Fortinet

Exam Questions NSE6_FNC-7.2

Fortinet NSE 6 - FortiNAC 7.2

NEW QUESTION 1
Which two policy types can be created on a FortiNAC Control Manager? (Choose two.)

A. Authentication
B. Network Access
C. Endpoint Compliance
D. Supplicant EasvConnect

Answer: AB

Explanation:
Network Access policies as a common type of policy in FortiNAC, used to dynamically provision access to connecting endpoints. While Authentication is typically a policy type in network access control systems like FortiNAC

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
Which group type can have members added directly from the FortiNAC Control Manager?

A. Administrator
B. Device
C. Port
D. Host

Answer: B

Explanation:
The study guide explains that there are six different types of groups in FortiNAC, including device, host, IP phone, port, user, and administrator groups. Groups created by administrative users or imported as a result of an LDAP integration can be used to organize elements but do not enforce any type of control or functionality directly

NEW QUESTION 4
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 5
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 6
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 7
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 8
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 9
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 10
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 10
Where do you look to determine which network access policy, if any is being applied to a particular host?

A. The Policy Details view for the host
B. The Connections view
C. The Port Properties view of the hosts port
D. The Policy Logs view

Answer: A

Explanation:
To determine which network access policy is applied to a particular host, you should look at the Policy Details window. This window provides information about the types of policies applied (such as Network Access, Authentication, Supplicant, etc.), including the profile name, policy name, configuration name, and any settings that make up the configuration.
FortiNAC p 382: "Under Network Access Settings - Policy Name - Name of the Network Access Policy that currently applies to the host."

NEW QUESTION 13
Where are logical network values defined?

A. In the model configuration view of each infrastructure device
B. In the port properties view of each port
C. On the profiled devices view
D. In the security and access field of each host record

Answer: A

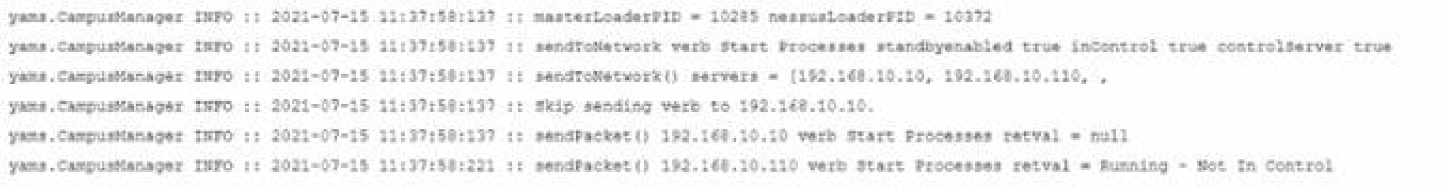
Explanation:
In FortiNAC, logical networks are an integral part of device management and network segmentation. These logical networks are defined and appear within the model configuration of each infrastructure device that is modeled in the topology tree. The configuration allows for the assignment of unique names and, optionally, descriptions to each logical network, thereby clarifying their purpose or use within the network infrastructure.
References: FortiNAC 7.2 Study Guide, Logical Networks Security Fabric and Firewall Tags section.

NEW QUESTION 14
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 19
View the output.



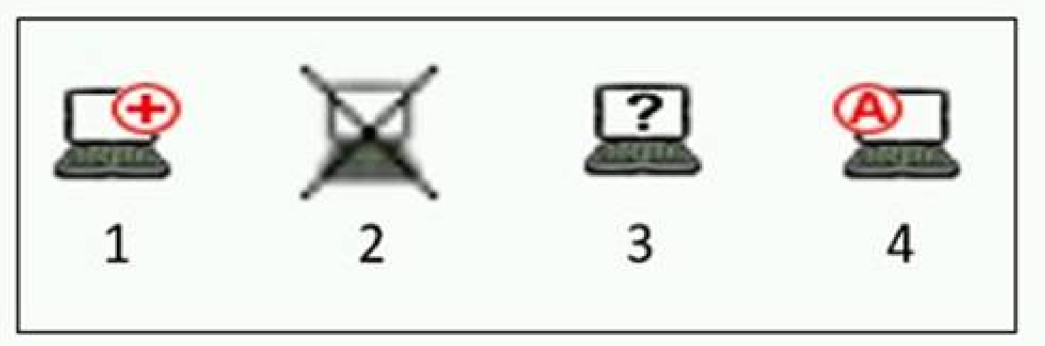
```
yams.CampusManager INFO :: 2021-07-15 11:37:58:137 :: masterLoaderPID = 10285 nessusLoaderPID = 10372
yams.CampusManager INFO :: 2021-07-15 11:37:58:137 :: sendToNetwork verb Start Processes standbyenabled true inControl true controlServer true
yams.CampusManager INFO :: 2021-07-15 11:37:58:137 :: sendToNetwork() servers = [192.168.10.10, 192.168.10.110, ,
yams.CampusManager INFO :: 2021-07-15 11:37:58:137 :: Skip sending verb to 192.168.10.10.
yams.CampusManager INFO :: 2021-07-15 11:37:58:137 :: sendPacket() 192.168.10.10 verb Start Processes retval = null
yams.CampusManager INFO :: 2021-07-15 11:37:58:221 :: sendPacket() 192.168.10.110 verb Start Processes retval = Running - Not In Control
```

Examine the communication between a primary FortiNAC (192.168.10.10) and a secondary FortiNAC (192.166.10.110) configured as an HA pair What is the current state of the FortiNAC HA pair?

A. The primary server Is running and in control.
B. The database replication failed.
C. The secondary server is running and in control.
D. Failover from the primary server to the secondary server is in progress.

Answer: A

NEW QUESTION 24
Refer to the exhibit, and then answer the question below.



Which host is rogue?

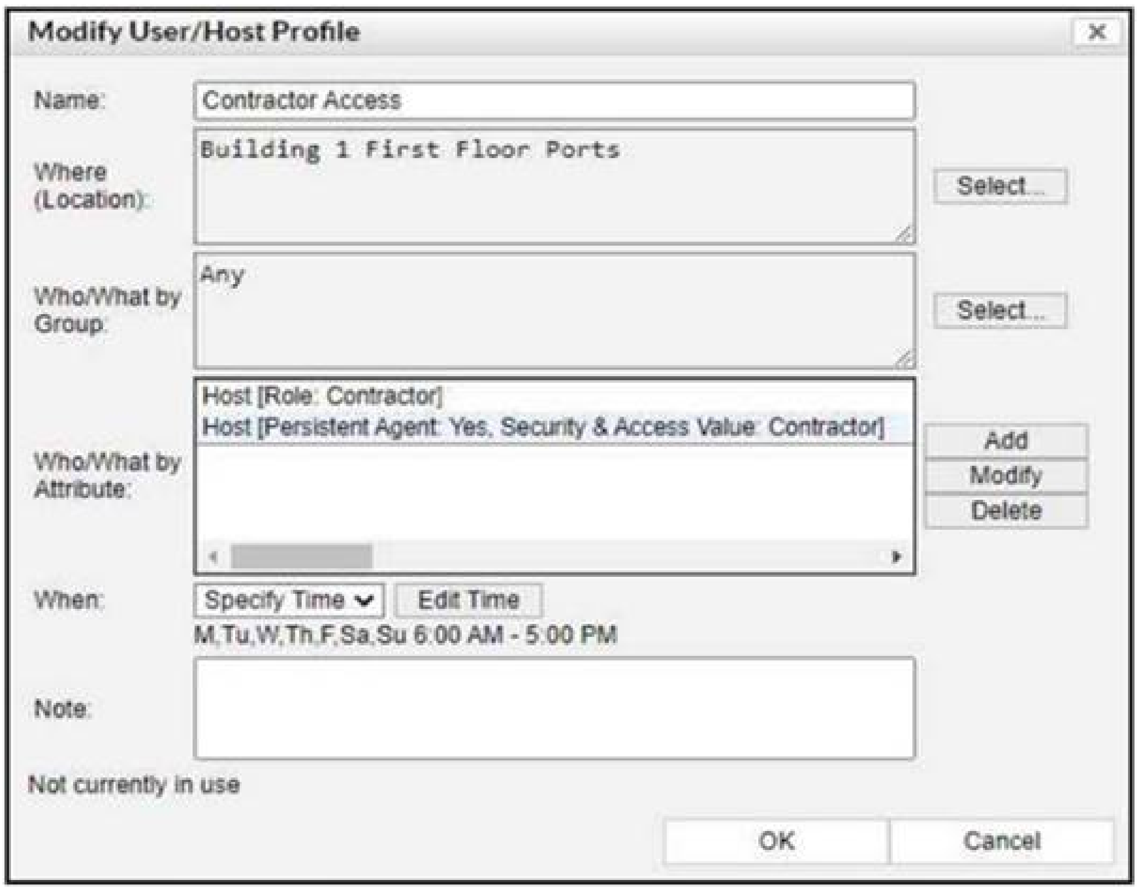
A. 1
B. 3
C. 2
D. 4

Answer: B

Explanation:
Reference: https://docs.fortinet.com/document/fortinac/8.6.0/administration-guide/283146/evaluating-rogue-hosts

NEW QUESTION 26

Refer to the exhibit.



Modify User/Host Profile

Name: Contractor Access

Where (Location): Building 1 First Floor Ports

Who/What by Group: Any

Who/What by Attribute:
Host [Role: Contractor]
Host [Persistent Agent: Yes, Security & Access Value: Contractor]

When: Specify Time
M,Tu,W,Th,F,Sa,Su 6:00 AM - 5:00 PM

Note:

Not currently in use

If a host is connected to a port in the Building 1 First Floor Ports group, what must also be true to match this user/host profile?

A. The host must have a role value of contractor, an installed persistent agent or a security access value of contractor, and be connected between 6 AM and 5 PM.
B. The host must have a role value of contractor or an installed persistent agent, a security access value of contractor, and be connected between 9 AM and 5 PM.
C. The host must have a role value of contractor or an installed persistent agent and a security access value of contractor, and be connected between 6 AM and 5 PM.
D. The host must have a role value of contractor or an installed persistent agent or a security access value of contractor, and be connected between 6 AM and 5 PM.

Answer: D

Explanation:
Looking at the provided exhibit which shows the Modify User/Host Profile window, the following must be true for a host to match the user/host profile:
? The host must be connected to a port within the "Building 1 First Floor Ports" group.
? The host must fulfill at least one of the following attributes:
? The host must be connected between the specified times of 6 AM and 5 PM on any day of the week.
The profile specifies that the host can match the profile by having any one of the listed attributes (Role as Contractor, Persistent Agent installed with specific security & access value), and the time condition must also be met. Therefore, the correct answer is D, which includes "or" conditions for the role value and persistent agent and specifies the correct time frame.

NEW QUESTION 29

......