

Re: What firewall for small medical research lab

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/security-basics/2006-05/msg00044.html>

- *From:* "Arturas Zalenekas" <security@xxxxxxxxxxxxxx>
 - *Date:* Mon, 1 May 2006 10:31:05 -0500 (CDT)
-

-----BEGIN PGP SIGNED MESSAGE-----

Hash: SHA1

Please do not say, that CheckPoint is the best commercial FW. I'm sick to hear that all the time. I also worked with CP and used all these "features". There is no BEST firewall, if you will not use it at the right place with right needs. The same is for IDS or IPS or what ever program or appliance that is. CheckPoint is a good FW, definitely, but there is also SGS2/3 from Symantec and PIX from Cisco. It always depends on which part of your network, how and for what you will use it. Only then is the chosen firewall product is the best in your network architecture.

@Smith:

Ignore the Gentoo suggestion, not because there is anything bad about gentoo but because of the amount of time and maintence involved to go that route.

Yes it's true that Gentoo OS takes a lot of time to set it up and maintain properly, but do not forget the experiance that you gain by setting it up. And don't tell me, that Gentoo is not a server distro. A lot of admins that I know (good ones) use Gentoo as a server. I use it too.

Kind regards,
Arturas Zalenekas
Network Security Engineer and Analyst

On Fri, April 28, 2006 19:31, Smith wrote:

I agree with Jordan Dallas 110%, go with OpenBSD. Ignore the Gentoo suggestion, not because there is anything bad about gentoo but because of the amount of time and maintence involved to go that route. When I wanted to learn firewalls and vpns, I researched Linux solutions and got so fed up reading how firewall and vpn features must be compiled into the kernel. I knew nothing about firewalls so I had a hard time learning firewalls/vpn's because of iptables and ipchains horrible syntax. Then I found OpenBSD and stayed with it since. OpenBSD has firewall and vpn compiled in and the syntax really is easy to learn.

Re: What firewall for small medical research lab

Plus OpenBSD and Checkpoint (the best commercial firewall) were the first to have stateful inspection when all the other guys like linux, sonicwall, and cisco pix had it a few years later if they even have it at all. If you don't know what stateful inspection means, lets just say its a very important firewall feature. You know what else, once you learn how to install OpenBSD by reading their FAQ, it takes literally 5 to 10 minutes to install a full blown system (which also means full blown fiirewall/vpn). Compare that to spending days/weeks just to get gentoo up and running and CONFIGURED! As far as cost, \$45 for OpenBSD if you want to support their cause by buying their CD or get it for free via ftp and take any old computer system preferably a Pentium II or better with two or three nic cards. Compare that to the other suggestions.

And before anybody flames me about some of the things I said, please note everything I said above (except about OpenBSD) is based off the situation as it stood back around 2002. I know a lot has changed now that it's 2006. So in 2002 I chose OpenBSD and never regretted it.

rmillisl@xxxxxxxxxxxxx wrote:

I have been asked to research what good, low cost, firewall solutions might prove suitable for a medical research lab at a local University to protect confidential patient data from outsiders.

In addition to other research I though I would ask here.

I realize a firewall is just one component of an overall security policy /
implementation.

Basically what is needed is a simple NAT box that generally keeps outsiders out, and allows authorized lab servers and workstations to access certain services out on the main building network (DNS, IMAP, POP, SMTP, HTTP, HTTPS, FTP, SSH) and through that network to the Internet (through the main building campus/network).

Cost is a very important factor so suggested solutions have been:

– Pay someone to set up a PC based firewall running on surplus hardware using either Fedora Core 5 and Shorewall 3.0.6 (to allow easy configuration of iptables rules). The hardware and software cost are low.

The time could add up. I have considerable experience with this so this would be the lowest learning curve. Problem is Fedora with its frequent updates may make managing this more of a chore.

– Pay someone to set up a a PC based firewall running on surplus hardware using either OpenBSD 3.7 or 3.8 and pf. The hardware and software cost

Re: What firewall for small medical research lab

are low. The time could add up. I have some OpenBSD experience and no pf background.

– Pay someone to set up a a Linksys or D-Link broadband switch/firewall/router. The hardware cost is low. The time to set up may be minimal (Plug&Play + some common sense and provided firewall/filter capabilities). Are these a serious and secure enough solution?

– Some other low cost hardware or software based alternative. What else might be out there that I don't know about that might be comparable in cost to the D-Link or Linksys options.

The PC based solutions I personally have the most confidence in with respect to hand crafting a minimal OS build and hardening and patching the OS and doing rules mostly by hand. With pf there is some concern of errors introduced due to learning curve.

Comments? Suggestions?

This List Sponsored by: Webroot

Don't leave your confidential company and customer records un-protected. Try Webroot's Spy Sweeper Enterprise(TM) for 30 days for FREE with no obligation. See why so many companies trust Spy Sweeper Enterprise to eradicate spyware from their networks. FREE 30-Day Trial of Spy Sweeper Enterprise

http://www.webroot.com/forms/enterprise_lead.php

-----BEGIN PGP SIGNATURE-----

Version: GnuPG v1.4.3 (GNU/Linux)

iD8DBQFEVim5B9mpD7YA v w4RA16nAJ0ecwkvgermmIU1FgvNA6RpcO8VPgCfSkN0
MhR+eh2fjEIC30oLqBjpuK0=
=d8wi

-----END PGP SIGNATURE-----

This List Sponsored by: Webroot

Don't leave your confidential company and customer records un-protected. Try Webroot's Spy Sweeper Enterprise(TM) for 30 days for FREE with no obligation. See why so many companies trust Spy Sweeper Enterprise to eradicate spyware from their networks.
FREE 30-Day Trial of Spy Sweeper Enterprise

http://www.webroot.com/forms/enterprise_lead.php
