Develop Your Abilities and Obtain Juniper JN0-637 Certification Without Difficulty

If you have questions about us, you can contact with us at any time via email or online service. We will give you the best suggestions on the JN0-637 study guide. And you should also trust the official cJN0-637 ertification. Or, you can try it by yourself by free downloading the demos of the JN0-637 learning braindumps. I believe you will make your own judgment. We are very confident in our JN0-637 exam questions.

Juniper JN0-637 Exam Syllabus Topics:

Topic	Details
Topic 1	• Logical Systems and Tenant Systems: This topic of the exam explores the concepts and functionalities of logical systems and tenant systems.
Topic 2	• Advanced Policy-Based Routing (APBR): This topic emphasizes on advanced policy-based routing concepts and practical configuration or monitoring tasks.
Topic 3	• Advanced IPsec VPNs: Focusing on networking professionals, this part covers advanced IPsec VPN concepts and requires candidates to demonstrate their skills in real-world applications.
Topic 4	• Multinode High Availability (HA): In this topic, aspiring networking professionals get knowledge about multinode HA concepts. To pass the exam, candidates must learn to configure or monitor HA systems.

>> Exam Cram JN0-637 Pdf <<

Free PDF Juniper - Reliable Exam Cram JN0-637 Pdf

Although the Juniper JN0-637 exam prep is of great importance, you do not need to be over concerned about it. With scientific review and arrangement from professional experts as your backup, and the most accurate and high quality content of our Juniper

JN0-637 Study Materials, you will cope with it like a piece of cake. So our JN0-637 learning questions will be your indispensable practice materials during your way to success.

Juniper Security, Professional (JNCIP-SEC) Sample Questions (Q119-Q124):

NEW QUESTION # 119
Which two types of source NAT translations are supported in this scenario? (Choose two.)

- A. translation of one IPv6 subnet to another IPv6 subnet without port address translation
- B. translation of one IPv4 subnet to one IPv6 subnet with port address translation
- C. translation of one IPv6 subnet to another IPv6 subnet with port address translation
- D. translation of IPv4 hosts to IPv6 hosts with or without port address translation

Answer: B,D

NEW QUESTION # 120
You are attempting to ping an interface on your SRX Series device, but the ping is unsuccessful.
What are three reasons for this behavior? (Choose three.)

- A. The device has J-Web enabled.
- B. The interface is not assigned to a security zone.
- C. The interface's host-inbound-traffic security zone configuration does not permit ping
- D. The interface has multiple logical units configured.
- E. The ping traffic is matching a firewall filter.

Answer: B,C,E

Explanation:
A: The interface is not assigned to a security zone.
* Explanation: SRX Series devices rely heavily on security zones for traffic management. If an interface isn't assigned to a zone, the device won't know how to handle traffic arriving on that interface, including ping requests (ICMP echo requests).

NEW QUESTION # 121
A company has acquired a new branch office that has the same address space as one of its local networks, 192.168.100.0/24. The offices need to communicate with each other. Which two NAT configurations will satisfy this requirement? (Choose two.)

- A. [edit security nat source]
  user@OfficeA# show rule-set OfficeBtoA {
  from zone OfficeB;
  to zone OfficeA;
  rule 1 {
  match {
  source-address 192.168.210.0/24;
  destination-address 192.168.200.0/24;
  }
  then {
  source-nat { interface; }
  }
  }
  }
- B. [edit security nat source]
  user@OfficeB# show rule-set OfficeAtoB {
  from zone OfficeA;
  to zone OfficeB;
  rule 1 {
  match {
  source-address 192.168.200.0/24;
  destination-address 192.168.210.0/24;

}
then {
source-nat { interface; }
}
}
}

- C. [edit security nat static]
  user@OfficeB# show rule-set From-Office-A {
  from interface ge-0/0/0.0;
  rule 1 {
  match {
  destination-address 192.168.210.0/24;
  }
  then {
  static-nat {
  prefix { 192.168.100.0/24; }
  }
  }
  }
  }
- D. [edit security nat static]
  user@OfficeA# show rule-set From-Office-B {
  from interface ge-0/0/0.0;
  rule 1 {
  match {
  destination-address 192.168.200.0/24;
  }
  then {
  static-nat {
  prefix { 192.168.100.0/24; }
  }
  }
  }
  }

Answer: C,D

NEW QUESTION # 122
A company has acquired a new branch office that has the same address space of one of its local networks, 192.168.100/24. The offices need to communicate with each other. Which two NAT configurations will satisfy this requirement? (Choose two.)

- A. [edit security nat source]
  user@OfficeB# show rule-set OfficeAtoB {
  from zone OfficeA;
  to zone OfficeB;
  rule 1 {
  match {
  source-address 192.168.200.0/24;
  destination-address 192.168.210.0/24;
  }
  then {
  source-nat {
  interface;
  }
  }
  }
  }
- B. [edit security nat static]
  user@OfficeB# show rule-set From-Office-A {
  from interface ge-0/0/0.0;

rule 1 {
match {
destination-address 192.168.210.0/24;
}
then {
static-nat {
prefix 192.168.100.0/24;
}
}
}
}

- C. [edit security nat static]
  user@OfficeA# show rule-set From-Office-B {
  from interface ge-0/0/0.0;
  rule 1 {
  match {
  destination-address 192.168.200.0/24;
  }
  then {
  static-nat {
  prefix 192.168.100.0/24;
  }
  }
  }
  }
- D. [edit security nat source]
  user@OfficeA# show rule-set OfficeBtoA {
  from zone OfficeB;
  to zone OfficeA;
  rule 1 {
  match {
  source-address 192.168.210.0/24;
  destination-address 192.168.200.0/24;
  }
  then {
  source-nat {
  interface;
  }
  }
  }
  }

Answer: A,D

Explanation:
The problem describes two offices needing to communicate, but both share the same IP address space, 192.168.100.0/24. To resolve this, NAT must be configured to translate the conflicting address spaces on each side. Here's how each of the configurations works:
Option A (Correct):
This source NAT rule translates the source address of traffic from Office B to Office A. By configuring source NAT, the source IP addresses from Office B (192.168.210.0/24) will be translated when communicating with Office A (192.168.200.0/24). This method ensures that there is no overlap in address space when packets are transmitted between the two offices.
Option D (Correct):
This is a source NAT rule configured on Office B, which translates the source addresses from Office A to prevent address conflicts. It ensures that when traffic is initiated from Office A to Office B, the overlapping address range (192.168.100.0/24) is translated.

NEW QUESTION # 123
Which two security intelligence feed types are supported?

- A. infected host feed

- B. Command and Control feed
- C. custom feeds
- D. malicious URL feed

Answer: A,C

Explanation:
The two security intelligence feed types that are supported are:
A) Infected host feed. An infected host feed is a security intelligence feed that contains the IP addresses of hosts that are infected by malware or compromised by attackers. The SRX Series device can download the infected host feed from the Juniper ATP Cloud or generate its own infected host feed based on the detection events from IDP. The SRX Series device can use the infected host feed to block or quarantine the traffic to or from the infected hosts based on the security policies1.
B) Command and Control feed. A command and control feed is a security intelligence feed that contains the IP addresses of servers that are used by malware or attackers to communicate with infected hosts.
The SRX Series device can download the command and control feed from the Juniper ATP Cloud or generate its own command and control feed based on the detection events from IDP. The SRX Series device can use the command and control feed to block or log the traffic to or from the command and control servers based on the security policies2.
The other options are incorrect because:
C) Custom feeds. Custom feeds are not a security intelligence feed type, but a feature that allows you to create your own security intelligence feeds based on your own criteria and sources. You can configure custom feeds by using the Junos Space Security Director or the CLI. Custom feeds are not supported by the Juniper ATP Cloud or the IDP3.
D) Malicious URL feed. Malicious URL feed is not a security intelligence feed type, but a feature that allows you to block or log the traffic to or from malicious URLs based on the security policies. The SRX Series device can download the malicious URL feed from the Juniper ATP Cloud or the Juniper Threat Labs. Malicious URL feed is not supported by the IDP4.
Reference: Infected Host Feed Overview Command and Control Feed Overview Custom Feed Overview Malicious URL Feed Overview

NEW QUESTION # 124
.....

Our JN0-637 guide torrent specially proposed different versions to allow you to learn not only on paper, but also to use mobile phones to learn. This greatly improves the students' availability of fragmented time. You can choose the version of JN0-637 learning materials according to your interests and habits. And if you buy the value pack, you have all of the three versions, the price is quite preferential and you can enjoy all of the study experiences. This means you can study JN0-637 Exam Engine anytime and anyplace for the convenience to help you pass the JN0-637 exam.

- kursy.cubeweb.iqhs.pl, onlinecourse.gooninstitute.com, wellbii.online, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, stancoo822.designertoblog.com, raywalk191.onesmablog.com, motionentrance.edu.np, www.stes.tyc.edu.tw, learnfrencheasy.com, stancoo822.onesmablog.com, Disposable vapes