

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, научно-исследовательской работы (получение первичных
навыков научно-исследовательской работы)
(указывается наименование практики)

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

Тема задания: изучение межсетевых экранов следующего поколения «UserGate» в условиях реальной
эксплуатации

Место прохождения практики: ООО «Юзергейт», 630090, г. Новосибирск, ул. Николева, 11
(полное наименование организации и структурного подразделения, индекс, адрес)

Сроки прохождения практики: с 02.10.2023 г. по 22.12.2023 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

(Ф.И.О. полностью)

(должность)

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

Отчет заслушан на заседании кафедры компьютерных систем
(наименование кафедры)

протокол _____ от «_____» _____ 20____ г.

Новосибирск 2023

Оглавление

| | |
|--|-----------|
| Введение | 3 |
| 1. Предметная область | 5 |
| 2. Принципы работы «Usergate» | 5 |
| 3. Создание и использование «стендов» | 7 |
| Заключение | 9 |
| Список литературы | 10 |

Введение

Цель прохождения практики состояла в изучение межсетевых экранов следующего поколения «UserGate» в условиях реальной эксплуатации. Для достижения этой цели нужно было решить следующие задачи:

- изучить основы информационной безопасности, компьютерных сетей и основных интернет-протоколов;
- изучить принципы работы межсетевого экрана нового поколения «Usergate»;
- научиться создавать «стенды» в гипервизоре Oracle VM VirtualBox для эмуляции работы межсетевого экрана;
- научиться использовать «стенды» для решения проблем, возникших у клиентов, использующих «Usergate».

Актуальность темы межсетевых экранов следующего поколения существенна в современном мире технологий, так как постоянно открываются новые способы осуществления атак на компьютерные сети, в то время как межсетевые экраны позволяют защищаться от них. Межсетевые экраны следующего поколения же являются их «продолжением» и поэтому позволяют гораздо более эффективно защищаться от различных атак. Также помимо этого они позволяют настраивать инфраструктуру и топологию компьютерной сети, производить мониторинг и диагностику, что делает их инструментом не только для предотвращения атак, но и для администрирования компьютерных сетей.

Организация, Usergate, в которой проходила практика, является российским разработчиком программного обеспечения и микроэлектроники и обеспечивает своими решениями информационную безопасность корпоративных сетей самого разного размера от малого и среднего бизнеса до крупных корпораций с распределенной инфраструктурой. В группу компаний UserGate входят ООО «Юзергейт» (разработка программного обеспечения) и ООО «Катунь Электроника» (разработка в области микроэлектроники) [1].

Практика проходила в подразделении под названием «Tech support», которое занимается решением проблем, возникших у клиентов Usergate, посредством создания «стендов» и эмуляции возникших сбоев и ошибок.

Предполагаемые результаты прохождения данной практики описывает следующий список:

- понимание основ информационной безопасности, компьютерных сетей и основных интернет-протоколов;

- умение пользоваться современными гипервизорами (в том числе Oracle VM VirtualBox);
- умение администрировать межсетевые экраны следующего поколения «Usergate»;
- умение эмулировать ошибки и сбои в компьютерных сетях посредством использования «стендов».

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 [2]. Например, «брандмауэр» 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 — Next Generation Firewall) — 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 [3].

Межсетевой экран нового поколения — это комплексный инструмент, предназначенный для контроля трафика, управления доступом пользователей и приложений, предотвращения атак [4].

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

2. Принципы работы «Usergate»

«Usergate» является межсетевым экраном ¹ со следующими возможностями [5]:

- системы обнаружения вторжений (IDS/IPS);
- Advanced Threat Protection ² (Опция);
- доступ к внутренним ресурсам через SSL VPN Portal;

¹ Компания Usergate предоставляет как аппаратные, так и программные решения, однако в рамках практики работа происходила лишь с программным решением — виртуальным межсетевым экраном нового поколения.

² Advanced Threat Protection включает в себя фильтрацию по категориям URL Filtering 3.0, морфологический анализ контента, облачный антивирус, поддержку списков Роскомнадзора, модуль блокировки рекламы ADblock.

- анализ и выгрузка информации об инцидентах безопасности (SIEM);
- обратный прокси (Reverse proxy);
- автоматизация реакции на угрозы безопасности информации (SOAR);
- контроль Приложений L7;
- защита почты (Mail Security) ³ (Опция);
- контроль доступа в интернет;
- дешифрование SSL;
- гостевой портал;
- идентификация пользователей;
- виртуальная частная сеть (VPN);
- поддержка АСУ ТП (SCADA);
- удаленное администрирование;
- безопасная публикация внутренних ресурсов и сервисов;
- поддержка концепции BYOD (Bring Your Own Device);
- поддержка высокой отказоустойчивости и кластеризации.

То есть «Usergate» не только производит анализ и фильтрацию сетевого трафика, но ещё и позволяет организовывать инфраструктуру сети (например, он позволяет настраивать правила NAT, выступать в качестве DHCP-сервера), производить удалённое администрирование, мониторинг и диагностику трафика, управлять авторизацией пользователей, их правами и ролями.

³ Mail Security включает в себя антиспам, антивирусную проверку почты, поддержку методов фильтрации нежелательной почты.

3. Создание и использование «стендов»

«Usergate» как виртуальный межсетевой экран нового поколения представлен фактически операционной системой, которая может установлена из ISO-образа. ISO-образ можно импортировать в любом современном гипервизоре (например, OracleVM VirtualBox или VMware Workstation). В рамках практики использовался гипервизор OracleVM VirtualBox.

Для эмуляции работы компьютерной сети необходимо эмулировать всех хостов в сети. В рамках обучения стенд состоял из шести виртуальных машин:

- виртуальная машина с «Usergate» (**UTM** — **Unified Threat Management**);
- виртуальная машина на операционной системе Debian 12.4.0, эмулирующая интернет-провайдера (**ISP** — **Internet Service Provider**);
- виртуальная машина на операционной системе Windows Server 2012, эмулирующая сервер некоторой компании, находящийся в локальной сети компании (**DC** — **Data Center**);
- три виртуальные машины на операционной системе Windows-10, две из которых эмулируют клиентов, находящихся в локальной сети некоторой компании (**CLI-A** и **CLI-B**, **CLI** — **Client**), а третий — клиента вне локальной сети компании, но имеющего доступ к локальной сети с помощью Remote Access VPN (**CLI-EXT** — **Client External**).

Стоит отметить, что конфигурация «стенда» заключается не только в поиске и импорте в гипервизор нужных ISO-образов операционных систем. Для полноценной работы стенда необходимо: осуществить настройку сетевой топологии в самом гипервизоре (указать сколько каждая виртуальная машины будет иметь виртуальных сетевых интерфейсов и какого они будут типа), осуществить настройку каждой виртуальной машины по-отдельности.

CLI-A, **CLI-B** и **DC** имели лишь один виртуальный сетевой интерфейс каждая, при этом интерфейсы этих виртуальных машин находились в одной локальной сети (*LOCAL-NETWORK*)¹. **UTM** же имела 2 виртуальных интерфейса: один — в виртуальной локальной сети *LOCAL-NETWORK*, а второй — в виртуальной

¹ Они находились в виртуальной локальной сети гипервизора, но тем не менее они не имели прямого доступа к сетевому пространству операционной системы, на которой был запущен гипервизор.

локальной сети *ISP-NETWORK*. **ISP** имела 2 виртуальных интерфейса: один в виртуальной локальной сети *ISP-NETWORK*, а второй виртуальный интерфейс имел тип «bridge», что означает, что он имеет доступ к сетевому пространству «хостовой» операционной системы. **CLI-EXT** имела лишь один интерфейс, у которого был тип «bridge».

На **CLI-A** и **CLI-B** не было никаких настроек поскольку все нужны IP-адреса и доступ к интернету они получали от **UTM**. На **DC** нужно было установить и настроить необходимые сервисы (такие как «Active Directory», «DNS-Manager» и центр управления сертификатами), а все нужные IP-адреса и доступ в интернет виртуальная машина получала от **UTM**. На **ISP** были настроены правила NAT и статические маршруты для доступа в интернет. На **CLI-EXT** был настроен доступ к **UTM** с помощью VPN (указан IP-адрес нужного интерфейса **UTM** и тип подключения). На **UTM** были произведены следующие настройки:

- настроена фильтрация контента по протоколам, URL, IP-адресам клиентов;
- настроены captive-портал и способы авторизации (через captive-портал, «прозрачная» авторизация по протоколу Kerberos);
- настроен сбор диагностических данных;
- настроены сценарии при атаках;
- настроена проверка писем электронной почты на наличие «вирусов» по протоколу ICAP.

Данный «стенд» использовался в рамках обучения. После обучения создавались различные «стенды» для решения проблем, возникших у пользователей продуктов Usergate.

Заключение

В результате прохождения практики были изучены принципы работы меж-
сетевого экрана следующего поколения «Usergate» и способы его администри-
рования. Также были получены навыки в создании «стендов» в гипервизоре
OracleVM VirtualBox для эмуляции работы компьютерных сетей и межсетевых
экранов.

Также был получен опыт работы с литературными источниками и выделения
необходимой и полезной информации, а также опыт работы в крупной россий-
ской компании наряду с её штатными сотрудниками.

В течение прохождения практики пришлось столкнуться с двумя трудностями:
трудность в работе с гипервизором OracleVM VirtualBox (а именно, настрой-
ке сетевой топологии); трудность в понимании принципов работы «Usergate»
ввиду многоплановости и сложности данного продукта.

Список литературы

- [1] *О компании UserGate [Электронный ресурс]*. URL: <https://www.usergate.com/ru/company/about-us>.
- [2] *Интернет-портал по информационной безопасности в сети [Электронный ресурс]*. URL: https://safe-surf.ru/glossary/ru/967/?sphrase_id=45658.
- [3] *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](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).
- [4] *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](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).
- [5] *Возможности виртуального межсетевого экрана «Usergate» [Электронный ресурс]*. URL: <https://www.usergate.com/ru/products/usergate-vm>.