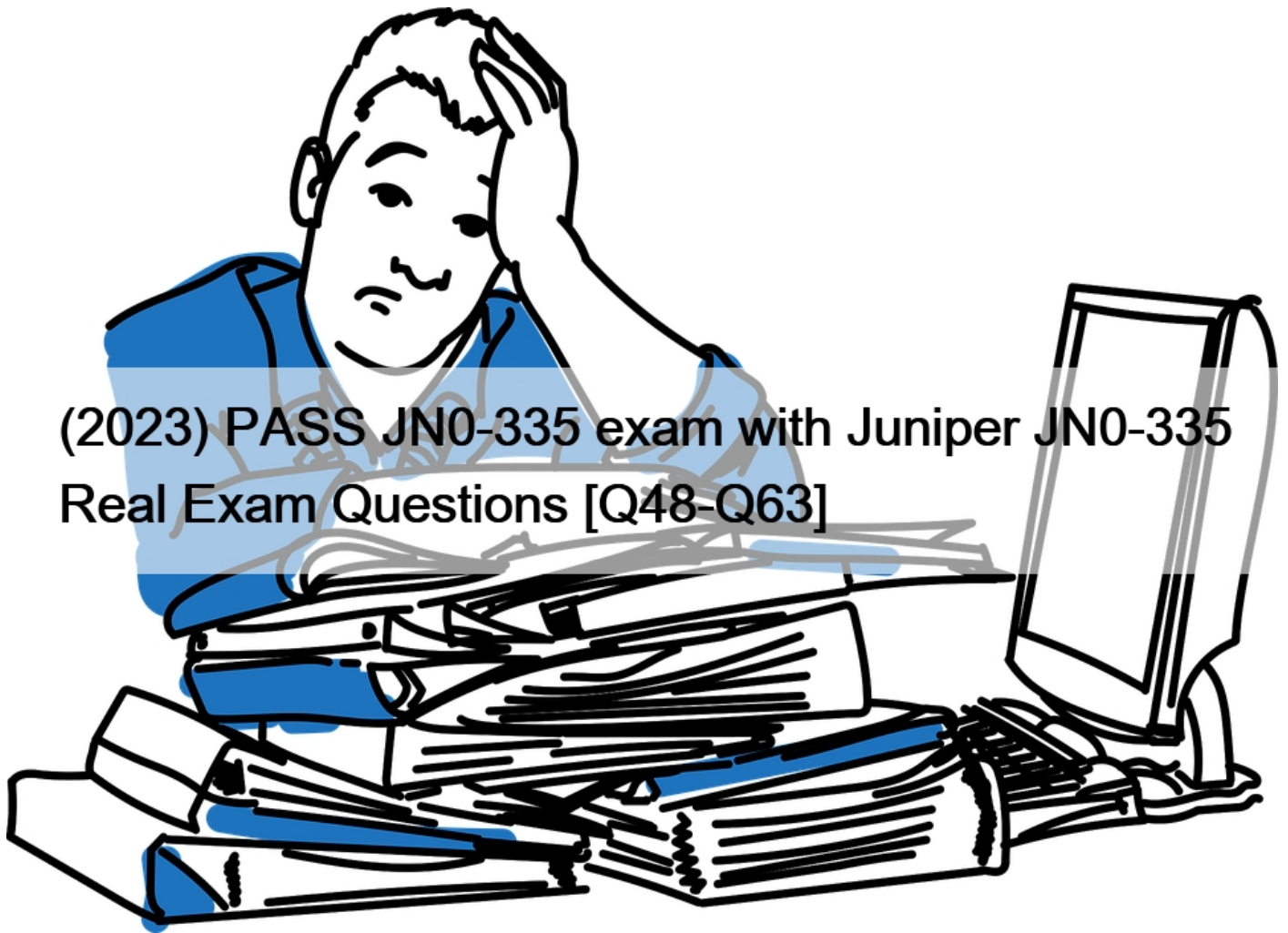


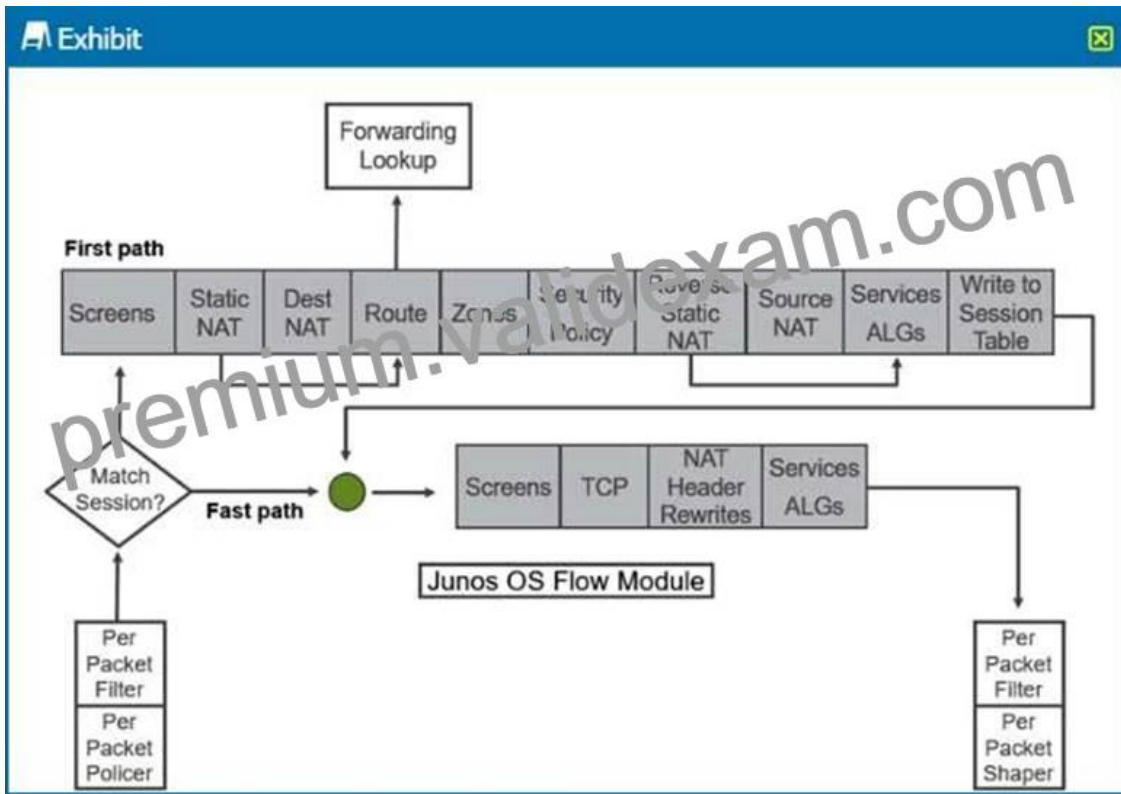
(2023) PASS JN0-335 exam with Juniper JN0-335 Real Exam Questions [Q48-Q63]



(2023) PASS JN0-335 exam with Juniper JN0-335 Real Exam Questions Real exam questions are provided for JNCIS-SEC tests, which can make sure you 100% pass

Juniper JN0-335 (Security, Specialist (JNCIS-SEC)) certification exam is designed for network security professionals who have intermediate knowledge of security technologies and Junos software for SRX Series devices. Security, Specialist (JNCIS-SEC) certification validates the candidates' understanding and skills in security technologies, security policies, VPNs, NAT, IPsec, and other security features.

NO.48 Click the Exhibit button.



Referring to the SRX Series flow module diagram shown in the exhibit, where is IDP/IPS processed?

- * Forwarding Lookup
- * Services ALGs
- * Screens
- * Security Policy

NO.49 Click the Exhibit button.

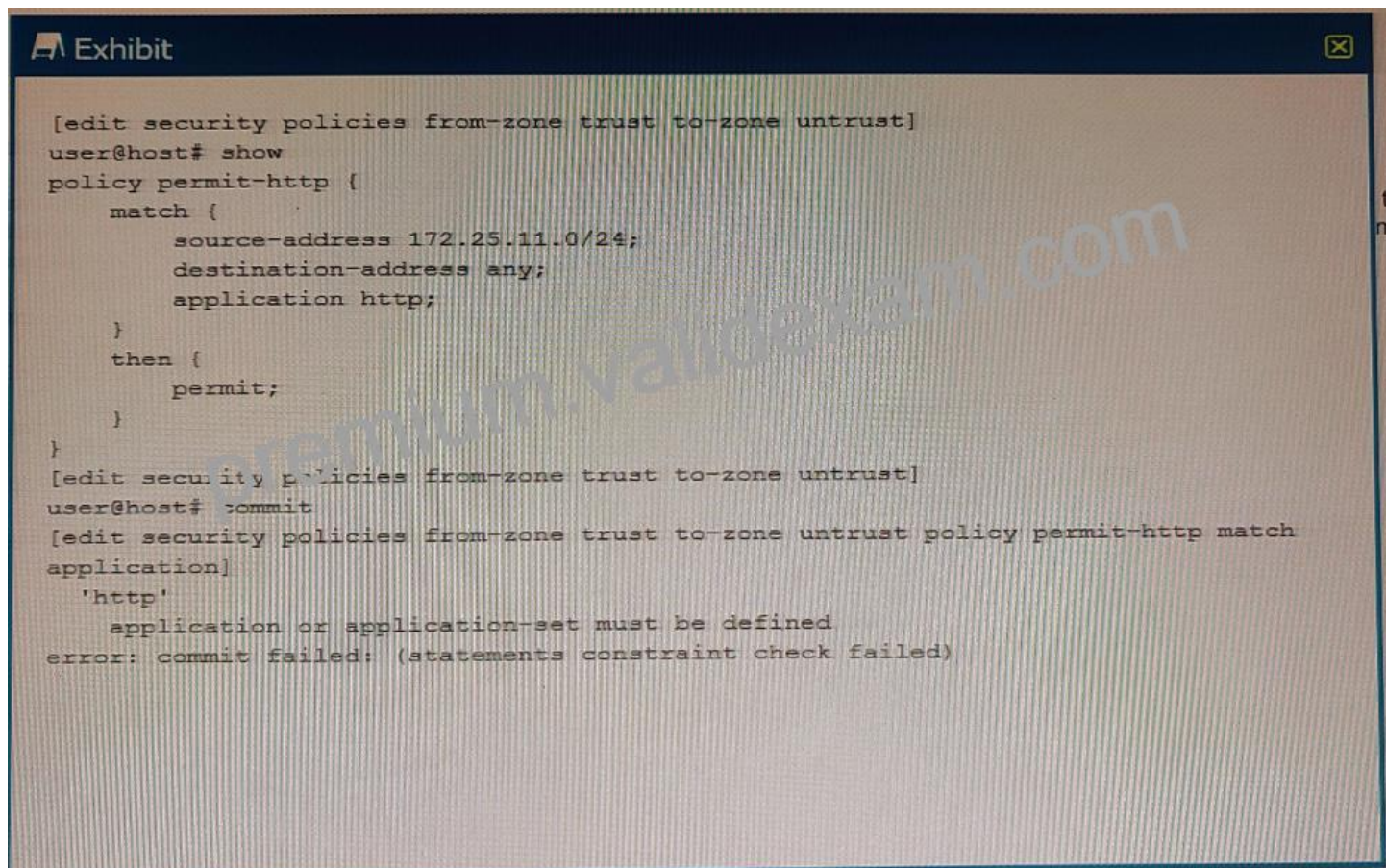
```
Exhibit
user@srx> show services user-identification identity-management status
Primary server :
  Address          : 172.25.11.130
  Port             : 443
  Connection method : HTTPS
  Connection status : Online
  Last received status message : Invalid client (400)
  Access token     : NULL
Secondary server :
  Address          : Not configured
```

You have configured your SRX Series device to receive authentication information from a JIMS server. However, the SRX is not receiving any authentication information.

Referring to the exhibit, how would you solve the problem?

- * Use the JIMS Administrator user interface to add the SRX device as client.
- * Generate an access token on the SRX device that matches the access token on the JIMS server.
- * Update the IP address of the JIMS server
- * Change the SRX configuration to connect to the JIMS server using HTTP.

NO.50 Exhibit



```
[edit security policies from-zone trust to-zone untrust]
user@host# show
policy permit-http {
  match {
    source-address 172.25.11.0/24;
    destination-address any;
    application http;
  }
  then {
    permit;
  }
}
[edit security policies from-zone trust to-zone untrust]
user@host# commit
[edit security policies from-zone trust to-zone untrust policy permit-http match
application]
'http'
  application or application-set must be defined
error: commit failed: (statements constraint check failed)
```

You are trying to create a security policy on your SRX Series device that permits HTTP traffic from your private 172.25.11.0/24 subnet to the Internet. You create a policy named permit-http between the trust and untrust zones that permits HTTP traffic. When you issue a commit command to apply the configuration changes, the commit fails with the error shown in the exhibit.

Which two actions would correct the error? (Choose two.)

- * Issue the rollback 1 command from the top of the configuration hierarchy and attempt the commit again.
- * Execute the Junos commit full command to override the error and apply the configuration.
- * Create a custom application named http at the [edit applications] hierarchy.
- * Modify the security policy to use the built-in Junos-http applications.

The error message indicates that the Junos-http application is not defined, so you need to either create a custom application or modify the security policy to use the built-in Junos-http application. Doing either of these will allow you to successfully commit the configuration.

NO.51 Which two statements about SRX Series device chassis clusters are true? (Choose two.)

- * Redundancy group 0 is only active on the cluster backup node.
- * Each chassis cluster member requires a unique cluster ID value.
- * Each chassis cluster member device can host active redundancy groups.
- * Chassis cluster member devices must be the same model.

1. Each chassis cluster member requires a unique cluster ID value: This statement is true. Each chassis cluster member must have a unique cluster ID assigned, which is used to identify each device in the cluster.

2. Each chassis cluster member device can host active redundancy groups: This statement is true. Both devices in a chassis cluster can host active redundancy groups, allowing for load balancing and failover capabilities.

The two statements about SRX Series device chassis clusters that are true are that each chassis cluster member requires a unique cluster ID value, and that each chassis cluster member device can host active redundancy groups. A unique cluster ID value is necessary so that all members of the cluster can be identified, and each chassis cluster member device can host active redundancy groups to ensure that the cluster is able to maintain high availability and redundancy. Additionally, it is not necessary for all chassis cluster member devices to be the same model, as long as all devices are running the same version of Junos software.

NO.52 You are asked to block malicious applications regardless of the port number being used. In this scenario, which two application security features should be used? (Choose two.)

- * AppFW
- * AppQoS
- * APPID
- * AppTrack

You can block applications and users based on network access policies, users and their job roles, time, and application signatures. You can also use Juniper Advanced Threat Prevention (ATP) to find and block commodity and zero-day cyberthreats within files, IP traffic, and DNS requests.

NO.53 What is the default timeout for a TCP session on an SRX Series device?

- * 1 minute
- * 1 hour
- * 30 seconds
- * 30 minutes

NO.54 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.

NO.55 You are asked to ensure that if the session table on your SRX Series device gets close to exhausting its resources, that you enforce a more aggressive age-out of existing flows. In this scenario, which two statements are correct? (Choose two.)

- * The early-ageout configuration specifies the timeout value, in seconds, that will be applied once the low-watermark value is met.
- * The early-ageout configuration specifies the timeout value, in seconds, that will be applied once the high-watermark value is met.
- * The high-watermark configuration specifies the percentage of how much of the session table is left before disabling a more aggressive age-out timer.
- * The high-watermark configuration specifies the percentage of how much of the session table can be allocated before applying a more aggressive age-out timer

The early-ageout configuration specifies the timeout value, in seconds, that will be applied once the high-watermark value is met. The high-watermark configuration specifies the percentage of how much of the session table can be allocated before applying a more aggressive age-out timer.

This ensures that the session table does not become full and cause traffic issues, and also ensures that existing flows are aged out quickly when the table begins to get close to being full.

NO.56 What are two elements of a custom IDP/IPS attack object? (Choose two.)

- * the attack signature
- * the severity of the attack
- * the destination zone
- * the exempt rulebase

NO.57 Which three statements about SRX Series device chassis clusters are true? (Choose three.)

- * Chassis cluster control links must be configured using RFC 1918 IP addresses.
- * Chassis cluster member devices synchronize configuration using the control link.
- * A control link failure causes the secondary cluster node to be disabled.
- * Recovery from a control link failure requires that the secondary member device be rebooted.
- * Heartbeat messages verify that the chassis cluster control link is working.

1. Chassis cluster member devices synchronize configuration using the control link: This statement is correct because the control link is used for configuration synchronization among other functions.

2. A control link failure causes the secondary cluster node to be disabled: This statement is correct because a control link failure causes the secondary node to become ineligible for primary role and remain in secondary role until the control link is restored.

3. Heartbeat messages verify that the chassis cluster control link is working: This statement is correct because heartbeat messages are sent periodically over the control link to monitor its status.

NO.58 Which two statements are true about mixing traditional and unified security policies? (Choose two.)

- * When a packet matches a unified security policy, the evaluation process terminates
- * Traditional security policies must come before unified security policies
- * Unified security policies must come before traditional security policies
- * When a packet matches a traditional security policy, the evaluation process terminates

NO.59 Click the Exhibit button.

```
user@srx> show configuration services
advanced-anti-malware {
  policy TPP {
    http {
      inspection-profile default profile;
      action block;
      notification {
        log;
      }
    }
    verdict-threshold 7;
    fallback-options {
      action permit;
      notification {
        log;
      }
    }
    default-notification {
      log;
    }
    whitelist-notification {
      log;
    }
    blacklist-notification {
      log;
    }
  }
}
```

```
user@srx> show configuration security policies
from-zone Client to-zone Internet {
  policy Rule-1 {
    match {
      source-address any;
      destination-address any;
      application any;
    }
  }
}
```

You have deployed Sky ATP to protect your network from attacks so that users are unable to download malicious files. However, after a user attempts to download a malicious file, they are still able to communicate through the SRX Series device.

Referring to the exhibit, which statement is correct?

- * Change the security policy from a standard security policy to a unified security policy.
- * Remove the fallback options in the advanced anti-malware policy.
- * Configure a security intelligence policy and apply it to the security policy.
- * Lower the verdict threshold in the advanced anti-malware policy.

NO.60 Data plane logging operates in which two modes? (Choose two.)

- * syslog
- * binary
- * event
- * stream

NO.61 What information does encrypted traffic insights (ETI) use to notify SRX Series devices about known malware sites?

- * certificates
- * dynamic address groups
- * MAC addresses
- * domain names

Encrypted traffic insights (ETI) uses domain names to notify SRX Series devices about known malware sites. ETI is a feature of the SRX Series firewall that can detect and block malware that is hidden in encrypted traffic. It works by analyzing the domain names of the websites that the encrypted traffic is attempting to access. If the domain name matches a known malware site, ETI will send an alert to the SRX Series device, which can then take appropriate action to block the traffic. ETI is a useful tool for protecting against threats that attempt to evade detection by hiding in encrypted traffic.

NO.62 What are two benefits of using a vSRX in a software-defined network? (Choose two.)

- * scalability
- * no required software license
- * granular security
- * infinite number of interfaces

Scalability: vSRX instances can be easily added or removed as the needs of the network change, making it a flexible option for scaling in a software-defined network.

Granular Security: vSRX allows for granular security policies to be enforced at the virtual interface level, making it an effective solution for securing traffic in a software-defined network.

The two benefits of using a vSRX in a software-defined network are scalability and granular security. Scalability allows you to increase the number of resources available to meet the demands of network traffic, while granular security provides a level of control and flexibility to your network security that is not possible with a traditional firewall. With a vSRX, you can create multiple levels of security policies, rules, and access control lists to ensure that only authorized traffic can enter and exit your network. Additionally, you would not require a software license to use the vSRX, making it an economical solution for those looking for increased security and flexibility.

NO.63 You have deployed JSA and you need to view events and network activity that match rule criteria.

You must view this data using a single interface.

Which JSA feature should you use in this scenario?

- * Log Collector
- * Assets
- * Network Activity
- * Offense Manager

Earning the Security, Specialist (JNCIS-SEC) certification demonstrates that an individual has the knowledge and skills to implement and configure Juniper Networks security solutions. Security, Specialist (JNCIS-SEC) certification is highly regarded in the industry and can lead to many career opportunities. With the increasing demand for security professionals, the JN0-335 certification exam is an important step towards a successful career in the field of security.

Latest JN0-335 Pass Guaranteed Exam Dumps Certification Sample Questions:

<https://www.validexam.com/JN0-335-latest-dumps.html>