



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

- ⚙️ **Instant Download** After Purchase
- ⚙️ **100% Money Back** Guarantee
- ⚙️ **365 Days** Free Update
- ⚙️ **800,000+** Satisfied Customers





QUESTION 1

You have tasked to design a new IPsec deployment with the following criteria:

1.

There are two HQ sites that all satellite offices must connect to

2.

The satellite offices do not need to communicate directly with other satellite offices

3.

No dynamic routing will be used

4.

The design should minimize the number of tunnels being configured.

Which topology should be used to satisfy all of the requirements?

A. Partial mesh

B. Hub-and-spoke

C. Fully meshed

D. Redundant

Correct Answer: B

QUESTION 2

Which of the following FortiGate configuration tasks will create a route in the policy route table? (Choose two.)

A. Static route created with a Named Address object

B. Static route created with an Internet Services object

C. SD-WAN route created for individual member interfaces

D. SD-WAN rule created to route traffic based on link latency

Correct Answer: BD

QUESTION 3

Which statements about the firmware upgrade process on an active-active HA cluster are true? (Choose two.)

A. The firmware image must be manually uploaded to each FortiGate.



- B. Only secondary FortiGate devices are rebooted.
- C. Uninterruptable upgrade is enabled by default.
- D. Traffic load balancing is temporally disabled while upgrading the firmware.

Correct Answer: BD

QUESTION 4

By default, when logging to disk, when does FortiGate delete logs?

- A. 30 days
- B. 1 year
- C. Never
- D. 7 days

Correct Answer: D

QUESTION 5

Which of the following statements is true regarding SSL VPN settings for an SSL VPN portal?

- A. By default, FortiGate uses WINS servers to resolve names.
- B. By default, the SSL VPN portal requires the installation of a client's certificate.
- C. By default, split tunneling is enabled.
- D. By default, the admin GUI and SSL VPN portal use the same HTTPS port.

Correct Answer: D

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: BC



QUESTION 7

How does FortiGate verify the login credentials of a remote LDAP user?

- A. FortiGate regenerates the algorithm based on the login credentials and compares it to the algorithm stored on the LDAP server.
- B. FortiGate sends the user-entered credentials to the LDAP server for authentication.
- C. FortiGate queries the LDAP server for credentials.
- D. FortiGate queries its own database for credentials.

Correct Answer: B

QUESTION 8

View the exhibit.

ID	Name	Source	Destination	Schedule	Service	Applications	URL Category	Action	NAT	Security Profiles	Log	Bytes
port 3 → port 1												
2	Video/Audio	all	all	always	ALL	Video/Audio	+	DENY		SSL certificate-inspection	All	76.74 kB
4	Social_Media	all	all	always	ALL	Social Media	Social Networking	DENY		SSL certificate-inspection	All	940.57 kB
3	ALLOW_ALL	all	all	always	ALL			ACCEPT	Custom		UTM	97.72 kB
Implicit												
0	Implicit Deny	all	all	always	ALL			DENY			Disabled	3.58 MB

Based on the configuration shown in the exhibit, what statements about application control behavior are true? (Choose two.)

- A. Access to all unknown applications will be allowed.
- B. Access to browser-based Social.Media applications will be blocked.
- C. Access to mobile social media applications will be blocked.
- D. Access to all applications in Social.Media category will be blocked.

Correct Answer: AB

QUESTION 9

Which statements correctly describe transparent mode operation? (Choose three.)

- A. All interfaces of the transparent mode FortiGate device must be on different IP subnets.
- B. Ethernet packets are forwarded based on destination MAC addresses, not IP addresses.
- C. The transparent FortiGate is visible to network hosts in an IP traceroute.



D. It permits inline traffic inspection and firewalling without changing the IP scheme of the network.

E. FortiGate acts as transparent bridge and forwards traffic at Layer 2.

Correct Answer: BDE

QUESTION 10

Which of the following services can be inspected by the DLP profile? (Choose three.)

A. NFS

B. FTP

C. IMAP

D. CIFS

E. HTTP-POST

Correct Answer: BCE

QUESTION 11

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



IPS Sensor

Edit IPS Sensor WINDOWS_SERVER [View IPS Signatures]

Name

Comments

IPS Signatures

+ Add Signatures 🗑 Delete ✎ Edit IP Exemptions

Name	Exempt IPs	Severity	Target	Service	OS	Action	Packet Logging
SMTPLoginBruteForce ⁰		🔵 🔴 🟢 🟡	Server	TCP_SMT	All	🚫 Block	🔴

IPS Filters

+ Add Filter ✎ Edit Filter 🗑 Delete

Filter Details	Action	Packet Logging
Location: server Protocol: SMTP	🚫 Block	🔴

Rate Based Signatures

Enable	Signature	Threshold	Duration (seconds)	Track By	Action	Block Duration (minutes)
<input checked="" type="checkbox"/>	IMAPLoginBruteForce <small>Memory Exhaustion DoS</small>	60	10	Source IP	🚫 Block	None
<input type="checkbox"/>	DigitalSignatureInvitedTCPConnectFileCheck DoS	5	1	Any	🚫 Block	None

Apply

DoS Policy

Incoming Interface 📶 port1 ▼

Source Address 📄 all + ✕

Destination Address 📄 all + ✕

Services 👤 ALL + ✕

L3 Anomalies

Name	<input type="checkbox"/> Status	<input type="checkbox"/> Logging	<input type="button" value="Pass"/> <input type="button" value="Block"/> Action	Threshold
ip_src_session	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="button" value="Pass"/> <input checked="" type="button" value="Block"/>	60
ip_dst_session	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="button" value="Pass"/> <input type="button" value="Block"/>	5000

When detecting attacks, which anomaly, signature, or filter will FortiGate evaluate first?

- A. SMTP.Login.Brute.Force
- B. IMAP.Login.brute.Force



C. ip_src_session

D. Location: server Protocol: SMTP

Correct Answer: B

QUESTION 12

When using WPAD DNS method, which FQDN format do browsers use to query the DNS server?

A. srv_proxy./wpad.dat

B. srv_tcp.wpad.

C. wpad.

D. proxy..wpad

Correct Answer: C

QUESTION 13

The FSSO Collector Agent set to advanced access mode for the Windows Active Directory uses which of the following?

A. LDAP convention B. NTLM convention

C. Windows convention ?NetBios\Username

D. RSSO convention

Correct Answer: A

QUESTION 14

Which of the following statements about central NAT are true? (Choose two.)

A. IP tool references must be removed from existing firewall policies before enabling central NAT.

B. Central NAT can be enabled or disabled from the CLI only.

C. Source NAT, using central NAT does not require a central SNAT policy.

D. Destination NAT, using central NAT, requires a VIP object as the destination address in a firewall.

Correct Answer: AB

QUESTION 15

Which action can be applied to each filter in the application control profile?



- A. Block, monitor, warning, and quarantine
- B. Allow, monitor, block and learn
- C. Allow, block, authenticate, and warning
- D. Allow, monitor, block, and quarantine

Correct Answer: D

[Latest NSE4_FGT-6.0
Dumps](#)

[NSE4_FGT-6.0 PDF Dumps](#)

[NSE4_FGT-6.0 Exam
Questions](#)