300-210

Implementing Cisco Threat Control Solutions

NWExam.com

SUCCESS GUIDE TO CISCO CERTIFICATION

Exam Summary – Syllabus – Questions

Table of Contents

Introduction to 300-210 Exam on Implementing Cisco Threat Control Solutions

A great way to start the Cisco Certified Network Professional Security (SITCS) preparation is to begin by properly appreciating the role that syllabus and study guide play in the Cisco 300-210 certification exam. This study guide is an instrument to get you on the same page with Cisco and understand the nature of the Cisco CCNP Security exam.

Our team of experts has composed this Cisco 300-210 exam preparation guide to provide the overview about Cisco Implementing Cisco Threat Control Solutions exam, study material, sample questions, practice exam and ways to interpret the exam objectives to help you assess your readiness for the Cisco SITCS exam by identifying prerequisite areas of knowledge. We recommend you to refer the simulation questions and practice test listed in this guide to determine what type of questions will be asked and the level of difficulty that could be tested in the Cisco CCNP Security certification exam.

Cisco 300-210 Certification Details:

Exam Name	Implementing Cisco Threat Control Solutions
Exam Number	300-210 SITCS
Exam Price	$300 USD
Duration	90 minutes
Number of Questions	65-75
Passing Score	Variable (750-850 / 1000 Approx.)
Recommended Training	Implementing Cisco Threat Control Solutions (SITCS)
Exam Registration	PEARSON VUE
Sample Questions	Cisco 300-210 Sample Questions
Practice Exam	**Cisco Certified Network Professional Security Practice Test**

Cisco 300-210 Exam Syllabus:

Section	Weight	Objectives
Content Security	27%	1 Cisco Cloud Web Security (CWS) a) Describe the features and functionality b) Implement the IOS and ASA connectors c) Implement the Cisco AnyConnect web security module d) Implement web usage control e) Implement AVC f) Implement antimalware g) Implement decryption policies 2 Cisco Web Security Appliance (WSA) a) Describe the features and functionality b) Implement data security c) Implement WSA identity and authentication, including transparent user identification d) Implement web usage control e) Implement AVC f) Implement antimalware and AMP g) Implement decryption policies h) Implement traffic redirection and capture methods (explicit proxy vs. transparent proxy) 3 Cisco Email Security Appliance a) Describe the features and functionality b) Implement email encryption c) Implement antispam policies d) Implement virus outbreak filter e) Implement DLP policies f) Implement antimalware and AMP g) Implement inbound and outbound mail policies and authentication h) Implement traffic redirection and capture methods i) Implement ESA GUI for message tracking
Network Threat Defense	22%	1 Cisco Next-Generation Firewall (NGFW) Security Services a) Implement application awareness b) Implement access control policies (URL-filtering, reputation based, file filtering) c) Configure and verify traffic redirection d) Implement Cisco AMP for Networks 2 Cisco Advanced Malware Protection (AMP) a) Describe cloud detection technologies

Section	Weight	Objectives
		b) Compare and contrast AMP architectures (public cloud, private cloud) c) Configure AMP endpoint deployments d) Describe analysis tools e) Describe incident response functionality f) Describe sandbox analysis g) Describe AMP integration
Cisco FirePOWER Next-Generation IPS (NGIPS)	20%	1 Configurations 2 Describe traffic redirection and capture methods a Describe preprocessors and detection engines b Implement event actions and suppression thresholds c Implement correlation policies d Describe SNORT rules e Implement SSL decryption policies 3 Deployments a Deploy inline or passive modes b Deploy NGIPS as appliance, virtual appliance, or module within an ASA c Describe the need for traffic symmetry d Compare inline modes: inline interface pair and inline tap mode
Security Architectures	17%	1 Design a web security solution a) Compare and contrast Cisco FirePOWER NGFW, WSA, and CWS b) Compare and contrast physical WSA and virtual WSA c) Describe the available CWS connectors 2 Design an email security solution a) Compare and contrast physical ESA and virtual ESA b) Describe hybrid mode 3 Design Cisco FirePOWER solutions a) Configure the virtual routed, switched, and hybrid interfaces b) Configure the physical routed interfaces
Troubleshooting, Monitoring, and Reporting Tools	14%	1 Design a web security solution a) Compare and contrast FirePOWER NGFW, WSA, and CWS b) Compare and contrast physical WSA and virtual WSA c) Describe the available CWS connectors

Section	Weight	Objectives
		2 Cisco Web Security Appliance (WSA) a) Implement the WSA Policy Trace tool b) Describe WSA reporting functionality c) Troubleshoot using CLI tools 3 Cisco Email Security Appliance (ESA) a) Implement the ESA Policy Trace tool b) Describe ESA reporting functionality c) Troubleshoot using CLI tools 4 Cisco FirePOWER a) Describe the Cisco FirePOWER Management Center dashboards and reports b) Implement health policy c) Configure email, SNMP, and syslog alerts d) Troubleshoot NGIPS using CLI tools

300-210 Sample Questions:

01. Which part of design methodology is important for identifying organizational goals?
a) Existing network and sites characterization
b) Conceptual architecture examination
c) Design of the network topology and solutions
d) Customer requirements identification
e) Design validation

02. Which two tasks are parts of characterizing an existing network?
(Choose two)
a) Using design tools to create a framework for the design
b) Collecting information using the existing documentation and direct organizational input
c) Using tools for automated auditing of the network
d) Identifying the business objectives of the organization

03. Which two of these reasons explain why you would modularize?
(Choose two)
a) To reduce the amount of data that the network device needs to process
b) To increase the amount of data that the network device needs to process
c) To reduce the amount of data that the engineer must manage
d) To increase the amount of data that the engineer must manage
e) To make it easier to have multiple routing protocols running in the network

04. Which two of these reasons explain why the hub-and-spoke topology is the basis for hierarchical design?
(Choose two)
a) It has better convergence than ring topology
b) It is the only topology compatible with Cisco devices
c) It scales better than full-mesh topology
d) It is the only standardized topology
e) It was invented before full-mesh and ring topologies

05. Which statement is true about a good IPv4 addressing plan?
a) Each individual point-to-point link should have its own separate /24 subnet
b) The user subnets size should always be designed for best fit because you can always allocate more addresses later
c) The management subnet should only be allocated after all other addressing is designed and implemented
d) You should dedicate a separate subnet for remote access

06. Which two statements about IPv6 addressing are true?
(Choose two)
a) The best way to subnet a /48 IPv6 prefix is to use IPv4 addresses and translate them from decimal to hexadecimal
b) Stateless autoconfiguration works with prefixes between /40 and /64
c) If you need a provider-independent address, you will need to go directly to IANA
d) /48 is a typical prefix that RIR or ISP assigns to you
e) If you use both IPv4 and IPv6 in your network, you want to strive to have a dual-stack network

07. Which two statements are true about campus design?
(Choose two)
a) For optimal distribution-to-core layer convergence, you should build triangles, not squares
b) Peering across the access layer should be limited as much as possible
c) Summarization within the campus network should be avoided
d) Within the campus, CEF should be disabled to get the best convergence
e) Summarization should not be performed at the boundary where the distribution layer of each building connects to the core

08. Which statement is true about VPNs?
a) With Layer 2 VPNs, the customer exchanges routes with SP routers
b) Examples of Layer 3 VPNs are VPLS and VPWS
c) With a Layer 2 VPN, the enterprise will maintain control over Layer 3 policies
d) From a provider perspective, Layer 2 VPNs are the most scalable solution

09. What are three properties and one-way requirements for voice traffic?
(Choose three)
a) Bursty
b) Smooth
c) Latency should be below 400 ms
d) Latency should be below 150 ms
e) Bandwidth required is roughly between 30 and 128 kbps
f) Bandwidth required is roughly between 0.5 and 20 Mbps

10. What are the main benefits of Cisco ACI?
a) Made by Cisco
b) Centralized application policy management
c) Requires that engineers configure each network device separately
d) Provides a platform-as-a-service infrastructure for running your applications

Answers to 300-210 Exam Questions:

Question: 01 Answer: d	Question: 02 Answer: b, c	Question: 03 Answer: a, c	Question: 04 Answer: a, c	Question: 05 Answer: d
Question: 06 Answer: d, e	Question: 07 Answer: a, b	Question: 08 Answer: c	Question: 09 Answer: b, d, e	Question: 10 Answer: b

Note: If you find any typo or data entry error in these sample questions, we request you to update us by commenting on this page or write an email on feedback@nwexam.com