

## Re: IPS, alternative solutions

**Source:** <http://www.derkeiler.com/Mailing-Lists/securityfocus/focus-ids/2004-09/0096.html>

---

**From:** Devdas Bhagat ([devdas\\_at\\_dvb.homelinux.org](mailto:devdas_at_dvb.homelinux.org))

**Date:** 09/26/04

Date: Sun, 26 Sep 2004 06:04:36 +0530

To: [focus-ids@securityfocus.com](mailto:focus-ids@securityfocus.com)

On 22/09/04 12:22 -0400, Mike Frantzen wrote:

>

> > *The way I see it, an IPS can attempt to contain your infestation and help reduce your legal exposure from outbound attacks that would otherwise make it to your partners... This is a value I can quantify and the best use case I have seen for IPS. The problem I have with it is that a properly implemented firewall can most likely do the same and provide much better overall value.*

>

> *One of the spots where an IPS beats a firewall hands down is on the interior of a large organization. I've seen too many large disfunctional companies that compartmentalize their departments by placing firewalls between each and every one. Marketing and sales can't*

Which is broken behaviour in the name of security. People who need access to certain data for normal work related purposes must be given such access. Those who don't need access should not be given such access.

I believe that this type of issue is largely caused by people equating firewalls with simple packet filters.

> *access engineering project schedules and feature lists on the engineering web server. Engineering can't access the support database to look for common issues and trends. No one can access their department's machines from their laptop when in a conference room... etc etc*

Actually, that is broken firewall design and/or implementation. If the requirements of the various customers are not met, then the firewall is just an impediment to work, or it lets too much traffic through.

In such cases, the company should be using proxies with proper authentication and logging to regulate traffic flow (IMHO firewalls should be a combination of packet filters and proxies anyway).

>

> *We end up with an authoritarian system where the firewalls inhibit the*

## SecurityFocus IDS: Re: IPS, alternative solutions

- > *communication inside the company. An IPS can maintain the security*
- > *compartmentalization and containment without impeding the free flow of*
- > *information between departments.*

No. an IPS is just an attempt at a proxy looking for bad things. In my book, this is equivalent to filtering untrusted user input for bad stuff instead of limiting it to known good stuff and removing the rest.

This should not be acceptable behaviour for security enforcement management and/or personnel.

Devdas Bhagat

---

Test Your IDS

Is your IDS deployed correctly?

Find out quickly and easily by testing it with real-world attacks from CORE IMPACT.

Go to [http://www.securityfocus.com/sponsor/CoreSecurity\\_focus-ids\\_040708](http://www.securityfocus.com/sponsor/CoreSecurity_focus-ids_040708) to learn more.

---