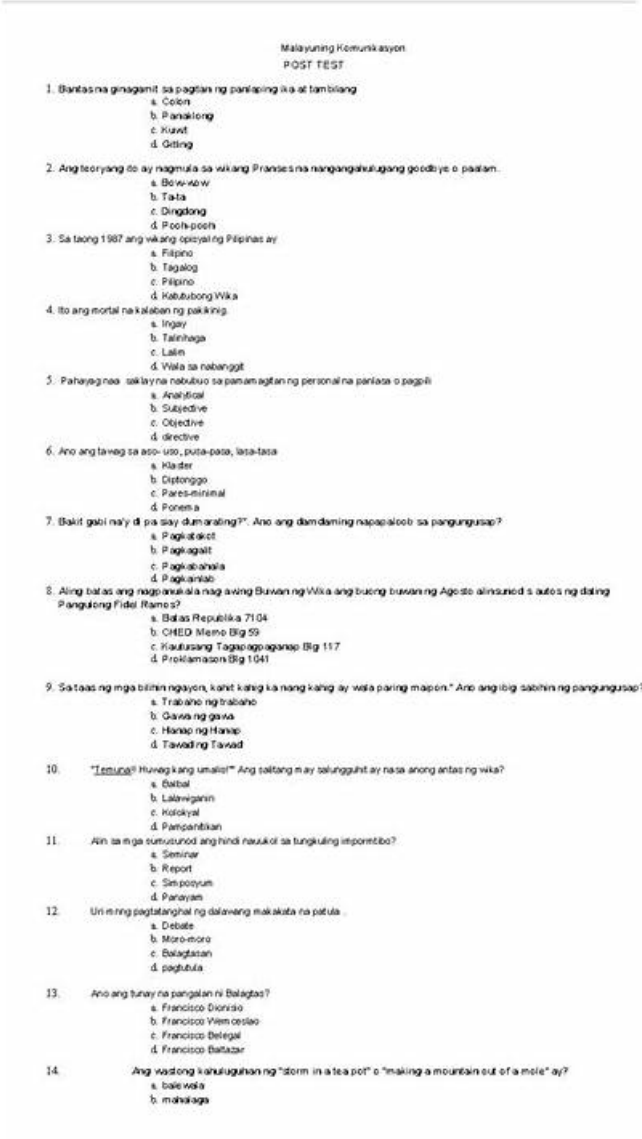
NSE5_FNC_AD_7.6 New Practice Materials & New NSE5_FNC_AD_7.6 Braindumps Questions



Malayuning Komunikasyon
POST TEST

1. Bantas na ginagamit sa pagtlan ng panlaping ika-at tambilang
   a. Colon
   b. Panaklong
   c. Kuwit
   d. Gitling
2. Ang teoryang ito ay nagmula sa wikang Pranses na nangangahulugang goodbye o paalam.
   a. Bow-wow
   b. Tata
   c. Dingdong
   d. Pooh-pooh
3. Sa taong 1987 ang wikang opisyal ng Pilipinas ay
   a. Filipino
   b. Tagalog
   c. Pilipino
   d. Kabutubong Wika
4. Ito ang mortal na kalaban ng pakikinig.
   a. Ingay
   b. Talinhaga
   c. Lalin
   d. Wala sa nabanggit
5. Pahayag nao saklaylna nabubuo sa pamamagitan ng personal na paniasa o pagpili
   a. Analytical
   b. Subjective
   c. Objective
   d. directive
6. Ano ang tawag sa aso- uso, puta-pasa, lasa-tasa
   a. Klaster
   b. Diptonggo
   c. Pares-minimal
   d. Ponema
7. Bakit gabi naiy di pa siay dumarating?". Ano ang damdaming napapaloob sa pangungusap?
   a. Pagkabalisit
   b. Pagkagalit
   c. Pagkabahala
   d. Pagkainlab
8. Aling batas ang nagpanukala nag awing Buwan ng Wika ang buong buwan ng Agosto alinsunod s autos ng dating Pangulong Fidel Ramos?
   a. Batas Republika 7104
   b. CHED Memo Blg 59
   c. Kautusang Tagapagpaganap Blg 117
   d. Proklamasion Blg 1041
9. Sa taas ng mga bilihin ngayon, kahit kahig ka nang kahig ay wala paring mapon." Ano ang ibig sabihin ng pangungusap?
   a. Trabaho ng trabaho
   b. Gawa ng gawa
   c. Hanap ng Hanap
   d. Tawad ng Tawad
10. "Tenuna!! Huwag kang umalis!" Ang salitang may salungguhit ay nasa anong antas ng wika?
    a. Balbal
    b. Lalawiganin
    c. Kolokyal
    d. Pampanitikan
11. Alin sa mga sumusunod ang hindi nauukol sa tungkuling impormtibo?
    a. Seminar
    b. Report
    c. Simposyum
    d. Panayam
12. Uri ning pagtatanghal ng dalawang makakata na patula.
    a. Debate
    b. Moro-moro
    c. Balagtasan
    d. pagtutula
13. Ano ang tunay na pangalan ni Balagtas?
    a. Francisco Dionisio
    b. Francisco Wenceslao
    c. Francisco Belegal
    d. Francisco Baltazar
14. Ang wastong kahuluganan ng "storm in a tea pot" o "making a mountain out of a mole" ay?
    a. bale wala
    b. mahalaga

There are more and more people to try their best to pass the NSE5_FNC_AD_7.6 exam, including many college students, a lot of workers, and even many housewives and so on. These people who want to pass the NSE5_FNC_AD_7.6 exam have regard the exam as the only one chance to improve themselves and make enormous progress. So they hope that they can be devoting all of their time to preparing for the NSE5_FNC_AD_7.6 Exam, but it is very obvious that a lot of people have not enough time to prepare for the important NSE5_FNC_AD_7.6 exam. Our NSE5_FNC_AD_7.6 exam questions can help you pass the NSE5_FNC_AD_7.6 exam with least time and energy.

Fortinet NSE5_FNC_AD_7.6 Exam Syllabus Topics:

Topic	Details
Topic 1	• 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.

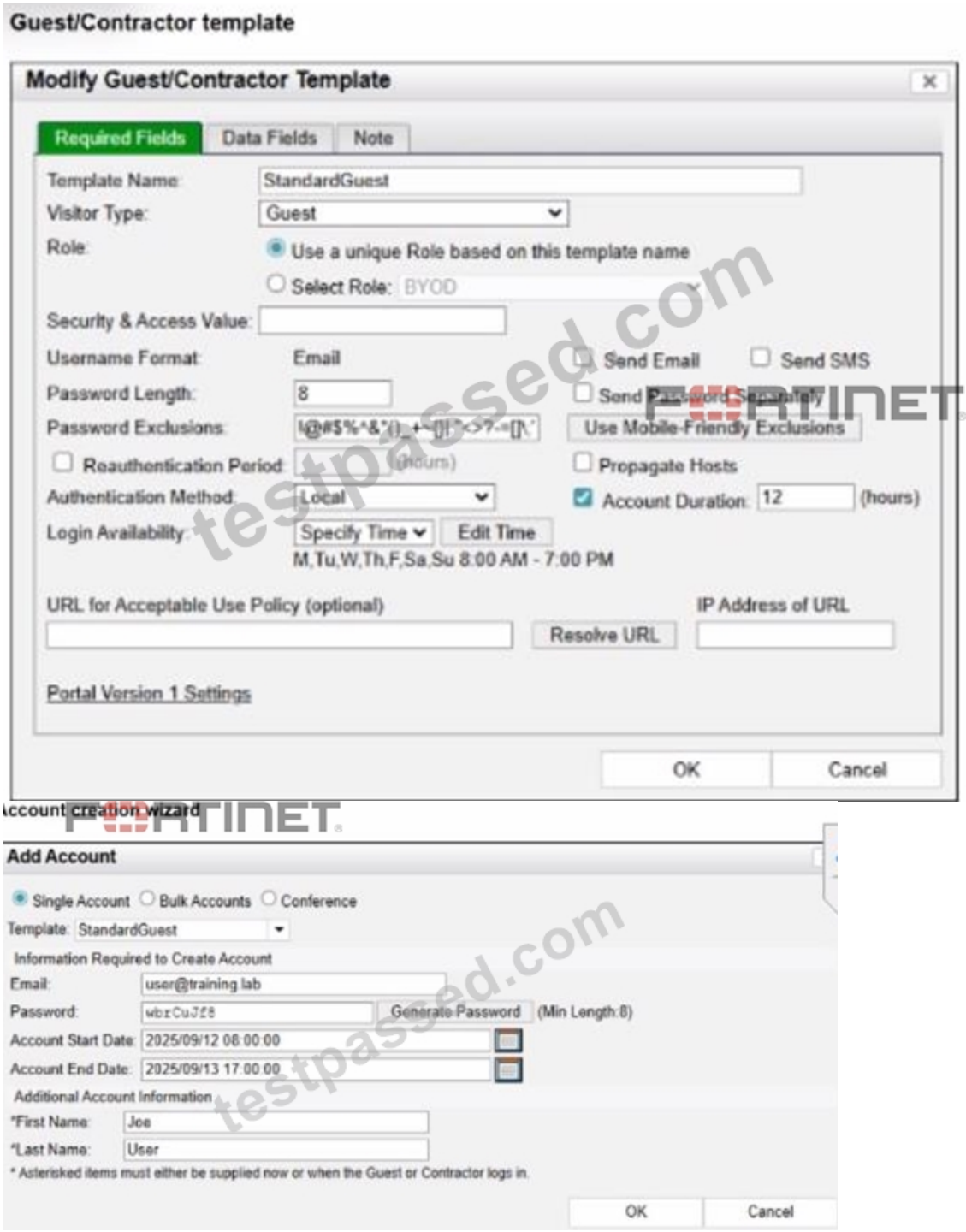
Topic 2	• Deployment and Provisioning: This domain focuses on configuring security automation for automatic event responses, implementing access control policies, setting up high availability for system redundancy, and creating security policies to enforce network security requirements.
Topic 3	• Integration: 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	• 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.

Pass Guaranteed 2026 NSE5_FNC_AD_7.6: Professional Fortinet NSE 5 - FortiNAC-F 7.6 Administrator New Practice Materials

With our NSE5_FNC_AD_7.6 exam questions, you can pass the exam with 100% success guaranteed. More importantly, if you purchase our NSE5_FNC_AD_7.6 practice materials, we believe that your life will get better and better. So why still hesitate? Act now, join us, and buy our study materials. You will feel very happy that you will be about to change well because of our NSE5_FNC_AD_7.6 Study Guide. Now you can go to free download the demos to check the content and function. It is easy and convenient.

Fortinet NSE 5 - FortiNAC-F 7.6 Administrator Sample Questions (Q31-Q36):

NEW QUESTION # 31
Refer to the exhibits.



Based on the given configurations and settings, on which date and time would a guest account created at 8:00 AM on 2025/09/12 expire?

- A. 2025/09/13 at 17:00:00
- B. 2025/09/12 at 7:00 PM
- C. 2025/09/12 at 17:00:00
- D. 2025/09/12 at 8:00 PM

Answer: A

Explanation:
Questio ns no: 22
Verified Answe r: D
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 expiration of a guest or contractor account is determined by the configuration settings within the Account Creation Wizard and the associated Guest/Contractor Template. While a template can define a default "Account Duration" (as seen

in the 12-hour setting in the second exhibit), the Account Creation Wizard allows an administrator to manually specify or override the start and end parameters for a specific user session.
According to the FortiNAC-F Administration Guide regarding guest management, the Account End Date field in the creation wizard is the definitive timestamp for when the account object will be disabled or deleted from the system. In the provided exhibit (Account Creation Wizard), the administrator has explicitly set the Account Start Date to 2025/09/12 08:00:00 and the Account End Date to 2025/09/13 17:00:00.
Even though the template indicates an "Account Duration" of 12 hours, this value typically serves as a pre-populated default. When a manual date and time are entered into the wizard, those specific values take precedence for that individual account. The account will remain active and valid until 5:00 PM (17:00:00) on the following day, 2025/09/13. It is also important to note the "Login Availability" from the template (8:00 AM - 7:00 PM); while the account exists until the 13th at 17:00:00, the user would only be able to authenticate during the active hours defined by the login schedule on both days.
"When creating an account, the administrator can select a template to provide default settings. However, specific values such as the Account End Date can be modified within the Account Creation Wizard. The date and time specified in the 'Account End Date' field determines the absolute expiration of the account. Once this time is reached, the account is moved to an expired state and the user's network access is revoked." - FortiNAC-F Administration Guide: Guest and Contractor Account Management.

NEW QUESTION # 32
Where should you configure MAC notification traps on a supported switch?

- A. On all ports on the switch
- B. Only on ports defined as learned uplinks
- C. On all ports except uplink ports
- D. Only on ports that generate linkup and linkdown traps

Answer: C

Explanation:
In FortiNAC-F, MAC notification traps (also known as MAC Move or MAC Change traps) are essential for achieving real-time visibility of endpoint connections and disconnections. When a device connects to a switch port, the switch generates an SNMP trap that informs FortiNAC-F of the new MAC address on that specific interface. This allows FortiNAC-F to immediately initiate the profiling and policy evaluation process without waiting for the next scheduled L2 poll.
According to the FortiNAC-F Administration Guide and Switch Integration documentation, MAC notification traps should be configured on all ports except uplink ports. Uplink ports are the interfaces that connect one switch to another or to the core network. Because these ports see the MAC addresses of every device on the downstream switches, enabling MAC notification on uplinks would cause the switch to send a massive volume of redundant traps to FortiNAC-F every time any device anywhere in the downstream branch moves or reconnects. This can overwhelm the FortiNAC-F process queue and degrade system performance.
By only enabling these traps on "edge" or "access" ports-where individual endpoints like PCs, printers, and VoIP phones connect-FortiNAC-F receives precise data regarding exactly where a device is physically located. Uplinks should be identified in the FortiNAC-F inventory as "Uplink" or "Learned Uplink," which tells the system to ignore MAC data seen on those specific ports.
"To ensure accurate host tracking and optimal system performance, SNMP MAC notification traps must be enabled on all access (downlink) ports. Do not enable MAC notification traps on uplink ports, as this will result in excessive and unnecessary trap processing. Uplink ports should be excluded to prevent the system from attempting to map multiple downstream MAC addresses to a single infrastructure interface." - FortiNAC-F Administration Guide: SNMP Configuration for Network Devices.

NEW QUESTION # 33
While discovering network infrastructure devices, a switch appears in the inventory topology with a question mark (?) on the icon. What would cause this?

- A. SNMP is not enabled on the switch.
- B. The SNMP ObjectID is not recognized by FortiNAC-F.
- C. The wrong SNMP community string was entered during discovery.
- D. A read-only SNMP community siring was used.

Answer: B

Explanation:
In FortiNAC-F, the Inventory topology uses specific icons to represent the status and model of discovered network infrastructure. When a switch or other network device is discovered via SNMP, FortiNAC-F retrieves its System ObjectID (sysObjectID) to identify the specific make and model. This OID is then compared against the internal database of supported device mappings.

A question mark (?) icon appearing on a discovered switch indicates that while the discovery process successfully communicated with the device (meaning SNMP credentials were correct), the SNMP ObjectID is not recognized or mapped in the current version of FortiNAC-F. This essentially means the device is "unsupported" by the current software out-of-the-box. Because the OID is unknown, FortiNAC-F does not know which CLI or SNMP command set to use for critical functions like L2 polling (host visibility) or VLAN switching (enforcement). To resolve this, an administrator can manually "Set Device Mapping" to a similar existing model or a "Generic SNMP Device" if only basic L3 visibility is required.
"Discovered devices displaying a '?' icon indicate the currently running version does not have a mapping for that device's System OID (device is not supported). Device mappings are used to manage the device by performing functions such as L2/L3 Polling, Reading, and Switching VLANs." - Fortinet Technical Tip: Options for devices unable to be modeled in Inventory.

NEW QUESTION # 34
While discovering network infrastructure devices, a switch appears in the inventory topology with a question mark (?) on the icon. What would cause this?

- A. SNMP is not enabled on the switch.
- B. The SNMP ObjectlD is not recognized by FortiNAC-F.
- C. The wrong SNMP community string was entered during discovery.
- D. A read-only SNMP community siring was used.

Answer: B

Explanation:
In FortiNAC-F, the Inventory topology uses specific icons to represent the status and model of discovered network infrastructure. When a switch or other network device is discovered via SNMP, FortiNAC-F retrieves its System ObjectID (sysObjectID) to identify the specific make and model. This OID is then compared against the internal database of supported device mappings.
A question mark (?) icon appearing on a discovered switch indicates that while the discovery process successfully communicated with the device (meaning SNMP credentials were correct), the SNMP ObjectID is not recognized or mapped in the current version of FortiNAC-F. This essentially means the device is "unsupported" by the current software out-of-the-box. Because the OID is unknown, FortiNAC-F does not know which CLI or SNMP command set to use for critical functions like L2 polling (host visibility) or VLAN switching (enforcement). To resolve this, an administrator can manually "Set Device Mapping" to a similar existing model or a "Generic SNMP Device" if only basic L3 visibility is required.
"Discovered devices displaying a '?' icon indicate the currently running version does not have a mapping for that device's System OID (device is not supported). Device mappings are used to manage the device by performing functions such as L2/L3 Polling, Reading, and Switching VLANs." - Fortinet Technical Tip: Options for devices unable to be modeled in Inventory.

NEW QUESTION # 35
When creating a user or host profile, which three criteria can you apply? (Choose three.)

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

Answer: C,D,E

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.
Criteria like an "applied access policy" (D) are the outcome of a profile match rather than a criterion used to define the profile itself.

Similarly, the "Adapter current VLAN" (C) is a dynamic state that changes based on enforcement and is not a standard static identifier used for profile matching.
"User/Host Profiles are used to identify the hosts and users to which a policy will apply. Profiles are created by selecting various criteria in the Who/What (Attributes and Groups) and Where (Locations) sections. Attributes can include Host Role, User Role, and OS. Group memberships allow matching based on internal or directory-based groups. Location criteria allow for filtering based on the device or port where the host is connected." - FortiNAC-F Administration Guide: User/Host Profile Configuration.

NEW QUESTION # 36
.....

The NSE5_FNC_AD_7.6 mock tests are specially built for you to evaluate what you have studied. These Fortinet NSE 5 - FortiNAC-F 7.6 Administrator (NSE5_FNC_AD_7.6) practice exams (desktop and web-based) are customizable, which means that you can change the time and questions according to your needs. Our NSE5_FNC_AD_7.6 Practice Tests teach you time management so you can pass the Fortinet NSE 5 - FortiNAC-F 7.6 Administrator (NSE5_FNC_AD_7.6) certification exam.