

## High performance IDS/Firewall

**Source:** <http://unix.derkeiler.com/Mailing-Lists/FreeBSD/performance/2003-05/0025.html>

---

**From:** Michael Conlen (*meconlen\_at\_obfuscated.net*)

**Date:** 05/28/03

Date: Wed, 28 May 2003 17:54:07 -0400

To: freebsd-performance@freebsd.org

I'm considering setting up a FreeBSD firewall/IDS system to handle 60-80Mbit/sec of traffic. The box would have three adapters, two of them bridging and one for access. I will place the IDS on the outside bridge interface and apply IPFW rules on the system as needed. My concern is what the failure order is if the system is under heavy load. My preferred order would be

snort (libpcap) drops packets and snort fails to detect  
firewall fails to block  
system drops packets

as it's more important for the system to be running than to identify or block the things we are trying to identify and block.

Is this the order things would fall over, or am I likely to cause the system to drop packets as soon as things get ugly.

PS: I'm considering a dual p4 2Gz 4GB of memory system, and SCSI-3 disk subsystem. and there's only one server on the "inside" of this network, so I don't think I'll have a major failure situation, unless someone suddenly generates over 20Mbit of DOS traffic, and those people usually go after the router...

--

Michael Conlen

---

freebsd-performance@freebsd.org mailing list

<http://lists.freebsd.org/mailman/listinfo/freebsd-performance>

To unsubscribe, send any mail to "freebsd-performance-unsubscribe@freebsd.org"