

Revisions in response to committee members' comments and suggestions:

1. Suggestion: add a discussion about the feasibility of proxy network-based DoS defense (regarding hiding the application's IP address).

Revision: revised Section 1.2, Section 2.2.2, and Section 3.2. Clarify that the proxy network-based DoS defense does not require the application's IP address to be hidden. It is sufficient to ensure that the proxy network is the only public interface for the application. (For example, an application can reside behind a distributed set of filters which blocks all packets except for those coming from a specific set of application proxies.)

2. Suggestion: add a discussion about the feasibility of large resource pool in practice.

Revision: added a discussion in Section 2.2.2, giving examples of large overlay networks, such as Akamai, Skype, and BitTorrent to justify our assumption of large resource pools.

3. Suggestion: add a section about deployment issues of proxy networks.

Revision: added Section 8.3. Discuss the key challenges in proxy network deployment, including:

- management and maintenance – installation and update of software packages and system configuration management for all the hosts in the system
- performance management – how to deploy a large proxy network system in a dynamic Internet environment to deliver good, predictable application performance
- diagnosis – how to detect and identify the cause(s) of performance anomalies as well as failures in a large proxy network system