

JN0-634^{Q&As}

Security, Professional (JNCIP-SEC)

Pass Juniper JN0-634 Exam with 100% Guarantee

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

<https://www.leads4pass.com/jn0-634.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@host show security idp-policy my-policy rulebase-ips
rule 1 {
  match {
    attacks {
      custom-attacks my-signature;
    }
  }
  then {
    action {
      no-action;
    }
  }
  terminal;
}
rule 2 {
  match {
    attacks {
      custom-attacks my-signature;
    }
  }
  then {
    action {
      ignore-connection;
    }
  }
}
rule 3 {
  match {
    attacks {
      custom-attacks my-signature;
    }
  }
  then {
    action {
      drop-packet;
    }
  }
}
rule 4 {
  match {
    attacks {
      custom-attacks my-signature;
    }
  }
  then {
    action {
      close-client-and-server;
    }
  }
}
```

You have recently committed the IPS policy shown in the exhibit. When evaluating the expected behavior, you notice that you have a session that matches all of the rules in your IPS policy.

In this scenario, which action would be taken?

- A. ignore-connection
- B. drop packet
- C. no-action
- D. close-client-and-server

Correct Answer: C

QUESTION 2

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

Which configuration accomplishes these objectives?

- A. bridge { block-non-ip-all; bpdu-vlan-flooding; }
- B. bridge { block-non-ip-all; bypass-non-ip-unicast; no-packet-flooding; }
- C. bridge { bypass-non-ip-unicast; bpdu-vlan-flooding; }
- D. bridge { block-non-ip-all; bypass-non-ip-unicast; bpdu-vlan-flooding; }

Correct Answer: A

QUESTION 3

Click the Exhibit button.

```
[edit: security policies global policy int-FW]
user@host# show
match {
    source-address any;
    destination-address any;
    application any;
}
then {
    permit;
}

user@host> show security user-identification local-authentication-table all

user@host>
```

You have configured integrated user firewall on the SRX Series devices in your network. However, you noticed that no users can access the servers that are behind the SRX Series devices.

Referring to the exhibit, what is the problem?

- A. The Kerberos service is not configured correctly on the Active Directory server.
- B. There are no authentication entries in the SRX Series device for the users.
- C. The security policy on the SRX Series device is configured incorrectly.
- D. The SAML service is not configured correctly on the Active Directory server.

Correct Answer: C

QUESTION 4

Click the Exhibit button.

```
[edit security utm]
user@host# show
feature-profile {
    content-filtering {
        profile web-traffic-profile {
            block-content-type {
                zip;
            }
        }
    }
}
utm-policy utm-web-policy {
    content-filtering {
        http-profile web-traffic-profile;
    }
}
```

The UTM policy shown in the exhibit has been applied to a security policy on a branch SRX Series device. In this scenario, which statement is true?

- A. HTTP downloads of ZIP files will be blocked.
- B. FTP downloads of ZIP files will be blocked.
- C. E-mail downloads of ZIP files will be blocked.
- D. ZIP files can be renamed with a new extension to pass through the filter.

Correct Answer: A

QUESTION 5

After using Security Director to add a new firewall policy rule on an SRX Series device, you notice that the hit count on the policy is not increasing. Upon further investigation, you find that the devices listed in the new rule are able to communicate as expected. Your firewall policy consists of hundreds of rules.

Using only Security Director, how do you find the rule that is allowing the communication to occur in this scenario?

- A. Generate a Top Firewall Rules report.
- B. Generate a Policy Analysis report.
- C. Generate a Top Source IPs report.
- D. Generate a Top Firewall Events report.

Correct Answer: D

[Latest JN0-634 Dumps](#)

[JN0-634 Study Guide](#)

[JN0-634 Braindumps](#)