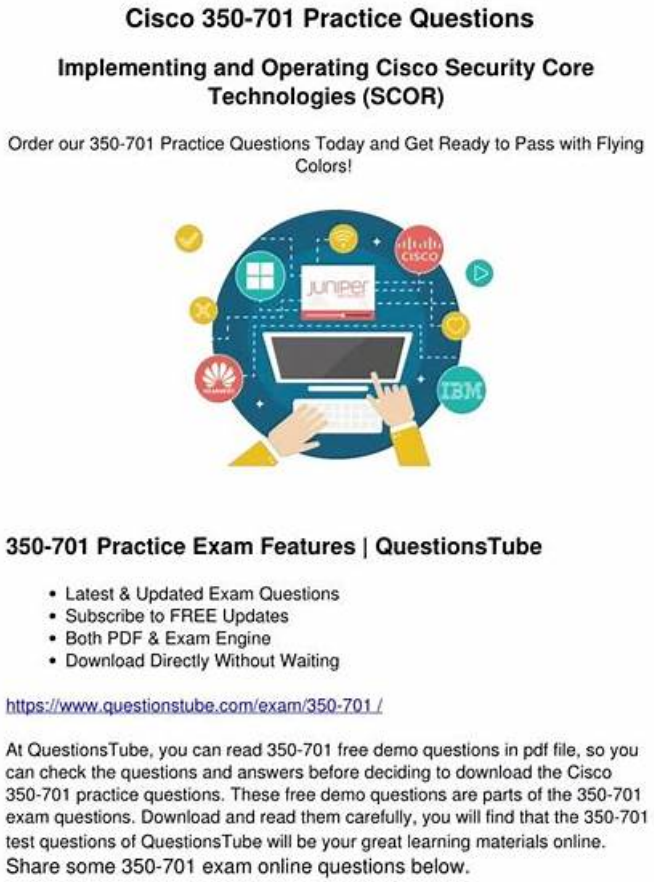
Take Your Exam Preparation to the Next Level with 350-701 Web-Based Practice Test



DOWNLOAD the newest Actual4Cert 350-701 PDF dumps from Cloud Storage for free: https://drive.google.com/open?id=1W_AlLantq4x9q4iHW42n-Mpm6j9BeBTL

If you want to buy our 350-701 training engine, you must ensure that you have credit card. We do not support deposit card and debit card to pay for the 350-701 exam questions. Also, the system will deduct the relevant money. If you find that you need to pay extra money for the 350-701 Study Materials, please check whether you choose extra products or there is intellectual property tax. All in all, you will receive our 350-701 learning guide via email in a few minutes.

Cisco 350-701 exam covers a wide range of security technologies, including network security, cloud security, endpoint protection, secure network access, visibility, and enforcement. Candidates are expected to have a strong understanding of these security technologies and their implementation in real-world scenarios. 350-701 Exam also tests candidates' abilities to configure, manage, and troubleshoot these technologies, as well as their knowledge of security policies and best practices.

>> 350-701 Reliable Test Tips <<

New Cisco 350-701 Test Tutorial, 350-701 Practice Exam Questions

With the rapid development of the world economy, it has been universally accepted that a growing number of people have longed to become the social elite. However, the competition of becoming the social elite is fierce for all people. The 350-701 latest dumps will

be a shortcut for a lot of people who desire to be the social elite. If you try your best to prepare for the 350-701 Exam and get the related certification in a short time, it will be easier for you to receive the attention from many leaders of the big company, and it also will be very easy for many people to get a decent job in the labor market by the 350-701 learning guide.

Network Security – 20%

- Implementing segmentation, access control policies, URL filtering, AVC, as well as malware protection;
- Implementing the management options for network security solutions such as perimeter security & intrusion prevention (single versus multidevice manager, in-band versus out-of-band, SFTP, DNS, SCP, CDP, and DHCP security & risks);
- Configuring AAA for network & device access (TACACS+, authentication & authorization, accounting, RADIUS & RADIUS flows, dACL);
- Comparing network security solutions that deliver the firewall capacity as well as intrusion prevention;
- Describing deployment models of network security architectures & solutions that deliver the firewall capacity as well as intrusion prevention;

Cisco 350-701 Certification Exam is designed for IT professionals who are interested in pursuing a career in the field of network security. Implementing and Operating Cisco Security Core Technologies certification exam is part of the Cisco Certified Network Professional (CCNP) Security program, which is an advanced level of certification for network security professionals. 350-701 exam tests the candidate's knowledge and skills in implementing and operating Cisco security core technologies, including network security, cloud security, endpoint protection, and secure network access.

Cisco Implementing and Operating Cisco Security Core Technologies Sample Questions (Q378-Q383):

NEW QUESTION # 378
Which type of DNS abuse exchanges data between two computers even when there is no direct connection?

- A. Network footprinting
- B. Command-and-control communication
- C. Data exfiltration
- D. Malware installation

Answer: C

Explanation:
Malware installation: This may be done by hijacking DNS queries and responding with malicious IP addresses.
Command & Control communication: As part of lateral movement, after an initial compromise, DNS communications is abused to communicate with a C2 server. This typically involves making periodic DNS queries from a computer in the target network for a domain controlled by the adversary. The responses contain encoded messages that may be used to perform unauthorized actions in the target network.
Network footprinting: Adversaries use DNS queries to build a map of the network. Attackers live off the terrain so developing a map is important to them.
Data theft (exfiltration): Abuse of DNS to transfer data; this may be performed by tunneling other protocols like FTP, SSH through DNS queries and responses. Attackers make multiple DNS queries from a compromised computer to a domain owned by the adversary. DNS tunneling can also be used for executing commands and transferring malware into the target network.

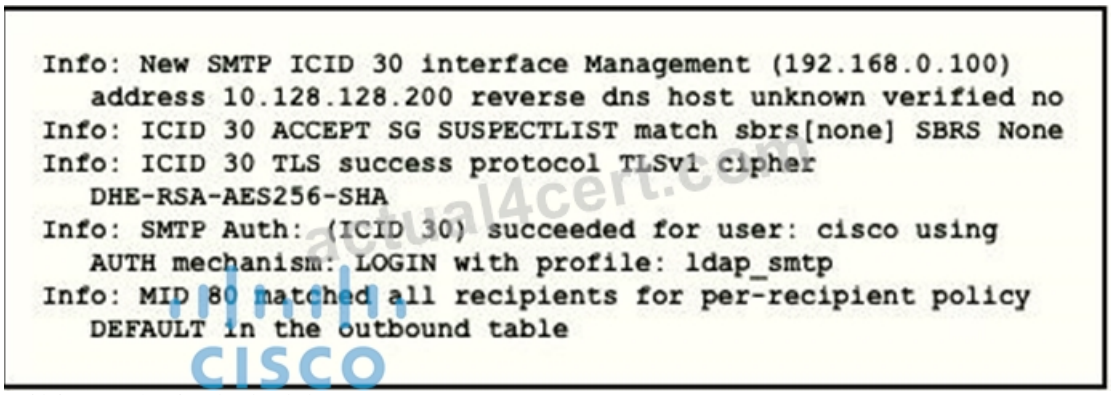
NEW QUESTION # 379
A company deploys an application that contains confidential data and has a hybrid hub-and-spoke topology.
The hub resides in a public cloud environment, and the spoke resides on-premises. An engineer must secure the application to ensure that confidential data in transit between the hub-and-spoke servers is accessible only to authorized users. The engineer performs these configurations:
* Segregation of duties
* Role-based access control
* Privileged access management
What must be implemented to protect the data in transit?

- A. MD5
- B. TLS 1.3
- C. AES-256

- D. SHA-512

Answer: B

NEW QUESTION # 380
Refer to the exhibit.



Which type of authentication is in use?

- A. LDAP authentication for Microsoft Outlook
- B. POP3 authentication
- C. external user and relay mail authentication
- D. SMTP relay server authentication

Answer: C

Explanation:
The TLS connections are recorded in the mail logs, along with other significant actions that are related to messages, such as filter actions, anti-virus and anti-spam verdicts, and delivery attempts. If there is a successful TLS connection, there will be a TLS success entry in the mail logs. Likewise, a failed TLS connection produces a TLS failed entry. If a message does not have an associated TLS entry in the log file, that message was not delivered over a TLS connection.
The TLS connections are recorded in the mail logs, along with other significant actions that are related to messages, such as filter actions, anti-virus and anti-spam verdicts, and delivery attempts. If there is a successful TLS connection, there will be a TLS success entry in the mail logs. Likewise, a failed TLS connection produces a TLS failed entry. If a message does not have an associated TLS entry in the log file, that message was not delivered over a TLS connection.
Reference:
The exhibit in this Qshows a successful TLS connection from the remote host (reception) in the mail log.
The TLS connections are recorded in the mail logs, along with other significant actions that are related to messages, such as filter actions, anti-virus and anti-spam verdicts, and delivery attempts. If there is a successful TLS connection, there will be a TLS success entry in the mail logs. Likewise, a failed TLS connection produces a TLS failed entry. If a message does not have an associated TLS entry in the log file, that message was not delivered over a TLS connection.
The exhibit in this Qshows a successful TLS connection from the remote host (reception) in the mail log.

NEW QUESTION # 381
Which network monitoring solution uses streams and pushes operational data to provide a near real-time view of activity?

- A. model-driven telemetry
- B. syslog
- C. SNMP
- D. SMTP

Answer: A

Explanation:
The traditional use of the pull model, where the client requests data from the network does not scale when what you want is near real-time data. Moreover, in some use cases, there is the need to be notified only when some data changes, like interfaces status, protocol neighbors change etc.
Model-Driven Telemetry is a new approach for network monitoring in which data is streamed from network devices continuously

using a push model and provides near real-time access to operational statistics.
Applications can subscribe to specific data items they need, by using standard-based YANG data models over NETCONF-YANG. Cisco IOS XE streaming telemetry allows to push data off of the device to an external collector at a much higher frequency, more efficiently, as well as data on-change streaming.

NEW QUESTION # 382
A network security engineer must export packet captures from the Cisco FMC web browser while troubleshooting an issue. When navigating to the address https://<FMC IP>/capure/CAPI/pcap/test.pcap, an error 403: Forbidden is given instead of the PCAP file. Which action must the engineer take to resolve this issue?

- A. Disable the proxy setting on the browser
- B. Enable the HTTPS server for the device platform policy
- C. Disable the HTTPS server and use HTTP instead
- D. Use the Cisco FTD IP address as the proxy server setting on the browser

Answer: B

Explanation:
The error 403: Forbidden indicates that the web server denied access to the requested resource, which in this case is the PCAP file. One possible reason for this error is that the HTTPS server is not enabled for the device platform policy, which is a configuration that applies to the FTD devices managed by the FMC. The device platform policy defines the settings for the management interface, the SSH access, the SNMP, the NTP, the DNS, and the HTTPS server. The HTTPS server allows the FMC to access the FTD devices via HTTPS and perform tasks such as packet capture, packet tracer, and file transfer. If the HTTPS server is not enabled for the device platform policy, the FMC cannot access the PCAP file from the FTD device via HTTPS.
Therefore, the engineer must enable the HTTPS server for the device platform policy in order to resolve this issue. To enable the HTTPS server for the device platform policy, the engineer must follow these steps:
* Log in to the FMC web interface and navigate to Devices > Platform Settings.
* Select the device platform policy that applies to the FTD device and click Edit.
* In the General tab, check the Enable HTTPS Server checkbox and click Save.
* Deploy the policy changes to the FTD device and wait for the deployment to complete.
* Try to access the PCAP file again from the FMC web browser using the same address.
Alternatively, the engineer can also enable the HTTPS server for the FTD device from the FTD CLI using the command configure network https-server enable. However, this method is not recommended because it may cause a configuration conflict with the FMC123 References ≔ 1: Use Firepower Threat Defense Captures and Packet Tracer - Cisco 2: Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager, Version 6.6 - Device Management Basics [Cisco Firepower NGFW] - Cisco 3: Cisco Firepower Threat Defense Command Reference - C through D Commands [Cisco Firepower NGFW] - Cisco

NEW QUESTION # 383
.....

- Latest 350-701 Material □ Printable 350-701 PDF □ 350-701 Reliable Test Tips □ Search for （ 350-701 ） and download it for free immediately on ➠ www.examcollectionpass.com □ □Valid 350-701 Exam Syllabus
- Pass Guaranteed Quiz 2025 Cisco 350-701 – Reliable Reliable Test Tips □ The page for free download of □ 350-701 □ on ➡ www.pdfvce.com □□□ will open immediately □350-701 Exam
- Valid Exam 350-701 Vce Free □ 350-701 Reliable Test Tips □ 350-701 Reliable Test Cram ☂ Search for □ 350-701 □ and obtain a free download on ☀ www.prep4away.com □☀□ ↖Latest 350-701 Exam Bootcamp
- www.l2tw.com, bbs.tongchai.org.cn, ncon.edu.sa, 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, study.stcs.edu.np, pct.edu.pk, 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, myportal.utt.edu.tt, longcai.xuzhijian.com.cn, Disposable vapes

BTW, DOWNLOAD part of Actual4Cert 350-701 dumps from Cloud Storage: https://drive.google.com/open?id=1W_AlLantq4x9q4iHW42n-Mpm6j9BeBTL