

Exam Questions NSE7_EFW-7.0

Fortinet NSE 7 - Enterprise Firewall 7.0

https://www.2passeasy.com/dumps/NSE7_EFW-7.0/



NEW QUESTION 1

View the exhibit, which contains an entry in the session table, and then answer the question below.

```
session info: proto=6 proto_state=11 duration=53 expire=265 timeout=300 flags=00000000
sockflag=00000000
origin-shaper=
reply-shaper=
per_ip_shaper=
ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
user=AALI state=redir log local may_dirty npu nlb none acct-ext
statistic (bytes/packets/allow_err): org=2651/17/1 reply=19130/28/1 tuples=3
tx speed (Bps/kbps): 75/0 rx speed (Bps/kbps): 542/4
origin->sink: org pre->post, reply pre->post dev=7->6/6->7 gw=172.20.121.2/10.0.0.2
hook=post dir=org act=snat 192.167.1.100:49545->216.58.216.238:443(172.20.121.96:49545)
hook=pre dir=reply act=dnat 216.58.216.238:443->172.20.121.96:49545 (192.167.1.100:49545)
hook=post dir=reply act=noop 216.58.216.238:443->192.167.1.100:49545 (0.0.0.0:0)
pos/(before, after) 0/(0,0), 0/(0,0)
src_mac=08:5b:0e:6c:7b:7a
misc=0 policy_id=21 auth_info=0 chk_client_info=0 vd=0
serial=007f2948 tos=ff/ff app_list=0 app=0 url_cat=41
dd_type=0 dd_mode=0
npu_state=00000000
npu info: flag=0x00/0x00, offload=0/0, ips_offload=0/0, epid=0/0, ipid=0/0, vlan=0x0000/0x0000
vlfid=0/0, vtag_in=0x0000/0x0000 in_npu=0/0, out_npu=0/0, fwd_en=0/0, qid=0/0
```

Which one of the following statements is true regarding FortiGate's inspection of this session?

- A. FortiGate applied proxy-based inspection.
- B. FortiGate forwarded this session without any inspection.
- C. FortiGate applied flow-based inspection.
- D. FortiGate applied explicit proxy-based inspection.

Answer: A

Explanation:

<https://kb.fortinet.com/kb/viewContent.do?externalId=FD30042>

NEW QUESTION 2

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 3

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 4

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
```

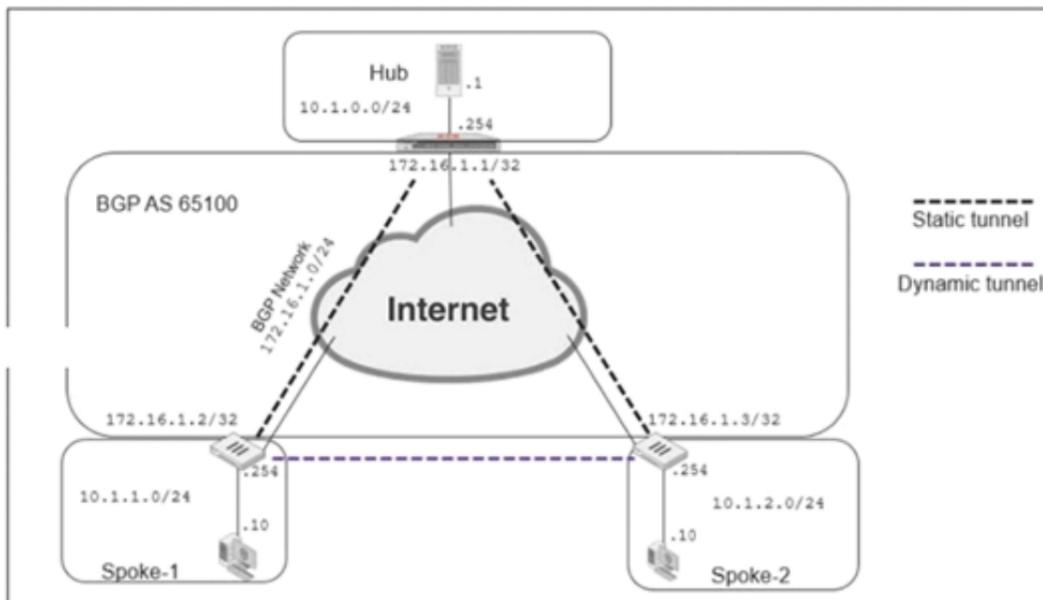
Which of the following statements about the exhibit are true? (Choose two.)

- 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 5

Exhibits:



```
show router bgp
router bgp
  as 65100
  router-id 172.16.1.1
fig neighbor-group
  edit "advpn"
    set remote-as 65100

    set route-reflector-client disable
  next
fig neighbor-range
  edit 1
    set prefix 172.16.1.0 255.255.255.0
    set neighbor-group "advpn"
  next
```

Refer to the exhibits, which contain the network topology and BGP configuration for a hub. An administrator is trying to configure ADVPN with a hub-spoke VPN setup using iBGP. All the VPNs are up and connected to the hub. The hub is receiving route information from both spokes over iBGP; however, the spokes are not receiving route information from each other. What change must the administrator make to the hub BGP configuration so that the routes learned by one spoke are forwarded to the other spokes?

- A. Configure an individual neighbor and remove neighbor-range configuration.
- B. Configure the hub as a route reflector client.
- C. Change the router id to 10.1.0.254.
- D. Make the configuration of remote-as different from the configuration of local-as.

Answer: B

NEW QUESTION 6

How does FortiManager handle FortiGuard requests from FortiGate devices, when it is configured as a local FDS?

- A. FortiManager can download and maintain local copies of FortiGuard databases.
- B. FortiManager supports only FortiGuard push to managed devices.
- C. FortiManager will respond to update requests only if they originate from a managed device.
- D. FortiManager does not support rating requests.

Answer: A

NEW QUESTION 7

An administrator wants to capture ESP traffic between two FortiGates using the built-in sniffer. If the administrator knows that there is no NAT device located between both FortiGates, what command should the administrator execute?

- A. diagnose sniffer packet any 'udp port 500'
- B. diagnose sniffer packet any 'udp port 4500'
- C. diagnose sniffer packet any 'esp'
- D. diagnose sniffer packet any 'udp port 500 or udp port 4500'

Answer: C

Explanation:

Capture IKE Traffic without NAT:diagnose sniffer packet 'host and udp port 500'

-----Capture ESP

Traffic without NAT:diagnose sniffer packet any 'host and esp'

-----Capture IKE

and ESP with NAT-T:diagnose sniffer packet any 'host and (udp port 500 or udp port 4500)'

NEW QUESTION 8

An administrator cannot connect to the GUI 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

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: AC

NEW QUESTION 10

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.

Answer: AD

NEW QUESTION 10

View the exhibit, which contains a partial routing table, and then answer the question below.

```
FGT # get router info routing-table all
...
Routing table for VRF=7
C 10.73.9.0/24 is directly connected, port2

Routing table for VRF=12
C 10.1.0.0/24 is directly connected, port3
S 10.10.4.0/24 [10/0] via 10.1.0.100, port3
C 10.64.1.0/24 is directly connected, port1

Routing table for VRF=21
S 10.1.0.0/24 [10/0] via 10.72.3.254, port4
C 10.72.3.0/24 is directly connected, port4
S 192.168.2.0/24 [10/0] via 10.72.3.254, port4
...
```

Assuming all the appropriate firewall policies are configured, which of the following pings will FortiGate route? (Choose two.)

- A. Source IP address 10.1.0.24, Destination IP address 10.72.3.20.
- B. Source IP address 10.72.3.27, Destination IP address 10.1.0.52.
- C. Source IP address 10.72.3.52, Destination IP address 10.1.0.254.
- D. Source IP address 10.73.9.10, Destination IP address 10.72.3.15.

Answer: BC

NEW QUESTION 11

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.

Answer: ABC

Explanation:

https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-advanced-routing-54/Routing_OSPF/OSPF_Bac

NEW QUESTION 14

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 19

Which statement about memory conserve mode is true?

- A. A FortiGate exits conserve mode when the configured memory use threshold reaches yellow.
- B. A FortiGate starts dropping all the new and old sessions when the configured memory use threshold reaches extreme.
- C. A FortiGate starts dropping new sessions when the configured memory use threshold reaches red
- D. A FortiGate enters conserve mode when the configured memory use threshold reaches red

Answer: D

NEW QUESTION 24

Examine the output from the BGP real time debug shown in the exhibit, then the answer the question below:

```
# diagnose ip router bgp all enable
# diagnose ip router bgp level info
# diagnose debug enable
"BGP: 10.200.3.1-Outgoing [DECODE] KAlive: Received!"
"BGP: 10.200.3.1-Outgoing [FSM] State: OpenConfirm Event: 26"
"BGP: 10.200.3.1-Outgoing [DECODE] Msg-Hdr: type 2, length 56"
"BGP: 10.200.3.1-Outgoing [DECODE] Update: Starting UPDATE decoding... Byte
(37), msg_size (37)"
"BGP: 10.200.3.1-Outgoing [DECODE] Update: NLRI Len(13)"
"BGP: 10.200.3.1-Outgoing [FSM] State: Established Event: 27"
"BGP: 10.200.3.1-Outgoing [RIB] Update: Received Prefix 0.0.0.0/0"
"BGP: 10.200.3.1-Outgoing [RIB] Update: Received Prefix 10.200.4.0/24"
"BGP: 10.200.3.1-Outgoing [RIB] Update: Received Prefix 10.200.3.0/24"
"BGP: 10.200.3.1-Outgoing [RIB] Update: Received Prefix 10.0.2.0/24"
"BGP: 10.200.3.1-Outgoing [FSM] State: Established Event: 34"
"BGP: 10.200.3.1-Outgoing [ENCODE] Msg-Hdr: Type 2"
"BGP: 10.200.3.1-Outgoing [ENCODE] Attr IP-Unicast: Tot-attr-len 20"
"BGP: 10.200.3.1-Outgoing [ENCODE] Update: Msg #5 Size 55"
"BGP: 10.200.3.1-Outgoing [FSM] State: Established Event: 34"
```

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

- A. BGP peers have successfully interchanged Open and Keepalive messages.
- B. Local BGP peer received a prefix for a default route.
- C. The state of the remote BGP peer is OpenConfirm.
- D. The state of the remote BGP peer will go to Connect after it confirms the received prefixes.

Answer: AB

NEW QUESTION 29

A FortiGate is rebooting unexpectedly without any apparent reason. What troubleshooting tools could an administrator use to get more information about the problem? (Choose two.)

- A. Firewall monitor.
- B. Policy monitor.
- C. Logs.
- D. Crashlogs.

Answer: CD

NEW QUESTION 34

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.

Answer: B

NEW QUESTION 39

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=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: 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.

Answer: C

NEW QUESTION 44

An administrator has configured a FortiGate device with two VDOMs: root and internal. The administrator has also created an inter-VDOM link that connects both VDOMs. The objective is to have each VDOM advertise some routes to the other VDOM via OSPF through the inter-VDOM link. What OSPF configuration settings must match in both VDOMs to have the OSPF adjacency successfully forming? (Choose three.)

- A. Router ID.
- B. OSPF interface area.
- C. OSPF interface cost.
- D. OSPF interface MTU.
- E. Interface subnet mask.

Answer: BDE

NEW QUESTION 47

Refer to the exhibit, which contains the debug output of diagnose dvm device list.

```
FMG-VM64# diagnose dvm device list
There are currently 1 devices/vdoms managed:
TYPE   OID   SN      HA      IP      NAME      ADOM      IPS  FIRMWARE
fmg/   217   FGVM01... -    10.200.1.1 Local-FortiGate My_ADOM 15.0.0831 6.0 MR4 (1579)
faz enabled
      |- STATUS: db: modified; conf: in sync; cond: pending; dm: retrieved; conn: up
      |- vdom: [3] root flags:0 adom:My_ADOM pkg: [imported] Local-FortiGate_root
```

Which two statements about the output shown in the exhibit are correct? (Choose two.)

- A. ADOMs are disabled on the FortiManager
- B. The FortiGate configuration is in sync with latest running revision history.
- C. There are pending device-level changes yet to be installed on Local-FortiGate.
- D. The policy package has been modified for Local-FortiGate.

Answer: BC

NEW QUESTION 49

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 xxxxxxxx
  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 52

The logs in a FSSO collector agent (CA) are showing the following error: failed to connect to registry: PIKA1026 (192.168.12.232)

What can be the reason for this error?

- A. The CA cannot resolve the name of the workstation.
- B. The FortiGate cannot resolve the name of the workstation.
- C. The remote registry service is not running in the workstation 192.168.12.232.
- D. The CA cannot reach the FortiGate with the IP address 192.168.12.232.

Answer: C

Explanation:

<https://kb.fortinet.com/kb/documentLink.do?externalID=FD30548>

NEW QUESTION 54

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 55

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 58

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 1179648 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
concermode: 0
shm last entered: n/a
system 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

Answer: AC

NEW QUESTION 59

Which of the following statements are correct regarding application layer test commands? (Choose two.)

- A. They are used to filter real-time debugs.
- B. They display real-time application debugs.
- C. Some of them display statistics and configuration information about a feature or process.
- D. Some of them can be used to restart an application.

Answer: CD

Explanation:

Application layer test commands don't display info in real time, but they do show statistics and configuration info about a feature or process. You can also use some of these commands to restart a process or execute a change in its operation.

NEW QUESTION 64

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 68

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 73

Examine the output from the 'diagnose debug authd fssolist' command; then answer the question below.

```
# diagnose debug authd fssolist —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. TRAININ
- C. LAB.
- D. The source IP address of the traffic arriving to the FortiGate from the workstation INTERNAL2.TRAININ
- E. LAB.
- F. The reserve DNS lookup forthe IP address 192.168.3.1.

Answer: C

NEW QUESTION 77

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 82

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

```
# diagnose debug rating
Locale      : English
License     : Contract
Expiration  : Thu Sep 28 17:00:00 20XX
--- Server List (Thu APR 19 10:41:32 20XX) ---
IP          Weight  RTT   Flags  TZ   Packets  Curr Lost  Total Lost
64.26.151.37  10     45    -5     -5   262432  0          846
64.26.151.35  10     46    -5     -5   329072  0          6806
66.117.56.37  10     75    -5     -5   71638   0          275
66.210.95.240 20     71    -8     -8   36875   0          92
209.222.147.36 20     103   DI     -8   34784   0          1070
208.91.112.194 20     107   D      -8   35170   0          1533
96.45.33.65   60     144   0      0    33728   0          120
80.85.69.41   71     226   1      1    33797   0          192
62.209.40.74  150    97    9      9    33754   0          145
121.111.236.179 45     44    F      -5   26410   26226     26227
```

Which statements are true regarding the Weight value?

- A. Its initial value is calculated based on the round trip delay (RTT).
- B. Its initial value is statically set to 10.
- C. Its value is incremented with each packet lost.
- D. It determines which FortiGuard server is used for license validation.

Answer: C

NEW QUESTION 86

Refer to the exhibit, which shows a FortiGate configuration.

```

config system fortiguard
  set protocol udp
  set port 8888
  set load-balance-servers 1
  set auto-join-forticloud enable
  set update-server-location any
  set sandbox-region ""
  set fortiguard-anycast disable
  set antispam-force-off disable
  set antispam-cache enable
  set antispam-cache-ttl 1800
  set antispam-cache-mpercent 2
  set antispam-timeout 7
  set webfilter-force-off enable
  set webfilter-cache enable
  set webfilter-cache-ttl 3600
  set webfilter-timeout 15
  set sdns-server-ip "208.91.112.220"
  set sdns-server-port 53
  unset sdns-options
  set source-ip 0.0.0.0
  set source-ip6 ::
  set proxy-server-ip 0.0.0.0
  set proxy-server-port 0
  set proxy-username ""
  set ddns-server-ip 0.0.0.0
  set ddns-server-port 443
end

```

An administrator is troubleshooting a web filter issue on FortiGate. The administrator has configured a web filter profile and applied it to a policy; however, the web filter is not inspecting any traffic that is passing through the policy. What must the administrator change to fix the issue?

- A. The administrator must increase webfilter-timeout.
- B. The administrator must disable webfilter-force-off.
- C. The administrator must change protocol to TCP.
- D. The administrator must enable fortiguard-anycast.

Answer: D

NEW QUESTION 88

Examine the output of the 'get router info ospf interface' command shown in the exhibit; 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 statements are true regarding the above output? (Choose two.)

- A. The port4 interface is connected to the OSPF backbone area.
- B. The local FortiGate has been elected as the OSPF backup designated router.
- C. There are at least 5 OSPF routers connected to the port4 network.
- D. Two OSPF routers are down in the port4 network.

Answer: AC

Explanation:

on BROADCAST network there are 4 neighbors, among which 1*DR +1*BDR. So our FG has 4 neighbors, but create adjacency only with 2 (with DR and BDR). 2 neighbors DROther (not down).

NEW QUESTION 93

In which two states is a given session categorized as ephemeral? (Choose two.)

- A. A TCP session waiting to complete the three-way handshake.
- B. A TCP session waiting for FIN ACK.

- C. A UDP session with packets sent and received.
- D. A UDP session with only one packet received.

Answer: AD

NEW QUESTION 97

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

# diagnose webfilter fortiguard statistics list	# diagnose webfilter fortiguard statistics list
Raring Statistics:	Cache Statistics:
-----	-----
DNS filures : 273	Maximum memory : 0
DNS lookups : 280	Memory usage : 0
Data send failures : 0	
Data read failures : 0	Nodes : 0
Wrong package type : 0	Leaves : 0
Hash table miss : 0	Prefix nodes : 0
Unknown server : 0	Exact nodes : 0
Incorrect CRC : 0	
Proxy requests failures : 0	Requests : 0
Request timeout : 1	Misses : 0
Total requests : 2409	Hits : 0
Requests to FortiGuard servers : 1182	Prefix hits : 0
Server errored responses : 0	Exact hits : 0
Relayed rating : 0	
Invalid profile : 0	No cache directives : 0
	Add after prefix : 0
Allowed : 1021	Invalid DB put : 0
Blocked : 3909	DB updates : 0
Logged : 3927	
Blocked Errors : 565	Percent full : 0%
Allowed Errors : 0	Branches : 0%
Monitors : 0	Leaves : 0%
Authenticates : 0	Prefix nodes : 0%
Warnings : 18	Exact nodes : 0%
Ovrd request timeout : 0	
Ovrd send failures : 0	Miss rate : 0%
Ovrd read failures : 0	Hit rate : 0%
Ovrd errored responses : 0	Prefix hits : 0%
...	Exact hits : 0%

Which one of the following statements explains why the cache statistics are all zeros?

- A. The administrator has reallocated the cache memory to a separate process.
- B. There are no users making web requests.
- C. The FortiGuard web filter cache is disabled in the FortiGate's configuration.
- D. FortiGate is using a flow-based web filter and the cache applies only to proxy-based inspection.

Answer: C

NEW QUESTION 100

Which two statements about OCVPN are true? (Choose two.)

- A. Only root vdom supports OCVPN.
- B. OCVPN supports static and dynamic IPs in WAN interface.
- C. OCVPN offers only Hub-Spoke VPNs.
- D. FortiGate devices under different FortiCare accounts can be used to form OCVPN.

Answer: AB

NEW QUESTION 105

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 109

Which two statements about an auxiliary session are true? (Choose two.)

- A. With the auxiliary session setting enabled, ECMP traffic is accelerated to the NP6 processor.
- B. With the auxiliary session setting enabled, two sessions will be created in case of routing change.
- C. With the auxiliary session setting disabled, for each traffic path, FortiGate will use the same auxiliary session.
- D. With the auxiliary session disabled, only auxiliary sessions will be offloaded.

Answer: CD

NEW QUESTION 114

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

```
FGT # 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
100.64.3.1    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. The local router's BGP state is Established with the 10.125.0.60 peer.
- B. Since the counters were last reset; the 10.200.3.1 peer has never been down.
- C. The local router has received a total of three BGP prefixes from all peers.
- D. The local router has not established a TCP session with 100.64.3.1.

Answer: AD

NEW QUESTION 118

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
```

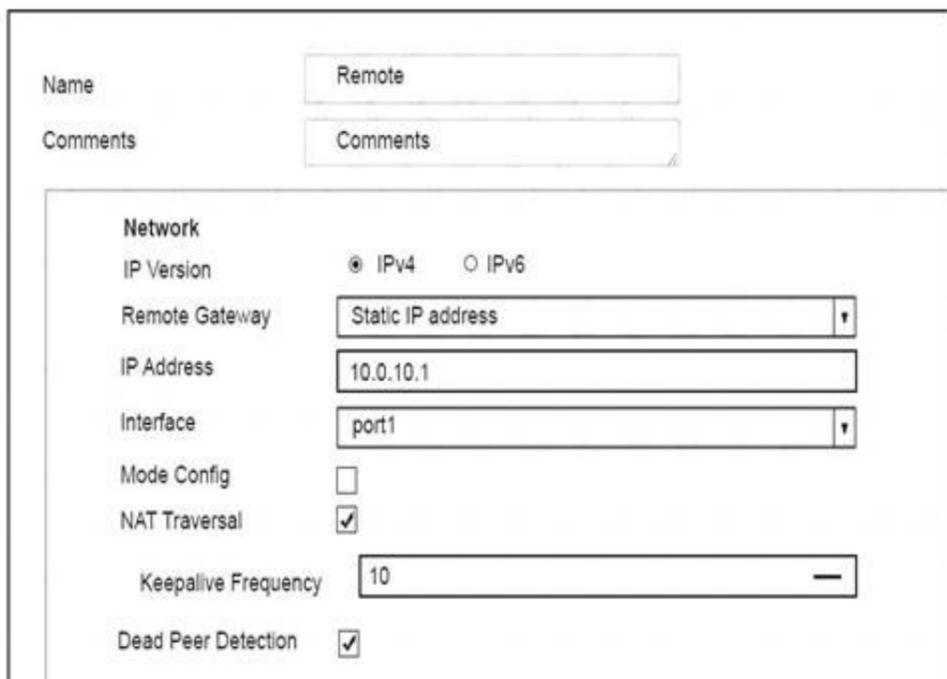
Which outbound interface will FortiGate use to route web traffic from internal users to the Internet?

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

Answer: C

NEW QUESTION 119

View the exhibit, which contains a screenshot of some phase-1 settings, and then answer the question below.



The VPN is up, and DPD packets are being exchanged between both IPsec gateways; however, traffic cannot pass through the tunnel. To diagnose, the administrator enters these CLI commands:

```
diagnose vpn ike log-filter src-add4 10.0.10.1
diagnose debug application ike-1
diagnose debug enable
```

However, the IKE real time debug does not show any output. Why?

- A. The debug output shows phases 1 and 2 negotiations onl
- B. Once the tunnel is up, it does not show any more output.
- C. The log-filter setting was set incorrectl
- D. The VPN's traffic does not match this filter.
- E. The debug shows only error message
- F. If there is no output, then the tunnel is operating normally.
- G. The debug output shows phase 1 negotiation onl
- H. After that, the administrator must enable the following real time debug: diagnose debug application ipsec -1.

Answer: B

NEW QUESTION 123

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

```
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=statistic/1 tun=intf/0 mode=auto/1 encap=none/0
proxyid_num=1 child_num=0 refernt=15 ilast=10 olast=792 auto-discovery=0
stat: rxp=0 txp=0 rxb=0 txb=0
dpd: mode=on-demand on=1 idle=20000ms 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: 0:10.1.2.0/255.255.255.0:0
dat: 0:10.1.1.0/255.255.255.0:0
SA: ref=3 options=2e type=00 soft=0 mtu=1438 expire=42403/0B replaywin=204B seqno=1
esn=replaywin_lastseq=00000000
life: type=01 bytes=0/0 timeout=43177/43200
dec: spi=ccclf66d esp=aes key=16 280e5cd6f9bacc65ac771556c464ffbd
ah=shal key=20 c68091d68753578785de6a7a6b276b506e527
```

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

- A. Anti-replay is enabled.
- B. DPD is disabled.
- C. Remote gateway IP is 10.200.4.1.
- D. Quick mode selectors are disabled.

Answer: AC

NEW QUESTION 128

View the exhibit, which contains the output of a real-time debug. Which statement about this output is true?

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

msg="received a request /tmp/.wad512_0_0.url.socket, addr_len=30:
d=training.fortinet.com:443, id=687, cat=255, vfname='root', vfid=0,
profile='default', type=0, client=10.1.10.1, url_source=1, url="/"
action=9(ftgd-allow) wf-act=5(ALLOW) user="N/A" src=10.1.10.1 sport=58334
dst=13.226.142.41 dport=443 service="https" cat=52 url_cat=52 ip_cat=0
hostname="training.fortinet.com" url="/"
```

Which of the following statements is true regarding this output?

- A. The requested URL belongs to category ID 255.
- B. The server hostname is training, fortinet.com.
- C. FortiGate found the requested URL in its local cache.
- D. This web request was inspected using the ftgd-allow web filler profile.

Answer: C

NEW QUESTION 130

Which two statements about the Security Fabric are true? (Choose two.)

- A. Only the root FortiGate collects network information and forwards it to FortiAnalyzer.
- B. FortiGate uses FortiTelemetry protocol to communicate with FortiAnalyzer.
- C. All FortiGate devices in the Security Fabric must have bidirectional FortiTelemetry connectivity.
- D. Branch FortiGate devices must be configured first.

Answer: BC

NEW QUESTION 135

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual NSE7_EFW-7.0 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the NSE7_EFW-7.0 Product From:

https://www.2passeasy.com/dumps/NSE7_EFW-7.0/

Money Back Guarantee

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 First Try
- * NSE7_EFW-7.0 Practice Test Questions in Multiple Choice Formats and Updates for 1 Year