Juniper

Exam Questions JN0-231

Security - Associate (JNCIA-SEC)

NEW QUESTION 1
What are three Junos UTM features? (Choose three.)

A. screens
B. antivirus
C. Web filtering
D. IDP/IPS
E. content filtering

Answer: BCE

NEW QUESTION 2
What are two Juniper ATP Cloud feed analysis components? (Choose two.)

A. IDP signature feed
B. C&C cloud feed
C. infected host cloud feed
D. US CERT threat feed

Answer: AB

Explanation:
The Juniper ATP Cloud feed analysis components are the IDP signature feed and the C&C cloud feed. The IDP signature feed provides a database of signatures from known malicious traffic, while the C&C cloud feed provides the IP addresses of known command and control servers. The infected host cloud feed and US CERT threat feed are not components of the Juniper ATP Cloud feed analysis.
To learn more about the Juniper ATP Cloud feed analysis components, refer to the Juniper Networks Security Automation and Orchestration (SAO) official documentation, which can be found at https://www.juniper.net/documentation/en_US/sao/topics/concept/security-automation-and-orchestration-overvi
The documentation provides an overview of the SAO platform and an in-depth look at the various components of the Juniper ATP Cloud feed analysis.

NEW QUESTION 3
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

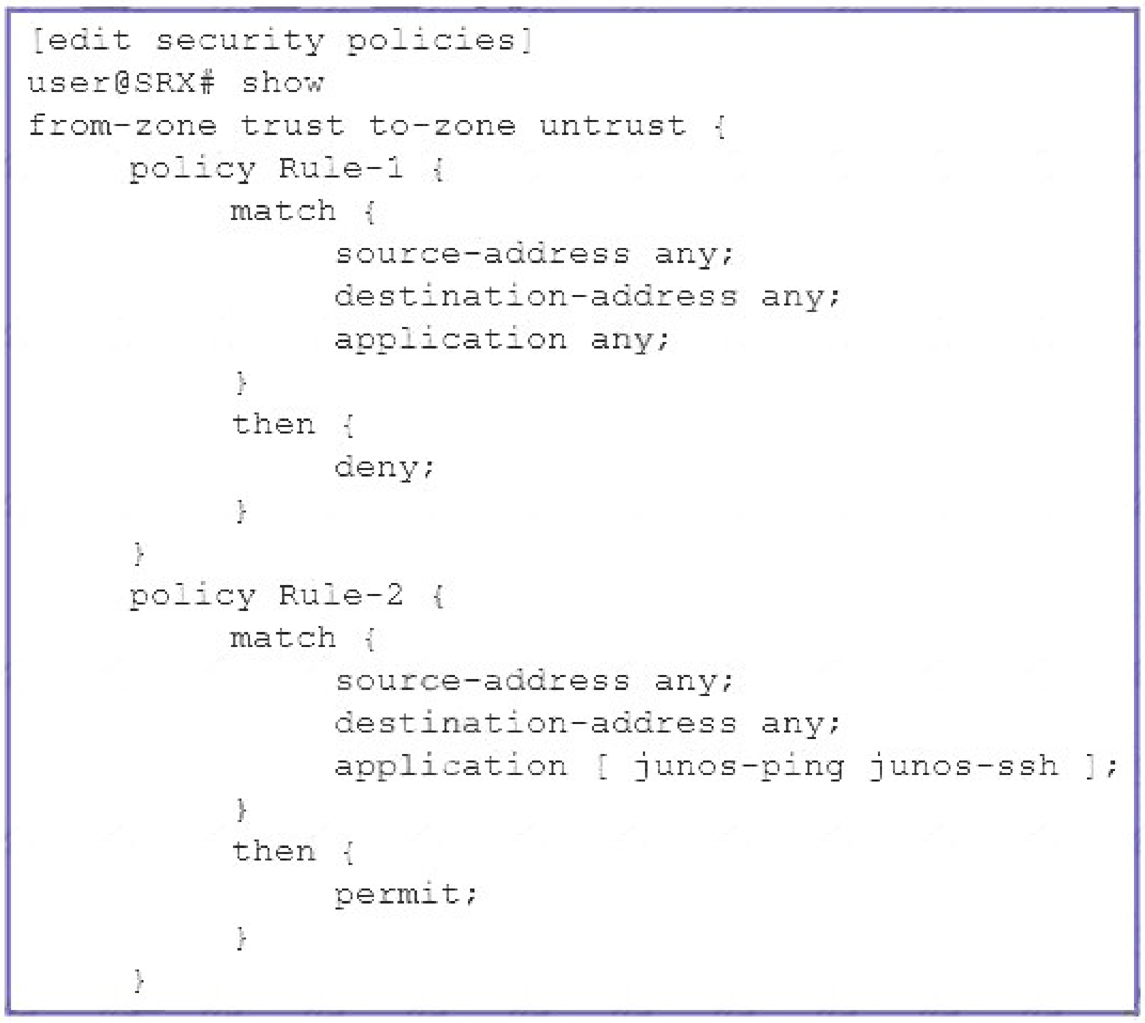
NEW QUESTION 4
You have configured a UTM feature profile.
Which two additional configuration steps are required for your UTM feature profile to take effect? (Choose two.)

A. Associate the UTM policy with an address book.
B. Associate the UTM policy with a firewall filter.
C. Associate the UTM policy with a security policy.
D. Associate the UTM feature profile with a UTM policy.

Answer: CD

Explanation:
For the UTM feature profile to take effect, it must be associated with a security policy and a UTM policy. The security policy defines the traffic flow and the actions that should be taken on the traffic, while the UTM policy defines the security features to be applied to the traffic, such as antivirus, intrusion prevention, and web filtering. The UTM feature profile provides the necessary configuration for the security features defined in the UTM policy.

NEW QUESTION 5
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 6
You want to deploy a NAT solution.
In this scenario, which solution would provide a static translation without PAT?

A. interface-based source NAT
B. pool-based NAT with address shifting
C. pool-based NAT with PAT
D. pool-based NAT without PAT

Answer: B

Explanation:
Translation of the original source IP address to an IP address from a user-defined address pool by shifting the IP addresses. This type of translation is one-to-one, static, and without port address translation. If the original source IP address range is larger than the IP address range in the user-defined pool, untranslated packets are dropped.
https://www.juniper.net/documentation/us/en/software/junos/nat/topics/topic-map/nat-security-source-and-sourc

NEW QUESTION 7
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 8
An application firewall processes the first packet in a session for which the application has not yet been identified.
In this scenario, which action does the application firewall take on the packet?

A. It allows the first packet.
B. It denies the first packet and sends an error message to the user.
C. It denies the first packet.
D. It holds the first packet until the application is identified.

Answer: D

Explanation:
This is necessary to ensure that the application firewall can properly identify the application and the correct security policies can be applied before allowing any traffic to pass through.
If the first packet was allowed to pass without first being identified, then the application firewall would not know which security policies to apply - and this could potentially lead to security vulnerabilities or breaches. So it's important that the first packet is held until the application is identified.

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 two IPsec hashing algorithms are supported on an SRX Series device? (Choose two.)

A. SHA-1
B. SHAKE128
C. MD5
D. RIPEMD-256

Answer: AC

NEW QUESTION 12
Which two security features inspect traffic at Layer 7? (Choose two.)

A. IPS/IDP
B. security zones
C. application firewall
D. integrated user firewall

Answer: AC

NEW QUESTION 15
When configuring antispam, where do you apply any local lists that are configured?

A. custom objects
B. advanced security policy
C. antispam feature-profile
D. antispam UTM policy

Answer: A

Explanation:
user@host# set security utm custom-objects url-pattern url-pattern-name https://www.juniper.net/documentation/us/en/software/junos/utm/topics/topic-map/security-local-list-antispam-f

NEW QUESTION 18
Which statement about global NAT address persistence is correct?

A. The same IP address from a source NAT pool will be assigned for all sessions from a given host.
B. The same IP address from a source NAT pool is not guaranteed to be assigned for all sessions from a given host.
C. The same IP address from a destination NAT pool will be assigned for all sessions for a given host.
D. The same IP address from a destination NAT pool is not guaranteed to be assigned for all sessions for a given host.

Answer: A

Explanation:
Use the persistent-nat feature to ensure that all requests from the same internal transport address are mapped to the same reflexive transport address (the public IP address and port created by the NAT device closest to the STUN server). The source NAT rule action can use a source NAT pool (with or without port translation) or an egress interface.

NEW QUESTION 20
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 21
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 25
Which statement about NAT is correct?

A. Destination NAT takes precedence over static NAT.
B. Source NAT is processed before security policy lookup.
C. Static NAT is processed after forwarding lookup.
D. Static NAT takes precedence over destination NAT.

Answer: D

NEW QUESTION 29
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 30
You are asked to verify that a license for AppSecure is installed on an SRX Series device. In this scenario, which command will provide you with the required information?

A. user@srx> show system license
B. user@srx> show services accounting
C. user@srx> show configuration system
D. user@srx> show chassis firmware

Answer: A

NEW QUESTION 32
What is the main purpose of using screens on an SRX Series device?

A. to provide multiple ports for accessing security zones
B. to provide an alternative interface into the CLI
C. to provide protection against common DoS attacks
D. to provide information about traffic patterns traversing the network

Answer: C

Explanation:
The main purpose of using screens on an SRX Series device is to provide protection against common Denial of Service (DoS) attacks. Screens help prevent network resources from being exhausted or unavailable by filtering or blocking network traffic based on predefined rules. The screens are implemented as part of the firewall function on the SRX Series device, and they help protect against various types of DoS attacks, such as TCP SYN floods, ICMP floods, and UDP floods.

NEW QUESTION 34
You have an FTP server and a webserver on the inside of your network that you want to make available to users outside of the network. You are allocated a single public IP address.
In this scenario, which two NAT elements should you configure? (Choose two.)

A. destination NAT
B. NAT pool
C. source NAT
D. static NAT

Answer: AB

Explanation:
With single Ip address it is port forwarding. So, destination NAT and a pool address point to the single public IP of the internet facing interface.

NEW QUESTION 35
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

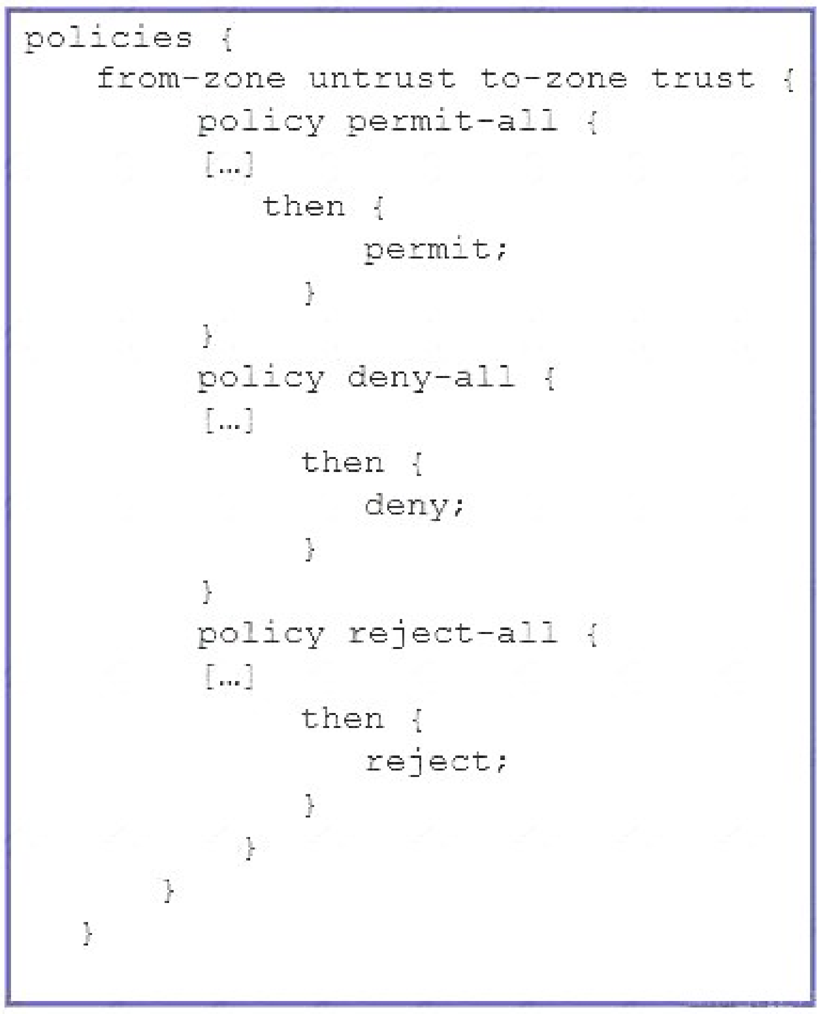
Explanation:
Juniper Advanced Threat Prevention (ATP) Cloud is a security service that helps organizations protect against advanced threats by providing real-time threat intelligence and automated response capabilities. It combines a cloud-based threat intelligence platform with the security capabilities 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 40
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 45
Click the Exhibit button.



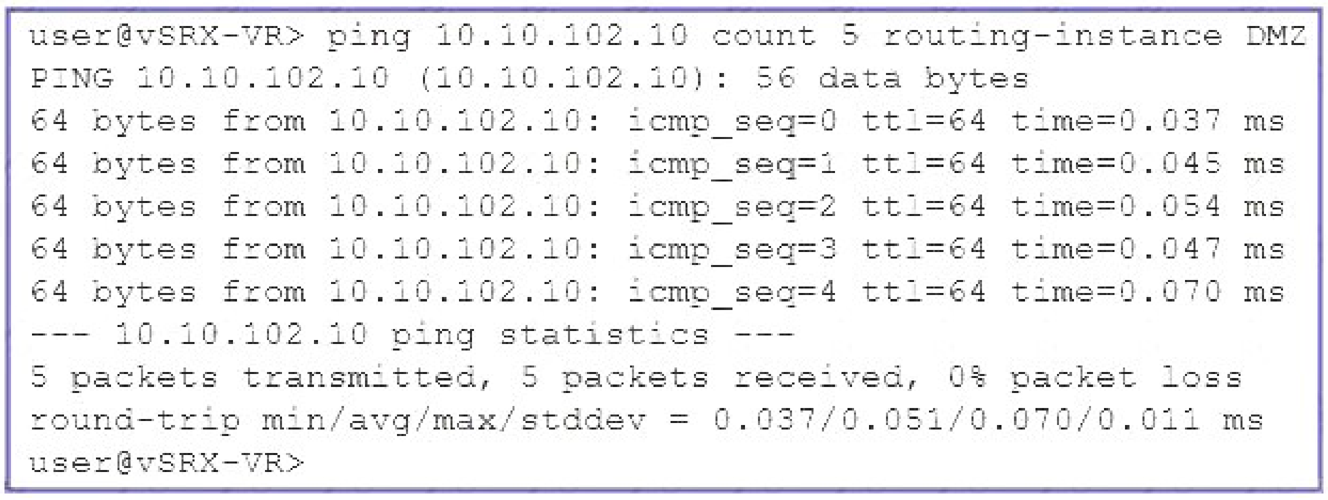
```
policies {
    from-zone untrust to-zone trust {
         policy permit-all {
         [...]
            then {
                 permit;
            }
         }
         policy deny-all {
         [...]
              then {
                 deny;
              }
         }
         policy reject-all {
         [...]
              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 46
Click the Exhibit button.



```
user@vSRX-VR> ping 10.10.102.10 count 5 routing-instance DMZ
PING 10.10.102.10 (10.10.102.10): 56 data bytes
64 bytes from 10.10.102.10: icmp_seq=0 ttl=64 time=0.037 ms
64 bytes from 10.10.102.10: icmp_seq=1 ttl=64 time=0.045 ms
64 bytes from 10.10.102.10: icmp_seq=2 ttl=64 time=0.054 ms
64 bytes from 10.10.102.10: icmp_seq=3 ttl=64 time=0.047 ms
64 bytes from 10.10.102.10: icmp_seq=4 ttl=64 time=0.070 ms
--- 10.10.102.10 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max/stddev = 0.037/0.051/0.070/0.011 ms
user@vSRX-VR>
```

Referring to the exhibit, which two statements are correct about the ping command? (Choose two.)

A. The DMZ routing-instance is the source.
B. The 10.10.102.10 IP address is the source.
C. The 10.10.102.10 IP address is the destination.
D. The DMZ routing-instance is the destination.

Answer: AC

NEW QUESTION 48
What are two features of the Juniper ATP Cloud service? (Choose two.)

A. sandbox
B. malware detection
C. EX Series device integration
D. honeypot

Answer: AB

NEW QUESTION 53
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 58
When transit traffic matches a security policy, which three actions are available? (Choose three.)

A. Allow
B. Discard
C. Deny
D. Reject
E. Permit

Answer: CDE

NEW QUESTION 59
You want to prevent other users from modifying or discarding your changes while you are also editing the configuration file.
In this scenario, which command would accomplish this task?

A. configure master
B. cli privileged
C. configure exclusive
D. configure

Answer: C

NEW QUESTION 63
......