

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.pass2lead.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

You are asked to configure a security policy on the SRX Series device. After committing the policy, you receive the "Policy is out of sync between RE and PFE ." error.

Which command would be used to solve the problem?

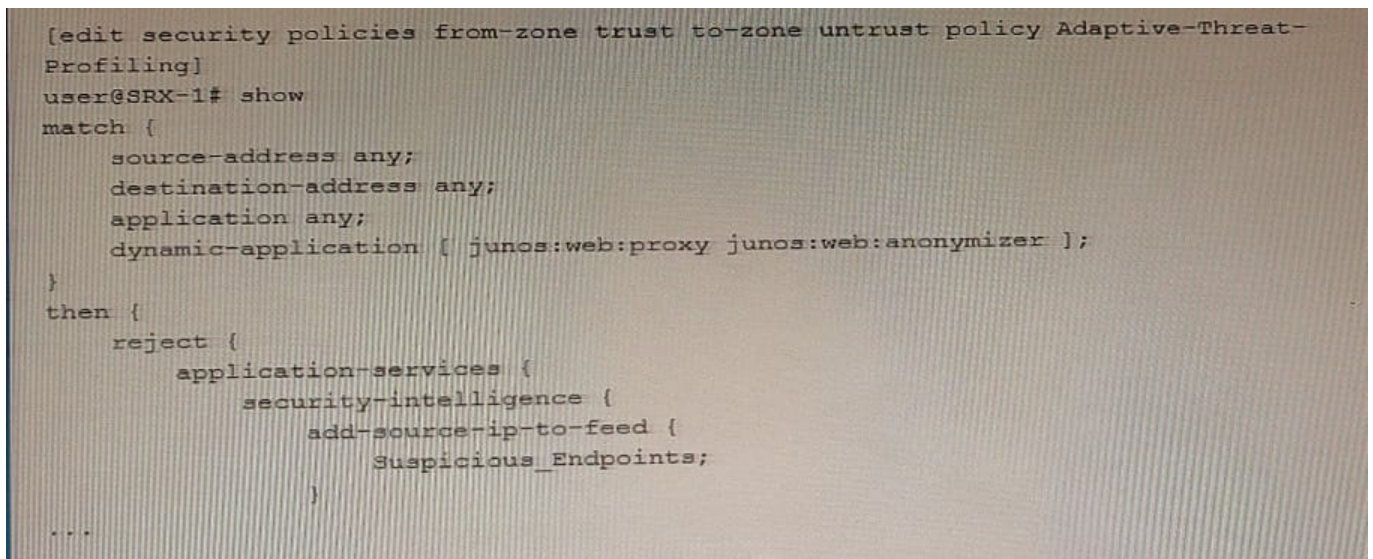
- A. request security polices resync
- B. request service-deployment
- C. request security polices check
- D. restart security-intelligence

Correct Answer: A

https://kb.juniper.net/InfoCenter/index?page=content&id=KB30443&cat=SRX_SERIES&act=p=LIST

QUESTION 2

Exhibit



```
[edit security policies from-zone trust to-zone untrust policy Adaptive-Threat-Profiling]
user@SRX-1# show
match {
    source-address any;
    destination-address any;
    application any;
    dynamic-application { junos:web:proxy junos:web:anonymizer };
}
then {
    reject {
        application-services {
            security-intelligence {
                add-source-ip-to-feed {
                    suspicious_endpoints;
                }
            }
        }
    }
}
...
```

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

- A. The suspicious_endpoints feed is only usable by the SRX-1 device.
- B. You must manually create the suspicious_endpoints feed in the Juniper ATP Cloud interface.
- C. The suspicious_endpoints feed is usable by any SRX Series device that is a part of the same realm as SRX-1
- D. Juniper ATP Cloud automatically creates the suspicious_endpoints feed after you commit the security policy.

Correct Answer: AC

QUESTION 3

Which statement is true about persistent NAT types?

- A. The target-host-port parameter cannot be used with IPv4 addresses in NAT46.
- B. The target-host parameter cannot be used with IPv6 addressee in NAT64.
- C. The target-host parameter cannot be used with IPv4 addresses in NAT46
- D. The target-host-port parameter cannot be used with IPv6 addresses in NAT64

Correct Answer: D

Explanation: NAT (Network Address Translation) is a method to map one IP address space into another by modifying network address information in the IP header of packets while they are in transit across a traffic routing device. There are different types of NAT, one of them is the persistent NAT which is a type of NAT that allows you to map the same internal IP address to the same external IP address each time a host initiates a connection.

QUESTION 4

Exhibit

```
Aug  3 01:28:23 01:28:23.434801:CID-0:THREAD_ID-01:RT: <172.20.201.10/59009->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.
```

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

- A. The source address is translated.
- B. The packet is an SSH packet
- C. The packet matches a user-configured policy
- D. The destination address is translated.

Correct Answer: AB

QUESTION 5

You are configuring transparent mode on an SRX Series device. You must permit IP-based traffic only, and BPDUs must be restricted to the VLANs from which they originate.

Which configuration accomplishes these objectives?

- A.

```
bridge {  
  block-non-ip-all;  
  bypass-non-ip-unicast;  
  no-packet-flooding;  
}
```
- B.

```
bridge {  
  block-non-ip-all;  
  bypass-non-ip-unicast;  
  bpdu-vlan-flooding;  
}
```
- C.

```
bridge {  
  bypass-non-ip-unicast;  
  bpdu-vlan-flooding;  
}
```
- D.

```
bridge {  
  block-non-ip-all;  
  bpdu-vlan-flooding;  
}
```

A. Option A

B. Option B

C. Option C

D. Option D

Correct Answer: D

https://www.juniper.net/documentation/us/en/software/junos/multicast-l2/topics/ref/statement/family-ethernet-switching-edit-interfaces-qfx-series.html#statement-name-statement__d26608e73