



Actual exam question from Fortinet's NSE5\_FCT-7.0

Question #: 1

Topic #: 1

[\[All NSE5\\_FCT-7.0 Questions\]](#)

---

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

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

Show Suggested Answer





Actual exam question from Fortinet's NSE5\_FCT-7.0

Question #: 2

Topic #: 1

[\[All NSE5\\_FCT-7.0 Questions\]](#)

---

Which statement about FortiClient comprehensive endpoint protection is true?

- A. It helps to safeguard systems from email spam.
- B. It helps to safeguard systems from advanced security threats, such as malware.
- C. It helps to safeguard systems from data loss.
- D. It helps to safeguard systems from DDoS.

Show Suggested Answer





Actual exam question from Fortinet's NSE5\_FCT-7.0

Question #: 3

Topic #: 1

[\[All NSE5\\_FCT-7.0 Questions\]](#)

---

Which two third-party tools can an administrator use to deploy FortiClient? (Choose two.)

- A. Microsoft Active Directory GPO
- B. Microsoft SCCM
- C. QR code generator
- D. Microsoft Windows Installer

Show Suggested Answer





Actual exam question from Fortinet's NSE5\_FCT-7.0

Question #: 4

Topic #: 1

[\[All NSE5\\_FCT-7.0 Questions\]](#)

---

In a FortiSandbox integration, what does the remediation option do?

- A. Deny access to a file when it sees no results
- B. Wait for FortiSandbox results before allowing files
- C. Alert and notify only
- D. Exclude specified files

Show Suggested Answer





Actual exam question from Fortinet's NSE5\_FCT-7.0

Question #: 5

Topic #: 1

[\[All NSE5\\_FCT-7.0 Questions\]](#)

---

An administrator is required to maintain a software vulnerability on the endpoints, without showing the feature on the FortiClient dashboard.

What must the administrator do to achieve this requirement?

- A. Click the hide icon on the vulnerability scan tab
- B. Use the default endpoint profile
- C. Disable select the vulnerability scan feature in the deployment package
- D. Select the vulnerability scan feature in the deployment package, but disable the feature on the endpoint profile

Show Suggested Answer





Actual exam question from Fortinet's NSE5\_FCT-7.0

Question #: 6

Topic #: 1

[\[All NSE5\\_FCT7.0 Questions\]](#)

---

An administrator deploys a FortiClient installation through the Microsoft AD group policy. After the installation is complete, all the custom configuration is missing. What could have caused this problem?

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

Show Suggested Answer



Actual exam question from Fortinet's NSE5\_FCT-7.0

Question #: 7

Topic #: 1

[\[All NSE5\\_FCT-7.0 Questions\]](#)

---

An administrator installs FortiClient on Windows Server.

What is the default behavior of real-time protection control?

- A. Real-time protection must update AV signature database.
- B. Real-time protection is disabled.
- C. Real-time protection sends malicious files to FortiSandbox when the file is not detected locally.
- D. Real-time protection must update the signature database from FortiSandbox.

Show Suggested Answer



Actual exam question from Fortinet's NSE5\_FCT-7.0

Question #: 8

Topic #: 1

[\[All NSE5\\_FCT7.0 Questions\]](#)


Refer to the exhibit, which shows the output of the ZTNA traffic log on FortiGate.

### Log Details

**General**

Absolute Date/Time 2021/11/25 08:59:18  
Time 08:59:18  
Duration 0s  
Session ID 6308  
Virtual Domain root

**Source**

IP 100.64.2.253  
Source Port 49964  
Country/Region Reserved  
Source Interface  port1  
User

**Destination**

IP 100.64.1.10  
Port 9443  
Country/Region Reserved  
Destination Interface root


**Application Control**

Application Name  
Category unscanned  
Risk undefined  
Protocol 6  
Service tcp/9443

**Data**

Received Bytes 0 B  
Received Packets 0  
Sent Bytes 0 B  
Sent Packets 0  
Message Denied: failed to match an API-gateway

**Action**

Action Deny: policy violation  
Security Action  Blocked  
Policy ID ZTNA-WAN (4)  
Policy UUID 23f88b34-4e0b-51ec-0e83-dab1019c2d5c  
Policy Type Firewall

What can you conclude from the log message?

- A. The remote user connection does not match the explicit proxy policy.
- B. The remote user connection does not match the ZTNA server configuration.
- C. The remote user connection does not match the ZTNA firewall policy.
- D. The remote user connection does not match the ZTNA rule configuration.

Show Suggested Answer





Actual exam question from Fortinet's NSE5\_FCT-7.0

Question #: 9

Topic #: 1

[\[All NSE5\\_FCT7.0 Questions\]](#)

---

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

- A. Deletes the compromised application process
- B. Blocks memory allocation to the compromised application process
- C. Terminates the compromised application process
- D. Patches the compromised application process

Show Suggested Answer



Actual exam question from Fortinet's NSE5\_FCT-7.0

Question #: 10

Topic #: 1

[\[All NSE5\\_FCT-7.0 Questions\]](#)

Refer to the exhibit.

The exhibit shows the FortiClient Web Filter configuration interface. The 'Site Categories' section is expanded, showing a list of categories with checkboxes. The 'General Interest - Personal' category is selected. Below this, a 'Web Filter Exclusions' dialog box is open, showing the following settings:

- URL: \*.facebook.com
- Action: Allow
- Type: Wildcard

At the bottom of the interface, the 'Exclusion List' is visible, showing a table with the following entry:

PERMISSION	TYPE	URL
Allow	Wildcard	*.facebook.com

Based on the settings shown in the exhibit, which action will FortiClient take when users try to access www.facebook.com?

- FortiClient will prompt a warning message to warn the user before they can access the Facebook website.
- FortiClient will block access to Facebook and its subdomains.
- FortiClient will monitor only the user's web access to the Facebook website.
- FortiClient will allow access to Facebook.

Show Suggested Answer



Actual exam question from Fortinet's NSE5\_FCT-7.0

Question #: 11

Topic #: 1

[\[All NSE5\\_FCT7.0 Questions\]](#)

---

Which component or device shares ZTNA tag information through Security Fabric integration?

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

Show Suggested Answer





Actual exam question from Fortinet's NSE5\_FCT-7.0

Question #: 12

Topic #: 1

[\[All NSE5\\_FCT-7.0 Questions\]](#)

---

Which two VPN types can a FortiClient endpoint user initiate from the Windows command prompt? (Choose two.)

- A. PPTP
- B. L2TP
- C. SSL VPN
- D. IPSec

Show Suggested Answer



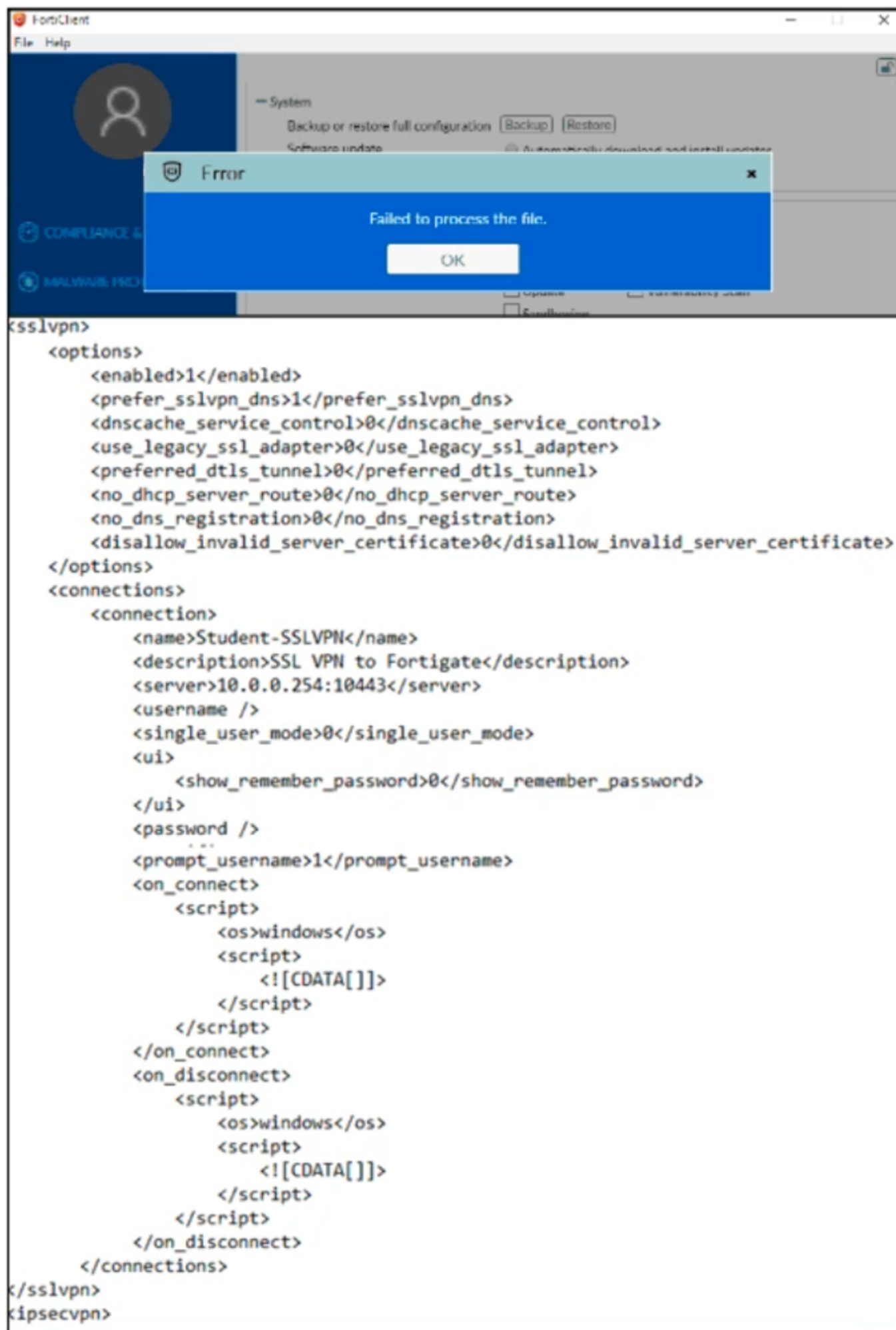
Actual exam question from Fortinet's NSE5\_FCT-7.0

Question #: 13

Topic #: 1

[\[All NSE5\\_FCT-7.0 Questions\]](#)

Refer to the exhibit.



An administrator has restored the modified XML configuration file to FortiClient and sees the error shown in the exhibit. Based on the XML settings, what must the administrator do to resolve the issue with the XML configuration file?

- A. The administrator must use a password to decrypt the file.
- B. The administrator must resolve the XML syntax error.
- C. The administrator must save the file as FortiClient-config.conf.
- D. The administrator must change the file format.

Show Suggested Answer

Actual exam question from Fortinet's NSE5\_FCT-7.0

Question #: 14

Topic #: 1

[\[All NSE5\\_FCT-7.0 Questions\]](#)

Refer to the exhibit.

**AntiVirus Protection**

**Settings**

- Scan files as they are downloaded or copied to my system
- Dynamic threat detection using threat intelligence data
- Block malicious websites
- Block known attack communication channels

**Scheduled Scan**

Schedule Type: Monthly ▾

Scan On: 1 ▾

Start:(HH:MM): 19 ▾ 30 ▾

Scan Type: Full Scan ▾

Disable Scheduled Scan

**Exclusions**

Add/remove files or folders to exclude from scanning

- C:\Desktop\Resources\

Based on the settings shown in the exhibit, which statement about FortiClient behaviour is true?

- A. FortiClient blocks and deletes infected files after scanning them.
- B. FortiClient copies infected files to the Resources folder without scanning them.
- C. FortiClient quarantines infected files and reviews later, after scanning them.
- D. FortiClient scans infected files when the user copies files to the Resources folder.

Show Suggested Answer

Actual exam question from Fortinet's NSE5\_FCT-7.0


Question #: 15

Topic #: 1

[\[All NSE5\\_FCT-7.0 Questions\]](#)

Refer to the exhibit.

Info	Deployment Service	Host WIN-EHVKBEA3S71 entered deployment state 230 (Install error-...	1 time since 2019-05-...
Error	Deployment Service	Failed to install FortiClient on fortilab.net\WIN-EHVKBEA3S71. Error c...	1 time since 2019-05-...
Info	Deployment Service	Failed to install FortiClient on fortilab.net\WIN-EHVKBEA3S71. Error code=30 (Failed to connect to the remote task service)	
Info	Deployment Service	Deploying FortiClient to fortilab.net\WIN-EHVKBEA3S71	1 time since 2019-05-...
Info	Deployment Service	There are 9 licenses available and 1 devices pending installation. Serv...	1 time since 2019-05-...
Info	Deployment Service	Host WIN-EHVKBEA3S71 entered deployment state 70 (Pending depl...	1 time since 2019-05-...
Info	Deployment Service	Host WIN-EHVKBEA3S71 entered deployment state 50 (Probed)	1 time since 2019-05-...

✖ Installer FortiClient-... No Connections  No Events

✖ Profile Fortinet-Trai...

✖ Gateway List Corp...

Based on the logs shown in the exhibit, why did FortiClient EMS fail to install FortiClient on the endpoint?

- A. The FortiClient antivirus service is not running.
- B. The Windows installer service is not running.
- C. The task scheduler service is not running.
- D. The remote registry service is not running.

Show Suggested Answer



Actual exam question from Fortinet's NSE5\_FCT-7.0

Question #: 16

Topic #: 1

[\[All NSE5\\_FCT7.0 Questions\]](#)

Refer to the exhibit.

```
xx/xx/20xx 9:05:05 AM Notice Firewall date=20xx-xx-xx time=09:05:04 logver=2 type=traffic level=notice sessionid=34252360
hostname=Win-Internal uid=C7F302B1D3EB4F05A77E38AD6202B8D7 devid=FCT8003611939390 fgtserial=FGVM010000042532 regip=N/A
srcname=firefox.exe srcproduct=Firefox srcip=10.0.1.10 srcport=62401 direction=outbound destinationip=199.59.148.82 remotename=N/A
destinationport=80 user=Administrator@TRAININGAD.TRAINING.LAB proto=6 rcvbyte=N/A sentbyte=N/A utmaction=blocked utmevent=appfirewall
threat=Twitter vd=root fctver=5.4.0.0780 os="Microsoft Windows Server 2012 R2 Standard Edition, 64-bit (build 9600)"
usingpolicy="default" service=http
```

```
xx/xx/20xx 9:05:54 AM Notice Firewall date=20xx-xx-xx time=09:05:53 logver=2 type=traffic level=notice sessionid=34252360
hostname=Win-Internal uid=C7F302B1D3EB4F05A77E38AD6202B8D7 devid=FCT8003611939390 fgtserial=FGVM010000042532 regip=N/A
srcname=firefox.exe srcproduct=Firefox srcip=10.0.1.10 srcport=62425 direction=outbound destinationip=104.25.62.28 remotename=N/A
destinationport=443 user=Administrator@TRAININGAD.TRAINING.LAB proto=6 rcvbyte=N/A sentbyte=N/A utmaction=blocked
utmevent=appfirewall threat=Proxy.Websites vd=root fctver=5.4.0.0780 os="Microsoft Windows Server 2012 R2 Standard Edition, 64-bit
(build 9600)" usingpolicy="default" service=https
```

```
xx/xx/20xx 9:28:23 AM Notice Firewall date=20xx-xx-xx time=09:28:22 logver=2 type=traffic level=notice sessionid=26453064
hostname=Win-Internal uid=C7F302B1D3EB4F05A77E38AD6202B8D7 devid=FCT8003611939390 fgtserial=FGVM010000042532 regip=N/A
srcname=firefox.exe srcproduct=Firefox srcip=10.0.1.10 srcport=62759 direction=outbound destinationip=208.71.44.31 remotename=N/A
destinationport=80 user=Administrator@TRAININGAD.TRAINING.LAB proto=6 rcvbyte=N/A sentbyte=N/A utmaction=blocked utmevent=appfirewall
threat=Yahoo.Games vd=root fctver=5.4.0.0780 os="Microsoft Windows Server 2012 R2 Standard Edition, 64-bit (build 9600)"
usingpolicy="default" service=http
```

Based on the FortiClient logs shown in the exhibit, which software application is blocked by the application firewall?

- A. Twitter
- B. Facebook
- C. Firefox
- D. Internet Explorer

Show Suggested Answer





Actual exam question from Fortinet's NSE5\_FCT-7.0

Question #: 17

Topic #: 1

[\[All NSE5\\_FCT7.0 Questions\]](#)

---

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?

- A. Web exclusion list
- B. FortiSandbox URL list
- C. Real-time protection list
- D. Block malicious websites on antivirus

Show Suggested Answer



Actual exam question from Fortinet's NSE5\_FCT-7.0

Question #: 18

Topic #: 1

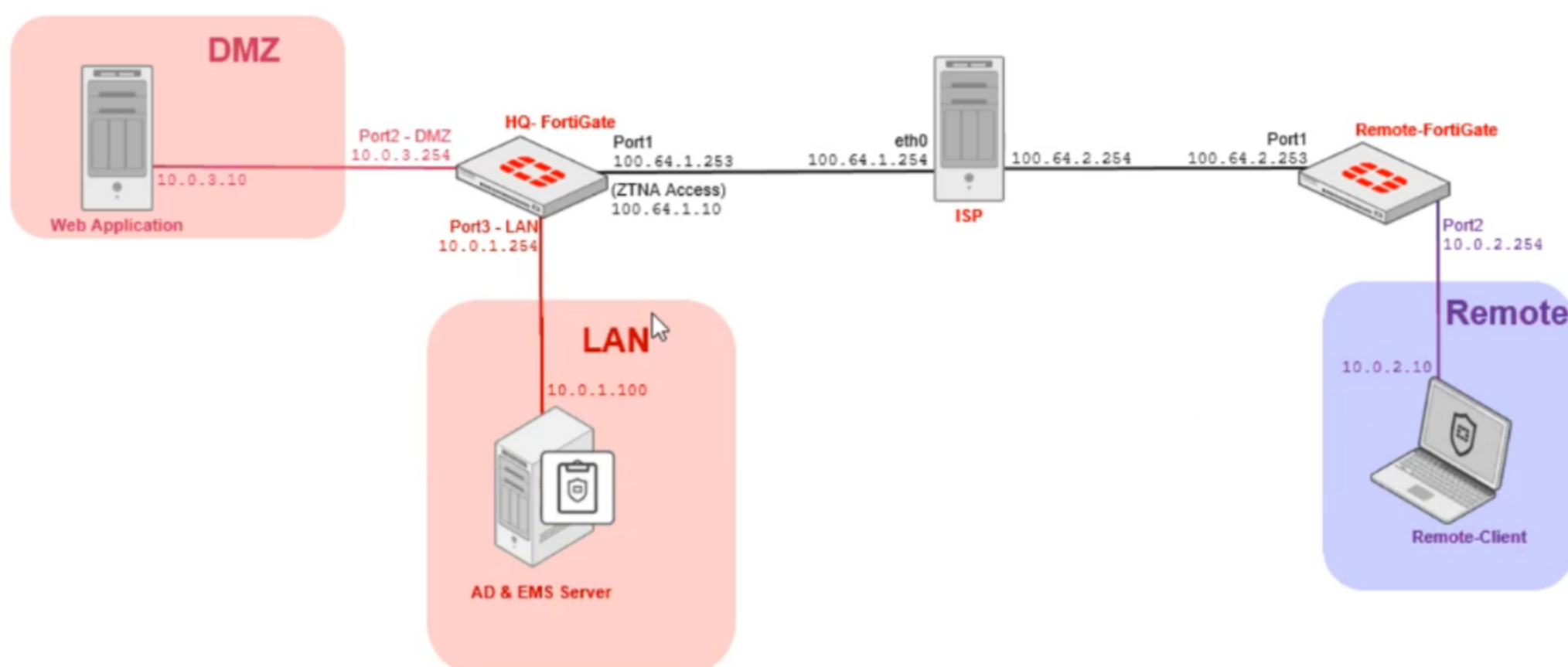
[\[All NSE5\\_FCT-7.0 Questions\]](#)

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?

Log - ZTNA Log - ZTNA



Log - ZTNA Log - ZTNA

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	SSL no-inspection
Logging Options	
Log Allowed Traffic	<input checked="" type="checkbox"/> Security Events <input checked="" type="checkbox"/> All Sessions
Comments	Write a comment... 0/1023
Enable this policy	<input checked="" type="checkbox"/>

- 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.

Show Suggested Answer

Actual exam question from Fortinet's NSE5\_FCT-7.0

Question #: 19

Topic #: 1

[\[All NSE5\\_FCT-7.0 Questions\]](#)

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

The screenshot displays the FortiClient EMS interface for an endpoint named 'Administrator'. The top navigation bar includes 'Remote-Client', 'Other Endpoints', 'Administrator', '10.0.2.20', 'Policy Default', 'EMS', 'VUL 99+', and 'SYS 1'. The main content area is divided into several sections:

- Summary:** Includes tabs for 'Webfilter Events', 'Vulnerability Events', and 'System Events'.
- Device Information:**
  - 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:** (edit icon)
  - Organization:** (edit icon)
  - 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 (with '+ Add' button)
- Status:** Managed
- Features:**
  - Antivirus installed
  - Anti-Ransomware installed
  - Cloud Based Malware Outbreak 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.

Show Suggested Answer

Actual exam question from Fortinet's NSE5\_FCT-7.0

Question #: 20

Topic #: 1

[\[All NSE5\\_FCT-7.0 Questions\]](#)

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

### Zero Trust Tagging Rule Set

Name

Tag Endpoint As ⓘ

Enabled

Comments

Rules ↻ Default Logic + Add Rule

Type	Value
<span>[-] Windows (2)</span>	
AntiVirus Software	<input type="checkbox"/> 1 AV Software is installed and running
OS Version	<input type="checkbox"/> 2 Windows Server 2012 R2 <input type="checkbox"/> 3 Windows 10

Rule Logic ⓘ

↻ Reset

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.

Show Suggested Answer





Actual exam question from Fortinet's NSE5\_FCT-7.0

Question #: 21

Topic #: 1

[\[All NSE5\\_FCT-7.0 Questions\]](#)

---

An administrator wants to simplify remote access without asking users to provide user credentials.

Which access control method provides this solution?

- A. ZTNA full mode
- B. SSL VPN
- C. L2TP
- D. ZTNA IP/MAC filtering mode

Show Suggested Answer





Actual exam question from Fortinet's NSE5\_FCT-7.0

Question #: 22

Topic #: 1

[\[All NSE5\\_FCT-7.0 Questions\]](#)

---

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

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

Show Suggested Answer





Actual exam question from Fortinet's NSE5\_FCT-7.0

Question #: 23

Topic #: 1

[\[All NSE5\\_FCT-7.0 Questions\]](#)

---

What is the function of the quick scan option on FortiClient?

- A. It scans programs and drivers that are currently running, for threats.
- B. It performs a full system scan including all files, executable files, DLLs, and drivers for threats.
- C. It allows users to select a specific file folder on their local hard disk drive (HDD), to scan for threats.
- D. It scans executable files, DLLs, and drivers that are currently running, for threats.

Show Suggested Answer





Actual exam question from Fortinet's NSE5\_FCT-7.0

Question #: 24

Topic #: 1

[\[All NSE5\\_FCT7.0 Questions\]](#)

---

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

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

Show Suggested Answer





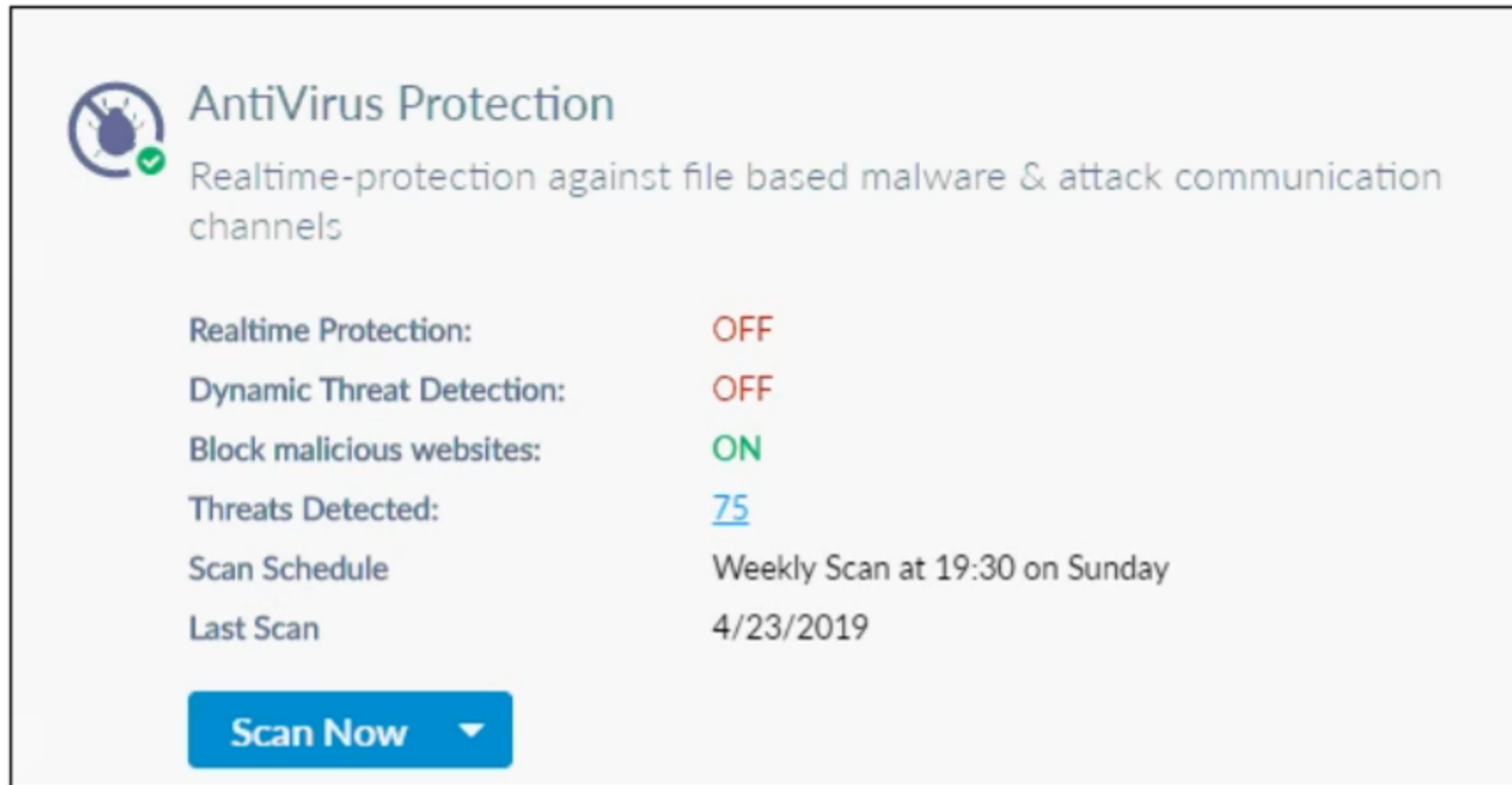
Actual exam question from Fortinet's NSE5\_FCT-7.0

Question #: 25

Topic #: 1

[\[All NSE5\\_FCT-7.0 Questions\]](#)

Refer to the exhibit.



**AntiVirus Protection**  
Realtime-protection against file based malware & attack communication channels

Realtime Protection:	OFF
Dynamic Threat Detection:	OFF
Block malicious websites:	ON
Threats Detected:	<u>75</u>
Scan Schedule	Weekly Scan at 19:30 on Sunday
Last Scan	4/23/2019

**Scan Now** ▼

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?

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

Show Suggested Answer

Actual exam question from Fortinet's NSE5\_FCT-7.0

Question #: 26

Topic #: 1

[\[All NSE5\\_FCT-7.0 Questions\]](#)

Refer to the exhibit.

The screenshot shows the configuration for a Security Fabric automation policy named 'Compromised Host Quarantine'. The policy is currently enabled. The action execution is set to 'Parallel'. The description field is empty. Below the configuration, a 'Stitch' diagram shows a 'Trigger' (represented by a biohazard icon) connected to an 'Action' (represented by a shield icon) named 'Compromised Host Quarantine\_quarantine-forticlient'. There is also an 'Add Action' button (represented by a plus icon).

Based on the Security Fabric automation settings, what action will be taken on compromised endpoints?

- A. Endpoints will be banned on FortiGate.
- B. Endpoints will be quarantined through a network device.
- C. An email notification will be sent for compromised endpoints.
- D. Endpoints will be quarantined through EMS.

Show Suggested Answer

Actual exam question from Fortinet's NSE5\_FCT-7.0

Question #: 27

Topic #: 1

[\[All NSE5\\_FCT7.0 Questions\]](#)

Refer to the exhibits, which show the Zero Trust Tag Monitor and the FortiClient GUI status.

The image shows two screenshots from the FortiClient management interface. The top screenshot is the 'Zero Trust Tag Monitor' page, which displays a table of endpoints. The bottom screenshot is the FortiClient GUI status page for the 'Remote-Client' endpoint.

**Zero Trust Tag Monitor Screenshot:**

FortiClient Endpoint Management Server

Endpoint with Tag

Remote-Users (1)

Endpoint	User	IP	Tagged on
Remote-Client	Administrator	10.0.2.20	2021-09-30 09:12:53

**FortiClient GUI Screenshot:**

FortiClient -- Zero Trust Fabric Agent

Administrator

ZERO TRUST TELEMETRY

REMOTE ACCESS

ZTNA CONNECTION RULES

VULNERABILITY SCAN

Notifications

Settings

About

Add Full Name

Phone Add Phone

Email Add Email

Get personal info from

- User Input
- OS Updated 9/30/2021 8:56:21 AM
- LinkedIn
- Google
- Salesforce

Status Online/Off-fabric

Hostname REMOTE-CLIENT

Domain

Remote-Client is tagged as Remote-Users on the FortiClient EMS Zero Trust Tag Monitor.

What must an administrator do to show the tag on the FortiClient GUI?

- Change the FortiClient system settings to enable tag visibility.
- Update tagging rule logic to enable tag visibility.
- Change the user identity settings to enable tag visibility.
- Change the endpoint control setting to enable tag visibility.

Show Suggested Answer

Actual exam question from Fortinet's NSE5\_FCT-7.0

Question #: 28

Topic #: 1

[\[All NSE5\\_FCT-7.0 Questions\]](#)

---

An administrator configures ZTNA configuration on the FortiGate for remote users.

Which statement is true about the firewall policy?

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

Show Suggested Answer





Actual exam question from Fortinet's NSE5\_FCT-7.0

Question #: 29

Topic #: 1

[\[All NSE5\\_FCT-7.0 Questions\]](#)

---

Why does FortiGate need the root CA certificate of FortiClient EMS?

- A. To update FortiClient client certificates
- B. To trust certificates issued by FortiClient EMS
- C. To revoke FortiClient client certificates
- D. To sign FortiClient CSR requests

Show Suggested Answer





Actual exam question from Fortinet's NSE5\_FCT-7.0

Question #: 30

Topic #: 1

[\[All NSE5\\_FCT-7.0 Questions\]](#)

---

Which statement about the FortiClient enterprise management server is true?

- A. It receives the configuration information of endpoints from FortiGate.
- B. It provides centralized management of multiple endpoints running FortiClient software.
- C. It receives the CA certificate from FortiGate to validate client certificates.
- D. It enforces compliance on the endpoints using tags.

Show Suggested Answer

