

## RE: The old question...

*Source:* <http://www.derkeiler.com/Mailing-Lists/securityfocus/focus-ids/2001-09/0168.html>

---

**From:** Robert D. Hughes ([rob@robhughes.com](mailto:rob@robhughes.com))

**Date:** 09/30/01

Subject: RE: The old question...

Date: Sat, 29 Sep 2001 21:01:35 -0500

Message-ID: <B95B566BD245174196CA4EE29E5818830D5FCB@HEXCH01.robhughes.com>

From: "Robert D. Hughes" <[rob@robhughes.com](mailto:rob@robhughes.com)>

To: "Matt Collins" <[matt@clues.com](mailto:matt@clues.com)>, <[Donovan.Denis@emc.com](mailto:Donovan.Denis@emc.com)>

Well, for one, I'm thinking that a proxy server for all those services that you're concerned about could go a long way towards alleviating your concerns. For instance, the Cyberguard firewall, when run in proxy mode, shuts down all the IM clients trying to tunnel through http traffic, or any other data-type that doesn't conform to legitimate requests and that is passed through the proxy. And since the firewall understands what's coming back, the same applies to return traffic. Further, you can proxy inbound traffic to your servers. The smtp proxy alone is very powerful in that you can block subjects, disallow certain characters (control characters are my favorite to block) from being sent to your mail server, etc. And I have an example of how to redirect the code red worm to a null port using the http proxy feature.

I understand where you're going, and you make very legitimate points. However, most of these are "dumb" protocols and the firewalls don't actually examine the traffic. Also, most applications other than file sharing apps tend to look a lot like normal traffic until you actually do a packet trace. Consider that you have someone running an IM client tunneled on port 80. They get a message. Its really on a few hundred bytes, and looks like a normal http response since when these things are running in proxy mode, message to them are sent to a server and their client regularly interrogates the server for new messages. I suppose with that you could look for clients that constantly connect to a single server, but a stock ticker or news ticker would do the same thing if it didn't just maintain a constant connection.

Anyway, the short answer to your question is that yes, I've heard some discussion on this topic, but no, I haven't heard any real conversation on it. But off the top of my head, I can't think of anything other than proxying and filtering all your connections both inbound and out that would do what you want.

Rob

SecurityFocus IDS: RE: The old question...

-----Original Message-----

From: Matt Collins [mailto:[matt@clues.com](mailto:matt@clues.com)]

Sent: Friday, September 28, 2001 6:08 AM

To: [Donovan\\_Denis@emc.com](mailto:Donovan_Denis@emc.com)

Cc: [Cedric.Royer@getronics.com](mailto:Cedric.Royer@getronics.com); [focus-ids@securityfocus.com](mailto:focus-ids@securityfocus.com)

Subject: Re: The old question...

On Fri, Sep 28, 2001 at 05:01:21AM -0400, [Donovan\\_Denis@emc.com](mailto:Donovan_Denis@emc.com) wrote:

> *i don't claim to be an expert in ids but i did look into this*  
> *(albeit in a swithced environment) and this is what i came up with*  
> *Note that we were looking at commercial ids systems, been using*  
> *realsecure for a while now.*  
>  
> *cheers,*  
> *denis*  
>

Yeah, I've got a few replies like this. I'm pretty cogniscant of IDS deployment and operation from a vanilla "Buy a probe, put it in, tune to your traffic, sit back, enjoy" point of view, but what I'm talking about here is a much more specific issue.

to clarify, as a hypothetical:

We have data; firewall logs, proxy usage logs, IDS logs.

We know that use is made of that infrastructure for legitimate web browsing, stock tickers, news sites and the like.

We \*also\* know that folks are using that infrastructure for application data streams tunnelled inside of legitimate HTTP requests; Stuff like the Java RMI tunnelling via HTTP POST, ICQ proxies, HTTPtunnel servers giving desktop Socks servers, and so forth, that pretty much make a mockery of our risk control and assessment procededures; the firewalls, if they permit HTTP and SSL to arbitrary external hosts on arbitrary ports, permit any semiskilled computer user access to any external resource; and potentially any external resource access to the internal LANs.

The trick is ,as I see it, first to identify those misusing the infrastructure; my initial thoughts on that are by building a statistical profile of

RE: The old question...

## SecurityFocus IDS: RE: The old question...

"normal" http traffic. I expect this to be short snappy connections – retrieval of an HTML page or GIF image, for example, with a small amount of outbound traffic for URL requests, CGI submissions, cookie responses, etc.

I would expect "tunnelled" traffic to be of a different nature; much more evenly balanced inbound/outbound connections, those using CONNECT methods to be established for far longer than usual, for interactive sessions the data to be much lower throughput and more "spikey" in terms of transfer, and so on.

I guess I'm talking about a statistical analysis of traffic flow, throughput and duration patterns to try and identify people tunnelling applications via HTTP and SSL, with an eye to expanding that to other such more sophisticated and covert channels at a later date (Sending data as FTP transfer feeds, bundling data into "packets" for POST requests, etc)

Once we've found a way to identify such connections semi-reliably we can look at enforcing more rigorous controls on them.

What I'm asking is if anyone has methodically addressed these issues already, knows of a forum where such methods are being discussed, knows of a commercial product that attempts to address and identify/control such protocol usurpation (is that a word? ;-)) or has any initial ideas on how to proceed.

Anything would be helpful; I've looked at the W3C's http traffic analysis's, which are a good start, but further statistical data on traffic usage, methodologies for gathering such data from an arbitrary environment and identifying tunnelled traffic, etc, would all be appreciated ;)

Uhm. Any ideas? Anyone interested? Or is life still "We have pattern matches for known exploits, anything else configure the traffic you expect and alert on exceptions"?

RE: The old question...

## SecurityFocus IDS: RE: The old question...

That's not really a viable approach for an open internet border; we need to do analysis on traffic patterns, I think, as it's not possible to define each and every web site on the internet that folks might want to visit, and deny everything else, and then effectively ensure such a policy remains up to date.

Bleugh.

Matt

---

- *Previous message:* [¼°À++â Yune Sung: "Re: Evaluation for IDS"](#)
- *Maybe in reply to:* [Matt Collins: "The old question..."](#)
- *Messages sorted by:* [\[ date \]](#) [\[ thread \]](#) [\[ subject \]](#) [\[ author \]](#) [\[ attachment \]](#)