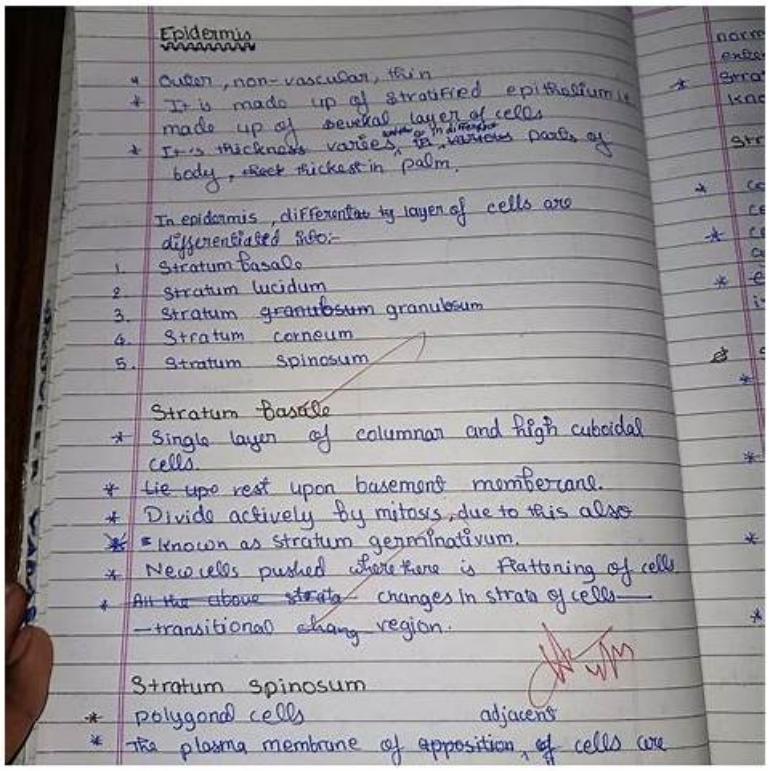
2026 Valid H12-725_V4.0 Exam Materials | High-quality HCIP-Security V4.0 100% Free Reliable Test Review



P.S. Free & New H12-725_V4.0 dumps are available on Google Drive shared by Dumpcollection: https://drive.google.com/open?id=146o9xxyJioC4pC-rqigSclnGOgb1Mv4p

Firstly, our company always feedbacks our candidates with highly-qualified H12-725_V4.0 study guide and technical excellence and continuously developing the most professional H12-725_V4.0 exam materials. Secondly, our H12-725_V4.0 study materials persist in creating a modern service oriented system and strive for providing more preferential activities for your convenience. Come and buy our H12-725_V4.0 Exam Materials, you will get more than you can imagine!

Huawei H12-725_V4.0 (HCIP-Security V4.0) Exam is one of the most popular certification exams in the field of network security. It is designed to test the skills and knowledge of candidates in various aspects of network security, including network security planning and design, network security implementation, network security management, and network security troubleshooting.

Huawei H12-725_V4.0 (HCIP-Security V4.0) certification exam is one of the most sought-after certifications in the IT industry. It is designed for IT professionals who want to validate their knowledge and skills in network security. HCIP-Security V4.0 certification covers a wide range of topics, including network security technologies, security management, and security policies and procedures.

>> Valid H12-725_V4.0 Exam Materials <<

Reliable H12-725_V4.0 Test Review & New H12-725_V4.0 Exam Duration

Learning knowledge is just like building a house, our H12-725_V4.0 training materials serve as making the solid foundation from the start with higher efficiency. Even if this is just the first time you are preparing for the exam, you can expect high grade. Taking full advantage of our H12-725_V4.0 Preparation exam and getting to know more about them means higher possibility of it. And if you have a try on our H12-725_V4.0 exam questions, you will love them.

Huawei H12-725_V4.0 (HCIP-Security V4.0) Certification Exam is designed for IT professionals who specialize in network security. HCIP-Security V4.0 certification exam equips candidates with the knowledge and skills required to design, deploy, and manage secure networks using Huawei technologies and products. The HCIP-Security V4.0 certification is a significant milestone for IT professionals looking to advance their careers in network security.

Huawei HCIP-Security V4.0 Sample Questions (Q34-Q39):

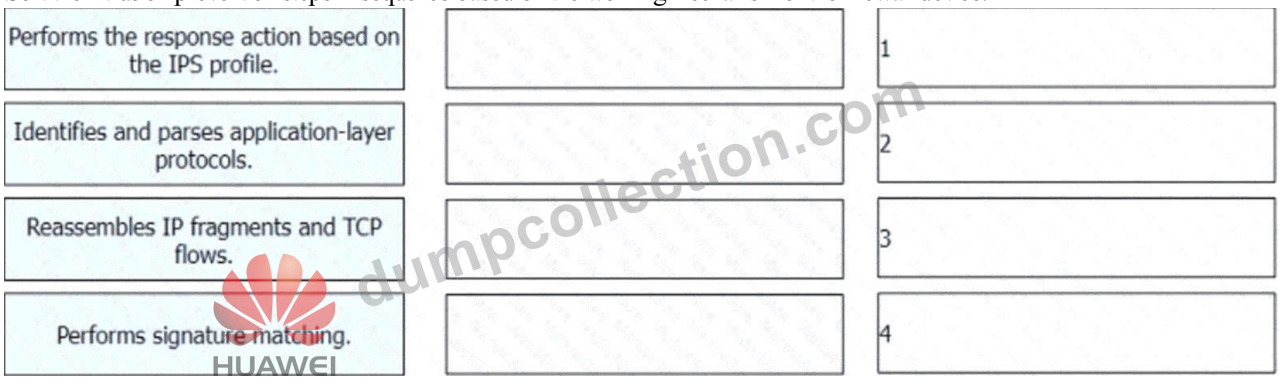
NEW QUESTION # 34
Network Access Control (NAC) is an end-to-end security control technology that works in combination with AAA to implement access authentication. Which of the following statements about NAC and AAA are true?(Select All that Apply)

- A. AAA is mainly used for interaction between users and access devices.
- B. An AAA server controls network access rights of users through authentication, authorization, and accounting.
- C. NAC is mainly used for interaction between access devices and authentication servers.
- D. NAC provides three authentication modes: 802.1X authentication, MAC address authentication, and Portal authentication.

Answer: A,B,C,D

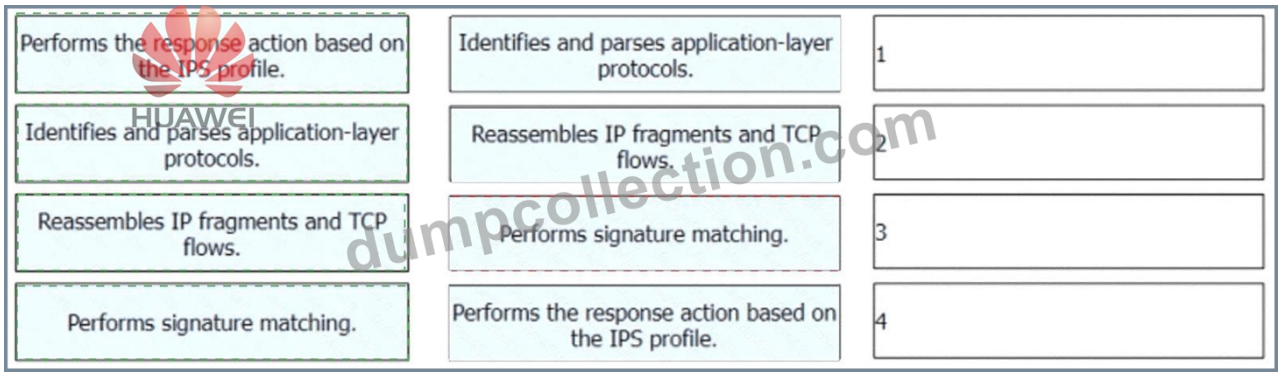
Explanation:
Comprehensive and Detailed Explanation:
* Network Access Control (NAC) and AAA work together for secure network access.
* Key functions:
* A. AAA handles user-to-device authentication.
* B. NAC handles device-to-server authentication.
* C. NAC supports 802.1X, MAC authentication, and Portal authentication.
* D. AAA enforces authentication, authorization, and accounting.
* Why are all options correct?
* Each option correctly describes a function of NAC or AAA.
HCIP-Security References:
* Huawei HCIP-Security Guide # NAC & AAA Integration

NEW QUESTION # 35
Sort the intrusion prevention steps in sequence based on the working mechanism of the firewall device.



Answer:

Explanation:



Explanation:
Intrusion Prevention Systems (IPS) in firewalls follow amulti-step processto detect and mitigate threats. The steps occur in a logical sequence:
1##Step 1: Identifies and Parses Application-Layer Protocols
* The firewall firstidentifies the protocol being used(e.g., HTTP, FTP, DNS, SMTP).
* Parsing the protocol helps the IPS engineunderstand how the data is structuredand what types of attacks might be embedded.
* This step is crucial for detectingprotocol-based attackslike SQL injection or cross-site scripting (XSS).
2##Step 2: Reassembles IP Fragments and TCP Flows
* Attackers oftensplit malicious payloads across multiple packetsto evade detection.
* The firewallreassembles fragmented packets and TCP flowsto reconstruct the full data stream.
* This step is critical for detectingevasion techniques such as fragmented attacks or out-of-order packet attacks.
3##Step 3: Performs Signature Matching
* Once the full data stream is reassembled, the IPScompares it against known attack signatures.
* Signature matching helps detect:
* Malware patterns(e.g., botnets, Trojans).
* Exploits targeting vulnerabilitiesin software and operating systems.
* Firewalls usepredefined signature databasesthat are regularly updated.
4##Step 4: Performs the Response Action Based on the IPS Profile
* If an attack is detected, the firewall takes anaction based on the IPS policy:
* Block the traffic(drop malicious packets).
* Alert the administrator(generate logs and alerts).
* Rate-limit traffic(slow down potential attack sources).
* Theresponse mechanism is customizablebased on security requirements.

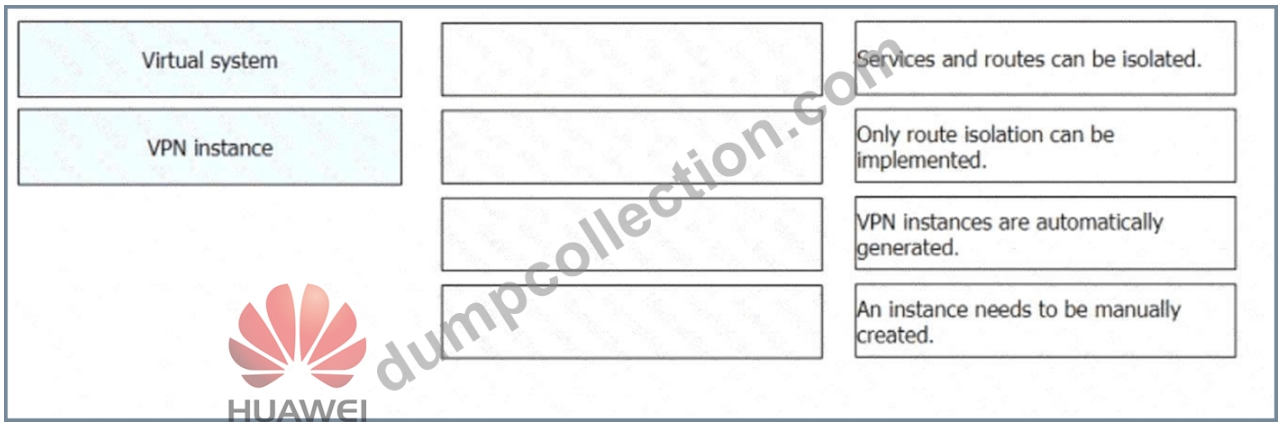
NEW QUESTION # 36
SYN scanning requires a fully established TCP connection and is recorded in system logs.

- A. FALSE
- B. TRUE

Answer: A

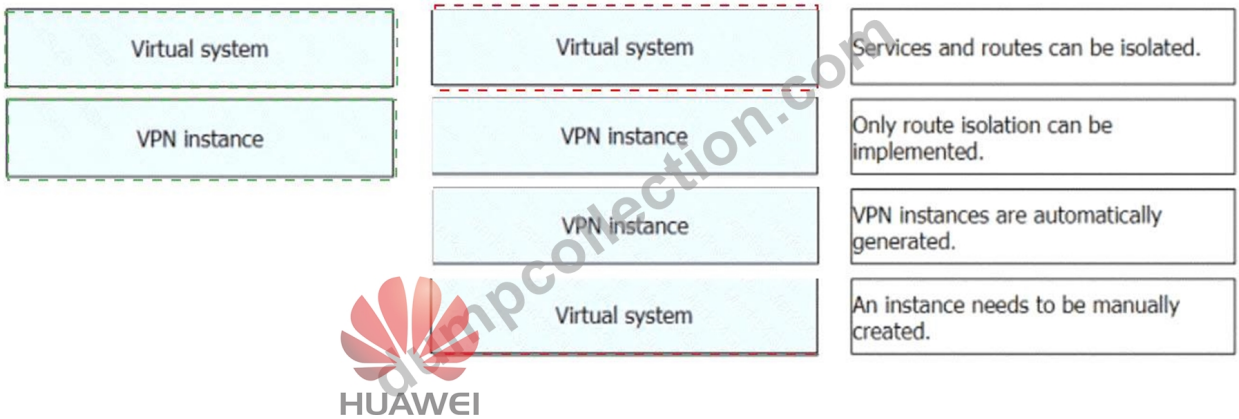
Explanation:
Comprehensive and Detailed Explanation:
* SYN scanning is a stealthy TCP scanning technique used by attackers to detect open ports.
* How SYN scanning works:
* The attacker sends aSYN packetto a target port.
* If the port isopen, the target responds with aSYN-ACK.
* Instead of completing the handshake with anACK, the attacker sends anRST (reset) packet, leaving the connection half-open.
* Why is this statement false?
* SYN scanning does NOT establish a full connection (three-way handshake).
* It may not always be recorded in system logs, depending on firewall settings.
HCIP-Security References:
* Huawei HCIP-Security Guide # TCP SYN Scanning & Intrusion Detection

NEW QUESTION # 37
Match the description about virtual systems and VPN instances.



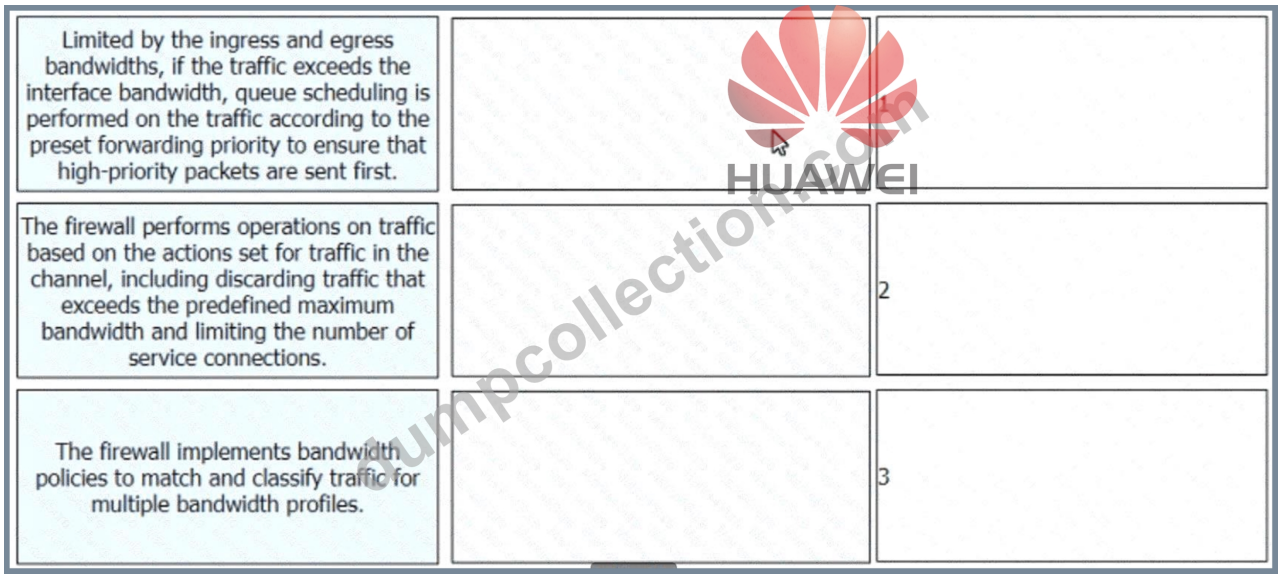
Answer:

Explanation:



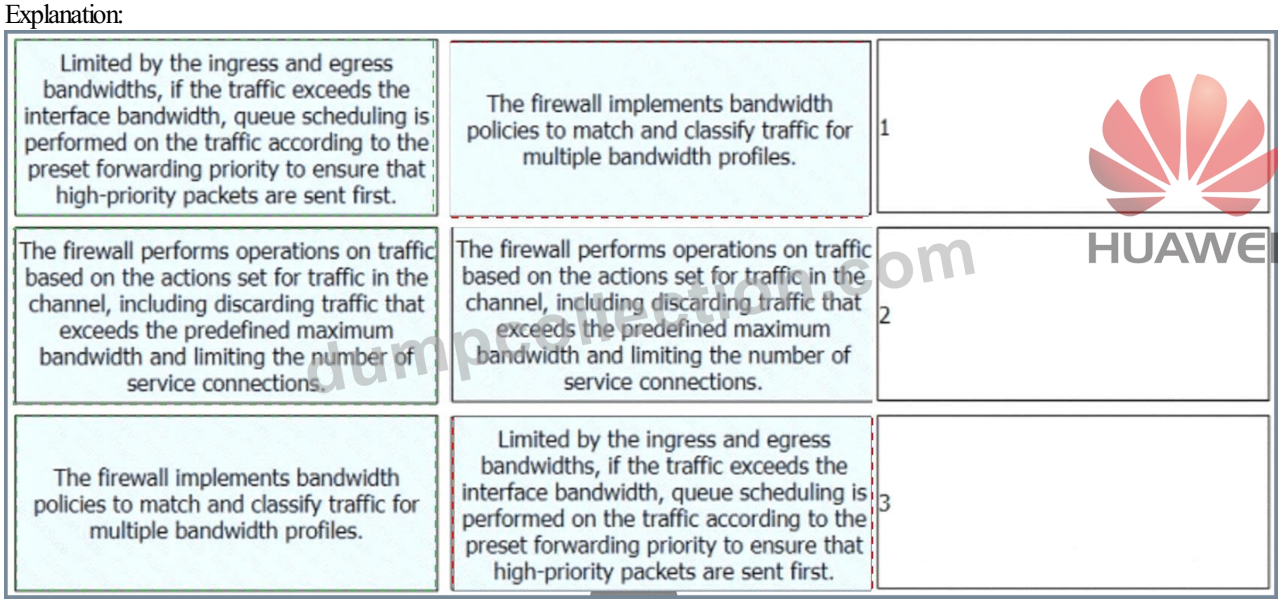
Explanation:
1. Virtual System # Services and routes can be isolated.
* A virtual system (VS)in Huawei firewalls is afully isolated security instancewithin a single physical firewall.
* Each virtual system hasseparate services, routing tables, policies, and security rules, ensuring full isolation between different users or tenants.
2. VPN Instance # Only route isolation can be implemented.
* AVPN instance (VRF - Virtual Routing and Forwarding)providesroute isolationfor different customer networks butdoes not isolate services or security policies.
* This is typically used inMPLS VPN deploymentswhere different customers share the same physical device but need isolated routing tables.
3. VPN Instance # VPN instances are automatically generated.
* In someMPLS VPNorSDN-managed networks, VPN instances can beautomatically createdwhen customer configurations are pushed via controllers.
* Dynamic routing protocols (e.g., BGP/MPLS VPN) can automatically generateVRF instancesbased on network policies.
4. Virtual System # An instance needs to be manually created.
* Unlike VPN instances,virtual systems must be manually createdby an administrator on the firewall.
* Each virtual system functions as acompletely independent firewall, requiring manual configuration of interfaces, policies, and routing settings.

NEW QUESTION # 38
Arrange the steps of the bandwidth management process on firewalls in the correct sequence.



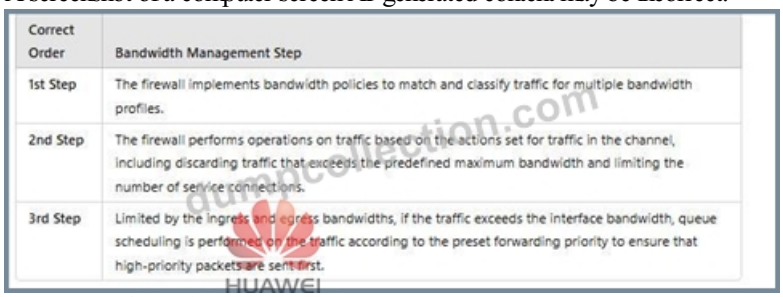
Answer:

Explanation:



Explanation:

A screenshot of a computer screen AI-generated content may be incorrect.



Correct Order	Bandwidth Management Step
1st Step	The firewall implements bandwidth policies to match and classify traffic for multiple bandwidth profiles.
2nd Step	The firewall performs operations on traffic based on the actions set for traffic in the channel, including discarding traffic that exceeds the predefined maximum bandwidth and limiting the number of service connections.
3rd Step	Limited by the ingress and egress bandwidths, if the traffic exceeds the interface bandwidth, queue scheduling is performed on the traffic according to the preset forwarding priority to ensure that high-priority packets are sent first.

HCIP-Security References:

* Huawei HCIP-Security Guide# Bandwidth Management & Traffic Control Policies
* Huawei QoS Configuration Guide# Traffic Classification, Policing, and Queue Scheduling

1##Step 1: Traffic Classification and Bandwidth Policy Matching

* The firewallfirst classifies trafficusing predefined bandwidth policies.
* These policies match traffic based on criteria such assource/destination IP, application type, and protocol.
* This step ensures that each type of traffic is categorized correctly before applying bandwidth restrictions.

2##Step 2: Traffic Processing Based on Bandwidth Policies

* Once traffic is classified,the firewall enforces bandwidth limits and security actions:
* Traffic exceeding the assigned bandwidth is discarded or throttled.
* Service connection limits are enforced to prevent excessive connections per user or application.

3##Step 3: Queue Scheduling and Priority Handling
* If trafficexceeds the available bandwidth, the firewallprioritizes high-priority trafficusing queue scheduling mechanisms.
* Techniques likeWeighted Fair Queuing (WFQ) and Priority Queuing (PQ)ensure thatcritical traffic (e.g., VoIP, business applications) is prioritized over less important traffic (e.g., downloads, streaming).

NEW QUESTION # 39

......