Отчёт

о прохождении учебной практики, научно-исследовательской работы (получение первичных навыков научно-исследовательской работы)

Изучение межсетевых экранов следующего поколения «UserGate» в условиях реальной эксплуатации

Выполнил: Кондренко Кирилл Павлович

Руководитель практики: Пестунова Тамара Михайловна

Новосибирск 2023

Введение

Цель: изучить межсетевые экраны следующего поколения «UserGate» в условиях реальной эксплуатации.

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».

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. [1]

Межсетевой экран нового поколения (**NGFW** — **N**ext **G**eneration **F**ire**w**all) — межсетевой экран для глубокой фильтрации трафика, интегрированный с **IDS** (**I**ntrusion **D**etection **S**ystem, система обнаружения вторжений) или **IPS** (**I**ntrusion **P**revention **S**ystem, система предотвращения вторжений) и обладающий возможностью контролировать и блокировать трафик на уровне приложений. [2]

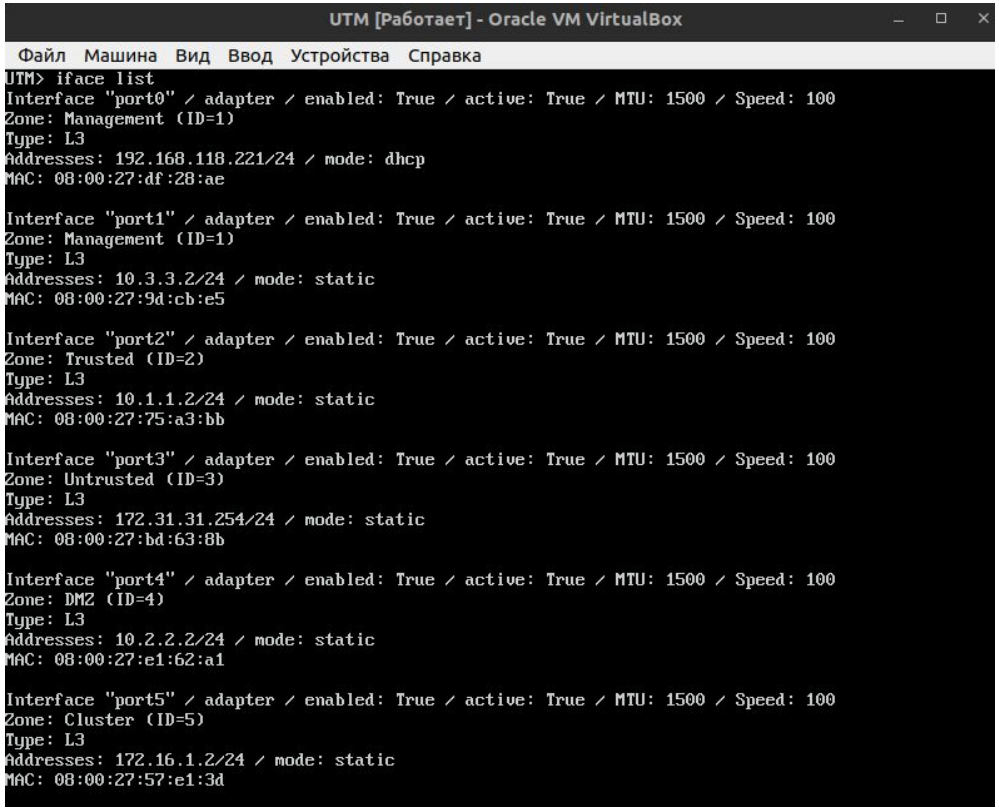
Межсетевой экран нового поколения — это комплексный инструмент, предназначенный для контроля трафика, управления доступом пользователей и приложений, предотвращения атак. [3]

Принципы работы «Usergate»

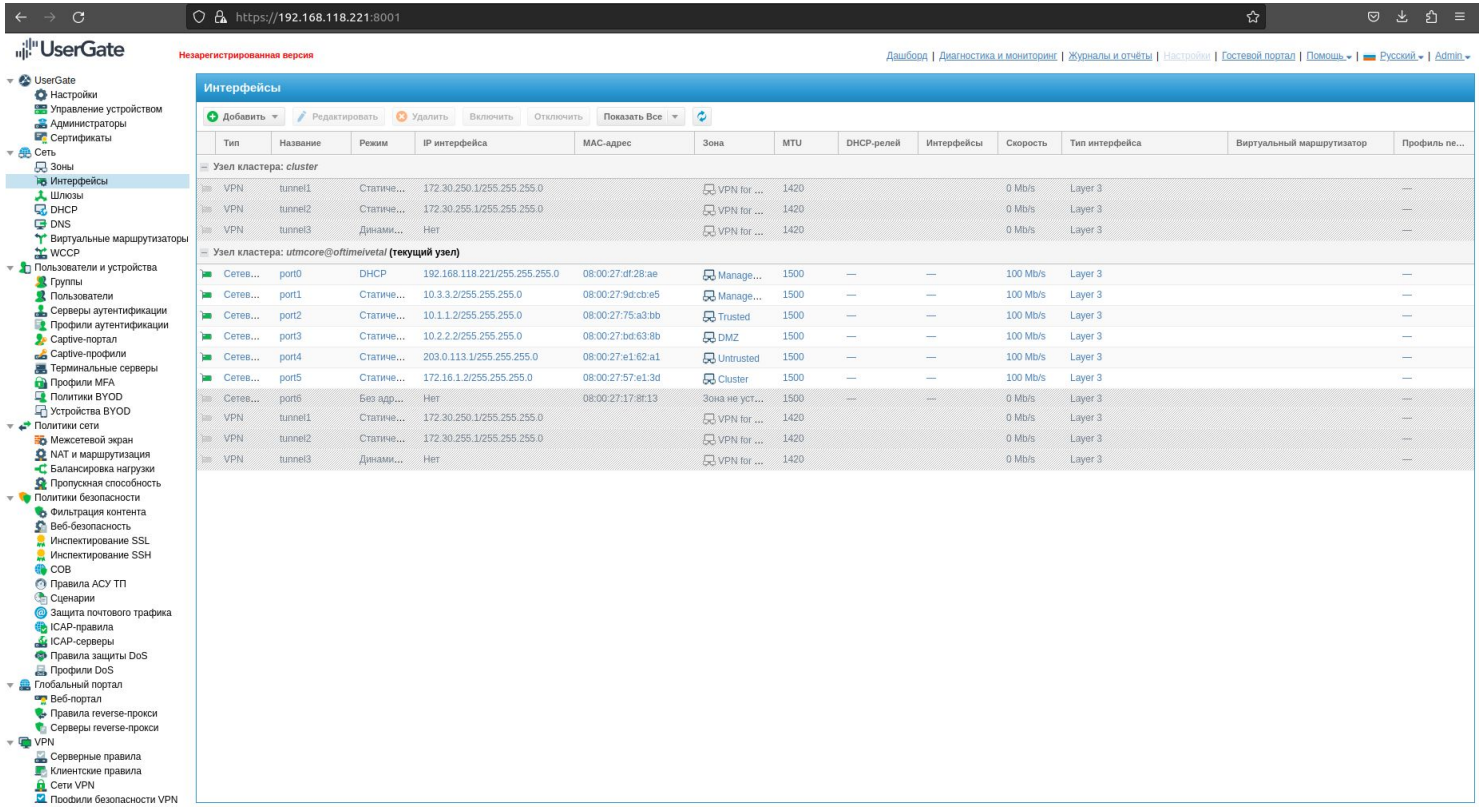
Возможности «Usergate» [4]:

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

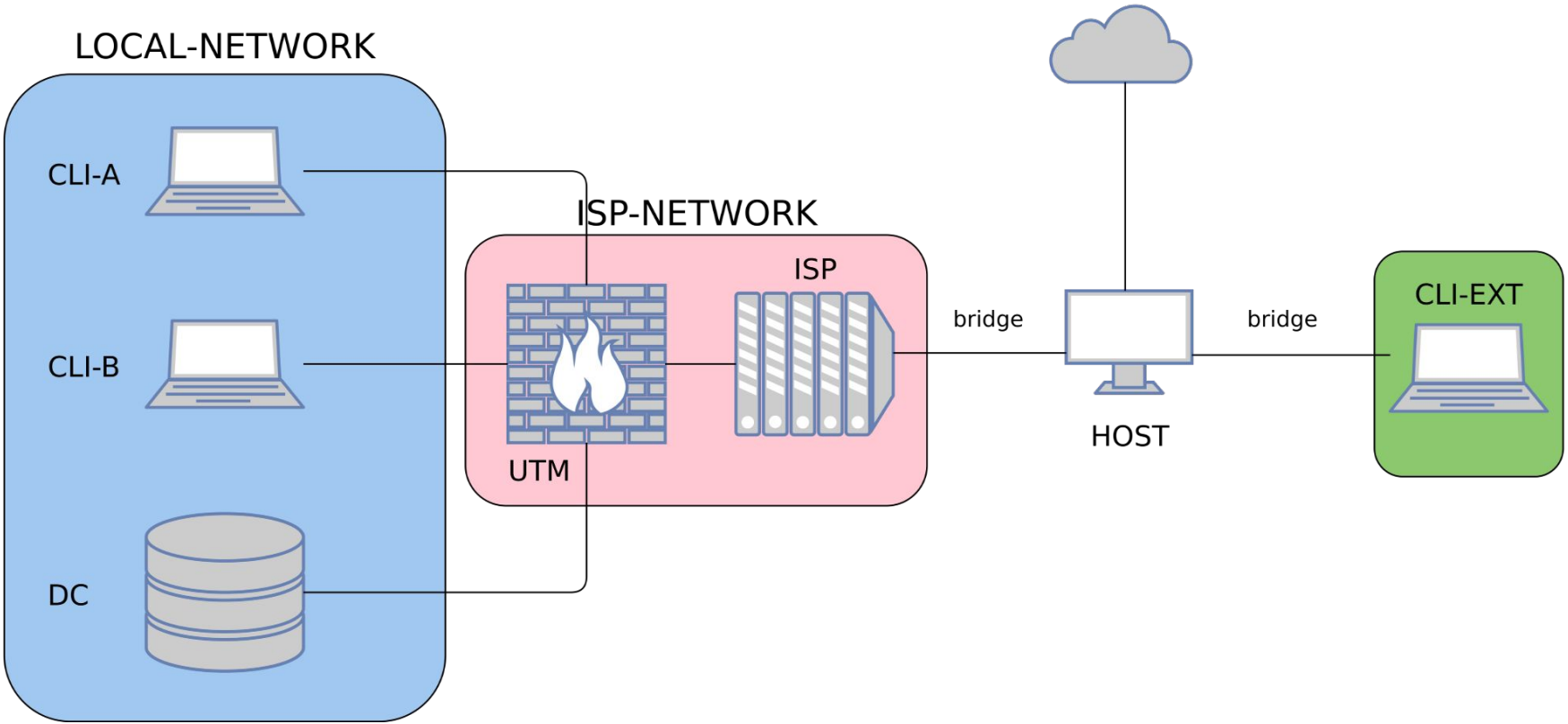
Принципы работы «Usergate»



Принципы работы «Usergate»



Создание и использование «стендов»



Создание и использование «стендов». Настройки

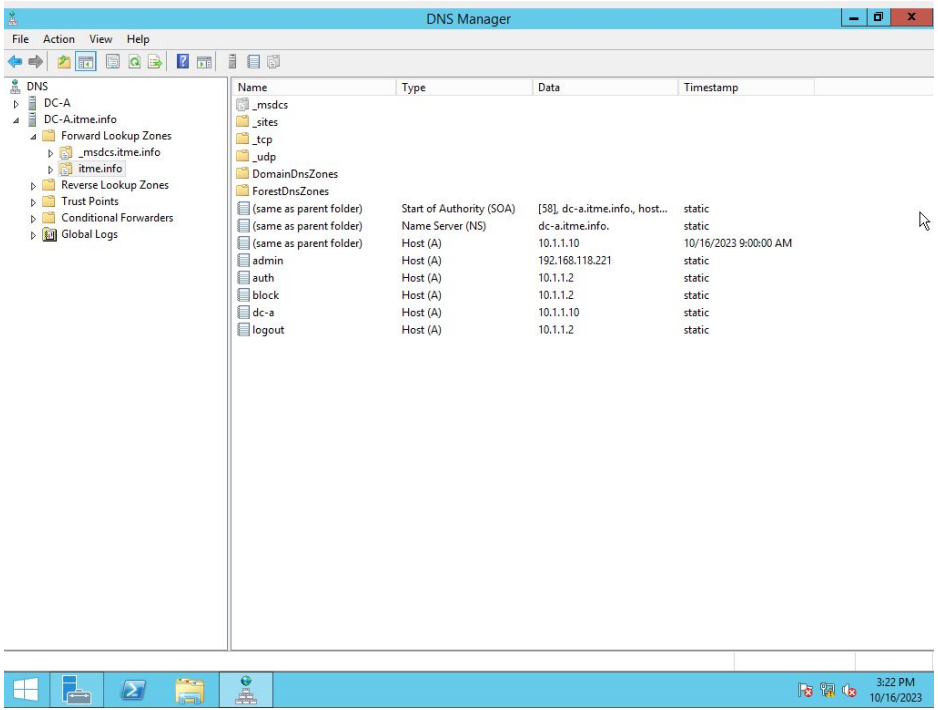
DC: «Active Directory», «DNS-Manager», центр управления сертификатами.

ISP: NAT, статические маршруты.

CLI-EXT: подключение к UTM через VPN.

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

Создание и использование «стендов». Настройки



Заключение

Были изучены принципы работы межсетевого экрана следующего поколения «Usergate» и способы его администрирования. Также были получены навыки в создании «стендов» в гипервизоре OracleVM VirtualBox для эмуляции работы компьютерных сетей и межсетевых экранов.

Был получен опыт работы с литературными источниками и выделения необходимой и полезной информации, а также опыт работы в крупной российской компании наряду с её штатными сотрудниками.

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

Список литературы

[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%D%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] Возможности виртуального межсетевого экрана «Usergate» [Электронный ресурс]. URL: https://www.usergate.com/ru/products/usergate-vm.