uAcademy

Поиск и устранение неисправностей в работе межсетевых экранов UserGate

Программа курса

О курсе

Код курса	UG.TSHOOT
Версия курса	1.0
Версия uOS	7.4
Длительность курса	5 дней / 40 академических часов
Описание	Интенсивный практический курс для системных/сетевых администраторов и инженеров по информационной безопасности, которые уже знакомы с базовой эксплуатацией UserGate NGFW и хотят научиться быстро диагностировать, локализовывать и устранять реальные проблемы в работе NGFW.
Аудитория	Опытные сетевые администраторы, инженеры по безопасности, администраторы UserGate (NGFW).
Предварительные требования	▪ уверенные знания TCP/IP, статической и динамической маршрутизации, NAT, сетевых протоколов (HTTP, TLS, DNS, ICMP); ▪ опыт эксплуатации межсетевого экрана UserGate и базовая работа с CLI; ▪ навыки работы с системными инструментами: dig/nslookup, tcpdump/Wireshark, curl, анализом системных логов; ▪ понимание принципов HA-кластеризации и VLAN; ▪ знания в рамках программы курсов «Введение в сетевую безопасность на базе продуктов UserGate» и «Администрирование межсетевых экранов UserGate NGFW 7.X»; ▪ понимание работы протоколов OSPF, BGP, SNMP.

Программа курса

1

Методы устранения неисправностей:

- системный подход к диагностике сетевых неисправностей;
- принципы диагностики;
- методологии устранения сетевых неисправностей;
- распространённые подходы к диагностике сетевых неисправностей;
- использование процедур устранения неисправностей;
- рекомендуемые практики планового обслуживания сетевого оборудования.

2

Инструменты устранения неисправностей:

- расширенный поиск в разделе «Политики сети»;
- раздел «Диагностика и мониторинг»;
- средства анализа трафика;
- средства просмотра логов;
- системные журналы устройств UserGate;
- поиск и фильтрация данных в журналах;
- использование команды с URL.

3

Установка и развёртывание ПАК и виртуального решения:

- установка ПАК;
- развёртывание виртуального решения;
- первоначальное подключение к устройству.

Лабораторная работа 3.1. «Коммутация и роли виртуальных машин»

4

Первоначальная конфигурация, активация лицензии:

- настройка port0;
- инициализация устройства;
- активация лицензии;
- настройки, необходимые для онлайн-активации лицензии;
- настройка синхронизации времени.

Лабораторная работа 4.1. «Топология стенда»

5

Кластеры:

- кластер конфигурации;
- кластер отказоустойчивости.

Лабораторная работа 5.1. «Знакомство со стендом. Восстановление доступа к центральному NGFW»

6

Настройки сети:

- зоны;
- физические интерфейсы;
- логические интерфейсы;
- шлюзы;
- виртуальные маршрутизаторы;
- DHCP;
- DNS.

Лабораторная работа 6.1. «Базовая настройка NGFW в филиале»

7

Политики сети:

- библиотеки: локальные и обновляемые;
- межсетевой экран;
- SNAT, NoNAT;
- DNAT и Port Forwarding;
- Policy-Based Routing;
- MultiWAN, MultiWAN в кластере;
- балансировка нагрузки;
- пропускная способность.

Лабораторная работа 7.1. «Отказоустойчивость сети и доступность устройств»

Лабораторная работа 7.2. «Политики сети»

Лабораторная работа 7.3. «Multihome, NAT»

8

Анализ приложений, СОВ:

- анализ приложений L7;
- система обнаружения вторжений.

Лабораторная работа 8.1. «Анализ приложений L7»

9

Сертификаты:

- локальный удостоверяющий центр;
- корпоративный удостоверяющий центр;
- инспектирование SSL.

Лабораторная работа 9.1. «Сертификаты, инспектирование SSL»

10

Идентификация пользователей:

- локальные пользователи;
- серверы аутентификации и профили аутентификации;
- Captive-портал;
- технология UserID;
- идентификация администраторов. Права доступа администраторов.

Лабораторная работа 10.1. «Ролевая модель администрирования»

Лабораторная работа 10.2. «UserID, WEC»

Лабораторная работа 10.3. «Гостевая сеть, авторизация с помощью captive-портала»

11

Маршрутизация:

- статическая маршрутизация;
- динамическая маршрутизация. OSPF;
- динамическая маршрутизация. BGP;
- динамическая маршрутизация. BFD.

Лабораторная работа 11.1. «Маршрутизация BGP и COB»

Лабораторная работа 11.2. «Маршрутизация OSPF»

12

Политики безопасности:

- прокси прозрачный и явный;
- фильтрация контента.

Лабораторная работа 12.1. «Политики безопасности»

13

VPN:

- Методы диагностики VPN.

Лабораторная работа 13.1. «VPN Site-to-Site»

14

Мониторинг и оповещения.

Лабораторная работа 14.1. «Мониторинг системы и бэкап конфигурации»

uAcademy