

Re: Linksys router as Firewall

Source: <http://www.derkeiler.com/Newsgroups/comp.security.firewalls/2003-07/1057.html>

From: Leythos (void_at_nowhere.com)

Date: 07/19/03

Date: Sat, 19 Jul 2003 14:48:05 GMT

In article <jh1hhv48ncnrf1dpsb9tm1lf648lpv4uso@4ax.com>, badnews@hansenonline.net says...

> On Fri, 18 Jul 2003 14:52:25 GMT, Leythos spoketh

>

> >firewall:

> >1. A computer that (

> >(b) regulates traffic between those networks for the purpose of

> >protecting the internal network from electronic attacks originating from

> >the external network.

>

> The BEFSR41 router does that.

None of the Linksys line provide filtering of the INBOUND connections that are FORWARDED – there is nothing inspected in the forwarded ports.

So, while it does isolate the external from the uninvited internal, it

has no means to inspect the packets for content (as most firewalls do).

> > The firewall is capable of handling the following

> >tasks: (a) isolating internal and external traffic (a bridge service);

>

> The BEFSR41 router does that.

The Linksys does not isolate internal from external, only external from

internal. Anything on the inside can get out without any restrictions

(unless you do MAC filtering or port filtering).

> >(d) filtering outgoing traffic for security and network usage rules

> >(filtering or monitoring service);

>

> The Linksys router does that.

It does not. You can filter outbound based only on MAC, IP, and PORT.

There is nothing to in any of those methods that allow the Linksys to

check the content of those packets.

>

> >(e) filtering incoming traffic for rogue data (viruses, spam,

> >inappropriate data (filtering), or improper actions (port scanning,

> >overload prevention, etc.;

comp.security.firewalls: Re: Linksys router as Firewall

>

> *Virus scanning and spam filtering is not a function of a firewall.*

All Firewall products (real ones) allow you to block attachments, headers, etc.... None of the Linksys do this. I don't think the (e) was suppose to mean that it scans the data, more that it allows admins to block file types and such.

> *The BEFSR41 router reports on some "improper actions" (port scanning), and also protects internal clients from "overload".*

The Linksys line can not determine a Syn Flood and then block the IP, it can block the Syn, but does not have the ability to add the IP to a block list – same with other forms of attacks. Spam filtering would only be done by block lists of IP's.

> >(f) *blocking forbidden external services or addresses (blocking, "network nanny"-functions);*

>

> *The BEFSX41 does have URL filtering, but not the BEFSR41*

None of them have the ability to subscribe to a list service that provides IP's of known bad subnets/IP or a web screening service. It would be nice if they added that feature, but then each device would need about 128MB of ram in it.

> >(i) *converting between different network protocols on different protocol levels (bridge when handling lower level protocols, gateway when handling higher level protocols);*

>

> *Got me there...*

>

> >(j) *traffic diverting (e.g., for cost optimizing, accounting, network planning, monitoring);*

>

> *Nope.*

>

> *So, I guess even the simple little BEFSR41 router fits most of the criteria for a firewall, doesn't it? Yet, it's hardly considered a firewall by any standard ...*

The linksys (all of them, and the D-Link, and others) are not firewall appliances, they are NAT boxes with some limited filtering ability. While most home users will greatly benefit from their use, they are not firewall appliances.

I always tell anyone with DSL or Cable (or a modem) that they need at least a router to keep people from getting "Direct" access to their systems from the net. I like the Linksys line of personal routers.

> *FWIW, the BEFSR41 is a barrier between a private and public network, and*

comp.security.firewalls: Re: Linksys router as Firewall

- > *it does a reasonably good job keeping the public network off the private*
- > *network, but not so good the other way around. The lack of granular*
- > *control of inbound/outbound connections are one of the biggest downside*
- > *to most of these small, cheap NAT routers...*

Lars – I agree with you. I can almost always be sure when I see your posts that I will agree with everything you type.

I used a linksys BEFSR41 for 3 years at home before I purchased a WatchGuard Firebox II. Now with a 4 meg pipe I need the FB-II and all it offers.

--

--

spamfree999@rrohio.com
(Remove 999 to reply to me)