NSE4_FGT-6.0^{Q&As}

Fortinet NSE 4 - FortiOS 6.0

Pass Fortinet NSE4_FGT-6.0 Exam with 100% Guarantee

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

https://www.passapply.com/nse4_fgt-6-0.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

View the exhibit.

```
date=2018-01-30 time=07:21:49 logid="0316013057" type="utm" subtype="webfilter"
eventtype="ftgd_blk" level="warning" vd="root" logtime=1517325709 policyid=1
sessionid=15332 srcip=10.0.1.20 scrport=59538 srcintf="port3" srcintfrole="undefined"
dstip=208.91.112.55 dstport=80 dstintf="port1" dstintfrole="undefined" proto=6
service="HTTP" hostname="lavito.tk" profile="Category-block-and-warning" action="blocked"
reqtype="direct" url="/" sentbyte=140 rcvdbyte=0 direction="outgoing" msg="URL belongs
a category with warnings enabled" method="domain" cat=0 catdesc="Unrated" crscore=30
crlevel="high"
```

ID	Name	From	To
2	IPS	port1	port3
1	Full_Access	port3	port1
0	Implicit Deny	☐ any	☐ any

What does this raw log indicate? (Choose two.)

A. FortiGate blocked the traffic.

B. type indicates that a security event was recorded.

C. 10.0.1.20 is the IP address for lavito.tk.

D. policyid indicates that traffic went through the IPS firewall policy.

Correct Answer: BD

QUESTION 2

How does FortiGate select the central SNAT policy that is applied to a TCP session?

A. It selects the SNAT policy specified in the configuration of the outgoing interface.

B. It selects the first matching central SNAT policy, reviewing from top to bottom.

C. It selects the central SNAT policy with the lowest priority.

D. It selects the SNAT policy specified in the configuration of the firewall policy that matches the traffic.

Correct Answer: B

QUESTION 3

Which statement about the IP authentication header (AH) used by IPsec is true?

A. AH does not provide any data integrity or encryption.

B. AH does not support perfect forward secrecy.

C. AH provides data integrity bur no encryption.

D. AH provides strong data integrity but weak encryption.

Correct Answer: C

QUESTION 4

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: A

QUESTION 5

View the certificate shown to the exhibit, and then answer the following question: The CA issued this certificate to which entity?

Field	Value
Version	V3
Serial Number	98765432
Signature algorithm	SHA256RSA
Issuer	cn=RootCA,o=BridgeAuthority, Inc., c=US
Valid from	Tuesday, October 3, 2016 4:33:37 PM
Valid to	Wednesday, October 2, 2019 5:03:37 PM
Subject	cn=John Doe, o=ABC, Inc..c=US
Public key	RSA (2048 bits)
Key Usage	keyCertSign
Extended Key Usage	Server Authentication (1.3.6.1.5.5.7.3.1), Client Authentication (1.3.6.1.5.5.7.3.2)
Basic Constraints	CA=True, Path Constraint=None
CRL Distribution Points	URL=http://webserver.abcinc.com/arlcert.crl

A. A root CA

B. A person

C. A bridge CA

D. A subordinate CA

Correct Answer: A

[NSE4_FGT-6.0 Study Guide](link)   [NSE4_FGT-6.0 Exam Questions](link)   [NSE4_FGT-6.0 Braindumps](link)