Cisco

210-260 Exam

Cisco Implementing Cisco Network Security Exam

Questions & Answers
Demo

Version: 34.0

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.html
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

Which three ESP fields can be encrypted during transmission? (Choose three.)

A. Security Parameter Index
B. Sequence Number
C. MAC Address
D. Padding
E. Pad Length

F. Next Header

Answer: D, E, F

Explanation:
The packet begins with two 4-byte fields (Security Parameters Index (SPI) and Sequence Number). Following these fields is the Payload Data, which has substructure that depends on the choice of encryption algorithm and mode, and on the use of TFC padding, which is examined in more detail later. Following the Payload Data are Padding and Pad Length fields, and the Next Header field. The optional Integrity Check Value (ICV) field completes the packet.
Source: https://tools.ietf.org/html/rfc4303#page-14

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.html

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.html

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.html

Question: 11

Which three statements about host-based IPS are true? (Choose three.)

A. It can view encrypted files.
B. It can have more restrictive policies than network-based IPS.
C. It can generate alerts based on behavior at the desktop level.
D. It can be deployed at the perimeter.
E. It uses signature-based policies.
F. It works with deployed firewalls.

Answer: A, B, C

Explanation:
If the network traffic stream is encrypted, HIPS has access to the traffic in unencrypted form.
HIPS can combine the best features of antivirus, behavioral analysis, signature filters, network firewalls, and application firewalls in one package.
Host-based IPS operates by detecting attacks that occur on a host on which it is installed. HIPS works by intercepting operating system and application calls, securing the operating system and application configurations, validating incoming service requests, and analyzing local log files for after-the-fact suspicious activity.
Source: http://www.ciscopress.com/articles/article.asp?p=1336425&seqNum=3

Question: 12

What three actions are limitations when running IPS in promiscuous mode? (Choose three.)

A. deny attacker
B. deny packet
C. modify packet
D. request block connection
E. request block host
F. reset TCP connection

Answer: A, B, C

Explanation:
In promiscuous mode, packets do not flow through the sensor. The disadvantage of operating in promiscuous mode, however, is the sensor cannot stop malicious traffic from reaching its intended target for certain types of attacks, such as atomic attacks (single-packet attacks). The response actions implemented by promiscuous sensor devices are post-event responses and often require assistance from other networking devices, for example, routers and firewalls, to respond to an attack.
Source: http://www.cisco.com/c/en/us/td/docs/security/ips/7-0/configuration/guide/cli/cliguide7/cli_interfaces.html

Question: 13

When an IPS detects an attack, which action can the IPS take to prevent the attack from spreading?

A. Deny the connection inline.
B. Perform a Layer 6 reset.
C. Deploy an antimalware system.
D. Enable bypass mode.

Answer: A

Explanation:
Deny connection inline: This action terminates the packet that triggered the action and future packets that are part of the same TCP connection. The attacker could open up a new TCP session (using different port numbers), which could still be permitted through the inline IPS.
Available only if the sensor is configured as an IPS.
Source: Cisco Official Certification Guide, Table 17-4 Possible Sensor Responses to Detected Attacks, p.465

Question: 14

What is an advantage of implementing a Trusted Platform Module for disk encryption?

A. It provides hardware authentication.
B. It allows the hard disk to be transferred to another device without requiring re-encryption.dis
C. It supports a more complex encryption algorithm than other disk-encryption technologies.
D. It can protect against single points of failure.

Answer: A

Explanation:
Trusted Platform Module (TPM) is an international standard for a secure cryptoprocessor, which is a dedicated microcontroller designed to secure hardware by integrating cryptographic keys into devices.
Software can use a Trusted Platform Module to authenticate hardware devices. Since each TPM chip has a unique and secret RSA key burned in as it is produced, it is capable of performing platform authentication.
Source: https://en.wikipedia.org/wiki/Trusted_Platform_Module#Disk_encryption

Question: 15

What is the purpose of the Integrity component of the CIA triad?

A. to ensure that only authorized parties can modify data
B. to determine whether data is relevant
C. to create a process for accessing data

D. to ensure that only authorized parties can view data

Answer: A

Explanation:
Integrity for data means that changes made to data are done only by authorized individuals/systems. Corruption of data is a failure to maintain data integrity.
Source: Cisco Official Certification Guide, Confidentiality, Integrity, and Availability, p.6

Question: 16

In a security context, which action can you take to address compliance?

A. Implement rules to prevent a vulnerability.
B. Correct or counteract a vulnerability.
C. Reduce the severity of a vulnerability.
D. Follow directions from the security appliance manufacturer to remediate a vulnerability.

Answer: A

Explanation:
In general, compliance means conforming to a rule, such as a specification, policy, standard or law.
Source: https://en.wikipedia.org/wiki/Regulatory_compliance

Question: 17

Which type of secure connectivity does an extranet provide?

A. other company networks to your company network
B. remote branch offices to your company network
C. your company network to the Internet
D. new networks to your company network

Answer: A

Explanation:
What is an Extranet? In the simplest terms possible, an extranet is a type of network that crosses organizational boundaries, giving outsiders access to information and resources stored inside the organization's internal network (Loshin, p. 14).
Source: https://www.sans.org/reading-room/whitepapers/firewalls/securing-extranet-connections-816

Question: 18

Which tool can an attacker use to attempt a DDoS attack?

A. botnet
B. Trojan horse
C. virus
D. adware

Answer: A

Explanation:
Denial-of-service (DoS) attack and distributed denial-of-service (DDoS) attack. An example is using a botnet to attack a target system.
Source: Cisco Official Certification Guide, Table 1-6 Additional Attack Methods, p.16

Question: 19

What type of security support is provided by the Open Web Application Security Project?

A. Education about common Web site vulnerabilities.
B. A Web site security framework.
C. A security discussion forum for Web site developers.
D. Scoring of common vulnerabilities and exposures.

Answer: A

Explanation:
The Open Web Application Security Project (OWASP) is a worldwide not-for-profit charitable organization focused on improving the security of software. Our mission is to make software security visible, so that individuals and organizations are able to make informed decisions . OWASP is in a unique position to provide impartial, practical information about AppSec to individuals, corporations, universities, government agencies and other organizations worldwide.
Source: https://www.owasp.org/index.php/Main_Page

Question: 20

What type of attack was the Stuxnet virus?

A. cyber warfare
B. hacktivism
C. botnet
D. social engineering

Answer: A

Explanation:
Stuxnet is a computer worm that targets industrial control systems that are used to monitor and control large scale industrial facilities like power plants, dams, waste processing systems and similar operations. It allows the attackers to take control of these systems without the operators knowing. This is the first attack we've seen that allows hackers to manipulate real-world equipment, which

makes it very dangerous.
Source: https://us.norton.com/stuxnet

Question: 21

What type of algorithm uses the same key to encrypt and decrypt data?

A. a symmetric algorithm
B. an asymmetric algorithm
C. a Public Key Infrastructure algorithm
D. an IP security algorithm

Answer: A

Explanation:
A symmetric encryption algorithm, also known as a symmetrical cipher, uses the same key to encrypt the data and decrypt the data.
Source: Cisco Official Certification Guide, p.93

Question: 22

Refer to the exhibit.

```
R1#show snmp
Chassis: FTX123456789
0 SNMP packets input
    6 Bad SNMP version errors
    3 Unknown community name
    9 Illegal operation for community name supplied
    4 Encoding errors
    2 Number of requested variables
    0 Number of altered variables
    98 Get-request PDUs
    12 Get-next PDUs
    2 Set-request PDUs
    0 Input queue packet drops (Maximum queue size 1000)
0 SNMP packets output
    0 Too big errors (Maximum packet size 1500)
    0 No such name errors
    0 Bad values errors
    0 General errors
    31 Response PDUs
    1 Trap PDUs
```

How many times was a read-only string used to attempt a write operation?

A. 9
B. 6
C. 4
D. 3
E. 2

Answer: A

Explanation:
To check the status of Simple Network Management Protocol (SNMP) communications, use the show snmp command in user EXEC or privileged EXEC mode.
Illegal operation for community name supplied: Number of packets requesting an operation not allowed for that community
Source: http://www.cisco.com/c/en/us/td/docs/ios/netmgmt/command

Question: 23

Refer to the exhibit.

```
R1> show clock detail
.22:22:35.123 UTC Tue Feb 26 2013
Time source is NTP
```

Which statement about the device time is true?

A. The time is authoritative, but the NTP process has lost contact with its servers.
B. The time is authoritative because the clock is in sync.
C. The clock is out of sync.
D. NTP is configured incorrectly.
E. The time is not authoritative.

Answer: A

Explanation:
Remember: The [.] at the beginning of the time tells us the NTP process has last contact with its servers. We know the time is authoritative because there would be a [*] at the beginning if not.

Question: 24

How does the Cisco ASA use Active Directory to authorize VPN users?

A. It queries the Active Directory server for a specific attribute for the specified user.
B. It sends the username and password to retrieve an ACCEPT or REJECT message from the Active Directory server.

C. It downloads and stores the Active Directory database to query for future authorization requests.
D. It redirects requests to the Active Directory server defined for the VPN group.

Answer: A

Explanation:
When ASA needs to authenticate a user to the configured LDAP server, it first tries to login using the login DN provided. After successful login to the LDAP server, ASA sends a search query for the username provided by the VPN user. This search query is created based on the naming attribute provided in the configuration. LDAP replies to the query with the complete DN of the user. At this stage ASA sends a second login attempt to the LDAP server. In this attempt, ASA tries to login to the LDAP server using the VPN user's full DN and password provided by the user. A successful login to the LDAP server will indicate that the credentials provided by the VPN user are correct and the tunnel negotiation will move to the Phase 2.
Source: http://www.networkworld.com/article/2228531/cisco-subnet/using-your-active-directory-for-vpn- authentication-on-asa.html

Question: 25

Which statement about Cisco ACS authentication and authorization is true?

A. ACS servers can be clustered to provide scalability.
B. ACS can query multiple Active Directory domains.
C. ACS uses TACACS to proxy other authentication servers.
D. ACS can use only one authorization profile to allow or deny requests.

Answer: A

Explanation:
ACS can join one AD domain. If your Active Directory structure has multi-domain forest or is divided into multiple forests, ensure that trust relationships exist between the domain to which ACS is connected and the other domains that have user and machine information to which you need access. So B is not correct.
Source: http://www.cisco.com/c/en/us/td/docs/net_mgmt/cisco_secure_access_control_system/5-8/ACS- ADIntegration/guide/Active_Directory_Integration_in_ACS_5-8.pdf + You can define multiple authorization profiles as a network access policy result. In this way, you maintain a smaller number of authorization profiles, because you can use the authorization profiles in combination as rule results, rather than maintaining all the combinations themselves in individual profiles. So D. is not correct + ACS 5.1 can function both as a RADIUS and RADIUS proxy server. When it acts as a proxy server, ACS receives authentication and accounting requests from the NAS and forwards the requests to the external RADIUS server. So C. is nor correct.
Source: http://www.cisco.com/c/en/us/td/docs/net_mgmt/cisco_secure_access_control_system/5-1/user/guide/ acsuserguide/policy_mod.html

Question: 26

Refer to the exhibit.

```
authentication event fail action next-method
authentication event no-response action authorize vlan 101
authentication order mab dotlx webauth
authentication priority dotlx mab
authentication port-control auto
dotlx pae authenticator
```

If a supplicant supplies incorrect credentials for all authentication methods configured on the switch, how will the switch respond?

A. The supplicant will fail to advance beyond the webauth method.
B. The switch will cycle through the configured authentication methods indefinitely.
C. The authentication attempt will time out and the switch will place the port into the unauthorized state.
D. The authentication attempt will time out and the switch will place the port into VLAN 101.

Answer: A

Explanation:
Flexible authentication (FlexAuth) is a set of features that allows IT administrators to configure the sequence and priority of IEEE 802.1X, MAC authentication bypass (MAB), and switch-based web authentication (local WebAuth).
Case 2: Order MAB Dot1x and Priority Dot1x MAB
If you change the order so that MAB comes before IEEE 802.1X authentication and change the default priority so that IEEE 802.1X authentication precedes MAB, then every device in the network will still be subject to MAB, but devices that pass MAB can subsequently go through IEEE 802.1X authentication.
Special consideration must be paid to what happens if a device fails IEEE 802.1X authentication after successful MAB. First, the device will have temporary network access between the time MAB succeeds and IEEE 802.1X authentication fails. What happens next depends on the configured event-fail behavior.
If next-method is configured and a third authentication method (such as WebAuth) is not enabled, then the switch will return to the first method (MAB) after the held period. MAB will succeed, and the device will again have temporary access until and unless the supplicant tries to authenticate again.
If next-method failure handling and local WebAuth are both configured after IEEE 802.1X authentication fails, local WebAuth ignores EAPoL-Start commands from the supplicant.
MAB -->MAB Pass--> Port Authorized by MAB --> EAPoL-Start Received --> IEEE 802.1x
MAB -->MAB Fail--> IEEE 802.1x
(config-if)#authentication order mab dot1x
(config-if)#authentication priority dot1x mab
Source: http://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/identity-based-networking-service/ application_note_c27-573287.html

Question: 27

Which EAP method uses Protected Access Credentials?

A. EAP-FAST
B. EAP-TLS
C. EAP-PEAP
D. EAP-GTC

Answer: A

Explanation:
Flexible Authentication via Secure Tunneling (EAP-FAST) is a protocol proposal by Cisco Systems as a replacement for LEAP. The protocol was designed to address the weaknesses of LEAP while preserving the "lightweight" implementation. Use of server certificates is optional in EAP-FAST. EAP-FAST uses a Protected Access Credential (PAC) to establish a TLS tunnel in which client credentials are verified.
Source: https://en.wikipedia.org/wiki/Extensible_Authentication_Protocol

Question: 28

What is one requirement for locking a wired or wireless device from ISE?

A. The ISE agent must be installed on the device.
B. The device must be connected to the network when the lock command is executed.
C. The user must approve the locking action.
D. The organization must implement an acceptable use policy allowing device locking.

Answer: A

Explanation:
Agents are applications that reside on client machines logging into the Cisco ISE network. Agents can be persistent (like the AnyConnect, Cisco NAC Agent for Windows and Mac OS X) and remain on the client machine after installation, even when the client is not logged into the network. Agents can also be temporal (like the Cisco NAC Web Agent), removing themselves from the client machine after the login session has terminated.
Source: http://www.cisco.com/c/en/us/td/docs/security/ise/2-0/admin_guide/b_ise_admin_guide_20/ b_ise_admin_guide_20_chapter_010101.html

Question: 29

What VPN feature allows traffic to exit the security appliance through the same interface it entered?

A. hairpinning
B. NAT
C. NAT traversal
D. split tunneling

Answer: A

Explanation:
In network computing, hairpinning (or NAT loopback) describes a communication between two hosts behind the same NAT device using their mapped endpoint. Because not all NAT devices support this communication configuration, applications must be aware of it.
Hairpinning is where a machine on the LAN is able to access another machine on the LAN via the external IP address of the LAN/router (with port forwarding set up on the router to direct requests to the appropriate machine on the LAN).
Source: https://en.wikipedia.org/wiki/Hairpinning

Question: 30

What VPN feature allows Internet traffic and local LAN/WAN traffic to use the same network connection?

A. split tunneling
B. hairpinning
C. tunnel mode
D. transparent mode

Answer: A

Explanation:
Split tunneling is a computer networking concept which allows a mobile user to access dissimilar security domains like a public network (e.g., the Internet) and a local LAN or WAN at the same time, using the same or different network connections. This connection state is usually facilitated through the simultaneous use of, a Local Area Network (LAN) Network Interface Card (NIC), radio NIC, Wireless Local Area Network (WLAN) NIC, and VPN client software application without the benefit of access control.
Source: https://en.wikipedia.org/wiki/Split_tunneling