Exam Questions JN0-231

Security - Associate (JNCIA-SEC)

https://www.2passeasy.com/dumps/JN0-231/

NEW QUESTION 1
Which two statements are correct about functional zones? (Choose two.)

A. Functional zones must have a user-defined name.
B. Functional zone cannot be referenced in security policies or pass transit traffic.
C. Multiple types of functional zones can be defined by the user.
D. Functional zones are used for out-of-band device management.

Answer: BD

NEW QUESTION 2
You want to block executable files ("exe) from being downloaded onto your network. Which UTM feature would you use in this scenario?

A. IPS
B. Web filtering
C. content filtering
D. antivirus

Answer: B

Explanation:
According to the Juniper Networks official JNCIA-SEC Exam Guide, web filtering is a feature used to control access to web content, including the ability to block specific types of files.
In the scenario mentioned, you want to block executable files from being downloaded, which can be accomplished by using web filtering. The feature allows administrators to configure policies that block specific file types, including "exe" files, from being downloaded.

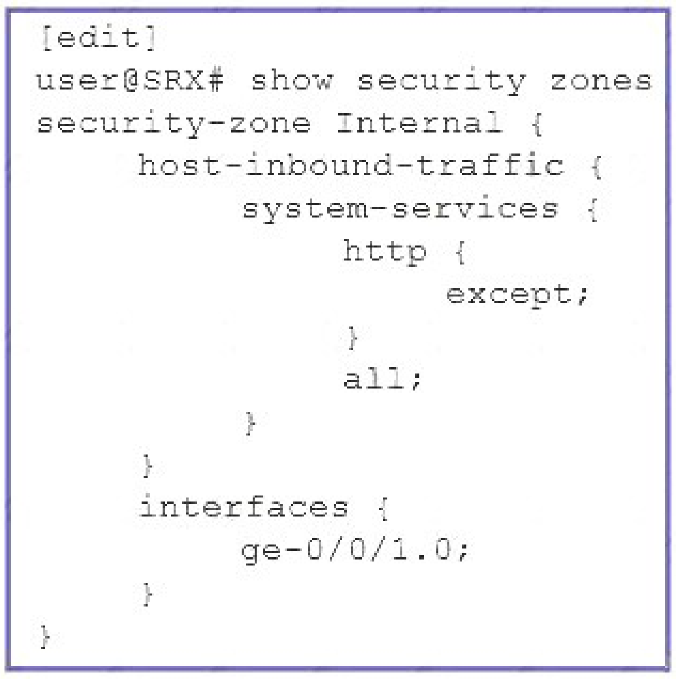
NEW QUESTION 3
Which three Web filtering deployment actions are supported by Junos? (Choose three.)

A. Use IPS.
B. Use local lists.
C. Use remote lists.
D. Use Websense Redirect.
E. Use Juniper Enhanced Web Filtering.

Answer: BDE

Explanation:
https://www.juniper.net/documentation/us/en/software/junos/utm/topics/concept/utm-web-filtering-overview.ht

NEW QUESTION 4
Click the Exhibit button.



```
[edit]
user@SRX# show security zones
security-zone Internal {
     host-inbound-traffic {
          system-services {
               http {
                    except;
               }
               all;
          }
     }
     interfaces {
          ge-0/0/1.0;
     }
}
```

What is the purpose of the host-inbound-traffic configuration shown in the exhibit?

A. to permit host inbound HTTP traffic and deny all other traffic on the internal security zone
B. to deny and log all host inbound traffic on the internal security zone, except for HTTP traffic
C. to permit all host inbound traffic on the internal security zone, but deny HTTP traffic
D. to permit host inbound HTTP traffic on the internal security zone

Answer: C

NEW QUESTION 5
Which Juniper Networks solution uses static and dynamic analysis to search for day-zero malware threats?

A. firewall filters
B. UTM
C. Juniper ATP Cloud

D. IPS

Answer: C

Explanation:
Malware Sandboxing
Detect and stop zero-day and commodity malware within web, email, data center, and application traffic targeted for Windows, Mac, and IoT devices. https://www.juniper.net/us/en/products/security/advanced-threat-prevention.html

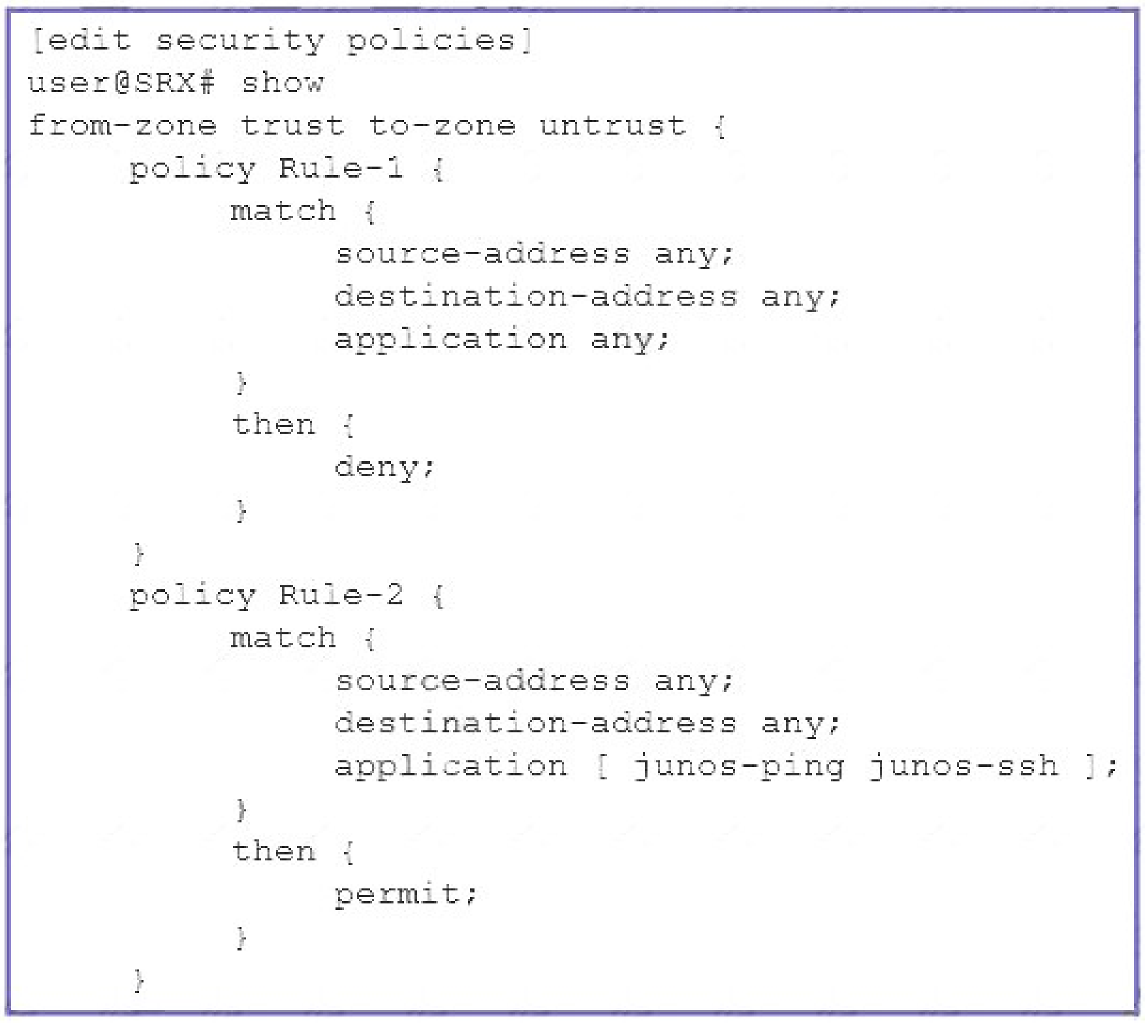
NEW QUESTION 6
What is the default value of the dead peer detection (DPD) interval for an IPsec VPN tunnel?

A. 20 seconds
B. 5 seconds
C. 10 seconds
D. 40 seconds

Answer: B

Explanation:
The default value of the dead peer detection (DPD) interval for an IPsec VPN tunnel is 5 seconds. DPD is a mechanism that enables the IPsec device to detect if the peer is still reachable or if the IPsec VPN tunnel is still active. The DPD interval determines how often the IPsec device sends DPD packets to the peer to check the status of the VPN tunnel. A value of 5 seconds is a common default, but the specific value can vary depending on the IPsec device and its configuration.

NEW QUESTION 7
Click the Exhibit button.



```
[edit security policies]
user@SRX# show
from-zone trust to-zone untrust {
    policy Rule-1 {
        match {
            source-address any;
            destination-address any;
            application any;
        }
        then {
            deny;
        }
    }
    policy Rule-2 {
        match {
            source-address any;
            destination-address any;
            application [ junos-ping junos-ssh ];
        }
        then {
            permit;
        }
    }
```

You are asked to allow only ping and SSH access to the security policies shown in the exhibit. Which statement will accomplish this task?

A. Rename policy Rule-2 to policy Rule-0.
B. Insert policy Rule-2 before policy Rule-1.
C. Replace application any with application [junos-ping junos-ssh] in policy Rule-1.
D. Rename policy Rule-1 to policy Rule-3.

Answer: B

NEW QUESTION 8
Which two statements about the Junos OS CLI are correct? (Choose two.)

A. The default configuration requires you to log in as the admin user.
B. A factory-default login assigns the hostname Amnesiac to the device.
C. Most Juniper devices identify the root login prompt using the % character.
D. Most Juniper devices identify the root login prompt using the > character.

Answer: AD

Explanation:
The two correct statements about the Junos OS CLI are that the default configuration requires you to log in as the admin user, and that most Juniper devices identify the root login prompt using the > character. The factory-default login assigns the hostname "juniper" to the device and the root login prompt is usually identified with the % character. More information about the Junos OS CLI can be found in the Juniper Networks technical documentation here:https://www.juniper.net/documentation/en_US/junos/topics/reference/command-summary/cli-overview.htm

NEW QUESTION 9
Which two components are configured for host inbound traffic? (Choose two.)

A. zone
B. logical interface
C. physical interface
D. routing instance

Answer: AB

NEW QUESTION 10
What does the number ‘‘2’’ indicate in interface ge—0/1/2?

A. The interface logical number
B. The physical interface card (PIC)
C. The port number
D. The flexible PIC concentrator (FPC)

Answer: C

NEW QUESTION 10
Which statement about service objects is correct?

A. All applications are predefined by Junos.
B. All applications are custom defined by the administrator.
C. All applications are either custom or Junos defined.
D. All applications in service objects are not available on the vSRX Series device.

Answer: C

Explanation:
"Service objects represent applications and services that can be assigned to a security policy rule. Applications and services can either be predefined by Junos software or custom defined by the administrator."

NEW QUESTION 11
You need to collect the serial number of an SRX Series device to replace it. Which command will accomplish this task?

A. show chassis hardware
B. show system information
C. show chassis firmware
D. show chassis environment

Answer: A

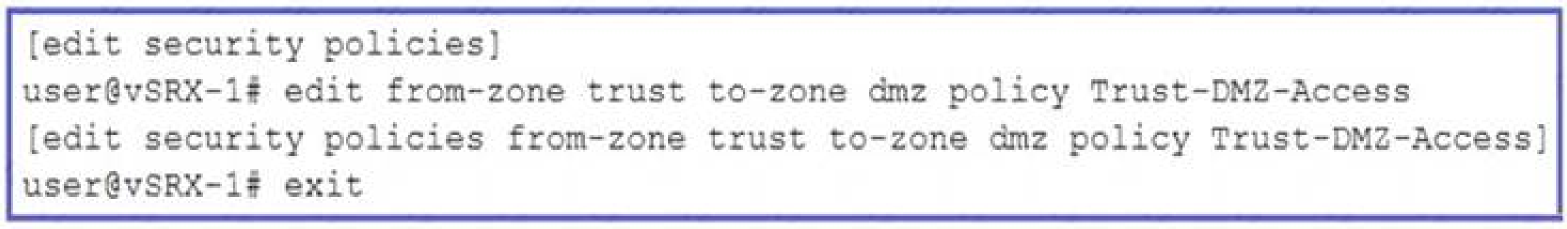
Explanation:
The correct command to collect the serial number of an SRX Series device is the show chassis hardware command [1]. This command will return the serial number of the device, along with other information about the device such as the model number, part number, and version.
This command is available in Junos OS. More information about the show chassis hardware command can be found in the Juniper Networks technical documentation here [1]: https://www.juniper.net/documentation/en_US/junos/topics/reference/command-summary/show-chassis-hardwa

NEW QUESTION 12
What information does the show chassis routing-engine command provide?

A. chassis serial number
B. resource utilization
C. system version
D. routing tables

Answer: B

NEW QUESTION 15
Click the Exhibit button.



```
[edit security policies]
user@vSRX-1# edit from-zone trust to-zone dmz policy Trust-DMZ-Access
[edit security policies from-zone trust to-zone dmz policy Trust-DMZ-Access]
user@vSRX-1# exit
```

Referring to the exhibit, a user is placed in which hierarchy when the exit command is run?

A. [edit security policies from-zone trust to-zone dmz] user@vSRX-1#
B. [edit] user@vSRX-1#
C. [edit security policies] user@vSRX-1#
D. user@vSRX-1>

Answer: A

NEW QUESTION 20
Which statement is correct about Web filtering?

A. The Juniper Enhanced Web Filtering solution requires a locally managed server.
B. The decision to permit or deny is based on the body content of an HTTP packet.
C. The decision to permit or deny is based on the category to which a URL belongs.
D. The client can receive an e-mail notification when traffic is blocked.

Answer: C

Explanation:
Web filtering is a feature that allows administrators to control access to websites by categorizing URLs into different categories such as gambling, social networking, or adult content. The decision to permit or deny access to a website is based on the category to which a URL belongs. This is done by comparing the URL against a database of categorized websites and making a decision based on the policy defined by the administrator.

NEW QUESTION 25
You are monitoring an SRX Series device that has the factory-default configuration applied. In this scenario, where are log messages sent by default?

A. Junos Space Log Director
B. Junos Space Security Director
C. to a local syslog server on the management network
D. to a local log file named messages

Answer: C

NEW QUESTION 26
What must be enabled on an SRX Series device for the reporting engine to create reports?

A. System logging
B. SNMP
C. Packet capture
D. Security logging

Answer: D

NEW QUESTION 28
Which statement is correct about unified security policies on an SRX Series device?

A. A zone-based policy is always evaluated first.
B. The most restrictive policy is applied regardless of the policy level.
C. A global policy is always evaluated first.
D. The first policy rule is applied regardless of the policy level.

Answer: A

NEW QUESTION 29
Which two non-configurable zones exist by default on an SRX Series device? (Choose two.)

A. Junos-host
B. functional
C. null
D. management

Answer: AC

Explanation:
Junos-host and null are two non-configurable zones that exist by default on an SRX Series device. Junos-host is the default zone for all internal interfaces and services, such as management and other loopback interfaces. The null zone is used to accept all traffic that is not explicitly accepted by other security policies, and is the default zone for all unclassified traffic. Both zones cannot be modified or deleted.
References:
https://www.juniper.net/documentation/en_US/junos/topics/task/configuration/security-zones-overview.html
https://www.juniper.net/documentation/en_US/junos/topics/reference/configuration-statement/security-zones-de

NEW QUESTION 31
Which two UTM features should be used for tracking productivity and corporate user behavior? (Choose two.)

A. the content filtering UTM feature
B. the antivirus UTM feature
C. the Web filtering UTM feature
D. the antispam UTM feature

Answer: AC

NEW QUESTION 33
What is the default timeout value for TCP sessions on an SRX Series device?

A. 30 seconds
B. 60 minutes
C. 60 seconds
D. 30 minutes

Answer: D

Explanation:
By default, TCP has a 30-minute idle timeout, and UDP has a 60-second idle timeout. Additionally, known IP protocols have a 30-minute timeout, whereas unknown ones have a 60-second timeout. Setting the inactivity timeout is very useful, particularly if you are concerned about applications either timing out or remaining idle for too long and filling up the session table. According to the Juniper SRX Series Services Guide, this can be configured using the 'timeout inactive' statement for the security policy.

NEW QUESTION 37
What are two functions of Juniper ATP Cloud? (Choose two.)

A. malware inspection
B. Web content filtering
C. DDoS protection
D. Geo IP feeds

Answer: AD

Explanation:
Juniper Advanced Threat Prevention (ATP) Cloud is a security service that helps organizations protect against advanced threats by providing real-time threat intelligence and automated response capabilities. It combines a cloud-based threat intelligence platform with the security capabilities of Juniper Networks security devices to provide comprehensive protection against advanced threats. The two functions of Juniper ATP Cloud include malware inspection and Geo IP feeds. The malware inspection component provides real-time protection against known and unknown threats by analyzing suspicious files and determining if they are malicious. The Geo IP feeds provide a global view of IP addresses and their associated countries, allowing organizations to identify and block traffic from known malicious countries.

NEW QUESTION 42
What is the order in which malware is detected and analyzed?

A. antivirus scanning –> cache lookup –> dynamic analysis –> static analysis
B. cache lookup –> antivirus scanning –> static analysis –> dynamic analysis
C. antivirus scanning –> cache lookup –> static analysis –> dynamic analysis
D. cache lookup –> static analysis –> dynamic analysis –> antivirus scanning

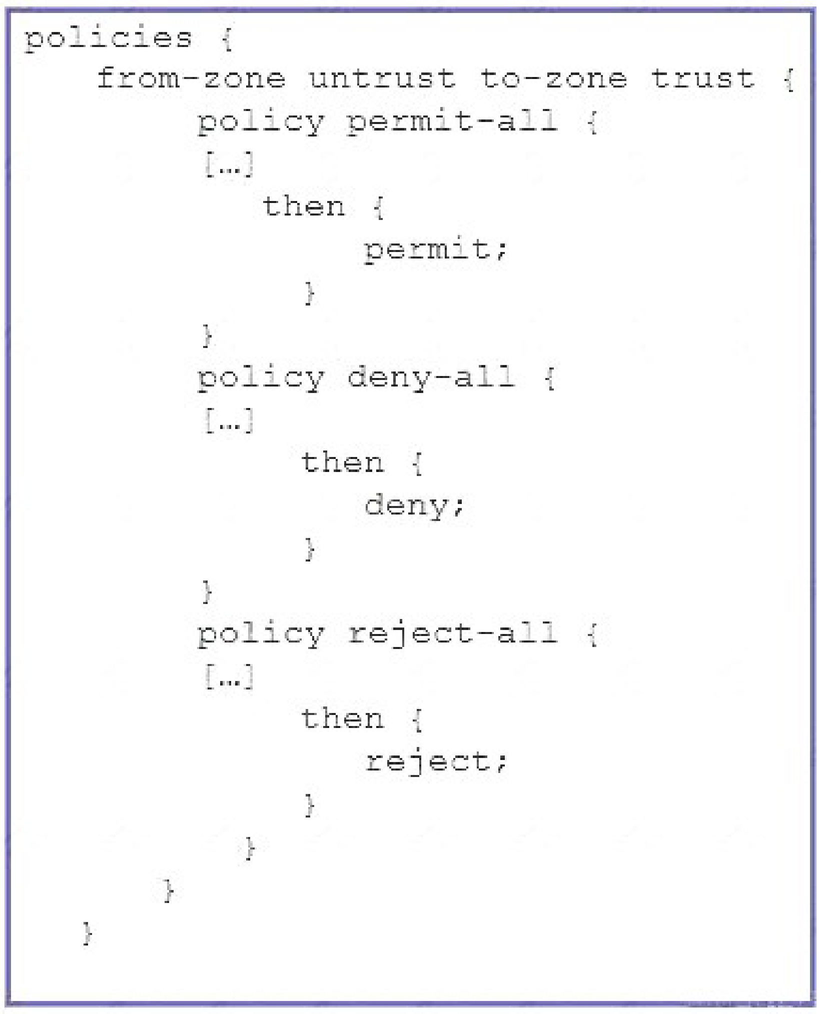
Answer: B

NEW QUESTION 46
Which statement is correct about global security policies on SRX Series devices?

A. The to-zone any command configures a global policy.
B. The from-zone any command configures a global policy.
C. Global policies are always evaluated first.
D. Global policies can include zone context.

Answer: D

NEW QUESTION 47
Click the Exhibit button.



```
policies {
   from-zone untrust to-zone trust {
        policy permit-all {
        [...]
           then {
                permit;
             }
        }
        policy deny-all {
        [...]
             then {
                deny;
             }
        }
        policy reject-all {
        [...]
             then {
                reject;
             }
          }
      }
  }
```

Which two statements are correct about the partial policies shown in the exhibit? (Choose two.)

A. UDP traffic matched by the deny-all policy will be silently dropped.
B. TCP traffic matched by the reject-all policy will have a TCP RST sent.
C. TCP traffic matched from the zone trust is allowed by the permit-all policy.
D. UDP traffic matched by the reject-all policy will be silently dropped.

Answer: AB

NEW QUESTION 48
You are configuring an SRX Series device. You have a set of servers inside your private network that need one-to-one mappings to public IP addresses. Which NAT configuration is appropriate in this scenario?

A. source NAT with PAT
B. destination NAT
C. NAT-T
D. static NAT

Answer: D

Explanation:
https://www.juniper.net/documentation/en_US/day-one-books/nat-and-pat-en.html
And the specific text that would support the above answer is as follows: "Static NAT, which requires manual configuration, is often the most appropriate configuration for mapping one internal address to one external address."

NEW QUESTION 53
Which two traffic types are considered exception traffic and require some form of special handling by the PFE? (Choose two.)

A. SSH sessions
B. ICMP reply messages
C. HTTP sessions
D. traceroute packets

Answer: BD

NEW QUESTION 55
Screens on an SRX Series device protect against which two types of threats? (Choose two.)

A. IP spoofing
B. ICMP flooding
C. zero-day outbreaks
D. malicious e-mail attachments

Answer: AB

Explanation:
ICMP flood
Use the ICMP flood IDS option to protect against ICMP flood attacks. An ICMP flood attack typically occurs when ICMP echo requests use all resources in responding, such that valid network traffic can no longer be processed.
The threshold value defines the number of ICMP packets per second (pps) allowed to be send to the same destination address before the device rejects further

ICMP packets.
IP spoofing
Use the IP address spoofing IDS option to prevent spoofing attacks. IP spoofing occurs when an invalid source address is inserted in the packet header to make the packet appear to come from a trusted source.
https://www.juniper.net/documentation/us/en/software/junos/denial-of-service/topics/topic-map/security-introdu

NEW QUESTION 57
What are two valid address books? (Choose two.)

A. 66.129.239.128/25
B. 66.129.239.154/24
C. 66.129.239.0/24
D. 66.129.239.50/25

Answer: AC

Explanation:
Network Prefixes in Address Books
You can specify addresses as network prefixes in the prefix/length format. For example, 203.0.113.0/24 is an acceptable address book address because it translates to a network prefix. However, 203.0.113.4/24 is not acceptable for an address book because it exceeds the subnet length of 24 bits. Everything beyond the subnet length must be entered as 0 (zero). In special scenarios, you can enter a hostname because it can use the full 32-bit address length.
https://www.juniper.net/documentation/us/en/software/junos/security-policies/topics/topic-map/security-address

NEW QUESTION 60
Which two statements are correct about IPsec security associations? (Choose two.)

A. IPsec security associations are bidirectional.
B. IPsec security associations are unidirectional.
C. IPsec security associations are established during IKE Phase 1 negotiations.
D. IPsec security associations are established during IKE Phase 2 negotiations.

Answer: AD

Explanation:
The two statements that are correct about IPsec security associations are that they are bidirectional and that they are established during IKE Phase 2 negotiations. IPsec security associations are bidirectional, meaning that they provide security for both incoming and outgoing traffic. IPsec security associations are established during IKE Phase 2 negotiations, which negotiates the security parameters and establishes the security association between the two peers. For more information, please refer to the Juniper Networks IPsec VPN Configuration Guide, which can be found on Juniper's website.

NEW QUESTION 65
Which two components are part of a security zone? (Choose two.)

A. inet.0
B. fxp0
C. address book
D. ge-0/0/0.0

Answer: BD

NEW QUESTION 69
Which two statements are correct about IKE security associations? (Choose two.)

A. IKE security associations are established during IKE Phase 1 negotiations.
B. IKE security associations are unidirectional.
C. IKE security associations are established during IKE Phase 2 negotiations.
D. IKE security associations are bidirectional.

Answer: AD

NEW QUESTION 74
When are Unified Threat Management services performed in a packet flow?

A. before security policies are evaluated
B. as the packet enters an SRX Series device
C. only during the first path process
D. after network address translation

Answer: D

Explanation:
https://iosonounrouter.wordpress.com/2018/07/07/how-does-a-flow-based-srx-work/

NEW QUESTION 78
In J-Web. the management and loopback address configuration option allows you to configure which area?

A. the IP address of the primary Gigabit Ethernet port

B. the IP address of the Network Time Protocol server
C. the CIDR address
D. the IP address of the device management port

Answer: D

Explanation:
J-W eb is a web-based interface for configuring and managing Juniper devices. The management and loopback address configuration option in J-Web allows you to configure the IP address of the device management port, which is used to remotely access and manage the device.

NEW QUESTION 80
......