

Fortinet.FCP_FCT_AD-7.2.by.TonyTinh.29q

Number: FCP_FCT_AD-7.2
Passing Score: 800
Time Limit: 120
File Version: 2.0

Exam Code: FCP_FCT_AD-7.2

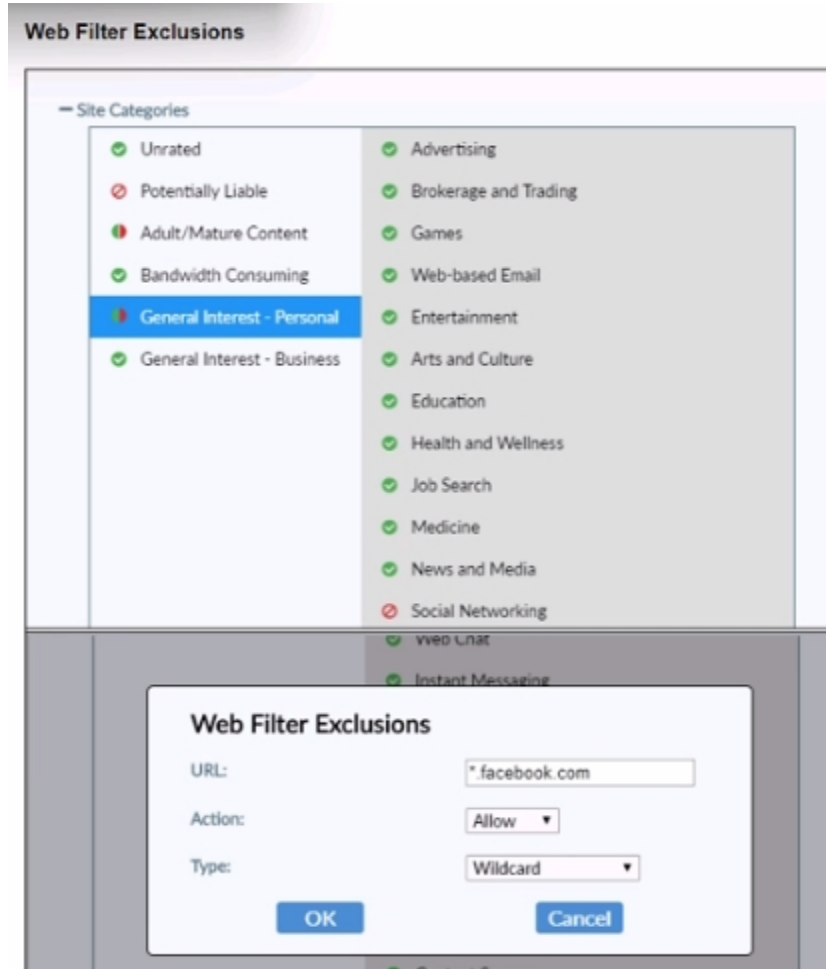
Exam Name: FCP - FortiClient EMS 7.2 Administrator



Exam A

QUESTION 1

Refer to the exhibit.



vdumps

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

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

Correct Answer: A

Section:

Explanation:

Observation of Web Filter Exclusions:

The exhibit shows a web filter exclusion for '*.facebook.com' with the action set to 'Allow.'

Evaluating Actions:

This configuration means that FortiClient will allow access to Facebook and its subdomains.

Conclusion:

When users try to access 'www.facebook.com,' FortiClient will allow the access based on the web filter exclusion settings.

FortiClient web filter configuration and exclusion documentation from the study guides.

QUESTION 2

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

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

Correct Answer: D

Section:

Explanation:

Understanding the Need for Root CA Certificate:

The root CA certificate of FortiClient EMS is necessary for FortiGate to trust certificates issued by FortiClient EMS.

Evaluating Use Cases:

FortiGate needs the root CA certificate to establish trust and validate certificates issued by FortiClient EMS.

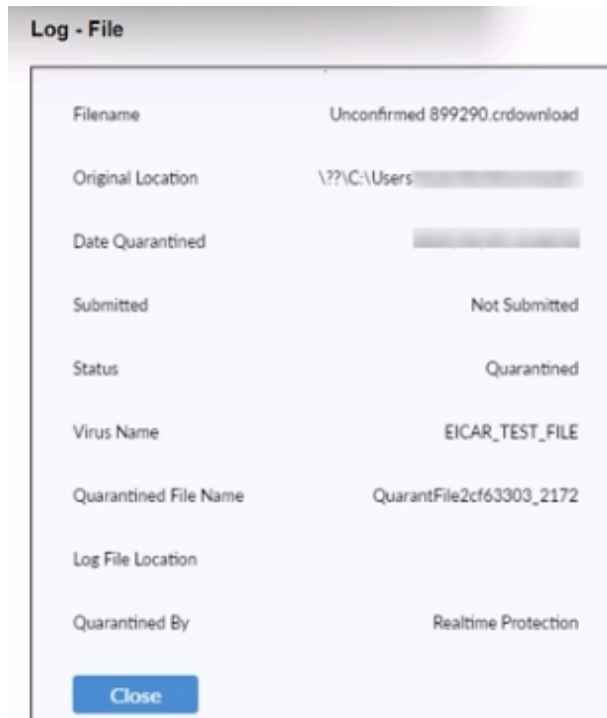
Conclusion:

The primary reason FortiGate needs the root CA certificate of FortiClient EMS is to trust certificates issued by FortiClient EMS.

FortiClient EMS and FortiGate certificate management documentation from the study guides.

QUESTION 3

Refer to the exhibit.



The logo for 'Vdumps' is displayed, featuring a stylized orange 'V' followed by the word 'dumps' in a grey, lowercase sans-serif font.

Based on the FortiClient log details shown in the exhibit, which two statements are true? (Choose two.)

- A. The filename is Unconfirmed 899290.crdownload.
- B. The file status is Quarantined
- C. The filename is sent to FortiSandbox for further inspection.
- D. The file location is \\?.D:\Users\.

Correct Answer: A, B

Section:

QUESTION 4

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

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

Correct Answer: B, D

Section:

Explanation:

Understanding Multi-Tenancy Mode:

Multi-tenancy mode allows multiple independent sites or tenants to be managed from a single FortiClient EMS instance.

Evaluating Benefits:

Licenses can be shared among sites, making it cost-effective (B).

It provides granular access and segmentation, allowing for detailed control and separation between tenants (D).

Eliminating Incorrect Options:

Separate host servers managing each site (A) is not a feature of multi-tenancy mode.

The fabric connector's use of an IP address (C) is unrelated to multi-tenancy benefits.

FortiClient EMS multi-tenancy configuration and benefits documentation from the study guides.

QUESTION 5

An administrator installs FortiClient EMS in the enterprise.

Which component is responsible for enforcing protection and checking security posture?

- A. FortiClient EMS tags
- B. FortiClient vulnerability scan
- C. FortiClient
- D. FortiClient EMS

Correct Answer: C

Section:

Explanation:

Understanding FortiClient EMS Components:

FortiClient EMS manages and configures endpoint security settings, while FortiClient installed on the endpoint enforces protection and checks security posture.

Evaluating Responsibilities:

FortiClient performs the actual enforcement of security policies and checks the security posture of the endpoint.

Conclusion:

The component responsible for enforcing protection and checking security posture is FortiClient (C).

FortiClient EMS and endpoint security documentation from the study guides.

QUESTION 6

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 application is blocked by the application firewall?

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

Correct Answer: A

Section:

Explanation:

Based on the FortiClient logs shown in the exhibit:

The first log entry shows the application 'firefox.exe' trying to access a destination IP, with the threat identified as 'Twitter.'

The action taken by the application firewall is 'blocked' with the event type 'appfirewall.'

This indicates that the application firewall has blocked access to Twitter.

Reference

FortiClient EMS 7.2 Study Guide, Application Firewall Logs Section

Fortinet Documentation on Interpreting FortiClient Logs

QUESTION 7

Which three features does FortiClient endpoint security include? (Choose three.)

- A. DLP
- B. Vulnerability management
- C. L2TP
- D. IPsec
- E. Real-time protection

Correct Answer: B, D, E

Section:

Explanation:



Understanding FortiClient Features:

FortiClient endpoint security includes several features aimed at protecting and managing endpoints.

Evaluating Feature Set:

Vulnerability management is a key feature of FortiClient, helping to identify and address vulnerabilities (B).

IPsec is supported for secure VPN connections (D).

Real-time protection is crucial for detecting and preventing threats in real-time (E).

Eliminating Incorrect Options:

Data Loss Prevention (DLP) (A) is typically managed by FortiGate or FortiMail.

L2TP (C) is a protocol used for VPNs but is not specifically a feature of FortiClient endpoint security.

FortiClient endpoint security features documentation from the study guides.

QUESTION 8

Which component or device defines ZTNA tag information in the Security Fabric integration?

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

Correct Answer: C

Section:

Explanation:

Understanding ZTNA:

Zero Trust Network Access (ZTNA) requires defining tags for identifying and managing endpoint access.

Evaluating Components:

FortiClient EMS is responsible for managing and defining ZTNA tag information within the Security Fabric.

Conclusion:

The correct component that defines ZTNA tag information in the Security Fabric integration is FortiClient EMS.

ZTNA and FortiClient EMS configuration documentation from the study guides.

QUESTION 9

Refer to the exhibit, which shows FortiClient EMS deployment, profiles.

Deployments					
+ Add Change Priority					
Name	Assigned Groups	Deployment Package	Scheduled Upgrade Time	Priority	Enabled
Deployment-1	All Groups	First-Time-Installation		1	<input type="checkbox"/>
Deployment-2	All Groups trainingAD.training.lab	To-Upgrade		2	<input checked="" type="checkbox"/>

When an administrator creates a deployment profile on FortiClient EMS, which statement about the deployment profile is true?

- A. Deployment-2 will upgrade FortiClient on both the AD group and workgroup.
- B. Deployment-1 will install FortiClient on new AO group endpoints.
- C. Deployment-2 will install FortiClient on both the AD group and workgroup.
- D. Deployment-1 will upgrade FortiClient only on the workgroup.

Correct Answer: A

Section:

Explanation:

Deployment Profiles Analysis:

Deployment-1 has the 'First-Time-Installation' package and is assigned to 'All Groups' with a priority of 1 but is not enabled.

Deployment-2 has the 'To-Upgrade' package, is assigned to both 'All Groups' and 'trainingAD.training.lab,' with a priority of 2 and is enabled.

Evaluating Deployment-2:

Deployment-2 will upgrade FortiClient on both 'All Groups' and 'trainingAD.training.lab' since it is enabled and assigned to these groups. This includes both AD (Active Directory) groups and workgroups.

Conclusion:

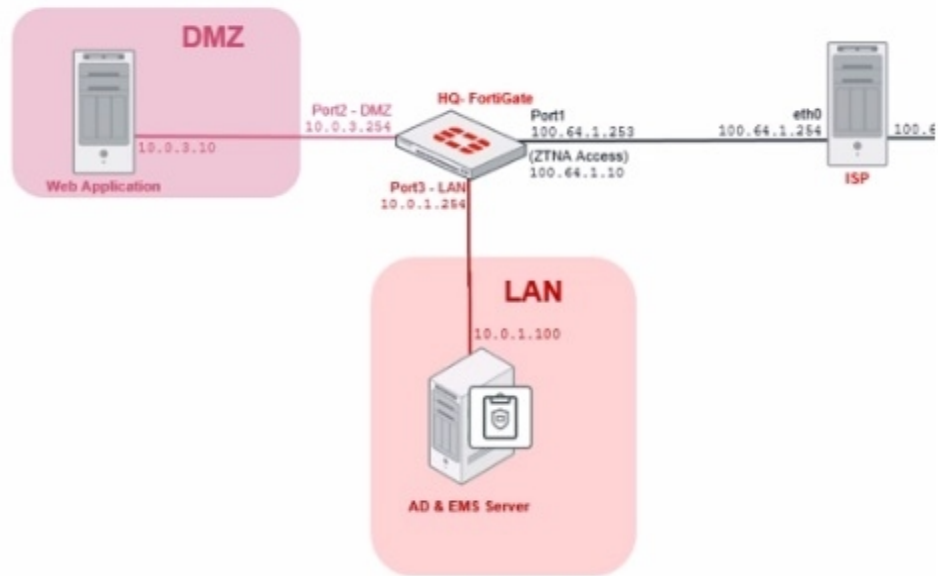
Since Deployment-2 is set to upgrade FortiClient on all the assigned groups and workgroups, the correct answer is A.

FortiClient EMS deployment and profile documentation from the study guides.

QUESTION 10

ZTNA Network Topology





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	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"/>



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?

- A. Remote-Client has not initiated a connection to the ZTNA access proxy.
- B. Remote-Client provided an empty client certificate to connect to the ZTNA access proxy.
- C. Remote-Client provided an invalid certificate to connect to the ZTNA access proxy.
- D. Remote-Client failed the client certificate authentication.

Correct Answer: D

Section:

QUESTION 11

Refer to the exhibits.

The first screenshot shows the configuration for two endpoint policies. The left policy is named 'Training' and is assigned to the 'trainingAD.training.lab' group. It uses the 'Optional' user profile, 'Training' profile, and 'Default' off-fabric profile. The right policy is named 'Sales' and is assigned to 'All Groups' and 'trainingAD.training.lab'. It uses the 'trainingAD.training.lab\student' user profile, 'Training' profile, and 'Default' off-fabric profile. Both policies have 'On-Fabric' detection rules and are enabled.

The second screenshot is a table titled 'Endpoint Policies' showing the configuration for the 'Training' and 'Sales' policies.

Name	Assigned Groups	Profile	Policy Components	Endpoint Count	Priority	Enabled
Training	trainingAD.training.lab	PROFILE Training OFF-FABRIC Default 100%	ON-FABRIC On-Fabric	1	1	Yes
Sales	All Groups trainingAD.training.lab	PROFILE Training OFF-FABRIC Default 100%	ON-FABRIC On-Fabric	1	2	Yes
Default		PROFILE Training OFF-FABRIC Default	ON-FABRIC On-Fabric	0	3	No

Which shows the configuration of endpoint policies.

Based on the configuration, what will happen when someone logs in with the user account student on an endpoint in the trainingAD domain?

- A. FortiClient EMS will assign the Sales policy
- B. FortiClient EMS will assign the Training policy
- C. FortiClient EMS will assign the Default policy
- D. FortiClient EMS will assign the Training policy for on-fabric endpoints and the Sales policy for the off-fabric endpoint

Correct Answer: B

Section:

Explanation:

Based on the configuration shown in the exhibits:

There are three endpoint policies configured: Training, Sales, and Default.

The 'Training' policy is assigned to the 'trainingAD.training.lab' group.

The 'Sales' policy is assigned to 'All Groups' and 'trainingAD.training.lab/student.'

The 'Default' policy has no specific groups assigned.

When someone logs in with the user account 'student' on an endpoint in the 'trainingAD' domain:

The 'Training' policy is specifically assigned to the 'trainingAD.training.lab' group.

The 'Sales' policy includes 'trainingAD.training.lab/student' but not the general 'trainingAD.training.lab' group.

The system will prioritize the most specific match for the group.

Therefore, FortiClient EMS will assign the 'Training' policy to the 'student' account logging into the 'trainingAD' domain as it matches the group 'trainingAD.training.lab' directly.

Reference

FortiClient EMS 7.2 Study Guide, Endpoint Policy Configuration Section

FortiClient EMS Documentation on Group Policy Assignment and Matching

QUESTION 12

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?

- 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

Correct Answer: D

Section:

Explanation:

When deploying FortiClient via Microsoft AD Group Policy, it is essential to ensure that the deployment package is correctly assigned to the target group. The absence of custom configuration after installation can be due to several reasons, but the most likely cause is:

Deployment Package Assignment: The FortiClient package must be assigned to the appropriate group in Group Policy Management. If this step is missed, the installation may proceed, but the custom configurations will not be applied.

Thus, the administrator must ensure that the FortiClient package is correctly assigned to the group to include all custom configurations.

Reference

FortiClient EMS 7.2 Study Guide, Deployment and Installation Section

Fortinet Documentation on FortiClient Deployment using Microsoft AD Group Policy

QUESTION 13


Refer to the exhibits.


Security Fabric Settings


FortiGate Telemetry


Security Fabric role **Serve as Fabric Root** Join Existing Fabric


Fabric name

Topology  **FGVM010000052731 (Fabric Root)**

Allow other FortiGates to join 


Pre-authorized FortiGates None  Edit

SAML Single Sign-On 


Management IP/FQDN  **Use WAN IP** Specify


Management Port **Use Admin Port** Specify


FortiAnalyzer Logging


IP address 

Logging to ADOM root

Storage usage  0% 144.55 MiB / 50.00 GiB


Analytics usage  0% 91.02 MiB / 35.00 GiB
(Number of days stored: 55/60)

Archive usage  0% 53.53 MiB / 15.00 GiB
(Number of days stored: 54/365)


Upload option  **Real Time** Every Minute Every 5 Minutes

SSL encrypt log transmission

Allow access to FortiGate REST API

Verify FortiAnalyzer certificate  FAZ-VMTM19008187

FortiClient Endpoint Management System (EMS)

Name 

IP/Domain Name

Serial Number

Hostname	EMSServer
Listen on IP	10.0.1.100 <small>FQDN is required when listening to all IPs.</small>
Use FQDN	<input checked="" type="checkbox"/>
FQDN	myemsserver
Remote HTTPS access	<input type="checkbox"/> <small>Only enforced when Windows Firewall is running.</small>
SSL certificate	No certificate imported

Based on the FortiGate Security Fabric settings shown in the exhibits, what must an administrator do on the EMS server to successfully quarantine an endpoint. when it is detected as a compromised host (IoC)?

- A. The administrator must enable remote HTTPS access to EMS.
- B. The administrator must enable FQDN on EMS.
- C. The administrator must authorize FortiGate on FortiAnalyzer.
- D. The administrator must enable SSH access to EMS.

Correct Answer: A

Section:

Explanation:

Based on the FortiGate Security Fabric settings shown in the exhibits, to successfully quarantine an endpoint when it is detected as a compromised host (IOC), the following step is required:

Enable Remote HTTPS Access to EMS: This setting allows FortiGate to communicate securely with FortiClient EMS over HTTPS. Remote HTTPS access is essential for the quarantine functionality to operate correctly, enabling the EMS server to receive and act upon the quarantine commands from FortiGate.

Therefore, the administrator must enable remote HTTPS access to EMS to allow the quarantine process to function properly.

Reference

FortiGate Infrastructure 7.2 Study Guide, Security Fabric and Integration with EMS Sections

Fortinet Documentation on Enabling Remote HTTPS Access to FortiClient EMS

QUESTION 14

Exhibit.

```

1:40:39 PM Information Vulnerability id=96521 msg="A vulnerability scan result has been logged" status=N/A vulncat="Operating
1:40:39 PM Information Vulnerability id=96520 msg="The vulnerability scan status has changed" status="scanning finished" vulnc
1:41:38 PM Information ESNAC id=96958 user=Admin msg="User social media information" social_srvc=os social_user=Admin
2:12:22 PM Information Config id=96882 msg="Policy 'Default' was received and applied"
2:13:27 PM Information ESNAC id=96958 user=Admin msg="User social media information" social_srvc=os social_user=Admin
2:14:32 PM Information ESNAC id=96959 emshostname=WIN-EHVKBEA3571 msg="Endpoint has AV whitelist engine version 6.00134 and si
2:14:54 PM Information Config id=96882 msg="Policy 'Default' was received and applied"
2:16:01 PM Information ESNAC id=96958 user=Admin msg="User social media information" social_srvc=os social_user=Admin
2:20:19 PM Information Config id=96883 msg="Compliance rules 'default' were received and applied"
2:20:23 PM Debug ESNAC PIPEMSG_CMD_ESNAC_STATUS_RELOAD_CONFIG
2:20:23 PM Debug ESNAC cb828898d1ae56916f84cc7909a1eb1a
2:20:23 PM Debug ESNAC Before Reload Config
2:20:23 PM Debug ESNAC ReloadConfig
2:20:23 PM Debug Scheduler stop_task() called
2:20:23 PM Debug Scheduler GUI change event
2:20:23 PM Debug Scheduler stop_task() called
2:20:23 PM Information Config id=96882 msg="Policy 'Fortinet-Training' was received and applied"
2:20:23 PM Debug Config 'scan on registration' is disabled - delete 'on registration' vulnerability scan.
2:20:23 PM Debug Config ImportConfig: tag <\forticlient_configuration\antiexploit\exclusion_applications> value is empty.

```

Based on the FortiClient logs shown in the exhibit, which endpoint profile policy is currently applied to the FortiClient endpoint from the EMS server?

- A. Fortinet-Training
- B. Default configuration policy c
- C. Compliance rules default

D. Default

Correct Answer: A

Section:

Explanation:

Observation of Logs:

The logs show a policy named 'Fortinet-Training' being applied to the endpoint.

Evaluating Policies:

The log entries indicate that the 'Fortinet-Training' policy was received and applied.

Conclusion:

Based on the logs, the currently applied policy on the FortiClient endpoint is 'Fortinet-Training'.

FortiClient EMS policy configuration and log analysis documentation from the study guides.

QUESTION 15

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 remote registry service is not running.
- D. The task scheduler service is not running.

Correct Answer: D

Section:

Explanation:

<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

QUESTION 16

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

- A. ZTNA manages access for remote users only.
- B. ZTNA provides role-based access.
- C. ZTNA provides a security posture check.

D. ZTNA manages access through the client only.

Correct Answer: B, C

Section:

Explanation:

ZTNA (Zero Trust Network Access) is a security architecture that is designed to provide secure access to network resources for users, devices, and applications. It is based on the principle of 'never trust, always verify,' which means that all access to network resources is subject to strict verification and authentication.

Two functions of ZTNA are:

ZTNA provides a security posture check: ZTNA checks the security posture of devices and users that are attempting to access network resources. This can include checks on the device's software and hardware configurations, security settings, and the presence of malware.

ZTNA provides role-based access: ZTNA controls access to network resources based on the role of the user or device. Users and devices are granted access to only those resources that are necessary for their role, and all other access is denied. This helps to prevent unauthorized access and minimize the risk of data breaches.

QUESTION 17

When site categories are disabled in FortiClient web filter, which feature can be used to protect the endpoint from malicious web access?

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

Correct Answer: D

Section:

Explanation:

Web Filter Functionality:

When site categories are disabled in the FortiClient web filter, the endpoint still requires protection from malicious web access.

Alternative Protection Features:

The web exclusion list can be used to manage and block specific URLs that are known to be malicious, providing a way to control and secure web access even without site categories being enabled.

Conclusion:

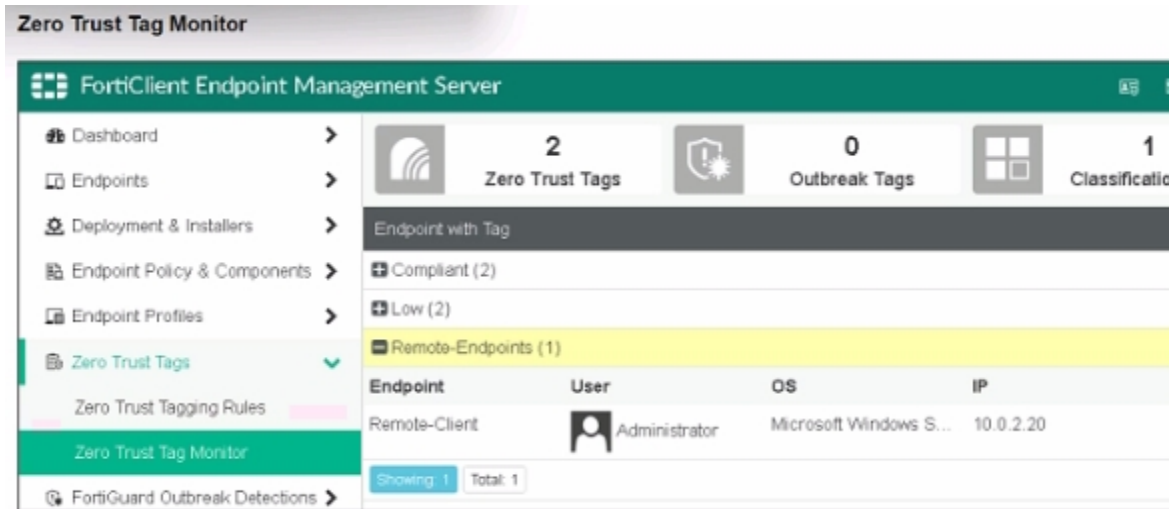
The correct feature that can be used to protect the endpoint in this scenario is the web exclusion list (D).

FortiClient web filter configuration and features from the study guides.

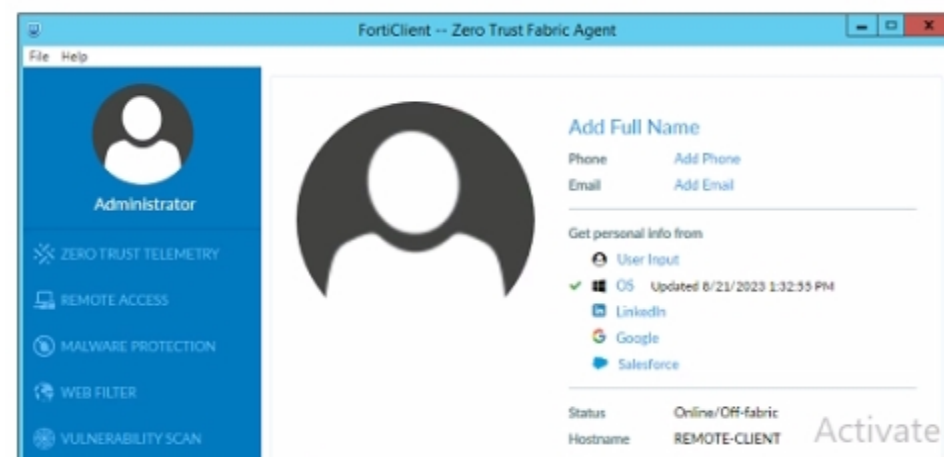
QUESTION 18

Exhibit.





FortiClient Status - GUI



Refer to the exhibits, which show the Zero Trust Tag Monitor and the FortiClient GUI status. Remote-Client is tagged as Remote-User* on the FortiClient EMS Zero Trust Tag Monitor. What must an administrator do to show the tag on the FortiClient GUI?

- A. Change the FortiClient EMS shared settings to enable tag visibility.
- B. Change the endpoint alerts configuration to enable tag visibility.
- C. Update tagging rule logic to enable tag visibility.
- D. Change the FortiClient system settings to enable tag visibility.

Correct Answer: B

Section:

Explanation:

Observation of Exhibits:

The exhibits show the Zero Trust Tag Monitor on FortiClient EMS and the FortiClient GUI status.

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

Enabling Tag Visibility:

To show the tag on the FortiClient GUI, the endpoint alerts configuration must be adjusted to enable tag visibility.

Verification:

The correct action is to change the endpoint alerts configuration to enable tag visibility, ensuring that the tag appears in the FortiClient GUI.

FortiClient EMS and FortiClient configuration documentation from the study guides.

QUESTION 19

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 littering mode

Correct Answer: A

Section:

Explanation:

Simplifying Remote Access:

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

Evaluating Access Control Methods:

ZTNA full mode can provide seamless access by leveraging device identity and posture, eliminating the need for user credentials for each access request.

Other methods like SSL VPN and L2TP typically require user credentials.

Conclusion:

The correct access control method that provides this solution is ZTNA full mode.

ZTNA section in the FortiGate Infrastructure 7.2 Study Guide.

QUESTION 20

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

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

Correct Answer: A

Section:

Explanation:

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

QUESTION 21

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 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: B, D

Section:

Explanation:

Based on the Remote-Client status shown in the exhibit:

Endpoint Policy: The 'Policy' field shows 'Default,' indicating that the endpoint has been assigned the Default endpoint policy.
Connection Status: The 'Location' field shows 'Off-Fabric,' meaning that the endpoint is currently off the corporate network (off-net).
Therefore, the two conclusions that can be made are:
The endpoint has been assigned the Default endpoint policy.
The endpoint is currently off-net.

Reference

FortiClient EMS 7.2 Study Guide, Endpoint Summary Information Section

Fortinet Documentation on Endpoint Policies and Status Indicators

QUESTION 22

A new chrome book is connected in a school's network.

Which component can the EMS administrator use to manage the FortiClient web filter extension installed on the Google Chromebook endpoint?

- A. FortiClient EMS
- B. FortiClient site categories
- C. FortiClient customer URL list
- D. FortiClient web filter extension

Correct Answer: A

Section:

Explanation:

For managing the FortiClient web filter extension installed on the Google Chromebook endpoint, the EMS administrator can use the following component:

FortiClient EMS (Enterprise Management Server) is designed to manage and control multiple FortiClient installations across various endpoints.

EMS provides centralized management for endpoint policies, including web filtering configurations.

The EMS administrator can configure and enforce web filter policies on Chromebooks through the EMS console.

Therefore, FortiClient EMS is the correct component for managing the web filter extension on Google Chromebook endpoints.

Reference

FortiClient EMS 7.2 Study Guide, Chromebook Management Section

Fortinet Documentation on FortiClient EMS and Web Filtering for Chromebooks

QUESTION 23

A FortiClient EMS administrator has enabled the compliance rule for the sales department Which Fortinet device will enforce compliance with dynamic access control?

- A. FortiClient
- B. FortiClient EMS
- C. FortiGate
- D. FortiAnalyzer

Correct Answer: C

Section:

Explanation:

Understanding Compliance Rules:

The compliance rule for the sales department needs to be enforced dynamically.

Enforcing Compliance:

FortiGate is responsible for enforcing compliance by integrating with FortiClient EMS to apply dynamic access control based on compliance status.

Conclusion:

The Fortinet device that will enforce compliance with dynamic access control is the FortiGate.

Compliance and enforcement documentation from FortiGate and FortiClient EMS study guides.

QUESTION 24

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

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

Correct Answer: B

Section:

Explanation:

Understanding FortiSandbox Integration:

In a FortiSandbox integration, various remediation options are available for handling suspicious files.

Evaluating Remediation Options:

The remediation option for alerting and notifying without blocking access or waiting for results is essential to understand.

Conclusion:

The correct action for the remediation option in this context is to alert and notify only.

FortiSandbox integration documentation from the study guides.

QUESTION 25

An administrator needs to connect FortiClient EMS as a fabric connector to FortiGate. What is the prerequisite to get FortiClient EMS to connect to FortiGate successfully?

- A. Import and verify the FortiClient EMS tool CA certificate on FortiGate.
- B. Revoke and update the FortiClient client certificate on EMS.
- C. Import and verify the FortiClient client certificate on FortiGate.
- D. Revoke and update the FortiClient EMS root CA.



Correct Answer: A

Section:

Explanation:

Connecting FortiClient EMS to FortiGate:

The administrator needs to establish a connection between FortiClient EMS and FortiGate as a fabric connector.

Prerequisites for Connection:

A key prerequisite is the import and verification of the FortiClient EMS tool CA certificate on FortiGate to ensure a trusted connection.

Conclusion:

The correct prerequisite for a successful connection is to import and verify the FortiClient EMS tool CA certificate on FortiGate.

FortiClient EMS and FortiGate connection and certificate management documentation from the study guides.

QUESTION 26

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

- A. FortiAnalyzer
- B. FortiGate
- C. FortiClient EMS
- D. FortiClient

Correct Answer: C

Section:

Explanation:

Understanding the Automation Process:

In the Security Fabric, automation processes can include actions such as quarantining an endpoint after an IOC (Indicator of Compromise) detection.

Evaluating Responsibilities:

FortiClient EMS plays a crucial role in endpoint management and can send notifications to quarantine endpoints.

Conclusion:

The correct security fabric component that sends a notification to quarantine an endpoint after IOC detection is FortiClient EMS.

FortiClient EMS and automation process documentation from the study guides.

QUESTION 27

An administrator configures ZTNA configuration on the FortiGate. Which statement is true about the firewall policy?

- A. It redirects the client request to the access proxy.
- B. It uses the access proxy.
- C. It defines ZTNA server.
- D. It only uses ZTNA tags to control access for endpoints.

Correct Answer: A

Section:

Explanation:

'The firewall policy matches and redirects client requests to the access proxy VIP' <https://docs.fortinet.com/document/fortigate/7.0.0/new-features/194961/basic-ztna-configuration>

QUESTION 28

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

Correct Answer: C

Section:

Explanation:

When FortiClient is installed on a Windows Server, the default behavior for real-time protection control is:

Real-time protection is disabled: By default, FortiClient does not enable real-time protection on server installations to avoid potential performance impacts and because servers typically have different security requirements compared to client endpoints.

Thus, real-time protection is disabled by default on Windows Server installations.

Reference

FortiClient EMS 7.2 Study Guide, Real-time Protection Section

Fortinet Documentation on FortiClient Default Settings for Server Installations

QUESTION 29

Which three types of antivirus scans are available on FortiClient? (Choose three)

- A. Proxy scan
- B. Full scan
- C. Custom scan



- D. Flow scan
- E. Quick scan

Correct Answer: B, C, E

Section:

Explanation:

FortiClient offers several types of antivirus scans to ensure comprehensive protection:

Full scan: Scans the entire system for malware, including all files and directories.

Custom scan: Allows the user to specify particular files, directories, or drives to be scanned.

Quick scan: Scans the most commonly infected areas of the system, providing a faster scanning option.

These three types of scans provide flexibility and thoroughness in detecting and managing malware threats.

Reference

FortiClient EMS 7.2 Study Guide, Antivirus Scanning Options Section

Fortinet Documentation on Types of Antivirus Scans in FortiClient

