



Vendor: Fortinet

Exam Code: NSE5_FNC_AD-7.6

Exam Name: Fortinet NSE 5 - FortiNAC-F 7.6 Administrator

Version: DEMO

QUESTION 1

An administrator manages a corporate environment where all users log into the corporate domain each time they connect to the network. The administrator wants to leverage login scripts to use a FortiNAC-F agent to enhance endpoint visibility

Which agent can be deployed as part of a login script?

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

Answer: B

Explanation:

The dissolvable agent is designed to be executed at user login and does not require permanent installation on the endpoint. This makes it suitable for deployment through domain login scripts, where it can run temporarily to collect endpoint posture and visibility information and then remove itself after execution.

QUESTION 2

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:

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 Tag as 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."

QUESTION 3

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: AB

Explanation:

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

QUESTION 4

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: BDE

Explanation:

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.

QUESTION 5

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

Explanation:

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."

QUESTION 6

Refer to the exhibit. What will happen to the host of a guest user created from this template if the time of connection is 8:00 PM?

Guest/Contractor Template

Add Guest/Contractor Template

Required Fields | Data Fields | Note

Template Name: StandardGuest

Visitor Type: Guest

Role: ☒ Use a unique Role based on this template name
☐ Select Role: Guest

Security & Access Value: StandardGuest

Username Format: Email ☐ Send Email ☐ Send SMS

Password Length: 8 ☐ Send Password Separately

Password Exclusions: !@#\$%^&*()_+~{|}~?~=[\]~ ☐ Use Mobile-Friendly Exclusions

☐ Reauthentication Period: (hours) ☐ Propagate Hosts

Authentication Method: Local ☐ Account Duration: (hours)

Login Availability: Specify Time Edit Time
M,Tu,W,Th,F 6:00 AM - 7:00 PM

URL for Acceptable Use Policy (optional) IP Address of URL

Resolve URL

Portal Version 1 Settings

OK Cancel

- A. The host will be marked as non-authenticated.
- B. The host will be marked as a rogue device.
- C. The host will be marked as at-risk.
- D. The host will be administratively disabled.

Answer: A

Explanation:

In FortiNAC-F, the Guest & Contractor Template is a configuration object that defines the parameters for accounts created by sponsors or through self-registration. One of the critical security controls within this template is the Login Availability setting. This setting restricts the specific days and times during which a guest or contractor is permitted to authenticate and access the network.

As shown in the exhibit, the "StandardGuest" template has Login Availability set to "Specify Time", with a schedule defined as Mon-Fri, 6:00 AM to 7:00 PM. If a guest user attempts to connect or authenticate at 8:00 PM, which is outside of the permitted window, FortiNAC-F's policy engine will automatically deny the authentication request. When an authentication attempt is denied due to schedule restrictions, the system does not move the host into the "Authenticated" or "Registered" state required for production access. Instead, the host is marked as non-authenticated in the adapter or host view.

QUESTION 7

What must an administrator configure to allow FortiNAC-F to process incoming syslog messages that are not supported by default?

- A. A Syslog Service Connector
- B. A Security Action
- C. A Security Event Parser
- D. A Log Receiver

Answer: C

Explanation:

FortiNAC-F provides a robust engine for processing security notifications from third-party devices. For standard integrations, such as FortiGate or Check Point, the system comes pre-loaded with templates to interpret incoming data. However, when an administrator needs FortiNAC-F to process syslog messages from a vendor or device that is not supported by default, they must configure a Security Event Parser.

The Security Event Parser acts as the translation layer. It uses regular expressions (Regex) or specific field mappings to identify key data points within a raw syslog string, such as the source IP address, the threat type, and the severity. Without a parser, FortiNAC-F may receive the syslog message but will be unable to "understand" its contents, meaning it cannot generate the necessary Security Event required to trigger automated responses. Once a parser is created, the system can extract the host's IP address from the message, resolve it to a MAC address via L3 polling, and then apply the appropriate security rules. This allows for the integration of any security appliance capable of sending RFC-compliant syslog messages.

"FortiNAC parses the information based on pre-defined security event parsers stored in FortiNAC's database... If the incoming message format is not recognized, a new Security Event Parser must be created to define how the system should extract data fields from the raw syslog message. This enables FortiNAC to generate a security event and take action based on the alarm configuration."

QUESTION 8

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 a 1+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 HA design, 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."

QUESTION 9

When creating a user or host profile, which three criteria can you apply? (Choose three.)

- A. Host or user group memberships
- B. Host or user attributes
- C. Adapter current VLAN
- D. An applied access policy
- E. Location

Answer: ABE

Explanation:

The User/Host Profile is the primary mechanism in FortiNAC-F for identifying and categorizing endpoints to determine their level of network access. According to the FortiNAC-F Administration Guide, a profile is built using a combination of criteria that define "Who" is connecting, "What" device they are using, and "Where" they are located on the network.

The three main categories of criteria available in the configuration are:

Host or User Attributes (B): This includes specific details such as the host's operating system, the user's role (e.g., Employee, Contractor), or custom attributes assigned to the record.

Host or User Group Memberships (A): Profiles can be configured to match endpoints that are members of specific internal FortiNAC groups or synchronized directory groups (like LDAP or Active Directory groups). This allows for broad policy application based on organizational structure.

Location (E): The "Where" component allows administrators to restrict a profile match to specific physical or logical areas of the network, such as a particular switch, a group of ports, or a specific SSID.

Thank You for Trying Our Product

Lead2pass Certification Exam Features:

- ★ More than **99,900** Satisfied Customers Worldwide.
- ★ Average **99.9%** Success Rate.
- ★ **Free Update** to match latest and real exam scenarios.
- ★ **Instant Download** Access! No Setup required.
- ★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.
- ★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.
- ★ **100%** Guaranteed Success or **100%** Money Back Guarantee.
- ★ **Fast**, helpful support **24x7**.



View list of all certification exams: <http://www.lead2pass.com/all-products.html>



Microsoft



ORACLE



CITRIX



JUNIPER
NETWORKS



EMC²
where information lives

10% Discount Coupon Code: ASTR14