Vendor: Juniper

Exam Code: JN0-632

Exam Name: Security, Professional (JNCIP-SEC)

Version: DEMO

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: B,D

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. FTPGET.,\x404040...40
B. HTTP GET *\404040..40
C. HTPPOST.*\x404040...40
D. HTTP GET *Vx40404CL.40
Answer: D

3.Click the Exhibit button.
In the exhibit, what does the configured screen do?
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

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?
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

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

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? (Choose two.)

A. route information for each remote device

B. persistent-nat

C. required security policies

D. no-nat-traversal

Answer: A,C

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.
Which VPN design satisfies your manager's concerns?

A. a transparent IPSec VPN

B. a hub-and-spoke VPN

C. a point-to-multipoint VPN

D. a group VPN

Answer: D

8.Click the Exhibit button

```
[edit security idp security-package]
user@srx# show
url http://sec-pack.juniper.net;
automatic {
    start-time "2011-4-21.00:01:00 +0000";
    interval 24;
}
```

Senior management reports that your company's network is being attacked by hackers exploiting a recently announced vulnerability. The attack is not being detected by the DP on your SRX Series device.
You suspect that your attack database is out of date. You check the version of the attack database and discover it is several weeks old. You configured your device to download updates automatically as shown in the exhibit.
What must you do for the automatic update to function properly?
A. Change the interval to daily by adding set automatic interval 1 to the configuration and commit the change.
B. Enable the automatic updates by adding set automatic enable to the configuration and commit the change.
C. Set the time zone on your device.
D. Change the URL of the update site to use https:// instead of http://.
Answer: B

9.You obtained a license tile from Juniper Networks for the SRX Series Services Gateway IPS feature set.
You want to install the license onto the SRX Series device.
Which statement is accurate?
A. The license file is automatically downloaded from the online license server, you need not do anything.
B. Transfer the file to the SRX Series device using FTP or SCP and install the license with the request system license add <filename> command.
C. The license file must be decrypted with the openssl utility before being installed on the SRX Series device.
D. TransferthefiletotheSRXfirewallusingFTPorSCPandinstallthelicensewiththe request system license install-permanent command.
Answer: B

10.You have been asked to configure a signature to block an attack released by a security vulnerability reporting agency. Which two characteristics of the attack must you understand to configure the attack object? (Choose two)
A. the source port of the attacker
B. a string or regular expression that occurs within the attack
C. the context where the attack pattern is found within the packet
D. the IPv4 routing header
Answer: B,C

11.In a group VPN the members rekey with the server using the Unicast PUSH method. This rekey mechanism is protected by which secure channel?
A. KEK
B. IPSec SA

C. TEK

D. IKE SA

Answer: A

12.Which two configuration tasks should you use to implement filter-based forwarding? (Choose two.)

A. Create a VRF routing instance.

B. Create a firewall filter with an action of virtual-channel

C. Create routing options with rib-groups.

D. Create routing options with interface routes.

Answer: C,D

13.Your corporate network consists of a central office and four branch offices. You are responsible for coming up with an effective solution to provide secure connectivity between the sites.

Which solution meets the requirements?

A. Implement firewall filters on each device.

B. Implement an H11 HS-based mesh between all sites.

C. Implement secure routing policies.

D. Implement a hub-and-spoke VPN

Answer: D

14.Click the Exhibit button.


```
user@srx# run show security flow session extensive
…
Session ID: 8444, Status: Normal
Flag: 0x84001000
Policy name: trust-to-untrust/6
Source NAT pool: Null
Maximum timeout: 2, Current timeout: 2
Session State: Valid
Start time: 1559573, Duration: 0
Client: FTP ALG, Group: 1, Resource: 1
   In: 11.1.1.10/20 --> 10.1.1.10/52304;tcp,
    Interface: ge-0/0/2.0,
    Session token: 0x7, Flag: 0x0x21
    Route: 0xe0010, Gateway: 11.1.1.10, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 2,
    Pkts: 5, Bytes: 330
   Out: 10.1.1.10/52304 --> 11.1.1.10/20;tcp,
    Interface: ge-0/0/1.0,
    Session token: 0x6, Flag: 0x0x20
    Route: 0x60010, Gateway: 10.1.1.10, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 2,
    Pkts: 4, Bytes: 208
Total sessions: 2
```

The client is downloading a file from the FTP server. The FTP control channel is established using a security policy named t rust-to-untrust.

Which statement is correct about the output in the exhibit regarding the data channel?

A. Passive FTP is being used to establish the data channel.

B. The pinhole has been opened by the FTP ALG for return traffic.

C. The session requires a separate security policy for return traffic.

D. The session is using NAT to translate IP addresses.

Answer: B

15.You want to verify how many security policies will match FTP traffic from source address 1.1.1.1 port 55000. to destination address 2.2.2.2 port 21.

Which operational mode command should you use?

A. show security match-policy from-zone trust source-ip 1.1.1.1 source-port 55000 to-zone untrust destination-ip 2.2.2.2 destination-port 21 protocol tcp result-count

B. test security match-policies from-zone trust source-ip 1.1.1.1 source-port 55000 to-zone untrust destination-ip 2.2.2.2 destination-port 21 protocol tcp result-count

C. show security match-policies from-zone trust source-ip 1.1.1.1 source-port 55000 to-zone untrust destination-ip 2.2.2.2 destination-port 21 protocol tcp result-count

D. show security match-policies from-zone trust source-ip 1.1.1.1 source-port 55000 to-zone untrust destination-ip 2.2.2.2 destination-port 21 protocol udp result-count

Answer: C

16.Click the Exhibit button

```
[edit security]
user@srx# show
ike {
    policy pol-ike {
        mode main;
        proposal-set standard;
        pre-shared-key ascii-text "$9$WDWXNb4aU.PQs2PQFnpu8X7"; ## SECRET-DATA
    }
    gateway hq {
        ike-policy pol-ike;
        address 192.168.41.3;
        external-interface ge-0/0/3;
    }
}
ipsec {
    policy pol-ipsec {
        proposal-set standard;
    }
    vpn ipsec-vpn {
        bind-interface st0.0;
        ike {
            gateway hq;
            ipsec-policy pol-ipsec;
        }
    }
...
```

The exhibit shows an IPSec tunnel configuration In an effort to increase the security of the tunnel, you must configure the tunnel to negotiate a new tunnel key during IKE phase 2.

How can the configuration be changed to accommodate this requirement/?

A. A new tunnel key is negotiated by default during phase 2; no configuration change is necessary.

B. PFS must be added to the IKE policy pol-ike.

C. PFS must be added to the IPSec policy poi-IPSec.
D. A new tunnel key cannot be negotiated in IKE phase 2 with route-based IPSec VPNs; a policy-based IPSec VPN must be
Answer: C

17.You configured all the required parameters to allow IPv6 address book entries. You successfully committed the configuration. You noticed that IPv4 traffic is still working as expected, but IPv6 traffic is being dropped.
What is the solution to the problem?
A. IPv4 and IPv6 address book entries will not work together
B. IPv6 flow-based mode must be enabled.
C. The SRX device must be rebooted.
D. IPv6 policy-based mode must be enabled.
Answer: C

18.Given the session shown below:
user@srx> show security flow session
Session ID: 3729, Policy name: nat-example-security-policy/6, Timeout: 2 In: 10.1.0.13/52939 > 207.17.137.229/80;tcp, If: ge-0/0/5.0 Out: 207.17.137.229/80 --> 172.19.101.42/2132;tcp, If: ge-0/0/0
Which statement is true?
A. The session indicates that destination NAT with no port translation is taking place.
B. The session indicates that no NAT is taking place.
C. The session indicates that source NAT is taking place.
D. The session indicates that destination NAT with port translation is taking place.
Answer: C

19.What are two implementations of NAT? (Choose two.)
A. source NAT
B. group NAT
C. filter-based NAT
D. destination NAT
Answer: A,D

20.You are notified that a particular application passing through a SRX3600 is not working properly. A request has been made to provide a packet capture of the application traffic as it egresses the SRX device.
What is required to capture the transit application traffic on the egress interface?
A. Create a firewall filter with the action packet-capture and apply the firewall filter to the egress interface.
B. Create a firewall filter with the action packet-mode and apply the firewall fitter to the egress interface.

C. Execute the operational mode command monitor traffic interface and specify the egress interface.
D. Configure the data path-debug capture parameters and start the packet capture from operational mode.
Answer: D