HIGHER QUALITY
BETTER SERVICE

CERTTREE

QUESTION & ANSWER

Provide One Year
Free Update!

https://www.certtree.com

Exam : **210-260**

Title : Implementing Cisco Network Security

Version : DEMO

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: AB
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

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.htm l

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

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.html MAB is an access control technique that Cisco provides and it is called MAC Authentication Bypass.

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