

Fortinet NSE4_FGT-6.2



Fortinet NSE 4 - FortiOS 6.2

Version: 2.0

QUESTION NO: 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.

Answer: A

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

QUESTION NO: 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

Answer: B

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

QUESTION NO: 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

Answer: C

Explanation:

QUESTION NO: 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.

Answer: A,B

Explanation:

QUESTION NO: 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

Answer: A

Explanation:

QUESTION NO: 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.

Answer: C,D

Explanation:

QUESTION NO: 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

Answer: A,D,E

Explanation:

QUESTION NO: 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.

Answer: B

Explanation:

QUESTION NO: 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.

Answer: D

Explanation:

QUESTION NO: 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

Answer: C

Explanation:

QUESTION NO: 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

Answer: D

Explanation:

QUESTION NO: 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.

Answer: A,B

Explanation:

QUESTION NO: 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.
B. **Administrative Access: FortiTelemetry.**
- C.
IP/Network Mask.
- D.
Role: **Security Fabric.**

Answer: B,C

Explanation:

QUESTION NO: 14

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

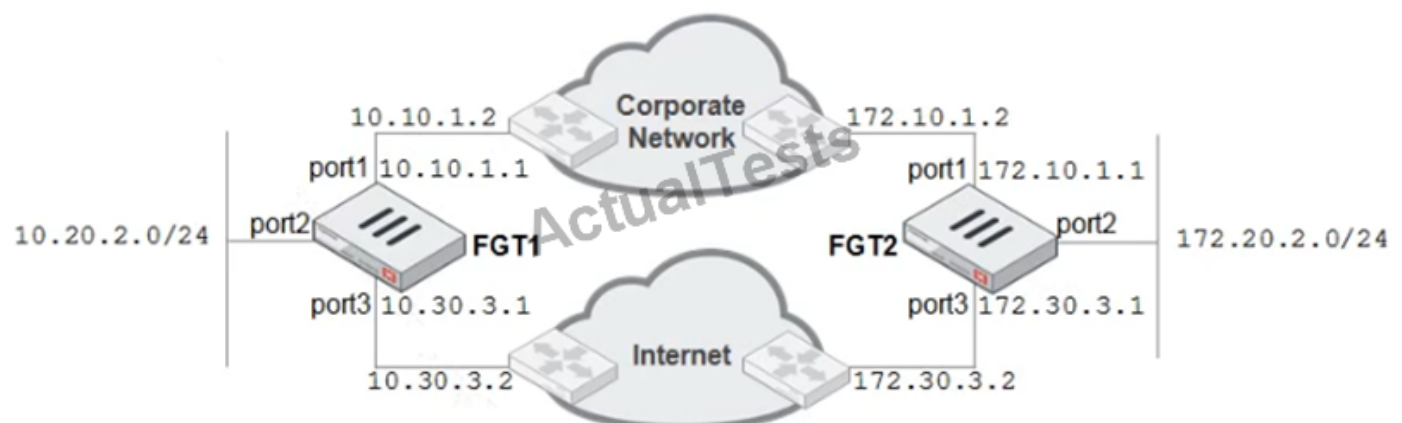
- A.**
It requires DC agents on every domain controller when used in multidomain environments.
- B.**
It is useful when users log in to DCs that are not monitored by a collector agent.
- C.**
It requires NTLM-enabled web browsers.
- D.**
It takes over as the primary authentication method when configured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

Answer: B,C

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

QUESTION NO: 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]

Answer: B,C

Explanation:

QUESTION NO: 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

Answer: C,D

Explanation:

QUESTION NO: 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.

Answer: A

Explanation:

QUESTION NO: 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.

Answer: D

Explanation:

QUESTION NO: 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

Answer: C,D

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

QUESTION NO: 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

Answer: A

Explanation:

QUESTION NO: 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

Answer: B,D

Explanation:

QUESTION NO: 22

Refer to the exhibits.

AV profile

Edit AntiVirus Profile

Name: default
 Comments: Scan files and block viruses. 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: default
 Comments: All default services. 21/255

Log Oversized Files ☐
 RPC over HTTP ☐

Protocol Port Mapping

Protocol	Any	Specify	Port
HTTP	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	80
SMTP	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	25
POP3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	110
IMAP	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	143
FTP	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	21
NNTP	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	119
MAPI	<input checked="" type="checkbox"/>		135
DNS	<input checked="" type="checkbox"/>		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) ☐

File transfer output

FileZilla Client Interface showing a successful FTP transfer.

Host: 10.200.3.254 Username: anonymous Password: Port: 223 Quickconnect

Status: Connecting to 10.200.3.254:223...
 Status: Connection established, waiting for welcome message...
 Status: Insecure server, it does not support FTP over TLS.
 Status: Logged in
 Status: Starting download of /pub/eicar.com
 Status: File transfer successful, transferred 68 bytes in 1 second

Local site: C:\Users\Administrator\Desktop\ Remote site: /pub

Filename	Size	Filetype	Last modified
..			
desktop.ini	282	Configuration ...	7/18/2017 1:54:01 ...
ecicar.com	68	MS-DOS Appli...	8/2/2017 7:13:57 AM
ecicar.com.txt	1,228	Text Document	7/27/2017 10:29:28...

8 files. Total size: 39,316,196 bytes

Filename	Size	Filetype	Last modified	Permissions	Owner/Gro...
..					
ecicar.com	68	MS-DOS A...	10/29/2014	-rw-r--r--	0 0

Selected 1 file. Total size: 68 bytes

Server/Local file Direction Remote file Size Priority Status

Queued files Failed transfers Successful transfers (1)

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

Answer: A

Explanation:

QUESTION NO: 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
<div>Search</div> <div>Cancel</div>	

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

Answer: B

Explanation:

QUESTION NO: 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.

Answer: C,D

Explanation:

QUESTION NO: 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.

Answer: A

Explanation:

QUESTION NO: 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

Answer: A

Explanation:

QUESTION NO: 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.

Answer: C,D

Explanation:

QUESTION NO: 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

Answer: D

Explanation:

QUESTION NO: 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.

Answer: B,C

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

QUESTION NO: 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.

Answer: A

Explanation:

QUESTION NO: 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

Answer: A,D

Explanation:

QUESTION NO: 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?

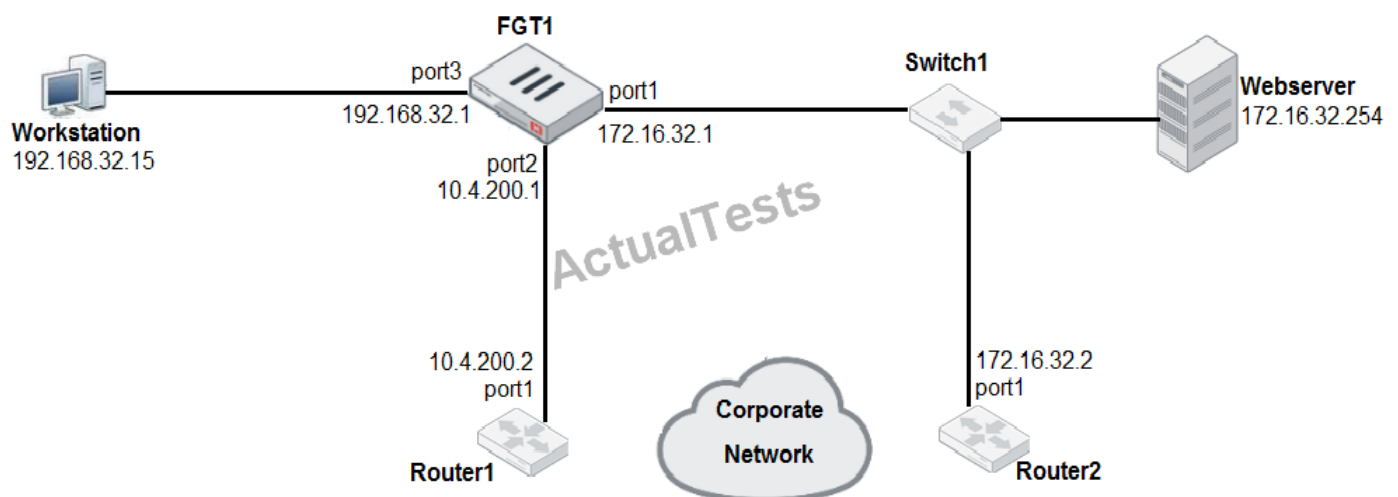
- A.**
The two VLAN sub interfaces can have the same VLAN ID, only if they have IP addresses in different subnets.
- B.**
The two VLAN sub interfaces must have different VLAN IDs.
- C.**
The two VLAN sub interfaces can have the same VLAN ID, only if they belong to different VDOMs.
- D.**
The two VLAN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

Answer: B

Explanation:

QUESTION NO: 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

Answer: A

Explanation:

QUESTION NO: 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.

Answer: B,C

Explanation:

QUESTION NO: 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.

Answer: B

Explanation:

QUESTION NO: 36

Refer to the exhibit.

Application Details

Name :	Category :	Technology :	Popularity :
Addicting Games	Game	Browser-Based	☆☆☆☆☆

Application Control Profile

Categories

▼ All Categories

Business (144, ☁6)	Cloud.IT (43)
Collaboration (268, ☁10)	Email (80, ☁12)
Game (87)	General.Interest (231, ☁7)
Mobile (3)	Network.Service (329)
P2P (63)	Proxy (166)
Remote.Access (84)	Social.Media (121, ☁31)
Storage.Backup (173, ☁17)	Update (50)
Video/Audio (160, ☁14)	VoIP (24)
Web.Client (23)	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.

Answer: D

Explanation:

QUESTION NO: 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.

Answer: D

Explanation:**QUESTION NO: 38**

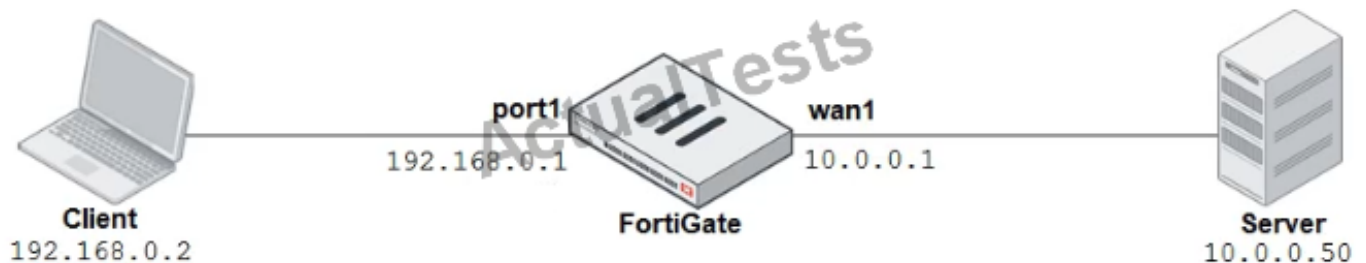
Which statement about the IP authentication header (AH) used by IPsec is true?

- 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.

Answer: C

Explanation:**QUESTION NO: 39**

Refer to the exhibits.



Explicit Proxy

☒ Explicit Web Proxy

Listen on Interfaces port1 + x

HTTP Port 8080 - 8080

HTTPS Port Use HTTP Port Specify

FTP over HTTP

Proxy auto-config (PAC) ☐

Proxy FQDN default.fqdn

Max HTTP request length 8 KB

Max HTTP message length 32 KB

Unknown HTTP version Best Effort Reject

Realm default

Default Firewall Policy Action Accept Deny

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'

Answer: A

Explanation:

QUESTION NO: 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.

Answer: B

Explanation:

QUESTION NO: 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.

Answer: C

Explanation:

QUESTION NO: 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

Answer: A,C,E

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

QUESTION NO: 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

Answer: D

Explanation:

QUESTION NO: 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.

Answer: A,D

Explanation:

QUESTION NO: 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.

Answer: A,C

Explanation:

QUESTION NO: 46

Refer to the exhibit.

The exhibit shows two static route configurations on a Fortinet firewall. Both routes are for the destination 172.13.24.0/255.255.255.0.

- Left Configuration (TunnelB):**
 - Destination: 172.13.24.0/255.255.255.0
 - Interface: TunnelB
 - Administrative Distance: 5
 - Status: Enabled
 - Priority: 30
- Right Configuration (TunnelA):**
 - Destination: 172.13.24.0/255.255.255.0
 - Interface: TunnelA
 - Administrative Distance: 10
 - Status: Enabled
 - 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.

Answer: A,D

Explanation:

QUESTION NO: 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

Answer: B

Explanation:

QUESTION NO: 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 user
- D.**
A CRL

Answer: B

Explanation:

QUESTION NO: 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.

Answer: D

Explanation:

QUESTION NO: 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.

Answer: C,D

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

QUESTION NO: 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.

Answer: D

Explanation:

QUESTION NO: 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.

Answer: A,B

Explanation:

QUESTION NO: 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

Answer: A

Explanation:

QUESTION NO: 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

Answer: B,C

Explanation:

QUESTION NO: 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

Answer: B,C

Explanation:

QUESTION NO: 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.

Answer: C

Explanation:

QUESTION NO: 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.

Answer: B

Explanation:

QUESTION NO: 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

Answer: C

Explanation:

QUESTION NO: 59

Refer to the exhibits.

IPS Sensor

Edit IPS Sensor WINDOWS_SERVER [View IPS Signatures]

Name: Comments:

IPS Signatures

[+ Add Signatures](#) [Delete](#) [Edit IP Exemptions](#)

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

IPS Filters

[+ Add Filter](#) [Edit Filter](#) [Delete](#)


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"/>	DigumAsteriskINVITE.TCPConnectionClose.DoS	5	1	Any	Block	None


[Apply](#)

DoS Policy

Incoming Interface  port1 ▼

Source Address  all + ✕

Destination Address  all + ✕

Services  ALL + ✕

L3 Anomalies

Name	<input type="checkbox"/> Status	<input type="checkbox"/> 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

Answer: B

Explanation:

QUESTION NO: 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.

Answer: A,B

Explanation:

QUESTION NO: 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.

Answer: B,C

Explanation:

QUESTION NO: 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

Answer: D

Explanation:

QUESTION NO: 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.

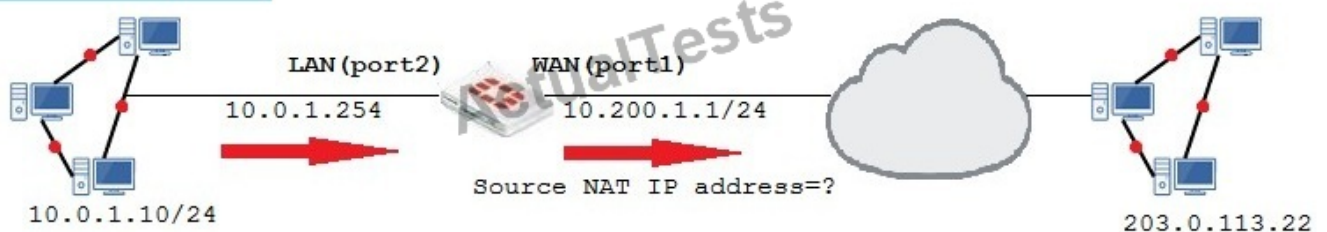
Answer: A,B,D

Explanation:

QUESTION NO: 64

Refer to the exhibits.

Network Diagram



Virtual IP

VIP type	IPv4
Name	VIP
Comments	Write a comment... 0/255
Color	Change
Network	
Interface	WAN (port1) ▼
Type	Static NAT
External IP address/range ⓘ	10.200.1.10
Mapped IP address/range	10.0.1.10
<input type="checkbox"/> Optional Filters	
<input type="checkbox"/> Port Forwarding	

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(port 1) → LAN(port 2) 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

Answer: A

Explanation:

QUESTION NO: 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.

Answer: C

Explanation:

QUESTION NO: 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.

Answer: B

Explanation:

QUESTION NO: 67

Refer to the exhibit.

+ Create New Edit Clone Delete				
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.

Answer: B

Explanation:

QUESTION NO: 68

Refer to the exhibit.

IPS Sensor



Name: [View IPS Signatures]

Comments: 0 / 255

IPS Signatures

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

IPS Filters

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

Forward Traffic Logs

#	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.

Answer: C

Explanation:

QUESTION NO: 69

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

- A.**
Spillover
- B.**

Volume

C.

Source IP

D.

Sessions

Answer: B,D

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

QUESTION NO: 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

Answer: C

Explanation:

QUESTION NO: 71

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

A.

Main mode does not support XAuth for user authentication.

- B.**
In aggressive mode, the remote peers are able to provide their peer IDs in the first message.
- C.**
FortiGate is able to handle NATed connections only in aggressive mode.
- D.**
FortiClient supports only aggressive mode.

Answer: B

Explanation:

QUESTION NO: 72

Which statement about the policy ID number of a firewall policy is true?

- A.**
It is required to modify a firewall policy using the CLI.
- B.**
It represents the number of objects used in the firewall policy.
- C.**
It changes when firewall policies are reordered.
- D.**
It defines the order in which rules are processed.

Answer: A

Explanation:

QUESTION NO: 73

Which two 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 disk logging.

C.

Enable a web filter security profile on the Full Access firewall policy.

D.

Enable **Log Allowed Traffic** on the Full Access firewall policy.

Answer: C,D

Explanation:

QUESTION NO: 74

An administrator is running the following sniffer command:

diagnose sniffer packet any "host 10.0.2.10" 3

Which three items will be included in the sniffer output? (Choose three.)

A.

IP header

B.

Interface name

C.

Packet payload

D.

Ethernet header

E.

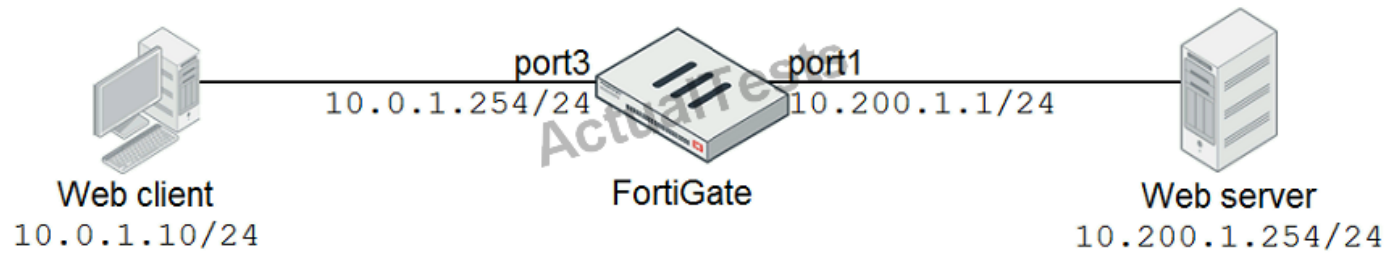
Application header

Answer: A,C,D

Explanation:

QUESTION NO: 75

Refer to the exhibit.



In the network shown in the exhibit, the web client cannot connect to the HTTP web server. The administrator runs the FortiGate built-in sniffer and gets 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
```

```
14.755510 port3 in 10.0.1.10.49256 ->
```

```
10.200.1.254.80: syn 868017830
```

What should the administrator do next to troubleshoot the problem?

A.

Capture the traffic using an external sniffer connected to port1.

B.

Run a sniffer on the web server.

C.

Execute another sniffer in the FortiGate, this time with the filter, "host 10.0.1.10".

D.

Execute a debug flow.

Answer: D

Explanation:

QUESTION NO: 76

Refer to the exhibit:

```

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]
S    *>          [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

```

Given the routing database shown in the exhibit, which two statements are correct? (Choose two.)

A.

The port3 default route has the lowest metric.

B.

The port3 default route has the highest distance.

C.

There will be eight routes active in the routing table.

D.

The port1 and port2 default routes are active in the routing table.

Answer: B,D

Explanation:

QUESTION NO: 77

Refer to the exhibit.

Admission Control

Security Mode

Captive Portal

Authentication Portal

Local

External

User Access ⓘ

Restricted to Groups

Allow all

The exhibit shows admission control settings.

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

A.

Groups defined in the captive portal configuration

B.

Only individual users – not groups – defined in the captive portal configuration

C.

All users

D.

Users and groups defined in the firewall policy

Answer: D**Explanation:****QUESTION NO: 78**

Which two configuration objects can you select in for the **Source** field of a firewall policy? (Choose two.)

A.

Firewall service

B.

FQDN address

C.

IP pool

D.

User or user group

Answer: B,D

Explanation:

QUESTION NO: 79

Which actions 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, monitor, block, and quarantine
- D.**
Allow, block, authenticate, and warning

Answer: C

Explanation:

QUESTION NO: 80

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

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

Answer: A

Explanation:**QUESTION NO: 81**

Refer to 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
```

Given the output of the # diagnose sys ha checksum cluster command shown in the exhibit, which two statements are correct? (Choose two.)

- A.**
The all VDOM is not synchronized between the primary and secondary FortiGate devices.

B.

The global configuration is synchronized between the primary and secondary FortiGate devices.

C.

The root VDOM is not synchronized between the primary and secondary FortiGate devices.

D.

The FortiGate devices have three VDOMs.

Answer: B,C

Explanation:

QUESTION NO: 82

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

A.

They can block DNS requests to known botnet command and control servers

B.

They can inspect HTTP traffic.

C.

They must be applied in firewall policies with SSL inspection enabled

D.

They can redirect blocked requests to a specific portal

Answer: A,D

Explanation:

QUESTION NO: 83

An administrator needs to strengthen the security for SSL VPN access.

Which three statements are best practices to do so? (Choose three.)

A.

Configure a client integrity check (host-check)

B.

Configure two-factor authentication using security certificates.

C.

Configure split tunneling

D.

Configure host restrictions by IP address or by MAC address.

E.

Configure SSL offloading to a content processor.

Answer: A,B,D**Explanation:****QUESTION NO: 84**

Refer to 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
```

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.

Which option is the most likely cause of the issue?

A.

High session timeout value

- B.**
High memory usage
- C.**
High CPU usage
- D.**
NAT port exhaustion

Answer: D

Explanation:

QUESTION NO: 85

Which process is involved in updating IPS from FortiGuard?

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

Answer: C

Explanation:

QUESTION NO: 86

Which two conditions are required for establishing an IPsec VPN between two FortiGate devices?
(Choose two.)

- A.**
If the VPN is configured as policy-based in one peer, it must also be configured as policy-based in the other peer.

B.

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.

C.

If XAuth is enabled as a server in one peer, it must be enabled as a client in the other peer.

D.

If the VPN is configured as route-based, there must be at least one firewall policy with the action set to **IPsec**.

Answer: B,C

Explanation:

QUESTION NO: 87

Refer to the exhibit.

```
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
```

The exhibit shows the two VLAN interfaces configuration.

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 condition must exist in order for the DHCP client to successfully get the dynamic IP address?

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




Answer: A

Explanation:

QUESTION NO: 88

Refer to the exhibit.

Edit Address

Category	Address Proxy Address
Name	Training
Color	 <input type="button" value="Change"/>
Type	HTTP Method ▼
Host	 all ▼
Request Method	POST  +
Show in Address List	<input checked="" type="checkbox"/>
Comments	<input type="text" value="Write a comment..."/> 0/255
Tags	<input type="button" value="⊕ Select Tags"/>

The exhibit contains a proxy address that an administrator created to block HTTP uploads.

Where must the proxy address be used?

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

Answer: D

Explanation:

QUESTION NO: 89

An administrator has configured central DNAT and virtual IPs.

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

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

Answer: A

Explanation:

QUESTION NO: 90

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

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

Answer: B

Explanation:

QUESTION NO: 91

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

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

Answer: A,D

Explanation:

QUESTION NO: 92

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

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

Answer: D

Explanation:

QUESTION NO: 93

Which statement about FortiGuard services for FortiGate is true?

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

Answer: C

Explanation:

QUESTION NO: 94

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

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

Answer: C

Explanation:

QUESTION NO: 95

When using SD-WAN, how must you configure a next-hop gateway address for a member

interface, so that FortiGate can forward Internet traffic?

A.

It must be configured in a policy route using the sdwan virtual interface.

B.

It must be learned automatically through a dynamic routing protocol.

C.

It must be configured in a static route using the sdwan virtual interface.

D.

It must be provided in the SD-WAN member interface configuration.

Answer: D

Explanation:

QUESTION NO: 96

Which statement about the FSSO collector agent timers is true?

A.

The **workstation verify interval** is used to periodically check if a workstation is still a domain member.

B.

The **dead entry timeout interval** is used to age out entries with an unverified status.

C.

The **user group cache expiry** is used to age out the monitored groups.

D.

The **IP address change verify interval** monitors the server IP address where the collector agent is installed.

Answer: B

Explanation:

QUESTION NO: 97

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

A.

WMI polling can increase bandwidth usage in large networks.

B.

The NetSessionEnum function is used to track user logoffs.

C.

The collector agent does not need to search any security event logs.

D.

The collector agent uses a Windows API to query DCs for user logins.

Answer: C,D

Explanation:

QUESTION NO: 98

Refer to the exhibit.

New SSL/SSH Inspection Profile

Name: Training

Comments: Write a comment... 0/255

SSL Inspection Options

Enable SSL Inspection of: Multiple Clients Connecting to Multiple Servers

Inspection Method: SSL Certificate Inspection Full SSL Inspection

CA Certificate: Fortinet_CA_SSL Download Certificate

Untrusted SSL Certificates: Allow Block View Trusted CAs List

An employee connects to <https://example.com> 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.

The 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.

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

Answer: D

Explanation:

QUESTION NO: 99

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 two actions can 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.

Answer: B,D

Explanation:

QUESTION NO: 100

Which statement about a One-to-One IP pool is true?

- A.**
It is used for destination NAT.
- B.**
It limits the client to 64 connections per IP pool.
- C.**
It allows the fixed mapping of an internal address range to an external address range.
- D.**
It does not use port address translation.

Answer: D

Explanation:

QUESTION NO: 101

Refer to the exhibit.

Edit IPS Sensor

Name

WINDOWS_SERVERS

[\[View IPS Signatures\]](#)

Comments

0/255

Block malicious URLs



IPS Signatures

<div> <div>+ Add Signatures</div> <div>🗑 Delete</div> <div>✎ Edit IP Exemptions</div> </div>							
Name	Exempt IPs	Severity	Target	Service	OS	Action	Packet Logging
NTP.Spoofed.KoD.DoS	0	<div><div></div></div>	Server, Client	UDP	Linux	Monitor	

IPS Filters

<div> <div>+ Add Filter</div> <div>✎ Edit Filter</div> <div>🗑 Delete</div> </div>		
Filter Details	Action	Packet Logging
Location: server OS: Windows	Block	

The exhibit shows the IPS sensor configuration.

If traffic matches this IPS sensor, which two actions is the sensor expected to take? (Choose two.)

A.

The sensor will allow attackers matching the **NTP.Spoofed.KoD.DoS** signature.

B.

The sensor will block all attacks aimed at Windows servers.

C.

The sensor will reset all connections that match these signatures.

D.

The sensor will gather a packet log for all matched traffic.

Answer: A,B

Explanation:

QUESTION NO: 102

An administrator wants to throttle the total volume of SMTP sessions to their email server.

Which DoS sensor can the administrator use to achieve this?

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

Answer: B

Explanation:

QUESTION NO: 103

A FortiGate device has multiple VDOMs.

Which statement about an administrator account configured with the default **prof_admin** profile is true?

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

Answer: C

Explanation:

QUESTION NO: 104

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

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

Answer: C

Explanation:

QUESTION NO: 105

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

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

Answer: B,C,D

Explanation:

QUESTION NO: 106

Which two statements about conserve mode are true? (Choose two.)

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

Answer: C,D

Explanation:

QUESTION NO: 107

Which two features are supported by web filter in flow-based inspection mode with NGFW mode set to profile-based? (Choose two.)

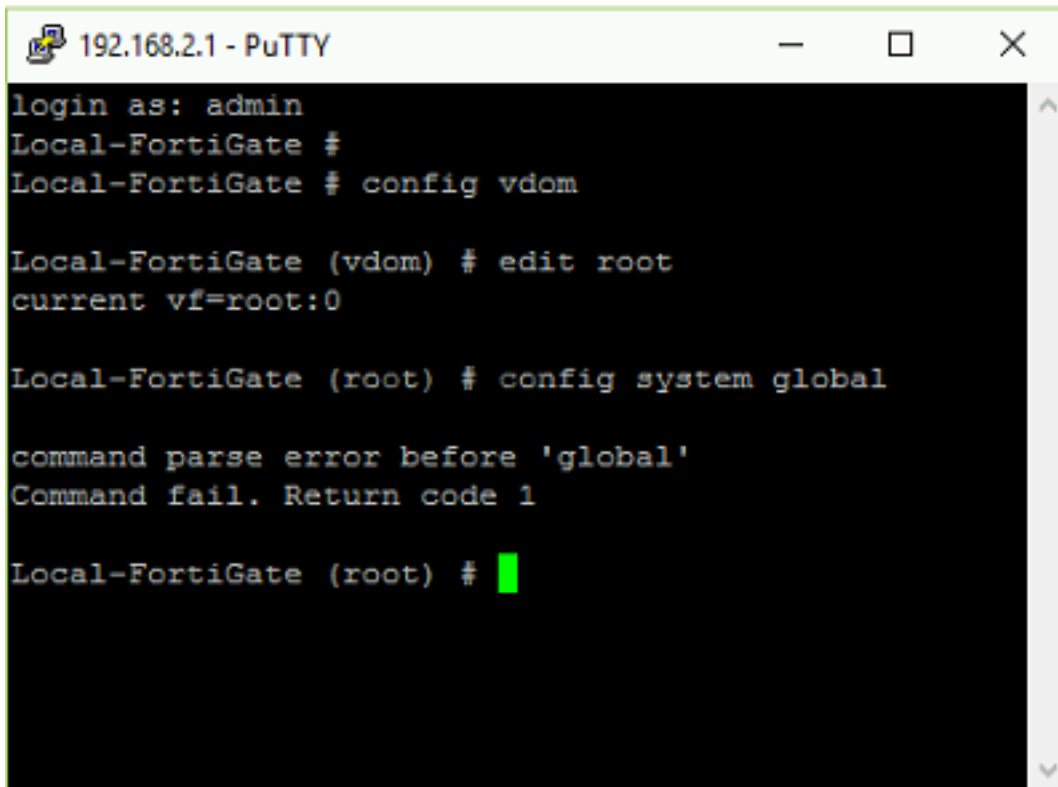
- A.**
Search engines
- B.**
FortiGuard Quotas
- C.**
Static URL
- D.**
Rating option

Answer: C,D

Explanation:

QUESTION NO: 108

Refer to the exhibit.



```
192.168.2.1 - PuTTY
login as: admin
Local-FortiGate #
Local-FortiGate # config vdom

Local-FortiGate (vdom) # edit root
current vf=root:0

Local-FortiGate (root) # config system global

command parse error before 'global'
Command fail. Return code 1

Local-FortiGate (root) #
```

Given the FortiGate CLI output, 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 command config system global does not exist in FortiGate.
- D.
The global settings cannot be configured from the root VDOM context.

Answer: D

Explanation:

QUESTION NO: 109

An administrator has configured a dialup IPsec VPN with XAuth.

Which statement best describes what occurs during this scenario?

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

Answer: D

Explanation:

QUESTION NO: 110

When override is enabled, which option shows the process and selection criteria that is used to elect the primary FortiGate in an HA cluster?

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

Answer: D

Explanation:

QUESTION NO: 111

HTTP public key pinning (HPKP) can be an obstacle to implementing full SSL inspection.

In which two ways can you resolve this problem? (Choose two.)

A.

Enable **Allow Invalid SSL Certificates** for the relevant security profile.

B.

Exempt those web sites that use HPKP from full SSL inspection.

C.

Install the CA certificate (that is required to verify the web server certificate) in the certificate stores of users' computers.

D.

Use a web browser that does not support HPKP.

Answer: B,D

Explanation:

QUESTION NO: 112

A company needs to provide SSL VPN access to two user groups. The company also needs to display a different welcome message for each group, on the SSL VPN login.

To meet these requirements, what is required in the SSL VPN configuration?

A.

Different virtual SSL VPN IP addresses 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 SSL VPN realms for each group

Answer: D

Explanation:

QUESTION NO: 113

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

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

Answer: B,D

Explanation:

QUESTION NO: 114

Which two 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 sends a DHCPINFORM request to the DHCP server.
- C.**
The DHCP server provides the PAC file for download.
- D.**
The browser needs to be preconfigured with the DHCP server IP address.

Answer: A,B

Explanation:

QUESTION NO: 115

Refer to the exhibit.

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

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

A.

Access to browser-based **Social.Media** applications will be blocked.

B.

Access to mobile social media applications will be blocked.

C.

Access to all applications in the **Social.Media** category will be blocked.

D.

Access to all unknown applications will be allowed.

Answer: A,D

Explanation:

QUESTION NO: 116

Which two statements about SSL VPN timers are true? (Choose two.)

A.

SSL VPN settings do not have customizable timers.

B.

SSL VPN timers prevent SSL VPN users from being logged out because of high network latency.

C.

SSL VPN timers disconnect idle SSL VPN users when a firewall policy authentication timeout occurs.

D.

SSL VPN timers allow to mitigate DoS attacks from partial HTTP requests.

Answer: B,D

Explanation:

QUESTION NO: 117

Refer to the exhibit.

```
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
origin->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
```

The exhibit contains a session diagnostic output.

Which statement about the session diagnostic output is true?

A.

The session is in CLOSE_WAIT state.

B.

The session is in TIME_WAIT state.

C.

The session is in LISTEN state.

D.

The session is in ESTABLISHED state.





Answer: D

Explanation:

QUESTION NO: 118

Refer to 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 srcport=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 rcvbyte=0 direction="outgoing" msg="URL belongs to
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	<input type="checkbox"/> any	<input type="checkbox"/> any

The exhibit shows a raw log and firewall policies.

What information does this raw log provide? (Choose two.)

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

Answer: A,B

Explanation:

QUESTION NO: 119

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

A.

A FortiGate device has 64 VDOMs, created by default.

B.

The root VDOM is the management VDOM, by default.

C.

Each VDOM maintains its own system time.

D.

Each VDOM maintains its own routing table.

Answer: B,D

Explanation: