# jn0-634 Dumps

# Security, Professional (JNCIP-SEC)

## https://www.certleader.com/jn0-634-dumps.html

**NEW QUESTION 1**
Which statement about transparent mode on an SRX340 is true?

A. You must reboot the device after configuring transparent mode.
B. Security policies applied to transparent mode zones require Layer 2 address matching.
C. Screens are not supported in transparent mode security zones.
D. All interfaces on the device must be configured with the ethernet-switching protocol family.

**Answer:** A


**NEW QUESTION 2**
Your manager has identified that employees are spending too much time posting on a social media site. You are asked to block user from posting on this site, but they should still be able to access any other site on the Internet.
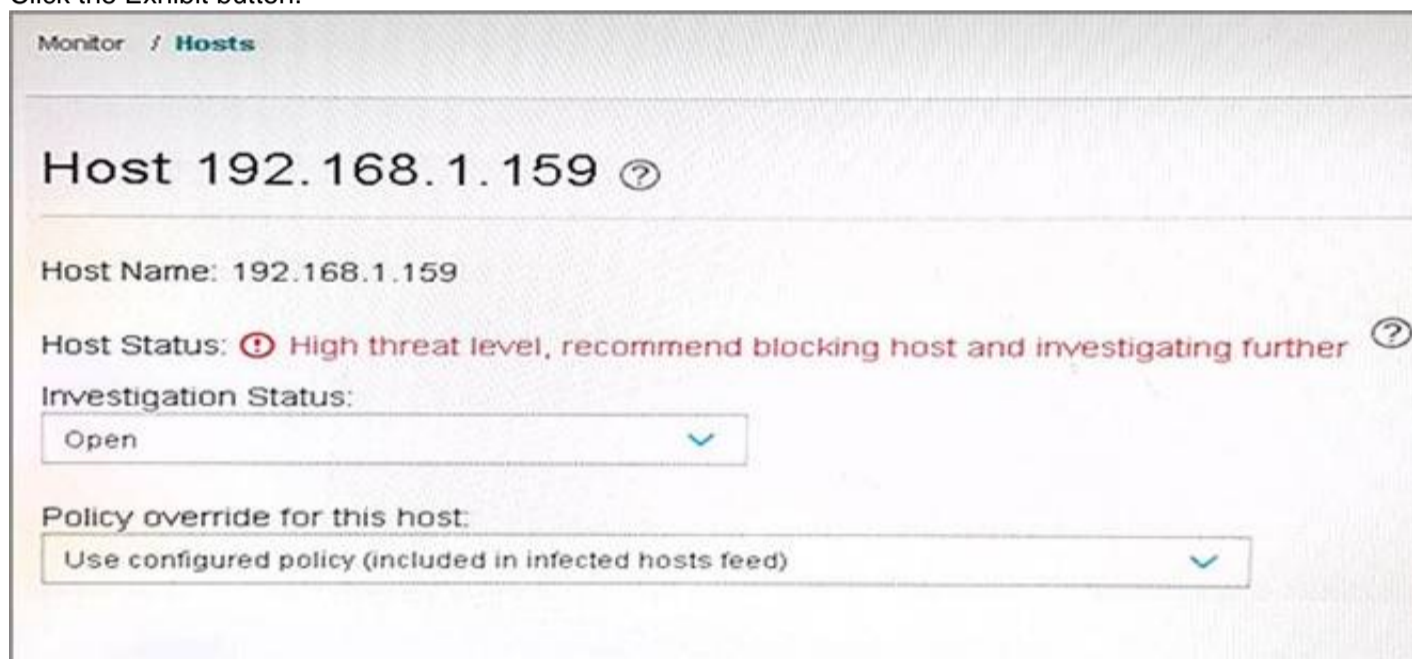In this scenario, which AppSecure feature will accomplish this task?

A. AppQoS
B. AppTrack
C. APpFW
D. APBR

**Answer:** C


**NEW QUESTION 3**
Click the Exhibit button.



Referring to the exhibit, the host has been automatically blocked from communicating on the network because a malicious file was downloaded. You cleaned the infected host and changed the investigation status to Resolved – Fixed.
What does Sky ATP do if the host then attempts to download a malicious file that would result in a threat score of 10?

A. Sky ATP does not log the connection attempt and an SRX Series device does not allow the host to communicate on the network.
B. Sky ATP logs the connection attempt and an SRX Series device does not allow the host to communicate on the network.
C. Sky ATP logs the connection attempt and an SRX Series device allows the host to communicate on the network.
D. Sky ATP does not log the connection attempt and an SRX Series device allows the host to communicate on the network.

**Answer:** C


**NEW QUESTION 4**
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 rl {
            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.

**Answer:** B

**NEW QUESTION 5**
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

**Answer:** D

**NEW QUESTION 6**
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.

**Answer:** A

**NEW QUESTION 7**
Which interface family is required for Layer 2 transparent mode on SRX Series devices?

A. LLDP
B. Ethernet switching
C. inet
D. VPLS

**Answer:** B

**NEW QUESTION 8**
You are using the integrated user firewall feature on an SRX Series device.
Which three parameters are stored in the Active Directory authentication table? (Choose three.)

A. IP address
B. MAC address
C. group mapping
D. username
E. password

**Answer:** ACD

**NEW QUESTION 9**
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.

**Answer:** C

**NEW QUESTION 10**
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 {
```

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.

**Answer:** B


**NEW QUESTION 10**
Click the Exhibit button.

```
[edit]
user@host# show interfaces ge-0/0/4
unit 0 {
      family ethernet-switching {
            interface-mode access;
            vlan {
                  members SV;
            }
      }
}

[edit]
user@host# show interfaces ge-0/0/5
unit 0 {
      family ethernet-switching {
            interface-mode access;
            vlan {
                  members SV;
            }
      }
}

[edit]
user@host# show vlans
SV {
      vlan-id 101;
}

[edit]
user@host# show security forwarding-options
secure-wire {
      access-sw {
            interface [ ge-0/0/4 ge-0/0/5 ];
      }
}

[edit]
user@host# commit
[edit security forwarding-options secure-wire access-sw]
      'interface ge-0/0/4'
            Interface name ge-0/0/4 is not valid
[edit security forwarding-options secure-wire access-sw]
      'interface ge-0/0/4'
            Error: two and only two logical interfaces are required for a
secure-wire
error: configurartion check-out failed
```

You are trying to implement secure wire on your SRX Series device. However, you are receiving the commit error shown in the exhibit.
What must you do to solve the problem?

A. Add the correct logical units to the interfaces in the secure wire.
B. Put the ge-0/0/4 and ge-0/0/5 interfaces in separate secure wires.
C. Change the Ethernet switching mode from access to trunk for the ge-0/0/4 and ge-0/0/5 interfaces.
D. Add the ge-0/0/4 and ge-0/0/5 interfaces to the SV VLAN.

**Answer:** A


**NEW QUESTION 12**
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.

**Answer:** CDE


**NEW QUESTION 15**

You have set up Sky ATP with the SRX Series devices in your network. However, your SRX Series devices are unable to communicate with the Sky ATP cloud because the communication is being blocked by a gateway network device.
Which two actions should you take to solve the problem? (Choose two.)

A. Open destination port 443 inbound from the Internet on the gateway network device.
B. Open destination port 8080 outbound from the Internet on the gateway network device.
C. Open destination port 443 outbound from the Internet on the gateway network device.
D. Open destination port 8080 inbound from the Internet on the gateway network device.

**Answer:** CD

**NEW QUESTION 20**
Your network includes SRX Series devices at the headquarters location. The SRX Series devices at this location are part of a high availability chassis cluster and are expected to support several UTM features.
Which two statements related to this environment are true? (Choose two.)

A. UTM features can be configured on either of the nodes within the cluster.
B. The chassis cluster must be configured for active/active mode.
C. UTM features must be configured on the primary node within the cluster.
D. The chassis cluster must be configured for active/backup mode.

**Answer:** AD

**NEW QUESTION 25**
Your network includes SRX Series devices at the headquarters location. The SRX Series devices at this location are part of a high availability chassis cluster and are configured for IPS. There has been a node failover.
In this scenario, which statement is true?

A. Existing sessions continue to be processed by IPS because of table synchronization.
B. Existing sessions are no longer processed by IPS and become firewall sessions.
C. Existing session continue to be processed by IPS as long as GRES is configured.
D. Existing sessions are dropped and must be reestablished so IPS processing can occur.

**Answer:** A

**NEW QUESTION 28**
What are three components of Software-Defined Secure Networks? (Choose three.)

A. Contrail
B. Sky ATP
C. SRX Series device
D. Security Director
E. Network Director

**Answer:** BCD

**NEW QUESTION 33**
Which AppSecure feature identifies applications that are present in traffic?

A. AppID
B. AppTrack
C. AppFW
D. AppQoS

**Answer:** A

**NEW QUESTION 37**
You are implementing user authentication on your network using an SRX Series device and want to ensure that there are redundant forms of authentication for users to access the network. You have configured the device with the integrated user firewall and user role firewall features. You are testing failover methods using the default priority values.
In this scenario, which two statements are true? (Choose two.)

A. If the user fails local authentication, then the Junos OS will attempt to authenticate the user with a user role firewall.
B. If the user fails user role firewall authentication, then the Junos OS will attempt to authenticate the user with an integrated user firewall.
C. If the user fails integrated user firewall authentication, then the Junos OS will attempt to authenticate with a user role firewall.
D. If the user fails local authentication, then the Junos OS will attempt to authenticate the user with an integrated user firewall.

**Answer:** CD

**NEW QUESTION 38**
Your manager has notices 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

**Answer:** C

**NEW QUESTION 43**
What is the required when deploying a log collector in Junos Space?

A. root user access to the log collector
B. a shared log file directory on the log collector
C. the IP address of interface eth1 on the log collector
D. a distributed deployment of the log collector nodes

**Answer:** A

**NEW QUESTION 47**
Click the Exhibit button.

```
<12>1 2016-02-18T01:32:50.391Z utm-srx550-b RT_UTM - WEBFILTER_URL_BLOCKED
[junos@2636.1.1.1.2.86 source-address="192.0.2.3" source-port="32056"
destination-address="198.51.100.2" destination-port="80" category="cat1"
reason="BY_BLACK_LIST" profile="uf1" url="www.example.com" obj="/"
username="N/A" roles="N/A] WebFilter: ACTION="URL Blocked" 192.0.2.3(32056)-
>198.51.100.2(80) CATEGORY="cat1" REASON="BY_BLACK_LIST" PROFILE="uf1"
URL=www.example.com OBJ=/ username N/A roles N/A
```

A customer submits a service ticket complaining that access to http://www.example.com/ has been blocked.
Referring to the log message shown in the exhibit, why was access blocked?

A. All illegal source port was utilized.
B. The URI matched a profile entry.
C. The user/role permissions were exceeded.
D. There was a website category infraction.

**Answer:** B

**NEW QUESTION 52**
Using the Policy Controller API, which configuration would post Sky ATP with PE mode to the Policy Enforcer controller configuration?

A. "configs": {"sdsn": false"cloudonly": true}
B. "configs": {"sdsn": false"cloud": false}
C. "configs": {"sdsn": true"cloudonly": false}
D. "configs": {"sdsn": false"cloud": true}

**Answer:** C

**NEW QUESTION 54**
......

# Thank You for Trying Our Product

* 100% Pass or Money Back

    All our products come with a 90-day Money Back Guarantee.

* One year free update

    You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

    We currently serve more than 30,000,000 customers.

* Shop Securely

    All transactions are protected by VeriSign!

**100% Pass Your jn0-634 Exam with Our Prep Materials Via below:**

https://www.certleader.com/jn0-634-dumps.html