



Alpha's iChart Security Architecture through the Dictaphone IDC

The cornerstone of the Alpha Transcriptions Internet Data Center (IDC) infrastructure is a redundant Cisco Systems Catalyst 6500 routing switch which interconnects the four segments servicing the iChart Enterprise Express application servers, as well as the ancillary servers used to service the infrastructure: redundant DNS, Redundant ACE SecurID servers, redundant WINS, redundant Cisco PIX firewalls, and redundant Cisco 3030 VPN Concentrators.

The IDC interfaces to the Internet via dual T3 pipes delivered on a pair of Cisco 7206 routers configured with HSRP to ensure high availability.

The emphasis throughout the architecture is to leverage the automatic redundancy available off the shelf from the vendors and supplement this with duplicate boxes when this is unavailable. For instance, VPN equipment has an unproven record for automatic redundancy. Therefore, to increase overall availability of the VPN infrastructure we implemented multiple such VPN concentrators.

The primary DNS entry serves the address of each concentrator in a round robin fashion to distribute the load across the boxes; each VPN client is further configured to establish a session with the alternate concentrator in case of failure of the main concentrator.

Security Policy

The security policy in force at iChart can be summarized in the following three rules:

1. All traffic flowing across the Internet to or from the IDC will be encrypted either by a VPN tunnel (DES or 3DES) or SSL Certificate
2. All traffic entering the IDC must pass through a PIX firewall, where strict policies are enforced to insure that only essential TCP/IP protocols are permitted from the outside
3. Strict firewall rules are also applied to any Internet traffic generated from inside the IDC, and only approved traffic is allowed out through the PIX firewall.

Users connecting to the IDC via home-based ISP connections are using the Cisco VPN 3000 Client software; all VPN sessions occur over IPSec and are encrypted using DES. Users are authenticated using three factors: a user ID, a PIN and a one-time password generated with a SecurID token card (FOB) assigned to each user.

The iChart model includes a site-to-site VPN connection between each VA facilities main location and the IDC. At VA facility location, a dedicated ISP connection of suitable bandwidth is provisioned and typically terminated on an Alpha-owned and maintained Cisco 3005 VPN Concentrator. This equipment is shipped pre-configured to enable connectivity between agreed upon customer IP segments and specific iChart servers. All communications are encrypted using 3DES. iChart-provided equipment, such as the Voice Capture Subsystem and the HIS interface gateway resides at each VA's main location, on the "safe" side of the VPN concentrator. All user-to-site and site-to-site ISP connections are the responsibility of the VA. We recommend that the facility procure their ISP connections from one of the Tier 1 ISP's.



Both dictators and transcriptionists must provide user ID's and password to gain access to the applications. The Enterprise Express application provides flexible control over the features users can access.

Data Protection Policy

ichart's data backup methodology includes daily full backups of all IDC servers. Tapes are rotated weekly and stored off site. On line storage of medical reports complies with the RFP for a period of 6 months.

System Management

The IDC is staffed during normal business hours, and the equipment is monitored 24/7 by ichart's management tools. IDC personnel are paged upon automated detection of equipment failures. Data Center ISPs monitor the network 24/7 and report any network failures to IDC personnel. All equipment capable of automatically failing over upon failure of a component is properly configured with a hot stand by unit. This includes routers, network switches, and VPN concentrators located at the IDC. Servers with limited built-in redundancy are configured with dual NIC and RAID 5 disk arrays. A fully configured spare server of each model is set aside to handle failure of a major server component in each batch of 36 servers installed in the IDC.