Wavecrest®**TechBrief**

Filtering and Identifying Web Activity by User Name

When a company implements a Web filtering and monitoring solution, it typically wants to filter and monitor the Web traffic flowing through its network by user name versus IP address for various reasons. Some of these reasons include curtailing casual surfing, protecting against security threats, and conserving bandwidth. Furthermore, a company's Acceptable Use Policy (AUP) is usually based on user names and/or groups of user names. Therefore, the application that enforces and monitors the company's AUP needs to identify Web activity by user name. IP addresses can be dynamic, and sometimes more than one employee can log on to a computer, and hence, more than one user name will be using the same IP address.

Many an IT administrator is tasked with ensuring that the company's employees are going through the proxy that is in place, so that Web activity can be monitored by user name. To get user names and authenticate users, IT administrators can choose any of the proxy configuration options and authentication methods described below.

Depending on the company's preference, one proxy configuration option may be more favorable than the other. Here, we will discuss applying browser settings manually, pushing out group policies using Active Directory (AD), using a captive portal, and installing client software. We will also touch on the different ways that you can authenticate your Internet users using our CyBlock products.

Applying Browser Settings Manually

Applying browser settings involves identifying a proxy server which is required if you need user names. User names are not available when a browser connects directly to a Web site. One of two settings is used in the browser–automatic or manual proxy configuration.

Automatic Configuration. This configuration relies on the use of a PAC file that specifies a proxy server (IP address or host name) and a port of the server. It also specifies that the user may go directly to the requested Web site as though using no proxy, if the proxy server cannot be found.

Automatic Configuration (PAC File)	
Advantages	**Disadvantages**
Suitable for small companies with few users.	Time-consuming setup for larger companies.
Provides direct access for remote and roaming employees.	Direct access produces no monitoring, filtering, or reporting.
Supported by all browsers.	Web site delay when browser first starts or when proxy server is down.
Simple setup.	Users can delete or change proxy settings.

Manual Configuration. In this configuration, the IT administrator enters the IP address or host name and port of the proxy server on each user's computer. There is no "Direct" option to allow access to the Internet, if the proxy server is down or the user leaves the network.

Manual Configuration (IP Address/Host Name & Port)	
Advantages	**Disadvantages**
Suitable for small companies with few users.	Time-consuming setup for larger companies.
Supported by all browsers.	No automatic direct access available.
Simple setup.	Requires manual disabling of proxy settings for direct access.
	Users can delete or change proxy settings.

Pushing Out Group Policies Using Active Directory

From the Active Directory server, a group policy is pushed out to set up users' browsers with a proxy configuration, that is, a PAC file or proxy server IP address/host name and port. Active Directory also allows you to disable the browser's Connections tab. Two other options in Active Directory disable changing the manual proxy setting and the automatic configuration setting.

Active Directory Group Policies	
Advantages	**Disadvantages**
Suitable for companies of all sizes.	AD updates are not automatically applied to all computers. May take time to apply change to all computers assigned to the policy.
Single setup on Active Directory server.	Supported by Internet Explorer primarily.
In Internet Explorer, users cannot delete or change proxy settings. Requires AD options set to disable.	Users can delete or change proxy settings in other browsers–Firefox and Chrome.

Using a Captive Portal

A captive portal can be set up in many ways. It can operate so that when an employee attempts to visit a Web site, he will be required to log on and accept an organization's AUP, if this option was configured. By logging on, user names are captured from Web traffic that is filtered and monitored. Guests can access the company's network by accepting the AUP. A wider range of devices and operating systems in the organization can be supported. A captive portal is also used as a method of authentication which is discussed later in this document.

Captive Portal	
Advantages	**Disadvantages**
Suitable for companies of all sizes.	Depending on setup, requires cookies to be enabled in the browser.
Supports large range of devices including non-Windows devices.	
Presents customizable logon page to new devices.	
Can be used with CyBlock Appliance inline requiring no browser settings on unmanaged devices in guest networks.	

Installing CyBlock Client

CyBlock Client is a thin client that makes requests to servers and can be installed manually on computers or remotely with a tool, such as PsExec. It does not require a browser for proxy configuration. It allows IT administrators to specify several proxy servers and has the ability to continuously poll these proxies in priority order. This list of IP addresses and ports override any proxy settings in the browser. CyBlock Client also has the ability to pass user names to the proxy which is discussed below.

CyBlock Client	
Advantages	**Disadvantages**
Suitable for companies of all sizes.	Installation required on each user's computer.
Easy deployment using PsExec.	Available for Windows computers only, not Linux.
No browser configuration necessary.	
Proxy servers sorted by user-defined priorities.	
Supports on-premises as well as remote employees.	
Users cannot delete or change proxy settings.	

Using Authentication Methods

CyBlock's Authentication Manager. Authentication Manager allows you to use different types of proxy authentication to support your organization, which may include your main office, remote users, and branch offices. You can choose to use NTLM, a captive portal, or a combination of both. Disabling authentication is also an option. For various network definitions, such as a single IP address, a range of IP addresses, or a host name, you can create rules specifying the authentication method to use.

> **NTLM.** This method uses a challenge/response protocol for authentication in which the proxy makes an authentication request, and the browser responds with the user name and password. NTLM is supported in the Windows environment, but is not fully supported in other environments.
>
> **Captive Portal.** In this authentication method, logon credentials can be used to authenticate employees, and guests are identified with a guest ID. The IT administrator controls the length of time before the browser must reauthenticate. As mentioned earlier with CyBlock Appliance inline, a captive portal supports authenticating users who are filtered in transparent proxy mode, but it will also work with CyBlock Software and CyBlock Cloud. For more information on authenticating with a captive portal, see Authenticating Your Internet Users.

CyBlock Client. Using CyBlock Client, user names are passed to the proxy providing the credentials needed to identify who is accessing your network. It does not require NTLM authentication or a captive portal.

Conclusion

If you are implementing a Web filtering and monitoring solution in your organization, many proxy configurations are available to allow you to manage your Web traffic by user name as well as authenticate your users. Whether it's applying browser settings manually or through Active Directory group policies, or using a captive portal or CyBlock Client, IT administrators need to weigh the advantages and disadvantages of each option. The solution that best serves the needs and resources of the company and its IT department may be one of these options.

About Wavecrest Computing

Wavecrest has over 20 years of proven history of providing reliable, accurate Web-use management and Advanced Log File Analyzer products across various industries. Managed Service Providers, IT Specialists, HR professionals, Forensics Investigators, and business managers trust Wavecrest's Cyfin and CyBlock products to manage the human factor in business Internet usage–managing cloud services, reducing liability risks, improving productivity, saving bandwidth, and controlling costs. Wavecrest is trusted by large government and commercial organizations such as US-CERT Homeland Security, U.S. Department of Justice, USPS Office of Inspector General, National Grid, Johns Hopkins, and a growing list of global enterprises and government agencies. We are a proud long-term GSA contract holder. For more information on the company, products, and partners, visit https://www.wavecrest.net.

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