

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

**Source:** <http://www.derkeiler.com/Mailing-Lists/Firewall-Wizards/2004-01/0022.html>

---

**From:** Wes Noonan ([mailinglists\\_at\\_wjnconsulting.com](mailto:mailinglists_at_wjnconsulting.com))

**Date:** 01/04/04

To: "'Paul Robertson'" <[proberts@patriot.net](mailto:proberts@patriot.net)>, "'Marcus J. Ranum'" <[mjr@ranum.com](mailto:mjr@ranum.com)>  
Date: Sat, 3 Jan 2004 18:08:59 -0600

One of the problems that we had when I was working for a company that made network performance management tools was dealing with this exact issue. Because every packet size is variable in most networks (ATM, etc. are obvious exceptions), the impact that many things have on the performance of a network device becomes almost impossible to make a general baseline statement about, much to the chagrin of the sales force. This is so true that Cisco (and most other vendors) typically refer to a set 64K packet size in the small print on all of their performance metrics, although this is obviously an impossible number to achieve in the real world.

The obvious performance impact on a router with ACLs has to do with the fact that every packet now must be processed by the router before it can be forwarded. This also requires the router to be able to queue and buffer the packet during processing. I seriously doubt that anyone could produce numbers more accurate than "In my environment, generally speaking" or "in an absolutely controlled environment, this is what we saw". I agree with Paul here though that the when you start trying to do things to the router itself you can really see the performance impact some of these other things have. I can't count how many routers I have seen reboot when trying to show the running config because the router was under too much stress for whatever reason (often times BGP routers that are skimpy on RAM).

Thanks.

Wes Noonan  
[mailinglists@wjnconsulting.com](mailto:mailinglists@wjnconsulting.com)  
<http://www.wjnconsulting.com>

> -----Original Message-----  
> From: [firewall-wizards-admin@honor.icsalabs.com](mailto:firewall-wizards-admin@honor.icsalabs.com) [<mailto:firewall-wizards-admin@honor.icsalabs.com>] On Behalf Of Paul Robertson  
> Sent: Saturday, January 03, 2004 17:40  
> To: Marcus J. Ranum  
> Cc: Bill James; 'David Pick'; [firewall-wizards@honor.icsalabs.com](mailto:firewall-wizards@honor.icsalabs.com)  
> Subject: RE: [fw-wiz] Comparisons between Router ACLs and Firewalls

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

>  
> *On Sat, 3 Jan 2004, Marcus J. Ranum wrote:*  
>  
> > *I've never found any good studies of ACL performance. Do you have any*  
> > *references you can point us to?*  
>  
> *Cisco used to publish some "can do \$foo access lists without impact" stuff*  
> *with certain models. If we're lucky, maybe Brian will see this and post*  
> *some pointers.*  
>  
> *The not-normal-ACL stuff carries a heavy penalty - as the extended ACL*  
> *stuff does if you want silicon switching- I did a whole look at the*  
> *switching methods versus performance stuff a while back when writing*  
> *TruSecure's router essential config guide- and for almost everything (AIR,*  
> *there were two cards on one model where things sucked) you didn't get into*  
> *trouble until you had more rules than sense. I think I left most of the*  
> *switching mode stuff out of the document in the end, because it just*  
> *confused people.*  
>  
> *Now, send packets \*to\* the router, or send packets where the router has to*  
> *go to CPU land to process them, and things get significantly different*  
> *(which is why you really want to ACL off your routers from the rest of the*  
> *world.)*  
>  
> *Paul*  
>  
-----  
> ---  
> *Paul D. Robertson "My statements in this message are personal*  
> *opinions*  
> *proberts@patriot.net which may have no basis whatsoever in fact."*  
> *probertson@trusecure.com Director of Risk Assessment TruSecure Corporation*  
>  
> \_\_\_\_\_  
> *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>