Juniper JN0-632

Security Professional (JNCIP-SEC)

Version: 6.4

Topic 1, Volume A

QUESTION NO: 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
Explanation: Inline Tap mode is supported in 10.2. It will have a positive impact on performance and will only be supported in dedicated mode. The processing will essentially be the same as it is in dedicated inline mode, however instead of flowd simply placing the packet in the IDPD queue to be processed, it will make a copy of the packet, put that in the queue, and forward on the original packet without waiting for IDPD to perform the inspection. This will mean that the IDP will not be a bottleneck in performance. The one limitation around this feature is that some attacks may be able to pass through the SRX without being blocked such as single packet attacks. However, even though the single packet attacks may not be blocked, most attacks will be blocked, and even in the case that an attack is let through the SRX can still close down the session and even send TCP resets if it is a TCP protocol and the Close Connection option is set.

QUESTION NO: 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

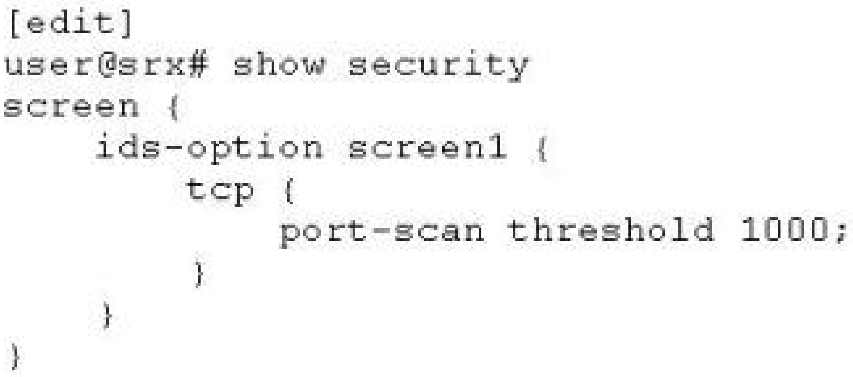
Answer: D

Explanation: Signature-based attack objects will be the most common form of attack object to configure. This is where you use regular expression matching to define what attack objects should be matched by the detector engine. The provided regular expression matches HTTP GET request containing *\x4040401..40. Here \x – hex based numbers, . - any symbol.

Reference: http://www.juniper.net/techpubs/en_US/idp5.1/topics/example/simple/intrusion-detection-prevention-custom-attack-object-compound-signature.html

QUESTION NO: 3

Click the Exhibit button.



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

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

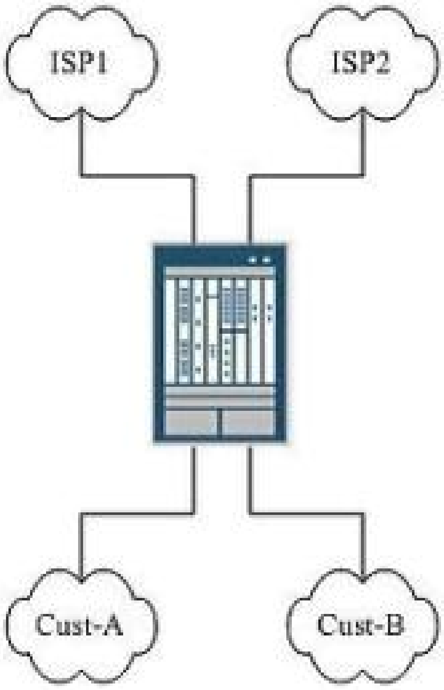
Answer: C

Explanation: The command prevents port scan attacks. A port scan attack occurs when an attacker sends packets with different port numbers to scan available services. The attack succeeds if a port responds. To prevent this attack, the device internally logs the number of different ports scanned from a single remote source. For example, if a remote host scans 10 ports in 0.005 seconds (equivalent to 5000 microseconds, the default threshold setting), the device flags this behavior as a port scan attack, and rejects further packets from the remote source.

Reference: http://www.juniper.net/techpubs/software/junos-es/junos-es93/junos-es-swcmdref/port-scan.html

QUESTION NO: 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
Explanation:

QUESTION NO: 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
Explanation:

QUESTION NO: 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
Reference: http://www.juniper.fr/techpubs/en_US/junos10.4/topics/example/nat-twice-

configuring.html

http://kb.juniper.net/library/CUSTOMERSERVICE/technotes/Junos_NAT_Examples.pdf

QUESTION NO: 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.

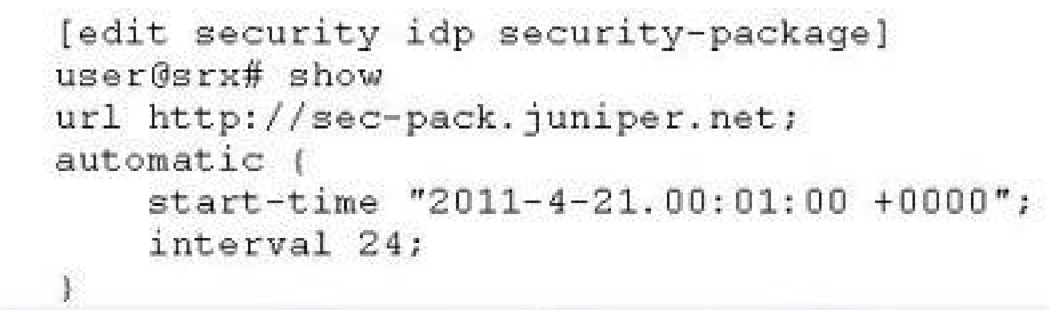
Which VPN design satisfies your manager's concerns?

A. a transparent IPSec VPN
B. a hub-and-spoke VPN
C. a point-to-multipoint VPN
D. a group VPN

Answer: D
Reference: http://juniper.fr/techpubs/software/junos-security/junos-security10.2/junos-security-swconfig-security/topic-45780.html

QUESTION NO: 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
Explanation:

QUESTION NO: 9

You obtained a license file 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. Transfer the file to the SRX firewall using FTP or SCP and install the license with the request system license install-permanent command.

Answer: B
Reference: http://www.juniper.net/techpubs/en_US/junos11.1/topics/reference/command-summary/request-system-license-add.html

QUESTION NO: 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
Reference: http://www.juniper.net/techpubs/en_US/nsm2011.1/topics/task/configuration/attack-signature-attack-object-creating-nsm.html

QUESTION NO: 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. IPSec SA
B. TEK
C. IKE SA

Answer: A
Explanation: The correct answer is: KEK
Introduction to group vpn:
there is three type of rekey methods:
pull methods: using IKE SA and no need for KEK
unicast push methods:using KEK with Ack mechanism
multicast push methods: KEK without Ack mechanism

QUESTION NO: 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
Reference: http://www.juniper.net/techpubs/en_US/junos10.3/topics/usage-guidelines/routing-configuring-filter-based-forwarding.html

QUESTION NO: 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?

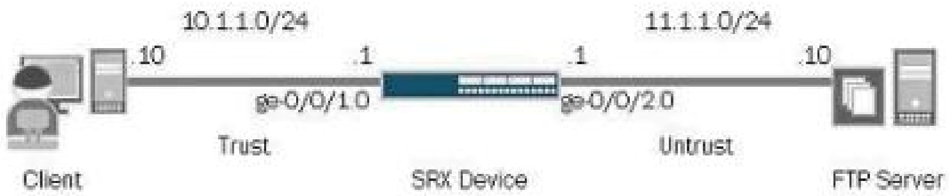
A. Implement firewall filters on each device.
B. Implement an HTTPS-based mesh between all sites.
C. Implement secure routing policies.
D. Implement a hub-and-spoke VPN.

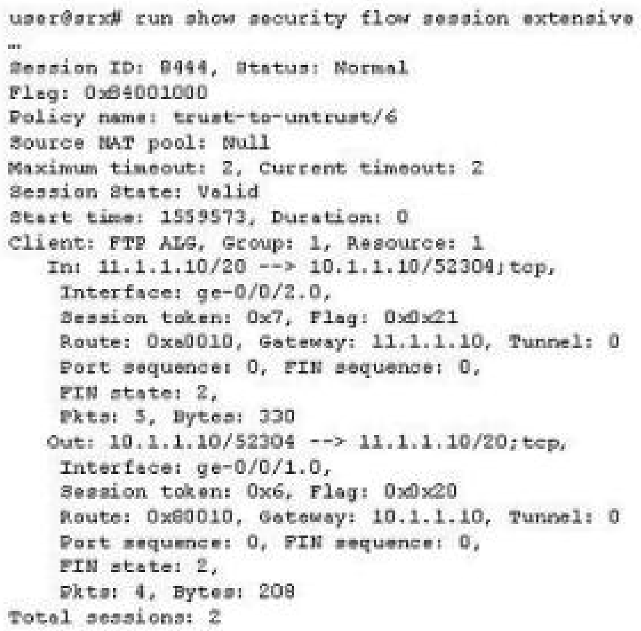
Answer: D
Reference:

http://www.juniper.net/techpubs/en_US/junos11.2/topics/example/vpn-hub-spoke-topologies-one-interface.html

QUESTION NO: 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: 0xa0010, 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: 0x80010, 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

Explanation:

QUESTION NO: 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.