

Re: [fw-wiz] Integrated IDS/IPS/Firewall (Cisco ASA and Juniper ISG)

# Re: [fw-wiz] Integrated IDS/IPS/Firewall (Cisco ASA and Juniper ISG)

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/Firewall-Wizards/2006-05/msg00097.html>

---

- *From:* Devdas Bhagat <[dvb@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:dvb@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx)>
  - *Date:* Sat, 27 May 2006 03:21:26 +0530
- 

On 26/05/06 09:51 -0400, Chris Blask wrote:

At 09:00 AM 26/05/2006, Paul D. Robertson wrote:

On Thu, 25 May 2006, Chris Blask wrote:

o The best gadget in the world is no good if the maker doesn't survive to support it.

Sure it is. The vendor isn't the only choice for support, and if it's good enough to be the best, it shouldn't \*need\* regular support.

I don't believe in static security. If something was good enough to be best it would still be imperfect.

Only the Sith deal in absolutes. Security is about balancing risk, not about perfection.

The "vendor" could be the open source community, in which case the source is there for everyone to support, but a great product from a dead or badly-acquired company can be worse than useless.

o Another analog to twist would be: a bunch of talented and enthusiastic guerillas may be good at the start of a conflict, but when it gets really serious you'll be unhappy if you are not the one with the integrated weapons platform...

And the time taken to deploy an integrated weapons platform can be too long to do anything.

1. You're comparing apples and oranges, soldiers against weapons.
2. With the right guerilla force, the shiny new expensive platform is already useless by the time you deploy it \*if it even makes sense for the conflict you're in rather than the last conflict that happened when the weapons platform makers all got their contracts.

Analogies are never very accurate (my favorite quote from an English teacher in HS: "There is no such thing as a synonym").

However, to pursue the military analogy:

History is full of tales of the vanquished who've felt their superior large-scale do-everything weapons could win. That's one of the reasons the US strategy to go to small light and mobile divisions is interesting—it's a step away from the traditional "bigger, more" philosophy of multi-billion dollar pork projects and Congress forcing the purchase of ineffective integrated weapons platforms.

o The reason the US military can successfully use "small and light" tactics today is that they have an integrated weapons platform.

I don't see any military force in the world today being small and light. Small and light was the group that took out the twin towers.

Robust standardized components tested to death (pun) interoperate in well defined ways, and small changes are enormously vetted before being released to the battlefield. Inventing new guns that take new bullets and are given to soldiers with new communications systems that use new protocols to sync up with new command structures that analyze data in new ways and provide tactical feedback in new schemas – well, that just wouldn't work real well. "Small and Light" in the US military context is only possible because they have developed "Huge and Heavy" amounts of testing and experience.

Except that the enemy isn't always willing to play by those rules. I suspect that <http://www.defensejournal.com/aug98/indiapakrivalry.htm> might be playing a role in the "small and light" techniques.

Of course, "small and light" can also be "we're just making this sh\*t up as we go along and don't mind dying", sometimes introducing the surprising successes of randomization. Ironically, by the time a new technique discovered that way becomes wide-spread, it often loses the characteristics of surprise and flexibility that makes it successful.

In infosec today we are coining terms and creating methods on a daily basis – this is not a mature area of endeavor. When it is a mature space, we will have much more "integrated" "weapons platforms", whether single-vendor or standards-based.

What the industry is steadfastly refusing to recognise is that the criminals have very large numbers of small and flexible units already deployed in the field. The criminals have bigger numbers of computers, more CPU cycles, more memory and more bandwidth than we do. And these are distributed all over the consumer IP space.

The people who can stop this problem have a vested interest in not doing so. It costs them money to run a clean network, and they don't get to bear the costs. And the people who are actually paying those costs aren't willing to shift the cost back.

We are bound by procedures and laws, criminals aren't. They can switch attack sources, bring more of them to bear on you and generally beat the hell out of your finances.

An insider seems dangerous, because (s)he can do so much more damage. To continue with the military analogy, the insider is a nuclear bomb. The external threats are mosquitoes. However, malaria kills more people than nuclear weapons do. But the fear of a nuke is far greater.

Integrated platforms sound good because they reduce apparent management cost. The cost of failure, on the other hand is far higher. When you start to add availability requirements, you start to add even more complexity. And then you have to worry about all these separate components interacting with each other on the same system.

As a rule of thumb, complexity is bad for management and security. Pretty GUIs and management interfaces hide the complexity, but do not reduce it. This is like undergoing plastic surgery to cure cancer.

Why is no one still pointing out the second most obvious hole in any security system: the desktop? (The most obvious is the user).

Move away from Windows and you suddenly have an increase in security [1]. I don't care about an anti-virus because my platform of choice is not vulnerable to those attacks. A host which is not listening to anything on the network is not vulnerable to direct attacks (except a packet

Re: [fw-wiz] Integrated IDS/IPS/Firewall (Cisco ASA and Juniper ISG)

flood or an IP stack hole). A host which is not connected to the network is not vulnerable to network based attacks.

Thin clients make this even nicer, and controllable.

You don't need an operating system or program monoculture. You need a data format monoculture. A format where data is explicitly separated from code. A good format will work across platforms and be usable with multiple applications. If one application is buggy, you should still be able to get work done without loing everything.

Put all your eggs in one basket and then watch that basket carefully works at a very high price.

I think of a good defense system like a cryptographic algorithm. I should know exactly what you have, how your components are managed and still not be able to break in.

Devdas Bhagat

[1] This is not to say that Linux is necessarily a viable alternative. Linux may be, but KDE and GNOME wouldn't figure in my choice of desktops. Keep in mind that Mac OS X, and \*BSD are choices too, as are other Unix systems.

Please ignore the crappy analogies in the mail.

---

firewall-wizards mailing list  
firewall-wizards@xxxxxxxxxxxxxxxxxxxxxxxxx  
<https://listserv.icsalabs.com/mailman/listinfo/firewall-wizards>