



JN0-635^{Q&As}

Security, Professional

Pass Juniper JN0-635 Exam with 100% Guarantee

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

<https://www.geekcert.com/jn0-635.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

Click the Exhibit button.



```
user@srx> show services advanced-anti-malware status
Server connection status:
  Server hostname: 172.25.11.120
  Server port: 443
  Proxy hostname: None
  Proxy port: None
  Control Plane:
    Connection time: 2019-11-04 02:19:57 UTC
    Connection status: Connected
  Service Plane:
    fpc0
    Connection active number: 0
    Connection retry statistics: 0

user@srx> show services security-intelligence category summary

Category name           :CC
Status                  :Enable
Description              :Command and Control data schema
Update interval         :1800s
TTL                     :3456000s
Feed name               :cc_ip_data
  Version               :N/A
  Objects number        :0
  Create time           :2019-08-22 06:49:32 PDT
  Update time           :2019-09-12 12:47:47 PDT
  Update status         :N/A
  Expired               :No
  Options               :N/A
Feed name               :cc_ipv6_data
  Version               :20180413.1
  Objects number        :1
  Create time           :2019-08-22 06:32:29 PDT
  Update time           :2019-09-12 12:48:27 PDT
  Update status         :Store succeeded
  Expired               :No
  Options               :N/A
Feed name               :cc_url_data
  Version               :N/A
  Objects number        :0
  Create time           :2019-08-22 06:45:32 PDT
  Update time           :N/A
  Update status         :N/A
  Expired               :No
  Options               :N/A
```

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

A. The SRX Series device is enrolled and communicating with a JATP Appliance



- B. The JATP Appliance cannot download the security feeds from the GSS servers
- C. The SRX Series device cannot download the security feeds from the JATP Appliance
- D. The SRX Series device is not enrolled but can communicate with the JATP Appliance

Correct Answer: CD

QUESTION 2

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.



```
[edit]
user@srx# show
...
interfaces (
  xe-0/0/1 {
    description "Connected to Finance";
    unit 0 {
      family inet {
        address 10.1.1.1/24;
      }
    }
  }
  xe-0/1/0 (
    description "Connected to Internet";
    unit 0 {
      family inet (
        address 192.168.2.2/30;
      )
    }
  }
  xe-0/2/1 {
    description "Connected to Sales";
    unit 0 {
      family inet {
        address 10.3.2.21/24;
      }
    }
  }
}
firewall {
  filter filter1 {
    term t1 {
      from {
        source-address {
          10.1.1.3/32;
        }
      }
      then {
        next-interface {
          xe-0/1/0.0;
          routing-instance evall;
        }
      }
    }
    term t2 {
      then {
        routing-instance default;
      }
    }
  }
}
routing-instances {
  evall {
    instance-type virtual-router;
    interface xe-0/1/0.0;
  }
}
```



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

Correct Answer: B

QUESTION 3

Click the Exhibit button.



```
[edit interfaces]
user@new-site-gateway# show st0
unit 0 {
  family inet {
    address 10.0.0.2/30;
  }
}

[edit interfaces]
user@new-site-gateway# show ge-0/0/2
unit 0 {
family inet {
dhcp ;
}

[edit security zones]
user@new-site-gateway# show security-zone untrust
interfaces {
  ge-0/0/2.0 {
    host-inbound-traffic {
      system-services {
        ike;
        dhcp;
      }
    }
  }
}

[edit security ike]
user@new-site-gateway# show
policy ike-pol-1 {
  mode main;
  proposal-set standard;
  pre-shared-key ascii - text " $9$6st6CpOhSeX7V1RwYZG69A"; ## SECRET-
DATA
}
gateway gate-1 {
  ike-policy ike-pol-1;
  address 203.0.113.5;
  local-identity hostname "srx1@srx.juniper.net";
  external-interface ge-0/0/2.0;
}
```

Your company has purchased a competitor and now must connect the new network to the existing one. The competitor's gateway device is receiving its ISP address using DHCP. Communication between the two sites must be secured; however, obtaining a static public IP address for the new site gateway is not an option at this time. The company has several requirements for this solution:

A site-to-site IPsec VPN must be used to secure traffic between the two sites; The IKE identity on the new site gateway device must use the hostname option; and Internet traffic from each site should exit through

its local Internet connection.

The configuration shown in the exhibit has been applied to the new site's SRX, but the secure tunnel is not working.

In this scenario, what configuration change is needed for the tunnel to come up?



- A. Remove the quotes around the hostname
- B. Bind interface st0 to the gateway
- C. Change the IKE policy mode to aggressive
- D. Apply a static address to ge-0/0/2

Correct Answer: C

QUESTION 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 CandC category and the cc_offic365 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.

Correct Answer: AC

QUESTION 5

You configured a security policy permitting traffic from the trust zone to the DMZ zone, inserted the new policy at the top of the list, and successfully committed it to the SRX Series device. Upon monitoring, you notice that the hit count does not increase on the newly configured policy.

In this scenario, which two commands would help you to identify the problem? (Choose two.)

- A. user@srx> show security zones trust detail
- B. user@srx> show security shadow-policies from zone trust to zone DMZ
- C. user@srx> show security match-policies from-zone trust to-zone DMZ source-ip 192.168.10.100/32 destination-ip 10.10.10.80/32 protocol tcp source-port 5806 destination-port 443
- D. user@srx> show security match-policies from-zone trust to-zone DMZ source-ip 192.168.10.100/32 destination-ip 10.10.10.80/32 protocol tcp source-port 5806 destination-port 443 result-count 10

Correct Answer: BD

Reference: https://www.juniper.net/documentation/en_US/junos/topics/topic-map/monitoringtroubleshooting-security-policy.html