JN0-634^{Q&As}

Security, Professional (JNCIP-SEC)

Pass Juniper JN0-634 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.passapply.com/jn0-634.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Juniper Official Exam Center

⚙ **Instant Download** After Purchase

⚙ **100% Money Back** Guarantee

⚙ **365 Days** Free Update

⚙ **800,000+** Satisfied Customers

QUESTION 1

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

Correct Answer: BCD

QUESTION 2

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.

Correct Answer: B

QUESTION 3

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

A. IDP

B. Sky ATP

C. AppQoS

D. AppFW

E. Web filtering

Correct Answer: ACD

QUESTION 4

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.
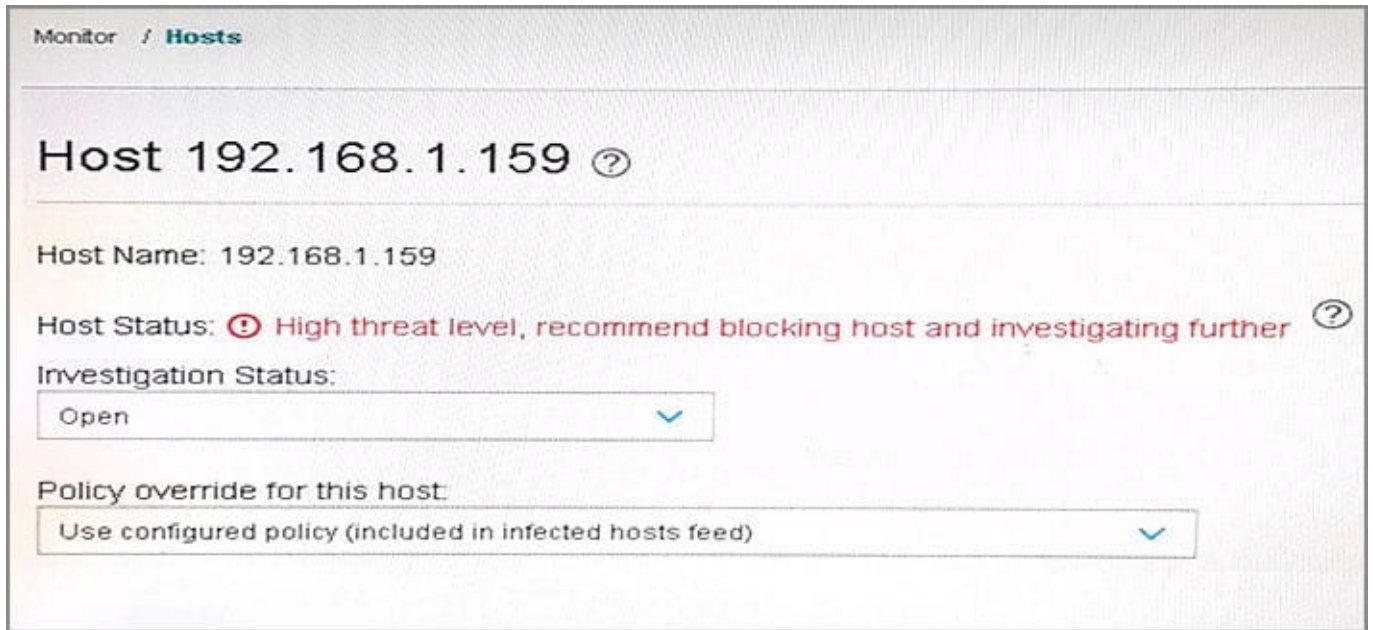
In this scenario, which two commands would you use to meet this requirement? (Choose two.)

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.*

Correct Answer: AC

QUESTION 5

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.

Correct Answer: C

QUESTION 6

Which two statements about enabling MACsec using static CAK security mode keys are true? (Choose two.)

A. CAK secures the data plane traffic.

B. SAK secures the data plane traffic.

C. SAK secures the control plane traffic.

D. CAK secures the control plane traffic.

Correct Answer: BD

QUESTION 7

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.

Correct Answer: D

QUESTION 8

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.

Correct Answer: D

QUESTION 9

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.

Correct Answer: B

QUESTION 10

Click the Exhibit button.

```
[edit security policies global policy int-FW]
user@host# show
match {
      source-address any;
      destination-address any;
      application any;
}
then {
      permit;
}

user@host> show security user-identification local-authentication-table all

user@host>
```

You have configured integrated user firewall on the SRX Series devices in your network. However, you noticed that no users can access the servers that are behind the SRX Series devices.

Referring to the exhibit, what is the problem?

A. The Kerberos service is not configured correctly on the Active Directory server.

B. There are no authentication entries in the SRX Series device for the users.

C. The security policy on the SRX Series device is configured incorrectly.

D. The SAML service is not configured correctly on the Active Directory server.

Correct Answer: C

QUESTION 11

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.

Correct Answer: C

QUESTION 12

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.

Correct Answer: AB

QUESTION 13

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

Correct Answer: C

QUESTION 14

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

Correct Answer: C

QUESTION 15

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.

Correct Answer: A