ЗАЩИТА КОМПЬЮТЕРНЫХ СЕТЕЙ НА ОСНОВЕ ТЕХНОЛОГИИ VIRTUAL PRIVATE NETWORK.

Е.И. Наполова, *магистрант МТУСИ, 111024, г. Москва, ул. Авиамоторная, 8А., Katya.napolova@mail.ru;*
С.В. Кожевников, *магистрант МТУСИ, 111024, г. Москва, ул. Авиамоторная, 8А.*

УДК 654.16

Аннотация. Статья посвящена современным VPN – сетям. Данная проблема очень актуальна в настоящее время, что связано главным образом с обеспечением безопасности в сети интернет. Меры безопасности используют как компании, так и обычные пользователи. Это позволяет персоналу работать удаленно и пользоваться данными фирмы без опасений утечки информации. Целью исследования является разработка алгоритма организации безопасного подключения распределенной корпоративной сети к интернету.

Ключевые слова: защита компьютерных сетей; технологии VIRTUAL PRIVATE NETWORK.

DEFENSE OF THE COMPUTER NETWORK BASED ON VIRTUAL PRIVATE NETWORKS TECHNOLOGY

Ekaterina Napolova, *graduate student MTUCI, 111024, Moscow, Aviamotornaya st., 8A.;*
Sergey Kozhevnikov, *graduate student MTUCI, 111024, Moscow, Aviamotornaya st., 8A.*

Annotation. The article is devoted to modern VPN networks. This problem is very relevant at the present time. This is mainly due to the security of the Internet. Security measures are used by both companies and ordinary users. This allows personnel to work remotely and use company data without fear of information leakage.

The aim of the study is to develop an algorithm for the organization of a secure connection of a distributed corporate network to the Internet.

Keywords: protection of computer networks; VIRTUAL PRIVATE NETWORK technology.

На любом предприятии, в процессе функционирования которого обрабатывается конфиденциальная информация, вместе с ней возникает необходимость ее защиты. Постоянно идет создание более совершенных каналов передачи данных, способов защиты этих каналов, их физиологиия и программное совершенствование системы передачи данных.

В зависимости от каналов передачи данных, в которых циркулирует информация, применяются различные методы ее защиты и требуются концептуально разные подходы к защите.

Для предприятий, отличительной особенностью которых является постоянный рост и увеличение штата сотрудников, а также имеющих удаленные офисы, наиболее оптимальным станет использование виртуальных частных сетей. Виртуальные частные сети (VPN – Virtual Private Network) представляют собой защищенное соединение, которое создается внутри незащищенной сети с использованием открытых каналов связи путем создания зашифрованного канала. Проще говоря, такое соединение можно представить как туннель, проложенный через интернет.

Виртуальные сети получили большое распространение за счет экономичности и высокой безопасности, особенно при использовании распределенных вычислительных сетей. В технологии VPN для защиты компьютерных сетей используются технологии, включающие в себя элементы межсетевого экранирования и механизмы криптографической защиты сетевого трафика [1, 2].

VPN с помощью специальных программ объединяет отдельные компьютеры и локальные сети для защиты передаваемой информации. При соединении с сервером, находящимся в сети общего доступа VPN, технология образует канал защищаемый информацию с помощью алгоритмов шифрования. Таким образом внутри незащищенной сети образуется защищенный туннель для передачи данных. Проще говоря, VPN позволяет виртуально подключить одну сеть к другой таким образом, как будто они соединены проводами, при этом весь исходящий и входящий трафик шифруется, что делает эту технологию безопасной.

Разработка алгоритма организации безопасного подключения распределенной корпоративной сети к интернету

Для разработки алгоритма необходимо представить типичную структуру организации сети предприятия. За основу взято предприятие малого или среднего бизнеса, имеющее центральный офис и несколько удаленных, и для которого требуется осуществлять обмен конфиденциальной информации между офисами. Вследствие ограниченности бюджета содержание выделенных провайдером каналов не представляется возможным, поэтому обмен информацией обеспечивается по открытым каналам интернета.

Требуется разработать архитектуру, включающую следующие компоненты: структуру главного и удаленных офисов, имеющих возможность осуществлять информационный обмен между собой, организацию безопасной сетевой инфраструктуры, характерной для сетей любого масштаба и обеспечивающей защиту от основных угроз информационной безопасности; гибкие возможности сетевых настроек.

На рис. 1 представлена высокоуровневая сетевая диаграмма, демонстрирующая различные типы бизнес-подключений, которые могут быть реализованы с использованием разрабатываемой архитектуры [3], включающей в себя центральный офис и два удаленных офиса. Сеть построена с помощью WAN-маршрутизаторов (Cisco 2811) и LAN-коммутаторов (Cisco Catalyst 2960).

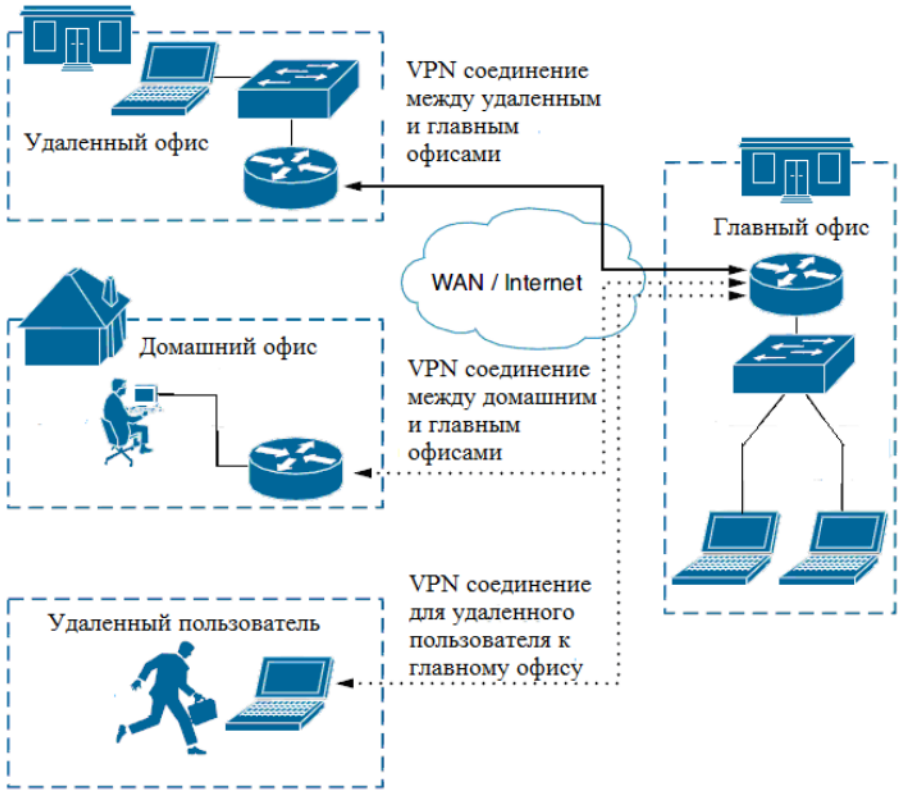

Рисунок 1

Для организации и поддержки данных возможностей при разработке архитектуры будут использованы следующие технологии: Standard Cisco IPSec, обеспечивающий VPN соединение между офисами предприятия; динамическая маршрутизация на основе протокола OSPFv2; технология PAT для трансляции частных IP-адресов в публичный IP-адрес; списки доступа ACL для ограничения доступа к ресурсам сети предприятия; технология VLAN для разграничения доступа внутри широковещательного домена локальной сети; контроль доступа к сетевым устройствам на основе парольной аутентификации с использованием списка привилегий; зеркалирование трафика на коммутирующем устройстве для контроля активности сети; удаленное управление сетевыми устройствами на основе защищенного протокола SSH.

Для реализации алгоритма необходимо было выбрать среду моделирования, отвечающую требованиям организации корпоративной распределенной сети предприятия. Для данной цели было предложено использовать официальную среду моделирования Cisco Packet Tracer v 6.2, в которой была построена и сконфигурирована распределенная корпоративная сеть, использующая каналы общего доступа для организации взаимодействия между офисами (структура сети представлена на рис. 2).

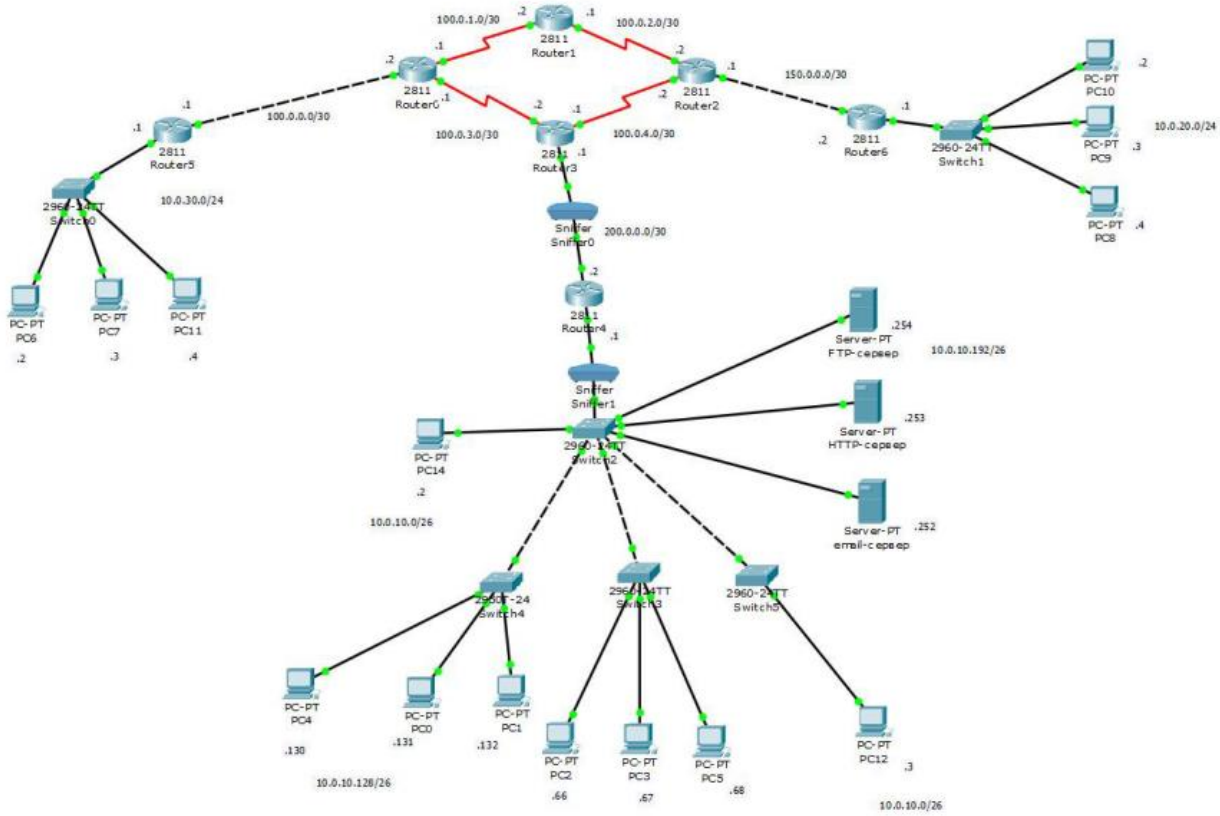

Рисунок 2

Перед подключением локальной сети офиса к интернету необходимо обеспечить внутреннюю безопасность локальной сети, поэтому была выбрана представленная очередность действий [4]:

1. Обеспечение безопасности локальной сети (разграничение доступа к сетевым устройствам, настройка удаленного управления сетевыми устройствами, настройка контроля добавления новых устройств, конфигурация VLAN).
2. Организация безопасного подключения к сети интернет (настройка зеркалирования трафика на центральном коммутаторе, настройка списков доступа к локальным и удаленным ресурсам, реализация VPN-соединения Standard Cisco IPSec между удаленными офисами, настройка PAT).

3. Проверка функционирования и защищенности сети.

Разграничение доступа к сетевым устройствам рассматривается как необходимая мера, ограничивающая доступ к изменению настроек сетевого оборудования и являющаяся обязательной мерой для пограничного сетевого оборудования [5, 6]. Для корректного использования сетевых устройств и разделения обязанностей требуется ввести привилегированный доступ к устройствам:

- пользователь не может применять изменения и смотреть файлы конфигурации;
- агент поддержки также имеет возможности пользователя и доступ к команде ping;
- помощник администратора имеет возможности агента поддержки и возможность перезагрузки оборудования;
- администратор имеет полный доступ к конфигурации устройства;
- подключение по протоколу telnet (настройка удаленного доступа) крайне небезопасно, так как передает пароли по сети в открытом виде; для защиты данного конфиденциального трафика используется протокол SSH.

Контроль добавления устройств. Реализуется за счет настройки безопасности портов на коммутаторах доступа. Каждому интерфейсу коммутатора ставится в соответствие MAC-адрес разрешенного для этого интерфейса сетевого адаптера. Данное решение также способно защитить локальную сеть от атак типа «отказ в обслуживании», которые реализуются с помощью переполнения таблицы MAC-адресов [7, 8].

Конфигурация VLAN. Каждое подразделение привязано к своему коммутатору доступа и находится в собственной VPN, интерфейсы данных коммутаторов ассоциируются с номером этой виртуальной сети. Интерфейсы коммутаторов, которые должны передавать трафик нескольких VPN, обозначаются как trunk-интерфейсы; на пограничном маршрутизаторе выделяются несколько подинтерфейсов для каждого VLAN.

Зеркалирование трафика на центральном коммутаторе. Используется для контроля, приходящего из сети интернет трафика при помощи IDS или анализатора трафика, который установлен на рабочей станции, контролируемой системным администратором. С использованием зеркалирования осуществляется скрытие контроля трафика для обычных пользователей сети и злоумышленников.

Настройка списков доступа ACL. Основными являются списки доступа к общим ресурсам сети – серверам. Данные списки отчасти выполняют функции межсетевого экрана, так как способны фильтровать трафик по адресу назначения, источника, типу протокола. Вследствие того, что контроль адресов осуществляется на пограничном маршрутизаторе, задачей для списков доступа к серверам является контроль допустимых для использования портов.

Реализация VPN-соединения между удаленными офисами. Настройка пограничных маршрутизаторов характеризуется методом обмена ключами (ISAK.MP), методом шифрования (AES), алгоритмом хеширования (SHA-1), методом аутентификации (обмен ключами при создании подключения), обмен ключами методом Диффи-Хеллмана второй группы (1024 бита).

Настройка PAT усложняется использованием технологии VPN для правильной конфигурации, которой необходимо исключение из транслирования трафика между удаленными офисами, так как протокол IPSec уже производит трансляцию для указанного в его списках доступа трафика.

Проверка работоспособности и защищенности сети, реализованной при помощи предложенного алгоритма, производится поэтапно. Первым этапом является проверка работоспособности и защищенности сетевого оборудования локальной сети. Вторым этапом считается проверка работоспособности и защищенности доступа в интернет и взаимодействия с удаленными офисами.

Таким образом, в результате применения предложенного нами алгоритма настройки VPN могут быть протестированы на корректность и соответствие требованиям безопасности. Смоделированная защищенная корпоративная сеть способна противодействовать основным угрозам безопасности и применима на практике.

Заключение

В данной статье была исследована технология функционирования VPN. В соответствии с представленной классификацией нами были выделены решения, реализуемые на канальном, сетевом и сеансовом уровнях модели OSI. Для практической реализации было выбрано решение на основе протокола IPSec за счет его широкой распространенности и стандартизованности. Также были изучены дополнительные средства обеспечения безопасности корпоративной сети. Был проведен анализ стека протоколов IPSec, рассмотрены его основные компоненты: AH, ESP, IKE. Выделены этапы установления соединения при организации туннеля и произведен криптоанализ данного стека протоколов. Был сделан вывод о соответствии использования стека протоколов IPSec для организации безопасного подключения к интернету распределенной корпоративной сети.

В ходе исследования были изучены варианты организации VPN-соединений на базе оборудования Cisco. Были проанализированы пять решений: DMNVPN, Easy VPN, GRE-based VPN, GET-VPN, standard IPSec, выделены преимущества, недостатки и определена сфера применения каждого из них. На основе исследования для реализации был выбран standard IPSec, ключевым преимуществом которого является его мультивендорность. Однако для случая, когда количество удаленных офисов велико, вместо standard IPSec рекомендуется использование DMNVPN или Easy VPN.

Был разработан алгоритм для организации безопасного подключения распределенной корпоративной сети к интернету средствами оборудования компании Cisco. Он включает этапы по обеспечению безопасности сетевого оборудования, внутренних ресурсов сети компании, организации безопасного взаимодействия между удаленными офисами и контроль доступа в интернет. Для реализации алгоритма была смоделирована типичная распределенная корпоративная сеть, включающая основной офис и несколько удаленных офисов. Реализация алгоритма была произведена в официальной среде моделирования Cisco Packet Tracer. Защита сети была проверена на работоспособность, по результатам которой был сделан вывод о том, что разработанный алгоритм может быть применен для обеспечения безопасного подключения к интернету распределенной корпоративной сети малого или среднего бизнеса.

Литература

1. Запечников С.В. Основы построения виртуальных частных сетей / С.В. Запечников, Н.Г. Милославская, А.И. Толстой. – М: Горячая Линия - Телеком, 2011. – 248 с.
2. Калашников С.К. История «болезней» VPN // Журнал сетевых решений, 2013. – № 11.
3. Корячко В.П. Анализ и проектирование маршрутов передачи данных в корпоративных сетях / В.П. Корячко, Д.А. Перепелкин, – М.: Горячая Линия -Телеком, 2010. – 236 с.
4. Семенов Ю.А. Алгоритмы телекоммуникационных сетей. В 3 частях. Часть 3. Процедуры, диагностика, безопасность / Ю.А. Семенов - М.: БИНОМ. Лаборатория знаний, 2007. – 512 с.
5. Лэммл Т. CCNA Cisco Certified Network Associate. Учебное руководство: учебное пособие. - 2-е изд., перераб. и доп. – М.: ЛОРИ, 2014. – 576 с.
6. Семенов Ю.А. Алгоритмы телекоммуникационных сетей. В 3 частях. Часть 1. Алгоритмы и протоколы каналов и сетей передачи данных / Ю.А. Семенов – М.: БИНОМ. Лаборатория знаний, 2007. – 640 с.
7. Лэммл Т. Настройка коммутаторов. Учебное руководство / Т. Лэммл, К. Хейлзю – М.: Лори, 2015. – 464 с.
8. Шаньгин В.Ф. Защита информации в компьютерных системах и сетях: учебное пособие. – М.: ДМК Пресс, 2012. – 592 с.