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.certbus.com/jn0-636.html

100% Passing Guarantee
100% Money Back Assurance

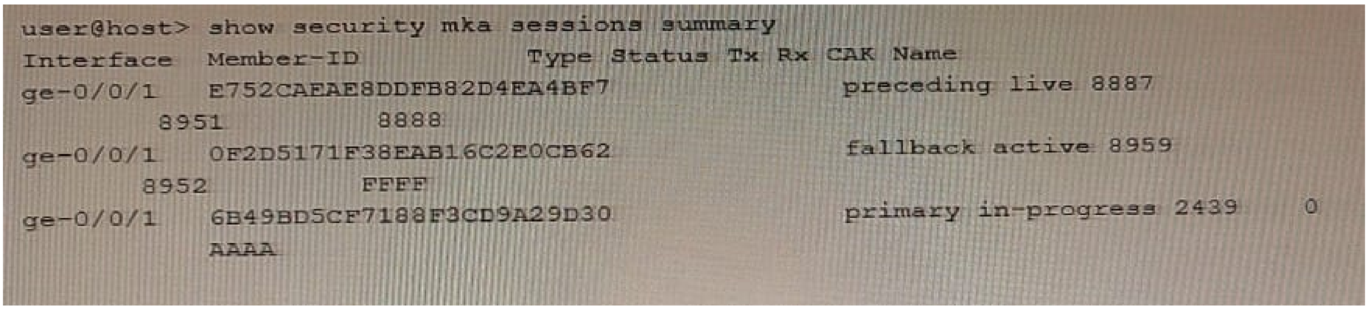
Following Questions and Answers are all new published by Juniper Official Exam Center

Instant Download After Purchase
100% Money Back Guarantee
365 Days Free Update
800,000+ Satisfied Customers

SATISFACTION GUARANTEED 100% SATISFACTION GUARANTEED

QUESTION 1

Exhibit



```
user@host> show security mka sessions summary
Interface   Member-ID            Type Status Tx Rx CAK Name
ge-0/0/1    E752CAEAE8DDFB82D4EA4BF7               preceding live 8887
         8951          8888
ge-0/0/1    0F2D5171F38EAB16C2E0CB62               fallback active 8959
        8952          FFFF
ge-0/0/1    6B49BD5CF7188F3CD9A29D30               primary in-progress 2439     0
            AAAA
```

Referring to the exhibit, which two statements are true about the CAK status for the CAK named "FFFP"? (Choose two.)

A. CAK is not used for encryption and decryption of the MACsec session.

B. SAK is successfully generated using this key.

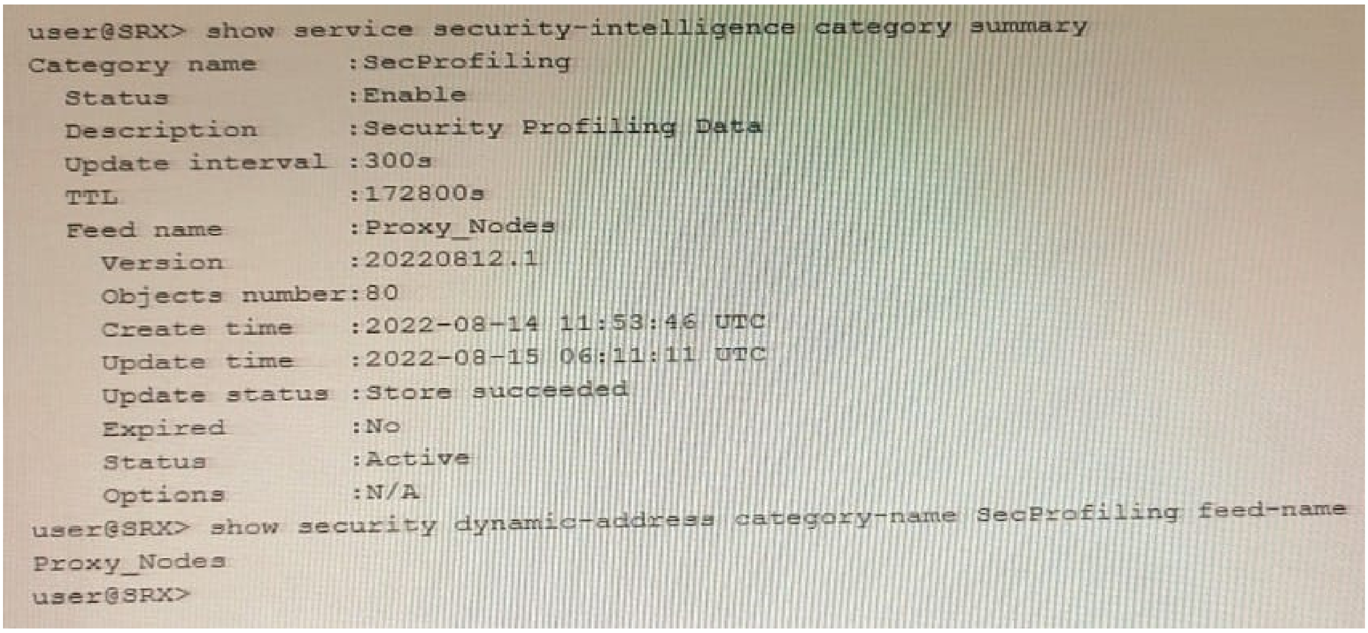
C. CAK is used for encryption and decryption of the MACsec session.

D. SAK is not generated using this key.

Correct Answer: CD

QUESTION 2

Exhibit You have recently configured Adaptive Threat Profiling and notice 20 IP address entries in the monitoring section of the Juniper ATP Cloud portal that do not match the number of entries locally on the SRX Series device, as shown in the exhibit.



```
user@SRX> show service security-intelligence category summary
Category name      :SecProfiling
  Status           :Enable
  Description      :Security Profiling Data
  Update interval :300s
  TTL              :172800s
  Feed name        :Proxy_Nodes
    Version        :20220812.1
    Objects number:80
    Create time    :2022-08-14 11:53:46 UTC
    Update time    :2022-08-15 06:11:11 UTC
    Update status :Store succeeded
    Expired        :No
    Status         :Active
    Options        :N/A
user@SRX> show security dynamic-address category-name SecProfiling feed-name
Proxy_Nodes
user@SRX>
```

What is the correct action to solve this problem on the SRX device?

A. You must configure the DAE in a security policy on the SRX device.

B. Refresh the feed in ATP Cloud.

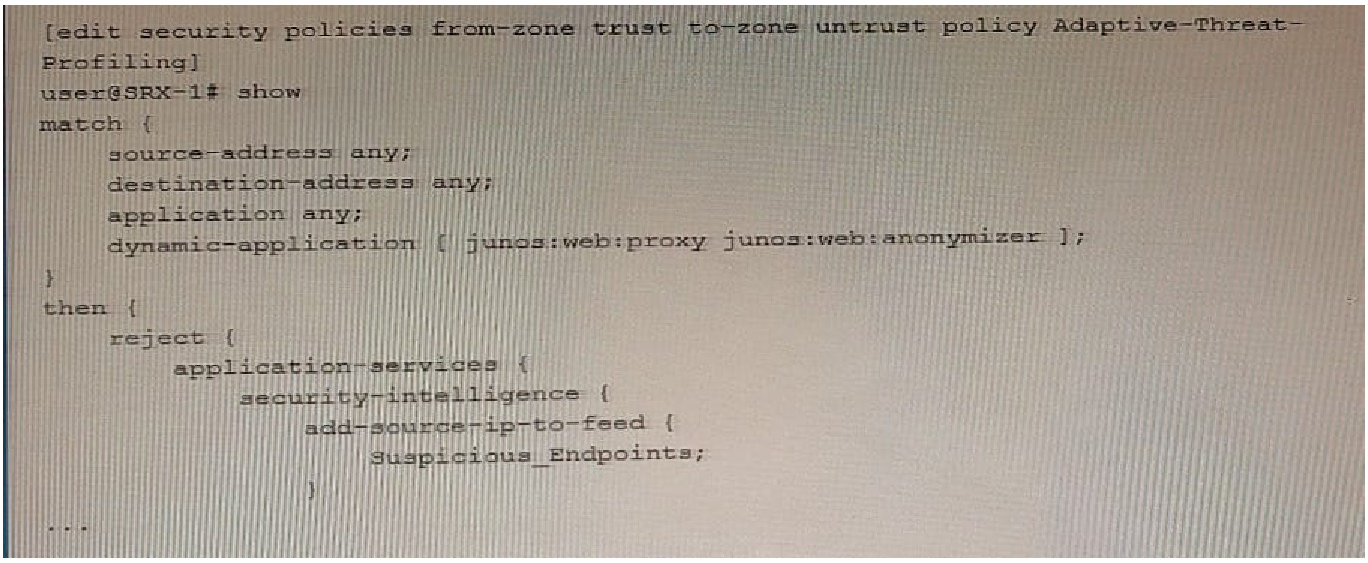
C. Force a manual download of the Proxy__Nodes feed.

D. Flush the DNS cache on the SRX device.

Correct Answer: C

QUESTION 3

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 3uspicious_Endpoint3 feed is only usable by the SRX-1 device.

B. You must manually create the suspicious_Endpoint3 feed in the Juniper ATP Cloud interface.

C. The 3uspiciou3_Endpoint3 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 3uopi\\'cioua_Endpoints feed after you commit the security policy.

Correct Answer: AC

QUESTION 4

You are asked to detect domain generation algorithms

Which two steps will accomplish this goal on an SRX Series firewall? (Choose two.)

A. Define an advanced-anti-malware policy under [edit services].

B. Attach the security-metadata-streaming policy to a security

C. Define a security-metadata-streaming policy under [edit

D. Attach the advanced-anti-malware policy to a security policy.

Correct Answer: BD

Explanation: To detect domain generation algorithms (DGAs) on an SRX Series firewall, you can use the security-metadata-streaming and advanced-anti-malware features. The first step is to define a security-metadata-streaming policy under

[edit services], which allows the firewall to receive and process metadata from a third- party security intelligence service. This metadata includes information about DGAs, which the firewall can use to identify and block malicious traffic. The

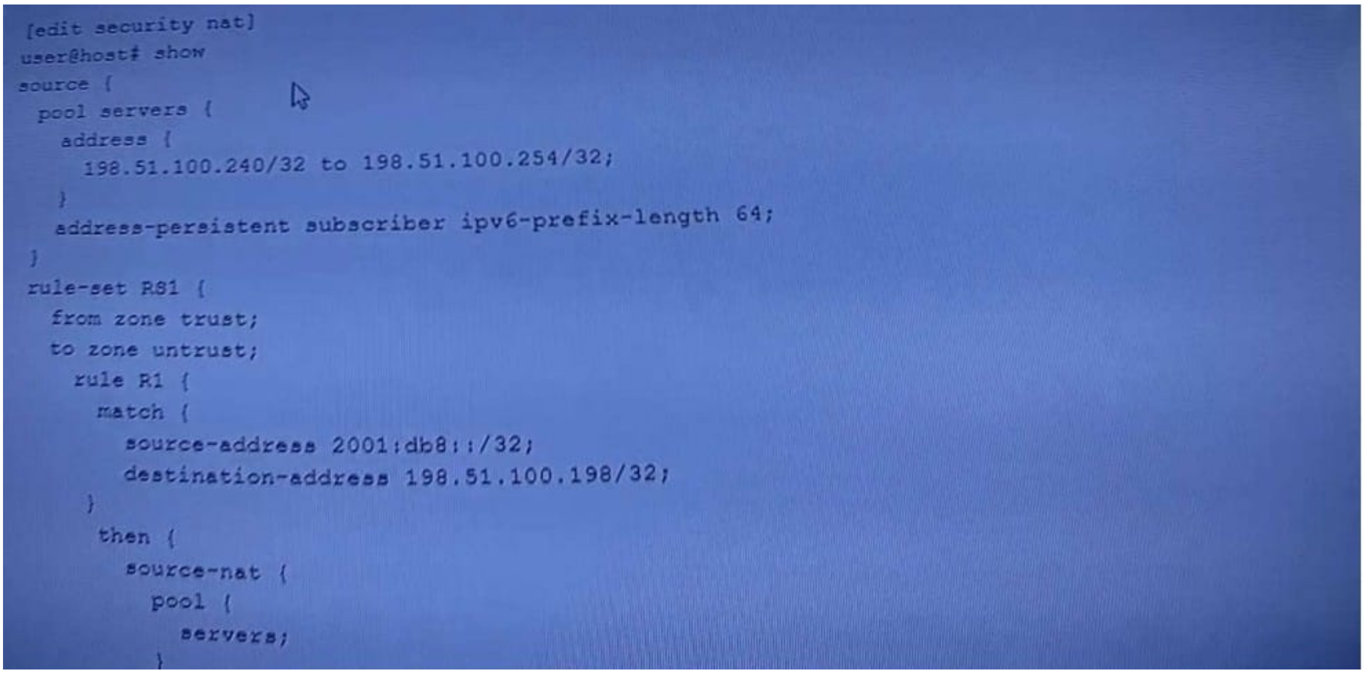
second step is to attach the security-metadata-streaming policy to a security policy, this will enable the firewall to inspect traffic against the DGA domains provided by the intelligence service.

The third step is to enable the advanced-anti-malware feature on the firewall, and attach an advanced-anti-malware policy to a security policy. This allows the firewall to detect and block malware based on signatures and behavioral analysis,

which can also detect and block traffic associated with DGAs.

QUESTION 5

Exhibit.



```
[edit security nat]
user@host# show
source {
  pool servers {
    address {
      198.51.100.240/32 to 198.51.100.254/32;
    }
    address-persistent subscriber ipv6-prefix-length 64;
  }
  rule-set RS1 {
    from zone trust;
    to zone untrust;
      rule R1 {
        match {
          source-address 2001:db8::/32;
          destination-address 198.51.100.198/32;
        }
        then {
          source-nat {
            pool {
              servers;
            }
```

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

A. The configured solution allows IPv6 to IPv4 translation.

B. The configured solution allows IPv4 to IPv6 translation.

C. The IPv6 address is invalid.

D. External hosts cannot initiate contact.

Correct Answer: AC

QUESTION 6

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

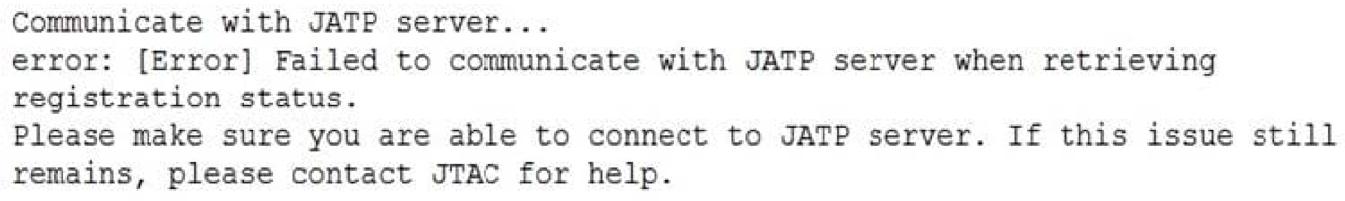
(XSS) attacks.

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.

QUESTION 7

Click the Exhibit button.



```
Communicate with JATP server...
error: [Error] Failed to communicate with JATP server when retrieving
registration status.
Please make sure you are able to connect to JATP server. If this issue still
remains, please contact JTAC for help.
```

When attempting to enroll an SRX Series device to JATP, you receive the error shown in the exhibit. What is the cause of the error?

A. The fxp0 IP address is not routable

B. The SRX Series device certificate does not match the JATP certificate

C. The SRX Series device does not have an IP address assigned to the interface that accesses JATP

D. A firewall is blocking HTTPS on fxp0

Correct Answer: C

Reference: https://kb.juniper.net/InfoCenter/index? page=contentandid=KB33979andcat=JATP_SERIESandactp=LIST

QUESTION 8

All interfaces involved in transparent mode are configured with which protocol family?

A. mpls

B. bridge

C. inet

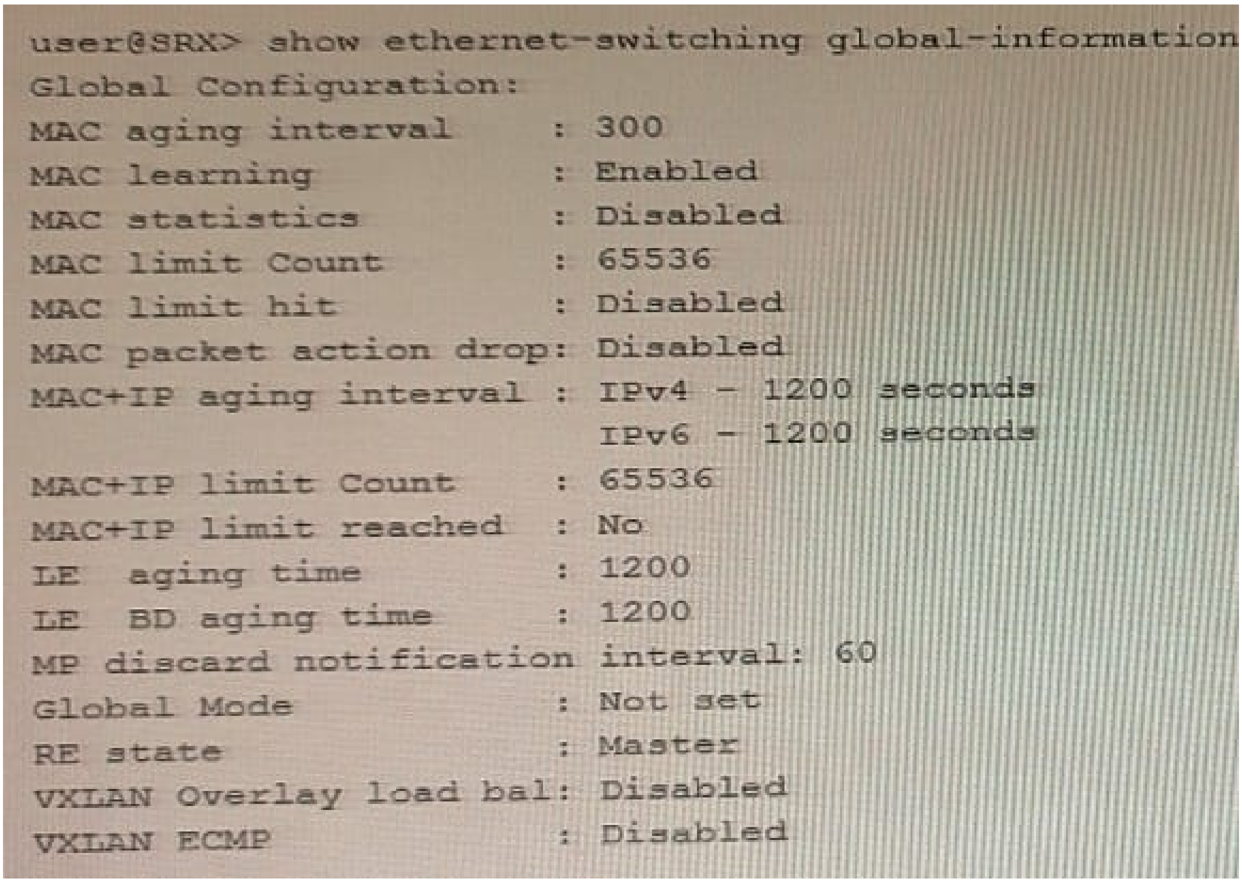
D. ethernet -- switching

Correct Answer: B

Explanation: In transparent mode, all interfaces involved are configured with the bridge protocol family. This allows the SRX device to act as a bridge between the interfaces and forward traffic transparently without any modification. The bridge interfaces can be configured to forward traffic based on layer 2 headers, such as MAC addresses, without the need for routing or IP addressing.

QUESTION 9

Exhibit You have configured the SRX Series device to switch packets for multiple directly connected hosts that are within the same broadcast domain However, the traffic between two hosts in the same broadcast domain are not matching any security policies



```
user@SRX> show ethernet-switching global-information
Global Configuration:
MAC aging interval        : 300
MAC learning              : Enabled
MAC statistics            : Disabled
MAC limit Count           : 65536
MAC limit hit             : Disabled
MAC packet action drop: Disabled
MAC+IP aging interval : IPv4 - 1200 seconds
                        IPv6 - 1200 seconds
MAC+IP limit Count        : 65536
MAC+IP limit reached      : No
LE  aging time            : 1200
LE  BD aging time         : 1200
MP discard notification interval: 60
Global Mode               : Not set
RE state                  : Master
VXLAN Overlay load bal: Disabled
VXLAN ECMP                : Disabled
```

Referring to the exhibit, what should you do to solve this problem?

A. You must change the global mode to security switching mode.

B. You must change the global mode to security bridging mode

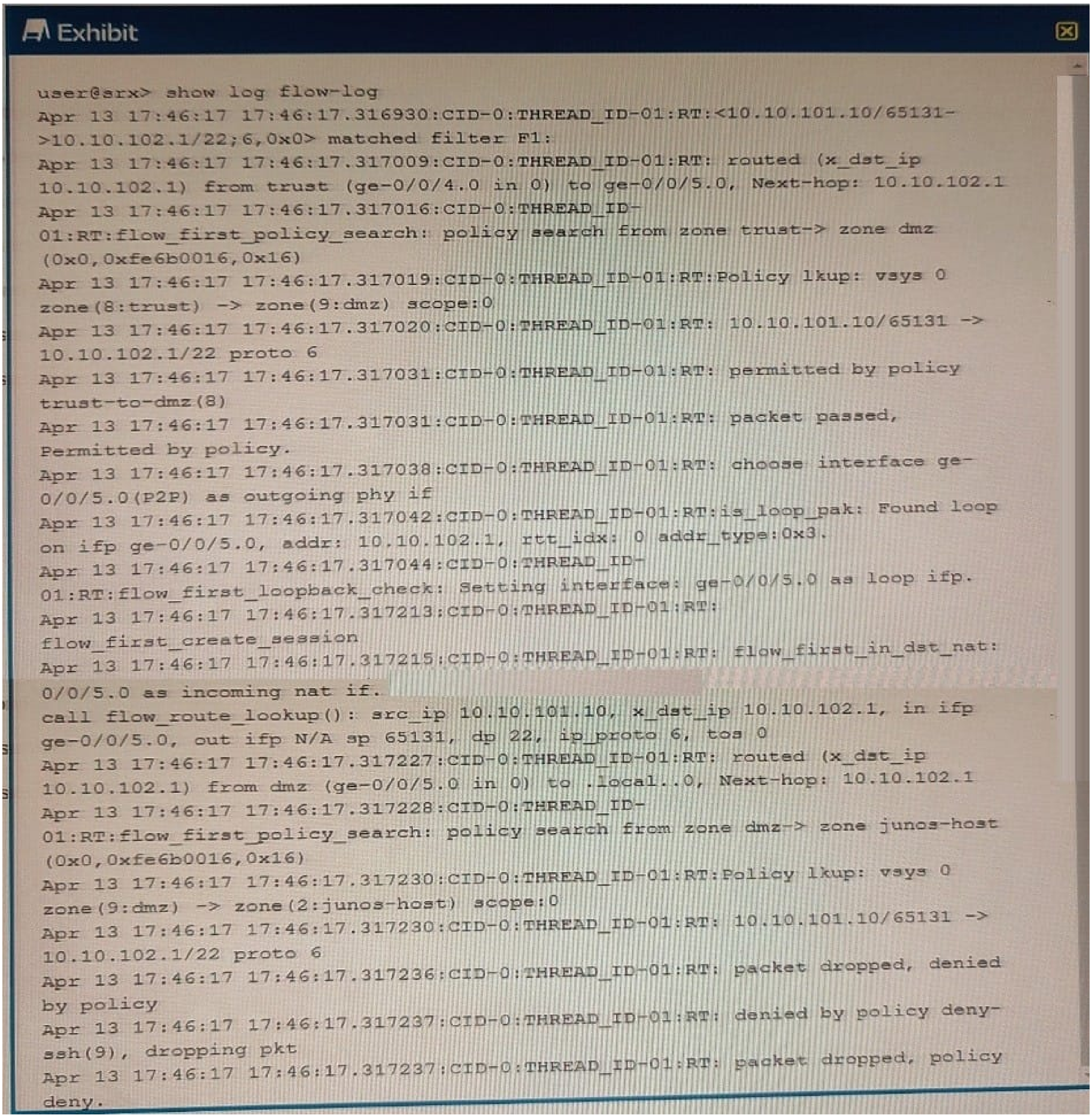
C. You must change the global mode to transparent bridge mode.

D. You must change the global mode to switching mode.

Correct Answer: B

QUESTION 10

Exhibit



```
user@srx> show log flow-log
Apr 13 17:46:17 17:46:17.316930:CID-0:THREAD_ID-01:RT:<10.10.101.10/65131-
>10.10.102.1/22;6,0x0> matched filter F1:
Apr 13 17:46:17 17:46:17.317009:CID-0:THREAD_ID-01:RT: routed (x_dst_ip
10.10.102.1) from trust (ge-0/0/4.0 in 0) to ge-0/0/5.0, Next-hop: 10.10.102.1
Apr 13 17:46:17 17:46:17.317016:CID-0:THREAD_ID-
01:RT:flow_first_policy_search: policy search from zone trust-> zone dmz
(0x0,0xfe6b0016,0x16)
Apr 13 17:46:17 17:46:17.317019:CID-0:THREAD_ID-01:RT:Policy lkup: vsys 0
zone(8:trust) -> zone(9:dmz) scope:0
Apr 13 17:46:17 17:46:17.317020:CID-0:THREAD_ID-01:RT: 10.10.101.10/65131 ->
10.10.102.1/22 proto 6
Apr 13 17:46:17 17:46:17.317031:CID-0:THREAD_ID-01:RT: permitted by policy
trust-to-dmz(8)
Apr 13 17:46:17 17:46:17.317031:CID-0:THREAD_ID-01:RT: packet passed,
Permitted by policy.
Apr 13 17:46:17 17:46:17.317038:CID-0:THREAD_ID-01:RT: choose interface ge-
0/0/5.0(P2P) as outgoing phy if
Apr 13 17:46:17 17:46:17.317042:CID-0:THREAD_ID-01:RT:is_loop_pak: Found loop
on ifp ge-0/0/5.0, addr: 10.10.102.1, rtt_idx: 0 addr_type:0x3.
Apr 13 17:46:17 17:46:17.317044:CID-0:THREAD_ID-
01:RT:flow_first_loopback_check: Setting interface: ge-0/0/5.0 as loop ifp.
Apr 13 17:46:17 17:46:17.317213:CID-0:THREAD_ID-01:RT:
flow_first_create_session
Apr 13 17:46:17 17:46:17.317215:CID-0:THREAD_ID-01:RT: flow_first_in_dst_nat:
0/0/5.0 as incoming nat if.
call flow_route_lookup(): src_ip 10.10.101.10, x_dst_ip 10.10.102.1, in ifp
ge-0/0/5.0, out ifp N/A sp 65131, dp 22, ip_proto 6, tos 0
Apr 13 17:46:17 17:46:17.317227:CID-0:THREAD_ID-01:RT: routed (x_dst_ip
10.10.102.1) from dmz (ge-0/0/5.0 in 0) to .local..0, Next-hop: 10.10.102.1
Apr 13 17:46:17 17:46:17.317228:CID-0:THREAD_ID-
01:RT:flow_first_policy_search: policy search from zone dmz-> zone junos-host
(0x0,0xfe6b0016,0x16)
Apr 13 17:46:17 17:46:17.317230:CID-0:THREAD_ID-01:RT:Policy lkup: vsys 0
zone(9:dmz) -> zone(2:junos-host) scope:0
Apr 13 17:46:17 17:46:17.317230:CID-0:THREAD_ID-01:RT: 10.10.101.10/65131 ->
10.10.102.1/22 proto 6
Apr 13 17:46:17 17:46:17.317236:CID-0:THREAD_ID-01:RT: packet dropped, denied
by policy
Apr 13 17:46:17 17:46:17.317237:CID-0:THREAD_ID-01:RT: denied by policy deny-
ssh(9), dropping pkt
Apr 13 17:46:17 17:46:17.317237:CID-0:THREAD_ID-01:RT: packet dropped, policy
deny.
```

You are using traceoptions to verify NAT session information on your SRX Series device. Referring to the exhibit, which two statements are correct? (Choose two.)

A. This is the last packet in the session.

B. The SRX Series device is performing both source and destination NAT on this session.

C. This is the first packet in the session.

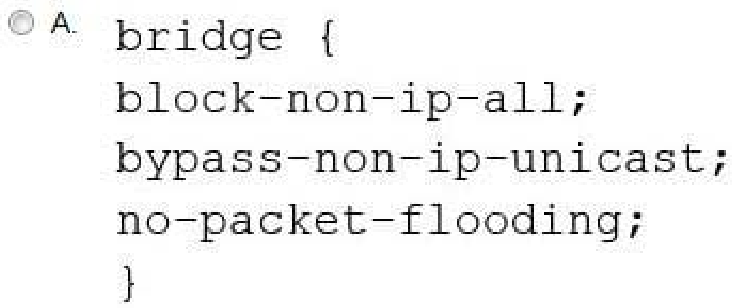
D. The SRX Series device is performing only source NAT on this session.

Correct Answer: AB

QUESTION 11

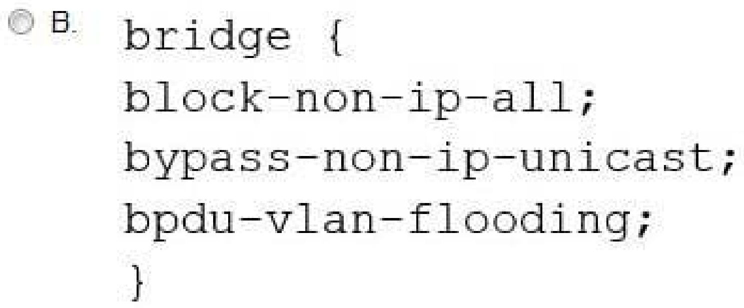
You are configuring transparent mode on an SRX Series device. You must permit IP-based traffic only, and BPDUs must be restricted to the VLANs from which they originate.

Which configuration accomplishes these objectives?



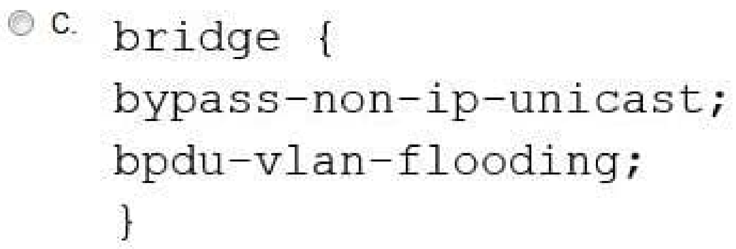
○ A.

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



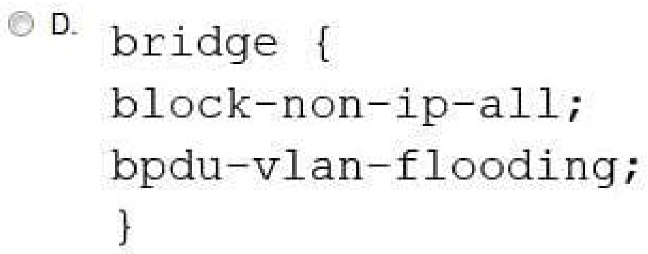
○ B.

```
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

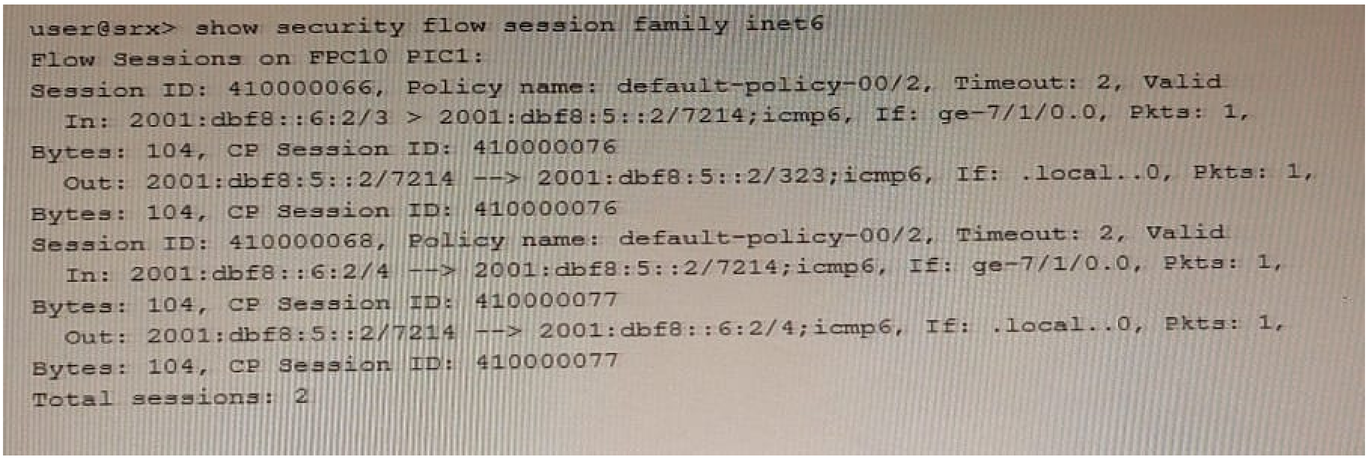
D. Option D

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

QUESTION 12

Exhibit



```
user@srx> show security flow session family inet6
Flow Sessions on FPC10 PIC1:
Session ID: 410000066, Policy name: default-policy-00/2, Timeout: 2, Valid
  In: 2001:dbf8::6:2/3 > 2001:dbf8:5::2/7214;icmp6, If: ge-7/1/0.0, Pkts: 1,
Bytes: 104, CP Session ID: 410000076
  Out: 2001:dbf8:5::2/7214 --> 2001:dbf8:5::2/323;icmp6, If: .local..0, Pkts: 1,
Bytes: 104, CP Session ID: 410000076
Session ID: 410000068, Policy name: default-policy-00/2, Timeout: 2, Valid
  In: 2001:dbf8::6:2/4 --> 2001:dbf8:5::2/7214;icmp6, If: ge-7/1/0.0, Pkts: 1,
Bytes: 104, CP Session ID: 410000077
  Out: 2001:dbf8:5::2/7214 --> 2001:dbf8::6:2/4;icmp6, If: .local..0, Pkts: 1,
Bytes: 104, CP Session ID: 410000077
Total sessions: 2
```

Which statement is true about the output shown in the exhibit?

A. The SRX Series device is configured with default security forwarding options.

B. The SRX Series device is configured with packet-based IPv6 forwarding options.

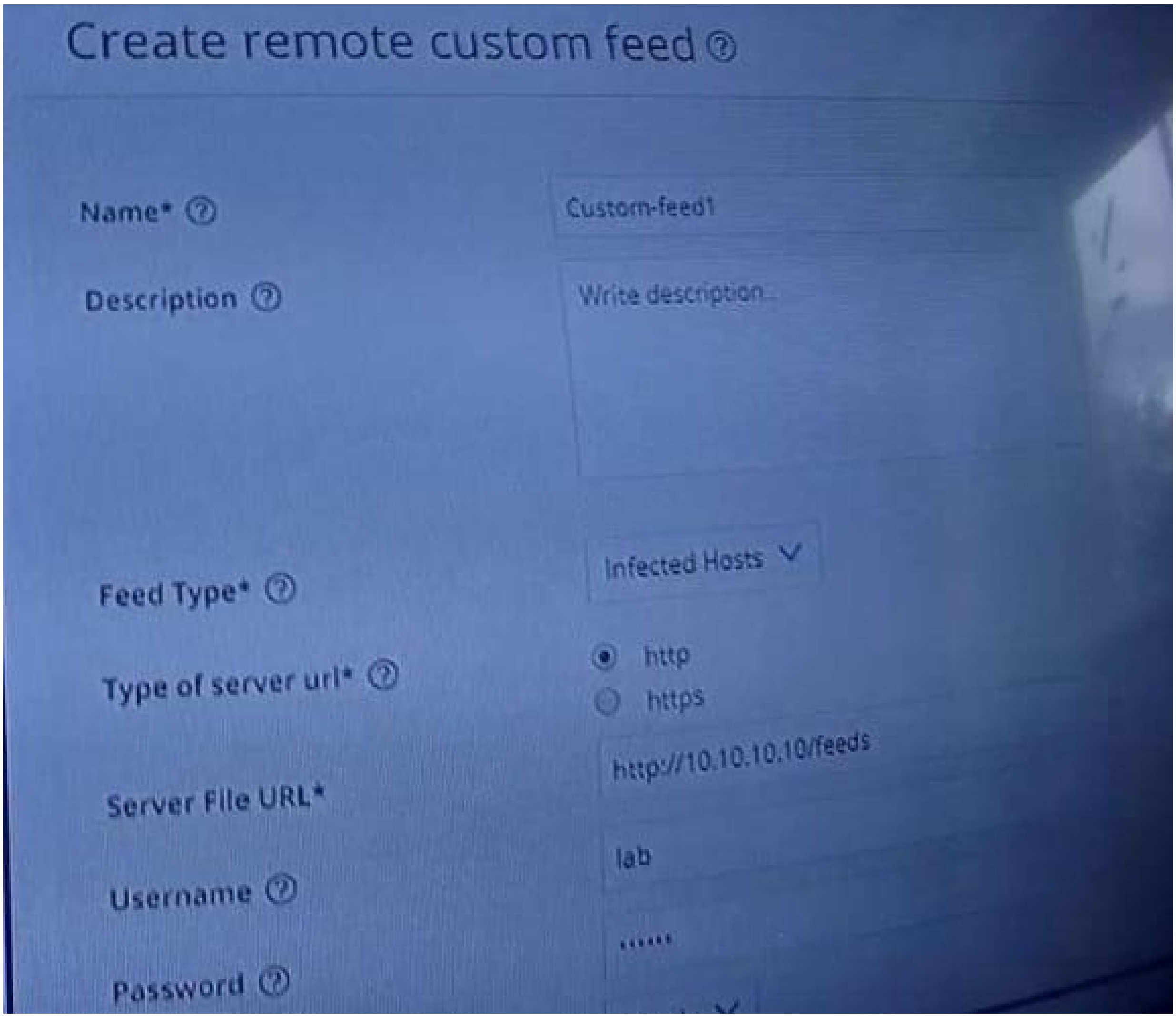
C. The SRX Series device is configured with flow-based IPv6 forwarding options.

D. The SRX Series device is configured to disable IPv6 packet forwarding.

Correct Answer: A

QUESTION 13

Exhibit.



Create remote custom feed

Name*	Custom-feed1
Description	Write description...
Feed Type*	Infected Hosts ∨
Type of server url*	● http ○ https
Server File URL*	http://10.10.10.10/feeds
Username	lab
Password	••••••

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

A. Juniper Networks will not investigate false positives generated by this custom feed.

B. The custom infected hosts feed will not overwrite the Sky ATP infected host\\'s feed.

C. The custom infected hosts feed will overwrite the Sky ATP infected host\\'s feed.

D. Juniper Networks will investigate false positives generated by this custom feed.

Correct Answer: AC

Explanation: https://www.juniper.net/documentation/en_US/junos-space18.1/policy-enforcer/topics/task/configuration/junos-space-policyenforcer-custom-feeds-infected-host- configure.html

QUESTION 14

You are not able to activate the SSH honeypot on the all-in-one Juniper ATP appliance. What would be a cause of this problem?

A. The collector must have a minimum of two interfaces.

B. The collector must have a minimum of three interfaces.

C. The collector must have a minimum of five interfaces.

D. The collector must have a minimum of four interfaces.

Correct Answer: D

Explanation: https://www.juniper.net/documentation/en_US/release- independent/jatp/topics/task/configuration/jatp-traffic-collectorsetting-ssh-honeypot- detection.html

QUESTION 15

What are two valid modes for the Juniper ATP Appliance? (Choose two.)

A. flow collector

B. event collector

C. all-in-one

D. core

Correct Answer: AC

Explanation: The Juniper ATP Appliance supports two valid modes of operation:

Flow Collector: This mode allows the Juniper ATP Appliance to collect and analyze network flow data to detect malicious activity.

All-in-One: This mode allows the Juniper ATP Appliance to perform both flow collection and event collection. It includes all the features of the Flow Collector and Event Collector mode.

Event collector and core are not valid modes for the Juniper ATP Appliance, the first one is focused on collecting events and the second one is a term that\\'s not related to the appliance.

JN0-636 PDF Dumps JN0-636 VCE Dumps JN0-636 Study Guide