

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 EasyConnect

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

When configuring isolation networks in the configuration wizard, why does a Layer 3 network type allow for more than one DHCP scope for each isolation network type?

- A. There can be more than one isolation network of each type.
- B. Any scopes beyond the first scope are used if the Initial scope runs out of IP addresses.
- C. Configuring more than one DHCP scope allows for DHCP server redundancy.
- D. The Layer 3 network type allows for one scope for each possible host status.

Answer: A

NEW QUESTION 3

View the command and output shown in the exhibit.

```
>Client -mac *C4:4E:12
Found 1 matches for client
Intel Corporation
  DBID = 606
  MAC = 00:03:47:C4:4E:12
  IP = null
  Medium = null
  Description = null
  Status = Connected
  State = Initial
  Type = DynamicClient
  Ident = null
  UserID = null
  ParentID = 576
  Role = NAC-Default
  Security Access Value = null
  OS = null
  Location = Building 1 Switch SuperStack II Switch 3900-2
  Client Not Authenticated = false
  Client needs to authenticate = false
  Logged On = false
  At-Risk = false
  Host role = NAC-Default
  VpnClient = false
```

What is the current state of this host?

- A. Rogue
- B. Registered
- C. Not authenticated
- D. At-Risk

Answer: A

Explanation:

The exhibit's command and output detail various attributes for a specific host, including the MAC address, connection status, and various other parameters. The status "Connected" and state "Initial" indicate that the host has been detected on the network but has not yet completed any authentication process. The lines "Client Not Authenticated = true" and "Client needs to authenticate = false" suggest that the host has not yet been authenticated. Therefore, the current state of the host is "Not authenticated," since there is a clear indication that the authentication process has not been completed for this host.

NEW QUESTION 4

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 5

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 6

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 7

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 8

Which connecting endpoints are evaluated against all enabled device profiling rules?

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

Answer: D

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

Based on FortiNAC's approach to device profiling and rule evaluation, rogue devices are evaluated against enabled device profiling rules each time they connect. This consistent evaluation ensures that rogue devices are properly classified and handled according to the latest network policies each time they attempt to access the network.

References

FortiNAC documentation on device profiling and rule evaluation.

NEW QUESTION 9

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

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

Answer: D

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>

Admin Guide on p. 362, "Matches if the device successfully responds to a WinRM client session request. User name and password credentials are required. If there are multiple credentials, each set of credentials will be attempted to find a potential match. The commands are used to automate interaction with the device. Each command is run via Powershell."

NEW QUESTION 10

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 10

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

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

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 12

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 15

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 19

Which three capabilities does FortiNAC Control Manager provide? (Choose three.)

- A. Global visibility
- B. Global authentication security policies
- C. Global infrastructure device inventory
- D. Global version control
- E. Pooled licenses

Answer: ADE

NEW QUESTION 21

Refer to the exhibit.

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

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

Answer: C

NEW QUESTION 24

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 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 31

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

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

Answer: B

Explanation:

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

NEW QUESTION 36

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

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

Answer: AD

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/7.2.2/administration-guide/92047/add-or-modify-a-scan>

NEW QUESTION 38

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 40

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 of 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 43

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 45

When FortiNAC passes a firewall tag to FortiGate, what determines the value that is passed?

- A. Security rule
- B. Device profiling rule
- C. RADIUS group attribute
- D. Logical network

Answer: B

NEW QUESTION 49

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

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

Answer: A

Explanation:

Expand the Persistent Agent folder. Select USB Detection from the tree.

Reference: <https://docs.fortinet.com/document/fortinac/7.2.2/administration-guide/814147/usb-detection>

* 1. Click System > Settings.

* 2. Expand the Persistent Agent folder.

* 3. Select USB Detection from the tree.

* 4. Click Add or select an existing USB drive and click Modify.

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

.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questions 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](#)