

IDECO NGFW. Интеграция. Управление. Администрирование. (NGFW19)

ID ID-NGFW19 Цена 80 000,- руб. Длительность 4 дня

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

Цели курса

Вы будете знать:

- 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.

Вы сможете:

- выполнять процедуру инициализации и начального конфигурирования кластера межсетевых экранов Ideco;
- настраивать маршрутизацию и одновременное подключение к нескольким Интернет-провайдерам.
- настраивать политики фильтрации и трансляции адресов;
- осуществлять настройку контент-фильтра;
- выполнять настройку анализа HTTP и HTTPS-трафика;
- планировать и развёртывать виртуальные частные сети;
- разрабатывать и реализовывать политику управления пропускной способностью каналов связи.

Содержание курса

В рамках данного курса рассматриваются основные возможности многофункционального межсетевого экрана Ideco NGFW. Слушатели получают 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.

Программа курса

- **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.*

- **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.*

- **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.*

- **Фильтрация трафика и трансляция адресов.**

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

- **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.*

- **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.*

- **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.*

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

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

- **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.*

- **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.*

- **Построение отказоустойчивых конфигураций** Кластеризация, Синхронизация сессий. *Практическая работа 13. Установка и конфигурирование кластера, состоящего из двух серверов IdecO.*

- **Централизованное управление межсетевыми экранами IdecO.** Возможности IdecO Center. Общие настройки. Управление объектами и правилами. *Практическая работа 14. Установка IdecO Center.*