Leads4Pass
https://www.leads4pass.com/jn0-636.html

JN0-636 ^{Q&As}

JN0-636^{Q&As}

Service Provider Routing and Switching Professional (JNCIP-SP)

Pass Juniper JN0-636 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.leads4pass.com/jn0-636.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Juniper
Official Exam Center

⚙ **Instant Download** After Purchase

⚙ **100% Money Back** Guarantee

⚙ **365 Days** Free Update

⚙ **800,000+** Satisfied Customers

QUESTION 1

Exhibit.

```
            [edit]
utton       user@srx# show system security-profile
            SP-1 {
hibit           policy {
                    maximum 100;
as                  reserved 50;
                }
an            zone {
                    maximum 100;
nr                  reserved 50;
              }
              nat-nopat-address {
                    maximum 115;
                    reserved 100;
              }
              nat-static-rule {
                    maximum 125;
                    reserved 100;
              }
            }

        [edit]
        user@srx# show tenants
        C-1 {
                security-profile {
                        SP-1;
```

Referring to the exhibit, which two statements are true? (Choose two.)

A. The c-1 TSYS has a reservation for the security flow resource.

B. The c-1 TSYS can use security flow resources up to the system maximum.

C. The c-1 TSYS cannot use any security flow resources.

D. The c-1 TSYS has no reservation for the security flow resource.

Correct Answer: CD

Explanation: https://www.juniper.net/documentation/en_US/junos/topics/topic- map/security-profile-logical-system.html

QUESTION 2

Your Source NAT implementation uses an address pool that contains multiple IPv4 addresses Your users report that when they establish more than one session with an external application, they are prompted to authenticate multiple times External hosts must not be able to establish sessions with internal network hosts.

What will solve this problem?

A. Disable PAT.

B. Enable destination NAT.

C. Enable persistent NAT

D. Enable address persistence.

Correct Answer: D

Explanation: The solution to this problem is to enable address persistence. This will ensure that the same external IP address is used for multiple sessions between an internal host and an external host. This will result in only one authentication being required, as the same external IP address will be used for all sessions.

QUESTION 3

You are asked to download and install the IPS signature database to a device operating in chassis cluster mode. Which statement is correct in this scenario?

A. You must download and install the IPS signature package on the primary node.

B. The first synchronization of the backup node and the primary node must be performed manually.

C. The first time you synchronize the IPS signature package from the primary node to the backup node, the primary node must be rebooted.

D. The IPS signature package must be downloaded and installed on the primary and backup nodes.

Correct Answer: D

QUESTION 4

Exhibit

```
Aug  3 01:28:23 01:28:23.434801:CID-0:THREAD_ID-01:RT:   <172.20.101.10/59009-
>10.0.1.129/22;6,0x0> matched filter MatchTraffic:
Aug  3 01:28:23 01:28:23.434805:CID-0:THREAD_ID-01:RT:   packet [64] ipid =
36644, @0xef3edece
Aug  3 01:28:23 01:28:23.434810:CID-0:THREAD_ID-01:RT:   ---- flow_process_pkt:
(thd 1): flow_ctxt type 15, common flag 0x0, mbuf 0x6918b800, rtbl_idx = 0
Aug  3 01:28:23 01:28:23.434817:CID-0:THREAD_ID-01:RT:   ge-
0/0/4.0:172.20.101.10/59009->10.0.1.129/22, tcp, flag 2 syn
Aug  3 01:28:23 01:28:23.434819:CID-0:THREAD_ID-01:RT:   find flow: table
0x206a60a0, hash 43106(0xffff), sa 172.20.101.10, da 10.0.1.129, sp 59009, dp
22, proto 6, tok 9, conn-tag 0x00000000
Aug  3 01:28:23 01:28:23.434822:CID-0:THREAD_ID-01:RT:   no session found,
start first path. in_tunnel - 0x0, from_cp_flag - 0
Aug  3 01:28:23 01:28:23.434826:CID-0:THREAD_ID-01:RT:
 flow_first_create_session
Aug  3 01:28:23 01:28:23.434834:CID-0:THREAD_ID-01:RT:   flow_first_in_dst_nat:
in <ge-0/0/3.0>, out <N/A> dst_adr 10.0.1.129, sp 59009, dp 22
Aug  3 01:28:23 01:28:23.434835:CID-0:THREAD_ID-01:RT:   chose interface ge-
0/0/4.0 as incoming nat if.
Aug  3 01:28:23 01:28:23.434838:CID-0:THREAD_ID-01:RT:
 flow_first_rule_dst_xlate: DST no-xlate: 0.0.0.0(0) to 10.0.1.129(22)
Aug  3 01:28:23 01:28:23.434849:CID-0:THREAD_ID-01:RT:   flow_first_routing:
vr_id 0, call flow_route_lookup(): src_ip 172.20.101.10, x_dst_ip 10.0.1.129,
in ifp ge-0/0/4.0, out ifp N/A sp 59009, dp 22, ip_proto 6, tos 0
Aug  3 01:28:23 01:28:23.434861:CID-0:THREAD_ID-01:RT:   routed (x_dst_ip
10.1.0.129) from trust (ge-0/0/4.0 in 0) to ge-0/0/2.0, Next-hop: 10.0.1.129
Aug  3 01:28:23 01:28:23.434863:CID-0:THREAD_ID-01:RT:
 flow_first_policy_search: policy search from zone trust-> zone untrust
(0x0,0xe6810016,0x16)
Aug  3 01:28:26 01:28:26.434137:CID-0:THREAD_ID-01:RT:   packet dropped, denied
by policy
Aug  3 01:28:26 01:28:26.434137:CID-0:THREAD_ID-01:RT:   denied by policy Deny-
Telnet(5), dropping pkt
Aug  3 01:28:26 01:28:26.434138:CID-0:THREAD_ID-01:RT:   packet dropped,
 policy deny.
```

Referring to the exhibit, which statement is true?

A. This custom block list feed will be used before the Juniper SecIntel

B. This custom block list feed cannot be saved if the Juniper SecIntel block list feed is configured.

C. This custom block list feed will be used instead of the Juniper SecIntel block list feed

D. This custom block list feed will be used after the Juniper SecIntel block list feed.

Correct Answer: D

QUESTION 5

You want to enforce I DP policies on HTTP traffic.

In this scenario, which two actions must be performed on your SRX Series device? (Choose two)

A. Choose an attacks type in the predefined-attacks-group HTTP-All.

B. Disable screen options on the Untrust zone.

C. Specify an action of None.

D. Match on application junos-http.

Correct Answer: AD

Explanation: To enforce IDP policies on HTTP traffic on an SRX Series device, the following actions must be performed:

Choose an attacks type in the predefined-attacks-group HTTP-All: This allows the SRX Series device to match on specific types of attacks that can occur within HTTP traffic. For example, it can match on SQL injection or cross-site scripting

(XSS) attacks.

Match on application junos-http: This allows the SRX Series device to match on HTTP traffic specifically, as opposed to other types of traffic. It is necessary to properly identify the traffic that needs to be protected. Disabling screen options on

the Untrust zone and specifying an action of None are not necessary to enforce IDP policies on HTTP traffic. The first one is a feature used to prevent certain types of attacks, the second one is used to take no action in case of a match.

[JN0-636 Practice Test](#)   [JN0-636 Exam Questions](#)   [JN0-636 Braindumps](#)