PassQueen
a.k.a dumpsqueen.com

SMB Specialization for Engineers

Cisco 700-501

Version Demo

Total Demo Questions: 7

Total Premium Questions: 72

Buy Premium PDF

https://passqueen.com

support@passqueen.com

QUESTION NO: 1

Which option describes server virtualization?

A. Consolidation of multiple server workloads onto a smaller number of more powerful servers

B. The aggregation of server workloads onto a smaller number of servers by running multiple server operating systems as virtual machines on shared hardware through a hypervisor

C. Reduction of on-premises server requirements through the elimination of low utilization servers and the transition to a SaaS solution

D. Consolidation of multiple server interface cards into a single network card that supports a large number of virtual interfaces

ANSWER: B

Explanation:

“The aggregation of server workloads onto a smaller number of servers by running multiple server operating systems as virtual machines on shared hardware through a hypervisor” correctly describes server virtualization. A hypervisor is the software layer that abstracts a physical server’s compute, memory, storage, and network resources, allowing multiple independent virtual machines to operate on one physical host. Each virtual machine has its own guest operating system and application workload, while remaining logically isolated from the others. This architecture enables organizations to use physical server capacity more efficiently, deploy workloads more flexibly, and reduce the amount of hardware required for a given set of services. Server virtualization is therefore more than simply placing workloads on fewer servers: it depends on the creation and operation of virtual machines through a virtualization layer. Cisco describes virtualization as abstracting physical resources so they can be pooled, allocated, and managed dynamically, a model that supports efficient data-center infrastructure and workload mobility. For additional background, see Cisco’s Data Center Virtualization overview and VMware’s virtual machine definition.

QUESTION NO: 2

Which two options are benefits of the Cisco ASA 5500-X Series over the Cisco ASA 5500 Series? (Choose two.)

A. Firewall throughput up to 12 Gb/s is provided.

B. The Cisco Content Security does not require an additional hardware module.

C. Cisco IPS throughput up to 650 Mb/s is provided

D. The Cisco IPS does not require an additional hardware module.

ANSWER: B D

Explanation:

The Cisco ASA 5500-X platform introduced an integrated services architecture that enabled advanced security services to run on the appliance without installing the separate, dedicated hardware service modules commonly associated with earlier ASA 5500 deployments. Consequently, “The Cisco Content Security does not require an additional hardware module.” is a platform benefit: content-security functionality could be delivered through the ASA’s integrated architecture and software/service licensing rather than through an added physical module. Similarly, “The Cisco IPS does not require an additional hardware module.” is correct because the 5500-X family supported integrated IPS capabilities, allowing intrusion-prevention services to be deployed without a separate IPS hardware card. This approach reduces appliance complexity, avoids consuming a physical expansion slot, and simplifies adoption of layered security services at the firewall. Cisco’s ASA 5500-X documentation describes the family’s integrated firewall, VPN, and security-services architecture, while Cisco’s IPS documentation describes intrusion-prevention deployment and capabilities. See the Cisco ASA 5500-X Series data sheet and Cisco IPS overview.

QUESTION NO: 3

Which two characteristics describe a successful mobility installation? (Choose two.)

A. Cisco Telepresence EX90 JS

B. Grow-as-you-go deployment

C. Access to information by any user, from any location, from any device

D. SMARTnet on every device

ANSWER: B C

Explanation:

A successful mobility installation is characterized by a scalable design and by secure, consistent access to business resources for users regardless of where they work or which approved endpoint they use. “Grow-as-you-go deployment” reflects a practical Cisco mobility architecture: an organization can begin with the wireless coverage, capacity, policy, and management features it currently needs, then expand the deployment as user counts, application demand, locations, and device density increase. This approach supports phased investment while retaining an architecture that can accommodate future requirements.

“Access to information by any user, from any location, from any device” expresses the core business outcome of enterprise mobility. Cisco mobility solutions are intended to provide reliable connectivity and application access for mobile users across the workplace, branches, home offices, and other authorized locations. In a successful implementation, identity-based access controls and centralized policy help deliver an appropriate user experience while protecting organizational resources. Cisco describes mobility as enabling people to connect securely and productively from anywhere, and its wireless portfolio emphasizes scalable, secure access for users and devices. See the Cisco wireless networking overview and Cisco wireless product portfolio.

QUESTION NO: 4

Which three design considerations are important when deploying Wi-Fi 6E access points? (Choose three.)

A. 6-GHz client-device support

B. Appropriate Power over Ethernet capacity

C. A current RF design or site survey

D. Removal of all 5-GHz wireless coverage

E. Use of only 2.4-GHz channels

F. Disabling network security policy for wireless clients

ANSWER: A B C

Explanation:

6-GHz client-device support, **appropriate Power over Ethernet capacity**, and **a current RF design or site survey** are important considerations for a Wi-Fi 6E deployment. Wi-Fi 6E extends Wi-Fi 6 capabilities into the 6-GHz band, but clients must support 6 GHz to use that spectrum. Legacy 2.4-GHz and 5-GHz clients continue to require coverage and capacity planning in their supported bands.

Many enterprise access points require PoE+ or higher power, depending on the model and enabled features. The access switching platform and power budget must therefore be validated before deployment. A current predictive design and, where necessary, an on-site survey are also important because 6-GHz propagation, channel planning, AP placement, and capacity requirements must be evaluated for the actual environment. Cisco describes Wi-Fi 6E and its 6-GHz capabilities in its Wi-Fi 6E solutions overview.

QUESTION NO: 5

Which option is a competitive advantage of Cisco security solutions?

A. Lowest priced offering

B. Stateful firewall capability

C. SpeedNet services

D. Cisco Security Intelligence Operations

ANSWER: D

Explanation:

Cisco Security Intelligence Operations is the competitive advantage identified here because Cisco security products are backed by Cisco's global threat-intelligence capability. This capability, now represented by Cisco Talos Intelligence Group, continuously collects and analyzes large volumes of telemetry, malware samples, vulnerabilities, and threat activity. The resulting intelligence is used to identify emerging attacks and distribute protections across Cisco's security portfolio. In practical terms, this gives organizations more current and coordinated detection, blocking, and incident-response capabilities than a security control operating without a large threat-research organization behind it.

Cisco describes Talos as one of the largest commercial threat-intelligence teams, providing intelligence that protects Cisco customers and powers security products. Its research includes threat detection, malware analysis, vulnerability discovery, and actionable security intelligence. This integrated intelligence is especially valuable for SMB customers because it helps deliver broad protection without requiring every customer to maintain an equivalent in-house research operation. Cisco's security approach therefore combines security controls with continuously updated intelligence and research expertise. See the Cisco Talos Intelligence Group and Cisco's security portfolio overview.

QUESTION NO: 6

Which Cisco management platform provides cloud-based infrastructure lifecycle management for Cisco UCS and Cisco HyperFlex environments?

A. Cisco Intersight

B. Cisco Meraki Systems Manager

C. Cisco Webex Control Hub

D. Cisco DNA Center

ANSWER: A

Explanation:

Cisco Intersight is correct because it provides cloud-operated infrastructure management for Cisco compute platforms, including Cisco UCS systems and Cisco HyperFlex environments. It gives administrators centralized inventory, health monitoring, configuration policy management, firmware recommendations, and lifecycle-management capabilities through a web-based service.

Intersight helps reduce the operational effort of managing distributed compute infrastructure by providing a common management model that can extend across locations. Its policy-driven approach also helps administrators apply consistent server and infrastructure configurations. Cisco describes its capabilities in the Cisco Intersight overview.

QUESTION NO: 7

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. Monitor Analysis Response System

B. Secure Infrastructure Optimization

C. Threat Operation Center

D. Security Intelligence Operations

ANSWER: D

Explanation:

Security Intelligence Operations is correct. Cisco used Security Intelligence Operations (SIO) to describe its global, back-end threat-intelligence ecosystem. Its purpose was to collect telemetry and threat data, identify malicious activity, investigate and analyze emerging threats, and turn those findings into actionable intelligence. That intelligence is distributed as timely updates, protections, alerts, and recommended practices so customers can strengthen defenses as the threat landscape changes. This operational model enables security controls to benefit from intelligence developed across Cisco's broad visibility into network, endpoint, email, web, and cloud threats, rather than relying only on locally observed events. In Cisco's current terminology, this threat-intelligence function is represented by Cisco Talos, which provides threat research and intelligence used to protect Cisco security products and customers. Cisco Talos describes itself as one of the largest commercial threat-intelligence organizations and publishes intelligence, research, and indicators that support detection and response. The description in the question therefore aligns with the legacy Security Intelligence Operations name used in the exam material. See Cisco Talos Intelligence Group and Cisco Talos threat intelligence.