

Re: Router's Firewall

Source: <http://www.derkeiler.com/Newsgroups/comp.security.firewalls/2002-10/5800.html>

From: luis (not@vaila.ble)

Date: 07/28/02

From: "luis" <not@vaila.ble>
Date: Sun, 28 Jul 2002 03:41:03 GMT

Hi Duane, thanks for your reply... I understand the risks of hosting web services from your own computers and that's why I don't do that, I use <http://blazingfast-communications.com/> . I use my home network for internal purposes only and I think ZoneAlarm does the job well in that regard. My concerns are more about what the router's capabilities are compared with ZA for the use I give to this network. Nevertheless your point has been taken and I am definitely consider your suggestions if I ever consider modifying my configuration.

Regards,
Luis

"Duane Arnold" <darnold92@Insightbb.com> wrote in message news:bbz09.56837\$uh7.6654@sccrnsc03...

> *Unless you are using Linksys model BEFSX41, which is the only model that*
> *indicates that it has firewall technology, then the router doesn't have a*
> *firewall. What your router does have is NAT. What that firewall is on*
> *BEFSX41, I don't know.*

>
> <http://www.homenethelp.com/web/explain/about-NAT.asp>

>
> *The current firmware being used by some Linksys routers do have the*
> *capability to incorporate a software firewall such has ZA. But ZA must be*
> *installed on a workstation, so how the router using ZA is protecting you*
> *entire network is beyond me.*

>
> *For most home users, ZA is a fine product which will protect a computer*
for

> *the most part. Port 80 is the WEB access port and port 21 is the FTP*
access
> *port on your machine.*

>
> *ZA is protecting those ports, because your not accepting or allowing any*
> *IP(s) to access those ports. But what if you decide you want a WEB site on*
> *one of your machines, then what? What are you going to do, only allow*
> *certain IP(s) access to your WEB site, or is the WEB site going to be open*
> *to the public, which means ZA is not blocking on any IP. I think you will*
be

comp.security.firewalls: Re: Router's Firewall

- > *using the later of the two.*
- >
- > *And there is the problem, because once a port is open, the router with its*
- > *NAT and SPI (Stateful Packet Inspection) are out of the picture. Well, SPI*
- > *is still in play a little bit, but ZA is out of the picture too. No*
software
- > *or appliance side firewall for the home market is going to protect your*
- > *machine once the port is open and the IP has been accepted and traffic is*
- > *flowing.*
- >
- > *So, let's say you have ACCEPTED an IP on port 80 and everything is cool*
NAT,
- > *SPI, and ZA are all cool with it, especially ZA, because ZA was told to*
- > *accept the IP. Now, what if that IP you accepted had it's own WEB site and*
- > *it was infected by a WORM or Trojan horse and one of them got put into the*
- > *network traffic, because that is what they do is reach out looking for*
other
- > *machines, between the two machines, what is going to stop it from*
reaching
- > *your machine?*
- >
- > *Nothing is going to stop it not NAT, SPI, or any firewall is going to*
stop.
- > *You could say that a anti virus software could stop it, but it is most*
- > *likely too late when anti virus software has detected it. Maybe a anti*
virus
- > *software that does real time scanning of files and memory would help, but*
- > *most people don't know to get that type of anti virus software.*
- >
- > *If ZA had an Intrusion Detection System (IDS) incorporated in it that*
- > *inspected the network traffic looking for anything malicious or suspicious*
- > *and block the IP, if found, then you would have some protection. ZA cannot*
- > *do this and none of the other ones can do it.*
- >
- > *The only one that can do this, actually look at network traffic and block*
- > *it, if something is malicious or suspicious in the traffic is BlackIce.*
- >
- > *BlackIce Defender a IDS/firewall is the only one that can protect the*
- > *machine in this manner. Not ZA, Tiny, Outpost, Sygate, which many consider*
- > *the best, or any of the other ones have IDS in them currently. So they*
- > *cannot do what BlackIce does to protect the machine.*
- >
- > *This same scenario happens in the reverse. If you go out to a Web site,*
you
- > *initiate the contact, that is infected, BlackIce will protect the machine.*
- >
- > *I went on about this a little bit, but you have the picture.*
- >
- > *Duane*
- >
- >

comp.security.firewalls: Re: Router's Firewall

> "luis" <not@vaila.ble> wrote in message
> news:DMv09.185613\$uw.99200@rwcrrnsc51.ops.asp.att.net...
> > Hi,
> > I would like to know how the firewall in the router works... and what
this
> > messages from the router's log would mean:
> >
> > Saturday, July 27, 2002 3:08:39 AM Unrecognized access from
> > 162.84.251.167:22339 to TCP port 21
> > Saturday, July 27, 2002 3:10:09 AM Unrecognized access from
> > 66.106.6.227:2917 to TCP port 80
> > Saturday, July 27, 2002 3:10:12 AM Unrecognized access from
> > 66.106.6.227:2917 to TCP port 80
> > Saturday, July 27, 2002 4:43:00 AM Unrecognized access from
> > 66.148.161.19:59483 to TCP port 21
> > Saturday, July 27, 2002 4:43:03 AM Unrecognized access from
> > 66.148.161.19:59483 to TCP port 21
> > Saturday, July 27, 2002 4:43:09 AM Unrecognized access from
> > 66.148.161.19:59483 to TCP port 21
> > Saturday, July 27, 2002 4:43:21 AM Unrecognized access from
> > 66.148.161.19:59483 to TCP port 21
> > Saturday, July 27, 2002 5:25:13 AM Unrecognized access from
> > 61.34.16.130:3284 to TCP port 53
> > Saturday, July 27, 2002 5:25:16 AM Unrecognized access from
> > 61.34.16.130:3284 to TCP port 53
> > Saturday, July 27, 2002 5:41:48 AM Unrecognized access from
> > 217.136.33.167:2717 to TCP port 21
> > Saturday, July 27, 2002 5:41:51 AM Unrecognized access from
> > 217.136.33.167:2717 to TCP port 21
> >
> > I am using ZA Pro in my computers and I know that any scan is being
> blocked,
> > I wonder if the routers is able to do that.
> > I know that Linksys installs ZA into their routers but all the routers I
> saw
> > claimed firewall protection as well.
> >
> > Thanks for your attention.
> > Luis.
> >
> >
> >
> >
> >

-
- **Next message:** [djtech: "KERIO & ICS & WINXP"](#)
 - **Previous message:** [Stephen Green: "Re: Zone Alarm Settings Help Please!!!"](#)
 - **In reply to:** [Duane Arnold: "Re: Router's Firewall"](#)
 - **Next in thread:** [Tracker: "Re: Router's Firewall"](#)
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)