

The Ultimate Firewall

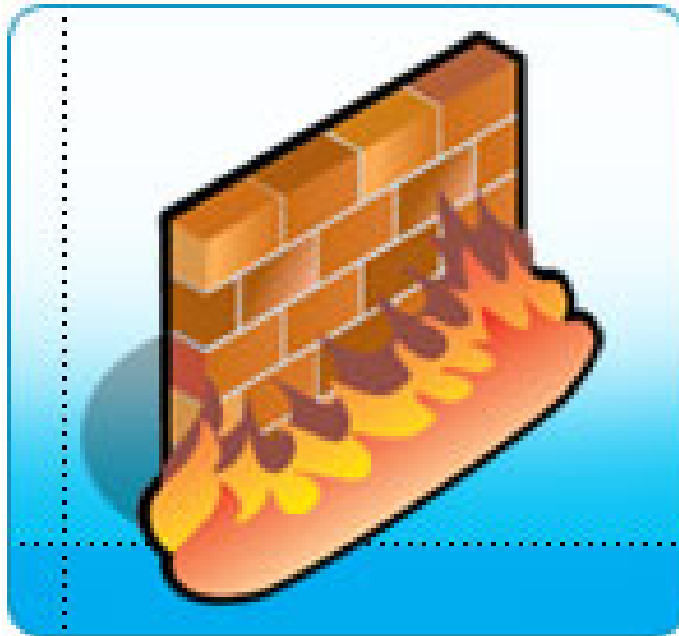
By Marcus Ranum

Perfection is a Hard Target

I've written 3 firewall products which, at various times, have been ground-breaking. My first, which later was known as the DEC SEAL, was a synthesis of good ideas from other firewall-builders(1) that became the first commercial internet firewall product. Back in the day, it cost \$75,000 - today you can get a decent firewall on Ebay for \$10. Then firewalls became really popular, and really stupid, and I got very sick of them. So I switched to working on something interesting: intrusion detection, and founded a company that made a kick-ass IDS. Sometime around then, I promised myself I was done with building firewalls. And a funny thing happened: all the IDS and firewall vendors merged to produce a thing called "Intrusion Prevention" - largely marketing bullshit. I used to have this article that I called the "Ultimate Firewall" - that I changed with the times.

How can you make a firewall that's better than a pair of bolt-cutters?

Well, I was sitting at some dumb conference or other and someone put up some dumb powerpoint slide or other with a dumb graphic that was supposed to look like a firewall for dummies.



(Oh, that's a firewall.....?)

It gave me the idea of making a firewall graphic that had some balls.

Diesel, Pick-ups, and Hay Bales

Living out on a farm, with a nice big yard, has some real advantages. For example, there are open places in my yard that you can't see from anyplace. Like our upper hay-field. It's about 80 acres; we usually cut it in August and bale it for the horses. Every year we tell ourselves "next year we won't bale so much!" but every winter ends with a bunch of hay-bales left in the barn.

So I decided to use a few bales of the "not so good" stuff as a firewall.

The Ultimate Firewall

By Marcus Ranum



(My Ultimate Firewall)

You'll notice there is a large hole sort of in the center. That represents TCP Port 80. Most firewalls have a big hole right about there, and so does mine. There's also what appears to be a bale missing at the upper right. That could be because I only threw 8 bales in my truck or it could represent the unfirewallable encrypted protocols like SSH and SSL. You decide. The photo is a bit grainy and cruddy-looking because it was shot at dusk; I didn't want to have the sun blot out the full effect of the firewall.

And what firewall would be complete without 4 gallons (give or take) of #2 diesel fuel to power it?

The Ultimate Firewall

By Marcus Ranum



(There goes port 80. I told you that would happen)

You are welcome to use my firewall icon in your powerpoint slides. You have to admit, it's a lot more intimidating than the usual powerpoint decorator. Namely:



The Ultimate Firewall

By Marcus Ranum

Conclusion

Like yours, my firewall didn't hold up very long. I lit a single match and dropped it right in port 80, and the whole thing was a ball of flames in seconds. It was nothing but smouldering ashes in 10 minutes. Oh, yeah, always park your pick-up truck upwind of your firewall and make sure your DMZ is big enough.

mjr.

Snowing, with 5 inches on the ground here at: Bellwether Farm, Morrisdale, PA

Jan 29, 2007

(1) In no particular order: Brian Reid, Geoff Mogul, Geoff Mulligan, Paul Vixie, Bill Cheswick, Steve Bellovin, Dave Presotto