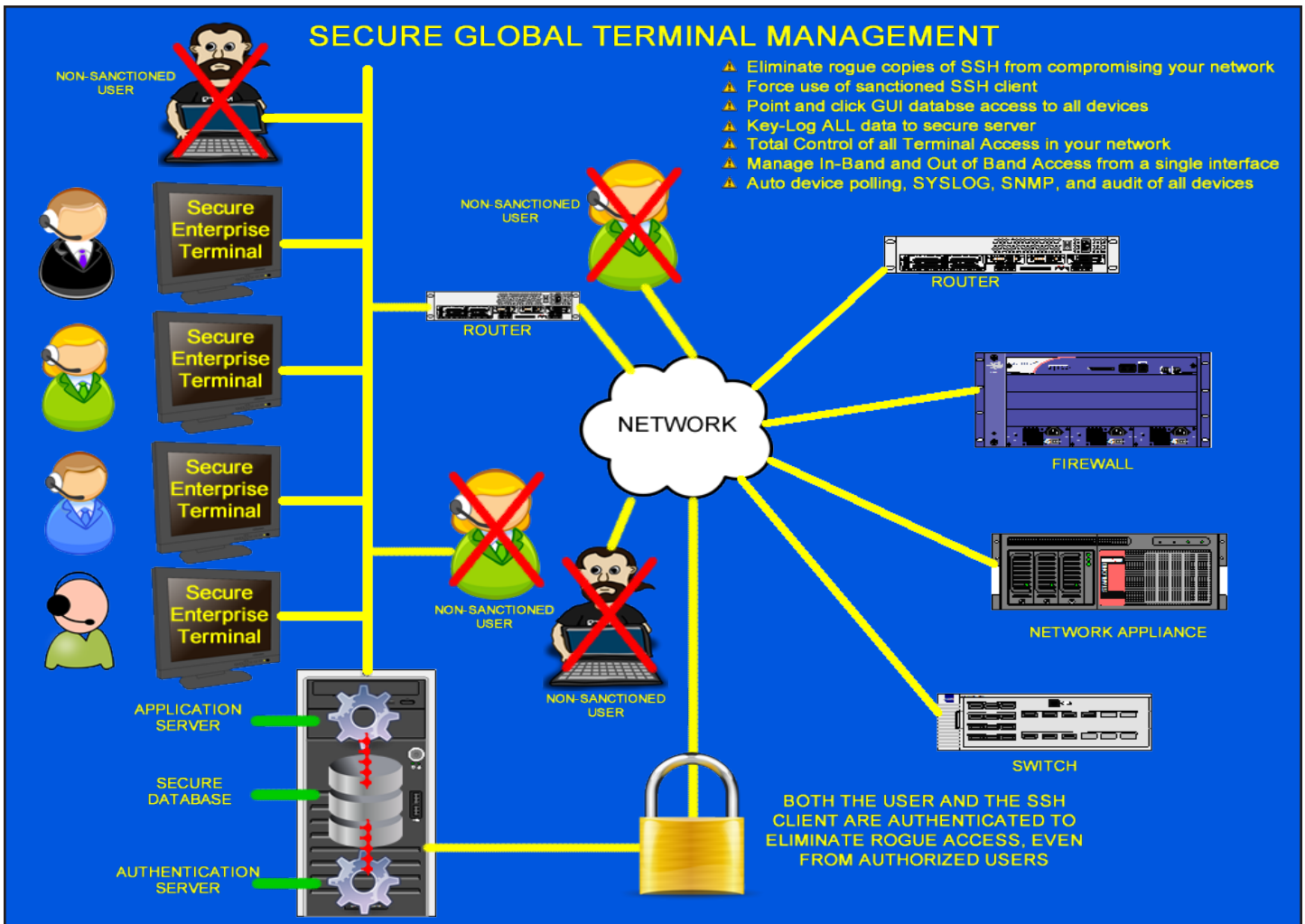




The addition of the Secure Global Terminal Management “GTM” to the Out of Band Manager “OBM”, provides a complete terminal access system that manages all SSH connections, In Band and Out of Band, from a single database and client “cockpit” view. The system also addresses the current haphazard nature of SSH clients and closes a potential security hole with open source SSH clients.

- OBM provides a single “cockpit” control of all the SSH connections on the network. All terminal access can be performed through one application.
- The OBM uses Client Server topology so all database information is stored securely in a central SQL database.
- Role Based Security allows granular control over functions allowed for each engineer or administrator.
- Terminal Access Discovery feature that finds all SSH, Telnet, and browser access on a network and places those devices in the database.
- All Sessions are Two Factor Authenticated to ensure that they are originating from the OBM Manager. This ensures that no rogue copies of SSH can access the network elements.
- All SSH session are “Keystroke Logged” to ensure that all functions performed on the network element are recorded and time-stamped with user information.
- The Network Administrator and/or Security Administrator is now sure that all SSH access is centrally authenticated, audited, and logged.
- All devices are periodically contacted (PING, Telnet, or SSH) to ensure they are responding. Errors can be sent off to Syslog or SNMP engines.



Terminal Access

is accomplished through the GUI interface. When an operator double clicks on a device, they are prompted with a connection preference (SSH, Encrypted Network, Encrypted Dial-up, or GPRS cellular) and then connected to the remote device through that interface. The operator can be authenticated in a number of ways and Encrypted using up to 256 bit AES CFB encryption.

