



# NSE5\_EDR-5.0<sup>Q&As</sup>

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.geekcert.com/nse5\\_edr-5-0.html](https://www.geekcert.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 events can trigger FortiEDR NGAV policy violations? (Choose two.)

- A. When a malicious file attempts to communicate externally
- B. When a malicious file is executed
- C. When a malicious file is read
- D. When a malicious file attempts to access data

Correct Answer: BC

NGAV reacts when a file is Saved, Read, or Executed Page 79 of the guide

**QUESTION 2**

Refer to the exhibits.

APPLICATIONS					
APPLICATION	VENDOR	REPUTATION	VULNERABILITY		
FileZilla	Signed	Tim Kosse	Unknown	Unknown	
3.50.0			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 ... <b>FORTINET</b>	Allow	According to policy
Servers Policy <b>FORTINET</b>	Deny	According to policy
Finance Policy	Deny	Manually
Simulation Communication Control Policy	Allow	According to policy
Isolation Policy <b>FORTINET</b>	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 FileZilla 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 3

A company requires a global communication policy for a FortiEDR multi-tenant environment.

How can the administrator achieve this?



- A. An administrator creates a new communication control policy and shares it with other organizations
- B. A local administrator creates new a communication control policy and shares it with other organizations
- C. A local administrator creates a new communication control policy and assigns it globally to all organizations
- D. An administrator creates a new communication control policy for each organization

Correct Answer: C

---

#### QUESTION 4

Refer to the exhibit.



### Process Creation

Summary    ↔ cmd.exe    ↔ PING.EXE    14-Feb-2022 12:33

---

**R2R2-kmv63**    Status ● **Running**    Internal IP **10.122.0.160**  
Up time **6min, 6sec**

**cmd.exe**    PID-8180 TID-8184    64 bit

Path: **C:\Windows\System32\cmd.exe**  
Executing user: **R2D2-KVM63\fortinet**  
Product: **Microsoft Windows Operating System, v10.0.19041.746**  
SHA1: **F1EFB0FDDC156E4C61C5F78A54700E4E7984D55D**

---

### Process Creation

**PING.EXE**    PID-5764    64 bit

Path: **C:\Windows\System32\PING.EXE**  
Executing user: **R2D2-KVM63\fortinet**  
Parent: **\Device\HarddiskVolume2\Windows\System32\cmd.exe ID-8180**  
Product: **Microsoft Windows Operating System, v10.0.19041.1**  
SHA1: **9C13C854A4EF98879D0CA880EF679B4C4ECCF518**  
Command line: **fortinet.com**

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

- A. The PING EXE process was blocked
- B. The user fortinet has executed a ping command
- C. The activity event is associated with the file action



D. There are no MITRE details available for this event

Correct Answer: BD

---

#### QUESTION 5

Refer to the exhibits.



Enable/Disable ▾ Isolate ▾ Export ▾ Uninstall

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

Search Collectors or Gro ▾ Q

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

```
Administrator: Command Prompt
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

[Latest NSE5\\_EDR-5.0 Dumps](#)

[NSE5\\_EDR-5.0 VCE Dumps](#)

[NSE5\\_EDR-5.0 Braindumps](#)