

Public/Private network split.

Source: <http://www.derkeiler.com/Newsgroups/comp.security.misc/2004-01/0499.html>

From: J. M. L. (*freaknightproductions_at_yahoo.com*)

Date: 01/29/04

Date: 28 Jan 2004 16:29:17 -0800

I have a question concerning trying to set up a public/private network... I have a retail establishment with DSL service. I currently use a DSL router to share that connection amongst my various staff computers. I want to add a wireless access point to the network so that my customers can use my DSL connection to get to the net... however... I don't want them to be able to see/touch/talk to any of the computers on the private part of my network.

I'm looking for the simplest way to implement a separation of this network -- minimal software set up -- just a dedicated black box that I can stick between the networks. Here's what I thought would work.

Plug in a new wireless broadband router's uplink port to one of the network ports on my private network. Lock down this router so ONLY TCP/IP traffic goes through, and lock down which ports are open. Theoretically, this would create a private network inside my private network... No one connected to my wireless router would be able to sniff packets on the private part of my network, because Ethernet packets won't be routed past the wireless broadband router, and no one on this wireless network would be able to do anything that I didn't want them to do -- I could close up specific ports by configuring the wireless router.

My questions are -- Is this possible? Can broadband routers be chained together like this to create segmented networks? Does the address forwarding that goes on between the ISP's network, and the first router get properly forward to the second router, and the equipment hanging off the second router?

Second, Does this actually provide me with the security that I believe it does?

If the answer to my first question is no, is there some kind of black box firewall that I can put between my private network, and a wireless access point that will provide me the kind of network segmentation/security that I want? Since I do not own a wireless access point, I figured my first solution would be cheaper than two dedicated pieces of equipment, but I wanted to verify if this would

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

work or not.

Any suggestions appreciated.

-JL