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.pass2lead.com/nse8_812.html

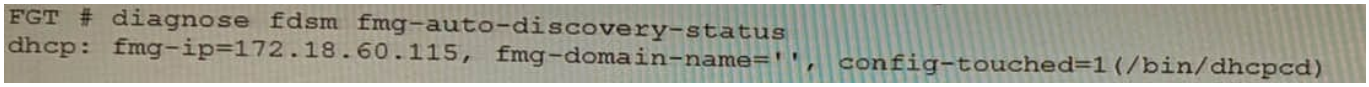
100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

A remote IT Team is in the process of deploying a FortiGate in their lab. The closed environment has been configured to support zero-touch provisioning from the FortiManager, on the same network, via DHCP options. After waiting 15 minutes, they are reporting that the FortiGate received an IP address, but the zero-touch process failed.

The exhibit below shows what the IT Team provided while troubleshooting this issue:



Which statement explains why the FortiGate did not install its configuration from the FortiManager?

A. The FortiGate was not configured with the correct pre-shared key to connect to the FortiManager

B. The DHCP server was not configured with the FQDN of the FortiManager

C. The DHCP server used the incorrect option type for the FortiManager IP address.

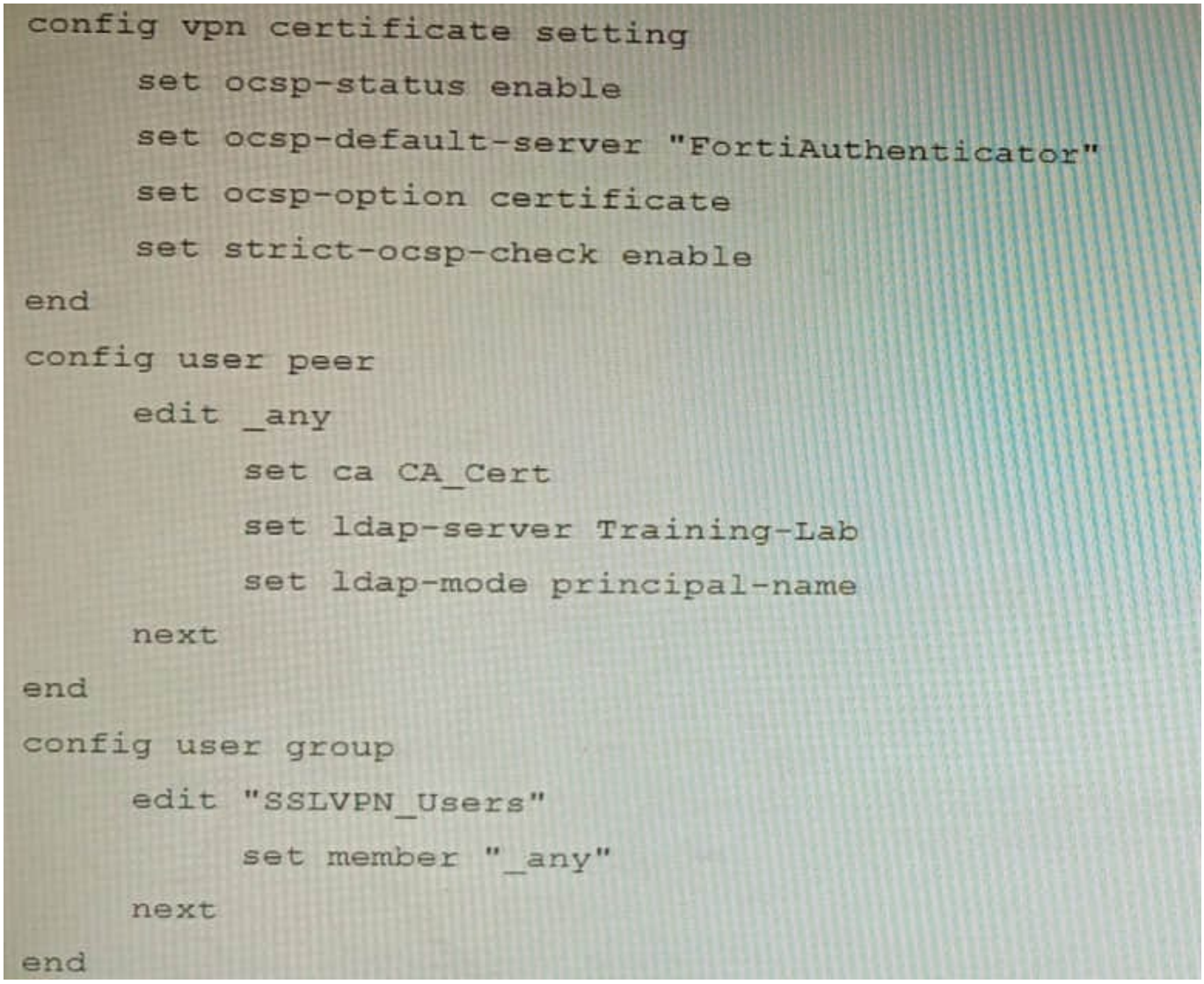
D. The configuration was modified on the FortiGate prior to connecting to the FortiManager

Correct Answer: C

Explanation: C is correct because the DHCP server used the incorrect option type for the FortiManager IP address. The option type should be 43 instead of 15, as shown in the FortiManager Administration Guide under Zero-Touch Provisioning > Configuring DHCP options for ZTP. References: https://docs.fortinet.com/document/fortimanager/7.4.0/administration-guide/568591/high-availabilityhttps://docs.fortinet.com/document/fortimanager/7.4.0/administration- guide/568591/high-availability/568592/configuring-ha-options

QUESTION 2

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.

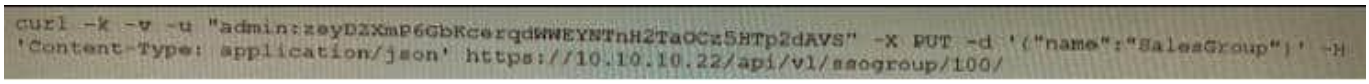
D. If the OCSP server is unreachable, authentication will succeed if the certificate matches the CA.

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 3

A customer wants to use the FortiAuthenticator REST API to retrieve an SSO group called SalesGroup. The following API call is being made with the \\'curl\\' utility:



Which two statements correctly describe the expected behavior of the FortiAuthenticator REST API? (Choose two.)

A. Only users with the "Full permission" role can access the REST API

B. This API call will fail because it requires that API version 2

C. If the REST API web service access key is lost, it cannot be retrieved and must be changed.

D. The syntax is incorrect because the API calls needs the get method.

Correct Answer: BD

Explanation: To retrieve an SSO group called SalesGroup using the FortiAuthenticator REST API, the following issues need to be fixed in the API call:

The API version should be v2, not v1, as SSO groups are only supported in version 2 of the REST API.

The HTTP method should be GET, not POST, as GET is used to retrieve information from the server, while POST is used to create or update information on the server. Therefore, a correct API call would look like this: curl -X GET -H

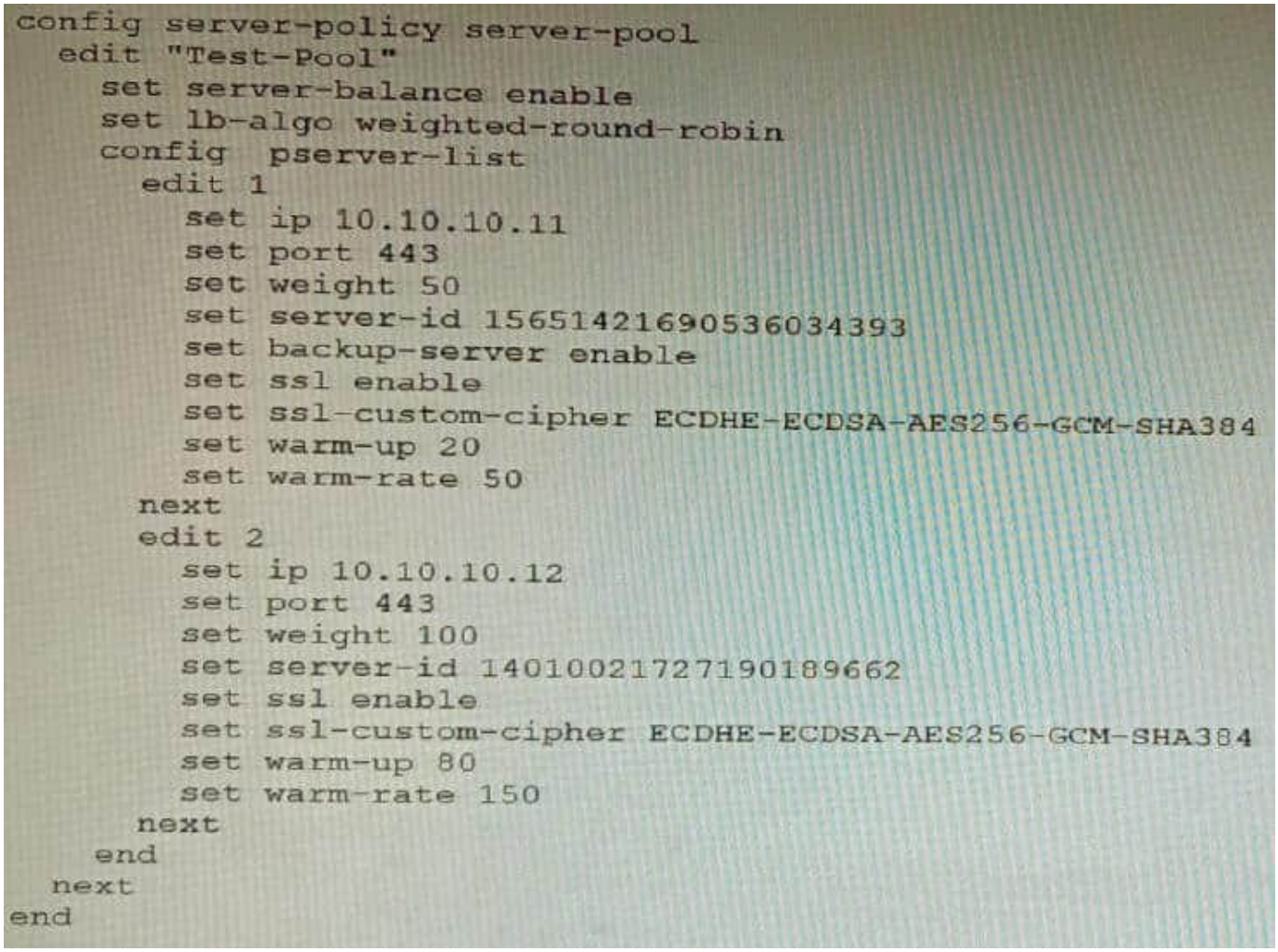
"Authorization: Bearer "

https://fac.example.com/api/v2/sso/groups/SalesGroup
References:https://docs.fortinet.com/document/fortiauthenticator/6.4.1/rest-api- solution-guide/927310/introduction

https://docs.fortinet.com/document/fortiauthenticator/6.4.1/rest-api-solution- guide/927311/sso-groups

QUESTION 4

Refer to the exhibit.



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.

QUESTION 5

SD-WAN is configured on a FortiGate. You notice that when one of the internet links has high latency the time to resolve names using DNS from FortiGate is very high.

You must ensure that the FortiGate DNS resolution times are as low as possible with the least amount of work. What should you configure?

A. Configure local out traffic to use the outgoing interface based on SD-WAN rules with a manual defined IP associated to a loopback interface and configure an SD-WAN rule from the loopback to the DNS server.

B. Configure an SD-WAN rule to the DNS server and use the FortiGate interface IPs in the source address.

C. Configure two DNS servers and use DNS servers recommended by the two internet providers.

D. Configure local out traffic to use the outgoing interface based on SD-WAN rules with the interface IP and configure an SD-WAN rule to the DNS server.

Correct Answer: D

Explanation: SD-WAN is a feature that allows users to optimize network performance and reliability by using multiple WAN links and applying rules based on various criteria, such as latency, jitter, packet loss, etc. One way to ensure that the FortiGate DNS resolution times are as low as possible with the least amount of work is to configure local out traffic to use the outgoing interface based on SD-WAN rules with the interface IP and configure an SD- WAN rule to the DNS server. This means that the FortiGate will use the best WAN link available to send DNS queries to the DNS server according to the SD-WAN rule, and use its own interface IP as the source address. This avoids NAT issues and ensures optimal DNS performance. References: https://docs.fortinet.com/document/fortigate/7.0.0/sd- wan/19662/sd-wan