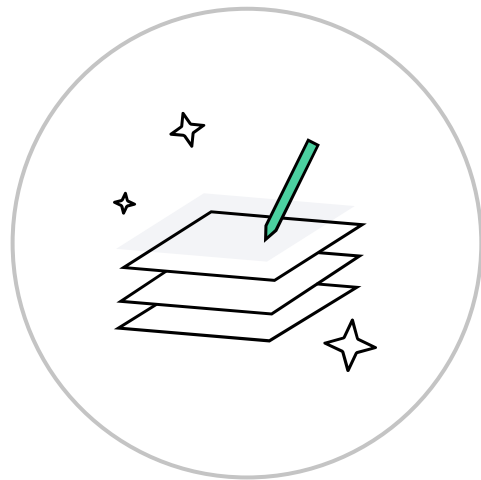
- 1 Удобство VPN сервисов заключается в простоте настройки и удобством пользования
- 2 Использование любого сервиса, где вы не контролируете всё прохождение информации сопряжено с рисками информационной безопасности
- 3 Необходимо всегда быть в курсе локальных законодательств, чтобы избежать возможных последствий



Домашнее задание

Давайте посмотрим вашу практику после лекции

- 1 Практика: домашнее задание (обязательное) с проверкой от преподавателя
- 2 Вопросы по домашнему заданию задавайте в чате учебной группы
- 3 Задачи можно сдавать по частям.
Зачёт по домашней работе ставят после того, как приняты все задачи



Задавайте вопросы. Оставляйте обратную связь по вебинару

Александр Гришин
Эксперт в области системного администрирования

