DUMPSBOSS.

Fortinet NSE 6 - FortiNAC-F 7.6 Administrator

Fortinet NSE6_FNC_AD-7.6

Version Demo

Total Demo Questions: 7

Total Premium Questions: 75

Buy Premium PDF

https://dumpsboss.co

support@dumpsboss.co

support@dumpsboss.co
dumpsboss.co

QUESTION NO: 1

An administrator wants to build a security rule that will quarantine contractors who attempt to access specific websites.

In addition to a user host profile, which Iwo components must the administrator configure to create the security rule? (Choose two.)

A. Methods

B. Action

C. Endpoint compliance policy

D. Trigger

E. Security String

ANSWER: B D

Explanation:

Action and **Trigger** are the required components in addition to the user host profile. A FortiNAC-F security rule associates a profile of applicable users or hosts with an event definition and the response that FortiNAC-F must perform. The trigger supplies the event criteria that identify the behavior of interest. For this use case, it can match security-event information received from an integrated device, such as data identifying that a contractor attempted to reach one of the restricted websites. This provides the condition that causes FortiNAC-F to evaluate the rule.

The action defines the automated enforcement response after the trigger matches for a host or user in the selected profile. To meet the stated objective, the action is configured to quarantine the matching endpoint, allowing FortiNAC-F to apply the organization's configured quarantine handling and restrict that endpoint's network access. Together, the user host profile scopes the policy to contractors, the trigger detects the prohibited web-access event, and the action executes quarantine. This event-to-response design is the basis of Security Incidents rule automation in FortiNAC-F. Fortinet's FortiNAC-F documentation is available through the FortiNAC-F 7.6 documentation portal; Fortinet also provides product documentation and release-specific resources through its documentation library.

QUESTION NO: 2

In which three ways would deploying a FortiNAC-F Manager into a large environment consisting of several FortiNAC-F CAs simplify management? (Choose three.)

A. Global infrastructure device inventory

B. Global version control

C. Global authentication security policies

D. Pooled licenses

E. Global visibility

ANSWER: B D E

Explanation:

FortiNAC-F Manager is intended to centralize operational functions for distributed FortiNAC-F deployments that contain multiple Control and Application servers. **Global version control** simplifies lifecycle management by enabling the administrator to manage FortiNAC-F software versions centrally and coordinate updates for managed CAs. This promotes a consistent software baseline across sites and reduces the administrative effort of handling each appliance independently.

Pooled licenses simplifies capacity administration because licensing is maintained centrally on the Manager and allocated to managed CAs according to their needs. Administrators can therefore manage entitlement consumption at the overall deployment level rather than treating capacity at every CA as a separate licensing task.

Global visibility provides a consolidated view of information from managed CAs. This is particularly useful in a large environment because administrators can monitor and locate relevant endpoint, adapter, and event information across the deployment from the central management system. Together, centralized software management, license pooling, and cross-system visibility are the core management benefits of the FortiNAC-F Manager architecture. Fortinet documentation for FortiNAC-F is available through the FortiNAC-F documentation portal, and Fortinet provides additional product architecture and centralized-management context on the FortiNAC product page.

QUESTION NO: 3

While deploying FortiNAC-F devices in a 1+1 HA configuration, the administrator has chosen to use the shared IP address option.

Which condition must be met for this type of deployment?

A. The isolation network type is layer 3.

B. There is a direct cable link between FortiNAC-F devices.

C. The primary and secondary administrative interfaces are on the same subnet.

D. The isolation network type is Layer 2.

ANSWER: C

Explanation:

The primary and secondary administrative interfaces are on the same subnet. This is a mandatory requirement when a FortiNAC-F 1+1 high-availability deployment uses a shared IP address. The shared address is a floating management address: it is held by the appliance currently operating as the active, or in-control, unit and transfers to the peer during failover or recovery. Administrators can therefore continue to reach the FortiNAC-F management interface using one consistent address instead of changing to the individual address of the surviving appliance.

For that address movement to work, both appliances' administrative interfaces must be connected to the same Layer 2 network and IP subnet. This allows the active unit to advertise ownership of the shared address on the local segment and enables hosts and the default gateway to update their ARP information after a role change. Fortinet specifically describes shared IP addressing as an L2 HA capability and instructs administrators not to use it when the primary and secondary servers are in different subnets. The shared address therefore provides a stable management endpoint while preserving HA failover behavior. See the Fortinet FortiNAC-F High Availability Guide and the FortiNAC-F Administration Guide.

QUESTION NO: 4

When preparing network infrastructure devices for visibility, what are the two main advantages of using MAC notification traps on supported devices instead of link-up and link-down traps? (Choose two.)

A. MAC notification traps include IP address information.

B. Overhead on FortiNAC-F and the infrastructure device is reduced.

C. Hosts connecting to downstream non-managed hubs are immediately learned.

D. Faster visibility updates with only a slight increase in processing.

ANSWER: B C

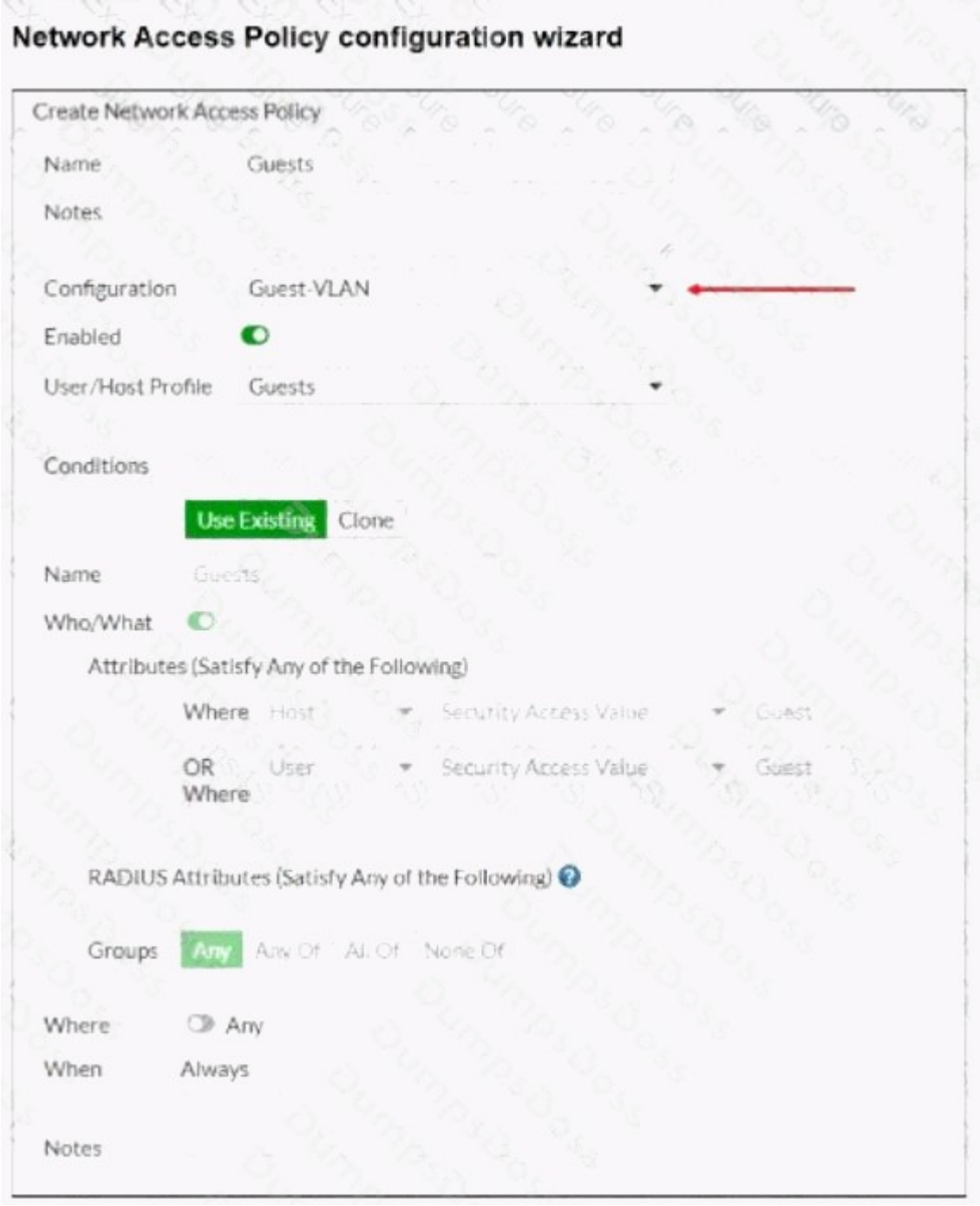
Explanation:

MAC notification traps reduce overhead because the notification supplies FortiNAC-F with the MAC-address and switch-port information associated with the learning or removal event. FortiNAC-F can therefore update its endpoint-location information directly, rather than treating a port-state notification as a trigger to query the device again to determine the current Layer 2 forwarding-table contents. This reduces follow-up management traffic and processing work for both FortiNAC-F and the infrastructure device, while also improving the timeliness of visibility data.

Hosts connecting to downstream non-managed hubs are immediately learned because MAC notification is based on MAC-address learning at the managed switch port, not solely on a physical link-state transition. A hub, IP phone, or comparable downstream device can remain connected while endpoints behind it appear or change. The managed switch learns the endpoint MAC address on its connected port and sends the MAC notification event, enabling FortiNAC-F to discover the endpoint without waiting for a separate downstream link-up event that may never be available. These capabilities make MAC notifications especially valuable where supported network devices can report MAC-table changes to FortiNAC-F. See the FortiNAC-F 7.6 Administration Guide and Fortinet's FortiNAC-F 7.6 documentation portal.

QUESTION NO: 5

Refer to the exhibit.



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

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 Guest-VLAN value is configured in the **Model configuration**. In FortiNAC, a network access policy defines the access state that FortiNAC applies when an endpoint matches the policy. The model configuration associated with that policy contains the device-specific connection and enforcement settings, including the VLAN information to assign for the relevant access state. Setting the guest VLAN there enables FortiNAC to instruct the managed network device to place qualifying guest endpoints into the intended guest network when the policy is enforced.

This placement is important because guest onboarding and portal workflows identify, register, or authenticate the guest, while the actual network segmentation outcome must be applied through the network access control enforcement configuration. The model configuration provides the switch, wireless-controller, or other supported-device context needed to map the policy result to the configured guest VLAN. Administrators should therefore ensure that the guest VLAN exists on the applicable network infrastructure and that the selected model configuration supports VLAN assignment for that device type. Fortinet's FortiNAC documentation describes network access policies and their enforcement configuration in the FortiNAC Administration Guide; product documentation is also available through the FortiNAC documentation portal.

QUESTION NO: 6

When configuring isolation networks in the configuration wizard, why does a layer 3 network typo allow for mora than ono DHCP scope for each isolation network typo?

A. The layer 3 network type allows for one scope for each possible host status.

B. Configuring more than one DHCP scope allows for DHCP server redundancy

C. There can be more than one isolation network of each type

D. Any scopes beyond the first scope are used if the initial scope runs out of IP addresses.

ANSWER: C

Explanation:

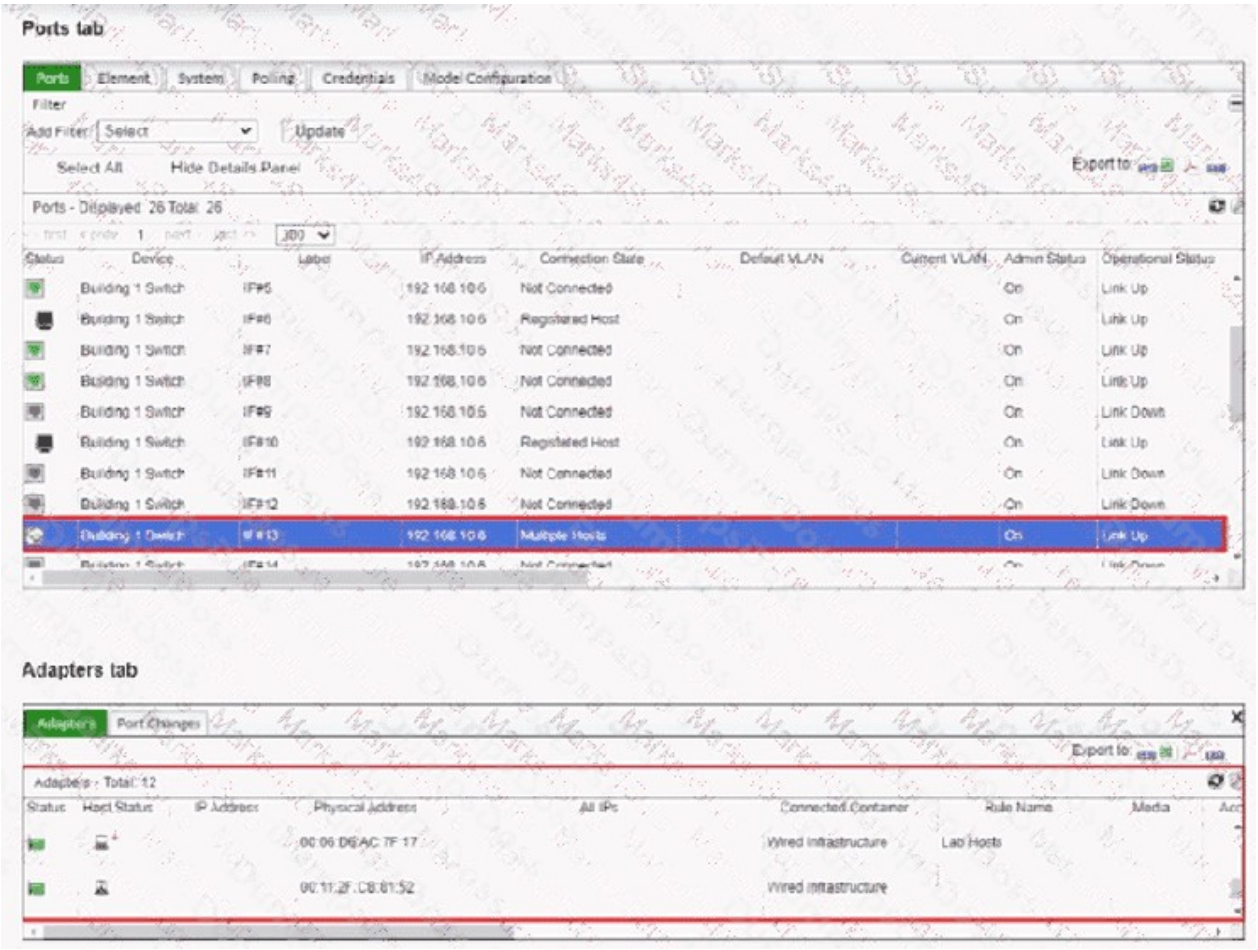
"There can be more than one isolation network of each type" is correct because a Layer 3 isolation configuration can represent multiple distinct isolation-network instances that serve the same isolation purpose. FortiNAC uses isolation networks to place endpoints into controlled network segments according to their current access or registration state. In a routed Layer 3 design, those segments can be separate IP subnets and can therefore require separate DHCP scopes to provide addressing for devices placed into each subnet.

The configuration wizard permits multiple scopes for an isolation-network type so the deployment can accommodate multiple Layer 3 isolation networks—for example, when different locations, VLANs, routing domains, or network segments need their own IP address pools while implementing the same isolation function. This supports scalable deployments without requiring every device assigned to a particular isolation type to use one shared subnet. The DHCP scopes define the address ranges available in the individual Layer 3 isolation segments, allowing FortiNAC to apply the intended isolation workflow across those segments.

For FortiNAC configuration concepts and administration guidance, see the FortiNAC-F 7.6 Administration Guide and the FortiNAC-F 7.6 documentation portal.

QUESTION NO: 7

Refer to the exhibits.



What would happen if the highlighted port with connected hosts was placed in both the Forced Registration and Forced Remediation port groups?

A. Both types of enforcement would be applied

B. Enforcement would be applied only to rogue hosts

C. Multiple enforcement groups could not contain the same port.

D. Only the higher ranked enforcement group would be applied.

ANSWER: A

Explanation:

Both types of enforcement would be applied is correct. FortiNAC-F permits a port to be included in more than one state-based enforcement system group, including Forced Registration and Forced Remediation. The applicable action is determined from the status of each endpoint detected through that port, rather than by selecting a single enforcement group for the port as a whole. Consequently, a host requiring registration can be directed to the registration isolation environment, while a host identified as at risk can be directed to the remediation or quarantine environment.

This is especially significant for the displayed connection because it has multiple hosts. FortiNAC-F maintains host-level state information and evaluates each connected endpoint independently. Associating the point of connection with both groups therefore makes the relevant enforcement workflow available for each host state encountered on that port. The configuration supports simultaneous state-based control outcomes across the connected endpoints, ensuring that registration and remediation controls are applied where their respective host conditions require them. Fortinet's FortiNAC documentation is available through the FortiNAC 7.6 documentation portal; related product and deployment resources are also published on the FortiNAC product page.