**Divide and Defend Firewall**

**By Walter Gress**

Firewall Aspects Overview

1. **The central idea is to have the firewall and its components in linked modules, making it harder to attack.**
2. **The Core, the Main Firewall controlling software is isolated from the rest of the network, inaccessible through any outside ports.**
3. **The D&D firewall uses micro or mini firewalls to block incoming ttacks. Being small and lightweight allows them to not only react quickly, there are multiple to handle multiple attackers, and should they crash they are lightweight enough that a new mini firewall can be thrown up again against the core.**
4. **A data abstraction layer exists between the Core and the “mini” firewalls that are created to defend against attacks. This DAL acts like a proxy, functioning ideally as the gateway portion of the firewall.**
5. **Each thread spawned by the DAL has firewall software running or “attached to” the thread.**
6. **When one mini firewall goes down, the Core (main firewall) immediately respawns a mini-firewall through the DAL.**
7. **Since the mini-firewalls take up little resources, they can be spawned, respawned, and so on again and again taking much effort to crash the host computer.**
8. **When a mini-firewall is generated, it generates according to the hostname and port currently being attacked. If other hostnames and ports are attacked, additional mini firewalls are spawned.**
9. **Since the Main Firewall (Core) software managing the mini firewalls is isolated, the enemy is unable to easily penetrate and attack the Core and in essence, for an analogy, “swats away flies”, the flies being the bots attempting at breaking into the system, the flyswatter(s) being the mini-firewalls.**