

100% Money Back
Guarantee

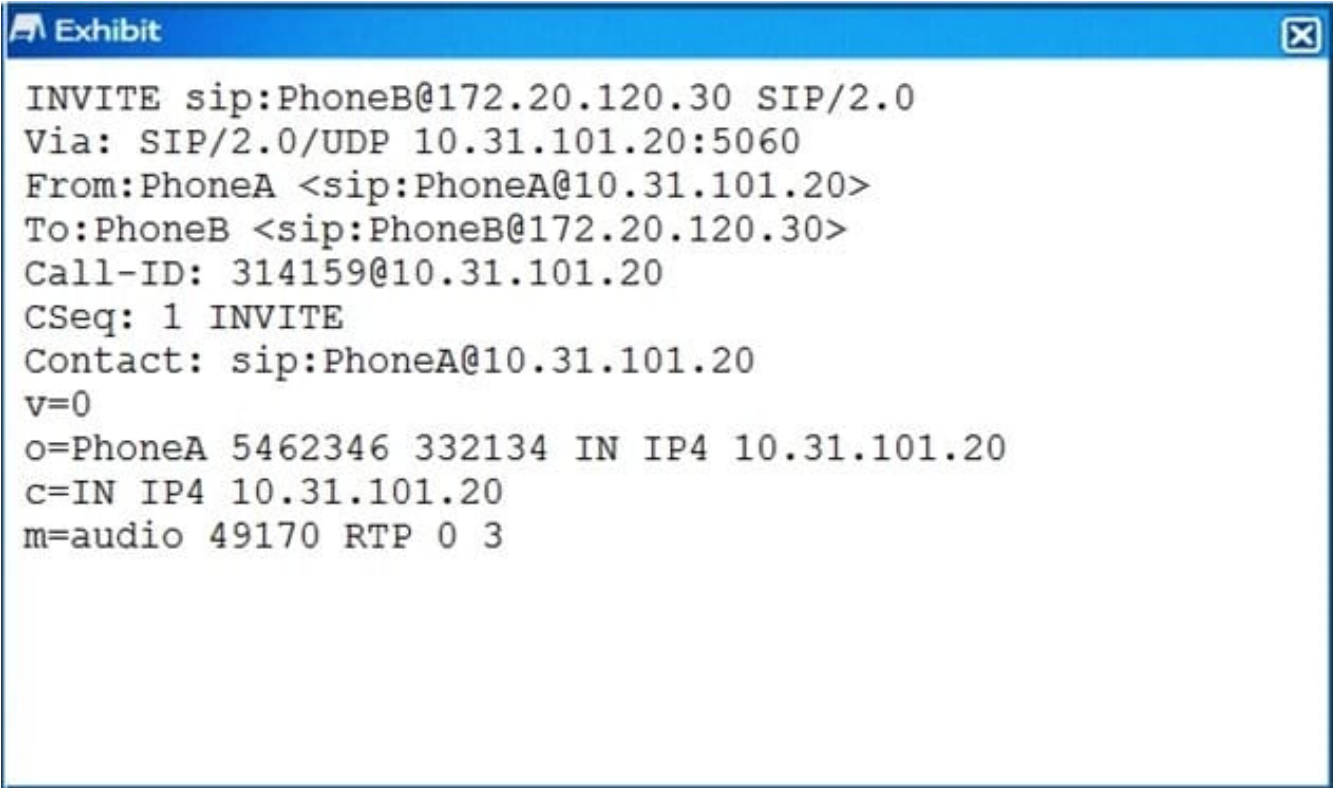
Vendor:Fortinet

Exam Code:NSE8_810

Exam Name:Fortinet Network Security Expert 8
Written Exam (810)

Version:Demo

QUESTION 1



```
Exhibit
INVITE sip:PhoneB@172.20.120.30 SIP/2.0
Via: SIP/2.0/UDP 10.31.101.20:5060
From:PhoneA <sip:PhoneA@10.31.101.20>
To:PhoneB <sip:PhoneB@172.20.120.30>
Call-ID: 314159@10.31.101.20
CSeq: 1 INVITE
Contact: sip:PhoneA@10.31.101.20
v=0
o=PhoneA 5462346 332134 IN IP4 10.31.101.20
c=IN IP4 10.31.101.20
m=audio 49170 RTP 0 3
```

Click the Exhibit button.

A FortiGate with the default configuration is deployed between two IP phones. FortiGate receives the INVITE request shown in the exhibit from Phone A (internal) to Phone B (external). Which two actions are taken by the FortiGate after the packet is received? (Choose two.)

- A. A pinhole will be opened to accept traffic sent to FortiGate's WAN IP address and ports 49169 and 49170.
- B. A pinhole will be opened to accept traffic sent to FortiGate's WAN IP address and ports 49170 and 49171.
- C. The phone A IP address will be translated to the WAN IP address in all INVITE header fields and the m: field of the SDP statement.
- D. The phone A IP address will be translated for the WAN IP address in all INVITE header fields and the SDP statement remains intact.

Correct Answer: BD

QUESTION 2

Click the Exhibit button.

Your customer is using dynamic routing to exchange the default route between two FortiGates using OSPFv2. The output of the `get router info ospf neighbor` command shows that the neighbor is up, but the default route does not appear in the routing neighbor shown below:

```
FG1 # get router info ospf neighbor
```

```
OSPF process 0:
```

Neighbor ID	Pri	State	Dead Time	Address	Interface
2.2.2.2	1	Full/-	00:00:38	192.168.10.2	port10

According to the exhibit, what is causing the problem?

```
FG2 # show router ospf
config router ospf
set default-information-originate always
set router-id 2.2.2.2
config area
edit 0.0.0.0
  next
  end
config ospf-interface
edit "P10"
  set interface "port10"
  set network-type broadcast
  next
  end
config network
edit 10
  set prefix 192.168.10.0 255.255.255.0
  next
  end
config redistribute "connected"
  end
config redistribute "static"
  end
end
```

- A. A prefix for the detail route is missing
- B. OSPF requires the redistribution of connected networks.
- C. There is an OSPF interface network-type mismatch.
- D. FG2 is within the wrong OSPF area.

Correct Answer: A

QUESTION 3

Exhibit

Installation

Management Host Preparation Logical Network Preparation Service Deployments

NSX Manager: 10.10.50.3

Network & Security Service Deployments

Network & security service are deployed on a set of clusters. Manage service deployments here by adding new services or deleting existing ones.

+ X | Actions Filter

Service	Version	Installation	Service Status	Cluster	Datastore	Port Group	IP Address Range
FGTVMX	5.6.0.1449	Failed	Unknown	VMX-Cluster	datastore1	VMX-DPortGr..	DHCP

1 items

When deploying a new FortiGate-VMX Security node, an administrator received the error message shown in the exhibit. In this scenario, which statement is correct?

- A. The vCenter was not able to locate the FortiGate-VMX's OVF file.
- B. The vCenter could not connect to the FortiGate Service Manager
- C. The NSX Manager was not able to connect to the FortiGate Service Manager's RestAPI service.
- D. The FortiGate Service Manager did not have the proper permission to register the FortiGate-VMX Service.

Correct Answer: D

QUESTION 4

You are administrating the FortiGate 5000 and FortiGate 7000 series products. You want to access the HTTPS GUI of the blade located in logical slot of the secondary chassis in a high-availability cluster.

Which URL will accomplish this task?

- A. https://192.168.1.99.44302
- B. https://192.168.1.99.44313
- C. https://192.168.1.99.44322
- D. https://192.168.1.99.44323

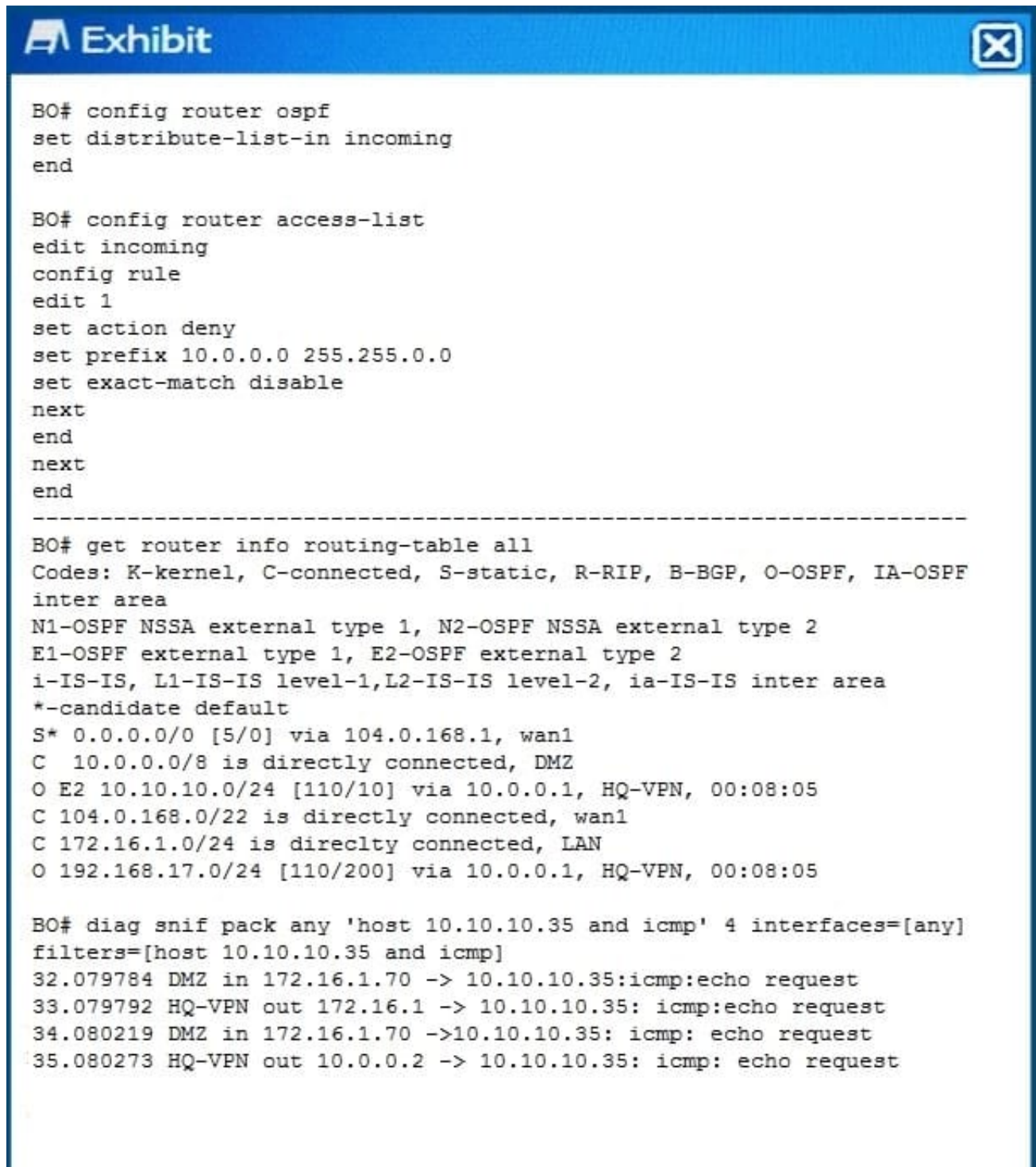
Correct Answer: B

QUESTION 5

Click the exhibit.

A VPN IPsec is connecting the headquarters office (HQ) with a branch office (BO) and OSPF is used to redistribute

routes between the offices. After deployment, a server with IP address 10.10.10.35 located on the DMZ network of the BO FortiGate, was reported unreachable from hosts located on the LAN network of the same FortiGate.

The image shows a screenshot of a FortiGate CLI session. At the top, there is a blue header with the word "Exhibit" and a close button. The CLI output is as follows:

```
BO# config router ospf
set distribute-list-in incoming
end

BO# config router access-list
edit incoming
config rule
edit 1
set action deny
set prefix 10.0.0.0 255.255.0.0
set exact-match disable
next
end
next
end

-----
BO# get router info routing-table all
Codes: K-kernel, C-connected, S-static, R-RIP, B-BGP, O-OSPF, IA-OSPF
inter area
N1-OSPF NSSA external type 1, N2-OSPF NSSA external type 2
E1-OSPF external type 1, E2-OSPF external type 2
i-IS-IS, L1-IS-IS level-1, L2-IS-IS level-2, ia-IS-IS inter area
*-candidate default
S* 0.0.0.0/0 [5/0] via 104.0.168.1, wan1
C 10.0.0.0/8 is directly connected, DMZ
O E2 10.10.10.0/24 [110/10] via 10.0.0.1, HQ-VPN, 00:08:05
C 104.0.168.0/22 is directly connected, wan1
C 172.16.1.0/24 is directly connected, LAN
O 192.168.17.0/24 [110/200] via 10.0.0.1, HQ-VPN, 00:08:05

BO# diag sniff pack any 'host 10.10.10.35 and icmp' 4 interfaces=[any]
filters=[host 10.10.10.35 and icmp]
32.079784 DMZ in 172.16.1.70 -> 10.10.10.35:icmp:echo request
33.079792 HQ-VPN out 172.16.1 -> 10.10.10.35: icmp:echo request
34.080219 DMZ in 172.16.1.70 ->10.10.10.35: icmp: echo request
35.080273 HQ-VPN out 10.0.0.2 -> 10.10.10.35: icmp: echo request
```

Referring to the exhibit, which statement is true?

- A. The ICMP packets are Being blocked by an implicit deny policy.
- B. The incoming access list should have an accept action instead deny action to solve the problem.
- C. A directly connected subnet is being partially superseded by an OSPF redistributed subnet.

D. Enabling NAT on the VPN firewall policy will solve the problem.

Correct Answer: B

QUESTION 6

You are building a FortiGala cluster which is stretched over two locations. The HA connections for the cluster are terminated on the data centers. Once the FortiGates have booted, they do form a cluster. The network operators inform you that CRC errors are present on the switches where the FortiGates are connected.

What would you do to solve this problem?

- A. Replace the cables where the CRC errors occur.
- B. Change the ethertype for the HA packets.
- C. Set the speedduplex setting to 1 Gbps /Full Duplex.
- D. Place the HA interfaces in dedicated VLANs.

Correct Answer: A

QUESTION 7

An organization has one central site And three remote sites. A FortiSIEM has been drafted on the central site and now all devices across the remote sites need to be monitored by the FortiSIEM.

When action would reduce the WAN usage by the monitoring system?

- A. Deploy a single Supervisor on the central site and enable WAN optimize on the WAN gateways.
- B. Install local Collection remote site.
- C. Disable monitoring on the remote sites during the day.
- D. install a Supervisor and a Collector for each remote site.

Correct Answer: B

QUESTION 8

Exhibit

Click the Exhibit button.

The exhibit shows the configuration of a service protection profile (SPP) in a FortiDDoS device.

Which two statements are true about the traffic matching being inspected by this SPP? (Choose two.)

Exhibit
✕

SPP ID 0

Inbound Operating Mode Detection Prevention

Outbound Operating Mode Detection Prevention

SYN Flood Mitigation Direction Inbound Outbound

SYN With Payload Direction Inbound Outbound

SYN Flood Mitigation Mode SYN Cookie ACK Cookie SYN Retransmission

Adaptive Mode Fixed Adaptive

Adaptive Limit (in percentage)
Range: 100-300

- A. Traffic that does match any spp policy will not be inspection by this spp.
- B. FortiDDoS will not send a SYNACK if a SYN packet is coming from an IP address that is not the legitimate IP (LIP) address table.
- C. FortiDooS will start dropping packets as soon as the traffic executed the configured maintain threshold.
- D. SYN packets with payloads will be drooped.

Correct Answer: AB

QUESTION 9

You cannot the FortiGales default gateway 10.10.10 .1 from the FortiGate CLI. The FortiGate interface facing the default gateway is wan 1 and its IP address 10.10 .10 K74 During the troubleshooting, tests, you confirmed that you can plug other IP addresses in the 10.10.10. 0/24 subnet from the FortiGAt e CLI without packets lost.

Which two CLI commands will help you to troubleshoot this problem? (Choose two.)

- A. diagnose ip arp list
- B. diag aniffer packet wan1 \\arp and host 10.10.10.1\\'
- C. diagnose hardware deviceinfo nice wan1
- D. diagnose debug flow filter addt 10.10.10.1
- E. diagnose debug flow trace trace 10

Correct Answer: AD

QUESTION 10

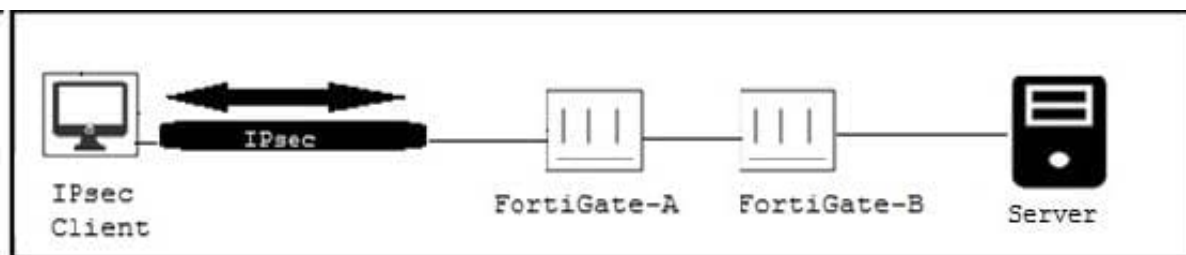
You want to manage a FortiCloud service. The FortiGate shows up in your list devices on the FortiCloud Web site, but all management functions are either missing or grayed out. Which statement is correct in this scenario?

- A. The managed FortiGate is running a version of FortiOS that is either too new or too old for FortCloud.
- B. The managed FortiGate requires that a FortiCloud management license be purchased and applied.
- C. You must manually configure system control-management on the FortiGate CLI and set the management type to fortiguard.
- D. The management tunnel mode on the managed FortiGate must be changed to normal.

Correct Answer: C

QUESTION 11

Click the Exhibit button.



Only users authenticated in FortiGate-B can reach the server. A customer wants to deploy a single sign-on solution for IPsec VPN users. Once a user is connected and authenticated to the VPN in FortiGate-A, the user does not need to authenticate again in FortiGate-B to reach the server.

Which two actions satisfy this requirement? (Choose two.)

- A. Use Kerberos authentication.
- B. FortiGate-A must generate a RADIUS accounting packets.
- C. Use FortiAuthenticator.
- D. Use the Collector Agent.

Correct Answer: BC

QUESTION 12

You must create a high Availability deployment with two FortiWebs in Amazon Services (AWS): each on different Availability Zones(AZ) from the same region. At the same time, each FortiWeb should be able to deliver content from the Web server of both of the AZs.

Which deployment would will this requirement?

- A. Configure the FortiWebs Active-Active Ha mode and use AWS Router 53 load Router balance the internal Web servers.
- B. Configure the FortiWebs in Active-Active HA mode and use AWS Elastic load Balancer (ELB) for the internal Web servers.
- C. Use AWS Router 53 to load balance FortiWebs in standone mode and use AWS Virtual private Cloud (VPC) peering to load balance the internal Web servers.
- D. Use AWS Elastic load Balancer (ELB) for both FortiWebs in standdone mode and the internal Web servers in an ELB sandwich.

Correct Answer: B