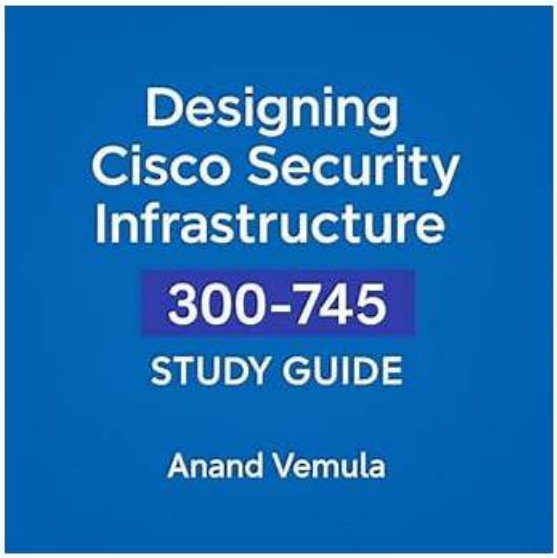
Pass Guaranteed 2026 Cisco Useful 300-745: Designing Cisco Security Infrastructure Braindump Pdf



P.S. Free 2026 Cisco 300-745 dumps are available on Google Drive shared by Pass4sures: https://drive.google.com/open?id=1CiP6xFCjD7my-pdG46jddmHSbhXMszlf

Nowadays, the development of technology is quickly. Also, our 300-745 exam guide will keep advancing. A lot of reforms have applied to the content and formats of our 300-745 learning guide according to our professional experts constantly efforts. We just hope that you will have a better experience when you study on our 300-745 Actual Exam. Act from now if you are still hesitating, our 300-745 study materials will enable you embrace a bright future.

Cisco 300-745 Exam Syllabus Topics:

Topic	Details
Topic 1	• Secure Infrastructure: Covers selecting security approaches for endpoints, identities, email, and modern environments like hybrid work, IoT, SaaS, and multi-cloud. Includes choosing VPN • tunneling solutions, securing management planes, and selecting the appropriate firewall architecture based on business needs.
Topic 2	• Applications: Focuses on selecting security solutions to protect applications and designing secure architectures for cloud-native, containerized, and serverless environments using segmentation. Also addresses security design impacts of emerging technologies like AI, ML, and quantum computing.
Topic 3	• Artificial Intelligence, Automation, and DevSecOps: Explores AI's role in securing network infrastructure, selecting tools for automated security architectures such as SOAR, IaC, and API tooling, and integrating security into DevSecOps workflows and pipelines to minimize deployment risk.
Topic 4	• Risk, Events, and Requirements: Covers SOC incident handling and response tools, modifying security designs to mitigate or respond to incidents, and applying frameworks like MITRE CAPEC, NIST SP 800-37, and SAFE. Includes matching regulatory and compliance requirements to business scenarios.

>> 300-745 Braindump Pdf <<

300-745 Valid Test Questions - Reliable 300-745 Real Test

If you want to constantly improve yourself and realize your value, if you are not satisfied with your current state of work, if you still spend a lot of time studying and waiting for 300-745 qualification examination, then you need our 300-745 material, which can help solve all of the above problems. I can guarantee that our study materials will be your best choice. Our 300-745 Study Materials have three different versions, including the PDF version, the software version and the online version, to meet the different needs, our products have many advantages, I will introduce you to the main characteristics of our 300-745 research materials.

Cisco Designing Cisco Security Infrastructure Sample Questions (Q42-Q47):

NEW QUESTION # 42
An IT company experienced the spread of malicious content between user endpoints, which impacted business critical resources. The company wants to implement a solution to control communication between individual endpoints on the network. Which approach achieves the goal?

- A. TrustSec
- B. profiling
- C. RADIUS
- D. posture

Answer: A

Explanation:
The spread of malicious content between endpoints is a classic case oflateral movement. To control and restrict communication between individual endpoints-regardless of their physical location or IP address- Cisco TrustSecis the recommended architectural approach. TrustSec moves away from traditional, IP-based Access Control Lists (ACLs), which are difficult to manage and scale, and instead usesScalable Group Tags (SGTs).
With TrustSec, every endpoint is assigned an SGT based on its role or security context (e.g., "Employee," "Contractor," or "HR"). Security policies are then defined in a centralized matrix (the egress policy matrix) that dictates which SGTs can talk to one another. For example, a policy can be set so that endpoints in the "Developer" group cannot communicate directly with endpoints in the "Sales" group, effectively preventing malware from hopping between machines. WhileRADIUS(Option A) is the protocol used for authentication, it does not perform the segmentation itself.Posture(Option C) checks the health of the device, andProfiling (Option D) identifies what the device is, but neither provides the policy-based traffic control of TrustSec. By implementing TrustSec, the company achievesmicro-segmentation, significantly reducing the internal attack surface and containing potential breaches within a single group, which is a core goal of modern secure infrastructure design.

NEW QUESTION # 43
Refer to the exhibit.
A software developer noticed that the application source code had been found on the internet. To avoid such an incident from happening again, the developer applied a DLP policy to prevent from uploading source code into generative AI tool like ChatGPT. When testing the policy, the developer noticed that it is still possible for the source code to be uploaded. Which action must the developer take to prevent this issue?

- A. Change the DLP action from Monitor to Block.
- B. Modify the data classifications.
- C. Move the ChatGPT Source Code rule to the bottom.
- D. Enable the rule.

Answer: A

Explanation:
In the provided exhibit of theCisco Data Loss Prevention (DLP) Policyinterface (likely within Cisco Umbrella or a similar cloud security gateway), the reason for the policy's failure to stop the upload is clearly visible in the "Action" column. The rule named"ChatGPT Source Code"is currently configured with the action set toMonitor.
According to theCisco SDSI v1.0objectives regarding application and data security, theMonitoraction is designed for visibility and auditing. It allows the traffic to pass through while generating a log entry for security analysts to review. This is often used during an

initial "discovery" phase to understand how data is moving without disrupting business processes. However, to fulfill the requirement ofpreventingthe unauthorized upload of sensitive data-such as application source code-the policy must be enforcement- centric. By selectingOption D, the developer changes the action from "Monitor" toBlock. In "Block" mode, the DLP engine will actively intercept the web request to ChatGPT, inspect the content for "Source Code" classifications, and drop the connection if a match is found, thereby preventing the data from leaving the corporate environment. While moving rules (Option B) can resolve conflicts if a "Block" rule is superseded by an "Allow" rule higher in the list, the primary issue here is the non-restrictive action of the specific rule itself. Modifying data classifications (Option C) is unnecessary if the engine is already correctly identifying the source code, as evidenced by the successful monitoring logs mentioned in the scenario. Changing the action to Block is the definitive step to ensure data integrity and prevent intellectual property theft.

NEW QUESTION # 44
An employee of a pharmaceutical company accidentally checked in code that contains AWS secret keys to a public GitHub repository, which exposes production resources to attackers.
Which mitigation strategy must a security engineer recommend to prevent future reoccurrence?

- A. Implement a phishing education campaign.
- B. Configure a SCM precommit hook.
- C. Add a web application firewall.
- D. Implement a more granular port security strategy.

Answer: B

Explanation:
An SCM (Source Code Management) precommit hook scans code for sensitive information such as AWS keys before it is committed. This prevents developers from accidentally pushing secrets to public repositories, protecting production resources from exposure.

NEW QUESTION # 45
A pharmaceutical company needs hub-and-spoke VPN topology. The design must be capable of building either partial or full mesh overlay networks. Which VPN solution must be implemented in the environment?

- A. DMVPN
- B. L2TP
- C. crypto maps
- D. SSL VPN

Answer: A

Explanation:
Dynamic Multipoint VPN (DMVPN) supports hub-and-spoke topologies while allowing flexibility to build partial or full mesh overlays as needed. It provides scalable and dynamic VPN tunnels without requiring static configuration, making it the best fit for the requirement.

NEW QUESTION # 46
A manufacturing company recently experienced a network-down scenario due to malware spread on the management network. The company wants to implement a solution to detect and mitigate a similar threat in the future and protect the overall network. Which solution meets the requirements?

- A. IPsec VPN
- B. endpoint detection and response
- C. encrypted threat analysis
- D. RADIUS

Answer: B

Explanation:
The spread of malware across a sensitive segment like themanagement networkhighlights a failure in host- level security and internal visibility. To detect and mitigate the spread of such threats and protect the overall network,Endpoint Detection and Response

(EDR)is the most effective choice among the options. In the Cisco security ecosystem, the endpoint is often the last line of defense and the most critical source of telemetry for malware incidents.
By deploying an EDR solution likeCisco Secure Endpoint, the manufacturing company gains the ability to identify the "patient zero" of the infection. EDR uses advanced features likeDevice TraversalandLateral Movementdetection to see how malware moves from one machine to another over the management network.
Once detected, the security team can use the EDR platform to initiate a "host isolation" command, effectively cutting off the infected device's communication with the rest of the network without physically unplugging it.
WhileEncrypted Threat Analytics (ETA)(Option C) is a powerful network-based feature for detecting malware in encrypted traffic without decryption, EDR provides the most granular control and response capabilities specifically for malwareresiding on and spreading betweenhosts. RADIUS (Option B) and IPsec VPNs (Option D) focus on access control and encryption of data in transit, respectively, but do not provide the behavioral analysis needed to stop a running malware outbreak once the network has already been accessed.

NEW QUESTION # 47
......

Once you have used our 300-745 exam training in a network environment, you no longer need an internet connection the next time you use it, and you can choose to use 300-745 exam training at your own right. Our 300-745 Exam Training do not limit the equipment, do not worry about the network, this will reduce you many learning obstacles, as long as you want to use 300-745 test guide, you can enter the learning state.

300-745 Valid Test Questions: https://www.pass4sures.top/CCNP-Security/300-745-testking-braindumps.html

P.S. Free 2026 Cisco 300-745 dumps are available on Google Drive shared by Pass4sures: https://drive.google.com/open?id=1CiP6xFCjD7my-pdG46jddmHSbhXMszlf