Описание курса «Технологии безопасности компьютерных сетей. Базовый курс D-Link»

Целевая аудитория

Курс «Технологии защиты информации в компьютерных сетях. Межсетевые экраны и Интернет-маршрутизаторы» предназначен для сетевых администраторов, специалистов предприятий, внедряющих новые информационные технологии, студентов специальности 090301 «Компьютерная безопасность», студентов и аспирантов направлений 230100 «Информатика и вычислительная техника», 010500 «Математическое обеспечение и администрирование информационных систем», 231000 «Программная инженерия», а также всех, кто интересуется современными сетевыми технологиями и принципами построения защищенных сетей.

Предварительная подготовка

Данный курс требует прохождения курсов «Основы сетевых технологий. Базовый курс D-Link» и «Технологии коммутации современных сетей Ethernet. Базовый курс D-Link».

Сертификаты

После прохождения курса, слушатель может сдать сертификационный экзамен и получить сертификат D-Link. Экзамен состоит из практической части, сдаваемой в авторизованном учебном центре и теста на портале дистанционного обучения D-Link.

Описание курса

Длительность курса – 72 академических часа. Курс включает лекционную и практическую части.

Целью курса является:

- определение таких понятий, как угрозы безопасности информационных сетей, различные типы атак на распределенные вычислительные системы, а также методы защиты информации, в том числе средства (программные и аппаратные) сетевой безопасности;
- знакомство с программно-аппаратными средствами обеспечения безопасности компьютерных сетей на примере межсетевых экранов и Интернет-маршрутизаторов D-Link;
- описание основных протоколов и функций, обеспечивающих работу и безопасность современных сетей всех масштабов (от сектора SOHO до сектора Enterprise). Рассматриваются примеры их использования, а также настройки на Интернет-маршрутизаторах и межсетевых экранах D-Link. В учебном материале приводится описание основных элементов управления межсетевых экранов NetDefend.

Курс может использоваться как независимый или часть более широкого курса в средних специальных, профессиональных и высших образовательных учреждениях.

После прохождения курса слушатели смогут:

- понимать принципы проектирования защищенной сети;
- выполнять настройку Интернет-маршрутизаторов и межсетевых экранов, и управлять доступом к ним;
- применять в сетях механизм DHCP;

- обеспечивать совместный доступ к USB-устройствам через сети Ethernet и Wi-Fi;
- использовать технологии резервирования и балансировки нагрузки для создания отказоустойчивых сетей;
- применять средства управления трафиком и качество обслуживания в сетях;
- управлять мультикастовым потоком в локальных сетях;
- создавать изолированные сети на основе технологии VLAN;
- создавать защищенные сетевые соединения, используя механизм VPN;
- использовать прозрачный режим межсетевых экранов;
- использовать разные механизмы обеспечения безопасности локальных сетей, в том числе системы обнаружения и предотвращения вторжений извне.

Оборудование

Минимальные требования:

Для проведения практических работ по курсу требуется следующее оборудование для одного рабочего места* (1 или 2 слушателя):

- 1 компьютер с последовательным портом;
- 1 межсетевой экран DFL-860E (ПО 2.27.05-RU-upgrade.img);
- 1 маршрутизатор DSR-250;
- 1 коммутатор DES-3200-10 или DES-3528 и консольный кабель к ним;
- кабели Ethernet.

**Одно рабочее место состоит из 2-4 компьютеров (в зависимости от практической работы) с сетевыми платами (Ethernet).*

Содержание курса

1. Основные понятия в области информационной безопасности

1.1 Основные термины в области информационной безопасности
1.2 Вредоносное ПО
1.3 Угрозы безопасности сетевых информационных систем
1.4 Формирование системы информационной безопасности
1.5 Мероприятия системы защиты информации технического характера

2. Механизмы защиты информации

2.1 Антивирусные средства защиты информации
2.2 Криптографические методы защиты информации
2.3 Способы предотвращения удаленных атак на информационные системы
2.4 Межсетевой экран
2.5 Прокси-сервер
2.6 Интернет-маршрутизатор
2.7 Технологии безопасности беспроводных сетей

3. Начальная настройка межсетевого экрана

3.1 Средства управления межсетевым экраном D-Link
3.2 Подключение через Web-интерфейс
3.3 Подключение через интерфейс командной строки (CLI)

4. Протоколы и функции, обеспечивающие работу сети

3.2 Сервисы DHCP
3.2 Сервис PPPoE
3.3 Сервисы DNS
3.1 Маршрутизация
3.4 Резервирование маршрутов (Route Failover)
3.5 Балансировка нагрузки сети
3.6 IGMP для IPTV
3.7 Поддержка UPnP
3.8 Качество обслуживания (QoS) и управление полосой пропускания трафика (Traffic Shaping)
3.9 Технология SharePort

5. Протоколы и функции обеспечения безопасности сети

4.2 Виртуальные локальные сети VLAN
4.3 Виртуальные частные сети (VPN)
4.4 Технология преобразования сетевых адресов (NAT)
4.5 Механизмы PAT и NAT
4.6 Прозрачный режим (Transparent mode)
4.7 Функции IDP, WCF, AV

6. Обзор маршрутизаторов и межсетевых экранов D-Link

Практические работы

- Практическая работа № 1. **Подключение и основные настройки межсетевого экрана посредством Web-интерфейса**
- Практическая работа № 2. **Конфигурирование межсетевого экрана посредством Web-интерфейса**
- Практическая работа № 3. **Конфигурирование межсетевого экрана посредством командной строки (CLI)**
- Практическая работа № 4. **Настройка DHCP-сервера, DHCP-клиента, PPPoE-клиента**
- Практическая работа № 5. **Маршрутизация**
- Практическая работа № 6. **Резервирование маршрутов (Route Failover). Настройка маршрутизации на основе правил (Policy-Based Routing)**
- Практическая работа № 7. **Настройка балансировки нагрузки трафика**
- Практическая работа № 8. **Настройка прохождения мультикастового потока через межсетевой экран**
- Практическая работа № 9. **Настройка VLAN в межсетевом экране**
- Практическая работа № 10. **Создание PPTP-соединения**
- Практическая работа № 11. **Создание IPSec-туннеля с использованием ключей**
- Практическая работа № 12. **Организация доступа из внешней сети во внутреннюю с использованием статического преобразования адресов (SAT)**

- Практическая работа №13. **Организация доступа к серверу, расположенному в сети DMZ**
- Практическая работа №14. **Настройка прозрачного режима (Transparent mode)**
- Практическая работа № 15. **Настройка прозрачного режима (Transparent mode) с использованием коммутируемого маршрута Switch Route**

Практические работы, выполняемые факультативно

- Практическая работа №1. **Настройка ограничения полосы пропускания трафика (Traffic Shaping)**
- Практическая работа №.2. **Создание VPN-туннеля на основе L2TP over IPSec**
- Практическая работа № 3. **Создание IPSec-туннеля на основе сертификатов**

Задания для самостоятельной работы