



**FCNSP**

**Fortinet Certified Network Security Professional**

Q&A

DEMO Version

Copyright (c) 2012 Chinatag LLC. All rights reserved.

## **Important Note Please Read Carefully**

For demonstration purpose only, this free version Chinatag study guide contains **10** full length questions selected from our full version products which have (average) more than **200** questions each.

This Study guide has been carefully written and compiled by Chinatag certification experts. It is designed to help you learn the concepts behind the questions rather than be a strict memorization tool. Repeated readings will increase your comprehension.

For promotion purposes, all PDF files are **not** encrypted. Feel free to distribute copies among your friends and let them know Chinatag website.

## **Study Tips**

This product will provide you questions and answers along with detailed explanations carefully compiled and written by our experts. Try to understand the concepts behind the questions instead of cramming the questions. Go through the entire document at least twice so that you make sure that you are not missing anything.

## **Latest Version**

We are constantly reviewing our products. New material is added and old material is revised. Free updates are available for 90 days after the purchase. You should check the products page on the <http://www.chinatag.com> website for an update 3-4 days before the scheduled exam date.

Please tell us what you think of our products. We appreciate both positive and critical comments as your feedback helps us improve future versions. Feedback on specific questions should be send to [feedback@chinatag.com](mailto:feedback@chinatag.com).

Thanks for purchasing our products and look forward to supplying you with all your Certification training needs.

Good studying!

Technical and Support Team  
Chinatag LLC.

**QUESTION NO: 1**

A portion of the device listing for a Forti Analyzer unit is displayed in the exhibit.



Which of the following statements best describes the reason why the FortiGate 60B unit is unable to archive data to the Fortianalyzer unit?

- A. the FortiGate unit is considered an unregistered device.
- B. the Forti gate unit has been blocked from sending archive data to the Fortianalyzer device by the administrator.
- C. the Fortigate unit has insufficient privileges. The administrator should edit the device entry in the fortianalyzer and modify the privileges.
- D. the Fortigate unit is being treated as a syslog device and is only permitted to send log data.

**Answer: A**

**Explanation:**

**QUESTION NO: 2**

Which of the following describes the difference between the ban and quarantine actions?

- A. A ban action prevents future transactions using the same protocol which triggered the ban. A quarantine action blocks all future transactions, regardless of the protocol.
- B. A ban action blocks the transaction. A quarantine action archives the data.

- C. A ban action has a finite duration. A quarantine action must be removed by an administrator,
- D. A ban action is used for known users. A quarantine action is used for unknown users.

**Answer: A**

**Explanation:**

**QUESTION NO: 3**

Which of the following is an advantage of using SNMP v3 Instead of SNMP v1/v2 when querying the FortiGate unit?

- A. Packet encryption
- B. MIB-based report uploads
- C. SNMP access limits through access lists
- D. Running SNMP service on a non-standard port is possible

**Answer: A**

**Explanation:**

**QUESTION NO: 4**

An administrator has formed a High Availability cluster involving two FortiGate 310B units.

[ Multiple ipstream Layer 2 switches] - [ FortiGate HA Cluster ] - [ Multiple downstream Layer 2 switches ]

The administrator wishes to ensure that a single link failure will have minimal impact upon the overall throughput of traffic through this duster.

Which of the following options describes the best step the administrator can take?

The administrator should...

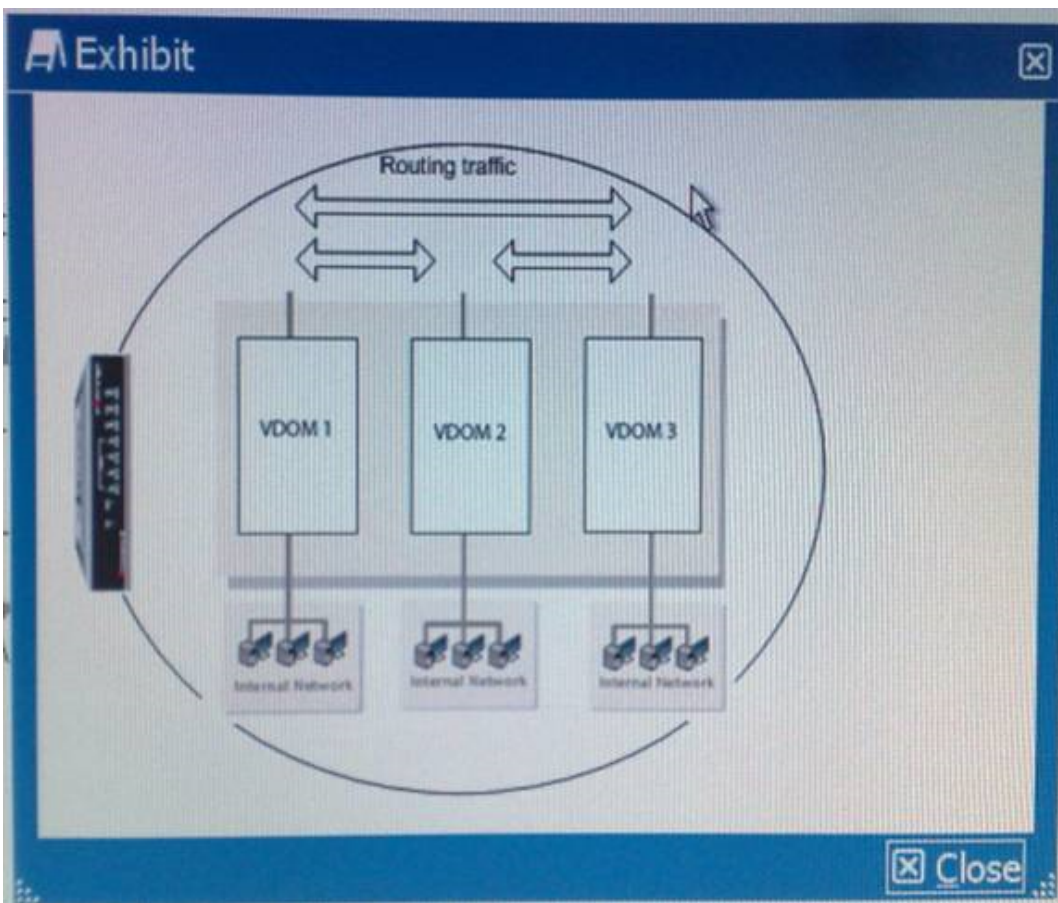
- A. setup a full-mesh design which uses redundant interfaces.
- B. increase the number of FortiGate units in the cluster and configure HA in Active-Active mode.
- C. enables monitoring of all active interfaces.
- D. configure the HA ping server feature to allow for HA failover in the event that a path is disrupted.

**Answer: D**

**Explanation:**

**QUESTION NO: 5**

FortiGate unit is configured with three Virtual Domains (VDOMs) as illustrated in the exhibit.



Which of the following statements are true if the network administrator wants to route traffic between all the VDOMs? (Select all that apply.)

- A.** The administrator should configure inter-VDOM links to avoid using external interfaces and routers.
- B.** As with all FortiGate unit interfaces, firewall policies must be in place for traffic to be allowed to pass through any Interface, including inter-VDOM links. This provides the same level of security internally as externally.
- C.** This configuration requires the use of an external router.
- D.** Inter-VDOM routing is automatically provided if all the subnets that need to be routed are locally attached. As each VDOM has an independent routing table, routing rules need to be set (for

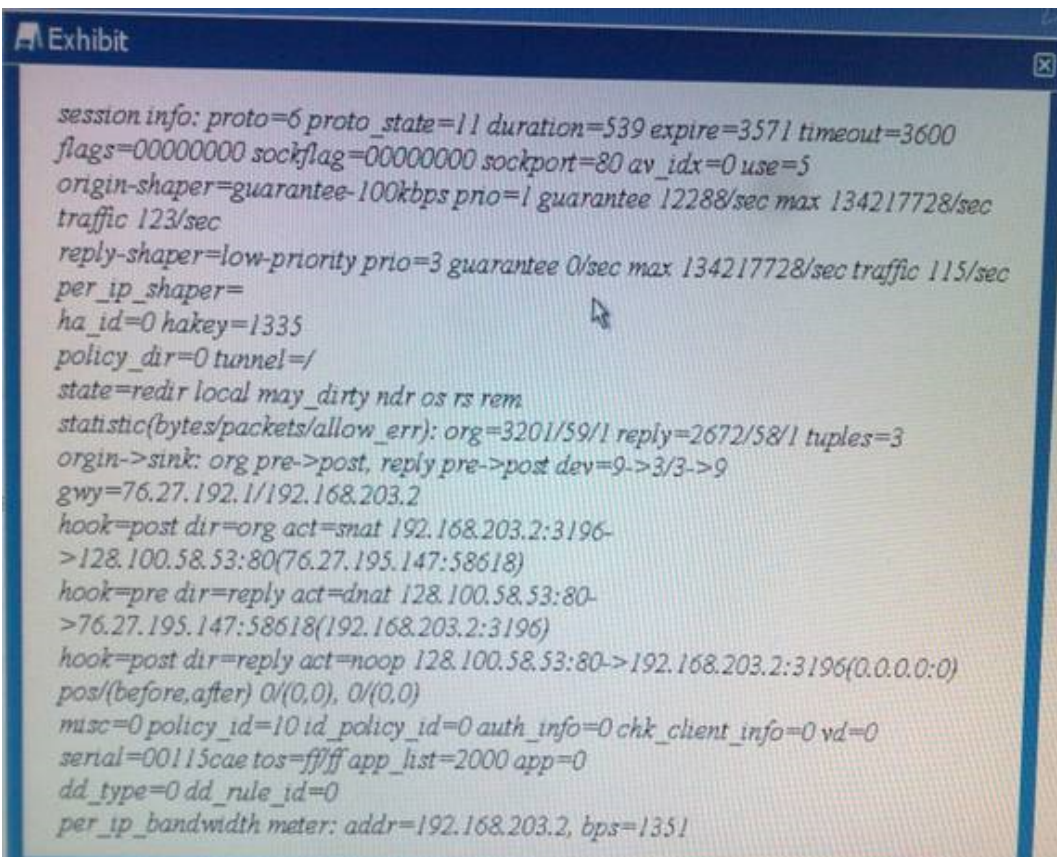
example, static routing, OSPF) in each VDOM to route traffic between VDOMs.

**Answer: A,B**

**Explanation:**

### QUESTION NO: 6

The diag sys session list command is executed in the CLI. The output of this command is shown in the exhibit.



```

session info: proto=6 proto_state=11 duration=539 expire=3571 timeout=3600
flags=00000000 sockflag=00000000 sockport=80 av_idx=0 use=5
origin-shaper=guarantee-100kbps prio=1 guarantee 12288/sec max 134217728/sec
traffic 123/sec
reply-shaper=low-priority prio=3 guarantee 0/sec max 134217728/sec traffic 115/sec
per_ip_shaper=
ha_id=0 hakey=1335
policy_dir=0 tunnel=/
state=redir local may_dirty ndr os rs rem
statistic(bytes/packets/allow_err): org=3201/59/1 reply=2672/58/1 tuples=3
origin->sink: org pre->post, reply pre->post dev=9->3/3->9
gwy=76.27.192.1/192.168.203.2
hook=post dir=org act=snat 192.168.203.2:3196-
>128.100.58.53:80(76.27.195.147:58618)
hook=pre dir=reply act=dnat 128.100.58.53:80-
>76.27.195.147:58618(192.168.203.2:3196)
hook=post dir=reply act=noop 128.100.58.53:80->192.168.203.2:3196(0.0.0.0)
pos/(before,after) 0/(0,0), 0/(0,0)
misc=0 policy_id=10 id_policy_id=0 auth_info=0 chk_client_info=0 vd=0
serial=00115cae tos=ffff app_list=2000 app=0
dd_type=0 dd_rule_id=0
per_ip_bandwidth meter: addr=192.168.203.2, bps=1351

```

Based on the output from this command, which of the following statements is correct?

- A. This is a UDP session.
- B. Traffic shaping is being applied to this session.
- C. This is an ICMP session.
- D. This traffic has been authenticated
- E. This session matches a firewall policy with ID 5.

**Answer: B**

**Explanation:**

**QUESTION NO: 7**

A DLP rule with an action of Exempt has been matched against traffic passing through the FortiGate unit. Which of the following statements is correct regarding how this transaction will be handled by the FortiGate unit?

- A. Any other matched EXP rules will be ignored with the exception of Archiving.
- B. Future files whose characteristics match this file will bypass DLP scanning.
- C. The traffic matching the DLP rule will bypass antivirus scanning.
- D. The client IP address will be added to a white list.

**Answer: A**

**Explanation:**

**QUESTION NO: 8**

Which of the following statements are correct regarding the configuration of a FortiGate unit as an SSL VPN gateway? (Select all that apply.)

- A. Tunnel mode can only be used if the SSL VPN user groups have at least one Host Check option enabled.
- B. The specific routes needed to access internal resources through an SSL VPN connection in tunnel mode from the client computer are defined in the routing widget associated with the SSL VPN portal.
- C. In order to apply a portal to a user, that user must belong to an SSL VPN user group.
- D. The portal settings specify whether the connection will operate in web-only or tunnel mode.

**Answer: C,D**

**Explanation:**

**QUESTION NO: 9**

Which of the following Items are considered to be advantages of using the application control

features on the FortiGate unit?

Implication control allows an administrator to:

- A. set a unique session-ttl for select applications.
- B. customizes application types in a similar way to adding custom IPS signatures.
- C. check, which applications are installed on workstations attempting to access the network.
- D. enables AV scanning per application rather than per policy.

**Answer: A**

**Explanation:**

**QUESTION NO: 10**

Which of the following statements is not correct regarding virtual domains (VDMs)?

- A. VDMs divide a single FortiGate unit into two or more virtual units that function as multiple, independent units.
- B. A management VDM handles SNMP, logging, alert email, and FDN-based updates.
- C. A backup management VDM will synchronize the configuration from an active management VDM.
- D. VDMs share firmware versions, as well as antivirus and IPS databases.
- E. Only administrative users with a super\_admin profile will be able to enter all VDMs to make configuration changes.

**Answer: C**

**Explanation:**