

Защита Web-трафика с помощью Cisco Web Security Appliance (v3.0) (SWSA)

ID CI-SWSA Цена 110 000,- руб. Длительность 2 дня

Кому следует посетить

Курс будет полезен:

- Архитекторам систем безопасности
- Системным архитекторам
- Сетевым администраторам
- Инженерам безопасности
- Техническим специалистам, которые занимаются обеспечением безопасности и контроля WEB-трафика
- Интеграторам и партнерам Cisco

Этот курс является частью следующих программ сертификаций

Cisco Certified Network Professional Security (CCNP SECURITY)

Предварительные требования

Для оптимального освоения материалов курса слушателям рекомендуется обладать следующими знаниями и навыками:

- Понимать принципы работы TCP/IP сервисов, включая Domain Name System (DNS), Secure Shell (SSH), FTP, Simple Network Management Protocol (SNMP), HTTP, и HTTPS
- Понимать принципы IP-маршрутизации

Данный опыт эквивалентен сертификации CCENT (и выше) или любой другой соответствующей сертификации сетевых вендоров.

Цели курса

После прохождения данного курса слушатели будут уметь:

- Объяснять архитектуру Cisco WSA
- Внедрять проху-сервисы
- Внедрять механизмы аутентификации
- Объяснять принципы работы политики инспектирования HTTPS-трафика
- Совершать настройки acceptable use control

- Защищать инфраструктуру от вредоносного ПО
- Внедрять механизм защиты от утечки корпоративных данных
- Мониторить и устранять неполадки в работе платформы Cisco WSA

Содержание курса

Данный курс учит слушателей внедрять, использовать и обслуживать решение Cisco® Web Security Appliance (WSA), управляемое Cisco Talos, для обеспечения расширенной защиты корпоративного email-трафика и для защиты от внешних web-угроз. В ходе теоретических лекций и практических лабораторных работ слушатели узнают, как внедрять проху-сервисы, использовать дополнительную аутентификацию, внедрять политики контроля HTTPS-трафика, использовать функции защиты от зловредного ПО, внедрять механизм защиты от утечки данных из внутренней сети в Интернет, а также, как мониторить работу платформы Cisco WSA.

Данный курс поможет подготовиться к сдаче экзамена Securing the Web with Cisco Web Security Appliance (300-725 SWSA), который позволит получить статус Cisco Certified Specialist - Web Content Security, или, в дальнейшем, статус CCNP® Security. После сдачи экзамена 300-725 SWSA:

- Вы получаете статус Cisco Certified Specialist - Web 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

Описание Cisco WSA

- Обзор основных технологий для защиты WEB-трафика
- Обзор решения Cisco WSA

Защита Web-трафика с помощью Cisco Web Security Appliance (v3.0) (SWSA)

- Функции Cisco WSA
- Архитектура Cisco WSA
- Proxy-сервисы
- Механизм Data Loss Prevention
- Cisco Cognitive Intelligence
- Инструменты управления
- Cisco Advanced Web Security Reporting (AWSR) и интеграция со сторонними решениями
- Cisco Content Security Management Appliance (SMA)

Внедрение Proxy-сервисов

- Сравнение режимов Explicit Forward vs. Transparent
- Перенаправление трафика в режиме Transparent Mode
- Протокол Web Cache Control Protocol
- Процессы передачи трафика Web Cache Communication Protocol (WCCP) Upstream и Downstream
- Proxy Bypass
- Proxy Caching
- Файлы Proxy Auto-Config (PAC)
- FTP-прокси
- Прокси Socket Secure (SOCKS)
- Proxy Access Log и заголовки HTTP
- Настройка оповещений для пользователей с использованием страниц End User Notification (EUN)

Использование аутентификации

- Протоколы аутентификации
- Authentication Realms
- Использование пользовательских данных
- Аутентификация в режимах Explicit (Forward) и Transparent Proxy
- Bypassing Authentication с Problematic Agents
- Отчетность
- Re-Authentication
- Аутентификация в FTP-прокси
- Поиск и устранение неполадок, тестирование аутентификации
- Интеграция с платформой Cisco Identity Services Engine (ISE)

Создание политик для контроля трафика HTTPS

- Обзор инспектирования Transport Layer Security (TLS)/Secure Sockets Layer (SSL)
- Обзор системы сертификатов
- Обзор политик HTTPS Decryption
- Активация функции HTTPS-прокси
- Access Control List (ACL) Tags для инспекций HTTPS
- Примеры логов

Анализ политик Differentiated Traffic Access и

идентификационных профилей

- Обзор политик доступа
- Access Policy Group
- Обзор Identification Profile
- Идентификационные профили и аутентификация
- Процесс обработки политик Access Policy и профилей Identification Profiles
- Другие типы политик
- Примеры логов
- ACL Decision Tags и группы политик
- Создание и использование Time-Based, Traffic Volume Acceptable Use политик, и пользовательских уведомлений

Защита от вредоносного программного обеспечения

- Фильтры репутации
- Сканирование Anti-Malware
- Сканирование исходящего трафика
- Настройки Anti-Malware и Reputation в политиках
- Анализ и фильтрация файлов на основе репутации
- Cisco Advanced Malware Protection
- Интеграция с Cisco Cognitive Intelligence

Настройки контроля доступа

- Контроль доступа к web-ресурсам
- Фильтрация URL
- Категории URL
- Dynamic Content Analysis Engine
- Контроль приложений
- Создание ограничений Media Bandwidth Limits
- Software as a Service (SaaS) Access Control
- Фильтрация контента для взрослых

Безопасность данных, защита от утечки данных

- Data Security
- Политика Data Security
- Анализ логов

Поиск и устранение неполадок в работе Cisco Web Security Appliance

- Мониторинг Cisco Web Security Appliance
- Отчеты Cisco WSA
- Мониторинг логов System Activity Through Logs
- Задачи системного администрирования
- Процесс поиска и устранения неполадок
- Command Line Interface

Дополнительные ссылки

Защита Web-трафика с помощью Cisco Web Security Appliance (v3.0) (SWSA)

- Сравнение моделей Cisco WSA
- Сравнение моделей Cisco SMA
- Обзор руководства «Connect, Install, and Configure»
- Развертывание шаблона Cisco Web Security Appliance Open Virtualization Format (OVF)
- Подключение портов Cisco Web Security Appliance Virtual Machine (VM) к правильным сетям
- Подключение Cisco Web Security Virtual Appliance
- Включение Layer 4 Traffic Monitor (L4TM)
- Запуск и использование System Setup Wizard
- Переподключение Cisco Web Security Appliance
- Обзор отказоустойчивых топологий
- Отказоустойчивость на физическом уровне
- Введение в Common Address Redundancy Protocol (CARP)
- Создание Failover Groups для High Availability
- Обзор архитектур и сценарии использования Cisco AnyConnect® Secure Mobility