FCNSP.V5 Q&As

Fortinet Certified Network Security Professional (FCNSP.v5)

QUESTION 1

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 2

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

A. The FortiGate unit receives periodic "Here I am" messages from the web cache.

B. The FortiGate unit polls all globally-defined web cache servers at a regular intervals.

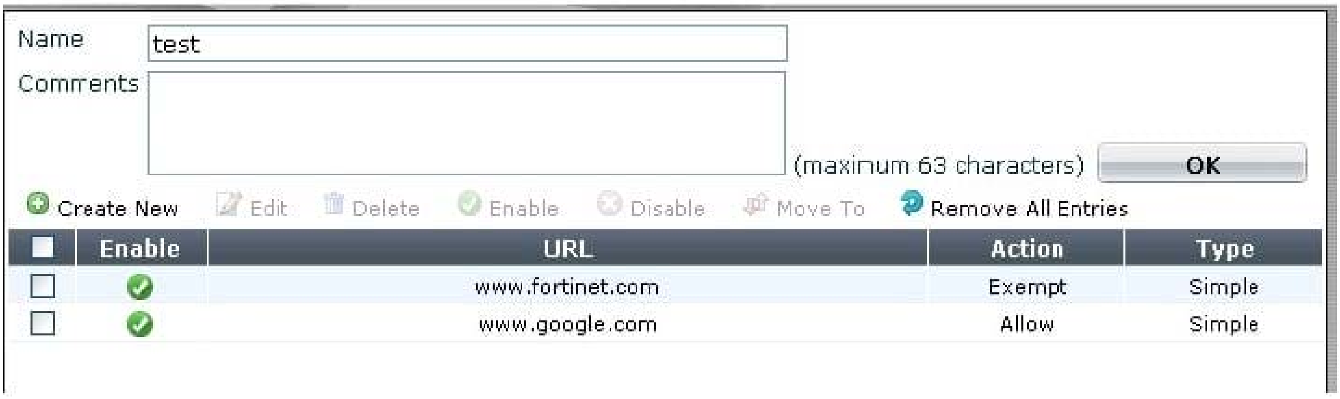
C. The FortiGate using uses the health check monitor to verify the availability of a web cache server.

D. The web cache sends an "I see you" message which is captured by the FortiGate unit.

Correct Answer: C

QUESTION 3

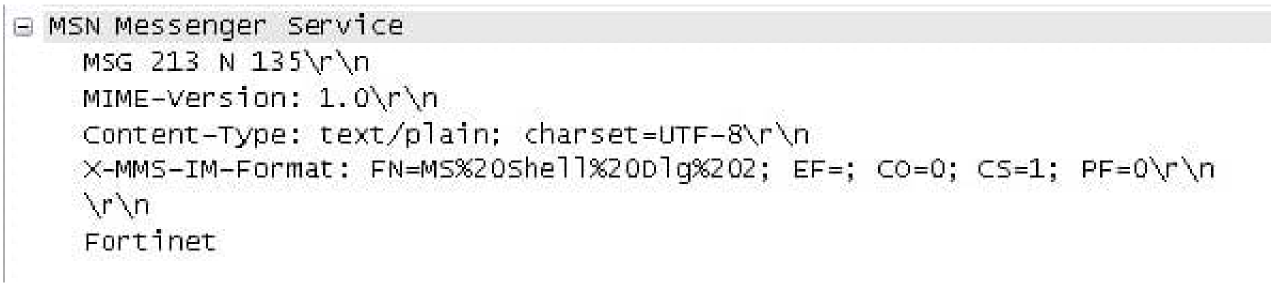
Which of the following describes the best custom signature for detecting the use of the word "Fortinet" in chat applications?



Name: test

Comments:

☐	Enable	URL	Action	Type
☐	✓	www.fortinet.com	Exempt	Simple
☐	✓	www.google.com	Allow	Simple



```
⊟ MSN Messenger Service
    MSG 213 N 135\r\n
    MIME-Version: 1.0\r\n
    Content-Type: text/plain; charset=UTF-8\r\n
    X-MMS-IM-Format: FN=MS%20Shell%20Dlg%202; EF=; CO=0; CS=1; PF=0\r\n
    \r\n
    Fortinet
```

A. The sample packet trace illustrated in the exhibit provides details on the packet that requires detection. F-SBID(--protocol tcp; --flow from_client; --pattern "X-MMS-IM-Format"; --pattern "fortinet"; -no_case;)

B. F-SBID(--protocol tcp; --flow from_client; --pattern "fortinet"; --no_case;)

C. F-SBID(--protocol tcp; --flow from_client; --pattern "X-MMS-IM-Format"; --pattern "fortinet"; --within 20; --no_case;)

D. F-SBID(--protocol tcp; --flow from_client; --pattern "X-MMS-IM-Format"; --pattern "fortinet"; --within 20;)

Correct Answer: A

QUESTION 4

Which of the following features could be used by an administrator to block FTP uploads while still allowing FTP downloads?

A. Anti-Virus File-Type Blocking

B. Data Leak Prevention

C. Network Admission Control

D. FortiClient Check

Correct Answer: B

QUESTION 5

Which of the following items is NOT a packet characteristic matched by a firewall service object?

A. ICMP type and code

B. TCP/UDP source and destination ports

C. IP protocol number

D. TCP sequence number

Correct Answer: D

QUESTION 6

The following ban list entry is displayed through the CLI.

get user ban list id cause src-ip-addr dst-ip-addr expires created 531 protect_client 10.177.0.21 207.1.17.1 indefinite Wed Dec 24 :21:33 2008 Based on this command output, which of the following statements is correct?

A. The administrator has specified the Attack and Victim Address method for the quarantine.

B. This diagnostic entry results from the administrator running the diag ips log test command. This command has no effect on traffic.

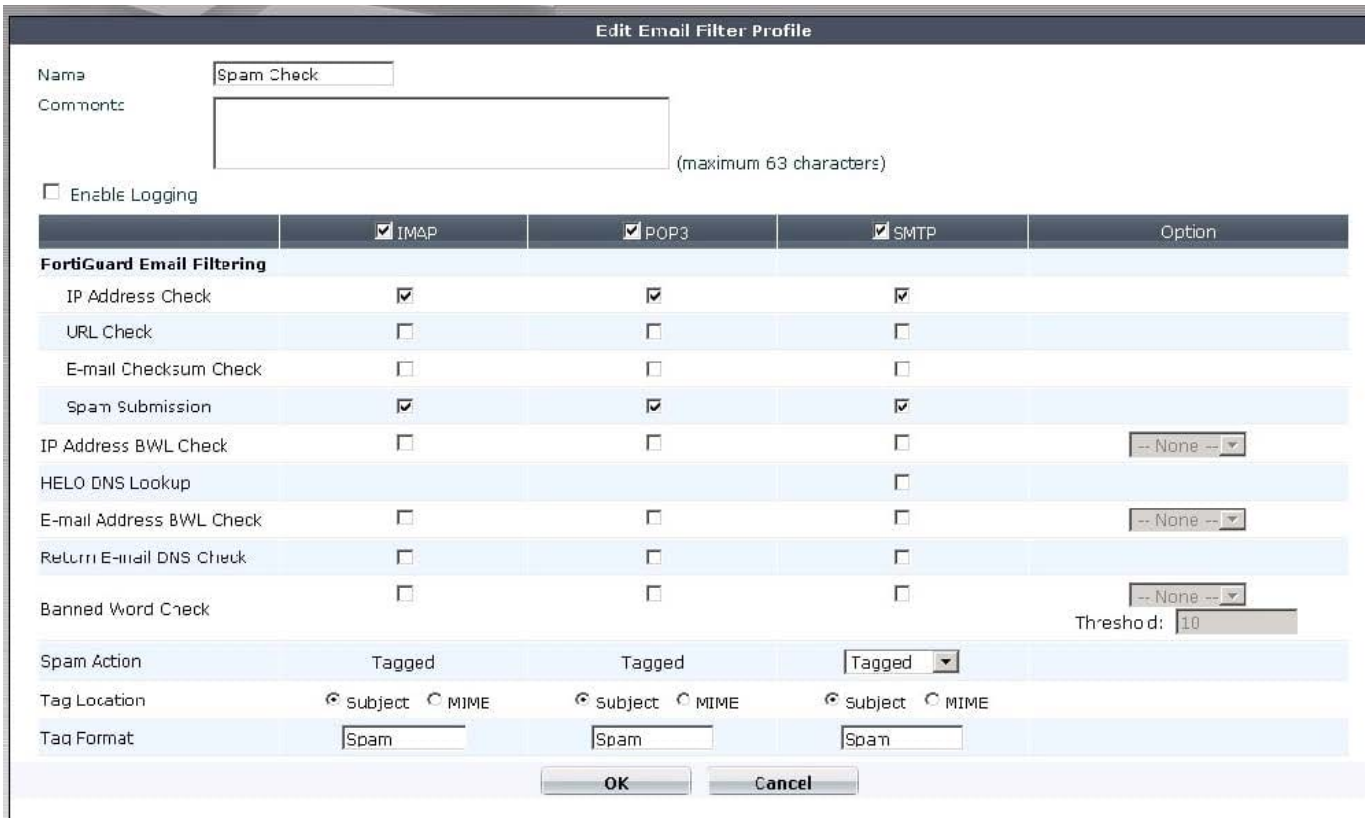
C. A DLP rule has been matched.

D. An attack has been repeated more than once during the holddown period; the expiry time has been reset to indefinite.

Correct Answer: A

QUESTION 7

A firewall policy has been configured for the internal email server to receive email from external parties through SMTP. Exhibits A and B show the AntiVirus and Email Filter profiles applied to this policy.



Edit Email Filter Profile

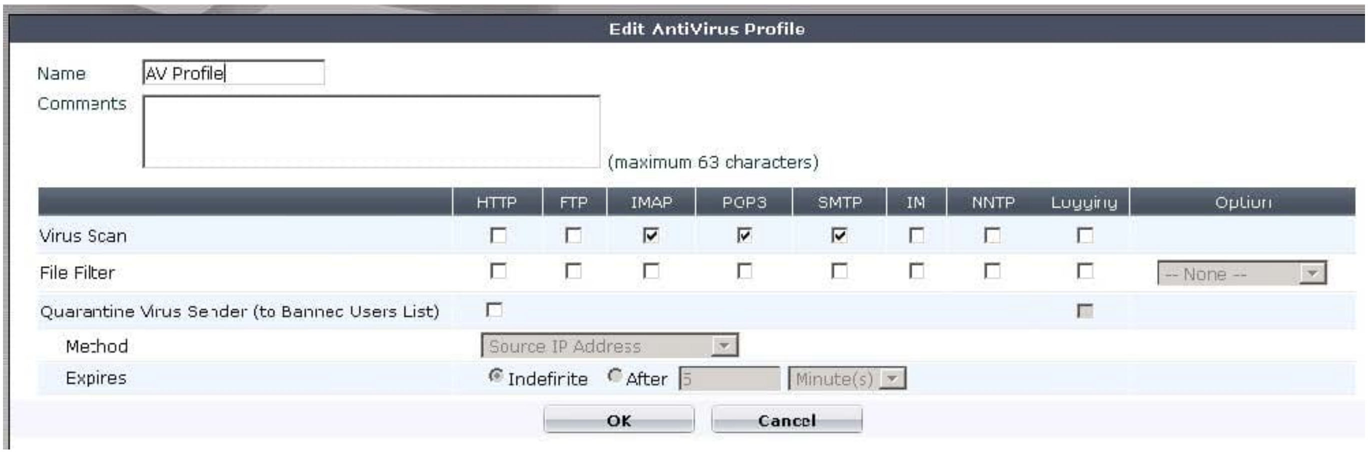
Name: Spam Check

Comments: (maximum 63 characters)

□ Enable Logging

	☑ IMAP	☑ POP3	☑ SMTP	Option
FortiGuard Email Filtering				
IP Address Check	☑	☑	☑	
URL Check	□	□	□	
E-mail Checksum Check	□	□	□	
Spam Submission	☑	☑	☑	
IP Address BWL Check	□	□	□	-- None --
HELO DNS Lookup			□	
E-mail Address BWL Check	□	□	□	-- None --
Return E-mail DNS Check	□	□	□	
Banned Word Check	□	□	□	-- None -- Threshold: 10
Spam Action	Tagged	Tagged	Tagged	
Tag Location	● Subject ○ MIME	● Subject ○ MIME	● Subject ○ MIME	
Tag Format	Spam	Spam	Spam	

OK | Cancel



Edit AntiVirus Profile

Name: AV Profile

Comments: (maximum 63 characters)

	HTTP	FTP	IMAP	POP3	SMTP	IM	NNTP	Logging	Option
Virus Scan	□	□	☑	☑	☑	□	□	□	
File Filter	□	□	□	□	□	□	□	□	-- None --
Quarantine Virus Sender (to Banned Users List)	□							□	
Method	Source IP Address								
Expires	● Indefinite ○ After 5 Minute(s)								

OK | Cancel

What is the correct behavior when the email attachment is detected as a virus by the FortiGate AntiVirus engine?

A. The FortiGate unit will remove the infected file and deliver the email with a replacement message to alert the recipient that the original attachment was infected.

B. The FortiGate unit will reject the infected email and notify both the sender and recipient.

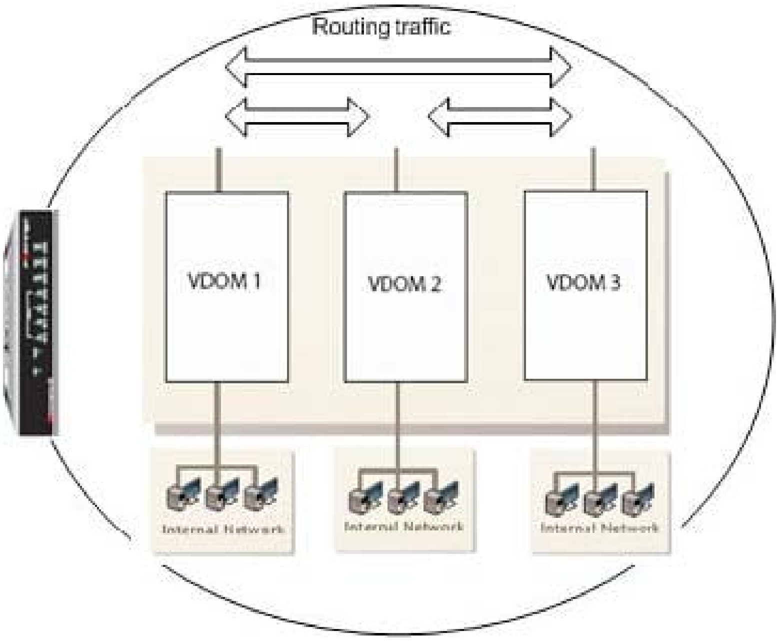
C. The FortiGate unit will remove the infected file and add a replacement message. Both sender and recipient are notified that the infected file has been removed.

D. The FortiGate unit will reject the infected email and notify the sender.

Correct Answer: A

QUESTION 8

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? (Select all that apply.)

A. The administrator should 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. This provides the same level of security internally as externally.

C. This configuration requires the use of an external router.

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 independant routing table, routing rules need to be set (for example, static routing, OSPF) in each VDOM to route traffic between VDOMs.

Correct Answer: ABE

QUESTION 9

In the case of TCP traffic, which of the following correctly describes the routing table lookups performed by a FortiGate unit when searching for a suitable gateway?

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

B. A look-up is done when the first packet coming from the client (SYN) arrives, and a second is performed when the first packet coming from the server (SYNC/ACK) arrives.

C. A look-up is done only during the TCP 3-way handshake (SYNC, SYNC/ACK, ACK).

D. A look-up is always done each time a packet arrives, from either the server or the client side.

Correct Answer: B

QUESTION 10

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

A. They both create separate broadcast domains.

B. Port Pairing works only for physical interfaces.

C. Forwarding Domains only apply to virtual interfaces.

D. They may contain physical and/or virtual interfaces.

E. They are only available in high-end models.

Correct Answer: AD

QUESTION 11

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

A. Exempt

B. Quarantine Interface

C. Block

D. None

Correct Answer: A

QUESTION 12

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

option.

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

A. The search items you are looking for are not contained in indexed log fields.

B. A quick search only searches data received within the last 24 hours.

C. You want the search to include the FortiAnalyzer\\'s local logs.

D. You want the search to include content archive data as well.

Correct Answer: A

QUESTION 13

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

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

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

C. Request: Internal Host -> Slave FG -> Internet -> Web Server

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

Correct Answer: A

QUESTION 14

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

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

A. The login event is sent to the Collector Agent.

B. The FortiGate unit receives the user information from the Domain Controller Agent of the Secondary Controller.

C. The Collector Agent performs the DNS lookup for the authenticated client\\'s IP address.

D. The user cannot be authenticated with the FortiGate device in this manner because each Domain Controller Agent requires a dedicated Collector Agent.

Correct Answer: AC

QUESTION 15

Which of the following represents the correct order of criteria used for the selection of a Master unit within a FortiGate High Availability (HA) cluster when master 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