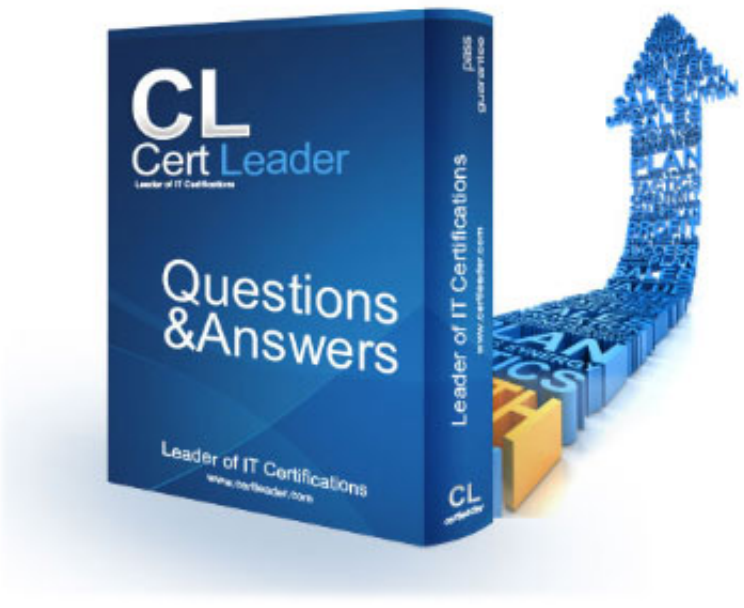
JN0-231 Dumps

Security - Associate (JNCIA-SEC)

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



NEW QUESTION 1
Which three operating systems are supported for installing and running Juniper Secure Connect client software? (Choose three.)

A. Windows 7
B. Android
C. Windows 10
D. Linux
E. macOS

Answer: ACE

Explanation:
Juniper Secure Connect client software is supported on the following three operating systems: Windows 7, Windows 10, and macOS. For more information, please refer to the Juniper Secure Connect Administrator Guide, which can be found on Juniper's website. The guide states: "The Juniper Secure Connect client is supported on Windows 7, Windows 10, and macOS." It also provides detailed instructions on how to install and configure the software for each of these operating systems.

NEW QUESTION 2
You are assigned a project to configure SRX Series devices to allow connections to your webservers. The webservers have a private IP address, and the packets must use NAT to be accessible from the
Internet. You do not want the webservers to initiate connections with external update servers on the Internet using the same IP address as customers use to access them.
Which two NAT types must be used to complete this project? (Choose two.)

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

Answer: CD

NEW QUESTION 3
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 4
You are deploying an SRX Series firewall with multiple NAT scenarios. In this situation, which NAT scenario takes priority?

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

Answer: A

Explanation:
This is because the interface NAT would allow the connections to pass through the firewall - and thus, would ensure that the appropriate ports are open in order to allow for the connections to be established.
This is a really important step in order to ensure that all of the appropriate traffic is allowed through the SRX Series firewall - and thus, it must be a priority when deploying the firewall.

NEW QUESTION 5
What are three primary match criteria used in a Junos security policy? (Choose three.)

A. application
B. source address
C. source port
D. class
E. destination address

Answer: ABE

NEW QUESTION 6
Which order is correct for Junos security devices that examine policies for transit traffic?

A. zone policies global policies default policies
B. default policies zone policies global policies
C. default policies global policies zone policies
D. global policies zone policies default policies

Answer: A

NEW QUESTION 7
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 8
Your ISP gives you an IP address of 203.0.113.0/27 and informs you that your default gateway is 203.0.113.1. You configure destination NAT to your internal server, but the requests sent to the webserver at 203.0.113.5 are not arriving at the server.
In this scenario, which two configuration features need to be added? (Choose two.)

A. firewall filter
B. security policy
C. proxy-ARP
D. UTM policy

Answer: BC

NEW QUESTION 9
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
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 10
Which two statements are correct about the integrated user firewall feature?(Choose two.)

A. It maps IP addresses to individual users.
B. It supports IPv4 addresses.
C. It allows tracking of non-Windows Active Directory users.
D. It uses the LDAP protocol.

Answer: AC

NEW QUESTION 11
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 13
Which Web filtering solution uses a direct Internet-based service for URL categorization?

A. Juniper ATP Cloud
B. Websense Redirect
C. Juniper Enhanced Web Filtering
D. local blocklist

Answer: C

Explanation:
Juniper Enhanced Web Filtering is a web filtering solution that uses a direct Internet-based service for URL categorization. This service allows Enhanced Web Filtering to quickly and accurately categorize URLs and other web content, providing real-time protection against malicious content. Additionally, Enhanced Web Filtering is able to provide detailed reporting on web usage, as well as the ability to define and enforce acceptable use policies.
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 17
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 20
Which IPsec protocol is used to encrypt the data payload?

A. ESP
B. IKE
C. AH
D. TCP

Answer: A

NEW QUESTION 24
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 29
Which two statements are correct about screens? (Choose two.)

A. Screens process inbound packets.
B. Screens are processed on the routing engine.
C. Screens process outbound packets.
D. Screens are processed on the flow module.

Answer: AD

NEW QUESTION 31
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 35
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 36
Which security policy type will be evaluated first?

A. A zone policy with no dynamic application set
B. A global with no dynamic application set
C. A zone policy with a dynamic application set
D. A global policy with a dynamic application set

Answer: D

NEW QUESTION 37
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 39
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 42
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 43
Which two IKE Phase 1 configuration options must match on both peers to successfully establish a tunnel? (Choose two.)

A. VPN name
B. gateway interfaces
C. IKE mode
D. Diffie-Hellman group

Answer: CD

NEW QUESTION 48
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 52
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 57
Which Juniper ATP feed provides a dynamic list of known botnet servers and known sources of malware downloads?

A. infected host cloud feed
B. Geo IP feed
C. C&C cloud feed
D. blocklist feed

Answer: A

NEW QUESTION 58
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 60
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 63
Which two services does Juniper Connected Security provide? (Choose two.)

A. protection against zero-day threats
B. IPsec VPNs
C. Layer 2 VPN tunnels
D. inline malware blocking

Answer: AD

NEW QUESTION 66
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 68
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 72
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 75
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 77
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 82
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 86
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 89
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 94
Which two statements about user-defined security zones are correct? (Choose two.)

A. Users cannot share security zones between routing instances.
B. Users can configure multiple security zones.
C. Users can share security zones between routing instances.
D. User-defined security zones do not apply to transit traffic.

Answer: BC

Explanation:
User-defined security zones allow users to configure multiple security zones and share them between routing instances. This allows users to easily manage multiple security zones and their associated policies. For example, a user can create a security zone for corporate traffic, a security zone for guest traffic, and a security zone for public traffic, and then configure policies to control the flow of traffic between each of these security zones. Transit traffic can also be managed using user-defined security zones, as the policies applied to these zones will be applied to the transit traffic as well.
References:
https://www.juniper.net/documentation/en_US/junos/topics/task/configuration/security-zones-overview-configu
https://www.juniper.net/documentation/en_US/junos/topics/task/security/security-zones-configuring-shared.htm

NEW QUESTION 95
.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your JN0-231 Exam with Our Prep Materials Via below:

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