KillTest

Higher Quality, Better Service!

Q&A

http://www.killtest.com

We offer free update service for one year.

Exam : **JN0-635**

Title : Security, Professional (JNCIP-SEC)

Version : DEMO

1.Click the Exhibit button.

```
user@srx> show security mka statistics

     Interface name: fxp1
     Received packets:                          3
     Transmitted packets:                       3
     Version mismatch packets:                  0
     CAK mismatch packets:                      6
     ICV mismatch packets:                      0
     Duplicate message identifier packets:      0
     Duplicate message number packets:          0
     Duplicate address packets:                 0
     Invalid destination address packets:       0
     Formatting error packets:                  0
     Old Replayed message number packets        0
```

While configuring the SRX345, you review the MACsec connection between devices and note that it is not working.

Referring to the exhibit, which action would you use to identify problem?

A. Verify that the formatting settings are correct between the devices and that the software supports the version of MACsec in use

B. Verify that the connectivity association key and the connectivity association key name match on both devices

C. Verify that the transmission path is not replicating packets or correcting frame check sequence error packets

D. Verify that the interface between the two devices is up and not experiencing errors

Answer: B

Explanation:

Reference:

https://www.juniper.net/documentation/en_US/junos/topics/reference/command-summary/show-security-mka-statistics.html

2.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;
            }
      }
}
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 the rules in your IPS policy.
In this scenario, which action would be taken?
A. drop packet
B. no-action
C. close-client-and-server
D. ignore-connection
Answer: B
Explanation:
Reference:
https://www.juniper.net/documentation/en_US/junos/topics/topic-map/security-idp-policy-rules-and-rulebases.html

3.Your organization has multiple Active Directory domains to control user access. You must ensure that security policies are passing traffic based upon the users' access rights.
What would you use to assist your SRX Series devices to accomplish this task?
A. JATP Appliance
B. JIMS
C. JSA
D. Junos Space
Answer: B
Explanation:
Reference: https://www.juniper.net/documentation/en_US/junos/topics/topic-map/security-user-auth-intergrated-user-firewall-overview.html

4.You are asked to set up notifications if one of your collector traffic feeds drops below 100 kbps.
Which two configuration parameters must be set to accomplish this task? (Choose two.)
A. Set a traffic SNMP trap on the JATP appliance
B. Set a logging notification on the JATP appliance
C. Set a general triggered notification on the JATP appliance
D. Set a traffic system alert on the JATP appliance
Answer: BD

5.You have configured static NAT for a webserver in your DMZ. Both internal and external users can reach the webserver using the webserver's IP address. However, only internal users can reach the webserver using the webserver's DNS name. When external users attempt to reach the webserver using the webserver's DNS name, an error message is received.
Which action would solve this problem?
A. Disable Web filtering
B. Use DNS doctoring
C. Modify the security policy
D. Use destination NAT instead of static NAT
Answer: B
Explanation:

Reference: https://www.juniper.net/documentation/en_US/junos/topics/topic-map/security-dns-algs.html