



Technical Bulletin – Network Security / Denial of Service attacks

Issued: September 2004

Last revised: September 2004

Bridges web products employ many technologies to ensure system security and prevent denial of service attacks¹;

- Firewalls and intrusion detection (network and host);
- Two-factor system authentication for administrative access;
- Page view rate monitoring technology to prevent HTTP denial of service attacks

Offending users are identified by IP address and site authentication information; depending on the nature and severity of the attack, user's access to Bridges' network services may be blocked.

To prevent automated downloads ('slurping') of Bridges' web products, the rate of page views for each individual user is monitored; should that rate exceed a humanly possible threshold, the offending user's information (site id, IP address) is logged and their current session terminated.

¹ A 'denial of service' attack is an attempt to prevent legitimate users of a service from using that service. A full definition can be found at [CERT](#)