

Fortinet Network Security Expert NSE4

**Fortinet Network Security Expert 4 Written Exam
(400)**

Thank You for Downloading NSE4 Updated Exam Questions

<https://certs4sale.com/fortinet/nse4-pdf-exam-dumps>

Version: 13.0

Question: 1

Which of the following sequences describes the correct order of criteria used for the selection of a master unit within a FortiGate high availability (HA) cluster when override is disabled?

- A. 1. port monitor, 2. unit priority, 3. up time, 4. serial number.
- B. 1. port monitor, 2. up time, 3. unit priority, 4. serial number.
- C. 1. unit priority, 2. up time, 3. port monitor, 4. serial number.
- D. 1. up time, 2. unit priority, 3. port monitor, 4. serial number.

Answer: B

Question: 2

Which statements are correct regarding URL filtering on a FortiGate unit? (Choose two.)

- A. The allowed actions for URL filtering include allow, block, monitor and exempt.
- B. The allow actions for URL filtering and Allow and Block only.
- C. URL filters may be based on patterns using simple text, wildcards and regular expressions.
- D. URL filters are based on simple text only and require an exact match.

Answer: A,C

Question: 3

Examine the following log message for IPS:

```
2012-07-01 09:54:28 oid=2 log_id=18433 type=ips subtype=anomaly pri=alert vd=root
severity="critical" src="192.168.3.168" dst="192.168.3.170" src_int="port2" serial=0
status="detected" proto=1 service="icmp" count=1 attack_name="icmp_flood" icmp_id="0xa8a4"
icmp_type="0x08" icmp_code="0x00" attack_id=16777316 sensor="1"
ref="http://www.fortinet.com/ids/VID16777316" msg="anomaly: icmp_flood, 51 > threshold 50"
```

Which statement is correct about the above log? (Choose two.)

- A. The target is 192.168.3.168.
- B. The target is 192.168.3.170.
- C. The attack was NOT blocked.
- D. The attack was blocked.

Answer: B,D

Question: 4

Regarding tunnel-mode SSL VPN, which three statements are correct? (Choose three.)

- A. Split tunneling is supported.
- B. It requires the installation of a VPN client.
- C. It requires the use of an Internet browser.
- D. It does not support traffic from third-party network applications.
- E. An SSL VPN IP address is dynamically assigned to the client by the FortiGate unit.

Answer: A,B,E

Question: 5

Examine the output below from the diagnose sys top command:

```
# diagnose sys top 1
Run time: 11 days, 3 hours and 29 minutes
OU,  ON,  1S,  99I;  971T,  528F,  160 KF
sshd      123      S      1.9      1.2
ipsendjine 61      S <    0.0      5.2
miglogd   45      S      0.0      4.9
pyfcgid   75      S      0.0      4.5
pyfcgid   73      S      0.0      3.9
```

Which statements are true regarding the output above (Choose two.)

- A. The sshd process is the one consuming most CPU.
- B. The sshd process is using 123 pages of memory.
- C. The command diagnose sys kill miglogd will restart the miglogd process.
- D. All the processes listed are in sleeping state.

Answer: A,D

Question: 6

A FortiGate administrator with the super_admin profile configures a virtual domain (VDM) for a new customer. After creating the VDM, the administrator is unable to reassign the dmz interface to the new VDM as the option is greyed out in the GUI in the management VDM.

What would be a possible cause for this problem?

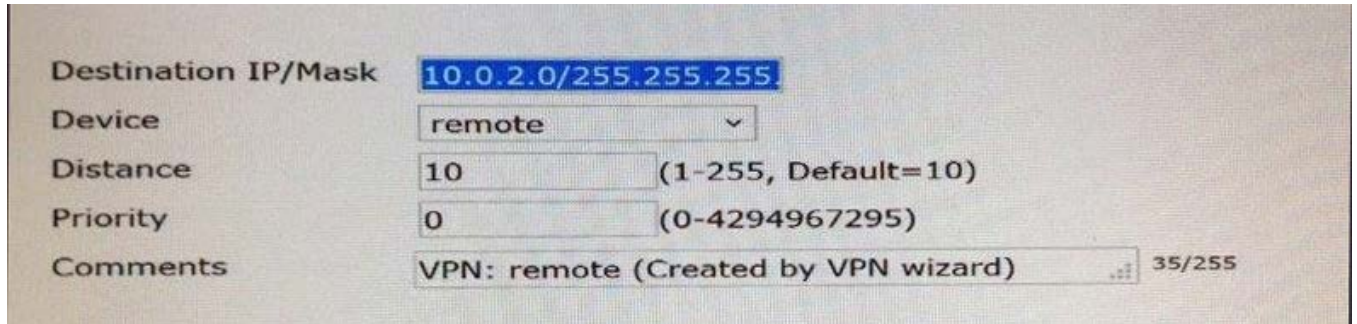
- A. The administrator does not have the proper permissions the dmz interface.

- B. The dmz interface is referenced in the configuration of another VDOM.
- C. Non-management VDOMs cannot reference physical interfaces
- D. The dmz interface is in PPPoE or DHCP mode.

Answer: B

Question: 7

Review the static route configuration for IPsec shown in the exhibit; then answer the question below.



Which statements are correct regarding this configuration? (Choose two.)

- A. Interface remote is an IPsec interface.
- B. A gateway address is not required because the interface is a point-to-point connection.
- C. A gateway address is not required because the default route is used.
- D. Interface remote is a zone.

Answer: A,B

Question: 8

In HA, the option Reserve Management Port for Cluster Member is selected as shown in the exhibit below.



Which statements are correct regarding this setting? (Choose two.)

- A. Interface settings on port7 will not be synchronized with other cluster members.
- B. The IP address assigned to this interface must not overlap with the IP address subnet assigned to another interface.
- C. When connecting to port7 you always connect to the master device.
- D. A gateway address may be configured for port7.

Answer: A,D

Question: 9

Which IPsec configuration mode can be used for implementing GRE-over-IPsec VPNs?

- A. Policy-based only.
- B. Route-based only.
- C. Either policy-based or route-based VPN.
- D. GRE-based only.

Answer: B

Question: 10

Which tasks fall under the responsibility of the SSL proxy in a typical HTTPS connection? (Choose two.)

- A. The web client SSL handshake.
- B. The web server SSL handshake.
- C. File buffering.
- D. Communication with the URL filter process.

Answer: A,B

Question: 11

Which statements are true regarding traffic shaping that is applied in an application sensor, and associated with the firewall policy? (Choose two.)

- A. Shared traffic shaping cannot be used.
- B. Only traffic matching the application control signature is shaped.
- C. Can limit the bandwidth usage of heavy traffic applications.
- D. Per-IP traffic shaping cannot be used.

Answer: B,C

Question: 12

What are valid options for handling DNS requests sent directly to a FortiGate's interface IP? (Choose three.)

- A. Conditional-forward.
- B. Forward-only.

- C. Non-recursive.
- D. Iterative.
- E. Recursive.

Answer: B,C,E

Question: 13

A FortiGate is configured to receive push updates from the FortiGuard Distribution Network, however, they are not being received.
Which is one reason for this problem?

- A. The FortiGate is connected to multiple ISPs.
- B. FortiGuard scheduled updates are enabled in the FortiGate configuration.
- C. The FortiGate is in Transparent mode.
- D. The external facing interface of the FortiGate is configured to get the IP address from a DHCP server.

Answer: D

Question: 14

Which statements are true regarding local user authentication? (Choose two.)

- A. Two-factor authentication can be enabled on a per user basis.
- B. Local users are for administration accounts only and cannot be used to authenticate network users.
- C. Administrators can create the user accounts in a remote server and store the user passwords locally in the FortiGate.
- D. Both the usernames and passwords can be stored locally on the FortiGate.

Answer: A,D

Question: 15

What methods can be used to access the FortiGate CLI? (Choose two.)

- A. Using SNMP.
- B. A direct connection to the serial console port.
- C. Using the CLI console widget in the GUI.
- D. Using RCP.

Answer: B,C

THANK YOU FOR DOWNLOADING NSE4 UPDATED EXAM QUESTIONS

Note: Thanks For Trying The Demo Of Our NSE4 Exam Product

Visit Our Site to Purchase the Full Set of Actual NSE4 Exam Questions With Answers.

Money Back Guarantee



Click The Link Below

<https://certs4sale.com/fortinet/nse4-pdf-exam-dumps>