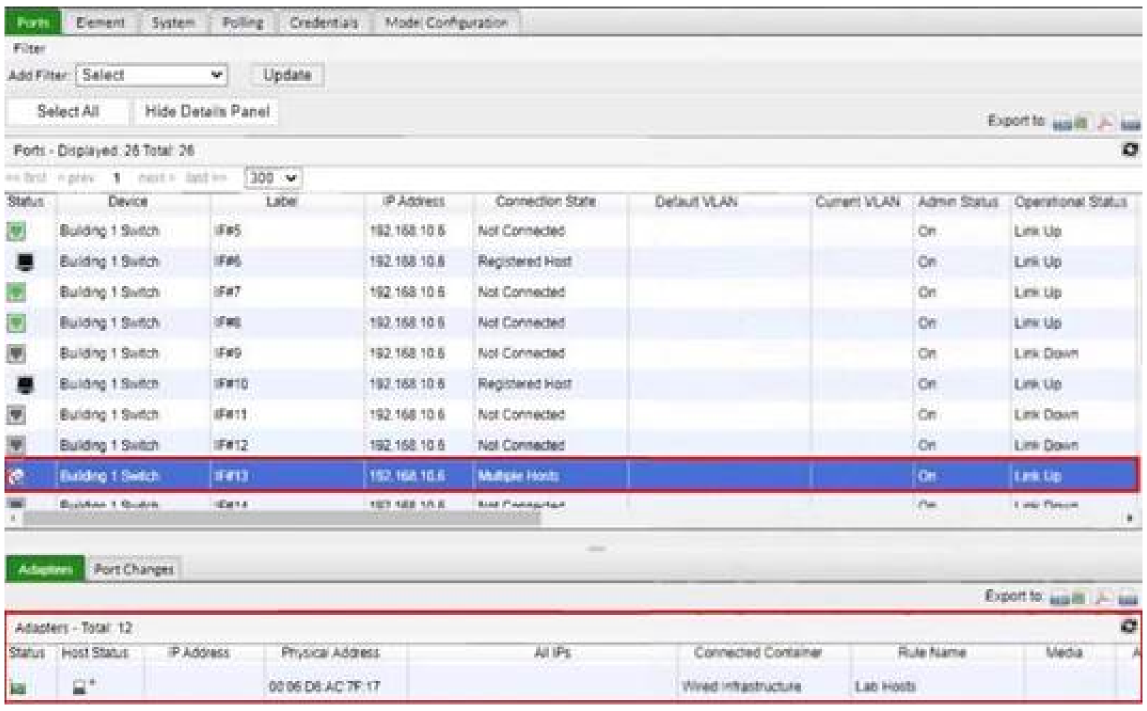
Fortinet

Exam Questions NSE6_FNC-7.2

Fortinet NSE 6 - FortiNAC 7.2

NEW QUESTION 1
Refer to the exhibit.



Ports - Displayed: 26 Total: 26

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
			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
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 3
An administrator wants the Host At Risk event to generate an alarm. What is used to achieve this result?

A. A security trigger activity
B. A security filter
C. An event to alarm mapping
D. An event to action mapping

Answer: C

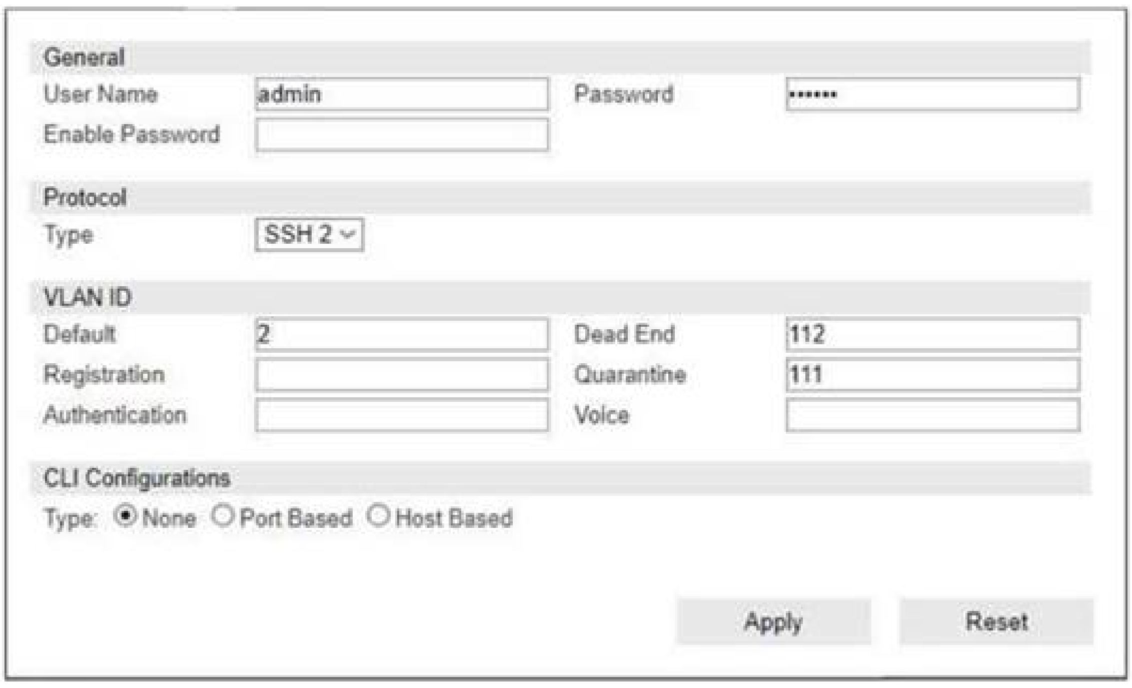
Explanation:
To generate an alarm from a Host At Risk event, an administrative user must create an Event to Alarm Mapping for the Vulnerability Scan Failed event. Within this alarm mapping, a host security action must be designated to mark the host at risk

NEW QUESTION 4
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 5
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 6
Which three communication methods are used by FortiNAC to gather information from and control, infrastructure devices? (Choose three.)

A. CLI
B. SMTP
C. SNMP
D. FTP
E. RADIUS

Answer: ACE

Explanation:
FortiNAC Study Guide 7.2 | Page 11
FortiNAC uses various methods to communicate with infrastructure devices such as SNMP for discovery and ongoing management, SSH or Telnet through the CLI for tasks related to the infrastructure, and RADIUS for handling specific types of requests

NEW QUESTION 7
Which two methods can be used to gather a list of installed applications and application details from a host? (Choose two.)

A. Agent technology
B. Portal page on-boarding options
C. MDM integration
D. Application layer traffic inspection

Answer: AC

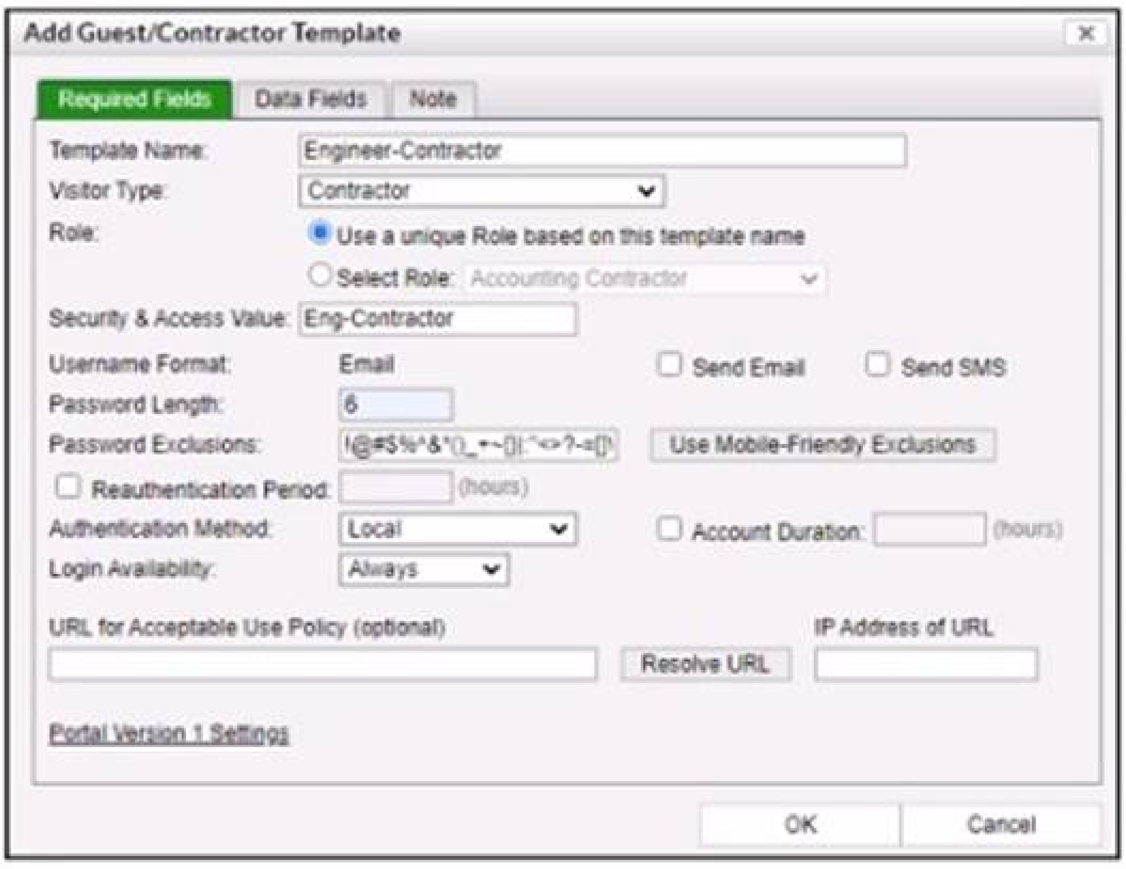
Explanation:
To gather a list of installed applications and application details from a host, two methods can be used:
? Agent technology: FortiNAC uses agent technology to collect all installed applications on an endpoint.
? Integration with MDMs (Mobile Device Management systems): MDMs that support application gathering can be integrated with FortiNAC to collect application information.
References
? FortiNAC 7.2 Study Guide, page 302

NEW QUESTION 8
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 9
Refer to the exhibit.



Add Guest/Contractor Template

Template Name: Engineer-Contractor
Visitor Type: Contractor
Role: ● Use a unique Role based on this template name
○ Select Role: Accounting Contractor
Security & Access Value: Eng-Contractor
Username Format: Email □ Send Email □ Send SMS
Password Length: 6
Password Exclusions: !@#$%^&*()_+~{}|:"<>?-=[]\ Use Mobile-Friendly Exclusions
□ Reauthentication Period: (hours)
Authentication Method: Local □ Account Duration: (hours)
Login Availability: Always
URL for Acceptable Use Policy (optional)
Resolve URL
IP Address of URL
Portal Version 1 Settings

When a contractor account is created using this template, what value will be set in the accounts Rote field?

A. Accounting Contractor
B. Eng-Contractor
C. Engineer-Contractor
D. Conti actor

Answer: C

NEW QUESTION 10
While troubleshooting a network connectivity issue, an administrator determines that a device was being automatically provisioned to an incorrect VLAN. Where would the administrator look to determine when and why FortiNAC made the network access change?

A. The Event view
B. The Admin Auditing view
C. The Port Changes view
D. The Connections view

Answer: C

NEW QUESTION 10
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 12
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 17
An administrator is configuring FortiNAC to manage FortiGate VPN users. As part of the configuration, the administrator must configure a few FortiGate firewall policies.
What is the purpose of the FortiGate firewall policy that applies to unauthorized VPN clients?

A. To deny access to only the production DNS server
B. To allow access to only the FortiNAC VPN interface
C. To allow access to only the production DNS server
D. To deny access to only the FortiNAC VPN interface

Answer: B

NEW QUESTION 21
With enforcement for network access policies and at-risk hosts enabled, what will happen if a host matches a network access policy and has a state of "at risk"?

A. The host is provisioned based on the default access defined by the point of connection.
B. The host is provisioned based on the network access policy.
C. The host is isolated.
D. The host is administratively disabled.

Answer: C

Explanation:
https://training.fortinet.com/pluginfile.php/1912463/mod_resource/content/26/FortiNAC_7.2_Study_Guide-Online.pdf C. Page 327 - moved to the quarantine isolation network

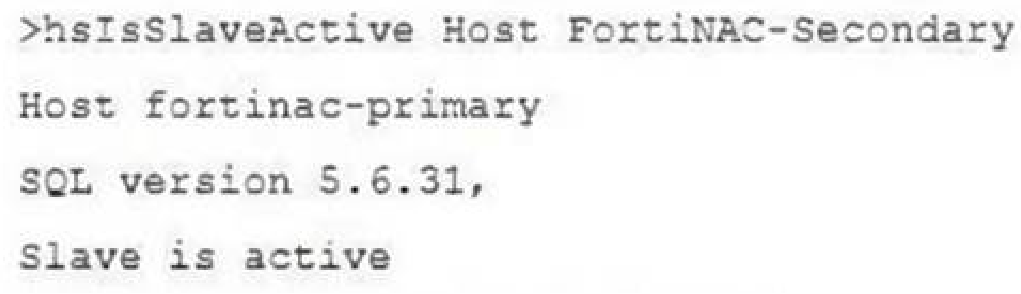
NEW QUESTION 24
When you create a user or host profile; which three criteria can you use? (Choose three.)

A. An applied access policy
B. Administrative group membership
C. Location
D. Host or user group memberships
E. Host or user attributes

Answer: CDE

Explanation:
Fortinac-admin-operations, P. 391

NEW QUESTION 28
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 33
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 38

......

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

NSE6_FNC-7.2 Practice Exam Features:

* NSE6_FNC-7.2 Questions and Answers Updated Frequently

* NSE6_FNC-7.2 Practice Questions Verified by Expert Senior Certified Staff

* NSE6_FNC-7.2 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* NSE6_FNC-7.2 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
Order The NSE6_FNC-7.2 Practice Test Here