Д.Е. Низовских, А.О. Рычков, И.Р. Зулькарнеев

Тюменский государственный университет, г.Тюмень
УДК 004.056

ПРОБЛЕМЫ ПОСТРОЕНИЯ ВИРТУАЛЬНОЙ ЛАБОРАТОРИИ VIPNET НА БАЗЕ VMWARE В ВУЗЕ

Аннотация. Был проведен анализ программного комплекса ViPNet. Раскрыты основные методы работы с ним, а также использование виртуальных машин в среде VMware. В результате разработана виртуальная лаборатория и протестированы практические работы для студентов, обучающихся информационной безопасности.

Ключевые слова: VPN, ViPNet, виртуализация, VMware, проектирование инфраструктуры.

ViPNet является самым распространённым программным комплексом защиты передаваемой информации среди государственных и бюджетных учреждений Российской Федерации. Он предназначен для криптографической защиты каналов передачи информации, управления и фильтрации сетевых потоков, межсетевого экранирования, реализации функционала ЭЦП и многого другого.

В связи с этим на кафедре информационной безопасности Тюменского государственного университета было принято решение о обязательной прохождении студентов обучению работе с программным комплексом ViPNet версии 4.x для повышения их ценности на рынке труда. Обучение студентов должно проводиться в специально созданной виртуальной лаборатории на базе ресурсов университета, которые использует инфраструктуру на базе VMware.

При реализации лаборатории выбор в пользу виртуализации был

сделан на основе ряда факторов. С виртуальными машинами возможно работать из любой точки земного шара в любое время, что актуально в связи с текущей ситуацией с COVID-19 и возможными повторениями подобных ситуаций в будущем. Также может быть реализована возможность работы нескольких студентов за одним стендом одновременно выполняя разные лабораторные работы. Для студента главным плюсом является отсутствие необходимости использования ресурсов собственного компьютера, которых будет недостаточно для выполнения лабораторных работ. С точки зрения образовательного процесса подобный подход позволяет преподавателю проверять работы в любое время или даже в режиме реального времени, а также оперативно разворачивать виртуальные стенды и масштабировать их под необходимое количество участников. Единственным и главным ограничением является размер доступных виртуальных ресурсов в университете.

Целью нашей работы стала проектирование, разработка и тестирование виртуальной сетевой инфраструктур для выполнения лабораторных работ на базе официальных практикумов ViPNet с возможностью дальнейшего масштабирования и тиражирования лабораторных стендов при минимизации используемых вычислительных мощностей.

Достижение данной цели обусловило выполнение следующих задач:

- проанализировать лабораторные практикумы ViPNet для определения оптимальной топологии сети;
- рассчитать минимально необходимые системные требования виртуальных машин;
- спроектировать эталонную виртуальную инфраструктуру для дальнейшего тиражирования;
- протестировать процесс выполнения лабораторных работ с целью обнаружения возможных ошибок и непредвиденных ситуаций.

В результате анализа лабораторных практикумов [1] и [2] была разработана оптимальная топология сети (рис. 1), позволяющая выполнить любые предложенные лабораторные работы, не относящихся к Policy Manager, для двух сетей ViPNet. Минимальное количество виртуальных машин (далее - ВМ) для виртуальной лаборатории составило 8:

- 2 ВМ для ViPNet Administrator;
- 2 ВМ для ViPNet Client и ViPNet Coordinator для Windows;
- 4 ВМ для ViPNet Coordinator HW;

Все ВМ объединены в 5 виртуальных частных сетей:

- 201 и 203: защищённая сеть ViPNet;
- 202: имитация глобальной сети;
- 204 и 205: виртуальная сеть для кластера горячего резервирования.

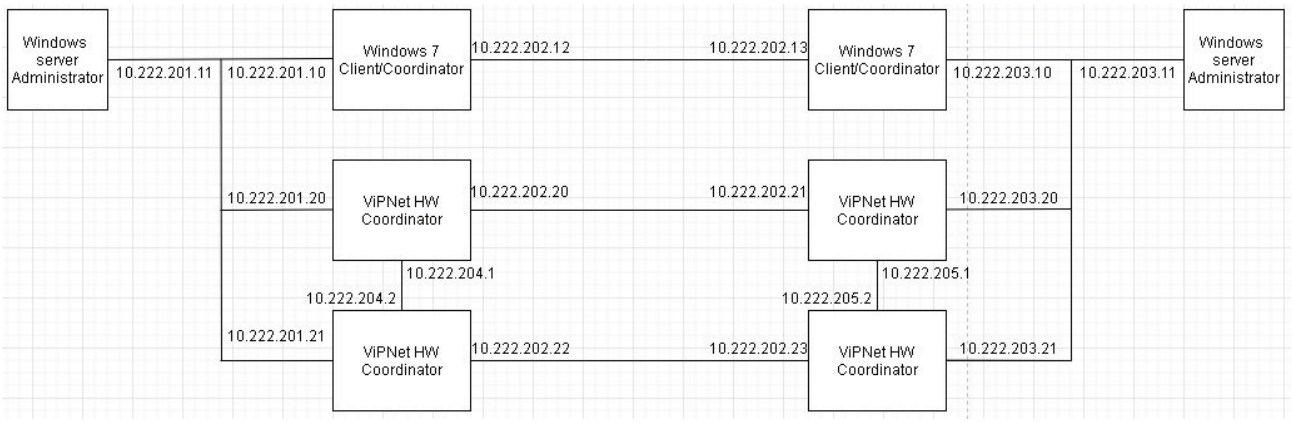

Рис. 1. Предварительная топология сети эталонной инфраструктуры.

На основе минимально необходимых требований программных модулей ViPNet, дополнительного программного обеспечения и требований операционных систем был произведен расчет затрачиваемых виртуальных ресурсов для лаборатории (таблица 1). Для экономии виртуальных мощностей университета при создании виртуальных машин необходимо использовать “тонкие” (thin) диски.

Таблица 1. Предварительные характеристики виртуальных машин.

Название виртуальной	Объем оперативной	Объем дискового	Кол-во ядер	Кол-во

машины	памяти, Гб	пространства, Гб	процессора	процессоров
Windows server administration	4	30	4	2
Windows 10 client/coordinator	2	22	2	3
ViPNet HW Coordinator	2	4	1	1
Итого	20	120	16	8

При тестировании стоит учитывать, что из-за политик безопасности университета студенты не будут иметь доступа к панели управления VMware Vsphere, а взаимодействие с виртуальными машинами будет происходить с помощью протокола RDP.

Так как программный комплекс ViPNet включает в себя такие программные компоненты, как ViPNet Coordinator и ViPNet Client, которые реализуют функции межсетевого экранирования, то при их инсталляции связь с виртуальной машиной при удалённом доступе будет потеряна. Это обусловлено тем, что ViPNet отключает все внешние соединения и требует верификацию.

Также стоит учитывать, что в VMware введен широкий список ограничений, усложняющих разработку лабораторного стенда. Все это привело к возникновению ряда проблем, не позволяющих выполнять лабораторные работы по курсу ViPNet в виртуальной инфраструктуре.

Проблема 1. После установки всех компонентов ViPNet Client и авторизации администратора будет автоматически включён брандмауэр. В случае завершения RDP сессии по какой-либо причине доступ к данной ВМ будет невозможен.

Решение: необходимо сразу после установки ViPNet Client до перезагрузки ВМ запустить модуль Монитор и добавить разрешающий открытый фильтр, разрешающий RDP подключения.

Проблема 2. При перезагрузке виртуальной машины, на которой установлен ViPNet Client пропадет возможность подключения к удаленному рабочему столу, так как при загрузке ОС появится

дополнительная авторизация от ViPNet.

Решение: необходимо сразу после установки ViPNet Client до перезагрузки ВМ запустить модуль Монитор. Зайти в режим администратора и выбрать опции “Автоматически входить в ViPNet” и “Разрешить сохранять пароль в реестре” и разрешение сохранения пароля в реестре. После этого при следующей авторизации необходимо выбрать опцию “сохранить пароль”.

Следующие две проблемы невозможно было решить при текущих настройках безопасности виртуальной инфраструктуры и существующей топологии сети.

Проблема 3. В процессе инсталляции ViPNet Coordinator для ОС Windows после установки дистрибутива ключа из специального файла происходит принудительный обрыв RDP-сессии без возможности повторного доступа или предварительной добавления разрешающих правил для RDP.

Проблема 4. Производим подготовку HW Coordinator. Для авторизации дистрибутива в сеть ViPNet необходимо передать в образ системы дистрибутив ключа. Достигается это тремя способами: через cd, usb, tftp.[3] В связи с ограничение доступа студента к панели управления VMware, то передача дистрибутива ключ не возможна. Первоначально предполагалась передача посредством протокола tftp, но из-за жестких ограничений созданными администраторами VMware заблокированы широковещательные запросы, в следствии виртуальная машина не могла получить IP-адрес через протокол DHCP, а назначить ip адрес машине до ее регистрации в сети ViPNet невозможно.

Решение: Пересмотр топологии сети и использование вложенной виртуализации для ВМ Windows 7 и ViPNet Coordinator HW. Передача дистрибутива ключа будет возможна с помощью монтирования iso образа содержащий дистрибутив ключа в качестве CD-диска.

Для этой задачи был выбран VirtualBox по причине его простоты и распространенности, а также малой нагрузки на вычислительные мощности.

В результате была построена новая топология сети с учетом вложенных ВМ (рис. 2). Стоит отметить также, что необходимо создавать сетевые мосты от внешних виртуальных частных сетей к вложенным ВМ. Для минимизации ресурсов кластеры ViPNet Coordinator HW объединяются во внутренней сети VirtualBox через дополнительный адаптер без использования отдельной виртуальной сети со стороны VMware.

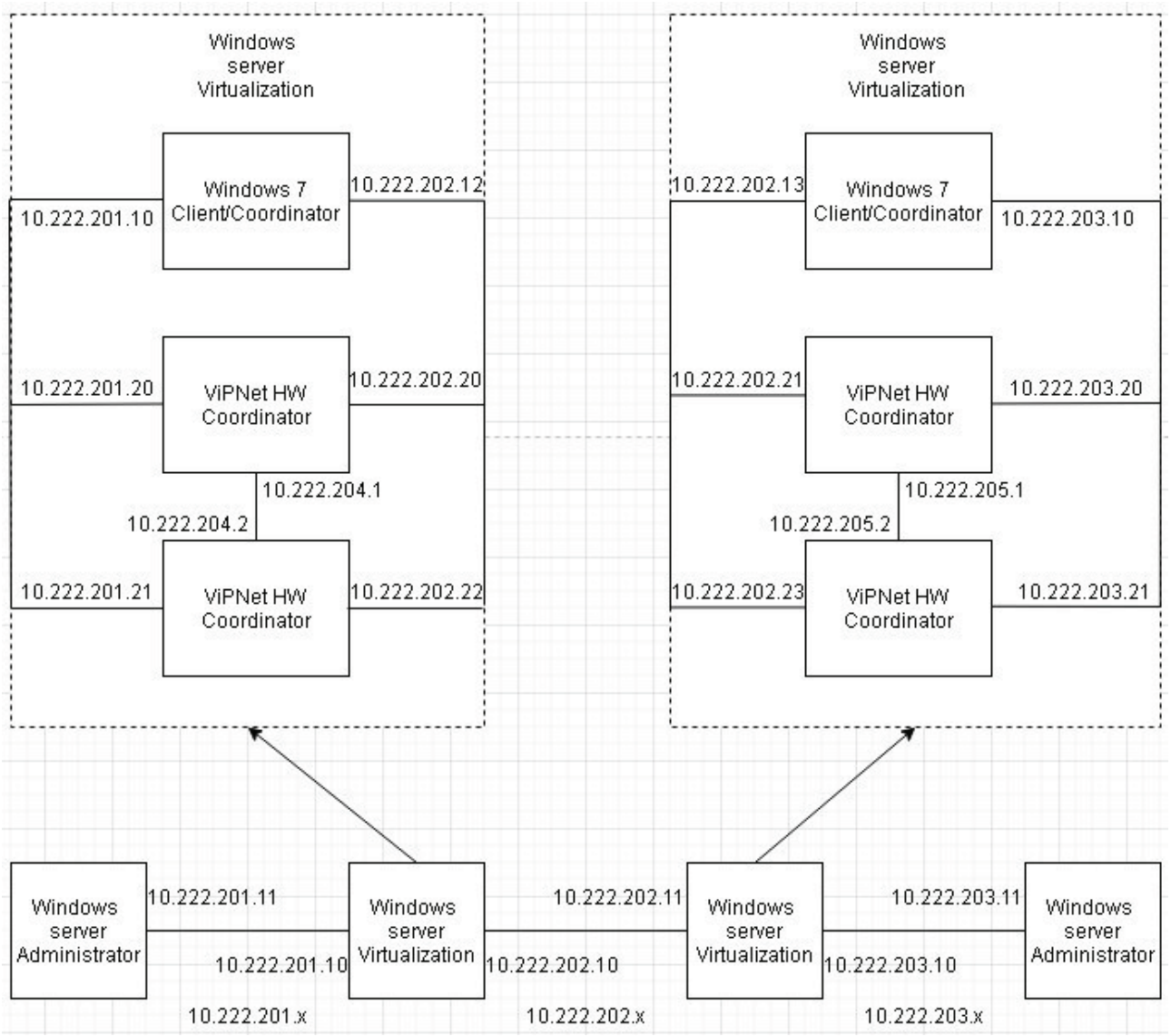

Рис.2. Итоговая топология сети.

Пересмотр топологии использование вложенной виртуализации привёл нас к следующим характеристикам виртуальных машин, которые представлены в таблице 2.

Таблица 2. Характеристики машин в VMware.

Название виртуальной машины	Объем оперативной памяти, Гб	Объем дискового пространства, Гб	Кол-во ядер процессора	Кол-во процессоров
Windows server administration	4	30	4	2
Windows server virtualization	8	30	4	2
Итого	24	120	16	4

Внутри каждой машины для вложенной виртуализации (Windows Server Virtualization) развернуты виртуальные машины с характеристиками, представленными в таблице 3.

Таблица 3. Характеристика виртуальных машин в VirtualBox.

Название виртуальной машины	Объем оперативной памяти, Гб	Объем дискового пространства, Гб	Кол-во ядер процессора	Кол-во процессоров
Windows 7 Client/Coordinator	2	14	1	1
ViPNet Coordinator	1	2	1	2
Итого	4	18	3	3

Важно проконтролировать, чтобы интерфейсы Windows относились к той же сети, что и IP-адреса. Это настраивается посредством сетевых мостов в VirtualBox.

Проблема 5. В ходе настройки координатора ViPNet Coordinator HW возникла проблема с невозможностью входа в привилегированный режим.

Решение: для исправления данной ситуации, необходимо выдать новый дистрибутив ключа в ViPNet УКЦ с созданным паролем администратора.

Проблема 6. При работе с ViPNet Coordinator HW icmp запросы не

проходят.

Решение: необходимо учесть, чтобы время на всех виртуальных машинах было идентично.

Проблема 7. При запросах отправленных с ViPNet Client в журнале пакетов ViPNet Coordinator HW не отображается icmp трафик.

Решение: на виртуальных машинах ViPNet Client изначально шлюзом установлен IP-адрес шлюза VMware, но в этом случае следует установить в качестве шлюза IP-адрес ViPNet Coordinator HW.

Проблема 8. При настройке туннелирования через конфигурацию на ViPNet HW Coordinator всплывает ошибка, показанная на рисунке 4.

Рис. 4. Настройка туннелирования.

Решение: во избежание данной проблемы необходимо все настройки туннелей производить со стороны центра управления сетью. После проведения всех правок необходимо сформировать и отправить справочники на данные узлы. Данные настройки будут внесены в конфигурацию туннелирования ViPNet Coordinator HW.

Заключение

Процесс создания виртуальной инфраструктуры для выполнения лабораторных работ по курсу ViPNet на базе VMware vSphere сталкивается с проблемами, не описанными в известных документах связанными с особенностью функционировании семейства ViPNet. Для нормального функционирования данной лаборатории необходимо использовать вложенную виртуализацию и произвести ряд настроек в самих продуктах ViPNet. При этом данные настройки необходимо учитывать при прохождении студентами лабораторного практикума. Дополнительно стоит

отметить необходимость использования минимально необходимых настроек для виртуализации, настроек виртуальных машин и минимального количества сетей для дальнейшего масштабирования созданной инфраструктуры для любого количества участников. В качестве вспомогательного материала к лабораторным практикумам всем студентам необходимо рекомендовать использовать официальные руководства по установке, настройки и администрированию продуктов ViPNet.

СПИСОК ЛИТЕРАТУРЫ

1. Гусев В.В., Чаплыгин В.Е. Администрирование системы защиты информации ViPNet (Windows & Linux) – М.: Горячая линия - Телеком, 2017. –365 с.

2. Гусев В.В. Программно-аппаратные комплексы ViPNet HW 4 – М.: 2017. – 144 с.

3. Михеев М.О. Администрирование VMware Vsphere 5 – М.: ДМК пресс, 2012. – С. 56 - 64.

4. ViPNet Coordinator HW 4 Подготовка к работе, – 2017. – С. 30 - 32.