

Juniper

Exam JN0-533

FWV, Specialist (JNCIS-FWV)

Verson: Demo

[Total Questions: 10]

Question No : 1

Click the Exhibit button.

```
ns5gt-> get route source
S: Static P: Permanent
```

```
Src-Routes for <trust-vr> (1 entries)
```

ID	IP-Prefix	Interface	Gateway	P Pref	Mtr	Vsys
* 1	5.5.5.0/24	eth0/0	1.1.1.1	SP 20	1	Root

Which two statements are true regarding the route shown in the exhibit? (Choose two.)

- A. 5.5.5.0/24 was configured as a source route with a next-hop IP address of 1.1.1.1 in the trust-vr.
- B. 5.5.5.0/24 was configured as a destination route with a next-hop IP address of 1.1.1.1 in the trust-vr.
- C. 5.5.5.0/24 was configured as a SIBR route with a next-hop IP address of 1.1.1.1 in the trust-vr.
- D. 5.5.5.0/24 was configured as a permanent source route.

Answer: A,D

Question No : 2

You have enabled BGP on your ScreenOS device and configured a single EBGP peer. The CLI shows that the BGP connection is transitioning between the CONNECT and ACTIVE states, but never reaching the ESTABLISHED state.

What are three reasons for this behavior? (Choose three.)

- A. The peer is blocking traffic destined for TCP port 179.
- B. The peer address is not configured correctly.
- C. The enable statement has not been configured for the peer.
- D. The peer AS number is not configured correctly.
- E. BGP has not been enabled on the virtual router.

Answer: A,B,D

Question No : 3

You want to know the username and IP address of users who logged in to the WebUI.

In which log would you find this information?

- A. admin log
- B. event log
- C. traffic log
- D. self log

Answer: B

Question No : 4

You want to enable the integrated Web-filtering feature on a ScreenOS device.

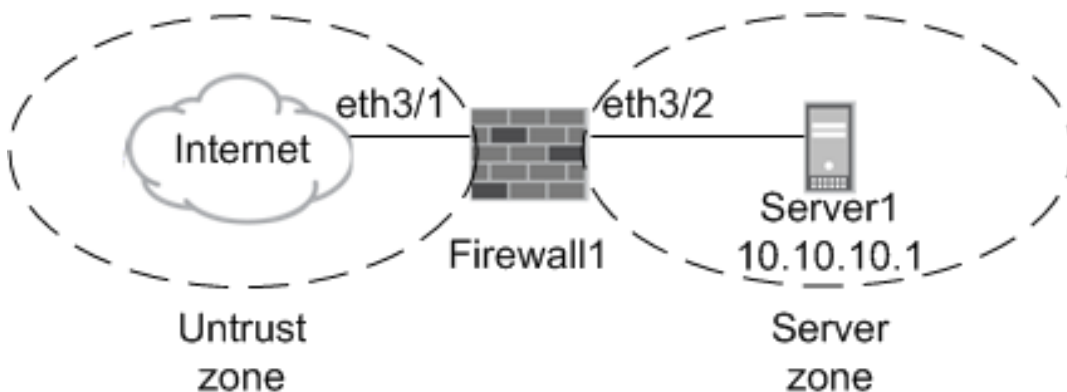
Which Web-filtering technology would be used?

- A. WebSense
- B. McAfee
- C. Symantec
- D. SurfControl

Answer: D

Question No : 5

Click the Exhibit button.



In the network shown in the exhibit, you have been asked to enable users in the Untrust zone to contact Server1 on TCP port 80 using IP address 1.1.1.1. You also need to allow Server1 to make connections to hosts in the Untrust zone. When Server1 makes connections to the Untrust zone, the source address of its traffic should be translated to 1.1.1.1.

What would you use to configure this behavior?

- A. MIP
- B. VIP
- C. DIP
- D. SIBR

Answer: A

Question No : 6

Which two statements are correct about internal antivirus scanning? (Choose two.)

- A. It includes a predefined file extension list for each protocol.
- B. It allows you to load-balance ICAP scan servers.
- C. It requires you to install a ScreenOS software license.
- D. It provides inbound spyware and phishing protection.

Answer: C,D

Question No : 7

You have configured integrated Web filtering in the ScreenOS software. You find that users trying to access <http://www.example.com> are being blocked by your Web-filtering configuration. However, you want all users to be able to access this Web site.

What are two methods to allow this traffic? (Choose two.)

- A. Configure an SC-CPA exception for the URL.
- B. Configure the URL as part of a custom category and allow requests in that category.
- C. Configure the URL as part of the blacklist.
- D. Configure the URL as part of the whitelist.

Answer: B,D

Question No : 8

Click the Exhibit button.

```
ns5-> get session
if 2(nspflag 800801):192.168.1.11/49237->74.125.235.48/443,6,a4badbf6bc41,sess token 3,vlan 0,tun 0,vsd 0,route
1,wsf 6
  if 8(nspflag 10800800):173.209.131.114/1034<-74.125.235.48/443,6,00222d52786c,sess token 4,vlan 0,tun 0,vsd
0,route 7,wsf 2
id 1568/s**,vsys 0,flag 00000000/0000/0001,policy 1,time 26, dip 2 module 0
  if 2(nspflag 800801):192.168.1.113/53514->123.176.112.241/80,6,842b2b91c303,sess token 3,vlan 0,tun 0,vsd
0,route 1,wsf 0
  if 8(nspflag 10800800):173.209.131.114/2120<-123.176.112.241/80,6,00222d52786c,sess token 4,vlan 0,tun 0,vsd
0,route 7,wsf 2
id 1571/s**,vsys 0,flag 00000000/0000/0001,policy 1,time 178, dip 2 module 0
```

Referring to the exhibit, what does the log show?

- A. The device is using VIP.
- B. The device is using DIP ID 4.
- C. The device is using source NAT.
- D. The device is using destination NAT.

Answer: C

Question No : 9

Which ScreenOS security feature helps protect against port scans and denial of service attacks?

- A. session-based stateful firewall
- B. IPsec VPNs
- C. security policies
- D. Screen options

Answer: B

Question No : 10

You must translate a range of public IP addresses to a range of internal IP addresses.

Which two mechanisms would you use to accomplish your objective? (Choose two.)

- A. MIP using masks
- B. VIP using masks
- C. policy-based NAT-dst
- D. policy-based NAT-src

Answer: A,C