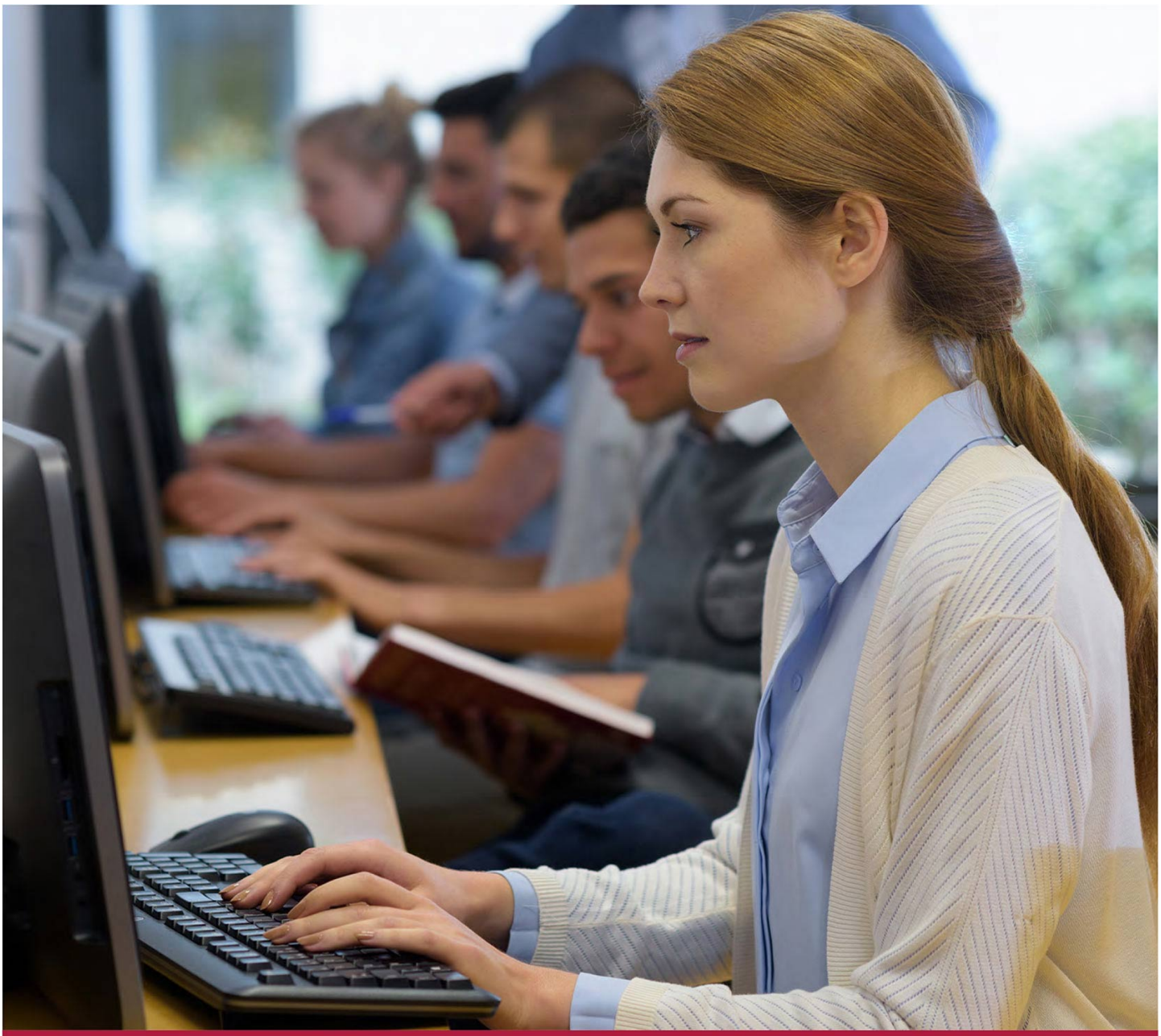
softline учебный центр



IDECO NGFW. Интеграция. Управление. Администрирование

Код курса: IDECO_NGFW_20

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

IDECO NGFW. Интеграция. Управление. Администрирование

Код курса: IDECO_NGFW_20

Длительность	32 ак. часа
Формат	
Разработчик курса	IDECO
Тип	Учебный курс
Способ обучения	Под руководством тренера

О курсе

В рамках данного курса рассматриваются основные возможности многофункционального межсетевого экрана Ideco NGFW. Слушатели получат знания, необходимые для использования устройств Ideco NGFW в корпоративной сети, их подключения и начального конфигурирования, а также навыки мониторинга и анализа событий, обнаруживаемых этими устройствами. Курс содержит сведения по настройке политик фильтрации трафика, трансляции сетевых адресов и анализа содержимого трафика. В курсе также представлена информация по построению виртуальных частных сетей различного типа на основе Ideco NGFW. Программа курса включает в себя полные сведения по настройке сетевых интерфейсов в Ideco NGFW для работы в различных режимах, настройку протоколов маршрутизации. Также рассматриваются варианты использования Ideco NGFW в отказоустойчивых конфигурациях.

Подробная информация

Профиль аудитории:

- Системные и сетевые администраторы, ответственные за безопасность компьютерных сетей, эффективную эксплуатацию средств защиты и средств анализа защищенности сетей;
- Администраторы информационной безопасности;
- Эксперты и аналитики по вопросам компьютерной безопасности, ответственные за анализ состояния информационной безопасности и определение требований к защищенности сетевых ресурсов.

Предварительные требования:

- Базовые знания по IP-сетям, основным протоколам и службам стека TCP/IP
- Навыки работы в ОС Linux: интерфейс командной строки, настройка сети
- Понимание принципов работы пакетных фильтров, прокси-серверов.
- Знакомство с инфраструктурой открытых ключей

По окончании курса слушатели изучат:

- Основные характеристики и режимы работы модулей фильтрации и анализа трафика;

- Технологии кластеризации, используемые в Ideco NGFW;
- Особенности построения отказоустойчивых конфигураций.
- Порядок разграничения доступа пользователей к сетевым ресурсам;
- Возможности Ideco NGFW по защите электронной почты и web-приложений.

Программа курса

Модуль 1. Введение в многофункциональные межсетевые экраны.

- Защита периметра. Типы межсетевых экранов. Краткий обзор ключевых возможностей Ideco NGFW. Редакции Ideco NGFW. Лицензирование.
- Практическая работа 1. Установка и начальное конфигурирование Ideco NGFW. «Быстрый старт». Обновление и резервное копирование. Разграничение доступа администраторов.
- Практическая работа 2. Управление доступом администраторов.

Модуль 2. Управление учётными записями пользователей.

- Способы хранения информации о пользователях. Личный кабинет. Методы идентификации пользователей. Веб-аутентификация. Авторизация по IP и MAC адресам. Авторизация по подсетям. Авторизация пользователей терминальных серверов.
- Практическая работа 3. Создание локальных пользователей и групп.

Модуль 3. Сетевые интерфейсы и маршрутизация.

- Типы сетевых интерфейсов в Ideco. VLAN-интерфейсы. Агрегированные интерфейсы. Зоны. Реализация функциональности маршрутизации в Ideco. Маршрутизация локальных и внешних сетей.
- Практическая работа 4. Настройка локального сегмента. Предоставление доступа в Интернет локальным пользователям Разрешение имён. Настройка DHCP и NTP.

Модуль 4. Фильтрация трафика и трансляция адресов.

- Принципы работы файрвола. Критерии фильтрации. Таблицы файрвола (FORWARD, DNAT, INPUT и SNAT). Правила трансляции. Варианты трансляции адресов. Разграничение доступа к сетевым ресурсам на уровне пользователей. Контроль приложений. Логгирование. Ограничение скорости.
- Практическая работа 5. Настройка правил фильтрации трафика и трансляции адресов.

Модуль 5. Интеграция с Active Directory/Samba DC.

- Ввод Ideco в домен. Настройка авторизации пользователей. SSO-аутентификация. Авторизации через журнал безопасности. Интеграция с ALD Pro.
- Практическая работа 6. Настройка интеграции с Active Directory/Samba DC.

Модуль 6. Подключение к Интернет-провайдерам.

- Использование нескольких Интернет-провайдеров. Особенности подключения посредством различных протоколов (L2TP, PPTP, PPPoE). Динамическая маршрутизация. Протоколы BGP и OSPF. Маршрутизация с учётом адреса источника.

- Практическая работа 7. Настройка подключения к двум интернет-провайдерам.

Модуль 7. Контент-фильтр.

- Принципы работы механизма контентной фильтрации. Фильтрация HTTPS-трафика. Управление SSL-сертификатами в Ideco. Анализ содержимого трафика: защита от спама, вирусов, разграничение доступа к web-ресурсам. Антивирусы веб-трафика. Использование внешних серверов контроля содержимого.
- Практическая работа 8. Создание правил для анализа веб-трафика.

Модуль 8. Публикация ресурсов.

- Публикация веб-приложений (обратный прокси-сервер). Схема фильтрации почтового трафика. Настройка почтовых клиентов.
- Практическая работа 9. Защита web-приложений. Почтовый релей.

Модуль 9. Защита от сетевых атак.

- Правила системы предотвращения вторжений. Пользовательские сигнатуры. Анализ журналов.
- Практическая работа 10. Настройка модуля защиты от атак.

Модуль 10. Построение виртуальных частных сетей.

- Разновидности виртуальных частных сетей (VPN). Топологии VPN. Особенности туннелирования трафика. IPsec VPN, SSTP, PPTP, IKEv2. Двухфакторная аутентификация. Аутентификация пользователей VPN средствами RADIUS. Использование Ideco client для подключения пользователей VPN. Инструменты настройки и мониторинга состояния VPN.
- Практическая работа 11. Построение виртуальной частной сети на основе IPsec. Настройка туннелирования и маршрутизации.

Модуль 11. Мониторинг работы Ideco NGFW.

- Панель мониторинга работы сервера в веб-интерфейсе. Журналы. Мониторинг сервера из консоли, системные утилиты Linux. Монитор трафика. Ideco Monitoring Bot. Использование SNMP. Zabbix-агент. Отчёты. Интеграция с SIEM-системами по протоколу syslog.
- Практическая работа 12. Мониторинг работы сервера с использованием SNMP и системы Zabbix. Построение отчётов.

Модуль 12. Построение отказоустойчивых конфигураций

- Кластеризация, Синхронизация сессий.
- Практическая работа 13. Установка и конфигурирование кластера, состоящего из двух серверов Ideco.

Модуль 13. Централизованное управление межсетевыми экранами Ideco.

- Возможности Ideco Center. Общие настройки. Управление объектами и правилами.
- Практическая работа 14. Установка Ideco Center.

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.