

RE: IPS Comparison

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2005-07/0314.html>

From: Security Focus (*Security.Focus_at_comcast.net*)

Date: 07/26/05

To: <dmecham@nitrosecurity.com>, <pen-test@securityfocus.com>

Date: Tue, 26 Jul 2005 04:43:55 -0500

Actually, any IPS that is deployed as a Syn-Proxy in Bridging mode has this same functionality, there are several out there that perform this function and don't even bother to mention it as it has become standard fare. One that I'm very familiar with that does market this feature is Melior, Inc.'s Barbican appliance www.ddos.com, they call it "cloaking". This is also their primary method for defeating pen-test attempts. All of these appliances are known to be limited in the number of TCP connections they can handle and are primarily solutions for smaller enterprises, hence the evolution of ASIC solutions for the larger enterprise. My favorite Intel/*nix inline solution these days is Reflex Security; I've implemented it at small and mid-size banks, and to date it has been the most effective, simplest and least expensive solution for IDS/IPS that I've encountered; my customers love it. www.reflexsecurity.com

The IDS focus list has covered IPS questions such as IP or no IP very extensively, you'd very well served by scanning that list for related discussions as many of the vendors' CTOs have chimed in to discuss the logic behind their chosen configurations and most importantly their customers as well.

-MD

Feel free to ask me offlist about the best kept secret in Certification Training CertTest.com CISSP, PMP, CISA/CISM, NSA IAM/IEM, BCP. If you or your people need to Cert up, this is the place to go. Their HQ office is right next door to me, I've seen first hand what a crack job these guys do.

-----Original Message-----

From: Darwin [mailto:dlmecham@gmail.com]

Sent: Monday, July 25, 2005 11:56 PM

To: pen-test@securityfocus.com

Subject: IPS Comparison

Hi,

Regarding IPS products.

SecurityFocus Penetration: RE: IPS Comparison

Take a look at <http://www.nitrosecurity.com>

This IPS is deployed without an IP address making it invisible.

Best Regards,

Darwin Mecham, CISSP