

Fortinet

Exam Questions FCP_FCT_AD-7.2

FCP-FortiClient EMS 7.2 Administrator



NEW QUESTION 1

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.

Answer: CD

Explanation:

? Understanding Multi-Tenancy Mode:

? Evaluating Benefits:

? Eliminating Incorrect Options:

References:

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

NEW QUESTION 2

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 enforces compliance on the endpoints using tags
- D. It receives the CA certificate from FortiGate to validate client certificates.

Answer: C

NEW QUESTION 3

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 file
- C. DLLs, and drivers for threats.
- D. It allows users to select a specific file folder on their local hard disk drive (HDD), to scan for threats.
- E. It scans executable file
- F. DLLs, and drivers that are currently running, for threats.

Answer: B

Explanation:

? Understanding Quick Scan Function:

? Evaluating Scan Scope:

? Conclusion:

References:

? FortiClient scanning options documentation from the study guides.

NEW QUESTION 4

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

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

Answer: BC

Explanation:

Administrators can use several third-party tools to deploy FortiClient:

? Microsoft SCCM (System Center Configuration Manager): SCCM is a robust tool used for deploying software across large numbers of Windows-based systems. It supports deployment of FortiClient through its software distribution capabilities.

? Microsoft Active Directory GPO (Group Policy Object): GPOs are used to manage user and computer settings in an Active Directory environment. Administrators can deploy FortiClient to multiple machines using GPO software installation settings.

These tools provide centralized and scalable methods for deploying FortiClient across numerous endpoints in an enterprise environment.

References

? FortiClient EMS 7.2 Study Guide, FortiClient Deployment Section

? Fortinet Documentation on FortiClient Deployment using SCCM and GPO

NEW QUESTION 5

An administrator has a requirement to add user authentication to the ZTNA access for remote or off-fabric users Which FortiGate feature is required in addition to ZTNA?

- A. FortiGate FSSO
- B. FortiGate certificates
- C. FortiGate explicit proxy
- D. FortiGate endpoint control

Answer: C

Explanation:

For adding user authentication to the ZTNA access for remote or off-fabric users, the following FortiGate feature is required in addition to ZTNA:

? FortiGate explicit proxy allows FortiGate to intercept web traffic for authentication purposes.

? ZTNA integrates with various FortiGate features to provide secure access and ensure that users are authenticated before accessing resources.

? By using an explicit proxy, FortiGate can handle web traffic and enforce authentication policies for remote users who are not directly on the corporate network (off-fabric).

Thus, the correct feature to use for this requirement is the FortiGate explicit proxy.

References

? FortiGate Security 7.2 Study Guide, ZTNA and Proxy Configuration Sections

? Fortinet Documentation on FortiGate Explicit Proxy and ZTNA Integration

NEW 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 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 application is blocked by the application firewall?

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

Answer: D

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.

References

? FortiClient EMS 7.2 Study Guide, Application Firewall Logs Section

? Fortinet Documentation on Interpreting FortiClient Logs

NEW QUESTION 7

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

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.

Answer: BD

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.

References

? FortiClient EMS 7.2 Study Guide, Endpoint Summary Information Section

? Fortinet Documentation on Endpoint Policies and Status Indicators

NEW QUESTION 8

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

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

Answer: BDE

Explanation:

? Understanding FortiClient Features:

? Evaluating Feature Set:

? Eliminating Incorrect Options:

References:

? FortiClient endpoint security features documentation from the study guides.

NEW QUESTION 9

An administrator is required to maintain a software vulnerability on the endpoints, without showing the feature on the FortiClient. What must the administrator do to achieve this requirement?

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

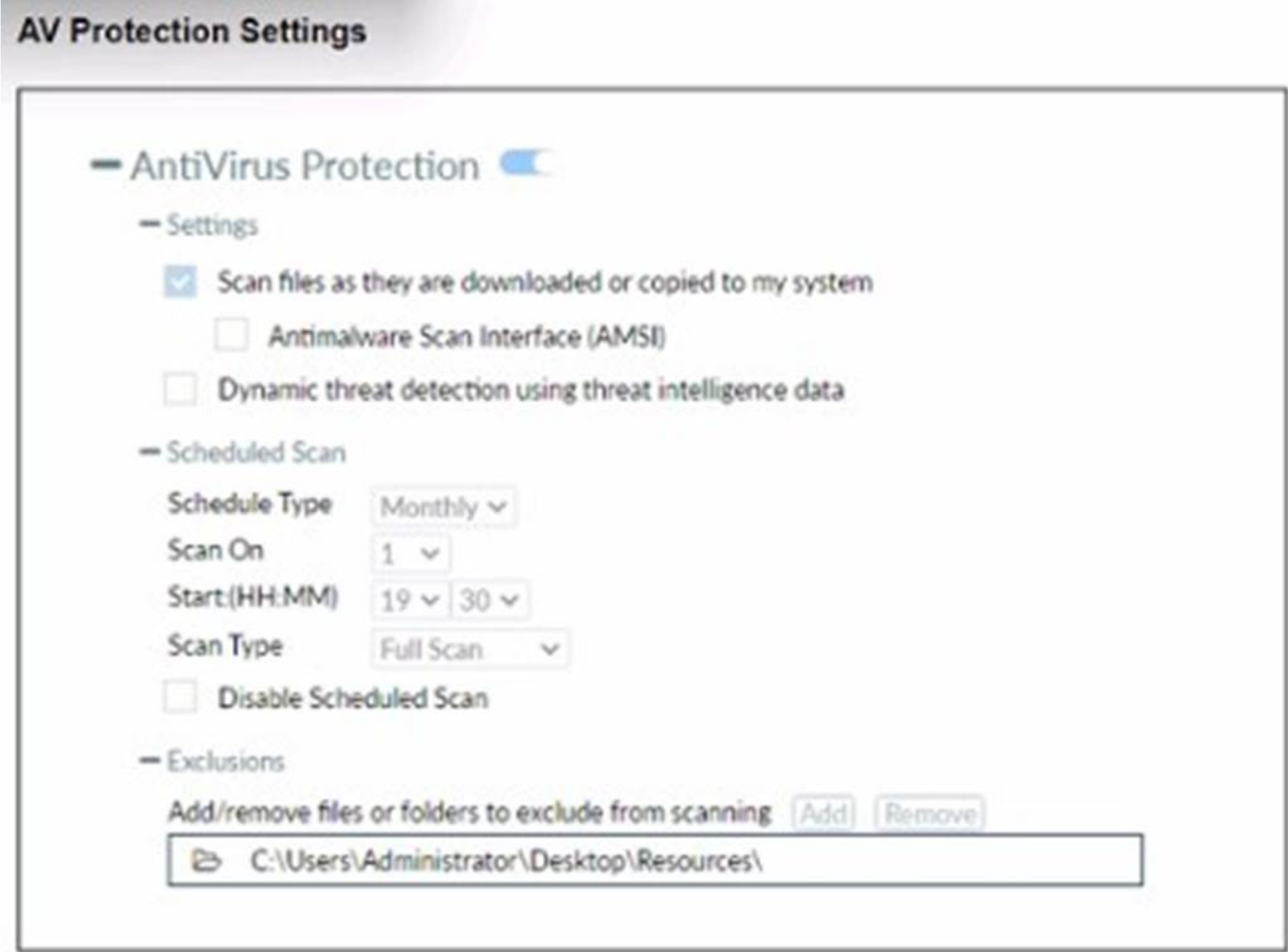
Answer: C

Explanation:

- ? Requirement Analysis:
- ? Evaluating Options:
- ? Conclusion:
- References:
- ? FortiClient EMS feature configuration and management documentation from the study guides.

NEW QUESTION 10

Refer to the exhibit.



Based on The settings shown in The exhibit, which statement about FortiClient behaviour is Hue?

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

Answer: A

Explanation:

Based on the settings shown in the exhibit, FortiClient is configured to scan files as they are downloaded or copied to the system. This means that if a user copies files to the ??Resources?? folder, which is not listed under exclusions, FortiClient will scan these files for infections. The exclusion path mentioned in the settings, "C:\Users\Administrator\Desktop\Resources", indicates that any files copied to this specific folder will not be scanned, but since the question implies that the ??Resources?? folder is not the same as the excluded path, FortiClient will indeed scan the files for infections.

NEW QUESTION 10

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

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

Answer: C

Explanation:

? Understanding ZTNA:

? Evaluating Components:

? Conclusion:

References:

? ZTNA and FortiClient EMS configuration documentation from the study guides.

NEW QUESTION 13

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.

Answer: A

Explanation:

? Deployment Profiles Analysis:

? Evaluating Deployment-2:

? Conclusion:

References:

? FortiClient EMS deployment and profile documentation from the study guides.

NEW 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.

Answer: BC

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.

NEW QUESTION 17

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

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

Answer: B

Explanation:

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.

NEW QUESTION 21

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

- A. Deny access to a tile when it sees no results

- B. Alert and notify only
- C. Exclude specified files
- D. Wait for FortiSandbox results before allowing files

Answer: B

Explanation:

- ? Understanding FortiSandbox Integration:
- ? Evaluating Remediation Options:
- ? Conclusion:
- References:
- ? FortiSandbox integration documentation from the study guides.

NEW QUESTION 26

Which statement about FortiClient enterprise management server is true?

- A. It provides centralized management of FortiGate devices.
- B. It provides centralized management of multiple endpoints running FortiClient software.
- C. It provides centralized management of FortiClient Android endpoints only.
- D. It provides centralized management of Chromebooks running real-time protection

Answer: B

Explanation:

FortiClient EMS is designed to provide centralized management and control of multiple endpoints running FortiClient software. It serves as a central management server that allows administrators to efficiently manage and configure a large number of FortiClient installations across the network.

NEW QUESTION 31

What does FortiClient do as a fabric agent? (Choose two.)

- A. Provides IOC verdicts
- B. Creates dynamic policies
- C. Provides application inventory
- D. Automates Responses

Answer: CD

NEW QUESTION 35

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

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

Answer: A

Explanation:

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

NEW QUESTION 36

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

- A. FortiAnalyzer
- B. FortiClient
- C. FortiClient EMS
- D. Forti Gate

Answer: D

NEW QUESTION 40

An administrator must add an authentication server on FortiClient EMS in a different security zone that cannot allow a direct connection. Which solution can provide secure access between FortiClient EMS and the Active Directory server?

- A. Configure and deploy a FortiGate device between FortiClient EMS and the Active Directory server.
- B. Configure Active Directory and install FortiClient EMS on the same VM.
- C. Configure a slave FortiClient EMS on a virtual machine.
- D. Configure an Active Directory connector between FortiClient EMS and the Active Directory server.

Answer: A

Explanation:

- ? Requirement:
- ? Solution Analysis:
- ? Evaluating Options:
- ? Conclusion:
- References:

? FortiClient EMS and FortiGate configuration and deployment documentation from the study guides.

NEW QUESTION 45

FortiClient EMS endpoint policies

Endpoint Policies									
+ Add Change Priority Refresh Clear Filters Edit									
Name	Assigned Groups	Profile Components		Policy Components		Endpoint Count	Priority	Enabled	
Sales	All Groups trainingAD.training.lab	VPN Training	ZTNA Training	ON-FABRIC On-Fabric	On-Fabric	1	1	<input type="checkbox"/>	
		WEB Training	VULN Training						
		MW Training	SB Training						
		FW Training	SYS Training						
Training	trainingAD.training.lab	VPN Training	ZTNA Training	ON-FABRIC On-Fabric	On-Fabric	1	2	<input checked="" type="checkbox"/>	
		WEB Training	VULN Training						
		MW Training	SB Training						
		FW Training	SYS Training						
Default		VPN Default	ZTNA Default			1	3	<input type="checkbox"/>	
		WEB Default	VULN Default						
		MW Default	SB Default						
		FW Default	SYS Default						

Refer to the exhibit, which shows multiple endpoint policies on FortiClient EMS. Which policy is applied to the endpoint in the AD group trainingAD

- A. The Training policy
- B. Both the Sales and Training policies because their priority is higher than the Default policy
- C. The Default policy because it has the highest priority
- D. The sales policy

Answer: A

Explanation:

? Observation of Endpoint Policies:

? Evaluating Policy Assignment:

? Conclusion:

References:

? FortiClient EMS policy configuration and priority management documentation from the study guides.

NEW QUESTION 48

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

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

Answer: A

Explanation:

FortiClient EMS is the component that shares ZTNA tag information through Security Fabric integration. ZTNA tags are synchronized from FortiClient EMS as inputs for the FortiGate application gateway. They can be used in ZTNA policies as security posture checks to ensure certain security criteria are met. FortiClient EMS can share ZTNA tags across multiple devices in the Fabric, such as FortiGate, FortiManager, and FortiAnalyzer. FortiClient EMS can also share ZTNA tags across multiple VDOMs on the same FortiGate device. FortiClient EMS can be configured to control the ZTNA tag sharing behavior in the Fabric Devices settings1. FortiGate is the device that enforces ZTNA policies using ZTNA tags. FortiGate can receive ZTNA tags from FortiClient EMS via Fabric Connector. FortiGate can also publish ZTNA services through the ZTNA portal, which allows users to access applications without installing FortiClient. FortiGate can also provide ZTNA inline CASB for SaaS application access control2.

FortiGate Access Proxy is a feature that enables FortiGate to act as a proxy for ZTNA traffic. FortiGate Access Proxy can be deployed in front of the application servers to provide ZTNA protection. FortiGate Access Proxy can also be deployed behind the application servers to provide ZTNA visibility. FortiGate Access Proxy can use ZTNA tags to identify and authenticate users and devices2.

FortiClient is the endpoint software that connects to ZTNA services. FortiClient can register ZTNA tags with FortiClient EMS based on the endpoint security posture. FortiClient can also use ZTNA tags to access ZTNA services published by FortiGate. FortiClient can also use ZTNA tags to access SaaS applications with ZTNA inline CASB2.

References :=

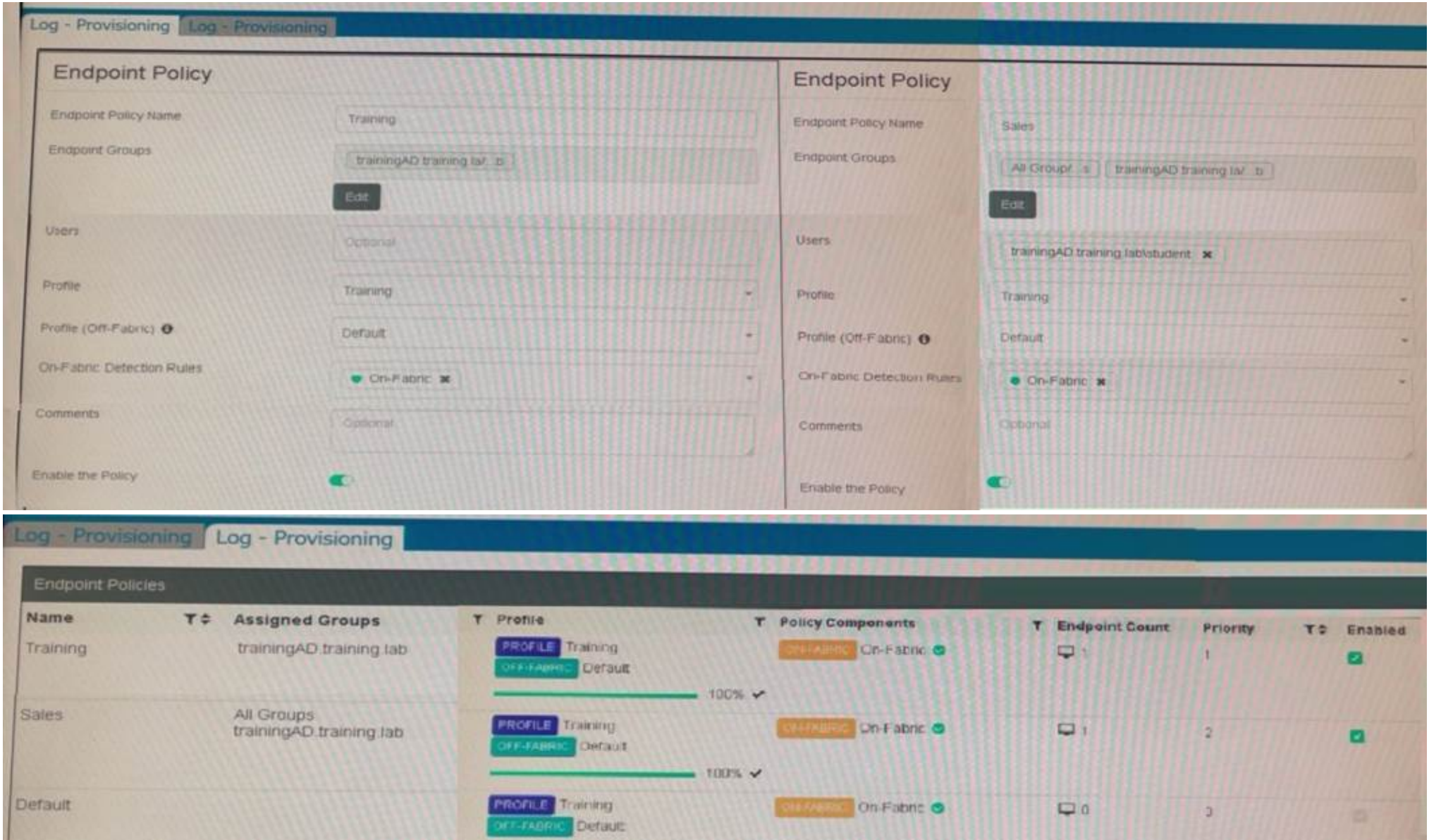
? Technical Tip: Behavior of ZTNA Tags shared across multiple vdoms or multiple FortiGate firewalls in the Security Fabric connected to the same FortiClient EMS Server

? Synchronizing FortiClient ZTNA tags

? Zero Trust Network Access (ZTNA) to Control Application Access

NEW QUESTION 50

Refer to the exhibits.



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

Answer: B

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. References
 ? FortiClient EMS 7.2 Study Guide, Endpoint Policy Configuration Section
 ? FortiClient EMS Documentation on Group Policy Assignment and Matching

NEW QUESTION 55

Which two VPNtypes can a FortiClientendpoint user inmate from the Windows command prompt? (Choose two)

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

Answer: CD

Explanation:

FortiClient supports initiating the following VPN types from the Windows command prompt:
 ? IPSec VPN:FortiClient can establish IPSec VPN connections using command line instructions.
 ? SSL VPN:FortiClient also supports initiating SSL VPN connections from the Windows command prompt.
 These two VPN types can be configured and initiated using specific command line parameters provided by FortiClient. References
 ? FortiClient EMS 7.2 Study Guide, VPN Configuration Section
 ? Fortinet Documentation on Command Line Options for FortiClient VPN

NEW QUESTION 59

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

Answer: A

Explanation:

? Simplifying Remote Access:

? Evaluating Access Control Methods:

? Conclusion:

References:

? ZTNA section in the FortiGate Infrastructure 7.2 Study Guide.

NEW QUESTION 63

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

FCP_FCT_AD-7.2 Practice Exam Features:

- * FCP_FCT_AD-7.2 Questions and Answers Updated Frequently
- * FCP_FCT_AD-7.2 Practice Questions Verified by Expert Senior Certified Staff
- * FCP_FCT_AD-7.2 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * FCP_FCT_AD-7.2 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The FCP_FCT_AD-7.2 Practice Test Here](#)