

DUMPS ARENA

Fortinet NSE 4 - FortiOS 6.4

Fortinet NSE4 FGT-6.4

Version Demo

Total Demo Questions: 10

Total Premium Questions: 121

Buy Premium PDF

<https://dumpsarena.com>

sales@dumpsarena.com

dumpsarena.com

QUESTION NO: 1

How does FortiGate act when using SSL VPN in web mode?

- A. FortiGate acts as an FDS server.
- B. FortiGate acts as an HTTP reverse proxy.
- C. FortiGate acts as DNS server.
- D. FortiGate acts as router.

ANSWER: B**Explanation:**

Reference: https://pub.kb.fortinet.com/ksmcontent/Fortinet-Public/current/Fortigate_v4.0MR3/fortigate-sslvpn-40-mr3.pdf

QUESTION NO: 2

A network administrator has enabled full SSL inspection and web filtering on FortiGate. When visiting any HTTPS websites, the browser reports certificate warning errors. When visiting HTTP websites, the browser does not report errors.

What is the reason for the certificate warning errors?

- A. The browser requires a software update.
- B. FortiGate does not support full SSL inspection when web filtering is enabled.
- C. The CA certificate set on the SSL/SSH inspection profile has not been imported into the browser.
- D. There are network connectivity issues.

ANSWER: C**Explanation:**

Reference: <https://kb.fortinet.com/kb/documentLink.do?externalID=FD41394>

QUESTION NO: 3

Refer to the exhibit, which contains a static route configuration.

Edit Static Route

Destination ⓘ **Subnet** **Internet Service**

Amazon-AWS ▼

Gateway Address 10.200.1.254

Interface port1 ▼

Comments Write a comment... 0/255

Status Enabled Disabled

An administrator created a static route for Amazon Web Services.

What CLI command must the administrator use to view the route?

- A. get router info routing-table all
- B. get internet service route list
- C. get router info routing-table database
- D. diagnose firewall proute list



ANSWER: D

Explanation:

Reference: <https://www.fortinetguru.com/2019/09/troubleshooting-sd-wan-fortios-6-2/>

QUESTION NO: 4

Refer to the exhibit.

	Name	Type	IP/Netmask	VLAN ID
Physical Interface 14				
	port1	Physical Interface	10.200.1.1/255.255.255.0	
	port1-vlan10	VLAN	10.1.10.1/255.255.255.0	10
	port1-vlan1	VLAN	10.200.5.1/255.255.255.0	1
	port10	Physical Interface	10.0.11.1/255.255.255.0	
	port2	Physical Interface	10.200.2.1/255.255.255.0	
	port2-vlan10	VLAN	10.0.10.1/255.255.255.0	10
	port2-vlan1	VLAN	10.0.5.1/255.255.255.0	1

Given the interfaces shown in the exhibit, which two statements are true? (Choose two.)

- A. Traffic between port2 and port2-vlan1 is allowed by default.
- B. port1-vlan10 and port2-vlan10 are part of the same broadcast domain.
- C. port1 is a native VLAN.
- D. port1-vlan1 and port2-vlan1 can be assigned in the same VDOM or to different VDOMs.

ANSWER: A D

QUESTION NO: 5

Which statement correctly describes NetAPI polling mode for the FSSO collector agent?

- A. NetAPI polling can increase bandwidth usage in large networks.
- B. The NetSessionEnum function is used to track user logouts.
- C. The collector agent uses a Windows API to query DCs for user logins.

D. The collector agent must search security event logs.

ANSWER: B

QUESTION NO: 6

Refer to the exhibit to view the firewall policy.

Name	Internet Access
Incoming Interface	port2
Outgoing Interface	port1
Source	all
Destination	all
Schedule	always
Service	DNS FTP HTTP HTTPS
Action	<input checked="" type="checkbox"/> ACCEPT <input type="checkbox"/> DENY
Inspection Mode	Flow-based Proxy-based
Security Profiles	
AntiVirus	<input checked="" type="checkbox"/> AV default
Web Filter	<input type="checkbox"/>
DNS Filter	<input type="checkbox"/>
Application Control	<input type="checkbox"/>
IPS	<input type="checkbox"/>
SSL Inspection	SSL certificate-inspection

Which statement is correct if well-known viruses are not being blocked?

- A. The firewall policy does not apply deep content inspection.
- B. The firewall policy must be configured in proxy-based inspection mode.
- C. The action on the firewall policy must be set to deny.
- D. Web filter should be enabled on the firewall policy to complement the antivirus profile.

ANSWER: D

QUESTION NO: 7

Which two statements are correct about SLA targets? (Choose two.)

- A. You can configure only two SLA targets per one Performance SLA.
- B. SLA targets are optional.
- C. SLA targets are required for SD-WAN rules with a Best Quality strategy.
- D. SLA targets are used only when referenced by an SD-WAN rule.

ANSWER: B D

QUESTION NO: 8

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

ANSWER: A C

QUESTION NO: 9

Which two statements are true about the Security Fabric rating? (Choose two.)

- A. It provides executive summaries of the four largest areas of security focus
- B. Many of the security issues can be fixed immediately by clicking Apply where available

- C. The Security Fabric rating is a free service that comes bundled with all FortiGate devices
- D. The Security Fabric rating must be run on the root FortiGate device in the Security Fabric

ANSWER: A D

QUESTION NO: 10

Refer to the exhibit.

```
Fortigate # diagnose sniffer packet any "icmp" 5
interfaces=[any]
filters=[icmp]
20.370482 port2 in 10.0.1.2 -> 8.8.8.8: icmp: echo request
0x0000  4500 003c 2f8f 0000 8001 f020 0a00 0102  E...</.....8..
0x0010  0808 0808 0800 4d5a 0001 0001 6162 6364  ....MZ....abcd
0x0020  6566 6768 696a 6b6c 6d6e 6f70 7172 7374  efg hijklm nopq rst
0x0030  7576 7761 6263 6465 6667 6869          uvw abcdefghi

20.370805 port1 out 10.56.240.228 -> 8.8.8.8: icmp: echo request
0x0000  4500 003c 2f8f 0000 7f01 0106 0a38 f0e4  E...</.....8..
0x0010  0808 0808 0800 6159 ec01 0001 6162 6364  ....aY....abcd
0x0020  6566 6768 696a 6b6c 6d6e 6f70 7172 7374  efg hijklm nopq rst
0x0030  7576 7761 6263 6465 6667 6869          uvw abcdefghi

20.372138 port1 in 8.8.8.8 -> 10.56.240.228: icmp: echo reply
0x0000  4500 003c 0000 0000 7501 3a95 0808 0808  E...<.....u.:....
0x0010  0a38 f0e4 0000 6959 ec01 0001 6162 6364  .8....iY....abcd
0x0020  6566 6768 696a 6b6c 6d6e 6f70 7172 7374  efg hijklm nopq rst
0x0030  7576 7761 6263 6465 6667 6869          uvw abcdefghi

20.372163 port2 out 8.8.8.8 -> 10.0.1.2: icmp: echo reply
0x0000  4500 003c 0000 0000 7401 2bb0 0808 0808  E...<...t.:....
0x0010  0a00 0102 0000 555a 0001 0001 6162 6364  .....UZ....abcd
0x0020  6566 6768 696a 6b6c 6d6e 6f70 7172 7374  efg hijklm nopq rst
0x0030  7576 7761 6263 6465 6667 6869          uvw abcdefghi
```

An administrator is running a sniffer command as shown in the exhibit.

Which three pieces of information are included in the sniffer output? (Choose three.)

- A. Interface name
- B. Ethernet header
- C. IP header
- D. Application header
- E. Packet payload

ANSWER: B C E

DUMPSARENA