

Введение в сетевую безопасность на базе продуктов UserGate

Программа курса



О курсе

Код курса	UG.INTRO
Длительность курса	5 дней / 40 академических часов
Описание	<p>В данном курсе рассматриваются основы построения корпоративных TCP/IP-сетей и принципы их защиты. Курс включает следующие темы:</p> <ul style="list-style-type: none">▪ базовые концепции организации TCP/IP-сетей, принципы передачи данных между устройствами, модель OSI;▪ принципы работы протокола Ethernet, коммутация трафика;▪ адресация протокола IPv4;▪ принципы маршрутизации трафика, построение таблицы маршрутизации;▪ основы работы протокола динамической маршрутизации OSPF;▪ защита сети с помощью межсетевого экрана нового поколения;▪ принципы инспектирования трафика межсетевым экраном UserGate;▪ механизмы трансляции сетевых адресов;▪ криптографические алгоритмы, технологии VPN;▪ построение защищенных туннелей для объединения офисов в единую сеть и для подключения удаленных пользователей.
Аудитория	<p>Курс предназначен для начинающих сетевых инженеров, сетевых администраторов и системных инженеров, технических специалистов отдела эксплуатации сети, специалистов отдела мониторинга и реагирования на инциденты информационной безопасности.</p>
Предварительные требования	<p>Для успешного прохождения курса вам необходимо обладать следующими знаниями и навыками:</p> <ul style="list-style-type: none">▪ навыки работы с ОС ПК;▪ базовые знания об IP-адресах.



Программа курса

1

Базовые концепции организации TCP/IP-сетей

Принципы передачи данных между

- архитектура сети;
- модель OSI;
- стек TCP/IP;
- инкапсуляция и декапсуляция.

Функции канального уровня модели OSI

- стандарт Ethernet;
- MAC-адрес;
- коммутаторы канального уровня (L2-коммутаторы);
- принципы работы коммутатора.

Функции сетевого уровня модели OSI

- протокол IP;
- бесклассовая IP-адресация;
- ICMP.

Знакомство с интерфейсом межсетевого экрана UserGate

- подключение к межсетевому экрану UserGate;
- графический интерфейс (GUI);
- интерфейс командной строки (CLI).

Процесс передачи данных по сети

- протокол ARP;
- шлюз по умолчанию.

Функции транспортного уровня модели OSI

- протоколы TCP и UDP.

Протоколы прикладного уровня модели OSI

- DHCP;
- DNS;
- SSH;
- HTTP.

Лабораторная работа 1.1. «Базовая настройка стенда»

- адресация протокола IPv4;
- знакомство со стендом;
- знакомство с NGFW UserGate;
- знакомство с маршрутизатором VyOS.

Лабораторная работа 1.2. «Механизмы передачи данных в локальной сети»

- анализ работы ARP;
- сетевые сервисы DNS и DHCP;
- знакомство со структурой пакета HTTP.



2

Основы IP-маршрутизации

Построение таблицы маршрутизации

- таблица маршрутизации;
- выбор маршрута в таблице.

Статическая маршрутизация

- статические маршруты на межсетевом экране UserGate;
- маршрут по умолчанию.

Протокол OSPF

- динамическая маршрутизация;
- OSPF;
- настройка OSPF на МЭ UserGate.

Лабораторная работа 2.1. «Основы IP-маршрутизации»

- таблица маршрутизации;
- статическая маршрутизация.

Лабораторная работа 2.2. «Внедрение протокола OSPF»

- базовая настройка OSPF с одной областью;
- дополнительные настройки OSPF.



3

Защита сети с помощью межсетевого экрана UserGate

Функции межсетевого экрана

- принципы фильтрации трафика: проблемы и решения;
- Next-Generation Firewall (NGFW).

Обзор NGFW UserGate

- экосистема продуктов UserGate SUMMA;
- межсетевой экран нового поколения;
- варианты поставки.

Способы внедрения NGFW UserGate

- способы внедрения одного узла;
- внедрение нескольких узлов.

Зоны и библиотеки элементов

- зоны;
- библиотеки элементов.

Политики сети

- правила межсетевого экрана;
- идентификация приложений;
- система обнаружения вторжений.

NAT

- способы трансляции адресов;
- настройка правил SNAT.

Обзор политик безопасности

- компоненты политики безопасности.

Лабораторная работа 3.1. «Инспекция трафика с помощью NGFW UserGate»

- правила межсетевого экрана;
- система обнаружения вторжений;
- трансляция адресов;
- дополнительные настройки безопасности.



4

Безопасность удаленных подключений

Введение в криптографические алгоритмы

- криптографические алгоритмы;
- инфраструктура открытых ключей.

Технологии VPN

- типы VPN;
- стек протоколов IPsec;
- L2TP/IPsec;
- GRE/IPsec;
- SSL/TLS.

Настройка VPN сайт-сайт на NGFW UserGate

- алгоритм настройки сервера
- алгоритм настройки клиента.

Настройка VPN удаленного доступа на NGFW UserGate

- процесс создания туннеля.

Лабораторная работа 4.1. «Безопасность удаленных подключений»

- настройка L2TP/IPsec VPN-туннеля сайт-сайт;
- настройка L2TP/IPsec VPN-туннеля удаленного доступа.

