DUMPSARENA

NSE5_FCT-7.0 NSE 5 - FortiClient EMS 7.0

Fortinet NSE5_FCT-7.0

Version Demo

Total Demo Questions: 10

Total Premium Questions: 49

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

QUESTION NO: 1

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

ANSWER: B C

QUESTION NO: 2

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

A. FortiClient EMS

B. FortiGate

C. FortiGate Access Proxy

D. FortiClient

ANSWER: A

QUESTION NO: 3

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

A. Wait for FortiSandbox results before allowing files

B. Exclude specified files

C. Alert and notify only

D. Deny access to a file when it sees no results

ANSWER: C

QUESTION NO: 4

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

A. It enforces access control

B. It redirects the client request to the access proxy

C. It defines the access proxy

D. It applies security profiles to protect traffic

ANSWER: A D

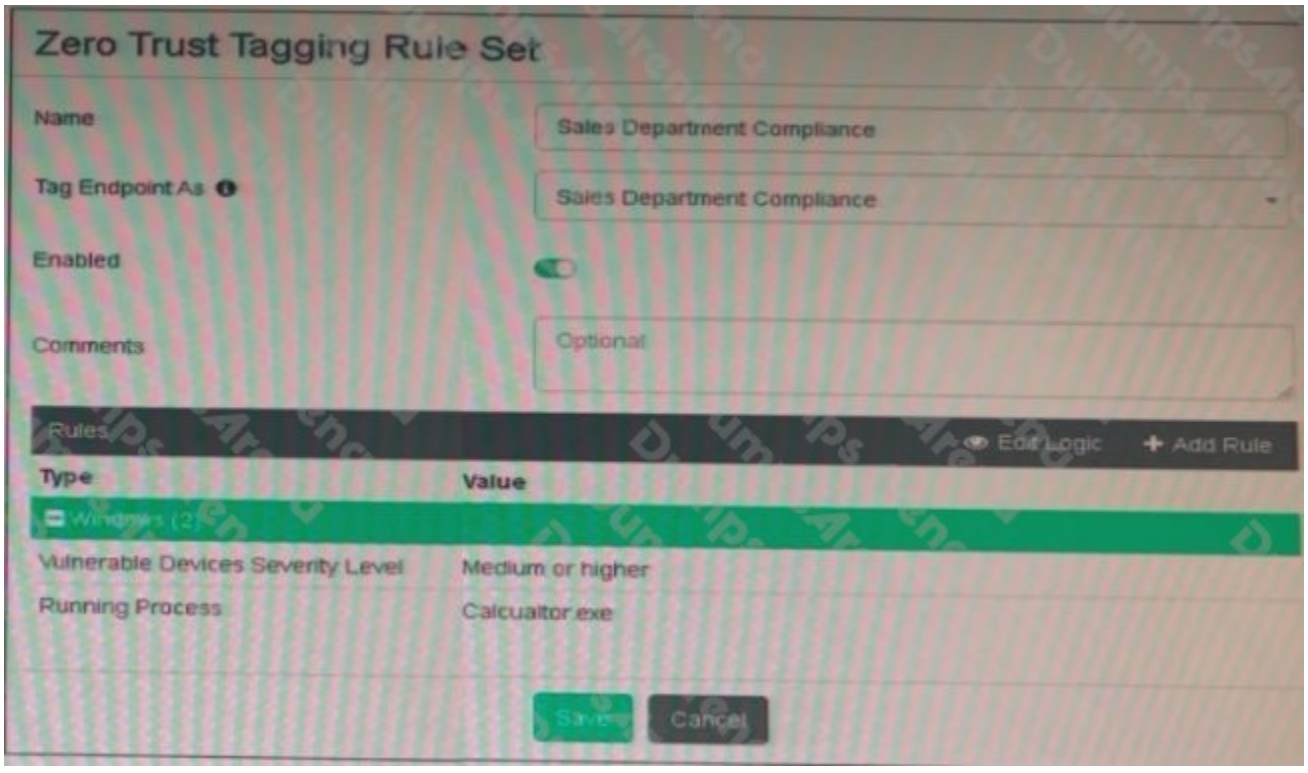
Explanation:

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

"ZTNA rules help control access by defining users and ZTNA tags to perform user authentication and security posture checks. And just like firewall policies, you can control the source and destination addresses, and apply appropriate security profiles to scan the traffic." https://docs.fortinet.com/document/fortigate/7.0.0/ztna-deployment/899992/configuring-ztna-rules-to-control-access

QUESTION NO: 5

Refer to the exhibit.



Based on the settings shown in the exhibit, which two actions must the administrator take to make the endpoint compliant? (Choose two.)

A. Enable the webfilter profile

B. Integrate FortiSandbox for infected file analysis

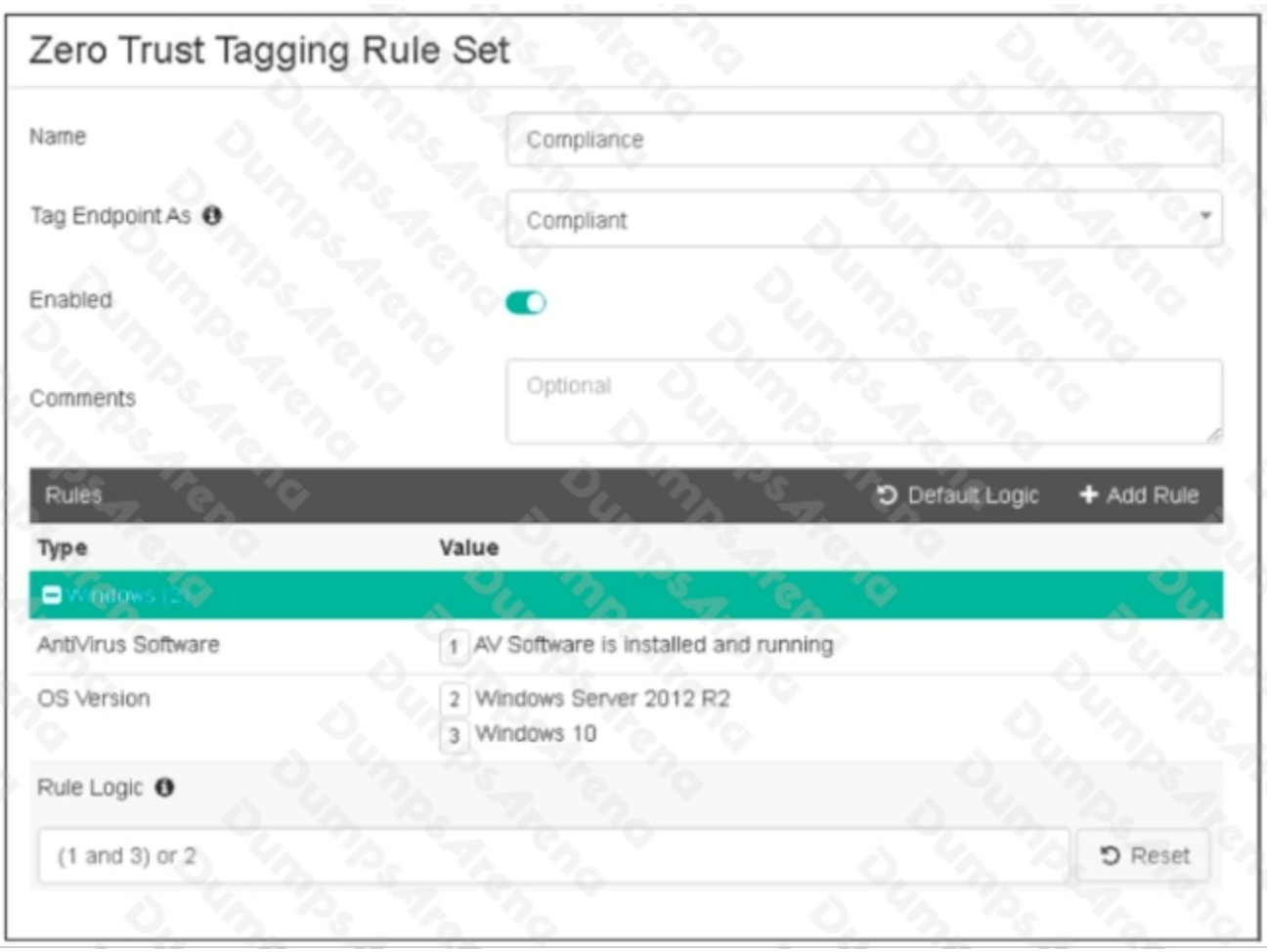
C. Patch applications that have vulnerability rated as high or above

D. Run Calculator application on the endpoint

ANSWER: C D

QUESTION NO: 6

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



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

A. The endpoint must satisfy that only Windows 10 is running.

B. The endpoint must satisfy that only AV software is installed and running.

C. The endpoint must satisfy that antivirus is installed and running and Windows 10 is running.

D. The endpoint must satisfy that only Windows Server 2012 R2 is running.

ANSWER: B C

QUESTION NO: 7

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

A. FortiGate FSSO

B. FortiGate certificates

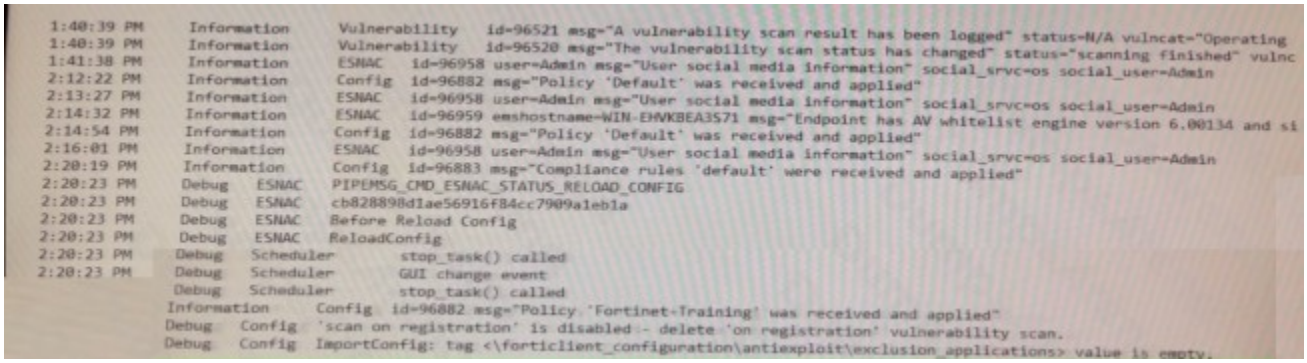
C. FortiGate explicit proxy

D. FortiGate endpoint control

ANSWER: C

QUESTION NO: 8

Refer to the exhibit.



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. Default

B. Compliance rules default

C. Fortinet- Training

D. Default configuration policy

ANSWER: C

QUESTION NO: 9

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

A. The fabric connector must use an IP address to connect to FortiClient EMS

B. It provides granular access and segmentation.

C. Licenses are shared among sites.

D. Separate host servers manage each site.

ANSWER: B D

Explanation:

FCT-EMS 7,0 Page 101 : You would use multi-tenancy in an MSSP environment to conserve resources and use the same license (the total number of FortiClient licenses are shared between sites)

QUESTION NO: 10

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.