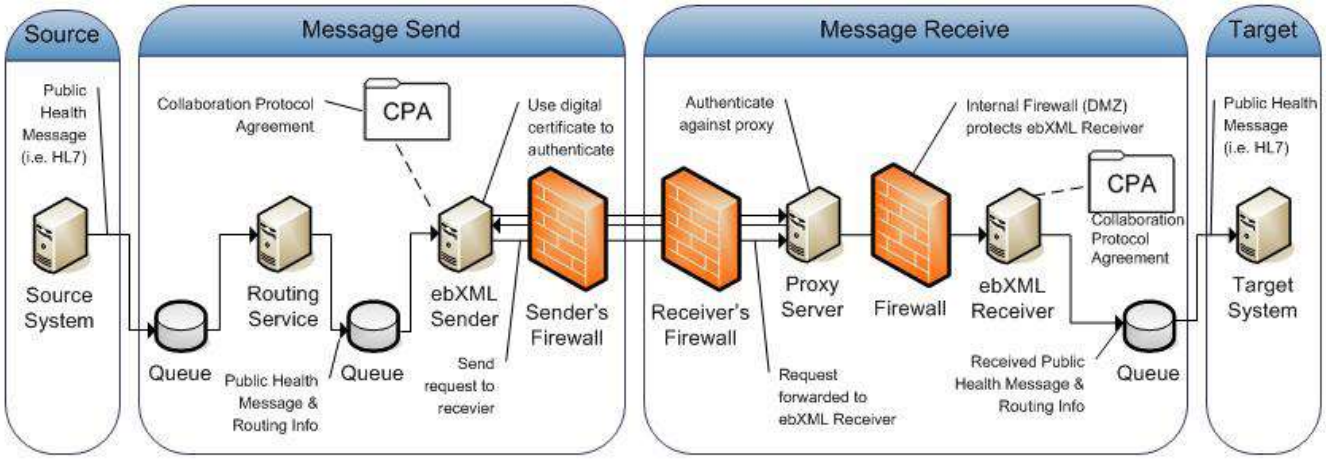
Infrastructure Architecture

Essential functional elements of the PHIN Secure Messaging integration point consist of the ability to securely send and receive public health messages between designated end-points.

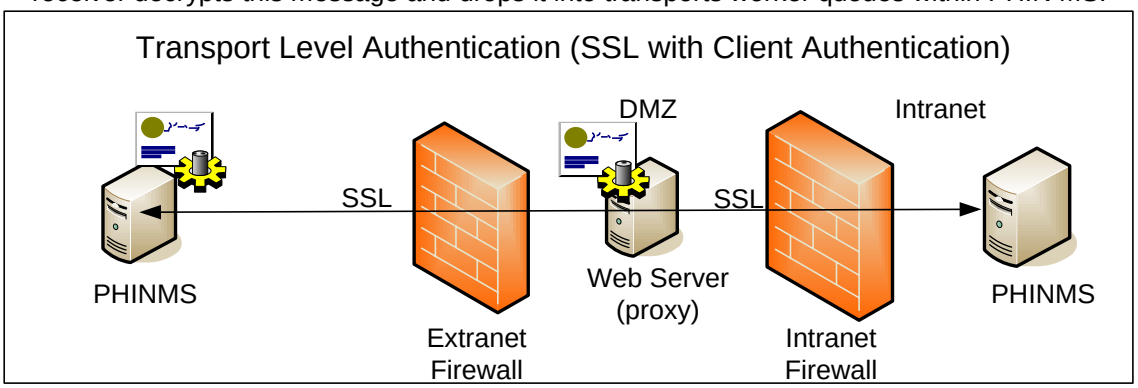
Technology Architecture



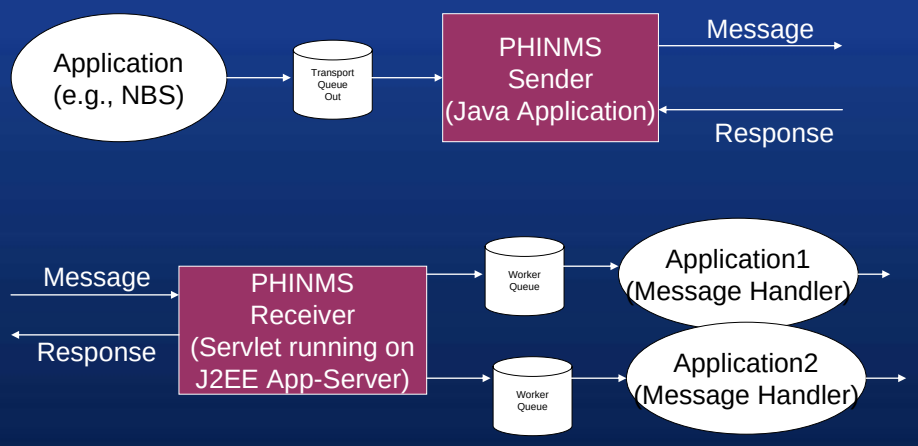
PHINMS Overview:

PHINMS securely sends and receives sensitive data over the Internet to public health information systems. This involves a common approach to security and encryption, a method for dealing with various firewalls and internet protection schemes, a standard way for addressing and routing content, a customary and consistent way for information systems to "shake hands" and confirm that an exchange was successful.

A message is composed and dropped in a transport queue table (database table) at the sender site. The PHINMS Sender reads the transport queue, creates an ebXML message, and posts this message to the URL of the web-server proxy (currently certified for IIS 5.0 and 6.0) in the PHINMS receivers (i.e., state Dept. Of Health) DMZ (Demilitarized Zone). This web-server authenticates the PHINMS sender using client-certificates over SSL and proxies the incoming request to the PHINMS receiver, which is deployed on the receivers Intranet. The PHINMS receiver decrypts this message and drops it into transports worker queues within PHIN MS.



Functional Components



Message Routing