DUMPSARENA

Security, Professional (JNCIP-SEC)

Juniper JN0-636

Version Demo

Total Demo Questions: 10

Total Premium Questions: 92

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

QUESTION NO: 1

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

A. flow collector

B. event collector

C. all-in-one

D. core

ANSWER: A C

QUESTION NO: 2

Your company uses non-Juniper firewalls and you are asked to provide a Juniper solution for zero-day malware protection. Which solution would work in this scenario?

A. Juniper ATP Cloud

B. Juniper Secure Analytics

C. Juniper ATP Appliance

D. Juniper Security Director

ANSWER: C

QUESTION NO: 3

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

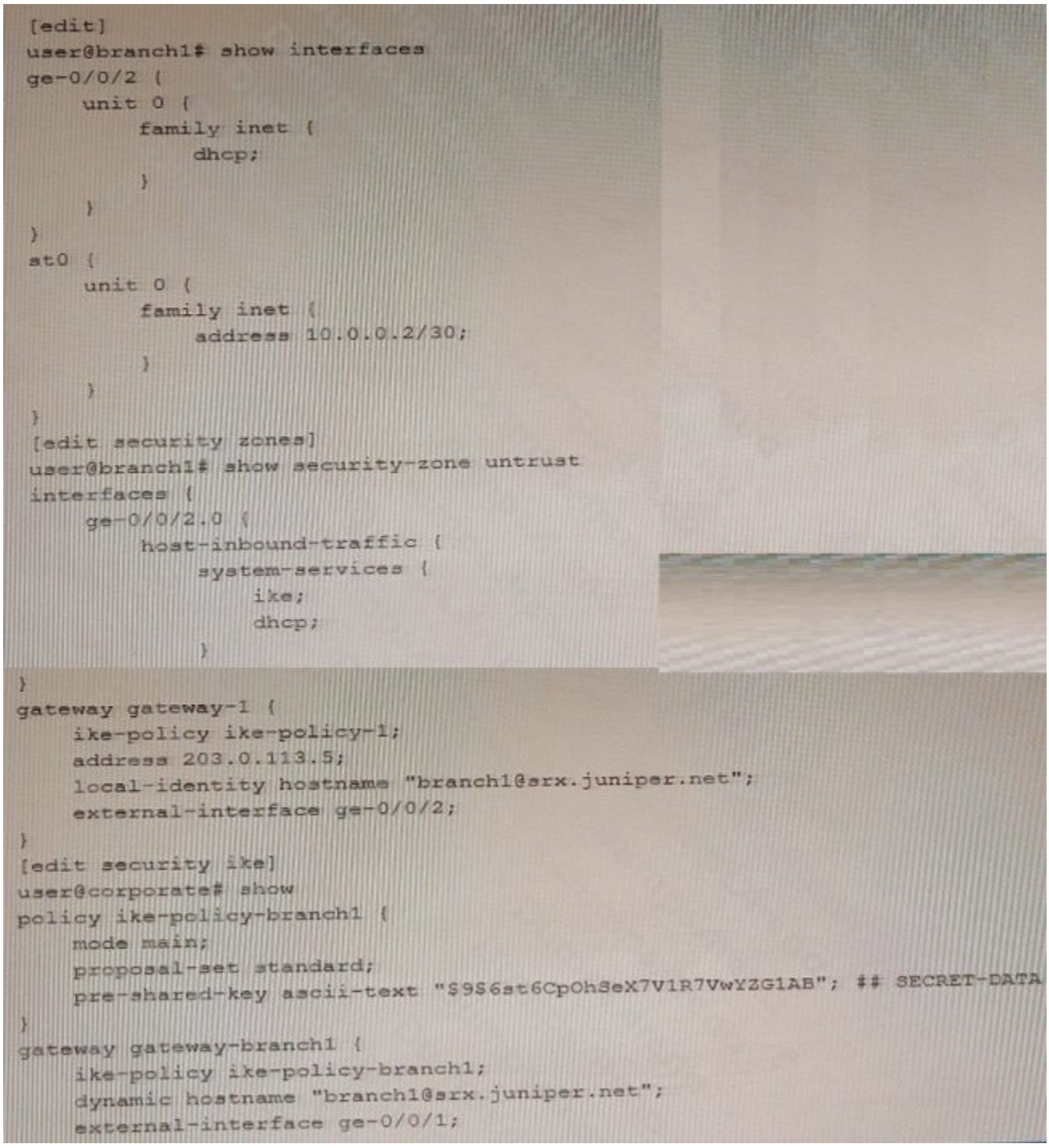
C. DNS security

D. Secure Web Proxy

ANSWER: C

QUESTION NO: 4

Exhibit



You are trying to configure an IPsec tunnel between SRX Series devices in the corporate office and branch1. You have committed the configuration shown in the exhibit, but the IPsec tunnel is not establishing.

In this scenario, what would solve this problem.

A. Add multipoint to the st0.0 interface configuration on the branch1 device.

B. Change the IKE proposal-set to compatible on the branch1 and corporate devices.

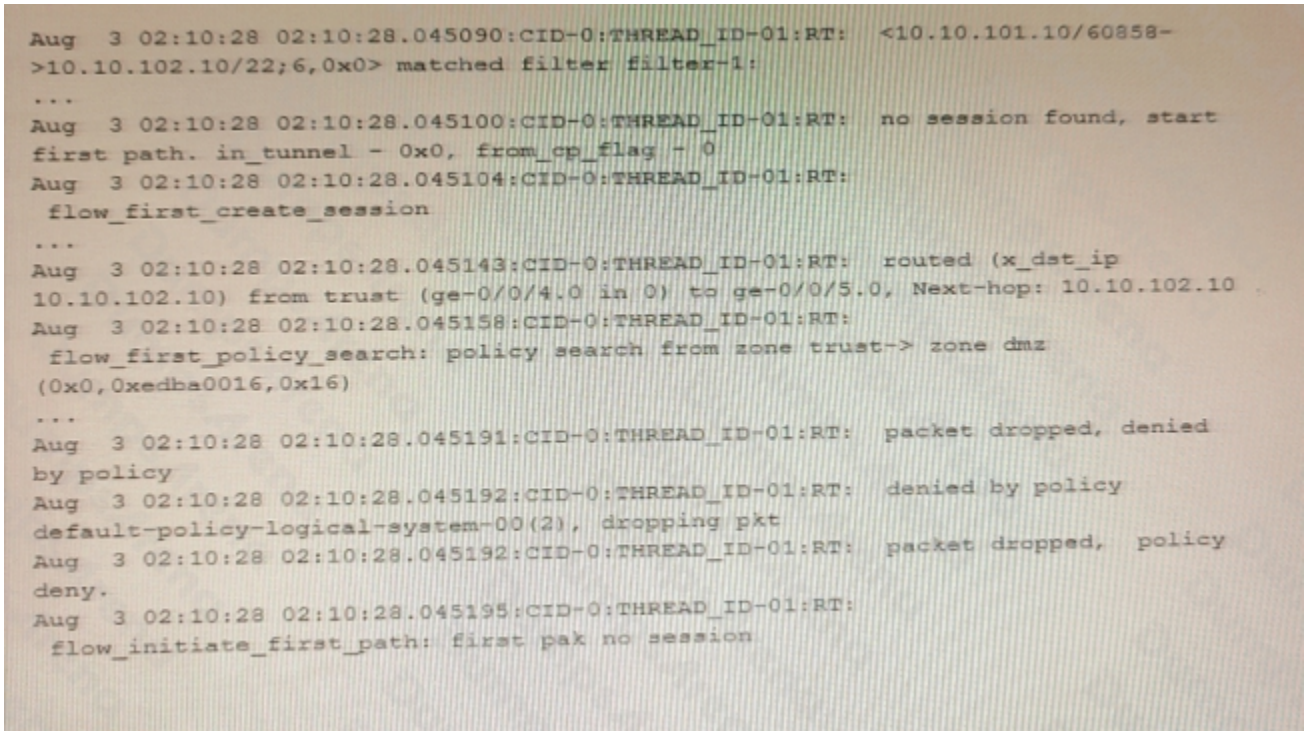
C. Change the local identity to inet advpn on the branch1 device.

D. Change the IKE mode to aggressive on the branch1 and corporate devices.

ANSWER: C

QUESTION NO: 5

Exhibit



Which two statements are correct about the output shown in the exhibit? (Choose two.)

A. The packet is processed as host inbound traffic.

B. The packet matches the default security policy.

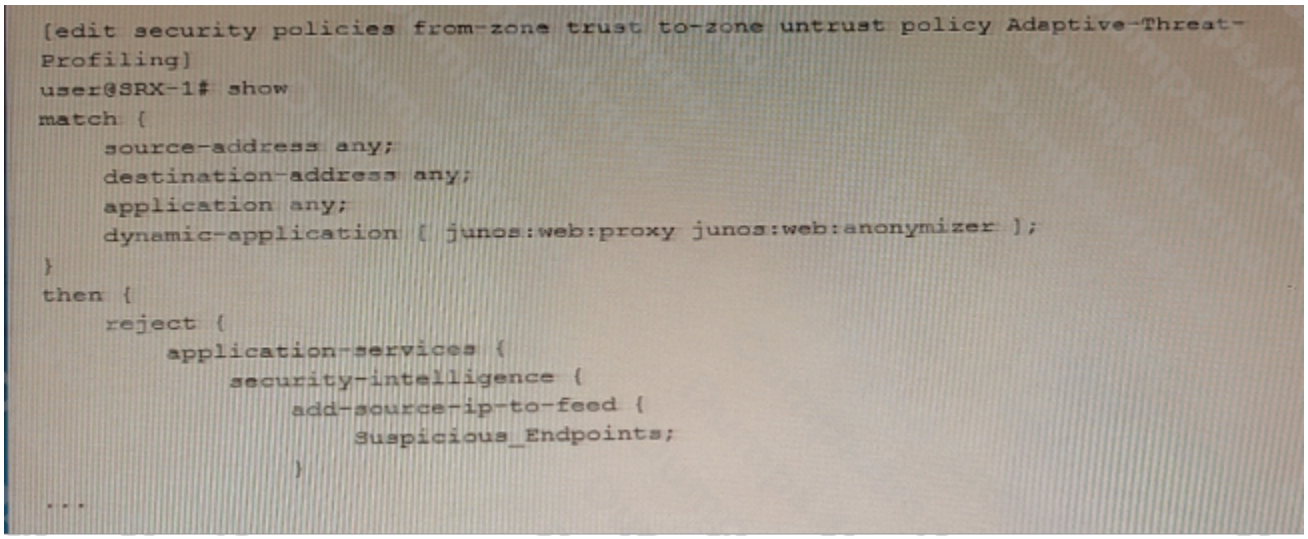
C. The packet matches a configured security policy.

D. The packet is processed in the first path packet flow.

ANSWER: A B

QUESTION NO: 6

Exhibit



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

A. The 3uspicious_Endpoint3 feed is only usable by the SRX-1 device.

B. You must manually create the suspicious_Endpoint3 feed in the Juniper ATP Cloud interface.

C. The 3uspiciou3_Endpoint3 feed is usable by any SRX Series device that is a part of the same realm as SRX-1

D. Juniper ATP Cloud automatically creates the 3uopi'cioua_Endpoints feed after you commit the security policy.

ANSWER: A C

QUESTION NO: 7

You are asked to detect domain generation algorithms

Which two steps will accomplish this goal on an SRX Series firewall? (Choose two.)

A. Define an advanced-anti-malware policy under [edit services].

B. Attach the security-metadata-streaming policy to a security

C. Define a security-metadata-streaming policy under [edit

D. Attach the advanced-anti-malware policy to a security policy.

ANSWER: A D

QUESTION NO: 8

You want to use selective stateless packet-based forwarding based on the source address.

In this scenario, which command will allow traffic to bypass the SRX Series device flow daemon?

A. set firewall family inet filter bypaa3_flowd term t1 then skip—services accept

B. set firewall family inet filter bypass_flowd term t1 then routing-instance stateless

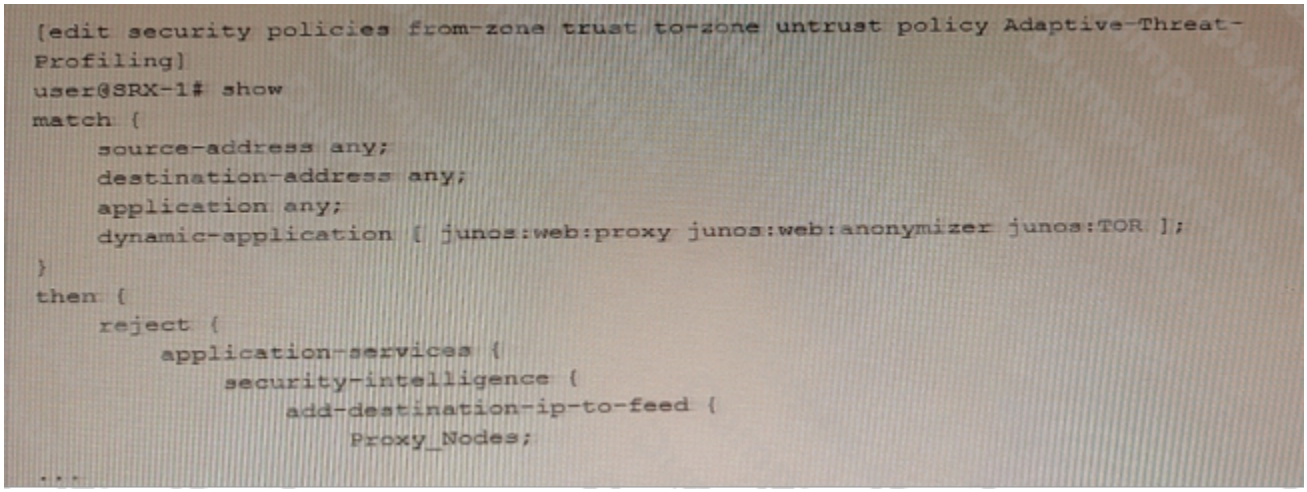
C. set firewall family inet filter bypas3_flowd term t1 then virtual-channel stateless

D. set firewall family inet filter bypass__f lowd term t1 then packet—mode

ANSWER: A

QUESTION NO: 9

Exhibit



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

A. The SRX-1 device can use the Proxy__Nodes feed in another security policy.

B. You can use the Proxy_Nodes feed as the source-address and destination-address match criteria of another security policy on a different SRX Series device.

C. The SRX-1 device creates the Proxy_wodes feed, so it cannot use it in another security policy.

D. You can only use the Proxy_Node3 feed as the destination-address match criteria of another security policy on a different SRX Series device.

ANSWER: A C

QUESTION NO: 10

You issue the command shown in the exhibit.

Which policy will be active for the identified traffic?

A. Policy p4

B. Policy p7

C. Policy p1

D. Policy p12

ANSWER: B