

[fw-wiz] Problems logging deny's on Cisco Routers?

Source: <http://www.derkeiler.com/Mailing-Lists/Firewall-Wizards/2004-03/0046.html>

From: Scott C. Kennedy (*sck_at_nogas.org*)

Date: 03/08/04

To: firewall-wizards@honor.icsalabs.com

Date: Mon, 08 Mar 2004 20:21:28 -0000

Has anyone else seen problems logging on Cisco Routers for deny ACLs?

I've been using Routers with ACLs for years and have never had problems for those sites too small or too diverse to use actual firewall devices. Yet, now I have a problem with a site that is using Cisco routers with 'extended' ACLs yet, the final line 'deny ip any any log' is not logging all the information.

In tests with NMap for the first 1,024 ports, the router only logs 30% of the UDP ports scanned and only 1% of the TCP ports scanned. This was a standard NMap full-TCP connect scan, with no odd flags.

So, what gives? Is this normal for Cisco Routers to not keep accurate logs of denied packets? If so, then how are you supposed to support ACLs on these devices without accurate logs. I'd expect some log drops under high stress, but these routers are barely putting 1 mb/s of traffic through them, and are less the 5% CPU busy, thus they should be able to provide higher than 1% accuracy.

Scott

firewall-wizards mailing list

firewall-wizards@honor.icsalabs.com

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