Free Questions for JN0-335 by dumpssheet

Shared by Rutledge on 29-01-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

You administer a JSA host and want to include a rule that sets a threshold for excessive firewall denies and sends an SNMP trap after receiving related syslog messages from an SRX Series firewall.

Which JSA rule type satisfies this requirement?

Options:

A- common

B- offense

C- flow

D- event

Answer:

D

Explanation:

To include a rule that sets a threshold for excessive firewall denies and sends an SNMP trap after receiving related syslog messages from an SRX Series firewall, you need to use an event rule type in JSA. An event rule type allows you to create custom rules based on the events that are collected and normalized by JSA from various sources, such as firewalls, routers, switches, servers, and so on. You can define the conditions, tests, and actions for an event rule, such as matching a specific event name, setting a threshold for the number of occurrences, and sending an SNMP trap to a specified host.Reference:=Creating a Custom Rule,Customizing the SNMP Trap Output

Question 2

Question Type: MultipleChoice

You want to control when cluster failovers occur.

In this scenario, which two specific parameters would you configure on an SRX Series device? (Choose two.)

Options:

A- hearcbeac-interval

B- heartbeac-address

C- hearcbeat-cos

D- hearcbeac-chreshold

Answer:

A, D

Explanation:

To control when cluster failovers occur, you need to configure two specific parameters on an SRX Series device: heartbeat-interval and heartbeat-threshold. These parameters determine how often the nodes in a cluster exchange heartbeat messages and how many consecutive heartbeats can be missed before a failover is triggered. The heartbeat-interval specifies the time interval in seconds between each heartbeat message. The default value is 1 second and the range is from 0.1 to 10 seconds. The heartbeat-threshold specifies the number of consecutive heartbeats that must be missed before a failover occurs. The default value is 3 and the range is from 2 to 255.Reference:=Configuring Chassis Clustering on SRX Series Devices,Chassis Cluster Redundancy Group Failover

Question 3

Question Type: MultipleChoice

Click the Exhibit button.

```
[edit services]
user@srx# show
security-intelligence {
    profile ATP_Infected-Hosts {
        category Infected-Hosts;
        rule Rule-1 {
            match {
                threat-level 8;
            }
            then {
                action {
                    block {
                        drop;
                    }
                }
            }
        }
    }
}
```

Referring to the exhibit, what will the SRX Series device do in this configuration?

Options:

A- Packets from the infected hosts with a threat level of 8 will be dropped and a log message will be generated.

B- Packets from the infected hosts with a threat level of 8 or above will be dropped and a log message will be generated.

C- Packets from the infected hosts with a threat level of 8 or above will be dropped and no log message will be generated.

D- Packets from the infected hosts with a threat level of 8 will be dropped and no log message will be generated.

Answer:

C

Explanation:

The exhibit shows a configuration snippet for security intelligence on an SRX Series device. Security intelligence is a feature that allows you to block or monitor traffic from malicious sources based on threat intelligence feeds from Juniper ATP Cloud or other providers. The configuration defines a profile for ATP Infected-Hosts, which is a feed that contains IP addresses of hosts that are infected with malware and communicate with command-and-control servers. The configuration also defines a rule for threat level 8, which is a parameter that indicates the severity of the threat. Based on this configuration, the SRX Series device will do the following:

Packets from the infected hosts with a threat level of 8 or above will be dropped: The action block-and-drop under the rule means that the device will block any traffic from the infected hosts that have a threat level equal to or higher than 8. This will prevent the hosts from sending or receiving malicious commands or data.

No log message will be generated: The absence of any log option under the rule means that the device will not generate any log message for the blocked traffic. This may reduce the load on the device and the logging server, but it may also limit the visibility and

analysis of the security events.

Question 4

Question Type: MultipleChoice

How does Juniper ATP Cloud protect a network from zero-day threats?

Options:

A- It uses a cache lookup.

B- It uses antivirus software.

C- It uses dynamic analysis.

D- It uses known virus signatures.

Answer:

C

Explanation:

Juniper ATP Cloud is a cloud-based service that provides advanced threat prevention and detection for your network. It integrates with SRX Series firewalls and MX Series routers to analyze files and network traffic for signs of malicious activity. Juniper ATP Cloud protects a network from zero-day threats by using dynamic analysis, which is a method of executing files in a sandbox environment and observing their behavior and network interactions. Dynamic analysis can uncover unknown malware that may evade static analysis or signature-based detection methods.

Question 5

Question Type: MultipleChoice

What are two requirements for enabling AppQoE? (Choose two.)

Options:

A- You need two SRX Series device endpoints.

B- You need two SRX Series or MX Series device endpoints.

C- You need an APPID feature license.

D- You need to configure AppQoE for reverse traffic.

Answer:

B, C

Explanation:

AppQoE is a feature that enables you to monitor and optimize the quality of experience for applications on your network. It uses application-aware routing and dynamic path selection to choose the best path for each application based on predefined or custom SLA profiles. AppQoE also provides visibility and reporting on application performance and network conditions. Two requirements for enabling AppQoE are:

You need two SRX Series or MX Series device endpoints: AppQoE can be configured between two SRX Series device endpoints or between an SRX Series device and an MX Series device in a hub-and-spoke or full mesh topology. The devices must run the same version of Junos OS and have the same AppQoE configuration.

You need an APPID feature license: AppQoE requires an APPID feature license to be installed on the SRX Series device. The APPID feature license enables application identification and classification, which are essential for AppQoE to work.

Question 6

Question Type: MultipleChoice

Click the Exhibit button.

```
user@srx> show chassis cluster status redundancy-group 1

Cluster: 1, Redundancy-Group: 1
    Device name              Priority    Status    Preempt
 Manual failover
    node0                    0           Secondary No       No
    node1                    200         Primary   No       No
```

Which two statements describe the output shown in the exhibit? (Choose two.)

Options:

A- Redundancy group 1 experienced an operational failure.

B- Redundancy group 1 was administratively failed over.

C- Node 0 is controlling traffic for redundancy group 1.

D- Node 1 is controlling traffic for redundancy group 1.

Answer:

B, D

Explanation:

The output shown in the exhibit displays the status of a chassis cluster redundancy group (RG) on an SRX Series device. A chassis cluster RG is a collection of objects, such as interfaces or services, that fail over together from one node to another in case of a failure or manual intervention. A chassis cluster RG can be primary on one node and backup on another node at any given time. Two statements that describe the output shown in the exhibit are:

Redundancy group 1 was administratively failed over: The output shows that redundancy group 1 has "Manual failover" set to "Yes". This indicates that redundancy group 1 was manually switched from one node to another using the request chassis cluster failover redundancy-group command.

Node 1 is controlling traffic for redundancy group 1: The output shows that node 1 has "Status" set to "Primary" for redundancy group 1. This means that node 1 is active and controlling traffic for redundancy group 1.

Question 7

Question Type: MultipleChoice

Click the Exhibit button.

```
user@host> show configuration policy-options
     prefix-list manager-ip {
     10.0.0.0/8;
     192.168.4.254/32;
}
user@host> show configuration firewall
     filter manager-ip {
     term block_non_manager {
          from      {
               source-address {
                    0.0.0.0/0;
               }
               source-prefix-list {
               manager-ip except;
               }
               protocol tcp;
               destination-port [ ssh https telnet http ];
     }
     then {
          discard;
     }
}
     term accept_everything_else {
          then accept;
     }
}
user@host> show configuration interfaces lo0
unit 0 {
```

You are validating the configuration template for device access. The commands in the exhibit have been entered to secure IP access to an SRX Series device.

Referring to the exhibit, which two statements are true? (Choose two.)

Options:

A- The device manager can access the device from 192.168.11.248.

B- The loopback interface blocks invalid traffic on its entry into the device.

C- The loopback interface blocks invalid traffic on its exit from the device.

D- The device manager can access the device from 10.253.1.2.

Answer:

B, D

Explanation:

The commands in the exhibit show how to configure a firewall filter on the loopback interface (lo0) of an SRX Series device. The loopback interface is a gateway for all the control traffic that enters the Routing Engine of the device. The firewall filter can be used to monitor and protect this control traffic from various attacks. Two statements that are true based on the exhibit are:

The loopback interface blocks invalid traffic on its entry into the device: The firewall filter applied on lo0 has a term that matches any packet with an invalid source address (such as 0.0.0.0/8 or 127.0.0.0/8) and discards it. This prevents spoofing or DoS attacks using invalid source addresses.

The device manager can access the device from 10.253.1.2: The firewall filter applied on lo0 has a term that matches any packet with a source address of 10.253.1.2 and accepts it. This allows the device manager to access the device from this IP address using protocols such as SSH, Telnet, HTTP, or HTTPS.

Question 8

Question Type: MultipleChoice

On an SRX Series firewall, what are two ways that Encrypted Traffic Insights assess the threat of the traffic? (Choose two.)

Options:

A- It decrypts the file in a sandbox.

B- It validates the certificates used.

C- It decrypts the data to validate the hash.

D- It reviews the timing and frequency of the connections.

Answer:

B, D

Explanation:

Encrypted Traffic Insights is a feature that enables the SRX Series firewall and the ATP Cloud to detect malicious threats that are hidden in encrypted traffic without decrypting the traffic. It does so by analyzing the metadata and connection patterns of the encrypted sessions. Two ways that Encrypted Traffic Insights assess the threat of the traffic are:

It validates the certificates used: The SRX Series firewall extracts the server certificate from the encrypted session and compares its signature with a blocklist of known malicious certificates provided by ATP Cloud. If there is a match, the session is blocked and reported as a threat.

It reviews the timing and frequency of the connections: The SRX Series firewall sends the connection details, such as source and destination IP addresses, ports, protocols, and timestamps, to ATP Cloud. ATP Cloud applies behavior analysis and machine learning algorithms to detect anomalous or suspicious patterns of connections, such as high frequency, low duration, or unusual timing.

Question 9

Question Type: MultipleChoice

When a security policy is modified, which statement is correct about the default behavior for active sessions allowed by that policy?

Options:

A- The active sessions allowed by the policy will be dropped.

B- Only policy changes that involve modification of the action field will cause the active sessions affected by the change to be dropped.

C- Only policy changes that involve modification of the application will cause the active sessions affected by the change to be dropped.

D- The active sessions allowed by the policy will continue unchanged.

Answer:

D

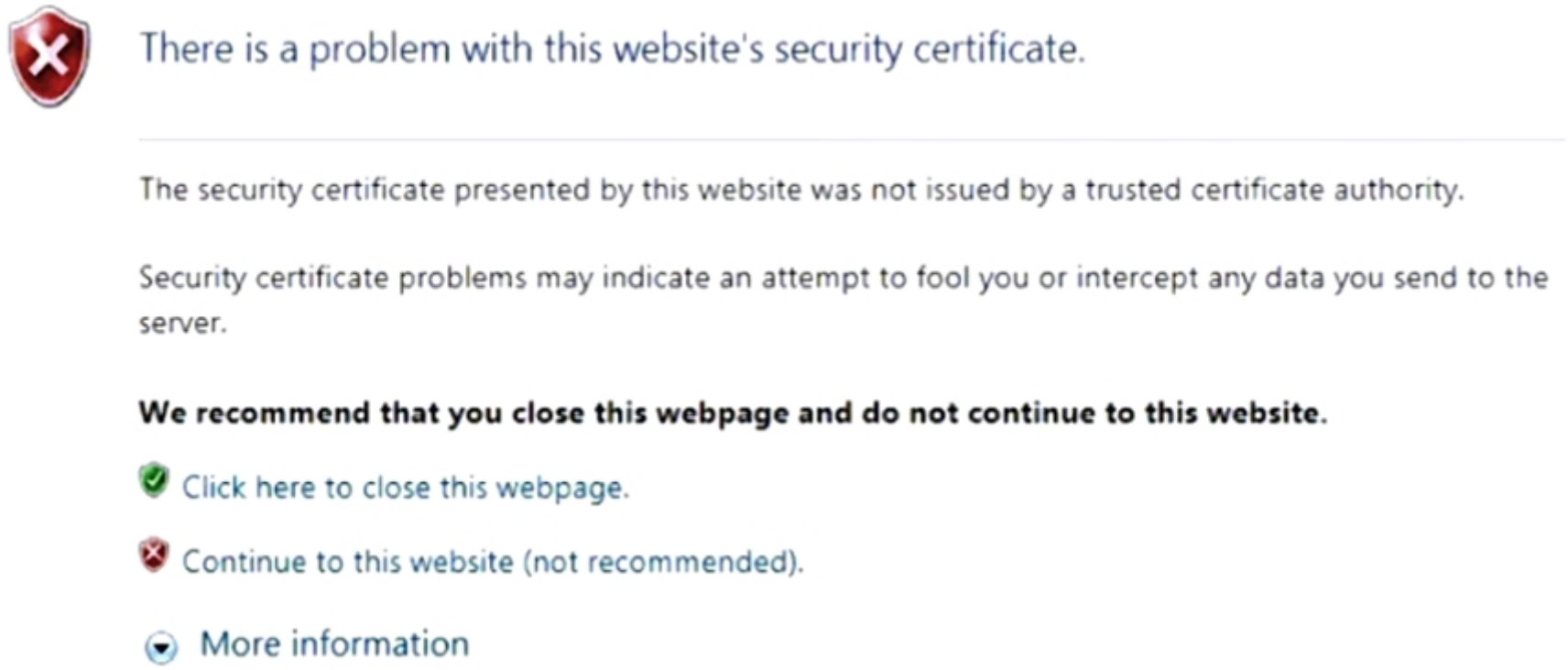
Explanation:

When you modify a security policy on the SRX Series device, the default behavior is that the existing sessions that match the policy will continue unchanged. This means that the policy modification will only affect new sessions that are initiated after the change. However, you can change this behavior by using the clear-policy-session command, which will clear all the sessions that match the modified policy and force them to re-evaluate the new policy.Reference:=JNCIS-SEC Certification,Open Learning - Security, Specialist (JNCIS-SEC),Security Policies (Advanced)

Question 10

Question Type: MultipleChoice

Click the Exhibit button.



You have implemented SSL client protection proxy. Employees are receiving the error shown in the exhibit.

How do you solve this problem?

Options:

A- Load a known good, but expired. CA certificate onto the SRX Series device.

B- Install a new SRX Series device to act as the client proxy

C- Reboot the SRX Series device.

D- Import the existing certificate to each client device.

Answer:

D

Explanation:

SSL client protection proxy is a feature that allows you to decrypt and inspect the SSL traffic from clients to servers. To do this, you need to install a certificate authority (CA) certificate on the SRX Series device and import the same certificate to each client device. This way, the SRX Series device can act as a proxy between the client and the server and perform security checks on the decrypted traffic. If the client device does not have the certificate installed, it will receive an error message like the one shown in the exhibit.Reference:=JNCIS-SEC Certification,Open Learning - Security, Specialist (JNCIS-SEC),SSL Proxy Configuration

Question 11

Question Type: MultipleChoice

Which two statements are correct about AppTrack? (Choose two.)

Options:

A- AppTrack can be configured for any defined logical system on an SRX Series device.

B- AppTrack identifies and blocks traffic flows that might be malicious regardless of the ports being used.

C- AppTrack collects traffic flow information including byte, packet, and duration statistics.

D- AppTrack can only be configured in the main logical system on an SRX Series device.

Answer:

A, C

Explanation:

AppTrack is a feature that allows you to monitor and analyze the application traffic on your SRX Series device. It can be configured for any defined logical system, which is a virtual router or switch within a physical device. AppTrack collects statistics such as bytes, packets, and duration for each application flow and displays them in reports or logs. AppTrack does not identify or block malicious traffic, that is the function of AppSecure or IDP/IPS.Reference:=JNCIS-SEC Certification,Open Learning - Security, Specialist (JNCIS-SEC),Application Security Theory