

NSE4_FGT-6.2.VCEplus.premium.exam.70q

Number: NSE4_FGT-6.2

Passing Score: 800

Time Limit: 120 min

File Version: 1.0



Website: <https://vceplus.com>

VCE to PDF Converter: <https://vceplus.com/vce-to-pdf/>

Facebook: <https://www.facebook.com/VCE.For.All.VN/>

Twitter : https://twitter.com/VCE_Plus

NSE4_FGT-6.2

Fortinet NSE 4 - FortiOS 6.2



Exam A

QUESTION 1

Examine the FortiGate configuration:

```
config user settings
    set auth-on-demand implicitly
end
```

What will happen to unauthenticated users when an active authentication policy is followed by a fall through policy without authentication?

- A. The user must log in again to authenticate.
- B. The user will be denied access to resources without authentication.
- C. The user will not be prompted for authentication.
- D. User authentication happens at an interface level.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://kb.fortinet.com/kb/documentLink.do?externalID=FD46875>

QUESTION 2 Which downstream FortiGate VDOM is used to join the Security Fabric when split-task VDOM is enabled on all FortiGate devices?

- A. FG-traffic VDOM B. Root VDOM
- C. Customer VDOM
- D. Global VDOM



Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://docs.fortinet.com/document/fortigate/6.2.0/new-features/287377/split-task-vdom-support>

QUESTION 3

In an HA cluster operating in active-active mode, which path is taken by the SYN packet of an HTTP session that is offloaded to a secondary FortiGate?

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 4 Which two statements about antivirus scanning mode are true?

(Choose two.)

- A. In proxy-based inspection mode, antivirus buffers the whole file for scanning, before sending it to the client.
- B. In full scan flow-based inspection mode, FortiGate buffers the file, but also simultaneously transmits it to the client.

- C. In proxy-based inspection mode, files bigger than the buffer size are scanned.
- D. In quick scan mode, you can configure antivirus profiles to use any of the available antivirus signature databases.

Correct Answer: AB

Section: (none)

Explanation

Explanation/Reference:

QUESTION 5 The FSSO collector agent set to advanced access mode for the Windows Active Directory uses which convention?

- A. LDAP
- B. Windows
- C. RSSO
- D. NTLM

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 6 Which two statements about virtual domains (VDOMs) are true?
(Choose two.)

- A. Transparent mode and NAT mode VDOMs cannot be combined on the same FortiGate.
- B. Each VDOM can be configured with different system hostnames.
- C. Different VLAN subinterfaces 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 7 What three FortiGate components are tested during the hardware test?
(Choose three.)

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

Correct Answer: ADE

Section: (none)

Explanation

Explanation/Reference:

QUESTION 8

A team manager has decided that, while some members of the team need access to a particular website, the majority of the team does not.

Which configuration option is the most effective way to support this request?

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 9

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" hostn
ame="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 10

When using WPAD DNS method, which 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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 11 Consider a new IPsec deployment with the following criteria:

- All satellite offices must connect to the two HQ sites.
- The satellite offices do not need to communicate directly with other satellite offices.
- Backup VPN is not required.
- The design should minimize the number of tunnels being configured.

Which topology should you use to satisfy all of the requirements?

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 12 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: AB

Section: (none)

Explanation

Explanation/Reference:

QUESTION 13

Refer to the exhibit.

You are configuring the root FortiGate to implement the Security Fabric. You are configuring port10 to communicate with a downstream FortiGate. The exhibit shows the default **Edit Interface**.

Edit Interface

Interface Name
port10(00:0C:29:0F:A9:F9)

Alias

Link Status
Up

Type
Physical Interface

Tags

Role
Undefined
Add Tag Category

Address

Addressing mode
Manual DHCP One-Arm Sniffer

IP/Network Mask

Administrative Access

IPv4
☐ HTTPS ☐ HTTP ☐ PING ☐ FMG-Access ☐ CAPWAP ☐ SSH ☐ SNMP ☐ FTM ☐ RADIUS Accounting ☐ FortiTelemetry

Receive LLDP
Use VDOM Setting Enable Disable

Transmit LLDP
Use VDOM Setting Enable Disable

☐ DHCP Server

Networked Devices

Device Detection



When configuring the root FortiGate to communicate with a downstream FortiGate, which two settings must you configure? (Choose two.)

- A. Enable **Device Detection**
- B. **Administrative Access: FortiTelemetry.**
- C. **IP/Network Mask.**
- D. **Role: Security Fabric.**

Correct Answer: BC

Section: (none)

Explanation

Explanation/Reference:

QUESTION 14 Which two statements about NTLM authentication are correct? (Choose two.)

- A. It requires DC agents on every domain controller when used in multidomain environments.
- B. It is useful when users log in to DCs that are not monitored by a collector agent.

- C. It requires NTLM-enabled web browsers.
- D. It takes over as the primary authentication method when configured alongside FSSO.

Correct Answer: BC

Section: (none)

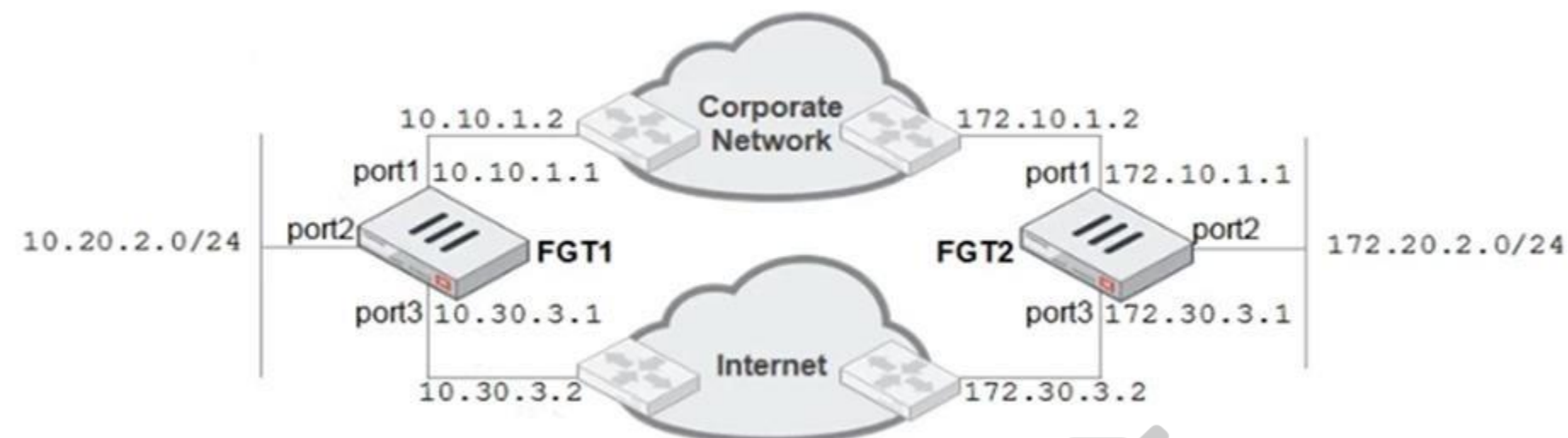
Explanation

Explanation/Reference:

Reference: <https://www.fortinetguru.com/2016/07/configuring-authenticated-access/12/>

QUESTION 15

Refer to the exhibit.



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. Given the network diagram shown in the exhibit, which two 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 10.30.3.2, port3 [5/0]
- C. 172.20.2.0/24 [25/0] via 10.10.1.2, port1 [5/0]
- D. 172.20.2.0/24 [1/150] via 10.30.3.2, port3 [10/0]

Correct Answer: BC

Section: (none)

Explanation

Explanation/Reference:

QUESTION 16 On a FortiGate with a hard disk, how frequently can you upload logs to FortiAnalyzer or FortiManager? (Choose two.)

- A. On-demand
- B. Hourly
- C. Every 5 minutes
- D. In real time

Correct Answer: CD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 17

Refer to the exhibit.

```
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
```

Given the partial output of an IKE real-time debug shown in the exhibit, which 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 18 An administrator needs to create an SSL-VPN connection for accessing an internal server using the bookmark, Port Forward.

Which step must the administrator take to successfully achieve 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 to 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 19 Which two static routes are not maintained in the routing table? (Choose two.)

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

Correct Answer: CD

Section: (none)

Explanation

Explanation/Reference:

Reference: https://help.fortinet.com/fadc/4-8-0/olh/Content/FortiADC/handbook/routing_static.htm

QUESTION 20 An administrator wants to configure a FortiGate as a DNS server. FortiGate must use a DNS database first, and then relay all irresolvable queries to an external DNS server. Which DNS method must you use?

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

- A. Creating an SD-WAN route for individual member interfaces
- B. Creating an SD-WAN rule to route traffic based on link latency
- C. Creating a static route with a named address object
- D. Creating a static route with an Internet services object

Correct Answer: BD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 22

Refer to the exhibits.

Edit AntiVirus Profile

Name

Comments

29/255

Scan Mode

Quick
Full

Detect Viruses

Block
Monitor

Inspected Protocols

HTTP

☒

SMTP

☒

POP3

☒

IMAP

☒

MAPI

☐

FTP

☒

CIFS

☐

APT Protection Options

Content Disarm and Reconstruction

☐

Treat Windows Executables in Email Attachments as Viruses

☒

Include Mobile Malware Protection

☒

Virus Outbreak Prevention

Use FortiGuard Outbreak Prevention Database

☐

Use External Malware Block List

☐

Name

Comments 21/255

Log Oversized Files ☐

RPC over HTTP ☐

Protocol Port Mapping

HTTP	<input checked="" type="checkbox"/>	Any	<input type="button" value="Specify"/>	<input type="text" value="80"/>
SMTP	<input checked="" type="checkbox"/>	Any	<input type="button" value="Specify"/>	<input type="text" value="25"/>
POP3	<input checked="" type="checkbox"/>	Any	<input type="button" value="Specify"/>	<input type="text" value="110"/>
IMAP	<input checked="" type="checkbox"/>	Any	<input type="button" value="Specify"/>	<input type="text" value="143"/>
FTP	<input checked="" type="checkbox"/>	Any	<input type="button" value="Specify"/>	<input type="text" value="21"/>
NNTP	<input checked="" type="checkbox"/>	Any	<input type="button" value="Specify"/>	<input type="text" value="119"/>
MAPI	<input checked="" type="checkbox"/>	<input type="text" value="135"/>		
DNS	<input checked="" type="checkbox"/>	<input type="text" value="53"/>		

Common Options

Comfort Clients ☐

Block Oversized File/Email ☐

Web Options

Chunked Bypass ☐

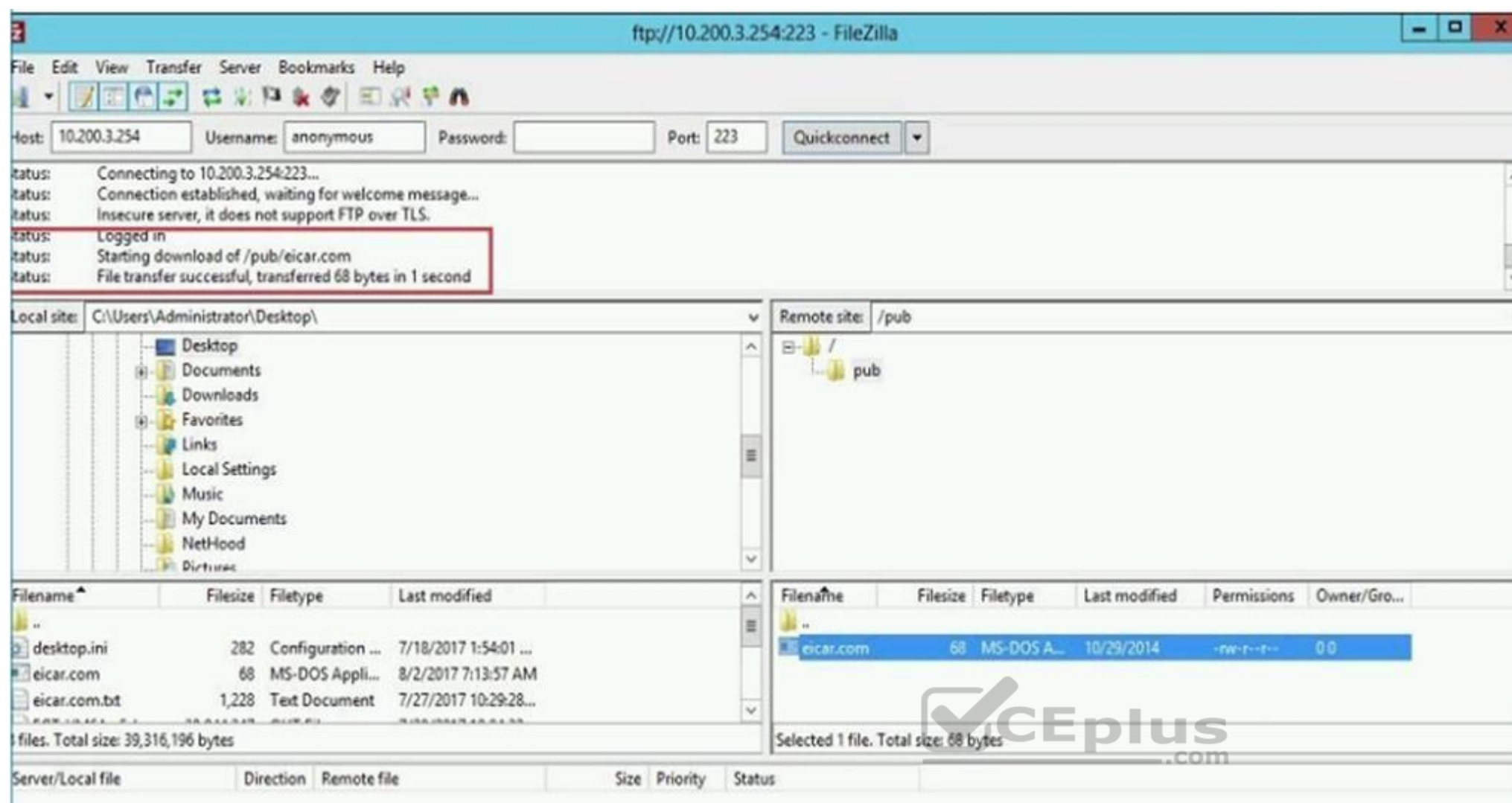
Add Fortinet Bar ☐

HTTP Policy Redirect ☐

Email Options

Allow Fragmented Messages ☒

Append Signature (SMTP) ☐



Given the antivirus profile and file transfer output shown in the exhibits, why is FortiGate *not* blocking the eicar.com file over FTP download?

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 23

Refer to the exhibit.

Address Object

Name	Type	Details
+ Address 14		
all	Subnet	0.0.0.0/0
facebook.com	FQDN	facebook.com
LOCAL_WINDOWS	Subnet	10.0.1.10/32

Internet Service Object

Name	Reputation	Direction	Number of entries
+ Internet Service Database 1/1457			
Facebook.Web	4	Destination	4.017

Firewall Policies

ID	From	To	Source	Destination	Schedule	Service	Action	NAT
2	port3	port1	LOCAL_WINDOWS	facebook.com	always	All_UDP	Accept	Enabled
3	port1	port3	facebook.com	LOCAL_WINDOWS	always	All_UDP	Accept	Enabled
4	port4	port1	LOCAL_WINDOWS	all	always	DNS HTTP HTTPS	Accept	Enabled
5	port3	port1	LOCAL_WINDOWS	Facebook.Web	always		Accept	Enabled
1	port3	port1	all	all	always	All	Accept	Enabled

Policy Lookup

Source Interface	port3
Protocol	TCP
Source	10.0.1.10
Source Port	Optional (1-65535)
Destination	facebook.com
Destination Port	443

Search

Cancel

The exhibits show the firewall policies and the objects used in the firewall policies. The administrator is using the **Policy Lookup** feature and has entered the search criteria shown in the exhibit.

Based on the input criteria, which of the following will be highlighted?

- A. The policy with ID 1
- B. The policy with ID 5
- C. The policies with ID 2 and 3

D. The policy with ID 4

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 24

Refer to the exhibit.

```
id=2 line=4677 msg= "vd-root received a packet (proto=6, 66.171.121.44:80 ->10.200.1.1:49886) from port1  
flag [S.], seq 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"
```

The exhibit shows the output from a debug flow.

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

- A. The packet was allowed by the firewall policy with the ID 00007fc0.
- B. The source IP address of the packet was translated to 10.0.1.10.
- C. FortiGate received a TCP SYN/ACK packet.
- D. FortiGate routed the packet through port3.

Correct Answer: CD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 25 What is required to create an inter-VDOM link between two VDOMs?

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 26 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 for 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: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 27

Refer to the exhibit.

Status	Name	Type	Virtual Domain	IP/Netmask
Physical (10)				
	port1	 Physical Interface	 VDOM2	10.200.1.1 255.255.0
	port2	 Physical Interface	 VDOM1	
VDOM Link (3)				
	InterVDOM	 VDOM Link	 VDOM1,  VDOM2	
	InterVDOM0	 VDOM Link Interface	 VDOM1	
	InterVDOM1	 VDOM Link Interface	 VDOM2	10.0.1.254 255.255.255.0

The exhibit shows network configurations. VDOM1 is operating in transparent mode. VDOM2 is operating in NAT 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.

Which two options must be included 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: CD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 28 NGFW mode allows policy-based configuration for most inspection rules.

Which security profile configuration does not change when you enable policy-based inspection?

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

Correct Answer: D
Section: (none)
Explanation
Explanation/Reference:

QUESTION 29 Which two statements about the firmware upgrade process on an active-active HA cluster are true? (Choose two.)

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

Correct Answer: BC

Section: (none)

Explanation

Explanation/Reference:

Reference: https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-high-availability-52/HA_operatingFirmUpgd.htm

QUESTION 30 Which statement about 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 31 Which two statements correctly describe how FortiGate performs route lookup, when searching for a suitable gateway? (Choose two.)

- A. Lookup is done on the first packet from the session originator
- B. Lookup is done on the last packet sent from the responder
- C. Lookup is done on every packet, regardless of direction
- D. Lookup is done on the first reply packet from the responder

Correct Answer: AD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 32 A FortiGate is operating in NAT mode and configured with two virtual LAN (VLAN) subinterfaces added to the physical interface.

In this scenario, which statement about the VLAN IDs is true?

- 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

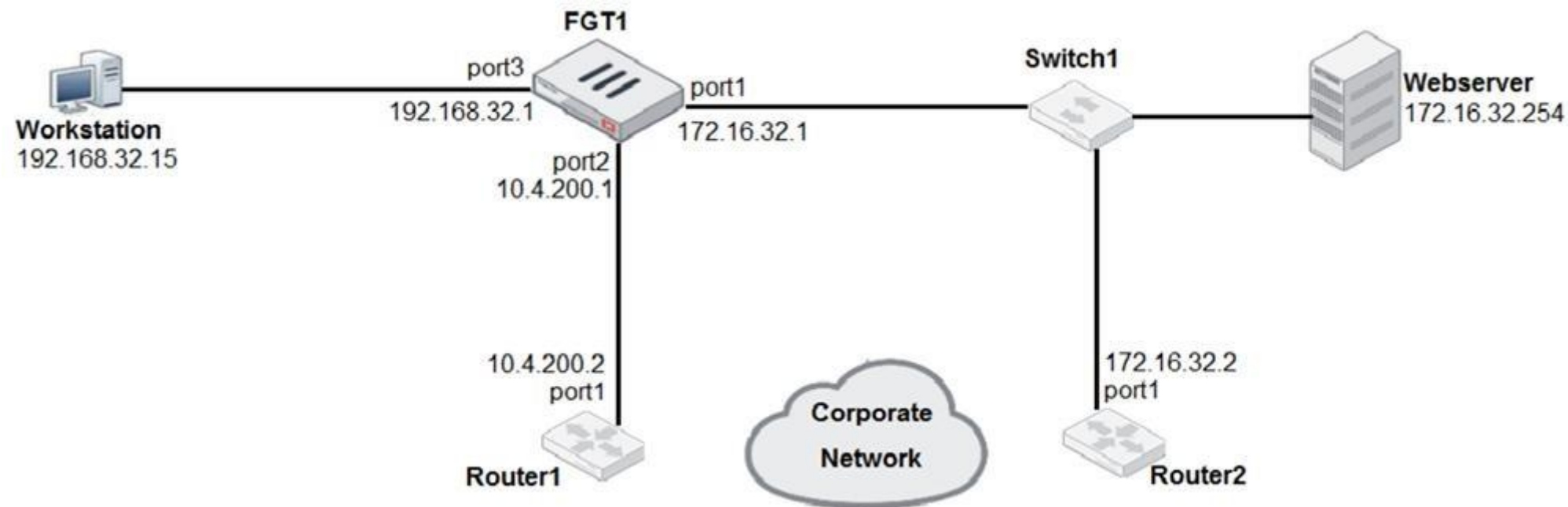
Section: (none)

Explanation

Explanation/Reference:

QUESTION 33

Refer to the exhibit.



Given the network diagram shown in the exhibit, which route is the best candidate route for FGT1 to route traffic from the workstation to the webserver?

- A. 172.16.32.0/24 is directly connected, port1
- B. 172.16.0.0/16 [50/0] via 10.4.200.2, port2 [5/0]
- C. 10.4.200.0/30 is directly connected, port2
- D. 0.0.0.0/0 [20/0] via 10.4.200.2, port2



Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 34 Which two statements about central NAT are true? (Choose two.)

- A. SNAT using central NAT does not require a central SNAT policy.
- B. Central NAT can be enabled or disabled from the CLI only.
- C. IP pool references must be removed from existing firewall policies, before enabling central NAT.
- D. DNAT using central NAT requires a VIP object as the destination address in a firewall policy.

Correct Answer: BC

Section: (none)

Explanation

Explanation/Reference:

QUESTION 35 Which condition must be met in order for a web browser to trust a web server certificate signed by a third-party CA?

- A. The private key of the CA certificate that is signed the browser certificate must be installed on the browser.

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 36
Refer to the exhibit.

Application Details

Name : Addicting Games

Category : Game

Technology : Browser-Based

Popularity : ☆☆☆☆

Application Control Profile

Categories

All Categories

Business (144, 6)

Collaboration (268, 10)

Game (87)

Mobile (3)

P2P (63)

Remote.Access (84)

Storage.Backup (173, 17)

Video/Audio (160, 14)

Web.Client (23)

Cloud.IT (43)

Email (80, 12)

General.Interest (231, 7)

Network.Service (329)

Proxy (166)

Social.Media (121, 31)

Update (50)

VoIP (24)

Unknown Applications

Network Protocol Enforcement

Application and Filter Overrides

Create New

Edit

Delete

Priority	Details	Type	Action
1	Addicting Games	Application	Allow
2	RISK	Filter	Block

A user located behind the FortiGate device is trying to go to <http://www.addictinggames.com> (**Addicting.Games**). The exhibit shows the application details and application control profile.

Based on this configuration, which statement is true?

- A. **Addicting.Games** will be blocked, based on the **Filter Overrides** configuration.
- B. **Addicting.Games** will be allowed only if the **Filter Overrides** action is set to **Learn**.

- C. **Addicting.Games** will be allowed, based on the **Categories** configuration.
- D. **Addicting.Games** will be allowed, based on the **Application Overrides** configuration.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 37

Refer to the exhibit.

```
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
```

The exhibit shows a FortiGate configuration.

How does 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: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 38 Which statement about the IP authentication header (AH) used by IPsec is true?

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

Correct Answer: C

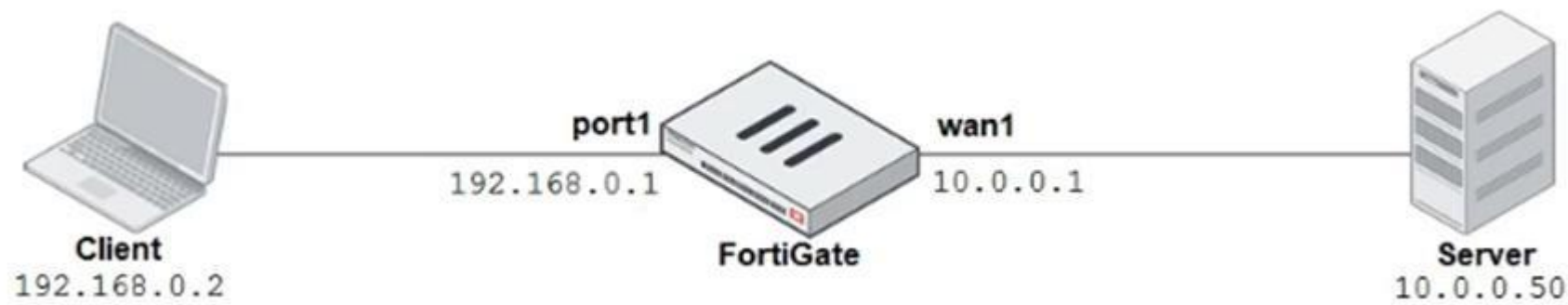
Section: (none)

Explanation

Explanation/Reference:

QUESTION 39

Refer to the exhibits.



Explicit Proxy

☒ Explicit Web Proxy

Listen on Interfaces

HTTP Port -

HTTPS Port

FTP over HTTP ☐

Proxy auto-config (PAC) ☐

Proxy FQDN

Max HTTP request length KB

Max HTTP message length KB

Unknown HTTP version

Realm

Default Firewall Policy Action



The exhibits show a network diagram and the explicit web proxy configuration.

In the command `diagnose sniffer packet`, what filter can you use to capture the traffic between the client and the explicit web proxy?

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 40 How do you format the FortiGate flash disk?

- A. Execute the CLI command `execute formatlogdisk`.
- B. Select the format boot device option from the BIOS menu.

- C. Load the hardware test (HQIP) image.
- D. Load a debug FortiOS image.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 41 If the **Services** field is configured in a Virtual IP (VIP), which statement is true when central NAT is used?

- A. The **Services** field prevents SNAT and DNAT from being combined in the same policy.
- B. The **Services** field is used when you need to bundle several VIPs into VIP groups.
- C. The **Services** field removes the requirement to create multiple VIPs for different services.
- D. The **Services** field prevents multiple sources of traffic from using multiple services to connect to a single computer.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 42 Which three types of traffic and attacks can be blocked by a web application firewall (WAF) profile? (Choose three.)

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



Correct Answer: ACE

Section: (none)

Explanation

Explanation/Reference:

Reference: https://help.fortinet.com/fweb/570/Content/FortiWeb/fortiweb-admin/web_protection.htm

QUESTION 43

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

- A. To generate logs
- B. To remove the NAT operation
- 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 44

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 FortiGate.
- B. Any web request sent to the 172.25.120.0/24 subnet is allowed to bypass the proxy.
- C. All requests not sent to fortinet.com or the 172.25.120.0/24 subnet, have to go through altproxy.corp.com: 8060.
- D. Any web request sent to fortinet.com is allowed to bypass the proxy.

Correct Answer: AD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 45 Which two statements correctly describe auto discovery VPN (ADVPN)? (Choose two.)

- A. IPSec tunnels are negotiated dynamically between spokes.
- B. ADVPN is supported only with IKEv2.
- C. It recommends the use of dynamic routing protocols, so that spokes can learn the routes to other 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 46

Refer to the exhibit.

Destination ⓘ	Subnet	Named Address	Internet Service
Interface	172.13.24.0/255.255.255.0 ▼		
Administrative Distance ⓘ	TunnelB ▼		
Comments	5		
Status	0/255		
<div style="display: flex; justify-content: space-around;"> Enabled Disabled </div>			
<div style="display: flex; justify-content: space-between; align-items: center;"> ⊞ Advanced Options </div>			
Priority ⓘ	30		

Destination ⓘ	Subnet	Named Address	Internet Service
Interface	172.13.24.0/255.255.255.0 ▼		
Administrative Distance ⓘ	TunnelA ▼		
Comments	10		
Status	0/255		
<div style="display: flex; justify-content: space-around;"> Enabled Disabled </div>			
<div style="display: flex; justify-content: space-between; align-items: center;"> ⊞ Advanced Options </div>			
Priority ⓘ	0		

Given to the static routes shown in the exhibit, which statements are correct? (Choose two.)

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

Correct Answer: AD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 47 To complete the final step of a Security Fabric configuration, an administrator must authorize all the devices on which device?

- A. FortiManager
- B. Root FortiGate
- C. FortiAnalyzer
- D. Downstream FortiGate

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 48 If the Issuer and Subject values are the same in a digital certificate, to which type of entity was the certificate issued?

- A. A subordinate CA
- B. A root CA
- C. A userD. A CRL

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 49

Examine the 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 50

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 are the two results of this configuration? (Choose two.)

- A. Device detection on all interfaces is enforced for 30 minutes.
- B. Denied users are blocked for 30 minutes.
- C. A session for denied traffic is created.
- D. The number of logs generated by denied traffic is reduced.

Correct Answer: CD

Section: (none)

Explanation



Explanation/Reference:

Reference: <https://kb.fortinet.com/kb/documentLink.do?externalID=FD46328>

QUESTION 51

Refer to the exhibit.

```
date=2017-08-31 time=12:50:06 logid=0316013057 type=utm subtype=webfilter eventtype=ftgd_blk
level=warning vd=root policyid=1 sessionid=149645 user="" srcip=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=dcmain cat=20 catdesc="Games" crscore=30 crlevel=high
```

The exhibit shows a web filtering log.

Which statement about the log message is true?

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 52 Which two statements about firewall policy NAT using the outgoing interface IP address with fixed port disabled are true?
(Choose two.)

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

Correct Answer: AB

Section: (none)

Explanation

Explanation/Reference:

QUESTION 53

Refer to the exhibit.

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

According to the certificate values shown in the exhibit, which type of entity was the certificate issued to?

- A. A user
- B. A root CA
- C. A bridge CA
- D. A subordinate

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 54

Which two actions are valid for a FortiGuard category-based filter, in a web filter profile, for a firewall policy in proxy-based inspection mode? (Choose two.)

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

Correct Answer: BC

Section: (none)

Explanation

Explanation/Reference:

QUESTION 55 Which two options are purposes of NAT traversal in IPsec? (Choose two.)

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

Correct Answer: BC

Section: (none)

Explanation

Explanation/Reference:

QUESTION 56 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 57

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

- A. It limits the scope of application control to scan traffic based on 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: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 58

An administrator is configuring an IPsec VPN between site A and site B. The **Remote Gateway** setting in both sites has been configured as **Static IP Address**. For site A, the local quick mode selector is 192.168.1.0/24 and the remote quick mode selector is 192.168.2.0/24.

Which subnet must the administrator configure for the local quick mode selector for site B?

- A. 192.168.1.0/24
- B. 192.168.0.0/8
- C. 192.168.2.0/24
- D. 192.168.3.0/24

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 59

Refer to the exhibits.

IPS Sensor

Edit IPS Sensor WINDOWS_SERVER [View IPS Signatures]

Name: EMAIL-SERVER-IPS

Comments:

IPS Signatures

Name	Exempt IPs	Severity	Target	Service	OS	Action	Packet Logging
SMTPLoginBruteForce		High	Server	TCP_SMT	All	Block	

IPS Filters

Filter Details	Action	Packet Logging
Location: server Protocol: SMTP	Block	

Rate Based Signatures

Enable	Signature	Threshold	Duration (seconds)	Track By	Action	Block Duration (minutes)
<input checked="" type="checkbox"/>	IMAPLoginBruteForce	60	10	Source IP	Block	None
<input type="checkbox"/>	DigumAsistent (SMTP TCP Connection Close G	5	1	Any	Block	None

Apply



DoS Policy

Incoming Interface: port1

Source Address: all

Destination Address: all

Services: ALL

L3 Anomalies

Name	Status	Logging	Pass	Block	Action	Threshold
ip_src_session	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Pass	Block		60
ip_dst_session	<input type="checkbox"/>	<input type="checkbox"/>	Pass	Block		5000

The exhibits show the IPS sensor and DoS policy configuration.

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

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 60 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 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 as a scheduled time
- D. Log downloads from the GUI are stored as LZ4 compressed files.

Correct Answer: AB

Section: (none)

Explanation

Explanation/Reference:



QUESTION 61

Refer to 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

Given the FortiGate interfaces shown in the exhibit, which two statements about the FortiGate interfaces configuration in the exhibit are true? (Choose two.)

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

Correct Answer: BC

Section: (none)

Explanation

Explanation/Reference:

QUESTION 62 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. The remote user's virtual IP address
- B. The public IP address of the FortiGate device
- C. The remote user's public IP address
- D. The internal IP address of the FortiGate device

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 63

An administrator observes that the `port1` interface *cannot* be configured with an IP address.

What are three possible reasons for this? (Choose three.)

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

Correct Answer: ABD

Section: (none)

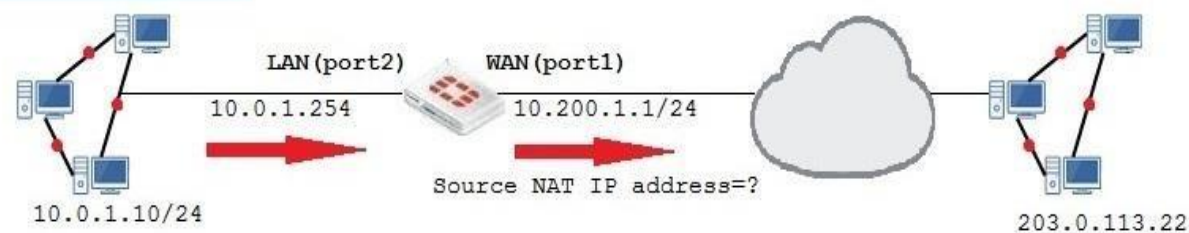
Explanation

Explanation/Reference:

QUESTION 64

Refer to the exhibits.

Network Diagram



Virtual IP

Name

Comments
0/255

Color
Change

Network

Interface

Type
Static NAT

External IP Address/Range
 -

Mapped IP Address/Range
 -

Optional Filters
☐

Port Forwarding
☐

OK Cancel

Firewall Policies

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

The exhibits contain a network diagram and 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 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 10.0.1.10/32?

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 65

Refer to the exhibit.

FortiGate Configuration

```
config system global

    set av-failopen pass

end
```

Debug command output

```
# 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
```



The exhibit shows FortiGate configuration and the output of the debug command.

Based on the diagnostic output, how is the FortiGate handling the traffic for new sessions that require proxy based inspection?

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 66 Which statement about SSL VPN settings for an SSL VPN portal is true?

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

Correct Answer: B

Section: (none)
Explanation

Explanation/Reference:

QUESTION 67

Refer to the exhibit.

<div><div>+ Create New</div><div> Edit</div><div> Clone</div><div> Delete</div></div>				
Destination	Gateway	Interface	Priority	Distance
172.20.168.0/24	172.25.176.1	port1	10	20
172.20.168.0/24	172.25.178.1	port2	20	20

The exhibit shows two static routes.

Which option accurately describes how FortiGate will handle these two routes to the same destination?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 68

Refer to the exhibit.



IPS Sensor

Name: **WINDOWS_SERVERS** [View IPS Signatures]

Comments: 0 / 255

IPS Signatures

+ Add Signatures Delete Edit IP Exemptions

Name	Exempt IPs	Severity	Target	Service	OS	Action	Packet Logging
No matching entries found							

IPS Filters

+ Add Filter Edit Filter Delete

Filter Details	Action	Packet Logging
Location:server OS:Windows	Block	

Apply

Forward Traffic Logs

Refresh Download Add Filter

#	Date/Time	Source	Destination	Application Name	Result	Policy
1	10:09:03	10.200.1.254	10.200.1.200	HTTPS	✓ 1.30kB/2.65 kB	2(Web-Server-Access-IPS)
2	10:09:03	10.200.1.254	10.200.1.200	HTTPS	✓ 1.30kB/2.65 kB	2(Web-Server-Access-IPS)
3	10:09:02	10.200.1.254	10.200.1.200	HTTPS	✓ 1.30kB/2.65 kB	2(Web-Server-Access-IPS)
4	10:09:02	10.200.1.254	10.200.1.200	HTTPS	✓ 1.30kB/2.65 kB	2(Web-Server-Access-IPS)
5	10:09:01	10.200.1.254	10.200.1.200	HTTPS	✓ 1.30kB/2.65 kB	2(Web-Server-Access-IPS)
6	10:08:59	10.200.1.254	10.200.1.200	HTTPS	✓ 1.30kB/2.65 kB	2(Web-Server-Access-IPS)
7	10:08:57	10.200.1.254	10.200.1.200	HTTPS	✓ 1.30kB/2.65 kB	2(Web-Server-Access-IPS)
8	10:08:57	10.200.1.254	10.200.1.200	HTTPS	✓ 1.30kB/2.65 kB	2(Web-Server-Access-IPS)
9	10:08:57	10.200.1.254	10.200.1.200	HTTPS	✓ 1.30kB/2.65 kB	2(Web-Server-Access-IPS)
10	10:08:57	10.200.1.254	10.200.1.200	HTTPS	✓ 1.30kB/2.65 kB	2(Web-Server-Access-IPS)

The exhibit shows the IPS sensor configuration and forward traffic logs.

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 69 Which two SD-WAN load balancing methods use interface weight value to distribute traffic?

- A. Spillover
- B. Volume
- C. Source IP
- D. Sessions

Correct Answer: BD

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://docs.fortinet.com/document/fortigate/6.0.0/handbook/49719/configuring-sd-wan-load-balancing>

QUESTION 70 Which certificate value can FortiGate use to determine the relationship between the issuer and the certificate?

- A. **Subject Key Identifier** value
- B. **SMMIE Capabilities** value
- C. **Subject** value
- D. **Subject Alternative Name** value

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

