

Re: Connection Sharing on demand

Source: <http://linux.derkeiler.com/Newsgroups/comp.os.linux.networking/2006-04/msg00228.html>

- *From:* ibuprofin@xxxxxxxxxxxxxxxxxxxxxxxxxxxx (Moe Trin)
 - *Date:* Sun, 09 Apr 2006 20:47:32 -0500
-

On 9 Apr 2006, in the Usenet newsgroup comp.os.linux.networking, in article <1144622185.434748.258620@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>, Luiz Borges wrote:

Assume – old PC is dialing in now.

Not dialing, its broadband and is always connected.

OK, then you are loosing me. Are you wanting something such that the user has to authenticate for each time they want an Internet service, and then have the connection drop after they are finished, or a set amount of time? That can be done as a firewall application with lots of wrappers, but I'm not sure what benefit it gives. You can also block all Internet access, and run an application server – where your users can log in and run selected Internet applications, perhaps with firewall restrictions of where they can connect.

Right now it uses static addressing, I planning in changing to DHCP to simplify future changes in network, and throw away all those IP listings.

That seriously complicates security. DHCP was *_never_* even semi-secure. Remember that for IP, there is no authentication in the protocol, and what little security you have is on IP and MAC addresses. Any extra security has to be built into the application layer.

When I said dial-up-like, I meant the user has to click a connection to input user and pass to get connect to the internet, and not really dial to ISP.

It can be done. For one example, you'd have the user connect to a server program on the gateway that accepts username/password, and that program then allows connections through the firewall for that IP or MAC address for

Re: Connection Sharing on demand

some set amount of time, or activity. The problem is that it is trivial to spoof IP and MAC addresses. Better would be simply blocking all Internet access from the desktop (easy firewall setup), and having the users SSH into the server and run Internet applications from there (only this computer is given access to the Internet). From a network point that is easy, and setting up an application server shouldn't be that hard. But when the user is allowed Internet access, what limitations apply? Protocol? Destination port number? If you need more than that, perhaps a proxy server would be a better solution. Another problem is file transfer – whether mail, FTP or downloaded web pages. What access do you give – and how to safely restrict it.

The "advantage" of the first (controlled gateway) or second (proxy) approach is that your users are still using their own computers that they are familiar with. If these are windoze, you still have the virus problem and so on. The advantage of the third (application server) approach is that it is one box that can be hardened very much. A problem occurs if the box is running Linux or BSD – while a lot of things look similar to windoze, these are different, and so there will be a training issue.

But then, there are also so many different brands of beer and cars and...

I know about that, that's why I taking suggestions... ;)

The distributions are exactly like cars or beers. They really are (at least) very similar, and the differences – the "which one is better" – is all personal opinion. The application you need (even assuming a proxy server will do) doesn't exist "out of the box". At the very least, you'd have to configure it. All distributions can do what you want. The question then becomes which one is more suitable for you. I don't speak Portuguese, but Conectiva (which is a Brazilian distribution) has an excellent reputation. There was a 'Console' Linux from Brazil as well. The advantage – the documentation is in your native language. On the other hand, a very small text only distribution might be more suitable as a firewall type device.

For what it is worth, I'm a network admin at a local division of a large company. Our users have "full" access at all times, except that we block access to many networks that are not "job related" – and there is written policy that describes how the network can be used. If the employees violate that policy, there is disciplinary results. Your original post mentioned blocking inbound connections – that's trivial to do with the firewall, but it is also in that policy.

Old guy

.