**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.**

Note to self: Look into Load Balancing

1. Firewall core hidden behind dummy host.

2. Spawns micro-firewall from monolithic core to block enemy attack on the dummy host ip address and then shifts dummy ip address to another (these dummy ip addresses are the address info for the Data Abstraction Layer). If a new dummy host attack occurs, the main firewall generates another micro-firewall and shifts the DAL’s dummy ip, and so on….This part I’m not sure of how to do: how to shift the DAL’s ip address. I considered adding another proxy, one proxy only outgoing and the other tying together Instead of changing the ip address of the DAL, change the connection between the DAL and this new, internal proxy. That way should the attacker try to attack , he wouldn’t get beyond the dummy proxy. (DAL)

3. When not under attack, the DAL operates as a normal gateway between the internal and external networks.

The main firewall core control all of the mini/micro firewalls that are spawned as threads from it.

The micro-firewalls are lightweight threads due to the fact that as few resources as possible are available in defense of a botnet attack.

**Example:**

Dummy IP Gateway (shifts ip addresses on attack)

(for example, on attack to its ip as 192.168.1.1 it will throw up a firewall on a thread and shift over to a new address, ex: 192.168..12.15

Performs Proxy duties for the Firewall

Legitimate., monolithic firewall

This firewall manages the lightweight, micro firewalls

LAN/WAN

Attack on 192.168.1.245

Microfirewall

To temp stop (block) attack

Alternative Firewall Using Double Proxy

**Example:**

Dummy IP Gateway (DAL)

Performs Proxy duties for the Firewall

Outgoing and incoming data IPs – static ips

Incoming go to the next proxy

LAN/WAN

Attack on 192.168.1.245

Microfirewall

To temp stop (block) attack

Another Dummy Proxy in the chain, however

“INNER PROXY”

Traffic goes out to DAL and out to the rest of the world through these two proxies.

Should we be attacked, the connection between the two will not be severed, but the outgoing address between the DAL and INNER PROXY will shifted while micro/mini firewalls block the attacker

Attacks, that is, the connection between this and DAL

Legitimate., monolithic firewall

This firewall manages the lightweight, micro firewalls. Leaves the actual blocking of ports to the micro-firewalls and the proxy through to the DAL and the INNERPROXY