JN0-520

Juniper

Juniper Networks Certified Internet Associate, FWV

Visit: http://www.pass4sureofficial.com/exams.asp?examcode=JN0-520

Pass4sureofficial.com is a reputable IT certification examination guide, study guides and audio exam provider, we not only ensure that you pass your JN0-520 exam in first attempt, but also you can get a high score to acquire Juniper certification.

If you use pass4sureofficial JN0-520 Certification questions and answers, you will experience actual JN0-520 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 JN0-520 exam. Every point from pass4sure JN0-520 PDF, JN0-520 review will help you take Juniper JN0-520 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 JN0-520 course:

** Up-to-Date Juniper JN0-520 questions taken from the real exam.*
** 100% correct Juniper JN0-520 answers you simply can't find in other JN0-520 courses.*
** All of our tests are easy to download. Your file will be saved as a JN0-520 PDF.*
** Juniper JN0-520 brain dump free content featuring the real JN0-520 test questions.*

Juniper JN0-520 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 JN0-520 exam training are an absolute favorite in the industry. You will pass Juniper JN0-520 certification test and career opportunities will be open for you.

JN0-520

QUESTION 1:

Exhibit

What does this icon indicate?
A.Logging is enabled on a policy
B.Counting is enabled on a policy
C.Scheduling is enabled on a policy
D.Authentication is enabled on policy
E.Address translation is enabled on a policy

Answer: A

Explanation:

Icon	Function	Description
	Permit	The NetScreen device passes all traffic to which the policy applies.
	Deny	The NetScreen device blocks all traffic to which the policy applies.
	Reject	The NetScreen device blocks all traffic to which the policy applies. It drops the packet and sends a TCP reset (RST) segment to the source host for TCP traffic and an ICMP "destination unreachable, port unreachable" message (type 3, code 3) for UDP traffic. For types of traffic other than TCP and UDP, the NetScreen device drops the packet without notifying the source host, which is also what occurs when the action is "deny".
	Policy-level NAT	The NetScreen device performs policy-based source or destination network address translation (NAT-src or NAT-dst) on all traffic to which the policy applies.
	Encapsulation and Decapsulation	The NetScreen device encapsulates all outbound VPN traffic and decapsulates all inbound VPN traffic to which the policy applies.
	Bidirectional VPN policies	A matching VPN policy exists for the opposite direction.
	Authentication	The user must authenticate himself/herself when initiating a connection.
	Antivirus	The NetScreen device sends all traffic to which the policy applies to its internal antivirus (AV) scanner.
	Deep Inspection	The NetScreen device performs Deep Inspection (DI) on all traffic to which the policy applies.
	Deep Inspection and Antivirus	The NetScreen device performs Deep Inspection and antivirus protection on all traffic to which the policy applies.
	URL Filtering	The NetScreen device sends all traffic to which the policy applies to an external URL filtering server.
	L2TP	The NetScreen device encapsulates all outbound L2TP traffic and decapsulates all inbound L2TP traffic to which the policy applies.
	Logging	All traffic is logged and made available for syslog and e-mail, if enabled.
	Counting	The NetScreen device counts (in bytes) the amount of traffic to which the policy applies.
	Alarm	When the amount of traffic surpasses a threshold that you have set, the NetScreen device makes an entry in the traffic log for this policy. Clicking the icon takes you to the traffic log located in the Reports section.

QUESTION 2:

What CLI command puts you into the policy configuration sub-mode, allowing you to add additional entries to the source, destination and/or service fields?
A.set policy id x
B.set multiple id x

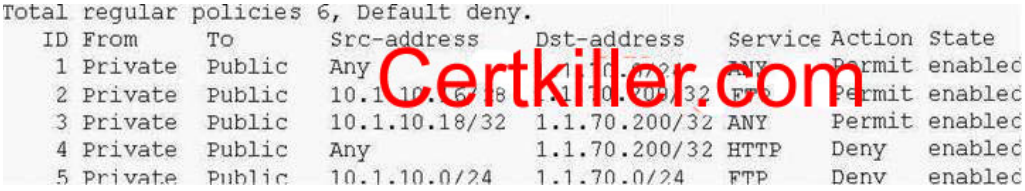
C.set policy id x multiple
D.set policy from trust tountrust 10.10.10.0; 10.10.11.0 anyanypermit

Answer: A

Explanation:
Every policy has an ID number, whether you define one or theNetScreendevice automatically assigns it. You can only define an ID number for a policy through the set policy command in the CLI:set policy idnumber... After you know the ID number, you can enter the policy context to issue further commands to modify the policy. Forexample :
Netscreen-> set policy id 1
Netscreen(policy:1)-> setsrc-address host2

QUESTION 3:

Exhibit



In order for this policy to be effective, what order should the policy statementsbein? The number refers to the Policy ID shown in the diagram.
A.12345
B.34251
C.45321
D.52134
E.53124

Answer: B

Explanation:
TheNetScreendevice checks all attempts to traverse the firewall against policies, beginning with the first one listed in the policy set for the appropriate list and moving through the list. Because theNetScreendevice applies the action specified in the policy to the first matching policy in the list, you must arrange them from the most specific to the most general. Policy ID 3 is the most specific policy because theSrc-address andDst-address have asubnetmaskof 32.So only 1 ip address for the source and 1 ip address for the destination.

QUESTION 4:

Which policy option allows you to view session addresses that have been translated?
A.Logging
B.Counters
C.Schedule
D.Authentication
E.Address translation

Answer: A
Explanations:
When you enable logging in a policy, theNetScreendevice logs all connections to which that particular policy
applies. You can view the logs through either theWebUIor CLI. Logging is a great feature for troubleshooting policies on yournetscreendevice.
IncorrectAnswers:
BWhen you enable counting in a policy, theNetScreendevice counts the total number of bytes of traffic to which this policy applies and records the information in historical graphs.
CBy associating a schedule to a policy, you can determine when the policy is in effect. You can configure schedules on a recurring basis and as a one-time event. Schedules provide a powerful tool in controlling the flow of network traffic and in enforcing network security.
DSelecting this option requires the auth user at the source address to authenticate his/her identity by supplying a user name and password before traffic is allowed to traverse the firewall or enter the VPN tunnel. TheNetScreendevice can use the local database or an external RADIUS,SecurID , or LDAP auth server to perform the authentication check.
ENetScreenprovides several mechanisms for applying network address translation (NAT). The concept of NAT comprises the translation of the IP address in an IP packet header and, optionally, the translation of the port number in the TCP segment or UDP datagram header. The translation can involve the source address (and optionally the source port number), the destination address (and optionally the destination port number), or a combination of translated elements. However you are not able to view translated addresses with this option.

QUESTION 5:

Ac Access Policy must contain which three (3) items?
A.Service
B.Authentication
C.Source address
D.Firewall settings
E.Action (permit, deny, tunnel)

Answer: A, C, E

Explanation:
A policy permits, denies, or tunnels specified types of trafficunidirectionallybetween two points. The type of traffic (or "service"), the location of the two endpoints, and the invoked action compose the basic elements of a policy. Although there can be other components, the required elements, which together constitute the core section of a policy, are as follows:
Direction - The direction of traffic between two security zones (from a source zone to a destination zone)
Source address - The address from which traffic initiates
Destination address - The address to which traffic is sent
Service - The type of traffic transmitted
Action - The action that theNetScreendevice performs when it receives traffic meeting the first

four criteria: deny, permit, reject, or tunnel
For example, the policy stated in the following CLI command permits FTP traffic from any address in the Trust zone to an FTP server named "server1" in the DMZ zone:
setpolicy from trust tountrustany server1 ftp permit
Direction:from trust tountrust(that is, from the Trust zone to theUntrustzone)
Source Address:any(that is, any address in the Trust zone. The term "any" stands for a predefined
addressthat applies to any address in a zone)
Destination Address:server1(a user-defined address in theUntrustzone address book)
Service:ftp(File Transfer Protocol)
Action:permit(thatNetScreendevice permits this traffic to traverse its firewall)

QUESTION 6:

You are trying to remove an address book entry by going to the Address Book -> List display of the Web UI, but you cannot find the remove option. What would cause this problem?
A.An address book entry can only be deleted from the command line interface. You will need to use the CLI to delete it.
B.The address book entry ismisconfigured. You need to correct the address book entry before it will allow you to delete
C.You cannot remove an address book entry from this screen. You need to use the delete option found under the management options screen.
D.The address book entry is being used by a policy. You must delete the policy or remove the address book entry from the policy before it ban be deleted.

Answer: D
Explanation :
Before you can set up many of theNetScreenfirewall, VPN, and traffic shaping features, you need to define
addressesin one or more address lists. The address list for a security zone contains the IP addresses or domain
namesof hosts or subnets whose traffic is either allowed, blocked, encrypted, or user-authenticated.
After you define anaddress.oran address group and associate it with a policy, you cannot change the address location to another zone (such as from Trust toUntrust). To change its location, you must first disassociate it from the underlying policy. Also keep the following in mind regarding to addresslists :
1.When using the CLI, you must create all of your address book entries before you make your policies.
2.You can modify everything about an address book entry except its zone.
3.You can not modify an address object from the CLI, you must first delete it and the recreate it.

QUESTION 7:

Addresses Book entries identify devices such as hosts and networks by their location in

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