JN0-632

Juniper

Security Profesional(JNCIP-SEC)

Visit: http://www.pass4sureofficial.com/exams.asp?examcode=JN0-632

Pass4sureofficial.com is a reputable IT certification examination guide, study guides and audio exam provider, we not only ensure that you pass your JN0-632 exam in first attempt, but also you can get a high score to acquire Juniper certification.

If you use pass4sureofficial JN0-632 Certification questions and answers, you will experience actual JN0-632 exam questions/answers. We know exactly what is needed and have all the exam preparation material required to pass the exam. Our Juniper exam prep covers over 95% of the questions and answers that may be appeared in your JN0-632 exam. Every point from pass4sure JN0-632 PDF, JN0-632 review will help you take Juniper JN0-632 exam much easier and become Juniper certified. All the Questions/Answers are taken from real exams.

Here's what you can expect from the Pass4sureOfficial Juniper JN0-632 course:

** Up-to-Date Juniper JN0-632 questions taken from the real exam.*
** 100% correct Juniper JN0-632 answers you simply can't find in other JN0-632 courses.*
** All of our tests are easy to download. Your file will be saved as a JN0-632 PDF.*
** Juniper JN0-632 brain dump free content featuring the real JN0-632 test questions.*

Juniper JN0-632 certification exam is of core importance both in your Professional life and Juniper certification path. With Juniper certification you can get a good job easily in the market and get on your path for success. Professionals who passed Juniper JN0-632 exam training are an absolute favorite in the industry. You will pass Juniper JN0-632 certification test and career opportunities will be open for you.

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: 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: 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: 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

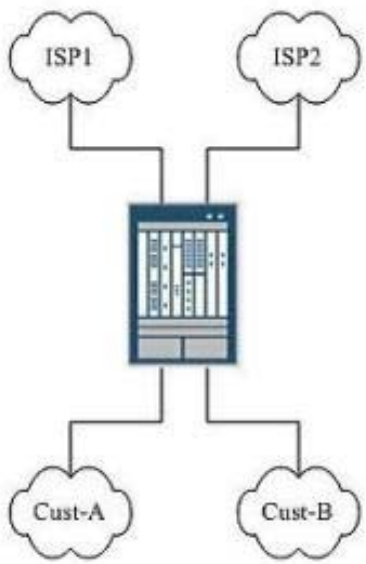
Answer: C

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: 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

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? (Choose two.)

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

Answer: A, C

Explanation:

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: 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: 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

QUESTION: 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. 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

Explanation:

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

QUESTION: 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: 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: D

Explanation:
It's true that Key Encryption Key (KEK) is used to encrypt rekey messages. But in the same time GDOI exchanges in Phase 2 must be protected by ISAKMP Phase 1 Sas. And GDOI groupkey- push exchange is one of the two types of GDOI exchanges: groupkey-pull and groupkey-push.

QUESTION: 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

Pass4SureOfficial.com Lifetime Membership Features;

- Pass4SureOfficial Lifetime Membership Package includes over **2500** Exams.
- **All** exams Questions and Answers are included in package.
- **All** Audio Guides are included **free** in package.
- **All** Study Guides are included **free** in package.
- **Lifetime** login access.
- Unlimited download, no account expiry, no hidden charges, just one time $99 payment.
- **Free updates** for Lifetime.
- **Free Download Access** to All new exams added in future.
- Accurate answers with explanations (If applicable).
- Verified answers researched by industry experts.
- Study Material **updated** on regular basis.
- Questions, Answers and Study Guides are downloadable in **PDF** format.
- Audio Exams are downloadable in **MP3** format.
- **No authorization** code required to open exam.
- **Portable** anywhere.
- 100% success ***Guarantee***.
- **Fast**, helpful support 24x7.

View list of All exams (Q&A) downloads
http://www.pass4sureofficial.com/allexams.asp

View list of All Study Guides (SG) downloads
http://www.pass4sureofficial.com/study-guides.asp

View list of All Audio Exams (AE) downloads
http://www.pass4sureofficial.com/audio-exams.asp

Download All Exams Samples
http://www.pass4sureofficial.com/samples.asp

To purchase $99 Lifetime Full Access Membership click here
http://www.pass4sureofficial.com/purchase.asp

3COM	CompTIA	Filemaker	IBM	LPI	OMG	Sun
ADOBE	ComputerAssociates	Fortinet	IISFA	McAfee	Oracle	Sybase
APC	CWNP	Foundry	Intel	McData	PMI	Symantec
Apple	DELL	Fujitsu	ISACA	Microsoft	Polycom	TeraData
BEA	ECCouncil	GuidanceSoftware	ISC2	Mile2	RedHat	TIA
BICSI	EMC	HDI	ISEB	NetworkAppliance	Sair	Tibco
CheckPoint	Enterasys	Hitachi	ISM	Network-General	SASInstitute	TruSecure
Cisco	ExamExpress	HP	Juniper	Nokia	SCP	Veritas
Citrix	Exin	Huawei	Legato	Nortel	See-Beyond	Vmware
CIW	ExtremeNetworks	Hyperion	Lotus	Novell	SNIA