PassQueen
a.k.a dumpsqueen.com

Huawei Certified ICT Professional - Constructing Service Security Network (HCIP-Security-CSSN V3.0)

Huawei H12-722

Version Demo

Total Demo Questions: 23

Total Premium Questions: 237

Buy Premium PDF

https://passqueen.com

support@passqueen.com

QUESTION NO: 1 - (SIMULATION)

The analysis and processing capabilities of traditional firewalls at the application layer are weak, and they cannot correctly analyze malicious codes that are mixed in the flow of allowed application teaching: many Attacks or malicious behaviors often use the firewall's open application data flow to cause damage, causing application layer threats to penetrate the firewall

A True

B. False

ANSWER: Check the explanation for the answer

Explanation:

Answer: A. True

Traditional firewalls primarily perform packet filtering and basic stateful inspection. Their application-layer parsing and content-analysis capability is limited, so malicious code or attacks hidden within permitted application traffic (such as HTTP/HTTPS or email traffic) can pass through an allowed firewall policy and attack internal systems.

This limitation is one reason NGFWs provide deeper application identification, intrusion prevention, antivirus, and content-security inspection.

QUESTION NO: 2

The user needs of a university are as follows:

1. The environment is large, and the total number of two-way traffic can reach 800M. Huawei USG6000 series firewall is deployed at its network node.

2. The intranet is divided into student area, server area, etc., users are most concerned about the security of the server area to avoid attacks from various threats.

3. At the same time, some pornographic websites in the student area are prohibited.

The external network has been configured as an untrust zone and the internal network has been configured as a trust zone on the firewall. How to configure the firewall to meet the above requirements?

155955cc-666171a2-20fac832-0c042c0415

A. You can directly turn on the AV, IRS protection functions, and URL filtering functions in the global environment to achieve the requirements

B. To the untrust direction, only enable AV and IPS protection functions for the server zone to protect the server

C. In the direction of untrust to the intranet, only the AV and IPS protection functions are turned on for the server area to protect the server

D. Go to the untrust direction to open the URL filtering function for the entire campus network, and filter some classified websites

ANSWER: C D

Explanation:

“In the direction of untrust to the intranet, only the AV and IPS protection functions are turned on for the server area to protect the server” is appropriate because traffic initiated from the Internet toward published or reachable server resources is the principal threat path for the server zone. A security policy matching the Untrust source zone and the server-area destination should have antivirus and intrusion-prevention profiles applied, allowing the firewall to inspect permitted traffic

and block malware or exploit activity before it reaches servers. This targeted deployment also avoids unnecessarily applying resource-intensive inspection to unrelated internal flows, an important consideration for an environment with substantial bidirectional traffic.

“Go to the untrust direction to open the URL filtering function for the entire campus network, and filter some classified websites” addresses the outbound web-access requirement. URL filtering is applied to security policies for traffic leaving the trusted campus network toward Untrust, using URL categories to block prohibited content such as pornography. In implementation, the policy can be further scoped by source address or user group to the student area when that granularity is required. Huawei next-generation firewalls support integrated antivirus, IPS, and URL-filtering capabilities as content-security functions; see the Huawei Next-Generation Firewall overview and Huawei firewall documentation.

QUESTION NO: 3

The following commands are configured on the Huawei firewall:

[USG] firewall defend ip-fragment enable

Which of the following situations will be recorded as an offensive behavior? (multiple choice)

A. DF bit is 1, and (MF bit is 1 or Fragment Offset is not 0).

B. DF bit is 0, and MF bit is 1 or Fragment Offset is not 0.

C. DF bit is 0, and Fragment Offset + Length> 65535.

D. The DF bit is 1, and Fragment Ofset + Length <65535.

ANSWER: A C

Explanation:

The IP-fragment defense feature examines whether IPv4 fragmentation-related header fields are logically consistent. “DF bit is 1, and (MF bit is 1 or Fragment Offset is not 0)” is an attack signature because DF (Don’t Fragment) instructs that the packet must not be fragmented. Consequently, a packet claiming DF is set while also declaring that more fragments follow (MF set) or that it is positioned after the beginning of a fragmented datagram (a nonzero Fragment Offset) contains contradictory fragmentation information. Such malformed headers can be used to evade security inspection or trigger inconsistent packet reassembly behavior, so the firewall records them as offensive traffic when IP-fragment defense is enabled.

“DF bit is 0, and Fragment Offset + Length > 65535” is also an offensive condition because the total reassembled IPv4 datagram would exceed the maximum IPv4 total-length field value of 65,535 bytes. This is an invalid fragment sequence and is a classic oversized-fragment or reassembly-evasion pattern. Huawei firewall documentation is available through the Huawei Enterprise documentation portal; the IPv4 fragmentation fields and the 65,535-byte datagram limit are defined in RFC 791.

QUESTION NO: 4

Regarding the file filtering technology in the USG6000 product, which of the following options is wrong?

A. It can identify the application that carries the file, the file transfer direction, the file type and the file extension.

B. Even if the file type is modified, it can also identify the true type of the file

C. It can identify the type of files transmitted by itself, and can block, alert and allow specific types of files.

D. It supports filtering the contents of compressed files after decompression.

ANSWER: D

Explanation:

“It supports filtering the contents of compressed files after decompression.” is the incorrect statement. On USG6000 firewalls, file filtering identifies and controls transferred files using metadata and characteristics available during protocol inspection, such as the transfer protocol/application, direction, filename extension, and the file’s actual type. The feature is intended to apply a configured file-filtering profile to traffic matched by a security policy, allowing the firewall to take the configured control action for the detected file type.

Compressed archives are a distinct inspection boundary: file filtering does not provide a general-purpose archive extraction capability that decompresses an archive and recursively filters its internal contents. Therefore, a policy cannot rely on file filtering to inspect every file contained inside a compressed package after decompression. This distinction is important when designing controls for archived or password-protected content; additional endpoint protection and malware-detection measures should be used where inspection of archive contents is required. Huawei’s security product information and documentation resources are available through the Huawei Firewall product page and the Huawei Enterprise Support documentation portal.

QUESTION NO: 5

Regarding the description of file reputation technology in anti-virus engines, which of the following options is correct?

A. Local reputation MD5 cache only has static cache, which needs to be updated regularly

B. File reputation database can only be upgraded by manual upgrade

C. File reputation is to perform virus detection by calculating the full text MD5 of the file to be tested and matching it with the local reputation MD5 cache

D. File reputation database update and upgrade can only be achieved through linkage with sandbox

ANSWER: C

Explanation:

File reputation is to perform virus detection by calculating the full text MD5 of the file to be tested and matching it with the local reputation MD5 cache. In this mechanism, the anti-virus engine calculates a deterministic MD5 digest for the complete file and uses that digest as an identifier for a reputation lookup. If the digest is found in the locally stored reputation cache, the engine can rapidly apply the reputation verdict associated with that exact file, such as a known malicious or trusted classification. This provides a fast first-stage detection path because it avoids immediately performing more resource-intensive content analysis for files whose identity and reputation are already known.

The wording “full text MD5” means that the hash is calculated from the entire file content, rather than from only a file name, extension, path, or partial content. MD5 is being used here as a file-fingerprint lookup value; its cryptographic collision limitations do not change the basic operation of a reputation-cache match. Huawei endpoint security solutions incorporate reputation and threat-intelligence capabilities as part of endpoint malware defense. See Huawei’s HiSec Endpoint overview and the MD5 algorithm definition in RFC 1321.

QUESTION NO: 6

The analysis and processing capabilities of traditional firewalls at the application layer are weak, and they cannot correctly analyze malicious codes that are mixed in the flow of allowed application teaching: many Attacks or malicious behaviors often use the firewall's open application data flow to cause damage, causing application layer threats to penetrate the firewall

A. True

B. False

ANSWER: A

Explanation:

True is correct. Traditional firewalls primarily enforce access-control policies using network and transport-layer properties such as source and destination addresses, ports, protocols, and connection state. This control is valuable for limiting

unauthorized connectivity, but it does not inherently establish whether content carried in a permitted application session is safe. Consequently, an attacker can deliver malicious payloads, exploit application vulnerabilities, or issue harmful requests through traffic that matches an allowed policy. For example, permitting web access or email delivery based on the required service ports does not by itself ensure that the exchanged files, requests, or embedded content are benign.

Effective protection against this class of risk requires security inspection that understands application protocols and examines content and behavior within allowed traffic. Huawei next-generation firewall capabilities include application identification and control, intrusion prevention, antivirus inspection, and other content-security functions intended to identify threats beyond basic port-and-protocol filtering. Huawei describes these capabilities in its Firewall Security Configuration Guide, while the broader role of application-aware inspection is outlined in Huawei's Next-Generation Firewall product information. Therefore, the statement accurately identifies a fundamental limitation of traditional firewall filtering when application-layer threats travel inside permitted data flows.

QUESTION NO: 7

Regarding intrusion detection I defense equipment, which of the following statements are correct? (multiple choice)

A. It cannot effectively prevent the virus from spreading from the Internet to the intranet.

B. The number of applications that NIP6000 can recognize reaches 6000+, which realizes refined application protection, saves export bandwidth, and guarantees key business services

Experience.

C. Protect the intranet from external attacks, and inhibit malicious flows, such as spyware, worms, etc. from flooding and spreading to the intranet.

D. Ability to quickly adapt to threat changes

ANSWER: B C D

Explanation:

Intrusion detection and prevention equipment is deployed at network boundaries and critical internal points to inspect traffic, identify malicious behavior, and enforce protective actions based on signatures, protocols, applications, reputation, and behavioral analysis. Therefore, "The number of applications that NIP6000 can recognize reaches 6000+, which realizes refined application protection, saves export bandwidth, and guarantees key business services

Experience.

" describes the purpose of application-aware security controls: recognizing applications enables granular policy enforcement and prioritization of important services. "Protect the intranet from external attacks, and inhibit malicious flows, such as spyware, worms, etc. from flooding and spreading to the intranet.

" is also correct because an IPS can detect and block exploit traffic and malware propagation attempts before they enter or traverse protected network segments. Finally, "Ability to quickly adapt to threat changes

" reflects a core operational requirement for modern IPS platforms: threat signatures, intelligence, and detection policies must be updated and adjusted as attacks evolve. NIST describes intrusion prevention systems as technologies that monitor events and can attempt to stop detected incidents, including by dropping malicious packets or terminating connections. See NIST SP 800-94: Guide to Intrusion Detection and Prevention Systems and Huawei's Enterprise Support portal for product documentation and security update resources.

QUESTION NO: 8

In the penetration stage of an APT attack, which of the following attack behaviors will the attacker generally have?

A. Long-term latency and collection of key data.

B. Leak the acquired key data information to a third party of interest

C. Through phishing emails, attachments with 0day vulnerabilities are carried, causing the user's terminal to become a springboard for attacks.

D. The attacker sends a C&C attack or other remote commands to the infected host to spread the attack horizontally on the intranet.

ANSWER: C

Explanation:

Through phishing emails, attachments with 0day vulnerabilities are carried, causing the user's terminal to become a springboard for attacks. This describes the initial-access and exploitation activity that characterizes the penetration stage of an advanced persistent threat. Attackers commonly craft convincing spear-phishing messages and deliver a malicious attachment or link to a targeted user. When the attachment exploits an unknown or unpatched vulnerability, or persuades the recipient to execute malicious content, the endpoint can be compromised and malware can establish an initial foothold. That compromised terminal then provides the attacker with an entry point from which later APT activities can be conducted, such as maintaining access, expanding through the environment, and accessing target resources. Huawei's security guidance identifies phishing as a significant delivery method for targeted threats and emphasizes endpoint and email protections to prevent such initial compromise. MITRE ATT&CK likewise documents spearphishing attachments as an Initial Access technique and exploitation for client execution as a means of obtaining code execution on a victim system. See MITRE ATT&CK: Spearphishing Attachment and MITRE ATT&CK: Exploitation for Client Execution.

QUESTION NO: 9

If the user's FTP operation matches the FTP filtering policy, what actions can be performed? (multiple choice)

A. Block

B. Declare

C. Alarm

D. Execution

ANSWER: A C

Explanation:

When a user's FTP operation matches an FTP filtering policy, the relevant enforcement actions are **Block** and **Alarm**. Blocking is the active protection action: the terminal-security or security gateway policy prevents the matched FTP operation from proceeding, helping enforce restrictions on file-transfer behavior defined by the organization. This is important because FTP operations can involve transferring files to or from protected systems and therefore may need to be stopped when they violate the configured control policy.

Alarm is the visibility and response action. It generates a security event for a matched operation so that administrators can identify the user activity, investigate the context, and respond according to the organization's incident-handling process. An alarm provides the operational record needed for monitoring and audit workflows, while blocking provides immediate policy enforcement. These actions can be selected together where the desired outcome is both to stop the prohibited FTP activity and to notify security operations personnel. Huawei's enterprise support and documentation portal provides product documentation and security-configuration guidance at Huawei Enterprise Support. Additional Huawei security documentation resources are available through the Huawei documentation portal.

QUESTION NO: 10

What are the typical technologies of anti-virus engines (multiple choice)

A. First package detection technology

B. Heuristic detection technology

C. Decryption technology

D. File reputation detection technology 5

ANSWER: A B D

Explanation:

Typical antivirus engines combine several complementary detection approaches so that both known and previously unseen threats can be identified. First package detection technology supports rapid inspection early in traffic or file transmission, enabling the security device to recognize known malicious content as soon as sufficient identifying data is available. This reduces the time before a threat can be blocked.

Heuristic detection technology evaluates suspicious code structures, instruction patterns, and other characteristics associated with malware. It is therefore useful when a sample does not exactly match an existing signature but exhibits features that indicate malicious intent. File reputation detection technology adds intelligence based on the known trustworthiness of a file, such as information derived from threat-intelligence or cloud-reputation sources. A malicious or low-reputation file can consequently be identified even when conventional local matching alone is insufficient.

Used together, these techniques provide layered detection coverage for known malware, variants, and suspicious files. Huawei's next-generation firewall portfolio includes antivirus and threat-intelligence capabilities for detecting and blocking malware, while NIST describes the importance of layered malware detection and response controls. See Huawei Firewall and NIST SP 800-83 Rev. 1.

QUESTION NO: 11

Fage attack means that the original address and target address of TOP are both set to the IP address of a certain victim. This behavior will cause the victim to report to it.

SYN-ACK message is sent from the address, and this address sends back an ACK message and creates an empty connection, which causes the system resource board to occupy or target

The host crashed.

A. True

B. False

ANSWER: A

Explanation:

The statement is true: the behavior described is the classic LAND (Local Area Network Denial) attack. In a LAND attack, an attacker crafts a TCP SYN packet whose source IP address and destination IP address are both the victim's address, usually also using the same source and destination port. The victim's TCP/IP stack treats the packet as a connection request and may send a SYN-ACK response to its own address. On vulnerable implementations, processing these self-referential packets can create invalid or incomplete connection state, consume CPU time and connection-table resources, or trigger instability. Repeated packets can therefore result in denial of service, including severe degradation or a host crash on systems lacking appropriate validation and attack protection.

The description's references to a SYN-ACK being sent to the victim's own address and the resulting abnormal connection state match the defining mechanism of LAND attacks. Modern firewalls and hosts commonly detect and discard packets with suspicious identical source and destination endpoint values, but this does not alter the classification of the attack described. MITRE documents this pattern as a denial-of-service technique in CAPEC-220: Client-Server Protocol Manipulation; TCP connection establishment behavior is specified in RFC 793.

QUESTION NO: 12

In the anti-virus policy configuration of Huawei USG6000 product, what are the response methods of HTTP protocol? (multiple choice)

A. Warning

B. Block and push the page

C. A warning dialog box pops up

D. All access to the client is prohibited

ANSWER: A B

Explanation:

For HTTP traffic, Huawei USG6000 antivirus policy processing supports the response methods **Warning** and **Block and push the page**. Warning allows the firewall to detect and record the virus event while generating an alert, which provides visibility for administrators and supports monitoring-oriented security policies. Block and push the page actively prevents the malicious HTTP content from being delivered and returns a replacement notification page to the user's browser. This browser-facing response is specifically practical for HTTP because the firewall can inject or redirect to an informational page within the HTTP exchange, helping users understand that access was stopped by the security policy. These actions are selected as part of the antivirus profile/policy behavior after the device identifies malicious content using its antivirus signature database and inspection engine. Huawei's USG firewall documentation describes antivirus as a content-security function that detects malicious files or traffic and applies configured actions to matched events. See the Huawei USG6000 Series product documentation and Huawei's Enterprise Support portal for the applicable configuration guides and version-specific antivirus policy details.

QUESTION NO: 13

Regarding the principle of least privilege for enterprise terminal accounts, which of the following statements are correct? (multiple choice)

A. Assign ordinary users standard user permissions whenever possible

B. Use separate administrative accounts for privileged operations

C. Grant temporary elevated privileges only for approved tasks

D. Periodically review and remove unnecessary permissions

E. Assign local administrator rights to all users for convenience

ANSWER: A B C D

Explanation:

Least privilege requires users, processes, and services to receive only the permissions necessary to perform their assigned tasks. Therefore, assigning ordinary users standard user permissions rather than local administrator permissions is correct. Separating administrative accounts from daily office accounts is also correct because it reduces exposure of privileged credentials during normal browsing, email, and document operations.

Granting temporary privileged access only when an approved task requires it is consistent with least privilege, particularly when the access is logged and removed after the task is completed. Reviewing and removing unnecessary permissions is also required because users can accumulate access rights after role changes. Assigning local administrator rights to all users for convenience is incorrect because it greatly increases the impact of malware execution and accidental configuration changes.

NIST describes least privilege as restricting access to the minimum necessary for authorized functions. See NIST Least Privilege.

QUESTION NO: 14

Regarding worms and viruses, which of the following statements is correct?

A. Worms exist in a parasitic way

155955cc-666171a2-20fac832-0c042c0413

B. Viruses mainly rely on system vulnerabilities to spread

C. The target of the worm infection is other computer systems on the network.

D. The virus exists independently in the computer system.

ANSWER: C

Explanation:

The target of the worm infection is other computer systems on the network. This is correct because a computer worm is malware designed to make copies of itself and propagate from an infected host to additional hosts, commonly through network services, shared resources, email mechanisms, or other communication paths. Its propagation objective is therefore inherently network-oriented: it seeks reachable systems that can become new infected hosts and continue the spread. This behavior can cause rapid, large-scale impact because each newly compromised system may scan for and infect further systems. Effective terminal-security controls consequently include timely vulnerability remediation, host firewalls, network segmentation, endpoint anti-malware protection, and monitoring for anomalous scanning or connection activity. CISA describes worms as self-replicating malware that spreads across networks without requiring user action, while NIST's glossary similarly identifies a worm as a self-propagating program that spreads over a network. These definitions directly support the statement's focus on other computer systems on the network as the target of worm infection. See CISA: Understanding Malware and NIST CSRC Glossary: Worm.

QUESTION NO: 15

Which of the following options belong to the keyword matching mode? (multiple choice)

A. Text

B. Regular expressions

C. Community word

D. Custom keywords

ANSWER: A B

Explanation:

Text and Regular expressions are keyword matching modes. Text matching is used when a security policy needs to identify a specific, fixed character string in monitored content. It is appropriate for stable terms such as a project name, an internal identifier, or a defined sensitive phrase. Regular-expression matching provides pattern-based identification, allowing one rule to recognize multiple content variants that follow the same format. This is useful where the protected information has a recognizable structure, such as an account-like identifier, document number, or a string with variable characters. Together, these modes allow terminal security and data-protection policies to balance precise literal matching with flexible structured-pattern detection. When implementing regular expressions, administrators should validate expressions against representative data and use sufficiently specific patterns to maintain reliable detection performance. Huawei enterprise support documentation is available through the Huawei Enterprise Support portal; Huawei security-product documentation and related configuration resources can also be located through the Huawei Enterprise documentation library.

QUESTION NO: 16

Regarding HTTP behavior, which of the following statements is wrong?

A. HTTP POST is generally used to send information to the server through a web page, such as forum posting x form submission, username I password login.

B. When the file upload operation is allowed, the alarm threshold and blocking threshold can be configured to control the size of the uploaded file.

C. When the size of the uploaded or downloaded file and the size of the content of the POST operation reach the alarm threshold, the system will generate log information to prompt the device management

And block behavior.

D. When the uploaded or downloaded file size, POST operation content size reaches the blocking threshold, the system will only block the uploaded or downloaded file, POST

operate.

ANSWER: C

Explanation:

The statement “When the size of the uploaded or downloaded file and the size of the content of the POST operation reach the alarm threshold, the system will generate log information to prompt the device management And block behavior.” is wrong because an alarm threshold is intended to provide monitoring and notification, rather than enforcement. In Huawei firewall HTTP-content control behavior, the alarm threshold is used to generate a log when the configured size is reached, allowing administrators to identify unusually large HTTP uploads, downloads, or POST request bodies and investigate them. Blocking is associated with the separately configured blocking threshold, which is the enforcement limit for the relevant HTTP transfer or POST operation. This separation allows a security administrator to set an earlier warning level before traffic reaches the level at which the device must deny it. HTTP POST is an HTTP request method that submits content to a server, so POST body size is an appropriate object for this type of inspection and threshold control. The relevant HTTP request semantics are defined in RFC 9110: HTTP Semantics. Huawei Enterprise technical documentation and product configuration resources are available through the Huawei Enterprise Support documentation portal.

QUESTION NO: 17

Which of the following options belong to the upgrade method of the anti-virus signature database of Huawei USG6000 products? (multiple choice)

A. Local upgrade

B. Manual upgrade

C. Online upgrade

D. Automatic upgrade

ANSWER: A C

Explanation:

Huawei USG6000 firewalls support two principal ways to obtain and install anti-virus signature databases: **Local upgrade** and **Online upgrade**. A local upgrade is used when an administrator obtains the signature-database package separately, such as from Huawei’s support portal, and uploads it to the firewall for installation. This is particularly useful in isolated, restricted, or otherwise offline network environments where the firewall cannot access Huawei’s update servers directly.

An online upgrade allows the firewall to contact the configured Huawei update service and download the current anti-virus signature database through the network. This method keeps terminal and network malware detection aligned with the latest threat intelligence and is the normal approach when the device has appropriate Internet access, routing, DNS, and licensing/entitlement conditions. Huawei documentation groups anti-virus signature-database updates under these local and online acquisition methods; scheduling or initiating an online retrieval describes operational handling of the online method rather than a separate database-upgrade category. See Huawei’s USG6000 documentation search and the Huawei signature-database upgrade documentation search.

QUESTION NO: 18

Which of the following options is not a feature of big data technology?

A. The data boy is huge

B. A wide variety of data

C. Low value density

D. Slow processing speed

ANSWER: D

Explanation:

“Slow processing speed” is the correct choice because big data technology is designed to process and analyze large-scale, diverse, rapidly generated data efficiently, rather than to make processing slow. A commonly used model describes big data through characteristics such as volume, variety, velocity, and value. “Velocity” specifically concerns the speed at which data is generated, transmitted, and must be handled; modern big-data platforms address this requirement through distributed storage, parallel computing, stream processing, and scalable compute resources. In practice, technologies such as Hadoop and Spark divide data and computation across multiple nodes so that workloads can be completed more quickly than would be possible on one system. Therefore, fast or scalable processing capability is a central objective of big-data technology, particularly where organizations need timely analytics from continually arriving data. Huawei’s data-intelligence and cloud big-data services likewise emphasize elastic, distributed processing for large volumes of data. Additional background on the standard characteristics and processing approach for big data is available from IBM’s Big Data overview and the Apache Hadoop project.

QUESTION NO: 19

Analysis is the core function of intrusion detection. The analysis and processing process of intrusion detection can be divided into three phases; build an analyzer to perform analysis on actual field data.

Which of the analysis, feedback and refinement is the function included in the first two stages?

A. Data analysis, data classification, post-processing

B. Data processing, data classification, post-processing

C. Data processing, attack classification, post-processing

D. Data processing, data classification, attack playback

ANSWER: B

Explanation:

Data processing, data classification, post-processing is correct because intrusion-detection analysis normally turns raw observations into useful security results through a structured pipeline. First, collected field data must be processed: this commonly includes parsing records, normalizing formats, removing unusable content, and extracting relevant features from traffic, host, or log events. The next essential function is classification, in which the analyzer uses signatures, rules, behavioral baselines, or statistical methods to categorize the processed events and identify likely attack-related activity. Post-processing then supports the outcome of analysis by correlating findings, prioritizing or aggregating alerts, recording results, and supplying feedback that can improve future detection logic. This model enables an analyzer to work consistently with large volumes of heterogeneous real-world security data while producing actionable intrusion-detection output. NIST’s intrusion-detection guidance describes the importance of analyzing monitored events and generating alerts from identified suspicious activity; see NIST SP 800-94, Guide to Intrusion Detection and Prevention Systems. The broader incident-handling lifecycle also emphasizes analysis and feedback-driven improvement, as documented in NIST SP 800-61 Rev. 2.

QUESTION NO: 20

Which of the following files can the sandbox detect? (multiple choice)

A. www file

B. PE file

C. Picture file

D. Mail

ANSWER: A B C

Explanation:

Sandbox analysis is intended to identify malicious behavior concealed in multiple file and content types, rather than being limited to traditional executable programs. A web file can be submitted or accessed for dynamic inspection because malicious web content may contain exploit code, malicious scripts, drive-by-download behavior, or links that trigger subsequent payload delivery. A PE file is a core sandbox-analysis target: Portable Executable content, including Windows executable programs and libraries, can be run in an isolated virtual environment so the system can observe behaviors such as process creation, file modification, persistence activity, and network communication.

Picture file inspection is also supported in the broader sandboxing workflow. Image-format files can be used to carry malformed content or exploit payloads aimed at vulnerabilities in image parsers and viewing software. Dynamic detection helps identify suspicious actions that become visible only when the content is opened or processed in an isolated environment. Huawei describes its security-analysis capabilities as combining threat detection with behavioral analysis, including advanced-threat inspection. See Huawei's enterprise security portfolio and Huawei Cloud's sandbox detection documentation for product and feature context.

QUESTION NO: 21

Regarding traditional firewalls, which of the following statements are correct? (multiple choice)

A. Lack of effective protection against application layer threats.

B. It cannot effectively resist the spread of viruses from the Internet to the intranet.

C. Ability to quickly adapt to changes in threats.

D. Unable to accurately control various applications, such as P2P, online games, etc. .

ANSWER: A B D

Explanation:

Traditional firewalls primarily make access-control decisions from network and transport-layer characteristics, such as source and destination addresses, protocols, ports, and connection state. Therefore, **"Lack of effective protection against application layer threats."** is correct: traffic that uses permitted ports can still contain threats that require application-aware inspection and security services. **"It cannot effectively resist the spread of viruses from the Internet to the intranet."** is also correct because conventional firewall policy enforcement alone does not provide the content inspection, anti-malware detection, and threat intelligence needed to identify many malicious files and payloads entering through authorized services. Finally, **"Unable to accurately control various applications, such as P2P, online games, etc. ."** is correct because these applications may use dynamic ports, port hopping, tunneling, or common protocols, making port-based rules insufficient for precise identification and control. Next-generation firewall capabilities address these limitations through application awareness, intrusion prevention, antivirus, and other deep-inspection features. Huawei describes its firewall portfolio as providing application-level visibility and integrated threat defense: Huawei Firewall. The need for inspection beyond basic packet filtering is also consistent with NIST guidance on firewall technologies: NIST SP 800-41 Rev. 1.

QUESTION NO: 22

Which of the following types of attacks are DDoS attacks? 2I

A. Single packet attack

B. Flood attack

C. Malformed message attack

D. Snooping scan attack

ANSWER: B

Explanation:

Flood attack is the correct answer. A DDoS attack uses many distributed sources—commonly compromised hosts in a botnet—to send a very large volume of traffic or requests to a target. The goal is to consume available bandwidth, forwarding capacity, connection-table entries, CPU resources, or application-processing capacity so that legitimate users cannot obtain normal service. Flooding is therefore a core DDoS technique and can use protocols such as TCP, UDP, ICMP, DNS, or HTTP, depending on the target and attack layer. The distributed nature of the sources makes filtering and tracing more difficult than for a single-origin denial-of-service event, because traffic can arrive from numerous addresses and networks simultaneously. Huawei anti-DDoS guidance identifies traffic flooding as a major protection scenario and describes detection and mitigation mechanisms designed to recognize abnormal traffic volumes and protect services. See Huawei's Anti-DDoS documentation and the CISA overview of denial-of-service attacks.

QUESTION NO: 23

The virus signature database on the device needs to be continuously upgraded from the security center platform. Which of the following is the website of the security center platform?

A. sec. huawei. com.

B. support.huaver: com

C. www. huawei. com

D. security.. huawei. com

ANSWER: A

Explanation:

The correct security center address is **sec.huawei.com**, represented in the option text as "sec. huawei. com." Huawei security devices can use the Huawei security center as the source for ongoing antivirus signature-database updates. These signature packages contain the latest malware-identification information, allowing the device's antivirus engine to recognize newly discovered threats without waiting for a full software release or manual local-file import.

For this update mechanism to work, the device must be able to resolve and reach the security-center domain through its configured management or service path. In an enterprise deployment, administrators should also ensure that DNS, routing, firewall policy, proxy settings where applicable, and the device clock are correctly configured so that scheduled signature retrieval and package validation can complete successfully. The security center is specifically intended for Huawei security intelligence and update services, making **sec.huawei.com** the appropriate platform address for continuous virus-signature upgrades. Huawei security-related resources and advisories are available through the Huawei Security Center and the Huawei Enterprise Support portal.