Технические науки

УДК 65

ОСНОВЫ И ОБЕСПЕЧЕНИЕ ЗАЩИТА ИНФОРМАЦИИ В ГЛОБАЛЬНЫХ СЕТЯХ И В СЕТИ ИНТЕРНЕТ[4]

С.С. Мухлисов, Н.Н. Зарипов, Бухарский государственный университет
(Бухара, Узбекистан)

Аннотация. В настоящей работе рассматриваются различные подходы по организации основы и обеспечение защита информации в глобальных сетях и в сети интернет. Выбран наиболее оптимальный вариант организации проведения специализированных дисциплин с точки зрения минимальных затрат временных и материальных ресурсов. В статье речь идет об использование информации в интернете и обеспечение их защит. А также эффективности защита информации в глобальных сетях.

Ключевые слова: Информационная безопасность, Интернет, защита информации, глобальные сети.

Основной проблемой Интернета как канала передачи информации является возможность атаки “maninthemiddle”. Злоумышленник подключается к линии между клиентом и сервером и подменяет передающуюся информацию. Возможны совершенно разные варианты этой атаки. Например, злоумышленник может "прикидываться" сервером и вводить клиента в заблуждение с целью извлечь выгоду из обмана. Следует отметить, что наиболее легко эту атаку может реализовать Интернет-провайдер. С целью обеспечения безопасного обмена разработаны различные протоколы защиты и созданы программные продукты, реализующие данные протоколы. Во всех подобных протоколах используются методы криптографии. Именно криптография позволяет:

- провести строгую аутентификацию сервера
- провести строгую аутентификацию клиента
- обеспечить шифрование данных, которыми обмениваются клиент и сервер.

Эти меры позволяют успешно противостоять атаке "maninthemiddle".

Защита на различных уровнях модели OSI

Наиболее распространенной моделью представления стека сетевых протоколов является модель OSI. Упрощенная модель OSI представлена на рисунке.

Что такое защита информации на каком-либо уровне модели OSI? Каждый последующий уровень сетевых пакетов инкапсулирован в предыдущем. То есть данные протокола прикладного уровня (например, HTTP) находится внутри пакета транспортного уровня (например, TCP), который находится внутри пакета сетевого уровня (например, IP), который находится внутри кадра канального уровня (например, кадра Ethernet).

[4] Статья представлена советником главного редактора и иностранным координатором в Узбекистане М.М. Бафаевым (Бухара, Узбекистан).

При защите информации на сетевом уровне шифруется содержимое пакета IP, то есть пакет TCP. В другом варианте защиты на сетевом уровне шифруется целый пакет IP и данный зашифрованный пакет в свою очередь инкапсулируется. Такая дополнительная инкапсуляция позволяет скрыть топологию сетей участников обмена.

Следует отметить, что защита, например, на канальном уровне обеспечивает абсолютно "прозрачное" использование сетевого уровня.

Канальный уровень

Одним из программных продуктов, реализующих защиту на канальном уровне, является OpenVPN (**www.openvpn.net**). Данный продукт позволяет организовать закрытую сеть на базе Интернет. При подключении к такой сети клиент проходит процедуру строгой криптографической аутентификации по цифровому сертификату, что обеспечивает защиту от несанкционированного доступа к ресурсам сети. Кроме того, обеспечивается шифрование сетевого трафика при работе в сети. OpenVPN поддерживает режимы работы "мост" и "маршрутизатор". При работе в режиме "мост" происходит шифрование и инкапсуляция кадров Ethernet. Следует отметить, что если шифрование обеспечивает защиту от доступа к передаваемой информации, то из-за инкапсуляции злоумышленник не сможет выяснить адресата передаваемой информации.

Рассмотрим задачи, которые возможно решить с помощью OpenVPN в режиме "мост".

Подключение удаленного сотрудника к корпоративной ЛВС (VPN-шлюз)

Решение данной задачи предполагает использование серверной части OpenVPN в качестве дополнительного шлюза в ЛВС организации. Сегмент ЛВС, доступный через VPN-шлюз, обычно называют доменом шифрования. Рабочие места и сервера, входящие в домен шифрования, не подключаются к VPN. При подключении к серверу OpenVPN клиент получает прозрачный доступ ко всем машинам, находящимся в домене шифрования. Получат ли подобный доступ к машине клиента машины из домена шифрования, зависит от настроек сервера OpenVPN.

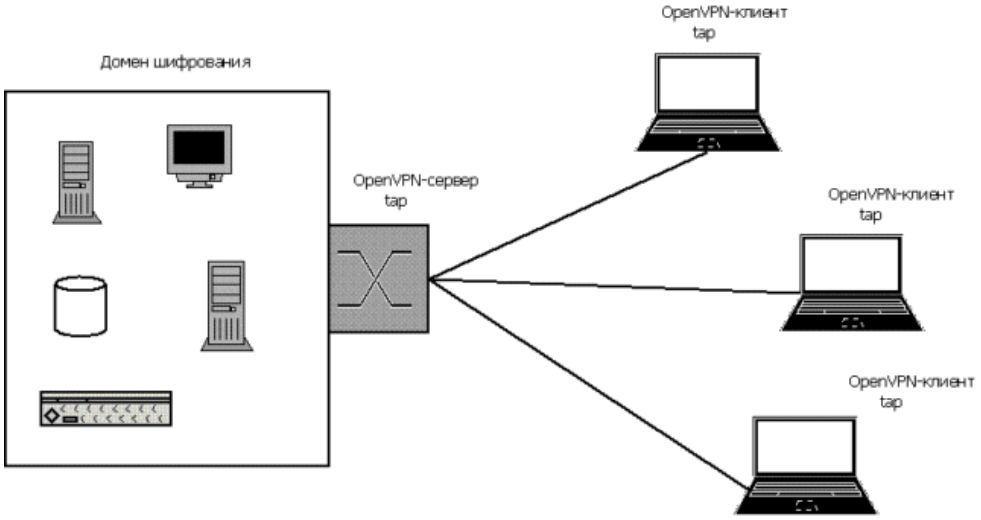

Рис.1

Объединение ЛВС филиалов организации в единую сеть

Другой задачей, которую можно решить с помощью OpenVPN, является объединение ЛВС филиалов организации в единую сеть через Интернет. В этом случае сервера OpenVPN устанавливается в качестве дополнительных шлюзов в свои ЛВС, а затем соединяются между собой.

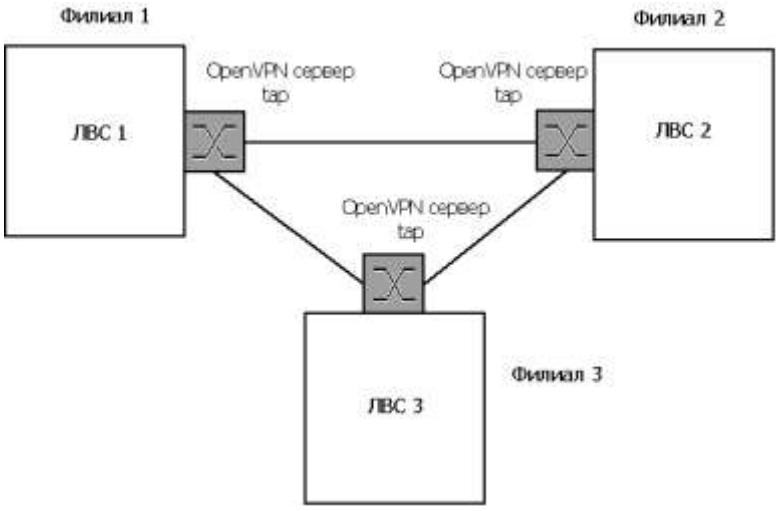

Рис.2

Объединение сегментов ЛВС нескольких организаций в единую сеть для ведения совместного проекта (межкорпоративный портал)

Основной проблемой при создании межкорпоративного портала является логическое разделение сети организации на два сегмента, один из которых предоставляет свой ресурс организациям парнерам, а другой закрыт для них. Для решения данной проблемы одна из организаций разворачивает на внешем адресе сервер OpenVPN. На все рабочие места и сервера, участвующие в портале, устанавливается клиент OpenVPN, и эти машины подключаются к серверу.

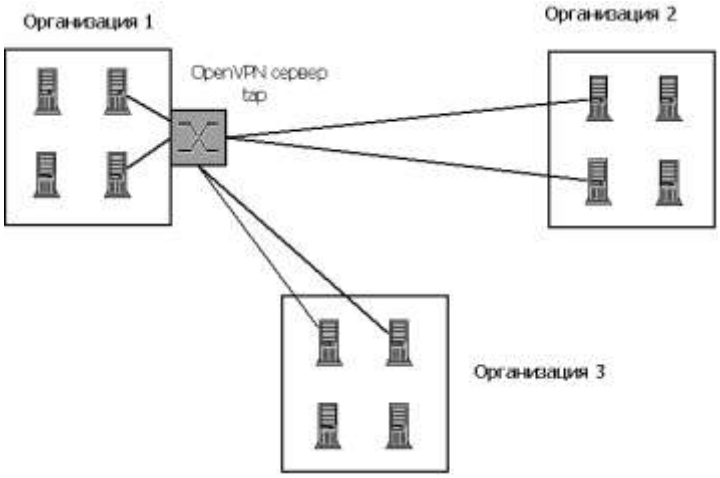

Рис.3

Подключение к ЛВС удаленных пользователей с низким уровнем доверия

Решение данной задачи требуется 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.

Создание нескольких логических сетей в одной физической сети

Решение данной задачи требуется, например, когда надо разделить трафик между внутренними департаментами организации, которые обращаются к серверам из одного физического сегмента. Особенность данного варианта в том, что VPN строится между узлами, находящимися, как правило, в одном сегменте сети, например, между рабочей станцией и сервером. Этот вариант похож на технологию VLAN, но вместо разделения трафика, используется его шифрование.

Анонимный серфинг

Под серфингом понимаются любые действия пользователя в Интернет. При этом интернет-провайдеру данного пользователя становятся известны web-сайты, на которые ходил пользователь; адресаты писем пользователя и т.п. Использование OpenVPN в качестве дополнительного "логического" шлюза в интернет, установленного на территории организации, в которой работает пользователь, обеспечивает анонимность серфинга.

Доступ к серверу, не имеющему внешнего адреса (экономия внешних адресов)

Сетевой уровень

OpenVPN в режиме "маршрутизатор" обеспечивает защиту информации на сетевом уровне. При этом так же происходит строгая атуентификация участников обмена по цифровому сертификату, но шифруются и инкапсулируются IP-пакеты, а не кадры Ethernet. Спектр задач, которые можно решить таким способом, в общем, не отличается от спектра задач, решаемых с помощью OpenVPN в режиме "мост". Следует иметь в виду, что режим

"маршрутизатор" является более производительным, чем режим "мост", но имеет и свои недостатки. В частности, не поддерживаются:

- сетевые протоколы, отличные от IP
- широковещательные запросы.

Транспортный уровень

Транспортные соединения используются для доступа к конкретному сетевому сервису, например web-сайту, терминальному серверу, почтовому серверу, серверу базы данных и т.п. Логические "концы" соединения называются портами.

Защита соединений на транспортном уровне (TCP-соединений) осуществляется по протоколу SSL/TLS. После установки транспортного соединения клиент инициирует процедуру "рукопожатия" с сервером. В результате этой процедуры происходит аутентификация сервера и клиента по цифровому сертификату, стороны договариваются об используемых алгоритмах шифрования – шифрсьютах. Шифрсьюты специальным образом "привязываются" к портам защищаемого соединения. Благодаря этому, все данные, попадающие в настроенный таким образом транспортный канал, шифруются отправителем и расшифровываются адресатом.

Для реализации защиты транспортного соединения приложение, осуществляющее обмен, должно использовать криптографическую библиотеку, реализующую SSL/TLS.

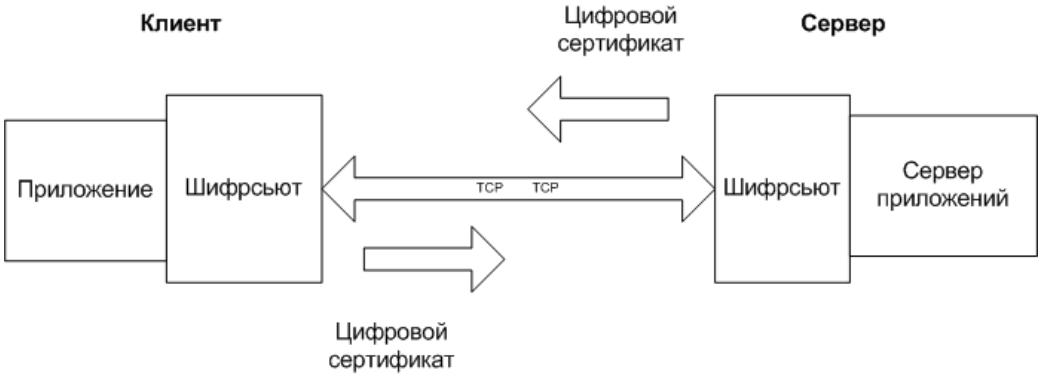

Рис.4

Часто бывает, что приложение было написано без защиты, или же используемые им шифрсьюты не удовлетворяют требованиям к безопасности. Например, все web-браузеры и web-сервера используют для защиты шифрсьюты, реализованные по импортным алгоритмам, а в РФ ФСБ требует в ряде случаев использовать шифрсьюты, реализованные по ГОСТ.

Для решения указанной проблемы модуль обеспечения безопасности канала следует отделить от приложения. Существенным плюсом данной схемы является то, что сами приложения не приходится модифицировать.

Именно такую схему можно реализовать с помощью продуктов **МагПроКриптоТуннель** (клиентская часть) и **МагПроКриптоСервер** (серверная часть).

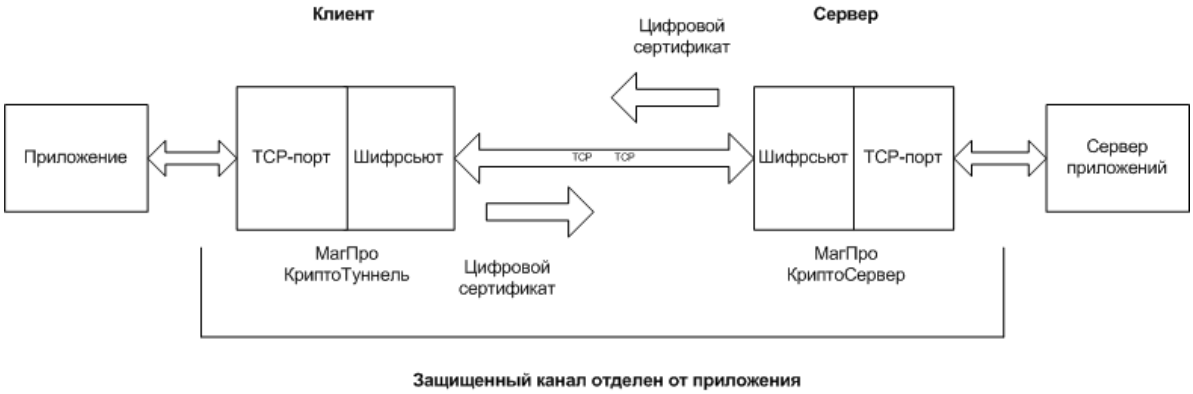

Рис.5

Использование этих продуктов позволяет обеспечить защиту практически любых прикладных протоколов и приложений, как-то:

- доступ к web-сайту по HTTP
- файловый обмен по WebDAV
- терминальный доступ по RDP (RemoteDesktop)
- электронная почта (SMTP, POP3, IMAP)
- доступ к базе данных по SQL
- общие папки по NFS
- произвольный обмен по TCP-соединению (без динамического открытия портов).

Литература:

1. Арестова О.Н., Бабанин Л.Н., Войскунский А.Е. Коммуникация в компьютерных сетях: психологические детерминанты и последствия // Вестник МГУ. Серия XIV. Психология. 2008. №4. С. 65-84.

2. Арестова О.Н., Бабанин Л.Н., Войскунский А.Е. Мотивация пользователей Интернет // Гуманитарные исследования в Интернете / Под ред. А.Е. Войскунского – М.: «Можайск-Терра», 2010. – 146 с.

3. Атепалихин М. С., Социальные сети в Интернет как средство массовой коммуникации // Всероссийский научно-практический семинар «Теория и практика межкультурной коммуникации. Массовая культура и массовые коммуникации»: (январь 2010 г.).

4. Олифер В. Г. Олифер Н. А. Компьютерные сети. Принципы, технологии, протоколы: Учебное пособие для вузов. 4-е изд. – СПб.: Питер, 2010. – 944 с.

5. Янг К.С. Диагноз – интернет-зависимость // Мир Интернет. 2008. №2. С. 202-211.

6. Internet World Stats. Usage and Population Statistics. – URL: http://www.internetworldstats.com/stats4.htm#europe

Muhlisov S.S., Zaripov N.N. Osnovy i obespechenie zashhita informacii v global'nyh setjah i v seti Internet // Nauka. Mysl'. - № 1-2. – 2016.

– ● –

Abstract. In the article the different approaches to the organization and for ensuring the protection of information in global networks and the Internet are examined. The authors select the best option of organization of specialized disciplines in terms of the minimum amount of time and material resources. The article focuses on the use of information in the Internet and the providing their protection. The effectiveness of information security in global networks is discussed.

Keywords: information safety, Internet, information security, global network.

.– ● –

Сведения об авторе

С.С. **Мухлисов** - преподаватель кафедры «Информационные технологии» Бухарского государственного университета (Бухара, Узбекистан).

Н.Н. **Зарипов** - преподаватель кафедры «Информационные технологии» Бухарского государственного университета (Бухара, Узбекистан).

– ● –

Подписано в печать 30.01.2016.