

## 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**

Click the Exhibit button.

```
user@host> 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              : Switching
```

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

- A. You can secure inter-VLAN traffic with a security policy on this device.
- B. You can secure intra-VLAN traffic with a security policy on this device.
- C. The device can pass Layer 2 and Layer 3 traffic at the same time.
- D. The device cannot pass Layer 2 and Layer 3 traffic at the same time.

**Answer:** AC

**NEW QUESTION 3**

You are using IDP on your SRX Series device and are asked to ensure that the SRX Series device has the latest IDP database, as well as the latest application signature database.

In this scenario, which statement is true?

- A. The application signature database cannot be updated on a device with the IDP database installed.
- B. You must download each database separately.
- C. The IDP database includes the latest application signature database.
- D. You must download the application signature database before installing the IDP database.

**Answer:** C

**NEW QUESTION 4**

Click the Exhibit button.

```
[edit security utm]
user@host# show
custom-objects {
    url-pattern {
        allow {
            value "user@example.com";
        }
        reject {
            value "user@example.com";
        }
    }
}
feature-profile {
    anti-spam {
        address-whitelist allow;
        address-blacklist reject;
        sbl {
            profile AS {
                sbl-default-server;
                spam-action block;
                custom-tag-string SPAM;
            }
        }
    }
}
```

Referring to the exhibit, which statement is true?

- A. E-mails from the user@example.com address are marked with SPAM in the subject line by the spam block list server.
- B. E-mails from the user@example.com address are blocked by the spam list server.
- C. E-mails from the user@example.com address are blocked by the reject blacklist.
- D. E-mails from the user@example.com address are allowed by the allow whitelist.

**Answer:** D

#### NEW QUESTION 5

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 6

While reviewing the Log and Reporting portion of Security Director, you find that multiple objects reference the same address. You want to use a standardized name for all of the objects.

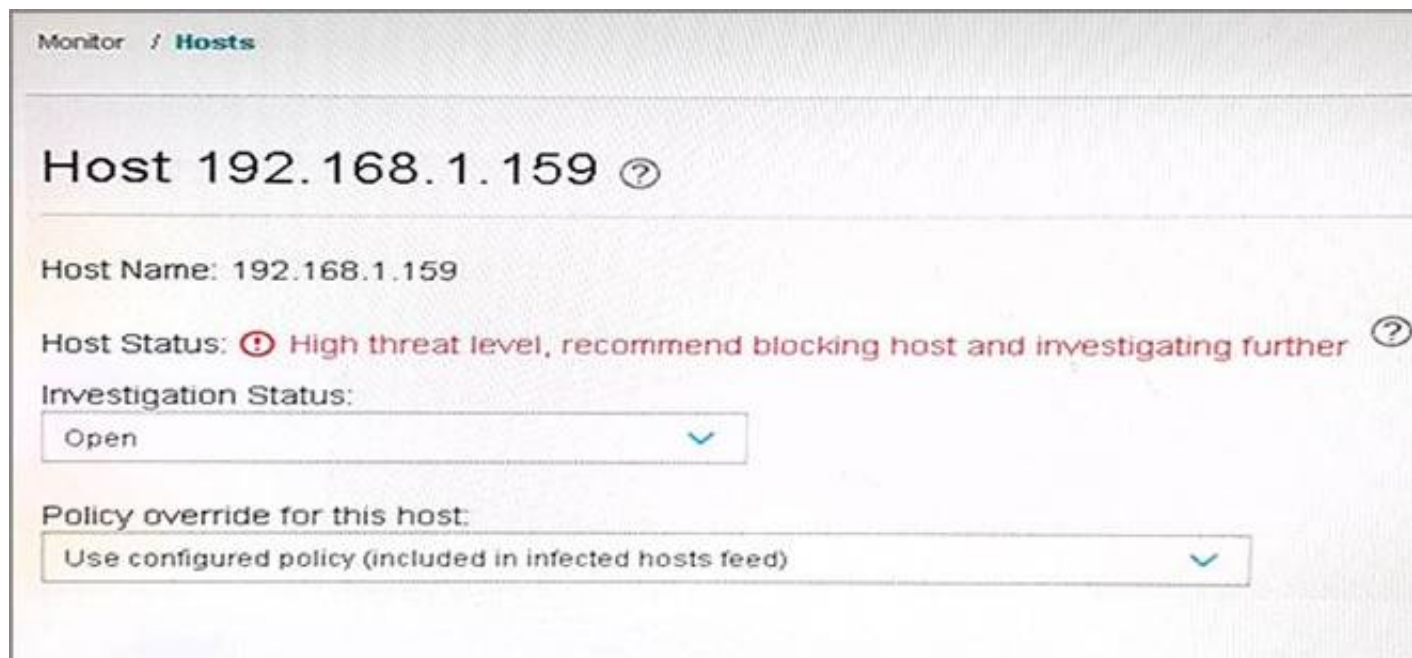
In this scenario, how would you create a standardized object name without searching the entire policy?

- A. Remove the duplicate objects.
- B. Merge the duplicate objects.
- C. Rename the duplicate objects.
- D. Replace the duplicate objects.

**Answer:** B

#### NEW QUESTION 7

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 8

Click the Exhibit button.

```
[edit]
user@host# show security policies from-zone internet to-zone dmz
policy dmz-pol1 {
    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-pol1 {
    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.

**Answer:** B

#### NEW QUESTION 9

Your network includes SRX Series devices at the headquarters location. The SRX Series devices at this location are part of a high available chassis cluster and are configured for IPS. There has been a node failover.

In this scenario, which two statements are true? (Choose two.)

- A. The IP action table is synchronized between the chassis cluster nodes.
- B. Cached SSL session ID information for existing sessions is not synchronized between nodes.
- C. The IP action table is not synchronized between the chassis cluster nodes.
- D. Cached SSL session ID information for existing session is synchronized between nodes.

**Answer:** CD

#### NEW QUESTION 10

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 10

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 14

Which Junos security feature is used for signature-based attack prevention?

- A. RADIUS
- B. AppQoS
- C. IPS
- D. PIM

**Answer:** C

#### NEW QUESTION 16

Click the Exhibit button.

```
policy allow-all {
  match {
    source-address any;
    destination-address any;
    application any;
  }
  then {
    permit {
      application-services {
        idp;
        utm-policy wf-policy_websense-home;
        application-firewall {
          rule-set demo-tracking_1;
        }
      }
    }
    log {
      session-init;
      session-close;
    }
  }
}
```

According to the policy shown in the exhibit, which application-services traffic will be processed first?

- A. the application traffic matchings the IDP rules
- B. the application traffic matchings the utm-policy log rule set
- C. the application traffic matchings the utm-policy wf-policy\_websense-home rules
- D. the application traffic matchings the application-firewall rule-set demo-tracking\_1 rule

**Answer:** A

#### NEW QUESTION 17

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 18

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-0/0/0;
  }
}
```

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 19

You are creating an IPS policy with multiple rules. You want traffic that matches rule 5 to silently be dropped, along with any future packets that match the appropriate attributes of the incoming traffic.

In this scenario, which ip-action parameter should you use?

- A. ip-block
- B. ip-close
- C. log-create
- D. timeout

**Answer: A**

#### NEW QUESTION 24

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

**Answer: CDE**

#### NEW QUESTION 25

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

**Answer: A**

#### NEW QUESTION 26

You have configured a log collector VM and Security Director. System logging is enabled on a branch SRX Series device, but security logs do not appear in the monitor charts.

How would you solve this problem?

- A. Configure a security policy to forward logs to the collector.
- B. Configure application identification on the SRX Series device.
- C. Configure security logging on the SRX Series device.
- D. Configure J-Flow on the SRX Series device.

**Answer: C**

#### NEW QUESTION 27

Click the Exhibit button.



Security Director is reporting the events shown in the exhibit.

If the fallback parameter is set to pass traffic, what would cause the events?

- A. The files are too large for the antivirus engine to process.
- B. The files are not scanned because they were permitted by a security policy.
- C. The files are not scanned because they are the wrong file format.
- D. The antivirus engine is unable to re-encrypt the files.

**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

What is a function of UTM?

- A. AppFW
- B. IPsec
- C. content filtering
- D. bridge mode

**Answer: C**

#### NEW QUESTION 34

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

**Answer:** C

#### NEW QUESTION 36

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="ufl" 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="ufl"
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 37

.....

## 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>