Fortinet.NSE5_FNC_AD-7.6.v2026-05-18.q29

Exam Code:	NSE5_FNC_AD-7.6
Exam Name:	Fortinet NSE 5 - FortiNAC-F 7.6 Administrator
Certification Provider:	Fortinet
Free Question Number:	29
Version:	v2026-05-18
# of views:	102
# of Questions views:	300
https://www.freecram.net/torrent/Fortinet.NSE5_FNC_AD-7.6.v2026-05-18.q29.html	

NEW QUESTION: 1
A healthcare organization is integrating FortiNAC-F with its existing MDM. Communication is failing between the systems.
What could be a probable cause?
A. Security Fabric traffic is failing
B. SSH communication is failing
C. REST API communication is failing
D. SOAP API communication is failing
Answer: (SHOW ANSWER)
The integration between FortiNAC-F and Mobile Device Management (MDM) platforms (such as Microsoft Intune, VMware Workspace ONE, or Jamf) is a critical component for providing visibility into mobile assets that do not connect directly to the managed infrastructure via standard wired or wireless protocols.
According to the FortiNAC-F MDM Integration Guide, the communication between the FortiNAC-F appliance and the MDM server is handled through REST API calls. FortiNAC-F acts as an API client, periodically polling the MDM server to retrieve device metadata, compliance status, and ownership information. If communication is failing, it is most likely because the API credentials (Client ID/Secret) are incorrect, the MDM's API endpoint is unreachable from the FortiNAC-F service port, or the SSL certificate presented by the MDM is not trusted by the FortiNAC-F root store.

NEW QUESTION: 2
Two FortiNAC-F devices have been configured as a 1+1 HA pair. The primary server went offline and a successful failover to the secondary has occurred.
What happens if the primary server comes back online?
A. The secondary server will update the primary and the servers will load balance until an administrator forces the primary to resume full control.
B. After five successful heartbeats between the servers, the primary server will resume control.
C. The primary server will determine that the secondary has control and power down for maintenance.

D. The primary and secondary servers will resume communication and the secondary will maintain control.
Answer: (SHOW ANSWER)
In a 1+1 HA configuration, once failover has occurred and the secondary assumes control, it remains the active controller when the original primary comes back online. The restored primary rejoins as the standby unit, and control is not automatically reverted.

NEW QUESTION: 3
Which three communication methods are used by FortiNAC to gather information from and control, infrastructure devices? (Choose three.)
A. SMTP
B. CLI
C. RADIUS
D. SNMP
E. FTP
Answer: B,C,D (LEAVE A REPLY)

NEW QUESTION: 4
In a wireless integration, what method does FortiNAC use to obtain connecting MAC address information?
A. Link traps
B. SNMP traps
C. RADIUS
D. Endstation traffic monitoring
Answer: C (LEAVE A REPLY)

NEW QUESTION: 5
Which group type can have members added directly from the FortiNAC Control Manager?
A. Host
B. Port
C. Device
D. Administrator
Answer: (SHOW ANSWER)

NEW QUESTION: 6
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.)
A. Remediation admin scan
B. MDM integration
C. Persistent agent
D. Custom scan

Answer: (SHOW ANSWER)
Compliance monitors require the persistent agent to continuously evaluate endpoint conditions such as registry keys and service status. A custom scan must be defined to specify the exact registry key and security service checks that the monitor will assess on the endpoint.

NEW QUESTION: 7
While troubleshooting a network connectivity issue, an administrator determines that a device was being automatically provisioned to an incorrect VLAN.
Where would the administrator look to identify when and why FortiNAC-F made the network access change?
A. The Port Changes view
B. The Security Event view
C. The Reports view
D. The Admin Auditing view
Answer: (SHOW ANSWER)
The Port Changes view records provisioning actions performed by FortiNAC-F, including VLAN changes, along with the associated reason and timestamp. This allows the administrator to determine when the network access change occurred and what triggered it.

NEW QUESTION: 8
In an isolation VLAN which three services does FortiNAC supply? (Choose three.)
A. NTP
B. DHCP
C. Web
D. ISMTP
E. DNS
Answer: (SHOW ANSWER)

NEW QUESTION: 9
When preparing network infrastructure devices for visibility, what are the two main advantages of using MAC notification traps on supported devices instead of linkup and linkdown traps? (Choose two.)
A. Overhead on FortiNAC-F and the infrastructure device will be reduced.
B. Faster visibility updates with only a slight increase in processing.
C. MAC notification traps will include IP address information.
D. Hosts connecting to downstream non-managed hubs will be immediately learned.
Answer: (SHOW ANSWER)
MAC notification traps provide immediate notification when a MAC address is learned or removed on a port, resulting in faster and more accurate visibility updates compared to relying only on link state changes. They also allow FortiNAC-F to learn multiple hosts connected behind downstream unmanaged hubs or switches because each MAC address event is reported individually.

NEW QUESTION: 10

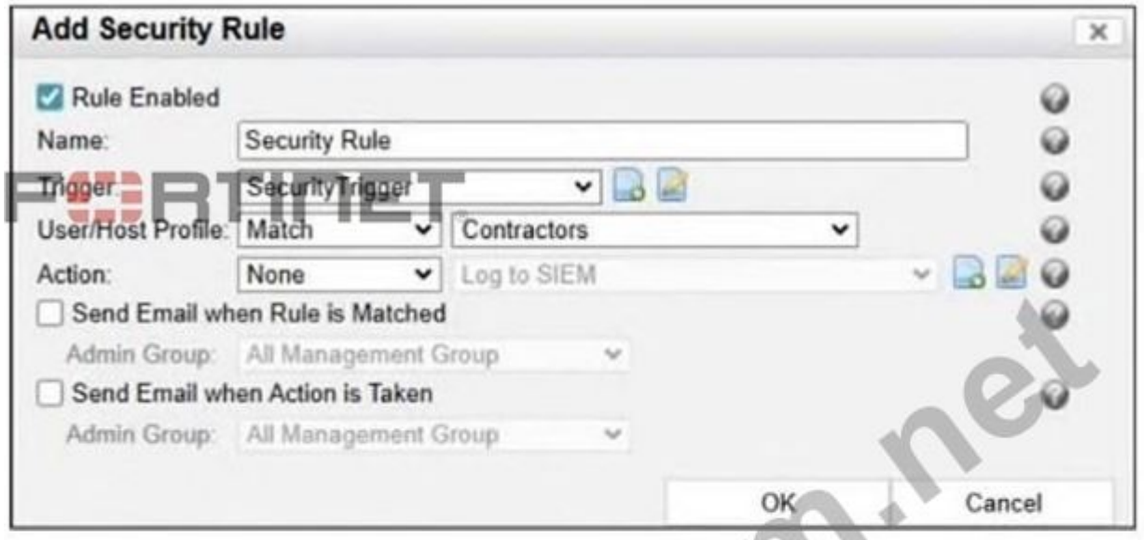
During the testing of a newly modeled infrastructure switch, the administrator is not seeing hosts as they connect or move from one port to another.
What would cause this issue?

A. The default scheduled polling is disabled.
B. Contact polling is not configured.
C. MAC notification traps are misconfigured.
D. Layer 3 polling is failing.
Answer: (SHOW ANSWER)
FortiNAC-F relies on correctly configured MAC notification (link) traps to detect hosts connecting or moving between ports in real time. If these traps are misconfigured, the system will not receive port-level MAC change events, so newly connected or moved hosts will not be detected as expected.

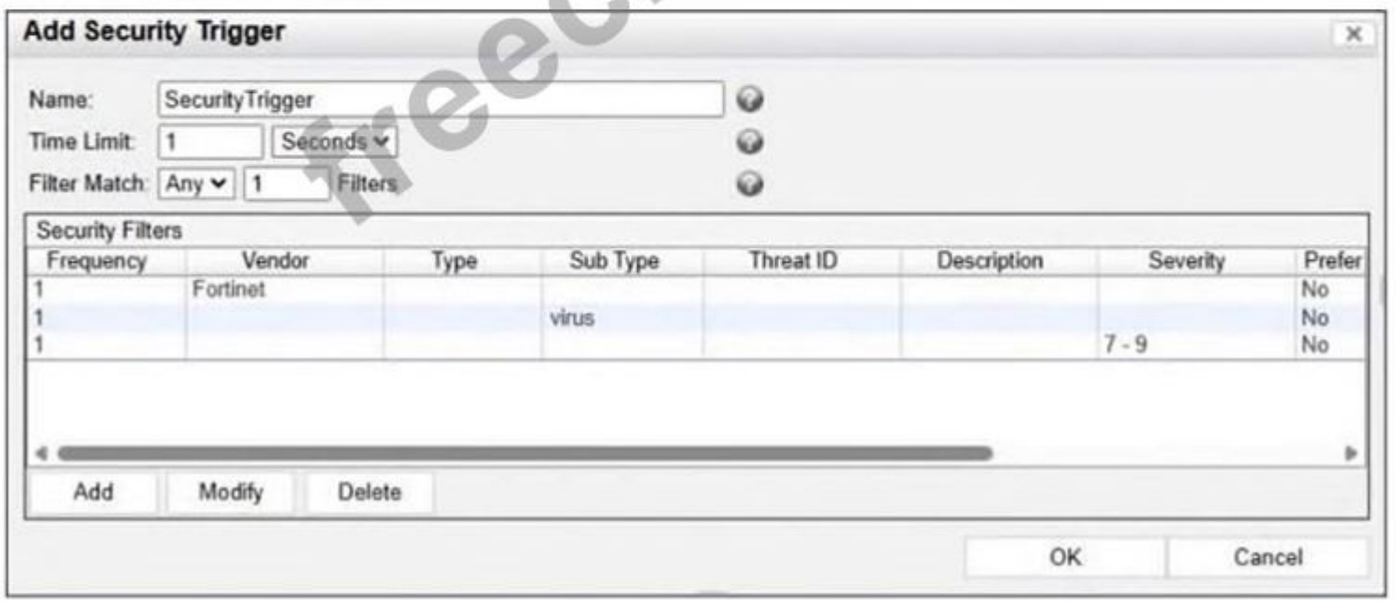
NEW QUESTION: 11
Which two things must be done to allow FortiNAC to process incoming syslog messages from an unknown vendor? (Choose two.)
A. The device must be added as a patch management server.
B. A security event parser must be created for the device.
C. The device sending the messages must be modeled in the Network Inventory view.
D. The device must be added as a log receiver.
Answer: (SHOW ANSWER)

NEW QUESTION: 12
Refer to the exhibits.

Security Rule configuration



Security Trigger configuration



Given the current configuration, what would happen if a contractor triggered two of the defined security filters?

A. A security alarm and two security events would be generated.

B. Three security events and one security alarm would be generated.

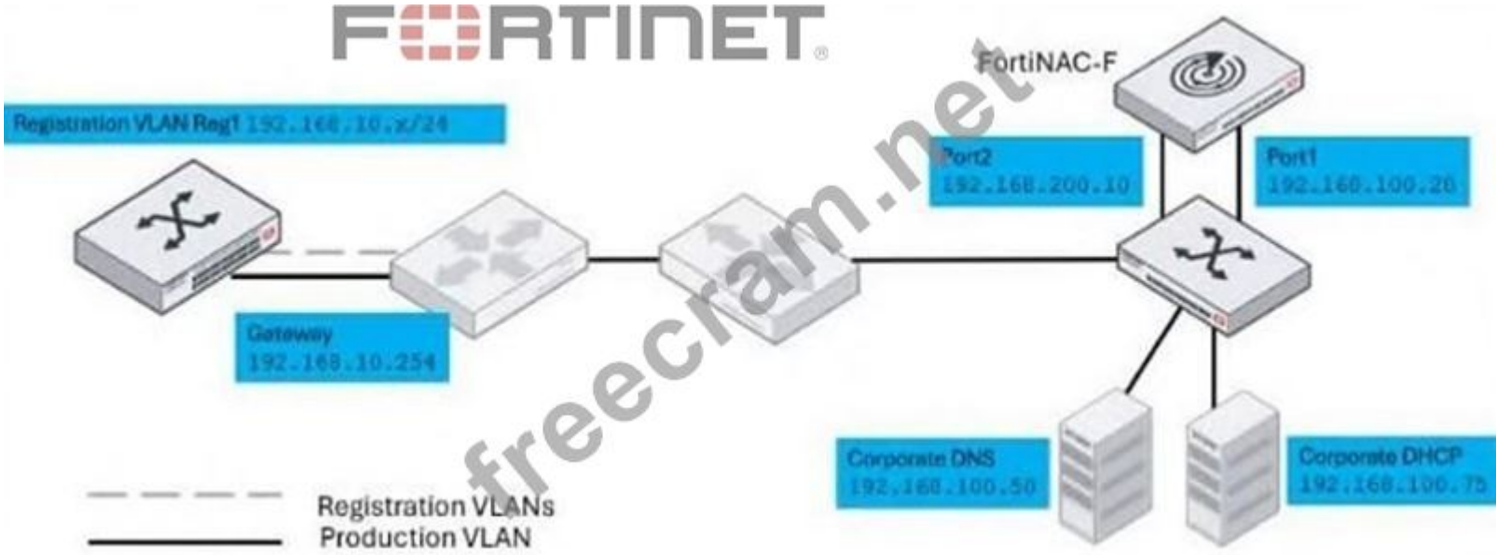
C. A security event and a security alarm would be generated.

D. Two security events would be generated, but no security alarm would be generated.

Answer: (SHOW ANSWER)

Each matched security filter generates its own security event. Since the trigger is configured to match any one filter within the defined time limit, multiple matched filters will generate multiple events, but only one security alarm is created when the security rule condition is satisfied.

NEW QUESTION: 13
Refer to the exhibit.



Given this topology, and a layer 3 registration network configuration, which IP address would be designated in the DHCP relay configuration for the registration network?
A. 192.168.200.10
B. 192.168.100.20
C. 192.168.100.75
D. 192.168.10.254
Answer: (SHOW ANSWER)
In a layer 3 registration design, the registration VLAN's gateway relays DHCP requests to the FortiNAC-F interface that serves the registration network. In this topology, that is the FortiNAC-F registration-side interface (Port2).

NEW QUESTION: 14
How can an administrator configure FortiNAC-F to normalize incoming syslog event levels across vendors?
A. Configure severity mappings.
B. Configure the vendor OUI settings.
C. Configure the security rule settings.
D. Configure event to alarm mappings.
Answer: (SHOW ANSWER)
FortiNAC-F serves as a central manager for security events originating from a diverse ecosystem of third-party security appliances, such as FortiGate, Check Point, and Cisco. Each vendor utilizes its own internal scale for severity levels within syslog messages (e.g., Check Point uses a
1? scale, while others may use 0?). To provide a consistent response regardless of the source, FortiNAC-F uses Severity Mappings to normalize these incoming values.
According to the FortiNAC-F Administration Guide, severity mappings allow the administrator to translate vendor-specific threat levels into standardized FortiNAC Security Levels (such as High, Medium, or Low Violation). When a syslog message arrives, the parser extracts the vendor's severity code, and the system

immediately references the Security Event Severity Level Mappings table to determine how that event should be categorized internally. This normalization is vital because it allows a single Security Alarm to be configured to respond to any "High Violation" event, whether it was reported as a "Critical" by one vendor or a "Level 5" by another.
Without these mappings, the administrator would have to create separate, redundant security rules for every vendor to account for their different naming conventions and numerical scales.
"Each vendor defines its own severity levels for syslog messages. The following table shows the equivalent FortiNAC security level... To normalize these events, configure the Severity Level Mappings found in the device integration guides. This allows FortiNAC to generate a consistent security event that can then trigger an alarm regardless of the reporting vendor's specific terminology."

NEW QUESTION: 15
An administrator has created several device profiling rules and evaluated all existing devices in the database. Some of the devices appear in the profiled devices view because they matched a rule, but they remain unknown and the registration column in the profiled devices view shows
"No".
What is the most likely cause?
A. The confirm device profiling rule option is not enabled.
B. The devices match more than one device profiling rule.
C. The device profiling rule has registration set to manual.
D. The devices have persistent agents installed, and the point of connection has PA optimization enabled.
Answer: (SHOW ANSWER)
In FortiNAC-F, Device Profiling Rules are used to automatically identify and categorize devices (such as IP cameras, printers, or IoT devices) based on fingerprints like DHCP fingerprints, OIDs, or MAC prefixes. When a device matches a rule, it appears in the Profiled Devices view.
However, matching a rule does not automatically register the device in the database unless the rule is configured to do so. If the devices appear in the view but remain "Unknown" and show
"No" in the registration column, it indicates that the "Confirm" (or "Auto-register") action has not been triggered.
In the Device Profiling Rule configuration, there is a setting called "Allow Auto- Approval" or "Confirm". If this is not enabled, the system identifies the device but waits for an administrator to manually approve the match before changing the host status from "Unknown" to
"Registered".
This is a common "safety" configuration used during the initial deployment phase to ensure that the profiling rules are accurate before the system begins automatically granting network access based on those matches.
"If a device matches a rule but is not registered, check the rule configuration. The Confirm option (within the Method or Rule settings) determines if the system automatically registers the device upon a match. If Confirm is not enabled, the device will remain in the 'Profiled' state with a registration status of 'No' until an administrator manually promotes the device."

NEW QUESTION: 16

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: (SHOW ANSWER)

The FortiNAC-F Manager (FortiNAC-M) is designed as a centralized management platform for large- scale distributed environments where multiple FortiNAC-F Control and Application (CA) appliances are deployed across different sites. According to the FortiNAC-F Manager Administration Guide, the deployment of a Manager simplifies administrative overhead in three specific ways:

First, it provides Global Version Control (B). The Manager serves as a central repository for firmware and software updates, allowing administrators to push specific versions to all managed CAs simultaneously, ensuring consistency across the entire fabric. Second, it enables Pooled Licenses (D). Instead of purchasing and managing individual licenses for every CA, licenses are centralized on the Manager. The Manager then distributes these licenses to the CAs as needed based on their host counts. This "floating" license model optimizes cost and prevents individual sites from running out of capacity while others have excess. Third, it offers Global Visibility (E).

The Manager aggregates host and device data from every managed CA into a single console.

This "single pane of glass" allows an administrator to search for a specific MAC address or user across the entire global organization without logging into individual servers.

NEW QUESTION: 17

A user was attempting to register their host through the registration captive portal. After successfully registering, the host remained in the registration VLAN. Which two conditions would cause this behavior? (Choose two.)

A. There is another unregistered host on the same port

B. There is no agent installed on the host.

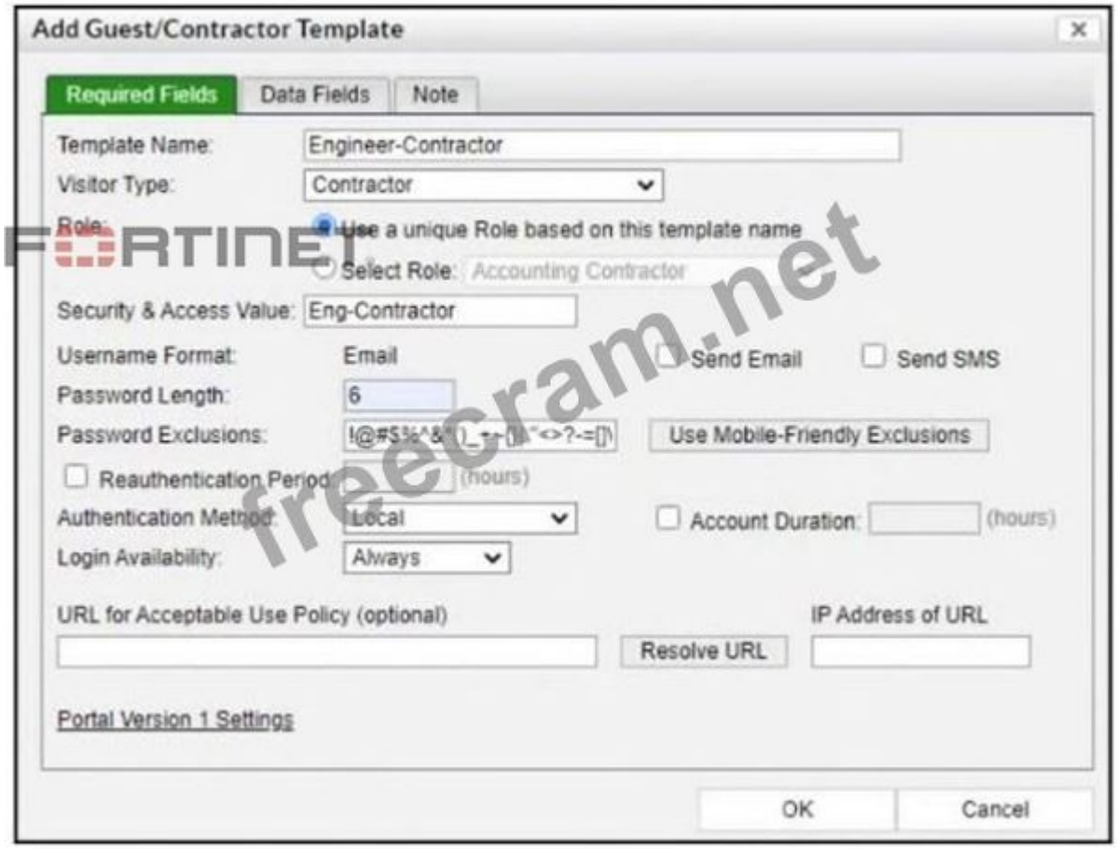
C. The port default VLAN is the same as the Registration VLAN.

D. The wrong agent s installed.

Answer: (SHOW ANSWER)

NEW QUESTION: 18
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.)
A. Mobile
B. Dissolvable
C. Passive
D. Persistent
Answer: (SHOW ANSWER)
The persistent agent remains installed on the endpoint and can perform scheduled compliance scans automatically without user interaction. The passive agent collects endpoint information without requiring installation or user action, enabling ongoing compliance evaluation transparently.

NEW QUESTION: 19
Refer to the exhibit.
Guest/Contractor template



When a contractor account is created using this template, which value is set in the accounts Role field?
A. Accounting Contractor
B. Eng-Contractor
C. Engineer-Contractor
D. Contractor

Answer: (SHOW ANSWER)

The template is configured to use a unique role based on the template name. Therefore, when the account is created, the Role field is automatically set to the template name, which is Engineer-Contractor.

NEW QUESTION: 20

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 portal configuration

C. In the User/Host profile

D. In the Guest template

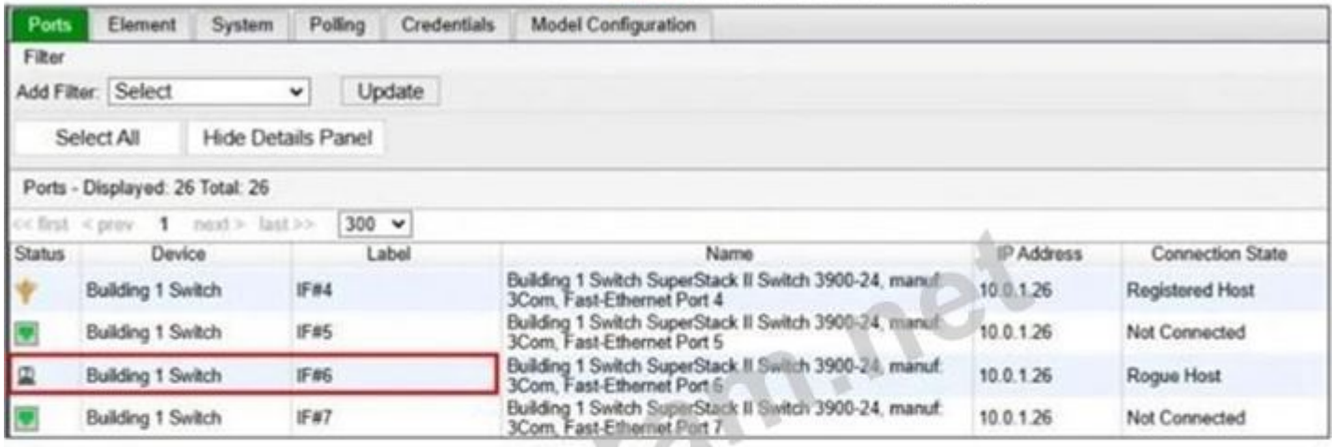
Answer: (SHOW ANSWER)

The Guest-VLAN value is defined within the switch Model configuration, where VLAN mappings and enforcement actions are configured. The network access policy references this configuration to apply the appropriate VLAN when the policy conditions are met.

NEW QUESTION: 21

Refer to the exhibits.

Ports Tab



Polling Tab

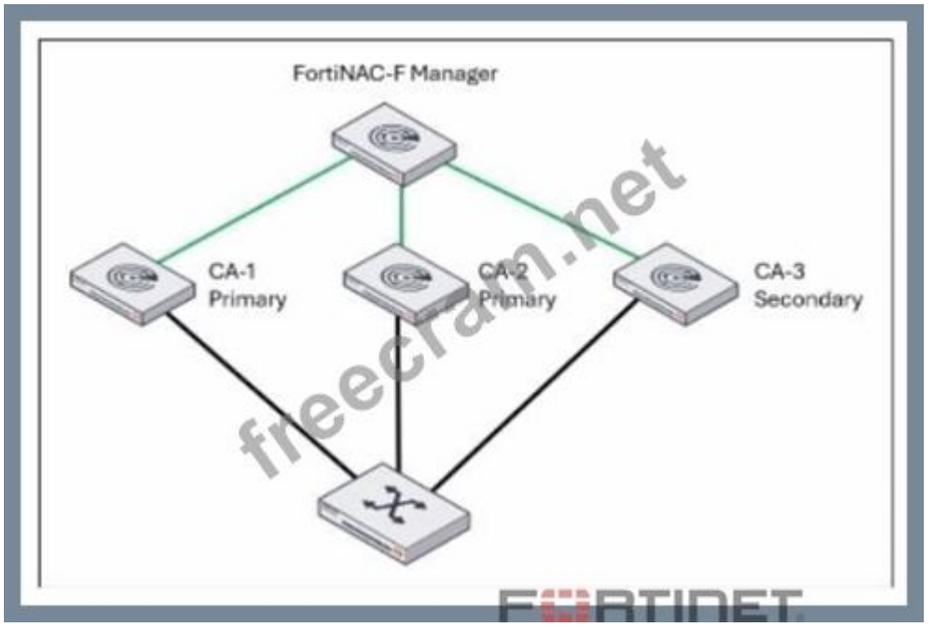
Model Configuration Tab

An administrator is troubleshooting visibility issues on a modeled switch. The switch is configured to use link traps and to provision hosts based on network access policies. The administrator is seeing hosts on ports with no hosts connected and not seeing hosts on ports where hosts are known to be connected.

What is the most likely cause?

A. The switch cannot be contacted by FortiNAC-F.
B. The credentials are incorrect.
C. The logical networks are set to deny.
D. The host has uninstalled the FortiNAC-F agent.
Answer: (SHOW ANSWER)
Incorrect switch credentials prevent FortiNAC-F from successfully performing SNMP-based polling (such as layer 2 host learning) needed to accurately learn and clear hosts per port. As a result, FortiNAC-F displays stale or missing host-to-port associations even though link traps are enabled.

NEW QUESTION: 22
Refer to the exhibit. A FortiNAC-F N+1 HA configuration is shown.



What will occur if CA-2 fails?
A. CA-1 and CA-3 will operate as a 1+1 HA cluster with CA-3 acting as a hot standby.
B. CA-3 will continue to operate as a secondary in an N+1 HA configuration.
C. CA-3 will be promoted to a primary and share management responsibilities with CA-1.
D. CA-3 will be promoted to a primary and FortiNAC-F manager will load balance between CA-1 and CA-3.
Answer: (SHOW ANSWER)
In an N+1 HA architecture managed by a FortiNAC-F Manager, if a primary CA fails, an available secondary CA is automatically promoted to primary. After CA-2 fails, CA-3 is promoted to a primary role, and the FortiNAC-F Manager load balances management and enforcement responsibilities between the remaining primary CAs, CA-1 and CA-3.

NEW QUESTION: 23
Which two requirements must be met to set up an N+1 HA cluster? (Choose two.)
A. A FortiNAC-F manager
B. A FortiNAC-F device designated as a secondary
C. A dedicated VLAN for primary and secondary synchronization

D. At least two FortiNAC-F devices designated as primary

Answer: (SHOW ANSWER)

The N+1 High Availability (HA) architecture was introduced in FortiNAC-F version 7.6 to provide a more scalable and flexible redundancy model compared to the traditional 1+1 active/passive setup.

In an N+1 configuration, a single secondary (standby) appliance can provide coverage for multiple primary (active) Control and Application (CA) appliances.

To set up an N+1 HA cluster, there are two fundamental structural requirements:

A FortiNAC-F Manager (FortiNAC-M): Unlike standard 1+1 HA, which can be configured directly between two CAs, N+1 management is centralized. The FortiNAC-M acts as the orchestrator that manages the failover groups, monitors the health of the primaries, and coordinates the promotion of the secondary server if a primary fails.

A FortiNAC-F device designated as a Secondary: The cluster must have one appliance explicitly configured with the Secondary failover role. This device remains in a standby state, receiving database replications from all N primaries in its group until it is called upon to take over the functions of a failed unit

NEW QUESTION: 24

An administrator wants to build device profiling rules based on network traffic, but the network session view is not populated with any records.

Which two settings can be enabled to gather network session information? (Choose two.)

A. Network traffic polling on any modeled infrastructure device

B. Firewall session polling on modeled FortiGate devices

C. Netflow setting on the FortiNAC-F interfaces

D. Layer 3 polling on the infrastructure devices

Answer: (SHOW ANSWER)

In FortiNAC-F, the Network Sessions view provides a real-time and historical log of traffic flows, including source/destination IP addresses, ports, and protocols. This data is essential for building Device Profiling Rules that rely on "Traffic Patterns" or "Network Footprints" to identify devices (e.g., an IP camera communicating with its specific NVR). If the network session view is empty, the system is not receiving the necessary flow or session data from the network infrastructure.

According to the FortiNAC-F Administration Guide, there are two primary methods to populate this view:

NetFlow/sFlow/IPFIX (C): FortiNAC-F can act as a flow collector. By enabling NetFlow settings on the FortiNAC-F service interface (port2/eth1) and configuring your switches or routers to export flow data to the FortiNAC IP, the system can parse these packets and record sessions.

Firewall Session Polling (B): For environments with FortiGate firewalls, FortiNAC-F can proactively poll the FortiGate via the REST API to retrieve its current session table. This is particularly useful as it provides session visibility without requiring the overhead of configuring NetFlow on every access layer switch.

NEW QUESTION: 25

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: (SHOW ANSWER)
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.

NEW QUESTION: 26
An administrator wants to create a conference manager administrator account but would like to limit the number of conference accounts that can be generated to 30.
Which statement about conference accounts is true?
A. In FortiNAC-F, conference accounts can be limited by multiples of 25, so the conference administrator could create 50 accounts.
B. The administrator can set a maximum of 30 conference accounts in the administrative profile for the conference manager.
C. The conference account limit is defined in the onboarding conference portal.
D. Conference account limits are defined in the conference guest and contractor template.
Answer: B (LEAVE A REPLY)
In FortiNAC-F, the Conference Manager is a specialized administrative role designed for delegated administration, often used by receptionists or event organizers to create temporary guest accounts. To maintain security and prevent the over-provisioning of credentials, FortiNAC-F allows for granular restrictions on these accounts.
According to the FortiNAC-F Administration Guide regarding Administrative Profiles, when an administrator creates a profile for a Conference Manager, they can define specific "Account Limits." Under the profile settings (located in System > Settings > Admin Profiles), there is a field specifically for "Max Accounts." By entering "30" into this field, the administrator ensures that any user assigned to this profile cannot exceed 30 active conference accounts at any given time.
This setting is distinct from the Portal configuration or the Guest templates. While templates define the type of account (e.g., duration and access level), the Administrative Profile defines the capabilities and limitations of the person creating those accounts. This ensures that even if a guest template allows for unlimited registrations, the specific administrator is physically restricted by the system from generating more than the allotted 30.

"Administrative Profiles define what an administrator can see and do within the system. For delegated administration roles like the Conference Manager, the 'Max Accounts' field in the Administrative Profile is used to specify the maximum number of accounts the user is permitted to create. Once this limit is reached, the user will be unable to generate additional accounts until existing ones expire or are deleted."

NEW QUESTION: 27
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. 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: (SHOW ANSWER)
With a layer 3 isolation network type, FortiNAC-F supports multiple isolation networks of the same type, each with its own routed subnet. This design allows administrators to define more than one DHCP scope per isolation network type to accommodate multiple layer 3 isolation segments.

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 allow access to only the production DNS server
B. To deny access to only the production DNS server
C. To allow access to only the FortiNAC VPN interface
D. To deny access to only the FortiNAC VPN interface
Answer: (SHOW ANSWER)

NEW QUESTION: 29
An administrator wants to use FortiNAC-F to prevent internal engineers from accessing specific websites as defined in web filter categories on FortiGate.
In addition to a security trigger and associated action, which configuration must also be defined on FortiNAC-F?
A. A profiling method
B. A firewall policy
C. A compliance policy
D. A user/host profile
Answer: (SHOW ANSWER)
To enforce restrictions based on web filter categories for internal engineers, FortiNAC-F must identify and group those users or their devices. A user/host profile defines the specific users or hosts (such as internal engineers) to which the security trigger and associated action will apply, enabling targeted enforcement.

Valid NSE5_FNC_AD-7.6 Dumps shared by EduDump.com for Helping Passing NSE5_FNC_AD-7.6 Exam! EduDump.com now offer the **newest NSE5_FNC_AD-7.6 exam dumps**, the EduDump.com NSE5_FNC_AD-7.6 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com NSE5_FNC_AD-7.6 dumps with Test Engine here: https://www.edudump.com/exams/Fortinet/NSE5_FNC_AD-7.6/premium/ (**71** Q&As Dumps, **35%OFF** **Special Discount Code: freecram**)