

FCNSP.V5^{Q&As}

Fortinet Certified Network Security Professional (FCNSP.v5)

Pass Fortinet FCNSP.V5 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

<https://www.pass2lead.com/fcnsp-v5.html>

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Fortinet
Official Exam Center

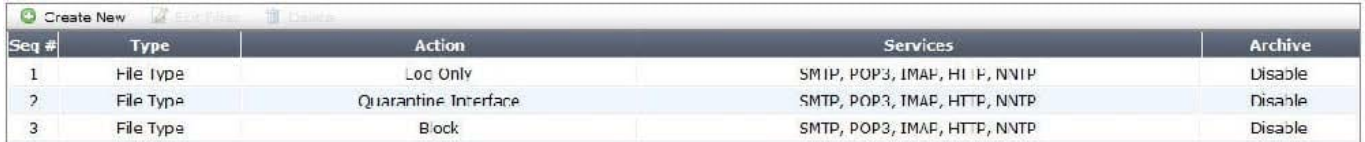
- ⚙️ **Instant Download** After Purchase
- ⚙️ **100% Money Back** Guarantee
- ⚙️ **365 Days** Free Update
- ⚙️ **800,000+** Satisfied Customers



QUESTION 1

Examine the Exhibits shown below, then answer the question that follows.

Review the following DLP Sensor (Exhibit 1):



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

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



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

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



Filter Type	Filter
File Name Pattern	*.exe

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



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

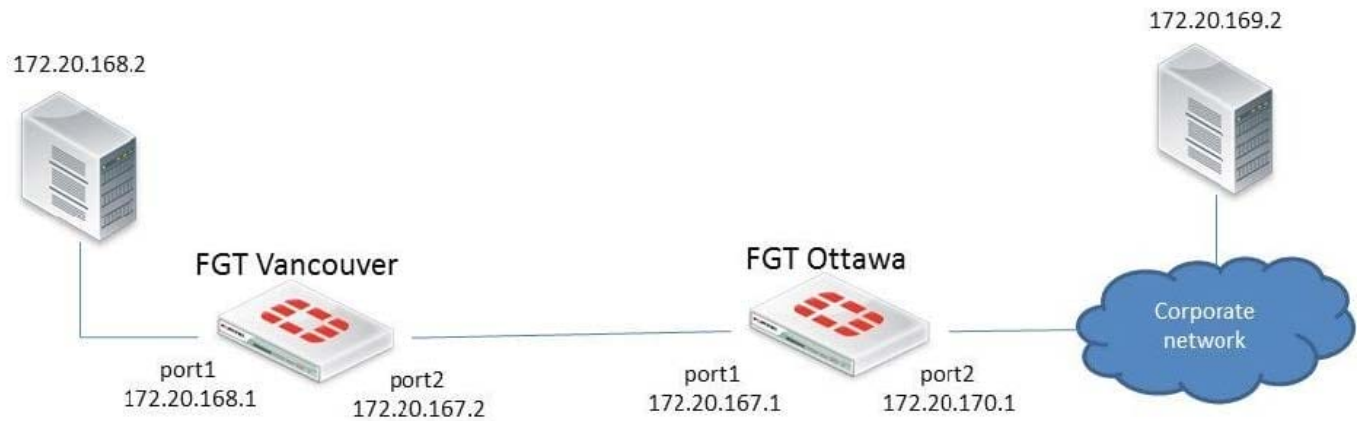
An MP3 file is renamed to `workbook.exe` and put into a ZIP archive. It is then sent through the FortiGate device over HTTP. It is intercepted and processed by the configuration shown in the above Exhibits 1-4. Assuming the file is not too large for the File scanning threshold, what action will the FortiGate unit take?

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

Correct Answer: A

QUESTION 2

Examine the Exhibit shown 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 unit 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 unit'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

QUESTION 3

An administrator configures a VPN and selects the Enable IPsec Interface Mode option in the phase 1 settings.

Which of the following statements are correct regarding the IPsec VPN configuration?

- A. To complete the VPN configuration, the administrator must manually create a virtual IPsec interface in Web Config under System > Network.
- B. The virtual IPsec interface is automatically created after the phase1 configuration.
- C. The IPsec policies must be placed at the top of the list.
- D. This VPN cannot be used as part of a hub and spoke topology.
- E. Routes were automatically created based on the address objects in the firewall policies.

Correct Answer: B

QUESTION 4

An issue could potentially occur when clicking Connect to start tunnel mode SSL VPN. The tunnel will start up for a few seconds, then shut down.

Which of the following statements best describes how to resolve this issue?

- A. This user does not have permission to enable tunnel mode. Make sure that the tunnel mode widget has been added to that user's web portal.
- B. This FortiGate unit may have multiple Internet connections. To avoid this problem, use the appropriate CLI command to bind the SSL VPN connection to the original incoming interface.
- C. Check the SSL adaptor on the host machine. If necessary, uninstall and reinstall the adaptor from the tunnel mode portal.
- D. Make sure that only Internet Explorer is used. All other browsers are unsupported.

Correct Answer: B

QUESTION 5

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

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

Correct Answer: A