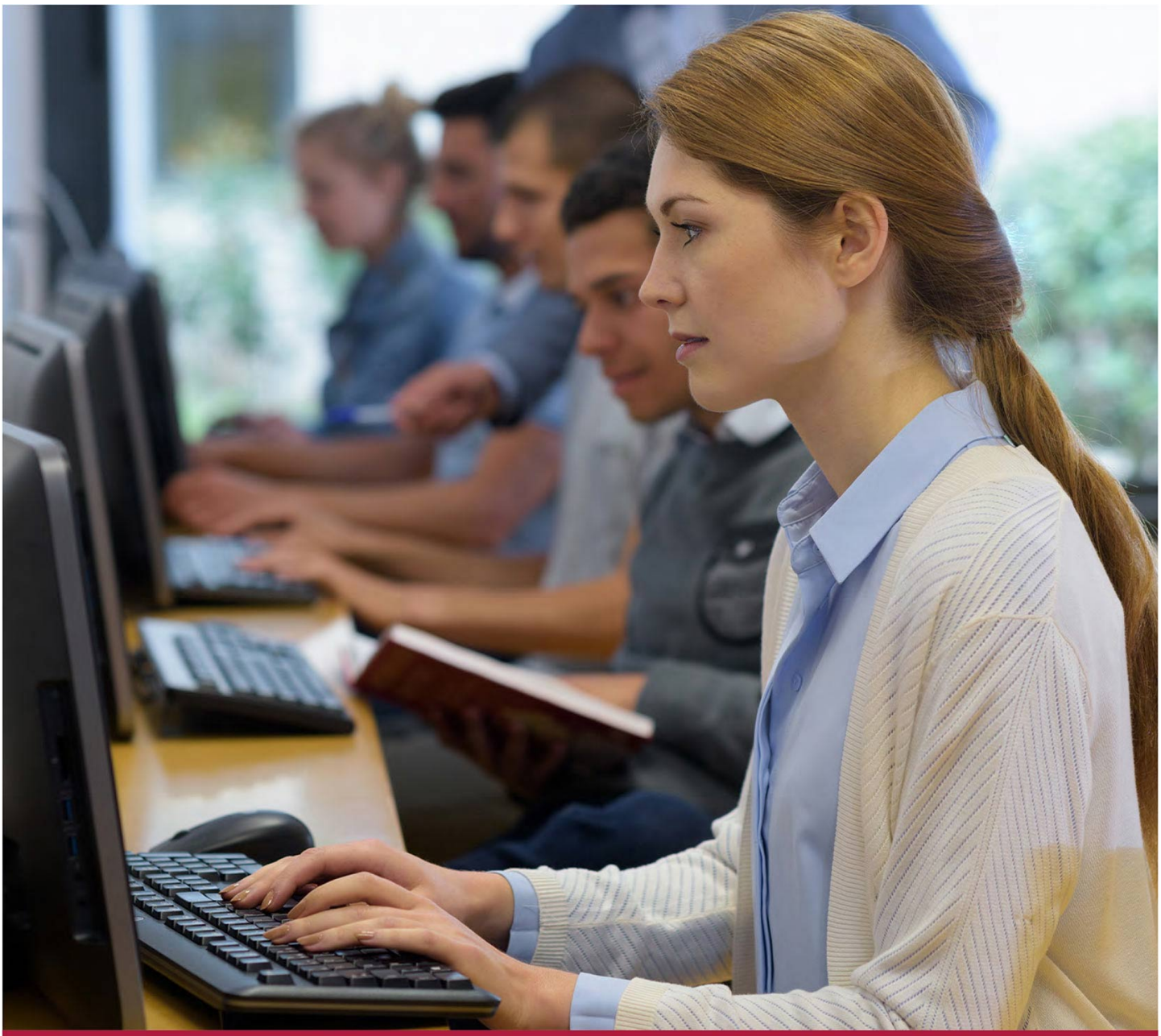
softline учебный центр



Администрирование межсетевых экранов UserGate NGFW 7.X. Ускоренный курс

Код курса: UG-NGFW7 FT

8 (800) 505-05-07 | edusales@softline.com | edu.softline.com

Администрирование межсетевых экранов UserGate NGFW 7.X. Ускоренный курс

Код курса: UG-NGFW7 FT

Длительность	50 ак. часов
Формат	
Разработчик курса	UserGate
Тип	Учебный курс
Способ обучения	Под руководством тренера

О курсе

В данном курсе рассматривается установка и конфигурирование межсетевых экранов UserGate, работающих под управлением операционной системы UGOS 7.X. 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.

Подробная информация

Профиль аудитории:

- системные инженеры и специалисты в области информационной безопасности, которым необходимо получить знания и навыки по работе с межсетевыми экранами UserGate

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;
- желательно обладать опытом работы в командной строке

По окончании курса слушатели изучат:

- устанавливать систему и выполнять первоначальную настройку;
- создавать кластеры конфигурации и отказоустойчивости;
- формировать политику безопасности: инспектирование SSL, контентная фильтрация, профили СОВ;
- идентифицировать пользовательский трафик через агентов, captive-портал и механизм UserID;

- настраивать VPN-туннели разных типов.

Программа курса

Модуль 1 «Установка и базовая настройка»

Обзор продуктов UserGate

- межсетевые экраны UserGate;
- экосистема UserGate SUMMA.

Установка и базовая настройка

- установка;
- первоначальная настройка.

Интерфейсы администратора

- обзор административных интерфейсов;
- графический интерфейс;
- интерфейс командной строки.

Лицензирование

- общие сведения о лицензировании;
- процесс активации лицензии;
- работа с обновлениями.

Ролевая модель доступа

- обзор ролевой модели;
- настройка ролевой модели.

Лабораторная работа 1.1. «Установка и базовая настройка»

- знакомство со стендом;
- базовая конфигурация;
- настройка ролевой модели;
- экспорт/импорт конфигурации;
- настройка DCFW в филиале.

Модуль 2 «Кластеры»

Кластер конфигурации

- обзор кластеров UserGate;
- настройка кластера конфигурации.

Отказоустойчивый кластер

- протоколы отказоустойчивости первого хопа (FHRP);
- концепции кластера отказоустойчивости;
- настройка кластера отказоустойчивости.

Лабораторная работа 2.1. «Кластеры»

- настройка кластера конфигурации;
- настройка отказоустойчивого кластера.

Модуль 3 «Сетевая конфигурация»

Зоны и сетевые интерфейсы

- зоны;
- сетевые интерфейсы.

Маршрутизация

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

Сетевые сервисы

- DNS;
- DHCP.

Сетевая диагностика

- мониторинг сети;
- протокол LLDP.

Лабораторная работа 3.1. «Сетевая конфигурация»

- маршрутизация;
- настройка DNS и DHCP;
- сетевая диагностика;
- компоненты UserGate SUMMA.

Модуль 4 «Политики сети»

Обзор политик сети

- обработка трафика на NGFW;
- обработка трафика на DCFW;
- библиотеки элементов;
- сценарии.

Политика межсетевого экрана

- правила политики межсетевого экрана;

- идентификация приложений;
- работа с правилами политики межсетевого экрана.

NAT и PBR

- правила NAT;
- маршрутизация с использованием политик (PBR).

Балансировка и управление пропускной способностью

- балансировка нагрузки;
- управление пропускной способностью.

Лабораторная работа 4.1. «Политики сети»

- работа с библиотеками;
- правила межсетевого экрана;
- трансляция адресов;
- правила балансировки.

Модуль 5 «Сертификаты и инспектирование SSL»

Применение сертификатов в NGFW

- цифровые сертификаты;
- настройки сертификатов на NGFW.

Инспектирование SSL

- обзор SSL/TLS;
- настройка инспектирования SSL;
- отправка дешифрованного трафика на внешние системы.

Инспектирование SSH

- обзор SSH;
- настройка инспектирования SSH.

Лабораторная работа 5.1. «Сертификаты и инспектирование SSL»

- цифровые сертификаты;
- инспектирование SSL и SSH.

Модуль 6 «Идентификация пользователей»

Компоненты идентификации пользователей

- способы идентификации;
- серверы аутентификации;
- профили аутентификации.

Технология UserID

- обзор UserID;
- настройка UserID.

Captive-портал, агенты авторизации, идентификация по атрибутам

- captive-портал;
- локальные пользователи и агенты авторизации.

Лабораторная работа 6.1. «Идентификация пользователей»

- технология UserID;
- captive-портал;
- локальные пользователи и агент аутентификации.

Модуль 7 «Политика безопасности»

Обзор политики безопасности

- компоненты политики безопасности;
- обработка трафика при включенных функциях политики безопасности на NGFW.

Настройка политик безопасности

- настройка фильтрации контента и веб-безопасности;
- система обнаружения вторжений.

Лабораторная работа 7.1. «Политика безопасности»

- фильтрация контента;
- система обнаружения вторжений.

Модуль 8. «Технологии представления удаленного доступа – I»

Обзор технологий удаленного доступа

- VPN-туннели;
- способы публикации ресурсов.

Настройка VPN сайт-сайт и VPN удаленного доступа

- настройка VPN-туннеля сайт-сайт;
- настройка VPN-туннелей удаленного доступа.

Лабораторная работа 8.1. «Технологии предоставления удаленного доступа»

- настройка IKEv2 VPN-туннеля сайт-сайт;
- настройка IKEv2 VPN-туннеля удаленного доступа;
- настройка L2TP/ipsec VPN-туннеля сайт-сайт;
- настройка L2TP/ipsec VPN-туннеля удаленного доступа.

Модуль 9. «Технологии представления удаленного доступа – II»

Веб-портал

- настройка веб-портала.

Reverse-прокси

- настройка reverse-прокси.

Лабораторная работа 9.1. «Технологии предоставления удаленного доступа»

- веб-портал;

Reverse-прокси.

Модуль 10. «Мониторинг, поиск и устранение неисправностей»

Средства диагностики и мониторинга

- мониторинг и диагностика;
- оповещения и SNMP.

Журналы и отчеты

- работа с журналами;
- отчеты .

Техническая поддержка и устранение неисправностей

- работа со службой технической поддержки UserGate;
- решение типовых проблем.

Лабораторная работа 10.1. «Мониторинг, журналы, отчетность»

- средства диагностики и мониторинга;
- журналы и отчеты.

Посмотреть расписание курса и записаться на обучение

Обращайтесь по любым вопросам
к менеджерам Учебного центра Softline

8 (800) 505-05-07 | edusales@softline.com

Ждём вас на занятиях в Учебном центре Softline!

Почему Учебный центр Softline?

Лидер на рынке корпоративного обучения.

Более 300 тысяч подготовленных IT-специалистов.

Гибкий индивидуальный подход в обучении, скидки и акции.

Широкая сеть представительств в крупнейших городах РФ и СНГ; дистанционный формат обучение на вашей территории или в арендованном классе в любой точке мира.

Высокотехнологичное оборудование

Более **18 лет** опыта работы

Международные сертификаты для IT-специалистов и пользователей в Центрах тестирования

Сертифицированные тренеры с богатым практическим опытом работы

Авторизации от мировых производителей ПО (Microsoft, Cisco, VMware, Citrix, Лаборатория Касперского, Oracle, Autodesk, Код безопасности и других).

Разработка курсов и тестов под заказ, внедрение корпоративных систем обучения.

Подробнее об Учебном центре Softline
Вы можете узнать из профайла.