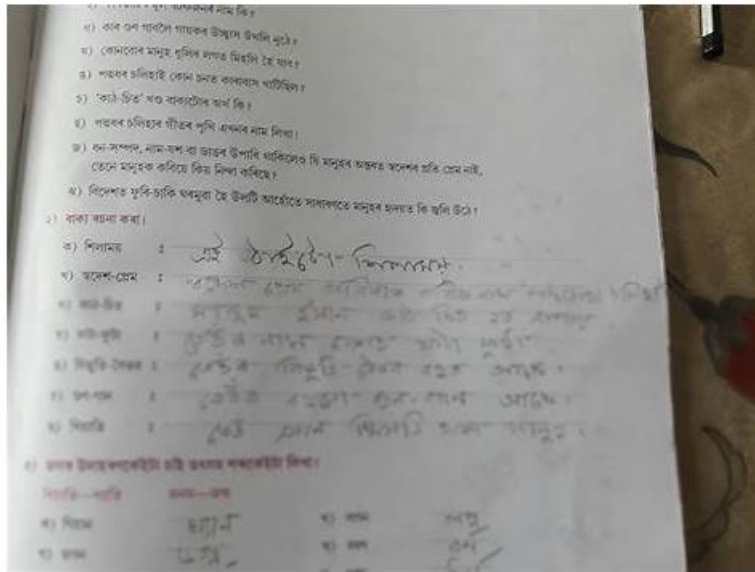# Pdf 350-701 Braindumps | Exam Sample 350-701 Questions

P.S. Free 2026 Cisco 350-701 dumps are available on Google Drive shared by TopExamCollection:
https://drive.google.com/open?id=1w0eCOY7WV04rxWOgLhfcv_7PhMVRA3bT

It is known to us that our 350-701 study materials have been keeping a high pass rate all the time. There is no doubt that it must be due to the high quality of our study materials. It is a matter of common sense that pass rate is the most important standard to testify the 350-701 Study Materials. The high pass rate of our study materials means that our products are very effective and useful for all people to pass their exam and get the related certification.

Secure Network Visibility, Access, and Enforcement – 15%

- Configuring and verifying the function of network access device, such as 802.1X, WebAuth, and MAB;
- Explaining identity management & secure network access concepts, such as profiling, posture assessment, guest services, as well as BYOD;
- Explaining the device compliance & application control benefits;
- Describing the network telemetry benefits;
- Explaining the capacity, benefits, and components of the security products & solutions, such as Cisco Stealthwatch, Cisco Umbrella Investigate, Cisco Stealthwatch Cloud, Cisco pxGrid, and others.
- Describing the exfiltration methods, including HTTPS, IRC, DNS tunneling, email, Messenger, and others;

Securing Cloud – 15%

- Determining deployment models, security capacity, and policy management to provide the security of Cloud;
- Configuring the Cloud logging & monitoring techniques;
- Explaining the DevSecOps concept (container orchestration, CI/CD pipeline, and security);
- Comparing the provider versus customer security responsibility for various Cloud service models;
- Explaining the application & workload security concepts.

>> Pdf 350-701 Braindumps <<

Exam Sample 350-701 Questions & 350-701 Exam Tips

Our 350-701 practice dumps are so popular that all our customers are giving high praise on its high-quality to help them pass the exams. Numerous of warming feedbacks from our worthy customers give us data and confidence. We have clear data collected from customers who chose our 350-701 training engine, the passing rate is 98-100 percent. So your chance of getting success will be increased greatly by our 350-701 exam questions!

Cisco Implementing and Operating Cisco Security Core Technologies Sample Questions (Q521-Q526):

NEW QUESTION # 521
Which function is performed by certificate authorities but is a limitation of registration authorities?

- A. accepts enrollment requests
- B. verifying user identity
- C. certificate re-enrollment
- D. CRL publishing

Answer: D

Explanation:
Certificate authorities (CAs) are responsible for issuing, renewing, revoking, and publishing digital certificates. They also maintain a certificate revocation list (CRL), which is a database of revoked certificates that can be checked by relying parties to verify the validity of a certificate. Registration authorities (RAs) are entities that assist CAs with the verification of user identities and enrollment requests. They do not issue certificates themselves, nor do they have access to the CRL. Therefore, CRL publishing is a function that is performed by CAs but is a limitation of RAs. References ≔ Some possible references are:
* Implementing and Operating Cisco Security Core Technologies (SCOR) v1.0, Module 4: Secure Connectivity, Lesson 4.1: VPN Fundamentals, Topic 4.1.1: Public Key Infrastructure (PKI)
* Easy guide to SSL certificate authorities, Namecheap
* How exactly are registration authorities related to certificate authorities?, Information Security Stack Exchange

NEW QUESTION # 522
Which two deployment modes does the Cisco ASA FirePower module support? (Choose two)

- A. passive monitor-only mode
- B. routed mode
- C. inline mode
- D. transparent mode
- E. active mode

Answer: C,E

Explanation:
Explanation You can configure your ASA FirePOWER module using one of the following deployment models: You can configure your ASA FirePOWER module in either an inline or a monitor-only (inline tap or passive) deployment. Reference: https://www.cisco.com/c/en/us/td/docs/security/asa/asa92/asdm72/firewall/asa-firewall-asdm/ modules-sfr.html You can configure your ASA FirePOWER module using one of the following deployment models:
You can configure your ASA FirePOWER module in either an inline or a monitor-only (inline tap or passive) deployment.
Reference:
Explanation You can configure your ASA FirePOWER module using one of the following deployment models: You can configure your ASA FirePOWER module in either an inline or a monitor-only (inline tap or passive) deployment. Reference: https://www.cisco.com/c/en/us/td/docs/security/asa/asa92/asdm72/firewall/asa-firewall-asdm/ modules-sfr.html

NEW QUESTION # 523
What is the function of the Context Directory Agent?

- A. maintains users' group memberships
- B. relays user authentication requests from Web Security Appliance to Active Directory
- C. reads the Active Directory logs to map IP addresses to usernames
- D. accepts user authentication requests on behalf of Web Security Appliance for user identification

Answer: C

Explanation:
Cisco Context Directory Agent (CDA) is a mechanism that maps IP Addresses to usernames in order to allow security gateways to understand which user is using which IP Address in the network, so those security gateways can now make decisions based on

those users (or the groups to which the users belong to). CDA runs on a Cisco Linux machine; monitors in real time a collection of Active Directory domain controller (DC) machines for authentication-related events that generally indicate user logins; learns, analyzes, and caches mappings of IP Addresses and user identities in its database; and makes the latest mappings available to its consumer devices. Reference: https://www.cisco.com/c/en/us/td/docs/security/ibf/cda_10/Install_Config_guide/cda10/cda_oveviw.html security gateways to understand which user is using which IP Address in the network, so those security gateways can now make decisions based on those users (or the groups to which the users belong to).

CDA runs on a Cisco Linux machine; monitors in real time a collection of Active Directory domain controller (DC) machines for authentication-related events that generally indicate user logins; learns, analyzes, and caches mappings of IP Addresses and user identities in its database; and makes the latest mappings available to its consumer devices.

Reference:

Cisco Context Directory Agent (CDA) is a mechanism that maps IP Addresses to usernames in order to allow security gateways to understand which user is using which IP Address in the network, so those security gateways can now make decisions based on those users (or the groups to which the users belong to). CDA runs on a Cisco Linux machine; monitors in real time a collection of Active Directory domain controller (DC) machines for authentication-related events that generally indicate user logins; learns, analyzes, and caches mappings of IP Addresses and user identities in its database; and makes the latest mappings available to its consumer devices. Reference: https://www.cisco.com/c/en/us/td/docs/security/ibf/cda_10/Install_Config_guide/cda10/cda_oveviw.html

NEW QUESTION # 524
What are two functions of TAXII in threat intelligence sharing? (Choose two.)

- A. determines how threat intelligence information is relayed
- B. determines the "what" of threat intelligence
- C. allows users to describe threat motivations and abilities
- D. Supports STIX information
- E. exchanges trusted anomaly intelligence information

Answer: A,D

NEW QUESTION # 525
An engineer is adding a Cisco DUO solution to the current TACACS+ deployment using Cisco ISE. The engineer wants to authenticate users using their account when they log into network devices. Which action accomplishes this task?

- A. Configure Cisco DUO with the external Active Directory connector and tie it to the policy set within Cisco ISE.
- B. Install and configure the Cisco DUO Authentication Proxy and configure the identity source sequence within Cisco ISE
- C. Modify the current policy with the condition MFASourceSequence DUO=true in the authorization conditions within Cisco ISE
- D. Create an identity policy within Cisco ISE to send all authentication requests to Cisco DUO.

Answer: B

Explanation:
accomplish the task is to install and configure the Cisco DUO Authentication Proxy and configure the identity source sequence within Cisco ISE. This will allow the engineer to integrate Cisco ISE with Cisco DUO for TACACS+ device administration using Active Directory as the primary authentication source and Cisco DUO as the secondary authentication source for multi-factor authentication (MFA). The steps to configure this solution are as follows12:
* Install and configure the Cisco DUO Authentication Proxy on a Windows or Linux machine. The proxy will act as a RADIUS server that communicates with Cisco ISE and a RADIUS client that communicates with Cisco DUO cloud. The proxy will also connect to Active Directory for the primary authentication of the users.
* Configure the proxy by editing the authproxy.cfg file. The file should include the following sections:
* [ad_client]: This section defines the connection parameters to Active Directory, such as the host, service_account_username, service_account_password, and search_dn.
* [radius_server_auto]: This section defines the RADIUS server parameters for the proxy, such as the ikey, skey, api_host, radius_ip_1, radius_secret_1, and client parameters. The ikey, skey, and api_host are obtained from the Cisco DUO web portal when creating a RADIUS application. The radius_ip_1 and radius_secret_1 are the IP address and shared secret of the Cisco ISE node that will send authentication requests to the proxy. The client parameter specifies the authentication method for Cisco DUO, such as auto, push, phone, or passcode.
* [main]: This section defines the global settings for the proxy, such as the debug, log_max_size, and log_max_files parameters.
* Restart the proxy service after saving the authproxy.cfg file.

* Configure Cisco ISE as a TACACS+ server and add the proxy as an external RADIUS server. The steps are as follows:
* Navigate to Administration > System > Deployment and enable the Device Administration Service on the appropriate node.
* Navigate to Work Centers > Device Administration > Network Resources and add the network devices that will use TACACS+ for device administration. Specify the device name, IP address, device type, and shared secret.
* Navigate to Work Centers > Device Administration > Network Access and add the proxy as an external RADIUS server. Specify the server name, IP address, port, shared secret, and timeout.
Optionally, enable the Continue for additional authorization policy option to allow Cisco ISE to perform authorization based on the user's Active Directory attributes after successful authentication by Cisco DUO.
* Navigate to Work Centers > Device Administration > Policy Elements > Results > TACACS Profiles and create a TACACS profile for device administration. Specify the profile name, type, and custom attributes, such as the shell:roles and shell:priv-lvl attributes.
* Navigate to Work Centers > Device Administration > Policy Sets and create a policy set for device administration. Specify the policy set name, conditions, and results. The conditions can be based on the device type, the protocol, or the identity source sequence. The results can be the TACACS profile and the external RADIUS server (the proxy).
* Configure the network devices to use TACACS+ for device administration and specify Cisco ISE as the TACACS+ server and the proxy as the RADIUS server. The configuration commands may vary depending on the device type and model, but the general syntax is as follows:
* aaa new-model
* aaa authentication login default group tacacs+ local
* aaa authorization exec default group tacacs+ local
* aaa accounting exec default start-stop group tacacs+
* tacacs server ISE
* address ipv4 <ISE IP address>
* key <ISE shared secret>
* radius server DUO
* address ipv4 <proxy IP address> auth-port <proxy port>
* key <proxy shared secret>
* Test the solution by logging into the network devices using Active Directory credentials. The user should receive a Cisco DUO prompt for the second factor authentication, such as a push notification, a phone call, or a passcode. After approving the second factor authentication, the user should be granted access to the device with the appropriate privileges based on the TACACS profile and the Active Directory attributes.
References := 1: Duo MFA Integration with ISE for TACACS+ Device Administration with Microsoft Active Directory Users - Cisco Community 2: Protecting Access to Network devices with ISE TACACS+ and DUO MFA - Cisco Community

NEW QUESTION # 526
......

We have three versions of Cisco 350-701 guide materials available on our test platform, including PDF, Software and APP online. The most popular one is PDF version of our Implementing and Operating Cisco Security Core Technologies 350-701 exam questions and you can totally enjoy the convenience of this version, and this is mainly because there is a demo in it, therefore help you choose what kind of 350-701 Practice Test are suitable to you and make the right choice.

Exam Sample 350-701 Questions: https://www.topexamcollection.com/350-701-vce-collection.html

- New 350-701 Dumps Free ☐ 350-701 Regualer Update ☐ 350-701 Free Vce Dumps ☐ Open website ▶ www.practicevce.com ◀ and search for ☐ 350-701 ☐ for free download ☐350-701 Exam Question
- Three Formats of Pdfvce Practice Material ☐ Search for ⇒ 350-701 ⇐ on ➤ www.pdfvce.com ☐ immediately to obtain a free download ☐350-701 Exam Braindumps
- A fully updated 350-701 exam guide from training and exam preparation expert www.validtorrent.com ☐ Go to website ➡ www.validtorrent.com ☐ open and search for ☐ 350-701 ☐ to download for free ☐Flexible 350-701 Learning Mode
- Pdf 350-701 Braindumps – The Best Exam Sample Questions for 350-701: Implementing and Operating Cisco Security Core Technologies ☐ Search for ☐ 350-701 ☐ on ▷ www.pdfvce.com ◁ immediately to obtain a free download ☐Most 350-701 Reliable Questions
- A fully updated 350-701 exam guide from training and exam preparation expert www.dumpsquestion.com ☐ Search for ⇒ 350-701 ⇐ and download it for free immediately on ☐ www.dumpsquestion.com ☐ ☐350-701 Reliable Exam Testking
- Make Exam Preparation Simple Cisco 350-701 Exam Questions ☐ Download ➡ 350-701 ☐ for free by simply entering [www.pdfvce.com] website ☐350-701 Visual Cert Exam
- 350-701 Reliable Braindumps Sheet ☐ New 350-701 Dumps Free ☐ 350-701 Reliable Braindumps Sheet ☐ The page for free download of ➡ 350-701 ☐ on ➡ www.practicevce.com ☐☐☐ will open immediately ☐New 350-701 Dumps Free

- Pdfvce Cisco 350-701 Real Questions Come In Three Different Formats 🔐 Open [www.pdfvce.com] and search for ➡ 350-701 🔐 to download exam materials for free 🔰350-701 Free Vce Dumps
- 350-701 Exam Practice Training Materials - 350-701 Test Dumps - www.prep4sures.top 🎊 Go to website ➽ www.prep4sures.top 🠐 open and search for ➡ 350-701 🠐🠐🠐 to download for free 🎇New 350-701 Test Question
- New 350-701 Test Forum 🃏 350-701 Visual Cert Exam 🥪 350-701 Exam Braindumps 🌷 Immediately open ➡ www.pdfvce.com 🠐🠐🠐 and search for ✔ 350-701 🠐✔ 🠐 to obtain a free download 🤡Reliable 350-701 Practice Questions
- 2026 Cisco High Hit-Rate Pdf 350-701 Braindumps 🚲 Download " 350-701 " for free by simply entering 「 www.dumpsquestion.com 」 website 🍃Useful 350-701 Dumps
- 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, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, Disposable vapes

2026 Latest TopExamCollection 350-701 PDF Dumps and 350-701 Exam Engine Free Share: https://drive.google.com/open?id=1w0eCOY7WV04rxWOgLhfcv_7PhMVRA3bT