УДК 004.7

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)

ТЕХНОЛОГИИ СОЗДАНИЯ ВИРТУАЛЬНЫХ ЧАСТНЫХ СЕТЕЙ.

Аннотация: Рассматриваются технологические процессы формирования виртуальных индивидуальных сетей трёх основных типов: внутренних, удалённого доступа, а также типа, условно именуемого «точка — точка». Приводится систематизирование программных и аппаратных средств концепции VPN. Описываются характерные черты операций авторизации и аутентификации в протоколе IPSe.

Ключевые слова: Виртуальные частные сети, туннелирование, шифрование, инкапсуляция, IPSec.

Technologies for creating virtual private networks.

Annotation: Technological processes of forming virtual separate networks of three main types are considered: internal, remote access, as well as the type conventionally referred to as point-to-point. The systematization of software and hardware of the VPN concept is given. The characteristic features of authorization and authentication operations in the IPSe protocol are described.

Keywords: Virtual private networks, tunneling, encryption, encapsulation, IPSec.

Большинству компаний в наше время приходится иметь дело с массовыми рынками логистики, что формирует конкретные условия: защищенность, безопасность и мгновенная связь должны быть гарантированы вне зависимости от того, в каком месте находятся офисы.

Информация, передаваемая посредством Сети Интернет, значительно больше уязвима, нежели сведения, переданные согласно внутренней сети компании. Удовлетворить потребность потребителя в безопасной связи

допустимо с поддержкой подсоединения к удаленным сетям согласно назначенным линиям, но данный подход решения задачи связан со значительными экономическими расходами. Улучшить инвестиции возможно, основав виртуальные частные сети (Virtual Private Network — VPN).

Основная часть. VPN — данные искусственного происхождения сети, какие применяют сеть интернет в качестве сферы передачи с протоколом туннелирования, обеспечивают конфиденциальность, гарантируют аутентификацию, но кроме того обеспечивают, что приобретенные сведения постоянно отвечают отправленной.

Иными словами, VPN — это сетевая разработка, которая гарантирует безопасное увеличение локальной сети с помощью публичной сети (такого рода, как сеть интернет), с поддержкой инкапсуляции, кодирования пакетов сведений в разных удаленных пунктах, общественной инфраструктуры передачи сведений. Это предоставляет возможность пользователю отсылать и получать сведения согласно единым либо общественным сетям, также, как через личную сеть. [1]

VPN делает отличное недорогое предложение с целью осуществлении междугородной сети на базе сети интернет также гарантирует аутентификацию пользователей либо компьютеров с поддержкой зашифрованных числовых подписей, либо паролей с целью конкретной идентификации. Кроме Того VPN гарантирует, что сведения, передаваемые отправителем, являются теми же, что были получены. Секретность при передаче сведений гарантируется с помощью кодирования.

Для осуществления такого рода сети следует обладать конкретными причинами, такими как стратегия защищенности с целью кодирования сведений (они никак не должны быть видны сторонним покупателям в сети); руководство ключами, для того чтобы гарантировать шифрование среди покупателями и сервером; взаимообмен сведениями, приложениями также

ресурсами; компьютер допуска и аутентификации с целью управления сетью; доказательство личности и статистический учет допуска; разрешение вопросов управления.

Поэтому VPN обязан определить местоположение для покупателя в пределах индивидуальной сети, гарантировать его сохранение и помощь некоторых протоколов, в таком случае сеть должна подвергать обработке единые протоколы к сети интернет, в частности IP. [2]

Существуют три ключевых вида VPN:

- Во-первых, VPN удаленного доступа, который складывается из покупателей, которые подсоединяются к фирме с удаленных девайсов, использующих сеть интернет в качестве канала доступа. После аутентификации они имеют положение, подобное тому, что нужно в локальной сети.
- Во-вторых, VPN вида «точка — точка». Данная модель применяется с целью подсоединения удаленных офисов к основной штаб-квартире. Сервер VPN регулярно подключен к сети интернет, берет на себя входящие соединения с веб-сайтов также формирует VPN-тоннель. Серверы подсоединены из удаленных офисов к Сети Интернет, а через него к VPN-туннелю в центральном офисе. Он применяется с целью ликвидации классических туннелей вида «точка — точка».
- В-третьих, внутренний VPN (over LAN). Он функционирует как обыкновенный VPN, в случае если располагается в той же локальной сети, но никак не в сети интернет также предназначается для выделения сфер и услуг внутренней сети, кроме того, с целью увеличения защищенности в беспроводный сети Wi-Fi.

Из Числа большого колличества протоколов, общедоступных для применения в VPN, обычным считается IPSec, однако поддерживаются и прочие протоколы, такие как PPTP, L2F, SSL/TLS, SSH и т. д. [3]

IPSec предполагает собою комплект стандартов защищенности для протокола IP и функционирует на сетевом уровне, снабжая охрану и аутентификацию IP-пакетов среди компьютеров в сети. Он гарантирует секретность, целостность и аутентификацию с поддержкой алгоритмов кодирования, хэширования, открытых ключей и числовых сертификатов. IPSec заключается в трех ключевых частях, двух протоколах защищенности, подобных IP-заголовку аутентификации (AH) и Encapsulated Security Payload (ESP) и одного ключа защищенности Internet Key Exchange (IKE).

В протоколе AH доля сведений протекает через алгоритм хеширования с источником аутентификации заголовка также прибавляется в качестве заголовка к пакету IPSec; целевые сведения вычисляют подобным методом, с поддержкой хэш-ключа, также, в случае если они одинаковы сведениям в заголовке AH, комплект проходит контроль подлинности.

Протокол ESP имеет подобную процедуру, главное его отличие от AH в этом, что информация шифруется с поддержкой шифровального хода с поддержкой ESP-ключа, таким образом может быть дешифровано только лишь получателем, которому известен ключ.

Протокол IKE обладает двумя режимами: тоннельным и передачей сведений. В порядке передачи содержание дейтаграммы в пределах AH либо ESP принадлежит к степени передачи, по этой причине заголовок IPSec пишется уже после заголовка IP и пред теми сведениями, которые обязаны являться защищенными. Он гарантирует взаимосвязь вида «точка — точка». В туннельном порядке, наоборот, применяются абсолютные IP-дейтаграммы, в том числе первоначальный заглавие IP. К IP-дейтаграмме прикрепляется AH либо ESP заглавие, но потом еще один заголовок IP с целью направления пакетов посредством сети. IKE считается обычным протоколом с целью настройки VPN.

Подобно, в рамках осуществлении имеется две крупные категории способов, которые базируются на аппаратных средствах и программном

обеспечении. Аппаратные ресурсы применяют конфигурации на уровне маршрутизаторов либо брандмауэров с целью удаленного подсоединения к виртуальной индивидуальной сети, а программное обеспечение применяет план либо комплект проектов в окончательном узле, для того чтобы подсоединиться к сети VPN.

Есть три метода осуществления подсоединения к VPN:

- Во-первых, подсоединение удаленного доступа, которое выполняется заказчиком либо пользователем посредством компьютера к индивидуальной сети.
- Второй вид — это маршрутизатор, который подключается к индивидуальной сети.
- Третий вид — это подсоединение брандмауэра к брандмауэру, в котором ресурс подключен к виртуальной индивидуальной сети. В данном виде взаимосвязи пакеты зачисляются с каждого пользователя сети интернет. Брандмауэр, который осуществляет соединение, осуществляет контроль подлинности ответчика и наоборот. [4]

Заключение. Так как конфигурации VPN легкодоступны на маршрутизаторах, межсетевых экранах также в самих операционных концепциях, они являются, с данной точки зрения, элементарными. Следует совершить их доступными для конечных пользователей, что даст возможность гарантировать результативное и элементарное применение сведений технологий обширным диапазоном экспертов в компьютерных сетях. Большое число протоколов и альтернатив усложняют процедуру настройки, однако именно это и гарантирует вероятность применения VPN в просторном диапазоне девайсов.

Список используемой литературы:

1. М.А Захватов, Построение виртуальных частных сетей (VPN) на базе технологии MPLS / М. А. Захватов. — Москва: изд-во Cisco Systems, 2001г.
2. Браун, С. Виртуальные частные сети / С. Браун. — Москва: изд-во «Лори», 2001г.
3. Олег Коленсников, Брайан Хетч, Linux. Создание виртуальных частных сетей (VPN), 2004г.
4. С.В. Запечников, Н.Г. Милославская, А.И. Толстой, Основы построения виртуальных частных сетей, 2011г.