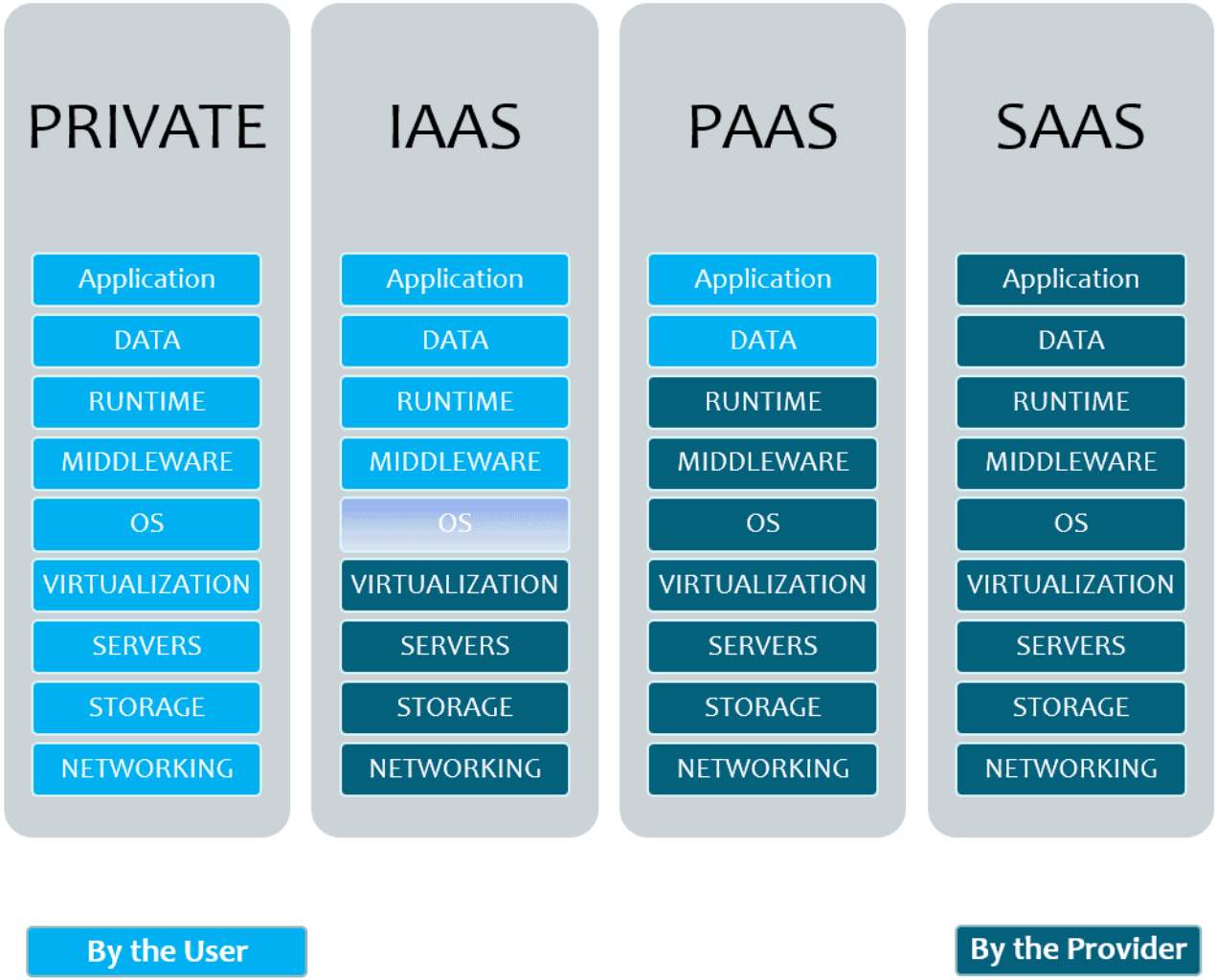
Тема 7
Безопасность виртуального окружения

Модели доступа к ресусам



Модели доступа к ресусам. Private

- Private — клиент иммеет полный доступ к оборудованию
- Например, физический доступ к серверу

Модели доступа к ресусам. IaaS

- IaaS — Infrastructure as a Service — инфраструктура как услуга
- Например, виртуальные серверы и виртуальная сеть. IBM Softlayer, Hetzner Cloud, Microsoft Azure, Amazon EC2, GigaCloud
- Клиент может устанавливать любое программное обеспечение и приложения

Модели доступа к ресусам. PaaS

- PaaS — Platform as a Service — платформа как услуга
- Например, веб-сервер или база данных. Google App Engine, IBM Bluemix, Microsoft Azure, VMWare Cloud Foundry
- Клиент управляет приложениями
- Провайдер управляет операционной системой

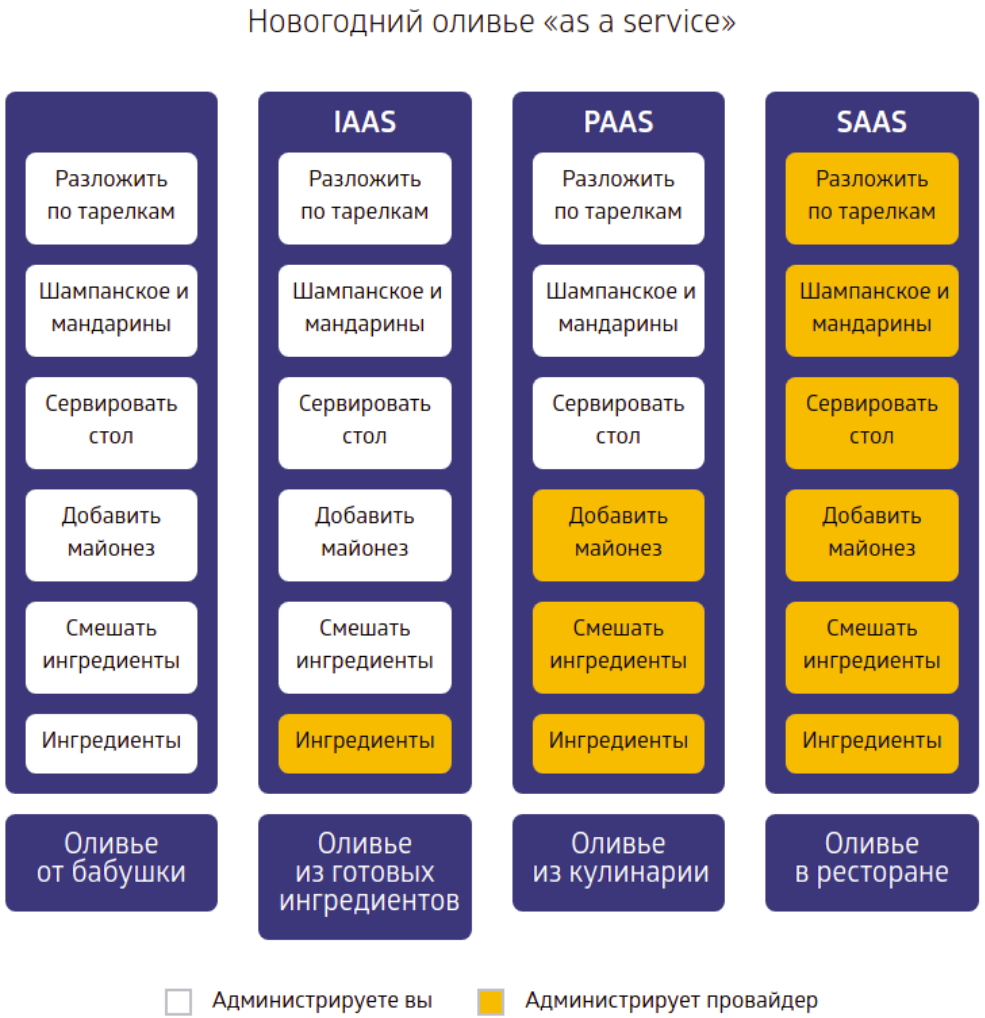
Модели доступа к ресусам. SaaS

- SaaS — Software as a Service — программное обеспечение как услуга
- Например, электронная почта или иное офисное приложение. Dropbox, Google Doc, Microsoft Office 365, Flickr, Facebook
- Клиент пользуется приложением
- Провайдер управляет базовыми настройками приложения

Модели доступа к ресусам

- **Если после определений и примеров не стало понятнее, то следующий слайд должен расставить все по своим местам**

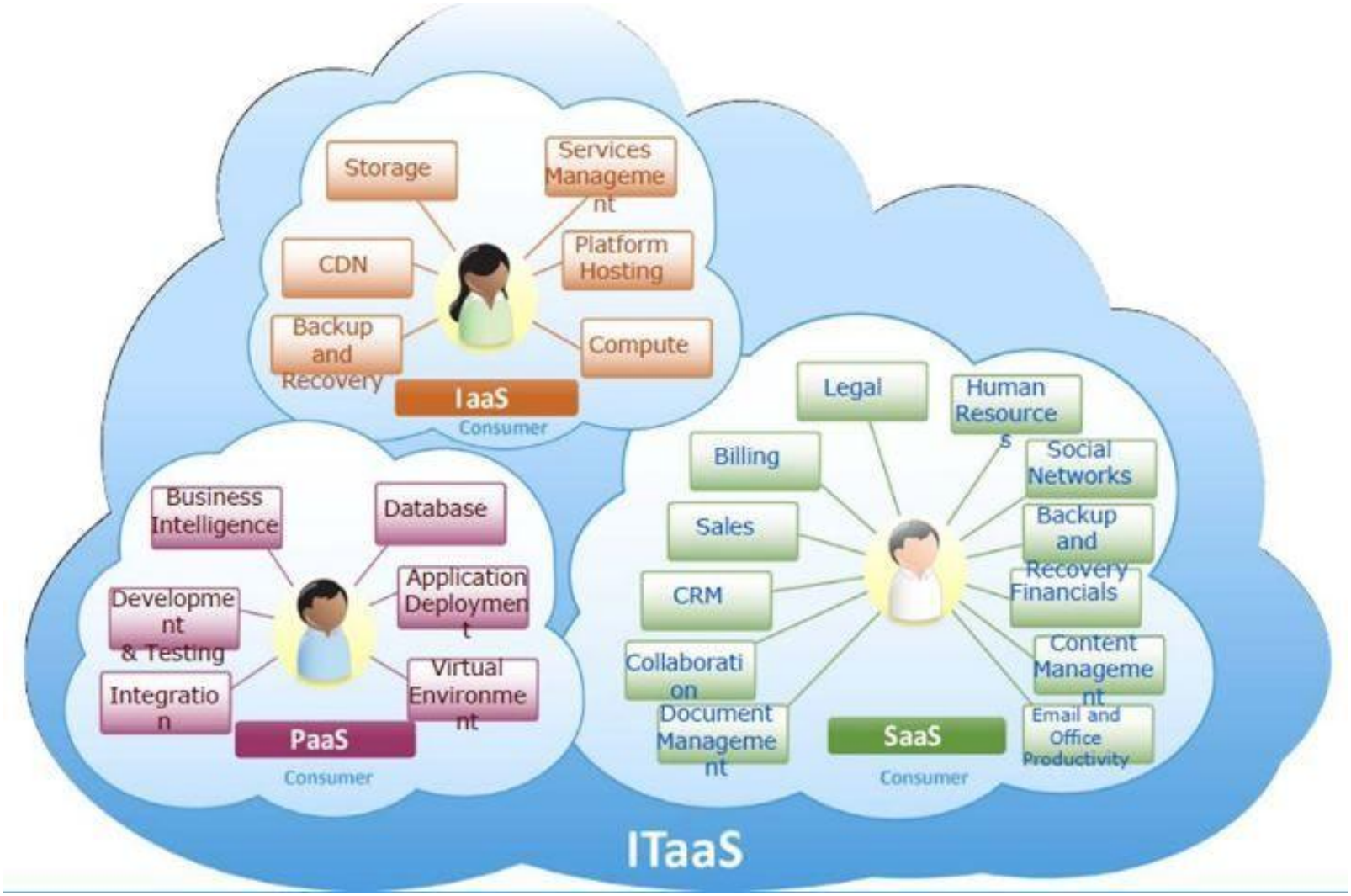
Модели доступа к ресусам



Модели доступа к ресусам

- ITaaS — IT as a Service(ИТ-аутсорсинг), модель предоставления информационных услуг, подразумевающая, что поставщик предоставляет эти услуги какому-либо бизнесу. Причем поставщиком может выступать как внутренняя ИТ-организация, так и внешняя ИТ-компания.
- ITaaS означает передачу работ по обслуживанию, поддержке, совершенствованию ИТ-инфраструктуры

Модели доступа к ресусам



Модели развертывания

- Частное облако
- Публичное облако
- Общественное облако
- Гибридное облако

Модели развертывания

- Частное облако — инфраструктура, предназначенная для использования одной организацией, включающей несколько потребителей (например, подразделений одной организации), возможно также клиентами и подрядчиками данной организации. Частное облако может находиться в собственности, управлении и эксплуатации как самой организации, так и третьей стороны (или какой-либо их комбинации), и

Модели развертывания

- **Публичное облако — инфраструктура, предназначенная для свободного использования широкой публикой. Публичное облако может находиться в собственности, управлении и эксплуатации коммерческих, научных и правительственных организаций (или какой-либо их комбинации). Публичное облако физически существует в юрисдикции владельца — поставщика услуг.**

Модели развертывания

- **Общественное облако — вид инфраструктуры, предназначенный для использования конкретным сообществом потребителей из организаций, имеющих общие задачи (например, миссии, требований безопасности, политики, и соответствия различным требованиям). Общественное облако может находиться в кооперативной (совместной) собственности, управлении и эксплуатации одной или более из организаций**

Модели развертывания

- **Гибридное облако — это комбинация из двух или более различных облачных инфраструктур (частных, публичных или общественных), остающихся уникальными объектами, но связанных между собой стандартизованными или частными технологиями передачи данных и приложений (например, кратковременное использование ресурсов публичных облаков для балансировки нагрузки между облаками).**

Безопасность доступа по сети

- Тунелирование и шифрование
- Удаленный доступ

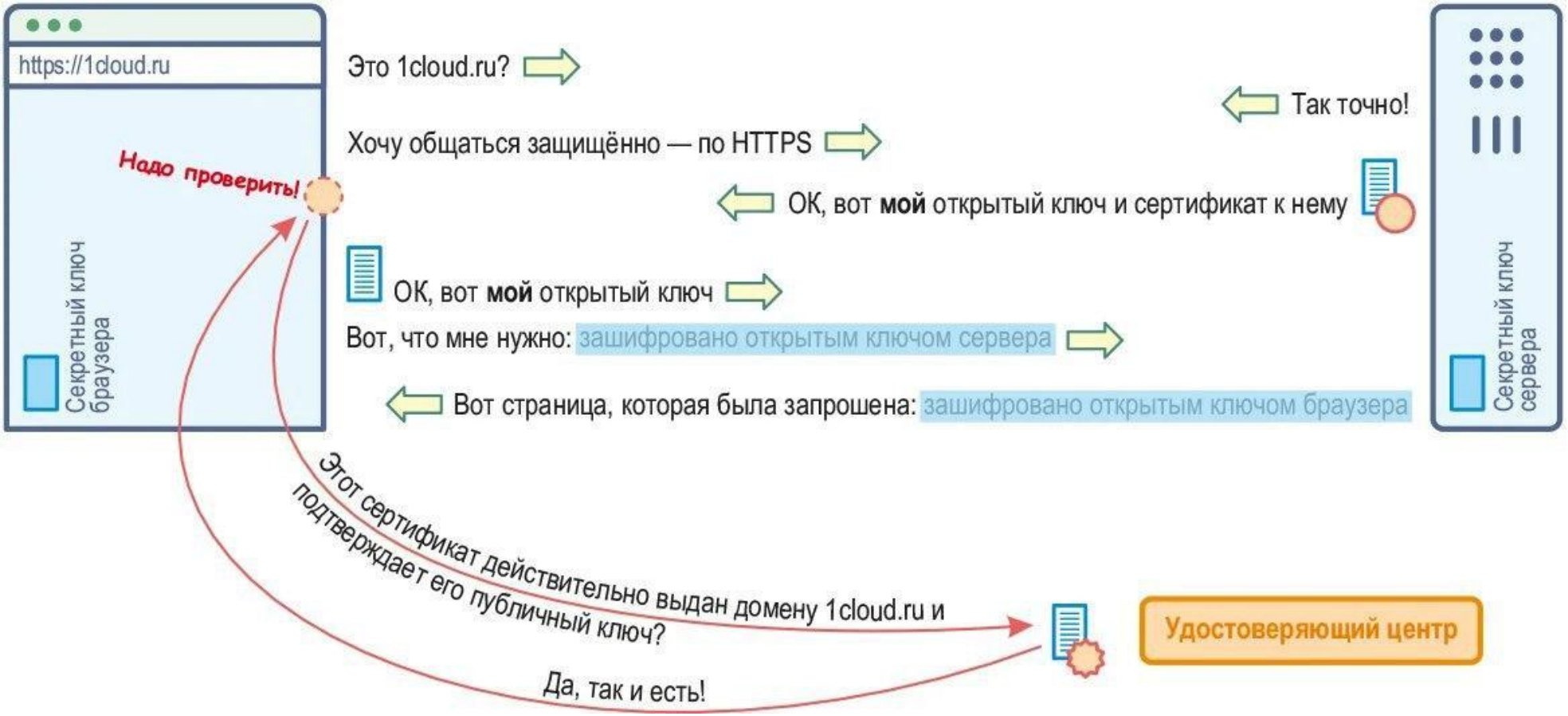
Тунелирование и шифрование

- **Туннелирование - это процесс инкапсуляции одного протокола в другой, чтобы обеспечить безопасную связь через небезопасную среду, которой обычно является Интернет**

Протоколы тунелирования. SSL VPN

- **Протокол безопасного уровня сокетов будет использовать криптографию, чтобы обеспечить безопасную связь и конфиденциальность аутентификации через Интернет.**

Протоколы тунелирования. SSL VPN



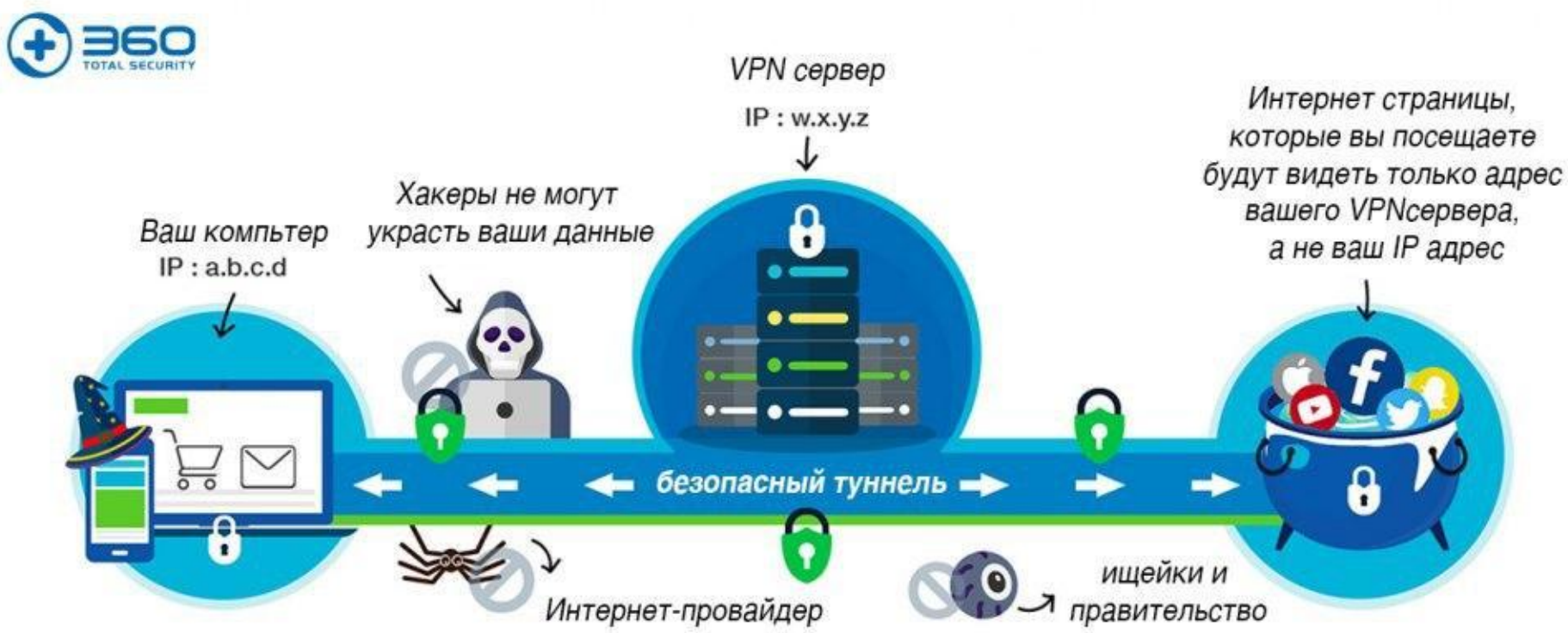
Протоколы тунелирования. VPN

- **Виртуальная частная сеть - обобщённое название технологий, позволяющих обеспечить одно или несколько сетевых соединений (логическую сеть) поверх другой сети (например Интернет)**

Задачи, которые решает VPN

- Адресация пакетов, предназначенных конкретным клиентам.
- Эффективное и в то же время не слишком жадное до ресурсов шифрование «на лету», исключающее прохождение информации в открытом виде.
- Аутентификация участников при подключении к сети и проверка источников данных для защиты сети от попадания в нее несанкционированных узлов и пакетов.

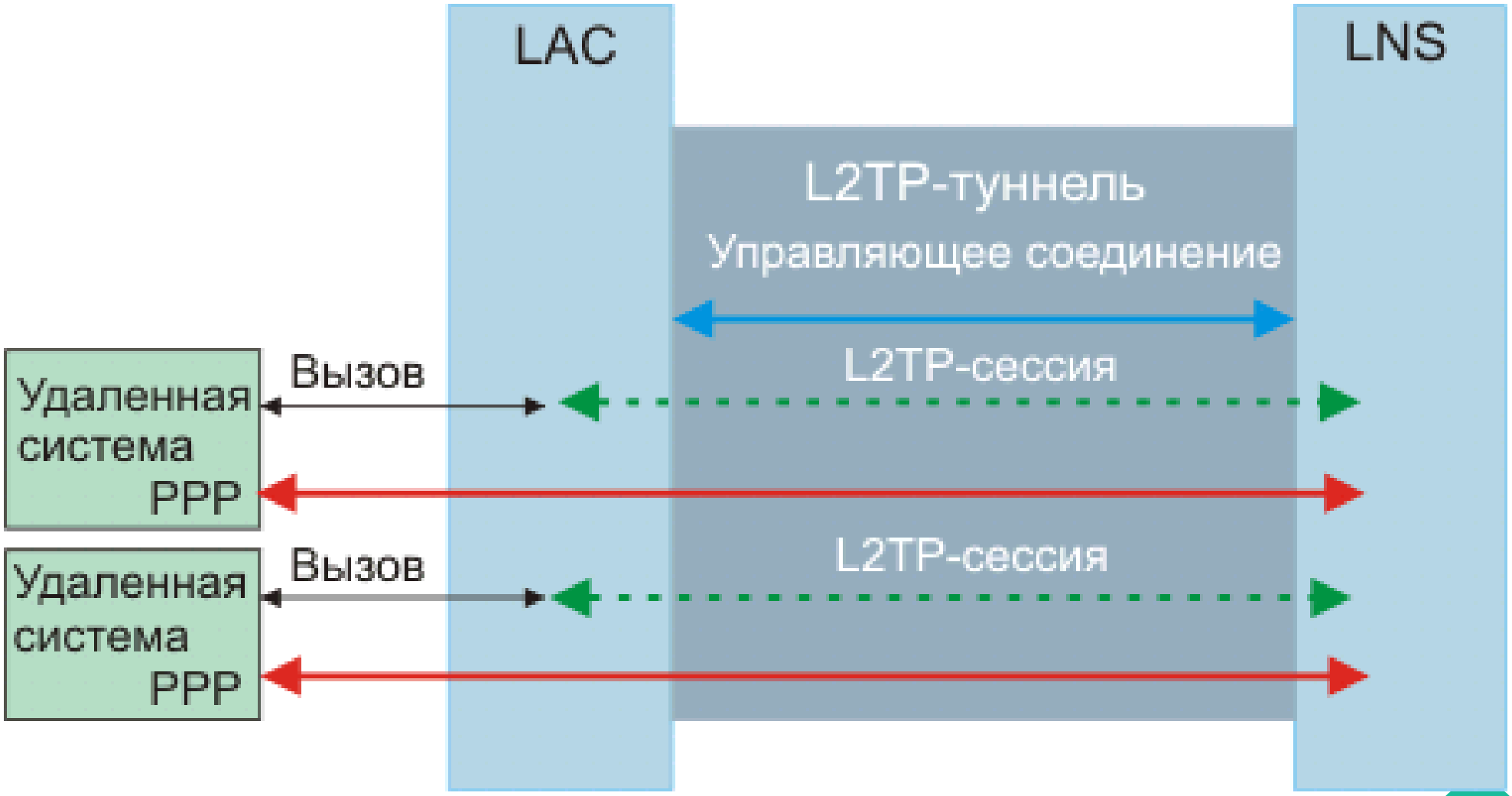
Протоколы тунелирования. VPN



Протоколы тунелирования. L2TP

- Протокол туннелирования уровня 2 является одним из наиболее часто используемых протоколов туннелирования. Он использует IP / Sec для аутентификации клиента в двухфазном процессе. Сначала он аутентифицирует компьютер, а затем пользователя. Аутентификация компьютеров помогает предотвратить man in the middle attack, таким образом, когда данные сначала перехватываются другим

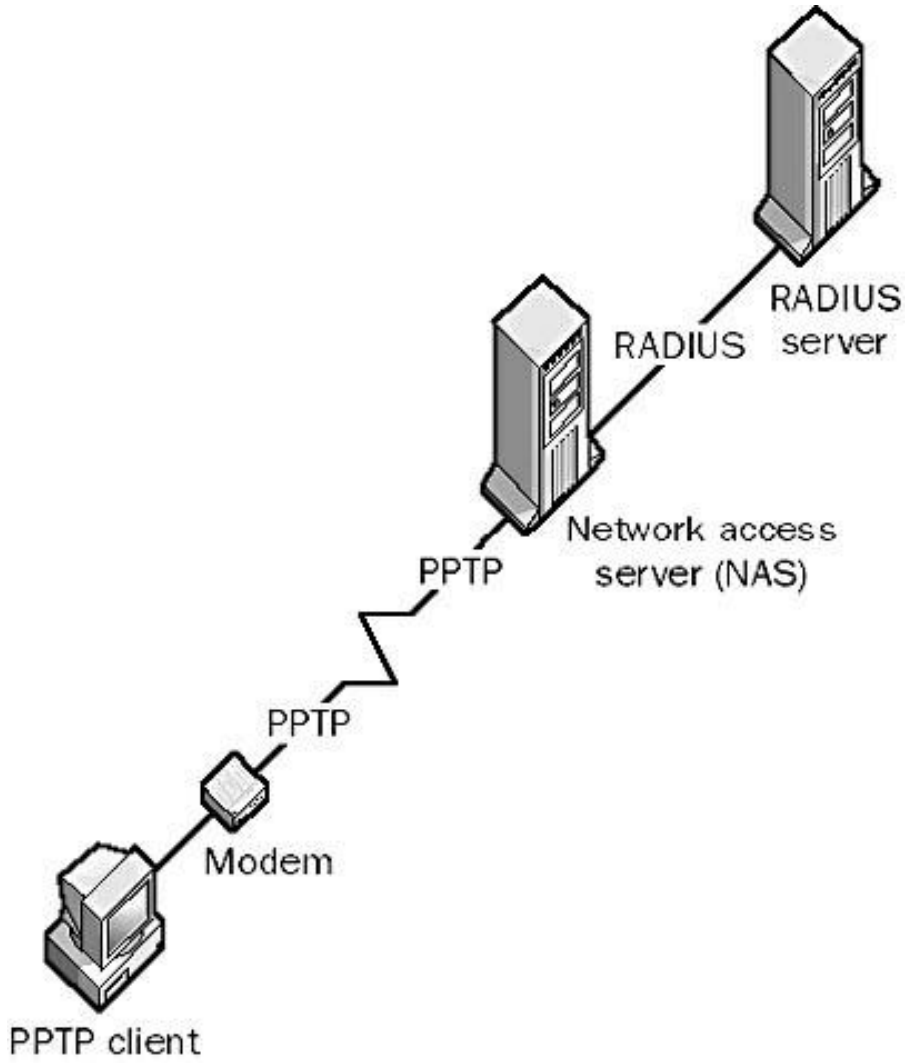
Протоколы тунелирования. L2TP



Протоколы тунелирования. PPTP

- Это протокол туннелирования точка-точка, который используется для создания защищенного туннеля между двумя точками в сети, через который будет использоваться другой протокол, такой как протокол точка-точка. Функциональность туннелирования обеспечивает основу для большей части VPN. Поскольку PPTP является широко используемым протоколом, другие протоколы туннелирования, такие как L2TP.

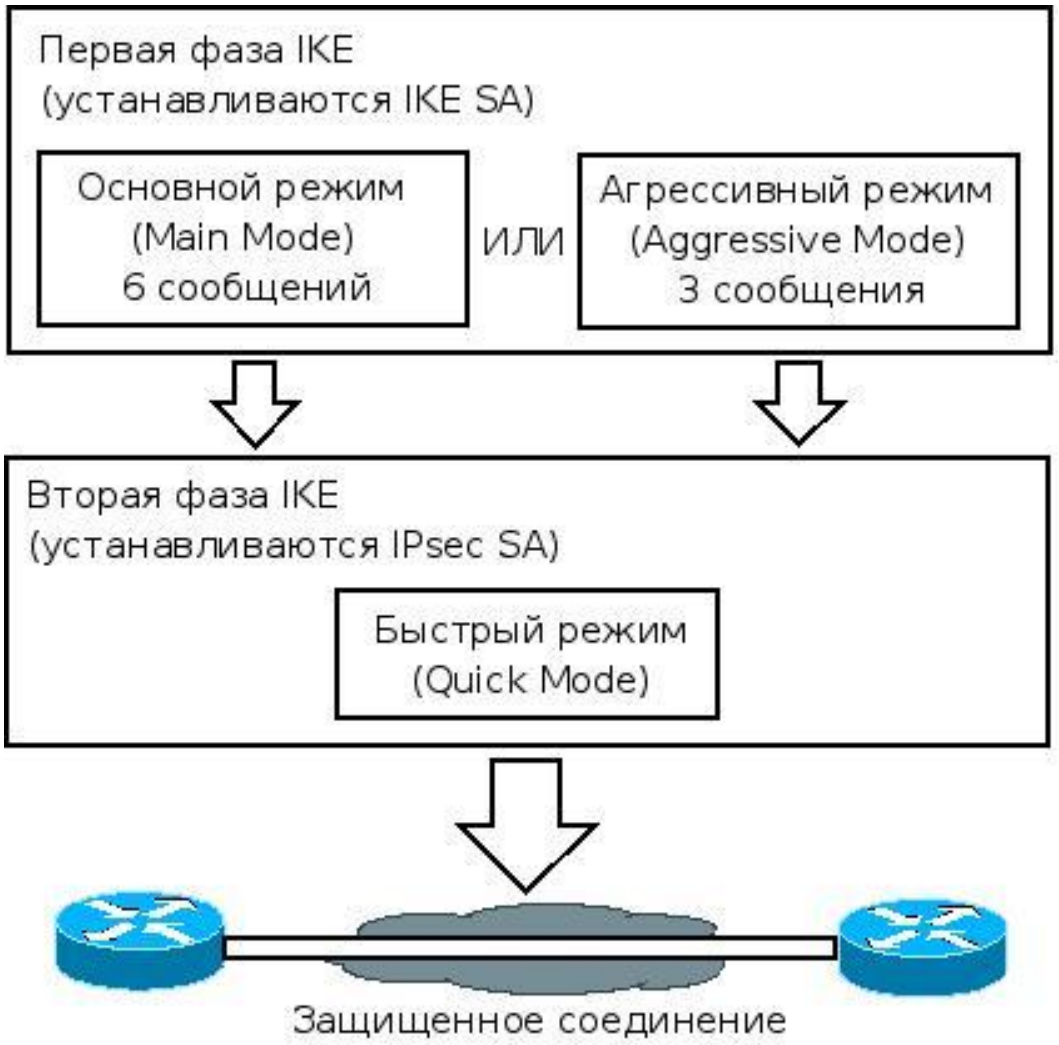
Протоколы тунелирования. PPTP



Протоколы тунелирования. IPSec

- IPSec является основой протоколов, предлагаемых для аутентификации соединения, а также для шифрования данных во время связи между двумя компьютерами. Он работает на сетевом уровне модели OSI и обеспечивает безопасность протоколов, работающих на более высоком уровне модели OSI. Более конкретно, этот IPSec имеет 3 основных способа защиты, таких как защита от подделки данных, проверка данных и

Протоколы тунелирования. IPSec

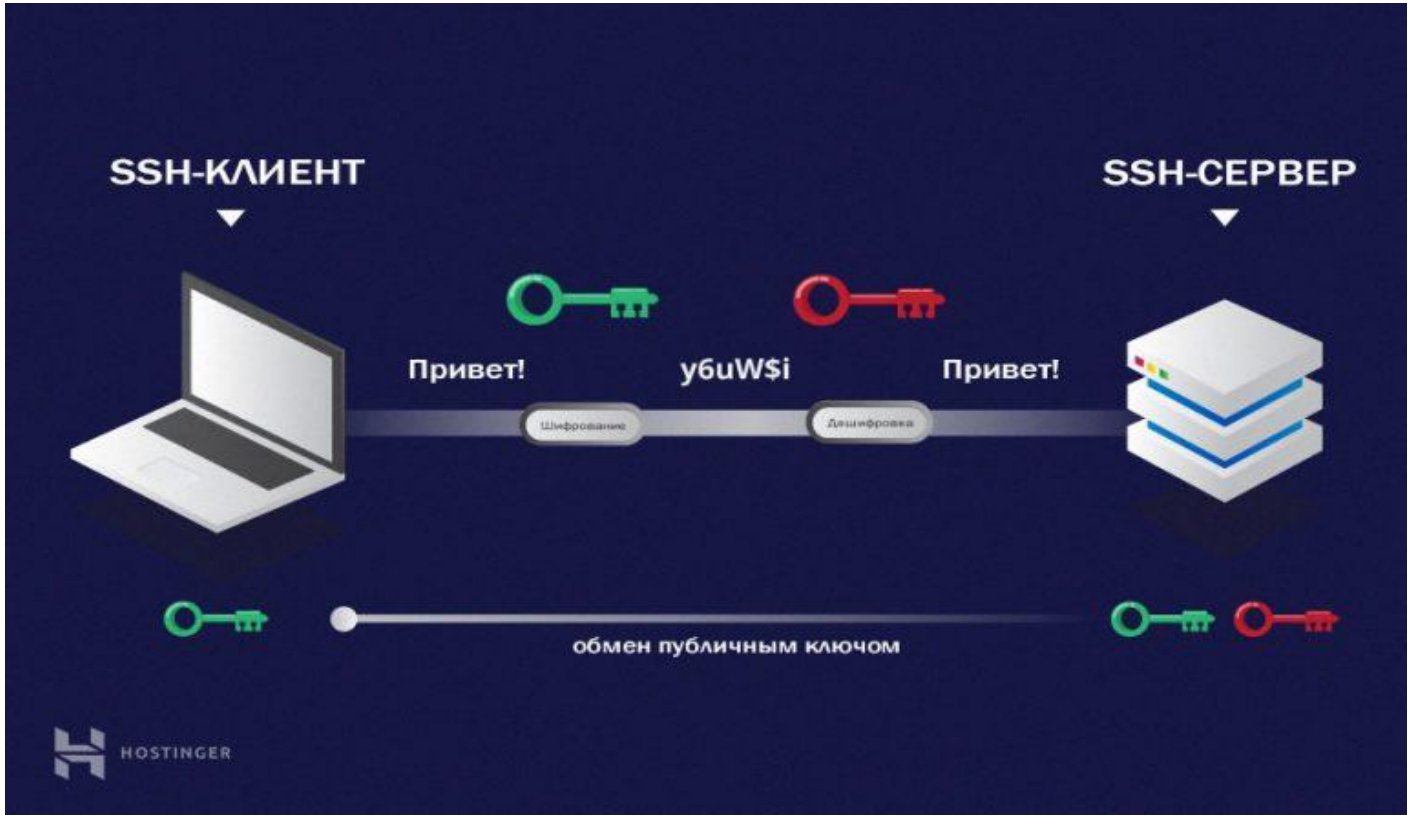


Удаленный доступ

- **Удаленный доступ означает, что пользователь не находится на устройстве, которое подключено к локальной сети организаций, но вместо этого он подключен за пределами локальной сети.**

Удаленный доступ. SSH

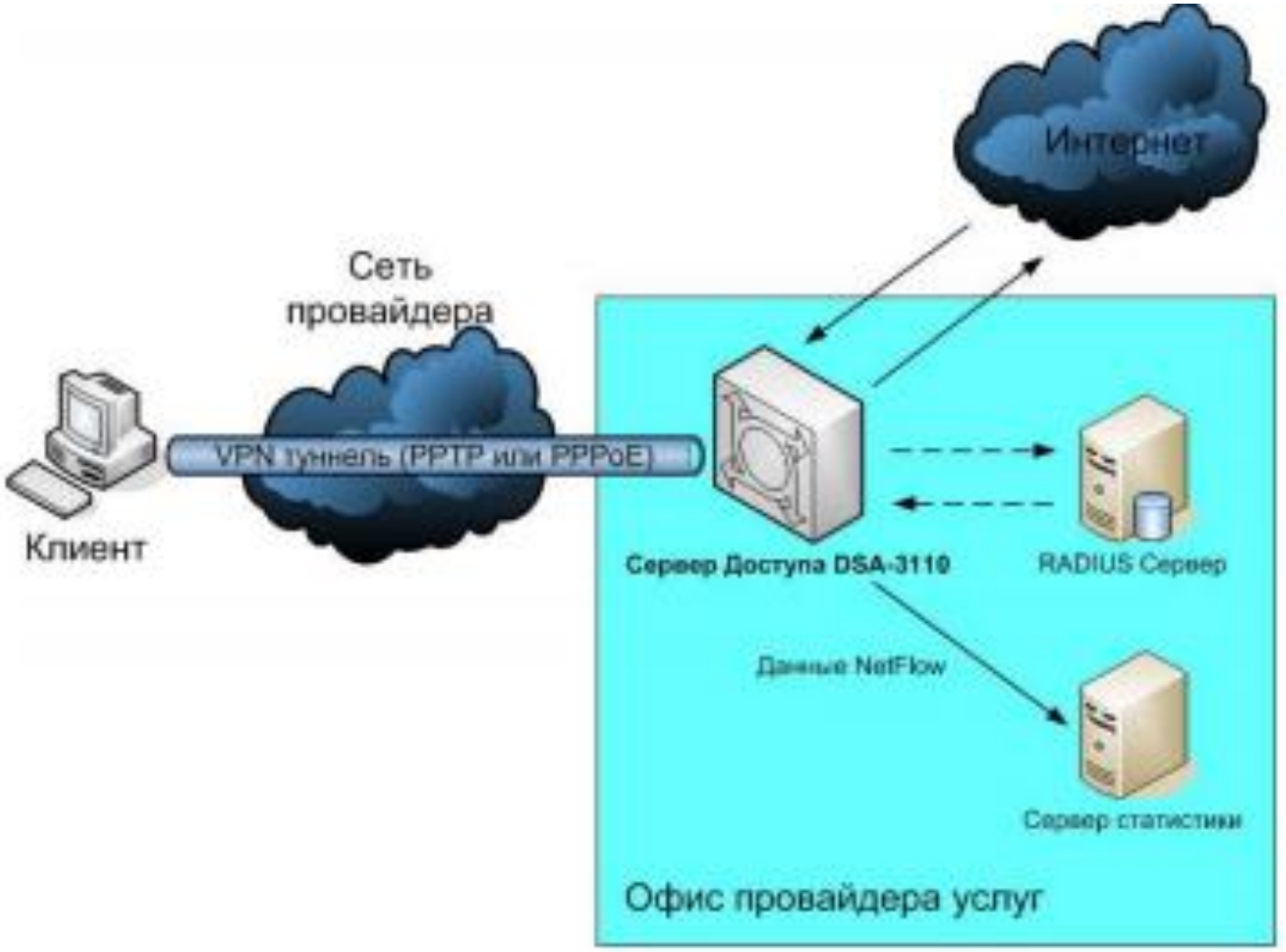
- Secure Shell - это программа, которая позволяет войти в систему на другом компьютере, а также перемещать файлы с 1 компьютера на другой компьютер. SSH предлагает безопасную связь и строгую аутентификацию через незащищенный канал. Он защищает сеть от атак, включая маршрутизацию IP-источников, IP spoofing и DNS spoofing. SSh доступен для Macintosh, Linux и Unix, а также работает с аутентификацией RSA. Он работает на


SSH-КЛИЕНТ
SSH-СЕРВЕР
Привет!
уБuW$i
Привет!
Шифрование
Дешифровка
обмен публичным ключом
HOSTINGER

Удаленный доступ. PPPoE

- Это протокол точка-точка через Ethernet, который более популярен из-за растущего числа пользователей, которые используют DSL-соединения и кабельные модемы для доступа в Интернет. Основная функция заключается в инкапсуляции кадров PPP в кадрах Ethernet

Удаленный доступ. PPPoE



Удаленный доступ. PPP

- **Протокол точка-точка - это протокол, который используется большинством пользователей в качестве стандартного протокола удаленного доступа. Он предлагает механизмы аутентификации, поддержку нескольких протоколов и проверку ошибок.**

Проблемы безопасности

- **Технологии виртуализации сами по себе являются средством для создания новых видов угроз, как, например, руткиты Blue Pill и SubVirt.**

Проблемы безопасности

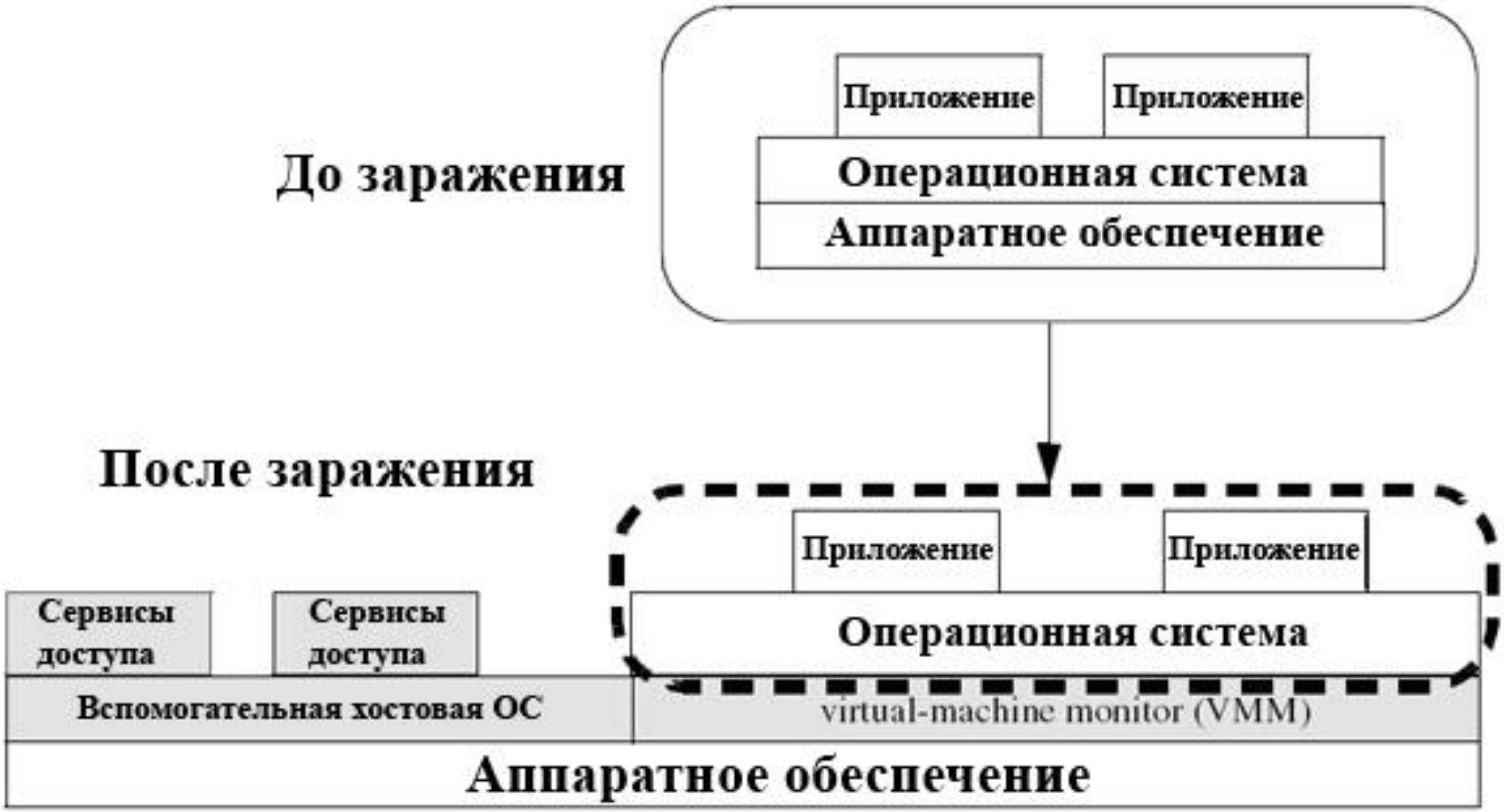
- **Руткиты — это вредоносные программы, которые проникают на компьютер различными путями. Например, руткит может попасть на компьютер с загруженной из интернета программой, либо с файлом из письма. Активируя руткит на компьютере, пользователь фактически предоставляет злоумышленникам доступ к своему PC.**

Проблемы безопасности. Blue Pill

Механизм работы руткита выглядит следующим образом:

- вредоносный код проникает в целевую систему
- затем происходит незаметная виртуализация хостовой системы, которая превращается в гостевую на данном компьютере, а Blue Pill действует как гипервизор, при этом не требуется перезагрузка операционной системы

Проблемы безопасности. Blue Pill



Проблемы безопасности. SubVirt

- SubVirt в отличие от Blue Pill, этот руткит может быть более просто обнаружен, поскольку не может быть установлен «на лету» и вносит некоторые изменения в структуру диска, что делает возможным обнаружение руткита при проверке диска на другом компьютере. Также SubVirt эмулирует аппаратные компоненты, отличающиеся от реального «железа», что позволяет просто обнаружить виртуализацию.

Способы защиты виртуальной инфраструктуры

- Защита данных не только внутри виртуальных машин, но и сами образы виртуальных систем
- Специализированные решения для защиты серверов виртуализации (sHype)
- Системы обнаружения или предотвращения вторжений (Intrusion Detection/Prevention Systems, IDS/IPS), для критически важных машин в пределах серверов виртуализации

Безопасность гипервизора

- Установка исправлений и обновлений от производителя гипервизора сразу же, как только они станут доступны. Поддержка этого исправным процессом управления патчами для уменьшения риска уязвимостей гипервизора.
- Неиспользуемое виртуальное железо, которое подключается к гипервизору, следует отключить.

Безопасность гипервизора

- Отключение ненужных сервисов, такие как буфер обмена или совместное использование файлов
- Проверка гипервизора на предмет наличия любых потенциальных признаков взлома. Отслеживание и анализ логов гипервизора.
- Двухфакторная аутентификация для любых действий администратора на гипервизоре.

Oracle

- **Рассмотрим как oracle подходит к безопасности своих реализаций моделей**

Доступ к сервисам со стороны сотрудников

- Для предоставления доступа используются защищенный туннель VPN с мультифакторной аутентификацией, а также политики доступа к системам управления компонентами инфраструктуры и облаком в среде Oracle Cloud.

Доступ к сервисам со стороны сотрудников

- Средства управления доступом к системе включают в себя системную аутентификацию, авторизацию, получение подтверждения доступа, подготовку данных и отзыв полномочий для сотрудников Oracle и других пользователей, определенных Oracle.
- Все действия пользователей, включая нажатия клавиш, записываются, чтобы можно было провести аудит и расследование

Сетевая архитектура

- **Брандмауэры, для мониторинга сетевых коммуникаций и управления ими как на внешних, так и внутренних границах сети**
- **Эти устройства используют политики транспортных потоков или списки контроля доступа (ACLs) для управления потоками трафика.**

Сетевая архитектура

- **Брандмауэры развертываются с использованием многоуровневого подхода, чтобы выполнять пакетную проверку с помощью политик безопасности, настроенных для фильтрации пакетов по протоколу, порту, источнику и IP-адресу с целью определения санкционированных источников, мест назначения и видов трафика.**

Сетевая архитектура. Защита от DDoS-атак

- Меры по защите от DDoS-атак и смягчения их последствий реализуются прежде всего с помощью сертифицированной платформы-брандмауэра с выделенной DOS-защитой.
- Устройства масштабируются, чтобы поддерживать большие объемы трафика и не терять соединение. Это обеспечивает защиту от атак на уровне 3–7 модели OSI.

Сетевая архитектура. Защита от DDoS-атак

- Даже если атака является широкомасштабной и злоумышленники пытаются создать нагрузку, превышающую пропускную способность каналов связи, или фальсифицируют подлинные подключения, пытаясь исчерпать объем памяти, природа среды для распределения нагрузки с использованием посредника позволяет изучать каждое подключение и реагировать на них, принимая или прекращая подключения в зависимости от

Сетевая архитектура. Защита от DDoS-атак

- Эти устройства активно анализируют все сеансы, проверяя протоколы, содержимое и брандмауэр веб-приложений (уровень 7).
- В этих устройствах используются также такие технологии, как шифрование файлов SYN-cookie, таблицы соединений большой емкости, поиск по шаблонам, проверка потоков, предотвращение затопления пакетами ICMP и TCP-переадресация в порядке поступления.

Сетевая архитектура. Обнаружение вторжений

- Сервисы Oracle Cloud Services используют системы обнаружения вторжения в сеть (NIDS) для защиты среды.
- Датчики NIDS развертываются в сети в режиме предотвращения вторжений (IPS) или обнаружения вторжений (IDS), чтобы отслеживать и блокировать подозрительный трафик, не пропуская его во внутреннюю сеть.

Сетевая архитектура. Обнаружение вторжений

- **Уведомления NIDS направляются в централизованную систему мониторинга, которая находится под управлением групп по обеспечению безопасности круглосуточно и без выходных.**

Зашифрованный доступ

- Для доступа к сервисам Oracle Cloud Service используется стандартный для отрасли протокол TLS
- Заказчики также могут получать доступ к сервисам Oracle Cloud посредством SSH или сервиса VPN с туннелем IPsec