Примечания к выпуску

CCNA Security. Внедрение системы сетевой безопасности 2.0

Последнее обновление: декабрь 5, 2017

Назначение

Курс Cisco CCNA® Security – это второй выпуск основной программы CCNA Security по сетевой безопасности Сетевой академии Cisco. Курс CCNA Security соответствует сертификационному экзамену Implementing Cisco Network Security (IINS) (Безопасность в сетях) (210-260). В настоящих примечаниях содержится подробное описание данного выпуска, включающее содержание курса, известные проблемы и информацию о поддержке.

Таблица 1. Содержание выпуска

Компонент	Описание
Содержание электронного курса	11 глав
Лабораторные работы	16 практических лабораторных работ с использованием маршрутизаторов 1941 и коммутаторов 2960
Проверка практических навыков	1 экзамен по проверке практических навыков с использованием оборудования
Упражнения, выполняемые в программе Cisco® Packet Tracer	13 упражнений, выполняемых в программе Packet Tracer Требуется версия PT 6.2.x или выше
Предварительное тестирование	Один предварительный тест, целью которого является проверка соответствия предварительным требованиям, а также текущего уровня учащихся. Таким образом, можно определить уровень знаний учащихся до начала курса, чтобы лучше спланировать и персонализировать учебную программу.
Контрольные работы по итогам глав	11 адаптируемых контрольных работ по материалу пройденных глав
Экзамены по главам	11 экзаменов по главам, содержащих вопросы с моделированием ситуации, вопросы с возможностью выбора из нескольких вариантов и вопросы, в которых надо заполнить пустые поля
Syntax Checker	41 упражнение на использование Syntax Checker
Проверка практических навыков в программе Packet Tracer	Одно задание в Packet Tracer на проверку практических навыков для лучшего усвоения приобретенных знаний
Финальный экзамен	Один финальный экзамен с несколькими вопросами для проверки практических навыков
Специальные возможности	11 глав, содержащих текст расширенного доступа и медиатекст. Видеоматериалы содержат скрытые субтитры (CC)

Известные проблемы и рекомендации

Элемент	Описание
Размер текстовой области	Если изменить размер текстовой области страницы, на следующих страницах сохранится такой же размер текстовой области. По окончании сеанса в браузере размер текстовой области возвращается к размеру по умолчанию.
PDF-файлы с заполняемыми формами	Откройте документы формата PDF в программе Adobe Reader и убедитесь, что поля заполняемых форм отображаются корректно. Эти документы не рекомендуется открывать в веб-браузере.
Syntax Checker	Функциональность данного инструмента ограничена отдельными инструкциями, приведенными в рамках задания на использование Syntax Checker.

Согласование материала сертификационного экзамена

Разница между версиями IINS 640-554 и IINS 210-260.

Темы, исключенные из курса	Темы, добавленные в курс
2.1.a Функция аудита безопасности CCP	1.1.b Описание технологии SIEM
2.1.b Функция блокировки CCP за один шаг	1.2.b Описание социальной инженерии
2.4 Описание перехода с IPv4 на IPv6 2.4.a Причины перехода на IPv6 2.4.b Понимание IPv6-адресации 2.4.c Назначение IPv6-адресов 2.4.d Особенности маршрутизации для IPv6	1.2.d Классификация векторов потери/утечки данных
3.1.a AAA с использованием CCP на маршрутизаторах	1.4. Описание сетевых топологий 1.4.a Локальная сеть комплекса зданий (Campus Area Network, CAN) 1.4.b Облако, глобальная сеть (Wide Area Network, WAN) 1.4.c Центр обработки данных 1.4.d Малые и домашние офисы (small office and home office, SOHO) 1.4.e Безопасность сети в виртуальной среде
4.1.c Типы ACL-списков (динамические, рефлексивные, временные)	2.1.c Конфигурирование и проверка безопасного доступа по протоколу SNMP v3 с использованием ACL-списка
4.1.j VLSM	2.4.b Описание решения по управлению мобильными устройствами (Mobile Device Management, MDM)
4.3.e. CCP	5.3 Реализация NAT на Cisco ASA 9.x
4.3.g VACL-списки	5.5 Функции межсетевого экрана на многофункциональном устройстве безопасности Cisco (Adaptive Security Appliance, ASA) 9.x
5.2.g CCP	7.1.a Фильтрация спама, фильтрация вредоносного ПО, DLP, черные списки, шифрование электронной почты
7.4 Внедрение межсетевого экрана с зонированием с использованием CCP	7.2.b Черные списки, фильтрация URL-адресов, сканирование вредоносного ПО, категоризация URL-адресов, фильтрация веб-приложений, шифрование TLS/SSL
8.3 Конфигурирование Cisco IOS IPS с использованием CCP 8.3.a Ведение журналов 8.3.b Сигнатуры	7.3.a Антивирусное ПО/защита от вредоносного ПО
9.4.a CCP	7.3.c Аппаратное/программное шифрование локальных данных

Соответствие целям сертификации

Посмотрите, в каких разделах курса CCNA Security рассматриваются задачи экзамена IINS 210-260

Задачи экзамена IINS 210-260	Разделы курса CCNAS v2.0
1.0 Концепция безопасности	
1.1. Общие принципы безопасности	Глава 1 Современные угрозы сетевой безопасности
1.1.a Описание конфиденциальности, целостности, доступности (CIA)	Раздел 1.2 Сетевые угрозы
1.1.b Описание технологии SIEM	Раздел 1.3 Нейтрализация угроз
1.1.c Определение общепринятых терминов безопасности	Глава 4 Внедрение технологий межсетевого экрана
1.1.d Определение общепринятых зон сетевой безопасности	Раздел 4.2 Технологии межсетевых экранов
	Глава 11 Управление безопасной сетью
	Раздел 11.1 Тестирование безопасности сети
1.2 Типичные угрозы безопасности	Глава 1 Современные угрозы сетевой безопасности
1.2.a Определение типичных сетевых атак	Раздел 1.1 Защита сетей
1.2.b Описание социальной инженерии	Раздел 1.2 Сетевые угрозы

Задачи экзамена IINS 210-260	Разделы курса CCNAS v2.0
1.2.c Определение вредоносного ПО 1.2.d Классификация векторов потери/утечки данных	Глава 11 Управление безопасной сетью Раздел 11.2 Разработка комплексной политики безопасности
1.3. Принципы криптографии 1.3.a Описание обмена ключами 1.3.b Описание алгоритма хеширования 1.3.c Сравнение симметричного и асимметричного шифрования, выявление разницы 1.3.d Описание цифровых подписей, сертификатов и PKI	Глава 7 Криптографические системы Раздел 7.2 Базовые сведения о целостности и аутентификации Раздел 7.3 Конфиденциальность Раздел 7.4 Криптография с открытым ключом
1.4. Описание сетевых топологий 1.4.a Локальная сеть комплекса зданий (Campus Area Network, CAN) 1.4.b Облако, глобальная сеть (Wide Area Network, WAN) 1.4.c Центр обработки данных 1.4.d Малые и домашние офисы (small office and home office, SOHO) 1.4.e Безопасность сети в виртуальной среде	Глава 1 Современные угрозы сетевой безопасности Раздел 1.1 Защита сетей Раздел 1.2 Сетевые угрозы
2.0 Защищенный доступ	
2.1 Защищенное управление 2.1.a Сравнение внутриполосных (In-band) и внеполосных (out of band) методов 2.1.b Конфигурирование управления защищенной сетью 2.1.c Конфигурирование и проверка безопасного доступа по протоколу SNMP v3 с использованием ACL-списка 2.1.d Конфигурирование и проверка безопасности для NTP 2.1.e Использование SCP для передачи файлов	Глава 2 Обеспечение безопасности сетевых устройств Раздел 2.1 Защита доступа к устройствам Раздел 2.3 Мониторинг устройств и управление ими
2.2 Принципы AAA 2.2.a Описание технологий RADIUS и TACACS+ 2.2.b Конфигурирование административного доступа на маршрутизаторе Cisco с использованием TACACS+ 2.2.c Проверка связи маршрутизатора Cisco с сервером TACACS+ 2.2.d Рассмотрение интеграции Active Directory с AAA 2.2.e Описание аутентификации и авторизации с использованием ACS и ISE	Глава 3 Аутентификация, авторизация и учет Раздел 3.3 Серверное решение AAA Раздел 3.4 Серверная аутентификация AAA
2.3 Аутентификация 802.1x 2.3.a Идентификация компонентов функций 802.1x	Глава 3 Аутентификация, авторизация и учет Раздел 3.5 Серверная авторизация и учет AAA
2.4 BYOD (Bring-Your-Own-Device, Принеси на работу свое устройство) 2.4.a Описание структуры архитектуры BYOD 2.4.b Описание решения по управлению мобильными устройствами (Mobile Device Management, MDM)	Глава 1 Современные угрозы сетевой безопасности Раздел 1.1 Защита сетей
3.0 Виртуальные частные сети (VPN)	
3.1 Принципы VPN 3.1.a Описание протоколов IPSec и режимов доставки (IKE, ESP, AH, туннельный режим, транспортный режим) 3.1.b Описание Hairpinning, Split Tunneling, Always-on, NAT Traversal	Глава 8 Внедрение виртуальных частных сетей (VPN) Раздел 8.2 Компоненты и функционирование IPsec VPN
3.2 VPN удаленного доступа (Remote Access)	Глава 10 Многофункциональное устройство безопасности Cisco (Adaptive

Задачи экзамена IINS 210-260	Разделы курса CCNAS v2.0
3.2.a Внедрение базовой сети SSL VPN без использования клиента с помощью ASDM 3.2.b Проверка подключения без использования клиента 3.2.a Внедрение базовой сети AnyConnect SSL VPN с помощью ASDM 3.2.d Проверка подключения AnyConnect 3.2.e Определение оценки профиля оконечного устройства	Security Appliance, ASA) с расширенной функциональностью Раздел 10.2 Конфигурация ASA VPN
3.3 Site-to-Site VPN 3.3.a Реализация сети IPSec site-to-site VPN с аутентификацией с общим ключом на маршрутизаторах Cisco и межсетевых экранах ASA 3.3.b Проверка сети IPSec site-to-site VPN	Глава 10 Многофункциональное устройство безопасности Cisco (Adaptive Security Appliance, ASA) с расширенной функциональностью Раздел 10.2 Конфигурация ASA VPN
4.0 Безопасная маршрутизация и коммутация	
4.1 Система безопасности на маршрутизаторах Cisco 4.1.a Конфигурирование нескольких уровней привилегий 4.1.b Конфигурирование доступа CLI на основе ролей IOS 4.1.c Внедрение отказоустойчивой конфигурации IOS	Глава 2 Обеспечение безопасности сетевых устройств Раздел 2.2 Назначение административных ролей Раздел 2.3 Мониторинг устройств и управление ими
4.2 Защита протоколов маршрутизации 4.2.a Внедрение аутентификации для обновления маршрутизации на OSPF	Глава 2 Обеспечение безопасности сетевых устройств Раздел 2.5 Защита плоскости управления
4.3 Защита плоскости управления 4.3.a Объяснение функции Control Plane Policing (ограничение плоскости управления)	Глава 2 Обеспечение безопасности сетевых устройств Раздел 2.5 Защита плоскости управления
4.4 Типичные атаки на уровне 2 4.4.a Описание атак на STP 4.4.b Описание спуфинга ARP 4.4.c Описание спуфинга MAC 4.4.d Описание переполнения таблицы CAM (таблицы MAC-адресов) 4.4.e Описание разведывательных атак CDP/LLDP 4.4.f Описание атак перехода в сетях VLAN 4.4.b Описание спуфинга DHCP	Глава 6 Обеспечение безопасности локальной сети (LAN) Раздел 6.2 Факторы, которые необходимо учитывать при обеспечении безопасности на уровне 2
4.5 Процедуры нейтрализации 4.5.a Внедрение спуфинга DHCP 4.5.b Внедрение динамического инспектирования ARP 4.5.c Внедрение функции Port Security 4.5.d Описание технологий BPDU Guard, Root Guard, Loop Guard 4.5.e Проверка процедур нейтрализации	Глава 6 Обеспечение безопасности локальной сети (LAN) Раздел 6.2 Факторы, которые необходимо учитывать при обеспечении безопасности на уровне 2
4.6 Безопасность VLAN 4.6.a Описание проблем обеспечения безопасности PVLAN 4.6.a Описание проблем обеспечения безопасности нативной (Native) VLAN	Глава 6 Обеспечение безопасности локальной сети (LAN) Раздел 6.2 Факторы, которые необходимо учитывать при обеспечении безопасности на уровне 2
5.0 Технологии межсетевых экранов Cisco	
5.1 Описание функциональных преимуществ и недостатков разных технологий межсетевых экранов 5.1.a Межсетевые экраны прокси-сервера	Глава 4 Внедрение технологий межсетевого экрана Раздел 4.2 Технологии межсетевых экранов

Задачи экзамена IINS 210-260	Разделы курса CCNAS v2.0
5.1.b Межсетевой экран уровня приложений 5.1c Персональный межсетевой экран	Глава 6 Обеспечение безопасности локальной сети (LAN) Раздел 6.1 Безопасность оконечных устройств
5.2 Сравнение межсетевых экранов с сохранением состояния и без 5.2.a Функционирование 5.2.b Функция таблицы состояний	Глава 4 Внедрение технологий межсетевого экрана Раздел 4.2 Технологии межсетевых экранов
5.3 Реализация NAT на Cisco ASA 9.x 5.3.a Статическое преобразование 5.3.b Динамическое преобразование 5.3.c PAT 5.3.d NAT на основе политик 5.3 e Проверка работы NAT	Глава 9 Внедрение многофункционального устройства защиты Cisco Adaptive Security Appliance (ASA) Раздел 9.2 Конфигурация межсетевого экрана ASA Глава 10 Многофункциональное устройство безопасности Cisco (Adaptive Security Appliance, ASA) с расширенной функциональностью Раздел 10.1 ASA Security Device Manager (ASDM)
5.4 Внедрение зонального межсетевого экрана 5.4.a Из зоны в зону 5.4.b Собственная зона	Глава 4 Внедрение технологий межсетевого экрана Раздел 4.2 Технологии межсетевых экранов
5.5 Функции межсетевого экрана на многофункциональном устройстве безопасности Cisco (Adaptive Security Appliance, ASA) 9.x 5.5.a Конфигурирование управления доступом для ASA 5.5.b Конфигурирование политик защищенного доступа 5.5.c Конфигурирование уровней безопасности интерфейса Cisco ASA 5.5.d Конфигурирование модульной системы политик (Modular Policy Framework, MPF) по умолчанию 5.5.e Описание режимов развертывания (межсетевой экран с маршрутизацией, прозрачный межсетевой экран) 5.5.f Описание способов реализации высокой доступности 5.5.g Описание контекстов безопасности 5.5.h Описание сервисов межсетевого экрана	Глава 9 Внедрение многофункционального устройства защиты Cisco Adaptive Security Appliance (ASA) Раздел 9.1 Знакомство с ASA Раздел 9.2 Конфигурация межсетевого экрана ASA
6.0 Системы предотвращения вторжений (IPS)	
6.1 Описание факторов, которые необходимо учесть при развертывании IPS 6.1.a Сравнение IPS на основе сети и IPS на основе хоста 6.1.b Режимы развертывания (Inline, Promiscuous – SPAN, tap) 6.1.c Размещение (позиционирование IPS в сети) 6.1.d Ложно позитивный, ложно негативный, истинно позитивный, истинно негативный	Глава 5 Внедрение системы предотвращения вторжений Раздел 5.1 Технологии IPS Раздел 5.2 Сигнатуры IPS
6.2 Описание технологий IPS 6.2.a Правила/сигнатуры 6.2.b Модули обнаружения/сигнатур 6.2.c Триггерные действия/ответы (отбрасывание, сброс, блокировка, предупреждение, мониторинг/регистрация в журнале, shun) 6.2.d Черный список (статический и динамический)	Глава 5 Внедрение системы предотвращения вторжений Раздел 5.2 Сигнатуры IPS
7.0. Безопасность контента и оконечных устройств	
7.1 Описание технологий нейтрализации угроз электронной почты	Глава 6 Обеспечение безопасности локальной сети (LAN)

Задачи экзамена IINS 210-260	Разделы курса CCNAS v2.0
7.1.a Фильтрация спама, фильтрация вредоносного ПО, DLP, черные списки, шифрование электронной почты	Раздел 6.1 Безопасность оконечных устройств
7.2 Описание технологий нейтрализации угроз веб-трафика	Глава 6 Обеспечение безопасности локальной сети (LAN)
7.2.a Локальные и облачные веб-прокси	Раздел 6.1 Безопасность оконечных устройств
7.2.b Черные списки, фильтрация URL-адресов, сканирование вредоносного ПО, категоризация URL-адресов, фильтрация веб-приложений, шифрование TLS/SSL	
7.3 Описание технологий нейтрализации угроз оконечным устройствам	Глава 5 Внедрение системы предотвращения вторжений
7.3.a Антивирусное ПО/защита от вредоносного ПО	Раздел 5.1 Технологии IPS
7.3.b Персональный межсетевой экран/HIPS	Глава 6 Обеспечение безопасности локальной сети (LAN)
7.3.c Аппаратное/программное шифрование локальных данных	Раздел 6.1 Безопасность оконечных устройств

Поддержка

Чтобы получить помощь по общим вопросам, связанным с материалом учебного курса, занятиями в аудитории или обучающими программами, обращайтесь в службу поддержки Сетевой академии Networking Academy™. Для этого войдите в среду обучения Cisco NetSpace и нажмите **Help > Contact Support** (Справка > Связаться со службой поддержки) в верхней части страницы.

Россия, 121614, Москва,
ул. Крылатская, д.17, к.4 (Krylatsky Hills)
Телефон: +7 (495) 961 1410,
факс: +7 (495) 961 1469
www.cisco.ru, www.cisco.com

Россия, 197198, Санкт-Петербург,
бизнес-центр «Арена Холл»,
пр. Добролюбова, д. 16, лит. А, корп. 2
Телефон: +7 (812) 313 6230,
факс: +7 (812) 313 6280
www.cisco.ru, www.cisco.com

Украина, 03038, Киев,
бизнес-центр «Горизонт Парк»,
ул. Николая Гринченко, 4В
Телефон: +38 (044) 391 3600,
факс: +38 (044) 391 3601
www.cisco.ua, www.cisco.com

Беларусь, 220034, Минск,
бизнес-центр «Виктория Плаза»,
ул. Платонова, д. 1Б, 3 п., 2 этаж.
Телефон: +375 (17) 269 1691,
факс: +375 (17) 269 1699
www.cisco.ru, www.cisco.com

Казахстан, 050059, Алматы, бизнес-центр «Самал Тауэрс», ул. О. Жолдасбекова, 97, блок А2, 14 этаж
Телефон: +7 (727) 244 2101,
факс: +7 (727) 244 2102

Азербайджан, AZ1010, Баку,
ул. Низами, 90А, «Лэндмарк» здание III, 3 этаж
Телефон: +994 (12) 437 4820,
факс: +994 (12) 437 4821

Узбекистан, 100000, Ташкент,
бизнес центр INCONEL, ул. Пушкина, 75, офис 605
Телефон: +998 (71) 140 4460,
факс: +998 (71) 140 4465