



1D0-571^{Q&As}

CIW V5 Security Essentials

Pass CIW 1D0-571 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

<https://www.passapply.com/1d0-571.html>

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by CIW Official Exam Center

- ⚙️ **Instant Download** After Purchase
- ⚙️ **100% Money Back** Guarantee
- ⚙️ **365 Days** Free Update
- ⚙️ **800,000+** Satisfied Customers





QUESTION 1

What is the primary strength of symmetric-key encryption?

- A. It allows easy and secure exchange of the secret key.
- B. It creates a hash of a text, enabling data integrity. It creates a hash of a text, enabling data integrity.
- C. It can encrypt large amounts of data very quickly.
- D. It provides non-repudiation services more efficiently than asymmetric-key encryption.

Correct Answer: C

QUESTION 2

A security breach has occurred in which a third party was able to obtain and misuse legitimate authentication information. After investigation, you determined that the specific cause for the breach was that end users have been placing their passwords underneath their keyboards. Which step will best help you resolve this problem?

- A. Discipline specific end users as object lessons to the rest of the staff and reset passwords on all systems immediately.
- B. Change all passwords on the company servers immediately and inform end users that their passwords will be changing on a regular basis.
- C. Set passwords to expire at specific intervals and establish mandatory continual training sessions.
- D. Inform end users that their passwords will be changing on a regular basis and require more complex passwords.

Correct Answer: C

QUESTION 3

Which of the following can help you authoritatively trace a network flooding attack?

- A. Your ISP
- B. Firewall logs
- C. Router logs
- D. Ping

Correct Answer: A

QUESTION 4

Which of the following describes the practice of stateful multi-layer inspection?



- A. Using a VLAN on a firewall to enable masquerading of private IP addresses
- B. Prioritizing voice and video data to reduce congestion
- C. Inspecting packets in all layers of the OSI/RM with a packet filter
- D. Using Quality of Service (QoS) on a proxy-oriented firewall

Correct Answer: C

QUESTION 5

Which of the following is considered to be the most secure default firewall policy, yet usually causes the most work from an administrative perspective?

- A. Configuring the firewall to respond automatically to threats
- B. Blocking all access by default, then allowing only necessary connections
- C. Configuring the firewall to coordinate with the intrusion-detection system
- D. Allowing all access by default, then blocking only suspect network connections

Correct Answer: B

[Latest 1D0-571 Dumps](#)

[1D0-571 PDF Dumps](#)

[1D0-571 Braindumps](#)