

Juniper

Exam Questions jn0-634

Security, Professional (JNCIP-SEC)



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 security idp
idp-policy base-policy {
  rulebase-ips {
    rule R1 {
      match {
        from-zone trust;
        source-address any;
        to-zone untrust;
        destination-address any;
        application default;
        attacks {
          predefined-attack-groups HTTP-Critical;
        }
      }
      then {
        action {
          mark-diffserv {
            10;
          }
        }
      }
    }
  }
}
```

Referring to the security policy shown in the exhibit, which two actions will happen as the packet is processed? (Choose two.)

- A. It passes unmatched traffic after modifying the DSCP priority.
- B. It marks and passes matched traffic with a high DSCP priority.
- C. It marks and passes matched traffic with a low DSCP priority.
- D. It passes unmatched traffic without modifying DSCP priority.

Answer: BD

NEW QUESTION 3

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 4

You have implemented APBR on your SRX Series device and are verifying that your changes are working properly. You notice that when you start the application for the first time, it does not follow the expected path.

What are two reasons that would cause this behavior? (Choose two.)

- A. The application system cache does not have an entry for the first session.
- B. The application system cache has been disabled.

- C. The application system cache already has an entry for this application.
- D. The advanced policy-based routing is applied to the ingress zone and must be moved to the egress zone.

Answer: AB

NEW QUESTION 5

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 6

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 7

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 8

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 9

You want to review AppTrack statistics to determine the characteristics of the traffic being monitored.
Which operational mode command would accomplish this task on an SRX Series device?

- A. show services application-identification statistics applications
- B. show services application-identification application detail
- C. show security application-tracking counters
- D. show services security-intelligence statistics

Answer: A

NEW QUESTION 10

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

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

Answer: C

NEW QUESTION 10

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 12

Your network includes SRX Series devices at all headquarter, data center, and branch locations. The headquarter and data center locations use high-end SRX Series devices, and the branch locations use branch SRX Series devices. You are asked to deploy IPS on the SRX Series devices using one of the available IPS deployment modes.

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

- A. Inline tap mode provides enforcement.
- B. Inline tap mode can be used at all locations.
- C. Integrated mode can be used at all locations.
- D. Integrated mode provides enforcement.

Answer: CD

NEW QUESTION 15

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 17

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

Answer: D

NEW QUESTION 20

Which IDP rule configuration will send an RST to any new session that meets the action criteria?

- A. ip-action block
- B. action close-client-and-server
- C. ip-action close
- D. action drop-connection

Answer: C

NEW QUESTION 22

Using content filtering on an SRX Series device, which three types of HTTP content are able to be blocked? (Choose three.)

- A. PDF files
- B. ZIP files
- C. Java applets

- D. Active X
- E. Flash

Answer: BCD

NEW QUESTION 23

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.

Answer: D

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 26

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.*

Answer: AC

NEW QUESTION 30

Click the Exhibit button.

```
user@host > show services user-identification authentication-table
authentication-source active-directory
Domain: example
Total entries: 1
Source IP      Username      groups(Ref by policy)  state
192.168.50.8   user1         grp1                   Initial
```

Which statement explains the current state value of the command output shown in the exhibit?

- A. A valid response was received from a domain PC probe, and the user is a valid domain user programmed in the PFE.
- B. An invalid response was received from a domain PC probe, and the user is an invalid domain user.
- C. A probe event generated an entry in the authentication table, but no probe response has been received from the domain PC.
- D. The user-to-address mapping was successfully read from the domain controller event logs, and an entry was added to the authentication table witch currently resides on the Routing Engine.

Answer: A

NEW QUESTION 35

Your network includes SRX Series devices configured with AppSecure.

Which two statements regarding the application identification engine are true? (Choose two.)

- A. Applications are only matched in traffic flows associated with client-to-server sessions.
- B. Applications are matched in traffic flows associated with client-to-server and server-to- client sessions.
- C. If the packets entering the engine match a known application, then processing continues.
- D. If the packets entering the engine match a known application, then processing stops.

Answer: BD

NEW QUESTION 37

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.

Answer: AB

NEW QUESTION 42

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;
    }
  }
}

```

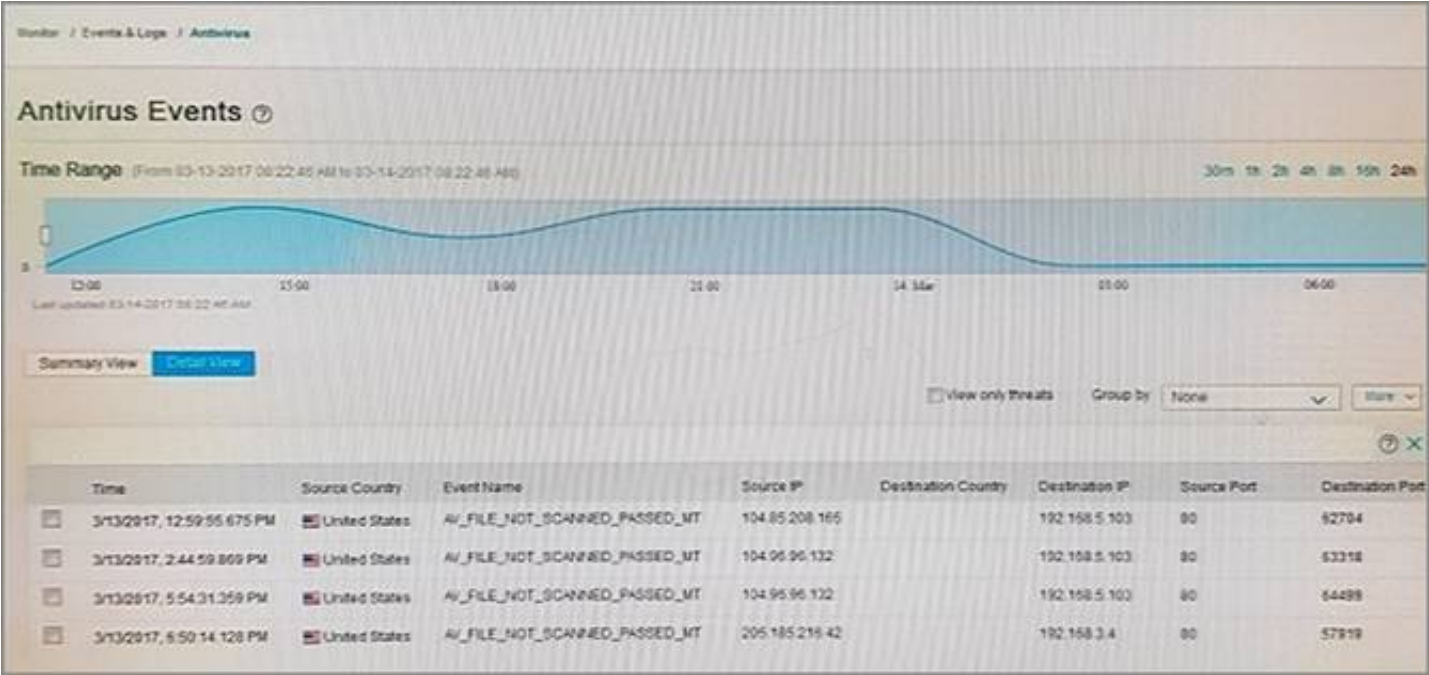
Your organization requests that you direct Facebook traffic out a different link to ensure that the bandwidth for critical applications is protected. Referring to the exhibit, which forwarding instance will be used on your SRX Series device?

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

Answer: C

NEW QUESTION 47

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 48

Which three components are part of the AppSecure services suite? (Choose three.)

- A. IDP
- B. Sky ATP
- C. AppQoS
- D. AppFW
- E. Web filtering

Answer: ACD

NEW QUESTION 53

Which two parameters are required to match in an IDP rule for the terminal option to take effect? (Choose two.)

- A. attacks custom-attacks
- B. attacks predefined-attacks
- C. application
- D. source-address

Answer: AB

NEW QUESTION 57

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 60

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;}

Answer: A

NEW QUESTION 61

Click the Exhibit button.

The exhibit shows two parts: a screenshot of the ESXi 'Resources' tab and a terminal window output.

Resources Tab:

Resource	Value
Consumed Host CPU:	121 MHz
Consumed Host Memory:	12027.00 MB
Active Guest Memory:	655.00 MB
Provisioned Storage:	628.11 GB
Not-shared Storage:	612.11 GB
Used Storage:	612.11 GB

Below the storage summary is a table for the storage pool:

Storage	Drive Type	Capacity	Free Space
rotating-storage	Non-SSD	1.82 TB	68%

Terminal Window:

```
LOG-COLLECTOR login: root
Password:
Last login: Thu Mar  9 20:19:08 from 10.0.1.110
[root@LOG-COLLECTOR ~]# df -h
Filesystem      Size  Used Avail Use% Mounted on
/dev/sda3        11G   1.8G   8.6G  18% /
tmpfs           7.8G     0  7.8G   0% /dev/shm
/dev/sda1        504M   39M  448M   9% /boot
/dev/mapper/data1_vg-elasticsearch 500G   3.8G  497G   1% /var/lib/elasticsearch
[root@LOG-COLLECTOR ~]#
```

Referring to the exhibit, you have expanded the disk storage size in ESXi for your log collector from 500 GB to 600 GB. However, your log collector's disk size has not changed.

Given the scenario, which two statements are true? (Choose two.)

- A. You must run a script from the console to expand the disk size.
- B. The ESXi storage parameter is not associated with the Elasticsearch disk size parameter.
- C. You must reboot the log collector for storage settings to be updated
- D. You must re-run the log collector setup script to update the storage settings.

Answer: AC

NEW QUESTION 63

You are scanning files that are being transferred from the Internet to hosts on your internal network with Sky ATP. However, you notice that files that are 1 GB in size are not being scanned by Sky ATP.

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

- A. The Sky ATP fallback option is set to permit.
- B. The Sky ATP engine or the SRX Series device is too busy.
- C. The 1 GB file size is larger than the scan size limit for Sky ATP.
- D. The Sky ATP policy on the SRX Series device is misconfigured.

Answer: CD

NEW QUESTION 65

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 67

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 71

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

jn0-634 Practice Exam Features:

- * jn0-634 Questions and Answers Updated Frequently
- * jn0-634 Practice Questions Verified by Expert Senior Certified Staff
- * jn0-634 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * jn0-634 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The jn0-634 Practice Test Here](#)