Бауманский учебный центр «Специалист»

Программа курса FortiGate: Безопасность (авторский формат) (FortiGate Security)

Код курса: **ФОРТИНЕТСЕК**

Тема	Ак. часов
Модуль 1. Введение в Fortinet UTM • Обзор основных возможностей FortiGate. • Режимы работы. • Учетная запись администратора, разграничение прав и доступа. • Восстановление пароля администратора. • Основы работы с виртуальными доменами и виртуальными частными сетями. • Резервное копирование и восстановление. • Обновление программного обеспечения. • Настройка встроенных серверов DNS и DHCP. • **Лабораторная работа: Ознакомление с базовыми настройками системы.**	**2**
Модуль 2. Политики безопасности • Соотнесение трафика с правилами по адресам, портам, пользователям, интерфейсам и зонам. • Настройка политик файервола. • Идентификация использованных объектов. • Изменение порядка правил для корректной работы. • Использование поиска по политике для определения подходящего правила. • **Лабораторные работы: Создание политики безопасности.**	**3**
Модуль 3. Трансляция адресов и портов (NAT and PAT) • Идеология трансляции адресов и портов. • Режимы работы трансляции адресов. • Настройка политики файервола для трансляции адресов источника и получателя. • Настройка централизованной трансляции (central NAT). • Интерпретация записей в таблице сессий. • Анализ вывода команды диагностики сессий, состояния TCP, UDP и ICMP сессий. • Использование логов для решения общих проблем с NAT, мониторинг сессий с NAT. • Рекомендации по настройке NAT. • **Лабораторная работа: Трансляция адресов.**	**3**
Модуль 4. Аутентификация пользователей • Основы аутентификации, методы аутентификации, протоколы. • Использование внешних серверов аутентификации. • Описание методов активной и пассивной аутентификации. • Настройка локальной, удаленной и двухфакторной аутентификации. • Настройка внешних серверов аутентификации. • Мониторинг пользователей на файерволе. • Использование методик отладки и рекомендаций. • **Лабораторная работа: Аутентификация пользователей.**	**2**

Модуль 5. Логирование и мониторинг • Основы логирования, типы и подтипы лог-записей, их структура и уровни. • Влияние логирования на производительность. • Опции локального логирования, настройка. • Выделение места на диске, мониторинг использования диска, действия при переполнении. • Возможности логирования на внешние устройства, настройка. • Настройка передачи логов, обеспечение надежности и использование шифрации. • Настройка логирования, работа демона miglogd. • Поиск и просмотр логов из командной строки и графического интерфейса. • Настройка предупреждений по почте и весовых параметров угроз. • Настройка резервного копирования логов, их выгрузки и загрузки. • **Лабораторная работа: Настройка логирования.**	**2**
Модуль 6. Работа с сертификатами • Понятие доверенных и недоверенных сертификатов. • Установление SSL соединения между FortiGate и SSL сервером. • Настройка инспектирования SSL трафика, два варианта настройки. • Использование полной инспекцию, помехи и их преодоление. • **Лабораторная работа: Использование сертификатов.**	**2**
Модуль 7. Фильтрация Web-трафика • Описание режимов проверки трафика в FortiOS. • Фильтрация трафика в режиме Flow, профили фильтрации web-трафика. • Работа с категориями, варианты действий. • Переопределение категорий, настройка пользовательских категорий. • Запрос рейтинга в FortiGuard, настройка квот. • Дополнительные возможности фильтрации в режиме Proxy. • Переопределение web-профайлов, настройка фильтрации поисковых запросов. • Фильтрация web-контента. • Фильтрация видеоконтента. • Фильтрация DNS и файлов. • Прикрепление профайлов к политике, анализ логов. • **Лабораторная работа: Фильтрация web-трафика.**	**2**
Модуль 8. Управление приложениями • Основы управления приложениями, определение типов приложений. • Сервисы управления приложениями в FortiGuard. • Сигнатуры приложений. • Настройка управления приложениями в режиме профайлов. • Настройка управления приложениями в режиме политик. • Использование управления приложениями для шейпинга трафика. • Активация логирования и мониторинга событий, связанных с управлением приложениями. • Рекомендации по настройке управления приложениями. • Отладка работы механизма управления приложениями. • **Лабораторная работа: Управление приложениями.**	**2**

Модуль 9. Настройка антивируса • Использование сигнатур антивируса. • Режимы работы антивируса. • Использование FortiSandbox. • Различные наборы сигнатур FortiGuard. • Сравнение режимов сканирования, применение профайлов в proxy и flow режимах. • Настройка профайлов и особенностей протоколов. • Логирование и мониторинг событий, связанных с работой антивируса, просмотр статистики. • Рекомендации по настройке антивируса. • Использование аппаратных акселераторов для антивирусного сканирования. • Отладка работы механизмов антивирусного сканирования. • **Лабораторная работа: Настройка антивируса.**	**2**
Модуль 10. IPS • Компоненты IPS. • Управление обновлениями IPS через FortiGuard. • Настройка сенсоров IPS. • Применение IPS к трафику через файервол. • Обнаружение DOS-атак, настройка DOS-политики. • Выбор методологии применения IPS. • Отладка работы системы IPS. • **Лабораторная работа: Настройка IPS.**	**2**
Модуль 11. Security Fabric • Идеология построения Fortinet Security Fabric. • Развертывание Fortinet Security Fabric. • Развитие Security Fabric дополнительными компонентами и функциями. • Рейтинги и топология. • **Лабораторная работа: Развертывание Security Fabric.**	**2**
Аудиторная нагрузка в классе с преподавателем	**24 ак.ч. + 24 ак.ч. самостоятельно**

По окончании обучения на курсе проводится итоговая аттестация. Аттестация проводится в виде теста на последнем занятии или на основании оценок практических работ, выполняемых во время обучения на курсе.

Контакты центра

Для частных лиц
+7 (495) 232-32-16

Для организаций
+7 (495) 780-48-44

E-mail
info@specialist.ru