



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

-  **Instant Download** After Purchase
-  **100% Money Back** Guarantee
-  **365 Days** Free Update
-  **800,000+** Satisfied Customers



**QUESTION 1**

Exhibit

```
Aug 3 01:28:23 01:28:23.434801:CID-0:THREAD_ID-01:RT: <172.20.101.10/59009-
>10.0.1.129/22;6,0x0> matched filter MatchTraffic:
Aug 3 01:28:23 01:28:23.434805:CID-0:THREAD_ID-01:RT: packet [64] ipid =
36644, @0xef3edece
Aug 3 01:28:23 01:28:23.434810:CID-0:THREAD_ID-01:RT: ---- flow_process_pkt:
(thd 1): flow_ctxt type 15, common flag 0x0, mbuf 0x6918b800, rtbl_idx = 0
Aug 3 01:28:23 01:28:23.434817:CID-0:THREAD_ID-01:RT: ge-
0/0/4.0:172.20.101.10/59009->10.0.1.129/22, tcp, flag 2 syn
Aug 3 01:28:23 01:28:23.434819:CID-0:THREAD_ID-01:RT: find flow: table
0x206a60a0, hash 43106(0xffff), sa 172.20.101.10, da 10.0.1.129, sp 59009, dp
22, proto 6, tok 9, conn-tag 0x00000000
Aug 3 01:28:23 01:28:23.434822:CID-0:THREAD_ID-01:RT: no session found,
start first path. in_tunnel - 0x0, from_cp_flag - 0
Aug 3 01:28:23 01:28:23.434826:CID-0:THREAD_ID-01:RT:
flow_first_create_session
Aug 3 01:28:23 01:28:23.434834:CID-0:THREAD_ID-01:RT: flow_first_in_dst_nat:
in <ge-0/0/3.0>, out <N/A> dst_adr 10.0.1.129, sp 59009, dp 22
Aug 3 01:28:23 01:28:23.434835:CID-0:THREAD_ID-01:RT: chose interface ge-
0/0/4.0 as incoming nat if.
Aug 3 01:28:23 01:28:23.434838:CID-0:THREAD_ID-01:RT:
flow_first_rule_dst_xlate: DST no-xlate: 0.0.0.0(0) to 10.0.1.129(22)
Aug 3 01:28:23 01:28:23.434849:CID-0:THREAD_ID-01:RT: flow_first_routing:
vr_id 0, call flow_route_lookup(): src_ip 172.20.101.10, x_dst_ip 10.0.1.129,
in ifp ge-0/0/4.0, out ifp N/A sp 59009, dp 22, ip_proto 6, tos 0
Aug 3 01:28:23 01:28:23.434861:CID-0:THREAD_ID-01:RT: routed (x_dst_ip
10.1.0.129) from trust (ge-0/0/4.0 in 0) to ge-0/0/2.0, Next-hop: 10.0.1.129
Aug 3 01:28:23 01:28:23.434863:CID-0:THREAD_ID-01:RT:
flow_first_policy_search: policy search from zone trust-> zone untrust
(0x0,0xe6810016,0x16)
Aug 3 01:28:26 01:28:26.434137:CID-0:THREAD_ID-01:RT: packet dropped, denied
by policy
Aug 3 01:28:26 01:28:26.434137:CID-0:THREAD_ID-01:RT: denied by policy Deny-
Telnet(5), dropping pkt
Aug 3 01:28:26 01:28:26.434138:CID-0:THREAD_ID-01:RT: packet dropped,
policy deny.
```

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

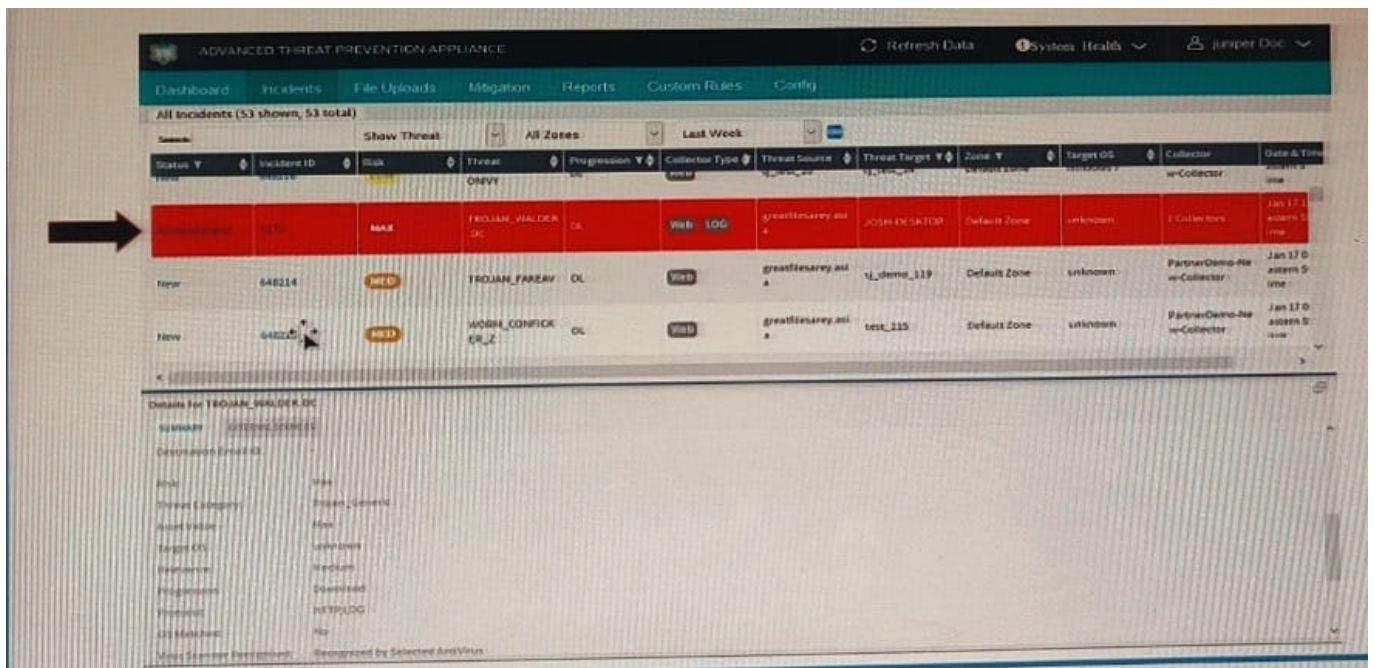
You want to identify potential threats within SSL-encrypted sessions without requiring SSL proxy to decrypt the session contents. Which security feature achieves this objective?

- 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.



```
# 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;
    }
  }
}
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.

[Latest JN0-636 Dumps](#)

[JN0-636 PDF Dumps](#)

[JN0-636 VCE Dumps](#)