KillTest

Mejor calidad. Mejor servicio

Preguntas de práctica

https://www.killtest.es

Actualizaciones gratuitas durante un año

Exam : **NSE6_FNC_AD-7.6**

Title : Fortinet NSE 6 - FortiNAC-F 7.6 Administrator

Version : DEMO

1.A network administrator is troubleshooting a network access issue for a specific host. The administrator suspects the host is being assigned a different network access policy than expected.
Where would the administrator look to identify which network access policy, if any, is being applied to a particular host?
A. The Policy Logs view
B. The Connections view
C. The Policy Details view for the host
D. The Port Properties view of the hosts port
Answer: C
Explanation:
When troubleshooting network access in FortiNAC-F, it is often necessary to verify exactly why a host has been granted a specific level of access. Since FortiNAC-F evaluates policies from the top down and assigns access based on the first match, an administrator needs a clear way to see the results of this evaluation for a specific live endpoint.
The Policy Details (C) view is the designated tool for this purpose. By navigating to the Hosts > Hosts (or Adapter View) in the Administration UI, an administrator can search for the specific MAC address or IP of the host in question. Right-clicking on the host record reveals a context menu from which Policy Details can be selected. This view provides a real-time " look " into the policy engine ' s decision for that specific host, showing the Network Access Policy that was matched, the User/Host Profile that triggered the match, and the resulting Network Access Configuration (VLAN/ACL) currently applied.
While Policy Logs (A) provide a historical record of all policy transitions across the system, they are often too high-volume to efficiently find a single host ' s current state. The Connections view (B) shows the physical port and basic status but lacks the granular policy logic breakdown. The Port Properties (D) view shows the configuration of the switch interface itself, which is only one component of the final access determination.
"To identify which policy is currently applied to a specific endpoint, use the Policy Details view. Navigate to Hosts > Hosts, select the host, right-click and choose Policy Details. This window displays the specific Network Access Policy, User/Host Profile, and Network Access Configuration currently in effect for that host record. " —FortiNAC-F Administration Guide: Policy Details and Troubleshooting.

2.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: D
Explanation:
In FortiNAC-F, the maximum number of conference attendees/accounts is controlled by the Guest & Contractor template, not by the sponsor’s administrative profile. The FortiNAC-F 7.6 Administrator Study Guide states that conference accounts are initiated by a sponsor but automatically generated by

FortiNAC-F, and specifically that “the maximum number of attendees is defined within the template.”
The Administration Guide provides the corresponding configuration field: Max Number Of Accounts, which is available when Visitor Type = Conference. Enabling this option allows the administrator to enter the maximum number of accounts that can ever be created using that template. Therefore, a value of exactly 30 can be configured; there is no requirement to use multiples of 25.
The administrative profile instead determines sponsor capabilities such as permitted account types, allowed templates, account-management scope, and maximum account duration. It does not define the numerical conference-account ceiling.
Thus, to enforce a limit of 30 conference accounts, configure Max Number Of Accounts = 30 in the conference Guest & Contractor template.
Study Guide
Reference: Guest and Contractor Management # Creating Conference Accounts, pp. 292–302.

3.An administrator wants to control user access to corporate resources by integrating FortiNAC-F with FortiGate using firewall tags defined on FortiNAC-F.
Where would the administrator assign the firewall tag value that will be sent to FortiGate?
A. RADIUS group attribute
B. Logical network
C. Device profiling rule
D. Security rule
Answer: B
Explanation:
Questions no:9
Verified **Answer:** B
Comprehensive and Detailed 250 to 300 words each Explanation with Exact Matched Extract from FortiNAC-
F Administrator library and documentation for current versions (including F 7.2, 7.4, and 7.6) documents:
In FortiNAC-F, the integration with FortiGate for Security Fabric and Single Sign-On (FSSO) allows the system to communicate the access level of an endpoint directly to the firewall using firewall tags. This eliminates the need for complex VLAN steering in some environments by allowing the FortiGate to apply policies based on these dynamic tags instead of just a physical or virtual network segment.
The actual assignment of the firewall tag value occurs within a Logical Network. In the FortiNAC-F architectural model, a Logical Network acts as a container for " Access Values ". When an administrator configures a Logical Network (located under Network > Logical Networks), they define what that network represents—such as " Corporate Access " or " Contractor Limited ". Within that definition, they assign the specific Firewall Tag that matches the tag created on the FortiGate. Once a user or host matches a Network Access Policy, FortiNAC-F identifies the associated Logical Network and pushes the defined tag to the FortiGate via the FSSO connector.
It is important to note that while Network Access Policies (and by extension Security Rules) are the logic engines that trigger the assignment, they do not hold the tag value itself. They simply point to a Logical Network, which serves as the central repository for that specific access configuration.
“To assign firewall tags, navigate to Network > Logical Networks. Select the desired logical network and click Edit. Under the Access Value section, select Firewall Tagas the type and enter the tag name exactly as it appears on the FortiGate. When a Network Access Policy matches a host, FortiNAC sends this tag

to the FortiGate as an FSSO message. " —FortiNAC-F Administration Guide: Logical Networks and Security Fabric Integration.

4.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:
In a1+1 High Availability (HA) deployment, FortiNAC-F supports two primary methods for management access: individual IP addresses or a Shared IP Address (also known as a Virtual IP or VIP). The Shared IP option is part of a Layer 2 Hade sign, which simplifies administration by providing a single URL or IP that always points to whichever appliance is currently in the " Active " or " In Control " state.
For a Shared IP configuration to function correctly, the Primary and Secondary administrative interfaces (port1) must be on the same subnet. This requirement exists because the Shared IP is a logical address that is dynamically assigned to the physical interface of the active unit. Since only one unit can own the IP at a time, both units must reside on the same broadcast domain (Layer 2) to ensure that ARP requests for the Shared IP are correctly answered and that the gateway remains reachable regardless of which unit is active. If the appliances were on different subnets (a Layer 3 HA design), a shared IP could not be used because it cannot " float " across different network segments; instead, administrators would need to manage each unit via its unique physical IP or use a FortiNAC Manager.
“For L2 HA configurations, click the Use Shared IP Address checkbox and enter the Shared IP Address information...If your Primary and Secondary Servers are not in the same subnet, do not use a shared IP address. The shared IP address moves between appliances during a failover and recovery and requires both units to reside on the same network. " —FortiNAC-F High Availability Reference Manual: Shared IP Configuration.

5.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.