

Exam Questions JN0-231

Security - Associate (JNCIA-SEC)

<https://www.2passeasy.com/dumps/JN0-231/>



NEW QUESTION 1

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 2

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 3

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 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

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 6

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 7

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."

NEW QUESTION 8

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 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 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 13

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 18

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 21

Which two statements are correct about global policies? (Choose two.)

- A. Global policies are evaluated after default policies.
- B. Global policies do not have to reference zone context.
- C. Global policies are evaluated before default policies.
- D. Global policies must reference zone contexts.

Answer: BC

Explanation:

Global policies are used to define rules for traffic that is not associated with any particular zone. This type of policy is evaluated first, before any rules related to specific zones are evaluated.

For more detailed information about global policies, refer to the Juniper Networks Security Policy Overview guide, which can be found at https://www.juniper.net/documentation/en_US/junos/topics/reference/security-policy-overview.html. The guide provides an overview of the Juniper Networks security policy architecture, as well as detailed descriptions of the different types of policies and how they are evaluated.

NEW QUESTION 26

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 29

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 33

Screens on an SRX Series device protect against which two types of threats? (Choose two.)

- A. IP spoofing
- B. ICMP flooding
- C. zero-day outbreaks
- D. malicious e-mail attachments

Answer: AB

Explanation:

ICMP flood

Use the ICMP flood IDS option to protect against ICMP flood attacks. An ICMP flood attack typically occurs when ICMP echo requests use all resources in

responding, such that valid network traffic can no longer be processed.

The threshold value defines the number of ICMP packets per second (pps) allowed to be sent to the same destination address before the device rejects further ICMP packets.

IP spoofing

Use the IP address spoofing IDS option to prevent spoofing attacks. IP spoofing occurs when an invalid source address is inserted in the packet header to make the packet appear to come from a trusted source.

<https://www.juniper.net/documentation/us/en/software/junos/denial-of-service/topics/topic-map/security-introdu>

NEW QUESTION 38

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 41

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 45

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 50

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 51

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual JN0-231 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the JN0-231 Product From:

<https://www.2passeasy.com/dumps/JN0-231/>

Money Back Guarantee

JN0-231 Practice Exam Features:

- * JN0-231 Questions and Answers Updated Frequently
- * JN0-231 Practice Questions Verified by Expert Senior Certified Staff
- * JN0-231 Most Realistic Questions that Guarantee you a Pass on Your First Try
- * JN0-231 Practice Test Questions in Multiple Choice Formats and Updates for 1 Year