Инженерный вестник Дона, №1 (2019)
ivdon.ru/ru/magazine/archive/n1y2019/5643

Особенности реализации виртуальных туннелей на основе служебных сетевых протоколов

А.В. Авакьянц, М.Ю. Урубкин, Д.В. Фатхи

Донской Государственный Технический Университет

Аннотация: Статья посвящена актуальной проблеме преодоления ограничений, накладываемых протоколом IP и применяемыми совместно с ним сетевыми технологиями, в частности трансляцией адресов, на структуру компьютерных сетей и доступность отдельных её узлов. В ней предлагается метод построения виртуальных сетевых туннелей на основе принципов стеганографии с использованием служебных сетевых протоколов, кратко описаны недостатки существующих технологий туннелирования.
В работе достаточно подробно изложен предлагаемый метод стеганографической инкапсуляции сетевых пакетов, описаны принципы формирования заголовков пакетов, приведены примеры протоколов для инкапсуляции. Материал статьи изложен последовательно, грамотно и соответствует общепринятым требованиям к научным работам. Представленный подход к решению задачи построения виртуальных туннелей обладает научной новизной и имеет практическую ценность.
Ключевые слова: Инкапсуляция, интернет протоколы, многоуровневые сетевые модели, стеганография, стеганографическая инкапсуляция пакетов, туннелирование.

Введение

Современные сетевые технологии представляют собой сложный набор взаимосвязанных протоколов, интерфейсов и алгоритмов взаимодействия различных устройств, правильное совместное применение которых позволяет решать широкий круг задач по обеспечению информационного обмена. Топологии сетей, сформированные в результате долгого исторического развития путём наслоения различных технологий, отличаются сложностью и разнородностью [1]. В связи с этим актуальной задачей является развитие методов туннелирования, которые позволяют создавать виртуальные соединения, и таким образом формировать логическую топологию сети, независящую от физического соединения её устройств.

1. Модель сетевого взаимодействия

Взаимодействие узлов компьютерной сети принято описывать с помощью многоуровневых моделей, таких как OSI (Open System Interconnection — модель взаимодействия открытых систем), представляющая скорее теоретический интерес, и TCP/IP, повсеместно используемая на практике. [2] Данные модели описывают согласованный набор протоколов, называемый стеком протоколов, совместное применение которых обеспечивает передачу как пользовательских данных, так и служебных сетевые сообщений, необходимых для правильной работы сети.

Важнейшим протоколом стека TCP/IP является протокол IP (Internet Protocol), на котором построено всё взаимодействие как в интернете, так и в локальных сетях. Он был разработан в 1981 году и, как следует из стандарта, [3] не был рассчитан на работу в сетях такого масштаба, который имеет сегодня интернет, и на определённом этапе развития столкнулся со следующими проблемами:

— лавинообразный рост сложности маршрутизации большого числа сетей;

— зависимость адреса от провайдера, сложность массового изменения адресов;

— исчерпание IP-адресов.

Для решения последней проблемы наиболее эффективным, и как следствие наиболее распространённым, средством является трансляция сетевых адресов (NAT — Network Address Translation). Данная технология позволяет заменять адреса большого числа компьютеров в локальной (в терминологии NAT — внутренней) сети на один адрес шлюза во внешней сети, которой, как правило, является интернет. Помимо экономии IP-адресов, использование NAT также приводит к повышению безопасности за счёт

сокрытия инфраструктуры внутренней сети, однако данная технология имеет важный недостаток — внутренняя сеть, находящаяся за устройством NAT, оказывается изолированной от внешних соединений и полностью «невидима» из интернета. Такая ситуация является неприемлемой для территориально распределённых организаций, чьи информационные ресурсы рассредоточены по нескольким внутренним сетям, поэтому для обеспечения связи между ними создают виртуальные частные сети, в основе которых лежат 2 технологии: шифрование и туннелирование.

2. Задача туннелирования

Туннелирование (от англ. tunnelling — «прокладка туннеля») — процесс, в ходе которого создается логическое соединение между двумя конечными точками посредством инкапсуляции различных протоколов. [4] Инкапсуляция — это процесс передачи данных с верхнего уровня приложений вниз по стеку протоколов к физическому уровню. При продвижении пакета данных по уровням сверху вниз каждый новый уровень добавляет к пакету свою служебную информацию в виде соответствующих заголовков.

В процессе инкапсуляции, выполняемой при туннелировании, выделяют следующие типы протоколов [5]:

— транспортируемый протокол, т.е. тот, чьи данные нужно передать через туннель;

— протокол инкапсуляции, который выполняет служебные функции передачи параметров туннеля и обозначение самого факта туннелирования;

— несущий протокол, предназначенный для передачи всей перечисленной выше информации по внешней сети.

От обычных многоуровневых сетевых моделей (таких как OSI или TCP/IP) туннелирование отличается тем, что транспортируемый протокол

относится к тому же или более низкому уровню, чем используемый в качестве туннеля несущий протокол (рис. 1).

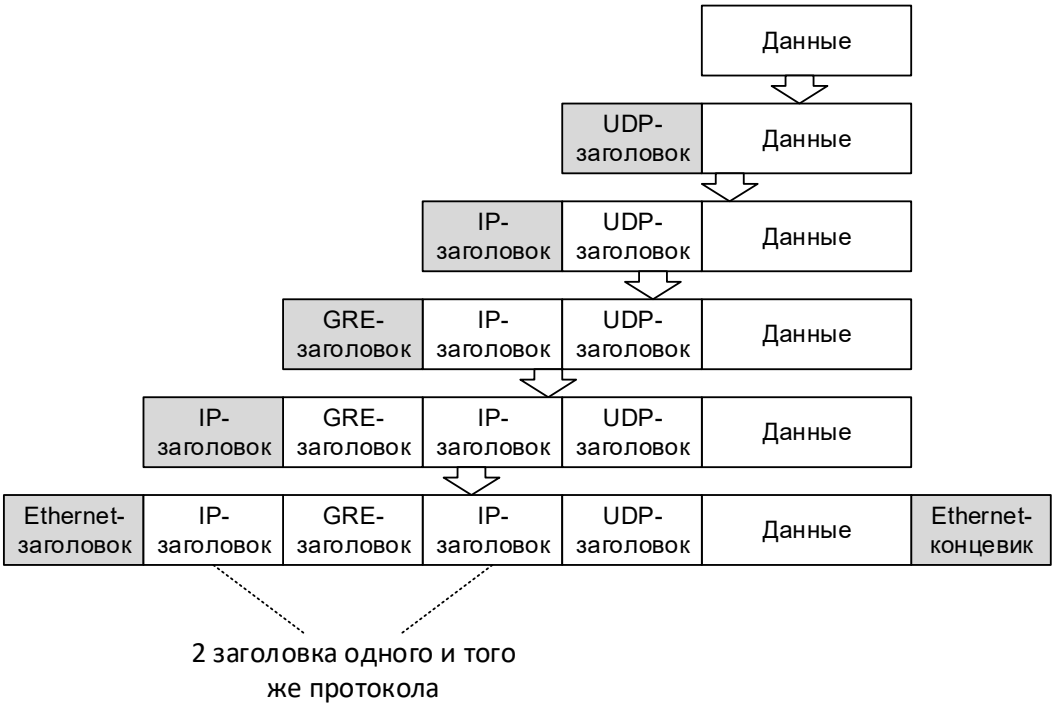

Рис. 1 – Инкапсуляция пакетов при туннелировании.

На рисунке 1 транспортируемыми протоколами являются UDP и IP, протоколом инкапсуляции — GRE, а несущим протоколом, также как и транспортируемым, — IP. Описанный подход является стандартным, вследствие чего легко распознаётся системами анализа трафика, а в случае отсутствия дополнительной защиты поддаётся дальнейшему анализу для извлечения полезной информации. В связи с этим перспективным может оказаться другой подход, основанный на принципах сетевой стеганографии — совокупности методов скрытой передачи данных с использованием особенностей работы сетевых протоколов [6].

3. Служебные сетевые протоколы для стеганографической инкапсуляции

Все сетевые протоколы условно можно разделить на 2 группы: протоколы, предназначенные для передачи полезной нагрузки (как правило пользовательских данных) и служебные протоколы, используемые только для обмена информацией о состоянии сети, её топологии, сопоставления адресов, а также выполняющие большое количество других функций, напрямую не связанных с передачей пользовательских данных, но необходимых для корректной работы сети. К первой группе относятся все протоколы прикладного уровня, а также протоколы TCP, UDP, IP и Ethernet, ко второй — ICMP, ARP, DHCP, DNS, все протоколы маршрутизации и также многие другие менее распространённые протоколы.

Как правило, при настройке систем анализа трафика, для служебных протоколов используют менее строгие правила чем для транспортных, а иногда и вовсе игнорируют их, что связано с экономией вычислительных ресурсов, а также представлением о том, что в служебных протоколах не будет пользовательских данных, представляющих интерес для анализа [7].

Наиболее простым для инкапсуляции туннелированных данных является протокол ICMP, в пакетах которого предусмотрено место для размещения каких-либо данных, напрямую не используемых самим протоколом [8,9].

Другим распространённым служебным протоколом является ARP (Address Resolution Protocol), предназначенный для сопоставления IP и MAC адресов. Его пакеты часто передаются по сети, не имеют чётких признаков, позволяющих отличить реальный пакет от поддельного, и не блокируются средствами защиты сетей. Несмотря на то, что в данном протоколе не предусмотрено отдельное поле для записи данных, можно использовать для

этих целей поля его заголовка, предназначенные для одного из адресов отправителя.

В случае, когда в сети применяется динамическая маршрутизация, пакеты используемого протокола маршрутизации можно применять для транспортировки пользовательских сообщений. Такие пакеты содержат большое количество данных, например, о топологии сети, для протокола ICMP, или об уже имеющихся маршрутах, для протокола RIP. Длина этих данных не ограничена, а их содержимое не может быть проверено промежуточным узлом, осуществляющим анализ трафика, в результате чего возможно добавление в пакет значительных объёмов данных не являющихся маршрутной информацией.

Независимо от выбранного несущего протокола, использование принципов стеганографии для внедрения данных в служебные сетевые пакеты сводится к определению потенциально избыточной информации в структуре пакета, её компрессии и записи в освободившееся место требуемой информации [10]. Данный принцип показан на рисунке 2.

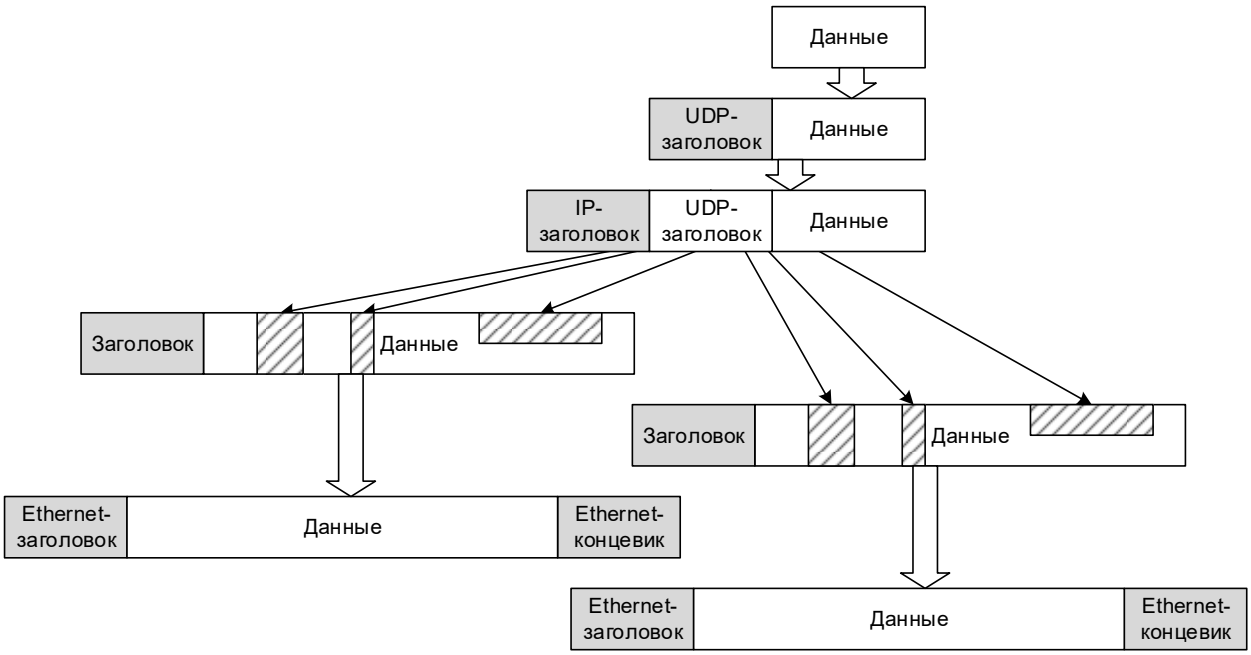

Рис. 2 – Стеганографическая инкапсуляция пакетов.

ЗАКЛЮЧЕНИЕ

Предлагаемый подход к построению виртуальных туннелей с использованием служебных сетевых протоколов позволяет обходить ограничения, налагаемые физической топологией сети, а используемые при этом методы стеганографии обеспечивают определённый уровень конфиденциальности передаваемых сообщений. Широкий набор служебных протоколов позволяет использовать описанные методы в любых сетях, а также разделять передаваемую информацию между несколькими протоколами, повышая общую скорость передачи и усложняя анализ данного трафика.

Литература

1. 1. Таненбаум Э., Уэзеролл Д. Компьютерные сети. 5-е изд. — СПб.: Питер, 2012. — 960 с.

2. Г.В. Бабенко, С.В. Белов Анализ трафика TCP/IP на основе методики допустимого порога и отклонения // Инженерный вестник Дона, 2011, №2 URL: ivdon.ru/ru/magazine/archive/n2y2011/446.

3. RFC 791. Internet protocol, 1981, URL: tools.ietf.org/html/rfc791.

4. Галушка В.В. Сети и системы передачи информации: учебное пособие // Ростов н/Д: Издательский центр ДГТУ, 2016. — 105 с.

5. Ibrahim, L., 2017. Virtual Private Network (VPN) Management and IPSec Tunneling Technology. Middle East Comprehensive Journal for Education and Science Publications (MECSJ), 1: pp.76-87.

6. Mazurczyk, W., S. Wendzel, S. Zander, A. Houmansadr and K. Szczypiorski, 2016. Information hiding in communication networks: fundamentals, mechanisms, applications, and countermeasures. John Wiley & Sons, pp.100-104.

7. Бирюков А. А. Информационная безопасность: защита и нападение. – 2-е изд., перераб. и доп. — М.: ДМК Пресс, 2017. — 434 с.

8. Галушка В.В., Петренкова С.Б., Дзюба Я.В., Панченко В.А. Сетевая стеганография на основе ICMP-инкапсуляции // Инженерный вестник Дона, 2018, №4. URL: ivdon.ru/ru/magazine/archive/n4y2018/5306.

9. Wojciech Frączek, Krzysztof Szczypiorski Perfect undetectability of network steganography. Security Comm. Networks, 2016, 9: pp. 2998–3010.

10. Павлин Д.В., Макосий А.И., Жданов О.Н. О сетевой стеганографии. Реализация алгоритма RSTEG // Решетневские чтения. 2014. №18(2). С. 322-324.

References

1. Tanenbaum Je., Ujezeroll D. Komp'juternye seti.[Computer network]. 5 izd. SPb.: Piter, 2012. 960 p.

2. G.V. Babenko, S.V. Belov Inženernyj vestnik Dona (Rus), 2011, №2. URL: ivdon.ru/ru/magazine/archive/n2y2011/446.

3. RFC 791. Internet protocol, 1981, URL: tools.ietf.org html rfc791.

4. Galushka V.V. Seti i sistemy peredachi informacii. [Networks and information transmission systems]. Uchebnoe posobie. Rostov n D: Izdatel'skij centr DGTU, 2016. 105 p.

5. Ibrahim, L., 2017. Virtual Private Network (VPN) Management and IPSec Tunneling Technology. Middle East Comprehensive Journal For Education And Science Publications (MECSJ), 1: pp. 76- 87.

6. Mazurczyk, W., S. Wendzel, S. Zander, A. Houmansadr and K. Szczypiorski, 2016. Information hiding in communication networks: fundamentals, mechanisms, applications, and countermeasures. John Wiley & Sons, p.100-104.

7. Birjukov A. A. Informacionnaja bezopasnost': zashhita i napadenie. [Information security: protection and attack]. 2 izd., pererab. i dop. M.: DMK Press, 2017. 434 p.
8. Galushka V.V., Petrenkova S.B., Dzjuba Ja.V., Panchenko V.A. Inženernyj vestnik Dona (Rus), 2018, №4. URL: ivdon.ru/ru/magazine/archive/n4y2018/5306.
9. Wojciech Frączek, Krzysztof Szczypiorski Perfect undetectability of network steganography. Security Comm. Networks, 2016, 9: pp.2998 3010.
10. Pavlin D.V., Makosiy A.I., Zhdanov O.N. Reshetnevskie chteniya. 2014. №18(2). pp. 322 324.