PassQueen
a.k.a dumpsqueen.com

HCIP-Security V4.0

Huawei H12-725_V4.0

Version Demo

Total Demo Questions: 2

Total Premium Questions: 22

Buy Premium PDF

https://passqueen.com

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, Network Security Policy Deployment and Management	7
Topic 2, Network Security Protection	7
Topic 3, Network Security Operation and Maintenance	7
Topic 4, Network Security Planning and Deployment	1
Total	22

QUESTION NO: 1

A security policy from the trust zone to the untrust zone contains a broad rule that permits all HTTP traffic. A later rule denies HTTP access from the Finance subnet to a specific Internet address. Users in the Finance subnet can still access that address. Which operation should be performed?

A. Move the specific deny rule above the broad permit rule.

B. Change the broad permit rule to use a higher source port range.

C. Add an additional permit rule below the specific deny rule.

D. Configure source NAT for the Finance subnet.

ANSWER: A

Explanation:

Huawei firewall security policies are matched in sequence. When the broad permit rule is matched first, subsequent rules are not evaluated for the session. Move the more specific deny rule above the broad permit rule so that Finance traffic to the specified destination is denied before the general HTTP permit rule can match. Changing the service definition or adding another rule below the broad permit rule does not correct the policy-order issue.

QUESTION NO: 2

A firewall validates a peer certificate during certificate-based VPN authentication. Which of the following checks are required to determine whether the certificate can be trusted? *(Select three)*

A. Verify that the certificate chain terminates at a trusted CA certificate.

B. Verify that the certificate is within its validity period.

C. Check certificate revocation status by using the configured revocation mechanism.

D. Obtain the peer private key to verify the certificate signature.

E. Verify that the peer uses the same source NAT address as the firewall.

ANSWER: A B C

Explanation:

The firewall must validate the certificate chain to a trusted CA, verify that the certificate is within its validity period, and check that the certificate has not been revoked through the configured revocation mechanism. The peer private key must remain private and is not provided to the firewall for certificate validation. A matching source NAT address is unrelated to certificate trust.