NSE6_FNC-8.5.VCEplus.premium.exam.30q

Number: NSE6_FNC-8.5
Passing Score: 800
Time Limit: 120 min
File Version: 1.0

NSE6_FNC-8.5

Fortinet NSE 6 – FortiNAC 8.5

Version 1.0

Exam A

QUESTION 1
Which three communication methods are used by the FortiNAC to gather information from, and control, infrastructure devices? (Choose three.)

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

Correct Answer: ABC
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Set up SNMP communication with FortiNAC
RADIUS Server that is used by FortiNAC to communicate
FortiNAC can be configured via CLI to use HTTP or HTTPS for OS updates instead of FTP.

Reference: https://docs.fortinet.com/document/fortinac/8.3.0/administration-guide/28966/snmp https://docs.fortinet.com/document/fortinac/8.8.0/administration-guide/938271/configure-radius-settings https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/e7ebbdaa-cabf-11ea-8b7d-00505692583a/FortiNAC_Deployment_Guide.pdf

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

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

Correct Answer: BCD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 3 How should you configure MAC notification traps on a
supported switch?

A. Configure them only on ports set as 802.1q trunks
B. Configure them on all ports except uplink ports
C. Configure them on all ports on the switch
D. Configure them only after you configure linkup and linkdown traps

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Configure SNMP MAC Notification traps on all access ports (do not include uplinks).

Reference: https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/be7fcde9-9685-11e9-81a4-00505692583a/Configuring_Traps_for_MAC_Notification.pdf **QUESTION 4** Which connecting endpoints are evaluated against all enabled device profiling rules?

A. Known trusted devices each time they change location
B. Rogues devices, each time they connect
C. Rogues devices, only when they connect for the first time
D. All hosts, each time they connect

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
FortiNAC process to classify rogue devices and create an organized inventory of known trusted registered devices.

Reference: https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/9529d49c-892c-11e9-81a4-00505692583a/FortiNAC_Device_Profiler_Configuration.pdf

QUESTION 5 What agent is required in order to detect an added USB drive?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Expand the Persistent Agent folder. Select USB Detection from the tree.

Reference: https://docs.fortinet.com/document/fortinac/8.5.2/administration-guide/814147/usb-detection

QUESTION 6 Which two of the following are required for endpoint compliance monitors? (Choose two.)

A. Logged on user
B. Security rule
C. Persistent agent
D. Custom scan

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:
Explanation:
DirectDefense's analysis of FireEye Endpoint attests that the products help meet the HIPAA Security Rule. In the menu on the left click the + sign next to Endpoint Compliance to open it.

Reference: https://www.fireeye.com/content/dam/fireeye-www/products/pdfs/cg-pci-and-hipaa-compliances.pdf https://docs.fortinet.com/document/fortinac/8.5.2/administration-guide/92047/add-or-modify-a-scan

QUESTION 7 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 added to the Forced Registration group.

B. The port is disabled.
C. The port is switched into the Dead-End VLAN.

D. The port becomes a threshold uplink.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 8 In a wireless integration, how does FortiNAC obtain connecting MAC address information?

A. Link traps
B. End station traffic monitoring
C. MAC notification traps
D. RADIUS

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Intelligent Access Points (IAPs) and controllers support two methods of RADIUS based authentication: RADIUS MAC authentication and 802.1x authentication.

Reference: https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/9019f7f8-200d-11e9-b6f6-f8bc1258b856/FortiNAC_Wireless_Integration_Overview.pdf

QUESTION 9 Which system group will force at-risk hosts into the quarantine network, based on point of connection?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A remediation plan is established, including a forensic analysis and a reload of the system. Also, users are forced to change their passwords as the system held local user accounts. Reference:

https://oit.rice.edu/quarantining-process-used-it-staff-members-introduction

QUESTION 10
During the on-boarding process through the captive portal, why would a host that successfully registered remain stuck in the Registration VLAN? (Choose two.)

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

Correct Answer: AD
Section: (none)
Explanation
Explanation/Reference:
Explanation:

Scenario 4: NAT detection disabled, using endpoint compliance policy and agent.

Reference: https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/868f1267-7299-11e9-81a4-00505692583a/fortinac-admin-operation-85.pdf

QUESTION 11 In which view would you find who made modifications to a Group?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
It’s important to audit Group Policy changes in order to determine the details of changes made to Group Policies by delegated users. Reference:

https://www.lepide.com/how-to/audit-chnages-made-to-group-policy-objects.html

QUESTION 12 Which agent is used only as part of a login script?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
If the logon script runs the logon application in persistent mode, configure your Active Directory server not to run scripts synchronously.

Reference: https://www.websense.com/content/support/library/deployctr/v76/init_setup_creating_and_running_logon_agent_script_deployment_tasks.aspx

QUESTION 13 Which two agents can validate endpoint compliance transparently to the end user? (Choose two.)

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

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Mobile agents use the network transparently.

Reference:

https://docs.fortinet.com/document/fortinac/8.3.0/administration-guide/377110/persistent-agent-certificate-validation https://docs.fortinet.com/document/fortinac/8.3.0/administration-guide/377110/persistent-agent-certificate-validation

QUESTION 14 Which command line shell and scripting language does FortiNAC use for WinRM?

A. Powershell
B. Bash
C. Linux
D. DOS

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Open Windows PowerShell or a command prompt. Run the following command to determine if you already have WinRM over HTTPS configured.

Reference: https://docs.fortinet.com/document/fortinac/8.7.0/administration-guide/246310/winrm-device-profile-requirements-and-setup

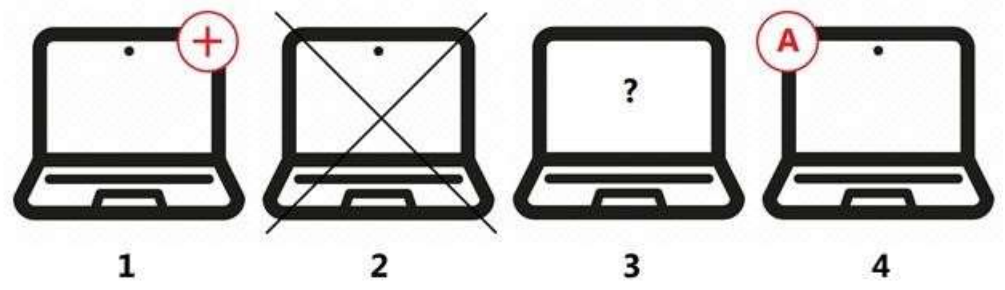
QUESTION 15 Where are logical network values defined?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.sciencedirect.com/topics/computer-science/logical-network

QUESTION 16
Refer to the exhibit, and then answer the question below.



Which host is rogue?

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

Correct Answer: C
Section: (none)
Explanation

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

QUESTION 17 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

Correct Answer: ACE
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.fortinet.com/document/fortinac/8.3.0/administration-guide/15797/user-host-profiles

QUESTION 18 What would happen if a port was placed in both the Forced Registration and the Forced Remediation port groups?

A. Both enforcement groups cannot contain the same port.
B. Only at-risk hosts would be impacted.
C. Only rogue hosts would be impacted.
D. Both types of enforcement would be applied.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.fortinet.com/document/fortinac/8.3.0/administration-guide/837785/system-groups

QUESTION 19 What causes a host's state to
change to "at risk"?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
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

QUESTION 20
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 network access policy.
B. The host is provisioned based on the default access defined by the point of connection.
C. The host is isolated.

D. The host is administratively disabled.
Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.fortinet.com/document/fortinac/8.6.0/administration-guide/49701/policy-assignment

QUESTION 21 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. MDM integration
C. Portal page on-boarding options
D. Application layer traffic inspection

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:
Reference: https://developer.apple.com/business/documentation/MDM-Protocol-Reference.pdf
https://docs.oracle.com/en/middleware/idm/identity-governance/12.2.1.3/omusg/managing-application-onboarding.html#GUID-4D0D5B18-A6F5-4231-852E-DB0D95AAE2D1

QUESTION 22 Which three of the following are components of a security rule?
(Choose three.)

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

Correct Answer: ABE
Section: (none)
Explanation

Explanation/Reference:
Reference: https://patents.google.com/patent/US20150200969A1/en

QUESTION 23 What capability do logical
networks provide?

A. VLAN-based inventory reporting
B. Interactive topology view diagrams
C. Application of different access values from a single access policy
D. Autopopulation of device groups based on point of connection

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
NTM also includes reporting utilities such as network and inventory reports. You can generate reports for subnets, switch ports, and VLANs.

Reference: https://logicalread.com/network-diagram/#.YBk9ZOgzbIU

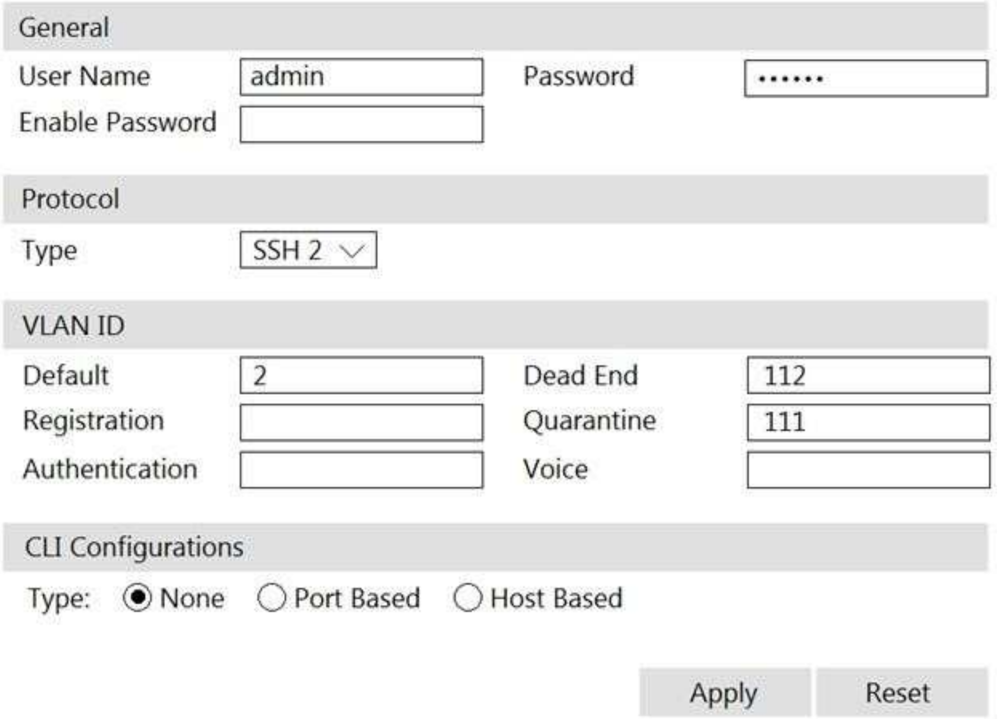
QUESTION 24
Which agent can receive and display messages from FortiNAC to the end user?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.fortinet.com/document/fortinac/8.7.0/administration-guide/594507/agent-packages

QUESTION 25
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 will occur?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The ability to limit the number of workstations that can connect to specific ports on the switch is managed with Port Security. If these limits are breached, or access from unknown workstations is attempted, the port can do any or all of the following: drop the untrusted data, notify the network administrator, or disable the port.

Reference: https://www.alliedtelesis.com/sites/default/files/documents/solutions-guides/lan_protection_solution_reva.pdf

QUESTION 26
Where do you look to determine what network access policy, if any, is being applied to a particular host?

A. The network access policy configuration
B. The **Port Properties** view of the hosts port
C. The **Policy Logs** view
D. The **Policy Details** view for the host

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.microsoft.com/en-us/windows-server/networking/technologies/nps/nps-np-overview

QUESTION 27 How are logical networks
assigned to endpoints?

A. Through Layer 3 polling configurations
B. Through network access policies
C. Through FortiGate IPv4 policies
D. Through device profiling rules

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/9819/viewing-and-controlling-network-risks-via-topology-view

QUESTION 28 In an isolation VLAN, which three services does FortiNAC supply?
(Choose three.)

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

Correct Answer: ADE
Section: (none)
Explanation

Explanation/Reference:
Reference: https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/8bec453a-b242-11e9-a989-00505692583a/AdminGuide-860-PDF.pdf

QUESTION 29 Where do you look to determine when and why the FortiNAC made an automated network
access change?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

Reference: https://docs.fortinet.com/document/fortigate/6.2.3/cookbook/536166/viewing-event-logs

QUESTION 30

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference: