РАЗРАБОТКА ИМИТАЦИОННОЙ МОДЕЛИ ВИРТУАЛЬНОЙ ЧАСТНОЙ СЕТИ ЭЛЕКТРОСВЯЗИ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ В СЕТЕВОМ СИМУЛЯТОРЕ NS-3

Врублевский С. С., Бысов А.А.
Кафедра связи, Военная академия Республики Беларусь
Минск, Республика Беларусь
E-mail: sergeyvrublevsky0@gmail.com

В докладе представлена имитационная модель виртуальной частной сети электросвязи специального назначения, которая позволяет проводить исследования виртуальных частных сетей.

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 туннелирования и средствами информационной безопасности [1].

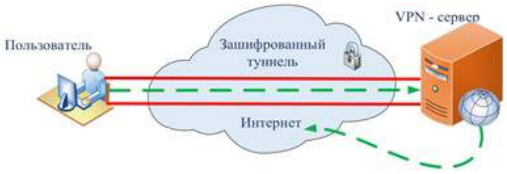

Рис. 1 – Фрагмент СЭСН с VPN-туннелем.

I. Основная часть

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].

Виртуальные частные сети, реализованные на базе протоколов третьего уровня, получили наибольшее распространение. Это обусловлено центральной ролью протокола IP в стеках протоколов модели OSI.

Сеть электросвязи специального назначения (СЭСН) – это сеть, предназначенная для обеспечения нужд государственного управления, национальной безопасности, обороны, охраны правопорядка, предупреждения и ликвидации чрезвычайных ситуаций [3]. Применение технологии VPN получило широкое распространение в СЭСН различных государств по следующим причинам:

- применение стандартных стеков протоколов (например, TCP/IP);
- использование средств IP-шифрования, для построения защищенных каналов (тунелей VPN);
- необходимостью разграничения трафика в зависимости от его класса и приоритета пользователей.

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)[4]. Данная среда моделирования представляет собой си-

мулятор 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).

Для имитации VPN-туннеля (далее – туннель) вида «IP-over-IP» была создана модель фрагмента СЭСН (рис. 2) с помощью симулятора NS-3 [5]. Этапы моделирования в NS-3 представлены на рис. 3.

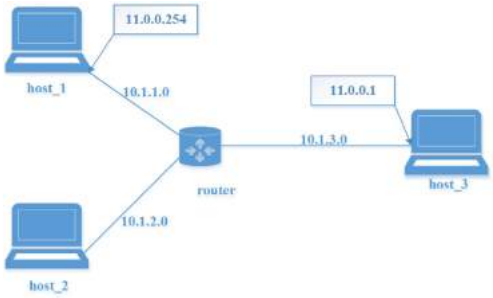

Рис. 2 – Фрагмент СЭСН с VPN-туннелем.

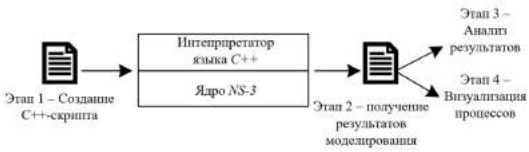

Рис. 3 – Этапы моделирования фрагмента СЭСН с помощью NS-3

Каждое из сетевых устройств имеет свой IP-адрес. Но при создании туннеля им присваивается виртуальные адреса. Для этого был реализован класс Tunnel, в котором реализуется данная функция. Для проверки функционирования имитационной модели был передан поток UDP трафика от host3 передается с виртуального адреса 11.0.0.1 на host1 с виртуальным адресом 11.0.0.254, что видно из рис. 4.

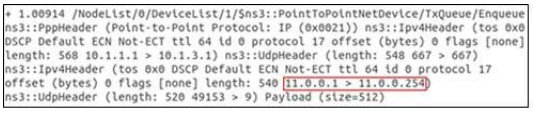

Рис. 4 – Событие моделирования, показывающее передачу потока трафика между виртуальными адресами.

Для визуализации процесса передачи потока трафика была использована среда NetAnim, что видно из рис. 5

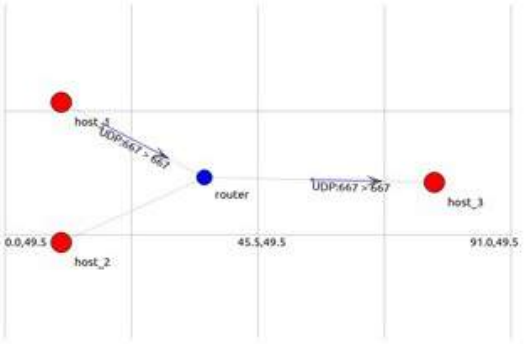

Рис. 5 – Визуализация передачи потока трафика в среде NetAnim.

II. Заключение

Построенная имитационная модель позволяет проводить исследование сетей VPN и является гибким инструментом дл анализа способов их планирования. Разработанный класс Tunnel для фрагмента сети позволит создать модель для полной СЭСН с VPN. Что и является далнейшим направлением исследования

III. Список литературы

1. Mitra, D. Virtual Private Networks: Joint Resource Allocation and Routing Design / D. Mitra, J. A. Morrison, K. G. Ramakrishnan // Proc. of the 18th Annual Joint Conference of the IEEE Computer and Communications Societies. – 1999. – P. 480–490.

2. Сапрыкин, А. В. Исследование и разработка методов анализа вероятностно-временных характеристик узлов сетей связи специального назначения: автореф. дисс. ... канд. тех. наук: 05.12.13 / А. В. Сапрыкин Поволжский гос. ун-т телекоммуникаций и информатики. –Самара, 2008. -16с.

3. Об электросвязи : Закон Респ. Беларусь от 19.05.2005г. №45-З : в ред. от 06.08.2007г. №277-З : с изм. и доп. от 24.05.2021г. №109-З. –Минск, 2021. – 34с.

4. NS-3 Model Library [Electronic resource] / – Mode of access: http://www.nsnam.org/docs/models/ns-3-model-library. – Date of access: 05.10.2021.

5. NS-3 Manual [Electronic resource] / – Mode of access: http://www.nsnam.org/docs/manual/ns-3-manual.pdf – Date of access: 05.10.2021.