

Re: IDS\IPS that can handle one Gig

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/focus-ids/2005-06/0017.html>

From: Ed Gibbs (ed_at_digitalconclave.com)

Date: 06/02/05

To: "Palmer, Paul (ISSAtlanta)" <PPalmer@iss.net>, <THolman@toplayer.com>, <prashant@juniper.net>
Date: Wed, 1 Jun 2005 15:22:54 -0700

Paul,

It has been proven over and over again that networking platforms built on the PC architecture does not perform equally to a ASIC/FPGA platform. Netscreen Firewall was a great example of how a ASIC/FPGA product could outperform anything Check Point could provide on Intel (including the Nokia/Check Point PC appliance!), especially with 64-byte UDP packets. IMHO, anyone placing a security device built around the PC architecture "in-line" is asking for trouble. Would you replace your purpose-built Cisco routers with PCs running Linux/Zebra? Of course not. Do you want an appliance with a hard-drive "in-line" on your network. No again. What happens when the H/D crashes, or in the case of financial/government entities, what if the appliance is physically stolen and configuration/alerts/etc, are on that H/D? That's happened.

McAfee IntruShield and TippingPoint UnityOne so far have proven performance in gig environments. Both products are built using ASIC/FPGAs and can outperform anything built on a PC to date. There's no compromising by disabling signatures to gain performance – both products really don't care if you have every signature and then some on.

–Ed

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

From: "Palmer, Paul (ISSAtlanta)" <PPalmer@iss.net>
To: <THolman@toplayer.com>; <prashant@juniper.net>; <focus-ids@securityfocus.com>
Sent: Wednesday, June 01, 2005 9:20 AM
Subject: RE: IDS\IPS that can handle one Gig

Tim Holman states:

- > *Agreed – with a system based around PCI / Intel architecture*
- > *(eg Netscreen IDP, Check Point Interspect/Smart Defense, Cisco*
- > *4200, ISS Proventia to name but a few), then it makes sense to*
- > *turn off various checks to improve performance, but at what*
- > *cost to security?*

SecurityFocus IDS: Re: IDS\IPS that can handle one Gig

This is not a valid conclusion. Whether or not you see performance gains by disabling checks does not correlate with the chipsets used. Some of the products you mentioned show consistent performance regardless of which checks have been enabled. In contrast, some of the "ASIC" technology products DO show significant performance differences depending on which checks are enabled.

Anyone making a decision based solely upon the perceived advantages of the advertised technology of the product is likely to be disappointed.

Paul

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

From: THolman@toplayer.com [mailto:THolman@toplayer.com]
Sent: Tuesday, May 31, 2005 6:54 PM
To: prashant@juniper.net; focus-ids@securityfocus.com
Subject: RE: IDS\IPS that can handle one Gig

Hi Prashant,

Agreed – with a system based around PCI / Intel architecture (eg Netscreen IDP, Check Point Interspect/Smart Defense, Cisco 4200, ISS Proventia to name but a few), then it makes sense to turn off various checks to improve performance, but at what cost to security?

Is it acceptable to turn off vital security features just because the shiny new IPS system that you've just bought cannot handle doing too many things at once?

Of course not! ...and to be completely brutal, anyone reading this who comes across such a situation should send this equipment back to the reseller as being unfit for purpose. There are plenty of network IPS's that are designed to do the job in hand with built-in ASIC technology (eg McAfee, TippingPoint and TopLayer) and offer far more punch for the money.

There are a whole realm of attacks specifically designed to evade IDS/IPS devices through use of fragments. The theory being that with fragmented traffic, an attack can spread itself across multiple packets, which all get past string search engines that are looking for a complete string, rather than bits of it.

With an IDS, this isn't a problem – the IDS can sit to one side, observe the packets coming in, take note once it has seen a stream of fragments and reassembled them, and quite happily spend a couple of seconds catching up with other stuff before it sends alerts about any signature matches it finds in both normal and reassembled traffic.

However, with an IPS, you're supposed to be analysing network traffic at line speeds, and you do not have the luxury of hanging around whilst a machine designed for client/server purposes works out whether or not

Re: IDS\IPS that can handle one Gig

SecurityFocus IDS: Re: IDS\IPS that can handle one Gig

there's an attack concealed within fragments. After all, most fragmented traffic is genuine traffic – you need to let it through.

Fragmented traffic is a real security threat that needs addressing, and disabling security measures that take steps to reassemble and verify such traffic will cause a failure of just about any security audit you throw at your network, plus leave you open to litigation if your failure to address such attacks causes a 3rd party loss.

Regards,

Tim

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

From: Prashant Khandelwal [mailto:prashant@juniper.net]
Sent: 30 May 2005 06:03
To: focus-ids@securityfocus.com
Subject: RE: IDS\IPS that can handle one Gig

Adding to this conversation one relevant point would be, Policies which are pushed on the sensor makes big difference in the performance of the box.

E.g.: If Fragmentation and reassembly turned off it can be observed that box performs better as it does not need to take care of tiny fragmented packets (In real life having such policies doesn't make any sense).

Over all One should know the Claimed performance figures with avg packet size ,What type of traffic was used for achieving that particular performance figure ,What kind of policies were pushed on the sensor. This can really help to know how a particular IPS can fit in your network environment.

My 2 cents
Cheers
Prashant

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

From: THolman@toplayer.com [mailto:THolman@toplayer.com]
Sent: Thursday, May 26, 2005 2:17 PM
To: focus-ids@securityfocus.com
Subject: RE: IDS\IPS that can handle one Gig

Hi Randall,

Throughput is unimportant when it comes to choosing an IDS/IPS, and to be honest, a bit of a bun fight when you place two vendors side by side and start scouring their datasheets for practical information.

What is important, however, is the number of packets per second the device can process, the maximum number of connections that such a device

Re: IDS\IPS that can handle one Gig

SecurityFocus IDS: Re: IDS\IPS that can handle one Gig

keeps state for, and last but not least, the latency that such a device will introduce into your network if placed inline.

The smaller the packets used in a test, the smaller the performance in terms of megabits. The larger the packets, the bigger the performance in terms of megabits. Unreliable, and totally abused by most vendors on their datasheets. It's quite easy to say 'we support 1000 Mbps', only to say in small print the average packet size is 595 bytes. You only need to search Google for '1000 Mbps 595 bytes' and you'll soon find out what I mean..
;)

The vendor in question, although claiming Gigabit performance, can only setup TCP connections at a rate of 5,000 per second – if you do the math, you'll soon find out that this represents less than TEN MEGABITS per second in 'throughput' terms.

Is it ethical to claim Gigabit performance, only for the potential end user to run a number of tests with small packet sizes and find out this is not the case?

The moral of the plot is to never trust a datasheet – either thoroughly test the products before purchase, or look toward an independent testing house, such as NSS (www.nss.co.uk), whom have the resources and experience to regularly generate test results that count.

At TopLayer, we regularly deploy into Gigabit environments, and encourage the customer to test (using Smartbits, Ixia or Spirent) for peace of mind. Rest assured, each time they do this, we pass with flying colours, and this is what makes us one of the top market leaders in Gigabit IPS solutions.

Regards,

Tim

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

From: Randall Jarrell [mailto:rgj@msn.com]

Sent: 19 May 2005 16:28

To: focus-ids@securityfocus.com

Subject: IDS\IPS that can handle one Gig

Greetings,

We are currently evaluating IDS\IPS vendors. We have tried two vendors, whom I will not name unless you ask me, that have made claims that they can handle a Gig of throughput but actually start to fail around the 300–500MB range.

Could anyone share a success story of a vendor they are using that is handling this type of traffic?

Re: IDS\IPS that can handle one Gig

SecurityFocus IDS: Re: IDS\IPS that can handle one Gig

Thanks in advance,

-RGJ

--
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%20focus-ids%20040708)
to learn more.

--
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%20focus-ids%20040708)
to learn more.

--
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%20focus-ids%20040708)
to learn more.

--
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%20focus-ids%20040708)
to learn more.

--
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%20focus-ids%20040708)
to learn more.

--
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%20focus-ids%20040708)
to learn more.