Free Cisco 300-540 SPCNI Practice Questions

Shared by Wilson on 13-08-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

An engineer must add VNF implementation definitions and VNF service definitions to an OpenStack deployment data model to deploy virtual routers and firewalls to an enterprise network. After the virtual machine resources are prepared, which action must be taken next?

Options:

A- Specify the operational characteristics.
B- Create the initial configuration for day zero.
C- Configure key performance indicator monitoring.
D- Define the NFV network.

Answer:

D

Explanation:

In an NFV environment following Cisco NFV Infrastructure and ETSI MANO architecture, the onboarding workflow for VNF deployment follows this high-level order:

Define VNF descriptors (VNFD and NSD)

-- Includes implementation details and service definitions.

Prepare virtual machine resources

-- Flavor, image, CPU/memory/storage, and placement.

Define the NFV network

-- This step builds the underlay/overlay connectivity needed for the VNF.

-- It includes virtual network creation, interfaces, VLs (Virtual Links), connection points, and mapping into OpenStack (Neutron networks, subnets, ports).

-- No VNF can be deployed until the NFV service networks (management, control, data, HA) are defined.

Apply Day-0 configuration

-- Bootstrapping/initial config.

Apply Day-1 operational characteristics

-- Routing, services, policies.

Configure operational monitoring (KPIs)

-- Performance and fault measurements.

Since the question states ''after the VM resources are prepared'', the next mandatory stage is defining the virtual network connectivity on which the VNFs will operate.

Question 2

Question Type: MultipleChoice

An engineer recently deployed a Secure Endpoint VPC in AirGap mode. Which command must be run in the Secure Endpoint Private Cloud portal to update the package to the latest version?

Options:

A- force update -y
B- rpm -qa
C- jamf-sync all
D- genisoimage

Answer:

A

Explanation:

Comprehensive and Detailed Explanation

In Cisco Secure Endpoint Private Cloud AirGap mode, Internet access is disabled. Updates must be uploaded manually and then triggered inside the Secure Endpoint console.

The command force update -y initiates the update of the manually uploaded Secure Endpoint package.

Other commands are not used for Secure Endpoint updates:

rpm -qa Lists Linux packages only

jamf-sync all Used for Apple JAMF integrations

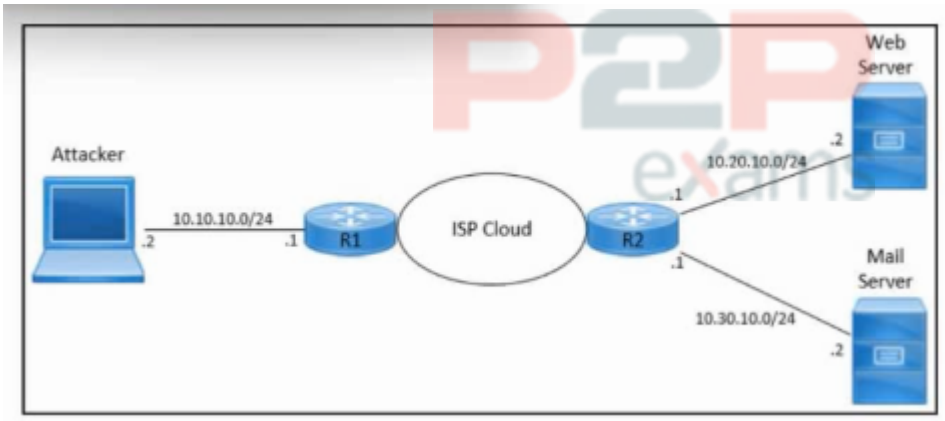
genisoimage Used to create ISO files, irrelevant to Secure Endpoint

Therefore, A is correct.

Question 3

Question Type: MultipleChoice

Refer to the exhibit.



Refer to the exhibit. An engineer must stop DDoS attacks on web and mail servers by using an ACL. Which two commands must be run on router R17? (Choose two.)

A. access-list 101 deny ip 10.10.10.2 255.255.255.255 10.20.10.2 255.255.255.255 B. access-list 101 deny ip 10.0.0.0 0.255.255.255 10.10.0.2 0.0.0.0 C. access-list 101 deny ip 10.10.10.2 255.255.255.255 10.30.10.2 255.255.255.255 D. access-list 101 deny ip 10.10.10.2 0.0.0.0 10.20.10.2 0.0.0.0 E. access-list 101 deny ip 10.10.10.2 0.0.0.0 10.30.10.2 0.0.0.0

Options:

Answer:

Explanation:

The attacker's IP is:

10.10.10.2

The servers under attack are:

Web Server: 10.20.10.2

Mail Server: 10.30.10.2

We must deny traffic from attacker servers.

Correct ACL format uses host wildcards (0.0.0.0):

deny ip 10.10.10.2 0.0.0.0 10.20.10.2 0.0.0.0

deny ip 10.10.10.2 0.0.0.0 10.30.10.2 0.0.0.0

These match D and E.

Question 4

Question Type: MultipleChoice

What is a benefit of using machine learning in Cisco AFM?

Options:

A- It enables AFM to predict potential network faults ahead of time.
B- It enables AFM to function without an Internet connection.
C- It enables AFM to perform hardware upgrades on network devices.
D- It enables AFM to consume fewer resources.

Answer:

A

Explanation:

Comprehensive and Detailed Explanation From Cisco SP Cloud & AFM Knowledge

Cisco AFM (Active Fault Manager), part of Cisco Crosswork, uses machine learning algorithms to:

Analyze large volumes of telemetry

Detect anomalies

Identify abnormal behavior patterns

Predict potential service-impacting faults before they occur

This predictive analytics capability is one of AFM's core advantages, enabling proactive fault avoidance rather than reactive troubleshooting.

The other options do not represent AFM functionality:

AFM does not require offline operation (B).

It does not upgrade hardware (C).

ML does not reduce resource usage (D); it increases analytical capability.

Thus, A is correct.

Question 5

Question Type: MultipleChoice

What is used to protect against an API logic flaw?

Options:

A- SSH encryption at rest
B- Data encryption at rest
C- Remediation of vulnerabilities
D- Data encryption in transit

Answer:

C

Explanation:

Comprehensive and Detailed Explanation

An API logic flaw is a weakness in the API's business logic --- not in encryption or transport security. It occurs when:

API functions are misused

Business rules are bypassed

Security validation is missing

Workflow logic is incorrect

These issues cannot be solved through encryption (at rest or in transit). They require:

Vulnerability remediation

Fixing API code logic

Updating API validation, flow control, and authentication logic

Thus the correct answer is C. Remediation of vulnerabilities.

Question 6

Question Type: MultipleChoice

What is a benefit of a carrier-neutral data center?

Options:

A- Reduction in foot traffic
B- Path diversity on multiple carriers
C- Lower electrical costs
D- Avoidance of a price lock-in

Answer:

B

Explanation:

Carrier-neutral facilities allow customers to connect to multiple telecom carriers, providing:

Physical path diversity

Redundancy

Competitive options

High availability for interconnects

Thus, path diversity on multiple carriers is the primary benefit.

Question 7

Question Type: MultipleChoice

What is a valid connection method between carrier-neutral facilities within the same metro area?

Options:

A- OSPF backbone area adjacency
B- private wireless connection
C- DWDM ring
D- CAT6e connection

Answer:

C

Explanation:

Comprehensive and Detailed Explanation Based on Designing and Implementing Cisco Service Provider Cloud Network Infrastructure Knowledge

When connecting carrier-neutral facilities (CNFs) or data centers within the same metropolitan area, service providers typically use high-bandwidth, low-latency optical transport methods. The most appropriate and commonly deployed interconnection technology is:

DWDM (Dense Wavelength Division Multiplexing) ring, which provides:

High capacity (10G, 40G, 100G, 400G)

Low latency

Redundancy through ring or mesh topologies

Multi-wavelength multiplexing for cost efficiency

Carrier-grade reliability for metro interconnect services

This aligns with cloud interconnect and metro transport design used in service provider environments.

Evaluation of the Options

A . OSPF backbone area adjacency

This is a routing protocol adjacency, not a physical connection method. It requires a transport link underneath but does not represent the physical interconnect itself.

B . Private wireless connection

Not suitable for CNF or metro DC interconnect because it lacks the bandwidth, reliability, and deterministic performance required for large-scale carrier-grade interconnects.

C . DWDM ring

This is the correct method. DWDM-based metro fiber rings are the standard for connecting carrier-neutral facilities in the same metro region.

D . CAT6e connection

This is limited to short-distance copper Ethernet (tens of meters). It is not used for metro-scale interconnects or between CNFs.

Question 8

Question Type: MultipleChoice

What is used to protect a web server against a DDoS attack?

Options:

A- Web Application Firewall
B- Device Authorization Control
C- Network Access Control
D- Wi-Fi Protected Access

Answer:

A

Explanation:

Comprehensive and Detailed Explanation

A Web Application Firewall (WAF) protects HTTP/HTTPS applications against:

DDoS attacks (layer 7)

Bot traffic

Request floods

SQL injection, XSS, OWASP Top 10 threats

Other options:

Device Authorization Control device authentication, not DDoS

NAC endpoint authorization, not DDoS

WPA Wi-Fi protection, irrelevant to web servers

Thus, the correct protection mechanism for web servers is A. Web Application Firewall.