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.pass4itsure.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

Your network includes SRX Series devices at all headquarter, data center, and branch locations. The headquarter and data center locations use high-end SRX Series devices, and the branch locations use branch SRX Series devices. You are asked to deploy IPS on the SRX Series devices using one of the available IPS deployment modes.

In this scenario, which two statements are true? (Choose two.)

A. Inline tap mode provides enforcement.

B. Inline tap mode can be used at all locations.

C. Integrated mode can be used at all locations.

D. Integrated mode provides enforcement.

Correct Answer: CD

QUESTION 2

Click the Exhibit button.

```
[edit security utm]
user@host# show
feature-profile {
    content-filtering {
        profile web-traffic-profile {
            block-content-type {
                zip;
            }
        }
    }
}
utm-policy utm-web-policy {
    content-filtering {
        http-profile web-traffic-profile;
    }
}
```

The UTM policy shown in the exhibit has been applied to a security policy on a branch SRX Series device. In this scenario, which statement is true?

A. HTTP downloads of ZIP files will be blocked.

B. FTP downloads of ZIP files will be blocked.

C. E-mail downloads of ZIP files will be blocked.

D. ZIP files can be renamed with a new extension to pass through the filter.

Correct Answer: A

QUESTION 3

You are using the integrated user firewall feature on an SRX Series device.

Which three parameters are stored in the Active Directory authentication table? (Choose three.)

A. IP address

B. MAC address

C. group mapping

D. username

E. password

Correct Answer: ACD

QUESTION 4

Click the Exhibit button.

```
user@host# show security idp
idp-policy base-policy {
        rulebase-ips {
                rule R1 {
                        match {
                                from-zone trust;
                                source-address any;
                                to-zone untrust;
                                destination-address any;
                                application default;
                                attacks {
                                        predefined-attack-groups HTTP-Critical;
                                }
                        }
                        then {
                        action {
                                mark-diffserv {
                                        10;
                                }
                        }
                }
        }
    }
}
```

Referring to the security policy shown in the exhibit, which two actions will happen as the packet is processed? (Choose two.)

A. It passes unmatched traffic after modifying the DSCP priority.

B. It marks and passes matched traffic with a high DSCP priority.

C. It marks and passes matched traffic with a low DSCP priority.

D. It passes unmatched traffic without modifying DSCP priority.

Correct Answer: BD

QUESTION 5

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 6

What is the required when deploying a log collector in Junos Space?

A. root user access to the log collector

B. a shared log file directory on the log collector

C. the IP address of interface eth1 on the log collector

D. a distributed deployment of the log collector nodes

Correct Answer: A

QUESTION 7

You are using IDP on your SRX Series device and are asked to ensure that the SRX Series device has the latest IDP database, as well as the latest application signature database.

In this scenario, which statement is true?

A. The application signature database cannot be updated on a device with the IDP database installed.

B. You must download each database separately.

C. The IDP database includes the latest application signature database.

D. You must download the application signature database before installing the IDP database.

Correct Answer: C

QUESTION 8

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 9

What is a function of UTM?

A. AppFW

B. IPsec

C. content filtering

D. bridge mode

Correct Answer: C

QUESTION 10

Click the Exhibit button.

Security Director is reporting the events shown in the exhibit.

If the fallback parameter is set to pass traffic, what would cause the events?

A. The files are too large for the antivirus engine to process.

B. The files are not scanned because they were permitted by a security policy.

C. The files are not scanned because they are the wrong file format.

D. The antivirus engine is unable to re-encrypt the files.

Correct Answer: A

QUESTION 11

SRX Series devices with AppSecure support which three custom signatures? (Choose three.)

A. MAC address-based mapping

B. latency detection mapping

C. IP protocol-based mapping

D. ICMP-based mapping

E. Layer 7-based signatures

Correct Answer: CDE

QUESTION 12

Your network includes SRX Series devices at the headquarters location. The SRX Series devices at this location are part of a high available chassis cluster and are configured for IPS. There has been a node failover.

In this scenario, which two statements are true? (Choose two.)

A. The IP action table is synchronized between the chassis cluster nodes.

B. Cached SSL session ID information for existing sessions is not synchronized between nodes.

C. The IP action table is not synchronized between the chassis cluster nodes.

D. Cached SSL session ID information for existing session is synchronized between nodes.

Correct Answer: CD

QUESTION 13

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 14

You are creating an IPS policy with multiple rules. You want traffic that matches rule 5 to silently be dropped, along with any future packets that match the appropriate attributes of the incoming traffic.

In this scenario, which ip-action parameter should you use?

A. ip-block

B. ip-close

C. log-create

D. timeout

Correct Answer: A

QUESTION 15

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

JN0-634 Study Guide   JN0-634 Exam Questions   JN0-634 Braindumps