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

QUESTION 1

A network administrator has enabled SSL certificate inspection and antivirus on FortiGate. When downloading an EICAR test file through HTTP, FortiGate detects the virus and blocks the file. When downloading the same file through HTTPS, FortiGate does not detect the virus and the file can be downloaded.

What is the reason for the failed virus detection by FortiGate?

A. Application control is not enabled

B. SSL/SSH Inspection profile is incorrect

C. Antivirus profile configuration is incorrect

D. Antivirus definitions are not up to date

Correct Answer: B

QUESTION 2

Which of the following are valid actions for FortiGuard category based filter in a web filter profile ui proxy-based inspection mode? (Choose two.)

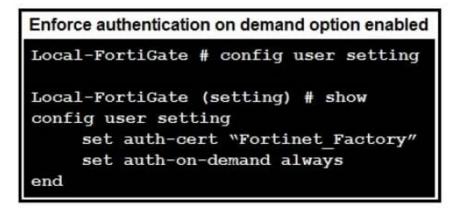A. Warning

B. Exempt

C. Allow

D. Learn

Correct Answer: AC

QUESTION 3

Refer to the exhibit.

Network interface configuration

Edit Interface

Name	▥ LAN(port3)
Alias	LAN
Type	▤ Physical Interface
Role ❶	Undefined ▼

Address

Addressing mode	**Manual** DHCP
IP/Netmask	10.0.1.254/255.255.255.0
Secondary IP address	⚪

Administrative Access

IPv4
- ☑ HTTPS ☑ HTTP ☑ PING
- ☐ FMG-Access ☑ SSH ☐ SNMP
- ☑ TELNET ☐ FTM ☐ RADIUS Accounting
- ☐ Security Fabric Connection ❶

Receive LLDP ❶	**Use VDOM Setting** Enable Disable
Transmit LLDP ❶	**Use VDOM Setting** Enable Disable

Network

Device detection ❶	⚪
Security mode	⬤ Captive Portal ▼
Authentication portal	**Local** External
User Access ❶	**Restricted to Groups** Allow all
User Groups	▦ HR ✕
	+
Exempt sources	+
Exempt destinations/services	+
Redirect after Captive Portal	**Original Request** Specific URL

Enforce authentication on demand option enabled

```
Local-FortiGate # config user setting

Local-FortiGate (setting) # show
config user setting
    set auth-cert "Fortinet_Factory"
    set auth-on-demand always
end
```

Firewall policies

Name	Source	Destination	Schedule	Service	Action	NAT
⊟ 🖼 LAN(port3) → 🖼 WAN(port1) ❷						
Sales Users	🏢 Sales 🖥LOCAL_SUBNET	🖥 all	🕓 always	🔲 ALL	✔ ACCEPT	✅ Enabled
Auth-Users	🖥LOCAL_SUBNET	🖥 all	🕓 always	🕓 ALL	✔ACCEPT	✅ Enabled

The exhibit contains a network interface configuration, firewall policies, and a CLI console configuration.

How will FortiGate handle user authentication for traffic that arrives on the LAN interface?

A. If there is a full-through policy in place, users will not be prompted for authentication.

B. Users from the Sales group will be prompted for authentication and can authenticate successfully with the correct credentials.

C. Authentication is enforced at a policy level; all users will be prompted for authentication.

D. Users from the HR group will be prompted for authentication and can authenticate successfully with the correct credentials.

Correct Answer: C

QUESTION 4

Refer to the exhibit.

Name	SLA_1	
Protocol	Ping HTTP DNS	
Servers	4.2.2.2	✗
	4.2.2.1	✗
Participants	All SD-WAN Members Specify	
	🔲 port1	✗
	🔲 port2	✗
	+	
Enable probe packets	⬤	

Which contains a Performance SLA configuration.

An administrator has configured a performance SLA on FortiGate. Which failed to generate any traffic. Why is FortiGate not generating any traffic for the performance SLA?

A. Participants configured are not SD-WAN members.

B. There may not be a static route to route the performance SLA traffic.

C. The Ping protocol is not supported for the public servers that are configured.

D. You need to turn on the Enable probe packets switch.

Correct Answer: D

Reference: https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/478384/performance-sla-linkmonitoring

QUESTION 5

Which statement regarding the firewall policy authentication timeout is true?

A. It is an idle timeout. The FortiGate considers a user to be "idle" if it does not see any packets coming from the user\\'s source IP.

B. It is a hard timeout. The FortiGate removes the temporary policy for a user\\'s source IP address after this timer has expired.

C. It is an idle timeout. The FortiGate considers a user to be "idle" if it does not see any packets coming from the user\\'s source MAC.

D. It is a hard timeout. The FortiGate removes the temporary policy for a user\\'s source MAC address after this timer has expired.

Correct Answer: A