

Re: Lets talk about firewalls – what do we as a group think a firewall should be/have?

Re: Lets talk about firewalls – what do we as a group think a firewall should be/have?

Source: <http://www.derkeiler.com/Newsgroups/comp.security.firewalls/2006-08/msg00496.html>

- *From:* ibuprofin@xxxxxxxxxxxxxxxxxxxxxxxxxxxx (Moe Trin)
 - *Date:* Tue, 22 Aug 2006 14:59:51 -0500
-

On Tue, 22 Aug 2006 in the Usenet newsgroup comp.security.firewalls, in article <vfDGg.68760\$u11.65861@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>, Leythos wrote:

We're talking a firewall, strictly a firewall, something that can be used in all cases. We'll brake down the features into Home/SOHO/etc... later.

To an extent, that's an awfully large stretch. A Home/SOHO is going to be quite a bit different compared to something used at a .edu with even 500 students. Yes, one would hope that the admins on that .edu had a lot more knowledge at choosing/configuring the network as well as the firewall, but your certification requirement (your item 12) is going to attract the attention of the Pointy-Haired crowd. The fact that there might be a difference between a POTS/?DSL/OC-3 would be a detail they'd ignore or at least not notice.

I'd also prefer to analyze the separate requirements, rather than slow them down. (break != brake)

5) A firewall should have a real DMZ if it claims to have a DMZ – meaning that it should have a physical jack for a DMZ that is not part of the same network as the LAN.

I agree to a point. Each interface of a firewall should be distinct from each other. However, a firewall does not necessarily need more than two interfaces, so a "DMZ interface" is not a requirement.

Re: Lets talk about firewalls – what do we as a group think a firewall should be/have?

I'll definitely agree with this one. IF it claims to have the capability of a DMZ, then this MUST (using the capitalization in the same way as in RFCs [see RFC2119]) provide this on a separate physical connection. If this separate connection is not provided, the supplier/vendor/what-ever MUST NOT claim a DMZ capability.

7) A firewall should clearly log/report all traffic, in/out, and make it easy to determine if it was approved/unapproved, etc...

Yes.

This should be configurable. I really don't want to see a mile long list of "packet allowed/disallowed" every ten minutes. On my home system, I purposely do not log 'disallowed inbound'. So what if some klown in South Whatiz scanned the box – the firewall blocked it (or there was nothing running on that port or protocol), and that's the end of that. Logging the source of UDP to ports in the range 1024 – 1050 is a waste of time/bandwidth/CPU-cycles, as most of that is messenger spam, and the last time I looked at it, most of the IPs were faked (wrong TTLs were the most obvious, IPs that haven't even been issued by the RIRs was another).

10) A firewall should provide for multiple subnets on any network interface.

I'm not sure I understand what you mean by that.

It also doesn't "fit" the normal use of the WAN side.

In my networks I have multiple networks behind each network in many cases. As an example, I might have a DMZ with a network with servers in it (say 192.168.16.1/24)

Not mentioned before – NAT, and perhaps 'port forwarding'. As regards the multiple networks, I could see this done with the rule associating network address (range) and a specific interface. This would be a part of RFC3704 filtering anyway.

Re: Lets talk about firewalls – what do we as a group think a firewall should be/have?

Re: Lets talk about firewalls – what do we as a group think a firewall should be/have?

and then inside that network I might have classrooms with their own isolated networks (10.1.0.1/24, 10.2.0.1/24...). The firewall has to know that there is also the 10.x.x.x networks on that interface or it will block traffic from them – or it should block traffic from them.

Your use of the DMZ is different from what I see to be normal. The only things we put in the DMZ are those hosts that need to be reachable from the WAN side. These would be the public DNS, mail, web, FTP servers and the like. Hosts that are not offering services to the WAN do not belong in the DMZ. In your example, the classrooms would likely not be offering such services, and probably should be isolated on their own NATing firewall – to allow (probably controlled) access OUT to the Internet, and limited (if any) access to the rest of the internal networks.

11) A firewall should not have DHCP Service enabled on the LAN/DMZ by default.

Make that "any service on any interface". One reasonable exception may be a service providing a (secure) configuration frontend on one distinct interface, that is marked as such (see also below).

I'd agree with this

Yes, but I was specifically thinking about Drop-In devices like the household NAT appliances that come with DHCP Service enabled to make it easy for users.

What do you propose instead? No DHCP – so it's static or LinkLocal? Or is it some other box separate from the firewall/user systems?

12) A firewall should be certified as a firewall by some reputable authority.

That only helps your legal department. If you think you need that: fine, but it's most definitely not a technical requirement for a firewall.

Re: Lets talk about firewalls – what do we as a group think a firewall should be/have?

Re: Lets talk about firewalls – what do we as a group think a firewall should be/have?

But, if it's not certified, then anyone can call an appliance a firewall and the public will buy it as a firewall – See all the residential devices out on the market.

I can see your point, but what do you define as a reputable authority?
ANSI? IEEE? IETF? NIST? NSA? Some supra-national entity from the EU,
or similar? Good Housekeeping magazine? ;-)

Old guy

.