NSE4_FGT-5.6 Q&As

Fortinet NSE 4 - FortiOS 5.6

Pass Fortinet NSE4_FGT-5.6 Exam with 100% Guarantee

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

https://www.leads4pass.com/nse4_fgt-5-6.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

What FortiGate feature can be used to prevent a cross-site scripting (XSS) attack? Response:

A. Web application firewall (WAF)

B. DoS policies

C. Rate based IPS signatures

D. One-arm sniffer

Correct Answer: A

QUESTION 2

When does the FortiGate enter into fail-open session mode? Response:

A. When CPU usage goes above the red threshold.

B. When a proxy (for proxy-based inspection) runs out of connections.

C. When memory usage goes above the red threshold.

D. When memory usage goes above the extreme threshold.

Correct Answer: B

QUESTION 3

Examine this output from a debug flow:

```
id=2 line=4677 msg="vd-root received a packet (proto=6, 66.171.121.44:80 - >10.200.1.1:49886) from port1. flag
[S.], seq 3567496940, ack 2176715502, win 5840"
id=2 line=4739 msg="Find an existing session, id-00007fc0, reply direction"
id=2 line=2733 msg="DNAT 10.200.1.1:49886 - > 10.0.1.10:49886"
id=2 line=2582 msg="find a route: flag=00000000 gw-10.0.1.10 via port3"
```

Which statements about the output are correct?

(Choose two.)

Response:

A. FortiGate received a TCP SYN/ACK packet.

B. The source IP address of the packet was translated to 10.0.1.10.

C. FortiGate routed the packet through port 3.

D. The packet was allowed by the firewall policy with the ID 00007fc0.

Correct Answer: BC

QUESTION 4

An administrator wants to monitor their network for any probing attempts aimed to exploit existing vulnerabilities in their servers. What must they configure on their FortiGate to accomplish this?

(Choose two.)

Response:

A. An application control profile and set all application signatures to monitor.

B. A DoS policy, and log all UDP and TCP scan attempts.

C. An IPS sensor to monitor all signatures applicable to the server.

D. A web application firewall profile to check protocol constraints.

Correct Answer: BC

QUESTION 5

Which statements about IP-based explicit proxy authentication are true?

(Choose two.)

Response:

A. IP-based authentication is best suited to authenticating users behind a NAT device.

B. Sessions from the same source address are treated as a single user.

C. IP-based authentication consumes less FortiGate\\'s memory than session-based authentication.

D. FortiGate remembers authenticated sessions using browser cookies.

Correct Answer: BC

QUESTION 6

Which are the different types of memory conserve mode that can occur on a FortiGate device?

(Choose two.)

Response:

A. System

B. Device

C. Kernel

D. Flow

Correct Answer: AC

QUESTION 7

Which statements about FortiGate inspection modes are true?

(Choose two.)

Response:

A. The default inspection mode is proxy based.

B. Switching from proxy-based mode to flow-based, then back to proxy-based mode, will not result in the original configuration.

C. Proxy-based inspection is not available in VDOMs operating in transparent mode.

D. Flow-based profiles must be manually converted to proxy-based profiles before changing the inspection mode from flow based to proxy based.

Correct Answer: AC

QUESTION 8

Which statements are true of public key infrastracture (PKI) users on FortiGate?

(Choose two.)

Response:

A. FortiGate must include the CA certificate that issued the PKI peer user certificate.

B. PKI users can belong to firewall user groups.

C. PKI users must authenticate with both a certificate and a password.

D. The first PKI user must be added to FortiGate through the GUI.

Correct Answer: AB

QUESTION 9

Which of the following statements about advanced AD access mode for the FSSO collector agent are true? (Choose two.)

Response:

A. FortiGate can act as an LDAP client to configure the group filters.

B. It is only supported if DC agents are deployed.

C. It supports monitoring of nested groups.

D. It uses the Windows convention for naming; that is, Domain\Username.

Correct Answer: AB

QUESTION 10

What FortiGate feature can be used to block a ping sweep scan from an attacker? Response:

A. Web application firewall (WAF)

B. Rate based IPS signatures

C. One-arm sniffer

D. DoS policies

Correct Answer: B

QUESTION 11

What protocol can be used to dynamically assign an IP address to a physical interface? Response:

A. PPPoE

B. IP Config

C. BOOTP

D. ICMP

Correct Answer: A

QUESTION 12

View the exhibit.

```
#diagnose hardware sysinfo shm

SHM COUNTER:           10316
SHM allocated:     617643792
SHM total:        1572380672
conserve mode:    on-mem
system last entered: Fri Jun 3 10:16:39    2016
sys fd last entered:    n/a
SHM FS total:     1607806976
SHM FS free:       990134272
SHM FS avail:      990134272
SHM FS alloc:      617672704
```

Based on this output, which statements are correct?

(Choose two.)

Response:

A. FortiGate generated an event log for system conserve mode.

B. FortiGate has entered in to system conserve mode.

C. By default, the FortiGate blocks new sessions.

D. FortiGate changed the global av-failopen settings to idledrop.

Correct Answer: BC

QUESTION 13

A FortiGate interface is configured with the following commands:

```
config system interface
edit "port1"
config ipv6
set ip6-address 2001:db8:1::254/64
set ip6-send-adv enable
config ip6-prefix-list
edit 2001:db8:1::/64
set autonomous-flag enable
set onlink-flag enable
end
```

What statements about the configuration are correct?

(Choose two.)

Response:

A. IPv6 clients connected to port1 can use SLAAC to generate their IPv6 addresses.

B. FortiGate can provide DNS settings to IPv6 clients.

C. FortiGate can send IPv6 router advertisements (RAs.)

D. FortiGate can provide IPv6 addresses to DHCPv6 client.

Correct Answer: AC

QUESTION 14

LDAP and RADIUS are both remote authentication servers that FortiGate can tie into for authentication. What is a key difference between these servers?

Response: A. Only LDAP can have a secure connection with FortiGate using a server certificate.

B. Only LDAP can be configured to authenticate groups as defined on the LDAP server.

C. Only LDAP provides authentication, authorization, and accounting (AAA) services.

D. Only RADIUS requires a distinguished name (i h.) to locate user records.

Correct Answer: A

QUESTION 15

Which component of FortiOS performs application control inspection? Response:

A. Kernel

B. Antivirus engine

C. IPS engine

D. Application control engine

Correct Answer: C

Latest NSE4_FGT-5.6 Dumps | NSE4_FGT-5.6 PDF Dumps | NSE4_FGT-5.6 Practice Test