NSE7_EFW Q&As

NSE7 Enterprise Firewall - FortiOS 5.4

Pass Fortinet NSE7_EFW Exam with 100% Guarantee

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

https://www.pass2lead.com/nse7_efw.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

View the exhibit, which contains the partial output of an IKE real time debug, and then answer the question below. The administrator does not have access to the remote gateway. Based on the debug output, what configuration changes can the administrator make to the local gateway to resolve the phase 1 negotiation error?

A. Change phase 1 encryption to AESCBC and authentication to SHA128.

B. Change phase 1 encryption to 3DES and authentication to CBC.

C. Change phase 1 encryption to AES128 and authentication to SHA512.

D. Change phase 1 encryption to 3DES and authentication to SHA256.

Correct Answer: C

QUESTION 2

Examine the output of the `get router info bgp summary\\' command shown in the exhibit; then answer the question below.

```
# get router info bgp summary
BGP router identifier 0.0.0.117, local AS number 65117
BGP table version is 104
3 BGP AS-PATH entries
0 BGP community entries

Neighbor        V    AS     MsgRcvd    MsgSent    TblVer    InQ    OutQ    Up/Down    State/PfxRcd
10.125.0.60     4    65060   1698       1756       103       0      0       03:02:49       1
10.127.0.75     4    65075   2206       2250       102       0      0       02:45:55       1
10.200.3.1      4    65501    101        115         0       0      0        never      Active
```

Which statements are true regarding the output in the exhibit? (Choose two.)

A. BGP state of the peer 10.125.0.60 is Established.

B. BGP peer 10.200.3.1 has never been down since the BGP counters were cleared.

C. Local BGP peer has not received an OpenConfirm from 10.200.3.1.

D. The local BGP peer has received a total of 3 BGP prefixes.

Correct Answer: AC

QUESTION 3

Four FortiGate devices configured for OSPF connected to the same broadcast domain. The first unit is elected as the designated router The second unit is elected as the backup designated router Under normal operation, how many OSPF full adjacencies are formed to each of the other two units?

A. 1

B. 2

C. 3

D. 4

Correct Answer: B

QUESTION 4

The CLI command set intelligent-mode controls the IPS engine\\'s adaptive scanning behavior. Which of the following statements describes IPS adaptive scanning?

A. Determines the optimal number of IPS engines required based on system load.

B. Downloads signatures on demand from FDS based on scanning requirements.

C. Determines when it is secure enough to stop scanning session traffic.

D. Choose a matching algorithm based on available memory and the type of inspection being performed.

Correct Answer: D

QUESTION 5

Examine the partial output from the IKE real time debug shown in the exhibit; then answer the question below.

```
#diagnose debug application ike-1
#diagnose debug enable
ike 0:····: 75: responder:aggressive mode get 1st message···
...
ike 0:····: 76: incoming proposal
ike 0:····: 76: proposal id=0:
ike 0:····: 76: protocol id=ISAKMP
ike 0:····: 76: trans_id=KEY_IKE.
ike 0:····: 76: encapsulation=IKE/none
ike 0:····: 76: type=OAKLEY_ENCRYPT_ALG, val=AES_CBC.
ike 0:····: 76: type=OAKLEY_HASH_ALG, val=SHA2_256.
ike 0:····: 76: type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0:····: 76: type=OAKLEY_GROUP, val=MODP2048.
ike 0:····: 76:ISAKMP SA lifetime=86400
ike 0:····: 76:my proposal, gw Remote:
ike 0:····: 76:proposal id=1:
ike 0:····: 76: protocol id=ISAKMP:
ike 0:····: 76: trans_id=KEY_IKE.
ike 0:····: 76: type=OAKLEY_ECNRYPT_ALG, val=DES_CBC.
ike 0:····: 76: type=OAKLEY_HASH_ALG, val=SHA2_256.
ike 0:····: 76: type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0:····: 76: type=OAKLEY_GROUP, val=MODP2048.
ike 0:····: 76:ISAKMP SA lifetime=86400
ike 0:····: 76:proposal id=1:
ike 0:····: 76: protocol id=ISAKMP:
ike 0:····: 76: trans id=KEY IKE.
ike 0:····: 76: encapsulation=IKE/none
ike 0:····: 76: type=OAKLEY_ECNRYPT_ALG, val=DES_CBC.
ike 0:····: 76: type=OAKLEY_HASH_ALG, val=SHA2_256.
ike 0:····: 76: type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0:····: 76: type=OAKLEY_GROUP, val=MODP1536.
ike 0:····: 76:ISAKMP SA lifetime=86400
ike 0:····: 76:negotiation failure
ike Negotiate ISAKMP SA Error:ike 0: ···: 76: no SA proposal chosen
```

Why didn\\'t the tunnel come up?

A. IKE mode configuration is not enabled in the remote IPsec gateway.

B. The remote gateway\\'s Phase-2 configuration does not match the local gateway\\'s phase-2 configuration.

C. The remote gateway\\'s Phase-1 configuration does not match the local gateway\\'s phase-1 configuration.

D. One IPsec gateway is using main mode, while the other IPsec gateway is using aggressive mode.

Correct Answer: B

QUESTION 6

Examine the output from the \\'diagnose debug authd fsso list\\' command; then answer the question below.

diagnose debug authd fsso list --FSSO logons-IP: 192.168.3.1 User: STUDENT Groups: TRAININGAD/USERS Workstation: INTERNAL2. TRAINING. LAB The IP address 192.168.3.1 is NOT the one used by the workstation INTERNAL2. TRAINING. LAB.

What should the administrator check?

A. The IP address recorded in the logon event for the user STUDENT.

B. The DNS name resolution for the workstation name INTERNAL2. TRAINING. LAB.

C. The source IP address of the traffic arriving to the FortiGate from the workstation INTERNAL2. TRAINING. LAB.

D. The reserve DNS lookup forthe IP address 192.168.3.1.

Correct Answer: C

QUESTION 7

View the exhibit, which contains the partial output of an IKE real-time debug, and then answer the question below.

```
ike 0:c49e59846861b0f6/0000000000000000:278:   responder:main mode get 1st message...
ike 0:c49e59846861b0f6/0000000000000000:278:   incoming proposal:
ike 0:c49e59846861b0f6/0000000000000000:278:   proposal id=0:
ike 0:c49e59846861b0f6/0000000000000000:278:     protocol id= ISAKMP:
ike 0:c49e59846861b0f6/0000000000000000:278:       trans_id=KEY_IKE
ike 0:c49e59846861b0f6/0000000000000000:278:       encapsulation=IKE/none
ike 0:c49e59846861b0f6/0000000000000000:278:         type=OAKLEY_ENCRYPT_ALG, val=3DES_CBC.
ike 0:c49e59846861b0f6/0000000000000000:278:         type=OAKLEY_HASH_ALG, val=PRESHARED_KEY
ike 0:c49e59846861b0f6/0000000000000000:278:         type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0:c49e59846861b0f6/0000000000000000:278:         type=OAKLEY_GROUP, val=MODP2048.
ike 0:c49e59846861b0f6/0000000000000000:278:   ISAKMP SA lifetime=86400
...
ike 0:c49e59846861b0f6/0000000000000000:278:   my proposal, gw VPN:
ike 0:c49e59846861b0f6/0000000000000000:278:   proposal id=1:
ike 0:c49e59846861b0f6/0000000000000000:278:     protocol id= ISAKMP:
ike 0:c49e59846861b0f6/0000000000000000:278:       trans_id=KEY_IKE
ike 0:c49e59846861b0f6/0000000000000000:278:       encapsulation=IKE/none
ike 0:c49e59846861b0f6/0000000000000000:278:         type=OAKLEY_ENCRYPT_ALG, val=AES_CBC,
key-len=256
ike 0:c49e59846861b0f6/0000000000000000:278:         type=OAKLEY_HASH_ALG, val=SHA2_256
ike 0:c49e59846861b0f6/0000000000000000:278:         type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0:c49e59846861b0f6/0000000000000000:278:         type=OAKLEY_GROUP, val=MODP2048
ike 0:c49e59846861b0f6/0000000000000000:278:   ISAKMP SA lifetime=86400
...
ike 0:c49e59846861b0f6/0000000000000000:278:   negotiation failure
ike Negotiate ISAKMP SA Error: ike 0:c49e59846861b0f6/0000000000000000:278:
proposal chosen
...
```

Why didn\\'t the tunnel come up?

A. The pre-shared keys do not match.

B. The remote gateway\\'s phase 2 configuration does not match the local gateway\\'s phase 2 configuration.

C. The remote gateway\\'s phase 1 configuration does not match the local gateway\\'s phase 1 configuration.

D. The remote gateway is using aggressive mode and the local gateway is configured to use man mode.

Correct Answer: C

QUESTION 8

View the IPS exit log, and then answer the question below.

diagnose test application ipsmonitor 3

ipsengine exit log"

pid = 93 (cfg), duration = 5605322 (s) at Wed Apr 19 09:57:26 2017

code = 11, reason: manual

What is the status of IPS on this FortiGate?

A. IPS engine memory consumption has exceeded the model-specific predefined value.

B. IPS daemon experienced a crash.

C. There are communication problems between the IPS engine and the management database.

D. All IPS-related features have been disabled in FortiGate\\'s configuration.

Correct Answer: B

QUESTION 9

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 10

Examine the partial output from two web filter debug commands; then answer the question below:

```
# diagnose test application urfilter 3
Domain | IP DB Ver   T URL
34000000 | 34000000   16.40224 P Bhttp://www.fgt99.com/
# get webfilter categories
g07 General Interest - Business:
   34 Finance and Banking
   37 Search Engines and Portals
   43 General organizations
   49 Business
   50 Information and computer security
   51 Government and Legal organizations
   52 Information Technology
```

Based on the above outputs, which is the FortiGuard web filter category for the web site www.fgt99.com?

A. Finance and banking

B. General organization.

C. Business.

D. Information technology.

Correct Answer: C

QUESTION 11

An administrator has configured a dial-up IPsec VPN with one phase 2, extended authentication (XAuth)

and IKE mode configuration. The administrator has also enabled the IKE real time debug:

diagnose debug application ike-1

diagnose debug enable

In which order is each step and phase displayed in the debug output each time a new dial-up user is

connecting to the VPN?

A. Phase1; IKE mode configuration; XAuth; phase 2.

B. Phase1; XAuth; IKE mode configuration; phase2.

C. Phase1; XAuth; phase 2; IKE mode configuration.

D. Phase1; IKE mode configuration; phase 2; XAuth.

Correct Answer: D

QUESTION 12

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

```
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 teb=0
dpd: mode=on-demand on=1 idle=20000 ms 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: 0:10.1.2.0/255.255.0:0
   dst: 0:10.1.1.0/255.255.255.0:0
   SA: ref=3 options=2e type=00 soft=0 mtu=1438 expire=42403/OB replaywin=2048 segno=1 esn=0
replaywin_lastseq=00000000
   life: type=01 bytes=0/0 timeout=43177/43200
   dec: spi=cccl f66d esp=aes key=16 280e5cd6f9bacc65ac771556c464ffbd
      ah=shal key=20 c68091d68753578785de6a7a6b276b506c527efe
   enc: spi=df14200b esp=aes key=16 b02a7e9f5542b69aff6aa391738ee393
   ah=shal key20 889f7529887c215c25950be2ba86e6fela5367be
   dec: pkts/bytes=0/0, enc:pkts/bytes=0/0
```

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

A. Anti-reply is enabled.

B. DPD is disabled.

C. Quick mode selectors are disabled.

D. Remote gateway IP is 10.200.5.1.

Correct Answer: A

QUESTION 13

Two independent FortiGate HA clusters are connected to the same broadcast domain. The administrator

has reported that both clusters are using the same HA virtual MAC address. This creates a duplicated

MAC address problem in the network.

What HA setting must be changed in one of the HA clusters to fix the problem?

A. Group ID.

B. Group name.

C. Session pickup.

D. Gratuitous ARPs.

Correct Answer: A

QUESTION 14

Examine the following partial output from two system debug commands; then answer the question below.

```
# diagnose hardware sysinfo memory
MemTotal: 3092728 kB
MemFree: 1954204 kB
MemShared: 0 kB
Buffers: 284 kB
Cached: 143004 kB
SwapCached: 0 kB
Active: 34092 kB
Inactive: 109256 kB
HighTotal: 117948 kB
HighFree: 853516 kB
LowTotal: 1913080 kB
LowFree: 1100688 kB
SwapTotal: 0 kB
SwapFree: 0 kB
# diagnose hardware sysinfo shm
SHM counter: 285
SHM allocated: 6823936
SHM total: 623452160
concervemode: 0
shm last entered: n/a
SHM FS total: 639725568
SHM FS free: 632614912
```

```
SHM FS alloc: 7110656
```

Which of the following statements are true regarding the above outputs? (Choose two.)

A. The unit is running a 32-bit FortiOS

B. The unit is in kernel conserve mode

C. The Cached value is always the Active value plus the Inactive value

D. Kernel indirectly accesses the low memory (LowTotal) through memory paging

Correct Answer: AC

QUESTION 15

Examine the output of the `diagnose sys session list expectation\\' command shown in the exhibit; than answer the question below.

```
#diagnose sys session list expectation

session info: proto= proto_state=0 0 duration=3 expire=26 timeout=3600
flags=00000000
sockflag='00000000'sockport=0'av_idx=0' use=3q
origin-shaper=q
reply-shaper=q
per-ip_shaper=q
ha_id=0'policy_dir=1'tunnel=/q
state=new complex
statistic (bytes/packets/allow_err): org=0/0/0 reply=0/0/0 tuples=2
orgin-> sink: org pre-> post, reply pre->post dev=2->4/4->2
gwy=10.0.1.10/10.200.1.254
hook=pre dir=org act=dnat 10.171.121.38:0 -> 10.200.1.1: 60426
(10.0.1.10: 50365)q
hook= pre dir=org act=noop 0.0.0.0.:0->0.0.0.0:0(0.0.0.0:0)
pos/(before, after) 0/(0,0),0/(0,0)
misc=0'policy_id=1'auth_info=0'chk_client_info=0'vd=0
serial1=00000e9'tos=ff/ff`ips_view=0 app_list=0'app=0
dd type=0'dd_mode=0q
```

Which statement is true regarding the session in the exhibit?

A. It was created by the FortiGate kernel to allow push updates from FotiGuard.

B. It is for management traffic terminating at the FortiGate.

C. It is for traffic originated from the FortiGate.

D. It was created by a session helper or ALG.

Correct Answer: A