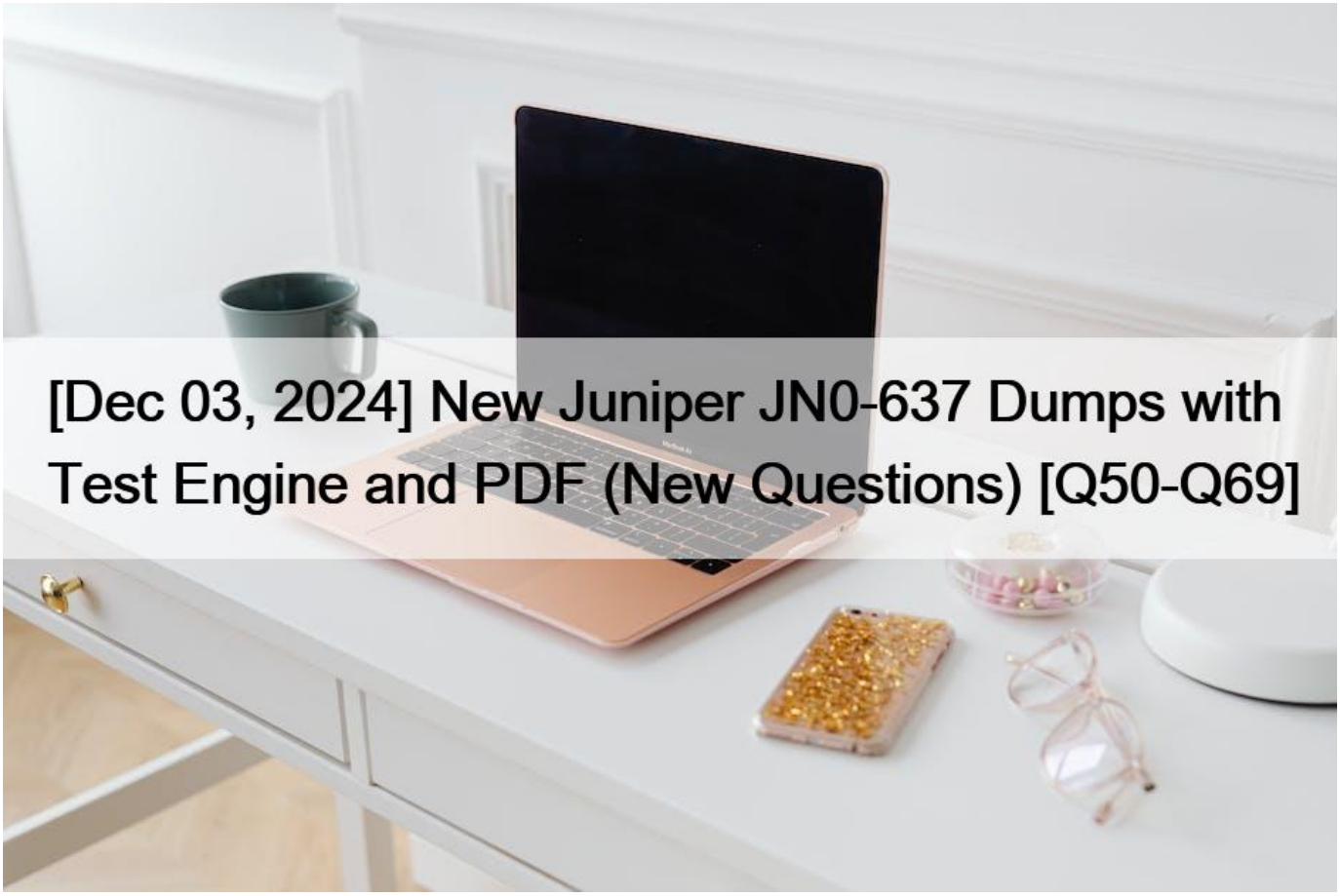
[Dec 03, 2024 New Juniper JN0-637 Dumps with Test Engine and PDF (New Questions) [Q50-Q69



[Dec 03, 2024 New Juniper JN0-637 Dumps with Test Engine and PDF (New Questions) Pass Your JN0-637 Exam Easily - Real JN0-637 Practice Dump Updated NEW QUESTION 50

Exhibit

```
user@srx> show security flow session family inet6
Flow Sessions on FPC10 PIC1:
Session ID: 410000066, Policy name: default-policy-00/2, Timeout: 2, Valid
  In: 2001:dbf8::6:2/3 > 2001:dbf8:5::2/7214;icmp6, If: ge-7/1/0.0, Pkts: 1,
Bytes: 104, CP Session ID: 410000076
  Out: 2001:dbf8:5::2/7214 --> 2001:dbf8:5::2/323;icmp6, If: .local..0, Pkts: 1,
Bytes: 104, CP Session ID: 410000076
Session ID: 410000068, Policy name: default-policy-00/2, Timeout: 2, Valid
  In: 2001:dbf8::6:2/4 --> 2001:dbf8:5::2/7214;icmp6, If: ge-7/1/0.0, Pkts: 1,
Bytes: 104, CP Session ID: 410000077
  Out: 2001:dbf8:5::2/7214 --> 2001:dbf8::6:2/4;icmp6, If: .local..0, Pkts: 1,
Bytes: 104, CP Session ID: 410000077
Total sessions: 2
```

Which statement is true about the output shown in the exhibit?
* The SRX Series device is configured with default security forwarding options.
* The SRX Series device is configured with packet-based IPv6 forwarding options.
* The SRX Series device is configured with flow-based IPv6 forwarding options.
* The SRX Series device is configured to disable IPv6 packet forwarding.

NEW QUESTION 51

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 52

According to the log shown in the exhibit, you notice the IPsec session is not establishing.

What is the reason for this behavior?
* Mismatched proxy ID
* Mismatched peer ID
* Mismatched preshared key
* Incorrect peer address.

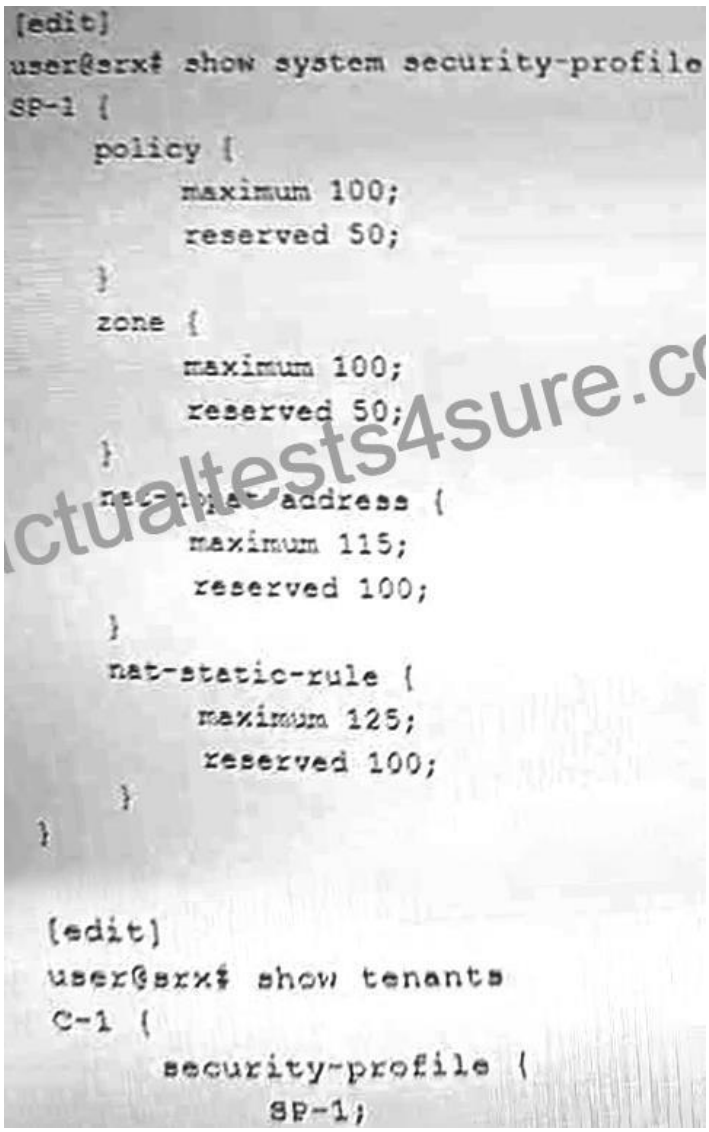
https://www.juniper.net/documentation/en_US/release-independent/nce/topics/example/policy-based-vpn-using-j-series-srxseries-device-configuring.html

NEW QUESTION 53

You are connecting two remote sites to your corporate headquarters site.You must ensure that all traffic is secured and sent directly between sites In this scenario, which VPN should be used?
* IPsec ADVPN
* hub-and-spoke IPsec VPN
* Layer 2 VPN
* full mesh Layer 3 VPN with EBGP

NEW QUESTION 54

Exhibit.



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

* The c-1 TSYS has a reservation for the security flow resource.
* The c-1 TSYS can use security flow resources up to the system maximum.
* The c-1 TSYS cannot use any security flow resources.
* The c-1 TSYS has no reservation for the security flow resource.

The system security profile named sp-1 has designated resources for policies and zones with a maximum of 100 and a reservation of 50 each. For NAT with no port address translation (nat-nopat- address), there is a maximum of 115 and a reservation of 100, and for static NAT rules (nat-static-rule), there is a maximum of 125 with 100 reserved.

When considering tenant systems, the profile applied (sp-1) will dictate the resources available to the tenant system named c-1.

The c-1 TSYS has a reservation for the security flow resource. – This would be true if the ‘security flow resource’ refers to policies and zones since there are reservations made in the profile sp-1.

The c-1 TSYS can use security flow resources up to the system maximum. – This is generally true for any tenant system unless there are explicit limits set that are lower than the system maximum.

NEW QUESTION 55

your company wants to take your juniper ATP appliance into private mode. You must give them a list of impacted features for this request.

Which two features are impacted in this scenario? (Choose two)
* False Positive Reporting
* Threat Progression Monitoring
* GSS Telemetry
* Cyber Kill Chain mapping

Your company wants to take your Juniper ATP Appliance into private mode. You must give them a list of impacted features for this request.

The two features that are impacted in this scenario are:

A) False Positive Reporting. False Positive Reporting is a feature that allows you to report false positive detections to Juniper Networks for analysis and improvement. False Positive Reporting requires an Internet connection to send the reports to Juniper Networks. If you take your Juniper ATP Appliance into private mode, False Positive Reporting will be disabled and you will not be able to report false positives1.

C) GSS Telemetry. GSS Telemetry is a feature that allows you to send anonymized threat data to Juniper Networks for analysis and improvement. GSS Telemetry requires an Internet connection to send the data to Juniper Networks. If you take your Juniper ATP Appliance into private mode, GSS Telemetry will be disabled and you will not be able to contribute to the threat intelligence community2.

The other options are incorrect because:

B) Threat Progression Monitoring. Threat Progression Monitoring is a feature that allows you to monitor the threat activity and progression across your network. Threat Progression Monitoring does not require an Internet connection and can be performed locally by the Juniper ATP Appliance. If you take your Juniper ATP Appliance into private mode, Threat Progression Monitoring will not be impacted and you will still be able to monitor the threat activity and progression3.

D) Cyber Kill Chain mapping. Cyber Kill Chain mapping is a feature that allows you to map the threat activity and progression to the stages of the Cyber Kill Chain framework. Cyber Kill Chain mapping does not require an Internet connection and can be performed locally by the Juniper ATP Appliance. If you take your Juniper ATP Appliance into private mode, Cyber Kill Chain mapping will not be impacted and you will still be able to map the threat activity and progression4.

Reference: False Positive Reporting GSS Telemetry

Threat Progression Monitoring Cyber Kill Chain Mapping

NEW QUESTION 56

You are required to secure a network against malware. You must ensure that in the event that a compromised host is identified within the network.

In this scenario after a threat has been identified, which two components are responsible for enforcing MAC-level infected host?
* SRX Series device
* Juniper ATP Appliance
* Policy Enforcer

* EX Series device

You are required to secure a network against malware. You must ensure that in the event that a compromised host is identified within the network, the host is isolated from the rest of the network.

In this scenario, after a threat has been identified, the two components that are responsible for enforcing MAC-level infected host are:

C) Policy Enforcer. Policy Enforcer is a software solution that integrates with Juniper ATP Cloud and Juniper ATP Appliance to provide automated threat remediation across the network. Policy Enforcer can receive threat intelligence feeds from Juniper ATP Cloud or Juniper ATP Appliance and apply them to the security policies on the SRX Series devices and the EX Series devices. Policy Enforcer can also enforce MAC-level infected host, which is a feature that allows you to quarantine a compromised host by blocking its MAC address on the switch port. Policy Enforcer can communicate with the EX Series devices and instruct them to apply the MAC-level infected host policy to the infected host1.

D) EX Series device. EX Series devices are Ethernet switches that can provide Layer 2 and Layer 3 switching capabilities and security features. EX Series devices can integrate with Policy Enforcer and Juniper ATP Cloud or Juniper ATP Appliance to provide automated threat remediation across the network. EX Series devices can support MAC-level infected host, which is a feature that allows them to quarantine a compromised host by blocking its MAC address on the switch port. EX Series devices can receive instructions from Policy Enforcer and apply the MAC-level infected host policy to the infected host2.

The other options are incorrect because:

A) SRX Series device. SRX Series devices are high-performance firewalls that can provide Layer 3 and Layer 4 security features and integrate with Juniper ATP Cloud or Juniper ATP Appliance to provide advanced threat prevention. SRX Series devices can receive threat intelligence feeds from Juniper ATP Cloud or Juniper ATP Appliance and apply them to the security policies. However, SRX Series devices cannot enforce MAC-level infected host, which is a feature that requires Layer 2 switching capabilities and is supported by EX Series devices3.

B) Juniper ATP Appliance. Juniper ATP Appliance is a hardware solution that provides advanced threat prevention by detecting and blocking malware, ransomware, and other cyberattacks. Juniper ATP Appliance can analyze the network traffic and identify the compromised hosts based on their behavior and communication patterns. Juniper ATP Appliance can also send threat intelligence feeds to Policy Enforcer and SRX Series devices to enable automated threat remediation across the network. However, Juniper ATP Appliance cannot enforce MAC-level infected host, which is a feature that requires Layer 2 switching capabilities and is supported by EX Series devices.

Reference: Policy Enforcer Overview EX Series Switches Overview

SRX Series Services Gateways Overview [Juniper ATP Appliance Overview]

NEW QUESTION 57

you are connecting two remote sites to your corporate headquarters site. You must ensure that traffic passes corporate headquarter.

* In this scenario, which VPN should be used?
* full mesh IPsec VPNs with tunnels between all sites
* a full mesh Layer 3 VPN with the BGP route reflector behind the corporate firewall device
* a Layer 3 VPN with the corporate firewall acting as the hub device
* hub-and-spoke IPsec VPN with the corporate firewall acting as the hub device

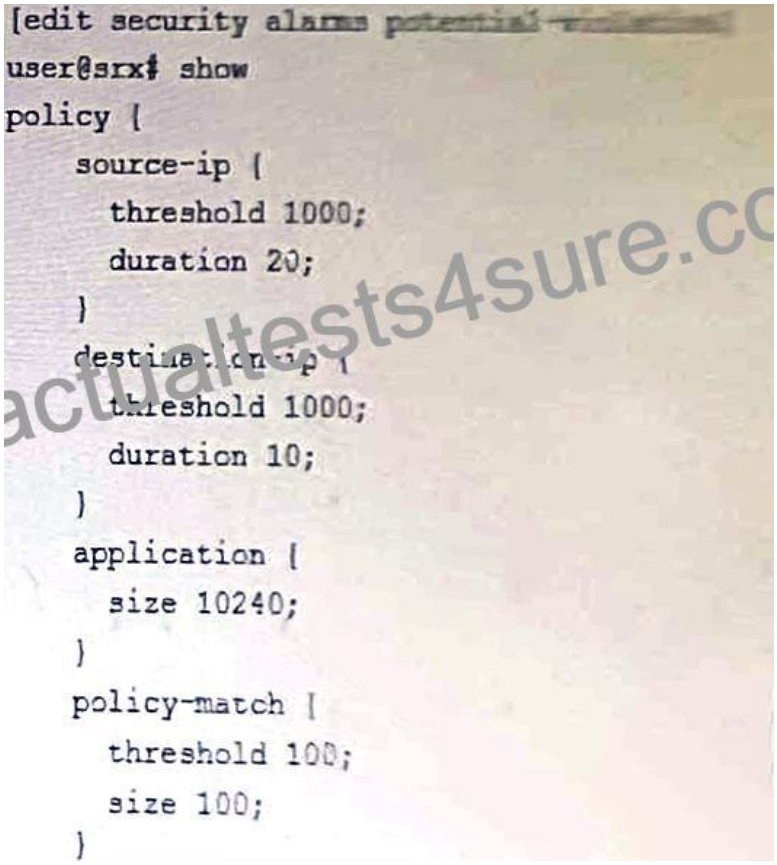
The most appropriate VPN topology when you need to ensure that all traffic from remote sites passes through the corporate headquarters would be a hub-and-spoke model. In this model, the corporate headquarters acts as the hub, and all remote sites (spokes) connect to it. This ensures that inter-site traffic goes through the headquarters, which can be important for security policy

enforcement, logging, or other centralized services.

Hub-and-spoke IPsec VPN with the corporate firewall acting as the hub device – This setup will ensure that all traffic from the remote sites is routed through the corporate headquarters, allowing centralized control and inspection of the traffic.

NEW QUESTION 58

Refer to the exhibit,



which two potential violations will generate alarm ? (Choose Two)
* the number of policy violations by a source network identifier
* the ratio of policy violation traffic compared to accepted traffic.
* the number of policy violation by a destination TCP port
* the number of policy violation to an application within a specified period

The exhibit shows a security policy configuration with a threshold of 1000 policy violations by a source network identifier and a threshold of 10 policy violations to an application within a specified period. If either of these thresholds are exceeded, an alarm will be generated. Therefore, the correct answer is A and D. The other options are incorrect because:

B) The ratio of policy violation traffic compared to accepted traffic is not a criterion for triggering an alarm.

The security policy configuration does not specify any ratio or percentage of policy violation traffic that would cause an alarm.

C) The number of policy violation by a destination TCP port is also not a criterion for triggering an alarm.

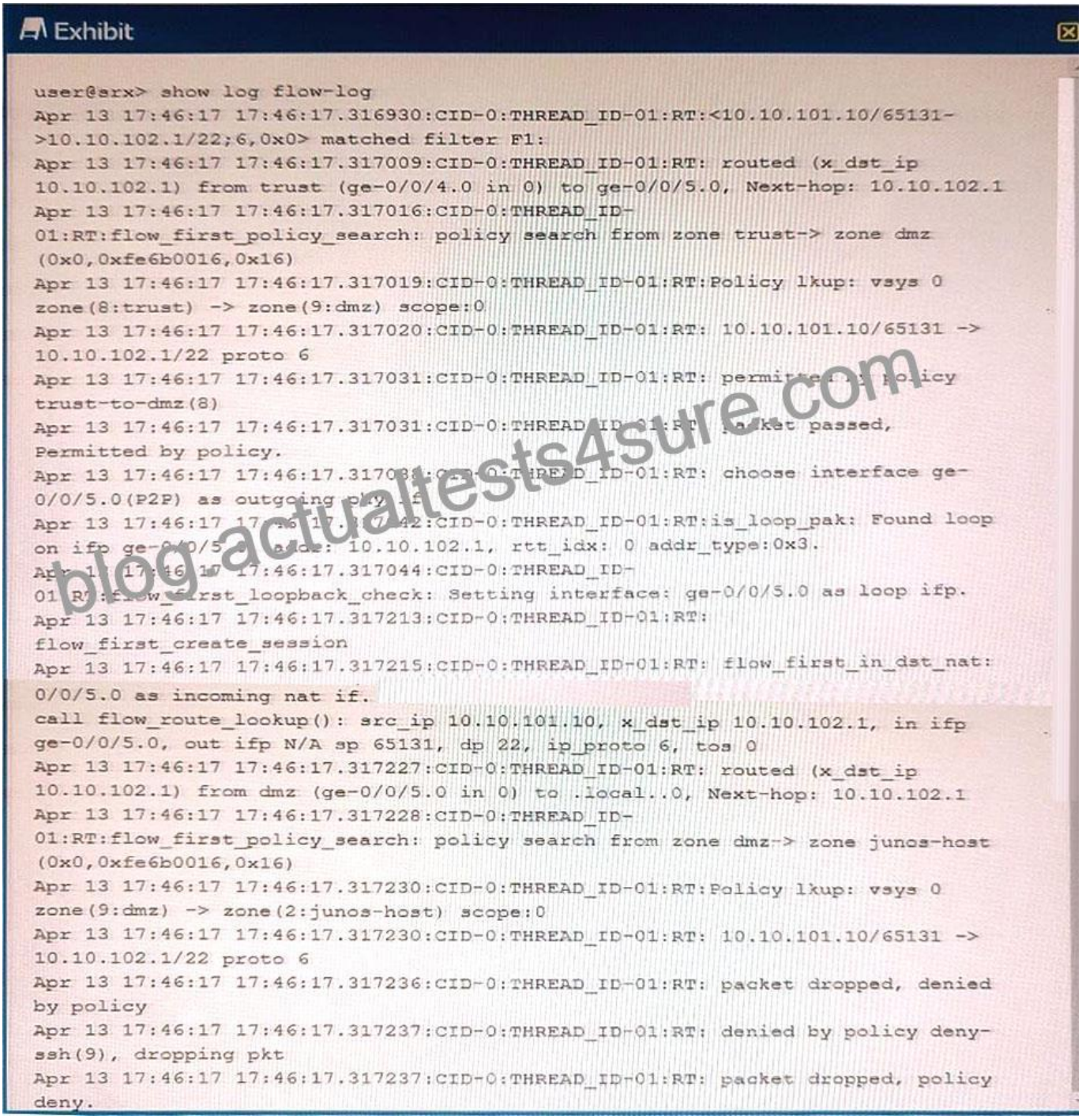
The security policy configuration does not specify any threshold or duration for policy violation by a destination TCP port.

Reference: policy (Security Alarms)

Monitoring Security Policy Violations

NEW QUESTION 59

Exhibit



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

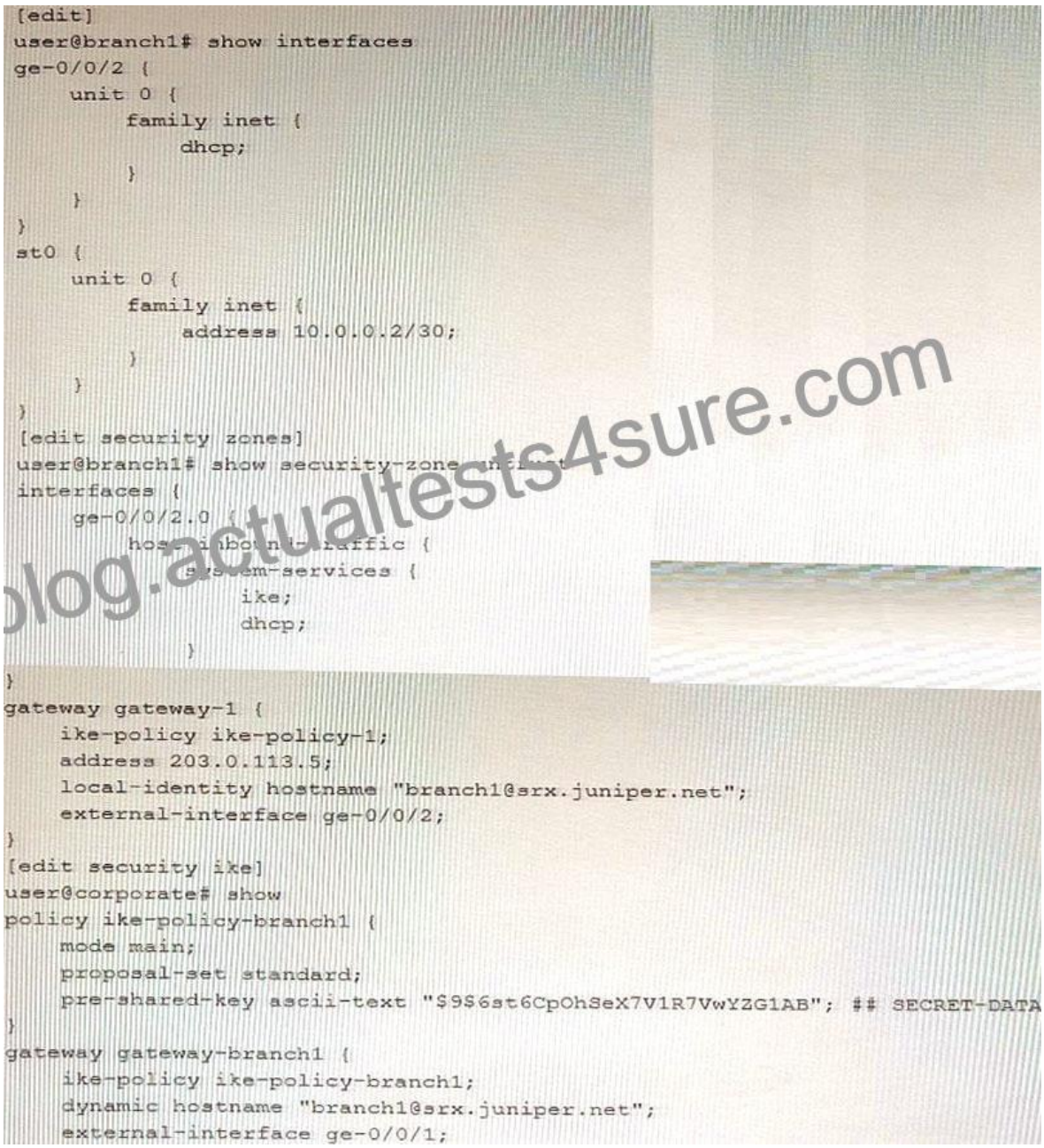
Referring to the exhibit, which two statements are correct? (Choose two.)
* This is the last packet in the session.
* The SRX Series device is performing both source and destination NAT on this session.
* This is the first packet in the session.
* The SRX Series device is performing only source NAT on this session.

NEW QUESTION 60

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 61

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.

* Add multipoint to the st0.0 interface configuration on the branch1 device.
* Change the IKE proposal-set to compatible on the branch1 and corporate devices.
* Change the local identity to inet advpn on the branch1 device.
* Change the IKE mode to aggressive on the branch1 and corporate devices.

NEW QUESTION 62

You are requested to enroll an SRX Series device with Juniper ATP Cloud.

Which statement is correct in this scenario?
* If a device is already enrolled in a realm and you enroll it in a new realm, the device data or configuration information is propagated to the new realm.
* The only way to enroll an SRX Series device is to interact with the Juniper ATP Cloud Web portal.
* When the license expires, the SRX Series device is disenrolled from Juniper ATP Cloud without a grace period
* Juniper ATP Cloud uses a Junos OS op script to help you configure your SRX Series device to connect to the Juniper ATP Cloud service.

NEW QUESTION 63

You have a webserver and a DNS server residing in the same internal DMZ subnet. The public Static NAT addresses for the servers are in the same subnet as the SRX Series devices internet-facing interface. You implement DNS doctoring to ensure remote users can access the webserver.

Which two statements are true in this scenario? (Choose two.)
* The DNS doctoring ALG is not enabled by default.
* The Proxy ARP feature must be configured.
* The DNS doctoring ALG is enabled by default.
* The DNS CNAME record is translated.

NEW QUESTION 64

Which two types of source NAT translations are supported in this scenario? (Choose two.)
* translation of IPv4 hosts to IPv6 hosts with or without port address translation
* translation of one IPv4 subnet to one IPv6 subnet with port address translation
* translation of one IPv6 subnet to another IPv6 subnet without port address translation
* translation of one IPv6 subnet to another IPv6 subnet with port address translation

NEW QUESTION 65

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

Which two steps accomplish this goal? (Choose two.)
* Configure Microsoft Azure as the service provider (SP).
* Configure Microsoft Azure as the identity provider (IdP).
* Configure Juniper ATP Cloud as the service provider (SP).
* Configure Juniper ATP Cloud as the identity provider (IdP).

NEW QUESTION 66

In an effort to reduce client-server latency transparent mode was enabled an SRX series device.

Which two types of traffic will be permitted in this scenario? (Choose Two)
* ARP
* Layer 2 non-IP multicast
* BGP
* IPsec

To answer this question, you need to know what transparent mode is and what types of traffic it permits.

Transparent mode is a mode of operation for SRX Series devices that provides Layer 2 bridging capabilities with full security services. In transparent mode, the SRX Series device acts as a bridge between two network segments and inspects the packets without modifying the source or destination information in the IP packet header. The SRX Series device does not have an IP address in transparent mode, except for the management interface1.

Therefore, the types of traffic that will be permitted in transparent mode are:

A) ARP (Address Resolution Protocol) traffic. ARP is a protocol that maps IP addresses to MAC addresses. ARP traffic is a type of Layer 2 traffic that does not require an IP address on the SRX Series device. ARP traffic is permitted in transparent mode to allow the SRX Series device to learn the MAC addresses of the hosts on the bridged network segments2.

B) Layer 2 non-IP multicast traffic. Layer 2 non-IP multicast traffic is a type of traffic that uses MAC addresses to send data to multiple destinations. Layer 2 non-IP multicast traffic does not require an IP address on the SRX Series device. Layer 2 non-IP multicast traffic is permitted in transparent mode to allow the SRX Series device to forward data to the appropriate destinations on the bridged network segments3.

The other options are incorrect because:

C) BGP (Border Gateway Protocol) traffic. BGP is a protocol that exchanges routing information between autonomous systems. BGP traffic is a type of Layer 3 traffic that requires an IP address on the SRX Series device. BGP traffic is not permitted in transparent mode, because the SRX Series device does not have an IP address in transparent mode, except for the management interface1.

D) IPsec (Internet Protocol Security) traffic. IPsec is a protocol that provides security and encryption for IP packets. IPsec traffic is a type of Layer 3 traffic that requires an IP address on the SRX Series device.

IPsec traffic is not permitted in transparent mode, because the SRX Series device does not have an IP address in transparent mode, except for the management interface1.

Reference: Transparent Mode Overview

ARP Support in Transparent Mode

Layer 2 Non-IP Multicast Traffic Support in Transparent Mode

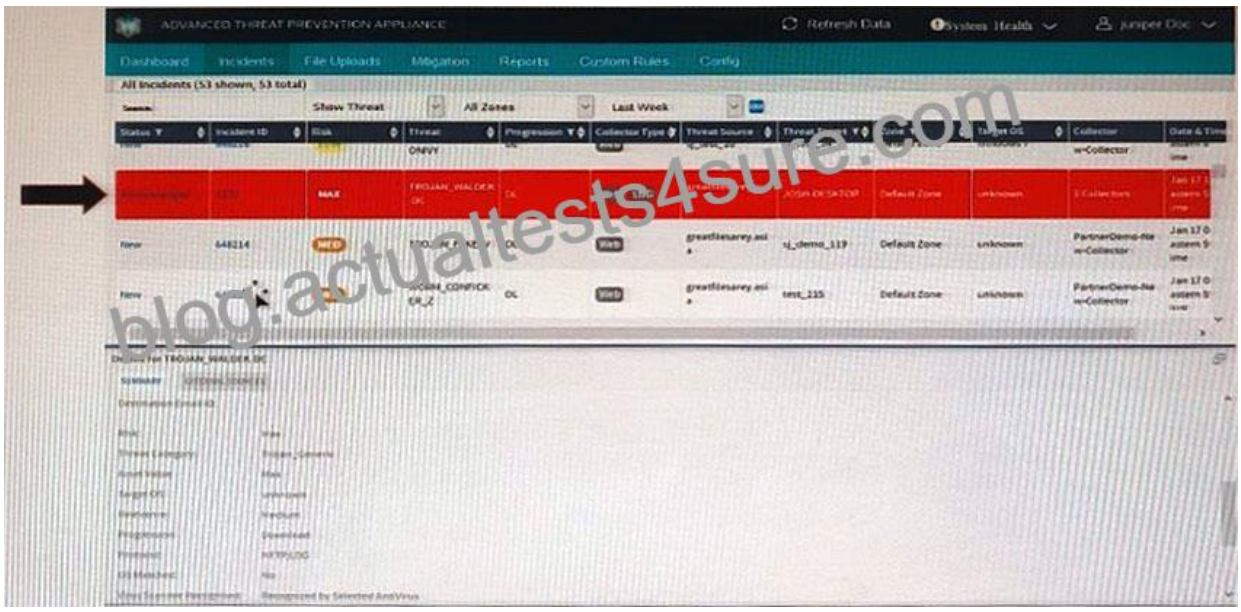
NEW QUESTION 67

You want to enroll an SRX Series device with Juniper ATP Appliance. There is a firewall device in the path between the devices.

In this scenario, which port should be opened in the firewall device?
* 8080
* 443
* 80
* 22

NEW QUESTION 68

Exhibit

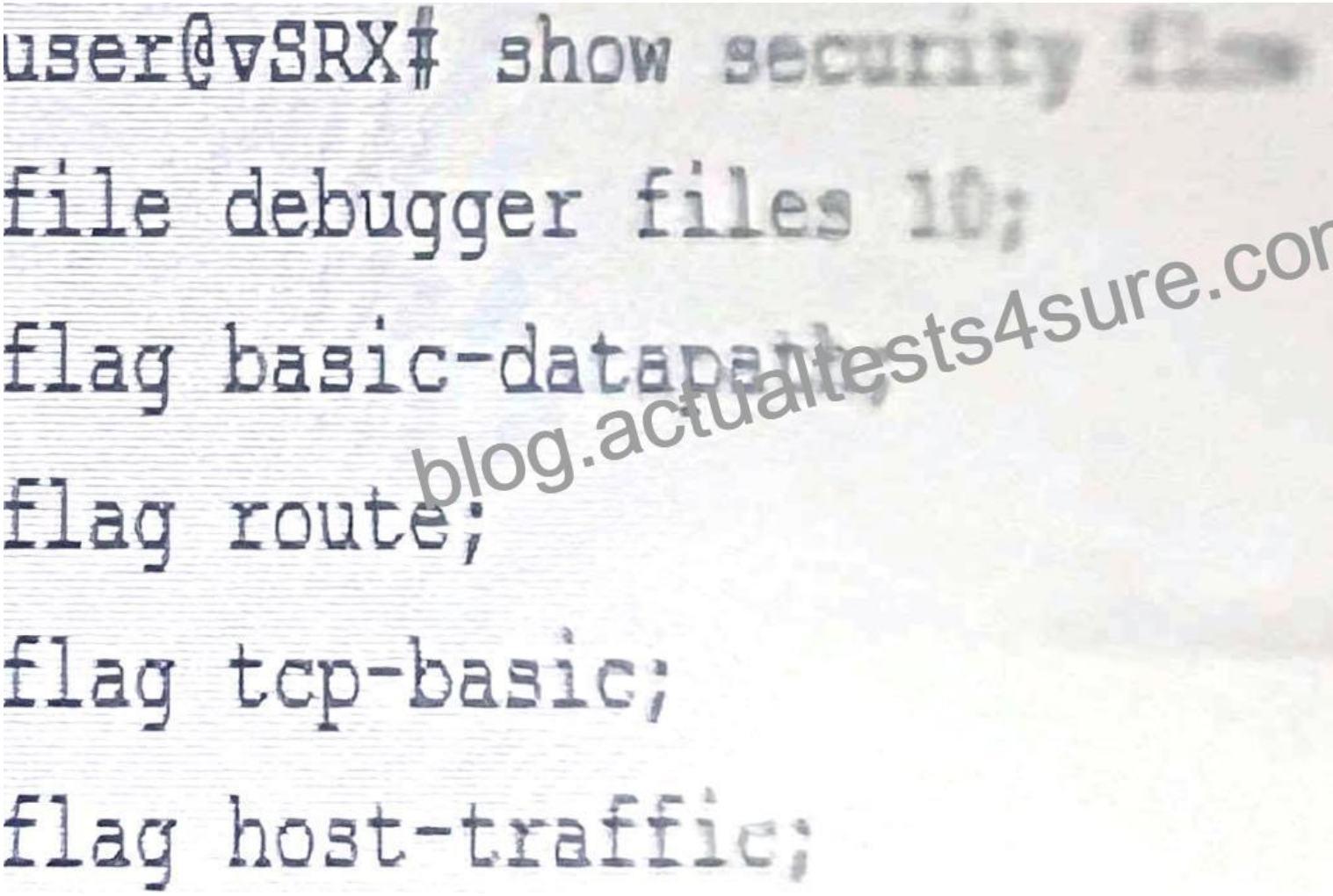


The highlighted incident (arrow) shown in the exhibit shows a progression level of “Download” in the kill chain.

What are two appropriate mitigation actions for the selected incident? (Choose two.)
* Immediate response required: Block malware IP addresses (download server or CnC server)
* Immediate response required: Wipe infected endpoint hosts.
* Immediate response required: Deploy IVP integration (if configured) to confirm if the endpoint has executed the malware and is infected.
* Not an urgent action: Use IVP to confirm if machine is infected.

NEW QUESTION 69

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.

Actualtests4sure just published the Juniper JN0-637 exam dumps!:
https://www.actualtests4sure.com/JN0-637-test-questions.html]