NSE7_EFW-6.2 Q&As

Fortinet NSE 7 - Enterprise Firewall 6.2

Pass Fortinet NSE7_EFW-6.2 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.certbus.com/nse7_efw-6-2.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Fortinet Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

What is the purpose of an internal segmentation firewall (ISFW)?

A. It inspects incoming traffic to protect services in the corporate DMZ.

B. It is the first line of defense at the network perimeter.

C. It splits the network into multiple security segments to minimize the impact of breaches.

D. It is an all-in-one security appliance that is placed at remote sites to extend the enterprise network.

Correct Answer: C

ISFW splits your network into multiple security segments. They serve as a breach containers from attacks that come from inside.

QUESTION 2

Which of the following statements is true regarding a FortiGate configured as an explicit web proxy?

A. FortiGate limits the number of simultaneous sessions per explicit web proxy user. This limit CANNOT be modified by the administrator.

B. FortiGate limits the total number of simultaneous explicit web proxy users.

C. FortiGate limits the number of simultaneous sessions per explicit web proxy user The limit CAN be modified by the administrator

D. FortiGate limits the number of workstations that authenticate using the same web proxy user credentials. This limit CANNOT be modified by the administrator.

Correct Answer: B

https://help.fortinet.com/fos50hlp/52data/Content/FortiOS/fortigate-WAN-opt- 52/web_proxy.htm#Explicit2 The explicit proxy does not limit the number of active sessions for each user. As a result the actual explicit proxy session count is usually much higher than the number of explicit web proxy users. If an excessive number of explicit web proxy sessions is compromising system performance you can limit the amount of users if the FortiGate unit is operating with multiple VDOMs.

QUESTION 3

An administrator has decreased all the TCP session timers to optimize the FortiGate memory usage. However, after the changes, one network application started to have problems. During the troubleshooting, the administrator noticed that the FortiGate deletes the sessions after the clients send the SYN packets, and before the arrival of the SYN/ACKs. When the SYN/ACK packets arrive to the FortiGate, the unit has already deleted the respective sessions. Which TCP session timer must be increased to fix this problem?

A. TCP half open.

B. TCP half close.

C. TCP time wait.

D. TCP session time to live.

Correct Answer: A

http://docslegacy.fortinet.com/fos40hlp/43prev/wwhelp/wwhimpl/common/html/wwhelp.htm?context=fgtandfile=CLI_get_Commands.58.25.html The tcp-halfopen-timer controls for how long, after a SYN packet, a session without SYN/ACK remains in the table. The tcp-halfclose-timer controls for how long, after a FIN packet, a session without FIN/ACK remains in the table. The tcp-timewait-timer controls for how long, after a FIN/ACK packet, a session remains in the table. A closed session remains in the session table for a few seconds more to allow any out-of- sequence packet.

QUESTION 4

Which statements about bulk configuration changes using FortiManager CLI scripts are correct? (Choose two.)

A. When executed on the Policy Package, ADOM database, changes are applied directly to the managed FortiGate.

B. When executed on the Device Database, you must use the installation wizard to apply the changes to the managed FortiGate.

C. When executed on the All FortiGate in ADOM, changes are automatically installed without creating a new revision history.

D. When executed on the Remote FortiGate directly, administrators do not have the option to review the changes prior to installation.

Correct Answer: BD

CLI scripts can be run in three different ways: Device Database: By default, a script is executed on the device database. It is recommend you run the changes on the device database (default setting), as this allows you to check what configuration changes you will send to the managed device. Once scripts are run on the device database, you can install these changes to a managed device using the installation wizard. Policy Package, ADOM database: If a script contains changes related to ADOM level objects and policies, you can change the default selection to run on Policy Package, ADOM database and can then be installed using the installation wizard. Remote FortiGate directly (through CLI): A script can be executed directly on the device and you don\\'t need to install these changes using the installation wizard. As the changes are directly installed on the managed device, no option is provided to verify and check the configuration changes through FortiManager prior to executing it.

QUESTION 5

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.

Correct Answer: B

QUESTION 6

Examine the following traffic log; then answer the question below. date-20xx-02-01 time=19:52:01

devname=master device_id="xxxxxxx" log_id=0100020007 type=event subtype=system pri critical vd=root

service=kemel status=failure msg="NAT port is exhausted."

What does the log mean?

A. There is not enough available memory in the system to create a new entry in the NAT port table.

B. The limit for the maximum number of simultaneous sessions sharing the same NAT port has been reached.

C. FortiGate does not have any available NAT port for a new connection.

D. The limit for the maximum number of entries in the NAT port table has been reached.

Correct Answer: B

QUESTION 7

Examine the following partial outputs from two routing debug commands; then answer the question below. # get router info kernel tab=254 vf=0 scope=0type=1 proto=11 prio=0 0.0.0.0/0.0.0.0/0->0.0.0.0/0 pref=0.0.0.0 gwy=10.200.1.254 dev=2(port1) tab=254 vf=0 scope=0type=1 proto=11 prio=10 0.0.0.0/0.0.0.0/0->0.0.0.0/0 pref=0.0.0.0 gwy=10.200.2.254 dev=3(port2) tab=254 vf=0 scope=253type=1 proto=2 prio=0 0.0.0.0/0.0.0.0/.->10.0.1.0/24 pref=10.0.1.254 gwy=0.0.0.0 dev=4(port3) # get router info routing-table all s*0.0.0.0/0 [10/0] via 10.200.1.254, portl [10/0] via 10.200.2.254, port2, [10/0] dO.0.1.0/24 is directly connected, port3 dO.200.1.0/24 is directly connected, portl d0.200.2.0/24 is directly connected, port2

Which outbound interface or interfaces will be used by this FortiGate to route web traffic from internal users to the Internet?

A. port!

B. port2.

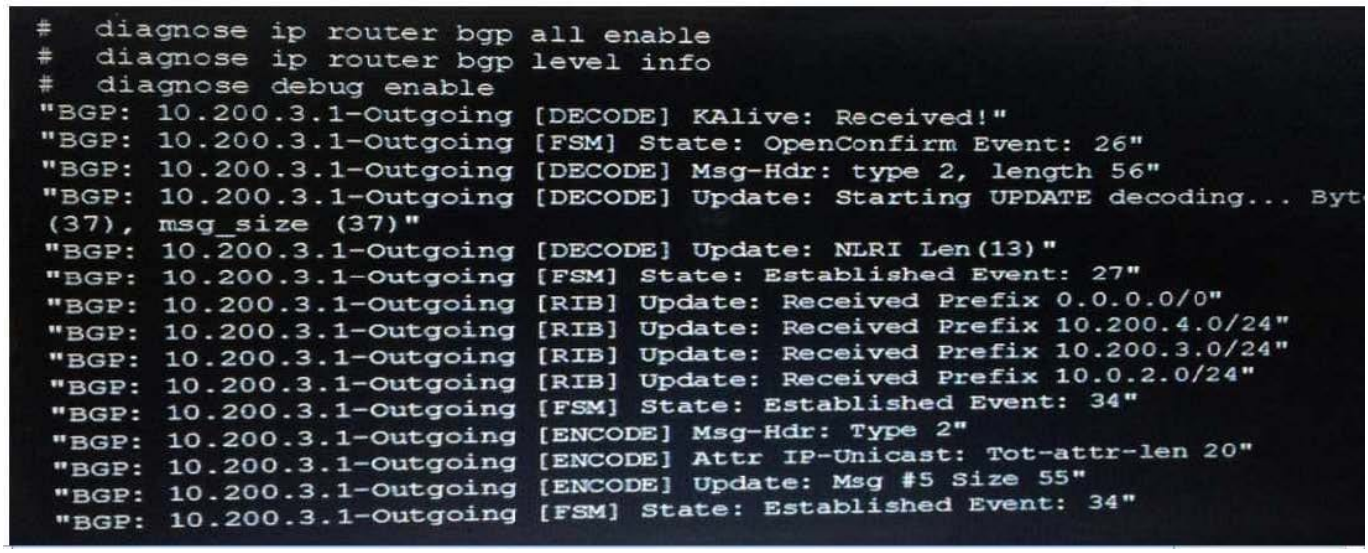
C. Both portl and port2.

D. port3.

Correct Answer: B

QUESTION 8

Examine the output from the BGP real time debug shown in the exhibit, then the answer the question below: Which statements are true regarding the output in the exhibit? (Choose two.)



A. BGP peers have successfully interchanged Open and Keepalive messages.

B. Local BGP peer received a prefix for a default route.

C. The state of the remote BGP peer is OpenConfirm.

D. The state of the remote BGP peer will go to Connect after it confirms the received prefixes.

Correct Answer: AB

QUESTION 9

An administrator has enabled HA session synchronization in a HA cluster with two members. Which flag is added to a primary unit\\'s session to indicate that it has been synchronized to the secondary unit?

A. redir.

B. dirty.

C. synced

D. nds.

Correct Answer: C

The synced sessions have the `synced\\' flag. The command `diag sys session list\\' can be used to see the sessions on the member, with the associated flags.

QUESTION 10

Which real time debug should an administrator enable to troubleshoot RADIUS authentication problems?

A. Diagnose debug application radius -1.

B. Diagnose debug application fnbamd -1.

C. Diagnose authd console -log enable.

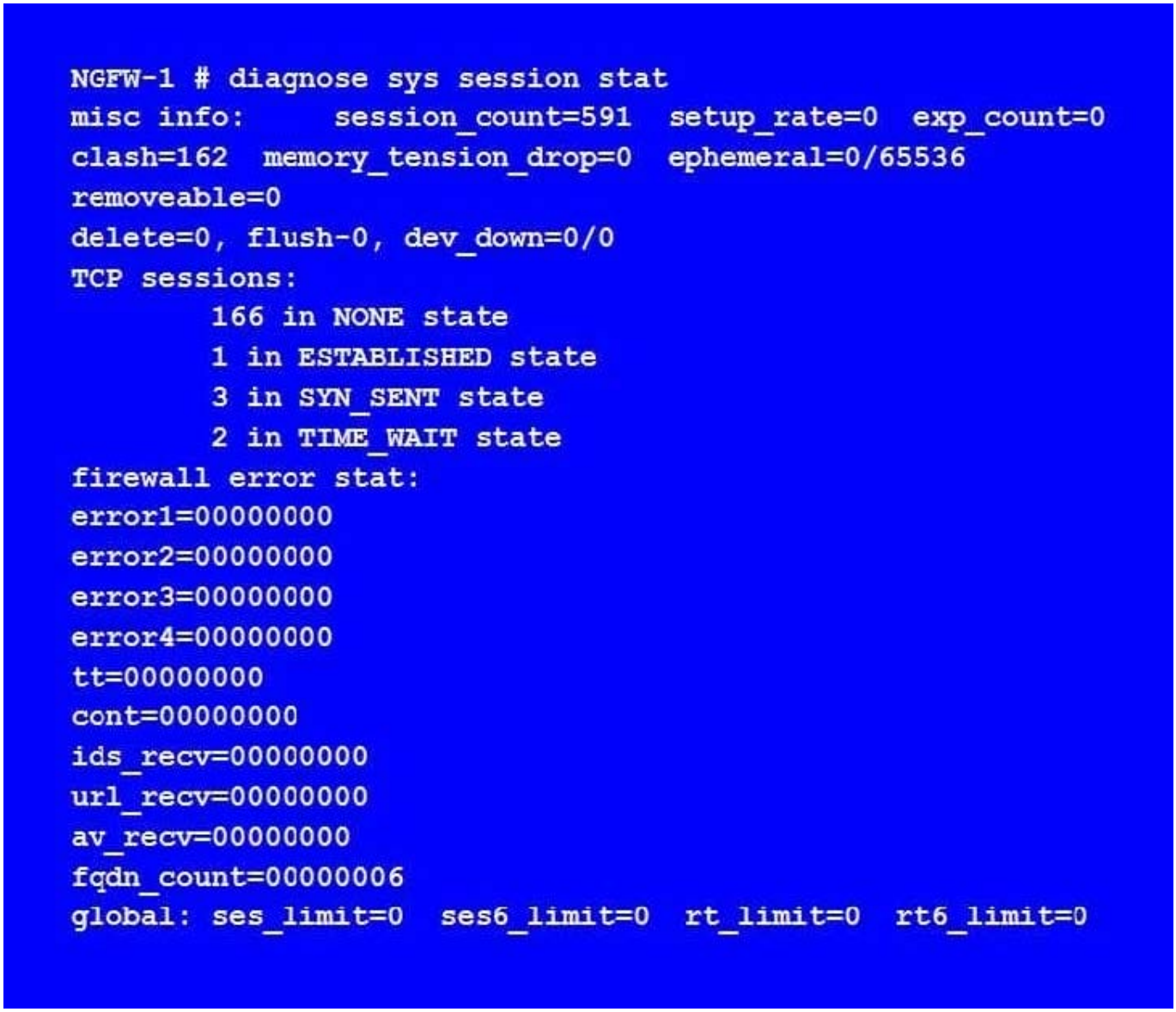
D. Diagnose radius console -log enable.

Correct Answer: B

https://kb.fortinet.com/kb/documentLink.do?externalID=FD32838

QUESTION 11

View the exhibit, which contains the output of diagnose sys session stat, and then answer the question below.



```
NGFW-1 # diagnose sys session stat
misc info:     session_count=591  setup_rate=0  exp_count=0
clash=162  memory_tension_drop=0  ephemeral=0/65536
removeable=0
delete=0, flush-0, dev_down=0/0
TCP sessions:
        166 in NONE state
        1 in ESTABLISHED state
        3 in SYN_SENT state
        2 in TIME_WAIT state
firewall error stat:
error1=00000000
error2=00000000
error3=00000000
error4=00000000
tt=00000000
cont=00000000
ids_recv=00000000
url_recv=00000000
av_recv=00000000
fqdn_count=00000006
global: ses_limit=0  ses6_limit=0  rt_limit=0  rt6_limit=0
```

Which statements are correct regarding the output shown? (Choose two.)

A. There are 0 ephemeral sessions.

B. All the sessions in the session table are TCP sessions.

C. No sessions have been deleted because of memory pages exhaustion.

D. There are 166 TCP sessions waiting to complete the three-way handshake.

Correct Answer: AC

https://kb.fortinet.com/kb/documentLink.do?externalID=FD40578

QUESTION 12

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

```
# conf rout stat
#    edit 0
#         set gateway 10.20.121.2
#         set priority 20
#         set device "wan1"
#    next
# end
```

Why didn\\'t the script make any changes to the managed device?

A. Commands that start with the # sign are not executed.

B. CLI scripts will add objects only if they are referenced by policies.

C. Incomplete commands are ignored in CLI scripts.

D. Static routes can only be added using TCL scripts.

Correct Answer: A

https://help.fortinet.com/fmgr/50hlp/56/5-6-2/FortiManager_Admin_Guide/1000_Device% 20Manager/2400_Scripts/1000_Script%20samples/02 00_CLI%20scripts+.htm#Error_Messages A sequence of FortiGate CLI commands, as you would type them at the command line. A comment line starts with the number sign (#). A comment line will not be executed.

QUESTION 13

In which two states is a given session categorized as ephemeral? (Choose two.)

A. A TCP session waiting to complete the three-way handshake.

B. A TCP session waiting for FIN ACK.

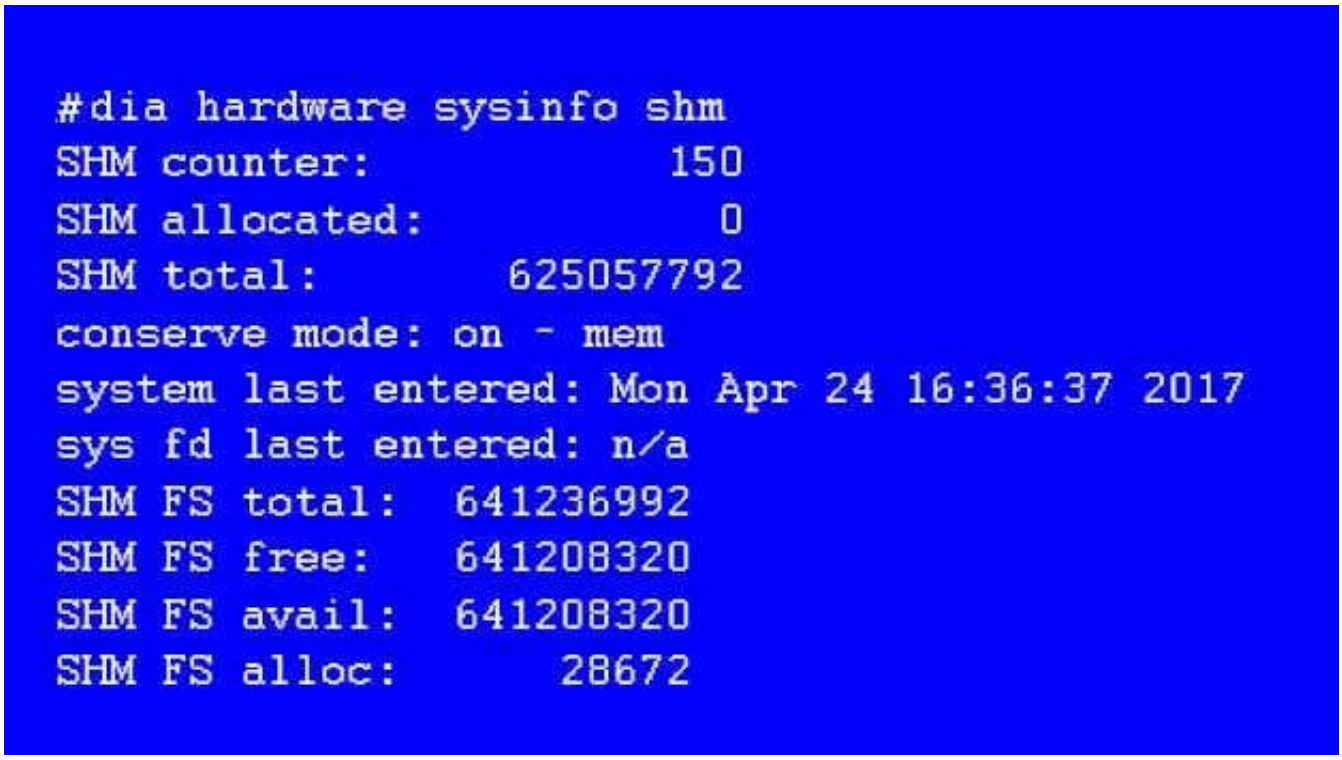
C. A UDP session with packets sent and received.

D. A UDP session with only one packet received.

Correct Answer: BC

QUESTION 14

View the exhibit, which contains the output of a debug command, and then answer the question below.



What statement is correct about this FortiGate?

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

B. It is currently in FD conserve mode.

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

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

Correct Answer: D

QUESTION 15

What configuration changes can reduce the memory utilization in a FortiGate? (Choose two.)

A. Reduce the session time to live.

B. Increase the TCP session timers.

C. Increase the FortiGuard cache time to live.

D. Reduce the maximum file size to inspect.

Correct Answer: AD