нетология

Сеть и сетевые протоколы: **VPN**

Андрей
Вахутинский

Андрей Вахутинский

Заместитель начальника IT-отдела

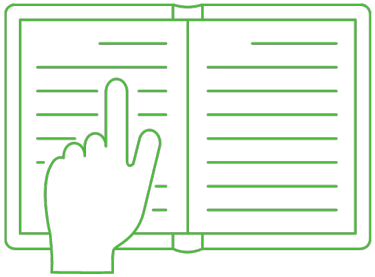
АО “ИНТЕКО”

Андрей Вахутинский

Предисловие

На этом занятии мы рассмотрим базовые концепции сетевых технологий, более полно познакомимся с технологиями удаленного доступа – VPN и IPsec:

- что такое VPN и туннель?
- какие существуют основные типы соединений?
- какие есть VPN протоколы?
- каковы режим, туннели, алгоритм работы IPsec?



План занятия

1. Предисловие
2. Использование VPN
3. VPN
4. Виды VPN
    - VPN Point-to-Point
    - VPN Remote access
    - VPN Site-to-Site
5. VPN протоколы
6. IPSec
7. VPN сервисы
8. Итоги
9. Домашнее задание

Использование VPN

VPN

OPENVPN

Check Point
SOFTWARE TECHNOLOGIES LTD.

infotecs
ViPNet

FORTINET

paloalto
NETWORKS

КОД безопасности
Континент 4

cisco

UserGate

КРИПТОПРО

Для чего используется VPN?

VPN

VPN (Virtual Private Network, виртуальная частная сеть) – механизм, позволяющий настроить подключение устройств через сети общего доступа, так, как если бы они находились в одной (частной) сети.

Использование VPN

Зачем нужен VPN для компаний:

- полный контроль сети (private);
- шифрование;
- единая адресация, разграничение доступа;
- контроль действий сотрудников.

Зачем нужен VPN для частных лиц:

- сокрытие / маскировка реального IP-адреса;
- доступ к заблокированным ресурсам.

VPN

Проблематика возникновения

Как мы помним из предыдущих лекций, компьютеру дома или на работе назначается частный IP-адрес.

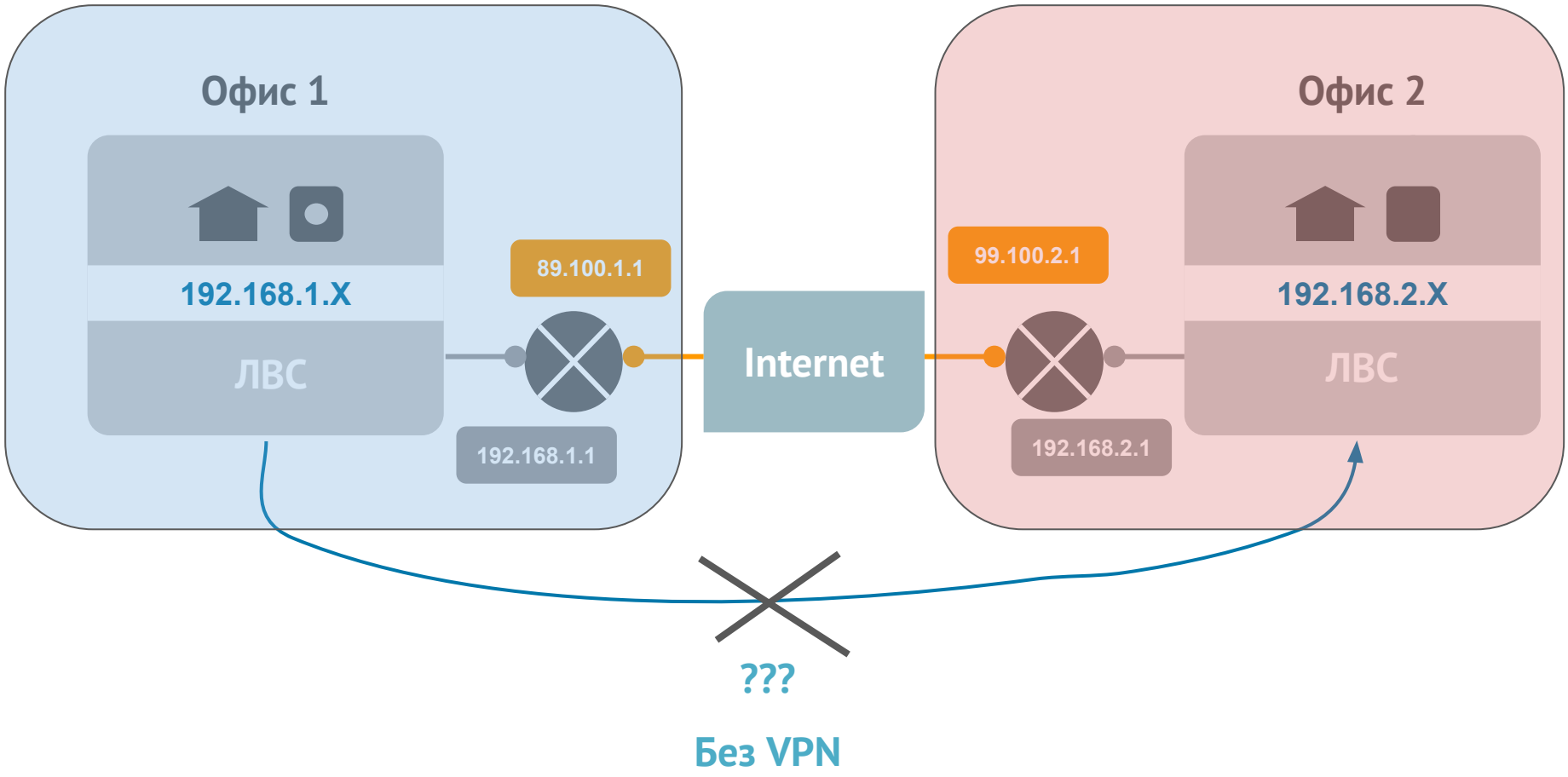
IP-адрес может использоваться только в локальных сетях и не может использоваться в сетях общего пользования.

В связи с эти возникает проблема:

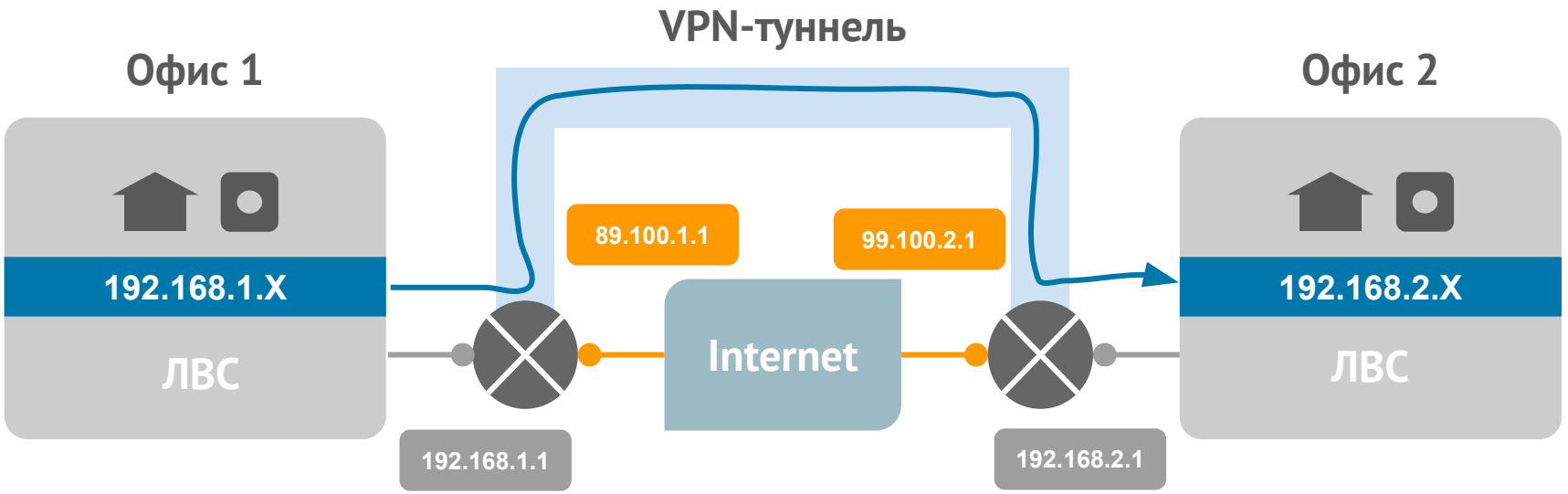
Как из дома получить доступ к сети на работе?

Другими словами, как объединить несколько частных адресов в одну сеть, используя только сети общего доступа (например, Интернет)?

Без использования VPN



При использовании VPN



Виды VPN

Виды VPN

- **Точка – точка** (Point-to-Point)
  Подключение двух устройств между собой. Например, объединение 2-х серверов.
- **Точка – сеть** (Remote Access)
  Подключение из дома к рабочей сети.
- **Сеть – сеть** (Site-to-Site или Router – Router)
  Объединение нескольких офисов в одну сеть.
- **VPN-сервис в браузере**
  Маскировка IP-адреса.

VPN Point-to-Point

VPN Point-to-Point

Все названия: Point-to-Point, p2p, точка-точка.

Этот вариант используется, если вам нужно соединить между собой 2 устройства.

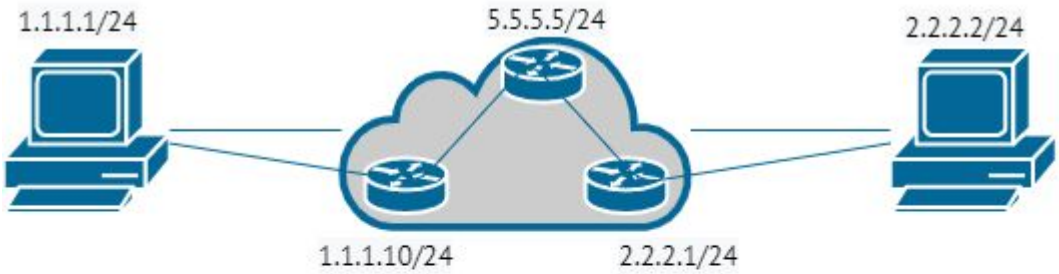
➡️ Например, для передачи секретной информации по открытым сетям (интернет).

После настройки VPN для устройств со стороны сетевого (L3) уровня всё будет выглядеть как если бы устройства соединили между собой проводом напрямую.

Часто этот «провод» называют **VPN-туннелем.**

VPN Point-to-Point

Без VPN



С VPN

VPN Remote access

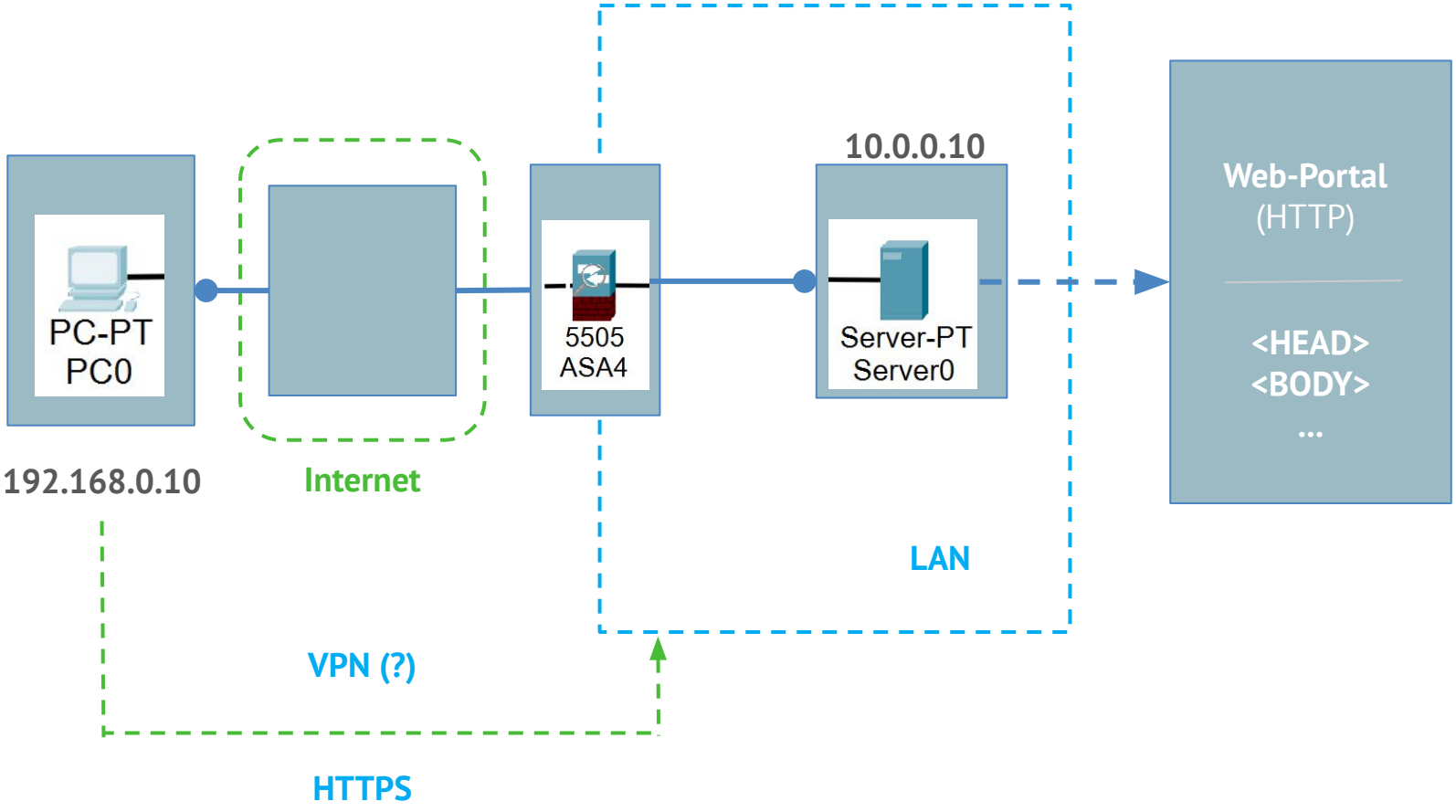
Clientless SSL VPN

Рассмотрим самый просто вид VPN Remote access ➡️

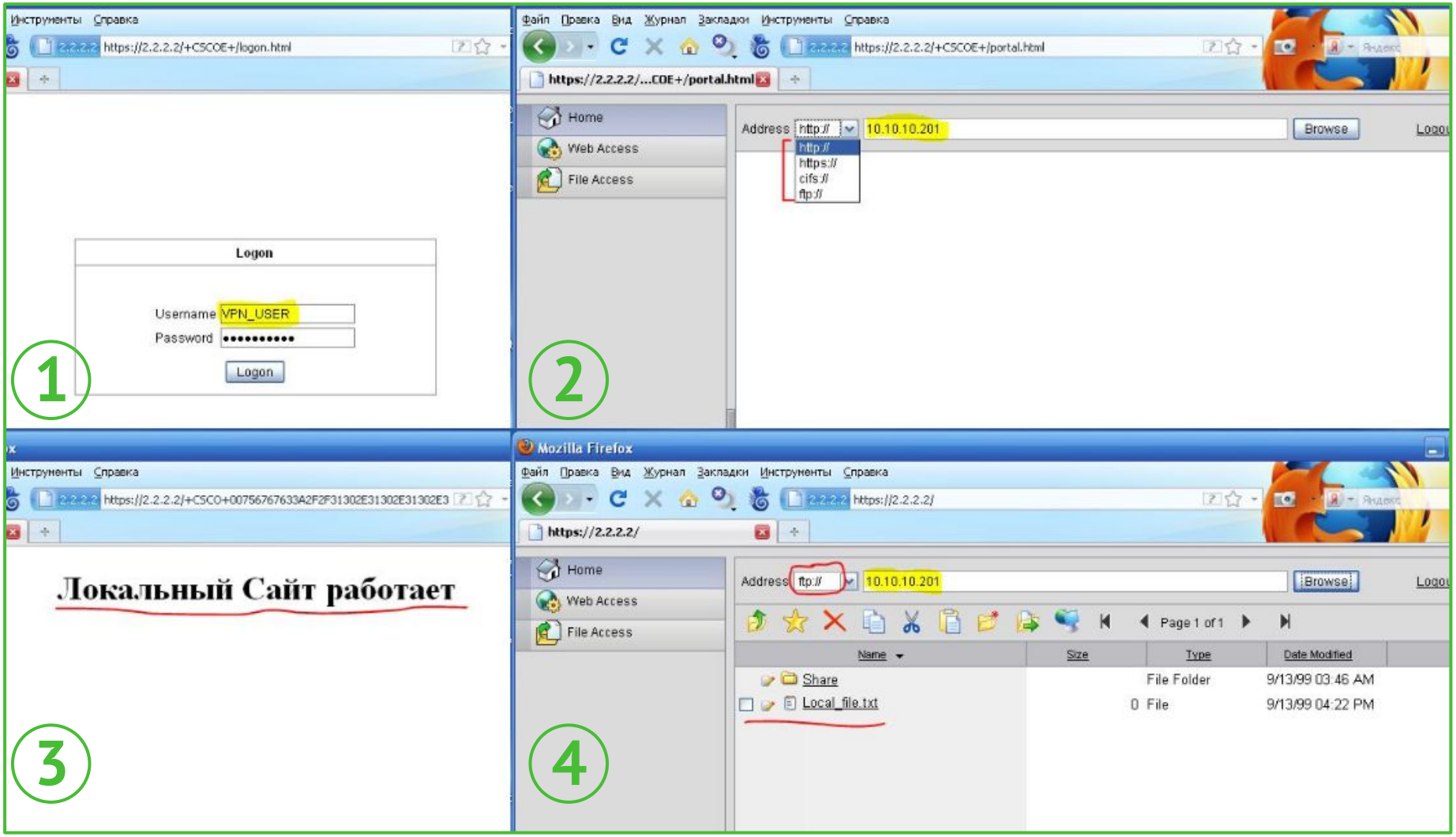
Clientless SSL VPN – подключение с помощью веб-браузера к внутреннему ресурсу компании, в нашем случае – веб серверу.

На практике, так часто реализуется подключение к Outlook Web Access (OWA) client.

Clientless SSL VPN



Clientless SSL VPN



SSL VPN Client

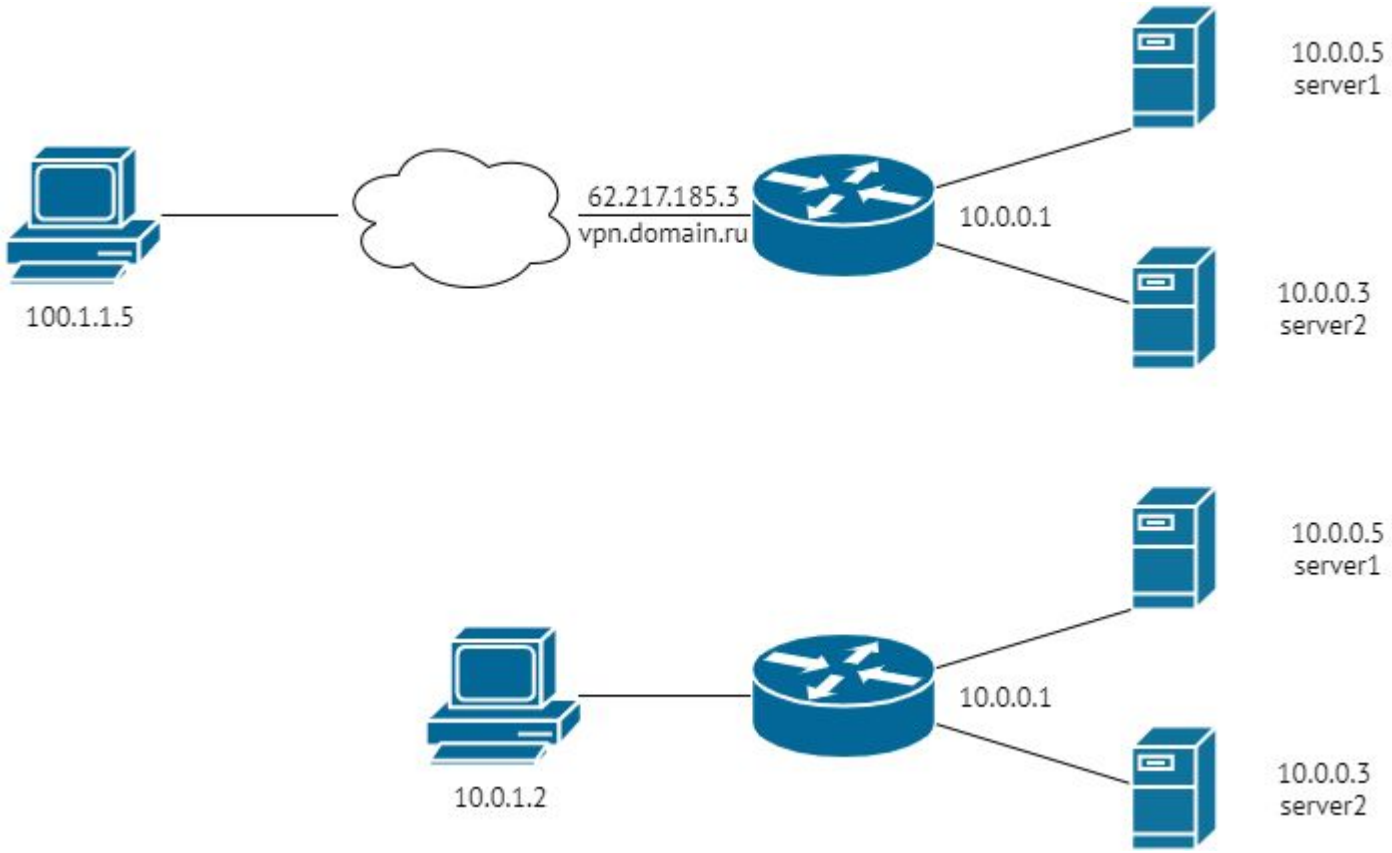
Рассмотрим один из самых популярных корпоративных VPN клиентов ➡️

Cisco Anyconnect VPN – подключение с помощью специального ПО (VPN клиента) к VPN серверу компании с использованием шифрования и авторизации.

Авторизация в первом варианте прозрачная, т.е. использование одного логина/пароля для авторизации во все системы внутри сети,

Во втором – с использованием двухфакторной аутентификации , т.е. с использованием дополнительного ПО, генерирующего одноразовые коды для входа.

Clientless SSL VPN



VPN Site-to-Site

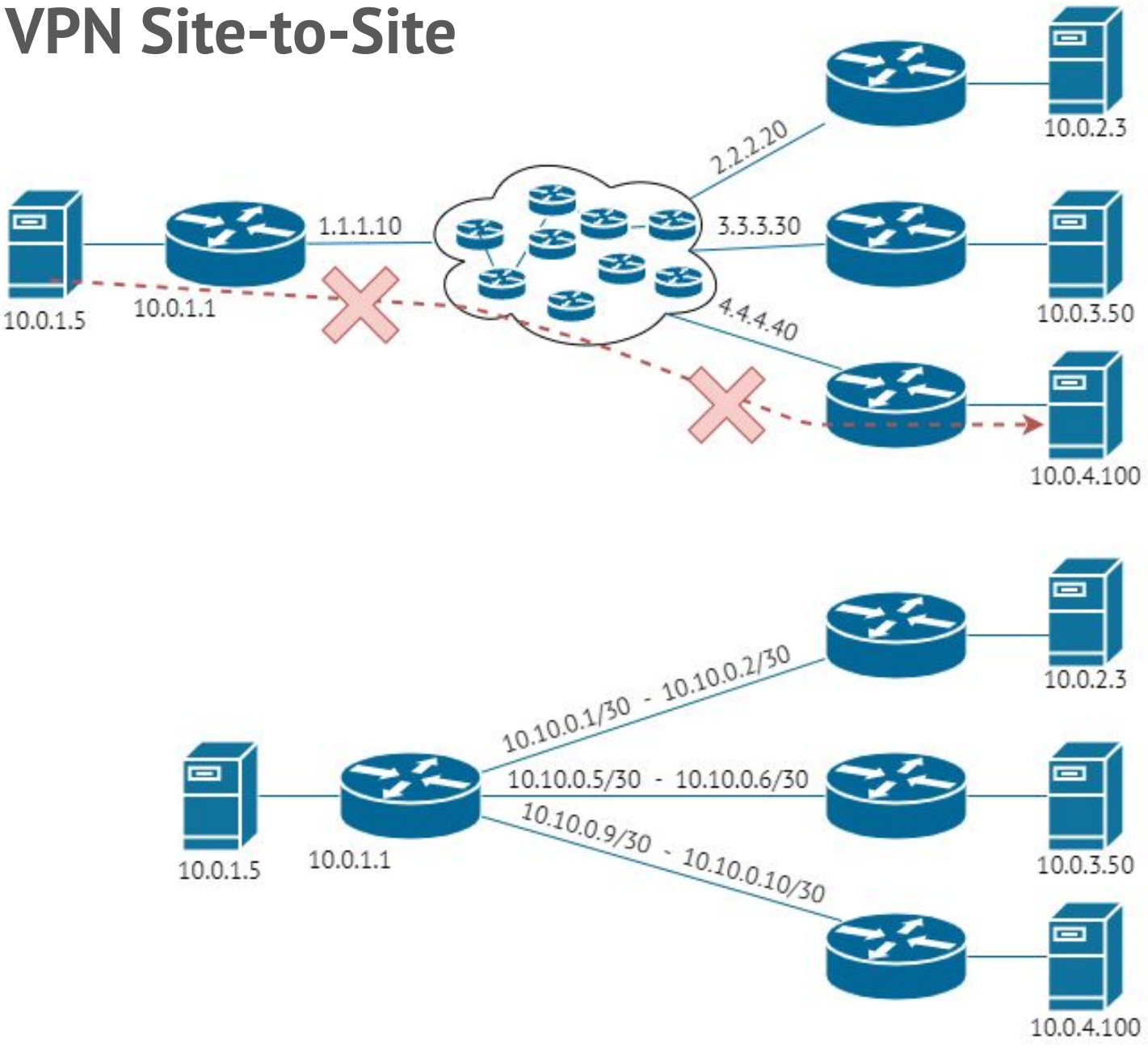
VPN Site-to-Site

Ещё один часто встречающийся в корпоративных сетях вид VPN.

Используется 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



Возможно, вы встречали такие услуги у операторов связи, как L2 VPN и L3 VPN.

В чем их разница?

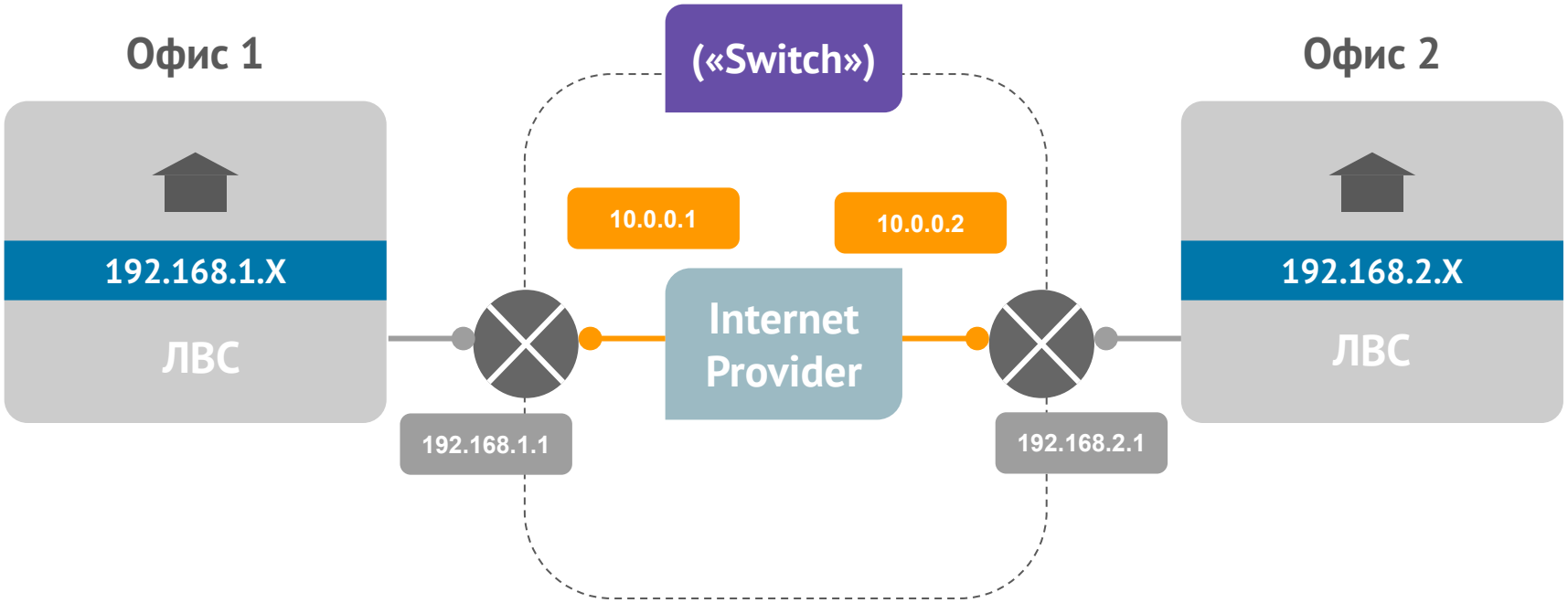
Провайдерские VPN

Детально углубляться в провайдерскую маршрутизацию на данной лекции не будем.

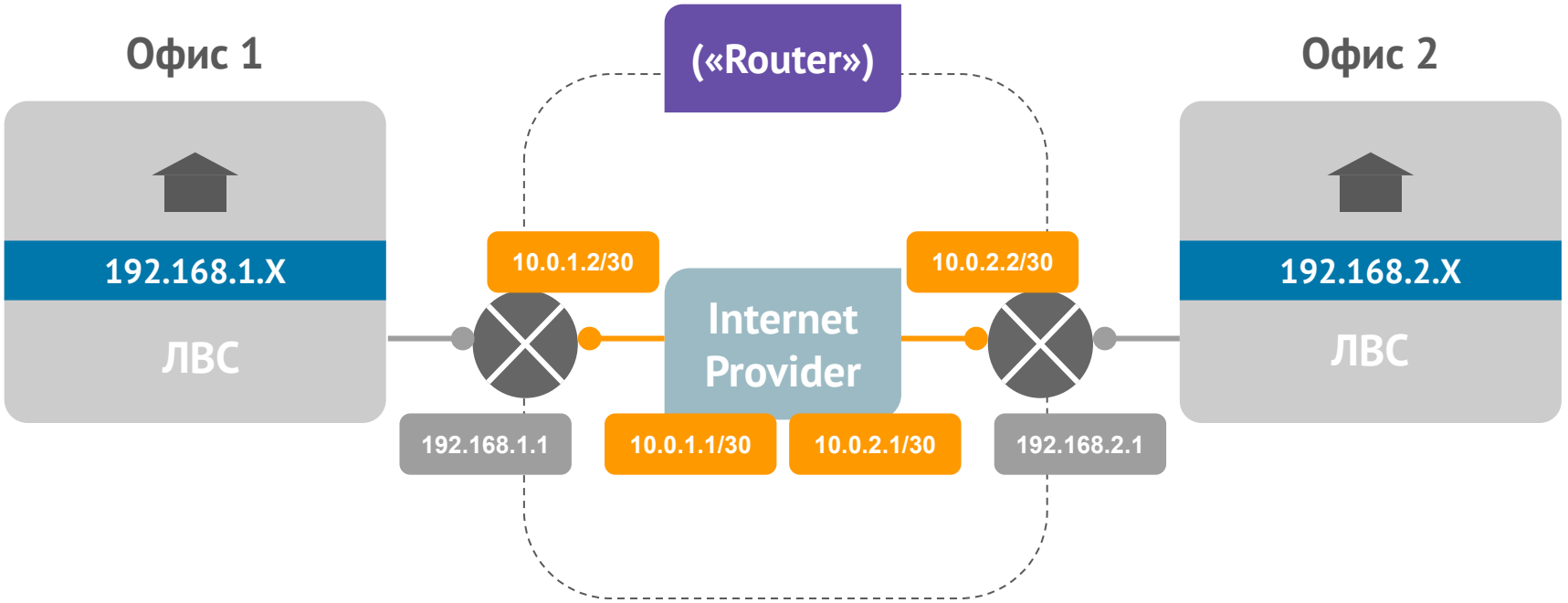
Основная суть – предоставить клиентам «собственную сеть» с использованием каналов оператора и подключения к ним офисов по всей стране.

- L2 VPN – провайдер предоставляет «как-будто» коммутатор;
- L3 VPN – провайдер предоставляет «как-будто» маршрутизатор.

L2 VPN


Офис 1
(«Switch»)
Офис 2
10.0.0.1
10.0.0.2
192.168.1.X
ЛВС
Internet Provider
192.168.2.X
ЛВС
192.168.1.1
192.168.2.1

L3 VPN


Офис 1
(«Router»)
Офис 2
192.168.1.X
ЛВС
10.0.1.2/30
10.0.2.2/30
Internet Provider
192.168.2.X
ЛВС
192.168.1.1
10.0.1.1/30
10.0.2.1/30
192.168.2.1

VPN протоколы

VPN протоколы

- **PPTP** – появился лет 20 назад, сейчас немного устарел;
- **L2TP** – по возрасту схож с PPTP, часто используется провайдерами. Не предлагает шифрования по умолчанию;
- **SSL** / **TLS** – почти нет проблем при работе через Интернет, т.к. поддерживается большим количеством серверов;
- **OpenVPN** – проект с открытым исходным кодом, основан на SSL / TLS;
- **IPSec** – специально разработан для создания безопасных соединений через IP-сети (будет рассмотрен далее).

Point-to-Point Tunneling Protocol

Point-to-Point Tunneling Protocol (PPTP) — один из старейших VPN протоколов, используемых до сих пор, изначально был разработан компанией Microsoft.

PPTP использует два соединения — одно для управления, другое для инкапсуляции данных.

Первое работает с использованием TCP, в котором порт сервера 1723.

Второе работает с помощью протокола GRE, который является транспортным протоколом (то есть заменой TCP/UDP).

Point-to-Point Tunneling Protocol

PPTP поддерживается нативно на всех версиях Windows и большинстве других операционных систем.

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.

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

Layer 2 Tunneling Protocol

Layer 2 Tunneling Protocol (L2TP) был впервые предложен в 1999 году. Поскольку L2TP сам по себе не обеспечивает шифрование или аутентификацию, часто с ним используется IPsec.

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.

Secure Socket Tunneling Protocol

Secure Socket Tunneling Protocol (SSTP) — проприетарный продукт от Microsoft. Как и PPTP не очень широко используется в VPN, но, в отличие от PPTP, у него не диагностированы серьезные проблемы с безопасностью.

SSTP отправляет трафик по SSL через TCP-порт 443.

Это делает его полезным 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.

OpenVPN

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

На сегодняшний день это, пожалуй, самый популярный протокол VPN. Будучи открытым стандартом, он прошел не одну независимую экспертизу безопасности.

В большинстве ситуаций, когда нужно подключение через VPN, скорее всего подойдет OpenVPN. Он стабилен и предлагает хорошую скорость передачи данных. OpenVPN использует стандартные протоколы TCP и UDP и это позволяет ему стать альтернативой IPsec тогда, когда провайдер блокирует некоторые протоколы VPN.

OpenVPN

Для работы OpenVPN нужно специальное клиентское программное обеспечение, а не то, которое работает из коробки.

Большинство VPN-сервисов создают свои приложения для работы с OpenVPN, которые можно использовать в разных операционных системах и устройствах.

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

➡️ Пример настройки

IPsec

Общие сведения

IPSec – стек сетевых протоколов для защищенной передачи данных через IP-сети.

IPsec обеспечивает аутентификацию, шифрование и проверку целостности передаваемых данных.

Описание стека IPsec занимает 12 документов RFC:

RFC 2401 – RFC 2412
tools.ietf.org/html/rfc2401

Режимы IPsec

Транспортный режим – работает поверх протокола IP и шифрует содержимое IP-пакета (payload).

Недостатком этого режима является то, что адреса отправителя и получателя не шифруются, поэтому можно проанализировать адреса и объем переданной информации.

Чаще всего используется для соединения между хостами.

Туннельный режим – создает новый IP-пакет, полностью шифруя исходный.

Использование туннельного режима сильно затрудняет анализ перехваченного трафика.

Чаще всего используется для передачи данных через Интернет.

Туннели IPsec

Туннелирование (tunneling) – это метод, используемый для передачи полезной нагрузки (кадра или пакета) одного протокола с использованием межсетевой инфраструктуры другого протокола.

Инкапсуляция в туннеле отличается от инкапсуляции в сетевых моделях тем, что в первом случае вкладываются данные этого же или более нижних сетевых уровней.

OSI: TCP ➡️ IP ➡️ Ethernet

Tunnel: Ethernet ➡️ IP ➡️ Ethernet или IP ➡️ IP ➡️ Ethernet

Security Association

Security Association (SA, безопасное соединение) – базовое понятие IPsec. Включает в себя информацию о криптографических протоколах и алгоритмах, ключах шифрования, определяет какие данные будут проходить через туннель.

Security Association

Чаще всего для создания SA используется Internet Security Association and Key Management Protocol (ISAKMP), для работы с ключами – протокол Internet Key Exchange (IKE).

Также следует помнить, что SA является однонаправленным, т.е. для взаимодействия нужно настроить два соединения.

Алгоритм работы IPsec

Установка и поддержка VPN туннеля происходит в два этапа:

- Фаза один;
- Фаза два.

Алгоритм работы фазы один

В этой фазе узлы договариваются о:

- методе идентификации;
- алгоритме шифрования;
- хэш алгоритме;
- группе Diffie Hellman.

Также происходит взаимная идентификация.

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

1

Алгоритм работы фазы два

В этой фазе генерируются ключи и узлы договариваются об используемой политике.

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

➡️ На этом установка туннеля считается завершенной.

VPN сервисы

VPN сервисы

Существует ряд сервисов, которые используют технологию VPN для безопасной и анонимной работы в сети Интернет.

Браузеры:

- Opera;
- Epic Privacy Browser;
- Google Chrome + Browsec addon;
- TOR.

VPN сервисы

Отдельные продукты:

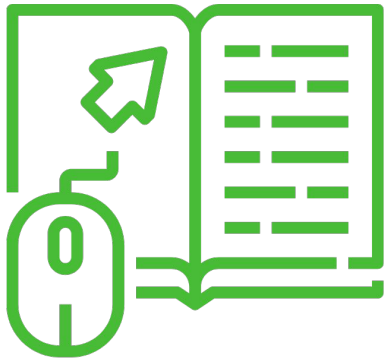
- Hotspot Shield;
- Betternet (есть реклама, но бесплатная версия работает хорошо);
- Kaspersky Secure Connection;
- Hola VPN (много рекламы, не рекомендуется к установке).

Итоги

Итоги

Сегодня мы познакомились с базовыми представлениями о технологиях удаленного доступа:

- VPN;
- стеке протоколов IPsec.



Домашнее задание

Домашнее задание

Давайте посмотрим ваше домашнее задание.

Настоятельно рекомендуем вам выполнять ДЗ в том же ритме, что и просмотр лекций.

- Вопросы по домашней работе задавайте **в чате** мессенджера Slack.
- Задачи можно сдавать **по частям**.
- Зачёт по домашней работе проставляется после того, как **приняты все задачи**.

нетология

Задавайте вопросы и пишите отзыв о лекции!

Андрей Вахутинский