Fortinet

FCP_FCT_AD-7.4

Fortinet FCP - FortiClient EMS 7.4 Administrator

Exams Boost
Boost Up Your Career

For More Information – Visit link below:

https://www.examsboost.com/

Product Version

✓ Up to Date products, reliable and verified.
✓ Questions and Answers in PDF Format.

Latest Version: 6.0

Question: 1

How can an administrator apply endpoint policies based on invitation?

A. Create security posture tags.
B. Create separate endpoint profiles.
C. Configure group assignment rules.
D. Configure on-fabric detection rules.

Answer: C

Question: 2

Refer to the exhibit.

```
[2025-02-20 10:59:10.8506451 UTC+00:00] [5244:5248] [FortiESNAC 258 info] Connecting to ems.training.lab:8013
[2025-02-20 10:59:10.8658308 UTC+00:00] [5244:5248] [FortiESNAC 264 error] Failed to resolve server address(11001):
No such host is known.
[2025-02-20 10:59:10.8660472 UTC+00:00] [5244:5248] [FortiESNAC 284 debug] Checking endpoint license change
[2025-02-20 10:59:10.8714141 UTC+00:00] [5244:5248] [FortiESNAC 149 debug] failure message:
[2025-02-20 10:59:10.9235075 UTC+00:00] [5244:5248] [FortiESNAC 337 debug] set REG_ESNAC_USER_ID
[2025-02-20 10:59:10.9237091 UTC+00:00] [5244:5248] [FortiESNAC 683 debug] Refreshing frontend info
[2025-02-20 10:59:10.9359240 UTC+00:00] [5244:5248] [FortiESNAC 161 debug] Endpoint state: Server Not Found
[2025-02-20 10:59:10.9359309 UTC+00:00] [5244:5248] [FortiESNAC 146 debug] In state: Server Select
[2025-02-20 10:59:10.9359998 UTC+00:00] [5244:5248] [FortiESNAC 498 info] Could not connect to any available EMS servers
[2025-02-20 10:59:10.9360798 UTC+00:00] [5244:5248] [FortiESNAC 284 debug] Checking endpoint license change
[2025-02-20 10:59:10.9439545 UTC+00:00] [5244:5248] [FortiESNAC 149 debug] failure message:
[2025-02-20 10:59:11.0173550 UTC+00:00] [5244:5248] [FortiESNAC 337 debug] set REG_ESNAC_USER_ID
[2025-02-20 10:59:11.0176929 UTC+00:00] [5244:5248] [FortiESNAC 683 debug] Refreshing frontend info
[2025-02-20 10:59:11.0430032 UTC+00:00] [5244:5248] [FortiESNAC 161 debug] Endpoint state: Server Not Found
[2025-02-20 10:59:11.0430096 UTC+00:00] [5244:5248] [FortiESNAC 146 debug] In state: Wait
[2025-02-20 10:59:13.4512008 UTC+00:00] [5244:6076] [FortiESNAC 52 debug] Received query: onnet-state
[2025-02-20 10:59:13.4512215 UTC+00:00] [5244:6076] [FortiESNAC 138 debug] send query reply [{"status":0,"status_msg":"not initialized"}]
[2025-02-20 10:59:13.4512472 UTC+00:00] [5244:6076] [FortiESNAC 144 debug] Query response: {"status":0,"status_msg":"not initialized"}
[2025-02-20 10:59:30.2850128 UTC+00:00] [5244:5248] [FortiESNAC 322 debug] Got event: License Expire Check
[2025-02-20 10:59:30.2850506 UTC+00:00] [5244:5248] [FortiESNAC 323 debug] Event ID (fb756b42******), Session ID (fb756b42******)
[2025-02-20 10:59:30.2850536 UTC+00:00] [5244:5248] [FortiESNAC 235 debug] Checking endpoint license expire
[2025-02-20 10:59:30.2876046 UTC+00:00] [5244:5248] [FortiESNAC 269 info] auth_period = 0
```

What is preventing FortiClient from registering with FortiClient EMS?

A. FortiClient could not reach the EMS server FQDN.
B. FortiClient user verification failed.
C. The FortiClient license expired.
D. FortiClient could not connect to the EMS server on port 8013.

Answer: A

Question: 3

What is the purpose of a webserver certificate in a FortiClient EMS deployment?

A. It is used by FortiClient Web Filter extension to perform SSL-inspection on web traffic.
B. It is used for telemetry connection from FortiClient to FortiClient EMS.
C. It is used to sign certificate requests from endpoints for zero trust network access (ZTNA).
D. It is used for communication with FortiGate as part of the Security Fabric.

Answer: D

Question: 4

Which two authentication methods are used for user verification on FortiClient EMS?
(Choose two.)

A. RADIUS
B. SAML
C. Local
D. TACACS

Answer: B,C

Question: 5

You are the administrator of VPN infrastructure that is struggling with performance issues due to most of their workforce now working remotely. The security architecture team is evaluating zero trust network access (ZTNA) as a potential replacement for their aging VPN deployment.
In what two ways does ZTNA differ from a conventional VPN?
(Choose two.)

A. More resource intensive
B. Continuous trust check
C. Based on network layer
D. Uses an access proxy

Answer: B,D

Question: 6

An administrator must provide web access to a zero trust network access (ZTNA) server hosted behind FortiGate. Which configuration must the administrator perform to achieve this outcome?

A. Add web server to the ZTNA destinations endpoint profile on FortiClient EMS.
B. Create a standard firewall policy with ZTNA webserver as the destination.
C. Manually install a ZTNA client certificate on the endpoint.

D. Configure a ZTNA server on FortiGate with service HTTPS.

Answer: D

Question: 7

Refer to the exhibit.

Log Details	
Source	100.64.1.1
Source Port	49578
Source Country/Region	Reserved
Source Interface	port2

Destination	
Real Server	100.64.0.1
Destination Port	9443
Destination Country/Region	Reserved

Application Control

Data	
Received Bytes	0 B
Sent Bytes	1.9 kB
LAN In	1900
LAN Out	3425
Message	Traffic denied because client certificate is empty

Action	
Action	deny
Threat	131072
ZTNA Rule	6
Policy UUID	196d3022-ee7e-51ef-f576-c4b73a9 b4e56
Policy Type	Firewall

Security	
Level	notice
Threat Level	high
Threat Score	30

Other	
Log event original timestamp	1739959570821785900
Timezone	-0800

Why was the traffic denied access to the zero trust network access (ZTNA) server?

A. The endpoint compliance status changed.
B. The FortiClient endpoint did not provide a client certificate.
C. The traffic matched a ZTNA deny policy.

D. The client certificate was revoked.

Answer: B

Question: 8

The security team must ensure that it uses the security posture information of an endpoint as part of the dynamic security policies matching criteria.
Which two pieces of information do endpoints provide in telemetry data to fabric devices?
(Choose two.)

A. Resource utilization
B. OS version
C. Vulnerability information
D. bandwidth

Answer: B,D

Question: 9

Which configuration on FortiGate quarantines the endpoint in a Security Fabric indicator of compromise (IOC) deployment?

A. Active connectors
B. Endpoint profile
C. Playbooks
D. Automation stitch

Answer: D

Question: 10

Which two statements about how full privileged access management (PAM) works with FortiClient are correct?
(Choose two.)

A. FortiClient EMS must have the FortiPAM add-on license applied.
B. Privileged access management must be enabled in the system settings endpoint profile.
C. FortiClient installer must have zero trust network access (ZTNA) and FortiPAM features enabled.
D. A FortiPAM standalone agent must be installed on the endpoint.

Thank You for Trying Our Product

For More Information – Visit link below:

https://www.examsboost.com/

15 USD Discount Coupon Code:

G74JA8UF

FEATURES

- ✓ **90 Days Free Updates**
- ✓ **Money Back Pass Guarantee**
- ✓ **Instant Download or Email Attachment**
- ✓ **24/7 Live Chat Support**
- ✓ **PDF file could be used at any Platform**
- ✓ **50,000 Happy Customer**