Q&A

Up-to-date Questions and Answers from authentic resources to improve knowledge and pass the exam at very first attempt.
----- Guaranteed.

KILL EXAMS

PASS

Juniper

JN0-231

Security - Associate (JNCIA-SEC)

Question: 26

You want to verify the peer before IPsec tunnel establishment.

What would be used as a final check in this scenario?

A. traffic selector
B. perfect forward secrecy
C. st0 interfaces
D. proxy ID

Answer: D

Explanation:

The proxy ID is used as a final check to verify the peer before IPsec tunnel establishment. The proxy ID is a combination of local and remote subnet and protocol, and it is used to match the traffic that is to be encrypted. If the proxy IDs match between the two IPsec peers, the IPsec tunnel is established, and the traffic is encrypted.

Reference:

Juniper Networks SRX Series Services Gateway IPsec Configuration Guide:

https://www.juniper.net/documentation/en_US/release-independent/junos/topics/topic-map/security-ipsec-vpn-configuring.html

Question: 27

Which feature would you use to protect clients connected to an SRX Series device from a SYN flood attack?

A. security policy
B. host inbound traffic
C. application layer gateway
D. screen option

Answer: D

Explanation:

A screen option in the SRX Series device can be used to protect clients connected to the device from a SYN flood attack. Screens are security measures that you can use to protect your network from various types of attacks, including SYN floods. A screen option specifies a set of rules to match against incoming packets, and it can take specific actions such as discarding, logging, or allowing the packets based on the rules.

Reference:

Juniper Networks SRX Series Services Gateway Screen Configuration Guide:
https://www.juniper.net/documentation/en_US/junos/topics/topic-map/security-screen-configuring.html

Question: 28

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.

Reference: https://www.juniper.net/documentation/en_US/junos/topics/concept/security-srx-series-firewall-screen-dos.html

Question: 29

You want to implement user-based enforcement of security policies without the requirement of certificates and supplicant software.

Which security feature should you implement in this scenario?

A. integrated user firewall
B. screens
C. 802.1X
D. Juniper ATP

Answer: D

Explanation:

In this scenario, you should implement Juniper ATP (Advanced Threat Prevention). Juniper ATP provides user-based enforcement of security policies without the requirement of certificates and supplicant software. It uses a combination of behavioral analytics, sandboxing, and threat intelligence to detect and respond to advanced threats in real time. Juniper ATP provides robust protection against targeted attacks, malicious insiders, and zero-day malware. For more information, please refer to the Juniper ATP product page on Juniper's website.

Question: 30

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.

Reference:

Juniper Networks JNCIA-SEC Exam Guide: https://www.juniper.net/training/certification/certification-exam-guides/jncia-sec-exam-guide/

Question: 31

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."

Reference:

Juniper Networks JNCIA-SEC Exam Guide: https://www.juniper.net/training/certification/certification-exam-guides/jncia-sec-exam-guide/

Question: 32

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-hardware.html.

Question: 33

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-Web 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.

Question: 34

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.

Question: 35

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: A,B

Question: 36

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: A,D

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.

Question: 37

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.

Question: 38

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

Question: 39

What is the order of the first path packet processing when a packet enters a device?

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

Answer: C

Question: 40

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

SAMPLE QUESTIONS

*These questions are for demo purpose only. **Full version** is up to date and contains actual questions and answers.*

Killexams.com is an online platform that offers a wide range of services related to certification exam preparation. The platform provides actual questions, exam dumps, and practice tests to help individuals prepare for various certification exams with confidence. Here are some key features and services offered by Killexams.com:

Actual Exam Questions: Killexams.com provides actual exam questions that are experienced in test centers. These questions are updated regularly to ensure they are up-to-date and relevant to the latest exam syllabus. By studying these actual questions, candidates can familiarize themselves with the content and format of the real exam.

Exam Dumps: Killexams.com offers exam dumps in PDF format. These dumps contain a comprehensive collection of questions and answers that cover the exam topics. By using these dumps, candidates can enhance their knowledge and improve their chances of success in the certification exam.

Practice Tests: Killexams.com provides practice tests through their desktop VCE exam simulator and online test engine. These practice tests simulate the real exam environment and help candidates assess their readiness for the actual exam. The practice tests cover a wide range of questions and enable candidates to identify their strengths and weaknesses.

Guaranteed Success: Killexams.com offers a success guarantee with their exam dumps. They claim that by using their materials, candidates will pass their exams on the first attempt or they will refund the purchase price. This guarantee provides assurance and confidence to individuals preparing for certification exams.

Updated Content: Killexams.com regularly updates its question bank and exam dumps to ensure that they are current and reflect the latest changes in the exam syllabus. This helps candidates stay up-to-date with the exam content and increases their chances of success.

Technical Support: Killexams.com provides free 24x7 technical support to assist candidates with any queries or issues they may encounter while using their services. Their certified experts are available to provide guidance and help candidates throughout their exam preparation journey.

For More exams visit https://killexams.com/vendors-exam-list
Kill your exam at First Attempt....Guaranteed!