

## Re: how to connect firewall to router

**Source:** <http://www.derkeiler.com/Newsgroups/comp.security.firewalls/2004-01/1985.html>

---

**From:** FT (*FT\_at\_nospam.kicks-ass.net*)

**Date:** 01/28/04

Date: Wed, 28 Jan 2004 22:29:46 +0000 (UTC)

"MyndPhlyp" <nobody@home.now> wrote in  
news:BQVRb.538\$jH6.224@newsread1.news.atl.earthlink.net:

>  
> <hamals@infinito.it> wrote in message  
> news:A8QRb.284657\$vO5.11560559@twister1.libero.it...  
>> Thanks for reply  
>>  
>> your explanation is very good....but if my adsl router has only one  
>> port  
> on  
>> lan side and this port is the firewall port, how can the firewall  
>> catch  
> the  
>> traffic for other IPs and direct it to the right pc?  
>  
> Thomas Hertel eludes to this. Maybe I can simplify with some  
> Networking 101.  
>  
> As packets travel a network, optimizations take place to route packets  
> to their intended destination based on the IP packet's network. (Yeah,  
> I know ... lots of double-talk that could just as well be found in a  
> politician's campaign speach.)  
>  
> I mentioned your netmask, network address, broadcast address and IP  
> addresses of at least 2 machines in your network. Your network also  
> recorded in ROUTE tables and DNS tables at your ISP. Your ISP's

Uh, DNS has nothing to do with how packets are routed on the internet.

> network is recorded in yet another ISP's (or InterNIC – the lowest  
> level authoritative "voice"). The whole thing acts like one big phone

The InerNIC hasn't assigned IP addresses for a number of years now. You're thinking of the IANA and the Regional Inernet Registries (ARIN, APNIC, RIPE and whatnot.)

## comp.security.firewalls: Re: how to connect firewall to router

- > *book. Each network knows what the various components are in their*
- > *little corner of the world and shares this information with the rest*
- > *of the world.*
- >
- > *As a packet travels through various relay points, a wrapper is placed*
- > *around the packet with information identifying the relay point as the*
- > *"reply to" machine. Your packet could be going through 10's or (heaven*
- > *forbid) 100's of relay points with each one adding more information to*
- > *the packet. It becomes a map of how the destination should respond.*
- >

No such thing happens. The packet may be put in various Layer 2 frames, but no actual routing information (besides the source and destination addresses) is added to the packet.

- > *When the packet gets to the destination, the destination unwraps all*
- > *the layers, locates the original message, responds appropriately and*
- > *rewraps the package sending it back to only that last relay point.*
- >
- > *The return process is the inverse of the sending process – as each*
- > *relay point receives the return message, it takes off its wrapper and*
- > *passes it to the next originator back through the chain.*
- >

Once again, the source and destination addresses are the only thing used to determine how the packet travels through the network.

- > *So (finally) we get back to your ADSL modem – just another relay point*
- > *for the Linux machine. If it were a private IP address, the ADSL modem*
- > *is actually the originator and it would look up in the NAT tables it*
- > *maintains to determine the ultimate final destination. Since your*
- > *Linux machine has a public address, the ADSL modem is not the*
- > *originator but rather just another relay point – the ADSL modem takes*
- > *off its wrapper and forwards the packet.*
- >
- > *The reason it must follow its original path on the return is because*
- > *that wrapper information contains MAC addresses – it's part of that*
- > *optimization I mentioned long ago.*
- >

Er, no. There is no guarantee that a packet going from point A to point B will take the same path as a packet going from point B to A will. Asymmetric routing happens all of the time on the internet.

- > *just firing the packet through your LAN network. All the devices on*
- > *your LAN "receive" that packet, but only the originator process the*
- > *packet's information – the rest discard the information. (Not the*
- > *complete truth, but it serves to illustrate the situation. Anybody can*
- > *listen in on a conversation if they can "hear" the packet.)*
- >

comp.security.firewalls: Re: how to connect firewall to router

That is only true if you are using a hub. Under normal circumstances an ethernet switch will only deliver ethernet frames to the port of machine that it is destined for.