NSE4_FGT-6.0.Premium.VCE.130q

Number: NSE4_FGT-6.0
Passing Score: 925
Time Limit: 120 min
File Version: 19.042

Copyright

The product of each order has its own encryption code, so you should use it independently.
If anyone who share the file we will disable the free update and account access.
Any unauthorized changes will be inflicted legal punishment. We reserve the right of final explanation for this statement.

Order ID: **********
PayPal Name: **********
PayPal ID: **********

Exam A

QUESTION 1
Examine this output from a debug flow:

```
id=2 line=4677 msg= "vd-root received a packet (photo =6, 66.171.121.44:80-
>10.200.1.1:49886) from port1. flag [S.], seg 3567496940, ack 2176715502, win
5840"
id=2 line= 4739 msg= "Find an existing session, id-00007fc0, reply direction"
id=2 line= 2733 msg "DNAT 10.200.1.1:49886->10.0.1.10:49886"
id=2 line=2582 msg= "find a route: flag= 00000000 gw-10.0.1.10 via port3"
```

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

A. FortiGate received a TCP SYN/ACK packet.
B. The source IP address of the packet was translated to 10.0.1.10.
C. FortiGate routed the packet through port 3.
D. The packet was allowed by the firewall policy with the ID 00007fc0.

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 2
Examine this FortiGate configuration:

```
config authentication setting
     set active-auth-scheme SCHEME1
end
config authentication rule
     edit WebProxyRule
       set srcaddr 10.0.1.0/24
       set active-auth-method SCHEME2
     next
end
```

How does the FortiGate handle web proxy traffic coming from the IP address 10.2.1.200 that requires authorization?

A. It always authorizes the traffic without requiring authentication.
B. It drops the traffic.
C. It authenticates the traffic using the authentication scheme SCHEME2.
D. It authenticates the traffic using the authentication scheme SCHEME1.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 3
Which of the following are purposes of NAT traversal in IPsec? (Choose two.)

A. To delete intermediary NAT devices in the tunnel path.
B. To dynamically change phase 1 negotiation mode aggressive mode.
C. To encapsulation ESP packets in UDP packets using port 4500.
D. To force a new DH exchange with each phase 2 rekey.

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 4
Which of the following statements correctly describes FortiGates route lookup behavior when searching for a suitable gateway? (Choose two)

A. Lookup is done on the trust packet from the session originator
B. Lookup is done on the last packet sent from the re spender
C. Lookup is done on every packet, regardless of direction
D. Lookup is done on the trust reply packet from the re spender

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 5
Examine the two static routes shown in the exhibit, then answer title following question.



Which of the following is the expected FortiGate behavior regarding these two routes to the same destination?

A. FortiGate will load balance all traffic across both routes.
B. FortiGate will use the port1 route as the primary candidate.
C. FortiGate will route twice as much traffic to the port2 route
D. FortiGate will only actuate the portl route m tlie routing table

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

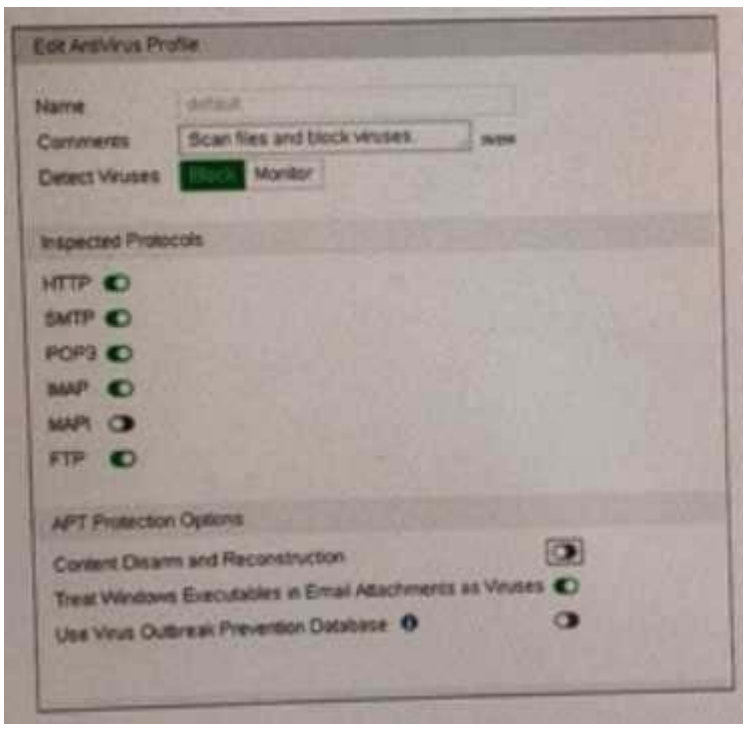
QUESTION 6
Which of the following statements about central NAT are true? (Choose two.)

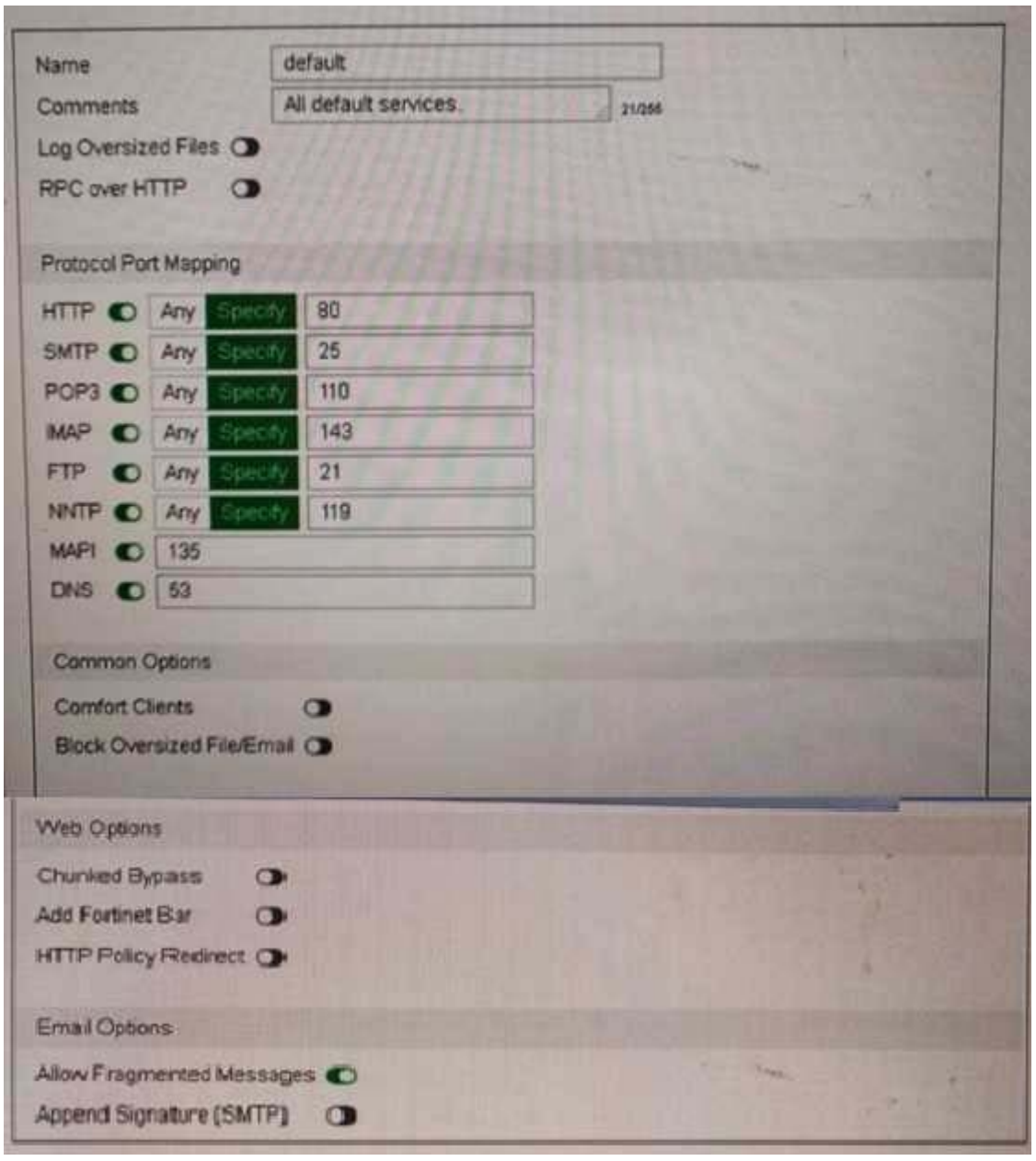
A. IP tool references must be removed from existing firewall policies before enabling central NAT.
B. Central NAT can be enabled or disabled from the CLI only.
C. Source NAT, using central NAT, requires at least one central SNAT policy.
D. Destination NAT, using central NAT, requires a VIP object as the destination address in a firewall policy.

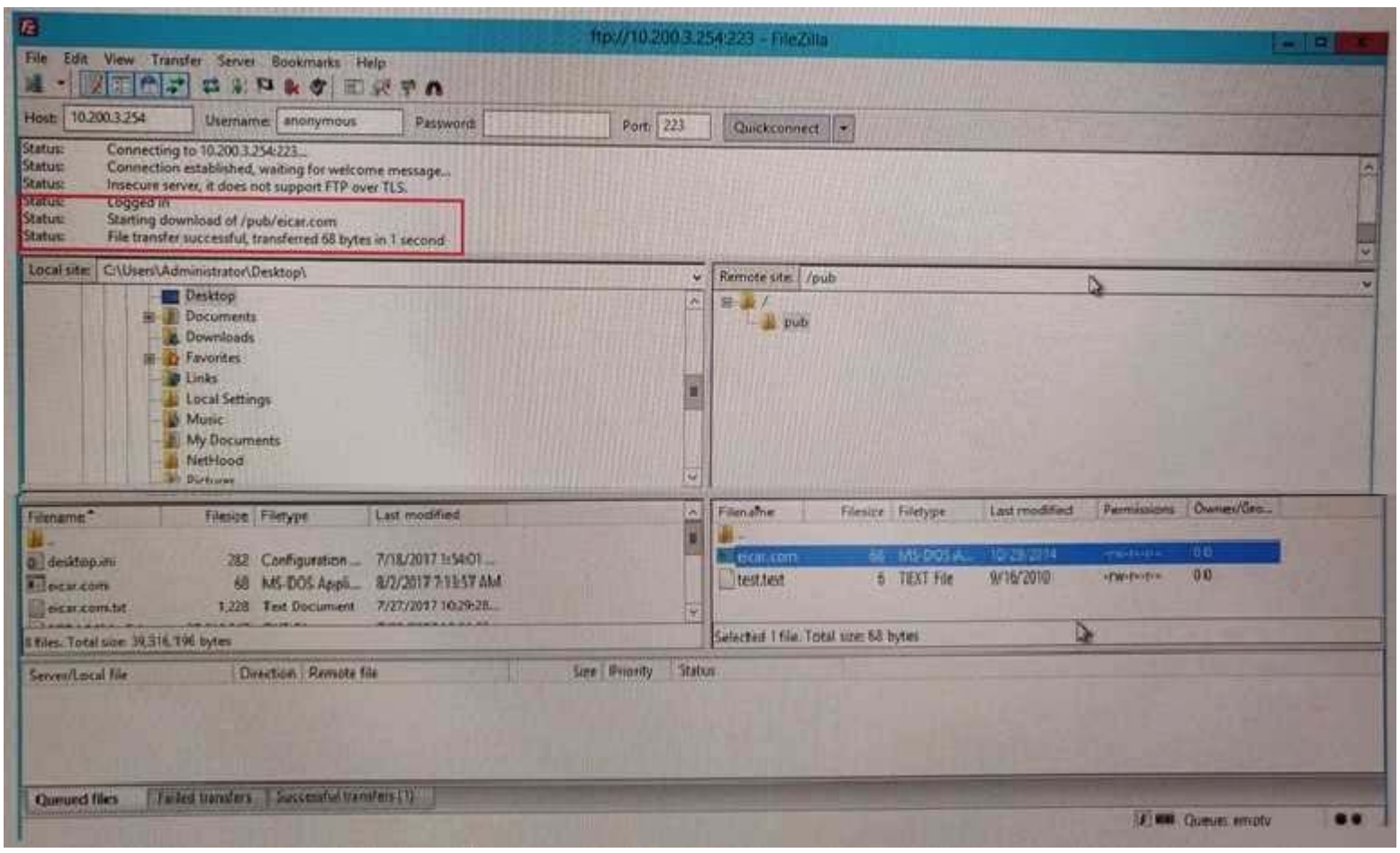
Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 7
Refer to the following exhibit.







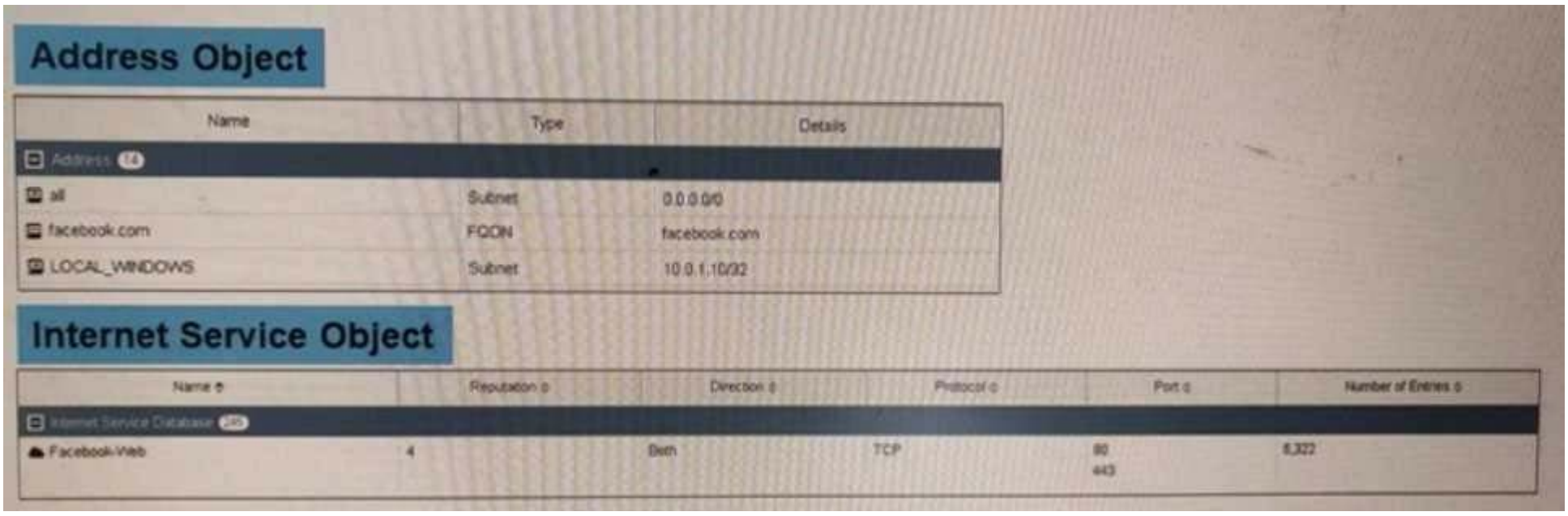
Why is FortiGate not blocking the test file over FTP download?

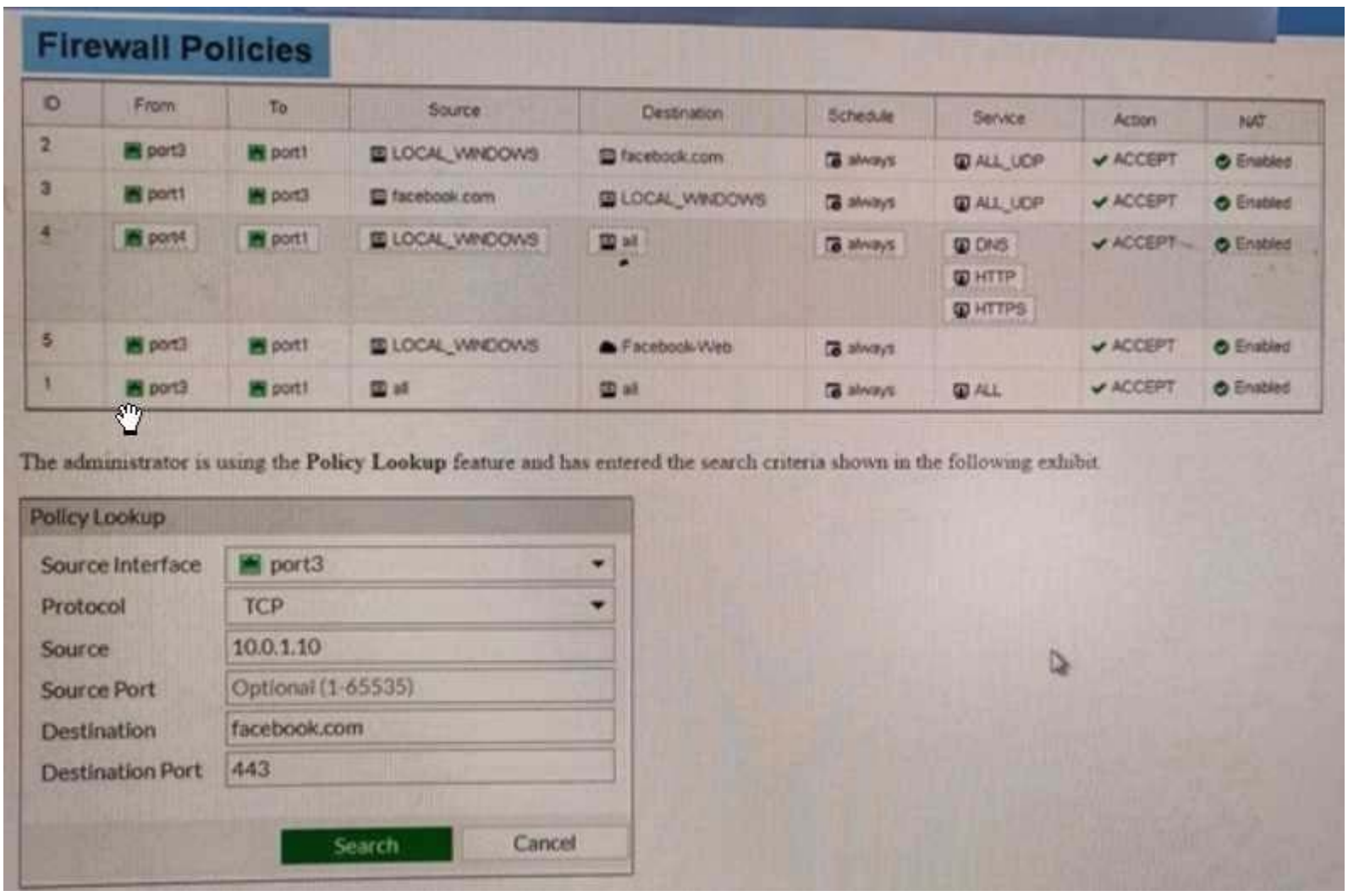
A. Deep-inspection must be enabled for FortiGate to fully scan FTP traffic.
B. FortiGate needs to be operating in flow-based inspection mode in order to scan FTP traffic.
C. The FortiSandbox signature database is required to successfully scan FTP traffic.
D. The proxy options profile needs to scan FTP traffic on a non-standard port.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 8
View the following exhibit, which shows the firewall policies and the object uses in the firewall policies.





The administrator is using the Policy Lookup feature and has entered the search create shown in the following exhibit.



Which of the following will be highlighted based oil the input criteria?

A. Policy with ID 1.
B. Policies with ID 2 and 3.
C. Policy with ID 5.
D. Policy with ID 4

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 9
An administrator wants to create a policy-based IPsec VPN tunnel between two FortiGate devices Winch configuration steps must be performed on both devices to support this scenario? (Choose three.)

A. Define the phase 1 parameters, without enabling IPsec interface mode
B. Define the phase 2 parameters.
C. Set the phase 2 encapsulation method to transport mode
D. Define at least one firewall policy, with the action set to IPsec.
E. Define a route to the remote network over the IPsec tunnel.

Correct Answer: CDE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 10
Which of the following statements about NTLM authentication are correct? (Choose two.)

A. It is useful when users log in to DCs that are not monitored by a collector agent.
B. It takes over as the primary authentication method when configured alongside FSSO.
C. Multi-domain environments require DC agents on every domain controller.
D. NTLM-enabled web browsers are required.

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 11
View the certificate shown to the exhibit, and then answer the following question:

Field	Value
Version	V3
Serial Number	98765432
Signature algorithm	SHA256RSA
Issuer	cn=RootCA,o=BridgeAuthority, Inc.,c=US
Valid from	Tuesday, October 3, 2016 4:33:37 PM
Valid to	Wednesday, October 2, 2019 5:03:37 PM
Subject	cn=John Doe, o=ABC, Inc.,c=US
Public key	RSA (2048 bits)
Key Usage	keyCertSign
Extended Key Usage	Server Authentication (1.3.6.1.5.5.7.3.1), Client Authentication (1.3.6.1.5.5.7.3.2)
Basic Constraints	CA=True, Path Constraint=None
CRL Distribution Points	URL=http://webserver.abcinc.com/arlcert.crl

The CA issued this certificate to which entity?

A. A root CA
B. A person
C. A bridge CA
D. A subordinate CA

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 12
Why does FortiGate keep TCP sessions in the session table for some seconds even after both sides (client and server) have terminated the session?

A. To remove the NAT operation.
B. To generate logs
C. To finish any inspection operations.
D. To allow for out-of-order packets that could arrive after the FIN/ACK packets.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 13
A FortiGate is operating in NAT mode and configured with two virtual LAN (VLAN) sub interfaces added to the physical interface.
Which statements about the VLAN sub interfaces can have the same VLAND ID, only if they have IP addresses in different subnets.

A. The two VLAN sub interfaces can have the same VLAN ID, only if they have IP addresses in different subnets.
B. The two VLAN sub interfaces must have different VLAN IDs.
C. The two VLAN sub interfaces can have the same VLAN ID, only if they belong to different VDOMs.
D. The two VLAN sub interfaces can have the same VLAN ID, only if they have IP addresses in the same subnet.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 14
You mc tasked to design a new IPsec deployment with the following criteria:

- There are two HQ sues that all satellite offices must connect to
- The satellite offices do not need to communicate directly with other satellite offices
- No dynamic routing will be used
- The design should minimize the number of tannels being configured.

Which topology should be used to satisfy all of the requirements?

A. Partial mesh
B. Hub-and-spoke
C. Fully meshed
D. Redundant

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 15
Which of the following statements is true regarding SSL VPN settings for an SSL VPN portal?

A. By default, FortiGate uses WINS servers to resolve names.
B. By default, the SSL VPN portal requires the installation of a client's certificate.
C. By default, split tunneling is enabled.
D. By default, the admin GUI and SSL VPN portal use the same HTTPS port.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 16
Which of the following conditions roust be met in order for a web browser to trust a web server certificate signed by a third-party CA?

A. The web-server certificate DM be installed on the browser
B. The public key of the web server certificate must be installed on die browser
C. The CA certificate that signed the web-server certificate inutile installed on the browser
D. The private key of the CA certificate that signed the browser certificate must be installed on the browser.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 17
When using WPAD DNS method, winch FQDN format do browsers use to query the DNS server?

A)

```
srv_proxy.<local-domain>/wpad.dat
```

B)

```
srv_tcp.wpad.<local-domain>
```

C)

```
wpad.<local-domain>
```

D)

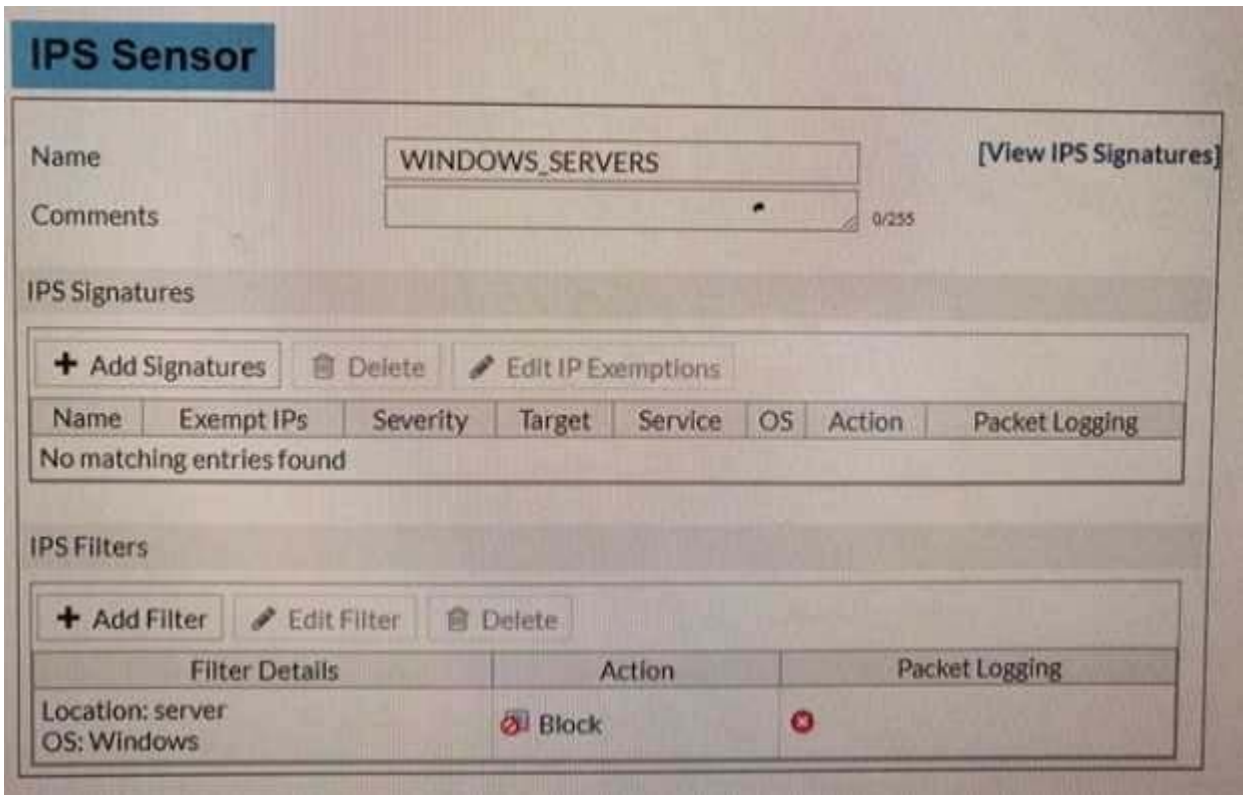
```
proxy.<local-domain>.wpad
```

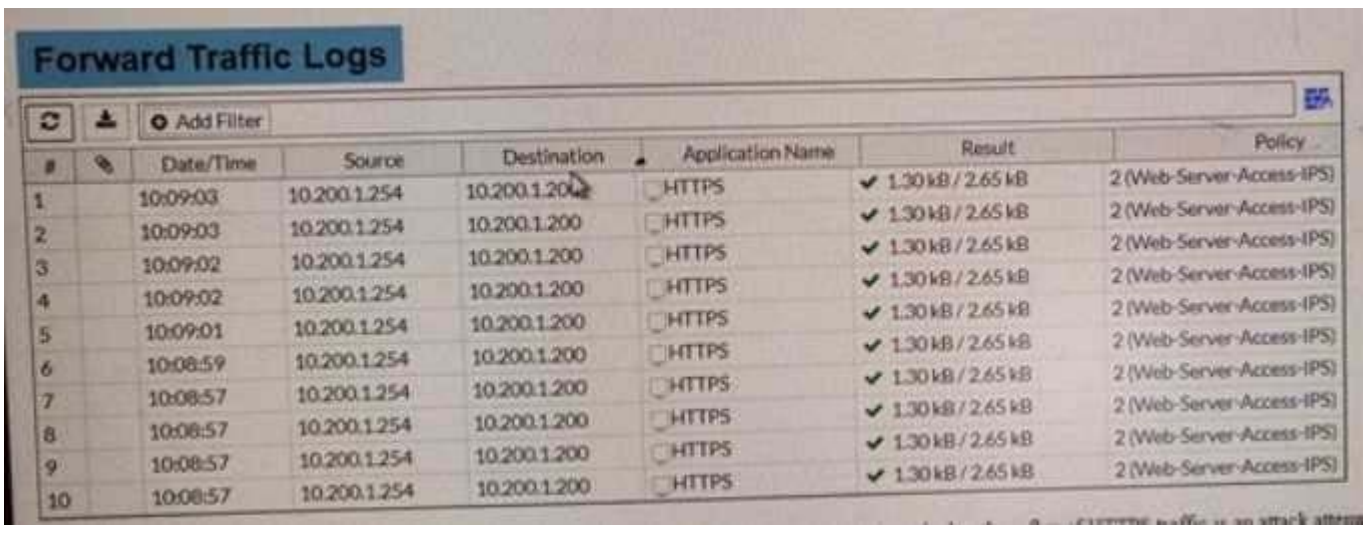
A. Option A
B. Option B
C. Option C
D. Option D

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 18
Examine the IPS sensor configuration and forward traffic logs shown in the exhibit; then, answer the question below.





An administrator has configured the WINDOS_SERVERS IPS sensor in an attempt to determine whether the influx of HTTPS traffic is an attack attempt or not. After applying the IPS sensor, FortiGate is still not generating any IPS logs for the HTTPS traffic.
What is a possible reason for this?

A. The IPS filter is missing the Protocol: HTTPS option.
B. The HTTPS signatures have not been added to the sensor.
C. A DoS policy should be used, instead of an IPS sensor.
D. A DoS policy should be used, instead of an IPS sensor.
E. The firewall policy is not using a full SSL inspection profile.

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:

QUESTION 19
What types of traffic and attacks can be blocked by a web application firewall (WAF) profile? (Choose three.)

A. Traffic to botnet servers
B. Traffic to inappropriate web sites
C. Server information disclosure attacks
D. Credit card data leaks
E. SQL injection attacks

Correct Answer: ACE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 20
Which statement about DLP on FortiGate is true?

A. It can archive files and messages.
B. It can be applied to a firewall policy in a flow-based VDOM
C. Traffic shaping can be applied to DLP sensors.
D. Files can be sent to FortiSandbox for detecting DLP threats.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 21
Examine this PAC file configuration.

```
function FindProxyForURL (url, host) {
 if (shExpMatch (url, "*.fortinet.com/*")) {
    return "DIRECT";}
 if (isInNet (host, "172.25.120.0", "255.255.255.0")) {
    return "PROXY" altproxy.corp.com: 8060";}
 return "PROXY proxy.corp.com: 8090";
}
```

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

A. Browsers can be configured to retrieve this PAC file from the FortiGate.
B. Any web request to the 172.25.120.0/24 subnet is allowed to bypass the proxy.
C. All requests not made to Fortinet.com or the 172.25.120.0/24 subnet, have to go through altproxy.corp.com: 8060.
D. Any web request fortinet.com is allowed to bypass the proxy.

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 22
Which statements about the firmware upgrade process on an active-active HA cluster are true? (Choose two.)

A. The firmware image must be manually uploaded to each FortiGate.
B. Only secondary FortiGate devices are rebooted.
C. Uninterruptable upgrade is enabled by default.
D. Traffic load balancing is temporally disabled while upgrading the firmware.

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 23
Which statements best describe auto discovery VPN (ADVPN). (Choose two.)

A. It requires the use of dynamic routing protocols so that spokes can learn the routes to other spokes.
B. ADVPN is only supported with IKEv2.
C. Tunnels are negotiated dynamically between spokes.
D. Every spoke requires a static tunnel to be configured to other spokes so that phase 1 and phase 2 proposals are defined in advance.

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 24
An administrator needs to create an SSL-VPN connection for accessing an internal server using the bookmark Port Forward. What step is required for this configuration?

A. Configure an SSL VPN realm for clients to use the port forward bookmark.
B. Configure the client application to forward IP traffic through FortiClient.
C. Configure the virtual IP address to be assigned t the SSL VPN users.
D. Configure the client application to forward IP traffic to a Java applet proxy.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 25
What FortiGate configuration is required to actively prompt users for credentials?

A. You must enable one or more protocols that support active authentication on a firewall policy
B. You must position the firewall policy for active authentication before a firewall policy foe passive authentication.
C. You must assign users to a group for active authentication
D. You must enable the Authentication setting on the firewall policy

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 26
Which statements are true regarding firewall policy NAT using the outgoing interface IP address with fixed port disabled? (Choose two.)

A. This is known as many-to-one NAT.
B. Source IP is translated to the outgoing interface IP.
C. Connections are tracked using source port and source MAC address.
D. Port address translation is not used.

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 27
If the Issuer and Subject values are the same in a digital certificate, which type of entity was the certificate issued to?

A. A CRL
B. A person
C. A subordinate CA
D. A root CA

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 28
What is the limitation of using a URL list and application control on the same firewall policy, in NCFW policy-based mode?

A. It limits the scope of application control to the browser-based technology category only.
B. It limits the scope of application control to scan application traffic based on application category only.
C. It limits the scope of application control to scan application traffic using parent signatures only
D. It limits the scope of application control to scan application traffic on DNS protocol only.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 29
The FSSO Collector Agent set to advanced access mode for the Windows Active Directory uses which of the following?

A. LDAP convention
B. NTLM convention
C. Windows convention - NetBios: Domain\Usemame
D. RSSO convention

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 30
Examine the following web filtering log.

```
Date=2016-08-31 time=12:50:06 logid=0316013057 type=utm subtype=webfilter eventtype=ftgd_blk level=warning
vd=root policyid=1 sessionid=149645 user= " " scrip=10.0.1.10 srcport=52919 srcintf= "port3"
dstip=54.230.128.169 dstport=80 dstintf= "port1" proto=6 service="HTTP" hostname= "miniclip.com"
profile= "default" action=blocked reqtype=direct url= "/" sentbyte=286 rcvdbyte=0 direction=outgoing msg= "URL
belongs to a category with warnings enabled" method=domain cat=20 catdesc="Games" crscore=30 crlevel=high
```

Which statement about the log message is true?

A. The action for the category Games is set to block.
B. The usage quota for the IP address 10.0.1.10 has expired.
C. The name of the applied web filter profile is default.
D. The web site miniclip.com matches a static URL filter whose action is set to Warning.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 31
Which of the following SD-WAN load 璟alancing method use interface weight value to distribute traffic? (Choose two.)

A. Source IP
B. Spillover
C. Volume
D. Session

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 32
Which is a requirement for creating an inter-VDOM link between two VDOMs?

A. The inspection mode of at least one VDOM must be proxy-based.
B. At least one of the VDOMs must operate in NAT mode.
C. The inspection mode of both VDOMs must match.
D. Both VDOMs must operate in NAT mode.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

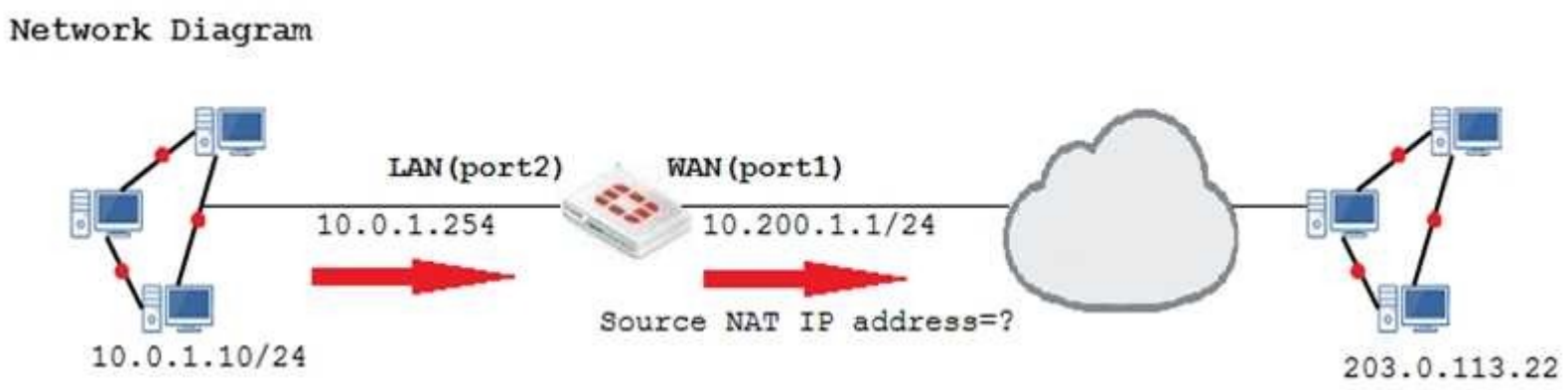
QUESTION 33
Which statement regarding the firewall policy authentication timeout is true?

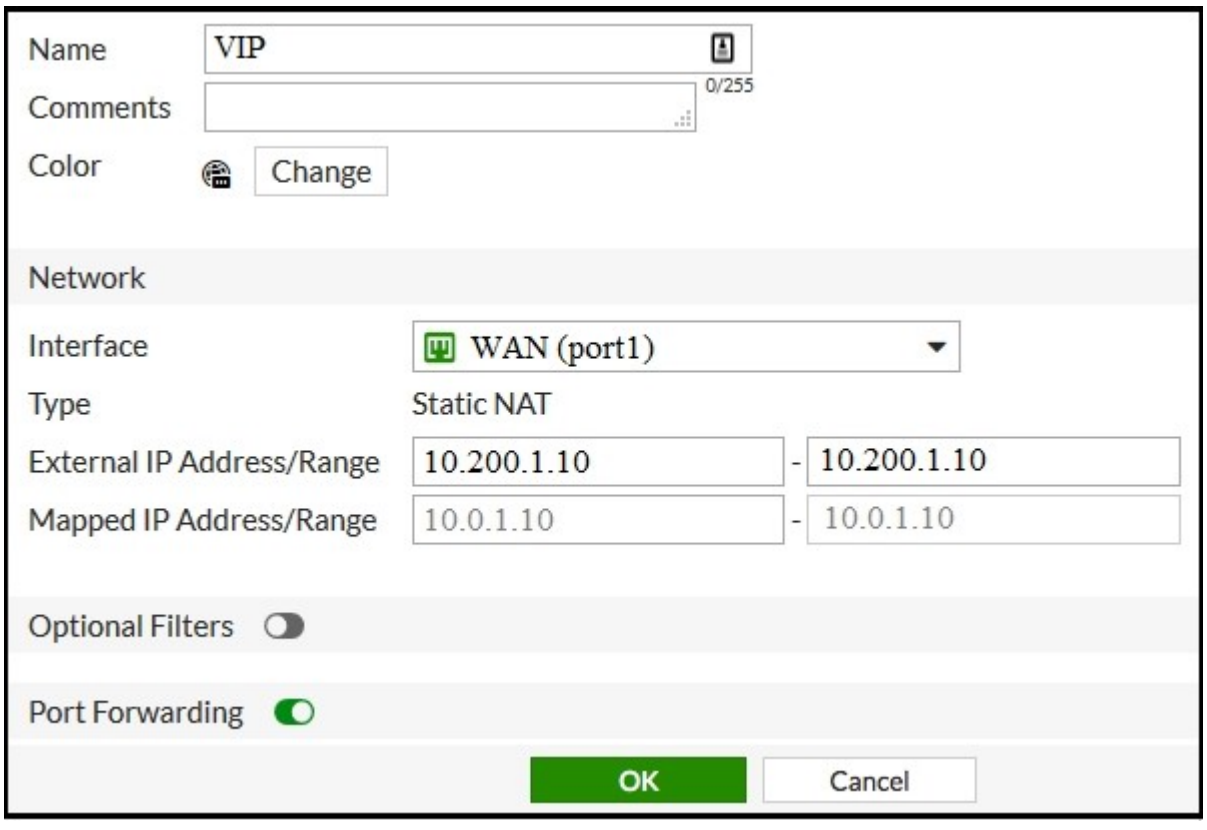
A. It is an idle timeout. The FortiGate considers a user to be "idle" if it does not see any packets coming from the user's source IP.
B. It is a hard timeout. The FortiGate removes the temporary policy for a user's source IP address after this timer has expired.
C. It is an idle timeout. The FortiGate considers a user to be "idle" if it does not see any packets coming from the user's source MAC.
D. It is a hard timeout. The FortiGate removes the temporary policy for a user's source MAC address after this timer has expired.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 34
Examine the exhibit, which contains a virtual IP and firewall policy configuration.





Firewall Policies

ID	Name	Source	Destination	Schedule	Service	Action	NAT
LAN(port2)→ WAN(port1) 1							
1	Full_Access	all	all	always	ALL	✔ ACCEPT	✔ Enabled
LAN(port 1)→ WAN(port 2) 1							
2	WebServer	all	VIP	always	ALL	✔ ACCEPT	✖ Disabled

The WAN (port1) interface has the IP address 10.200.1.1/24. The LAN (port2) interface has the IP address 10.0.1.254/24.
The first firewall policy has NAT enabled on the outgoing interface address. The second firewall policy is configured with a VIP as the destination address.
Which IP address will be used to source NAT the Internet traffic coming from a workstation with the IP address 10.0.1.10/24?

A. 10.200.1.10
B. Any available IP address in the WAN (port1) subnet 10.200.1.0/24
C. 10.200.1.1
D. 10.0.1.254

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 35
What FortiGate components are tested during the hardware test? (Choose three.)

A. Administrative access
B. HA heartbeat
C. CPU
D. Hard disk
E. Network interfaces

Correct Answer: CDE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 36
How do you format the FortiGate flash disk?

A. Load a debug FortiOS image.
B. Load the hardware test (HQIP) image.
C. Execute the CLI command execute formatlogdisk.
D. Select the format boot device option from the BIOS menu.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

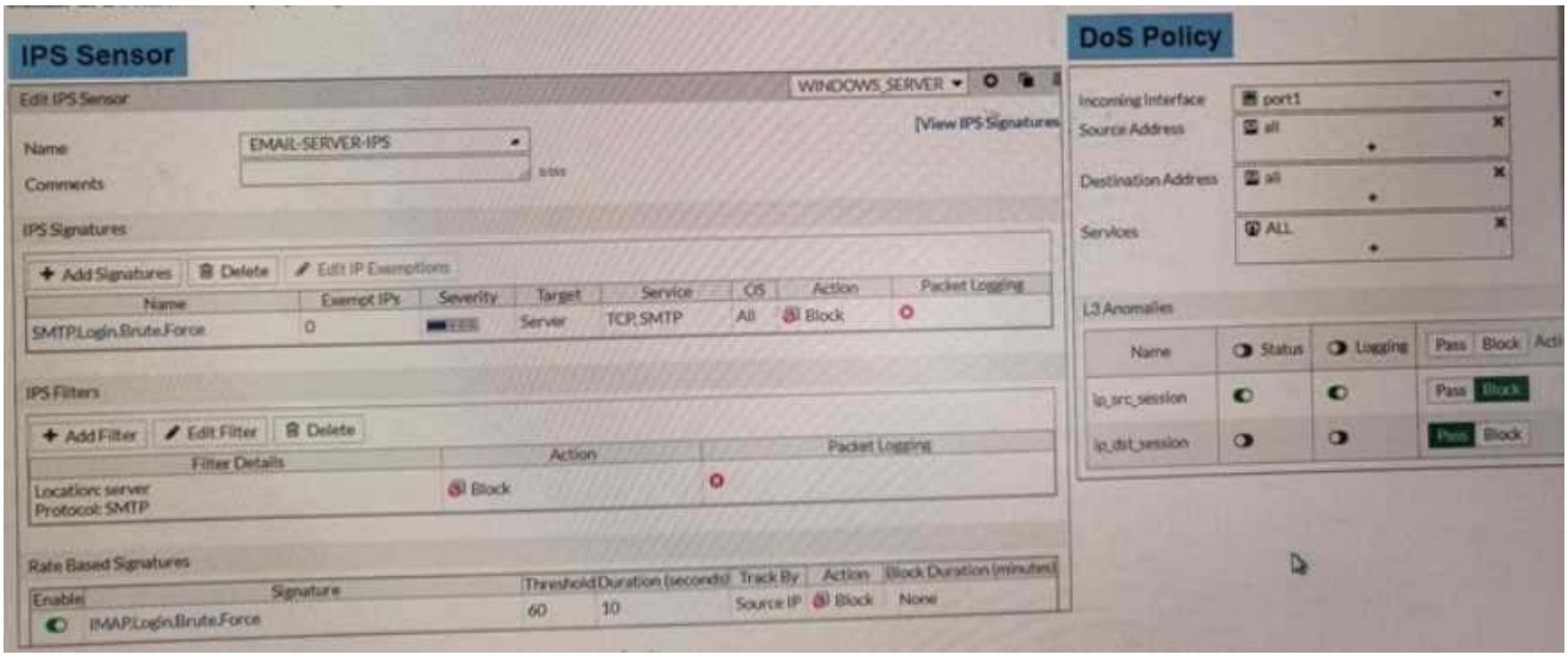
QUESTION 37
Which of the following are valid actions for FortiGuard category based filter in a web filter profile ui proxy-based inspection mode? (Choose two.)

A. Warning
B. Exempt
C. Allow
D. Learn

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 38
Examine the IPS sensor and DoS policy configuration shown in the exhibit, then answer the question below.



When detecting attacks, which anomaly, signature, or filter will FortiGate evaluate first?

A. SMTP.Login.Brute.Force
B. IMAP.Login.brute.Force
C. ip_src_session
D. Location: server Protocol: SMTP

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 39
NGFW mode allows policy-based configured for most impaction rules. Which security profile's configuration does not change when you enable policy-based impaction?

A. Antivirus
B. Web proxy
C. Web filtering
D. Application control

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 40
Which of the following FortiGate configuration tasks will create a route in the policy route table? (Choose two.)

A. Static route created with a Named Address object
B. Static route created with an Internet Services object
C. SD-WAN route created for individual member interfaces
D. SD-WAN rule created to route traffic based on link latency

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 41
Which statement about the IP authentication header (AH) used by IPsec is true?

A. AH does not provide any data integrity or encryption.
B. AH does not support perfect forward secrecy.
C. AH provides data integrity but no encryption.
D. AH provides strong data integrity but weak encryption.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

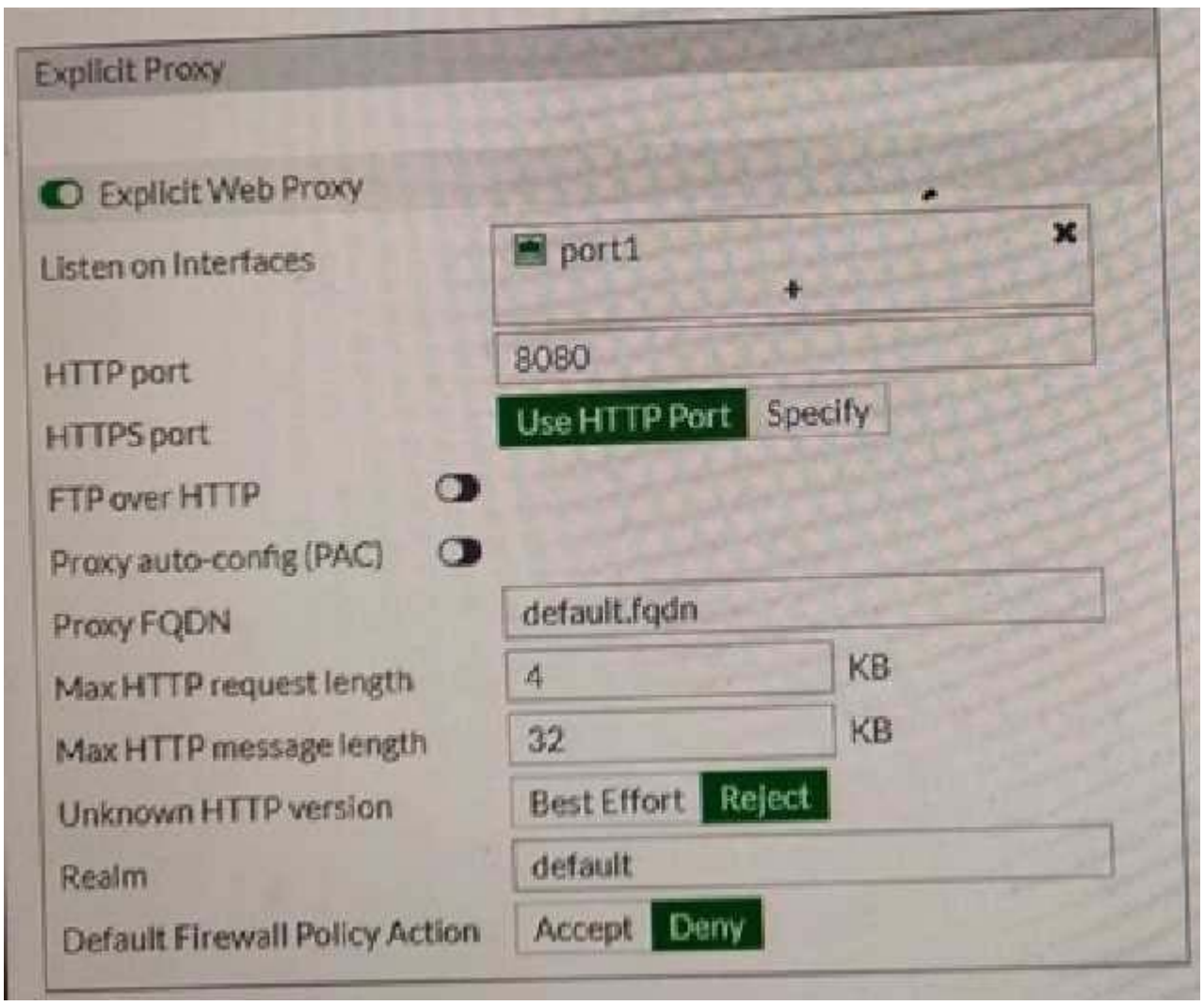
QUESTION 42
If the Services field is configured in a Virtual IP (VIP), which of the following statements is true when central NAT is used?

A. The Services field removes the requirement of creating multiple VIPs for different services.
B. The Services field is used when several VIPs need to be bundled into VIP groups.
C. The Services field does not allow source NAT and destination NAT to be combined in the same policy.
D. The Services field does not allow multiple sources of traffic, to use multiple services, to connect to a single computer.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 43
Examine this explicit web proxy configuration:



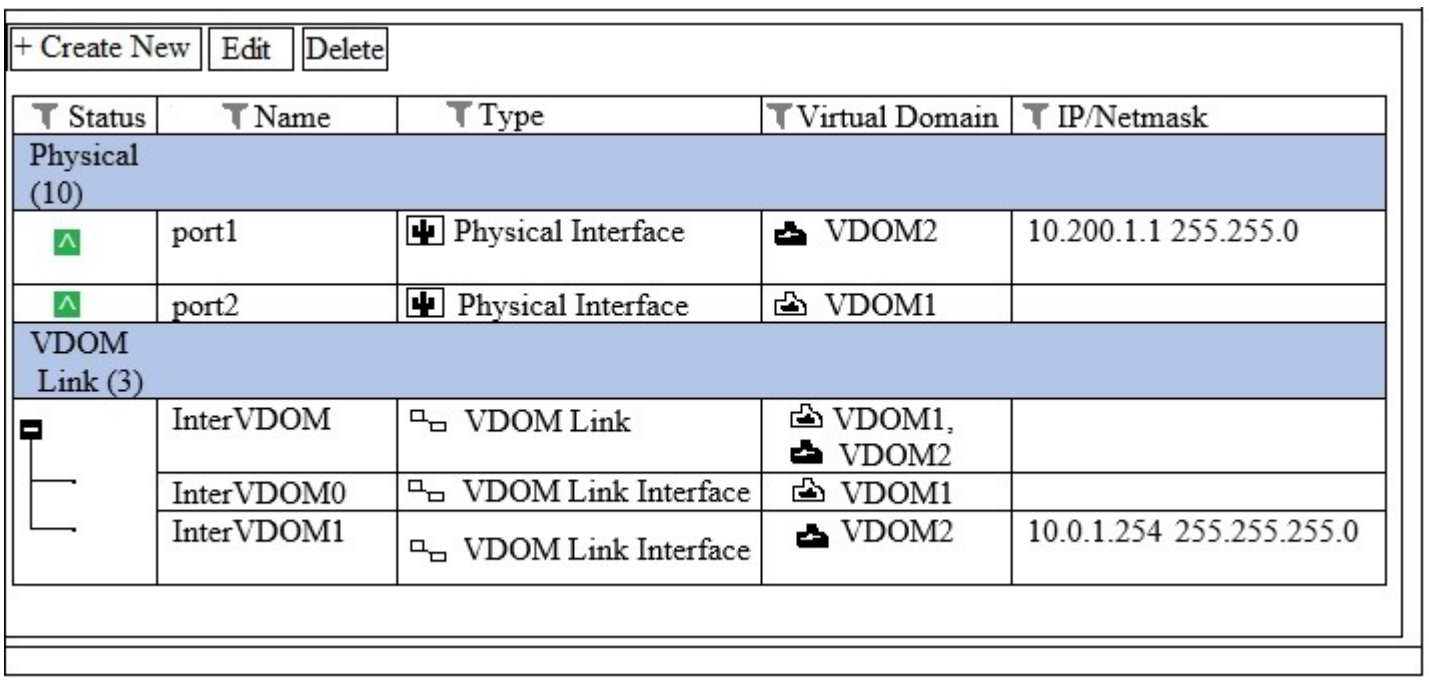
What filter can be used u, the command diagnose sniffer packet to capture the traffic between the client and the explicit web pray?

A. `host 10.0.0.50 and port 80'
B. `host 192.168.0.1 and port 80'
C. `host 192.168.0.2 and port 8080'
D. `host 10.0.50.1 and port 8080'

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 44
View the exhibit.



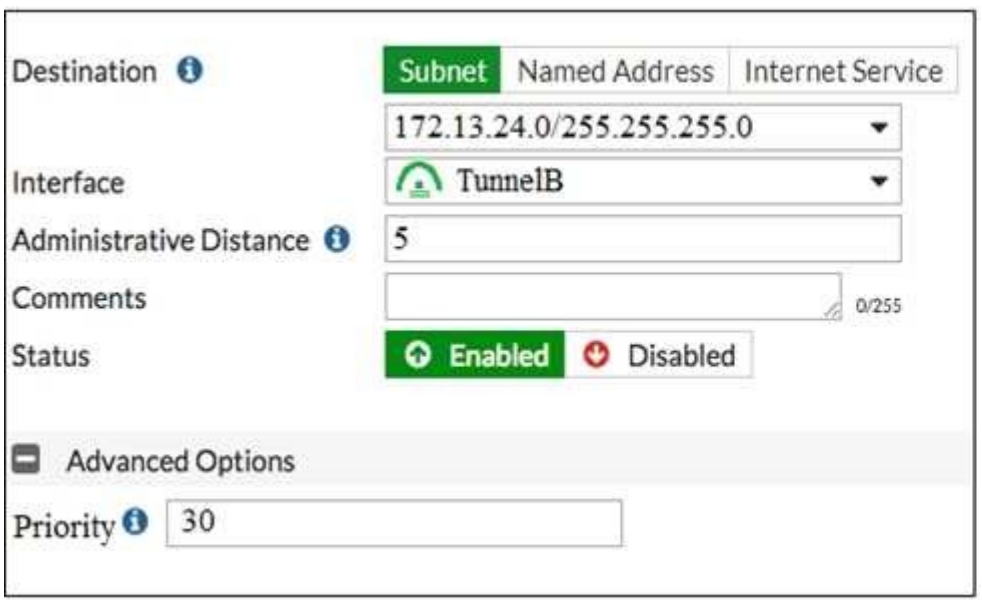
VDOM1 is operating is transparent mode VDOM2 is operating in NAT Route mode. There is an inter- VDOM link between both VDOMs. A client workstation with the IP address 10.0.1.10/24 is connected to port2. A web server with the IP address 10.200.1.2/24 is connected to port1. What is required in the FortiGate configuration to route and allow connections from the client workstation to the web server? (Choose two.)

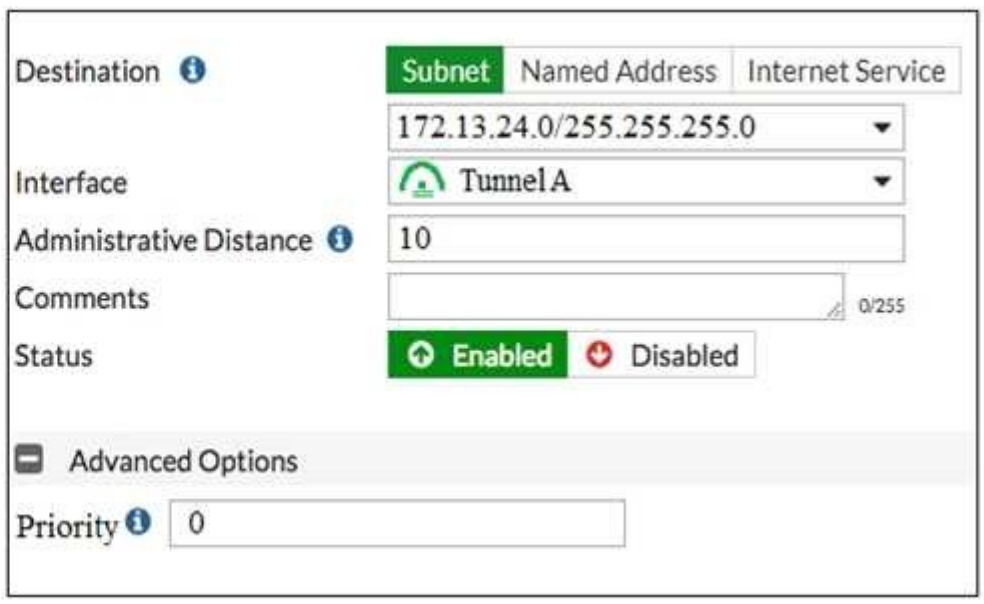
A. A static or dynamic route in VDOM2 with the subnet 10.0.1.0/24 as the destination.
B. A static or dynamic route in VDOM1 with the subnet 10.200.1.0/24 as the destination.
C. One firewall policy in VDOM1 with port2 as the source interface and InterVDOM0 as the destination interface.
D. One firewall policy in VDOM2 with InterVDOM1 as the source interface and port1 as the destination interface.

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 45
View the exhibit.





Which of the following statements are correct? (Choose two.)

A. This setup requires at least two firewall policies with the action set to IPsec.
B. Dead peer detection must be disabled to support this type of IPsec setup.
C. The TunnelB route is the primary route for reaching the remote site. The TunnelA route is used only if the TunnelB VPN is down.
D. This is a redundant IPsec setup.

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:

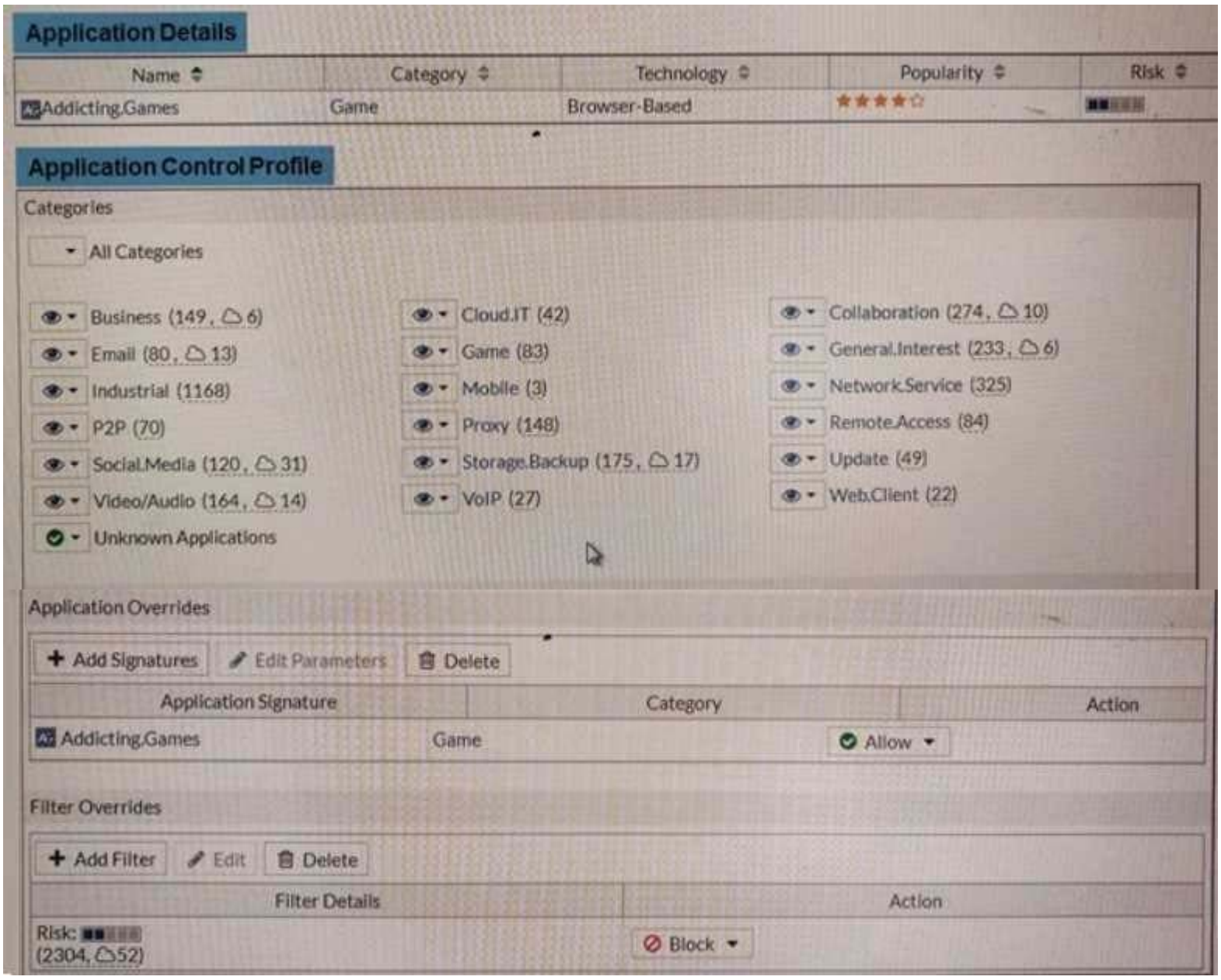
QUESTION 46
What criteria does FortiGate use to look for a matching firewall policy to process traffic? (Choose two.)

A. Services defined in the firewall policy.
B. Incoming and outgoing interfaces
C. Highest to lowest priority defined in the firewall policy.
D. Lowest to highest policy ID number.

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 47
View the exhibit.



A user behind the FortiGate is trying to go to http://www.addictinggames.com (Addicting.Games). Based on this configuration, which statement is true?

A. Addicting.Games is allowed based on the Application Overrides configuration.
B. Addicting.Games is blocked based on the Filter Overrides configuration.
C. Addicting.Games can be allowed only if the Filter Overrides actions is set to Exempt.
D. Addicting.Games is allowed based on the Categories configuration.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 48
Which of the following static routes are not maintained in the routing table? (Choose two.)

A. Named Address routes
B. Dynamic routes
C. ISDB routes
D. Policy routes

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 49
Which Statements about virtual domains (VDOMs) arc true? (Choose two.)

A. Transparent mode and NAT/Route mode VDOMs cannot be combined on the same FortiGate.
B. Each VDOM can be configured with different system hostnames.
C. Different VLAN sub-interfaces of the same physical interface can be assigned to different VDOMs.
D. Each VDOM has its own routing table.

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 50
An administrator wants to configure a FortiGate as a DNS server FortiGate must use us DNS database first, and then relay all irresolvable queries to an external DNS server. Which of the following DNS method must you UM?

A. Recursive
B. Non-recursive
C. Forward to primary and secondary DNS
D. Forward to system DNS

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 51
What files are sent to FortiSandbox for inspection in flow-based inspection mode?

A. All suspicious files that do not have their hash value in the FortiGuard antivirus signature database.
B. All suspicious files that are above the defined oversize limit value in the protocol options.
C. All suspicious files that match patterns defined in the antivirus profile.
D. All suspicious files that are allowed to be submitted to FortiSandbox in the antivirus profile.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 52
Which statements about a One-to-One IP pool are true? (Choose two.)

A. It is used for destination NAT.
B. It allows the fixed mapping of an internal address range to an external address range.
C. It does not use port address translation.
D. It allows the configuration of ARP replies.

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 53
A company needs to provide SSL VPN access to two user groups. The company also needs to display different welcome messages on the SSL VPN login screen for both user groups. What is required in the SSL VPN configuration to meet these requirements?

A. Different SSL VPN realms for each group.
B. Two separate SSL VPNs in different interfaces mapping the same ssl.root.
C. Two firewall policies with different captive portals.
D. Different virtual SSL VPN IP addresses for each group.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 54
An administrator is investigating a report of users having intermittent issues with browsing the web.
The
administrator ran diagnostics and received the output shown in the exhibit.

```
# diagnose sys session stat
misc info: session_count=16 setup_rate=0 exp_count=0 clash=889
memory_tension_drop=0 ephemeral=1/16384 removeable=3
delete=0, flush=0, dev_down=16/69
firewall error stat:
error1=00000000
error2=00000000
error3=00000000
error4=00000000
tt=00000000
cont=0005e722
ids_recv=000fdc94
url_recv=00000000
av_recv=001fee47
fqdn_count=00000000
tcp reset stat: syncqf=119 acceptqf=0 no-listener=3995 data=0 ses=2 ips=0
global: ses_limit=0 ses6_limit=0 rt_limit=0 rt6_limit=0
```

Examine the diagnostic output shown exhibit. Which of the following options is the most likely cause of this issue?

A. NAT port exhaustion
B. High CPU usage
C. High memory usage
D. High session timeout value

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 55
An administrator has configured central DNAT and virtual IPs. Which of the following can be selected in the firewall policy Destination field?

A. A VIP group
B. The mapped IP address object of the VIP object
C. A VIP object
D. An IP pool

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 56
An administrator needs to strengthen the security for SSL VPN access. Which of the following statements are best practices to do so? (Choose three.)

A. Configure split tunneling for content inspection.
B. Configure host restrictions by IP or MAC address.
C. Configure two-factor authentication using security certificates.
D. Configure SSL offloading to a content processor (FortiASIC).
E. Configure a client integrity check (host-check).

Correct Answer: CDE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 57
Which statement about FortiGuard services for FortiGate is true?

A. The web filtering database is downloaded locally on FortiGate.
B. Antivirus signatures are downloaded locally on FortiGate.
C. FortiGate downloads IPS updates using UDP port 53 or 8888.
D. FortiAnalyzer can be configured as a local FDN to provide antivirus and IPS updates.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 58
Which of the following route attributes must be equal for static routes to be eligible for equal cost multipath (ECMP) routing? (Choose two.)

A. Priority
B. Metric
C. Distance
D. Cost

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 59
View the exhibit.

```
Local-FortiGate # diagnose sys ha checksum cluster

================== FGVM010000058290 ==================

is_manage_master()=1, is_root_master()=1
debugzone
global: 85 26 52 f2 f9 6e 3c c9 f5 21 1a 78 69 b6 20 bd
root: 30 51 63 1b 2d ef 77 aa f7 50 00 25 4d 42 a9 7d
all: 38 28 3d e4 24 8f 5b 10 8a 64 30 f2 34 13 c1 35

checksum
global: 85 26 52 f2 f9 6e 3c c9 f5 21 1a 78 69 b6 20 bd
root: 30 51 63 1b 2d ef 77 aa f7 50 00 25 4d 42 a9 7d
all: 38 28 3d e4 24 8f 5b 10 8a 64 30 f2 34 13 c1 35

================== FGVM010000058289 ==================

is_manage_master()=0, is_root_master()=0
debugzone
global: 85 26 52 f2 f9 6e 3c c9 f5 21 1a 78 69 b6 20 bd
root: 30 51 63 1b 2d ef 77 aa f7 50 00 25 4d 8a 55 8b
all: 38 28 3d e4 24 8f 5b 10 8a 64 30 f2 34 dc 9a 43

checksum
global: 85 26 52 f2 f9 6e 3c c9 f5 21 1a 78 69 b6 20 bd
root: 30 51 63 1b 2d ef 77 aa f7 50 00 25 4d 8a 55 8b
all: 38 28 3d e4 24 8f 5b 10 8a 64 30 f2 34 dc 9a 43
```

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

A. The all VDOM is not synchronized between the primary and secondary FortiGate devices.
B. The root VDOM is not synchronized between the primary and secondary FortiGate devices.
C. The global configuration is synchronized between the primary and secondary FortiGate devices.
D. The FortiGate devices have three VDOMs.

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:

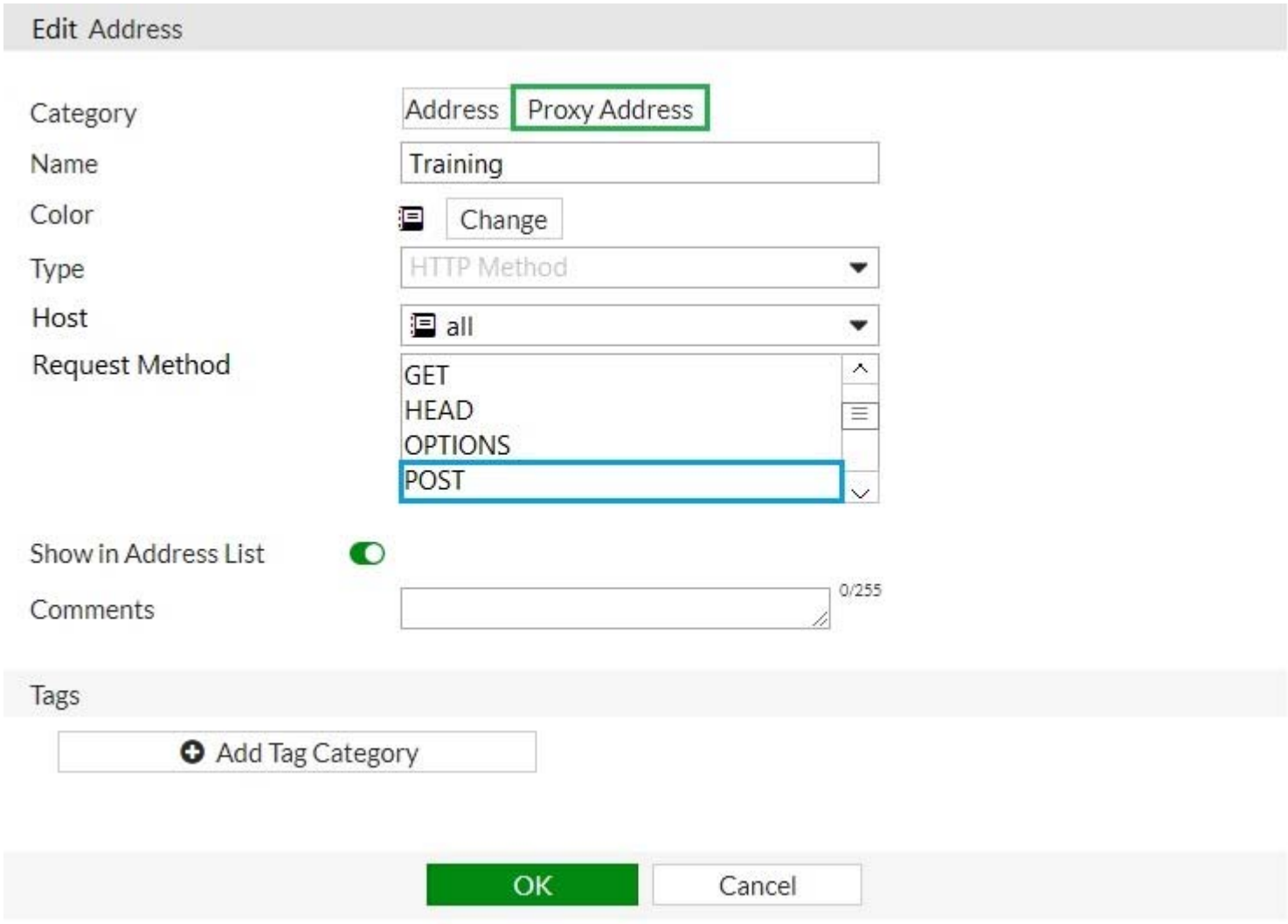
QUESTION 60
Which statement is true regarding the policy ID number of a firewall policy?

A. Defines the order in which rules are processed.
B. Represents the number of objects used in the firewall policy.
C. Required to modify a firewall policy using the CLI.
D. Changes when firewall policies are reordered.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 61
An administrator wants to block HTTP uploads. Examine the exhibit, which contains the proxy address created for that purpose.



Where must the proxy address be used?

A. As the source in a firewall policy.
B. As the source in a proxy policy.
C. As the destination in a firewall policy.
D. As the destination in a proxy policy.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 62
Which statement is true regarding SSL VPN timers? (Choose two.)

A. Allow to mitigate DoS attacks from partial HTTP requests.
B. SSL VPN settings do not have customizable timers.
C. Disconnect idle SSL VPN users when a firewall policy authentication timeout occurs.
D. Prevent SSL VPN users from being logged out because of high network latency.

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 63
An administrator has configured two VLAN interfaces:

```
config system interface
  edit "VLAN10"
        set vdom "VDOM1"
        set forward-domain 100
        set role lan
        set interface "port9"
        set vlanid 10
     next
     edit "VLAN5"
        set vdom "VDOM1"
        set forward-domain 50
        set role lan
        set interface "port10"
        set vlanid 5
     next
end
```

A DHCP server is connected to the VLAN10 interface. A DHCP client is connected to the VLAN5 interface. However, the DHCP client cannot get a dynamic IP address from the DHCP server. What is the cause of the problem?

A. Both interfaces must belong to the same forward domain.
B. The role of the VLAN10 interface must be set to server.
C. Both interfaces must have the same VLAN ID.
D. Both interfaces must be in different VDOMs.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 64
Which of the following statements about virtual domains (VDOMs) are true? (Choose two.)

A. The root VDOM is the management VDOM by default.
B. A FortiGate device has 64 VDOMs, created by default.
C. Each VDOM maintains its own system time.
D. Each VDOM maintains its own routing table.

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 65
Which statements correctly describe transparent mode operation? (Choose three.)

A. All interfaces of the transparent mode FortiGate device must be on different IP subnets.
B. Ethernet packets are forwarded based on destination MAC addresses, not IP addresses.
C. The transparent FortiGate is visible to network hosts in an IP traceroute.
D. It permits inline traffic inspection and firewalling without changing the IP scheme of the network.
E. FortiGate acts as transparent bridge and forwards traffic at Layer 2.

Correct Answer: BDE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 66
Which one of the following processes is involved in updating IPS from FortiGuard?

A. FortiGate IPS update requests are sent using UDP port 443.
B. Protocol decoder update requests are sent to service.fortiguard.net.
C. IPS signature update requests are sent to update.fortiguard.net.
D. IPS engine updates can only be obtained using push updates.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 67
How does FortiGate select the central SNAT policy that is applied to a TCP session?

A. It selects the SNAT policy specified in the configuration of the outgoing interface.
B. It selects the first matching central SNAT policy, reviewing from top to bottom.
C. It selects the central SNAT policy with the lowest priority.
D. It selects the SNAT policy specified in the configuration of the firewall policy that matches the traffic.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 68
Which of the following conditions are required for establishing an IPSec VPN between two FortiGate devices? (Choose two.)

A. If XAuth is enabled as a server in one peer, it must be enabled as a client in the other peer.
B. If the VPN is configured as route-based, there must be at least one firewall policy with the action set to IPSec.
C. If the VPN is configured as DialUp User in one peer, it must be configured as either Static IP Address or Dynamic DNS in the other peer.
D. If the VPN is configured as a policy-based in one peer, it must also be configured as policy-based in the other peer.

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

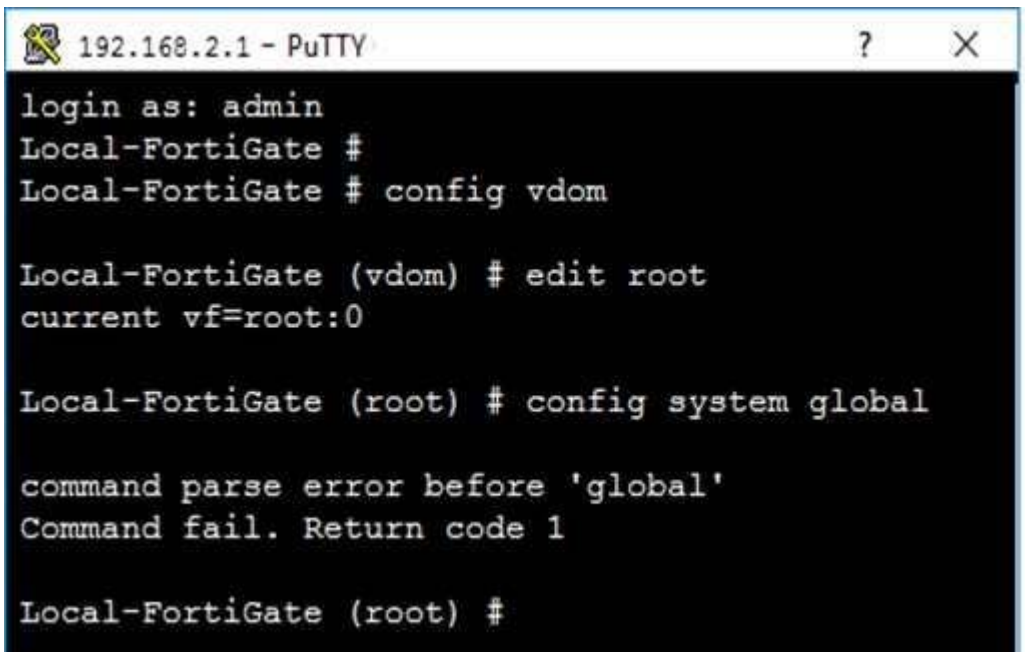
QUESTION 69
Which of the following statements about converse mode are true? (Choose two.)

A. FortiGate stops sending files to FortiSandbox for inspection.
B. FortiGate stops doing RPF checks over incoming packets.
C. Administrators cannot change the configuration.
D. Administrators can access the FortiGate only through the console port.

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 70
View the exhibit.



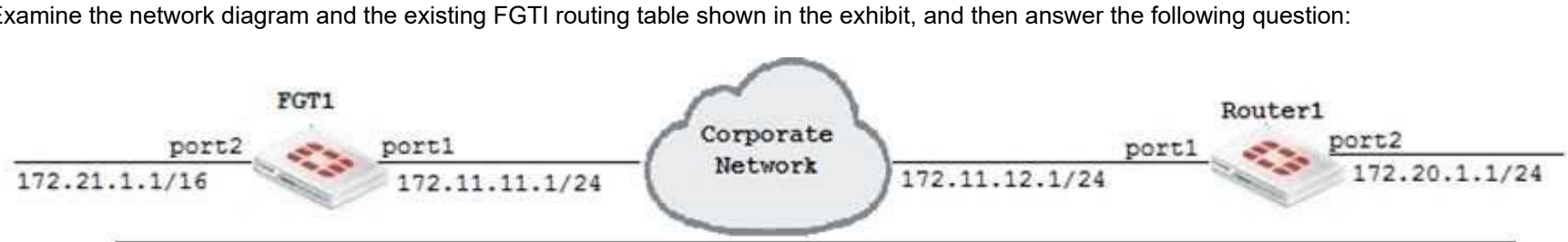
Why is the administrator getting the error shown in the exhibit?

A. The administrator must first enter the command edit global.
B. The administrator admin does not have the privileges required to configure global settings.
C. The global settings cannot be configured from the root VDOM context.
D. The command config system global does not exist in FortiGate.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

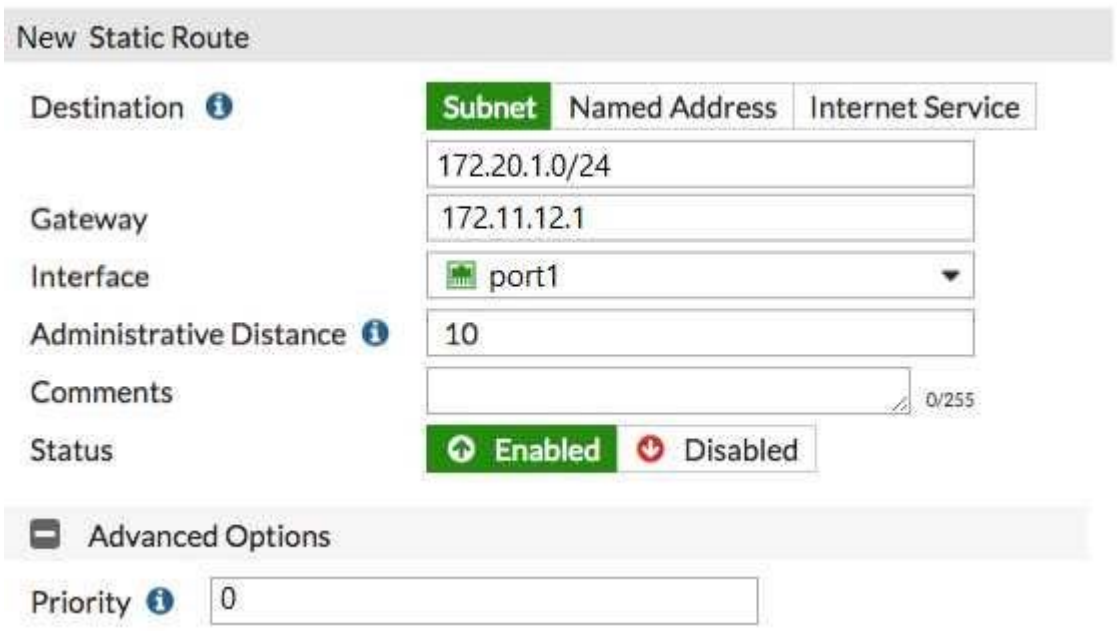
QUESTION 71
Examine the network diagram and the existing FGTI routing table shown in the exhibit, and then answer the following question:




```
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 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      172.20.0.0/16 [10/0] via 172.21.1.2, port2
C      172.21.0.0/16 is directly connected, port2
C      172.11.11.0/24 is directly connected, port1
```

An administrator has added the following static route on FGTI.



Since the change, the new static route is not showing up in the routing table. Given the information provided, which of the following describes the cause of this problem?

A. The new route's destination subnet overlaps an existing route.
B. The new route's Distance value should be higher than 10.
C. The Gateway IP address is not in the same subnet as port1.
D. The Priority is 0, which means that this route will remain inactive.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 72
Which configuration objects can be selected for the Source field of a firewall policy? (Choose two.)

A. Firewall service
B. User or user group
C. IP Pool
D. FQDN address

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 73
View the exhibit.



Which users and user groups are allowed access to the network through captive portal?

A. Users and groups defined in the firewall policy.
B. Only individual users ?not groups ?defined in the captive portal configuration
C. Groups defined in the captive portal configuration
D. All users

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 74
NGFW mode allows policy-based configuration for most inspection rules. Which security profile's configuration does not change when you enable policy-based inspection?

A. Web filtering
B. Antivirus
C. Web proxy
D. Application control

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 75
During the digital verification process, comparing the original and fresh hash results satisfies which security requirement?

A. Authentication.
B. Data integrity.
C. Non-repudiation.
D. Signature verification.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 76
An administration wants to throttle the total volume of SMTP sessions to their email server. Which of the following DoS sensors can be used to achieve this?

A. tcp_port_scan
B. ip_dst_session
C. udp_flood
D. ip_src_session

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 77
Why must you use aggressive mode when a local FortiGate IPSec gateway hosts multiple dialup tunnels?

A. In aggressive mode, the remote peers are able to provide their peer IDs in the first message.
B. FortiGate is able to handle NATed connections only in aggressive mode.
C. FortiClient only supports aggressive mode.
D. Main mode does not support XAuth for user authentication.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 78
View the exhibit:



The client cannot connect to the HTTP web server. The administrator ran the FortiGate built-in sniffer and got the following output:

```
FortiGate # diagnose sniffer packet any "port 80" 4
interfaces=[any]
filters=[port 80]
11.510058 port3 in 10.0.1.10.49255 -> 10.200.1.254.80: syn 697263124
11.760531 port3 in 10.0.1.10.49256 -> 10.200.1.254.80: syn 868017830
14.505371 port3 in 10.0.1.10.49255 -> 10.200.1.254.80: syn 697263124
11.755510 port3 in 10.0.1.10.49256 -> 10.200.1.254.80: syn 868017830
```

What should be done next to troubleshoot the problem?

A. Run a sniffer in the web server.
B. Execute another sniffer in the FortiGate, this time with the filter "host 10.0.1.10".
C. Capture the traffic using an external sniffer connected to port1.
D. Execute a debug flow.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 79
Which of the following statements about policy-based IPsec tunnels are true? (Choose two.)

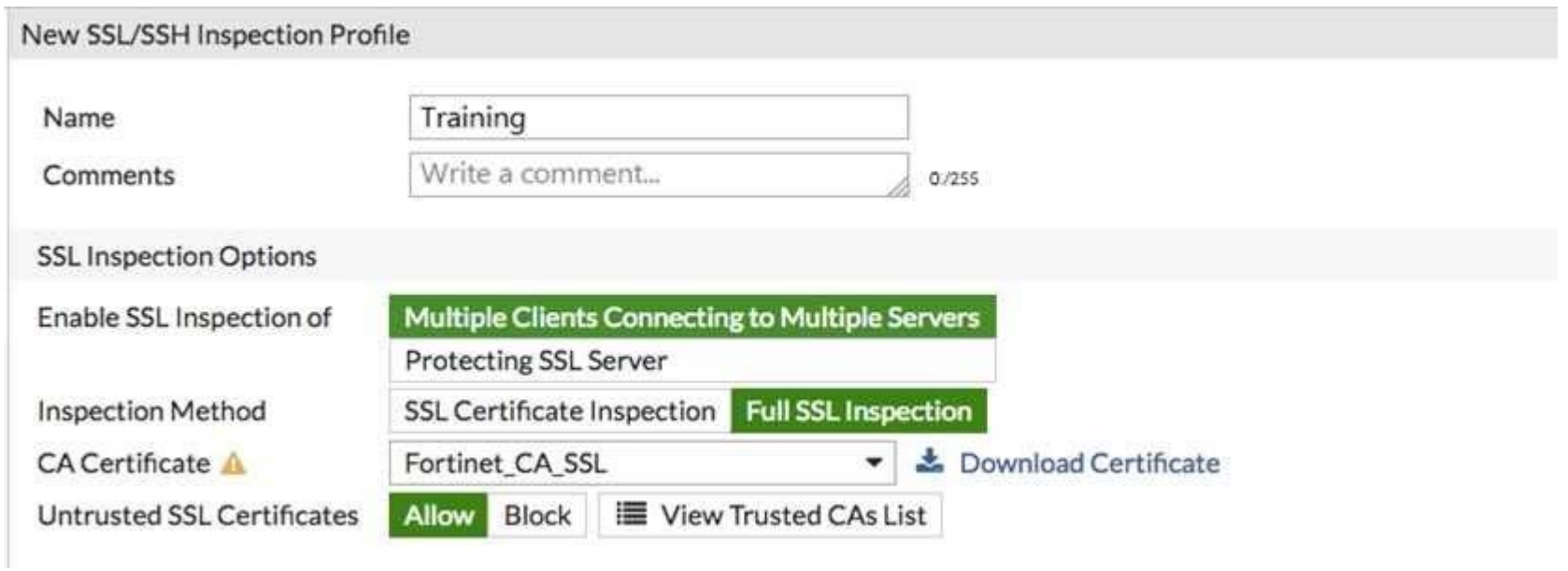
A. They can be configured in both NAT/Route and transparent operation modes.

B. They support L2TP-over-IPsec.
C. They require two firewall policies: one for each directions of traffic flow.
D. They support GRE-over-IPsec.

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 80
An employee connects to the https://example.com on the Internet using a web browser. The web server's certificate was signed by a private internal CA. The FortiGate that is inspecting this traffic is configured for full SSL inspection.
This exhibit shows the configuration settings for the SSL/SSH inspection profile that is applied to the policy that is invoked in this instance. All other settings are set to defaults. No certificates have been imported into FortiGate. View the exhibit and answer the question that follows.



Which certificate is presented to the employee's web browser?

A. The web server's certificate.
B. The user's personal certificate signed by a private internal CA.
C. A certificate signed by Fortinet_CA_SSL.
D. A certificate signed by Fortinet_CA_Untrusted.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 81
When override is enabled, which of the following shows the process and selection criteria that are used to elect the primary FortiGate in an HA cluster?

A. Connected monitored ports > HA uptime > priority > serial number
B. Priority > Connected monitored ports > HA uptime > serial number
C. Connected monitored ports > priority > HA uptime > serial number
D. HA uptime > priority > Connected monitored ports > serial number

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 82
Examine the IPS sensor configuration shown in the exhibit, and then answer the question below.



What are the expected actions if traffic matches this IPS sensor? (Choose two.)

A. The sensor will gather a packet log for all matched traffic.
B. The sensor will not block attackers matching the A32S.Botnet signature.
C. The sensor will block all attacks for Windows servers.
D. The sensor will reset all connections that match these signatures.

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 83
How can you block or allow to Twitter using a firewall policy?

A. Configure the Destination field as Internet Service objects for Twitter.
B. Configure the Action field as Learn and select Twitter.
C. Configure the Service field as Internet Service objects for Twitter.
D. Configure the Source field as Internet Service objects for Twitter.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 84
Which statements about HA for FortiGate devices are true? (Choose two.)

A. Sessions handled by proxy-based security profiles cannot be synchronized.
B. Virtual clustering can be configured between two FortiGate devices that have multiple VDOMs.
C. HA management interface settings are synchronized between cluster members.
D. Heartbeat interfaces are not required on the primary device.

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 85
An administrator is configuring an antivirus profiles on FortiGate and notices that Proxy Options is not listed under Security Profiles on the GUI. What can cause this issue?

A. FortiGate needs to be switched to NGFW mode.
B. Proxy options section is hidden by default and needs to be enabled from the Feature Visibility menu.
C. Proxy options are no longer available starting in FortiOS 5.6.
D. FortiGate is in flow-based inspection mode.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 86
An administrator has configured a route-based IPsec VPN between two FortiGate devices. Which statement about this IPsec VPN configuration is true?

A. A phase 2 configuration is not required.
B. This VPN cannot be used as part of a hub-and-spoke topology.

C. A virtual IPsec interface is automatically created after the phase 1 configuration is completed.
D. The IPsec firewall policies must be placed at the top of the list.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 87
What settings must you configure to ensure FortiGate generates logs for web filter activity on a firewall policy called Full Access? (Choose two.)

A. Enable Event Logging.
B. Enable a web filter security profile on the Full Access firewall policy.
C. Enable Log Allowed Traffic on the Full Access firewall policy.
D. Enable disk logging.

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 88
An administrator is attempting to allow access to https://fortinet.com through a firewall policy that is configured with a web filter and an SSL inspection profile configured for deep inspection. Which of the following are possible actions to eliminate the certificate error generated by deep inspection? (Choose two.)

A. Implement firewall authentication for all users that need access to fortinet.com.
B. Manually install the FortiGate deep inspection certificate as a trusted CA.
C. Configure fortinet.com access to bypass the IPS engine.
D. Configure an SSL-inspection exemption for fortinet.com.

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 89
How does FortiGate verify the login credentials of a remote LDAP user?

A. FortiGate regenerates the algorithm based on the login credentials and compares it to the algorithm stored on the LDAP server.
B. FortiGate sends the user-entered credentials to the LDAP server for authentication.
C. FortiGate queries the LDAP server for credentials.
D. FortiGate queries its own database for credentials.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 90
Which action can be applied to each filter in the application control profile?

A. Block, monitor, warning, and quarantine
B. Allow, monitor, block and learn
C. Allow, block, authenticate, and warning
D. Allow, monitor, block, and quarantine

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 91
View the exhibit.

ID	Name	Source	Destination	Schedule	Service	Applications	URL Category	Action	NAT	Security Profiles	Log	Bytes
port3 → port1 3												
2	Video/Audio	all	all	always	ALL	Video/Audio	+	DENY		certificate-inspection	All	76.74 kB
4	Social_Media	all	all	always	ALL	Social Media	Social Networking	DENY		certificate-inspection	All	940.57 kB
3	ALLOW_ALL	all	all	always	ALL			ACCEPT	Custom		UTM	97.72 kB
Implicit 1												
0	Implicit Deny	all	all	always	ALL			DENY			Disabled	3.58 MB

Based on the configuration shown in the exhibit, what statements about application control behavior are true? (Choose two.)

A. Access to all unknown applications will be allowed.
B. Access to browser-based Social.Media applications will be blocked.
C. Access to mobile social media applications will be blocked.
D. Access to all applications in Social.Media category will be blocked.

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 92
HTTP Public Key Pinning (HPKP) can be an obstacle to implementing full SSL inspection. What solutions could resolve this problem? (Choose two.)

A. Enable Allow Invalid SSL Certificates for the relevant security profile.
B. Change web browsers to one that does not support HPKP.
C. Exempt those web sites that use HPKP from full SSL inspection.
D. Install the CA certificate (that is required to verify the web server certificate) stores of users' computers.

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 93
View the exhibit.

```
date=2018-01-30 time=07:21:49 logid="0316013057" type="utm" subtype="webfilter"
eventtype="ftgd_blk" level="warning" vd="root" logtime=1517325709 policyid=1
sessionid=15332 srcip=10.0.1.20 scrport=59538 srcintf="port3" srcintfrole="undefined"
dstip=208.91.112.55 dstport=80 dstintf="port1" dstintfrole="undefined" proto=6
service="HTTP" hostname="lavito.tk" profile="Category-block-and-warning" action="blocked"
reqtype="direct" url="/" sentbyte=140 rcvdbyte=0 direction="outgoing" msg="URL belongs
a category with warnings enabled" method="domain" cat=0 catdesc="Unrated" crscore=30
crlevel="high"
```

ID	Name	From	To
2	IPS	port1	port3
1	Full_Access	port3	port1
0	Implicit Deny	any	any

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

A. FortiGate blocked the traffic.
B. type indicates that a security event was recorded.
C. 10.0.1.20 is the IP address for lavito.tk.
D. policyid indicates that traffic went through the IPS firewall policy.

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 94
Which of the following statements are true when using WPAD with the DHCP discovery method? (Choose two.)

A. If the DHCP method fails, browsers will try the DNS method.
B. The browser needs to be preconfigured with the DHCP server's IP address.
C. The browser sends a DHCPONFORM request to the DHCP server.
D. The DHCP server provides the PAC file for download.

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 95
Examine the routing database shown in the exhibit, and then answer the following question:

```
FGT1 # get router info routing-table database
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
       > - selected route, * - FIB route, p - stale info

S     *> 0.0.0.0/0 [10/0] via 172.20.121.2, port1, [20/0]
      *>           [10/0] via 10.0.0.2, port2, [30/0]
S        0.0.0.0/0 [20/0] via 192.168.15.2, port3, [10/0]
C     *> 10.0.0.0/24 is directly connected, port2
S        172.13.24.0/24 [10/0] is directly connected, port4
C     *> 172.20.121.0/24 is directly connected, port1
S     *> 192.167.1.0/24 [10/0] via 10.0.0.2, port2
C     *> 192.168.15.0/24 is directly connected, port3
```

Which of the following statements are correct? (Choose two.)

A. The port3 default route has the highest distance.
B. The port3 default route has the lowest metric.
C. There will be eight routes active in the routing table.
D. The port1 and port2 default routes are active in the routing table.

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 96
If traffic matches a DLP filter with the action set to Quarantine IP Address, what action does FortiGate take?

A. It notifies the administrator by sending an email.
B. It provides a DLP block replacement page with a link to download the file.
C. It blocks all future traffic for that IP address for a configured interval.
D. It archives the data for that IP address.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 97
An administrator is running the following sniffer command:

diagnose sniffer packet any "host 10.0.2.10" 3

What information will be included in the sniffer output? (Choose three.)

A. IP header
B. Ethernet header
C. Packet payload
D. Application header
E. Interface name

Correct Answer: ABC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 98
Which of the following statements about the FSSO collector agent timers is true?

A. The workstation verify interval is used to periodically check of a workstation is still a domain member.
B. The IP address change verify interval monitors the server IP address where the collector agent is installed, and the updates the collector agent configuration if it changes.
C. The user group cache expiry is used to age out the monitored groups.
D. The dead entry timeout interval is used to age out entries with an unverified status.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 99
A FortiGate device has multiple VDOMs. Which statement about an administrator account configured with the default prof_admin profile is true?

A. It can create administrator accounts with access to the same VDOM.
B. It cannot have access to more than one VDOM.
C. It can reset the password for the admin account.
D. It can upgrade the firmware on the FortiGate device.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 100
Which of the following features is supported by web filter in flow-based inspection mode with NGFW mode set to profile-based?

A. FortiGuard Quotas
B. Static URL
C. Search engines
D. Rating option

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 101
By default, when logging to disk, when does FortiGate delete logs?

A. 30 days
B. 1 year
C. Never
D. 7 days

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 102
Examine the exhibit, which contains a session diagnostic output.

```
session info: proto=6 proto_state=01 duration=26 expire=3594 timeout=3600 flags=00000000 sockflag=
00000000 sockport=0 av_idx=0 use=4
origin-shaper=
reply-shaper=
per_ip_shaper=
ha_id=0 policy-dir=0 tunnel=/ vlan_cos=0/255
state=may_dirty
statistic(bytes/packets/allow_err): org=1490/14/1 reply=10479/13/1 tuples=2
tx speed (Bps/kbps):56/0 rx speed(Bps/kbps):397/3
orgin->sink: org pre->post, reply pre->post dev=5->3/3->5 gwy=10.200.1.254/10.0.1.10
hook=post dir=org act=snat 10.0.1.10:60267->52.84.125.124:443(10.200.1.100:60267)
hook=pre dir=reply act=dnat 52.84.125.124:443->10.200.1.100:60267(10.0.1.10:60267)
pos/ (before,after) 0/(0,0), 0/(0,0)
misc=0 policy_id=1 auth_info=0 chk_client_info=0 vd=0
serial=00009bd8 tos=ff/ff app_list=0 app=0 url_cat=0
dd_type=0 dd_mode=0
total session 129
```

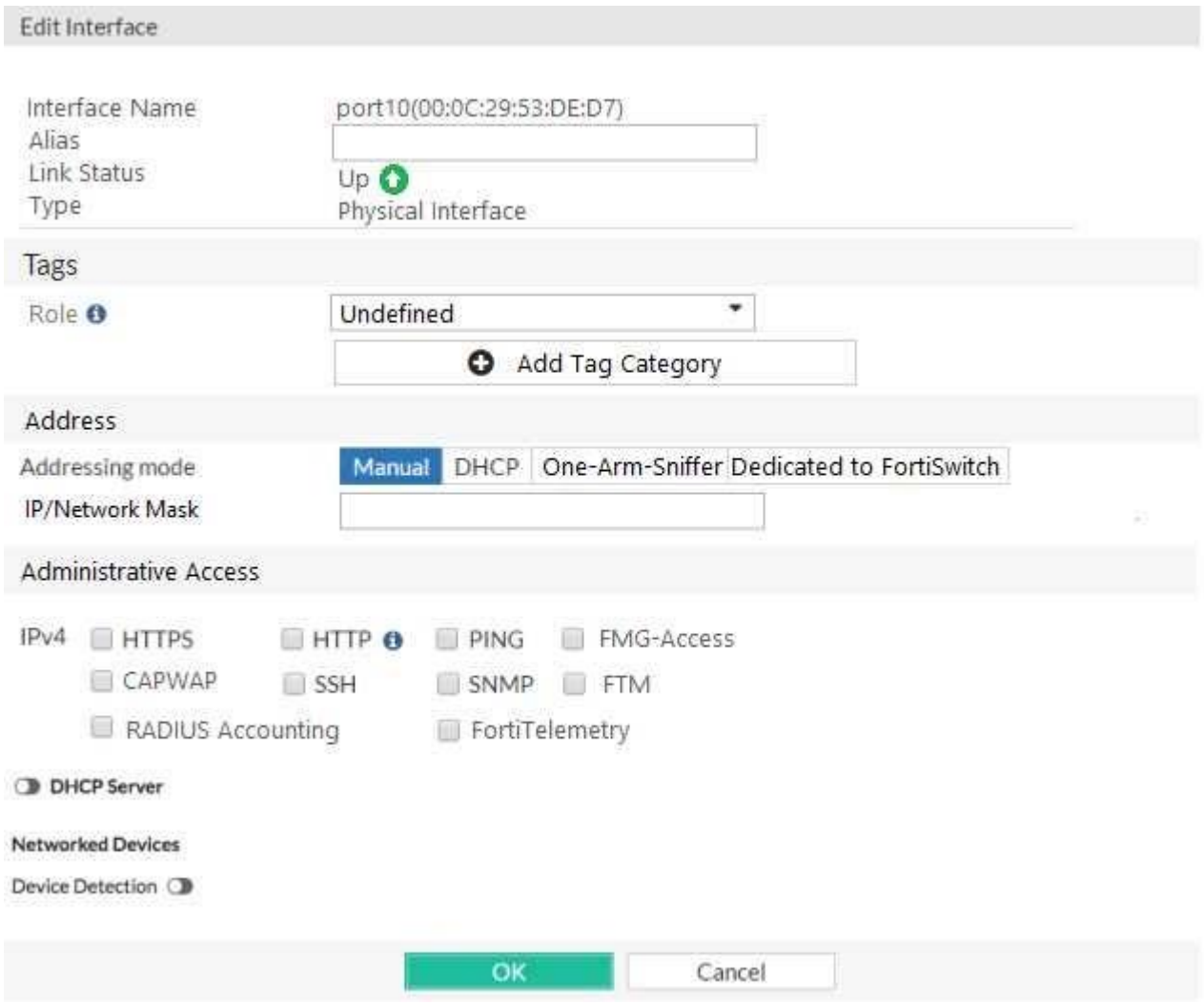
Which of the following statements about the session diagnostic output is true?

A. The session is in ESTABLISHED state.
B. The session is in LISTEN state.
C. The session is in TIME_WAIT state.
D. The session is in CLOSE_WAIT state.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 103
You are configuring the root FortiGate to implement the security fabric. You are configuring port10 to communicate with a downstream FortiGate. View the default Edit Interface in the exhibit below:



When configuring the root FortiGate to communicate with a downstream FortiGate, which settings are required to be configured? (Choose two.)

A. Device detection enabled.
B. Administrative Access: FortiTelemetry.
C. IP/Network Mask.
D. Role: Security Fabric.

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 104
When browsing to an internal web server using a web-mode SSL VPN bookmark, which IP address is used as the source of the HTTP request?

A. remote user's public IP address
B. The public IP address of the FortiGate device.
C. The remote user's virtual IP address.
D. The internal IP address of the FotiGate device.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 105
Examine this output from a debug flow:

```
id=20085 trace_id=1 func=print_pkt_detail line=5363 msg="vd-root received a packet(proto=1,
10.0.1.10:1->10.200.1.254:2048)
from port3. type=8, code=0, id=1, seq=33."
id=20085 trace_id=1 func=init_ip_session_common line=5519 msg="allocate a new session=00000340"
id=20085 trace_id=1 func=vf_ip_route_input_common line=2583 msg="find a route: flag=04000000 gw=10.200.1.254 via
port1"
id=20085 trace_id=1 func=fw_forward_handler line=586 msg="Denied by forward policy check (policy 0)"
```

Why did the FortiGate drop the packet?

A. The next-hop IP address is unreachable.
B. It failed the RPF check.
C. It matched an explicitly configured firewall policy with the action DENY.
D. It matched the default implicit firewall policy.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 106
Examine the exhibit, which shows the output of a web filtering real time debug.

```
Local-FortiGate  #  diagnose  debug enable

Local-FortiGate  #  diagnose debug application urlfilter -1

Local-FortiGate #  msg= "received a request /tmp/.wad_192_0_0.url.socket, addr_len
=31 : d=www.bing.com : 80, id=29, vfname= 'root', vfid=0, profile= 'default', type=0,
  client=10.0.1.10, url_source=1, url= "/"
Url matches local rating
action=10 (ftgd-block) wf-act=3 (BLOCK) user= "N/A" src=10.0.1.10 sport=63683 dst=2
04.79.197.200 dport=80 service= "http" cat=26 cat_desc= "Malicious Websites"
hostname= www.bing.com url= "/"
```

Why is the site www.bing.com being blocked?

A. The web site www.bing.com is categorized by FortiGuard as Malicious Websites.
B. The user has not authenticated with the FortiGate yet.
C. The web server IP address 204.79.197.200 is categorized by FortiGuard as Malicious Websites.
D. The rating for the web site www.bing.com has been locally overridden to a category that is being blocked.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 107
View the exhibit:

Status	Name	VLAN ID	Type	IP/Netmask
Physical(12)				
	port1		Physical Interface	10.200.1.1 255.255.255.0
	port1-VLAN1	1	VLAN	10.200.5.1 255.255.255.0
	port1-VLAN10	10	VLAN	10.0.10.1 255.255.255.0
	port2		Physical Interface	10.200.2.1 255.255.255.0
	port2-VLAN1	1	VLAN	10.0.5.1 255.255.255.0
	port2-VLAN10	10	VLAN	10.0.20.254 255.255.255.0
	port3		Physical Interface	10.0.1.254 255.255.255.0

Which statement about the exhibit is true? (Choose two.)

A. Broadcast traffic received in port1-VLAN10 will not be forwarded to port2-VLAN10.
B. port-VLAN1 is the native VLAN for the port1 physical interface.
C. port1-VLAN10 and port2-VLAN10 can be assigned to different VDOMs.
D. Traffic between port1-VLAN1 and port2-VLAN1 is allowed by default.

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:

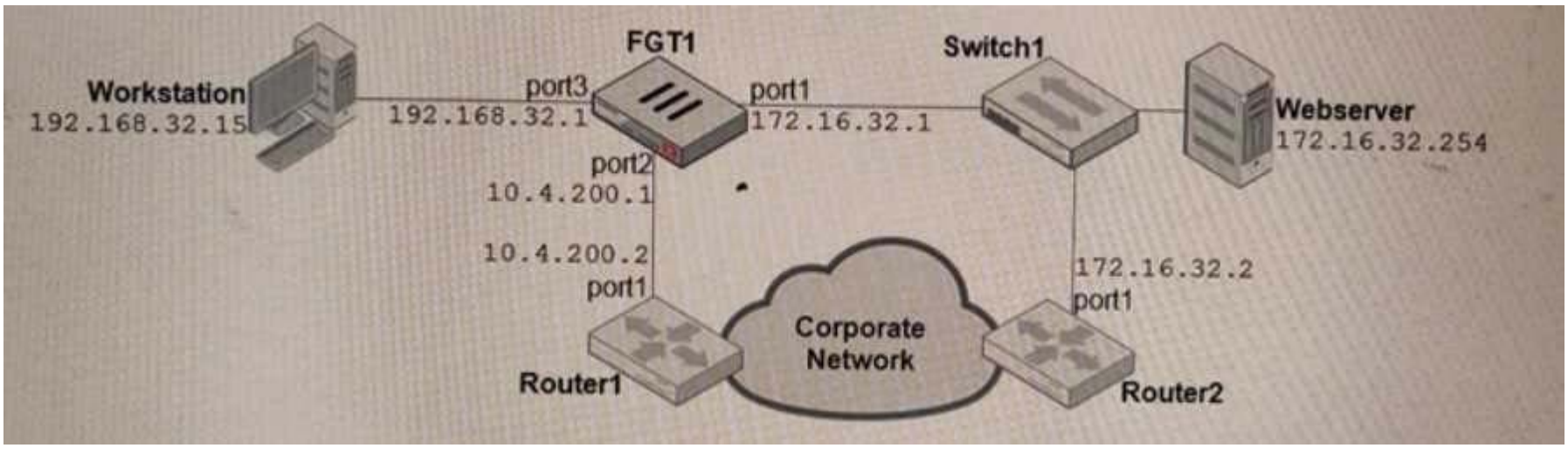
QUESTION 108
Which of the following statements about backing up logs from the CLI and downloading logs from the GUI are true? (Choose two.)

A. Log downloads from the GUI are limited to the current log filter view
B. Log backups from the CLI cannot be restored to another FortiGate.
C. Log backups from the CLI can be configured to upload to FTP at a scheduled time
D. Log downloads from the GUI are stored as LZ4 compressed files.

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 109
Examine the network diagram shown in the exhibit, then answer the following question:



Which one of the following routes is the best candidate route for FGT1 to route traffic from the Workstation to the Web server?

A.
```
172.16.0.0/16 [50/0] via 10.4.200.2, port2 [5/0]
```

B.
```
0.0.0.0/0 [20/0] via 10.4.200.2, port2
```

C.
```
10.4.200.0/30 is directly connected, port2
```

D.
```
172.16.32.0/24 is directly connected, port1
```

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 110
A team manager has decided that while some members of the team need access to particular website, the majority of the team does not. Which configuration option is the most effective option to support this request?

A. Implement a web filter category override for the specified website.
B. Implement web filter authentication for the specified website
C. Implement web filter quotas for the specified website.
D. Implement DNS filter for the specified website.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 111
Which of the following statements are best practices for troubleshooting FSSO? (Choose two.)

A. Include the group of guest users in a policy.
B. Extend timeout timers.
C. Guarantee at least 34 Kbps bandwidth between FortiGate and domain controllers.
D. Ensure all firewalls allow the FSSO required ports.

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 112
Which statements about antivirus scanning mode are true? (Choose two.)

A. In proxy-based inspection mode antivirus buffers the whole file for scarring before sending it to the client.
B. In flow-based inspection mode, you can use the CLI to configure antivirus profiles to use protocol option profiles.
C. In proxy-based inspection mode, if a virus is detected, a replacement message may not be displayed immediately.
D. In quick scan mode, you can configure antivirus profiles to use any of the available signature data bases.

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 113
In a high availability (HA) cluster operating in active-active mode, which of the following correctly describes the path taken by the SYN packet of an HTTP session that is offloaded to a secondary FortiGate?

A. Client > primary FortiGate> secondary FortiGate> primary FortiGate> web server.
B. Client > secondary FortiGate> web server.
C. Client >secondary FortiGate> primary FortiGate> web server.
D. Client> primary FortiGate> secondary FortiGate> web server.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 114
An administrator is configuring an IPsec between site A and site B. The Remotes Gateway setting in both sites has been configured as Static IP Address. For site A, the local quick mode selector is 192.16.1.0/24 and the remote quick mode selector is 192.16.2.0/24. How must the administrator configure the local quick mode selector for site B?

A. 192.168.3.0.24
B. 192.168.2.0.24
C. 192.168.1.0.24
D. 192.168.0.0.8

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 115
An administrator has configured the following settings:

```
config system settings
set ses-denied-traffic enable
end

config system global
set block-session-timer 30
end
```

What does the configuration do? (Choose two.)

A. Reduces the amount of logs generated by denied traffic.
B. Enforces device detection on all interfaces for 30 minutes.
C. Blocks denied users for 30 minutes.
D. Creates a session for traffic being denied.

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 116
An administrator observes that the port1 interface cannot be configured with an IP address. What can be the reasons for that? (Choose three.)

A. The interface has been configured for one-arm sniffer.
B. The interface is a member of a virtual wire pair.
C. The operation mode is transparent.
D. The interface is a member of a zone.
E. Captive portal is enabled in the interface.

Correct Answer: ABC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 117
What information is flushed when the chunk-size value is changed in the config dlp settings?

A. The database for DLP document fingerprinting
B. The supported file types in the DLP filters
C. The archived files and messages
D. The file name patterns in the DLP filters

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 118
Which is the correct description of a hash result as it relates to digital certificates?

A. A unique value used to verify the input data
B. An output value that is used to identify the person or deuce that authored the input data.
C. An obfuscation used to mask the input data.
D. An encrypted output value used to safe-guard die input data

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 119
Examine the exhibit, which shows the partial output of an IKE real-time debug.

```
ike 0: comes 172.20.187.114:500->172.20.186.222:500,ifindex=2....
ike 0: IKEv1 exchange=Identity Protection id=4497f0b077c742b5/0000000000000000 len=296
ike 0:4497f0b077c742b5/0000000000000000:8: responder: main mode get 1st message...
...
ike 0:4497f0b077c742b5/0000000000000000:8: SA proposal chosen, matched gateway Remote
ike 0: found Remote 172.20.186.222 2 -> 172.20.187.114:500
...
ike 0:Remote:8: sent IKE msg (ident_r1send): 172.20.186.222:500->172.20.187.114:500, len=160
ike 0: comes 172.20.187.114:500->172.20.186.222:500,ifindex=2....
ike 0:Remote:8: responder:main mode get 2nd message...
....
ike 0:Remote:8: sent IKE msg (ident_r2send): 172.20.186.222:500->172.20.187.114:500, len=292
ike 0:Remote:8: ISAKMP SA 4497f0b077c742b5/fbbb59b259a0fc3e key 24:DCD18FBE7CFA138E27B06F
ike 0: comes 172.20.187.114:500->172.20.186.222:500,ifindex=2....
ike 0:Remote:8: responder: main mode get 3rd message...
...
ike 0:Remote:8: PSK authentication succeeded
ike 0:Remote:8: authentication OK
ike 0:Remote:8: established IKE SA 4497f0b077c742b5/fbbb59b259a0fc3e
```

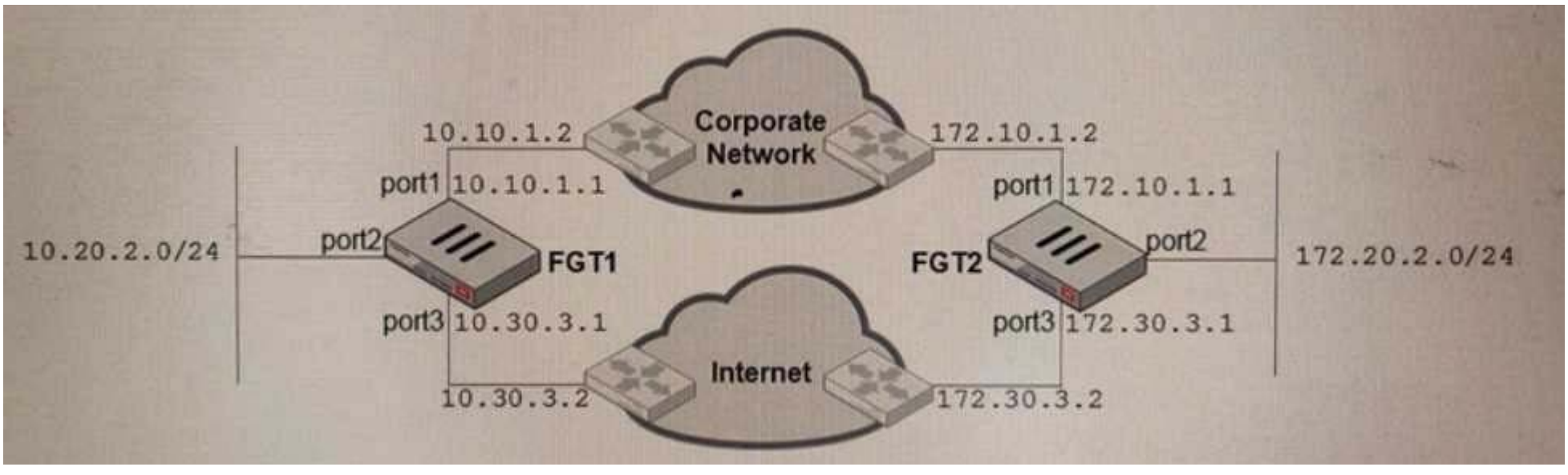
Which of the following statement about the output is true?

A. The VPN is configured to use pre-shared key authentication.
B. Extended authentication (XAuth) was successful.
C. Remote is the host name of the remote IPsec peer.
D. Phase 1 went down.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 120
Examine the network diagram shown in the exhibit, and then answer the following question:



A firewall administrator must configure equal cost multipath (ECMP) routing on FGT1 to ensure both port1 and port3 links are used at the same time for all traffic destined for 172.20.2.0/24. Which of the following static routes will satisfy this requirement on FGT1? (Choose two.)

A. 172.20.2.0/24 (1/0) via 10.10.1.2, port1 [0/0]
B. 172.20.2.0/24 (25/0) via 10.10.3.2, port3 [5/0]
C. 172.20.2.0/24 (1/150) via 10.10.3.2, port3 [10/0]
D. 172.20.2.0/24 (1/150) via 10.30.3.2, port3 [10/0]

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 121
On a FortiGate with a hard disk, how can you upload logs to FortiAnalyzer or FortiManager? (Choose two.)

A. hourly
B. real tune
C. on-demand
D. store-and-upload

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 122
Examine this FortiGate configuration:

```
config system global
  set av-failopen pass
end
```

Examine the output of the following debug command:

```
# diagnose hardware sysinfo conserve
memory conserve mode: on
total RAM: 3040 MB
memory used: 2948 MB 97% of total RAM
memory freeable: 92 MB 3% 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 the FortiGate handling the traffic for new sessions that require inspection?

A. It is allowed, but with no inspection
B. It is allowed and inspected as long as the inspection is flow based
C. It is dropped.
D. It is allowed and inspected, as long as the only inspection required is antivirus.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 123
Which of the following statements correctly describes FortiGates route lookup behavior when searching for a suitable gateway? (Choose two)

A. Lookup is done on the trust packet from the session originator
B. Lookup is done on the last packet sent from the re spender
C. Lookup is done on every packet, regardless of direction
D. Lookup is done on the trust reply packet from the re spender

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 124
The FSSO Collector Agent set to advanced access mode for the Windows Active Directory uses which of the following?

A. LDAP convention
B. NTLM convention
C. Windows convention - NetBios: Domain\Usemame
D. RSSO convention

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 125
Which configuration objects can be selected for the Source field of a firewall policy? (Choose two.)

A. Firewall service
B. User or user group
C. IP Pool
D. FQDN address

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 126
When using SD-WAN, how do you configure the next-hop gateway address for a member interface so that FortiGate can forward Internet traffic?

A. It must be configured in a static route using the sdwan virtual interface.
B. It must be provided in the SD-WAN member interface configuration.
C. It must be configured in a policy-route using the sdwan virtual interface.
D. It must be learned automatically through a dynamic routing protocol.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 127
Which of the following services can be inspected by the DLP profile? (Choose three.)

A. NFS
B. FTP
C. IMAP
D. CIFS
E. HTTP-POST

Correct Answer: BCE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 128
Which of the following statements describe WMI polling mode for the FSSO collector agent? (Choose two.)

A. The NetSessionEnum function is used to track user logoffs.
B. WMI polling can increase bandwidth usage in large networks.
C. The collector agent uses a Windows API to query DCs for user logins.
D. The collector agent do not need to search any security event logs.

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 129
Which statements about DNS filter profiles are true? (Choose two.)

A. They can inspect HTTP traffic.
B. They can redirect blocked requests to a specific portal.
C. They can block DNS requests to known botnet command and control servers.
D. They must be applied in firewall policies with SSL inspection enabled.

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 130
An administrator has configured a dialup IPsec VPN with XAuth. Which statement best describes what occurs during this scenario?

A. Phase 1 negotiations will skip preshared key exchange.
B. Only digital certificates will be accepted as an authentication method in phase 1.C
C. Dialup clients must provide a username and password for authentication.
D. Dialup clients must provide their local ID during phase 2 negotiations.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference: