iSite SSL Security
Hospital Security

Today's healthcare institutions demand greater access to information and avenues of communication among clinicians, patients, administrators, vendors, employees, and suppliers. Healthcare institutions that use the Internet to achieve greater access to patient information must implement significant safeguards to protect its network and data.

The key to addressing this information security risk is a comprehensive Internet security architecture. The solution may require multiple layers of security using best-of-breed products from a variety of vendors. The integration and manageability of these multiple products are essential factors in the achievement of a secure architecture.

Security administrators must be confident that applications can properly authenticate users and that Internet gateways will always enforce the appropriate security policy. They must also be able to define and apply security policies across multiple technologies including firewalls, VPNs and QoS devices, manage reports on network activity, and maintain the proper system configurations. These tasks can pose significant challenges to the security administrator tasked with securing a healthcare institution's network infrastructure. This document explains the ways in which Stentor addresses security issues across Local Area Networks, Wide Area Networks and on the external Internet.

The iSite System

Stentor's iSite medical image and information management system is based on standard TCP/IP (Internet) communications protocols and is compatible with many standard security and encryption methods:

- Virtual Private Networks (VPNs) - to allow remote users to securely connect to the site network.
- “Extranets” by enabling Secure Sockets Layer (SSL) - an Internet security protocol used by Internet browsers and Web servers to transmit sensitive information - to allow secure controlled access to outside users without having to administer a VPN and VPN client access.
- Deploy iSite behind internal secure firewalls.

iSite Client/Server Transfer

There are five principal types of traffic that normally occur as an iSite Client is in contact with the iSite Server:

1. Login – The iSite client sends username and password to the server for authentication.
2. Browsing and selection – http traffic on port 80 using Active Server Pages.
3. Study Meta Data Transfer – Detailed textual study information is sent to the Client using a Stentor proprietary protocol via CORBA on port 6464.
4. iSyntax image transfer initialization – A “seed” view for each image is sent using Stentor’s proprietary iSyntax protocol via CORBA on port 6464.

5. iSyntax image interaction – The iSite Client dynamically requests additional image information as a user pans and zooms images. Data is transferred using Stentor’s proprietary iSyntax protocol via CORBA on port 6464. This additional data depends on the “seed” and is meaningless without it.

Stentor’s iSite clients (remote or internal) communicate with the iSite server (behind the firewall) on a dedicated network. When retrieving images and patient information, the client asks the server for “packets” of image data via the secure network. Image reconstruction occurs on the client side, the server simply sends the image data across the network.

VPNs with iSite 3.0

Stentor works with the hospital to create a private network that uses a public network (usually the Internet) to connect remote sites or users together. Instead of using a dedicated, real-world connection such as a leased line, the VPN uses “virtual” connections routed through the Internet from the hospital’s private network to the remote site.

Implementation of VPN Security with iSite 3.0

VPN with iSite is the most secure mode of security and uses several methods for keeping a hospital’s connection and data secure:

- **Firewalls** - A firewall provides a strong barrier between the private network and the Internet. You can set firewalls to restrict the number of open ports, what type of packets are passed through and which protocols are allowed through.

- **Encryption** - This is the process of taking all the data that one computer is sending to another and encoding it into a form that only the other computer will be able to decode.

Implementation of Secure Socket Layer with iSite 3.0.

Extranets are often created by enabling Secure Socket Layer (SSL) on a server and allowing authenticated users to access the server from any Internet address. By default, client-server network traffic with iSite is restricted to two fixed IP addresses:

- “TCP/IP port 80” for what is called Hypertext Transport Protocol (http) and is used primarily for browsing and selecting imaging studies for review (when SSL certs are installed port 443 is used instead of port 80); and

- “Port 6464” which contains Stentor’s proprietary iSyntax protocol traffic - Common Object Request Broker Architecture (CORBA).

SSL Certificates are used to identify one end or both ends of each transaction and can be installed on the iSite Server and the web server portion of the iSite Server can be SSL enabled. The result is that the http traffic for port 80 is encrypted using 128 bit Data Encryption Standard (DES). All communications that transfer on Port 6464 utilize Stentor’s proprietary protocols.