

Firewall-Wizards: RE: IPS (was: [fw-wiz] Sources for Extranet Designs?)

RE: IPS (was: [fw-wiz] Sources for Extranet Designs?)

Source: <http://www.derkeiler.com/Mailing-Lists/Firewall-Wizards/2004-02/0239.html>

From: Christopher Lee (*clee_at_myhome.homeip.net*)

Date: 02/27/04

To: "'Stiennon, Richard'" <Richard.Stiennon@gartner.com>, "'Ben Nagy'" <ben@iagu.net>, <firewall-wizards@honor.icsalabs.com>
Date: Thu, 26 Feb 2004 22:44:35 -0500

Just an FYI. Radware's DefensePro (or its IPS add-on on their platform, in general) does not do packet re-assembly (i.e. reconstruction of the data streams/sessions), it merely does string-matchings on the packets alone. I don't know Netscreen IDP, but I am curious to know if (and how) it actually reassembles packets before its inspection...

Chris

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

From: firewall-wizards-admin@honor.icsalabs.com
[mailto:firewall-wizards-admin@honor.icsalabs.com] On Behalf Of Stiennon, Richard
Sent: February 26, 2004 12:51 PM
To: Ben Nagy; firewall-wizards@honor.icsalabs.com
Subject: RE: IPS (was: [fw-wiz] Sources for Extranet Designs?)

Here are the definitions I am working with:

Network IPS:

An inline device that assembles packets into streams or sessions and parses them.

Multiple methodologies to determine malicious intent. Usually includes signature, protocol anomaly, behavior and flow capabilities.

The ability to drop sessions associated with attacks. Note, this is dramatically different than a firewall that can close *connections* based on source-destination-port.

Definitions are often helped out by a set of reference vendors. In my mind, Tippingpoint, TopLayer, Radware, NAI Intrushield, Netscreen IDP, Reflex Security and even Checkpoint Intrespect all fit this definition.

Host IPS:

A software shim (firewall) that sits between the kernel and the application.

RE: IPS (was: [fw-wiz] Sources for Extranet Designs?)

Firewall-Wizards: RE: IPS (was: [fw-wiz] Sources for Extranet Designs?)

System calls are intercepted and blocked if they are outside the "allow" policy. Much simpler space with only three vendors, Cisco Secure Agent (was Okena), NAI Enterscept, and Sana Security. A start up called Araksha is also looking at this space but they go much deeper into the application at run time.

The firewall vendors are excited by IPS because it is a product that can be deployed deep inside a network. Initial traction is being gained at public universities, mostly in the US where there is an objection to firewalls based on "academic freedom". Some of the network IPS vendors are profiting from the need to throttle undesirable traffic (file sharing) at universities.

Best,

–Richard Stiennon

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

From: firewall-wizards-admin@honor.icsalabs.com
[mailto:firewall