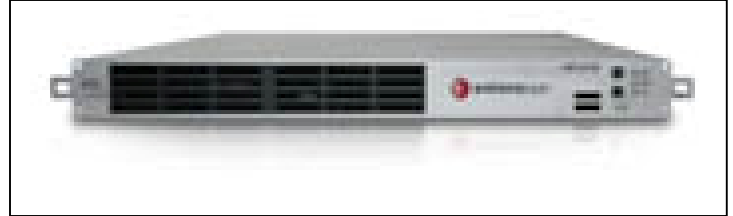


Enterasys Guest and Secure Staff Wireless Information Sheet

Overview

In an effort to increase connectivity beyond the confines of a wired network, the IT department has introduced an Enterasys RoamAbout Wireless Switch into the Towns network infrastructure. This new device gives us the capability to allow Guests to access the internet from select sites throughout Town without compromising network security.



Through the same wireless access points that are used by Guests, Town staff with Town provided wireless laptops can have secure access to their resources such as J&K drives, Outlook email and filtered internet. In addition to mobility, this also allows us to provide new sites network connectivity without the expense of installing internal wiring at that location.

Staff wireless security is achieved through the use of 802.1X. This is a combination of technologies that uses internal Certificate Servers, RADIUS Authentication and randomly generated and rotating wireless encryption keys. This all happens in the background and is transparent to the user.

Guest access is accomplished through the use of a separate Virtual Local Area Network and Open Access Points. Traffic for guests is not encrypted. The only requirement for Guests is that they accept a Terms and Conditions agreement for use of the network.

Highlights

- Secure Staff access to network resources from specific locations
- Network security is preserved while allowing access for both Staff and Guests
- Free access to the internet for Guest users

Interaction with Other Systems

- Certificate Servers
- IAS RADIUS Authentication Server
- Active Directory enabled

Project Details

- Project # 07-3427
- Implemented 12/12/2006