UserGate

# Администрирование межсетевых экранов UserGate 6

Программа курса

# О курсе

**Код курса**

UG6P01

**Длительность курса**

5 дней / 40 академических часа

**Описание**

В данном курсе рассматривается установка и конфигурирование межсетевых экранов UserGate. Вы научитесь выполнять установку и первоначальную настройку, создавать кластеры конфигурации и отказоустойчивости, формировать политику безопасности, включающую в себя инспектирование SSL, контроль доступа пользователей, настройку системы предотвращения вторжений, VPN-туннели и многие другие функции.

В курсе также рассматривается журналирование с использованием UserGate Log Analyzer и централизованное управление устройствами с использованием UserGate Management Center.

**Аудитория**

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

**Предварительные требования**

Для успешного прохождения курса вам необходимо обладать следующими знаниями и навыками:

- 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;
- желательно обладать опытом работы в командной строке.

# Программа курса

1

## Межсетевое экранирование и продукты компании UserGate

### Эволюция угроз и защиты от них

- современные угрозы;
- традиционные средства защиты VS UserGate.

### Продукты компании UserGate

- группа компаний UserGate;
- обзор моделей межсетевых экранов;
- обзор функционала;
- дополняющие продукты.

### Лабораторная работа 1.1. «Знакомство со стендом»

- топология стенда и коммутация устройств;
- начальная конфигурация устройств.

# 2

## Установка и базовая настройка

### Установка

- аппаратные межсетевые экраны;
- виртуальные межсетевые экраны;
- подключение.

### Интерфейсы администратора

- графический интерфейс;
- интерфейс командной строки;
- меню загрузки и системные утилиты.

### Лицензирование

- правила лицензирования;
- дополнительно лицензируемые модули;
- регистрация продукта.

### Ролевая модель доступа

- администраторы и профили администраторов;
- серверы авторизации;
- работа с административными учетными записями.

### Лабораторная работа 2.1. «Базовая конфигурация»

- знакомство с интерфейсом;
- ролевая модель и администраторы.

3

# Кластеры

## Кластер конфигурации

- обзор кластера конфигурации;
- настройка кластера конфигурации.

## Кластер отказоустойчивости

- протокол VRRP;
- обзор кластера отказоустойчивости;
- актив-Пассив;
- актив-Актив;
- переключение узлов;
- настройка.

## Лабораторная работа 3.1. «Кластеры»

- настройка кластера конфигурации;
- настройка кластера отказоустойчивости;
- подключение UserGate Log Analyzer.

# 4

## Сетевая конфигурация

### Зоны

- описание;
- параметры контроля зоны;
- защита от IP-Spoofing;
- защита от DoS-атак;
- создание и настройка зоны.

### Сетевые интерфейсы

- общая информация;
- настройка логических интерфейсов.

### Маршрутизация

- виртуальные маршрутизаторы;
- шлюзы;
- статическая и динамическая маршрутизация.

### Сетевые сервисы

- DNS;
- DHCP.

### Лабораторная работа 4.1. «Сетевая конфигурация»

- настройка шлюзов и маршрутизации;
- настройка DNS;
- настройка DHCP;
- настройка протокола OSPF.

5

## Политики сети

### Обзор политик сети

- компоненты политик сети;
- журналы.

### Библиотеки элементов

- морфология;
- сервисы;
- IP-адреса;
- useragent браузеров;
- типы контента;
- списки URL;
- календари;
- полосы пропускания;
- профили АСУ ТП;
- шаблоны страниц;
- категории URL;
- измененные категории URL;
- приложения;
- почтовые адреса;
- номера телефонов;
- профили СОВ;
- профили оповещений;
- профили NetFlow;
- профили SSL.

### Политика межсетевого экрана

- обзор;
- параметры правил и их настройка.

### NAT и маршрутизация

- обзор;
- правила NAT;
- правила DNAT;
- правила Port Forwarding;
- Network Mapping;
- маршрутизация с использованием политик.

### Балансировка нагрузки

- обзор;
- настройка балансировки TCP/UDP.

### Управление пропускной способностью

- настройка правил пропускной способности.

### Лабораторная работа 5.1. «Политики сети»

- создание объектов в библиотеке;
- настройка базовой политики безопасности;
- настройка подключения к Интернет;
- эмуляция сбоя и проверка работы кластера;
- обновление библиотек.

6

## Сертификаты и инспектирование SSL

### Цифровые сертификаты

- обзор алгоритмов шифрования;
- цифровые сертификаты;
- управление сертификатами.

### Инспектирование SSL

- SSL/TLS;
- инспектирование SSL.

### Лабораторная работа 6.1. «Сертификаты и политика инспектирования SSL»

- работа с сертификатами;
- настройка политики инспектирования SSL.

7

# Идентификация пользователей

## Пользователи и группы

- обзор;
- создание пользователей;
- профили авторизации.

## Идентификация пользователей

- обзор методов авторизации ;
- Captive-портал;
- агенты авторизации.

## Лабораторная работа 7.1. «Идентификация пользователей»

- настройка Captive-портала;
- настройка аутентификации Kerberos;
- установка и настройка агента авторизации;
- авторизация по атрибутам пользователя.

8

## Политика безопасности

### Обзор политики безопасности

- компоненты политики безопасности;
- журналы.

### Фильтрация контента

- обзор;
- настройка фильтрации контента.

### Веб-безопасность

- обзор;
- настройка веб-безопасности.

### Система обнаружения и предотвращения вторжений

- обзор;
- настройка СОВ.

### Сценарии

- обзор;
- настройка сценария.

### Защита от DoS-атак

- обзор;
- настройка защиты от DoS-атак.

### Прочие средства защиты

- правила АСУ ТП;
- защита почтового трафика;
- работа с внешними ICAP-серверами.

### Лабораторная работа 8.1. «Политика безопасности»

- фильтрация контента;
- система обнаружения вторжений (СОВ);
- сценарии.

9

# VPN

## Обзор технологий VPN

- типы VPN;
- IPSec.

## Remote Access

- настройка сервера;
- настройка клиента.

## Site-to-Site

- настройка сервера;
- настройка клиента.

## Веб-портал (SSL VPN)

- обзор веб-портала;
- настройка веб-портала.

## Лабораторная работа 9.1. «VPN»

- Site-to-Site VPN;
- Remote Access VPN;
- SSL VPN;
- Reverse Proxy.

# 10

## Мониторинг, журналы отчетность

### Диагностика и мониторинг

- дашборд;
- диагностика и мониторинг.

### Журналы, отчеты и техническая поддержка

- журналы;
- отчеты;
- техническая поддержка.

### Лабораторная работа 10.1. «Мониторинг и диагностика»

- журналы, отчеты и диагностика;
- поиск и устранение неисправностей.

# 11

## Централизованное управление

### Архитектура UserGate Management Center

- концепции централизованного управления;
- рекомендации по внедрению UserGate MC.

### Установка и базовая настройка

- установка;
- базовая настройка;
- администраторы и интерфейс.

### Управление МЭ UserGate

- процесс централизованного управления;
- добавление управляемых устройств.

### Лабораторная работа 11.1. «Централизованное управление»

- настройка UserGate MC;
- подключение UTM-B к UserGate MC и применение группы шаблонов.

UserGate

www.usergate.ru | academy@usergate.ru