KEYNET Network Security Manager

Secure, Centralized,

Cipher X®

Network Security Device

Management System

The KEYNET Network Security Manager simplifies the configuration and management a global networks of TCC's Cipher X 7210, 7211, and 7220 Network Security Devices. With an intuitive user interface and automated polling of alarms and logs, a network expert is not needed for trusted key and device management.

Centralized Management

KEYNET provides centralized key and device management of a global network of Cipher X family of Network Security Devices. All device configurations including security policies are intuitively managed with a user-friendly interface. Automatic polling of alarms and logs monitor device status. KEYNET also securely generates, stores and distributes middle and high-layer encryption keys to ensure the critical security of the network.

Cipher X Encryption

The wire speed Cipher X 7210, 7211, and 7220 devices provide strategic-level communications security for global networks. They integrate seamlessly into existing or new networks without impacting network performance. The Cipher X family provides performance from 100 Mb/s to 10 Gb/s and is highly flexible, supporting a vast number of network configurations and a wide range of network security requirements.

Cipher X 7211 Encryptor

Multiple Layers of Protection

The KEYNET Network Security Manager consists of a Windows 7 ultimate rack mount server and 1RU tamper-proof hardware-based security vault. The security vault is outside the Windows environment and generates and deploys the middle and upper level keys used in TCC's three-tier symmetric key management hierarchy.

KEYNET securely communicates with all Cipher X Network Security Devices using SNMP with TCC's secure extensions. Additionally, device management is user authenticated to provide control and traceability of changes. Two levels of role-based security are provided: crypto officers have full control capabilities, while operators are restricted to monitoring privileges.

Benefits

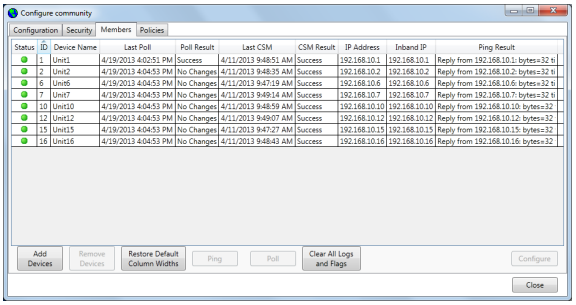
- Easy to use, centralized management platform
- Automated key and device management requires little human interaction
- Hardware-based security vault protects highly critical keys
- Multiple layers of protection
- User-authenticated device configuration and deployment for traceability
- Manages remote software updates
- Simple provisioning and management of security policies
- Intuitive user-friendly interface
- Network expert not needed to manage network security

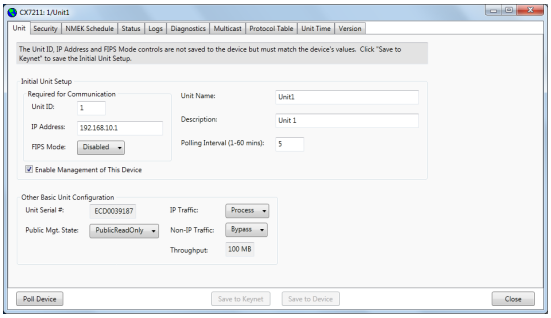
KEYNET
Network Security Manager

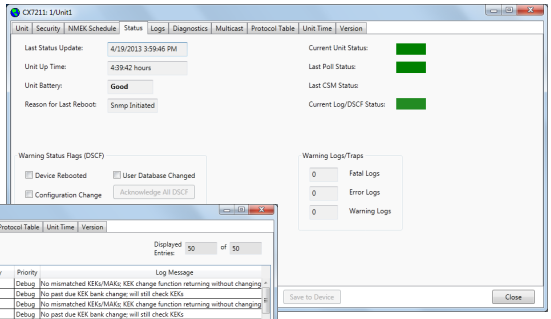
Flexible Network Configurations and Security Policies

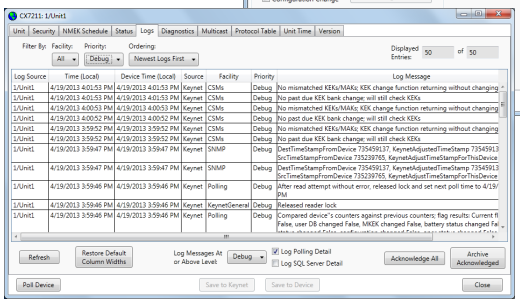
KEYNET configures and monitors the robust Cipher X Family security policy enforcement engine. Policies indicate how data is treated in the encryptors, including: pass through, cipher or block. Policies are based on a wide range of configurable parameters such as VLAN tags, L2/3 source and destination addresses, L3/4 protocol and port numbers. The flexibility of the Cipher X's security policy engine provides wide-ranging support of network configurations and security requirements, while KEYNET simplifies their provisioning and management. Simple policy entries in KEYNET establish the policies without complex router reconfiguration required.

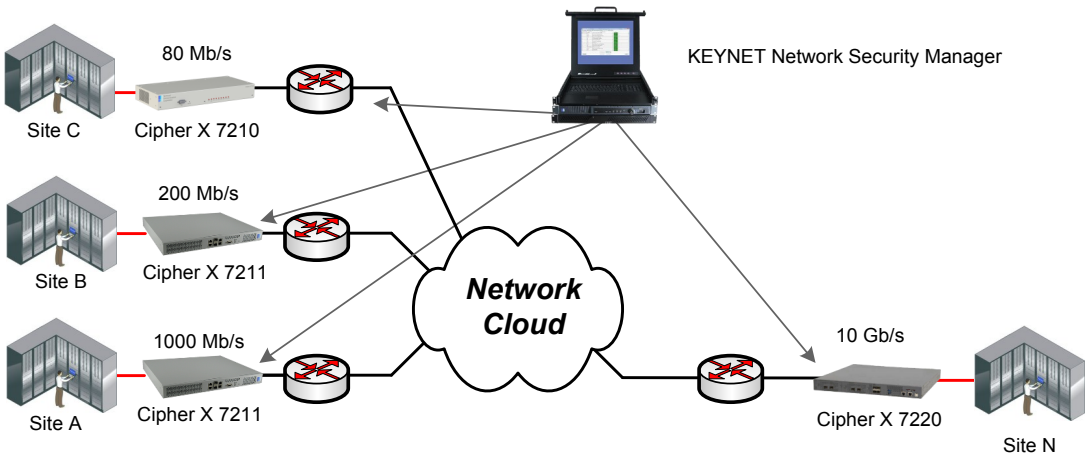
Optimized Network Encryption











For more than 50 years, Technical Communications Corporation has specialized in superior-grade secure communications systems and customized solutions, supporting our CipherONE® best-in-class criteria, to protect highly sensitive voice, data and video transmitted over a wide range of networks. Government entities, military agencies and corporate enterprises in over 115 countries have selected TCC's proven security to protect their communications.

Communicate in Confidence

TECHNICAL COMMUNICATIONS CORPORATION
100 Domino Drive, Concord, MA 01742 U.S.A.
+1-978-287-5100, Online request: www.tccsecure.com/sales
Fax: +1-978-371-1280, Web: www.tccsecure.com