



ERF Wireless CryptoVue™ Network Security Appliance

The ERF Wireless CryptoVue™ Network Security Appliance is the cornerstone of an enterprise-wide network security system consisting of software, site-based hardware devices, secret biometric crypto keys and a collection of secure servers to perform network encryption, 24/7 monitoring and enforcement of rigid controls. The development of the device was spearheaded by the former Chairman/CEO and founder of FundsXpress, a leading Internet banking company that built a reputation on its exceptional network encryption system.

After numerous discussions with auditors, bankers, cryptologists and banking examiners, the ERF Wireless CryptoVue Network Security Appliance was developed to satisfy both stringent auditing standards and U.S. federal banking regulations covering both enterprise land-based lines and wireless network security.

Each location on the enterprise network has a powered CryptoVue™ device installed on-premises in a secure enclosure with cables connected between its two Ethernet interfaces and the respective LAN and WAN network points. The CryptoVue device implements triple DES IPsec encrypted tunnels to encapsulate Layer 3 data LAN to LAN over the WAN network to each location in the enterprise. The device also implements a packet filtering firewall to block the propagation of any traffic on the WAN network from any device other than an authenticated CryptoVue device. The device also routes encrypted packets of traffic to other authenticated CryptoVue devices on the WAN between the associated LANs and multiple internal LAN subnets across the network.



Key to the system architecture and design, the CryptoVue software implements a special routine during the install process that pulls the required CryptoVue configuration file off a separate Secret Biometric Crypto Key for each location. This feature greatly simplifies the setup of an encrypted microwave or land-line network that often contains hundreds of separately configured IPsec encrypted tunnels to and from each location.



Before performing configuration or other changes, the CryptoVue software also requires all utilities to check for the presence of the Secret Biometric Crypto Key (obtained from a secure location and requiring an index finger scan by authorized security personnel), an authenticated user login (user name and paraphrase password entered by the entity's IT manager) and acknowledgement of the event by the remote CryptoVue Monitoring Server. The enforcement of triple controls is a key distinguishing feature of the CryptoVue System and addresses regulatory concerns with securing microwave networks.

The CryptoVue Monitoring Server simultaneously tracks the status of all encryption and radio devices on the enterprise network. Each CryptoVue device initiates a secure session with the CryptoVue Monitoring Server and advises the server of its status at configurable intervals. The WAN side NICs of the CryptoVue devices are also polled at regular intervals by the CryptoVue

Polling Server that sits on-site at the entity's operations center and is connected to the encrypted microwave WAN subnet.

The CryptoVue Polling Server reports device status and performance data back to the CryptoVue Monitoring Server which will issue an alert if it doesn't get a successful status report from any CryptoVue or radio device. The CryptoVue Monitoring Server is also used to generate the initial configuration files for each CryptoVue device and writes it to a specially encoded Secret Crypto Key that is specific to that device's location.

A CryptoVue Gateway Server is maintained so all CryptoVue devices can be reached via an encrypted PPP over SSH session for maintenance and central administration. However, a CryptoVue device will not permit such connections to take place unless its coded Secret Crypto Key has been inserted into the matching device by the authorized security personnel and a successful login authentication has been entered by the entity's IT manager. A CryptoVue Repository Server is also maintained for CryptoVue devices to automatically poll at configurable intervals for critical software updates. The design and automation developed for the CryptoVue System, including the setup process, monitoring, polling, central administration and software updating, is very unique and is the result of an extensive R&D effort by ERF Wireless.

The ERF Wireless CryptoVue Network Security Appliance conforms to the following requirements:

- Data packets sent or received by CryptoVue devices across the WAN are triple DES encrypted.
- Data packets originating from a CryptoVue device are only being routed across the WAN to another authenticated CryptoVue device inside IPsec encrypted tunnels.
- A CryptoVue device's Packet Filtering Firewall blocks propagation of any data traffic on the WAN that has not originated from an authenticated CryptoVue device located within the encrypted network.
- The CryptoVue software insures that encrypted data packets forwarded to a CryptoVue device from an authenticated CryptoVue device have not been modified in transit.
- Remote logins to the CryptoVue device can only originate from the trusted CryptoVue Gateway Server, and can only occur when a coded Secret Crypto Key has been inserted into the matching CryptoVue by the FI's security officer, and the FI's IT manager has authenticated the connection via an on-site login to the CryptoVue device.
- Software downloaded and installed through the encrypted update mechanism on the CryptoVue device was digitally signed by ERF Wireless, a trust authority.

About ERF Wireless – ERF Wireless is the leading provider of encrypted private microwave and fiber enterprise networks to financial institutions. ERF Wireless, Inc. (OTCBB:ERFW) is a fully reporting public corporation with headquarters located in League City, Texas. For more information, please visit our web site at www.erfwireless.com/enterprise or call 512-352-7118.

