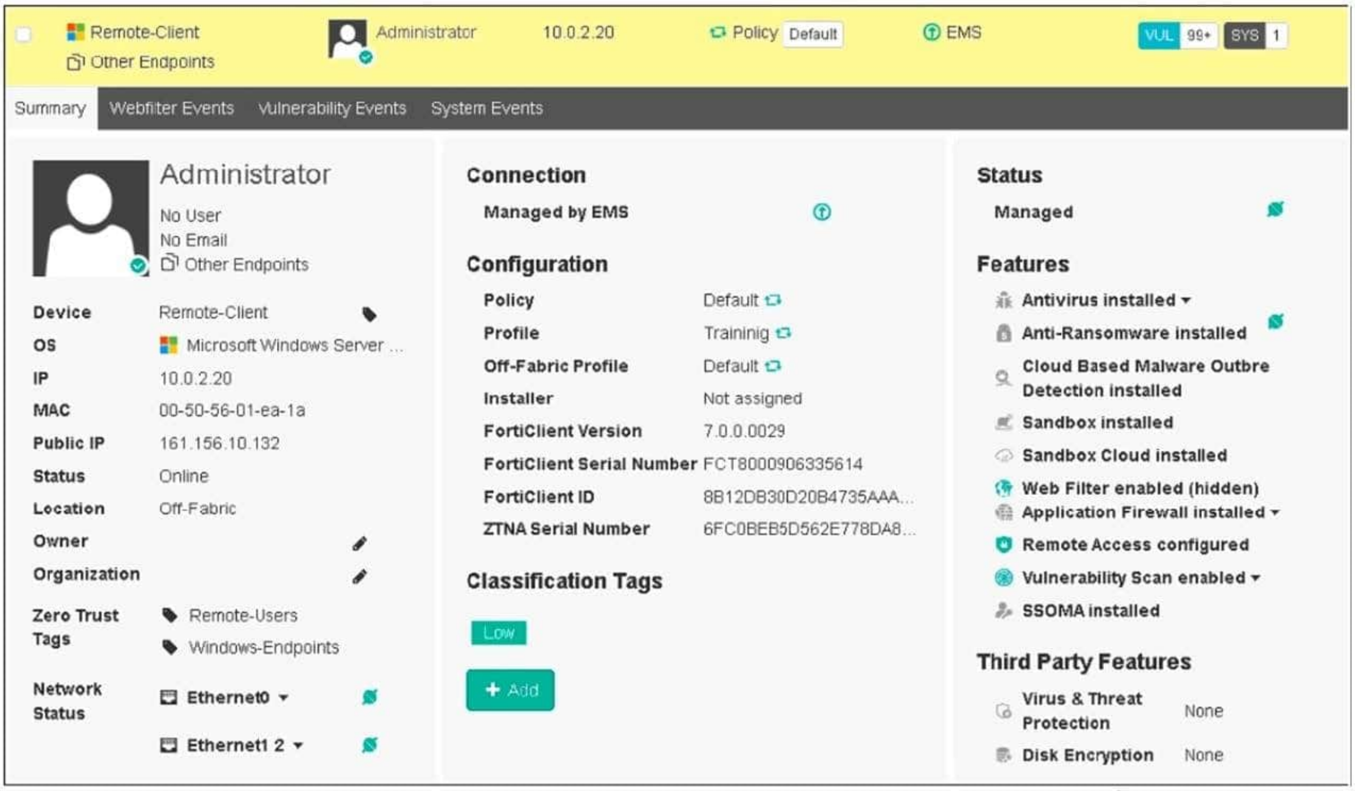
NSE5_FCT-7.0^{Q&As}

Fortinet NSE 5 - FortiClient EMS 7.0

Pass Fortinet NSE5_FCT-7.0 Exam with 100% Guarantee

QUESTION 1

Refer to the exhibit, which shows the endpoint summary information on FortiClient EMS.



Remote-Client
Other Endpoints
Administrator
10.0.2.20
Policy Default
EMS
VUL 99+ SYS 1

Summary | Webfilter Events | Vulnerability Events | System Events

Administrator
No User
No Email
Other Endpoints

Device	Remote-Client
OS	Microsoft Windows Server ...
IP	10.0.2.20
MAC	00-50-56-01-ea-1a
Public IP	161.156.10.132
Status	Online
Location	Off-Fabric
Owner	
Organization	
Zero Trust Tags	Remote-Users Windows-Endpoints
Network Status	Ethernet0 Ethernet1 2

Connection
Managed by EMS

Configuration

Policy	Default
Profile	Traininig
Off-Fabric Profile	Default
Installer	Not assigned
FortiClient Version	7.0.0.0029
FortiClient Serial Number	FCT8000906335614
FortiClient ID	8B12DB30D20B4735AAA...
ZTNA Serial Number	6FC0BEB5D562E778DA8...

Classification Tags
Low
+ Add

Status
Managed

Features
- Antivirus installed
- Anti-Ransomware installed
- Cloud Based Malware Outbre Detection installed
- Sandbox installed
- Sandbox Cloud installed
- Web Filter enabled (hidden)
- Application Firewall installed
- Remote Access configured
- Vulnerability Scan enabled
- SSOMA installed

Third Party Features

Virus & Threat Protection	None
Disk Encryption	None

What two conclusions can you make based on the Remote-Client status shown above? (Choose two.)

A. The endpoint is classified as at risk.

B. The endpoint has been assigned the Default endpoint policy.

C. The endpoint is configured to support FortiSandbox.

D. The endpoint is currently off-net.

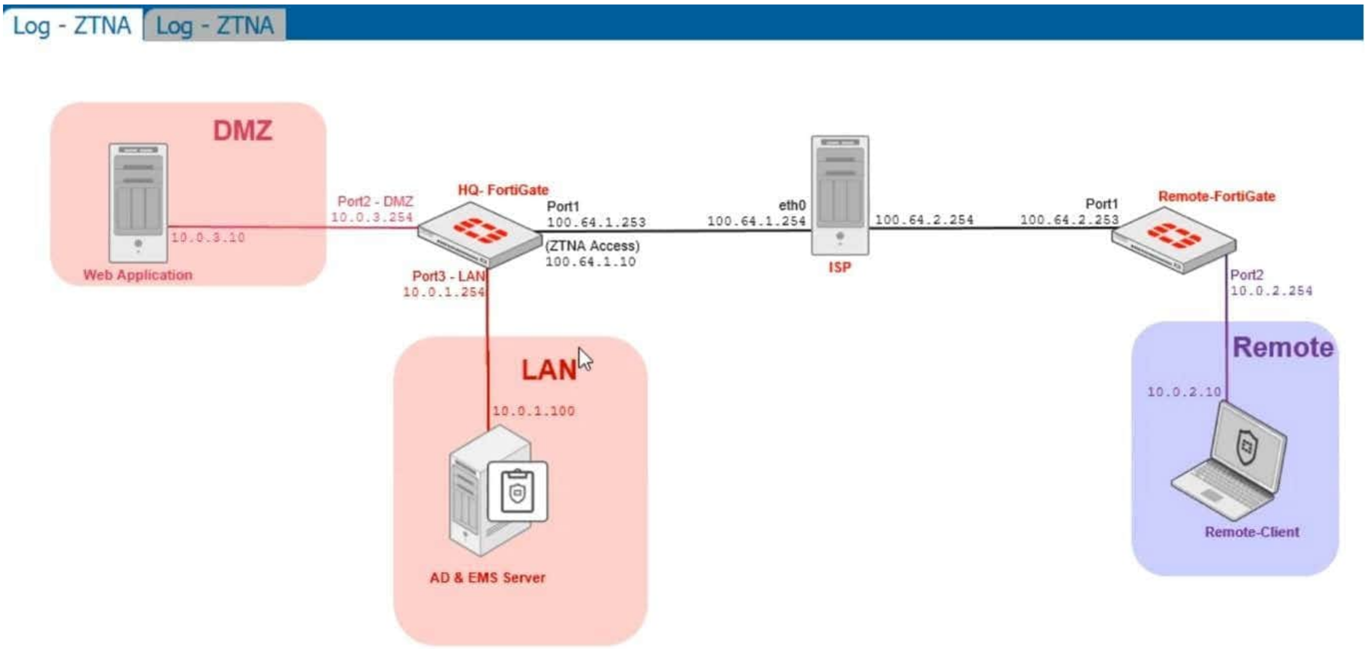
Correct Answer: BD

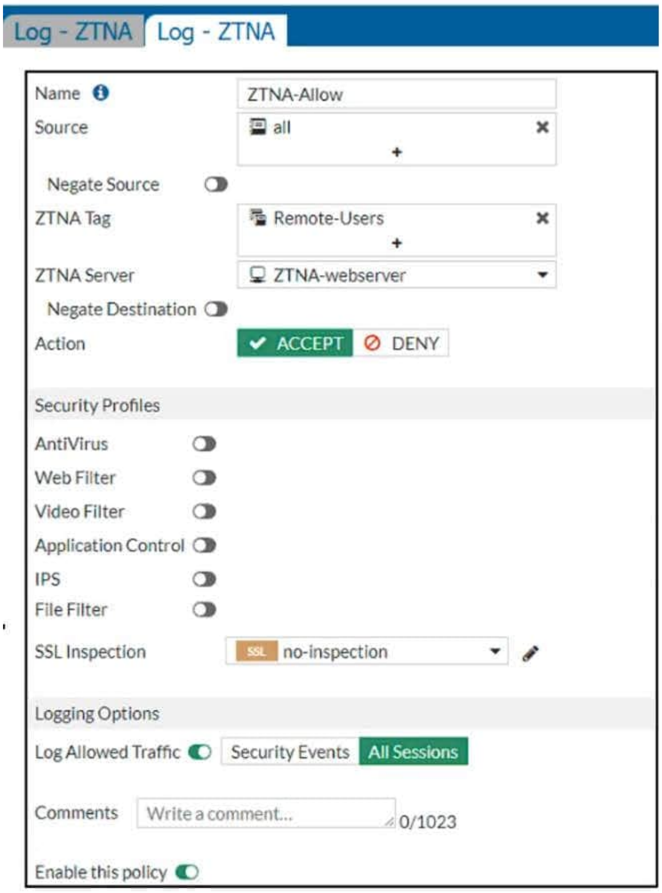
QUESTION 2

Refer to the exhibits, which show a network topology diagram of ZTNA proxy access and the ZTNA rule configuration.

An administrator runs the diagnose endpoint record list CLI command on FortiGate to check Remote-Client endpoint information, however Remote-Client is not showing up in the endpoint record list.

What is the cause of this issue?





Name	ZTNA-Allow
Source	all
Negate Source	○
ZTNA Tag	Remote-Users
ZTNA Server	ZTNA-webserver
Negate Destination	○
Action	✓ ACCEPT / DENY

Security Profiles

AntiVirus	○
Web Filter	○
Video Filter	○
Application Control	○
IPS	○
File Filter	○
SSL Inspection	SSL no-inspection

Logging Options

Log Allowed Traffic	● Security Events / All Sessions
Comments	Write a comment... 0/1023
Enable this policy	●

A. Remote-Client failed the client certificate authentication.

B. Remote-Client provided an empty client certificate to connect to the ZTNA access proxy.

C. Remote-Client has not initiated a connection to the ZTNA access proxy.

D. Remote-Client provided an invalid certificate to connect to the ZTNA access proxy.

Correct Answer: C

QUESTION 3

Which security fabric component sends a notification to quarantine an endpoint after IOC detection in the automation process?

A. FortiAnalyzer

B. FortiClient

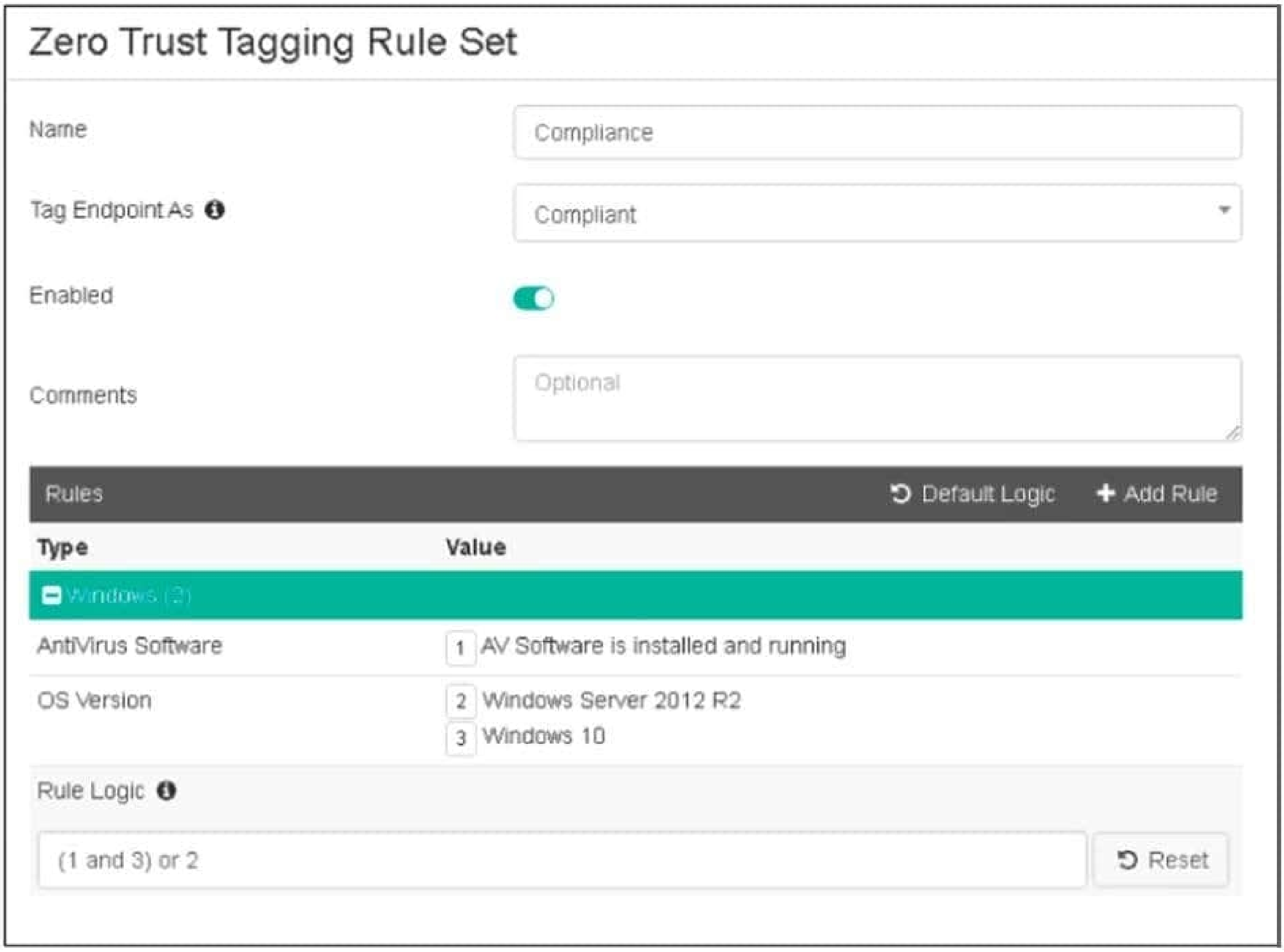
C. ForbClient EMS

D. Forti Gate

Correct Answer: D

QUESTION 4

Refer to the exhibit, which shows the Zero Trust Tagging Rule Set configuration.



Zero Trust Tagging Rule Set

Name: Compliance

Tag Endpoint As: Compliant

Enabled: ●

Comments: Optional

Type	Value
Windows (2)	
AntiVirus Software	1 AV Software is installed and running
OS Version	2 Windows Server 2012 R2 3 Windows 10

Rule Logic: (1 and 3) or 2

Which two statements about the rule set are true? (Choose two.)

A. The endpoint must satisfy that only Windows 10 is running.

B. The endpoint must satisfy that only AV software is installed and running.

C. The endpoint must satisfy that antivirus is installed and running and Windows 10 is running.

D. The endpoint must satisfy that only Windows Server 2012 R2 is running.

Correct Answer: CD

QUESTION 5

What action does FortiClient anti-exploit detection take when it detects exploits?

A. Blocks memory allocation to the compromised application process

B. Patches the compromised application process

C. Deletes the compromised application process

D. Terminates the compromised application process

Correct Answer: D

The anti-exploit detection protects vulnerable endpoints from unknown exploit attacks. FortiClient monitors the behavior of popular applications, such as web browsers (Internet Explorer, Chrome, Firefox, Opera), Java/Flash plug-ins, Microsoft Office applications, and PDF readers, to detect exploits that use zero-day or unpatched vulnerabilities to infect the endpoint. Once detected, FortiClient terminates the compromised application process.