# Foreword

As one of the first technologies employed to protect networks from unauthorized access, the firewall has come to exemplify network security. While an overall security strategy requires the harmonious integration of people, process, and technology to reduce risk, there is no doubt that firewalls can be a very valuable security tool when properly implemented. Today, the use of firewalls has become such an accepted practice that their deployment in one fashion or another is virtually a foregone conclusion when designing and building networks. Recognizing this need, Cisco Systems has developed and continues to improve upon its line of PIX firewalls. These systems have steadily gained market leadership by demonstrating an excellent mix of functionality, performance, and flexibility.

Firewalls have become increasingly sophisticated devices as the technology has matured. At its most basic level, a firewall is intended to enforce a security policy governing the network traffic that passes through it. To this basic functionality, Cisco has added many features such as network address translation (NAT), virtual private networks (VPN), and redundant architectures for high availability. Management systems are typically installed along with the firewall to assist with monitoring and administrating the device. A maxim of IT security is that technology is only as effective as the people responsible for its operation. Therefore, it is extremely important for the technical staff managing PIX firewalls to understand the technical functionality of these devices, as this will result in better security and more efficient operation of the equipment.