NSE8_812 Q&As

Network Security Expert 8 Written Exam

Pass Fortinet NSE8_812 Exam with 100% Guarantee

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

https://www.geekcert.com/nse8_812.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

Which two statements are correct on a FortiGate using the FortiGuard Outbreak Protection Service (VOS)? (Choose two.)

A. The FortiGuard VOS can be used only with proxy-base policy inspections.

B. If third-party AV database returns a match the scanned file is deemed to be malicious.

C. The antivirus database queries FortiGuard with the hash of a scanned file

D. The AV engine scan must be enabled to use the FortiGuard VOS feature

E. The hash signatures are obtained from the FortiGuard Global Threat Intelligence database.

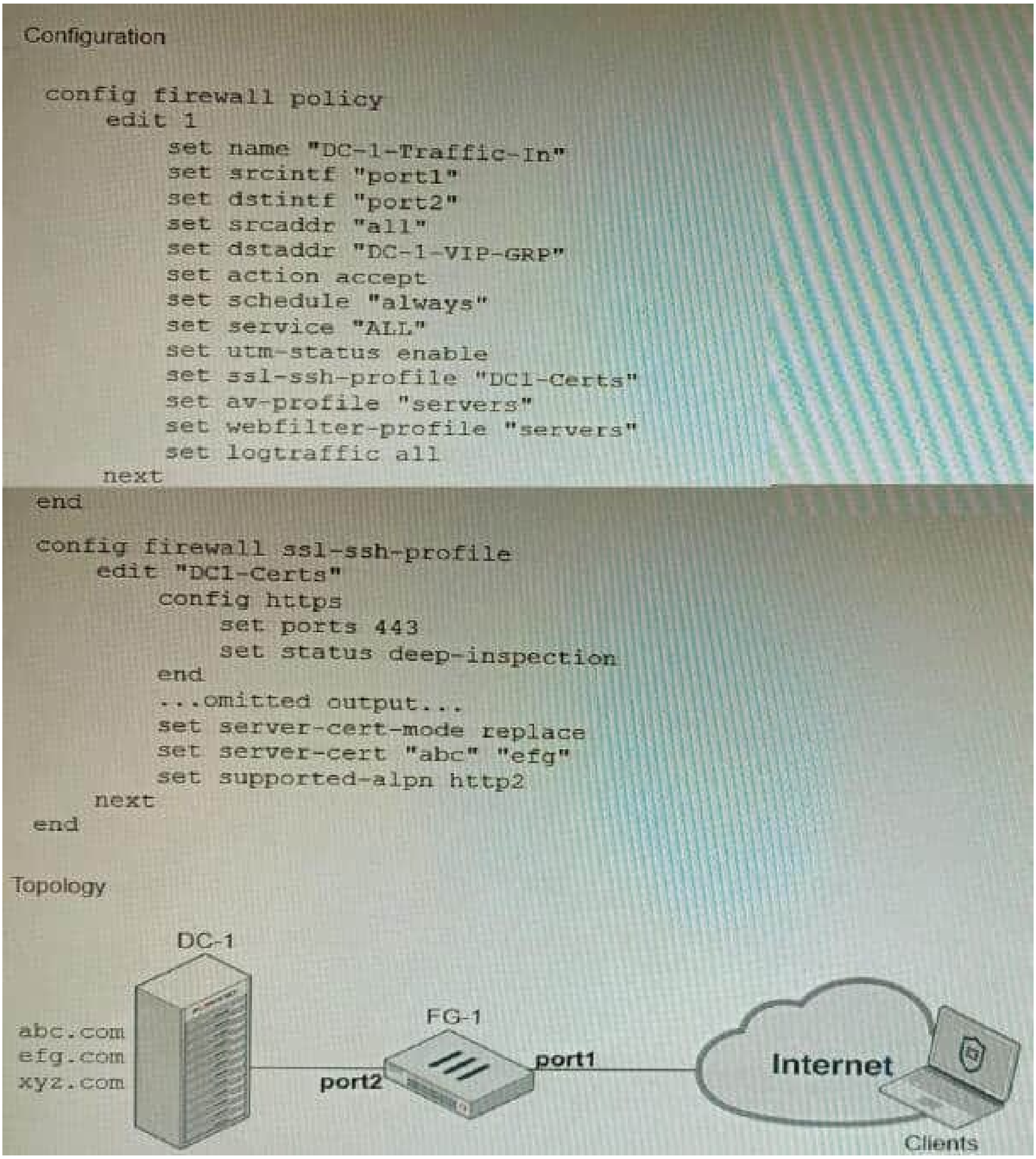
Correct Answer: CE

C. The antivirus database queries FortiGuard with the hash of a scanned file. This is how the FortiGuard VOS service works. The FortiGate queries FortiGuard with the hash of a scanned file, and FortiGuard returns a list of known malware signatures that match the hash.

E. The hash signatures are obtained from the FortiGuard Global Threat Intelligence database. This is where the FortiGuard VOS service gets its hash signatures from. The FortiGuard Global Threat Intelligence database is updated regularly with new malware signatures.

QUESTION 2

Refer to the exhibits, which show a firewall policy configuration and a network topology.



Configuration

```
config firewall policy
    edit 1
        set name "DC-1-Traffic-In"
        set srcintf "port1"
        set dstintf "port2"
        set srcaddr "all"
        set dstaddr "DC-1-VIP-GRP"
        set action accept
        set schedule "always"
        set service "ALL"
        set utm-status enable
        set ssl-ssh-profile "DC1-Certs"
        set av-profile "servers"
        set webfilter-profile "servers"
        set logtraffic all
    next
end

config firewall ssl-ssh-profile
    edit "DC1-Certs"
        config https
            set ports 443
            set status deep-inspection
        end
        ...omitted output...
        set server-cert-mode replace
        set server-cert "abc" "efg"
        set supported-alpn http2
    next
end
```

Topology

An administrator has configured an inbound SSL inspection profile on a FortiGate device (FG-1) that is protecting a data center hosting multiple web pages-Given the scenario shown in the exhibits, which certificate will FortiGate use to handle requests to xyz.com?

A. FortiGate will fall-back to the default Fortinet_CA_SSL certificate.

B. FortiGate will reject the connection since no certificate is defined.

C. FortiGate will use the Fortinet_CA_Untrusted certificate for the untrusted connection,

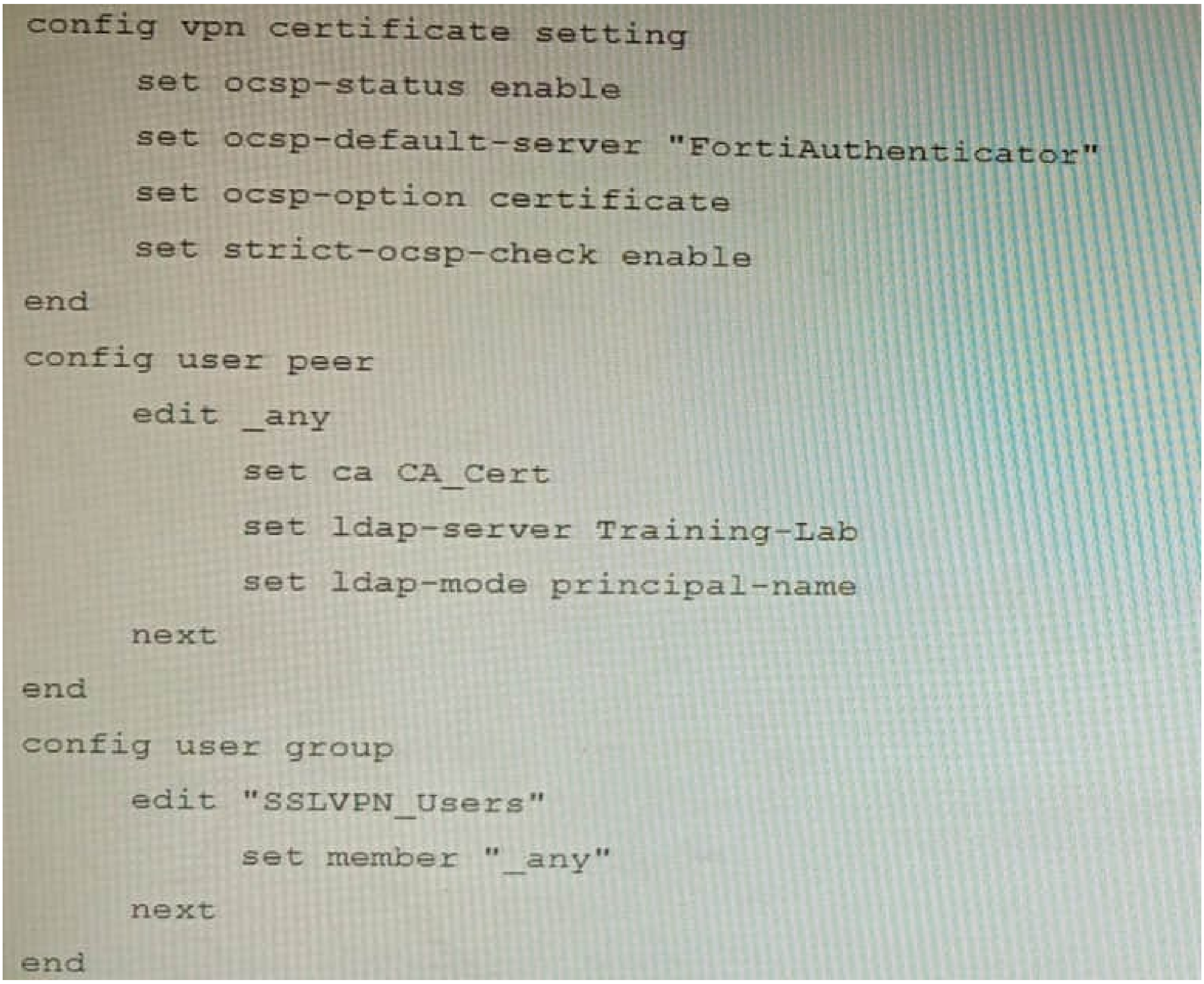
D. FortiGate will use the first certificate in the server-cert list--the abc.com certificate

Correct Answer: A

Explanation: When using inbound SSL inspection, FortiGate needs to present a certificate to the client that matches the requested domain name. If no matching certificate is found in the server-cert list, FortiGate will fall-back to the default Fortinet_CA_SSL certificate, which is self-signed and may trigger a warning on the client browser. References:https://docs.fortinet.com/document/fortigate/6.4.0/cookbook/103437/inbound- ssl-inspection

QUESTION 3

An administrator has configured a FortiGate device to authenticate SSL VPN users using digital certificates. A FortiAuthenticator is the certificate authority (CA) and the Online Certificate Status Protocol (OCSP) server. Part of the FortiGate configuration is shown below:



```
config vpn certificate setting
    set ocsp-status enable
    set ocsp-default-server "FortiAuthenticator"
    set ocsp-option certificate
    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
```

Based on this configuration, which two statements are true? (Choose two.)

A. OCSP checks will always go to the configured FortiAuthenticator

B. The OCSP check of the certificate can be combined with a certificate revocation list.

C. OCSP certificate responses are never cached by the FortiGate.

D. If the OCSP server is unreachable, authentication will succeed if the certificate matches the CA.

Correct Answer: BD

B is correct because the OCSP check of the certificate can be combined with a certificate revocation list (CRL). This means that the FortiGate will check the OCSP server to see if the certificate has been revoked, and it will also check the CRL to see if the certificate has been revoked. D is correct because if the OCSP server is unreachable, authentication will succeed if the certificate matches the CA. This is because the FortiGate will fall back to using the CRL if the OCSP server is unreachable. The other options are incorrect. Option A is incorrect because OCSP checks can go to other OCSP servers, not just the FortiAuthenticator. Option C is incorrect because OCSP certificate responses can be cached by the FortiGate. References: Configuring SSL VPN authentication using digital certificates | FortiGate / FortiOS 7.2.0 - Fortinet Document Library Online Certificate Status Protocol (OCSP) | FortiGate / FortiOS 7.2.0 - Fortinet Document Library Certificate Revocation Lists (CRLs) | FortiGate / FortiOS 7.2.0 - Fortinet Document Library

QUESTION 4

You are migrating the branches of a customer to FortiGate devices. They require independent routing tables on the LAN side of the network.

After reviewing the design, you notice the firewall will have many BGP sessions as you have two data centers (DC) and two ISPs per DC while each branch is using at least 10 internal segments.

Based on this scenario, what would you suggest as the more efficient solution, considering that in the future the number of internal segments, DCs or internet links per DC will increase?

A. No change in design is needed as even small FortiGate devices have a large memory capacity.

B. Acquire a FortiGate model with more capacity, considering the next 5 years growth.

C. Implement network-id, neighbor-group and increase the advertisement-interval

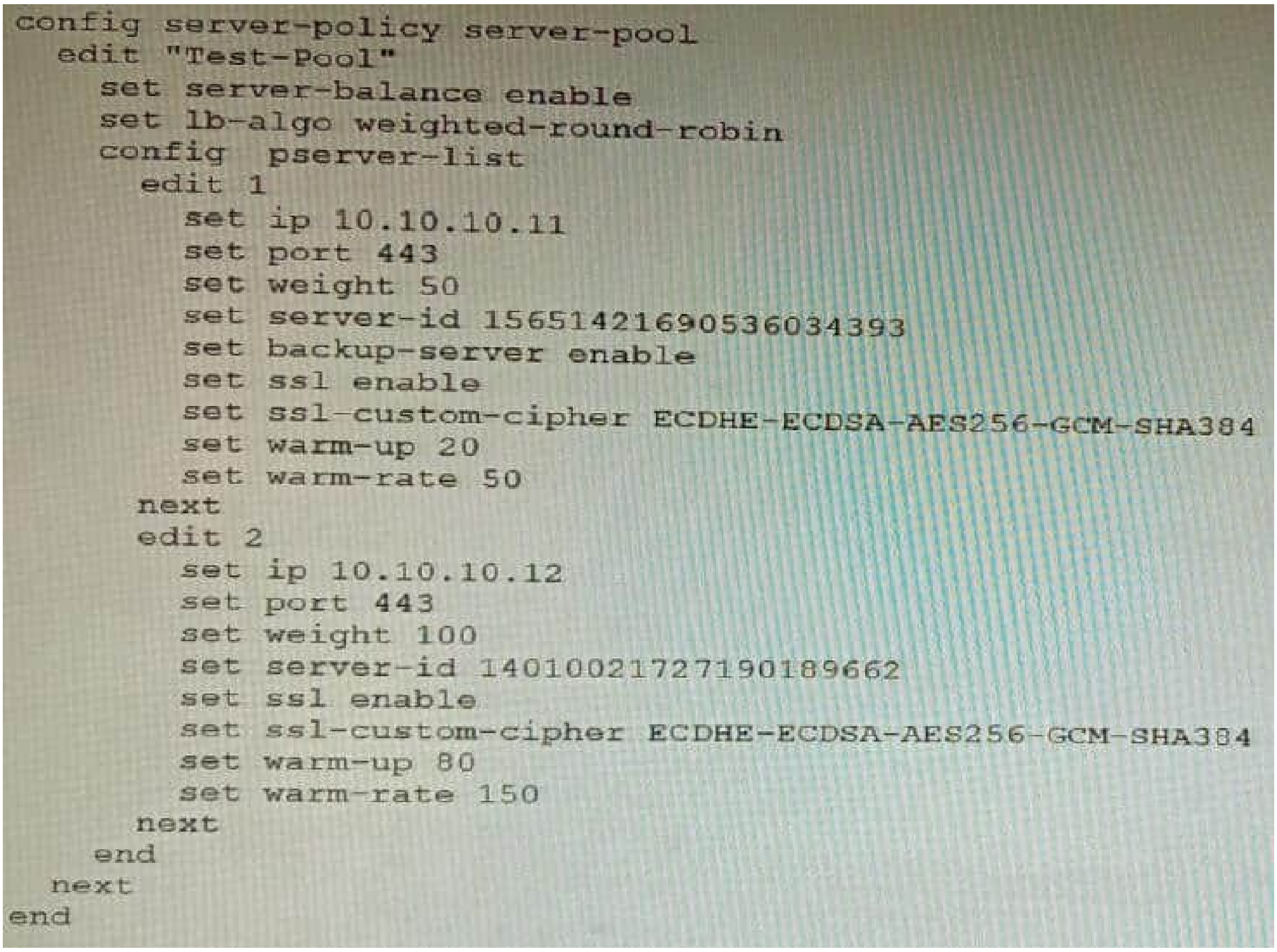
D. Redesign the SD-WAN deployment to only use a single VPN tunnel and segment traffic using VRFs on BGP

Correct Answer: D

Explanation: Using multiple VPN tunnels and BGP sessions for each internal segment is not scalable and efficient, especially when the number of segments, DCs or internet links per DC increases. A better solution is to use a single VPN tunnel per branch and segment traffic using virtual routing and forwarding (VRF) instances on BGP. This way, each VRF can have its own routing table and BGP session, while sharing the same VPN tunnel. References:https://docs.fortinet.com/document/fortigate/6.4.0/cookbook/103439/sd-wan- with-vrf-and-bgp

QUESTION 5

Refer to the exhibit.



```
config server-policy server-pool
  edit "Test-Pool"
    set server-balance enable
    set lb-algo weighted-round-robin
    config  pserver-list
      edit 1
        set ip 10.10.10.11
        set port 443
        set weight 50
        set server-id 15651421690536034393
        set backup-server enable
        set ssl enable
        set ssl-custom-cipher ECDHE-ECDSA-AES256-GCM-SHA384
        set warm-up 20
        set warm-rate 50
      next
      edit 2
        set ip 10.10.10.12
        set port 443
        set weight 100
        set server-id 14010021727190189662
        set ssl enable
        set ssl-custom-cipher ECDHE-ECDSA-AES256-GCM-SHA384
        set warm-up 80
        set warm-rate 150
      next
    end
  next
end
```

A FortiWeb appliance is configured for load balancing web sessions to internal web servers. The Server Pool is configured as shown in the exhibit.

How will the sessions be load balanced between server 1 and server 2 during normal operation?

A. Server 1 will receive 25% of the sessions, Server 2 will receive 75% of the sessions

B. Server 1 will receive 20% of the sessions, Server 2 will receive 66.6% of the sessions

C. Server 1 will receive 33.3% of the sessions, Server 2 will receive 66 6% of the sessions

D. Server 1 will receive 0% of the sessions Server 2 will receive 100% of the sessions

Correct Answer: A

Explanation: The Server Pool in the exhibit is configured with a weight of 20 for server 1 and a weight of 60 for server 2. This means that server 1 will receive 20% of the sessions and server 2 will receive 75% of the sessions.

The following formula is used to calculate the load balancing between servers in a Server Pool:

weight_of_server_1 / (weight_of_server_1 + weight_of_server_2) In this case, the formula is:

20 / (20 + 60) = 20 / 80 = 0.25 = 25%

Therefore, server 1 will receive 25% of the sessions and server 2 will receive 75% of the sessions.