Fortinet

Exam Questions NSE7_EFW-7.0

Fortinet NSE 7 - Enterprise Firewall 7.0

NEW QUESTION 1
Refer to the exhibit, which shows a session entry. Which statement about this session is true?

```
session info: proto=1 proto_state=00 duration=1 expire=59 timeout
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 tup
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.
hook=post dir=org act=snat 10.1.10.10:40602->10.200.5.1:8(10.200.
hook=pre dir=reply act=dnat 10.200.5.1:60430->10.200.1.1:0(10.1.1
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
```

A. It is an ICMP session from 10.1.10.10 to 10.200.5. 1.
B. It is a TCP session in close_wait state, from 10.
C. 10.10 to 10.200.1.1.
D. It is an ICMP session from 10.1.10.10 to 10.200.1.1.
E. It is a TCP session in the established state, from 10.1.10.10 to 10.200.5.1.

Answer: A

NEW QUESTION 2
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.

Answer: B

NEW QUESTION 3
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 use
B. This limit CANNOT be modified by the administrator.
C. FortiGate limits the total number of simultaneous explicit web proxy users.
D. FortiGate limits the number of simultaneous sessions per explicit web proxy user The limit CAN be modified by the administrator
E. FortiGate limits the number of workstations that authenticate using the same web proxy user credentials.This limit CANNOT be modified by the administrator.

Answer: B

Explanation:
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.

NEW QUESTION 4
What does the dirty flag mean in a FortiGate session?

A. Traffic has been blocked by the antivirus inspection.
B. The next packet must be re-evaluated against the firewall policies.
C. The session must be removed from the former primary unit after an HA failover.
D. Traffic has been identified as from an application that is not allowed.

Answer: B

Explanation:
https://kb.fortinet.com/kb/viewContent.do?externalId=FD40119&sliceId=1

NEW QUESTION 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: AD

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

NEW QUESTION 6
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.

Answer: C

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

NEW QUESTION 7
View the exhibit, which contains the output of a debug command, and then answer the question below.

```
# get router info ospf interface port4
port4 is up, line protocol is up
    Internet Address 172.20.121.236/24, Area 0.0.0.0, MTU 1500
    Process ID 0, Router ID 0.0.0.4, Network Type BROADCAST, Cost: 1
    Transmit Delay is 1 sec, State DROther, Priority 1
    Designated Router (ID) 172.20.140.2, Interface Address 172.20.121.2
  Backup Designated Router (ID) 0.0.0.1, Interface Address 172.20.121.239
    Timer intervals configured, Hello 10.000, Dead 40, Wait 40, Retransmit 5
        Hello due in 00:00:05
    Neighbor Count is 4, Adjacent neighbor count is 2
    Crypt Sequence Number is 411
    Hello received 106, sent 27, DD received 7 sent 9
    LS-Req received 2 sent 2, LS-Upd received 7 sent 5
    LS-Ack received 4 sent 3, Discarded 1
```

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

A. In the network on port4, two OSPF routers are down.
B. Port4 is connected to the OSPF backbone area.
C. The local FortiGate's OSPF router ID is 0.0.0.4
D. The local FortiGate has been elected as the OSPF backup designated router.

Answer: BC

NEW QUESTION 8
An administrator cannot connect to the GIU of a FortiGate unit with the IP address 10.0.1.254. The administrator runs the debug flow while attempting the
connection using HTTP. The output of the debug flow is shown in the exhibit:

```
# diagnose debug flow filter port 80
# diagnose debug flow trace start 5
# diagnose debug enable

id=20085 trace_id=5 msg="vd-root received a packet(proto=6,
10.0.1.10:57459->10.0.1.254:80) from port3. flag [S], seq 3190430861, ack
0, win 8192"
id=20085 trace_id=5 msg="allocate a new session-0000008c"
id=20085 trace_id=5 msg="iprope_in_check() check failed on policy 0, drop"
```

Based on the error displayed by the debug flow, which are valid reasons for this problem? (Choose two.)

A. HTTP administrative access is disabled in the FortiGate interface with the IP address 10.0.1.254.
B. Redirection of HTTP to HTTPS administrative access is disabled.
C. HTTP administrative access is configured with a port number different than 80.
D. The packet is denied because of reverse path forwarding check.

Answer: AC

NEW QUESTION 9
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.

Answer: A

Explanation:
https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-high-availability-52/HA_failoverVMAC.htm

NEW QUESTION 10
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?

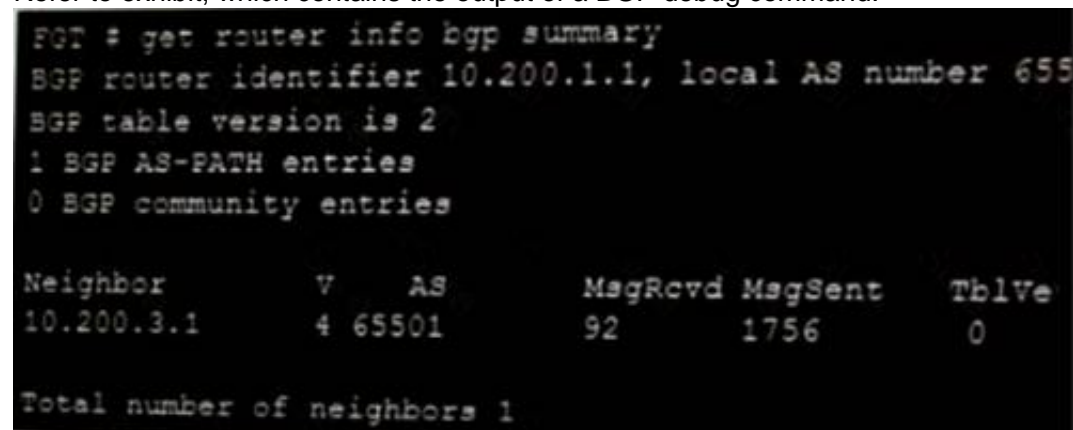A. redir.
B. dirty.
C. synced
D. nds.

Answer: C

Explanation:
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.

NEW QUESTION 10
Refer to exhibit, which contains the output of a BGP debug command.

Which statement explains why the state of the 10.200.3.1 peer is Connect?

A. The local router is receiving BGP keepalives from the remote peer, but the local peer has not received the OpenConfirm yet.
B. The TCP session to 10.200.3.1 has not completed the three-way handshake.
C. The local router is receiving the BGP keepalives from the peer, but it has not received a BGP prefix yet.
D. The local router has received the BGP prefixes from the remote peer.

Answer: B

Explanation:
BGP neighbor states and how they change:• Idle: Initial state• Connect: Waiting for a successful three-way TCP connection• Active: Unable to establish the TCP session• OpenSent: Waiting for an OPEN message from the peer• OpenConfirm: Waiting for the keepalive message from the peer• Established: Peers have successfully exchanged OPEN and keepalive messages

NEW QUESTION 12
Examine the following partial outputs from two routing debug commands; then answer the question below:

```
#get router info routing-table database
S      0.0.0.0/. [20/0] via 10.200.2.254, port2, [10/0]
S      *> 0.0.0.0/0 [10/0] via 10.200.1.254, port1
# get router info routing-table all
S*     0.0.0.0/0 [10/0] via 10.200.1.254, port1
```

Why the default route using port2 is not displayed in the output of the second command?

A. It has a lower priority than the default route using port1.
B. It has a higher priority than the default route using port1.
C. It has a higher distance than the default route using port1.
D. It is disabled in the FortiGate configuration.

Answer: C

Explanation:
http://kb.fortinet.com/kb/viewContent.do?externalId=FD32103

NEW QUESTION 16
Refer to the exhibits.

```
config vpn ipsec phase1-interface
  edit "user-1"
    set type dynamic
    set interface "port1"
    set mode main
    set xauthtype auto
    set authusrgrp "Users-1"
    set peertype any
    set dhgrp 14 15 19
    set proposal aes128-sha256 aes256-sha384
    set psksecret <encrypted_password>
  next
```

Which contain the partial configurations of two VPNs on FortiGate.
An administrator has configured two VPNs for two different user groups. Users who are in the Users-2 group are not able to connect to the VPN. After running a diagnostics command, the administrator discovered that FortiGate is not matching the user-2 VPN for members of the Users-2 group.
Which two changes must administrator make to fix the issue? (Choose two.)

A. Use different pre-shared keys on both VPNs
B. Enable Mode Config on both VPNs.
C. Set up specific peer IDs on both VPNs.
D. Change to aggressive mode on both VPNs.

Answer: CD

NEW QUESTION 20
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. The administrator decides to enable the setting link-failed-signal to fix the problem.
Which statement about this setting is true?

A. It sends an ARP packet to all connected devices, indicating that the HA virtual MAC address is reachable through a new master after a failover.
B. It sends a link failed signal to all connected devices.
C. It disabled all the non-heartbeat interfaces in all HA members for two seconds after a failover.
D. It forces the former primary device to shut down all its non-heartbeat interfaces for one second, while the failover occurs.

Answer: D

NEW QUESTION 21
When using the SSL certificate inspection method for HTTPS traffic, how does FortiGate filter web requests when the browser client does not provide the server name indication (SNI) extension?

A. FortiGate uses CN information from the Subject field in the server's certificate.
B. FortiGate switches to the full SSL inspection method to decrypt the data.
C. FortiGate blocks the request without any further inspection.
D. FortiGate uses the requested URL from the user's web browser.

Answer: A

NEW QUESTION 22
A FortiGate's portl is connected to a private network. Its port2 is connected to the Internet. Explicit web proxy is enabled in port1 and only explicit web proxy users can access the Internet. Web cache is NOT enabled. An internal web proxy user is downloading a file from the Internet via HTTP. Which statements are true regarding the two entries in the FortiGate session table related with this traffic? (Choose two.)

A. Both session have the local flag on.
B. The destination IP addresses of both sessions are IP addresses assigned to FortiGate's interfaces.
C. One session has the proxy flag on, the other one does not.
D. One of the sessions has the IP address of port2 as the source IP address.

Answer: AD

NEW QUESTION 27
A FortiGate device has the following LDAP configuration:

```
config user ldap
    edit "WindowsLDAP"
        set server "10.0.1.10"
        set cnid "cn"
        set dn "cn=Users, dc=trainingAD, dc=training, dc=lab"
        set type regular
        set username "dc=trainingAD, dc=training, dc=lab"
        set password xxxxxxx
    next
end
```

The administrator executed the 'dsquery' command in the Windows LDAp server 10.0.1.10, and got the following output:
>dsquery user –samid administrator

"CN=Administrator, CN=Users, DC=trainingAD, DC=training, DC=lab" Based on the output, what FortiGate LDAP setting is configured incorrectly?

A. cnid.
B. username.
C. password.
D. dn.

Answer: B

Explanation:
https://kb.fortinet.com/kb/viewContent.do?externalId=FD37516

NEW QUESTION 29
View the exhibit, which contains a partial web filter profile configuration, and then answer the question below.

Which action will FortiGate take if a user attempts to access www.dropbox.com, which is categorized as File Sharing and Storage?

A. FortiGate will exempt the connection based on the Web Content Filter configuration.
B. FortiGate will block the connection based on the URL Filter configuration.
C. FortiGate will allow the connection based on the FortiGuard category based filter configuration.
D. FortiGate will block the connection as an invalid URL.

Answer: B

Explanation:
fortigate does it in order Static URL -> FortiGuard – > Content -> Advanced (java, cookie removal..)so block it in first step

NEW QUESTION 34
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.

Answer: B

Explanation:
https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-ipsecvpn-54/IPsec_VPN_Concepts/IKE_Packet

NEW QUESTION 35
Which statement is true regarding File description (FD) conserve mode?

A. IPS inspection is affected when FortiGate enters FD conserve mode.
B. A FortiGate enters FD conserve mode when the amount of available description is less than 5%.
C. FD conserve mode affects all daemons running on the device.
D. Restarting the WAD process is required to leave FD conserve mode.

Answer: B

NEW QUESTION 36
What global configuration setting changes the behavior for content-inspected traffic while FortiGate is in system conserve mode?

A. av-failopen
B. mem-failopen
C. utm-failopen
D. ips-failopen

Answer: A

Explanation:
https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-security-profiles-54/Other_Profile_Consideratio

NEW QUESTION 39
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.

Answer: D

Explanation:
The command diagnose test application ipsmonitor includes many options that are useful for troubleshooting purposes.Option 3 displays the log entries generated every time an IPS engine process stopped. There are various reasons why these logs are generated:Manual: Because of the configuration, IPS no longer needs to run (that is, all IPS-releated features have been disabled)

NEW QUESTION 43
When does a RADIUS server send an Access-Challenge packet?

A. The server does not have the user credentials yet.
B. The server requires more information from the user, such as the token code for two-factor authentication.
C. The user credentials are wrong.
D. The user account is not found in the server.

Answer: B

NEW QUESTION 45
Which two conditions must be met for a statistic route to be active in the routing table? (Choose two.)

A. The link health monitor (if configured) is up.
B. There is no other route, to the same destination, with a higher distance.
C. The outgoing interface is up.
D. The next-hop IP address is up.

Answer: AC

NEW QUESTION 48
Which configuration can be used to reduce the number of BGP sessions in an IBGP network?

A. Neighbor range
B. Route reflector
C. Next-hop-self
D. Neighbor group

Answer: B

Explanation:
Route reflectors help to reduce the number of IBGP sessions inside an AS. A route reflector forwards the routers learned from one peer to the other peers. If you configure route reflectors, you dont' need to create a full mesh IBGP network. All clients in a cluster only talck to route reflector to get sync routing updates. Route reflectors pass the routing updates to other route reflectors and border routers within the AS.

NEW QUESTION 52
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.

Answer: A

NEW QUESTION 55
Which statement about the designated router (DR) and backup designated router (BDR) in an OSPF multi-access network is true?

A. FortiGate first checks the OSPF ID to elect a DR.
B. Non-DR and non-BDR routers will form full adjacencies to DR and BDR only.
C. BDR is responsible for forwarding link state information from one router to another.
D. Only the DR receives link state information from non-DR routers.

Answer: B

NEW QUESTION 57
Refer to the exhibit, which contains the partial output of the get vpn ipsec tunnel details command.

```
Hub # get vpn ipsec tunnel details
gateway
    name: 'Hub2Spoke1'
    type: route-based
    local-gateway: 10.10.1.1:0 (static)
    remote-gateway: 10.10.2.2:0 (static)
    mode: ike-v1
    interface: 'wan2' (6)
    rx packets: 1025 bytes: 524402 errors: 0
    tx packets: 641 bytes: 93 errors: 0
    dpd: on-demand/negotiated idle: 20000ms retry: 3 count: 0
    selectors
        name: 'Hub2Spoke1'
        auto-negotiate: disable
        mode: tunnel
        src: 0:192.168.1.0/0.0.0.0:0
        dst: 0:10.10.20.0/0.0.0.0:0
        SA
          lifetime/rekey: 43200/32137
          mtu: 1438
          tx-esp-seq: 2ce
          replay: enabled
          inbound
            spi: 01e54b14
            enc:  aes-cb 914dc5d092667ed436ea7f6efb867976
            auth: sha1 a81b019d4cdfda32ce51e6b01d0b1ea42a74adce
          outbound
            spi: 3dd3545f
            enc:  aes-cb 017b8ff6c4ba21eac99b22380b7de74d
```

Based on the output, which two statements are correct? (Choose two.)

A. Phase 2 authentication is set to sha1 on both sides.
B. Anti-replay is disabled.
C. Hub2Spoke1 is a policy-based VPN.
D. Hub2Spoke1 is configured on interface wan2.

Answer: AD

NEW QUESTION 60
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.

Answer: AD

NEW QUESTION 64
An administrator has configured two FortiGate devices for an HA cluster. While testing the HA failover, the administrator noticed that some of the switches in the network continue to send traffic to the former primary unit. The administrator decides to enable the setting link-failed-signal to fix the problem. Which statement is correct regarding this command?

A. Forces the former primary device to shut down all its non-heartbeat interfaces for one second while the failover occurs.
B. Sends an ARP packet to all connected devices, indicating that the HA virtual MAC address is reachable through a new master after a failover.
C. Sends a link failed signal to all connected devices.
D. Disables all the non-heartbeat interfaces in all the HA members for two seconds after a failover.

Answer: A

NEW QUESTION 69
View the exhibit, which contains the output of a diagnose command, and then answer the question below.

```
       diagnose sys session list expectation

session info: proto=6 proto_state-00 duration=3 expire=26 timeout=3600 flags=00000000
sockflag=00000000 sockport=0 av_idx=0 use=3
origin-shaper=
reply-shaper=
ha_id-0 policy_dir=1 tunnel=/
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)
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
serial=000000e9 tos=ff/ff ips_view=0 app_list=0 app=0
dd_type=0 dd_mode=0
```

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

A. This is an expected session created by a session helper.
B. Traffic in the original direction (coming from the IP address 10.171.122.38) will be routed to the next-hop IP address 10.0.1.10.
C. Traffic in the original direction (coming from the IP address 10.171.122.38) will be routed to the next-hop IP address 10.200.1.1.
D. This is an expected session created by an application control profile.

Answer: AC

NEW QUESTION 72
View these partial outputs from two routing debug commands:

```
# get router info kernel
tab=254 vf=0 scope=0 type=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=0 type=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=10.200.2.254
dev=3(port2)
tab=254 vf=0 scope=253 type=1 proto=2 prio=0 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, port1
               [10/0] via 10.200.2.254, port2, [10/0]
C      10.0.1.0/24 is directly connected, port3
C      10.200.1.0/24 is directly connected, port1
C      10.200.2.0/24 is directly connected, port2
```

Which outbound interface will FortiGate use to route web traffic from internal users to the Internet?

A. Both port1 and port2
B. port3
C. port1
D. port2

Answer: C

NEW QUESTION 74
Which two statements about FortiManager is true when it is deployed as a local FDS? (Choose two.)

A. It caches available firmware updates for unmanaged devices.
B. It can be configured as an update server, or a rating server, but not both.
C. It supports rating requests from both managed and unmanaged devices.
D. It provides VM license validation services.

Answer: CD

NEW QUESTION 75
What is the diagnose test application ipsmonitor 99 command used for?

A. To enable IPS bypass mode
B. To provide information regarding IPS sessions
C. To disable the IPS engine
D. To restart all IPS engines and monitors

Answer: D

NEW QUESTION 80
Refer to the exhibit, which contains the output of diagnose sys session list.

```
# diagnose sys session list
session info: proto=6 proto_state=01 duration=73 expire=3597 timeout=3600
flags=00000000 sockflag=00000000 sockport=0 av_idx=0 use=3
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
state=may_dirty synced none app_ntf
statistic(bytes/packets/allow_err): org=822/11/1 reply=9037/15/1 tuples=2
orgin->sink: org pre->post, reply pre->post dev=4->2/2->4
gwy=100.64.1.254/10.0.1.10
hook=post dir=org act=snat 10.0.1.10:65464->54.192.15.182:80(100.64.1.1:65464)
hook=pre dir=reply act=dnat 54.192.15.182:80->100.64.1.1:65464(10.0.1.10:65464)
pos/(before,after) 0/(0,0), 0/(0,0)
misc=0 policy_id=1 auth_info=0 chk_client_info=0 vd=0
serial=00000098 tos=ff/ff ips_view=0 app_list=0 app=0
dd_type=0 dd_mode=0
```

If the HA ID for the primary unit is zero (0), which statement about the output is true?

A. This session cannot be synced with the slave unit.
B. The inspection of this session has been offloaded to the slave unit.
C. The master unit is processing this traffic.
D. This session is for HA heartbeat traffic.

Answer: C

NEW QUESTION 81
......

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

NSE7_EFW-7.0 Practice Exam Features:

* NSE7_EFW-7.0 Questions and Answers Updated Frequently

* NSE7_EFW-7.0 Practice Questions Verified by Expert Senior Certified Staff

* NSE7_EFW-7.0 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* NSE7_EFW-7.0 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
Order The NSE7_EFW-7.0 Practice Test Here