



IP Address Category

Explanation of the "IP Address" Category in Wavecrest Products

Wavecrest Computing
2006 Vernon Place
Melbourne, FL 32901
Toll-free: 877-442-9346
Voice: 321-953-5351
Fax: 321-953-5350

www.wavecrest.net

From time to time prospects or customers ask us, “What is the purpose of the ‘IP Address’ category used by Wavecrest products?” The short answer is --- it’s used to capture and segregate the IP addresses of Web sites that the product was unable to associate with ‘regular’ categories. Customers can then analyze them to identify network security threats, traffic to intranet sites, or other patterns of interest.

Here’s a bit more detail.

First note that our products identify many IP addresses and place them in content categories. The Wavecrest URL (control) list contains many such addresses.

Unfortunately though, initially unidentifiable IP addresses still appear from time to time. Generally speaking, we see three types, i.e., addresses associated with:

1. Internal (and partner) Web pages
2. Innocent links on Web sites
3. Possible malware or virus servers

When the product encounters any of these three types, it places them in a special ‘IP Address’ category. Customers can then run reports on that category the same way they do on any other category. In addition, if the customer runs a Top Non-Categorized report, the uncategorized IP addresses will be listed along with uncategorized domain names.

Because the traffic associated with unidentified IP addresses can be important or even dangerous, it’s obviously desirable to pursue the matter further. So what can be done? Well, with a bit of work—and in some cases with some help from Wavecrest—it is possible to:

- determine the source and purpose of most of the addresses
- categorize the legitimate ones
- isolate/neutralize the malicious ones

Let’s see how this is done. We’ll take it one ‘type’ at a time.

1. **Internal and Partner Web Pages.** Some unidentified IP addresses may have resulted from users going to internal (intranet) or partner sites. (These normally would not be in the Wavecrest URL list.) To address this issue, start by running a Top Non-Categorized Sites Report or IP Address Category Report. Using your local knowledge, try to determine the IP addresses of those sites and then enter the information in one or more custom categories. If you wish, give the addresses recognizable names. (Instructions on how to create custom categories can be found in our manual.)
2. **Innocent links on Web Sites.** These addresses could be associated with image or ad servers. If you want to address this issue, send a copy of a Top Non-Categorized Sites (“OtherWise”) Report to Wavecrest (sites@wavecrest.net). Our categorization team will then research and categorize the unidentified IPs for you the same way they categorize domains. If you would like to identify the IPs yourself, you can use IP address lookup tools such as the one available from <http://www.networksolutions.com>. This tool will provide you with information about the owner of the IP address (es) of interest. For example, the owner of the IP address could be a marketing company that serves ads, or it could be an image server. Once identified, if you desire, you can add the addresses to one or more custom categories. If you wish, give the addresses recognizable names.
3. **Possible Malware or Virus Servers.** Some of the unidentified IP addresses could be associated with malware, spyware or virus servers. The clue here is very high around-the-clock traffic. This is an indication that the user’s computer has been infected or attacked. The solution in these cases is to isolate the internal computer(s) and remove the malware/spyware or virus. Here’s an approach you can use to help solve this problem.
 - a. Using the Dashboard run a Trend report on the IP Address category and look for any unusual spikes. If you see anything suspicious then ...
 - b. Run a category audit on the IP Address category and look for large amounts of activity coming from a particular PC(s). Make a note of the IP address(es) and then scan for infected files.

Summary. The IP address category was created to be a ‘red flag’ for customers. Its purpose is to alert them that further action may be needed to resolve problems or to simply give them a more complete and comprehensive picture of all Web activity at their locations.