NSE8_811 Q&As

Fortinet NSE 8 Written Exam (NSE8_811)

Pass Fortinet NSE8_811 Exam with 100% Guarantee

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

https://www.passapply.com/nse8_811.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

Refer to the exhibit.

```
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 snif 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 172.16.1.70 -> 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
```

A VPN IPsec is connecting the headquarters office (HQ) with a branch office (BO). 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.

Referring to the exhibit, which statement is true?

A. The ICMP packets are being blocked by an implicit deny policy.

B. A directly connected subnet is being partially superseded by an OSPF redistributed subnet.

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

D. The incoming access list should have an accept action instead of a deny action to solve the problem.

Correct Answer: B

QUESTION 2

A company has just rolled out new remote sites and now you need to deploy a single firewall policy to all of these sites to allow Internet access using FortiManager. For this particular firewall policy, the source address object is called LAN, but its value will change according to the site the policy is being installed.

Which statement about creating the object LAN is correct?

A. Create a new object called LAN and enable per-device mapping.

B. Create a new object called LAN and promote it to the global database.

C. Create a new object called LAN and use it as a variable on a TCL script.

D. Create a new object called LAN and set meta-fields per remote site.

Correct Answer: A

QUESTION 3

You want to manage a FortiGate with the FortiCloud service. The FortiGate shows up in your list of 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 management tunnel mode on the managed FortiGate must be changed to normal.

B. The managed FortiGate is running a version of FortiOS that is either too new or too old for FortiCloud.

C. The managed FortiGate requires that a FortiCloud management license be purchased and applied.

D. You must manually configure system central-management on the FortiGate CLI and set the management type to fortiguard.

Correct Answer: D

QUESTION 4

You must create a High Availability deployment with two FortiWebs in Amazon Web 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 servers of both of the AZs.

Which deployment would fulfill this requirement?

A. Configure the FortiWebs in Active-Active HA mode and use AWS Elastic Load Balancer (ELB) for the internal Web servers.

B. Use AWS Elastic Load Balancer (ELB) for both the FortiWebs in standalone mode and the internal Web servers in an ELB sandwich.

C. Configure the FortiWebs in Active-Active HA mode and use AWS Route 53 to load balance the internal Web servers.

D. Use AWS Route 53 to load balance the FortiWebs in standalone mode and use AWS Virtual Private Cloud (VPC) Peering to load balance the internal Web servers.

Correct Answer: B

QUESTION 5

You configured a firewall policy with only a Web filter profile for accessing the Internet. Access to websites belonging to the "Information Technology" category are blocked and to the "Business" category are allowed. SSL deep inspection is not enabled on this policy.

A user wants to access the website https://www.it-acme.com which presents a certificate with CN=www.acme.com. The it-acme.com domain is categorized as "Information Technology" and the acme.com domain is categorized as "Business".

Which statement regarding this scenario is correct?

A. The FortiGate is able to read the URL within HTTPS sessions when using SSL certificate inspection so the website will be blocked by the "Information Technology".

B. The website will be blocked by category "Information Technology" as the SNI takes precedence over the certificate name.

C. The website will be allowed by category "Business" as the certificate name takes precedence over the URL.

D. Only with SSL deep inspection enabled will the FortiGate be able to categorized this website.

Correct Answer: B