

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

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 меж сетевого экрана нового поколения «Usergate»;
- научиться создавать «стенды» в гипервизоре Oracle VM VirtualBox для эмуляции работы меж сетевого экрана;
- научиться использовать «стенды» для решения проблем, возникших у клиентов, использующих «Usergate».

Предметная область

Межсетевой экран (FW — Firewall) — 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 — 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. [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»

```
UTM [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка
UTM> iface list
Interface "port0" / adapter / enabled: True / active: True / MTU: 1500 / Speed: 100
Zone: Management (ID=1)
Type: L3
Addresses: 192.168.118.221/24 / mode: dhcp
MAC: 08:00:27:df:28:ae

Interface "port1" / adapter / enabled: True / active: True / MTU: 1500 / Speed: 100
Zone: Management (ID=1)
Type: L3
Addresses: 10.3.3.2/24 / mode: static
MAC: 08:00:27:9d:cb:e5

Interface "port2" / adapter / enabled: True / active: True / MTU: 1500 / Speed: 100
Zone: Trusted (ID=2)
Type: L3
Addresses: 10.1.1.2/24 / mode: static
MAC: 08:00:27:75:a3:bb

Interface "port3" / adapter / enabled: True / active: True / MTU: 1500 / Speed: 100
Zone: Untrusted (ID=3)
Type: L3
Addresses: 172.31.31.254/24 / mode: static
MAC: 08:00:27:bd:63:8b

Interface "port4" / adapter / enabled: True / active: True / MTU: 1500 / Speed: 100
Zone: DMZ (ID=4)
Type: L3
Addresses: 10.2.2.2/24 / mode: static
MAC: 08:00:27:e1:62:a1

Interface "port5" / adapter / enabled: True / active: True / MTU: 1500 / Speed: 100
Zone: Cluster (ID=5)
Type: L3
Addresses: 172.16.1.2/24 / mode: static
MAC: 08:00:27:57:e1:3d
```

Принципы работы «Usergate»

← → ↻ <https://192.168.118.221:8001> ☆ ⌵ ⌵ ⌵ ⌵

UserGate Незарегистрированная версия [Дашборд](#) | [Диагностика и мониторинг](#) | [Журналы и отчёты](#) | [Настройки](#) | [Гостевой портал](#) | [Помощь](#) | [Русский](#) | [Admin](#)

UserGate

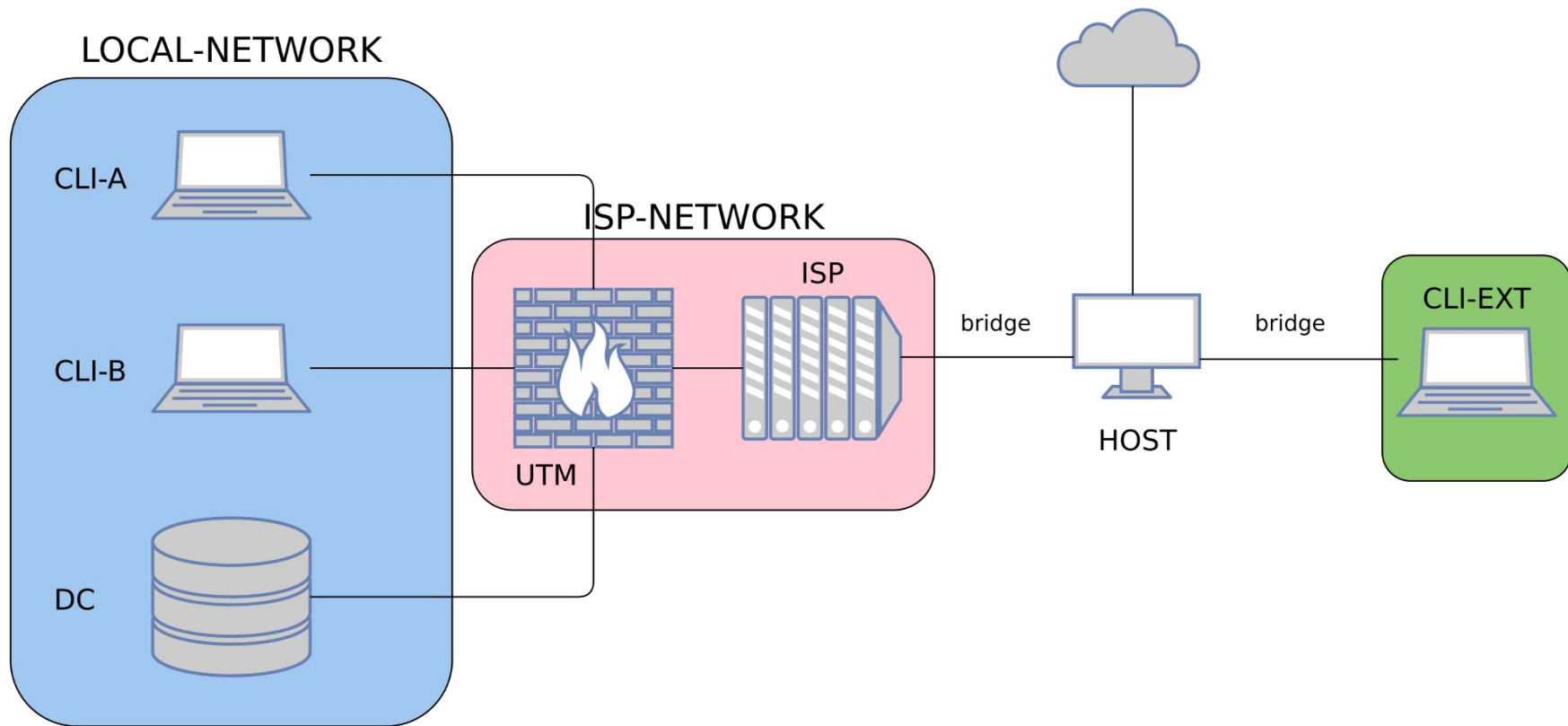
- Настройки
 - Управление устройством
 - Администраторы
 - Сертификаты
- Сеть
 - Зоны
 - Интерфейсы
 - Шлюзы
 - DHCP
 - DNS
 - Виртуальные маршрутизаторы
 - WCCP
- Пользователи и устройства
 - Группы
 - Пользователи
 - Серверы аутентификации
 - Профили аутентификации
 - Сaptive-портал
 - Сaptive-профили
 - Терминальные серверы
 - Профили MFA
 - Политии BYOD
 - Устройства BYOD
- Политии сети
 - Межсетевой экран
 - NAT и маршрутизация
 - Балансировка нагрузки
 - Пропускная способность
- Политии безопасности
 - Фильтрация контента
 - Веб-безопасность
 - Инспектирование SSL
 - Инспектирование SSH
 - СОВ
 - Правила ACU TP
 - Сценарии
 - Защита почтового трафика
 - ICAP-правила
 - ICAP-серверы
 - Правила защиты DoS
 - Профили DoS
- Глобальный портал
 - Веб-портал
 - Правила reverse-прокси
 - Серверы reverse-прокси
- VPN
 - Серверные правила
 - Клиентские правила
 - Сети VPN
 - Политии безопасности VPN

Интерфейсы

[Добавить](#) [Редактировать](#) [Удалить](#) [Включить](#) [Отключить](#) [Показать Все](#)

Тип	Название	Режим	IP интерфейса	MAC-адрес	Зона	MTU	DHCP-релей	Интерфейсы	Скорость	Тип интерфейса	Виртуальный маршрутизатор	Профиль пе...
Узел кластера: cluster												
VPN	tunnel1	Статиче...	172.30.250.1/255.255.255.0		VPN for ...	1420			0 Mb/s	Layer 3		
VPN	tunnel2	Статиче...	172.30.255.1/255.255.255.0		VPN for ...	1420			0 Mb/s	Layer 3		
VPN	tunnel3	Динами...	Нет		VPN for ...	1420			0 Mb/s	Layer 3		
Узел кластера: utmcore@offtimeiveta (текущий узел)												
Сетев...	port0	DHCP	192.168.118.221/255.255.255.0	08:00:27:df:28:a6	Manage...	1500	—	—	100 Mb/s	Layer 3		
Сетев...	port1	Статиче...	10.3.3.2/255.255.255.0	08:00:27:9d:cb:e5	Manage...	1500	—	—	100 Mb/s	Layer 3		
Сетев...	port2	Статиче...	10.1.1.2/255.255.255.0	08:00:27:75:a3:bb	Trusted	1500	—	—	100 Mb/s	Layer 3		
Сетев...	port3	Статиче...	10.2.2.2/255.255.255.0	08:00:27:bd:63:8b	DMZ	1500	—	—	100 Mb/s	Layer 3		
Сетев...	port4	Статиче...	203.0.113.1/255.255.255.0	08:00:27:e1:62:a1	Untrusted	1500	—	—	100 Mb/s	Layer 3		
Сетев...	port5	Статиче...	172.16.1.2/255.255.255.0	08:00:27:57:e1:3d	Cluster	1500	—	—	100 Mb/s	Layer 3		
Сетев...	port6	Без адр...	Нет	08:00:27:17:8f:13	Зона не уст...	1500	—	—	0 Mb/s	Layer 3		
VPN	tunnel1	Статиче...	172.30.250.1/255.255.255.0		VPN for ...	1420			0 Mb/s	Layer 3		
VPN	tunnel2	Статиче...	172.30.255.1/255.255.255.0		VPN for ...	1420			0 Mb/s	Layer 3		
VPN	tunnel3	Динами...	Нет		VPN for ...	1420			0 Mb/s	Layer 3		

Создание и использование «стендов»



Создание и использование «стендов».

Настройки

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

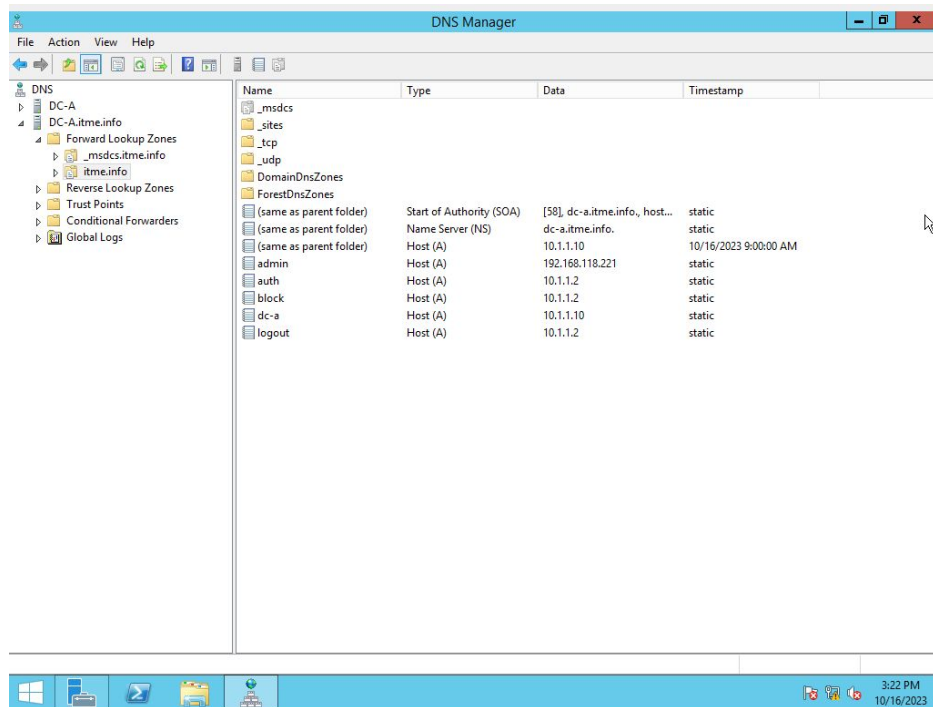
ISP: NAT, статические маршруты.

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%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).

[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](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>.