DUMPSARENA

Fortinet NSE 7 - Enterprise Firewall 7.0

Fortinet NSE7_EFW-7.0

Version Demo

Total Demo Questions: 10

Total Premium Questions: 163

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

QUESTION NO: 1

Which the following events can trigger the election of a new primary unit in a HA cluster? (Choose two.)

A. Primary unit stops sending HA heartbeat keepalives.

B. The FortiGuard license for the primary unit is updated.

C. One of the monitored interfaces in the primary unit is disconnected.

D. A secondary unit is removed from the HA cluster.

ANSWER: A C

QUESTION NO: 2

Refer to the exhibit, which contains partial output from an IKE real-time debug.

```
ike 0:624000:98: responder: main mode get 1st message...
ike 0:624000:98: VID DPD AFCAD71368A1F1C96B8696FC77570100
ike 0:624000:98: VID FRAGMENTATION 4048B7D56EBCE88525E7DE7F00D6C2D3
ike 0:624000:98: VID FRAGMENTATION 4048B7D56EBCE88525E7DE7F00D6C2D3C0000000
ike 0:624000:98: VID FORTIGATE 8299031757A36082C6A621DE00000000
ike 0:624000:98: incoming proposal:
ike 0:624000:98: proposal id = 0:
ike 0:624000:98:   protocol id = ISAKMP:
ike 0:624000:98:     trans_id = KEY_IKE.
ike 0:624000:98:     encapsulation = IKE/none
ike 0:624000:98:         type=OAKLEY_ENCRYPT_ALG, val=AES_CBC, key-len=256
ike 0:624000:98:         type=OAKLEY_HASH_ALG, val=SHA2_256.
ike 0:624000:98:         type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0:624000:98:         type=OAKLEY_GROUP, val=MODP2048.
ike 0:624000:98: ISAKMP SA lifetime=86400
ike 0:624000:98: proposal id = 0:
ike 0:624000:98:   protocol id = ISAKMP:
ike 0:624000:98:     trans_id = KEY_IKE.
ike 0:624000:98:     encapsulation = IKE/none
ike 0:624000:98:         type=OAKLEY_ENCRYPT_ALG, val=AES_CBC, key-len=256
ike 0:624000:98:         type=OAKLEY_HASH_ALG, val=SHA2_256.
ike 0:624000:98:         type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0:624000:98:         type=OAKLEY_GROUP, val=MODP1536.
ike 0:624000:98: ISAKMP SA lifetime=86400
ike 0:624000:98: my proposal, gw Remotesite:
ike 0:624000:98: proposal id = 1:
ike 0:624000:98:   protocol id = ISAKMP:
ike 0:624000:98:     trans_id = KEY_IKE.
ike 0:624000:98:     encapsulation = IKE/none
iike 0:624000:98:         type=OAKLEY_ENCRYPT_ALG, val=AES_CBC, key-len=128
ike 0:624000:98:         type=OAKLEY_HASH_ALG, val=SHA.
ike 0:624000:98:         type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0:624000:98:         type=OAKLEY_GROUP, val=MODP2048.
ike 0:624000:98: ISAKMP SA lifetime=86400
ike 0:624000:98: proposal id = 1:
ike 0:624000:98:   protocol id = ISAKMP:
ike 0:624000:98:     trans_id = KEY_IKE.
ike 0:624000:98:     encapsulation = IKE/none
ike 0:624000:98:         type=OAKLEY_ENCRYPT_ALG, val=AES_CBC, key-len=128
ike 0:624000:98:         type=OAKLEY_HASH_ALG, val=SHA.
ike 0:624000:98:         type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0:624000:98:         type=OAKLEY_GROUP, val=MODP1536.
ike 0:624000:98: ISAKMP SA lifetime=86400
ike 0:624000:98: negotiation failure
ike Negot:624ea7b1bba276fb/0000000000000000:98: no SA proposal chosen
```

The administrator does not have access to the remote gateway.

Based on the debug output, which configuration change can the administrator make to the local gateway to resolve the phase 1 negotiation error?

A. In the phase 1 network configuration, set the IKE version to 2.

B. In the phase 1 proposal configuration, add AES128-SHA128 to the list of encryption algorithms.

C. In the phase 1 proposal configuration, add AESCBC-SHA2 to the list of encryption algorithms.

D. In the phase 1 proposal configuration, add AES256-SHA256 to the list of encryption algorithms.

ANSWER: D

Explanation:

https://docs.fortinet.com/document/fortigate/7.0.0/administration-guide/238852

QUESTION NO: 3

You have configured FortiManager as a local FDS to provide FortiGate AV and IPS updates, but FortiGate devices are not receiving updates to their AV signature databases, IPS engines, or IPS signature databases.

Which two settings need to be verified for these features to function? (Choose two.)

A. FortiGate needs to have the server list entry for FortiManager set to server-type update under config system central-management.

B. FortiManager needs to be the license validation server for FortiGate devices trying to retrieve updated AV and IPS packages.

C. Service access needs to be enabled on FortiManager under System Settings > Network.

D. FortiGate needs to have include-default-servers disabled under config system central-management.

ANSWER: A C

Explanation:

NSE 7.0 Guide page 184-185

QUESTION NO: 4

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

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

Which one of the following statements about this FortiGate is correct?

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

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

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

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

ANSWER: D

QUESTION NO: 5

What events are recorded in the crashlogs of a FortiGate device? (Choose two.)

A. A process crash.

B. Configuration changes.

C. Changes in the status of any of the FortiGuard licenses.

D. System entering to and leaving from the proxy conserve mode.

ANSWER: A D

Explanation:

diagnose debug crashlog read

275: 2014-08-05 13:03:53 proxy=acceptor service=imap session fail mode=activated276: 2014-08-05 13:03:53 proxy=acceptor service=ftp session fail mode=activated277: 2014-08-05 13:03:53 proxy=acceptor service=nntp session fail mode=activated278: 2014-08-06 11:05:47 service=kernel conserve=on free="45034 pages" red="45874 pages" msg="Kernel279: 2014-08-06 11:05:47 enters conserve mode"280: 2014-08-06 13:07:16 service=kernel conserve=exit free="86704 pages" green="68811 pages"281: 2014-08-06 13:07:16 msg="Kernel leaves conserve mode"282: 2014-08-06 13:07:16 proxy=imd sysconserve=exited total=1008 free=349 marginenter=201283: 2014-08-06 13:07:16 marginexit=302

QUESTION NO: 6

An administrator has configured two FortiGate devices for an HA cluster. While testing HA failover, the administrator notices that some of the switches in the network continue to send traffic to the former primary device.

What can the administrator do to fix this problem?

A. Configure remote link monitoring to detect an issue in the forwarding path.

B. Configure set send-garp-on-failover enable under config system ha on both cluster members.

C. Verify that the speed and duplex settings match between the FortiGate interfaces and the connected switch ports.

D. Configure set link-failed-signal enable under config system ha on both cluster members.

ANSWER: D

Explanation:

Virtual MAC Address and Failover - The new primary broadcasts Gratuitous ARP packets to notify the network that each virtual MAC is now reachable through a different switch port. - Some high-end switches might not clear their MAC table correctly after a failover - Solution: Force former primary to shut down all its interfaces for one second when the failover happens (excluding heartbeat and reserved management interfaces): #Config system ha set link-failed-signal enable end - This simulates a link failure that clears the related entries from MAC table of the switches.

QUESTION NO: 7

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

```
FGT # get router info ospf neighbor

OSPF process 0:
Neighbor ID     Pri   State           Dead Time     Address         Interface
0.0.0.69          1   Full/DR         00:00:32      10.126.0.69     wan1
0.0.0.117         1   Full/DROther    00:00:34      10.126.0.117    wan2
0.0.0.2           1   Full/ -         00:00:38      172.16.1.2      ToRemote
```

What can be concluded from the debug command output?

A. The OSPF router with the ID 0.0.0.69 has its OSPF priority set to 0.

B. The local FortiGate has a different MTU value from the OSPF router with ID 0.0.0.2, based on the state information.

C. There are more than two OSPF routers on the wan2 network.

D. The interface ToRemote is a broadcast OSPF network.

ANSWER: C

Explanation:

Enterprise_Firewall_7.0_Study_Guide-Online.pdf p 296

QUESTION NO: 8

How are bulk configuration changes made using FortiManager CLI scripts? (Choose two.)

A. When run on the All FortiGate in ADOM, changes are automatically installed without the creation of a new revision history.

B. When run on the Device Database, changes are applied directly to the managed FortiGate device.

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

D. When run on the Policy Package, ADOM database, you must use the installation wizard to apply the changes to the managed FortiGate device

ANSWER: C D

Explanation:

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 andpolicies, 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 NO: 9

Refer to the exhibit, which shows the output of a web filtering diagnose command.

```
# diagnose webfilter fortiguard statistics list
...

Rating Statistics:
==================
DNS failures                  :          273
DNS lookups                   :          280
Data send failures            :            0
Data read failures            :            0
Wrong package type            :            0
Hash table miss               :            0
Unknown server                :            0
Incorrect CRC                 :            0
Proxy request failures        :            0
Request timeout               :            1
Total requests                :         2409
Requests to FortiGuard servers:         1182
Server errored responses      :            0
Relayed rating                :            0
Invalid profile               :            0

Allowed                       :         1021
Blocked                       :         3909
Logged                        :         3927
Blocked Errors                :          565
Allowed Errors                :            0
Monitors                      :            0
Authenticates                 :            0
Warnings:                     :           18
Ovrd request timeout          :            0
Ovrd send failures            :            0
Ovrd read failures            :            0
Ovrd errored responses        :            0
...
```

```
# diagnose webfilter fortiguard statistics list
...

Cache Statistics:
=================
Maximum memory                :            0
Memory usage                  :            0

Nodes                         :            0
  Leaves                      :            0
  Prefix nodes                :            0
  Exact nodes                 :            0

Requests                      :            0
Misses                        :            0
Hits                          :            0
  Prefix hits                 :            0
  Exact hits                  :            0

No cache directives           :            0
Add after prefix              :            0
Invalid DB put                :            0
DB updates                    :            0

Percent full                  :           0%
  Branches                    :           0%
  Leaves                      :           0%
    Prefix nodes              :           0%
    Exact nodes               :           0%

Miss rate                     :           0%
Hit rate                      :           0%
  Prefix hits                 :           0%
  Exact hits                  :           0%
```

Which configuration change would result in non-zero results in the cache statistics section?

A. set server-type rating under config system central-management

B. set webfilter-cache enable under config system fortiguard

C. set webfilter-force-off disable under config system fortiguard

D. set ngfw-mode policy-based under config system settings

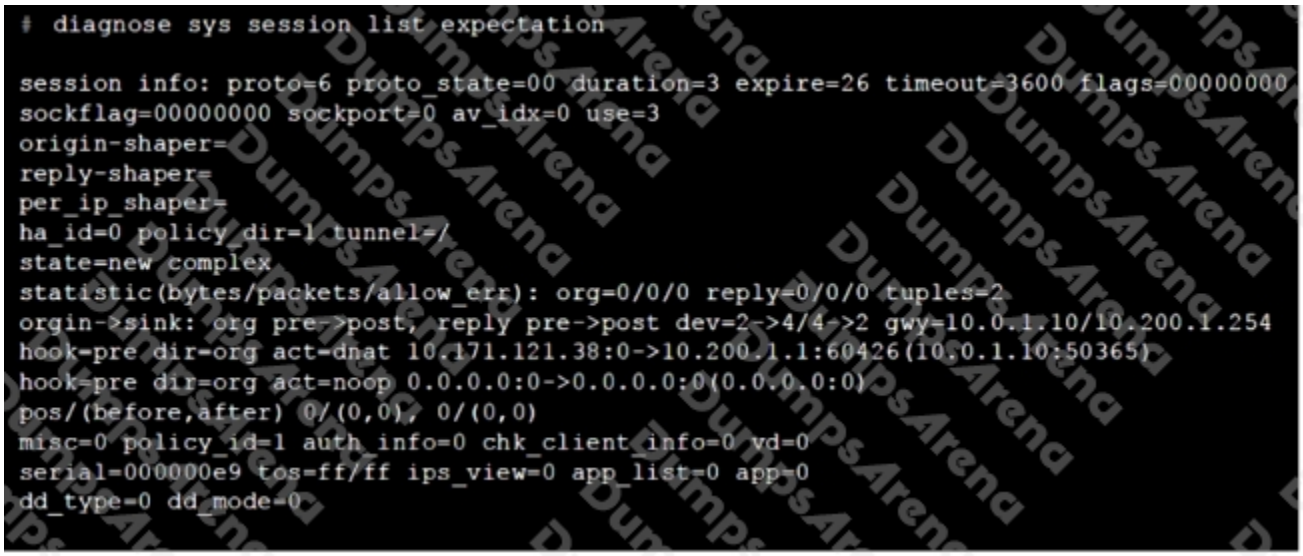
ANSWER: B

Explanation:

Enterprise_Firewall_7.0_Study_Guide-Online.pdf p 362

QUESTION NO: 10

Refer to the exhibit, which shows the output of a diagnose command.



What can you conclude from the output shown in the exhibit? (Choose two.)

A. This is a pinhole session created to allow traffic for a protocol that requires additional sessions to operate through FortiGate.

B. This is an expected session created by the IPS engine.

C. Traffic in the original direction (coming from the IP address 10.171.121.38) will be routed to the next-hop IP address 10.200.1.1.

D. Traffic in the original direction (coming from the IP address 10.171.121.38) will be routed to the next-hop IP address 10.0.1.10.

ANSWER: A D

Explanation:

Enterprise_Firewall_7.0_Study_Guide-Online.pdf p 110, 111, 115