**Exam Code: H12-724**
**Exam Name:** HCIP Security (Fast track) V1.0

*V*dumps

**Exam A**

**QUESTION 1**
Viruses can damage computer systems. v Change and damage business data: spyware collects, uses, and disperses sensitive information of corporate employees.
These malicious pastoral software seriously disturb the normal business of the enterprise. Desktop anti-disease software can solve the problem of central virus and indirect software from the overall situation.

A. True
B. False

**Correct Answer: B**
**Section:**

**QUESTION 2**
Which of the following options are common behavioral characteristics of viruses? (multiple choices)

A. Download and backdoor features
B. Information collection characteristics
C. Self-hidden features
D. Network attack characteristics

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

**QUESTION 3**
Which of the following signature attributes cannot be configured for IP custom signature?

A. ID
B. Message length
C. Agreement
D. Direction

**Correct Answer: B**
**Section:**

**QUESTION 4**
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. .

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

**QUESTION 5**
The whitelist rule of the firewall anti-virus module is configured as ("*example*, which of the following matching methods is used in this configuration?

A. Prefix matching
B. Suffix matching
155955cc-666171a2-20fac832-0c042c043
C. Keyword matching
D. Exact match

**Correct Answer: C**
**Section:**

**QUESTION 6**
UDP is a connectionless protocol. UDP Flood attacks that change sources and ports will cause performance degradation of network devices that rely on session forwarding.
Even the session table is exhausted, causing the network to be paralyzed. Which of the following options is not a preventive measure for UDP Flood attacks?

A. UDP fingerprint learning
B. Associated defense
C. current limit
D. First packet discarded

**Correct Answer: D**
**Section:**

**QUESTION 7**
Regarding the processing flow of file filtering, which of the following statements is wrong?

A. After the file decompression fails, the file will still be filtered. .
B. The application identification module can identify the type of application that carries the file.
C. Protocol decoding is responsible for analyzing the file data and file transmission direction in the data stream.
D. The file type recognition module is responsible for identifying the true type of the file and the file extension based on the file data

**Correct Answer: A**
**Section:**

**QUESTION 8**
Huawei WAF products are mainly composed of front-end execution, back-end central systems and databases. Among them, the database mainly stores the front-end detection rules and black Whitelist and other configuration files.

A. True
B. False

**Correct Answer: A**
**Section:**

**QUESTION 9**
Misuse detection is through the detection of similar intrusions in user behavior, or those that use system flaws to indirectly violate system security rules To detect intrusions in the system. Which of the following is not a feature of misuse detection 2

A. Easy to implement

B. Accurate detection

C. Effective detection of impersonation detection of legitimate users

D. Easy to upgrade

**Correct Answer: C**
**Section:**

**QUESTION 10**
Huawei NIP6000 products have zero-setting network parameters and plug-and-play functions, because the interfaces and interface pairs only work on layer 2 without Set the IP address.

A. True

B. False

**Correct Answer: A**
**Section:**

**QUESTION 11**
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 155955cc-666171a2-20fac832-0c042c044

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.

**Correct Answer: D**
**Section:**

**QUESTION 12**
Which aspects of information security will be caused by unauthorized access? (multiple choice)

A. Confidentiality

B. Integrity

C. Availability

D. Recoverability

**Correct Answer: A, B**
**Section:**

**QUESTION 13**
Network attacks are mainly divided into two categories: single-packet attacks and streaming attacks.
Single-packet attacks include scanning and snooping attacks, malformed packet attacks, and special reports.
Wen attack.

A. True

B. False

**Correct Answer: A**
**Section:**

**QUESTION 14**
Which of the following attacks are attacks against web servers? (multiple choices)

A. Website phishing deception
B. Website Trojan
C. SQL injection
D. Cross-site scripting attacks 2335

**Correct Answer: C, D**
**Section:**

**QUESTION 15**
Which of the following is the correct configuration idea for the anti-virus strategy?

A. Load the feature library
B. Configure security policy and reference AV Profile
C. Apply and activate the license
D. Configure AV Profile
E. Submit
F. 3->1->4->2->5
G. 3->2->4->1->5
H. 3->2->1->4->5
I. 3->1->2->4->5

**Correct Answer: A**
**Section:**

**QUESTION 16**
In the security protection system of the cloud era, reforms need to be carried out in the three stages before, during and after the event, and a closed-loop continuous improvement should be formed.
And development. Which of the following key points should be done in "things"? (multiple choice)

A. Vulnerability intelligence
B. Defense in Depth
C. Offensive and defensive situation
D. Fight back against hackers
   155955cc-666171a2-20fac832-0c042c045

**Correct Answer: B, D**
**Section:**

**QUESTION 17**
Huawei NIP6000 products provide carrier-class high-reliability mechanisms from multiple levels to ensure the stable operation of equipment.
Which of the following options belong to the network reliability? (multiple choice)

A. Dual machine hot backup

B. Power supply. 1+1 redundant backup

C. Hardware Bypass

D. Link-group

**Correct Answer: A, D**
**Section:**

**QUESTION 18**
Which of the following options are common reasons for IPS detection failure? (multiple choices)

A. IPS policy is not submitted for compilation

B. False Policy IDs are associated with IPS policy domains

C. The IPS function is not turned on

D. Bypass function is closed in IPS

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

**QUESTION 19**
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 announce specific types of files.

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

**Correct Answer: C**
**Section:**

**QUESTION 20**
Based on the anti-virus gateway of streaming scan, which of the following descriptions is wrong?

A. Rely on state detection technology and protocol analysis technology

B. The performance is higher than the agent-based method

C. The cost is smaller than the agent-based approach

D. The detection rate is higher than the proxy-based scanning method

**Correct Answer: D**
**Section:**

**QUESTION 21**
Regarding the strong statement of DNS Request Flood attack, which of the following options is correct?

A. The DNS Request Flood attack on the cache server can be redirected to verify the legitimacy of the source

B. For the DNS Reguest Flood attack of the authorization server, the client can be triggered to send DINS requests in TCP packets: to verify The legitimacy of the source IP.

C. In the process of source authentication, fire prevention will trigger the client to send DINS request via TCP report to verify the legitimacy of the source IP, but in a certain process It will consume the TCP connection

resources of the OINS cache server.

D. Redirection should not be implemented on the source IP address of the attacked domain name, and the destination P address of the attacked domain name should be implemented in the wild.

**Correct Answer: C**
**Section:**

**QUESTION 22**
Regarding the anti-spam response code, which of the following statements is wrong?

A. The response code will vary depending on the RBL service provider.
155955cc-666171a2-20fac832-0c042c046
B. USG treats mails that match the answer code as spam.
C. If the response code is not returned or the response code is not configured on the USG, the mail is released.
D. The response code is specified as 127.0.0.1 in the second system.

**Correct Answer: D**
**Section:**

**QUESTION 23**
The configuration command to enable the attack prevention function is as follows; n [FW] anti-ddos syn-flood source-detect [FW] anti-ddos udp-flood dynamic-fingerprint-learn [FW] anti-ddos udp-frag-flood dynamic fingerprint-learn [FW] anti-ddos http-flood defend alert-rate 2000 [Fwj anti-ddos htp-flood source-detect mode basic Which of the following options is correct for the description of the attack prevention configuration? (multiple choice)

A. The firewall has enabled the SYN Flood source detection and defense function
B. The firewall uses the first packet drop to defend against UDP Flood attacks.
C. HTTP Flood attack defense uses enhanced mode for defense
D. The threshold for HTTP Flood defense activation is 2000.

**Correct Answer: A, D**
**Section:**

**QUESTION 24**
The application behavior control configuration file takes effect immediately after being referenced, without configuration submission.

A. True
B. False

**Correct Answer: A**
**Section:**

**QUESTION 25**
Regarding the description of keywords, which of the following is correct? (multiple choice)

A. Keywords are the content that the device needs to recognize during content filtering.
B. Keywords include predefined keywords and custom keywords.
C. The minimum length of the keyword that the text can match is 2 bytes. ,
D. Custom keywords can only be defined in text mode.

**Correct Answer: A, B**
Section:

**QUESTION 26**
IPS is an intelligent intrusion detection and defense product. It can not only detect the occurrence of intrusions, but also can respond in real time through certain response methods.
Stop the occurrence and development of intrusions, and protect the information system from substantial attacks in real time. According to the description of PS, the following items are wrong?

A. IPS is an intrusion detection system that can block real-time intrusions when found
B. IPS unifies IDS and firewall
C. IPS must use bypass deployment in the network
D. Common IPS deployment modes are in-line deployment,

**Correct Answer: C**
Section:

**QUESTION 27**
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 down, and MF bit is also 1 or Fragment Offset is not 0, 155955cc-666171a2-20fac832-0c042c047
B. DF bit is 023, 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.

**Correct Answer: A, C**
Section:

**QUESTION 28**
Huawei's USG000 product can identify the true type of common files and over-check the content.
Even if the file is hidden in a compressed file, or change the extension The name of the exhibition can't escape the fiery eyes of the firewall.

A. True
B. False

**Correct Answer: A**
Section:

**QUESTION 29**
For the description of the Anti DDOS system, which of the following options is correct? C

A. The detection center is mainly to pull and clean the attack flow according to the control strategy of the security management center, and re-inject the cleaned normal flow back to the customer.
   User network, send to the real destination.
B. The management center mainly completes the processing of attack events, controls the drainage strategy and cleaning strategy of the cleaning center, and responds to various attack events and attack flows.
   View in categories and generate reports.
C. The main function of the Green Washing Center is to detect and analyze DDoS attack traffic on the flow from mirroring or splitting, and provide analysis data to The management center makes a judgment.
D. The firewall can only be used for inspection equipment

**Correct Answer: B**
Section:

**QUESTION 30**
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

**Correct Answer: A, C**
Section:

**QUESTION 31**
Regarding the global configuration of file filtering configuration files for Huawei USG6000 products, which of the following descriptions is correct?

A. File filtering, content filtering and anti-virus detection cannot be performed when the file is damaged. At this time, the documents can be released or blocked according to business requirements.
B. When the file extension does not match, if the action is "Allow" or "Alarm", file filtering, content filtering and anti-virus are performed according to the file type Detection.
C. When the number of compression layers of a file is greater than the configured "Maximum Decompression Layers", the firewall cannot filter the file.
D. When the file type cannot be recognized, file filtering, content filtering and anti-virus detection are not performed.

**Correct Answer: C**
Section:

**QUESTION 32**
In Huawei USG6000 products, IAE provides an integrated solution, all content security detection functions are integrated in a well-designed In the high-performance engine. Which of the following is not the content security detection function supported by this product?

A. Application recognition and perception
B. URL classification and filtering
C. Video content filtering
D. Intrusion prevention 155955cc-666171a2-20fac832-0c042c048

**Correct Answer: C**
Section:

**QUESTION 33**
Which of the following options does not belong to the basic DDoS attack prevention configuration process?

A. The system starts traffic statistics.
B. System related configuration application, fingerprint learning.
C. The system starts attack prevention.
D. The system performs preventive actions.

**Correct Answer: B**
Section:

**QUESTION 34**
Regarding the network intrusion detection system (NIDS), which of the following statements is wrong?

A. It is mainly used for real-time monitoring of the information of the critical path of the network, listening to all packets on the network, collecting data, and analyzing suspicious objects
B. Use the newly received network packet as the data source;
C. Real-time monitoring through the network adapter, and analysis of all communication services through the network;
D. Used to monitor network traffic, and can be deployed independently.

**Correct Answer: B**
**Section:**

**QUESTION 35**
Cloud sandbox refers to deploying the sandbox in the cloud and providing remote detection services for tenants. The process includes:

A. Report suspicious files
B. Retrospective attack
C. Firewall linkage defense
D. Prosecution in the cloud sandbox
   For the ordering of the process, which of the following options is correct?
E. 1-3-4-2
F. 1-4-2-3
G. 1-4-3-2
H. 3-1-4-2:

**Correct Answer: C**
**Section:**

**QUESTION 36**
What content can be filtered by the content filtering technology of Huawei USG6000 products?
(multiple choice)

A. Keywords contained in the content of the uploaded file
B. Keywords contained in the downloaded file
C. File type
D. File upload direction 335

**Correct Answer: A, B**
**Section:**

**QUESTION 37**
Regarding the sequence of file filtering technology processing flow, which of the following is correct?
(1) The security policy is applied as permit
(2) Protocol decoding
(3) File type recognition
(4) Application recognition
(5) File filtering

A. (1)(2)(3)(4)(5)
155955cc-666171a2-20fac832-0c042c049
B. (1)(4)(2)(3)(5)
C. (1)(2)(4)(3)(5)
D. (1)(3)(2)(4)(5)

**Correct Answer: B**
**Section:**

**QUESTION 38**
Which of the following statements about IPS is wrong?

A. The priority of the coverage signature is higher than that of the signature in the signature set.
B. When the "source security zone" is the same as the "destination security zone", it means that the IPS policy is applied in the domain.
C. Modifications to the PS policy will not take effect immediately. You need to submit a compilation to update the configuration of the IPS policy.
D. The signature set can contain either predefined signatures or custom signatures. 832335

**Correct Answer: D**
**Section:**

**QUESTION 39**
Due to differences in network environment and system security strategies, intrusion detection systems are also different in specific implementation. From the perspective of system composition, the main Which four major components are included?

A. Event extraction, intrusion analysis, reverse intrusion and remote management.
B. Incident extraction, intrusion analysis, intrusion response and on-site management.
C. Incident recording, intrusion analysis, intrusion response and remote management.
D. Incident extraction, intrusion analysis, intrusion response and remote management.

**Correct Answer: D**
**Section:**

**QUESTION 40**
For the description of URPF technology, which of the following options are correct? (multiple choice)

A. The main function is to prevent network attacks based on source address spoofing.
B. In strict mode, it does not check whether the interface matches. As long as there is a route to the source address, the message can pass.
C. The loose mode not only requires corresponding entries in the forwarding table, but also requires that the interface must match to pass the URPF check.
D. Use URPF's loose mode in an environment where routing symmetry cannot be guaranteed.

**Correct Answer: A, D**
**Section:**

**QUESTION 41**
Which of the following descriptions about the black and white lists in spam filtering is wrong? c

A. Set local blacklist and whitelist: Both blacklist and whitelist can be configured at the same time, or only one of them can be configured.

B. In the "Whitelist" text box, enter the P address and mask of the SMTP Server to be added to the whitelist. You can enter multiple IP addresses, one IP address Address one line. v

C. Enter the IP address and mask of the SMITP Server to be added to the blacklist in the "Blacklist" text box, you can enter multiple IP addresses, one IP Address one line.

D. The priority of the blacklist is higher than that of the whitelist.

**Correct Answer: D**
**Section:**

**QUESTION 42**
Which of the following options belong to the network layer attack of the TCP/IP protocol stack?
(multiple choice)

A. Address scanning

B. Buffer overflow p

C. Port scan

D. IP spoofing

**Correct Answer: A, D**
**Section:**

**QUESTION 43**
For the URL is htpt://www.abcd. com:8080/news/education. aspx?name=tom&age=20, which option is path?

A. htttp://www.abcd. com:8080/news/education. aspx

B. htttp://www.abcd. com:8080,te

C. /news/education. aspx

D. /news/education. aspx?name=tom&age=20

**Correct Answer: C**
**Section:**

**QUESTION 44**
The process of a browser carrying a cookie to request resources from a server is shown in the following figure. Which of the following steps contains SessionID information in the message?



A. 3-4

B. 1-3-4

C. 5-6

D. 2-4

**Correct Answer: A**
**Section:**

**QUESTION 45**
SQl injection attacks generally have the following steps:
①Elevate the right
②Get the data in the database
③Determine whether there are loopholes in the webpage
④ Determine the database type
For the ordering of these steps, which of the following options is correct?

A. 3412

B. 3421

C. 4123

D. 4213

**Correct Answer: B**
**Section:**

**QUESTION 46**
Which of the following options are correct for the configuration description of the management center ATIC? (multiple choice)

A. The drainage task needs to be configured on the management center, and when an attack is discovered, it will be issued to the cleaning center.

B. It is necessary to configure the protection object on the management center to guide the abnormal access flow in etpa

C. Port mirroring needs to be configured on the management center to monitor abnormal traffic.
155955cc-666171a2-20fac832-0c042c0411

D. The reinjection strategy needs to be configured on the management center to guide the flow after cleaning. Q:

**Correct Answer: A, B**
**Section:**

**QUESTION 47**
USG6000V software logic architecture is divided into three planes: management plane, control plane and

A. Configuration plane

B. Business plane

C. Log plane

D. Data forwarding plane

**Correct Answer: D**
**Section:**

**QUESTION 48**
The network-based intrusion detection system is mainly used to monitor the information of the critical path of the network in real time, listen to all packets on the network, collect data, and divide Analyze the suspicious object, which of the following options are its main features? (multiple choices)

A. Good concealment, the network-based monitor does not run other applications, does not provide network services, and may not respond to other computers, so Not vulnerable to attack.

B. The monitoring speed is fast (the problem can be found in microseconds or seconds, and the hostbased DS needs to take an analysis of the audit transcripts in the last few minutes

C. Need a lot of monitors.

D. It can detect the source address and destination address, identify whether the address is illegal, and locate the real intruder.

**Correct Answer: A, B**
**Section:**

**QUESTION 49**
Huawei USG6000 products can scan and process certain file transfer protocols for viruses, but which of the following protocols is not included?

A. POP3

B. IMAP

C. FTP

D. TFTP

**Correct Answer: D**
**Section:**

**QUESTION 50**
Malicious code usually uses RootKit technology in order to hide itself. RootKit modifies the kernel of the system by loading a special driver.
To hide itself and the role of designated files.

A. True

B. False

**Correct Answer: A**
**Section:**

**QUESTION 51**
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

**Correct Answer: B**
**Section:**
**Explanation:**
155955cc-666171a2-20fac832-0c042c0412

**QUESTION 52**
The results of the RBL black and white list query on the firewall are as follows:

```
<USG> display rbl-filter whitelist
=================================================
RBL whitelist(2):
IP address Mask
-------------------------------------------------
10.17.1.0 255.255.255.0
10.18.1.0 255.255.255.0
=================================================
<USG> display rbl-filter blacklist
=================================================
RBL blacklist(1):
IP address Mask
-------------------------------------------------
10.18.1.0 255.255.255.0
10.18.2.0 255.255.255.0
=================================================
```

Based on the above information only, which of the following statements is correct? (multiple choice)

A. Mail with source address 10.17.1.0/24 will be blocked
B. Mail with source address 10.18.1.0/24 will be blocked
C. Mail with source address 10.17.1.0/24 will be released
D. Mail with source address 10.18.1.0/24 will be released

**Correct Answer: C, D**
**Section:**

**QUESTION 53**
Content filtering is a security mechanism for filtering the content of files or applications through Huawei USCG00 products. Focus on the flow through deep recognition Contains content, the device can block or alert traffic containing specific keywords.

A. True
B. False

**Correct Answer: A**
**Section:**

**QUESTION 54**
Which of the following options is not a special message attack?

A. ICMP redirect message attack) 0l
B. Oversized ICMP packet attack
C. Tracert packet attack
D. IP fragment message item

**Correct Answer: D**
**Section:**

**QUESTION 55**
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.

**Correct Answer: C**
**Section:**

**QUESTION 56**
Information security is the protection of information and information systems to prevent unauthorized access, use, leakage, interruption, modification, damage, and to improve For confidentiality, integrity and availability. ,

A. True
B. False

**Correct Answer: A**
**Section:**

**QUESTION 57**
When you suspect that the company's network has been attacked by hackers, you have carried out a technical investigation. Which of the following options does not belong to the behavior that occurred in the early stage of the attack?

A. Planting malware
B. Vulnerability attack
C. Web application attacks
D. Brute force

**Correct Answer: A**
**Section:**

**QUESTION 58**
Which of the following options will not pose a security threat to the network?

A. Hacking
B. Weak personal safety awareness
C. Open company confidential files
D. Failure to update the virus database in time

**Correct Answer: C**
**Section:**

**QUESTION 59**
Regarding computer viruses, which of the following options is correct?

A. Patching the system can completely solve the virus intrusion problem
B. Computer viruses are latent, they may be latent for a long time, and only when they encounter certain conditions will they begin to carry out sabotage activities
C. Computer viruses are contagious. They can spread through floppy disks and CDs, but they will not spread through the Internet.
D. All computer viruses must be parasitic in files and cannot exist independently

**Correct Answer: B**
**Section:**

**QUESTION 60**
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

**Correct Answer: C**
**Section:**

**QUESTION 61**
Since the sandbox can provide a virtual execution environment to detect files in the network, the sandbox can be substituted when deploying security equipment Anti-Virus, IPS, spam detection and other equipment.

A. True
    155955cc-666171a2-20fac832-0c042c0414
B. False

**Correct Answer: B**
**Section:**

**QUESTION 62**
When a virus is detected in an email, which of the following is not the corresponding action for detection?

A. Warning
B. Block
C. Declare
D. Delete attachments

**Correct Answer: B**
**Section:**

**QUESTION 63**
Regarding the description of intrusion detection technology, which of the following statements is correct?

A. It is impossible to detect violations of security policies.
B. It can detect all kinds of authorized and unauthorized intrusions.
C. Unable to find traces of the system being attacked.
D. is an active and static security defense technology.
   155955cc-666171a2-20fac832-0c042c0425

**Correct Answer: B**
**Section:**

**QUESTION 64**
If the regular expression is "abc. de", which of the following will not match the regular expression?

A. abcde
B. abcdde
C. abclde
D. abc+de

**Correct Answer: A**
**Section:**

**QUESTION 65**
If the processing strategy for SMTP virus files is set to alert, which of the following options is correct?

A. Generate logs and discard
B. Generate logs and forward them
C. Delete the content of the email attachment
D. Add announcement and generate log

**Correct Answer: B**
**Section:**

**QUESTION 66**
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

**Correct Answer: D**
**Section:**

**QUESTION 67**

The realization of content security filtering technology requires the support of the content security combination license.

A. True
B. False

**Correct Answer: A**
**Section:**
**Explanation:**
155955cc-666171a2-20fac832-0c042c0426

**QUESTION 68**

The following figure is a schematic diagram of the detection file of the firewall and the sandbox system linkage.



The Web reputation function is enabled on the firewall, and website A is set as a trusted website and website B is set as a suspicious website.
Which of the following statements is correct

A. The files obtained by users from website A and website B will be sent to the inspection node for inspection.
B. When a user visits website B, although the firewall will extract the file and send it to the detection node, the user can still access normally during the detection process Site B.
C. After the detection node detects the suspicious file, it not only informs the firewall in the figure of the result, but also informs other network devices connected to it.
D. Assuming that website A is an unknown website, the administrator cannot detect the traffic file of this website sC

**Correct Answer: C**
**Section:**

**QUESTION 69**

Configure the following commands on the Huawei firewall:
[USG] interface G0/0/1 [USG] ip urpf loose allow-defult-route acl 3000
Which of the following options are correct? (multiple choice)

A. For loose inspection: if the source address of the packet exists in the FB of the firewall: the packet passes the inspection directly

B. For the case where the default route is configured, but the parameter allow-defult-route is not configured. As long as the source address of the packet is in the FIB table of the firewall If it does not exist, the message will be rejected.

C. For the situation where the default route is configured and the parameter allow-defult-route is matched at the same time, if the source address of the packet is in the FIB table of the firewall If the packet does not exist in the loose check mode, all packets will pass the URPF check and be forwarded normally.
155955cc-666171a2-20fac832-0c042c0427

D. For the configuration of the default route, and at the same time matching the parameter allowdefult- route, if the source address of the message is in the FIB table of the firewall If it does not exist in the l0e check, the packet cannot pass the URPF check.

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

**QUESTION 70**
With regard to APT attacks, the attacker often lurks for a long time and launches a formal attack on the enterprise at the key point of the incident.
Generally, APT attacks can be summarized into four stages:

A. Collecting Information & Intrusion

B. Long-term lurking & mining

C. Data breach

D. Remote control and penetration
Regarding the order of these four stages, which of the following options is correct?

E. 2-3-4-1

F. 1-2-4-3

G. 1-4-2-3

H. 2-1-4-3

**Correct Answer: C**
**Section:**

**QUESTION 71**
When using the two-way SSL function to decrypt HTTPS packets, the value of the reverse proxy levelrepresents the number of times the packet can be decrypted.

A. True

B. False

**Correct Answer: B**
**Section:**

**QUESTION 72**
In the construction of information security, the intrusion detection system plays the role of a monitor.
It monitors the flow of key nodes in the information system.
In-depth analysis to discover security incidents that are occurring. Which of the following are its characteristics?. c0O

A. IDS can be linked with firewalls and switches to become a powerful "assistant" of firewalls, which can better and more accurately control access between domains.

B. It is impossible to correctly analyze the malicious code doped in the allowed application data stream.

C. Unable to detect malicious operations or misoperations from internal killings.

D. Cannot do in-depth inspection

**Correct Answer: A**
**Section:**

**QUESTION 73**
There are several steps in a stored XSS attack
There are several steps in a stored XSS attack
①The attacker hijacks the user session
②The attacker submits an issue containing known JavaScript
③User login
④The user requests the attacker's question 5
⑤The server responds to the attacker's JavaScript
⑥ The user's browser sends a session token to the attacker
⑦The attacker's JavaScript is executed in the user's browser
For the ordering of these steps, which of the following options is correct?

A. ③②⑦⑥④⑤①

B. ③②④⑤⑦⑥①

C. ③②④⑥⑤⑦①
    155955cc-666171a2-20fac832-0c042c0428

D. ⑧②⑤⑦④⑥①

**Correct Answer: B**
**Section:**

**QUESTION 74**
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

**Correct Answer: A**
**Section:**

**QUESTION 75**
An enterprise administrator configures a Web reputation website in the form of a domain name, and configures the domain name as www. abc; example. com. .
Which of the following is the entry that the firewall will match when looking up the website URL?

A. example

B. www. abc. example. com

C. www.abc. example

D. example. com

**Correct Answer: A**

**Section:**

**QUESTION 76**
When a data file hits the whitelist of the firewall's anti-virus module, the firewall will no longer perform virus detection on the file.

A. True
B. False

**Correct Answer: A**
**Section:**

**QUESTION 77**
What content can be filtered by the content filtering technology of Huawei USG6000 products?

A. File content filtering
B. Voice content filtering
C. Apply content filtering..
D. The source of the video content

**Correct Answer: A, C**
**Section:**

**QUESTION 78**
If you combine security defense with big data technology, which of the following statements are correct? (multiple choice)

A. In the learning process, you should start from collecting samples, analyze their characteristics and then perform machine learning.
B. Machine learning only counts a large number of samples, which is convenient for security administrators to view.
C. In the detection process, the characteristics of unknown samples need to be extracted and calculated to provide samples for subsequent static comparisons.
D. Security source data can come from many places, including data streams, messages, threat events, logs, etc.

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

**QUESTION 79**
Use BGP protocol to achieve diversion, the configuration command is as follows [sysname] route-policy 1 permit node 1 [sysname-route-policy] apply community no-advertise [sysname-route-policy] quit [sysname]bgp100 155955cc-666171a2-20fac832-0c042c04 29 [sysname-bgp] peer [sysname-bgp] import-route unr [sysname- bgpl ipv4-family unicast [sysname-bgp-af-ipv4] peer 7.7.1.2 route-policy 1 export [sysname-bgp-af-ipv4] peer 7.7.1.2 advertise community [sysname-bgp-af-ipv4] quit [sysname-bgp]quit Which of the following options is correct for the description of BGP diversion configuration?
(multiple choice)

A. Use BGP to publish UNR routes to achieve dynamic diversion.
B. After receiving the UNR route, the peer neighbor will not send it to any BGP neighbor.
C. You also need to configure the firewall ddos bgp-next-hop fib-filter command to implement backinjection.
D. The management center does not need to configure protection objects. When an attack is discovered, it automatically issues a traffic diversion task.

**Correct Answer: A, B**
**Section:**

**QUESTION 80**

Which of the following options does not belong to the security risk of the application layer of the TCP/IP protocol stack?

A. Virus

B. Buffer overflow ?

C. System vulnerabilities

D. Port scan

**Correct Answer: D**
**Section:**

**QUESTION 81**

Intrusion detection is a network security technology used to detect any damage or attempt to damage the confidentiality, integrity or availability of the system. Which of the following What is the content of the intrusion detection knowledge base?

A. Complete virus sample

B. Complete Trojan Horse

C. Specific behavior patterns

D. Security Policy

**Correct Answer: C**
**Section:**

**QUESTION 82**

The administrator has configured file filtering to prohibit internal employees from uploading development files, but internal employees can still upload development files. Which of the following is not allowed Can the reason?

A. The file filtering configuration file is not referenced in the security policy

B. File filtering configuration file is incorrect

C. License is not activated.

D. The action configuration of the file extension does not match is incorrect

**Correct Answer: D**
**Section:**

**QUESTION 83**

Regarding the Anti-DDoS cloud cleaning solution; which of the following statements is wrong?

A. Ordinary attacks will usually be cleaned locally first.

B. If there is a large traffic attack on the network, send it to the cloud cleaning center to share the cleaning pressure.

C. Since the Cloud Cleaning Alliance will direct larger attack flows to the cloud for cleaning, it will cause network congestion.

D. The closer to the attacked self-labeled cloud cleaning service, the priority will be called.
155955cc-666171a2-20fac832-0c042c0430

**Correct Answer: C**
**Section:**

**QUESTION 84**

The processing flow of IPS has the following steps;

A. Reorganize application data
B. Match the signature
C. Message processing
D. Protocol identification
   Which of the following is the correct order of the processing flow?
E. 4-1-2-3
F. 1-4-2-3
G. 1-3-2-4
H. 2-4-1-3:

**Correct Answer: B**
**Section:**

**QUESTION 85**
An enterprise administrator configures the Web reputation system as shown in the figure. Regarding the configuration, which of the following statements is correct?



A. The content in No. 2 must be configured.
B. In addition to this page configuration, you also need to enable the firewall and sandbox linkage, otherwise the page configuration is invalid
C. The content in No. 4 must be configured.
D. After the configuration is completed, you need to submit the configuration to take effect.

**Correct Answer: B**
**Section:**

**QUESTION 86**
In the deployment of Huawei NIP6000 products, only port mirroring can be used for streaming replication.

A. True

B. False

**Correct Answer: B**
**Section:**

**QUESTION 87**
Which of the following is not an abnormal situation of the file type recognition result?

A. The file extension does not match.
B. Unrecognized file type
C. File corruption
D. The file is compressed

**Correct Answer: D**
**Section:**

**QUESTION 88**
For SYIN Flood attacks, TCP source authentication and TCP proxy can be used for defense. Which of the following descriptions is correct?

A. TCP proxy means that the firewall is deployed between the client and the server. When the SYI packet sent by the client to the server passes through the firewall, the The firewall replaces the server and establishes a three-way handshake with the client. Generally used in scenarios where the back and forth paths of packets are inconsistent.
B. During the TCP proxy process, the firewall will proxy and respond to each SYN message received, and maintain a semi-connection, so when the SYN message is When the document flow is heavy, the performance requirements of the firewall are often high.
C. TCP source authentication has the restriction that the return path must be consistent, so the application of TCP proxy is not common. State "QQ: 9233
D. TCP source authentication is added to the whitelist after the source authentication of the client is passed, and the SYN packet of this source still needs to be verified in the future.

**Correct Answer: B**
**Section:**

**QUESTION 89**
Which of the following technologies can achieve content security? (multiple choice)

A. Web security protection
B. Global environment awareness
C. Sandbox and big data analysis
D. Intrusion prevention

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

**QUESTION 90**
Which of the following iterations is correct for the description of the management center?

A. The management server of the management center is responsible for the cleaning of abnormal flow, as well as the collection and analysis of business data, and storage, and is responsible for the summary The stream is reported to the management server for report presentation.
B. The data coking device is responsible for the cleaning of abnormal flow, the centralized management and configuration of equipment, and the presentation of business reports.
C. The data collector and management server support distributed deployment and centralized deployment. Centralized deployment has good scalability.

D. The management center is divided into two parts: management server and teaching data collector.

**Correct Answer: D**
**Section:**

**QUESTION 91**
The IPS function of Huawei USG6000 supports two response methods: blocking and alarming.

A. True
B. False

**Correct Answer: A**
**Section:**

**QUESTION 92**
If the Huawei USG600 product uses its own protocol stack cache for all files passing through the device and then performs a virus scan, then the device uses It is the stream scanning method.

A. True
B. False

**Correct Answer: B**
**Section:**

**QUESTION 93**
When the device recognizes a keyword during content filtering detection, which response actions can the device perform? (multiple choice)

A. Warning
B. Block
C. Declare
D. Operate by weight

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

**QUESTION 94**
Which of the following options is wrong for the description of the cleaning center?

A. The cleaning center completes the functions of drainage, cleaning, and re-injection of the flow after cleaning in the abnormal flow.
B. There are two types of drainage methods: static drainage and dynamic drainage.
C. Re-injection methods include: policy route re-injection, static route re-injection, VVPN backinjection and layer 2 same.
D. The cleaning equipment supports rich and flexible attack prevention technologies, but it is ineffective against cc attacks and ICMP Flood attacks.

**Correct Answer: D**
**Section:**

**QUESTION 95**
Regarding Huawei's anti-virus technology, which of the following statements is wrong?

A. The virus detection system cannot directly detect compressed files

B. The anti-virus engine can detect the file type through the file extension

C. Gateway antivirus default file maximum decompression layer is 3 layers

D. The implementation of gateway antivirus is based on proxy scanning and stream scanning

**Correct Answer: B**
**Section:**

**QUESTION 96**
When you suspect that the company's network has been attacked by hackers, you have carried out a technical investigation. Which of the following options does not belong to the behavior that occurred in the early stage of the attack?

A. Planting malware

B. Vulnerability attack"

C. We6 Application Click

D. Brute force

**Correct Answer: A**
**Section:**

**QUESTION 97**
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

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

**QUESTION 98**
Threats detected by the big data intelligent security analysis platform will be synchronized to each network device at the same time C and then collected from the network device Collect it in the log for continuous learning and optimization.

A. True
155955cc-666171a2-20fac832-0c042c0433

B. False

**Correct Answer: A**
**Section:**

**QUESTION 99**
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

**Correct Answer: A**
**Section:**

**QUESTION 100**
Which of the following options are the possible reasons why a certain signature is not included after the IPS policy configuration is completed? (multiple choice)

A. Direction is not enabled

B. The direction is turned on, but no specific direction is selected

C. The severity level of the configuration is too high

D. The protocol selection technique is correct

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

**QUESTION 101**
Which of the following descriptions about viruses and Trojans are correct? (multiple choices)

A. Viruses are triggered by computer users

B. Viruses can replicate themselves

C. Trojan horses are triggered by computer users

D. Trojans can replicate themselves

**Correct Answer: A, B**
**Section:**

**QUESTION 102**
After enabling the IP policy, some services are found to be unavailable. Which of the following may be caused by? (multiple choice)

A. Only packets in one direction pass through the firewall

B. The same message passes through the firewall multiple times

C. IPS underreporting

D. Excessive traffic causes the Bypass function to be enabled

**Correct Answer: A, B**
**Section:**

**QUESTION 103**
URL filtering technology can perform URL access control on users according to different time objects and address objects to achieve precise management of users.
The purpose of the Internet behavior.

A. True

B. False

**Correct Answer: A**

**Section:**

**QUESTION 104**
Which of the following are the control items of HTTP behavior?) (multiple choice)

A. POST operation
B. Browse the web
C. Acting online
D. File upload and download

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

**QUESTION 105**
Which of the following options is correct for the sequence of the flow-by-stream detection of AntiDDoS?

A. The Netflow analysis device samples the current network flow;
B. Send a drainage command to the cleaning center;
C. Discover the DDoS attack stream;
D. Netior: analysis equipment sends alarms to ATIC management center
E. The abnormal flow is diverted to the cleaning center for further inspection and cleaning; 6. The cleaning center sends the host route of the attacked target IF address server to the router to achieve drainage 7. The cleaning log is sent to the management center to generate a report; 8. The cleaned traffic is sent to the original destination server.
F. 1-3-4-2-5-6-7-8
G. 1-3-2-4-6-5-7-8
H. 1-3-4-2-6-5-8-7
I. 1-3-24-6-5-8-7

**Correct Answer: C**
**Section:**

**QUESTION 106**
File filtering technology can filter files based on the application of the file, the file transfer direction, the file type and the file extension.

A. True
B. False

**Correct Answer: A**
**Section:**

**QUESTION 107**
The anti-virus feature configured on the Huawei USG6000 product does not take effect. Which of the following are the possible reasons? (multiple choice)

A. The security policy does not reference the anti-virus configuration file.
B. The anti-virus configuration file is configured incorrectly.
C. The virus signature database version is older.
D. No virus exceptions are configured.

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

**QUESTION 108**
After the user deploys the firewall anti-virus strategy, there is no need to deploy anti-virus software

A. True
B. False.

**Correct Answer: B**
Section:

**QUESTION 109**
Which of the following descriptions are correct for proxy-based anti-virus gateways? (multiple choice)

A. The detection rate is higher than the flow scanning method
B. System overhead will be relatively small
C. Cache all files through the gateway's own protocol stack
D. More advanced operations such as decompression, shelling, etc. can be performed

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

**QUESTION 110**
When the license of Huawei USG6000 product expires, the RBL function will be unavailable, and users can only use the local black and white list to filter junk mail.
155955cc-666171a2-20fac832-0c042c0435

A. True
B. False

**Correct Answer: A**
Section:

**QUESTION 111**
For the description of the principles of HTTP Flood and HTTPS Flood blow defense, which of thefollowing options are correct? (multiple choice)

A. HTTPS Flood defense modes include basic mode, enhanced mode and 302 redirection.
B. HTTPS Flood defense can perform source authentication by limiting the request rate of packets.
C. The principle of HTTPS Flood attack is to request URIs involving database operations or other URIsthat consume system resources, causing server resource consumption.
   Failed to respond to normal requests.
D. The principle of HTTPS Flood attack is to initiate a large number of HTTPS connections to thetarget server, causing the server resources to be exhausted and unable to respond to regularrequests.begging.

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

**QUESTION 112**
Under the CLI command, which of the following commands can be used to view the AV engine and virus database version?

A. display version av-sdb
B. display utm av version
C. display av utm version
D. display utm version

**Correct Answer: A**
**Section:**

**QUESTION 113**
Which of the following statement is correct about Policy Center system client function?

A. NAC Agent support MAC account login.
B. Web page login for authentication and can perform checks Strategy.
C. Web Agent login for identity certification and security certification.
D. NAC Agent cannot be installed on Windows Vista operating system.

**Correct Answer: A**
**Section:**

**QUESTION 114**
Which of the following elements does PDCA include? (Choose 3 answers)

A. Plan
B. Implementation
C. termination
D. Monitoring

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

**QUESTION 115**
Place refers to the terminal environment when end-user use strategy management center access to controlled network office, which options are correct about place? (Choose 2 answers)

A. strategy management center only support the default place
B. The default place only support by way of cable access network scenario
C. can be customized places
D. when allocation strategy template for the end user, need to select the corresponding places

**Correct Answer: C, D**
**Section:**

**QUESTION 116**
Terminal fault diagnosis tool can diagnose fault, also can collect terminal information.

A. TRUE
B. FALSE

**Correct Answer: A**
Section:

**QUESTION 117**
An enterprise has 3 server, which is the most reasonable plan when deploy Policy Center system planning?

A. manager + controller + FTP + witness database, controller + master database + FTP, controller + mirror database+ FTP
B. manager + controller + FTP + master database, controller + FTP + witness database, controller + FTP + mirror database
C. manager + controller + FTP + mirror database, controller + FTP + witness database, controller + FTP + master database
D. manager + controller + FTP, controller + FTP + witness databases, controller + FTP + master database

**Correct Answer: A**
Section:

**QUESTION 118**
SACG query right-manager information as follows, which options are correct? (Select 2 answers)

```
[USG2200]dis right-manager server-group
17:35:21  2013/10/14
Server group state  :  Enable
Server number       :   1
Server ip address      Port   State      Master
   1.1.1.2            3288    active       Y
   2.1.1.1            3288    active       N
```

A. SACG and IP address 2.1.1.1 server linkage is not successful
B. SACG linkage success with controller.
C. master controller IP address is 1.1.1.2.
D. master controller IP address is 2.1.1.1.

**Correct Answer: A, B**
Section:

**QUESTION 119**
For full encryption registered mobile storage devices must be formatted to normal use in not installed NAC client terminal host.

A. TRUE
B. FALSE

**Correct Answer: A**
Section:

**QUESTION 120**
What equipment do Policy Center supported servers include? (Choose 3 answers)

A. remote control device
B. mail server

C. Internet behavior management equipment

D. log collection server

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

**QUESTION 121**
Which of the following technology, administrators can according to business requirements, to scale to achieve load sharing of business flow?

A. Resource pool mechanism

B. weighting mechanism

C. load balancing

D. Hot Standby

**Correct Answer: A, B**
**Section:**

**QUESTION 122**
Which is correct about the following Policy Center troubleshooting process?

A. Hardware fault-> connection fault-> NAC client fault-> Policy Center server fault

B. connection fault-> Hardware fault-> NAC client fault-> Policy Center server fault

C. Hardware fault-> connection fault-> Policy Center server fault-> NAC client fault

D. hardware fault-> NAC client fault-> connection fault-> Policy Center server fault

**Correct Answer: A**
**Section:**

**QUESTION 123**
The following is a hardware SACG increase firewall configuration, which statement below is true?
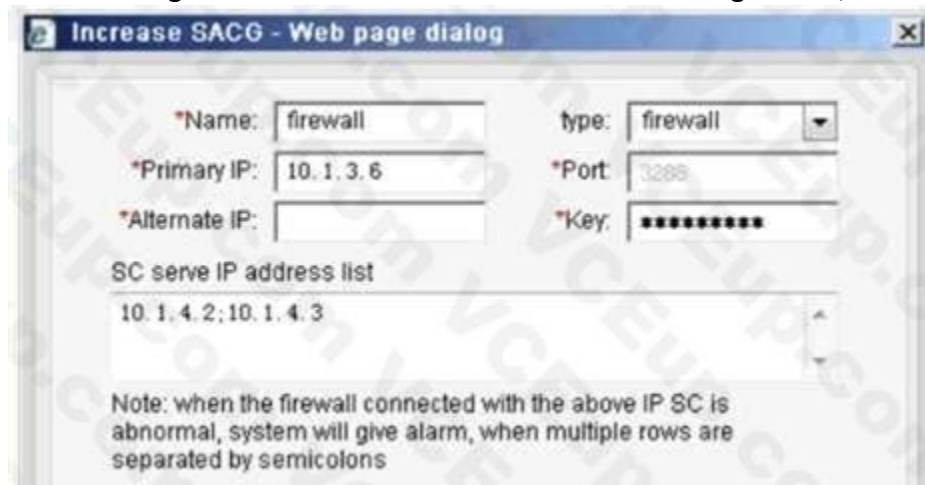


A. Primary IP: 10.1.3.6 on behalf of SM Manager IP address.

B. Primary IP: 10.1.3.6 on behalf of Policy Center linkage firewall interface IP address, the standby IP can enter another interface IP address of the firewall.

C. Primary IP: 10.1.3.6 on behalf of Policy Center linkage firewall interface IP address, the standby IP can enter another alternate firewall interface IP address.

D. Main IP is the Policy Center reaches the next-hop firewall device interface address

**Correct Answer: A, C**
**Section:**

**QUESTION 124**
Which of the following is the default port number of Portal authentication service?

A. 1812
B. 1813
C. 50200
D. 50300

**Correct Answer: A, C**
**Section:**

**QUESTION 125**
When configuring the terminal visits, we put some equipment configured exception equipment ,which of the following statements are true about the exception equipment?

A. the exception equipment IP is not in controlled network segment.
B. terminal in isolation domain can not access exception equipment .
C. only through security authentication terminals can access exception equipment.
D. through identity authentication terminals can access exception equipment.

**Correct Answer: A, D**
**Section:**

**QUESTION 126**
Which patches does Policy Center support to management?(Choose 3 answers)

A. Microsoft Windows operating system patches
B. Microsoft SQL Windows database patch
C. Microsoft Internet Explorer patches
D. android system patches

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

**QUESTION 127**
SQI Server2005 may not be properly installed, which of the following may be the possible reasons?

A. 1433 port are occupied by the other processes
B. equipment 21 port is occupied
C. without prior installation of Microsoft SQL Server 2005 Toolkit
D. The operating system is Microsoft Windows Server 2003

**Correct Answer: A**
**Section:**

**QUESTION 128**
Which of the following options are right 802. 1X The description of the access process is correct?
(Multiple choice).

A. Through the entire authentication process, the terminal passes EAP The message exchanges information with the server.
B. Terminal and 802.1X Switch EAP Message interaction,802.1X Switch and server use Radius Message exchange information
C. 802.1X Authentication does not require security policy checks.
D. use MD5 The algorithm checks the information.

**Correct Answer: B, D**
**Section:**

**QUESTION 129**
BY00 The products and textiles provided by the history solution program cover the entire terminal network\Application and management and other fields/include: Serialization BC Equipment, paperless network system network access support, VPN Gateway, terminal security customer ladder software, authentication system, mobile device management(MDN),move eSpace UC.

A. True
B. False

**Correct Answer: A**
**Section:**

**QUESTION 130**
For the terminal Wi-Fi The order of the push, which of the following is correct?

A. Any Office Mobile office system push Wi-Fi Configuration
B. Any Office The mobile office department automatically applies for a certificate.
C. The administrator configures the enterprise Wi-Fi Push.
D. The terminal automatically connects to the enterprise Wi-Fi.
E. 1-2-3-4
F. 4-2-3-1
G. 3-2-1-4
H. 2-3-1-4

**Correct Answer: C**
**Section:**

**QUESTION 131**
Which of the following options is right PKI The sequence description of the work process is correct?

A. PKI Entity direction CA ask CA Certificate. .
B. PKI Entity received CA After the certificate, install CA Certificate.
C. CA receive PKI Entity CA When requesting a certificate, add your own CA Certificate reply to PKI entity.
D. PKI Entity direction CA Send a certificate registration request message.
E. PKI When the entities communicate with each other, they need to obtain and install the local certificate of the opposite entity.
F. PKI Entity received CA The certificate information sent.

G. PKI After the entity installs the local certificate of the opposite entity,Verify the validity of the local certificate of the peer entity. When the certificate is valid,PC The public key of the certificate is used for encrypted communication between entities.

H. CA receive PKI The entity's certificate registration request message.

I. 1-3-5-4-2-6-7-8

J. 1-3-5-6-7-4-8-2

K. 1-3-2-7-6-4-5-8

L. 1-3-2-4-8-6-5-7

**Correct Answer: D**
Section:

**QUESTION 132**
About in WLAN User isolation technology is used in the networking environment. Which of the following statements is wrong?

A. User isolation between groups means that users in different groups cannot communicate, but internal users in the same group can communicate

B. Isolation within a user group means that users within the same group cannot communicate with each other.

C. The user isolation function is related to the same AP Layer 2 packets between all wireless users on the Internet cannot be forwarded to each other

D. Intra-group isolation and inter-group isolation cannot be used at the same time

**Correct Answer: D**
Section:

**QUESTION 133**
When using local guest account authentication, usually use(Portal The authentication method pushes the authentication page to the visitor. Before the user is authenticated, when the admission control device receives the HTTP The requested resource is not Portal Server authentication URL When, how to deal with the access control equipment.

A. Discard message

B. URL Address redirected to Portal Authentication page

C. Direct travel

D. Send authentication information to authentication server

**Correct Answer: B**
Section:

**QUESTION 134**
The administrator issues notices to users in the form of announcements, such as the latest software and patch installation notices. Which of the following options of the announcement is incorrect?

A. Announcements can be issued by the security department

B. The terminal must have a proxy client installed to receive announcements.

C. If the system issues an announcement and the proxy client is not online, the announcement information will not be received after going online.

D. Announcements can be issued by account.

**Correct Answer: C**
Section:

**QUESTION 135**
When managing guest accounts, you need to create a guest account policy and set the account creation method. For the account creation method, which of the following descriptions is wrong?

A. When adding accounts individually, you can choose to create them individually.

B. If there are a lot of users, you can choose to create in batches.

C. If there are many users, you can choose database synchronization

D. In order to facilitate management and improve user experience, self-registration can be used.

**Correct Answer: C**
**Section:**

**QUESTION 136**
On WIDS functional WLAN Regarding the judgment of illegal devices in the network, which of the following statements are correct? (Multiple choice)

A. all Ad-hoc The device will be directly judged as an illegal device

B. Not this AC Access AP Is illegal AP

C. Not this AC Access STA Is illegal STA

D. Not this AC Access STA,Also need to check access AP Does it contain law

**Correct Answer: A, D**
**Section:**

**QUESTION 137**
Wired 802.1X During authentication, if the access control equipment is deployed at the Jiangju layer, this deployment method has the characteristics of high security performance, multiple management equipment, and complex management.

A. True

B. False

**Correct Answer: B**
**Section:**

**QUESTION 138**
Which of the following options is for Portal The description of the role of each role in the authentication system is correct?

A. The client is Any 0fice software.

B. Portal The role of the server is to receive client authentication requests, provide free portal services and authentication interfaces, and exchange client authentication information with access devices.

C. RADIUS The role of the server is to authenticate all the users in the network segment HTTPRequests are redirected to Portal server.

D. The role of admission control equipment is to complete the authentication, authorization and accounting of users.

**Correct Answer: B**
**Section:**

**QUESTION 139**
Which of the following options are relevant to MAC Certification and MAC The description of bypass authentication is correct? (Multiple choice)

A. MAC Certification is based on MAC The address is an authentication method that controls the user's network access authority. It does not require the user to install any client software.

B. MAC Bypass authentication is first performed on the devices that are connected to the authentication 802 1X Certification;If the device is 802. 1X No response from authentication, re-use MAC The authentication method verifies the legitimacy of the device.

C. MAC During the authentication process, the user is required to manually enter the user name or password.

D. MAC The bypass authentication process does not MAC The address is used as the user name and password to automatically access the network.

**Correct Answer: A, B**
**Section:**

**QUESTION 140**
About the hardware SACG Certification deployment scenarios, which of the following descriptions are correct? (Multiple choice)

A. SACG Authentication is generally used in scenarios where a stable network performs wired admission control.

B. SACG Authentication is generally used in scenarios where new networks are used for wireless admission control.

C. SACG It is generally deployed in a bypass mode without changing the original network topology.

D. SACG Essentially through 802.1X Technology controls access users.

**Correct Answer: A, C**
**Section:**

**QUESTION 141**
Traditional network single--The strategy is difficult to cope with the current complex situations such as diversified users, diversified locations, diversified terminals, diversified applications, and insecure experience.

A. True

B. False

**Correct Answer: A**
**Section:**

**QUESTION 142**
A network adopts Portal Authentication, the user finds the pushed Web No username entered on the page/The place of the password. This failure may Which of the following causes?

A. Agile Controller-Campus There is no corresponding user on.

B. switch AAA Configuration error.

C. The switch is not turned on Portal Function.

D. Portal The push page on the server is wrong.

**Correct Answer: D**
**Section:**

**QUESTION 143**
Portal The second-level authentication method of authentication refers to the direct connection between the client and the access device(Or only layer devices exist in between),The device can learn the user's MAC Address and can be used IP with MAC Address to identify the user.

A. True

B. False

**Correct Answer: A**
**Section:**

**QUESTION 144**

Mobile smartphone, tablet PC users through Any Office Client and AE Establish IPSec Encrypted tunnel, After passing the certification and compliance check, visit the enterprise business.

A.  True
B.  False

**Correct Answer: B**
**Section:**

**QUESTION 145**
Typical application scenarios of terminal security include: Desktop management, illegal outreach and computer peripheral management.

A.  True
B.  False

**Correct Answer: A**
**Section:**

**QUESTION 146**
Web Standards that come with the client and operating system 8021 The instrument client only has the function of identity authentication: It does not support the execution of inspection strategies and monitoring strategies. Any Office The client supports all inspection strategies and monitoring strategies.

A.  True
B.  False

**Correct Answer: A**
**Section:**

**QUESTION 147**
MAC Certification refers to 802.1x In the protocol authentication environment, the terminal does not respond to the connection control device after accessing the network 802.1x When protocol authentication is requested, the access control does not automatically obtain the terminal's MAC The address is sent as a credential to access the network RADIUS The server performs verification.

A.  True
B.  False

**Correct Answer: B**
**Section:**

**QUESTION 148**
Sort all services according to user group and account: By the end IP The address range is timesharing, if it is a user group, a small terminal with an account IP Address range allocation for the same business(Chen Gongji outside business) I
The business assigned to the one with the highest priority will take effect.
Which of the following is correct regarding the order of priority?

A.  account>user group>terminal IP Address range
B.  By the end P Address range>account number>user group
C.  account>Terminal protection address range>user group
D.  user group>terminal P Address range>Account

**Correct Answer: C**
**Section:**

**QUESTION 149**
The multi-level defense system is mainly reflected in the network level and the system level. Which of the following options are used for security defense at the network level? (Multiple choice)

A. software SACG
B. hardware SACG
C. 802.1X switch
D. Authentication server

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

**QUESTION 150**
Location refers to the end user's use AC-Campus The terminal environment when accessing the controlled network office. Which of the following options is correct for the description of the place?

A. Different places can have different security policies.
B. The location has nothing to do with safety.
C. There can only be one place in the company.
D. Place and location have nothing to do.

**Correct Answer: A**
**Section:**

**QUESTION 151**
Identity authentication determines whether to allow access by identifying the identity of the access device or user.

A. True
B. False

**Correct Answer: A**
**Section:**

**QUESTION 152**
Regarding the description of the account blacklist, which of the following options is wrong?

A. The automatic account lock and manual account lock functions cannot be activated at the same time.
B. For automatically locked accounts, if the number of incorrect passwords entered by the terminal user during authentication exceeds the limited number of times within a limited time, the account will be automatically locked.
C. For manually locked accounts, the administrator needs to manually add the account to the locked account list.
D. Manually lock the account and delete it from the list, the lock of the account will be released.

**Correct Answer: A**
**Section:**

**QUESTION 153**

Agile Controller-Campus All components are supported Windows System and Linux system.

A. True
B. False

**Correct Answer: A**
**Section:**

**QUESTION 154**
According to the user's access5W1H Conditions determine access rights andQoS Strategy for5W1Ho[Which of the following descriptions are correct? (Multiple choice)

A. WhoTo determine the ownership of the access device(Company standard,BYOD Wait)
B. WhoseTo determine the identity of the access person(member I, Visitors, etc.)
C. How Determine the access method(Wired, wireless, etc.)
D. WhatTo determine the access device(PC,iOS Wait)

**Correct Answer: C, D**
**Section:**

**QUESTION 155**
Which of the following cybersecurity threats exist only in WLAN In the network?

A. Brute force
B. Crowd attack
C. DoS Denial of service attack
D. Weak IV attack

**Correct Answer: D**
**Section:**

**QUESTION 156**
After the user is successfully authenticated, Agile Controller-Campus Which of the following actions can be performed on the user(Multiple choice)

A. To use Any Office The connected user performs remote assistance.
B. Force users to go offline.
C. Audit users' online and offline records.
D. Disable the mobile certificate account/Disable and assign roles.

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

**QUESTION 157**
In Portal authentication, which of the following parameters must be configured on the switch?
(Multiple choice)

A. Portal server IP
B. Portal page URL

C. shared-key

D. Portal Protocol version

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

**QUESTION 158**
Use on the terminal Portal The authentication is connected to the network, but you cannot jump to the authentication page. The possible reason does not include which of the following options?

A. Agile Controller-Campus Configured on Portal The authentication parameters are inconsistent with the access control device.

B. Access device Portal The authentication port number of the template configuration is 50100 ,Agile Controlle-Campus The above is the default.

C. CS Did not start

D. When the page is customized, the preset template is used.

**Correct Answer: D**
**Section:**

**QUESTION 159**
Which of the following options is about SACG The description of the online process is wrong?

A. Terminal and Agile Controller-Campus Server communication SSL encryption

B. Authentication fails, end users can only access resources in the pre-authentication domain

C. Security check passed,Agile Controller-Campus Server notification SACG Will end user's IP Address switch to isolated domain

D. Agile Controller-Campus Server gives SACG Carrying domain parameters in the message

**Correct Answer: C**
**Section:**

**QUESTION 160**
Traditional access control policy passed ACL or VLAN Can not be achieved with IP Address decoupling, in IP The maintenance workload is heavy when the address changes. And because the agile network introduces the concept of security group, it can achieve the same IP Address decoupling.

A. True

B. False

**Correct Answer: A**
**Section:**

**QUESTION 161**
Use on access control equipment test-aaa Command test and Radius When the server is connected, the running result shows a timeout, which may be caused by incorrect account or password configuration.

A. True

B. False

**Correct Answer: B**
**Section:**

**QUESTION 162**

Agile Controller-Campus As RADIUS When the server performs authentication, how many ends need to be configured for authentication on the admission control device?

A.  1812

B.  1813

C.  8443

D.  8080

**Correct Answer: A**
**Section:**

**QUESTION 163**
Which of the following options is not a challenge brought by mobile office?

A.  The mobile office platform is safe and reliable and goes online quickly.

B.  Users can access the network safely and quickly.

C.  Unified terminal management and fine control.

D.  Network gateway deployment

**Correct Answer: D**
**Section:**

**QUESTION 164**
Windows in environment,Agile Controller-Campus After the installation is successful, how to manually start the management center(MC)? (Multiple choice)

A.  Double click on the desktop"Start Server"The shortcut starts.

B.  choose"Start>all programs> Huawei> MCServer> StartServer.

C.  choose"Start>all programs> Huawei> Agile Controller> Server Startup Config"To manually start the required components.

D.  choose"Start 3 all programs> Huawei> MCServer> Sever Startup Conig",Manually start the required components

**Correct Answer: A, B**
**Section:**

**QUESTION 165**
When configuring the antivirus software policy, if you set"The required antivirus software violation level is not installed or running"for"generally"And check"out Now serious violation of the rules prohibits access to the network"Options. When the user uses Any office Certify, The certification is passed, but the result of the security check Can the user access the network when the virus software is not turned on?

A.  Can access the network? Can also access network resources.

B.  Cannot access the network.

C.  Can pick up? The network needs to be repaired before you can access network resources.

D.  You can access the network, but you need to re-authenticate to access network resources.

**Correct Answer: C**
**Section:**

**QUESTION 166**
Which of the following methods can be used to protect enterprise terminal security?

A. Access control
B. Encrypted access
C. Business isolation
D. Audit billing

**Correct Answer: A**
**Section:**

**QUESTION 167**
Which of the following options is Agile Controller-Campus middle SC The main function of the component?

A. As Agile Controller-Campus The management center is responsible for formulating the overall strategy.
B. As Agile Controller-Campus The management interface is used to configure and monitor the system.
C. Integrated with standards RADIUS server,Porta Server, etc., responsible for linking with network access equipment to realize user-based network access control Strategy.
D. As Agile Controller-Campus 'S security assistance server, responsible for iRadar Analysis and calculation of reported security incidents.

**Correct Answer: C**
**Section:**

**QUESTION 168**
Import the user information of the AD server on the Agile Controller-Campus to realize the user's access authentication. If the user is in the Agile.
The user information is not found on the Controller-Campus. Which of the following actions will be performed in the next step?

A. Straight forward to return authentication failure information.
B. Discard user information.
C. User 91 Information sent to AD The server performs verification.
D. Synchronize the database again.

**Correct Answer: C**
**Section:**

**QUESTION 169**
VIP Experience guarantee, from which two aspects are the main guarantees VIP User experience?
(Multiple choice)

A. bandwidth
B. Forwarding priority
C. Authority
D. Strategy

**Correct Answer: A, B**
**Section:**

**QUESTION 170**
User access authentication technology does not include which of the following options?

A. Authentication

B.  Isolation repair'

C.  Security check

D.  Access control

**Correct Answer: B**
**Section:**

**QUESTION 171**
In the WLAN wireless access scenario, which of the following network security technologies belong to user access security? (Multiple choice)

A.  AP Certification

B.  Link authentication

C.  User access authentication

D.  data encryption

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

**QUESTION 172**
Which of the following options are relevant to Any Office The description of the solution content is correct? (Multiple choice)

A.  Provide unified and secure access to enterprise mobile applications on mobile terminals.

B.  The tunnel is dedicated and cannot be penetrated by viruses.

C.  Applications are quickly integrated and can be extended.

D.  It can be quickly integrated and docked with the enterprise application cloud platform.

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

**QUESTION 173**
MAC Bypass authentication means that after the terminal is connected to the network, the access control device automatically obtains the terminal MAC Address, which is sent to RADIUS The server performs euverification.

A.  True

B.  False

**Correct Answer: B**
**Section:**

**QUESTION 174**
When the account assigned by the administrator for the guest is connected to the network, the audit action that the administrator can perform on the guest does not include which of the following options?

A.  Visitor online and offline records

B.  Force users to go offline

C.  Account deactivation 1 reset Password

D.  Send a warning message to the user

**Correct Answer: D**

**Section:**

**QUESTION 175**
In the visitor reception hall of a company, there are many temporary terminal users, and the administrator hopes that users do not need to provide any account numbers and passwords. access Internet. Which of the following authentication methods can be used for access?

A. Local account authentication
B. Anonymous authentication
C. AD Account Verification
D. MAC Certification

**Correct Answer: B**
**Section:**

**QUESTION 176**
Agile Controller-Campus The department includes four parts of the management center(MC)Business manager(SM)And business controller(SC)And client network access equipment (NAD)As a component of the solution, it is linked with the service controller to realize user access control and free mobility.

A. True
B. False

**Correct Answer: A**
**Section:**

**QUESTION 177**
Visitors can access the network through their registered account. Which of the following is not an account approval method?

A. Exemption from approval
B. Administrator approval
C. Receptionist approval
D. Self-approved by visitors

**Correct Answer: D**
**Section:**

**QUESTION 178**
Regarding the application scenarios of Agile Controller-Campus centralized deployment and distributed deployment, which of the following options are correct? (Multiple select)

A. If most end users work in one area and a few end users work in branch offices, centralized deployment is recommended.
B. If most end users are concentrated on--Offices in several regions, and a small number of end users work in branches. Distributed deployment is recommended.
C. If end users are scattered in different geographical locations, a distributed deployment solution is recommended.
D. If end users are scattered in different regions, a centralized deployment solution is recommended.

**Correct Answer: A, C**
**Section:**

**QUESTION 179**

Security authentication is mainly achieved through security policies. The terminal host support management for the security check of monthly users is mainly realized by loose check policies. End user behavior management is mainly realized by monitoring policies. If users need to formulate policies according to their own wishes, they can use them. Custom strategy.

A. True

B. False

**Correct Answer: A**
**Section:**

**QUESTION 180**
Portal At the time of certification, pass Web After the browser enters the account password for authentication, it prompts" Authenticating.."The status lasts for a long time before it shows that the authentication is successful. Which of the following reasons may cause this phenomenon?

A. Multiple Agile Controller The same terminal IP Address added Portal" Access terminal IP Address list", Some of them Agile Controller The server and the terminal cannot communicate normally.

B. Portal The template is configured with an incorrect password.

C. Agile Controller-Campus There are too many authorization rules on the "It takes a lot of time to find 835

D. Insufficient curtains of the terminal equipment result in a relatively large delay.

**Correct Answer: A**
**Section:**

**QUESTION 181**
In a WLAN network, intra-group isolation and inter-group isolation can be used at the same time.

A. True

B. False

**Correct Answer: A**
**Section:**

**QUESTION 182**
In the Agile Controller-Campus solution, which device is usually used as the hardware SACG?

A. router

B. switch

C. Firewall

D. IPS

**Correct Answer: C**
**Section:**

**QUESTION 183**
When a guest needs to access the network through an account, which of the following methods can be used to access? (Multiple choice)

A. Create new account

B. Use existing social media accounts

C. No authentication, no account required

D. Scan public QR code

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

**QUESTION 184**
Which of the following options is for Portal The statement of the gateway access process is correct?

A. Portal gateway initiates Radius Challenge request message, including user name and password information
B. The ACL issued by the server to the access gateway is carried in the Portal protocol message
C. Issue policies while performing identity authentication
D. The Portal server needs to pass the security check result to the access gateway device

**Correct Answer: D**
Section:

**QUESTION 185**
In the terminal security all-round defense system, use PPT-PDCA The model can effectively implement terminal security defense. Which of the following options does not belong to PPT Model?

A. technology
B. Process
C. organization
D. plan

**Correct Answer: D**
Section:

**QUESTION 186**
The traditional campus network is based on IP As the core network, if there are mobile office users, which of the following options is not the problem that mobile office users face when deploying access authentication?

A. The user distribution range is large, and the access control requirements are high.
B. The deployment of the access control strategy is significant.
C. Access rights are difficult to control.
D. User experience technology

**Correct Answer: A**
Section:

**QUESTION 187**
Which of the following options is not included in the mobile terminal life cycle?

A. Obtain
B. deploy
C. run
D. Uninstall

**Correct Answer: D**

**Section:**

**QUESTION 188**
In the process of establishing CAPWAP channel between AP and AC, AP and AC negotiate to establish CAPWAP tunnel. In this process, CAPWAP tunnel is established.
Use DTLS to encrypt and transmit UDP packets. What are the encryption methods supported by DTLS? (multiple choice)

A. Certificate encryption

B. AES encryption

C. PSK encryption

D. Plaintext encryption

**Correct Answer: A, C**
**Section:**

**QUESTION 189**
When performing terminal access control, the authentication technology that can be used does not include which of the following options?

A. 8021X Certification

B. SACG Certification p2-

C. Bypass authentication

D. Portal Certification

**Correct Answer: C**
**Section:**

**QUESTION 190**
There are three roles in the XMPP protocol: server, gateway, and client. Corresponding to the free mobility solution: Agile Controller-Campus as For the server, Huawei USG6000 series firewall acts as the gateway; the agile switch acts as the client.

A. True

B. False

**Correct Answer: B**
**Section:**

**QUESTION 191**
In order to increase AP The security can be AC Going online AP Perform authentication. Currently Huawei AC What are the supported authentication methods? (Multiple choice)

A. MAC Certification

B. Password authentication

C. Not certified:

D. SN Certification

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

**QUESTION 192**

Which of the following options is not a cyber security threat caused by weak personal security awareness?

A. Disclosure of personal information
B. Threats to the internal network
C. Leaking corporate information
D. Increasing the cost of enterprise network operation and maintenance

**Correct Answer: D**
**Section:**

**QUESTION 193**
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

**Correct Answer: A, B**
**Section:**

**QUESTION 194**
The most common form of child-like attack is to send a large number of seemingly legitimate packets to the target host through Flood, which ultimately leads to network bandwidth. Or the equipment resources are exhausted. Which of the following options is not included in traffic attack packets?

A. TCP packets
B. UDP packet
C. ICMP message
D. FTP message

**Correct Answer: D**
**Section:**

**QUESTION 195**
Buffer overflows, Trojan horses, and backdoor attacks are all attacks at the application layer.

A. True
B. False

**Correct Answer: A**
**Section:**

**QUESTION 196**
The user needs of a university are as follows:

A. 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.
B. 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.

C. 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

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

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

F. 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

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

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

**QUESTION 197**
For special message attacks, which of the following option descriptions is correct?

A. Special control packet attack is a potential attack and does not have direct destructive behavior

B. The attacker probes the network structure by sending special control messages to launch a real attack.

C. Special control message attacks do not have the ability to detect the network structure. Only scanning attacks can detect the network.

D.

**Correct Answer:**
**Section:**
**Explanation:**
Answer:
Explanation:

**QUESTION 198**
When the Anti DDoS system finds the attack flow, the state will redirect the attack flow to the cleaning device. After the cleaning device is cleaned, it will flow back.
Note to the original link, which of the following options does not belong to the method of reinjection?

A. Policy routing back annotation,

B. GRE back note:

C. MPLS LSP back injection

D. BGP back-annotation

**Correct Answer: D**
**Section:**

**QUESTION 199**
Portal page push rules have priority, and the rules with higher priority are matched with the user's authentication information first. If none of the configured rules match, The default rules are used.

A. True

B. False

**Correct Answer: A**
**Section:**

**QUESTION 200**

The following is the 802.1X access control switch configuration:

[S5720]dot1x authentication-method eap
[S5720-GigabitEthernet0/0/1] port link-type access
[S5720-GigabitEthemet0/0/1] port default vlan 11
[S5720-GigabitEthernet0/0/1] authentication dot1x

Assuming that GE0/0/1 is connected to user 1 and user 2 through the HUB, which of the following options is correct?

A. After user 1 is authenticated, user 2 can access network resources without authentication

B. User 1 and User 2 must be individually authenticated before they can access network resources

C. GE0/0/1 does not need to enable dot1X

D. Neither user 1 nor user 2 can pass the authentication and access network resources.

**Correct Answer: A**
**Section:**

**QUESTION 201**
Using Agile Controller-Campus for visitor management, users can obtain the account they applied for in a variety of ways, but which of the following are not included A way?

A. Short message

B. E-mail

C. Web Print

D. Voicemail

**Correct Answer: D**
**Section:**

**QUESTION 202**
Jailbroken mobile terminal\Mobile terminals with non-compliant applications installed or terminals with non-compliant lock screen passwords connecting to the corporate network for office operations are not safe for companies. Any 0fice
How to solve the problem of mobile office system?

A. Directly discard data sent by devices that do not comply with regulations

B. Certification of non-compliant equipment.

C. Check for non-compliant terminals, Prohibit unsafe devices from accessing the network.

D. Send alarm information to notify the administrator to deal with it.

**Correct Answer: C**
**Section:**