IT认证电子书

质　量　更　高　　服　务　更　好

半年免费升级服务

http://www.itrenzheng.com

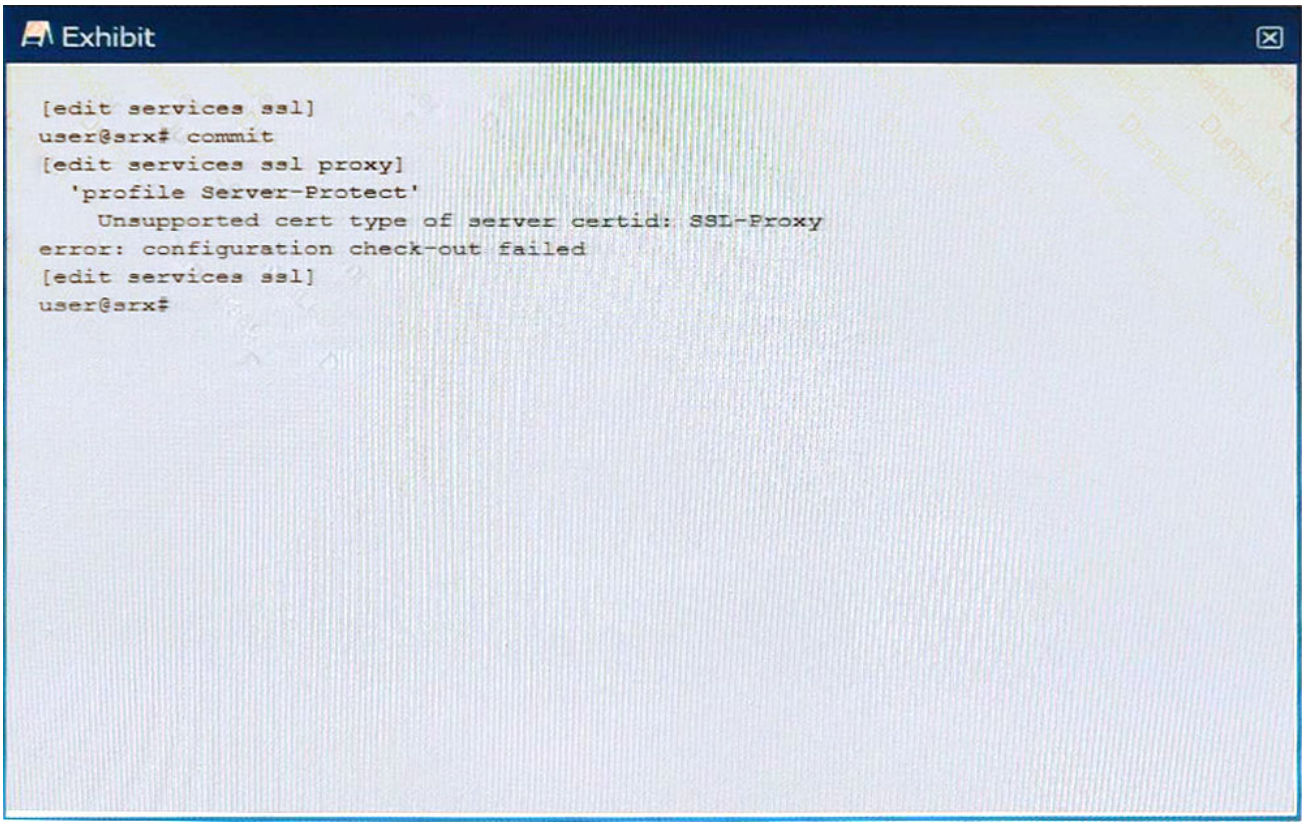
Exam : **JN0-335**

Title : Security, Specialist (JNCIS-SEC)

Version : DEMO

1.A client has attempted communication with a known command-and-control server and it has reached the configured threat level threshold.
Which feed will the clients IP address be automatically added to in this situation?
A. the command-and-control cloud feed
B. the allowlist and blocklist feed
C. the custom cloud feed
D. the infected host cloud feed
Answer: D
Explanation:
Infected hosts are internal hosts that have been compromised by malware and are communicating with external C&C servers3. Juniper ATP Cloud provides infected host feeds that list internal IP addresses or subnets of infected hosts along with a threat level3. Once the Juniper ATP Cloud global threshold for an infected host is met, that host is added to the infected host feed and assigned a threat level of 10 by the cloud4. You can also configure your SRX Series device to block traffic from these IP addresses using security policies4.

2.Exhibit

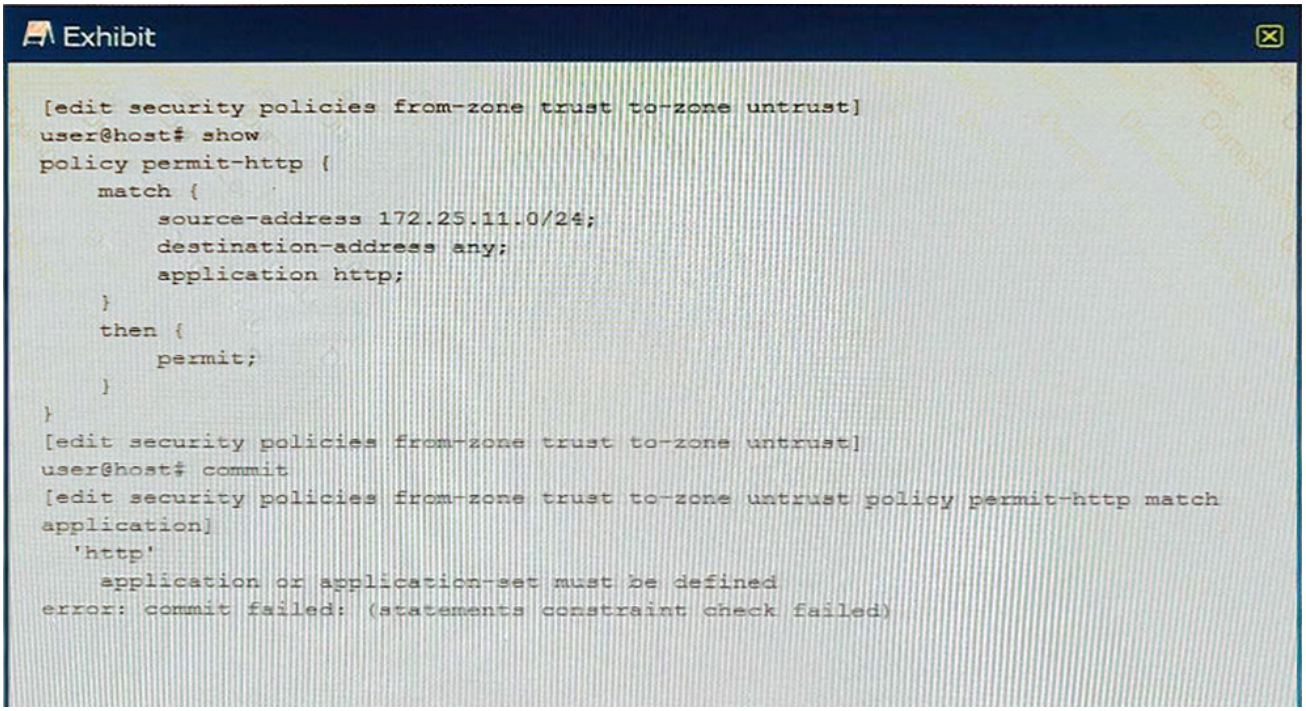


When trying to set up a server protection SSL proxy, you receive the error shown.
What are two reasons for this error? (Choose two.)
A. The SSL proxy certificate ID is part of a blocklist.
B. The SSL proxy certificate ID does not have the correct renegotiation option set.
C. The SSL proxy certificate ID is for a forwarding proxy.
D. The SSL proxy certificate ID does not exist.
Answer: A D

Explanation:
Two possible reasons for this error are that the SSL proxy certificate ID does not exist, or the SSL proxy certificate ID is part of a blocklist. If the SSL proxy certificate ID does not exist, you will need to generate a new certificate. If the SSL proxy certificate ID is part of a blocklist, you will need to contact the source of the blocklist to remove it. Additionally, you may need to check that the SSL proxy certificate ID has the correct renegotiation option set, as this is necessary for proper server protection. For more information, you can refer to the Juniper Security documentation at https://www.juniper.net/documentation/en_US/junos/topics/reference/configuration-statement/security-ssl-pro

3.You are asked to reduce the load that the JIMS server places on your
Which action should you take in this situation?
A. Connect JIMS to the RADIUS server
B. Connect JIMS to the domain Exchange server
C. Connect JIMS to the domain SQL server.
D. Connect JIMS to another SRX Series device.
Answer: D
Explanation:
JIMS server is a Juniper Identity Management Service that collects user identity information from different authentication sources for SRX Series devices12. It can connect to SRX Series devices and CSO platform in your network1.

4.Exhibit



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

5.What are two types of system logs that Junos generates? (Choose two.)
A. SQL log files
B. data plane logs
C. system core dump files
D. control plane logs
Answer: B D
Explanation:
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.