

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/2004-02/0243.html>

---

**From:** Kowsik Guruswamy (KGuruswa\_at\_netscreen.com)

**Date:** 02/27/04

To: "'Christopher Lee'" <clee@myhome.homeip.net>, "'Stiennon,Richard'" <Richard.Stiennon@gartner.com>  
Date: Fri, 27 Feb 2004 09:33:04 -0800

Pretty much any layer-7 processing for TCP traffic mandates TCP stream reassembly. Looking at TCP segments, one at a time, really doesn't get you anywhere.

Yes, Netscreen IDP does perform reassembly [and a lot more] before inspection.

K.

ps: I work for Netscreen.

> -----Original Message-----

> From: Christopher Lee [mailto:clee@myhome.homeip.net]

> Sent: Thursday, February 26, 2004 7:45 PM

> To: 'Stiennon,Richard'; 'Ben Nagy';

> firewall-wizards@honor.icsalabs.com

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

>

>

> 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

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

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

- > *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.*
- > *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,*

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

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

>  
> -Richard Stiennon  
>  
>  
> -----Original Message-----  
> From: firewall-wizards-admin@honor.icsalabs.com  
> [mailto:firewall-wizards-admin@honor.icsalabs.com]On Behalf  
> Of Ben Nagy  
> Sent: Thursday, February 26, 2004 9:06 AM  
> To: firewall-wizards@honor.icsalabs.com  
> Subject: RE: IPS (was: [fw-wiz] Sources for Extranet Designs?)  
>  
>  
> Can I just jump in and ask what *\_exactly\_* people think "IPS"  
> means? I know  
> I'm asking for a definition debate and we've all seen a bunch  
> of those over  
> the years, but I'm concerned that the "buzzword" factor has lead to  
> compression in terms of vocab.  
>  
> I don't see the basic "attach an IDS to a firewall and have  
> the firewall do  
> stuff based on signatures" concept as amazingly useful (my personal  
> opinion). However lots of companies are producing stuff which  
> they are also  
> calling IPS (us included; consider that a disclaimer).  
>  
> Intrusion Prevention can be done at a number of places  
>  
> 1. The Firewall  
> 2. The Network (inline IPS lives here)  
> 3. The Host (cross platform issues here!)  
> - 3a. The Host Network level (TDI or driver stuff, where the  
> current PFWs  
> live)  
> - 3b. The Host Kernel / Memory Mangement level (systrace,  
> pax, and their  
> windows friends)  
>  
> Of those places, we can work on  
>  
> 1. Attack Signatures (easy to evade, prone to false  
> positives, reactive)  
> 2. Anomaly detection (statistical stuff, less configuration, foolable)  
> 3. Rule Based (hard to program, slower, better suited to a host model)  
> 4. Traffic / rate based.  
>  
> There is a lot of technical depth to the pros and cons of  
> each approach [1].  
> My own opinion is that the problem of malware, worms and the  
> newer attack

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

- > *vectors (VPN, wireless, laptops etc) pretty much makes it*
- > *pointless to focus*
- > *too much on FW based IPS.*
- >
- > *Basically, firewalls are perimeter based, have huge problems*
- > *coping with*
- > *threats that are above the network level, and it's always*
- > *going to be hard*
- > *work to stretch their capacities. Witness the profound marketing and*
- > *technical failure of the proxy firewall, for example. (ok,*
- > *maybe that sounds*
- > *like a troll. ;)*
- >
- > *However, even the crappiest personal firewall has a*
- > *reasonable chance to*
- > *contain malware by using application firewalling (this app*
- > *can bind ports*
- > *this one can't). The ways that is being approached today is pretty*
- > *primitive, and there is a lot of work to do – yes – but it's*
- > *a start. I see*
- > *future potentiallllllll in an anomaly based approach which*
- > *can really step*
- > *in at the network level – buuut...*
- >
- > *Anyways, I'll restrict the rant, but the point is that it's*
- > *an overused*
- > *term, it's Gartnerised, but it's genuinely interesting. I'd*
- > *love to hear*
- > *some of your opinions about the viability of the various approaches –*
- > *because it's fairly clear that we need \_some\_ new approach.*
- >
- > *ben*
- >
- > *[1] European readers with too much time on their hands could*
- > *come and hear*
- > *me waffle about this at Infosecurity Europe. Those of you out*
- > *there who know*
- > *more about this than I do are welcome to clue me up in advance. ;)*
- >
- > > -----Original Message-----
- > > *From: firewall-wizards-admin@honor.icsalabs.com*
- > > *[mailto:firewall-wizards-admin@honor.icsalabs.com] On Behalf*
- > > *Of Don Parker*
- > > *Sent: Tuesday, February 24, 2004 12:00 AM*
- > > *To: Marcus J. Ranum; Wes Noonan; 'Baumann, Sean C.'; 'R. DuFresne'*
- > > *Cc: 'Paul Robertson'; firewall-wizards@honor.icsalabs.com*
- > > *Subject: RE: [fw-wiz] Sources for Extranet Designs?*
- > >
- > > *Yes indeed IPS is an excellent technology that is slowly*
- > > *maturing. There is still nothing wrong with the IDS though.*
- > > *[...]*

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

>>  
>> *On Feb 23, "Marcus J. Ranum" <mjr@ranum.com> wrote:*  
>>  
>> *Wes Noonan wrote:*  
>> *>IPS would be a no brainer for me in this scenario.*  
>>  
>> *I. Hate. To. Admit. It. But. You. May. Be Right.*  
>>  
>> *IPS hype aside, and ignoring what the Gartner idiots think,*  
>> *there's a conceptual value to the IPS concept. Basically, a*  
>> *firewall implements one of 2 policies:*  
>> *- Permit*  
>> *- Deny*  
>>  
>> *IPS (i.e.: a signature-based firewall) adds a third option to*  
>> *the policy matrix:*  
>> *- Permit*  
>> *- Deny*  
>> *- Permit it as long as it is not obviously abusive*  
>> *(e.g.: signature*  
>> *hasn't fired)*  
>  
>  
> \_\_\_\_\_  
> *firewall-wizards mailing list*  
> *firewall-wizards@honor.icsalabs.com*  
> <http://honor.icsalabs.com/mailman/listinfo/firewall-wizards>  
>  
> \_\_\_\_\_  
> *firewall-wizards mailing list*  
> *firewall-wizards@honor.icsalabs.com*  
> <http://honor.icsalabs.com/mailman/listinfo/firewall-wizards>  
>  
>  
> \_\_\_\_\_  
> *firewall-wizards mailing list*  
> *firewall-wizards@honor.icsalabs.com*  
> <http://honor.icsalabs.com/mailman/listinfo/firewall-wizards>  
>

\_\_\_\_\_  
firewall-wizards mailing list  
firewall-wizards@honor.icsalabs.com  
<http://honor.icsalabs.com/mailman/listinfo/firewall-wizards>