PassQueen
a.k.a dumpsqueen.com

Designing Cisco Enterprise Networks for Field Engineers (ENDESIGN)

Cisco 500-490

Version Demo

Total Demo Questions: 7

Total Premium Questions: 70

Buy Premium PDF

https://passqueen.com

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, Network Design Methodology	10
Topic 2, Enterprise Campus Design	18
Topic 3, Enterprise WAN Design	17
Topic 4, Network Security Services	25
Total	70

QUESTION NO: 1

Which Cisco SD-WAN component is responsible for providing centralized management, configuration, and monitoring for the SD-WAN overlay?

A. vSmart controller

B. vBond orchestrator

C. vManage

D. WAN Edge router

ANSWER: C

Explanation:

Cisco vManage is responsible for centralized management, configuration, monitoring, and lifecycle operations in a Cisco SD-WAN deployment. Administrators use vManage to create device and feature templates, deploy policies, monitor application and tunnel performance, and troubleshoot the fabric from a common management interface. The vSmart controller distributes control-plane policy, while the vBond orchestrator assists with device onboarding and controller discovery. See the Cisco SD-WAN Controllers documentation.

QUESTION NO: 2

Which two statements are true regarding Cisco ISE? (Choose two.)

A. In distributed deployments, failover from primary to secondary Policy Administration Nodes happens automatically.

B. ISE can detected endpoints whose addresses have been translated via NAT.

C. In two-node standalone ISE deployments, failover must be done manually.

D. ISE supports IPv6 downloadable ACLs.

E. ISE supports up to 100 Policy Services Nodes.

F. The number of logs that ISE can retain is determined by your disk space.

ANSWER: D F

Explanation:

Cisco ISE supports IPv6 downloadable ACLs. Downloadable ACLs are defined in Cisco ISE authorization profiles and delivered to supported network access devices through RADIUS authorization. An IPv6 dACL can contain IPv6-specific access-control entries, allowing the authorization result to enforce access policy for IPv6 traffic as well as for IPv4 traffic where the device platform and software support the feature. This enables identity-based segmentation and restricted-access policies in dual-stack and IPv6 network designs.

The number of logs that ISE can retain is determined by your disk space. Cisco ISE stores operational, monitoring, and reporting data locally, and available storage directly affects how much historical information can remain on a node. Retention is also governed by configurable data-purging settings, which define how long particular categories of monitoring and reporting data are preserved. Administrators should therefore size ISE storage according to expected authentication volume, endpoint activity, reporting requirements, and required retention periods; forwarding selected logs to an external syslog or SIEM platform can provide longer-term retention. Cisco documents authorization profiles and downloadable ACL behavior in its Cisco ISE Administrator Guide, and describes monitoring, logging, and retention considerations in the Monitoring and Troubleshooting documentation.

QUESTION NO: 3

Which two primary categories are displayed on the overall health page of the assurance component in the Cisco DNA Center? (Choose two.)

A. Client

B. Server

C. Access-Distribution

D. Core

E. Wired

F. Network

ANSWER: A F

Explanation:

The correct primary categories are **Client** and **Network**. Cisco DNA Center Assurance, now commonly branded Cisco Catalyst Center Assurance, presents an overall health view that separates the user-experience perspective from the infrastructure perspective. The Client category summarizes client health and helps operations teams evaluate the connectivity experience of endpoints, including the health of wired and wireless clients. This high-level client-oriented view is intended to quickly identify whether users are being affected by connectivity or experience issues.

The Network category provides the corresponding infrastructure-level health perspective. It summarizes the health of the network environment and gives engineers a starting point for investigating conditions that may affect service delivery. Using these two top-level categories enables an operator to distinguish between endpoint/client experience and the underlying network state before drilling into more detailed assurance dashboards, issue investigations, or device-specific telemetry.

Cisco documentation describes Assurance as providing visibility into client and network health, using collected telemetry and analytics to identify and troubleshoot problems. See the Cisco Catalyst Center Assurance documentation and the Cisco Catalyst Center developer documentation.

QUESTION NO: 4

Whichtwostatements regarding CiscoSD-WANvEdge routers canmitigate DoS attacks against the infrastructure? (Choose two.)

A. The vEdge routers run on hardened Linux operating systems.

B. Only authorized controllers are allowed to communicate back to the vEdg e router after the vEdge router establishes connection with the controllers.

C. In case of direct Internet access, the only traffic allowed back is the traffic matching the state table entries on the vEdge router.

D. Open Certificate Authority and automated enrollment feature.

E. By default, all incoming traffic is denied at the transport (WAN) side interfaces.

ANSWER: B C

Explanation:

Only authorized controllers are allowed to communicate back to the vEdg e router after the vEdge router establishes connection with the controllers is correct because Cisco SD-WAN uses authenticated, mutually established control-plane sessions. A vEdge router initiates its secure connections to the SD-WAN controllers, and communications received in that context must come from authenticated controller infrastructure. This limits exposure to unsolicited control-plane traffic and reduces the opportunity for an attacker to impersonate a controller or consume router resources with unauthorized control connections.

In case of direct Internet access, the only traffic allowed back is the traffic matching the state table entries on the vEdge router is also correct. Direct Internet access uses stateful traffic handling: return packets are permitted only when they correspond to an existing, valid flow recorded in the router's state table. This prevents arbitrary unsolicited inbound traffic from being accepted merely because the router has Internet connectivity, helping protect the branch infrastructure from connection attempts and traffic floods directed at internal endpoints. Cisco describes SD-WAN security controls and authenticated control connections in its SD-WAN Security overview and documents stateful firewall behavior in the Cisco SD-WAN Security Configuration Guide.

QUESTION NO: 5

Which option will help build your customers platform during the discovery phase?

A. POV report

B. detailed design

C. high-level design

D. PO

E. business case

ANSWER: E

Explanation:

business case is correct because the discovery phase establishes the business rationale for an intended platform or technology initiative before the solution is designed in detail. It documents the customer's business drivers, desired outcomes, current-state challenges, anticipated benefits, major costs, risks, and the measures that will be used to evaluate success. This creates a shared basis for deciding whether to proceed and for aligning stakeholders on the value the platform is expected to deliver.

For a Cisco partner or account team, a well-developed business case turns discovery findings into an actionable investment proposal. It helps connect technical capabilities to business priorities such as improving user experience, reducing operational complexity, strengthening resilience, or enabling growth. The resulting outcome can guide subsequent architecture and design activities by ensuring that the platform is tied to agreed customer objectives rather than technology choices alone. Cisco describes its lifecycle and advisory approach as helping customers align technology strategy and architecture with business goals; see Cisco Architecture Advisory Services and Cisco Customer Experience Services.

QUESTION NO: 6

Which Cisco ISE persona is responsible for processing RADIUS authentication and authorization requests from network access devices?

A. Policy Administration Node

B. Policy Service Node

C. Monitoring Node

D. pxGrid Controller

ANSWER: B

Explanation:

The **Policy Service Node** is responsible for processing RADIUS authentication, authorization, accounting, profiling, posture, and guest-related requests from network access devices. In a distributed Cisco ISE deployment, Policy Service Nodes are placed to provide scalable and resilient access services close to users, endpoints, and network devices. The Policy Administration Node is used to configure and administer policy, while the Monitoring Node collects logs and reporting data. See the Cisco ISE Administrator Guide.

QUESTION NO: 7

Which Cisco product supports SD-Access and specifically built to address new challenges faced by enterprises?

A. ASR 1000-HX

B. ISR 4221

C. CSRv virtual router

D. Catalyst 6807-XL w/ Sup6T and C6800 10G line cards

E. Catalyst 9500

F. Nexus 7700 w/ Sup2E and M3 line cards

ANSWER: E

Explanation:

Catalyst 9500 is correct because it is part of Cisco's Catalyst 9000 switching family, a platform designed for the evolving requirements of enterprise networks, including stronger security, automation, cloud integration, mobility, and scale. Within a Cisco Software-Defined Access deployment, Catalyst 9500 switches can provide the fabric's control-plane and border functions. These roles support the scalable deployment of the SD-Access fabric, connect the fabric to external networks and services, and enable policy-based segmentation across the enterprise. Cisco identifies Catalyst 9500 Series switches as high-performance enterprise core and aggregation switches and documents their support for Cisco SD-Access deployment roles. The Catalyst 9000 family was built to address modern enterprise challenges such as operational complexity, IoT adoption, changing user and device mobility needs, and advanced security threats. Therefore, Catalyst 9500 directly matches both parts of the question: SD-Access support and a design focused on contemporary enterprise-network demands. See Cisco's Catalyst 9500 Series overview and the Cisco SD-Access Design Guide for platform capabilities and fabric-role guidance.