Number: H12-731_V2.0
Passing Score: 800
Time Limit: 120
File Version: 4.0

Exam Code: H12-731_V2.0
Exam Name: HCIE-Security (Written) V2.0

Exam A

QUESTION 1
Which of the following types of journals cannot use the Netflow format? (single selection).

A. URL session logs
B. Half-connection session logs
C. IPV6NAT64 SESSION LOGS
D. IPV4 SESSION LOGS

Correct Answer: A
Section:

QUESTION 2
The following describes user authentication Which ones are correct? (multiple selection).

A. Users whose security policies are allowed but whose identity authentication is not passed cannot access resources normally
B. If the user is a MAC address single-item bound user Other users can also use this MAC address to log in normally.
C. Users with two-way iP/MAC binding can obtain dynamic IP address o through DHCP
D. Configure two-way binding of MAC addresses for a user to be exempt from authentication? If there are three layers of device elbows between the user and FW, the user can go online normally

Correct Answer: A, B
Section:

QUESTION 3
One of the reasons why traditional passive defense does not protect against APT attacks is that traditional defense methods cannot correlate and analyze threats.

A. TRUE
B. FALSE

Correct Answer: A
Section:

QUESTION 4
Which of the following options are part of the Internet Behavior? (multiple selection).

A. Keywords that users search for using search engines
B. Sending and receiving emails
C. User QQ account and its online and offline time
D. User profiles

Correct Answer: A, B, C
Section:

QUESTION 5
Which of the following describes the business process of the network trapping scheme wrong?
(single selection).

A. The attacker initiates a network scanning attack The purpose is to probe the network structure.
B. The business that the attacker eventually attacks is a deliberately constructed counterfeit food business. Therefore, all the actions of the attacker are monitored and reported to the CIS platform
C. When the access traffic reaches the trapping probe A collision between the probe needle and the trap will be used to send the access flow to the trap
D. Trapping probes can analyze the frequency of scanning different destination IPs or ports for the same source address Then a virtual MAC responds to the attacker.

Correct Answer: B
Section:

QUESTION 6
The following is a description of FW's audit conduct. Which one is correct? (single selection).

A. After you create or modify an audit profile , the configuration content takes effect immediately.
B. By default , the audit function of outgoing file content is enabled by default.
C. By default HTTP status code audit mode is the default mode Only common HTTP status codes areaudited.

Correct Answer: C
Section:

QUESTION 7
Which of the following situational aware detection attacks can DDOS attacks, firewall bypasses, and malware outreach attacks know? (multiple selection).

A. C&C anomaly detection
B. Hidden channel detection
C. Encrypted traffic detection
D. Meteor base rod anomaly detection

Correct Answer: A, B, C, D
Section:

QUESTION 8
When Hisec Insight is linked with terminals, it is mainly linked with the EDR of third-party vendors with cooperative relationships.

A. TRUE
B. FALSE

Correct Answer: A
Section:

QUESTION 9
Regarding situational awareness, is the following description correct?

A. Perception of elements in the environment
B. Rationale for the current situation

C. A projection of a longer period of time in the future
D. Perception of elements in a temporal and spatial environment An understanding of their meaning, and a projection of their later state

Correct Answer: D
Section:

QUESTION 10
The main role of the audit system is to audit security events after the fact To provide sufficient evidence, a security audit product must have which of the following features7

A. Protect the security of user communications and the integrity of data, and prevent malicious users from intercepting and tampering with data It can fully protect users from malicious damage during operation
B. It can provide fine-grained access control to maximize the security of user resources
C. It provides centralized management of all server and network device accounts, which can complete the monitoring and management of the entire life cycle of the account
D. It can automatically display the user's operation process and monitor the user's every behavior Determine whether the user's behavior poses a danger to the internal network security of the enterprise

Correct Answer: D
Section:

QUESTION 11
On the principle of defense against trapping Which of the following is described as incorrect=

A. By deceiving network detection activities, fake resources are displayed, so that attackers cannot discover real system information and vulnerabilities
B. Interact with the attack campaign to confirm the intent and discover the attacker before the breach occurs
C. Trapping systems discover and block attacker attacks
D. Interference Attack Gathering System Information diaphragmatic weakness determination" process, inducing the attacker to expose the intention

Correct Answer: C
Section:

QUESTION 12
Which of the following does HiSec Insight's big data processing not include?

A. Data preprocessing
B. Flow data collection
C. Distributed storage
D. Distributed indexes

Correct Answer: B
Section:

QUESTION 13
Multi-factor authentication is mainly used in scenarios of login protection and operation protection.

A. TRUE
B. FALSE

Correct Answer: A
Section:

QUESTION 14
When there is a large amount of data (such as photos, videos or database files, etc.) that need to be added and unsealed, the user can encrypt and decrypt the data by encrypting the data with the number of watermarks, and the data can be encrypted and decrypted without transmitting a large amount of data over the network

A. TRUE
B. FALSE

Correct Answer: B
Section:

QUESTION 15
Which of the following features can be used for operation auditing of HUAWEI CLOUD bastion hosts?

A. report analysis
B. Double License
C. Work order management
D. Action playback

Correct Answer: A, C, D
Section:

QUESTION 16
When a user terminates the use of HUAWEI CLOUD services, as a service provider, we should ensure the security of user data operations.

A. Transmission security
B. Storage security
C. Destroy security
D. Collect security

Correct Answer: C
Section:

QUESTION 17
After you deploy HUAWEI CLOUD WAF Traffic to the tenant's Neb server is sent directly to the origin server Cloud WAF intercepts and detects traffic whose destination IP address is the IP address of the origin server.

A. TRUE
B. FALSE

Correct Answer: B
Section:

QUESTION 18
Which of the following services are security management services in HUAWEI CLOUD solutions?

A. DDOS Anti-DDoS Pro IP services
B. Situational awareness services
C. SSL certificate management service

D. Security Expert Services

Correct Answer: A, B, C, D
Section:

QUESTION 19
The purpose of access control is to provide access to authorized subjects and prevent any unauthorized and intentional access.

A. TRUE
B. FALSE

Correct Answer: A
Section:

QUESTION 20
When USG Firewall sends logs outward, it supports several different log information encapsulation formats Which of the following items is a supported firewall format?

A. Netflow format
B. Datafl ow format
C. Binary format
D. Syslog format

Correct Answer: A, C, D
Section:

QUESTION 21
USG firewall's DDoS attack prevention techniques include which of the following?

A. Current limiting technology
B. Cryptography
C. Fingerprint technology
D. Source detection technology

Correct Answer: A, C, D
Section:

QUESTION 22
By default, the firewall authenticates traffic that passes through itself.

A. TRUE
B. FALSE

Correct Answer: B
Section:

QUESTION 23
There are many firewall security policies in the data center network, and the administrator enables the policy backup acceleration function, and the source address matching conditions of the security policy are modified It can be effective immediately.

A. TRUE
B. FALSE

Correct Answer: B
Section:

QUESTION 24
If a user queries the security log of the AD server using single sign-on through the firewall, the firewall can immediately take the user offline after the user logs out.

A. TRUE
B. FALSE

Correct Answer: B
Section:

QUESTION 25
If the database O&M workload is much greater than the host O&M workload, you can choose to have an independent department outside the original O&M bastion host The database bastion host.

A. TRUE
B. FALSE

Correct Answer: A
Section:

QUESTION 26
With the following description of the load balancing feature of USG Firewall Server, what are the correct items?

A. The IP address specified in the security policy should be the IP address of the real server
B. The IP address specified in the security policy should be the IP address of the virtual server
C. Modifying the destination IP address and destination port number of a packet occurs after querying the inter-domain security policy
D. Modifying the destination IP address and destination port number occurs before querying the inter-domain security policy

Correct Answer: A, D
Section:

QUESTION 27
Control of ping packets to the USG firewall itself The access control management function of the interface takes precedence over the security policy.

A. TRUE
B. FALSE

Correct Answer: A
Section:

QUESTION 28
Which is the more correct number of DNS servers that can be bound to each outbound interface in the USC Firewall DNS Transparent Proxy function?

A. 2
B. 3
C. 4
D. 1

Correct Answer: A
Section:

QUESTION 29
A description of the following IPv6 Secure Neighbor Discovery feature information for one of the interfaces Which one is wrong?

```
<FN> display ipv6 security interface lOge 1/0/1
(L): Link local address
SEND: Security ND
SEND information for the interface : 10GE1/0/1
```

IPv6 address	PrefixLength	Collision Count
2001::209F:2FTB:DCF2:F28C	64	0

```
SEND sec value                  :1
SENDsecurity modifier value     :C70D :F872:5AF8:CFB4:8D67:3E30:8594:2626
SEND RSA key label bound        :Huawei
SEND NDminiman key length value :512
SEND NDnaxinrun key length value : 2048
SEND ND Tinestanp delta value   : 300
SEND ND Timestanp fuzz value    :1
SEND ND Timestap drift value    :1
SEND ND fully secured mode      :enable
```

A. The minimum key length that the interface can accept is 512
B. The maximum key length that the interface can accept is 2048
C. The interface does not have strict security mode enabled
D. The security level of the CGA address is 1

Correct Answer: C
Section:

QUESTION 30
In the following description of the USG firewall security policy, which one is wrong?

A. When the firewall is equipped with the undo firewall packet-filter basic-protocol enable command, unicast packets are not controlled by security policies
B. By default... Broadcast packets are not controlled by security policies
C. In the case of the province, multicast packets are not controlled by security policies
D. By default... Unicast packets are controlled by security policies

Correct Answer: A
Section:

QUESTION 31
The USG firewall is connected to the corporate intranet through a router After the firewall is configured with the cross-Layer 3 MAC identification feature, then the security policy of the firewall can configure the MAC address as a match condition o

A. TRUE
B. FALSE

Correct Answer: A
Section:

QUESTION 32
Configure the source NAT policy for the campus network egress firewall to use the internal network users to access the external network, if you need to use security policies to block access to the external network The source IP address matched in the security policy is the private IP address of the user.

A. TRUE
B. FALSE

Correct Answer: A
Section:

QUESTION 33
An important purpose of adopting a distributed denial-of-service attack architecture is to isolate network contacts Protect attackers... So that it will not be tracked by the monitoring system while the attack is in progress

A. TRUE
B. FALSE

Correct Answer: A
Section:

QUESTION 34
Let's see which devices can be used as Huawei CIS (Cybersecurity Intelligence system.). Trapping probes in network security intelligence systems?

A. firewall
B. switchboard
C. router
D. server

Correct Answer: A, B
Section:

QUESTION 35
With the prevalence of e-commerce, online banking, e-government The business value of WEB servers is getting higher and higher, and the security threats faced by web servers are also increasing, and the defense against the web application layer has become an inevitable trend, WAF (WebApplication Firewall WEB APPLICATION FIREWALL) PRODUCTS BEGAN TO BECOME POPULAR.
As shown in the figure The firewall uses the deployment mode of transparent proxy About the deployment mode of WAF using transparent proxy Which of the following options is described incorrectly.

A. You need to configure the IP address and route for the forwarding interface of the WAF
B. The agent works in route-forwarding mode instead of bridge mode
C. JUDGING FROM THE ANGULARITY OF THE WEB CLIENT THE WEB CLIENT IS STILL DIRECTLY ACCESSING THE SERVER AND IS NOT AWARE OF THE EXISTENCE OF WAF
D. Minimal network changes enable zero-configuration deployment

Correct Answer: A
Section:

QUESTION 36
The web reputation feature categorizes websites and differentiates them according to different classifications. When a user visits a potentially risky website, it can be promptly alerted or blocked by the system • thus helping the user quickly confirm the security of the target website. Which of the following options does not fall under the classification of Web Reputation Sites?

A. Default trusted Web site
B. Customize trusted websites
C. Customize the suspicious station
D. Predefined trusted websites

Correct Answer: A
Section:

QUESTION 37
With the continuous development of network technology The firewall is also completing its own upgrade The technology evolution that firewalls have undergone includes which of the following options

A. Stateful Detection Firewall
B. App Proxy Firewall
C. Packet filtering firewall
D. Web firewall

Correct Answer: A, B, C
Section:

QUESTION 38
NIP provides security mechanisms from multiple levels such as administrators and logs to build the security of operation and maintenance Which of the following security options are included?

A. Administrator decentralization and domain management mechanism
B. Anti-brute force mechanism
C. Protection mechanism for sensitive user information
D. Access channel control

Correct Answer: A, B, C, D
Section:

QUESTION 39
PT (Advanced Persistent Threat) attacks are stealthy and persistent computer intrusion processes, usually orchestrated by certain personnel For specific goals.

A. TRUE
B. FALSE

Correct Answer: A
Section:

QUESTION 40
Employees visit illegal or malicious websites at will Viruses, Trojans, and worms will be attacked, so we need to enable URL filtering. Which of the following options is a feature of URL Shopping?

A. Great impact on performance However, only HTTP/HTTPS access is controlled
B. The impact on performance is small And all services corresponding to the domain name can be controlled
C. Control in the domain name resolution stage, control the granularity Control can only be done down to the domain name level
D. Control is performed during the URL request phase of making HTTP/HTTPs Fine control granularityCan be controlled down to the directory and file level

Correct Answer: A, D
Section:

QUESTION 41
Trojans due to infection of other files It also destroys computer systems, and at the same time replicates itself, so Trojans have the characteristics of traditional computer viruses.

A. TRUE
B. FALSE

Correct Answer: B
Section:

QUESTION 42
When NIP is deployed at the Internet perimeter, it is generally deployed in the egress firewall or router back, transparent access network. Which of the following features is the main focus of the summer scene

A. Intrusion prevention
B. App control
C. Content filtering
D. Anti-virus

Correct Answer: A, B, D
Section:

QUESTION 43
Based on years of deep understanding of customer needs and professional research in security, Huawei launched the Anti-DDoS solution, which does not include which of the following options is less

A. Suga Center
B. Testing Center
C. Traffic Center
D. Cleaning center

Correct Answer: A, B, D
Section:

QUESTION 44
The global nature of the Internet exposes Teb services to attacks of varying sizes, sizes, and sophistications So which of the following options can secure Web services?

A. run IIS Lockdown Wizzard
B. Install the latest operating system patches
C. Disable default and management of web sites
D. Disable network printing

Correct Answer: A, B, C, D
Section:

QUESTION 45
NIP's service interfaces are all working at Layer 2, which can not change the customer's existing network topology. It provides direct and transparent access to the customer network In addition, the default threat protection policy is configured, and protection can be started after connecting to the network.

A. TRUE
B. FALSE

Correct Answer: A
Section:

QUESTION 46
Broiler chickens Also known as a zombie, it usually refers to a machine that can be controlled remotely by hackers and is often used in DDOS attacks.

A. TRUE
B. FALSE

Correct Answer: A
Section:

QUESTION 47
The signature filter will batch out signatures, and usually set to a uniform action for ease of management. If an app wants to treat it differently You can also use exception signatures to match O's from signature filters

A. TRUE
B. FALSE

Correct Answer: A

Section:

QUESTION 48
About black box testing in paint through testing Primarily to find problems with which of the following options?

A. Test the validity of internal data structures
B. Whether there are initialization or terminating errors
C. Whether the performance can meet the requirements
D. Whether there are incorrect or missing features

Correct Answer: B, C, D
Section:

QUESTION 49
The server can set or read the information contained in the cookie This maintains state in the user's session with the server.

A. TRUE
B. FALSE

Correct Answer: A
Section:

QUESTION 50
Which of the following options are the main dangers of computer Trojans?

A. Personal accounts, passwords and other information were stolen
B. Cause the system to slow down or even freeze
C. Illegal remote control of a computer
D. User files are corrupted

Correct Answer: A, B, C, D
Section:

QUESTION 51
Hard drives are non-volatile memory on the host computer that uses a hard spinning platter It stores and retrieves data on a flat magnetic surface. So which of the following options does the data hard disk save file saved in the hard disk?

A. cluster
B. object
C. slice
D. piece

Correct Answer: A
Section:

QUESTION 52
Which of the following options protects against SMRF attacks?

A. If the source address of an ICMP request packet is a broadcast address, the packet is discarded
B. If the destination address of an ICMP request packet is a network address, the packet is discarded
C. If the destination address of an ICMP request packet is a broadcast address, the packet is discarded
D. If the source address of the ICMP request packet is the host address The message is discarded

Correct Answer: A
Section:

QUESTION 53
Which of the following options fall under the Security Manager requirements in Graded Protection 2.0?

A. Grading and filing
B. System administration
C. Audit management
D. Centralized control

Correct Answer: B, C, D
Section:

QUESTION 54
In general, which level of level of protection requirements does the non-secret-related information system in the county-level unit need to meet?

A. Autonomous protection level
B. Guidance on protection levels
C. Mandatory protection level
D. Supervise the level of protection

Correct Answer: B
Section:

QUESTION 55
Which of the following options is a pseudonymized method for data?

A. Tokenization
B. hash
C. encrypt
D. Generalization

Correct Answer: A, B, C
Section:

QUESTION 56
Which of the following actions are considered measures to ensure access control security?

A. Encrypt the storage key
B. Back up data information

C. Set up network isolation
D. Set the session timeout

Correct Answer: C, D
Section:

QUESTION 57
Anonymization and pseudonymization of data While reducing the risk of data privacy leakage, it will also reduce the availability of data

A. TRUE
B. FALSE

Correct Answer: A
Section:

QUESTION 58
Requirements for physical facilities in the computer room in Class Protection 2.0

A. Intrusion prevention
B. Electromagnetic protection
C. Personnel authorization

Correct Answer: B
Section:

QUESTION 59
The path by which Trojan files spread

A. mailbox
B. Instant messaging
C. U disk
D. X

Correct Answer: A, B, C
Section:

QUESTION 60
How long does the three-level guarantee re-evaluate

A. Half
B. - years
C. 2 years

Correct Answer: B
Section:

QUESTION 61
The General Data Protection Regulation (GDPR) aims to protect personal data, which of the following options are fundamental rights of data subjects (multiple choices)?

A. Control
B. Weak expulsion
C. Right of Access
D. Right to information

Correct Answer: B, C, D
Section:

QUESTION 62
Which of the following options is required by Security Manager in Graded Protection 2.0 (multiselect

A. Audit management
B. Grading and filing
C. Centralized control
D. System administration

Correct Answer: A, C, D
Section:

QUESTION 63
What should I do when my personal privacy information is violated or leaked (multiple choices)?

A. Obtain privacy information of infringers and warn them.
B. Self-help measures Require the infringer to stop the infringement
C. Filing a lawsuit in the people's court
D. Call the police and ask the public security organs to deal with it.

Correct Answer: A, C, D
Section:

QUESTION 64
Anonymization or pseudonymization of personal data reduces the risk to data subjects, which of the following basic principles for processing for personal reasons is met?

A. principle of accuracy
B. The principle of minimization of doctrinal teachings
C. Lawful and proper The principle of transparency
D. The principle of attribution

Correct Answer: B
Section:

QUESTION 65
Which of the following options is part of the business security resiliency (multiple choices)?

A. Establish a secure business environment
B. Improve situational awareness and resiliency of your business

C. Build defense-in-depth capabilities for your business
D. Do a good job of protecting the equipment at the point

Correct Answer: A, B, C
Section:

QUESTION 66
A backdoor is a hacking method that obtains access to a program or system from a relatively stealthy channel But it does not overrule the security controls of the software.

A. TRUE
B. FALSE

Correct Answer: B
Section:

QUESTION 67
In the first half of 2021 alone, there were 944 data breaches that resulted in 3.3 billion data records being compromised. Organizations must follow the principle of which of the following options to keep data safe at all times.

A. in the file system Data at rest is protected on the database through storage technology
B. Check database backups regularly
C. Protection of data in use when using or processing data
D. Protect data in transit as it travels across the network

Correct Answer: A, B, C, D
Section:

QUESTION 68
Common means of protecting against SYN Flood political attacks are link restriction techniques and link proxy techniques Among them, connection broker technology refers to the detection of TCP connection rate Set the check alarm value to send messages and block attack traffiC.

A. TRUE
B. FALSE

Correct Answer: B
Section:

QUESTION 69
Data storage security is part of the customer's overall security program It is also an important part of data center security and organizational security. Which of the following options is important to keep your data storage secure?

A. Encrypted storage of data
B. Ensure data integrity
C. Data Backup and Recovery
D. Protection against data destruction

Correct Answer: A, B, C, D
Section:

QUESTION 70
Due to the presence of a large number of decoys in the network Attackers will be caught up in an online world where the real is indistinguishable. Attackers often need to spend a lot of time to distinguish the authenticity of information, thereby delaying the attacker's network attack, giving defenders more response time, and reducing the possibility of attackers attacking real systems.

A. TRUE
B. FALSE

Correct Answer: A
Section:

QUESTION 71
Data destruction refers to the use of various technical means to completely delete the data in computer storage devices, so as to prevent unauthorized users from using residual data to restore the original data information, so as to achieve the purpose of protecting key dat a. Which of the following options is wrong about how data is destroyed?

A. Storage media such as disk or tape It's all magnetic technology If it can destroy its magnetic structure The existing data no longer exists.
B. In addition to low-level formatting of disks and tapes, it can also be done in the form of physical rhetoric
C. Since tapes can be used repeatedly, data can be destroyed using overwrite. As long as the disk is overwritten once Data cannot be interpreted.
D. Destruction of the entity's storage media Make the data unreadable by the system It is also one of the ways to ensure the confidentiality and security of data.

Correct Answer: D
Section:

QUESTION 72
Which of the following options are the main dangers of computer Trojans?

A. User files are corrupted
B. Illegal remote control of a computer
C. Personal accounts, passwords and other information are stolen
D. Cause the system to slow down or even freeze

Correct Answer: A, B, C, D
Section:

QUESTION 73
When the Abnormal Traffic Inspection & Control System^ defense strategy of the Abnormal Traffic Monitoring System ATIC selects the anti-uninstall action, it utilizes the status code (targeted) for which of the following options GET request method redirection) to prove the true identity of the client?

A. 300
B. 301
C. 303
D. 302

Correct Answer: D
Section:

QUESTION 74
Whitelisting may not properly handle complex obfuscation, which could allow attackers to subvert filters and potentially inject SQL language.

A. TRLE
B. FALSE

Correct Answer: A
Section:

QUESTION 75
Although DDoS attacks are distributed, DoS attacks are more powerful and destructive than DDoS attacks .

A. TRUE
B. FALSE

Correct Answer: B
Section:

QUESTION 76
Nmap can only be used to scan a single host, but it cannot be used to scan a large computer network to find out which hosts and services of interest are found

A. TRUE
B. FALSE

Correct Answer: B
Section:

QUESTION 77
The FireHunter series of sandboxes gives accurate results based on the analysis Real-time detection, blocking and reporting of grayscale ¦Flow volume Effectively avoid the rapid spread of unknown threat attacks and the loss of enterprise core information assets.

A. TRUE
B. FALSE

Correct Answer: A
Section:

QUESTION 78
NIP can scan the uploaded files for viruses to prevent intranet PCs from being infected with viruses.

A. TRLE
B. FALSE

Correct Answer: A
Section:

QUESTION 79
NIP Network Intelligent Protection System can support troubleshooting which of the following options7

A. ESP card troubleshooting function

B. Ping and Tracer! Means of detection
C. View and download diagnostic information
D. Channel diagnosis function between NIP and network management software or daily host computer

Correct Answer: A, B, C, D
Section:

QUESTION 80
DAS (Direct Attach STorage) is a storage method that connects directly to the host server Each host server has its own storage device o features about DA5 Which of the following options is incorrectly described?

A. DAS has the advantages of high bandwidth and low latency
B. DAS does not support file sharing with heterogeneous operating systems
C. DAS is usually used in a single network environment with minimal data exchange and low performance requirements
D. DAS is a type of block storage

Correct Answer: A
Section:

QUESTION 81
About Huawei's firewall defense technology against SYN Flood Which of the following options is correctly described?

A. The limiting method of limiting the number of TCP half-open connections can prevent SYN Flood political attacks
B. Through SYN Cookie technology, SYN Flood can be prevented
C. By purchasing inter-domain security policies, SYN Flood attacks can be prevented
D. The TCP new connection rate limiting method protects against SYN Flood attacks

Correct Answer: A, D
Section:

QUESTION 82
Which of the following options is a virtual firewall use case?

A. Multi-tenant app environment Enable the virtual firewall to implement an independent port for administrative privileges
B. Network traffic isolation between VMs is not possible
C. VPN group and network environment Enable the virtual firewall for forward isolation
D. Isolation of different security areas of the campus network

Correct Answer: A, B, C
Section:

QUESTION 83
Each element of the audit policy can be flexibly configured, which is convenient for users to classify, classify audit and response, so how many elements the audit strategy includes

A. 3
B. 1
C. 2
D. 4

Correct Answer: D
Section:

QUESTION 84
HiSec Insight's detection of unknown files relies primarily on sandbox detection.

A. TRUE
B. FALSE

Correct Answer: A
Section:

QUESTION 85
Which of the following are important to the corporate network?

A. Prevent DOS attacks by hackers
B. Provide security
C. System stability
D. Network serviceability

Correct Answer: C, D
Section:

QUESTION 86
The intensity of a system security threat is only related to the vulnerability of the system, and a wellprotected system is basically immune to attack.

A. TRUE
B. FALSE

Correct Answer: B
Section:

QUESTION 87
in the architecture of software-defined security Which of the following feature descriptions is correct?

A. Security resources that can be pooled with features Security functions can be divided and combined, and elastically scalable
B. The functional interface should provide northbound API interfaces to meet the requirements of flexible service configuration
C. The security resource pool that carries the security business function can be a hardware resource pool or a software resource pool
D. Need to provide rich security functions to meet the needs of the business

Correct Answer: A, B, C, D
Section:

QUESTION 88
Regarding ECA probe carrier entities, which of the following cannot be ECA probe carrier entities?

A. S switch

B. firewall
C. CE switch
D. HiSec Insight flow probe

Correct Answer: D
Section:

QUESTION 89
HiSec Insight's detection principle for XSS attacks is based on IPs signature libraries, such as detecting JS code features (script, alert), etC. o

A. TRUE
B. FALSE

Correct Answer: B
Section:

QUESTION 90
When using server authentication Before visiting the business, the visitor first logs in through the client or potal authentication page The firewall then proactively obtains the user's login information (including the username and IP address used by the visitor) from the server (single selection).

A. TRUE
B. FALSE

Correct Answer: B
Section:

QUESTION 91
Which of the following is not a cybersecurity threat (single selection).

A. DDOS attacks
B. Phishing attacks
C. IP Spoofing
D. IP address scanning

Correct Answer: B
Section:

QUESTION 92
Which of the following belong to the development of information security? Extravagant selection)

A. Information assurance stage
B. Big data security stage
C. Artificial intelligence security stage
D. Communication confidentiality stage

Correct Answer: A, D
Section:

QUESTION 93
Which of the following can be used as a Huawei IPS device to determine intrusion behavior? (single selection).

A. Session table
B. signature
C. Routing table
D. IP address

Correct Answer: B
Section:

QUESTION 94
Which of the following information cannot be scanned by the nmap tool? (single selection).

A. Operating system version
B. Port
C. Services
D. System vulnerabilities

Correct Answer: D
Section:

QUESTION 95
Which of the following attacks can be addressed using cybertrapping? (Single selection)

A. DDos
B. Malformed message attack
C. TCP port scanning
D. Oversized ICMP packet attack

Correct Answer: C
Section:

QUESTION 96
Which of the following are the following ways to protect enterprise users from viruses? (Multiple selection)

A. Close unnecessary ports of the host
B. Install anti-virus software
C. Patching
D. Enhance safety awareness

Correct Answer: A, B, C, D
Section:

QUESTION 97
If it is in the intrusion prevention configuration file Signatures, signature filters, and exception signatures are used at the same time When there is a configuration to the configuration file The following is about the order of matching Which option is correct? (single selection).

A. Exception Signature>Signature>Signature filter
B. Exception Signature>Signature Over Filter>Signature
C. Signature>Signature Filter >Exception Signature
D. Signature filter >Signature>Exception signature

Correct Answer: B
Section:

QUESTION 98
The following describes how to create a trap account Which one is correct? (single selection).

A. The following describes how to create a trap account Which one is correct? (single selection).
B. Create a local account named Administrator and set its permissions to the most, plus a strong password of more than 10 digits
C. Create a local account named Administrator and set its permissions to the minimum, plus a weak password less than 6 digits
D. Create a local account named Administrator and set its permissions to the minimum, plus a strong password of more than 10 digits
E. Create a local account named Administrator and set its permissions to maximum Plus a weak password less than 6 digits

Correct Answer: C
Section:

QUESTION 99
In the HCIE-Security V2.0 course architecture, which of the following pieces are included? (multiple selection).

A. Cloud security
B. Security operations and analytics
C. Security attack and defense technology
D. Code auditing

Correct Answer: A, B, C
Section:

QUESTION 100
Determine the goal, 2 Intranet forwarding' 3 Intranet penetration, 4 Trace removal, 5 Information Collection, 6 Vulnerability detection, 7 Exploit vulnerabilities, 8 Write test reports. The following is the correct understanding of the penetration test process' (single selection).

A. 1-5-6-7-4-2-3-8
B. 1-5-6-7-2-3-4-8
C. 1 -5-6-7-3-2-4-8
D. ·5·2·3·4·6·7·8

Correct Answer: B
Section:

QUESTION 101
A data center creates subnet A and subnet B under the same VPC network If you add the host to security group A and move it out of the default security group, which of the following is correct? (single selection).

A. A and B are able to visit each other
B. and B are not accessible
C. Only A is allowed to access B
D. Only B is allowed to access A

Correct Answer: B
Section:

QUESTION 102
Which of the following is not a way to back up data? (Single selection)

A. Server-Less ?
B. Client-Less backup
C. LAN-Free S?
D. LAN backup

Correct Answer: B
Section:

QUESTION 103
Which of the following options is not part of the base metric of CVSS assessment? (single selection).

A. Scope
B. Attack vector
C. Availability impact
D. Vulnerability severity level

Correct Answer: D
Section:

QUESTION 104
What are the following descriptions of cybertrapping techniques that are wrong? (multiple selection).

A. Trapping needles support simulation services
B. The trapping technology scheme consists of two parts: trap and trapping probe
C. The trapping probe is a honeypot
D. The trapping probe is responsible for identifying the scanning behavior in the network and directing traffic to the trap

Correct Answer: A, C
Section:

QUESTION 105
Which of the following options is a DDOS attack against the application layer? (multiple selection).

A. DNS reflection attacks
B. UDP fragmentation attacks
C. HTTP slow attacks

D. TCPSYN flood attack

Correct Answer: A, C
Section:

QUESTION 106
If you can successfully access www.huawei.com network resources, which of the following protocols is not involved? (single selection).

A. HTTP
B. TCP
C. DNS
D. Telnet

Correct Answer: D
Section:

QUESTION 107
In which of the following cyberattacks might a virus attack be applied? (Multiple selection)

A. Sabotage
B. Infiltration
C. Elevation of power
D. Information Collection

Correct Answer: A, B, C, D
Section:

QUESTION 108
With the following description of the difference between stored XSS and reflected XSS, what are the correct items? (multiple selection).

A. Attacks caused by stored XSS are persistent
B. The attack code of stored XSS is stored on the target server
C. The attack code of the reflected XSS is stored on the target server
D. Attacks caused by reflective XSS are persistent

Correct Answer: A, B
Section:

QUESTION 109
The target IP address information can be collected through attacks, such as distributed denial-ofservice attacks to obtain the target's IP information. (single selection).

A. TRUE
B. FALSE

Correct Answer: B
Section:

QUESTION 110
The following is a description of wide management Which one is incorrect? (single selection).

A. The functions of ensuring width and forwarding priority can only have an effect on traffic flowing through the firewall
B. Enabling the bandwidth management function will occupy the CPU resources of the device
C. If width management is used at the same time as the NAT Server function When configuring the destination address of the bandwidth management policy, you should specify the address before translation
D. If bandwidth management and source NAT are used at the same time, you should specify the address before translation when configuring the source address matching condition of the bandwidth policy

Correct Answer: C
Section:

QUESTION 111
Which of the following can be used to block C&C attacks? (multiple selection).

A. RAT (Remote Access Tools)??
B. DGA (Domain Generation Algorithm. Domain name generation algorithm) domain name detection
C. Perform environment detection virtually
D. Matching silkworm library

Correct Answer: A, B
Section:

QUESTION 112
In the cyber attack chain... Each stage may use multiple attack methods, or one attack method can be used in multiple stages. (single selection).

A. TRUE
B. FALSE

Correct Answer: A
Section:

QUESTION 113
Which is the correct order for IPS to process traffic? (single selection).

A. Data reorganization, > characteristic matching, > application identification, > corresponding processing
B. Corresponding processing, data reorganization, > trait matching, application identification
C. Corresponding treatment, characteristics matching. Application identification, data reorganization
D. Data reorganization. App recognition. Trait matching. Deal accordingly

Correct Answer: D
Section:

QUESTION 114
In the WAF defense-in-depth system, which of the following security checks is used to protect against CC attacks? (single selection).

A. Content security check
B. Access behavior security check

C. Security checks for sensitive information
D. Network security inspection

Correct Answer: B
Section:

QUESTION 115
Digital signature technology can guarantee the credibility of the data source and verify whether the data has been tampered with during transmission. (Single selection)

A. TRUE
B. FALSE

Correct Answer: A
Section:

QUESTION 116
Which of the following standard bills is relevant to security audits? (Multiple selection)

A. sox
B. IS027001
C. IS022000
D. Graded protection

Correct Answer: A, B, D
Section:

QUESTION 117
The following describes the role of logs Which one is wrong? (single selection).

A. Attack traceability
B. Log storage
C. Virus blockade
D. O&M failure analysis

Correct Answer: C
Section:

QUESTION 118
Categorize vulnerabilities by common ways Which of the following types of vulnerabilities should XSS fall into? (single selection).

A. Webloophole
B. Host vulnerabilities
C. Middleware vulnerabilities
D. Database vulnerabilities

Correct Answer: A
Section:

QUESTION 119
A VPCA and VPCB are created under a virtual data center VDC, and host A (192.168.1.100/24) is applied for in the VPCA Filed Host B (1921682100/24). Now configure VPC access Create a virtual firewall security policy as follows:
Security-policy Source-zone any destination-zone any source-address 192.168.2.100 32 destination-address 192.168.1.100 32 action permit Which of the following statements is correct?

A. A and B cannot visit each other
B. Only A is allowed to access B
C. A and B are able to visit each other
D. Only B is allowed to visit A

Correct Answer: D
Section:

QUESTION 120
Which of the following options is not included in virtualization security? (single selection).

A. Physical machine security
B. Virtualization platform security
C. Virtualized inter-network security
D. Virtual machine security

Correct Answer: D
Section:

QUESTION 121
If you want to intelligently select traffic for the source IP address, you can use which of the following intelligent routing methods^ (single selection).

A. Global traffic steering strategy
B. Policy routing and routing
C. ISProuting
D. Health check

Correct Answer: B
Section:

QUESTION 122
In the cloud data center network Where are Anti-DDos appliances deployed? (single selection).

A. Security operation and maintenance area
B. Secure storage area
C. Border network area
D. Secure computing area

Correct Answer: C
Section:

QUESTION 123

The following is a description of DNS transparent proxy Which ones are correct? (multiple selection).

A. The DNS proxy function replaces the source address header in the DNS request packet.
B. After enabling the DNS transparent proxy function The DNS server address to replace is determined for the outgoing interface
C. In the case of NGFW as the exit network and the DNS server of the enterprise intranet The DNS transparent proxy function can still be implemented normally.
D. Two DNS requests for the same user in the case of DNS transparent proxies The replaced address may be different.

Correct Answer: B, D
Section:

QUESTION 124
In the following description of IPv6 security features, which one is wrong? (single selection).

A. As IPv6 DNS and other related protocols are designed for security
B. IPv6 addresses can be generated by encryption However, privacy headers are not supported
C. AH, and ES can be used as extension headers for IPv6 IPsec is used for additional security.
D. The IPv6 address is 128 bits to ensure that the source address is trusted

Correct Answer: D
Section:

QUESTION 125
The following describes the network layer protection plan for HUAWEI CLOUD security architecture Which one is incorrect? (single selection).

A. Tenants can be isolated through security group networks.
B. Fire protection is implemented between HUAWEI CLOUD and the customer network
C. Cloud network perimeter protection DDos can only be achieved by deploying anti-DDoS appliances.
D. The cloud network boundary protects service availability through DDos defense.

Correct Answer: C
Section:

QUESTION 126
To protect against viruses, which of the following security appliances can be deployed at the cloud network perimeter? (single selection).

A. Bastion host
B. Database audit
C. Anti-DDos
D. Sandbox

Correct Answer: D
Section:

QUESTION 127
Which of the following options does not need to be designed when implementing data storage security in the cloud? (Single selection)

A. Document encryption

B. Key management
C. Database encryption
D. Data upload encryption

Correct Answer: D
Section:

QUESTION 128
The following describes the transparent proxy deployment features of WAF Which is correct?
(multiple selection).

A. The content of the packet is not changed when it is forwarded
B. There is no need for the network layer, and the application layer can be changed There is also no need to make configuration changes on any device
C. Traffic needs to be redirected to the WAF device.
D. The client does not directly establish a connection with the server, which can hide the server

Correct Answer: A, B
Section:

QUESTION 129
When you realize the security of cloud transmission Which of the following do we generally consider? (multiple selection).

A. Data source authentication
B. Data encryption efficiency
C. Encryption of transmission data
D. Integrity check

Correct Answer: A, B, C, D
Section:

QUESTION 130
In • User Login Web Page with User Name and Password Medium The following is about Username" Which one is described correctly? (single selection).

A. Identification
B. Identity authentication
C. Billing
D. Authorization

Correct Answer: A
Section:

QUESTION 131
The following describes the differences between ISMS and graded protection What are the correct options? (multiple selection).

A. The construction result of 1SMS is to establish a set of ISMS system documents for the organization Strongly strengthen the Organization's information security, and the result of the rating assessment is to give whether the subject meets the stated security level requirements.
B. The graded protection system is a basic system for ensuring information security Both technology and qualifications are taken into account The focus is on how to leverage existing sophisticated protection critical

information systems It mainly reflects the classification of hierarchies Protect the idea of focus. While ISMS is mainly from the perspective of security management The focus is on the establishment of information security guidelines, policies and security management systems and security management organizations within the organization or its specific scope, and their effective implementation, which mainly reflects the role and importance of security management.

C. The implementation objects of graded protection are mainly those of various enterprise units, while the implementation objects of ISMS are mainly government departments such as party and government organs at all levels that have the requirements of information system levels.

D. The complete implementation process of ISMS runs through the entire life cycle of the information system The complete implementation process of graded protection runs through the entire life cycle of the management system of the organization or a specific scope of the organization , and can be synchronized with the management system of a specific scope of the organization or organization. It can also be carried out on the basis that its management system has been established.

Correct Answer: A, B
Section:

QUESTION 132
Which of the following devices can be used to sense the intranet situation in conjunction with situational awareness technology? (Multiple selection)

A. Agile-controller DCN
B. FireHunter
C. VSCAN
D. SecoManager

Correct Answer: A, B, D
Section:

QUESTION 133
If the attributes of the file all match the match conditions of the rule Then this file successfully matches the rules for the file to be overmixed with the poppy file. If one of the conditions does not match • The next rule continues to be matched, and so on If all the rules do not match FW will discard the file o (single selection).

A. TRUE
B. FALSE

Correct Answer: B
Section:

QUESTION 134
When it is not in the same deployment as the log server, only FW can send conference logs to the log server through the IPSec tunnel and GRE tunnel (single selection).

A. TRUE
B. FALSE

Correct Answer: B
Section:

QUESTION 135
Which of the following devices can work with situational awareness to isolate infected hosts? (single selection).

A. Agile-controller Campus
B. gile-controller DCN
C. SecoManager

D. EDR

Correct Answer: A
Section:

QUESTION 136
The IPS function of Huawei's intrusion prevention device is not controlled by License (radio selection).

A. TRUE
B. FALSE

Correct Answer: B
Section:

QUESTION 137
The collection of subdomains includes the collection (single selection) of the target's top-level domain name, second-level domain name, third-level domain name and other domain names

A. TRUE
B. FALSE

Correct Answer: A
Section:

QUESTION 138
When you use ATIC for defense policy configuration, the defense system that can be configured does not include which of the following options> (single selection).

A. Blocking
B. Current limiting
C. Defense
D. Detection

Correct Answer: D
Section:

QUESTION 139
With the following description of network scanning defense technology, which is correct? (single selection).

A. For port scanning, you can defend by setting the value of the access frequency bureau.
B. If the access frequency is set too high More false positives will be generated, blocking normal access traffic.
C. If the rate at which its source IP accesses other protected addresses or ports exceeds the set access frequency threshold, this behavior is regarded as scanning behavior And add the purpose to the blacklist to block scan
D. If the frequency of the set direction is too low The scanning behavior is not recognized.

Correct Answer: C
Section:

QUESTION 140
Which of the following threats cannot be detected by the sandbox virtual execution environment?
(Single selection)

A. C&C??
B. PDF file virus
C. PE file virus
D. Web file virus

Correct Answer: A
Section:

QUESTION 141
The following describes the network scanning defense technology Which one is wrong? (single selection).

A. The trapping probe has a business simulation function.
B. Firewalls and switch devices can act as trapping probes.
C. In networking mode where the trap and the trap probe are on the same firewall| CIS and SecoManager are not required for trapping Closed-loop threat linkage can be completed directly through FW.
D. The trapping system produces a unique fingerprint for each attacker Able to record hacker IP, operating system Information such as browser type, type of attack weapon, etC.

Correct Answer: A
Section:

QUESTION 142
The sandbox is actively protected against viruses (single selection)

A. TRUE
B. FALSE

Correct Answer: B
Section:

QUESTION 143
The following describes FW's application behavior control features Which one is correct? (single selection).

A. For FTP behavior, application behavior control can limit the size of upload/download files, but cannot control the upload/download line separately
B. For IM behavior You can set a black whitelist The priority relationship between the black and white list and the provincial action is: blacklist, white list, default action.
C. When creating a security strategy Application behavior control and yellow files can be combined with users, time periods, and other objects to achieve the purpose of application control for different users and different time periods.
D . For HTTP behavior The application behavior control function can be controlled by DEToperation in POST.

Correct Answer: C
Section:

QUESTION 144
In the Anh-DDos system What are the functions that ATIC can complete as a management center?
(multiple selection).

A. reports an exception
B. Policy discipline

C. Report management
D. Clean the flow

Correct Answer: B, C
Section:

QUESTION 145
Which of the following is wrong about Huawei's approach to business security resilience? (single selection).

A. Achieve active security through correlation analysis and collaborative joint defense.
B. Abandon the traditional passive cyber threat defense mode and achieve security resilience with business as the center .
C. Use Al technology to compensate for the lag of threat defense.
D. Active security and passive defense through the department Protect against attacks at all stages of the cyber attack chain.

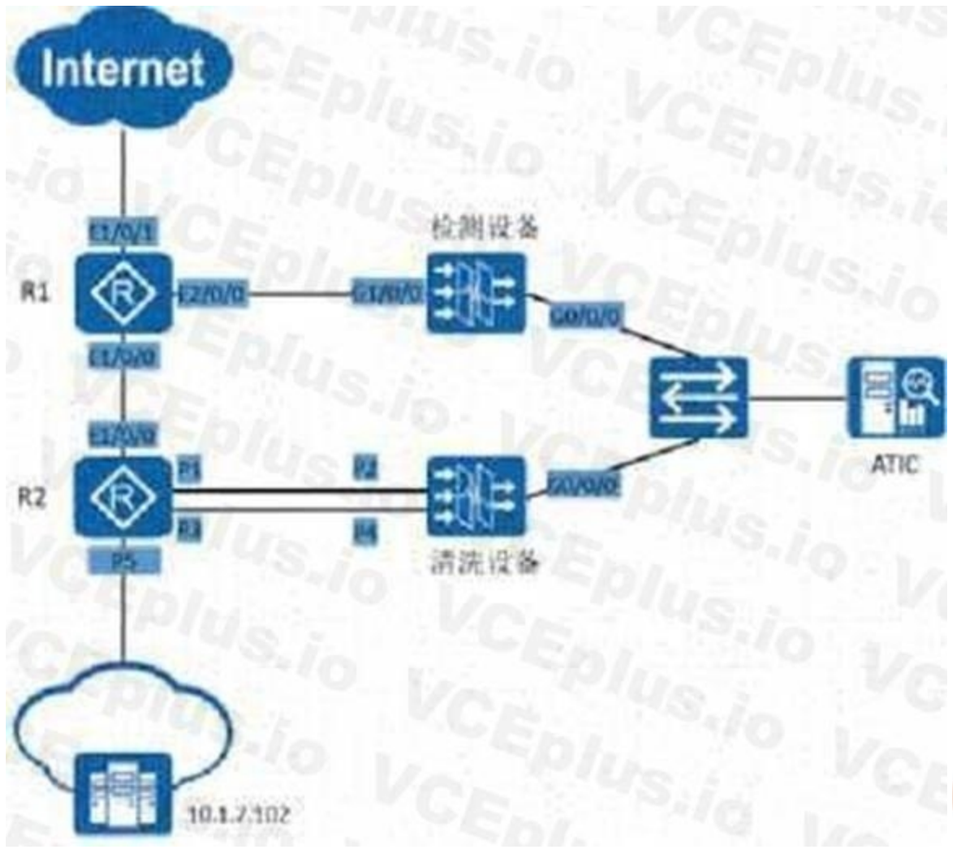
Correct Answer: B
Section:

QUESTION 146
In the Anti-DDos system, the function of cleaning devices is to detect anomalous traffic in the network and escalate to the management centre (single selection).

A. TRUE
B. FALSE

Correct Answer: B
Section:

QUESTION 147
As shown in the following figure, you use the bypass method to deploy the Anti-DDoS system 8GP drainage UN route is used. The port numbers of the P1-P5 devices in the figure, what happens if a routing policy is not configured on R1 to direct cleansed traffic to P5? (single selection).



A. After the inspection equipment is cleaned, it will be sent to the cleaning equipment again
B. The flow to be detected is discarded by the cleaning equipment
C. The detection flow cannot be cleaned by Wang Chang
D. The traffic to be detected cannot reach the detection equipment

Correct Answer: A
Section:

QUESTION 148
Domain name information collection is the first step in technical means information collection Domain name information can be collected through a domain name lookup website such as hois (single selection).

A. TRUE
B. FALSE

Correct Answer: A
Section:

QUESTION 149
The following is a description of FW's DNS filtering feature What are the correct options? (multiple selection).

A. The DNS overcast function has a great impact on the performance of the device compared to the URL overcast, but all services corresponding to the domain name can be controlled.

B. DNS filtering can be controlled at the stage of initiating HTTP/HHPS URL requests.
C. DNS filtering can release or block requests for different time periods or different users/groups by referencing time periods or users/groups.
D. The DNS filtering function is usually used in enterprise gateways to effectively manage users' access to network resources

Correct Answer: C, D
Section:

QUESTION 150
The following is a description of the trapping technique The correct ones are which women's multiple choices).

A. If the attacker cannot notice the fake service provided by the honeypot, the capture efficiency of the honeypot is relatively low
B. Honeypot technology is to absorb the network by deploying some king machines as bait Trick attackers into attacking them This allows attacks to be captured and analyzed
C. Discuss the access layer switch equipment as honeypot equipment
D. The honeypile can only passively wait for the attacker to attack

Correct Answer: A, B, D
Section:

QUESTION 151
What are the options for the IPDRR process? (multiple selection).

A. Response
B. Plan
C. Protection
D. Recovery

Correct Answer: A, C, D
Section:

QUESTION 152
The following is a humble description of transparent and reverse proxies Which items are correct?
(multiple selection).

A. The deployment method of reverse proxy requires directing traffic to the WAF device.
B. The deployment method of transparent proxy requires directing traffic to the WAF device.
C. The deployment method of transparent proxy is to connect devices in the network.
D. The deployment method of reverse proxy is to connect devices in the network.

Correct Answer: A, C
Section:

QUESTION 153
The following describes port scanning Which is wrong? (single selection).

A. TCP port scanning uses the three-way handshake feature
B. The purpose of port scanning is to determine what kind of services are enabled on the peer host, so as to find an entry for intrusion.
C. When the scanner sends a Syn message If the peer does not reply, the peer port is down.

D. For UDP port scanning It is to determine whether the port is open by sending a UDP data packet to the peer with a specific port number and observing whether the ICMP port is unreachable packet.

Correct Answer: C
Section:

QUESTION 154
Which of the following measures can protect against viruses that spread through zero-day vulnerabilities? (multiple selection).

A. Partial sandbox
B. Deploy firewalls
C. Use situational awareness technology
D. Deploy missing equipment

Correct Answer: A, C
Section:

QUESTION 155
Huawei's network security intelligence system CIS can only be linked with which of the following devices to block viruses?

A. Firewall
B. Agile Controller-Campus
C. SecoManager
D. AgileController-DCN

Correct Answer: A
Section:

QUESTION 156
Zombie networks are used to spread viruses and cannot launch DDos attacks

A. TRUE
B. FALSE

Correct Answer: B
Section:

QUESTION 157
The SQL injection vulnerability occurs due to the lack of validation of the legitimacy of user input

A. TRUE
B. FALSE

Correct Answer: A
Section:

QUESTION 158
In the capacity building of the security team, it is generally divided into management positions and technical posts, which of the following are not the key responsibilities of technical positions? (single selection).

A. Responsible for security vulnerability detection and protection.
B. Responsible for organizing the emergency handling of information security emergencies.
C. Responsible for formulating enterprise-level information security technology planning and technical architecture.
D. Responsible for organizing and carrying out information system security graded protection work

Correct Answer: C
Section:

QUESTION 159
Which of the following scenarios is for network intrusion prevention? (multiple selection).

A. IDC or server cluster frontend.
B. The front end of the firewall for the exit of the corporate network.
C. Between branches of the company's network interconnection.
D. The boundary between the campus network and the Internet?

Correct Answer: A, C, D
Section:

QUESTION 160
The following describes the configuration contents of the firewall file filtering feature Which one is wrong, (single selection).

A. Use the command display current-configuration to display configuration information for the default configuration file itself.
B. The administrator should first clarify which types of files need to be purged, and then select the types of files that the device can support Finally, fill in the remaining file types in "Custom extension".
C. When the default configuration file is referenced by the command line configuration security policy You need to enter the full profile name Otherwise, it cannot be successfully referenced.
D. Under the command line interface, you can view the configuration information in the default configuration file through the command display profile type url-filter.

Correct Answer: A
Section:

QUESTION 161
The following describes the implementation of server IP address planning in the firewall server load balancing function, which are the correct items? (multiple selection).

A. It cannot be the same as the virtualization server address
B. It cannot be the same as the address of other servers on the Internet
C. It cannot be the same as the IP address of the server
D. Cannot be intertwined with the outgoing IP address of the FW

Correct Answer: A, C, D
Section:

QUESTION 162
Huawei proposes • Partition Defense Unified Detection - Security Scheme Which of the following partitions requires a summer firewall").

A. Internet boundaries
B. Business service area
C. Office network

D. Core exchange area

Correct Answer: A, B, C
Section:

QUESTION 163
Let's take the L2TP over IPSec in the dual-machine scenario What is wrong with the description is the egg? (single selection).

A. In this scenario, Fireproof will assign an IP address to the client
B. After the L2TF tunnel is established, the user cannot access the Internet normally
C. The parameters set by the client should match the parameters set on the firewall.
D. The client should initiate a dial-up connection to the virtual address of the dual machine.

Correct Answer: B
Section:

QUESTION 164
Which options below are the main changes in Equal Protection 2.0 compared to Equal Protection 1.0' (multiple choices).

A. The classification of general safety requirements is more detailed.
B. The workflow of equal protection assessment is more detailed.
C. Added expansion requirements.
D. The security requirements of each level are more detailed.

Correct Answer: A, B, C, D
Section:

QUESTION 165
The following describes the security risks caused by ordinary users Which gas single choice is wrong)

A. Unauthorized access to business systems unrelated to their own work
B. The user copies the screen content, My Screen or copied by other unlawful means Download the data library.
C. Fake user identity query and obtain data resulting in data leakage 5JL
D. Accidental operation causes the O&M database to be deleted, Destruction.

Correct Answer: D
Section:

QUESTION 166
In accordance with the provisions of the National Cybersecurity Law... Private clouds need to comply with the basic requirements of classified information security protection, but do not necessarily need to comply with cloud computing scaling requirements.

A. TRUE
B. FALSE

Correct Answer: B
Section:

QUESTION 167
Which of the following health check descriptions is correct? (Selection)

A. You do not need to configure a security policy to allow health check packets.
B. The outbound interface of the probe message does not need to be fixed
C. After specifying the junction of the link health check The outgoing interface of the health probe packet can be consistent with the incoming interface of the response packet.
D. When configuring the protocol and port of the health check, check whether the corresponding protocol and port are enabled on the peer side.

Correct Answer: D
Section:

QUESTION 168
The following description of the IPv6 stateless address DAD check, which one is wrong? (single selection).

A. IPv6 duplicate address detection technology is similar to free ARP in IPv4 Used to detect duplicate IPv4 host addresses when the address is divided into IE or when the host is connected to the network.
B. The test address enables broadcast communication.
C. The node sends a Neighbor Request (NS) packet to the test address it will use If you receive a Neighbor Notification (NA) message from another site then proves that the address has already been used.
D. When the interface is configured as an IPv6 address , DAD is used to detect whether the IPv6 address to be used is unique within the local link.

Correct Answer: B
Section:

QUESTION 169
The following describes the authentication method and authentication domain relationship for Internet users single sign-on What are the correct ones? (multiple selection).

A. The firewall participates in the authentication process of single sign-on users, so authentication configuration can be performed in the authentication domain.
B. If no other authentication domain exists on the server, the default authentication domain is online.
C. Single sign-on in progress Firewalls can also be bound to users based on IP/MAC addresses Identify the authentication domain to which the local user belongs
D. Single sign-on users need to be online on the firewall Policy control based on user Therefore, the single sign-on user must also belong to a certain authentication domain.

Correct Answer: C, D
Section:

QUESTION 170
The following description of security protection, which one is correct?(single selection)

A. The packets received by the Ethernet interface cannot be bound to the corresponding relationship between the source IP address and the MAC address
B. When FW is deployed behind a NAT device, there may be a large amount of traffic accessing different destination ports with the same source IP address In this scenario, you cannot enable port scanning and attack prevention.
C. ASPF function will not affect device performance.
D. When FW works in transparent mode You can enable IP spoofing attack prevention.

Correct Answer: B
Section:

QUESTION 171
By default, two subnets of the same VPC network deployed in different physical resource pools cannot access each other.

A. TRUE
B. FALSE

Correct Answer: B
Section:

QUESTION 172
Digital certificates can ensure the credibility of the public key of the communicating partner in the process of data transmission.

A. TRUE
B. FALSE

Correct Answer: A
Section:

QUESTION 173
Which of the following implementation elements is a multi-choice that can be controlled throughout cloud operations).

A. Security policy deployment
B. Account authority management
C. Risks can be identified
D. The operation can be audited

Correct Answer: A, C, D
Section:

QUESTION 174
At this time, there is no defense against C&C attacks that use TLS for encryption

A. TRUE
B. FALSE

Correct Answer: B
Section:

QUESTION 175
Which of the following behaviors does not pose an information security risk. (Single selection)

A. Close unnecessary host ports
B. Misoperation
C. Important files are not encrypted
D. Connect to public WIFI

Correct Answer: A
Section:

QUESTION 176

Which of the following is not part of the changing trend in cyberattacks? (Single selection)

A. Physicalization of attack methods
B. Complication of attack methods
C. The attack method changes little
D. Diversification of attack objectives

Correct Answer: C
Section:

QUESTION 177
Which of the following options is used to obtain information in penetration testing? (single selection).

A. Connect to open ports Log in to the server
B. Exploit the vulnerability to implant a backdoor into the host
C. Use the tool to scan the port open by the server?
D. Extract super administrator permissions for ordinary users.

Correct Answer: C
Section:

QUESTION 178
Which of the following options allows complete destruction of data, (multiple selection)

A. Degaussing method
B. Multiple divisions
C. Overwriting
D. Mashing method

Correct Answer: A, C, D
Section:

QUESTION 179
The trap configuration of the switching machine is as follows: deception deception enable deception detect-network id 1 192.168.1.0 255.255.255.0 deception detect-network id 1 192.168.2.0 255.255.255.0 deception decoy destination 192.0.2.100 Which of the following descriptions of this configuration is correct? (single selection).

A. The IP address used by the Ax deception decoy destination to configure the trapping probe
B. The Deception Detect-Network ID is used to configure the detection network for trapping
C. Deception Enable should be configured under the interface.
D. Deception is used to turn on the device's trapping function

Correct Answer: B
Section:

QUESTION 180
The following describes the service identification Which item ? (single selection) is wrong

A. Service identification is a reconnaissance technique that identifies the type of service provided by the server.
B. The SSH protocol will actively inform visitors of their version information.
C. An attacker can retrieve the relevant hole according to the service version and exploit it.
D. The identification of all services can be achieved through port scanning technology.

Correct Answer: D
Section:

QUESTION 181
Formatting your computer means that the files have been completely erased Unable to fix.

A. TRUE
B. FALSE

Correct Answer: B
Section:

QUESTION 182
The sandbox cannot link the anti-virus with which of the following devices, (single selection).

A. Firewall
B. switchboard
C. Router
D. CIS

Correct Answer: C
Section:

QUESTION 183
Which of the following is not a virus exemption method? (single selection).

A. Modify system files
B. Parasitic in macro files
C. Modify the memory signature
D. Modify the file signature

Correct Answer: B
Section:

QUESTION 184
If you are deploying a WAF appliance in your network for the first time, which is the correct option for the WAF configuration process sequencing? (single).
1, View logs Understand security events in your network 2, Add protection sites 3, Custom rule groups 4, After going live, the strategy is adjusted

A. 1-2-3-4
B. 3-2-1-4
C. 3-1-2-4.
D. 1-3-2-4

Correct Answer: A
Section:

QUESTION 185
Which of the following authentication methods is password authentication? (single selection).

A. What do you have
B. What do you do
C. What you are
D. What do you know

Correct Answer: D
Section:

QUESTION 186
The following describes the hot standby of the dual machine What are the wrong items? (multiple selection).

A. Under the condition that the firewall service interface works at Layer 2 and connects the router upstream and downstream It is recommended to use a staff-sharing network.
B. Under the condition that the firewall service interface works at Layer 2 and connects the switch upstream and downstream Support staff sharing networking
C. The firewall service interface works in the case of three-layer, uplink and downlink connection to the router You can use primary/standby networking.
D. The firewall service interface works under the networking condition of Layer 3, uplink and downlink connecting routers You cannot use load-sharing groups.

Correct Answer: B, D
Section:

QUESTION 187
The Pv6 multicast address range is FE80::/10

A. TRUE
B. FALSE

Correct Answer: B
Section:

QUESTION 188
Which of the following options is a major cause of business disruption in the cloud? (multiple selection).

A. Vulnerabilities
B. Data breach
C. Cyber attacks
D. Viruses

Correct Answer: A, C, D
Section:

QUESTION 189
If the attacker uses a fake address to launch a TCP flood attack Which of the following defenses is most effective? (single).

A. Source verification
B. Fingerprint learning
C. Session checking
D. Load inspection

Correct Answer: A
Section:

QUESTION 190
The following description of deploying the CIS data ingestation feature is correct? (single selection).

A. When the log collector transmits logs to the big data platform It is recommended to use SSL Because the SSL method is more secure But the overhead is greater.
B. By deploying the image function on the stream probe , the Netflow data stream is sent to the big data platform.
C. Syslog B aims to normalize before reporting to the big data platform But Netflow B does not normalize.
D. By deploying the spectroscopic function on the flow probe Send information elements to the big data platform.

Correct Answer: A
Section:

QUESTION 191
XSS vulnerabilities are injection vulnerabilities formed by sending invalid database commands

A. TRUE
B. FALSE

Correct Answer: B
Section:

QUESTION 192
In the stage of incident response What do the following security personnel need to do? (Selection).

A. Perform root cause analysis
B. Control events
C. Collect evidence
D. Rebuild the system

Correct Answer: B
Section: