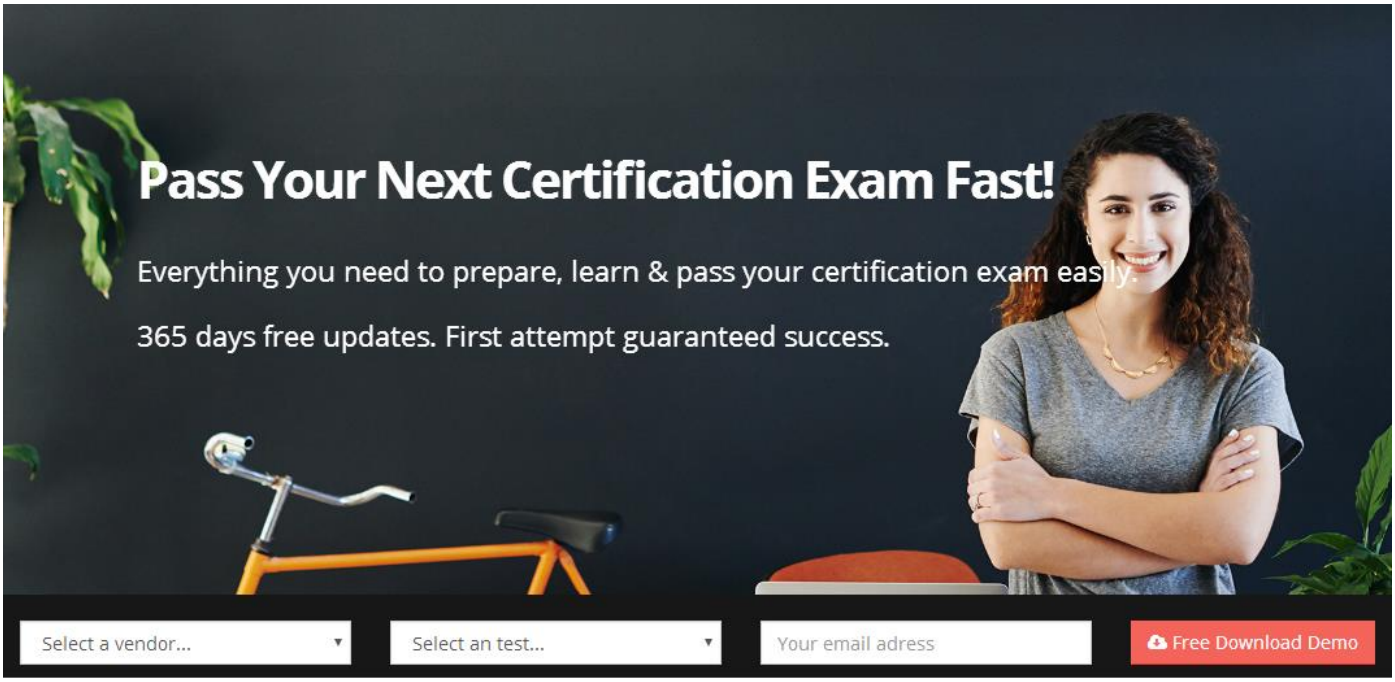
Exams4sures



Security & Privacy

Exams4sures respect customer privacy. We use McAfee's security service to provide you with utmost security for your personal information & peace of mind.

Instant Download

After Payment, our system will send you the products you purchase in mailbox in a minute after payment. If not received within 2 hours, please contact Exams4sures.

365 Days Free Updates

Free update is available within 365 days after your purchase. After 365 days, you will get 50% discounts for updating.

Try Before Buy

Exams4sures offers free demo of each product. You can check out the interface, question quality and usability of our practice exams before you decide to buy.

48923+
Happy Clients

48923+
Shares

97846+
Downloads

9999+
Years in Business

http://www.exams4sures.com/

Everything you need to prepare, learn & pass your certification exam easily.

Exam : **H12-711_V4.0**

Title : HCIA-Security V4.0

Vendor : Huawei

Version : DEMO

NO.1 Which of the following statements is incorrect about information transmission through the heartbeat link between two firewalls that work in hot standby mode?

A. Heartbeat packets are sent to synchronize configuration commands and status information between the two firewalls.

B. Heartbeat packets are periodically sent by the two firewalls to check whether the peer device is alive.

C. VGMP packets are sent to check the status of the peer device, so as to determine whether a switchover is required.

D. Configuration consistency check packets are sent to check whether key configurations of the two firewalls are consistent.

Answer: A

Explanation:

In Huawei firewall hot standby, the heartbeat link is mainly used to maintain the backup relationship and monitor peer status. Through this link, the two firewalls periodically exchange heartbeat packets to confirm whether the peer device is alive and operating normally. This makes statement B correct.

The heartbeat link also carries VGMP-related packets , which help the devices determine their active or standby roles and decide whether a switchover is necessary when faults or status changes occur. Therefore, statement C is also correct.

In addition, the firewalls can exchange configuration consistency check information to verify whether key configurations on both devices match, so statement D is correct as well.

The incorrect statement is A . Configuration and status synchronization between hot standby firewalls is not described simply as heartbeat packets being used to synchronize configuration commands and status information. Heartbeat packets are mainly for liveness detection and status maintenance , while configuration or session synchronization is handled by dedicated hot standby synchronization mechanisms rather than ordinary heartbeat packets themselves. Therefore, A is the incorrect statement.

NO.2 The trigger modes of the built-in Portal authentication in the firewall include pre-authentication and ____ authentication.

Answer:

session

NO.3 Which of the following descriptions about the heartbeat interface is wrong ( )?

A. It is recommended to configure at least two heartbeat interfaces. - One heartbeat interface is used as the master, and the other heartbeat interface is used as the backup.

B. The interface MTU value is greater than 1500 and cannot be used as a heartbeat interface

C. The connection method of the heartbeat interface can be directly connected, or it can be connected through a switch or router

D. MGMT interface (Gigabi tEtherneto/0/0) cannot be used as heartbeat interface

Answer: B

NO.4 Which of the following types of malicious code on your computer includes?

A. Oral virus

B. Trojan horses

C. Port SQL injection
D. Oral spyware
Answer: A B C D

NO.5 Database operation records can be used as ___ evidence to backtrack security events.
Answer:
electronic

NO.6 Which of the following is the numbering range of Layer 2 ACLs?
A. The 3000~3999
B. The 4000~4999
C. The 1000~1999
D. @2000~2999
Answer: A

NO.7 A three-way handshake is required to establish a TCP connection, and a four-way handshake is required to end a TCP connection.
A. TRUE
B. FALSE
Answer: A
Explanation From HCIA-Security documents:
TCP is a connection-oriented transport protocol, so it must establish a reliable session before user data can be exchanged. To create the session, TCP uses the three-way handshake: the initiator sends a SYN to request a connection and advertise its initial sequence number, the responder replies with SYN/ACK to acknowledge the request and provide its own initial sequence number, and finally the initiator sends an ACK to confirm receipt. This process confirms bidirectional reachability, synchronizes sequence numbers, and prepares both ends for reliable delivery, retransmission control, and flow control.
To end a TCP connection gracefully, TCP performs an orderly close in both directions (full-duplex). One endpoint sends FIN to indicate it has no more data to send, the peer responds with ACK . When the peer is also ready to stop sending, it transmits its own FIN , and the original endpoint responds with a final ACK .
Because each direction is closed independently, termination is typically described as a four-way handshake .

NO.8 Which of the following zones is not the firewall default security zone?
A. Trust
B. The Local
C. DMZ
D. Management
Answer: D

NO.9 Which of the following is the correct sequence for incident response management
1. Detection 2 Report 3 Mitigation 4 Lessons learned 5 Fix 6 Recovery 7 Response

A. 1- > 3- > 2- > 7- > 6- > 5- > 4
B. 1- > 7- > 3- > 2- > 6- > 5- > 4
C. 1- > 3- > 2- > 7- > 5- > 6- > 4
D. 1- > 2- > 3- > 7- > 6- > 5- > 4
Answer: B

NO.10 Among the various aspects of the risk assessment of IS027001, which of the following does not belong to the system design and release process?
A. Hold a summary meeting of the project in the information security management stage
B. Determine risk disposal measures and implement rectification plans
C. Determine risk tolerance and risk appetite
D. System integration and information security management system document preparation
Answer: A

NO.11 As shown in the figure, packet obtaining software is used to obtain some packets on a terminal. Which of the following statements is correct about the obtained packet information?

192.168.1.2	192.168.1.1	TCP	nfs > http [SYN] Seq=0 Win=81
192.168.1.1	192.168.1.2	TCP	http > nfs [SYN, ACK] Seq=0 A
192.168.1.2	192.168.1.1	TCP	nfs > http [ACK] Seq=1 Ack=1

A. The terminal sends a TCP connection establishment request to 192.168.1.1.
B. The terminal sends a TCP connection termination request to 192.168.1.1.
C. The terminal uses Telnet to log in to another device.
D. The terminal uses HTTP to log in to another device.
Answer: A
Explanation:
The packet capture in the figure shows three TCP packets exchanged between 192.168.1.2 and 192.168.1.1 .
The first packet from 192.168.1.2 # 192.168.1.1 contains the [SYN] flag. In TCP communication, the SYN flag indicates that a host is requesting to establish a TCP connection . This is the first step of the TCP three- way handshake process.
The second packet from 192.168.1.1 # 192.168.1.2 contains [SYN, ACK] , meaning the destination host acknowledges the request and agrees to establish the connection while sending its own synchronization request. The third packet from 192.168.1.2 # 192.168.1.1 contains [ACK] , confirming the response and completing the connection establishment process.
This sequence (SYN # SYN/ACK # ACK) clearly indicates the TCP connection establishment procedure , not termination. TCP connection termination normally involves FIN and ACK flags rather than SYN. Although the capture shows ports such as nfs > http , the packets shown only represent the TCP handshake and do not confirm application-layer login activities such as Telnet or HTTP authentication. Therefore, the correct statement is that the terminal is sending a TCP connection establishment request to 192.168.1.1 .

NO.12 During the process of establishing IPSec VPN between peers FW_A and FW_B, two types of security associations need to be established in two stages. In the first stage, _____ is established to verify the identity of the peers.

Answer:
IKE SA

NO.13 ____- The goal is to provide a rapid, composed and effective response in emergency situations, thereby enhancing the ability of the business to recover immediately from a disruptive event.
Answer:
business continuity plan

NO.14 When logging in to the web UI through HTTPS, you need to specify a local certificate issued by a CA that the web browser trusts for the HTTPS client on the device. Because the web browser can verify the local certificate, this approach avoids malicious attacks and ensures secure logins of administrators.
A. TRUE
B. FALSE
Answer: A
Explanation From HCIA-Security documents:
HTTPS protects web-based management by combining encryption with server identity authentication . For the browser to trust the device's HTTPS service, the device must present a server certificate that can be validated by the browser. That is why administrators often configure the device to use a local certificate (the device's certificate) that is issued by a trusted CA or whose CA chain has been imported into the browser/OS trust store. When the certificate is trusted, the browser can verify the certificate chain, validity period, and hostname binding, which helps prevent attackers from impersonating the device during login.
If a device uses a self-signed or untrusted certificate, the browser shows warnings and users may click through them, increasing the risk of man-in-the-middle attacks and credential theft. Using a CA-trusted certificate strengthens administrator logins by ensuring the management page you connect to is genuinely the intended device and that the session is encrypted end-to-end.

NO.15 Which of the following statements is incorrect about L2TP?
A. L2TP VPN is mainly used in remote office scenarios to provide remote intranet resource access for employees on business trips.
B. L2TP VPN is a tunneling technology used to transmit PPP packets.
C. PPP packets can be directly transmitted on the Internet.
D. L2TP VPN can provide remote access services for employees on business trips, regardless of whether they access the Internet through traditional dial-up or Ethernet.
Answer: C
Explanation From HCIA-Security documents:
L2TP is a Layer 2 tunneling protocol designed to carry PPP frames across an IP network by encapsulating them inside L2TP tunnels. That's why statement B is correct: L2TP's job is to transport PPP traffic through a tunnel between an L2TP Access Concentrator and an L2TP Network Server. In typical remote-access VPN use, employees connect from outside (hotel, home, mobile network) and reach internal resources through the VPN, so A and D match common deployment scenarios.
The incorrect statement is C because PPP is not routable over the public Internet by itself. PPP was originally meant for point-to-point links (like dial-up or serial links). On an IP network such as the

Internet, PPP frames must be encapsulated by a method like L2TP (often paired with IPsec for confidentiality and integrity) or converted via technologies such as PPPoE/PPPoA for specific access networks.