

# Online CompTIA CAS-005 Practice Test Engine Designed by Experts



2026 Latest PrepAwayTest CAS-005 PDF Dumps and CAS-005 Exam Engine Free Share: <https://drive.google.com/open?id=1Op0jckMvQxwMjIYxN4j-V6PyIxykb0dr>

The pass rate reaches 98.95%, and if you choose us, we can ensure you pass the exam. CAS-005 study materials are edited by skilled professionals, and they are quite familiar with the dynamics of the exam center, therefore CAS-005 study materials can meet your needs for exam. What's more, we offer you free demo to try before purchasing CAS-005 Exam Dumps, so that you can know the mode of the complete version. If you have any questions about CAS-005 study materials, you can ask for our service stuff for help.

## CompTIA CAS-005 Exam Syllabus Topics:

Topic	Details
Topic 1	<ul style="list-style-type: none"><li>• Governance, Risk, and Compliance: This section of the exam measures the skills of CompTIA security architects that cover the implementation of governance components based on organizational security requirements, including developing policies, procedures, and standards. Candidates will learn about managing security programs, including awareness training on phishing and social engineering.</li></ul>
Topic 2	<ul style="list-style-type: none"><li>• Security Operations: This domain is designed for CompTIA security architects and covers analyzing data to support monitoring and response activities, as well as assessing vulnerabilities and recommending solutions to reduce attack surfaces. Candidates will apply threat-hunting techniques and utilize threat intelligence concepts to enhance operational security.</li></ul>
Topic 3	<ul style="list-style-type: none"><li>• Security Engineering: This section measures the skills of CompTIA security architects that involve troubleshooting common issues related to identity and access management (IAM) components within an enterprise environment. Candidates will analyze requirements to enhance endpoint and server security while implementing hardware security technologies. This domain also emphasizes the importance of advanced cryptographic concepts in securing systems.</li></ul>
Topic 4	<ul style="list-style-type: none"><li>• Security Architecture: This domain focuses on analyzing requirements to design resilient systems, including the configuration of firewalls and intrusion detection systems.</li></ul>

>> New CAS-005 Test Experience <<

## Pass Guaranteed Quiz CAS-005 - CompTIA SecurityX Certification Exam Perfect New Test Experience

If you want to be a part of a great company, such as CAS-005, preparing and taking the exam with CAS-005 study guide will be

your best choice, because there have been more and more big companies to pay real attention to these people who have passed the CAS-005 Exam and have got the related certification in the past years. It is a generally accepted fact that the CAS-005 exam has attracted more and more attention and become widely acceptable in the past years.

## CompTIA SecurityX Certification Exam Sample Questions (Q72-Q77):

### NEW QUESTION # 72

A company wants to install a three-tier approach to separate the web, database, and application servers. A security administrator must harden the environment which of the following is the best solution?

- A. Configuring a SASb solution to restrict users to server communication
- B. Deploying a VPN to prevent remote locations from accessing server VLANs
- C. installing a firewall and making it the network core
- **D. Implementing microsegmentation on the server VLANs**

**Answer: D**

Explanation:

The best solution to harden a three-tier environment (web, database, and application servers) is to implement microsegmentation on the server VLANs.

Enhanced Security: Microsegmentation creates granular security zones within the data center, allowing for more precise control over east-west traffic between servers. This helps prevent lateral movement by attackers who may gain access to one part of the network.

Isolation of Tiers: By segmenting the web, database, and application servers, the organization can apply specific security policies and controls to each segment, reducing the risk of cross-tier attacks.

Compliance and Best Practices: Microsegmentation aligns with best practices for network security and helps meet compliance requirements by ensuring that sensitive data and systems are properly isolated and protected.

### NEW QUESTION # 73

A company's SIEM is continuously reporting false positives and false negatives. The security operations team has implemented configuration changes to troubleshoot possible reporting errors. Which of the following sources of information best supports the required analysis process?

(Choose two.)

- **A. Third-party reports and logs**
- **B. Trends**
- C. Dashboards
- D. Network traffic summaries
- E. Alert failures
- F. Manual review processes

**Answer: A,B**

Explanation:

When dealing with false positives and false negatives reported by a Security Information and Event Management (SIEM) system, the goal is to enhance the accuracy of the alerts and ensure that actual threats are identified correctly. The following sources of information best support the analysis process:

Third-party reports and logs: Utilizing external sources of information such as threat intelligence reports, vendor logs, and other third-party data can provide a broader perspective on potential threats. These sources often contain valuable insights and context that can help correlate events more accurately, reducing the likelihood of false positives and false negatives.

Trends: Analyzing trends over time can help in understanding patterns and anomalies in the data.

By observing trends, the security team can distinguish between normal and abnormal behavior, which aids in fine-tuning the SIEM configurations to better detect true positives and reduce false alerts.

### NEW QUESTION # 74

A security administrator is reviewing the following code snippet from a website component:

```
<link rel="stylesheet" type="text/css" font-weight: normal;
font-style: normal;
if ((is_admin() " (function_exists ('get_hex_cache')) != true {add_action('wp-head' . 'get_hex_cache',12) function
get_hex_cache () { return print (hex2bin('3c7',(file_get_contents ('dir' /inc.tmp)...
21487592579325342038509345083453432452523435235345523453242353424523453452345389627656385793257839537854362038263053
2804508325
```

A review of the inc.tmp file shows the following:

```
21487592579325342038509345083453432452523435235345523453242353424523453452345389627656385793257839537854362038263053
2804508325
```

Which of the following is most likely the reason for inaccuracies?

- A. The WAF is configured to be in transparent mode.
- **B. A content management solution plug-in has been exploited.**
- C. A search engine's bots are being blocked at the firewall.
- D. The relevant stylesheet has become corrupted.

**Answer: B**

Explanation:

The code indicates that a WordPress (CMS) plug-in has likely been exploited. The function `get_hex_cache()` combines obfuscated PHP code (`hex2bin`) with external file retrieval (`inc.tmp`). This is characteristic of malicious plug-in injections in content management systems such as WordPress, where attackers inject backdoors or malicious scripts through vulnerable plug-ins.

Option B (search engine bots blocked) and C (corrupted stylesheet) would not explain injected PHP logic. Option D (WAF in transparent mode) reduces security controls but does not create malicious functions inside the CMS code.

The presence of obfuscated data in `inc.tmp` strongly suggests tampering. Exploited CMS plug-ins are a common initial access vector, often used to hide persistent malware or web shells.

## NEW QUESTION # 75

A software development team requires valid data for internal tests. Company regulations, however do not allow the use of this data in cleartext. Which of the following solutions best meet these requirements?

- A. Implementing data obfuscation
- B. Configuring data hashing
- **C. Deploying tokenization**
- D. Replacing data with null record

**Answer: C**

Explanation:

Tokenization replaces sensitive data elements with non-sensitive equivalents, called tokens, that can be used within the internal tests. The original data is stored securely and can be retrieved if necessary. This approach allows the software development team to work with data that appears realistic and valid without exposing the actual sensitive information.

Configuring data hashing (Option A) is not suitable for test data as it transforms the data into a fixed-length value that is not usable in the same way as the original data. Replacing data with null records (Option C) is not useful as it does not provide valid data for testing. Data obfuscation (Option D) could be an alternative but might not meet the regulatory requirements as effectively as tokenization.

Reference:

CompTIA Security+ Study Guide

NIST SP 800-57 Part 1 Rev. 5, "Recommendation for Key Management"

PCI DSS Tokenization Guidelines

## NEW QUESTION # 76

An IPSec solution is being deployed. The configuration files for both the VPN concentrator and the AAA server are shown in the diagram.

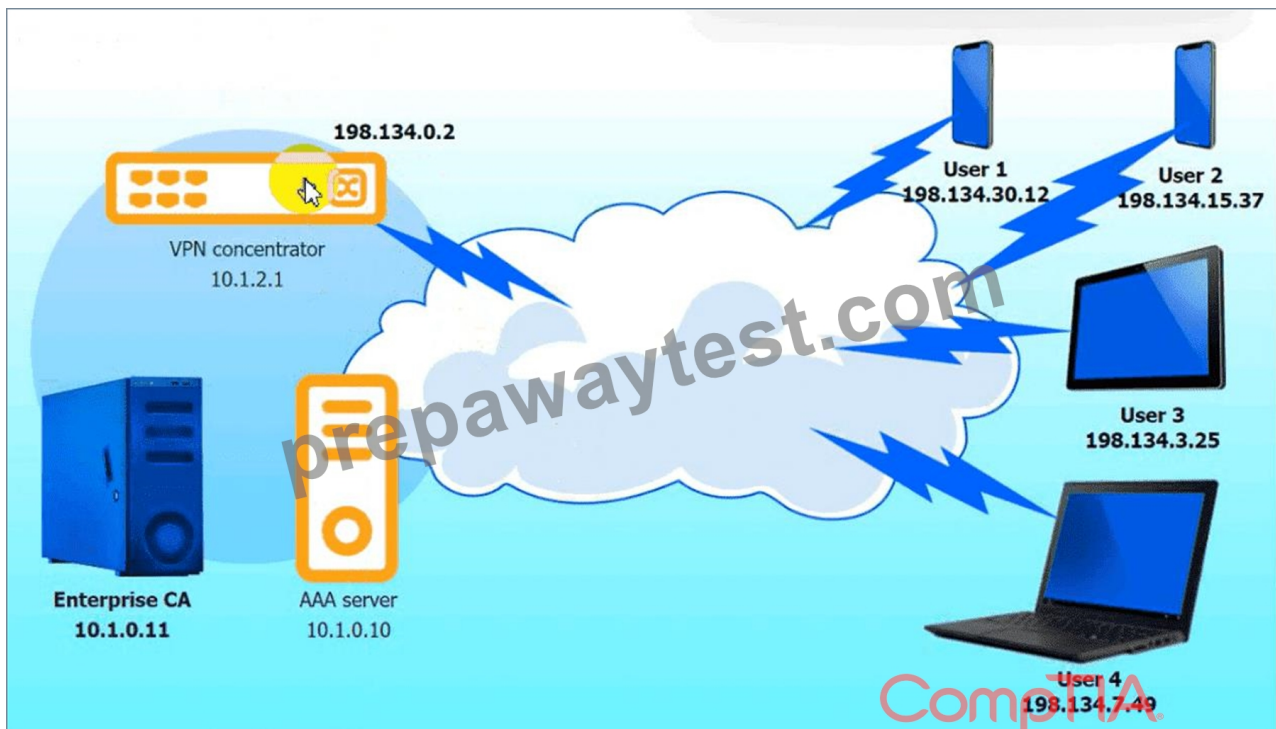
Complete the configuration files to meet the following requirements:

\* The EAP method must use mutual certificate-based authentication (With issued client certificates).

\* The IKEv2 Cipher suite must be configured to the MOST secure authenticated mode of operation,

\* The secret must contain at least one uppercase character, one lowercase character, one numeric character, and one special character, and it must meet a minimum length requirement of eight characters, INSTRUCTIONS Click on the AAA server and VPN concentrator to complete the configuration.

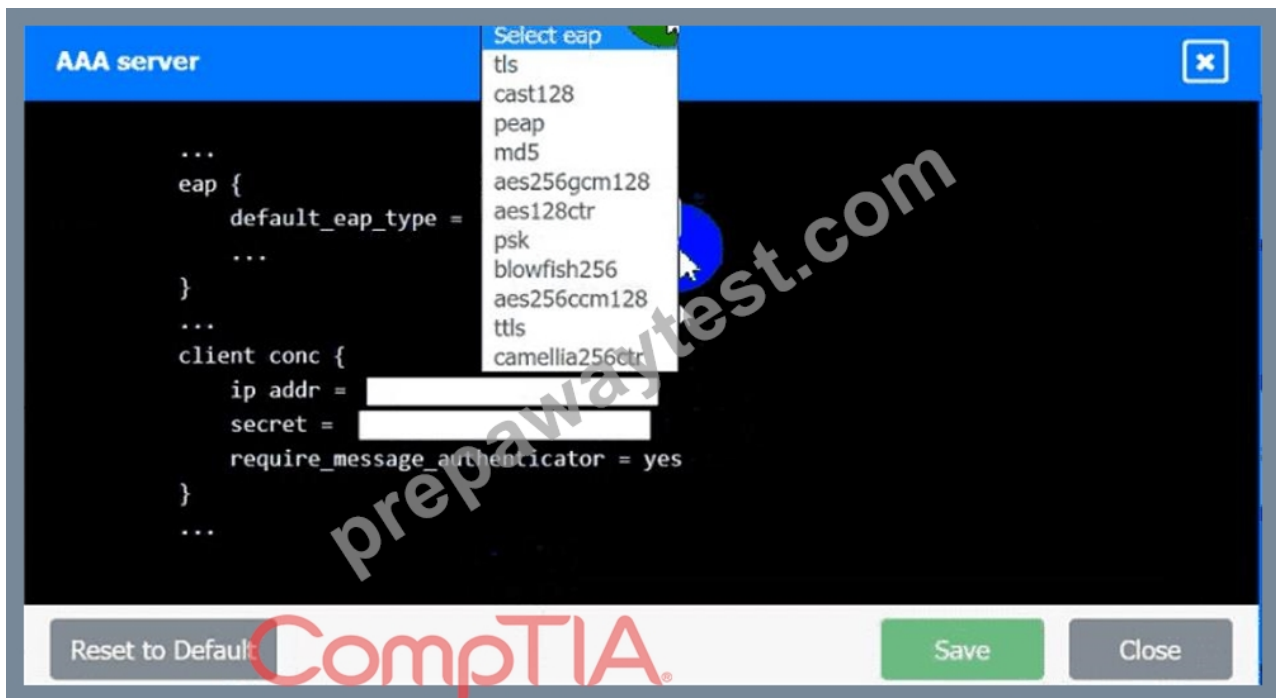
Fill in the appropriate fields and make selections from the drop-down menus.



VPN Concentrator:



AAA Server:



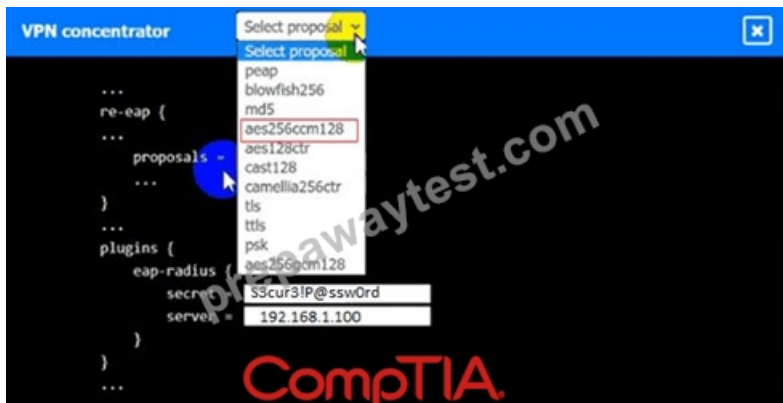
**Answer:**

Explanation:

See the answer below in Explanation

Explanation:

VPN Concentrator:



AAA Server:





