# NSE5_EDR-5.0 Q&As

Fortinet NSE 5 - FortiEDR 5.0

## Pass Fortinet NSE5_EDR-5.0 Exam with 100% Guarantee

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

**https://www.certbus.com/nse5_edr-5-0.html**

100% Passing Guarantee
100% Money Back Assurance

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

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

**QUESTION 1**

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

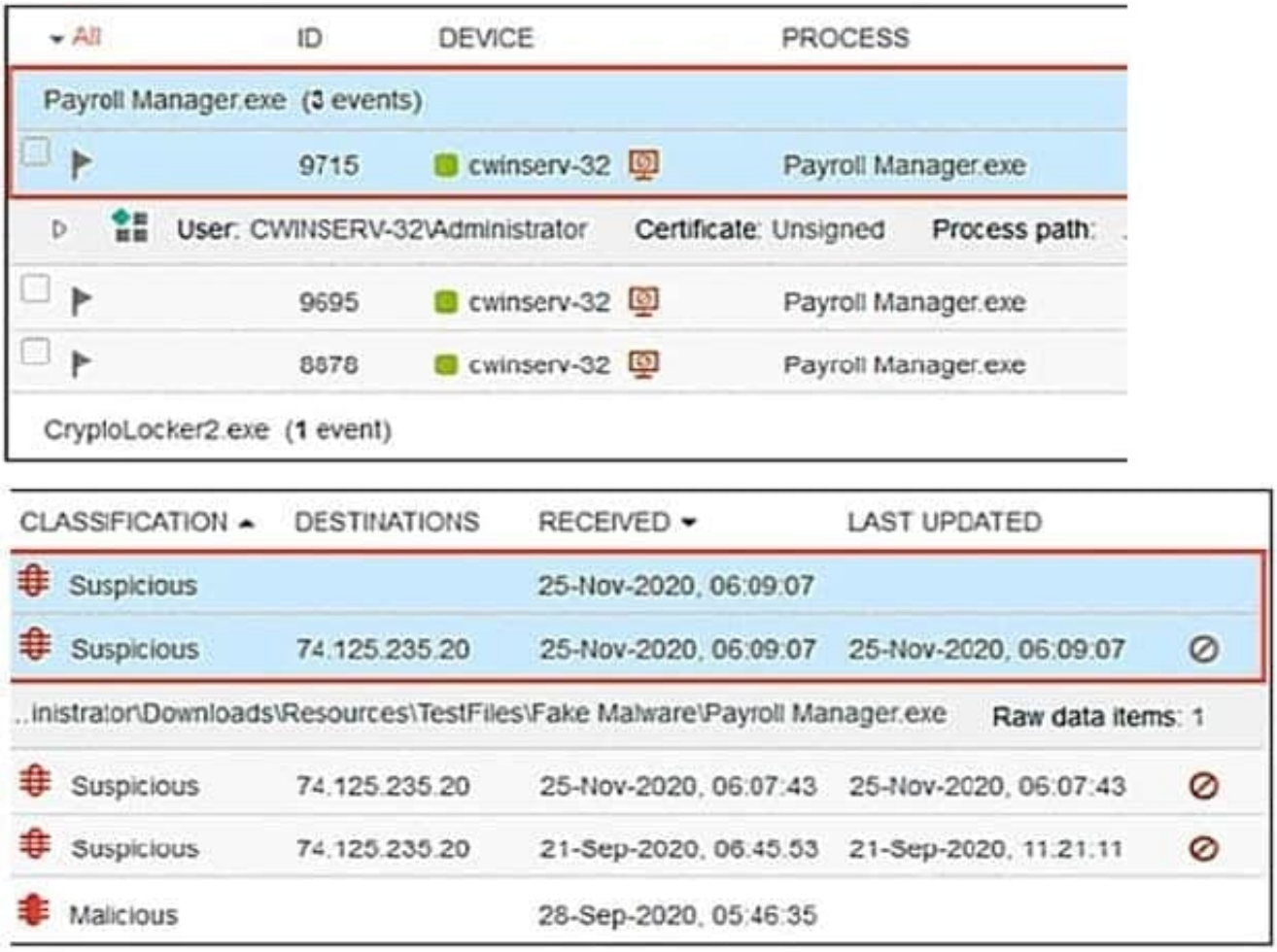
D. A valid API user with access to connectors

Correct Answer: CD

**QUESTION 2**

Refer to the exhibit.

The exhibit shows an event viewer.




What is true about the Payroll Manager.exe event?

A. An event has not been handled by a console admin

B. An event has been deleted

C. A rule assigned action is set to block but the policy is in simulation mode

D. An event has been handled by the communication control policy

Correct Answer: C

**QUESTION 3**

Refer to the exhibit.


TestApplication.exe.exe (3 events)
Malicious
15-Feb-2022, 13:31:39
5894314
R2D2-kvm63
TestApplication.exe.exe
Malicious
8.8.8.8
15-Feb-2022, 13:31:39
15-Feb-2022, 13:31:39
Logged-in User:
Process owner:
Certificate:
Process path:
R2D2-KVM63\fortinet
R2D2-KVM63\fortinet
Unsigned
C:\Users\fortinet\Desktc
CLASSIFICATION DETAILS
Malicious
Threat name: Unknown
Threat family: Unknown
Threat type: Unknown
History
Malicious, by Fortinet, on 15-Feb-2022, 13:31:41
Triggered Rules
Exfiltration Prevention
Invalid Checksum - Connection Attempt from Application wi...
Malicious File Detected
Suspicious Packer - Activity by an Application packed by a S...
Writeable Code - Identified an Executable with Writable Code


TestApplication.exe.exe (3 events)
Malicious
5894314
R2D2-kvm63
TestApplication.exe.exe
Malicious
Logged-in User:
Process owner:
Certificate:
Process path:
R2D2-KVM63\fortinet
R2D2-KVM63\fortinet
Unsigned
C:\Users\fortinet\Desktc


15-Feb-2022, 13:31:39
8.8.8.8
15-Feb-2022, 13:31:39
15-Feb-2022, 13:31:39
CLASSIFICATION DETAILS
Malicious
Threat name: Unknown
Threat family: Unknown
Threat type: Unknown
History
Malicious, by Fortinet, on 15-Feb-2022, 13:31:41
Triggered Rules
Exfiltration Prevention
Invalid Checksum - Connection Attempt from Application wi...
Malicious File Detected
Suspicious Packer - Activity by an Application packed by a S...
Writeable Code - Identified an Executable with Writable Code

Based on the event shown in the exhibit, which two statements about the event are true? (Choose two.)

A. The NGAV policy has blocked TestApplication exe

B. TestApplication exe is sophisticated malware

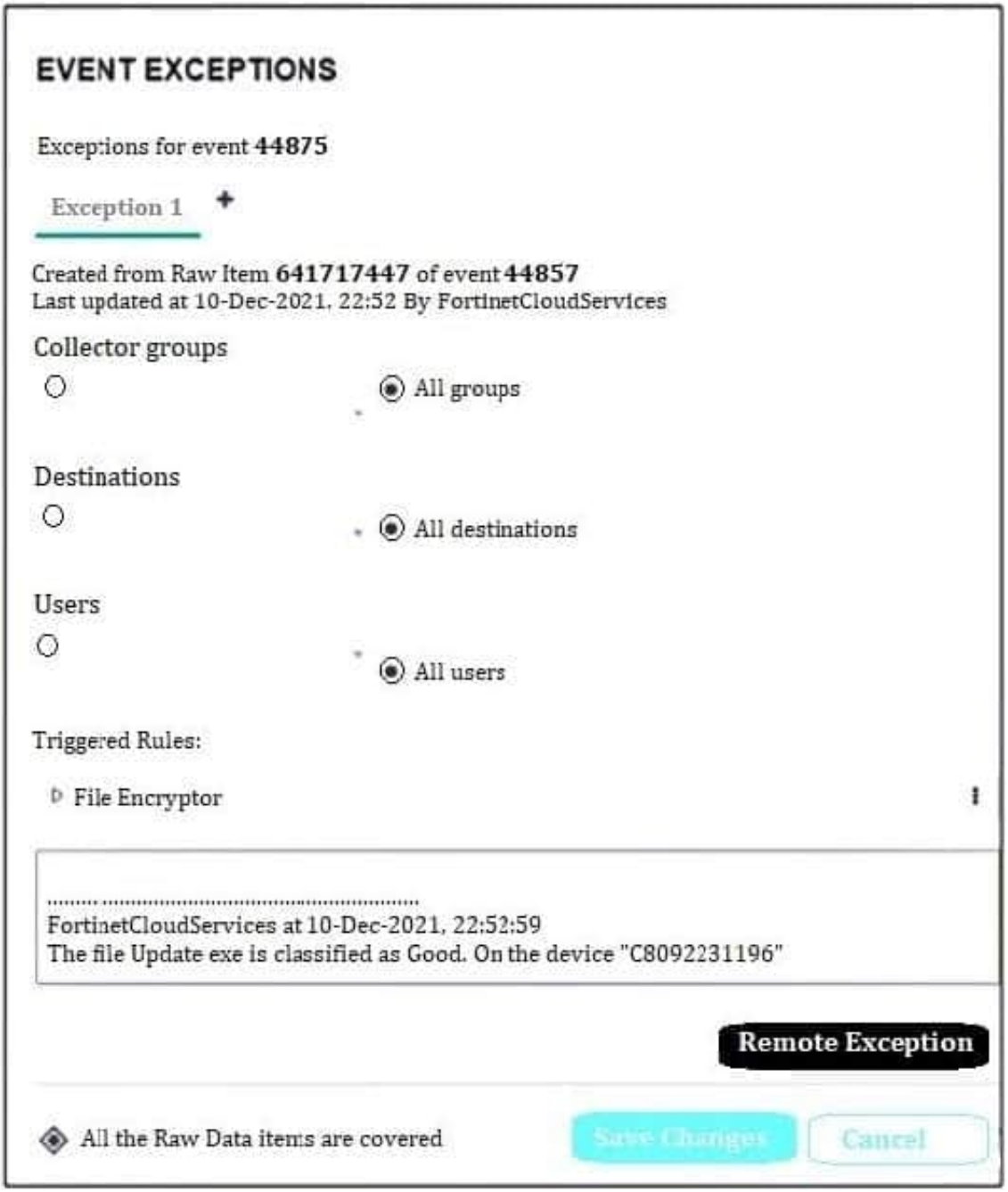
C. The user was able to launch TestApplication exe

D. FCS classified the event as malicious

Correct Answer: BC

**QUESTION 4**

Refer to the exhibit.




Based on the event exception shown in the exhibit which two statements about the exception are true? (Choose two)

A. A partial exception is applied to this event

B. FCS playbooks is enabled by Fortinet support

C. The exception is applied only on device C8092231196

D. The system owner can modify the trigger rules parameters

Correct Answer: AC

**QUESTION 5**

Which threat hunting profile is the most resource intensive?

A. Comprehensive

B. Inventory

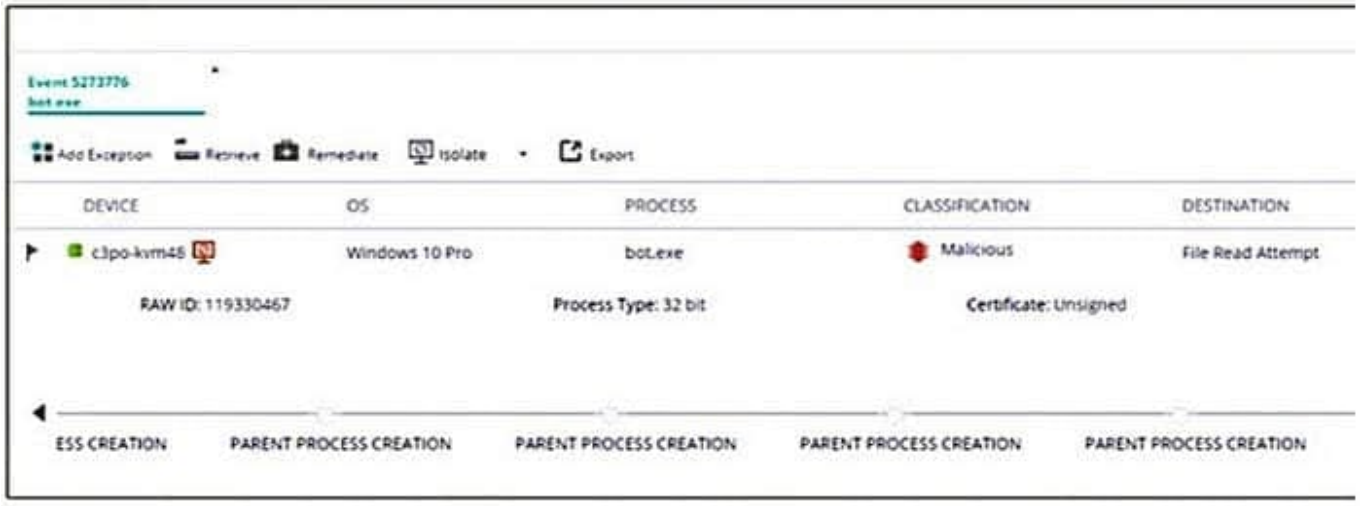
C. Default

D. Standard Collection

Correct Answer: A

**QUESTION 6**

Exhibit.





Based on the forensics data shown in the exhibit, which two statements are true? (Choose two.)

A. An exception has been created for this event

B. The forensics data is displayed m the stacks view

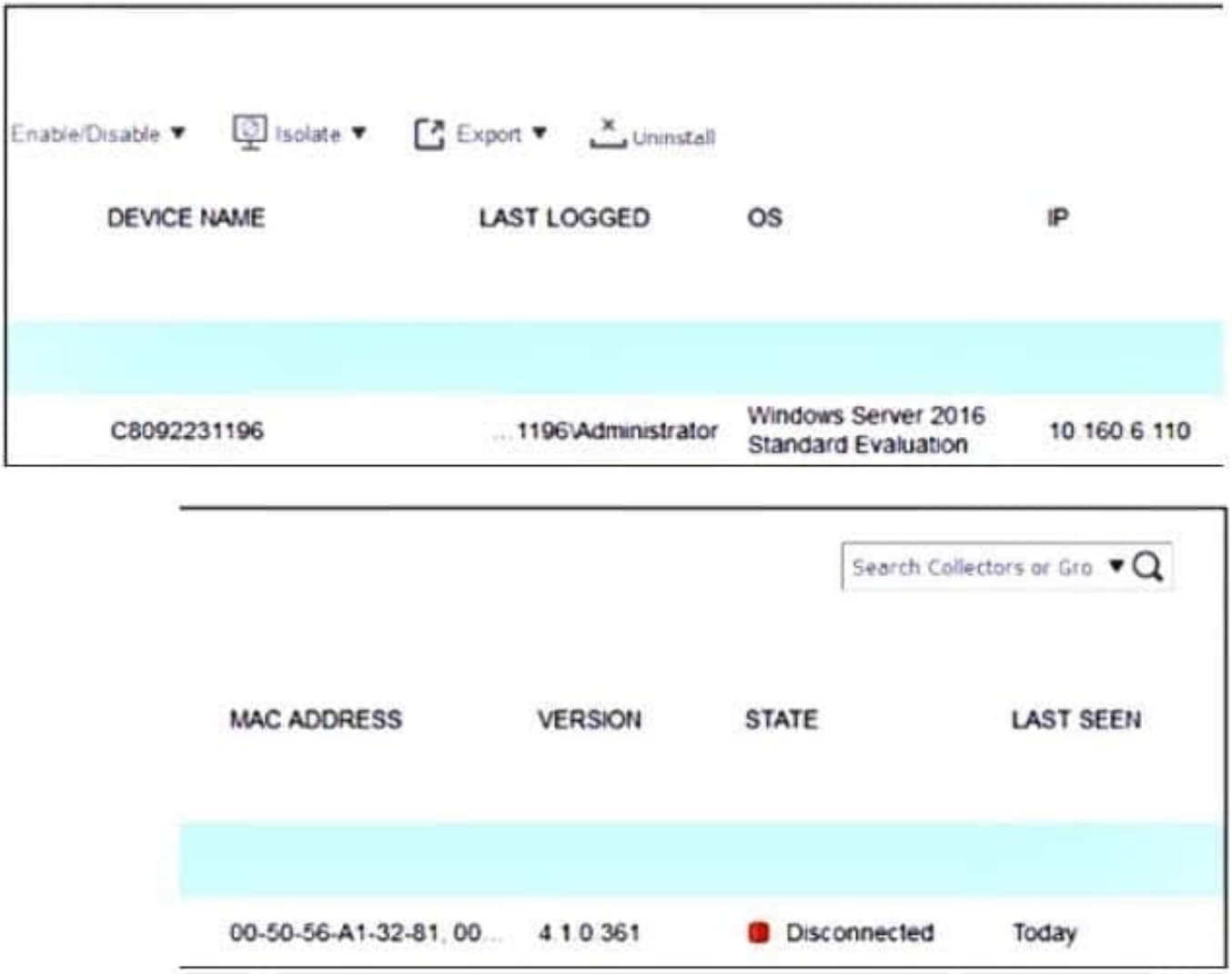
C. The device has been isolated

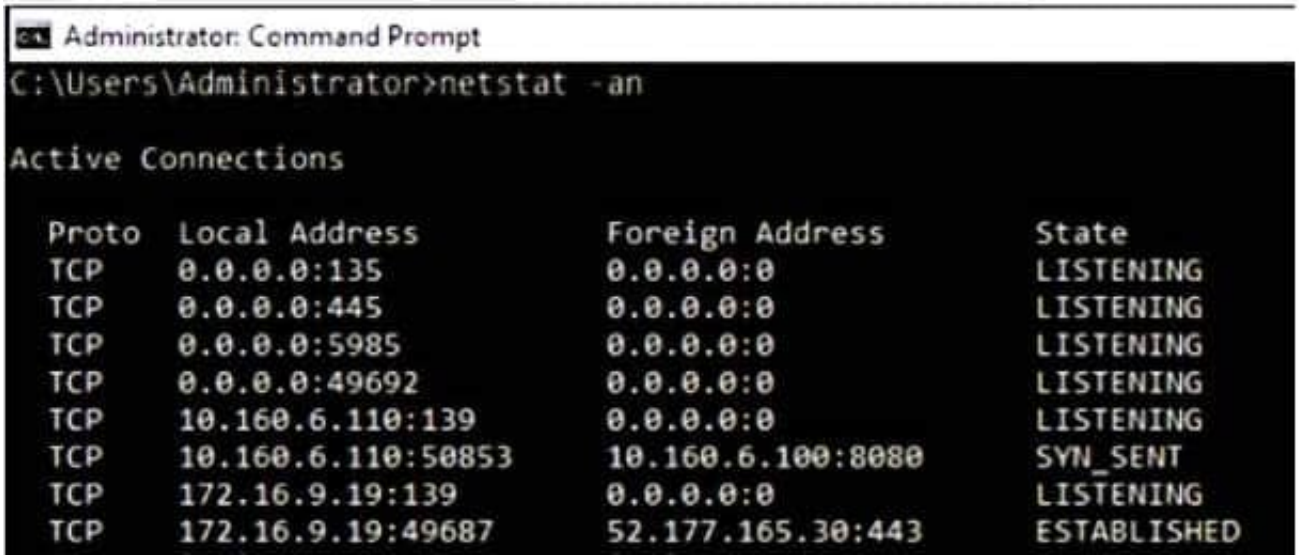
D. The exfiltration prevention policy has blocked this event

Correct Answer: BC

**QUESTION 7**

Refer to the exhibits.



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

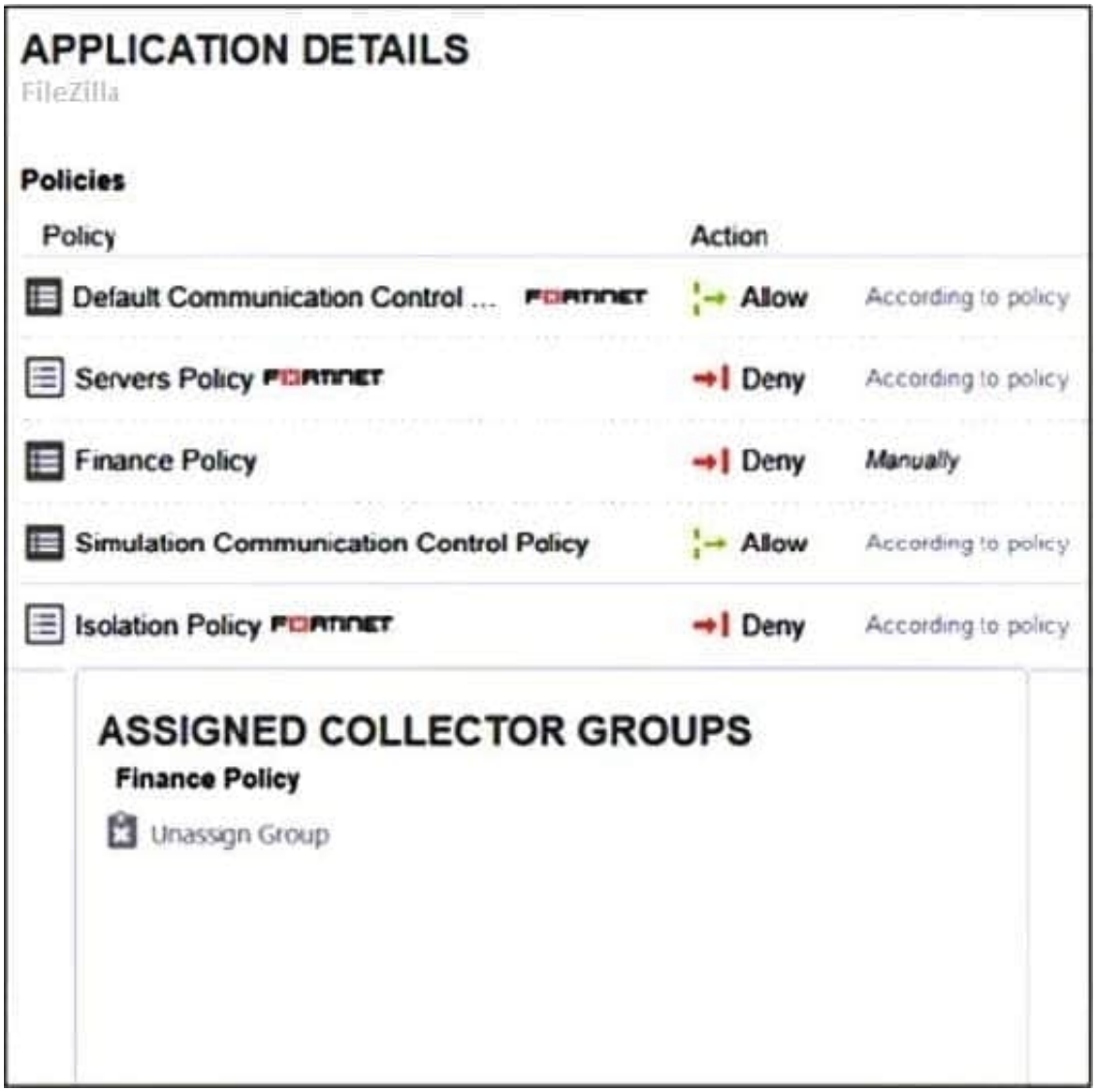
C. Reinstall collector agent and use port 555

D. Reinstall collector agent and use port 6514

Correct Answer: B

**QUESTION 8**

Refer to the exhibits.




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 9**

FortiXDR relies on which feature as part of its automated extended response?

A. Playbooks

B. Security Policies

C. Forensic

D. Communication Control

Correct Answer: A

**QUESTION 10**

What is the benefit of using file hash along with the file name in a threat hunting repository search?

A. It helps to make sure the hash is really a malware

B. It helps to check the malware even if the malware variant uses a different file name

C. It helps to find if some instances of the hash are actually associated with a different file

D. It helps locate a file as threat hunting only allows hash search

Correct Answer: B