Securing Calls to the PSTN

These steps should be taken at every installation. No IP network should be considered secure - people plug in unprotected wireless bridges under their desks, computers are routinely compromised by Trojan programs, and firewalls have long lists of published and unpatched holes in them. The purpose of these precautions is to protect your system from unauthorized calls that you may have to pay for.

1. Every PSTN gateway must be configured to have an access list such that it will not accept any IP call toward the PSTN that does not come from the IP address of some sipXecs proxy: see the documentation for your gateway for how to configure this.
2. The sipXecs users and groups should define who has the permissions to make PSTN calls. In the default configuration, this includes LongDistance, RestrictedCalling, LocalCalling, etc.
3. Every dial plan that routes to a gateway must define some required permission for any billable call. Since most business services charge even for local calls, this means that every dial rule that goes to a gateway - *except the Emergency Dialing (911) rule* - must include some required permission.
4. Any SBC or other entry point for SIP requests into the network must be configured so that it always routes any call to the sipXecs proxy. That puts the proxy in position to enforce the calling rules.
5. Authentication must not be disabled in the authproxy - there is a way to do this, but it is there only for development testing purposes and should never be done on any system with access to the PSTN.