uAcademy

Администрирование межсетевых экранов UserGate NGFW 7.X

Программа курса

О курсе

Код курса	UG.NGFW7 I
Версия курса	1.0
Версия uOS	7.4
Длительность курса	5 дней / 40 академических часов
Описание	В данном курсе рассматривается установка и конфигурирование межсетевых экранов UserGate NGFW, работающих под управлением операционной системы uOS 7.X. Вы научитесь выполнять установку и первоначальную настройку системы, создавать кластеры конфигурации и отказоустойчивости, настраивать правила межсетевого экрана и трансляции адресов, формировать политику безопасности, включающую в себя инспектирование SSL, внедрять механизмы контроля доступа пользователей, обеспечивать работу различных типов VPN-туннелей. В курсе также рассматривается журналирование с использованием UserGate Log Analyzer.
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.
Предварительные требования	▪ знания сетевых моделей ISO/OSI и TCP/IP; ▪ знания основных сетевых протоколов: IP, TCP, UDP, DNS, DHCP, HTTP, HTTPS, FTP, SSH и других; ▪ знания принципов работы протокола IP и IP-маршрутизации (статическая и динамическая маршрутизация, шлюз по умолчанию, IP-адресация, маска подсети); ▪ базовые знания процессов аутентификации и авторизации и соответствующих протоколов; ▪ понимание концепций межсетевого экранирования; ▪ опыт работы с операционными системами на базе Windows и/или Linux; ▪ опыт работы в командной строке (желательно).

Программа курса

1

Внедрение межсетевого экрана UserGate NGFW

- Обзор межсетевых экранов UserGate NGFW
- Установка ПАК и развёртывание виртуальной платформы
- Интерфейсы администратора
- Лицензирование и обновления

Лабораторная работа 1.1. «Знакомство с лабораторным стендом»

2

Базовая настройка

- Ролевая модель доступа администраторов
- Концепция зон и параметры настройки зон
- Сетевые интерфейсы
- Маршрут по умолчанию (шлюз)
- 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

- Кластер конфигурации
- Кластер отказоустойчивости

Лабораторная работа 3.1. «Кластер межсетевых экранов»

- Кластер конфигурации
- Кластер отказоустойчивости
- Первоначальная настройка политик сети

Программа курса предварительная, могут быть внесены незначительные изменения.

4

Сетевая конфигурация

- Статическая маршрутизация
- Динамическая маршрутизация (OSPF)
- Сетевые сервисы
- 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

- Обработка трафика на NGFW
- Библиотеки элементов
- Правила межсетевого экрана
- Идентификация приложений
- Система обнаружения вторжений (СОВ)
- Работа с журналами
- 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

- Обзор криптографических алгоритмов и PKI
- Работа с цифровыми сертификатами
- Правила инспектирования SSL

Лабораторная работа 6.1. «Инспектирование трафика SSL»

- Работа с цифровыми сертификатами
- Инспектирование SSL

7

Обзор политик безопасности

- Компоненты политик безопасности
- Обработка трафика при включённых функциях политик безопасности на NGFW
- Работа с правилами контентной фильтрации

Лабораторная работа 7.1. «Базовая политика безопасности»

- Фильтрация контента

Программа курса предварительная, могут быть внесены незначительные изменения.

8

Идентификация пользователей

- Компоненты идентификации пользователей
- Локальные пользователи
- Серверы аутентификации
- Технология UserID

Лабораторная работа 8.1. «Идентификация пользователей»

- Локальные пользователи
- Технология UserID

9

Технологии VPN

- Обзор технологий VPN
- Настройка VPN-туннелей сайт–сайт
- 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 удаленного доступа»

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

10

Мониторинг работы системы и обслуживание

- Средства мониторинга
- Оповещения и SNMP
- Журналы и отчёты
- Резервное копирование
- 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)

- Обзор компонентов экосистемы
- Функции Management Center
- Обзор UserGate WAF
- Обзор UserGate SIEM
- Обзор UserGate Client
- Профессиональные сервисы

Программа курса предварительная, могут быть внесены незначительные изменения.

12

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

Программа курса предварительная, могут быть внесены незначительные изменения.

uAcademy