Fortinet

FCP_FAZ_AD-7.4 Exam

FCP - FortiAnalyzer 7.4 Administrator

Questions & Answers
Demo

Version: 4.1

Question: 1

Which two statements regarding ADOM modes are true? (Choose two.)

A. In normal mode, the disk quota of the ADOM is fixed and cannot be modified, but in advanced mode, the disk quota of the ADOM is flexible.
B. You can change ADOM modes only through the CLI.
C. In an advanced mode ADOM, you can assign FortiGate VDOMs from a single FortiGate device to multiple FortiAnalyzer ADOMs.
D. Normal mode is the default ADOM mode.

Answer: C, D

Question: 2

What is the purpose of the FortiAnalyzer command diagnose system print netstat?

A. It provides network statistics for active connections, including the protocols, IP addresses, and connection states.
B. It provides the complete routing table, including directly connected routes.
C. It provides the static DNS table, including the host names and their expiration timers.
D. It provides NTP server information, including server IPs. stratum, poll time, and latency.

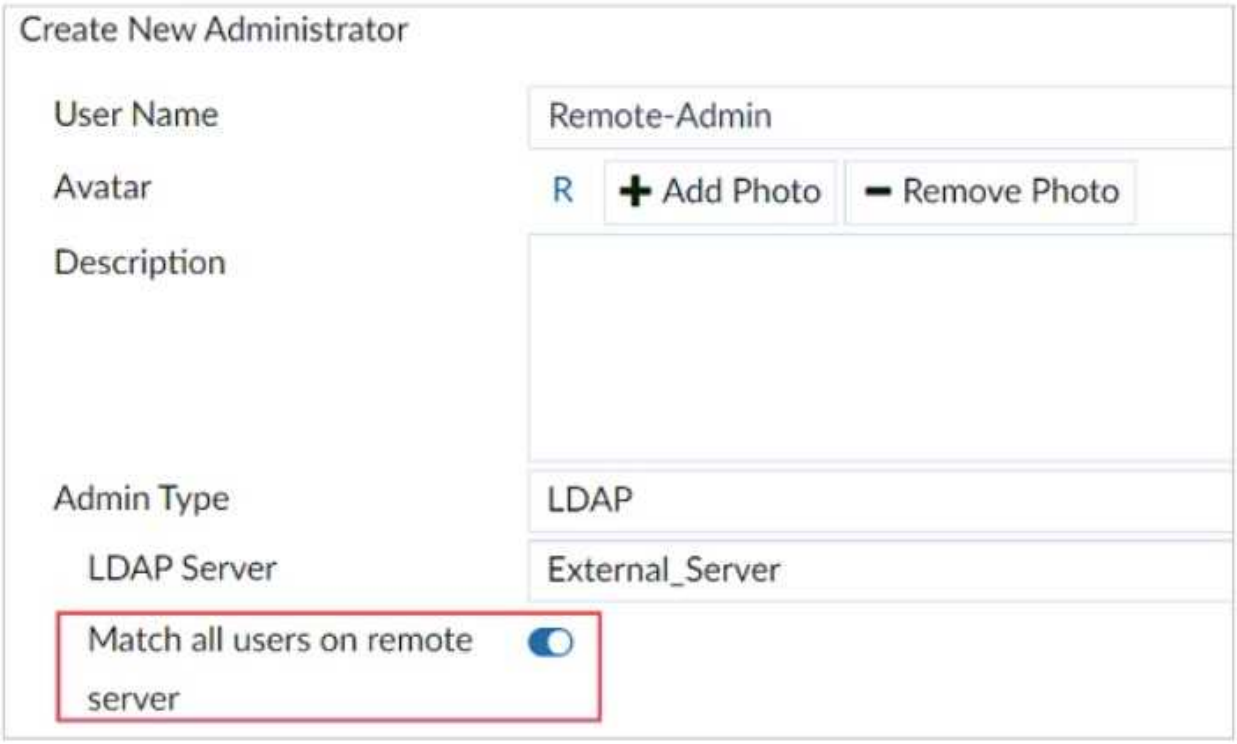
Answer: A

Explanation:

The diagnose system print netstat command in FortiAnalyzer provides detailed information on active network connections, similar to the netstat command found in many operating systems.

Question: 3

Refer to the exhibit.



The exhibit shows the creation of a new administrator on FortiAnalyzer.

What are two effects of enabling the choice Match all users on remote server when configuring a new administrator? (Choose two.)

A. It allows user accounts in the LDAP server to use two-factor authentication.
B. It creates a wildcard administrator using an LDAP server.
C. User Remote-Admin from the LDAP server will be able to log in to FortiAnalyzer at any time.
D. Administrators can log in to FortiAnalyzer using their credentials on the remote LDAP server.

Answer: B, D

Explanation:

Enabling this option allows any user authenticated by the LDAP server to log in to FortiAnalyzer, effectively creating a wildcard administrator.

Question: 4

The connection status of a new device on FortiAnalyzer is listed as Unauthorized.
What does that status mean?

A. It is a device whose registration has not yet been accepted in FortiAnalvzer.
B. It is a device that has not yet been assigned an ADOM.
C. It is a device that is waiting for you to configure a pre-shared key.
D. It is a device that FortiAnalvzer does not support.

Answer: A

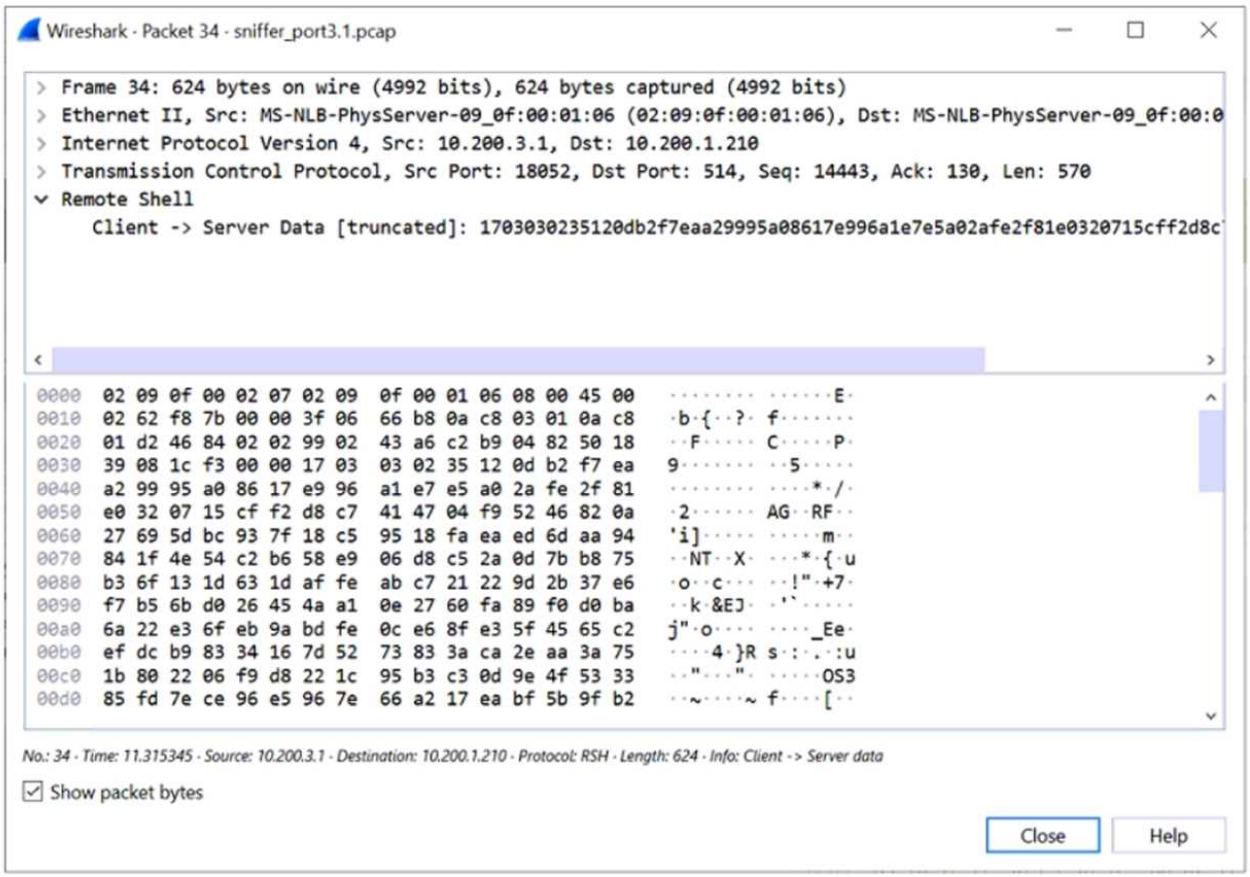
Explanation:

The "Unauthorized" status indicates that the device has been discovered or attempted to connect but has not yet been authorized for management by FortiAnalyzer. It requires an administrator to approve or authorize the device before it can be fully managed.

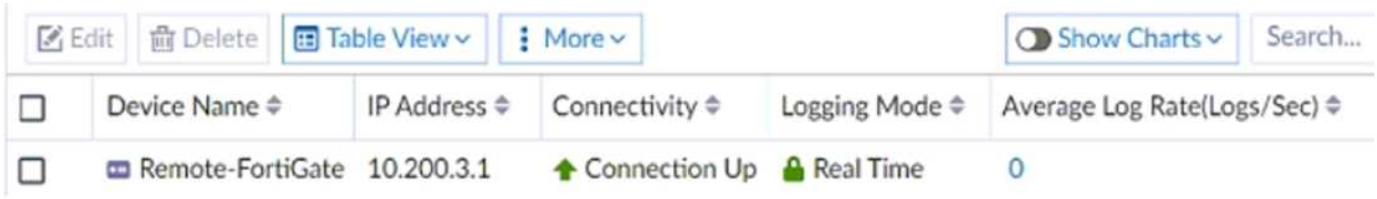
Question: 5

Refer to the exhibit.

FortiAnalyzer packet capture on Wireshark



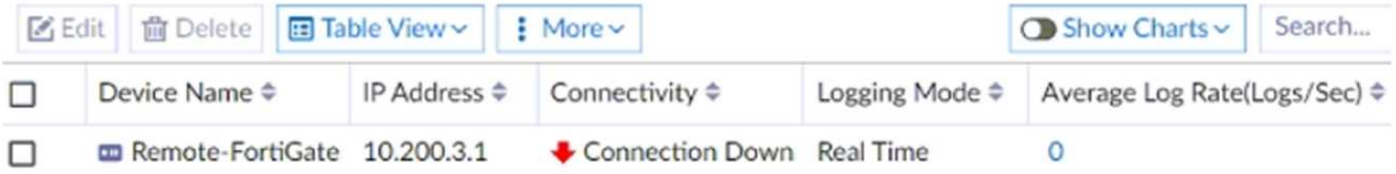
Which image corresponds to the packet capture shown in the exhibit?
A)



B)

C)

D)



A. Option A
B. Option B
C. Option C
D. Option D

Answer: A

Explanation:

Chosen image shows the device Remote-FortiGate with the IP 10.200.3.1 and a connection status of "Connection Up," which is consistent with the packet capture details showing active communication between the client and server.