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.leads4pass.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

What conditions are required for two FortiGate devices to form an OSPF adjacency? (Choose three.)

A. IP addresses are in the same subnet.

B. Hello and dead intervals match.

C. OSPF IP MTUs match.

D. OSPF peer IDs match.

E. OSPF costs match.

Correct Answer: ABD

QUESTION 2

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 3

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/PrxRcd
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 4

Examine the output of the `diagnose ips anomaly list\\' command shown in the exhibit; then answer the question below.

```
# diagnose ips anomaly list

list nids meter:
id=ip_dst_session      ip=192.168.1.10     dos_id=2    exp=3646    pps=0    freq=0
id=udp_dst_session     ip=192.168.1.10     dos_id=2    exp=3646    pps=0    freq=0
id=udp_scan            ip=192.168.1.110    dos_id=1    exp=649     pps=0    freq=0
id=udp_flood           ip=192.168.1.110    dos_id=2    exp=653     pps=0    freq=0
id=tcp_src_session     ip=192.168.1.110    dos_id=1    exp=5175    pps=0    freq=8
id=tcp_port_scan       ip=192.168.1.110    dos_id=1    exp=175     pps=0    freq=0
id=ip_src_session      ip=192.168.1.110    dos_id=1    exp=5649    pps=0    freq=30
id=udp_src_session     ip=192.168.1.110    dos_id=1    exp=5649    pps=0    freq=22
```

Which IP addresses are included in the output of this command?

A. Those whose traffic matches a DoS policy.

B. Those whose traffic matches an IPS sensor.

C. Those whose traffic exceeded a threshold of a matching DoS policy.

D. Those whose traffic was detected as an anomaly by an IPS sensor.

Correct Answer: A

QUESTION 5

View the exhibit, which contains a session entry, and then answer the question below.

```
session info: proto=1 proto_state=00 duration=1 expire=59 timeout=0 flags=00000000
sockflag=00000000 sockport=0 av_idx=0 use=3
origin-shaper=
reply-shaper=
per_ip_shaper=
ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
state=log may_dirty none
statistic(bytes/packets/allow_err): org=168/2/1 reply=168/2/1 tuples=2
tx speed(Bps/kbps): 97/0 rx speed(Bps/kbps): 97/0
orgin->sink: org pre->post, reply pre->post dev=9->3/3->9 gwy=10.200.1.254/10.1.0.1
hook=post dir=org act=snat 10.1.10.10:40602->10.200.5.1:8(10.200.1.254/10.1.0.1
hook=pre dir=reply act=dnat 10.200.5.1:60430->10.200.1.1:0(10.1.10.10:40602)
misc=0 policy_id=1 auth_info=0 chk_client_info=0 vd=0
serial=0002a5c9 tos=ff/ff app_list=0 app=0 url_cat=0
dd_type=0 dd_mode=0
```

Which statement is correct regarding this session?

A. It is an ICMP session from 10.1.10.10 to 10.200.1.1.

B. It is an ICMP session from 10.1.10.10 to 10.200.5.1.

C. It is a TCP session in ESTABLISHED state from 10.1.10.10 to 10.200.5.1.

D. It is a TCP session in CLOSE_WAIT state from 10.1.10.10 to 10.200.1.1.

Correct Answer: A