Отчёт

о прохождении учебной практики, эксплуатационной практики

Развёртывание и анализ программно-аппаратного комплекса «РУБИКОН-К»

Выполнил: Кондренко Кирилл Павлович

Руководитель практики: Пестунова Тамара Михайловна

Новосибирск 2024

Введение

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

Задачи:

- изучение официальной документации «РУБИКОН-К»;
- инсталляция программного обеспечения, необходимого для развёртывания «РУБИКОН-К»;
- настройка, тестирование и проверка работоспособности установленного «РУБИКОН-К»;
- анализ «РУБИКОН-К» в качестве межсетевого экрана.

Предметная область

Вторжение (**Intrusion**) — несанкционированный доступ к сети или подсоединённой к сети системе, т.е. преднамеренный или случайный несанкционированный доступ к информационной системе, включая злонамеренную деятельность против информационной системы или несанкционированное использование ресурсов в информационной системе [1]

Система обнаружения вторжений (**IDS** — **I**ntrusion **D**etection **S**ystem) — система, используемая для идентификации того факта, что была предпринята попытка вторжения, вторжение происходит или произошло, а также для возможного реагирования на вторжение [2]

Система предотвращения вторжений (**IPS** — **I**ntrusion **P**revention **S**ystem) — вид систем обнаружения вторжений, специально предназначенных для обеспечения активной возможности реагирования [3]

Предметная область

Межсетевой экран (**FW — F**ire**w**all) — 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 [4]

Межсетевой экран нового поколения (**NGFW** — **N**ext **G**eneration **F**ire**w**all) — межсетевой экран для глубокой фильтрации трафика, интегрированный с **IDS** или **IPS** (**I**ntrusion **P**revention **S**ystem, система предотвращения вторжений) и обладающий возможностью контролировать и блокировать трафик на уровне приложений [5]

РУБИКОН-К

«РУБИКОН-К» — программно-аппаратный комплекс, разработанный в компании «Эшелон», который объединяет функции маршрутизатора, межсетевого экрана и системы обнаружения вторжений.

Комплекс сертифицирован **ФСТЭК** (**Ф**едеральная **С**лужба по **Т**ехническому и **Э**кспортному **К**онтролю России).

Варианты исполнения:

- РУБИКОН-К mini — для небольших сетей;
- РУБИКОН-К 1U — для средних сетей;
- РУБИКОН-К Высокопроизводительный — для больших сетей;
- РУБИКОН-К Мультипортовый — для крупных сетей.

Возможности РУБИКОН-К

- 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).

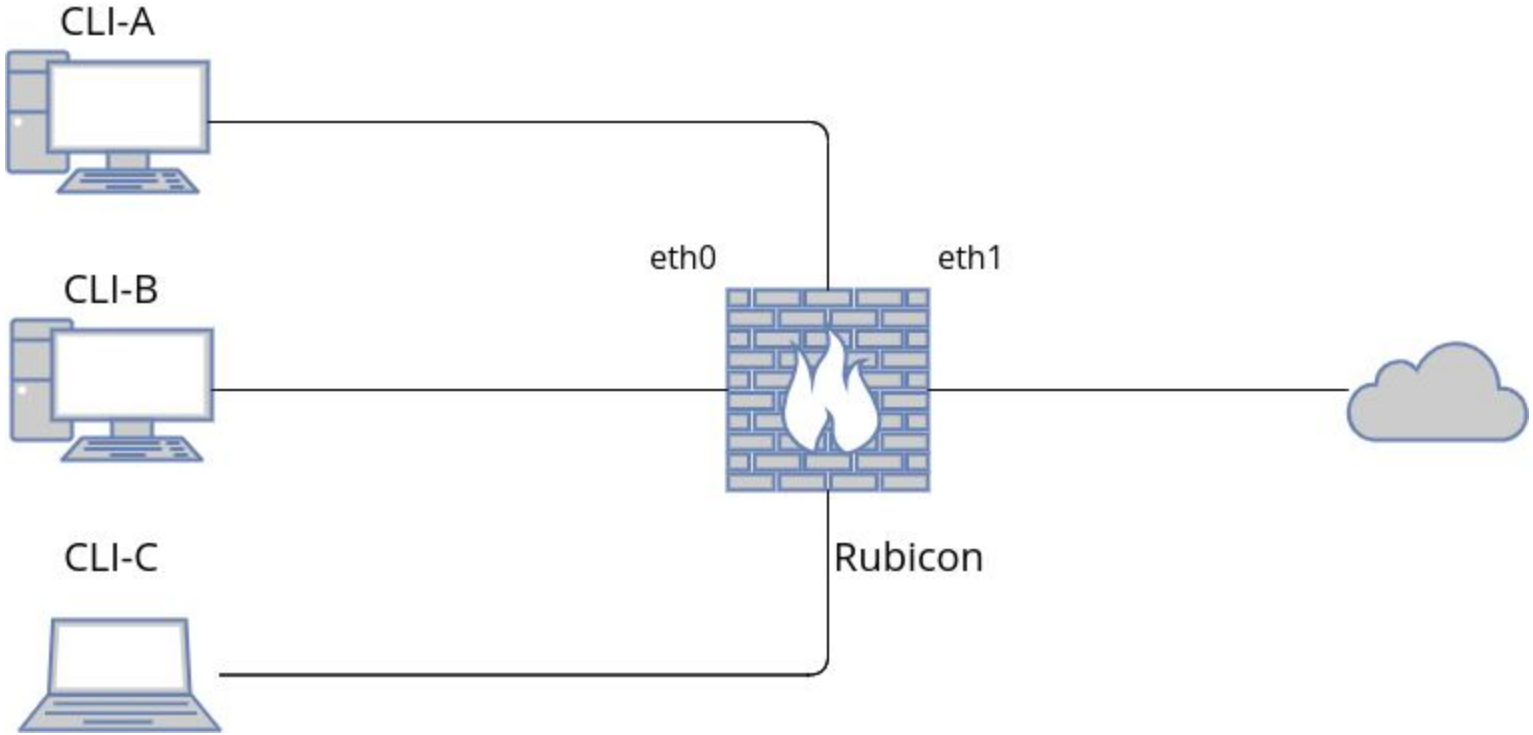
РУБИКОН-К

Для прохождения учебной практики «РУБИКОН-К» был предоставлен в виде ISO-образа с некоторым дистрибутивом Linux, поэтому встал вопрос соответствующего его развёртывания.

Была выбрана программа типа Hypervisor «Oracle VM VirtualBox», позволяющая производить инсталляцию, настройку и использование операционных систем, установленных на ISO-образах.

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. Однако в ходе тестирования обнаружилось, что некоторые заявленные преимущества «Рубикон-К» в данной комплектации на самом деле не имеют места.


CLI-A
CLI-B
CLI-C
eth0
eth1
Rubicon

Отсутствующие возможности РУБИКОН-К

- трансляция сетевых адресов;

- в веб-интерфейсе «РУБИКОН-К» виден лишь один сетевой интерфейс.

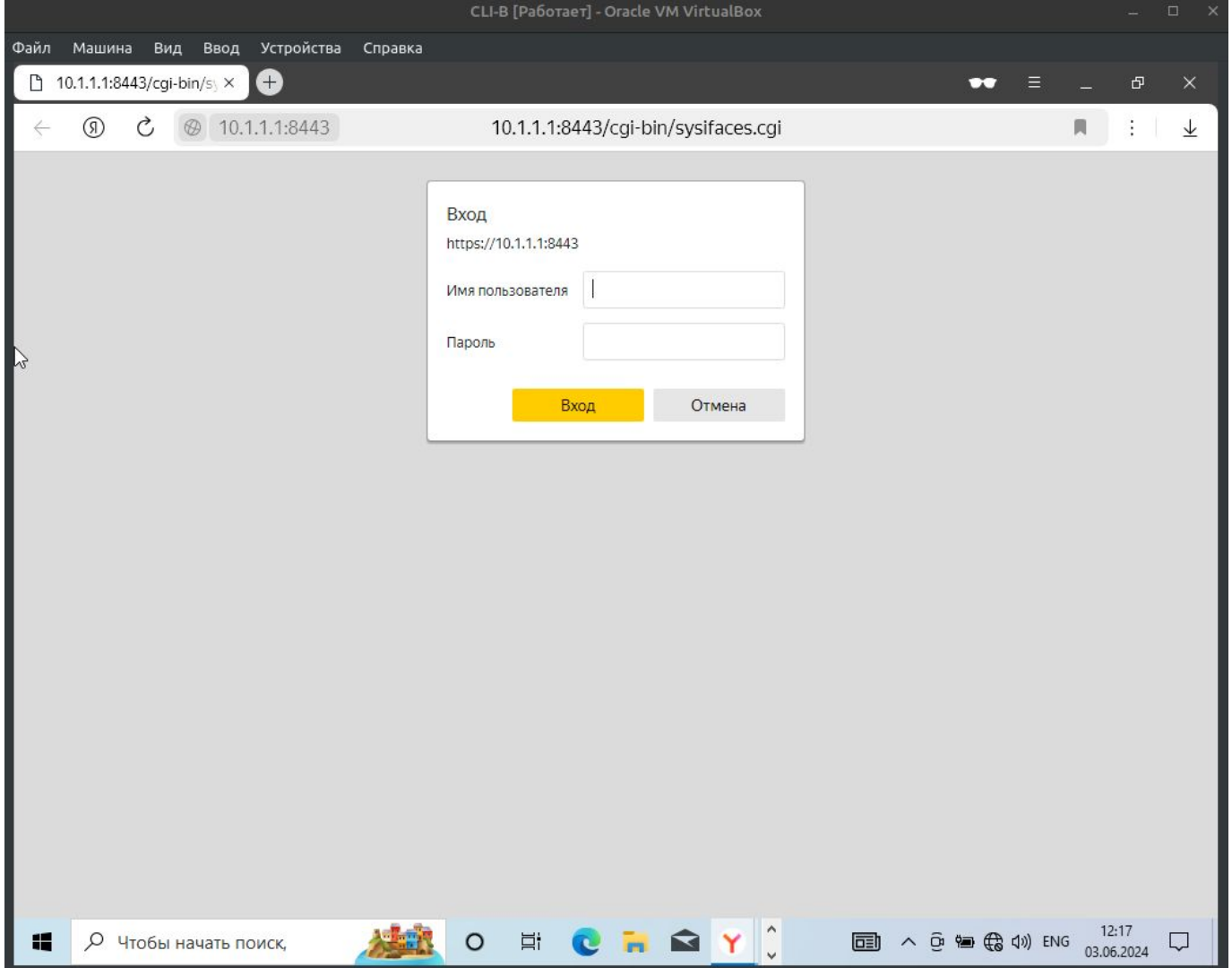
Дополнительная настройка РУБИКОН-К

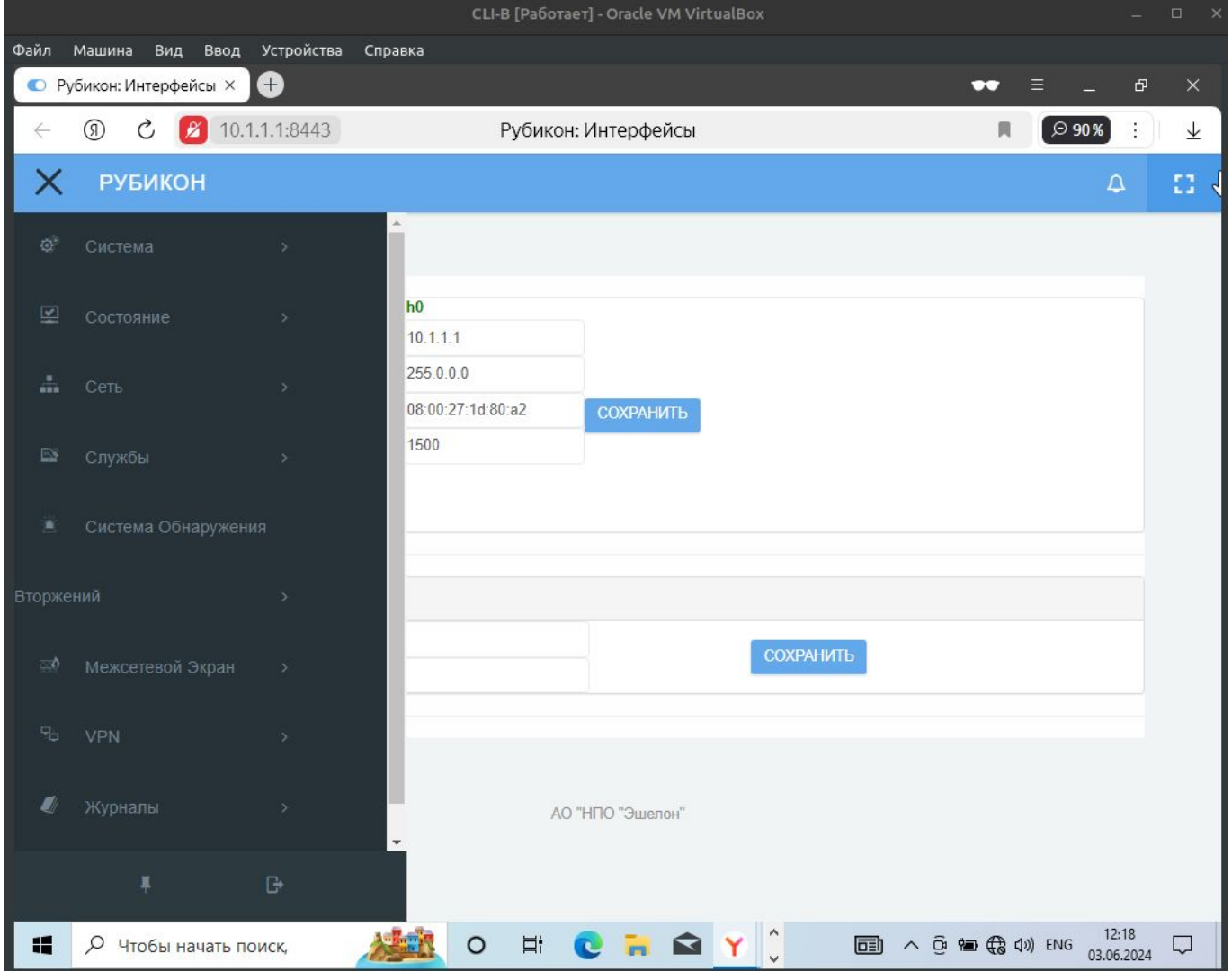
$ ifconfig eth1 up

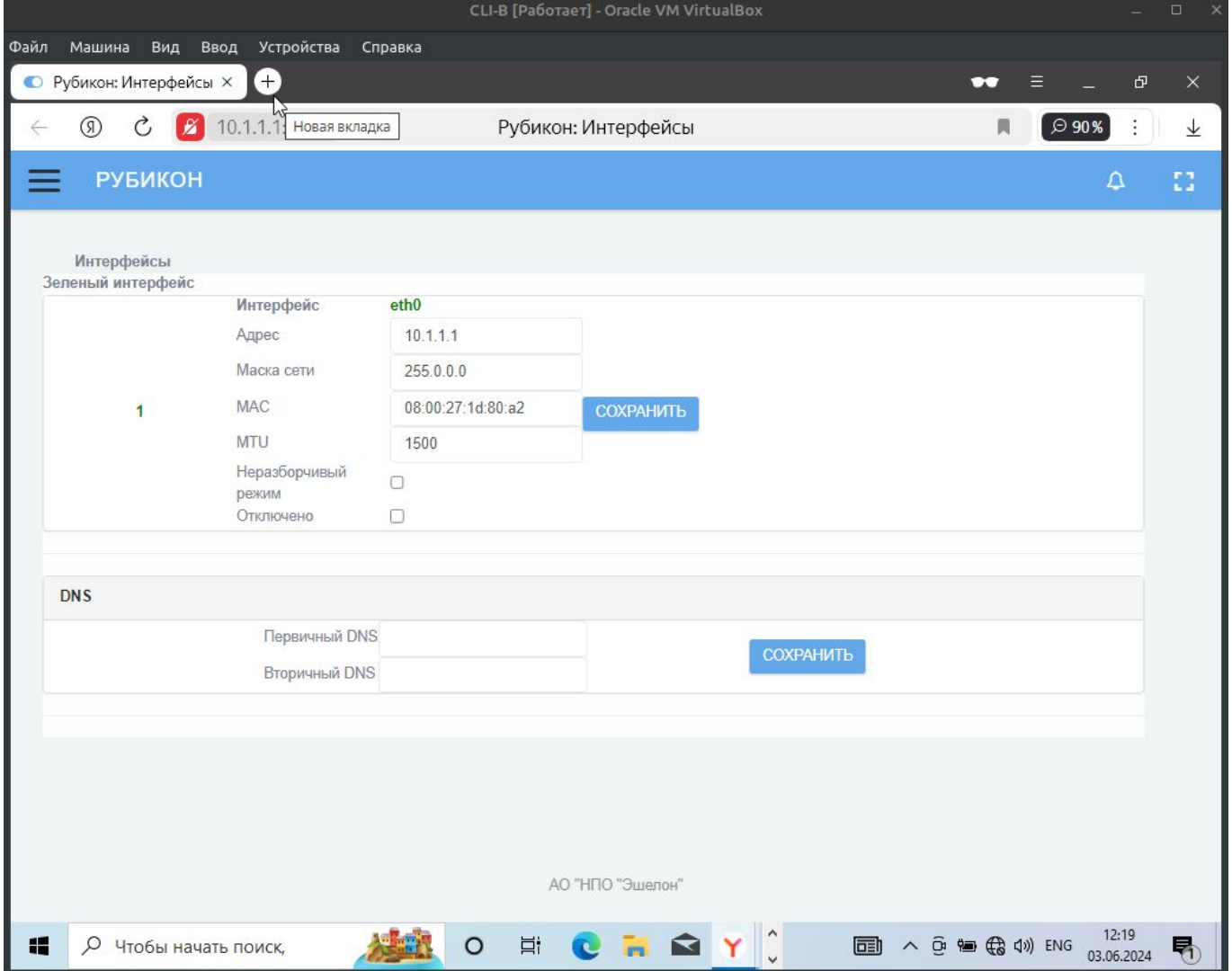
$ ifconfig eth1 192.168.1.100 netmask 255.255.255.0

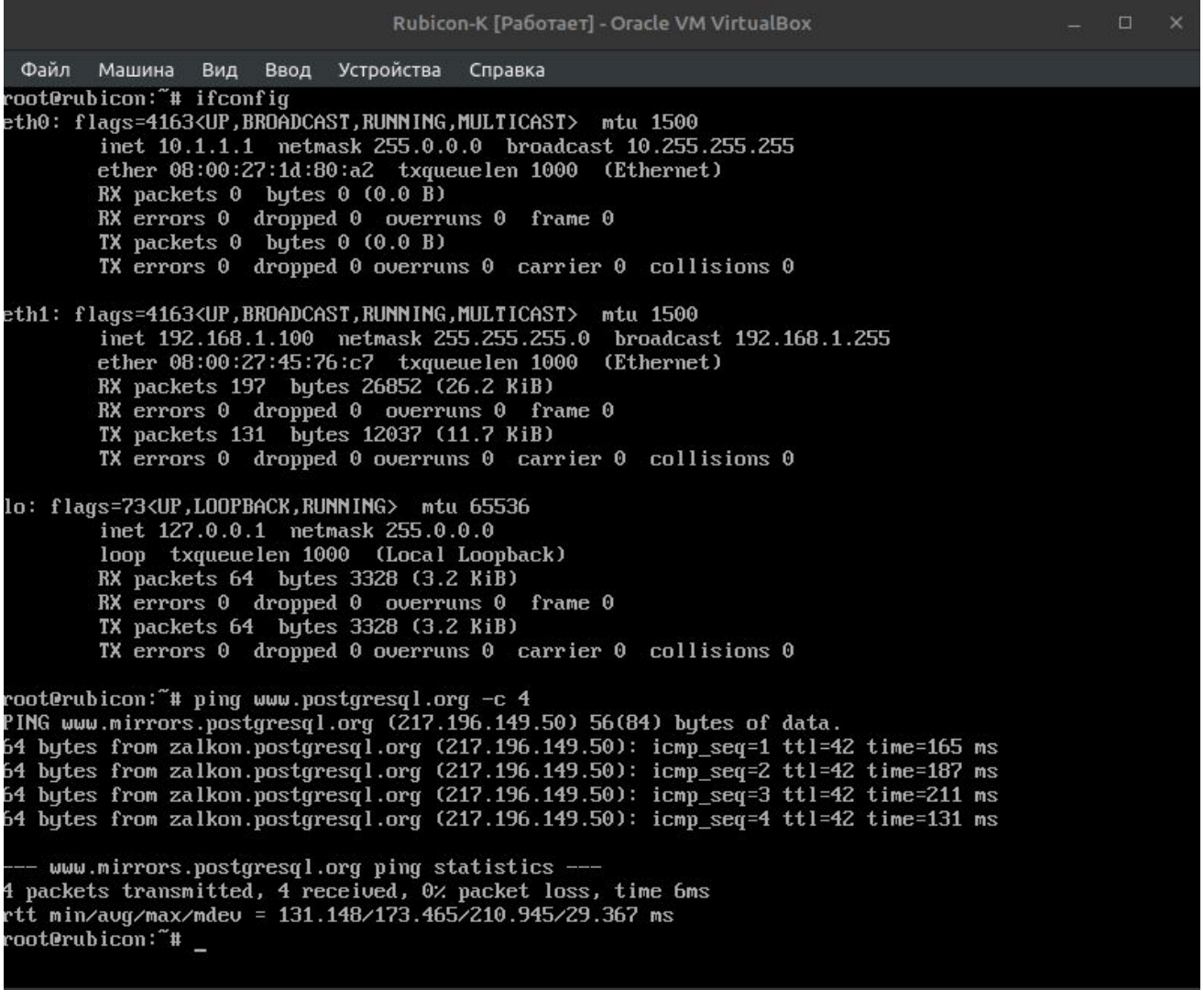
$ ip route add default via 192.168.1.1 dev eth1

$ echo "nameserver 192.168.1.1" >> /etc/resolv.conf


CLI-B [Работает] - Oracle VM VirtualBox
Файл Машина Вид Ввод Устройства Справка
10.1.1.1:8443/cgi-bin/sysifaces.cgi
Вход
https://10.1.1.1:8443
Имя пользователя
Пароль
Вход
Отмена
Чтобы начать поиск,
ENG
12:17
03.06.2024


CLI-B [Работает] - Oracle VM VirtualBox
Файл Машина Вид Ввод Устройства Справка
Рубикон: Интерфейсы
10.1.1.1:8443
Рубикон: Интерфейсы
90%
РУБИКОН
Система
Состояние
Сеть
Службы
Система Обнаружения
Вторжений
Межсетевой Экран
VPN
Журналы
h0
10.1.1.1
255.0.0.0
08:00:27:1d:80:a2
1500
СОХРАНИТЬ
СОХРАНИТЬ
АО "НПО "Эшелон"
Чтобы начать поиск,
ENG
12:18
03.06.2024


CLI-B [Работает] - Oracle VM VirtualBox
Файл Машина Вид Ввод Устройства Справка
Рубикон: Интерфейсы
10.1.1.1
Новая вкладка
Рубикон: Интерфейсы
90%
РУБИКОН
Интерфейсы
Зеленый интерфейс
Интерфейс eth0
Адрес 10.1.1.1
Маска сети 255.0.0.0
1
MAC 08:00:27:1d:80:a2
СОХРАНИТЬ
MTU 1500
Неразборчивый режим
Отключено
DNS
Первичный DNS
Вторичный DNS
СОХРАНИТЬ
АО "НПО "Эшелон"
Чтобы начать поиск,
ENG
12:19
03.06.2024


Rubicon-K [Работает] - Oracle VM VirtualBox
Файл Машина Вид Ввод Устройства Справка
root@rubicon:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 10.1.1.1 netmask 255.0.0.0 broadcast 10.255.255.255
ether 08:00:27:1d:80:a2 txqueuelen 1000 (Ethernet)
RX packets 0 bytes 0 (0.0 B)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 0 bytes 0 (0.0 B)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 192.168.1.100 netmask 255.255.255.0 broadcast 192.168.1.255
ether 08:00:27:45:76:c7 txqueuelen 1000 (Ethernet)
RX packets 197 bytes 26852 (26.2 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 131 bytes 12037 (11.7 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
loop txqueuelen 1000 (Local Loopback)
RX packets 64 bytes 3328 (3.2 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 64 bytes 3328 (3.2 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
root@rubicon:~# ping www.postgresql.org -c 4
PING www.mirrors.postgresql.org (217.196.149.50) 56(84) bytes of data.
64 bytes from zalkon.postgresql.org (217.196.149.50): icmp_seq=1 ttl=42 time=165 ms
64 bytes from zalkon.postgresql.org (217.196.149.50): icmp_seq=2 ttl=42 time=187 ms
64 bytes from zalkon.postgresql.org (217.196.149.50): icmp_seq=3 ttl=42 time=211 ms
64 bytes from zalkon.postgresql.org (217.196.149.50): icmp_seq=4 ttl=42 time=131 ms
--- www.mirrors.postgresql.org ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 6ms
rtt min/avg/max/mdev = 131.148/173.465/210.945/29.367 ms
root@rubicon:~# _

Сравнение РУБИКОН-К и Usergate

- «Usergate» поддерживает кластеризацию и отказоустойчивость, «РУБИКОН-К» — нет;
- «Usergate» позволяет объединять сетевые интерфейсы в группы, называемые «зонами»;
- «Usergate» позволяет объединять в общие группы номера телефонов, электронные адреса, сетевые интерфейсы, списки URL и приложения для более удобного их конфигурирования и использования;
- «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.

Выводы

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».

Ещё был получен опыт изучения официальных документаций.

Трудности

- 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;

- использованная комплектация «РУБИКОН-К» не поддерживает трансляцию сетевых адресов;

- в веб-интерфейсе «РУБИКОН-К» виден лишь один сетевой интерфейс.

Использованные источники

[1] Интернет-портал по информационной безопасности в сети — вторжение [Электронный ресурс]. URL: https://safe-surf.ru/glossary/ru/806/?sphrase_id=45961

[2] Интернет-портал по информационной безопасности в сети — система обнаружения вторжений [Электронный ресурс]. URL: https://safe-surf.ru/glossary/ru/1150/?sphrase_id=45963

[3] Интернет-портал по информационной безопасности в сети — система предотвращения вторжений [Электронный ресурс]. URL: https://safe-surf.ru/glossary/ru/1152/?sphrase_id=45966

[4] Интернет-портал по информационной безопасности в сети — межсетевой экран [Электронный ресурс]. URL: https://safe-surf.ru/glossary/ru/967/?sphrase_id=45967

[5] Энциклопедия «Касперского» - межсетевой экран нового поколения [Электронный ресурс]. URL: https://encyclopedia.kaspersky.ru/glossary/next-generation-firewall-ngfw/#:~:text=NGFW%20(Next%20Generation%20Firewall%2C%20межсетевой,блокировать%20трафик%20на%20уровне%20приложений

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