NSE8_811$^{Q\&As}$

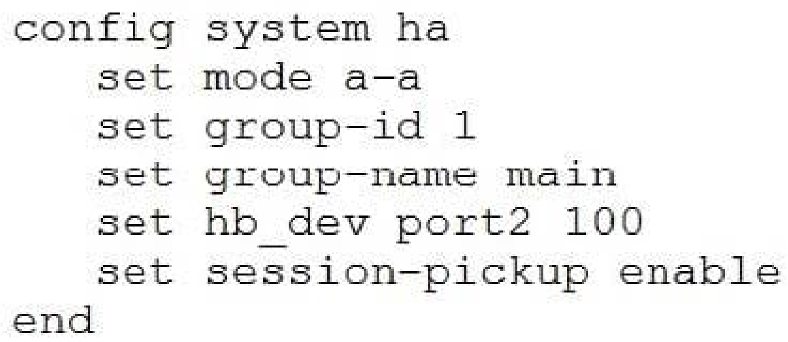
Fortinet NSE 8 Written Exam (NSE8_811)

Pass Fortinet NSE8_811 Exam with 100% Guarantee

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

QUESTION 1

You have configured an HA cluster with two FortiGate devices. You want to make sure that you are able to manage the individual cluster members directly using port3.



```
config system ha
    set mode a-a
    set group-id 1
    set group-name main
    set hb_dev port2 100
    set session-pickup enable
end
```

Referring to the configuration shown, in which two ways can you accomplish this task? (Choose two.)

A. Create a management VDOM and disable the HA synchronization for this VDOM, assign port3 to this VDOM, then configure specific IPs for port3 on both cluster members.

B. Configure port3 to be a dedicated HA management interface; then configure specific IPs for port3 on both cluster members.

C. Allow administrative access in the HA heartbeat interfaces.

D. Disable the sync feature on port3; then configure specific IPs for port3 on both cluster members.

Correct Answer: AB

QUESTION 2

A customer is experiencing problems with a legacy L3/L4 firewall device and the IPv6 SIP VoIP traffic. Their device is dropping SIP packets, consequently, it cannot process SIP voice calls.

Which solution will solve the customer\\'s problem?

A. Replace their legacy device with a FortiGate and deploy a FortiVoice to extract information from the body of the IPv6 SIP packet.

B. Deploy a FortiVoice and enable IPv6 SIP.

C. Deploy a FortiVoice and enable an IPv6 SIP session helper.

D. Replace their legacy device with a FortiGate and configure it to extract information from the body of the IPv6 SIP packet.

Correct Answer: A

QUESTION 3

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 4

You are asked to add a FortiDDoS to the network to combat detected slow connection attacks such as

Slowloris.

Which prevention mode on FortiDDoS will protect you against this specific type of attack?

A. asymmetric mode

B. aggressive aging mode

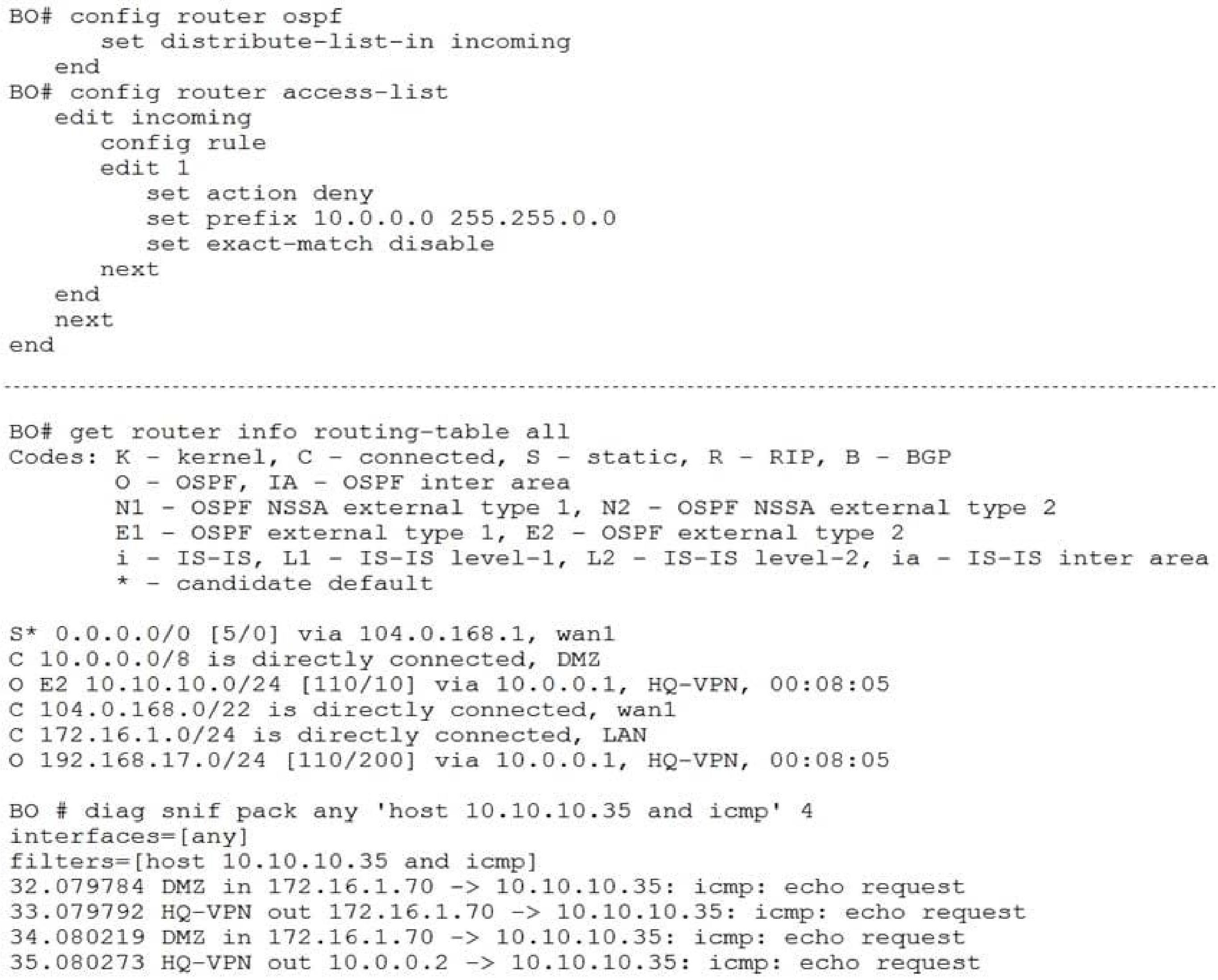
C. rate limiting mode

D. blocking mode

Correct Answer: B

QUESTION 5

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

NSE8_811 PDF Dumps NSE8_811 Study Guide NSE8_811 Braindumps