

Fortinet.Premium.NSE4-5.4.by.VCEplus.576q

Number: NSE4-5.4
Passing Score: 800
Time Limit: 120 min
File Version: 5.0



Certification: NSE4

Certification Full Name: Network Security Expert

Certification Provider: Fortinet

Exam Code: NSE4-5.4

Exam Name: Fortinet Network Security Expert - FortiOS 5.4

Website: www.vceplus.com

Free Exam: <https://vceplus.com/exam-nse4-fortinet/>

Questions & Answers Exam Engine is rigorously checked before being put up for sale. We make sure there is nothing irrelevant in NSE4-5.4 exam products and you get latest questions. We strive to deliver the best NSE4-5.4 exam product for top grades in your first attempt.

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

Google+ : <https://plus.google.com/+Vcepluscom>

LinkedIn : <https://www.linkedin.com/company/vceplus>

Exam A**QUESTION 1**

A FortiGate interface is configured with the following commands:

```
config system interface
edit "port1"
config ipv6
set ip6-address 2001:db8:1::254/64
set ip6-send-adv enable
config ip6-prefix-list
edit 2001:db8:1::/64
set autonomous-flag enable
set onlink-flag enable
end
```

What statements about the configuration are correct? (Choose two.)

- A. IPv6 clients connected to port1 can use SLAAC to generate their IPv6 addresses.
- B. FortiGate can provide DNS settings to IPv6 clients.
- C. FortiGate can send IPv6 router advertisements (RAs.)
- D. FortiGate can provide IPv6 addresses to DHCPv6 client.

Correct Answer: AC

Section: (none)

Explanation

Explanation/Reference:

QUESTION 2

Which of the following Fortinet hardware accelerators can be used to offload flow-based antivirus inspection? (Choose two.)

- A. SP3
- B. CP8
- C. NP4
- D. NP6

Correct Answer: AB

Section: (none)

Explanation

Explanation/Reference:

QUESTION 3

Under what circumstance would you enable **LEARN** as the **Action** on a firewall policy?

- A. You want FortiGate to compile security feature activity from various security-related logs, such as virus and attack logs.
- B. You want FortiGate to monitor a specific security profile in a firewall policy, and provide recommendations for that profile.
- C. You want to capture data across all traffic and security vectors, and receive learning logs and a report with recommendations.
- D. You want FortiGate to automatically modify your firewall policies as it learns your networking behavior.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:



QUESTION 4

What methods can be used to deliver the token code to a user who is configured to use two-factor authentication? (Choose three.)

- A. Code blocks
- B. SMS phone message
- C. FortiToken
- D. Browser pop-up window
- E. Email

Correct Answer: BCE

Section: (none)

Explanation

Explanation/Reference:

QUESTION 5

You are tasked to architect a new IPsec deployment with the following criteria:

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

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

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:



QUESTION 6

View the exhibit.

Destination	Subnet	Named Address	Internet Service
	172.13.24.0/255.255.255.0		
Device	TunnelB		
Administrative Distance	5		
Comments	0/255		
Status	<input checked="" type="checkbox"/> Enabled <input type="checkbox"/> Disabled		
Advanced Options			
Priority	30		

Destination	Subnet	Named Address	Internet Service
	172.13.24.0/255.255.255.0		
Device	TunnelA		
Administrative Distance	10		
Comments			
Status	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled		
<input type="checkbox"/> Advanced Options			
Priority	0		

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

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

Correct Answer: AB

Section: (none)

Explanation

Explanation/Reference:

QUESTION 7

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

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

Correct Answer: CD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 8

An administrator needs to offload logging to FortiAnalyzer from a FortiGate with an internal hard drive. Which statements are true? (Choose two.)

- A. Logs must be stored on FortiGate first, before transmitting to FortiAnalyzer
- B. FortiGate uses port 8080 for log transmission
- C. Log messages are transmitted as plain text in LZ4 compressed format (store-and-upload method).
- D. FortiGate can encrypt communications using SSL encrypted OFTP traffic.

Correct Answer: AC

Section: (none)

Explanation

Explanation/Reference:



QUESTION 9

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

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

Correct Answer: BD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 10

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

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

Correct Answer: ABC

Section: (none)

Explanation

Explanation/Reference:

QUESTION 11

View the example routing table.

```
s* 0.0.0.0/0 [10/0] via 172.20.121.2, port1
C   172.20.121.0/24 is directly connected, port1
C   172.20.168.0/24 is directly connected, port2
C   172.20.167.0/24 is directly connected, port3
S   10.20.30.0/26 [10/0] via 172.20.168.254, port2
S   10.20.30.0/24 [10/0] via 172.20.167.254, port3
```

Which route will be selected when trying to reach 10.20.30.254?

- A. 10.20.30.0/26 [10/0] via 172.20.168.254, port2
- B. The traffic will be dropped because it cannot be routed.
- C. 10.20.30.0/24 [10/0] via 172.20.167.254, port3
- D. 0.0.0.0/0 [10/0] via 172.20.121.2, port1

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Address (Host or Network)	Netmask (i.e. 24)	Netmask for sub/supernet (optional)
10.20.30.0	/ 26	move to:
<input type="button" value="Calcular"/> limpiar		
<p>Address: 10.20.30.0 00001010.00010100.00011110.00 000000</p> <p>Netmask: 255.255.255.192 = 26 11111111.11111111.11111111.11 000000</p> <p>Wildcard: 0.0.0.63 00000000.00000000.00000000.00 111111</p> <p>=></p> <p>Network: 10.20.30.0/26 00001010.00010100.00011110.00 000000</p> <p>HostMin: 10.20.30.1 00001010.00010100.00011110.00 000001</p> <p>HostMax: 10.20.30.62 00001010.00010100.00011110.00 111110</p> <p>Broadcast: 10.20.30.63 00001010.00010100.00011110.00 111111</p> <p>Hosts/Net: 62 Class A, Private Internet</p>		

AprendaRedes.com, Versión: 0.38

Address (Host or Network)	Netmask (i.e. 24)	Netmask for sub/supernet (optional)
10.20.30.0	/ 24	move to:
<input type="button" value="Calcular"/> limpiar		
<p>Address: 10.20.30.0 00001010.00010100.00011110. 00000000</p> <p>Netmask: 255.255.255.0 = 24 11111111.11111111.11111111. 00000000</p> <p>Wildcard: 0.0.0.255 00000000.00000000.00000000. 11111111</p> <p>=></p> <p>Network: 10.20.30.0/24 00001010.00010100.00011110. 00000000</p> <p>HostMin: 10.20.30.1 00001010.00010100.00011110. 00000001</p> <p>HostMax: 10.20.30.254 00001010.00010100.00011110. 11111110</p> <p>Broadcast: 10.20.30.255 00001010.00010100.00011110. 11111111</p> <p>Hosts/Net: 254 Class A, Private Internet</p>		

AprendaRedes.com, Versión: 0.38

QUESTION 12

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

- A. The FortiGate unit's public IP address
- B. The FortiGate unit's internal IP address
- C. The remote user's virtual IP address

D. The remote user's public IP address

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 13

What is FortiGate's behavior when local disk logging is disabled?

- A. Only real-time logs appear on the FortiGate dashboard.
- B. No logs are generated.
- C. Alert emails are disabled.
- D. Remote logging is automatically enabled.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:



QUESTION 14

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

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

Correct Answer: BCE

Section: (none)

Explanation

Explanation/Reference:

QUESTION 15

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

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

Correct Answer: BD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 16

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

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

Correct Answer: CDE

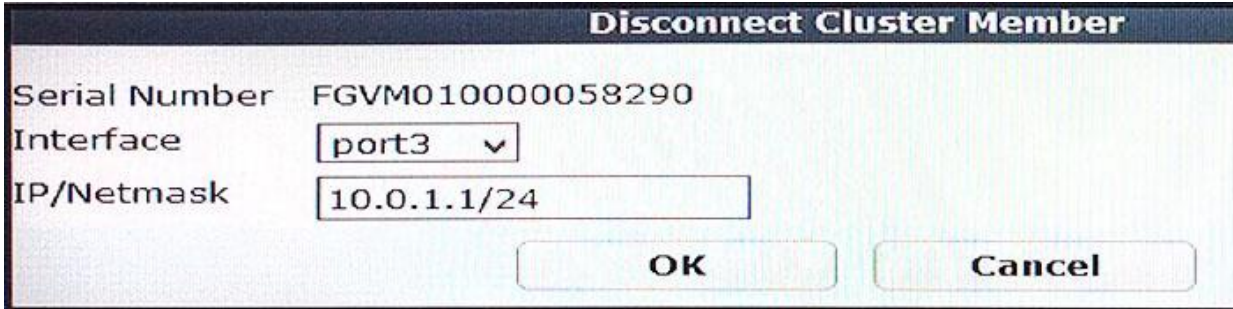
Section: (none)

Explanation

Explanation/Reference:

QUESTION 17

View the exhibit.



What is the effect of the **Disconnect Cluster Member** operation as shown in the exhibit? (Choose two.)

- A. The HA mode changes to standalone.
- B. The firewall policies are deleted on the disconnected member.
- C. The system hostname is set to the FortiGate serial number.
- D. The port3 is configured with an IP address for management access.

Correct Answer: AD

Section: (none)

Explanation



Explanation/Reference:

QUESTION 18

What step is required to configure an SSL VPN to access to an internal server using port forward mode?

- A. Configure the virtual IP addresses to be assigned to the SSL VPN users.
- B. Install FortiClient SSL VPN client
- C. Create a SSL VPN realm reserved for clients using port forward mode.
- D. Configure the client application to forward IP traffic to a Java applet proxy.

Correct Answer: D

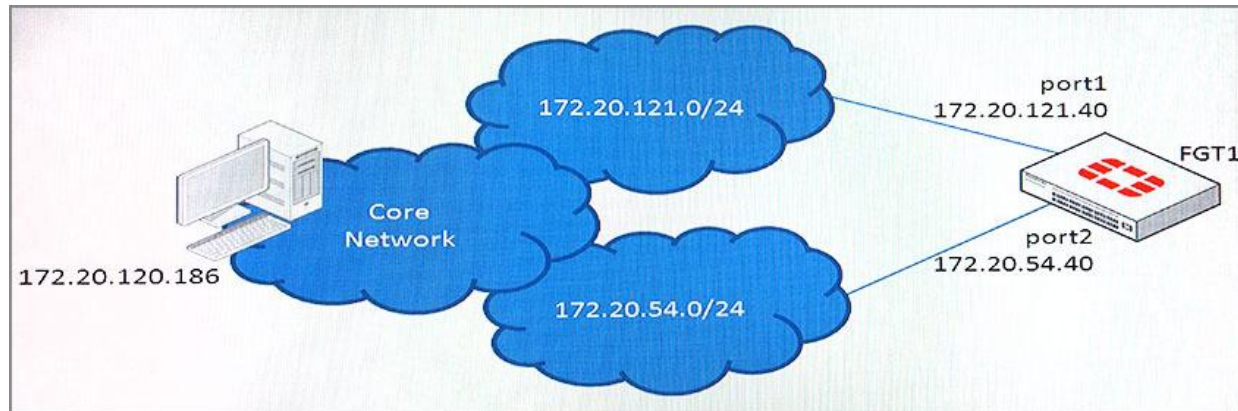
Section: (none)

Explanation

Explanation/Reference:

QUESTION 19

View the exhibit.



This is a sniffer output of a telnet connection request from 172.20.120.186 to the port1 interface of FGT1.

```
FGT1 # di sniff pack any "host 172.20.120.186 and port 23" 4

4.571724 port1 in 172.20.120.186.60584 -> 172.20.121.40.23: syn 273086
7.575327 port1 in 172.20.120.186.60584 -> 172.20.121.40.23: syn 273086
9.571446 port1 in 172.20.120.186.60584 -> 172.20.121.40.23: syn 273086
```

In this scenario, FGT1 has the following routing table:

```
S* 0.0.0.0/0 [10/0] via 172.20.54.254, port2
C 172.20.54.0/24 is directly connected, port2
C 172.20.121.0/24 is directly connected, port1
```

Assuming telnet service is enabled for port1, which of the following statements correctly describes why FGT1 is not responding?

- A. The port1 cable is disconnected.
- B. The connection is dropped due to reverse path forwarding check.
- C. The connection is denied due to forward policy check.
- D. FGT1's port1 interface is administratively down.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 20

An administrator needs to be able to view logs for application usage on your network. What configurations are required to ensure that FortiGate generates logs for application usage activity? (Choose two.)

- A. Enable a web filtering profile on the firewall policy.
- B. Create an application control policy.
- C. Enable logging on the firewall policy.
- D. Enable an application control security profile on the firewall policy.

Correct Answer: CD

Section: (none)

Explanation

Explanation/Reference:

Explanation:

By default the fortigate have one app control to monitor and for that not need create other app control and it necessary active logs in the policy to monitoring.

The screenshot shows the configuration interface for an SSL VPN. The 'Application Control' section is highlighted with a red box and contains a toggle switch for 'Application Control' (turned on), a dropdown menu set to 'APP default', and a pencil icon. Below this are 'IPS' and 'DLP Sensor' toggle switches (both off), and 'SSL/SSH Inspection' with a dropdown set to 'certificate-inspection' and a pencil icon. The 'Logging Options' section is also highlighted with a red box and contains a toggle switch for 'Log Allowed Traffic' (turned on), a dropdown menu set to 'Security Events', and a green button labeled 'All Sessions'. Below this are 'Generate Logs when Session Starts' and 'Capture Packets' toggle switches (both off). At the bottom, there is a 'Comments' section with a text input field containing 'Write a comment...' and a character count '0/1023'. An 'Enable this policy' toggle switch is turned on. At the very bottom, there is a large 'VCEplus' watermark and two buttons: 'OK' and 'Cancel'.

QUESTION 21

A company needs to provide SSL VPN access to two user groups. The company also needs to display different welcome messages on the SSL VPN login screen for both user groups.

What is required in the SSL VPN configuration to meet these requirements?

- A. Two separated SSL VPNs in different interfaces of the same VDOM
- B. Different SSL VPN realms for each group
- C. Different virtual SSLVPN IP addresses for each group
- D. Two firewall policies with different captive portals

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:



The screenshot shows a web browser window with the address bar displaying `cookbook.fortinet.com/multi-realm-ssl-vpn/`. The page content includes three paragraphs: 1) An introduction stating the recipe will teach how to create a multi-realm SSL VPN tunnel with different portals for different user groups. 2) An example scenario where user `ckent` has full access to both web portal and tunnel mode, while user `dprince` has web-only access, and testing is done with Mozilla Firefox and FortiClient. 3) Prerequisites stating a local interface must be configured on the FortiGate and SSL-VPN Realms must be enabled in the Features store (System > Config > Features).

QUESTION 22

Examine the routing database.



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

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

- A. The `port3` default route has the lowest metric, making it the best route.
- B. There will be eight routes active in the routing table.
- C. The `port3` default has a higher distance than the `port1` and `port2` default routes.

D. Both port1 and port2 default routers are active in the routing table.

Correct Answer: CD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 23

View the exhibit.



When a user attempts to connect to an HTTPS site, what is the expected result with this configuration?

- A. The user is required to authenticate before accessing sites with untrusted SSL certificates.
- B. The user is presented with certificate warnings when connecting to sites that have untrusted SSL certificates.
- C. The user is allowed access all sites with untrusted SSL certificates, without certificate warnings.
- D. The user is blocked from connecting to sites that have untrusted SSL certificates (no exception provided).

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 24

View the exhibit.

Edit Interface	
Interface Name	port1 (00:0C:29:29:38:DA)
Alias	<input type="text"/>
Link Status	Up
Type	Physical Interface
Virtual Domain	root
Role	Undefined

When **Role** is set to **Undefined**, which statement is true?

- A. The GUI provides all the configuration options available for the **port1** interface.
- B. You cannot configure a static IP address for the **port1** interface because it allows only DHCP addressing mode.
- C. Firewall policies can be created from only the **port1** interface to **any** interface.
- D. The **port1** interface is reserved for management only.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 25

Which statement is true regarding the policy ID numbers of firewall policies?

- A. Change when firewall policies are re-ordered.
- B. Defines the order in which rules are processed.
- C. Are required to modify a firewall policy from the CLI.
- D. Represent the number of objects used in the firewall policy.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

The ID no change when re-ordered and the rules are processed to top to bottom not by ID.

ID	Seq.#	Name	Source	Destination
port1 - port2 (1 - 2)				
2	1	VALID2	autoupdate.opera.com	all
1	2	VALID	Prueba	all

QUESTION 26

An administrator needs to inspect all web traffic (including Internet web traffic) coming from users connecting to SSL VPN. How can this be achieved?

- A. Disabling split tunneling
- B. Configuring web bookmarks
- C. Assigning public IP addresses to SSL VPN clients
- D. Using web-only mode

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:



QUESTION 27

Which traffic inspection features can be executed by a security processor (SP)? (Choose three.)

- A. TCP SYN proxy
- B. SIP session helper
- C. Proxy-based antivirus
- D. Attack signature matching
- E. Flow-based web filtering



Correct Answer: CDE

Section: (none)

Explanation

Explanation/Reference:

QUESTION 28

An administrator has configured two VLAN interfaces:

```
config system interface
  edit "VLAN10"
    set vdom "VDM1"
    set forward-domain 100
    set role lan
    set interface "port9"
    set vlanid 10
  next
  edit "VLAN5"
    set vdom "VDM1"
    set forward-domain 50
    set role lan
    set interface "port10"
    set vlanid 5
  next
end
```



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

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

```
4.126138 vlan160_p2 in 192.168.182.93 -> 192.168.182.78: icmp: echo request
4.126190 vlan18_p3 out 192.168.182.93 -> 192.168.182.78: icmp: echo request
4.126196 port3 out 192.168.182.93 -> 192.168.182.78: icmp: echo request
4.126628 vlan18_p3 in 192.168.182.78 -> 192.168.182.93: icmp: echo reply
4.126661 vlan160_p2 out 192.168.183.48 -> 192.168.182.93: icmp: echo reply
4.126667 port2 out 192.168.183.48 -> 192.168.182.93: icmp: echo reply
```

Forwarding Domains

A forwarding domain is used to create separate broadcast domains and confine traffic across two or more ports. It also allows learning the same MAC in different VLANs (IVL). See section "VLAN trunking and MAC address learning" on page 20 for more details.

A forwarding domain and its associated ID number are unique across one VDOM, or a FortiGate with VDOMs disabled. Each new VDOM will create a new bridge instance in the FortiGate.



Even though the forwarding domain ID is not in relation with the actual VLAN numbers, it is recommended, for maintenance and troubleshooting purposes, to configure one forwarding domain per VLAN and use the same forwarding domain ID as the VLANs ID.

Once forwarding domains are configured, it is possible to configure firewall policies only between ports or VLAN belonging to the same forwarding domain.



QUESTION 29
View the exhibit.

Application Details

Name	Category	Technology	Popularity	Risk
Addicting.Games	Game	Browser-Based	☆☆☆☆	Exempt

Application Control Profile

Categories

Botnet	Game	Proxy	Video/Audio
Business	General Interest	Remote Access	VoIP
Cloud.IT	Mobile	Social Media	Web.Client
Collaboration	Network.Service	Storage.Backup	Unknown Applications
Email	P2P	Update	

Application Overrides

+ Add Signatures Edit Parameters Delete

Application Signature	Category	Action
Addicting.Games	Game	Monitor

Filter Overrides

+ Add Filter Edit Delete

Filter Details	Action
Risk: Low	Block

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

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 30

What are the purposes of NAT traversal in IPsec? (Choose two.)

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

Correct Answer: AB

Section: (none)

Explanation

Explanation/Reference:

QUESTION 31

Which statements about application control are true? (Choose two.)

- A. Enabling application control profile in a security profile enables application control for all the traffic flowing through the FortiGate.
- B. It cannot take an action on unknown applications.
- C. It can inspect encrypted traffic.
- D. It can identify traffic from known applications, even when they are using non-standard TCP/UDP ports.

Correct Answer: CD

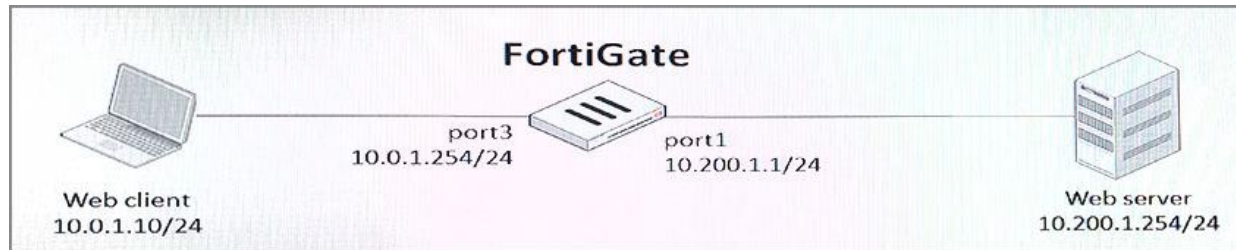
Section: (none)

Explanation

Explanation/Reference:

QUESTION 32

View the exhibit.



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

```

FortiGate # diagnose sniffer packet any "port 80" 4
interfaces=[any]
filters=[port 80]
11.510058 port3 in 10.0.1.10.49255 -> 10.200.1.254.80: syn 697263124
11.760531 port3 in 10.0.1.10.49255 -> 10.200.1.254.80: syn 868017830
14.505371 port3 in 10.0.1.10.49255 -> 10.200.1.254.80: syn 697263124
14.755510 port3 in 10.0.1.10.49255 -> 10.200.1.254.80: syn 868017830
  
```

What should be done next to troubleshoot the problem?

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 33

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

- A. It is useful when users log in to DCs that are not monitored by a collector agent.
- B. It takes over as the primary authentication method when configured alongside FSSO.

- C. Multi-domain environments require DC agents on every domain controller.
- D. NTLM-enabled web browsers are required.

Correct Answer: AD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 34

What FortiGate feature can be used to allow IPv6 clients to connect to IPv4 servers?

- A. IPv6-over-IPv4 IPsec
- B. NAT64
- C. IPv4-over-IPv6 IPsec
- D. NAT66

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:



QUESTION 35

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

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

Correct Answer: AC

Section: (none)

Explanation

Explanation/Reference:

QUESTION 36

View the exhibit.

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

Which statements about the exhibit are true? (Choose two.)

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

Correct Answer: AD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 37

Which statement about the firewall policy authentication timeout is true?

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 38

Which of the following settings and protocols can be used to provide secure and restrictive administrative access to FortiGate? (Choose three.)

- A. Trusted host
- B. HTTPS
- C. Trusted authentication
- D. SSH
- E. FortiTelemetry

Correct Answer: ABD

Section: (none)

Explanation

Explanation/Reference:



QUESTION 39

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

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 40

How can a browser trust a web-server certificate signed by a third party CA?

- A. The browser must have the CA certificate that signed the web-server certificate installed.
- B. The browser must have the web-server certificate installed.
- C. The browser must have the private key of CA certificate that signed the web-browser certificate installed.
- D. The browser must have the public key of the web-server certificate installed.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 41

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

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 42

An administrator has enabled proxy-based antivirus scanning and configured the following settings:

```
config firewall profile-protocol-options
edit default
config http
set oversize-limit 10
set options oversize
end
end
```

Which statement about the above configuration is true?

- A. Files bigger than 10 MB are not scanned for viruses and will be blocked.
- B. FortiGate scans only the first 10 MB of any file.
- C. Files bigger than 10 MB are sent to the heuristics engine for scanning.
- D. FortiGate scans the files in chunks of 10 MB.

Correct Answer: A

Section: (none)

Explanation



Explanation/Reference:

QUESTION 43

Examine this output from the `diagnose sys top` command:

```
# diagnose sys top 1
Run Time: 11 days, 3 hours and 29 minutes
ON, 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 about the output are true? (Choose two.)

- A. `sshd` is the process consuming most memory
- B. `sshd` is the process consuming most CPU
- C. All the processes listed are in sleeping state
- D. The `sshd` process is using 123 pages of memory

Correct Answer: BC

Section: (none)

Explanation

Explanation/Reference:

QUESTION 44

An administrator has created a custom IPS signature. Where does the custom IPS signature have to be applied?

- A. In an IPS sensor
- B. In an interface.
- C. In a DoS policy.
- D. In an application control profile.



Correct Answer: A

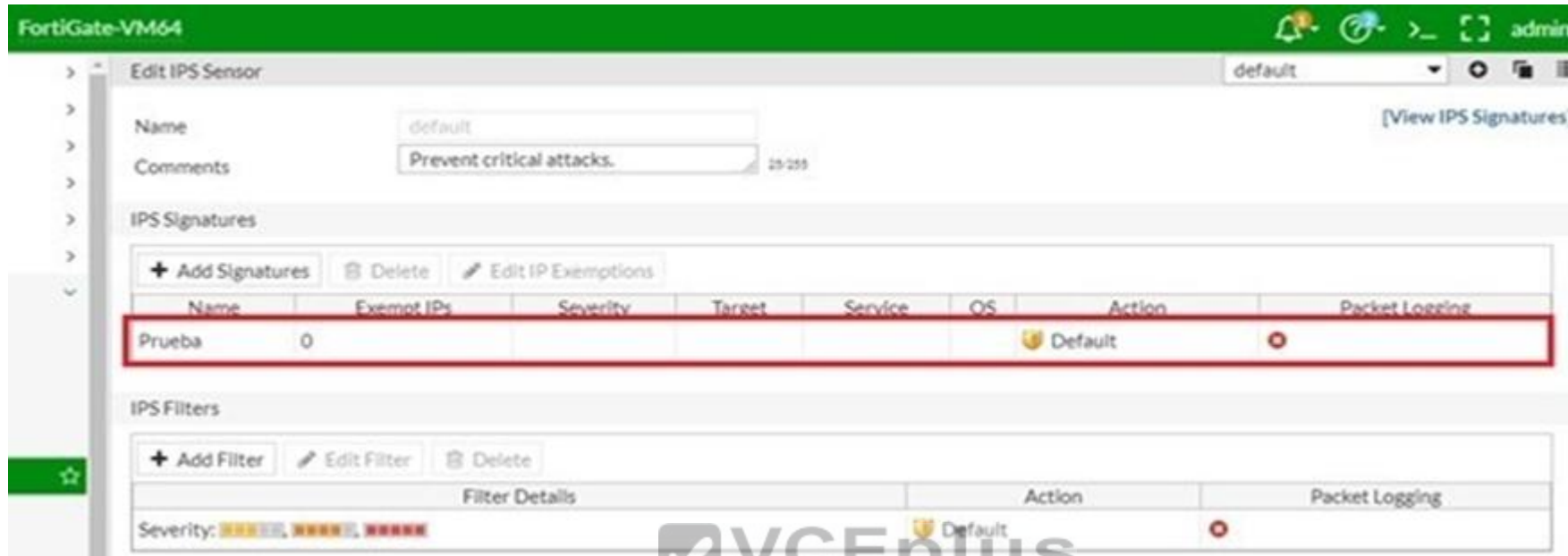
Section: (none)

Explanation

Explanation/Reference:

Explanation:

I create a custom signature then I try to add and appear only in IPS sensor.



QUESTION 45

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

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 46

Which statements about high availability (HA) for FortiGates are true? (Choose two.)

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

Correct Answer: AC

Section: (none)

Explanation

Explanation/Reference:

QUESTION 47

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

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

Correct Answer: AB

Section: (none)

Explanation

Explanation/Reference:

QUESTION 48

Which statement about the FortiGuard services for the FortiGate is true?

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

Correct Answer: A

Section: (none)

Explanation:

AntiVirus	Licensed (Expires on)	Upload Package
AV Definitions	Version 50.00823	
AV Engine	Version 5.00247	
Botnet IPs	Version 4.00022	View List
Botnet Domains	Version 1.00791	View List

Which statements about antivirus scanning using flow-based full scan are true? (Choose two.)

- VCeplus**
The first connection attempt only if a virus
VCE To PDF - Free Practice Exam

Section: (none)

Explanation

Explanation/Reference:

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

- A. A phase 2 configuration is not required.
- B. This VPN cannot be used as part of a hub and spoke topology.
- C. The IPsec firewall policies must be placed at the top of the list.
- D. A virtual IPsec interface is automatically created after the phase 1 configuration is completed.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 51

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

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:



QUESTION 52

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

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Central NAT Table

The central NAT table enables you to define, and control with more granularity, the address translation performed by the FortiGate unit. With the NAT table, you can define the rules which dictate the source address or address group and which IP pool the destination address uses.

While similar in functionality to IP pools, where a single address is translated to an alternate address from a range of IP addresses, with IP pools there is no control over the translated port. When using the IP pool for source NAT, you can define a fixed port to guarantee the source port number is unchanged. If no fix port is defined, the port translation is randomly chosen by the FortiGate unit. With the central NAT table, you have full control over both the IP address and port translation.

The FortiGate unit reads the NAT rules in a top-down methodology, until it hits a matching rule for the incoming address. This enables you to create multiple NAT policies that dictate which IP pool is used based on the source address. The NAT policies can be rearranged within the policy list as well. NAT policies are applied to network traffic after a security policy.

QUESTION 53

When using WPAD DNS method, what is the FQDN format that browsers use to query the DNS server?

- A. wpad.<local-domain>
- B. srv_tcp.wpad.<local-domain>
- C. srv_proxy.<local-domain>/wpad.dat
- D. proxy.<local-domain>.wpad



Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 54

An administrator is using the FortiGate built-in sniffer to capture HTTP traffic between a client and a server, however, the sniffer output shows only the packets related with TCP session setups and disconnections. Why?

- A. The administrator is running the sniffer on the internal interface only.
- B. The filter used in the sniffer matches the traffic only in one direction.
- C. The FortiGate is doing content inspection.
- D. TCP traffic is being offloaded to an NP6.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 55

Which of the following statements about advanced AD access mode for FSSO collector agent are true? (Choose two.)

- A. It is only supported if DC agents are deployed.
- B. FortiGate can act as an LDAP client configure the group filters.
- C. It supports monitoring of nested groups.
- D. It uses the Windows convention for naming, that is, Domain\Username.

Correct Answer: BC

Section: (none)

Explanation

Explanation/Reference:



QUESTION 56

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

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

Correct Answer: AC

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Address	autoupdate.opera.com
Type	FQDN
FQDN	autoupdate.opera.com
Interface	<input type="checkbox"/> any
Resolved To	Unresolved FQDN: autoupdate.opera.com

Address	User	Device
Search		
ADDRESS (7)		
autoupdate.opera.com		

Select Entries

Address

User

Device

Q Search

+

USER (1)

Local (1)

guest

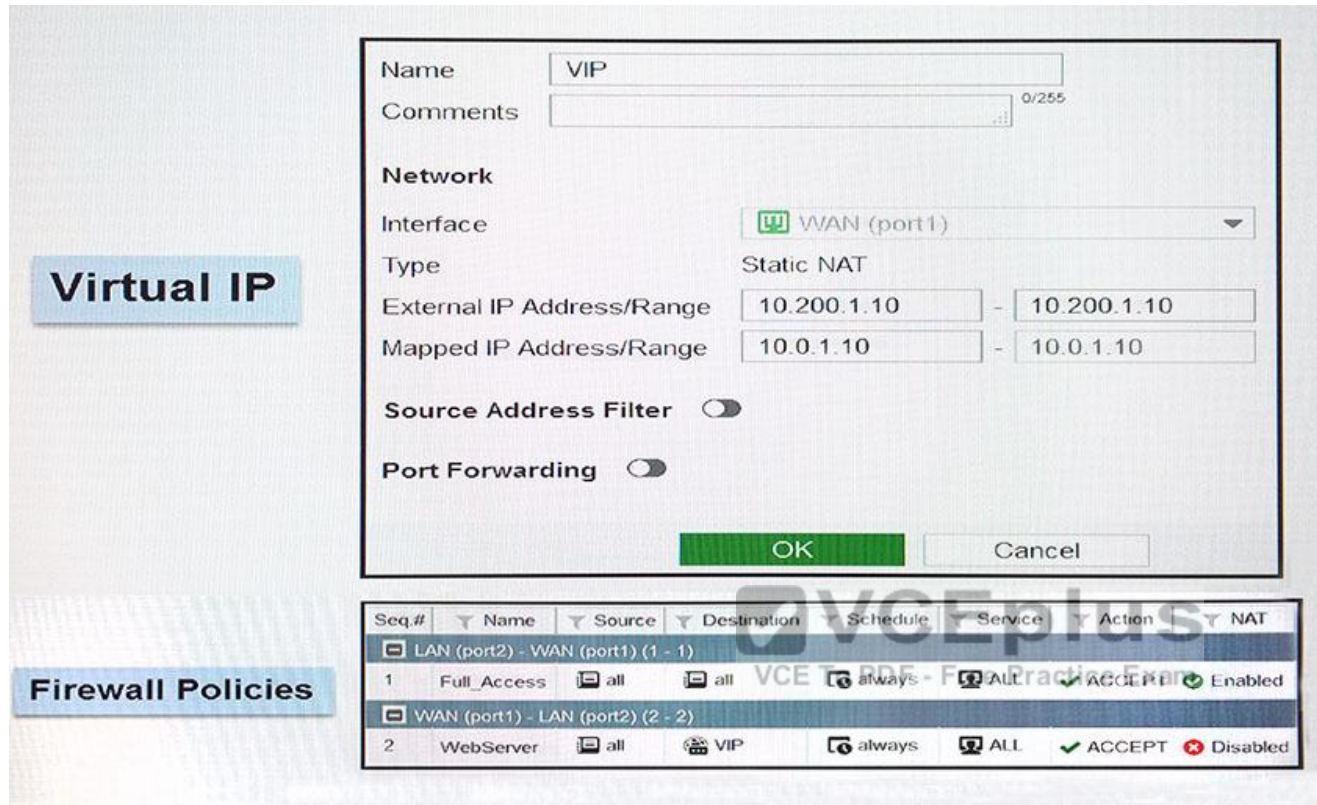
USER GROUP (2)

Guest-group

SSO_Guest_Users

QUESTION 57

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



The **WAN(port1)** interface has the IP address 10.200.1.1/24. The **LAN(port2)** interface has the IP address 10.0.1.254/24.

The top firewall policy has NAT enabled using outgoing interface address. The second firewall policy configured with a virtual IP (**VIP**) as the destination address.

Which IP address will be used to source NAT the Internet traffic coming from a workstation with the IP address 10.0.1.10/24?

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 58

Which statement about data leak prevention (DLP) on a FortiGate is true?

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:



QUESTION 59

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

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

Correct Answer: CD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 60

Which statements about IP-based explicit proxy authentication are true? (Choose two.)

- A. IP-based authentication is best suited to authenticating users behind a NAT device.
- B. Sessions from the same source address are treated as a single user.
- C. IP-based authentication consumes less FortiGate's memory than session-based authentication.
- D. FortiGate remembers authenticated sessions using browser cookies.

Correct Answer: BC

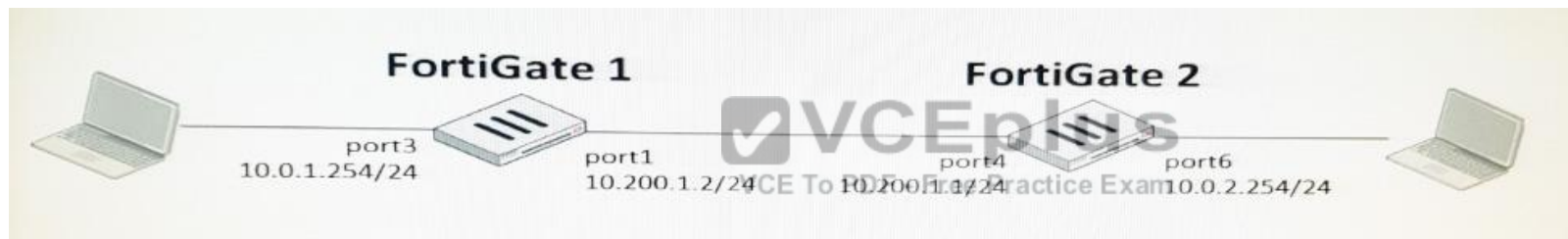
Section: (none)

Explanation

Explanation/Reference:

QUESTION 61

View the Exhibit.



The administrator needs to confirm that FortiGate 2 is properly routing that traffic to the 10.0.1.0/24 subnet. The administrator needs to confirm it by sending ICMP pings to FortiGate 2 from the CLI of FortiGate 1. What ping option needs to be enabled before running the ping?

- A. Execute ping-options source port1
- B. Execute ping-options source 10.200.1.1.
- C. Execute ping-options source 10.200.1.2
- D. Execute ping-options source 10.0.1.254

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 62

How can you format the FortiGate flash disk?

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 63

How do you configure inline SSL inspection on a firewall policy? (Choose two.)

- A. Enable one or more flow-based security profiles on the firewall policy.
- B. Enable the SSL/SSH Inspection profile on the firewall policy.
- C. Execute the inline ssl inspection CLI command.
- D. Enable one or more proxy-based security profiles on the firewall policy.

Correct Answer: AB

Section: (none)

Explanation

Explanation/Reference:

QUESTION 64

Which traffic sessions can be offloaded to a NP6 processor? (Choose two.)

- A. IPv6
- B. RIP
- C. GRE
- D. NAT64

Correct Answer: AD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 65

View the exhibit.

```
#diagnose hardware sysinfo shm
```

```
SHM COUNTER:          10316
```

```
SHM allocated:        617643792
```

```
SHM total:            1572380672
```

```
conserve mode:        on-mem
```

```
system last entered:  Fri Jun 3 10:16:39 2016
```

```
sys fd last entered:   n/a
```

```
SHM FS total:          1607806976
```

```
SHM FS free:           990134272
```

```
SHM FS avail:          990134272
```

```
SHM FS alloc:          617672704
```

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

- A. FortiGate generated an event log for system conserve mode.
- B. FortiGate has entered in to system conserve mode.
- C. By default, the FortiGate blocks new sessions.
- D. FortiGate changed the global av-failopen settings to idledrop.

Correct Answer: BC

Section: (none)

Explanation

Explanation/Reference:**QUESTION 66**

An administrator has blocked Netflix login in a cloud access security inspection (CASI) profile. The administrator has also applied the CASI profile to a firewall policy.

What else is required for the CASI profile to work properly?

- A. You must enable logging for security events on the firewall policy.
- B. You must activate a FortiCloud account.
- C. You must apply an application control profile to the firewall policy.
- D. You must enable SSL inspection on the firewall policy.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

**QUESTION 67**

How does FortiGate look for a matching firewall policy to process traffic?

- A. From top to bottom, based on the sequence numbers.
- B. Based on best match.
- C. From top to bottom, based on the policy ID numbers.
- D. From lower to higher, based on the priority value.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 68

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

- A. Apply an application control profile allowing BitTorrent to a firewall policy and configure a traffic shaping policy.
- B. Enable the shape option in a firewall policy with service set to BitTorrent.
- C. Apply a traffic shaper to a BitTorrent entry in the SSL/SSH inspection profile.
- D. Apply a traffic shaper to a protocol options profile.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 69

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

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



Correct Answer: AD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 70

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 71**

Examine this output from a debug flow:

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

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

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

Correct Answer: AC

Section: (none)

Explanation**Explanation/Reference:****QUESTION 72**

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 73

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 74

What statement describes what DNS64 does?

- 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 75

What does the command `diagnose debug fsso-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 76

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 77

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 78

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 79**

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?

- 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 80

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 81

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 82**

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 83**

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 84**

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

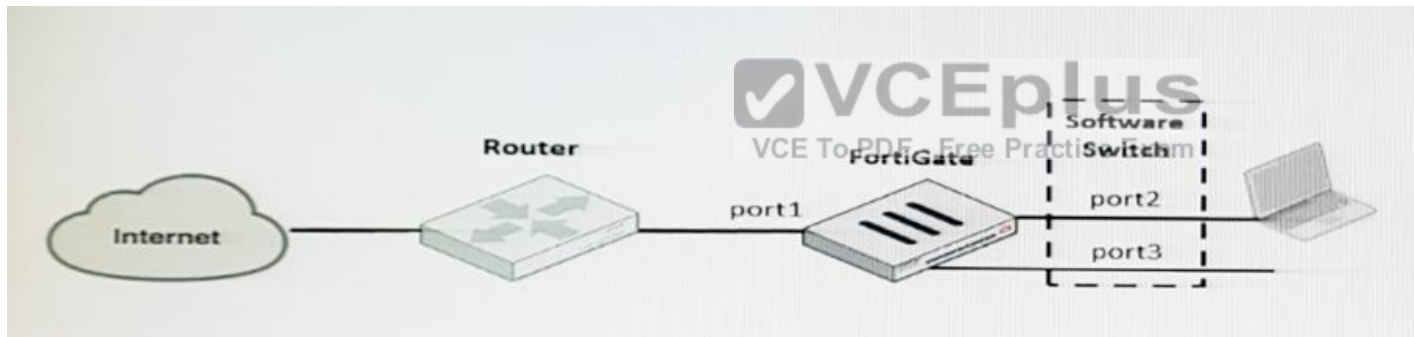
Section: (none)

Explanation

Explanation/Reference:

QUESTION 85

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 86

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 87

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

MAC Reservation + Access Control		
<div> + Create New Edit Delete Add from DHCP Client List </div>		
MAC Address	Action or IP	Description
00:0c:29:29:38:da	10.0.1.254	
Unknown MAC Addresses	Block	
Type	<div> Regular IPsec </div>	

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 88

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 89

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 90**

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

- 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 91**

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

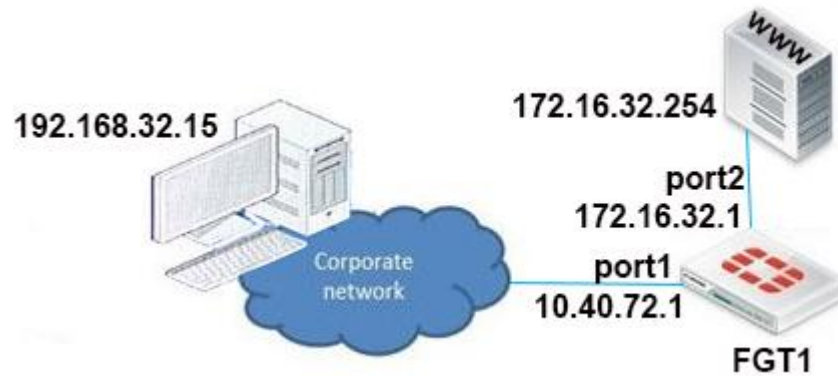
- A. You must enable one or more protocols that support active authentication on a firewall policy.
- B. You must assign users to a group for active authentication.
- C. You must place the firewall policy for active authentication before a firewall policy for passive authentication.
- D. You must enable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

Correct Answer: B

Section: (none)

Explanation**Explanation/Reference:****QUESTION 92**

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 93

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 94

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

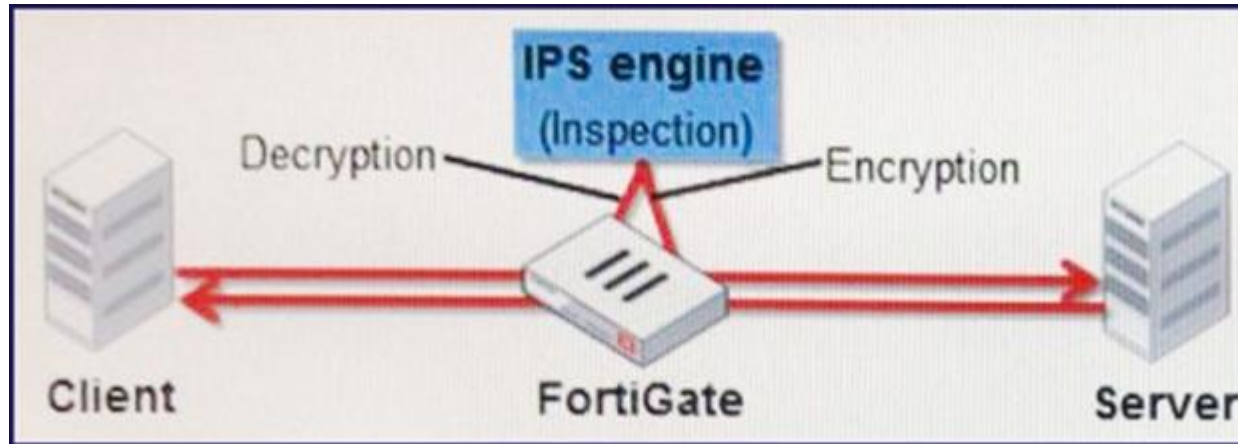
Section: (none)

Explanation

Explanation/Reference:

QUESTION 95

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 96

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 97

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 98

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 99

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 100

Examine the following web filtering log.

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

Which statement about the log message is true?

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 101

Examine this output from a debug flow:

```
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"
```

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

- 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)

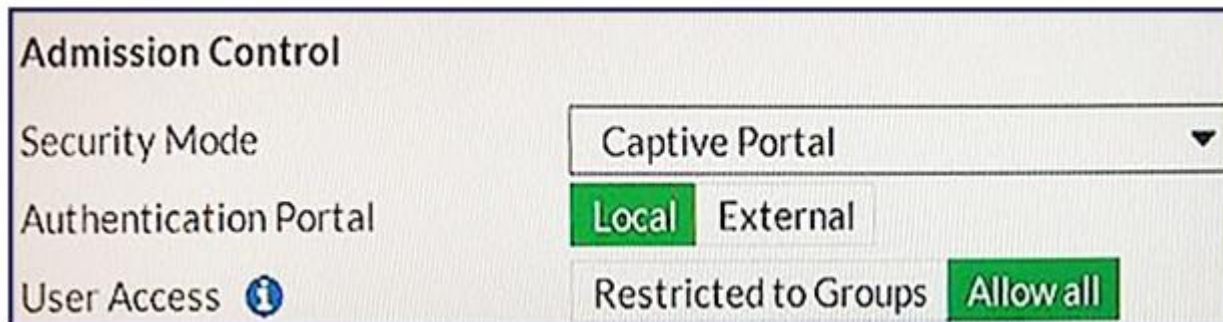
Explanation

Explanation/Reference:



QUESTION 102

View the exhibit.



The screenshot shows the 'Admission Control' configuration page in FortiGate. It includes the following settings:

- Security Mode:** Captive Portal (selected from a dropdown menu)
- Authentication Portal:** Local (selected button), External (unselected button)
- User Access:** Restricted to Groups (selected button), Allow all (unselected button)

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 103

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 104

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 105**

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 106**

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 107**

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 108

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 109

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 temporally disabled while upgrading the firmware.

Correct Answer: BD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 110

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

```
Local-FortiGate # diagnose debug enable

Local-FortiGate # diagnose debug application urlfilter -1

Local-FortiGate # msg= "received a request /tmp/.wad_192_0_0.url.socket,
=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= "/"
```

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

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 111

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 112

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 113

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 114

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.)

- 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 115

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:

<div> Create New Edit Delete Section View Global View Search </div>						
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 116

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 117

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 118

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 119

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 120

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 121

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 122

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 123

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

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

Correct Answer: BC

Section: (none)

Explanation

Explanation/Reference:

QUESTION 124

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 125

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 126

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 127

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 128

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 129

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 130

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 131

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 132

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 133**

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 134**

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

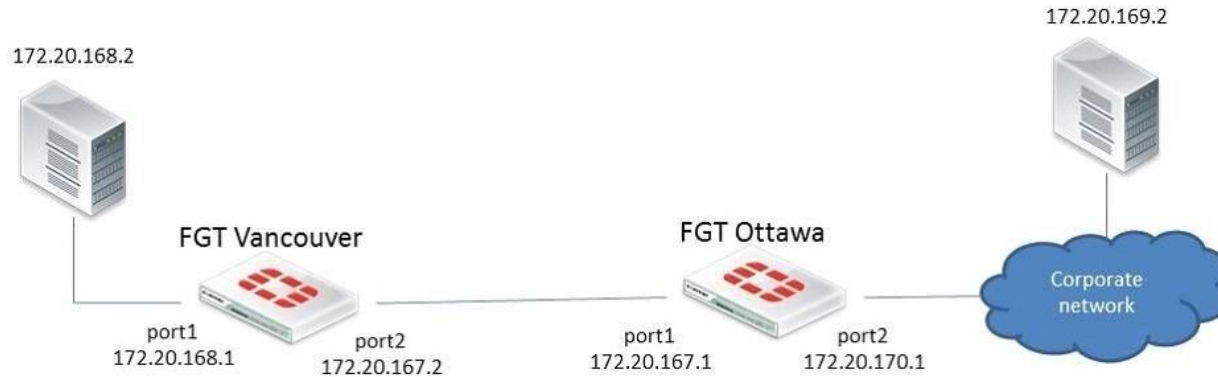
Section: (none)

Explanation

Explanation/Reference:

QUESTION 135

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?

- 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 136

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
S    *>          [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 137

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 allow-subnet-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 138

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 139

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 140

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 141

A FortiGate administrator with the super_admin profile configures a virtual domain (VDOM) for a new customer. After creating the VDOM, the administrator is unable to reassign the dmz interface to the new VDOM as the option is greyed out in the GUI in the management VDOM. 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 VDOM.
- C. Non-management VDOMs cannot reference physical interfaces.
- D. The dmz interface is in PPPoE or DHCP mode.

Correct Answer: B

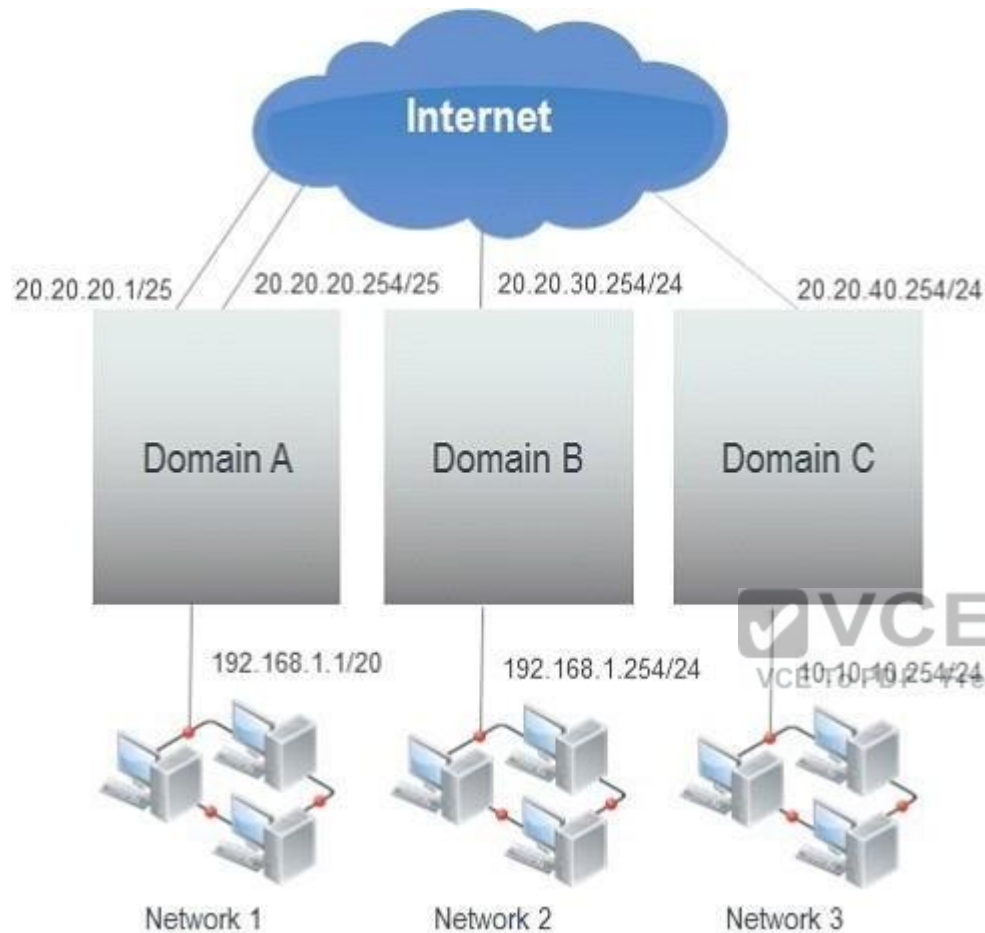
Section: (none)

Explanation

Explanation/Reference:

QUESTION 142

A FortiGate unit is configured with three Virtual Domains (VDOMs) 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 143

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 144

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 145

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 146

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 147

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 148

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 149

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

Destination IP/Mask	<input type="text" value="10.0.2.0/255.255.255"/>	
Device	<input type="text" value="remote"/>	
Distance	<input type="text" value="10"/>	(1-255, Default=10)
Priority	<input type="text" value="0"/>	(0-4294967295)
Comments	<input type="text" value="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 150

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 eeeecac3a58161f3390fa612b794c776654c86aef51fbc7542906223d56ebb3
      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 151

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

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

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 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 152

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

- 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:

QUESTION 153

Review the IKE debug output for IPsec shown in the exhibit below.

```
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 9E2606AC7AE83D7A612DA78D3AB3F94508100501734C5CDF000000540B0000181C047F014CBEF1BOEC8DA915F3B18AE
A000000200000000101108D299E2606AC7AE83D7A612DA78D3AB3F9450000009C
ike 0:Remote_1:10: out 9E2606AC7AE83D7A612DA78D3AB3F94508100501734C5CDF0000005CB3CC431065A1737144B02F1AACE79C1BE712B84
BB84E5FA7A967FE99C7B731057FF33728BB42AA983E79C919DA9B64EBC087EFOA02666C1FBD2C62F
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
```

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 154

Review the configuration for FortiClient IPsec shown in the exhibit.

New FortiClient VPN

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

OK Cancel

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 155

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

Name remote

Comments VPN: remote (Created by VPN wizard)

Network ✓✕

IP Version IPv4

Remote Gateway Static IP Address

IP Address 10.200.3.1

Interface port1

Mode Config ☐

NAT Traversal ☒

Keepalive Frequency 10

Dead Peer Detection ☒

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 156

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 lgyy=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 9e2c5d0fc055fa0149bd66024732e9a85bbe8016
-----
```

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 157

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 158

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 159

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 160

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 161

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 162

Which is the following statement 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 163

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 164

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 165

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 166

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 167

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 168**

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 169**

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 170**

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.
- 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 171

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 172

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 173

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

```
# diagnose sys top 1
Run Time: 11 days, 3 hours and 29 minutes
0U, 0N, 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 174

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 175

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 176

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 177

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 178

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 179

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 180

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 181

Two FortiGate units with NP6 processors form an active-active cluster. The cluster is doing security profile (UTM) inspection over all the user traffic. What statements are true regarding the sessions that the master unit is offloading to the slave unit for inspection? (Choose two.)

- A. They are accelerated by hardware in the master unit.
- B. They are not accelerated by hardware in the master unit.
- C. They are accelerated by hardware in the slave unit.
- D. They are not accelerated by hardware in the slave unit.



Correct Answer: AD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 182

How is the FortiGate password recovery process?

- A. Interrupt boot sequence, modify the boot registry and reboot. After changing the password, reset the boot registry.
- B. Log in through the console port using the "maintainer" account within several seconds of physically power cycling the FortiGate.
- C. Hold down the CTRL + Esc (Escape) keys during reboot, then reset the admin password.
- D. Interrupt the boot sequence and restore a configuration file for which the password has been modified.

Correct Answer: B

Section: (none)

Explanation**Explanation/Reference:****QUESTION 183**

What are valid options for handling DNS requests sent directly to a FortiGate's interface IP? (Choose three.)

- A. Conditional-forward.
- B. Forward-only.
- C. Non-recursive.
- D. Iterative.
- E. Recursive.

Correct Answer: BCE

Section: (none)

Explanation**Explanation/Reference:****QUESTION 184**

When creating FortiGate administrative users, which configuration objects specify the account rights?

- A. Remote access profiles.
- B. User groups.
- C. Administrator profiles.
- D. Local-in policies.

Correct Answer: C

Section: (none)

Explanation**Explanation/Reference:****QUESTION 185**

Which statements are true regarding the factory default configuration? (Choose three.)

- A. The default web filtering profile is applied to the first firewall policy.
- B. The 'Port1' or 'Internal' interface has the IP address 192.168.1.99.
- C. The implicit firewall policy action is ACCEPT.
- D. The 'Port1' or 'Internal' interface has a DHCP server set up and enabled (on device models that support DHCP servers).
- E. Default login uses the username: admin (all lowercase) and no password.

Correct Answer: BDE

Section: (none)

Explanation

Explanation/Reference:

QUESTION 186

What methods can be used to access the FortiGate CLI? (Choose two.)

- A. Using SNMP.
- B. A direct connection to the serial console port.
- C. Using the CLI console widget in the GUI.
- D. Using RCP.



Correct Answer: BC

Section: (none)

Explanation

Explanation/Reference:

QUESTION 187

What capabilities can a FortiGate provide? (Choose three.)

- A. Mail relay.
- B. Email filtering.
- C. Firewall.
- D. VPN gateway.
- E. Mail server.

Correct Answer: BCD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 188

Which network protocols are supported for administrative access to a FortiGate unit? (Choose three.)

- A. SNMP
- B. WINS
- C. HTTP
- D. Telnet
- E. SSH

Correct Answer: CDE

Section: (none)

Explanation

Explanation/Reference:



QUESTION 189

Which is an advantage of using SNMP v3 instead of SNMP v1/v2 when querying a FortiGate unit?

- A. MIB-based report uploads.
- B. SNMP access limited by access lists.
- C. Packet encryption.
- D. Running SNMP service on a non-standard port is possible.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 190

What logging options are supported on a FortiGate unit? (Choose two.)

- A. LDAP
- B. Syslog
- C. FortiAnalyzer
- D. SNMP

Correct Answer: BC

Section: (none)

Explanation

Explanation/Reference:

QUESTION 191

What is the maximum number of FortiAnalyzer/FortiManager devices a FortiGate unit can be configured to send logs to?

- A. 1
- B. 2
- C. 3
- D. 4

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 192

Regarding the header and body sections in raw log messages, which statement is correct?

- A. The header and body section layouts change depending on the log type.
- B. The header section layout is always the same regardless of the log type. The body section layout changes depending on the log type.
- C. Some log types include multiple body sections.
- D. Some log types do not include a body section.

Correct Answer: B

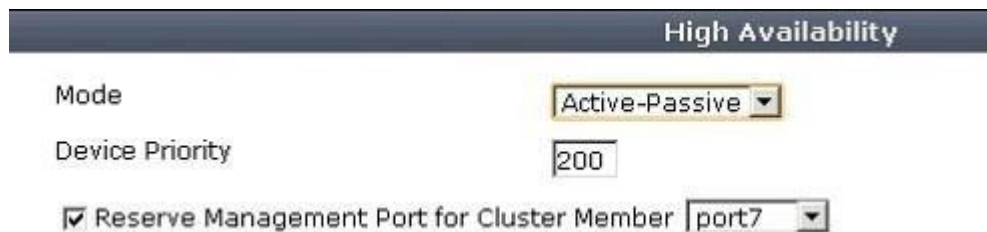
Section: (none)

Explanation

Explanation/Reference:

QUESTION 193

In HA, the option Reserve Management Port for Cluster Member is selected as shown in the exhibit below.



The screenshot shows the 'High Availability' configuration window in a FortiGate device. It includes the following settings:

- Mode:** Active-Passive (selected from a dropdown menu)
- Device Priority:** 200 (entered in a text box)
- Reserve Management Port for Cluster Member:** port7 (selected from a dropdown menu, with a checked checkbox)

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

- A. Interface settings on port7 will not be synchronized with other cluster members.
- B. The IP address assigned to this interface must not overlap with the IP address subnet assigned to another interface.
- C. When connecting to port7 you always connect to the master device.
- D. A gateway address may be configured for port7.

Correct Answer: AD

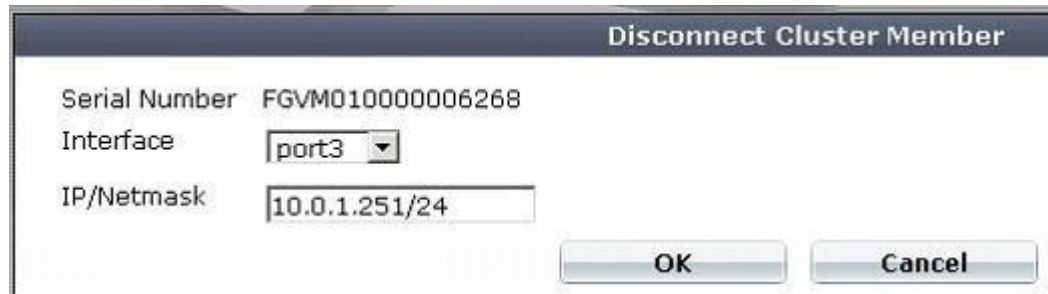
Section: (none)

Explanation

Explanation/Reference:

QUESTION 194

The exhibit shows the Disconnect Cluster Member command in a FortiGate unit that is part of a HA cluster with two HA members.



What is the effect of the Disconnect Cluster Member command as given in the exhibit. (Choose two.)

- A. Port3 is configured with an IP address for management access.
- B. The firewall rules are purged on the disconnected unit.
- C. The HA mode changes to standalone.
- D. The system hostname is set to the unit serial number.

Correct Answer: AC

Section: (none)

Explanation

Explanation/Reference:

QUESTION 195

Which firewall objects can be included in the Destination Address field of a firewall policy? (Choose three.)

- A. IP address pool.
- B. Virtual IP address.
- C. IP address.
- D. IP address group.
- E. MAC address

Correct Answer: BCD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 196

Which header field can be used in a firewall policy for traffic matching?

- A. ICMP type and code.
- B. DSCP.
- C. TCP window size.
- D. TCP sequence number.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 197

The order of the firewall policies is important. Policies can be re-ordered from either the GUI or the CLI. Which CLI command is used to perform this function?

- A. set order
- B. edit policy
- C. reorder
- D. move

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 198

Examine the following CLI configuration:

```
config system session-ttl
set default 1800
end
```

What statement is true about the effect of the above configuration line?

- A. Sessions can be idle for more than 1800 seconds.
- B. The maximum length of time a session can be open is 1800 seconds.
- C. After 1800 seconds, the end user must re-authenticate.
- D. After a session has been open for 1800 seconds, the FortiGate sends a keepalive packet to both client and server.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 199

In which order are firewall policies processed on a FortiGate unit?

- A. From top to down, according with their sequence number.
- B. From top to down, according with their policy ID number.
- C. Based on best match.
- D. Based on the priority value.



Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 200

Which statements are true regarding local user authentication? (Choose two.)

- A. Two-factor authentication can be enabled on a per user basis.
- B. Local users are for administration accounts only and cannot be used to authenticate network users.
- C. Administrators can create the user accounts is a remote server and store the user passwords locally in the FortiGate.
- D. Both the usernames and passwords can be stored locally on the FortiGate

Correct Answer: AD