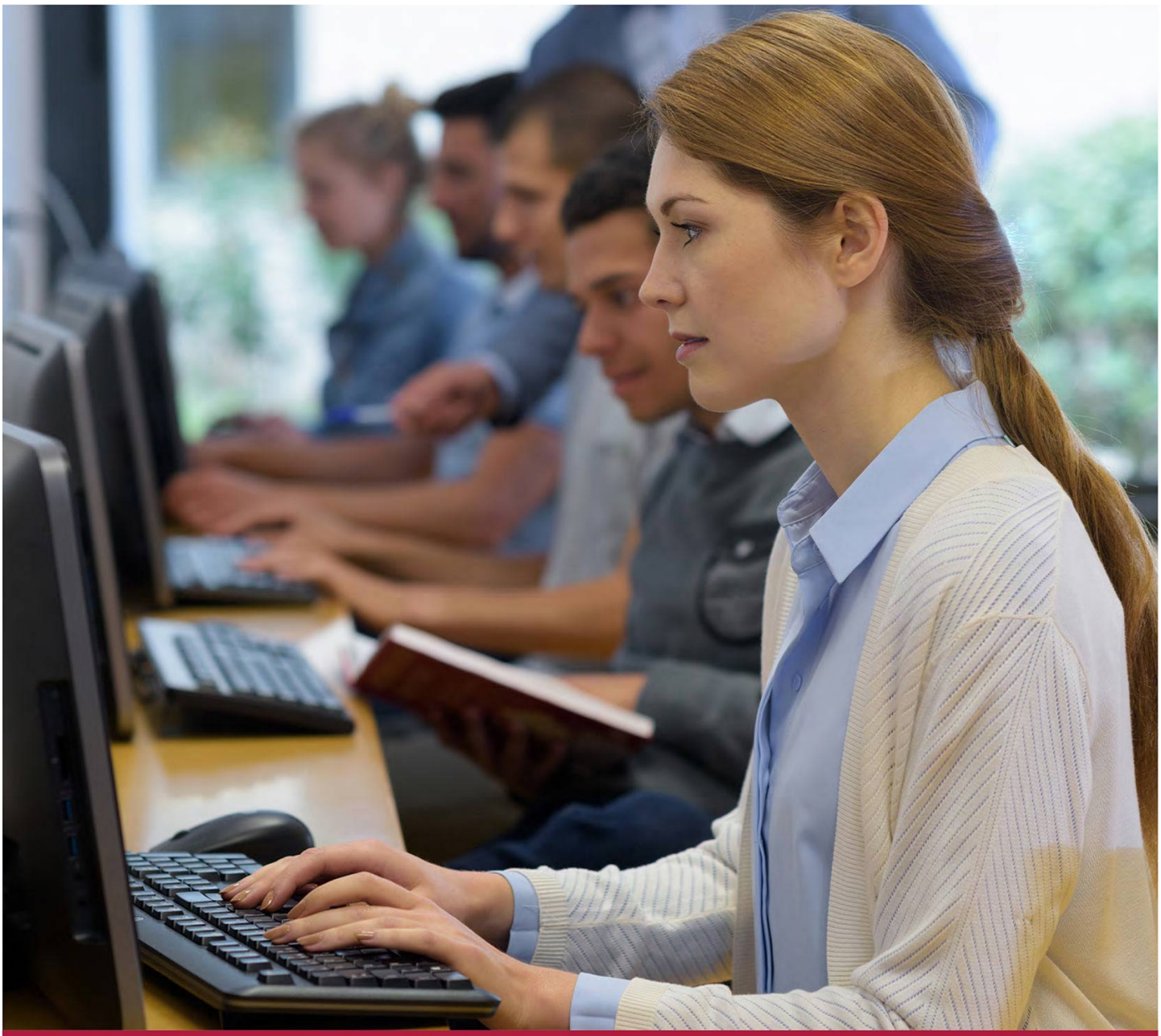
softline учебный центр



Kaspersky NGFW

Код курса: KL 007.1

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

Kaspersky NGFW

Код курса: KL 007.1

Длительность	16 ак. часов
Формат	
Разработчик курса	Лаборатория Касперского
Тип	Учебный курс
Способ обучения	Под руководством тренера

О курсе

Kaspersky NGFW — это комплексное решение корпоративного класса для эффективной защиты корпоративных сетей от современных киберугроз. Курс посвящен освоению функционала, особенностей архитектуры и методик настройки данного решения. Материалы содержат теоретические лекции, практические руководства и обширные лабораторные занятия, позволяющие закрепить полученные знания. Программа курса охватывает широкий спектр вопросов: начиная от базовой настройки устройства и заканчивая управлением различными модулями безопасности и работой с внешними системами. Лабораторные работы построены на примере развертывания и настройки управляющего центра, оркестратора, службы каталогов, а также среды мониторинга. Основные цели курса: изучение архитектурных особенностей и функций Kaspersky NGFW освоение методов настройки и диагностики устройства практическое овладение средствами сегментирования, изоляции и фильтрации трафика овладение методами настройки и контроля NAT, глубоких проверок пакетов (DPI), SSL Inspection, DNS Security, Web Control, антивирусной защиты и IDS/IPS настраивать мониторинг, диагностику и устранять неисправности

Подробная информация

Профиль аудитории:

- инженеры технической поддержки
- пресейл-инженеры

Предварительные требования:

- понимание основ сетевых технологий: TCP/IP, DHCP, NAT, знание принципов работы маршрутизации и коммутации на уровне CCNA/HCNA
- иметь представление о работе классических межсетевых экранов предыдущего поколения
- базовые знания сетевой безопасности: правила МЭ, SSL/TLS, контроль приложений
- базовый опыт работы с системами мониторинга
- умение читать и интерпретировать сетевую статистику и журналы событий
- начальные навыки администрирования операционных систем Windows Server и Linux, включая основы работы с Active Directory (AD)
- знания установки платформы OSMP

- основные представления о настройке протокола динамической маршрутизации BGP
- иметь представление о базовом управлении платформы KUMA

По окончании курса слушатели изучат:

- современные угрозы и вызовы, которые могут быть нейтрализованы внедрением межсетевого экрана нового поколения
- функционирование архитектуры и схемы обработки трафика NGFW, процесс взаимодействия модулей безопасности
- выполнение базовой настройки NGFW, управление сетевыми объектами и правилами фильтрации
- процесс настройки и управления ключевыми модулями безопасности: контролем приложений (App-Control), системой обнаружения и предотвращения вторжений (IDPS), антивирусом, веб-контролем (Web Control) и фильтрацией DNS
- настройку и применение политики расшифровки и инспектирования TLS/SSL трафика для противодействия скрытым угрозам
- реализацию трансляции сетевых адресов (NAT) и настройки динамической маршрутизации (BGP)
- организовывать интеграцию NGFW с внешними системами (оркестратор KNBE, платформа OSMP, Zabbix) для автоматизации и мониторинга

Программа курса

Темы:

1. Введение

1.1. Вызовы

1.2. Решение от Kaspersky

1.3. Принцип работы KSN

2. Базовая настройка NGFW
3. Архитектура

3.1. Пакет и поток

3.2. Межсетевой экран и App-control

3.3. Межсетевой экран, App-control и DNS security

3.4. Межсетевой экран, App-control и глубокий анализ трафика

3.5. Межсетевой экран, App-control и SSL-inspection

3.6. Общая схема обработки трафика

4. Модули безопасности

4.1. Сегментация и изоляция

4.2. User awareness

4.3. Межсетевой экран

4.4. Deep packet inspection

4.5. SSL-inspection

4.6. Группы профилей безопасности

4.7. DNS security

4.8. Web control

4.9. Antivirus

4.10. IDPS

4.11. Менеджер сессий

5. Модули, функции и компоненты

5.1. NAT

5.2. Кластер

5.3. Агенты настройки

5.4. Агенты настройки: KLNAGENT

5.5. Агенты настройки: KNBEagent

5.6. Мониторинг с помощью Zabbix

5.7. Работа с конфигурацией

5.8. Взаимодействие с внешними системами

5.9. Автоматическое создание правил NGFW

5.10. Обновление

5.11. Поиск и устранение неисправностей

6. Спецификации

6.1. Платформы

6.2. Лицензии

Лабораторные работы:

Лабораторная работа № 1. Развернуть управляющие и служебные системы

Задание A: Настройте платформу OSMP

Задание B: Разверните оркестратор KNBE

Задание C: Настройте оркестратор KNBE

Задание D: Разверните службу UAWS

Задание E: Настройте службу UAWS

Лабораторная работа № 2. Базовая настройка межсетевого экрана Kaspersky NGFW Задание A: Запуск всех виртуальных машин и подключение к консоли NGFW

Задание B: Настройка и проверка сетевых параметров NGFW

Задание C: Подключение межсетевого экрана к платформе OSMP

Задание D: Подключение межсетевого экрана к оркестратору KNBE и службе UAWS

Задание E: Подключение межсетевого экрана к системе мониторинга Zabbix

Задание F: Управление сетевыми настройками NGFW

Задание H: Создание группы управляемых устройств и перемещение NGFW в состав группы

Задание L: Создание политики межсетевого экрана

Задание G: Настройка передачи журнала сетевых соединений в KUMA OSMP

Задание I: Создание сетевых объектов

Лабораторная работа № 3. Управление правилами фильтрации и контроль приложений

Задание A: Создание правил фильтрации с журналированием сетевых соединений

Задание B: Создание правила FW с детектированием сервисов

Лабораторная работа № 4. Настройка NAT

Задание A: Настройка NAT для выхода из LAN и MGMT в WAN

Задание B: Настройка Static NAT для отдельного сервиса

Лабораторная работа № 5. Настройка контроля приложений

Задание A: Создайте правило для блокировки протокола SSH

Лабораторная работа № 6. Настройка контроля приложений на основе SNI

Задание A: Создание правила для блокирования трафика приложения Telegram

Задание B: Использование FQDN в правилах фильтрации

Задание C: Использование доменных учетных записей и групп в правилах фильтрации

Лабораторная работа № 7. Настройка системы обнаружения и предотвращения вторжений (IDPS)

Задание A: Предотвращение сетевого сканирования

Задание B: Блокирование атак на основе уязвимостей

Лабораторная работа № 8. Расшифровка и инспектирование трафика TLS

Задание A: Настройка расшифровки и инспектирование трафика TLS

Задание B: Добавление сертификата MITM с помощью групповой политики

Задание C: Использование исключений

Лабораторная работа № 9. Настройка фильтрации веб-приложений

Задание A: Создание правила для блокировки доступа к Dropbox

Задание B: Проверка работы правила блокировки

Лабораторная работа № 10. Защита от вредоносных программ и URL-адресов

Задание A: Блокирование загрузки вредоносных программ

Задание B: Блокирование вредоносных и потенциально опасных URL-адресов. Использование исключений

Лабораторная работа № 11. Настройка фильтрации Веб-трафика "Web control"

Задание A: Настройка правила Web Control

Задание B: Проверка работы Web Control

Лабораторная работа № 12. Настройка инспектирования DNS трафика

Задание A: Создание и применение профиля DNS Security к групповому профилю безопасности

Задание B: Проверка работы инспектирования, фильтрации DNS-запросов и информации о событиях DNS Security

Лабораторная работа № 13. Настройка response на алерт из KUMA

Задание A: Настройка response на событие из KUMA

Задание B: Проверка работы алерта и плейбука, а также автоматическое создание правила межсетевого экрана

Лабораторная работа № 14. Базовая настройка протокола динамической маршрутизации BGP

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.