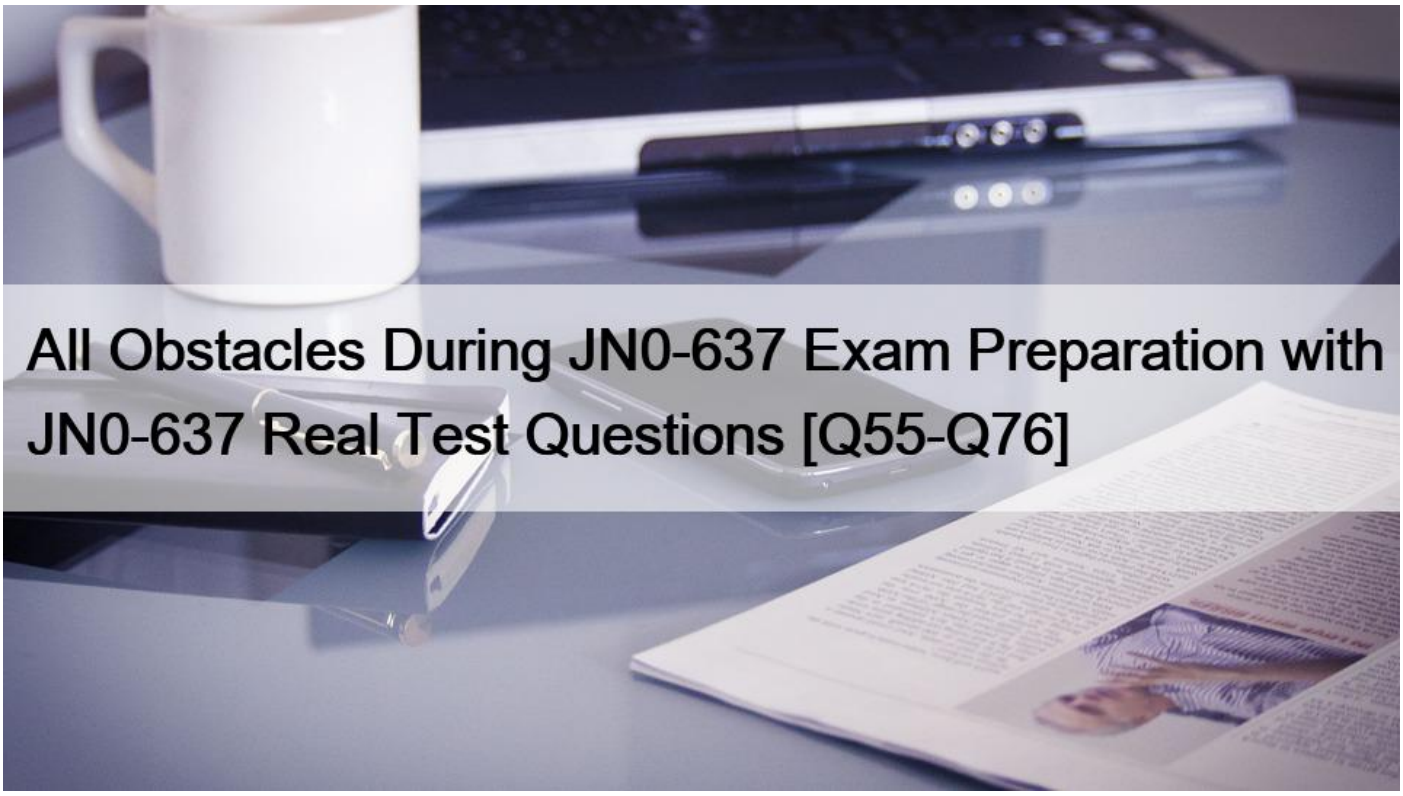
All Obstacles During JN0-637 Exam Preparation with JN0-637 Real Test Questions [Q55-Q76



All Obstacles During JN0-637 Exam Preparation with JN0-637 Real Test Questions Fully Updated Free Actual Juniper JN0-637 Exam Questions NEW QUESTION 55

Which two security intelligence feed types are supported?
* infected host feed
* Command and Control feed
* custom feeds
* malicious URL feed

The two security intelligence feed types that are supported are:

A) Infected host feed. An infected host feed is a security intelligence feed that contains the IP addresses of hosts that are infected by malware or compromised by attackers. The SRX Series device can download the infected host feed from the Juniper ATP Cloud or generate its own infected host feed based on the detection events from IDP. The SRX Series device can use the infected host feed to block or quarantine the traffic to or from the infected hosts based on the security policies1.

B) Command and Control feed. A command and control feed is a security intelligence feed that contains the IP addresses of servers that are used by malware or attackers to communicate with infected hosts.

The SRX Series device can download the command and control feed from the Juniper ATP Cloud or generate its own command and control feed based on the detection events from IDP. The SRX Series device can use the command and control feed to block or log the traffic to or from the command and control servers based on the security policies2.

The other options are incorrect because:

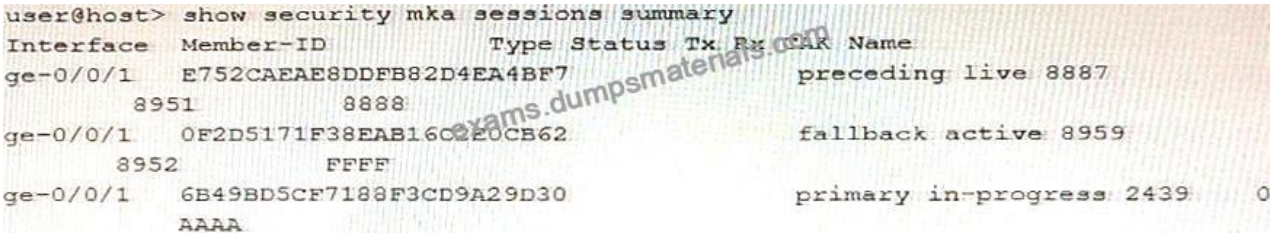
C) Custom feeds. Custom feeds are not a security intelligence feed type, but a feature that allows you to create your own security intelligence feeds based on your own criteria and sources. You can configure custom feeds by using the Junos Space Security Director or the CLI. Custom feeds are not supported by the Juniper ATP Cloud or the IDP3.

D) Malicious URL feed. Malicious URL feed is not a security intelligence feed type, but a feature that allows you to block or log the traffic to or from malicious URLs based on the security policies. The SRX Series device can download the malicious URL feed from the Juniper ATP Cloud or the Juniper Threat Labs. Malicious URL feed is not supported by the IDP4.

Reference: Infected Host Feed Overview Command and Control Feed Overview Custom Feed Overview Malicious URL Feed Overview

NEW QUESTION 56

Exhibit

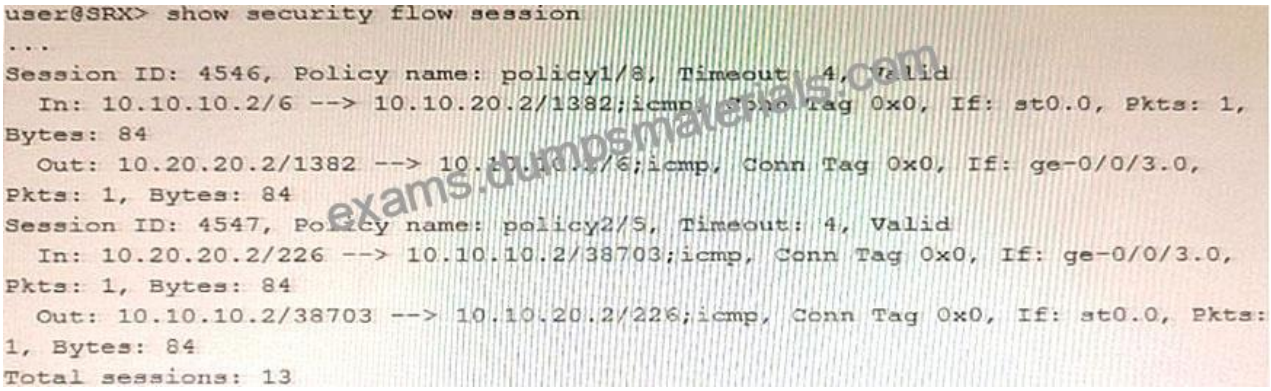


Referring to the exhibit, which two statements are true about the CAK status for the CAK named

“FFFP”? (Choose two.)
* CAK is not used for encryption and decryption of the MACsec session.
* SAK is successfully generated using this key.
* CAK is used for encryption and decryption of the MACsec session.
* SAK is not generated using this key.

NEW QUESTION 57

Exhibit



You are validating bidirectional traffic flows through your IPsec tunnel. The 4546 session represents traffic being sourced from the remote end of the IPsec tunnel. The 4547 session represents traffic that is sourced from the local network destined to the remote network.

Which statement is correct regarding the output shown in the exhibit?
* The remote gateway address for the IPsec tunnel is 10.20.20.2
* The session information indicates that the IPsec tunnel has not been established
* The local gateway address for the IPsec tunnel is 10.20.20.2
* NAT is being used to change the source address of outgoing packets

NEW QUESTION 58

You are asked to control access to network resources based on the identity of an authenticated device.

Which three steps will accomplish this goal on the SRX Series firewalls? (Choose three)
* Configure an end-user-profile that characterizes a device or set of devices
* Reference the end-user-profile in the security zone
* Reference the end-user-profile in the security policy.
* Apply the end-user-profile at the interface connecting the devices
* Configure the authentication source to be used to authenticate the device

To control access to network resources based on the identity of an authenticated device on the SRX Series firewalls, you need to perform the following steps:

A) Configure an end-user-profile that characterizes a device or set of devices. An end-user-profile is a device identity profile that contains a collection of attributes that are characteristics of a specific group of devices, or of a specific device, depending on the attributes configured in the profile. The end-user- profile must contain a domain name and at least one value in each attribute. The attributes include device-identity, device-category, device-vendor, device-type, device-os, and device-os-version1. You can configure an end-user-profile by using the Junos Space Security Director or the CLI2.

C) Reference the end-user-profile in the security policy. A security policy is a rule that defines the action to be taken for the traffic that matches the specified criteria, such as source and destination addresses, zones, protocols, ports, and applications. You can reference the end-user-profile in the source-end-user- profile field of the security policy to identify the traffic source based on the device from which the traffic issued. The SRX Series device matches the IP address of the device to the end-user-profile and applies the security policy accordingly3. You can reference the end-user-profile in the security policy by using the Junos Space Security Director or the CLI4.

E) Configure the authentication source to be used to authenticate the device. An authentication source is a system that provides the device identity information to the SRX Series device. The authentication source can be Microsoft Windows Active Directory or a third-party network access control (NAC) system.

You need to configure the authentication source to be used to authenticate the device and to send the device identity information to the SRX Series device. The SRX Series device stores the device identity information in the device identity authentication table5. You can configure the authentication source by using the Junos Space Security Director or the CLI6.

The other options are incorrect because:

B) Referencing the end-user-profile in the security zone is not a valid step to control access to network resources based on the identity of an authenticated device. A security zone is a logical grouping of interfaces that have similar security requirements. You

can reference the user role in the security zone to identify the user who is accessing the network resources, but not the end-user-profile7.

D) Applying the end-user-profile at the interface connecting the devices is also not a valid step to control access to network resources based on the identity of an authenticated device. You cannot apply the end- user-profile at the interface level, but only at the security policy level. The end-user-profile is not a firewall filter or a security policy, but a device identity profile that is referenced in the security policy1.

Reference: End User Profile Overview Creating an End User Profile source-end-user-profile Creating Firewall Policy Rules Understanding the Device Identity Authentication Table and Its Entries Configuring the Authentication Source for Device Identity user-role

NEW QUESTION 59

You are not able to activate the SSH honeypot on the all-in-one Juniper ATP appliance.

What would be a cause of this problem?
* The collector must have a minimum of two interfaces.
* The collector must have a minimum of three interfaces.
* The collector must have a minimum of five interfaces.
* The collector must have a minimum of four interfaces.

https://www.juniper.net/documentation/en_US/release-independent/jatp/topics/task/configuration/jatp-traffic-collectorsetting-ssh-honeypot-detection.html

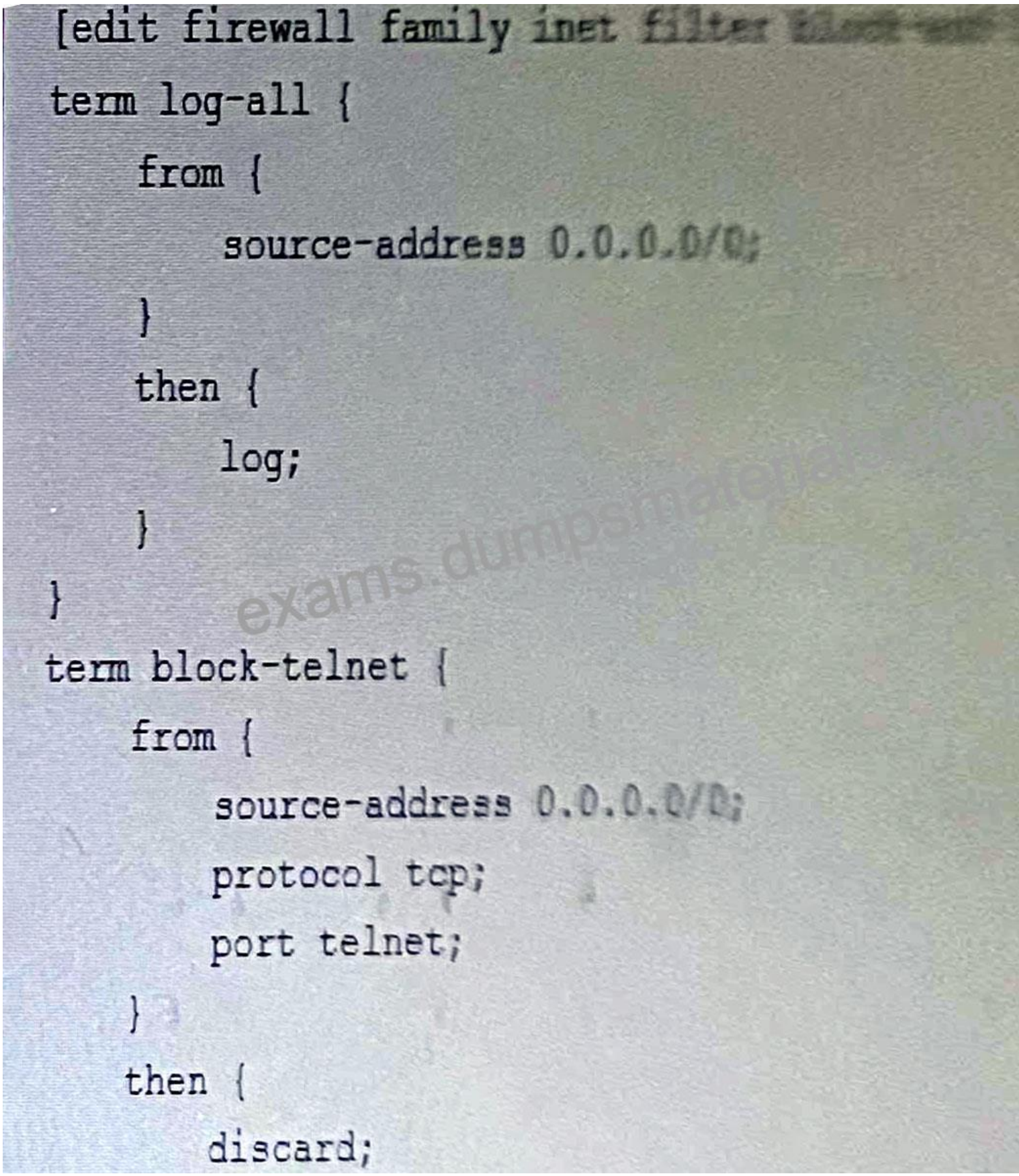
NEW QUESTION 60

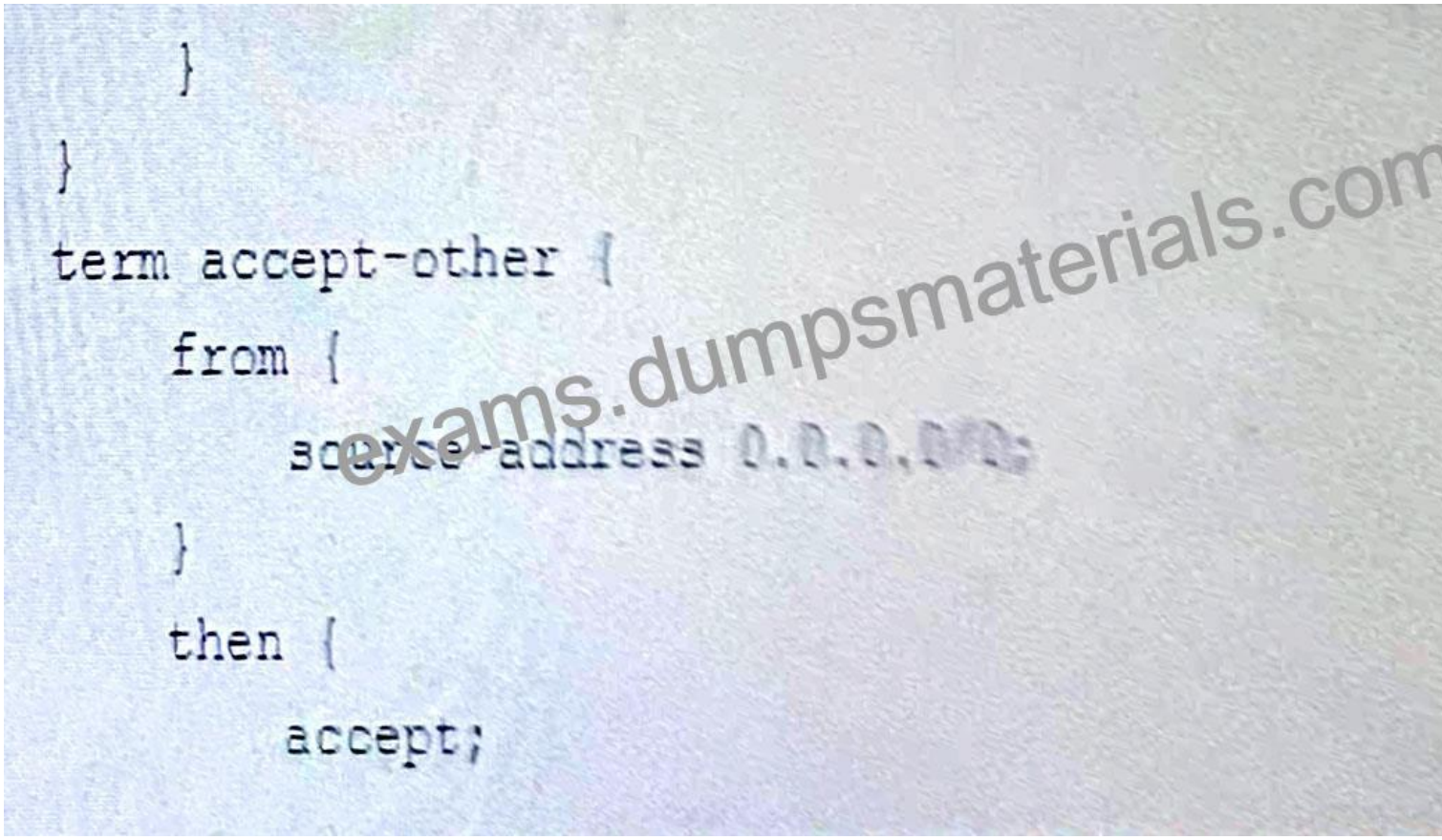
Your company wants to use the Juniper Seclntel feeds to block access to known command and control servers, but they do not want to use Security Director to manage the feeds.

Which two Juniper devices work in this situation? (Choose two)
* EX Series devices
* MX Series devices
* SRX Series devices
* QFX Series devices

NEW QUESTION 61

Exhibit:


[edit firewall family inet filter
term log-all {
from {
source-address 0.0.0.0/0;
}
then {
log;
}
}
term block-telnet {
from {
source-address 0.0.0.0/0;
protocol tcp;
port telnet;
}
then {
discard;



You are troubleshooting a firewall filter shown in the exhibit that is intended to log all traffic and block only inbound telnet traffic on interface ge-0/0/3.

How should you modify the configuration to fulfill the requirements?
* Modify the log-all term to add the next term action
* Delete the log-all term
* Add a term before the log-all term that blocks Telnet
* Apply a firewall filter to the loopback interface that blocks Telnet traffic

To modify the configuration to fulfill the requirements, you need to modify the log-all term to add the next term action.

The other options are incorrect because:

B) Deleting the log-all term would prevent logging all traffic, which is one of the requirements. The log-all term matches all traffic from any source address and logs it to the system log file1.

C) Adding a term before the log-all term that blocks Telnet would also prevent logging all traffic, because the log-all term would never be reached. The firewall filter evaluates the terms in sequential order and applies the first matching term. If a term before the log-all term blocks Telnet, then the log-all term would not match any traffic and no logging would occur2.

D) Applying a firewall filter to the loopback interface that blocks Telnet traffic would not block inbound Telnet traffic on interface ge-0/0/3, which is another requirement. The loopback interface is a logical interface that is always up and reachable. It is used for routing and management purposes, not for filtering traffic on physical interfaces3.

Therefore, the correct answer is A. You need to modify the log-all term to add the next term action. The next term action instructs the firewall filter to continue evaluating the subsequent terms after matching the current term. This way, the log-all term would log all traffic and then proceed to the block-telnet term, which would block only inbound Telnet traffic on interface ge-0/0/34. To modify the log-all term to add the next term action, you need to perform the following steps:

Enter the configuration mode: user@host> configure

Navigate to the firewall filter hierarchy: user@host# edit firewall family inet filter block-telnet Add the next term action to the log-all term: user@host# set term log-all then next term Commit the changes: user@host# commit Reference: log (Firewall Filter Action) Firewall Filter Configuration Overview loopback (Interfaces) next term (Firewall Filter Action)

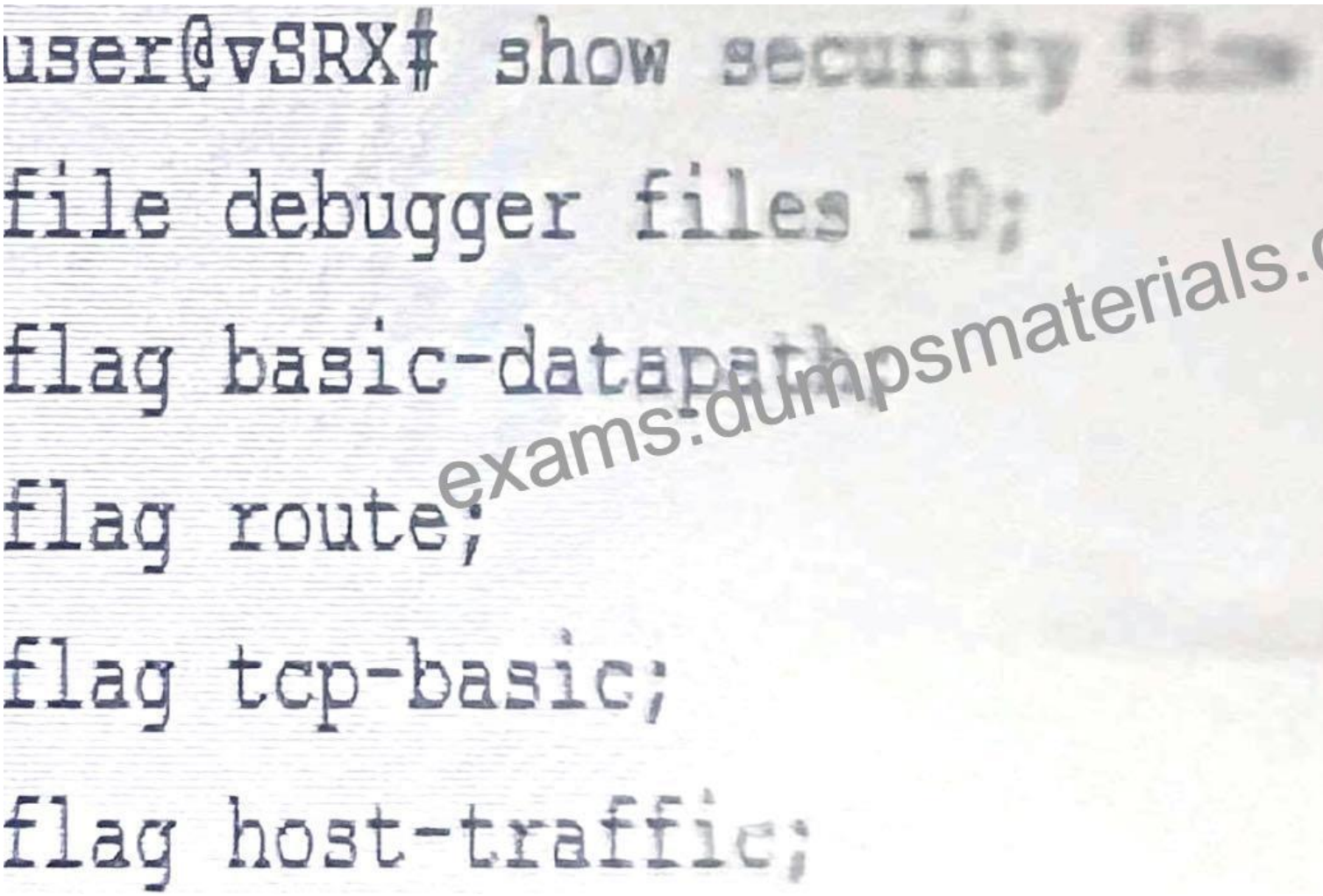
NEW QUESTION 62

You are required to deploy a security policy on an SRX Series device that blocks all known Tor network IP addresses.

Which two steps will fulfill this requirement? (Choose two.)
* Enroll the devices with Juniper ATP Appliance.
* Enroll the devices with Juniper ATP Cloud.
* Enable a third-party Tor feed.
* Create a custom feed containing all current known MAC addresses.

NEW QUESTION 63

Exhibit:



The security trace options configuration shown in the exhibit is committed to your SRX series firewall.

Which two statements are correct in this Scenario? (Choose Two)
* The file debugger will be readable by all users.
* Once the trace has generated 10 log files, older logs will be overwritten.
* Once the trace has generated 10 log files, the trace process will halt.
* The file debugger will be readable only by the user who committed this configuration

Once the trace has generated 10 log files, older logs will be overwritten. – This is generally true if the configuration includes a file count limit and the ‘world-readable’ flag. Without the ‘world-readable’ flag, only the file’s owner or superuser can read the file. If the ‘no-world-readable’ flag is set, only the user that created the file and root can read it.

Once the trace has generated 10 log files, the trace process will halt. – This would be true only if the ‘files’ statement is used without the ‘world-readable’ or ‘no-world-readable’ flag. If ‘no-world-readable’ is set, the trace files are not readable by all users.

NEW QUESTION 64

Exhibit

```
user@srx> show interfaces ge-0/0/5.0 extensive | find security
Security : Zone: dmz
Allowed host-inbound traffic : bootp bfd bgp dns dvmrp igmp ldp msdp nhrp ospf
ospf3 pgm pim rip ripng router- discovery rsvp sap vrrp dhcp finger
```

Referring to the exhibit, which three protocols will be allowed on the ge-0/0/5.0 interface? (Choose three.)
* IBGP
* OSPF
* IPsec
* DHCP
* NTP

NEW QUESTION 65

You have the NAT rule, shown in the exhibit, applied to allow communication across an IPsec tunnel between your two sites with identical networks.

Which statement is correct in this scenario?
* The NAT rule with translate the source and destination addresses.
* The NAT rule will only translate two addresses at a time.
* The NAT rule in applied to the N/A routing instance.
* 10 packets have been processed by the NAT rule.

NEW QUESTION 66

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?
* Disable PAT.
* Enable destination NAT.
* Enable persistent NAT
* Enable address persistence.

NEW QUESTION 67

You have designed the firewall filter shown in the exhibit to limit SSH control traffic to yours SRX Series device without affecting other traffic.

Which two statement are true in this scenario? (Choose two.)
* The filter should be applied as an output filter on the loopback interface.
* Applying the filter will achieve the desired result.
* Applying the filter will not achieve the desired result.
* The filter should be applied as an input filter on the loopback interface.

Based on general practices, to limit SSH control traffic to an SRX device without affecting other traffic, you would typically apply a firewall filter as an input filter on the loopback interface. The filter would specify the allowed source addresses or networks for SSH and deny all other SSH traffic.

Therefore, the two statements that are likely to be true, in general, are:

Applying the filter will achieve the desired result (assuming the filter is correctly written).

The filter should be applied as an input filter on the loopback interface (as this is the standard practice).

NEW QUESTION 68

You are asked to detect domain generation algorithms

Which two steps will accomplish this goal on an SRX Series firewall? (Choose two.)
* Define an advanced-anti-malware policy under [edit services].
* Attach the security-metadata-streaming policy to a security
* Define a security-metadata-streaming policy under [edit
* Attach the advanced-anti-malware policy to a security policy.

NEW QUESTION 69

you configured a security policy permitting traffic from the trust zone to the untrust zone but your traffic not hitting the policy.

In this scenario, which cli command allows you to troubleshoot traffic problem using the match criteria?
* show security policy-report
* show security application-tracking counters
* show security match-policies
* request security policies check

To troubleshoot the traffic problem using the match criteria, you need to use the show security match- policies CLI command.

The other options are incorrect because:

A) The show security policy-report CLI command displays the policy report, which is a summary of the policy usage statistics, such

as the number of sessions, bytes, and packets that match each policy. It does not show the match criteria or the reason why the traffic is not hitting the policy1.

B) The show security application-tracking counters CLI command displays the application tracking counters, which are the statistics of the application usage, such as the number of sessions, bytes, and packets that match each application. It does not show the match criteria or the reason why the traffic is not hitting the policy2.

D) The request security policies check CLI command checks the validity and consistency of the security policies, such as the syntax, the references, and the conflicts. It does not show the match criteria or the reason why the traffic is not hitting the policy3.

Therefore, the correct answer is C. You need to use the show security match-policies CLI command to troubleshoot the traffic problem using the match criteria. The show security match-policies CLI command displays the policies that match the specified criteria, such as the source and destination addresses, the zones, the protocols, and the ports. It also shows the action and the hit count of each matching policy.

You can use this command to verify if the traffic is matching the expected policy or not, and if not, what policy is blocking or rejecting the traffic4

NEW QUESTION 70

A company wants to paron their physical SRX series firewall into multiple logical units and assign each unit (tenant) to a department within the organization. You are the primary administrator of firewall and a colleague is the administrator for one of the departments.

Which two statements are correct about your colleague? (Choose two)
* The colleague can configure the resources allocated and routing protocols
* The colleague can access and view the resources of the tenant system.
* The colleague can create and assign logical interfaces to the tenant system
* The colleague can modify the number of allocated resources for the tenant system

A)company wants to partition their physical SRX series firewall into multiple logical units and assign each unit (tenant) to a department within the organization. You are the primary administrator of the firewall and a colleague is the administrator for one of the departments.

The two statements that are correct about your colleague are:

B) The colleague can access and view the resources of the tenant system. A tenant system is a type of logical system that is created and managed by the primary administrator of the firewall. A tenant system has its own discrete administrative domain, logical interfaces, routing instances, security policies, and other features. The primary administrator can assign a tenant system to a department within the organization and delegate the administration of the tenant system to a colleague. The colleague can access and view the resources of the tenant system, such as the allocated CPU, memory, and bandwidth, and the configured interfaces, zones, and policies1.

C) The colleague can create and assign logical interfaces to the tenant system. A logical interface is a software interface that represents a subset of the physical interface. A logical interface can have its own address, encapsulation, and routing parameters. The primary administrator can allocate a number of logical interfaces to a tenant system and allow the colleague to create and assign logical interfaces to the tenant system. The colleague can configure the logical interfaces with the appropriate address, encapsulation, and routing parameters for the tenant system2.

The other statements are incorrect because:

A) The colleague cannot configure the resources allocated and routing protocols. The resources allocated and routing protocols are configured by the primary administrator of the firewall. The primary administrator can allocate a fixed amount of resources, such as CPU, memory, and bandwidth, to a tenant system and specify the routing protocols that are allowed for the tenant system. The colleague cannot modify the resources allocated or routing protocols for the tenant system1.

D) The colleague cannot modify the number of allocated resources for the tenant system. The number of allocated resources for the tenant system is configured by the primary administrator of the firewall. The primary administrator can allocate a fixed amount of resources, such as CPU, memory, and bandwidth, to a tenant system and monitor the resource usage of the tenant system. The colleague cannot modify the number of allocated resources for the tenant system1.

Reference: Understanding Tenant Systems Understanding Logical Interfaces

NEW QUESTION 71

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

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

and receives the following output:

What is the problem in this scenario?
* The device is directly enrolled with Juniper ATP Cloud.
* The device is already enrolled with Policy Enforcer.
* The SRX Series device does not have a valid license.
* Junos Space does not have matching schema based on the

NEW QUESTION 72

Which two additional configuration actions are necessary for the third-party feed shown in the exhibit to work properly? (Choose two.)
* You must create a dynamic address entry with the IP filter category and the ipfilter_office365 value.
* You must create a dynamic address entry with the C&C category and the cc_offic365 value.
* You must apply the dynamic address entry in a security policy.
* You must apply the dynamic address entry in a security intelligence policy.

NEW QUESTION 73

Click the Exhibit button.

```
Communicate with JATP server...
error: [Error] Failed to communicate with JATP server when retrieving
registration status.
Please make sure you are able to connect to JATP server. If this issue still
remains, please contact JTAC for help.
```


When attempting to enroll an SRX Series device to JATP, you receive the error shown in the exhibit.

What is the cause of the error?

* The fxp0 IP address is not routable
* The SRX Series device certificate does not match the JATP certificate
* The SRX Series device does not have an IP address assigned to the interface that accesses JATP
* A firewall is blocking HTTPS on fxp0

Reference:

https://kb.juniper.net/InfoCenter/index?page=content&id=KB33979&cat=JATP_SERIES&actp=LIST

NEW QUESTION 74

You issue the command shown in the exhibit.

Which policy will be active for the identified traffic?
* Policy p4
* Policy p7
* Policy p1
* Policy p12

NEW QUESTION 75

You are asked to share threat intelligence from your environment with third party tools so that those tools can be identify and block lateral threat propagation from compromised hosts.

Which two steps accomplish this goal? (Choose Two)
* Configure application tokens in the SRX Series firewalls to limit who has access
* Enable Juniper ATP Cloud to share threat intelligence
* Configure application tokens in the Juniper ATP Cloud to limit who has access
* Enable SRX Series firewalls to share Threat intelligence with third party tool.

To share threat intelligence from your environment with third party tools, you need to enable Juniper ATP Cloud to share threat intelligence and configure application tokens in the Juniper ATP Cloud to limit who has access. The other options are incorrect because:

A) Configuring application tokens in the SRX Series firewalls is not necessary or sufficient to share threat intelligence with third party tools. Application tokens are used to authenticate and authorize requests to the Juniper ATP Cloud API, which can be used to perform various operations such as submitting files, querying C&C feeds, and managing allowlists and blocklists1. However, to share threat intelligence with third party tools, you need to enable the TAXII service in the Juniper ATP Cloud, which is a different protocol for exchanging threat information2.

D) Enabling SRX Series firewalls to share threat intelligence with third party tools is not possible or supported. SRX Series firewalls can send potentially malicious objects and files to the Juniper ATP Cloud for analysis and receive threat intelligence from the Juniper ATP Cloud to block malicious traffic3.

However, SRX Series firewalls cannot directly share threat intelligence with third party tools. You need to use the Juniper ATP Cloud as the intermediary for threat intelligence sharing. Therefore, the correct answer is B and C. You need to enable Juniper ATP Cloud to share threat intelligence and configure application tokens in the Juniper ATP Cloud to limit who has access.

To do so, you need to perform the following steps:

Enable and configure the TAXII service in the Juniper ATP Cloud. TAXII (Trusted Automated eXchange of Indicator Information) is a protocol for communication over HTTPS of threat information between parties.

STIX (Structured Threat Information eXpression) is a language used for reporting and sharing threat information using TAXII. Juniper ATP Cloud can contribute to STIX reports by sharing the threat intelligence it gathers from file scanning. Juniper ATP Cloud also uses threat information from STIX reports as well as other sources for threat prevention2. To enable and configure the TAXII service, you need to select Configure > Threat Intelligence Sharing in the Juniper ATP Cloud WebUI, move the knob to the right to Enable TAXII, and move the slidebar to designate a file sharing threshold2. Configure application tokens in the Juniper ATP Cloud. Application tokens are used to authenticate and authorize requests to the Juniper ATP Cloud API and the TAXII service. You can create and manage application tokens in the Juniper ATP Cloud WebUI by selecting Configure > Application Tokens. You can specify the name, description, expiration date, and permissions of each token. You can also revoke or delete tokens as needed. You can use the application tokens to limit who has access to your shared threat intelligence by granting or denying permissions to the TAXII service1.

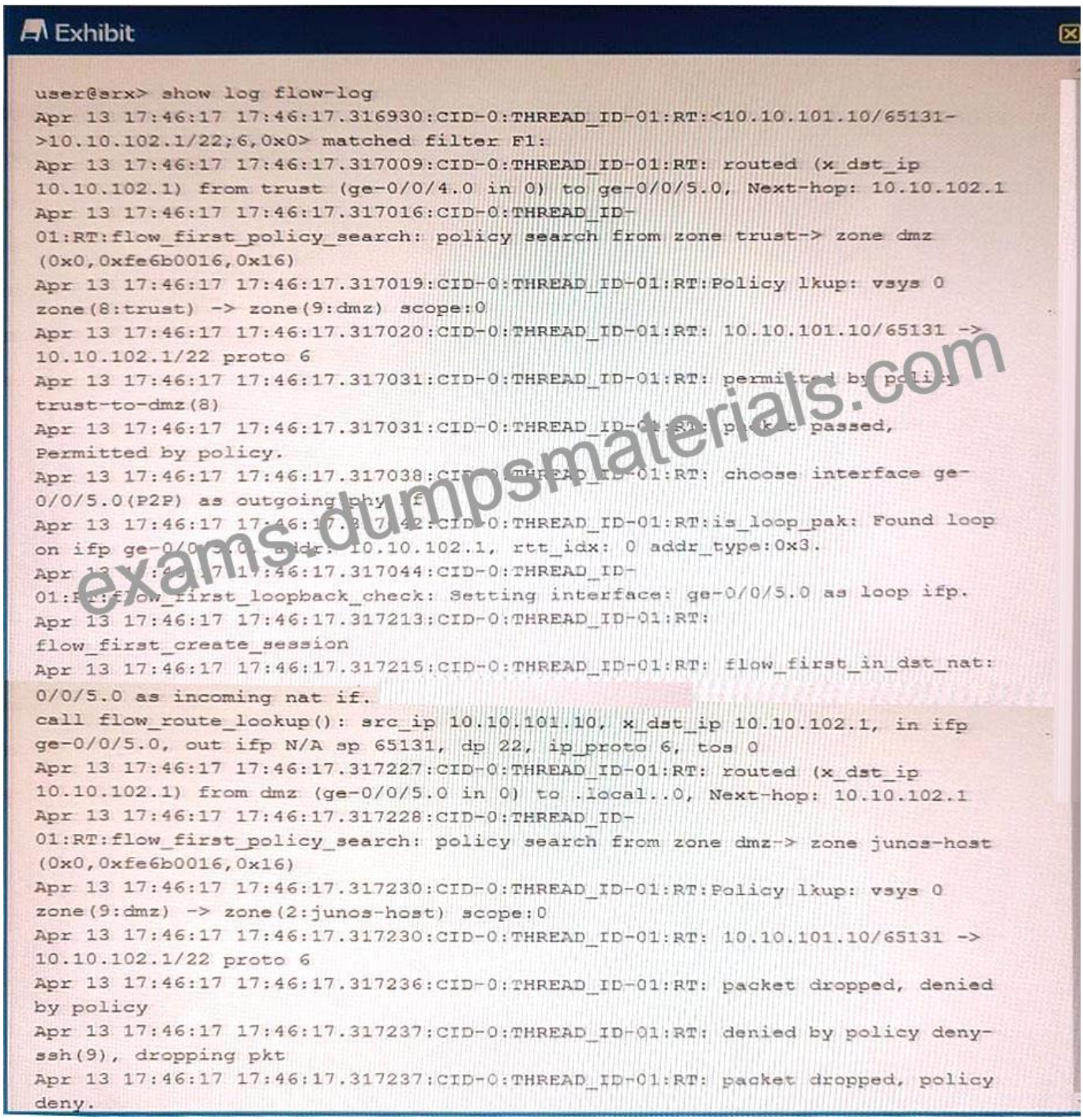
Reference: Threat Intelligence Open API Setup Guide

Configure Threat Intelligence Sharing

About Juniper Advanced Threat Prevention Cloud

NEW QUESTION 76

Exhibit



You are using traceoptions to verify NAT session information on your SRX Series device.

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

* This is the last packet in the session.
* The SRX Series device is performing both source and destination NAT on this session.
* This is the first packet in the session.
* The SRX Series device is performing only source NAT on this session.

Validate your JN0-637 Exam Preparation with JN0-637 Practice Test:
https://www.dumpsmaterials.com/JN0-637-real-torrent.html]