Prepare Smart for Success Free Fortinet FCP_FGT_AD-7.6 Exam Questions and Answers

Ready to pass faster? Grab free and updated Fortinet FCP - FortiGate 7.6 Administrator exam PDF questions now. Get authentic FCP_FGT_AD-7.6 dumps packed with verified answers and secure your certification success with PrepBolt FCP_FGT_AD-7.6 exam pdf questions and answers.

Thank you for Downloading FCP_FGT_AD-7.6 exam PDF Demo

https://prepbolt.com/FCP_FGT_AD-7.6.html

Question 1

Question Type: MultipleChoice

You are analyzing connectivity problems caused by intermediate devices blocking traffic in SSL VPN environment.

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

Options:

A- You can turn off IKE fragmentation to fix large certificate negotiation problems.
B- You should use IPsec to solve issues with fragment drops and large certificate exchanges.
C- You can use SSL VPN tunnel mode to prevent problems with blocked ESP and UDP ports (500 or 4500).
D- You can configure a hub-and-spoke topology with SSL VPN tunnels to bypass blocked UDP ports.

Answer:

A, C

Explanation:

Disabling IKE fragmentation helps resolve issues caused by intermediate devices blocking large fragmented packets during certificate negotiation.

Using SSL VPN tunnel mode encapsulates traffic over HTTPS, bypassing blocks on ESP and UDP ports commonly used by IPsec.

Question 2

Question Type: MultipleChoice

You have created a web filter profile named restrict_media-profile with a daily category usage quota.

When you are adding the profile to the firewall policy, the restrict_media-profile is not listed in the available web profile drop down.

What could be the reason?

Options:

A- The firewall policy is in no-inspection mode instead of deep-inspection.
B- The inspection mode in the firewall policy is not matching with web filter profile feature set.
C- The web filter profile is already referenced in another firewall policy.
D- The naming convention used in the web filter profile is restricting it in the firewall policy.

Answer:

B

Explanation:

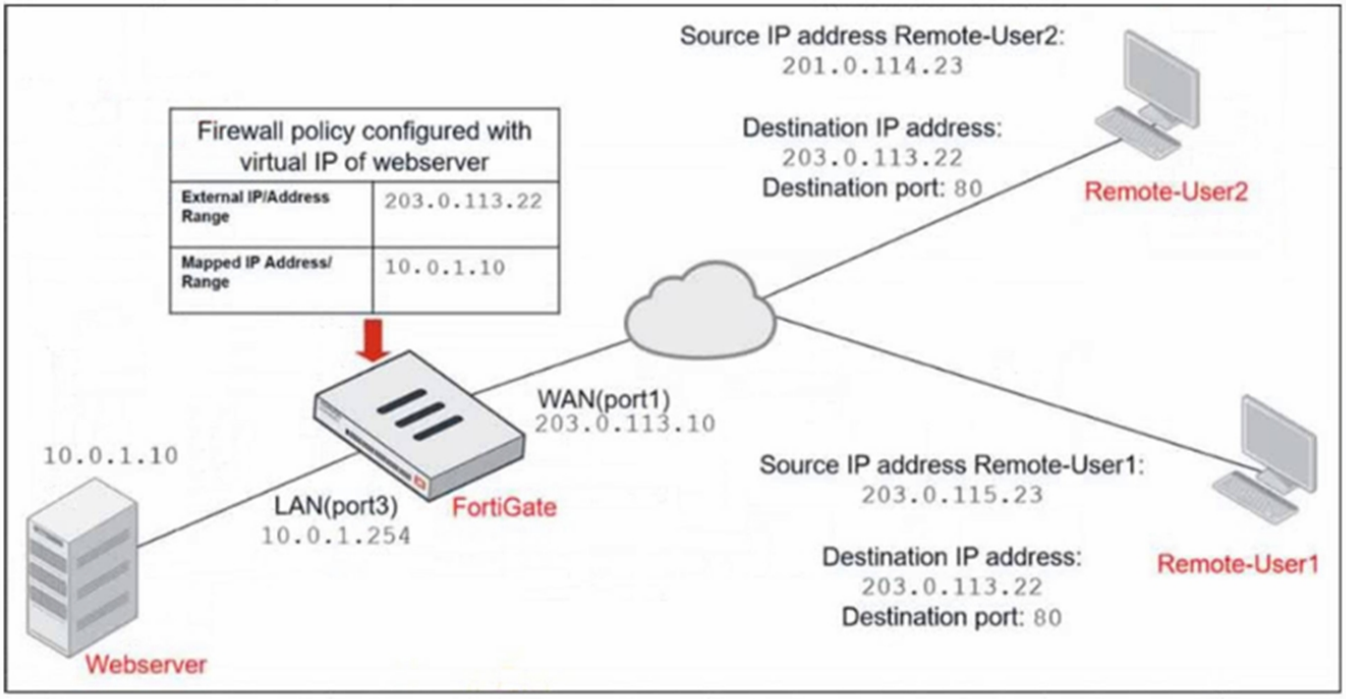
Web filter profiles with category usage quotas require the firewall policy to be in proxy-based (deep) inspection mode; if the inspection mode does not match this requirement, the profile will not appear in the drop-down list.

Question 3

Question Type: MultipleChoice

Refer to the exhibits.

Network diagram



Firewall address object

Firewall policies

ID	Name	Source	Destination	Schedule	Service	Action
WAN (port1) → LAN (port3) 2						
4	Deny	Deny_IP	all	always	ALL	DENY
3	Allow_access	all	Webserver	always	ALL	ACCEPT

The exhibits show a diagram of a FortiGate device connected to the network, and the firewall configuration.

An administrator created a Deny policy with default settings to deny Webserver access for Remote-User2.

The policy should work such that Remote-User1 must be able to access the Webserver while preventing Remote-User2 from accessing the Webserver.

Which additional configuration can the administrator add to a deny firewall policy, beyond the default behavior, to block Remote-User2 from accessing the Webserver?

Options:

A- Disable match-vip in the Allow_access policy
B- Configure a One-to-One IP Pool object in a new policy.
C- Set the Destination address as Webserver in the Deny policy.
D- Set the Destination address as Deny_IP in the Allow_access policy.

Answer:

C

Explanation:

To block Remote-User2's access to the Webserver, the deny policy must explicitly specify the Webserver as the destination address; otherwise, it denies traffic to all destinations, which is not the desired behavior.

Question 4

Question Type: MultipleChoice

Which three statements explain a flow-based antivirus profile? (Choose three.)

Options:

A- FortiGate buffers the whole file but transmits to the client at the same time.
B- Flow-based inspection uses a hybrid of the scanning modes available in proxy-based inspection.
C- If a virus is detected, the last packet is delivered to the client.
D- Flow-based inspection optimizes performance compared to proxy-based inspection.
E- The IPS engine handles the process as a standalone.

Answer:

A, B, D

Explanation:

Flow-based antivirus buffers the entire file while simultaneously transmitting data to the client to minimize latency.

Flow-based inspection combines multiple scanning techniques from proxy-based modes for efficient detection.

Flow-based inspection provides better performance by processing traffic on the fly without full proxy overhead.

Question 5

Question Type: MultipleChoice

An administrator wants to configure dead peer detection (DPD) on IPsec VPN for detecting dead tunnels. The requirement is that FortiGate sends DPD probes only when there is no inbound traffic.

Which DPD mode on FortiGate meets this requirement?

Options:

A- Enabled
B- On Idle
C- Disabled
D- On Demand

Answer:

A

Explanation:

The 'On Idle' DPD mode configures FortiGate to send DPD probes only when no inbound traffic is detected, meeting the requirement to send probes only when the tunnel is idle.

Question 6

Question Type: MultipleChoice

Which three statements about SD-WAN performance SLAs are true? (Choose three.)

Options:

A- They rely on session loss and jitter.

B- They can be measured actively or passively.
C- They are applied in a SD-WAN rule lowest cost strategy.
D- They monitor the state of the FortiGate device.
E- All the SLAtargets can be configured.

Answer:

A, B, E

Explanation:

SD-WAN SLAs monitor metrics like packet loss and jitter to evaluate link performance.

SLA measurements can be performed using active probing or passive monitoring.

Administrators can configure all SLA target parameters to define performance criteria.

Question 7

Question Type: MultipleChoice

A network administrator enabled antivirus and selected an SSL inspection profile on a firewall policy.

When downloading an EICAR test file through HTTP, FortiGate detects the virus and blocks the file. When downloading the same file through HTTPS, FortiGate does not detect the virus and does not block the file, allowing it to be downloaded.

The administrator confirms that the traffic matches the configured firewall policy.

What are two reasons for the failed virus detection by FortiGate? (Choose two.)

Options:

A- The selected SSL inspection profile has certificate inspection enabled.
B- The website is exempted from SSL inspection.
C- The El CAR test file exceeds the protocol options oversize limit.
D- The browser does not trust the FortiGate self-signed CA certificate.

Answer:

B, D

Question 8

Question Type: MultipleChoice

FortiGate is operating in NAT mode and has two physical interfaces connected to the LAN and DMZ networks respectively.

Which two statements about the requirements of connected physical interfaces on FortiGate are true? (Choose two.)

Options:

A- Both interfaces must have the interface role assigned.
B- Both interfaces must have directly connected routes on the routing table.
C- Both interfaces must have DHCP enabled and interfaces set to LAN and DMZ roles assigned.
D- Both interfaces must have IP addresses assigned.

Answer:

B, D

Explanation:

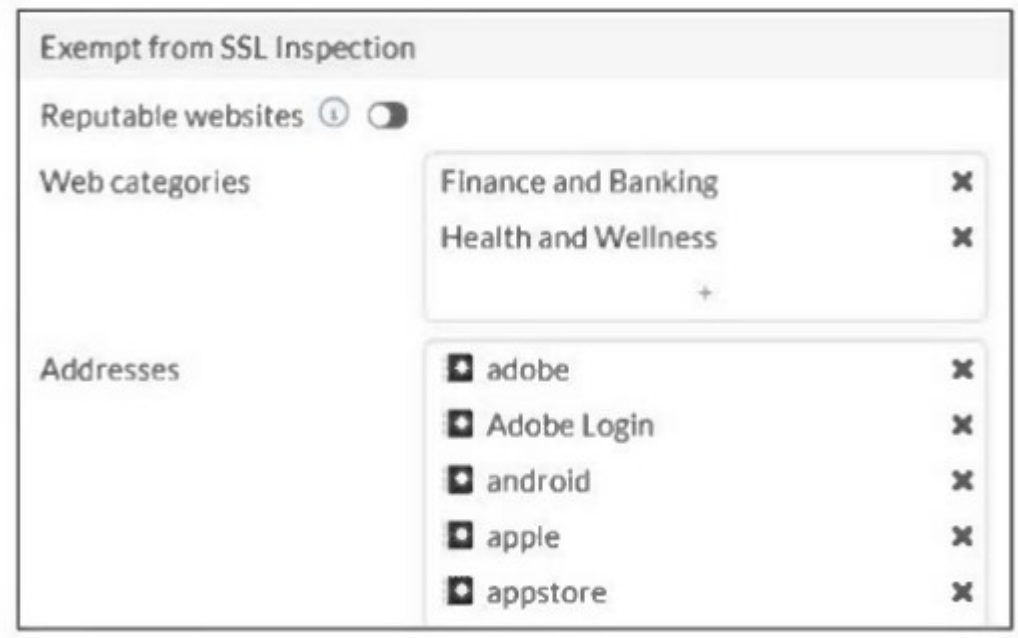
Interfaces must have directly connected routes in the routing table to forward traffic correctly.

Interfaces must have IP addresses assigned to communicate within their respective networks.

Question 9

Question Type: MultipleChoice

Refer to the exhibit.



The predefined deep-inspection and custom-deep-inspection profiles exclude some web categories from SSL inspection, as shown in the exhibit.

For which two reasons are these web categories exempted? (Choose two.)

Options:

A- The FortiGate temporary certificate denies the browser's access to websites that use HTTP Strict Transport Security.
B- These websites are in an allowlist of reputable domain names maintained by FortiGuard.
C- The resources utilization is optimized because these websites are in the trusted domain list on FortiGate.
D- The legal regulation aims to prioritize user privacy and protect sensitive information for these websites.

Answer:

A, D

Explanation:

FortiGate's temporary SSL certificate may cause access denial to sites using HTTP Strict Transport Security (HSTS), so such sites are exempted from deep SSL inspection.

Legal regulations require exemption of certain categories to protect user privacy and sensitive information, so these web categories are excluded from SSL inspection.

Thank You for trying FCP_FGT_AD-7.6 PDF Demo

To try our FCP_FGT_AD-7.6 practice exam software visit link below

https://prepbolt.com/FCP_FGT_AD-7.6.html

Start Your FCP_FGT_AD-7.6 Preparation

Use Coupon “SAVE50” for extra 50% discount on the purchase of Practice Test Software. Test your FCP_FGT_AD-7.6 preparation with actual exam questions.