

Длительность: 5 дней

Администрирование межсетевых экранов UserGate NGFW 7.X (UG.NGFW7 I)

Аудитория

- Курс предназначен для системных инженеров и специалистов в области информационной безопасности, которым необходимо получить знания и навыки по работе с межсетевыми экранами UserGate NGFW 7.X.

Требования

Для эффективного обучения на курсе слушатели должны обладать следующими знаниями и навыками:

- Знание сетевых моделей ISO/OSI и TCP/IP
- Знание основных сетевых протоколов: IP, TCP, UDP, DNS, DHCP, HTTP, HTTPS, FTP, SSH и других
- Понимание принципов IP-маршрутизации: статической и динамической, IP-адресации, масок подсети, шлюза по умолчанию
- Базовое понимание аутентификации, авторизации и соответствующих протоколов
- Понимание концепций межсетевого экранирования
- Опыт работы с Windows и/или Linux
- Базовое понимание PKI и цифровых сертификатов
- Опыт работы в командной строке — желательно

Цели

Уметь:

- устанавливать систему и выполнять первоначальную настройку;
- создавать кластеры конфигурации и отказоустойчивости;
- настраивать правила межсетевого экрана и NAT;
- формировать политику безопасности, в том числе с инспектированием SSL;
- настраивать контроль доступа пользователей;
- разворачивать VPN-туннели разных типов;
- вести журналирование с помощью UserGate Log Analyzer

Содержание

Курс посвящён установке и настройке межсетевых экранов UserGate NGFW на операционной системе uOS 7.X

Программа

1. Внедрение межсетевого экрана UserGate NGFW

1.1. Обзор межсетевых экранов UserGate NGFW

1.2. Установка ПАК и развёртывание виртуальной платформы

1.3. Интерфейсы администратора

1.4. Лицензирование и обновления

Лабораторная работа 1.1 «Знакомство с лабораторным стендом»

2. Базовая настройка

2.1. Ролевая модель доступа администраторов

2.2. Концепция зон и параметры настройки зон

2.3. Сетевые интерфейсы

2.4. Маршрут по умолчанию (шлюз)

2.5. Сетевая диагностика

Лабораторная работа 2.1 «Внедрение и базовая настройка межсетевого экрана»

- первоначальная настройка межсетевого экрана
- настройка базовых параметров и активация лицензии
- создание локального администратора
- базовая настройка устройства в филиале

3. Кластеры

3.1. Кластер конфигурации

3.2. Кластер отказоустойчивости

Лабораторная работа 3.1 «Кластер межсетевых экранов»

- кластер конфигурации
- кластер отказоустойчивости
- первоначальная настройка политик сети

4. Сетевая конфигурация

4.1. Статическая маршрутизация

4.2. Динамическая маршрутизация (OSPF)

4.3. Сетевые сервисы

4.4. Подключение системы хранения журналов UserGate LogAn

Лабораторная работа 4.1 «Маршрутизация»

- статическая маршрутизация
- протокол OSPF

Лабораторная работа 4.2 «Сетевые сервисы»

- настройка DNS и DHCP
- подключение UserGate LogAn

5. Политики сети

5.1. Обработка трафика на NGFW

5.2. Библиотеки элементов

5.3. Правила межсетевого экрана

5.4. Идентификация приложений

5.5. Система обнаружения вторжений (COB)

5.6. Работа с журналами

5.7. Правила трансляции сетевых адресов (NAT) и маршрутизации (PBR)

Лабораторная работа 5.1 «Политики сети»

- работа с библиотеками
- правила межсетевого экрана
- правила трансляции адресов

6. Инспектирование SSL

6.1. Обзор криптографических алгоритмов и PKI

6.2. Работа с цифровыми сертификатами

6.3. Правила инспектирования SSL

Лабораторная работа 6.1 «Инспектирование трафика SSL»

- работа с цифровыми сертификатами
- инспектирование SSL

7. Обзор политик безопасности

7.1. Компоненты политик безопасности

7.2. Обработка трафика при включённых функциях политик безопасности на NGFW

7.3. Работа с правилами контентной фильтрации

Лабораторная работа 7.1 «Базовая политика безопасности»

- Фильтрация контента

8. Идентификация пользователей

8.1. Компоненты идентификации пользователей

8.2. Локальные пользователи

8.3. Серверы аутентификации

8.4. Технология UserID

Лабораторная работа 8.1 «Идентификация пользователей»

- локальные пользователи
- технология UserID

9. Технологии VPN

9.1. Обзор технологий VPN

9.2. Настройка VPN-туннелей сайт–сайт

9.3. Настройка VPN-туннелей удалённого доступа

Лабораторная работа 9.1 «Настройка VPN-туннеля сайт-сайт»

- настройка IKEv2 VPN-туннеля сайт–сайт
- настройка L2TP/IPsec VPN-туннеля сайт–сайт (опциональное задание)

Лабораторная работа 9.2 «Настройка VPN-туннеля удалённого доступа»

- настройка IKEv2 VPN-туннеля удалённого доступа
- настройка L2TP/IPsec VPN-туннеля удалённого доступа (опциональное задание)

10. Мониторинг работы системы и обслуживание

10.1. Средства мониторинга

10.2. Оповещения и SNMP

10.3. Журналы и отчёты

10.4. Резервное копирование

10.5. Техническая поддержка и устранение неисправностей

Лабораторная работа 10.1 «Мониторинг, журналы, отчётность»

- Средства диагностики и мониторинга

- Журналы и отчёты

11. Обзор экосистемы UserGate SUMMA (опциональный материал)

11.1. Обзор компонентов экосистемы

11.2. Функции UserGate Management Center

11.3. Обзор UserGate WAF

11.4. Обзор UserGate SIEM

11.5. Обзор UserGate Client

11.6. Профессиональные сервисы

12. Лабораторная работа 12.1. «Итоговая самостоятельная практическая работа» (опциональная лабораторная работа)