

Actual4Dump



Choose the version that fits your needs	PDF Version	Desktop Test Engine	Online Test Engine
Latest and Up-to-Date exam dumps with real exam questions answers.	✓	✓	✓
Get 12-Months free updates without any extra charges.	✓	✓	✓
Experience same exam environment before appearing in the certification exam.	✗	✓	✓
100% exam passing guarante in the first attempt.	✓	✓	✓
20% discount on more than one license and 30% discount on 5+ license purchases.	✗	✓	✓
100% secure purchase on SSL.	✓	✓	✓
Completely private purchase without sharing your personal info with anyone.	✓	✓	✓

<http://www.actual4dump.com>

Superb Exam Dumps Materials lead you to get your certification easily - Actual4dump

Exam : **NSE5_FCT-7.0**

Title : Fortinet NSE 5 - FortiClient
EMS 7.0

Vendor : Fortinet

Version : DEMO

NO.1 An administrator installs FortiClient EMS in the enterprise.

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

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

Answer: D

Explanation

FortiClient is the component that is responsible for enforcing protection and checking security posture on the endpoints. FortiClient provides features such as antivirus, web filtering, firewall, vulnerability scan, and VPN.

FortiClient EMS is the management server that centrally configures and monitors FortiClient endpoints.

FortiClient EMS tags are used to group endpoints based on criteria such as OS, IP address, or domain.

FortiClient vulnerability scan is a feature that detects and fixes security issues on the endpoints.

References := FortiClient EMS Compliance with EMS and FortiOS

NO.2 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=C7F302B1D3E84F05A77E38AD6202B8D7 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=C7F302B1D3E84F05A77E38AD6202B8D7 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=C7F302B1D3E84F05A77E38AD6202B8D7 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: A

Explanation

the Twitter was Blocked see line 5 in the exhibit

NO.3 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

NO.4 An administrator wants to simplify remote access without asking users to provide user credentials.

Which access control method provides this solution"?

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

Answer: B

NO.5 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 allows users to select a specific file folder on their local hard disk drive (HDD), to scan for threats.
- C. It performs a full system scan including all files, executable files, DLLs, and drivers for threats.

Answer: A