

IT 认证电子书



质 量 更 高 服 务 更 好

半年免费升级服务

<http://www.itrenzheng.com>

Exam : **NSE4_FGT-7.0**

Title : **Fortinet NSE 4 - FortiOS 7.0**

Version : **DEMO**

1.Which two statements about FortiGate FSSO agentless polling mode are true? (Choose two.)

- A. FortiGate uses the AD server as the collector agent.
- B. FortiGate uses the SMB protocol to read the event viewer logs from the DCs.
- C. FortiGate does not support workstation check.
- D. FortiGate directs the collector agent to use a remote LDAP server.

Answer: B,D

Explanation:

Reference: <https://kb.fortinet.com/kb/documentLink.do?externalID=FD47732>

2.FortiGuard categories can be overridden and defined in different categories. To create a web rating override for example.com home page, the override must be configured using a specific syntax.

Which two syntaxes are correct to configure web rating override for the home page? (Choose two.)

- A. www.exaple.com
- B. www.example.com/index.html
- C. example.com
- D. www.example.com:443

Answer: A,C

Explanation:

When using FortiGuard category filtering to allow or block access to a website, one option is to make a web rating override and define the website in a different category. Web ratings are only for host names" "no URLs or wildcard characters are allowed".

3.Refer to the exhibits to view the firewall policy (Exhibit A) and the antivirus profile (Exhibit B).
Exhibit A.

Edit Policy


Name ⓘ	Internet Access		
Incoming Interface	 port2		▼
Outgoing Interface	 port1		▼
Source	 all		×
		+	
Destination	 all		×
		+	
Schedule	 always		▼
Service	 ALL		×
		+	
Action	<input checked="" type="checkbox"/> ACCEPT	<input type="checkbox"/> DENY	
Inspection Mode	<input checked="" type="checkbox"/> Flow-based	<input type="checkbox"/> Proxy-based	
Firewall/Network Options			
NAT	<input checked="" type="checkbox"/>		
IP Pool Configuration	<input checked="" type="checkbox"/> Use Outgoing Interface Address	<input type="checkbox"/> Use Dymanic IP Pool	
Preserve Source Port	<input type="checkbox"/>		
Protocol Options	<input checked="" type="checkbox"/> PROT default		▼ ✎
Security Profiles			
AntiVirus	<input checked="" type="checkbox"/> AV default		▼ ✎
Web Filter	<input type="checkbox"/>		
DNS Filter	<input type="checkbox"/>		
Application Control	<input type="checkbox"/>		
IPS	<input type="checkbox"/>		
File Filter	<input type="checkbox"/>		
SSL Inspection ⚠	<input checked="" type="checkbox"/> SSL deep-inspection		▼ ✎
Decrypted Traffic Mirror	<input type="checkbox"/>		

Exhibit B.

Edit AntiVirus Profile

Name

Comments 29/255

Detect Viruses Block Monitor

Feature set Flow-based Proxy-based

Inspected Protocols

HTTP

SMTP

POP3

IMAP

FTP

CIFS

APT Protection Options

Treat Windows Executables in Email Attachments as Viruses

Include Mobile Malware Protection

Quarantine

Virus Outbreak Prevention

Use FortiGuard Outbreak Prevention Database

Use External Malware Block List

Use EMS threat feed

Which statement is correct if a user is unable to receive a block replacement message when downloading an infected file for the first time?

- A. The flow-based Inspection is used, which resets the last packet to the user.
- B. The volume of traffic being inspected is too high for this model of FortiGate.
- C. The firewall policy performs the full content inspection on the file.
- D. The intrusion prevention security profile needs to be enabled when using flow-based inspection mode.

Answer: A

4.Which three options are the remote log storage options you can configure on FortiGate? (Choose three.)

- A. FortiSandbox
- B. FortiCloud
- C. FortiSIEM
- D. FortiCache
- E. ForiAnalyzer

Answer: B,C,E

Explanation:

Reference:

<https://docs.fortinet.com/document/fortigate/6.0.0/handbook/265052/logging-and-reportingoverview>

5.Which statement correctly describes NetAPI polling mode for the FSSO collector agent?

- A. NetAPI polling can increase bandwidth usage in large networks.
- B. The NetSessionEnum function is used to track user logouts.
- C. The collector agent must search security event logs.
- D. The collector agent uses a Windows API to query DCs for user logins.

Answer: B

Explanation:

Reference:

https://kb.fortinet.com/kb/microsites/search.do?cmd=displayKC&docType=kc&externalId=FD34906&sliceId=1&docTypeID=DT_KCARTICLE_1_1&dialogID=210966035&statId=1%20%20210968009%27