KaozhengPro

IT認證考試題庫

專業平臺

考證寶提供最新考古題與模擬試題
協助您高效通過認證考試

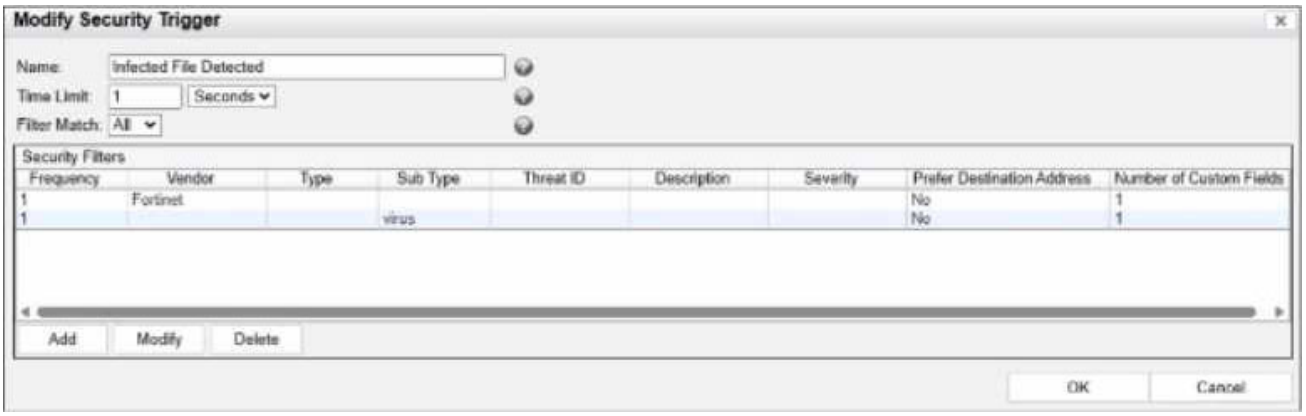
www.kaozhengpro.com

Exam : **NSE5_FNC_AD_7.6**

Title : Fortinet NSE 5 - FortiNAC-F 7.6 Administrator

Version : DEMO

1.Refer to the exhibit.



What would FortiNAC-F generate if only one of the security fitters is satisfied?

A. A normal alarm

B. A security event

C. A security alarm

D. A normal event

Answer: D

Explanation:

In FortiNAC-F, Security Triggers are used to identify specific security-related activities based on incoming data such as Syslog messages or SNMP traps from external security devices (like a FortiGate or an IDS). These triggers act as a filtering mechanism to determine if an incoming notification should be escalated from a standard system event to a Security Event.

According to the FortiNAC-F Administrator Guide and relevant training materials for versions 7.2 and 7.4, the Filter Match setting is the critical logic gate for this process. As seen in the exhibit, the "Filter Match" configuration is set to "All". This means that for the Security Trigger named "Infected File Detected" to "fire" and generate a Security Event or a subsequent Security Alarm, every single filter listed in the Security Filters table must be satisfied simultaneously by the incoming data.

In the provided exhibit, there are two filters: one looking for the Vendor "Fortinet" and another looking for the Sub Type "virus". If only one of these filters is satisfied (for example, a message from Fortinet that does not contain the "virus" subtype), the logic for the Security Trigger is not met. Consequently, FortiNAC-F does not escalate the notification. Instead, it processes the incoming data as a Normal Event, which is recorded in the Event Log but does not trigger the automated security response workflows associated with security alarms.

"The Filter Match option defines the logic used when multiple filters are defined. If 'All' is selected, then all filter criteria must be met in order for the trigger to fire and a Security Event to be generated. If the criteria are not met, the incoming data is processed as a normal event. If 'Any' is selected, the trigger fires if at least one of the filters matches." — FortiNAC-F Administration Guide: Security Triggers Section.

2.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.

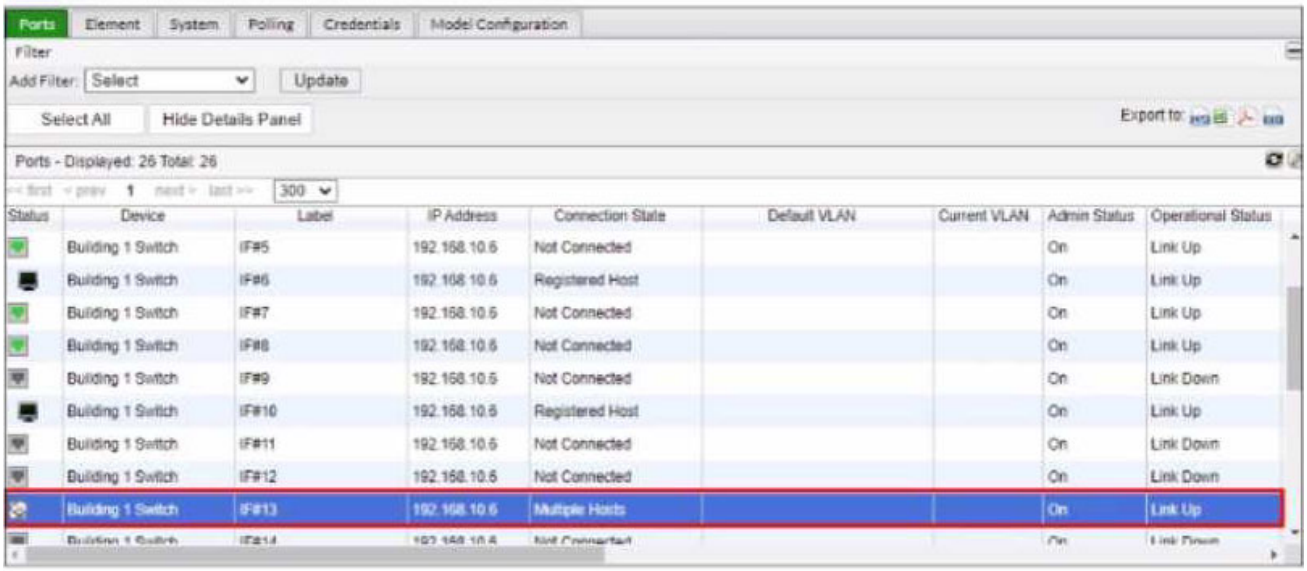
Answer: C
Explanation:
In FortiNAC-F, the Layer 3 Network type is specifically designed for deployments where the isolation networks—such as Registration, Remediation, and Dead End—are separated from the FortiNAC appliance's service interface (port2) by one or more routers. This architecture is common in large, distributed enterprise environments where endpoints in different physical locations or branches must be isolated into subnets that are local to their respective network equipment.
The reason the Configuration Wizard allows for more than one DHCP scope for a single isolation network type (state) is that there can be more than one isolation network of each type across the infrastructure. For instance, if an organization has three different sites, each site might require its own unique Layer 3 registration subnet to ensure efficient routing and to accommodate local IP address management. By allowing multiple scopes for the "Registration" state, FortiNAC can provide the appropriate IP address, gateway, and DNS settings to a rogue host regardless of which site's registration VLAN it is placed into.
When an endpoint is isolated, the network infrastructure (via DHCP Relay/IP Helper) directs the DHCP request to the FortiNAC service interface. FortiNAC then identifies which scope to use based on the incoming request's gateway information. This flexibility ensures that the system is not limited to a single flat subnet for each isolation state, supporting a scalable, multi-routed network topology.
"Multiple scopes are allowed for each isolation state (Registration, Remediation, Dead End, VPN, Authentication, Isolation, and Access Point Management). Within these scopes, multiple ranges in the lease pool are also permitted... This configWizard option is used when Isolation Networks are separated from the FortiNAC Appliance's port2 interface by a router." — FortiNAC-F Configuration Wizard Reference Manual: Layer 3 Network Section.

3.When FortiNAC-F is managing VPN clients connecting through FortiGate, why must the clients run a FortiNAC-F agent?
A. To transparently update The client IP address upon successful authentication
B. To collect user authentication details
C. To collect the client IP address and MAC address
D. To validate the endpoint policy compliance
Answer: C
Explanation:
When FortiNAC-F manages VPN clients through a FortiGate, the agent plays a fundamental role in device identification that standard network protocols cannot provide on their own. In a standard VPN connection, the FortiGate establishes a Layer 3 tunnel and assigns a virtual IP address to the client. While the FortiGate sends a syslog message to FortiNAC-F containing the username and this assigned IP address, it typically does not provide the hardware (MAC) address of the remote endpoint's physical or virtual adapter.
FortiNAC-F relies on the MAC address as the primary unique identifier for all host records in its database. Without the MAC address, FortiNAC-F cannot correlate the incoming VPN session with an existing host record to apply specific policies or track the device's history. By running either a Persistent or Dissolvable Agent, the endpoint retrieves its own MAC address and communicates it directly to the FortiNAC-F service interface. This allows the "IP to MAC" mapping to occur. Once FortiNAC-F has both the IP and the MAC, it can successfully identify the device, verify its status, and send the appropriate

FSSO tags or group information back to the FortiGate to lift network restrictions.
Furthermore, while the agent can also perform compliance checks (Option D), the architectural requirement for the agent in a managed VPN environment is primarily driven by the need for session data correlation—specifically the collection of the IP and MAC address pairing.
"Session Data Components: • User ID (collected via RADIUS, syslog and API from the FortiGate).
• Remote IP address for the remote user connection (collected via syslog and API from the FortiGate and from the FortiNAC agent). • Device IP and MAC address (collected via FortiNAC agent). ... The Agent is used to provide the MAC address of the connecting VPN user (IP to MAC)." — FortiNAC-F FortiGate VPN Integration Guide: How it Works Section.

4.Refer to the exhibits.

Ports tab



Adapters tab

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: D
Explanation:
In FortiNAC-F, Port Groups are used to apply specific enforcement behaviors to switch ports. When a

port is assigned to an enforcement group, such as Forced Registration or Forced Remediation, FortiNAC-F overrides normal policy logic to force all connected adapters into that specific state. The exhibit shows a port (IF#13) with "Multiple Hosts" connected, which is a common scenario in environments using unmanaged switches or hubs downstream from a managed switch port.
According to the FortiNAC-F Administrator Guide, it is possible for a single port to be a member of multiple port groups. However, when those groups have conflicting enforcement actions—such as one group forcing a registration state and another forcing a remediation state—FortiNAC-F utilizes a ranking system to resolve the conflict. In the FortiNAC-F GUI under Network > Port Management > Port Groups, each group is assigned a rank. The system evaluates these ranks, and only the higher ranked enforcement group is applied to the port. If a port is in both a Forced Registration group and a Forced Remediation group, the group with the numerical priority (rank) will dictate the VLAN and access level assigned to all hosts on that port.
This mechanism ensures consistent behavior across the fabric. If the ranking determines that "Forced Registration" is higher priority, then even a known host that is failing a compliance scan (which would normally trigger Remediation) will be held in the Registration VLAN because the port-level enforcement takes precedence based on its rank.
"A port can be a member of multiple groups. If more than one group has an enforcement assigned, the group with the highest rank (lowest numerical value) is used to determine the enforcement for the port. When a port is placed in a group with an enforcement, that enforcement is applied to all hosts connected to that port, regardless of the host's current state." — FortiNAC-F Administration Guide: Port Group Enforcement and Ranking.

5.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 lwo 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:
In FortiNAC-F, the Security Incidents engine is used to automate responses to security threats reported by external devices. When an administrator wants to enforce a policy, such as quarantining contractors who access restricted websites, they must create a Security Rule. A Security Rule acts as the "if-then" logic that correlates incoming security data with the internal host database.
The documentation specifies that a Security Rule consists of three primary configurable components:
User/Host Profile: This identifies who or what the rule applies to (in this case, "Contractors").
Trigger: This is the event that initiates the rule evaluation. In this scenario, the Trigger would be configured to match specific syslog messages or NetFlow data indicating access to prohibited websites. Triggers use filters to match vendor-specific data, such as a "Web Filter" event from a FortiGate.
Action: This defines what happens when the Trigger and User/Host Profile are matched. For this scenario, the administrator would select a "Quarantine" action, which instructs FortiNAC-F to move the

endpoint to a restricted VLAN or apply a restrictive ACL.
While "Methods" (A) relate to authentication and "Security Strings" (E) are used for specific SNMP or CLI matching, they are not the structural components of a Security Rule in the Security Incidents menu.
"Security Rules are used to perform a specific action based on certain criteria... To configure a Security Rule, navigate to Logs > Security Incidents > Rules. Each rule requires a Trigger to define the event criteria, an Action to define the automated response (such as Quarantine), and a User/Host Profile to limit the rule to specific groups." — FortiNAC-F Administration Guide: Security Rules and Incident Management.