By Marcus Ranum

The Ultimately Secure DEEP PACKET INSPECTION AND APPLICATION SECURITY SYSTEM
Featuring signature-less anomaly detection and blocking technology with application awareness and layer-7 state tracking!!!

Now available in Petabyte-capable appliance form factor!*

(Formerly: The Ultimately Secure INTRUSION PREVENTION SYSTEM
Featuring signature-less anomaly detection and blocking technology!!)

[attention: You may have noticed that this is just an old article that I wrote in 1994, with the title changed. This, in itself, is a metaphor for the whole Intrusion Prevention market hype. What you're getting, thanks to Gartner's unrestrained hyping of this non-existent not-ready-for-prime-time "concept technology" is that everyone who has something old that can be re-branded as ***intrusion prevention*** is rushing to update their powerpoints. I felt it was only right that I follow suit.]

The Ultimately Secure
DEEP PACKET INSPECTION AND APPLICATION SECURITY SYSTEM

By Marcus Ranum

(Formerly: The ULTIMATELY Secure Firewall Stateful Adaptive Packet Destruction Enterprise-Class Gigabit Intrusion Prevention System)

Installation Instructions

- **For best effect** install the firewall between the CPU unit and the wall outlet. Place the jaws of the firewall across the power cord, and bear down firmly. *Be sure to wear rubber gloves while installing the firewall* or assign the task to a junior system manager. If the firewall is installed properly, all the lights on the CPU will turn dark and the fans will grow quiet. This indicates that the system has entered a **secure state**
- **For Internet use** install the firewall between the demarc of the T1 to the Internet. Place the jaws of the firewall across the T1 line lead, and bear down firmly. When your Internet service provider's network operations center calls to inform you that they have lost connectivity to your site, the firewall is correctly installed.

If I had a dollar....

If I had a dollar for every time I've seen someone post "I need a 100% secure firewall, that lets me do everything" I'd be retired by now.

The fact is, that if you're connecting your network to anything else, you're running a risk. Period. Usually, that risk can be reduced, often dramatically, by employing basic security precautions such as firewalls. **But** a firewall is a *risk reduction* system, it is not a *risk mitigation* system -- there is, always, some danger that something can go fatally wrong with anything built by humans.

The firewall above is the only 100% *guaranteed* secure solution.

(* May have a performance impact on traffic if prevention is enabled)