МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «НОВОСИБИРСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

ФАКУЛЬТЕТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Кафедра компьютерных систем

Направление подготовки 09.03.01 Информатика и вычислительная техника

Направленность (профиль) Программная инженерия и компьютерные науки

ОТЧЕТ

о прохождении учебной практики, эксплуатационной практики
(указывается наименование практики)

Обучающегося Кондренко Кирилла Павловича **группы №** 21203 **курса** 3
(Ф.И.О. полностью)

Тема задания: развёртывание и анализ программно-аппаратного комплекса «РУБИКОН-К»

Место прохождения практики: Лаборатория современных компьютерных технологий, 630090, г. Новосибирск, ул. Пирогова, д. 1, каб. 1127
(полное наименование организации и структурного подразделения, индекс, адрес)

Сроки прохождения практики: с 05.02.2024 г. по 24.05.2024 г.

Руководитель практики от профильной организации _____ _____
(Ф.И.О. полностью, должность) (подпись)

Руководитель практики от НГУ Пестунова Тамара Михайловна, доцент _____
(Ф.И.О. полностью, должность) (подпись)

Руководитель ВКР Пестунова Тамара Михайловна доцент
(Ф.И.О. полностью) (должность)

Оценка по итогам защиты отчета:_____
(неудовлетворительно, удовлетворительно, хорошо, отлично)

Отчет заслушан на заседании кафедры _____
(наименование кафедры)

протокол _____от «_____» _____ 20_____г.

Новосибирск 2024

Оглавление

Введение

Цель прохождения практики состояла в развёртывании и анализе программно-аппаратного комплекса «РУБИКОН-К». Для достижения этой цели нужно было решить следующие задачи:

- изучить официальную документацию «Рубикон-К»;
- произвести инсталляция программного обеспечения, необходимого для развёртывания «Рубикон-К»;
- произвести настройку, тестирование и проверку работоспособности установленного «Рубикон-К»;
- Проанализировать и рассмотреть «Рубикон-К» в качестве межсетевого экрана.

Также дополнительной задачей являлось сравнение «Рубикон-К» с межсетевым экраном нового поколения «Usergate».

Актуальность темы межсетевых экранов и систем обнаружения вторжений существенна в современном мире технологий, так как постоянно открываются новые способы осуществления атак на компьютерные сети, когда как межсетевые экраны и системы обнаружения вторжений позволяют защищаться от них.

Предполагаемые результаты прохождения данной практики описывает следующий список:

- навыки чтения официальных документаций;
- умение производить инсталляцию ПО, необходимого для развёртывания других приложений;
- навыки настройки, тестирования и проверки работоспособности ПО;
- навыки в сравнении различных программно-аппаратных комплексов и межсетевых экранов.

1. Предметная область

Межсетевой экран — это локальное (однокомпонентное) или функционально - распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в автоматизированную систему и/или выходящей из автоматизированной системы [1]. Например, «брандмауер» в семействе операционных систем Windows можно считать межсетевым экраном. В общем случае межсетевые экраны позволяют лишь осуществлять контроль и фильтрацию трафика для защиты от различных атак (Например, IP-spoofing, SYN-flood).

Межсетевой экран нового поколения (**NGFW** — **N**ext **G**eneration **F**ire**w**all) — межсетевой экран для глубокой фильтрации трафика, интегрированный с IDS (Intrusion Detection System, система обнаружения вторжений) или IPS (Intrusion Prevention System, система предотвращения вторжений) и обладающий возможностью контролировать и блокировать трафик на уровне приложений [2].

Межсетевой экран нового поколения — это комплексный инструмент, предназначенный для контроля трафика, управления доступом пользователей и приложений, предотвращения атак [3].

То есть межсетевой экран следующего поколения расширяет возможности «обычного» межсетевого экрана и объединяет в себе функциональность антивирусов, брандмауэров и других приложений безопасности.

Система обнаружения вторжений (**IDS** — **I**ntrusion **D**etection **S**ystem) — специализированная система, используемая для идентификации того факта, что была предпринята попытка вторжения, вторжение происходит или произошло, а также для возможного реагирования на вторжение в информационные системы и сети [4].

Система предотвращения вторжений (**IPS** — **I**ntrusion **P**revention **S**ystem) — вид систем обнаружения вторжений, специально предназначенных для обеспечения активной возможности реагирования [5].

2. «Рубикон-К»

Программно-аппаратный комплекс «Рубикон-К», разработанный в компании «Эшелон», объединяет функции маршрутизатора, межсетевого экрана типа «А» и типа «Б» четвертого класса защиты и системы обнаружения вторжений уровня сети четвертого класса защиты [6]. Комплекс сертифицирован ФСТЭК России. «Рубикон-К» имеет 4 варианта исполнения [6]:

1. «РУБИКОН-К mini» — для небольших сетей;
2. «РУБИКОН-К 1U» — для средних сетей;
3. «РУБИКОН-К Высокопроизводительный» — для больших сетей;
4. «Рубикон-К miniРУБИКОН-К Мультипортовый» — для крупных сетей.

«Рубикон-К» обладает следующими преимуществами [6]:

- web-интерфейс управления с ролевой моделью доступа;
- выполнение основных функций коммутации сетевых пакетов (коммутатор уровня L2 и коммутатор уровня L3);
- поддержка статической и динамической маршрутизации;
- возможность резервирования на уровне устройств (по протоколу CARP);
- возможность резервирования на уровне портов (bridge, VLAN, bonding);
- возможность резервирования на уровне каналов связи по средствам динамической маршрутизации с использованием протоколов OSPF, BGP;
- возможность построение VPN туннелей с использованием протоколов IPSec, OpenVPN и GRE;
- возможность трансляции сетевых адресов (NAT);
- выполнение фильтрации сетевых пакетов в режиме маршрутизатора (при использовании в режиме L3 коммутатора) по основным заголовкам сетевых пакетов;

- выполнение фильтрации сетевых пакетов в прозрачном режиме (при использовании в режиме L2 коммутатора) по основным заголовкам сетевых пакетов;
- возможность фильтрации сетевых пакетов по мандатным меткам отечественных защищенных операционных систем (Astra Linux и МСВС);
- наличие системы обнаружения вторжений (IDS);
- наличие системы предотвращения вторжений (IPS);
- возможность анализа сетевого трафика средствами СОВ, поступающего от внешних источников, с использованием технологии SPAN-порта;
- возможность функционирования СОВ в прозрачном режиме;
- наличие HTTP-прокси и FTP-прокси;
- возможность совместного использования HTTP-прокси с внешним антивирусом (по протоколу ICAP);

2.1 Развёртывание

Для прохождения учебной практики «Рубикон-К» был предоставлен в виде ISO-образа с некоторым дистрибутивом Linux, поэтому встал вопрос соответствующего его развёртывания. Для этого была выбрана программа типа Hypervisor «Oracle VM VirtualBox», позволяющая производить инсталляцию, настройку и использование операционных систем, установленных на ISO-образах. Данное ПО было выбрано потому что на момент начала прохождения практики имелся положительный опыт при работе с ним.

2.2 Настройка и тестирование

Для проверки работоспособности «Рубикон-К» в «Oracle VM VirtualBox» были настроены ещё три виртуальные машины, две из которых использовали операционную систему «Windows 10-22h2», а оставшаяся — «Linux Mint 21.3 cinnamon».

Базовая настройка «Рубикон-К» производилась согласно руководству администратора [7]. Однако в ходе тестирования обнаружилось, что некоторые заявленные преимущества «Рубикон-К» в данной комплектации на самом деле не

имеют места. Так, например, возможность трансляции сетевых адрес отсутствует [1]. Из этого сразу же следует, что проверить возможности работы «Рубикон-К», связанные с доступом к сети «Интернет» можно лишь частично [2].

Несмотря на отсутствие трансляции сетевых адресов была проверена работоспособность следующих возможностей:

- веб-интерфейс и его ролевая система;
- проверка статуса «Рубикон-К»;
- настройка сетевых интерфейсов;
- настройка меню веб-интерфейса;
- настройка статических и динамических маршрутов;
- DHCP-сервер;
- ограничения трафика.

[1] в руководстве администратора [7] сказано, что трансляция сетевых адресов происходит автоматически, а ручная настройка трансляции не предусмотрена.

[2] виртуальная машина с «Рубикон-К» имела доступ к сети «Интернет», однако, для полной проверки её работоспособности, все остальные виртуальные машины в стенде должны были бы иметь доступ к сети «Интернет» исключительно через виртуальную машину с «Рубикон-К», однако это не представляется возможным из-за отсутствия трансляции сетевых адресов в данной комплектации.

3. Сравнение «Рубикон-К» и «Usergate»

«Рубикон-К» и «Usergate» являются современными межсетевыми экранами, но второй заявлен как межсетевой экран нового поколения, в то время как первый — нет. Тем не менее, существуют различия в их возможностях:

- «Usergate» поддерживает кластеризацию и отказоустойчивость, «Рубикон-К» — нет [1];
- «Usergate» позволяет объединять сетевые интерфейсы в группы, называемые «зонами», для более быстрого и удобного их конфигурирования, поскольку доступна конфигурация как самих интерфейсов, так и «зон»;
- «Usergate» позволяет объединять в общие группы номера телефонов, электронные адреса, сетевые интерфейсы, списки URL и приложения для более удобного их конфигурирования и использования. Например, можно запрещать или разрешать трафик через группу URL, а не через единичные URL;
- «Usergate» в отличие от «Рубикон-К» поддерживает конфигурацию всех типов трансляции сетевых адресов;
- «Usergate» поддерживает авторизацию пользователей, используя данные о записях из таких источников как «LDAP» и «Active Directory», а также позволяет авторизовать пользователя используя прозрачную авторизацию по протоколу Kerberos, в то время как учётные записи в «Рубикон-К» настраиваются исключительно в нём, и при этом авторизоваться можно лишь по логину и паролю.

[1] «Рубикон-К» поддерживает лишь резервное копирование и автоматическое восстановление, в то время как «Usergate> поддерживает работу с кластером отказоустойчивости, работающем по протоколу VRRP.

Заключение

В результате прохождения практики был развёрнут, проанализирован и оттестирован программно-аппаратный комплекс «Рубикон-К». Также было проведено его сравнение с межсетевым экраном нового поколения «Usergate», показавшее, что в «Usergate» больше возможностей, чем в «Рубикон-К». Также был получен опыт изучения официальных документаций.

В течение прохождения практики пришлось столкнуться с двумя основными трудностями:

1. ISO-образ, в виде которого поставляется «Рубикон-К», изначально имел пароль, не указанный в документации, поэтому пришлось найти способ сброса пароля без повреждения ISO-образа;

2. Как уже было упомянуто ранее, использованная комплектация «Рубикон-К» не поддерживает трансляцию сетевых адресов, что ограничивает возможности его использования и тестирования.

Список использованных источников

[1] *Интернет-портал по информационной безопасности в сети [Электронный ресурс]*. URL: https://safe-surf.ru/glossary/ru/967/?sphrase_id=45658.

[2] *Энциклопедия «Касперского» [Электронный ресурс]*. URL: https://encyclopedia.kaspersky.ru/glossary/next-generation-firewall-ngfw/#:~:text=NGFW%20(Next%20Generation%20Firewall%2C%20%D0%BC%D0%B5%D0%B6%D1%81%D0%B5%D1%82%D0%B5%D0%B2%D0%BE%D0%B9,%D0%B1%D0%BB%D0%BE%D0%BA%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D1%82%D1%8C%20%D1%82%D1%80%D0%B0%D1%84%D0%B8%D0%BA%20%D0%BD%D0%B0%20%D1%83%D1%80%D0%BE%D0%B2%D0%BD%D0%B5%20%D0%BF%D1%80%D0%B8%D0%BB%D0%BE%D0%B6%D0%B5%D0%BD%D0%B8%D0%B9.

[3] *Интерактивный словарь «Сбера» [Электронный ресурс]*. URL: https://www.sberbank.ru/ru/person/kibrary/vocabulary/ngfw#:~:text=NGFW%20(Next-Generation%20Firewall%20%D0%BF%D0%B5%D1%80%D0%B5%D0%B2%D0%BE%D0%B4%20%D1%81,%D0%B1%D1%80%D0%B0%D0%BD%D0%B4%D0%BC%D0%B0%D1%83%D1%8D%D1%80%D0%BE%D0%B2%20%D0%B8%20%D0%B4%D1%80%D1%83%D0%B3%D0%B8%D1%85%20%D0%BF%D1%80%D0%B8%D0%BB%D0%BE%D0%B6%D0%B5%D0%BD%D0%B8%D0%B9%20%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D0%B8.

[4] *Интернет-портал по информационной безопасности в сети - система обнаружения вторжений [Электронный ресурс]*. URL: https://safe-surf.ru/glossary/ru/1150/?sphrase_id=45681.

[5] *Интернет-портал по информационной безопасности в сети - система предотвращения вторжений [Электронный ресурс]*. URL: https://safe-surf.ru/glossary/ru/1152/?sphrase_id=45681.

[6] *РУБИКОН-К [Электронный ресурс]*. URL: https://npo-echelon.ru/production/65/10595.

[7] *НПЕШ.465614.004РА Руководство администратора. 1996 [Электронный ресурс]*.