JN0-636 Q&As

Service Provider Routing and Switching Professional (JNCIP-SP)

Pass Juniper JN0-636 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

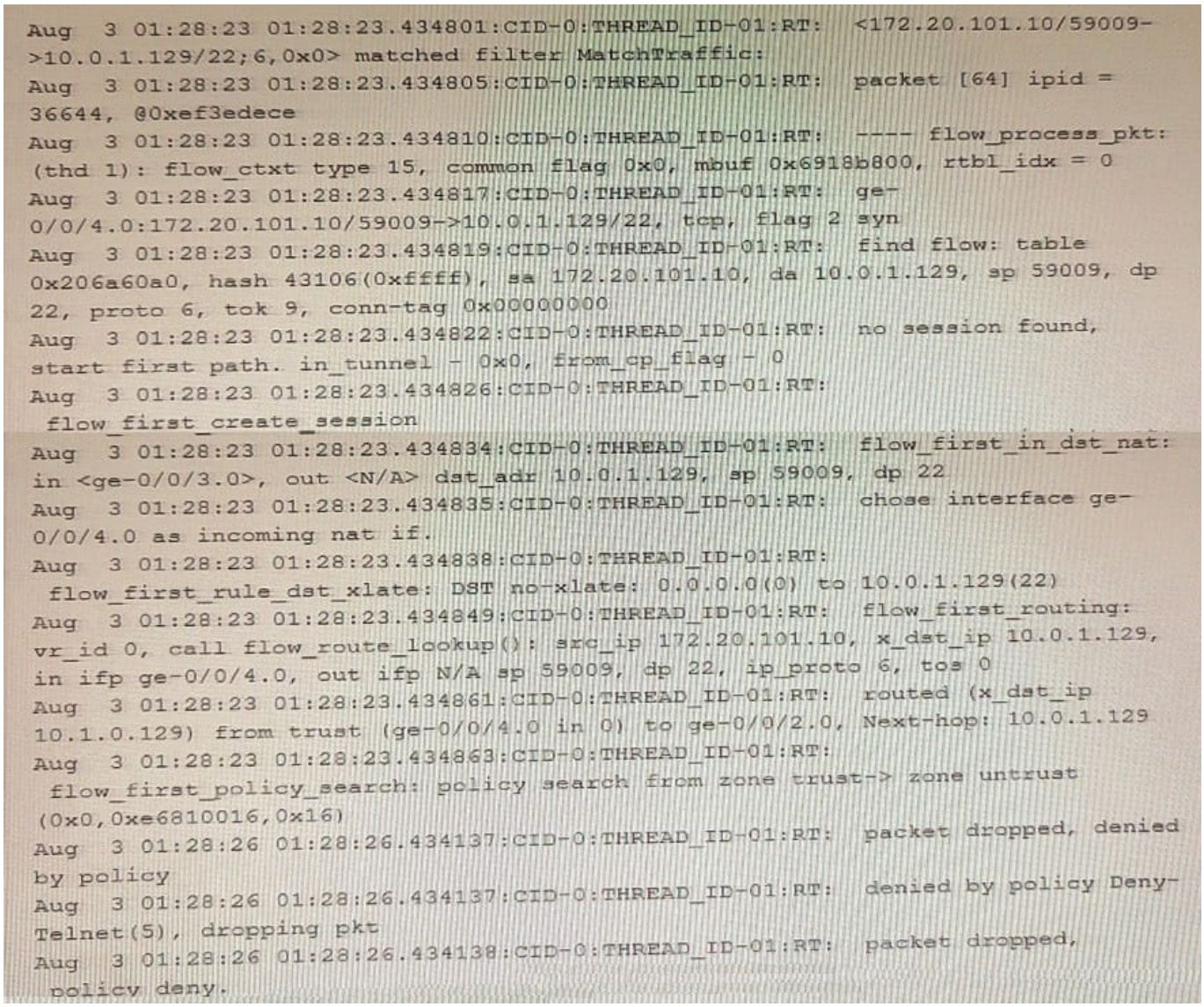
https://www.pass4itsure.com/jn0-636.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Juniper Official Exam Center

QUESTION 1

Exhibit



Referring to the exhibit, which statement is true?

A. This custom block list feed will be used before the Juniper SecIntel

B. This custom block list feed cannot be saved if the Juniper SecIntel block list feed is configured.

C. This custom block list feed will be used instead of the Juniper SecIntel block list feed

D. This custom block list feed will be used after the Juniper SecIntel block list feed.

Correct Answer: D

QUESTION 2

You want to identify potential threats within SSL-encrypted sessions without requiring SSL proxy to decrypt the session contents. Which security feature achieves this objective?

A. infected host feeds

B. encrypted traffic insights

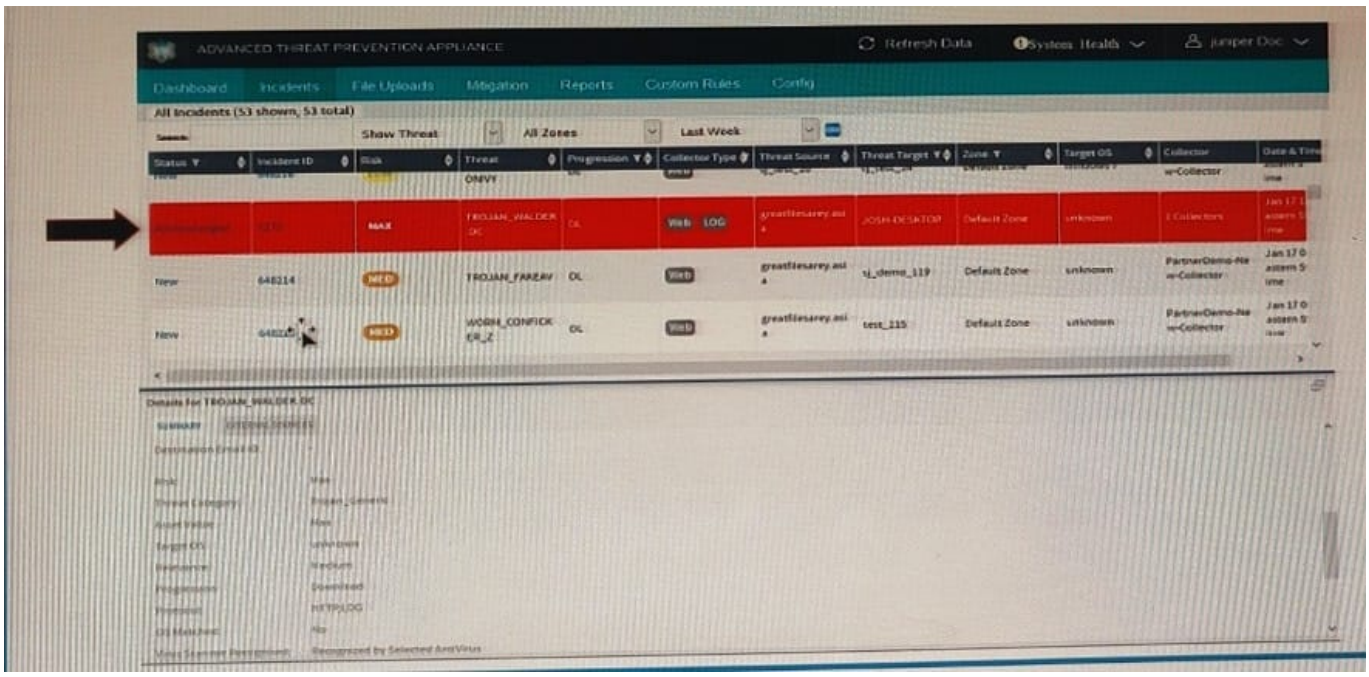
C. DNS security

D. Secure Web Proxy

Correct Answer: C

QUESTION 3

Exhibit



The highlighted incident (arrow) shown in the exhibit shows a progression level of "Download" in the kill chain. What are two appropriate mitigation actions for the selected incident? (Choose two.)

A. Immediate response required: Block malware IP addresses (download server or CnC server)

B. Immediate response required: Wipe infected endpoint hosts.

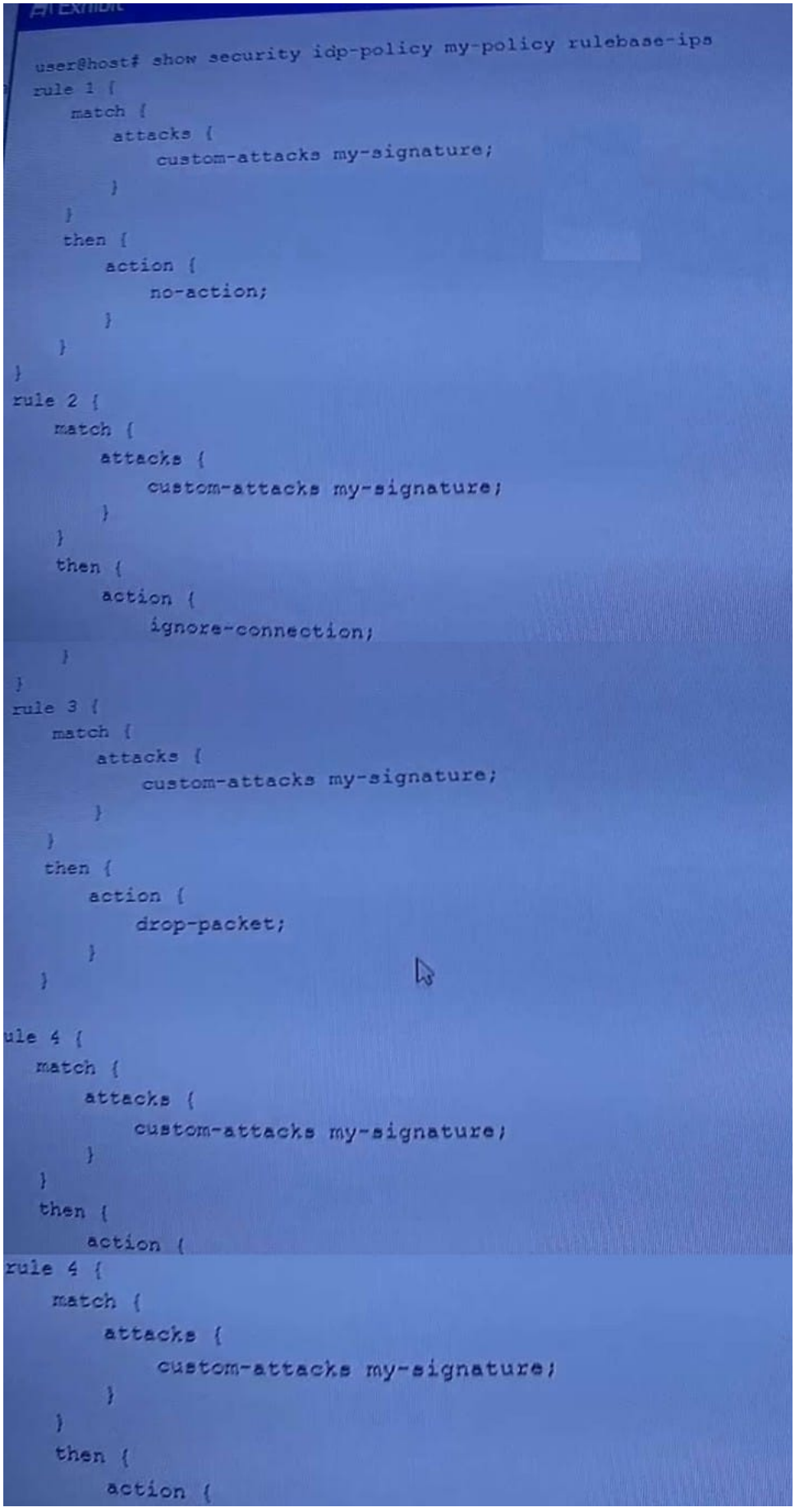
C. Immediate response required: Deploy IVP integration (if configured) to confirm if the endpoint has executed the malware and is infected.

D. Not an urgent action: Use IVP to confirm if machine is infected.

Correct Answer: BD

QUESTION 4

Exhibit.



```
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;
        }
    }

ule 4 {
    match {
        attacks {
            custom-attacks my-signature;
        }
    }
    then {
        action {
rule 4 {
    match {
        attacks {
            custom-attacks my-signature;
        }
    }
    then {
        action {
```

A hub member of an ADVPN is not functioning correctly.

Referring the exhibit, which action should you take to solve the problem?

A. [edit interfaces] root@vSRX-1# delete st0.0 multipoint

B. [edit interfaces] user@hub-1# delete ipsec vpn advpn-vpn traffic-selector

C. [edit security] user@hub-1# set ike gateway advpn-gateway advpn suggester disable

D. [edit security] user@hub-1# delete ike gateway advpn-gateway advpn partner

Correct Answer: B

QUESTION 5

What are two valid modes for the Juniper ATP Appliance? (Choose two.)

A. flow collector

B. event collector

C. all-in-one

D. core

Correct Answer: AC

Explanation: The Juniper ATP Appliance supports two valid modes of operation:

Flow Collector: This mode allows the Juniper ATP Appliance to collect and analyze network flow data to detect malicious activity.

All-in-One: This mode allows the Juniper ATP Appliance to perform both flow collection and event collection. It includes all the features of the Flow Collector and Event Collector mode.

Event collector and core are not valid modes for the Juniper ATP Appliance, the first one is focused on collecting events and the second one is a term that\\'s not related to the appliance.