NSE8_811 Q&As

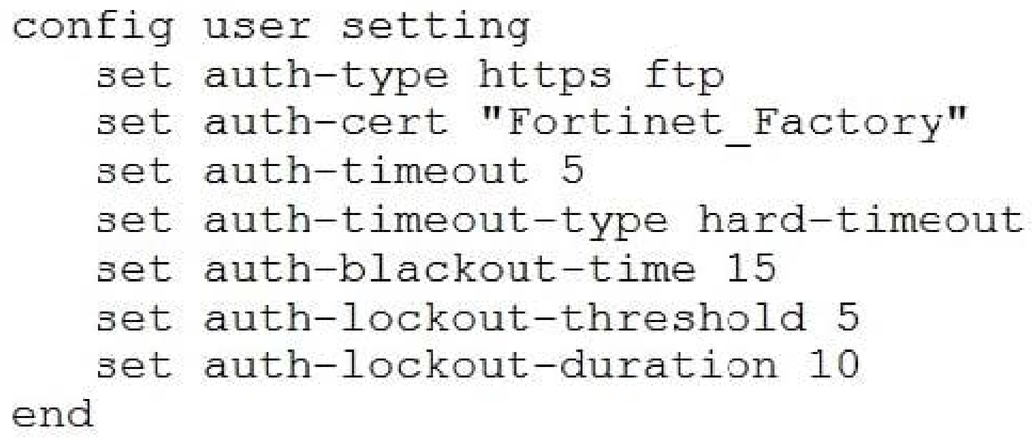
Fortinet NSE 8 Written Exam (NSE8_811)

Pass Fortinet NSE8_811 Exam with 100% Guarantee

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

QUESTION 1

Consider the following configuration setting:



```
config user setting
    set auth-type https ftp
    set auth-cert "Fortinet_Factory"
    set auth-timeout 5
    set auth-timeout-type hard-timeout
    set auth-blackout-time 15
    set auth-lockout-threshold 5
    set auth-lockout-duration 10
end
```

Which two statements about local authentication are true? (Choose two.)

A. The FortiGate will allow the TCP connection when a ClientHello message indicating a renegotiation is received.

B. The user\\'s IP address will be blocked 15 seconds after five login failures.

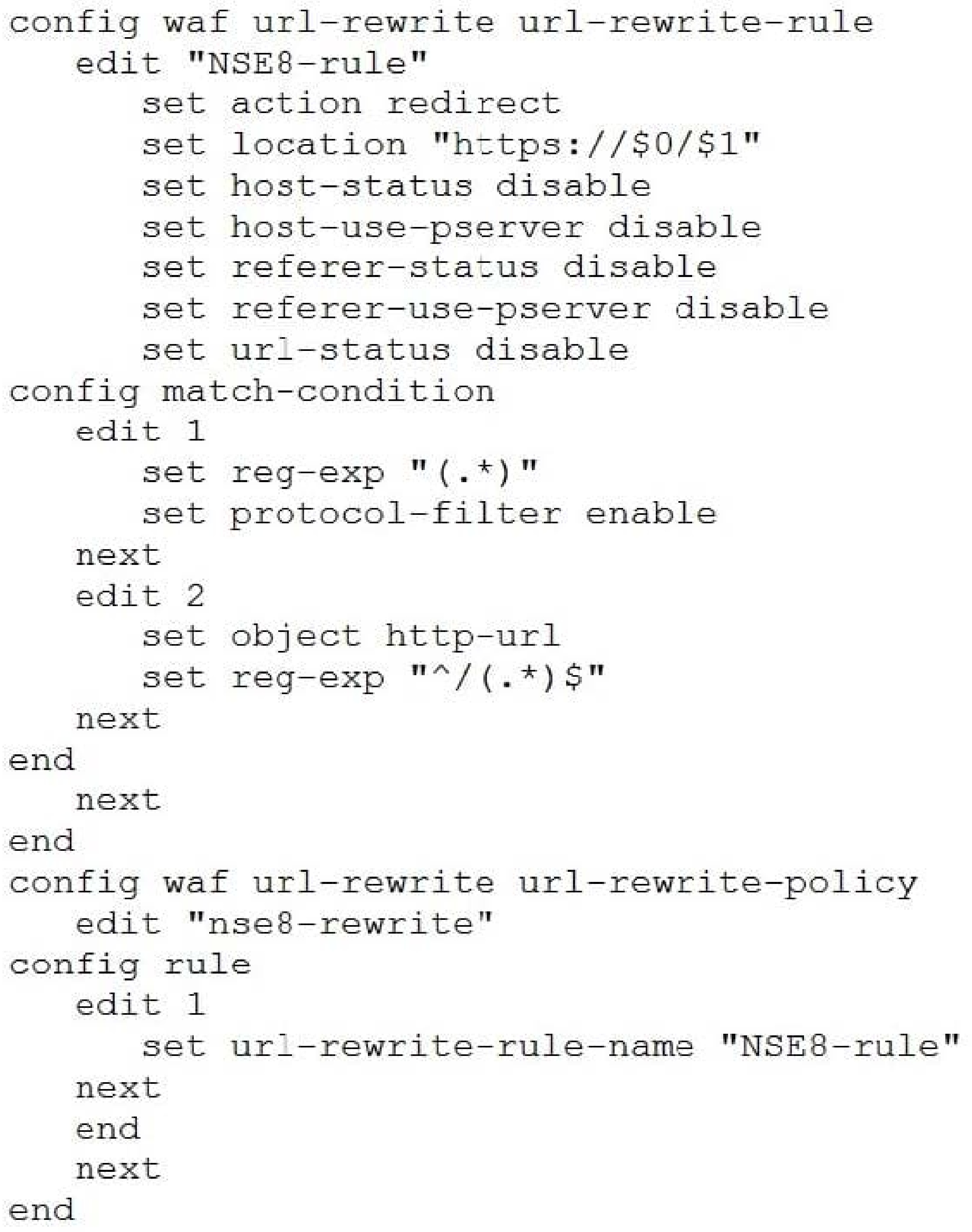
C. The user will be blocked 15 seconds after five login failures.

D. The user will need to re-authenticate after five minutes.

Correct Answer: BD

QUESTION 2

Refer to the exhibit.



```
config waf url-rewrite url-rewrite-rule
   edit "NSE8-rule"
      set action redirect
      set location "https://$0/$1"
      set host-status disable
      set host-use-pserver disable
      set referer-status disable
      set referer-use-pserver disable
      set url-status disable
config match-condition
   edit 1
      set reg-exp "(.*)"
      set protocol-filter enable
   next
   edit 2
      set object http-url
      set reg-exp "^/(.*)$"
   next
end
   next
end
config waf url-rewrite url-rewrite-policy
   edit "nse8-rewrite"
config rule
   edit 1
      set url-rewrite-rule-name "NSE8-rule"
   next
   end
   next
end
```

The exhibit shows the steps for creating a URL rewrite policy on a FortiWeb. Which statement represents the purpose of this policy?

A. The policy redirects all HTTPS URLs to HTTP.

B. The policy redirects all HTTP URLs to HTTPS.

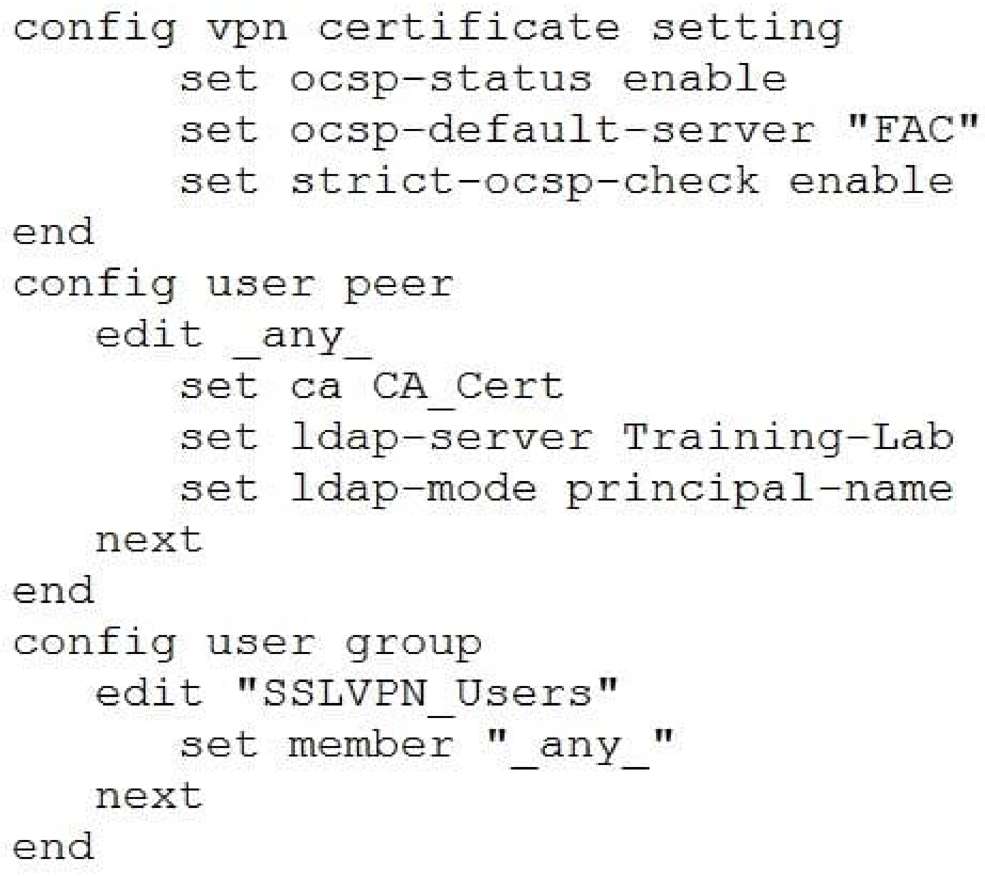
C. The policy redirects only HTTP URLs containing the ^/(.*)$ string to HTTPS.

D. The policy redirects only HTTPS URLs containing the ^/(.*)$ string to HTTP.

Correct Answer: B

QUESTION 3

Refer to the exhibit.



```
config vpn certificate setting
        set ocsp-status enable
        set ocsp-default-server "FAC"
        set strict-ocsp-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 using digital certificates. A partial FortiGate configuration is shown in the exhibit.

Referring to the exhibit, which two statements about this configuration are true? (Choose two.)

A. The authentication will fail if the user certificate does not contain the user principal name (UPN) information.

B. The authentication will fail if the user certificate does not contain the CA_Cert string in the CA field.

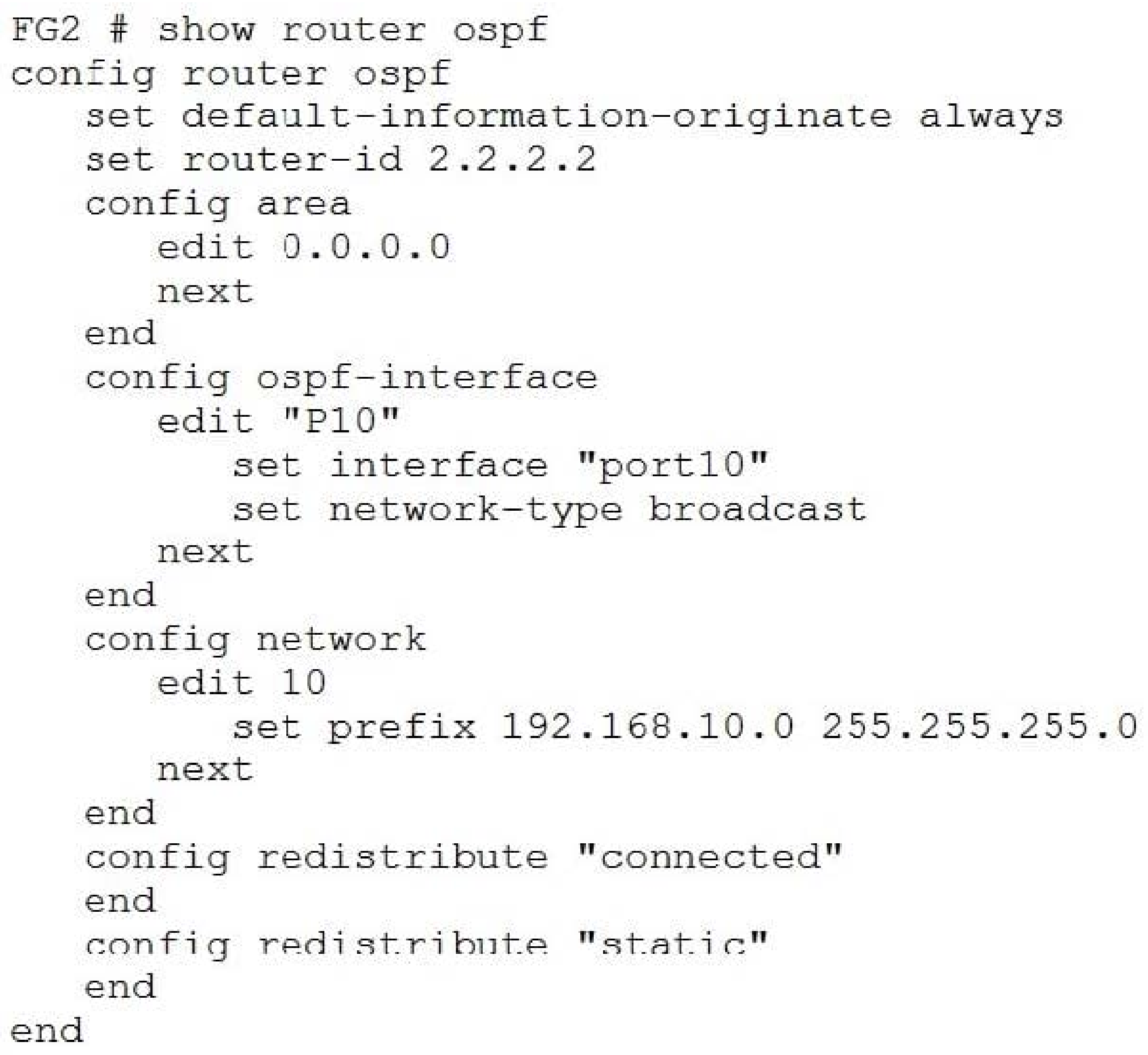
C. The authentication will fail if the OCSP server is down.

D. OCSP is used to verify that the user-signed certificate has not expired.

Correct Answer: AC

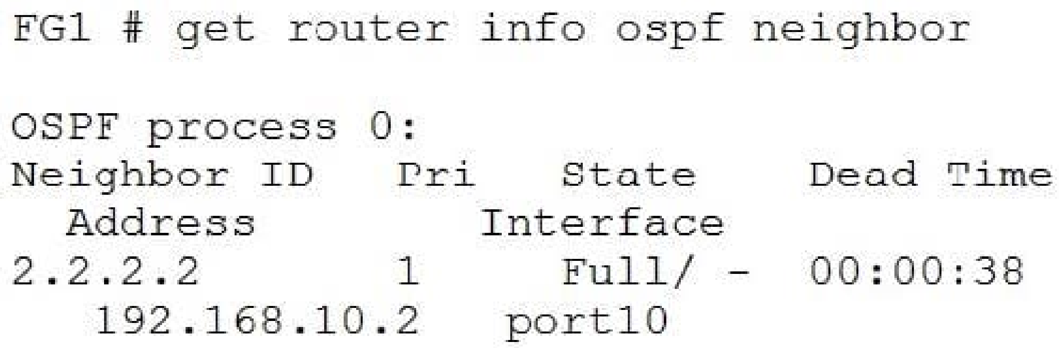
QUESTION 4

Refer to the exhibit.



```
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 customer is using dynamic routing to exchange the default route between two FortiGate devices 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?

A. FG2 is within the wrong OSPF area.

B. OSPF requires the redistribution of connected networks.

C. There is an OSPF interface network-type mismatch.

D. A prefix for the default route is missing.

Correct Answer: C

QUESTION 5

A customer wants to use a central RADIUS server for management authentication when connecting to the FortiGate GUI and to provide different levels of access for different types of employees.

Which three actions are required to provide the requested functionality? (Choose three.)

A. Create a wildcard administrator on the FortiGate.

B. Enable radius-vdom-override in the CLI.

C. Create multiple administrator profiles with matching RADIUS VSAs.

D. Enable accprofile-override in the CLI.

E. Set the RADIUS authentication type to MS-CHAPv2.

Correct Answer: ACD

QUESTION 6

You want to access the JSON API on FortiManager to retrieve information on an object. In this scenario, which two methods will satisfy the requirement? (Choose two.)

A. Download the WSDL file from FortiManager administration GUI.

B. Make a call with the curl utility on your workstation.

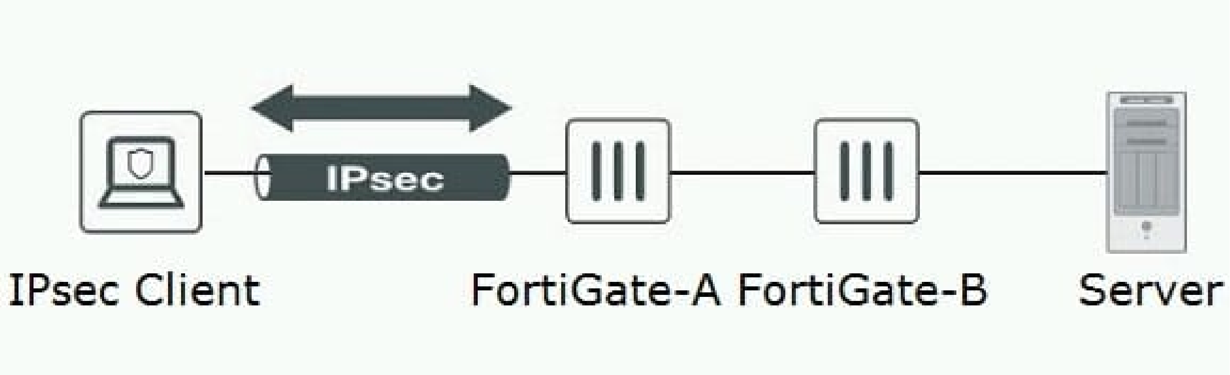
C. Make a call with the SoapUI API tool on your workstation.

D. Make a call with the Web browser on your workstation.

Correct Answer: AC

QUESTION 7

Refer to the exhibit.



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.

Referring to the exhibit, which two actions satisfy this requirement? (Choose two.)

A. Use Kerberos authentication.

B. Use the Collector Agent.

C. Use FortiAuthenticator.

D. FortiGate-A must generate a RADIUS accounting packet.

Correct Answer: CD

QUESTION 8

FortiMail is configured with the protected domain "internal.lab".

Which two envelope addresses will need an access control rule to relay e-mail sent for unauthenticated users? (Choose two.)

A. MAIL FROM: training@internal.lab; RCPT TO: student@internal.lab

B. MAIL FROM: student@internal.lab; RCPT TO: student@fortinet.com

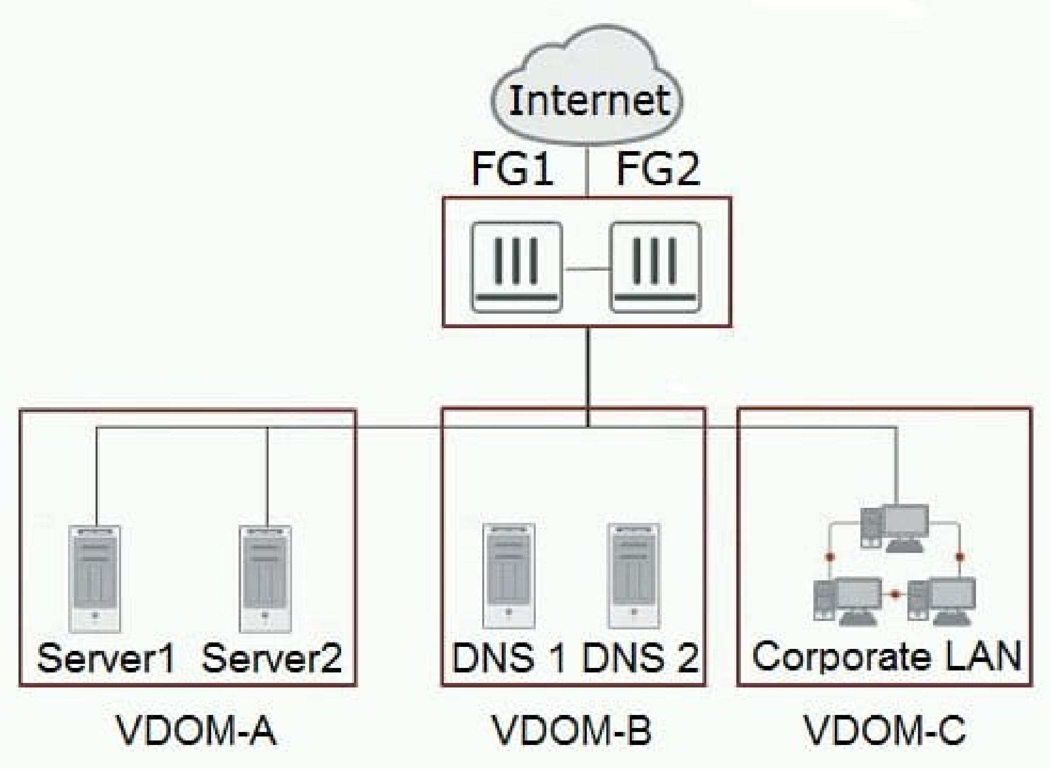
C. MAIL FROM: training@fortinet.com; RCPT TO: student@fortinet.com

D. MAIL FROM: student@fortinet.com; RCPT TO: student@internal.lab

Correct Answer: BC

QUESTION 9

Refer to the exhibit.



You need to apply the security features listed below to the network shown in the exhibit.

High grade DDoS protection Web security and load balancing for Server 1 and Server 2 Solution must be PCI DSS compliant Enhanced security to DNS 1 and DNS 2

What are three solutions for this scenario? (Choose three.)

A. FortiDDoS between FG1 and FG2 and the Internet

B. FortiADC for VDOM-A

C. FortiWeb for VDOM-A

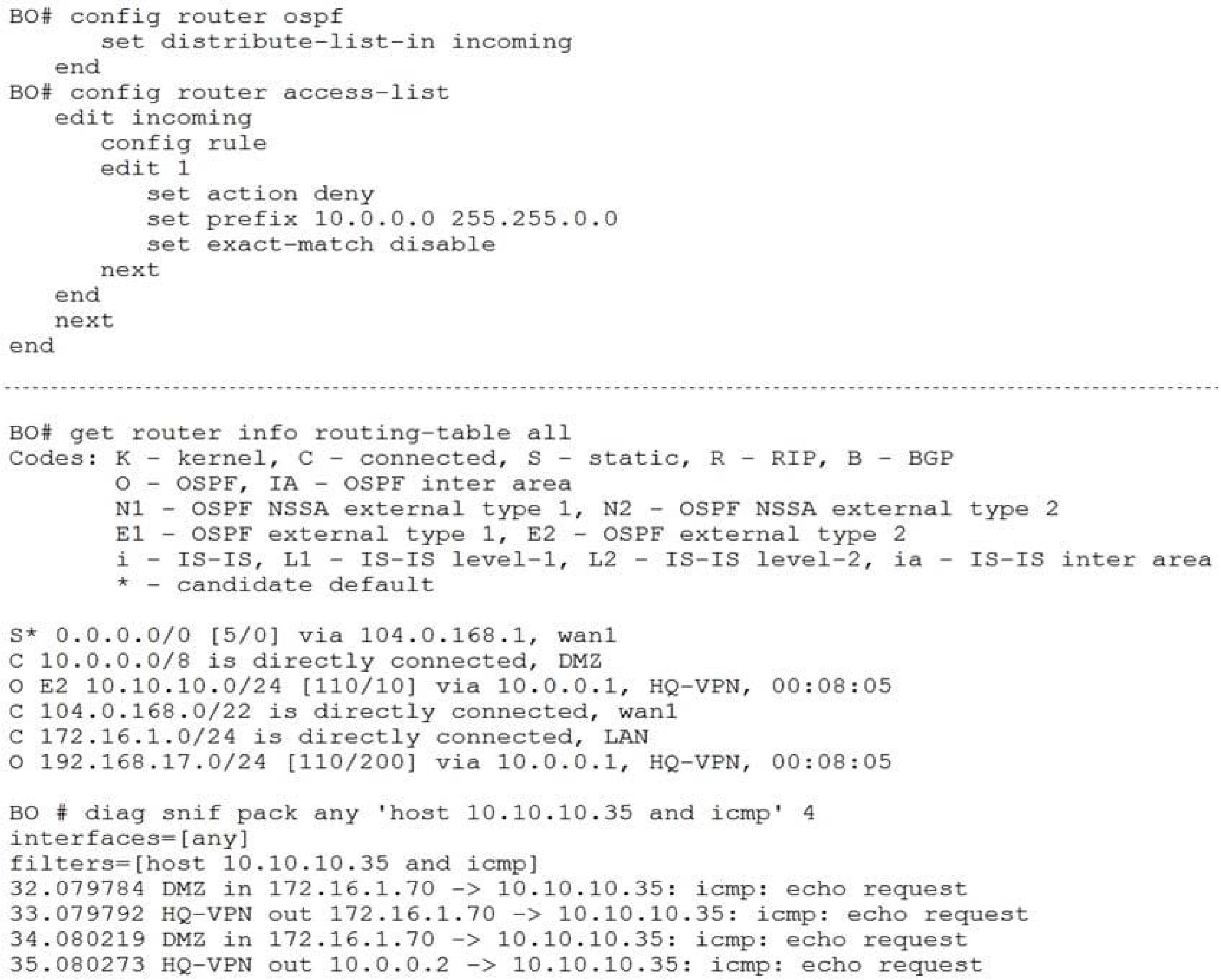
D. FortiADC for VDOM-B

E. FortiDDoS between FG1 and FG2 and VDOMs

Correct Answer: ACD

QUESTION 10

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