

## Re: protecting DHCP servers

**Source:** <http://www.derkeiler.com/Mailing-Lists/securityfocus/focus-linux/2002-05/0033.html>

---

**From:** Carl R. Friend ([cfriend@mathworks.com](mailto:cfriend@mathworks.com))

**Date:** 05/21/02

Date: Tue, 21 May 2002 13:46:55 -0400

To: Seth Arnold <[sarnold@wirex.com](mailto:sarnold@wirex.com)>, Akop Pogosian <[akopps@CSUA.Berkeley.EDU](mailto:akopps@CSUA.Berkeley.EDU)>

From: "Carl R. Friend" <[cfriend@mathworks.com](mailto:cfriend@mathworks.com)>

At 18:22 2002/05/17 -0700, Seth Arnold wrote:

>e.g., if your dhcp server has two NICs:

>

>eth0 is connected to the untrusted network

>eth1 is connected to trusted subnet

>

>you would want as some very early rules to block packets with source

>0.0.0.0 from entering on interface eth0. You would block similarly

>source 255.255.255.255, sources 10.x.x.x, or 172.xx.x or 192.168.x.x

>from entering on eth0, if the untrusted network would always have valid

>routable IPs, or perhaps require IPs in one of those ranges if the

>network connected to eth0 has IPs in only that range.

It would help here to know what DHCP server is running on the host on which iptables rules are sought for. If the server is the ISC one, one should remember that that particular implementation functions much as a sniffer and actually sits *\_ahead\_* of the iptables rulesets. In this case, the best practise would be to drop incoming DHCP packets (or those that look like incoming DHCP packets) before they ever reach the DHCP server; the border router is most likely the place for this.

Cheers.

---

| Carl Richard Friend (UNIX Sysadmin) | The MathWorks |  
| Minicomputer Collector / Enthusiast | Natick, Massachusetts |  
| [mailto:carl\\_friend@mathworks.com](mailto:carl_friend@mathworks.com) |-----+  
| <http://www.ultranet.com/~crfriend/museum/> | ICBM: 42:18N 71:21W |

---

- **Previous message:** [Scott Gifford: "Re: protecting DHCP servers"](#)
- **In reply to:** [Seth Arnold: "Re: protecting DHCP servers"](#)
- **Next in thread:** [Scott Gifford: "Re: protecting DHCP servers"](#)
- **Messages sorted by:** [\[ date \]](#) [\[ thread \]](#) [\[ subject \]](#) [\[ author \]](#) [\[ attachment \]](#)