DUMPSBOSS.COM

Fortinet NSE 7 - Enterprise Firewall 6.4

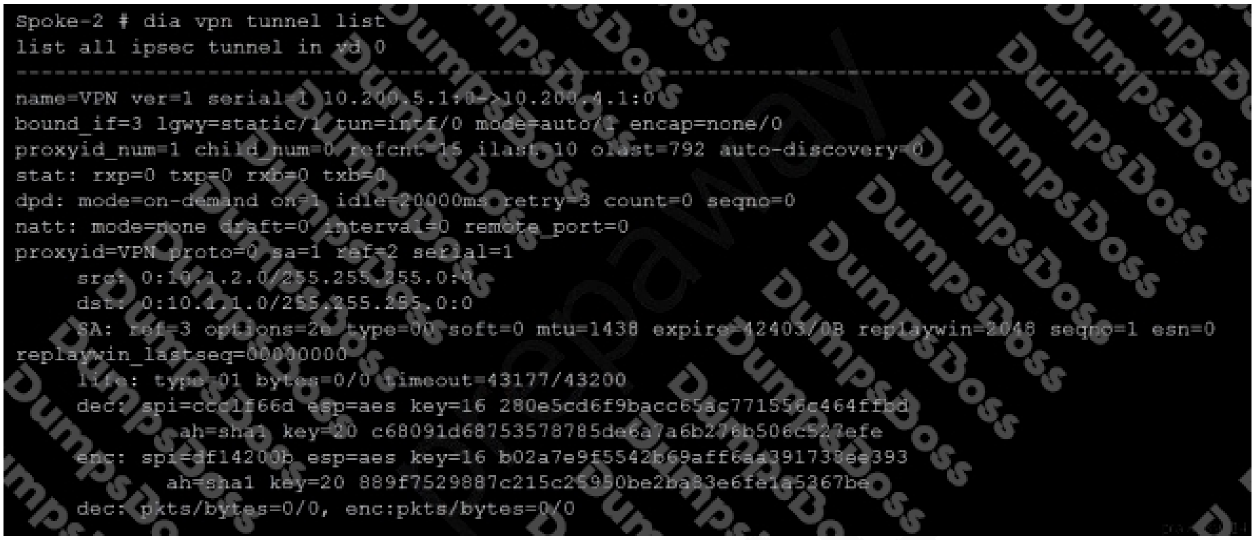
Fortinet NSE7_EFW-6.4

Version Demo

Total Demo Questions: 5

QUESTION NO: 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=static/1 tun=intf/0 mode=auto/1 encap=none/0
proxyid_num=1 child_num=0 refcnt=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
     dst: 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=2048 seqno=1 esn=0
replaywin_lastseq=00000000
     life: type=01 bytes=0/0 timeout=43177/43200
     dec: spi=ccc1f66d esp=aes key=16 280e5cd6f9bacc65ac771556c464ffbd
             ah=sha1 key=20 c68091d68753578785de6a7a6b276b506c527efe
     enc: spi=df14200b esp=aes key=16 b02a7e9f5542b69aff6aa391738ee393
            ah=sha1 key=20 889f7529887c215c25950be2ba83e6fe1a5367be
     dec: pkts/bytes=0/0, enc:pkts/bytes=0/0
```

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

A. Anti-replay is enabled

B. The remote gateway IP is 10.200.4.1.

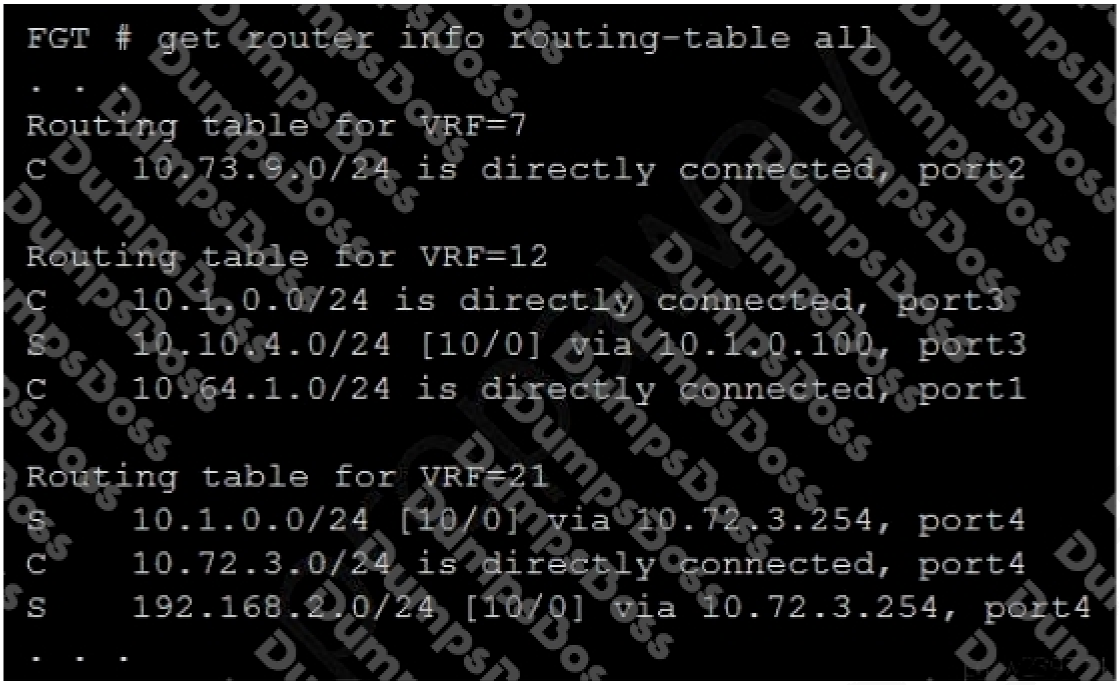
C. DPD is disabled.

D. Quick mode selectors are disabled.

ANSWER: A B

QUESTION NO: 2

Refer to the exhibit, which shows a partial routing table.



```
FGT # get router info routing-table all
. . .
Routing table for VRF=7
C     10.73.9.0/24 is directly connected, port2

Routing table for VRF=12
C     10.1.0.0/24 is directly connected, port3
S     10.10.4.0/24 [10/0] via 10.1.0.100, port3
C     10.64.1.0/24 is directly connected, port1

Routing table for VRF=21
S     10.1.0.0/24 [10/0] via 10.72.3.254, port4
C     10.72.3.0/24 is directly connected, port4
S     192.168.2.0/24 [10/0] via 10.72.3.254, port4
. . .
```

Assuming all the appropriate firewall policies are configured, which two pings will FortiGate route? (Choose two.)

A. Source IP address: 10.73.9.10, Destination IP address: 10.72.3.15

B. Source IP address: 10.72.3.52, Destination IP address: 10.1.0.254

C. Source IP address: 10.10.4.24, Destination IP address: 10.72.3.20

D. Source IP address: 10.1.0.10, Destination IP address: 10.64.1.52

ANSWER: B D

Explanation:

Only the source/destination pairs within the same VRF will be able to ping each other.

QUESTION NO: 3

How does FortiManager handle FortiGuard 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.

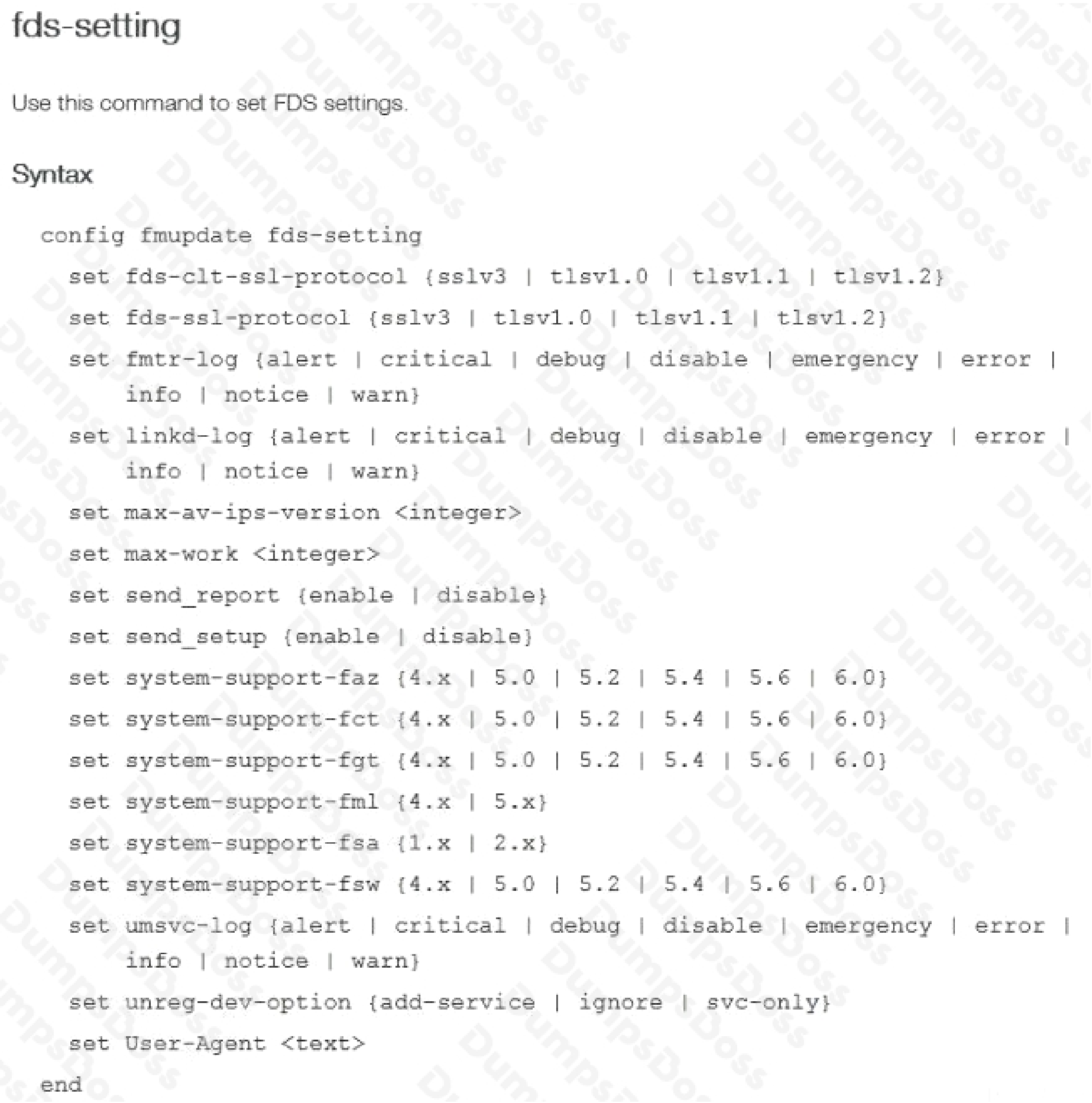
C. FortiManager does not support web filter rating requests.

D. FortiManager supports only FortiGuard push update to managed devices.

ANSWER: B

Explanation:

Reference: https://docs.fortinet.com/document/fortimanager/6.0.6/cli-reference/330471/fds-setting#fds-setting



fds-setting

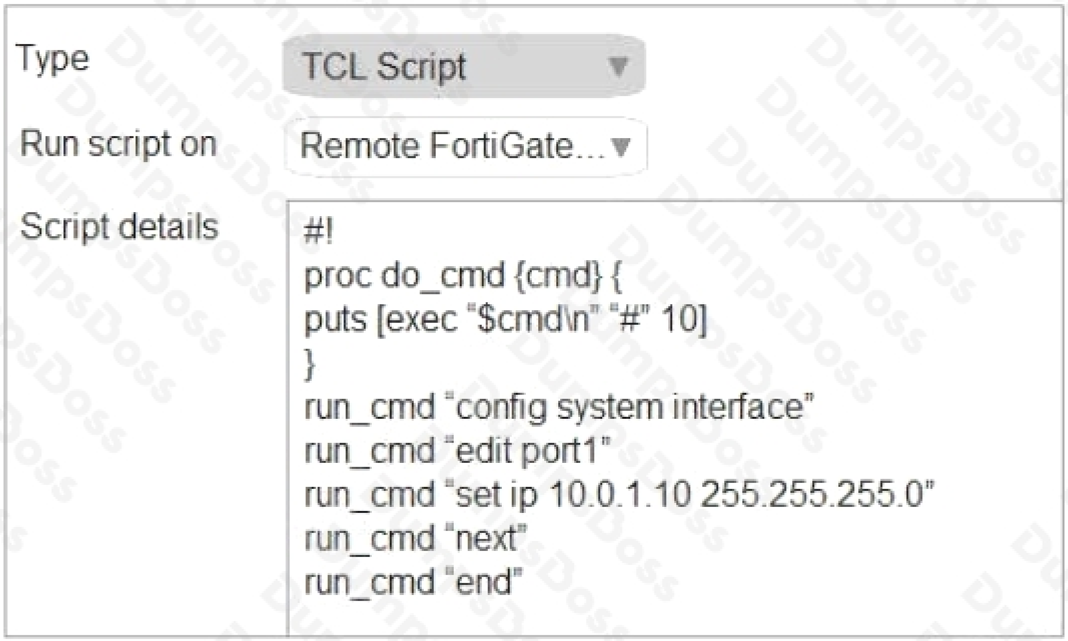
Use this command to set FDS settings.

Syntax

```
config fmupdate fds-setting
  set fds-clt-ssl-protocol {sslv3 | tlsv1.0 | tlsv1.1 | tlsv1.2}
  set fds-ssl-protocol {sslv3 | tlsv1.0 | tlsv1.1 | tlsv1.2}
  set fmtr-log {alert | critical | debug | disable | emergency | error |
      info | notice | warn}
  set linkd-log {alert | critical | debug | disable | emergency | error |
      info | notice | warn}
  set max-av-ips-version <integer>
  set max-work <integer>
  set send_report {enable | disable}
  set send_setup {enable | disable}
  set system-support-faz {4.x | 5.0 | 5.2 | 5.4 | 5.6 | 6.0}
  set system-support-fct {4.x | 5.0 | 5.2 | 5.4 | 5.6 | 6.0}
  set system-support-fgt {4.x | 5.0 | 5.2 | 5.4 | 5.6 | 6.0}
  set system-support-fml {4.x | 5.x}
  set system-support-fsa {1.x | 2.x}
  set system-support-fsw {4.x | 5.0 | 5.2 | 5.4 | 5.6 | 6.0}
  set umsvc-log {alert | critical | debug | disable | emergency | error |
      info | notice | warn}
  set unreg-dev-option {add-service | ignore | svc-only}
  set User-Agent <text>
end
```

QUESTION NO: 4

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



Type: TCL Script

Run script on: Remote FortiGate...

Script details:

```
#!
proc do_cmd {cmd} {
puts [exec "$cmd\n" "#" 10]
}
run_cmd "config system interface"
run_cmd "edit port1"
run_cmd "set ip 10.0.1.10 255.255.255.0"
run_cmd "next"
run_cmd "end"
```

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

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

A. The TCL script must start with #include <>.

B. The TCL command run_cmd has not been created.

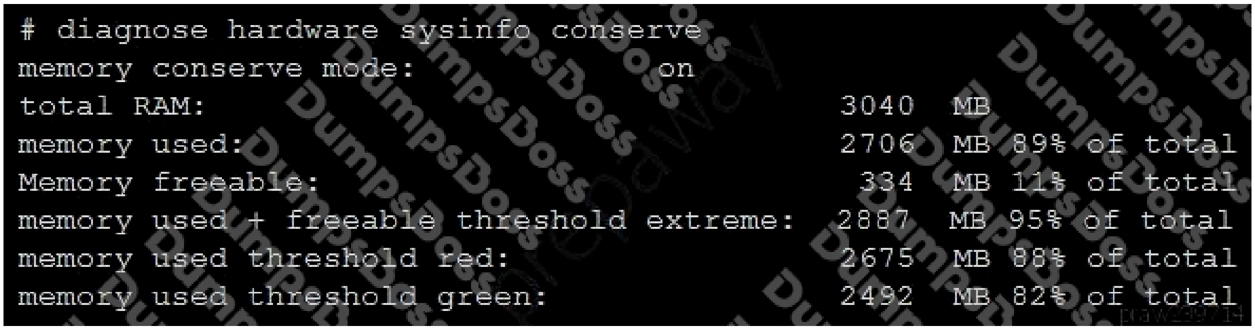
C. Changes to an interface configuration can be made only by a CLI script.

D. Incomplete commands are ignored in TCL scripts.

ANSWER: B

QUESTION NO: 5

Refer to the exhibit, which contains the output of a debug command.



```
# diagnose hardware sysinfo conserve
memory conserve mode:                 on
total RAM:                                3040  MB
memory used:                              2706  MB 89% of total
Memory freeable:                           334  MB 11% of total
memory used + freeable threshold extreme: 2887  MB 95% of total
memory used threshold red:                2675  MB 88% of total
memory used threshold green:              2492  MB 82% of total
```

What can be concluded about the conserve mode shown in the exhibit?

A. It is currently in memory conserve mode because of high memory usage.

B. It is currently in extreme conserve mode because of high memory usage.

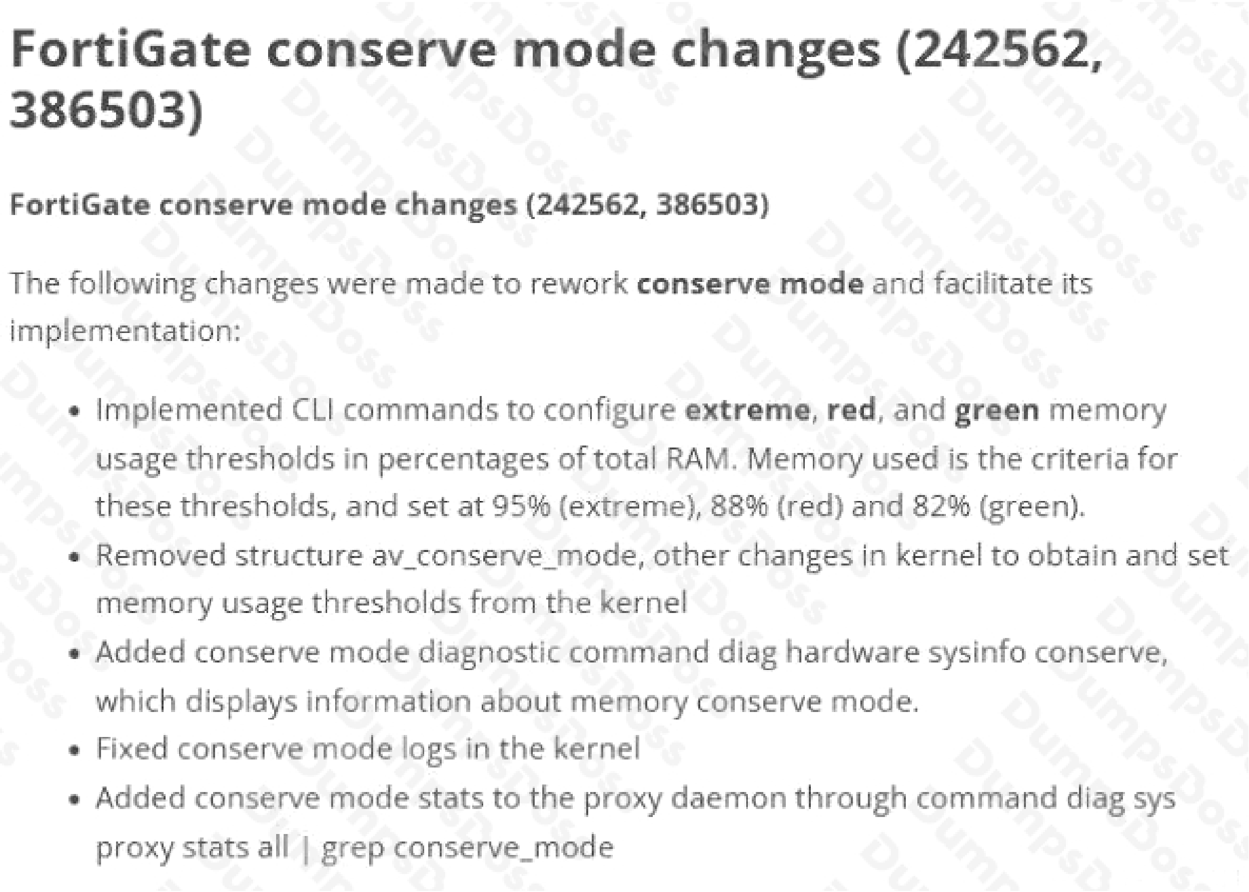
C. It is currently in system conserve mode because of high CPU usage.

D. It is currently in proxy conserve mode because of high memory usage.

ANSWER: A

Explanation:

Reference: https://www.fortinetguru.com/2017/09/fortigate-conserve-mode-changes-242562-386503/



FortiGate conserve mode changes (242562, 386503)

FortiGate conserve mode changes (242562, 386503)

The following changes were made to rework **conserve mode** and facilitate its implementation:

- Implemented CLI commands to configure **extreme**, **red**, and **green** memory usage thresholds in percentages of total RAM. Memory used is the criteria for these thresholds, and set at 95% (extreme), 88% (red) and 82% (green).
- Removed structure av_conserve_mode, other changes in kernel to obtain and set memory usage thresholds from the kernel
- Added conserve mode diagnostic command diag hardware sysinfo conserve, which displays information about memory conserve mode.
- Fixed conserve mode logs in the kernel
- Added conserve mode stats to the proxy daemon through command diag sys proxy stats all | grep conserve_mode