# SSL1000 Security Appliance

The challenge of securing your mainframe consoles and applications over the corporate network continues to intensify as network boundaries are eliminated and enterprise networks are opened to customers, suppliers and numerous employees and locations. Trying to balance corporate security policies, federally mandated security policies (such as HIPAA), LANs, WANs, firewalls, VPNs, and local and offsite network infrastructure often seems like a relentless battle.

Visara created the SSL1000 to help you meet the demands of your network environment. The SSL1000 concept is simple - encrypted sessions on the network side, clear text on your side. No complicated security policies to administer. No waiting for corporate-wide enterprise security policies to be implemented. Place the SSL1000 in front of your TN3270 servers (or in the rack right above them), configure upstream and downstream TCP/IP addresses and ports, and you've got the security of 128-bit 3DES encryption, compatible with the built-in security of Visara NCTs, IBM Personal Communications, Attachmate Extra, and many other TN3270 and Telnet emulators. It can provide SSL security for Visara console concentrators, or any other lan attached server, including IBM 2074s or the mainframe itself. Why waste your most expensive MIPs doing SSL encryption?

With no requirements for a keyboard, monitor or mouse, the SSL1000 is managed locally or remotely with a web browser. You can monitor and log who is connected, when, and for how long. It also includes automatic failover to an alternate server - which you can configure independently for each session.

Whether your data travels across the Internet or just across the room, wired or wireless, you'll have protection from LAN monitoring, and intrusive hackers with the Visara SSL1000.

# SSL1000 Security Appliance

## Product Specifications

- 1U rack-mountable unit, 2+Ghz Pentium 4
- Includes two 10/100/1000 ethernet connections
- 1000 simultaneous sessions
- Supports 128 bit Secure Socket Layer (SSL 3.0) and 168 bit Transport Layer Security (SSL 3.1)
- Provides automatic failover when a connection is made - if the connection to the primary server fails, the connection is redirected to the configured backup server. Every path defined can have a unique primary and backup server.
- Configurable List of authorized client IP addresses and subnets
- Configurable Primary and Alternate server IP addresses
- Connection can be configured for no encryption to do a passthrough for “trusted” users, and for clients that don’t support SSL.
- Management of the unit is by Telnet client or Web Browser:
  - Management is password protected.
  - Browser access is secure (HTTPS).
  - Configuration can be modified without restarting the Gateway application (current connections not affected)
  - Display who is currently connected to which server
  - Configurable inactivity timer that would disconnect an idle client
  - Manually disconnect a client
  - Manually restart the GW application, or reboot the whole GW unit
- Logging of all connections/disconnections/lost connections, etc.
- SSL Certificate management provides a self-signed server certificate, and the ability to import one from a recognized Certificate Authority

“Check Box” interoperability has been tested with the following TN3270 Clients (Meaning that all you have to do to secure the connection is check the SSL Encryption configuration item in the client setup. The client may require installation of our SSL Certificate.)

- IBM Personal Communications
- Attachmate EXTRA
- Hummingbird HOST EXPLORER
- Visara 1883
- Zephyr PASSPORT
- SDI TN3270 PLUS