

NSE4-5.4.exam.190q

Number: NSE4-5.4
Passing Score: 800
Time Limit: 120 min
File Version: 4.0



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

<https://vceplus.com/>

NSE4-5.4

Fortinet Network Security Expert 4 Written Exam - FortiOS 5.4

Exam A

QUESTION 1

Which file names will match the *.tiff file name pattern configured in a data leak prevention filter? (Choose two.)



<https://vceplus.com/>

- A. tiff.tiff
- B. tiff.png
- C. tiff.jpeg
- D. gif.tiff

Correct Answer: AD

Section: (none)

Explanation

Explanation/Reference:



QUESTION 2

An administrator has configured a dialup IPsec VPN with XAuth. Which method statement best describes this scenario?

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 3

Examine this output from a debug flow:

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

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

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

Correct Answer: AC

Section: (none)

Explanation



Explanation/Reference:

QUESTION 4

Which component of FortiOS performs application control inspection?

- A. Kernel
- B. Antivirus engine
- C. IPS engine
- D. Application control engine

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 5

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

- A. They support GRE-over-IPsec.
- B. They can be configured in both NAT/Route and transparent operation modes.
- C. They require two firewall policies: one for each direction of traffic flow.
- D. They support L2TP-over-IPsec.

Correct Answer: BD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 6

What statement describes what DNS64 does?



<https://vceplus.com/>

- A. Converts DNS A record lookups to AAAA record lookups.
- B. Translates the destination IPv6 address of the DNS traffic to an IPv4 address.
- C. Synthesizes DNS AAAA records from A records.
- D. Translates the destination IPv4 address of the DNS traffic to an IPv6 address.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 7

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

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 8

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

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 9

An administrator has configured the following settings:

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

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

What does the configuration do? (Choose two.)

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

Correct Answer: AD

Section: (none)

Explanation

Explanation/Reference:



QUESTION 10

Which statements about FortiGate inspection modes are true? (Choose two.)

- A. The default inspection mode is proxy based.
- B. Switching from proxy-based mode to flow-based, then back to proxy-based mode, will not result in the original configuration.
- C. Proxy-based inspection is not available in VDOMs operating in transparent mode.
- D. Flow-based profiles must be manually converted to proxy-based profiles before changing the inspection mode from flow based to proxy based.

Correct Answer: AC

Section: (none)

Explanation

Explanation/Reference:

QUESTION 11

Examine the following interface configuration on a FortiGate in transparent mode:

```
config system interface
  edit <interface name>
    set stop-forward enable
  end
```

Which statement about this configuration is correct?



<https://vceplus.com/>

- A. The FortiGate generates spanning tree BPDU frames.
- B. The FortiGate device forwards received spanning tree BPDU frames.
- C. The FortiGate can block an interface if a layer-2 loop is detected.
- D. Ethernet layer-2 loops are likely to occur.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 12

Examine this PAC file configuration.

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

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

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

Correct Answer: AD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 13

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

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 14

A FortiGate is operating in NAT/Route mode and configured with two virtual LAN (VLAN) sub-interfaces added to the same physical interface.

Which statement about the VLAN IDs in this scenario is true?

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:



QUESTION 15

Which of the following statements are true when using Web Proxy Auto-discovery Protocol (WPAD) with the DHCP discovery method? (Choose two.)

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

Correct Answer: AD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 16

What inspections are executed by the IPS engine? (Choose three.)

- A. Application control
- B. Flow-based data leak prevention

- C. Proxy-based antispam
- D. Flow-based web filtering
- E. Proxy-based antivirus

Correct Answer: ABD

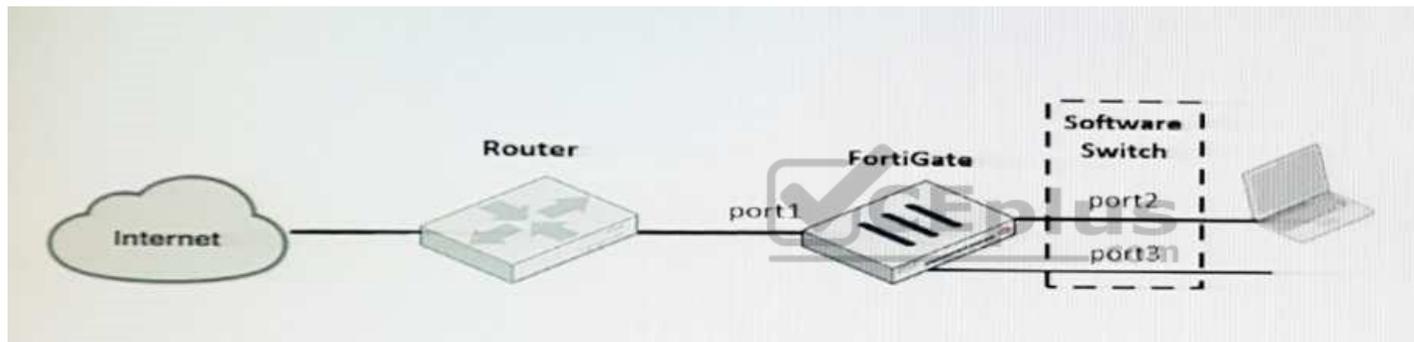
Section: (none)

Explanation

Explanation/Reference:

QUESTION 17

Examine the exhibit.



A client workstation is connected to FortiGate port2. The Fortigate port1 is connected to an ISP router. Port2 and port3 are both configured as a software switch.

What IP address must be configured in the workstation as the default gateway?

- A. The port2's IP address.
- B. The router's IP address.
- C. The FortiGate's management IP address.
- D. The software switch interface's IP address.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 18

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

- A. The dead entry timeout interval is used to age out entries with an unverified status.
- B. The workstation verify interval is used to periodically check if a workstation is still a domain member.
- 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, and updates the collector agent configuration if it changes.

Correct Answer: A

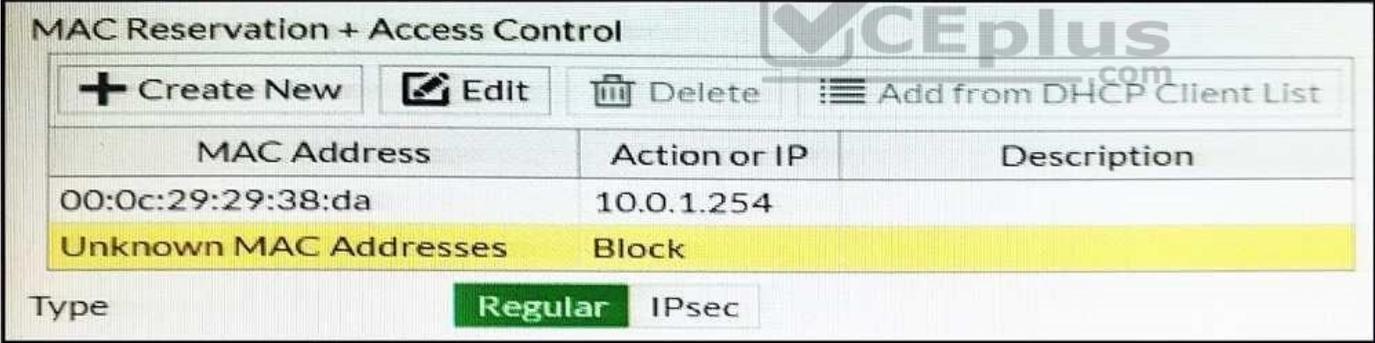
Section: (none)

Explanation

Explanation/Reference:

QUESTION 19

An administrator has enabled the DHCP Server on the port1 interface and configured the following based on the exhibit.



MAC Address	Action or IP	Description
00:0c:29:29:38:da	10.0.1.254	
Unknown MAC Addresses	Block	

Type: Regular IPsec

Which statement is correct based on this configuration?

- A. The MAC address 00:0c:29:29:38:da belongs to the port1 interface.
- B. Access to the network is blocked for the devices with the MAC address 00:0c:29:29:38:da and the IP address 10.0.1.254.
- C. 00:0c:29:29:38:da is the virtual MAC address assigned to the secondary IP address (10.0.1.254) of the port1 interface.
- D. The IP address 10.0.1.254 is reserves for the device with the MAC address 00:0c:29:29:38:da.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 20

An administrator wants to create a policy-based IPsec VPN tunnel between two FortiGate devices.

Which configuration steps must be performed on both units to support this scenario? (Choose three.)

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

Correct Answer: ACE

Section: (none)

Explanation

Explanation/Reference:



QUESTION 21

View the Exhibit.

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

```
-----FGVM010000058290-----
is_manage_mastrer ()=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_mastrer ()=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
```

Which statements are correct based on this output? (Choose two.)

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

Correct Answer: AC

Section: (none)

Explanation

Explanation/Reference:

QUESTION 22

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



<https://vceplus.com/>

- A. Web caching slows down web browsing due to constant read-write cycles from FortiGate memory.
- B. When a client makes a web request, the proxy checks if the requested URL is already in memory.
- C. Only heavy content is cached, for example, videos, images, audio and so on.
- D. Web caching is supported in both explicit and implicit proxy.

Correct Answer: BD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 23

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 assign users to a group for active authentication.
- C. You must place the firewall policy for active authentication before a firewall policy for passive authentication.
- D. You must enable the **Authentication** setting on the firewall policy.

Correct Answer: B

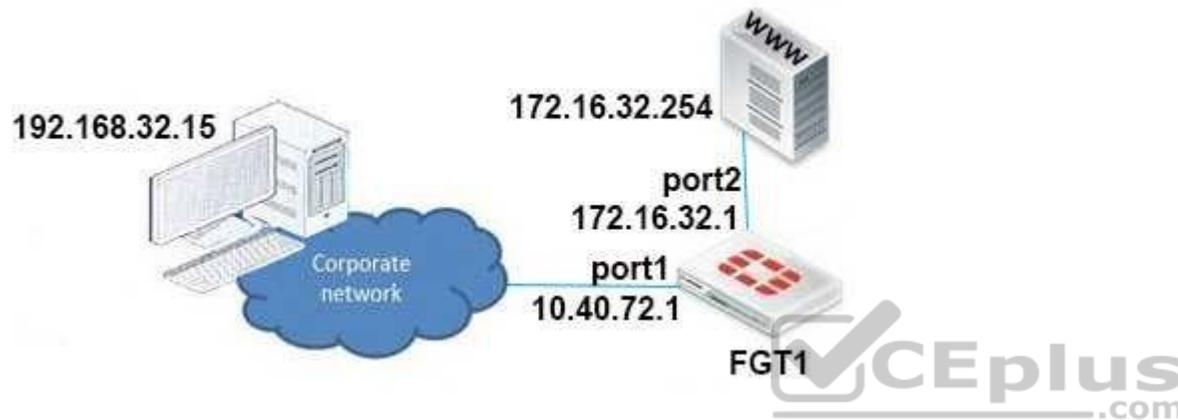
Section: (none)

Explanation

Explanation/Reference:

QUESTION 24

View the exhibit.



In this scenario, FGT1 has the following routing table:

```
S* 0. 0. 0. 0/0 [10/0] via 10. 40. 72. 2, port1
C 172. 16. 32. 0/24 is directly connected, port2
C 10. 40. 72. 0/30 is directly connected, port1
```

A user at 192.168.32.15 is trying to access the web server at 172.16.32.254. Which of the following statements best describe how the FortiGate will perform reverse path forwarding checks on this traffic? (Choose two.)

- A. Strict RPF check will deny the traffic.
- B. Strict RPF check will allow the traffic.
- C. Loose RPF check will allow the traffic.
- D. Loose RPF check will deny the traffic.

Correct Answer: BD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 25

View the exhibit.

```
date=2016-08-24 time=06:23:52 logid=0316013056 type=utm subtype=webfilter
eventtype=ftgd_blk level=warning vd=root policyid=1 sessionid=819 user= " " scrip=10.0.1.10
srcport=58901 srcintf= "port3" dstip=104.31.72.91 dstport=80 dstintf= "port1" proto=6
service= "HTTP" hostname= "mind-surf.net" profile="Category_Monitor" action=blocked
reqtype=direct url="/drogas" sentbyte=144 rcvbyte=0 direction=outgoing msg= "URL belongs
to a denied category in policy" method=domain cat=1 catdesc= "Drug Abuse" crscore=40
crlevel=high
```

What does the log message indicate? (Choose two.)

- A. The log type is utm.
- B. 10.0.1.10 is the IP address for mind-surf.net.
- C. FortiGate blocked the traffic.
- D. Firewall policy ID 6 matched the traffic.



Correct Answer: AC

Section: (none)

Explanation

Explanation/Reference:

QUESTION 26

Which election criterion is used to elect the primary FortiGate in a high availability (HA) cluster when override is enabled?

- A. uptime > priority > port monitor > serial number
- B. port monitor > uptime > priority > serial number
- C. priority > port monitor > uptime > serial number
- D. port monitor > priority > uptime > serial number

Correct Answer: D

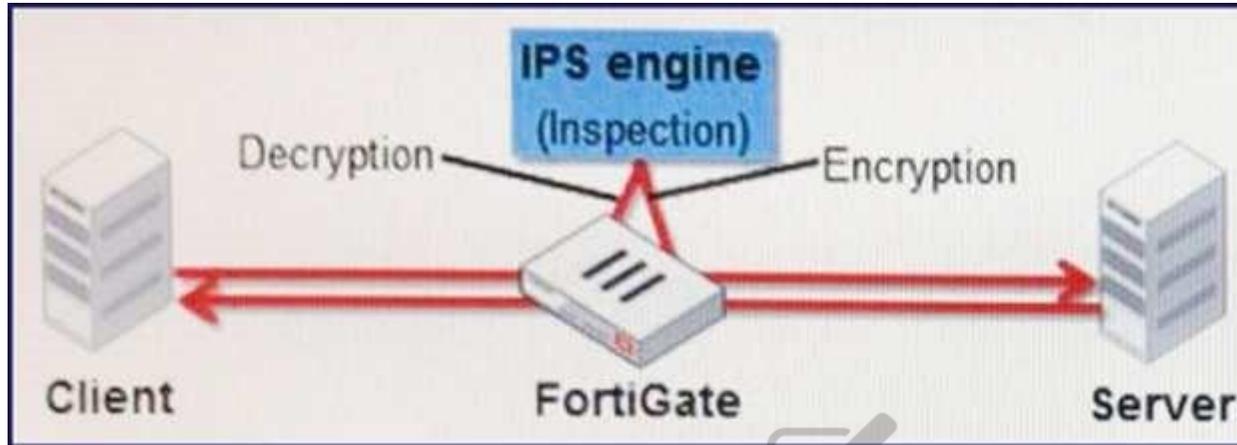
Section: (none)

Explanation

Explanation/Reference:

QUESTION 27

View the exhibit.



What does this exhibit represent?

- A. SSL handshake
- B. Interchanging digital certificates
- C. Certificate signing request (CSR)
- D. Inline SSL inspection

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 28

Which condition must be met to offload the encryption and decryption of IPsec traffic to an NP6 processor?

- A. Phase 2 must use an encryption algorithm supported by the NP6.
- B. Anti-replay must be disabled.

- C. IPsec traffic must not be inspected by a session helper.
- D. No content inspection can be applied to traffic that is going to be encrypted.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 29

What FortiGate feature can be used to prevent a cross-site scripting (XSS) attack?

- A. Web application firewall (WAF)
- B. DoS policies
- C. Rate based IPS signatures
- D. One-arm sniffer

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:



QUESTION 30

What is the purpose of the **Policy Lookup** feature?

- A. It searches the matching policy based on an input criteria.
- B. It enables hidden security profiles with full logging capabilities and generates **Learning Reports** based on an input criteria.
- C. It finds duplicate objects in firewall policies.
- D. It creates a new firewall policy based on an input criteria.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 31

View the exhibit.

Name: wan-load-balance
 Type: WAN Links Interface
 Interface State: ↑ Enable ↓ Disable

WAN LLB

+ Create New ✎ Edit 🗑 Delete

Seq.#	Interface	Status	Gateway
1	port1	✔	172.20.32.1
2	port2	✔	10.16.48.1

Load Balancing Algorithm

Volume Sessions Spillover **Source-Destination IP** Source IP

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

- A. next-hop IP address is not required when configuring a static route that uses the wan-load balance interface.
- B. Sessions will be load-balanced based on source and destination IP addresses.
- C. Each member interface requires its own firewall policy to allow traffic.
- D. The **wan-load-balance** interface must be manually created.

Correct Answer: AB

Section: (none)

Explanation

Explanation/Reference:

QUESTION 32

Examine the following web filtering log.

Which statement about the log message is true?

- A. The action for the category **Games** is set to block.
- B. The usage quota for the IP address 10.0.1.10 has expired.

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

- C. The name of the applied web filter profile is default.
- D. The web site miniclip.com matches a static URL filter whose action is set to **Warning**.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 33

Examine this output from a debug flow:

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



<https://vceplus.com/>

```
id=2 line=4677 msg="vd-root received a packet (proto=6, 66.171.121.44:80 - >10.200.1.1:4
[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"
```

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

Correct Answer: BD

Section: (none)

Explanation

Explanation/Reference:



QUESTION 34

View the exhibit.



The screenshot shows the 'Admission Control' configuration page. It includes a 'Security Mode' dropdown menu set to 'Captive Portal'. Below it, there are two radio buttons for 'Authentication Portal': 'Local' (which is selected and highlighted in green) and 'External'. At the bottom, there is a 'User Access' section with an information icon and a 'Restricted to Groups' dropdown menu set to 'Allow all' (highlighted in green).

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

- A. Only individual users—not groups—defined in the captive portal configuration.
- B. Groups defined in the captive portal configuration
- C. All users

D. Users and groups defined in the firewall policy.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 35

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

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:



QUESTION 36

An administrator has disabled **Accept push updates** under **Antivirus & IPS Updates**. Which statements is true when this setting is disabled?

- A. The extreme database is disabled.
- B. New AV definitions are not added to FortiGate as soon as they are releases by FortiGuard.
- C. Administrators cannot manually upload new AV definitions to the FortiGate.
- D. FortiGate does not send files to FortiSandbox for inspection.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 37

An administrator needs to create a tunnel mode SSLVPN to access an internal web server from the Internet. The web server is connected to `port1`. The Internet is connected to `port2`. Both interfaces belong to the VDOM named `Corporation`. What interface must be used as the source for the firewall policy that will allow this traffic?

- A. `ssl.root`
- B. `ssl.Corporation`
- C. `port2`
- D. `port1`

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 38

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

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 39

View the exhibit.

```
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) # █
```

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

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 40

What FortiGate feature can be used to block a ping sweep scan from an attacker?

- A. Web application firewall (WAF)
- B. Rate based IPS signatures
- C. One-arm sniffer
- D. DoS policies

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 41

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

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

Correct Answer: BD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 42

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

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

A. The web server IP address 204.79.197.200 is categorized by FortiGuard as **Malicious Websites**.

```
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,
=31 : d=www.bing.com : 80, id=29, vfname= 'root', vfid=0, profile= 'default'
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=63
04.79.197.200 dport=80 service= "http" cat=26 cat_desc= "Malicious Website"
hostname= www.bing.com url= "/"
```

B. The rating for the web site `www.bing.com` has been locally overridden to a category that is being blocked.

C. The web site `www.bing.com` is categorized by FortiGuard as Malicious Websites.

D. The user has not authenticated with the FortiGate yet.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 43

View the exhibit.

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

===== FGVM010000058290 =====

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

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

===== FGVM010000058289 =====

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

Which statements are correct, based on this output? (Choose two.)

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

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

Correct Answer: AC

Section: (none)

Explanation

Explanation/Reference:

QUESTION 44

What IPv6 extension header can be used to provide encryption and data confidentiality?

- A. Mobility
- B. ESP
- C. Authentication
- D. Destination options

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:



QUESTION 45

Which two statements are true about IPsec VPNs and SSL VPNs? (Choose two.)

- A. SSL VPN creates a HTTPS connection. IPsec does not.
- B. Both SSL VPNs and IPsec VPNs are standard protocols.
- C. Either a SSL VPN or an IPsec VPN can be established between two FortiGate devices.
- D. Either a SSL VPN or an IPsec VPN can be established between an end-user workstation and a FortiGate device.

Correct Answer: AD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 46

Alert emails enable the FortiGate unit to send email notifications to an email address upon detection of a pre-defined event type. Which of the following are some of the available event types in Web Config? (Select all that apply.)



<https://vceplus.com/>

- A. Intrusion detected.
- B. Successful firewall authentication.
- C. Oversized file detected.
- D. DHCP address assigned.
- E. FortiGuard Web Filtering rating error detected.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 47

A user logs into a SSL VPN portal and activates the tunnel mode.

The administrator has enabled split tunneling. The exhibit shows the firewall policy configuration:



Seq.#	Source	Destination	Schedule	Service	Action	NAT
port2 - port1 (1 - 1)						
1	all	all	always	ALL	✓ ACCEPT	✓ Enable
ssl.root (SSL VPN interface) - port2 (2 - 2)						
2	all training	Internal_Servers	always	ALL	✓ ACCEPT	✗ Disable
Implicit (3 - 3)						
3	all	all	always	ALL	⊘ DENY	

Which static route is automatically added to the client's routing table when the tunnel mode is activated?

- A. A route to a destination subnet matching the Internal_Servers address object.
- B. A route to the destination subnet configured in the tunnel mode widget.
- C. A default route.
- D. A route to the destination subnet configured in the SSL VPN global settings.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 48

Regarding tunnel-mode SSL VPN, which three statements are correct? (Choose three.)

- A. Split tunneling is supported.
- B. It requires the installation of a VPN client.
- C. It requires the use of an Internet browser.
- D. It does not support traffic from third-party network applications.
- E. An SSL VPN IP address is dynamically assigned to the client by the FortiGate unit.

Correct Answer: ABE

Section: (none)

Explanation

Explanation/Reference:

QUESTION 49

DLP archiving gives the ability to store session transaction data on a FortiAnalyzer unit for which of the following types of network traffic? (Select all that apply.)

- A. SNMP
- B. IPSec
- C. SMTP
- D. POP3
- E. HTTP

Correct Answer: CDE

Section: (none)

Explanation

Explanation/Reference:



QUESTION 50

Which statements regarding banned words are correct? (Choose two.)

- A. Content is automatically blocked if a single instance of a banned word appears.
- B. The FortiGate updates banned words on a periodic basis.
- C. The FortiGate can scan web pages and email messages for instances of banned words.
- D. Banned words can be expressed as simple text, wildcards and regular expressions.

Correct Answer: CD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 51

Examine the following FortiGate web proxy configuration; then answer the question below:

```
config web-proxy explicit
set pac-file-server-status enable
set pac-file-server-port 8080
set pac-file-name wpad.dat
end
```

Assuming that the FortiGate proxy IP address is 10.10.1.1, which URL must an Internet browser use to download the PAC file?

- A. https://10.10.1.1:8080
- B. https://10.10.1.1:8080/wpad.dat
- C. http://10.10.1.1:8080/
- D. http://10.10.1.1:8080/wpad.dat

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:



QUESTION 52

Which statements are true regarding the use of a PAC file to configure the web proxy settings in an Internet browser? (Choose two.)

- A. Only one proxy is supported.
- B. Can be manually imported to the browser.
- C. The browser can automatically download it from a web server.
- D. Can include a list of destination IP subnets where the browser can connect directly to without using a proxy.

Correct Answer: CD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 53

Which two methods are supported by the web proxy auto-discovery protocol (WPAD) to automatically learn the URL where a PAC file is located? (Choose two.)

- A. DHCP

- B. BOOTP
- C. DNS
- D. IPv6 auto configuration

Correct Answer: AC

Section: (none)

Explanation

Explanation/Reference:

QUESTION 54

What is a valid reason for using session based authentication instead of IP based authentication in a FortiGate web proxy solution?

- A. Users are required to manually enter their credentials each time they connect to a different web site.
- B. Proxy users are authenticated via FSSO.
- C. There are multiple users sharing the same IP address.
- D. Proxy users are authenticated via RADIUS.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:



QUESTION 55

Which two web filtering inspection modes inspect the full URL? (Choose two.)

- A. DNS-based.
- B. Proxy-based.



<https://vceplus.com/>

- C. Flow-based.
- D. URL-based

Correct Answer: BC

Section: (none)

Explanation

Explanation/Reference:



QUESTION 56

Which web filtering inspection mode inspects DNS traffic?

- A. DNS-based
- B. FQDN-based
- C. Flow-based
- D. URL-based

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 57

Which statements are correct regarding URL filtering on a FortiGate unit? (Choose two.)

- A. The allowed actions for URL filtering include allow, block, monitor and exempt.
- B. The allowed actions for URL filtering are Allow and Block only.
- C. URL filters may be based on patterns using simple text, wildcards and regular expressions.
- D. URL filters are based on simple text only and require an exact match.

Correct Answer: AC

Section: (none)

Explanation

Explanation/Reference:

QUESTION 58

Which of the following regular expression patterns make the terms "confidential data" case insensitive?

- A. [confidential data]
- B. /confidential data/i
- C. i/confidential data/
- D. "confidential data"



Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 59

Which statements are correct regarding application control? (Choose two.)

- A. It is based on the IPS engine.
- B. It is based on the AV engine.
- C. It can be applied to SSL encrypted traffic.
- D. Application control cannot be applied to SSL encrypted traffic.

Correct Answer: AC

Section: (none)

Explanation

Explanation/Reference:

QUESTION 60

How do you configure a FortiGate to apply traffic shaping to P2P traffic, such as BitTorrent?

- A. Apply a traffic shaper to a BitTorrent entry in an application control list, which is then applied to a firewall policy.
- B. Enable the shape option in a firewall policy with service set to BitTorrent.
- C. Define a DLP rule to match against BitTorrent traffic and include the rule in a DLP sensor with traffic shaping enabled.
- D. Apply a traffic shaper to a protocol options profile.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 61

Which statements are true regarding traffic shaping that is applied in an application sensor, and associated with a firewall policy? (Choose two.)

- A. Shared traffic shaping cannot be used.
- B. Only traffic matching the application control signature is shaped.
- C. Can limit the bandwidth usage of heavy traffic applications.
- D. Per-IP traffic shaping cannot be used.

Correct Answer: BC

Section: (none)

Explanation

Explanation/Reference:

QUESTION 62

A static route is configured for a FortiGate unit from the CLI using the following commands:

```
config router static edit 1
set device "wan1"
set distance 20
set gateway 192.168.100.1
next
end
```

Which of the following conditions is NOT required for this static default route to be displayed in the FortiGate unit's routing table?

- A. The Administrative Status of the wan1 interface is displayed as Up.
- B. The Link Status of the wan1 interface is displayed as Up.
- C. All other default routes should have an equal or higher distance.
- D. You must disable DHCP client on that interface.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:



QUESTION 63

When does a FortiGate load-share traffic between two static routes to the same destination subnet?

- A. When they have the same cost and distance.
- B. When they have the same distance and the same weight.
- C. When they have the same distance and different priority.
- D. When they have the same distance and same priority.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 64

Examine the static route configuration shown below; then answer the question following it. (Choose two.)

```
config router static
edit 1
set dst 172.20.1.0 255.255.255.0
set device port1
set gateway 172.11.12.1
set distance 10
set weight 5
next
edit 2
set dst 172.20.1.0 255.255.255.0
set blackhole enable
set distance 5
set weight 10
next
end
```

Which of the following statements correctly describes the static routing configuration provided? (Choose two.)

- A. All traffic to 172.20.1.0/24 is dropped by the FortiGate.
- B. As long as port1 is up, all traffic to 172.20.1.0/24 is routed by the static route number 1. If the interface port1 is down, the traffic is routed using the blackhole route.
- C. The FortiGate unit does NOT create a session entry in the session table when the traffic is being routed by the blackhole route.
- D. The FortiGate unit creates a session entry in the session table when the traffic is being routed by the blackhole route.

Correct Answer: AC

Section: (none)

Explanation

Explanation/Reference:

QUESTION 65

In the case of TCP traffic, which of the following correctly describes the routing table lookups performed by a FortiGate operating in NAT/Route mode, when searching for a suitable gateway?

- A. A lookup is done only when the first packet coming from the client (SYN) arrives

- B. A lookup is done when the first packet coming from the client (SYN) arrives, and a second one is performed when the first packet coming from the server (SYN/ ACK) arrives.
- C. Three lookups are done during the TCP 3-way handshake (SYN, SYN/ACK, ACK).
- D. A lookup is always done each time a packet arrives, from either the server or the client side.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 66

Examine the two static routes to the same destination subnet 172.20.168.0/24 as shown below; then answer the question following it.

```
config router static
edit 1
set dst 172.20.168.0 255.255.255.0
set distance 20
set priority 10
set device port1
next
edit 2
set dst 172.20.168.0 255.255.255.0
set distance 20
set priority 20
set device port2
next
end
```



Which of the following statements correctly describes the static routing configuration provided above?

- A. The FortiGate evenly shares the traffic to 172.20.168.0/24 through both routes.
- B. The FortiGate shares the traffic to 172.20.168.0/24 through both routes, but the port2 route will carry approximately twice as much of the traffic.
- C. The FortiGate sends all the traffic to 172.20.168.0/24 through port1.
- D. Only the route that is using port1 will show up in the routing table.

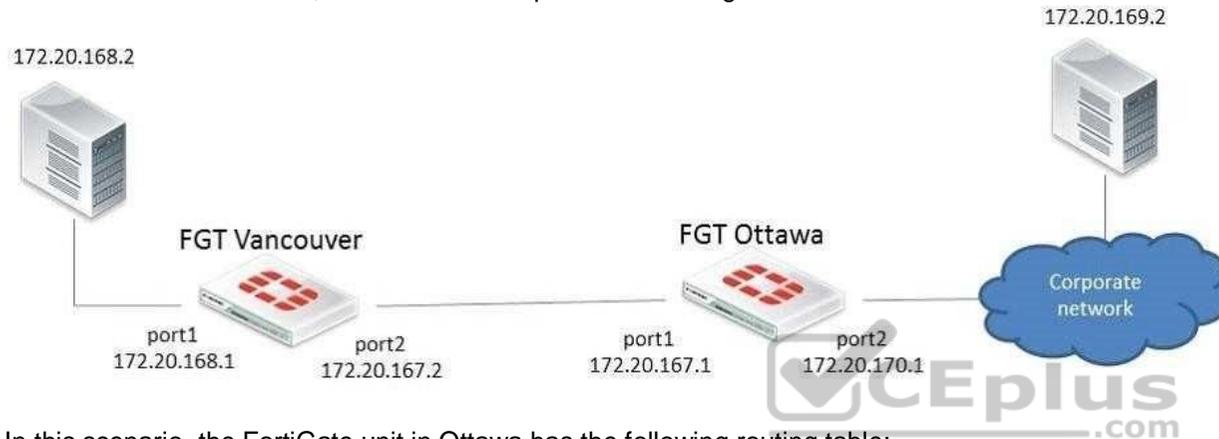
Correct Answer: C

Section: (none)
Explanation

Explanation/Reference:

QUESTION 67

Examine the exhibit below; then answer the question following it.



In this scenario, the FortiGate unit in Ottawa has the following routing table:

```
S* 0.0.0.0/0 [10/0] via 172.20.170.254, port2
C 172.20.167.0/24 is directly connected, port1
C 172.20.170.0/24 is directly connected, port2
```

Sniffer tests show that packets sent from the source IP address 172.20.168.2 to the destination IP address 172.20.169.2 are being dropped by the FortiGate located in Ottawa. Which of the following correctly describes the cause for the dropped packets?



<https://vceplus.com/>

- A. The forward policy check.
- B. The reverse path forwarding check.
- C. The subnet 172.20.169.0/24 is NOT in the Ottawa FortiGate's routing table.
- D. The destination workstation 172.20.169.2 does NOT have the subnet 172.20.168.0/24 in its routing table.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 68

Review the output of the command get router info routing-table database shown in the exhibit below; then answer the question following it.

```
STUDENT # 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 10.200.1.254, port1
    *>           [10/0] via 10.200.2.254, port2, [5/0]
C   *> 10.0.1.0/24 is directly connected, port3
S   *> 10.0.2.0/24 [20/0] is directly connected, Remote_2
S   *> 10.0.2.0/24 [10/0] is directly connected, Remote_1
C   *> 10.200.1.0/24 is directly connected, port1
C   *> 10.200.2.0/24 is directly connected, port2
```

Which two statements are correct regarding this output? (Choose two.)

- A. There will be six routes in the routing table.
- B. There will be seven routes in the routing table.
- C. There will be two default routes in the routing table.
- D. There will be two routes for the 10.0.2.0/24 subnet in the routing table.

Correct Answer: AC

Section: (none)

Explanation

Explanation/Reference:

QUESTION 69

Examine the exhibit; then answer the question below.



The Vancouver FortiGate initially had the following information in its routing table:

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

Afterwards, the following static route was added:

```
config router static
edit 6
set dst 172.20.1.0 255.255.255.0
set priority 0
set device port1
set gateway 172.11.12.1
next
end
```



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

- A. The subnet 172.20.1.0/24 is overlapped with the subnet of one static route that is already in the routing table (172.20.0.0/16), so, we need to enable `allowsubnet-overlap` first.
- B. The 'gateway' IP address is NOT in the same subnet as the IP address of port1.
- C. The priority is 0, which means that the route will remain inactive.
- D. The static route configuration is missing the distance setting.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 70

A FortiGate is configured with three virtual domains (VDOMs). Which of the following statements is correct regarding multiple VDOMs?

- A. The FortiGate must be a model 1000 or above to support multiple VDOMs.
- B. A license has to be purchased and applied to the FortiGate before VDOM mode could be enabled.
- C. Changing the operational mode of a VDOM requires a reboot of the FortiGate.
- D. The FortiGate supports any combination of VDOMs in NAT/Route and transparent modes.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:



QUESTION 71

Which statements are correct regarding virtual domains (VDOMs)? (Choose two.)

- A. VDOMs divide a single FortiGate unit into two or more virtual units that each have dedicated memory and CPUs.
- B. A management VDOM handles SNMP, logging, alert email, and FDN-based updates.
- C. VDOMs share firmware versions, as well as antivirus and IPS databases.
- D. Different time zones can be configured in each VDOM.

Correct Answer: BC

Section: (none)

Explanation

Explanation/Reference:

QUESTION 72

A FortiGate is configured with multiple VDOMs. An administrative account on the device has been assigned a Scope value of VDOM:root. Which of the following settings will this administrator be able to configure? (Choose two.)

- A. Firewall addresses.
- B. DHCP servers.
- C. FortiGuard Distribution Network configuration.
- D. System hostname.

Correct Answer: AB

Section: (none)

Explanation

Explanation/Reference:

QUESTION 73

A FortiGate administrator with the super_admin profile configures a virtual domain (VDM) for a new customer. After creating the VDM, the administrator is unable to reassign the dmz interface to the new VDM as the option is greyed out in the GUI in the management VDM. What would be a possible cause for this problem?

- A. The administrator does not have the proper permissions to reassign the dmz interface.
- B. The dmz interface is referenced in the configuration of another VDM.
- C. Non-management VDMs cannot reference physical interfaces.
- D. The dmz interface is in PPPoE or DHCP mode.

Correct Answer: B

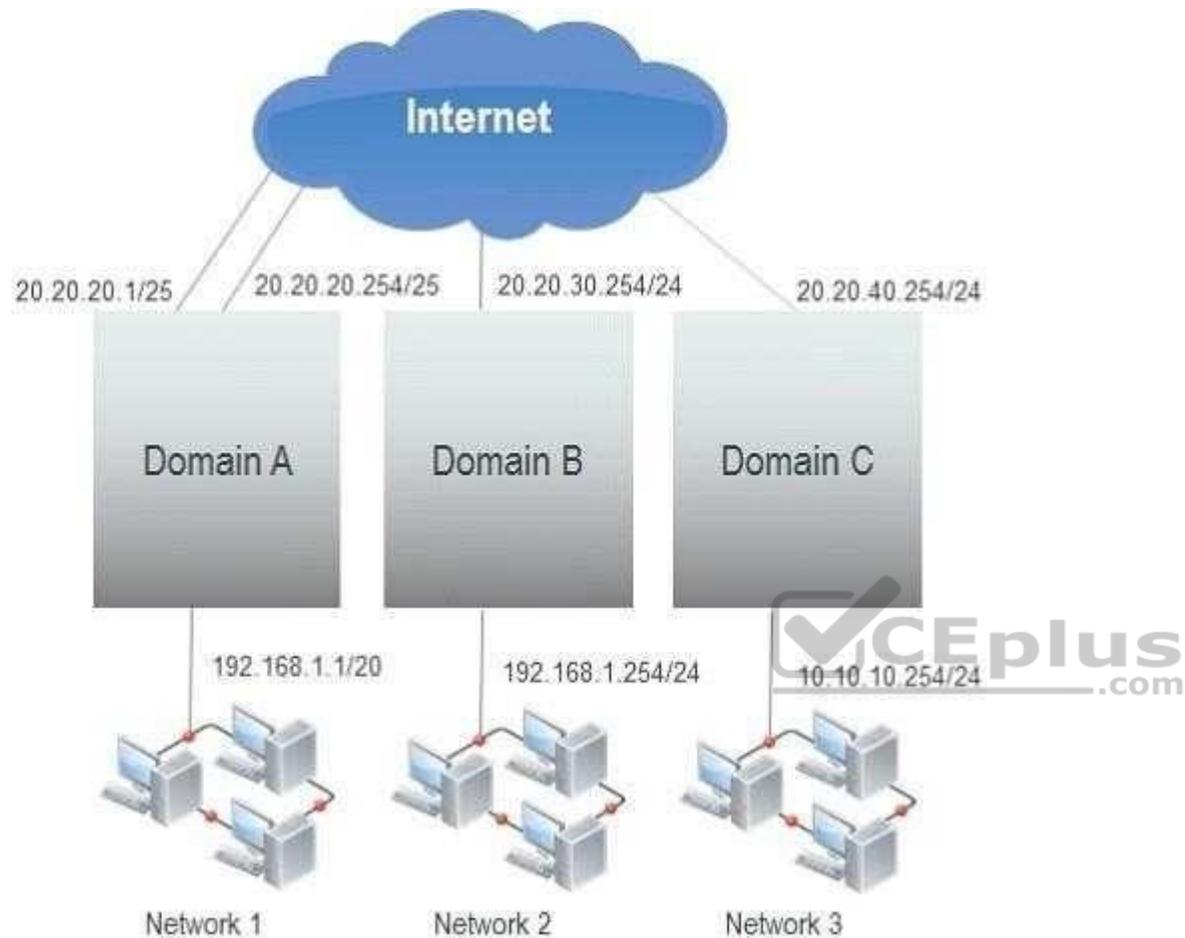
Section: (none)

Explanation

Explanation/Reference:

QUESTION 74

A FortiGate unit is configured with three Virtual Domains (VDMs) as illustrated in the exhibit.



Which of the following statements are true if the network administrator wants to route traffic between all the VDOMs? (Choose three.)

- A. The administrator can configure inter-VDOM links to avoid using external interfaces and routers.
- B. As with all FortiGate unit interfaces, firewall policies must be in place for traffic to be allowed to pass through any interface, including inter-VDOM links.
- C. This configuration requires a router to be positioned between the FortiGate unit and the Internet for proper routing.
- D. Inter-VDOM routing is automatically provided if all the subnets that need to be routed are locally attached.
- E. As each VDOM has an independent routing table, routing rules need to be set (for example, static routing, OSPF) in each VDOM to route traffic between VDOMs.

Correct Answer: ABE

Section: (none)

Explanation

Explanation/Reference:

QUESTION 75

A FortiGate is operating in NAT/Route mode and configured with two virtual LAN (VLAN) sub- interfaces added to the same physical interface. Which one of the following statements is correct regarding the VLAN IDs in this scenario?

- 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 if they are connected to different L2 IEEE 802.1Q compliant switches.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:



QUESTION 76

Which statements are correct for port pairing and forwarding domains? (Choose two.)

- A. They both create separate broadcast domains.
- B. Port Pairing works only for physical interfaces.
- C. Forwarding Domain only applies to virtual interfaces.
- D. They may contain physical and/or virtual interfaces.

Correct Answer: AD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 77

In transparent mode, forward-domain is an CLI setting associate with _____.

- A. static route

- B. a firewall policy
- C. an interface
- D. a virtual domain

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 78

Which of the following sequences describes the correct order of criteria used for the selection of a master unit within a FortiGate high availability (HA) cluster when override is disabled?

- A. 1. port monitor, 2. unit priority, 3. up time, 4. serial number.
- B. 1. port monitor, 2. up time, 3. unit priority, 4. serial number.
- C. 1. unit priority, 2. up time, 3. port monitor, 4. serial number.
- D. 1. up time, 2. unit priority, 3. port monitor, 4. serial number.



Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 79

Which of the following statements are correct about the HA command diagnose sys ha reset- uptime? (Choose two.)

- A. The device this command is executed on is likely to switch from master to slave status if override is disabled.
- B. The device this command is executed on is likely to switch from master to slave status if override is enabled.
- C. This command has no impact on the HA algorithm.
- D. This command resets the uptime variable used in the HA algorithm so it may cause a new master to become elected.

Correct Answer: AD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 80

What are the requirements for a HA cluster to maintain TCP connections after device or link failover? (Choose two.)

- A. Enable session pick-up.
- B. Enable override.
- C. Connections must be UDP or ICMP.
- D. Connections must not be handled by a proxy.

Correct Answer: AD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 81

Review the static route configuration for IPsec shown in the exhibit; then answer the question below.

Destination IP/Mask	10.0.2.0/255.255.255
Device	remote
Distance	10 (1-255, Default=10)
Priority	0 (0-4294967295)
Comments	VPN: remote (Created by VPN wizard) 35/255

Which statements are correct regarding this configuration? (Choose two.)

- A. Interface remote is an IPsec interface.
- B. A gateway address is not required because the interface is a point-to-point connection.
- C. A gateway address is not required because the default route is used.
- D. Interface remote is a zone.

Correct Answer: AB

Section: (none)

Explanation

Explanation/Reference:

QUESTION 82

Review the IPsec diagnostics output of the command diagnose vpn tunnel list shown in the exhibit.



```
STUDENT # diagnose vpn tunnel list
list all ipsec tunnel in vd 0
-----
name=Remote_1 ver=1 serial=1 10.200.1.1:0->10.200.3.1:0 lgy=static tun=intf mode=auto bound_if=2
proxyid_num=1 child_num=0 refcnt=6 ilast=2 olast=2
stat: rxp=8 txp=8 rxb=960 txb=480
dpd: mode=active on=1 idle=5000ms retry=3 count=0 seqno=128
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=P2_Remote_1 proto=0 sa=1 ref=2 auto_negotiate=0 serial=1
  src: 0:0.0.0.0/0.0.0.0:0
  dst: 0:0.0.0.0/0.0.0.0:0
  SA: ref=3 options=0000000f type=00 soft=0 mtu=1412 expire=1486 replaywin=1024 seqno=1
  life: type=01 bytes=0/0 timeout=1753/1800
  dec: spi=b95a77fe esp=aes key=32 84ed410c1bb9f61e635a49563c4e7646e9e110628b79b0ac03482d05e3b6a0e6
      ah=sha1 key=20 6bddbfad7161237daa46c19725dd0292b062dda5
  enc: spi=9293e7d4 esp=aes key=32 951befd87860cdb59b98b170a17dcb75f77bd541bdc3a1847e54c78c0d43aa13
      ah=sha1 key=20 8a5bedd6a0ce0f8daf7593601acfe2c618a0d4e2
-----
name=Remote_2 ver=1 serial=2 10.200.2.1:0->10.200.4.1:0 lgy=static tun=intf mode=auto bound_if=3
proxyid_num=1 child_num=0 refcnt=6 ilast=0 olast=0
stat: rxp=0 txp=0 rxb=0 txb=0
dpd: mode=active on=1 idle=5000ms retry=3 count=0 seqno=0
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=P2_Remote_2 proto=0 sa=1 ref=2 auto_negotiate=0 serial=1
  src: 0:0.0.0.0/0.0.0.0:0
  dst: 0:0.0.0.0/0.0.0.0:0
  SA: ref=3 options=0000000f type=00 soft=0 mtu=1280 expire=1732 replaywin=1024 seqno=1
  life: type=01 bytes=0/0 timeout=1749/1800
  dec: spi=b95a77ff esp=aes key=32 582af59d71635b835c9208878e0e3f3fe31ba1dfd88ff83ca9bab1ed66ac325e
      ah=sha1 key=20 0d951e62a1bcb63232df6d0fb86df49ab714f53b
  enc: spi=9293e7d5 esp=aes key=32 eeeecacf3a58161f3390fa612b794c776654c86aef51fbc7542906223d56ebb3
      ah=sha1 key=20 09eaa3085bc30a59091f182eb3d11550385b8304
```

Which of the following statements is correct regarding this output? (Select one answer).

- A. One tunnel is rekeying.
- B. Two tunnels are rekeying.
- C. Two tunnels are up.
- D. One tunnel is up.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 83

Review the IPsec phase 2 configuration shown in the exhibit; then answer the question below.



Phase 2 Selectors

Name	Local Address	Remote Address
	0.0.0.0/0.0.0.0	0.0.0.0/0.0.0.0

Edit Phase 2 ✓ X

Name: remote

Comments: VPN: remote (Created by VPN wizard)

Local Address: Subnet 0.0.0.0/0.0.0.0

Remote Address: Subnet 0.0.0.0/0.0.0.0

Advanced...

Phase 2 Proposal

Encryption: AES256 Authentication: SHA512  Add

Enable Replay Detection

Enable Perfect Forward Secrecy (PFS)

Diffie-Hellman Group: 21 20 19 18 17
 16 15 14 5 2 1

Local Port: All

Remote Port: All

Protocol: All

Autokey Keep Alive:

Auto-negotiate:

Key Lifetime: Seconds

Seconds: 43200

Which statements are correct regarding this configuration? (Choose two.).

- A. The Phase 2 will re-key even if there is no traffic.
- B. There will be a DH exchange for each re-key.
- C. The sequence number of ESP packets received from the peer will not be checked.
- D. Quick mode selectors will default to those used in the firewall policy.

Correct Answer: AB

Section: (none)

Explanation

Explanation/Reference:

QUESTION 84

Which statement is an advantage of using a hub and spoke IPsec VPN configuration instead of a fully-meshed set of IPsec tunnels?



<https://vceplus.com/>

- A. Using a hub and spoke topology provides full redundancy.
- B. Using a hub and spoke topology requires fewer tunnels.
- C. Using a hub and spoke topology uses stronger encryption protocols.
- D. Using a hub and spoke topology requires more routes.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

```
STUDENT # ike 0: comes 10.200.3.1:500->10.200.1.1:500,ifindex=2...
ike 0: IKEv1 exchange=Informational id=9e2606ac7ae83d7a/612da78d3ab3f945:15b10705 len=92
ike 0: in 9E2606AC7AE83D7A612DA78D3AB3F9450810050115B107050000005C26E2A7EC8461AC15E9BBC705B6C1F667A41957AED11FB7003C07
37BD934DD38E1A2074348E08FD6B39146C618525C6EC51E2F26885B6BB8E035F52B4
ike 0:Remote_1:10: dec 9E2606AC7AE83D7A612DA78D3AB3F9450810050115B107050000005C0B000018E281874EECF170EB5222D6A4E3A027C
0000000200000000101108D289E2606AC7AE83D7A612DA78D3AB3F9450000009C17511ED8EE549507
ike 0:Remote_1:10: notify msg received: R-U-THERE
ike 0:Remote_1:10: enc 9E2606AC7AE83D7A612DA78D3AB3F94508100501734C5CDF000000540B0000181C047F014CBEF1B0EC8DA915F3B18AE
A000000200000000101108D299E2606AC7AE83D7A612DA78D3AB3F9450000009C
ike 0:Remote_1:10: out 9E2606AC7AE83D7A612DA78D3AB3F94508100501734C5CDF0000005CB3CC431065A1737144B02F1AACE79C1BE712B84
BB84E5FA7A967FE99C7B731057FF33728BB42AA983E79C919DA9B64EBCE087EFOA02666C1FBD2C62F
ike 0:Remote_1:10: sent IKE msg (R-U-THERE-ACK): 10.200.1.1:500->10.200.3.1:500, len=92, id=9e2606ac7ae83d7a/612da78d3
734c5cdf
ike 0:Remote_1: link is idle 2 10.200.1.1->10.200.3.1:500 dpd=1 seqno=34
```

QUESTION 85

Review the IKE debug output for IPsec shown in the exhibit below.
Which statements is correct regarding this output?

- A. The output is a phase 1 negotiation.
- B. The output is a phase 2 negotiation.
- C. The output captures the dead peer detection messages.
- D. The output captures the dead gateway detection packets.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 86

Review the configuration for FortiClient IPsec shown in the exhibit.



New FortiClient VPN

Name	<input type="text" value="FClient"/>
Local Outgoing Interface	<input type="text" value="port1"/>
Authentication Method	<input type="text" value="Pre-shared Key"/>
Pre-shared Key	<input type="password" value="....."/>
User Group	<input type="text" value="training"/>
Address Range Start IP	<input type="text" value="172.20.1.1"/>
Address Range End IP	<input type="text" value="172.20.1.5"/>
Subnet Mask	<input type="text" value="255.255.255.0"/>
<input checked="" type="checkbox"/> Enable IPv4 Split Tunnel	
Accessible Networks	<input type="text" value="STUDENT_INTERNAL"/>
DNS Server	<input checked="" type="radio"/> Use System DNS <input type="radio"/> Specify <input type="text" value="0.0.0.0"/>

Which statement is correct regarding this configuration?

- A. The connecting VPN client will install a route to a destination corresponding to the student_internal address object.
- B. The connecting VPN client will install a default route.
- C. The connecting VPN client will install a route to the 172.20.1.[1-5] address range.
- D. The connecting VPN client will connect in web portal mode and no route will be installed.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 87

Review the IPsec phase 1 configuration in the exhibit; then answer the question below.

Name	remote
Comments	VPN: remote (Created by VPN wizard)



The image shows a configuration window titled "Network" with a yellow background. It contains the following settings:

IP Version	IPv4
Remote Gateway	Static IP Address
IP Address	10.200.3.1
Interface	port1
Mode Config	<input type="checkbox"/>
NAT Traversal	<input checked="" type="checkbox"/>
Keepalive Frequency	10
Dead Peer Detection	<input checked="" type="checkbox"/>

Which statements are correct regarding this configuration? (Choose two.)

- A. The remote gateway address on 10.200.3.1.
- B. The local IPsec interface address is 10.200.3.1.
- C. The local gateway IP is the address assigned to port1.
- D. The local gateway IP address is 10.200.3.1.

Correct Answer: AC

Section: (none)

Explanation

Explanation/Reference:

QUESTION 88

Review the IPsec diagnostics output of the command diagnose vpn tunnel list shown in the exhibit below.

```
STUDENT # diagnose vpn tunnel list
list all ipsec tunnel in vd 0
-----
name=FCClient_0 ver=1 serial=3 10.200.1.1:4500->10.200.3.1:64916 lgwy=static tun=intf mode=dial_inst bound_if=2
parent=FCClient index=0
proxyid_num=1 child_num=0 refcnt=8 ilast=2 olast=2
stat: rxp=59 txp=0 rxb=15192 txb=0
dpd: mode=active on=1 idle=5000ms retry=3 count=0 seqno=10
natt: mode=keepalive draft=32 interval=10 remote_port=64916
proxyid=FCClient proto=0 sa=1 ref=2 auto_negotiate=0 serial=1
  src: 0:0.0.0.0-255.255.255.255:0
  dst: 0:172.20.1.1-172.20.1.1:0
  SA: ref=3 options=00000006 type=00 soft=0 mtu=1280 expire=1717 replaywin=1024 seqno=1
  life: type=01 bytes=0/0 timeout=1791/1800
  dec: spi=a29046e9 esp=3des key=24 0525830c6fd67ca37e9d6dad174d175e24f97c3b87f428fa
      ah=sha1 key=20 982f8ba194f3f797773efc605c8321b728dabf1d
  enc: spi=19be4052 esp=3des key=24 da597cb7fec913528f8598d1aa7ecd17156a2a7a4afeeb4c
      ah=sha1 key=20 9e2c5d0fc055fa0149bc66024732e9a85bbe8016
-----
```



Which statements are correct regarding this output? (Choose two.)

- A. The connecting client has been allocated address 172.20.1.1.
- B. In the Phase 1 settings, dead peer detection is enabled.
- C. The tunnel is idle.
- D. The connecting client has been allocated address 10.200.3.1.

Correct Answer: AB

Section: (none)

Explanation

Explanation/Reference:

QUESTION 89

Which IPsec mode includes the peer id information in the first packet?

- A. Main mode.
- B. Quick mode.

- C. Aggressive mode.
- D. IKEv2 mode.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 90

Which statements are correct properties of a partial mesh VPN deployment. (Choose two.)

- A. VPN tunnels interconnect between every single location.
- B. VPN tunnels are not configured between every single location.
- C. Some locations are reached via a hub location.
- D. There are no hub locations in a partial mesh.

Correct Answer: BC

Section: (none)

Explanation



Explanation/Reference:

QUESTION 91

Examine the following log message for IPS and identify the valid responses below. (Select all that apply.)

```
2012-07-01 09:54:28 oid=2 log_id=18433 type=ips subtype=anomaly
pri=alert vd=root severity="critical" src="192.168.3.168"
dst="192.168.3.170" src_int="port2" serial=0 status="detected" proto=1
service="icmp" count=1 attack_name="icmp_flood" icmp_id="0xa8a4"
icmp_type="0x08" icmp_code="0x00" attack_id=16777316 sensor="1"
ref="http://www.fortinet.com/ids/VID16777316" msg="anomaly:
icmp_flood,
51 > threshold 50"
```

- A. The target is 192.168.3.168.

- B. The target is 192.168.3.170.
- C. The attack was detected and blocked.
- D. The attack was detected only.
- E. The attack was TCP based.

Correct Answer: BD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 92

Identify the statement which correctly describes the output of the following command:

```
diagnose ips anomaly list
```

- A. Lists the configured DoS policy.
- B. List the real-time counters for the configured DoS policy.
- C. Lists the errors captured when compiling the DoS policy.
- D. Lists the IPS signature matches.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 93

Review the IPS sensor filter configuration shown in the exhibit

Pattern Based Signatures and Filters

 Create New  Edit  Delete				
Severity	Target	OS	Action	Packet Logging
Critical	Server	Linux	 Block	

Based on the information in the exhibit, which statements are correct regarding the filter? (Choose two.)

- A. It does not log attacks targeting Linux servers.
- B. It matches all traffic to Linux servers.
- C. Its action will block traffic matching these signatures.
- D. It only takes effect when the sensor is applied to a policy.

Correct Answer: CD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 94

Which of the following statements are true regarding application control? (choose two)

- A. Application control is based on TCP destination port numbers.
- B. Application control is proxy based.
- C. Encrypted traffic can be identified by application control.
- D. Traffic Shaping can be applied to the detected application traffic.



Correct Answer: CD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 95

FSSO provides a single sign on solution to authenticate users transparently to a FortiGate unit using credentials stored in Windows active directory.

Which of the following statements are correct regarding FSSO in a Windows domain environment when agent mode is used? (Choose two.)

- A. An FSSO collector agent must be installed on every domain controller.
- B. An FSSO domain controller agent must be installed on every domain controller.
- C. The FSSO domain controller agent will regularly update user logon information on the FortiGate unit.
- D. The FSSO collector agent will receive user logon information from the domain controller agent and will send it to the FortiGate unit.

Correct Answer: BD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 96

Which statement is one disadvantage of using FSSO NetAPI polling mode over FSSO Security Event Log (WinSecLog) polling mode?

- A. It requires a DC agent installed in some of the Windows DC.
- B. It runs slower.
- C. It might miss some logon events.
- D. It requires access to a DNS server for workstation name resolution.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:



QUESTION 97

Which are two requirements for DC-agent mode FSSO to work properly in a Windows AD environment? (Choose two.)

- A. DNS server must properly resolve all workstation names.
- B. The remote registry service must be running in all workstations.
- C. The collector agent must be installed in one of the Windows domain controllers.
- D. A same user cannot be logged in into two different workstations at the same time.

Correct Answer: AB

Section: (none)

Explanation

Explanation/Reference:

QUESTION 98

Which statement describes what the CLI command diagnose debug authd fssolist is used for

- A. Monitors communications between the FSSO collector agent and FortiGate unit.
- B. Displays which users are currently logged on using FSSO.
- C. Displays a listing of all connected FSSO collector agents.
- D. Lists all DC Agents installed on all domain controllers.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 99

When the SSL proxy is NOT doing man-in-the-middle interception of SSL traffic, which certificate field can be used to determine the rating of a website?

- A. Organizational Unit.
- B. Common Name.
- C. Serial Number.
- D. Validity.



Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 100

Which tasks fall under the responsibility of the SSL proxy in a typical HTTPS connection? (Choose two.)

- A. The web client SSL handshake.
- B. The web server SSL handshake.
- C. File buffering.
- D. Communication with the URL filter process.

Correct Answer: AB

Section: (none)

Explanation

Explanation/Reference:

QUESTION 101

Bob wants to send Alice a file that is encrypted using public key cryptography.

Which of the following statements is correct regarding the use of public key cryptography in this scenario?

- A. Bob will use his private key to encrypt the file and Alice will use her private key to decrypt the file.
- B. Bob will use his public key to encrypt the file and Alice will use Bob's private key to decrypt the file.
- C. Bob will use Alice's public key to encrypt the file and Alice will use her private key to decrypt the file.
- D. Bob will use his public key to encrypt the file and Alice will use her private key to decrypt the file.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 102

Which Fortinet products & features could be considered part of a comprehensive solution to monitor and prevent the leakage of sensitive data? (Select all that apply.)

- A. Archive non-compliant outgoing e-mails using FortiMail.



<https://vceplus.com/>

- B. Restrict unofficial methods of transferring files such as P2P using Application Control lists on a FortiGate.
- C. Monitor database activity using FortiAnalyzer.
- D. Apply a DLP sensor to a firewall policy.
- E. Configure FortiClient to prevent files flagged as sensitive from being copied to a USB disk.

Correct Answer: ABD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 103

For data leak prevention, which statement describes the difference between the block and quarantine actions?

- A. A block action prevents the transaction.
A quarantine action blocks all future transactions, regardless of the protocol.
- B. A block action prevents the transaction. A quarantine action archives the data.
- C. A block action has a finite duration.
A quarantine action must be removed by an administrator.
- D. A block action is used for known users.
A quarantine action is used for unknown users.

Correct Answer: A

Section: (none)

Explanation



Explanation/Reference:

QUESTION 104

In which process states is it impossible to interrupt/kill a process? (Choose two.)

- A. S-Sleep
- B. R-Running
- C. D-Uninterruptable Sleep
- D. Z-Zombie

Correct Answer: CD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 105

Examine at the output below from the diagnose sys top command:

```
# diagnose sys top 1
Run Time: 11 days, 3 hours and 29 minutes
OU, ON, 1S, 99I; 971T, 528F, 160KF
sshd 123 S 1.9 1.2
ipsengine 61 S < 0.0 5.2
miglogd 45 S 0.0 4.9
pyfcgid 75 S 0.0 4.5
pyfcgid 73 S 0.0 3.9
```

Which statements are true regarding the output above? (Choose two.)

- A. The sshd process is the one consuming most CPU.
- B. The sshd process is using 123 pages of memory.
- C. The command diagnose sys kill miglogd will restart the miglogd process.
- D. All the processes listed are in sleeping state.

Correct Answer: AD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 106

Examine the following output from the diagnose sys session list command:



```
session info: proto=6 proto_state=65 duration=3 expire=9 timeout=3600
flags=00000000 sockflag=00000000 sockport=443 av_idx=9 use=5
origin-shaper=guarantee-100kbps prio=2 guarantee 12800Bps max
134217728Bps traffic 13895Bps
reply-shaper=guarantee-100kbps prio=2 guarantee 12800Bps max
134217728Bps traffic 13895Bps
state=redir local may_dirty ndr npu nlb os rs
statistic(bytes/packets/allow_err): org=864/8/1 reply=2384/7/1 tuples=3
origin->sink: org pre->post, reply pre->post dev=7->6/6->7
gwy=172.17.87.3/10.1.10.1
hook=post dir=org act=snat
192.168.1.110:57999->74.201.86.29:443(172.17.87.16:57999)
hook=pre dir=reply act=dnat 74.201.86.29:443-
>172.17.87.16:57999(192.168.1.110:57999)
hook=post dir=reply act=noop
74.201.86.29:443->192.168.1.110:57999(0.0.0.0:0)
misc=0 policy_id=1 id_policy_id=0 auth_info=0 chk_client_info=0 vd=0
npu info: flag=0x00/0x00, offload=0/0, ips_offload=0/0, epid=0/0,
ipid=0/0, vlan=0/0
```

Which statements are true regarding the session above? (Choose two.)

- A. Session Time-To-Live (TTL) was configured to 9 seconds.
- B. FortiGate is doing NAT of both the source and destination IP addresses on all packets coming from the 192.168.1.110 address.
- C. The IP address 192.168.1.110 is being translated to 172.17.87.16.
- D. The FortiGate is not translating the TCP port numbers of the packets in this session.

Correct Answer: CD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 107

Which statements are correct regarding an IPv6 over IPv4 IPsec configuration? (Choose two.)

- A. The source quick mode selector must be an IPv4 address.
- B. The destination quick mode selector must be an IPv6 address.
- C. The Local Gateway IP must be an IPv4 address.
- D. The remote gateway IP must be an IPv6 address.

Correct Answer: BC

Section: (none)

Explanation

Explanation/Reference:

QUESTION 108

Which statements are true regarding IPv6 anycast addresses? (Choose two.)

- A. Multiple interfaces can share the same anycast address.
- B. They are allocated from the multicast address space.
- C. Different nodes cannot share the same anycast address.
- D. An anycast packet is routed to the nearest interface.



Correct Answer: AD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 109

What functions can the IPv6 Neighbor Discovery protocol accomplish? (Choose two.)

- A. Negotiate the encryption parameters to use.
- B. Auto-adjust the MTU setting.
- C. Autoconfigure addresses and prefixes.
- D. Determine other nodes reachability.

Correct Answer: CD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 110

Which is one of the conditions that must be met for offloading the encryption and decryption of IPsec traffic to an NP6 processor?

- A. No protection profile can be applied over the IPsec traffic.
- B. Phase-2 anti-replay must be disabled.
- C. Both the phase 1 and phases 2 must use encryption algorithms supported by the NP6.
- D. IPsec traffic must not be inspected by any FortiGate session helper.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:



QUESTION 111

Which statements are true about offloading antivirus inspection to a Security Processor (SP)? (Choose two.)

- A. Both proxy-based and flow-based inspection are supported.
- B. A replacement message cannot be presented to users when a virus has been detected.
- C. It saves CPU resources.
- D. The ingress and egress interfaces can be in different SPs.

Correct Answer: BC

Section: (none)

Explanation

Explanation/Reference:

QUESTION 112

Which IP packets can be hardware-accelerated by a NP6 processor? (Choose two.)

- A. Fragmented packet.

- B. Multicast packet.C. SCTP packet
- D. GRE packet.

Correct Answer: BC

Section: (none)

Explanation

Explanation/Reference:

QUESTION 113

Each UTM feature has configurable UTM objects such as sensors, profiles or lists that define how the feature will function.

An administrator must assign a set of UTM features to a group of users. Which of the following is the correct method for doing this?

- A. Enable a set of unique UTM features under "Edit User Group".
- B. The administrator must enable the UTM features in an identify-based policy applicable to the user group.
- C. When defining the UTM objects, the administrator must list the user groups which will use the UTM object.
- D. The administrator must apply the UTM features directly to a user object.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 114

Which of the following items represent the minimum configuration steps an administrator must perform to enable Data Leak Prevention for traffic flowing through the FortiGate unit? (Select all that apply.)

- A. Assign a DLP sensor in a firewall policy.
- B. Apply one or more DLP rules to a firewall policy.
- C. Enable DLP globally using the config sys dlp command in the CLI.
- D. Define one or more DLP rules.
- E. Define a DLP sensor.
- F. Apply a DLP sensor to a DoS sensor policy.

Correct Answer: ADE

Section: (none)

Explanation

Explanation/Reference:

QUESTION 115

Because changing the operational mode to Transparent resets device (or vdom) to all defaults, which precautions should an Administrator take prior to performing this? (Select all that apply.)

- A. Backup the configuration.
- B. Disconnect redundant cables to ensure the topology will not contain layer 2 loops.
- C. Set the unit to factory defaults.
- D. Update IPS and AV files.

Correct Answer: AB

Section: (none)

Explanation

Explanation/Reference:



QUESTION 116

Which of the following statements best describes the proxy behavior on a FortiGate unit during an FTP client upload when FTP splice is disabled?

- A. The proxy will not allow a file to be transmitted in multiple streams simultaneously.
- B. The proxy sends the file to the server while simultaneously buffering it.
- C. If the file being scanned is determined to be infected, the proxy deletes it from the server by sending a delete command on behalf of the client.
- D. If the file being scanned is determined to be clean, the proxy terminates the connection and leaves the file on the server.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 117

Which part of an email message exchange is NOT inspected by the POP3 and IMAP proxies?



<https://vceplus.com/>

- A. TCP connection
- B. File attachments
- C. Message headers
- D. Message body

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:



QUESTION 118

The FortiGate Web Config provides a link to update the firmware in the System > Status window. Clicking this link will perform which of the following actions?

- A. It will connect to the Fortinet support site where the appropriate firmware version can be selected.
- B. It will send a request to the FortiGuard Distribution Network so that the appropriate firmware version can be pushed down to the FortiGate unit.
- C. It will present a prompt to allow browsing to the location of the firmware file.
- D. It will automatically connect to the Fortinet support site to download the most recent firmware version for the FortiGate unit.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 119

Which of the following statements correctly describes how a push update from the FortiGuard Distribution Network (FDN) works?

- A. The FDN sends push updates only once.
- B. The FDN sends package updates automatically to the FortiGate unit without requiring an update request.
- C. The FDN continues to send push updates until the FortiGate unit sends an acknowledgement.
- D. The FDN sends a message to the FortiGate unit that there is an update available and that the FortiGate unit should download the update.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 120

Which of the following statements best describes the green status indicators that appear next to different FortiGuard Distribution Network services as illustrated in the exhibit?



Backup & Restore Revision Control **FortiGuard**

FortiGuard Distribution Network

Support Contract		
Availability	Valid Contract FortiOS 3.000 (Expires 2009-03-11)	✔
FortiGuard Subscription Services		
AntiVirus	Valid License (Expires 2009-03-11)	✔
AV Definitions	8.836 (Updated 2008-03-12 via <i>Manual Update</i>) [Update]	✔
Extended set	9.004 (Updated 2008-04-22 via <i>Manual Update</i>)	

Intrusion Protection	Valid License (Expires 2009-03-11)	✔
IPS Definitions	2.506 (Updated 2008-05-27 via <i>Manual Update</i>) [Update]	✔

Web Filtering	Valid License (Expires 2009-03-11)	✔

AntiSpam	Valid License (Expires 2009-03-11)	✔

Management Service	Unreachable [Update]	⊗

Analysis Service	Expired [Renew] [Update]	⊙

▶ **AntiVirus and IPS Options**
 ▶ **Web Filtering and AntiSpam Options**
 ▶ **Management and Analysis Service Options**

Apply

- A. They indicate that the FortiGate unit is able to connect to the FortiGuard Distribution Network.
- B. They indicate that the FortiGate unit has the latest updates that are available from the FortiGuard Distribution Network.
- C. They indicate that updates are available and should be downloaded from the FortiGuard Distribution Network to the FortiGate unit.
- D. They indicate that the FortiGate unit is in the process of downloading updates from the FortiGuard Distribution Network.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 121

Data Leak Prevention archiving gives the ability to store files and message data onto a FortiAnalyzer unit for which of the following types of network traffic? (Select all that apply.)

- A. SNMP
- B. IPSec
- C. SMTP
- D. POP3
- E. HTTP

Correct Answer: CDE

Section: (none)

Explanation

Explanation/Reference:



QUESTION 122

Which of the following statements are correct regarding Application Control?

- A. Application Control is based on the IPS engine.
- B. Application Control is based on the AV engine.
- C. Application Control can be applied to SSL encrypted traffic.
- D. Application Control cannot be applied to SSL encrypted traffic.

Correct Answer: AC

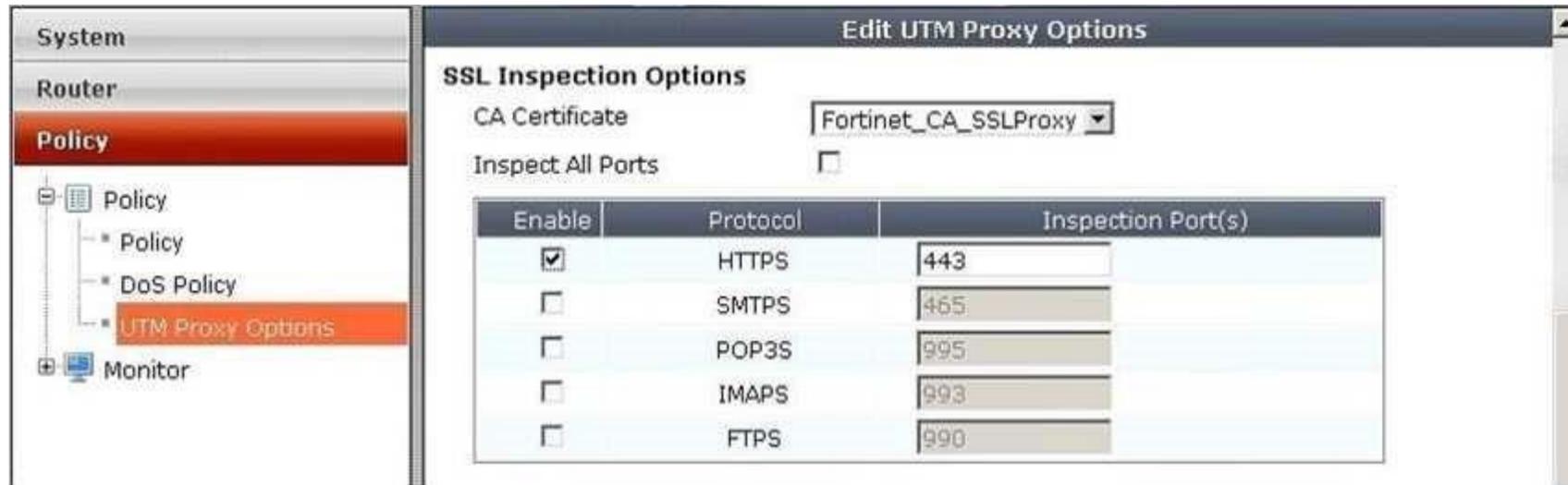
Section: (none)

Explanation

Explanation/Reference:

QUESTION 123

Examine the exhibit shown below then answer the question that follows it.



Within the UTM Proxy Options, the CA certificate Fortinet_CA_SSLProxy defines which of the following:

- A. FortiGate unit's encryption certificate used by the SSL proxy.
- B. FortiGate unit's signing certificate used by the SSL proxy.
- C. FortiGuard's signing certificate used by the SSL proxy.
- D. FortiGuard's encryption certificate used by the SSL proxy.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 124

Shown below is a section of output from the debug command `diag ip arp list`.

```
index=2 ifname=port1 172.20.187.150 00:09:0f:69:03:7e state=00000004
use=4589 confirm=4589 update=2422 ref=1
```

In the output provided, which of the following best describes the IP address 172.20.187.150?

- A. It is the primary IP address of the port1 interface.
- B. It is one of the secondary IP addresses of the port1 interface.
- C. It is the IP address of another network device located in the same LAN segment as the FortiGate unit's port1 interface.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 125

Review the output of the command get router info routing-table all shown in the Exhibit below; then answer the question following it.

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

S*    0.0.0.0/0 [10/0] via 10.200.1.254, port1
      [10/0] via 10.200.2.254, port2, [5/0]
C     10.0.1.0/24 is directly connected, port3
O     10.0.2.0/24 [110/101] via 172.16.2.1, Remote_1, 00:00:21
      [110/101] via 172.16.2.2, Remote_2, 00:00:21
C     10.200.1.0/24 is directly connected, port1
C     10.200.2.0/24 is directly connected, port2
C     172.16.1.1/32 is directly connected, Remote_1
C     172.16.1.2/32 is directly connected, Remote_2
C     172.16.2.1/32 is directly connected, Remote_1
C     172.16.2.2/32 is directly connected, Remote_2
```

Which one of the following statements correctly describes this output?

- A. The two routes to the 10.0.2.0/24 subnet are ECMP routes and traffic will be load balanced based on the configured ECMP settings.
- B. The route to the 10.0.2.0/24 subnet via interface Remote_1 is the active and the route via Remote_2 is the backup.
- C. OSPF does not support ECMP therefore only the first route to subnet 10.0.1.0/24 is used.

D. 172.16.2.1 is the preferred gateway for subnet 10.0.2.0/24.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 126

Review the IPsec phase1 configuration in the Exhibit shown below; then answer the question following it.



New Phase 1

Name

Comments 0/255

Remote Gateway

IP Address

Local Interface

Mode Aggressive Main (ID protection)

Authentication Method

Pre-shared Key

Peer Options

Accept any peer ID

Advanced... (XAUTH, NAT Traversal, DPD)

Enable IPsec Interface Mode

IKE Version 1 2

Local Gateway IP Main Interface IP Specify

P1 Proposal

1 - Encryption Authentication

DH Group 1 2 5 14

Keylife (120-172800 seconds)

Local ID (optional)

XAUTH Disable Enable as Client Enable as Server

NAT Traversal Enable

Keepalive Frequency (10-900 seconds)

Dead Peer Detection Enable

Which of the following statements are correct regarding this configuration? (Select all that apply).

- A. The phase1 is for a route-based VPN configuration.
- B. The phase1 is for a policy-based VPN configuration.

- C. The local gateway IP is the address assigned to port1.
- D. The local gateway IP address is 10.200.3.1.

Correct Answer: AC

Section: (none)

Explanation

Explanation/Reference:

QUESTION 127

Review the output of the command `config router ospf` shown in the Exhibit below; then answer the question following it.



```
STUDENT (ospf) # show
config router ospf
  config area
    edit 0.0.0.0
    next
  end
  config network
    edit 1
      set prefix 10.0.1.0 255.255.255.0
    next
    edit 2
      set prefix 172.16.0.0 255.240.0.0
    next
  end
  config ospf-interface
    edit "R1_OSPF"
      set interface "Remote_1"
      set ip 172.16.1.1
      set mtu 1436
      set network-type point-to-point
    next
    edit "R2_OSPF"
      set cost 20
      set interface "Remote_2"
      set ip 172.16.1.2
      set mtu 1436
      set network-type point-to-point
    next
  end
  config redistribute "connected"
  end
  config redistribute "static"
  end
  config redistribute "rip"
  end
  config redistribute "bgp"
  end
  config redistribute "isis"
  end
```

Which one of the following statements is correct regarding this output?

- A. OSPF Hello packets will only be sent on interfaces configured with the IP addresses 172.16.1.1 and 172.16.1.2.
- B. OSPF Hello packets will be sent on all interfaces of the FortiGate device.
- C. OSPF Hello packets will be sent on all interfaces configured with an address matching the 10.0.1.0/24 and 172.16.0.0/12 networks.
- D. OSPF Hello packets are not sent on point-to-point networks.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 128

Examine the static route configuration shown below; then answer the question following it. (Select all that apply.)

```
config router static
edit 1
set dst 172.20.1.0 255.255.255.0
set device port1
set gateway 172.11.12.1
set distance 10
set weight 5
next
edit 2
set dst 172.20.1.0 255.255.255.0
set blackhole enable
set distance 5
set weight 10
next
end
```



Which of the following statements correctly describes the static routing configuration provided? (Select all that apply.)

- A. All traffic to 172.20.1.0/24 will always be dropped by the FortiGate unit.

- B. As long as port1 is up, all the traffic to 172.20.1.0/24 will be routed by the static route number 1. If the interface port1 is down, the traffic will be routed using the blackhole route.
- C. The FortiGate unit will NOT create a session entry in the session table when the traffic is being routed by the blackhole route.
- D. The FortiGate unit will create a session entry in the session table when the traffic is being routed by the blackhole route.
- E. Traffic to 172.20.1.0/24 will be shared through both routes.

Correct Answer: AC

Section: (none)

Explanation

Explanation/Reference:

QUESTION 129

Which of the following statements are correct regarding virtual domains (VDMs)? (Select all that apply.)

- A. VDMs divide a single FortiGate unit into two or more virtual units that function as multiple, independent units.
- B. A management VDM handles SNMP, logging, alert email, and FDN-based updates.
- C. VDMs share firmware versions, as well as antivirus and IPS databases.
- D. Only administrative users with a 'super_admin' profile will be able to enter multiple VDMs to make configuration changes.

Correct Answer: ABC

Section: (none)

Explanation

Explanation/Reference:

QUESTION 130

Which of the following statements are TRUE for Port Pairing and Forwarding Domains? (Select all that apply.)

- A. They both create separate broadcast domains.
- B. Port Pairing works only for physical interfaces.
- C. Forwarding Domains only apply to virtual interfaces.
- D. They may contain physical and/or virtual interfaces.
- E. They are only available in high-end models.

Correct Answer: AD

Section: (none)
Explanation

Explanation/Reference:

QUESTION 131

Examine the Exhibits shown below, then answer the question that follows. Review the following DLP Sensor (Exhibit 1):

Seq #	Type	Action	Services	Archive
1	File Type	Log Only	SMTP, POP3, IMAP, HTTP, NNTP	Disable
2	File Type	Quarantine Interface	SMTP, POP3, IMAP, HTTP, NNTP	Disable
3	File Type	Block	SMTP, POP3, IMAP, HTTP, NNTP	Disable

Review the following File Filter list for rule #1 (Exhibit 2):

Filter Type	Filter
File Type	Audio (mp3)
File Type	Audio (wma)
File Type	Audio (wav)

Review the following File Filter list for rule #2 (Exhibit 3):

Filter Type	Filter
File Name Pattern	*.exe

Review the following File Filter list for rule #3 (Exhibit 4):

Filter Type	Filter
File Type	Archive (arj)
File Type	Archive (bzip)
File Type	Archive (cab)
File Type	Archive (zip)

An MP3 file is renamed to `workbook.exe` and put into a ZIP archive. It is then sent through the FortiGate device over HTTP. It is intercepted and processed by the configuration shown in the above Exhibits 1-4.

Assuming the file is not too large for the File scanning threshold, what action will the FortiGate unit take?

- A. The file will be detected by rule #1 as an `Audio (mp3)`, a log entry will be created and it will be allowed to pass through.
- B. The file will be detected by rule #2 as a "*.exe", a log entry will be created and the interface that received the traffic will be brought down.
- C. The file will be detected by rule #3 as an Archive(zip), blocked, and a log entry will be created.
- D. Nothing, the file will go undetected.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 132

What are the requirements for a cluster to maintain TCP connections after device or link failover? (Select all that apply.)

- A. Enable session pick-up.
- B. Only applies to connections handled by a proxy.
- C. Only applies to UDP and ICMP connections.
- D. Connections must not be handled by a proxy.

Correct Answer: AD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 133

What advantages are there in using a hub-and-spoke IPSec VPN configuration instead of a fully-meshed set of IPSec tunnels? (Select all that apply.)

- A. Using a hub and spoke topology is required to achieve full redundancy.
- B. Using a hub and spoke topology simplifies configuration because fewer tunnels are required.
- C. Using a hub and spoke topology provides stronger encryption.
- D. The routing at a spoke is simpler, compared to a meshed node.

Correct Answer: BD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 134

The eicar test virus is put into a zip archive, which is given the password of "Fortinet" in order to open the archive. Review the configuration in the exhibits shown below; then answer the question that follows.

Exhibit A - Antivirus Profile:



Inspection Mode

Proxy Flow-based

Block Connections to Botnet Servers

Protocol	Virus Scan and Removal
Web	
HTTP	<input checked="" type="checkbox"/>
Email	
SMTP	<input type="checkbox"/>
POP3	<input type="checkbox"/>
IMAP	<input type="checkbox"/>
MAPI	<input type="checkbox"/>
File Transfer	
FTP	<input type="checkbox"/>
SMB	<input type="checkbox"/>
IM	
ICQ, Yahoo, MSN Messenger	<input type="checkbox"/>

Exhibit B - Non-default UTM Proxy Options Profile:

Protocol Port Mapping

Enable	Protocol	Inspection Port(s)	
<input checked="" type="checkbox"/>	HTTP	<input type="radio"/> Any <input checked="" type="radio"/> Specify	8080
<input checked="" type="checkbox"/>	SMTP	<input type="radio"/> Any <input checked="" type="radio"/> Specify	25
<input checked="" type="checkbox"/>	POP3	<input type="radio"/> Any <input checked="" type="radio"/> Specify	110
<input checked="" type="checkbox"/>	IMAP	<input type="radio"/> Any <input checked="" type="radio"/> Specify	143
<input checked="" type="checkbox"/>	FTP	<input type="radio"/> Any <input checked="" type="radio"/> Specify	21
<input checked="" type="checkbox"/>	NNTP	<input type="radio"/> Any <input checked="" type="radio"/> Specify	119
<input checked="" type="checkbox"/>	MAPI		135
<input checked="" type="checkbox"/>	DNS		53

Exhibit C - DLP Profile:

Seq #	Type	Action	Services	Archive
1.	Encrypted	Block	POP3, HTTP	Disable

Which of one the following profiles could be enabled in order to prevent the file from passing through the FortiGate device over HTTP on the standard port for that protocol?

- A. Only Exhibit A
- B. Only Exhibit B
- C. Only Exhibit C with default UTM Proxy settings.
- D. All of the Exhibits (A, B and C)
- E. Only Exhibit C with non-default UTM Proxy settings (Exhibit B).

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 135

With FSSO, a domain user could authenticate either against the domain controller running the Collector Agent and Domain Controller Agent, or a domain controller running only the Domain Controller Agent.

If you attempt to authenticate with the Secondary Domain Controller running only the Domain Controller Agent, which of the following statements are correct? (Select all that apply.)



<https://vceplus.com/>

- A. The login event is sent to the Collector Agent.
- B. The FortiGate unit receives the user information from the Domain Controller Agent of the Secondary Controller.
- C. The Collector Agent performs the DNS lookup for the authenticated client's IP address.
- D. The user cannot be authenticated with the FortiGate device in this manner because each Domain Controller Agent requires a dedicated Collector Agent.

Correct Answer: AC

Section: (none)

Explanation

Explanation/Reference:

QUESTION 136

In Transparent Mode, forward-domain is an attribute of _____.

- A. an interface
- B. a firewall policy
- C. a static route
- D. a virtual domain

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 137

Review the CLI configuration below for an IPS sensor and identify the correct statements regarding this configuration from the choices below. (Select all that apply.)

```
config ips sensor
edit "LINUX_SERVER"
set comment ''
set replacemsg-group ''
set log enable
config entries
edit 1
set action default
set application all
set location server
set log enable
set log-packet enable s
set os Linux
set protocol all
set quarantine none
set severity all
set status default
next
end
next
end
```



- A. The sensor will log all server attacks for all operating systems.
- B. The sensor will include a PCAP file with a trace of the matching packets in the log message of any matched signature.
- C. The sensor will match all traffic from the address object `LINUX_SERVER`.
- D. The sensor will reset all connections that match these signatures.
- E. The sensor only filters which IPS signatures to apply to the selected firewall policy.

Correct Answer: BE

Section: (none)

Explanation

Explanation/Reference:

QUESTION 138

In which of the following report templates would you configure the charts to be included in the report?

- A. Layout Template
- B. Data Filter Template
- C. Output Template
- D. Schedule Template

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:



QUESTION 139

A DLP rule with an action of Exempt has been matched against traffic passing through the FortiGate unit. Which of the following statements is correct regarding how this transaction will be handled by the FortiGate unit?

- A. Any other matched DLP rules will be ignored with the exception of Archiving.
- B. Future files whose characteristics match this file will bypass DLP scanning.
- C. The traffic matching the DLP rule will bypass antivirus scanning.
- D. The client IP address will be added to a white list.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 140

An administrator is examining the attack logs and notices the following entry:

```
type=ips subtype=signature pri=alert vd=root serial=1995
attack_id=103022611 src=69.45.64.22 dst=192.168.1.100 src_port=80
dst_port=4887 src_int=wlan dst_int=internal sta-tus=detectedproto=6
service=4887/tcp user=N/A group=N/A msg=web_client:
IE.IFRAME.BufferOverflow.B
```

Based on the information displayed in this entry, which of the following statements are correct? (Select all that apply.)

- A. This is an HTTP server attack.
- B. The attack was detected and blocked by the FortiGate unit.
- C. The attack was against a FortiGate unit at the 192.168.1.100 IP address.
- D. The attack was detected and passed by the FortiGate unit.

Correct Answer: CD

Section: (none)

Explanation

Explanation/Reference:



QUESTION 141

What advantages are there in using a hub-and-spoke IPSec VPN configuration instead of a fully-meshed set of IPSec tunnels? (Select all that apply.)

- A. Using a hub and spoke topology is required to achieve full redundancy.
- B. Using a hub and spoke topology simplifies configuration.
- C. Using a hub and spoke topology provides stronger encryption.
- D. Using a hub and spoke topology reduces the number of tunnels.

Correct Answer: BD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 142

An administrator wishes to generate a report showing Top Traffic by service type. They notice that web traffic overwhelms the pie chart and want to exclude the web traffic from the report. Which of the following statements best describes how to do this?

- A. In the Service field of the Data Filter, type 80/tcp and select the NOT checkbox.
- B. Add the following entry to the Generic Field section of the Data Filter: service="!web".
- C. When editing the chart, uncheck wlog to indicate that Web Filtering data is being excluded when generating the chart.
- D. When editing the chart, enter 'http' in the Exclude Service field.

Correct Answer: A

Section: (none)

Explanation

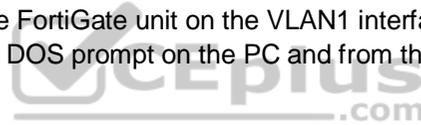
Explanation/Reference:

QUESTION 143

A network administrator connects his PC to the INTERNAL interface on a FortiGate unit.

The administrator attempts to make an HTTPS connection to the FortiGate unit on the VLAN1 interface at the IP address of 10.0.1.1, but gets no connectivity.

The following troubleshooting commands are executed from the DOS prompt on the PC and from the CLI.



```
C:\>ping 10.0.1.1
Pinging 10.0.1.1 with 32 bytes of data:
Reply from 10.0.1.1: bytes=32 time=1ms TTL=255
Reply from 10.0.1.1: bytes=32 time<1ms TTL=255
Reply from 10.0.1.1: bytes=32 time<1ms TTL=255
Reply from 10.0.1.1: bytes=32 time<1ms TTL=255
user1 # get system interface
== [ internal ]
name. internal mode. static ip: 10.0.1.254 255.255.255.128 status: up
netbios-forward. disable type. physical mtu-override. disable
== [ vlan1 ]
name. vlan1 mode. static ip: 10.0.1.1 255.255.255.128 status: up netb
ios-forward. disable type. vlan mtu-override. disable
user1 # diagnose debug flow trace start 100
user1 # diagnose debug ena
user1 # diagnose debug flow filter daddr 10.0.1.1 10.0.1.1
id=20085 trace_id=274 msg="vd-root received a packet(proto=6,
10.0.1.130:47927- >10.0.1.1:443) from internal."
id=20085 trace_id=274 msg="allocate a new session-00000b1b"
id=20085 trace_id=274 msg="find SNAT: IP-10.0.1.1, port-43798"
id=20085 trace_id=274 msg="iprope_in_check() check failed, drop"
```

Based on the output from these commands, which of the following explanations is a possible cause of the problem?

- A. The Fortigate unit has no route back to the PC.
- B. The PC has an IP address in the wrong subnet.
- C. The PC is using an incorrect default gateway IP address.
- D. The FortiGate unit does not have the HTTPS service configured on the VLAN1 interface.
- E. There is no firewall policy allowing traffic from INTERNAL-> VLAN1.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 144

Which of the following methods does the FortiGate unit use to determine the availability of a web cache using Web Cache Communication Protocol (WCCP)?

- A. The FortiGate unit receives periodic "Here I am" messages from the web cache.
- B. The FortiGate unit polls all globally-defined web cache servers at a regular intervals.
- C. The FortiGate using uses the health check monitor to verify the availability of a web cache server.
- D. The web cache sends an "I see you" message which is captured by the FortiGate unit.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 145

A FortiGate unit is configured with multiple VDOMs. An administrative account on the device has been assigned a Scope value of VDOM:root. Which of the following items would an administrator logging in using this account NOT be able to configure?

- A. Firewall addresses
- B. DHCP servers
- C. FortiGuard Distribution Network configuration
- D. PPTP VPN configuration



Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 146

Which of the following statements is correct regarding the antivirus scanning function on the FortiGate unit?

- A. Antivirus scanning provides end-to-end virus protection for client workstations.
- B. Antivirus scanning provides virus protection for the HTTP, Telnet, SMTP, and FTP protocols.
- C. Antivirus scanning supports banned word checking.
- D. Antivirus scanning supports grayware protection.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 147

WAN optimization is configured in Active/Passive mode. When will the remote peer accept an attempt to initiate a tunnel?

- A. The attempt will be accepted when the request comes from a known peer and there is a matching WAN optimization passive rule.
- B. The attempt will be accepted when there is a matching WAN optimization passive rule.
- C. The attempt will be accepted when the request comes from a known peer.
- D. The attempt will be accepted when a user on the remote peer accepts the connection request.

Correct Answer: A

Section: (none)

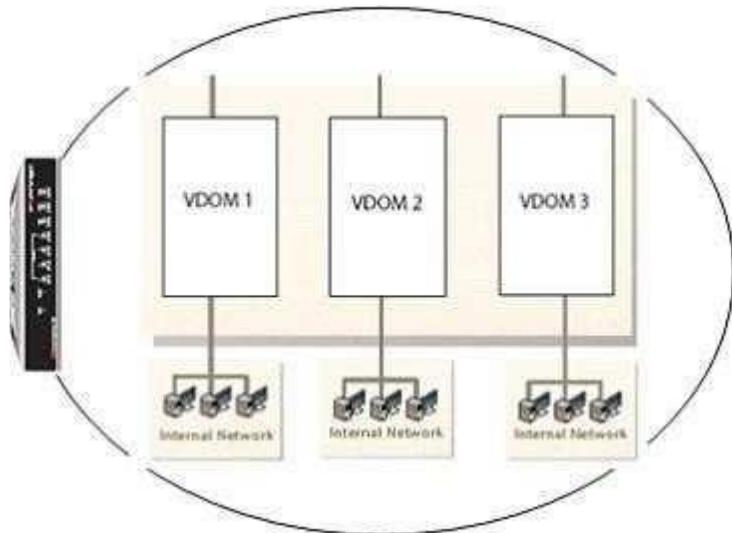
Explanation

Explanation/Reference:



QUESTION 148

A FortiGate unit is configured with three Virtual Domains (VDOMs) as illustrated in the exhibit.



Which of the following statements are correct regarding these VDOMs? (Select all that apply.)

- A. The FortiGate unit supports any combination of these VDOMs in NAT/Route and Transparent modes.
- B. The FortiGate unit must be a model 1000 or above to support multiple VDOMs.
- C. A license had to be purchased and applied to the FortiGate unit before VDOM mode could be enabled.
- D. All VDOMs must operate in the same mode.
- E. Changing a VDOM operational mode requires a reboot of the FortiGate unit.
- F. An admin account can be assigned to one VDOM or it can have access to all three VDOMs.

Correct Answer: AF

Section: (none)

Explanation

Explanation/Reference:

QUESTION 149

Both the FortiGate and FortiAnalyzer units can notify administrators when certain alert conditions are met. Considering this, which of the following statements is NOT correct?

- A. On a FortiGate device, the alert condition is based either on the severity level or on the log type, but not on a combination of the two.
- B. On a FortiAnalyzer device, the alert condition is based either on the severity level or on the log type, but not on a combination of the two.
- C. Only a FortiAnalyzer device can send the alert notification in the form of a syslog message.
- D. Both the FortiGate and FortiAnalyzer devices can send alert notifications in the form of an email alert.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 150

Which of the following statements is correct regarding the FortiGuard Services Web Filtering Override configuration as illustrated in the exhibit?

New Override Rule

Type:

URL:

Scope:

IP:

Off-site URLs:

Hour: Minute: Second:

Year: Month: Day:



<https://vceplus.com/>

- A. Any client on the same subnet as the authenticated user is allowed to access www.yahoo.com/images/.
- B. A client with an IP of address 10.10.10.12 is allowed access to any subdirectory that is part of the www.yahoo.com web site.
- C. A client with an IP address of 10.10.10.12 is allowed access to the www.yahoo.com/images/ web site and any of its offsite URLs.
- D. A client with an IP address of 10.10.10.12 is allowed access to any URL under the www.yahoo.com web site, including any subdirectory URLs, until August 7, 2009.
- E. Any client on the same subnet as the authenticated user is allowed to access www.yahoo.com/images/ until August 7, 2009.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 151

SSL Proxy is used to decrypt the SSL-encrypted traffic. After decryption, where is the traffic buffered in preparation for content inspection?

- A. The file is buffered by the application proxy.
- B. The file is buffered by the SSL proxy.
- C. In the upload direction, the file is buffered by the SSL proxy.
In the download direction, the file is buffered by the application proxy.
- D. No file buffering is needed since a stream-based scanning approach is used for SSL content inspection.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 152

An administrator logs into a FortiGate unit using an account which has been assigned a super_admin profile. Which of the following operations can this administrator perform?

- A. They can delete logged-in users who are also assigned the super_admin access profile.
- B. They can make changes to the super_admin profile.
- C. They can delete the admin account if the default admin user is not logged in.
- D. They can view all the system configuration settings but can not make changes.
- E. They can access configuration options for only the VDOMs to which they have been assigned.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:



QUESTION 153

Which of the following statements is correct about how the FortiGate unit verifies username and password during user authentication?

- A. If a remote server is included in a user group, it will be checked before local accounts.
- B. An administrator can define a local account for which the password must be verified by querying a remote server.
- C. If authentication fails with a local password, the FortiGate unit will query the authentication server if the local user is configured with both a local password and an authentication server.
- D. The FortiGate unit will only attempt to authenticate against Active Directory if Fortinet Server Authentication Extensions are installed and configured.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 154

Which of the following cannot be used in conjunction with the endpoint compliance check?

- A. HTTP Challenge Redirect to a Secure Channel (HTTPS) in the Authentication Settings.
- B. Any form of firewall policy authentication.
- C. WAN optimization.
- D. Traffic shaping.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 155

In the Tunnel Mode widget of the web portal, the administrator has configured an IP Pool and enabled split tunneling.

Which of the following statements is true about the IP address used by the SSL VPN client?

- A. The IP pool specified in the SSL-VPN Tunnel Mode Widget Options will override the IP address range defined in the SSL-VPN Settings.
- B. Because split tunneling is enabled, no IP address needs to be assigned for the SSL VPN tunnel to be established.
- C. The IP address range specified in SSL-VPN Settings will override the IP address range in the SSL-VPN Tunnel Mode Widget Options.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 156

The Host Check feature can be enabled on the FortiGate unit for SSL VPN connections. When this feature is enabled, the FortiGate unit probes the remote host computer to verify that it is "safe" before access is granted.

Which of the following items is NOT an option as part of the Host Check feature?

- A. FortiClient Antivirus software
- B. Microsoft Windows Firewall software
- C. FortiClient Firewall software
- D. Third-party Antivirus software

Correct Answer: B

Section: (none)

Explanation



Explanation/Reference:

QUESTION 157

Which of the following report templates must be used when scheduling report generation?

- A. Layout Template
- B. Data Filter Template
- C. Output Template
- D. Chart Template

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 158

Which of the following statements is not correct regarding virtual domains (VDMs)?

- A. VDMs divide a single FortiGate unit into two or more virtual units that function as multiple, independent units.
- B. A management VDM handles SNMP, logging, alert email, and FDN-based updates.
- C. A backup management VDM will synchronize the configuration from an active management VDM.
- D. VDMs share firmware versions, as well as antivirus and IPS databases.
- E. Only administrative users with a super_admin profile will be able to enter all VDMs to make configuration changes.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 159

Which of the following must be configured on a FortiGate unit to redirect content requests to remote web cache servers?

- A. WCCP must be enabled on the interface facing the Web cache.
- B. You must enabled explicit Web-proxy on the incoming interface.
- C. WCCP must be enabled as a global setting on the FortiGate unit.
- D. WCCP must be enabled on all interfaces on the FortiGate unit through which HTTP traffic is passing.

Correct Answer: A

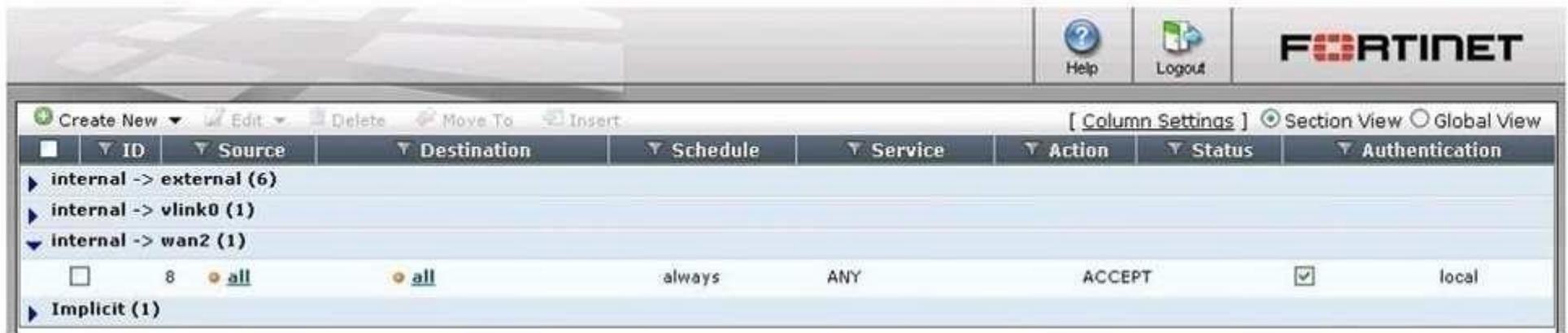
Section: (none)

Explanation

Explanation/Reference:

QUESTION 160

Which of the following statements is correct based on the firewall configuration illustrated in the exhibit?



The screenshot shows the Fortinet firewall policy configuration interface. The top bar includes 'Help' and 'Logout' buttons, and the 'FORTINET' logo. Below the navigation bar, there are tabs for 'Section View' and 'Global View'. The main area displays a table of firewall policies with columns for ID, Source, Destination, Schedule, Service, Action, Status, and Authentication. The table shows several policies, including 'internal -> external (6)', 'internal -> vlink0 (1)', 'internal -> wan2 (1)', and 'Implicit (1)'. The 'internal -> wan2 (1)' policy is expanded to show its configuration: ID 8, Source 'all', Destination 'all', Schedule 'always', Service 'ANY', Action 'ACCEPT', Status checked, and Authentication 'local'.

ID	Source	Destination	Schedule	Service	Action	Status	Authentication
internal -> external (6)							
internal -> vlink0 (1)							
internal -> wan2 (1)							
8	all	all	always	ANY	ACCEPT	<input checked="" type="checkbox"/>	local
Implicit (1)							

- A. A user can access the Internet using only the protocols that are supported by user authentication.
- B. A user can access the Internet using any protocol except HTTP, HTTPS, Telnet, and FTP. These require authentication before the user will be allowed access.
- C. A user must authenticate using the HTTP, HTTPS, SSH, FTP, or Telnet protocol before they can access any services.
- D. A user cannot access the Internet using any protocols unless the user has passed firewall authentication.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 161

Which of the following statements is correct regarding the NAC Quarantine feature?

- A. With NAC quarantine, files can be quarantined not only as a result of antivirus scanning, but also for other forms of content inspection such as IPS and DLP.
- B. NAC quarantine does a client check on workstations before they are permitted to have administrative access to FortiGate.
- C. NAC quarantine allows administrators to isolate clients whose network activity poses a security risk.
- D. If you chose the quarantine action, you must decide whether the quarantine type is NAC quarantine or File quarantine.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 162

What advantages are there in using a fully Meshed IPSec VPN configuration instead of a hub and spoke set of IPSec tunnels?

- A. Using a hub and spoke topology is required to achieve full redundancy.
- B. Using a full mesh topology simplifies configuration.
- C. Using a full mesh topology provides stronger encryption.
- D. Full mesh topology is the most fault-tolerant configuration.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 163

An administrator wishes to generate a report showing Top Traffic by service type, but wants to exclude SMTP traffic from the report. Which of the following statements best describes how to do this?

- A. In the Service field of the Data Filter, type 25/smtp and select the NOT checkbox.
- B. Add the following entry to the Generic Field section of the Data Filter: service="!smtp".
- C. When editing the chart, uncheck mlog to indicate that Mail Filtering data is being excluded when generating the chart.
- D. When editing the chart, enter 'dns' in the Exclude Service field.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 164

An organization wishes to protect its SIP Server from call flooding attacks. Which of the following configuration changes can be performed on the FortiGate unit to fulfill this requirement?

- A. Apply an application control list which contains a rule for SIP and has the "Limit INVITE Request" option configured.

- B. Enable Traffic Shaping for the appropriate SIP firewall policy.
- C. Reduce the session time-to-live value for the SIP protocol by running the configure system session-ttl CLI command.
- D. Run the set udp-idle-timer CLI command and set a lower time value.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 165

In a High Availability configuration operating in Active-Active mode, which of the following correctly describes the path taken by a load-balanced HTTP session?

- A. Request: Internal Host -> Master FG -> Slave FG -> Internet -> Web Server
- B. Request: Internal Host -> Master FG -> Slave FG -> Master FG -> Internet -> Web Server
- C. Request: Internal Host -> Slave FG -> Internet -> Web Server
- D. Request: Internal Host -> Slave FG -> Master FG -> Internet -> Web Server

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 166

Which of the following DLP actions will override any other action?

- A. Exempt
- B. Quarantine Interface
- C. Block
- D. None

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 167

A FortiClient fails to establish a VPN tunnel with a FortiGate unit.

The following information is displayed in the FortiGate unit logs:

```
msg="Initiator: sent 192.168.11.101 main mode message #1 (OK) "  
msg="Initiator: sent 192.168.11.101 main mode message #2 (OK) "  
msg="Initiator: sent 192.168.11.101 main mode message #3 (OK) "  
msg="Initiator: parsed 192.168.11.101 main mode message #3 (DONE) "  
msg="Initiator: sent 192.168.11.101 quick mode message #1 (OK) "  
msg="Initiator: tunnel 192.168.1.1/192.168.11.101 install ipsec sa"  
msg="Initiator: sent 192.168.11.101 quick mode message #2 (DONE) "  
msg="Initiator: tunnel 192.168.11.101, transform=ESP_3DES, HMAC_MD5"  
msg="Failed to acquire an IP address"
```

Which of the following statements is a possible cause for the failure to establish the VPN tunnel?

- A. An IPsec DHCP server is not enabled on the external interface of the FortiGate unit.
- B. There is no IPsec firewall policy configured for the policy-based VPN.
- C. There is a mismatch between the FortiGate unit and the FortiClient IP addresses in the phase 2 settings.
- D. The phase 1 configuration on the FortiGate unit uses Aggressive mode while FortiClient uses Main mode.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 168

Which of the following statements correctly describes the deepscan option for HTTPS?



<https://vceplus.com/>

- A. When deepscan is disabled, only the web server certificate is inspected; no decryption of content occurs.
- B. Enabling deepscan will perform further checks on the server certificate.
- C. Deepscan is only applicable to mail protocols, where all IP addresses in the header are checked.
- D. With deepscan enabled, archived files will be decompressed before scanning for a more comprehensive file inspection.

Correct Answer: A

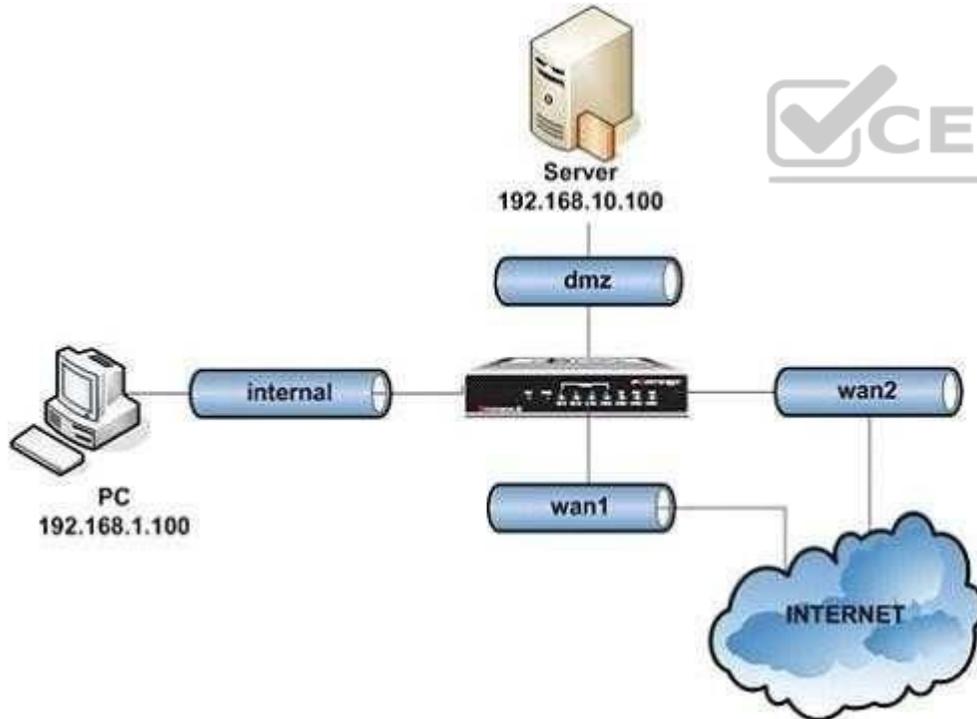
Section: (none)

Explanation

Explanation/Reference:

QUESTION 169

An intermittent connectivity issue is noticed between two devices located behind the FortiGate dmz and internal interfaces. A continuous sniffer trace is run on the FortiGate unit that the administrator will convert into a .cap file for an off-line analysis with a sniffer application.



Given the high volume of global traffic on the network, which of the following CLI commands will best allow the administrator to perform this troubleshooting operation?

- A. diagnose sniffer packet any
- B. diagnose sniffer packet dmz "" 3
- C. diagnose sniffer packet any "host 192.168.1.100 and host 192.168.10.100 " 3
- D. diagnose sniffer packet any "host 192.168.1.100 and host 192.168.10.100 " 4

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 170

The following ban list entry is displayed through the CLI.

```
get user ban list
id cause src-ip-addr dst-ip-addr expires created
531 protect_client 10.177.0.21 207.1.17.1 indefinite Wed Dec 24 :21:33
2008
```

Based on this command output, which of the following statements is correct?

- A. The administrator has specified the Attack and Victim Address method for the quarantine.
- B. This diagnostic entry results from the administrator running the diag ips log test command. This command has no effect on traffic.
- C. A DLP rule has been matched.
- D. An attack has been repeated more than once during the holddown period; the expiry time has been reset to indefinite.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 171

A network administrator needs to implement dynamic route redundancy between a FortiGate unit located in a remote office and a FortiGate unit located in the central office.

The remote office accesses central resources using IPSec VPN tunnels through two different Internet providers.

What is the best method for allowing the remote office access to the resources through the FortiGate unit used at the central office?

- A. Use two or more route-based IPSec VPN tunnels and enable OSPF on the IPSec virtual interfaces.
- B. Use two or more policy-based IPSec VPN tunnels and enable OSPF on the IPSec virtual interfaces.
- C. Use route-based VPNs on the central office FortiGate unit to advertise routes with a dynamic routing protocol and use a policy-based VPN on the remote office with two or more static default routes.
- D. Dynamic routing protocols cannot be used over IPSec VPN tunnels.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 172

When performing a log search on a FortiAnalyzer, it is generally recommended to use the Quick Search option.

What is a valid reason for using the Full Search option, instead?

- A. The search items you are looking for are not contained in indexed log fields.
- B. A quick search only searches data received within the last 24 hours.
- C. You want the search to include the FortiAnalyzer's local logs.
- D. You want the search to include content archive data as well.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 173

The diag sys session list command is executed in the CLI. The output of this command is shown in the exhibit.

```
session info: proto=6 proto_state=11 duration=539 expire=3571 timeout=3600
flags=00000000 sockflag=00000000 sockport=80 av_idx=0 use=5
origin-shaper=guarantee-100kbps prio=1 guarantee 12288/sec max 134217728/sec
traffic 123/sec
reply-shaper=low-priority prio=3 guarantee 0/sec max 134217728/sec traffic 115/sec
per_ip_shaper=
ha_id=0 hakey=1335
policy_dir=0 tunnel=/
state=redir local may_dirty ndr os rs rem
statistic(bytes/packets/allow_err): org=3201/59/1 reply=2672/58/1 tuples=3
origin->sink: org pre->post, reply pre->post dev=9->3/3->9
gwy=76.27.192.1/192.168.203.2
hook=post dir=org act=snat 192.168.203.2:3196-
>128.100.58.53:80(76.27.195.147:58618)
hook=pre dir=reply act=dnat 128.100.58.53:80-
>76.27.195.147:58618(192.168.203.2:3196)
hook=post dir=reply act=noop 128.100.58.53:80->192.168.203.2:3196(0.0.0.0:0)
pos/(before,after) 0/(0,0), 0/(0,0)
misc=0 policy_id=10 id_policy_id=0 auth_info=0 chk_client_info=0 vd=0
serial=00115cae tos=fff/app_list=2000 app=0
dd_type=0 dd_rule_id=0
per_ip_bandwidth meter: addr=192.168.203.2, bps=1351
```

Based on the output from this command, which of the following statements is correct?

- A. This is a UDP session.
- B. Traffic shaping is being applied to this session.
- C. This is an ICMP session.
- D. This traffic has been authenticated.
- E. This session matches a firewall policy with ID 5.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 174

What protocol cannot be used with the active authentication type?

- A. Local
- B. RADIUS
- C. LDAP
- D. RSO

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:



QUESTION 175

Review the exhibit of an explicit proxy policy configuration. If there is a proxy connection attempt coming from the IP address 10.0.1.5, and from a user that has not authenticated yet, what action does the FortiGate proxy take?

Seq.#	To	Source	Destination	Users	Schedule	Action	AV	Settings
▼ web (1 - 2)								
1	port1	10.0.1.0/24	all	↓	↓	✓ ACCEPT	↓	
1.1				Student	always			
2	port1	10.0.0.0/8	all		always	✓ ACCEPT		

- A. User is prompted to authenticate. Traffic from the user Student will be allowed by the policy #1. Traffic from any other user will be allowed by the policy #2.
- B. User is not prompted to authenticate. The connection is allowed by the proxy policy #2.
- C. User is not prompted to authenticate. The connection will be allowed by the proxy policy #1.

D. User is prompted to authenticate. Only traffic from the user Student will be allowed. Traffic from any other user will be blocked.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 176

Which of the following statements are true regarding DLP File Type Filtering? (Choose two.)

- A. Filters based on file extension
- B. Filters based on fingerprints
- C. Filters based on file content
- D. File types are hard coded in the FortiOS

Correct Answer: AC

Section: (none)

Explanation

Explanation/Reference:

Explanation:



Filter

Type Messages Files

Containing

File size over KB

Specify File Types

Regular Expression

Encrypted

Filter

Type Messages Files

Containing

Regular Expression

QUESTION 177

Which of the following settings can be configured per VDOM? (Choose three.)

- A. Operating mode (NAT/route or transparent)
- B. Static routes
- C. Hostname
- D. System time
- E. Firewall Policies

Correct Answer: ABE

Section: (none)

Explanation

Explanation/Reference:

QUESTION 178

Which protocols can you use for secure administrative access to a FortiGate? (Choose two)

- A. SSH
- B. Telnet
- C. NTLM
- D. HTTPS

Correct Answer: AD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 179

What are examples of correct syntax for the session table diagnostics command? (Choose two.)

- A. diagnose sys session filter clear
- B. diagnose sys session src 10.0.1.254
- C. diagnose sys session filter
- D. diagnose sys session filter list dst.

Correct Answer: AC

Section: (none)

Explanation

Explanation/Reference:

QUESTION 180

Which statement best describes the objective of the SYN proxy feature available in SP processors?

- A. Accelerate the TCP 3-way handshake
- B. Collect statistics regarding traffic sessions

- C. Analyze the SYN packet to decide if the new session can be offloaded to the SP processor
- D. Protect against SYN flood attacks.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 181

Which of the following are possible actions for static URL filtering? (Choose three.)

- A. Allow
- B. Block
- C. Exempt
- D. Warning
- E. Shape

Correct Answer: ABC

Section: (none)

Explanation

Explanation/Reference:



QUESTION 182

Which statement best describes what SSL VPN Client Integrity Check does?

- A. Blocks SSL VPN connection attempts from users that has been blacklisted.
- B. Detects the Windows client security applications running in the SSL VPN client's PCs.
- C. Validates the SSL VPN user credential.
- D. Verifies which SSL VPN portal must be presented to each SSL VPN user.
- E. Verifies that the latest SSL VPN client is installed in the client's PC.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 183

A FortiGate is configured to receive push updates from the FortiGuard Distribution Network, however, they are not being received.

Which is one reason for this problem?

- A. The FortiGate is connected to multiple ISPs.
- B. FortiGuard scheduled updates are enabled in the FortiGate configuration.
- C. The FortiGate is in Transparent mode.
- D. The external facing interface of the FortiGate is configured to get the IP address from a DHCP server.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:



QUESTION 184

Which best describe the mechanism of a TCP SYN flood?

- A. The attacker keeps open many connections with slow data transmission so that other clients cannot start new connections.
- B. The attacker sends a packet designed to "sync" with the FortiGate.
- C. The attacker sends a specially crafted malformed packet, intended to crash the target by exploiting its parser.
- D. The attacker starts many connections, but never acknowledges to fully form them.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 185

Which traffic can match a firewall policy's "Services" setting? (Choose three.)

- A. HTTP
- B. SSL

- C. DNS
- D. RSS
- E. HTTPS

Correct Answer: ACE

Section: (none)

Explanation

Explanation/Reference:

QUESTION 186

Acme Web Hosting is replacing one of their firewalls with a FortiGate. It must be able to apply port forwarding to their back-end web servers while blocking virus uploads and TCP SYN floods from attackers. Which operation mode is the best choice for these requirements?



<https://vceplus.com/>

- A. NAT/route
- B. NAT mode with an interface in one-arm sniffer mode
- C. Transparent mode
- D. No appropriate operation mode exists

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 187

Which of the following statements are true about the SSL Proxy certificate that must be used for SSL Content Inspection? (Choose two.)

- A. It cannot be signed by a private CA
- B. It must have either the field "CA=True" or the field "Key Usage=KeyCertSign"
- C. It must be installed in the FortiGate device
- D. The subject field must contain either the FQDN, or the IP address of the FortiGate device

Correct Answer: CD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 188

A FortiGate device is configured to perform an AV & IPS scheduled update every hour.

```
Virus Definitions
-----
Version: 21.00487
Contract Expiry Date: Tue Apr 29 00:00:00 2014
Last Updated using scheduled update on Mon Jan
20 01:05:33 2014
Last Update Attempt: Mon Jan 20 10:08:56 2014
Result: Updates Installed
```

```
FG100D3G12800939 # exe time
current time is: 10:35:35
last ntp sync: Mon Jan 20 09:51:59 2014
```

Given the information in the exhibit, when will the next update happen?

- A. 01:00
- B. 02:05
- C. 11:00
- D. 11:08

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 189

Which of the following statements describe some of the differences between symmetric and asymmetric cryptography? (Choose two.)

- A. In symmetric cryptography, the keys are publicly available. In asymmetric cryptography, the keys must be kept secret.
- B. Asymmetric cryptography can encrypt data faster than symmetric cryptography
- C. Symmetric cryptography uses one pre-shared key. Asymmetric cryptography uses a pair of keys
- D. Asymmetric keys can be sent to the remote peer via digital certificates. Symmetric keys cannot

Correct Answer: CD

Section: (none)

Explanation

Explanation/Reference:



QUESTION 190

An Internet browser is using the WPAD DNS method to discover the PAC file's URL. The DNS server replies to the browser's request with the IP address 10.100.1.10. Which URL will the browser use to download the PAC file?

- A. <http://10.100.1.10/proxy.pac>
- B. <https://10.100.1.10/>
- C. <http://10.100.1.10/wpad.dat>
- D. <https://10.100.1.10/proxy.pac>

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:



<https://vceplus.com/>

