

Fortinet

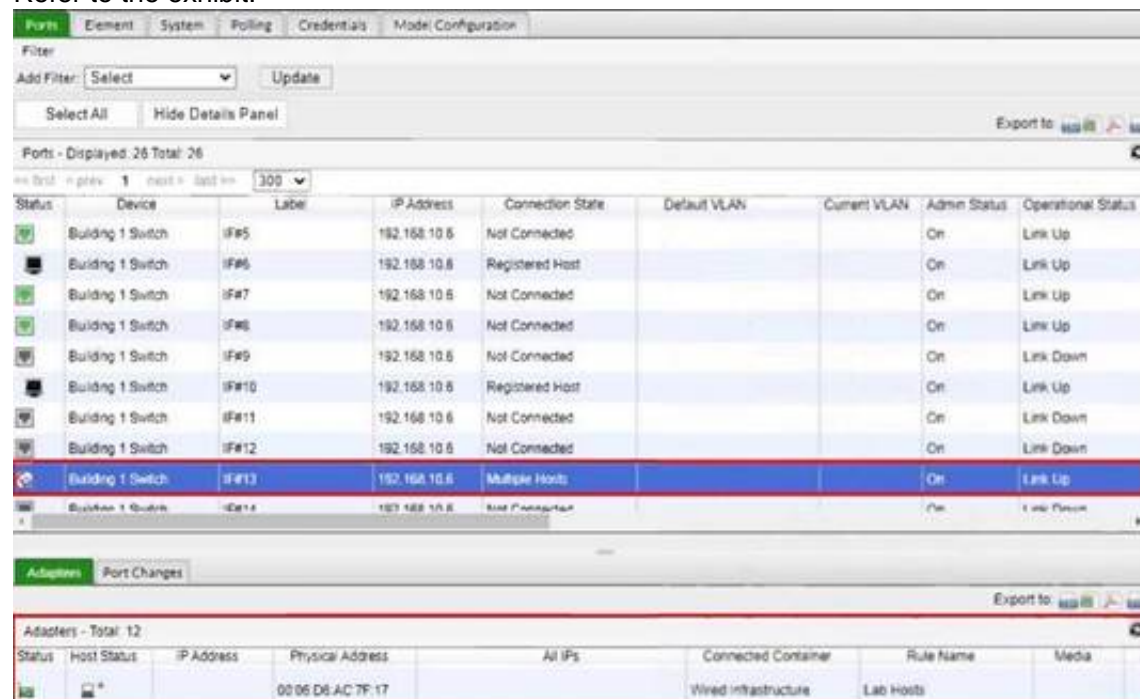
Exam Questions NSE6_FNC-7.2

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

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

Which two things must be done to allow FortiNAC to process incoming syslog messages from an unknown vendor? (Choose two.)

- A. A security event parser must be created for the device.
- B. The device sending the messages must be modeled in the Network Inventory view.
- C. The device must be added as a patch management server.
- D. The device must be added as a log receiver.

Answer: AB

Explanation:

To allow FortiNAC to process incoming syslog messages from an unknown vendor, two steps must be taken:

? Creation of a customized event parser: This enables FortiNAC to parse and integrate syslog messages from any vendor or device, as long as the messages are in CSV, CEF, or Tag/Value format.

? Modeling the device in the Topology view: Any device that sends syslog messages to FortiNAC must be modeled in this view. FortiNAC will not process syslog or trap messages unless the source address belongs to a device modeled in the topology.

References

? FortiNAC 7.2 Study Guide, pages 428 and 399

NEW QUESTION 3

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 4

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 5

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 6

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 7

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 8

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 9

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 10

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 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 15

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 20

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 21

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 23

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 26

Which two device classification options can register a device automatically and transparently to the end user? (Choose two.)

- A. Dissolvable agent
- B. Dot1xAuto Registration
- C. Device importing
- D. MDM integration
- E. Captive portal

Answer: BD

Explanation:

The FortiNAC 7.2 Study Guide does not explicitly mention Dot1x Auto Registration and MDM integration as the specific device classification options for automatic and transparent registration to the end user. However, based on the general functioning of FortiNAC, Dot1x Auto Registration and MDM integration are typically used for such purposes. The guide discusses automatic device registration in the context of profiling rules

NEW QUESTION 28

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 32

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 34

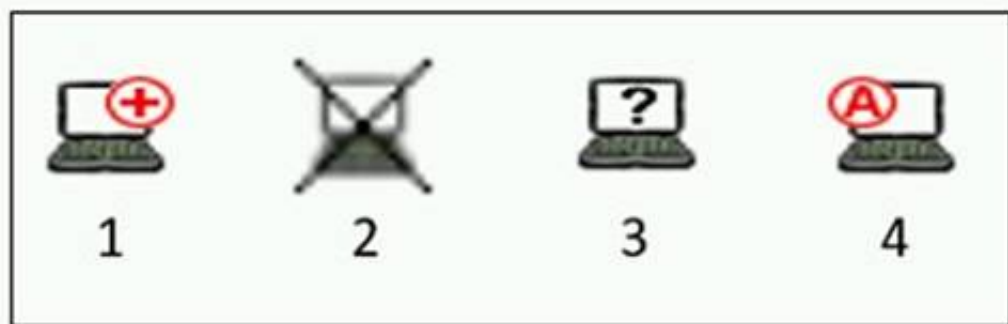
During the on-boarding process through the captive portal, what are two reasons why a host that successfully registered would remain stuck in the Registration VLAN? (Choose two.)

- 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 39

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 43

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 46

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

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

Answer: D

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>

NEW QUESTION 51

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 53

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 55

.....

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](#)