

Considerations When Planning a Deployment of C-series Controllers

When you plan an SRC deployment, take into consideration requirements for security and high availability to comply with your organization's standard practices:

- **Hardware redundancy**—Because each C-series Controller contains all SRC core components, the platforms can provide redundancy for each other. If a C-series Controller is inaccessible, other platforms can manage the routers, services, and subscribers.

In the event of a hardware failure, one C-series Controller can be replaced with another one. The Juniper Networks database and the SAE synchronize with the software on other platforms. During routine system maintenance and software upgrades, a C-series Controller can be taken out of service then returned to service and the data synchronized.

- **High availability for the Juniper Networks database**—The database provides a robust redundancy scheme that you can customize for your deployment. The configuration lets you specify which databases are primary and which are secondary, and how data is propagated among a number of databases.
- **High availability for SRC components** —Components such as SAE and NIC let you configure high availability separately for each software component, which means that software redundancy can be configured as a mesh over a number of C-series Controllers.
- **Secure remote access**—Remote access to the SRC CLI can be set up through Telnet or SSH and to the C-Web interface through http or https.
- **Directory connections**—You can secure connections between the directory and other applications through secure LDAP.
- **Web applications**—Applications can leverage the security configured for your Web application server.
- **RADIUS server**—Because RADIUS is stateless, you can configure a sufficient number of RADIUS servers for the load, and you can configure both the routers and the SAE to load balance across them.
- **Common Open Policy Service (COPS) connections**— The JUNOSe routers can be configured with primary, secondary, and tertiary COPS servers, so it is possible to configure many failover schemes. This flexibility lets you locate backup SAEs remotely to provide geographical redundancy or close to the routers they manage to improve network performance.

It is also possible for SAE servers to redirect existing and new COPS connections to other, more lightly loaded SAE servers. This COPS connection redirection can be triggered manually during a scheduled maintenance window or automatically based on SAE load monitoring.

- **Load balancing for the network information collector (NIC)**—You can provide load balancing for the NIC in the following ways:
 - Deploy two or more NIC hosts that each have the same configuration, and then configure NIC proxies to load balance across the NIC hosts.
 - Run the NIC hosts locally in the Dynamic Service Activator (DSA).

- For NIC scenarios that require an SAE plug-in to track data about individual subscribers for a deployment in a large network, deploy NIC hosts to handle parts of the network with a different set of NIC hosts to aggregate requests.