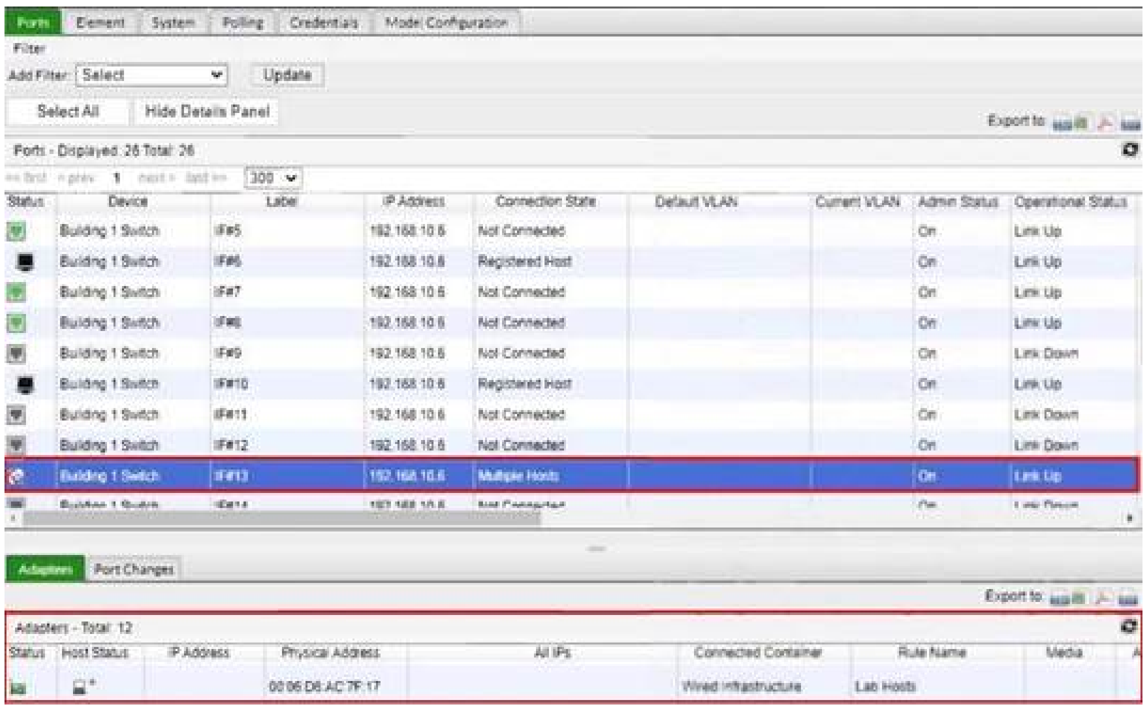
Fortinet

Exam Questions NSE6_FNC-7.2

Fortinet NSE 6 - FortiNAC 7.2

NEW QUESTION 1
Refer to the exhibit.



Status	Device	Label	IP Address	Connection State	Default VLAN	Current VLAN	Admin Status	Operational Status
	Building 1 Switch	IF#5	192.168.10.6	Not Connected			On	Link Up
	Building 1 Switch	IF#6	192.168.10.6	Registered Host			On	Link Up
	Building 1 Switch	IF#7	192.168.10.6	Not Connected			On	Link Up
	Building 1 Switch	IF#8	192.168.10.6	Not Connected			On	Link Up
	Building 1 Switch	IF#9	192.168.10.6	Not Connected			On	Link Down
	Building 1 Switch	IF#10	192.168.10.6	Registered Host			On	Link Up
	Building 1 Switch	IF#11	192.168.10.6	Not Connected			On	Link Down
	Building 1 Switch	IF#12	192.168.10.6	Not Connected			On	Link Down
	Building 1 Switch	IF#13	192.168.10.6	Multiple Hosts			On	Link Up
	Building 1 Switch	IF#14	192.168.10.6	Not Connected			On	Link Down

Adapters - Total: 12

Status	Host Status	IP Address	Physical Address	All IPs	Connected Container	Rule Name	Media	A
			00:06:D6:AC:7F:17		Wired Infrastructure	Lab Hosts		

What would happen if the highlighted port with connected hosts was placed in both the Forced Registration and Forced Remediation port groups?

A. Multiple enforcement groups could not contain the same port.
B. Only the higher ranked enforcement group would be applied.
C. Both types of enforcement would be applied.
D. Enforcement would be applied only to rogue hosts.

Answer: B

Explanation:
In systems like FortiNAC, when a port is designated to be in multiple enforcement groups, it is common for only the higher-priority or higher-ranked group's policies to be applied. This is to prevent conflicting enforcement actions from being attempted on the same port. Although the specific details of the priority or ranking system are not provided in the extracted references, the principle of hierarchical policy enforcement suggests that only the policies of the higher-ranked group would be applied to the port.
References
? FortiNAC documentation would typically outline this behavior in sections discussing port group enforcement or policy application.

NEW QUESTION 2
During an evaluation of state-based enforcement, an administrator discovers that ports that should not be under enforcement have been added to enforcement groups. In which view would the administrator be able to determine who added the ports to the groups?

A. The Alarms view
B. The Admin Auditing view
C. The Event Management view
D. The Security Events view

Answer: B

NEW QUESTION 3
By default, if after a successful Layer 2 poll, more than 20 endpoints are seen connected on a single switch port simultaneously, what happens to the port?

A. The port becomes a threshold uplink
B. The port is disabled
C. The port is added to the Forced Registration group
D. The port is switched into the Dead-End VLAN

Answer: A

Explanation:
If more than 20 endpoints are seen connected on a single switch port simultaneously after a successful Layer 2 poll, the port is designated as an uplink. FortiNAC will ignore all physical addresses learned on an uplink port and will not perform any control operations on it

NEW QUESTION 4
In a wireless integration, what method does FortiNAC use to obtain connecting MAC address information?

A. SNMP traps
B. RADIUS
C. Endstation traffic monitoring
D. Link traps

Answer: B

Explanation:
In a wireless integration, FortiNAC uses RADIUS to obtain connecting MAC address information. This includes RADIUS requests to FortiNAC and subsequent RADIUS responses from FortiNAC to the requesting device

NEW QUESTION 5
Which three are components of a security rule? (Choose three.)

A. Methods
B. Security String
C. Trigger
D. User or host profile
E. Action

Answer: CDE

Explanation:
Components of a security rule in FortiNAC include:
? Trigger: The condition or event that initiates the evaluation of the rule.
? User or Host Profile: A requirement that can be added to a rule to specify the user or host profile that must be matched.
? Action: The activities or responses that FortiNAC performs when the rule is matched.
References
? FortiNAC 7.2 Study Guide, page 419

NEW QUESTION 6
By default, if more than 20 hosts are seen connected on a single port simultaneously, what will happen to the port?

A. The port is switched into the Dead-End VLAN.
B. The port becomes a threshold uplink.
C. The port is disabled.
D. The port is added to the Forced Registration group.

Answer: B

Explanation:
Admin Guide p. 754: Threshold Uplink—The Uplink mode has been set as Dynamic and FortiNAC has determined that the number of MAC addresses on the port exceeds the System Defined Uplink count. All hosts read on this port are ignored.

NEW QUESTION 7
What method of communication does FortiNAC use to control VPN host access on FortiGate?

A. RSSO
B. Security Fabric
C. RADIUS accounting
D. SAMLSSO

Answer: B

NEW QUESTION 8
Which two are required for endpoint compliance monitors? (Choose two.}

A. Custom scan
B. ZTNA agent
C. Persistent agent
D. MDM integration

Answer: AC

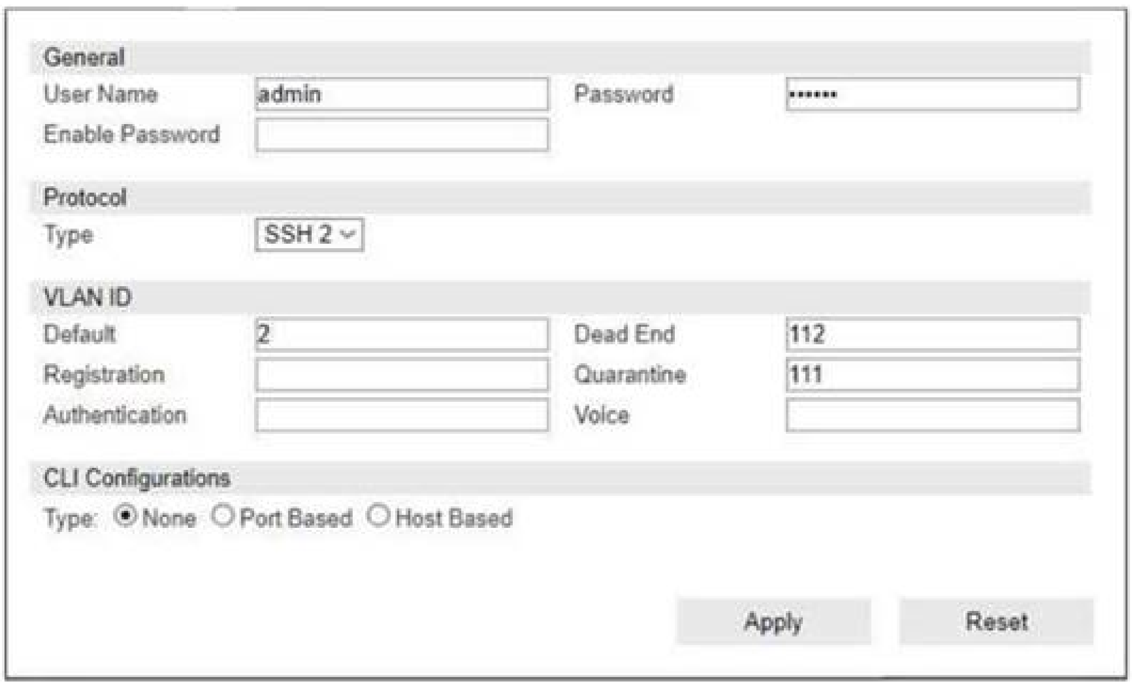
NEW QUESTION 9
Where should you configure MAC notification traps on a supported switch?

A. Configure them only after you configure linkup and linkdown traps.
B. Configure them on all ports on the switch.
C. Configure them only on ports set as 802 1g trunks.
D. Configure them on all ports except uplink ports.

Answer: C

Explanation:
In general, for network switches supporting MAC notification traps, it's advisable to configure these traps on all ports except uplink ports. Uplink ports are used for connecting to other switches or network infrastructure devices and typically don't need MAC notification traps, which are more relevant for end-device connectivity monitoring.
The study guide specifies that MAC notification traps should not be configured on interfaces that are uplinks. They are the preferred method for learning and updating Layer 2 information and should be used whenever available, but not on uplink interfaces.

NEW QUESTION 10
Refer to the exhibit.



General

User Name	admin	Password	••••••
Enable Password			

Protocol

Type: SSH 2

VLAN ID

Default	2	Dead End	112
Registration		Quarantine	111
Authentication		Voice	

CLI Configurations

Type: ● None ○ Port Based ○ Host Based

If you are forcing the registration of unknown (rogue) hosts, and an unknown (rogue) host connects to a port on the switch, what occurs?

A. The host is moved to VLAN 111.
B. The host is moved to a default isolation VLAN.
C. No VLAN change is performed.
D. The host is disabled.

Answer: A

Explanation:
The exhibit shows a configuration panel where VLAN IDs are specified for different states, such as Default, Registration, and Authentication. When forcing the registration of unknown (rogue) hosts, if an unknown host connects to a port on the switch, the FortiNAC system will move the host to the VLAN designated for Registration. In the exhibit, the VLAN ID for Registration is set to 111, hence the host would be moved to VLAN 111 to undergo the registration process.

NEW QUESTION 10
What would occur if both an unknown (rogue) device and a known (trusted) device simultaneously appeared on a port that is a member of the Forced Registration port group?

A. The port would be provisioned for the normal state host, and both hosts would have access to that VLAN.
B. The port would not be managed, and an event would be generated.
C. The port would be provisioned to the registration network, and both hosts would be isolated.
D. The port would be administratively shut down.

Answer: C

Explanation:
When a rogue device connects to a port in the Forced Registration port group, FortiNAC's response is to isolate that device by moving it to a registration captive network. This is part of FortiNAC's state-based control mechanism, where the system acts based on the state of the device (normal, rogue, etc.) and the group or port it is connected to. In this specific scenario, the focus is on the isolation of the rogue device, and the guide does not explicitly detail the simultaneous handling of the normal device.
References: FortiNAC 7.2 Study Guide, State-Based Control section.

NEW QUESTION 11
In an isolation VLAN which three services does FortiNAC supply? (Choose three.)

A. NTP
B. DHCP
C. Web
D. DNS
E. ISMTP

Answer: BCD

Explanation:
In an isolation VLAN, FortiNAC supplies DHCP and DNS services. The guide specifies that FortiNAC has a DHCP scope defined for a particular VLAN and should be the only DHCP server available to hosts on that VLAN. Additionally, hosts on the VLAN would get a DNS server configuration of the FortiNAC IP for that VLAN

NEW QUESTION 16
What causes a host's state to change to "at risk"?

A. The host has failed an endpoint compliance policy or admin scan.
B. The logged on user is not found in the Active Directory.
C. The host has been administratively disabled.
D. The host is not in the Registered Hosts group.

Answer: A

Explanation:
Failure – Indicates that the host has failed the scan. This option can also be set manually. When the status is set to Failure the host is marked "At Risk" for the selected scan.

Reference: https://docs.fortinet.com/document/fortinac/8.3.0/administration-guide/241168/host-health-and-scanning
p. 244 of the Study Guide, "A state of at-risk indicates the host has failed a scan. This could be a compliance scan or an administrative scan."

NEW QUESTION 17
When FortiNAC is managing VPN clients connecting through FortiGate. why must the clients run a FortiNAC agent?

A. To collect user authentication details
B. To meet the client security profile rule for scanning connecting clients
C. To collect the client IP address and MAC address
D. To transparently update the client IP address upon successful authentication

Answer: B

NEW QUESTION 18
Which system group will force at-risk hosts into the quarantine network, based on point of connection?

A. Physical Address Filtering
B. Forced Quarantine
C. Forced Isolation
D. Forced Remediation

Answer: D

Explanation:
Forced Quarantine, study guide 7.2 pag 245 and 248

NEW QUESTION 23
Which devices would be evaluated by device profiling rules?

A. Rogue devices, each time they connect
B. All hosts, each time they connect
C. Known trusted devices, each time they change location
D. Rogue devices, only when they are initially added to the database

Answer: B

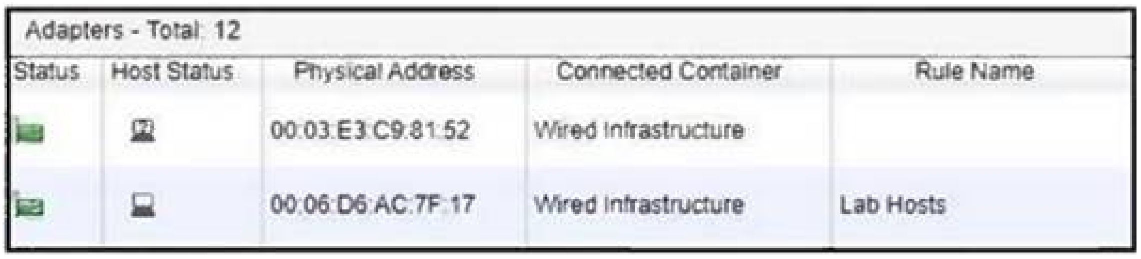
Explanation:
Device profiling rules in FortiNAC are used to evaluate and classify rogue devices. These rules can be configured to automatically, manually, or through sponsorship evaluate and classify unknown untrusted devices as they are identified and created. References
? FortiNAC 7.2 Study Guide, page 98

NEW QUESTION 26
When FortiNAC is managing FortiGate VPN users, why is an endpoint compliance policy necessary?

A. To confirm installed security software
B. To validate the VPN user credentials
C. To designate the required agent type
D. To validate the VPN client being used

Answer: A

NEW QUESTION 27
Refer to the exhibit.



Adapters - Total: 12

Status	Host Status	Physical Address	Connected Container	Rule Name
🟩	💻	00:03:E3:C9:81:52	Wired Infrastructure	
🟩	💻	00:06:D6:AC:7F:17	Wired Infrastructure	Lab Hosts

Considering the host status of the two hosts connected to the same wired port, what will happen if the port is a member of the Forced Registration port group?

A. The port will be provisioned for the normal state host, and both hosts will have access to that VLAN.
B. The port will not be managed, and an event will be generated.
C. The port will be provisioned to the registration network, and both hosts will be isolated.
D. The port will be administratively shut down.

Answer: C

Explanation:
The exhibit shows the status of two hosts connected to a wired infrastructure and indicates their respective MAC addresses and the rule name associated with them. When a port is a member of the Forced Registration port group, and multiple hosts with different statuses are connected to that port, FortiNAC will provision the port to the registration network, which is designed to isolate hosts until they are verified or registered. This ensures that unregistered or unauthorized hosts do not gain access to the network. Therefore, both hosts will be isolated in the registration network according to FortiNAC policy for such scenarios.

NEW QUESTION 30

Which agent can receive and display messages from FortiNAC to the end user?

A. Dissolvable
B. Persistent
C. Passive
D. MDM

Answer: B

Explanation:
The persistent agent has the ability to display messages on the desktop of an endpoint. These messages can target an individual host, a group of hosts, or all hosts with the persistent agent installed. The messaging options include sending a message content with an optional web address link

NEW QUESTION 34
Which three circumstances trigger Layer 2 polling of infrastructure devices? (Choose three.)

A. Manual polling
B. Scheduled poll timings
C. A failed Layer 3 poll
D. A matched security policy
E. Linkup and Linkdown traps

Answer: ABE

Explanation:
A. Manual Polling: This is when an administrator or network operator initiates a poll manually to gather information or check the status of the network devices. This can be done for immediate troubleshooting or assessment.
* B. Scheduled Poll Timings: Network management systems often have the capability to schedule regular polls of devices to check their status or monitor their performance. These scheduled polls can be set at regular intervals (such as every few minutes, hours, or daily) depending on the requirements of the network.
* E. Linkup and Linkdown Traps: SNMP (Simple Network Management Protocol) traps, like Linkup and Linkdown, are automated notifications sent from network devices to a management system. A Linkup trap indicates that a particular interface has become active (up), while a Linkdown trap indicates that an interface has become inactive (down). These traps can trigger Layer 2 polling to ascertain the current status of network interfaces and devices.

NEW QUESTION 36
Two FortiNAC devices have been configured in an HA configuration. After five failed heartbeats between the primary device and secondary device, the primary device fail to ping the designated gateway. What happens next?

A. The primary device continues to operate as the in-control device and changes the status or secondary device to contact lost.
B. The primary device changes its designation to secondary, and the secondary device changes to primary.
C. The primary device shuts down NAC processes and changes to a management down status.
D. The primary device waits 3 minutes and attempts to re-establish the HA heartbeat before attempting a second ping of the gateway.

Answer: C

NEW QUESTION 41
During the on-boarding process through the captive portal, what are two reasons why a host that successfully registered would remain stuck in the Registration VLAN? (Choose two.)

A. The wrong agent is installed.
B. The port default VLAN is the same as the Registration VLAN.
C. Bridging is enabled on the host.
D. There is another unregistered host on the same port.

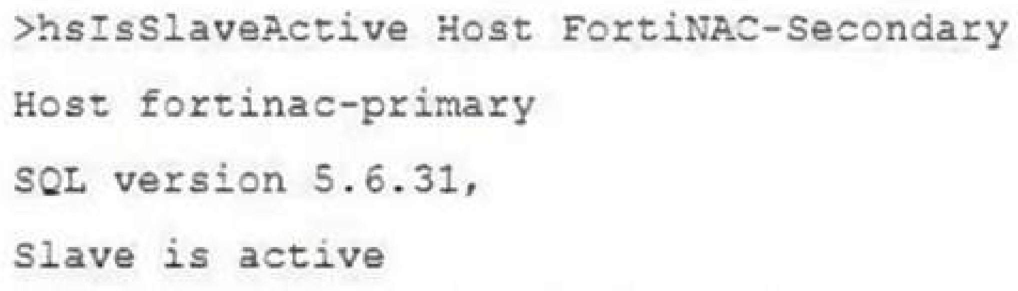
Answer: BD

NEW QUESTION 42
How does FortiGate update FortiNAC about VPN session information?

A. API calls to FortiNAC
B. Syslog messages
C. SNMP traps
D. Security Fabric Integration

Answer: B

NEW QUESTION 47
View the command and output.



```
>hsIsSlaveActive Host FortiNAC-Secondary

Host fortinac-primary

SQL version 5.6.31,

Slave is active
```

What is the state of database replication?

A. Secondary to primary synchronization failed.
B. Primary to secondary synchronization failed.
C. Secondary to primary synchronization was successful.
D. Primary to secondary database synchronization was successful.

Answer: D

Explanation:
The command and output shown in the exhibit indicate that the host FortiNAC-Secondary is referencing FortiNAC-Primary, and it states "Slave is active." In database replication terminology within a high availability setup, the term "Slave is active" typically means that the secondary server (slave) is actively receiving data from the primary server (master). This implies that the synchronization process from the primary to the secondary database has been successful and is currently active.
References
? FortiNAC 7.2 Study Guide, Security Policies section

NEW QUESTION 48
Which two agents can validate endpoint compliance transparently to the end user? (Choose two.)

A. Dissolvable
B. Mobile
C. Passive
D. Persistent

Answer: AD

Explanation:
Both dissolvable and persistent agents can be used to validate endpoint compliance transparently to the end user. The persistent agent stays resident on the endpoint and performs scheduled scans in the background. The dissolvable agent is a run- once agent that dissolves after reporting its results, leaving no footprint on the endpoint

NEW QUESTION 50
What capability do logical networks provide?

A. Point of access-base autopopulation of device groups'
B. Interactive topology view diagrams
C. Application of different access values from a single access policy
D. IVLAN -based inventory reporting

Answer: C

Explanation:
Logical Networks allow you to create fewer Network Access Policies than before. (FortiNAC - What's new in FortiNAC 7.2)
Logical networks in FortiNAC decouple a policy from a specific access value, allowing for the application of different access values from a single access policy. This is done based on the point of connection, significantly reducing the number of network access policies needed and simplifying network access policy management

NEW QUESTION 53
......