Cisco

210-260 Exam

Cisco Implementing Cisco Network Security Exam

Version: 39.0

Question: 1

Which two services define cloud networks? (Choose two.)

A. Infrastructure as a Service
B. Platform as a Service
C. Security as a Service
D. Compute as a Service
E. Tenancy as a Service

Answer: A, B

Explanation:
The NIST's definition of cloud computing defines the service models as follows:[2] + Software as a Service (SaaS). The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.
+ Platform as a Service (PaaS). The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.
+ Infrastructure as a Service (IaaS). The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls).
Source: https://en.wikipedia.org/wiki/Cloud_computing#Service_models

Question: 2

In which two situations should you use out-of-band management? (Choose two.)

A. when a network device fails to forward packets
B. when you require ROMMON access
C. when management applications need concurrent access to the device

D. when you require administrator access from multiple locations
E. when the control plane fails to respond

Answer: A,B

Explanation:
OOB management is used for devices at the headquarters and is accomplished by connecting dedicated management ports or spare Ethernet ports on devices directly to the dedicated OOB management network hosting the management and monitoring applications and services. The OOB management network can be either implemented as a collection of dedicated hardware or based on VLAN isolation.
Source:
http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Security/SAFE_RG/SAFE_rg/chap9.html

Question: 3

In which three ways does the TACACS protocol differ from RADIUS? (Choose three.)

A. TACACS uses TCP to communicate with the NAS.
B. TACACS can encrypt the entire packet that is sent to the NAS.
C. TACACS supports per-command authorization.
D. TACACS authenticates and authorizes simultaneously, causing fewer packets to be transmitted.
E. TACACS uses UDP to communicate with the NAS.
F. TACACS encrypts only the password field in an authentication packet.

Answer: A, B, C

Question: 4

According to Cisco best practices, which three protocols should the default ACL allow on an access port to enable wired BYOD devices to supply valid credentials and connect to the network? (Choose three.)

A. BOOTP
B. TFTP
C. DNS
D. MAB
E. HTTP
F. 802.1x

Answer: A, B, C

Explanation:
ACLs are the primary method through which policy enforcement is done at access layer switches for wired devices within the campus.

ACL-DEFAULT--This ACL is configured on the access layer switch and used as a default ACL on the port. Its purpose is to prevent un-authorized access.
An example of a default ACL on a campus access layer switch is shown below:
Extended IP access list ACL-DEFAULT
10 permit udp any eq bootpc any eq bootps log (2604 matches) 20 permit udp any host 10.230.1.45 eq domain
30 permit icmp any any
40 permit udp any any eq tftp
50 deny ip any any log (40 matches)
As seen from the output above, ACL-DEFAULT allows DHCP, DNS, ICMP, and TFTP traffic and denies everything else.
Source:
http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Borderless_Networks/Unified_Access/
BYOD_Design_Guide/BYOD_Wired
MAB is an access control technique that Cisco provides and it is called MAC Authentication Bypass.

Question: 5

Which two next-generation encryption algorithms does Cisco recommend? (Choose two.)

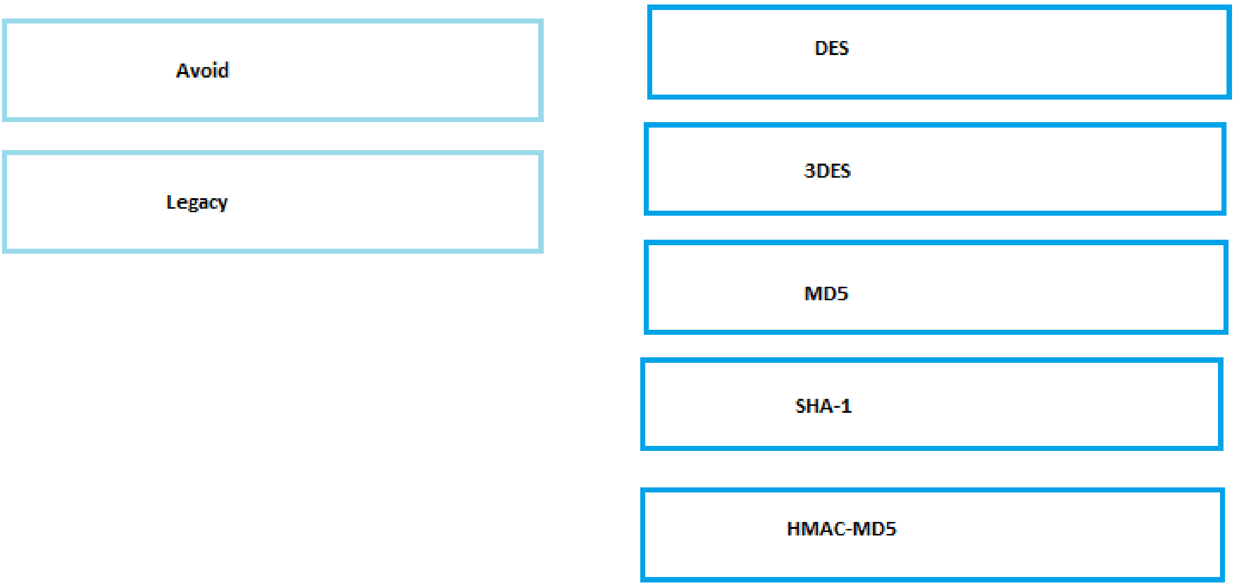
A. AES
B. 3DES
C. DES
D. MD5
E. DH-1024
F. SHA-384

Answer: A, F

Explanation:
The Suite B next-generation encryption (NGE) includes algorithms for authenticated encryption, digital signatures, key establishment, and cryptographic hashing, as listed here:
+ Elliptic Curve Cryptography (ECC) replaces RSA signatures with the ECDSA algorithm + AES in the Galois/Counter Mode (GCM) of operation
+ ECC Digital Signature Algorithm
+ SHA-256, SHA-384, and SHA-512
Source: Cisco Official Certification Guide, Next-Generation Encryption Protocols, p.97

Question: 6

DRAG DROP
Drag the recommendations on the left to the Cryptographic Algorithms on the right. Options will be used more than once.



Avoid

Legacy

DES

3DES

MD5

SHA-1

HMAC-MD5

Answer:

DES = Avoid
3DES = Legacy
MD5 = Avoid
SHA-1 = Legacy
HMAC-MD5 = Legacy

Explanation:
https://www.cisco.com/c/en/us/about/security-center/next-generation-cryptography

Question: 7

What are two default Cisco IOS privilege levels? (Choose two.)

A. 0
B. 1
C. 5
D. 7
E. 10
F. 15

Answer: B, F

Explanation:
By default, the Cisco IOS software command-line interface (CLI) has two levels of access to commands: user EXEC mode (level 1) and privileged EXEC mode (level 15).
Source:
http://www.cisco.com/c/en/us/td/docs/ios/12_2/security/configuration/guide/fsecur_c/scfpass.htm

l

Question: 8

Which two authentication types does OSPF support? (Choose two.)

A. plaintext
B. MD5
C. HMAC
D. AES 256
E. SHA-1
F. DES

Answer: A, B

Explanation:
These are the three different types of authentication supported by OSPF + Null Authentication--This is also called Type 0 and it means no authentication information is included in the packet header. It is the default.
+ Plain Text Authentication--This is also called Type 1 and it uses simple clear-text passwords.
+ MD5 Authentication--This is also called Type 2 and it uses MD5 cryptographic passwords.
Source: http://www.cisco.com/c/en/us/support/docs/ip/open-shortest-path-first-ospf/13697-25

Question: 9

Which two features are commonly used by CoPP and CPPr to protect the control plane?

A. QoS
B. traffic classification
C. access lists
D. policy maps
E. class maps
F. Cisco Express Forwarding

Answer: A, B

Explanation:
For example, you can specify that management traffic, such as SSH/HTTPS/SSL and so on, can be ratelimited (policed) down to a specific level or dropped completely.
Another way to think of this is as applying quality of service (QoS) to the valid management traffic and policing to the bogus management traffic.
Source: Cisco Official Certification Guide, Table 10-3 Three Ways to Secure the Control Plane, p.269

Question: 10

Which two statements about stateless firewalls are true? (Choose two.)

A. They compare the 5-tuple of each incoming packet against configurable rules.
B. They cannot track connections.
C. They are designed to work most efficiently with stateless protocols such as HTTP or HTTPS.
D. Cisco IOS cannot implement them because the platform is stateful by nature.
E. The Cisco ASA is implicitly stateless because it blocks all traffic by default.

Answer: A, B

Explanation:
In stateless inspection, the firewall inspects a packet to determine the 5-tuple--source and destination IP addresses and ports, and protocol--information contained in the packet. This static information is then compared against configurable rules to determine whether to allow or drop the packet.
In stateless inspection the firewall examines each packet individually, it is unaware of the packets that have passed through before it, and has no way of knowing if any given packet is part of an existing connection, is trying to establish a new connection, or is a rogue packet.
Source: http://www.cisco.com/c/en/us/td/docs/wireless/asr_5000/19-0/XMART/PSF/19-PSF-Admin/19-PSF- Admin_chapter_01