Hospital Network Secures Voice and Data Traffic with Engage Encryption Solutions

End User: Hospital Network

Type: Healthcare

Profile: Regional healthcare provider including hospitals, clinics, and urgent care facilities.

Summary

Concern about data breaches is on the rise as healthcare organizations are increasingly targets of both internal and external data snooping, hacking, and theft. The negative consequences can include fines, investigation and legal fees, computer and voice network downtime, and ultimately can impact an organizations reputation.

The IT organization of a major regional healthcare system, taking these threats seriously, put in place a plan to encrypt data in motion between their different facilities. This included both packet data and T1 voice circuits.

After researching network encryption equipment providers, the hospital IT team determined the Engage Communication BlackDoor packet and BlackBond link encryptors were an ideal fit.

Solution

Engage "Black" products utilize highly secure 256 bit Advanced Encryption Standard (AES) symmetrical key encryption. The BlackDoor encryptor provides packet encryption at layer 2 or layer 3 for 10/100 and 1 Gig Ethernet connections, and offers copper or fiber based interfaces. The BlackBond encryptor provides link encryption for T1 or E1 circuits.

In this case a combination of 10/100 and Gigabit Ethernet BlackDoor encryptors were used. One server unit was deployed for key management and the other units were BlackDoor client devices. The BlackBond was installed on all T1 voice circuits interconnecting PBXs and Key Systems at the various healthcare locations. The BlackBond encrypts both full and fractional T1 traffic, is an extremely low latency device, and is transparent to the T1 payload. Consequently the "plug and play" insertion of the BlackBond onto existing T1 circuits was seamless.

Both the BlackDoor and BlackBond are available in stand-alone and slot-card configurations. The Engage CHUB chassis was installed at the main data center location with BlackDoor Gig, BlackDoor 10/100, and BlackBond T1 slot cards all inserted in the same chassis. The chassis was configured with redundant power supplies. Satellite facilities were outfitted with stand-alone BlackDoor and BlackBond units.

To further protect the data traffic, the Hospital elected to encrypt the entire IP packet payload and header so that snooping on the links would not reveal source and destination IP address information. IP tunnels were created between BlackDoors at the various locations to accomplish this.

Implementation

Engage provided detailed training to the Hospital network operations staff and the BlackDoor and BlackBond equipment were delivered on time. Equipment installation was also completed per schedule and configuring and turning up the solution went smoothly with some assistance from Engage technical support.

With data and voice encryption in place, the Hospital has added another level of protection in the continuous battle to secure sensitive patient records, corporate data, and voice communications.