VCE & PDF
Pass4itSure.com

NSE4_FGT-6.4$^{Q\&As}$

Fortinet NSE 4 - FortiOS 6.4

Pass Fortinet NSE4_FGT-6.4 Exam with 100% Guarantee

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

https://www.pass4itsure.com/nse4_fgt-6-4.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

SATISFACTION GUARANTEED
100%
SATISFACTION GUARANTEED

QUESTION 1

You have enabled logging on your FortiGate device for Event logs and all Security logs, and you have set up logging to use the FortiGate local disk.

What is the default behavior when the local disk is full?

A. Logs are overwritten and the only warning is issued when log disk usage reaches the threshold of 95%.

B. No new log is recorded until you manually clear logs from the local disk.

C. Logs are overwritten and the first warning is issued when log disk usage reaches the threshold of 75%.

D. No new log is recorded after the warning is issued when log disk usage reaches the threshold of 95%.

Correct Answer: C

Reference: https://docs.fortinet.com/document/fortigate/6.4.0/cli-reference/462620/log-disk-setting

QUESTION 2

Which three statements about security associations (SA) in IPsec are correct? (Choose three.)

A. Phase 2 SAs are used for encrypting and decrypting the data exchanged through the tunnel.

B. An SA never expires.

C. A phase 1 SA is bidirectional, while a phase 2 SA is directional.

D. Phase 2 SA expiration can be time-based, volume-based, or both.

E. Both the phase 1 SA and phase 2 SA are bidirectional.

Correct Answer: ACD

QUESTION 3

Which three methods are used by the collector agent for AD polling? (Choose three.)

A. FortiGate polling

B. NetAPI

C. Novell API

D. WMI

E. WinSecLog

Correct Answer: BDE

Reference: https://kb.fortinet.com/kb/documentLink.do?externalID=FD47732

QUESTION 4

Refer to the exhibits.

Exhibit A | Exhibit B

```
# get system performance status
CPU states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
CPU0 states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
Memory: 2061108k total, 1854997k used (90%), 106111k free (5.1%), 100000k freeable (4.8%)
Average network usage: 83 / 0 kbps in 1 minute, 81 / 0 kbps in 10 minutes, 81 / 0 kbps in 30
minutes
Average sessions: 5 sessions in 1 minute, 3 sessions in 10 minutes, 3 sessions in 30 minutes
Average session setup rate: 0 sessions per second in last 1 minute, 0 sessions per second in last
10 minutes, 0 sessions per second in last 30 minutes
Virus caught: 0 total in 1 minute
IPS attacks blocked: 0 total in 1 minute
Uptime: 10 days,  3 hours,  28 minutes
```

Exhibit A | Exhibit B

```
config system global
     set memory-use-threshold-red 88
     set memory-use-threshold-extreme 95
     set memory-use-threshold-green 82
end
```

Exhibit A shows system performance output. Exhibit B shows a FortiGate configured with the default configuration of high memory usage thresholds. Based on the system performance output, which two statements are correct? (Choose two.)

A. Administrators can access FortiGate only through the console port.

B. FortiGate has entered conserve mode.

C. FortiGate will start sending all files to FortiSandbox for inspection.

D. Administrators cannot change the configuration.

Correct Answer: BD

QUESTION 5

Refer to the exhibit.

```
vcluster_nr=1
vcluster_0: start_time=1593701974(2020-07-02 10:59:34), state/o/chg_time=2(work)/2
(work)/1593701169(2020-07-02 10:46:09)
      pingsvr_flip_timeout/expire=3600s/2781s
      'FGVM010000064692': ha_prio/o=1/1, link_failure=0, pingsvr_failure=0, flag=
0x00000000, uptime/reset_cnt=198/0
      'FGVM010000065036': ha_prio/o=0/0, link_failure=0, pingsvr_failure=0, flag=
0x00000001, uptime/reset_cnt=0/1
```

The exhibit displays the output of the CLI command: diagnose sys ha dump-by vcluster. Which two statements are true? (Choose two.)

A. FortiGate SN FGVM010000065036 HA uptime has been reset.

B. FortiGate devices are not in sync because one device is down.

C. FortiGate SN FGVM010000064692 is the primary because of higher HA uptime.

D. FortiGate SN FGVM010000064692 has the higher HA priority.

Correct Answer: AC

QUESTION 6

Which of the following statements about backing up logs from the CLI and downloading logs from the GUI are true? (Choose two.)

A. Log downloads from the GUI are limited to the current filter view

B. Log backups from the CLI cannot be restored to another FortiGate.

C. Log backups from the CLI can be configured to upload to FTP as a scheduled time

D. Log downloads from the GUI are stored as LZ4 compressed files.

Correct Answer: AB

QUESTION 7

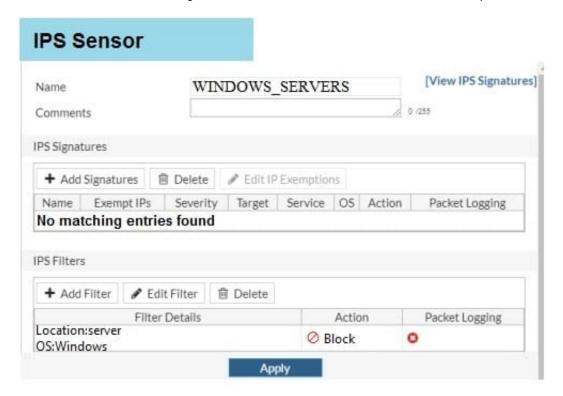Which two statements about antivirus scanning mode are true? (Choose two.)

A. In proxy-based inspection mode, files bigger than the buffer size are scanned.

B. In flow-based inspection mode, FortiGate buffers the file, but also simultaneously transmits it to the client.

C. In proxy-based inspection mode, antivirus scanning buffers the whole file for scanning, before sending it to the client.

D. In flow-based inspection mode, files bigger than the buffer size are scanned.

Correct Answer: BC

QUESTION 8

Examine the IPS sensor configuration shown in the exhibit, and then answer the question below.

IPS Sensor

Name	WINDOWS_SERVERS	[View IPS Signatures]
Comments		0 /255

IPS Signatures

+ Add Signatures   🗑 Delete   ✏ Edit IP Exemptions

Name	Exempt IPs	Severity	Target	Service	OS	Action	Packet Logging
No matching entries found							

IPS Filters

+ Add Filter   ✏ Edit Filter   🗑 Delete

Filter Details	Action	Packet Logging
Location:server OS:Windows	⊘ Block	🚫

Apply

Forward Traffic Logs

🔄 ⬇ ⊕ Add Filter

#	🔖	Date/Time	Source	Destination	Application Name	Result	Policy
1		10:09:03	10.200.1.254	10.200.1.200	HTTPS	✔ 1.30kB/2.65 kB	2(Web-Server-Access-IPS)
2		10:09:03	10.200.1.254	10.200.1.200	HTTPS	✔ 1.30kB/2.65 kB	2(Web-Server-Access-IPS)
3		10:09:02	10.200.1.254	10.200.1.200	HTTPS	✔ 1.30kB/2.65 kB	2(Web-Server-Access-IPS)
4		10:09:02	10.200.1.254	10.200.1.200	HTTPS	✔ 1.30kB/2.65 kB	2(Web-Server-Access-IPS)
5		10:09:01	10.200.1.254	10.200.1.200	HTTPS	✔ 1.30kB/2.65 kB	2(Web-Server-Access-IPS)
6		10:08:59	10.200.1.254	10.200.1.200	HTTPS	✔ 1.30kB/2.65 kB	2(Web-Server-Access-IPS)
7		10:08:57	10.200.1.254	10.200.1.200	HTTPS	✔ 1.30kB/2.65 kB	2(Web-Server-Access-IPS)
8		10:08:57	10.200.1.254	10.200.1.200	HTTPS	✔ 1.30kB/2.65 kB	2(Web-Server-Access-IPS)
9		10:08:57	10.200.1.254	10.200.1.200	HTTPS	✔ 1.30kB/2.65 kB	2(Web-Server-Access-IPS)
10		10:08:57	10.200.1.254	10.200.1.200	HTTPS	✔ 1.30kB/2.65 kB	2(Web-Server-Access-IPS)

An administrator has configured the WINDOWS_SERVERS IPS sensor in an attempt to determine whether the influx of HTTPS traffic is an attack attempt or not. After applying the IPS sensor, FortiGate is still not generating any IPS logs for the HTTPS traffic.

What is a possible reason for this?

A. The IPS filter is missing the Protocol: HTTPS option.

B. The HTTPS signatures have not been added to the sensor.

C. A DoS policy should be used, instead of an IPS sensor.

D. A DoS policy should be used, instead of an IPS sensor.

E. The firewall policy is not using a full SSL inspection profile.

Correct Answer: E

QUESTION 9

NGFW mode allows policy-based configuration for most inspection rules. Which security profile\\'s configuration does not change when you enable policy-based inspection?

A. Web filtering

B. Antivirus

C. Web proxy

D. Application control

Correct Answer: B

QUESTION 10

Refer to the exhibit.

```
# diagnose test application ipsmonitor
1: Display IPS engine information
2: Toggle IPS engine enable/disable status
3: Display restart log
4: Clear restart log
5: Toggle bypass status
98: Stop all IPS engines
99: Restart all IPS engines and monitor
```

Examine the intrusion prevention system (IPS) diagnostic command.

Which statement is correct If option 5 was used with the IPS diagnostic command and the outcome was a decrease in the CPU usage?

A. The IPS engine was inspecting high volume of traffic.

B. The IPS engine was unable to prevent an intrusion attack.

C. The IPS engine was blocking all traffic.

D. The IPS engine will continue to run in a normal state.

Correct Answer: A

QUESTION 11

What is the limitation of using a URL list and application control on the same firewall policy, in NGFW policy-based mode?

A. It limits the scope of application control to the browser-based technology category only.

B. It limits the scope of application control to scan application traffic based on application category only.

C. It limits the scope of application control to scan application traffic using parent signatures only

D. It limits the scope of application control to scan application traffic on DNS protocol only.

Correct Answer: B

QUESTION 12

Examine this output from a debug flow:

```
id=20085 trace_id=1 func=print_pkt_detail line=5363 msg="vd-root received a packet(proto=1,
10.0.1.10:1->10.200.1.254:2048)
from port3. type=8, code=0, id=1, seq=33."
id=20085 trace_id=1 func=init_ip_session_common line=5519 msg="allocate a new session=00000340"
id=20085 trace_id=1 func=vf_ip_route_input_common line=2583 msg="find a route: flag=04000000 gw=10.200.1.254 via
port1"
id=20085 trace_id=1 func=fw_forward_handler line=586 msg="Denied by forward policy check (policy 0)"
```

Why did the FortiGate drop the packet?

A. The next-hop IP address is unreachable.

B. It failed the RPF check.

C. It matched an explicitly configured firewall policy with the action DENY.

D. It matched the default implicit firewall policy.

Correct Answer: D

https://kb.fortinet.com/kb/documentLink.do?externalID=13900

QUESTION 13

Which two statements are correct about a software switch on FortiGate? (Choose two.)

A. It can be configured only when FortiGate is operating in NAT mode

B. Can act as a Layer 2 switch as well as a Layer 3 router

C. All interfaces in the software switch share the same IP address

D. It can group only physical interfaces

Correct Answer: AC

QUESTION 14

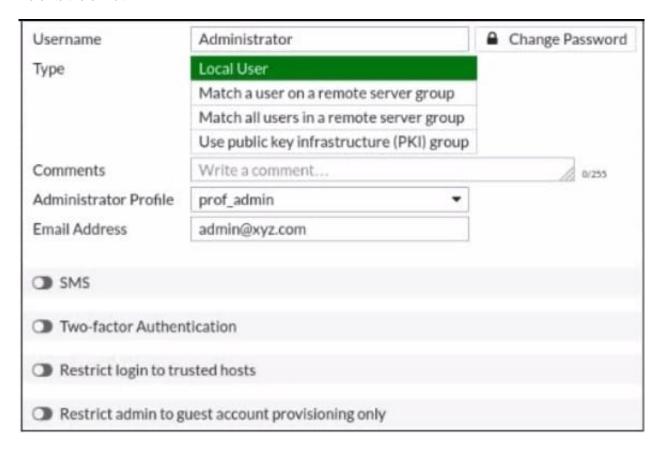Which two configuration settings are synchronized when FortiGate devices are in an active-active HA cluster? (Choose two.)

A. FortiGuard web filter cache

B. FortiGate hostname

C. NTP

D. DNS

Correct Answer: CD

QUESTION 15

Refer to the exhibit.

The global settings on a FortiGate device must be changed to align with company security policies. What does the Administrator account need to access the FortiGate global settings?

A. Change password

B. Enable restrict access to trusted hosts

C. Change Administrator profile

D. Enable two-factor authentication

Correct Answer: C

Latest NSE4_FGT-6.4 Dumps

NSE4_FGT-6.4 PDF Dumps

NSE4_FGT-6.4 Practice Test