

Free PDF Fortinet - NSE5_FNC_AD_7.6 - Fortinet NSE 5 - FortiNAC-F 7.6 Administrator-Valid Latest Exam Pattern



Pass4Leader has collected the frequent-tested knowledge into our NSE5_FNC_AD_7.6 practice materials for your reference according to our experts' years of diligent work. So our NSE5_FNC_AD_7.6 exam materials are triumph of their endeavor. By resorting to our NSE5_FNC_AD_7.6 practice materials, we can absolutely reap more than you have imagined before. We have clear data collected from customers who chose our NSE5_FNC_AD_7.6 training engine, the passing rate is 98-100 percent. So your chance of getting success will be increased greatly by our NSE5_FNC_AD_7.6 exam questions.

Fortinet NSE5_FNC_AD_7.6 Exam Syllabus Topics:

| Topic | Details |
|---------|---|
| Topic 1 | <ul style="list-style-type: none">Deployment and Provisioning: This domain focuses on configuring security automation for automatic event responses, implementing access control policies, setting up high availability for system redundancy, and creating security policies to enforce network security requirements. |
| Topic 2 | <ul style="list-style-type: none">Concepts and Initial Configuration: This domain covers organizing infrastructure devices within FortiNAC-F and understanding isolation networks for quarantining non-compliant devices. It includes using the configuration wizard for initial system setup and deployment. |
| Topic 3 | <ul style="list-style-type: none">Integration: This domain addresses connecting FortiNAC-F with other systems using Syslog and SNMP traps, managing multiple instances through FortiNAC-F Manager, and integrating Mobile Device Management for extending access control to mobile devices. |
| Topic 4 | <ul style="list-style-type: none">Network Visibility and Monitoring: This domain covers managing guest and contractor access, utilizing logging options for tracking network events, configuring device profiling for automatic device identification and classification, and troubleshooting network device connection issues. |

>> Latest NSE5_FNC_AD_7.6 Exam Pattern <<

Exam Questions For Fortinet NSE5_FNC_AD_7.6 [Revised] - The Best Method To Pass The Exam

Our company never sets many restrictions to the NSE5_FNC_AD_7.6 exam question. Once you pay for our study materials, our

system will automatically send you an email which includes the installation packages. You can conserve the NSE5_FNC_AD_7.6 real exam dumps after you have downloaded on your disk or documents. Whenever it is possible, you can begin your study as long as there has a computer. In addition, all installed NSE5_FNC_AD_7.6 study tool can be used normally. In a sense, our NSE5_FNC_AD_7.6 Real Exam dumps equal a mobile learning device. We are not just thinking about making money. Your convenience and demands also deserve our deep consideration. At the same time, your property rights never expire once you have paid for money. So the NSE5_FNC_AD_7.6 study tool can be reused after you have got the NSE5_FNC_AD_7.6 certificate. You can donate it to your classmates or friends. They will thank you so much.

Fortinet NSE 5 - FortiNAC-F 7.6 Administrator Sample Questions (Q34-Q39):

NEW QUESTION # 34

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 no agent installed on the host.
- B. The wrong agent is installed.
- C. The port default VLAN is the same as the Registration VLAN.
- D. There is another unregistered host on the same port

Answer: C,D

Explanation:

The process of moving a host from a Registration VLAN to a Production VLAN (Access VLAN) is a fundamental part of the FortiNAC-F "VLAN steering" workflow. When a host successfully registers via the captive portal, FortiNAC-F evaluates its Network Access Policies to determine the correct VLAN. If the host remains stuck in the Registration VLAN despite a successful registration, it is typically due to port-level restrictions or the presence of other unregistered devices.

The two most common reasons for this behavior as per the documentation are:

The port default VLAN is the same as the Registration VLAN: If the "Default VLAN" field in the switch port's model configuration is set to the same ID as the Registration VLAN, the port will not change state because FortiNAC-F believes it is already in its "normal" or "forced" state.

There is another unregistered host on the same port: FortiNAC-F maintains the security posture of the physical port. If multiple hosts are connected to a single port (e.g., via a hub or unmanaged switch) and at least one host remains "Rogue" (unregistered), FortiNAC-F will generally keep the entire port in the isolation/registration VLAN to prevent the unregistered host from gaining unauthorized access to the production network.

Issues with agents (A, B) typically prevent a host from completing compliance or registration but do not usually result in a "stuck" status after registration has already been marked as successful in the system.

"If a port is identified as having Multiple Hosts, and those hosts require different levels of access, FortiNAC remains in the most restrictive state (Registration or Isolation) until all hosts on that port are authorized... Additionally, verify the Default VLAN setting for the port; if the Default VLAN and Registration VLAN match, the system will not trigger a VLAN change upon registration." - FortiNAC-F Administration Guide: Troubleshooting Host Management.

NEW QUESTION # 35

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 visibility
- B. Pooled licenses
- C. Global infrastructure device inventory
- D. Global version control
- E. Global authentication security policies

Answer: A,B,D

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.

While the Manager can assist with configuration templates, authentication security policies (C) and infrastructure modeling (A) are still predominantly managed at the local CA level to ensure site-specific logic and performance.

"The FortiNAC Manager provides a central management console for multiple FortiNAC-F servers (CAs). Key benefits include: * License Management: Licenses are pooled on the Manager and allocated to managed CAs as needed. * Software Management: Firmware updates can be centrally managed and pushed to all CAs from the Manager. * Centralized Monitoring: Provides a global view of all hosts, adapters, and events across the entire managed environment." - FortiNAC-F Manager Administration Guide: Overview and Benefits.

NEW QUESTION # 36

Refer to the exhibit.

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

- A. A security event
- B. A normal event
- C. A normal alarm
- D. A security alarm

Answer: B

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.

NEW QUESTION # 37

Refer to the exhibit.

An administrator has configured the DHCP scope for a registration isolation network, but the isolation process isn't working. What is the problem with the configuration?

- A. The gateway defined for the scope is incorrect.
- B. The label uses a system-reserved value.
- C. The lease pool does not contain a complete subnet.
- D. The domain name server designation is incorrect.

Answer: A

Explanation:

In a FortiNAC-F deployment, the configuration of the DHCP scope for isolation networks (Registration, Remediation, etc.) must

perfectly align with the underlying network infrastructure to ensure that isolated hosts can communicate with the FortiNAC appliance. In the provided exhibits, there is a clear discrepancy between the DHCP configuration and the Network Topology. As shown in the "Network Topology" exhibit, the Registration Network resides on a router interface (or sub-interface) with the IP address 192.168.180.1. This address represents the default gateway for any host placed into the Registration VLAN. However, the "DHCP configuration" exhibit shows the scope "REG-ScopeOne" configured with a Gateway of 10.0.1.254. This 10.0.1.254 address belongs to the management/service network (port2 of FortiNAC), not the registration subnet. If a host in the Registration VLAN receives this incorrect gateway via DHCP, it will attempt to send all off-link traffic to an unreachable IP, preventing it from loading the Captive Portal or communicating with the FortiNAC server.

According to the FortiNAC-F Configuration Wizard Reference, when defining a Layer 3 network scope, the "Gateway" field must contain the IP address of the router interface that acts as the gateway for that specific isolation VLAN. The FortiNAC appliance itself usually sits on a different subnet, and traffic is directed to it via the router's DHCP Relay (IP Helper) and DNS redirection. "When configuring scopes for a Layer 3 network, the Gateway value must be the IP address of the router interface for that subnet. This allows the host to reach its local gateway to route traffic. If the gateway is misconfigured, the host will be unable to reach the FortiNAC eth1/port2 interface for registration... Ensure the Gateway matches the network topology for the isolation VLAN." - FortiNAC-F Configuration Wizard Reference Manual: DHCP Scopes.

NEW QUESTION # 38

A healthcare organization is integrating FortiNAC-F with its existing MDM. Communication is failing between the systems. What could be a probable cause?

- A. REST API communication is failing
- B. Security Fabric traffic is failing
- C. SSH communication is failing
- D. SOAP API communication is failing

Answer: A

Explanation:

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.

While SSH (B) is used for switch CLI management and the Security Fabric (A) uses proprietary protocols for FortiGate synchronization, neither is the primary vehicle for MDM data exchange. SOAP API (D) is an older protocol that has been largely replaced by REST in modern FortiNAC integrations.

"FortiNAC integrates with MDM systems by utilizing REST API communication to query the MDM database for device information. To establish this link, administrators must configure the MDM Service Connector with the appropriate API URL and authentication credentials. If the 'Test Connection' fails, verify that the FortiNAC can reach the MDM provider via the REST API port (usually HTTPS 443)." - FortiNAC-F Administration Guide: MDM Integration and Troubleshooting.

NEW QUESTION # 39

.....

With the Fortinet NSE 5 - FortiNAC-F 7.6 Administrator (NSE5_FNC_AD_7.6) web-based practice exam, you get the same features as a NSE5_FNC_AD_7.6 desktop practice test software. It includes real Fortinet NSE5_FNC_AD_7.6 exam questions to help you understand each topic. The web-based NSE5_FNC_AD_7.6 Practice Exam is compatible with every operating system including Mac, Linux, iOS, Windows, and Android. This Fortinet NSE5_FNC_AD_7.6 practice exam works fine on Chrome, Internet Explorer, Microsoft Edge, Opera, etc.

NSE5_FNC_AD_7.6 New Test Bootcamp: https://www.pass4leader.com/Fortinet/NSE5_FNC_AD_7.6-exam.html

- High Pass-Rate Fortinet Latest NSE5_FNC_AD_7.6 Exam Pattern - NSE5_FNC_AD_7.6 Free Download Download ➔ NSE5_FNC_AD_7.6 for free by simply entering "www.vce4dumps.com" website Reliable NSE5_FNC_AD_7.6 Test Blueprint
- Useful and reliable NSE5_FNC_AD_7.6 training dumps - high-quality Fortinet NSE5_FNC_AD_7.6 training material

Go to website ➡ www.pdfvce.com □ open and search for (NSE5_FNC_AD_7.6) to download for free □
□NSE5_FNC_AD_7.6 Test Duration

- Demo NSE5_FNC_AD_7.6 Test □ Exam NSE5_FNC_AD_7.6 Success □ NSE5_FNC_AD_7.6 Study Center □
Easily obtain “NSE5_FNC_AD_7.6” for free download through 《 www.prepawaypdf.com 》 □Reliable
NSE5_FNC_AD_7.6 Exam Materials
- NSE5_FNC_AD_7.6 Study Questions - NSE5_FNC_AD_7.6 Free Demo - NSE5_FNC_AD_7.6 Valid Torrent □
Search for ➡ NSE5_FNC_AD_7.6 □ and download it for free immediately on ✓ www.pdfvce.com □✓ □ □Valid
NSE5_FNC_AD_7.6 Exam Answers
- Well-Prepared Latest NSE5_FNC_AD_7.6 Exam Pattern Spend Your Little Time and Energy to Pass
NSE5_FNC_AD_7.6 exam casually □ Immediately open ➡ www.troytecdumps.com □ and search for ⚡
NSE5_FNC_AD_7.6 □⚡□ to obtain a free download □Valid NSE5_FNC_AD_7.6 Exam Answers
- Reliable NSE5_FNC_AD_7.6 Exam Voucher □ Reliable NSE5_FNC_AD_7.6 Exam Voucher □
NSE5_FNC_AD_7.6 Passleader Review □ Download (NSE5_FNC_AD_7.6) for free by simply searching on ➡
www.pdfvce.com □ □New NSE5_FNC_AD_7.6 Exam Sample
- Useful and reliable NSE5_FNC_AD_7.6 training dumps - high-quality Fortinet NSE5_FNC_AD_7.6 training material □
Search for { NSE5_FNC_AD_7.6 } and obtain a free download on ▷ www.examcollectionpass.com □ □Valid
NSE5_FNC_AD_7.6 Exam Answers
- Well-Prepared Latest NSE5_FNC_AD_7.6 Exam Pattern Spend Your Little Time and Energy to Pass
NSE5_FNC_AD_7.6 exam casually □ Easily obtain ➡ NSE5_FNC_AD_7.6 □ for free download through ✓
www.pdfvce.com □✓ □ □Reliable NSE5_FNC_AD_7.6 Exam Materials
- NSE5_FNC_AD_7.6 Exam Dumps 100% Guarantee You Get NSE5_FNC_AD_7.6 Exam - www.prepawayexam.com □
□ Simply search for 【 NSE5_FNC_AD_7.6 】 for free download on 「 www.prepawayexam.com 」 □Reliable
NSE5_FNC_AD_7.6 Exam Voucher
- NSE5_FNC_AD_7.6 Quiz Torrent: Fortinet NSE 5 - FortiNAC-F 7.6 Administrator - NSE5_FNC_AD_7.6 Quiz
Braindumps - NSE5_FNC_AD_7.6 Study Guide □ Go to website (www.pdfvce.com) open and search for ⇒
NSE5_FNC_AD_7.6 ⇡ to download for free □Valid NSE5_FNC_AD_7.6 Exam Answers
- NSE5_FNC_AD_7.6 Exam Dumps 100% Guarantee You Get NSE5_FNC_AD_7.6 Exam - www.troytecdumps.com □
Open website ➡ www.troytecdumps.com □ and search for ➤ NSE5_FNC_AD_7.6 □ for free download ~~Demo
NSE5_FNC_AD_7.6 Test
- www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt,
myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt,
myportal.utt.edu.tt, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw,
www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, Disposable vapes