Защита межфилиальной связи

Обеспечение безопасности представляет собой одну из важнейших задач при использовании в бизнесе Интернета для общего доступа. Для защиты данных при их передаче через Интернет используются виртуальные частные сети (Virtual Private Networks, VPN).

VPN применяется для создания частного туннеля через сеть общего доступа. Для защиты данных от несанкционированного доступа можно использовать шифрование в этом туннеле в Интернете, а также аутентификацию.

В этой лекции описываются понятия и процессы, относящиеся к сетям VPN, а также преимущества внедрения сетей VPN и базовые протоколы, необходимые для настройки этих сетей.

По мере роста предприятия малого или среднего бизнеса возникает необходимость в предоставлении заказчикам, удалённым сотрудникам и сотрудникам с проводным/беспроводным подключением доступа к основной сети из любого местоположения.

Как сетевой администратор предприятия вы решили внедрить сети VPN, обеспечивающие безопасность связи, упрощенный доступ к сети и сокращение затрат.

Задача сетевого администратора предприятия — гарантировать, что все сетевые администраторы приступят к процессу планирования VPN, используя один и тот же набор данных.

Нужно исследовать четыре основных области данных VPN и предоставить их команде сетевых администраторов:

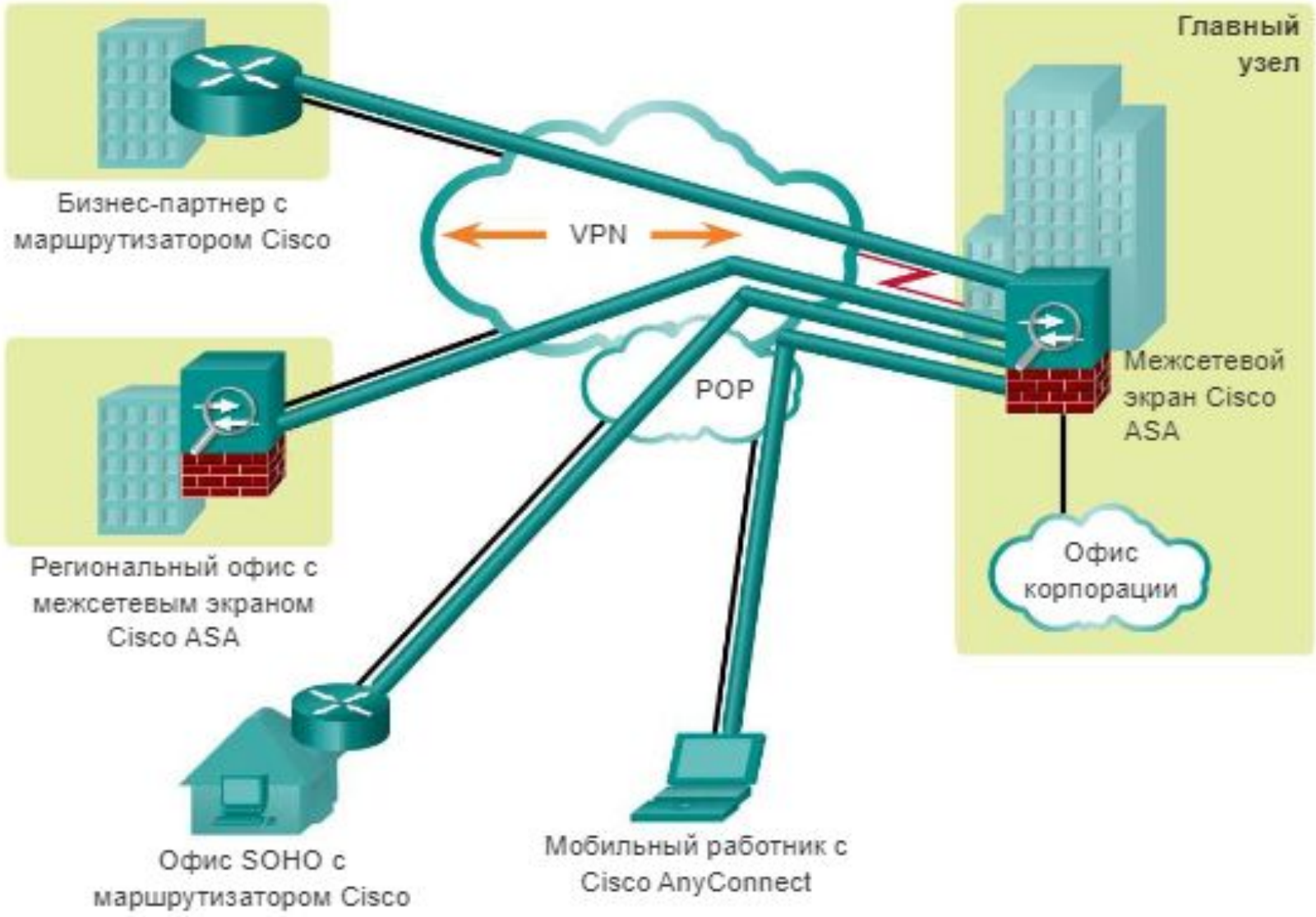
1. Краткое определение сетей VPN
2. Некоторые общие факты о VPN
3. IPsec как возможность защиты VPN
4. Способы использования туннелирования в сетях VPN

Основы сетей VPN

Организациям требуются безопасные, надёжные и недорогие способы соединения между собой нескольких сетей, которые позволят подключать филиалы и поставщиков к сети главного офиса корпорации.

Кроме того, с учётом увеличения количества удалённых сотрудников предприятиям всё чаще требуются безопасные, надёжные и экономичные решения для подключения сотрудников, работающих в секторе SOHO (Small Office/Home Office — малый офис/домашний офис), а также в других удалённых местоположениях, к ресурсам корпоративных узлов.

На рисунке показаны топологии, применяемые в современных сетях для подключения удалённых местоположений. В одних случаях удалённые местоположения подключаются только к центральному офису, тогда как в других случаях они подключаются к дополнительным узлам.



Организации используют сети VPN для сквозной конфиденциальной сетевой связи через сети сторонних компаний, например, через Интернет или сети экстранет. Туннель устраняет барьер, связанный с расстоянием, и позволяет удалённым пользователям получать доступ к сетевым ресурсам на центральном узле.

VPN представляет собой частную сеть, которая создаётся с помощью туннелирования в публичной сети (как правило, в Интернете).

VPN — это среда передачи данных со строгим контролем доступа, позволяющим устанавливать равноправные подключения в пределах определённого целевого сообщества.

Первые сети VPN представляли собой обычные IP-туннели, в которых проверка подлинности или шифрование данных не выполнялись.

Например, универсальная инкапсуляция при маршрутизации (Generic Routing Encapsulation, **GRE**) — это протокол туннелирования, разработанный компанией Cisco, который позволяет инкапсулировать пакеты протоколов сетевого уровня различного типа внутри IP-туннелей. Благодаря этому создаётся виртуальный канал «точка-точка» до маршрутизаторов Cisco в удалённых точках поверх IP-сети.

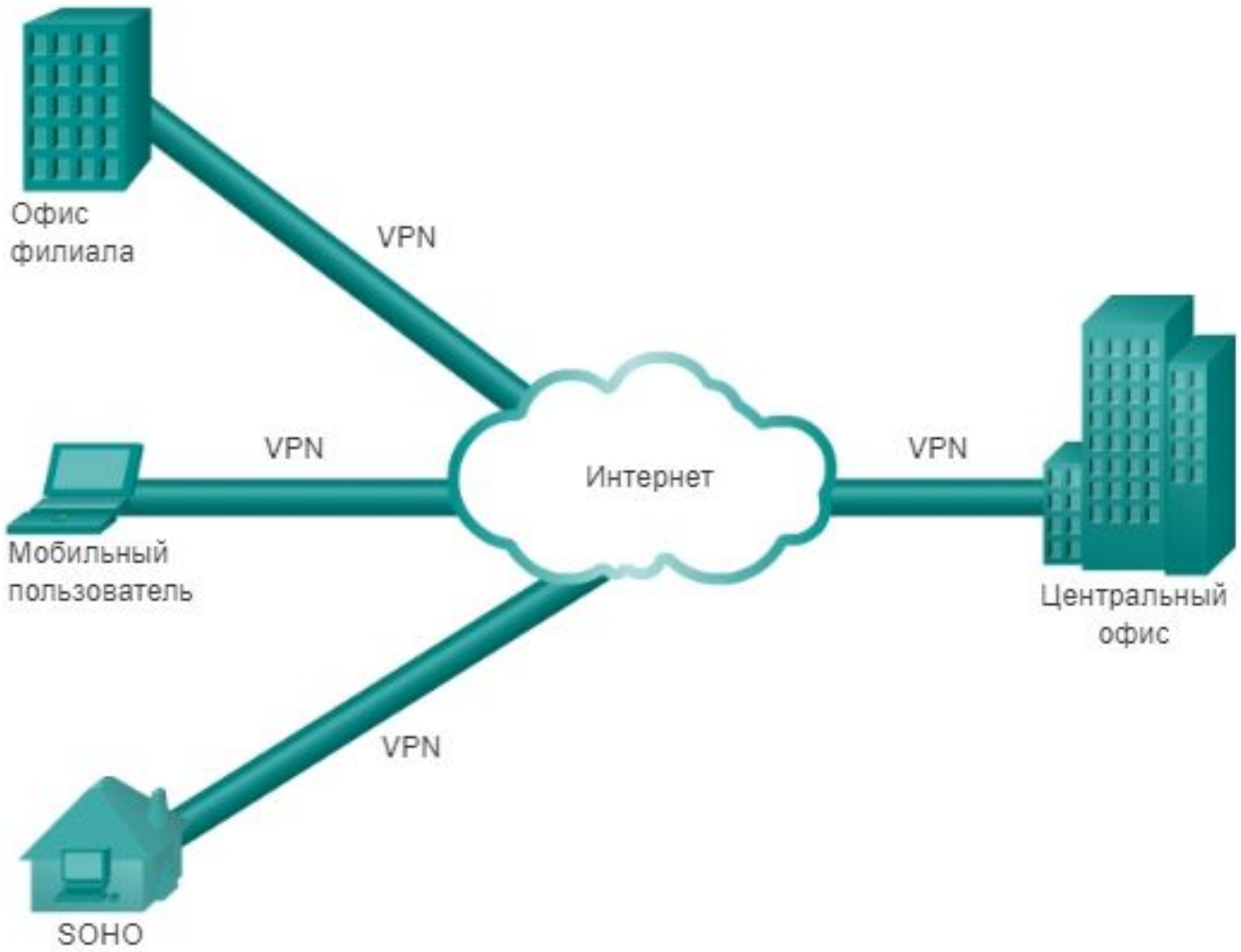
В настоящее время под виртуальными частными сетями обычно понимают защищённую реализацию сети VPN с шифрованием (например, IPsec VPN).

Для реализации сетей VPN требуется шлюз VPN. Шлюзом VPN может быть маршрутизатор, межсетевой экран или устройство адаптивной защиты Cisco ASA (Adaptive Security Appliance).

ASA — это автономный межсетевой экран, который объединяет в пределах одного образа программного обеспечения функции межсетевого экрана, концентратора VPN, а также системы предотвращения вторжений.

Преимущества VPN

Как показано на рисунке, в сети VPN применяются виртуальные подключения, которые проходят от частной сети организации через Интернет к удалённому узлу или компьютеру сотрудника. Информация, поступающая из частной сети, передаётся в защищённом режиме по публичной сети, что позволяет создать виртуальную сеть.



Ниже указаны преимущества сети VPN:

1. **Сокращение затрат** — сети VPN позволяют организациям использовать предоставляемую сторонними компаниями недорогую транспортную среду Интернета для подключения удалённых офисов и пользователей к основному узлу, то есть отказаться от применения дорогостоящих выделенных каналов WAN и банков модемов.
2. **Масштабируемость** — благодаря сетям VPN организации могут использовать инфраструктуру Интернета в пределах интернет-провайдеров и устройств, что позволяет упростить процедуру добавления новых пользователей.
3. **Совместимость с широкополосной технологией** — благодаря сетям VPN мобильные и удалённые сотрудники могут эффективно использовать высокоскоростную широкополосную связь, например, DSL и кабельные каналы, для доступа к сетям своих организаций.
4. **Безопасность** — сети VPN могут поддерживать различные механизмы защиты, обеспечивающие наивысший уровень безопасности, благодаря применению сложных протоколов шифрования и аутентификации, позволяющих защищать данные от несанкционированного доступа.

Типы сетей VPN

PPTP VPN

PPTP VPN — это протокол туннелирования точка-точка. Как видно из названия, PPTP VPN создает туннель и захватывает данные. Это самый распространенный тип VPN. PPTP VPN позволяют подключиться к сети VPN через существующее интернет-подключение. Этот тип VPN прекрасно подходит как для бизнеса, так и для домашнего использования.

Для доступа к сети используется пароль. PPTP идеальны для дома и бизнеса, так как они не требуют установки дополнительного оборудования и позволяют обходиться дешевыми и несложными приложениями. PPTP хорошо совместимы с Windows, Mac и Linux.

И хотя PPTP VPN демонстрируют множество преимуществ, не обошлось без недостатков. Главный из них — это то, что протокол PPTP не использует шифрования. Кроме того, основа PPTP — это протокол PPP, что также не обеспечивает высокий уровень безопасности.

Site-to-Site VPN

Узел-узел или Роутер-Роутер — это самый распространенный тип VPN в бизнесе. Особенно это характерно для компаний с офисами как в разных частях одной страны, так и в нескольких странах, что позволяет связать все компьютеры в единую сеть. Также они известны как интранет-VPN (VPN по внутренней сети). Другой вариант также возможен.

Компании, использующие VPN узел-узел, подключаются к серверам других компаний таким же образом, как и экстранет-VPN. Говоря простым языком, этот тип VPN — своего рода мост, соединяющий сети в разных локациях, обеспечивая безопасное соединение и подключение к интернету.

Как и PPTP, VPN типа узел-узел создает безопасную сеть. Однако, выделенная линия не предусмотрена, так что разные компьютеры компании могут подключаться к сети. В отличие от PPTP, шифрование производится либо при помощи специальных устройств, либо при помощи приложений на обоих концах сети.

L2TP VPN

L2TP означает «Протокол туннелирования второго уровня», он был разработан компаниями Microsoft и Cisco. VPN на основе протокола L2TP сочетается с другим протоколом, что обеспечивает более безопасное соединение.

При протоколе L2TP формируется туннель между двумя точками подключения L2TP, а также при помощи другого протокола, например, IPsec, производится шифрование данных.

L2TP действует подобно PPTP. Главное сходство — отсутствие шифрования и основа на протоколе PPP. Разница же — это защита и сохранность данных. VPN на основе L2TP обеспечивают более безопасное и надежное соединение.

Ipsec

IPsec — это сокращение, означающее «Безопасность интернет-протокола». IPsec — это VPN-протокол, используемый для того, чтобы обеспечить безопасность в сети. Протокол устанавливает туннель до удаленного узла. Каждая сессия проверяется, пакеты данных шифруются, так что протокол IPsec обеспечивает высокий уровень безопасности соединения.

Существует два режима, в которых работает этот протокол. Транспортный и туннельный. Оба служат для защиты передачи данных между разными сетями. В транспортном режиме шифруется сообщение в пакете данных.

В туннельном режиме шифруется весь пакет данных. Преимущество использования IPsec заключается в том, что он может быть применен в дополнение к другим протоколам, чтобы повысить защиту сети.

И хотя IPsec — это полезный и удобный протокол, однако основной минус — это долгое время установки клиентских приложений.

SSL and TLS

SSL — это протокол защищенных сокетов, TLS — безопасность на транспортном уровне. Они работают как один протокол. Оба используются для создания VPN. В этом подключении веб-браузер работает как клиент, пользователь получает доступ к специальным приложениям вместо всей сети.

SSL и TSL используются в онлайн-продажах. SSL и TSL предоставляют защищенную сессию от браузера до сервера с приложением. Браузер легко переключается на SSL, не требуя никаких дополнительных действий со стороны пользователя.

Абсолютное большинство современных браузеров уже включает в себя SSL и TSL. SSL-подключение содержит https вместо http в адресе.

MPLS VPN

VPN-сервисы с поддержкой технологии многопротокольной коммутации с использованием меток (MPLS) лучше всего использовать для подключений типа сайт-к-сайту. Все потому, что **MPLS** — это наиболее гибкий вариант с максимум возможностей для адаптации.

MPLS основываются на определенных стандартах, используемых для ускорения распределения сетевых пакетов по множеству протоколов.

VPN-сервисы с поддержкой MPLS — это системы, представляющие собой VPN-сервисы, настроенные для работы с интернет-провайдерами, когда два или более сайтов могут объединиться между собой, формируя VPN, используя для этого мощности одного и того же интернет-провайдера.

Впрочем, самым большим минусом VPN-сервисов с поддержкой MPLS является тот факт, что такую сеть настроить куда сложнее, чем остальные VPN. Сложнее и вносить в нее модификации. Как следствие, услуги VPN-сервисов с поддержкой MPLS обходятся пользователям дороже.

Hybrid VPN

Гибридная сеть VPN сочетает в себе MPLS и IPSec. Оба типа используются отдельно на различных узлах. Однако, иногда узел допускает одновременное подключение обоих типов протоколов. Это делается с целью повысить надежность MPLS при помощи IPSec.

IPSec, как уже упоминалось ранее, требуют наличия определенного оборудования. Обычно это роутер или многоцелевое устройство безопасности. При его помощи данные шифруются и образуют VPN-туннель. MPLS используются на канале передачи информации при помощи передающего оборудования.
Для соединения этих двух типов VPN устанавливается шлюз, где устраняется IPSec и производится подключение к MPLS с сохранением безопасности данных.

Гибридные VPN используются компаниями, так как MPLS очень часто не подходит для их узлов. MPLS обеспечивает множество преимуществ по сравнению с общим подключением, однако цена высока. При помощи гибридной сети вы можете подключиться к центральному узлу через удаленный. Гибридные VPN наиболее дорогие, но при этом очень гибкие в настройке.

Основы GRE

Универсальная инкапсуляция при маршрутизации (Generic Routing Encapsulation, GRE) — один из примеров базового, незащищённого протокола создания туннелей для site-to-site VPN.

GRE — это протокол туннелирования, разработанный компанией Cisco, позволяющий инкапсулировать пакеты протоколов различного типа внутри IP-туннелей. Благодаря этому создаётся виртуальный канал «точка-точка» до маршрутизаторов Cisco в удалённых точках поверх IP-сети.

GRE предназначен для управления процессом передачи многопротокольного и группового IP-трафика между двумя и более площадками, между которыми связь может обеспечиваться только по IP. Он может инкапсулировать пакеты протоколов различного типа в IP-туннеле.

Как показано на рисунке, интерфейс туннеля поддерживает заголовки для всех указанных ниже протоколов:

1. Инкапсулированный протокол (или «протокол-пассажир»), например IPv4, IPv6, AppleTalk, DECnet или IPX
2. Протокол инкапсуляции (или несущий протокол), в данном случае GRE
3. Протокол доставки («протокол-транспорт»), например IP, который передаёт данные протокола инкапсуляции.

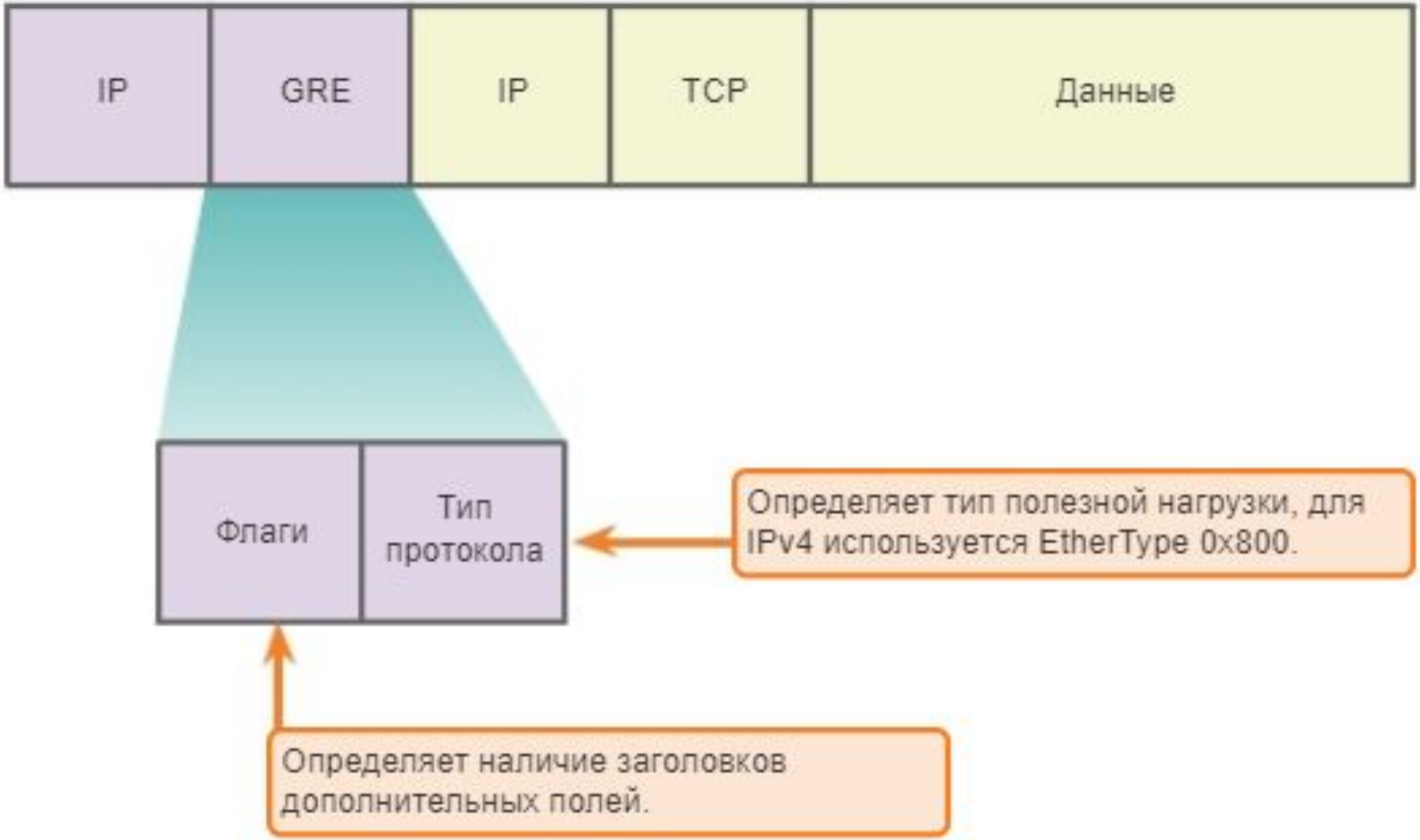
Характеристики GRE

GRE — это протокол туннелирования, разработанный компанией Cisco, который позволяет инкапсулировать пакеты протоколов различного типа внутри IP-туннелей и создавать виртуальный канал «точка-точка» до маршрутизаторов Cisco в удалённых точках поверх IP-сети.

Туннелирование IP с помощью GRE позволять расширять сеть через однопротокольную магистральную среду. Это обеспечивается путем соединения между собой различных многопротокольных подсетей в однопротокольной магистральной среде.

Протокол GRE обладает следующими характеристиками:

1. Спецификации GRE определены в стандарте IETF (RFC 2784).
2. Во внешнем заголовке IP в поле протокола используется значение 47, указывающее на то, что за ним будет следовать заголовок GRE.
3. При инкапсуляции GRE для поддержки инкапсуляции любого протокола 3 уровня модели OSI в заголовке GRE используется поле «типа протокола» (protocol type). Типы протоколов определены в стандарте RFC 1700 как «EtherTypes».
4. Сам протокол GRE является протоколом без отслеживания состояния (stateless) и по умолчанию не содержит механизмов управления потоком.
5. Для защиты полезной нагрузки в протоколе GRE отсутствуют какие-либо стойкие механизмы безопасности.
6. Заголовок GRE вместе с заголовком IP туннелирования, указанным на рисунке, создаёт, по крайней мере, 24 байта дополнительной служебной информации для туннелированных пакетов.


IP
GRE
IP
TCP
Данные
Флаги
Тип протокола
Определяет тип полезной нагрузки, для IPv4 используется EtherType 0x800.
Определяет наличие заголовков дополнительных полей.

Настройка туннелей GRE

GRE используется для создания туннеля VPN между двумя узлами, как показано на рисунке. Для реализации туннеля GRE сетевой администратор должен сначала узнать IP-адреса конечных точек туннеля.

После этого для настройки туннеля GRE следует выполнить следующую процедуру:

Шаг 1. Создайте интерфейс туннеля с помощью команды **interface tunnel number**.

Шаг 2. Укажите IP-адрес источника туннеля.

Шаг 3. Укажите IP-адрес назначения туннеля.

Шаг 4. Укажите IP-адрес для интерфейса туннеля.

Шаг 5. (Дополнительно) Укажите на интерфейсе туннеля в качестве используемого режима режим GRE Режим GRE является режимом по умолчанию для интерфейса туннеля в программном обеспечении Cisco IOS.

На рисунке приведен пример базовой настройки туннеля GRE для маршрутизатора R1.

Настройка R1:

```
R1(config)# interface Tunnel0
R1(config-if)# tunnel mode gre ip
R1(config-if)# ip address 192.168.2.1 255.255.255.0
R1(config-if)# tunnel source 209.165.201.1
R1(config-if)# tunnel destination 198.133.219.87
R1(config-if)# router ospf 1
R1(config-router)# network 192.168.2.0 0.0.0.255 area 0
```

Настройка маршрутизатора R2 на рисунке зеркальна по отношению к настройке R1.

Настройка R2:

```
R2(config)# interface Tunnel0
R2(config-if)# tunnel mode gre ip
R2(config-if)# ip address 192.168.2.2 255.255.255.0
R2(config-if)# tunnel source 198.133.219.87
R2(config-if)# tunnel destination 209.165.201.1
R2(config-if)# router ospf 1
R2(config-router)# network 192.168.2.0 0.0.0.255 area 0
```

Для минимальной настройки требуется указать адреса источника и назначения туннеля. Подсеть IP также необходимо настроить таким образом, чтобы обеспечить связь по IP через канал туннеля.

Для обоих интерфейсов туннеля в качестве источника туннеля указан локальный интерфейс serial S0/0/0, а в качестве назначения туннеля — интерфейс serial S0/0/0 маршрутизатора, с которым устанавливается туннель.

IP-адрес назначается интерфейсам туннеля на обоих маршрутизаторах. Настройка протокола OSPF также позволяет обмениваться маршрутами через туннель GRE.

Описания отдельных команд для туннеля GRE приведены на рисунке.

Команда	Описание
`tunnel mode gre ip`	Указывает, что режимом работы интерфейса туннеля является GRE по IP.
`tunnel source ip_address`	Указывает адрес источника туннеля.
`tunnel destination ip_address`	Указывает адрес назначения туннеля.
`ip address ip_address mask`	Указывает IP-адрес интерфейса туннеля.

Примечание. При настройке туннелей GRE может оказаться трудно запомнить, какие сети IP связаны с физическими интерфейсами, а какие — с интерфейсами туннеля. Следует помнить, что перед созданием туннеля GRE физические интерфейсы уже настроены.

Команды **tunnel source** и **tunnel destination** указывают на IP-адреса предварительно настроенных физических интерфейсов. Команды **ip address** на интерфейсах туннеля определяют сеть IP, созданную специально для туннеля GRE.

Настройка туннеля GRE

Для наблюдения и устранения неполадок в туннелях GRE можно использовать несколько команд. Для определения работоспособности интерфейса туннеля используйте команду **show ip interface brief**, как показано на рисунке.

```
R1# show ip interface brief | include Tunnel

Tunnel0              192.168.2.1     YES manual up      up
```

```
R1# show interface Tunnel 0
Tunnel0 is up, line protocol is up
  Hardware is Tunnel
  Internet address is 192.168.2.1/24
  MTU 17916 bytes, BW 100 Kbit/sec, DLY 50000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation TUNNEL, loopback not set
  Keepalive not set
  Tunnel source 209.165.201.1, destination 209.165.201.2
  Tunnel protocol/transport GRE/IP
<выходные данные опущены>
```

Для проверки состояния туннеля GRE используйте команду **show interface tunnel**. Протокол канального уровня в интерфейсе туннеля GRE активен до тех пор, пока существует маршрут до адреса назначения туннеля.

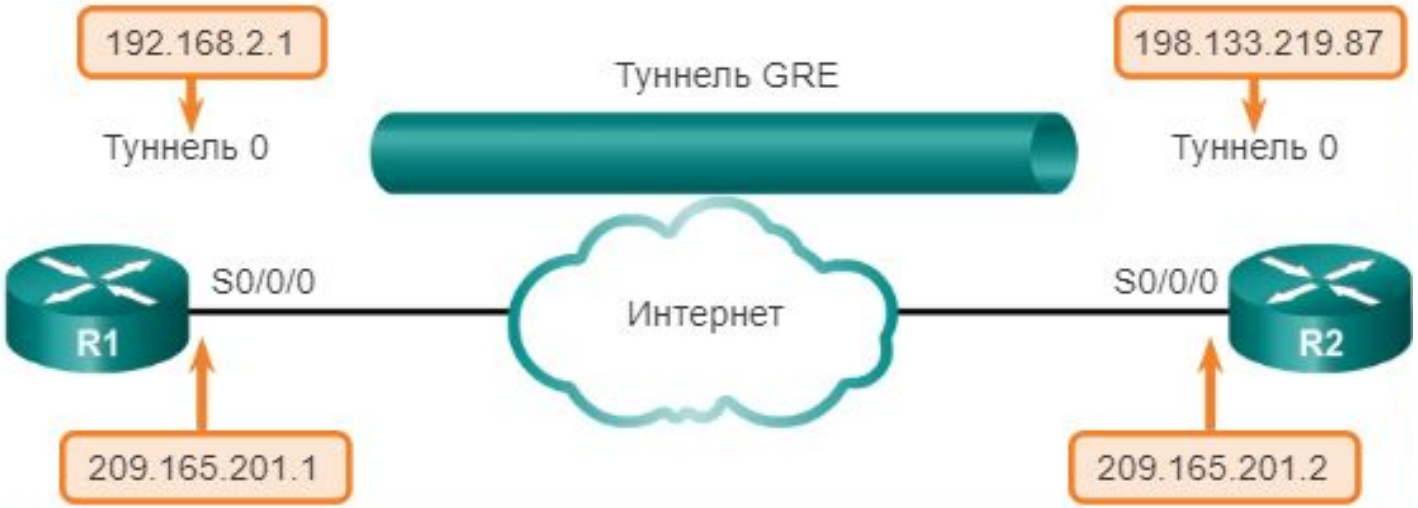
Перед реализацией туннеля GRE между IP-адресами физических интерфейсов на противоположных сторонах потенциального туннеля GRE должна уже существовать связь по IP. Транспортный протокол туннелирования отображается в выходных данных, также показанных на рисунке предыдущего слайда.

Если OSPF также настроен на обмен маршрутами по туннелю GRE, то с помощью команды **show ip ospf neighbor** убедитесь, что через интерфейс туннеля установлены отношения смежности OSPF. На рисунке видно, что адрес соседнего устройства OSPF находится в сети IP, созданной для туннеля GRE.

```
R1# show ip ospf neighbor

Neighbor ID     Pri State           Dead Time   Address     Interface
209.165.201.2   0   FULL/  -        00:00:37    192.168.2.2   Tunnel0
```

На рисунке с помощью средства проверки синтаксиса (Syntax Checker) настройте и проверьте туннель GRE на маршрутизаторе R2, а затем на R1.



Настройте маршрутизатор R2 следующим образом:

- Создайте интерфейс туннеля 0
- Для режима туннеля установите значение GRE, используя IP в качестве протокола доставки
- Назначьте IP-адрес 192.168.2.2/24
- В качестве источника туннеля введите 198.133.219.87
- В качестве назначения туннеля введите 209.165.201.1
- Настройте OSPF, используя идентификатор процесса 1
- Объявите сеть 192.168.2.0/24 для области 0

```
R2(config)#
```

Сброс | Показать | Показать всё

GRE считается VPN, так как это частная сеть, которая создаётся посредством туннелирования через публичную сеть. Благодаря инкапсуляции туннель GRE создаёт виртуальный канал «точка-точка» до маршрутизаторов Cisco в удалённых точках поверх IP-сети.

Преимущества GRE заключаются в том, что его можно использовать для туннелирования трафика, отличного от IP, по сети IP, что делает возможным расширение сети путем подключения различных многопротокольных подсетей через однопротокольную магистральную среду.

GRE также поддерживает процесс туннелирования групповой рассылки IP (IP multicast). Это означает, что в туннеле можно использовать протоколы маршрутизации, что позволяет обеспечивать динамический обмен данными о маршрутизации в виртуальной сети.

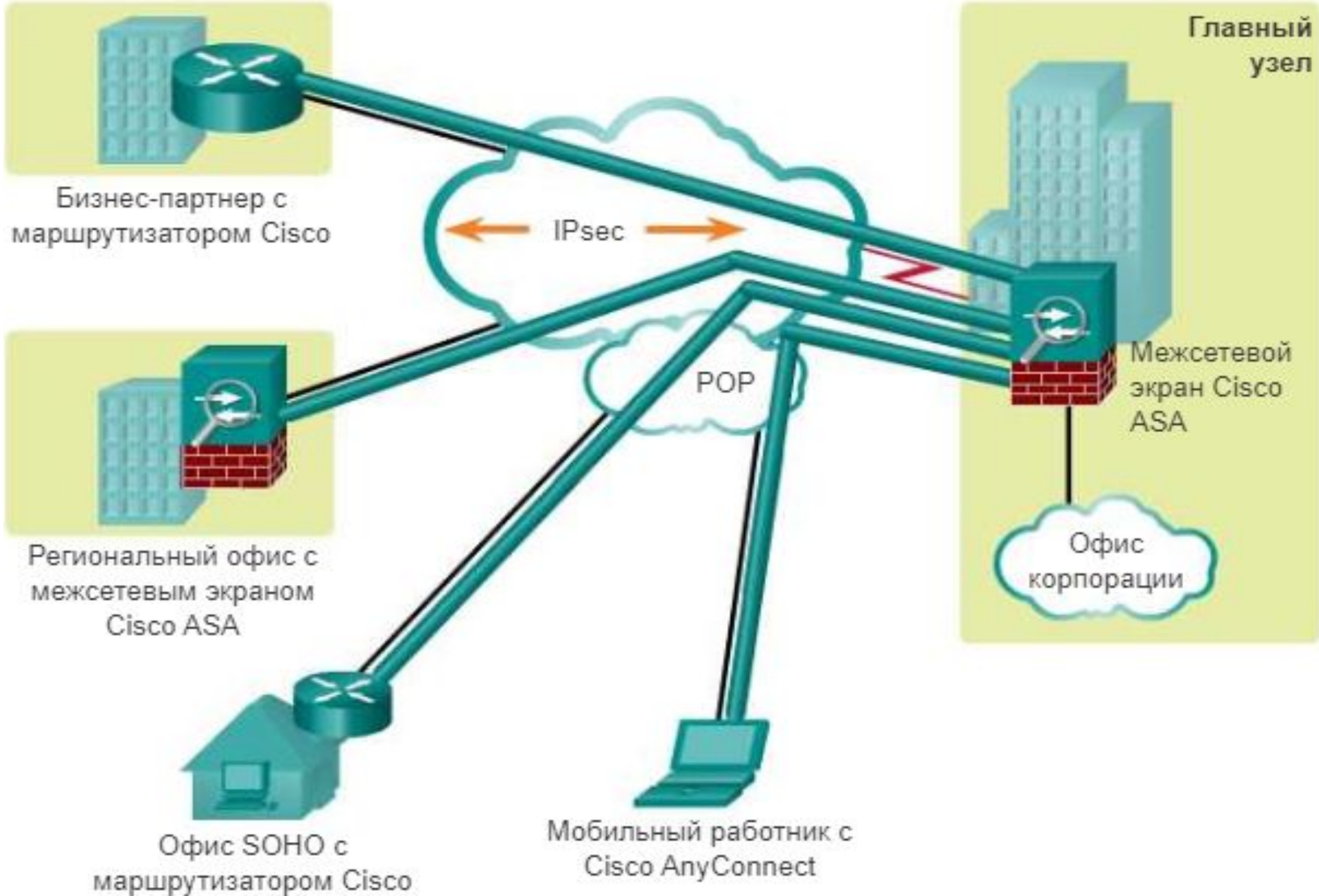
Наконец, на практике часто создаются туннели GRE «IPv6 по IPv4», где IPv6 является инкапсулированным протоколом, а IPv4 — протоколом-транспортом. В будущем их роли, очевидно, поменяются местами, так как IPv6 становится стандартным протоколом IP.

Однако GRE не обеспечивает шифрования и никаких других механизмов безопасности. Поэтому данные, отправляемые по туннелю GRE, не защищены. Если требуется безопасная передача данных, то необходимо настроить сети VPN с IPsec или с SSL.

Общие сведения об Ipsec

Сети VPN с IPsec обеспечивают гибкую и масштабируемую связь. Межфилиальные соединения могут обеспечивать безопасную, высокоскоростную и надёжную удалённую связь. При помощи VPN с IPsec информация из частной сети передаётся в защищённом режиме по публичной сети.

Благодаря этому можно создать виртуальную сеть, а не использовать выделенное подключение на 2 уровне, как показано на рисунке. Для обеспечения конфиденциальности данных трафик шифруется.


Главный узел
Бизнес-партнер с маршрутизатором Cisco
IPsec
POP
Межсетевой экран Cisco ASA
Региональный офис с межсетевым экраном Cisco ASA
Офис корпорации
Офис SOHO с маршрутизатором Cisco
Мобильный работник с Cisco AnyConnect

IPsec — это стандарт IETF, который определяет способ настройки сети VPN в защищённом режиме с помощью протокола IP.

IPsec представляет собой структуру открытых стандартов, определяющую правила для организации защищённой связи. Протокол IPsec не связан с конкретными методами шифрования и аутентификации, алгоритмами обеспечения безопасности или технологией обмена ключами.

Для обеспечения безопасной связи в протоколе IPsec используются существующие алгоритмы. IPsec позволяет создавать новые, более качественные алгоритмы, для разработки которых корректировать существующие стандарты IPsec не потребуется.

Защита протокола IP

IPsec функционирует на сетевом уровне, обеспечивая защиту и аутентификацию пакетов IP между взаимодействующими устройствами IPsec, которые также называются узлами (peer). IPsec позволяет защитить путь между парой шлюзов, парой компьютеров или между шлюзом и компьютером.

В результате IPsec может защищать практически любой трафик приложений, так как можно реализовать защиту на уровнях с 4-го по 7-й.

Во всех реализованных решениях протокола IPsec применяется незашифрованный заголовок 3-го уровня, поэтому никаких проблем с маршрутизацией не существует. IPsec функционирует поверх любых протоколов 2-го уровня, таких как Ethernet, ATM и Frame Relay.

Ниже указаны основные особенности протокола IPsec:

1. **IPsec** — это структура открытых стандартов, независимая от алгоритмов.
2. IPsec обеспечивает конфиденциальность и целостность данных, а также аутентификацию источника.
3. IPsec действует как протокол сетевого уровня, защищая пакеты IP и проверяя их подлинность.

Сервисы безопасности Ipsec

На рисунке (слайд №39) показано, что сервисы безопасности IPsec выполняют следующие важные функции:

1. **Конфиденциальность (шифрование)** — в сети VPN частные данные передаются по публичной сети. Поэтому ключевой задачей является обеспечение конфиденциальности данных. Для этого перед передачей данных по сети выполняется шифрование данных.

Шифрование — это процесс кодирования всех данных, отправляемых с одного компьютера на другой, в ту форму, которую может декодировать только принимающий компьютер. В случае перехвата сообщения злоумышленник (хакер) не сможет его прочесть. IPsec предоставляет расширенные функции безопасности (например, криптостойкие алгоритмы шифрования).

2. Целостность данных — Получатель может убедиться, что данные были нормально переданы через Интернет и никак не были изменены. Важно не только обеспечить шифрование данных в публичной сети, но и убедиться, что они не были изменены в пути.

3. Аутентификация — позволяет проверить, кто был источником отправленных данных. Это необходимо для защиты от атак, использующих спуфинг (подмену отправителя). Аутентификация позволяет гарантировать установление подключения к нужному партнеру по связи. Получатель может проверять подлинность источника пакета, сертифицируя источник информации.

4. Защита от повторов — позволяет обнаруживать и отклонять повторные пакеты, а также предотвращать спуфинг. Благодаря защите от повторов можно убедиться, что пакет является уникальным и не дублированным.

Сокращение CIA (ЦРУ) во многих случаях позволяет вспомнить четыре эти функции:

1. **Конфиденциальность(confidentiality)**
2. **Целостность (integrity)**
3. **Проверка подлинности (authentication)**
4. **Защита от повторов (Repeat Protection)**

Конфиденциальность

Целостность данных

Аутентификация

16	24	32 бита
Идентификатор ассоциации безопасности (SPI)		
Порядковый номер		
Полезная нагрузка (переменной длины)		
Заполнение (0-255 байт)		
	Длина заполнителя	Следующий заголовок
Данные аутентификации (переменные)		

Защита от повторов

Конфиденциальность и шифрование

Конфиденциальность трафика VPN поддерживается с помощью шифрования. Открытые (незашифрованные) данные, передаваемые через Интернет, могут быть перехвачены и прочитаны.

Для сохранения приватности данных используется шифрование. Благодаря цифровому шифрованию данных они остаются нечитаемыми до тех пор, пока не будут расшифрованы авторизованным получателем.

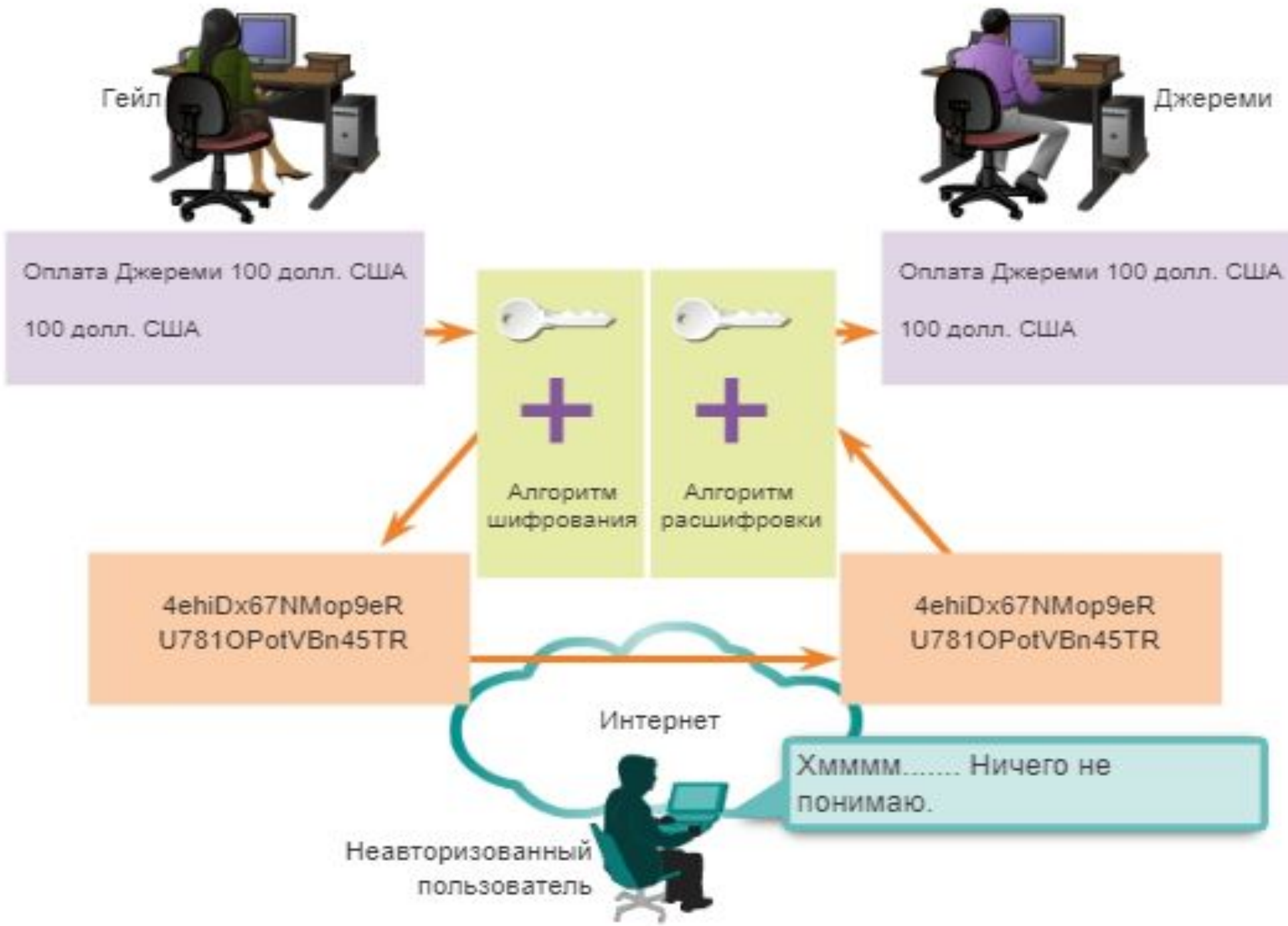
Для обеспечения зашифрованного режима связи и отправитель, и получатель должны знать правила, используемые для преобразования исходного сообщения в закодированную форму. Правила основаны на алгоритмах и соответствующих ключах.

В контексте шифрования алгоритм представляет собой математическую последовательность действий, в которой сообщение, текст, цифры или все они сочетаются со строкой цифр, называемой ключом.

Выходные данные предстают в виде нечитаемой зашифрованной строки. Алгоритм шифрования также определяет способ расшифровки зашифрованного сообщения. Без правильного ключа дешифровать данные практически невозможно.

На рисунке (Слайд №42) видно, что Гейл хочет выполнить электронный перевод денежных средств через Интернет к Джереми. На локальной стороне документ объединяется с ключом и подвергается процедуре шифрования.

Выходные данные представляют собой шифр текст. Затем этот шифр текст посылается через Интернет. На удалённой стороне сообщение снова объединяется с ключом и пропускается через алгоритм шифрования в обратном направлении. Выходные данные представляют собой исходный финансовый документ.


Гейл
Джереми
Оплата Джереми 100 долл. США
100 долл. США
Оплата Джереми 100 долл. США
100 долл. США
Алгоритм шифрования
Алгоритм расшифровки
4ehiDx67NMop9eR
U781OPotVBn45TR
4ehiDx67NMop9eR
U781OPotVBn45TR
Интернет
Хммммм..... Ничего не понимаю.
Неавторизованный пользователь

Конфиденциальность достигается шифрованием трафика при передаче через VPN. Степень безопасности зависит от длины ключа в алгоритме шифрования и сложности самого алгоритма.

Если хакер попытается взломать ключ посредством атаки методом последовательного перебора, то количество вариантов для перебора будет зависеть от длины ключа.

Время обработки всех возможных вариантов зависит от вычислительной мощности компьютера злоумышленника. Поэтому чем короче ключ, тем проще его взломать.

Например, если для взлома 64-битового ключа относительно мощному компьютеру понадобится приблизительно один год, то для взлома 128-битового ключа тому же компьютеру может понадобиться от 10 до 19 лет.

Алгоритмы шифрования

Степень безопасности зависит от длины ключа в алгоритме шифрования. По мере увеличения длины ключа вероятность взлома шифра уменьшается. Однако, чем длиннее ключ, тем больше ресурсов процессора будет требоваться при шифровании и расшифровывании данных.

Алгоритмы DES и 3DES больше не считаются надёжными, поэтому для шифрования в протоколе IPsec рекомендуется использовать AES. Наивысший уровень безопасности для шифрования сетей VPN между устройствами Cisco с помощью протокола IPsec обеспечивается 256-битовым вариантом AES.

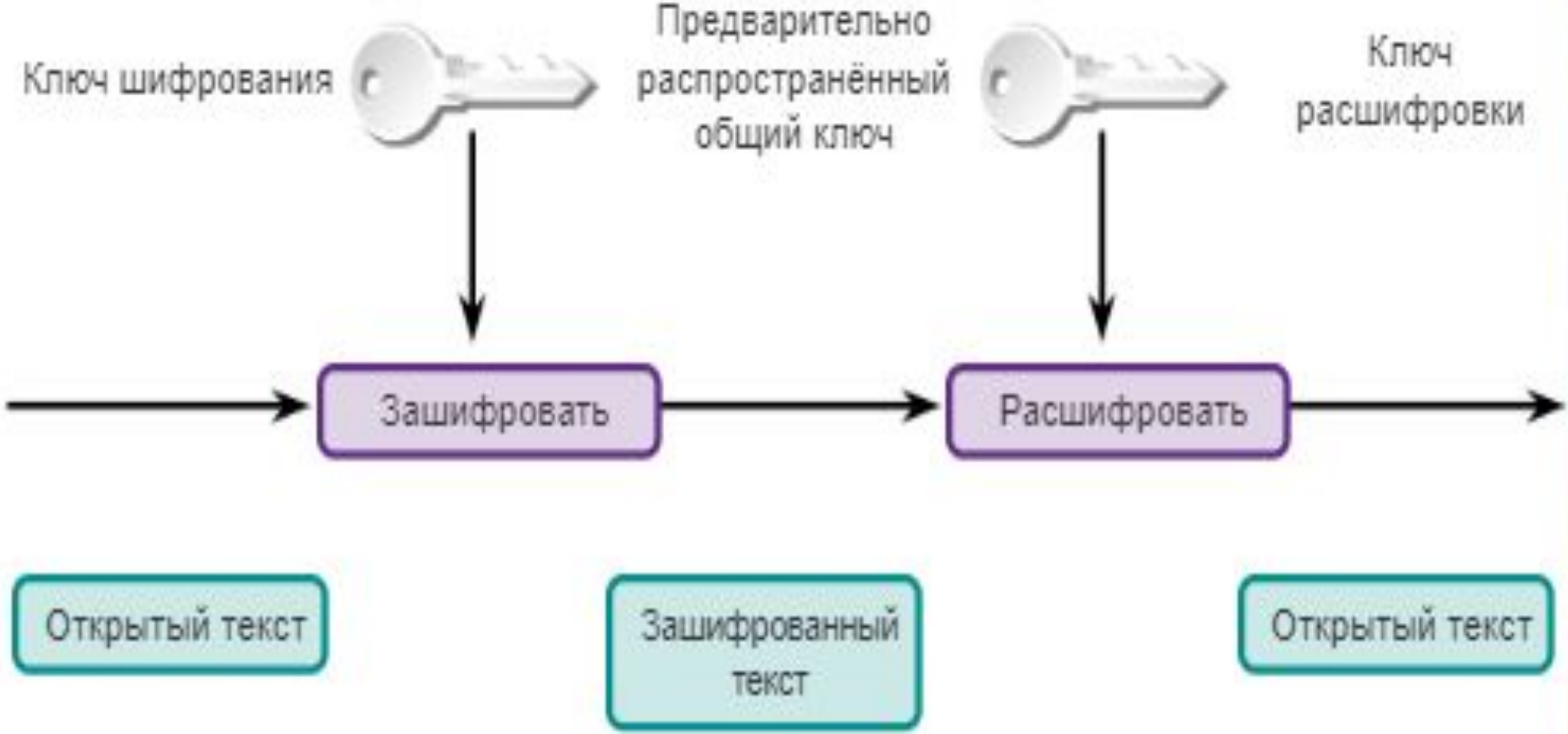
Кроме того, с учетом взлома 512- и 768-битовых ключей Ривеста-Шамира-Эдльмана (RSA) компания Cisco рекомендует использовать 2048-битовые ключи в варианте RSA (если он применяется на этапе аутентификации IKE).

Симметричное шифрование

В алгоритмах шифрования, например, AES, требуется общий секретный ключ для выполнения как шифрования, так и расшифровки. Для декодирования информации ключ должны знать оба сетевых устройства.

При шифровании с помощью симметричного ключа (также называемом шифрованием с помощью секретного ключа) каждое устройство шифрует данные перед их отправкой по сети на другое устройство.

При шифровании с помощью симметричного ключа необходимо знать, какие устройства общаются друг с другом, чтобы на каждом устройстве было можно настроить один и тот же ключ (Слайд №46).


Ключ шифрования
Предварительно распространённый общий ключ
Ключ расшифровки
Зашифровать
Расшифровать
Открытый текст
Зашифрованный текст
Открытый текст

Например, отправитель создаёт кодированное сообщение, где каждая буква меняется на букву, следующую через две буквы ниже в алфавите (то есть A становится C, B становится D и т. д.). В этом случае слово SECRET превращается в UGETGV. Отправитель уже сообщил получателю, что секретный ключ — это смещение на 2.

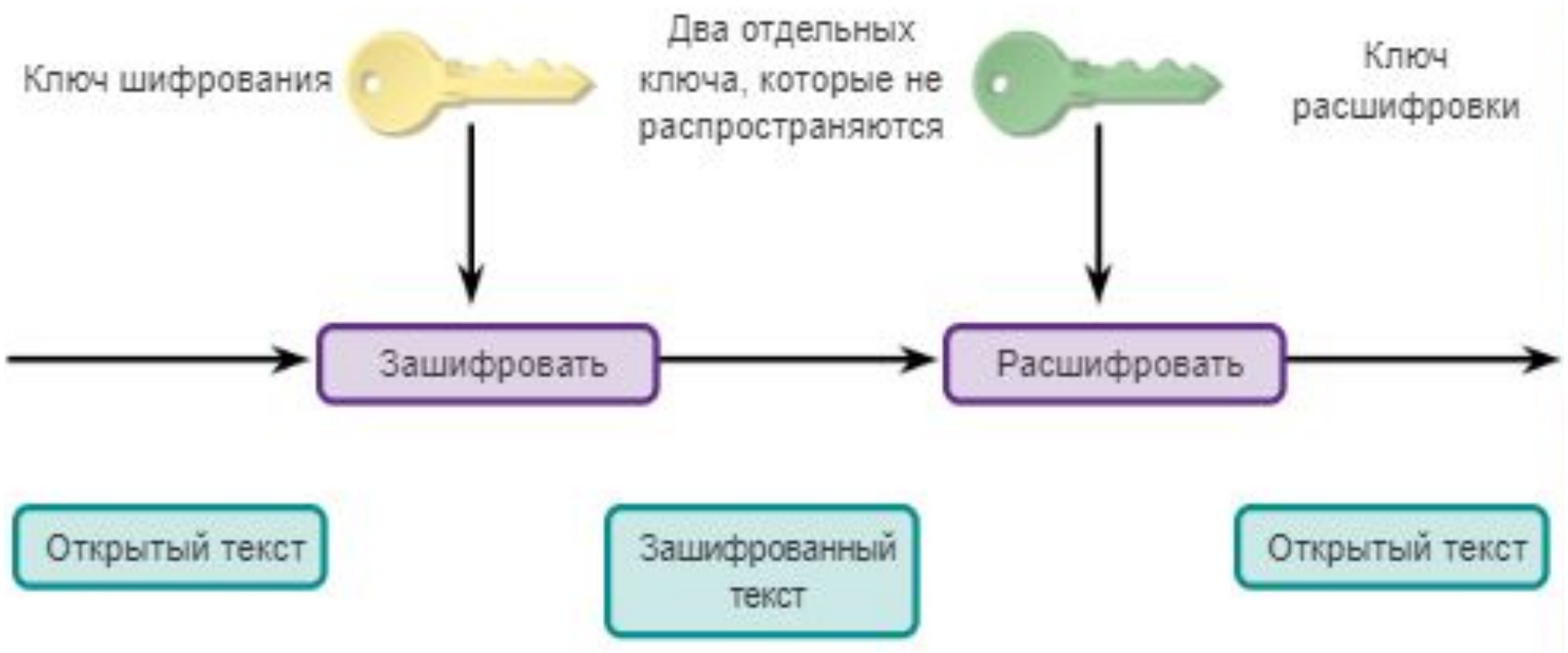
Когда получатель получает сообщение UGETGV, его компьютер раскодирует сообщение путем обратного смещения на две буквы и получает слово SECRET. Любой другой пользователь, смотрящий на это сообщение, видит его в зашифрованном виде. Чтобы такое сообщение не выглядело абракадаброй, необходимо знать секретный ключ.

Ниже указаны особенности симметричных алгоритмов:

1. Используется криптография на основе симметричных ключей;
2. При шифровании и расшифровке используется один и тот же ключ;
3. Обычно используется для шифрования содержимого сообщения.
4. Примеры: DES, 3DES и AES

Асимметричное шифрование

При асимметричном шифровании для шифрования и расшифровки используются разные ключи. Знание одного из ключей не позволяет хакеру вычислить второй ключ и декодировать информацию. Один ключ служит для зашифровывания сообщения, второй для его расшифровывания. Выполнять операцию шифрования и расшифровки с помощью одного и того же ключа нельзя.



Одним из вариантов асимметричного шифрования является шифрование открытым ключом, где применяется сочетание секретного и открытого (публичного) ключей. Получатель предоставляет открытый ключ любому отправителю, с которым данному получателю нужно общаться.

Для зашифровывания сообщения отправитель использует секретный ключ, который объединяется с открытым ключом получателя. Кроме того, отправитель должен сообщить свой открытый ключ получателю. Для расшифровки сообщения получатель будет использовать открытый ключ отправителя вместе со своим собственным секретным ключом.

Ниже указаны особенности асимметричных алгоритмов:

1. Используется криптография с открытым ключом
2. При шифровании и расшифровке используются разные ключи
3. Обычно применяется при управлении цифровыми сертификатами и ключами
4. Примеры: RSA

Обмен ключами Диффи – Хеллмана (Diffie Hellman)

Алгоритм Диффи-Хеллмана (DH) не является механизмом шифрования и обычно не используется для шифрования данных. Он позволяет обеспечивать безопасный обмен ключами, которые используются для шифрования данных.

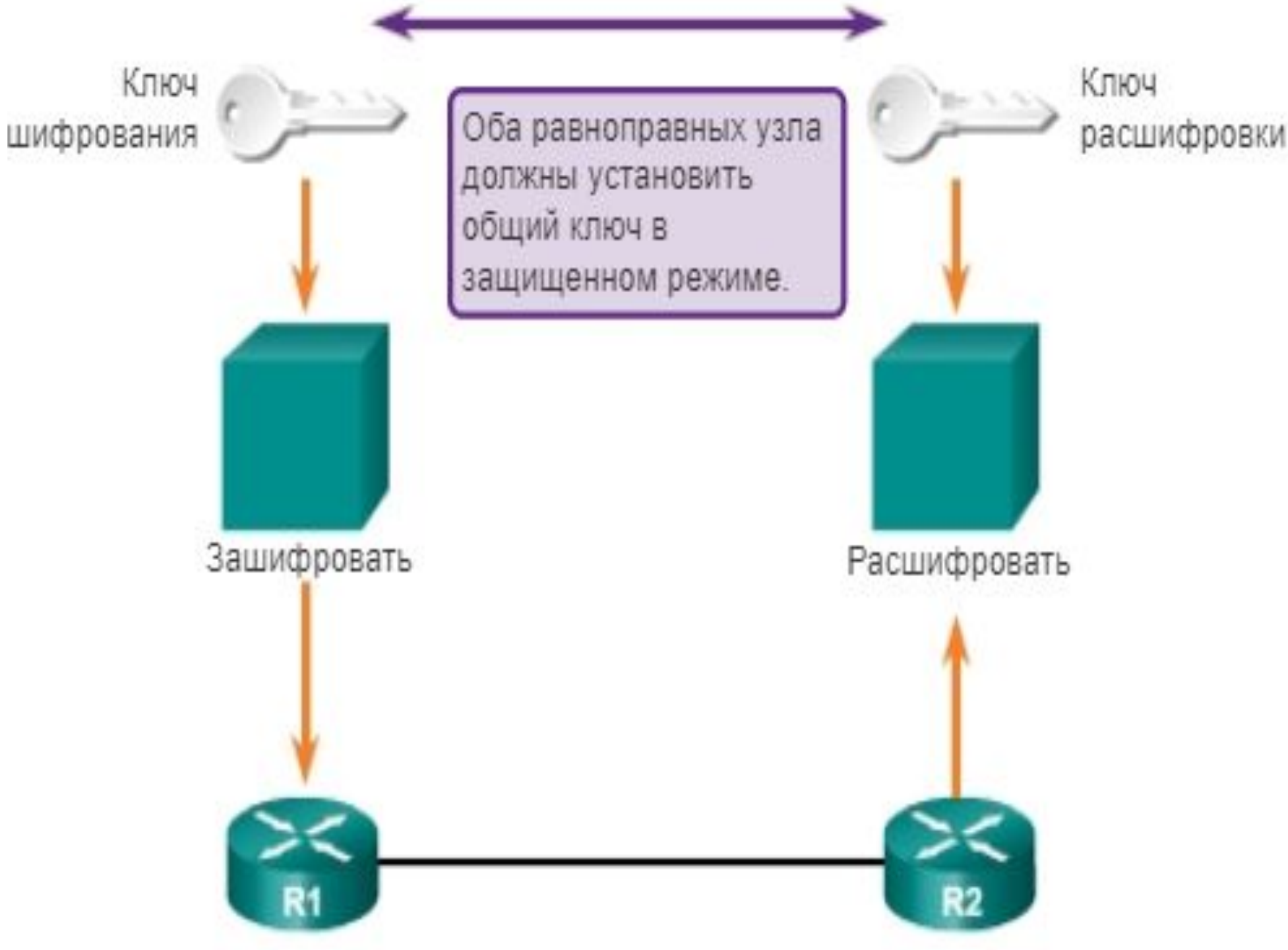
Алгоритмы DH позволяют двум сторонам установить общий секретный ключ, который используется алгоритмами шифрования и хеширования.

Алгоритм DH, разработанный Уитфилдом Диффи и Мартином Хеллманом в 1976 г., стал первой системой, где применялись открытый ключ или асимметричные криптографические ключи. В настоящее время DH является составной частью стандарта IPsec.

Кроме того, алгоритм DH применяется в протоколе OAKLEY. OAKLEY используется протоколом IKE, представляющим собой общую структуру, которая называется протоколом ассоциаций безопасности и управления ключами в Интернете (Internet Security Association and Key Management Protocol, ISAKMP).

Для выполнения шифрования и расшифровки алгоритмам шифрования (например DES, 3DES и AES), а также алгоритмам хеширования MD5 и SHA-1 требуется симметричный общий секретный ключ.

Каким образом зашифровывающее и расшифровывающее устройства могут получить информацию об общем секретном ключе? Самым простым методом обмена ключами является метод обмена открытым ключом между зашифровывающим и расшифровывающим устройствами.


Ключ шифрования
Оба равноправных узла должны установить общий ключ в защищенном режиме.
Ключ расшифровки
Зашифровать
Расшифровать
R1
R2

Целостность и алгоритмы хеширования

Для обеспечения целостности и проверки подлинности трафика сети VPN применяются алгоритмы хеширования. Целостность данных и проверка подлинности обеспечиваются хеш-кодами, которые гарантируют отсутствие искажений передаваемых сообщений неавторизованными лицами.

Хеш-код, также называемый дайджестом сообщения, представляет собой число, который создаётся из строки текста. Хеш-код имеет меньший размер, чем сам текст. Он создаётся с помощью формулы таким образом, что получение такого же значения хеш-кода из другого текста крайне маловероятно.

Исходный отправитель создаёт хеш-код сообщения и отправляет его вместе с самим сообщением. Получатель анализирует сообщение и хеш-код, создаёт другой хеш-код на основе полученных сообщений и сравнивает оба хеш-кода. Если они совпадают, то получатель может быть с достаточным основанием уверен в целостности исходного сообщения.

На рисунке показано, что Гейл отправил Алексу электронный денежный перевод в размере 100 долл. США. Джереми перехватил и изменил данный перевод таким образом, чтобы показать, что он является получателем, а сумма перевода составляет 1000 долл. США. В этом случае, если использовался алгоритм целостности данных, то хеш-коды не совпадут друг с другом, и транзакция окажется недействительной.

Данные VPN передаются через Интернет общего доступа. Как показано на рисунке, существует вероятность перехвата и изменения этих данных. Для защиты от этой угрозы на компьютерах в сообщение могут добавляться хеш-коды.

Если переданный хеш-код совпадает с полученным хеш-кодом, это означает, что обеспечена целостность сообщения. Однако если хеш-коды не совпадают, то сообщение было изменено.

Для проверки целостности и подлинности сообщения в сетях VPN используется код аутентификации без использования каких-либо дополнительных механизмов.

Код аутентификации сообщений на основе хешей (**Hash-based Message Authentication Code, HMAC**) — это механизм аутентификации сообщений с помощью функций хеширования. HMAC с обменом ключами представляет собой алгоритм целостности данных, гарантирующий целостность сообщения.

HMAC имеет два параметра:

1. Вводимое сообщение и секретный ключ (известный только автору сообщения)
2. Предполагаемым получателям

Отправитель сообщения использует функцию HMAC для создания значения (кода аутентификации сообщения), формируемого путем переработки секретного ключа и вводимого сообщения. Код аутентификации сообщения отправляется вместе с сообщением.

Получатель вычисляет код аутентификации сообщения в полученном сообщении с помощью того же ключа и функции HMAC, которые использовал отправитель.

Затем получатель сравнивает вычисленный результат с полученным кодом аутентификации сообщения. Если оба значения совпадают, это означает, что получено правильное сообщение, а получатель может быть уверен в том, что отправитель является членом сообщества пользователей, применяющих данный общий ключ.

Существуют два наиболее распространённых алгоритма HMAC:

1. **MD5** — используется 128-битовый общий секретный ключ. Сообщение произвольной длины и 128-битовый общий секретный ключ объединяются друг с другом и обрабатываются алгоритмом хеширования HMAC-MD5. В результате создаётся 128-битовый хеш-код. Хеш-код добавляется к исходному сообщению и перенаправляется на удалённую сторону.

2. **SHA** — в SHA-1 используется 160-битовый общий секретный ключ. Сообщение переменной длины и 160-битовый общий секретный ключ объединяются друг с другом и обрабатываются алгоритмом хеширования HMAC-SHA1. В результате создаётся 160-битовый хеш-код. Хеш-код добавляется к исходному сообщению и перенаправляется на удалённую сторону.

Примечание. В ОС Cisco IOS также поддерживаются 256-, 384- и 512-битовые варианты SHA.

Аутентификация Ipsec

В сетях IPsec VPN поддерживается функция аутентификации. Если ваши партнеры по бизнесу находятся от вас на большом расстоянии, то важно знать, с кем вы говорите по телефону, кто отправляет вам электронное сообщение или факс. Это же справедливо и для сетей VPN.

Как указано на рисунке, подлинность устройства на другом конце туннеля VPN должна быть проверена, прежде чем можно будет считать, что канал связи является защищённым.

Существуют два метода аутентификации собеседника:

1. **PSK** — секретный ключ, заранее известный двум пользователям, которые общаются по защищённому каналу. В методе предварительно распространённых общих ключей (PSK) используются криптографические алгоритмы с симметричным ключом.
2. **Подписи RSA** — для аутентификации равноправных узлов выполняется обмен цифровыми сертификатами. Локальное устройство создаёт хеш-код и шифрует его с помощью своего закрытого ключа.

В алгоритме IPsec для аутентификации в контексте IKE (Internet Key Exchange) — стандартный протокол набора протоколов Ipsec) используется алгоритм RSA (криптографическая система с открытым ключом).

В RSA применяется схема цифровой подписи, благодаря которой каждое устройство прикрепляет цифровую подпись к набору данных и передаёт его другому пользователю.

Для создания цифрового сертификата с уникальным идентификатором, назначаемого каждому равноправному узлу для аутентификации, в алгоритме подписывания RSA используется центр сертификации (CA).

Сам цифровой сертификат идентификации похож на ключ PSK, но обеспечивает гораздо более высокий уровень безопасности.

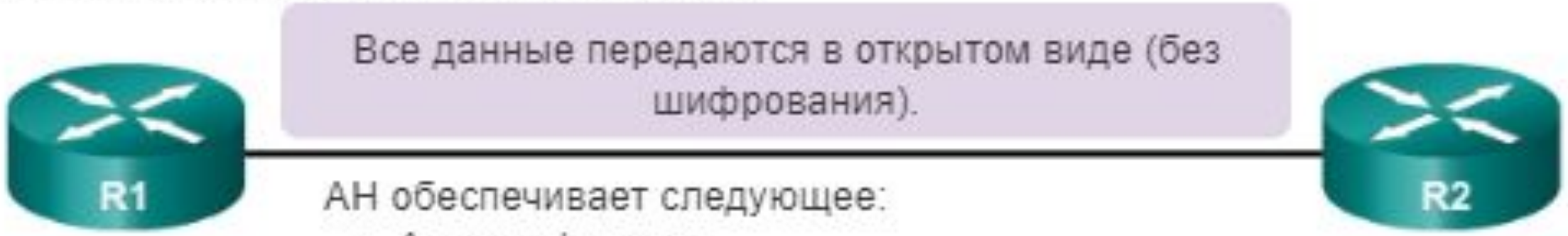
Структура протокола Ipsec

Как указано выше, набор протоколов IPsec описывает способ обмена сообщениями для защиты сеансов связи, но он основан на применении существующих алгоритмов.

На рисунке (Слайд №62) показаны два основных протокола IPsec:

1. **Аутентифицирующий заголовок (Authentication Header, AH)** — AH представляет собой специальный протокол, применяемый в тех случаях, когда обеспечение конфиденциальности не требуется или запрещено. Он обеспечивает аутентификацию и целостность данных для пакетов IP, передаваемых между двумя системами.
2. **Протокол шифрования полезной нагрузки (Encapsulating Security Payload, ESP)** — это протокол безопасности, который обеспечивает конфиденциальность и аутентификацию путем шифрования пакета IP. В процессе шифрования пакета IP скрываются данные и идентификаторы источника и назначения.

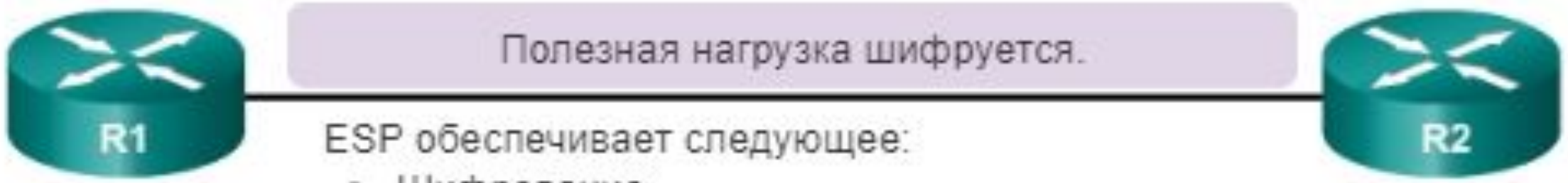
Аутентифицирующий заголовок (AH)



AH обеспечивает следующее:

- Аутентификация
- Целостность

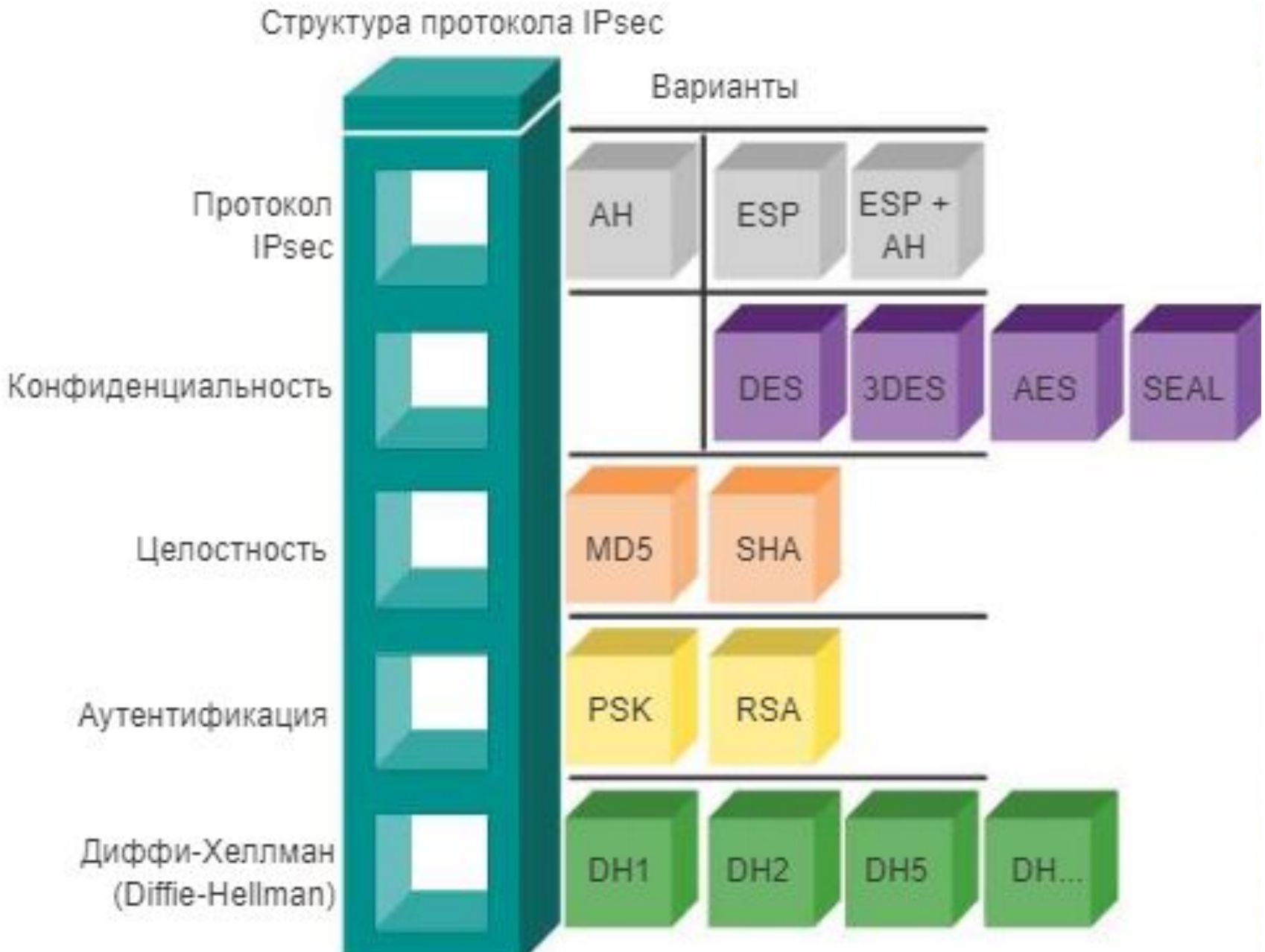
Шифрование полезной нагрузки (ESP)



ESP обеспечивает следующее:

- Шифрование
- Аутентификация
- Целостность

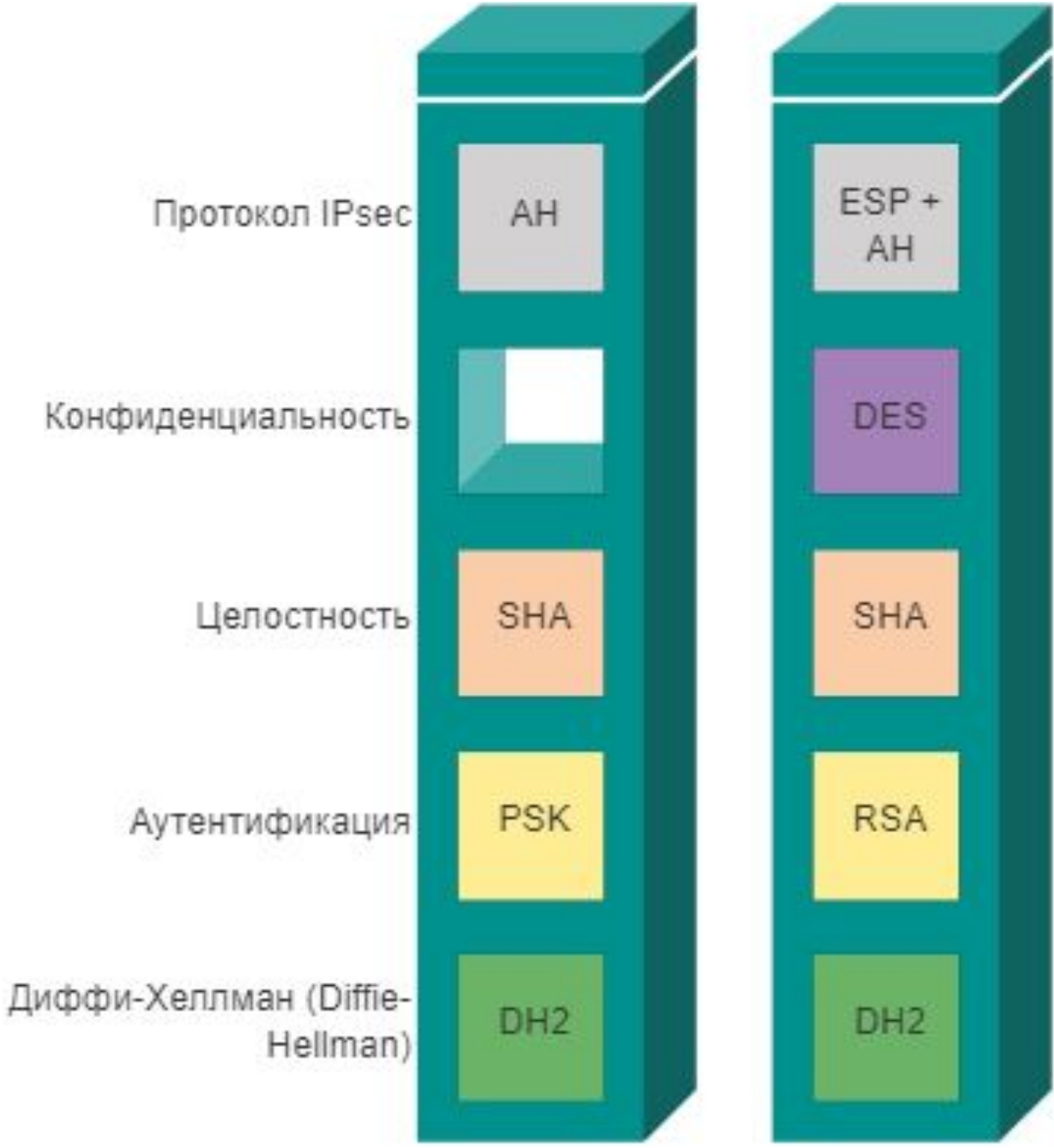
На рис. 21 показаны компоненты настройки IPsec.



Существует пять основных компоновочных блока структуры IPsec, которые необходимо выбрать:

1. **Набор протоколов IPsec** — при настройке шлюза IPsec для предоставления услуг безопасности необходимо выбрать, какие из протоколов IPsec будут использоваться. Можно выбрать как использование только ESP или только AH, так и совместное использование ESP и AH.

На практике почти всегда используют варианты ESP или ESP+AH, так как сам AH не предоставляет функцию шифрование данных.



2. Конфиденциальность (если выбран вариант использования IPsec с протоколом ESP) — выбранный алгоритм шифрования должен наилучшим образом обеспечивать требуемый уровень безопасности: DES, 3DES или AES.

3. Целостность — гарантирует, что содержимое не было изменено в процессе передачи. Для выполнения данной функции применяются алгоритмы хеширования. Можно выбрать MD5 и SHA.

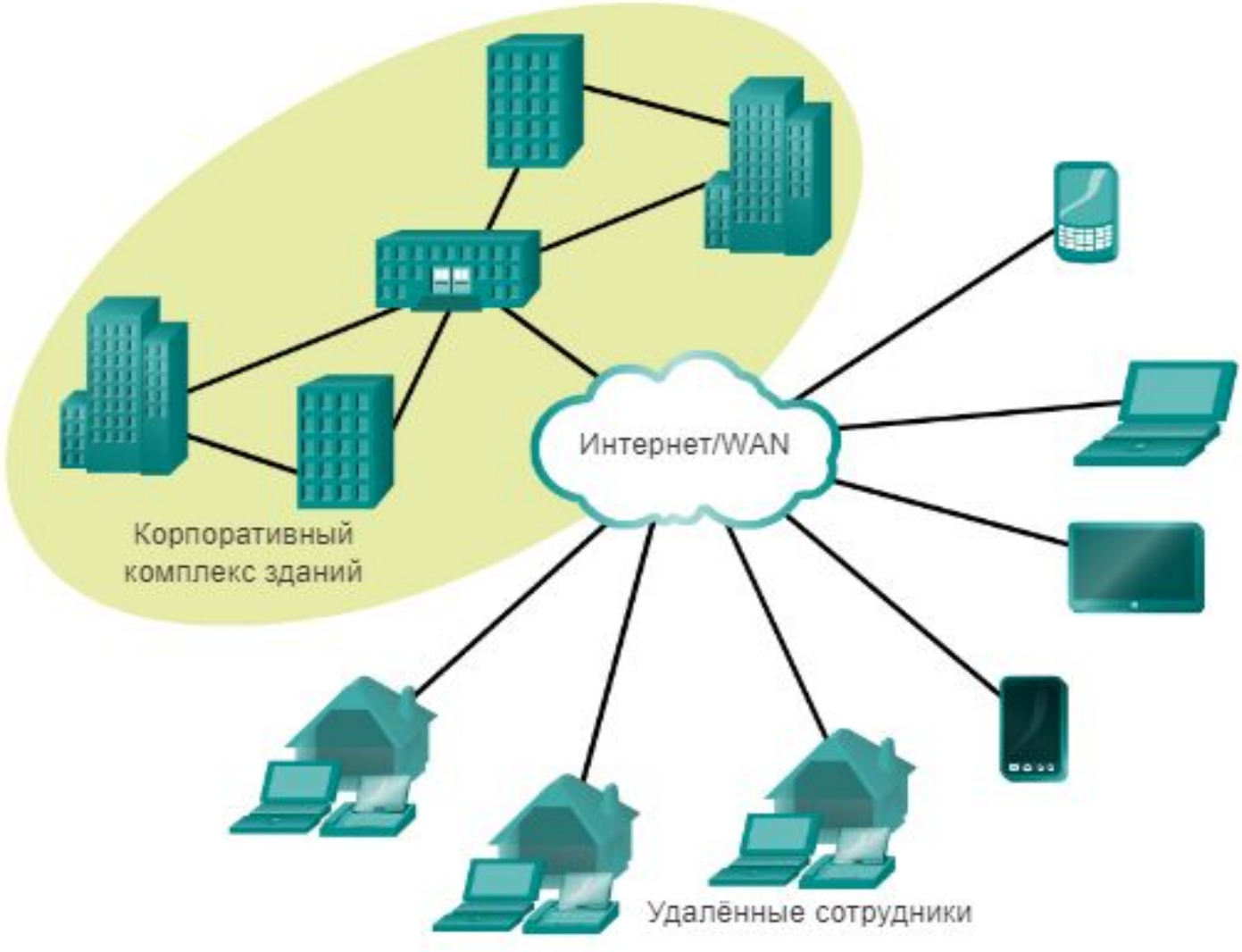
4. Аутентификация — определяет способ проверки подлинности устройств на обоих концах туннеля VPN. Доступные варианты: PSK или RSA.

5. Группа алгоритмов DH — определяет способ генерации общего секретного ключа между узлами. Существует несколько вариантов, но DH24 обеспечивает наивысший уровень безопасности.

Удаленный доступ

Сети VPN стали логичным решением для организации удалённого доступа по многим причинам. Они обеспечивают безопасную связь с соответствующими правами доступа для отдельных пользователей, например, сотрудников, подрядчиков и партнеров.

Они также позволяют повысить уровень производительности путем безопасного расширения корпоративной сети и приложений, снижения затрат на организацию связи и повышения гибкости.



Решение VPN для удаленного доступа

Существуют два основных способа развёртывания сетей VPN для создания удалённого доступа:

1. Secure Sockets Layer (SSL)
2. Протокол Ipsec

Используемый метод создания сети VPN основан на требованиях к доступу пользователей, а также процедурах ИТ в организации. Технологии IPsec и SSL VPN делают возможным доступ практически к любому сетевому приложению или ресурсу.

Сети VPN на основе SSL предлагают такие функции, как простое установление связи с настольных систем, не находящихся под управлением компании, минимальное сопровождение ПО настольных компьютеров или его полное отсутствие и веб-порталы, настраивающиеся под пользователя при его входе в систему.

Cisco SSl VPN

Cisco IOS SSL VPN представляет собой первое в своей отрасли решение SSL VPN на основе маршрутизатора.

Данное решение обеспечивает «повсеместную» связь не только для компьютеров, находящихся под управлением компании, но и для принадлежащих сотрудникам ПК, настольных компьютеров подрядчиков и бизнес-партнеров, а также терминалов для доступа к Интернету.

Протокол SSL поддерживает различные алгоритмы шифрования для таких операций, как взаимная проверка подлинности сервера и клиента, передача сертификатов и настройка сеансовых ключей.

Решения Cisco SSL VPN можно настраивать для предприятий любого размера. Эти решения предоставляют множество возможностей и преимуществ системы удалённого доступа, к которым относятся:

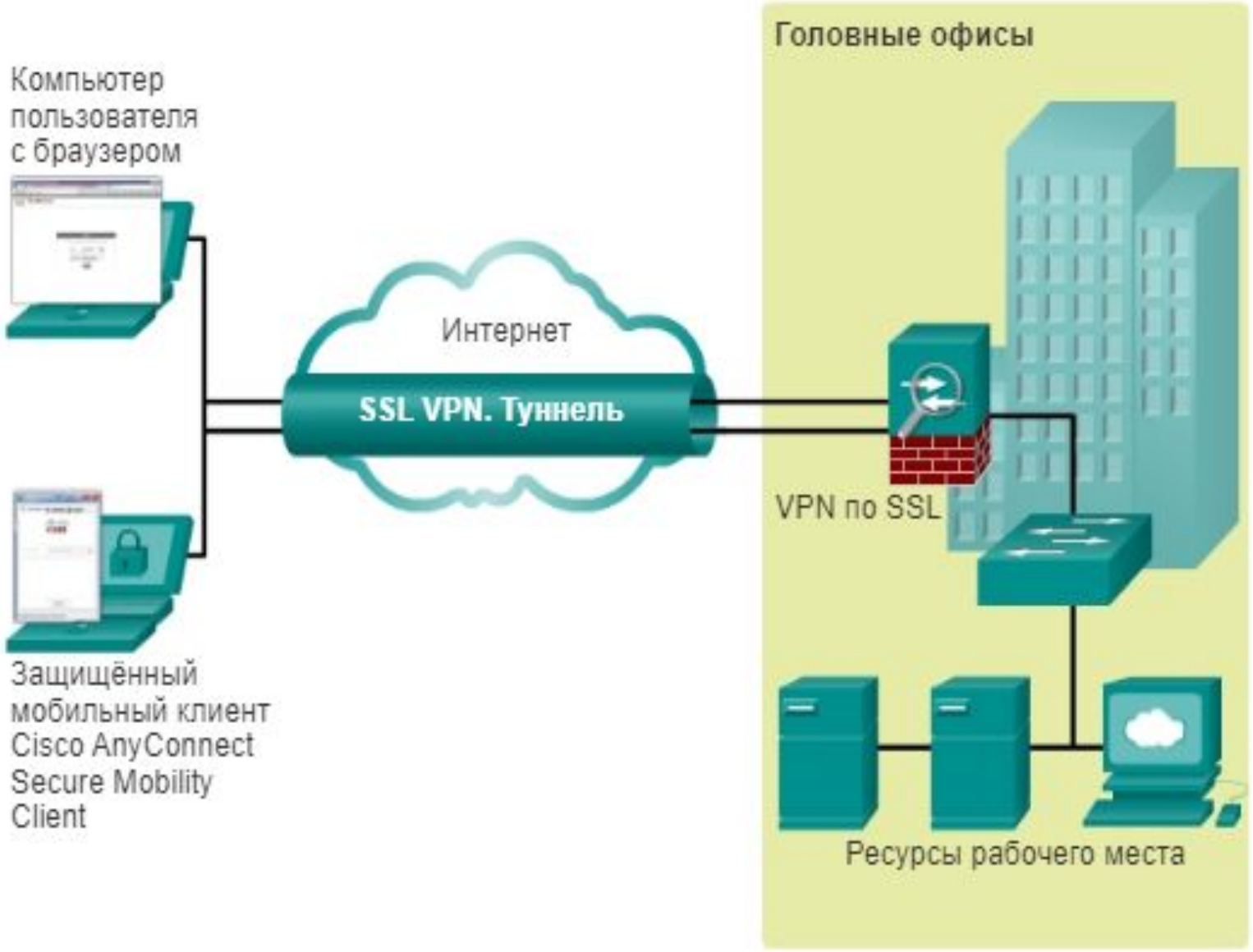
1. Веб-ориентированный, не требующий наличия клиентского ПО, полный доступ к сети, для организации которого на компьютерах не нужно заранее устанавливать специальное ПО.

2. Защита подключения VPN от вирусов, червей, программ-шпионов и злоумышленников благодаря интеграции на платформе Cisco SSL VPN функций обеспечения безопасности для сети и оконечных точек.

3. Использование одного устройства как для SSL VPN, так и для IPsec VPN. Это позволяет сократить затраты и упростить систему управления благодаря надёжному предоставлению служб сетей VPN удалённого доступа и между объектами на основе единой платформы с унифицированным управлением.

Аппаратно-программный комплекс Cisco ASA поддерживает два основных режима развёртывания, применяемых в решениях Cisco SSL VPN, как показано на рисунке:

1. **Cisco AnyConnect Secure Mobility Client с SSL** — требуется клиент Cisco AnyConnect Client
2. **Cisco Secure Mobility SSL VPN без клиента (clientless)** — требуется веб-браузер



На аппаратно-программном комплексе Cisco ASA должена быть настроена поддержка SSL VPN туннелей.

Решение Cisco SSl VPN

Защищённый мобильный клиент Cisco AnyConnect Secure Mobility Client с SSL

Вариант SSL VPN с использованием клиентского ПО предоставляет пользователям, подлинность которых проверена, полный сетевой доступ к корпоративным ресурсам, аналогичный доступу из локальной сети.

Однако на удалённых пользовательских устройствах должно быть установлено клиентское приложение, например Cisco VPN Client или более недавно появившийся клиент AnyConnect.

В общем случае удалённые пользователи для построения SSL туннеля с Cisco ASA, на которой настроено полное туннелирование и SSL VPN, используют клиент Cisco AnyConnect Secure Mobility Client, показанный на рисунке.

После того, как Cisco ASA установит VPN-соединение с удалённым пользователем, этот пользователь может пересылать трафик IP в туннель SSL.

Для выполнения этой функции клиент Cisco AnyConnect Secure Mobility Client создаёт виртуальный сетевой интерфейс.

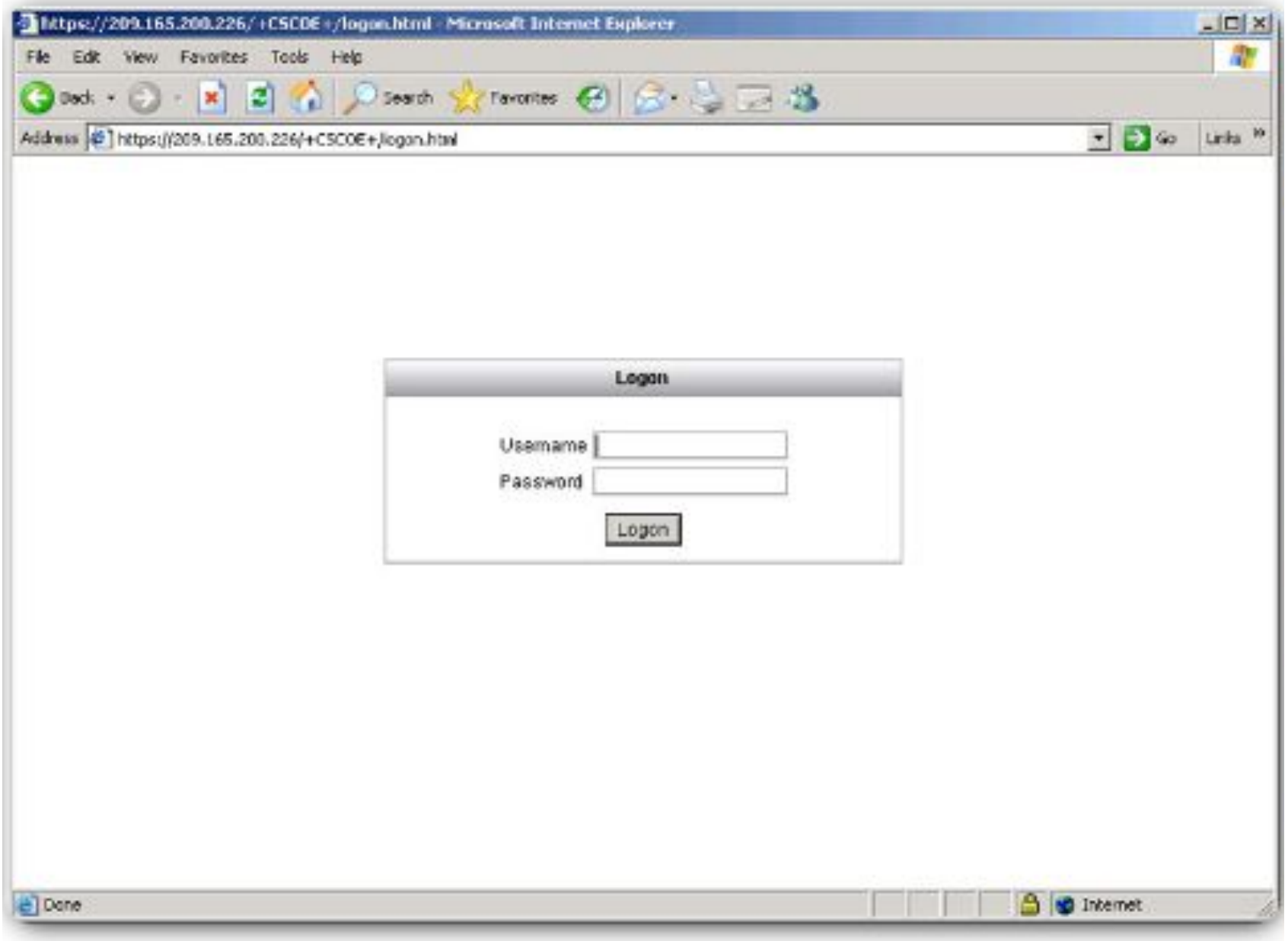
Клиент может использовать любое приложение для доступа к любому ресурсу, расположенному за шлюзом VPN на базе Cisco ASA, с учетом правил доступа.

Cisco Secure Mobility VPN на основе SSL без клиента

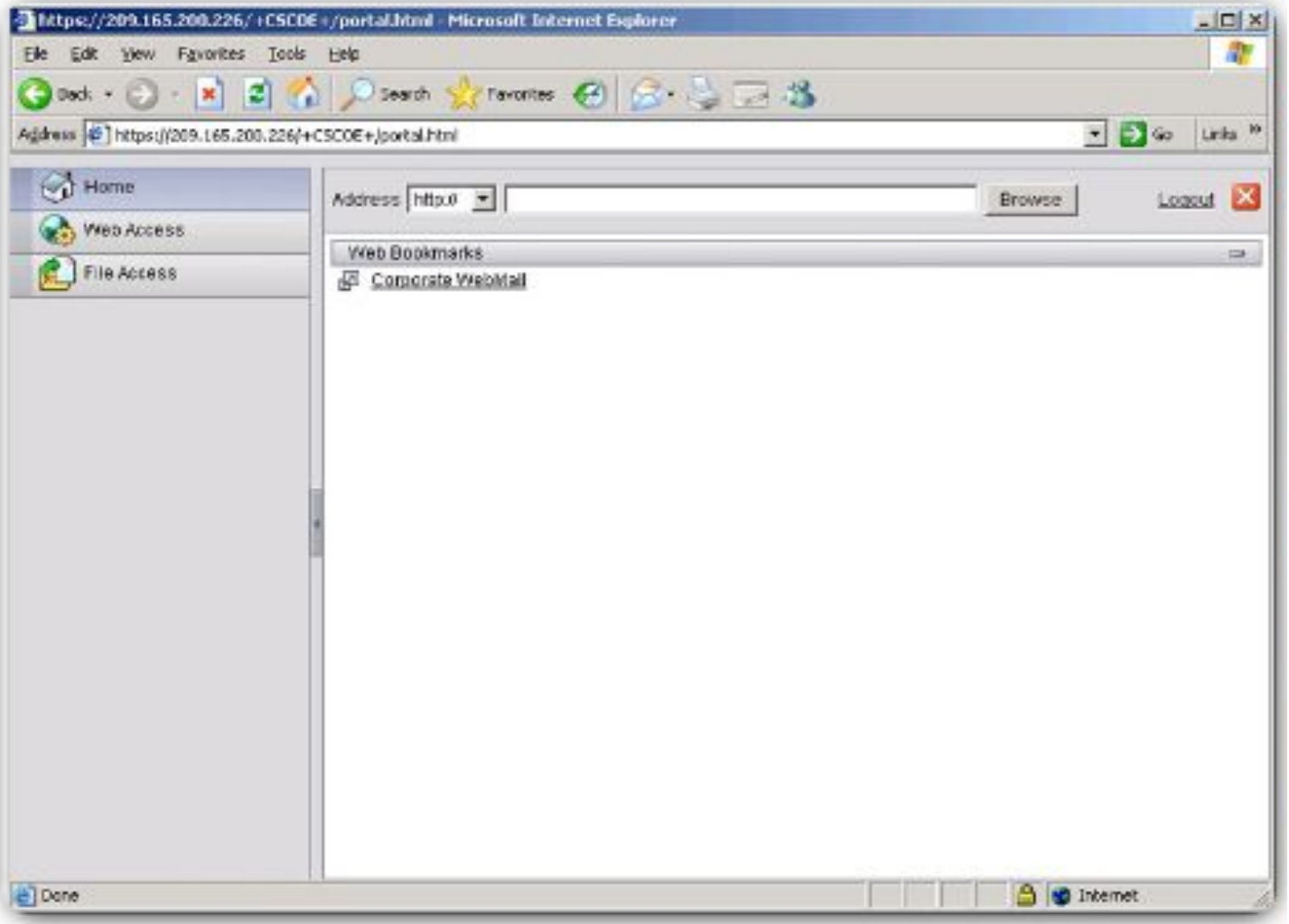
Модель развёртывания VPN на основе SSL без клиентского ПО позволяет корпорациям предоставлять доступ к корпоративным ресурсам даже в том случае, когда удалённое устройство не управляется корпоративной системой управления.

В этой модели развёртывания в качестве устройства-посредника для доступа к сетевым ресурсам используется Cisco ASA. При этом обеспечивается наличие интерфейса веб-портала, позволяющего удалённым устройствам просматривать сеть с помощью перенаправления портов.

В базовом решении SSL VPN без клиентского ПО на основе Cisco ASA для установления SSL-соединения с устройством безопасности Cisco ASA удалённые пользователи используют стандартный веб-браузер, как показано на рисунке.



Аппаратно-программный комплекс Cisco ASA предоставляет пользователю функции веб-портала, через который можно получить доступ к внутренним ресурсам. В базовом решении без клиентского ПО пользователь может получить доступ только к некоторым службам, например, внутренним веб-приложениям, а также к ресурсам для предоставления доступа к файлам, доступным через веб-интерфейс, как показано на рисунке.



Сети VPN удаленного доступа с использованием Ipsec

Многим приложениям для аутентификации и шифрования данных требуется уровень безопасности подключения VPN удалённого доступа с использованием IPsec.

При развёртывании сетей VPN для удалённых сотрудников и небольших филиалов простота развёртывания является крайне важным фактором, если отсутствуют технические ресурсы, необходимые для настройки VPN на маршрутизаторе на удалённой площадке.

Функция Cisco Easy VPN обеспечивает высокую гибкость, масштабируемость и простоту использования для сетей IPsec VPN между объектами, а также подобных сетей удалённого доступа.

Решение Cisco Easy VPN состоит из трёх компонентов:

1. **Cisco Easy VPN в режиме Server** — маршрутизатор Cisco IOS или межсетевой экран Cisco ASA Firewall, работающий как начальное устройство в межфилиальных сетях VPN или сетях VPN удалённого доступа.

2. **Cisco Easy VPN в режиме Remote** — Маршрутизатор Cisco IOS или межсетевой экран Cisco ASA Firewall, работающий как удалённый клиент VPN.

3. **Клиент Cisco VPN Client** — приложение, которое поддерживается пользовательским ПК и используется для доступа к серверу Cisco VPN.

Cisco Easy VPN в режиме Server позволяет мобильным и удалённым сотрудникам, применяющим клиент VPN Client на своих компьютерах либо Cisco Easy VPN в режиме Remote на граничном маршрутизаторе, создавать защищённые туннели IPsec для доступа к внутренней сети в центральном офисе, как показано на рисунке.

Cisco Easy VPN

- Согласовывает параметры туннеля
- Строит туннели в соответствии с заданными параметрами
- Проверяет подлинность пользователей с помощью имён пользователей, имён групп и паролей
- Управляет ключами безопасности для шифрования и расшифровки

Cisco Easy VPN в режиме Server и Remote

Cisco Easy VPN в режиме Server

Cisco Easy VPN в режиме Server позволяет мобильным и удалённым сотрудникам, применяющим клиентское ПО VPN Client на своих компьютерах, создавать защищённые туннели IPsec для доступа к внутренней сети в центральном офисе, где находятся наиболее важные данные и приложения.

Он позволяет маршрутизаторам Cisco IOS и межсетевым экранам Cisco ASA функционировать в качестве начального устройства в межфилиальных сетях VPN либо сетях VPN удалённого доступа.

На устройствах удалённых офисов применяется Cisco Easy VPN в режиме Remote или приложение Cisco VPN Client для подключения к серверу, который затем применяет определённые политики безопасности на удалённом устройстве VPN. Благодаря этому гарантируется, что перед установлением подключения удалённые устройства будут иметь новейшие политики.

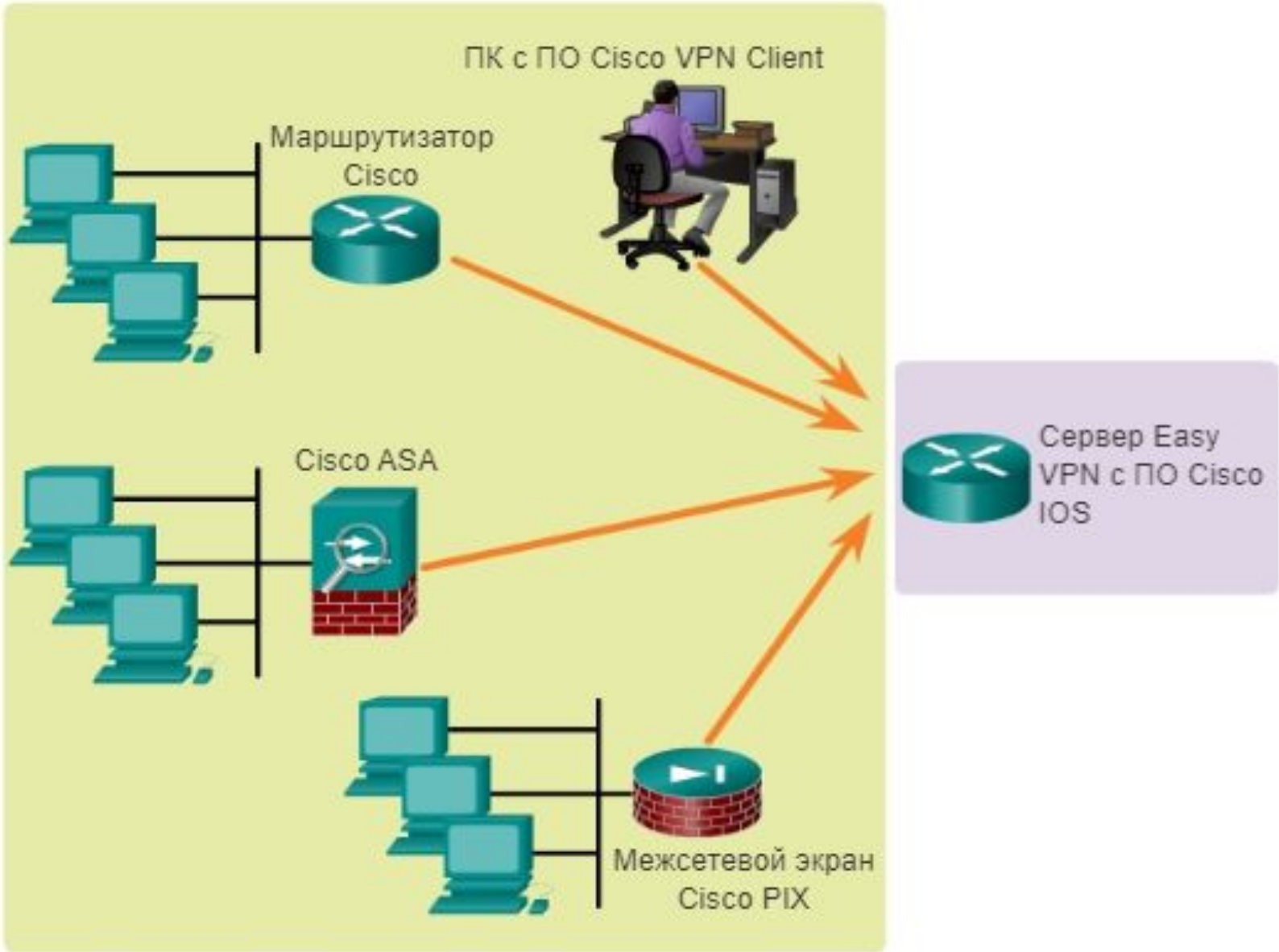
Cisco Easy VPN в режиме Remote

Cisco Easy VPN в режиме Remote позволяет маршрутизаторам Cisco IOS или программным клиентам функционировать в качестве удалённых клиентов VPN.

Эти устройства могут получать политики безопасности с устройства Cisco Easy VPN в режиме Server, что позволяет снизить требования к настройке сети VPN на удалённом объекте.

Это недорогое решение идеально подходит для удалённых офисов с минимальной поддержкой ИТ или при установке большого объёма телекоммуникационного оборудования клиента (CPE), когда крайне желательно избежать индивидуальной настройки многочисленных удалённых устройств.

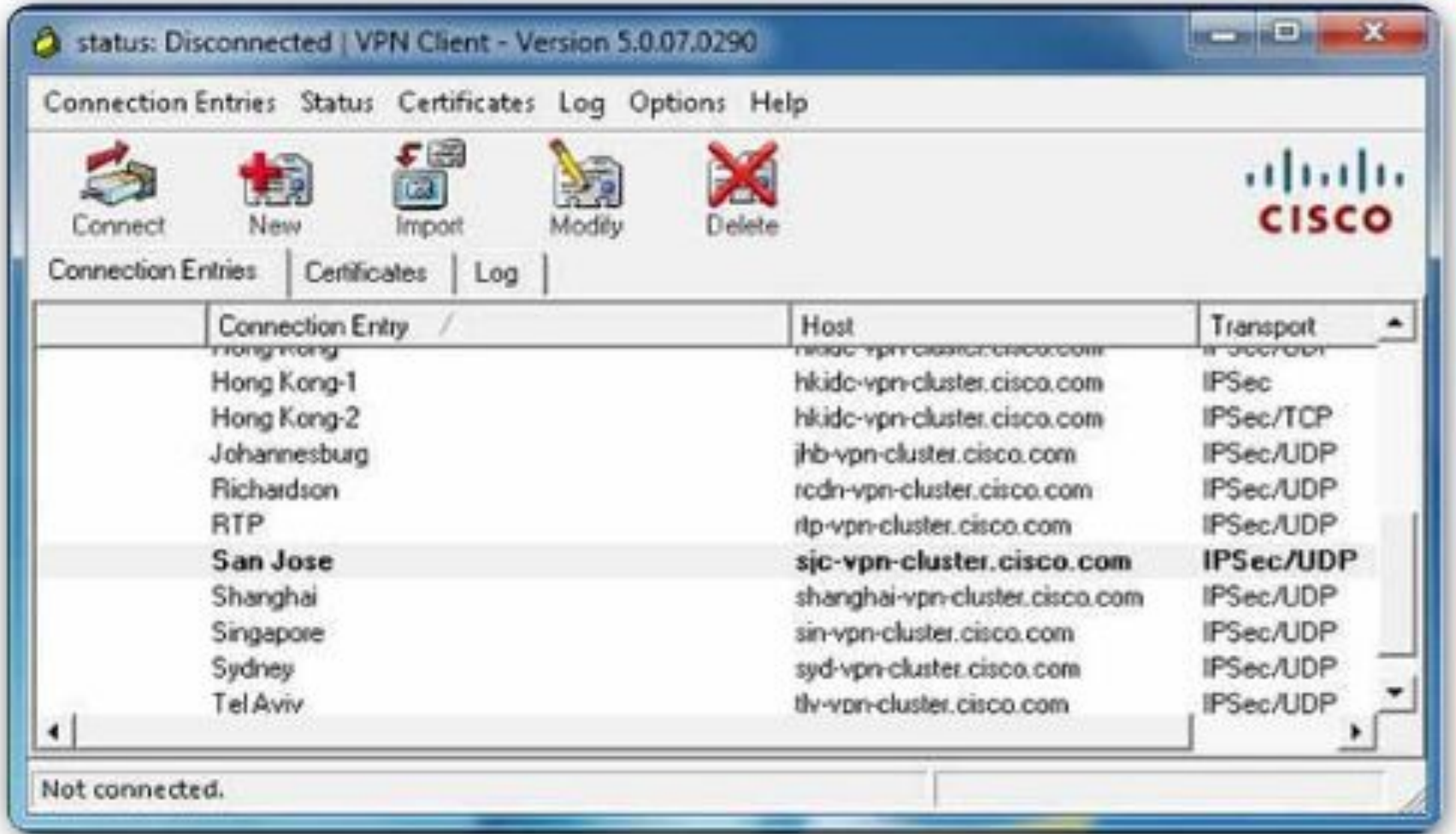
На рисунке показаны три сетевые устройства с активированной функцией Easy VPN Remote, причём все эти устройства подключаются к серверу Easy VPN для получения параметров настройки.



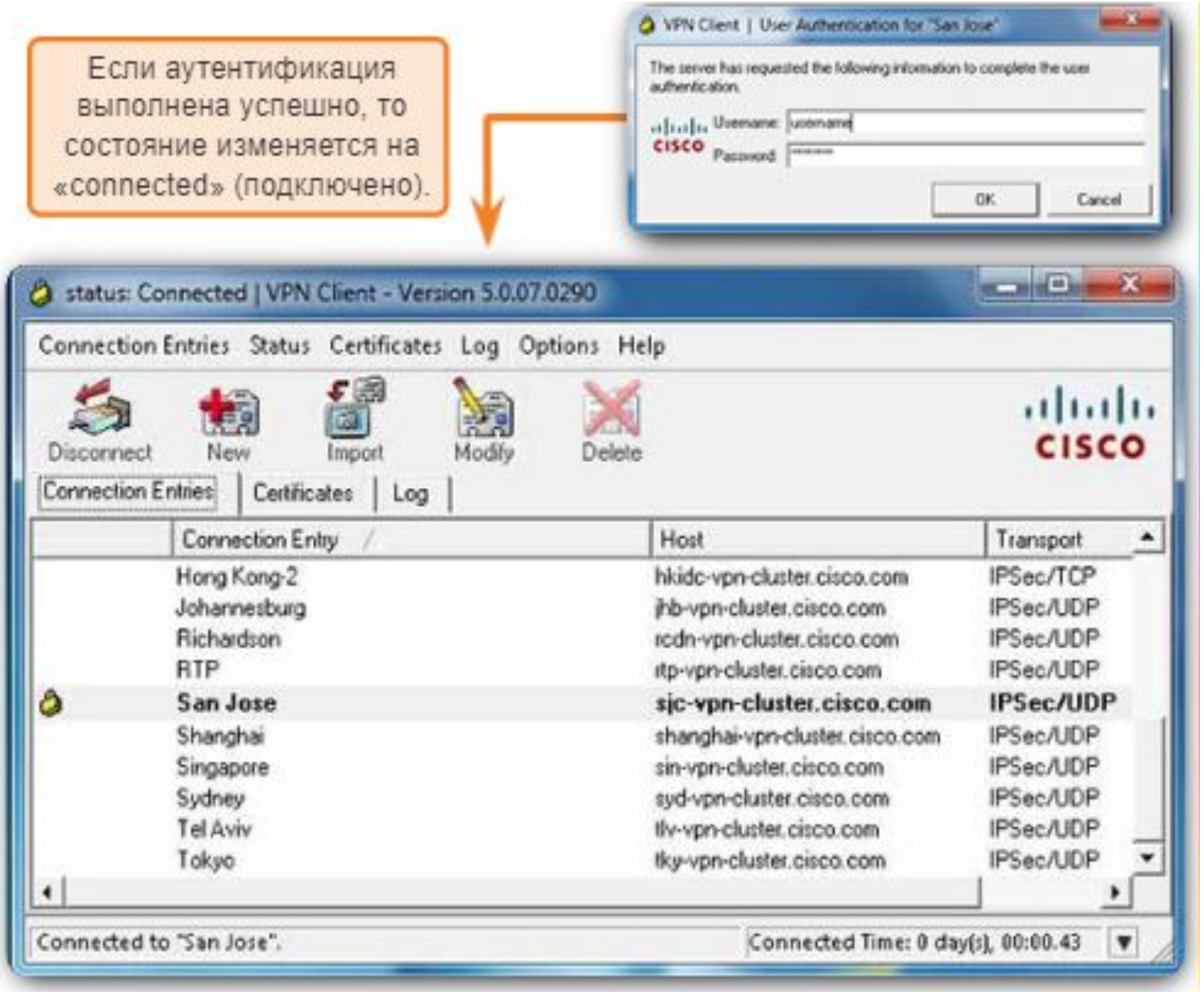
Cisco Easy VPN в режиме Client

Приложение Cisco VPN Client является простым в установке и применении. Оно позволяет организациям устанавливать сквозные, зашифрованные туннели VPN для обеспечения безопасной связи для мобильных или удалённых сотрудников.

Для инициации подключения IPsec с помощью клиента Cisco VPN все пользователи должны открыть окно приложения Cisco VPN Client, как показано на рисунке.



Это приложение отображает все доступные предварительно настроенные узлы. Для выбора объекта дважды щёлкните на него, и клиент VPN инициирует подключение IPsec. В диалоговом окне аутентификации пользователя подлинность пользователя проверяется по имени пользователя и паролю, как показано на рисунке.



После аутентификации приложение Cisco VPN Client отображает состояние «connected» (подключён). Большинство параметров сети VPN определяется на сервере Cisco IOS Easy VPN Server, что позволяет упростить процесс развёртывания.

После инициации удалённым пользователем процесса создания VPN-туннеля сервер Cisco Easy VPN отправляет клиенту политики IPsec, сводя к минимуму необходимость настройки на стороне клиента.

Это простое и хорошо масштабируемое решение идеально подходит для развёртывания большого количества удалённых устройств, когда индивидуальная настройка политик для многочисленных удалённых ПК нерациональна.

Данная архитектура также гарантирует, что для всех подключений будут использоваться новейшие политики безопасности, и позволяет устранить эксплуатационные расходы, связанные с поддержкой системы управления согласованными политиками и ключами.

Сравнение IPsec и SSL

Как показано на рисунке (Слайд №86), технологии IPsec VPN и SSL VPN дают возможность доступа практически к любому сетевому приложению или ресурсу.

Сети VPN на основе SSL предлагают такие функции, как простое установление связи с настольных систем, не находящихся под управлением компании, минимальное сопровождение ПО настольных компьютеров или его полное отсутствие и веб-порталы, настраивающиеся под пользователя при его входе в систему.

	SSL	IPsec
Приложения	Веб-приложения, обмен файлами, электронная почта	Все приложения на основе IP
Шифрование	**Средний - высокий уровень** При длине ключей от 40 до 256 битов	**Высокий уровень** При длине ключей от 56 до 256 битов
Аутентификация	**Средний уровень** Односторонняя или двусторонняя аутентификация	**Высокий уровень** Двусторонняя аутентификация с использованием общих секретных ключей или цифровых сертификатов
Сложность подключения	**Низкий уровень** Требуется только браузер	**Средний уровень** Может оказаться сложным для недостаточно технически подкованных пользователей
Варианты подключения	Может подключиться любое устройство	Могут подключаться только конкретные устройства с конкретными настройками

Протокол IPsec превосходит SSL по нескольким важным характеристикам:

1. Количество поддерживаемых приложений
2. Стойкость шифрования
3. Строгость аутентификации
4. Общий уровень безопасности

Если речь идет об обеспечении безопасности, то IPsec является превосходным решением. Если первоочередными задачами являются поддержка и простота развёртывания, то следует иметь в виду протокол SSL.

Сети VPN с использованием протоколов IPsec и SSL являются взаимодополняющими, так как они позволяют решить различные задачи. В зависимости от потребностей организация может реализовать сеть одного или обоих типов.

Указанный выше взаимодополняющий подход позволяет одиночному устройству, например, маршрутизатору ISR или межсетевому экрану ASA, удовлетворять все требования пользователя к удалённому доступу.

Хотя во многих решениях предлагаются либо IPsec, либо SSL, решения компании Cisco для сетей VPN удалённого доступа одновременно поддерживают обе технологии (в рамках единой платформы) и обеспечивают унифицированное управление.

Одновременная реализация технологий IPsec и SSL позволяет организациям настраивать свои сети VPN удалённого доступа без какого-либо дополнительного усложнения оборудования или управления.