PassQueen
a.k.a dumpsqueen.com

Cisco Small and Medium Business Engineer (SMBE)

Cisco 700-750

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, SMB Architecture	8
Topic 2, Cisco SMB Solutions	49
Topic 3, Cisco SMB Switching Solutions	1
Topic 4, Cisco SMB Wireless Solutions	2
Topic 5, Cisco SMB Security Solutions	26
Total	86

QUESTION NO: 1

Which three features are key benefits of Ciscoâ€™s SMART IT solutions for SMBs? (Choose three)

A. Automated decision-making

B. Reduced physical security

C. Enhanced data analytics

D. Improved operational efficiency

E. Decreased IT costs

ANSWER: A C D

Explanation:

Cisco SMART IT solutions for small and medium-sized businesses emphasize using cloud-managed networking, automation, visibility, and intelligence to help organizations accomplish more with limited IT resources. **Automated decision-making** is a key benefit because Cisco platforms can use telemetry, alerts, policy-based controls, and AI-assisted insights to identify conditions that require attention and accelerate operational responses. **Enhanced data analytics** is also central: network, application, client, and security visibility enables IT teams to understand usage and performance trends, investigate issues, and make informed planning decisions. **Improved operational efficiency** follows from centralized management and automation, which reduce repetitive administrative work and simplify deployment, monitoring, troubleshooting, and policy enforcement across locations. These benefits are particularly valuable to SMBs because they commonly need enterprise-grade outcomes without maintaining large specialized IT teams. Cisco positions its SMB portfolio around simplified, secure, and scalable technology operations, while Cisco Meraki provides cloud management, analytics, and automation capabilities that support these outcomes. See Cisco’s Small Business solutions overview and its Cisco Meraki platform overview.

QUESTION NO: 2

Which key feature does Meraki offer for managing hybrid workforces?

A. provides intent-based GUI-based WAN configuration and management

B. provides APIs to allow developers to save time by taking advantage of a platform's implementation

C. provides real-time monitoring but no access to analytics

D. networking and security functions remain separate and not integrated into a single service

ANSWER: B

Explanation:

Meraki provides APIs to allow developers to save time by taking advantage of a platform's implementation. The Meraki Dashboard API gives organizations programmatic access to many cloud-managed networking capabilities that would otherwise require repetitive manual dashboard actions. For hybrid-work environments, this helps IT teams operate consistently at scale as users, devices, branch sites, and remote-work requirements change. Developers and administrators can use automation to retrieve organization and network information, provision and configure supported resources, apply standardized settings, collect monitoring data, and integrate Meraki operations with service-management, asset-management, security, or internal workflow tools. This is especially valuable when a distributed workforce requires rapid deployment and consistent policy administration across many locations rather than one-off device-by-device changes. Cisco documents that Dashboard API operations use HTTPS and enable interaction with the Meraki Dashboard platform through RESTful requests, supporting automated operational workflows. The cloud-managed Dashboard also provides centralized visibility and management, making API-driven automation a practical capability for organizations supporting hybrid users and distributed infrastructure. See the Cisco Meraki Dashboard API documentation and Cisco's Meraki Dashboard overview.

QUESTION NO: 3

Which Cisco solution is crucial for securing SMB's remote work environments?

A. Cisco Firepower

B. Cisco Duo

C. Cisco AnyConnect

D. Cisco Nexus

ANSWER: B

Explanation:

Cisco Duo is crucial for securing an SMB remote-work environment because it provides identity-centered protection through multi-factor authentication, device visibility, and adaptive access policies. In a distributed environment, employees access SaaS applications, VPNs, and internal resources from networks and devices that may not be directly managed by the organization. Duo helps ensure that access is granted only after the user's identity is verified and the device meets the organization's security requirements. This supports a zero-trust approach: authentication and device trust are evaluated before access to protected applications is allowed, rather than relying solely on the user's network location or a password.

For SMBs, Duo is particularly practical because it is cloud-delivered, integrates with common applications and remote-access infrastructure, and can be deployed without building extensive on-premises identity-security infrastructure. Its controls address common remote-work risks such as compromised credentials, phishing-based password theft, and unmanaged endpoints. Cisco describes Duo as a solution for secure access that verifies users and assesses device trust before allowing access to applications. Cisco's SMB security guidance also positions identity and access protection as a core component of securing users working from any location. See Cisco Duo Product and Cisco Secure Remote Work for Small Business.

QUESTION NO: 4

An SMB is planning technology for a new distributed office model. The business has limited IT staff, expects to add locations over time, and must protect users working from office and home. Which three design priorities best support a practical Cisco SMB solution? (Choose three)

A. Centralized cloud management

B. Separate management tools for every site

C. Scalable connectivity

D. Consistent identity-based security

E. Treating the office network as inherently trusted

ANSWER: A C D

Explanation:

Centralized cloud management, **scalable connectivity**, and **consistent identity-based security** directly address the stated requirements. Cloud management reduces operational burden for a small IT team, scalable connectivity supports additional sites and users, and identity-based controls protect access regardless of user location.

Separate management tools for every site increase complexity, while treating the office network as inherently trusted conflicts with a Zero Trust approach for hybrid work.

QUESTION NO: 5

Which Cisco product is part of the smart experience for empowering IT?

A. Meraki Sensors

B. Meraki Cameras

C. Meraki Insight

D. Umbrella

ANSWER: C

Explanation:

Meraki Insight is part of Cisco's smart experience for empowering IT because it gives IT teams application-aware visibility into the user experience across the network. It is designed to help administrators understand how network conditions affect critical applications, particularly web applications and WAN-connected services, rather than requiring them to troubleshoot from isolated device metrics alone. Through the Meraki dashboard, teams can use Insight to monitor application performance, identify poor-performing paths, and isolate contributing conditions such as WAN latency, packet loss, DNS resolution delays, or slow web-server response. This actionable visibility supports a more proactive operational model: IT staff can investigate user-impacting issues quickly and use shared dashboard data to make informed remediation decisions. Cisco describes Meraki Insight as providing end-to-end visibility and assurance for the digital experience, aligning directly with the goal of simplifying network operations and empowering IT teams. Cisco's unified-experience announcement also places Meraki Insight within the broader portfolio of capabilities intended to make IT management smarter and more efficient. See Cisco Meraki Insight and Cisco Newsroom.

QUESTION NO: 6

An SMB is reviewing whether a proposed solution will continue to deliver value after deployment. Which three activities best support a lifecycle-focused customer engagement? (Choose three)

A. Measure outcomes against the customer's objectives

B. Support adoption of the deployed capabilities

C. Review changing business and technology requirements

D. End engagement when the purchase order is issued

E. Recommend products before understanding the current environment

ANSWER: A B C

Explanation:

Measuring outcomes against the customer's objectives, helping users adopt the deployed capabilities, and reviewing changing requirements all support lifecycle value. They allow the partner to demonstrate whether the solution is delivering the intended operational and business benefits and to identify opportunities for improvement as the customer evolves.

Ending engagement immediately after the purchase order is issued ignores adoption and outcome realization. Recommending products without understanding the current environment is product-led rather than customer-outcome-led.

QUESTION NO: 7

A partner is conducting a Business Value Demonstration for an SMB that is considering secure networking for new branch locations. Which three actions best reflect a value-focused sales engagement? (Choose three)

A. Relating the solution to the customer's branch challenges

B. Leading only with a feature inventory

C. Showing measurable operational outcomes

D. Demonstrating a relevant deployment use case

E. Promising the lowest price regardless of requirements

ANSWER: A C D

Explanation:

Relating the solution to the customer's branch challenges, **showing measurable operational outcomes**, and **demonstrating a relevant deployment use case** are value-focused actions. They connect the proposed architecture to the customer's priorities, such as reducing troubleshooting time, improving security consistency, or simplifying branch deployment.

Leading only with a feature inventory does not establish business relevance. Promising the lowest price regardless of requirements can undermine solution fit and does not demonstrate customer value.

QUESTION NO: 8

What does the smart SMB experience enable?

A. Building a smarter network

B. Building smarter security

C. Protecting the outside of an office space

D. Building smarter workspaces

ANSWER: A

Explanation:

Building a smarter network is correct because the Cisco Smart SMB Experience centers on giving small and midsize businesses an intelligent, simplified network foundation that can support day-to-day operations and business growth. Cisco positions this experience around making enterprise-grade networking more attainable for SMBs through solutions that are easier to deploy, manage, monitor, and scale. This includes cloud-managed and automated capabilities that help IT teams gain visibility into users, devices, applications, and network performance without requiring the operational complexity traditionally associated with enterprise infrastructure.

A smarter network is the enabling layer for reliable connectivity across wired, wireless, remote-access, and cloud environments. It allows an SMB to adopt modern services while retaining centralized control and consistent operational insight. Cisco's SMB portfolio emphasizes secure connectivity, streamlined management, and scalable network platforms as core elements of helping businesses operate more efficiently. In that context, the Smart SMB Experience is fundamentally about building the intelligent network environment on which broader business capabilities can run. See Cisco's Small Business Solutions overview and the Cisco SMBE exam topics for the solution and skills context.