



IDECO NGFW Novum

Код курса: IDECO_NOVUM

IDECO NGFW Novum

Код курса: IDECO_NOVUM

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 Novum. Слушатели получают знания, необходимые для использования устройств Ideco NGFW Novum в корпоративной сети, их подключения и начального конфигурирования, приобретут навыки настройки политик фильтрации трафика, трансляции сетевых адресов, контентной фильтрации. Курс содержит сведения по интеграции Ideco NGFW в сетевую инфраструктуру, по настройке взаимодействия с внешними каталогами учётных записей. В курсе представлена информация по построению виртуальных частных сетей различного типа на основе Ideco NGFW Novum, а также рассматриваются варианты использования Ideco NGFW Novum 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 Novum

- особенности построения отказоустойчивых конфигураций
- порядок разграничения доступа пользователей к сетевым ресурсам
- возможности Ideco NGFW Novum 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 Novum. Редакции Ideco NGFW Novum. Технология виртуальных контекстов.
Лицензирование.
Практическая работа 1. Установка и начальное конфигурирование Ideco NGFW Novum.
«Быстрый старт». Обновление и резервное копирование. Разграничение доступа администраторов.
Практическая работа 2. Управление доступом администраторов.
- Управление учётными записями пользователей
Способы хранения информации о пользователях.
- 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
- Сетевые интерфейсы
Типы и роли сетевых интерфейсов в Ideco. VLAN-интерфейсы. Агрегированные интерфейсы.
Зоны.
Практическая работа 4. Настройка локального сегмента. Предоставление доступа в Интернет локальным пользователям
- Настройка инфраструктурных сервисов DNS, NTP, DHCP в Ideco.
- Разрешение имён. Модуль DNS Security. Настройка DHCP и NTP.
Практическая работа 5. Настройка DNS, DHCP, NTP в Ideco

Модуль 2.

- Фильтрация трафика и трансляция адресов
Принципы работы межсетевого экрана. Критерии фильтрации. Таблицы межсетевого экрана (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 6. Настройка правил фильтрации трафика и трансляции адресов.
- Интеграция с Active Directory/Samba DC
Возможности интеграции. Ввод Ideco в домен. Настройка авторизации пользователей. SSO-аутентификация. Авторизации через журнал безопасности. Интеграция с ALD Pro.
Практическая работа 7. Настройка интеграции с Active Directory/Samba DC
- Маршрутизация
Использование нескольких Интернет-провайдеров. Динамическая маршрутизация. Протоколы BGP и OSPF. Маршрутизация на основе политик.
Практическая работа 8. Настройка подключения к двум интернет-провайдерам.
- Контент-фильтр

Принципы работы механизма контентной фильтрации. Фильтрация HTTPS-трафика. Управление SSL-сертификатами в Idesco. Анализ содержимого трафика: защита от спама, вирусов, разграничение доступа к web-ресурсам. Антивирусы веб-трафика. Использование внешних серверов контроля содержимого. Практическая работа 9. Создание правил для анализа веб-трафика

Модуль 3.

- Публикация ресурсов
Публикация веб-приложений (обратный прокси-сервер). Схема фильтрации почтового трафика. Настройка почтовых клиентов.
Практическая работа 10. Защита веб-приложений. Почтовый релей.
- Защита от сетевых атак.
Правила системы предотвращения вторжений. Пользовательские сигнатуры. Анализ журналов.
Практическая работа 11. Настройка модуля защиты от атак.
- Построение виртуальных частных сетей
Разновидности виртуальных частных сетей (VPN). Топологии VPN. Особенности туннелирования трафика. IPsec VPN, SSTP, IKEv2. Инструменты настройки и мониторинга состояния VPN.
Практическая работа 12. Построение сети Site-to-site на основе IPsec.
Практическая работа 13. Использование GRE over IPsec.

Модуль 4.

- Удаленный доступ пользователей
Двухфакторная аутентификация. Аутентификация пользователей VPN средствами RADIUS. Личный кабинет. Использование Idesco client для подключения пользователей VPN.
Практическая работа 14. Подключение пользователей (удалённый доступ).
Практическая работа 15. Удалённый доступ SSL VPN
Практическая работа 16. Удалённый доступ через Idesco Client.
- Мониторинг работы Idesco NGFW Novum
Панель мониторинга работы сервера в вебинтерфейсе. Журналы. Мониторинг сервера из консоли, системные утилиты Linux. Монитор трафика. Idesco Monitoring Bot. Использование SNMP. Zabbix-агент. Отчёты. Интеграция с SIEM-системами по протоколу syslog.
Практическая работа 17. Мониторинг работы сервера с использованием SNMP и системы Zabbix. Построение отчётов.
- Построение отказоустойчивых конфигураций
Кластеризация, Синхронизация сессий.
Практическая работа 18. Установка и конфигурирование кластера, состоящего из двух серверов Idesco
- Централизованное управление межсетевыми экранами Idesco
Возможности Idesco Center. Общие настройки. Управление объектами и правилами.
Практическая работа 19. Установка Idesco 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](#).