Concord Network Security

Concord's fully redundant IP fax platform supports multiple secure methods for customers to connect. Concord supports TLS (Transport Layer Security) for secure e-mail, HTTPS (Hyper Text Transport Protocol Secure) for web services as well as VPNs (Virtual Private Network). Alternatively, leased lines are also supported. Concord data centers are protected by state of the art firewalls and intrusion detection systems and all access by employees is monitored and logged. Strict password strength and change requirements are enforced.

As a result, the Concord IP fax service can be used in compliance with all common rules and regulations such as HIPAA, Sarbanes Oxley (SOX), Gramm-Leach Bliley (GLB), Payment Card Industry (PCI) Security Alliance (SA), Know Your Customer, Basel II and many more.

SECURE HTTP

Concord's web services utilize HTTPS, the same technology and encryption used daily for online banking and a host of other secure applications. HTTPS utilizes SSL (Secure Socket Layer) and Concord mandates a minimum of 256Bit encryption. HTTPS is always used for access to Concord's AAC even if the customer connects to Concord through a VPN (in that case, HTTPS traffic can be routed through the VPN).

TRANSPORT LAYER SECURITY

The same SSL encryption can also be used for SMTP. Unlike with a VPN, where the entire communications link is encrypted, TLS only encrypts the actual message communication. For e-mail-based fax services, TLS can be as secure as a VPN and offers some benefits in the case of customers recovering from a catastrophic event in the customers data center.

VIRTUAL PRIVATE NETWORKS

Concord provides VPN security through Cisco equipment and provides a unique DMZ (Demilitarized Zone) for each customer to insure information integrity between customers. VPNs are a very secure way of transmitting data but require some configuration on both the Concord and customer sides. To insure redundancy, a separate VPN between the customer and Concord's Seattle data center as well as a VPN between the customer and Concord's Chicago data center is required. Often, customers have multiple locations for redundancy; each of those locations should have its own VPN configured to both Concord data centers.