Виртуализация криптокоммутаторов Континент в среде Oracle VirtualBox

А. С. Коваль, email: koval@cs.vsu.ru [1]

[1] ФГБОУ ВО «Воронежский Государственный Университет»

Аннотация. *Выступление посвящено опыту развертывания и применения АПКШ Континент в режиме криптокоммутаторов для проведения исследований и учебных практических занятий в области программно-аппаратных систем защиты информации.*

Ключевые слова: *программно-аппаратные системы защиты информации, крипто-коммутаторы, АПКШ Континент, L2VPN.*

Введение

Виртуализация сетевых инфраструктур с программно-аппаратными средствами защиты информации для исследования их характеристик, проверки работоспособности решений на их основе и в учебных целях используется широко и обсуждалась, в частности, на прошлой конференции IPMT-2020 [2]. Однако особенности виртуальных сред накладывают некоторые ограничения на функции виртуализированного оборудования, а иногда и изменяют сами функции. Далее рассматриваются особенности поведения и характеристики пропускной способности виртуализированного аппаратно-программного комплекса шифрования (АПКШ) «Континент» ООО «Код Безопасности» [1] в среде Oracle Virtual Box [3].

1. Топология сети

Минимальная топология для работы с L2 и L3 VPN включает в себя три филиала и центр, представленный АРМ «Админ» (рис.1).

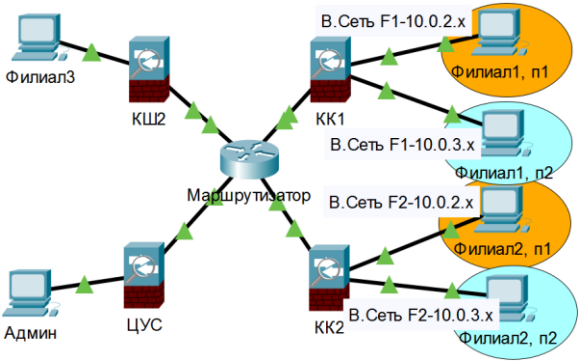

Рис. 1. Минимальная топология для L2 и L3 VPN

Управляется топология с рабочего места администратора - «Админ» и АПКШ Континент в роли центра управления сетью - «ЦУС». Первые два филиала имеют отдельные сети двух подразделений «п1» и «п2», сформированные с помощью криптокоммутаторов «ККІ» и «ККІ2». Третий филиал используется для L3VPN на основе криптошлюзов КШ2 и ЦУС. Маршрутизатором всех сетей топологии является ОС Windows Server 2008R2. Виртуальные машины в Oracle Virtual Box снабжены четырьмя сетевыми интерфейсами, что минимально достаточно для подобных топологий. До 8 интерфейсов можно получить с помощью утилиты командной строки modifyvm.

2. Криптокоммутация

Сети подразделений 1 и 2 данной топологии находятся как в филиале 1, так и 2, поэтому необходимо создать два изолированных L2-туннеля. Для этого в филиалах размещены два криптокоммутатора ККІ и ККІ2, доступные для управления через внешние интерфейсы, подключенные к маршрутизатору. Через эти же интерфейсы проходит туннелируемый трафик. В топологии требуется четыре виртуальные сети для трафика двух подразделений в двух филиалах и четыре конечных узла для тестирования. Однако L2VPN трафик в такой конфигурации не будет проходить через интерфейсы криптокоммутаторов. Это связано с несоответствием статуса «сетевое оборудование» и метода виртуализации, ориентированного на работу хоста. Оборудование вполне может принимать кадры с MAC-адресом назначения, отличающимся от адреса интерфейса, в частности, для порта криптокоммутатора – это обычный режим. Поэтому необходим «promiscuous» (неразборчивый) режим работы порта, обращенного в сторону конечной сети (рис. 2).

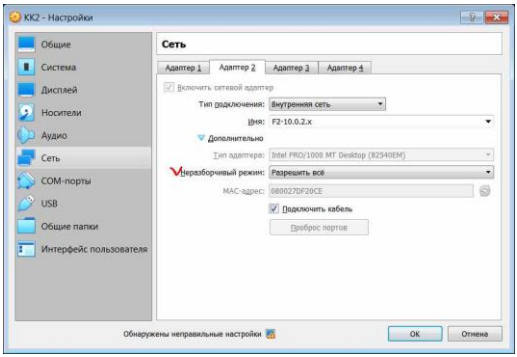

Рис. 2. Виртуальная сеть F2-10.0.2.x и режим работы порта

В вышеприведенной топологии внешние интерфейсы криптокоммутаторов могут находиться как в одной сети, так и в разных. В последнем варианте, трафик будет проходить через маршрутизатор. На практике это соответствует близко расположенным филиалам или филиалам, подключенным к разным сетям провайдеров. Результаты нагрузочного тестирования для обоих вариантов оказались примерно одинаковыми (рис. 3). Это связано с ограничением трафика на криптокоммутаторах из-за повышенных требований к процессорным ресурсам криптоалгоритмов, выполняемых на КК1 и КК2. Следует помнить, что оценка производительности выполняется на виртуализированных «Континентах» и зависит от производительности компьютера, на котором выполняется Virtual Box.

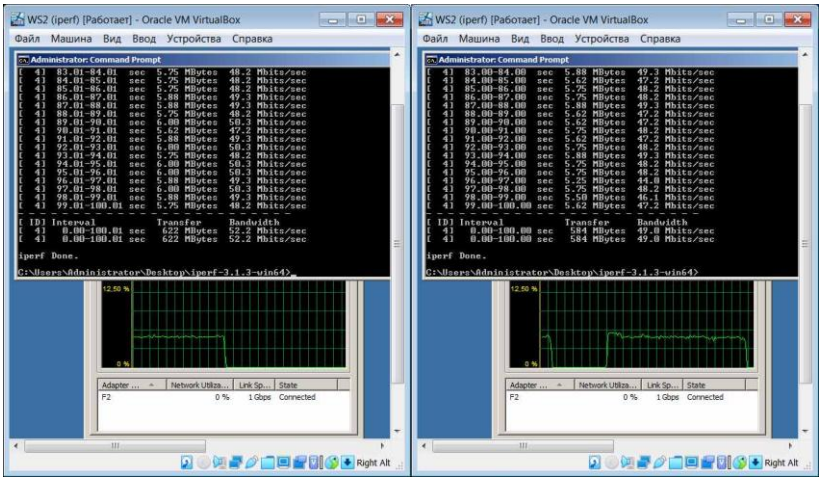

Рис. 3. Пропускная способность L2VPN инфраструктуры

Для сравнения приводится оценка пропускной способности L3VPN инфраструктуры, выполненная на той же топологии. Участвуют два криптошлюза: КШ2 и ЦУС (рис. 4).

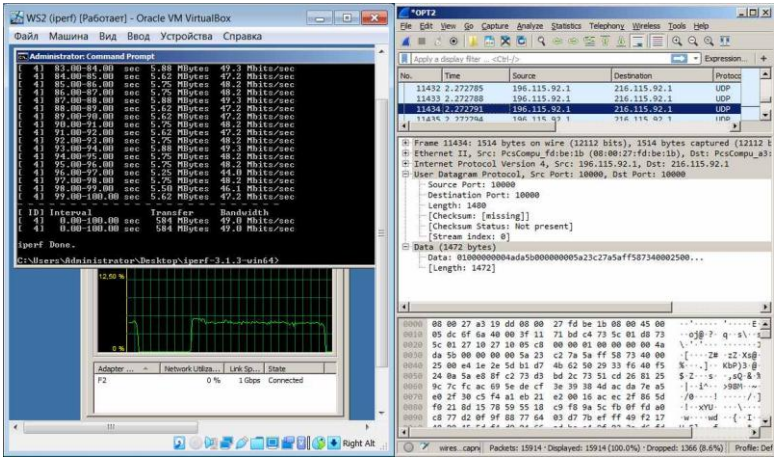

Рис. 4. Пропускная способность L3VPN и дамп трафика

Результаты нагрузочного тестирования L3VPN оказались близкими к результатам L2VPN при соединении криптокоммутаторов через маршрутизатор (49 Мбит/сек). Как и в случае L2VPN, узким местом

является процессорный ресурс виртуальных хостов, выполняющих криптопреобразование (ЦУС и КШ2).

Заключение

В работе рассматриваются особенности реализации инфраструктуры защищенной сети в виртуальной среде Oracle Virtual Box. Определены пропускные способности L2 и L3 VPN реализаций, особенности режимов портов виртуальных интерфейсов для криптокоммутаторов.

Литература

1. Аппаратно-программный комплекс шифрования "Континент" [Электронный ресурс] : Сайт АПКШ Континент. – Режим доступа : https://www.securitycode.ru/products/apksh_kontinent

2. Коваль А.С. Опыт создания виртуальных лабораторий распределенных систем защиты информации / А.С. Коваль // Информатика : Проблемы, методология, технологии : материалы XX Международной научно – методической конференции, Воронеж, 13-14 февр. 2020 г. – Воронеж : Издательский дом ВГУ, 2020.

3. Платформа VirtualBox [Электронный ресурс] : Сайт продукта виртуализации VirtualBox. – Режим доступа : https://www.virtualbox.org