# Prepare Smart for Success Free Fortinet NSE6_FNC_AD-7.6 Exam Questions and Answers

Ready to pass faster? Grab free and updated Fortinet NSE 6 - FortiNAC-F 7.6 Administrator exam PDF questions now. Get authentic NSE6_FNC_AD-7.6 dumps packed with verified answers and secure your certification success with PrepBolt NSE6_FNC_AD-7.6 exam pdf questions and answers.

Thank you for Downloading NSE6_FNC_AD-7.6 exam PDF Demo

https://prepbolt.com/NSE6_FNC_AD-7.6.html

# Question 1

Question Type: MultipleChoice

An administrator is configuring FortiNAC-F 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 clients not yet authorized by FortiNAC-F? (Choose one answer)

## Options:

A- To allow access to only the production DNS server
B- To allow access to only the production DNS server
C- To allow access to only the FortiNAC-F VPN interface
D- To allow access to only the FortiGate VPN interface

## Answer:

C

## Explanation:

The firewall policy for an unauthorized VPN host is an isolation policy. When a remote endpoint first establishes its VPN tunnel, FortiGate assigns the client an IP address plus two DNS servers: the production DNS server as primary and the FortiNAC-F Port2 VPN-context address as secondary. Until FortiNAC-F validates the endpoint, FortiGate firewall policies restrict the client's traffic so that it can communicate only with the FortiNAC-F Port2 VPN interface.

This restriction deliberately prevents access to the primary production DNS server. Consequently, DNS resolution against the primary server fails and the endpoint falls back to the secondary DNS server---FortiNAC-F. FortiNAC-F then resolves the request toward its VPN isolation interface and presents the VPN captive portal. The user can subsequently run or download the required FortiNAC-F agent, allowing FortiNAC-F to perform identification and endpoint-compliance validation.

After successful authorization, FortiNAC-F sends the appropriate group/tag information to FortiGate, causing the host to match a different firewall policy that permits the required production resources and blocks the isolation interface.

Study Guide Reference: Advanced Features FortiGate VPN Integration VPN Host Isolation and Firewall Policies, pp. 346--354.

# Question 2

Question Type: MultipleChoice

As part of a company policy, all end stations must be scanned for compliance each day. The security administrators want to satisfy this requirement without any necessary interaction from the end user. Which two agents can provide that functionality? (Choose two.)

## Options:

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

## Answer:

B, C

## Explanation:

The correct answers are B and C. The persistent agent is the strongest fit because it is installed and stays resident on the endpoint. The study guide states that after deployment, the persistent agent communicates back to FortiNAC-F every 15 minutes and performs scheduled scans in the background, transparent to the end user. That directly satisfies the requirement for recurring compliance scans without user involvement.

The passive agent can also scan Windows domain end stations without end-user interaction. The guide states that the passive agent is deployed through login/logoff scripts and administrative templates, and that passive agent registration can register and scan hosts associated with LDAP or Active Directory users. If enabled, the passive agent scans the host to verify compliance with the appropriate endpoint policy.

Option A is wrong because the dissolvable agent is a run-once agent that requires manual end-user interaction in the captive portal, then removes itself after reporting results. Option D is not the best answer for this requirement because the mobile agent is specifically for Android onboarding and is manually installed; it is not the general solution for daily compliance scanning of all end stations.

# Question 3

Question Type: MultipleChoice

Refer to the output below.

```
INFO yams.CampusManager - masterLoaderPID = 2754377 nessusLoaderPID = 2754516
INFO yams.CampusManager - sendToNetwork verb Start Processes standbyenabled true inControl true controlServer true
INFO yams.CampusManager - Skip sending verb to 192.168.10.10 because local ip is 192.168.10.10
INFO yams.CampusManager - sendPacket() 192.168.10.10 verb Start Processes retval = null
[grpc-default-executor-3560] INFO yams.CampusManager - isCampusManagerCheckOK system true, in control true, final true
INFO yams.CampusManager - sendPacket() 192.168.10.110 verb Start Processes retval = Running - Not In Control
```

Examine the communication between a primary FortiNAC-F (192.168.10.10) and a secondary FortINAC-F (192.168.10.110) configured as a 1+1 HA pair. What is the current state of the FortiNAC-F HA pair?

## Options:

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

## Answer:

D

## Explanation:

The correct answer is D. The log output shows the local IP address as 192.168.10.10, which the question identifies as the primary FortiNAC-F server. In the same output, FortiNAC-F reports inControl true and controlServer true, which means the local primary server is currently the control server. The line showing communication to 192.168.10.110 returns Running - Not In Control, confirming that the secondary server is alive but is not the active controlling node.

This matches FortiNAC-F 1+1 HA behavior. The study guide describes a 1+1 HA pair as an active-passive deployment where one FortiNAC-F device is designated primary and the other secondary. Database and configuration synchronization keep the devices aligned, but only one server is in control at a time. If the primary fails, the secondary assumes control automatically; otherwise, the primary remains the active control server.

Option A is wrong because the secondary explicitly reports Not In Control. Option B is wrong because the output does not show database replication failure. Option C is wrong because failover is not in progress; the output shows a stable state where the primary is in control and the secondary is running as the passive node.

# Question 4

Question Type: MultipleChoice

An administrator wants FortiNAC-F to pass firewall tags to FortiGate to leverage dynamic address groups used in firewall policies. On FortiNAC-F, what determines the values that are passed?

## Options:

A- Model configuration
B- Device profiling rule
C- Security rule
D- RADIUS group attribute

## Answer:

A

## Explanation:

The correct answer is A. FortiNAC-F passes firewall tags to FortiGate through Security Fabric integration so FortiGate can use those values as dynamic address groups in firewall policies. The study guide explains that firewall tags are administrator-defined string values and that FortiNAC-F dynamically assigns them based on a security policy or logical network. More specifically for network access enforcement, it states that the network access configuration defines the logical network, and the logical network defines the firewall tag through the device model configuration.

This is the same mechanism used in VPN and Fabric workflows: the FortiGate device model contains the mappings of logical networks to the actual tags or groups that FortiNAC-F sends to FortiGate. The guide states that FortiNAC-F network access policies and logical networks determine the group or tag information, while the FortiGate model configuration contains the mappings used for the values sent.

Option B is not the best answer because a device profiling rule can classify a device and may cause it to match a policy, but it does not directly define the FortiGate tag value sent for policy enforcement. Option C can apply firewall tags in security automation scenarios, but the standard FortiGate dynamic address group mapping is defined in model configuration. Option D is unrelated; RADIUS attributes are used in RADIUS access responses, not FortiGate Fabric tag propagation.

# Question 5

Question Type: MultipleChoice

An administrator wants to continually monitor endpoints for the existence of a specific registry key and the status of a required security service. Which two requirements must be in place for the administrator to use FortiNAC-F compliance monitors? (Choose two.)

## Options:

A- MDM integration
B- Persistent agent
C- Custom scan
D- Remediation admin scan

## Answer:

B, C

## Explanation:

The correct answers are B and C. FortiNAC-F must have a persistent agent on the endpoint if the goal is continual or background endpoint monitoring. The study guide states that the persistent agent is an install-and-stay resident agent and that, after deployment, it communicates back to FortiNAC-F every 15 minutes. It also performs scheduled scans in the background without normal user interaction unless the scan fails. That is the agent model required for continuous compliance monitoring, not a one-time captive portal scan.

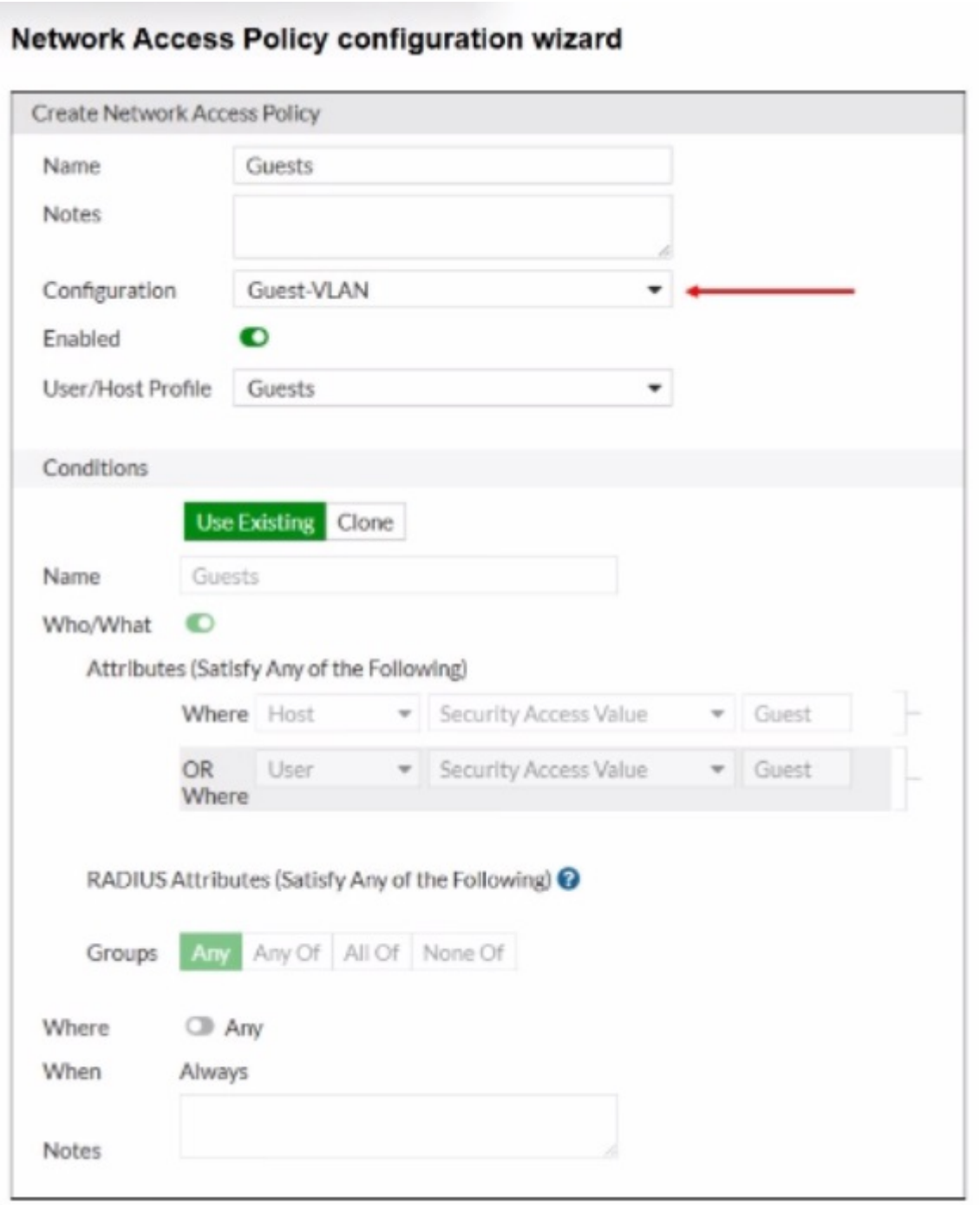
A custom scan is also required because the administrator wants to check very specific endpoint conditions: a registry key and a security service. The FortiNAC-F study guide lists Windows custom scan types including Registry Keys and Service, which directly match the two conditions in the question.

Option A is wrong because MDM integration is used to synchronize mobile device data, retrieve MDM-known hosts, receive MDM host updates, and apply policies based on MDM attributes; it is not the required mechanism for checking Windows registry keys or Windows service status. Option D is wrong because a remediation admin scan is not what defines the compliance check itself. The compliance logic must be created as a custom scan, and continuous monitoring requires the persistent agent.

# Question 6

Question Type: MultipleChoice

Refer to the exhibit.




When configuring guest access using a network access policy, where would an administrator configure the Guest-VLAN value?

## Options:

A- In the Model configuration
B- In the Guest template
C- In the User/Host profile
D- in the Guest portal configuration

## Answer:

A

## Explanation:

The correct answer is A. In the exhibit, Guest-VLAN is selected as the network access policy Configuration. That policy configuration points to a logical network, but the actual access value for that logical network is not defined inside the guest template, user/host profile, or guest portal. The FortiNAC-F study guide explains that logical networks translate policy-level names into device-specific access values, and those values are configured in the Model Configuration of the infrastructure device. It specifically states that device-specific configurations for infrastructure devices associate the configuration values with the devices, and that after a logical network is created, it appears within the model configuration of each modeled infrastructure device.

So, Guest-VLAN is the logical network selected by the network access policy, while the actual VLAN ID, VLAN name, SSID role, controller group, or vendor-specific access value is configured under the relevant switch, AP, controller, or firewall Model Configuration. Option B is wrong because the guest template defines guest account properties such as role, security/access value, password settings, account duration, and login availability. Option C is wrong because the user/host profile defines the matching condition for guests. Option D is wrong because the guest portal controls onboarding or login behavior, not the infrastructure access value used to provision the endpoint.

# Question 7

Question Type: MultipleChoice

When creating a device profiling rule, what is an advantage of modeling the endpoint as a device in the inventory view?

## Options:

A- The device will have historic connection logs.
B- The devices can have scheduled connection status polling.
C- The devices will have connection logs.
D- The devices can be associated with a logged on user.

## Answer:

B

## Explanation:

The correct answer is B. When a device profiling rule classifies an endpoint, the Register as setting can place the device in the host view, the topology/inventory view, or both. The study guide explains that if the profiled endpoint is registered into the topology view, the administrator must select a topology

container.

The advantage of modeling the endpoint as a device in the inventory view is that it can be treated as a pingable device, where FortiNAC-F can use Contact Status settings. The guide explains that a modeled pingable device has contact status controls that allow polling to be enabled or disabled, the polling interval to be set, and the last successful and last attempted poll to be displayed.

Option A and option C are not the best answers because connection logs are associated with host connection tracking, not the key advantage of placing a profiled endpoint into inventory as a modeled device. Option D is wrong because user association applies more naturally to hosts or BYOD ownership workflows; it is not the main benefit of inventory modeling. The tested benefit is scheduled reachability monitoring through contact status polling.

# Thank You for trying NSE6_FNC_AD-7.6 PDF Demo

## To try our NSE6_FNC_AD-7.6 practice exam software visit link below

https://prepbolt.com/NSE6_FNC_AD-7.6.html

# Start Your NSE6_FNC_AD-7.6 Preparation

Use Coupon “SAVE50” for extra 50% discount on the purchase of Practice Test Software. Test your NSE6_FNC_AD-7.6 preparation with actual exam questions.