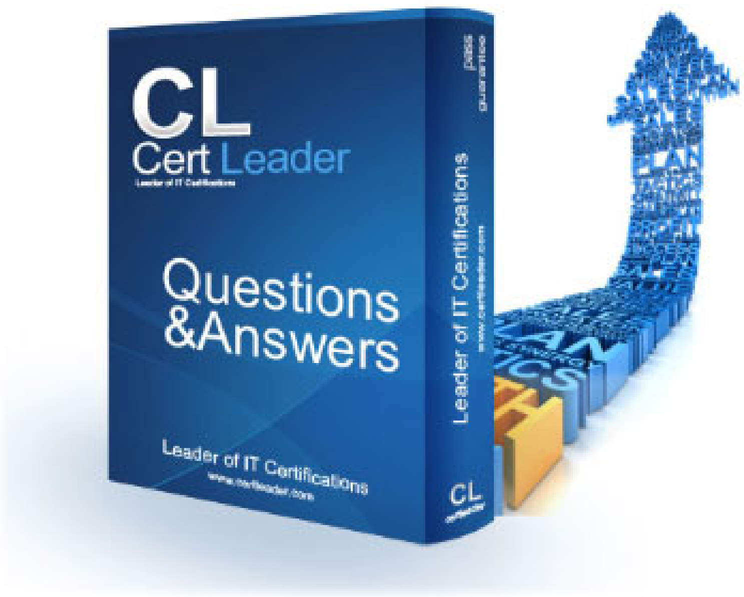
JN0-231 Dumps

Security - Associate (JNCIA-SEC)

https://www.certleader.com/JN0-231-dumps.html



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

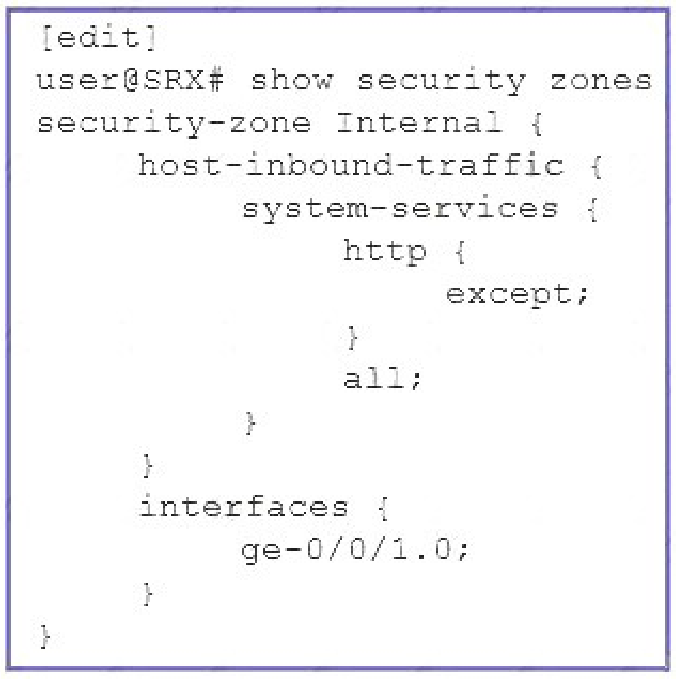
Explanation:
According to the Juniper Networks official JNCIA-SEC Exam Guide, web filtering is a feature used to control access to web content, including the ability to block specific types of files.
In the scenario mentioned, you want to block executable files from being downloaded, which can be accomplished 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
What is the correct order in which interface names should be identified?

A. system slot number –> interface media type –> port number –> line card slot number
B. system slot number –> port number –> interface media type –> line card slot number
C. interface media type –> system slot number –> line card slot number –> port number
D. interface media type –> port number –> system slot number –> line card slot number

Answer: C

NEW QUESTION 4
Click the Exhibit button.



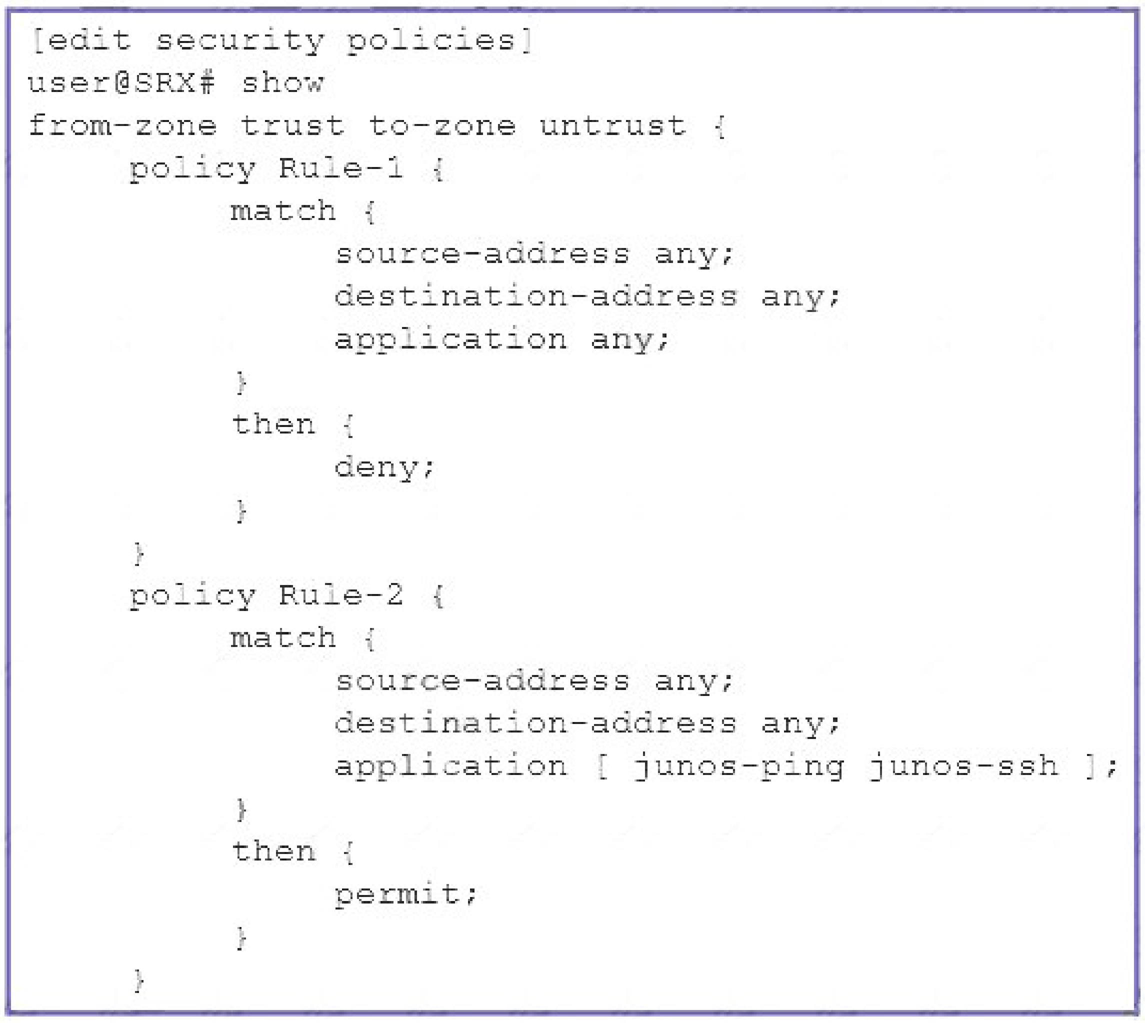
```
[edit]
user@SRX# show security zones
security-zone Internal {
     host-inbound-traffic {
          system-services {
               http {
                    except;
               }
               all;
          }
     }
     interfaces {
          ge-0/0/1.0;
     }
}
```

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
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 provide remote access to an internal development environment for 10 remote developers.
Which two components are required to implement Juniper Secure Connect to satisfy this requirement? (Choose two.)

A. an additional license for an SRX Series device
B. Juniper Secure Connect client software
C. an SRX Series device with an SPC3 services card
D. Marvis virtual network assistant

Answer: AB

NEW QUESTION 7
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 8
Which statement is correct about static NAT?

A. Static NAT supports port translation.
B. Static NAT rules are evaluated after source NAT rules.
C. Static NAT implements unidirectional one-to-one mappings.
D. Static NAT implements unidirectional one-to-many mappings.

Answer: C

Explanation:
Static NAT (Network Address Translation) is a type of NAT that maps a public IP address to a private IP address. With static NAT, a one-to-one mapping is created between a public IP address and a private IP address. This means that a single public IP address is mapped to a single private IP address, and all

incoming traffic to the public IP address is forwarded to the private IP address.

NEW QUESTION 9
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 10
Which two statements are true about Juniper ATP Cloud? (Choose two.)

A. Juniper ATP Cloud is an on-premises ATP appliance.
B. Juniper ATP Cloud can be used to block and allow IPs.
C. Juniper ATP Cloud is a cloud-based ATP subscription.
D. Juniper ATP Cloud delivers intrusion protection services.

Answer: CD

Explanation:
Juniper ATP Cloud is a cloud-based ATP subscription that delivers advanced threat protection services, such as URL categorization, file reputation analysis, and malware analysis. It is able to quickly and accurately categorize URLs and other web content, and can also provide detailed reporting on web usage, as well as the ability to define and enforce acceptable use policies. Additionally, Juniper ATP Cloud is able to block and allow specific IPs, providing additional protection against malicious content.
References:
https://www.juniper.net/documentation/en_US/junos-space-security-director/topics/task/configuration/security-s
https://www.juniper.net/documentation/en_US/junos-space-security-director/topics/task/configuration/security-s

NEW QUESTION 10
You want to enable the minimum Juniper ATP services on a branch SRX Series device. In this scenario, what are two requirements to accomplish this task? (Choose two.)

A. Install a basic Juniper ATP license on the branch device.
B. Configure the juniper-atp user account on the branch device.
C. Register for a Juniper ATP account on https://sky.junipersecurity.net.
D. Execute the Juniper ATP script on the branch device.

Answer: CD

Explanation:
https://manuals.plus/m/95fded847e67e8f456453182a54526ba3224a61a337c47177244d345d1f3b19e.pdf

NEW QUESTION 11
Corporate security requests that you implement a policy to block all POP3 traffic from traversing the Internet firewall.
In this scenario, which security feature would you use to satisfy this request?

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

Answer: C

NEW QUESTION 16
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 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
Which statement is correct about packet mode processing?

A. Packet mode enables session-based processing of incoming packets.
B. Packet mode works with NAT, VPNs, UTM, IDP, and other advanced security services.
C. Packet mode bypasses the flow module.
D. Packet mode is the basis for stateful processing.

Answer: C

NEW QUESTION 25
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 30
Which statement is correct about Junos security policies?

A. Security policies enforce rules that should be applied to traffic transiting an SRX Series device.
B. Security policies determine which users are allowed to access an SRX Series device.
C. Security policies control the flow of internal traffic within an SRX Series device.
D. Security policies identity groups of users that have access to different features on an SRX Series device.

Answer: A

Explanation:
The correct statement about Junos security policies is that they enforce rules that should be applied to traffic transiting an SRX Series device. Security policies control the flow of traffic between different zones on the SRX Series device, and dictate which traffic is allowed or denied. They can also specify which application and service requests are allowed or blocked. More information about Junos security policies can be found in the Juniper Networks technical documentation here: https://www.juniper.net/documentation/en_US/junos/topics/task/configuration/security-policies-overview.html.

NEW QUESTION 34
Which two statements are correct about the null zone on an SRX Series device? (Choose two.)

A. The null zone is created by default.
B. The null zone is a functional security zone.
C. Traffic sent or received by an interface in the null zone is discarded.
D. You must enable the null zone before you can place interfaces into it.

Answer: AC

Explanation:
According to the Juniper SRX Series Services Guide, the null zone is a predefined security zone that is created on the SRX Series device when it is booted. Traffic that is sent to or received on an interface in the null zone is discarded. The null zone is not a functional security zone, so you cannot enable or disable it.

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

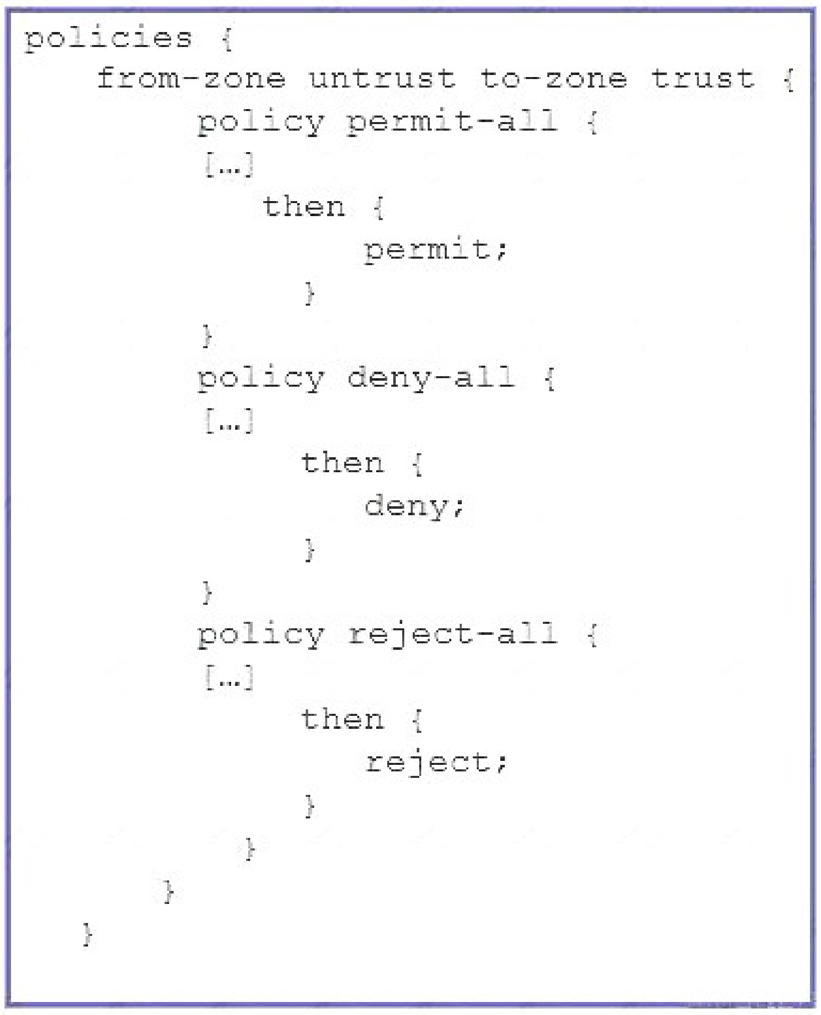
Explanation:
Juniper Advanced Threat Prevention (ATP) Cloud is a security service that helps organizations protect against advanced threats by providing real-time threat intelligence and automated response capabilities. It combines a cloud-based threat intelligence platform with the security capabilities 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 39
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 40
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 44
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 45
You must monitor security policies on SRX Series devices dispersed throughout locations in your organization using a 'single pane of glass' cloud-based solution.
Which solution satisfies the requirement?

A. Juniper Sky Enterprise
B. J-Web
C. Junos Secure Connect
D. Junos Space

Answer: D

Explanation:
Junos Space is a management platform that provides a single pane of glass view of SRX Series devices dispersed throughout locations in your organization. It provides visibility into the security policies of the devices, allowing you to quickly identify and respond to security threats. Additionally, it provides the ability to manage multiple devices remotely and in real-time, enabling you to quickly deploy and update security policies on all devices. For more information, please refer to

the Juniper Networks Junos Space Network Director User Guide, which can be found on Juniper's website.

NEW QUESTION 48
What does the number “2” indicate in interface ge-0/1/2?

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

Answer: D

NEW QUESTION 52
......