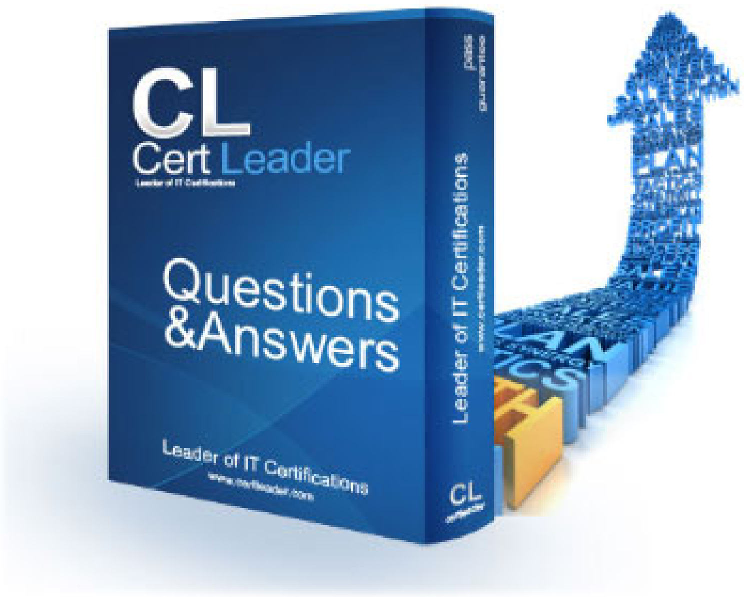
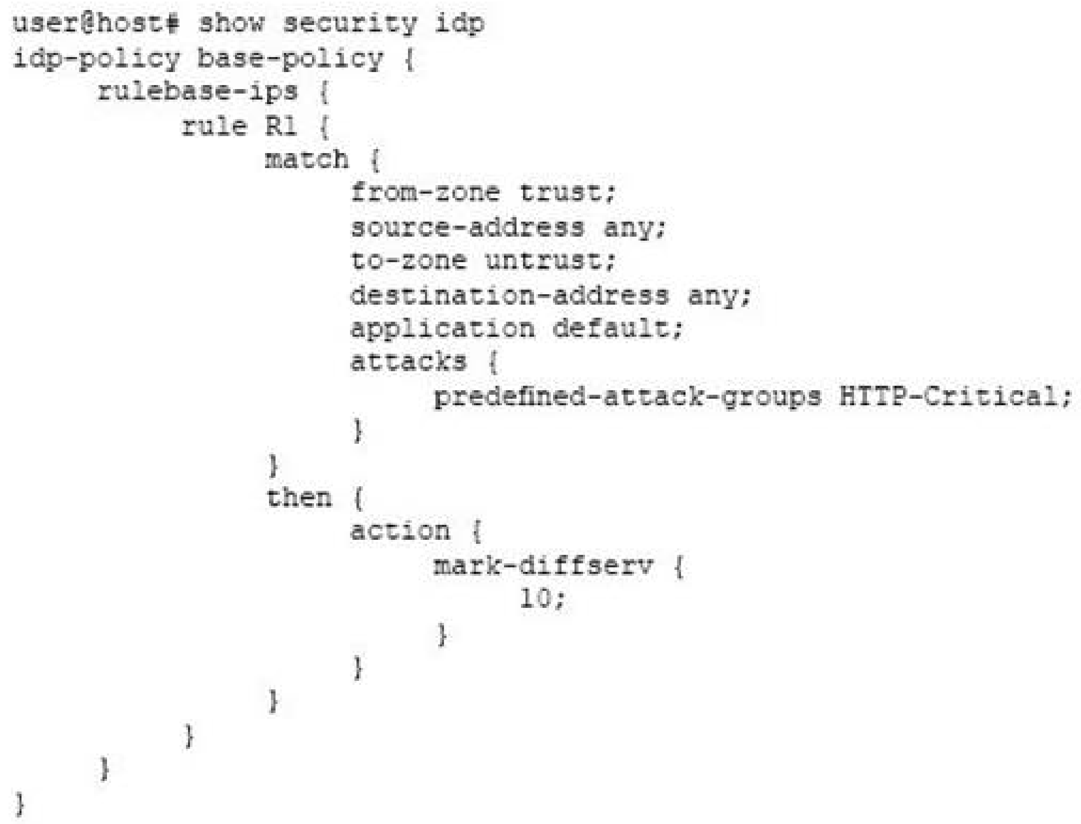
jn0-634 Dumps

Security, Professional (JNCIP-SEC)

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



NEW QUESTION 1
Click the Exhibit button.



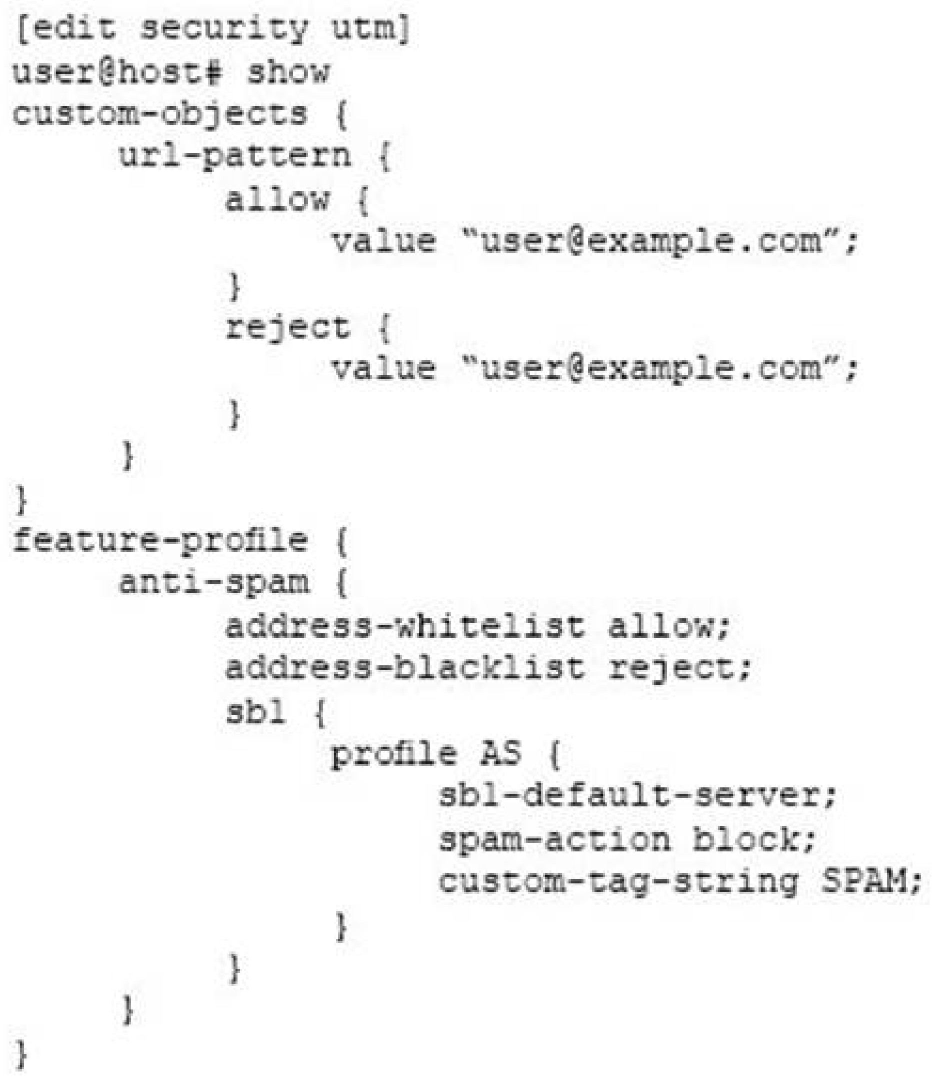
```
user@host# show security idp
idp-policy base-policy {
     rulebase-ips {
          rule R1 {
               match {
                    from-zone trust;
                    source-address any;
                    to-zone untrust;
                    destination-address any;
                    application 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.



```
[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.

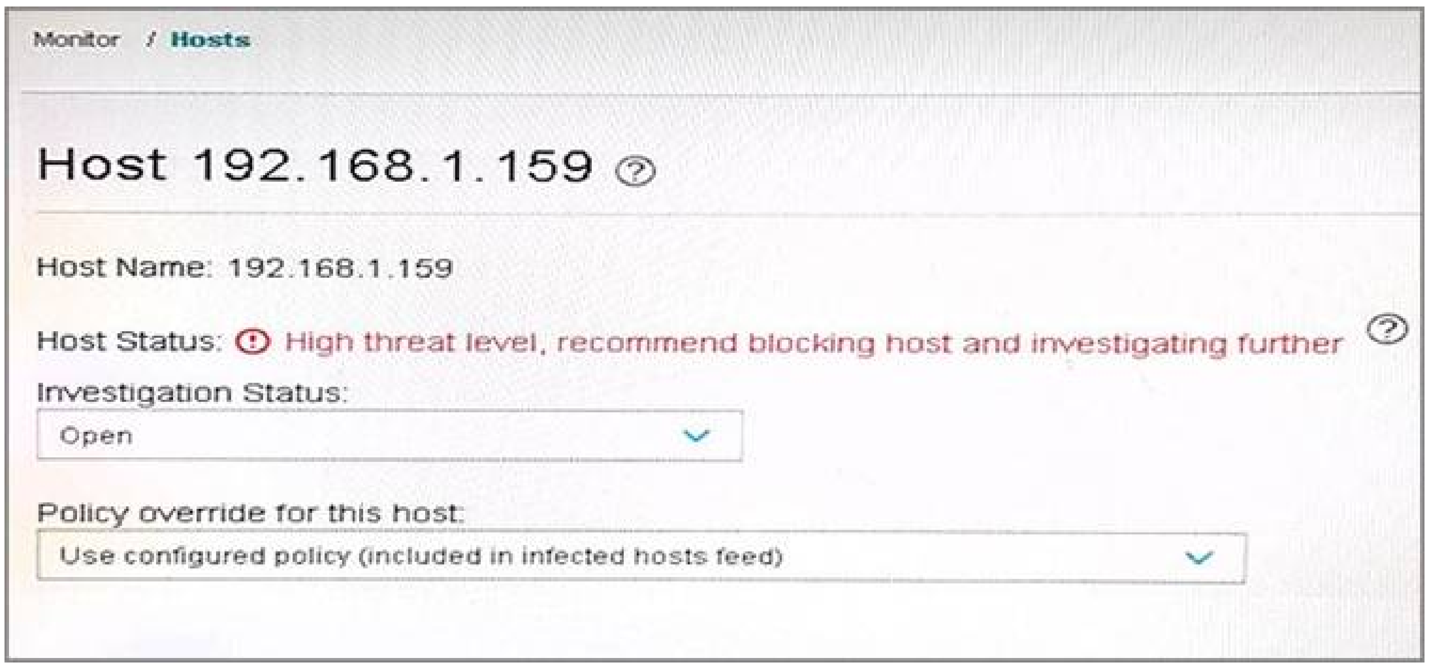
Answer: D

NEW QUESTION 3
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 4
Click the Exhibit button.



Monitor / Hosts

Host 192.168.1.159

Host Name: 192.168.1.159

Host Status: High threat level, recommend blocking host and investigating further

Investigation Status:
Open

Policy override for this host:
Use configured policy (included in infected hosts feed)

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.

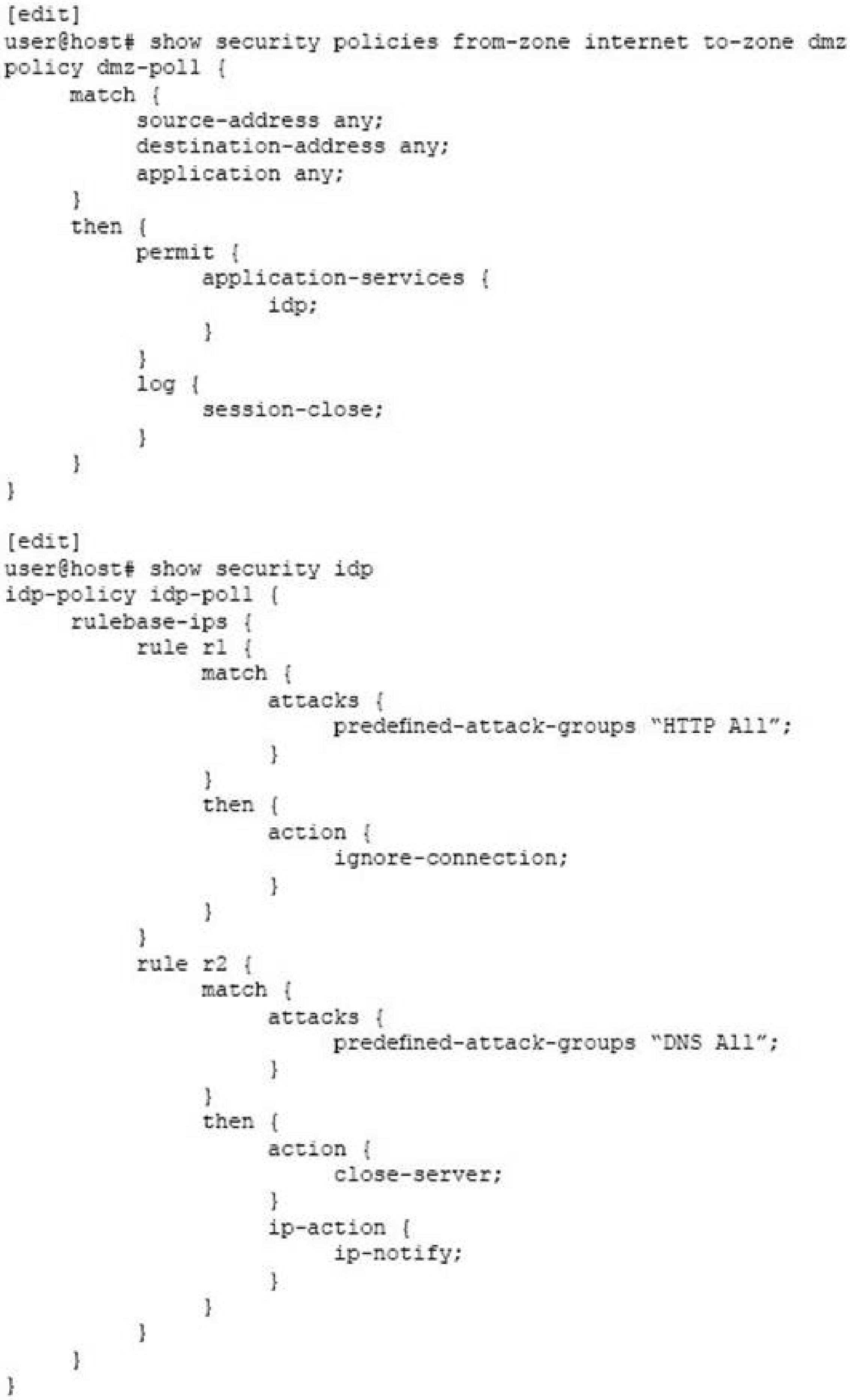
Answer: C

NEW QUESTION 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-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 7
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 8
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 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

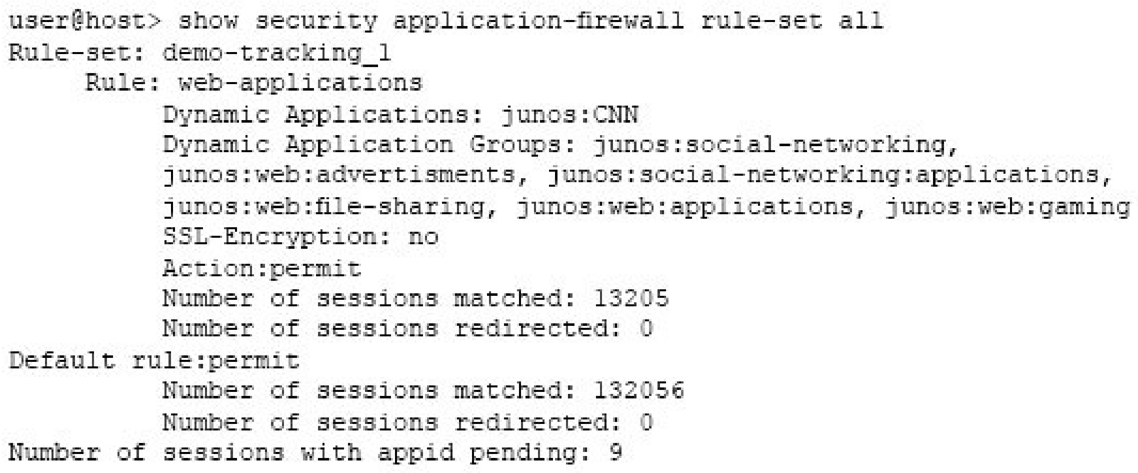
Answer: A

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.



```
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.

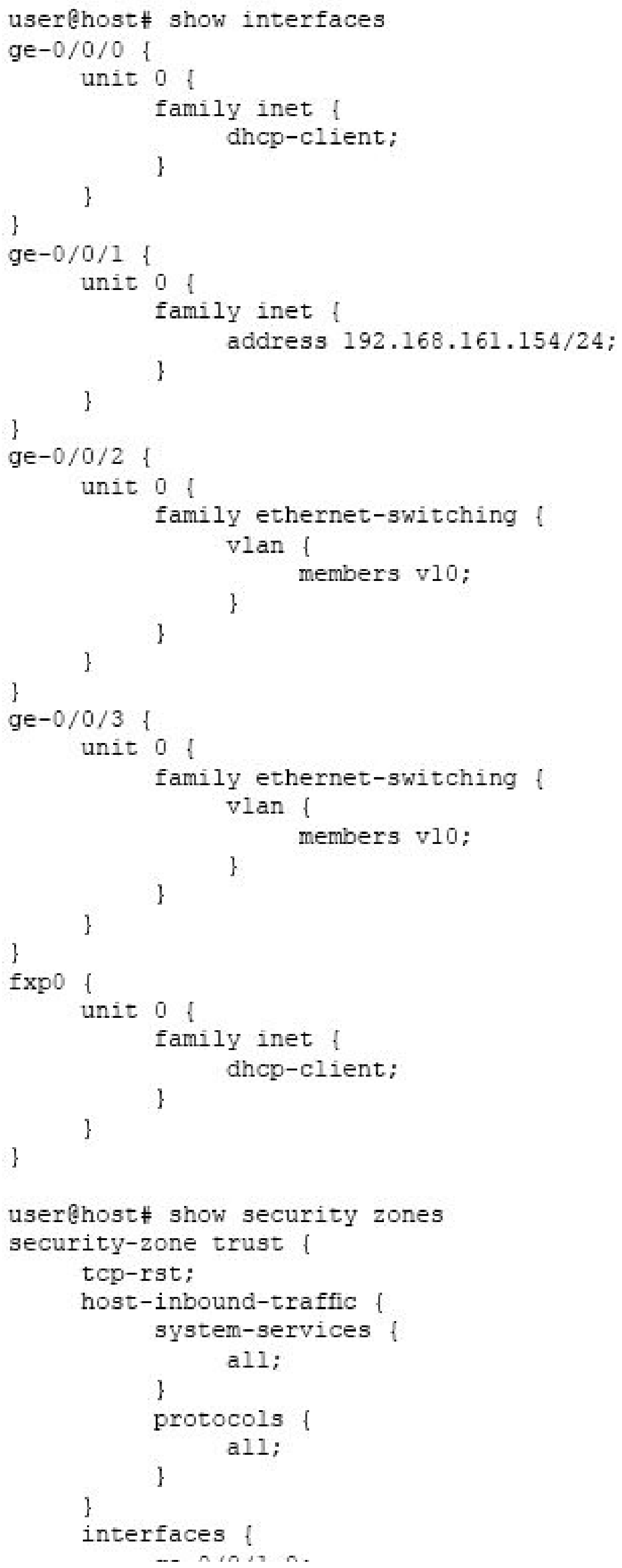
Answer: AC

NEW QUESTION 13
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 17
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-0/0/1.0;
```

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 18
Which browser is supported by Security Director with Logging and Reporting?

A. Firefox
B. Agora
C. PowerBrowser
D. Mosaic

Answer: A

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 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 25
A customer has recently deployed a next-generation firewall, sandboxing software, cloud access security brokers (CASB), and endpoint protection.
In this scenario, which tool would provide the customer with additional attack prevention?

A. Junos Space Cross Provisioning Platform
B. Contrail
C. Security Director Policy Enforcer
D. Network Director Inventory Manager

Answer: C

NEW QUESTION 26
To which three UTM components would the custom-objects parameter apply? (Choose three.)

A. Sky ATP
B. antispam
C. content filtering
D. antivirus
E. Web filtering

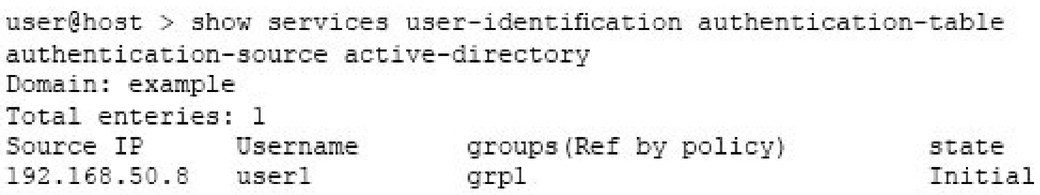
Answer: BCE

NEW QUESTION 31
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 33
Click the Exhibit button.



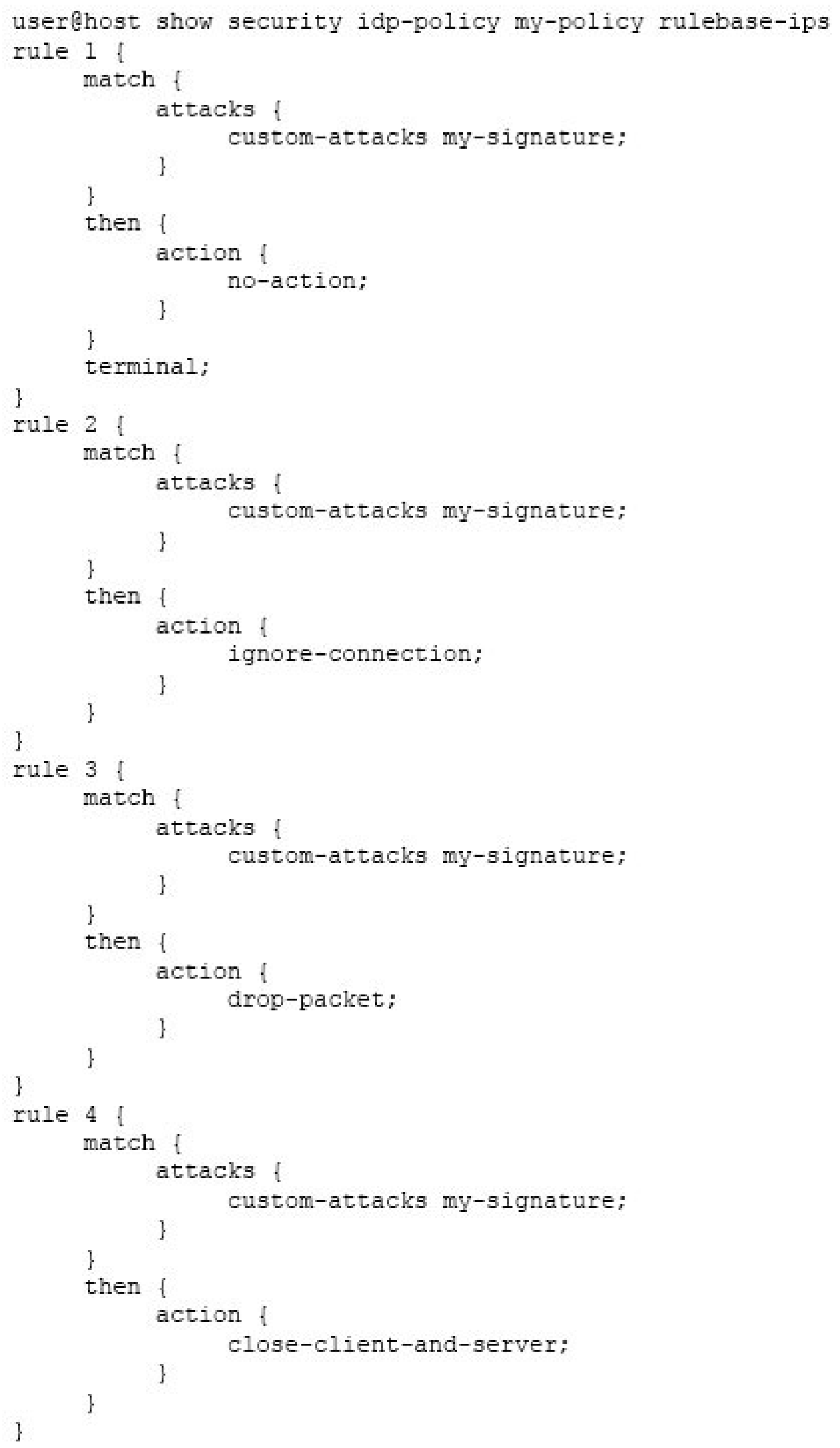
```
user@host > show services user-identification authentication-table
authentication-source active-directory
Domain: example
Total enteries: 1
Source IP      Username       groups(Ref by policy)          state
192.168.50.8   user1          grp1                           Initial
```

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 36
Click the Exhibit button.



```
user@host show security idp-policy my-policy rulebase-ips
rule 1 {
     match {
          attacks {
               custom-attacks my-signature;
          }
     }
     then {
          action {
               no-action;
          }
     }
     terminal;
}
rule 2 {
     match {
          attacks {
               custom-attacks my-signature;
          }
     }
     then {
          action {
               ignore-connection;
          }
     }
}
rule 3 {
     match {
          attacks {
               custom-attacks my-signature;
          }
     }
     then {
          action {
               drop-packet;
          }
     }
}
rule 4 {
     match {
          attacks {
               custom-attacks my-signature;
          }
     }
     then {
          action {
               close-client-and-server;
          }
     }
}
```

You have recently committed the IPS policy shown in the exhibit. When evaluating the expected behavior, you notice that you have a session that matches all of the rules in your IPS policy.
In this scenario, which action would be taken?

A. ignore-connection
B. drop packet
C. no-action
D. close-client-and-server

Answer: C

NEW QUESTION 38
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 40
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 43

What is a function of UTM?

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

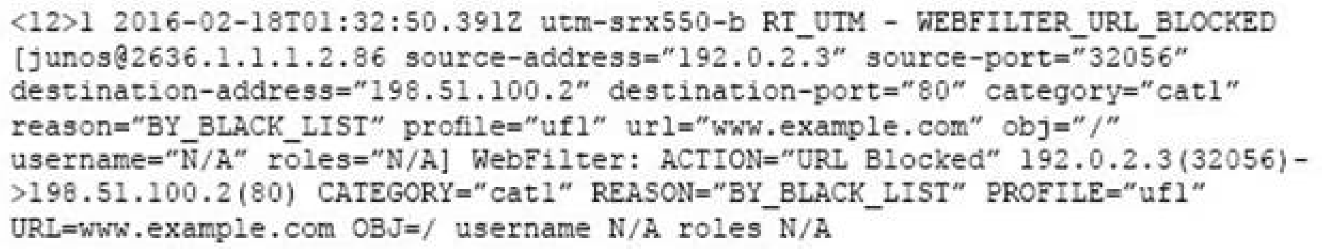
Answer: C

NEW QUESTION 44
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 45
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 46
......

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