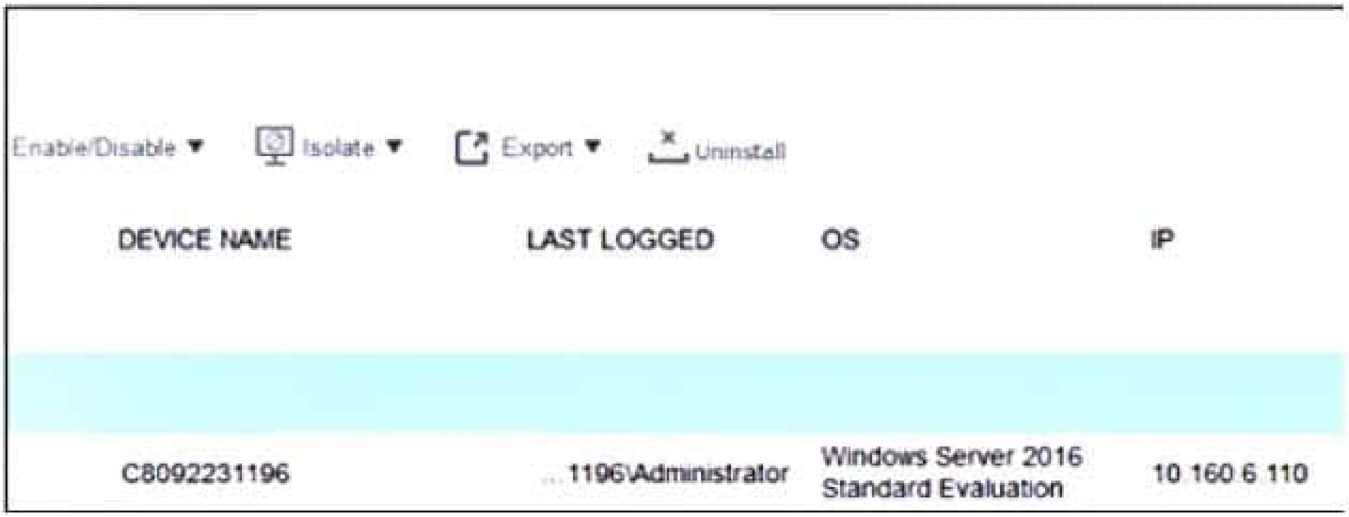
NSE5_EDR-5.0^Q&As^

Fortinet NSE 5 - FortiEDR 5.0

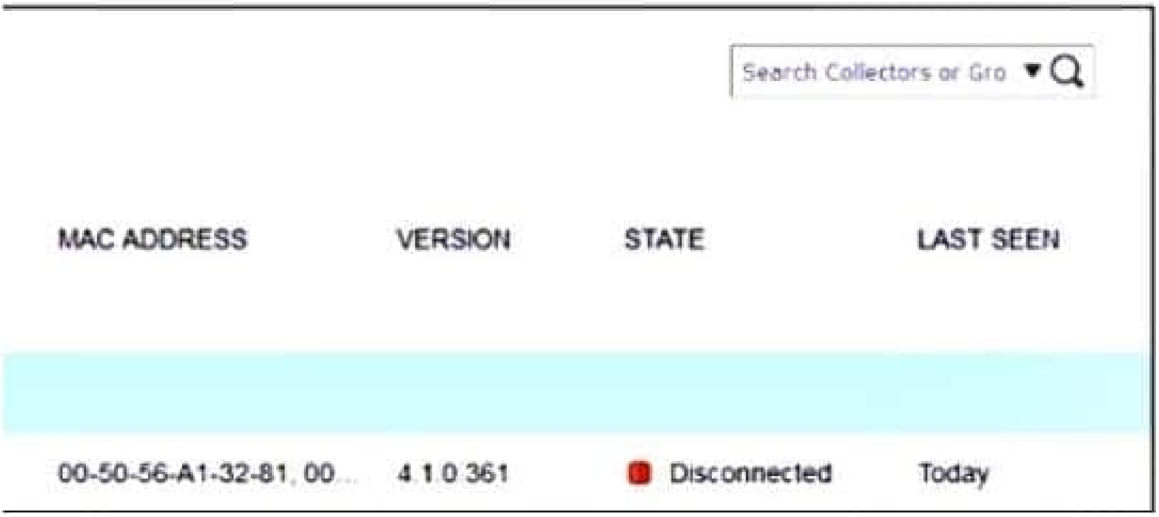
Pass Fortinet NSE5_EDR-5.0 Exam with 100% Guarantee

QUESTION 1

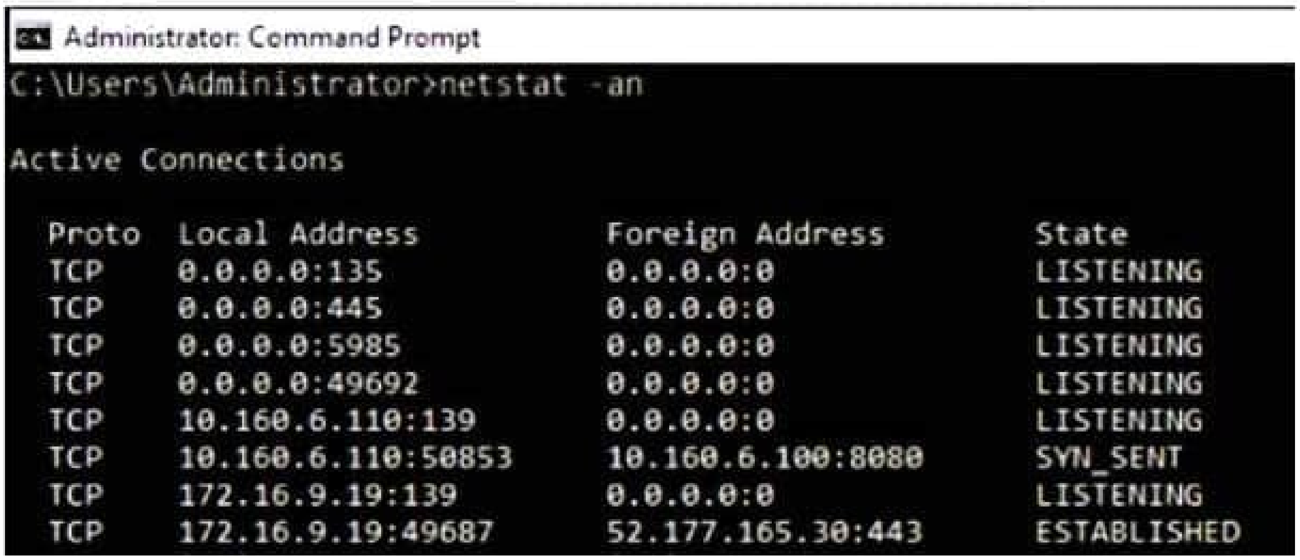
Refer to the exhibits.



DEVICE NAME	LAST LOGGED	OS	IP
C8092231196	...1196\Administrator	Windows Server 2016 Standard Evaluation	10.160.6.110



MAC ADDRESS	VERSION	STATE	LAST SEEN
00-50-56-A1-32-81, 00...	4.1.0.361	🟥 Disconnected	Today



```
C:\Users\Administrator>netstat -an

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:5985           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49692          0.0.0.0:0              LISTENING
  TCP    10.160.6.110:139       0.0.0.0:0              LISTENING
  TCP    10.160.6.110:50853     10.160.6.100:8080      SYN_SENT
  TCP    172.16.9.19:139        0.0.0.0:0              LISTENING
  TCP    172.16.9.19:49687      52.177.165.30:443      ESTABLISHED
```

The exhibits show the collector state and active connections. The collector is unable to connect to aggregator IP address 10.160.6.100 using default port. Based on the netstat command output what must you do to resolve the connectivity issue?

A. Reinstall collector agent and use port 443

B. Reinstall collector agent and use port 8081

C. Reinstall collector agent and use port 555

D. Reinstall collector agent and use port 6514

Correct Answer: B

QUESTION 2

Which two statements are true about the remediation function in the threat hunting module? (Choose two.)

A. The file is removed from the affected collectors

B. The threat hunting module sends the user a notification to delete the file

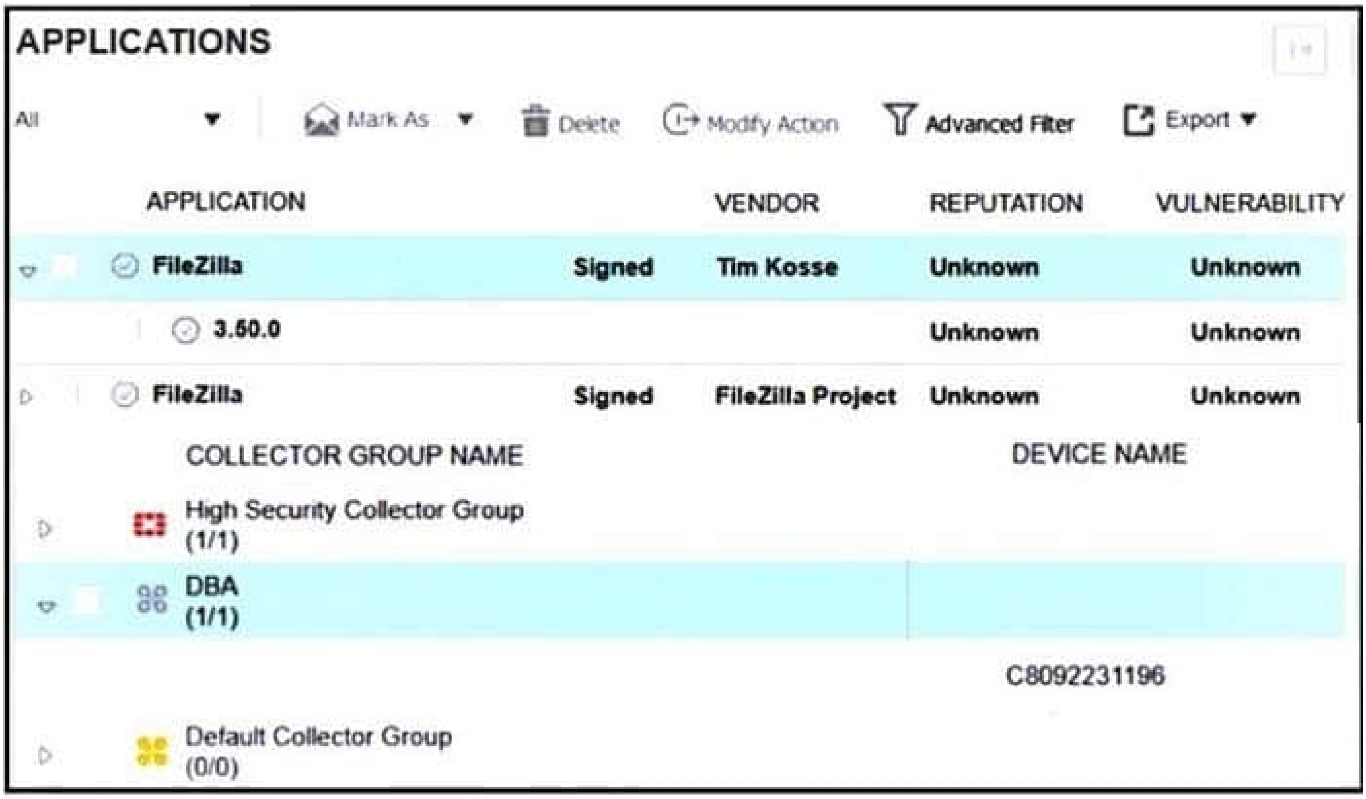
C. The file is quarantined

D. The threat hunting module deletes files from collectors that are currently online.

Correct Answer: AD

QUESTION 3

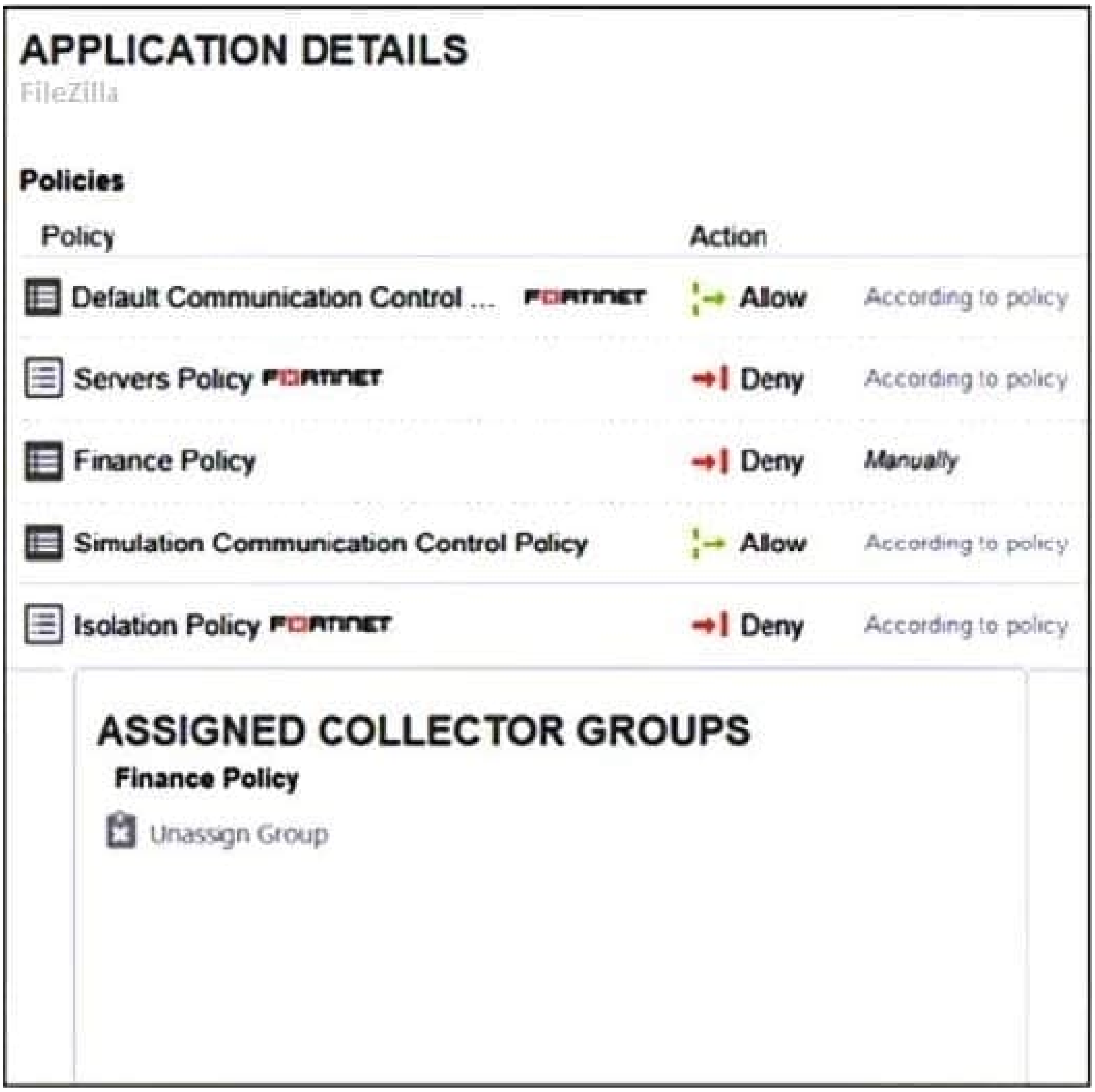
Refer to the exhibits.



APPLICATIONS

APPLICATION		VENDOR	REPUTATION	VULNERABILITY
FileZilla	Signed	Tim Kosse	Unknown	Unknown
3.60.0			Unknown	Unknown
FileZilla	Signed	FileZilla Project	Unknown	Unknown

COLLECTOR GROUP NAME	DEVICE NAME
High Security Collector Group (1/1)	
DBA (1/1)	
	C8092231196
Default Collector Group (0/0)	



APPLICATION DETAILS

FileZilla

Policies

Policy	Action	
Default Communication Control ... FORTINET	Allow	According to policy
Servers Policy FORTINET	Deny	According to policy
Finance Policy	Deny	Manually
Simulation Communication Control Policy	Allow	According to policy
Isolation Policy FORTINET	Deny	According to policy

ASSIGNED COLLECTOR GROUPS

Finance Policy

Unassign Group

The exhibits show application policy logs and application details Collector C8092231196 is a member of the Finance group What must an administrator do to block the FileZilia application?

A. Deny application in Finance policy

B. Assign Finance policy to DBA group

C. Assign Finance policy to Default Collector Group

D. Assign Simulation Communication Control Policy to DBA group

Correct Answer: B

QUESTION 4

Which two criteria are requirements of integrating FortiEDR into the Fortinet Security Fabric? (Choose two.)

A. Core with Core only functionality

B. A Forensics add-on license

C. Central Manager connected to FCS

D. A valid API user with access to connectors

Correct Answer: CD

QUESTION 5

How does the FortiEDR approach compare to the traditional EDR? (Choose two.)

A. FortiEDR blocks threats in real time, eliminating the response gap

B. Traditional EDR is faster

C. There is no difference in response time

D. FortiEDR requires less staff

Correct Answer: AD