УДК 654.16

Авласевич Д.В., студент,
4 курс, Институт финансов, экономики и управления,
Тольяттинский государственный университет,
Тольятти (Россия)
Дмитриев Н.А., студент,
4 курс, Институт финансов, экономики и управления,
Тольяттинский Государственный Университет,
Тольятти (Россия)
Кириллов А.А., студент,
4 курс, Институт финансов, экономики и управления,
Тольяттинский Государственный Университет,
Тольятти (Россия)
Бачинский А.Г. магистрант
1 курс, Институт машиностроения,
Тольяттинский государственный университет,
Тольятти (Россия)
Avlasevich DV, student,
4th year, Institute of Finance, Economics and Management,
Tolyatti State University,
Tolyatti (Russia)
Dmitriev NA, student,
4th year, Institute of Finance, Economics and Management,
Tolyatti State University,
Tolyatti (Russia)
Kirillov AA, student,
4th year, Institute of Finance, Economics and Management,
Tolyatti State University,
Tolyatti (Russia)
Bachinsky A.G. undergraduate

1 year, Institute of Mechanical Engineering,
Togliatti State University,
Tolyatti (Russia)

ЗАЩИТА КОМПЬЮТЕРНЫХ СЕТЕЙ НА ОСНОВЕ ТЕХНОЛОГИИ VIRTUAL.

Аннотация: Публикация посвящена прогрессивным VPN – сетям. Предоставленная проблема весьма актуальна в наше время, что связано главным образом с предоставлением защищенности в сети интернет. Меры защищенности применяют как фирмы, так и простые пользователи. Это дает возможность персоналу функционировать удаленно и пользоваться сведениями компании без опасений потери данных. Целью изучения является создание метода компании безопасного подсоединения распределенной коллективной сети к сети интернет.

Ключевые слова: Защита сетей; VPN; методы защиты.

Protection of computer networks based on virtual technology.

Annotation: The publication is dedicated to progressive VPN networks. This is due to the need to protect rights on the Internet. And so just the users. This enables staff to function remotely and use data. Distribution of a collective network on the Internet.

Keywords: Network protection; VPN; protection methods.

В каждой компании, в ходе функционирования которого обрабатывается конфиденциальные сведения, совместно с ней появляется потребность ее охраны. Регулярно проходит формирование наиболее безупречных каналов передачи сведений, методов охраны данных каналов, их физиология также программное усовершенствование концепции передачи сведений.

В зависимости от каналов передачи сведений, в которых циркулируют сведения, используются разнообразные способы ее охраны и необходимы концептуально различные комбинации в охране.

Для компаний, характерной чертой которых считается непрерывный рост и повышение штата работников, а также обладающих удаленными офисами, наилучшим будет применение условных индивидуальных сетей. Виртуальные индивидуальные сети (VPN – Virtual Private Network) предполагают собой оберегаемое соединение, формируемое внутри незащищенной сети с применением открытых каналов взаимосвязи путем формирования зашифрованного канала. Проще говоря, подобное соединение возможно представить, как тоннель, протянутый посредством сети интернет.

Виртуальные сети приобрели огромное продвижение за счет экономичности и значительной защищенности, в особенности при применении распределенных вычислительных сетей. В схеме VPN для охраны компьютерных сетей применяются технологические процессы, содержащие в себе компоненты межсетевого экранирования и механизмы шифровальной охраны сетевого трафика. VPN с поддержкой специализированных программ связывает отдельные пк и местные сети с целью охраны представляемых данных.

При сочетании с сервером, пребывающим в сети общего доступа VPN, методика формирует путь, оберегаемый сведения со поддержкой алгоритмов кодирования. Подобным способом внутри открытой сети появляется безопасный тоннель с целью передачи сведений. Проще говоря, VPN дает возможность виртуально подсоединить одну сеть к другой таким образом, как будто бы они объединены проводами, при этом полный исходящий и входящий трафик кодируется. Это создает данную технологию не опасной.

Создание метода компании не опасного подсоединения распределенной коллективной сети к интернету.

С целью исследования метода следует предположить стандартную структуру компании сети фирмы. За основание принята организация небольшого либо посредственного коммерциала, обладающее главным офисом и рядом удаленных, и для которого необходимо реализовывать обмен секретными данными среди представительств. Из-За ограниченности бюджета сущность назначенных интернет – провайдером каналов никак не является допустимым, по этой причине обмен данными гарантируется согласно открытым каналам сети интернет.

Необходимо создать архитектуру, содержащую соответствующее элементы: структуру основного также удаленных представительств, обладающих правом реализовывать информационный взаимообмен между собой, систему безопасной сетевой инфраструктуры, отличительной для сетей каждого масштаба также обеспечивающей охрану от ключевых опасностей информационной защищенности; гибкие способности сетевых опций.

На рис. 1 изображена высокоуровневая сетевая диаграмма, показывающая разнообразные виды бизнес-подключений, которые имеют все шансы быть реализованными с применением разрабатываемой архитектуры, содержащей в себе главный офис и два удаленных офиса. Сеть создана с поддержкой WAN-маршрутизаторов также LAN-коммутаторов.

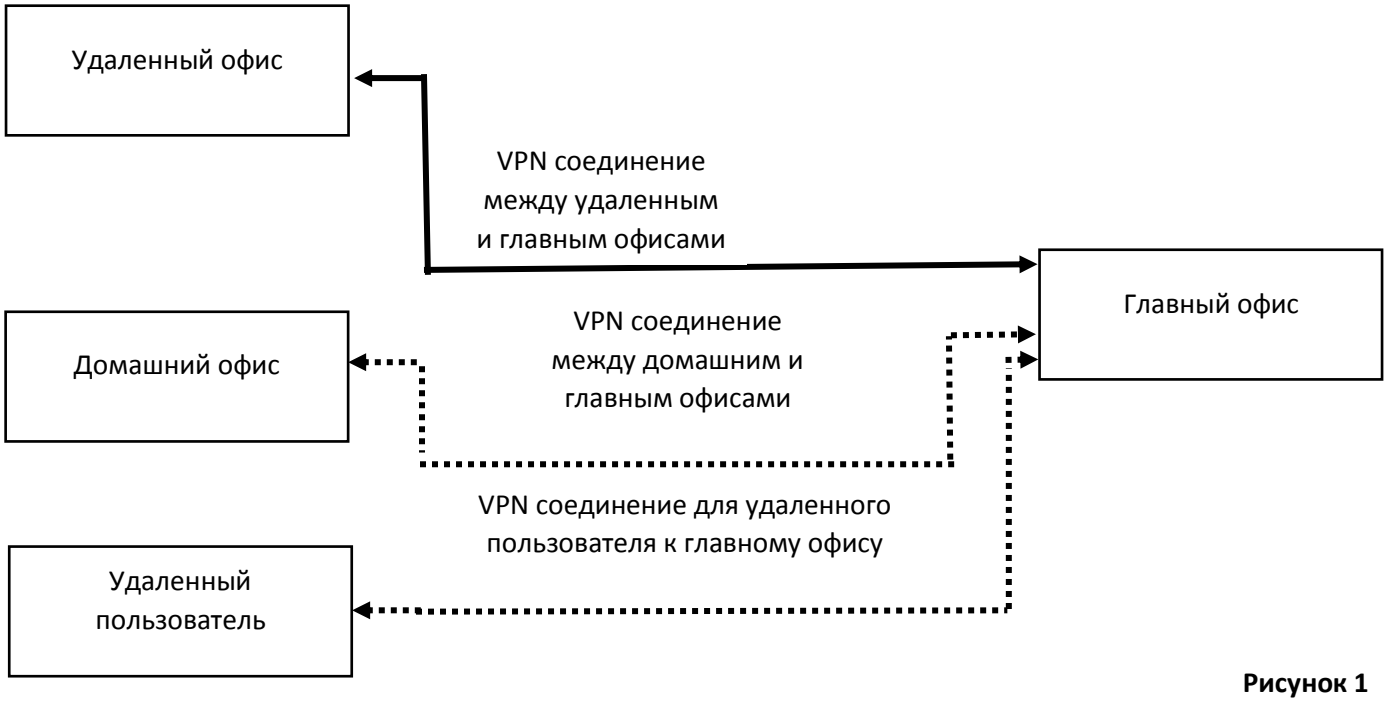

Рисунок 1

Для компании и поддержки данных способностей при исследовании архитектуры будут применены соответствующие технологические процессы: Standard Cisco IPSec, гарантирующий VPN соединение среди представительствами компании; динамическая маршрутизация в базе протокола OSPFv2; методика PAT с целью трансляции индивидуальных IP-адресов в публичный IP-адрес; перечни доступа ACL с целью лимитирования допуска к ресурсам сети компании; методика VLAN с целью разделения допуска изнутри вещательного домена местной сети; управление допуском к сетевым приборам на основании парольной аутентификации с применением перечня преимуществ; зеркалирование трафика в перестановочном устройстве с целью контроля активности сети; удаленное руководство сетевыми приборами на базе защищенного протокола SSH.

С Целью осуществлении метода следует подобрать сферу моделирования, отвечающую условиям компании коллективной распределенной сети компании. Для этой цели было предложено применять

служебную сферу моделирования Cisco Packet Tracer v 6.2, в которой была создана и сконфигурирована распределенная коллективная сеть, использующая каналы единого допуска для компании взаимодействия среди представительств.

Перед подсоединением местной сети представительства к сети интернет следует гарантировать внутреннюю защищенность местной сети, по этой причине существовала представленная последовательность операций:

1. Предоставление защищенности местной сети (разделение доступа к сетевым приборам, регулирование удаленного управления сетевыми приборами, установка контроля присоединения новейших приборов, структура VLAN).

2. Предприятие безопасного подсоединения к сети интернет (регулирование, зеркалирование трафика в основном коммутаторе, установка списков допуска к местным и отдаленным ресурсам, осуществление VPN-объединения Standard Cisco IPSec среди удаленных представительств, регулирование PAT). [2]

3. Контроль функционирования и безопасности сети. Разделение доступа к сетевым приборам рассматривается так же, как важный критерий, который сдерживает доступ к изменению опций сетевого оборудования и является неотъемлемым критерием для соседнего сетевого оснащения. Для правильного применения сетевых приборов и распределения обязательств необходимо внедрить преимущественный допуск к приборам:

• пользователь никак не способен осуществлять модификации и оценивать файлы конфигурации;

• агент поддержки в свою очередь обладает возможностями пользователя и допуском к инструкции ping;

• помощник администратора обладает способностью агента поддержки и правом

перезагрузки оснащения;

• администратор обладает полным допуском к конфигурации приборов;

• подключение согласно протоколу telnet (регулирование удаленного доступа) весьма рискованно, потому что транслирует пароли по сети в открытом варианте; с целью защиты секретного трафика применяется акт SSH. [1]

Контролирование прибавления приборов. Реализуется за счет опции защищенности портов в коммутаторах допуска. Каждому интерфейсу коммутатора устанавливается в соответствие MAC-код допустимого для данного интерфейса сетевого адаптера. Это разрешение в свою очередь может уберечь местную сеть от атак вида «отказ в обслуживании», реализующиеся с поддержкой переполнения таблицы MAC-адресов.

Структура VLAN. Каждое отделение привязано к собственному коммутатору доступа и располагается в своей VPN, интерфейсы сведений коммутаторов соединяются с номером данной виртуальной сети. Интерфейсы коммутаторов, которые обязаны транслировать трафик многих VPN, классифицируются как trunk-интерфейсы; в соседнем маршрутизаторе отделяется некоторое количество подинтерфейсов для каждого VLAN.

Зеркалирование трафика в основном коммутаторе. Применяется с целью контролирования, прибывающего из интернета трафика при поддержке IDS либо анализатора трафика, который определен в рабочей станции, регулируемой системным администратором. С применением зеркалирования исполняется маскировка контролирования трафика в интересах простых пользователей интернета и злоумышленников. [2]

Регулирование списков доступа ACL. Главными считаются перечни доступа к единым ресурсам сети – серверам. Эти перечни частично осуществляют функции межсетевого экрана, потому что могут выбирать трафик согласно адресу направления, ключа, виду протокола.

Из-За того, что управление адресов исполняется в соседном маршрутизаторе, проблемой для списков допуска к серверам считается поверка возможных для применения портов.

Осуществление VPN-объединения среди удаленными представительствами. Регулирование соседних маршрутизаторов характеризуется способом обмена ключами (ISAK.MP), схемой кодирования (AES), методом хеширования (SHA-1), способом аутентификации (взаимообмен ключами при формировании подсоединения), взаимообмен ключами способом Диффи-Хеллмана второй категории (1024 бита).

Регулирование PAT усугубляется применением технологических процессов VPN с целью верной конфигурации, которой требуется исключение из транслирования трафика среди удаленными представительствами, потому как акт IPSec ранее изготавливает передачу ради подтвержденного в его перечнях допуска трафика. [3]

Контроль работоспособности, а также безопасности сети, реализованной при поддержке предложенного метода, выполняется постепенно. Первоначальным шагом считается контроль работоспособности и безопасности сетевого оснащения местной сети. Следующим шагом является контроль работоспособности и безопасности допуска в сеть интернет и взаимодействия с удаленными представительствами.

Итак, в следствии использования предложенного нами метода регулирования VPN имеют все шансы быть протестированы на правильность и соответствие условиям безопасности. Смоделированная оберегаемая коллективная сеть может препятствовать главным угрозам защищенности и применима на практике.

Заключение. В этой статье была изучена методика функционирования VPN. В согласовании с презентованной систематизацией нами были выделены постановления, реализуемые в канальной, сетевой и сеансовой

степенях модификации OSI. С Целью фактического осуществления было подобрано решение на базе протокола IPSec из-за его обширной распространенности также стандартизированности. Кроме Того существовали исследованы вспомогательные ресурсы предоставления защищенности коллективной сети. Было проведено исследование стека протоколов IPSec, пересмотрены его главные элементы: AH, ESP, IKE. Выделены шаги определения объединения при компании туннеля и проведен анализ этого стека протоколов. Было сформировано заключение о согласовании применения стека протоколов IPSec с целью компании безопасного подсоединения к сети интернет распределенной коллективной сети.

В процессе изучения были исследованы виды компании VPN-сочетаний на базе оснащения Cisco. Были проанализированы пять заключений: DMNVPN, Easy VPN, GRE-based VPN, GET-VPN, standard IPSec, выделены достоинства, недочеты и установлен диапазон использования любого из них. В базе изучения для осуществления был подобран standard IPSec, основным превосходством которого считается его мультивендорность. Но для случая, когда число удаленных представительств обширно, взамен standard IPSec рекомендовано применение DMNVPN либо Easy VPN.

Был сконструирован метод для компании безопасного подсоединения распределенной коллективной сети к интернету средствами оборудования фирмы Cisco. Он содержит этапы по обеспечению защищенности сетевого оснащения, внутренних ресурсов сети фирмы, компании не опасного взаимодействия среди удаленными представительствами и управление доступом в сети интернет. С Целью осуществления метода была смоделирована стандартная распределенная коллективная сеть, содержащая главный офис и ряд удаленных представительств. Реализация метода была сделана в служебной сфере прогнозирования Cisco Packet Tracer. Охрана сети

была испытана на функциональность, по итогам которой было сформировано заключение о том, что созданный метод может использоваться с целью предоставления не опасного подсоединения к интернету распределенной коллективной сети небольшого либо посредственного коммерциала. [4]

Список используемой литературы:

1. С.К. Калашников История «болезней» VPN // Журнал сетевых решений, 2013г.
2. Ю.А. Семенов, Алгоритмы телекоммуникационных сетей. В 3 частях. Часть 3. Процедуры, диагностика, безопасность / Ю.А. Семенов - М.: БИНОМ. Лаборатория знаний, 2007г.
3. В.Г. Олифер, Н.А. Олифер. Безопасность компьютерных сетей, 2017г.
4. Лэммл Т. CCNA Cisco Certified Network Associate. Учебное руководство: учебное пособие. - 2-е изд., перераб. и доп. – М.: ЛОРИ, 2002г.