Up-to-date Questions and Answers from authentic resources to improve knowledge and pass the exam at very first attempt. ----- Guaranteed.

KILL EXAMS

JN0-636 MCQs
JN0-636 TestPrep
JN0-636 Study Guide
JN0-636 Practice Test
JN0-636 Exam Questions

PASS

Juniper

JN0-636

Security, Professional (JNCIP-SEC)

Question: 181

SRX Series device enrollment with Policy Enforcer fails To debug further, the user issues the following commandshow configuration services securityâintelligence url

https://cloudfeeds.argon.juniperaecurity.net/api/manifeat.xml

and receives the following output:

What is the problem in this scenario?

A. The device is directly enrolled with Juniper ATP Cloud.
B. The device is already enrolled with Policy Enforcer.
C. The SRX Series device does not have a valid license.
D. Junos Space does not have matching schema based on the

Answer: C

Question: 182

You are asked to deploy filter-based forwarding on your SRX Series device for incoming traffic sourced from the 10.10 100 0/24 network in this scenario, which three statements are correct? (Choose three.)

A. You must create a forwarding-type routing instance.
B. You must create and apply a firewall filter that matches on the source address 10.10.100.0/24 and then sends this traffic to your routing
C. You must create and apply a firewall filter that matches on the destination address 10 10.100.0/24 and then sends this traffic to your routing instance.
D. You must create a RIB group that adds interface routes to your routing instance.
E. You must create a VRF-type routing instance.

Answer: A,B,D

Question: 183

You are asked to provide single sign-on (SSO) to Juniper ATP Cloud.

Which two steps accomplish this goal? (Choose two.)

A. Configure Microsoft Azure as the service provider (SP).
B. Configure Microsoft Azure as the identity provider (IdP).
C. Configure Juniper ATP Cloud as the service provider (SP).
D. Configure Juniper ATP Cloud as the identity provider (IdP).

Answer: B,C

Question: 184

You want to identify potential threats within SSL-encrypted sessions without requiring SSL proxy to decrypt the session contents.

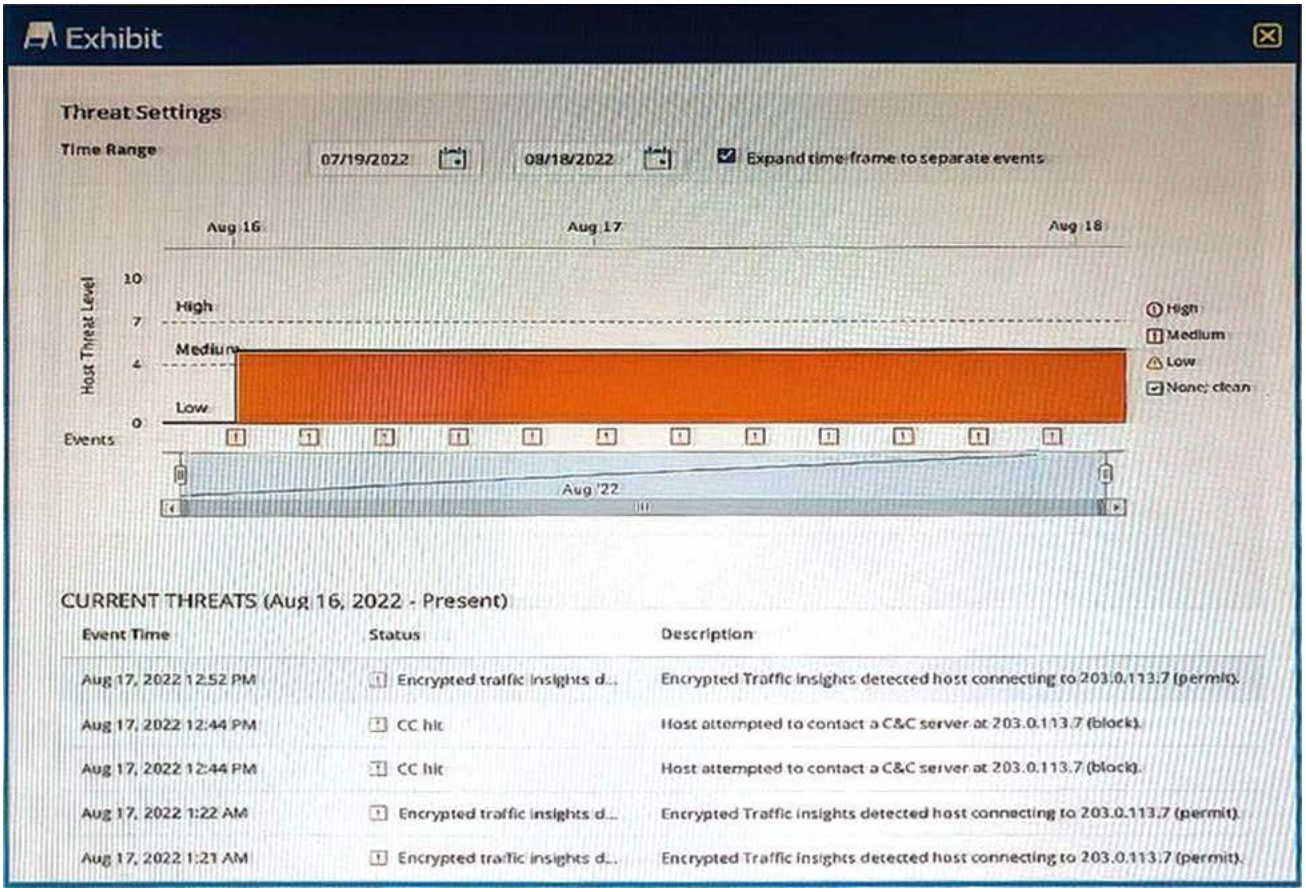
Which security feature achieves this objective?

A. infected host feeds
B. encrypted traffic insights
C. DNS security
D. Secure Web Proxy

Answer: B

Question: 185

Exhibit



You are using ATP Cloud and notice that there is a host with a high number of ETI and C&C hits sourced from the same investigation and notice that some of the events have not been automatically mitigated.

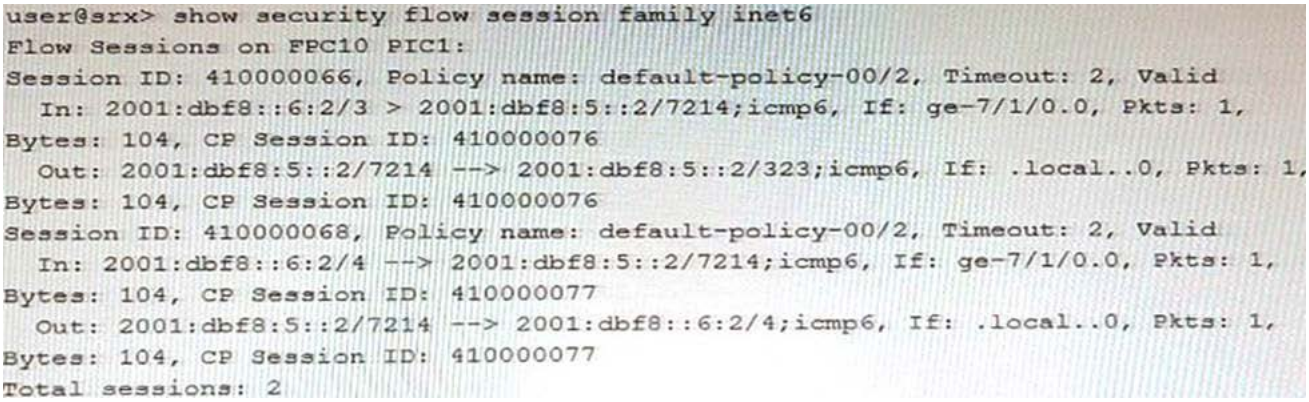
Referring to the exhibit, what is a reason for this behavior?

A. The C&C events are false positives.
B. The infected host score is globally set bellow a threat level of 5.
C. The infected host score is globally set above a threat level of 5.
D. The ETI events are false positives.

Answer: D

Question: 186

Exhibit



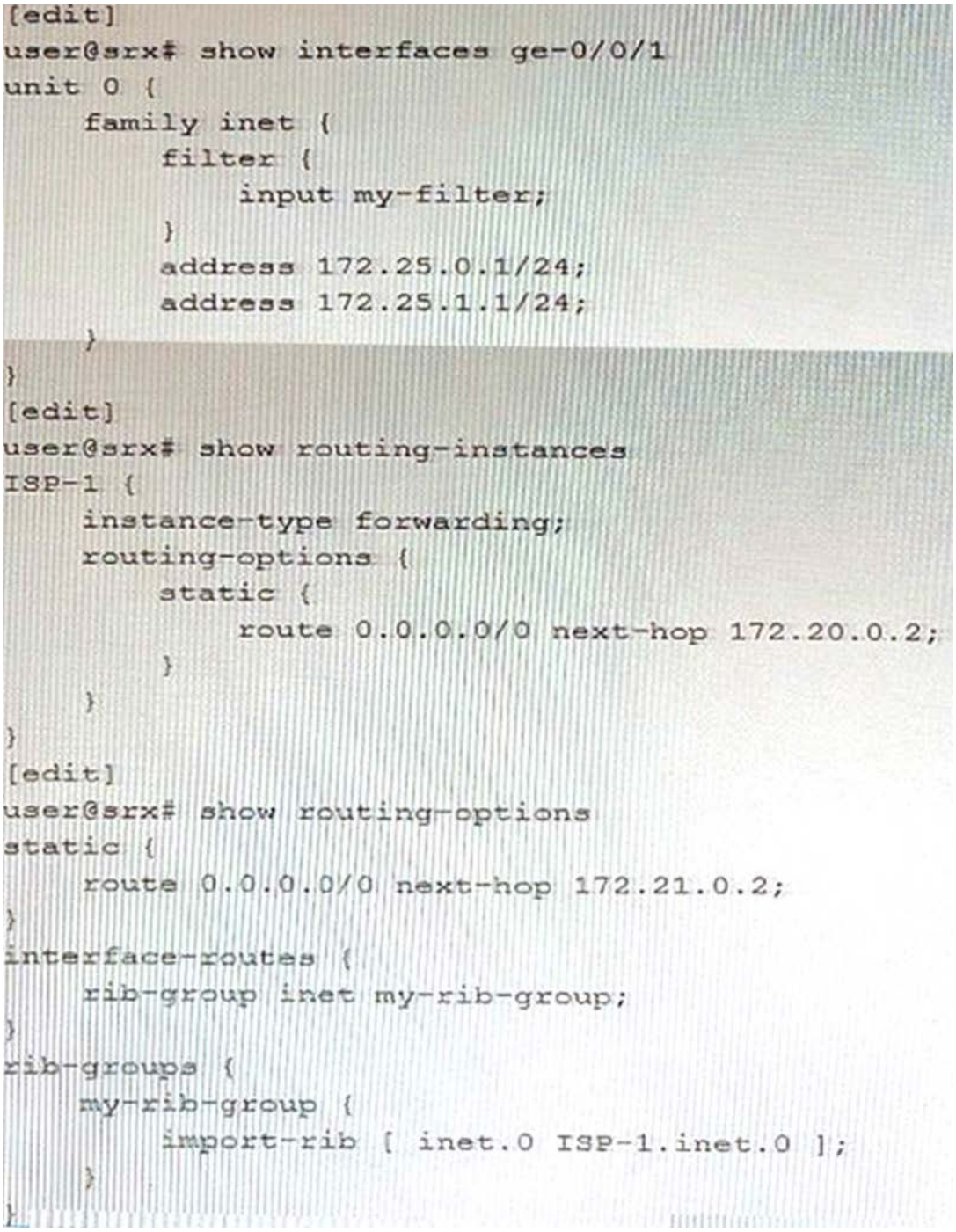
Which statement is true about the output shown in the exhibit?

A. The SRX Series device is configured with default security forwarding options.
B. The SRX Series device is configured with packet-based IPv6 forwarding options.
C. The SRX Series device is configured with flow-based IPv6 forwarding options.
D. The SRX Series device is configured to disable IPv6 packet forwarding.

Answer: A

Question: 187

Exhibit



```
[edit]
user@srx# show interfaces ge-0/0/1
unit 0 {
    family inet {
        filter {
            input my-filter;
        }
        address 172.25.0.1/24;
        address 172.25.1.1/24;
    }
}
[edit]
user@srx# show routing-instances
ISP-1 {
    instance-type forwarding;
    routing-options {
        static {
            route 0.0.0.0/0 next-hop 172.20.0.2;
        }
    }
}
[edit]
user@srx# show routing-options
static {
    route 0.0.0.0/0 next-hop 172.21.0.2;
}
interface-routes {
    rib-group inet my-rib-group;
}
rib-groups {
    my-rib-group {
        import-rib [ inet.0 ISP-1.inet.0 ];
    }
}
```

You are implementing filter-based forwarding to send traffic from the 172.25.0.0/24 network through ISP-1 while sending all other traffic through your connection to ISP-2. Your ge-0/0/1 interface connects to two networks, including the 172.25.0.0/24 network. You have implemented the configuration shown in the exhibit. The traffic from the 172.25.0.0/24 network is being forwarded as expected to 172.20.0.2, however traffic from the other network (172.25.1.0/24) is not being forwarded to the upstream 172.21.0.2 neighbor.

In this scenario, which action will solve this problem?

A. You must specify that the 172.25.1.1/24 IP address is the primary address on the ge-0/0/1 interface.
B. You must apply the firewall filter to the lo0 interface when using filter-based forwarding.
C. You must add another term to the firewall filter to accept the traffic from the 172.25.1.0/24 network.
D. You must create the static default route to neighbor 172.21 0.2 under the ISP-1 routing instance hierarchy.

Answer: D

Question: 188

Exhibit

```
May 23 05:20:34 Vendor-Id: 0 Attribute Type:Reply-Message(18) Value:string-type
Length:36
May 23 05:20:34 authd_radius_parse_message:generic-type:18
May 23 05:20:34 Vendor-Id: 0 Attribute Type:Reply-Message(18) Value:string-type
Length:15
May 23 05:20:34 authd_radius_parse_message:generic-type:18
May 23 05:20:34 Framework - module(radius) return: FAILURE
```

You configure a traceoptions file called radius on your returns the output shown in the exhibit

What is the source of the problem?

A. An incorrect password is being used.
B. The authentication order is misconfigured.
C. The RADIUS server IP address is unreachable.
D. The RADIUS server suffered a hardware failure.

Answer: D

Question: 189

Your Source NAT implementation uses an address pool that contains multiple IPv4 addresses Your users report that when they establish more than one session with an external application, they are prompted to authenticate multiple times External hosts must not be able to establish sessions with internal network hosts

What will solve this problem?

A. Disable PA
B. Enable destination NA
C. Enable persistent NAT
D. Enable address persistence.

Answer: B

Question: 190

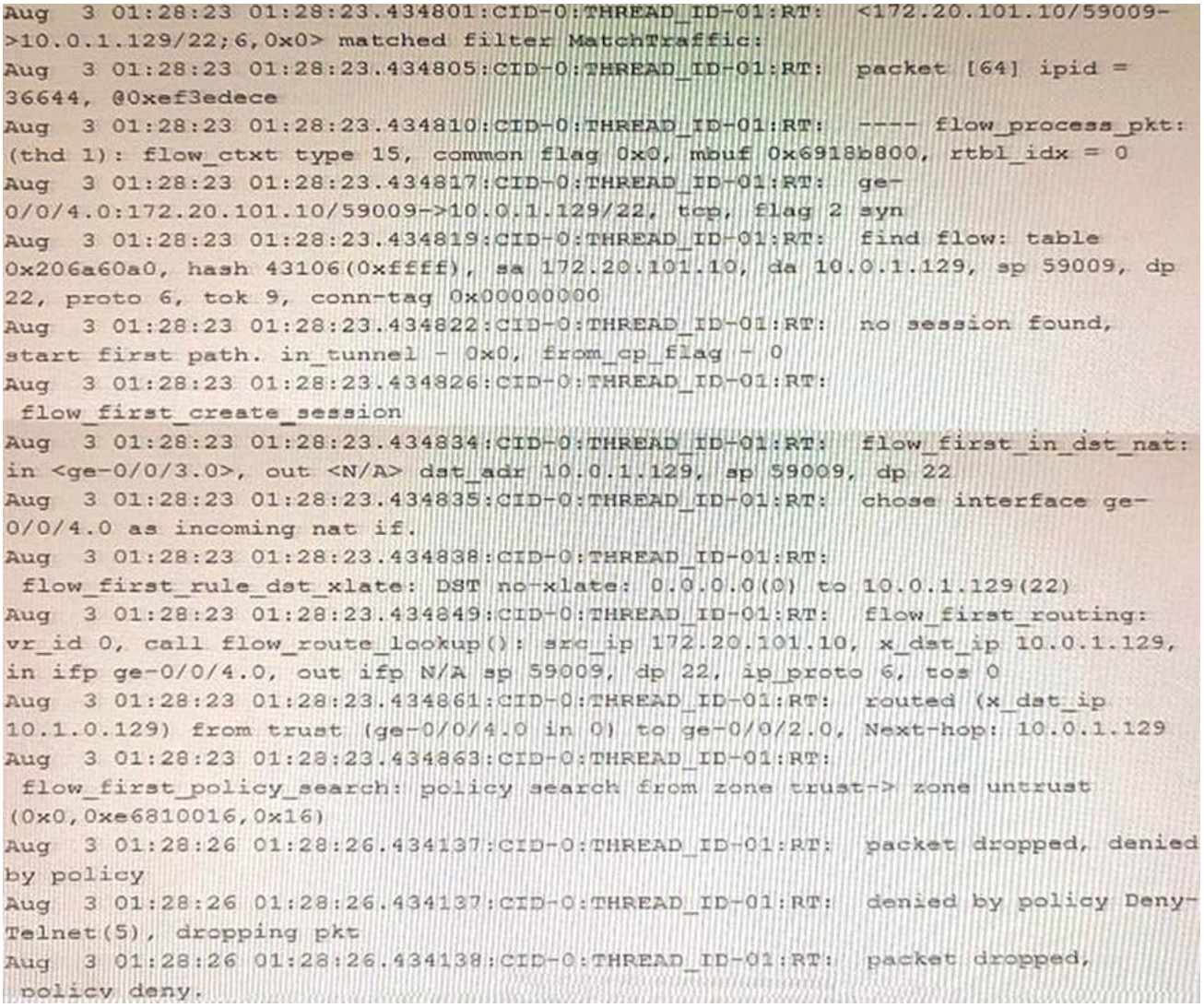
What is the purpose of the Switch Microservice of Policy Enforcer?

A. to isolate infected hosts
B. to enroll SRX Series devices with Juniper ATP Cloud
C. to inspect traffic for malware
D. to synchronize security policies to SRX Series devices

Answer: A

Question: 191

Exhibit



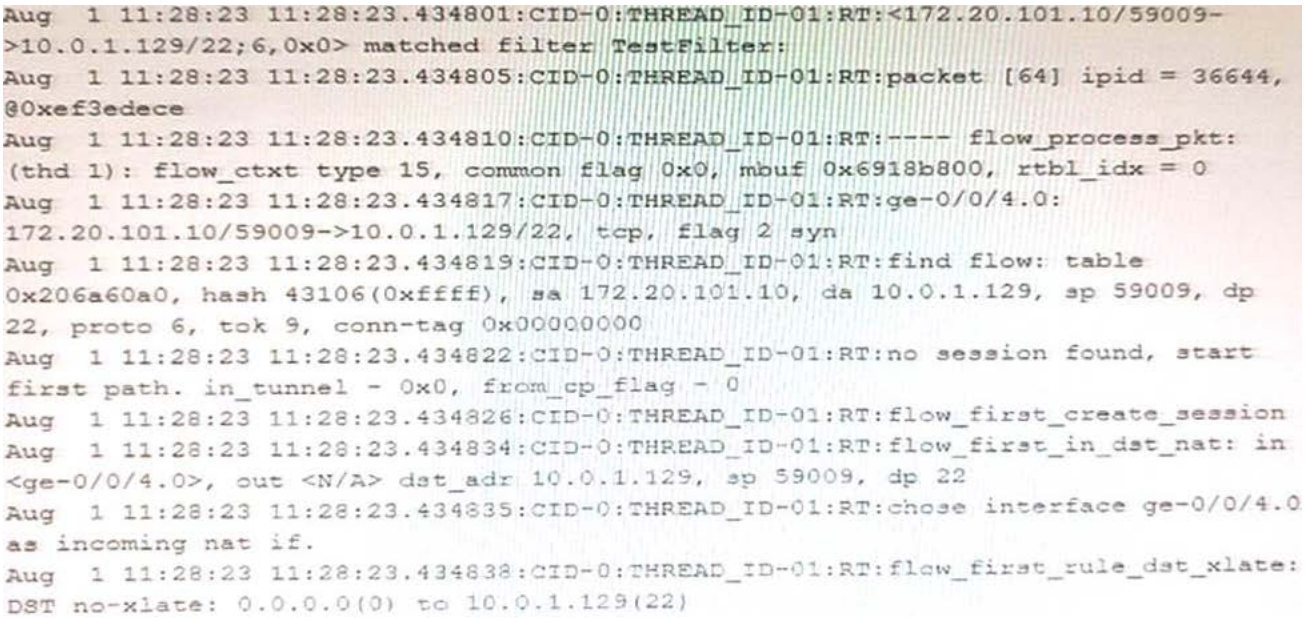
Referring to the exhibit, which statement is true?

A. This custom block list feed will be used before the Juniper Seclntel
B. This custom block list feed cannot be saved if the Juniper Seclntel block list feed is configured.
C. This custom block list feed will be used instead of the Juniper Seclntel block list feed
D. This custom block list feed will be used after the Juniper Seclntel block list feed.

Answer: D

Question: 192

Exhibit



The exhibit shows a snippet of a security flow trace.

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

A. This packet arrived on interface ge-0/0/4.0.
B. Destination NAT occurs.
C. The capture is a packet from the source address 172.20.101.10 destined to 10.0.1.129.
D. An existing session is found in the table.

Answer: A,C,D

Question: 193

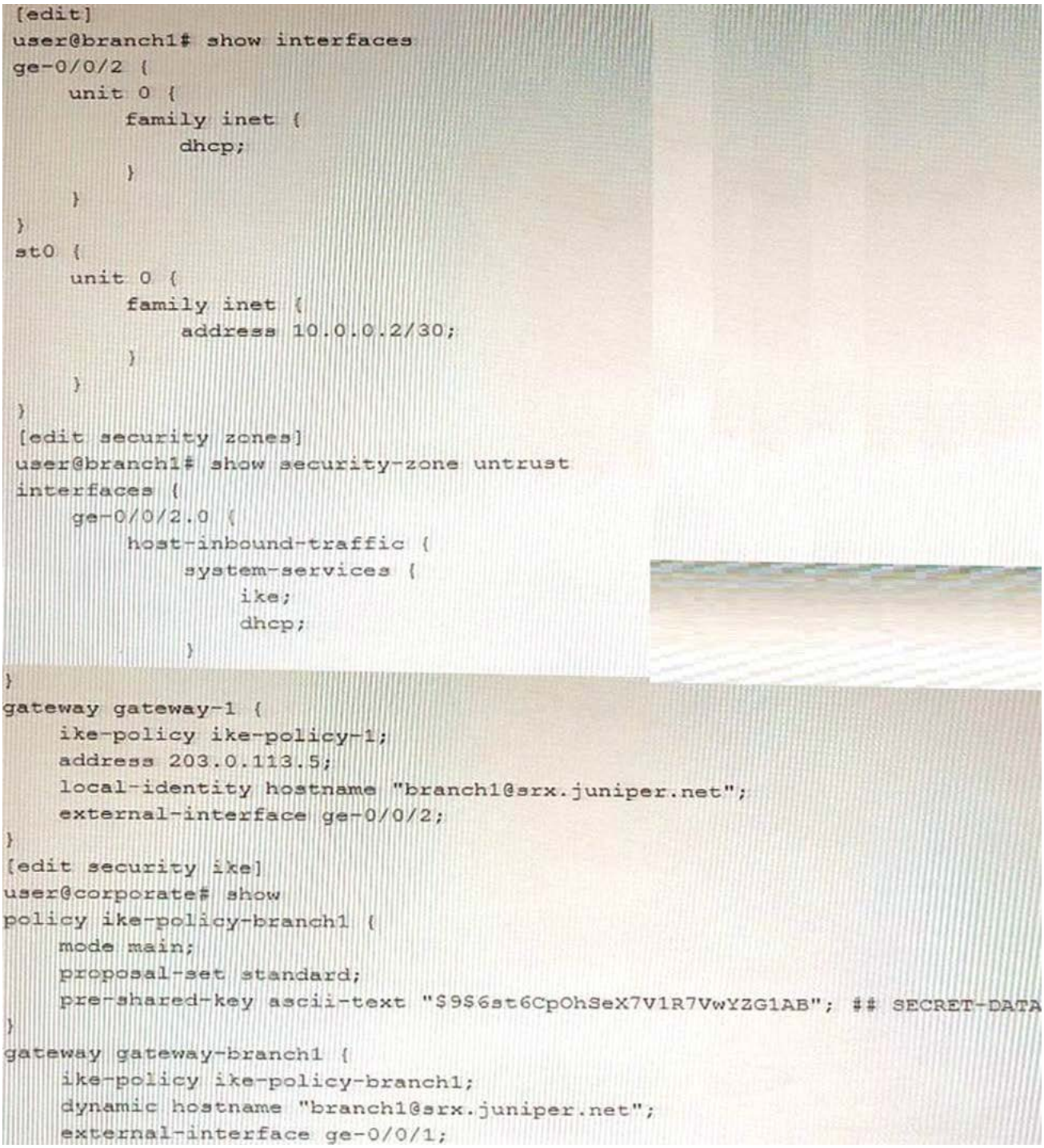
Regarding IPsec CoS-based VPNs, what is the number of IPsec SAs associated with a peer based upon?

A. The number of traffic selectors configured for the VP
B. The number of CoS queues configured for the VP
C. The number of classifiers configured for the VP
D. The number of forwarding classes configured for the VP

Answer: A

Question: 194

Exhibit



```
[edit]
user@branch1# show interfaces
ge-0/0/2 {
    unit 0 {
        family inet {
            dhcp;
        }
    }
}
st0 {
    unit 0 {
        family inet {
            address 10.0.0.2/30;
        }
    }
}
[edit security zones]
user@branch1# show security-zone untrust
interfaces {
    ge-0/0/2.0 {
        host-inbound-traffic {
            system-services {
                ike;
                dhcp;
            }
}
gateway gateway-1 {
    ike-policy ike-policy-1;
    address 203.0.113.5;
    local-identity hostname "branch1@srx.juniper.net";
    external-interface ge-0/0/2;
}
[edit security ike]
user@corporate# show
policy ike-policy-branch1 {
    mode main;
    proposal-set standard;
    pre-shared-key ascii-text "$9$6st6CpOhSeX7V1R7VwYZG1AB"; ## SECRET-DATA
}
gateway gateway-branch1 {
    ike-policy ike-policy-branch1;
    dynamic hostname "branch1@srx.juniper.net";
    external-interface ge-0/0/1;
```

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: 195

You want to configure a threat prevention policy.

Which three profiles are configurable in this scenario? (Choose three.)

A. device profile
B. SSL proxy profile
C. infected host profile
D. C&C profile
E. malware profile

Answer: A,D,E

Question: 196

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: 197

You are deploying a virtualization solution with the security devices in your network Each SRX Series device must support at least 100 virtualized instances and each virtualized instance must have its own discrete administrative domain.

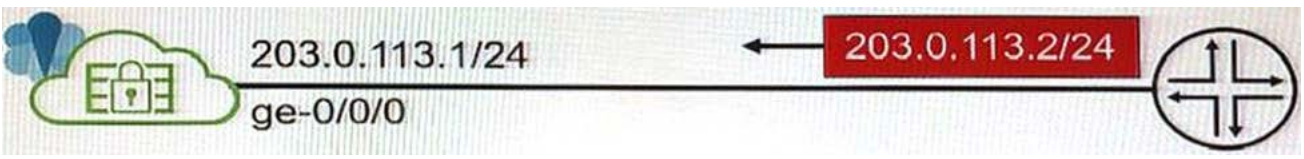
In this scenario, which solution would you choose?

A. VRF instances
B. virtual router instances
C. logical systems
D. tenant systems

Answer: C

Question: 198

Exhibit



You configure Source NAT using a pool of addresses that are in the same subnet range as the external ge-0/0/0 interface on your vSRX device. Traffic that is exiting the internal network can reach external destinations, but the

return traffic is being dropped by the service provider router.

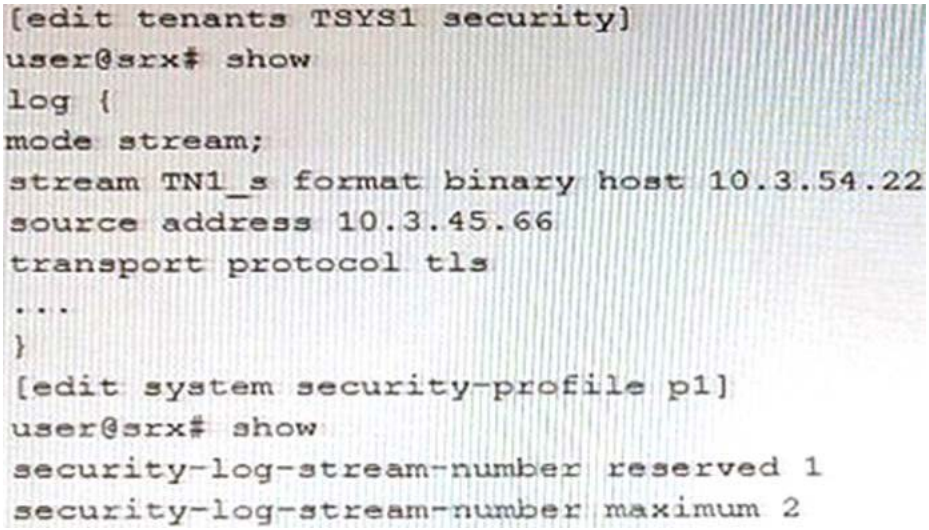
Referring to the exhibit, what must be enabled on the vSRX device to solve this problem?

A. STUN
B. Proxy ARP
C. Persistent NAT
D. DNS Doctoring

Answer: D

Question: 199

Exhibit



An administrator wants to configure an SRX Series device to log binary security events for tenant systems.

Referring to the exhibit, which statement would complete the configuration?

A. Configure the tenant as TSYS1 for the pi security profile.
B. Configure the tenant as root for the pi security profile.
C. Configure the tenant as master for the pi security profile.
D. Configure the tenant as local for the pi security profile

Answer: B

Question: 200

Your company wants to use the Juniper Seclntel feeds to block access to known command and control servers, but they do not want to use Security Director to manage the feeds.

Which two Juniper devices work in this situation? (Choose two)

A. EX Series devices
B. MX Series devices
C. SRX Series devices

D. QFX Series devices

Answer: B,C

KILLEXAMS.COM

Killexams.com is a leading online platform specializing in high-quality certification exam preparation. Offering a robust suite of tools, including MCQs, practice tests, and advanced test engines, Killexams.com empowers candidates to excel in their certification exams. Discover the key features that make Killexams.com the go-to choice for exam success.

Exam Questions:

Killexams.com provides exam questions that are experienced in test centers. These questions are updated regularly to ensure they are up-to-date and relevant to the latest exam syllabus. By studying these questions, candidates can familiarize themselves with the content and format of the real exam.

Exam MCQs:

Killexams.com offers exam MCQs in PDF format. These questions contain a comprehensive collection of questions and answers that cover the exam topics. By using these MCQs, candidate can enhance their knowledge and improve their chances of success in the certification exam.

Practice Test:

Killexams.com provides practice test through their desktop test engine and online test engine. These practice tests simulate the real exam environment and help candidates assess their readiness for the actual exam. The practice test cover a wide range of questions and enable candidates to identify their strengths and weaknesses.

Guaranteed Success:

Killexams.com offers a success guarantee with the exam MCQs. Killexams claim that by using this materials, candidates will pass their exams on the first attempt or they will get refund for the purchase price. This guarantee provides assurance and confidence to individuals preparing for certification exam.

Updated Contents:

Killexams.com regularly updates its question bank of MCQs to ensure that they are current and reflect the latest changes in the exam syllabus. This helps candidates stay up-to-date with the exam content and increases their chances of success.