Free Questions for NSE7_ZTA-7.2 by actualtestdumps

Shared by Rosa on 22-07-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Which statement is true about disabled hosts on FortiNAC?

Options:

A- They are quarantined and placed in the remediation VLAN

B- They are placed in the authentication VLAN to reauthenticate

C- They are marked as unregistered rogue devices

D- They are placed in the dead end VLAN

Answer:

A

Explanation:

They are quarantined and placed in the remediation VLAN. This is a standard practice in network access control systems where non-compliant or disabled hosts are isolated in a VLAN where they can be remediated or reviewed.

Question 2

Question Type: MultipleChoice

Which two types of configuration can you associate with a user/host profile on FortiNAC? (Choose two.)

Options:

A- Service Connectors

B- Network Access

C- Inventory

D- Endpoint compliance

Answer:

B, D

Explanation:

User/host profiles are used to map sets of hosts and users to different types of policies or rules on FortiNAC. Among the options given, network access and endpoint compliance are the two types of configuration that can be associated with a user/host profile. Network access configuration determines the VLAN, CLI configuration or VPN group that is assigned to a host or user based on their profile. Endpoint compliance configuration defines the policies that check the host or user for compliance status, such as antivirus, firewall, patch level, etc. Service connectors and inventory are not types of configuration, but features of FortiNAC that allow integration with other services and devices, and collection of host and user data, respectively.Reference:=User/host profiles | FortiNAC 9.4.0 - Fortinet DocumentationandUser/host profiles | FortiNAC 9.4.0 - Fortinet Documentation

Question 3

Question Type: MultipleChoice

What happens when FortiClient EMS is configured as an MDM connector on FortiNAC?

Options:

A- FortiNAC sends the host data to FortiClient EMS to update its host database

B- FortiClient EMS verifies with FortiNAC that the device is registered

C- FortiNAC polls FortiClient EMS periodically to update already registered hosts in FortiNAC

D- FortiNAC checks for device vulnerabilities and compliance with FortiClient

Answer:

C

Explanation:

When FortiClient EMS is configured as an MDM connector on FortiNAC, it allows FortiNAC to obtain host information from FortiClient EMS and use it for network access control. FortiNAC polls FortiClient EMS periodically (every 5 minutes by default) to update already registered hosts in FortiNAC. This ensures that FortiNAC has the latest host data from FortiClient EMS, such as device type, OS, IP address, MAC address, hostname, and FortiClient version. FortiNAC can also use FortiClient EMS as an authentication source for devices that have FortiClient installed.FortiNAC does not send any data to FortiClient EMS or check for device vulnerabilities and compliance with FortiClient123.Reference:=1: MDM Service Connectors | FortiClient EMS Integration2: FortiClient EMS Device Integration|FortiNAC 9.4.0 - Fortinet Documentation3: Technical Tip: Integration with FortiClient EMS

Question 4

Question Type: MultipleChoice

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

Options:

A- LLDP

B- SNMP

C- API

D- SSH

Answer:

B

Explanation:

FortiNAC uses a variety of methods to identify devices on the network, such as Vendor OUI, DHCP fingerprinting, and device profiling12.One of the supported communication methods that FortiNAC uses for initial device identification during discovery is SNMP (Simple Network Management Protocol)3.SNMP is a protocol that allows network devices to exchange information and monitor their status4.FortiNAC can use SNMP to read information from switches and routers, such as MAC addresses, IP addresses, VLANs, and port status3.SNMP can also be used to configure network devices and enforce policies4.Reference:1: Identification | FortiNAC 9.4.0 - Fortinet Documentation2: Device profiling process | FortiNAC 8.3.0 | Fortinet Document Library3: Using FortiNAC to identify medical devices - James Pratt4: How does FortiNAC identify a new device on the network?

Question 5

Question Type: MultipleChoice

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

Options:

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

Answer:

B, D

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 6

Question Type: **MultipleChoice**

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?

Options:

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

Answer:

D

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.

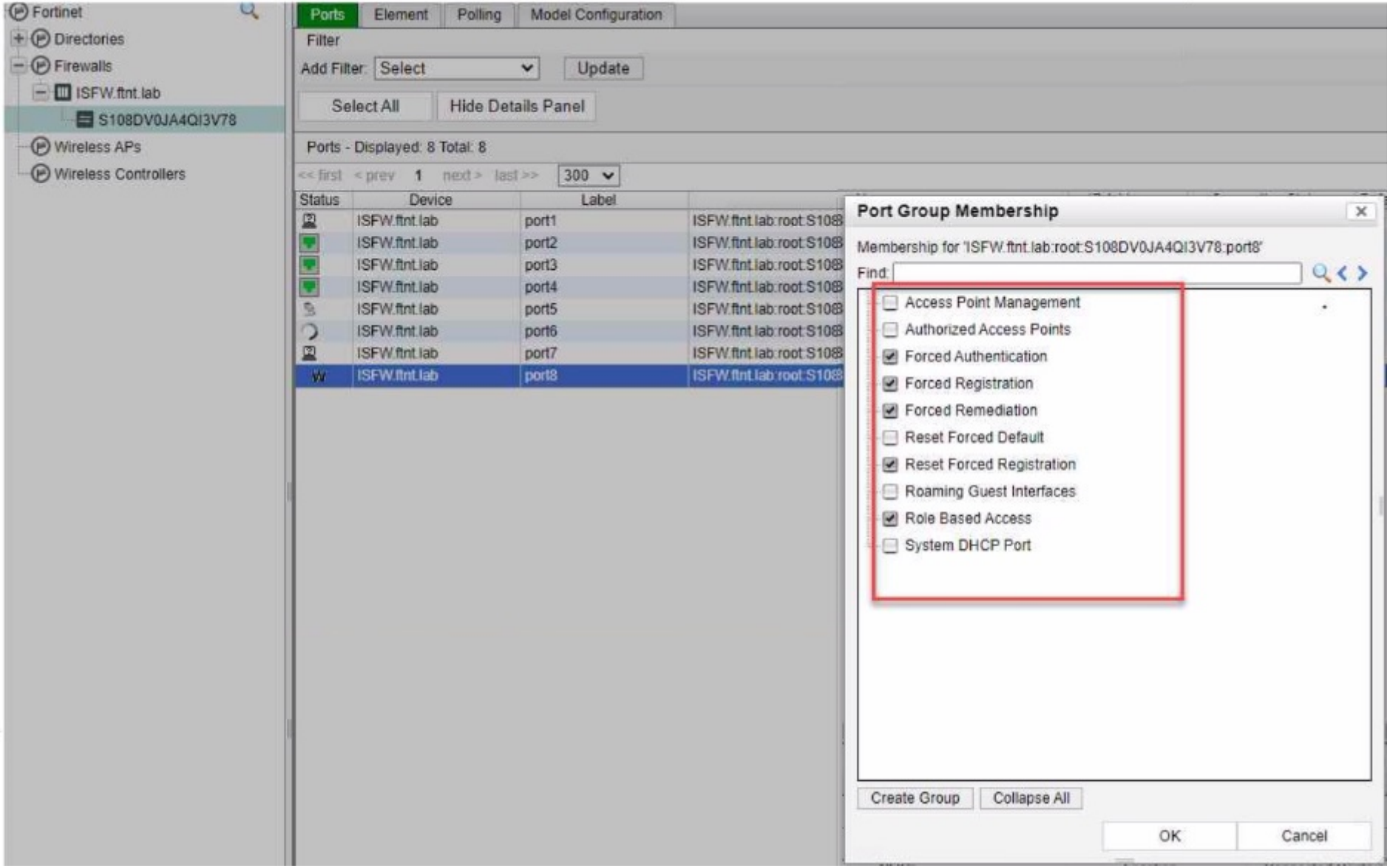
B) The endpoint is disabled: A disabled status is typically indicated by a different icon or status indicator.

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

Question 7

Question Type: **MultipleChoice**

Exhibit.


Fortinet
Directories
Firewalls
ISFW.ftnt.lab
S108DV0JA4QI3V78
Wireless APs
Wireless Controllers
Ports
Element
Polling
Model Configuration
Filter
Add Filter: Select
Update
Select All
Hide Details Panel
Ports - Displayed: 8 Total: 8
<< first < prev 1 next > last >> 300
Status
Device
Label
ISFW.ftnt.lab port1
ISFW.ftnt.lab port2
ISFW.ftnt.lab port3
ISFW.ftnt.lab port4
ISFW.ftnt.lab port5
ISFW.ftnt.lab port6
ISFW.ftnt.lab port7
ISFW.ftnt.lab port8
Port Group Membership
Membership for 'ISFW.ftnt.lab:root:S108DV0JA4QI3V78:port8'
Find:
Access Point Management
Authorized Access Points
Forced Authentication
Forced Registration
Forced Remediation
Reset Forced Default
Reset Forced Registration
Roaming Guest Interfaces
Role Based Access
System DHCP Port
Create Group
Collapse All
OK
Cancel

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

Options:

A- Forced Authentication

B- Forced Registration

C- Forced Remediation

D- Reset Forced Registration

Answer:

C

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.

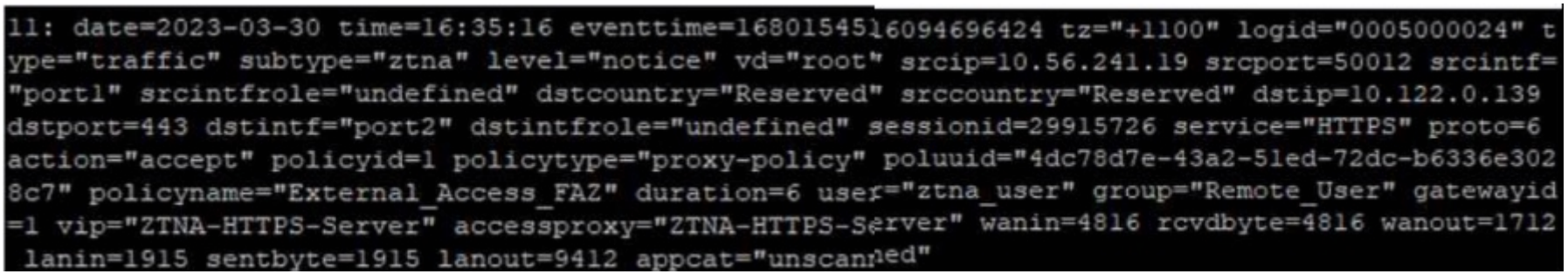
B) Forced Registration: This group is used to ensure that all devices are registered before they are allowed on the network.

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

Question 8

Question Type: MultipleChoice

Exhibit.



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

Options:

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

Answer:

A

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 9

Question Type: **MultipleChoice**

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?

Options:

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

Answer:

A

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 10

Question Type: MultipleChoice

An administrator has to configure LDAP authentication tor ZTNA HTTPS access proxy Which authentication scheme can the administrator apply1?

Options:

A- Basic

B- Form-based

C- Digest

D- NTLM

Answer:

B

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.