



NSE4_FGT-7.0^{Q&As}

Fortinet NSE 4 - FortiOS 7.0

Pass Fortinet NSE4_FGT-7.0 Exam with 100% Guarantee

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

https://www.pass4itsure.com/nse4_fgt-7-0.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

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
rpd_b_link_id= 00000000 rpd_b_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.

Correct Answer: C

QUESTION 2

What is the limitation of using a URL list and application control on the same firewall policy, in NGFW policy-based mode?

- A. It limits the scope of application control to the browser-based technology category only.
- B. It limits the scope of application control to scan application traffic based on application category only.
- C. It limits the scope of application control to scan application traffic using parent signatures only
- D. It limits the scope of application control to scan application traffic on DNS protocol only.

Correct Answer: B

QUESTION 3

Which two statements about antivirus scanning mode are true? (Choose two.)



- A. In proxy-based inspection mode, files bigger than the buffer size are scanned.
- B. In flow-based inspection mode, FortiGate buffers the file, but also simultaneously transmits it to the client.
- C. In proxy-based inspection mode, antivirus scanning buffers the whole file for scanning, before sending it to the client.
- D. In flow-based inspection mode, files bigger than the buffer size are scanned.

Correct Answer: BC

An antivirus profile in full scan mode buffers up to your specified file size limit. The default is 10 MB. That is large enough for most files, except video files. If your FortiGate model has more RAM, you may be able to increase this threshold. Without a limit, very large files could exhaust the scan memory. So, this threshold balances risk and performance. Is this tradeoff unique to FortiGate, or to a specific model? No. Regardless of vendor or model, you must make a choice. This is because of the difference between scans in theory, that have no limits, and scans on real-world devices, that have finite RAM. In order to detect 100% of malware regardless of file size, a firewall would need infinitely large RAM--something that no device has in the real world. Most viruses are very small. This table shows a typical tradeoff. You can see that with the default 10 MB threshold, only 0.01% of viruses pass through.

QUESTION 4

To complete the final step of a Security Fabric configuration, an administrator must authorize all the devices on which device?

- A. FortiManager
- B. Root FortiGate
- C. FortiAnalyzer
- D. Downstream FortiGate

Correct Answer: B

QUESTION 5

View the exhibit.



Application Details

Name	Category	Technology	Popularity	Risk
Addicting Games	Game	Browser-Based	☆☆☆☆☆	Risk

Application Control Profile

Categories

- All Categories
- Business (149, 6)
- Email (80, 13)
- Industrial (1168)
- P2P (70)
- Social.Media (120, 31)
- Video/Audio (164, 14)
- Unknown Applications
- Cloud.IT (42)
- Game (83)
- Mobile (3)
- Proxy (148)
- Storage.Backup (175, 17)
- VoIP (27)
- Collaboration (274, 10)
- General.Interest (233, 6)
- Network.Service (325)
- Remote.Access (84)
- Update (49)
- Web.Client (22)

Application Overrides

+ Add Signatures | Edit Parameters | Delete

Application Signature	Category	Action
Addicting Games	Game	Allow

Filter Overrides

+ Add Filter | Edit | Delete

Filter Details	Action
Risk (2304, 52)	Block

A user behind the FortiGate is trying to go to <http://www.addictinggames.com> (Addicting Games). Based on this configuration, which statement is true?

- A. Addicting.Games is allowed based on the Application Overrides configuration.
- B. Addicting.Games is blocked on the Filter Overrides configuration.
- C. Addicting.Games can be allowed only if the Filter Overrides actions is set to Exempt.
- D. Addcting.Games is allowed based on the Categories configuration.

Correct Answer: A

QUESTION 6

A FortiGate is operating in NAT mode and configured with two virtual LAN (VLAN) sub interfaces added to the physical interface.

Which statements about the VLAN sub interfaces can have the same VLAN ID, only if they have IP addresses in different subnets.

- A. The two VLAN sub interfaces can have the same VLAN ID, only if they have IP addresses in different subnets.
- B. The two VLAN sub interfaces must have different VLAN IDs.
- C. The two VLAN sub interfaces can have the same VLAN ID, only if they belong to different VDOMs.
- D. The two VLAN sub interfaces can have the same VLAN ID, only if they have IP addresses in the same subnet.

Correct Answer: B

FortiGate_Infrastructure_6.0_Study_Guide_v2-Online.pdf ?gt; page 147 "Multiple VLANs can coexist in the same



physical interface, provide they have different VLAN ID"

QUESTION 7

View the exhibit.

Destination ⓘ	Subnet Named Address Internet Service
	172.13.24.0/255.255.255.0
Interface	TunnelB
Administrative Distance ⓘ	5
Comments	<input type="text"/>
Status	<input checked="" type="checkbox"/> Enabled <input type="checkbox"/> Disabled
Advanced Options	
Priority ⓘ	30

Destination ⓘ	Subnet Named Address Internet Service
	172.13.24.0/255.255.255.0
Interface	TunnelA
Administrative Distance ⓘ	10
Comments	<input type="text"/>
Status	<input checked="" type="checkbox"/> Enabled <input type="checkbox"/> Disabled
Advanced Options	
Priority ⓘ	0

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

- A. This setup requires at least two firewall policies with the action set to IPsec.
- B. Dead peer detection must be disabled to support this type of IPsec setup.
- C. The TunnelB route is the primary route for reaching the remote site. The TunnelA route is used only if the TunnelB VPN is down.
- D. This is a redundant IPsec setup.

Correct Answer: CD

QUESTION 8

Refer to the exhibit.



The diagram shows two FortiGate devices connected to the Internet. HQ-FortiGate is on the left with port1 (10.10.100.10) and Remote-FortiGate is on the right with port2 (10.10.200.10). Below the diagram are two screenshots of the FortiGate configuration interface for an IPsec tunnel.

Left Screenshot (HQ-FortiGate Configuration):

- Network:** IP Version: IPv4; Remote Gateway: Static IP Address; IP Address: 10.10.200.10; Interface: port1; Local Gateway: Disabled; Mode Config: Disabled; NAT Traversal: Enabled; Keepalive Frequency: 10; Dead Peer Detection: On Idle; Forward Error Correction: Disabled.
- Authentication:** Method: Pre-shared Key; Pre-shared Key: [Redacted]
- IKE:** Version: 1; Mode: Aggressive; Main (ID protection) selected.
- Peer Options:** Accept Types: Any peer ID.
- Phase 1 Proposal:** Add; Encryption: AES128, Authentication: SHA1; Encryption: AES256, Authentication: SHA256.
- Diffie-Hellman Group:** 5, 2 selected.
- Key Lifetime (seconds):** 86400.
- Local ID:** [Empty]

Right Screenshot (Remote-FortiGate Configuration):

- Network:** IP Version: IPv4; Remote Gateway: Static IP Address; IP Address: 10.10.100.10; Interface: port1; Local Gateway: Disabled; Mode Config: Disabled; NAT Traversal: Enabled; Keepalive Frequency: 10; Dead Peer Detection: On Demand; Forward Error Correction: Disabled.
- Authentication:** Method: Pre-shared Key; Pre-shared Key: [Redacted]
- IKE:** Version: 1; Mode: Aggressive; Main (ID protection) selected.
- Phase 1 Proposal:** Add; Encryption: AES256, Authentication: SHA256.
- Diffie-Hellman Group:** 2, 5 selected.
- Key Lifetime (seconds):** 86400.
- Local ID:** [Empty]



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 preshared 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.

Correct Answer: AD

QUESTION 9

Which statement about the policy ID number of a firewall policy is true?

- A. It is required to modify a firewall policy using the CLI.
- B. It represents the number of objects used in the firewall policy.
- C. It changes when firewall policies are reordered.
- D. It defines the order in which rules are processed.

Correct Answer: A

QUESTION 10

An administrator has configured a route-based IPsec VPN between two FortiGate devices. Which statement about this IPsec VPN configuration is true?

- A. A phase 2 configuration is not required.
- B. This VPN cannot be used as part of a hub-and-spoke topology.
- C. A virtual IPsec interface is automatically created after the phase 1 configuration is completed.
- D. The IPsec firewall policies must be placed at the top of the list.

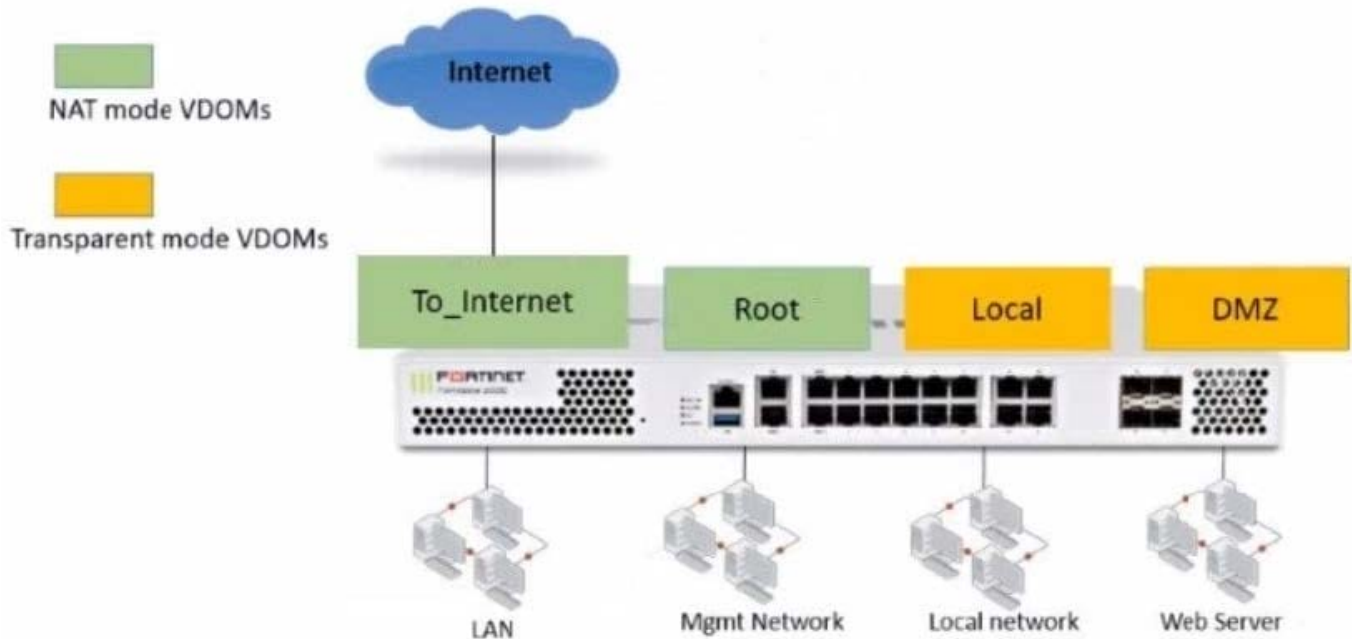
Correct Answer: C

In a route-based configuration, FortiGate automatically adds a virtual interface with the VPN name (Infrastructure Study Guide, 206)

QUESTION 11



Refer to the exhibit.



The Root and To_Internet VDOMs are configured in NAT mode. The DMZ and Local VDOMs are configured in transparent mode.

The Root VDOM is the management VDOM. The To_Internet VDOM allows LAN users to access the internet. The To_Internet VDOM is the only VDOM with internet access and is directly connected to ISP modem.

With this configuration, which statement is true?

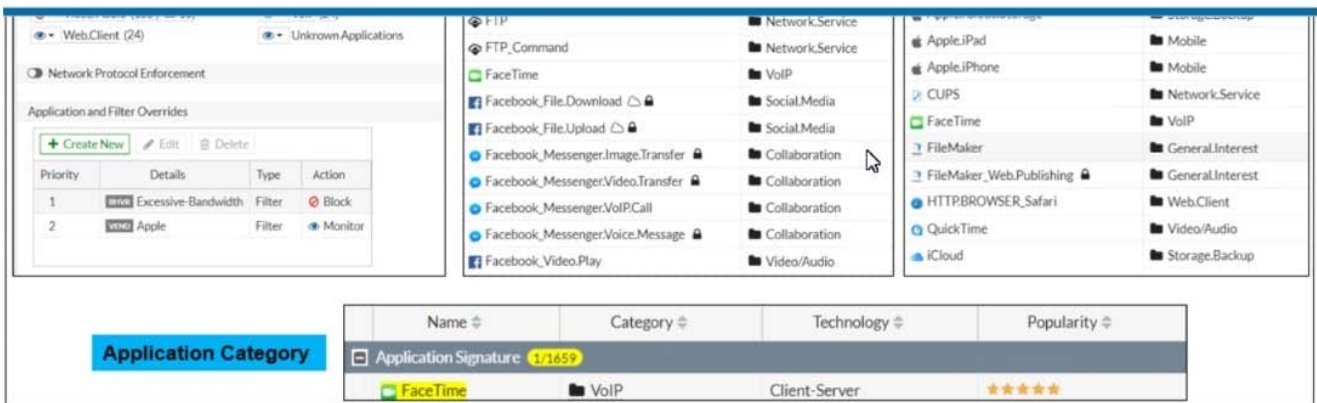
- A. Inter-VDOM links are required to allow traffic between the Local and Root VDOMs.
- B. A static route is required on the To_Internet VDOM to allow LAN users to access the internet.
- C. Inter-VDOM links are required to allow traffic between the Local and DMZ VDOMs.
- D. Inter-VDOM links are not required between the Root and To_Internet VDOMs because the Root VDOM is used only as a management VDOM.

Correct Answer: A

Reference: <https://kb.fortinet.com/kb/documentLink.do?externalID=FD46542>

QUESTION 12

Refer to the exhibit to view the application control profile.



Based on the configuration, what will happen to Apple FaceTime?

- A. Apple FaceTime will be blocked, based on the Excessive-Bandwidth filter configuration
- B. Apple FaceTime will be allowed, based on the Apple filter configuration.
- C. Apple FaceTime will be allowed only if the filter in Application and Filter Overrides is set to Learn
- D. Apple FaceTime will be allowed, based on the Categories configuration.

Correct Answer: A

QUESTION 13

An administrator is running the following sniffer command:

```
diagnose sniffer packet any "host 192.168.2.12" 5
```

Which three pieces of Information will be Included in me sniffer output? {Choose three.}

- A. Interface name
- B. Packet payload
- C. Ethernet header
- D. IP header
- E. Application header

Correct Answer: ABD

QUESTION 14

Examine the IPS sensor configuration shown in the exhibit, and then answer the question below.



IPS Sensor

Name: [View IPS Signatures]

Comments: 0 / 255

IPS Signatures

+ Add Signatures Delete Edit IP Exemptions

Name	Exempt IPs	Severity	Target	Service	OS	Action	Packet Logging
No matching entries found							

IPS Filters

+ Add Filter Edit Filter Delete

Filter Details	Action	Packet Logging
Location:server OS:Windows	<input checked="" type="radio"/> Block	<input checked="" type="radio"/>

Apply

Forward Traffic Logs

Refresh Download Add Filter

#	Date/Time	Source	Destination	Application Name	Result	Policy
1	10:09:03	10.200.1.254	10.200.1.200	<input type="checkbox"/> HTTPS	✓ 1.30kB/2.65 kB	2(Web-Server-Access-IPS)
2	10:09:03	10.200.1.254	10.200.1.200	<input type="checkbox"/> HTTPS	✓ 1.30kB/2.65 kB	2(Web-Server-Access-IPS)
3	10:09:02	10.200.1.254	10.200.1.200	<input type="checkbox"/> HTTPS	✓ 1.30kB/2.65 kB	2(Web-Server-Access-IPS)
4	10:09:02	10.200.1.254	10.200.1.200	<input type="checkbox"/> HTTPS	✓ 1.30kB/2.65 kB	2(Web-Server-Access-IPS)
5	10:09:01	10.200.1.254	10.200.1.200	<input type="checkbox"/> HTTPS	✓ 1.30kB/2.65 kB	2(Web-Server-Access-IPS)
6	10:08:59	10.200.1.254	10.200.1.200	<input type="checkbox"/> HTTPS	✓ 1.30kB/2.65 kB	2(Web-Server-Access-IPS)
7	10:08:57	10.200.1.254	10.200.1.200	<input type="checkbox"/> HTTPS	✓ 1.30kB/2.65 kB	2(Web-Server-Access-IPS)
8	10:08:57	10.200.1.254	10.200.1.200	<input type="checkbox"/> HTTPS	✓ 1.30kB/2.65 kB	2(Web-Server-Access-IPS)
9	10:08:57	10.200.1.254	10.200.1.200	<input type="checkbox"/> HTTPS	✓ 1.30kB/2.65 kB	2(Web-Server-Access-IPS)
10	10:08:57	10.200.1.254	10.200.1.200	<input type="checkbox"/> HTTPS	✓ 1.30kB/2.65 kB	2(Web-Server-Access-IPS)

An administrator has configured the WINDOWS_SERVERS IPS sensor in an attempt to determine whether the influx of HTTPS traffic is an attack attempt or not. After applying the IPS sensor, FortiGate is still not generating any IPS logs for the HTTPS traffic.

What is a possible reason for this?

- A. The IPS filter is missing the Protocol: HTTPS option.
- B. The HTTPS signatures have not been added to the sensor.
- C. A DoS policy should be used, instead of an IPS sensor.
- D. A DoS policy should be used, instead of an IPS sensor.
- E. The firewall policy is not using a full SSL inspection profile.



Correct Answer: E

QUESTION 15

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.

Correct Answer: BD

[Latest NSE4_FGT-7.0 Dumps](#)

[NSE4_FGT-7.0 Practice Test](#)

[NSE4_FGT-7.0 Braindumps](#)