

Exam Questions NSE8_810

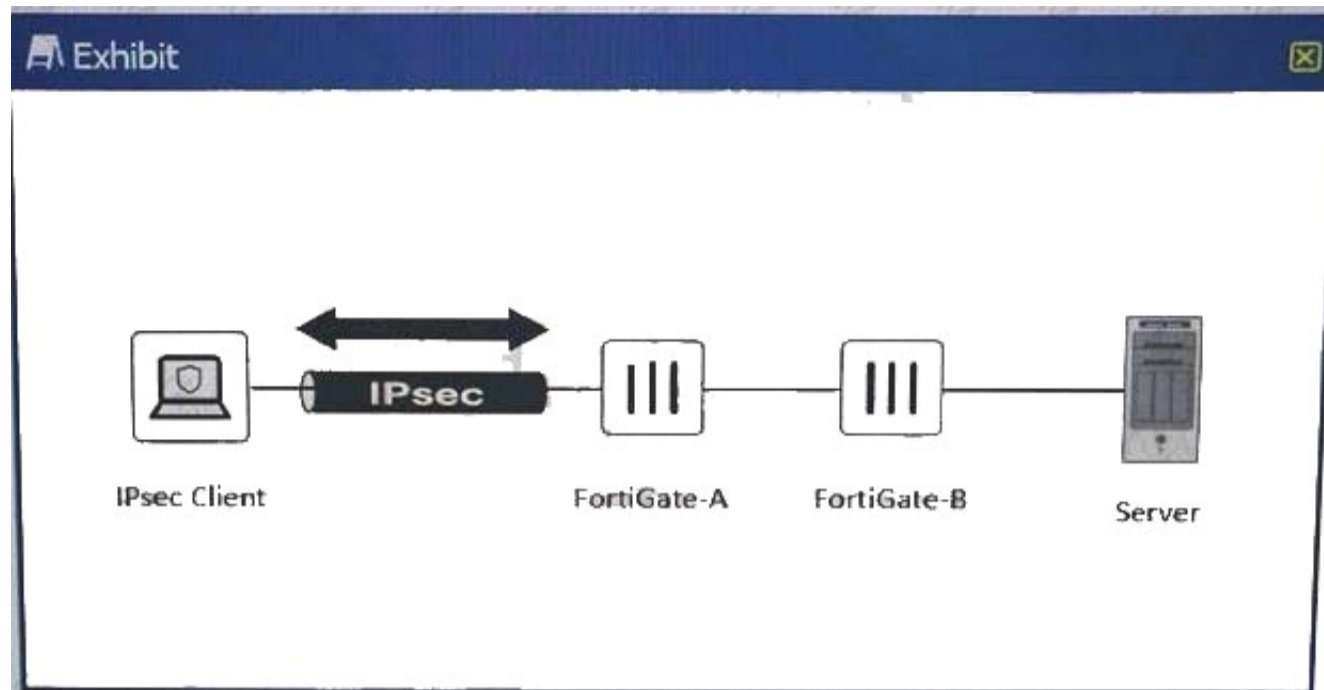
Fortinet Network Security Expert 8 Written Exam (810)

https://www.2passeasy.com/dumps/NSE8_810/



NEW QUESTION 1

Exhibit



Only users authenticated in FortiGate-B reach the server. A customer wants to deploy a single sign-on solution for VPN users. Once a user's 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 Agen

Answer: CD

NEW QUESTION 2

You have a customer experiencing problem with a legacy L3L4 firewall device and IPV6 SIP VoIP traffic. They devices is dropping SIP packets, consequently, it process SIP voice calls. Which solution would solve the customer's problem?

- A. Deploy a FortiVoice and enable IPv6 SIP.
- B. Replace their legacy device with a FortiGate and configure it to extract information from the body of the IPv6 packet.
- C. Deploy a FotiVoice and enable an IPv6 SIP session helper.
- D. Replace their legacy device with a FortiGate and deploy a FortiVoice to extract information from the body of the IPv6 SIP packet

Answer: A

NEW QUESTION 3

You configure an outgoing firewall policy with a web filter for accessing the internet. The access to URL [https:// itacm.co](https://itacm.co) and web belonging to the same category should be blocked. You notice that the Web server presents a certificate with CN=www acme.com. The www.it.acme site is as " information Technology and the www.acme.com site is categorized as "Business".

Which statements is correct in this scenario?

- A. Category "information Technology" needs to be blocked, the FortiGate is able to inspect the URL with HTTPS sessions.
- B. Category "Business" need a to be block: the certificate name takes precedence over the SNI.
- C. SSL inspection must be configured to deep-inspection: the category "information Technology "needs to be blocked.
- D. Category :information Technology" needs to be blocked, the SNI takes precedence over the certificate nam

Answer: A

NEW QUESTION 4

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

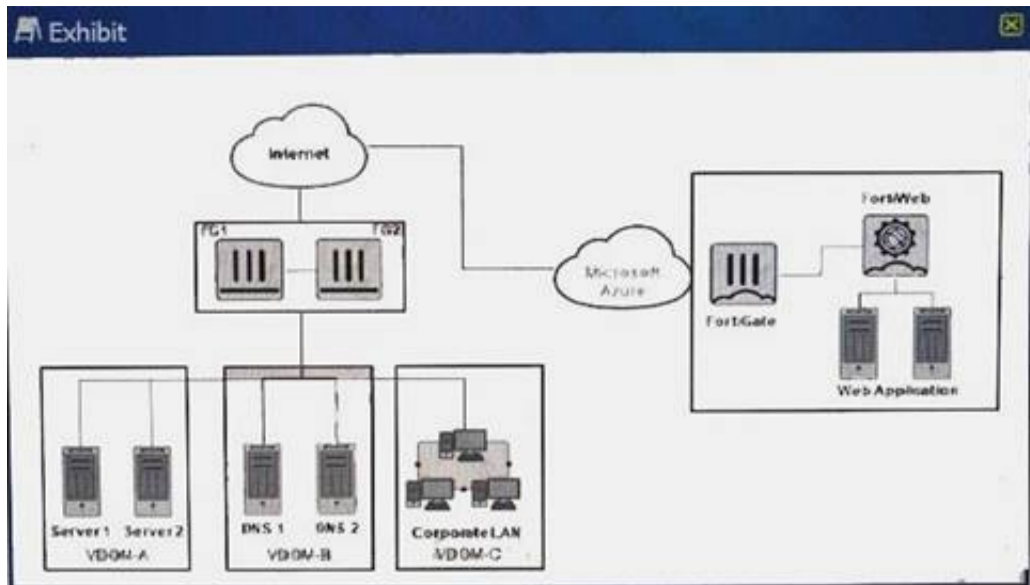
According to the exhibit, what is causing the problem?

- 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 are

Answer: A

NEW QUESTION 5

Exhibit



A customer has just finished their Azure deployment to ensure a Web application behind a FortiWeb. Now they want to add components to protect against advanced threats (zero day attacks), centrally manage the entire environment, and centrally monitor Fortinet and non-Fortinet products. Which Fortinet will stand by these requirements?

- A. Use FortiAnalyzer for monitoring in Azure, FortiSIEM for management, and FortiSandbox for zero day attacks on their local network.
- B. Use FortiAnalyzer for monitoring Azure, FortiSIEM for management, and FortiGate for zero day attacks on their local network.
- C. Use FortiManager for management in Azure, FortiSIEM for monitoring and FortiSandbox for zero day attacks on their local network.
- D. Use FortiSIEM for management Azure, FortiManager for management, and FortiGate for zero day attacks on their local network.

Answer: A

NEW QUESTION 6

Central NAT was configured on a FortiGate firewall to sniff ICMP packets out to a host on the internet egresses with the port IP address instead of the virtual IP (VIP) that was configured.

Referring to the exhibit, which configuration change ensures that ICMP traffic is also translated?

A)

```
config firewall ippool
  edit "secondary_ip"
    set arp-intf 'port1'
  next
end
```

B)

```
config firewall central-nat-map
  edit 1
    set protocol 1
  next
end
```

C)

```
config firewall central-nat-map
  edit 1
    unset protocol
  next
end
```

D)

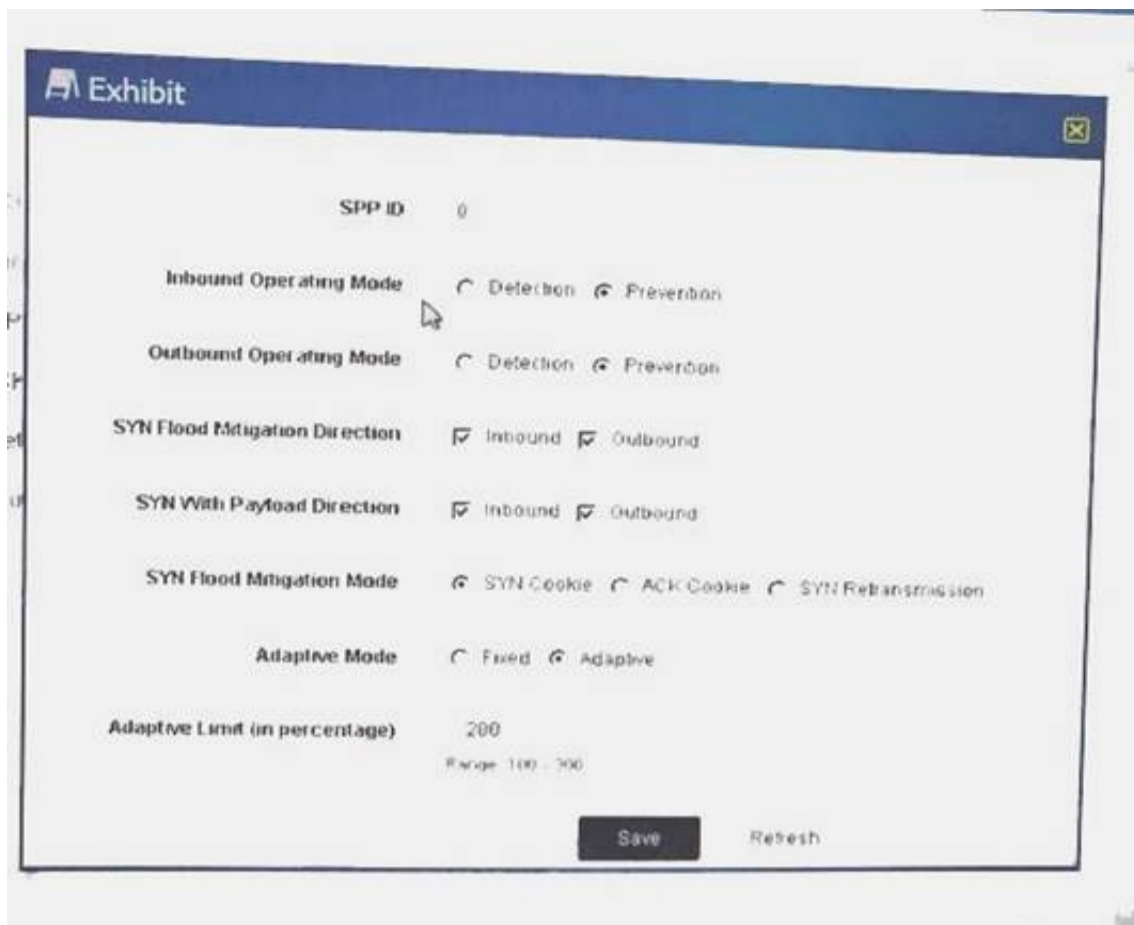
```
config firewall central-nat-map
  edit 1
    set orig-addr "all"
  next
end
```

- A. Option A
- B. Option B
- C. Option C
- D. Option D

Answer: C

NEW QUESTION 7

Exhibit



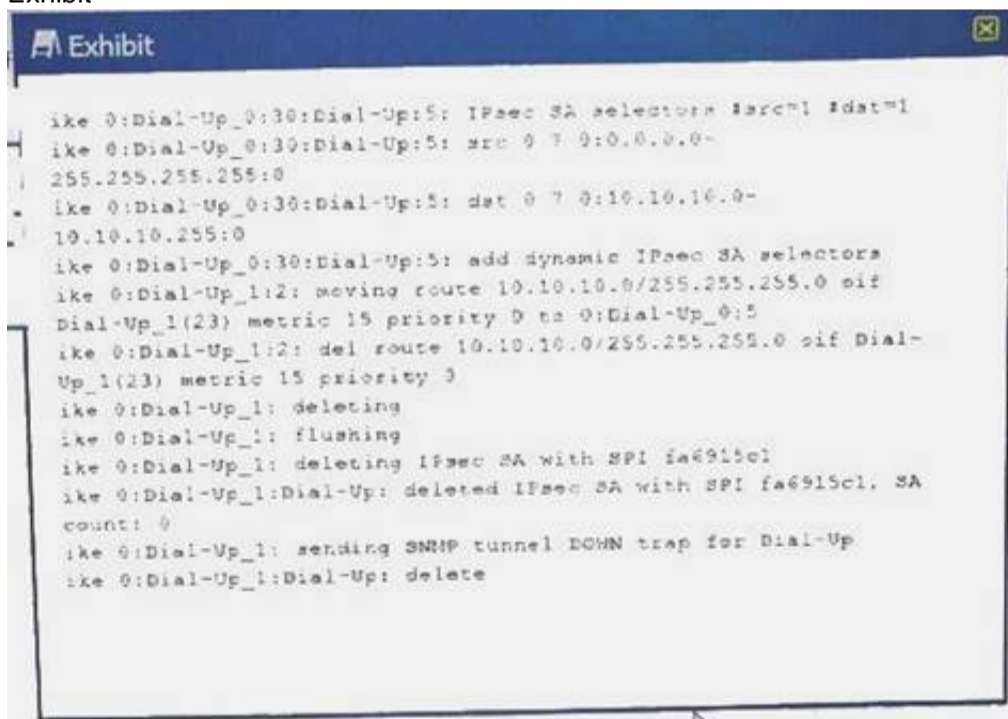
The exhibit shows the configuration of a service protection profile (SPP) in a FortiDDoS device. Which two statements are true about the traffic matching being inspection by this SPP? (Choose two.)

- 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 droope

Answer: AB

NEW QUESTION 8

Exhibit



A FortiGate configure for a dial IPsec VPN to allow multiple remote FortiGate to connect to it. However, FortiGate A and B have problems connecting to the VPN. Only one of them can be connected at a time. If site B tries to connect while site A is connected, site A disconnected. The IKE real time shows debug shoes the output in the exhibit when site A is disconnected.

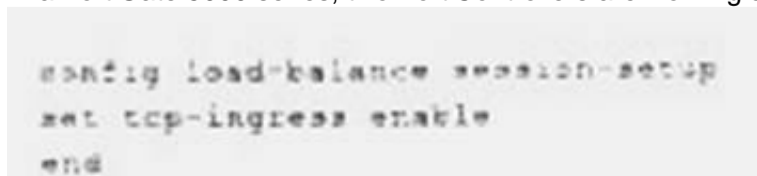
Which of the following setting should be excluded in the dial-up configuration to allow both to be VPNs to be connected at the same time?

- A. set enforce-unique-id disable
- B. set add-router enable
- C. set single-source disable
- D. set router-overlap allow

Answer: A

NEW QUESTION 9

In a FortiGate 5000 series, two FortiControllers are working as an SLBC cluster in a-p mode. The configuration shown below is applied.



When statement is true on how new TCP sessions are handled by the Distributor Processor (DP). The new session added the DP session table is automatically deleted, if the traffic is denied by the processing worker.

- A. No new session is added in the DP session table until the processing worker accepts the traffic.
- B. A new session added in the DP session table remains in the table until the traffic is denied by the processing worker.
- C. A new session added in the OP session table remains in the table only if traffic is accepted by the processing worker.

Answer: C

NEW QUESTION 10

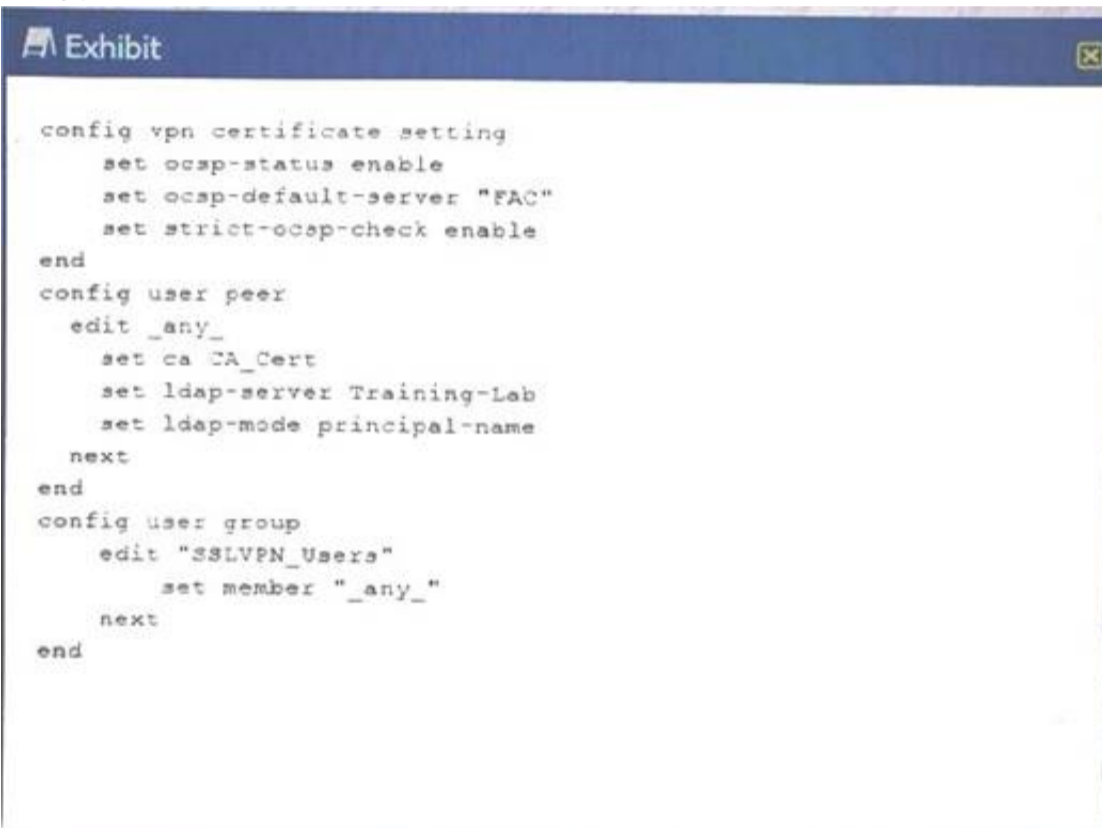
Exhibit
A VPN IPsec is connecting the headquarters office (HQ) with a branch office. OSPF is used to route between the offices. After deployment, a server with IP address 10.10.10.35 located on the DMZ network of the BO FortiGate was reported unreachable from hosts located on the LAN network of the same FortiGate. 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 of a 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.

Answer: A

NEW QUESTION 10

Exhibit



```

config vpn certificate setting
    set oosp-status enable
    set oosp-default-server "FAC"
    set strict-oosp-check enable
end
config user peer
    edit _any_
        set ca CA_Cert
        set ldap-server Training-Lab
        set ldap-mode principal-name
    next
end
config user group
    edit "SSLVPN_Users"
        set member "_any_"
    next
end

```

A FortiGate device is configured to authenticate SSL VPN users digital certificates. Part of the FortiGate configuration is shown in the exhibit. Which two statements are true in this scenario?

- A. The authentication will fail if the OCSP server is down.
- B. OCSP is used to verify that the user-signed certificate has not expired.
- C. The authentication will fail if the certificate does not contain user principle name (UPN) information.
- D. The authentication will fail if the user certificate does not contain the CA_Cert string in the Failure

Answer: A

NEW QUESTION 15

You are asked to implement a single FortiGate 5000 chassis using Session-aware Load Balance Cluster (SLBC) with Active-passive for Controllers. The configuration shown below, with the rest of the configuration set to the default values.

```

config system ha
    set mode dual
    set password fortinet123456
    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 FortiControllers was connected on the same network.
- B. The priority should be set higher for FortiControllers on slot-1.
- C. The b1 interface of the two FortiControllers do not see each other.
- D. The chassis ID settings on FortiControllers on slot 2 should be set to 2.

Answer: A

NEW QUESTION 19

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual NSE8_810 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the NSE8_810 Product From:

https://www.2passeasy.com/dumps/NSE8_810/

Money Back Guarantee

NSE8_810 Practice Exam Features:

- * NSE8_810 Questions and Answers Updated Frequently
- * NSE8_810 Practice Questions Verified by Expert Senior Certified Staff
- * NSE8_810 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * NSE8_810 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year