ISLEVER

JN0-632

Security, Professional (JNCIP-SEC)

DEMO

https://www.islever.com/jn0-632.html

https://www.islever.com/juniper.html

For the most up-to-date exam questions and materials, we recommend visiting our website, where you can access the latest content and resources.

Note: The answer is for reference only, you need to understand all question.

QUESTION 1
You are concerned about the latency introduced in processing packets through the IPS signature database and want to configure the SRX Series device to minimize latency. You decide to configure inline tap mode.

Which two statements are true? (Choose two)

A. When packets pass through for firewall inspection, they are not copied to the IPS module.
B. Packets passing through the firewall module are copied to the IPS module for processing as the packets continue through the forwarding process.
C. Traffic that exceeds the processing capacity of the IPS module will be dropped.
D. Traffic that exceeds the processing capacity of the IPS module will be forwarded without being inspected by the IPS module.

Answer: BD

QUESTION 2
You create a custom attack signature with the following criteria:

-- HTTP Request:
-- Pattern: *\x<404040...40
-- Direction Client to Server

Which client request would be identified as an attack?

A. FTP GET.,\x404040...40
B. HTTP GET *\404040..40
C. HTPPOST.*\x404040...40
D. HTTP GET *\x4040401.40

Answer: D

QUESTION 3
Click the Exhibit button.

In the exhibit, what does the configured screen do?

Exhibit:

```
[edit]
user@srx# show security
screen {
    ids-option screen1 {
        tcp {
            port-scan threshold 1000;
        }
    }
}
```

A. It blocks TCP connection from a host when more than 1000 successive TCP connections are received.
B. It blocks TCP connections for a host when more than 1000 connections are received within 3600 seconds.
C. It blocks TCP connection attempts from a host when more than 10 connection attempts are made within 1000 microseconds.
D. It blocks TCP connections from the host for 1000 seconds when a host is identified as a TCP scan source.

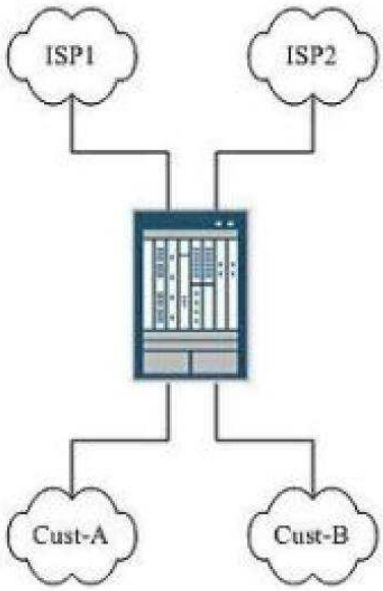
Answer: C

QUESTION 4
Click the Exhibit button.

In the exhibit, Customer A and Customer B connect to the same SRX Series device. ISP1 and ISP2 are also directly connected to the SRX device. Customer A's traffic must use ISP1, and Customer B's traffic must use ISP2.

Which configuration will create the required routing tables?

Exhibit:



A. set routing-options rib-groups fbf import-rib [custA.inet.0 custB.inet.0]
B. set routing-options rib-groups fbf export-rib [custA.inet.0 custB.inet.0]
C. set routing-options rib-groups fbf import-rib [custA.inet.0 custB.inet.0 inet.0]
D. set routing-options rib-groups fbf export-rib [custA.inet.0 custB.inet.0 inet.0]

Answer: C

QUESTION 5
You must configure a site-to-site VPN connection between your company and a business partner. The security policy of your organization states that the source of incoming traffic must be authenticated by a neutral party to prevent spoofing of an unauthorized source gateway.

What accomplishes this goal?

A. Use a manual key exchange to encrypt/decrypt traffic.
B. Generate internal Diffie-Hellman public/private key pairs on each VPN device and exchange public keys with the business partner.
C. Use a third-party certificate authority and exchange public keys with the business partner.
D. Use a private X.509 PKI certificate and verify it against a third-party certificate revocation list (CRL).

Answer: C

QUESTION 6
Company A and Company B are using the same IP address space. You are using static NAT to provide dual translation between the two networks.

Which two additional requirements are needed to fully allow end-to-end communication? (Choosetwo.)

A. route information for each remote device
B. persistent-nat
C. required security policies
D. no-nat-traversal

Answer: AC

QUESTION 7
Your company is deploying a new WAN that uses transport over a private network infrastructure to provide an any-to-any topology. Your manager is concerned about the confidentiality of data as it crosses the WAN. Scalability of the SRX Series device's ability to perform IKE key exchanges is a key consideration.