DUMPS⚜ARENA

HCNP-Security-CISN (Huawei Certified Network Professional - Constructing Infrastructure of Security Network)

Huawei H12-721

Version Demo

Total Demo Questions: 15

Total Premium Questions: 245

Buy Premium PDF

QUESTION NO: 1

A SSL VPN login authentication is unsuccessful, and the prompt says "wrong user name or password." What is wrong?

A. The username and password entered incorrectly.

B. There is a user or group filter field configuration error.

C. There is a certificates filter field configuration error.

D. The administrator needs to configure the source IP address of the terminal restriction policy.

ANSWER: D

QUESTION NO: 2

As shown in Figure, firewall is in stateful failover networking environment, the firewall interfaces are in the business routing mode, and up and down are the router with OSPF configured.
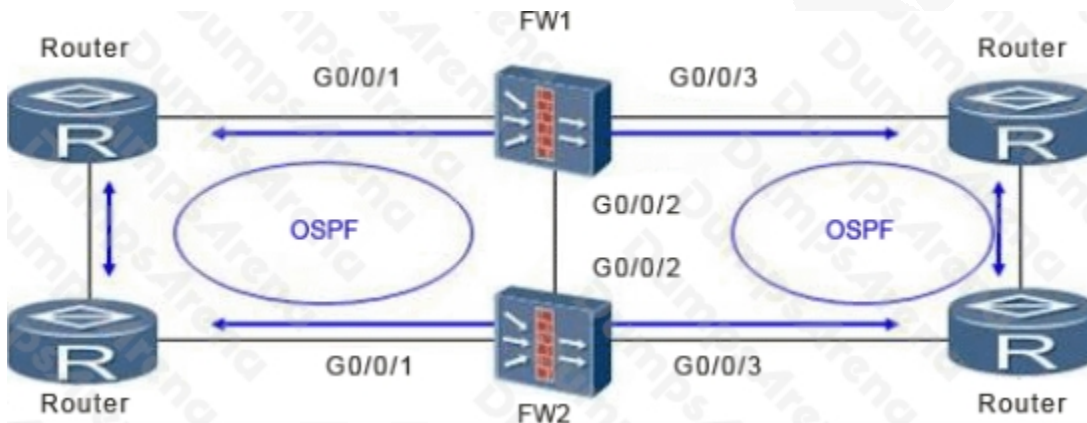
Assuming the OSPF protocol convergence Recovery time is 30s, following best configuration management is to seize on the HRP?

A. hrp preempt delay 20

B. hrp preempt delay 40

C. hrp preempt delay 30

D. undo hrp preempt deplay
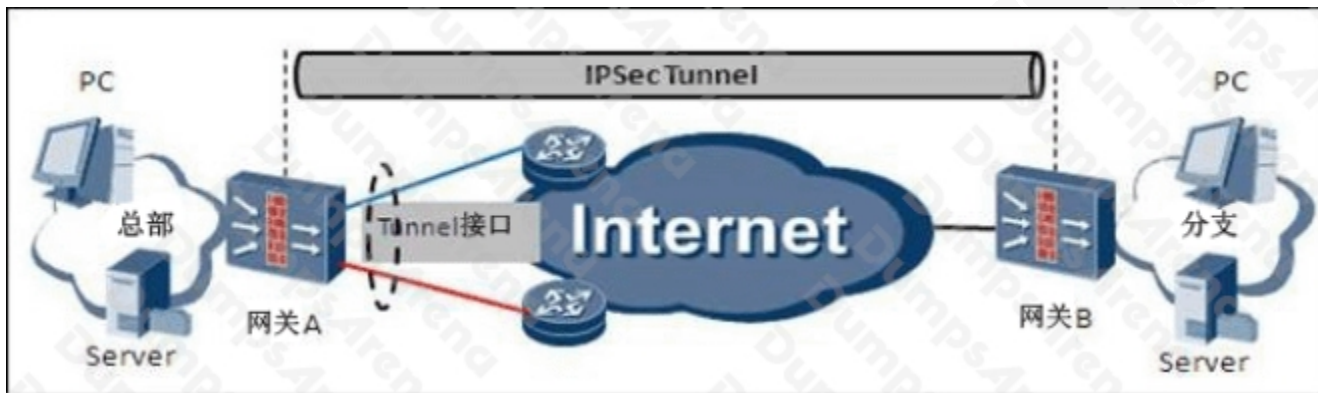
ANSWER: B

QUESTION NO: 3

Which of the following is the role of Message5 and Message6 with the main mode IKE negotiation process?

A. Runs the DH algorithm

B. negotiate set of proposals

C. mutual authentication

D. negotiate IPsec SA

ANSWER: C

QUESTION NO: 4

In standby IPsec link backup scenarios like the one shown below, you can use the link IPsec tunneling technology.

A. TRUE

B. FALSE

ANSWER: A

QUESTION NO: 5

In USG equipment, which statement is correct on current-configuration files and saved-configuration profile? (Choose two answers)

A. ELI administrators to configure a feature USG device, the device will modify Saved-configuration immediately.

B. See the next startup configuration file to load the device display saved-configuration.

C. When executing the Save command, the device will be current-configuration is copied to the saved-configuration.

D. When executing the Save command, current-configuration commands to take effect.

ANSWER: B C

QUESTION NO: 6

BFD static route topology is shown in Figure A. On the firewall, administrator needs to do the following configuration:
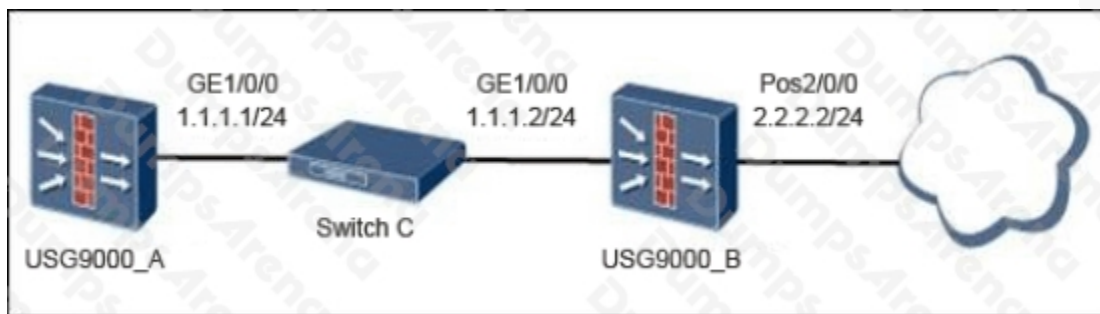
[USG9000_A] bfd

[USG9000_A-bfd] quit

[USG9000_A] bfd aa bind peer-ip 1.1.1.2

[USG9000_A-bfd-session-aa] discriminator local 10

[USG9000_A-bfd-session-aa] discriminator remote 20

Which of the following commands should be added to the firewall configuration to achieve BFD for static route? (Choose two answers)

A. [USG9000_A-bfd-session-aa] commit

B. [USG9000_A] bfd aa bind local-ip 1.1.1.1

C. [USG9000_A] ip route-static 0.0.0.0 0 1.1.1.2 track bfd-session aa

D. [USG9000_A] ip route-static 0.0.0.0 0 1.1.1.2 bind bfd-session aa

ANSWER: A C

QUESTION NO: 7

Which of the following statements is wrong regarding IPsec?

A. Under Transfer Mode, ESP does not validate the IP header

B. AH can not verify that the data uses encrypted packets

C. ESP can support NAT traversal

D. The AH protocol uses the 3DES algorithm for data validation

ANSWER: D

QUESTION NO: 8

An administrator using the following command to view the state of device components

```
<sysname> display device
Slot #    Type        Online    Status
- - - - - - - - - - - - - - - - - - - - - - - - - - -
0         RPU         Present   Normal
3         ADSL2+       Present  Abnormal
4         PWR         Present   Normal
5         FAN         Present   Normal
```

Slot3 board is status abnormal, what are the possible causes? (Choose three answers)

A. The device does not support this interface cards.

B. The Interface Card is damaged.

C. The backplane or damaged pins on the motherboard, such as incorrect installation lead pin board tilt.

D. The ADSL phone line is faulty.

ANSWER: A B C

QUESTION NO: 9

Which of the following statements is correct one for the dual hot standby in conjunction with IPSec functionality?

A. USG supports IPsec primary backup mode of hot standby.

B. Load does not support IPsec stateful failover under balancing.

C. You must configure the session fast backup.

D. You must configure preemption

ANSWER: A

QUESTION NO: 10

When an attack occurs, the attacked host (1.1.129.32) was able to capture many packets as shown. Based on the information shown, what kind of attack is this?

16 9.472315 1.1.129.32 1.1.129.32 TCP 21935 > http [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1

⊞ Frame 16: 62 bytes on wire (496 bits), 62 bytes captured (496 bits)
⊞ Ethernet II, Src: Dell_a9:e9:ef (00:24:e8:a9:e9:ef), Dst: HuaweiSy_00:f3:c8 (00:22:a1:00:f3:c8)
⊟ Internet Protocol Version 4, Src: 1.1.129.32 (1.1.129.32), Dst: 1.1.129.32 (1.1.129.32)
    version: 4
    Header length: 20 bytes
  ⊞ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transpor
    Total Length: 48
    Identification: 0x2b59 (11097)
  ⊟ Flags: 0x02 (Don't Fragment)
      0... .... = Reserved bit: Not set
      .1.. .... = Don't fragment: Set
      ..0. .... = More fragments: Not set
    Fragment offset: 0
    Time to live: 128
    Protocol: TCP (6)
  ⊞ Header checksum: 0xcb2c [correct]
    Source: 1.1.129.32 (1.1.129.32)
    Destination: 1.1.129.32 (1.1.129.32)
⊟ Transmission Control Protocol, Src Port: 21935 (21935), Dst Port: http (80), Seq: 0, Len: 0
    Source port: 21935 (21935)
    Destination port: http (80)
    [Stream index: 9]

```
0000  00 22 a1 00 f3 c8 00 24  e8 a9 e9 ef 08 00 45 00    ."......$......E.
0010  00 30 2b 59 40 00 80 06  cb 2c 01 01 81 20 01 01    .0+Y@... .,.. ..
0020  81 20 55 af 00 50 fc 1c  12 6b 00 00 00 00 70 02    . U..P.. .k....p.
0030  ff ff 1a 4c 00 0a 02 04  05 b4 04 02 01 01          ...L....... .....
```

A. Smurf attack

B. Land Attack

C. WinNuke

D. Ping of Death attack

ANSWER: B

QUESTION NO: 11

With the USG firewall, which two commands can be used to view equipment components (control board, fans, power supplies, etc.) run state and memory / CPU usage? (Choose two answers)

A. display device

B. display environment

C. display version

D. dir

ANSWER: A B

QUESTION NO: 12

In the use of virtual firewall technology: The two VPN users can travel over the public network Root VFW, log on to their respective private network VPN and get direct access to the private network resources.

According to the characteristics of VPN Firewall that provides multiple instances of business, which of the following statements is correct? (Choose three answers)

A. safe, VPN user authentication and authorization access through the firewall, after a visit with independent access virtual firewall system for users to manage different resources VPN users are completely isolated.

B. VPN flexible and reliable access to support from the public network to the VPN, can also support VPN to VPN from two modes.

C. easy to maintain, the user does not have superuser privileges on the system administrator account can manage the entire firewall (including each virtual firewall service).

D. strict access control permissions, firewall can control access VPN access permissions based on user name, password, so that employees can make a business trip, the super user (VPN require access to different resources), such as different users with different access rights.

ANSWER: A B D

QUESTION NO: 13

In the IKE V1 pre-shared key mode capture shown, what data is shown in the main role?

```
⊞ Frame 5 (198 bytes on wire, 198 bytes captured)
⊞ Ethernet II, Src: 00:e0:fc:d8:df:2a, Dst: 00:18:82:1f:2e:09
⊞ Internet Protocol, Src Addr: 1.1.1.1 (1.1.1.1), Dst Addr: 1.1.1.2 (1.1.1.2)
⊞ User Datagram Protocol, Src Port: isakmp (500), Dst Port: isakmp (500)
⊟ Internet Security Association and Key Management Protocol
     Initiator cookie: 0x568C4BAC3BCF2DFE
     Responder cookie: 0x09B1E93A64C977E6
     Next payload: Hash (8)
     Version: 1.0
     Exchange type: Quick Mode (32)
   ⊞ Flags
     Message ID: 0x64825321
     Length: 156
     Encrypted payload (128 bytes)
```

A. The negotiation phase SA 2

B. The negotiation phase SA 1

C. A random number used to exchange D-H public value, needed for the exchange of identity information

ANSWER: A

QUESTION NO: 14

Which of the following statements about IPsec and IKE following are correct? (Choose three answers)

A. With IPsec there are two ways to establish the security association, manual mode (manual) and IKE auto-negotiation (Isakmp) mode.

B. IKE aggressive mode can be selected based on negotitations initiated by the tunnel endpoint IP address or ID, to find the corresponding authentication word and finalize negotiations.

C. The NAT traversal function is used to delete the IKE negotiation verification process for UDP port numbers, while achieving a VPN tunnel to discover the NAT gateway function. If a NAT gateway device is used, then the data transfer after the IPsec uses UDP encapsulation.

D. IKE security mechanisms include DH Diffie-Hellman key exchange and distribution; improve the security front (Perfect Forward Secrecy PFS), encryption, and SHA1 algorithms.

ANSWER: A B C

QUESTION NO: 15

When using the SSL VPN client, it initiates network expansion "Connect gateway mate lost", what are the causes of this failure? (Choose three answers)

A. If you are using a proxy server, network extension client proxy server settings wrong.

B. PC and virtual gateway routing between unreachable.

C. network expansion between the client and the virtual gateway connection is blocked by the firewall.

D. Username and password configuration errors.

ANSWER: A B C