

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



https://www.pass4itsure.com/nse4_fgt-7-0.html 2024 Latest pass4itsure NSE4_FGT-7.0 PDF and VCE dumps Download

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

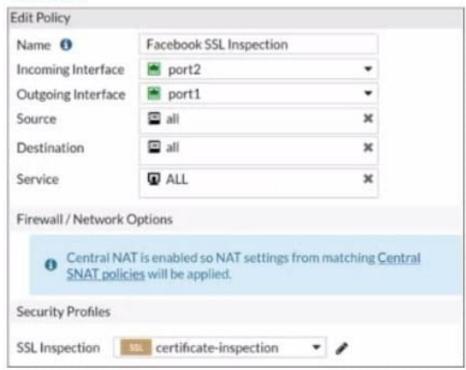
Correct Answer: B

https traffic requires SSL decryption. Check the ssh inspection profile

QUESTION 2

Refer to the exhibits.

Exhibit A



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

2024 Latest pass4itsure NSE4_FGT-7.0 PDF and VCE dumps Download

Exhibit B



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

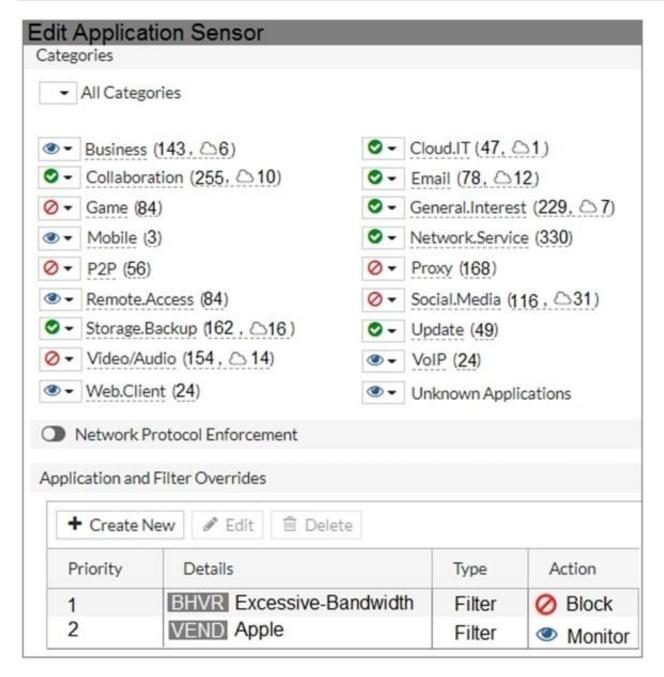
D. It is allowed and inspected, as long as the only inspection required is antivirus.

Correct Answer: C

QUESTION 4

Refer to the exhibit to view the application control profile.





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

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

2024 Latest pass4itsure NSE4_FGT-7.0 PDF and VCE dumps Download

QUESTION 5

Refer to the exhibit.

```
config firewall
edit 1
config firewall policy
                                                                  FIREWALL POLICIES
      edit 1
                                                                                                      set uuld 6491d126-c798-51ea-1319-4ad84b543a
                                                                                                      set proxy transparent-web
            set name "INTERNET"
                                                                                                      set srcintf "port3"
set dstintf "port1"
set srcaddr "all"
set dstaddr "EICAR"
set service "webproxy
            set uuid b11ac58c-791b-51e7-4600-12f829a689d9
            set srcintf "port3"
set dstintf "port1"
set srcaddr "LOCAL_SUBNET"
                                                                                                      set action accept
set schedule "always
set logtraffic all
            set dstaddr "all'
                                                                                                      set utm-status enable
set ssl-ssh-profile "
            set action accept
                                                                                                                             certificate-inspection'
            set schedule "always"
                                                                                                      set av-profile "default
            set service "ALL"
                                                                                                  edit 2
            set utm-status enable
                                                                                                      set uuld 6a1c74c6-c794-51ea-e646-4f70ae2bc5f9
                                                                                                      set proxy transparent-web
set srcintf "port2"
set dstintf "port1"
set srcaddr "all"
set dstaddr "all"
            set inspection-mode proxy
            set http-policy-redirect enable
            set ssl-ssh-profile "certificate-inspection"
            set av-profile "default"
                                                                                                       set service "webproxy
            set logtraffic all
                                                                                                      set action accept
                                                                                                      set status disable
            set logtraffic-start enable
                                                                                                      set schedule "always
            set ippool enable
                                                                                                      set logtraffic disable
            set poolname "ProxyPool"
                                                                                                      set ssl-ssh-profile "certificate-inspection"
            set nat enable
      next
                                                                                                      set uuid 818fb8b6-c797-51ea-d848-a7c2952ceea9
                                                                                                      set proxy transparent-web
set srcintf "port3"
set dstintf "port1"
set srcaddr "all"
set dstaddr "all"
end
config firewall proxy-address
                                                                       PROXY ADDRESS
      edit "EICAR
                                                                                                       set service "webproxy
                                                                                                      set action accept
set status disable
             set uuid 5a24bdaa-c792-51ea-2c89-a9f79e2bdc96
             set type host-regex
                                                                                                      set schedule "always
set logtraffic all
             set host-regex ".*eicar\\.org"
                                                                                                      set utm-status enable
      next
                                                                                                                             'certificate-inspection'
                                                                                                      set ssl-ssh-profile "cer
set av-profile "default"
end
                                                                                                  next
```

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