Juniper - Professional JN0-637 Authentic Exam Questions

2025 Latest Actual4test JN0-637 PDF Dumps and JN0-637 Exam Engine Free Share: https://drive.google.com/open?id=1sXJmSLLtu49QfzLY_5pEuDWIX5XFK0PS

The purpose of our product is to let the clients master the JN0-637 quiz torrent and not for other illegal purposes. Our system is well designed and any person or any organization has no access to the information of the clients. So please believe that we not only provide the best JN0-637 test prep but also provide the best privacy protection. Take it easy. If you really intend to pass the JN0-637 Exam, our software will provide you the fast and convenient learning and you will get the best study materials and get a very good preparation for the exam. The content of the JN0-637 guide torrent is easy to be mastered and has simplified the important information.

Juniper JN0-637 Exam Syllabus Topics:

Topic	Details
Topic 1	• Troubleshooting Security Policies and Security Zones: This topic assesses the skills of networking professionals in troubleshooting and monitoring security policies and zones using tools like logging and tracing.
Topic 2	• Logical Systems and Tenant Systems: This topic of the exam explores the concepts and functionalities of logical systems and tenant systems.
Topic 3	• Automated Threat Mitigation: This topic covers Automated Threat Mitigation concepts and emphasizes implementing and managing threat mitigation strategies.
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.
Topic 5	• Advanced Policy-Based Routing (APBR): This topic emphasizes on advanced policy-based routing concepts and practical configuration or monitoring tasks.

Topic 6	- Advanced Network Address Translation (NAT): This section evaluates networking professionals' expertise in advanced NAT functionalities and their ability to manage complex NAT scenarios.
Topic 7	- 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.

>> JN0-637 Authentic Exam Questions <<

Valid Exam JN0-637 Preparation | JN0-637 Exam Sample Questions

The advantages of our JN0-637 cram guide is plenty and the price is absolutely reasonable. The clients can not only download and try out our products freely before you buy them but also enjoy the free update and online customer service at any time during one day. The clients can use the practice software to test if they have mastered the JN0-637 Test Guide and use the function of stimulating the test to improve their performances in the real test. So our products are absolutely your first choice to prepare for the test JN0-637 certification.

Juniper Security, Professional (JNCIP-SEC) Sample Questions (Q82-Q87):

NEW QUESTION # 82
In an effort to reduce client-server latency transparent mode was enabled an SRX series device.
Which two types of traffic will be permitted in this scenario? (Choose Two)

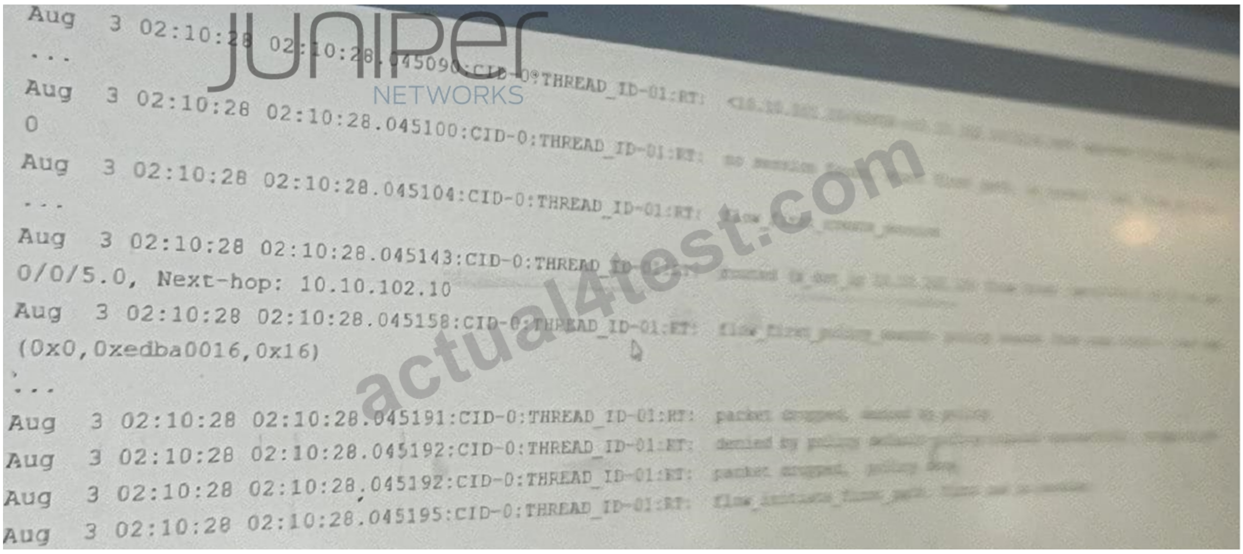
- A. Layer 2 non-IP multicast
- B. BGP
- C. ARP
- D. IPsec

Answer: A,C

Explanation:
To answer this question, you need to know what transparent mode is and what types of traffic it permits.
Transparent mode is a mode of operation for SRX Series devices that provides Layer 2 bridging capabilities with full security services. In transparent mode, the SRX Series device acts as a bridge between two network segments and inspects the packets without modifying the source or destination information in the IP packet header. The SRX Series device does not have an IP address in transparent mode, except for the management interface1.
Therefore, the types of traffic that will be permitted in transparent mode are:
A) ARP (Address Resolution Protocol) traffic. ARP is a protocol that maps IP addresses to MAC addresses. ARP traffic is a type of Layer 2 traffic that does not require an IP address on the SRX Series device. ARP traffic is permitted in transparent mode to allow the SRX Series device to learn the MAC addresses of the hosts on the bridged network segments2.
B) Layer 2 non-IP multicast traffic. Layer 2 non-IP multicast traffic is a type of traffic that uses MAC addresses to send data to multiple destinations. Layer 2 non-IP multicast traffic does not require an IP address on the SRX Series device. Layer 2 non-IP multicast traffic is permitted in transparent mode to allow the SRX Series device to forward data to the appropriate destinations on the bridged network segments3.
The other options are incorrect because:
C) BGP (Border Gateway Protocol) traffic. BGP is a protocol that exchanges routing information between autonomous systems. BGP traffic is a type of Layer 3 traffic that requires an IP address on the SRX Series device. BGP traffic is not permitted in transparent mode, because the SRX Series device does not have an IP address in transparent mode, except for the management interface1.
D) IPsec (Internet Protocol Security) traffic. IPsec is a protocol that provides security and encryption for IP packets. IPsec traffic is a type of Layer 3 traffic that requires an IP address on the SRX Series device.
IPsec traffic is not permitted in transparent mode, because the SRX Series device does not have an IP address in transparent mode, except for the management interface1.
Reference: Transparent Mode Overview
ARP Support in Transparent Mode
Layer 2 Non-IP Multicast Traffic Support in Transparent Mode

NEW QUESTION # 83

Exhibit:



```
Aug  3 02:10:28 02:10:28.045090:CID-0:THREAD_ID-01:RT: <10.10.101.[illegible]
...
Aug  3 02:10:28 02:10:28.045100:CID-0:THREAD_ID-01:RT: no session found [illegible]
0
Aug  3 02:10:28 02:10:28.045104:CID-0:THREAD_ID-01:RT: flow_first_create_session
...
Aug  3 02:10:28 02:10:28.045143:CID-0:THREAD_ID-01:RT: [illegible]
0/0/5.0, Next-hop: 10.10.102.10
Aug  3 02:10:28 02:10:28.045158:CID-0:THREAD_ID-01:RT: flow_first_policy_search: policy search [illegible]
(0x0,0xedba0016,0x16)
...
Aug  3 02:10:28 02:10:28.045191:CID-0:THREAD_ID-01:RT: packet dropped, denied by policy
Aug  3 02:10:28 02:10:28.045192:CID-0:THREAD_ID-01:RT: denied by policy default-policy-[illegible]
Aug  3 02:10:28 02:10:28.045192:CID-0:THREAD_ID-01:RT: packet dropped, policy deny
Aug  3 02:10:28 02:10:28.045195:CID-0:THREAD_ID-01:RT: flow_initiate_first_path: [illegible]
```

Which two statements are correct about the output shown in the exhibit. (Choose Two)

- A. The packet is dropped by the default security policy.
- B. The packet is dropped by a configured security policy.
- C. The data shown requires a traceoptions flag of basic-datapath.
- D. The data shown requires a traceoptions flag of host-traffic.

Answer: A,C

NEW QUESTION # 84

You are deploying threat remediation to endpoints connected through third-party devices.
In this scenario, which three statements are correct? (Choose three.)

- A. The RADIUS server sends Status-Server messages to update infected host information to the connector.
- B. The connector queries the RADIUS server for the infected host endpoint details and initiates a change of authorization (CoA) for the infected host.
- C. The connector uses an API to gather endpoint MAC address information from the RADIUS server.
- D. All third-party switches in the specified network are automatically mapped and registered with the RADIUS server.
- E. All third-party switches must support AAA/RADIUS and Dynamic Authorization Extensions to the RADIUS protocol.

Answer: B,C,E

Explanation:
For threat remediation in a third-party network, the RADIUS protocol is necessary to communicate with the RADIUS server for details about infected hosts. CoA enables security measures to be enforced based on endpoint information provided by the RADIUS server. Details on this setup can be found in Juniper RADIUS and AAA Documentation.
When deploying threat remediation to endpoints connected through third-party devices, such as switches, the following conditions must be met for proper integration and functioning:
* Explanation of Answer A (Support for AAA/RADIUS and Dynamic Authorization Extensions):
* Third-party switches must supportAAA (Authentication, Authorization, and Accounting)and RADIUSwithDynamic Authorization Extensions. These extensions allow dynamic updates to be made to a session's authorization parameters, which are essential for enforcing access control based on threat detection.
* Explanation of Answer B (Connector Gathers MAC Information via API):
* Theconnectoruses an API to gather MAC address information from theRADIUS server. This MAC address data is necessary to identify and take action on infected hosts or endpoints.
* Explanation of Answer D (Connector Initiates CoA):
* Theconnectorqueries the RADIUS server for infected host details and triggers aChange of Authorization (CoA)for the infected host. The CoA allows the connector to dynamically alter the host's access permissions or isolate the infected host based on its threat status.
Juniper Security Reference:
* Threat Remediation via RADIUS: Dynamic remediation actions, such as CoA, can be taken based on information received from

the RADIUS server regarding infected hosts. Reference: Juniper RADIUS and CoA Documentation.

NEW QUESTION # 85

You have deployed an SRX Series device at your network edge to secure Internet-bound sessions for your local hosts using source NAT. You want to ensure that your users are able to interact with applications on the Internet that require more than one TCP session for the same application session.
Which two features would satisfy this requirement? (Choose two.)

- A. double NAT
- B. persistent NAT
- C. address persistence
- D. STUN

Answer: B,C

Explanation:
Address persistence ensures that the same NAT IP address is used for all sessions originating from a single source IP. Persistent NAT maintains connections for applications needing multiple sessions, like VoIP.
Additional details are available in Juniper NAT Documentation.
For applications that require multiple TCP sessions for the same application session (such as VoIP or certain online games), the SRX device needs to handle NAT properly to maintain session continuity. Here's what helps:
* Address Persistence (Answer A): Address persistence ensures that multiple sessions initiated by the same internal host are mapped to the same external IP address. This is crucial for applications that use multiple TCP sessions to maintain a stateful connection with the external server.
Command Example:
bash
Copy code

```
set security nat source persistent-nat address-persistence
```

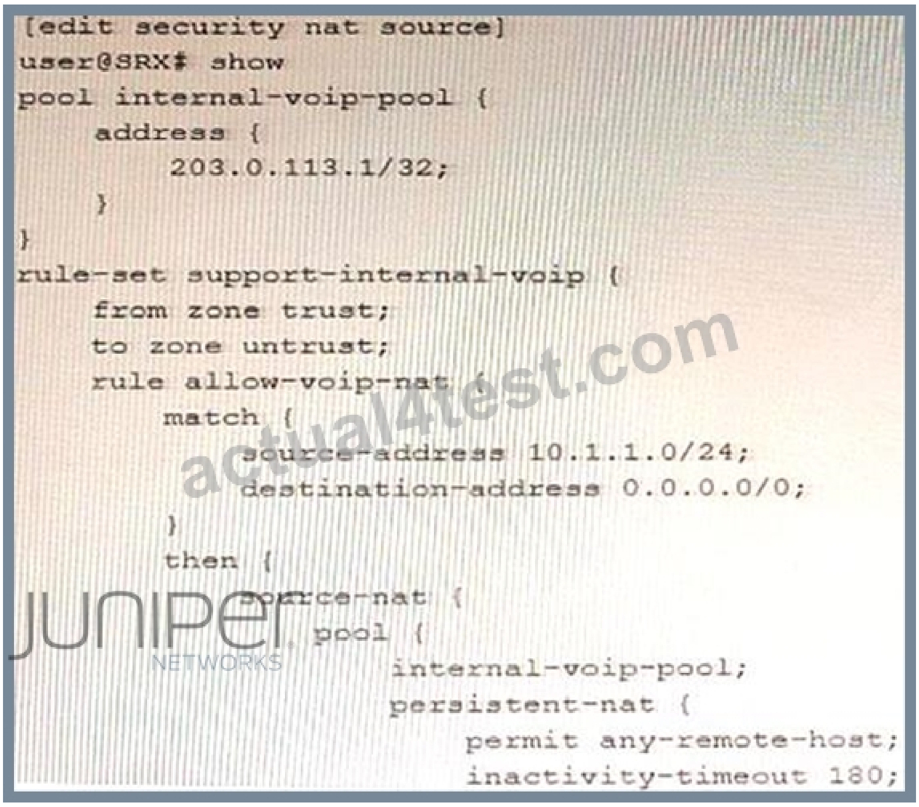
* Persistent NAT (Answer C): This feature allows the external server to initiate new connections to the internal client using the same NAT translation. It's essential for applications that require consistent NAT mappings across multiple sessions.
Command Example:
bash
Copy code

```
set security nat source persistent-nat permit target-host-port
```

These features ensure that applications with multiple TCP sessions work seamlessly across NAT.

NEW QUESTION # 86

Exhibit



```
[edit security nat source]
user@SRX# show
pool internal-voip-pool {
    address {
        203.0.113.1/32;
    }
}
rule-set support-internal-voip {
    from zone trust;
    to zone untrust;
    rule allow-voip-nat {
        match {
            source-address 10.1.1.0/24;
            destination-address 0.0.0.0/0;
        }
        then {
            source-nat {
                pool {
                    internal-voip-pool;
                    persistent-nat {
                        permit any-remote-host;
                        inactivity-timeout 180;
```

Referring to the exhibit, an internal host is sending traffic to an Internet host using the 203.0.113.1 reflexive address with source port 54311.
Which statement is correct in this situation?

- A. Only the Internet host that the internal host originally communicated with can initiate traffic to reach the internal host using the 203.0.113.1 address, source port 54311, and a random destination port.
- B. Only the Internet host that the internal host originally communicated with can initiate traffic to reach the internal host using the 203.0 113.1 address, a random source port, and destination port 54311.
- C. Any host on the Internet can initiate traffic to reach the internal host using the 203.0.113.1 address, source port 54311, and a random destination port.
- D. Any host on the Internet can initiate traffic to reach the internal host using the 203.0.113.1 address, a random source port, and destination port54311.

Answer: C

NEW QUESTION # 87

......

As we all know, practice makes perfect. It's also applied into preparing for the exam. JN0-637 training materials of us contain both quality and quantity, and you will get enough practice if you choose us. In addition, JN0-637 exam cram cover most of the knowledge points for the exam, and you can master the major knowledge points for the exam as well as improve your professional ability in the process of learning. We are pass guarantee and money back guarantee if you fail to pass your exam by using JN0-637 Exam Dumps of us. Online and offline service are available by us, if you have any questions, you can consult us.

- Free PDF Quiz Juniper - Pass-Sure JN0-637 Authentic Exam Questions ✴ Simply search for □ JN0-637 □ for free download on 「 www.practicevce.com 」 □Exam JN0-637 Tests
- Free PDF Quiz Juniper - Pass-Sure JN0-637 Authentic Exam Questions ↗ Simply search for " JN0-637 " for free download on [www.pdfvce.com] □Exam JN0-637 Tests
- JN0-637 Reliable Dumps □ JN0-637 Reliable Dumps □ JN0-637 Reliable Dumps □ Download 【 JN0-637 】 for free by simply entering ➽ www.dumpsquestion.com □ website □Reliable JN0-637 Braindumps
- JN0-637 Authentic Exam Questions has 100% pass rate, Security, Professional (JNCIP-SEC) □ Enter □ www.pdfvce.com □ and search for { JN0-637 } to download for free □JN0-637 Valid Exam Blueprint
- Selecting The JN0-637 Authentic Exam Questions Means that You Have Passed Security, Professional (JNCIP-SEC) □ Open □ www.examcollectionpass.com □ enter ▹ JN0-637 ◃ and obtain a free download □JN0-637 Reliable Dumps
- JN0-637 Exam Learning □ JN0-637 Vce Torrent □ JN0-637 Vce Torrent □ Easily obtain free download of ⇛ JN0-637 ⇚ by searching on ➽ www.pdfvce.com □ □Training JN0-637 Material
- Pass Guaranteed Quiz Trustable Juniper - JN0-637 - Security, Professional (JNCIP-SEC) Authentic Exam Questions □ 「 www.prepawaypdf.com 」 is best website to obtain ➠ JN0-637 □ for free download □Valid JN0-637 Exam Forum
- 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, webanalyticsbd.com, shortcourses.russellcollege.edu.au, 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, www.stes.tyc.edu.tw, 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, myportal.utt.edu.tt, www.stes.tyc.edu.tw, xpertable.com, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, Disposable vapes

DOWNLOAD the newest Actual4test JN0-637 PDF dumps from Cloud Storage for free: https://drive.google.com/open?id=1sXJmSLLtu49QfzLY_5pEuDWIX5XFK0PS