NSE4_FGT-6.0

Number: 000-000
Passing Score: 800
Time Limit: 120 min
File Version: 1.0

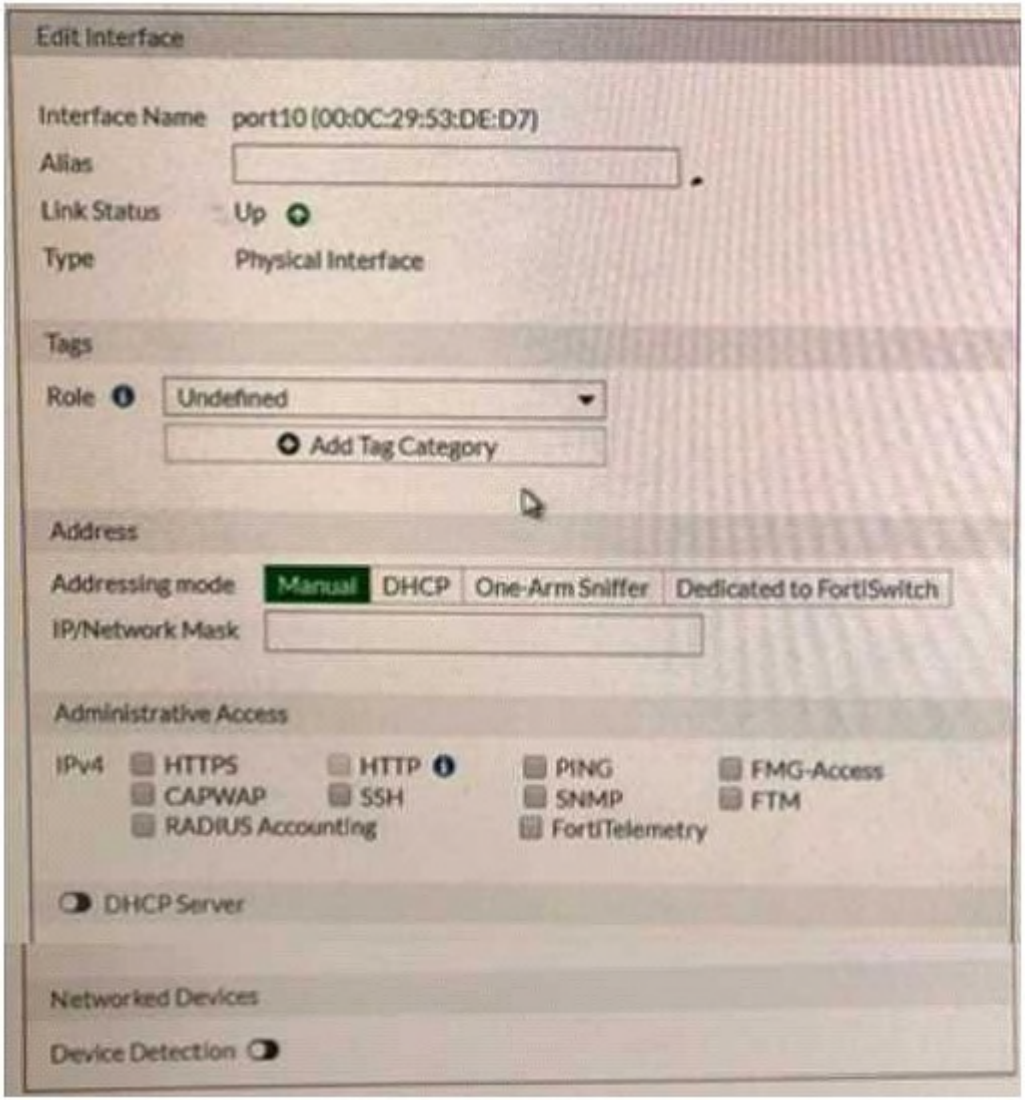
Fortinet NSE 4 - FortiOS 6.0 Exam

NSE4_FGT-6.0

Exam A

QUESTION 1

You are configuring the root FortiGate to implement the security fabric. You are configuring port 10 to communicate with a downstream FartiGate. View the default Edit InterFace in the exhibit below;



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

A. Administrative Access FortiTelemetrT
B. IP/Network Mask.

C. Device Detection enabled.
D. Role Security Fabric.

Answer: BD
Explanation/Reference:

QUESTION 2

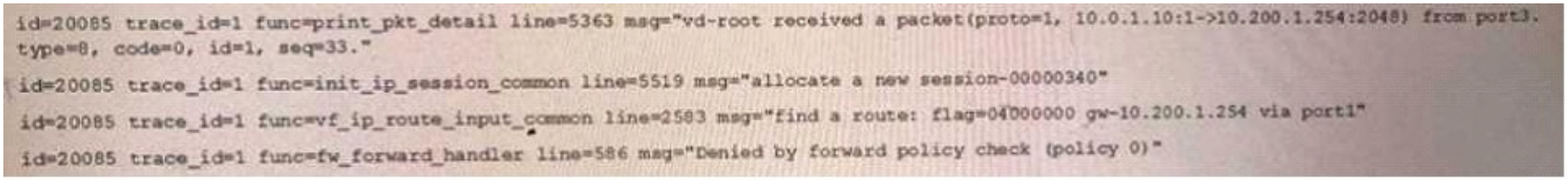
When browsing to an internal web server using a web-mode SSL VPN bookmark, which IP address is used as the source of the HTTP request?

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.

Answer: D
Explanation/Reference:

QUESTION 3

Examine this output from a debug flow:



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

Answer: D
Explanation/Reference:

QUESTION 4

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= "/"
```

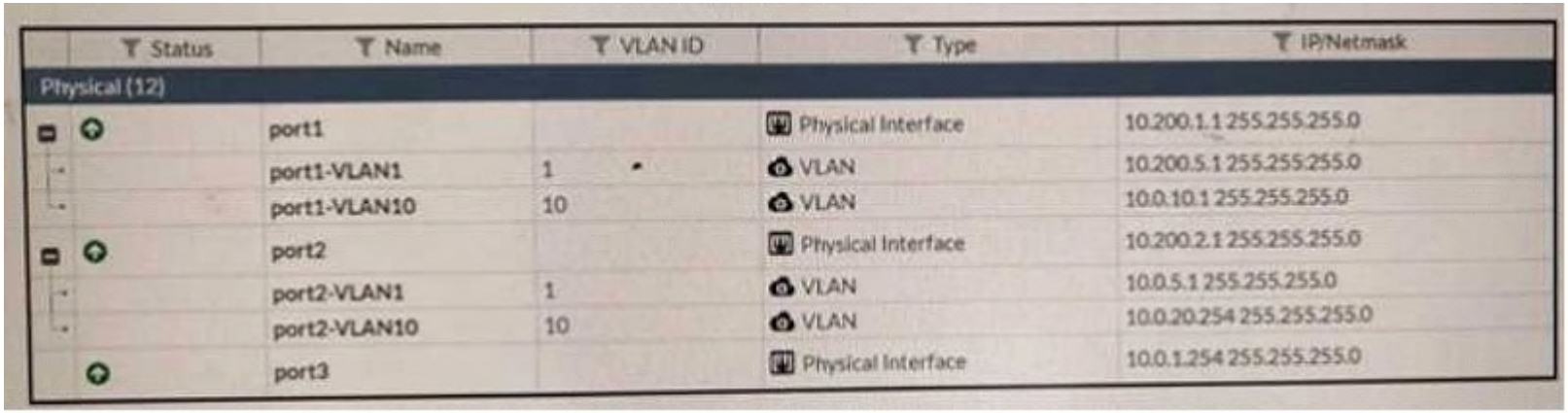
Why is the site www.bing.com being blocked?

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

Answer: A
Explanation/Reference:

QUESTION 5

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

Answer: AD
Explanation/Reference:

QUESTION 6

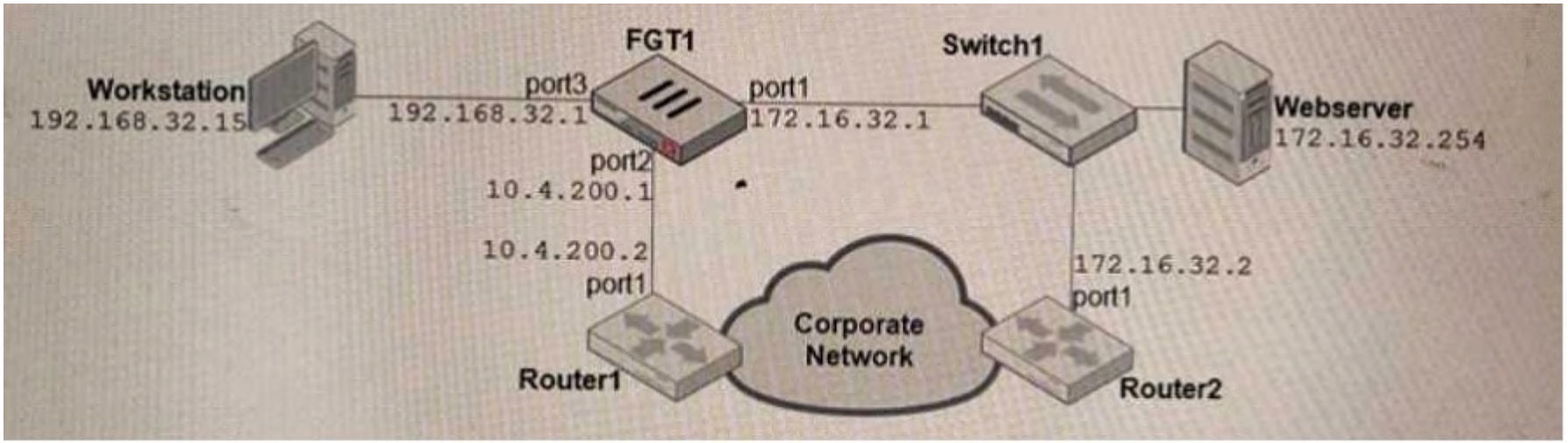
Which of the following statements about backing up logs from the CLI and downloading logs from the GUI are true? (Choose two.)

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.

Answer: BC
Explanation/Reference:

QUESTION 7

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?

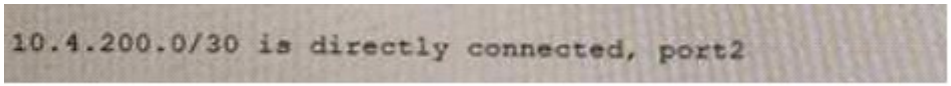
A.

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

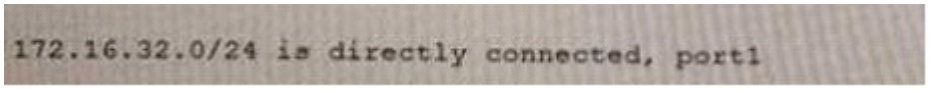
B.

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

C.



D.



E. Option A
F. Option B
G. Option C
H. Option D

Answer: D
Explanation/Reference:

QUESTION 8

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.

Answer: A
Explanation/Reference:

QUESTION 9

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"
```

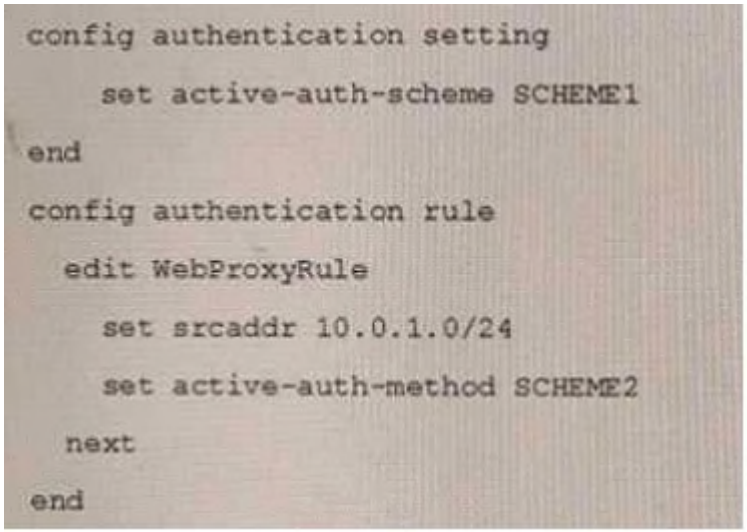
Which statements about the output are correct? (Choose two.)

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.

Answer: AC
Explanation/Reference:

QUESTION 10

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

Answer: B
Explanation/Reference:

QUESTION 11

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

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

Answer: AC
Explanation/Reference:

QUESTION 12

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.

Answer: BD
Explanation/Reference:

QUESTION 13

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.

Answer: D
Explanation/Reference:

QUESTION 14

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

Answer: A
Explanation/Reference:

QUESTION 15

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.

Answer: AC
Explanation/Reference:

QUESTION 16

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

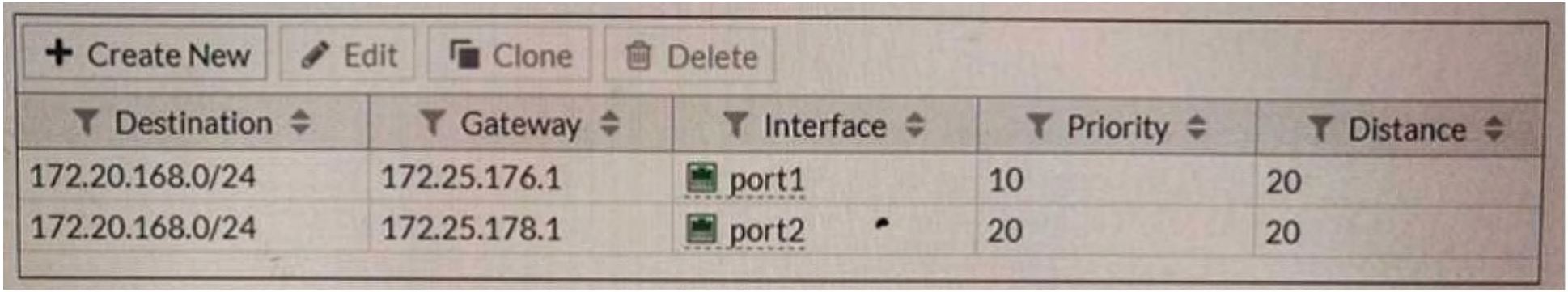
A. Lookup is done on the trust packet from the session originator
B. Lookup is done on the last packet sent from the re spender
C. Lookup is done on every packet, regardless of direction

D. Lookup is done on the trust reply packet from the re spender

Answer: AB
Explanation/Reference:

QUESTION 17

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

Answer: C
Explanation/Reference:

QUESTION 18

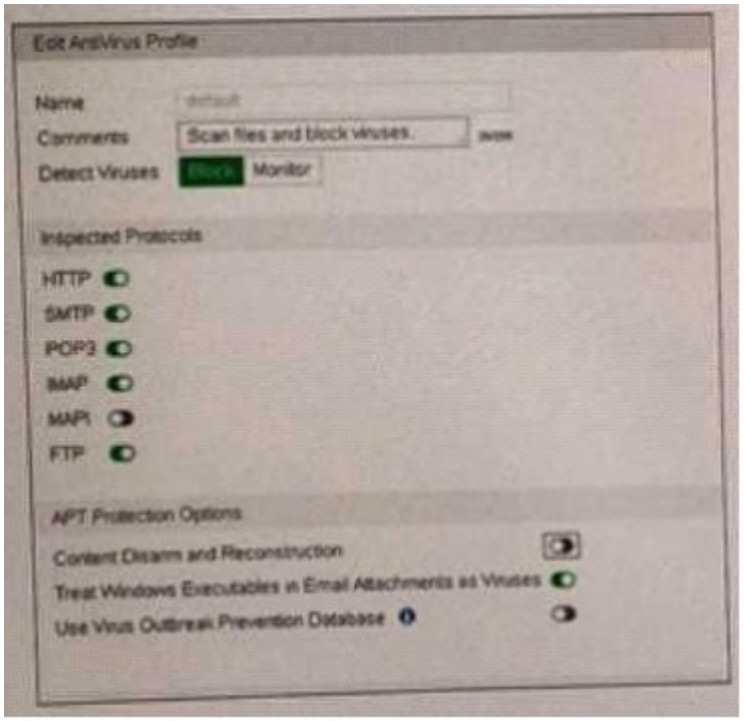
Which of the following statements about central NAT are true? (Choose two.)

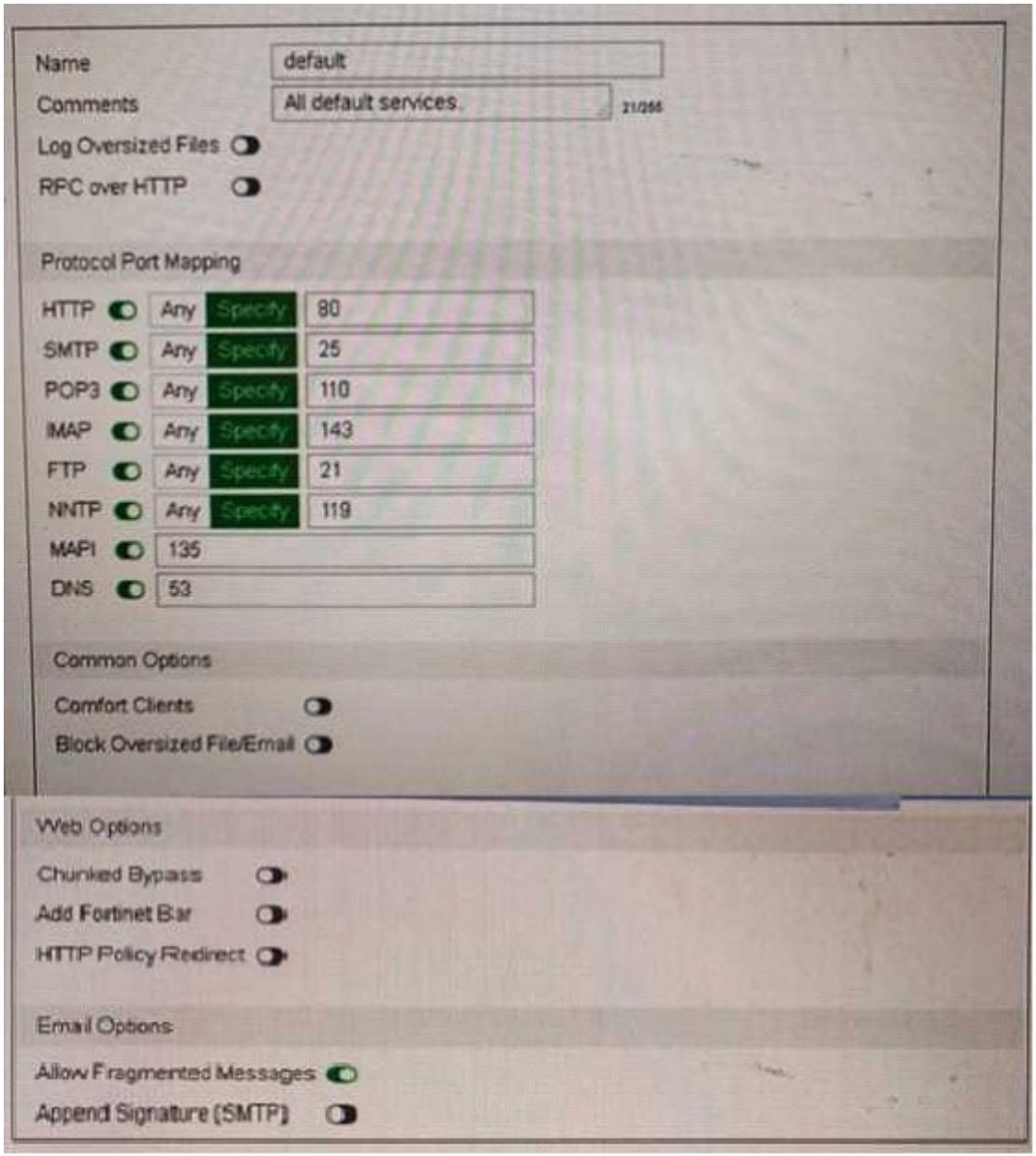
A. IP tool references must be removed from existing firewall policies before enabling central NAT.
B. Central NAT can be enabled or disabled from the CLI only.
C. Source NAT, using central NAT, requires at least one central SNAT policy.
D. Destination NAT, using central NAT, requires a VIP object as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

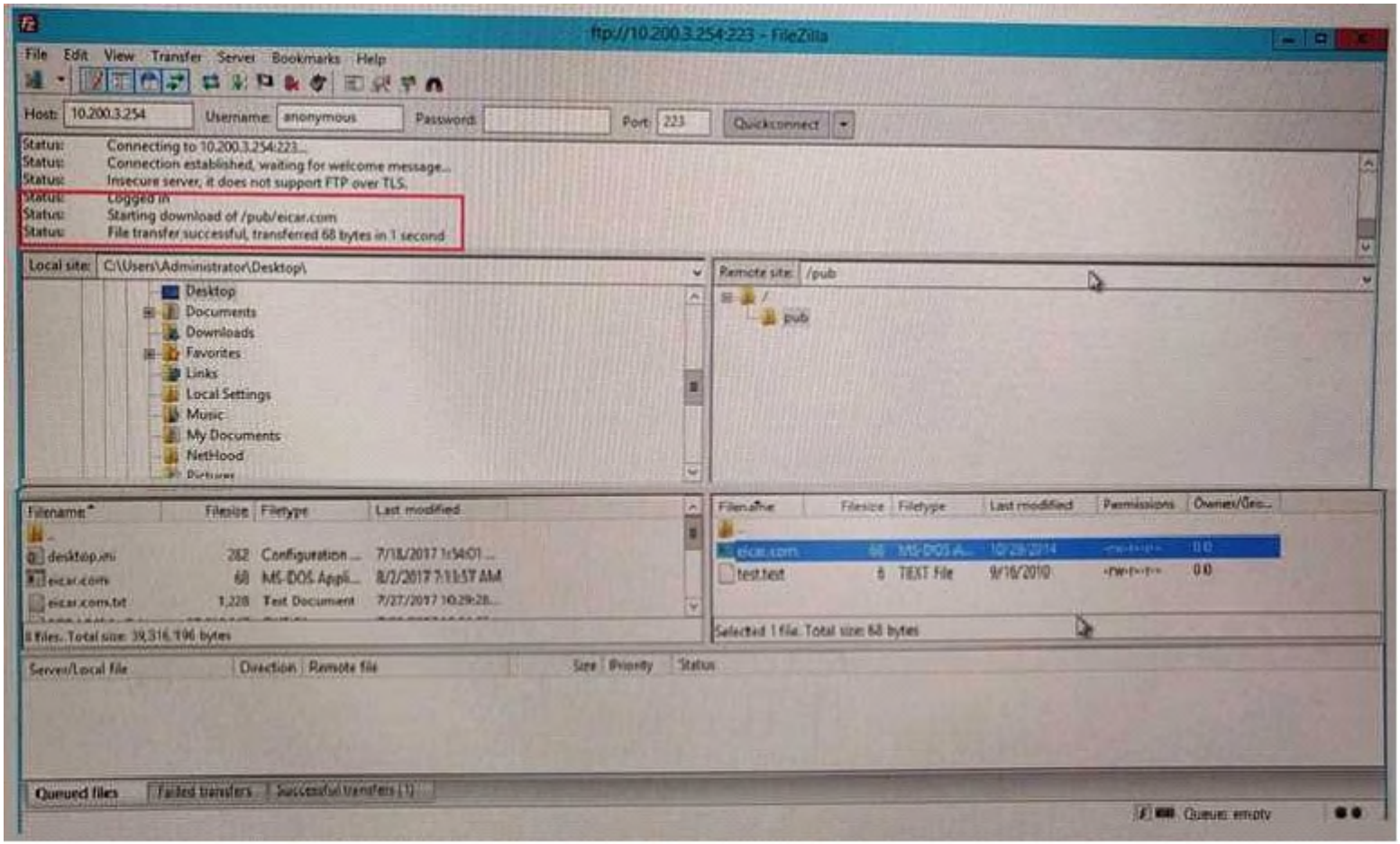
Answer: AB
Explanation/Reference:

QUESTION 19

Refer to the following exhibit.







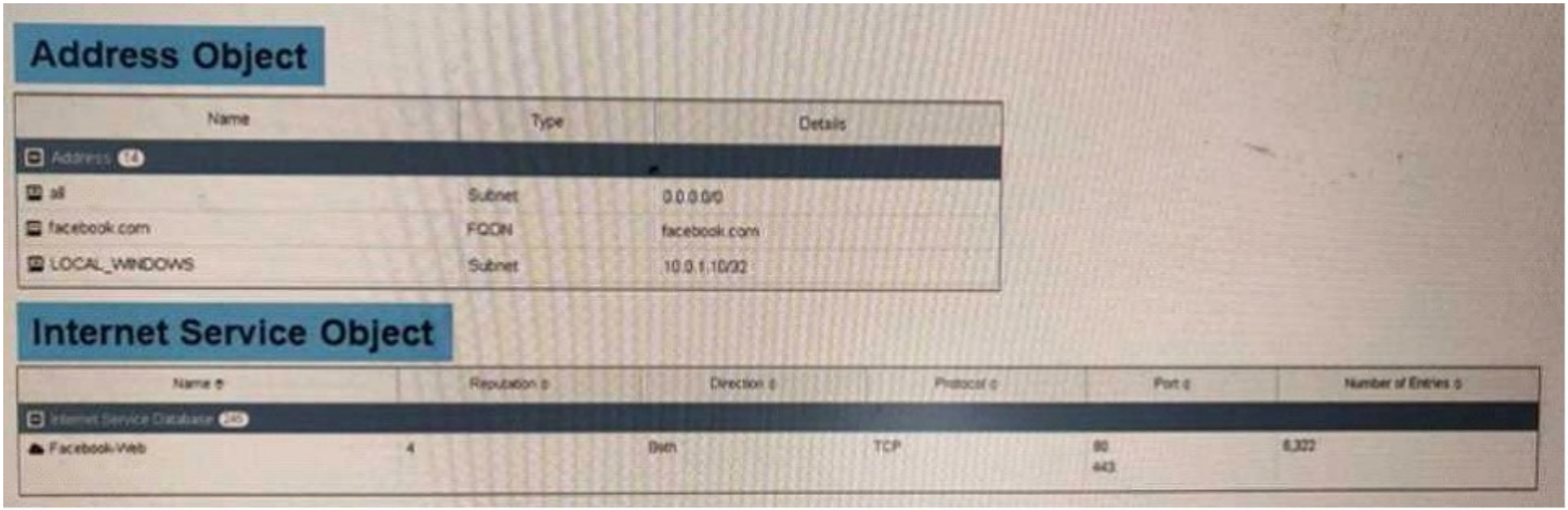
Why is FortiGate not blocking the test file over FTP download?

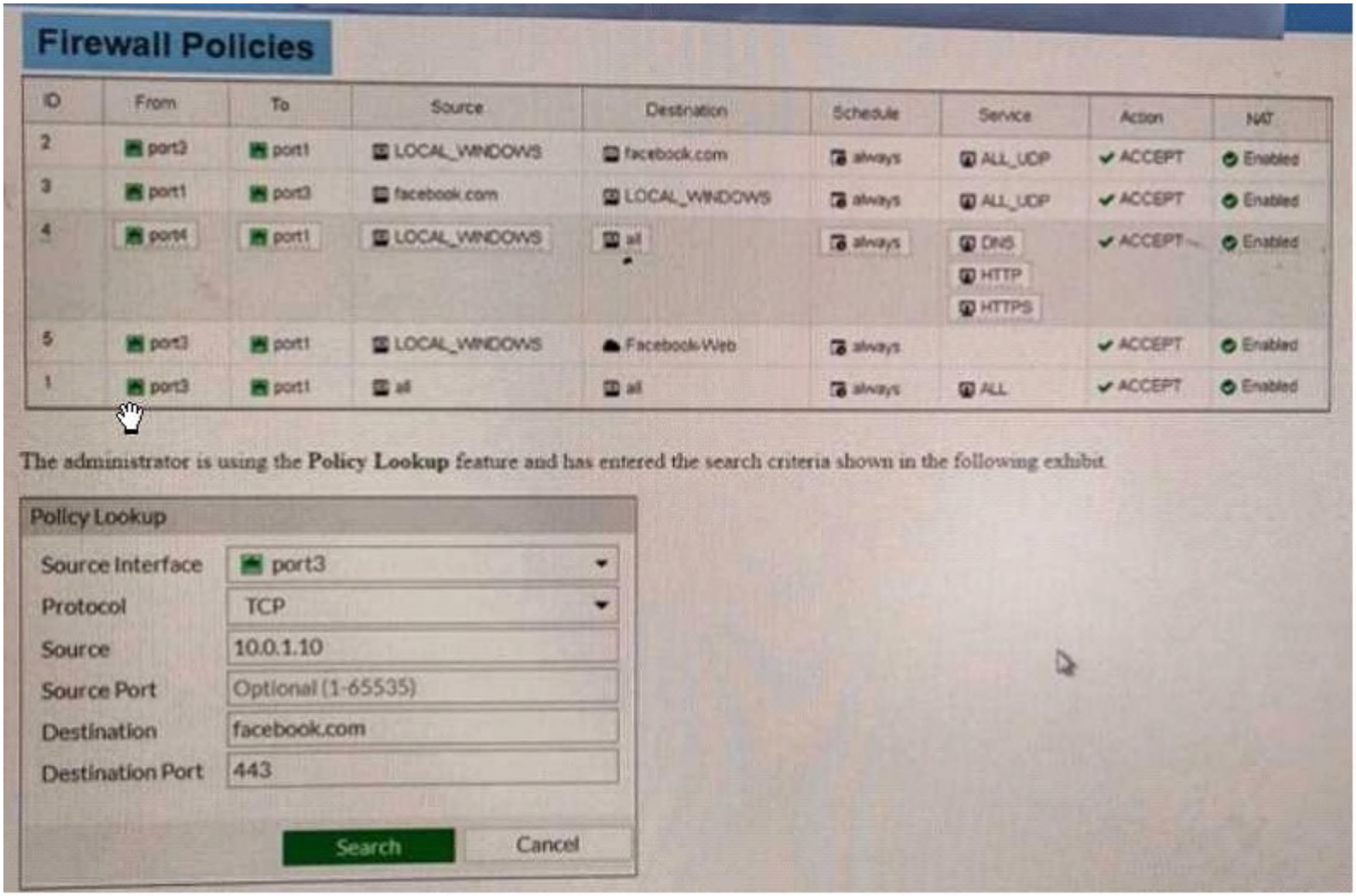
A. Deep-inspection must be enabled for FortiGate to fully scan FTP traffic.
B. FortiGate needs to be operating in flow-based inspection mode in order to scan FTP traffic.
C. The FortiSandbox signature database is required to successfully scan FTP traffic.
D. The proxy options profile needs to scan FTP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

Answer: D
Explanation/Reference:

QUESTION 20

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

Answer: B
Explanation/Reference:

QUESTION 21

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.

Answer: CDE
Explanation/Reference:

QUESTION 22

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.

Answer: AD
Explanation/Reference:

QUESTION 23

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

Answer: A
Explanation/Reference:

QUESTION 24

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.

Answer: D
Explanation/Reference:

QUESTION 25

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.

Answer: B
Explanation/Reference:

QUESTION 26

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.
Winch topology should be used to satisfy all of the requirements?

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

Answer: C
Explanation/Reference:

QUESTION 27

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.

Answer: A
Explanation/Reference:

QUESTION 28

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.

Answer: D
Explanation/Reference:

QUESTION 29

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.

Answer: AD
Explanation/Reference:

QUESTION 30

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.

Answer: ABC
Explanation/Reference:

QUESTION 31

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

Answer: A
Explanation/Reference:

QUESTION 32

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

Answer: A
Explanation/Reference:

QUESTION 33

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

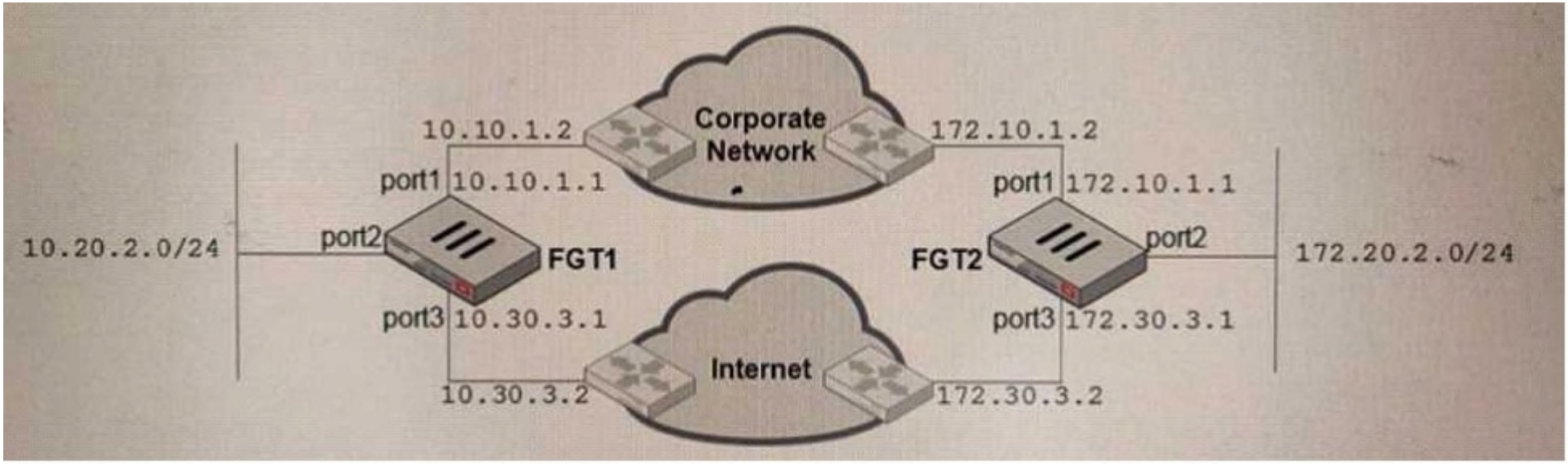
Which of the following statement about the output is true?

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

Answer: A
Explanation/Reference:

QUESTION 34

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]

Answer: AB
Explanation/Reference:

QUESTION 35

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

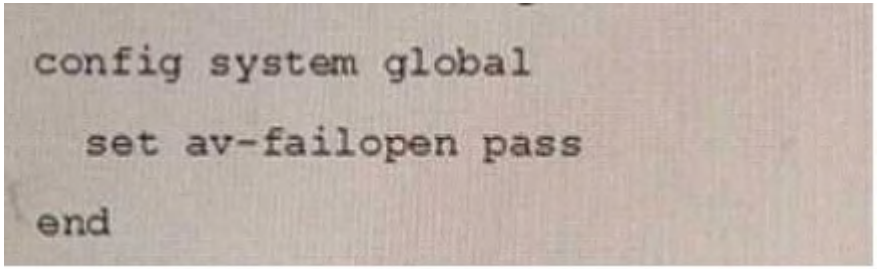
A. hourly
B. real tune

C. on-demand
D. store-and-upload

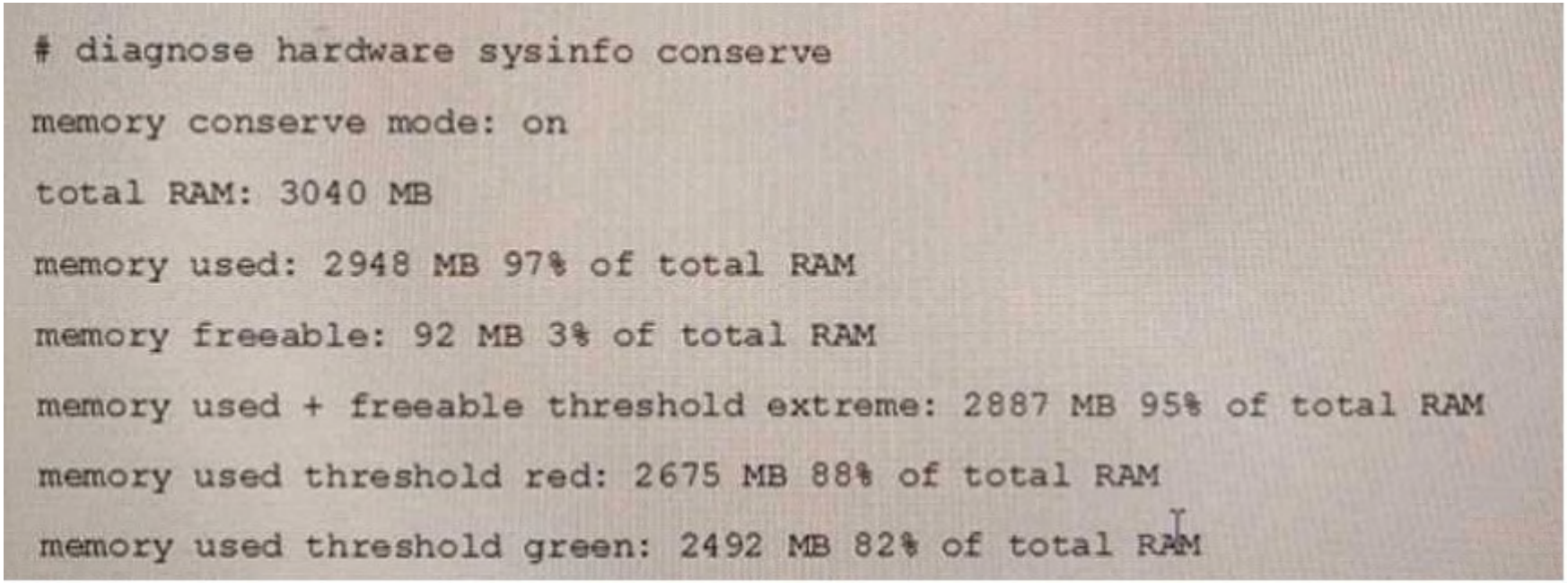
Answer: BD
Explanation/Reference:

QUESTION 36

Examine this FortiGate configuration:



Examine the output of the following debug command:



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.

Answer: C
Explanation/Reference:

QUESTION 37

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.

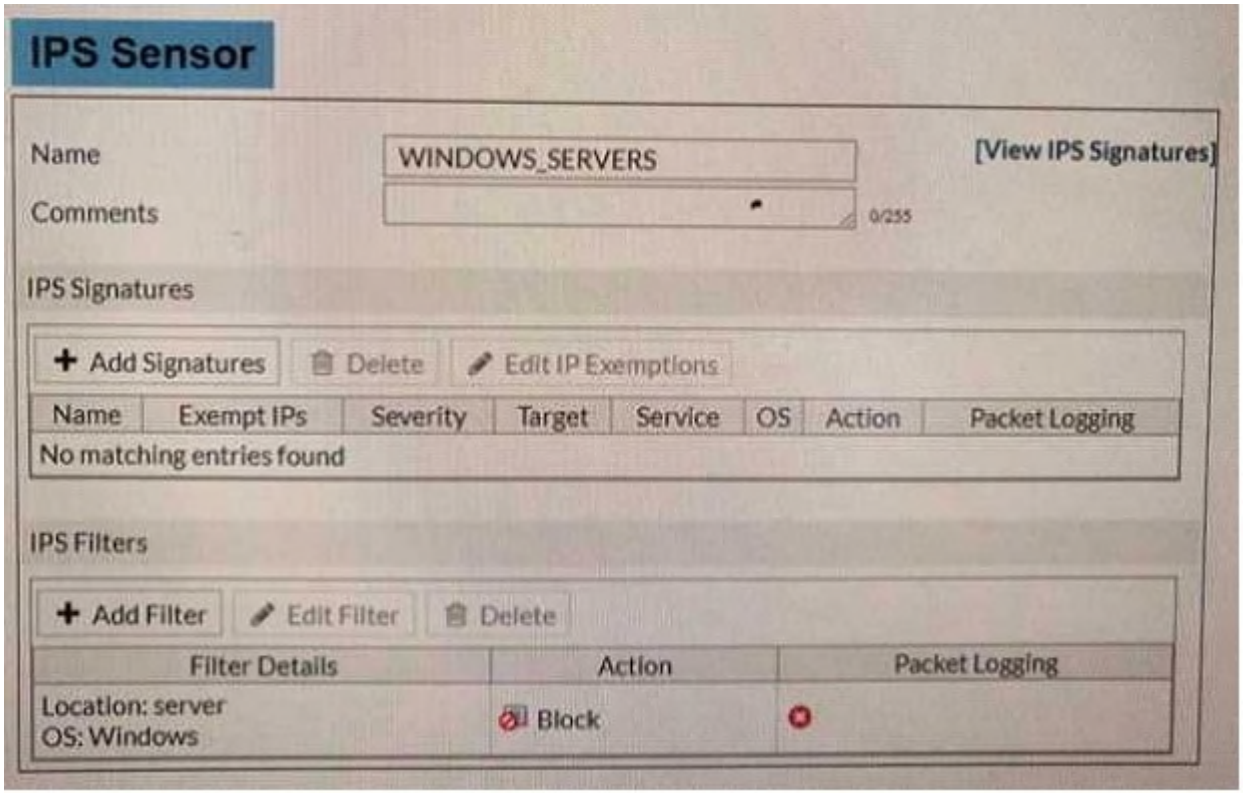
```
proxy.<local-domain>.wpad
```

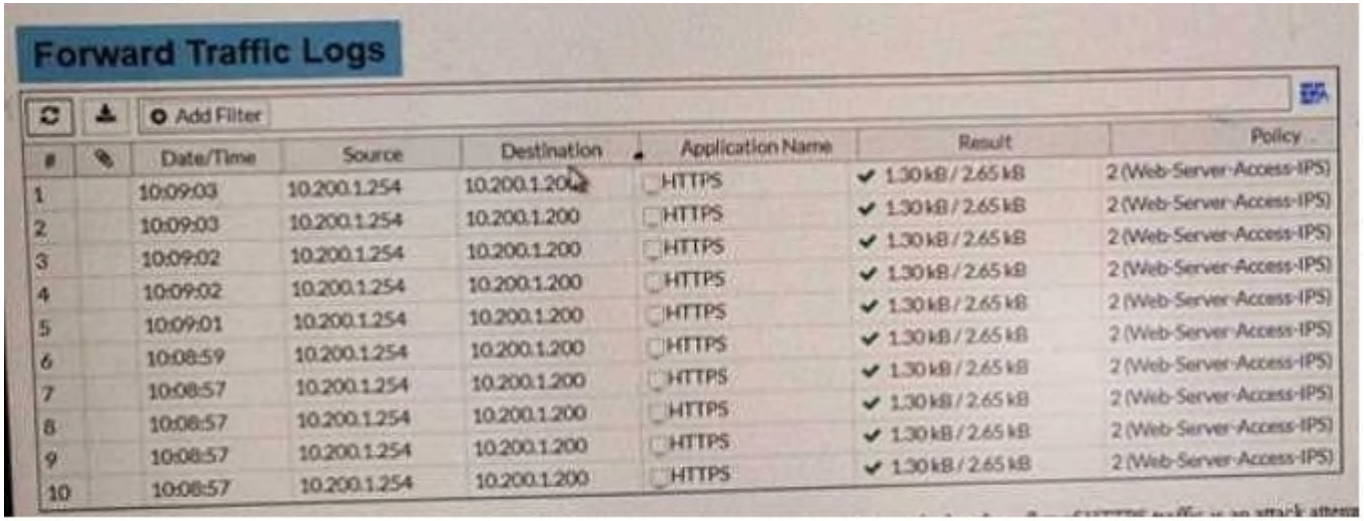
E. Option A
F. Option B
G. Option C
H. Option D

Answer: C
Explanation/Reference:

QUESTION 38

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.

Answer: E
Explanation/Reference:

QUESTION 39

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

Answer: ACE
Explanation/Reference:

QUESTION 40

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.

Answer: A
Explanation/Reference:

QUESTION 41

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.

Answer: AD
Explanation/Reference:

QUESTION 42

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.

Answer: BD
Explanation/Reference:

QUESTION 43

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.

Answer: AC
Explanation/Reference:

QUESTION 44

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.

Answer: D
Explanation/Reference:

QUESTION 45

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

Answer: C
Explanation/Reference:

QUESTION 46

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.

Answer: BD
Explanation/Reference:

QUESTION 47

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

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

Answer: A
Explanation/Reference:

QUESTION 48

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.

Answer: D
Explanation/Reference:

QUESTION 49

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

Answer: C
Explanation/Reference:

QUESTION 50

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.

Answer: D
Explanation/Reference:

QUESTION 51

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

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

Answer: CD
Explanation/Reference:

QUESTION 52

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.

Answer: A
Explanation/Reference:

QUESTION 53

Which statement regarding the firewall policy authentication timeout is true?

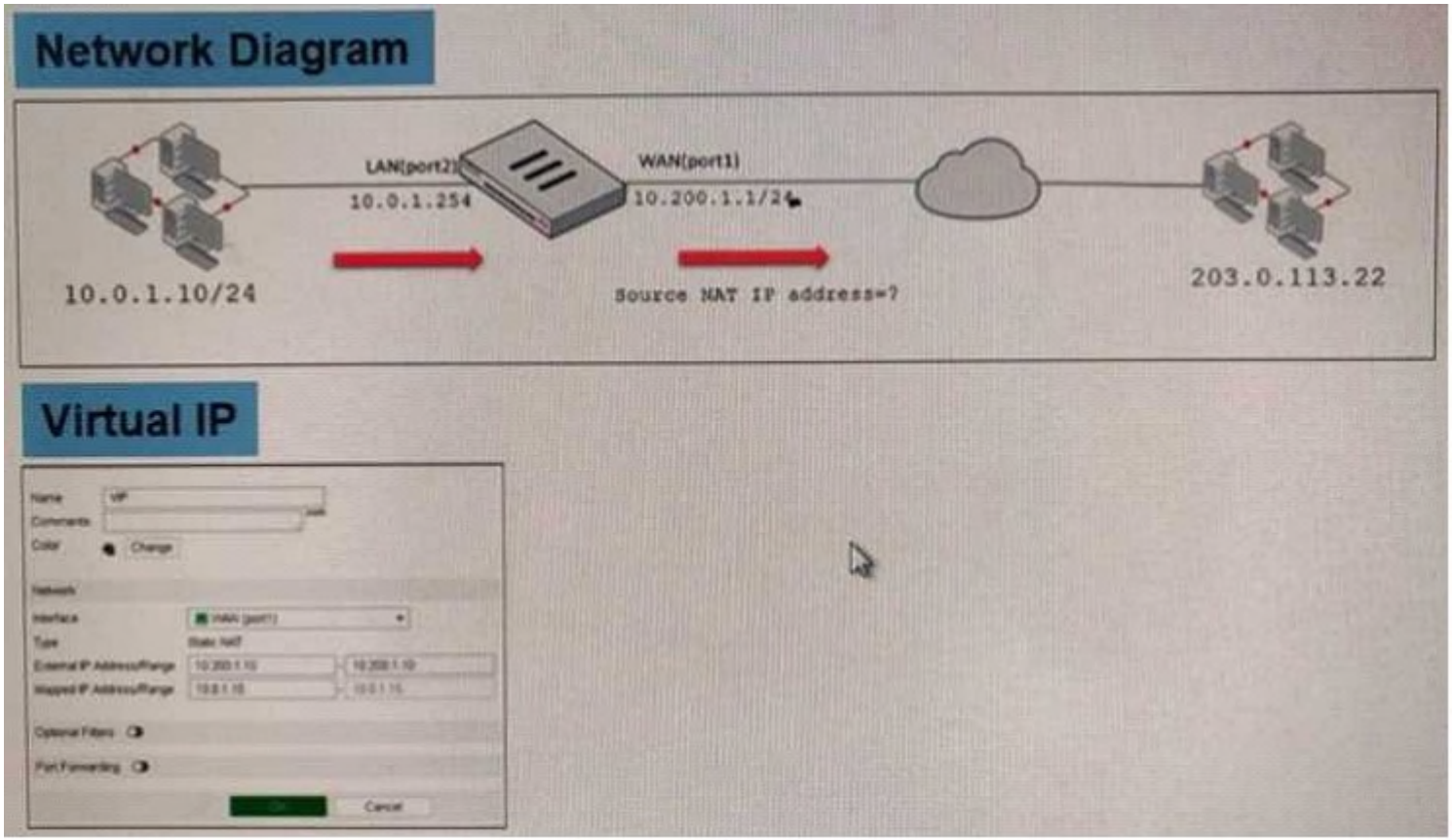
A. It is an idle timeout. The FortiGate considers a user to be "idle" if it does not see any packets coming from the user's source IP.
B. It is a hard timeout. The FortiGate removes the temporary policy for a user's source IP address after this timer has expired.
C. It is an idle timeout. The FortiGate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

Answer: A
Explanation/Reference:

QUESTION 54

Examine the Exhibit, which contains a virtual IP and firewall policy configuration.



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 top firewall policy has NAT enabled using outgoing interface address. The second firewall policy configured with a virtual IP (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. 10.200.1.1
B. 10.0.1.254
C. Any available IP address in the WAN(port1) subnet 10.200.1.0/24
D. 10.200.1.10

Answer: D
Explanation/Reference:

QUESTION 55

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

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

Answer: ACE
Explanation/Reference:

QUESTION 56

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.

Answer: D
Explanation/Reference:

QUESTION 57

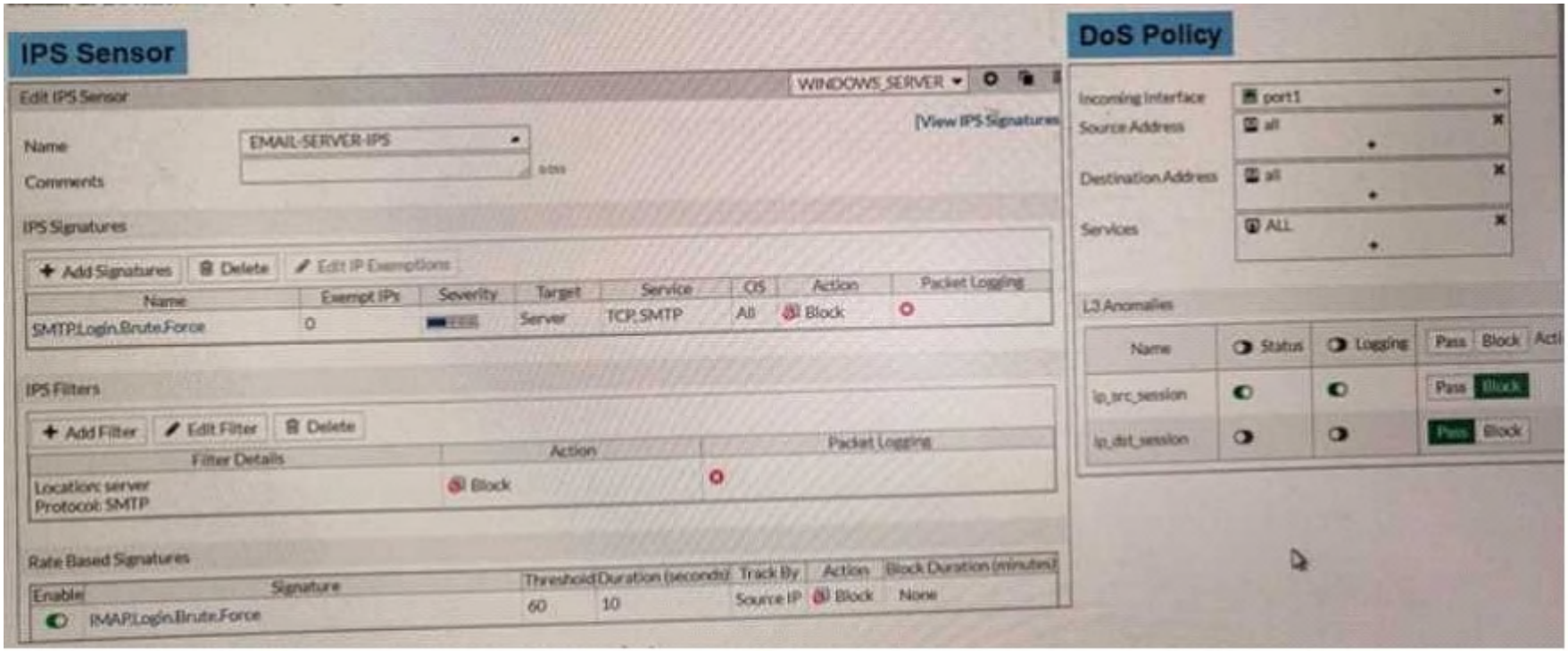
Which of the following are valid actions for FortiGuard category based filter in a web filter profile ui proxy-based inspection mode? (Choose two.)

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

Answer: AC
Explanation/Reference:

QUESTION 58

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

Answer: B
Explanation/Reference:

QUESTION 59

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

Answer: D
Explanation/Reference:

QUESTION 60

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

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

Answer: AD
Explanation/Reference:

QUESTION 61

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.

Answer: C
Explanation/Reference:

QUESTION 62

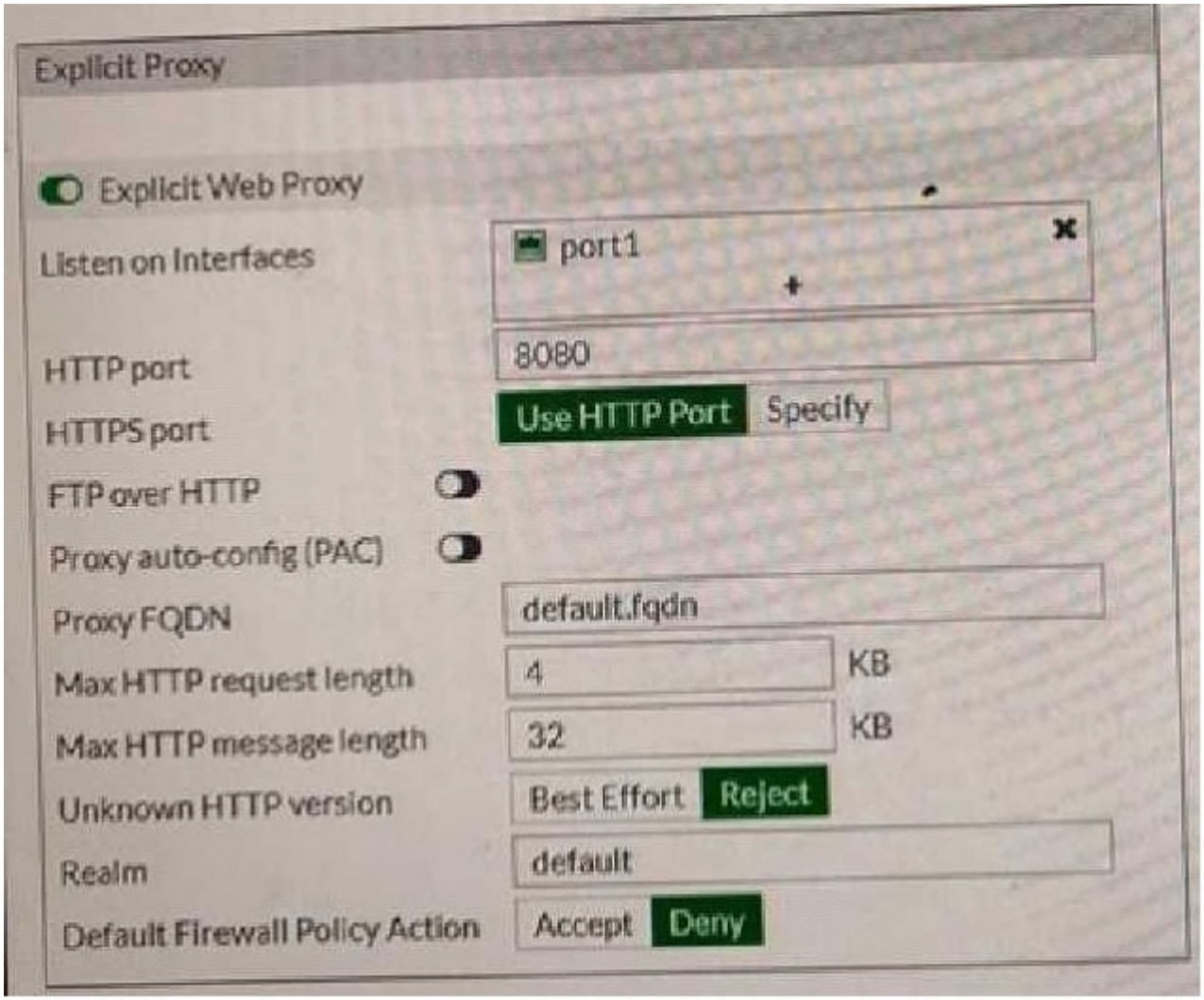
If the Services field is configured in a Virtual IP (VIP), which of the following statements is true when central NAT is used?

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.

Answer: A
Explanation/Reference:

QUESTION 63

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?

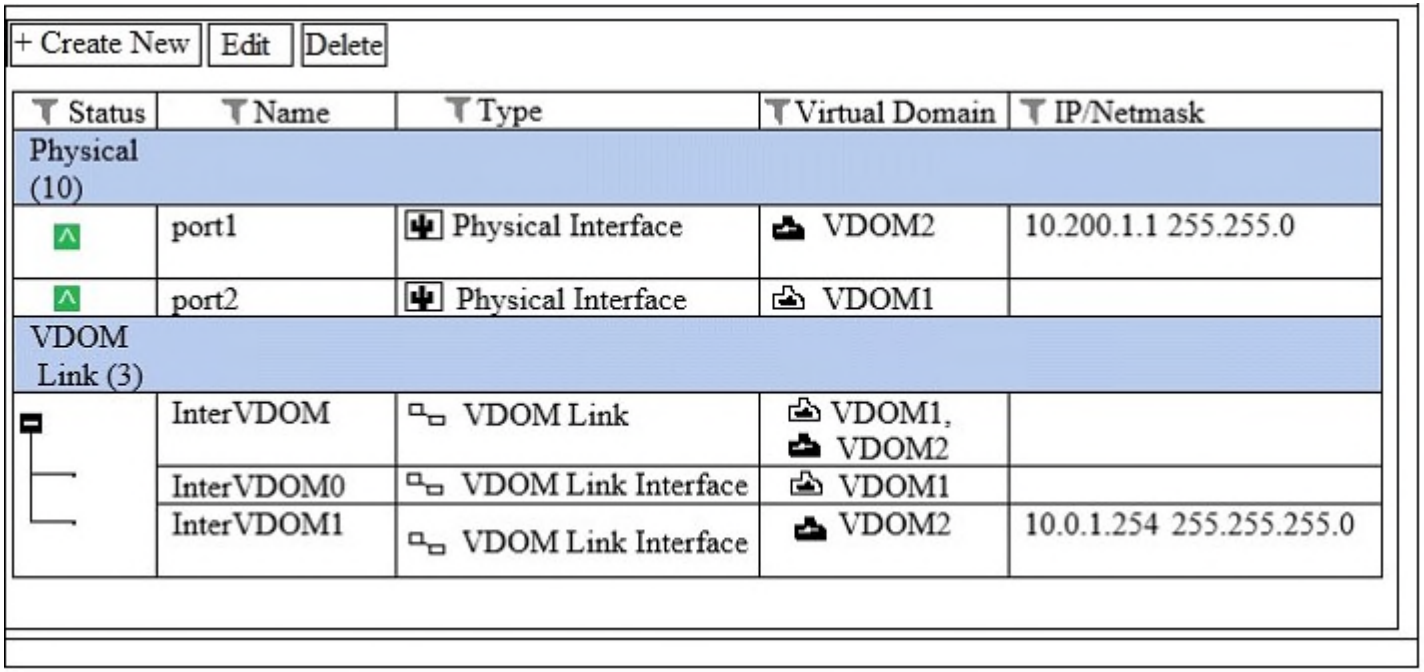
A. `host 10.0.0.50 and port 80'
B. `host 192.168.0.1 and port 80'
C. `host 192.168.0.2 and port 8080'

D. `host 10.0.50.1 and port 8080'

Answer: B
Explanation/Reference:

QUESTION 64

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.)

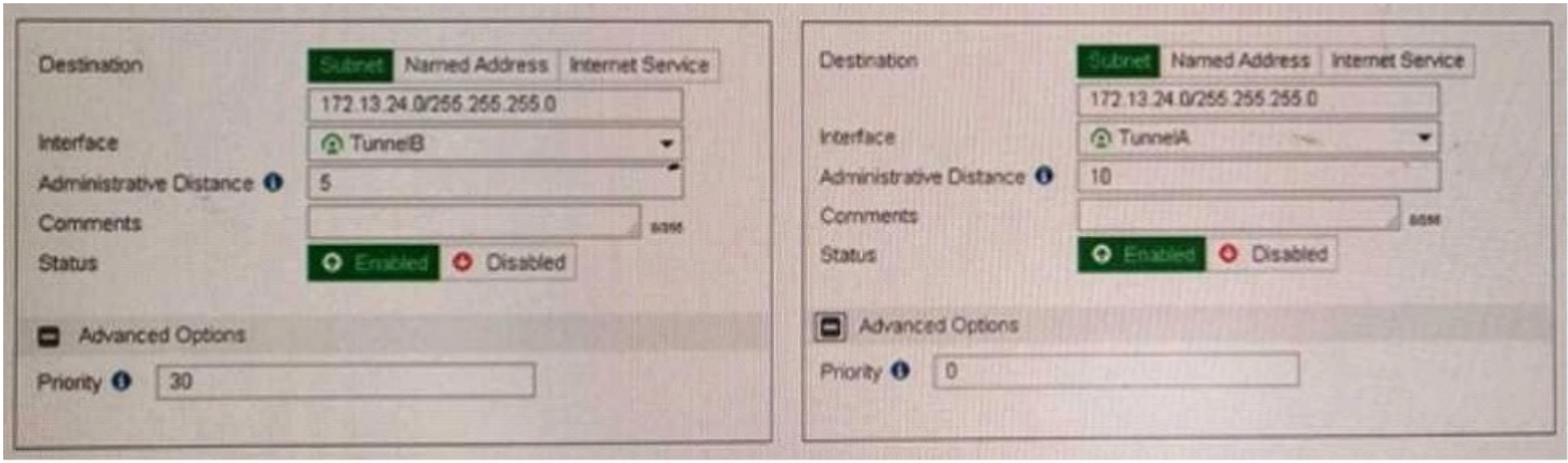
A. A static or dynamic route in VDOM2 with the subnet 10.0.1.0/24 as the destination.

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.

Answer: AC
Explanation/Reference:

QUESTION 65

View the exhibit.



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

A. This is a redundant IPsec setup.
B. The TunnelB route is the primary one for searching the remote site. The TunnelA route is used only if the TunnelB VPN is down.
C. This setup requires at least two firewall policies with action set to IPsec.

D. Dead peer detection must be disabled to support this type of IPsec setup.

Answer: AB
Explanation/Reference:

QUESTION 66

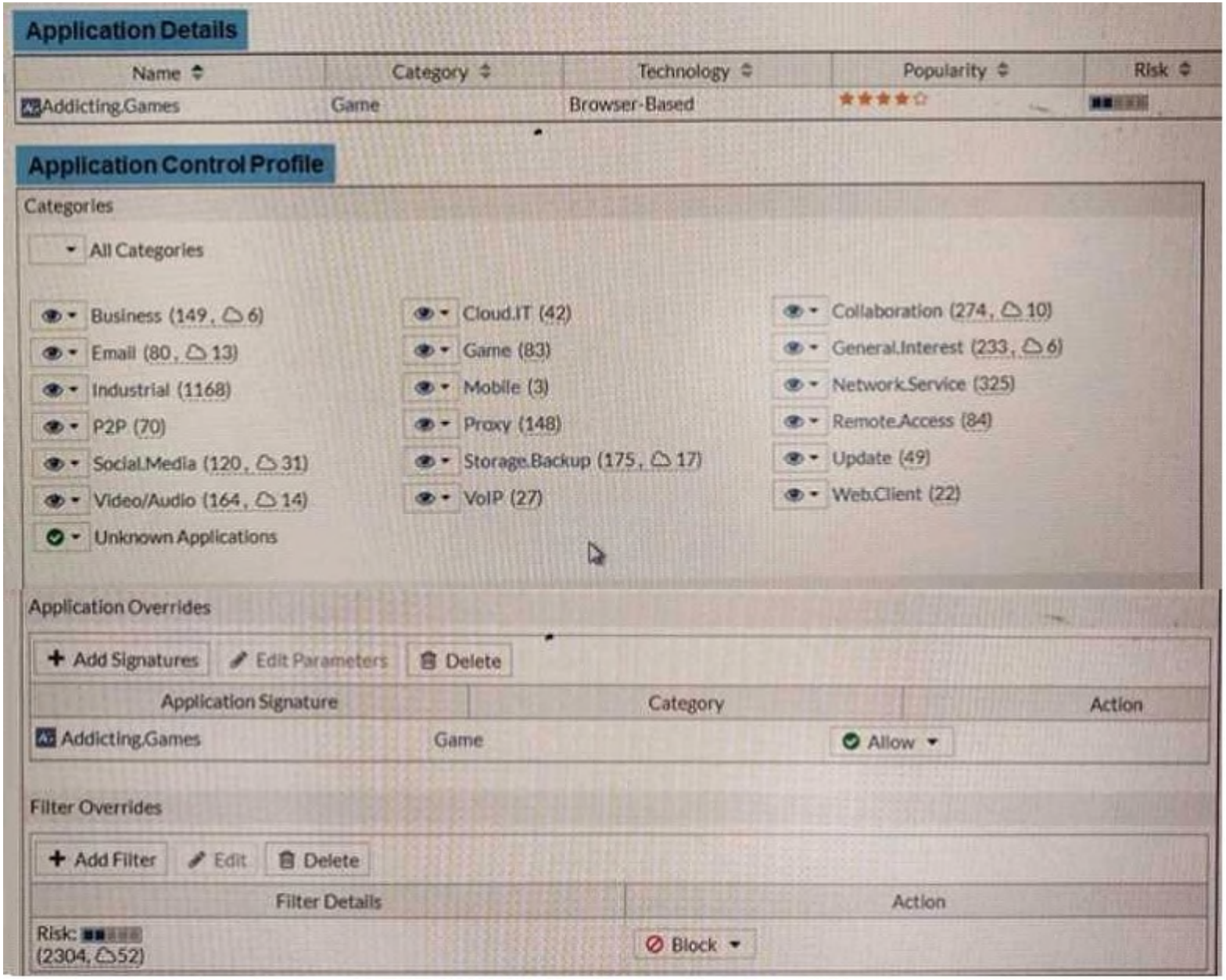
What criteria does FortiGate use to look for a matching firewall policy to process traffic? (Choose two.)

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.

Answer: BC
Explanation/Reference:

QUESTION 67

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.

Answer: A
Explanation/Reference:

QUESTION 68

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

Answer: BD
Explanation/Reference:

QUESTION 69

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.

Answer: CD
Explanation/Reference:

QUESTION 70

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

Answer: A
Explanation/Reference: