JN0-636 Q&As

Service Provider Routing and Switching Professional (JNCIP-SP)

Pass Juniper JN0-636 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.passapply.com/jn0-636.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Juniper Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

Regarding IPsec CoS-based VPNs, what is the number of IPsec SAs associated with a peer based upon?

A. The number of traffic selectors configured for the VPN.

B. The number of CoS queues configured for the VPN.

C. The number of classifiers configured for the VPN.

D. The number of forwarding classes configured for the VPN.

Correct Answer: D

Explanation: In IPsec CoS-based VPNs, the number of IPsec Security Associations (SAs) associated with a peer is based on the number of forwarding classes configured for the VPN. The forwarding classes are used to classify and prioritize different types of traffic, such as voice and data traffic. Each forwarding class requires a separate IPsec SA to be established between the peers, in order to provide the appropriate level of security and quality of service for each type of traffic.

QUESTION 2

You want to use selective stateless packet-based forwarding based on the source address.

In this scenario, which command will allow traffic to bypass the SRX Series device flow daemon?

A. set firewall family inet filter bypaa3_flowd term t1 then skip--services accept

B. set firewall family inet filter bypass_flowd term t1 then routing-instance stateless

C. set firewall family inet filter bypas3_flowd term t1 then virtual-channel stateless

D. set firewall family inet filter bypass__f lowd term t1 then packet--mode

Correct Answer: C

QUESTION 3

Your company wants to use the Juniper SecIntel feeds to block access to known command and control servers, but they do not want to use Security Director to manage the feeds. Which two Juniper devices work in this situation? (Choose two)

A. EX Series devices

B. MX Series devices

C. SRX Series devices

D. QFX Series devices

Correct Answer: BC

Explanation: Juniper MX and SRX series devices support the integration of SecIntel feeds, which provide information about known command and control servers, for the purpose of blocking access to them. These devices can be configured to use the SecIntel feeds without the need for Security Director to manage the feeds. EX series and QFX series devices are not capable of working in this situation, as they do not support the integration of SecIntel feeds.

QUESTION 4

To analyze and detect malware, Juniper ATP Cloud performs which two functions? (Choose two.)

A. cache lookup: to see if the file is seen already and known to be malicious

B. antivirus scan: with a single vendor solution to see if the file contains any potential threats

C. dynamic analysis: to see what happens if you execute the file in a real environment

D. static analysis: to see what happens if you execute the file in a real environment

Correct Answer: AC

Explanation: Juniper ATP Cloud performs cache lookup to see if the file is seen already and known to be malicious and dynamic analysis to see what happens if you execute the file in a real environment.

QUESTION 5

Your IPsec VPN configuration uses two CoS forwarding classes to separate voice and data traffic. How many IKE security associations are required between the IPsec peers in this scenario?

B. 3

C. 4

D. 2

Correct Answer: A

Explanation: An IKE security association (SA) is a set of parameters that define how the Internet Key Exchange (IKE) protocol will authenticate and establish the secure channel between the IPsec VPN peers. When you configure an IPsec

VPN, one IKE SA is created between the peers, regardless of how many CoS forwarding classes are used to separate the traffic. The SA will be used to negotiate the IPsec SA parameters, such as encryption algorithms and keys.

In this scenario, only 1 IKE security association is required between the IPsec peers, no matter how many CoS forwarding classes are used to separate the voice and data traffic.