Huawei
H19-408
Huawei Certified Specialist Professional-Presales-Network Security Planning and Design

For More Information – Visit link below:
https://www.examsempire.com/

Product Version

1. **Up to Date products, reliable and verified.**
2. **Questions and Answers in PDF Format.**



Latest Version: 6.0

Question: 1

A government agency's security architect is reviewing what an active/standby NGFW pair keeps consistent through HRP backup. The architect wants to know which settings can be configured once on the active firewall and relied on to appear on the standby.
Which items does HRP back up from the active firewall to the standby?
(Choose two.)

A. Security policies
B. Interface IP addresses
C. NAT policies
D. Routes learned through OSPF

Answer: A,C

Question: 2

A regional ISP offers managed firewall services to several small enterprises from one shared firewall cluster in its data center. The customers use overlapping private address ranges, each wants its own security policies and NAT rules, and each must manage its own policies without seeing or affecting another customer's configuration.
Which firewall capability should the ISP's design rely on?

A. A security zone per customer, all within one shared policy set
B. Virtual systems, one per customer
C. Separate VLAN interfaces per customer with common NAT rules
D. Hot standby between two firewalls, with policies split per member

Answer: B

Question: 3

An e-commerce retailer's public storefront sits behind a stateful firewall that permits only HTTPS to the web servers. Penetration testers nevertheless extracted customer records by submitting crafted input in a search form, which the application passed to its database as part of a query.
Which security device is designed to address this attack in front of the web servers?

A. A second stateful firewall layer with stricter port rules
B. An Anti-DDoS cleaning device ahead of the firewall

C. An SSL VPN gateway for customer access to the storefront
D. A web application firewall

Answer: D

Question: 4

A container-shipping company's firewall logs show one external address sending probes to hundreds of ports across the servers in its DMZ within a few minutes. No connection has succeeded yet, but the security team wants such sources stopped automatically before an exploit follows.
Which basic firewall function addresses this need?

A. Scanning attack defense, which detects probing and blacklists the source
B. NAT Server, which hides the real server addresses behind a public address
C. ASPF, which tracks multi-channel protocols and opens dynamic data ports
D. Bandwidth management, which limits the traffic rate allowed from each source

Answer: A

Question: 5

A municipal government's firewall has an untrust zone facing the internet and a DMZ zone holding its public website. The DMZ has a higher security priority than the untrust zone. Internet users connect to the website through the firewall.
How is the direction of this traffic described in firewall terminology?

A. Outbound, from a higher- to a lower-priority zone
B. Outbound, from a lower- to a higher-priority zone
C. Inbound, from a higher- to a lower-priority zone
D. Inbound, from a lower- to a higher-priority zone

Answer: D

Question: 6

After a ransomware incident, a regional bank restores its branch systems from offline backups, verifies that the restored data is clean, and revises its recovery plan so that the next restoration is faster.
Which function of the IPDRR (Identify, Protect, Detect, Respond, Recover) framework do these activities belong to?

A. Respond, which contains and analyzes an incident while it is unfolding
B. Recover, which restores capabilities and services affected by an incident

C. Protect, which puts safeguards in place to limit potential events
D. Identify, which builds an understanding of assets, risks and business context

Answer: B

Question: 7

An energy utility's campus has NGFWs, switches and wireless controllers, each producing its own logs. During a recent incident, analysts could not connect events across these devices into one picture of how the attacker moved. The utility wants a component that collects logs and traffic data from the whole network and correlates them to expose advanced threats.
In Huawei's campus security solution, which component performs this role?

A. FireHunter, the sandbox that runs suspicious files in a virtual environment
B. The egress NGFW, correlating the logs held in its own local storage
C. HiSec Insight, the situational-awareness platform
D. Anti-DDoS, detecting and cleaning traffic floods at the campus border

Answer: C

Question: 8

A city hospital cannot patch an internal web server for several weeks because the clinical software vendor has not yet certified the fix. The firewall must keep allowing clinicians' web traffic to the server, but the security team wants attack traffic that tries to exploit the known vulnerability detected and blocked in the meantime.
Which content-security function is designed for this?

A. Intrusion prevention with exploit signatures
B. File blocking by file type and transfer direction
C. URL filtering by site category
D. Antivirus scanning of downloads

Answer: A

Question: 9

A logistics company sends daily shipment manifests from its regional depots to headquarters over a leased line. An internal review finds that several manifests arrived with altered delivery addresses. The files were not disclosed to anyone outside the company, and the transfer service stayed available throughout the period.
Which security property did this incident primarily violate?

A. Confidentiality, as the manifests were read by unauthorized outside parties
B. Availability, as the transfer service was interrupted
C. Non-repudiation, as a depot later denied having sent its manifest file
D. Integrity, as the manifest contents were changed without authorization

Answer: D

Question: 10

Staff in one office subnet at a regional hospital report intermittently slow access and certificate warnings when opening internal web portals. Users on other subnets are unaffected. The network team finds that, on affected PCs, the MAC address recorded for the default gateway matches an ordinary workstation on the same subnet rather than the gateway itself.
Which attack best explains these symptoms?

A. MAC flooding that fills the access switch table so frames are broadcast
B. ARP spoofing that puts the rogue workstation between users and the gateway
C. A SYN flood against the portal servers exhausting their connection resources
D. DNS cache poisoning on the internal DNS server redirecting portal names

Answer: B

Thank You for Trying Our Product

Special 16 USD Discount Coupon: NSZUBG3X

Email: support@examsempire.com

Check our Customer Testimonials and ratings available on every product page.

Visit our website.

https://examsempire.com/