Which statement about the HA override setting in FortiGate HA clusters is true?

Select one:

- It enables monitored ports.
- You must configure override settings manually and separately for each cluster member.
- It synchronizes device priority on all cluster members.
- It reboots FortiGate.

Examine this FortiGate configuration:

```
config system global
  set av-failopen pass
end
config ips global
  set fail-open disable
end
```

Examine the output of the following debug command:

```
# diagnose hardware sysinfo conserve
memory conserve mode: on
total RAM: 3040 MB
memory used: 2706 MB 89% of total RAM
memory freeable: 334 MB 11% of total RAM
memory used + freeable threshold extreme: 2887 MB 95% of total RAM
memory used threshold red: 2675 MB 88% of total RAM
memory used threshold green: 2492 MB 82% of total RAM
```

Based on the diagnostic outputs above, how is FortiGate handling new packets that require IPS inspection?

Select one:

- They are dropped.
- They are allowed and inspected as long as no additional proxy-based inspection is required.
- They are allowed and inspected.
- They are allowed, but with no inspection.

Which two statements about antivirus scanning in a firewall policy set to proxy-based inspection mode are true? (Choose two.)

Select one or more:

- The client must wait for the antivirus scan to finish scanning before it receives the file.
- If a virus is detected, a block replacement message is displayed immediately.
- FortiGate sends a reset packet to the client if antivirus reports the file as infected.
- A file does not need to be buffered completely before it is moved to the antivirus engine for scanning.

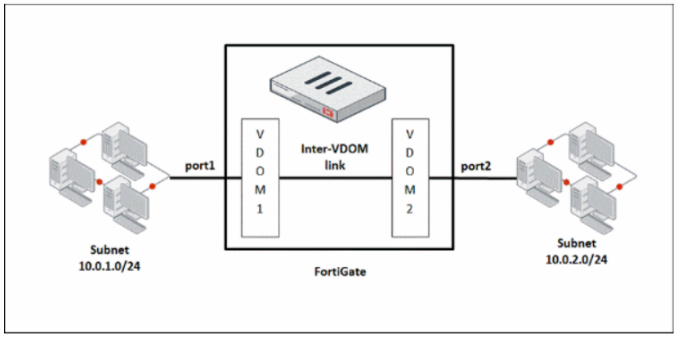
Which statement about firewall policy NAT is true?

Select one:

- DNAT can automatically apply to multiple firewall policies, based on DNAT rules.
- SNAT can automatically apply to multiple firewall policies, based on SNAT policies.
- DNAT is not supported.
- You must configure SNAT for each firewall policy.

Examine the exhibit, which shows a FortiGate with two VDOMs: VDOM1 and VDOM2.

Both VDOMs are operating in NAT/route mode. The subnet `10.0.1.0/24` is connected to VDOM1. The subnet `10.0.2.0/24` is connected to VDOM2. There is an inter-VDOM link between VDOM1 and VDOM2. Also, necessary firewall policies are configured in VDOM1 and VDOM2.



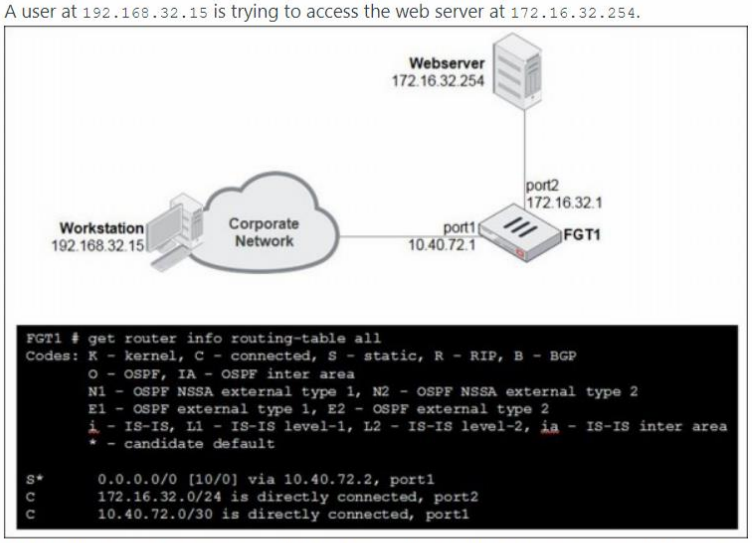
Which two static routes are required in the FortiGate configuration to route traffic between both subnets through an inter-VDOM link? (Choose two.)

Select one or more:

- A static route in VDOM1 for the destination subnet of `10.0.2.0/24`
- A static route in VDOM2 with the destination subnet matching the subnet assigned to the inter-VDOM link
- A static route in VDOM2 for the destination subnet `10.0.1.0/24`
- A static route in VDOM1 with the destination subnet matching the subnet assigned to the inter-VDOM link

View the exhibit.

A user at 192.168.32.15 is trying to access the web server at 172.16.32.254.




```
FGT1 # get router info routing-table all
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

S*      0.0.0.0/0 [10/0] via 10.40.72.2, port1
C       172.16.32.0/24 is directly connected, port2
C       10.40.72.0/30 is directly connected, port1
```

Which two statements best describe how the FortiGate will perform reverse path forwarding (RPF) checks on this traffic? (Choose two.)

Select one or more:

- ☐ Strict RPF check will deny the traffic.
- ☐ Loose RPF check will allow the traffic.
- ☐ Strict RPF check will allow the traffic.
- ☐ Loose RPF check will deny the traffic.

Which three methods can be used to deliver the token code to a user who is configured to use two-factor authentication? (Choose three.)

Select one or more:

- ☐ Voicemail message
- ☐ Instant message app
- ☐ SMS text message
- ☐ FortiToken
- ☐ Email

View the exhibit.

```
date=2021-03-16 time=14:45:16 logid=0317013312 type=utm subtype=webfilter eventtype=ftgd_allow level=notice vd="root" policyid=2
identidx=1 sessionid=31232959 user="anonymous" group="ldap_users" srcip=192.168.1.24 srcport=63355 srcintf="port2"
dstip=66.171.121.44 dstport=80 dstintf="port1" service="http" hostname="www.fortinet.com" profiletype="Webfilter_Profile"
profile="default" status="passthrough" reqtype="direct" url="/" sentbyte=304 rcvdbyte=60135 msg="URL belongs to an allowed
category in policy" method=domain class=0 cat=140 catdesc="custom1"
```

What does this raw log indicate? (Choose two.)

Select one or more:

- ☐ FortiGate allowed the traffic to pass
- ☐ The traffic matches the webfilter profile on firewall policy ID 2.
- ☐ The traffic originated from 66.171.121.44.
- ☐ 192.168.1.24 is the IP address for www.fortinet.com.

FortiGate has been configured for firewall authentication. When attempting to access an external website, the user is not presented with a login prompt.

What is the most likely reason for this situation?

Select one:

- The user is using a super admin account.
- The user was authenticated using passive authentication.
- The user is using a guest account profile.
- No matching user account exists for this user.

Which two statements about incoming and outgoing interfaces in firewall policies are true? (Choose two.)

Select one or more:

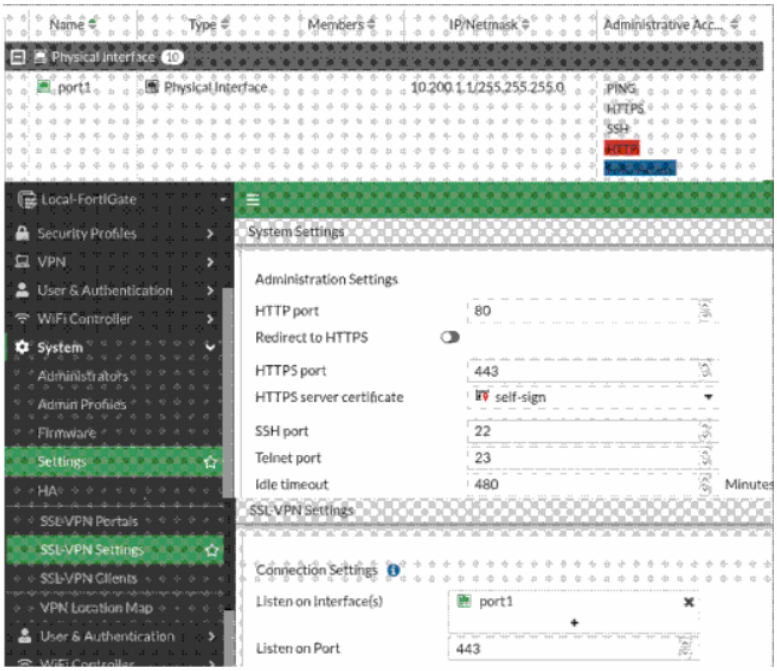
- [ ] Multiple interfaces can be selected as incoming and outgoing interfaces.
- [ ] An incoming interface is mandatory in a firewall policy, but an outgoing interface is optional.
- [ ] Only the **any** interface can be chosen as an incoming interface.
- [ ] A zone can be chosen as the outgoing interface.

What is eXtended Authentication (XAuth)?

Select one:

- It is an IPsec extension that authenticates remote VPN peers using a preshared key.
- It is an IPsec extension that forces remote VPN users to authenticate using their credentials (username and password).
- It is an IPsec extension that forces remote VPN users to authenticate using their local ID.
- It is an IPsec extension that authenticates remote VPN peers using digital certificates.

View the exhibit.



Which statement about the configuration settings is true?

Select one:

- When a remote user accesses `https://10.200.1.1:443`, the SSL-VPN login page opens.
- The settings are invalid. The administrator settings and the SSL-VPN settings cannot use the same port.
- When a remote user accesses `http://10.200.1.1:443`, the SSL-VPN login page opens.
- When a remote user accesses `https://10.200.1.1:443`, the FortiGate login page opens.

Which two configuration settings are global settings? (Choose two.)

Select one or more:

- [ ] User & Device settings
- [ ] Firewall policies
- [ ] FortiGuard settings
- [ ] HA settings

Which statement best describes the role of a DC agent in an FSSO DC agent mode solution?

Select one:

- It captures the login and logoff events and forwards them to the collector agent.
- It captures the login events and forwards them to the collector agent.
- It captures the user IP address and workstation name and forwards them to FortiGate.
- It captures the login events and forwards them to FortiGate.

Which three actions are valid for static URL filtering? (Choose three.)

Select one or more:

- [ ] Exempt
- [ ] Shape
- [ ] Allow
- [ ] Block
- [ ] Warning

Which load balancing method is *not* supported in equal cost multipath (ECMP) load balancing, but *is* supported in SD-WAN?

Select one:

- Source IP based
- Volume based
- Source-destination IP based
- Weight based

Examine the following log message attributes:

```
subtype="webfilter" hostname=www.youtube.com profile="default" action="passthrough" msg="URL belongs to a category with warnings enabled"
```

Which two statements about the log are correct? (Choose two.)

Select one or more:

- [ ] The user was prompted to decide whether to proceed or go back.
- [ ] The category action was set to warning.
- [ ] The website was allowed on the first attempt.
- [ ] The user failed authentication.

An administrator has configured central DNAT and virtual IPs.

Which item can be selected in the firewall policy **Destination** field?

Select one:

- An IP pool
- A VIP object
- The mapped IP address object of the VIP object
- A VIP group

An administrator wants to monitor their network for any probing attempts aimed to exploit existing vulnerabilities in their servers.

Which two items must they configure on their FortiGate to accomplish this? (Choose two.)

Select one or more:

- [ ] An application control profile and set all application signatures to monitor
- [ ] A DoS policy, and log all UDP and TCP scan attempts
- [ ] An IPS sensor to monitor all signatures applicable to the server
- [ ] A web application firewall profile to check protocol constraints

Examine this partial output from the `diagnose sys session list` CLI command:

```
diagnose sys session list
session info: proto=6 proto_state=05 duration=2 expire=78 timeout=3600 flags=00000000 sockflag=00000000 sockport=0 av_idx=0 use=3
```

What does this output state?

Select one:

- `proto_state=05` means there is only one-way traffic.
- `proto_state=05` is the UDP state.
- `proto_state=05` is the ICMP state.
- `proto_state=05` is the TCP state.

Which two statements about the application control profile mode are true? (Choose two.)

Select one or more:

- [ ] It cannot be used in conjunction with IPS scanning.
- [ ] It can scan only unsecure protocols.
- [ ] It can be selected in either flow-based or proxy-based firewall policy.
- [ ] It uses flow-based scanning techniques, regardless of the inspection mode used.

View the exhibit.

Which two behaviors result from this full (deep) SSL configuration? (Choose two.)

Select one or more:

- ☐ A temporary untrusted FortiGate certificate replaces the server certificate when the server certificate is untrusted.
- ☐ The browser bypasses all certificate warnings and allows the connection.
- ☐ A temporary trusted FortiGate certificate replaces the server certificate when the server certificate is trusted.
- ☐ A temporary trusted FortiGate certificate replaces the server certificate, even when the server certificate is untrusted.

Which three settings and protocols can be used to provide secure and restrictive administrative access to FortiGate? (Choose three.)

Select one or more:

- ☐ HTTPS
- ☐ Trusted authentication
- ☐ SSH
- ☐ FortiTelemetry
- ☐ Trusted host

What does the command `diagnose debug fsso-polling refresh-user` do?

Select one:

- ○ It displays status information and some statistics related to the polls done by FortiGate on each DC.
- ○ It enables agentless polling mode real-time debug.
- ○ It refreshes user group information from any servers connected to FortiGate using a collector agent.
- ○ It refreshes all users learned through agentless polling.

Examine the exhibit showing a routing table.

```
FGT1 # get router info routing-table all
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

S*       0.0.0.0/0 [10/0] via 172.20.121.2, port1
C        172.20.121.0/24 is directly connected, port1
C        172.20.168.0/24 is directly connected, port2
C        172.20.167.0/24 is directly connected, port3
S        10.20.30.0/26 [10/0] via 172.20.168.254, port2
S        10.20.30.0/24 [10/0] via 172.20.167.254, port3
S        10.30.20.0/24 [10/0] via 172.20.121.2, port1
```

Which route will be selected when trying to reach `10.20.30.254`?

Select one:

- `10.20.30.0/26 [10/0] via 172.20.168.254, port2`
- `10.30.20.0/24 [10/0] via 172.20.121.2, port1`
- `0.0.0.0/0 [10/0] via 172.20.121.2, port1`
- `10.20.30.0/24 [10/0] via 172.20.167.254, port3`

Which statement about traffic flow in an active-active HA cluster is true?

Select one:

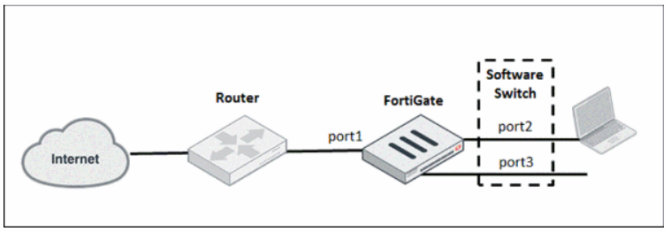
- All FortiGate devices are assigned the same virtual MAC addresses for the HA heartbeat interfaces to redistribute to the sessions.
- The ACK from the client is received on the physical MAC address of the primary device.
- The secondary device responds to the primary device with a SYN/ACK, and then the primary device forwards the SYN/ACK to the client.
- The SYN packet from the client always arrives at the primary device first.

Which two statements about FortiGate antivirus databases are true? (Choose two.)

Select one or more:

- [ ] The extended database is available on all FortiGate models.
- [ ] The extended database is available only if AI scanning is enabled.
- [ ] The extreme database is available only on certain FortiGate models.
- [ ] The quick scan database is part of the normal database.

Examine the exhibit:



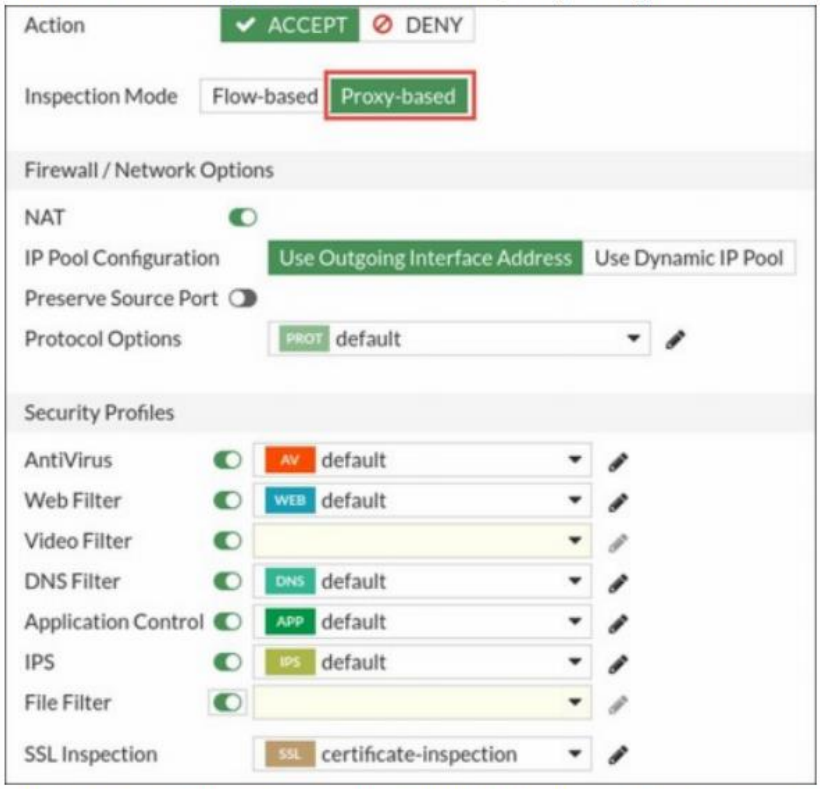
A client workstation is connected to FortiGate port2. FortiGate port1 is connected to an ISP router. port2 and port3 are both configured as a software switch.

Which IP address must be configured on the workstation as the default gateway?

Select one:

- The router IP address
- The FortiGate management IP address
- The port2 IP address
- The software switch interface IP address

Examine the exhibit, which shows a firewall policy configured with multiple security profiles.



Which two security profiles are handled by the IPS engine? (Choose two.)

Select one or more:

- [ ] Application Control
- [ ] AntiVirus
- [ ] Web Filter
- [ ] IPS

What two settings *must* you configure when FortiGate is being deployed as a root FortiGate in a Security Fabric topology? (Choose two.)

Select one or more:

- [ ] FortiManager IP address
- [ ] Fabric name
- [ ] FortiAnalyzer IP address
- [ ] Pre-authorize downstream FortiGate devices

An administrator needs to create a tunnel mode SSL-VPN to access an internal web server from the internet. The web server is connected to port1. The internet is connected to port2. Both interfaces belong to the VDOM named `Corporation`.

What interface must be used as the source for the firewall policy that will allow this traffic?

Select one:

- ○ `port1`
- ○ `ssl.Corporation`
- ○ `port2`
- ○ `ssl.root`

Which two statements about the SD-WAN feature on FortiGate are true? (Choose two.)

Select one or more:

- [ ] SD-WAN provides route failover protection, but cannot load balance traffic.
- [ ] Each member interface requires its own firewall policy to allow traffic.
- [ ] An SD-WAN static route does not require a next-hop gateway IP address.
- [ ] FortiGate supports only one SD-WAN interface per VDOM.

An administrator configured antivirus profile in a firewall policy set to flow-based inspection mode. While testing the configuration, the administrator noticed that `eicar.com` test files can be downloaded using HTTPS protocol only.

What is causing this issue?

Select one:

- ○ Hardware acceleration is in use.
- ○ HTTPS protocol is not enabled under **Inspected Protocols**.
- ○ The test file is larger than the oversize limit.
- ○ Full content inspection for HTTPS is disabled.

Which two statements correctly describe the differences between IPsec main mode and IPsec aggressive mode? (Choose two.)

Select one or more:

- [ ] Six packets are usually exchanged during main mode, while only three packets are exchanged during aggressive mode.
- [ ] The first packet of aggressive mode contains the peer ID, while the first packet of main mode does not.
- [ ] Main mode cannot be used for dialup VPNs, while aggressive mode can.
- [ ] Aggressive mode supports XAuth, while main mode does not.