Test JN0-637 Dump | Reliable JN0-637 Exam Question

P.S. Free & New JN0-637 dumps are available on Google Drive shared by Test4Engine: https://drive.google.com/open?id=1oGjRPc4kMGrZ9pbeBaI12IK6_m4lpbDD

Where can you purchase the best quality and cheapest JN0-637 exam dumps? Test4Engine will meet all examinees'needs with cheaper price and high quality JN0-637 exam dumps and answers. The sales of JN0-637 certification training materials on Test4Engine site is in front of the same work areas. The passing rate of our JN0-637 VCE Dumps is 100%. In a word, choosing Test4Engine for you to pass JN0-637 test is equal to choose success.

Juniper JN0-637 Exam Syllabus Topics:

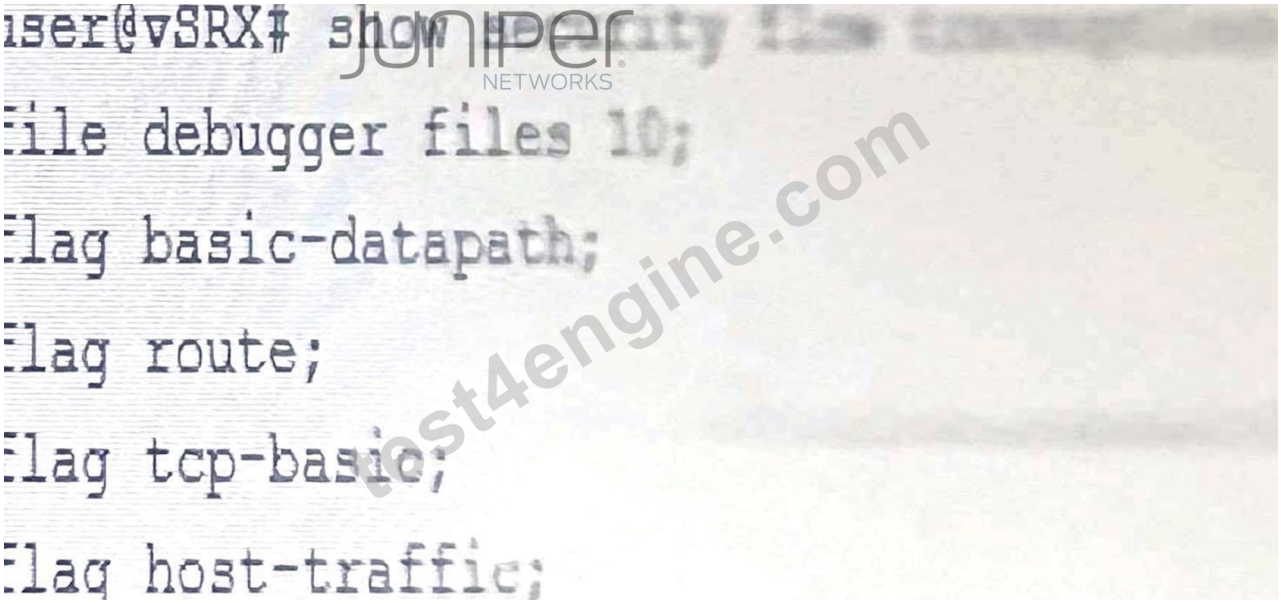
Topic	Details
Topic 1	• Advanced IPsec VPNs: Focusing on networking professionals, this part covers advanced IPsec VPN concepts and requires candidates to demonstrate their skills in real-world applications.
Topic 2	• Advanced Policy-Based Routing (APBR): This topic emphasizes on advanced policy-based routing concepts and practical configuration or monitoring tasks.
Topic 3	• Automated Threat Mitigation: This topic covers Automated Threat Mitigation concepts and emphasizes implementing and managing threat mitigation strategies.
Topic 4	• Advanced Network Address Translation (NAT): This section evaluates networking professionals' expertise in advanced NAT functionalities and their ability to manage complex NAT scenarios.

Reliable Juniper JN0-637 Exam Question - Examcollection JN0-637 Questions Answers

Of course, when we review a qualifying exam, we can't be closed-door. We should pay attention to the new policies and information related to the test JN0-637 certification. For the convenience of the users, the JN0-637 test materials will be updated on the homepage and timely update the information related to the qualification examination. Annual qualification examination, although content broadly may be the same, but as the policy of each year, the corresponding examination pattern grading standards and hot spots will be changed, the JN0-637 Test Prep can help users to spend the least time to pass the exam.

Juniper Security, Professional (JNCIP-SEC) Sample Questions (Q14-Q19):

NEW QUESTION # 14
Exhibit:



The security trace options configuration shown in the exhibit is committed to your SRX series firewall.
Which two statements are correct in this Scenario? (Choose Two)

- A. The file debugger will be readable by all users.
- B. The file debugger will be readable only by the user who committed this configuration
- C. Once the trace has generated 10 log files, older logs will be overwritten.
- D. Once the trace has generated 10 log files, the trace process will halt.

Answer: C,D

Explanation:
Once the trace has generated 10 log files, older logs will be overwritten. - This is generally true if the configuration includes a file count limit and the 'world-readable' flag. Without the 'world-readable' flag, only the file's owner or superuser can read the file. If the 'no-world-readable' flag is set, only the user that created the file and root can read it.
Once the trace has generated 10 log files, the trace process will halt. - This would be true only if the 'files' statement is used without the 'world-readable' or 'no-world-readable' flag. If 'no-world-readable' is set, the trace files are not readable by all users.

NEW QUESTION # 15
Exhibit:

```
Aug  3 02:10:28 02:10:28.045090:CID-0:THREAD_ID-01:RT:  <10.10.101.10/60858->10.10.102.10/22;6,0x0> matched filter filter-1:
...
Aug  3 02:10:28 02:10:28.045100:CID-0:THREAD_ID-01:RT:  no session found, start first path. in_tunnel - 0x0, from_cp_flag -
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:  routed (x_dst_ip 10.10.102.10) from trust (ge-0/0/4.0 in 0) to ge-
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 from zone trust-> zone dmz
(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-logical-system-00(2), dropping pkt
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: first pak no session
```


Referring to the flow logs exhibit, which two statements are correct? (Choose two.)

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

Answer: C,D

Explanation:
* Understanding the Flow Log Output:
From the flow logs in the exhibit, we can observe the following key events:
* The session creation was initiated (flow_first_create_session), but the policy searchfailed (flow_first_policy_search), which implies that no matching policy was found between the zones involved (zone trust-> zone dmz).
* The packet was dropped with the reason "denied by policy." This shows that the packet was dropped either due to no matching security policy or because the default policy denies the traffic (packet dropped, denied by policy).
* The line denied by policy default-policy-logical-system-00(2) indicates that the default security policy is responsible for denying the traffic, confirming that no explicit security policy was configured to allow this traffic.
* Explanation of Answer A (Dropped by the default security policy):
The log message clearly states that the packet was dropped by the default security policy (default-policy- logical-system-00). In Junos, when a session is attempted between two zones and no explicit policy exists to allow the traffic, the default policy is to deny the traffic. This is a common behavior in Junos OS when a security policy does not explicitly allow traffic between zones.
* Explanation of Answer D (Requires traceoptions flag of basic-datapath):
The information displayed in the log involves session creation, flow policy search, and packet dropping due to policy violations, which are all part of basic packet processing in the data path. This type of information is logged when the traceoptions flag is set tobasic-datapath. The basic-datapath traceoption provides detailed information about the forwarding process, including policy lookups and packet drops, which is precisely what we see in the exhibit.
* The traceoptions flaghost-traffic(Answer C) is incorrect because host-traffic is typically used for traffic destined to or generated from the Junos device itself (e.g., SSH or SNMP traffic to the SRX device), not for traffic passing through the device.
* To capture flow processing details like those shown, you need the basic-datapath traceoptions flag, which provides details about packet forwarding and policy evaluation.
Step-by-Step Configuration for Tracing (Basic-Datapath):
* Enable flow traceoptions:
To capture detailed information about how traffic is being processed, including policy lookups and flow session creation, enable traceoptions for the flow.
bash

Copy code
set security flow traceoptions file flow-log
set security flow traceoptions flag basic-datapath
* Apply the configuration and commit:
bash
Copy code
commit
* View the logs:
Once enabled, you can check the trace logs for packet flows, policy lookups, and session creation details:
bash
Copy code
show log flow-log
This log will contain information similar to the exhibit, including session creation attempts and packet drops due to security policy.
Juniper Security Reference:
* Default Security Policies: Juniper SRX devices have a default security policy to deny all traffic that is not explicitly allowed by user-defined policies. This is essential for security best practices. Reference:
Juniper Networks Documentation on Security Policies.
* Traceoptions for Debugging Flows: Using traceoptions is crucial for debugging and understanding how traffic is handled by the SRX, particularly when issues arise from policy misconfigurations or routing. Reference: Juniper Traceoptions.
By using the basic-datapath traceoptions, you can gain insights into how the device processes traffic, including policy lookups, route lookups, and packet drops, as demonstrated in the exhibit.

NEW QUESTION # 16
Exhibit:

```
[edit routing-instances]
user@vSRX-1# show
APBR-1 {
    routing-options {
        static {
            route 0.0.0.0/0 next-hop 172.16.9.2;
        }
    }
}
[edit routing-options]
user@vSRX-1# show
interface-routes {
    rib-group inet APBR-group;
}
static {
    route 0.0.0.0/0 next-hop 192.168.101.1;
}
rib-groups {
    APBR-group {
        import-rib [ inet.0 APBR-1.inet.0 ];
    }
}
[edit security advance-policy-based-routing]
user@vSRX-1# show
profile APBR-profile {
    rule ssh {
        match {
```

Exhibit

```
        import-rib [ inet.0 APBR-1.inet.0 ];
    }
}
[edit security advance-policy-based-routing]
user@vSRX-1# show
profile APBR-profile {
    rule ssh {
        match {
            dynamic-application junos:SSH;
        }
        then {
            routing-instance APBR-1;
        }
    }
}
from-zone DC9-zone {
    policy move-ssh {
        match {
            source-address any;
            destination-address any;
            application any;
        }
        then {
            application-services {
                advance-policy-based-routing-profile APBR-profile;
            }
        }
    }
```


You are having problems configuring advanced policy-based routing.
What should you do to solve the problem?

- A. Change the routing instance to a virtual router instance.
- B. Remove the default static route from the main instance configuration.
- C. Change the routing instance to a forwarding instance.
- D. Apply a policy to the APBR RIB group to only allow the exact routes you need.

Answer: C

NEW QUESTION # 17
You are asked to deploy Juniper atp appliance in your network. You must ensure that incidents and alerts are sent to your SIEM. In this scenario, which logging output format is supported?

- A. binay
- B. WELF
- C. JSON
- D. CEF

Answer: D

Explanation:
The Juniper ATP Appliance platform collects, inspects and analyzes advanced and stealthy web, file, and email-based threats that exploit and infiltrate client browsers, operating systems, emails and applications. Juniper ATP Appliance's detection of malicious attacks generates incident and event details that can be sent to connected SIEM platforms in CEF, LEEF or Syslog formats1. CEF (Common Event Format) is an open log management standard that improves the interoperability of security-related information from different vendors2. Juniper ATP Appliance supports CEF format for sending events and system audit notifications to SIEM servers. You can configure the CEF format in the Juniper ATP Appliance Central Manager WebUI Config > Notifications > SIEM Settings1. Therefore, the correct answer is C. CEF is a supported logging output format for Juniper ATP Appliance.
The other options are incorrect because:
A) WELF (WebTrends Enhanced Log Format) is a proprietary log format developed by WebTrends Corporation for web analytics3. Juniper ATP Appliance does not support WELF format for SIEM integration.
B) JSON (JavaScript Object Notation) is a lightweight data-interchange format that is easy for humans and machines to read and write4. Juniper ATP Appliance supports JSON format for HTTP API results, but not for SIEM notifications1.
D) Binary is a numeric system that uses only two digits: 0 and 1. Binary is not a logging output format for Juniper ATP Appliance or any SIEM platform.

Reference: SIEM Syslog, LEEF and CEF Logging
Common Event Format Configuration Guide
WebTrends Enhanced Log Format
JSON

NEW QUESTION # 18
Your IPsec tunnel is configured with multiple security associations (SAs). Your SRX Series device supports the CoS-based IPsec VPNs with multiple IPsec SAs feature. You are asked to configure CoS for this tunnel.
Which two statements are true in this scenario? (Choose two.)

- A. The local and remote gateways must have the forwarding classes defined in the same order.
- B. A maximum of eight forwarding classes can be configured for a VPN with the multi-sa forwarding- classes statement.
- C. A maximum of four forwarding classes can be configured for a VPN with the multi-sa forwarding- classes statement.
- D. The local and remote gateways do not need the forwarding classes to be defined in the same order.

Answer: B,D

Explanation:
Explanation:

NEW QUESTION # 19
.....

Our company is a well-known multinational company, has its own complete sales system and after-sales service worldwide. In the same trade at the same time, our JN0-637 real study dumps have become a critically acclaimed enterprise, so, if you are preparing for the exam qualification and obtain the corresponding certificate, so our company launched JN0-637 exam questions are the most reliable choice of you. The service tenet of our company and all the staff work mission is: through constant innovation and providing the best quality service, make the JN0-637 question guide become the best customers electronic test study materials. No matter where you are, as long as you buy the JN0-637 real study dumps, we will provide you with the most useful and efficient learning materials. As you can see, the advantages of our research materials are as follows.

What's more, part of that Test4Engine JN0-637 dumps now are free: https://drive.google.com/open?id=1oGjRPc4kMGrZ9pbeBaI12IK6_m4lpbDD