NSE8_810$^{Q\&As}$

Fortinet Network Security Expert 8 Written Exam (810)

Pass Fortinet NSE8_810 Exam with 100% Guarantee

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

https://www.pass4itsure.com/nse8_810.html

100% Passing Guarantee
100% Money Back Assurance

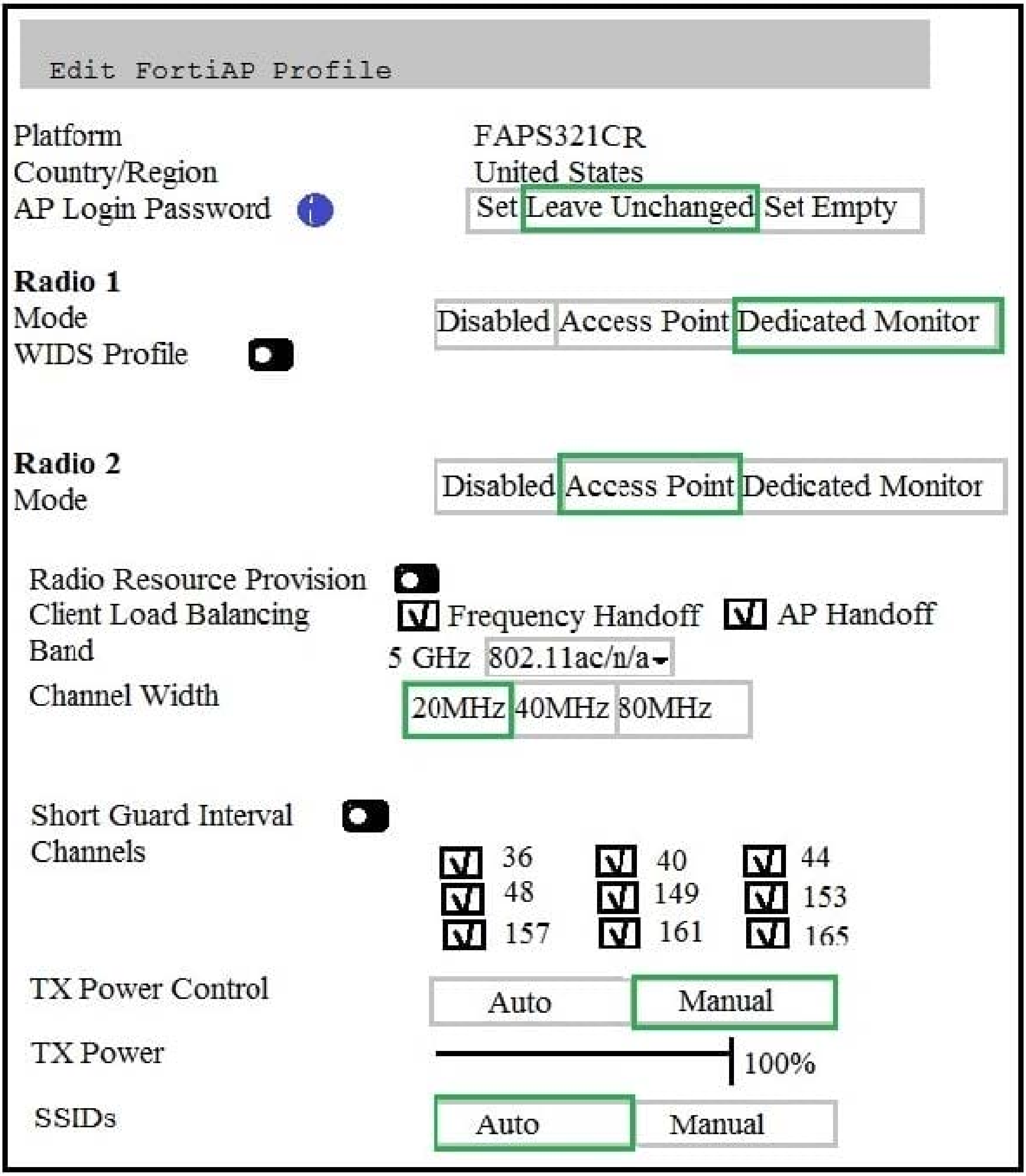
Following Questions and Answers are all new published by Fortinet Official Exam Center

QUESTION 1

Click the Exhibit button.

The FortiAP profile used by the FortiGate managed AP is shown in the exhibit.

Which two statements are correct in this scenario? (Choose two.)



Edit FortiAP Profile

Platform FAPS321CR
Country/Region United States
AP Login Password Set [✓ Leave Unchanged] Set Empty

Radio 1
Mode Disabled Access Point [✓ Dedicated Monitor]
WIDS Profile ●

Radio 2
Mode Disabled [✓ Access Point] Dedicated Monitor

Radio Resource Provision ●
Client Load Balancing ☑ Frequency Handoff ☑ AP Handoff
Band 5 GHz 802.11ac/n/a
Channel Width [✓ 20MHz] 40MHz 80MHz

Short Guard Interval ●
Channels
☑ 36 ☑ 40 ☑ 44
☑ 48 ☑ 149 ☑ 153
☑ 157 ☑ 161 ☑ 165

TX Power Control Auto [✓ Manual]
TX Power 100%
SSIDs [✓ Auto] Manual

A. All FortiAPs using thre profile will nave Radio 1 scan rogue access points.

B. Map this profile to SSlDs that you want to be available on the FortiAPs using this profile.

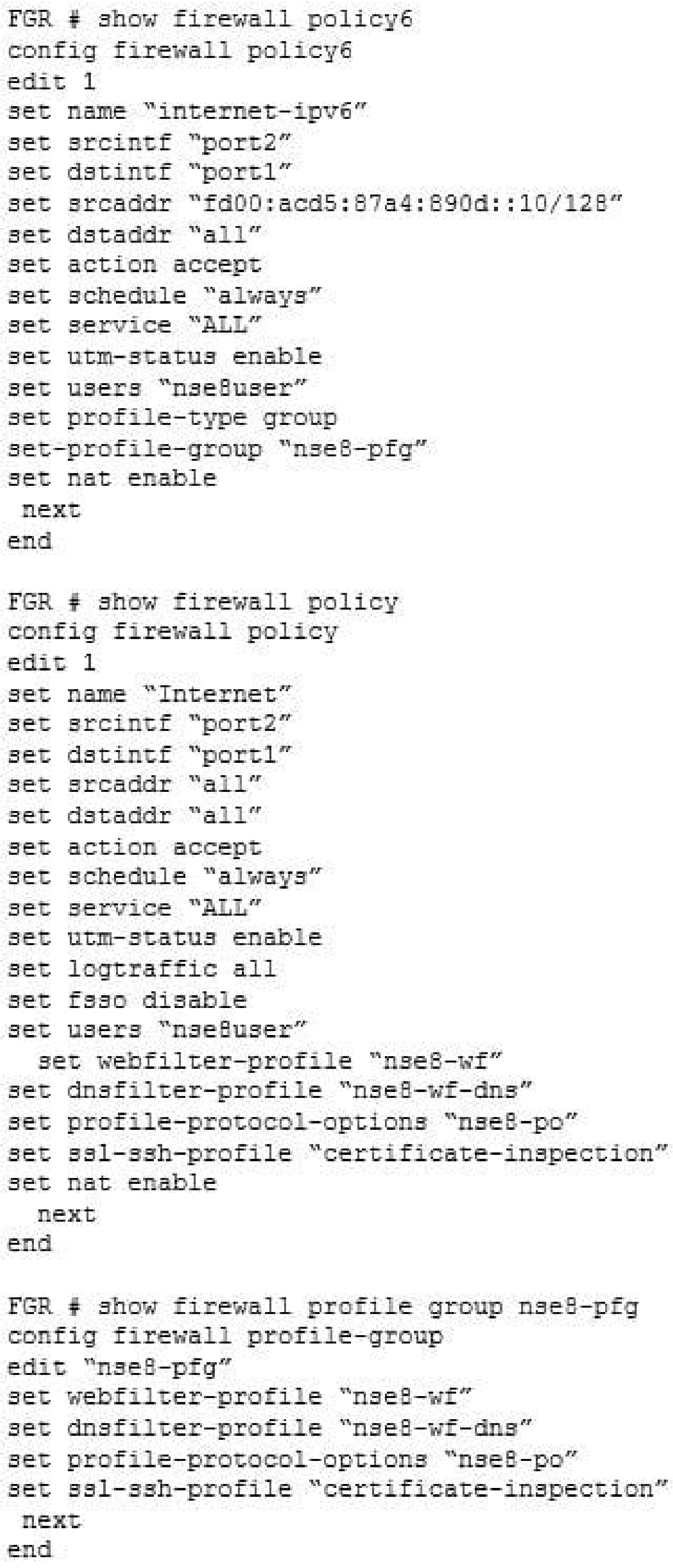
C. All FortiAPs using this profile will have Radio 1 monitor wireless clients.

D. Interference will be prevented between FortiAPs using this profile.

Correct Answer: AD

QUESTION 2

Click the Exhibit button. Referring to the exhibit, which two statements are true? (Choose two.)



```
FGR # show firewall policy6
config firewall policy6
edit 1
set name “internet-ipv6”
set srcintf “port2”
set dstintf “port1”
set srcaddr “fd00:acd5:87a4:890d::10/128”
set dstaddr “all”
set action accept
set schedule “always”
set service “ALL”
set utm-status enable
set users “nse8user”
set profile-type group
set-profile-group “nse8-pfg”
set nat enable
 next
end

FGR # show firewall policy
config firewall policy
edit 1
set name “Internet”
set srcintf “port2”
set dstintf “port1”
set srcaddr “all”
set dstaddr “all”
set action accept
set schedule “always”
set service “ALL”
set utm-status enable
set logtraffic all
set fsso disable
set users “nse8user”
  set webfilter-profile “nse8-wf”
set dnsfilter-profile “nse8-wf-dns”
set profile-protocol-options “nse8-po”
set ssl-ssh-profile “certificate-inspection”
set nat enable
  next
end

FGR # show firewall profile group nse8-pfg
config firewall profile-group
edit “nse8-pfg”
set webfilter-profile “nse8-wf”
set dnsfilter-profile “nse8-wf-dns”
set profile-protocol-options “nse8-po”
set ssl-ssh-profile “certificate-inspection”
 next
end
```

A. The IPv4 traffic for nse8user is filtered using the DNS profile.

B. The IPv6 traffic for nse8user is filtered using the DNS profile.

C. The IPv4 policy is allowing security profile groups.

D. The Web traffic for nse8user is being filtered differently in IPv4 and IPv6.

Correct Answer: AD

QUESTION 3

A FortOS devices is used for termination of VPNs for number of remote spoke VPN units (designated group A spokes) using a phase 1 main mode dial-up tunnel using pre-shared. Your company recently acquired another organization. You are asked establish VPN correctively for the newly acquired organization\\'s sites which new devices will be provisioned (designated Group B spokes). Both exiting (Group A) and new (Group B) spoke units are dynamically addressed. You are asked to ensure that spokes from the acquired organization (Group B) have different access permission than your

existing VPN spokes (Group A).

Which two solutions meet the represents for the new spoke group? (Choose two.)

A. implements a new phase 1 dial-up mode tunnel with preshared keys and XAuth. Use identity to filter traffic.

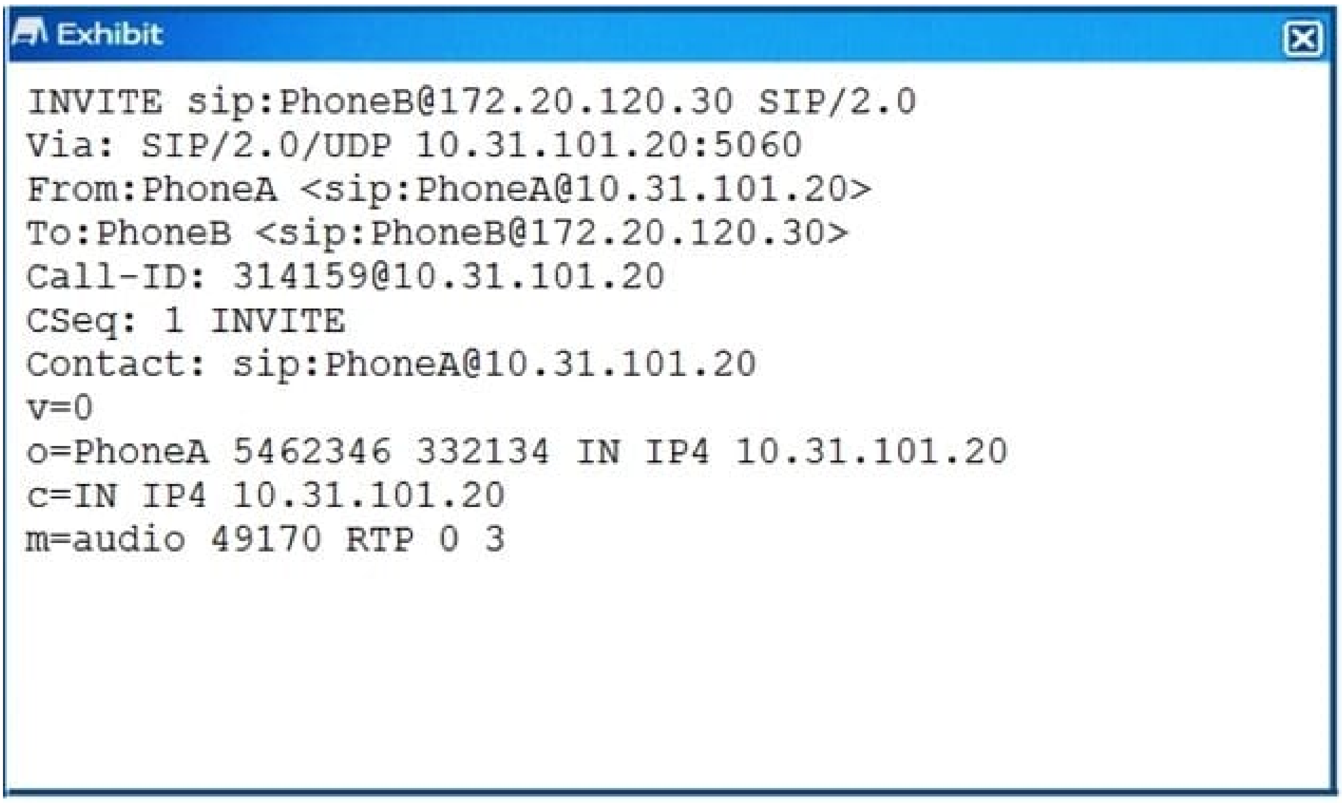
B. Implement a new phase 1 dial-up main mode tunnel with a different pre-shared key than the Group A spokes. Use standard policies to filter for the new dial-up tunnel

C. Implement a new phase 1 dial-up main mode tunnel with certificate authentication. Use standard policies to filter for the dial-up tunnel.

D. Implement separate phase 1 dial-up aggressive mode tunnels with a distinct peer ID. Use standard policies to filter traffic for the new dial-up tunnel.

Correct Answer: AB

QUESTION 4



```
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 form 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 49l70 and 49171.

C. The phone A IP address will be translated lo 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 5

You are asked to implement a single FortiGate 5000 chassis using Session-aware Load Balance Cluster (SLBC) with Active ?Passive FortinControllers. Both FortiControllers have the configuration shown below, with the rest of the configuration set to the default values:

onfig system ha

set mode dual

set password fortinetnse8

set group-id 5

set chassis-id 1

set minimize-chassis-failover enable

set hbdev "b1"

end

Both FortiControllers show Master status. What is the problem in this scenario?

A. The management interface of both FotiControllers was connected on the some network.

B. The priority should be set higher for ForControllers on slot-1.

C. The b1 interface the two FortiConrollers do not see each other.

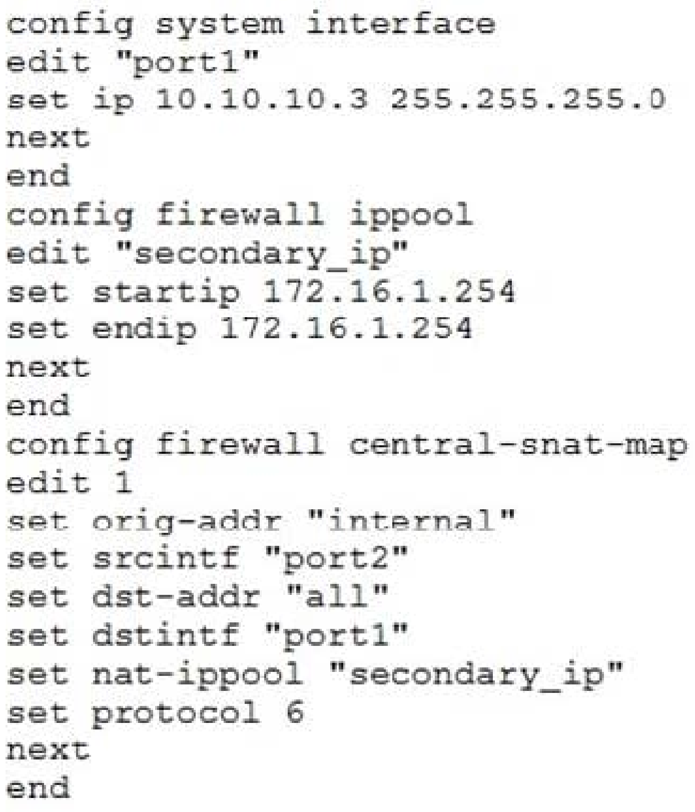
D. The chassis ID settings on FotiControllers on slot 2 should be set to 2.

Correct Answer: B

QUESTION 6

Click the Exhibit button.

Central NAT was configured on a FortiGate firewall. A sniffer shows ICMP packets out to a host on the Internet egresses with the port1 IP address instead of the virtual IP(VIP) that was configured. Referring to the exhibit, which configuration will ensure that ICMP traffic is also translated?



```
config system interface
edit "port1"
set ip 10.10.10.3 255.255.255.0
next
end
config firewall ippool
edit "secondary_ip"
set startip 172.16.1.254
set endip 172.16.1.254
next
end
config firewall central-snat-map
edit 1
set orig-addr "internal"
set srcintf "port2"
set dst-addr "all"
set dstintf "port1"
set nat-ippool "secondary_ip"
set protocol 6
next
end
```

A. config firewall ippool edit "secondry_ip" set arp-intf `port1\\' next end

B. config firewall central-snat-map edit 1 set protocol 1 next end

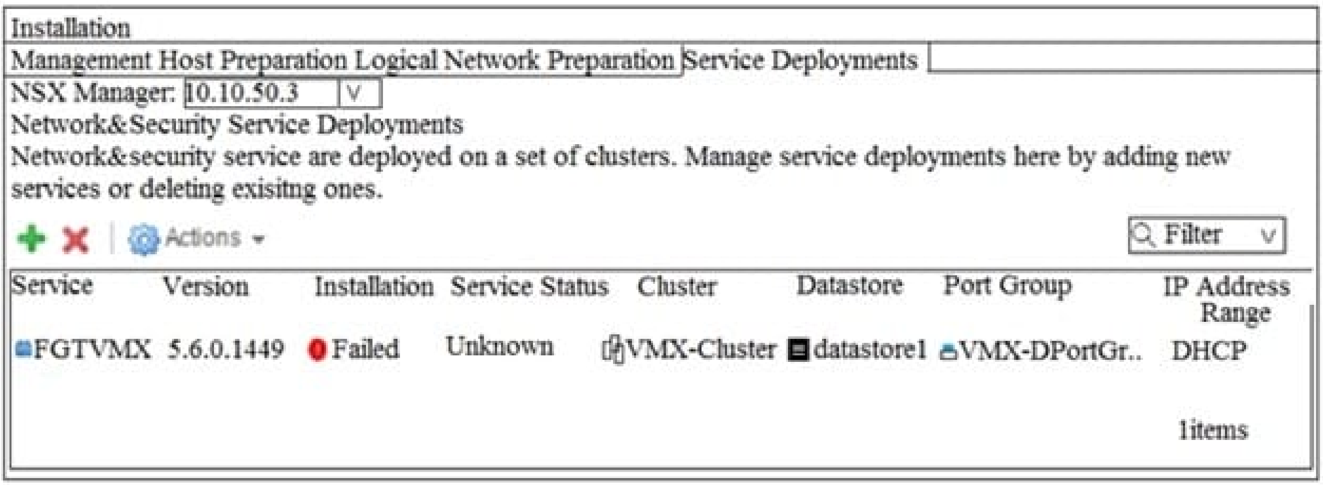
C. config firewall central-snat-map edit 1 unset protocol next end

D. config firewall central-snat-map edit 1 set orig-addr "all" next end

Correct Answer: B

QUESTION 7

Exhibit



Installation

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 exisitng ones.

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

1items

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 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 on the FortiGate Service Manager\\'s RestAPI service.

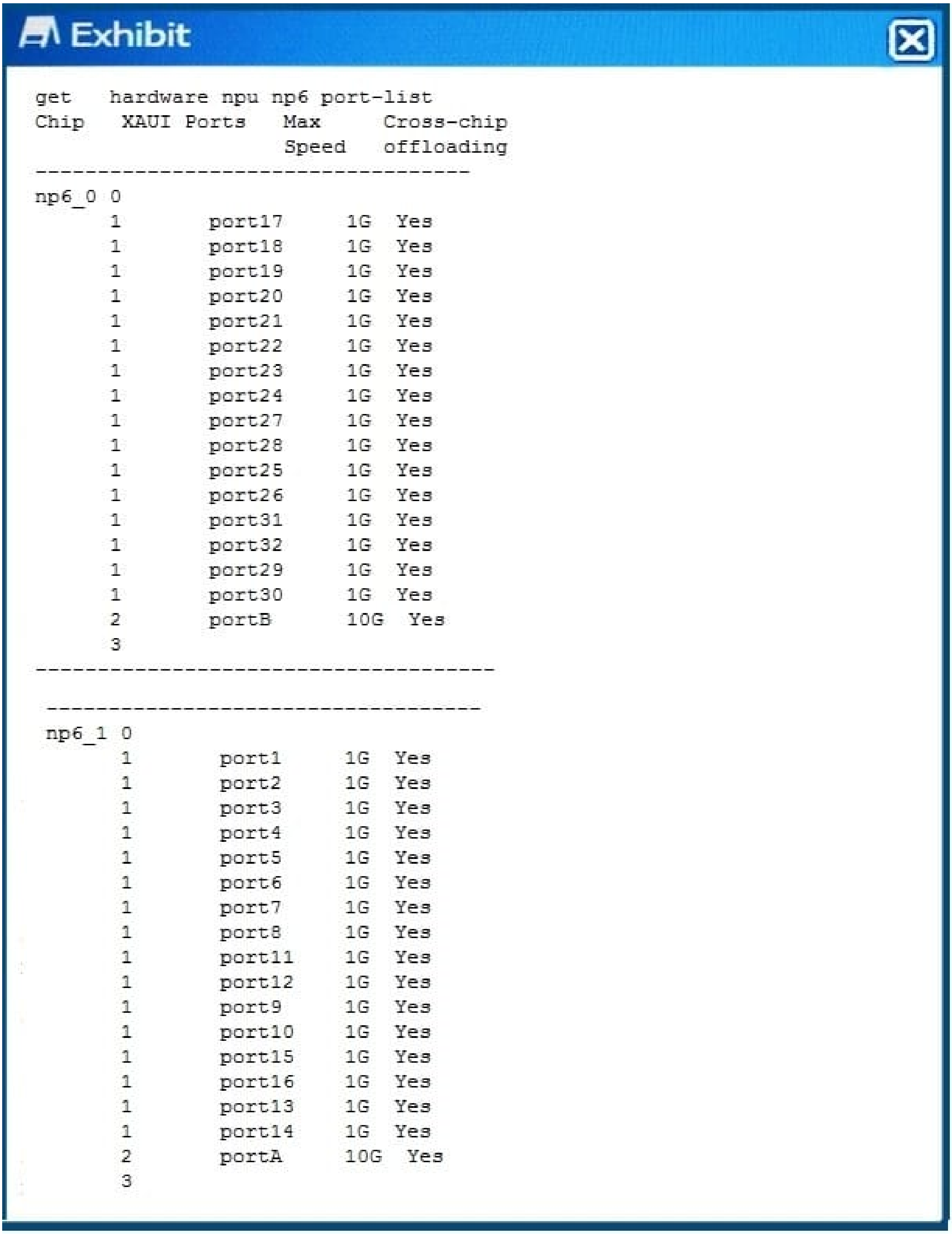
D. The FortiGate Service Manager did not have the proper permission to register the FortiGate-VMX Service.

Correct Answer: D

QUESTION 8

Exhibit Click the Exhibit button. You are trying to configure Link-Aggregation Group (LAG), but ports A and B do not appear on the list of

member options. Referring to the exhibit, which statement is correct in this situation?



```
get   hardware npu np6 port-list
Chip   XAUI Ports    Max      Cross-chip
                     Speed    offloading
-----------------------------------
np6_0 0
      1       port17     1G   Yes
      1       port18     1G   Yes
      1       port19     1G   Yes
      1       port20     1G   Yes
      1       port21     1G   Yes
      1       port22     1G   Yes
      1       port23     1G   Yes
      1       port24     1G   Yes
      1       port27     1G   Yes
      1       port28     1G   Yes
      1       port25     1G   Yes
      1       port26     1G   Yes
      1       port31     1G   Yes
      1       port32     1G   Yes
      1       port29     1G   Yes
      1       port30     1G   Yes
      2       portB      10G   Yes
      3
-------------------------------------

 -----------------------------------
 np6_1 0
       1       port1      1G   Yes
       1       port2      1G   Yes
       1       port3      1G   Yes
       1       port4      1G   Yes
       1       port5      1G   Yes
       1       port6      1G   Yes
       1       port7      1G   Yes
       1       port8      1G   Yes
       1       port11     1G   Yes
       1       port12     1G   Yes
       1       port9      1G   Yes
       1       port10     1G   Yes
       1       port15     1G   Yes
       1       port16     1G   Yes
       1       port13     1G   Yes
       1       port14     1G   Yes
       2       portA      10G   Yes
       3
```

A. The FortiGate model being used does not support LAG.

B. The FortiGate model does not have an Integrated Switch Fabric (ISF).

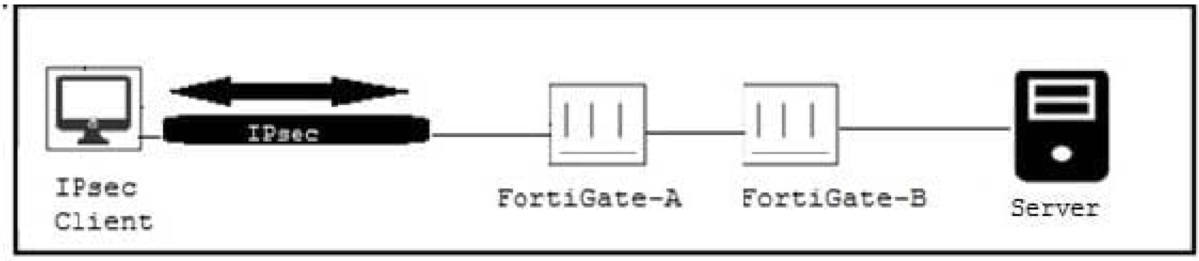
C. The FortiGate SFP+ slot does not have the correct module.

D. The FortiGate interfaces are defective and require replacement.

Correct Answer: B

QUESTION 9

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 ? to reach the server.

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

A. Use Kerberos authentication.

B. FortiGate-A must generate a RADUIS accounting packets.

C. Use FortiAuthenticator.

D. Use the Collector Agent.

Correct Answer: BC

QUESTION 10

You deploy a FortiGate device in a remote office based on the requirements shown below.

-- Due to company\\'s security policy, management IP of your FortiGate is not allowed to access the Internet.

-- Apply Web Filtering, Antivirus, IPS and Application control to the protected subnet. -- Be managed by a

central FortiManager in the head office.

Which action will help to achieve the requirements?

A. Configure a default route and make sure that the FortiGate device can pmg to service fortiguard net.

B. Configure the FortiGuard override server and use the IP address of the FortiManager

C. Configure the FortiGuard override server and use the IP address of service, fortiguard net.

D. Configure FortiGate to use FortiGuard Filtering Port 8888.

Correct Answer: B