**МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН**

**Некоммерческое акционерное общество**
**АЛМАТИНСКИЙ УНИВЕРСИТЕТ ЭНЕРГЕТИКИ И СВЯЗИ**

**кафедра** "Компьютерные технологии"

**«Допущен к защите»**
**Заведующий кафедрой** _____
_____
(Ф.И.О., ученая степень, звание)
_____ «_____»_____ **20__ г.**
(подпись)

# ДИПЛОМНЫЙ ПРОЕКТ

**На тему:** "Проектирование сети с подключением удаленных филиалов и мобильных сотрудников с использованием технологии Virtual Private Network"

**Специальность** "Вычислительная техника и программное обеспечение"

**Выполнил (а)** Лонашенко Е.А. ВТ-10-4
(Фамилия и инициалы) группа

**Научный руководитель** Тергеусизова А.С. старший преподаватель
(Фамилия и инициалы, ученая степень, звание)

**Консультанты:**

**по экономической части:**
Ергешева З.Д., ст. преподаватель
(Фамилия и инициалы, ученая степень, звание)
Ергешева «13» 05 2014 г.
(подпись)

**по безопасности жизнедеятельности:**
Джаманбаев Н.Г. д.т.н., профессор
(Фамилия и инициалы, ученая степень, звание)
_____ «11» 05 2014 г.
(подпись)

**по применению вычислительной техники:**
Тергеусизова А.С., ст. преподаватель
(Фамилия и инициалы, ученая степень, звание)
_____ «22» мая 2014 г.
(подпись)

_____
(Фамилия и инициалы, ученая степень, звание)
_____ «_____»_____ 20___ г.
(подпись)

**Нормоконтролер:** Гусупов Д.М.
(Фамилия и инициалы, ученая степень, звание)
_____ «22» мая 2014 г.
(подпись)

**Рецензент:** _____
(Фамилия и инициалы, ученая степень, звание)
_____ «_____»_____ 20___ г.
(подпись)

**Алматы 2014 г.**

**МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН**

**Некоммерческое акционерное общество**
**АЛМАТИНСКИЙ УНИВЕРСИТЕТ ЭНЕРГЕТИКИ И СВЯЗИ**

Факультет "Информационные технологии"
Специальность "Вычислительная техника и программное обеспечение"
Кафедра "Компьютерные технологии"

# ЗАДАНИЕ

на выполнение дипломного проекта

Студент Лопашенко Евгения Андреевна
(фамилия, имя, отчество)

Тема проекта "Проектирование сети с подключением удаленных филиалов и мобильных сотрудников с использованием технологии Virtual Private Network"

утверждена приказом ректора № 115 от «24» сентября 2013 г.

Срок сдачи законченной работы «10» июня 2014 г.

Исходные данные к проекту требуемые параметры результатов проектирования (исследования) и исходные данные объекта
на основе компании ТОО "TNS-INTEC" выполнить проектирование сети с подключением удаленных филиалов и мобильных сотрудников с использованием технологии Virtual Private Network. Для создания виртуальных частных сетей : архитектура протокола IPSec.

Перечень подлежащих разработке дипломного проекта вопросов или краткое содержание дипломного проекта:
1. VPN - виртуальные частные сети
2. IPSec - протокол защиты сетевого трафика
3. Проектирование сети с подключением удаленных филиалов и мобильных сотрудников с использованием технологии VPN для ТОО "TNS-INTEC".
4. Безопасность жизнедеятельности
5. Бизнес - план

Перечень графического материала (с точным указанием обязательных чертежей)

1. Схема сети
2. Структурная схема сети компании с технологией IPSec VPN.
3. Структурная схема организации сети.

Рекомендуемая основная литература

1. Дьяченко В.А., Анализ проблем информационной безопасности в компьютерной сети, организации подключенной к сети Интернет
2. Николай Богданович, Построение безопасных сетей на основе VPN.
3. Щербо В.К., Стандарты вычислительных сетей.

Консультанты по проекту с указанием относящихся к ним разделов

| Раздел | Консультант | Сроки | Подпись |
|---|---|---|---|
| БЖД | Дьяченко Н.Г. | 11.04 - 11.05.14 | |
| Экономика | Ерешева З.Д. | 15.04. - 13.05.14 | Ерешева |
| Нормоконтроль | Тугупов Дум. | 22.05.14г. | |
| Основная часть | Терлеусова А.С | 22.05.14г. | |
| | | | |
| | | | |
| | | | |
| | | | |

Г Р А Ф И К
подготовки дипломного проекта

| № п/п | Наименование разделов, перечень разрабатываемых вопросов | Сроки представления руководителю | Примечание |
|---|---|---|---|
| 1 | VPN - виртуальные частные сети | 11.04 - 22.04 | |
| 2. | IPSec - протокол защиты сетевого трафика | 23.04. - 04.05. | |
| 3. | Проектирование сети | 05.05 - 22.05.14 | |
| 4. | BPCD | 11.04 - 11.05.14. | |
| 5. | Бизнес - план | 15.04 - 13.05.14. | |

Дата выдачи задания «3» марта 2014 г.

Заведующий кафедрой _____ Курмалбаев З.К.
(подпись) (Фамилия и инициалы)

Руководитель _____ Тергеусова Д.С
(подпись) (Фамилия и инициалы)

Задание принял к исполнению
студент _____ Лонашенко Е.А.
(подпись) (Фамилия и инициалы)

**Аннотация**

В данном дипломном проекте рассмотрено построение сети с подключением удаленных филиалов и мобильных сотрудников с использованием технологии Virtual Private Network.

В дипломе также представлены технологии создания виртуальных частных сетей, архитектура протокола IPSec, схема построения сети и состав оборудования.

В проекте проведен анализ потенциально опасных и вредных факторов воздействия на оператора в процессе обслуживания и проектирования сети.

Разработан бизнес–план внедрения данного проекта.

**Аңдатпа**

Айтылмыш дипломдық жобада аудың құрылысы алыстат– филиалдың және ұтқыр қызметкердің қосуымен мен игерушілік Virtual Private Network технологиясының қара.

Дипломда да ауани жеке аудың жаралғанының технологиялары, IPSec хаттамасының сәулеті, аудың құрылысының нобайы және жабдықтың құрамының ұсын.

Жобада әсердің қауіпті және зарарлы факторының анализы әлеуетті операторға ара үдеріс күту және аудың жобала– өткіздір–өткізу.

**Abstract**

In this diploma project considers the construction of a network connecting remote offices and mobile workers using technology Virtual Private Network.

In the diploma also presented the technology of virtual private networks, protocol architecture IPSec, a scheme for constructing the network structure and equipment.

The project analyzed the potentially dangerous and harmful factors of operator exposure during maintenance and network design.

The business plan for the implementation of this project.

## Содержание

## Введение

В современных условиях развитых информационных технологий, преимущества создания виртуальных частных сетей не могут быть не оценены. Но перед тем как перечислить наиболее очевидные, полезные, неоспоримые способы построения виртуальных частных сетей, необходимо разъяснить само понятие.

VPN (Virtual Private Network) или виртуальная частная сеть – это технология, при реализации которой выполняется обмен информации по виртуальному каналу с удаленной локальной сетью через сеть общего пользования с воспроизведением частного подключения. В данном контексте Интернет или другая интрасеть могут подразумеваться как сеть общего пользования.

Несколько лет тому назад невозможно было представить, насколько может поменяться стиль жизни и работы. Во многих организациях используется труд совместителей и удаленных сотрудников, которые работают на домашних компьютерах, а также используют услуги интернет–кафе, либо зон доступа беспроводных сетей общего пользования.

На данный момент для пользователей более важным является вопрос о том, как соединиться с корпоративной информационной системой. При этом им требуется широкополосное соединение независимо от того, используется ли фиксированная сеть или же Wi–Fi–доступ, так как нередко пользователи вынуждены работать в пути. В наше время все более популярными становятся виртуальные технологии, которые занимают в современной компании приоритетное положение. Так как они дают возможность устранения привязки голосовых сервисов к одному рабочему месту. Для получения данных услуг не требуется навсегда однозначное размещение сотрудников в офисе, нет необходимости вообще там находиться – достаточно использовать удаленное подключение. Многие организации внедряют решения с фиксированной и мобильной связью, чтобы обеспечить эффективное подключение мобильных сотрудников с помощью терминалов, которые могут работать с голосовыми сервисами и услугами по передаче данных. Это дает возможность таким работникам постоянно находиться на связи. Особо остро встает вопрос о доступе и аутентификации пользователей, когда есть удаленный доступ, особенно при переходе из одной сети общего пользования в другую [1].

Кроме того, многие компании предусматривают возможность доступа только к определенным корпоративным ресурсам и приложениям для партнеров, консультантов и клиентов. То есть очень многим может понадобиться доступ к вышеуказанным ресурсам из вне, не попадая под контроль IT–служб организации.

Появившееся многообразие вариантов доступа потребовало более серьезного отношения к обеспечению безопасности.

По мере большей распространенности высокоскоростного доступа к интернету все больше пользователей обращаются к корпоративным сетям, применяя широкополосные подключения.

Для резервирования информационной системы могут применяться различные возможности доступа. Широкополосные резервные каналы имеют возможность обеспечивать катастрофо устойчивость методом репликации данных на удаленных серверах. Что позволит уменьшить потери данных, а также поддержать работоспособность всей сети, как при неприятностях местного масштаба, таких, как выход из строя узла связи в связи с ударом молнии, обслуживающего головной офис компании, так и в случае масштабных стихийных бедствий, вроде ураганов и землетрясений [1].

В данном дипломном проекте будет рассмотрена технология Virtual Private Network для безопасного подключения к серверу компании ТОО “TNS-INTEC” в головном офисе в Астане из филиала в городе Алматы, которая занимается установкой оборудования для учета электропотребления на электровозах, а также установкой датчиков уровня воды и топлива в баке, температуры масла, топлива, охлаждающей жидкости, датчиков частоты вращения на тепловозах, а также, сбором и отправкой показаний с локомотивов.

# 1 VPN – виртуальные частные сети

## 1.1 Концепция построения защищенных сетей

Компьютеры, сети, Интернет в нашей повседневной жизни стали неотъемлемой частью. Наш насыщенный технологиями, быстроразвивающийся мир с каждым днем все больше становится зависимым от компьютерных технологий и сетей. Однако эта зависимость возникла не внезапно. С каждым годом финансирование компьютерных технологий значительно возрастало, и неудивительно, что эти технологии проникли практически во все сферы деятельности человека.

На заре развития компьютерных технологий большинство людей не могли представить, насколько широко эти технологии будут использоваться в самом недалеком будущем. Поэтому, наверное, многие не решались уделять много времени и усилий для освоения того, что, в конце концов, могло оказаться обыкновенной забавой. По сравнению с требованиями современного рынка труда количество людей, работавших в то время в области компьютерных технологий, было ничтожно мало. Люди, работавшие в этом тесном сообществе, были хорошо знакомы и доверяли друг другу. Кроме того, в это сообщество допускались только избранные, которые заслуживали доверия. Таким образом, в те времена проблемы безопасности в области компьютерных технологий практически отсутствовали. И достаточно долгое время специалисты в области компьютерных технологий не уделяли внимания безопасности компьютерных сетей.

В настоящее время огромное количество сетей объединено посредством Интернет. Поэтому очевидно, что для безопасной работы такой огромной системы необходимо принимать определенные меры безопасности, поскольку практически с любого компьютера можно получить доступ к любой сети любой организации, причем опасность значительно возрастает по той причине, что для взлома компьютера к нему вовсе не требуется физического доступа [2].

В связи с широким распространением Интернет, при разработке и применении распределенных информационных сетей и систем одной из самых актуальных задач является решение проблем информационной безопасности.

В связи с бурным развитием сетей коллективного доступа в мире произошел качественный скачок в распространении и доступности информации. Пользователи получили дешевые и доступные каналы связи.

Стремясь к экономии средств, предприятия используют такие каналы для передачи критичной коммерческой информации. Однако принципы построения Интернет открывают злоумышленникам возможности кражи или преднамеренного искажения информации. Не обеспечена достаточно надежная защита от проникновения нарушителей в корпоративные и ведомственные сети.

Любая организация, будь она производственной, торговой, финансовой компании или государственным учреждением, обязательно сталкивается с

вопросом передачи информации между своими филиалами, а также с вопросом защиты этой информации. Не каждая фирма может себе позволить иметь собственные физические каналы доступа, и здесь помогает технология VPN, на основе которой и соединяются все подразделения и филиалы, что обеспечивает достаточную гибкость и одновременно высокую безопасность сети, а также существенную экономию затрат.

Виртуальная частная сеть (VPN – Virtual Private Network) создается на базе общедоступной сети Интернет. И если связь через Интернет имеет свои недостатки, главным из которых является то, что она подвержена потенциальным нарушениям защиты и конфиденциальности, то VPN могут гарантировать, что направляемый через Интернет трафик так же защищен, как и передача внутри локальной сети. В тоже время виртуальные сети обеспечивают существенную экономию затрат по сравнению с содержанием собственной сети глобального масштаба.

В основе концепции построения защищенных виртуальных частных сетей VPN лежит достаточно простая идея: если в глобальной сети есть два узла, которые хотят обменяться информацией, то для обеспечения конфиденциальности и целостности передаваемой по открытым сетям информации между ними необходимо построить виртуальный туннель, доступ к которому должен быть чрезвычайно затруднен всем возможным активным и пассивным внешним наблюдателям. Термин «виртуальный» указывает на то, что соединение между двумя узлами сети не является постоянным (жестким) и существует только во время прохождения трафика по сети.

Преимущества, получаемые компанией при формировании таких виртуальных туннелей, заключаются, прежде всего, в значительной экономии финансовых средств [1].

История зарождения VPN уходит своими корнями далеко в 60–е годы прошлого столетия, когда специалисты инженерно–технического отдела нью–йоркской телефонной компании разработали систему автоматического установления соединений абонентов АТС – Centrex (Central Exchange). Другими словами это не что иное, как виртуальная частная телефонная сеть, т.к. арендовались уже созданные каналы связи, т.е. создавались виртуальные каналы передачи голосовой информации. В настоящее время данная услуга заменяется более продвинутым ее аналогом – IP–Centrex. Соблюдение конфиденциальности было важным аспектом при передаче информации уже достаточно длительное время, приблизительно в 1900 году до н.э. первые попытки криптографии проявляли египтяне, искажая символы сообщений. А в XV веке уже нашей эры математиком Леоном Батистом Альберти была создана первая криптографическая модель. В наше время именно виртуальная частная сеть может обеспечить достаточную надежность передаваемой информации вместе с великолепной гибкостью и расширяемостью системы.

Главная выгода от использования VPN для удаленного доступа – совокупность стоимостной эффективности возможного использования общедоступной сетевой среды для транспортирования частной информации и

высокого уровня безопасности. Защищенная виртуальная сеть может предоставить множество уровней безопасности, включая усовершенствование конфиденциальности, целостности и аутентификации. Поскольку VPN использует существующую сетевую инфраструктуру, ее можно реализовать достаточно быстро, так как нет необходимости прокладывать новые (выделенные) линии связи. Комбинация безопасности, быстрой установки и рентабельности с точки зрения стоимости может сделать VPN превосходным коммерческим коммуникационным решением.

## 1.2 Понятие и принципы VPN

VPN, или Virtual Private Network, что в переводе означает Виртуальная Частная Сеть – это криптосистема, позволяющая защитить данные при передаче их по незащищенной сети, такой как Интернет. Несмотря на то, что данное описание подходит и для криптосистемы SSH, VPN имеет другое предназначение. SSH разрабатывался как средство, позволяющее пользователю безопасно зайти и удалённо управлять другим компьютером. Цель VPN – прозрачный доступ к ресурсам сети, где пользователь может делать всё то, что он делает обычно независимо от того, насколько он удалён.

По этой причине VPN приобрёл популярность среди дистанционных работников и офисов, которые нуждаются в совместном использовании ресурсов территориально разделённых сетей.

VPN соединение всегда состоит из канала типа точка–точка, также известного под названием *туннель* (Рисунок 1.1).

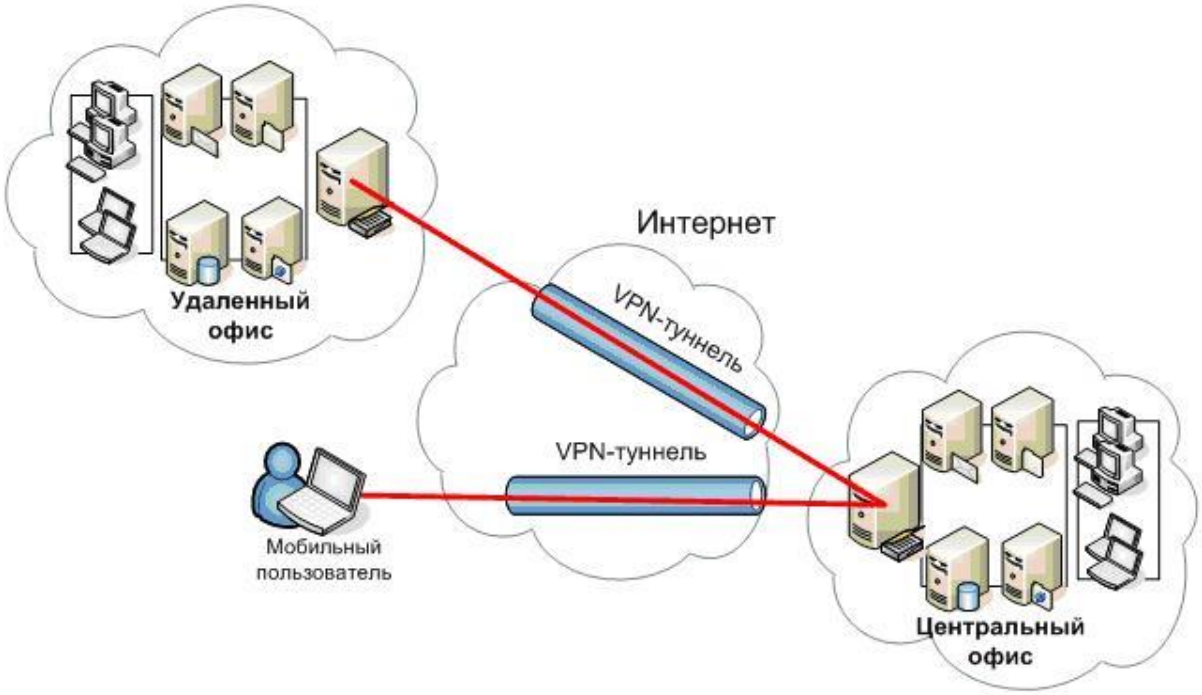


Рисунок 1.1 – VPN–туннель

Туннель создаётся в незащищённой сети, в качестве которой чаще всего выступает Интернет. Соединение точка–точка подразумевает, что оно всегда устанавливается между двумя компьютерами, которые называются узлами или *peers*. Каждый peer отвечает за шифрование данных до того, как они попадут в туннель и расшифровке этих данных после того, как они туннель покинут.

Хотя VPN туннель всегда устанавливается между двумя точками, каждый peer может устанавливать дополнительные туннели с другими узлами. Для примера, когда трём удалённым станциям необходимо связаться с одним и тем же офисом, будет создано три отдельных VPN туннеля к этому офису. Для всех туннелей peer на стороне офиса может быть одним и тем же.

Независимо от используемого ПО, все VPN работают по следующим принципам:

1 Каждый из узлов идентифицирует друг друга перед созданием туннеля, чтобы удостовериться, что шифрованные данные будут отправлены на нужный узел.

2 Оба узла требуют заранее настроенной политики, указывающей какие протоколы могут использоваться для шифрования и обеспечения целостности данных.

3 Узлы сверяют политики, чтобы договориться об используемых алгоритмах; если это не получается, то туннель не устанавливается.

4 Как только достигнуто соглашение по алгоритмам, создаётся ключ, который будет использован в симметричном алгоритме для шифрования/расшифровки данных.

VPN и беспроводные технологии не конкурируют, а дополняют друг друга. VPN работает поверх разделяемых сетей общего пользования, обеспечивая в то же время конфиденциальность за счет специальных мер безопасности и применения туннельных протоколов, таких как туннельный протокол на канальном уровне (Layer Two Tunneling Protocol – L2TP). Смысл их в том, что, осуществляя шифрование данных на отправляющем конце и дешифрирование на принимающем, протокол организует «туннель», в который не могут проникнуть данные, не зашифрованные должным образом. Дополнительную безопасность может обеспечить шифрование не только самих данных, но и сетевых адресов отправителя и получателя. Беспроводную локальную сеть можно сравнить с разделяемой сетью общего пользования, а в некоторых случаях (хот–споты, узлы, принадлежащие сообществам) она таковой и является [3].

VPN отвечает трем условиям: конфиденциальность, целостность и доступность. Следует отметить, что никакая VPN не является устойчивой к DoS– или DDoS–атакам и не может гарантировать доступность на физическом уровне просто в силу своей виртуальной природы и зависимости от нижележащих протоколов.

## 1.3 Классификация VPN

Классифицировать VPN решения можно по нескольким основным параметрам.

*По степени защищенности используемой среды*

Защищённые

Наиболее распространённый вариант виртуальных частных сетей. С его помощью возможно создать надежную и защищенную сеть на основе ненадёжной сети, как правило, Интернета. Примером защищённых VPN являются: IPSec, OpenVPN и PPTP.

Доверительные

Используются в случаях, когда передающую среду можно считать надёжной и необходимо решить лишь задачу создания виртуальной подсети в рамках большей сети. Проблемы безопасности становятся неактуальными. Примерами подобных VPN решений являются: Multi–protocol label switching (MPLS) и L2TP (Layer 2 Tunnelling Protocol) (точнее будет сказать, что эти протоколы перекладывают задачу обеспечения безопасности на другие, например L2TP, как правило, используется в паре с IPSec).

*По способу реализации*

В виде специального программно–аппаратного обеспечения

Реализация VPN сети осуществляется при помощи специального комплекса программно–аппаратных средств. Такая реализация обеспечивает высокую производительность и, как правило, высокую степень защищённости.

*В виде программного решения*

Используют персональный компьютер со специальным программным обеспечением, обеспечивающим функциональность VPN.

*Интегрированное решение*

Функциональность VPN обеспечивает комплекс, решающий также задачи фильтрации сетевого трафика, организации сетевого экрана и обеспечения качества обслуживания.

*По назначению*

Intranet VPN

Используют для объединения в единую защищённую сеть нескольких распределённых филиалов одной организации, обменивающихся данными по открытым каналам связи.

Remote Access VPN

Используют для создания защищённого канала между сегментом корпоративной сети (центральным офисом или филиалом) и одиночным пользователем, который, работая дома, подключается к корпоративным ресурсам с домашнего компьютера, корпоративного ноутбука, смартфона или интернет–киоска.

Extranet VPN

Используют для сетей, к которым подключаются «внешние» пользователи (например, заказчики или клиенты). Уровень доверия к ним

намного ниже, чем к сотрудникам компании, поэтому требуется обеспечение специальных «рубежей» защиты, предотвращающих или ограничивающих доступ последних к особо ценной, конфиденциальной информации.

Internet VPN

Используется для предоставления доступа к интернету провайдерами, обычно если по одному физическому каналу подключаются несколько пользователей. Протокол PPPoE стал стандартом в ADSL–подключениях. L2TP был широко распространён в середине 2000–х годов в домовых сетях: в те времена внутрисетевой трафик не оплачивался, а внешний стоил дорого. Это давало возможность контролировать расходы: когда VPN–соединение выключено, пользователь ничего не платит. В настоящее время проводной интернет дешёвый или безлимитный, а на стороне пользователя зачастую есть маршрутизатор, на котором включать–выключать интернет не так удобно, как на компьютере. Поэтому L2TP–доступ отходит в прошлое.

Client/Server VPN

Он обеспечивает защиту передаваемых данных между двумя узлами (не сетями) корпоративной сети. Особенность данного варианта в том, что VPN строится между узлами, находящимися, как правило, в одном сегменте сети, например, между рабочей станцией и сервером. Такая необходимость очень часто возникает в тех случаях, когда в одной физической сети необходимо создать несколько логических сетей. Например, когда надо разделить трафик между финансовым департаментом и отделом кадров, обращающихся к серверам, находящимся в одном физическом сегменте. Этот вариант похож на технологию VLAN, но вместо разделения трафика, используется его шифрование.

*По типу протокола*

Существуют реализации виртуальных частных сетей под TCP/IP, IPX и AppleTalk. Но на сегодняшний день наблюдается тенденция к всеобщему переходу на протокол TCP/IP, и абсолютное большинство VPN решений поддерживает именно его. Адресация в нём чаще всего выбирается в соответствии со стандартом RFC5735, из диапазона Приватных сетей TCP/IP.

*По уровню сетевого протокола*

По уровню сетевого протокола на основе сопоставления с уровнями эталонной сетевой модели ISO/OSI [4].

### 1.4 Виды соединения VPN

Организовывая безопасные каналы передачи информации в учреждениях несправедливо не рассмотреть вариант организации полноценной частной сети. На рисунке 1.2 изображен вариант организации частной сети небольшой компанией с 2 филиалами.

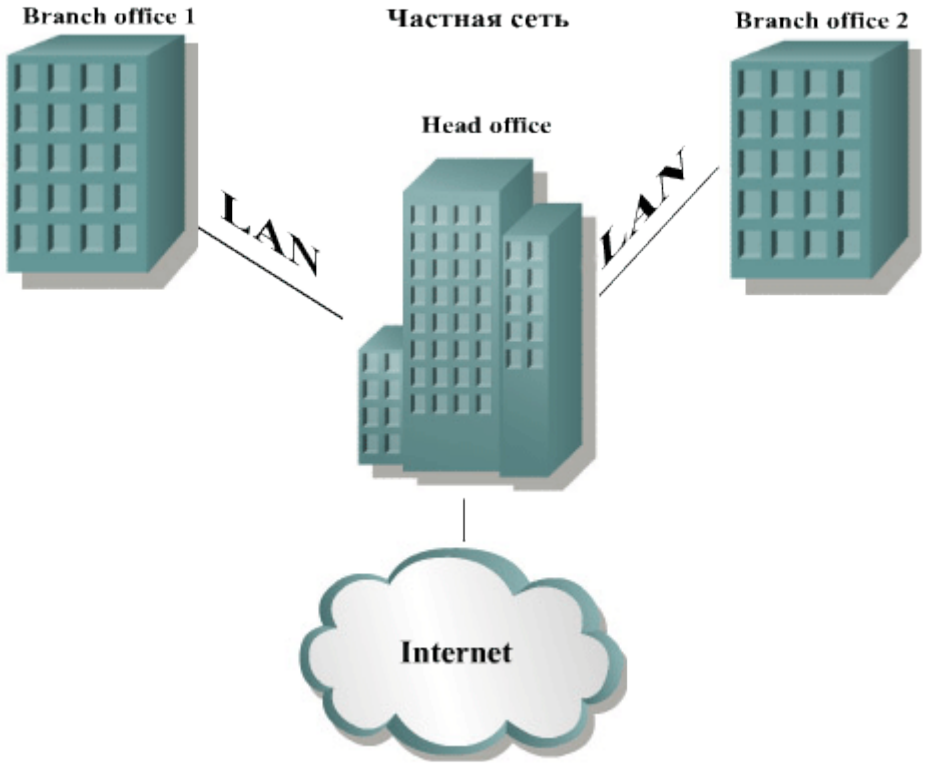


Рисунок 1.2 – Вариант организации частной сети небольшой компанией с 2 филиалами

Доступ во внешнюю сеть может осуществляться как через центральный офис, так и децентрализовано. Данная организация сети обладает следующими неоспоримыми преимуществами:

- высокая скорость передачи информации, фактически скорость при таком соединении будет равна скорости локальной сети предприятия;
- безопасность, передаваемые данные не попадают в сеть общего пользования;
- за пользование организованной сетью ни кому не надо платить, действительно капитальные вложения будут только на стадии изготовления сети.

На рисунке 1.3 изображен аналогичный вариант организации сети учреждения с филиалами, но только с использованием виртуальных частных сетей.


Рисунок 1.3 – Вариант организации сети учреждения с филиалами, с использованием виртуальных частных сетей

В данном случае преимущества, приведенные для частных сетей, оборачиваются недостатками для виртуальных частных сетей, но так ли значительны эти недостатки? Давайте разберемся:

- скорость передачи данных. Провайдеры могут обеспечить достаточно высокоскоростной доступ в Интернет, однако с локальной, проверенной временем 100 Мбит сетью он все равно не сравнится. Но так ли важно каждый день перекачивать сотни мегабайт информации через организованную сеть. Для доступа к локальному сайту предприятия, пересылки электронного письма с документом вполне достаточно скорости, которой могут обеспечить Интернет–провайдеры;
- безопасность передаваемых данных. При организации VPN передаваемая информация попадает во внешнюю сеть, поэтому об организации безопасности придется позаботиться заранее. Но уже сегодня существуют достаточно стойкие к атакам алгоритмы шифрования информации, которые позволяют владельцам передаваемых данных не беспокоиться за безопасность. Подробнее о способах обеспечения безопасности и алгоритмах шифрования чуть ниже;
- за организованную сеть никому не надо платить. Достаточно спорное преимущество, поскольку в противовес дешевизне пользования сетью стоят большие капитальные затраты на ее создание, которые могут оказаться неподъемными для небольшого учреждения. В то же время плата за использование Интернет в наши дни сама по себе достаточно демократичная, а гибкие тарифы позволяю выбрать каждому оптимальный пакет.

Теперь разберемся с наиболее очевидными преимуществами VPN:

- Масштабируемость системы. При открытии нового филиала или добавления сотрудника, которому позволено пользоваться удаленным доступом не нужно никаких дополнительных затрат на коммуникации.
- Гибкость системы. Для VPN не важно, откуда вы осуществляете доступ. Отдельно взятый сотрудник может работать из дома, а может во время чтения почты из корпоративного почтового ящика фирмы пребывать в командировке в абсолютно другом государстве. Также стало возможным использовать так называемые мобильные офисы, где нет привязки к определенной местности.
- Из предыдущего вытекает, что для организации своего рабочего места человек географически неограничен, что при использовании частной сети практически невозможно.

Отдельным пунктом можно выделить создание не проводных частных сетей, а беспроводных. При таком подходе можно даже рассмотреть вариант со своим спутником. Однако в этом случае начальные затраты достигают астрономических высот, скорость снижается фактически до скорости пользования всемирной паутиной, а для надежного обеспечения безопасности необходимо применять опять таки шифрование. И в итоге получаем туже виртуальную частную сеть, только с неимоверно высокими начальными затратами и затратами на поддержание в рабочем состоянии всего оборудования.

В VPN наиболее целесообразно выделить следующие три основных способа:

1 Удаленный доступ отдельно взятых сотрудников к корпоративной сети организации через модем либо общедоступную сеть (Рисунок 1.4).

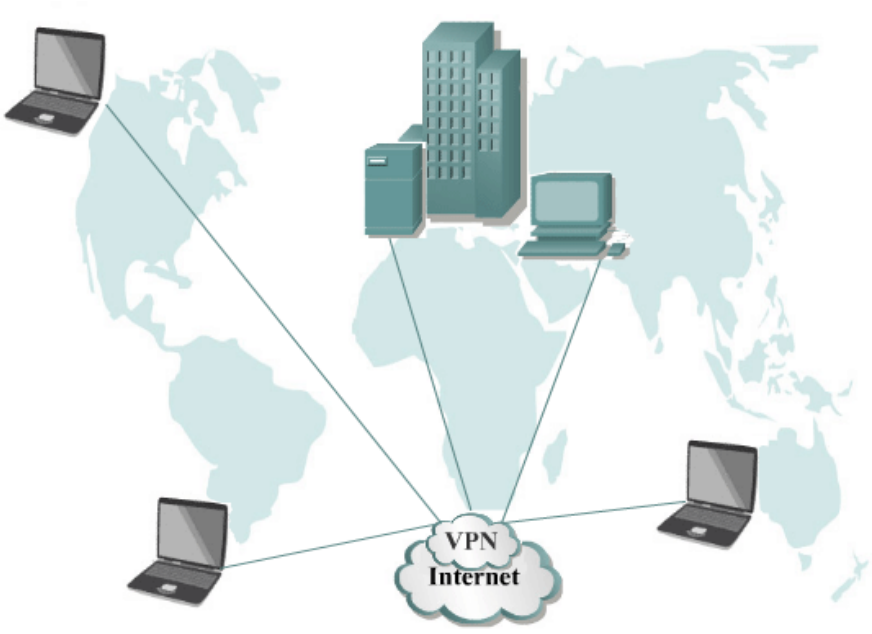


Рисунок 1.4 – Удаленный доступ отдельно взятых сотрудников

Организация такой модели виртуальной частной сети предполагает наличие VPN–сервера в центральном офисе, к которому подключаются удаленные клиенты. Удаленные клиенты могут работать на дому, либо, используя переносной компьютер, из любого места планеты, где есть доступ к всемирной паутине.

Данный способ организации виртуальной частной сети целесообразно применять в случаях:

- географически не привязанного доступа сотрудников к корпоративной сети организации;
- доступа к Интернету. Часто провайдеры создают для своих клиентов VPN подключения для организации доступа к ресурсам Интернет.

2 Связь в одну общую сеть территориально распределенных филиалов фирмы (Рисунок 1.5). Этот способ называется Intranet VPN.

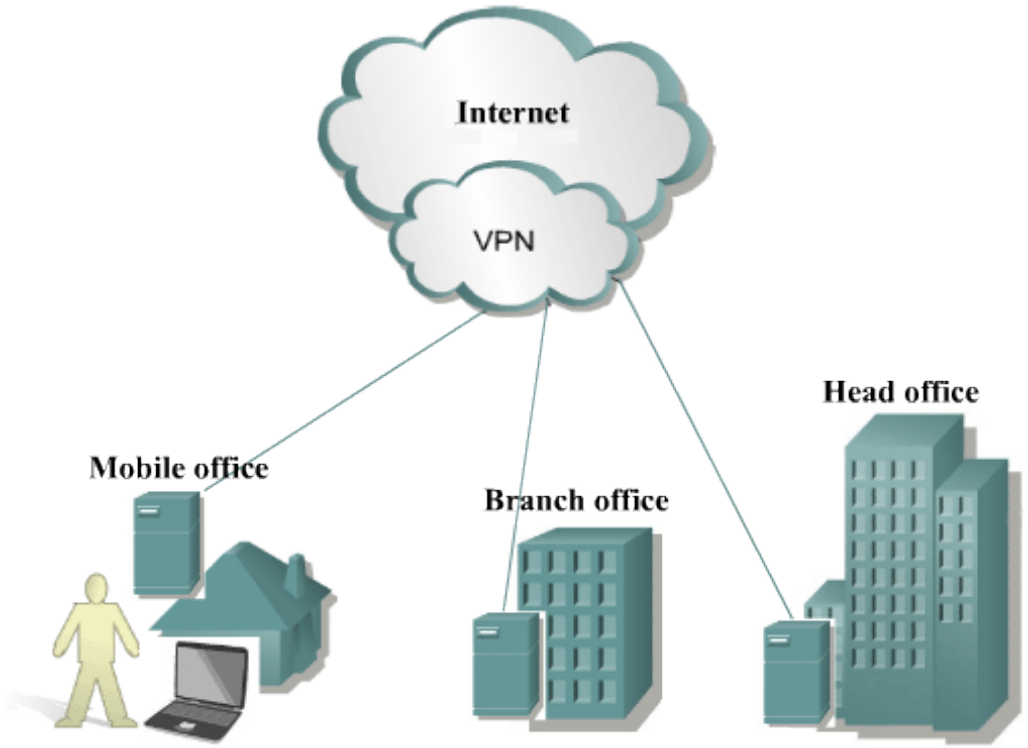


Рисунок 1.5 – Intranet VPN

При организации такой схемы подключения требуется наличие VPN серверов равное количеству связываемых офисов.

Данный способ целесообразно использовать как для обыкновенных филиалов, так и для мобильных офисов, которые будут иметь доступ к ресурсам «материнской» компании, а также без проблем обмениваться данными между собой.

3 Так называемый Extranet VPN, когда через безопасные каналы доступа предоставляется доступ для клиентов организации. Набирает широкое распространение в связи с популярностью электронной коммерции.

В этом случае для удаленных клиентов будут очень урезаны возможности по использованию корпоративной сети, фактически они будут ограничены доступом к тем ресурсам компании, которые необходимы при работе со своими клиентами, например, сайта с коммерческими предложениями, а VPN используется в этом случае для безопасной пересылки конфиденциальных данных [5].

### 1.5 Компоненты VPN

Сеть VPN состоит из четырех ключевых компонентов:

- Сервер VPN.
- Алгоритмы шифрования.
- Система аутентификации.
- Протокол VPN.

Эти компоненты реализуют соответствие требованиям по безопасности, производительности и способности к взаимодействию. То, насколько правильно реализована архитектура VPN, зависит от правильности определения требований. Определение требований должно включать в себя следующие аспекты:

1 Сервер VPN

Сервер VPN представляет собой компьютер, выступающий в роли конечного узла соединения VPN (Рисунок 1.6).

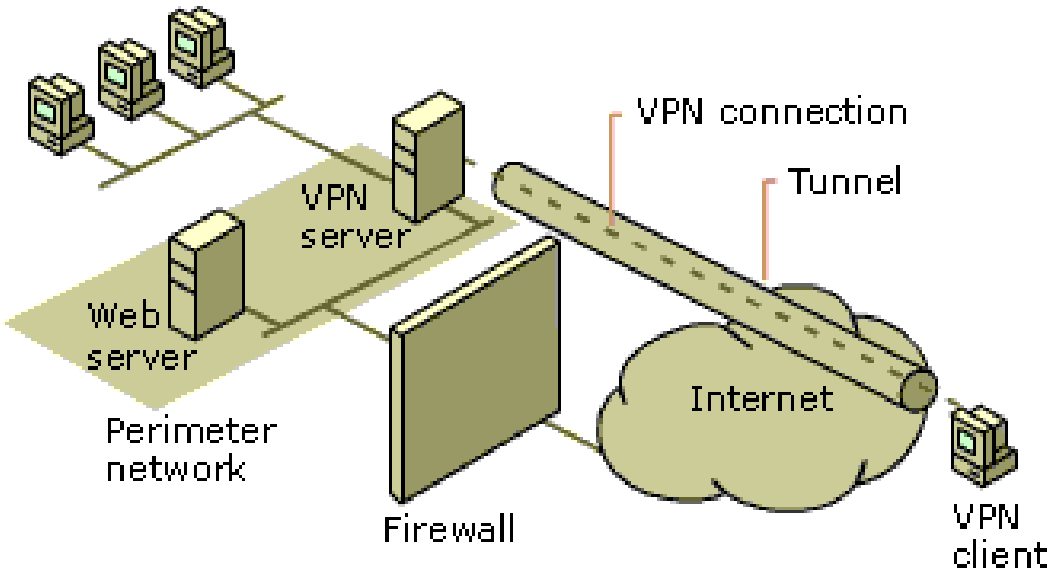


Рисунок 1.6 – Конфигурация сервера VPN

Данный сервер должен обладать характеристиками, достаточными для поддержки ожидаемой нагрузки. Большая часть производителей программного обеспечения VPN должна предоставлять рекомендации по поводу производительности процессора и конфигурации памяти, в зависимости числа единовременных VPN–соединений. Следует обеспечить наличие системы с соответствующими параметрами, а также позаботиться о ее дальнейшей модернизации.

2 Алгоритмы шифрования

Алгоритм шифрования, используемый в VPN, должен быть стандартным мощным алгоритмом шифрования (ранее в лекциях была приведена более подробная информация о системах шифрования). Возникает вопрос: какая же система шифрования самая лучшая? Вообще, все стандартные и мощные алгоритмы могут эффективно использоваться при построении VPN. Различные производители отдают предпочтение различным алгоритмам, в зависимости от ограничений реализации продукта, аспектов, связанных с лицензированием, и предпочтений по программированию. Приобретая программный пакет VPN, следует выслушать комментарии специалистов и убедиться в том, что производитель использует мощный алгоритм шифрования.

3 Система аутентификации

Третьим компонентом архитектуры VPN является система аутентификации. Система аутентификации VPN должна быть двухфакторной. Пользователи могут проходить аутентификацию с использованием того, что они знают, того, что у них есть или с помощью данных о том, кем они являются. При использовании пользовательских VPN отдается предпочтение первым двум вариантам.

4 Протокол VPN

Протокол VPN определяет, каким образом система VPN взаимодействует с другими системами в Интернете, а также уровень защищенности трафика. Если рассматриваемая организация использует VPN только для внутреннего информационного обмена, вопрос о взаимодействии можно оставить без внимания. Однако если организация использует VPN для соединения с другими организациями, собственные протоколы использовать, скорее всего, не удастся. Протокол VPN оказывает влияние на общий уровень безопасности системы. Причиной этому является тот факт, что протокол VPN используется для обмена ключами шифрования между двумя конечными узлами. Если этот обмен не защищен, злоумышленник может перехватить ключи и затем расшифровать трафик, сведя на нет все преимущества VPN [6].

### 1.6 Методы шифрования в VPN

Поскольку данные в виртуальных частных сетях передаются через общедоступную сеть, следовательно, они должны быть надежно защищены от посторонних глаз. Для реализации защиты передаваемой информации

существует множество протоколов, которые защищают VPN, но все они подразделяются на два вида и работают в паре:

- протоколы, инкапсулирующие данные и формирующие VPN соединение;
- протоколы, шифрующие данные внутри созданного туннеля.

Первый тип протоколов устанавливает туннелированное соединение, а второй тип отвечает непосредственно за шифрование данных. Рассмотрим некоторые стандартные, предлагаемые всемирно признанным мировым лидером в области разработки операционных систем, решения.

В качестве стандартного набора предлагается сделать выбор из двух протоколов, точнее будет сказать наборов:

1 PPTP (Point–to–Point Tunneling Protocol) – туннельный протокол «точка–точка», детище Microsoft и является расширением PPP (Point–to–Point Protocol), следовательно, использует его механизмы подлинности, сжатия и шифрования. Протокол PPTP является встроенным в клиент удаленного доступа Windows XP. При стандартном выборе данного протокола компанией Microsoft предлагается использовать метод шифрования MPPE (Microsoft Point–to–Point Encryption). Можно передавать данные без шифрования в открытом виде.

Инкапсуляция данных по протоколу PPTP происходит путем добавления заголовка GRE (Generic Routing Encapsulation) и заголовка IP к данным обработанных протоколом PPP.

PPTP удалось добиться популярности благодаря тому, что это первый протокол туннелирования, который был поддержан корпорацией Microsoft. Все версии Microsoft Windows, начиная с Windows 95 OSR2, включают в свой состав PPTP–клиент, однако существует ограничение на два одновременных исходящих соединения. А сервис удалённого доступа для Microsoft Windows включает в себя PPTP сервер.

Главная уязвимость PPTP на сегодняшний день заключается в слабости алгоритмов парольной аутентификации (MSCHAP, MSCHAPv2), а также в том, что при использовании этих алгоритмов сессионные ключи MPPE получаются из пользовательского пароля. Ведь редкий пользователь установит себе пароль типа «3hEML@4rj897#KJK$$», его будет сложновато запомнить, а вот, например, пароль «boomer» запомнить легко. А наличие простого пароля хотя бы у одного пользователя делает возможным проникновение злоумышленника во внутреннюю сеть организации [7].

2 L2TP (Layer Two Tunneling Protocol) – более совершенный протокол, родившийся в результате объединения протоколов PPTP (от Microsoft) и L2F (от Cisco), вобравший в себя все лучшее из этих двух протоколов. Предоставляет более защищенное соединение, нежели первый вариант, шифрование происходит средствами протокола IPSec (IP–security). L2TP является также встроенным в клиент удаленного доступа Windows XP, более того при автоматическом определении типа подключения клиент сначала

пытается соединиться с сервером именно по этому протоколу, как являющимся более предпочтительным в плане безопасности.

Инкапсуляция данных происходит путем добавления заголовков L2TP и IPSec к данным обработанным протоколом PPP. Шифрование данных достигается путем применения алгоритма DES (Data Encryption Standard) или 3DES. Именно в последнем случае достигается наибольшая безопасность передаваемых данных, однако в этом случае придется расплачиваться скоростью соединения, а также ресурсами центрального процессора.

В вопросе применения протоколов компания Microsoft и Cisco образуют некий симбиоз: протокол PPTP – разработка Microsoft, но используется совместно с GRE, а это продукт Cisco, далее более совершенный в плане безопасности протокол L2TP – это ни что иное, как гибрид, вобравший в себя все лучшее PPTP и L2F, да правильно, разработанный Cisco. Возможно именно поэтому VPN, при правильном подходе в организации, считается надежным способом передачи конфиденциальных данных [4].

### 1.7 Достоинства и недостатки VPN

Виртуальные частные сети имеют несколько преимуществ над традиционными частными сетями. Главные из них – экономичность, гибкость и удобство использования.

Экономичность. С помощью VPN–сетей предприятиям удается хотя бы частично ограничить рост числа модемов, серверов доступа, коммутируемых линий и других технических средств, которые организации вынуждены внедрять, чтобы обеспечить удаленным пользователям доступ к своим корпоративным сетям. Кроме того, виртуальные частные сети дают возможность удаленным пользователям обращаться к сетевым ресурсам компании не по дорогим арендованным линиям, а через местную телефонную связь.

Особенно выгодны виртуальные частные сети в тех случаях, когда пользователи удалены на большие расстояния и поэтому арендованные линии обходятся очень дорого, а также когда таких пользователей много, в связи с чем и им требуется большое количество арендованных линий. Однако эти преимущества могут сойти на нет, если объем трафика в VPN–сети настолько велик, что система не успевает зашифровывать и расшифровывать пакеты данных. Чтобы избежать возникновения таких узких мест, предприятие вынуждено покупать дополнительное оборудование.

Кроме того, из–за относительной новизны технологии VPN и сложности используемых средств безопасности системный администратор для виртуальной сети обходится дороже, чем для традиционной.

Исследовательская компания Forrester Research опубликовала следующие данные, характеризующие преимущество применения VPN поверх Internet (из расчета 1000 пользователей) по сравнению с созданием центра удаленного доступа (Remote Access Service) (Таблица 1.1).

Т а б л и ц а 1.1 – Преимущество применения VPN поверх Internet

| Статья затрат | Удаленный доступ (в млн. долл.) | VPN(в млн. долл.) |
|---|---|---|
| Оплата услуг провайдера связи | 1,08 | 0,54 |
| Расходы на эксплуатацию | 0,3 | 0,3 |
| Капиталовложения | 0,1 | 0,02 |
| Прочие расходы | 0,02 | 0,03 |
| Всего | 1,5 | 0,89 |

Из таблицы можно видеть, что использование VPN позволяет снизить многие статьи затрат, включая закупку коммуникационного оборудования, оплату услуг Internet–провайдера и т.д. Эти, а также другие исследования, позволили Международной Ассоциации Компьютерной Безопасности (International Computer Security Association, ICSA) причислить технологию VPN к десятке самых известных технологий, которые будут в первую очередь применяться многими компаниями.

Гибкость и удобство. Эти достоинства виртуальных частных сетей объясняются тем, что в отличие от традиционных такие сети могут обеспечить удаленный доступ к ресурсам компании любому уполномоченному пользователю, имеющему связь с Internet. Благодаря этому VPN–сети позволяют партнерам легко получить доступ к сетевым ресурсам предприятия через Internet, что способствует укреплению альянсов и повышению конкурентоспособности. Этого трудно достичь с помощью традиционных частных сетей, так как предприятия, желающие совместно использовать сетевые ресурсы, часто имеют несовместимые системы. Особенно остро эта проблема возникает, когда большое число организаций, таких как крупное предприятие розничной торговли и его поставщики, хотят работать вместе через сеть.

Но виртуальные частные сети имеют и недостатки. Проблемы защиты данных, недостаток надежности и производительности, а также отсутствие открытых стандартов затрудняют широкое распространение виртуальных частных сетей.

Защита. Для большинства технологий Internet вопросы обеспечения безопасности при передаче данных являются ключевыми. И виртуальные частные сети не исключение. Для них главные проблемы заключаются в аутентификации пользователей с помощью паролей и защите зашифрованного VPN–канала (тоннеля). Кроме того, сетевые администраторы должны тщательно выбирать методы, которые помогают пользователям получать доступ к виртуальным частным сетям.

Эти проблемы заставили некоторых потенциальных пользователей усомниться в том, что степень защиты данных будет удовлетворительной, если виртуальной частной сетью управляет провайдер услуг Internet. Чтобы успокоить недоверчивых пользователей, провайдеры поддерживают широкий

набор различных схем шифрования и аутентификации. Например, фирма Aventail, выпускающая ПО для виртуальных частных сетей, предлагает пакет программ для аутентификации клиентов и шифрования на уровне сеанса. Компания VPNet Technologies поставляет оборудование, устанавливаемое между маршрутизатором и глобальной сетью, которое выполняет шифрование, аутентификацию и сжатие данных.

Большинство поставщиков используют методы шифрования с 56–разрядным ключом, соответствующие стандарту DES. По их мнению, такая длина ключа обеспечивает достаточно высокий уровень безопасности. Однако многие эксперты и аналитики полагают, что 56–разрядный ключ недостаточно надежен. Некоторые поставщики продуктов для виртуальных частных сетей предлагают шифрование со 112–разрядным ключом. Тем не менее следует помнить, что увеличение длины ключа снижает производительность, так как чем сложнее алгоритм шифрования, тем более интенсивной вычислительной обработки он требует.

### 1.8 Перспективы VPN

По мере своего развития VPN превратятся в системы взаимосвязанных сетей, которые будут соединять мобильных пользователей, торговых партнеров и поставщиков с критически важными корпоративными приложениями, работающими в протоколе IP. VPN станут фундаментом для новых коммерческих операций и услуг, которые будут стимулировать рынок и помогать модернизировать производство.

Вероятно, первым из основных компонентов завтрашних VPN станет сервер каталогов, содержащий профили конечных пользователей и данные о конфигурации сети. При наличии сетевых каталогов и обеспечении безопасности информации и качества обслуживания конечные пользователи смогут практически мгновенно устанавливать соединения по VPN.

Вполне возможно, что будет использоваться протокол IpV6, работы над которым активно продолжаются. Данный протокол обладает всеми возможностями взаимодействия с VPN, какие только могут пожелать сетевые разработчики, в частности, управление полосой пропускания, определение принадлежности IpV6–пакетов к конкретному потоку (например, высший приоритет будут получать пакеты мультимедийных данных для передачи в реальном времени).

Главные игроки сетевого рынка уже активно готовятся к грядущему буму VPN. Нынешние вендоры программного обеспечения и оборудования предлагают наборы устройств для создания и эксплуатации VPN.

Выгоду от развертывания VPN следующего поколения получат не только сетевые разработчики. Не менее заинтересованы в них и операторы. Фирмы AT&T Level 3 Communications, MCI Worldcom и Sprint создают высокоскоростные IP–каналы в ATM–сетях для передачи видео, голоса и данных. VPN в настоящее время оказывают едва ли не решающее влияние на

разработку стратегии глобальных операторов, в частности, Unisource (AT&T, Telia, PTT Suisse и PTT Netherlands), Concert (BT/MCI) и Global One (Deutsche Telekom, France Telekom). Чем больше компаний будут предлагать VPN–услуги, тем заметнее будет расти их качество и падать цены, что, в свою очередь, повлияет на число клиентов.

Каждая революция в бизнесе начиналась с изобретения, которое способствовало активизации частной инициативы. Например, разделение перевозчиков и компаний, эксплуатирующих государственную железную дорогу, привело к резкому росту коммерческих перевозок. То же самое происходит при создании VPN поверх национальных и международных телекоммуникационных инфраструктур. Ближайшее время покажет, к каким изменениям это приведет.

## 2 IPSEC – протокол защиты сетевого трафика

Подключение любой корпоративной сети к публичной вызывает два типа угроз:

– несанкционированный доступ к ресурсам локальной сети, полученный в результате входа в эту сеть;

– несанкционированный доступ к данным при передаче трафика по публичной сети.

Для создания защищенного канала средства VPN используют процедуры шифрования, аутентификации и авторизации.

Шифрование. Методов шифрования довольно много, поэтому важно, чтобы на концах туннеля использовался один и тот же алгоритм шифрования. Кроме того, для успешного дешифрования данных источнику и получателю данных необходимо обменяться ключами шифрования. Следует отметить, что шифрование сообщений необходимо не всегда. Часто оно оказывается довольно дорогостоящей процедурой, требующей дополнительных приставок для маршрутизаторов, без которых они не могут одновременно с шифрованием обеспечивать приемлемый уровень быстродействия.

Аутентификация. Под аутентификацией понимается определение пользователя или конечного устройства. Аутентификация позволяет устанавливать соединения только между легальными пользователями и, соответственно, предотвращает доступ к ресурсам сети несанкционированных пользователей.

В процедуре участвуют две стороны: одна доказывает свою аутентичность, а другая ее проверяет и принимает решение.

Авторизация. Авторизация подразумевает предоставление абонентам различных видов услуг. Каждому пользователю предоставляются определенные администратором права доступа. Эта процедура выполняется после процедуры аутентификации и позволяет контролировать доступ санкционированных пользователей к ресурсам сети [15].

### 2.1 Технологии создания виртуальных частных сетей

Среди технологий построения VPN можно назвать такие технологии, как: IPSec VPN, MPLS VPN, VPN на основе технологий туннелирования. Во всех перечисленных случаях трафик посылается в сеть провайдера по протоколу IP, что позволяет провайдеру оказывать не только услуги VPN, но и различные дополнительные сервисы (контроль за работой клиентской сети, хостинг Web и почтовых служб, хостинг специализированных приложений клиентов).

*IPSec VPN.* Технология IPSec – стандарт Internet, при этом ее смело можно назвать одной из наиболее популярных и перспективных технологий обеспечения безопасности трафика в сетях IP. Стандарты IPSec обеспечивают высокую степень гибкости, позволяя выбирать нужный режим защиты (с

шифрованием или только с обеспечением аутентичности и целостности данных), а также использовать различные алгоритмы аутентификации и шифрования. Режим инкапсуляции IPSec позволяет изолировать адресные пространства клиента и провайдера за счет применения двух IP–адресов – внешнего и внутреннего.

Чаще всего IPSec нужны для поддерживаемых клиентом VPN (CPVPN), когда он самостоятельно создает туннели IPSec через сеть IP провайдера. Причем от последнего требуется только предоставление стандартного сервиса по объединению сетей – а значит, доступны как услуги в пределах сети провайдера, так и услуги Internet. Сложность конфигурирования IPSec VPN высокая – поскольку туннели IPSec представляют собой туннели «точка–точка», то при полносвязной топологии их количество пропорционально N x (N–1). Необходимо учесть еще и непростую задачу поддержания инфраструктуры ключей.

IPSec может применяться и для создания VPN, поддерживаемых провайдером, – туннели в них также строятся на базе устройств клиента (CE–based), но эти устройства удаленно конфигурируются и управляются провайдером.

*VPN на основе туннелирования через IP*. Этот термин объединяет различные технологии, которые для образования VPN используют туннели через сеть IP провайдера. Туннель обеспечивает изоляцию адресного пространства клиента, он может переносить незашифрованный трафик (GRE, L2TP) или же шифровать его (PPTP).

Таблицы маршрутизации для клиентов могут быть построены автоматически – с помощью протокола BGP и техники виртуального маршрутизатора. Виртуальный маршрутизатор соответствует случаю, когда для каждого узла клиента создается отдельная таблица маршрутизации. Протокол BGP с расширениями позволяет изолировать маршрутную информацию различных VPN, распространяя ее только между виртуальными маршрутизаторами, принадлежащими одной VPN. В некоторых вариантах таких VPN обеспечивается автоматическое построение туннеля во время добавления нового узла к сети провайдера (и соответствующем конфигурировании виртуального маршрутизатора). В этой ситуации сложность конфигурирования VPN становится пропорциональной не числу туннелей, а числу узлов – т. е. достигается масштабируемость обычных сетей IP.

С точки зрения пользователя, такие VPN ничем не отличаются от стандартной сети IP, так как их функциональность скрыта от пользователя наложенной структурой [14].

Недостатком данного типа VPN можно считать применение не очень распространенных методов туннелирования (а в случае PPTP они даже не являются стандартом Internet), что сдерживает их развитие и не сулит хороших перспектив.

*MPLS VPN*. Этот тип VPN сочетает свойства VPN второго и третьего уровней, так как доставка трафика до пограничного устройства сети провайдера

осуществляется с помощью протокола IP (третий уровень), а внутри сети провайдера – с помощью MPLS. Правда, уровень MPLS определить не так просто – это постоянная тема яростных (и часто безрезультатных) споров о терминологии, но продвижение пакетов на основе локальных меток соответствует второму уровню. Сегодня основным документом, описывающим организацию MPLS VPN, считается информационный RFC 2547, подготовленный специалистами Cisco Systems.

Методика продвижения, аналогичная виртуальным каналам ATM/FR, обеспечивает MPLS VPN безопасность примерно в той же степени, что и ATM/FR VPN.

MPLS VPN использует разделение адресных пространств клиентов с помощью виртуального маршрутизатора, а протокол BGP с расширениями обеспечивает автоматическое построение таблиц маршрутизации клиентов. Пути MPLS между узлами клиентов устанавливаются автоматически, также с помощью BGP, так что сложность конфигурирования MPLS VPN пропорциональна количеству узлов клиента – это хорошая масштабируемость.

MPLS VPN не обеспечивают безопасность за счет шифрования и аутентификации, как это делает IPSec или PPTP, но допускает применение данных технологий как дополнительных мер защиты в случае необходимости.

На рисунке 2.1 представлен общий вариант построения виртуальной частной сети на базе общедоступной сети провайдера. Сеть каждого клиента состоит из территориально распределенных офисов, которые связаны между туннелями, проложенными через сеть провайдера.

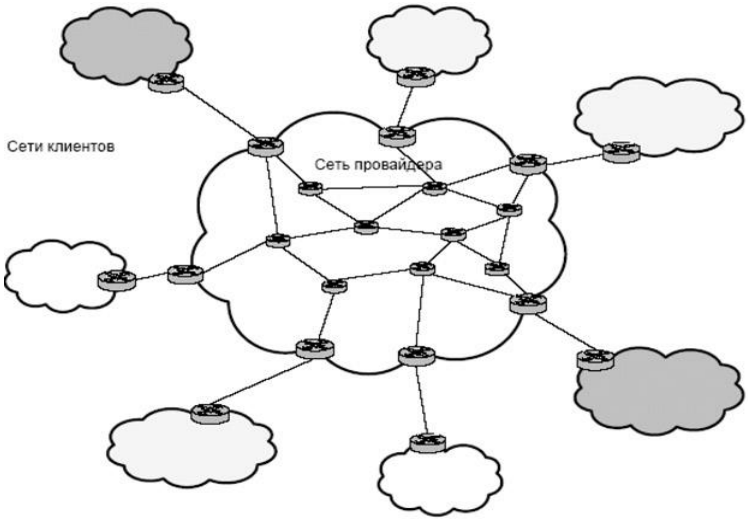


Рисунок 2.1 – Общий вариант построения виртуальной частной сети

## 2.2 Необходимость защиты данных

В конце шестидесятых годов американское агентство перспективных исследований в обороне DARPA приняло решение о создании экспериментальной сети под названием ARPANet. В семидесятых годах

ARPANet стала считаться действующей сетью США, и через эту сеть можно было получить доступ к ведущим университетским и научным центрам США. В начале восьмидесятых годов началась стандартизация языков программирования, а затем и протоколов взаимодействия сетей. Результатом этой работы стала разработка семиуровневой модели сетевого взаимодействия ISO/OSI и семейства протоколов TCP/IP, которое стало основой для построения как локальных, так и глобальных сетей.

Базовые механизмы информационного обмена в сетях TCP/IP были в целом сформированы в начале восьмидесятых годов, и были направлены прежде всего на обеспечение доставки пакетов данных между различными операционными системами с использованием разнородных каналов связи. Несмотря на то, что идея создания сети ARPANet (впоследствии превратившейся в современный Интернет) принадлежала правительственной оборонной организации, фактически сеть зародилась в исследовательском мире, и наследовала традиции открытости академического сообщества. Ещё до коммерциализации Интернета (которая произошла в середине девяностых годов) многие авторитетные исследователи отмечали проблемы, связанные с безопасностью стека протоколов TCP/IP. Основные концепции протоколов TCP/IP не полностью удовлетворяют (а в ряде случаев и противоречат) современным представлениям о компьютерной безопасности [16].

До недавнего времени сеть Интернет использовалась в основном для обработки информации по относительно простым протоколам: электронная почта, передача файлов, удалённый доступ. Сегодня, благодаря широкому распространению технологий WWW, всё активнее применяются средства распределённой обработки мультимедийной информации. Одновременно с этим растёт объём данных, обрабатываемых в средах клиент/сервер и предназначенных для одновременного коллективного доступа большого числа абонентов. Разработано несколько протоколов прикладного уровня, обеспечивающих информационную безопасность таких приложений, как электронная почта (PEM, PGP и т.п.), WWW (Secure HTTP, SSL и т.п.), сетевое управление (SNMPv2 и т.п.). Однако наличие средств обеспечения безопасности в базовых протоколах семейства TCP/IP позволит осуществлять информационный обмен между широким спектром различных приложений и сервисных служб.

В документе "Безопасность архитектуры Интернет" описываются основные области применения дополнительных средств безопасности в сети Интернет, а именно защита от несанкционированного мониторинга, подмены пакетов и управления потоками данных. В числе первоочередных и наиболее важных защитных мер указывалась необходимость разработки концепции и основных механизмов обеспечения целостности и конфиденциальности потоков данных. Поскольку изменение базовых протоколов семейства TCP/IP вызвало бы полную перестройку сети Интернет, была поставлена задача обеспечения безопасности информационного обмена в открытых телекоммуникационных сетях на базе существующих протоколов. Таким

образом, начала создаваться спецификация Secure IP, дополнительная по отношению к протоколам IPv4 и IPv6.

### 2.3 Архитектура IPSec

IP Security – это комплект протоколов, касающихся вопросов шифрования, аутентификации и обеспечения защиты при транспортировке IP–пакетов; в его состав сейчас входят почти 20 предложений по стандартам и 18 RFC (Рисунок 2.2).

Спецификация IP Security (известная сегодня как IPsec) разрабатывается Рабочей группой IP Security Protocol IETF. Первоначально IPsec включал в себя 3 алгоритмо–независимые базовые спецификации, опубликованные в качестве RFC–документов "Архитектура безопасности IP", "Аутентифицирующий заголовок (AH)", "Инкапсуляция зашифрованных данных (ESP)" (RFC1825, 1826 и 1827). Необходимо заметить, что в ноябре 1998 года Рабочая группа IP Security Protocol предложила новые версии этих спецификаций, имеющие в настоящее время статус предварительных стандартов, это RFC2401 – RFC2412. Отметим, что RFC1825–27 на протяжении уже нескольких лет считаются устаревшими и реально не используются. Кроме этого, существуют несколько алгоритмо–зависимых спецификаций, использующих протоколы MD5, SHA, DES.

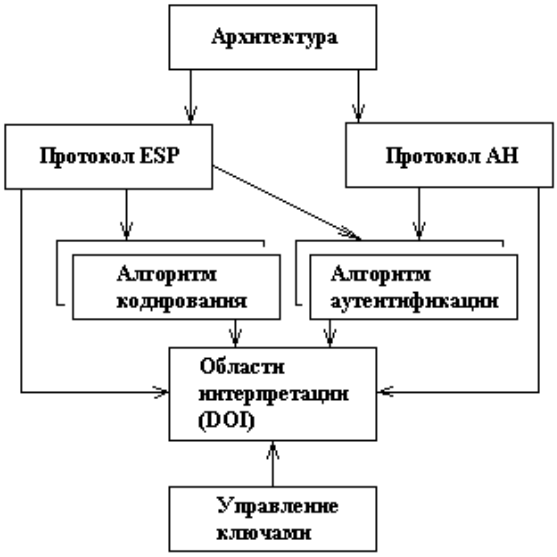


Рисунок 2.2 – Архитектура IPSec

Рабочая группа IP Security Protocol разрабатывает также и протоколы управления ключевой информацией. В задачу этой группы входит разработка Internet Key Management Protocol (IKMP), протокола управления ключами прикладного уровня, не зависящего от используемых протоколов обеспечения безопасности. В настоящее время рассматриваются концепции управления ключами с использованием спецификации Internet Security Association and Key

Management Protocol (ISAKMP) и протокола Oakley Key Determination Protocol. Спецификация ISAKMP описывает механизмы согласования атрибутов используемых протоколов, в то время как протокол Oakley позволяет устанавливать сессионные ключи на компьютеры сети Интернет. Ранее рассматривались также возможности использования механизмов управления ключами протокола SKIP, однако сейчас такие возможности реально практически нигде не используются. Создаваемые стандарты управления ключевой информацией, возможно, будут поддерживать Центры распределения ключей, аналогичные используемым в системе Kerberos. Протоколами ключевого управления для IPSec на основе Kerberos сейчас занимается относительно новая рабочая группа KINK (Kerberized Internet Negotiation of Keys).

Гарантии целостности и конфиденциальности данных в спецификации IPsec обеспечиваются за счет использования механизмов аутентификации и шифрования соответственно. Последние, в свою очередь, основаны на предварительном согласовании сторонами информационного обмена т.н. "контекста безопасности" – применяемых криптографических алгоритмов, алгоритмов управления ключевой информацией и их параметров. Спецификация IPsec предусматривает возможность поддержки сторонами информационного обмена различных протоколов и параметров аутентификации и шифрования пакетов данных, а также различных схем распределения ключей. При этом результатом согласования контекста безопасности является установление индекса параметров безопасности (SPI), представляющего собой указатель на определенный элемент внутренней структуры стороны информационного обмена, описывающей возможные наборы параметров безопасности [17].

По сути, IPSec, который станет составной частью IPv6, работает на третьем уровне, т. е. на сетевом уровне. В результате передаваемые IP–пакеты будут защищены прозрачным для сетевых приложений и инфраструктуры образом. В отличие от SSL (Secure Socket Layer), который работает на четвертом (т.е. транспортном) уровне и теснее связан с более высокими уровнями модели OSI (Рисунок 2.3), IPSec призван обеспечить низкоуровневую защиту.

| Уровни TCP/IP | Уровни ISO/OSI |
|---|---|
| 4. Прикладных программ | 7. Прикладных программ<br>6. Представление данных |
| 3. Транспортный | 5. Сеансовый<br>4. Транспортный |
| 2. Межсетевой | 3. Сетевой |
| 1. Доступа к сети | 2. Канальный<br>1. Физический |

Рисунок 2.3 – Модель OSI/ISO

К IP–данным, готовым к передаче по виртуальной частной сети, IPSec добавляет заголовок для идентификации защищенных пакетов. Перед передачей по Internet эти пакеты инкапсулируются в другие IP–пакеты. IPSec поддерживает несколько типов шифрования, в том числе Data Encryption Standard (DES) и Message Digest 5 (MD5).

Чтобы установить защищенное соединение, оба участника сеанса должны иметь возможность быстро согласовать параметры защиты, такие как алгоритмы аутентификации и ключи. IPSec поддерживает два типа схем управления ключами, с помощью которых участники могут согласовать параметры сеанса. Эта двойная поддержка в свое время вызвала определенные трения в IETF Working Group.

С текущей версией IP, IPv4, могут быть использованы или Internet Secure Association Key Management Protocol (ISAKMP), или Simple Key Management for Internet Protocol. С новой версией IP, IPv6, придется использовать ISAKMP, известный сейчас как IKE, хотя не исключается возможность использования SKIP. Однако, следует иметь в виду, что SKIP уже давно не рассматривается как кандидат управления ключами, и был исключён из списка возможных кандидатов ещё в 1997 г.

***Заголовок AH***

Аутентифицирующий заголовок (AH) является обычным опциональным заголовком и, как правило, располагается между основным заголовком пакета IP и полем данных. Наличие AH никак не влияет на процесс передачи информации транспортного и более высокого уровней. Основным и единственным назначением AH является обеспечение защиты от атак, связанных с несанкционированным изменением содержимого пакета, и в том числе от подмены исходного адреса сетевого уровня. Протоколы более высокого уровня должны быть модифицированы в целях осуществления проверки аутентичности полученных данных.

Формат AH достаточно прост и состоит из 96–битового заголовка и данных переменной длины, состоящих из 32–битовых слов. Названия полей достаточно ясно отражают их содержимое: Next Header указывает на следующий заголовок, Payload Len представляет длину пакета, SPI является указателем на контекст безопасности и Sequence Number Field содержит последовательный номер пакета (Рисунок 2.4).


Рисунок 2.4 – Формат заголовка AH

Последовательный номер пакета был введен в AH в 1997 году в ходе процесса пересмотра спецификации IPsec. Значение этого поля формируется отправителем и служит для защиты от атак, связанных с повторным использованием данных процесса аутентификации. Поскольку сеть Интернет не гарантирует порядок доставки пакетов, получатель должен хранить информацию о максимальном последовательном номере пакета, прошедшего успешную аутентификацию, и о получении некоторого числа пакетов, содержащих предыдущие последовательные номера (обычно это число равно 64).

В отличие от алгоритмов вычисления контрольной суммы, применяемых в протоколах передачи информации по коммутируемым линиям связи или по каналам локальных сетей и ориентированных на исправление случайных ошибок среды передачи, механизмы обеспечения целостности данных в открытых телекоммуникационных сетях должны иметь средства защиты от внесения целенаправленных изменений. Одним из таких механизмов является специальное применение алгоритма MD5: в процессе формирования AH последовательно вычисляется хэш–функция от объединения самого пакета и некоторого предварительно согласованного ключа, а затем от объединения полученного результата и преобразованного ключа. Данный механизм применяется по умолчанию в целях обеспечения всех реализаций IPv6, по крайней мере, одним общим алгоритмом, не подверженным экспортным ограничениям.

***Заголовок ESP***

В случае использования инкапсуляции зашифрованных данных заголовок ESP является последним в ряду опциональных заголовков, "видимых" в пакете. Поскольку основной целью ESP является обеспечение конфиденциальности данных, разные виды информации могут требовать применения существенно различных алгоритмов шифрования. Следовательно, формат ESP может претерпевать значительные изменения в зависимости от используемых криптографических алгоритмов (Рисунок 2.5).

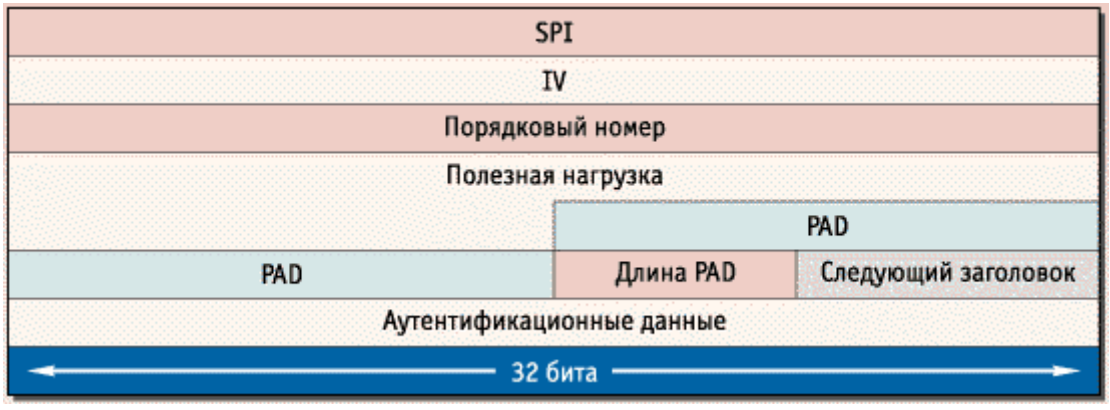


Рисунок 2.5 – Формат заголовка ESP

Тем не менее, можно выделить следующие обязательные поля: SPI, указывающее на контекст безопасности и Sequence Number Field, содержащее последовательный номер пакета. Поле "ESP Authentication Data" (контрольная сумма), не является обязательным в заголовке ESP. Получатель пакета ESP расшифровывает ESP заголовок и использует параметры и данные применяемого алгоритма шифрования для декодирования информации транспортного уровня.

Различают два режима применения ESP и AH (а также их комбинации) – транспортный и туннельный.

***Транспортный режим***

Транспортный режим используется для шифрования поля данных IP пакета, содержащего протоколы транспортного уровня (TCP, UDP, ICMP), которое, в свою очередь, содержит информацию прикладных служб. Примером применения транспортного режима является передача электронной почты. Все промежуточные узлы на маршруте пакета от отправителя к получателю используют только открытую информацию сетевого уровня и, возможно, некоторые опциональные заголовки пакета (в IPv6). Недостатком транспортного режима является отсутствие механизмов скрытия конкретных отправителя и получателя пакета, а также возможность проведения анализа трафика. Результатом такого анализа может стать информация об объемах и направлениях передачи информации, области интересов абонентов, расположение руководителей.

***Туннельный режим***

Туннельный режим предполагает шифрование всего пакета, включая заголовок сетевого уровня. Туннельный режим применяется в случае необходимости скрытия информационного обмена организации с внешним миром. При этом, адресные поля заголовка сетевого уровня пакета, использующего туннельный режим, заполняются межсетевым экраном организации и не содержат информации о конкретном отправителе пакета. При передаче информации из внешнего мира в локальную сеть организации в качестве адреса назначения используется сетевой адрес межсетевого экрана. После расшифровки межсетевым экраном начального заголовка сетевого уровня пакет направляется получателю.

Протокол IPSec можно использовать как в транспортном, так и в туннельном режиме (Рисунок 2.6). В первом случае заголовок IPSec размещается между сетевым (IP) и транспортным (TCP или UDP) заголовками обычного IP–пакета. Транспортный режим разработан для применения на оконечных системах. Работа в этом режиме отражается на всех входящих в группу системах и в большинстве случаев требуется перепрограммирование приложений.

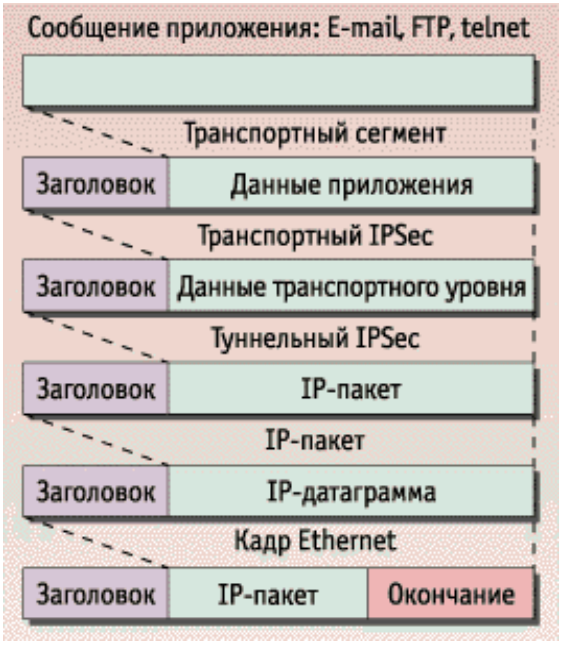


Рисунок 2.6 – Инкапсуляция протоколов

***Security Associations***

Security Association (SA) – это соединение, которое предоставляет службы обеспечения безопасности трафика, который передаётся через него. Два компьютера на каждой стороне SA хранят режим, протокол, алгоритмы и ключи, используемые в SA. Каждый SA используется только в одном направлении. Для двунаправленной связи требуется два SA. Каждый SA реализует один режим и протокол; таким образом, если для одного пакета необходимо использовать два протокола (как например AH и ESP), то требуется два SA.

***Политика безопасности***

Политика безопасности хранится в SPD (База данных политики безопасности). SPD может указать для пакета данных одно из трёх действий: отбросить пакет, не обрабатывать пакет с помощью IPSec, обработать пакет с помощью IPSec. В последнем случае SPD также указывает, какой SA необходимо использовать (если, конечно, подходящий SA уже был создан) или указывает, с какими параметрами должен быть создан новый SA.

SPD является очень гибким механизмом управления, который допускает очень хорошее управление обработкой каждого пакета. Пакеты классифицируются по большому числу полей, и SPD может проверять некоторые или все поля для того, чтобы определить соответствующее действие. Это может привести к тому, что весь трафик между двумя машинами будет передаваться при помощи одного SA, либо отдельные SA будут использоваться для каждого приложения, или даже для каждого TCP соединения.

***ISAKMP/Oakley***

Протокол ISAKMP определяет общую структуру протоколов, которые используются для установления SA и для выполнения других функций управления ключами. ISAKMP поддерживает несколько Областей Интерпретации (DOI), одной из которых является IPSec–DOI. ISAKMP не определяет законченный протокол, а предоставляет "строительные блоки" для различных DOI и протоколов обмена ключами.

Протокол Oakley – это протокол определения ключа, использующий алгоритм замены ключа Диффи–Хеллмана. Протокол Oakley поддерживает идеальную прямую безопасность (Perfect Forward Secrecy – PFS). Наличие PFS означает невозможность расшифровки всего траффика при компрометации любого ключа в системе.

***IKE***

IKE – протокол обмена ключами по умолчанию для ISAKMP, на данный момент являющийся единственным. IKE находится на вершине ISAKMP и выполняет, собственно, установление как ISAKMP SA, так и IPSec SA. IKE поддерживает набор различных примитивных функций для использования в протоколах. Среди них можно выделить хэш–функцию и псевдослучайную функцию (PRF).

Хэш–функция – это функция, устойчивая к коллизиям. Под устойчивостью к коллизиям понимается тот факт, что невозможно найти два разных сообщения $m_1$ и $m_2$, таких, что $H(m_1)=H(m_2)$, где $H$ – хэш функция.

Что касается псеводслучайных функций, то в настоящее время вместо специальных PRF используется хэш функция в конструкции HMAC (HMAC – механизм аутентификации сообщений с использованием хэш функций). Для определения HMAC нам понадобится криптографическая хэш функция (обозначим её как H) и секретный ключ K. Мы предполагаем, что H является хэш функцией, где данные хэшируются с помощью процедуры сжатия, последовательно применяемой к последовательности блоков данных. Мы обозначим за B длину таких блоков в байтах, а длину блоков, полученных в результате хэширования – как L (L<B). Ключ K может иметь длину, меньшую или равную B. Если приложение использует ключи большей длины, сначала мы должны хэшировать сам ключ с использованием H, и только после этого использовать полученную строку длиной L байт, как ключ в HMAC. В обоих случаях рекомендуемая минимальная длина для K составляет L байт.

Из описания следует, что IKE использует для аутентификации сторон HASH величины.

## 2.4 Атаки на AH, ESP и IKE

Все виды атак на компоненты IPSec можно разделить на следующие группы: атаки, эксплуатирующие конечность ресурсов системы (типичный пример – атака "Отказ в обслуживании", Denial–of–service или DOS–атака),

атаки, использующие особенности и ошибки конкретной реализации IPSec и, наконец, атаки, основанные на слабостях самих протоколов. AH и ESP. Если используемый криптоалгоритм стоек, а определенный с ним трансформ не вносит дополнительных слабостей (это не всегда так, поэтому правильнее рассматривать стойкость всей системы – Протокол–Трансформ–Алгоритм), то с этой стороны все нормально. Что остается? Replay Attack – нивелируется за счет использования Sequence Number (в одном единственном случае это не работает – при использовании ESP без аутентификации и без AH). Далее, порядок выполнения действий (сначала шифрация, потом аутентификация) гарантирует быструю отбраковку "плохих" пакетов (более того, именно такой порядок действий наиболее безопасен, обратный порядок в некоторых, правда очень частных случаях, может привести к потенциальным дырам в безопасности; к счастью, ни SSL, ни IKE, ни другие распространенные протоколы с порядком действий "сначала аутентифицировать, потом зашифровать", к этим частным случаям не относятся). Остается Denial–Of–Service атака. Как известно, это атака, от которой не существует полной защиты. Тем не менее, быстрая отбраковка плохих пакетов и отсутствие какой–либо внешней реакции на них (согласно RFC) позволяют более–менее хорошо справляться с этой атакой. В принципе, большинству известным сетевым атакам (sniffing, spoofing, hijacking и т.п.) AH и ESP при правильном их применении успешно противостоят. С IKE несколько сложнее. Протокол очень сложный, тяжел для анализа. Кроме того, в силу опечаток (в формуле вычисления HASH_R) при его написании и не совсем удачных решений (тот же HASH_R и HASH_I) он содержит несколько потенциальных "дыр" (в частности, в первой фазе не все Payload в сообщении аутентифицируются), впрочем, они не очень серьезные и ведут, максимум, к отказу в установлении соединения. От атак типа replay, spoofing, sniffing, hijacking IKE более–менее успешно защищается. С криптографией несколько сложнее, – она не вынесена, как в AH и ESP, отдельно, а реализована в самом протоколе. Тем не менее, при использовании стойких алгоритмов и примитивов (PRF), проблем быть не должно. В какой–то степени можно рассматривать как слабость IPsec то, что в качестве единственного обязательного к реализации криптоалгоритма в нынешних спецификациях указывается DES (это справедливо и для ESP, и для IKE), 56 бит ключа которого уже не считаются достаточными. Тем не менее, это чисто формальная слабость – сами спецификации являются алгоритмо–независимыми, и практически все известные вендоры давно реализовали 3DES (а некоторые уже и AES).Таким образом, при правильной реализации, наиболее "опасной" атакой остается Denial–Of–Service [18].

# 3 Проектирование сети с подключением удаленных филиалов и мобильных сотрудников с использованием технологии VPN для ТОО “TNS–INTEC”

## 3.1 Место реализации проекта

ТОО "TNS–INTEC" с момента своего образования в 1997 году является научно–производственной фирмой, основная сфера деятельности которой состоит в разработке, проектировании, производстве, поставке и монтаже комплексных средств автоматизации и энергетики в различных областях промышленности (Рисунок 3.1).


Рисунок 3.1 – Логотип фирмы

Целью организации является обеспечение растущего казахстанского рынка системами автоматизации и электротехнического оборудования с помощью внедрения лучших мировых технологий и стандартов, повышая критерии производственной эффективности для местных производителей, иностранных инвесторов и частных предпринимателей.

TNS–Intec является научно–производственной фирмой, основная сфера деятельности которой состоит в разработке, проектировании, производстве, поставке и монтаже комплексных средств автоматизации и энергетики в различных областях промышленности. Основные направления деятельности: решение комплекса задач по автоматизации технологических процессов в области добычи и транспортировки нефти и газа; разработка и внедрение АСКУЭ, разработка и внедрение автоматизированных систем управления технологическими процессами. Автоматизация в различных областях промышленности. Проектирование и внедрение взрывозащищенного электротехнического оборудования, аппаратуры и систем автоматизации контрольно–измерительных приборов и автоматики нефтегазовой, горной, металлургической и техническое обслуживание взрывозащищенного электротехнического оборудования противоаварийной защиты и сигнализации Сервисное обслуживание средств и систем автоматизации конструкторских работ. Реализация проектных, конструкторских работ по средствам и системам автоматизации. Проектирование и внедрение систем учета энергоносителей на базе системы «Emcos Corporate», расходы Внедрение автоматизированной

системы управления уличным освещением (АСУ УО) нового поколения, имеющую три режима: вечер, ночь и новый режим, регламентированный Европейским Союзом – режим пригашения уличного освещения. В Европейском Союзе запрещена экономия электроэнергии путем частичного отключения ламп уличного освещения. Внедрением автоматизированной системы управления технологическими параметрами энергетических подстанций нового поколения. АСУТП, предоставляемая нами совместно с СП ЗАО «Sigma Telas», позволяет полностью автоматизировать электрические подстанции всех уровней напряжения, от 500 до 0,4кВ. Автоматизация АстанаТеплоТранзит, АО "КазТрансОйл", РГП «Канал им. Сатпаева», АО НК «Казахстан Темір Жолы», ТОО «КокшетауЭнерго», Министерства Финансов РК, АО «Локомотив», Sigma Telas Emcos, Elgama, Electronika, Siemens.

В данный момент компания осуществляет проект АСУ ЭДТ для АО «Локомотив». АО «Локомотив» является одним из крупных потребителей дизельного топлива и электроэнергии, как среди компаний группы АО «НК «КТЖ», так и по стране, в целом. Доля расходов топливно–энергетических ресурсов составляет 40% от общего бюджета расходов предприятия, из числа которых 97% приходится на тягу поездов. В связи с этим, повышение энергоэффективности рассматривается как значительный вклад в будущее, а внедрение автоматизированной системы управления энергией для локомотивного хозяйства – большим шагом к энергосбережению.

Начиная с 2013 года, в АО «Локомотив» поэтапно внедряет автоматизированную систему управления «Энергодиспетчерская тяга» (АСУ ЭДТ). Работа ведется в рамках заключенного долгосрочного договора между АО «Локомотив» и АО «Транстелеком». Согласно этому договору АО «Транстелеком» взял на себя функцию единого интегратора и обеспечит внедрение АСУ ЭДТ «под ключ», включая все составляющие системы: программное обеспечение; сервисное оборудование; пункты ввода информации в локомотивных депо; персональные устройства хранения данных машинистов; бортовое оборудование локомотивов; информационный обмен локомотива и центрального сервера. Кроме того, «Транстелеком» занимается вопросами подготовки персонала «Локомотива» для работы с АСУ ЭДТ и предоставляет доступ пользователей к данным и функциональности этой системы.

Проект АСУ ЭДТ направлен на то, чтобы комплексно, автоматизировано и информационно поддерживать бизнес–процессы по учету, контролю и анализу потребления топливно–энергетических ресурсов. Система без участия человека сможет сопоставить фактический расход дизельного топлива и электроэнергии с параметрами проделанной каждым локомотивом работы, а именно: расстояние, скорость движения, вес груза, режим работы, профиль пути, и дать сигнал к аномальным отклонениям расхода топлива или режима эксплуатации локомотива. Одна из функций АСУ ЭДТ направлена на то, чтобы исключить факты несанкционированного расхода дизельного топлива. Система имеет возможность создавать оптимальный подбор мощности локомотивов под конкретный поезд, выявлять «узкие места», как в процессах эксплуатации, так и

в организации движения поездов, выявлять резервы уменьшения простоя локомотивов, уменьшить запасы топлива на складах за счет улучшения логистики их поставок. Информация, которая будет собираться АСУ ЭДТ в реальном времени, позволит не только получить предельно прозрачную отчетность, но и создаст оптимальные условия для оперативного принятия управленческих решений.

### 3.2 Разработка структурной схемы организации сети

Основной задачей данного дипломного проекта является проектирование защищенной сети между головным офисом в городе Астана и удаленным филиалом в городе Алматы. (Рисунок 3.2).

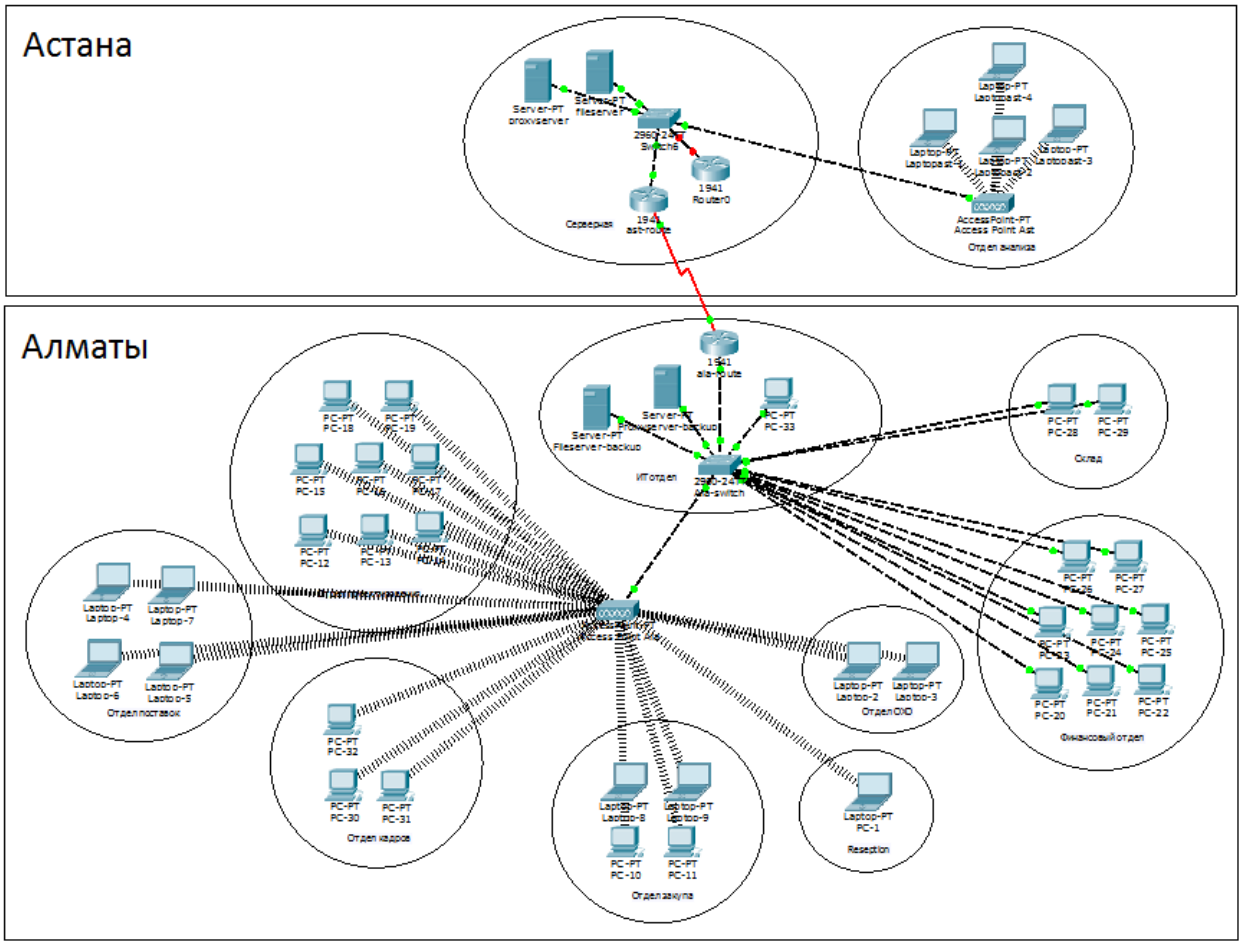


Рисунок 3.2 – Схема построения защищенной сети между головным офисом в городе Астана и удаленным филиалом в городе Алматы

Так как компания занимается автоматизацией подвижных составов, этот проект крайне необходим для того, чтобы автоматизировано и информационно поддерживать бизнес–процессы по учету, контролю и анализу потребления топливно–энергетических ресурсов.

Также это необходимо и для удаленных сотрудников, находящихся в командировках (Рисунок 3.3). В любой момент времени получить данные с локомотива, обработать их, составить отчет – залог успешной работы как для сотрудника так и для организации.

Среди всех основных выгод, можно выделить преимущества VPN для клиента:

– Высокие скорости подключения.

– Гарантированная полоса пропускания виртуальных каналов связи.

– Отсутствие оплаты за кабельные линии, соединяющие локальные сети.

– Более экономичное, надежное и безопасное решение для создания VPN.

Основные преимущества в работе компании при использовании VPN–доступа в том, что уменьшаются затраты на:

– Закупку, монтаж и конфигурирование серверов удаленного доступа и модемов.

– Сетевое оборудование.

– Управление клиентским программным обеспечением.

– Контроль трафика удаленного доступа.

– Телефонные соединения.

– Количество высококвалифицированных сетевых администраторов.

– Требуемое число портов доступа при увеличивающемся количестве удаленных пользователей.

– Линии связи.

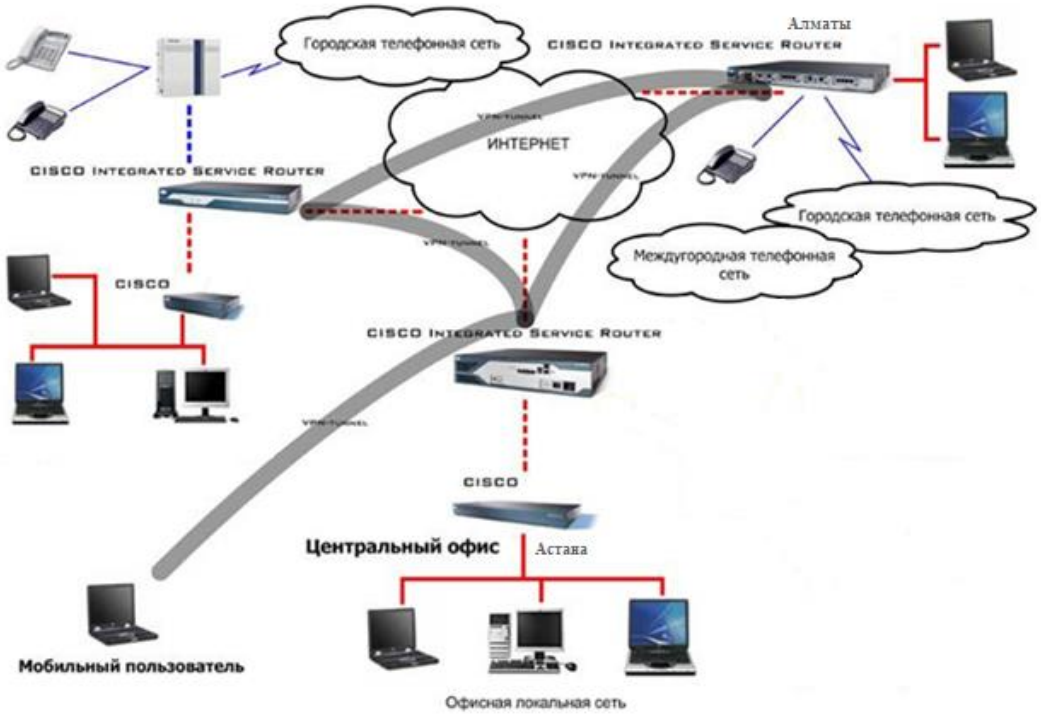


Рисунок 3.3 – Структурная схема организации сети

## 3.3 Описание и характеристики выбранного оборудования

На сегодняшний день рынок оборудования представлен большим разнообразием производителей. Выбор того или иного производителя должен проводится с учетом множества факторов, основные из них это: годность оборудования для реализации данного проекта, используемая технология, совместимость с другим оборудованием, стоимость оборудования.

При сравнении производителей большое преимущество имеет продукция компании Cisco Systems. Это американская транснациональная компания, разрабатывающая и продающая сетевое оборудование. Одна из крупнейших в мире, специализирующихся в области высоких технологий, которая стремится представить полный спектр сетевого оборудования, и таким образом предоставить возможность клиенту закупить абсолютно всё необходимое сетевое оборудование исключительно у Cisco Systems.

Проект будет финансироваться из собственных средств компании. Установкой будут заниматься местные специалисты, работающие в данной компании, настройкой и обслуживанием системы – специалист, владеющий знаниями по VPN–технологии.

Для реализации данного проекта потребуется использовать различное оборудование. Перечень и краткое описание применения оборудования с соответствующими стоимостными показателями приведены ниже.

### 3.3.1 Маршрутизатор Cisco ISR серии 1900

Cisco® ISR 1900 – серия маршрутизаторов с интеграцией сервисов, разработанная на основании 25–летнего опыта Cisco в области инноваций и создания передовых решений (Рисунок 3.4). Архитектура новых платформ обеспечивает поддержку следующего этапа развития филиалов организаций, перенося мультимедийные средства совместной работы и средства виртуализации на уровень филиала и позволяя существенно сократить операционные издержки. Платформы маршрутизаторов Cisco ISR второго поколения позволяют решать не только сегодняшние задачи, но и те задачи, которые возникнут в будущем, поскольку в них используются многоядерные процессоры, средства коммутации Gigabit Ethernet с поддержкой расширенной спецификации POE, а также новые возможности управления и мониторинга потребления энергии. При этом производительность платформы существенно повышена. Кроме того, новый универсальный образ операционной системы Cisco IOS® и модуль Services Ready Engine позволяют разделить развертывание оборудования и программного обеспечения, тем самым обеспечивая надежную технологическую основу, способную быстро адаптироваться к постоянно изменяющимся требованиям сети. В целом маршрутизаторы Cisco ISR серии 1900 обеспечивают беспрецедентное снижение совокупной стоимости владения и высочайший уровень гибкости сети, которые поддерживаются интеллектуальными средствами интеграции лучших в отрасли средств

обеспечения безопасности, системы унифицированных коммуникаций, технологий создания беспроводных сетей и прикладных сервисов.

Серия Cisco® 1941 является развитием лучшей в своем классе серии маршрутизаторов Cisco с интеграцией сервисов 1841 и состоит из двух моделей – Cisco 1941 и Cisco 1941W. В дополнение к поддержке широкого спектра беспроводных и проводных соединений, характерной для всей серии Cisco 1941, в конструкции модели Cisco 1941W предусмотрена интегрированная точку доступа стандарта IEEE 802.11n, которая обладает обратной совместимостью с точками доступа стандартов IEEE 802.11a/b/g.

Все маршрутизаторы Cisco ISR серии 1900 поддерживают встроенные средства аппаратного ускорения шифрования, дополнительный межсетевой экран, систему предотвращения вторжений и сервисы приложений. Кроме того, платформы поддерживают широчайший спектр проводных или беспроводных интерфейсов, например, T1/E1, xDSL, 3G и GE.


Рисунок 3.4 – Маршрутизатор Cisco ISR 1941

**Основные бизнес–преимущества**

Маршрутизаторы Cisco с интеграцией сервисов второго поколения (ISR G2) обеспечивают превосходную адаптивность и интеграцию сервисов. Разработанная с учетом требований к масштабируемости, модульная архитектура этих платформ позволяет наращивать и адаптировать их возможности в соответствии с развитием вашей организации. Бизнес–

преимущества маршрутизаторов Cisco ISR серии 1941 перечислены в таблице 3.1.

Т а б л и ц а 3.1 – Основные функциональные возможности и преимущества маршрутизаторов Cisco ISR 1941

| Преимущество | Описание |
|---|---|
| Интеграция сервисов | Маршрутизаторы Cisco ISR 1941 обеспечивают повышенную интеграцию сервисов передачи данных, обеспечения безопасности, организации беспроводных сетей и мобильности, позволяя существенно снизить операционные издержки. |
| Сервисы по запросу | В каждом ISR G2 используется единый универсальный образ операционной системы Cisco IOS®. Единый программный образ содержит все наборы функций Cisco IOS, которые активируются при помощи программной лицензии. Это позволяет вашей организации быстро развертывать расширенные функции, не загружая новый образ IOS. Для поддержки новых функциональных возможностей был увеличен объем памяти в конфигурации по умолчанию.<br>Модуль Cisco Services Ready Engine (SRE) реализует новую эксплуатационную модель, позволяющую снизить капитальные расходы (CapEx) и выполнить развертывание всех необходимых сервисов приложений на одном интегрированном вычислительном модуле. |
| Высокая производительность интегрированных сервисов | Маршрутизаторы Cisco ISR серии 1941 могут развертываться в высокоскоростных средах WAN и обеспечивают совокупную пропускную способность одновременно работающих сервисов до 25 Мбит/с.<br>Мультигигабитная коммутационная структура обеспечивает высокую пропускную способность межмодульных каналов без ущерба для производительности системы маршрутизации. |
| Энергосбережение | В архитектуру маршрутизаторов Cisco ISR 1941 заложены следующие функции энергосбережения:<br>Маршрутизаторы Cisco ISR серии 1941 обеспечивают интеллектуальное управление электропитанием и позволяют заказчику регулировать энергопотребление модулей в зависимости от времени суток. В дальнейшем планируется реализовать поддержку технологии Cisco EnergyWise.<br>Модульность и интеграция сервисов в рамках единой платформы, выполняющей множество функций, оптимизирует расход материалов при изготовлении и потребление энергии в процессе эксплуатации.<br>Гибкость платформы и постоянное развитие как программных, так и аппаратных возможностей удлиняет жизненный цикл продукта и сокращает все аспекты совокупной стоимости владения, включая использование материалов и энергопотребление.<br>Каждая платформа снабжена источниками питания с высоким КПД. |

*Окончание таблицы 3.1*

| Преимущество | Описание |
|---|---|
| | |
| Адаптивность сети | Разработанная для удовлетворения бизнес–потребностей заказчиков, модульная архитектура маршрутизаторов Cisco ISR 1941 поддерживает широкий спектр производительности модульных интерфейсов и сервисов, которые могут устанавливаться по мере изменения потребностей вашей сети.<br>Модульные интерфейсы обладают повышенной пропускной способностью, поддерживают различные варианты подключения и обеспечивают отказоустойчивость сети. |
| Энергосбережение | В архитектуру маршрутизаторов Cisco ISR 1941 заложены следующие функции энергосбережения:<br>Маршрутизаторы Cisco ISR серии 1941 обеспечивают интеллектуальное управление электропитанием и позволяют заказчику регулировать энергопотребление модулей в зависимости от времени суток. В дальнейшем планируется реализовать поддержку технологии Cisco EnergyWise.<br>Модульность и интеграция сервисов в рамках единой платформы, выполняющей множество функций, оптимизирует расход материалов при изготовлении и потребление энергии в процессе эксплуатации.<br>Гибкость платформы и постоянное развитие как программных, так и аппаратных возможностей удлиняет жизненный цикл продукта и сокращает все аспекты совокупной стоимости владения, включая использование материалов и энергопотребление.<br>Каждая платформа снабжена источниками питания с высоким КПД. |
| Защита инвестиций | Маршрутизаторы Cisco ISR 1941 обеспечивают максимальную защиту инвестиций, поддерживая:<br>Возможность повторного использования обширного спектра существующих модулей, поддерживаемых маршрутизаторами Cisco ISR предыдущего поколения, обеспечивает снижение TCO.<br>Широкий набор программных функций Cisco IOS, перенесенных с платформы Cisco ISR предыдущего поколения, и внедренных в единый универсальный программный образ.<br>Гибкость, обеспечивающая развитие возможностей платформы по мере роста потребностей компании. |

**Возможности и преимущества модульности**

Модульная архитектура маршрутизаторов Cisco 1941 (Таблица 3.2) обеспечивает надежную защиту инвестиций заказчиков. Большинство модулей, созданных для маршрутизаторов Cisco предыдущих поколений, таких как Cisco ISR 1841, поддерживаются маршрутизаторами Cisco 1941. Кроме того, модули, используемые в маршрутизаторах Cisco 1941, могут легко устанавливаться в другие маршрутизаторы Cisco, что обеспечивает максимальную защиту инвестиций. К преимуществам типовых интерфейсных карт по всей сети относятся значительное снижение сложности управления ресурсами,

упрощение запуска крупных сетей и унификации конфигураций филиалов разных размеров.

Таблица 3.2 – Модульность – функциональные возможности и преимущества

| Функциональная возможность | Преимущества |
|---|---|
| Расширенная высокоскоростная интерфейсная карта WAN Cisco (EHWIC)<br>  | ● Слот для EHWIC пришел на замену слоту высокоскоростной интерфейсной карты HWIC и может поддерживать исходный режим HWIC, интерфейсные карты WAN (WIC), интерфейсные карты для передачи голоса (VIC) и комбинированные интерфейсные карты (VWIC)<br>● Два встроенных слота для EHWIC в маршрутизаторе Cisco 1941 обеспечивают гибкость формирования конфигурации за счет возможности использования двух модулей. Поддерживаются один сдвоенный модуль HWIC–D или одинарный модуль EHWIC/HWIC в паре со вторым одинарным модулем E–HIC/HWIC.<br>● Каждый слот для HWIC обладает высокой пропускной способностью передачи данных<br>Суммарно до 1,6 Гбит/с в направлении процессора маршрутизатора<br>Суммарно до 2 Гбит/с в направлении других модулей в рамках мультигигабитной коммутационной структуры (MGF) |
| Внутренний сервисный модуль Cisco (ISM)<br>  | ● Один слот для ISM обеспечивает гибкость, которая необходима для интеграции интеллектуальных сервисных модулей, не требующих интерфейсных портов.<br>● Слот для ISM заменяет слот для модулей AIM, существующие AIM слотом ISM не поддерживаются.<br>● Каждый слот ISM обладает высокой пропускной способностью передачи данных<br>Суммарно до 4 Гбит/с в направлении процессора маршрутизатора<br>Суммарно до 2 Гбит/с в направлении других модулей в рамках мультигигабитной коммутационной структуры (MGF)<br>● Питанием слотов ISM можно управлять при помощи расширений, схожих с архитектурой Cisco EnergyWise, что позволяет компаниям сократить энергопотребление сетевой инфраструктуры. Полноценная поддержка EnergyWise будет доступна в будущих обновлениях программного обеспечения.<br>Примечание: Cisco 1941 не может совмещать ISM и WLAN на одном шасси. Обращайтесь к информации по заказу товарных позиций WLAN. |

*Окончание таблицы 3.2*

| Функциональная возможность | Преимущества |
|---|---|
| Слоты Compact Flash | В конструкции маршрутизатора Cisco 1941 предусмотрено два внешних слота Compact Flash. Каждый слот поддерживает высокоскоростные носители емкостью до 4 Гбайт. |
| Порты USB 2.0 | Поддерживается два высокоскоростных порта USB 2.0. Порты USB обеспечивают возможность использования альтернативных токенов безопасности и хранения данных. |

**Инновационные возможности операционной системы Cisco IOS**

Возможности маршрутизаторов Cisco ISR 1941 основаны на лучшей в отрасли специализированной операционной системе Cisco IOS. Разработанная для широкого развертывания в самых ответственных сегментах корпоративных сетей, сетей общего пользования и сетей операторов связи, операционная система Cisco IOS версий 15M и 15T обеспечивает поддержку широкого спектра сетевых технологий Cisco. Сюда входят новые функции и свойства, появившиеся в версиях 12.4 и 12.4T, а также инновации, охватывающие множество технологических областей – таких, как информационная безопасность, голосовая связь, обеспечение высокой доступности, IP–маршрутизация и групповая адресация, обеспечение качества обслуживания (QoS), мобильность IP–адресов, поддержка технологий MPLS, VPN и встроенные средства управления.

Средства безопасности необходимы для защиты интеллектуальной собственности компании и обеспечения непрерывности бизнеса. Они также позволяют расширить рабочее пространство компании и включить в рабочий процесс тех сотрудников, которым требуется доступ к корпоративным ресурсам в любое время и из любой точки мира. Маршрутизаторы с интеграцией сервисов Cisco серии 1900 функционируют в соответствии с концепцией Cisco SAFE, позволяющей организациям своевременно идентифицировать и эффективно предотвращать сетевые угрозы безопасности, а также адаптироваться к ним. Маршрутизаторы Cisco серии 1900 позволяют реализовать защищенное бизнес–взаимодействие и обеспечивают безопасную платформу для совместную работу.

Лицензия на комплект средств обеспечения информационной безопасности Cisco IOS для маршрутизаторов Cisco серии 1900 позволяет использовать широкий спектр базовых функций информационной безопасности, таких как расширенный контроль и управление работой приложений, защита от угроз и архитектуры шифрования, которые позволяют формировать масштабируемые и управляемые сети VPN в рамках одного решения. Маршрутизаторы Cisco 1941 поддерживают встроенные средства аппаратного ускорения шифрования, что позволяет повысить пропускную способность IPSec при одновременном снижении загрузки процессора

маршрутизатора по сравнению с решениями, использующими только программные средства шифрования. Маршрутизаторы Cisco позволяют создать комплексное и гибкое решение для обеспечения безопасности филиалов, включающее следующие функции:

- Защищенные каналы связи. Защищенные средства совместной работы с использованием GETVPN, DMVPN или Enhanced Easy VPN.
- Интегрированные средства управления угрозами. Отражение комплексных сетевых атак и угроз при помощи межсетевого экрана Cisco IOS Firewall, зонированного межсетевого экрана Cisco IOS Zone–Based Firewall, IOS IPS, средств фильтрации содержимого IOS Content Filtering и средств гибкого анализа пакетов (FPM).
- Управление идентификацией. Интеллектуальные механизмы защиты оконечного оборудования с использованием технологий аутентификации, авторизации и учета (AAA), а также инфраструктуры шифрования с открытым ключом (PKI).

Технические характеристики маршрутизатора Cisco 1941 указаны в таблице 3.3.

Т а б л и ц а 3.3 – Технические характеристики с интеграцией сервисов Cisco 1941

| **Сервисы и слоты** | |
|---|---|
| Встроенные средства аппаратного ускорения шифрования (IPSec + SSL) | Да |
| Всего встроенных LAN 10/100/1000 | 2 |
| Порты RJ–45 | 2 |
| Слоты EHWIC | 2 |
| Сдвоенные слоты EHWIC (при использовании сдвоенного слота EHWIC будут заняты два слота EHWIC) | 1 |
| Слоты ISM | 1 |
| Память (DDR2 с коррекцией ошибок [ECC] ECC DRAM) | 512 Мбайт |
| Память (DDR2 ECC DRAM) – максимально | 2 Гбайт |
| Compact Flash (внешн.) – по умолчанию | слот 0: 256 Мбайт<br>слот 1: н/д |
| Compact Flash (внешн.) – максимально | слот 0: 4 Гбайт<br>слот 1: 4 Гбайт |
| Внешний USB слот для Flash–памяти (тип A) | 2 |
| Консольный порт USB (тип B) (до 115,2 кбит/с) | 1 |
| Консольный последовательный порт (до 115,2 кбит/с) | 1 |
| Внешний последовательный порт (до 115,2 кбит/с) | 1 |
| Поддержка резервирования блока питания | Нет |
| **Технические характеристики системы питания** | |
| Входное напряжение переменного тока | 100–240 В ~ |
| Частота входного переменного тока | 47–63 Гц |
| Диапазон рабочих токов для БП пер–го тока (макс.) (A) | 1,5–0,6 |
| Входной переменный ток перегрузки | <50 A |
| Номинальная потребляемая мощность (без модулей) | 35 Вт |

*Окончание таблицы 3.3*

| **Сервисы и слоты** | |
|---|---|
| Предельная мощность БП переменного тока | 110 Вт |
| Предельная мощность питания через PoE (только платформа) | 110 Вт |
| Предельная мощность устройства PoE с питанием через PoE | 80 Вт |
| **Физические характеристики** | |
| Габариты, В x Ш x Г (дюймы) | 3,5 x 13,5 x 11,5 |
| Высота в стойке | 2 RU |
| 19–дюймовая стойка (48,3 см) EIA | В комплекте |
| Крепление на стену (см. инструкцию по монтажу для правильной установки) | Да |
| Масса с БП переменного тока (без модулей) | 5,44 кг |
| Масса с питанием от POE (без модулей) | 5,8 кг |
| Максимальная масса в полной конфигурации | 6,35 кг |
| Поток воздуха | От перед. панели к боковым |
| **Характеристики окружающей среды** | |
| **Условия эксплуатации** | |
| Температура – на высотах до 1800 м | 0–40 °C |
| Температура – на высотах до 3000 м | 0–25 °C |
| Высота | 3000 м |
| Влажность | от 10% до 85% отн. |
| Акустика: звуковое давление (ном./макс.) | 26/46 дБА |
| Акустика: звуковая мощность (ном./макс.) | 36/55 дБА |
| **Условия хранения и транспортировки** | |
| Температурный диапазон | от –40 до + 70 °C |
| Влажность | от 5% до 95% отн. |
| Высота | 4570 м |
| **Соответствие нормативным требованиям** | |
| Безопасность | UL 60950–1<br>CAN/CSA C22.2 No. 60950–1<br>EN 60950–1<br>AS/NZS 60950–1<br>IEC 60950–1 |
| Электромагнитная совместимость | 47 CFR, часть 15<br>ICES–003 Класс A<br>EN55022 Класс A<br>CISPR22 Класс A<br>AS/NZS 3548 Класс A<br>VCCI V–3<br>CNS 13438<br>EN 300–386<br>EN 55024, CISPR 24<br>EN50082–1 |
| Телекоммуникационные характеристики | TIA/EIA/IS–968<br>CS–03<br>ANSI T1.101<br>ITU–T G.823, G.824<br>IEEE 802.3<br>Директива RTTE |

### 3.3.2 Коммутатор Cisco Catalyst серии 2960–S с ПО LAN Base

Коммутаторы Cisco® Catalyst® серии 2960–S являются ведущими продуктами среди коммутаторов второго уровня. Их использование позволяет упростить эксплуатацию ИТ–инфраструктуры, повысить уровень безопасности бизнес–процессов, обеспечить устойчивую работу сети, а также предоставить пользователям возможность работы в "сетях без границ". Коммутаторы Cisco Catalyst серии 2960–S поддерживают новую технологию стекирования коммутаторов Cisco FlexStack с использование сетевых подключений 1 и 10 Гбит/с, а также технологию Power over Ethernet Plus (PoE+) с коммутаторами Cisco Catalyst серии 2960, обеспечивающими поддержку сетевых подключений Fast Ethernet и поддержку PoE. Коммутаторы Cisco Catalyst серии 2960–S – это коммутаторы доступа с фиксированной конфигурацией, предназначенные для сетей крупных и средних предприятий, а также их филиалов, позволяющие снизить совокупную стоимость владения. Коммутатор Cisco Catalyst 2960–S показан на рисунке 3.5.

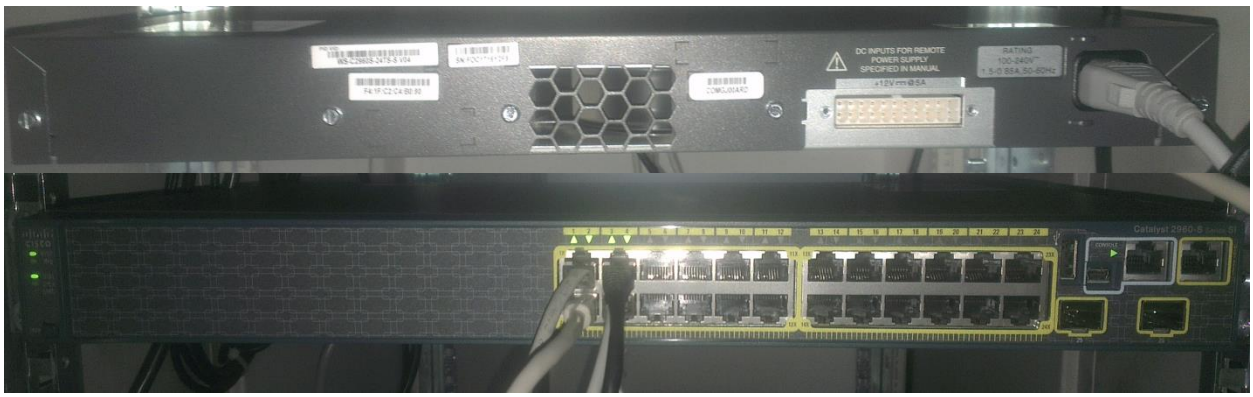

Рисунок 3.5 – Коммутаторы Cisco Catalyst серии 2960–S

Новые функции коммутаторов Cisco Catalyst серии 2960–S с ПО LAN Base:

– порт каскадирования, поддерживающий технологии Ethernet 10 и 1 Гбит/с с помощью адаптера SFP+, для обеспечения непрерывности ведения бизнеса и быстрого перехода на технологию 10 GbE;

– возможность подключения настольных компьютеров к 24 или 48 портам Gigabit Ethernet;

– модуль стекирования Cisco FlexStack с пропускной способностью 40 Гбит/с, облегчающий работу за счет использования единой конфигурации и упрощенного обновления коммутаторов;

– технология PoE+ с мощностью до 30 Вт для одного порта обеспечивает поддержку новейших устройств PoE+;

– дополнительные источники питания с фиксированной мощностью 740 Вт и 370 Вт для коммутаторов PoE+;

– поддержка USB–накопителей для резервного копирования и распространения файлов, а также для упрощения эксплуатации;

– широкий набор программных средств, обеспечивающих простоту эксплуатации, защиту бизнес–процессов, устойчивость и работу в "сетях без границ";

– ограниченная гарантия на оборудование в течение его жизненного цикла, включая замену в течение следующего рабочего дня, а также обслуживание и поддержку в течение 90 дней.

В таблице 3.4 показана конфигурация коммутаторов Cisco Catalyst серии 2960–S.

Таблица 3.4 – Конфигурация коммутаторов Cisco Catalyst серии 2960–S с ПО LAN Base

| Модель коммутатора Cisco Catalyst серии 2960–S | Описание | Порты каскадирования | Доступное питание PoE |
|---|---|---|---|
| Порты каскадирования 10 Gigabit Ethernet с возможностью подключения к каналам Ethernet 10/100/1000 Мбит/с | | | |
| Cisco Catalyst 2960S–48FPD–L | 48 портов Ethernet 10/100/1000 Мбит/с PoE+ | 2 порта 10 Gigabit Ethernet SFP+ или два порта 1 Gigabit Ethernet SFP | 740 Вт |
| Cisco Catalyst 2960S–48LPD–L | 48 портов Ethernet 10/100/1000 Мбит/с PoE+ | 2 порта 10 Gigabit Ethernet SFP+ или два порта 1 Gigabit Ethernet SFP | 370 Вт |
| Cisco Catalyst 2960S–24PD–L | 24 порта Ethernet 10/100/1000 Мбит/с PoE+ | 2 порта 10 Gigabit Ethernet SFP+ или два порта 1 Gigabit Ethernet SFP | 370 Вт |
| Cisco Catalyst 2960S–48TD–L | 48 портов Ethernet 10/100/1000 Мбит/с | 2 порта 10 Gigabit Ethernet SFP+ или два порта 1 Gigabit Ethernet SFP | – |
| Cisco Catalyst 2960S–24TD–L | 24 порта Ethernet 10/100/1000 Мбит/с | 2 порта 10 Gigabit Ethernet SFP+ или два порта 1 Gigabit Ethernet SFP | – |
| Порты каскадирования Gigabit Ethernet с возможностью подключения к каналам Ethernet 10/100/100 Мбит/с | | | |
| Cisco Catalyst 2960S–48FPS–L | 48 портов Ethernet 10/100/1000 Мбит/с PoE+ | 4 порта Gigabit Ethernet (SFP) | 740 Вт |
| Cisco Catalyst 2960S–48LPS–L | 48 портов Ethernet 10/100/1000 Мбит/с PoE+ | 4 порта Gigabit Ethernet (SFP) | 370 Вт |
| Cisco Catalyst 2960S–24PS–L | 24 порта Ethernet 10/100/1000 Мбит/с PoE+ | 4 порта Gigabit Ethernet (SFP) | 370 Вт |
| Cisco Catalyst 2960S–48TS–L | 48 портов Ethernet 10/100/1000 Мбит/с | 4 порта Gigabit Ethernet (SFP) | – |
| Cisco Catalyst 2960S–24TS–L | 24 порта Ethernet 10/100/1000 Мбит/с | 4 порта Gigabit Ethernet (SFP) | – |

**Технология стекирования Cisco FlexStack**

Технология стекирования Cisco FlexStack, которая основана на использовании модуля, поддерживающего горячую замену, и ПО Cisco IOS® обеспечивает подлинное стекирование, при котором все коммутаторы, объединенные в стек, работают как один коммутатор. Технология Cisco FlexStack обеспечивает формирование единого уровня данных, использование единой конфигурации и возможность управления всей группой коммутаторов с использованием одного IP–адреса. Преимущество подлинного стекирования состоит в снижении совокупной стоимости владения за счет упрощения управления и повышения доступности. Технология Cisco FlexStack поддерживает взаимодействие коммутаторов, входящих в стек, включая каналы EtherChannel, технологию SPAN и технологию FlexLink. Модуль стекирования может быть добавлен в любой коммутатор Cisco Catalyst серии 2960–S с ПО LAN Base для быстрой модернизации коммутатора с целью обеспечения его работы в стеке. Добавленный к стеку коммутатор будет обновлен до необходимой версии ОС Cisco IOS® и сразу же станет членом стека. На рисунке 3.6 показан модуль стекирования FlexStack для коммутаторов Cisco Catalyst серии 2960–S.

Рисунок 3.6 – Коммутаторы Cisco Catalyst 2960–S с модулями Cisco FlexStack и кабелями стекирования

**Технология Power over Ethernet Plus**

Помимо технологии PoE 802.3af коммутаторы Cisco Catalyst серии 2960–S поддерживают технологию Power over Ethernet Plus (PoE+) (стандарт IEEE 802.3at), обеспечивающую мощность до 30 Вт на один порт. Коммутаторы Cisco Catalyst серии 2960–S позволяют снизить совокупную стоимость владения при развертываниях с использованием IP–телефонов Cisco, точек доступа к беспроводной сети (WLAN) Cisco Aironet® или любых оконечных устройств, совместимых с IEEE 802.3af. Технология PoE позволяет устранить потребность в обеспечении питания устройств с поддержкой PoE от сети электропитания и исключить затраты на дополнительные электрические кабели и цепи, которые в противном случае необходимы при развертываниях IP–

телефонов и сетей WLAN. В таблице 3.5 показаны сочетания источников питания, необходимые для различных потребностей PoE.

Таблица 3.5 – Возможности коммутаторов по обеспечению электропитания с использованием технологий PoE и PoE+

| Модель коммутатора | Максимальное число портов PoE+ (IEEE 802.3at)* | Максимальное число портов PoE (IEEE 802.3af )* | Доступное питание PoE |
|---|---|---|---|
| Порты каскадирования 10 Gigabit Ethernet с возможностью подключения к каналам Ethernet 10/100/1000 Мбит/с | | | |
| Cisco Catalyst 2960S–48FPD–L | 24 порта с мощностью до 30 Вт | 48 портов с мощностью до 15,4 Вт | 740 Вт |
| Cisco Catalyst 2960S–48LPD–L | 12 портов с мощностью до 30 Вт | 24 порта с мощностью до 15,4 Вт<br>48 портов с мощностью до 7,7 Вт | 370 Вт |
| Cisco Catalyst 2960S–24PD–L | 12 портов с мощностью до 30 Вт | 24 порта с мощностью до 15,4 Вт | 370 Вт |
| Порты каскадирования Gigabit Ethernet с возможность подключения к каналам Ethernet 10/100/1000 Мбит/с | | | |
| Cisco Catalyst 2960S–48FPS–L | 24 порта с мощностью до 30 Вт | 48 портов с мощностью до 15,4 Вт | 740 Вт |
| Cisco Catalyst 2960S–48LPS–L | 12 портов с мощностью до 30 Вт | 24 порта с мощностью до 15,4 Вт<br>48 портов с мощностью до 7,7 Вт | 370 Вт |
| Cisco Catalyst 2960S–24PS–L | 12 портов с мощностью до 30 Вт | 24 порта с мощностью до 15,4 Вт | 370 Вт |

**Коммутаторы Cisco Catalyst серии 2960–S обеспечивают работу "сетей без границ" Cisco.**

Архитектура "Сети без границ" Cisco создает новое рабочее пространство, обеспечивая безопасное, надежное и прозрачное подключение любых пользователей, независимо от их местоположения, с помощью любых устройств и к любым ресурсам. Архитектура "Сети без границ" Cisco решает основные задачи отрасли ИТ и бизнеса, обеспечивая работу без границ за счет более тесного взаимодействия с сотрудниками и заказчиками.

Работа без границ возможна только при использовании интеллектуальных сетевых элементов, созданных и спроектированных в соответствии с потребностями глобального рабочего пространства. Основным компонентом данной архитектуры является уровень доступа Cisco, который предоставляет такие сервисы "сетей без границ" как мобильность, безопасность и устойчивость работы, а также упрощает эксплуатацию, увеличивая

производительность и эффективность работы. Если система организации доступа к сети является интеллектуальной, ей известен идентификатор пользователя, а также местонахождение пользователя в сети. Ей известен тип устройства, подключающегося к сети, что позволяет выполнить автоматическую настройку сети для обеспечения требуемого уровня QoS надежной доставки данных. Она учитывает особенности сетевых сервисов для оптимизации работы пользователей. Только интеллектуальная система организации доступа к сети позволяет предприятию безопасно и незаметно устранить границы.

На уровне доступа в модели "сетей без границ" Cisco особое внимание уделяется предоставлению решений по четырем основным направлениям:

- устойчивость;
- простота эксплуатации;
- безопасность без границ;
- работа без границ.

**Устойчивость**

Коммутаторы Cisco Catalyst позволяют увеличить экологичность работы благодаря значительной экономии электроэнергии, интеграции сервисов и непрерывному процессу внедрения инноваций, таких как технология Cisco EnergyWise. Эта технология является решением для всего предприятия, позволяющим контролировать энергозатраты и снижать уровень потребления энергии с помощью настраиваемых политик. Технология Cisco EnergyWise и коммутаторы Cisco Catalyst позволяют сократить объем выбросов парниковых газов и снизить уровень энергозатрат, обеспечивая эффективную работу предприятия. Возможности коммутаторов Cisco Catalyst серии 2960–S по обеспечению устойчивости реализованы в форме следующих наборов функций.

- технология Cisco EnergyWise;
- эффективная работа коммутатора;
- интеллектуальное управление энергопотреблением.

**Эффективная работа коммутатора**

Коммутаторы Cisco Catalyst серии 2960–S, спроектированные и разработанные компанией Cisco, обеспечивают оптимальный уровень потребления электроэнергии, возможности контроля над потреблением энергии и низкие энергозатраты для ведущей в отрасли системы управления энергопотреблением. Порты коммутатора Cisco Catalyst серии 2960–S могут использовать режимы пониженного энергопотребления, чтобы неиспользуемые порты могли переходить в состояние низкого потребления энергии.

**Интеллектуальное управление Power over Ethernet**

Модели Cisco Catalyst серии 2960–S PoE поддерживают новейшие устройства PoE+, включая IP–телефоны Cisco и точки доступа к беспроводной

сети Cisco Aironet также любые конечные устройства, совместимые с IEEE 802.3af, за счет обеспечения выходной мощности до 30 Вт на один порт.

– Управление энергопотреблением на уровне порта позволяет определить значение предельной мощности на уровне порта.

– Датчики мощности PoE измеряют фактический уровень потребленной портом энергии, что обеспечивает более продуманное управление подключенными к сети устройствами.

– Протокол CDP версии 2 позволяет коммутаторам согласовывать более точные настройки энергопотребления при подключении к устройствам Cisco, питание которых необходимо обеспечить, таким как IP–телефоны или точки доступа к беспроводной сети, в соответствии со стандартом IEEE.

– Структура PoE MIB обеспечивает упреждающий контроль над энергопотреблением и позволяет заказчикам устанавливать различные пороговые значения для уровней мощности.

**Безопасность без границ**

Коммутаторы Cisco Catalyst серии 2960–S обеспечивают надежную защиту от угроз на втором уровне сетевой модели для предотвращения атак типа "посредник" (таких как подмена MAC– или IP–адреса, а также отправка ложных ARP–ответов). TrustSec, основной элемент архитектуры безопасности без границ, помогает предприятиям защитить свои сети, данные и ресурсы с помощью контроля доступа на основе политик, работы в сети с поддержкой идентификации и учета ролей, интегрированной и повсеместной защиты, а также обеспечения конфиденциальности. Безопасность без границ обеспечивается следующими наборами функций коммутаторов Cisco Catalyst серии 2960–S:

- защита от угроз;
- Cisco TrustSec;
- другие усовершенствованные функции безопасности.

**Защита от угроз**

Встроенные средства обеспечения безопасности Cisco – это ведущее в отрасли решение, реализованное в коммутаторах Cisco Catalyst и обеспечивающее упреждающую защиту критически важной сетевой инфраструктуры. Предоставляя мощные и простые в использовании инструменты для эффективного предотвращения большинства распространенных и потенциально вредоносных угроз безопасности второго уровня, встроенные средства обеспечения безопасности Cisco обеспечивают надежную защиту сети. Встроенные средства обеспечения безопасности Cisco включают функции защиты на уровне порта, контроль DHCP–трафика, динамический анализ ARP–трафика и IP Source guard.

– Механизм защиты на уровне порта защищает доступ к порту доступа или транковому порту на основании MAC–адреса. Он ограничивает количество

известных MAC–адресов для предотвращения переполнения таблицы MAC–адресов.

– Функции контроля DHCP–трафика предотвращают подделку сервера DHCP злоумышленниками и отправку фиктивных адресов. Эта функция используется другими основными функциями обеспечения безопасности для предотвращения ряда других атак, например, отправки ложных ARP–ответов.

– Динамический анализ ARP–трафика (DAI) помогает гарантировать целостность пользовательской среды, препятствуя нарушению безопасности по сути незащищенного протокола ARP.

– Функция IP Source Guard предотвращает имитацию или использование злоумышленником IP–адреса другого пользователя за счет создания таблицы соответствия между IP–адресом и MAC–адресом клиента, портом и VLAN.

**Cisco TrustSec**

Решение TrustSec защищает доступ к сети, усиливает политики безопасности и предоставляет решения безопасности на основе стандартов, например, 802.1X, обеспечивая безопасную совместную работу и соблюдение политик. Возможности TrustSec вобрали в себя такие присущие компании Cisco черты, как лидерское мышление, инновации и стремление к успеху клиентов. Новыми возможностями TrueSec являются:

– гибкая аутентификация, поддерживающая несколько механизмов аутентификации, включая 802.1X, резервный метод аутентификации по MAC–адресу и веб–аутентификацию, с помощью единой последовательной конфигурации;

– открытый режим, создающий удобную для пользователей среду для функционирования средств 802.1X;

– интеграция технологии профилирования устройств и гостевого доступа, реализованных на коммутаторах Cisco, для значительного усиления системы безопасности с одновременным уменьшением трудозатрат при развертывании и эксплуатации;

– изменение авторизации и вызовы с возможностью загрузки RADIUS для функций комплексного управления политиками;

– модули 802.1X с поддержкой NEAT обеспечивают расширенный защищенный доступ, при котором компактные коммутаторы в комнатах для проведения переговоров характеризуются таким же уровнем безопасности, как и коммутаторы в закрытом коммутационном шкафу.

## 3.4 Настройка протокола безопасности IPSec на роутерах в головном офисе Астаны и филиале – Алматы

IP Security – это комплект протоколов, касающихся вопросов шифрования, аутентификации и обеспечения защиты при транспортировке IP–пакетов; в его состав сейчас входят почти 20 предложений по стандартам и 18 RFC. Продукты Cisco для поддержки VPN используют набор протоколов IPSec,

являющийся на сегодня промышленным стандартом обеспечения широких возможностей VPN. IPSec предлагает механизм защищенной передачи данных в IP–сетях, обеспечивая конфиденциальность, целостность и достоверность данных, передаваемых через незащищенные сети типа Internet.

**Как работает IPSec**

IPSec опирается на ряд технологических решений и методов шифрования, но действие IPSec в общем можно представить в виде следующих шагов (Рисунок 3.7).

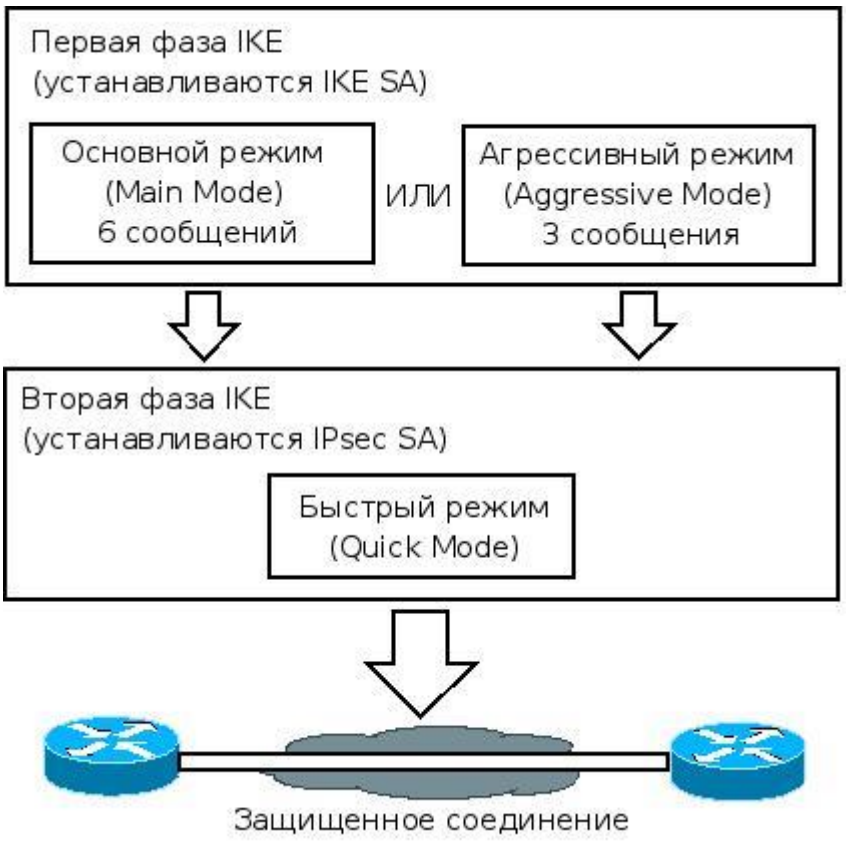


Рисунок 3.7 – Шаги действия IPSec (фазы IKE)

- Шаг 1. *Начало процесса IPSec.* Трафик, которому требуется шифрование в соответствии с политикой защиты IPSec, согласованной сторонами IPSec, начинает IKE–процесс.
- Шаг 2. *Первая фаза IKE.* IKE–процесс выполняет аутентификацию сторон IPSec и ведет переговоры о параметрах ассоциаций защиты IKE, в результате чего создается защищенный канал для ведения переговоров о параметрах ассоциаций защиты IPSec в ходе второй фазы IKE.
- Шаг 3. *Вторая фаза IKE.* IKE–процесс ведет переговоры о параметрах ассоциации защиты IPSec и устанавливает соответствующие ассоциации защиты IPSec для устройств сообщающихся сторон.

• Шаг 4. *Передача данных.* Происходит обмен данными между сообщающимися сторонами IPSec, который основывается на параметрах IPSec и ключах, хранимых в базе данных ассоциаций защиты.

• Шаг 5. *Завершение работы туннеля IPSec.* Ассоциации защиты IPSec завершают свою работу либо в результате их удаления, либо по причине превышения предельного времени их существования.

**Шаг 1. Начало процесса IPSec**

Тип трафика, который должен защищаться средствами IPSec, определяется в рамках политики защиты для VPN. Затем эта политика реализуется в виде команд конфигурации интерфейсов устройств каждой стороны IPSec. Например, в маршрутизаторах Cisco и брандмауэрах PIX Firewall для определения трафика, подлежащего шифрованию, используют списки доступа. Списки доступа реализуют политику шифрования, например, с помощью операторов permit, указывающих, что соответствующий трафик должен шифроваться, и операторов deny, запрещающих шифрование соответствующего трафика. В случае клиента Cisco VPN используются окна меню, где указываются соединения, которым должна обеспечиваться защита IPSec. Когда подлежащий шифрованию трафик генерируется клиентом IPSec или проходит через него, клиент инициирует следующий шаг процесса, начиная первую фазу IKE.

**Шаг 2. Первая фаза IKE**

Главной целью обмена данными, происходящего в первой фазе IKE, является аутентификация сторон IPSec и создание защищенного канала между сторонами, позволяющего начать обмен IKE. В ходе первой фазы IKE выполняются следующие действия.

• Ведутся переговоры о согласовании политики ассоциаций защиты IKE между сторонами, чтобы обеспечить защиту обмена IKE. Ассоциация защиты IKE получает согласованные параметры IKE и является двусторонней.

• Выполняется аутентифицированный обмен Диффи–Хеллмана, в результате которого выбирается общий секретный ключ для использования в алгоритмах шифрования IPSec.

• Выполняется аутентификация и обеспечивается защита сторон IPSec.

• Устанавливается защищенный туннель для ведения переговоров о параметрах второй фазы IKE.

**Шаг 3. Вторая фаза IKE (QuickMode)**

Задачей второй фазы IKE является согласование параметров ассоциации защиты IPSec с целью создания туннеля IPSec. В этой фазе выполняются следующие действия.

– Ведутся переговоры о параметрах ассоциации защиты IPSec, защищаемые существующей ассоциацией защиты IKE.

– Устанавливаются ассоциации защиты IPSec.

– Периодически возобновляются переговоры об ассоциациях защиты IPSec, чтобы гарантировать защиту.

– В необязательном порядке может выполняться дополнительный обмен Диффи–Хеллмана.

Вторая фаза IKE выполняется только в быстром режиме, после того как в результате первой фазы IKE создается защищенный туннель. Затем ведутся переговоры о согласованной политике IPSec, извлекается общий секретный материал для работы алгоритмами защиты IPSec и создаются ассоциации защиты IPSec. В быстром режиме выполняется обмен оказиями, которые обеспечивают защиту от воспроизведения сообщений. Оказии используются для того, чтобы гарантировать создание новых секретных ключей и не допустить проведения атак воспроизведения, в результате которых противник мог бы создать "фальшивые" ассоциации защиты.

**Шаг 4. Передача данных**

После завершения второй фазы IKE и создания ассоциаций защиты IPSec в быстром режиме, начинается обмен информацией через туннель IPSec, связывающий стороны IPSec. Пакеты шифруются и дешифруются с помощью алгоритмов шифрования и ключей, указанных ассоциацией защиты IPSec. Ассоциация защиты IPSec задает также предел времени своего существования в килобайтах передаваемых данных или в секундах. Ассоциация защиты имеет специальный счетчик, значение которого уменьшается на единицу за каждую секунду или после передачи каждого килобайта данных.

**Шаг 5. Завершение работы туннеля IPSec**

Ассоциации защиты IPSec завершают свою работу либо по причине их удаления, либо потому, что оказывается превышен предел времени их существования. Когда ассоциации защиты завершают работу, соответствующие им ключи тоже становятся недействительными. Если для потока данных требуются новые ассоциации защиты IPSec, в рамках протокола IKE снова выполняется обмен второй фазы, а если необходимо, то и первой. В результате успешного их завершения создаются новые ассоциации защиты и новые ключи. Новые ассоциации защиты могут создаваться и до истечения времени существования предыдущих, чтобы поток данных мог двигаться непрерывно. Обычно переговоры второй фазы выполняются чаще, чем переговоры первой фазы.

**Настройка IPSec для работы с общими ключами**

На рисунке 3.8 показана структурная схема сети ТОО “TNS–INTEC” с технологией IPSec VPN.

Процесс настройки средств Cisco IOS для использования заранее согласованных ключей IKE в маршрутизаторах Cisco предполагает решение следующих основных задач.

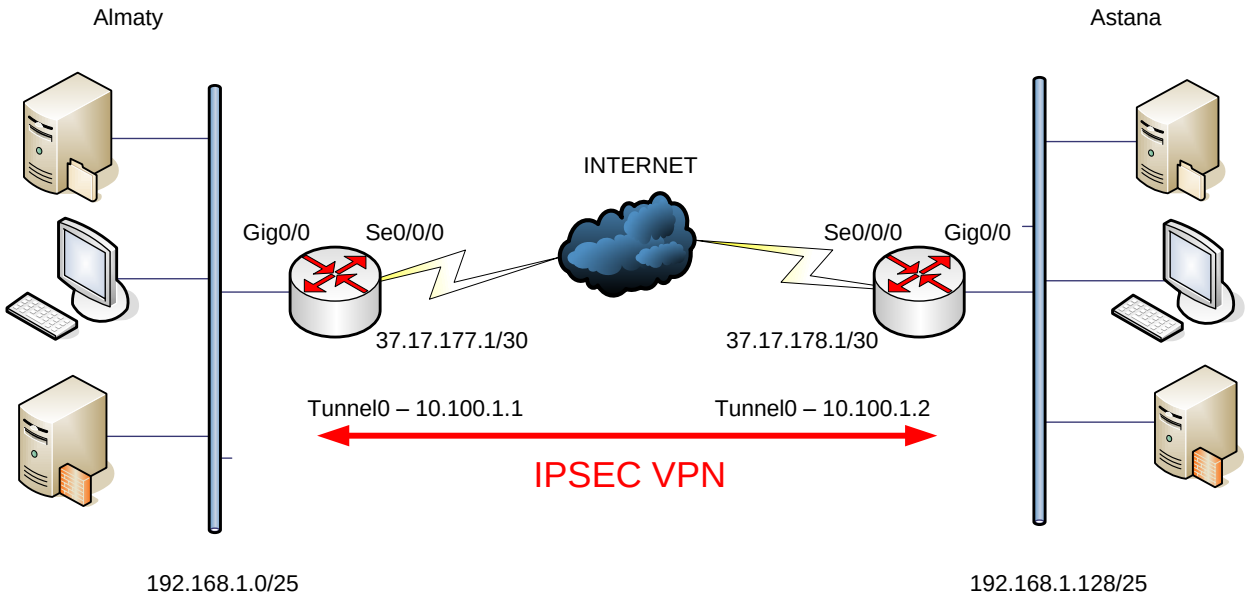


Рисунок 3.8 – Структурная схема сети компании с технологией IPSec VPN

•Задача 1. Подготовка к использованию IPSec. Определение деталей политики шифрования, идентификация хостов и сетей, которые необходимо защитить, выяснение характеристик сторон IPSec, возможностей IPSec, которые будут необходимы, а также проверка того, что существующие списки доступа, применяемые для фильтрования пакетов, позволяют использовать IPSec.

•Задача 2. Настройка IKE. Активизация средств IKE, создание политики IKE и проверка правильности выбранной конфигурации.

•Задача 3. Настройка IPSec. Определение множеств преобразований, создание списков шифрованного доступа и криптографических карт, а также применение криптографических карт к соответствующим интерфейсам.

•Задача 4. Тестирование и контроль IPSec. Проверка правильности функционирования IPSec с помощью show, debug и других аналогичных команд и решение возможных проблем.

**Задача 1. Подготовка к использованию IPSec**

Перед тем как приступить непосредственно к настройке маршрутизаторов, для успешного построения сети IPSec требуется предварительное планирование. Планирование должно начинаться с определения политики защиты IPSec на основе требований общей политики защиты компании. В процессе планирования выполняются следующие основные шаги.

*Шаг 1.* Определение политики IKE взаимодействия сторон IPSec (первая фаза IKE), в зависимости от числа сторон и их размещения.

*Шаг 2.* Определение политики IPSec для учета параметров сторон IPSec (вторая фаза IKE), в частности IP–адресов и режимов IPSec.

*Шаг 3.* Проверка текущей конфигурации с помощью команд write terminal, show isakmp, show crypto map и других команд show.

*Шаг 4.* Проверка работоспособности сети при отключенных средствах шифрования (с помощью команд ping и направления нешифрованного трафика к месту назначения).

*Шаг 5.* Проверка того, что списки доступа, определяющие фильтрацию пакетов, разрешают движение трафика IPSec.

**Задача 2. Настройка IKE для работы с общими ключами**

Следующей задачей настройки IPSec является выбор параметров IKE в соответствии с той информацией о сети, которая была выяснена ранее. Процесс настройки IKE состоит из следующих шагов.

*Шаг 1.* Активизация или отключение IKE с помощью команды crypto isakmp enable.

*Шаг 2.* Создание политик IKE с помощью команд crypto isakmp policy.

*Шаг 3.* Выбор общих ключей с помощью команды crypto isakmp key и связанных с ней команд.

*Шаг 4.* Проверка конфигурации IKE с помощью команды show crypto isakmp policy.

**Шаг 1. Активизация или отключение IKE**

Первым шагом настройки IKE является активизация или отключение IKE. Активизировать IKE глобально можно с помощью команды crypto isakmp enable, а отменить использование IKE – с помощью той же команды с префиксом no. По умолчанию протокол IKE активизирован. Этот протокол активизируется глобально для всех интерфейсов в маршрутизаторе, поэтому нет необходимости активизировать IKE для каждого интерфейса в отдельности. На интерфейсах, не используемых для IPSec, IKE можно отключить с помощью операторов списка доступа, запрещающих использование UDP– порта 500 (тем самым обеспечивается защита от атак блокирования сервиса).

**Шаг 2. Создание политик IKE**

Следующим шагом настройки IKE является определение набора политик IKE, используемых при создании связей IKE между сторонами IPSec. Политика IKE определяет набор параметров, которые могут использоваться в процессе переговоров согласования IKE. В таблице 3.6 представлены элементы политики IKE.

Определив параметры политики IKE, используйте команду crypto isakmp policy, чтобы задать политику IKE, или команду no crypto isakmp policy, чтобы удалить соответствующую политику. Указанная команда имеет следующий синтаксис:

Crypto isakmp policy *приоритет*

Т а б л и ц а 3.6 – Политика IKE для двух маршрутизаторов

| Параметр | Значение для маршрутизатора ast–route | Значение для маршрутизатора ala–route |
|---|---|---|
| Алгоритм шифрования сообщений | DES | DES |
| Алгоритм гарантии целостности (алгоритм хэширования) сообщений | SHA | SHA |
| Метод аутентификации сторон | Согласованный ключ | Согласованный ключ |
| Параметры обмена ключами (идентификатор группы Диффи–Хеллмана) | Группа 1 (768–битовый вариант алгоритма Диффи– Хеллмана) | Группа 1 (768–битовый вариант алгоритма Диффи–Хеллмана) |
| Предел времени существования ассоциаций защиты, установленных с помощью ISAKMP | 86400 (по умолчанию) | 86400 (по умолчанию) |
| IP–адрес стороны IPSec | 37.17.178.1 | 37.17.177.1 |

*Приоритет* – Однозначно идентифицирует политику IKE, присваивая ей приоритет. Используйте целое число от 1 до 10000, где 1 – наивысший приоритет, а 10000 – наименьший.

**Шаг 3. Согласование общих ключей**

Важным шагом процесса настройки средств поддержки IKE является установка режима идентификации IKE и согласование ключей.

*Установка режима идентификации*

Стороны IPSec выполняют взаимную аутентификацию в ходе переговоров IKE с помощью заранее согласованных общих ключей и идентификации объекта IKE. Идентификатором объекта может быть IP–адрес маршрутизатора или имя хоста. Программное обеспечение Cisco IOS по умолчанию использует метод идентификации по IP–адресу.

**Задача 3. Настройка IPSec**

Следующей задачей настройки IPSec в Cisco IOS является установка ранее определенных параметров шифрования IPSec. Действия, которые необходимо выполнить для этого в маршрутизаторах Cisco, являются следующими.

*Шаг 1.* Определение наборов преобразований с помощью команды crypto ipsec transform–set.

*Шаг 2.* Настройка списков доступа посредством команды access–list.

*Шаг 3.* Настройка криптографических карт с помощью команды crypto map.

*Шаг 4.* Применение криптографических карт к интерфейсам с помощью команд interface и crypto map.

В таблице 3.7 представлены элементы политики IPSec поддерживаемые программным обеспечением Cisco IOS.

Т а б л и ц а 3.7 – Элементы политики IPSec

| Параметр | Значение для стороны A | Значение для стороны B |
|---|---|---|
| *Набор преобразований* | esp–des, esp–sha–hmac | esp–des, esp–sha–hmac |
| *Режим IPSec* | Туннельный | Туннельный |
| *Алгоритм хэширования* | SHA | SHA |
| *Имя удаленного хоста* | ast–route | ala–route |
| *Интерфейс* | Serial 0 | Serial 0 |
| *IP–адрес удаленной стороны* | 37.17.178.1 | 37.17.177.1 |
| *IP–адрес хостов, которые должны быть защищены* | 192.168.1.0 | 192.168.1.129 |
| *Тип трафика для шифрования* | TCP | TCP |
| *Установка ассоциаций защиты* | ipsec–isakmp | ipsec–isakmp |

**Шаг 1. Определение набора преобразований**

Первым шагом настройки IPSec в Cisco IOS является использование политики защиты IPSec для определения набора преобразований, представляющего собой совокупность конкретных алгоритмов IPSec, с помощью которых реализуется политика защиты для выбранного трафика. В рамках ассоциации защиты IKE выполняются операции согласования (в ходе второй фазы IKE, быстрый режим), в результате которых стороны соглашаются использовать конкретный набор преобразований для защиты потока данных.

Набор преобразований объединяет следующие элементы IPSec:

- механизм шифрования данных: преобразование ESP (Encapsulating Security Payload);
- режим IPSec (транспортный или туннельный).

Набор преобразований определяется с помощью команды глобальной конфигурации crypto ipsec transform–set, активизирующей конфигурационный режим crypto–transform. Чтобы удалить набор преобразований, используйте указанную команду с префиксом no.

Команда имеет следующий синтаксис:

Crypto ipsec transform–set имя–набора преобразование1 [преобразование2 [преобразование3]]

**Шаг 2. Установка глобальных пределов существования для ассоциаций защиты IPSec**

Пределы существования ассоциаций защиты IPSec указывают, как долго ассоциации защиты IPSec остаются действительными, т.е. когда потребуется их переустановка. Программное обеспечение Cisco IOS поддерживает глобальное значение предела существования, применимого сразу ко всем криптографическим картам. Глобальное значение может быть изменено соответствующей записью криптографической карты. Пределы существования применимы только к ассоциациям защиты, создаваемым посредством IKE.

Созданные вручную ассоциации защиты не прекращают своего существования автоматически. Перед тем как ассоциация защиты прекратит свое существование, проводятся переговоры о создании новой, чтобы обеспечить непрерывность потока данных. Изменить глобальные значения пределов существования для ассоциаций защиты IPSec можно с помощью команды глобальной конфигурации crypto ipsec security–association lifetime. Чтобы восстановить значение предела существования, заданное по умолчанию, используется команда с префиксом no. Указанная команда имеет следующий синтаксис: cryptoipsec security–association lifetime {seconds секунды| kilobytes килобайты)

**Шаг 3. Создание списков шифрованного доступа**

Еще одним шагом настройки IPSec является настройка списков шифрованного доступа, которые используются для определения трафика IP, защищаемого (или не защищаемого) средствами IPSec. Списки шифрованного доступа в рамках IPSec выполняют следующие функции.

- Выбор исходящего трафика, подлежащего защите средствами IPSec.
- Обработка входящего трафика на предмет выявления трафика IPSec.
- Выявление и фильтрация входящего трафика, подлежащего защите средствами IPSec.
- Удовлетворение запросов создания ассоциаций защиты IPSec в процессе согласования IKE.

При создании списков шифрованного доступа используются расширенные списки доступа IP. Списки шифрованного доступа выявляют данные, которым требуется защита. Синтаксис списков шифрованного доступа ничем не отличается от синтаксиса расширенных списков доступа IP, но в списках шифрованного доступа ключевые слова интерпретируются иначе. Ключевое слово permit означает, что соответствующие пакеты должны шифроваться, а deny означает отказ от шифрования.

**Шаг 4. Создание криптографических карт**

При создании криптографических карт, с помощью средств IPSec можно установить ассоциации защиты для потоков данных, подлежащих шифрованию. Записи криптографических карт определяют параметры ассоциаций защиты IPSec, связывая следующие элементы конфигурации.

– Трафик, который должен защищаться средствами IPSec (списком шифрованного доступа), и степень детализации трафика, защищаемого набором ассоциаций защиты.

– Пункт назначения, куда направляется трафик IPSec (описание удаленной стороны IPSec).

– Локальный адрес, который должен использоваться для трафика IPSec.

– Тип защиты IPSec, применяемый к указанному трафику (наборы преобразований).

– Способ создания ассоциаций защиты: создание вручную или посредством IKE.

– Другие параметры, которые могут понадобиться при создании ассоциаций защиты IPSec.

**Шаг 5. Применение криптографических карт к интерфейсам**

Последним шагом настройки IPSec является применение набора записей криптографической карты к интерфейсу с помощью команды cryptomap в режиме конфигурации интерфейса. Используйте данную команду с префиксом no, чтобы удалить криптографическую карту с интерфейса. Указанная команда имеет следующий синтаксис: Cryptomap имя–карты. Как только вы примените криптографическую карту, в базе данных ассоциаций защиты в памяти системы будут установлены параметры ассоциации защиты.

**Задача 4. Тестирование и контроль IPSec**

Завершающей задачей процесса настройки IPSec для работы с общими ключами является проверка текущих установок и функциональных возможностей IPSec. Программное обеспечение Cisco IOS предлагает ряд команд show, clear и debug, с помощью которых можно проконтролировать работу IKE и IPSec. Их использование обсуждается в следующих разделах.

***Команды IKE***

Команды, описанные в следующих разделах, можно использовать для проверки конфигурации и действия IKE.

Команду show crypto isakmp policy режима EXEC можно использовать для того, чтобы выяснить параметры политики IKE.

Команду show crypto isakmp sa режима EXEC можно использовать для того, чтобы увидеть параметры всех текущих ассоциаций защиты IKE

```
ast–route#sh cr is sa
IPv4 Crypto ISAKMP SA
dst          src          state          conn–id slot status
37.17.177.1  37.17.178.1  QM_IDLE          1073  0 ACTIVE
IPv6 Crypto ISAKMP SA
```

Команду clear crypto isakmp глобальной конфигурации можно применять для очистки активных соединений IKE. Эта команда имеет следующий синтаксис: clear crypto isakmp [id–соедииеиия], где id–соединения (необязательный) идентифицирует соединение, которое требуется очистить. Если значение параметра не указано, будут очищены все существующие соединения.

Команда debug crypto isakmp режима EXEC используется для отображения сообщений о событиях IKE. Использование этой команды с префиксом no отключает вывод отладочных данных.

***Команды IPSec***

Команды, описываемые в следующих разделах, можно применять для проверки параметров конфигурации и контроля действия IPSec.

Командой show crypto ipsec transform–set режима EXEC можно воспользоваться для проверки размещенных наборов преобразований. Указанная команда имеет следующий синтаксис:

show crypto ipsec transform–set [tag имя–набора]

```
ast–route#sh cr ip sa
interface: Serial0/0/0
    Crypto map tag: MAP1, local addr 37.17.178.1
   protected vrf: (none)
   local  ident (addr/mask/prot/port): (37.17.178.1/255.255.255.255/47/0)
   remote  ident (addr/mask/prot/port): (37.17.177.1/255.255.255.255/47/0)
   current_peer 37.17.177.1 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 46038, #pkts encrypt: 46038, #pkts digest: 0
   #pkts decaps: 46192, #pkts decrypt: 46192, #pkts verify: 0
   #pkts compressed: 0, #pkts decompressed: 0
   #pkts not compressed: 0, #pkts compr. failed: 0
   #pkts not decompressed: 0, #pkts decompress failed: 0
   #send errors 1, #recv errors 0
     local crypto endpt.: 37.17.178.1, remote crypto endpt.:37.17.177.1
     path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/0
     current outbound spi: 0x2B736623(728983075)
     inbound esp sas:
      spi: 0x7A92656D(2056414573)
        transform: esp–des esp–sha–hmac ,
        in use settings ={Tunnel, }
        conn id: 2005, flow_id: FPGA:1, crypto map: MAP1
        sa timing: remaining key lifetime (k/sec): (4525504/1348)
        IV size: 16 bytes
        replay detection support: N
        Status: ACTIVE
     inbound ah sas:
     inbound pcp sas:
     outbound esp sas:
      spi: 0x2B736623(728983075)
        transform: esp–des esp–sha–hmac ,
        in use settings ={Tunnel, }
        conn id: 2006, flow_id: FPGA:1, crypto map: MAP1
        sa timing: remaining key lifetime (k/sec): (4525504/1348)
        IV size: 16 bytes
        replay detection support: N
        Status: ACTIVE
     outbound ah sas:
     outbound pcp sas:
```

### 3.5 Инструкция по настройке VPN–соединения для Windows 7

В правом нижнем углу рабочего стола (рядом с часами) найти и нажать значок подключений, в появившемся окне выбрать «Центр управления сетями и общим доступом» (Рисунок 3.9).

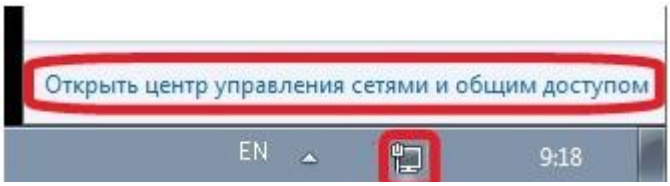


Рисунок 3.9 – Значок подключений на панели задач

Если значок подключений отсутствует, следует воспользоваться меню «ПУСК», где в строке поиска ввести слово «центр». В появившемся списке необходимо выбрать «Центр управления сетями и общим доступом» (Рисунок 3.10).

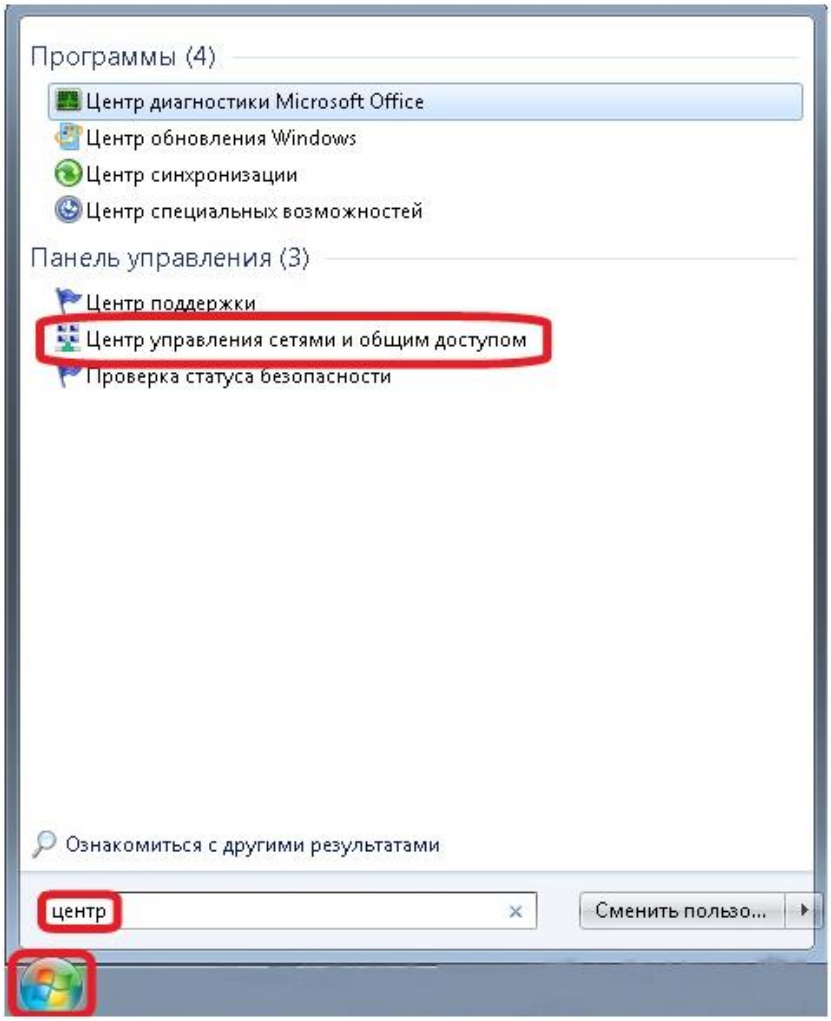


Рисунок 3.10 – Строка поиска в меню «Пуск»

В открывшемся окне следует выбрать пункт «Настройка нового подключения или сети» (Рисунок 3.11).

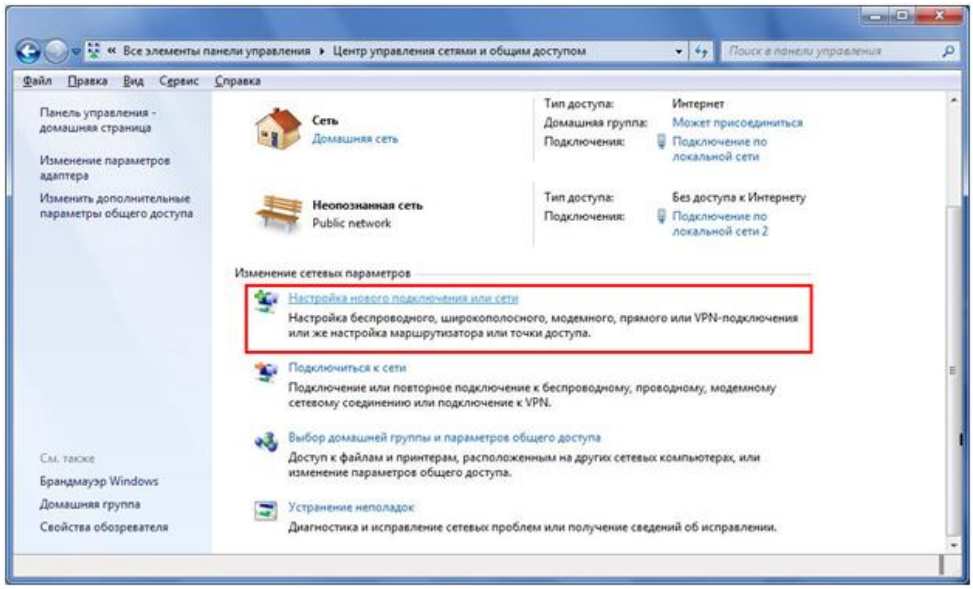


Рисунок 3.11 – Пункт «Настройка нового подключения или сети»

В появившемся окне выбора вариантов необходимо выбрать пункт «Подключение к рабочему месту» и нажать кнопку «Далее» (Рисунок 3.12).

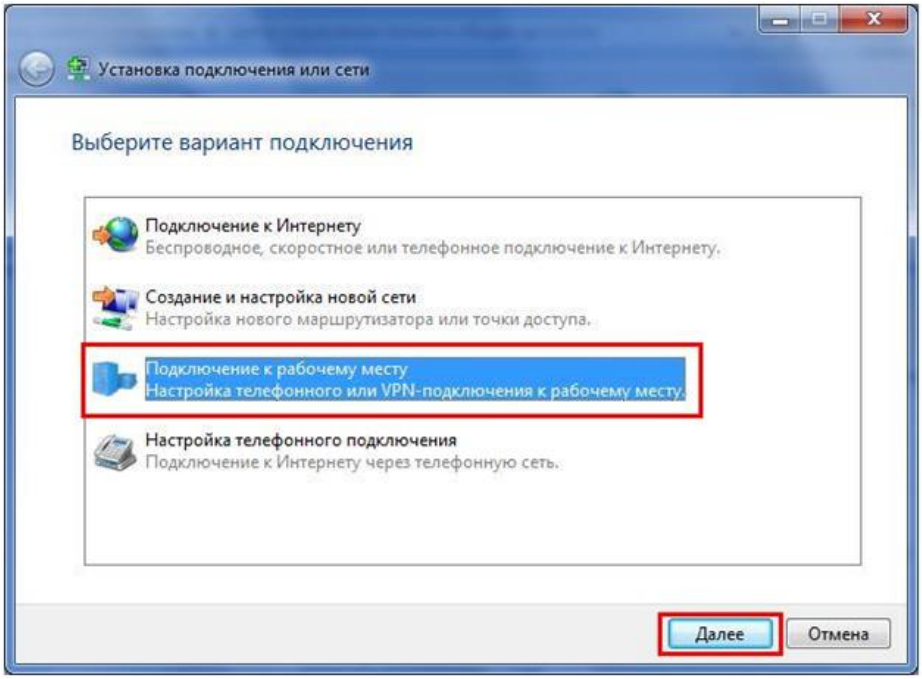


Рисунок 3.12 – Пункт «Подключение к рабочему месту»

Если в системе уже существуют какие–либо подключения удаленного доступа, появится следующее окно, в котором нужно поставить указатель «Нет, создать новое подключение» и нажать кнопку «Далее» (Рисунок 3.13).

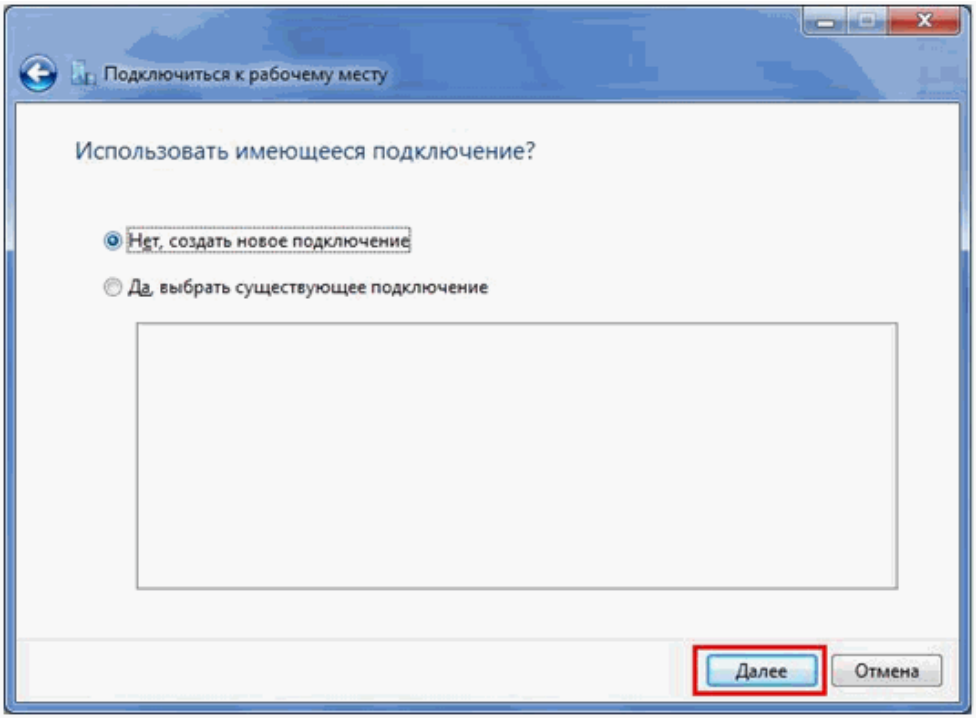


Рисунок 3.13 – Указатель «Нет, создать новое подключение»

В открывшемся окне выбрать «Использовать мое подключение к Интернету (VPN)» (Рисунок 3.14).

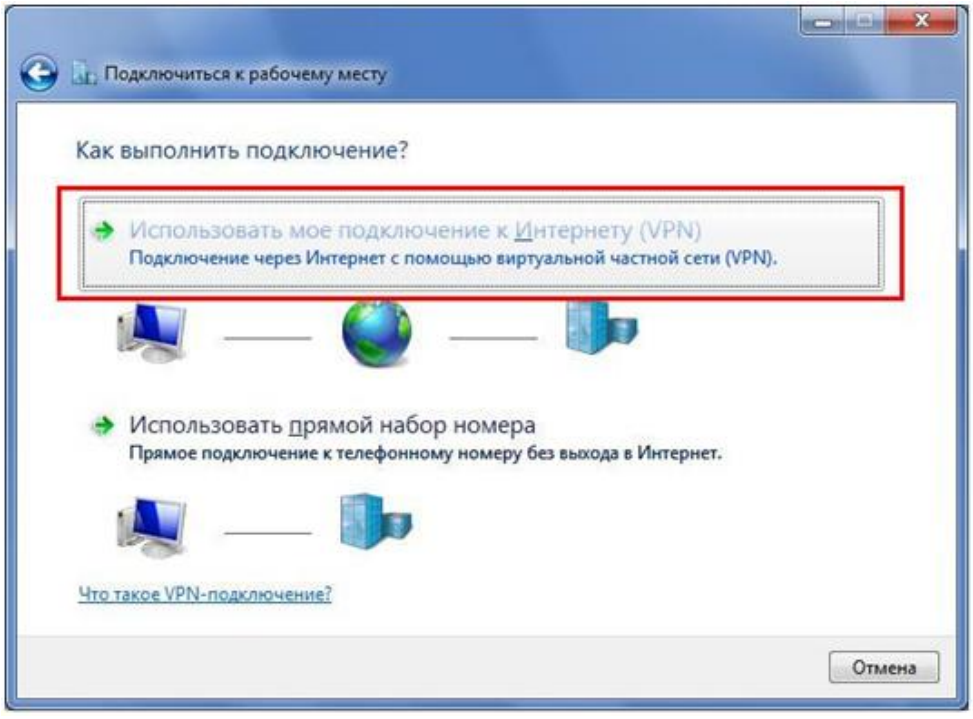


Рисунок 3.14 – Пункт «Использовать мое подключение к интернету VPN»

В поле «Адрес в Интернете» следует ввести адрес. В поле «Имя местоназначения» ввести имя местоназначения и установить галочку в поле

«Не подключаться сейчас, только выполнить установку для подключения в будущем», после чего нажать кнопку «Далее» (Рисунок 3.15).

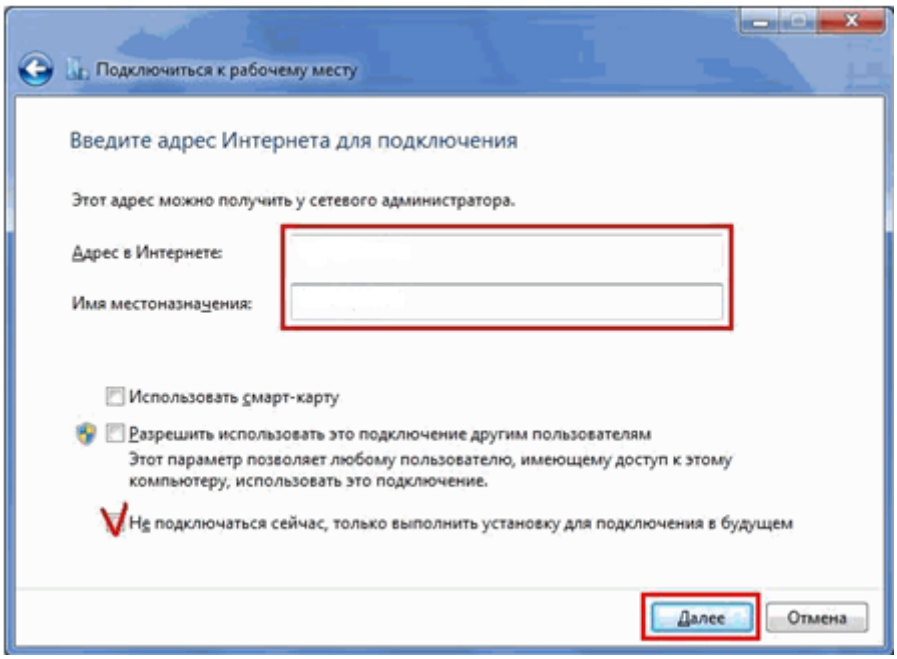


Рисунок 3.15 – Вводимые поля

В поле «Пользователь» следует ввести Ваш логин для VPN, а в поле «Пароль» соответственно Ваш пароль и нажать кнопку «Создать/Подключить» (Рисунок 3.16).

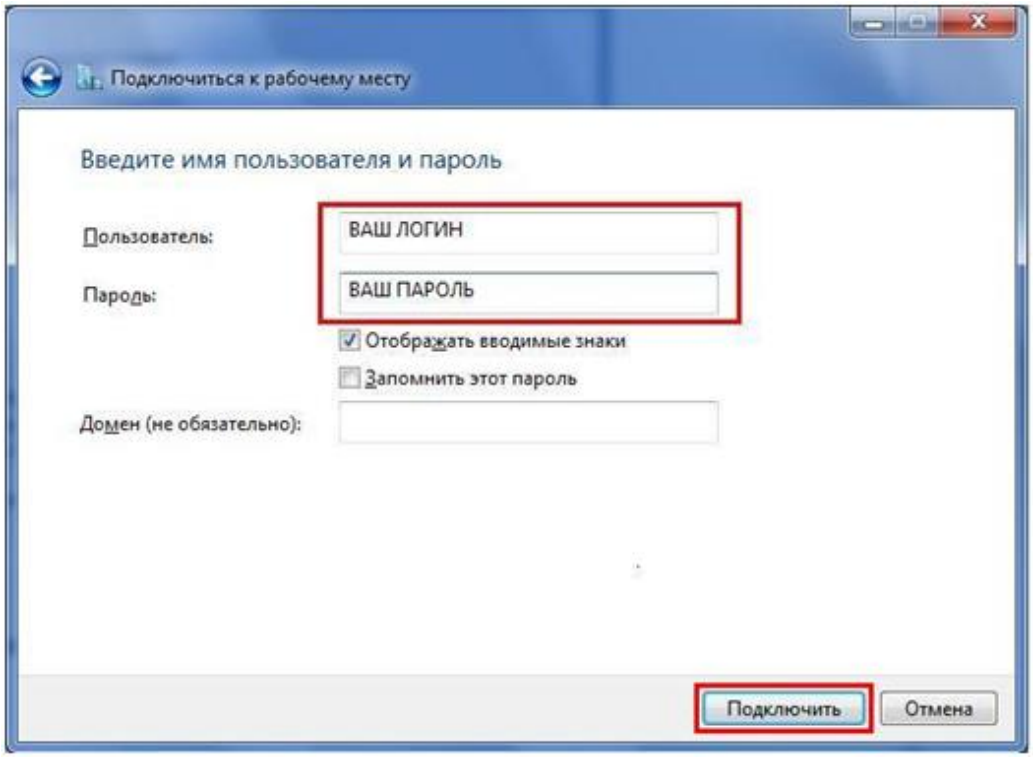


Рисунок 3.16 – Введение логина и пароля

Следующее появившееся окно необходимо просто закрыть (Рисунок 3.17).

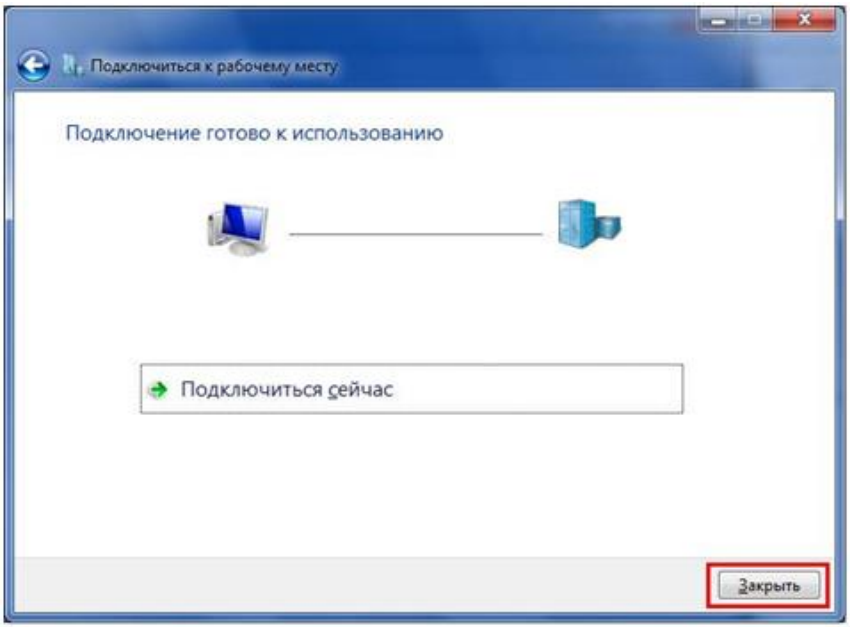


Рисунок 3.17

Теперь следует снова открыть «Центр управления сетями и общим доступом» и выбрать пункт «Подключиться к сети» (Рисунок 3.18).

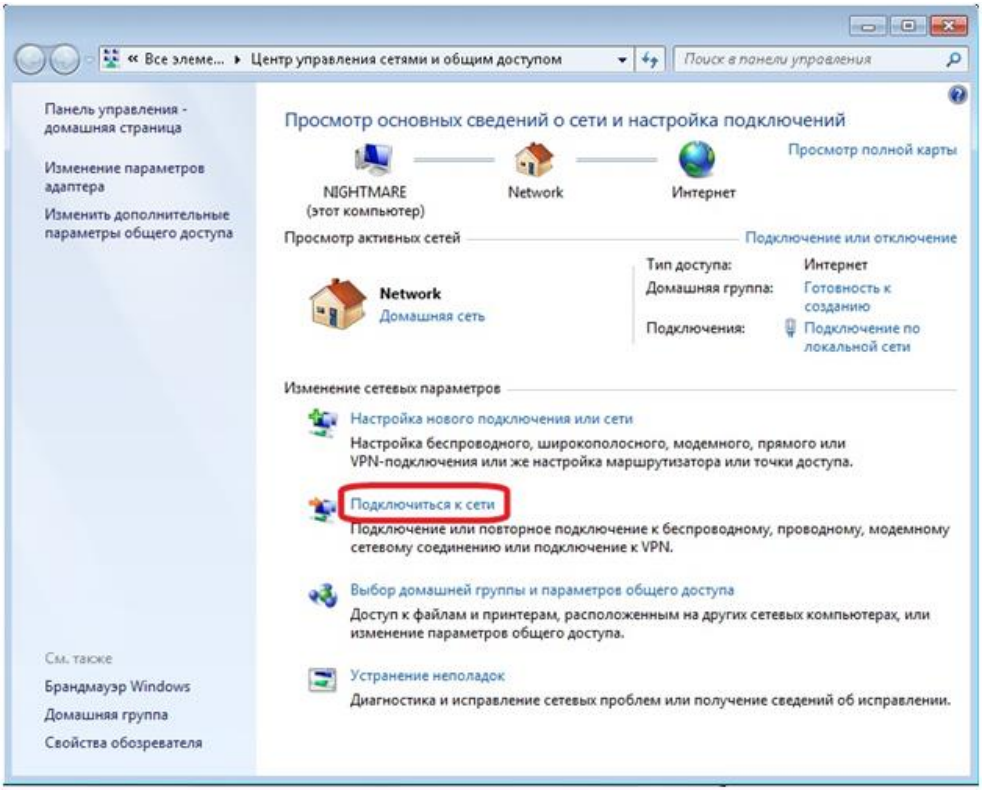


Рисунок 3.18 – Окно «Центр управления сетями и общим доступом»

Далее необходимо выбрать созданное вами подключение и нажать кнопку «Подключение» (Рисунок 3.19).

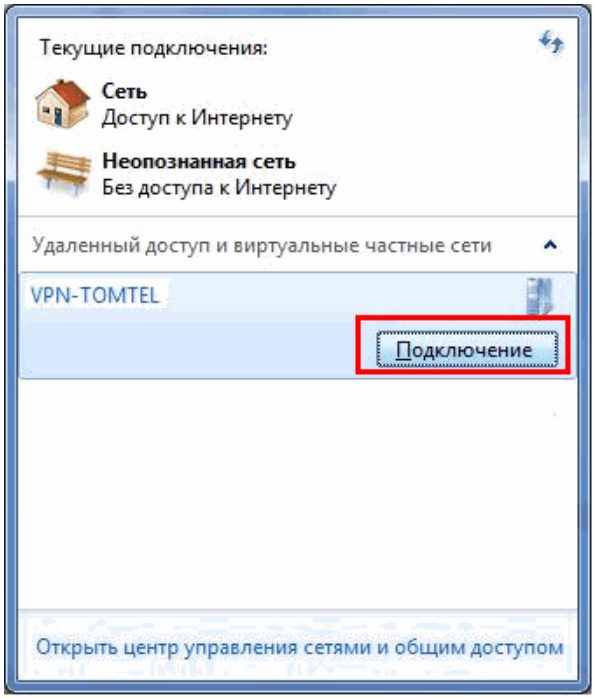


Рисунок 3.19 – Выбор подключения

В «Подключение» необходимо нажать кнопку «Свойства» (Рисунок 3.20).

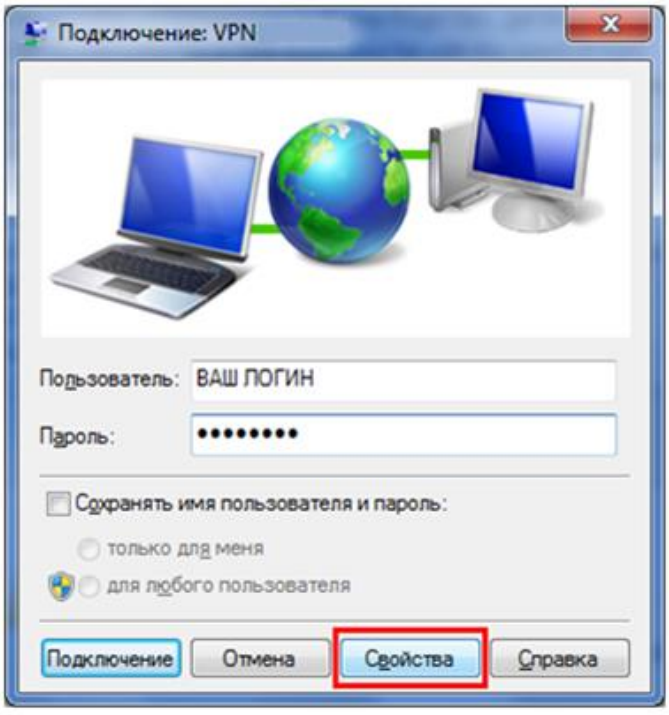


Рисунок 3.20 – Выбор «Свойства» в окне подключения

В открывшейся вкладке «Общие» необходимо убедиться в отсутствии галочки в отмеченной позиции (Рисунок 3.21).

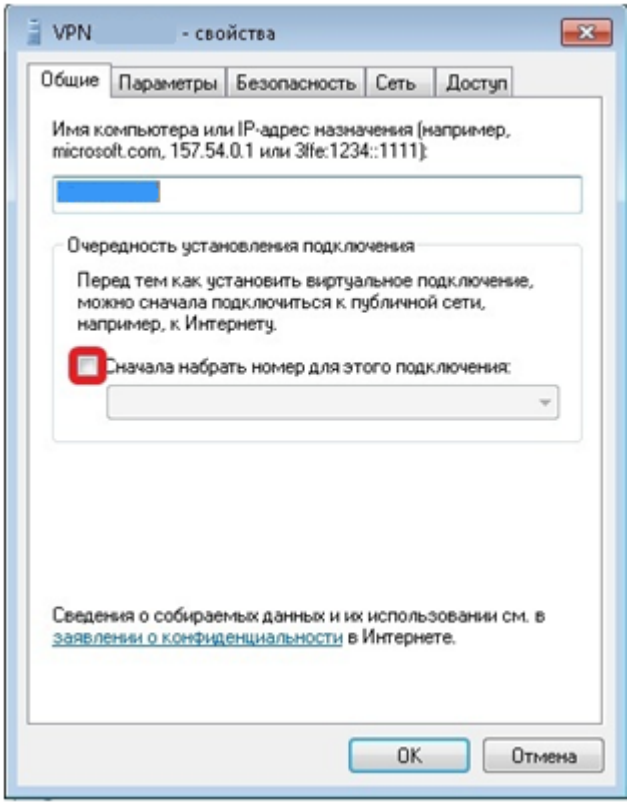


Рисунок 3.21 – Вкладка «Общие»

Затем следует перейти на вкладку «Параметры» и убрать галочку «Включать домен входа в Windows» (Рисунок 3.22).

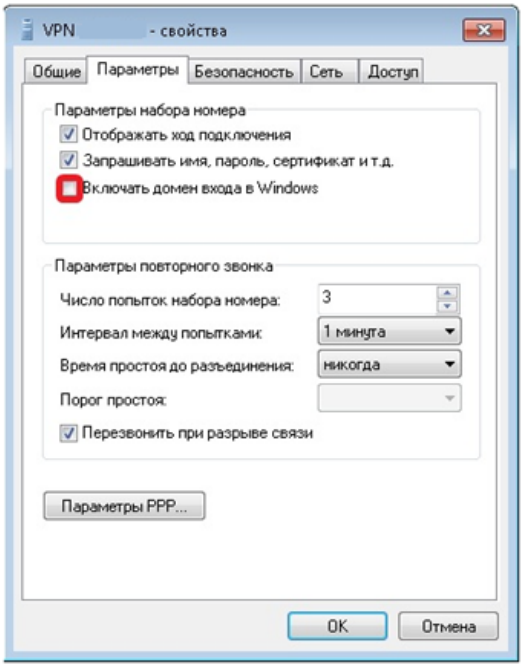


Рисунок 3.22 – Вкладка «Параметры»

На вкладке «Безопасность» очень внимательно выберите параметры настройки как указано ниже (Рисунок 3.23).

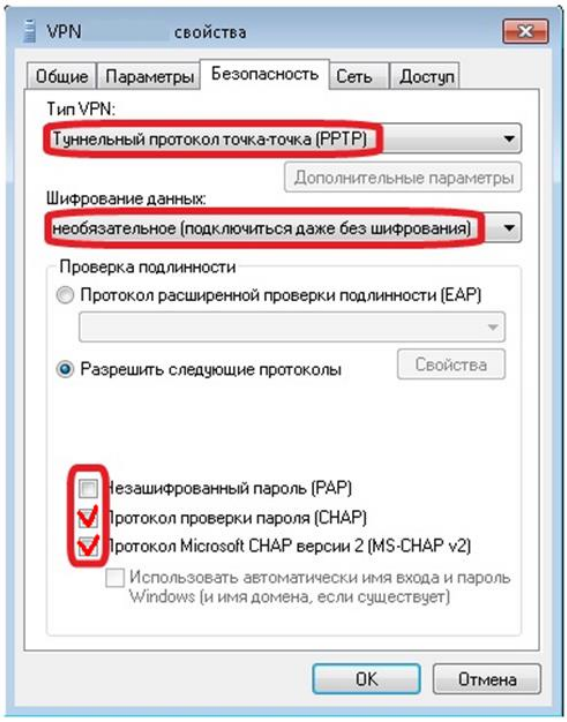


Рисунок 3.23 – Вкладка «Безопасность»

На открывшейся вкладке «Сеть» отключаем необязательные компоненты в соответствии с рисунком и нажать кнопку «ОК» (Рисунок 3.24).

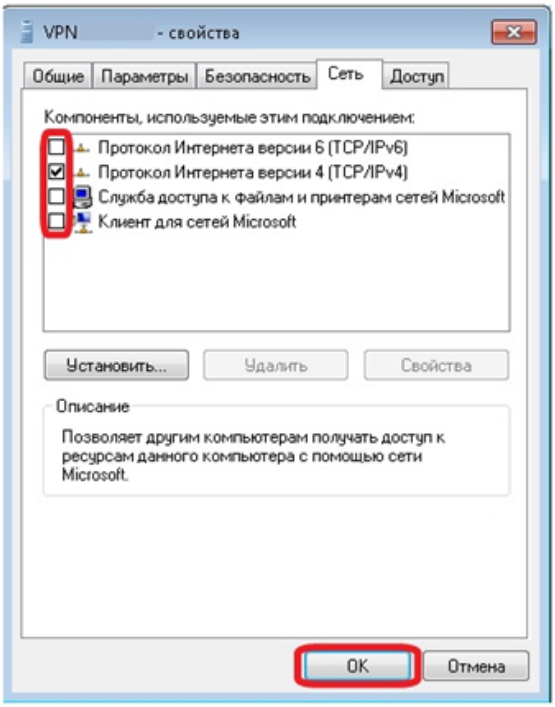


Рисунок 3.24 – Вкладка «Сеть»

Теперь необходимо установить соединение с VPN–сервером. Для этого нажмите кнопку «Подключение» (Рисунок 3.25).

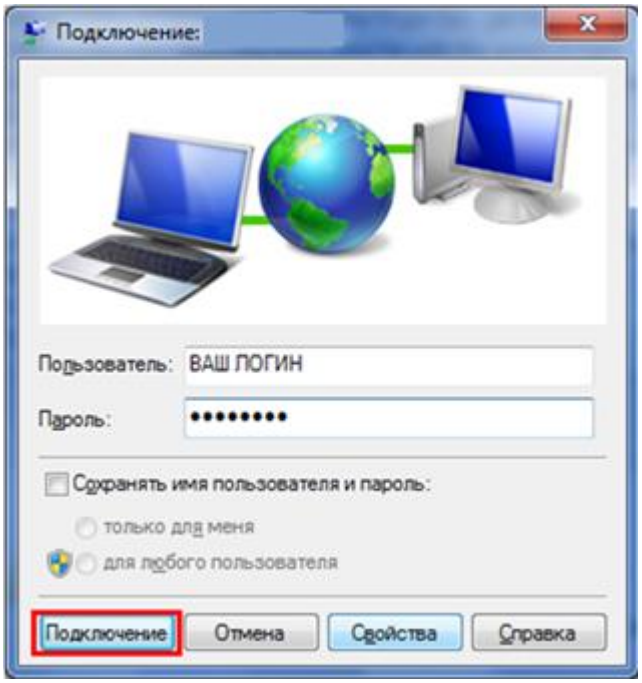


Рисунок 3.25 – Окно «Подключение»

Следует ознакомиться с некоторыми особенностями VPN–соединений:

1 Рекомендуется при подключении к VPN–серверу убедиться в том, что Интернет на портале пользователя.

2 При использовании VPN–соединения некоторые программы могут, несмотря на включенный VPN, продолжать пользоваться обычным каналом.

3 Отчет по VPN сессии может формироваться не мгновенно. После разрыва VPN соединения может пройти до 1 часа времени, прежде, чем будет сделано начисление по итогам сессии.

## Заключение

В данном дипломном проекте была рассмотрена технология Virtual Private Network для безопасного подключения к серверу компании ТОО “TNS-INTEC” в головном офисе в городе Астана из филиала в городе Алматы.

В ходе выполнения проекта были проработаны все варианты создания качественной и надежной сети коммерческого предприятия. В проекте использовалось оборудование Cisco Systems – всемирно известного производителя телекоммуникационных устройств.

В разделе безопасность жизнедеятельности были проведены: анализ потенциально опасных и вредных факторов воздействия на оператора в процессе обслуживания и проектирования сети, расчет мощности охлаждения серверной и анализ пожарной безопасности.

В экономической части проекта был проанализирован рынок и представлен бизнес–план с указанием сравнительной экономической эффективности капитальных вложений.

## Список использованной литературы


1 Сайт http://www.seti.com.ua. – Журнал Сети и телекоммуникации. – №7–8.

2 Дьеченко В.А., Анализ проблем информационной безопасности в компьютерной сети, организации подключенной к сети Интернет. – М., 2009.

3 Сайт http://www.opennet.ru/docs/RUS/vpn_ipsec/

4 Сайт http://ru.wikipedia.org/wiki/IPsec#Security_Policy_Database

5 Николай Колдовский. Построение безопасных сетей на основе VPN. – М.: Инфра–М, 2011.

6 Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы: Учебник. – Санкт–Петербург: Питер, 2001.

7 Щербо В.К. Стандарты вычислительных сетей. – М.: Кудиц–Образ, 2000.

8 Верховский Е.И. Пожарная безопасность на предприятиях радиоэлектроники. – М.: Высшая школа, 1987.

9 Аманбаев У.А. Экономика предприятия. –Алматы: Бастау, 2012.

10 Буров В.П. Бизнес–план фирмы. – М.: Инфра–М, 2011.

11 Куатова Д.Я. Экономика предприятия. – Алматы: Экономика, 2011.

12 Еркешева З.Д., Боканова Г.Ш., Методические указания к выполнению экономической части дипломных работ для студентов специальности 5В070400 – Вычислительная техника и программное обеспечение. – Алматы: АУЭС, 2014. – 40 с.

13 Сайт http://kunegin.narod.ru/ref5/ipsec/doc09.htm

14 Сайт http://www.opennet.ru/docs/RUS/vpn_ipsec/

15 Сайт http://www.ixbt.com/comm/ipsecure.shtml

16 Сайт http://daily.sec.ru/2008/09/08/Virtualnie–chastnie–seti–vibor–optimalnogo–podhoda.html

17 Сайт http://www.micom.net.ru/networks/

**Приложение А**

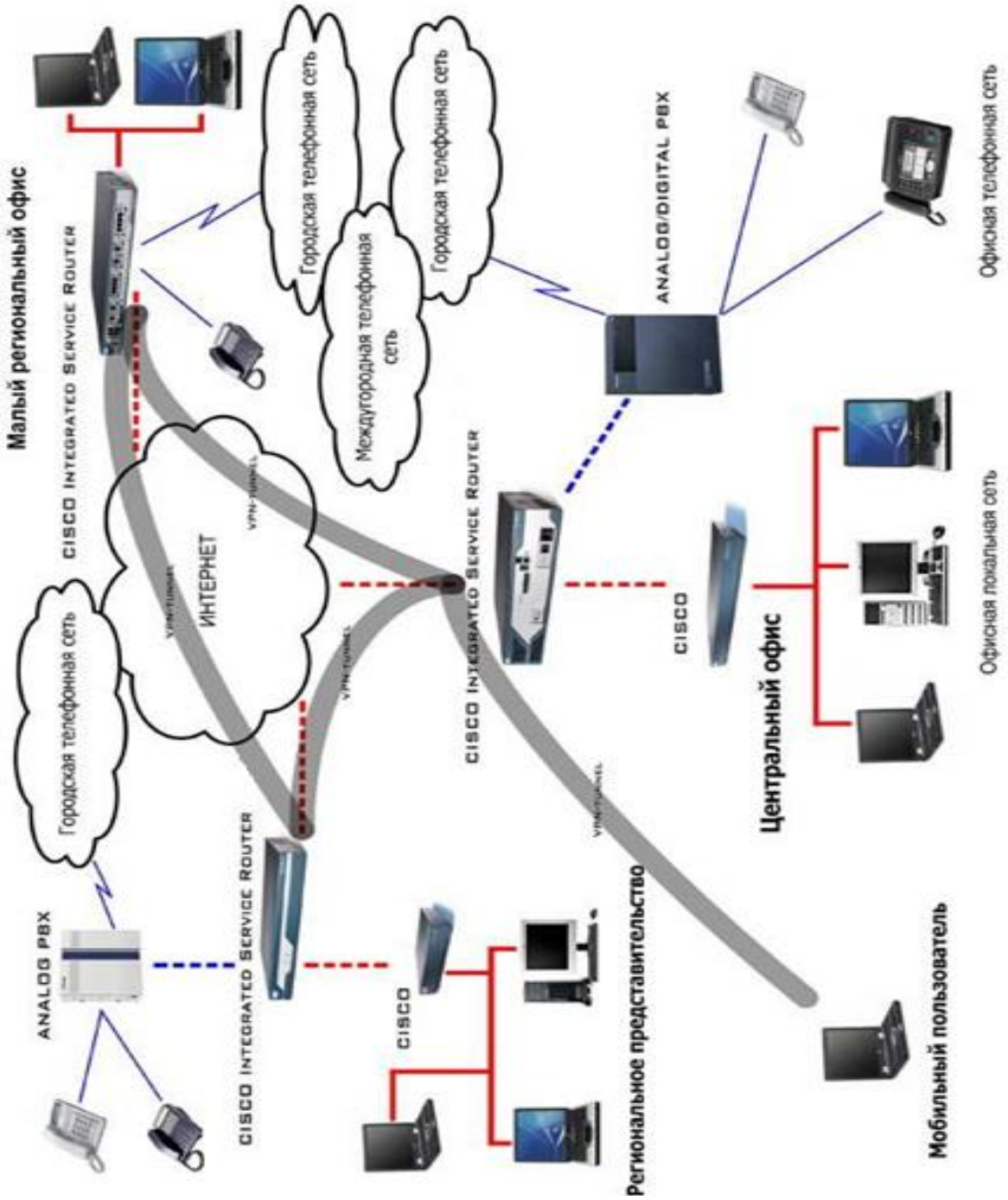


Рисунок А.1 – Структурная схема организации сети

**Приложение Б**

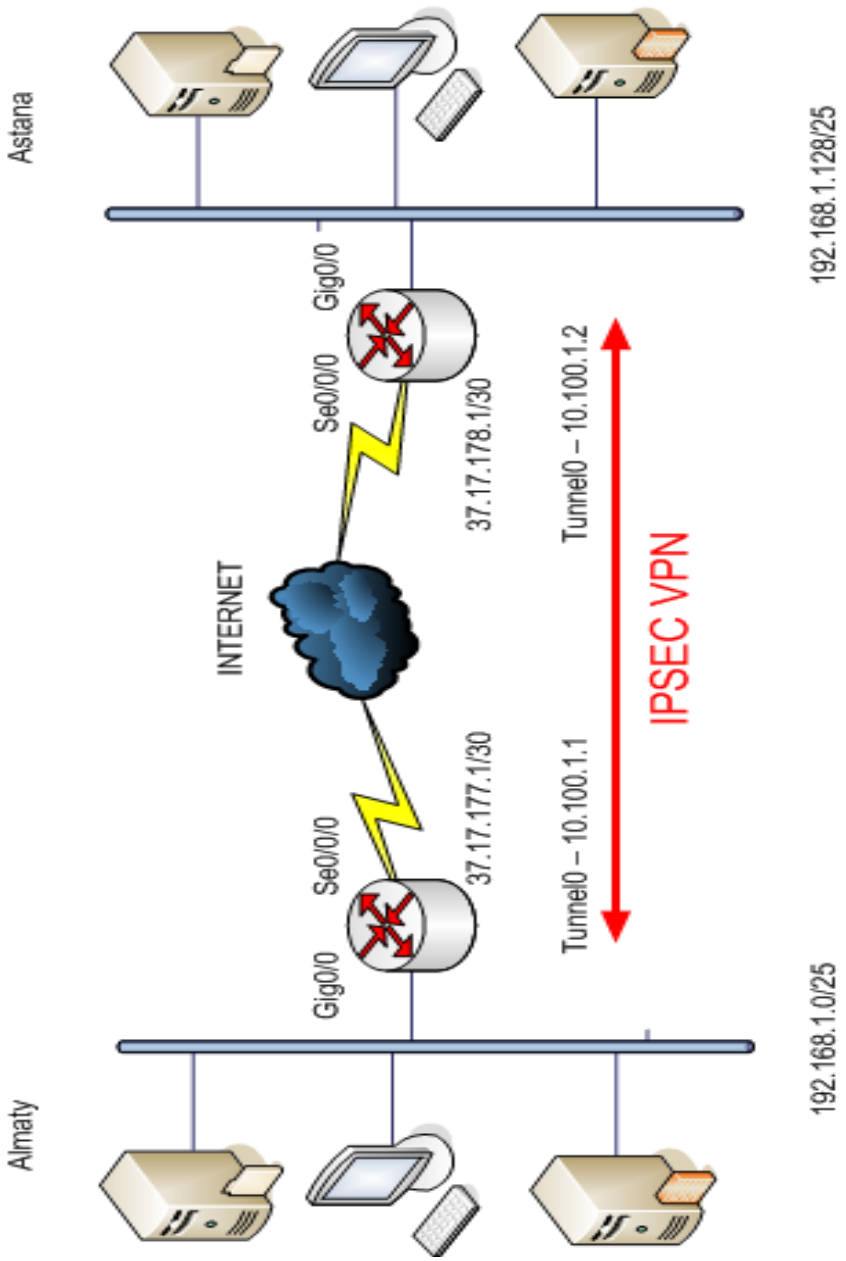


Рисунок Б.1 – Структурная схема сети компании с технологией IPSec VPN

## Приложение В

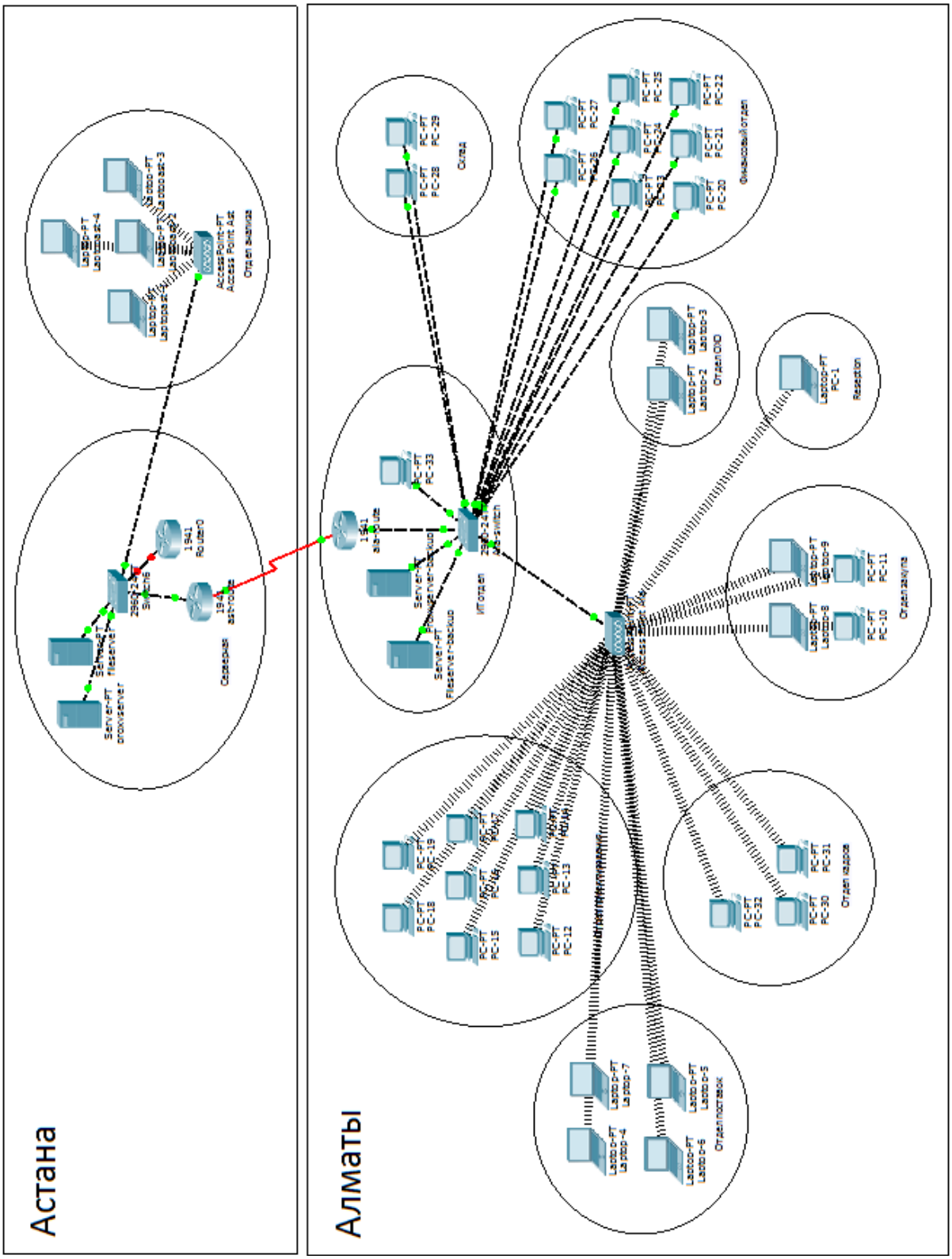


Рисунок В.1 – Схема сети

## Приложение Г

## Конфигурация маршрутизаторов

```
ast–route#sh run
Building configuration...

Current configuration : 1425 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password–encryption
!
hostname ast–route
!
clock timezone almaty 6
!
crypto isakmp policy 1
 authentication pre–share
!
crypto isakmp key key address 37.17.177.1
!
!
crypto ipsec transform–set TSET esp–des esp–sha–hmac
!
crypto map MAP1 10 ipsec–isakmp
 description IPSsec–to–Almaty
 set peer 37.17.177.1
 set transform–set TSET
 match address 101
!
license udi pid CISCO1941/K9 sn FTX1524B2L3
license boot module c1900 technology–package securityk9
!
spanning–tree mode pvst
!
interface Tunnel0
 ip address 10.100.1.2 255.255.255.252
 tunnel source Serial0/0/0
 tunnel destination 37.17.177.1
 tunnel mode gre ip
!
interface GigabitEthernet0/0
 no ip address
 duplex auto
 speed auto
!
interface GigabitEthernet0/0.10
 description local
 encapsulation dot1Q 10
```

```
ip address 192.168.1.129 255.255.255.128
!
interface GigabitEthernet0/1
 no ip address
 duplex auto
 speed auto
!
interface Serial0/0/0
 description link–to–almaty
 ip address 37.17.178.1 255.255.255.248
 encapsulation ppp
 crypto map MAP1
!
interface Serial0/0/1
 no ip address
!
interface Vlan1
 no ip address
 shutdown
!
ip classless
ip route 192.168.1.0 255.255.255.128 10.100.1.1
!
access–list 101 permit gre host 37.17.178.1 host 37.17.177.1
!
line con 0
!
line aux 0
!
line vty 0 4
 login
!
End

ala–route#sh run
Building configuration...

Current configuration : 1596 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password–encryption
!
hostname ala–route
!
ip dhcp excluded–address 192.168.1.1 192.168.1.9
!
ip dhcp pool local
 network 192.168.1.0 255.255.255.128
```

```
 default–router 192.168.1.1
 dns–server 8.8.8.8
clock timezone almaty 6
!
crypto isakmp policy 1
 authentication pre–share
!
crypto isakmp key key address 37.17.178.1
!
crypto ipsec transform–set TSET esp–des esp–sha–hmac
!
crypto map MAP1 10 ipsec–isakmp
 description IPSec–to–Astana
 set peer 37.17.178.1
 set transform–set TSET
 match address 101
!
license udi pid CISCO1941/K9 sn FTX15246GEL
license boot module c1900 technology–package securityk9
!
spanning–tree mode pvst
!
interface Tunnel0
 ip address 10.100.1.1 255.255.255.252
 tunnel source Serial0/0/0
 tunnel destination 37.17.178.1
 tunnel mode gre ip
!
interface GigabitEthernet0/0
 no ip address
 duplex auto
 speed auto
!
interface GigabitEthernet0/0.10
 description local
 encapsulation dot1Q 10
 ip address 192.168.1.1 255.255.255.128
!
interface GigabitEthernet0/1
 no ip address
 duplex auto
 speed auto
!
interface Serial0/0/0
 description link–to–astana
 ip address 37.17.177.1 255.255.255.248
 encapsulation ppp
 clock rate 125000
 crypto map MAP1
```

```
!
interface Serial0/0/1
 no ip address
!
interface Vlan1
 no ip address
 shutdown
!
ip classless
ip route 192.168.1.128 255.255.255.128 10.100.1.2
!
access–list 101 permit gre host 37.17.177.1 host 37.17.178.1
!
line con 0
!
line aux 0
!
line vty 0 4
 login
!
end
```