



**Free Questions for NSE5\_FCT-7.0 by go4braindumps**

**Shared by Yang on 12-12-2023**

**For More Free Questions and Preparation Resources**

**Check the Links on Last Page**

# Question 1

---

**Question Type:** MultipleChoice

---

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

Rules

↺ Default Logic

+ Add Rule

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

↺ Reset

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

**Options:**

---

- 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.

**Answer:**

---

C, D

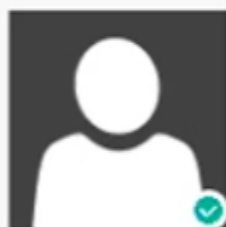
## Question 2

---

**Question Type:** MultipleChoice

---

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



## 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	Training
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
- Anti-Rans
- Cloud B
- Detection
- Sandbox
- Sandbox
- Web Filter
- Applicatio
- Remote A
- Vulnerabi
- SSOMA in

### Third Party

- Virus & T
- Protectio
- Disk Encr

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

**Options:**

---

- 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.

**Answer:**

---

B, D

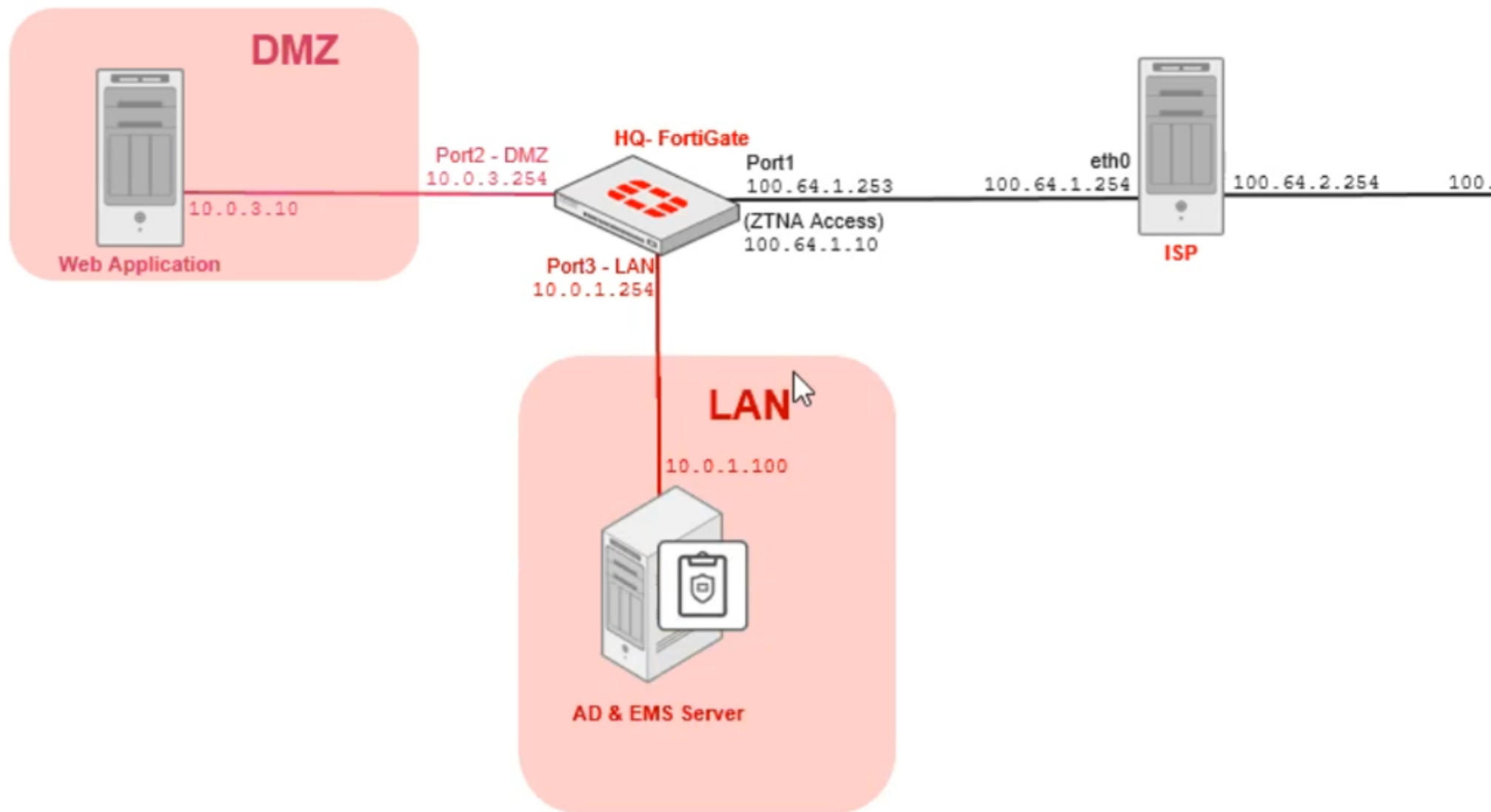
## Question 3

---

**Question Type:** MultipleChoice










---

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







Name 	ZTNA-Allow
Source	 all  +
Negate Source	<input type="checkbox"/>
ZTNA Tag	 Remote-Users  +
ZTNA Server	 ZTNA-webserver 
Negate Destination	<input type="checkbox"/>
Action	<input checked="" type="checkbox"/> ACCEPT <input type="checkbox"/> DENY
Security Profiles	
AntiVirus	<input type="checkbox"/>
Web Filter	<input type="checkbox"/>
Video Filter	<input type="checkbox"/>
Application Control	<input type="checkbox"/>
IPS	<input type="checkbox"/>
File Filter	<input type="checkbox"/>
SSL Inspection	<span>SSL</span> no-inspection  
Logging Options	
Log Allowed Traffic <input checked="" type="checkbox"/>	Security Events <input type="checkbox"/> All Sessions <input checked="" type="checkbox"/>

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?

### Options:

---

- 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.

### Answer:

---

A

### Explanation:

---

'You can use CLI Command [...] to verify the presence of matching endpoint record [...] If any of the Information is missing or incomplete, client certificate authentication might fail because FortiClient cannot locate corresponding endpoint entry.' There is probably a typo there and it should read: 'because FortiGate cannot locate corresponding endpoint entry.' --> see Admin guide for 'endpoint record list' and CLI command in that context. <https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/25915/establish-device-identity-and-trust-context-with-forticlient-ems>

## Question 4

---

**Question Type:** MultipleChoice

---

Which component or device shares device status information through ZTNA telemetry?

### Options:

---

- A- FortiClient
- B- FortiGate
- C- FortiGate Access Proxy
- D- FortiClient EMS

### Answer:

---

A

### Explanation:

---

FortiClient communicates directly with FortiClient EMS to continuously share device status information through ZTNA telemetry.

## Question 5

---

**Question Type:** MultipleChoice

---

An administrator deploys a FortiClient installation through the Microsoft AD group policy. After installation is complete, all the custom configuration is missing.

What could have caused this problem?

### Options:

---

- A- The FortiClient exe file is included in the distribution package
- B- The FortiClient MST file is missing from the distribution package
- C- FortiClient does not have permission to access the distribution package.
- D- The FortiClient package is not assigned to the group

### Answer:

---

D

## Question 6

---

Question Type: MultipleChoice

---

Refer to the exhibit.



Based on the settings shown in the exhibit what action will FortiClient take when it detects that a user is trying to download an infected file?

### Options:

---

- A- Blocks the infected files as it is downloading
- B- Quarantines the infected files and logs all access attempts
- C- Sends the infected file to FortiGuard for analysis
- D- Allows the infected file to download without scan

### Answer:

---

D

### Explanation:

---

Block Malicious Website has nothing to do with infected files. Since Realtime Protection is OFF, it will be allowed without being scanned.

## Question 7

---

**Question Type: MultipleChoice**

---

Refer to the exhibit.

```
config user fsso
  edit "Server"
    set type fortiems
    set server "10.0.1.200"
    set password ENC ebT9fHIMXIBykhWCSnG;P+Tpi/EjEdQu4hAa24LiKxHolWI7JyX
    set ssl enable
  next
end
```

Based on the CLI output from FortiGate. which statement is true?

### Options:

---

- A- FortiGate is configured to pull user groups from FortiClient EMS
- B- FortiGate is configured with local user group
- C- FortiGate is configured to pull user groups from FortiAuthenticator
- D- FortiGate is configured to pull user groups from AD Server.

### Answer:

---

A

## Question 8

---

Question Type: MultipleChoice

---

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

### Options:

---

- A- It enforces access control
- B- It redirects the client request to the access proxy
- C- It defines the access proxy
- D- It applies security profiles to protect traffic

### Answer:

---

A, D

### Explanation:

---

'A ZTNA rule is a proxy policy used to enforce access control. ZTNA tags or tag groups can be defined to enforce zero trust role based access. Security profiles can be configured to protect this traffic.'

'ZTNA rules help control access by defining users and ZTNA tags to perform user authentication and security posture checks. And just like firewall policies, you can control the source and destination addresses, and apply appropriate security profiles to scan the traffic.'

<https://docs.fortinet.com/document/fortigate/7.0.0/ztna-deployment/899992/configuring-ztna-rules-to-control-access>



## Question 9

---

**Question Type:** MultipleChoice

---

Which two benefits are benefits of using multi-tenancy mode on FortiClient EMS? (Choose two.)

### Options:

---

- A- The fabric connector must use an IP address to connect to FortiClient EMS
- B- It provides granular access and segmentation.
- C- Licenses are shared among sites.
- D- Separate host servers manage each site.

### Answer:

---

B, C

### Explanation:

---

Licenses are shared among sites: In multi-tenancy mode, licenses can be shared among the different tenant accounts or sites within FortiClient EMS. This means that a pool of licenses can be allocated and utilized across multiple sites or deployments as needed. It

helps optimize license utilization and reduces the need for individual licenses for each site or customer.

It provides granular access and segmentation: Multi-tenancy mode allows for the creation of separate tenant accounts or groups within FortiClient EMS. Each tenant can have their own set of policies, configurations, and access rights, providing granular control and segmentation. This enables organizations to manage multiple sites or customer deployments separately within a single FortiClient EMS instance.

## Question 10

---

**Question Type:** MultipleChoice

---

When site categories are disabled in FortiClient webfilter and antivirus (malicious websites), which feature can be used to protect the endpoint from malicious web access?

### Options:

---

- A- Web exclusion list
- B- Real-time protection list
- C- Block malicious websites on antivirus

**D-** FortiSandbox URL list

**Answer:**

---

A

**Explanation:**

---

Site Categories enables site categories from FortiGuard. When site categories are disabled, FortiClient is protected by the exclusion list. For all categories below, you can configure an action for the entire site category by selecting either Block, Warn, Allow, or Monitor. Each site category is shown on this slide.

**To Get Premium Files for NSE5\_FCT-7.0 Visit**

**[https://www.p2pexams.com/products/nse5\\_fct-7.0](https://www.p2pexams.com/products/nse5_fct-7.0)**

**For More Free Questions Visit**

**<https://www.p2pexams.com/fortinet/pdf/nse5-fct-7.0>**

