Security

LightWave Server™ provides a number of built in security features to ensure that your applications and NonStop Server remain secure.

Transport Security

LightWave Server uses OpenSSL to provide transport security using the latest version of TLS. Client applications can take advantage of this feature by simply invoking API requests using the HTTPS protocol.

User Authentication

LightWave Server maintains its own User and Group identity store which is managed from the LightWave Server Management Console. API clients authenticate with LightWave Server using standard HTTP Basic or Digest authentication.

Rules Based Access Control

Access to API services is controlled using the configuration and application of Access Control Policies. Policies can be configured to restrict API service access to specific users, groups, or client source IP addresses. For example, any of the following rules can be created:

- Allow group "hr" access to the Employee service which provides the employee management API.
- Allow user "janedoe" access to the process API, but only if connecting from IP subnet 10.0.0.0/28.
- Restrict requests to specific CORS origins.

Network Isolation

Although not a specific feature of LightWave Server, because LightWave Server uses the HTTP protocol, it's possible to use any number of web-application network isolation techniques to isolate your NonStop Server network from client application networks. For example, if your NonStop Server is providing back end services for a mobile Intenet application, you can isolate your NonStop Server network from the Internet using a secure HTTP proxy. Many such web application isolation products are available providing various levels of security, access control, and logging. Please consult with your Network and/or Security personnel for more information regarding your specific needs. The diagram below shows a simple example of a proxy being used with a LightWave Server application.