



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**

A network administrator has enabled SSL certificate inspection and antivirus on FortiGate. 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 the file can be downloaded.

What is the reason for the failed virus detection by FortiGate?

- A. Application control is not enabled
- B. SSL/SSH Inspection profile is incorrect
- C. Antivirus profile configuration is incorrect
- D. Antivirus definitions are not up to date

Correct Answer: B

https traffic requires SSL decryption. Check the ssh inspection profile

QUESTION 2

Refer to the exhibits.

Exhibit A

Edit Policy

| | |
|--------------------|-------------------------|
| Name | Facebook SSL Inspection |
| Incoming Interface | port2 |
| Outgoing Interface | port1 |
| Source | all |
| Destination | all |
| Service | ALL |

Firewall / Network Options

Central NAT is enabled so NAT settings from matching Central SNAT policies will be applied.

Security Profiles

SSL Inspection: certificate-inspection

**Exhibit B**

The screenshot shows the 'Edit Policy' configuration for a policy named 'Facebook Access'. The configuration is as follows:

| Field | Value |
|----------------------------|---|
| Name | Facebook Access |
| Incoming Interface | port2 |
| Outgoing Interface | port1 |
| Source | all |
| Destination | all |
| Schedule | always |
| Service | App Default |
| Application | Facebook, Facebook_Like.Button, Facebook_Video.Play |
| URL Category | + |
| Action | ACCEPT |
| Firewall / Network Options | |
| Protocol Options | PRX default |

The exhibits show the SSL and authentication policy (Exhibit A) and the security policy (Exhibit B) for Facebook.

Users are given access to the Facebook web application. They can play video content hosted on Facebook but they are unable to leave reactions on videos or other types of posts.

Which part of the policy configuration must you change to resolve the issue?

- A. The SSL inspection needs to be a deep content inspection.
- B. Force access to Facebook using the HTTP service.
- C. Additional application signatures are required to add to the security policy.
- D. Add Facebook in the URL category in the security policy.

Correct Answer: A

The lock logo behind Facebook_like.Button indicates that SSL Deep Inspection is Required.

QUESTION 3

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 4

Refer to the exhibit to view the application control profile.



Edit Application Sensor

Categories

| <input "="" button"="" checkbox"="" type="button" value="Unknown Applications</td></tr></tbody></table><p><input type="/> Network Protocol Enforcement <p>Application and Filter Overrides</p> <p><input type="button" value="+ Create New"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/></p> <table><thead><tr><th>Priority</th><th>Details</th><th>Type</th><th>Action</th></tr></thead><tbody><tr><td>1</td><td>BHVR Excessive-Bandwidth</td><td>Filter</td><td><input type="button" value="Block"/></td></tr><tr><td>2</td><td>VEND Apple</td><td>Filter</td><td><input type="button" value="Monitor"/></td></tr></tbody></table> | Priority | Details | Type | Action | 1 | BHVR Excessive-Bandwidth | Filter | <input type="button" value="Block"/> | 2 | VEND Apple | Filter | <input type="button" value="Monitor"/> |
|--|---------------------------------|---------|--|--------|---|---------------------------------|--------|--------------------------------------|---|-------------------|--------|--|
| Priority | Details | Type | Action | | | | | | | | | |
| 1 | BHVR Excessive-Bandwidth | Filter | <input type="button" value="Block"/> | | | | | | | | | |
| 2 | VEND Apple | Filter | <input type="button" value="Monitor"/> | | | | | | | | | |

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 5**

Refer to the exhibit.

```
config firewall policy
edit 1
set name "INTERNET"
set uuid b11ac58c-791b-51e7-4600-12f829a689d9
set srcintf "port3"
set dstintf "port1"
set srcaddr "LOCAL_SUBNET"
set dstaddr "all"
set action accept
set schedule "always"
set service "ALL"
set utm-status enable
set inspection-mode proxy
set http-policy-redirect enable
set ssl-ssh-profile "certificate-inspection"
set av-profile "default"
set logtraffic all
set logtraffic-start enable
set ippool enable
set poolname "ProxyPool"
set nat enable
next
end

config firewall proxy-address
edit "EICAR"
set uuid 5a24bdaa-c792-51ea-2c89-a9f79e2bdc96
set type host-regex
set host-regex ".*eicar\\.org"
next
end
```

FIREWALL POLICIES

```
config firewall
edit 1
set uuid 6491d126-c79b-51ea-1319-4ed94b543a8e
set proxy transparent-web
set srcintf "port3"
set dstintf "port1"
set srcaddr "all"
set dstaddr "EICAR"
set service "webproxy"
set action accept
set schedule "always"
set logtraffic all
set utm-status enable
set ssl-ssh-profile "certificate-inspection"
set av-profile "default"
next
edit 2
set uuid 6a1c74c6-c794-51ea-e646-4f70ae2bc5f9
set proxy transparent-web
set srcintf "port3"
set dstintf "port1"
set srcaddr "all"
set dstaddr "all"
set service "webproxy"
set action accept
set status disable
set schedule "always"
set logtraffic disable
set ssl-ssh-profile "certificate-inspection"
next
edit 3
set uuid 818fb8b6-c797-51ea-d848-a7c2952ceea9
set proxy transparent-web
set srcintf "port3"
set dstintf "port1"
set srcaddr "all"
set dstaddr "all"
set service "webproxy"
set action accept
set status disable
set schedule "always"
set logtraffic all
set utm-status enable
set ssl-ssh-profile "certificate-inspection"
set av-profile "default"
next
end
```

PROXY ADDRESS

The exhibit shows a CLI output of firewall policies, proxy policies, and proxy addresses. How does FortiGate process the traffic sent to <http://www.fortinet.com>?

- A. Traffic will be redirected to the transparent proxy and it will be allowed by proxy policy ID 3.
- B. Traffic will not be redirected to the transparent proxy and it will be allowed by firewall policy ID 1.
- C. Traffic will be redirected to the transparent proxy and It will be allowed by proxy policy ID 1.
- D. Traffic will be redirected to the transparent proxy and it will be denied by the proxy implicit deny policy.

Correct Answer: D

[NSE4_FGT-7.0 PDF Dumps](#)

[NSE4_FGT-7.0 Exam Questions](#)

[NSE4_FGT-7.0 Braindumps](#)