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

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

Correct Answer: A

QUESTION 2

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 3

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 4

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 5

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;
        ge-0/0/2.0;
    }
}
security-zone untrust {
    screen untrust-screen;
    host-inbound-traffic {
        system-services {
            dhcp;
            ping;
            ssh;
            ike;
        }
    }
    interfaces {
        ge-0/0/0.0;
    }
}
security-zone protected {
    host-inbound-traffic {
        system-services {
            dhcp;
            ping;
            ssh;
            ike;
        }
    }
    interfaces {
        ge-0/0/3.0;
    }
}

user@host# show vlans
v10 {
    vlan-id 10;
}
```

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.

Correct Answer: B