

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.certbus.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 interfaces
ge-0/0/0 {
  unit 0 {
    family inet {
      dhcp-client;
    }
  }
}
ge-0/0/1 {
  unit 0 {
    family inet {
      address 192.168.161.154/24;
    }
  }
}
ge-0/0/2 {
  unit 0 {
    family ethernet-switching {
      vlan {
        members v10;
      }
    }
  }
}
ge-0/0/3 {
  unit 0 {
    family ethernet-switching {
      vlan {
        members v10;
      }
    }
  }
}
fxp0 {
  unit 0 {
    family inet {
      dhcp-client;
    }
  }
}

user@host# show security zones
security-zone trust {
  tcp-rst;
  host-inbound-traffic {
    system-services {
      all;
    }
    protocols {
      all;
    }
  }
  interfaces {
    ge-0/0/1.0;
    ge-0/0/2.0;
  }
}
security-zone untrust {
  screen untrust-screen;
  host-inbound-traffic {
    system-services {
      dhcp;
      ping;
      ssh;
      ike;
    }
  }
  interfaces {
    ge-0/0/0.0;
  }
}
security-zone protected {
  host-inbound-traffic {
    system-services {
      dhcp;
      ping;
      ssh;
      ike;
    }
  }
  interfaces {
    ge-0/0/3.0;
  }
}

user@host# show vlans
v10 {
  vlan-id 10;
}

```

You have enabled mixed mode on an SRX Series device. You are unable to commit the configuration shown in the exhibit.

What is the problem in this scenario?

- A. A Layer 3 interface has not been configured on VLAN v10.
- B. The trust zone cannot contain both Layer 2 and Layer 3 interfaces.
- C. STP is not enabled under the host-inbound-traffic system services hierarchy on the trust and protected security zones.
- D. An IRB interface has not been configured.

Correct Answer: B

QUESTION 2

You need to add all of the sites in the domain example.com to urllist2. You decide to use wildcards to account for any changes made to the domain in the future.

In this scenario, which two commands would you use to meet this requirement? (Choose two.)

- A. set custom-objects url-pattern urllist2 value http://*.example.com
- B. set custom-objects url-pattern urllist2 value http://*example.com
- C. set custom-objects url-pattern urllist2 value http://*.example.???
- D. set custom-objects url-pattern urllist2 value http://*.example.*

Correct Answer: AC

QUESTION 3

After downloading the new IPS attack database, the installation of the new database fails. What caused this condition?

- A. The new attack database no longer contained an attack entry that was in use.
- B. The new attack database was revoked between the time it was downloaded and installed.
- C. The new attack database was too large for the device on which it was being installed.
- D. Some of the new attack entries were already in use and had to be deactivated before installation.

Correct Answer: A

QUESTION 4

What is the correct application mapping sequence when a user goes to Facebook for the first time through an SRX Series device?

- A. first packet > process packet > check application system cache > classify application > process packet > match and identify application
- B. first packet > check application system cache > process packet > classify application > match and identify application
- C. first packet > check application system cache > classify application > process packet > match and identify application
- D. first packet > process packet > check application system cache > classify application > match and identify application

Correct Answer: D

QUESTION 5

Which feature of Sky ATP is deployed with Software-Defined Secure Networks?

- A. zero-day threat mitigation
- B. software image snapshot support
- C. device inventory management
- D. service redundancy daemon configuration support

Correct Answer: A

QUESTION 6

Click the Exhibit button.

```
user@host# show security advance-policy-based-routing
profile profile1 {
  rule rule-appl {
    match {
      dynamic-application junos:HTTP;
    }
    then {
      routing-instance R1;
    }
  }
  rule rule-app2 {
    match {
      dynamic-application junos:junos:web:social-networking;
    }
    then {
      routing-instance R2;
    }
  }
  rule rule-app3 {
    match {
      dynamic-application junos:YAHOO;
    }
    then {
      routing-instance R3;
    }
  }
}
```

Your organization requests that you direct Facebook traffic out a different link to ensure that the bandwidth for critical applications is protected.

Referring to the exhibit, which forwarding instance will be used on your SRX Series device?

- A. R3
- B. R1
- C. R2
- D. inet.0

Correct Answer: C

QUESTION 7

Click the Exhibit button.

```
[edit]
user@host# show interfaces
ge-0/0/3 {
  unit 0 {
    family inet {
      address 10.1.1.1/24;
    }
  }
}
ge-0/0/4 {
  unit 0 {
    family ethernet-switching {
      interface-mode access;
      vlan;
      members SV;
    }
  }
}
ge-0/0/5 {
  unit 0 {
    family ethernet-switching {
      interface-mode access;
      vlan {
        members SV;
      }
    }
  }
}
irb {
  unit 0 {
    family inet {
      address 172.20.101.101/24;
    }
  }
}

[edit]
user@host# show vlans
SV {
  vlan-id 101;
  13-interface irb.0;
}

[edit]
user@host# show security zones security-zone L2
interfaces {
  irb.0;
}

[edit]
user@host# show security polciies

[edit]
user@host#

[edit]
user@host# run show ethernet-switching global-information
Global Configuration:

MAC aging interval      : 300
MAC learning            : Enabled
MAC statistics          : Disabled
MAC limit Count         : 65535
MAC limit hit           : Disabled
MAC packet action drop  : Disabled
LE aging time           : 1200
LE VLAN aging time      : 1200
Global Mode             : Transparent bridge
```

Two hosts on the same subnet are connected to an SRX340 using interfaces ge-0/0/4 and ge-0/0/5. The two hosts can communicate with each other, but they cannot communicate with hosts outside of their subnet.

Referring to the exhibit, which three actions would you take to solve this problem? (Choose three.)

- A. Add the ge-0/0/4 and ge-0/0/5 interfaces to the L2 zone.
- B. Remove the irb.0 interface from the L2 zone.
- C. Set the SRX340 to Ethernet switching mode.
- D. Configure a security policy to permit the traffic.
- E. Reboot the SRX340.

Correct Answer: CDE

QUESTION 8

SRX Series devices with AppSecure support which three custom signatures? (Choose three.)

- A. MAC address-based mapping
- B. latency detection mapping
- C. IP protocol-based mapping
- D. ICMP-based mapping
- E. Layer 7-based signatures

Correct Answer: CDE

QUESTION 9

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 10

Your manager has noticed a drop in productivity and believes it is due to employees checking their social media feeds too frequently. You are asked to provide analytical statistics for this traffic within your network on an hourly basis.

Which AppSecure feature should be used to collect this information?

- A. AppQoS
- B. AppFW
- C. AppTrack
- D. APBR

Correct Answer: C

QUESTION 11

Click the Exhibit button.

```
[edit services advanced-anti-malware policy SKY_policy1]
user@host# show
match {
    application HTTP;
    verdict-threshold 6;
}
then {
    action block;
    notification {
        log;
    }
}
inspection-profile Test_Profile;
fallback-options {
    action permit;
    notification {
        log;
    }
}
default-notification {
    log;
}
whitelist-notification {
    log;
}
blacklist-notification {
    log;
}
```

Referring to the exhibit, you have configured a Sky ATP policy to inspect user traffic. However, you have noticed that encrypted traffic is not being inspected.

In this scenario, what must you do to solve this issue?

- A. Change the policy to inspect HTTPS traffic.
- B. Configure the PKI feature.
- C. Configure the SSL forward proxy feature.
- D. Change the policy to inspect TLS traffic.

Correct Answer: C

QUESTION 12

Which two statements about the integrated user firewall feature of the Junos OS are true? (Choose two.)

- A. The maximum number of supported active directory servers is ten.
- B. IPv6 addresses are not supported.
- C. The maximum number of supported active directory servers is five.
- D. IPv6 addresses are supported.

Correct Answer: AB

QUESTION 13

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

QUESTION 14

Click the Exhibit button.

```
[edit]
user@host# show security policies from-zone internet to-zone dmz
policy dmz-poll {
    match {
        source-address any;
        destination-address any;
        application any;
    }
    then {
        permit {
            application-services {
                idp;
            }
        }
        log {
            session-close;
        }
    }
}

[edit]
user@host# show security idp
idp-policy idp-poll {
    rulebase-ips {
        rule r1 {
            match {
                attacks {
                    predefined-attack-groups "HTTP All";
                }
            }
            then {
                action {
                    ignore-connection;
                }
            }
        }
        rule r2 {
            match {
                attacks {
                    predefined-attack-groups "DNS All";
                }
            }
            then {
                action {
                    close-server;
                }
                ip-action {
                    ip-notify;
                }
            }
        }
    }
}
```

Referring to the configuration shown in the exhibit, which statement explains why traffic matching the IDP signature DNS:OVERFLOW:TOO-LONG-TCP-MSG is not being stopped by the SRX Series device?

- A. The security policy dmz-pol1 has an action of permit.
- B. The IDP policy idp-pol1 is not configured as active.
- C. The IDP rule r2 has an ip-action value of notify.
- D. The IDP rule r1 has an action of ignore-connection.

Correct Answer: B

QUESTION 15

You have been notified by your colocation provider that your infrastructure racks will no longer be adjacent to each other.

In this scenario, which technology would you use to secure all Layer 2 and Layer 3 traffic between racks?

- A. IPsec
- B. GRE
- C. 802.1BR
- D. MACsec

Correct Answer: D

[JN0-634 Practice Test](#)

[JN0-634 Study Guide](#)

[JN0-634 Braindumps](#)