

Fortinet.NSE7\_ZTA-7.2.by.Utany.18q

Website: [www.VCEplus.io](http://www.VCEplus.io)

Twitter: [https://twitter.com/VCE\\_Plus](https://twitter.com/VCE_Plus)

**Exam Code: NSE7\_ZTA-7.2**

**Exam Name: Fortinet NSE 7 - Zero Trust Access 7.2**



## Exam A

### QUESTION 1

Which three methods can you use to trigger layer 2 polling on FortiNAC? (Choose three)

- A. Polling scripts
- B. Link traps
- C. Manual polling
- D. Scheduled tasks
- E. Polling using API

**Correct Answer: A, C, D**

**Section:**

**Explanation:**

To trigger layer 2 polling on FortiNAC, the three methods are:

A) Polling scripts: These are scripts configured within FortiNAC to actively poll the network at layer 2 to gather information about connected devices.

C) Manual polling: This involves manually initiating a polling process from the FortiNAC interface to gather current network information.

D) Scheduled tasks: Polling can be scheduled as regular tasks within FortiNAC, allowing for automated, periodic collection of network data.

The other options are not standard methods for layer 2 polling in FortiNAC:

B) Link traps: These are more related to SNMP trap messages rather than layer 2 polling.

E) Polling using API: While APIs are used for various integrations, they are not typically used for initiating layer 2 polling in FortiNAC.

FortiNAC Layer 2 Polling Documentation.

Configuring Polling Methods in FortiNAC.

### QUESTION 2

Which two statements are true regarding certificate-based authentication for ZTNA deployment? (Choose two.)

- A. FortiGate signs the client certificate submitted by FortiClient.
- B. The default action for empty certificates is block
- C. Certificate actions can be configured only on the FortiGate CLI
- D. Client certificate configuration is a mandatory component for ZTNA

**Correct Answer: B, D**

**Section:**

**Explanation:**

Certificate-based authentication is a method of verifying the identity of a device or user by using a digital certificate issued by a trusted authority. For ZTNA deployment, certificate-based authentication is used to ensure that only authorized devices and users can access the protected applications or resources.

B) The default action for empty certificates is block. This is true because ZTNA requires both device and user verification before granting access. If a device does not have a valid certificate issued by the ZTNA CA, it will be blocked by the ZTNA gateway. This prevents unauthorized or compromised devices from accessing the network.

D) Client certificate configuration is a mandatory component for ZTNA. This is true because ZTNA relies on client certificates to identify and authenticate devices. Client certificates are generated by the ZTNA CA and contain the device ID, ZTNA tags, and other information. Client certificates are distributed to devices by the ZTNA management server (such as EMS) and are used to establish a secure connection with the ZTNA gateway.

A) FortiGate signs the client certificate submitted by FortiClient. This is false because FortiGate does not sign the client certificates. The client certificates are signed by the ZTNA CA, which is a separate entity from FortiGate. FortiGate only verifies the client certificates and performs certificate actions based on the ZTNA tags.

C) Certificate actions can be configured only on the FortiGate CLI. This is false because certificate actions can be configured on both the FortiGate GUI and CLI. Certificate actions are the actions that FortiGate takes based on the ZTNA tags in the client certificates. For example, FortiGate can allow, block, or redirect traffic based on the ZTNA tags.

1: Technical Tip: ZTNA for Corporate hosts with SAML authentication and FortiAuthenticator as IDP

2: Zero Trust Network Access - Fortinet

### QUESTION 3

Which one of the supported communication methods does FortiNAC use for initial device identification during discovery?

- A. LLDP
- B. SNMP
- C. API
- D. SSH

**Correct Answer: B**

**Section:**

**Explanation:**

FortiNAC uses a variety of methods to identify devices on the network, such as Vendor OUI, DHCP fingerprinting, and device profiling<sup>1</sup>. One of the supported communication methods that FortiNAC uses for initial device identification during discovery is SNMP (Simple Network Management Protocol)<sup>3</sup>. SNMP is a protocol that allows network devices to exchange information and monitor their status<sup>4</sup>. FortiNAC can use SNMP to read information from switches and routers, such as MAC addresses, IP addresses, VLANs, and port status<sup>3</sup>. SNMP can also be used to configure network devices and enforce policies<sup>4</sup>. Reference: <sup>1</sup>: Identification | FortiNAC 9.4.0 - Fortinet Documentation <sup>2</sup>: Device profiling process | FortiNAC 8.3.0 | Fortinet Document Library <sup>3</sup>: Using FortiNAC to identify medical devices - James Pratt <sup>4</sup>: How does FortiNAC identify a new device on the network?

### QUESTION 4

An administrator has to configure LDAP authentication for ZTNA HTTPS access proxy. Which authentication scheme can the administrator apply?

- A. Basic
- B. Form-based
- C. Digest
- D. NTLM

www.VCEplus.io

**Correct Answer: B**

**Section:**

**Explanation:**

LDAP (Lightweight Directory Access Protocol) authentication for ZTNA (Zero Trust Network Access) HTTPS access proxy is effectively implemented using a Form-based authentication scheme. This approach allows for a secure, interactive, and user-friendly means of capturing credentials. Form-based authentication presents a web form to the user, enabling them to enter their credentials (username and password), which are then processed for authentication against the LDAP directory. This method is widely used for web-based applications, making it a suitable choice for HTTPS access proxy setups in a ZTNA framework.

Reference: FortiGate Security 7.2 Study Guide, LDAP Authentication configuration sections.

### QUESTION 5

FortiNAC has alarm mappings configured for MDM compliance failure, and FortiClient EMS is added as a MDM connector. When an endpoint is quarantined by FortiClient EMS, what action does FortiNAC perform?

- A. The host is isolated in the registration VLAN
- B. The host is marked at risk
- C. The host is forced to authenticate again
- D. The host is disabled

**Correct Answer: A**

**Section:**

**Explanation:**

In the scenario where FortiNAC has alarm mappings configured for MDM (Mobile Device Management) compliance failure and FortiClient EMS (Endpoint Management System) is integrated as an MDM connector, the typical response when an endpoint is quarantined by FortiClient EMS is to isolate the host in the registration VLAN. This action is consistent with FortiNAC's approach to network access control, focusing on ensuring network security.

and compliance. By moving the non-compliant or quarantined host to a registration VLAN, FortiNAC effectively segregates it from the rest of the network, mitigating potential risks while allowing for further investigation or remediation steps.

Reference: FortiNAC documentation, MDM Compliance and Response Actions.

#### QUESTION 6

Exhibit.

```
11: date=2023-03-30 time=16:35:16 eventtime=1680154516094696424 tz="+1100" logid="0005000024" t
ype="traffic" subtype="ztna" level="notice" vd="root" srcip=10.56.241.19 srcport=50012 srcintf=
"port1" srcintfrole="undefined" dstcountry="Reserved" srccountry="Reserved" dstip=10.122.0.139
dstport=443 dstintf="port2" dstintfrole="undefined" sessionid=29915726 service="HTTPS" proto=6
action="accept" policyid=1 policytype="proxy-policy" poluuid="4dc78d7e-43a2-51ed-72dc-b6336e302
8c7" policyname="External_Access_FAZ" duration=6 user="ztna_user" group="Remote_User" gatewayid
=1 vip="ZTNA-HTTPS-Server" accessproxy="ZTNA-HTTPS-Server" wanin=4816 rcvdbyte=4816 wanout=1712
lanin=1915 sentbyte=1915 lanout=9412 appcat="unscanned"
```

Based on the ZTNA logs provided, which statement is true?

- A. The Remote\_user ZTNA tag has matched the ZTNA rule
- B. An authentication scheme is configured
- C. The external IP for ZTNA server is 10.122.0.139.
- D. Traffic is allowed by firewall policy 1

**Correct Answer: A**

**Section:**

**Explanation:**

Based on the ZTNA logs provided, the true statement is:

A) The Remote\_user ZTNA tag has matched the ZTNA rule: The log includes a user tag 'ztna\_user' and a policy name 'External\_Access\_FAZ', which suggests that the ZTNA tag for 'Remote\_User' has successfully matched the ZTNA rule defined in the policy to allow access.

The other options are not supported by the information in the log:

B) An authentication scheme is configured: The log does not provide details about an authentication scheme.

C) The external IP for ZTNA server is 10.122.0.139: The log entry indicates 'dstip=10.122.0.139' which suggests that this is the destination IP address for the traffic, not necessarily the external IP of the ZTNA server.

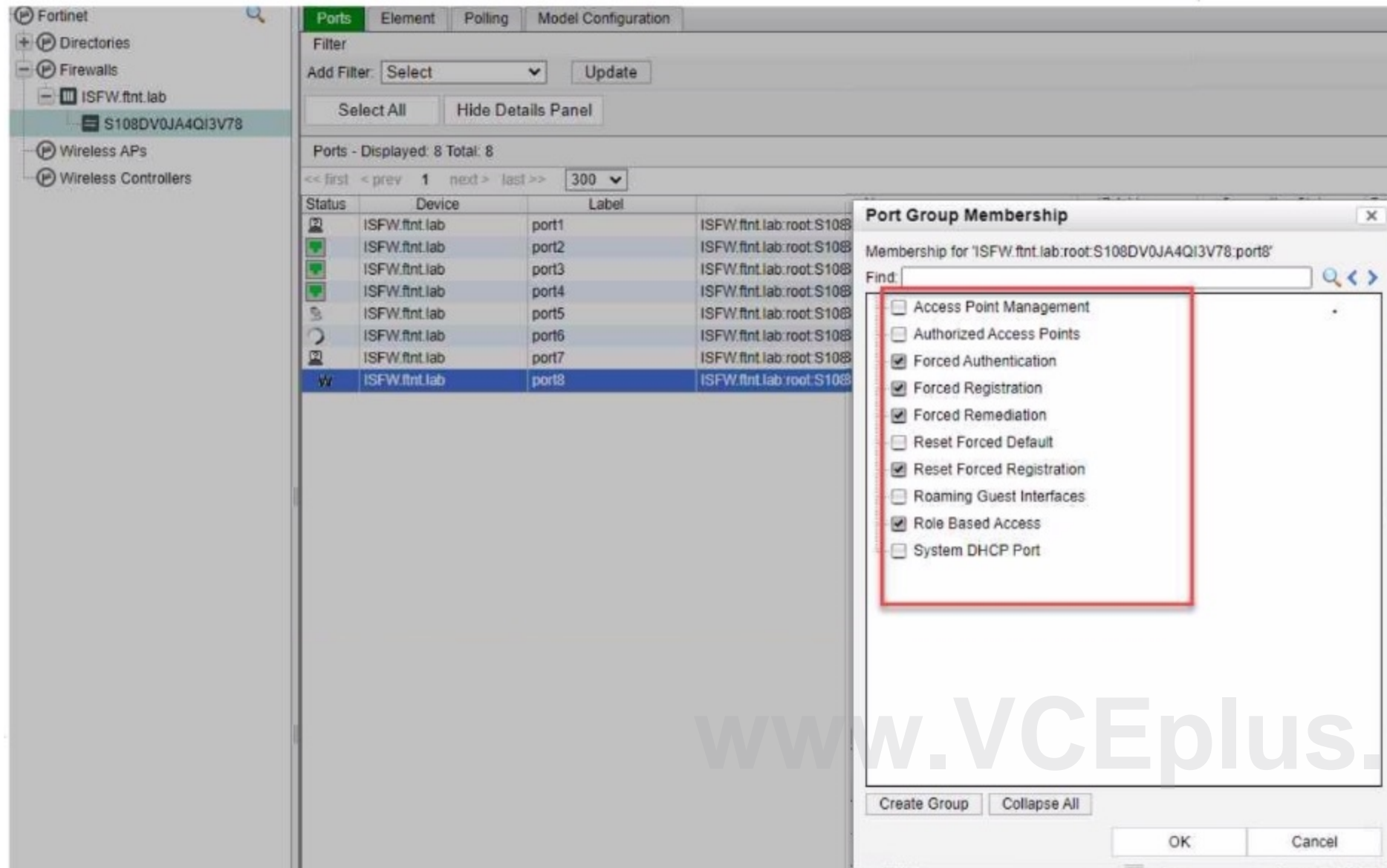
D) Traffic is allowed by firewall policy 1: The log entry 'policyid=1' indicates that the traffic is matched to firewall policy ID 1, but it does not explicitly state that the traffic is allowed; although the term 'action=accept' suggests that the action taken by the policy is to allow the traffic, the answer option D could be considered correct as well.

Interpretation of FortiGate ZTNA Log Files.

Analyzing Traffic Logs for Zero Trust Network Access.

#### QUESTION 7

Exhibit.



Which port group membership should you enable on FortiNAC to isolate rogue hosts'?

- A. Forced Authentication
- B. Forced Registration
- C. Forced Remediation
- D. Reset Forced Registration

**Correct Answer: C**

**Section:**

**Explanation:**

In FortiNAC, to isolate rogue hosts, you should enable the:

C) Forced Remediation: This port group membership is used to isolate hosts that have been determined to be non-compliant or potentially harmful. It enforces a remediation process on the devices in this group, often by placing them in a separate VLAN or network segment where they have limited or no access to the rest of the network until they are remediated.

The other options are not specifically designed for isolating rogue hosts:

A) Forced Authentication: This is used to require devices to authenticate before gaining network access.

B) Forced Registration: This group is used to ensure that all devices are registered before they are allowed on the network.

D) Reset Forced Registration: This is used to reset the registration status of devices, not to isolate them.

**QUESTION 8**

Exhibit.

Host Name ⇅	Host Status	IP Address ⇅	Physical Address ⇅
		10.1.50.2	00:0C:29:6B:9A:4E
hr	 w	10.1.104.101	00:0C:29:0D:86:A5
			00:0C:29:7B:43:94

Which statement is true about the hr endpoint?

- A. The endpoint is a rogue device
- B. The endpoint is disabled
- C. The endpoint is unauthenticated
- D. The endpoint has been marked at risk

**Correct Answer: D**

**Section:**

**Explanation:**

Based on the exhibit showing the status of the hr endpoint, the true statement about this endpoint is:

D) The endpoint has been marked at risk: The 'w' next to the host status for the 'hr' endpoint typically denotes a warning, indicating that the system has marked it as at risk due to some security policy violations or other concerns that need to be addressed.

The other options do not align with

the provided symbol 'w' in the context of FortiNAC:

A) The endpoint is a rogue device: If the endpoint were rogue, we might expect a different symbol, often indicating a critical status or alarm.

B) The endpoint is disabled: A disabled status is typically indicated by a different icon or status indicator.

C) The endpoint is unauthenticated: An unauthenticated status would also be represented by a different symbol or status indication, not a 'w'.

#### QUESTION 9

Which factor is a prerequisite on FortiNAC to add a Layer 3 router to its inventory?

- A. Allow HTTPS access from the router to the FortiNAC ethO IP address
- B. Allow FTP access to the FortiNAC database from the router
- C. The router responding to ping requests from the FortiNAC eth1 IP address
- D. SNMP or CLI access to the router to carry out remote tasks

**Correct Answer: D**

**Section:**

**Explanation:**

FortiNAC uses SNMP or CLI to communicate with network devices such as routers and switches. To add a Layer 3 router to its inventory, FortiNAC needs to have SNMP or CLI access to the router to perform remote tasks such as polling, VLAN assignment, and port shutdown. Without SNMP or CLI access, FortiNAC cannot manage the router or its ports. Therefore, SNMP or CLI access is a prerequisite for adding a Layer 3 router to FortiNAC's inventory. Reference: <https://docs.fortinet.com/document/fortinac/9.4.0/administration-guide/105927/inventory>

<https://docs.fortinet.com/document/fortinac/9.4.0/administration-guide/344098/l3-polling>

#### QUESTION 10

Which configuration is required for FortiNAC to perform an automated incident response based on the FortiGate traffic?

- A. FortiNAC should be added as a participant in the Security Fabric



- B. FortiNAC requires read-write SNMP access to FortiGate.
- C. FortiNAC should be configured as a syslog server on FortiGate
- D. FortiNAC requires HTTPS access to FortiGate for API calls

**Correct Answer: A**

**Section:**

**Explanation:**

For FortiNAC to perform automated incident response based on FortiGate traffic, the required configuration is:

A) FortiNAC should be added as a participant in the Security Fabric: By integrating FortiNAC into the Fortinet Security Fabric, it can respond to incidents based on traffic analysis performed by FortiGate. This allows for coordinated and automated responses to security events.

The other options are not specifically required for automated incident response in this context:

B) FortiNAC requires read-write SNMP access to FortiGate: While SNMP access is important for certain functions, it is not the key requirement for this specific use case.

C) FortiNAC should be configured as a syslog server on FortiGate: Configuring FortiNAC as a syslog server is useful for log collection but not specifically for automated incident response based on traffic.

D) FortiNAC requires HTTPS access to FortiGate for API calls: HTTPS access for API calls is important for integration, but it is not the primary requirement for automated incident response based on FortiGate traffic analysis.

FortiNAC Integration with FortiGate for Incident Response.

Fortinet Security Fabric Documentation.

#### QUESTION 11

What are the three core principles of ZTA? (Choose three.)

- A. Verity
- B. Be compliant
- C. Certify
- D. Minimal access
- E. Assume breach

www.VCEplus.io

**Correct Answer: A, D, E**

**Section:**

**Explanation:**

Zero Trust Architecture (ZTA) is a security model that follows the philosophy of "never trust, always verify" and does not assume any implicit trust for any entity within or outside the network perimeter. ZTA is based on a set of core principles that guide its implementation and operation. According to the NIST SP 800-207, the three core principles of ZTA are:

A) Verify and authenticate. This principle emphasizes the importance of strong identification and authentication for all types of principals, including users, devices, and machines. ZTA requires continuous verification of identities and authentication status throughout a session, ideally on each request. It does not rely solely on traditional network location or controls. This includes implementing modern strong multi-factor authentication (MFA) and evaluating additional environmental and contextual signals during authentication processes.

D) Least privilege access. This principle involves granting principals the minimum level of access required to perform their tasks. By adopting the principle of least privilege access, organizations can enforce granular access controls, so that principals have access only to the resources necessary to fulfill their roles and responsibilities. This includes implementing just-in-time access provisioning, role-based access controls (RBAC), and regular access reviews to minimize the surface area and the risk of unauthorized access.

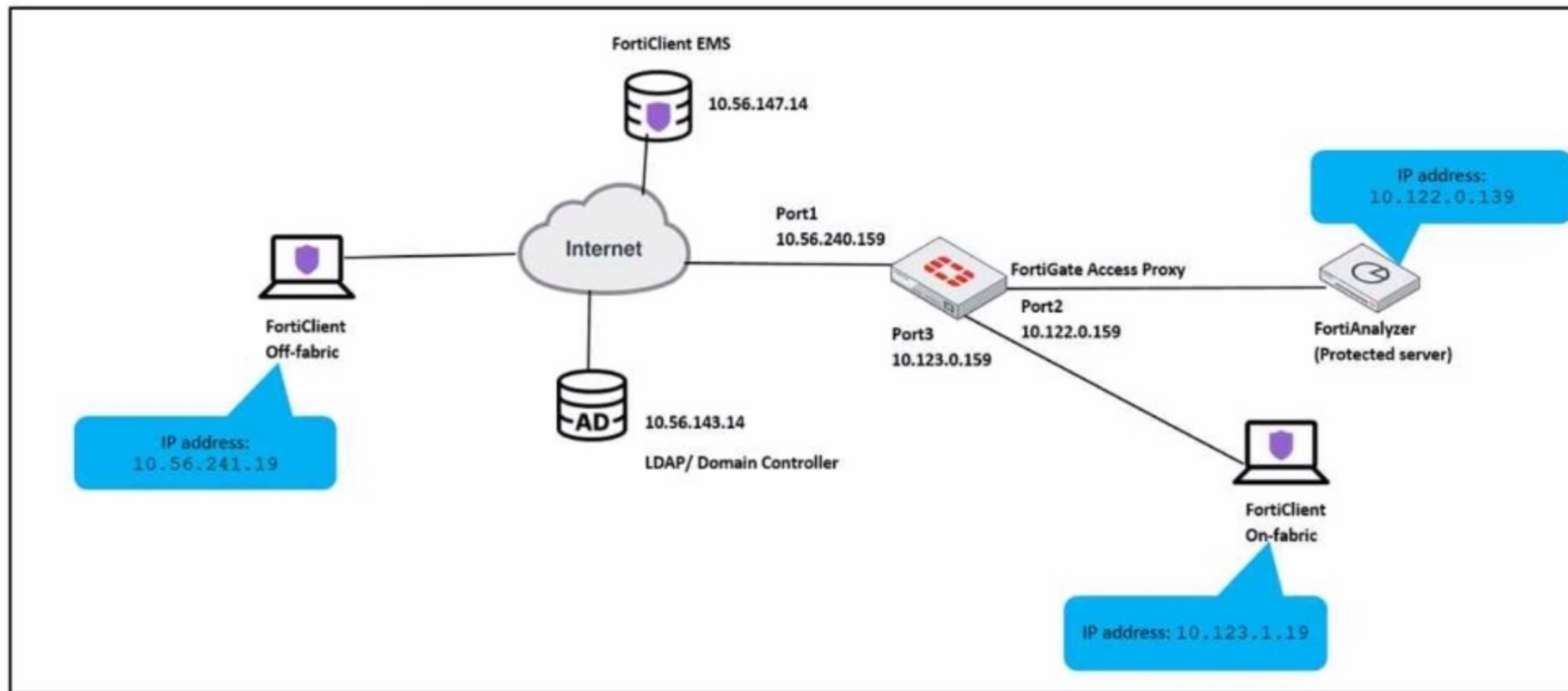
E) Assume breach. This principle assumes that the network is always compromised and that attackers can exploit any vulnerability or weakness. Therefore, ZTA adopts a proactive and defensive posture that aims to prevent, detect, and respond to threats in real-time. This includes implementing micro-segmentation, end-to-end encryption, and continuous monitoring and analytics to restrict unnecessary pathways, protect sensitive data, and identify anomalies and potential security events.

1: Understanding Zero Trust principles - AWS Prescriptive Guidance

2: Zero Trust Architecture - NIST

#### QUESTION 12

Exhibit.



An administrator has to provide on-fabric clients with access to FortiAnalyzer using ZTNA tags  
Which two conditions must be met to achieve this task? (Choose two.)

- A. The on-fabric client should have FortiGate as its default gateway
- B. The ZTNA server must be configured on FortiGate
- C. The ZTNA rule must be configured on FortiClient
- D. The IP/MAC based firewall policy must be configured on FortiGate

**Correct Answer: A, B**

**Section:**

**Explanation:**

For on-fabric clients to access FortiAnalyzer using ZTNA tags, the following conditions must be met:

- A) The on-fabric client should have FortiGate as its default gateway: This is essential to ensure that all client traffic is routed through FortiGate, where ZTNA policies can be enforced.
- B) The ZTNA server must be configured on FortiGate: For ZTNA tags to be effectively used, the ZTNA server, which processes and enforces these tags, must be configured on the FortiGate appliance.

Configuring ZTNA tags and tagging rules

Synchronizing FortiClient ZTNA tags

FortiAnalyzer

Technical Tip: ZTNA Tags fail to synchronize between FortiClient and FortiGate

### QUESTION 13

An administrator wants to prevent direct host-to-host communication at layer 2 and use only FortiGate to inspect all the VLAN traffic What three things must the administrator configure on FortiGate to allow traffic between the hosts? (Choose three.)

- A. Configure proxy ARP to allow traffic
- B. Block intra-VLAN traffic in the VLAN interface settings
- C. Add the VLAN interface to a software switch
- D. Configure static routes to allow subnets



E. Configure a firewall policy to allow the desired traffic between hosts

**Correct Answer: B, D, E**

**Section:**

**Explanation:**

To prevent direct host-to-host communication at layer 2 and use only FortiGate to inspect all the VLAN traffic, an administrator must configure:

B) Block intra-VLAN traffic in the VLAN interface settings: This setting prevents direct communication between hosts within the same VLAN, forcing traffic to be routed through FortiGate for inspection.

D) Configure static routes to allow subnets: By setting up static routes, the administrator ensures that traffic between different subnets is correctly routed through the FortiGate for inspection and policy enforcement.

E) Configure a firewall policy to allow the desired traffic between hosts: Firewall policies on the FortiGate will dictate what traffic is permitted between hosts, ensuring that only authorized traffic is allowed.

The other options are not typically required for this setup:

A) Configure proxy ARP to allow traffic: Proxy ARP is not necessary for this scenario as it involves answering ARP requests on behalf of another host, which is not relevant to blocking intra-VLAN traffic.

C) Add the VLAN interface to a software switch: This would create a switch-like environment on the FortiGate, which is counterproductive to the goal of preventing direct host-to-host communication at layer 2.

FortiGate VLAN Configuration Guide.

Blocking Intra-VLAN Communication in FortiGate.

#### QUESTION 14

Which statement is true about FortiClient EMS in a ZTNA deployment?

A. Uses endpoint information to grant or deny access to the network

B. Provides network and user identity authentication services

C. Generates and installs client certificates on managed endpoints

D. Acts as ZTNA access proxy for managed endpoints

**Correct Answer: A**

**Section:**

**Explanation:**

In a ZTNA (Zero Trust Network Access) deployment, FortiClient EMS:

A) Uses endpoint information to grant or deny access to the network: FortiClient EMS plays a critical role in ZTNA by using information about the endpoint, such as its security posture and compliance status, to determine whether to grant or deny network access.

The other options do not accurately represent the role of FortiClient EMS in ZTNA:

B) Provides network and user identity authentication services: While it contributes to the overall ZTNA strategy, FortiClient EMS itself does not directly provide authentication services.

C) Generates and installs client certificates on managed endpoints: Certificate management is typically handled by other components in the ZTNA framework.

D) Acts as ZTNA access proxy for managed endpoints: FortiClient EMS does not function as an access proxy; its role is more aligned with endpoint management and policy enforcement.

FortiClient EMS in Zero Trust Network Access Deployment.

Role of FortiClient EMS in ZTNA.

#### QUESTION 15

Exhibit.

Status	Host Name	Host Role	Operating System
 W	hr	Corporate	Windows Server 2019 ...
			

Which two statements are true about the hr endpoint? (Choose two.)

A. The endpoint application inventory could not be retrieved

B. The endpoint is marked as a rogue device

C. The endpoint has failed the compliance scan

D. The endpoint will be moved to the remediation VLAN

**Correct Answer: B, C**

**Section:**

**Explanation:**

Based on the exhibit, the true statements about the hr endpoint are:

B) The endpoint is marked as a rogue device: The 'w' symbol typically indicates a warning or an at-risk status, which can be associated with an endpoint being marked as rogue due to failing to meet the security compliance requirements or other reasons.

C) The endpoint has failed the compliance scan: The 'w' symbol can also signify that the endpoint has failed a compliance scan, which is a common reason for an endpoint to be marked as at risk.

#### QUESTION 16

With the increase in IoT devices, which two challenges do enterprises face? (Choose two.)

A. Bandwidth consumption due to added overhead of IoT

B. Maintaining a high performance network

C. Unpatched vulnerabilities in IoT devices

D. Achieving full network visibility

**Correct Answer: C, D**

**Section:**

**Explanation:**

With the increase in IoT devices, enterprises face many challenges in securing and managing their network and data. Two of the most significant challenges are:

Unpatched vulnerabilities in IoT devices (Option C): IoT devices are often vulnerable to cyber attacks due to their increased exposure to the internet and their limited computing resources. Some of the security challenges in IoT include weak password protection, lack of regular patches and updates, insecure interfaces, insufficient data protection, and poor IoT device management<sup>12</sup>. Unpatched vulnerabilities in IoT devices can allow hackers to exploit them and compromise the network or data. For example, the Mirai malware infected IoT devices by using default credentials and created a massive botnet that launched DDoS attacks on internet services<sup>2</sup>.

Achieving full network visibility (Option D): IoT devices can generate a large amount of data that needs to be collected, processed, and analyzed. However, many enterprises lack the tools and capabilities to monitor and manage the IoT devices and data effectively. This can result in poor performance, inefficiency, and security risks. Achieving full network visibility means having a clear and comprehensive view of all the IoT devices, their status, their connectivity, their data flow, and their potential threats. This can help enterprises optimize their network performance, ensure data quality and integrity, and detect and prevent any anomalies or attacks<sup>3</sup>.

#### QUESTION 17

exhibit.

```
[182:root:10]sslvpn_auth_check_usrgroup:2962 forming user/group list from policy.
[182:root:10]sslvpn_auth_check_usrgroup:3008 got user (0) group (0:1).
[182:root:10]sslvpn_validate_user_group_list:1850 validating with SSL VPN authentication
[182:root:10]sslvpn_validate_user_group_list:2864 got user (0:0), group (0:0) peer group
[182:root:10]fam_cert_send_req:1164 peer group 'SSL_VPN_Users' is sent for verification.
[182:root:10]fam_cert_send_req:1170 doing authentication for 1 group(s).
[2354] handle_req-Rcvd auth_cert req id=180791387, len=1111, opt=0
[974] __cert_auth_ctx_init-req_id=180791387, opt=0
[103] __cert_chg_st- 'Init'
[140] fnbamd_cert_load_certs_from_req-1 cert(s) in req.
[661] __cert_init-req_id=180791387
[710] __cert_build_chain-req_id=180791387
[257] fnbamd_chain_build-Chain discovery, opt 0x13, cur total 1
[273] fnbamd_chain_build-Following depth 0
[308] fnbamd_chain_build-Extend chain by system trust store. (good: 'CA_Cert_1')
[273] fnbamd_chain_build-Following depth 1
[97] fnbamd_chain_build-Self-sign detected.
[1] __cert_chg_st- 'Init' -> 'Validation'
[1] __cert_verify-req_id=180791387
[32] __cert_verify-Chain is complete.
[457] fnbamd_cert_verify-Chain number:2
[471] fnbamd_cert_verify-Following cert chain depth 0
[533] fnbamd_cert_verify-Issuer found: CA_Cert_1 (SSL_DPI opt 1)
[471] fnbamd_cert_verify-Following cert chain depth 1
[675] fnbamd_cert_check_group_list-checking group with name 'SSL_VPN_Users'
[490] __check_add_peer-check 'student'
[366] peer_subject_cn_check-Cert subject 'CN = student'
[304] __RDN_match-Checking 'CN' val 'STUDENT' -- no match.
[397] peer_subject_cn_check-checking CN 'STUDENT' failed
[497] __check_add_peer-'student' check ret:bad
[191] __get_default_ocsp_ctx-def_ocsp_ctx=(nil), no_ocsp_query=0, ocsp_enabled=0
[867] __cert_verify_do_next-req_id=180791387
[99] __cert_chg_st- 'Validation' -> 'Done'
[912] __cert_done-req_id=180791387
[1663] fnbamd_auth_session_done-Session done, id=180791387
[957] __fnbamd_cert_auth_run-Exit, req_id=180791387
[1700] create_auth_cert_session-fnbamd_cert_auth_init returns 0, id=180791387
[1619] auth_cert_success-id=180791387
[1059] fnbamd_cert_auth_copy_cert_status-req_id=180791387
[833] fnbamd_cert_check_matched_groups-checking group with name 'SSL_VPN_Users'
[903] fnbamd_cert_check_matched_groups-not matched
```

User student is not able to log in to SSL VPN

Given the output showing a real-time debug: which statement describes the login failure?

- A. Unable to verify chain of trust for the peer certificate
- B. CN does not match the user peer configuration
- C. student is not part of the usergroup SSL\_VPN\_Users.
- D. Client certificate has expired

**Correct Answer: C**

**Section:**

**Explanation:**

Given the output showing a real-time debug, the statement that describes the login failure is:

C) student is not part of the usergroup SSL\_VPN\_Users: The debug log contains a line that says 'fnbam\_cert\_check\_group\_list-checking group with name 'SSL\_VPN\_Users' followed by 'peer\_check\_add\_peer\_check\_student' and later 'RDN\_match-Checking 'CN' val 'STUDENT' -- no match.' This suggests that the certificate presented has a common name (CN) of 'student', which does not match or is not authorized under the 'SSL\_VPN\_Users' group expected for successful authentication.

#### QUESTION 18

In which FortiNAC configuration stage do you define endpoint compliance?

- A. Device onboarding
- B. Management configuration
- C. Policy configuration
- D. Network modeling

**Correct Answer: C**

**Section:**

**Explanation:**

Endpoint compliance is defined in the policy configuration stage of FortiNAC. Endpoint compliance policies specify which endpoint compliance configuration and user/host profile are applied to a host based on its location, user, and device type. Endpoint compliance configurations define whether a host is required to download an agent and undergo a scan, permitted access with no scan, or denied access. The scan parameters and security actions are also configured in the endpoint compliance configurations. Therefore, to define endpoint compliance, you need to create and assign endpoint compliance policies and configurations in the policy configuration stage of FortiNAC. Reference:= <https://docs.fortinet.com/document/fortinac/9.4.0/administration-guide/985922/endpoint-compliance-policies>  
<https://docs.fortinet.com/document/fortinac/9.4.0/fortinac-manager/161887/endpoint-compliance-configurations>

www.VCEplus.io