

# DUMPSQUEEN

## Security Professional (JNCIP-SEC)

Juniper JN0-636

Version Demo

Total Demo Questions: 10

Total Premium Questions: 92

Buy Premium PDF

<https://dumpsqueen.com>

[support@dumpsqueen.com](mailto:support@dumpsqueen.com)

dumpsqueen.com

## QUESTION NO: 1

You are asked to look at a configuration that is designed to take all traffic with a specific source ip address and forward the traffic to a traffic analysis server for further evaluation. The configuration is no longer working as intended.

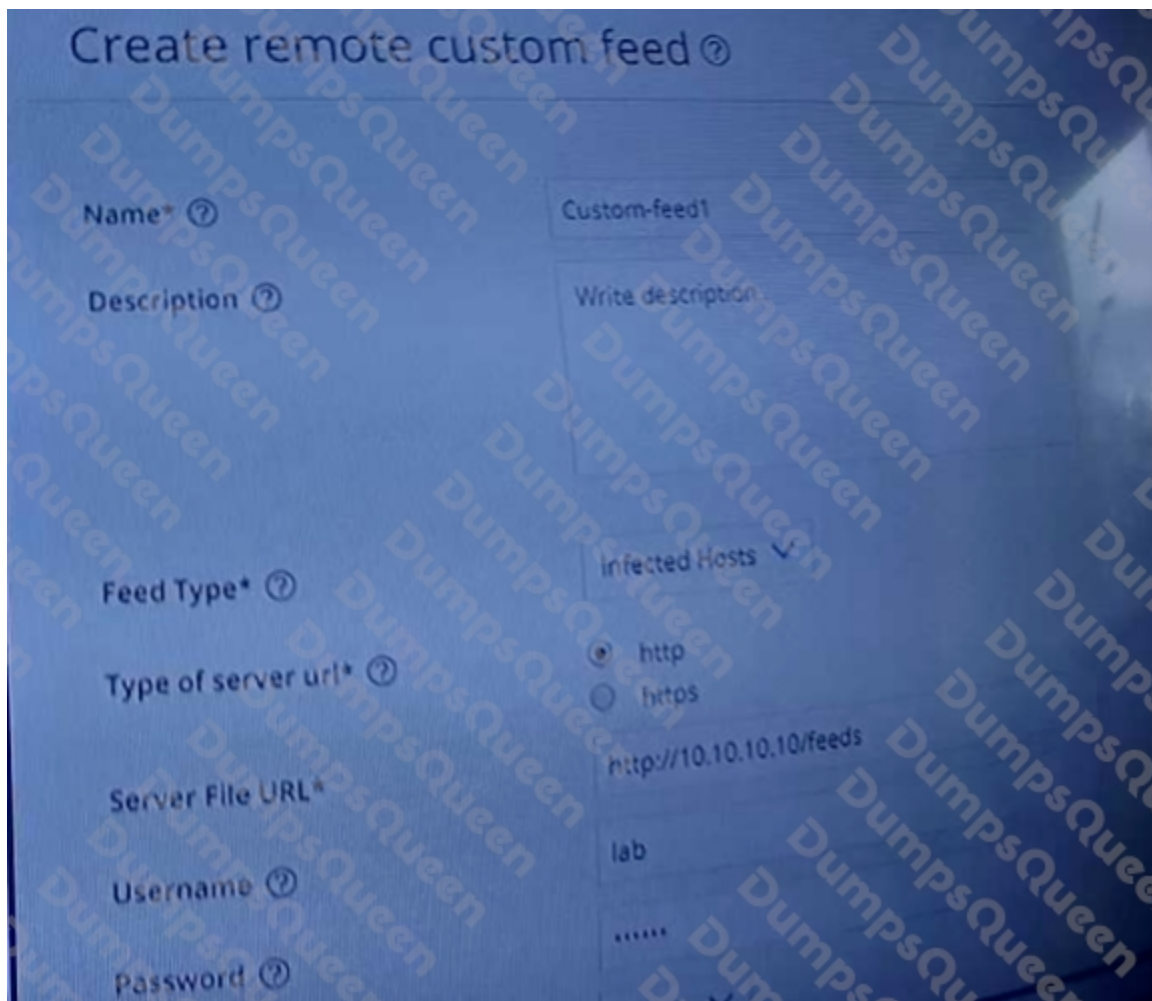
Referring to the exhibit which change must be made to correct the configuration?

- A. Apply the filter as in input filter on interface xe-0/2/1.0
- B. Apply the filter as in input filter on interface xe-0/0/1.0
- C. Create a routing instance named default
- D. Apply the filter as in output filter on interface xe-0/1/0.0

**ANSWER: B**

## QUESTION NO: 2

Exhibit.



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.

**ANSWER: A C**

### QUESTION NO: 3

What is the purpose of the Switch Microservice of Policy Enforcer?

- A. to isolate infected hosts
- B. to enroll SRX Series devices with Juniper ATP Cloud
- C. to inspect traffic for malware

D. to synchronize security policies to SRX Series devices

**ANSWER: B**

## QUESTION NO: 4

Which two additional configuration actions are necessary for the third-party feed shown in the exhibit to work properly? (Choose two.)

- A. You must create a dynamic address entry with the IP filter category and the ipfilter\_office365 value.
- B. You must create a dynamic address entry with the C&C category and the cc\_office365 value.
- C. You must apply the dynamic address entry in a security policy.
- D. You must apply the dynamic address entry in a security intelligence policy.

**ANSWER: A C**

## QUESTION NO: 5

You issue the command shown in the exhibit.

Which policy will be active for the identified traffic?

- A. Policy p4
- B. Policy p7
- C. Policy p1
- D. Policy p12

**ANSWER: B**

## QUESTION NO: 6

Exhibit

```
May 23 05:20:34 Vendor-Id: 0 Attribute Type:Reply-Message(18) Value:string-type
Length:36
May 23 05:20:34 authd_radius_parse_message:generic-type:18
May 23 05:20:34 Vendor-Id: 0 Attribute Type:Reply-Message(18) Value:string-type
Length:15
May 23 05:20:34 authd_radius_parse_message:generic-type:18
May 23 05:20:34 Framework - module(radius) return: FAILURE
```

You configure a traceoptions file called radius on your returns the output shown in the exhibit

What is the source of the problem?

- A. An incorrect password is being used.
- B. The authentication order is misconfigured.
- C. The RADIUS server IP address is unreachable.
- D. The RADIUS server suffered a hardware failure.

**ANSWER: D**

## QUESTION NO: 7

In Juniper ATP Cloud, what are two different actions available in a threat prevention policy to deal with an infected host? (Choose two.)

- A. Send a custom message
- B. Close the connection.
- C. Drop the connection silently.
- D. Quarantine the host.

**ANSWER: C D**

## QUESTION NO: 8

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\_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 suspicious\_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 suspicious\_Endpoints feed after you commit the security policy.

**ANSWER: A C**

## QUESTION NO: 9

Exhibit

```
user@host> show security mka sessions summary
Interface  Member-ID          Type Status Tx Rx  CAK Name
-----
ge-0/0/1   E752CAFAE8DDFB82D4EA4BF7 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 "FFFF"? (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.

**ANSWER: C D**

## QUESTION NO: 10

While troubleshooting security policies, you added the count action. Where do you see the result of this action?

- A. In the show security policies hit-count command output.
- B. In the show security flow statistics command output.
- C. In the show security policies detail command output.
- D. In the show firewall log command output.

**ANSWER: D**