

RE: Help me

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/security-basics/2005-02/0369.html>

From: Randy Johnson (*randyj_at_holydiver.com*)

Date: 02/24/05

To: "'Tran Nguyen Vu'" <tran.vunguyen@gmail.com>, <security-basics@securityfocus.com>
Date: Thu, 24 Feb 2005 11:59:27 -0800

As a double check of what your ISP says, you could use MRTG to determine what kind of bandwidth your router is seeing.

Additionally, you could enable logging on your router to determine what / who /when these attacks are happening.

Further (although I'm not that familiar with ISA) doesn't ISA have the capability to log what it drops ?

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

From: Tran Nguyen Vu [mailto:tran.vunguyen@gmail.com]

Sent: Monday, February 21, 2005 3:20 AM

To: security-basics@securityfocus.com

Subject: Help me

Dear all,

I have a problem and i dont know how to explain.

Last month, my ISP give our company a report about the capacity download and upload, It was about 47GB.

The problem is my isa server has logged at about 7GB data down/upload.

When I asked them explain this great unequal capacity they said that although My isa firewall prevented almost requests from the untrust network (so this request was not included in capacity logfile and only 7GB was allowed),their server logged all requests to my router and firewall from the other local Loop . It mean, there are 40GB data of requests that not except (attack, scan ping ...) in a month.

So I make some caculation, every second, there are 16035 byte attack (I call "attack" because I was not allowed.

Everybody help me explain this situation. I know, A request does not have big capacity and my ISA server was not logged any attack!

Please help me. (sorry because of my english!)

Thanks in advance.