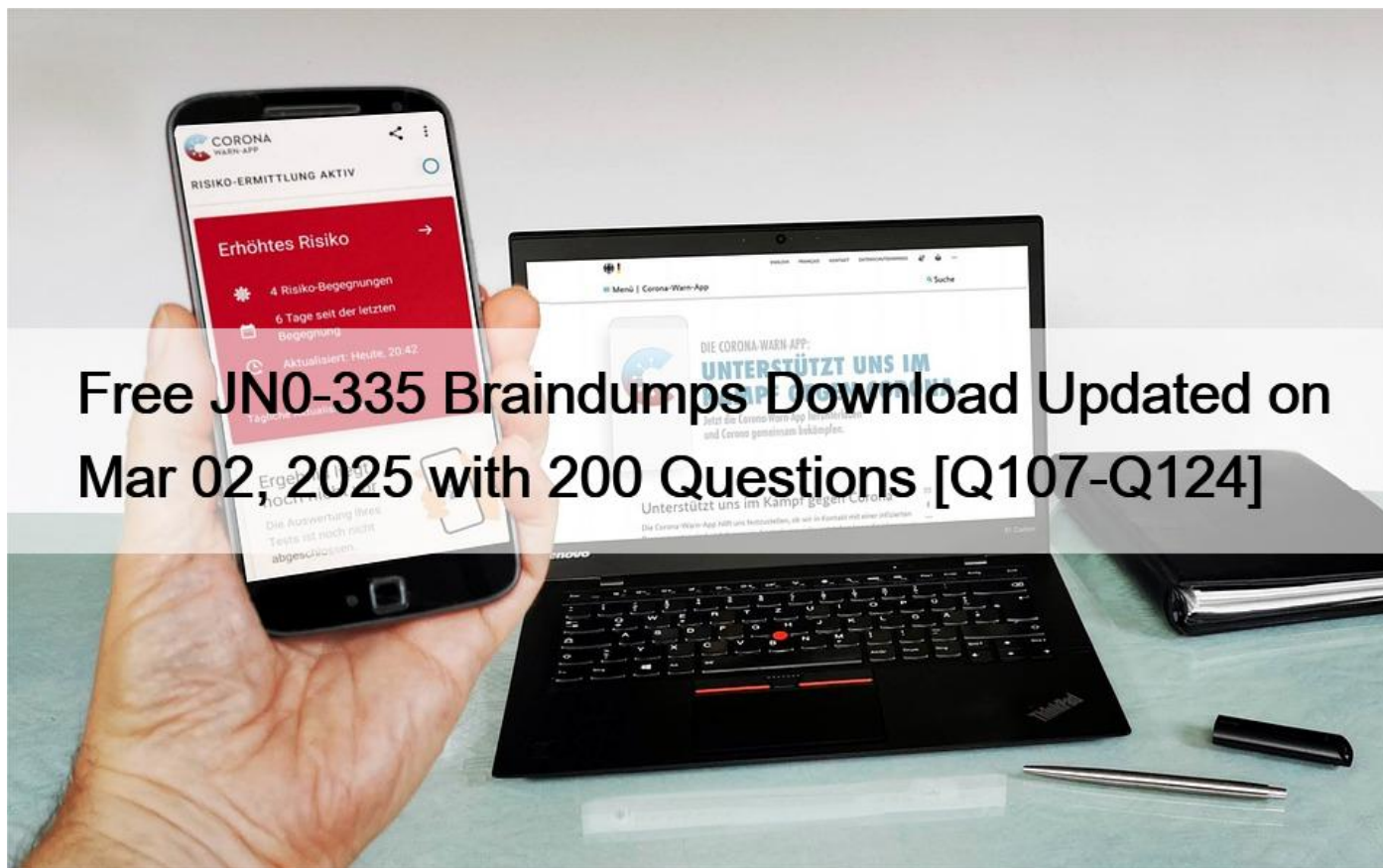


Free JN0-335 Braindumps Download Updated on Mar 02, 2025 with 200 Questions [Q107-Q124]



Free JN0-335 Braindumps Download Updated on Mar 02, 2025 with 200 Questions [Q107-Q124]

Free JN0-335 Braindumps Download Updated on Mar 02, 2025 with 200 Questions
Juniper JN0-335 Exam Practice Test Questions

The JN0-335 certification exam covers a wide range of topics, including Junos Security Architecture, Security Policies, Symmetric and Asymmetric Encryption, Next-Generation Security Services, Junos Layer 2 and Layer 3 VPNs, and Junos IPSec VPNs. JN0-335 exam aims to test the candidate's understanding of Juniper Networks security products and their ability to configure and manage these products effectively.

QUESTION 107

Click the Exhibit button.

```
user@srx> show security flow session
Session ID: 19068, Policy name: trust-to-untrust, Timeout: 1800, Valid
Resource information : FTP ALG, 1, 0
  In: 172.20.104.10/58479 --> 172.18.1.2/21;tcp, Conn Tag: 0x0, If: ge-0/0/3.0,
Pkts: 42, Bytes: 1796,
  Out: 172.18.1.2/21 --> 172.20.104.10/58479;tcp, Conn Tag: 0x0, If: ge-0/0/4.0,
Pkts: 43, Bytes: 2739,
```

Which two statements are true about the session shown in the exhibit? (Choose two.)

- * Two security policies are required for bidirectional traffic flow.
- * The ALG was enabled by manual configuration.
- * The ALG was enabled by default.
- * One security policy is required for bidirectional traffic flow.

QUESTION 108

What is the default timeout period for a TCP session in the session table of a Junos security device?

- * 1 minute
- * 60 minutes
- * 15 minutes
- * 30 minutes

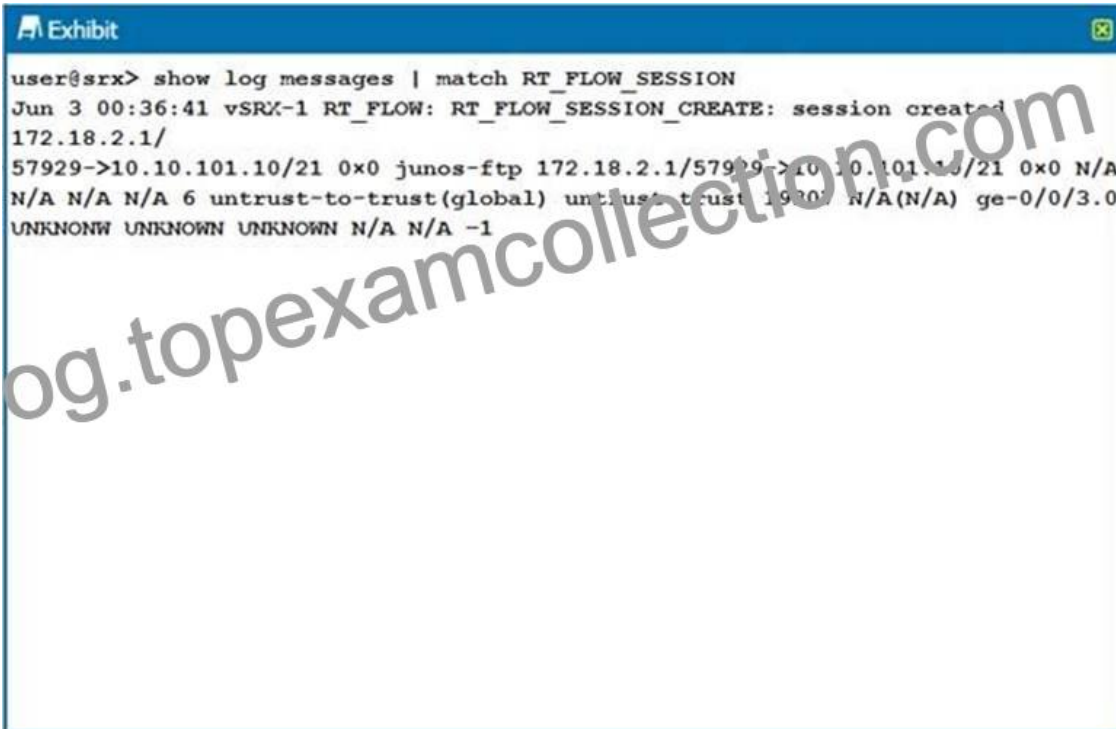
QUESTION 109

Which two statements describe how rules are used with Juniper Secure Analytics? (Choose two.)

- * When a rule is triggered, JSA can respond by sending an e-mail to JSA administrators.
- * Rules are defined on Junos Space Security Director, and then pushed to JSA log collectors.
- * A rule defines matching criteria and actions that should be taken when an events matches the rule.
- * When a rule is triggered, JSA can respond by blocking all traffic from a specific source address.

QUESTION 110

Click the Exhibit button.



```
user@srx> show log messages | match RT_FLOW_SESSION
Jun 3 00:36:41 vSRX-1 RT_FLOW: RT_FLOW_SESSION_CREATE: session created
172.18.2.1/
57929->10.10.101.10/21 0x0 junos-ftp 172.18.2.1/57929->10.10.101.10/21 0x0 N/A
N/A N/A N/A 6 untrust-to-trust(global) untrust trust 1930 N/A(N/A) ge-0/0/3.0
UNKNOWN UNKNOWN UNKNOWN N/A N/A -1
```

The output shown in the exhibit is displayed in which format?

- * syslog
- * sd-syslog
- * binary
- * WELF

QUESTION 111

Your JIMS server is unable to view event logs.

Which two actions would you take to solve this issue? (Choose two.)

- * Enable the correct host-inbound-traffic rules on the SRX Series devices.
- * Enable remote event log management within Windows Firewall on the necessary Exchange servers.
- * Enable remote event log management within Windows Firewall on the necessary domain controllers.
- * Enable remote event log management within Windows Firewall on the JIMS server.

If your JIMS server is unable to view event logs, two actions that you would take to solve this issue are:

Enable remote event log management within Windows Firewall on the necessary Exchange servers: JIMS (Juniper Identity Management Service) is a Windows service that collects user, device, and group information from Active Directory domains or syslog sources and provides it to SRX Series devices for identity-based security policies. JIMS relies on the event logs generated by the domain controllers and Exchange servers to track user logins, logouts, and IP address changes. If the Windows Firewall on the Exchange servers blocks the remote event log management, JIMS cannot access the event logs and obtain the user identity information. Therefore, you need to enable remote event log management within Windows Firewall on the Exchange servers that are configured as event sources in JIMS.

Enable remote event log management within Windows Firewall on the necessary domain controllers: Similarly, if the Windows Firewall on the domain controllers blocks the remote event log management, JIMS cannot access the event logs and obtain the user identity information. Therefore, you need to enable remote event log management within Windows Firewall on the domain controllers that are configured as event sources in JIMS.

QUESTION 112

Which two statements about the DNS ALG are correct? (Choose two.)

- * The DNS ALG supports DDNS.
- * The DNS ALG supports VPN tunnels.
- * The DNS ALG performs DNS doctoring.
- * The DNS ALG does not support NAT.

The DNS ALG is an application layer gateway that handles data associated with locating and translating domain names into IP addresses. It runs on port 53 and monitors DNS query and reply packets. Two statements about the DNS ALG that are correct are:

The DNS ALG supports DDNS: DDNS is Dynamic DNS, which is a method of updating DNS records in real time to reflect changes in network configurations or hostnames. The DNS ALG can process DDNS messages differently from DNS messages and perform address translation in the query part of the message.

The DNS ALG performs DNS doctoring: DNS doctoring is a technique of modifying the DNS reply packets to replace the original IP addresses with translated IP addresses that are suitable for the destination network. This allows the clients to access servers that are located behind NAT devices or in different networks.

QUESTION 113

When a security policy is modified, which statement is correct about the default behavior for active sessions allowed by that policy?

- * The active sessions allowed by the policy will be dropped.
- * Only policy changes that involve modification of the action field will cause the active sessions affected by the change to be dropped.
- * Only policy changes that involve modification of the application will cause the active sessions affected by the change to be dropped.
- * The active sessions allowed by the policy will continue unchanged.

QUESTION 114

Referring to the exhibit which statement is true?

```
user@srx> show security flow session
Session ID: 61524, Policy name: Internet-access/9,
  In: 10.10.12.37/37466 --> 10.111.111.254/80;tcp,
0/0/0.0, Pkts: 3, Bytes: 1023,
  Out: 10.111.111.254/80 --> 10.10.12.37/9241,tcp,
0/0/1/0, Pkts: 0, Bytes: 0,
user@srx> show services application-identification
Application System Cache Configurations:
  application-cache: on
    Cache lookup for security-services: off
    Cache lookup for miscellaneous-services: on
  cache-entry-timeout: 3600 seconds
pic: 0/0
Logical system name: root-logical-system
```

- * SSL proxy functions will ignore the session.
- * SSL proxy leverages post-match results.
- * SSL proxy must wait for return traffic for the final match to occur.
- * SSL proxy leverages pre-match result

QUESTION 115

The output shown in the exhibit is displayed in which format?

```
Exhibit
user@srx> show log messages | match RT_FLOW_SESSION
Jun 3 00:36:41 vSRX-1 RT_FLOW: RT_FLOW_SESSION_CREATE: session created
172.18.2.1/
57929->10.10.101.10/21 0x0 junos-ftp 172.18.2.1/57929->10.10.101.10/21 0x0 N/A
N/A N/A N/A 6 untrust-to-trust(global) untrust-trust 3307 N/A(N/A) ge-0/0/3.0
UNKNOWN UNKNOWN UNKNOWN N/A N/A -1
```

- * syslog
- * sd-syslog
- * binary
- * WELF

QUESTION 116

You are experiencing excessive packet loss on one of your two WAN links route traffic from the degraded link to the working link
Which AppSecure component would you use to accomplish this task?

- * AppFW
- * AppQoE
- * AppQoS
- * APBR

APBR (Application Path-Based Routing) is an AppSecure component which can be used to route traffic from the degraded link to the working link in order to reduce packet loss. APBR is a policy-based routing solution that allows you to configure rules to direct traffic to the most appropriate path, based on application, user, or network metrics.

QUESTION 117

What are two examples of RTOs? (Choose two.)

- * IPsec SA entries
- * session table entries
- * fabric link probes
- * control link heartbeats

QUESTION 118

Which two statements about SRX chassis clustering are correct? (Choose two.)

- * SRX chassis clustering supports active/passive and active/active for the data plane.
- * SRX chassis clustering only supports active/passive for the data plane.
- * SRX chassis clustering supports active/passive for the control plane.
- * SRX chassis clustering supports active/active for the control plane.

SRX chassis clustering supports active/passive and active/active for the data plane. In an active/active configuration, both cluster members process and forward traffic, which increases throughput and provides redundancy. For the control plane, SRX chassis clustering supports active/active, meaning that both cluster members can process and forward control traffic, providing redundancy and improved scalability

QUESTION 119

You are asked to create an IPS-exempt rule base to eliminate false positives from happening.

Which two configuration parameters are available to exclude traffic from being examined?

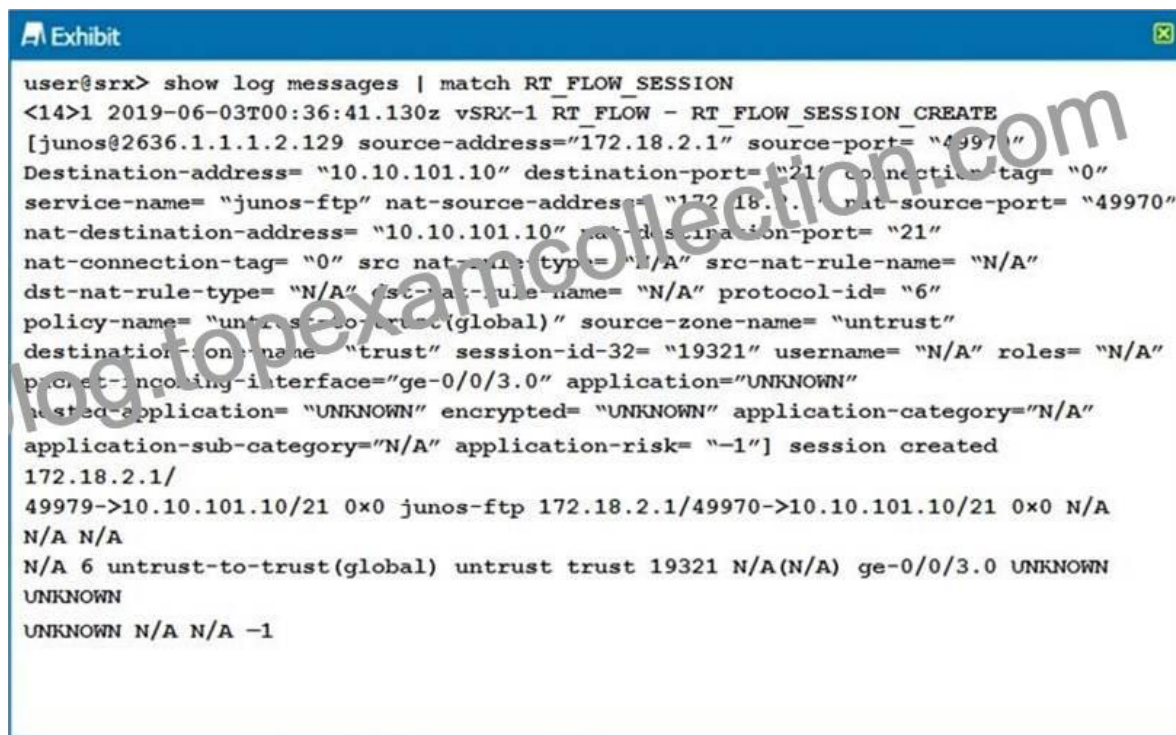
(Choose two.)

- * source port
- * source IP address
- * destination IP address
- * destination port

To exclude traffic from being examined by IPS, you can use the source IP address and/or destination port as criteria for the exemption. This is achieved by configuring an IPS-exempt rule base that includes specific exemption rules based on these criteria.

QUESTION 120

Click the Exhibit button.



```
user@srx> show log messages | match RT_FLOW_SESSION
<14>1 2019-06-03T00:36:41.130z vSRX-1 RT_FLOW - RT_FLOW_SESSION_CREATE
[junos@2636.1.1.1.2.129 source-address="172.18.2.1" source-port= "49970"
Destination-address= "10.10.101.10" destination-port= "21" connection-tag= "0"
service-name= "junos-ftp" nat-source-address= "172.18.2.1" nat-source-port= "49970"
nat-destination-address= "10.10.101.10" nat-destination-port= "21"
nat-connection-tag= "0" src-nat-rule-type= "N/A" src-nat-rule-name= "N/A"
dst-nat-rule-type= "N/A" dst-nat-rule-name= "N/A" protocol-id= "6"
policy-name= "untrust-to-trust(global)" source-zone-name= "untrust"
destination-zone-name= "trust" session-id-32= "19321" username= "N/A" roles= "N/A"
protect-incoming-interface="ge-0/0/3.0" application="UNKNOWN"
trusted-application= "UNKNOWN" encrypted= "UNKNOWN" application-category="N/A"
application-sub-category="N/A" application-risk= "-1"] session created
172.18.2.1/
49979->10.10.101.10/21 0x0 junos-ftp 172.18.2.1/49970->10.10.101.10/21 0x0 N/A
N/A N/A
N/A 6 untrust-to-trust(global) untrust trust 19321 N/A(N/A) ge-0/0/3.0 UNKNOWN
UNKNOWN
UNKNOWN N/A N/A -1
```

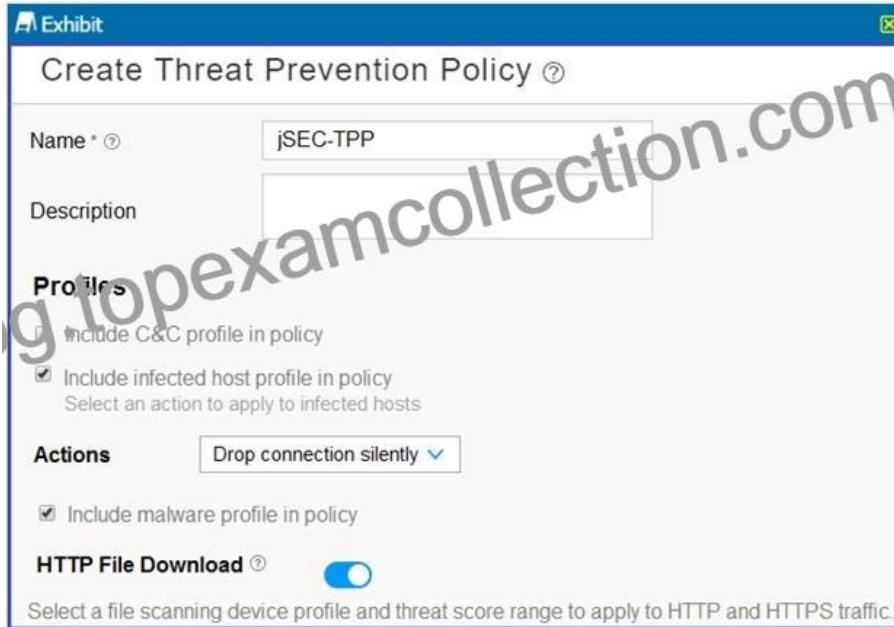
The output shown in the exhibit is displayed in which format?

- * syslog
- * WELF
- * binary

* sd-syslog

QUESTION 121

Referring to the exhibit, which statement is true?



- * Hosts are always able to communicate through the SRX Series device no matter the threat score assigned to them on the infected host feed.
- * Hosts are unable to communicate through the SRX Series device after being placed on the infected host feed with a high enough threat score.
- * Malicious HTTP file downloads are never blocked.
- * Malicious HTTP file downloads are always blocked.

QUESTION 122

Your network uses a remote e-mail server that is used to send and receive e-mails for your users.

In this scenario, what should you do to protect users from receiving malicious files through e-mail?

- * Deploy Sky ATP IMAP e-mail protection
- * Deploy Sky ATP MAPI e-mail protection
- * Deploy Sky ATP SMTP e-mail protection
- * Deploy Sky ATP POP3 e-mail protection

QUESTION 123

Which statement describes the AppTrack module in AppSecure?

- * The AppTrack module provides enforcement with the ability to block traffic, based on specific applications.
- * The AppTrack module provides control by the routing of traffic, based on the application.
- * The AppTrack module identifies the applications that are present in network traffic.
- * The AppTrack module provides visibility and volumetric reporting of application usage on the network.

QUESTION 124

What are two types of system logs that Junos generates? (Choose two.)

- * SQL log files
- * data plane logs
- * system core dump files
- * control plane logs

The two types of system logs that Junos generates are control plane logs and data plane logs.

Control plane logs are generated by the Junos operating system and contain system-level events such as system startup and shutdown, configuration changes, and system alarms. Data plane logs are generated by the network protocol processes and contain messages about the status of the network and its components, such as routing, firewall, NAT, and IPS. SQL log files and system core dump files are not types of system logs generated by Junos.

The JN0-335 exam is intended for professionals who have experience in networking and security. JN0-335 exam is ideal for those who are looking to advance their careers in the field of security. Security, Specialist (JNCIS-SEC) certification is also useful for network administrators, security engineers, and security consultants who want to validate their skills and knowledge in the field of security.

Updated Verified JN0-335 dumps Q&As - Pass Guarantee or Full Refund:

<https://www.topexamcollection.com/JN0-335-vce-collection.html>