

Re: Public/Private network split.

Source: <http://www.derkeiler.com/Newsgroups/comp.security.misc/2004-02/0087.html>

From: BLH (*blh_9_at_hotmail.com*)

Date: 02/04/04

Date: 4 Feb 2004 02:16:23 -0800

freaknightproductions@yahoo.com (J. M. L.) wrote in message
news:<1624fd18.0402031213.42be061d@posting.google.com>...

> *Thank you for everyone's replies? I am a bit confused, but feel a*

> *little more confident.*

> *To address several points raised by BLH? User behavior falls outside*

> *the scope of the security I am trying to set up ? P2P bandwidth stuff*

> *can be cracked down on by blocking ports, If I'm not mistaken? If I*

> *only open up port 80, that means that the only IP application would be*

> *web browsers. I've raised the same concerns you have had with the*

> *owner, and if there proves to be a problem down the road, he will*

> *remove the service, or create user agreements, and MAC address*

> *registration, or some other arrangement.*

>

> *The only thing I am currently trying to address is the security of the*

> *staff computers on the network.*

>

> *Since my suggested set up wasn't clear, let me do it again.*

>

> *ISP*

> |

> | *- Phone Line*

> |

> | *ADSL MODEM (ISP UPLINK, PPPOE single IP address)*

> |

> | *-ethernet cable*

> |

> | *{Linksys Broadband Router (192.168.1.xxx)}*

> | | | *- ethernet cables*

> | | *{Various staff computers/swtiches}*

> |

> | *-ethernet cable*

> |

> | *{AS yet to be determined Router with wireless access point --*

> | *192.168.2.xxx}*

> | | | | *-802.11b*

> | | | |

> | *Various public wireless clients*

> |

comp.security.misc: Re: Public/Private network split.

- > *Okay? I understand that you can't filter out ethernet packets? that's*
- > *the transport that the TCP/IP protocols are piggy backed on? However,*
- > *I thought that if you used a router or switch, you could prevent*
- > *people from sniffing and spoofing packets from one side of the switch*
- > *to the other, or at least make it orders of magnitude more difficult.*
- > *When I asked if I was getting the kind of security I thought I was*
- > *with the above arrangement, this is what I was referring to.*
- >
- > *Is there a box out there that fits into the above diagram, that is*
- > *configurable enough to do lock down, and give me that type of*
- > *security? I don't want people on the wireless .2 network to sniff*
- > *packets and see what kind of equipment I am running, or do port scans*
- > *on the equipment on the .1 network.*
- >
- > *I know I could set up a linux box with a dual nick and have a*
- > *firewall, routing, etc under linux, except that falls outside the*
- > *scope of my expertise? Its got to cost under \$200, and have less then*
- > *10 hours of set up time (tweaking and configuring router, testing*
- > *security etc)) and its gotta just run without administration once it*
- > *is in place.*
- >
- > *Obviously not all consumer grade Broadband routers are created equal?*
- > *I've used linksys and SMC equipment in the past, and been happy enough*
- > *in my home network environments. Office/enterprise grade equipment is*
- > *fine, as long as I can figure out how to configure it, and it meets my*
- > *price point. Any recommendations on specific hardware or critiques of*
- > *the above diagram are definitely appreciated.*

I can't answer for your Linksys router but hopefully the following generic info should be of help.

Assuming that your Linksys broadband router has one LAN port or a layer 2 switch built in all of your staff devices will be on 192.168.1.xxx including the WAN port of the new wireless router. For example if the LAN port of your Linksys is 192.168.1.1 the uplink port of your wireless router could be 192.168.1.2 and the 802.11b side would be 192.168.2.xxx. Therefore the gateway for the wireless router would be 192.168.1.1 and the Linksys (which is also default gateway for your staff devices) would have a route back to 192.168.2.xxx otherwise web traffic would not be able to get back to the wireless users. Unless you are able to set up filters in the Linksys, devices on 192.168.2.xxx would be able to communicate with devices on 192.168.1.xxx networks, although they would not see packets only sent between 192.168.1.xxx devices or broadcasts. This is just basic routing.

If you don't want to play with filters or the Linksys is not able to you could consider a third router between the Linksys and your staff network which would put them on 192.168.3.xxx for example. In this way both networks would access the internet via 192.168.1.1 but could be invisible to each other.

comp.security.misc: Re: Public/Private network split.

Only opening port 80 on the wireless router could be a bit restricting
– what about https, nntp, ftp, telnet, ipsec, realaudio etc etc?

Just a few more pence worth

BH