PassQueen
a.k.a dumpsqueen.com

Cisco Enterprise Networks SDA, SDWAN and ISE Exam for System Engineers

Cisco 500-470

Version Demo

Total Demo Questions: 8

Total Premium Questions: 86

Buy Premium PDF

https://passqueen.com

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, Cisco DNA Center	13
Topic 2, Cisco SD-Access	15
Topic 3, Cisco SD-WAN	26
Topic 4, Cisco ISE	32
Total	86

QUESTION NO: 1

What is the default interval for BFD packets?

A. 5 Seconds

B. 10 Seconds

C. 15 Seconds

D. 1 Seconds

ANSWER: D

Explanation:

1 Seconds is correct in the Cisco SD-WAN context: the default Bidirectional Forwarding Detection (BFD) packet interval on an SD-WAN tunnel is 1,000 milliseconds, which equals one second. Cisco SD-WAN uses BFD over the secure data-plane tunnels to continuously verify that a path is usable. Each WAN edge sends BFD control traffic at the configured hello interval, and the peer uses the received packets together with the detection multiplier to determine whether the tunnel remains alive. With the default one-second interval, the platform has a predictable baseline for tunnel liveliness monitoring while avoiding unnecessarily aggressive control traffic on every transport connection. This value can be tuned per tunnel interface or transport color when a deployment requires faster failure detection, subject to the available bandwidth and device-resource capacity. The interval must be understood as the transmission cadence of BFD packets; overall failure-detection time also depends on the BFD multiplier negotiated for the session. Cisco documents the default BFD hello interval as 1,000 ms in its SD-WAN configuration guidance. See Cisco's BFD configuration documentation and the Cisco SD-WAN design guide.

QUESTION NO: 2

Which two platforms can host a vEdge Cloud router ? (Choose Two) Verified

A. AWS

B. Dreamhost

C. Digitalcloud

D. Google

E. Microsoft Azure

ANSWER: A E

Explanation:

AWS and Microsoft Azure are the supported public-cloud platforms for hosting a vEdge Cloud router in the vEdge/Viptela SD-WAN deployment model covered by this question. A vEdge Cloud instance provides the SD-WAN edge function as a virtual appliance in the cloud, allowing cloud workloads and virtual private cloud networks to participate in the SD-WAN fabric. The router establishes secure control-plane and data-plane connectivity to the SD-WAN overlay and applies centrally managed policy in the same general manner as a physical vEdge device.

Cisco's vEdge Cloud deployment guidance specifically documents Amazon Web Services and Microsoft Azure workflows, including the cloud-specific virtual-machine image, interface design, routing, and bootstrap requirements. In AWS, the vEdge Cloud image is deployed as an EC2 instance; in Azure, it is deployed as an Azure virtual machine. These documented deployment targets are therefore the two appropriate choices. Cisco's SD-WAN cloud-on-ramp architecture uses these supported virtual edge deployments to connect cloud environments consistently with branch and data-center sites. See Cisco's vEdge Cloud Deployment Guide and the Cisco SD-WAN overview for platform and architecture context.

QUESTION NO: 3

Which three statements best describe Cisco ISE configuration capabilities? (Choose three.)

A. Cisco Active Advisor provides additional guidance for ISE deployments.

B. ISE Deployment Assistant (IDA) is a built in application designed to accelerate the deployment of Cisco Identity Service Engine (ISE)

C. ISE requires an understanding of the command line for set-up and configuration.

D. Cisco ISE includes wireless setup wizard and visibility wizard.

E. ISE wizards and per-canned configurations ease ISE roll-out significantly.

ANSWER: B D E

Explanation:

ISE Deployment Assistant (IDA) is a built-in guided workflow intended to speed up Cisco ISE implementation. It leads administrators through deployment-related tasks and helps apply recommended practices for common access-control scenarios, reducing the amount of manual initial configuration required. Cisco ISE also provides setup and configuration wizards, including the Wireless Setup Wizard and Visibility Wizard. These guided tools streamline deployment by assisting with wireless-access configuration and with enabling endpoint visibility capabilities, such as profiling and related contextual information used by policy decisions.

ISE wizards and pre-canned configurations also make an ISE rollout more efficient because they provide guided configuration flows and reusable, predefined settings for common network-access use cases. Administrators can use these capabilities to establish foundational policy components, network-device settings, authentication and authorization behavior, and endpoint-access workflows more consistently than configuring every element individually. Together, the deployment assistant, specialized wizards, and reusable configurations support faster and more standardized ISE deployments while still allowing policies to be tailored to organizational requirements. Cisco documents the available ISE configuration wizards in its ISE Wizards documentation and describes wireless onboarding configuration in the Wireless Setup Wizard guide.

QUESTION NO: 4

Which three items are required for an 802.1X authentication exchange? (Choose three)

A. Supplicant

B. Authenticator

C. Authentication server

D. DHCP server

E. Network Time Protocol server

ANSWER: A B C

Explanation:

An IEEE 802.1X deployment includes a **supplicant**, an **authenticator**, and an **authentication server**. The endpoint acts as the supplicant, the switch or wireless device controls access as the authenticator, and Cisco ISE commonly acts as the authentication server.

The supplicant and authenticator exchange EAP messages over EAPOL on the access link. The authenticator communicates with the authentication server, typically by using RADIUS. A DHCP server may provide addressing after access is authorized, but it is not one of the three required 802.1X roles. See the Cisco IEEE 802.1X Overview.

QUESTION NO: 5

Which three statements are true regarding Cisco SDWAN license tiers? (Choose three.)

A. With Pro license, control and data policies are supported

B. With Plus license, split-tunnel is supported

C. With Pro license, unlimited segmentations are supported

D. With Plus license, Hub and spoke, partial mesh are supported

E. With Enterprise license, vAnalytics is included

F. With Enterprise license, TCP optimization is not supported

ANSWER: A B E

Explanation:

Cisco SD-WAN licensing tiers package features at progressively broader operational and assurance levels. **With Pro license, control and data policies are supported** because policy is a core SD-WAN capability used to influence route advertisement and traffic forwarding behavior centrally from Cisco SD-WAN Manager. Control policies govern control-plane information, while data policies control how traffic is handled in the forwarding plane.

With Plus license, split-tunnel is supported because this capability enables selected traffic, such as trusted SaaS or internet-bound traffic, to use local internet egress while traffic requiring inspection or private-network access follows the SD-WAN fabric path. This supports efficient cloud and internet access designs.

With Enterprise license, vAnalytics is included because the Enterprise tier adds advanced analytics and assurance capabilities. vAnalytics uses WAN telemetry and application-performance data to provide visibility into application experience, identify trends, and help operations teams make informed capacity and policy decisions. Cisco's SD-WAN licensing documentation describes subscription-based feature entitlements and the association of analytics capabilities with higher-tier licenses. See the Cisco SD-WAN Licensing Overview and the Cisco SD-WAN solution data sheet.

QUESTION NO: 6

Which Cisco ISE feature enables a network device to apply a per-session access control list received through RADIUS?

A. Downloadable ACL

B. VLAN assignment

C. Posture assessment

D. Endpoint profiling

ANSWER: A

Explanation:

Downloadable ACL is correct. Cisco ISE can return a downloadable ACL, commonly called a dACL, in the RADIUS authorization response. The network access device retrieves and applies the ACL for the authenticated session, allowing ISE to enforce identity-based access without requiring a separate static ACL for every user or endpoint group.

A VLAN assignment changes Layer 2 network placement, while a Security Group Tag supports TrustSec group-based policy. Posture assessment evaluates endpoint compliance. Cisco documents dACL authorization results in the Cisco ISE Authorization documentation.

QUESTION NO: 7

Which options are Network Access Device types?

A. Switches, Wireless Controllers, and Routers

B. Switches, Routers, and VPN Gateways

C. Switches, Wireless Controllers, and VPN Gateways

D. Wireless Controllers, Routers, and VPN Gateways

ANSWER: C

Explanation:

Switches, Wireless Controllers, and VPN Gateways are Network Access Device types because each can act as the network enforcement point that requests authentication and authorization decisions from Cisco Identity Services Engine. In an ISE deployment, a switch commonly provides wired access control, a wireless LAN controller provides centralized wireless client access control, and a VPN gateway controls remote-access sessions. These devices are configured as network devices in ISE and typically communicate with ISE through RADIUS for services such as authentication, authorization, and accounting. ISE uses the configured device definition, including its IP address and shared secret, to recognize and trust RADIUS requests from that enforcement point. This relationship is fundamental to applying identity-based access policies consistently across wired, wireless, and remote-access connections. Cisco's ISE documentation describes network devices as the devices that enforce access policy and are added to ISE so they can use RADIUS services; the Cisco Validated Design guidance also covers these wired, wireless, and VPN enforcement integrations. See the Cisco ISE Administrator Guide and the Cisco Secure Access architecture resources.

QUESTION NO: 8

Whatis a challenge of having an SD-Access Centralized design where a single fabric encompasses the main site and all branch sites across the WAN?

A. End to End Routing is not supported

B. DNA Center does not support it.

C. SSIDs would be the same across all sites

D. Since the traffic is encapsulated, SD-WAN features can't be used to optimize/route traffic.

ANSWER: D

Explanation:

Since the traffic is encapsulated, SD-WAN features can't be used to optimize/route traffic. In a centralized SD-Access design, an end host's traffic is carried across the WAN inside an SD-Access VXLAN tunnel. The original packet headers, including the inner source and destination IP addresses and transport-layer details used for application classification, are not directly visible to the SD-WAN forwarding and policy functions. SD-WAN therefore makes decisions using the outer encapsulation rather than the original application flow. This limits the ability to apply application-aware routing, differentiated quality-of-service treatment, and security policy based on the original user, endpoint, or application information while the traffic remains encapsulated. In practical terms, the WAN can treat this traffic as an overlay flow rather than independently recognizing and steering each application contained within it. This is a fundamental design consideration when extending one SD-Access fabric domain from a central site to branches over a WAN: the centralized fabric model preserves fabric connectivity, but it reduces the SD-WAN layer's visibility into the inner traffic needed for granular optimization. Cisco's SD-Access deployment guidance describes centralized fabric designs and their WAN extension considerations, while Cisco's SD-WAN documentation explains application-aware routing based on traffic classification and path measurements. See Cisco SD-Access Design Guide and Cisco SD-WAN Application-Aware Routing.