

Re: Networking/Security Question...

Source: <http://unix.derkeiler.com/Mailing-Lists/FreeBSD/net/2004-09/0150.html>

From: Vince Hoffman (*jhary_at_unsane.co.uk*)

Date: 09/11/04

Date: Sat, 11 Sep 2004 12:11:11 +0100 (BST)

To: Dan <dan@skyinternet.co.uk>

On Fri, 10 Sep 2004, Dan wrote:

> *Hello.*

Hi Dan,

> *My first post here, Hope you're all well and enjoying the summer.*

> *Okay, this is likely to be an extremely exhaustive post, so I'd really be grateful if you could spare the time to read and reply please...*

>

> *Let me first introduce you to the scenario. We are a not for profit organisation that I'm dealing with during free time. We have fortunately (as it's Internet based) had funds to get a Leased Line – after about a year of negotiating with various UK providers, we finally got the price completely down – although still scarily high as we're a not for profit.*

>

> *As mentioned, I do this in my spare time, and do not lie I have "expertise" in this field. However, I have researched, and compiled a very simple step by step guide of what I *think* I should be doing to a) install the Leased Line and get it working, and b) secure the network.*

>

> *Please have a look through and comment on whether you agree, or where I've completely gone wrong. The Leased Line is due to be installed in a few weeks time, so basically I want to have a completely clear set of instructions and knowing I'm doing everything right so I'm not stumped when the time comes!*

>

> *Okay...*

>

> *I.*

> *Obviously complete the process to get the Leased Line.*

> *The will consist of 2 visits to the presmise, one to install an NTU and the other to install the circuit.*

>

Sounds right, I'm assuming a BT tail (ie you will get a BT box no matter

who your ISP is,) Although it can mean more or less visits for no reason i've ever worked out ;)

> 2.

> *The router will come "preconfigured" – not quite sure what that exactly involves. The router itself will be a Cisco 1721.*

>

If it means the same as where i work (small ISP) then it means that they will have the router configured and connected and you shouldnt touch it, other than to plug your switch/firewall in unless they say to. If they dont connect it all you need to do is plug the router in, attach the router to the MTU (this can be in a number of ways but i'll assume an E1 (2Mbps) line which is normaly presented as X.21 (uses a thickish blue green cable whith a D plug at each end, the cisco end has a higher density of pins) As i say though your ISP should connect this or talk you through it.

> *As I want to perhaps support up 4 or 5 PC's through the connection my new*

> *ISP's response regarding it was: "The 1721 will allow as many PC's as*

> *you*

> *wish to connect. The machines would need to be networking together but*

> *the*

> *whole network can be given access by a single router. With regards to*

> *IP's we*

> *will allocate a block of 8 IP's with the leased line. These could be*

> *assigned*

> *to individual machines (one will be needed for the router).*

>

quick comment here. 8 IPs = /29 or 255.255.255.248 netmask. this does not mean 8 usable IPS. it means 6 usable (minus broadcast and network number) minus the router gives 5 usable, just enough but no spare unless -- see my preferred setup below.

> *To achieve this, as I'd ideally like each machine to have a "public"*

> *internet address. To explain myself:*

>

> *PC1: 211.167.0.1 -- running a HTTPD. -- running FreeBSD.*

> *PC2: 211.167.0.2 -- running a mail daemon. -- running FreeBSD.*

> *PC3: 211.167.0.3 -- just internet access. -- running XP.*

> *PC4: 211.167.0.4 -- again internet access. -- running XP.*

> *PC5: 211.167.0.5 -- internet access through a Netgear HE102 Access*

> *Point and Netgear HA501 PC card. -- running XP.*

>

> *I have no idea what the IPs would be, but I'm sure you'll get the point*

> *I'm trying to make...*

> *Therefore to achieve that, I'll need to purchase a Switch that would*

> *plug into the Router itself.*

>

> *I want to use an External Switch to link all the PC's to the connection.*

freebsd-net: Re: Networking/Security Question...

- > *With advice from some people, it seems people prefer Swithces to Hubs*
- > *because it only directs data when it's needed. Are you able to recommend*
- > *a decent 8 port external switch that'd be suited? I searched sites like*
- > *dabs.com and there's just so many, I don't which are suitable.*

Again down to personal preference really, get the best you can afford.

- >
- > 3.
- > *This switch would need to be connected to the Router with a Cat5 cable*
- > *- could you advise what port it'd go into?*
- > *I tried reading the guide at*
- > *<http://www.cisco.com/univercd/cc/td...hig/1721ovw.htm> about the Ethernet,*
- > *Auxiliary, and Console port, and I *think* it's the Auxiliry one?*
- > *Is the "Ethernet" port used to actually connect the router to the NTU?*

No the Ethernet is for your use, plug the router into the ethernet port.

- >
- > 4.
- > *Each PC wanting to access the connection, including 3 PC's and one*
- > *laptop would need to do the following:*
- > *2 x FreeBSD servers would need a Cat5 cable from an Ethernet card in*
- > *the Boxes to the Switch.*
- > *1 x Windows machine would need a Cat5 cable from an Ethernet card in*
- > *the box to the switch.*
- > *1 x Laptop (Netgear HE102 Access Point) talking to a HA501 PC card on*
- > *the Laptop.*
- >
- > *In the FreeBSD machines, I'd need to use the following in /etc/rc.conf:*
- > *ifconfig_sis0="inet the.ip.here netmask 255.255.255.0"*

No 8 IPS is not 255.255.255.0, use the netmask your ISP provides, (most likely /29 == 255.255.255.248

- >
- > *where sis0 is the Ethernet in that particular machine, "the.ip.here"*
- > *the public IP assigned to me by the ISP (I'll be getting a block of them)*
- > *and ensure /etc/hosts and /etc/resolv.conf are all set.*
- > *I'd also need to repeat this on the 2 Windows machines, though their*
- > *setup is very simple...*
- >
- > *Do you agree this is the right idea for the actual "network setup"?*
- >

Couple of points, unless you are expecting very high traffic and or the website is a complex scripted thing with a sql backend, Web and Mail can easily run from one box/IP but thats a personal preference thing, Also is there a reason for each workstation to have a real IP ? Windows directly exposed to the internet is rarely a good thing, even with XP sp2 having the firewall on by default.

My preferred setup here would be to have a FreeBSD firewall (2 network cards) connected to the router with a crossover cable, and to the switch with the other network card. The firewall has all the external IPs assigned to its external interface, and a private IP on its internal interface. Give your mail and web servers internal IPs, Setup IPFW/IPF and NATD/IPNAT as preferred to NAT all traffic sent to the IP you want to belong to your mailserver to the mailserver's private IP, and the same with the webserver. Setup appropriate firewall rules limiting access to your web and mail server. 1 set of firewall rules to maintain instead of many.

NAT your workstations to another IP and possibly setup a DHCP server on one of your FreeBSD servers for your Windows clients, this allows more flexibility for growth in network usage i.e. you have a visitor with a laptop wants to access the internet via the Netgear access point, can be done with your setup unless someone else gives up their IP. This way also leaves one external IP spare for future useage.

Setup the Firewall to have the router as its default route and everything else to have the firewall's internal IP as their gateway, make sure the firewall has `gateway_enable="YES"` in `rc.conf`.

Talking of access points, make sure you use some kind of security on it. WEP is still probably the easiest and better than nothing, but have a look what your AP and clients support.

> Now my questions begin regarding security for the services in particular. Would it be "sufficient" to just run IPFW rules on each of the FreeBSD servers, and software firewalls on the Windows machines? Or, could you recommend a Hardware Firewall that and how it'd integrate into the above setup please?

See above.

I use `ipf` so I can't really comment on IPFW commands.
(IPFW seems very good I have just never got round to learning it.)

> For the FreeBSD machines I thought the following rules (again researching to find these – but I may very well be incorrect):

```
>
> # Define the firewall command (as in /etc/rc.firewall) for easy
> # reference. Helps to make it easier to read.
> fwcmd="/sbin/ipfw"
>
> # Force a flushing of the current rules before we reload.
> $fwcmd -f flush
>
> # Allow all connections that have dynamic rules built for them,
> # but deny established connections that don't have a dynamic rule.
> # See ipfw(8) for details.
> $fwcmd add check-state
```

freebsd-net: Re: Networking/Security Question...

> *\$fwcmd add pass tcp from any to any keep-state*
>
> *# Allow all localhost connections*
> *\$fwcmd add 100 pass all from any to any via lo0*
> *\$fwcmd add 200 deny log all from any to 127.0.0.0/8*
> *\$fwcmd add 300 deny log ip from 127.0.0.0/8 to any*
>
> *# Allow all connections from my network card that I initiate*
> *\$fwcmd add allow tcp from me to any out xmit any setup keep-state*
> *\$fwcmd add deny log tcp from me to any*
> *\$fwcmd add allow ip from me to any out xmit any keep-state*
> *\$fwcmd add allow all from 192.168.0.0/24 to any*
>
> *# Everyone on the Internet is allowed to connect to the following*
> *# services on the machine. This example specifically allows connections*
> *# to sshd and a webserver.*
> *\$fwcmd add allow tcp from any to any keep-state*
> *\$fwcmd add allow tcp from any to me 80 setup*
>
> *# This sends a RESET to all ident packets.*
> *\$fwcmd add reset log tcp from any to me 113 in recv any*
>
> *# Enable ICMP: remove type 8 if you don't want your host to be pingable*
> *\$fwcmd add allow icmp from any to any icmptypes 0,3,8,11,12,13,14*
>
> *# Deny all the rest.*
> *\$fwcmd add deny log ip from any to any*
>
> *How's this?*
>
> *Obviously, for each there'd be different rules as they'll be running*
different daemons, so I'd just alter the \$fwcmd add allow tcp from any to
>me 80 setup line...
>
> *Thanks very much for reading, and I hope I've been clear in explaining*
>this "scenario" – I really appreciate your advice, and our community
>thanks you.

Your welcome.

Your suggestions look like they will work fine, but as i say, with no room for growth, and slightly more complex to maintain (more sets of firewall rules etc,) if slightly easier to seup.

Vince

>
> *Regards,*
> _____
> *freebsd-net@freebsd.org mailing list*
> *<http://lists.freebsd.org/mailman/listinfo/freebsd-net>*
> *To unsubscribe, send any mail to "freebsd-net-unsubscribe@freebsd.org"*
>

freebsd-net: Re: Networking/Security Question...

freebsd-net@freebsd.org mailing list

<http://lists.freebsd.org/mailman/listinfo/freebsd-net>

To unsubscribe, send any mail to "freebsd-net-unsubscribe@freebsd.org"