

Exam Questions NSE4_FGT-7.2

Fortinet NSE 4 - FortiOS 7.2

https://www.2passeasy.com/dumps/NSE4_FGT-7.2/



NEW QUESTION 1

Which two protocols are used to enable administrator access of a FortiGate device? (Choose two.)

- A. FTM
- B. SSH
- C. HTTPS
- D. FortiTelemetry

Answer: BC

NEW QUESTION 2

Refer to the exhibit.

```
# diagnose test application ipsmonitor

1: Display IPS engine information
2: Toggle IPS engine enable/disable status
3: Display restart log
4: Clear restart log
5: Toggle bypass status
6: Submit attack characteristics now
10: IPS queue length
11: Clear IPS queue length
12: IPS L7 socket statistics
13: IPS session list
14: IPS NTurbo statistics
15: IPSA statistics
...
97: Start all IPS engines
98: Stop all IPS engines
99: Restart all IPS engines and monitor
```

Examine the intrusion prevention system (IPS) diagnostic command shown in the exhibit.

If option 5 is used with the IPS diagnostic command and the outcome is a decrease in the CPU usage, what is the correct conclusion?

- A. The IPS engine is unable to prevent an intrusion attack.
- B. The IPS engine is inspecting a high volume of traffic.
- C. The IPS engine will continue to run in a normal state.
- D. The IPS engine is blocking all traffic.

Answer: B

NEW QUESTION 3

Which three methods are used by the collector agent for AD polling? (Choose three.)

- A. FortiGate polling
- B. NetAPI
- C. Novell API
- D. WMI
- E. WinSecLog

Answer: BDE

NEW QUESTION 4

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.)

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

Answer: AD

NEW QUESTION 5

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

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

E. Flow-based inspection optimizes performance compared to proxy-based inspection.

Answer: ADE

NEW QUESTION 6

Which two inspection modes can you use to configure a firewall policy on a profile-based next-generation firewall (NGFW)? (Choose two.)

- A. Proxy-based inspection
- B. Certificate inspection
- C. Flow-based inspection
- D. Full Content inspection

Answer: AC

NEW QUESTION 7

Refer to the exhibits.

The exhibits show the firewall policies and the objects used in the firewall policies.

The administrator is using the Policy Lookup feature and has entered the search criteria shown in the exhibit.

Exhibit A

Exhibit B

Address Object

Name	Details
IP Range/Subnet	
LOCAL_CLIENT	10.0.1.10/32
all	0.0.0.0
FQDN	
facebook.com	facebook.com

Internet Service Object

Name	Direction	Number of Entries
Predefined Internet Services		
Facebook-Web	Destination	26,578
IP	Port	Protocol
1.9.91.17 - 1.9.91.18	80	TCP
	443	
	8443	
1.9.91.17 - 1.9.91.18	443	UDP
1.9.91.30	443	UDP

Firewall Policies

ID	From	To	Source	Destination	Schedule	Service	Action	NAT
3	port3	port1	LOCAL_CLIENT	facebook.com	always	ULL_UDP	✓ ACCEPT	✓ Enabled
1	port1	port3	facebook.com	LOCAL_CLIENT	always	ULL_UDP	✓ ACCEPT	✓ Enabled
4	port4	port1	LOCAL_CLIENT	all	always	HTTP DNS HTTPS	✓ ACCEPT	✓ Enabled
5	port3	port1	LOCAL_CLIENT	Facebook-Web	always	Internet Service	✓ ACCEPT	✓ Enabled
2	port3	port1	all	all	always	ALL	✓ ACCEPT	✓ Enabled

Exhibit A
Exhibit B

Policy Lookup

Incoming Interface	port3
IP Version	IPv4
Protocol	TCP
Source	10.0.1.10
Source Port	Optional (1-65535)
Destination	facebook.com
Destination Port	443

Search
Close

Which policy will be highlighted, based on the input criteria?

- A. Policy with ID 4.
- B. Policy with ID 5.
- C. Policies with ID 2 and 3.
- D. Policy with ID 4.

Answer: A

NEW QUESTION 8

Refer to the exhibit.

```

FGT1 # get router info routing-table database
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       > - selected route, * - FIB route, p - stale info

S      *> 0.0.0.0/0 [10/0] via 172.20.121.2, port1, [20/0]
S      *>          [10/0] via 10.0.0.2, port2, [30/0]
S      0.0.0.0/0 [20/0] via 192.168.15.2, port3, [10/0]
C      *> 10.0.0.0/24 is directly connected, port2
S      172.13.24.0/24 [10.0] is directly connected, port4
C      *> 172.20.121.0/24 is directly connected, port1
S      *> 192.167.1.0/24 [10/0] via 10.0.0.2, port2
C      *> 192.168.15.0/24 is directly connected, port3
    
```

Given the routing database shown in the exhibit, which two statements are correct? (Choose two.)

- A. The port3 default route has the highest distance.
- B. The port3 default route has the lowest metric.
- C. There will be eight routes active in the routing table.
- D. The port1 and port2 default routes are active in the routing table.

Answer: AD

NEW QUESTION 9

Which of the following statements is true regarding SSL VPN settings for an SSL VPN portal?

- A. By default, FortiGate uses WINS servers to resolve names.
- B. By default, the SSL VPN portal requires the installation of a client's certificate.
- C. By default, split tunneling is enabled.
- D. By default, the admin GUI and SSL VPN portal use the same HTTPS port.

Answer: D

NEW QUESTION 10

Examine this PAC file configuration.

Which of the following statements are true? (Choose two.)

- A. Browsers can be configured to retrieve this PAC file from the FortiGate.

- B. Any web request to the 172.25. 120.0/24 subnet is allowed to bypass the proxy.
- C. All requests not made to Fortinet.com or the 172.25. 120.0/24 subnet, have to go through altproxy.corp.com: 8060.
- D. Any web request fortinet.com is allowed to bypass the proxy.

Answer: AD

NEW QUESTION 10

Which two statements are correct regarding FortiGate HA cluster virtual IP addresses? (Choose two.)

- A. Heartbeat interfaces have virtual IP addresses that are manually assigned.
- B. A change in the virtual IP address happens when a FortiGate device joins or leaves the cluster.
- C. Virtual IP addresses are used to distinguish between cluster members.
- D. The primary device in the cluster is always assigned IP address 169.254.0.1.

Answer: BD

NEW QUESTION 12

Refer to the exhibit, which contains a session diagnostic output.

```
session info: proto=17 proto_state=01 duration=254 expire=179 timeout=0 flags=00000000 socktype=0 sockport=0 av_idx=0 use=3
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ helper=dns-udp vlan_cos=0/255
state=log may_dirty f00 log-start
statistic(bytes/packets/allow_err): org=1420/22/1 reply=5678/22/1 tuples=2
tx speed(Bps/kbps): 5/0 rx speed(Bps/kbps): 22/0
origin->sink: org pre->post, reply pre->post dev=5->3/3->5 gwy=10.200.1.254/10.0.1.200
hook=post dir=org act=snat 10.0.1.200:2486->208.91.112.53:53(10.200.1.1:62902)
hook=pre dir=reply act=dnat 208.91.112.53:53->10.200.1.1:62902(10.0.1.200:2486)
misc=0 policy_id=3 auth_info=0 chk_client_info=0 vd=0
serial=0001fc1e tos=ff/ff app_list=0 app=0 url_cat=0
rpdb_link_id= 00000000 rpdb_svc_id=0 ngfwid=n/a
npu_state=0x040000
```

Which statement is true about the session diagnostic output?

- A. The session is a UDP unidirectional state.
- B. The session is in TCP ESTABLISHED state.
- C. The session is a bidirectional UDP connection.
- D. The session is a bidirectional TCP connection.

Answer: C

Explanation:

<https://kb.fortinet.com/kb/viewContent.do?externalId=FD30042>

NEW QUESTION 15

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

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 ☐

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:

· "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.

NEW QUESTION 16

An administrator is configuring an Ipsec between site A and siteB. The Remotes Gateway setting in both sites has been configured as Static IP Address. For site A, the local quick mode selector is 192.168. 1.0/24 and the remote quick mode selector is 192.168.2.0/24. Which subnet must the administrator configure for the local quick mode selector for site B?

- A. 192.168.3.0/24
- B. 192.168.2.0/24
- C. 192.168. 1.0/24
- D. 192.168.0.0/8

Answer: C

NEW QUESTION 18

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

NEW QUESTION 22

An administrator needs to increase network bandwidth and provide redundancy.
What interface type must the administrator select to bind multiple FortiGate interfaces?

- A. VLAN interface
- B. Software Switch interface
- C. Aggregate interface
- D. Redundant interface

Answer: C

NEW QUESTION 24

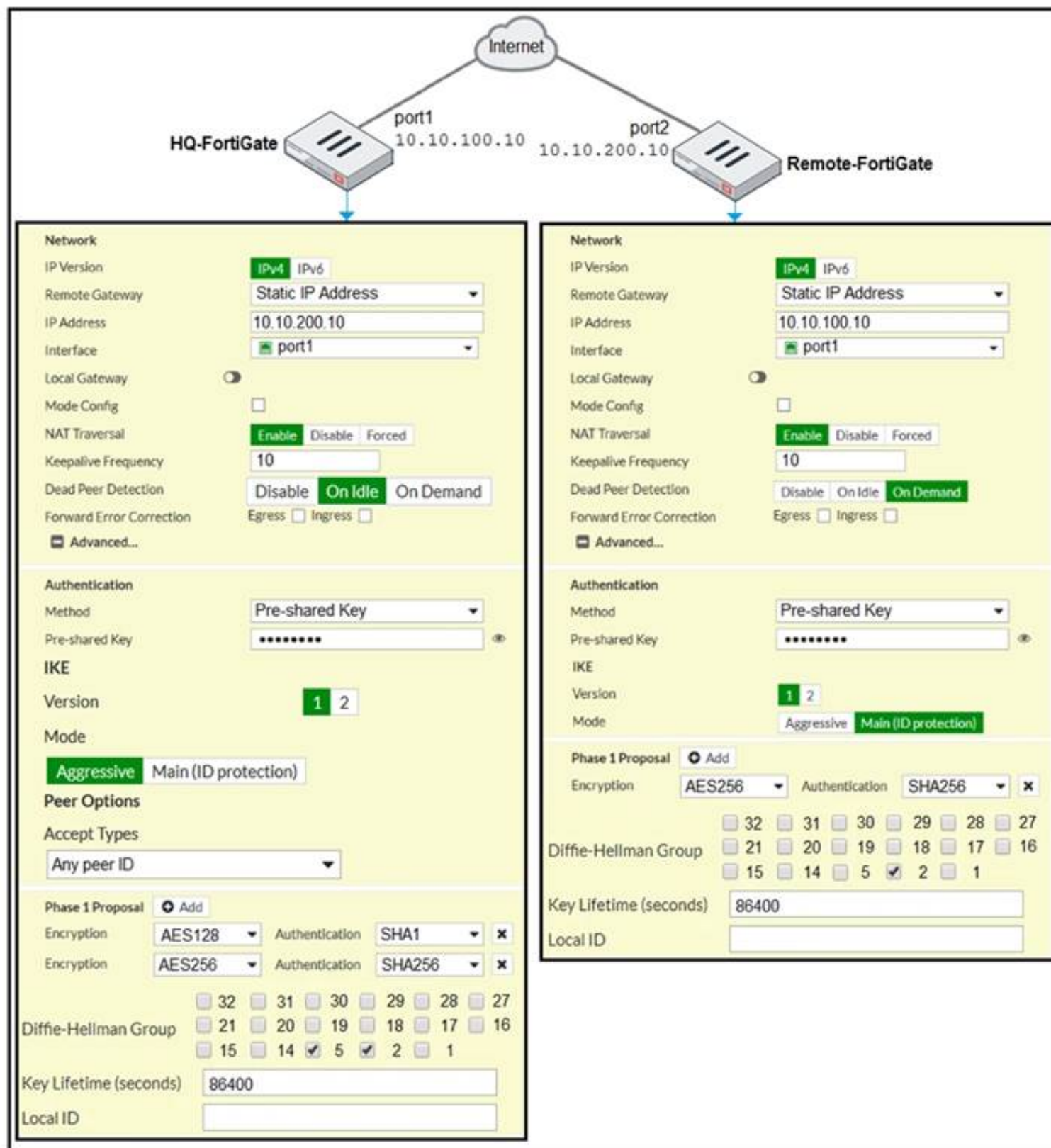
Which CLI command will display sessions both from client to the proxy and from the proxy to the servers?

- A. diagnose wad session list
- B. diagnose wad session list | grep hook-pre&&hook-out
- C. diagnose wad session list | grep hook=pre&&hook=out
- D. diagnose wad session list | grep "hook=pre"&"hook=out"

Answer: A

NEW QUESTION 25

A network administrator is troubleshooting an IPsec tunnel between two FortiGate devices. The administrator has determined that phase 1 fails to come up. The administrator has also re-entered the pre-shared key on both FortiGate devices to make sure they match.



Based on the phase 1 configuration and the diagram shown in the exhibit, which two configuration changes will bring phase 1 up? (Choose two.)

- A. On HQ-FortiGate, set IKE mode to Main (ID protection).
- B. On both FortiGate devices, set Dead Peer Detection to On Demand.
- C. On HQ-FortiGate, disable Diffie-Helman group 2.
- D. On Remote-FortiGate, set port2 as Interface.

Answer: AD

NEW QUESTION 29

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual NSE4_FGT-7.2 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the NSE4_FGT-7.2 Product From:

https://www.2passeasy.com/dumps/NSE4_FGT-7.2/

Money Back Guarantee

NSE4_FGT-7.2 Practice Exam Features:

- * NSE4_FGT-7.2 Questions and Answers Updated Frequently
- * NSE4_FGT-7.2 Practice Questions Verified by Expert Senior Certified Staff
- * NSE4_FGT-7.2 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * NSE4_FGT-7.2 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year