PassQueen
a.k.a dumpsqueen.com

Security Architecture for Systems Engineer (SASE)

Cisco 500-651

Version Demo

Total Demo Questions: 14

Total Premium Questions: 147

Buy Premium PDF

https://passqueen.com

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, Cisco Security Architecture	15
Topic 2, Cisco Security Solutions	132
Total	147

QUESTION NO: 1

Which two options are attack vectors protected by Identity and Access Control? (Choose two.)

A. Backups

B. Mobile

C. Endpoints

D. Cloud apps

E. Voicemail

ANSWER: B C

Explanation:

Identity and Access Control protects **Mobile** and **Endpoints** by verifying user and device identity before permitting access to enterprise resources. Mobile devices are frequently outside the traditional network perimeter, so strong authentication, multifactor authentication, device trust checks, and adaptive access policies reduce the risk that lost, compromised, or unmanaged devices can be used to access corporate applications. Cisco Duo provides this type of identity-based protection by enforcing trusted access and multifactor authentication for users and devices.

Endpoints are also a central Identity and Access Control enforcement point. Access-control systems can identify endpoints, assess contextual attributes such as device type and posture, and apply authorization policy before granting network or application access. Cisco Identity Services Engine supports policy-based access control and device visibility, helping ensure that only authenticated users and appropriately authorized endpoints receive access. Together, these controls reduce exposure from credential misuse and unauthorized device connections, whether the access attempt originates from a managed workstation, an unmanaged endpoint, or a mobile device. See Cisco Duo and Cisco Identity Services Engine.

QUESTION NO: 2

Which is a key feature of Cisco Defense Orchestra?

A. Profiles devices connected to customer ’s network

B. Orchestrates security policy management from one place

C. Consolidates configuration management

D. Protects customer’s network against zero-day attacks

ANSWER: B

Explanation:

Orchestrates security policy management from one place is correct. Cisco Defense Orchestrator (CDO) is a cloud-delivered management platform designed to provide centralized visibility and consistent policy administration across supported Cisco security products, including Secure Firewall devices and cloud-delivered Firewall Management Center. Rather than requiring administrators to individually access each managed device or separate management console, CDO provides a common workspace for creating, deploying, and monitoring security policies. This centralized orchestration helps security teams apply standardized controls across distributed environments, reduce operational complexity, and maintain policy consistency as the network grows. CDO also supports workflows such as policy analysis, object management, change tracking, and deployment of policy updates to the appropriate targets. These capabilities make centralized security-policy orchestration the defining feature described in the answer. Cisco documents CDO as a platform that simplifies the management of security policies across an organization’s Cisco security infrastructure. For additional details, see the Cisco Defense Orchestrator product page and the Cisco Defense Orchestrator documentation.

QUESTION NO: 3

Which license subscription terms are available for AMP licensing?

A. 1 month 3 months 6 months

B. 1 year. 5 years. 10 years

C. 5 years 10 years 30 years

D. 1 year. 3 years. 6 years

E. 1 year, 3 years, 5 years

ANSWER: E

Explanation:

The available subscription terms for Cisco AMP licensing are **1 year, 3 years, and 5 years**. AMP, now generally marketed within the Cisco Secure Endpoint portfolio, is licensed as a time-based subscription rather than as a perpetual software entitlement. The selected term establishes how long the organization is entitled to use the security service, receive threat intelligence, obtain software and feature updates, and access the associated cloud-based management and protection capabilities. A customer can select the duration that best matches its procurement cycle, budget model, and planned security-platform lifecycle; longer terms provide a multiyear entitlement while retaining the ongoing subscription services required for effective endpoint and malware protection. Cisco ordering and licensing materials identify one-year, three-year, and five-year durations for these endpoint-security subscriptions. Cisco's current Secure Endpoint product information is available at Cisco Secure Endpoint, and Cisco's product documentation portal is available at Cisco Secure Endpoint Support Documentation.

QUESTION NO: 4

Which feature of AnyConnect provides you the ability to identify data breaches as they happen?

A. Flexible AAA Options

B. Network Visibility Module

C. Differentiated Mobile Access

D. Trusted Network Detection

ANSWER: B

Explanation:

Network Visibility Module is correct because it extends network telemetry collection to endpoints running Cisco AnyConnect, now Cisco Secure Client. The module captures endpoint flow information, including details such as source and destination addresses, ports, protocols, process information, and user context. It exports this rich flow telemetry to Cisco security-analytics platforms, where it can be correlated with network activity and analyzed for suspicious behavior.

This endpoint-aware visibility is especially valuable for detecting data breaches as they occur. Security teams can identify abnormal data transfers, unexpected communications with external destinations, unusual application behavior, and potentially compromised devices, even when traffic originates from remote users or operates outside traditional network-monitoring locations. The resulting context supports faster investigation and response by connecting a network flow to the specific endpoint process and user responsible for it.

Cisco describes the Network Visibility Module as providing deep endpoint visibility through flow telemetry for security analytics and threat detection. See Cisco's Network Visibility Module overview and the Cisco Secure Client product page.

QUESTION NO: 5

Which are two main challenges of securing web and e -mail? (Choose two.)

A. Data Loss Prevention: having the ability to remediate issues as they arise.

B. AMP: securing cloud apps.

C. Protecting against data centers.

D. Investigate: detecting issues in real time.

ANSWER: A D

Explanation:

Having the ability to remediate issues as they arise and detecting issues in real time are core operational challenges for web and email security. Modern web and email environments generate a high volume of events, alerts, malicious messages, risky URLs, and potentially harmful file activity. Security teams must identify relevant activity quickly enough to reduce exposure, then contain and remediate the affected users, messages, endpoints, or accounts before an incident spreads.

Cisco positions email security as protection that includes threat detection, investigation, response, and remediation capabilities, rather than merely blocking known malicious content. Similarly, Cisco XDR focuses on correlating telemetry across security controls so analysts can detect threats, investigate their scope, and take response actions more efficiently. These requirements make timely detection and practical remediation central challenges, particularly when organizations have limited analyst time and threats evolve rapidly. Effective security architecture therefore needs both accurate, real-time visibility and workflows or automation that support swift remediation. See Cisco Secure Email and Cisco XDR.

QUESTION NO: 6

What are three main challenges addressed by Cisco's cloud delivered securit y solutions? (Choose three.)

A. Threats are becoming too advanced for traditional hardware

B. Solutions often require frequent hardware updates

C. Employees are unable to work remotely

D. Businesses are using email too frequently

E. Frequently installing new servers, appliances, and devices adds to the maintenance workload

F. IT staff must continuously grow with a dditional specializations to address the solutions

ANSWER: B E F

Explanation:

Cisco cloud-delivered security solutions address the operational burden created by deploying, refreshing, and maintaining security infrastructure in every location. "Solutions often require frequent hardware updates" identifies the challenge of appliance lifecycle management: capacity, feature, and security requirements can drive refreshes and upgrades. With a cloud-delivered service, the provider operates and updates the underlying infrastructure, while customers consume the service through centrally managed policies.

"Frequently installing new servers, appliances, and devices adds to the maintenance workload" is also a core challenge. Physical deployment introduces staging, shipping, installation, patching, monitoring, replacement, and site-by-site consistency work. Cloud-delivered security reduces dependence on this distributed hardware footprint and enables protection to be applied through a service rather than repeated appliance rollouts.

"IT staff must continuously grow with a dditional specializations to address the solutions" reflects the skills and operational complexity that cloud delivery is intended to reduce. Centralized management and provider-operated infrastructure help smaller teams apply consistent security controls without operating every component themselves. Cisco describes Secure Access as a cloud-delivered security service that converges security functions and simplifies secure access, while Cisco Umbrella provides cloud-delivered protection managed through a centralized dashboard. See Cisco Secure Access and Cisco Umbrella.

QUESTION NO: 7

What are three benefits that Cisco Umbrella brings to DNS-Layer Security? (Choose three.)

A. Helps provide breach mitigation

B. Blocks Domains/IPs associated with malware, phising, etc

C. Delivers cloud based recursive DNS

D. Provides profiling of devices

E. Logs all internet activity

F. Provides Sandboxing of malware

ANSWER: B C E

Explanation:

Cisco Umbrella DNS-Layer Security uses a globally distributed, cloud-based recursive DNS service to apply security policy before a client establishes a connection to an Internet destination. This architecture enables it to block DNS requests for known or predicted malicious destinations, including domains and IP addresses associated with malware, phishing, command-and-control infrastructure, and other threats. Stopping the DNS resolution prevents the endpoint from reaching the harmful destination and provides protection regardless of the application port or protocol subsequently intended for use.

The service also delivers recursive DNS from Cisco's cloud, avoiding the need to deploy and maintain on-premises recursive DNS infrastructure while supporting consistent enforcement for protected users and networks. Umbrella records DNS activity and provides searchable reporting and investigation data, giving security teams visibility into Internet destination requests, policy actions, identities, and devices. This DNS telemetry supports threat investigation, monitoring, and incident response. Cisco describes these DNS-security capabilities at Cisco Umbrella DNS-Layer Security; reporting and DNS-activity investigation are documented in the Umbrella DNS Activity Search guide.

QUESTION NO: 8

Which Cisco solution falls under Advanced Threat?

A. Email Defense

B. Identity Services Engine

C. Malware Protection

D. Anti-spoofing

ANSWER: C

Explanation:

Malware Protection is the correct answer because advanced-threat capabilities are designed to identify, analyze, block, and remediate malicious files and malware throughout their lifecycle. In Cisco's security portfolio, this capability has historically been known as Advanced Malware Protection (AMP) and is now represented by Cisco Secure Endpoint. It uses multiple detection and analysis techniques, including file reputation, static and dynamic file analysis, behavioral telemetry, and retrospective security. Retrospective protection is particularly important for advanced threats: if a file initially appears safe but is later determined to be malicious, security teams can identify where it executed and take remediation action. These capabilities help organizations address sophisticated malware, ransomware, and evasive threats that may bypass a single point-in-time inspection. Cisco positions Secure Endpoint as an endpoint-security solution that prevents, detects, and responds to advanced threats while providing visibility into endpoint activity and incident context. This alignment with malware detection, threat analysis, and response is why Malware Protection belongs to the Advanced Threat solution area. See Cisco's Secure Endpoint overview and the Cisco Advanced Malware Protection information.

QUESTION NO: 9

What are two key points of the Cisco Security and Threat Landscape module? (Choose two.)

A. The Cisco Security Solutions Portfolio drives customer business outcomes by providing threat-centric defense, visibility and control, and flexible solutions

B. The threat landscape is expanding, becoming more complex, and threats are increasingly costing more to customers

C. The Cisco Security Solutions Portfolio stops all threat from entering a customers network.

D. Customers need several solutions to protect their environment.

ANSWER: A B

Explanation:

The Cisco Security and Threat Landscape module emphasizes that the security environment is continuously changing: attack surfaces are growing as organizations use cloud services, remote access, applications, endpoints, and interconnected networks. Threat actors also evolve their techniques and can create significant operational, financial, and reputational consequences for customers. Recognizing this expanding complexity and cost is essential to framing security conversations around risk reduction, faster detection, and effective response.

The module also presents the Cisco Security Solutions Portfolio as an integrated, outcome-focused approach. Cisco security capabilities are intended to provide threat-centric defense, broad visibility and control, and flexibility for differing customer architectures and deployment requirements. Threat-centric defense supports protection before, during, and after an attack, while visibility and control help security teams understand activity across their environment and apply consistent policy. Flexible solutions allow customers to adopt security controls across network, cloud, endpoint, identity, and application environments as their needs change. This aligns with Cisco's broader approach of connecting security capabilities and telemetry to improve resilience and simplify security operations. See Cisco's Security portfolio overview and its overview of extended detection and response.

QUESTION NO: 10

Which Policy and Access solution technology combines posture checks and authentication across wired, wireless, and VPN networks?

A. Cisco AnyConnect

B. Next Generation Intrusion Prevention System

C. Cisco Stealthwatch

D. ASA 2100 series

E. Cisco Identity Services Engine (ISE)

ANSWER: E

Explanation:

Cisco Identity Services Engine (ISE) is the Cisco Policy and Access solution that centrally applies identity-based access control and endpoint compliance assessment across wired, wireless, and remote-access VPN connections. ISE acts as a policy decision and RADIUS/AAA platform: it authenticates users and devices, gathers contextual information such as identity, device type, location, and security state, and then authorizes the appropriate level of network access. Its posture service evaluates whether endpoints meet an organization's compliance requirements, such as required antivirus, antimalware, operating-system updates, firewall status, or other configured conditions. Based on the result, ISE can permit access, restrict access, or direct the endpoint to remediation resources. For remote users, Cisco Secure Client (formerly AnyConnect) can serve as an endpoint component that communicates posture information, but ISE is the policy-and-access technology that correlates posture and authentication consistently across wired, wireless, and VPN access methods. Cisco documents ISE as providing secure network access through centralized policy enforcement and contextual endpoint

visibility, including posture assessment. See the Cisco ISE data sheet and Cisco's Identity Services Engine Administrator Guide.

QUESTION NO: 11

Which three values are provided by NGFW and NGIPS in the "Campus NGFW"? (Choose three.)

A. Dynamic routing port to meet all network needs.

B. Differentiated Mobile Access

C. Additional firewalls across all platforms

D. High throughput maintained while still protecting domain against threats

E. Identity Services Engine

F. Flexible AAA Options

ANSWER: A B D

Explanation:

Campus NGFW and NGIPS deployments provide security that is designed to fit into an enterprise campus without sacrificing the routing, user-access, or performance requirements of that environment. **Dynamic routing port to meet all network needs.** represents the ability to integrate firewall enforcement into routed campus designs and adapt to diverse network topologies. **Differentiated Mobile Access** reflects the ability to apply access and security treatment based on users, devices, and connection context, which is particularly relevant for mobile users in campus networks. **High throughput maintained while still protecting domain against threats** is a core NGFW/NGIPS value: inspection and threat prevention must scale to campus traffic volumes while enforcing security controls. Cisco describes Secure Firewall Threat Defense as combining application visibility and control, intrusion prevention, and advanced malware protection, while its firewall platforms are built to deliver high performance for enterprise deployments. These values together support secure, scalable campus connectivity with threat inspection integrated into the network path. See Cisco's firewall portfolio overview and NGIPS overview.

QUESTION NO: 12

How does AMP's file reputation feature help customers?

A. It automatically detects polymorphic variants of known malware

B. It increases time to detection with exact data analytics

C. It increases the protection to systems with exact fingerprinting

D. It enables secure web browsing with cognitive threat analytics

ANSWER: C

Explanation:

AMP's file reputation feature increases protection to systems with exact fingerprinting. The feature calculates a cryptographic hash, commonly a SHA-256 value, for a file and submits that fingerprint to Cisco's cloud-based threat intelligence. Cisco AMP can then associate the exact file with a reputation or disposition, such as malicious, clean, or unknown, based on global telemetry and threat research. This enables a security policy to make an informed detection or blocking decision before the exact known-bad file can execute on an endpoint. Because the fingerprint uniquely identifies the file's contents, reputation provides a fast and scalable way to recognize files that Cisco intelligence has already classified and to enforce that classification across protected systems. Cisco describes Secure Endpoint (formerly AMP for Endpoints) as using file reputation and global threat intelligence to identify and stop malware, while retaining visibility into file activity. See Cisco's Secure Endpoint product information and its Advanced Malware Protection solution overview.

QUESTION NO: 13

Which is a key feature of Cisco Defense Orchestrator?

A. Simplifies security policy management

B. Identifies sensitive data in cloud environments

C. Detects anomalous traffic on customer's network

D. Provides retrospective security

ANSWER: A

Explanation:

Simplifies security policy management is a key feature of Cisco Defense Orchestrator (CDO). CDO is a cloud-delivered management platform designed to provide centralized visibility and consistent policy administration across supported Cisco security products, including Cisco Secure Firewall devices and cloud-delivered firewall services. Rather than requiring administrators to configure policies independently on each managed device, CDO provides workflows to create, edit, validate, and deploy policy changes from a central interface. This helps security teams standardize access-control and network-security policy, reduce configuration inconsistency, and operate more efficiently across distributed environments. Cisco also positions CDO as a platform for managing security policies and device configurations at scale, with features such as policy analysis, object management, change deployment, and audit-oriented visibility. These capabilities directly support simplified security-policy management for organizations operating multiple firewalls and locations. See the Cisco Defense Orchestrator product page and the Cisco Defense Orchestrator documentation for product capabilities and management workflows.

QUESTION NO: 14

Which three options does Cisco provide customers in terms of “Visibility and Control” against today’s threats? (Choose three.)

A. Granular device visibility and management

B. Unparalleled network a nd endpoint visibility

C. 18-month device release cycle

D. Bandwith Utilization Monitoring

E. Comprehensive policy enforcement

F. Fast device policy updates

ANSWER: A B E

Explanation:

Cisco’s visibility-and-control capabilities are centered on establishing a detailed understanding of devices, users, endpoints, traffic, and activity, then consistently applying security policy based on that context. **Granular device visibility and management** is correct because Cisco security platforms identify and classify connected assets, allowing administrators to understand what is present in the environment and manage access according to device context. **Unparalleled network a nd endpoint visibility** is correct because Cisco correlates telemetry across the network and endpoint layers, improving detection, investigation, and operational awareness. **Comprehensive policy enforcement** is correct because visibility becomes actionable when policy can be applied consistently to control communications, segmentation, and access across the environment. These capabilities align with Cisco’s security approach of using broad telemetry and identity-aware controls to reduce risk while enforcing intended access outcomes. Cisco describes Secure Firewall as providing visibility and control across the network, while Cisco Identity Services Engine provides contextual visibility and policy enforcement for users and devices. See Cisco Secure Firewall and Cisco Identity Services Engine.