УДК 004.7

ТЕХНОЛОГИИ СОЗДАНИЯ ВИРТУАЛЬНЫХ ЧАСТНЫХ СЕТЕЙ

Хесус Назарет Бенитес Гонсалес
Донской государственный технический университет, Ростов-на-Дону, Российская Федерация

ing.jnb@gmail.com

Рассматриваются технологии создания виртуальных частных сетей трёх основных типов: внутренних, удалённого доступа и типа, условно называемого «точка — точка». Приводится классификация программных и аппаратных средств построения *VPN*. Описываются особенности процедур авторизации и аутентификации в протоколе *IPSec*.

Ключевые слова: виртуальные частные сети, туннелирование, шифрование, инкапсуляция, *IPSec*

UDC 004.7

VIRTUAL PRIVATE NETWORKS DESIGN TECHNOLOGIES

Jesús Nazareth Benitez González
Don State Technical University, Rostov-on-Don, Russian Federation

ing.jnb@gmail.com

The article deals with the design technologies of virtual private networks of three main types: internal, remote access and point-to-point. The paper provides the classification of software and hardware *VPN* creation. It contains the features of the authorization and authentication procedures to the *IPSec* protocol.

Keywords: virtual private networks, tunneling, encryption, encapsulation, *IPSec*

Введение. Многим компаниям в настоящее время приходится иметь дело с глобальными рынками логистики, что создаёт определенные требования: безопасность, надежность и быстрая связь должны быть обеспечены независимо от того, где расположены офисы.

Данные, передаваемые через Интернет, гораздо более уязвимы, чем данные, переданные по внутренней сети организации. Удовлетворить потребность потребителя в безопасной связи возможно с помощью подключения к удаленным сетям по выделенным линиям, однако этот путь решения проблемы связан с высокими финансовыми затратами. Оптимизировать вложения можно, создав виртуальные частные сети (*Virtual Private Network — VPN*).

Основная часть. *VPN* — это искусственные сети, которые используют интернет в качестве среды передачи с протоколом туннелирования, гарантируют конфиденциальность, обеспечивают аутентификацию, а также гарантируют, что полученная информация всегда соответствует отправленной [1]. Другими словами, *VPN* — это сетевая технология, которая обеспечивает безопасное расширение локальной сети посредством публичной сети (такой, как интернет), с помощью инкапсуляции, шифрования пакетов данных в различных удаленных точках, публичной инфраструктуры передачи данных. Это дает возможность пользователю отправлять и получать данные по общим или общественным сетям, так же, как через частную сеть.

VPN предлагает недорогое решение для реализации междугородной сети на основе интернета и обеспечивает аутентификацию пользователей или компьютеров с помощью зашифрованных цифровых подписей или паролей для однозначной идентификации. Также *VPN* гарантирует, что данные, передаваемые отправителем, являются теми же, что были получены. Конфиденциальность при передаче данных обеспечивается посредством шифрования.

Для реализации такой сети необходимо иметь определенные основания, такие как политика безопасности для шифрования данных (они не должны быть видны посторонним клиентам в сети); управление ключами, чтобы обеспечить кодирование между клиентами и сервером; обмен данны-

ми, приложениями и ресурсами; сервер доступа и аутентификации для управления сетью; подтверждение личности и статистический учет доступа; решение проблем управления. Таким образом, *VPN* должен установить адрес для клиента в пределах частной сети, обеспечить его сохранение и поддержку нескольких протоколов, то есть сеть должна обрабатывать общие протоколы к сети интернет, в частности *IP*.

Существуют три основных типа *VPN* [2]. Во-первых, *VPN* удаленного доступа, который состоит из клиентов, которые подключаются к компании с удаленных устройств, использующих интернет в качестве канала доступа. После аутентификации они имеют статус, аналогичный тому, который необходим в локальной сети.

Во-вторых, *VPN* типа «точка — точка». Эта схема используется для подключения удаленных офисов к центральной штаб-квартире. Сервер *VPN* постоянно подключен к интернету, принимает входящие соединения с сайтов и создает *VPN*-туннель. Серверы подключены из удаленных офисов к Интернету, а через него к *VPN*-туннелю в центральном офисе. Он используется для устранения традиционных туннелей типа «точка — точка».

В-третьих, внутренний *VPN* (*over LAN*). Он работает как обычный *VPN*, если находится в той же локальной сети, а не в сети интернет и служит для выделения областей и услуг внутренней сети, а также для повышения безопасности в беспроводной сети *Wi-Fi*.

Среди множества протоколов, доступных для использования в *VPN*, стандартным является *IPSec*, но поддерживаются и другие протоколы, такие как *PPTP, L2F, SSL/TLS, SSH* и т. д.

IPSec представляет собой набор стандартов безопасности для протокола *IP* и действует на сетевом уровне, обеспечивая защиту и аутентификацию *IP*-пакетов между компьютерами в сети [3]. Он обеспечивает конфиденциальность, целостность и аутентификацию с помощью алгоритмов шифрования, хэширования, открытых ключей и цифровых сертификатов. *IPSec* состоит из трех основных компонентов, двух протоколов безопасности, таких как *IP*-заголовок аутентификации (*AH*) и *Encapsulated Security Payload* (*ESP*) и одного ключа безопасности *Internet Key Exchange* (*IKE*) [4].

В протоколе *AH* часть данных проходит через алгоритм хеширования с ключом аутентификации заголовка и добавляется в качестве заголовка к пакету *IPSec*; целевые данные вычисляют таким же способом, с помощью хэш-ключа, и, если они равны данным в заголовке *AH*, пакет проходит проверку подлинности.

Протокол *ESP* имеет аналогичную операцию, основное его отличие от *AH* в том, что сообщение шифруется с помощью криптографического процесса с помощью *ESP*-ключа, так что может быть расшифровано только получателем, которому известен ключ.

Протокол *IKE* имеет два режима: туннельный и передачи данных. В режиме передачи содержание дейтаграммы в пределах *AH* или *ESP* относится к уровню передачи, поэтому заголовок *IPSec* пишется после заголовка *IP* и перед теми данными, которые должны быть защищены. Он обеспечивает связь типа «точка — точка». В туннельном режиме, напротив, используются полные *IP*-дейтаграммы, включая исходный заголовок *IP*. К *IP*-дейтаграмме прикрепляется *AH* или *ESP* заголовок, а затем еще один заголовок *IP* для направления пакетов через сеть. *IKE* является стандартным протоколом для настройки *VPN*.

Аналогично, в рамках реализации есть две большие группы методов, которые основываются на аппаратных средствах и программном обеспечении. Аппаратные средства используют конфигурации на уровне маршрутизаторов или брандмауэров для удаленного подключения к вирту-

альной частной сети, а программное обеспечение использует программу или набор программ в конечном узле, чтобы подключиться к сети *VPN*.

Существуют три способа реализации подключения к *VPN*. Во-первых, подключение удаленного доступа, которое производится заказчиком или пользователем через компьютер к частной сети. Второй тип — это маршрутизатор, который подключается к частной сети; третий тип — это подключение брандмауэра к брандмауэру, в котором источник подключен к виртуальной частной сети. В этом типе связи пакеты поступают от любого пользователя сети интернет. Брандмауэр, который реализует соединение, выполняет проверку подлинности ответчика и наоборот.

Заключение. Поскольку конфигурации *VPN* доступны на маршрутизаторах, межсетевых экранах и в самих операционных системах, они являются, с данной точки зрения, простыми. Необходимо сделать их доступными для конечных пользователей, что позволит обеспечить эффективное и простое использование данных технологий широким кругом специалистов в компьютерных сетях. Множество протоколов и вариантов усложняют процесс настройки, но именно это и обеспечивает возможность использования *VPN* на широком спектре устройств.

Библиографический список.

1. Захватов, М. А. Построение виртуальных частных сетей (*VPN*) на базе технологии *MPLS* / М. А. Захватов. — Москва : изд-во Cisco Systems, 2001. — 52 с.
2. Браун, С. Виртуальные частные сети / С. Браун. — Москва : изд-во «Лори», 2001. — 504 с.
3. Xenakis, C. DINÁMICO NETWORT basados en VPN segura DESPLIEGUE EN GPRS / C. Xenakis, L. Merakos, 2002. — 240 с.
4. Amato, V. Programa Cisco Networking Academy. Guía del Año imprimación / Vito Amato. — Cisco System editorial, 2003. — 382 с.