Subject: Nginx detects my HN IP address
Posted by silentninja on Mon, 23 Mar 2009 20:24:57 GMT
View Forum Message <> Reply to Message

This is kinda wierd..

HN => CentOS 5 x86_64 (IP ended in 11, Telecom, Argentina)
VE => Debian 5 (IP ended in 91)

My IP is totally different (x.x.x.140, Telefonica, Argentina)

1. On the VE I have installed nginx to use as a www server (really a reverse proxy www server). So I've set it up following a simple tutorial... everything is working.

2. I've then noticed that nginx detects not my IP from localhost (127.0.0.1), and not my IP from the VE (x.x.x.91) but the IP from the HN (x.x.x.11) and logs it...

x.x.x.11 - - [23/Mar/2009:20:12:52 +0000] "GET /ip.php HTTP/1.1" 200 81 "-" "Mozilla/5.0 (X11; U; Linux i686; es-AR; rv:1.9.0.7) Gecko/2009030422 Ubuntu/8.10 (intrepid) F$
x.x.x.11 - - [23/Mar/2009:20:12:53 +0000] "GET /ip.php HTTP/1.1" 200 81 "-" "Mozilla/5.0 (X11; U; Linux i686; es-AR; rv:1.9.0.7) Gecko/2009030422 Ubuntu/8.10 (intrepid) F$
x.x.x.11 - - [23/Mar/2009:20:12:54 +0000] "GET /ip.php HTTP/1.1" 200 81 "-" "Mozilla/5.0 (X11; U; Linux i686; es-AR; rv:1.9.0.7) Gecko/2009030422 Ubuntu/8.10 (intrepid) F$
x.x.x.11 - - [23/Mar/2009:20:12:55 +0000] "GET /ip.php HTTP/1.1" 200 81 "-" "Mozilla/5.0 (X11; U; Linux i686; es-AR; rv:1.9.0.7) Gecko/2009030422 Ubuntu/8.10 (intrepid) F$
x.x.x.11 - - [23/Mar/2009:20:14:37 +0000] "GET /spool/www/members_ng HTTP/1.1" 404 306 "-" "Mozilla/5.0 (X11; U; Linux i686; es-AR; rv:1.9.0.7) Gecko/2009030422 Ubuntu/8.$
x.x.x.11 - - [23/Mar/2009:20:15:44 +0000] "GET /ip.php HTTP/1.1" 200 81 "-" "Mozilla/5.0 (X11; U; Linux i686; es-AR; rv:1.9.0.7) Gecko/2009030422 Ubuntu/8.10 (intrepid) F$

Note: The logfile is cropped but the important thing is that strange IP number detection (.11) because the packets should NOT be passing from the HN, but should be get by the VE to detect the original IP number that's needed.

The httpd requests somehow detects that is being forwarded from the HN to the VE, before the nginx forwards it from the 80 port to the 81 port on localhost (127.0.0.1 is detected on the Apache server, plus the .11 address but not the .91 address).

This must be fixed, what can I do about it ?

Subject: Re: Nginx detects my HN IP address
Posted by silentninja on Wed, 25 Mar 2009 06:44:34 GMT
View Forum Message <> Reply to Message

I'm still having this issue, it won't bother me to have the VE's ip being logged instead of mine, but..

I DO care that the HN IP's is being logged by an internal VE.. it's kinda insecure plus anoying because all my stats are broken now.

This is the information from accessing directly to the Apache 2.2 with a phpinfo() script

SERVER_NAME xxx.210.xxx.91
SERVER_ADDR xxx.210.xxx.91
SERVER_PORT 81
REMOTE_ADDR xxx.210.xxx.11

As you can see, it detects that the HN is visiting Apache, and not MY ip. Apache is running on port 81, that's ok. Nginx proxying, by the way, answers quite similar:

HTTP_HOST xxx.210.xxx.91
HTTP_X_REAL_IP xxx.210.xxx.11
HTTP_X_FORWARDED_FOR 190.210.25.11
SERVER_NAME xxx.210.xxx.91
SERVER_ADDR 127.0.0.1
SERVER_PORT 81
REMOTE_ADDR xxx.210.xxx.11

None of those IP is the one that should be seen, those are localhost, hn and ve ip's.

Any information that you want I can give it to you. Maybe something is missing on my configuration of the Apache to work properly on OpenVZ, or viceversa from the HN iptables/vz to work correctly; because i've tested on another webserver with Apache 1.3 and without the nginx redirection and it worked properly:

REMOTE_ADDR 190.48.xxx.15 (My remote IP number)
REMOTE_PORT 16494
SCRIPT_FILENAME /home/xxx/phpinfo.php
SERVER_ADDR 201.235.xxx.xxx (The VE current IP number)
(HN ip address is not shown)

Subject: Re: Nginx detects my HN IP address
Posted by silentninja on Wed, 25 Mar 2009 07:06:02 GMT
View Forum Message <> Reply to Message

Now I think I know why this happened !

On my "iptables -t nat" settings, I've setup this line:

MASQUERADE all -- anywhere   anywhere

To allow some IP redirections that I've set there before.. I think it might be doing something wierd though because of it masquerades all requests from every IP address.

EDIT: YEAH ! It was because of that, but I cannot remove that line, because my IP redirections won't work properly.. I might have to edit that a little so it doesn't touch the venet0 address.