

## Re: firewall question

**Source:** <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2002-02/0062.html>

---

**From:** John Adams ([jadams@inktomi.com](mailto:jadams@inktomi.com))

**Date:** 02/14/02

Date: Thu, 14 Feb 2002 12:04:14 -0800 (PST)  
From: "John Adams" <[jadams@inktomi.com](mailto:jadams@inktomi.com)>  
To: leon <[leon@inyc.com](mailto:leon@inyc.com)>

On Wed, 13 Feb 2002, leon wrote:

> *So to reiterate; is there a way to configure pix or checkpoint to  
> judge the connection based on protocol as opposed to arbitrary things  
> like source ip, destination IP or port numbers?*

Here you're discussing a type of firewall known as a application-aware (or context-aware) firewall. They're available, but the time it takes to process individual packets and recognize if they are of the correct application can impact performance.

Application level proxies fall into this class (but are not transparent to the end user), and some features on the Cisco PIX (like the application aware 'fix-ups' help to close up application holes.

There's no way right now to have the PIX deny based on application traffic, but if you look at the filter language on the checkpoint, it would be trivial to write an application aware handler for specific ports.

(If you really want to hose the AIM users, though, completely blackhole [login.oscar.aol.com](mailto:login.oscar.aol.com) and 198.81.24/24)

--john

--

John Adams . Sr. Security Engineer . Inktomi Corporation  
[jadams@inktomi.com](mailto:jadams@inktomi.com) . Security Operations . FC 2.2.36  
My options are not that of Inktomi Corporation, nor do they  
represent any security policies or practices that may be in use.

---

This list is provided by the SecurityFocus Security Intelligence Alert (SIA) Service. For more information on SecurityFocus' SIA service which automatically alerts you to the latest security vulnerabilities please see: <https://alerts.securityfocus.com/>

---

• **Previous message:** [Edward Jones: "Gradute Survey"](#)

SecurityFocus Penetration: Re: firewall question

- *In reply to:* leon: "firewall question"
- *Next in thread:* dr.kaos: "Re: firewall question"
- *Messages sorted by:* [ date ] [ thread ] [ subject ] [ author ] [ attachment ]