Providing You 100% Pass-Rate 350-701 Reliable Test Sims with 100% Passing Guarantee

P.S. Free 2026 Cisco 350-701 dumps are available on Google Drive shared by PassExamDumps: https://drive.google.com/open?id=1qAuMaiLUN5JSld4pCBZPS_fpWQawHqd4

Every day is new beginning; we will have a good mood. Hot and outstanding IT certification will be a good beginning for your IT career road. Cisco 350-701 current exam content will be a strong helper for you. If you want to realize your dream and get a certification, PassExamDumps provide the best valid Cisco 350-701 Current Exam Content materials to help you pass tests. And you will have a great progress in a short time.

Cisco 350-701 Exam Syllabus Topics:

Section	Weight	Objectives
Securing the Cloud	15%	- Cloud workload protection and compliance - Hybrid and multi-cloud security integration - Cisco Umbrella, Cloudlock, and Secure Access solutions - Cloud security architectures and service models
Network Security	20%	- Firewall and IPS deployment, configuration, and management - Network security monitoring and logging - Security segmentation and policy enforcement - VPN technologies: site-to-site, remote access, and secure connectivity
Content Security	15%	- Web security: proxy, URL filtering, DLP, and AMP integration - Content inspection and threat prevention - Email security: SEG, anti-spam, anti-malware, encryption, and DMARC
Secure Network Access, Visibility, and Enforcement	15%	- 802.1X, MAB, and TrustSec architecture - Network visibility, telemetry, and security analytics - Identity services and policy control with Cisco ISE - Access control and compliance enforcement
Endpoint Protection and Detection	10%	- Cisco Secure Endpoint deployment and management - Endpoint protection platforms (EPP) and endpoint detection and response (EDR) - Threat intelligence and incident response for endpoints
Security Concepts	25%	- Security principles, zero trust architecture, and compliance frameworks - Common threats and vulnerabilities in on-premises and cloud environments - Automation and APIs in security solutions - Cryptography and security protocols

Why PassExamDumps Is One Of The Best Platform To Prepare For Cisco 350-701 Exam?

PassExamDumps is unlike other exam materials that are available on the market, 350-701 study torrent specially proposed different versions to allow you to learn not only on paper, but also to use mobile phones to learn. You can choose the version of 350-701 training guide according to your interests and habits. And if you buy the value pack, you have all of the three versions, the price is quite preferential and you can enjoy all of the study experiences. This means you can study 350-701 Exam Engine anytime and anyplace for the convenience these three versions bring.

Cisco Implementing and Operating Cisco Security Core Technologies Sample Questions (Q137-Q142):

NEW QUESTION # 137
Which two activities can be done using Cisco DNA Center? (Choose two)

- A. Provision
- B. Design
- C. DHCP
- D. Accounting
- E. DNS

Answer: A,B

Explanation:
Explanation Cisco DNA Center has four general sections aligned to IT workflows: Design: Design your network for consistent configurations by device and by site. Physical maps and logical topologies help provide quick visual reference. The direct import feature brings in existing maps, images, and topologies directly from Cisco Prime Infrastructure and the Cisco Application Policy Infrastructure Controller Enterprise Module (APIC-EM), making upgrades easy and quick. Device configurations by site can be consolidated in a "golden image" that can be used to automatically provision new network devices. These new devices can either be pre-staged by associating the device details and mapping to a site. Or they can be claimed upon connection and mapped to the site. Policy: Translate business intent into network policies and apply those policies, such as access control, traffic routing, and quality of service, consistently over the entire wired and wireless infrastructure. Policy-based access control and network segmentation is a critical function of the Cisco Software-Defined Access (SDAccess) solution built from Cisco DNA Center and Cisco Identity Services Engine (ISE). Cisco AI Network Analytics and Cisco Group-Based Policy Analytics running in the Cisco DNA Center identify endpoints, group similar endpoints, and determine group communication behavior. Cisco DNA Center then facilitates creating policies that determine the form of communication allowed between and within members of each group. ISE then activates the underlying infrastructure and segments the network creating a virtual overlay to follow these policies consistently. Such segmenting implements zero-trust security in the workplace, reduces risk, contains threats, and helps verify regulatory compliance by giving endpoints just the right level of access they need. Provision: Once you have created policies in Cisco DNA Center, provisioning is a simple drag-and-drop task. The profiles (called scalable group tags or "SGTs") in the Cisco DNA Center inventory list are assigned a policy, and this policy will always follow the identity. The process is completely automated and zero-touch. New devices added to the network are assigned to an SGT based on identity-greatly facilitating remote office setups. Assurance: Cisco DNA Assurance, using AI/ML, enables every point on the network to become a sensor, sending continuous streaming telemetry on application performance and user connectivity in real time. The clean and simple dashboard shows detailed network health and flags issues. Then, guided remediation automates resolution to keep your network performing at its optimal with less mundane troubleshooting work. The outcome is a consistent experience and proactive optimization of your network, with less time spent on troubleshooting tasks. Reference: https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/dna-center/nb-06-dna-center-so-cte-en.html Cisco DNA Center has four general sections aligned to IT workflows:
Design: Design your network for consistent configurations by device and by site. Physical maps and logical topologies help provide quick visual reference. The direct import feature brings in existing maps, images, and topologies directly from Cisco Prime Infrastructure and the Cisco Application Policy Infrastructure Controller Enterprise Module (APIC-EM), making upgrades easy and quick. Device configurations by site can be consolidated in a "golden image" that can be used to automatically provision new network devices. These new devices can either be pre-staged by associating the device details and mapping to a site. Or they can be claimed upon connection and mapped to the site.
Policy: Translate business intent into network policies and apply those policies, such as access control, traffic routing, and quality of service, consistently over the entire wired and wireless infrastructure. Policy-based access control and network segmentation is a critical function of the Cisco Software-Defined Access (SDAccess) solution built from Cisco DNA Center and Cisco Identity

Services Engine (ISE). Cisco AI Network Analytics and Cisco Group-Based Policy Analytics running in the Cisco DNA Center identify endpoints, group similar endpoints, and determine group communication behavior. Cisco DNA Center then facilitates creating policies that determine the form of communication allowed between and within members of each group. ISE then activates the underlying infrastructure and segments the network creating a virtual overlay to follow these policies consistently. Such segmenting implements zero-trust security in the workplace, reduces risk, contains threats, and helps verify regulatory compliance by giving endpoints just the right level of access they need.
Provision: Once you have created policies in Cisco DNA Center, provisioning is a simple drag-and-drop task.
The profiles (called scalable group tags or "SGTs") in the Cisco DNA Center inventory list are assigned a policy, and this policy will always follow the identity. The process is completely automated and zero-touch. New devices added to the network are assigned to an SGT based on identity-greatly facilitating remote office setups.
Assurance: Cisco DNA Assurance, using AI/ML, enables every point on the network to become a sensor, sending continuous streaming telemetry on application performance and user connectivity in real time. The clean and simple dashboard shows detailed network health and flags issues. Then, guided remediation automates resolution to keep your network performing at its optimal with less mundane troubleshooting work.
The outcome is a consistent experience and proactive optimization of your network, with less time spent on troubleshooting tasks.
Explanation Cisco DNA Center has four general sections aligned to IT workflows: Design: Design your network for consistent configurations by device and by site. Physical maps and logical topologies help provide quick visual reference. The direct import feature brings in existing maps, images, and topologies directly from Cisco Prime Infrastructure and the Cisco Application Policy Infrastructure Controller Enterprise Module (APIC-EM), making upgrades easy and quick. Device configurations by site can be consolidated in a "golden image" that can be used to automatically provision new network devices. These new devices can either be pre-staged by associating the device details and mapping to a site. Or they can be claimed upon connection and mapped to the site.
Policy: Translate business intent into network policies and apply those policies, such as access control, traffic routing, and quality of service, consistently over the entire wired and wireless infrastructure. Policy-based access control and network segmentation is a critical function of the Cisco Software-Defined Access (SDAccess) solution built from Cisco DNA Center and Cisco Identity Services Engine (ISE). Cisco AI Network Analytics and Cisco Group-Based Policy Analytics running in the Cisco DNA Center identify endpoints, group similar endpoints, and determine group communication behavior. Cisco DNA Center then facilitates creating policies that determine the form of communication allowed between and within members of each group. ISE then activates the underlying infrastructure and segments the network creating a virtual overlay to follow these policies consistently. Such segmenting implements zero-trust security in the workplace, reduces risk, contains threats, and helps verify regulatory compliance by giving endpoints just the right level of access they need. Provision: Once you have created policies in Cisco DNA Center, provisioning is a simple drag-and-drop task. The profiles (called scalable group tags or "SGTs") in the Cisco DNA Center inventory list are assigned a policy, and this policy will always follow the identity. The process is completely automated and zero-touch. New devices added to the network are assigned to an SGT based on identity-greatly facilitating remote office setups. Assurance: Cisco DNA Assurance, using AI/ML, enables every point on the network to become a sensor, sending continuous streaming telemetry on application performance and user connectivity in real time. The clean and simple dashboard shows detailed network health and flags issues. Then, guided remediation automates resolution to keep your network performing at its optimal with less mundane troubleshooting work. The outcome is a consistent experience and proactive optimization of your network, with less time spent on troubleshooting tasks. Reference: https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/dna-center/nb-06-dna-center-so-cte-en.html

NEW QUESTION # 138
Which Cisco solution does Cisco Umbrella integrate with to determine if a URL is malicious?

- A. Cisco Dynamic
- B. Cisco AMP
- C. Cisco anyconnect
- D. Cisco Talos

Answer: D

NEW QUESTION # 139
How does DNS Tunneling exfiltrate data?

- A. An attacker sends an email to the target with hidden DNS resolvers in it to redirect them to a malicious domain.
- B. An attacker uses a non-standard DNS port to gain access to the organization's DNS servers in order to poison the resolutions.
- C. An attacker registers a domain that a client connects to based on DNS records and sends malware through that connection.

- D. An attacker opens a reverse DNS shell to get into the client's system and install malware on it.

Answer: C

Explanation:
DNS tunneling is a technique that exploits the DNS protocol to tunnel malware and other data through a client-server model. DNS tunneling can be used for data exfiltration, command and control, or IP-over-DNS tunneling. DNS tunneling works by encoding the information of other protocols or programs in DNS queries and responses. An attacker registers a domain, such as badsite.com, and sets up a malicious DNS server that can interpret the encoded data. The attacker then infects a client with malware that can send and receive DNS queries to the attacker's domain. The malware can use DNS queries to request commands from the attacker, or to send sensitive data to the attacker. The DNS queries and responses look like normal DNS traffic, but they contain hidden data that can bypass network defenses123. References := 1: What Is DNS Tunneling? - Palo Alto Networks 2: What is DNS Tunneling? - Check Point Software 3: What Is DNS Tunneling and How to Detect and Prevent Attacks

NEW QUESTION # 140
What are the two most commonly used authentication factors in multifactor authentication? (Choose two)

- A. biometric factor
- B. encryption factor
- C. time factor
- D. knowledge factor
- E. confidentiality factor

Answer: A,D

Explanation:
Multi-factor Authentication (MFA) is an authentication method that requires the user to provide two or more verification factors to gain access to a resource. MFA requires means of verification that unauthorized users won't have. Proper multi-factor authentication uses factors from at least two different categories. MFA methods: + Knowledge - usually a password - is the most commonly used tool in MFA solutions. However, despite their simplicity, passwords have become a security problem and slow down productivity. + Physical factors - also called possession factors-use tokens, such as a USB dongle or a portable device, that generate a temporary QR (quick response) code. Mobile phones are commonly used, as they have the advantage of being readily available in most situations. + Inherent - This category includes biometrics like fingerprint, face, and retina scans. As technology advances, it may also include voice ID or other behavioral inputs like keystroke metrics. Because inherent factors are reliably unique, always present, and secure, this category shows promise. + Location-based and time-based - Authentication systems can use GPS coordinates, network parameters, and metadata for the network in use, and device recognition for MFA. Adaptive authentication combines these data points with historical or contextual user data. A time factor in conjunction with a location factor could detect an attacker attempting to authenticate in Europe when the user was last authenticated in California an hour prior, for example. + Time-based one-time password (TOTP) - This is generally used in 2FA but could apply to any MFA method where a second step is introduced dynamically at login upon completing a first step. The wait for a second step-in which temporary passcodes are sent by SMS or email-is usually brief, and the process is easy to use for a wide range of users and devices. This method is currently widely used. + Social media - In this case a user grants permission for a website to use their social media username and password for login. This provide an easy login process, and one generally available to all users. + Risk-based authentication - Sometimes called adaptive multi-factor authentication, this method combines adaptive authentication and algorithms that calculate risk and observe the context of specific login requests. The goal of this method is to reduce redundant logins and provide a more user-friendly workflow. + Push-based 2FA - Push-based 2FA improves on SMS and TOTP 2FA by adding additional layers of security while improving ease of use. It confirms a user's identity with multiple factors of authentication that other methods cannot. Because push-based 2FA sends notifications through data networks like cellular or Wi-Fi, users must have data access on their mobile devices to use the 2FA functionality. Reference: https://www.cisco.com/c/en/us/products/security/what-is-multi-factor-authentication.html The two most popular authentication factors are knowledge and inherent (including biometrics like fingerprint, face, and retina scans. Biometrics is used commonly in mobile devices).
verification factors to gain access to a resource. MFA requires means of verification that unauthorized users won't have.
Proper multi-factor authentication uses factors from at least two different categories.
MFA methods:
+ Knowledge - usually a password - is the most commonly used tool in MFA solutions. However, despite their simplicity, passwords have become a security problem and slow down productivity.
+ Physical factors - also called possession factors-use tokens, such as a USB dongle or a portable device, that generate a temporary QR (quick response) code. Mobile phones are commonly used, as they have the advantage of being readily available in most situations.
+ Inherent - This category includes biometrics like fingerprint, face, and retina scans. As technology advances, it may also include

voice ID or other behavioral inputs like keystroke metrics. Because inherent factors are reliably unique, always present, and secure, this category shows promise.
+ Location-based and time-based - Authentication systems can use GPS coordinates, network parameters, and metadata for the network in use, and device recognition for MFA. Adaptive authentication combines these data points with historical or contextual user data.
A time factor in conjunction with a location factor could detect an attacker attempting to authenticate in Europe when the user was last authenticated in California an hour prior, for example.
+ Time-based one-time password (TOTP) - This is generally used in 2FA but could apply to any MFA method where a second step is introduced dynamically at login upon completing a first step. The wait for a second step-in which temporary passcodes are sent by SMS or email-is usually brief, and the process is easy to use for a wide range of users and devices. This method is currently widely used.
+ Social media - In this case a user grants permission for a website to use their social media username and password for login. This provide an easy login process, and one generally available to all users.
+ Risk-based authentication - Sometimes called adaptive multi-factor authentication, this method combines adaptive authentication and algorithms that calculate risk and observe the context of specific login requests.
The goal of this method is to reduce redundant logins and provide a more user-friendly workflow.
+ Push-based 2FA - Push-based 2FA improves on SMS and TOTP 2FA by adding additional layers of security while improving ease of use. It confirms a user's identity with multiple factors of authentication that other methods cannot. Because push-based 2FA sends notifications through data networks like cellular or Wi-Fi, users must have data access on their mobile devices to use the 2FA functionality.
Reference:
The two most popular authentication factors are knowledge and inherent (including biometrics like fingerprint, Multi-factor Authentication (MFA) is an authentication method that requires the user to provide two or more verification factors to gain access to a resource. MFA requires means of verification that unauthorized users won't have. Proper multi-factor authentication uses factors from at least two different categories. MFA methods: + Knowledge - usually a password - is the most commonly used tool in MFA solutions. However, despite their simplicity, passwords have become a security problem and slow down productivity. + Physical factors - also called possession factors-use tokens, such as a USB dongle or a portable device, that generate a temporary QR (quick response) code. Mobile phones are commonly used, as they have the advantage of being readily available in most situations. + Inherent - This category includes biometrics like fingerprint, face, and retina scans. As technology advances, it may also include voice ID or other behavioral inputs like keystroke metrics. Because inherent factors are reliably unique, always present, and secure, this category shows promise. + Location-based and time-based - Authentication systems can use GPS coordinates, network parameters, and metadata for the network in use, and device recognition for MFA. Adaptive authentication combines these data points with historical or contextual user data. A time factor in conjunction with a location factor could detect an attacker attempting to authenticate in Europe when the user was last authenticated in California an hour prior, for example. + Time-based one-time password (TOTP) - This is generally used in 2FA but could apply to any MFA method where a second step is introduced dynamically at login upon completing a first step. The wait for a second step-in which temporary passcodes are sent by SMS or email-is usually brief, and the process is easy to use for a wide range of users and devices. This method is currently widely used. + Social media - In this case a user grants permission for a website to use their social media username and password for login. This provide an easy login process, and one generally available to all users. + Risk-based authentication - Sometimes called adaptive multi-factor authentication, this method combines adaptive authentication and algorithms that calculate risk and observe the context of specific login requests. The goal of this method is to reduce redundant logins and provide a more user-friendly workflow. + Push-based 2FA - Push-based 2FA improves on SMS and TOTP 2FA by adding additional layers of security while improving ease of use. It confirms a user's identity with multiple factors of authentication that other methods cannot. Because push-based 2FA sends notifications through data networks like cellular or Wi-Fi, users must have data access on their mobile devices to use the 2FA functionality. Reference: https://www.cisco.com/c/en/us/products/security/what-is-multi-factor-authentication.html The two most popular authentication factors are knowledge and inherent (including biometrics like fingerprint, face, and retina scans. Biometrics is used commonly in mobile devices).

NEW QUESTION # 141
Which two request of REST API are valid on the Cisco ASA Platform? (Choose two.)

- A. Get
- B. Connect
- C. Option
- D. Put
- E. Push

Answer: A,D

NEW QUESTION # 142
.....

So we can say that the Implementing and Operating Cisco Security Core Technologies (350-701) practice test questions are real, valid, and updated and these will greatly help you in 350-701 exam preparation. The availability of Implementing and Operating Cisco Security Core Technologies (350-701) exam questions in three different formats, free demo download facility, affordable price, free three months updated 350-701 Exam Questions download facility, and verified and real Implementing and Operating Cisco Security Core Technologies (350-701) exam questions are the top features of PassExamDumps 350-701 exam questions.

350-701 Exam Sample Questions: https://www.passexamdumps.com/350-701-valid-exam-dumps.html

- 350-701 Latest Exam Online □ 350-701 Free Test Questions □ 350-701 Reliable Test Bootcamp □ Search for 「 350-701 」 on ➤ www.vce4dumps.com □ immediately to obtain a free download □350-701 Free Test Questions
- 350-701 Reliable Test Pattern □ 350-701 Valid Test Guide □ 350-701 Reliable Test Bootcamp □□ Easily obtain free download of □ 350-701 □ by searching on ✔ www.pdfvce.com □✔□ □350-701 Reliable Torrent
- 350-701 – 100% Free Reliable Test Sims | Useful Implementing and Operating Cisco Security Core Technologies Exam Sample Questions □ Search for [350-701] and download it for free on □ www.dumpsquestion.com □ website □350-701 Valid Dumps Files
- Excellent 350-701 Reliable Test Sims - Leader in Certification Exams Materials - Practical 350-701 Exam Sample Questions □ Copy URL ☀ www.pdfvce.com □☀□ open and search for ➥ 350-701 □ to download for free □350-701 Reliable Torrent
- First-grade Cisco 350-701 Reliable Test Sims | Try Free Demo before Purchase □ Easily obtain free download of ✔ 350-701 □✔□ by searching on { www.practicevce.com } □350-701 Latest Exam Online
- Use 350-701 Practice Exam Software For Self Evaluation □ Download " 350-701 " for free by simply entering （ www.pdfvce.com ） website □Vce 350-701 Download
- 350-701 PDF Dumps - Effortless Solution To Pass Exam □ Search on ▸ www.troytecdumps.com ◂ for 《 350-701 》 to obtain exam materials for free download □Vce 350-701 Download
- Use 350-701 Practice Exam Software For Self Evaluation □ Open website 【 www.pdfvce.com 】 and search for ▸ 350-701 ◂ for free download ☘350-701 Valid Test Guide
- New 350-701 Exam Simulator □ 350-701 Latest Exam Online ❣ Vce 350-701 Download □ Search on ✔ www.troytecdumps.com □✔□ for □ 350-701 □ to obtain exam materials for free download □350-701 Valid Dumps Files
- Valid 350-701 Reliable Test Sims – The Best Exam Sample Questions for 350-701 - High Pass-Rate 350-701 Test Questions □ Easily obtain ✔ 350-701 □✔□ for free download through ⇛ www.pdfvce.com ⇚ □Latest 350-701 Exam Simulator
- 350-701 Latest Exam Online □ 350-701 Valid Dumps Files □ Latest 350-701 Test Guide □ Open 【 www.examcollectionpass.com 】 and search for ▹ 350-701 ◃ to download exam materials for free □350-701 Reliable Torrent
- myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, www.stes.tyc.edu.tw, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, www.stes.tyc.edu.tw, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, www.stes.tyc.edu.tw, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, Disposable vapes

DOWNLOAD the newest PassExamDumps 350-701 PDF dumps from Cloud Storage for free: https://drive.google.com/open?id=1qAuMaiLUN5JSld4pCBZPS_fpWQawHqd4