Juniper JN0-634 Exam

Volume: 65 Questions

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

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: B,D

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: A,C

Question: 4
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

Question: 5
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

Question: 6
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

Question: 7
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.

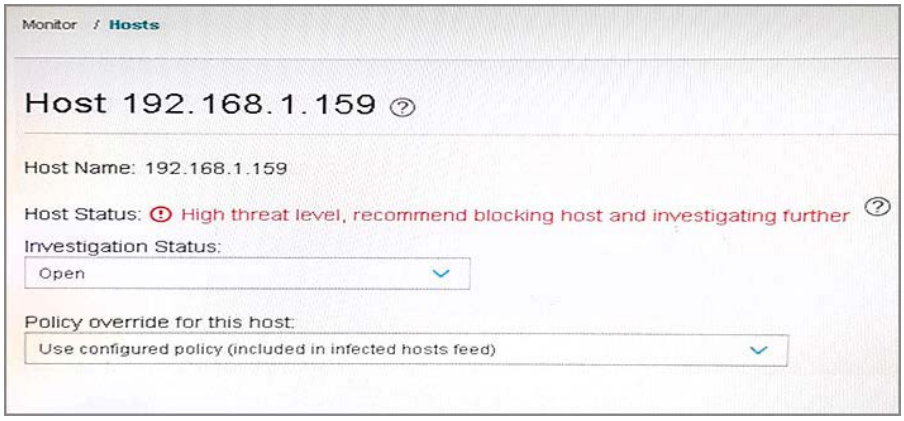
B. Merge the duplicate objects.

C. Rename the duplicate objects.

D. Replace the duplicate objects.

Answer: B

Question: 8
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

Question: 9
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: A,B

Question: 10
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

Question: 11
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: C,D

Question: 12
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

Question: 13
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

Question: 14
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

Question: 15
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

Question: 16
Which Junos security feature is used for signature-based attack prevention?

A. RADIUS

B. AppQoS

C. IPS

D. PIM

Answer: C

Question: 17
Click the Exhibit button.

```
user@host> show security application-firewall rule-set all
Rule-set: demo-tracking_1
     Rule: web-applications
          Dynamic Applications: junos:CNN
          Dynamic Application Groups: junos:social-networking,
          junos:web:advertisments, junos:social-networking:applications,
          junos:web:file-sharing, junos:web:applications, junos:web:gaming
          SSL-Encryption: no
          Action:permit
          Number of sessions matched: 13205
          Number of sessions redirected: 0
Default rule:permit
          Number of sessions matched: 132056
          Number of sessions redirected: 0
Number of sessions with appid pending: 9
```

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

A. The application firewall rule is not inspecting encrypted traffic.

B. There are two rules configured in the rule set.

C. The rule set uses application definitions from the predefined library.

D. The configured rule set matches most analyzed applications.

Answer: A,C

Question: 18
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

Question: 19
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: A,C,D