# 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.certbus.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**

Which two policies must be configured to allow traffic on a policy-based next-generation firewall (NGFW) FortiGate? (Choose two.)

A. Firewall policy

B. Policy rule

C. Security policy

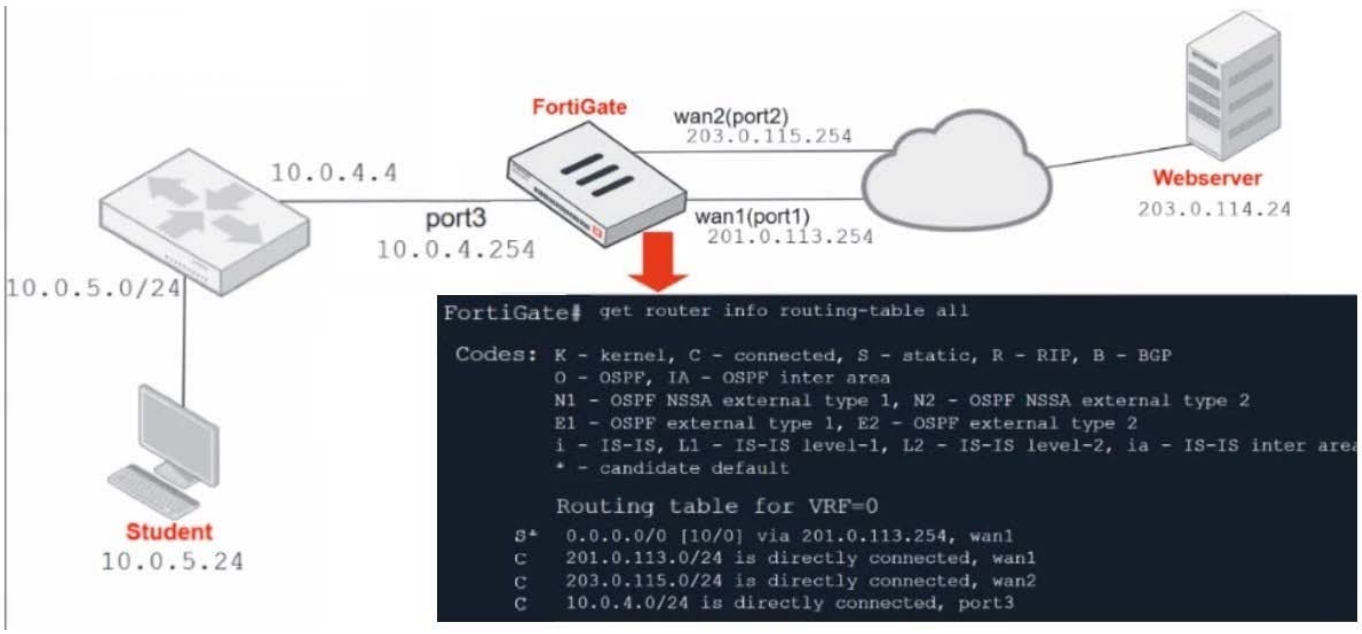
D. SSL inspection and authentication policy

Correct Answer: CD

Reference: https://docs.fortinet.com/document/fortigate/5.6.0/cookbook/38324/ngfw-policy-based-mode

**QUESTION 2**

Refer to the exhibit.




Which contains a network diagram and routing table output.

The Student is unable to access Webserver.

What is the cause of the problem and what is the solution for the problem?

A. The first packet sent from Student failed the RPF check. This issue can be resolved by adding a static route to 10.0.4.0/24 through wan1.

B. The first reply packet for Student failed the RPF check. This issue can be resolved by adding a static route to 10.0.4.0/24 through wan1.

C. The first reply packet for Student failed the RPF check. This issue can be resolved by adding a static route to 203.0.114.24/32 through port3.

D. The first packet sent from Student failed the RPF check. This issue can be resolved by adding a static route to 203.0.114.24/32 through port3.

Correct Answer: D

**QUESTION 3**

Exhibit:


Refer to the exhibit to view the authentication rule configuration In this scenario, which statement is true?

A. IP-based authentication is enabled

B. Route-based authentication is enabled

C. Session-based authentication is enabled.

D. Policy-based authentication is enabled

Correct Answer: C

Reference: https://kb.fortinet.com/kb/documentLink.do?externalID=FD45387

**QUESTION 4**

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 5**

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.

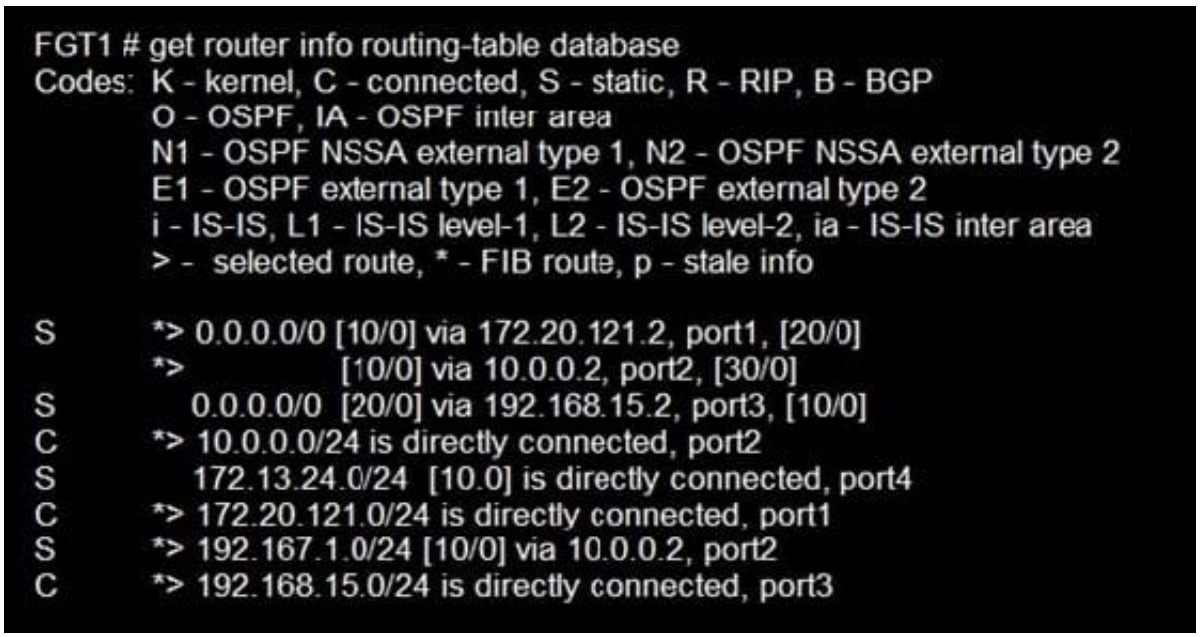
C. It limits the scope of application control to scan application traffic using parent signatures only

D. It limits the scope of application control to scan application traffic on DNS protocol only.

Correct Answer: B

**QUESTION 6**

Refer to the exhibit.



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.

Correct Answer: AD

**QUESTION 7**

Which three statements about security associations (SA) in IPsec are correct? (Choose three.)

A. Phase 2 SAs are used for encrypting and decrypting the data exchanged through the tunnel.

B. An SA never expires.

C. A phase 1 SA is bidirectional, while a phase 2 SA is directional.

D. Phase 2 SA expiration can be time-based, volume-based, or both.

E. Both the phase 1 SA and phase 2 SA are bidirectional.

Correct Answer: ACD

**QUESTION 8**

Examine this FortiGate configuration:

```
config authentication setting
     set active-auth-scheme SCHEME1
end
config authentication rule
     edit WebProxyRule
       set srcaddr 10.0.1.0/24
       set active-auth-method SCHEME2
     next
end
```

How does the FortiGate handle web proxy traffic coming from the IP address 10.2.1.200 that requires authorization?

A. It always authorizes the traffic without requiring authentication.

B. It drops the traffic.

C. It authenticates the traffic using the authentication scheme SCHEME2.

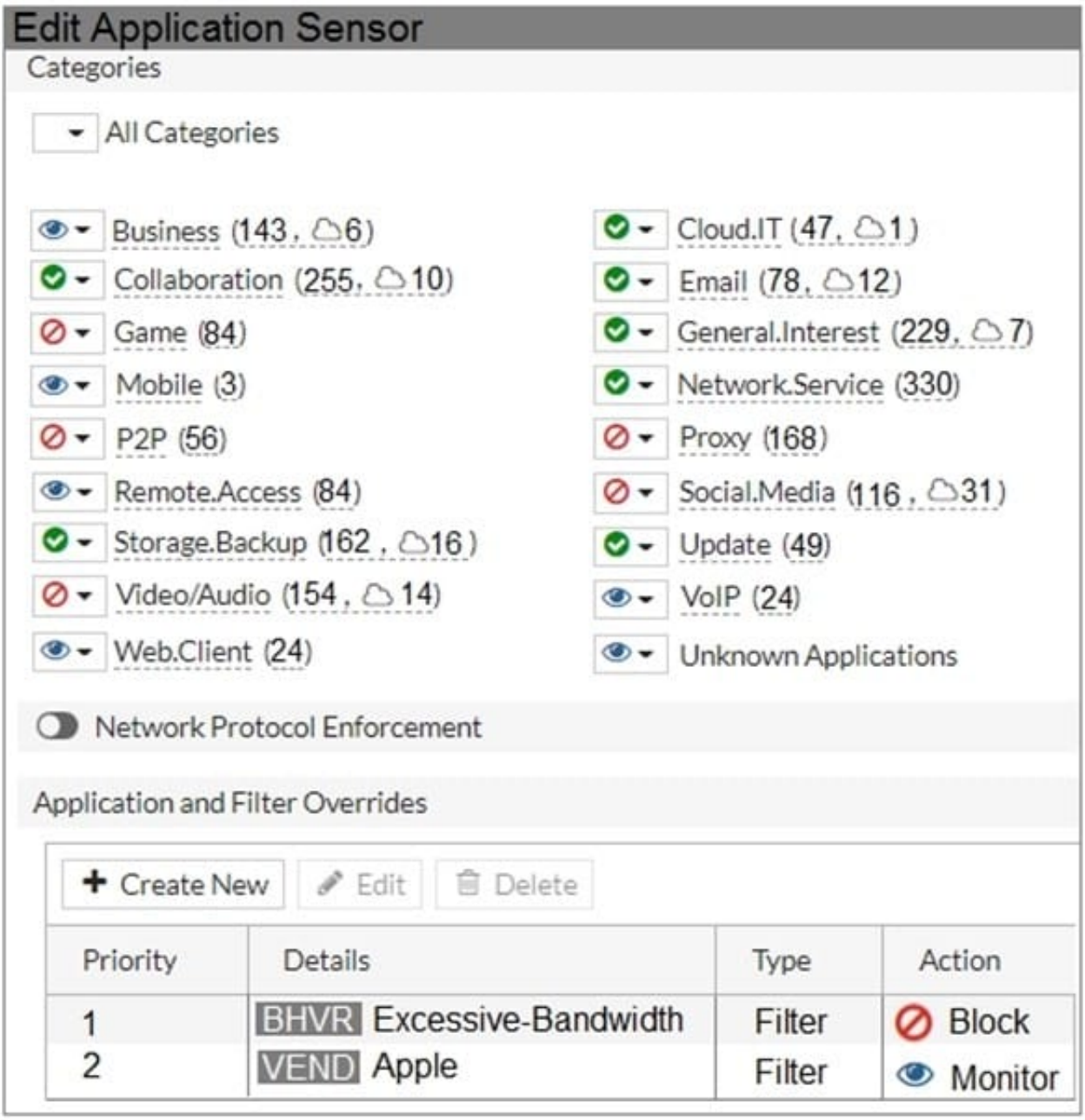
D. It authenticates the traffic using the authentication scheme SCHEME1.

Correct Answer: D

"What happens to traffic that requires authorization, but does not match any authentication rule? The active and passive SSO schemes to use for those cases is defined under config authentication setting"

**QUESTION 9**

Refer to the exhibit to view the application control profile.




Users who use Apple FaceTime video conferences are unable to set up meetings.

In this scenario, which statement is true?

A. Apple FaceTime belongs to the custom monitored filter.

B. The category of Apple FaceTime is being monitored.

C. Apple FaceTime belongs to the custom blocked filter.

D. The category of Apple FaceTime is being blocked.

Correct Answer: C

**QUESTION 10**

Examine this output from a debug flow:

```
id=20085 trace_id=1 func=print_pkt_detail line=5363 msg="vd-root received a packet(proto=1,
10.0.1.10:1->10.200.1.254:2048)
from port3. type=8, code=0, id=1, seq=33."
id=20085 trace_id=1 func=init_ip_session_common line=5519 msg="allocate a new session=00000340"
id=20085 trace_id=1 func=vf_ip_route_input_common line=2583 msg="find a route: flag=04000000 gw=10.200.1.254 via
port1"
id=20085 trace_id=1 func=fw_forward_handler line=586 msg="Denied by forward policy check (policy 0)"
```

Why did the FortiGate drop the packet?

A. The next-hop IP address is unreachable.

B. It failed the RPF check.

C. It matched an explicitly configured firewall policy with the action DENY.

D. It matched the default implicit firewall policy.

Correct Answer: D

https://kb.fortinet.com/kb/documentLink.do?externalID=13900

**QUESTION 11**

Which two statements about SSL VPN between two FortiGate devices are true? (Choose two.)

A. The client FortiGate requires a client certificate signed by the CA on the server FortiGate.

B. The client FortiGate requires a manually added route to remote subnets.

C. The client FortiGate uses the SSL VPN tunnel interface type to connect SSL VPN.

D. Server FortiGate requires a CA certificate to verify the client FortiGate certificate.

Correct Answer: CD

Reference: https://docs.fortinet.com/document/fortigate/6.2.9/cookbook/266506/ssl-vpn-with-certificateauthentication

**QUESTION 12**

Examine this FortiGate configuration:

```
config system global
     set av-failopen pass
end
```

Examine the output of the following debug command:

```
# diagnose hardware sysinfo conserve
memory conserve mode: on
total RAM: 3040 MB
memory used: 2948 MB 97% of total RAM
memory freeable: 92 MB 3% of total RAM
memory used + freeable threshold extreme: 2887 MB 95% of total RAM
memory used threshold red: 2675 MB 88% of total RAM
memory used threshold green: 2492 MB 82% of total RAM
```

Based on the diagnostic outputs above, how is the FortiGate handling the traffic for new sessions that require inspection?

A. It is allowed, but with no inspection

B. It is allowed and inspected as long as the inspection is flow based

C. It is dropped.

D. It is allowed and inspected, as long as the only inspection required is antivirus.

Correct Answer: C

**QUESTION 13**

If the Issuer and Subject values are the same in a digital certificate, which type of entity was the certificate issued to?

A. A CRL

B. A person

C. A subordinate CA

D. A root CA

Correct Answer: D

**QUESTION 14**

Which three authentication timeout types are availability for selection on FortiGate? (Choose three.)

A. hard-timeout

B. auth-on-demand

C. soft-timeout

D. new-session

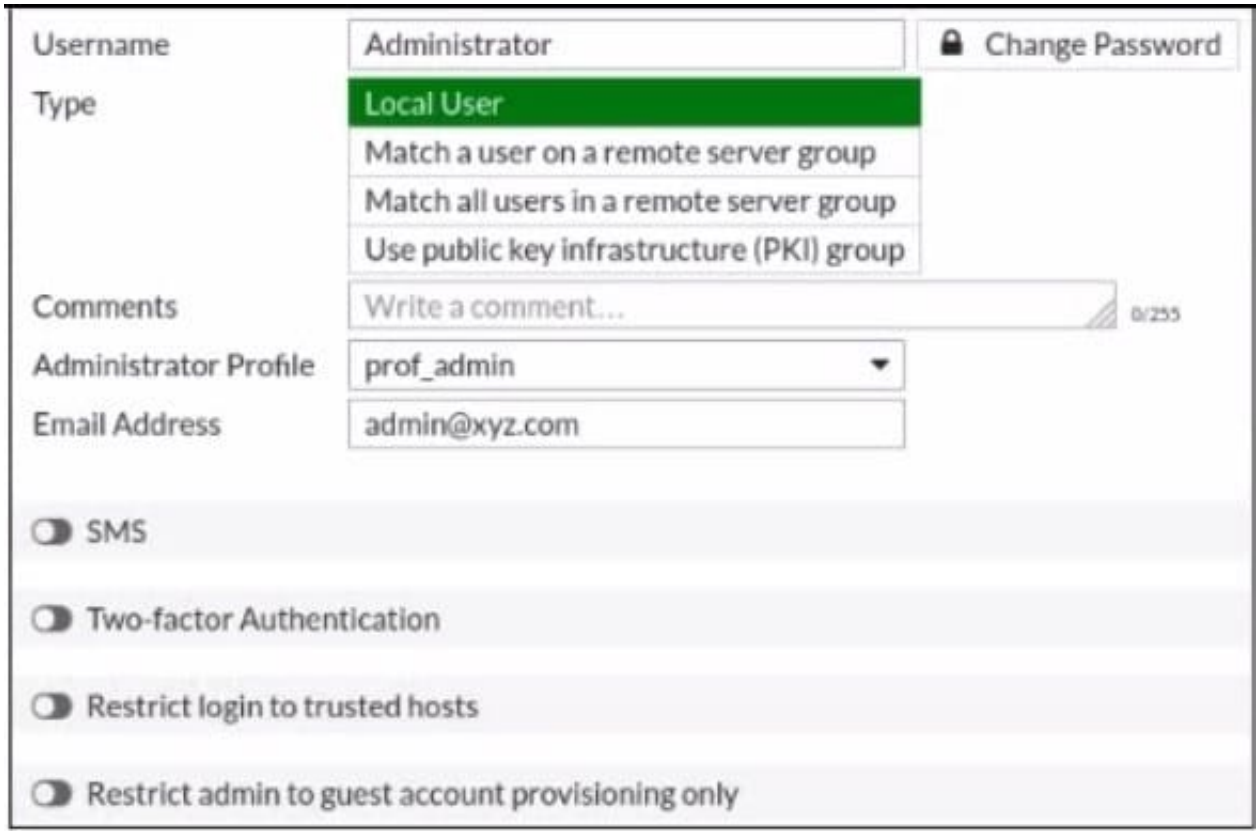
E. Idle-timeout

Correct Answer: ADE

https://kb.fortinet.com/kb/documentLink.do?externalID=FD37221

**QUESTION 15**

Refer to the exhibit.




The global settings on a FortiGate device must be changed to align with company security policies. What does the Administrator account need to access the FortiGate global settings?

A. Change password

B. Enable restrict access to trusted hosts

C. Change Administrator profile

D. Enable two-factor authentication

Correct Answer: C

Reference: https://kb.fortinet.com/kb/documentLink.do?externalID=FD34502