PassQueen
a.k.a dumpsqueen.com

Fortinet NSE 7 - Enterprise Firewall 6.2

Fortinet NSE7_EFW-6.2

Version Demo

Total Demo Questions: 12

Total Premium Questions: 120

Buy Premium PDF

https://passqueen.com

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, System configuration	11
Topic 2, Firewall policies and authentication	12
Topic 3, Routing	31
Topic 4, VPN	13
Topic 5, Content inspection	16
Topic 6, High availability	9
Topic 7, Security Fabric	1
Topic 8, Diagnostics	27
Total	120

QUESTION NO: 1

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

```
Student# get router info bgp summary
BGP router indentifier 10.200.1.1, local AS number 65500
BGP table version is 2
1 BGP AS-PATH entries
0 BGP community entries

Neighbor   V     AS   MsgRcvd  MsgSent  TblVer  InQ  OutQ  Up/Down  State/PfxRcd
10.200.3.1 4  65501        92      112       0    0     0    never    Connect

Total number of neighbors 1
```

Which statement can explain why the state of the remote BGP peer 10.200.3.1 is Connect?

A. The local peer is receiving the BGP keepalives from the remote peer but it has not received any BGP prefix yet.

B. The TCP session for the BGP connection to 10.200.3.1 is down.

C. The local peer has received the BGP prefixed from the remote peer.

D. The local peer is receiving the BGP keepalives from the remote peer but it has not received the OpenConfirm yet.

ANSWER: B

Explanation:

The TCP session for the BGP connection to 10.200.3.1 is down. In the BGP finite-state machine, the `Connect` state means that BGP has initiated a TCP transport connection to the configured neighbor and is waiting for that TCP connection to complete. BGP cannot exchange its OPEN, KEEPALIVE, or UPDATE messages until the TCP three-way handshake succeeds and the transport session is established. Therefore, a peer shown as `Connect` in `get router info bgp summary` indicates that the BGP process is attempting to establish connectivity to the remote peer but does not yet have an established TCP session.

This status commonly leads an administrator to verify IP reachability to the neighbor address, routing to that address, TCP port 179 accessibility, and whether the remote BGP process is listening and correctly configured. Once TCP establishment succeeds, the BGP state machine can progress to OPEN message exchange and then, after successful negotiation, to the Established state. RFC 4271 defines the Connect state as waiting for completion of the TCP connection, as described in the BGP state-machine specification. FortiGate BGP configuration and operational behavior are documented in the FortiGate 6.2 Administration Guide.

QUESTION NO: 2

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 3190430061, 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: A C

Explanation:

The valid causes are that HTTP administrative access is not enabled on the interface assigned 10.0.1.254, or that FortiGate has been configured to use a nondefault HTTP administration port. Administrative GUI traffic terminating on a FortiGate is handled as local-in traffic, rather than as traffic traversing a firewall policy. Therefore, for an HTTP connection sent to TCP port 80 to be accepted, the receiving interface must permit the HTTP administrative access service and FortiGate must be listening for HTTP administration on that destination port. If HTTP is absent from the interface `allowaccess` configuration, the local-in processing path cannot accept the management connection. Similarly, if the global HTTP administrative port has been changed, a browser connection that omits a port number still attempts TCP/80 and will not reach the management HTTP service; the administrator must use the configured port explicitly in the URL. These settings are configured independently: interface administrative-access permissions determine which management protocols can enter through an interface, while the administrative-port setting determines the TCP port on which the corresponding service listens. Fortinet documents the interface administrative-access controls in its FortiOS Administration Guide and the configurable management-port behavior in the FortiOS CLI Reference.

QUESTION NO: 3

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

Explanation:

The remote gateway's phase 1 configuration does not match the local gateway's phase 1 configuration. The IKE real-time debug indicates that negotiation fails during the initial IKE security-association establishment, before the peers can successfully create the IPsec phase 2 security associations. Phase 1 must produce a mutually acceptable IKE proposal and matching peer parameters so that both devices can establish the encrypted management channel used for subsequent IPsec negotiation. Relevant settings include the IKE version, exchange mode for IKEv1, encryption and authentication algorithms, Diffie-Hellman group, lifetime, and—in configurations that use them—the peer ID and authentication settings. When no common phase 1 proposal or compatible phase 1 peer configuration is available, the FortiGate cannot advance the negotiation to phase 2 and the tunnel remains down. Fortinet recommends using IKE debugging to identify the negotiation stage and then comparing the phase 1 settings on both peers, including the proposals and Diffie-Hellman group. See Fortinet's IPsec troubleshooting documentation and the FortiGate IPsec VPN administration guide for phase 1 configuration and diagnostic guidance.

QUESTION NO: 4

Which setting controls how FortiGate distributes sessions across equal-cost IPv4 routes?

A. v4-ecmp-mode

B. route-cache

C. asymroute

D. strict-src-check

ANSWER: A

Explanation:

The `v4-ecmp-mode` setting controls the method FortiGate uses to distribute IPv4 sessions across equal-cost multipath routes. Equal-cost routes must have the same destination prefix, administrative distance, and priority before FortiGate can use them as ECMP paths. The configured ECMP mode then determines which packet or session fields are used to select one of the available next hops.

ECMP provides path utilization and redundancy when multiple equivalent routes are available. It differs from route priority, which is used to prefer one otherwise equivalent route over another. Refer to the FortiOS 6.2 system settings CLI reference and the FortiOS 6.2 Administration Guide.

QUESTION NO: 5

What is the behavior of an IPsec phase 1 interface configured with dead peer detection (DPD) set to on-idle?

A. FortiGate sends DPD probes only when no tunnel traffic has been detected for the configured idle period.

B. FortiGate sends DPD probes for every packet that crosses the tunnel.

C. FortiGate sends DPD probes only after Phase 2 expires.

D. FortiGate disables IKE keepalive processing permanently.

ANSWER: A

Explanation:

With DPD configured as `on-idle`, FortiGate sends DPD probe messages only when the IPsec tunnel has been idle for the configured period. The probes determine whether the remote peer remains reachable when normal protected traffic is not providing evidence that the tunnel is still operational.

If the remote peer does not respond to the required DPD probes, FortiGate can remove the stale IKE security association and allow a new negotiation to occur when traffic needs the tunnel. This avoids continuously sending DPD probes while regular tunnel traffic is already present. See the FortiOS 6.2 IPsec phase1-interface CLI reference.

QUESTION NO: 6

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: A D

Explanation:

Reducing the session time to live can reduce FortiGate memory utilization because each active session requires an entry in the session table and associated state information. A shorter time to live removes inactive or abandoned sessions sooner, reducing the number of concurrent session records retained in memory. This must be tuned with awareness of application behavior so that legitimate idle connections are not prematurely aged out.

Reducing the maximum file size to inspect also lowers memory consumption. Security inspection processes, particularly content and file-based inspection, can require FortiGate to hold file data and related inspection state while a transfer is being analyzed. Limiting the maximum inspectable file size places an upper bound on the resources used for individual inspected transfers, which is especially useful when the device handles many simultaneous downloads or uploads. Fortinet documents session behavior, policy settings, and inspection-related configuration in its FortiOS 6.2 Administration Guide and FortiOS 6.2 CLI Reference.

QUESTION NO: 7

View the exhibit, which contains the output of a diagnose command, and then 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  262432   0          846
64.26.151.35    10      46          -5  329072   0          6806
66.117.56.37    10      75          -5  71638    0          275
65.210.95.240   20      71          -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   33728    0          120
80.85.69.41     71      226         1   33797    0          192
62.209.40.74    150     97          9   33754    0          145
121.111.236.179 45      44     F    -5  26410    26226      26227
```

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

A. FortiGate will probe 121.111.236.179 every fifteen minutes for a response.

B. Servers with the D flag are considered to be down.

C. Servers with a negative TZ value are experiencing a service outage.

D. FortiGate used 209.222.147.3 as the initial server to validate its contract.

ANSWER: A D

Explanation:

The diagnostic output identifies the FortiGuard Distribution Network servers that FortiGate can use for contract validation and indicates their current reachability state. **FortiGate will probe 121.111.236.179 every fifteen minutes for a response.** is correct because the server is marked as failed. FortiGate retains failed FortiGuard servers in its server list and periodically tests them; the retry interval shown for this failed server is 15 minutes. This allows the appliance to detect when a previously unreachable server becomes available again without requiring manual intervention.

FortiGate used 209.222.147.3 as the initial server to validate its contract. is also correct. The diagnostic fields identify the initial FortiGuard server selected for validation, and the displayed initial-server address is 209.222.147.3. Contract validation is required for FortiGate to confirm entitlement to FortiGuard services and receive the appropriate update and rating services. The server-selection and health information in this diagnostic output is useful when troubleshooting connectivity to FortiGuard infrastructure. Fortinet documents FortiGuard Distribution Network behavior and connectivity troubleshooting in the FortiGuard Distribution Network documentation and the FortiOS 6.2 Administration Guide.

QUESTION NO: 8

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

Explanation:

The `diagnose test application ipsmonitor 99` command is used to restart all IPS engines and IPS monitor processes on the FortiGate. The IPS monitor is responsible for supervising the IPS engine processes that inspect traffic against configured intrusion-prevention signatures. Restarting these components is an operational troubleshooting action that can be useful when IPS inspection processes are unresponsive, have encountered an internal error, or need to be reinitialized after diagnostic work. When the command runs, FortiGate stops and starts the relevant IPS engines and monitors rather than merely displaying their session information. Because IPS processes are restarted, administrators should use it deliberately during troubleshooting and account for the possibility of a brief interruption or reinitialization of deep inspection activity while the services return to a healthy state. This command is part of the diagnostic CLI tooling available to diagnose FortiGate security-processing behavior; it is not a permanent configuration command. Fortinet's FortiOS CLI reference documents the diagnostic command framework, and the IPS documentation describes how the IPS engine performs signature-based traffic inspection. See the FortiOS 6.2 CLI Reference and the FortiOS 6.2 Intrusion Prevention documentation.

QUESTION NO: 9

Which two configuration settings change the behavior for content-inspected traffic while FortiGate is in conserve mode? (Choose two.)

A. IPS failopen

B. mem failopen

C. AV failopen

D. UTM failopen

ANSWER: A C

Explanation:

FortiGate enters conserve mode when available memory reaches the configured threshold. In this state, resource-intensive content inspection can be affected so that the firewall can preserve memory and continue handling essential traffic. **IPS failopen** controls the IPS engine's behavior when it cannot inspect traffic because of conserve-mode resource constraints. Enabling its fail-open behavior permits traffic to continue rather than requiring IPS inspection to complete. **AV failopen** provides the corresponding behavior for antivirus inspection: it determines whether traffic can be passed when the antivirus engine cannot process the content under low-memory conditions. These settings are independently configurable because IPS and antivirus are separate inspection functions, and an administrator may need different availability-versus-inspection behavior for each one. They are global FortiOS controls intended specifically to define the treatment of traffic when inspection resources are unavailable. Fortinet documents the available global antivirus fail-open setting and related system-wide controls in the FortiOS 6.2 CLI Reference: config system global. Additional operational context for managing FortiGate resources and inspection features is available in the FortiOS 6.2 Administration Guide.

QUESTION NO: 10

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:

The correct meaning is: “The next packet must be re-evaluated against the firewall policies.” FortiGate normally processes the first packet of a flow against the policy and creates a session entry. Later packets can use that established session entry, which avoids performing a complete policy lookup for every packet. A session marked with the `dirty` flag has been identified as needing revalidation, typically because a relevant configuration change affects its forwarding or policy treatment. On receipt of the next packet for that flow, FortiGate reevaluates the session against the current policy configuration and updates its handling as required. This mechanism allows policy-related changes to take effect for existing traffic without treating the dirty marker itself as an antivirus verdict, application-control result, or an HA-session-removal instruction. The flag is therefore a session-state indicator that tells FortiGate the cached decision cannot simply continue unchanged and must be checked again using the active firewall rules. Fortinet’s session troubleshooting material describes session flags and their operational meaning; see Fortinet KB FD40119 and the FortiOS 6.2 session management documentation.

QUESTION NO: 11

Which statements are true regarding FortiGate policy routes? (Choose two.)

A. They are evaluated before the normal routing table.

B. They can specify an output interface and a gateway.

C. They replace the need for a matching firewall policy.

D. They are evaluated only after the longest-prefix route is selected.

ANSWER: A B

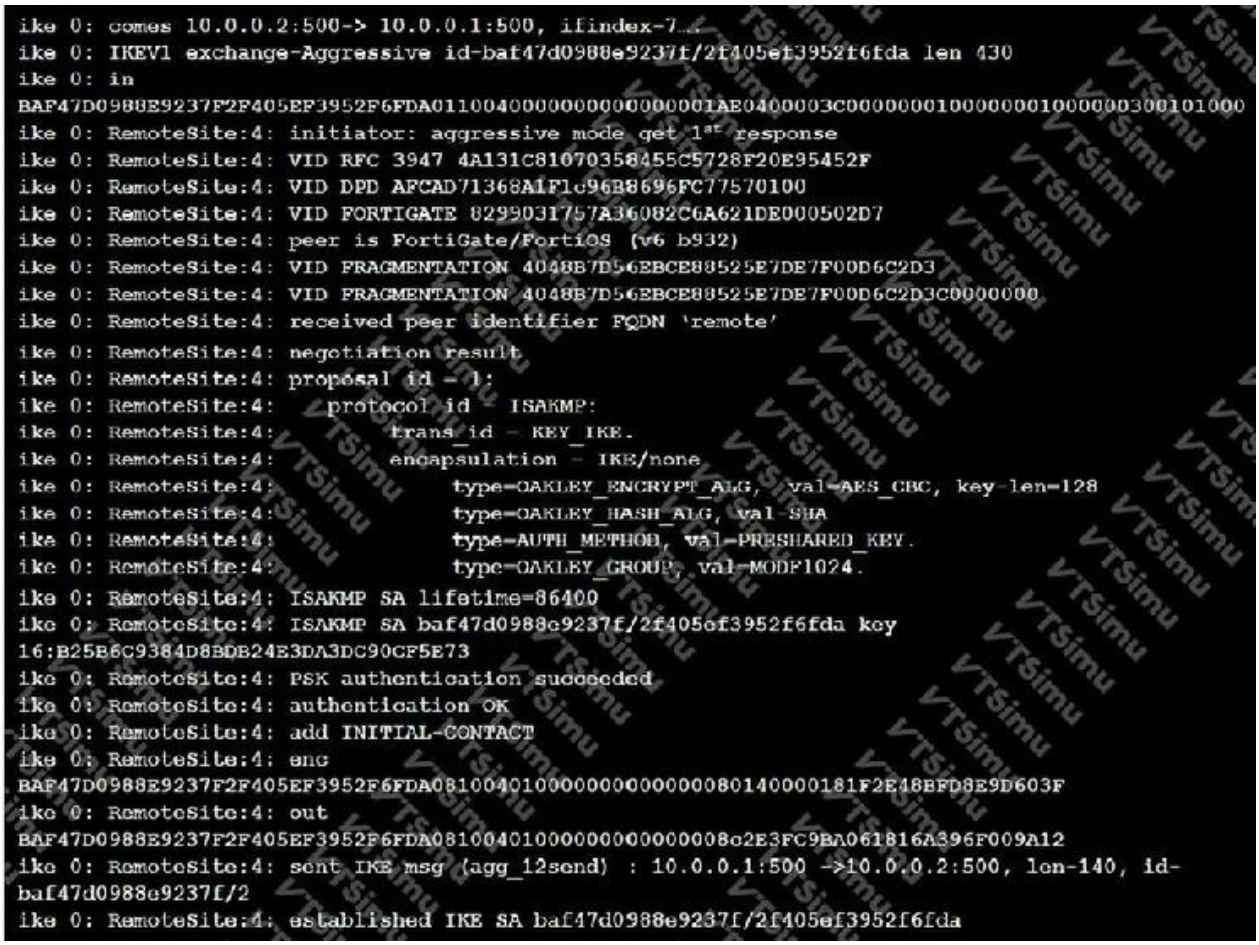
Explanation:

Policy routes are evaluated before the normal routing table. When a packet matches the configured incoming interface, source, destination, protocol, or other policy-route criteria, FortiGate applies the matching policy route before performing the conventional destination-based route lookup. This allows administrators to steer selected traffic through a specific WAN connection or next hop.

A policy route can specify an output interface and a gateway. The output interface identifies the path that FortiGate must use, while the gateway identifies the next-hop address for the selected traffic. A policy route does not replace the firewall policy requirement; traffic must still be permitted by a matching firewall policy. See the FortiOS 6.2 Administration Guide for policy-routing configuration details.

QUESTION NO: 12

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



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.

ANSWER: B D

Explanation:

The correct statements are **It shows a phase 1 negotiation.** and **The initiator has provided remote as its IPsec peer ID.** The debug is recording IKE security-association establishment, which is the VPN phase in which the two peers negotiate IKE parameters, authenticate one another, and establish the protected IKE SA before IPsec phase 2 child SAs are created. FortiGate IKE real-time debugging reports this exchange using IKE/phase-1 processing messages and also displays identification payload information. The identity value `remote` is supplied by the initiating peer as its IKE/IPsec peer ID, rather than being an address inferred from packet delivery details. Peer IDs are used during IKE authentication and can be configured as strings, FQDNs, user FQDNs, or IP-address identities depending on the VPN configuration. This interpretation follows the IKEv2 definition of the IKE SA and Identification payloads in RFC 7296. Fortinet's FortiGate documentation also describes using IKE debug output to inspect VPN negotiation and identity/authentication processing: FortiOS 6.2 Administration Guide.