NSE7^(Q&As)

Fortinet Troubleshooting Professional

Pass Fortinet NSE7 Exam with 100% Guarantee

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

https://www.pass4itsure.com/nse7.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

Examine the following partial output from a sniffer command; then answer the question below.

```
# diagnose sniff packet any 'icmp' 4
interfaces= [any]
filters = [icmp]
2.101199 wan2 in 192.168.1.110-> 4.2.2.2: icmp: echo request
2.101400 wan1 out 172.17.87.16-> 4.2.2.2: icmp: echo request
......
2.123500 wan2 out 4.2.2.2-> 192.168.1.110: icmp: echo reply
244 packets received by filter
5 packets dropped by kernel
```

What is the meaning of the packets dropped counter at the end of the sniffer?

A. Number of packets that didn\\'t match the sniffer filter.

B. Number of total packets dropped by the FortiGate.

C. Number of packets that matched the sniffer filter and were dropped by the FortiGate.

D. Number of packets that matched the sniffer filter but could not be captured by the sniffer.

Correct Answer: C

QUESTION 2

View the exhibit, which contains the output of a BGP debug command, and 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

Total number of neighbors 3
```

Which of the following statements about the exhibit are true? (Choose two.)

A. For the peer 10.125.0.60, the BGP state of is Established.

B. The local BGP peer has received a total of three BGP prefixes.

C. Since the BGP counters were last reset, the BGP peer 10.200.3.1 has never been down.

D. The local BGP peer has not established a TCP session to the BGP peer 10.200.3.1.

Correct Answer: BC

QUESTION 3

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

```
# diagnose debug application urlfilter -1
# diagnose debug enable

msg="received a request /tmp/.ipsengine_498_0_0.url.socket, addr_len=37:
d=www.fortinet.com:80
id=83, vfname='root', vfid=0, profile='default', type=0, client=10.0.1.10,
url_source=1, url="/"
msg="Found it in cache.   URL cat=52" IP cat=52user="N/A" src=10.0.1.10
sport=60348 dst=66.171.121.44 dport=80 service="http" hostname="
www.fortinet.com" url="/" matchType=prefix
action=10(ftgd-block) wf-act=3(BLOCK) user="N/A" src=10.0.1.10 sport=60348
dst=66.171.121.44
dport=80 service="http" cat=52 cat desc="Information Technology"
hostname="fortinet.com"
url="/"
```

Which of the following statements is true regarding this output? (Choose two.)

A. This web request was inspected using the root web filter profile.

B. FortiGate found the requested URL in its local cache.

C. The requested URL belongs to category ID 52.

D. The web request was allowed by FortiGate.

Correct Answer: BC

QUESTION 4

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

ike 0: comes 10.0.0.2:500->10.0.0.1:500, ifindex=7.... ike 0: IKEv1 exchange=Aggressive
id=baf47d0988e9237f/2f405ef3952f6fda len=430 ike 0: in

BAF47D0988E9237F2F405EF3952F6FDA011004000000000000001AE0400003C00000
001000000001000000300101000 ike 0:RemoteSite:4: initiator: aggressive mode get 1st response... ike 0:RemoteSite:4:
VID RFC 3947 4A131c81070358455C5728F20E95452F ike 0:RemoteSite:4: VID DPD
AFCAD71368A1F1C96B8696FC77570100 ike 0:RemoteSite:4: VID FORTIGATE
8299031757A36082C6A621DE000502D7 ike 0:RemoteSite:4: peer is FortiGate/Fortios (v5 b727)

ike 0:RemoteSite:4: VID FRAGMENTATION 4048B7D56EBCE88525E7DE7F00D6C2D3 ike 0:RemoteSite:4: VID
FRAGMENTATION 4048B7D56EBCE88525E7DE7F00D6C2D3C0000000

ike 0:RemoteSite:4: received peer identifier FQDN `remore\\'

ike 0:RemoteSite:4: negotiation result

ike 0:RemoteSite:4: proposal id = 1:

ike 0:RemoteSite:4: protocol id = ISAKMP:

ike 0:RemoteSite:4: trans_id = KEY_IKE.

ike 0:RemoteSite:4: encapsulation = IKE/none

ike 0:RemoteSite:4: type=OAKLEY_ENCRYPT_ALG, val=AES_CBC, key ?en=128

ike 0:RemoteSite:4: type=OAKLEY_HASH_ALG, val=SHA.

ike 0:RemoteSite:4: type-AUTH_METHOD, val=PRESHARED_KEY.

ike 0:RemoteSite:4: type=OAKLEY_GROUP, val=MODP1024.

ike 0:RemoteSite:4: ISAKMP SA lifetime=86400

ike 0:RemoteSite:4: ISAKMP SA baf47d0988e9237f/2f405ef3952f6fda key 16:

B25B6C9384D8BDB24E3DA3DC90CF5E73

ike 0:RemoteSite:4: PSK authentication succeeded

ike 0:RemoteSite:4: authentication OK

ike 0:RemoteSite:4: add INITIAL-CONTACT

ike 0:RemoteSite:4: enc BAF47D0988E9237F405EF3952F6FDA081004010000000000000080140000181F2E48BF
D8E9D603F ike 0:RemoteSite:4: out

BAF47D0988E9237F405EF3952F6FDA0810040100000000000008C2E3FC9BA061816A 396F009A12

ike 0:RemoteSite:4: sent IKE msg (agg_i2send): 10.0.0.1:500-10.0.0.2:500, len=140, id=baf47d0988e9237f/2 ike
0:RemoteSite:4: established IKE SA baf47d0988e9237f/2f405ef3952f6fda

Which statements about this debug output are correct? (Choose two.)

A. The remote gateway IP address is 10.0.0.1.

B. It shows a phase 1 negotiation.

C. The negotiation is using AES128 encryption with CBC hash.

D. The initiator has provided remote as its IPsec peer ID.

Correct Answer: BD

QUESTION 5

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