УДК 061.68

ИМИТАЦИОННОЕ МОДЕЛИРОВАНИЕ ФРАГМЕНТА СЕТИ ЭЛЕКТРОСВЯЗИ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ С ТЕХНОЛОГИЕЙ IPSEC В СЕТЕВОМ СИМУЛЯТОРЕ NS-3

С.С. ВРУБЛЕВСКИЙ, Е.В. МАШКИН

Военная академия Республики Беларусь, Республика Беларусь

Поступила в редакцию 31 октября 2021

Аннотация. Разработан класс для сетевого симулятора Network Simulator 3, имитирующий работу VPN-шлюза. Показано, что разработанный класс работает имитирует основные процессы протокола IPSec.

Ключевые слова: имитационное моделирование, стек протоколов IPSec, Network Simulator 3.

Введение

Виртуальная частная сеть (Virtual Private Network – VPN) – представляет собой выделенную сеть передачи данных, построенную на инфраструктуре телекоммуникационной сети общего пользования, в которой конфиденциальность и защищенность информации пользователя обеспечивается механизмами шифрования и разграничения трафика (рис. 1) [1].

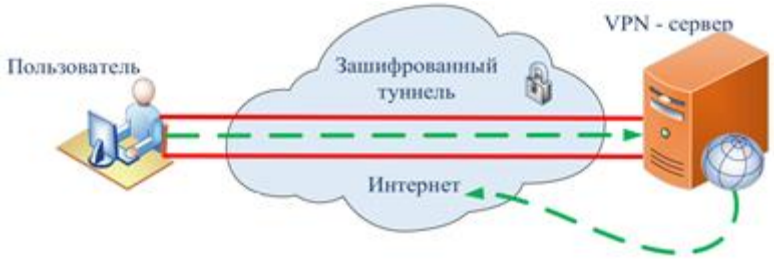

Рис. 1. Виртуальная частная сеть

Виртуальные частные сети подразделяются на:

– сети, построенные на оборудовании, которое устанавливается на стороне клиента и служит для его подключения к сети провайдера;

– сети, построенные на оборудовании, которое устанавливается на стороне провайдера.

И те, и другие подразделяются на три класса в зависимости от принципа организации связи пользователей сети:

– ведомственные (внутрикорпоративные) сети VPN – как правило, строятся на собственной сетевой инфраструктуре без использования ресурсов сети связи общего пользования;

– межведомственные (межкорпоративные) сети VPN – используют как собственную сетевую инфраструктуру, так и инфраструктуру сети провайдера;

– сети VPN удаленного доступа – данный класс сетей VPN предполагает подключение пользователя к сети VPN при помощи специального аппаратного (криптомаршрутизаторы) и программного (Cisco AnyConnect Secure Mobility Client, Avast SecureLine VPN) обеспечения.

Виртуальные частные сети могут быть реализованы на базе протоколов модели OSI на следующих уровнях:

– канальный – L2VPN (L2TP, PPTP, VPLS, VPWS);

– сетевой – L3VPN (IPSec, GRE, BGP/MPLS, VPRN);

– сеансовый – L5VPN [2].

Создание ведомственных (замкнутых) сетей VPN оправдано при использовании аппаратуры IP-шифрования с целью разграничения общего и зашифрованного трафика. Примером ведомственных сетей VPN могут служить сети электросвязи специального назначения (СЭСН), банковские сети и др. На сегодняшний день в СЭСН для создания сетей VPN используется стек протоколов IPSec.

Стек протоколов IPSec и его особенности

Стек протоколов IPSec обеспечивает аутентификацию, целостность и конфиденциальность при помощи алгоритмов шифрования, хеширования, открытых ключей и цифровых сертификатов, стандартизованного консорциум Internet Engineering Task Force (IETF). Стек протоколов IPSec включает в себя протоколы:

– аутентификации – Authentication Header (AH);

– шифрования – Encapsulated Security Payload (ESP);

– обмена ключами – Internet Key Exchange (IKE).

Протоколы AH и ESP могут передавать данные в двух режимах:

– туннельном (IP-пакеты защищаются целиком, включая их заголовки);

– транспортном (защищается только содержимое IP-пакетов).

Широкое распространение нашел туннельный режим работы данных протоколов. В данном режиме исходный пакет инкапсулируется в новый IP-пакет, и передача данных по сети выполняется на основании заголовка нового IP-пакета.

Основным достоинством протокола IPSec является то, что данный протокол поддерживает все виды приложений (видеоконференцсвязь, VoIP, передача данных и т.д.) и может шифровать или аутентифицировать весь трафик на сетевом уровне. Но в тоже время использование данного протокола уменьшает скорость передачи информационных потоков, а также увеличивает время доставки пакета данных в сети.

Имитационная модель фрагмента сети с технологией IPSec в сетевом симуляторе Network Simulator 3

Для создания надежно функционирующей СЭСН необходимо еще на этапе проектирования знать возможные характеристики узлов сети, ввиду того что современный мультисервисный трафик, циркулирующий в сети обладает свойствами самоподобия, который не поддается строгому математическому анализу. Основным инструментом анализа может являться имитационное моделирование без использования реального сетевого оборудования.

Одним из средств имитационного моделирования компьютерных сетей является сетевой симулятор Network Simulator 3 (NS-3). Данная среда моделирования представляет собой симулятор сети связи с дискретными событиями, предназначенный для исследований и использования в образовательных целях. Поддерживает большой стек протоколов и позволяет моделировать компьютерные сети с различными топологиями. Является бесплатным программным обеспечением с открытым исходным кодом (C++ / Python), а также работает с внешними инструментами анимации, анализа данных (создает файлы формата .pcap для работы с Wireshark, а также трейс-файлы в формате ASCII) и визуализации (NetAnim) [3].

Для имитации VPN-туннеля на основе технологии IPsec была создана модель фрагмента СЭСН (рис. 2) с помощью симулятора NS-3, которая состоит из трех оконечных устройств и одного маршрутизатора [4].

а *б*

Рис. 2. Фрагмент СЭСН с VPN-туннелем: *а* – схема сети; *б* – схема сети в NetAnim

Для проведения имитационного моделирования необходимо пройти четыре этапа (рис. 3):

– создание C++ – скрипта, описывающего модель сети;
– получение результатов;
– анализ результатов с помощью трейс- и .pcap файлов;
– визуализация процессов в сети.

Рис. 3. Этапы моделирования фрагмента СЭСН с помощью NS-3

Каждое из сетевых устройств имеет свой IP-адрес. Но при создании туннеля им присваивается виртуальные адреса. Для этого был разработан класс Tunnel, в котором реализуется данная функция. Для проверки функционирования имитационной модели поток UDP-трафика от host_3 передается с виртуального адреса 11.0.0.1 на host_1 с виртуальным адресом 11.0.0.254, что видно из рис. 4. На котором изображено событие моделирования, показывающее передачу потока трафика между виртуальными адресами, а также видно, как пакет с данными (в синей рамке) инкапсулируется в пакет IPSec (в желтой рамке).

```
+ 1.00914 /NodeList/0/DeviceList/1/$ns3::PointToPointNetDevice/TxQueue/Enqueue
ns3::PppHeader (Point-to-Point Protocol: IP (0x0021)) ns3::Ipv4Header (tos 0x0
DSCP Default ECN Not-ECT ttl 64 id 0 protocol 17 offset (bytes) 0 flags [none]
length: 568 10.1.1.1 > 10.1.3.1) ns3::UdpHeader (length: 548 667 > 667)
ns3::Ipv4Header (tos 0x0 DSCP Default ECN Not-ECT ttl 64 id 0 protocol 17
offset (bytes) 0 flags [none] length: 540 11.0.0.1 > 11.0.0.254)
ns3::UdpHeader (length: 520 49153 > 9) Payload (size=512)
```

Рис. 4. Событие моделирования, показывающее передачу потока трафика между виртуальными адресами

В таблице показано влияние процедур функционирования VPN-шлюза на параметры передаваемого UDP-трафика: пиковую (p) и среднюю (r) скорость передачи информационных потоков, длину генерируемых пакетов (L).

Значение параметров трафика на входе и на выходе VPN-шлюза

Место измерения параметров трафика	Значения параметров трафика		
	p, Мбит/с	r, Мбит/с	L, Байт
На входе VPN-шлюза	2,3	0,91	1482
На выходе VPN-шлюза	1,80	1,23	1530

Исходя из выходных данных моделирования можно сделать вывод, что каждый пакет передается с одного виртуального интерфейса на другой, использование VPN-шлюза влияет на параметры передаваемого трафика, уменьшая скорость передачи информационных потоков и увеличивая длину IP-пакета.

Заключение

Таким образом разработанный класс Tunnel для фрагмента сети полностью имитирует применение технологии IPSec, что видно из проведенных испытаний данного класса. Данный класс позволит создать модель полной СЭСН с VPN. Что и является дальнейшим направлением исследования.

SIMULATION OF A SPECIAL PURPOSE TELECOMMUNICATION NETWORK FRAGMENT WITH IPSEC TECHNOLOGY IN THE NS-3 NETWORK SIMULATOR

S.S. VRUBLEVSKY, E.V. MASHKIN

Abstract. A class for the network simulator Network Simulator 3 has been developed to simulate the operation of a VPN gateway. It is shown that the developed class works by simulating the basic processes of the IPSec protocol.

Keywords: simulation, IPSec protocol stack, Network Simulator 3.

Список литературы

1. Mitra D., Morrison J.A., Ramakrishnan K.G. Proc. of the 18th Annual Joint Conference of the IEEE Computer and Communications Societies, 1999. 490 p.
2. Сапрыкин А.В. Исследование и разработка методов анализа вероятностно-временных характеристик узлов сетей связи специального назначения: автореф. дис. канд. тех. наук: 05.12.13 / А.В. Сапрыкин; Поволжский гос. ун-т телекоммуникаций и информатики. Самара, 2018. 16 с.
3. NS-3 Model Library [Electronic resource]. URL: https://www.nsnam.org/docs/models/ns-3-model-library.
4. NS-3 Manual [Electronic resource]. URL: https://www.nsnam.org/docs/manual/ns-3-manual.pdf.