

DUMPSQUEEN

HCIP-Security-CSSN V3.0

Huawei H12-722 V3.0

Version Demo

Total Demo Questions: 10

Total Premium Questions: 192

Buy Premium PDF

<https://dumpsqueen.com>

support@dumpsqueen.com

dumpsqueen.com

QUESTION NO: 1

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

- A. It cannot effectively prevent the virus from spreading from the Internet to the intranet.
- B. The number of applications that NIP6000 can recognize reaches 6000+, which realizes refined application protection, saves export bandwidth, and guarantees key business services

Experience.

- C. Protect the intranet from external attacks, and inhibit malicious flows, such as spyware, worms, etc. from flooding and spreading to the intranet.
- D. Ability to quickly adapt to threat changes

ANSWER: B C D

QUESTION NO: 2

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.

ANSWER: B

QUESTION NO: 3

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.

ANSWER: A D

QUESTION NO: 4

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

ANSWER: A B C D

QUESTION NO: 5

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 back-injection.
- D. The management center does not need to configure protection objects. When an attack is discovered, it automatically issues a traffic diversion task.

ANSWER: A B

QUESTION NO: 6

Which of the following options describes the IntelliSense engine IAE incorrectly?

- A. IAE's content security detection functions include application identification and perception, intrusion prevention, and Web application security.
- B. Full English name: intelligent Awareness Engine.
- C. The core of C.IAE is to organically centralize all content security-related detection functions.
- D. The security detection of the IAE engine is parallel, using a message-based file processing mechanism, which can receive file fragments and perform security checks.

ANSWER: D

QUESTION NO: 7

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

ANSWER: B

QUESTION NO: 8

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

- A.** HTTP POST is generally used to send information to the server through a web page, such as forum posting x form submission, username I password login.
- B.** When the file upload operation is allowed, the alarm threshold and blocking threshold can be configured to control the size of the uploaded file.
- C.** When the size of the uploaded or downloaded file and the size of the content of the POST operation reach the alarm threshold, the system will generate log information to prompt the device management

And block behavior.

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

ANSWER: D

QUESTION NO: 9

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

ANSWER: D

QUESTION NO: 10

Tianyu Nei answered the role of safety filtering technology, which of the following is still correct? (multiple choice)

- A.** File filtering can reduce the risk of malicious code execution and virus infection in the internal network by blocking the transmission of fixed types of files, and it can also prevent

Prevent employees from leaking company confidential documents to the Internet.

B. Content filtering can prevent the disclosure of confidential information and the transmission of illegal information

C. The application behavior control function can finely control common HTTP behaviors and FTP behaviors.

D. Mail filtering refers to the management and control of mail sending and receiving, including preventing the flooding of spam and anonymous emails, and controlling the sending and receiving of illegal emails.

ANSWER: A B C D