

Re: Linksys router as Firewall

Source: <http://www.derkeiler.com/Newsgroups/comp.security.firewalls/2003-07/0947.html>

From: Leythos (void_at_nowhere.com)

Date: 07/17/03

Date: Thu, 17 Jul 2003 12:39:09 GMT

In article <iklchvcvtqf2a378255jydcovtn5bri3fp@4ax.com>, noemail@noemail.net says...

> On Tue, 15 Jul 2003 02:50:23 GMT, "mhicaoidh"

> <mhicaoidh@hotmail.com> wrote:

>

> > Taking a moment's reflection, IOStorm mused:

> > |

> > | You might be confused about the definition of the term firewall.

> >

> > > In a loose definition, I suppose you could call NAT a firewall.

> > > However, the firewall effect is a by-product of how a NAT router works.

> > > Routers are not anywhere near firewalls in terms of being able to control

> > > specific packets and ports. If in response to an out-bound packet, the

> > > router will let anything and everything through. You can play a bit with

> > > Port Forwarding, Triggering, and the like ... but a router alone is still

> > > not a firewall by any industry standard.

>

> A firewall is a device or software between the local system and the

> internet, period.

I can see that you've never worked in a position that required any knowledge of security. A firewall is defined as follows:

firewall: 1. A computer that (a) acts as an interface between two networks (e.g., the Internet and an private network, respectively), and (b) regulates traffic between those networks for the purpose of protecting the internal network from electronic attacks originating from the external network. The firewall is capable of handling the following tasks: (a) isolating internal and external traffic (a bridge service); (b) making internal addresses invisible and directly unaccessible from outside and passing through authorized traffic after proper checking (a proxy service); (c) facilitating protected (encrypted) connections to cooperative parties over public networks (a tunneling service); (d) filtering outgoing traffic for security and network usage rules (filtering or monitoring service); (e) filtering incoming traffic for rogue data (viruses, spam, inappropriate data (filtering), or improper actions (port scanning, overload prevention, etc.); (f) blocking forbidden external services or addresses (blocking, "network nanny"–

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

functions); (g) providing log-in services for authorized outside users and simulating the approved outside user as an inside user (proxy, log-in server); (h) caching network traffic (cache service); (i) converting between different network protocols on different protocol levels (bridge when handling lower level protocols, gateway when handling higher level protocols); (j) traffic diverting (e.g., for cost optimizing, accounting, network planning, monitoring); (k) providing consistent, open entry to the internal network (portal service) and facilitating public network address and connection sharing (proxy service). 2. [A] system designed to defend against unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both. [INFOSEC-99] Synonyms front-end security filter, proxy.

--
--

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