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.leads4pass.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

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 2

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 3

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

A. RADIUS

B. AppQoS

C. IPS

D. PIM

Correct Answer: C

QUESTION 4

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.

Correct Answer: B

QUESTION 5

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

Correct Answer: A

QUESTION 6

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.

Correct Answer: AC

QUESTION 7

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.

Correct Answer: CD

QUESTION 8

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 9

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.

Correct Answer: A

QUESTION 10

The Software-Defined Secure Networks Policy Enforcer contains which two components? (Choose two.)

A. SRX Series device

B. Sky ATP

C. Policy Controller

D. Feed Connector

Correct Answer: CD

QUESTION 11

Which AppSecure feature identifies applications that are present in traffic?

A. AppID

B. AppTrack

C. AppFW

D. AppQoS

Correct Answer: A

QUESTION 12

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.

Correct Answer: AB

QUESTION 13

What is a function of UTM?

A. AppFW

B. IPsec

C. content filtering

D. bridge mode

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

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

Correct Answer: D

Latest JN0-634 Dumps   JN0-634 VCE Dumps   JN0-634 Study Guide