PassQueen
a.k.a dumpsqueen.com

SMB Specialization for Account Managers

Cisco 700-505

Version Demo

Total Demo Questions: 7

Total Premium Questions: 72

Buy Premium PDF

https://passqueen.com

support@passqueen.com

QUESTION NO: 1

Which three business outcomes can be used to position a Cisco secure networking solution to an SMB customer? (Choose three.)

A. Reduce the risk of business disruption

B. Improve visibility into users, devices, and network activity

C. Support secure access for remote and mobile users

D. Guarantee that no security incident can occur

E. Eliminate the need for security policies

F. Remove all customer responsibility for user training

ANSWER: A B C

Explanation:

Reduce the risk of business disruption is correct because security controls help protect applications, users, and network resources from threats that can interrupt operations. **Improve visibility into users, devices, and network activity** is also correct because visibility helps IT teams identify what is connected, understand traffic behavior, and investigate potential security issues.

Support secure access for remote and mobile users is correct because modern secure-networking solutions can extend policy and protection beyond a single office. These outcomes help an account manager connect security investments to continuity, productivity, and risk management rather than discussing features alone. See Cisco's Security portfolio overview.

QUESTION NO: 2

Your customer states that employees are using personal devices to access SaaS applications and internal resources.

Which customer concern should be explored first when positioning a secure access solution?

A. How to apply consistent access policies to users and devices

B. How to eliminate all employee-owned devices

C. How to prevent employees from using cloud applications

D. How to replace all wireless access points immediately

ANSWER: A

Explanation:

How to apply consistent access policies to users and devices is correct because personal devices and cloud applications expand the number of access paths that must be secured. The customer needs to determine who is requesting access, the security posture of the device, and which applications or resources that user should be allowed to reach.

Discussing policy consistency helps connect the technology conversation to business risk, user productivity, and operational simplicity. Cisco secure-access solutions use identity, device, and contextual information to support policy-based access decisions. See Cisco's Secure Access Service Edge overview.

QUESTION NO: 3

Which option is a competitive advantage of Cisco security solutions?

A. Cisco Security Intelligence

B. Operations

C. Stateful firewall capability

D. Lowest priced offering

E. SpeedNet services

ANSWER: A

Explanation:

Cisco Security Intelligence is a competitive advantage because Cisco security products are informed by broad, continuously updated threat intelligence. Cisco draws telemetry and research from its security ecosystem, including Cisco Talos, to identify malicious infrastructure, malware, phishing activity, vulnerabilities, and emerging attacker techniques. That intelligence can be operationalized across security controls, helping customers detect, block, investigate, and respond to threats with more context and speed. This is especially valuable for small and midsize organizations, which may not have dedicated threat-research teams but still need protections that evolve as the threat landscape changes. Cisco Talos describes itself as one of the largest commercial threat-intelligence teams and publishes research that supports Cisco's security capabilities. The advantage is therefore not merely a single appliance feature; it is the intelligence-driven security value available across Cisco's portfolio and services. See Cisco Talos Intelligence Group and Cisco's overview of its Talos threat intelligence.

QUESTION NO: 4

Which statement about TrustSec is true?

A. It monitors all the devices on the network, and turns them off when they are not needed.

B. It provides a policy-based, scalable platform that offers integrated posture, profiling, and guest services to make context-aware access control decisions.

C. It provides secure rich-media and collaboration services to optimize real-time voice and video applications.

D. It provides defense against denial of service attacks.

ANSWER: B

Explanation:

It provides a policy-based, scalable platform that offers integrated posture, profiling, and guest services to make context-aware access control decisions. Cisco TrustSec is an identity- and context-based access-control architecture that centralizes policy definition and distributes enforcement throughout the network. It uses contextual information, such as user or device identity, security posture, and endpoint characteristics, to classify connections and apply the appropriate access policy. A core TrustSec capability is the use of Security Group Tags and Security Group Access Control Lists, which allow access decisions to be based on logical group membership rather than on IP-address or VLAN topology. Cisco Identity Services Engine commonly supplies the integrated functions named in the statement: it can profile endpoints, assess posture, manage guest access, authenticate users and devices, and communicate the resulting authorization context to TrustSec-enabled infrastructure. This combination gives organizations scalable, consistent policy enforcement as users and devices connect across wired, wireless, and remote-access environments. Cisco describes TrustSec as a solution for defining and enforcing role- and context-aware segmentation policy across the network. See Cisco's TrustSec configuration documentation and its Identity Services Engine overview.

QUESTION NO: 5

Which option is the back-end security ecosystem that detects threat activity, researches and analyzes those threats: and provides real-time updates along with best practices to allow organizations to be informed and protected?

A. Threat Operation Center

B. Secure Infrastructure Optimization

C. Monitor Analysis Response System

D. Security Intelligence Operations

ANSWER: D

Explanation:

Security Intelligence Operations is correct. Cisco used the Security Intelligence Operations (SIO) name for its global, cloud-based security-intelligence infrastructure. Its purpose is to collect and correlate telemetry from a broad range of sources, identify emerging malicious activity, and turn research and analysis into actionable intelligence. This intelligence can be delivered in near real time to Cisco security products, helping customers recognize threats and apply current protections and recommended practices without relying solely on locally observed events.

The description's emphasis on a back-end ecosystem is important: Security Intelligence Operations is not merely an individual monitoring tool or a one-time optimization engagement. It represents the intelligence and research capability behind security controls, including continuously updated information about malicious domains, IP addresses, malware, spam, and other indicators of compromise. Cisco has since consolidated and evolved much of this threat-research function under Cisco Talos, but SIO is the terminology that matches the product and architecture description used in this question. Cisco describes Talos as one of the largest commercial threat-intelligence teams, providing the research and intelligence that informs Cisco security protections. See Cisco Talos Threat Intelligence and Cisco Talos Intelligence Blog.

QUESTION NO: 6

Which two options are advantages of Cisco Data Center solutions over the competition? (Choose two.)

A. end-to-end optimization

B. seamless installation

C. scalability without complexity

D. embedded self service

ANSWER: C D

Explanation:

Cisco Data Center solutions are designed to provide **scalability without complexity** by using a unified architecture and policy-based management model. In particular, Cisco Unified Computing System platforms use service profiles and centralized management to apply consistent server, network, and connectivity policies as infrastructure grows. This helps organizations add compute capacity and adapt workloads while maintaining operational consistency rather than introducing separate management processes for each component. Cisco documents the UCS portfolio's unified approach at Cisco Unified Computing System.

Embedded self service is also an advantage because Cisco's management and automation capabilities enable IT teams to expose approved, policy-controlled infrastructure resources for consumption by internal users or application teams. Self-service provisioning reduces manual fulfillment effort, improves delivery speed, and helps preserve governance through centrally defined templates and policies. Cisco Intersight extends this operational model with cloud-based infrastructure lifecycle management, automation, and orchestration capabilities, described at Cisco Intersight. Together, these capabilities support efficient scaling and faster delivery of data-center services.

QUESTION NO: 7

Which two product portfolios help make up the FlexPod Express solution? (Choose two.)

A. Cisco UCS C-Series Server

B. Cisco ISR 2900 and 3900 Series

C. Cisco Nexus 3048 Switch

D. Cisco UCS E-Series Servers

E. Cisco ISR 1900, 2900, and 3900 Series

F. Cisco Nexus 5000

ANSWER: A C

Explanation:

FlexPod Express is a compact, prevalidated converged-infrastructure architecture intended for small and midsize deployments, branch locations, and organizations needing a simpler entry point into FlexPod. Its compute layer is built with Cisco UCS C-Series rack servers, which provide the processing, memory, and integrated networking capabilities used to host virtualized workloads and applications. The Cisco Nexus 3048 Switch provides the Ethernet switching component specified for the original FlexPod Express design, delivering the low-latency network connectivity between the compute and storage components. Together, Cisco UCS C-Series Server and Cisco Nexus 3048 Switch represent the Cisco compute and networking portfolios in this FlexPod Express configuration; NetApp storage completes the overall validated solution. Cisco's FlexPod Express material identifies UCS C-Series rack-mount servers and Nexus 3000 Series switches, including the Nexus 3048, as core components of the architecture. See Cisco's FlexPod solution overview and the FlexPod Express overview.