

Защита email-трафика с помощью Cisco Email Security Appliance (v3.1) (SESA)

ID CI-SESA Цена 223 900,- руб. Длительность 4 дня

Кому следует посетить

- Инженерам безопасности
- Администраторам систем безопасности
- Архитекторам решений по обеспечению безопасности
- Сетевым инженерам
- Сетевым администраторам
- Техническим специалистам, работающим с ESA
- Сетевым менеджерам
- Системным архитекторам
- Интеграторам и партнерам Cisco

Этот курс является частью следующих программ сертификаций

Cisco Certified Network Professional Security (CCNP SECURITY)

Предварительные требования

Слушатели данного курса должны обладать опытом работы и знаниями в следующих областях:

- Основы TCP/IP, включая IP адресацию и разбиение сетей на подсети, статическую маршрутизацию, DNS
- Опыт работы с SMTP и знания о форматах Интернет сообщений, форматах и частях MIME сообщений
- Опыт работы с командной строкой и графическим интерфейсом AsyncOS рекомендуется.

Цели курса

После прохождения данного курса слушатели будут уметь:

- Понимать принципы работы Cisco Email Security Appliance (ESA)
- Администрировать Cisco Email Security Appliance (ESA)
- Контролировать спам с помощью Talos SenderBase
- Использовать антивирусную защиту
- Использовать централизованные политики
- Использовать фильтры контента
- Использовать фильтры сообщений
- Настраивать механизм предотвращения утечки данных

- Настраивать и использовать запросы в LDAP
- Аутентифицировать сессии Simple Mail Transfer Protocol (SMTP)
- Использовать аутентификацию для писем
- Шифровать письма
- Использовать системные карантин
- Настраивать кластер
- Тестировать работу платформы, устранять неполадки

Содержание курса

Данный курс учит слушателей внедрять и использовать Cisco® Email Security Appliance для защиты корпоративной почтовой системы от фишинга, компрометации писем и программ вымогателей. Теоретические лекции и практические лабораторные работы позволяют познакомиться с централизованной политикой управления и контроля email-трафика на Cisco® Email Security Appliance. Кроме того, слушатели узнают, как разворачивать ESA в сети, устранять неполадки в работе и настраивать такие ключевые функции как: защита от вредоносного ПО, блокировка спама, антивирусная защита, фильтры outbreak, шифрование, карантин, защита от утечки данных.

Данный курс поможет подготовиться к сдаче экзамена Securing Email with Cisco Email Security Appliance (300-720 SESA), который позволит получить статус Certified Specialist - Email Content Security, или, в дальнейшем, статус CCNP® Security. После сдачи экзамена:

- Вы получаете статус Certified Specialist - Email Content Security
- Вы можете претендовать на получение статуса CCNP® Security. Для завершения сертификации CCNP® Security необходимо, также, сдать экзамен Implementing and Operating Cisco Security Core Technologies (350-701 SCOR)

Программа курса

Обзор платформы Cisco Email Security Appliance

Защита email-трафика с помощью Cisco Email Security Appliance (v3.1) (SESA)

- Обзор Cisco Email Security Appliance
- Обзор основных технологий
- Cisco Email Security Appliance Data Sheet
- Обзор SMTP
- Обзор процесса обработки Email
- Сценарии установки
- Базовая настройка Cisco Email Security Appliance
- Централизованные сервисы Cisco Content Security Management Appliance (SMA)
- Обзор версии ОС AsyncOS 11.x

Администрирование Cisco Email Security Appliance

- Управление системой
- Управление и мониторинг с использованием Command Line Interface (CLI)
- Расширенные настройки в GUI
- Расширенные сетевые настройки
- Использование Email Security Monitor
- Отслеживание сообщений
- Логирование

Контролирование доменов отправителей и получателей

- Настройка публичных и частных Listeners
- Таблица отправителей (HAT)
- Таблица получателей (RAT)
- Настройка маршрутизации и функций доставки

Контролирование спама с использованием SensorBase и Anti-Spam

- Обзор SenderBase
- Anti-Spam
- Управление Graymail
- Списки URL на основе репутации
- Анализ и фильтрация файлов на основе репутации
- Подтверждение отказов

Использование возможностей Anti-Virus и фильтров Outbreak Filters

- Обзор антивирусного сканирования
- Антивирусная фильтрация Sophos
- Фильтрация McAfee
- Сканирование вирусов
- Outbreak Filters
- Управление фильтрами Outbreak Filters

Использование Mail-политик

- Обзор Email Security Manager
- Обзор политик Mail Policies
- Совпадение пользователей с политикой Mail Policy

- Разделение сообщения
- Настройка политик Mail Policies

Использование фильтров контента

- Обзор
- Условия
- Действия
- Фильтрация сообщений на основе контента
- Обзор текстовых ресурсов
- Тестирование правил фильтрации на основе словарей
- Text Resources
- Управление Text Resource

Использование Message Filters в политиках

- Обзор Message Filters
- Компоненты
- Процесс работы фильтров
- Правила
- Действия фильтров
- Сканирование вложений
- Использование CLI для управления фильтрами сообщений
- Примеры
- Настройка Scan Behavior

Защита от утечки данных

- Обзор процесса сканирования Data Loss Prevention (DLP)
- Настройка Data Loss Prevention
- Политики для защиты от утечки данных
- Действия
- Обновление движка DLP Engine и категорий сообщений

й

Использование LDAP

- Обзор LDAP
- Работа с LDAP
- Использование запросов LDAP Queries
- Настройка внешней аутентификации через LDAP для пользователей
- Тестирование серверов и запросов
- Использование LDAP для предотвращения атаки Directory Harvest Attack
- Spam Quarantine Alias Consolidation Queries
- Подтверждение получателя с использованием сервера SMTP

Защита email-трафика с помощью Cisco Email Security Appliance (v3.1) (SESA)

Аутентификация сессий SMTP

- Настройка AsyncOS для аутентификации SMTP
- Аутентификация сессий SMTP с использованием клиентских сертификатов
- Проверка подлинности клиентского сертификата
- Аутентификация пользователей с использованием LDAP Directory
- Аутентификация SMTP Connection Over Transport Layer Security (TLS) с использованием клиентских сертификатов
- Установление TLS-соединения с ESA
- Обновление списка отозванных сертификатов

Аутентификация Email

- Обзор
- Настройка подписей DomainKeys и DomainKeys Identified Mail (DKIM)
- Проверка входящих сообщений с помощью DKIM
- Обзор Sender Policy Framework (SPF) и проверки SIDF
- Domain-based Message Authentication Reporting and Conformance (DMARC)
- Обнаружение поддельных сообщений

Шифрование сообщений

- Обзор Cisco Email Encryption
- Шифрование сообщений
- Добавление заголовков шифрования к сообщению
- Message Transfer Agents (MTA)
- Работа с сертификатами
- Управление списком Certificate Authorities
- Включение TLS в Listener Host Access Table (HAT)
- Включение TLS и проверка сертификатов
- Secure/Multipurpose Internet Mail Extensions (S/MIME)

Системные карантины и методы доставки

- Описание карантин
- Спам-карантин
- Централизованный спам-карантин
- Использование Safelists и Blocklists для контроля доставки сообщений
- Карантины Policy, Virus, Outbreak
- Управление карантинами
- Работа с сообщениями, которые находятся в различных карантинах
- Методы доставки

Централизованное управление с использованием кластеров

- Обзор
- Организация кластера

- Создание и подключение к кластеру
- Управление кластером
- Взаимодействие внутри кластера
- Загрузка конфигураций на платформы, которые собраны в кластер
- Рекомендации и лучшие практики

Тестирование и устранение неполадок

- Debugging Mail Flow Using Test Messages: Trace
- Устранение сетевых неполадок
- Устранение проблем Listener
- Устранение проблем с доставкой сообщения
- Нагрузка
- Оповещения о событиях
- Неполадки на физическом уровне
- Работа с технической поддержкой

Дополнительные ссылки

- Сравнение моделей для различных типов архитектур
- Требования к ресурсам для внедрения виртуальных ESA
- Лицензирование

Список лабораторных работ:

- Проверка и тестирование настроек Cisco ESA
- Базовое администрирование
- Вредоносное ПО во вложениях (Macro Detection)
- Нежелательные URL в сообщениях
- Нежелательные URL внутри вложений
- Интеллектуальная обработка не сканируемых сообщений
- Исследование AMP Cloud Intelligence
- Интеграция Cisco ESA с AMP Console
- Антивирусная защита
- Фильтрация контента и использование Outbreak Filters
- Сканирование вложений
- Настройка Data Loss Prevention
- Интеграция Cisco ESA с LDAP, включение LDAP Accept Query
- Domain Keys Identified Mail (DKIM)
- Sender Policy Framework (SPF)
- Обнаружение поддельных сообщений
- Настройка Cisco SMA для мониторинга и создания отчетов