NSE4_FGT-7.2 Q&As

Fortinet NSE 4 - FortiOS 7.2

Pass Fortinet NSE4_FGT-7.2 Exam with 100% Guarantee

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

https://www.pass4itsure.com/nse4_fgt-7-2.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Fortinet Official Exam Center

QUESTION 1

Refer to the exhibit.

The exhibit shows the output of a diagnose command.

```
# diagnose firewall proute list
list route policy info(vf=root):
id=2130903041(0x7f030001) vwl_service=1(Critical-DIA) vwl_mbr_seq=1 2 dscp_tag=0xff 0xff
flags=0x0 tos=0x00 tos_mask=0x00 protocol=0 sport=0-65535 iif=0 dport=1-65535 path(2)
oif=3(port1) oif=4(port2)
source(1): 10.0.1.0-10.0.1.255
destination wildcard(1): 0.0.0.0/0.0.0.0
internet service(3): GoToMeeting(4294836966,0,0,0, 16354)
Microsoft.Office.365.Portal(4294837474,0,0,0, 41468) Salesforce(4294837976,0,0,0, 16920)
hit_count=0 last_used=2022-02-23 05:46:43
```

What does the output reveal about the policy route?

A. It is an ISDB route in policy route.

B. It is a regular policy route.

C. It is an ISDB policy route with an SDWAN rule.

D. It is an SDWAN rule in policy route.

Correct Answer: D

FortiGate Infrastructure 7.2 Study Guide (p.59): "ISDB routes and SD-WAN rules are assigned an ID higher than 65535. However, SD-WAN rule entries include the vwl_service field, and ISDB route entries don\\'t."

QUESTION 2

Which CLI command allows administrators to troubleshoot Layer 2 issues, such as an IP address conflict?

A. get system status

B. get system performance status

C. diagnose sys top

D. get system arp

Correct Answer: D

"If you suspect that there is an IP address conflict, or that an IP has been assigned to the wrong device, you may need

to look at the ARP table."

QUESTION 3

Which two statements are true about the FGCP protocol? (Choose two.)

A. FGCP elects the primary FortiGate device.

B. FGCP is not used when FortiGate is in transparent mode.

C. FGCP runs only over the heartbeat links.

D. FGCP is used to discover FortiGate devices in different HA groups.

Correct Answer: AC

The FGCP (FortiGate Clustering Protocol) is a protocol that is used to manage high availability (HA) clusters of FortiGate devices. It performs several functions, including the following:

FGCP elects the primary FortiGate device: In an HA cluster, FGCP is used to determine which FortiGate device will be the primary device, responsible for handling traffic and making decisions about what to allow or block. FGCP uses a

variety of factors, such as the device\\'s priority, to determine which device should be the primary.

FGCP runs only over the heartbeat links: FGCP communicates between FortiGate devices in the HA cluster using the heartbeat links. These are dedicated links that are used to exchange status and control information between the devices.

FGCP does not run over other types of links, such as data links.

Reference:

https://docs.fortinet.com/document/fortigate/6.4.0/ports-and-protocols/564712/fgcp-fortigate-clustering-protocol

FortiGate Infrastructure 7.2 Study Guide (p.292): "FortiGate HA uses the Fortinet- proprietary FortiGate Clustering Protocol (FGCP) to discover members, elect the primary FortiGate, synchronize data among members, and monitor the health

of members. To discover and monitor members, the members broadcast heartbeat packets over all configured heartbeat interfaces."

QUESTION 4

Which statement about video filtering on FortiGate is true?

A. Full SSL Inspection is not required.

B. It is available only on a proxy-based firewall policy.

C. It inspects video files hosted on file sharing services.

D. Video filtering FortiGuard categories are based on web filter FortiGuard categories.

Correct Answer: B

Reference: https://docs.fortinet.com/document/fortigate/7.0.0/new-features/190873/video-filtering

QUESTION 5

Refer to the exhibits.

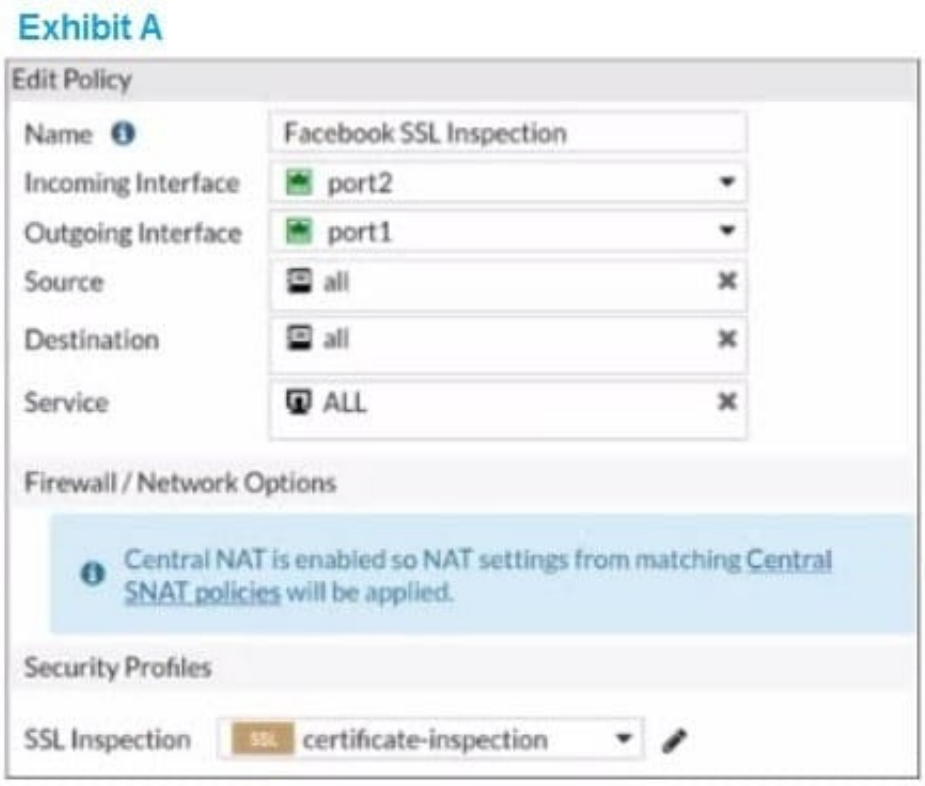

Exhibit B

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. Make SSL inspection needs to be a deep content inspection.

B. Force access to Facebook using the HTTP service.

C. Get the 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

They can play video (tick) content hosted on Facebook, but they are unable to leave reactions on videos or other types of posts. This indicate that the rule are partially working as they can watch video but cant react, i.e. liking the content. So must be an issue with the SSL inspection rather then adding an app rule.