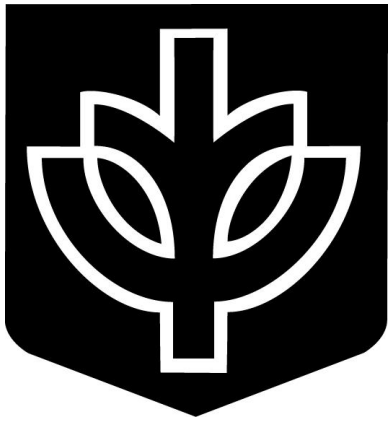
FIREWALL CHANGE CONTROL POLICIES AND PROCEDURES



Information Security Team
DePaul University
1 East Jackson Boulevard
Chicago, Illinois 60604 US
https://infosec.depaul.edu/

13th December 2002

Copyright Notice

Document Classification

This document is classified as **sensitive** according to the DePaul University Information Security Team classification guidelines [1]. This document may be distributed, either whole or part, to the University community as per the guidelines stated in section titled *Copyright Notice*. Distribution outside the University requires prior consent of the DePaul University Information Security Team.

Revision

Revision 1.4, created 2002/12/13 22:12:24 (UTC).

Contents

1 Summary

Firewalls act as access control devices and are often integrated into network and system designs to control access from a centralized position. These devices assist in building a comprehensive “defense-in-depth” strategy towards securing an organization’s assets. The DePaul University Information Security Team (INFOSEC) has determined the procedures in this document to be the best policies and procedures currently for controlling management requests of firewalls and other access control devices, and should be used by managers of such devices.

2 Roles

Proper delegation of authority for changes to critical security devices such as a firewall requires roles to be defined. There are three roles defined in this document:

1. Firewall Manager: responsible for normal administration and monitoring of the device(s).

2. Request Liaison: a person properly authenticated and authorized, through the steps listed in this document, to make change requests to the firewall managers.

3. Authentication Authority: a trusted body entitled to designate a request liaison.

These roles are more clearly defined in the following sections.

2.1 Firewall Manager

The Firewall Manager is responsible for daily administration of the firewall and represents the only technical authority to make changes to the system, whether the system be an access control device or a logical firewall. A person elected or assigned the responsibilities of Firewall Manager should be chosen based on security experience and understanding of network and security principles.

2.2 Request Liaison

A Request Liaison is a person nominated to the Authentication Authority. The initial nomination and second may be performed by the following personnel.

- Division Director
- Division Manager
- Current Liaison
- INFOSEC Member

Nominations may occur at anytime to the Authentication Authority. The second nomination *must occur* within seventy-two (72) hours of the initial nomination. All nominations require a digital signature be made with a publicly available digital key. A person cannot nominate or second themselves. The term length for a Request Liaison is one (1) year. A Request Laision may hold a maximum of ten (10) consecutive terms.

Nominations that do not occur as per these guidelines will be silently discarded by the Authentication Authority.

2.3 Authentication Authority

The Authentication Authority is a trusted body entitled to designate or revoke Request Liaison status, generate and/or sign encryption keys for secure communications, and mitigate conflicts of interests between the Request Liaison and Firewall Manager.

Within DePaul University INFOSEC is the primary Authentication Authority, though other Authentication Authorities may be organized. The Authentication Authority *must* have a public key export to *at least* three (3) major public key servers.

3 Encryption

Encryption is used to security "scramble" data to save it from prying eyes. Electronic mail is an insecure medium for transmitting private, sensitive information. By the proper use of encryption, email may act as the transport for encrypted information.

3.1 Key Signing

Proper key signing by the Authentication Authority will allow communication between the Request Liaison and Firewall Manager, both of which may be under different Organizational Units, to be trusted. The Authentication Authority requires that a public key be submitted for each Firewall Manager and Request Liaison. This key will be signed with an exportable signature valid for one (1) year. The Authentication Authority may require proper identification through a valid drivers license, state identification or passport. A University ID card *will not* be considered a valid form of identification.

Communication between the Firewall Manager and Request Liaison should be performed using strong asymmetric encryption. A digital signature should be trusted only when checking with the exported key signed by the Authentication Authority.

3.2 Algorithms

At this time, the following cipher algorithms are recommended for encrypted communication.

- `3DES`
- `CAST5`
- `AES, AES192, AES256`
- `TWOFISH`

The following list of hash algorithms are recommended for providing digital signatures.

- `MD5`
- `SHA1`
- `RIPEMD160`

4 Change Requests

Change request communication should occur between the Request Liaison and Firewall Manager securely via encrypted email. Requests *must* be digitally signed by the Request Liaison. It is the responsibility of the Firewall Manager to verify this signature to be correctly made with the exported key received from the Authentication Authority.

4.1 Time Requirements

The Request Liaison should allow the Firewall Manager forty-eight (48) hours to analyze the request and make the policy change, where possible. Policy changes to the firewall may not be possible if the change requires alteration of an exisiting configuration, or may cause service interruption. In this situation, the Request Liaison and Firewall Manager should plan to make such changes during the normal maintenance window.

References

[1] Sensitive Information and Data Security Classes
The DePaul University Information Security Team
Pancer, E., Request for Comments No. 0303, May, 2002