

Re: Internet Sharing – Security

Source: <http://www.derkeiler.com/Newsgroups/comp.security.firewalls/2002-04/0080.html>

From: Jeremy Marks (jmarks@futurenet-consulting.com)

Date: 04/01/02

From: jmarks@futurenet-consulting.com (Jeremy Marks)

Date: Mon, 01 Apr 2002 19:38:31 GMT

Can you recommend the steps that I would need to take once I have OpenBSD 3.0 installed on my system.

Can you recommend the best instructional pages on the web to accomplish what I need?

Thanks.

On Mon, 01 Apr 2002 02:04:04 GMT, "Berk S. Daemon"
<someone@somewhere.com> wrote:

>
> "Jeremy Marks" <jmarks@futurenet-consulting.com> wrote in message
> <news:3ca78713.18760716@news.west.cox.net...>
>> Thank you for your post. A few more points to make:
>> 1. Company A: Their T1 line (As well as all of their telephone
>> lines) is cross connected between their computer room in their suite
>> and their 1st floor demarc. This area was unable to be found
>> (probably in another suite that we had no access to).
>>
>> Therefore, for simplicity, the current high speed connection and
>> router had to stay in A's computer room. So, we ran a cable from A's
>> computer room to the 1st floor demarc, found an extra four pair of
>> cabling that went to the ground floor's main demarc/telco room (approx
>> 120feet through conduit) and patched it over. This brought us a
>> connection from A to the main building demarc room.
>>
>> 2. Company B (my client): has a cat5e cable run approximately 240 feet
>> from main demarc to its suite (2nd floor).
>>
>> Our main idea was to put the internet sharing device in the main
>> demarc room (floor G1), share it using a firewall and routing, then
>> send to each company using a different IP segmentation and other
>> methods for accomplishing security. Having such short time, money and
>> all that, we used kept A's setup the same and merely plugged their
>> newly extended line into the hub, thus giving us a hot line down to
>> the main demarc (G1). We put a hub in between to boost the signal and

>> finished by sending the signal up to our tenant (B) on floor 2.
>>
>> Now that we successfully have gained the desired internet connection,
>> our client will be able to operate business come Monday morning. We
>> had two days to get a solution and I believe that we did admirably in
>> even getting internet to our client.
>>
>> Now, the question goes to two parts:
>> 1. Short-Term: how do we best segment and secure the networks so that
>> they can share the internet but not see the other company's
>> network--using the topology and cabling currently setup?
>> 2. Long-Term: how do we accomplish this in a month or two when my
>> client has its T1 operating and company A will be sharing of this?
>>
>> My guesses:
>> 1. Some hardware in the main telco room/demarc (G1) to share the
>> internet and secure company B's network.
>> 2. A linux box (or something similar) in the main telco room/demarc
>> (G1) to segment the networks and provide sharing.
>>
>> Any more insight? Thanks.
>>
>>
>>
>> On Sun, 31 Mar 2002 19:25:08 +0200, Tony Earnshaw
>> <tonni@billy.demon.nl> wrote:
>>
>> >Jeremy Marks wrote:
>> >
>> >> Thanks for reading this long post!!!
>> >> Jeremy
>> >
>> >
>> >I'm a Unix/Linux person :c)
>> >
>> >Sounds like a small setup ("hubs? Why not programmable switches?").
>> >
>> >If it isn't already, replace the router with a good firewall; resell the
>> >router to someone else for something else. For a small setup, an
>> >inexpensive Linux 2.4.x firewall with Netfilter and ISC DHCP is fine.
>> >
>> >Should cost you around \$2,000 for a top machine for this purpose. Linux
>> >costs you \$0,02.
>> >
>> >Logically ("in your head") segregate 192.168.0.0/16 (your own
>> >description) so that it becomes 192.168.1.0/24 and 192.168.2.0/24.
>> >Logically assign 1.0 to A and 2.0 to B.
>> >
>> >Determine the MAC number of each machine on the cable (this is only for
>> >a small setup. For a large setup this is an organisational nightmare).
>> >Let the DHCP server assign ip numbers on the basis of MAC numbers.

>>>
>>> *Configure the firewall/router to the Internet so that there is NO
>>> routing possible between the 1.0 and 2.0 subnetworks. Choose a basic
>>> policy of deny everything from everywhere to everywhere. This includes
>>> blocking 255.255.255.255 broadcasts and any calls to ports 137 through
>139.*
>>>
>>> *From what you say, your mail server, web server etc. are on the
>>> Internet (probably looked after by your ISP), therefore:*
>>>
>>> *Configure the router/firewall to do stateful/state aware NAT from the
>>> internal LAN to whatever external services are necessary, e.g. mail,
>>> http/shhttp, whatever you want. Block all traffic from the Internet to
>>> the internal LAN that is not stateful (in this case stateful = internal
>>> -> external and back only if a TCP or UDP connection is already
>>> established). Block all spoofing, source routing, rfc1918 traffic from
>>> outside.*
>>>
>>> *The above will work.*
>>>
>>> *If you don't know what I'm talking about, hire a Unix/Linux man who
>>> does. Look in the Netfilter (netfilter@lists.samba.org) mail list for an
>>> _experienced_ person in your district. Make sure you can get on with him.*
>>>
>>> *The whole cabling thing from your side was a botch up, because you
>>> wanted to get the assignment and listened too hard to "cost arguments".
>>> Never suggest a cabling solution such as this again! The two firms will
>>> sooner or later have to be cable-segregated, it should have been at the
>>> outset.*
>>>
>
> *I'm a UNIX/BSD guy... I used to be into Linux too but have moved on...*
>
> *What would make more sense for something like this is a simple OpenBSD
> (free'er than Linux you can say) Transparent Bridging Firewall to 'segment'
> the two RFC1918 based LANs while still allowing NAT without any subnetting,
> IP changes or what not.
> Especially if they're big networks, I wouldn't recommend re-subnetting for a
> temporary solution like this nor doing NAT over NAT, or even routing to
> another NAT'd segment.*
>
> *I'd personally recommend IPFilter www.ipfilter.net if you choose to do
> things the hard way like he mentioned, which will be more of a headache to
> implement and depending on the Linux distro will be more resource intensive,
> and less secure than say an OpenBSD firewall.*
>
> *IPFilter is nice in that it's not limited to just Linux, unlike
> IPTables/NetFilter – and does 'true' stateful inspection, not just
> pseudo-stateful inspection.
> Runs, on more platforms such as: FreeBSD, OpenBSD, NetBSD, Linux, Solaris,
> SunOS, HP-UX, x-mach, etc.. etc..*

>It's good in that if you know it for one, you know it for any! So you're not
>limiting yourself to just knowing one and one only, especially when you
>might need a better solution than Linux can offer such as OpenBSD
>Transparent Bridging Firewall.
>
>With the transparent bridging firewall that you can do in OpenBSD, you can
>still filter all packets as per normal, true fully stateful inspection
>firewalling, block source routing, IP options, short packets, fragments,
>modulate state, normalize the packets, etc..
>
>As of OpenBSD 3.0+ they have replaced IPF with PF (IPF still available if you
>prefer) but with PF you can get even more granular with things such as:
>
>State Modulation
>Packet Normalization
>Automatic Ruleset Optimization
>Variables
>Sets
>etc...
>
>Now with a transparent bridge (meaning, without any IP addresses) it is also
>a lot more secure than a conventional NAT Router/Firewall in that it's
>technically uncompromisable, in comparison to a firewall with IP addresses.
>As any bridge, it simple works at layer 2 forwarding packets between
>interfaces and thus allowing you to filter those packets that pass through
>the bridge.
>
>I'd even recommend this 'infront' of your main firewall.
>
>Other options in the works are Transparent NAT B–Router (bridging router,
>doing NAT without any ip addresses – seems impossible but it's not).
>
>If you need any advice, or any questions on this just lemme know and I'll
>help you out.
>
>Regards!
>
>

-
- **Next message:** [Bubba Jean: "Re: Zone Alarm connects to the Internet on startup"](#)
 - **Previous message:** [Mike: "Cisco VPN and Netopa r9100??"](#)
 - **In reply to:** [Berk S. Daemon: "Re: Internet Sharing – Security"](#)
 - **Next in thread:** [Berk S. Daemon: "Re: Internet Sharing – Security"](#)
 - **Reply:** [Berk S. Daemon: "Re: Internet Sharing – Security"](#)
 - **Messages sorted by:** [\[date \] \[thread \] \[subject \] \[author \] \[attachment \]](#)