Cisco CCNA Security 210-260 Certification Exam Details

Cisco 210-260 certifications are globally accepted and add significant value to your IT professional. The certification will give you a serious idea of every one of the workings of the network models as well as the devices which might be utilized by it. NWexam.com is proud to offer to you the best quality Cisco Exam Guides.

The Cisco 210-260 Exam is challenging, and thorough preparation is crucial for success. This cert guide is designed to allow you to prepare for the CCNA Security certification exam. It contains reveal set of the individuals covered about the Professional exam. These guidelines for the IINS will help make suggestions from the study process to your certification.

To have Implementing Cisco Network Security certification, you are required to pass IINS 210-260 exam. This exam is produced keeping in mind the input of pros in the market and reveals how Cisco merchandise is employed in organizations around the globe.
210-260 Implementing Cisco Network Security Exam Summary

? Exam Name: Implementing Cisco Network Security
? Exam Code: 210-260
? Exam Price: $300 (USD)
? Duration: 90 mins
? Number of Questions: 60-70
? Passing Score: Variable (750-850 / 1000 Approx.)
210-260 Exam Guide:
? How I pass Cisco 400-201 Certification in first attempt?
? How to organize for 400-201 exam on CCIE Supplier
Topics covered inside the CCNA Security 210-260 Exam
[1]. Security Concepts (12%)

1 Common security principles
a) Describe confidentiality, integrity, availability (CIA)
b) Describe SIEM technology
c) Identify common security terms
d) Identify common network security zones

2 Common security threats
a) Identify common network attacks
b) Describe social engineering
c) Identify malware
d) Classify the vectors of knowledge loss/exfiltration

3 Cryptography concepts
a) Describe key exchange
b) Describe hash algorithm
c) Compare and contrast symmetric and asymmetric encryption
d) Describe digital signatures, certificates, and PKI

4 Describe network topologies
a) Campus area network (CAN)
b) Cloud, wide area network (WAN)
c) Data center
d) Small office/home office (SOHO)
e) Network security for an electronic environment

[2]. Secure Access (14%)
1 Secure management
a) Compare in-band and out-of band
b) Configure secure network management
c) Configure and verify secure access through SNMP v3 having an ACL
d) Configure and verify security for NTP
e) Use SCP for file transfer

2 AAA concepts
a) Describe RADIUS and TACACS+ technologies
b) Configure administrative access with a Cisco router using TACACS+
c) Verify connectivity over a Cisco router into a TACACS+ server
d) Explain the combination of Active Directory with AAA
e) Describe authentication and authorization using ACS and ISE

3 802.1X authentication
a) Identify the functions 802.1X components

4 BYOD

a) Describe the BYOD architecture framework
b) Describe the function of mobile device management (MDM)

[3]. VPN (17%)

1 VPN concepts
a) Describe IPsec protocols and delivery modes (IKE, ESP, AH, tunnel mode, transport mode)
b) Describe hairpinning, split tunneling, always-on, NAT traversal

2 Remote access VPN
a) Implement basic clientless SSL VPN using ASDM
b) Verify clientless connection
c) Implement basic AnyConnect SSL VPN using ASDM
d) Verify AnyConnect connection
e) Identify endpoint posture assessment

3 Site-to-site VPN
a) Implement an IPsec site-to-site VPN with pre-shared key authentication on Cisco routers and ASA firewalls
b) Verify an IPsec site-to-site VPN
[4]. Secure Routing and Switching (18%)

1 Security on Cisco routers
a) Configure multiple privilege levels
b) Configure Cisco IOS role-based CLI access
c) Implement Cisco IOS resilient configuration

2 Securing routing protocols
a) Implement routing update authentication on OSPF

3 Securing the control plane
a) Explain the function of control plane policing

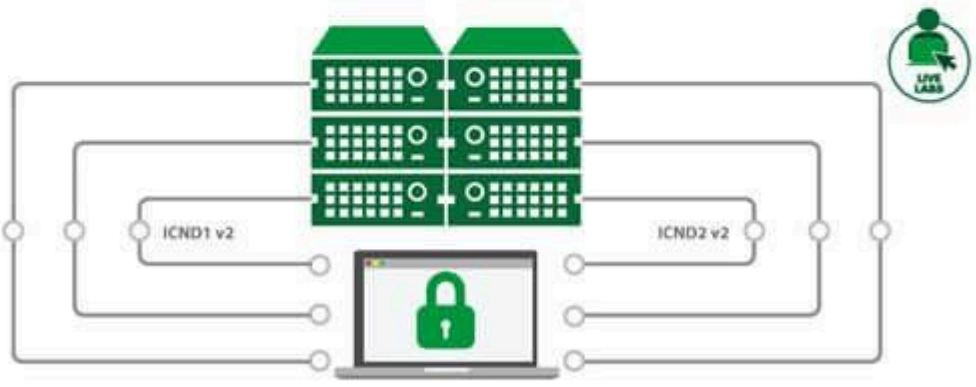
4 Common Layer 2 attacks
a) Describe STP attacks
b) Describe ARP spoofing
c) Describe MAC spoofing
d) Describe CAM table (MAC address table) overflows
e) Describe CDP/LLDP reconnaissance

f) Describe VLAN hopping
g) Describe DHCP spoofing

5 Mitigation procedures
a) Implement DHCP snooping
b) Implement Dynamic ARP Inspection
c) Implement port security
d) Describe BPDU guard, root guard, loop guard
e) Verify mitigation procedures

6 VLAN security
a) Describe the protection implications of a PVLAN
b) Describe the protection implications of the native VLAN

[5]. Cisco Firewall Technologies (18%)



1 Describe operational pros and cons of the different firewall technologies
a) Proxy firewalls
b) Application firewall

c) Personal firewall

2 Compare stateful vs. stateless firewalls
a) Operations
b) Aim of the state table

3 Implement NAT on Cisco ASA 9.x
a) Static
b) Dynamic
c) PAT
d) Policy NAT
e) Verify NAT operations

4 Implement zone-based firewall
a) Zone to zone
b) Self zone

5 Firewall features on the Cisco Adaptive Security Appliance (ASA) 9.x
a) Configure ASA access management
b) Configure security access policies
c) Configure Cisco ASA interface security levels
d) Configure default Cisco Modular Policy Framework (MPF)
e) Describe modes of deployment (routed firewall, transparent firewall)
f) Describe types of implementing high availability
g) Describe security contexts
h) Describe firewall services

[6]. IPS (9%)

1 Describe IPS deployment considerations
a) Network-based IPS vs. host-based IPS
b) Modes of deployment (inline, promiscuous - SPAN, tap)
c) Placement (positioning with the IPS inside the network)
d) False positives, false negatives, true positives, true negatives

2 Describe IPS technologies
a) Rules/signatures
b) Detection/signature engines
c) Trigger actions/responses (drop, reset, block, alert, monitor/log, shun)

d) Blacklist (static and dynamic)
[7]. Content and Endpoint Security (12%)

1 Describe mitigation technology for email-based threats
a) SPAM filtering, anti-malware filtering, DLP, blacklisting, email encryption

2 Describe mitigation technology for web-based threats
a) Local and cloud-based web proxies
b) Blacklisting, URL filtering, malware scanning, URL categorization, web application filtering, TLS/SSL decryption

3 Describe mitigation technology for endpoint threats
a) Anti-virus/anti-malware
b) Personal firewall/HIPS
c) Hardware/software encryption of local data

Which questions is for the Cisco 210-260 exams?
? Single answer multiple choice
? Multiple answer multiple choice
? Drag and Drop (DND)
? Router Simulation
? Testlet
CCNA Security 210-260 Practice Exam Questions.
Grab a comprehension out there Cisco 210-260 sample answers and questions and enhance your 210-260 exam preparation towards attaining an Implementing Cisco Network Security Certification. Answering these sample questions could make familiar with like questions you may expect for the actual exam. Doing practice with CCNA Security IINS questions and answers ahead of the exam whenever possible is the key to passing the Cisco 210-260 certification exam.

210-260 Implementing Cisco Network Security Sample Questions:-

01. Which type of traffic inspection uses pattern matching?
a) Signature-based inspection
b) Statistical anomaly detection
c) Protocol verification
d) Policy-based inspection
Answer: a

02. Which from the following authentication mechanisms works extremely well with SNMP version 3?
(Choose two)
a) AES
b) MD5
c) 3DES
d) SHA
Answer: b, d

03. Exactly what is the most popular type of spoofing?
a) Application spoofing
b) Service spoofing
c) DHCP spoofing
d) Ip spoofing
e) MAC address spoofing
Answer: d

04. Which option mitigates VLAN Hopping and Double-tagging VLAN Hopping Attacks?
a) Making sure that the native VLAN with the trunk ports differs from the native VLAN of the user ports
b) Making sure that the native VLAN of the trunk ports is equivalent to the native VLAN in the user ports
c) Setting the back port to “off.”
d) Enabling auto trunking negotiations.
Answer: a

05. What sort of attack is prevented when you configure Secure Shell (SSH)?
a) DoS session spoofing
b) Man-in-the-middle attack
c) Dictionary attack
d) Buffer overflow
Answer: b

06. Which in the following is never portion of an IKE Phase 2 process?
a) Main mode
b) Specifying a hash (HMAC)
c) Running DH (PFS)
d) Negotiating the transform set to make use of
Answer: a

07. Exactly what are three key top features of URL filtering?
(Choose three)
a) Predefined URL categories
b) Malware protection
c) Custom URL categories
d) Dynamic content analysis
Answer: a, c, d

08. Which type of VPN technologies are apt to be found in a site-to-site VPN?
a) SSL
b) TLS
c) HTTPS
d) IPsec
Answer: d

09. Which two statements are the case with the present threatscape?
(Choose two)
a) We have market is the sole industry that is exempt from attack.
b) The threat landscape is actually evolving.
c) Due to recent improvements in security technology, password attacks not play an important role in the threatscape.
d) It's so complex that it must be impossible to catalog in its entirety.
Answer: b, d

10. Which three statements are true about firewalls?
(Choose three)
a) If the system within a security zone is compromised, a firewall can help to offer the attack within that zone.
b) A firewall can prevent undesired use of a network security zone.
c) Modern firewalls give you a complete network security solution.
d) Firewalls typically will protect you between and within network security zones.
e) A firewall can introduce a performance bottleneck.
Answer: a, b, e

For more info about Cisco IINS check the best webpage.