Juniper

Exam Questions JN0-231

Security - Associate (JNCIA-SEC)

About Exambible

Your Partner of IT Exam

Found in 1998

Exambible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, Exambible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

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
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 3
What are two characteristics of a null zone? (Choose two.)

A. The null zone is configured by the super user.
B. By default, all unassigned interfaces are placed in the null zone.
C. All ingress and egress traffic on an interface in a null zone is permitted.
D. When an interface is deleted from a zone, it is assigned back to the null zone.

Answer: BD

NEW QUESTION 4
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 5
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 6
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 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
You are investigating a communication problem between two hosts and have opened a session on the SRX Series device closest to one of the hosts and entered the show security flow session command.
What information will this command provide? (Choose two.)

A. The total active time of the session.
B. The end-to-end data path that the packets are taking.
C. The IP address of the host that initiates the session.
D. The security policy name that is controlling the session.

Answer: CD

NEW QUESTION 9
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
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 10
You are installing a new SRX Series device and you are only provided one IP address from your ISP. In this scenario, which NAT solution would you implement?

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

Answer: C

NEW QUESTION 14
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 16
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 18
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 20
Which two addresses are valid address book entries? (Choose two.)

A. 173.145.5.21/255.255.255.0
B. 153.146.0.145/255.255.0.255
C. 203.150.108.10/24
D. 191.168.203.0/24

Answer: AC

Explanation:
The correct address book entries are:
* 173.145.5.21/255.255.255.0
* 203.150.108.10/24
Both of these entries represent a valid IP address and subnet mask combination, which can be used as an address book entry in a Juniper device.

NEW QUESTION 21
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 22
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 26
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 30
You are asked to configure your SRX Series device to block all traffic from certain countries. The solution must be automatically updated as IP prefixes become allocated to those certain countries.
Which Juniper ATP solution will accomplish this task?

A. Geo IP
B. unified security policies
C. IDP
D. C&C feed

Answer: A

Explanation:
Juniper ATP Geo IP can help to accomplish this task by using geolocation services to determine the geographical location of IP addresses. As IP prefixes get allocated to the countries that you have specified, the Geo IP solution will automatically update the configured firewall policies to block any traffic that is coming from those specific countries.
This is a great solution for blocking specific countries - as it will allow for a more personalized and targeted approach to firewall policies - and thus, to increase the effectiveness of the solution at blocking potential malicious traffic.

NEW QUESTION 34
In this scenario, which two IP packets will match the criteria? (Choose two.)

A. 192.168.1.21
B. 192.168.0.1
C. 192.168.1.12
D. 192.168.22.12

Answer: CD

NEW QUESTION 36
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 41

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 46
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 51
What is an IP addressing requirement for an IPsec VPN using main mode?

A. One peer must have dynamic IP addressing.
B. One peer must have static IP addressing.
C. Both peers must have dynamic IP addresses.
D. Both peers must have static IP addressing.

Answer: D

NEW QUESTION 53
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 57
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 60
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 64
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 66
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 68
What is the order of the first path packet processing when a packet enters a device?

A. security policies –> screens –> zones
B. screens –> security policies –> zones
C. screens –> zones –> security policies
D. security policies –> zones –> screens

Answer: C

NEW QUESTION 71
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 73
Your company is adding IP cameras to your facility to increase physical security. You are asked to help protect these loT devices from becoming zombies in a DDoS attack.
Which Juniper ATP feature should you configure to accomplish this task?

A. IPsec
B. static NAT
C. allowlists
D. C&C feeds

Answer: D

Explanation:
Juniper ATP should be configured with C&C feeds that contain lists of malicious domains and IP addresses in order to prevent IP cameras from becoming zombies in a DDoS attack.
This is an important step to ensure that the IP cameras are protected from malicious requests - and thus, they will not be able to be used in any DDoS attacks against the facility.

NEW QUESTION 78
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 83
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 86
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 87
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 88
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 92
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 95
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 96
What is the number of concurrent Secure Connect user licenses that an SRX Series device has by default?

A. 3
B. 4
C. 2
D. 5

Answer: C

Explanation:
The number of concurrent Secure Connect user licenses that an SRX Series device has by default is 2. Secure Connect is a feature of Juniper SRX Series devices that allows you to securely connect to remote networks via IPsec VPN tunnels. Each SRX Series device comes with two concurrent Secure Connect user licenses by default, meaning that it can support up to two simultaneous IPsec VPN connections. For more information, please refer to the Juniper Networks SRX Series Services Gateways Security Configuration Guide, which can be found on Juniper's website.

NEW QUESTION 99
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 103
.....

Relate Links

100% Pass Your JN0-231 Exam with Exambible Prep Materials

https://www.exambible.com/JN0-231-exam/

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - https://www.exambible.com/