EXAMTOPICS

- Expert Verified, Online, **Free**.

Question #1 *Topic 1*

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

A. FortiClient

B. FortiGate

C. FortiGate Access Proxy

D. FortiClient EMS

**Suggested Answer:** *D*

*Community vote distribution*

A (100%)

**BrunoLu** Highly Voted 1 year, 6 months ago

A is correct,Pag 235

upvoted 7 times

**FlyFish_JD** Most Recent 3 months, 2 weeks ago

In the study guide, it is said:

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

Apparently, it is FortiClient sharing the device status with EMS.

upvoted 1 times

**3ecbf33** 5 months, 1 week ago

A is correct page 235

upvoted 1 times

**Alinutzu** 5 months, 2 weeks ago

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

upvoted 1 times

**Wanduka** 11 months, 3 weeks ago

I believe is A

upvoted 4 times

**soporte127** 1 year, 4 months ago

is opcion A:

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

upvoted 2 times

**anilsol** 1 year, 8 months ago

When On-net and Off-net FortiClient endpoints register to FortiClient EMS, device information, log on user information, and security posture are all shared over ZTNA telemetry with the EMS server.

upvoted 1 times

**Ah_Leb** 1 year, 8 months ago

**Selected Answer: A**

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

upvoted 4 times

> **cihansan** 1 year, 6 months ago
>
> so, correct answer D. FortiClient EMS right?
>
> upvoted 1 times
>
> > **soporte127** 1 year, 5 months ago
> >
> > is A or D ?
> >
> > upvoted 1 times

Question #2 *Topic 1*

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.

**Suggested Answer:** *B*

*Community vote distribution*

B (100%)

**Ah_Leb** 1 year, 8 months ago

**Selected Answer: B**

FortiClient provides comprehensive endpoint protection for your Windows-based, Mac-based, and Linuxbased desktops, laptops, file servers, and mobile devices such as iOS and Android. It helps you to safeguard
your systems with advanced security technologies, all of which you can manage from a single management
console.

upvoted 3 times

**Armando1985** 1 year, 9 months ago

**Selected Answer: B**

FortiClient has enhanced capabilities for the detection of malware. The protection includes antivirus protection, anti-ransomware, cloud-based malware protection, anti-exploit and removable media access

upvoted 4 times

Question #3 *Topic 1*

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

**Suggested Answer:** *AB*

*Community vote distribution*

AB (100%)

**jr01239a** Highly Voted 1 year, 6 months ago

A&B - https://docs.fortinet.com/document/forticlient/7.2.0/ems-administration-guide/374506/initially-deploying-forticlient-software-to-endpoints

upvoted 5 times

**Ah_Leb** Most Recent 1 year, 8 months ago

**Selected Answer: AB**

I think it's AB

upvoted 3 times

Question #4 *Topic 1*

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

**Suggested Answer:** *C*

*Community vote distribution*

C (100%)

**Ah_Leb** Highly Voted 👍 1 year, 7 months ago

Selected Answer: C

Under 'Remediation Options' section, there are only two options (Quarantine infected files, Alert & Notify only). https://docs.fortinet.com/document/forticlient/6.0.0/administration-guide/657996/configuring-submission-access-and-remediation#:~:text=disable%20this%20feature.-,Remediation%20Options,-Quarantine%20infected%20files

upvoted 6 times

**dawni** 4 months, 3 weeks ago

yes, I think it is C, although it had to wait to FortiSandbox veredict, finally the options on Remediation are just those 2: https://docs.fortinet.com/document/forticlient/7.2.0/ems-administration-guide/836582/sandbox (quarantine or Alert&Notify)

upvoted 1 times

**FlyFish_JD** Most Recent ⊙ 3 months, 2 weeks ago

In the Study Guide, it is said:

"The Remediation Actions setting allows you to select either Quarantine or Alert & Notify when a malicious file is detected."

Since the answers do not have the Quarantine option, answer C is the correct one.

upvoted 1 times

**stevefltr** 1 year, 5 months ago

Selected Answer: C

P.191 of FCT Study Guide 7.0

upvoted 2 times

**Tomer676** 1 year, 7 months ago

The Answer IS B
Wait for FortiSandbox results before allowing file access

see fortinet docs: https://docs.fortinet.com/document/forticlient/6.0.0/administration-guide/657996/configuring-submission-access-and-remediation

upvoted 2 times

**colcorn** 11 months ago

I agree with this. Alert & Notify is one of the things remediation options can do. Both options must wait for fortisandbox to process the results before doing either option.

upvoted 1 times

**BrunoLu** 1 year, 6 months ago

according the link,the Answer is C

upvoted 2 times

Question #5 *Topic 1*

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

**Suggested Answer:** *D*

*Community vote distribution*

A (100%)

⊟ **mordechayd** Highly Voted 👍 1 year, 7 months ago

Selected Answer: A

the correct answer is A , to hide a feature you can click on the hide (eye) icon on the top of the profile

upvoted 10 times

⊟ **elo1234** Highly Voted 👍 1 year, 6 months ago

Selected Answer: A

Correct answer is A. In EMS tabs Endpont profiles>Manage profiles> Profile>Vulterability Scan>click on eye icon.

upvoted 7 times

⊟ **jmunr88** Most Recent 🕘 9 months ago

correct answer is A. Page 207. "you can use the eye icon to show or hide features in the end user's view on Forticlient. When you select hide, the feature still runs in the background, but the endpoint user cannot see it. This is very useful when you are inspecting traffic without the user's knowledge."

upvoted 1 times

⊟ **DonDaddaRhymes** 9 months, 1 week ago

Selected Answer: A

It's A, however knowing FortiClient it's always bugged showing different features on different clients with same settings haha

upvoted 2 times

⊟ **Eggrolls** 1 year, 1 month ago

Selected Answer: A

Answer is A

page 179 Study Guide

upvoted 5 times

⊟ **Cyberdaso** 1 year, 3 months ago

The correct answer is A

upvoted 5 times

⊟ **stevefltr** 1 year, 5 months ago

Selected Answer: A

Correct answer is A

upvoted 6 times

Question #6 *Topic 1*

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.

**Suggested Answer:** *B*

*Community vote distribution*

A (100%)

⊟ **Olivier_A** Highly Voted 👍 1 year, 2 months ago

**Selected Answer: A**

Study Guide p.49

upvoted 5 times

⊟ **pqdmoraes** Most Recent 🕒 8 months ago

**Selected Answer: A**

A is correct. A transform file (.mst) is file that passes customized configuration settings to the MSI installer package. p. 49 study guide 7.0 (both files must be available, MSI and MST)

upvoted 2 times

⊟ **foobarasdf123** 1 year, 1 month ago

**Selected Answer: A**

Installation .msi File is beeing provided as default only from EMS Server. Customization is implemented by .mst Transform File

upvoted 4 times

Question #7 *Topic 1*

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.

**Suggested Answer:** *B*

*Community vote distribution*

B (100%)

**Eggrolls** 1 year, 1 month ago

**Selected Answer: B**

Answer is B
Study Guide page 181

upvoted 3 times

**Eggrolls** 1 year, 1 month ago

**Selected Answer: B**

Tested it multiple time. Answer B is correct.

upvoted 2 times

**Ah_Leb** 1 year, 4 months ago

**Selected Answer: B**

By default, Malware Protection (including Realtime-protection) is disabled on the FortiClient EMS Default endpoint profile.

upvoted 2 times

**jr01239a** 1 year, 6 months ago

B. FortiClient automatically disables realtime protection when:

The OS is a server, or
Exchange Server is detected, or
SQL Server is detected.

https://docs.fortinet.com/document/forticlient/6.0.0/administration-guide/609339/microsoft-windows-computer

upvoted 3 times

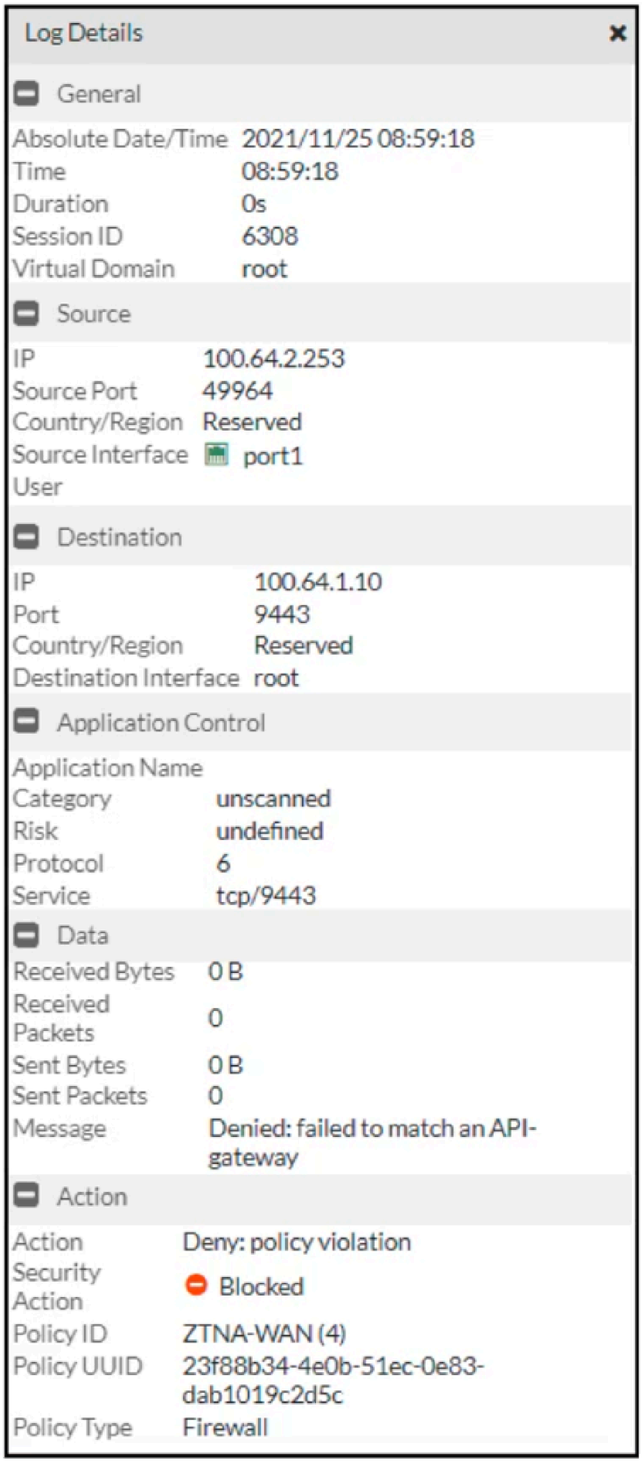
**tachy_22** 1 year, 6 months ago

Forticlient automatically disables RTP after installation when one of the following is true: The OS is a server, Exchanger Server is detected and SQL Server is detected (Pag181)

upvoted 1 times

Question #8 Topic 1

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.

**Suggested Answer:** *C*

*Community vote distribution*

B (100%)

**Tomer676** Highly Voted 1 year, 7 months ago

The Answer is C

API gateway cannot be matched:

When connecting to the ZTNA access proxy, the client tries to connect to an API gateway that does not match any virtual host.

take from fortinet Docs: https://docs.fortinet.com/document/fortigate/7.0.0/new-features/608477/ztna-logging-enhancements-7-0-1

Its meen that is no firewall policy to the server that client want to access

upvoted 7 times

**jr01239a** Highly Voted 1 year, 6 months ago

C.

Empty Client Certificate = "Denied: empty client certificate"
Failed Client Certificate = "Denied: client certificate authentication failed"
API gateway that does not match any virtual host = "Denied: failed to match an API-gateway"
API gateway but the real server cannot be reached = "Denied: failed to match an API-gateway"
A ZTNA rule (proxy policy ) cannot be matched = "Denied: failed to match a proxy-policy"
HTTPS SNI virtual host does not match the HTTP host header = "Denied: failed to match an API-gateway"

=======================
Wrong Access Proxy
Right Access Proxy, down/missing Real Server
Right Access Proxy, wrong URI

======================
ZTNA Server = defines the access proxy VIP and the real servers that clients will connect to
ZTNA Rule (Proxy Policy) = enforce access control
Firewall Policy (Full ZTNA) = The firewall policy matches and redirects client requests to the access proxy VIP.

upvoted 5 times

**Wanduka** Most Recent 11 months, 3 weeks ago

More than one answer seems right. Any additional comments?

upvoted 1 times

**johnnd** 1 year, 1 month ago

Selected Answer: B

Page 286 of study Guide.

upvoted 2 times

**erosramos322** 1 year, 1 month ago

Selected Answer: B

API gateway cannot be matched or real servers cannot be reached

upvoted 3 times

**aguilazoo** 1 year, 7 months ago

Selected Answer: B

The aswer is B

upvoted 3 times

**mhizha** 1 year, 8 months ago

The answer is D.

Page 238 of the study guide reads, "This slide shows the UTM and traffic logs that are generated when FortiGate connects to the ZTNA access proxy but is unable to match the ZTNA rule (proxy policy). For example, no ZTNA rule is matched for the ZTNA tag assigned to the endpoint."

I had now way to paste the slide but if you check page 238 you will see the slide with the logs.

upvoted 1 times

**Eggrolls** 1 year, 1 month ago

I think he meant page 286 Study Guide seems its B

upvoted 2 times

Question #9 *Topic 1*

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

**Suggested Answer:** *C*

*Community vote distribution*

C (100%)

**Ah_Leb** Highly Voted 1 year, 7 months ago

Selected Answer: C

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.

upvoted 8 times

**BrunoLu** 1 year, 6 months ago

pag 190

upvoted 2 times

**Ciscopass** Most Recent 1 year ago

Selected Answer: C

Answer is C

upvoted 3 times

**Olivier_A** 1 year, 2 months ago

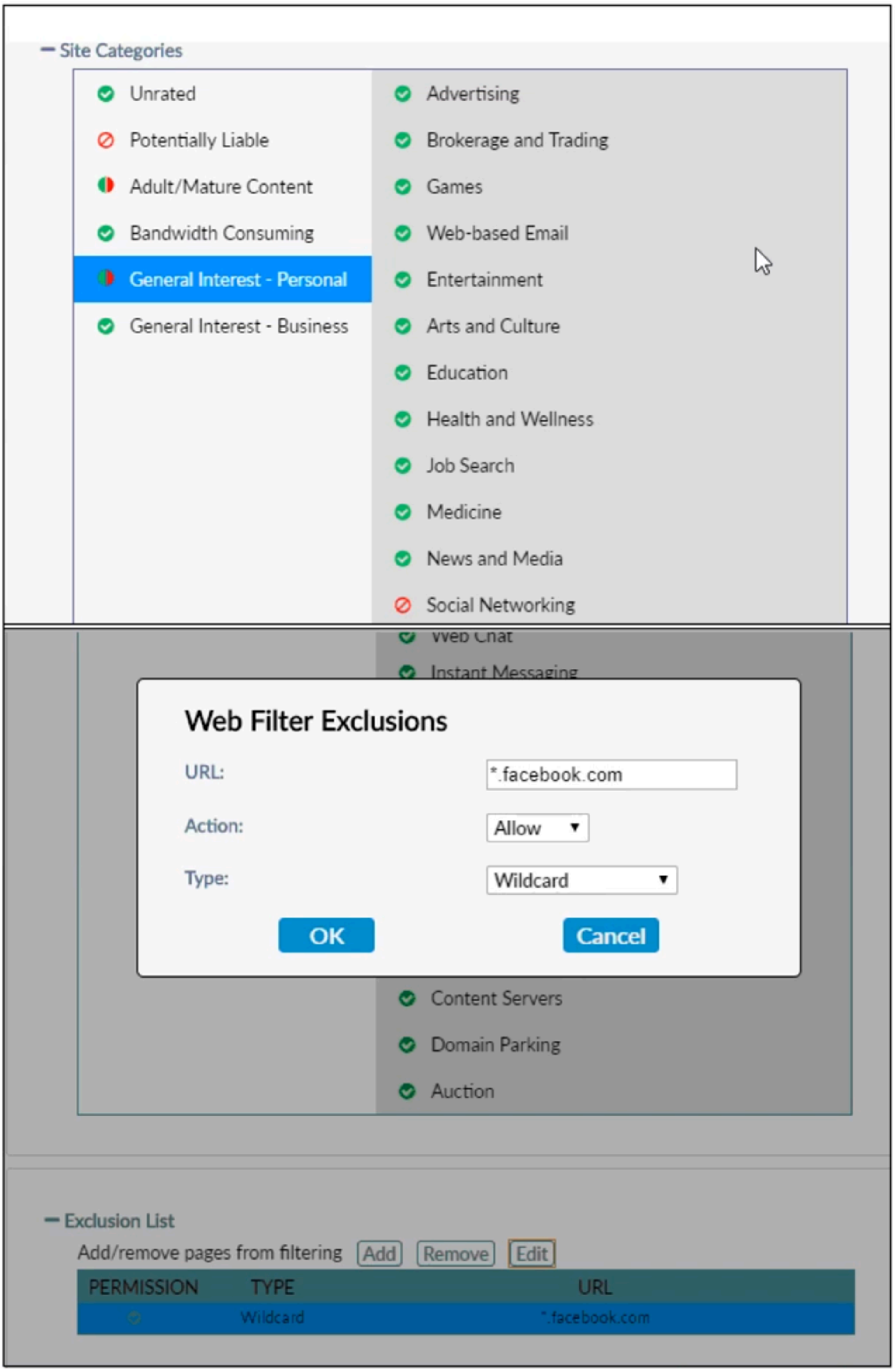
Selected Answer: C

Study Guide P.190

upvoted 3 times

## Question #10 *Topic 1*

Refer to the exhibit.



**− Site Categories**

- ✓ Unrated
- ⊘ Potentially Liable
- ◐ Adult/Mature Content
- ✓ Bandwidth Consuming
- ◐ General Interest - Personal
- ✓ General Interest - Business

- ✓ Advertising
- ✓ Brokerage and Trading
- ✓ Games
- ✓ Web-based Email
- ✓ Entertainment
- ✓ Arts and Culture
- ✓ Education
- ✓ Health and Wellness
- ✓ Job Search
- ✓ Medicine
- ✓ News and Media
- ⊘ Social Networking
- ✓ Web Chat
- ✓ Instant Messaging
- ✓ Content Servers
- ✓ Domain Parking
- ✓ Auction

**Web Filter Exclusions**

URL: *.facebook.com

Action: Allow

Type: Wildcard

**− Exclusion List**

Add/remove pages from filtering

| PERMISSION | TYPE | URL |
|---|---|---|
| ✓ | Wildcard | *.facebook.com |

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

A. FortiClient will prompt a warning message to warn the user before they can access the Facebook website.

B. FortiClient will block access to Facebook and its subdomains.

C. FortiClient will monitor only the user’s web access to the Facebook website.

D. FortiClient will allow access to Facebook.

**Suggested Answer:** *D*

*Community vote distribution*

D (100%)

**Eggrolls** 1 year, 1 month ago

**Selected Answer: D**

I think its D

Study Guide page 202

upvoted 3 times

**soporte127** 1 year, 4 months ago

is the option d

upvoted 3 times

Question #11 *Topic 1*

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

A. FortiClient

B. FortiClient EMS

C. FortiGate

D. FortiGate Access Proxy

**Suggested Answer:** *B*

*Community vote distribution*

B (100%)

**Ah_Leb** Highly Voted 1 year, 7 months ago

**Selected Answer: B**

Based on the Study_Guide from training.fortinet.com, FortiClient EMS shares the tag information with FortiGate through Security Fabric integration.

upvoted 6 times

**soporte127** 1 year, 5 months ago

why no c ?

upvoted 1 times

**arleekhan** 1 year, 4 months ago

FortiClient EMS Monitor ZTNA Rules and Shared ZTNA Tags to Any Device of Security Fabric. Answer is B

upvoted 2 times

**Brand0n** Most Recent 11 months, 1 week ago

B / Study Guide page.235

upvoted 1 times

**almade17** 1 year, 4 months ago

FortiClient EMS comparte la información de la etiqueta con FortiGate a través de la integración de Security Fabric. FortiClient se comunica directamente con FortiClient EMS para compartir continuamente la información del estado del dispositivo a través de la telemetría ZTNA

Study_guide pp 235

upvoted 2 times

**soporte127** 1 year, 4 months ago

Is option B:

*FortiClient EMS* shares the tag information with FortiGate through Security Fabric integration.

upvoted 4 times

**Tomer676** 1 year, 7 months ago

The Answer Is C

Because this is a test on EMS, they mean which other component in the network shares the TAG, and according to Fortinet's articles, it means FortiGate

See Fortinet Docs: https://docs.fortinet.com/document/fortigate/7.2.3/administration-guide/335228/synchronizing-forticlient-ztna-tags

upvoted 1 times

Question #12 *Topic 1*

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

**Suggested Answer:** *CD*

*Community vote distribution*

CD (100%)

**Olivier_A** 1 year, 2 months ago

**Selected Answer: CD**

Study Guide P.32

upvoted 3 times

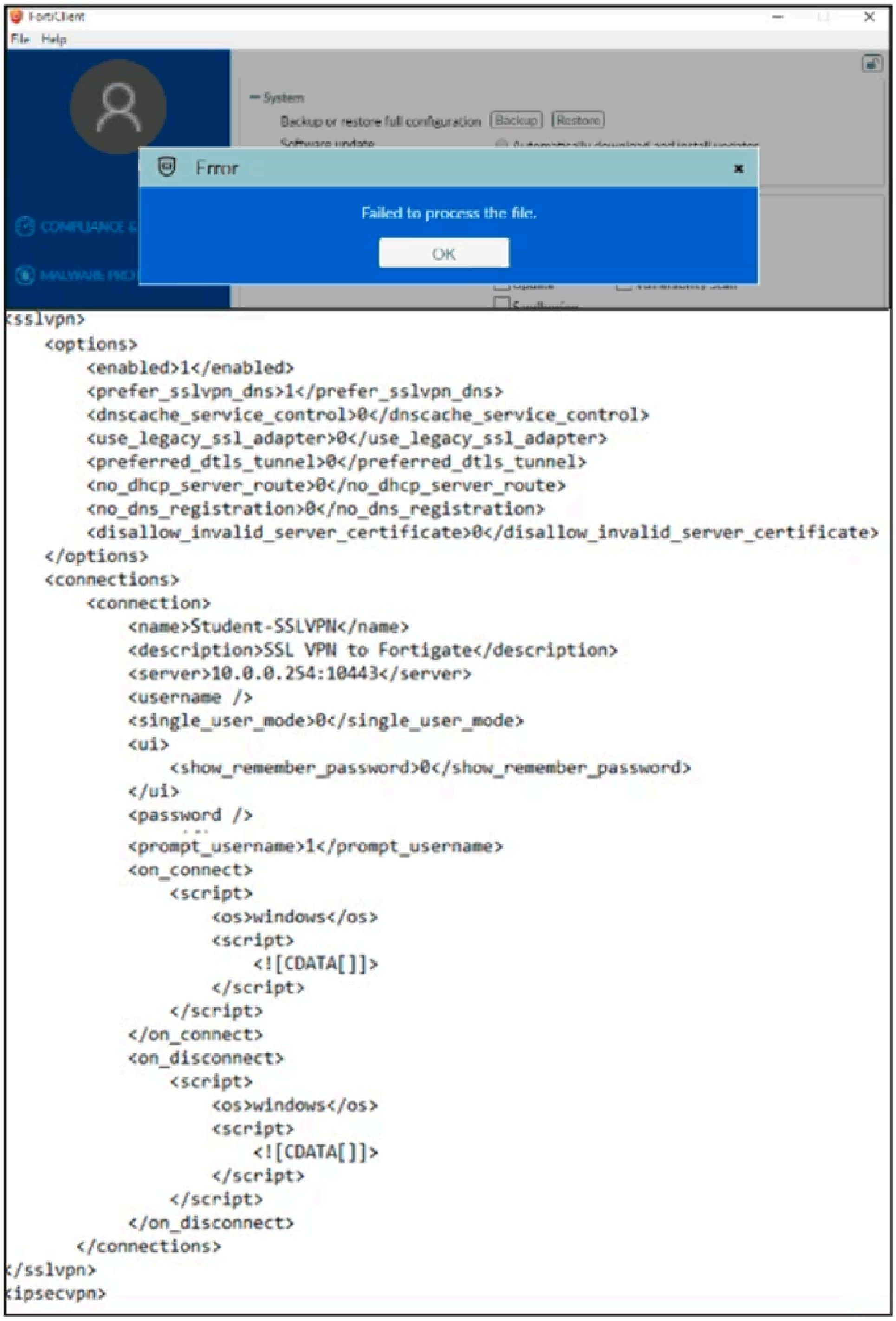
**soporte127** 1 year, 5 months ago

is for my CD

upvoted 3 times

## Question #13 *Topic 1*

Refer to the exhibit.



Failed to process the file.

```
<sslvpn>
    <options>
        <enabled>1</enabled>
        <prefer_sslvpn_dns>1</prefer_sslvpn_dns>
        <dnscache_service_control>0</dnscache_service_control>
        <use_legacy_ssl_adapter>0</use_legacy_ssl_adapter>
        <preferred_dtls_tunnel>0</preferred_dtls_tunnel>
        <no_dhcp_server_route>0</no_dhcp_server_route>
        <no_dns_registration>0</no_dns_registration>
        <disallow_invalid_server_certificate>0</disallow_invalid_server_certificate>
    </options>
    <connections>
        <connection>
            <name>Student-SSLVPN</name>
            <description>SSL VPN to Fortigate</description>
            <server>10.0.0.254:10443</server>
            <username />
            <single_user_mode>0</single_user_mode>
            <ui>
                <show_remember_password>0</show_remember_password>
            </ui>
            <password />
            <prompt_username>1</prompt_username>
            <on_connect>
                <script>
                    <os>windows</os>
                    <script>
                        <![CDATA[]]>
                    </script>
                </script>
            </on_connect>
            <on_disconnect>
                <script>
                    <os>windows</os>
                    <script>
                        <![CDATA[]]>
                    </script>
                </script>
            </on_disconnect>
       </connections>
</sslvpn>
<ipsecvpn>
```

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.

**Suggested Answer:** *B*

*Community vote distribution*

B (100%)

**mda2h** 11 months, 2 weeks ago

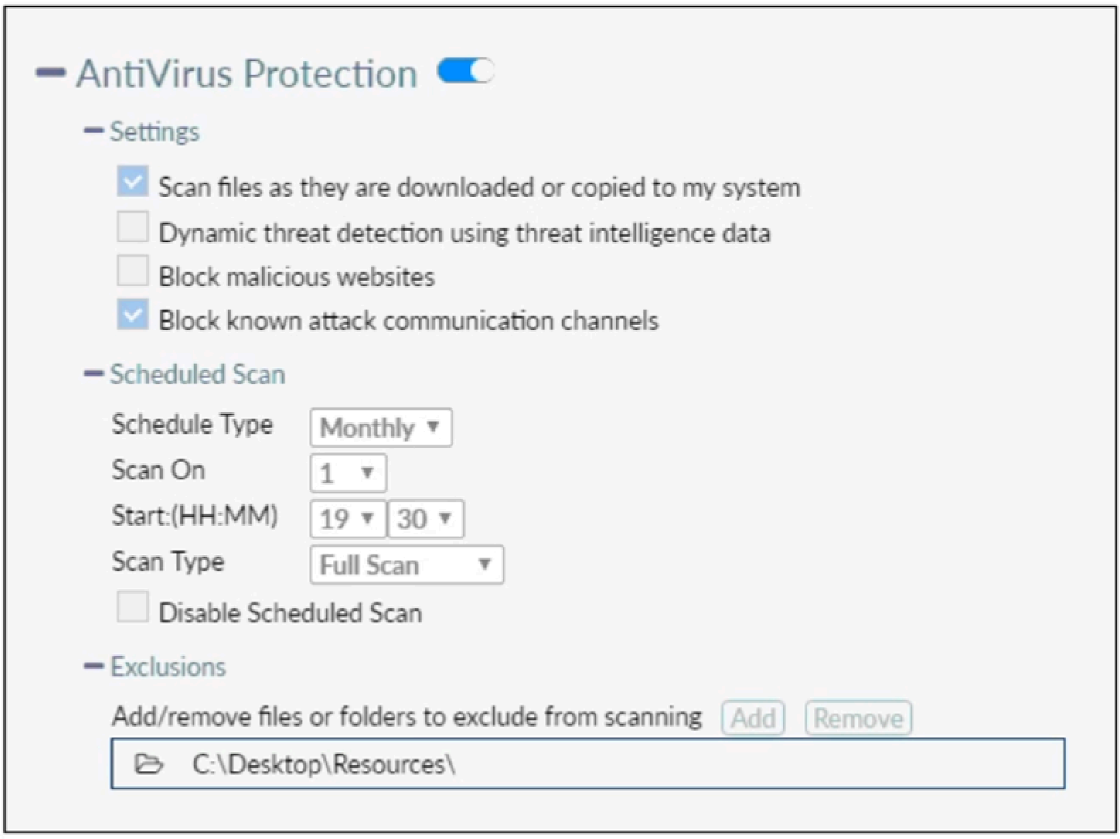
**Selected Answer: B**

missing </connections> at the bottom

upvoted 2 times

Question #14 *Topic 1*

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 [Add] [Remove]

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.

**Suggested Answer:** *A*

*Community vote distribution*

C (65%) B (35%)

**Tomer676** Highly Voted 1 year, 7 months ago

The Answer Is C

The FortiClient does not delete the file, it quarantines the file for its inspection, then after X days it is deleted

upvoted 9 times

**baasjasper** Highly Voted 1 year, 3 months ago

**Selected Answer: C**

among the options provided, the statement that aligns with typical FortiClient behavior is:

C. FortiClient quarantines infected files and reviews them later after scanning them.

upvoted 5 times

**piipo** Most Recent 7 months, 3 weeks ago

**Selected Answer: C**

Answer Is C

upvoted 1 times

**jmunr88** 10 months ago

C is correct page 186

upvoted 2 times

**mda2h** 11 months, 2 weeks ago

**Selected Answer: C**

I correct my previous answer

B. is false, it's not FortiClient that copies the file, the OS does it

Answer is C

upvoted 2 times

**mda2h** 11 months, 2 weeks ago

**Selected Answer: B**

A. False = what is deleted in Full Scan are rootkits, while files are only scanned

C. False= two choices when infected fiels is detected: deny access or quarantine. If choose quarantine, multiple options are possible including, restore, delete, submit to FortiGuard ...etc default action is not to rescan later

D. False = the folder is in the exclusion list, files/folders added there are not scanned

upvoted 1 times

**foobarasdf123** 1 year ago

**Selected Answer: B**

Should be B. See study Guide FCT7.0 p. 184

"If you want to exclude specific files or folders from the anti virus scan, but still want to perform an antivirus scan on the rest of the system, you can configure an exclusion list. The files and folders that you add to this list are excluded from antivirus scanning."

upvoted 2 times

> **DonDaddaRhymes** 9 months, 1 week ago
>
> Read the answer again..... it says "FortiClient copies infected files to the Resources folder without scanning them." why in earth would FortiClient copy infected files to a excluded folder? that sounds like a huge vulnerability within forticlient haha...
>
> upvoted 1 times

**Eggrolls** 1 year, 1 month ago

**Selected Answer: C**

Answer seems C not A

Action On Virus Discovery

Warn the User If a Process Attempts to Access Infected Files

Quarantine Infected Files. You can use FortiClient to view, restore, or delete the quarantined file, as well as view the virus name, submit the file to FortiGuard, and view logs.

Deny Access to Infected Files

Ignore Infected Files

upvoted 3 times

**tachy_22** 1 year, 5 months ago

C is correct.

Resources Folder is excluded in the Full Scan so B and D are false. If Full Scan detects infected file moves to the quarantine so A is false too.

upvoted 5 times

**BrunoLu** 1 year, 6 months ago

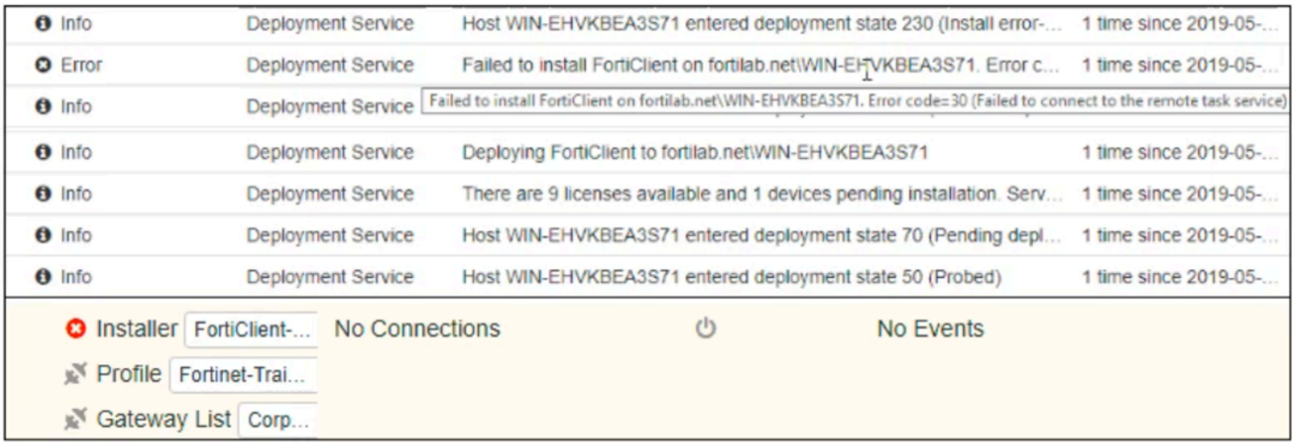
**Selected Answer: B**

Resources folder is exclude,so it will not scan

upvoted 3 times

Question #15 Topic 1

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.

**Suggested Answer:** *C*

*Community vote distribution*

C (100%)

**Skey** 1 year, 1 month ago

**Selected Answer: C**

https://community.fortinet.com/t5/FortiClient/Technical-Note-FortiClient-fails-to-install-from-FortiClient-EMS/ta-p/193680

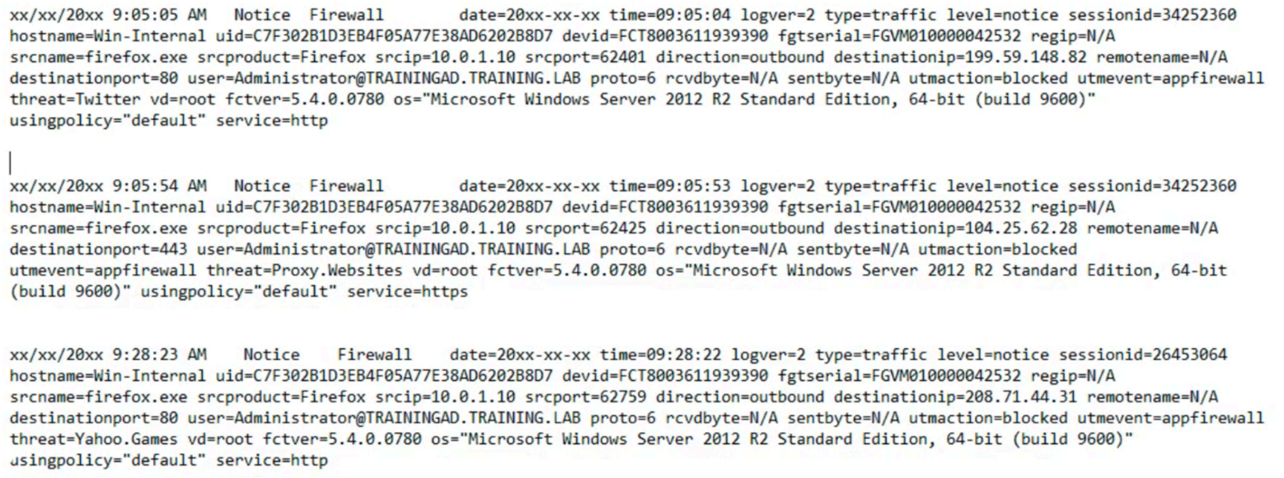
The deployment service error message may be caused by any of the following. Try eliminating them all, one at a time.

1. Wrong username or password in the EMS profile
2. Endpoint is unreachable over the network
3. Task Scheduler service is not running
4. Remote Registry service is not running
5. Windows firewall is blocking connection

upvoted 4 times

Question #16 Topic 1

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 rcvdbyte=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 rcvdbyte=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 rcvdbyte=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

**Suggested Answer:** *C*

*Community vote distribution*

C (65%) A (35%)

**soporte127** Highly Voted 1 year, 5 months ago

is A (twitter)

upvoted 5 times

**soporte127** 1 year, 5 months ago

pag. 342

upvoted 5 times

**BrunoLu** Highly Voted 1 year, 6 months ago

**Selected Answer: C**

it blocked the trffic about Twitter□Proxy website□Yahoo.Game, and all of this triffic run on the Firefox

upvoted 5 times

**arleekhan** 1 year, 4 months ago

I think so.

upvoted 2 times

**dalmiroy2k** Most Recent 4 months, 3 weeks ago

**Selected Answer: A**

It's a trick question. Firefox.exe is not something you can block in Application firewall categories.

upvoted 1 times

**piipo** 7 months, 3 weeks ago

**Selected Answer: C**

The question asked is not the destination but the software blocked on the device, and the correct answer is Firefox.

upvoted 2 times

**belcher29** 11 months, 1 week ago

**Selected Answer: C**

The question is asking what software application is being blocked. Not the category specified in the firewall rule. C, Firefox.

upvoted 4 times

**nimesh_netco** 11 months, 3 weeks ago

**Selected Answer: A**

The answer is A. Study Guide P.342

upvoted 1 times

**foobarasdf123** 1 year, 1 month ago

**Selected Answer: A**

These are Application Firewall Logs. Therefore Application Signatures match. In this Case the Application is Twitter (via HTTP)

upvoted 2 times

**Olivier_A** 1 year, 2 months ago

**Selected Answer: A**

A is the correct Answer. P.342 on Study Guide

upvoted 4 times

**baasjasper** 1 year, 3 months ago

**Selected Answer: C**

Source app is firefox.exe (twitter and yahoo are blocked, within the app; firefox.)

so answer is C!

upvoted 4 times

**Lyanne** 1 year, 4 months ago

A (twitter)

upvoted 4 times

**tachy_22** 1 year, 5 months ago

A is correct. Threat=Twitter

If firefox were we would see in the exported log threat=HTTP.BROWSER_Firefox.

upvoted 3 times

> **DonDaddaRhymes** 9 months, 1 week ago
>
> Yes true, but question says "in this log" so could be interpreted as the used application which makes it C tricky question. I honestly still think that fortinet means A. Twitter
>
> upvoted 1 times

**Tomer676** 1 year, 7 months ago

The Answer is A

the Twitter was Blocked

see line 5 in the exibit

upvoted 2 times

Question #17 *Topic 1*

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

**Suggested Answer:** *A*

*Community vote distribution*

A (86%) 14%

**myrmidon3** 2 months, 2 weeks ago

**Selected Answer: A**

The Categories setting enables site categories from FortiGuard. When site categories are disabled, FortiClient is protected by the exclusion list. For all categories in this section, you can configure an action for the entire site category by selecting either Block, Warn, Allow, or Monitor.
FortiClient EMS 7.2 Administrator Study Guide p215

upvoted 1 times

**johnnd** 1 year, 1 month ago

**Selected Answer: C**

page 183 from the study guide.
"Block malicious websites blocks all access to malicious websites."

upvoted 1 times

**mlopin** 1 year, 1 month ago

Answer A ,
the question is about WebFilter AND Antivirus
check P201, "Enable webfiltering on forticlient ... affects the block access to malicious websites setting in antivirus protection"
it seems like a priority on webfilter, so answer should be A

upvoted 1 times

**Olivier_A** 1 year, 2 months ago

**Selected Answer: A**

Study Guide P.201

upvoted 1 times

**almade17** 1 year, 4 months ago

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.

upvoted 2 times

**Ah_Leb** 1 year, 4 months ago

**Selected Answer: A**

When site categories are disabled, FortiClient is protected by the exclusion list. Study guide page 201.

upvoted 2 times

**elo1234** 1 year, 5 months ago

**Selected Answer: A**

A is correct. -> "
You can enable or disable Site Categories in the Web Filter settings page. When site categories are disabled, the exclusion list protects FortiClient."

upvoted 2 times

**tachy_22** 1 year, 5 months ago

A is correct. You can configure a exclusion list to block a specific website in the Web Filter when you have disabled Site Categories.

upvoted 2 times

⊟ **Tomer676** 1 year, 7 months ago

See the question

its not Blockd, its DISABLE

so the answer is C

the Real-time protection list can blocked

upvoted 3 times

⊟ **johnnd** 1 year, 1 month ago

Yup, page 183 from the study guide.

"Block malicious websites blocks all access to malicious websites."

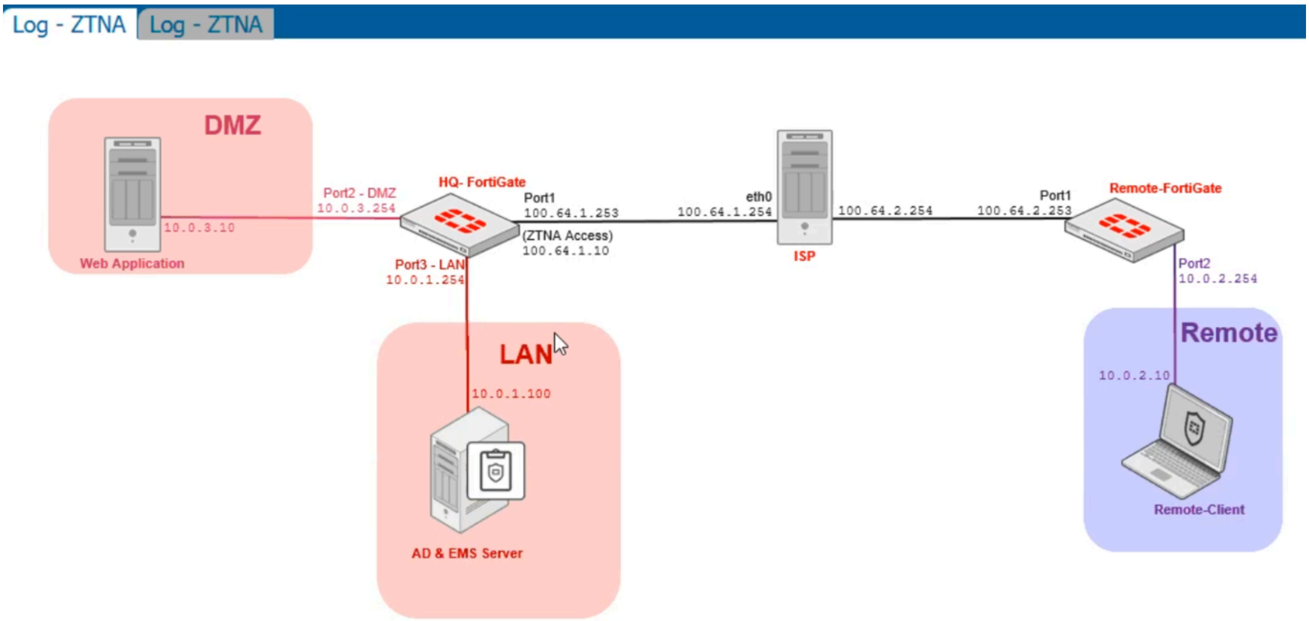
upvoted 1 times

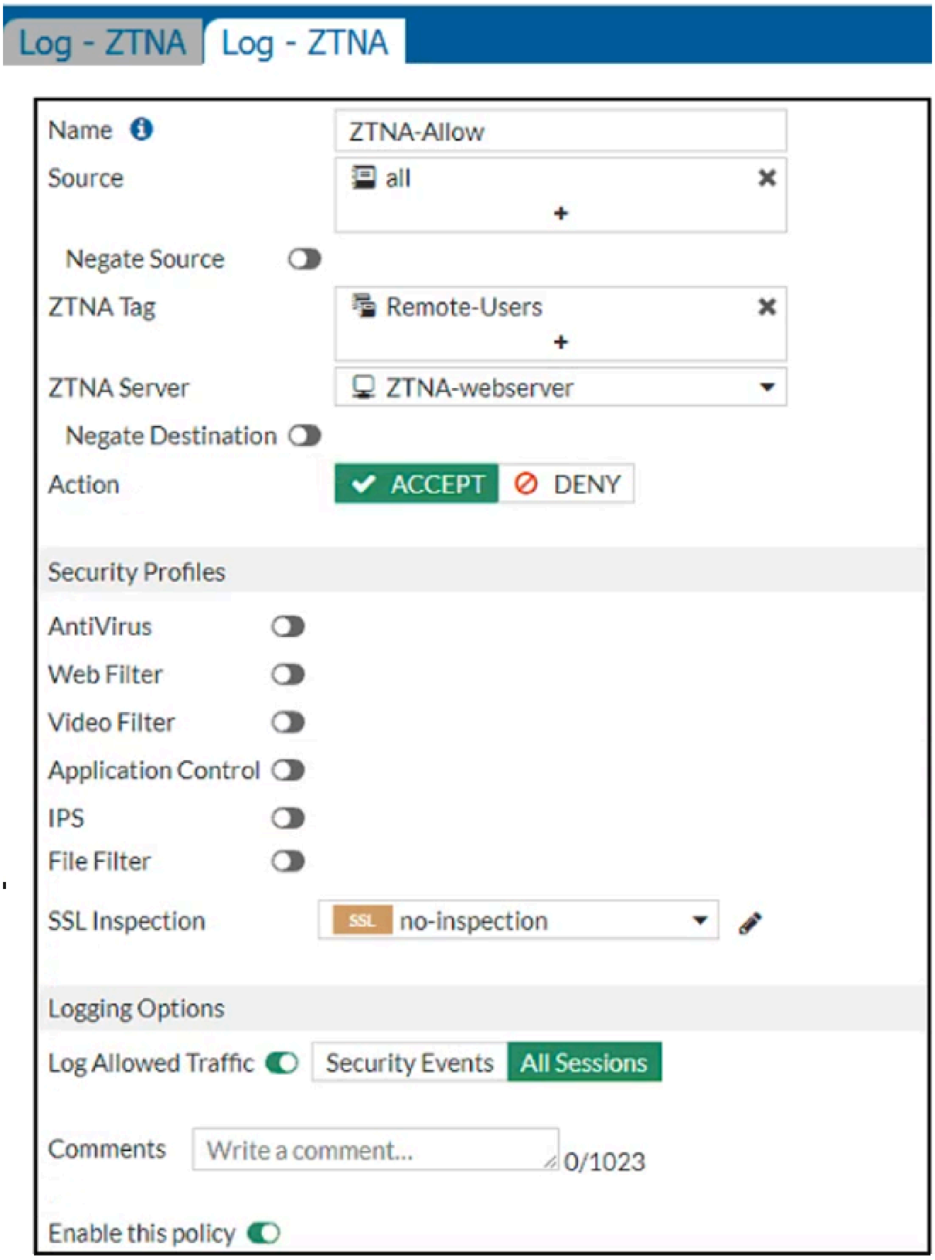
Question #18 Topic 1

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.

**Suggested Answer:** *C*

*Community vote distribution*

A (100%)

**Lyanne** Highly Voted 1 year, 4 months ago

A - page 249 study guide

upvoted 8 times

**ash0x48** Most Recent 12 months ago

**Selected Answer: A**

A - page 249 study guide

upvoted 1 times

**foobarasdf123** 1 year ago

**Selected Answer: A**

should be A: page 249 study guide:

"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

upvoted 2 times

**Eggrolls** 1 year, 1 month ago

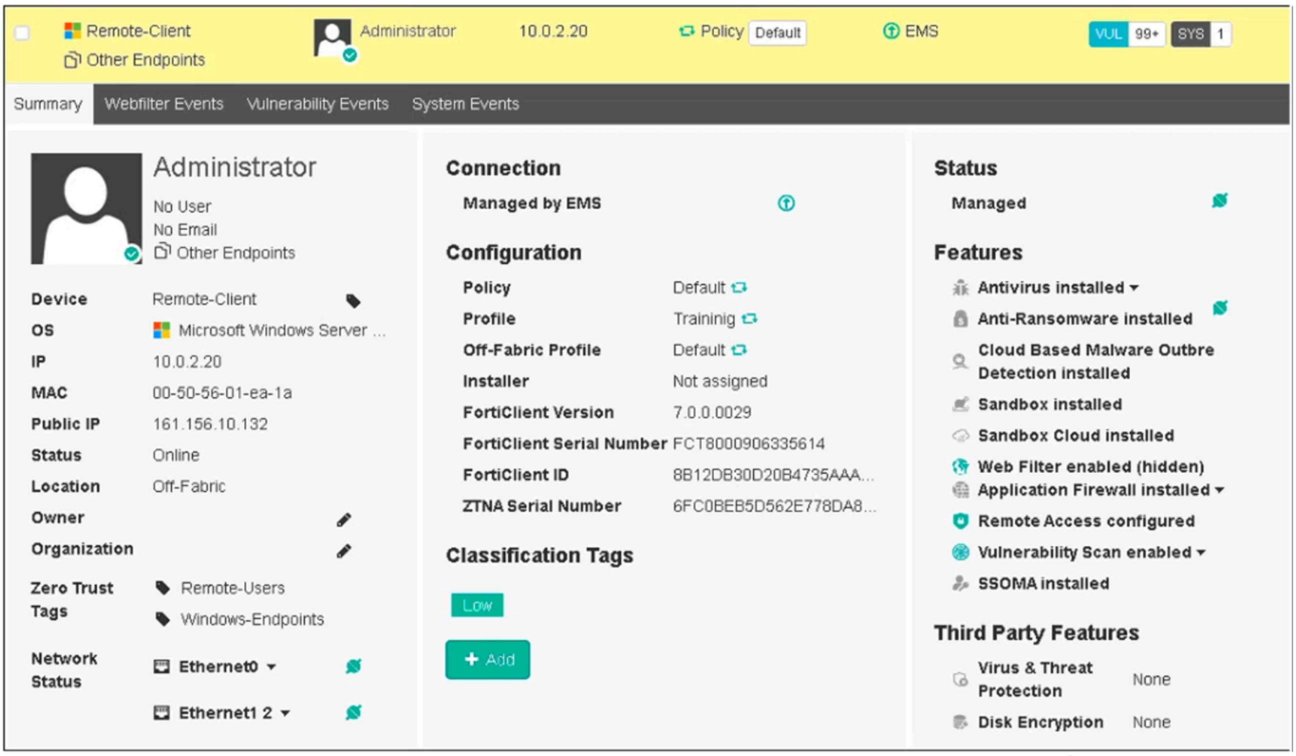
**Selected Answer: A**

Answer is A

upvoted 1 times

Question #19 *Topic 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<br>Windows-Endpoints |
| Network Status | Ethernet0<br>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.

**Suggested Answer:** *B*

*Community vote distribution*

B (57%) A (43%)

**Newnurlife** Highly Voted 1 year, 9 months ago

Hi, this is a multiple-choice question and assumes two correct answers. My choice is B,D.

upvoted 20 times

**Ah_Leb** 1 year, 4 months ago

Agreed, BD

upvoted 4 times

**soporte127** 1 year, 3 months ago

porque the d? if the computer is online

upvoted 1 times

**Zixusen** 1 year, 2 months ago

Because it doesn't say that the client it offline, only off-net (off-fabric)

Correct answer is B & D.

upvoted 3 times

**Tomer676** Highly Voted 1 year, 7 months ago

The Answer is B,D

upvoted 8 times

**Brand0n** Most Recent 11 months, 1 week ago

B,D / In study guide, the word 'off-net' is used same as 'off-fabric' or 'remote client'.

upvoted 2 times

**Tara_K** 11 months, 2 weeks ago

Correct answer is B,C because antivirus/sandbox installed

upvoted 1 times

**thinasci01** 1 year ago

B and C is correct answer.

upvoted 1 times

**Eggrolls** 1 year, 1 month ago

Selected Answer: B

B & D for sure.

upvoted 4 times

**tachy_22** 1 year, 6 months ago

I think AB because endpoint is classified as Security Risk because there are 99+ Vulnerabilities. Endpoint policy is default.

upvoted 1 times

**BrunoLu** 1 year, 6 months ago

Selected Answer: A

Answer is AB,Because the Antivirus is not install.

D:The status is online,so it cann't D

upvoted 3 times

> **Zixusen** 1 year, 2 months ago
>
> It doesn't say that the client it offline, only off-net (off-fabric).
>
> Correct answer is B & D.
>
> upvoted 3 times