UniGuard *AES*

Secure Out of Band Management with Advanced Encryption Standard

√ **NIST certified AES & 3DES** √ **Self-contained Database**
√ **RSA SecurID Ready** √ **Centrally Managed**
√ **Network Interface Option** √ **Supports Client & Host modes**

The Problem

Access to console ports on Routers, Firewalls, Network Appliances, etc., cannot be protected by network security when out of band access is required. Secure Out of Band Management and Network security are mutually exclusive events.

The Solution

The UniGuard connects directly to multiple console ports and provides the highest level of protection regardless of the status of the network. This is done by maintaining an internal security database that is updated by a "patented" central database manager on an "as needed" basis. This internal database provides fast, reliable, AES encryption, and/or two factor authentication. Full **NIST certified AES** or 3DES encryption can be enabled by using a UniGuard Client(s) at the NOC center.

RSA Secured

The UniGuard has the option to authenticate RSA tokens "on board" without needing access to the network. If the network option is installed the device can check for access to the RSA Server prior to authenticating on board.

Network Capability

An optional network interface provides in band access to the device supporting **hardware** encrypted network access along with real time monitoring, reporting, etc.. The device will also check the telco line status periodically and report back to the manager.
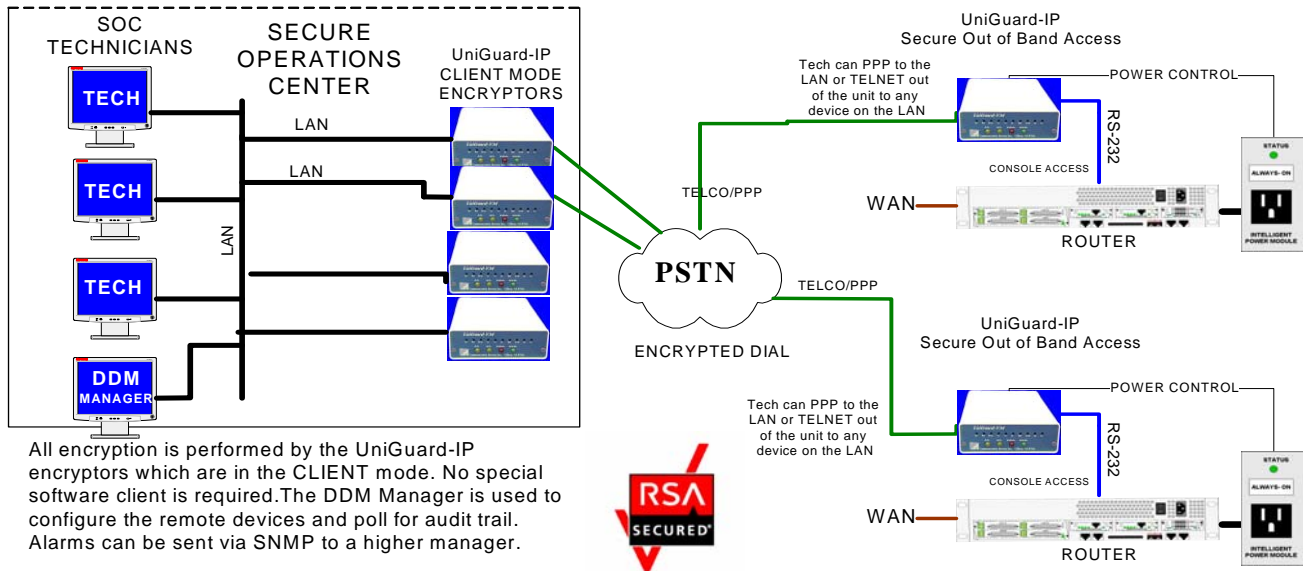
Security Management

DDM, Distributed Database Manager, can manage an unlimited number of CDI devices remotely from a single(ODBC) or multiple(SQL) workstations. This eliminates the need to update each unit individually when there is a database change. Audit trail reports are extracted automatically.

Deployment

Any standard modem installtion can be replaced by a UniGuard. Examples include console ports on; Routers, Fire walls, PBX's, DSLAM's, ATM switches, power stations, utilities, and more!

http://www.outofbandmanagement.com

SECURE OUT OF BAND MANAGEMENT
OVER DIAL-UP WITH POWER CONTROL

SOC TECHNICIANS

SECURE OPERATIONS CENTER

UniGuard-IP CLIENT MODE ENCRYPTORS

TECH

TECH

TECH

DDM MANAGER

LAN

LAN

LAN

PSTN

TELCO/PPP

ENCRYPTED DIAL

TELCO/PPP

UniGuard-IP Secure Out of Band Access

Tech can PPP to the LAN or TELNET out of the unit to any device on the LAN

POWER CONTROL

RS-232

CONSOLE ACCESS

WAN

ROUTER

STATUS
ALWAYS-ON
INTELLIGENT POWER MODULE

UniGuard-IP Secure Out of Band Access

Tech can PPP to the LAN or TELNET out of the unit to any device on the LAN

POWER CONTROL

RS-232

CONSOLE ACCESS

WAN

ROUTER

STATUS
ALWAYS-ON
INTELLIGENT POWER MODULE

All encryption is performed by the UniGuard-IP encryptors which are in the CLIENT mode. No special software client is required.The DDM Manager is used to configure the remote devices and poll for audit trail. Alarms can be sent via SNMP to a higher manager.

RSA SECURED

CDI
Communication Devices, Inc.

Communication Devices Inc.
1 Forstmann Court
Clifton, NJ 07011
1.973.772.6997

This is a typical Secure Out of Band Management configuration for a Managed Security Provider. The UniGuard-IP is connected to the console port of a Routers . A LAN connection also attaches the UniGuard-IP to the remote LAN. In the event of a problem, the SOC technician can 3DES dial-up to the UniGuard-IP. This will then allow console access . The tech can also PPP connect to the remote LAN or TELNET out of the unit to a remote device. At no time is the UniGuard-IP relying on network security to operate as the network is in question when the device is used.

The above diagram displays a typical network implementation of UniGuards protecting router console ports in a network. A variety of application specific cables are available for device connection. More information regarding cabling options can be found at http://www.commdevices.com/cable_kits.htm.

Modes of Operation
The UniGuard can operate as a Client encryptor in the NOC or as a host based remote encryptor in the field.

Host based encryptors are used to protect remote sites from unauthorized access.

Client encryptors reside in the NOC and can encrypt with any of the host based UniGuards or Port Authorities in the field.

Part Numbers

UG-AES-US	Standard unit US Power
UG-AES-UK	Standard unit UK Power
UG-AES-EU	Standard unit European Power
UG-AES-100IP	Unit with 100M network interface, Add **-US**, **-UK**, **-EU** for power.
DC48C	48VDC power adapter
PCM-US	Power control module 110VAC
PCM-EU	Power control module 220VAC

Specifications

Length	7 Inches (17.5 CM)
Width	4.1 Inches (10.5 CM)
Height	1.6 Inches (4.0 CM)
Power	110VAC 1 AMP, 220VAC .5 AMP, 48VDC 150ma
Weight	1.4 LBS (635 Grams)
Misc.	NIST AES & TDES, RSA, FCC PART 15, PART 68, CE, UL60950