Fortinet

NSE4_FGT-7.0 Exam

Fortinet NSE 4 - FortiOS 7.0

Questions & Answers
Demo

ExamsLand provides 100% free Fortinet NSE4_FGT-7.0 practice questions and answers in pdf. Instant access.
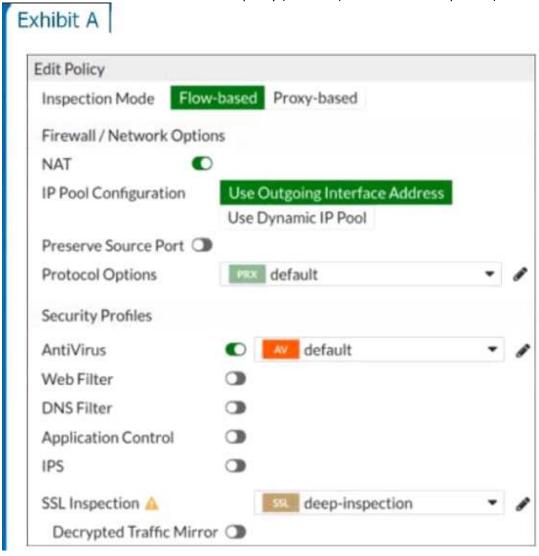
Page 2

Version: 4.0

Topic 1, Main Questions

Question: 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: BD

Explanation:

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

Question: 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 for the home page? (Choose two.)

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

Answer: BC

Explanation:

FortiGate_Security_6.4 page 384

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".

ExamsLand provides 100% free Fortinet NSE4_FGT-7.0 practice questions and answers in pdf. Instant access.

Page 3

Question: 3

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

Exhibit A

Edit Policy

Inspection Mode   **Flow-based**   Proxy-based

Firewall / Network Options

NAT   ⬤

IP Pool Configuration   **Use Outgoing Interface Address**

                      Use Dynamic IP Pool

Preserve Source Port ⬤

Protocol Options   PRX default   ▾   ✎

Security Profiles

AntiVirus   ⬤   AV default   ▾   ✎

Web Filter   ◯

DNS Filter   ◯

Application Control   ◯

IPS   ◯

SSL Inspection ⚠   SSL deep-inspection   ▾   ✎

   Decrypted Traffic Mirror ⬤

ExamsLand provides 100% free Fortinet NSE4_FGT-7.0 practice questions and answers in pdf. Instant access.

Page 4

Exhibit B

Edit AntiVirus Profile

Name	default
Comments	Scan files and block viruses. 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 ◉

Virus Outbreak Prevention ⓘ

Use FortiGuard Outbreak Prevention Database ◯

Use External Malware Block List ⓘ ⚠ ◯

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

Answer: B

Explanation:

ExamsLand provides 100% free Fortinet NSE4_FGT-7.0 practice questions and answers in pdf. Instant access.

Page 5

• "ONLY" If the virus is detected at the "START" of the connection, the IPS engine sends the block replacement message immediately
• When a virus is detected on a TCP session (FIRST TIME), but where "SOME PACKETS" have been already forwarded to the receiver, FortiGate "resets the connection" and does not send the last piece of the file. Although the receiver got most of the file content, the file has been truncated and therefore, can't be opened. The IPS engine also caches the URL of the infected file, so that if a "SECOND ATTEMPT" to transmit the file is made, the IPS engine will then send a block replacement message to the client instead of scanning the file again.

In flow mode, the FortiGate drops the last packet killing the file. But because of that the block replacement message cannot be displayed. If the file is attempted to download again the block message will be shown.

Question: 4

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

A. FortiCache
B. FortiSIEM
C. FortiAnalyzer
D. FortiSandbox
E. FortiCloud

Answer: BCE

Explanation:

Reference: https://docs.fortinet.com/document/fortigate/6.0.0/handbook/265052/logging-and-reporting-overview

Question: 5

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

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

Answer: D

Explanation:

Reference: https://kb.fortinet.com/kb/documentLink.do?externalID=FD34906

https://kb.fortinet.com/kb/microsites/search.do?cmd=displayKC&docType=kc&externalId=FD34906&slic

eId=1&docTypeID=DT_KCARTICLE_1_1&dialogID=210966035&stateId=1%200%20210968009%27)

Thank You For Trying NSE4_FGT-7.0 PDF Demo

To try our NSE4_FGT-7.0 Premium Files visit link below:

https://examsland.com/latest-exam-questions/NSE4_FGT-7.0/

Start Your NSE4_FGT-7.0 Preparation

Use Coupon EL25 for extra 25% discount on the purchase of Practice Test Software.