Vendor: Fortinet

Exam Code: NSE7_EFW-6.2

Exam Name: Fortinet NSE 7 - Enterprise Firewall 6.2

Version: DEMO

QUESTION 1
Refer to the exhibit, which contains the partial output of a diagnose command.

```
Spoke-2 # dia vpn tunnel list
list all ipsec tunnel in vd 0
------------------------------------------------------------------------------------------
name=VPN ver=1 serial=1 10.200.5.1:0 -> 10.200.4.1:0
bound_if=3 lgwy=statistic/1 tun=intf/0 mode=auto/1 encap=none/0
proxyid_num=1 child_num=0 refernt=15 ilast=10 olast=792 auto-discovery=0
stat: rxp=0 txp=0 rxb=0 txb=0
dpd: mode=on-demand on=1 idle=20000ms retry=3 count=0 seqno=0
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=VPN proto=0 sa=1 ref=2 serial=1
     src: 0:10.1.2.0/255.255.255.0:0
     dat: 0:10.1.1.0/255.255.255.0:0
     SA: ref=3 options=2e type=00 soft=0 mtu=1438 expire=42403/0B replaywin=204B seqno=1
esn=replaywin_lastseq=00000000
     life: type=01 bytes=0/0 timeout=43177/43200
     dec: spi=cccf66d esp=aes key=16 280e5cd6f9bacc65ac771556c464ffbd
            ah=sha1 key=20 c68091d68753578785de6a7a6b276b506e527
```

Based on the output, which two statements are correct? (Choose two.)

A. Anti-replay is enabled.
B. DPD is disabled.
C. Remote gateway IP is 10.200.4.1.
D. Quick mode selectors are disabled.

Answer: AC

QUESTION 2
Which two statements about application layer test commands are true? (Choose two.)

A. They are used to filter real-time debugs.
B. They display real-time application debugs.
C. Some of them can be used to restart an application.
D. Some of them display statistics and configuration information about a feature or process.

Answer: CD

QUESTION 3
What is the diagnose test application ipsmonitor 99 command used for?

A. To enable IPS bypass mode
B. To provide information regarding IPS sessions
C. To disable the IPS engine
D. To restart all IPS engines and monitors

Answer: D

QUESTION 4

Refer to the exhibit, which contains the output of diagnose sys session list.

```
# diagnose sys session list
session info: proto=6 proto_state=01 duration=73 expire=3597 timeout=3600
flags=00000000 sockflag=00000000 sockport=0 av_idx=0 use=3
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
state=may_dirty synced none app_ntf
statistic(bytes/packets/allow_err): org=822/11/1 reply=9037/15/1 tuples=2
orgin->sink: org pre->post, reply pre->post dev=4->2/2->4
gwy=100.64.1.254/10.0.1.10
hook=post dir=org act=snat 10.0.1.10:65464->54.192.15.182:80(100.64.1.1:65464)
hook=pre dir=reply act=dnat 54.192.15.182:80->100.64.1.1:65464(10.0.1.10:65464)
pos/(before,after) 0/(0,0), 0/(0,0)
misc=0 policy_id=1 auth_info=0 chk_client_info=0 vd=0
serial=00000098 tos=ff/ff ips_view=0 app_list=0 app=0
dd_type=0 dd_mode=0
```

If the HA ID for the primary unit is zero (0), which statement about the output is true?

A. This session cannot be synced with the slave unit.
B. The inspection of this session has been offloaded to the slave unit.
C. The master unit is processing this traffic.
D. This session is for HA heartbeat traffic.

Answer: C

QUESTION 5
How does FortiManager handle FortiGate requests from FortiGate devices, when it is configured as a local FDS?

A. FortiManager will respond to update requests only from a managed device.
B. FortiManager can download and maintain local copies of FortiGuard databases.
C. FortiManager supports only FortiGuard push update to managed devices.
D. FortiManager does not support web filter rating requests.

Answer: B

QUESTION 6
Which two conditions must be met for a statistic route to be active in the routing table? (Choose two.)

A. The link health monitor (if configured) is up.
B. There is no other route, to the same destination, with a higher distance.
C. The outgoing interface is up.
D. The next-hop IP address is up.

Answer: AC

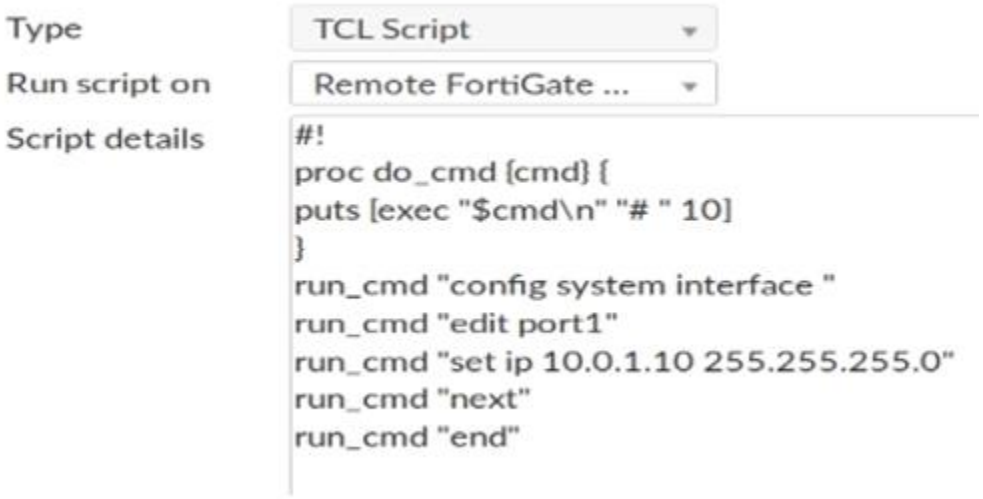
QUESTION 7

When using the SSL certificate inspection method to inspect HTTPS traffic, how does FortiGate filter web requests when the client browser does not provide the server name indication (SNI) extension?

A. FortiGate uses the requested URL from the user's web browser.
B. FortiGate uses the CN information from the Subject field in the server certificate.
C. FortiGate blocks the request without any further inspection.
D. FortiGate switches to the full SSL inspection method to decrypt the data.

Answer: B

QUESTION 8
Refer to the exhibit, which contains a TCL script configuration on FortiManager.



An administrator has configured the TCL script on FortiManager, but failed to apply any changes to the managed device after being executed.

Why did the TCL script fail to make any changes to the managed device?

A. Changes in an interface configuration can only be done by CLI script.
B. The TCL script must start with #include <>.
C. Incomplete commands are ignored in TCL scripts.
D. The TCL command run_cmd has not been created.

Answer: D

Thank You for Trying Our Product

Lead2pass Certification Exam Features:

★ More than **99,900** Satisfied Customers Worldwide.

★ Average **99.9%** Success Rate.

★ **Free Update** to match latest and real exam scenarios.

★ **Instant Download** Access! No Setup required.

★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.

★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.

★ **100%** Guaranteed Success or **100%** Money Back Guarantee.

★ **Fast**, helpful support **24x7**.

View list of all certification exams: http://www.lead2pass.com/all-products.html

10% Discount Coupon Code: **ASTR14**