

RE: [fw-wiz] Comparisons between Router ACLs and Firewalls

Source: <http://www.derkeiler.com/Mailing-Lists/Firewall-Wizards/2004-01/0011.html>

From: Bill James (*bubbagates_at_comcast.net*)

Date: 01/03/04

To: "'David Pick'" <d.m.pick@qmul.ac.uk>

Date: Sat, 3 Jan 2004 17:29:47 -0500

The problem with using ACL's is the load they can add to a router. Most of Cisco's newer IOS' have IP Inspection and do OK but can add a tremendous load on the router. I have seen problems with IP Inspection process for smtp on IOS creating issues with the Domino Email server (Lotus Notes) where a PIX and IPTables have no issues at all

Logging for a firewall based router leaves allot to be desired. I have implemented Router, IPTables and PIX based firewalls and logging is pretty good for both PIX and Iptables depending on the level you choose....

At home I use IPTables for my firewall and have pretty good luck with it

Bill James

The objective of all dedicated employees should be to thoroughly analyze all situations, anticipate all problems prior to their occurrence, have answers for these problems, and move swiftly to solve these problems when called upon.

However, When you are up to your ass in alligators it is difficult to remind yourself your initial objective was to drain the swamp.

> -----Original Message-----

> From: *firewall-wizards-admin@honor.icsalabs.com*

> [*mailto:firewall-wizards-admin@honor.icsalabs.com*] On Behalf

> Of David Pick

> Sent: Thursday, January 01, 2004 6:17 PM

> To: *sd2mcleo@engmail.uwaterloo.ca*

> Cc: *firewall-wizards@honor.icsalabs.com*

> Subject: Re: [fw-wiz] Comparisons between Router ACLs and Firewalls

>

>

> There are several different "firewall" technologies that work

Firewall-Wizards: RE: [fw-wiz] Comparisons between Router ACLs and Firewalls

> *at different layers in the protocol stack. One of these is*
> *"packet filtering" and router ACLs are just one particular*
> *implementation of this general technique. They are, in the*
> *real world, an important implementation because there are*
> *usually more routers than there are firewalls in a network*
> *and using this allows more control points to be used and*
> *also allow for more depth to your defences.*
>
> *In the network I control at my place of work we're replacing*
> *Cisco routers by PCs running FreeBSD and IPFilter so that we*
> *can have better controls at more levels in the protocol stack*
> *than is provided by simple ACLs.*
>
> --
> *David Pick*
>
> _____
> *firewall-wizards mailing list*
> *firewall-wizards@honor.icsalabs.com*
> *<http://honor.icsalabs.com/mailman/listinfo/firewall-wizards>*

firewall-wizards mailing list
firewall-wizards@honor.icsalabs.com
<http://honor.icsalabs.com/mailman/listinfo/firewall-wizards>