

Re: [fw-wiz] Re: firewall-wizards digest, Vol 1 #1229 – 18 msgs

Source: <http://www.derkeiler.com/Mailing-Lists/Firewall-Wizards/2004-03/0060.html>

From: Dale W. Carder (dwcarder_at_doit.wisc.edu)

Date: 03/10/04

To: Bill Van Emburg <bve@quadrix.com>

Date: Tue, 09 Mar 2004 17:30:51 -0600

I am a vlan bigot. If that offends you, read no further! :-)

On Mar 7, 2004, at 11:15 AM, Bill Van Emburg wrote:

- > *I, personally, am a very big fan of separate physical switches per*
- > *segment.*
- > ...
- > *protects you against the *next* bug to be found in your switch*
- > *vendor's VLAN software (because ALL CODE HAS BUGS ... security 101,*
- > *right?)*
- > ...
- > *is easier to maintain*

So now you have to update the firmware and maintain the configurations on 'n' many separate switches instead only a few? I believe that less to maintain is easier.

- > *(how many spare 6500s do you have in *your* infrastructure?)*

14. High Availability was a design requirement.

- > *and allows for easy separation of control (do *you* have a good way to*
- > *have separate VLANs administered by different sysadms?).*

We have a few hundred vlans, most of each with it's own sysadmin, and each with its own security domain.

- > *From a security perspective, you should physically isolate segments*
- > *with different levels of security tolerance, whenever possible.*

I claim that one can do that with vlans, and it is a special case of "physically".

- > *For segments with similar security tolerance, you might decide that*
- > *there are advantages in your scenario, although I'll still argue that*
- > *my points above are valid in most of the scenarios I've seen.*

I think we're looking at a sizing issue, the more networks you have, the more switches you need in this case.

With vlans, more networks doesn't mean you need to buy more switches.

I would like to encourage the use of vlans as a means of increasing security.

I believe that since you can easily create many separate segments using vlan capable hardware you already own or are considering buying, this separation will encourage the practice of identifying and implementing more security between networks.

You could create vlans for every class of machine, every department, every business function, whatever you wanted, and make them separate layer 2 networks.

> *In particular, if your infrastructure is small, it almost never pays*
> *to go with a huge switch.... (just my \$0.035 -- I never give just*
> *\$0.02! ; -)*

That is true. Buy the appropriate sized equipment for your network with the functions you require, and compare among vendors.

Dale

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