

[Linux.com](http://linux.com)

Search

Search

Search

[Log in](#) | [Create Account](#) | [Submit Story](#)

- - [Articles](#)
 - [Case studies](#)
 - [Features](#)
 - [News](#)
 - [NewsVac](#)
 - [Reviews](#)
 - [Documentation](#)
 - [What Are Linux HOWTOs?](#)
 - [Where Can I Get Linux HOWTOs?](#)
 - [HOWTO Translations](#)
 - [Categorized List of HOWTOs](#)
 - [Single list of HOWTOs](#)
 - [Single list of mini-HOWTOs](#)
 - [Unmaintained HOWTOs](#)
 - [Writing and Submitting a HOWTO](#)
 - [Copyright Information](#)
 - [Distributions](#)
 - [Forums](#)
 - [Sponsor Solutions](#)
 - [Open Source and Linux from HP](#)
 - [About Us](#)

What is Linux?



[Learn about Linux](#)



[Download Linux](#)



[Get Linux help](#)

Feeds

- [Features](#)
- [NewsVac](#)
- [Forums](#)
- [News](#)
- [Video](#)
- [Comments](#)

Special Offers

Get special offers on:

- Linux
- Application Dev
- Programming
- Software

Email:

Submit

[Ads by Google](#)

Feature: Linux

Gambling on Linux pays off in Nevada

By on July 24, 2003 (8:00:00 AM)

 [Share](#)  [Print](#)  [Comments](#)

- by [Karen D. Schwartz](#) -

When Churchill County School District in Fallon, Nev., asked Dan O'Barr to find a replacement for an aging and expensive PIX firewall in 2000, the technology manager for the school district learned it would cost \$20,000 to upgrade the hardware and acquire additional licenses through Cisco Systems. O'Barr decided he had nothing to lose by trying to create a firewall with Linux. Even though he didn't have much experience with the operating system at the time -- and virtually no experience using it in a firewall environment -- he was confident that he could learn how to make it work.

O'Barr ordered a small rack-mounted server from Dell Computer Corp. for about \$1,300, downloaded a copy of Red Hat Linux, and proceeded to create a firewall. The result was a firewall O'Barr says was as good or better

than anything the school district ever had with the PIX system -- at a significant cost savings.

After that success, O'Barr was hooked. He learned everything he could about Linux, becoming a vocal proponent -- and a thorn in the side of Nevada's Department of Information Technology, which had a history of support for Microsoft products. He became well-versed in Linux, eager to try it on other projects. He would soon have his chance.

Soon after the firewall project was completed, O'Barr left the Churchill County School District for a position as network administrator of the Nevada Department of Corrections. There, he faced his biggest challenge yet. After spending a year maintaining and troubleshooting an inmate records management system called the Nevada Criminal Information System (NCIS), he was promoted and tasked with consolidating the Department's networks, communications, and infrastructure around twisted pair Ethernet and TCP/IP.

Because the department's systems ran on different platforms with different networking schemes, the challenge was daunting. NCIS was developed in Revelation, a DOS database development environment based on PICK, with software residing on Netware 3.12 servers and client 286 machines connected via ARCnet cabling and IPX. A second system, which allowed people to share files via the Internet, ran on a Dell PowerEdge 4400 running Windows 2000 Server. A third system housed a DB2-based banking and inmate accounting system, running on an IBM AS/400 with Twinax cabling and leased SNA lines.

O'Barr set about his task by switching from the State of Nevada's Microsoft-based Web server to one running Red Hat Linux 7.1, the Apache Web server, and Web scripting language PHP, all on a donated Dell Pentium II workstation. He installed PostgreSQL, an open source database, and used it to add an inmate search function, which allowed state employees, attorneys and the general public to access inmate data from the legacy NCIS system -- data that had never been accessible to anyone except state employees. The system went live on Sept. 10, 2001, but its success was overshadowed by the events that followed, so the system was never formally announced or demonstrated to the general public.

Even without publicity, the Web-based system has become quite popular. In one recent month, the site received 35,000 unique visitors, and averages about 10 percent growth each month. Today, law enforcement agencies might check the system to determine if a crime may have been committed by a recently released prisoner, attorneys may use it to help build their cases, families access the system to determine the location and visiting hours of incarcerated relatives, and victims of crime use it to check that perpetrators are still in prison.

O'Barr's suspicions had been right. Linux fit the bill -- and the price was right. O'Barr relied on donated PC equipment and downloaded software, creating a system without cost, except the cost of his time. That was extremely important, especially in Nevada, which is growing so fast that the government has had to find ways to provide services for a growing population without additional funding, O'Barr says.

As usage grows, cost savings continue to mount. "We significantly underestimated how valuable a public relations tool a Web site can be if it's done right," O'Barr says. "The Web site has cut down tremendously on the amount of calls and questions that our public information desk receives, and it's been a great help in getting information to the public."

That initial Linux success at the Department of Corrections gave O'Barr enough confidence to turn his attention to the Nevada Staffing Information System (NSIS), a staffing and overtime system written in Visual Basic and Microsoft Access. Because Access doesn't scale particularly well, efficiently handle the amount of data generated, or work well over a WAN link, O'Barr and his team developed a front end around Microsoft Access with PostgreSQL on the back end. Since the client computers already had Access, the net cost, other than man-hours, was \$0.

Over time, O'Barr has found additional benefits to using Linux. For state government -- and for the Department of Corrections in particular -- security is paramount. Although O'Barr says that Microsoft's security is first-rate, "you get the feeling that Open Source software is generally written by folks in the trenches," he says. "It may be rougher around the edges, and not always as 'nice,' but it has been more secure by design."

O'Barr's confidence in Linux' security has been borne out by time. Other than two unplanned interruptions in service due to a hard drive/controller problem, the system has experienced no downtime in the two years it has been operating. And that's particularly important with systems operating behind prison walls, he says.

To make Linux work in any environment, O'Barr says it's critical to train network administrators in how to use and troubleshoot the system. "Linux isn't really that hard to manage if you understand networking, but if you don't -- and a lot of people who run Windows networks really don't understand networking -- you'll have a hard time," he says. To prevent problems, O'Barr recommends taking the time to learn the ins and outs of the operating system. Once you do so, day-to-day management should be just as easy as managing Windows, he says.

But despite the clear benefits of Linux, it may not be for everyone. In addition to making sure network administrators can handle the operating system, O'Barr says a generally technically proficient staff is imperative.

"Look at your staff and see who already knows Linux or can learn it. Then ask yourself if the software you need exists, or if you can readily create software for Linux that will work. If the answers to both questions are yes, there is no reason not to go with Linux. But if you've got people who call Microsoft on a regular basis or have a key application that can't tie into it, you might be better off going with commercial software," he says.

As for Nevada, O'Barr says the future of Linux is bright. One major reason, he says, is cost.

"If I were to buy Windows XP Professional to put on a PC I have right now, it would cost \$200, and Microsoft Office would cost another \$340. That's \$540 in Microsoft software alone just to have a functioning computer," O'Barr says. "I can put a version of Linux on it with OpenOffice and it will meet the needs of 80% of our users."

To increase usage, O'Barr would start by outfitting just a few early adopters with the Linux systems. "The only way to prove it works is by getting it in under the radar," he notes. If the pilots work well, the Department may consider rolling out Linux workstations to as many users as possible.

But before he gets to the point of Linux on the desktop, O'Barr plans to move away from NetWare 3. By upgrading to Netware 6.5, he will be creating a migration strategy, because Novell network services are being ported to work on top of Linux. If everything goes as planned, all of the Department's file and print serving will be moved to a Linux kernel, with NetWare services potentially operating on top of it. The system would replace any Windows servers now in use as well as the NetWare servers currently used for file and print sharing.

As word of his success spreads, O'Barr is finding out that other agencies are either using Linux or considering its use. He recently found out that Nevada's Department of Health has 12 Linux servers, and more state agencies also may be experimenting with it, although nobody will talk about it.

"Sometimes it's political suicide to say you're going to do it when everybody loves Microsoft, so they don't say a word, yet they are meeting critical business needs and doing great things," he says.

Karen D. Schwartz is a writer and editor based in the Washington, D.C., area, specializing in technology and business issues.

- [Write for us - and get paid!](#) -

 [Share](#) | [Print](#) | [Comments](#)

Related Links

Other articles in category Linux:

- [Revised Slackware keeps it simple](#) Dec 23, 2008
- [openSUSE 11.1 makes Christmas come early](#) Dec 18, 2008
- [PC/OS: Insert CD, use desktop](#) Dec 05, 2008
- [Indian GNU/Linux advocate and independent FOSS consultant Raj Mathur \(video\)](#) Dec 03, 2008
- [Fedora 10 proves infrastructure matter](#) Nov 26, 2008

Sponsored links:

- [Best deals: Linux](#)

Comments

on [Gambling on Linux pays off in Nevada](#)

Note: Comments are owned by the poster. We are not responsible for their content.

As Much As I Love Linux

Posted by: Anonymous Coward on July 24, 2003 05:54 PM

It is not the best choice for a firewall. A BSD would be better, imo.

And no, I am not a BSD zealot, I am simply suggesting what I believe is the best tool for the job.

#

Re:As Much As I Love Linux

Posted by: Anonymous Coward on July 24, 2003 06:51 PM

Why would BSD be a better choice? Maybe because you heard some BSD zealot say so? Linux iptables is very effective and with add-ons like <http://shorewall.net> it becomes an extremely easy to administer firewall. BSD has no advantages over Linux these days.

#

Re:As Much As I Love Linux

Posted by: Anonymous Coward on July 24, 2003 08:52 PM

Depends on your hardware i think.

I have found that more recent linux distributions are very heavy on the memory.

If you are running on a decently stacked box (And DELLs are quite decent hardware, despite what you may think of the company) this wont be a problem, and the ease of system administration compared to the BSDs

would make it more than worth it.

Have you tried to run Red hat 8 on a P300 recently? The machine i used had 256Mb of ram and SCSI disks, but it still ran like a pig because of KDE which these distributions seem to insist on installing instead of a light WM.

But hardware is cheap, and the reliability depends on what you are doing with it.

I am running a 486 25 as a SMB file server and it tells me it has been up just under a year now. It runs Red hat 5.2 with up to date SAMBA and no other services running. (Dont anyone say NFS is better, i've tried it, and quite frankly its advocates are lying)

BSDs only have an advantage these days on their weight. Linuxes are bloated these days. You have trouble getting to a command prompt in 16Mb of memory.

My ADSL router at home (a MRI compact box thing) seems to run one of the BSDs, Cant remember which one. I suspect getting enough hardware to do this into a single chip to support Linux 2.2+ would be a lot more hassle.

Horses for courses et al. Wouldnt *dream* of using a BSD as a desktop machine.

#

Re:As Much As I Love Linux

Posted by: Anonymous Coward on July 24, 2003 09:15 PM

16MB is too big for Linux. A loadable Linux firewall system requires only 1.3MB with some space left on a floppy! It depends on what you install and how you config your Linux, not hardware. Cars from small street always yield the big one. Hardware is physical object, but software is virtual, and flexible. So you can use software to fit the hardware, but not the reverse.

#

Re:As Much As I Love Linux

Posted by: Anonymous Coward on July 24, 2003 09:59 PM

Please, what FUD. One does not need a whole RedHat install to run a firewall. In fact all one needs is the kernel, some modules and a bootloader to run a Linux firewall. Linux netfilter(iptables) is the most powerful firewalling software around right now. Combine that with squid and you have a great solution. My company still has pentium boxes out in the field that run great with Linux Kernel 2.4 and iptables.

#

Re:As Much As I Love Linux

Posted by: jlguallar on July 25, 2003 12:08 AM
Agreed.

Just do a Red Hat Linux Custom/expert install. Unselect everything but iptables and ssh.

Update the firewall (behind a firewall), set remote syslogging, stablish an update policy, subscribe to bugtraq and maintain a proactive security approach.

Remember, security is a job, not an OS.

Peace,
Josep

<#>

Re:As Much As I Love Linux

Posted by: Anonymous Coward on July 29, 2003 11:31 PM
Redhat has a firewall/minimal install that pretty much does it by itself.

<#>

Re:As Much As I Love Linux

Posted by: Jonathan Bartlett on July 24, 2003 11:19 PM
"Have you tried to run Red hat 8 on a P300 recently? The machine i used had 256Mb of ram and SCSI disks, but it still ran like a pig because of KDE which these distributions seem to insist on installing instead of a light WM."

You don't need ANY WM if you are using it as a router.

<#>

Re:As Much As I Love Linux

Posted by: Anonymous Coward on July 24, 2003 11:59 PM
I did a firewall on a pentium classic clocked at 200Mhz with about 16 MB of memory and a 200MB hard drive. I allocated swap space so that I could get through the install(text mode) and striped out anything that didn't have to do with the firewall. Once I was done, I could ssh into the machine and get a command prompt and still not have used more than 8-10MB of memory and no swap space. My guess is that I could have made it run on less of a machine, but what's the point? This was a machine headed for the trash anyway.

<#>

Re:As Much As I Love Linux

Posted by: Anonymous Coward on July 25, 2003 05:31 AM
(Dont anyone say NFS is better, i've tried it, and quite frankly its advocates are lying).

I'm going to say their wrong as well, and then also say that you're wrong.

SMB and NFS (at least in their current forms on the *nix platform) are for two different pruposes. It's like comparing either one of them to ftp. Sure, they all transfer files over a network, but the implementation, and their purposes are quite different.

<#>

Re:As Much As I Love Linux

Posted by: Anonymous Coward on July 25, 2003 01:02 PM

"...Depends on your hardware i think.

I have found that more recent linux distributions are very heavy on the memory..."

I think it is more accurate to say that some of the more popular Linux distributions have become hogs.

But some aren't. I run Slackware 9 on 486SX machines with 8 MB ram. Granted, 16 MB is required to install, but I have a box with 16 MB and a 4X CDROM so I can swap hard drives into it for installs, and then move them to less potent machines.

Compare package versions and you'll find that Slackware is as up to date as the latest releases from RedHat, Mandrake and SuSE, and it will run side by side with recent FreeBSD releases on that 486SX 25. I have a stack of them that I got from a DOS POS in a department store and they run Slackware just fine. (They make nice satellite office mail servers, too.)

<#>

Re:As Much As I Love Linux

Posted by: Anonymous Coward on July 25, 2003 10:44 PM

smoothwall is a pretty good linux firewall also. I have it running on a pentium 100 with 16megs of memory and a 1 gig hard drive. You don't get much leaner than that!

<#>

Re:As Much As I Love Linux

Posted by: Anonymous Coward on July 29, 2003 11:29 PM

smoothwall is a pretty good linux firewall also. I have it running on a pentium 100 with 16megs of memory and a 1 gig hard drive. You don't get much leaner than that!

Hmmm... freesco: <http://www.freesco.org> - I have it running on a 486 with 16MB, and no hard drive, I could go even lower on the memory if I had to.

<#>

Re:As Much As I Love Linux

Posted by: Dan O'Barr on July 25, 2003 11:02 PM

Hmmm, I have RedHat 9 running nicely on a P-233 w/64MB of RAM (2GB hard drive). You don't need X-windows on a server...

<#>

Re:As Much As I Love Linux

Posted by: Anonymous Coward on July 26, 2003 04:14 AM

EXACTELY... why would u want a X manager on a firewall system?<nobr> <wbr></nobr>...any good Linux admin will avoid X as to reduce the usage of system resources and prevent any additional system problems and security risks.

<#>

Re:As Much As I Love Linux

Posted by: Anonymous Coward on July 25, 2003 10:05 AM

OpenBSD is more secure, and more mature in terms of its firewalling, than Linux seems to be. YMMV, though.<nobr> <wbr></nobr>;)

The simplicity of OpenBSD makes it a particularly good candidate for a firewall. It is difficult to make Red Hat as thin as it needs to be to act as efficiently as a firewall, though there are alternative, specialized distributions that moot that argument.

OpenBSD also has some security features that are not available in most Linux distributions (randomized shared library offsets, read-execute exclusivity, etc.); its focus on security may make it easier to sleep at night.<nobr> <wbr></nobr>;)

<#>

Re:As Much As I Love Linux

Posted by: Anonymous Coward on July 30, 2003 04:25 AM

OpenBSD is more secure ****OUT OF THE BOX**** yes. You are talking about a firewall only box here so it is as secure as you make your firewall rules. You can't tell me that OpenBSD locked down with pf is going to be more secure than Linux locked down with iptables because they will both be exactly the same. Both would have exactly 1 service running.. sshd. And if both sshd's are up to date, they will be running the same version.

As for speed, it would take a couple of hardcore kernel d00ds to honestly benchmark the differences, and even then, I hypothesize that it would be very close.

<#>

Excellent Article

Posted by: Anonymous Coward on July 24, 2003 06:20 PM

Thanks, Karen, for the excellent article.

I was just thinking how nice it would be, if the Microsoft Senior Management were to be incacerated here, once somebody properly punishes them for their crimes.

<#>

Linux to the rescue!

Posted by: Anonymous Coward on July 24, 2003 09:28 PM
That's the cool thing about Linux.

More and more, everyday IS/IT people need to solve some kinda problem. They try with the MS stuff but they get frustrated or don't have any money to get the job done. So they hear that Linux may help. After a brief learning curve they are surprised by it's capabilities and find they can solve many other problems and create really elegant solutions using Linux.

That's why Linux is so great and powerfull.

<#>

What PIX did he buy

Posted by: Anonymous Coward on July 24, 2003 09:32 PM
I am not sure what kind of PIX he bought but most of the quotes I got were around \$300 to \$2K. Now, It may be fun for a hobbyist, however I would look into what is required to build and what you get with a PIX. Also, on Cisco's site they have easy setups and about as much learning curve. What is the \$20K for?

<#>

Re:What PIX did he buy

Posted by: Anonymous Coward on July 25, 2003 01:43 AM
The 20K is for support, the unlimited user license, and probably several interfaces.

<#>

Re:What PIX did he buy

Posted by: Anonymous Coward on July 25, 2003 03:46 AM
I'm guessing he was quoted for a PIX 525 with unlimited licenses. Even the limited ones are low five figures, though. I know this because our shop is a Cisco shop when it comes to the network infrastructure, so we have to price these on a regular basis (we're pretty big--about 250,000 folks).

You can probably get a PIX 520 (128MB DRAM, Pentium-II/350 CPU) with an unlimited license, used, on eBay, for about \$5-7K. I've seen those prices. Brand new or used, PIX Firewalls are pricey.

<#>

Re:What PIX did he buy

Posted by: Anonymous Coward on July 25, 2003 10:31 PM
You can probably get a PIX 520 (128MB DRAM, Pentium-II/350 CPU) with an unlimited license, used, on eBay, for about \$5-7K. I've seen those prices. Brand new or used, PIX Firewalls are pricey.

yeah but who wants to pay that for an old customized intel machine with eisa slots... yawn..

<#>

Re:What PIX did he buy

Posted by: Dan O'Barr on July 25, 2003 10:47 PM

I don't remember the exact model, but the equipment cost at least \$8,000 at the time, and the connection licenses would've cost something like \$12,000. I had almost 1,000 client computers at the time. Yes, a little pix today costs \$500, but a big PIX, a few years ago, was (and still is) spendy. What's funny is that this comment sounds like it comes from another inexperienced system administrator, one who has never administered a network bigger than 100 nodes.

<#>

smoothwall

Posted by: Anonymous Coward on July 24, 2003 10:53 PM

this gpl firewall is easy to setup. I've used it on a few projects:

smoothwall.org or its offshoot:

ipcop.org

Just FYI

<#>

Refreshing news indeed! Thanks Karen.

Posted by: Jef on July 24, 2003 10:53 PM

This is the type of story that needs to get out to the press. It truly shows the versatility one can enjoy when employing the Linux OS to solve problems/challenges.

<#>

This is a joke

Posted by: Anonymous Coward on July 25, 2003 01:22 AM

Is this story some kind of joke? Replacing a 2000 model Cisco PIX with Linux? I've never laughed so hard.

"Even though he didn't have much experience with the operating system at the time -- and virtually no experience using it in a firewall environment -- he was confident that he could learn how to make it work."

So he admits he didn't know shit about firewalls, so how does he know his Linux firewall is better than his PIX? Easily, he doesn't. There is no way a Linux firewall could live up to a PIX. There was a project called Freesco that wanted to replace Cisco and others. How far did that get? Not very far. I'm in agreement with the first poster, if this guy had a clue he would have went with OpenBSD for a firewall. But he doesn't have a clue, so this story

is pretty much irrelevant.

<#>

2000 AD

Posted by: gerardm on July 25, 2003 01:52 AM
Not Cisco 2000..

<#>

Re:This is a joke

Posted by: Anonymous Coward on July 25, 2003 02:41 AM

No I am sure it is not, and I am sure you haven't read it properly. It was reported that this guy didn't know about Linux, it didn't say he didn't know about firewalls and how they operate. In addition, he was pointing out how much money he had saved by not taking the CISCO route on an upgrade, and how much more function he was getting from the linux option. Since a Cisco firewall is none other than a Unix-alike system running on top of a processor, there is no reason why linux on a fast machine cannot outperform it. OK, there might be faster buses inside a Cisco device, but you are unlikely to get much performance benefit for a dial-up or ADSL line over Linux. In addition, you have to pay separately for any additional monitoring tools. In any case, if you are so knowledgeable on networking and networking kit, why don't you have a go at trying to break through his firewall. That's assuming you have got the time, with all the security patches you are going to need to install on all CISCO products right now!

Sure, nobody really doubts that for serious network 'grunt' workloads you cannot beat CISCO. But the key point here is that the guy replaced all this cost with a much cheaper and equally viable solution which probably had more additional function. Maybe your IT boss doesn't care about throwing money around to get 'Rolls Royce' solutions, but many other people right now have seriously restrained budgets.

<#>

Re:This is a joke

Posted by: Anonymous Coward on July 25, 2003 03:59 AM

1.) Cursing doesn't get you any additional credibility and actually makes you look worse.

2.) Freesco is actually an attempt at a Cisco router (e. g. 3640) replacement, not a PIX replacement. Like a Cisco router, Freesco can do packet filtering (statefully) due to its 2.4 kernel. BTW, it turns out it's actually pretty good for that.

As for the rest, I work with PIX Firewalls on a regular basis, and the vast majority of the stuff that you'd need out of a firewall can indeed be satisfied with the Linux 2.4 kernel's netfilter mechanism (known perhaps better by its user-space utility, iptables). Unlike ipchains, netfilter/iptables is indeed a stateful packet filter, like the PIX. Unless you need that last 5-10% of functionality--and we're talking special cases here--a GNU/Linux or OpenBSD firewall solution would do just as well as a PIX would do. Plus, if you need lots of throughput, just put GNU/Linux or OpenBSD on, say, an Athlon 2600+ or Pentium-4 2.6GHz with, say, 1GB DRAM, and you have something that will actually handily outrun even the PIX 535 for a lot less money (we have two 535's, so I

have some experience in this arena).

The biggest thing I can see people buying PIXes for is the failover (that's why we have 'em). Not everyone needs that or can afford it. In his case, he could simply build two \$700 PCs (2.6GHz, 1GB DRAM) and have one sitting by as a spare, if he needs that. Or, he could set up LVS clustering and have failover that way.

#

Re:This is a joke

Posted by: Anonymous Coward on July 25, 2003 04:51 AM

Hmmmmmmmm, Funny to me some of the posts here seem quite amusing, I don't imagine any of the "haters" have much experience with "Linux Firewalls" namely "Iptables". BSD is great but I believe they still use "ipfwadm" a bit old and obsolete. Linux firewalls using iptables are more and more popping up as replacements for Cisco, this is becoming a common thing, you learn the "shell" set a dedicated machine whose only service is to route and forward packets, set up ipmasquerading, ip forwarding, a LAN, a DMZ, use encrypted ssh to admin. etc. etc. as for cisco, oh yeah there great, but<nobr> <wbr></nobr>..... people get too confident and when the bugs hit as they have recently with the new exploit people tend to try and ignore them until they get hacked.

#

Re:This is a joke

Posted by: Anonymous Coward on July 25, 2003 06:03 AM

I don't imagine any of the "haters" have much experience with "Linux Firewalls" namely "Iptables". BSD is great but I believe they still use "ipfwadm" a bit old and obsolete.

Well, I don't imagine you have much experience with BSD firewalls. Most of them use IP filter (or IPF for short) which is also available for Solaris, HP-UX etc. OpenBSD however, ships with PF - because of a licensing issue a while back.

Both IPF and PF are highly competent firewalls and very actively developed, especially PF. Old and obsolete?!?

I regularly use Linux's iptables, IPF and PF. The most striking difference is not functional, but more ease of use. IPF/PF rulesets is almost like spoken language. Iptables rules on the other hand tend to become quite unreadable when you have a large/complicated network.

#

Re:This is a joke

Posted by: Anonymous Coward on July 25, 2003 07:53 AM

so how does he know his Linux firewall is better than his PIX?

What do you mean by "better", and why should he care? The real question is not which one is "better" by some arbitrary judgement, but what gets the job done. Obviously, the Linux firewall was a success, so it doesn't really matter if it can "live up to a PIX" under some circumstances that may never actually be encountered.

<#>

Re:This is a joke

Posted by: Anonymous Coward on July 25, 2003 10:22 AM
If Cisco is the perfect solution for you, fine.

This person has found a solution that works for him.

It is all about solving problems, sometimes the budget is the biggest problem.

Never step on a \$20 to pick up a \$5.

<#>

Re:This is a joke

Posted by: Anonymous Coward on July 25, 2003 11:18 PM
Always step on the \$20 first !!!!

if a sudden gush of wind appears and blows the \$5 bill away, the \$20 bill will still be under your foot!

<#>

Re:This is a joke

Posted by: Anonymous Coward on July 25, 2003 07:18 PM
All I can say is "WOW!"

I bow to your superiour knowledge in firewalls. Your enlightened opinion on OpenBSD vs. Linux is also of huge value. Never mind that OpenBSD firewalls vs. PIX won't cut it, if the source of your mirth is to be believed. Wow...

PIX firewalls is excellent. It has a proper stateful engine, comparable (if not better) than other enterprise-level firewalls like Checkpoint FW-1. Like FW-1, PIX is uproariously expensive, and is getting more and more so. With budget cuts and the like, I can totally understand why educational institutions the world over cannot carry on justifying the cost of a PIX/FW-1/NAI Gauntlet or the like. Enter Open Source. Yes, OpenBSD would also have fit the bill, and would have been perfect for this application. In fact, OpenBSD's ipf would have been a lot easier to admin due to the fact that the configs are almost like talking English, as opposed to Netfilter's rather cryptic chains approach.

Be that as it may, if you want a pure feature-by-feature showdown, Netfilter will in almost all cases win hands down. When last did you, enlightened security guru, look at the latest Netfilter Patch-o-Matic for what it can do? When last did you have a really really good look at the capabilities of the OpenBSD packet filter? Well, in both these cases you will see that they far exceed the feature list of the Cisco PIX. Both have fantastic stateful

engines, with Netfilter winning by a short margin due to all the extra, esoteric packet mangling capabilities that gets included by droves.

Anyway, this is not about PIX vs. Linux vs. OpenBSD, the fact is that you didn't read the article properly and were merely trawling for flames. The author did exactly the right thing for his own circumstances, and in fact does have a superior security solution. OK, it's not backed by the Cisco support structure, but who gives a flying squirrel about that if you don't have the money for such support in the first place.

Go home and learn to read, mister security expert. Sad to read replies like yours.

<#>

Re: This is a joke

Posted by: Anonymous Coward on July 26, 2003 03:43 AM

I am not an anonymous reader. I am his mother-in-law. That alone, should speak for itself. Most mother-in-laws don't care for their son-in-laws. This is one great exception. This man is a wonderful man. He is very well learned in his own right. He studies and studies and knows what he talks about. He spends hours of his own time learning about these things. I would be anonymous too if I was the person who wrote this article. To have to use the word "shit" in his article tells most about his own abilities. And his sentence "he would have went" is a clue to me that Dan O'Barr is much more learned starting with the English language. Unless this person gets better in his English, I wouldn't criticize anyone else.

<#>

We Know Already

Posted by: Anonymous Coward on July 26, 2003 11:57 PM

You're preaching to the converted here. We know all this.

As for the BSD thing, unless you have a significant amount of throughput a BSD system isn't really going to make any difference to performance. Going with a Linux distro is a good choice.

<#>

This story has been archived. Comments can no longer be posted.

[Ads by Google](#)

[Use Cisco Pix Firewall?](#)

Get Powerful Firewall Analysis.
Compare/Analyze Policies & More!
AthenaSecurity.net/Free-30Day-Trial

[Cisco Configuration tool](#)

Free Configuration Management tool
for Cisco Routers Switches Firewall
deviceexpert.com/cisco-config

Unlocking True ERP Value

PwC Insights & Strategies On Making
ERP Work Smarter For Your
Business.
www.pwc.com/us/erp

Sponsor Links

[Try QNX embedded RTOS & tools FREE for 30 days](#)
[Track & Manage Your Source Code--Free Download!](#)
[Search over 90K tech jobs at Dice.com.](#)
[You want Linux? And you want it fast?](#)
[Across the country. Ahead of our time.](#)
[SourceForge.net CCA 2008: Where Open Source Wins](#)

© Copyright 1999-2008 - [SourceForge](#), Inc., All Rights Reserved

About [Linux.com](#) - [Privacy Statement](#) - [Terms of Use](#) - [Advertise](#) - [Trademark](#) - [Ask Linux Questions](#) - [Write for Us](#) - [RSS Feed](#)
[ThinkGeek](#) - [Slashdot](#) - [SourceForge.net](#) - [freshmeat](#) - [Surveys](#) - [Jobs](#)

