Juniper

Exam Questions jn0-634

Security, Professional (JNCIP-SEC)

NEW QUESTION 1
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 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
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 5
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 6
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.

Answer: B

NEW QUESTION 7
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 8
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 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
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 10
What are three types of content that are filtered by the Junos UTM feature set? (Choose three.)

A. IMAP
B. HTTP
C. SIP
D. SSL
E. FTP

Answer: ABE

NEW QUESTION 14
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.

Answer: C

NEW QUESTION 18
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 19
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 21

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 23
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 24
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 26
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 29
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.

Answer: A

NEW QUESTION 30
Click the Exhibit button.

```
user@host > show services user-identification authentication-table
authentication-source active-directory
Domain: example
Total enteries: 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 31
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 36
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 37
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 42
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 44
Click the Exhibit button.

```
[edit security idp]
user@host# show
idp-policy example-idp-policy {
     rulebase-ips {
          rule r1 {
               match {
                    source-address 10.1.0.0/146;
                    attacks {
                         predefined-attack-groups "HTTP - All";
                    }
               }
               then {
                    action {
                         no-action;
                    }
                    notification {
                         log-attacks;
                    }
               }
          }
rule r2 {
     match {
          source-address 10.1.1.85/32;
          attacks {
               predefined-attack-groups "HTTP - All";
          }
     }
     then {
          action {
               mark-diffserv {
                    8;
               }
          }
     }
}
rule r3 {
     match {
          source-address 10.0.0.0/8;
          attacks {
               predefined-attack-groups "HTTP - All";
          }
     }
     then {
          action {
               drop-connection;
          }
     }
}
rule r4 {
     match {
          source-address any;
          attacks {
               predefined-attack-groups "HTTP - All";
          }
     }
     then {
          action {
               close-client-and-server;
          }
     }
          }
     }
}
```

Referring to the exhibit, a user with IP address 10.1.1.85 generates a request that triggers the HTTP:EXT:DOT-LNK IDP signature that is a member of the "HTTP – All" predefined attack group.
In this scenario, which statement is true?

A. The session will be closed and a reset sent to the client and server.
B. A Differentiated Services code point value of 8 will be applied.
C. No action will be taken and the attack information will be logged.
D. The session will be dropped with no reset sent to the client or server.

Answer: D

NEW QUESTION 48
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

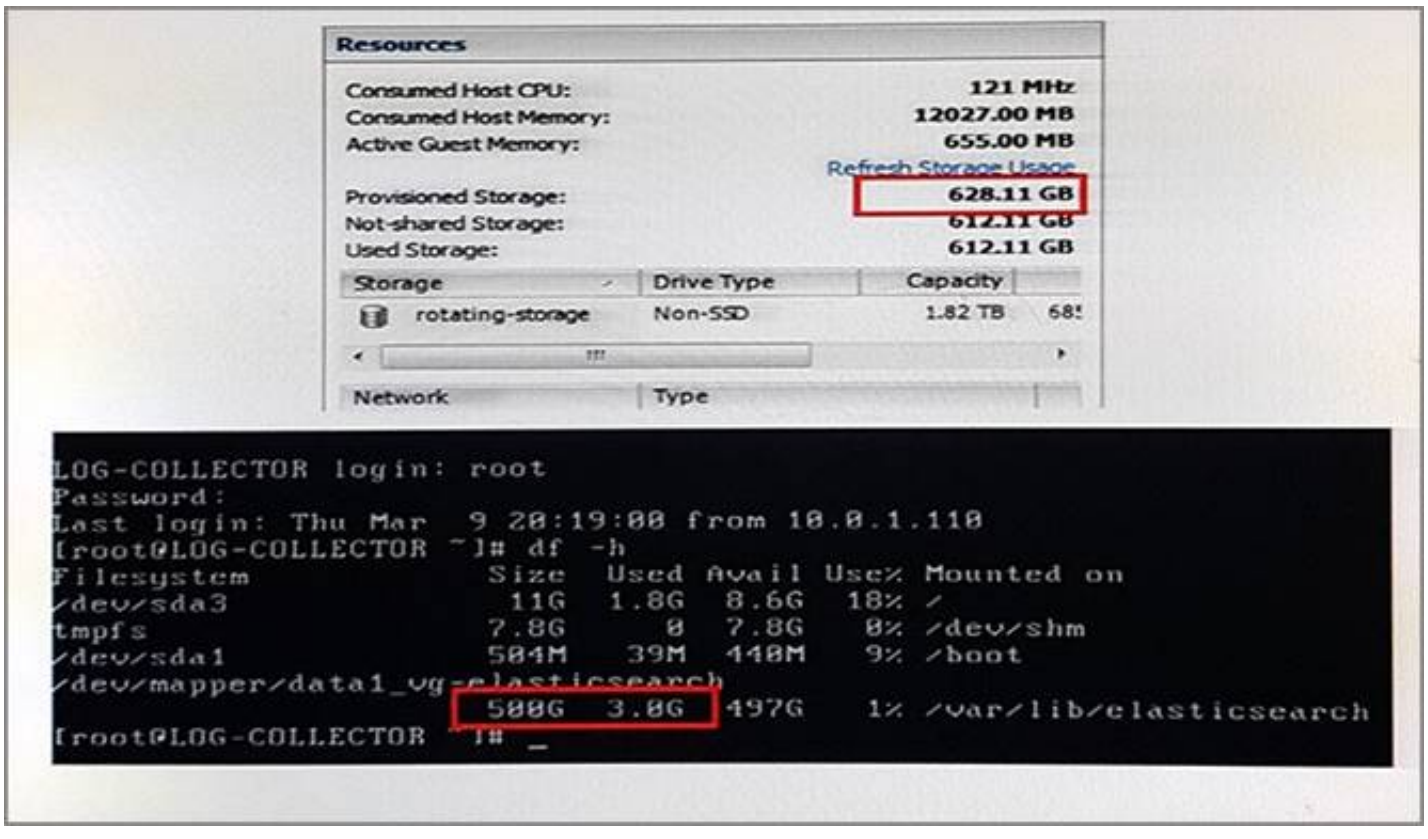
Answer: AB

NEW QUESTION 50
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 51
Click the Exhibit button.



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 52
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 failback 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 56
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 57
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 60
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 63
.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questons 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