IP Addresses Category

An explanation of the IP Addresses category in Wavecrest products

From time to time prospects or customers ask us, “What is the purpose of the IP Addresses category used by Wavecrest products?” The short answer is–it is 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 these IP addresses to identify network security threats, traffic to intranet sites, or other patterns of interest.

Here is 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 Addresses 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 Noncategorized Sites 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 is obviously desirable to pursue the matter further. So what can be done? Well, with a bit of work–and in some cases with help from Wavecrest–it is possible to:

- Determine the source and purpose of most of the addresses.
- Categorize the legitimate ones.
- Isolate or neutralize the malicious ones.

Let us see how this is done. We will 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 Noncategorized Sites report or a Category Audit report on the IP Addresses category. 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 Noncategorized Sites (OtherWise) report to Wavecrest (sites@wavecrest.net). Our categorization team will then research and categorize the unidentified IP addresses for you the same way they categorize domains. If you would like to identify the IP addresses yourself, you can use an IP address lookup tool. The tool will provide you with information about the owner of the IP address 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,

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 this case is to isolate the internal computer and remove the malware/spyware or virus. Here is an approach you can use to help solve this problem.
   a. Using the Dashboard, run a Trend report on the IP Addresses category and look for any unusual spikes.
   b. If you see anything suspicious, run a Category Audit report on the IP Addresses category, and look for large amounts of activity coming from a particular computer. Make a note of the IP addresses, and then scan for infected files.

Summary. The IP Addresses category was created to be a red flag for customers. Its purpose is to alert you that further action may be needed to resolve problems, or simply give you a more complete or comprehensive picture of all Web activity at your location.

About Wavecrest Computing

Since 1996, Wavecrest Computing has provided business and government clients with reliable, accurate employee Web-access security, employee Web-use monitoring and analytics, and Cloud Access Security Broker (CASB) solutions. IT specialists, HR professionals, and business managers trust Wavecrest's Cyfin® and CyBlock® products to manage employee Internet usage with today's distributed workforce in mind–reducing liability risks, improving productivity, managing cloud services, saving bandwidth, and controlling costs.

Wavecrest has over 3,000 clients worldwide, including Blue Cross Blue Shield, MillerCoors, National Grid, Rolex, Siemens, Superior Court of California, U.S. Dept. of Veterans Affairs, and a growing list of global enterprises and government agencies. For more information on our company, products, and partners, visit www.wavecrest.net.

WAVECREST
COMPUTING

Wavecrest Computing
904 East New Haven Avenue
Melbourne, FL 32901
toll-free: 877-442-9346
voice: 321-953-5351
fax: 321-953-5350