

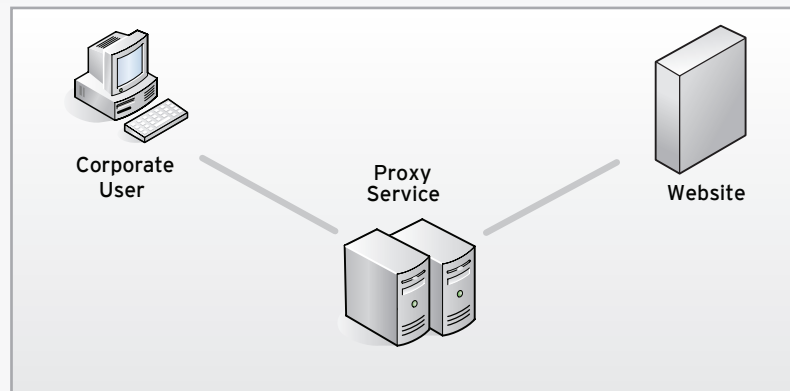


Filter Avoidance Protection

Anonymous Proxy Guard™

What is it?

A proxy in the context of filter avoidance or “anonymous proxy” is a server or website that acts as a go-between for requests from workstations/clients seeking some kind of resource (web page, file, connection etc.). A client connects to the proxy service which then requests the resource from another server. The proxy service then provides the resource by connecting to the relevant server or website and requesting the service or resource on behalf of the client keeping the requesters identity unknown. A proxy server may alter the client’s request or the server’s response, and sometimes it may serve the request without contacting the specified server.



The primary function of a proxy in regards to filter avoidance is to obscure both the requested content (web page, file etc.) and who is requesting the content. Proxy services and websites are generally free, easily available and very simple to use making them attractive to anyone who uses the Internet.

Why It Matters

Most organizations deploy Web filtering technology to help with the dangers, distractions and delays that come from operating in cyberspace. Odds are very good however that users have no trouble bypassing traditional content filters. Using anonymous proxy technologies the desired content is accessed and the process doesn’t draw attention in IT reports and logs the way unapproved web activity does so the use is frequent and often spreads from user to user as successful methods are identified.

Proxies make it very easy to defeat content filtering systems and break Internet usage policy. Proxy sites can deploy quickly and often use ip addresses instead of words in the url to make categorization by filters ineffective. Manually adding the hundreds if not thousands of individual proxy sites to a block filter list on a daily basis is time consuming and unrealistic for most IT teams. Some URL filters can help in that they can categorize IP address but because many proxy systems use encryption even the hostname requested is hidden. Though filtering by database is popular, the effectiveness is highly questionable because of the growth of SSL proxy systems. To make matters worse Web based malware routinely exploits proxy sites and networks used by employees to avoid filters in order to cause damage.

Uncontrolled access to the Internet can also cause bandwidth congestion. A single user visiting media heavy sites such as youtube.com or hulu.com can easily generate Gigabits of traffic in a very short period of time. With an increasing amount of relevant traffic dependent on available bandwidth, the

NETWORK COMPOSER FEATURES:

VISIBILITY

- Complete Traffic Visibility™
- Application Traffic (including Layer 7)
- Web 2.0 Content
- Users/Group/Device Activity
- Web, P2P, Anonymous Proxy Traffic
- Malware Threats
- Traffic Trends
- Active Reporting with Multi-Correlation of Data
- Bandwidth Usage Reports

SECURITY

- Complete Traffic Protection™
- Anonymous Proxy Guard™
- Zero-day Threat Protection
- Triple Layer URL / Web 2.0 Filtering
- Malicious Web Site Blocking
- Web 2.0 Infected Site Detection
- Spyware Removal

CONTROL

- Complete Traffic Management™
- Internet Traffic Acceleration/Optimization
- Dynamic Application/Bandwidth Shaping and Allocation
- Web Content Prioritization
- Web Category/URL Shaping
- Web 2.0 management

“Money well spent! We look at the reports several times a day and forward any concerns to the principal for discipline.”

--Technology Director
Bandera Independent
School District



inability to correctly manage and control recreational surfing can hurt an organization in many ways. With all the investment they've made in deploying and updating Web filters, they're essentially back where they've started once employees have learned to bypass them.

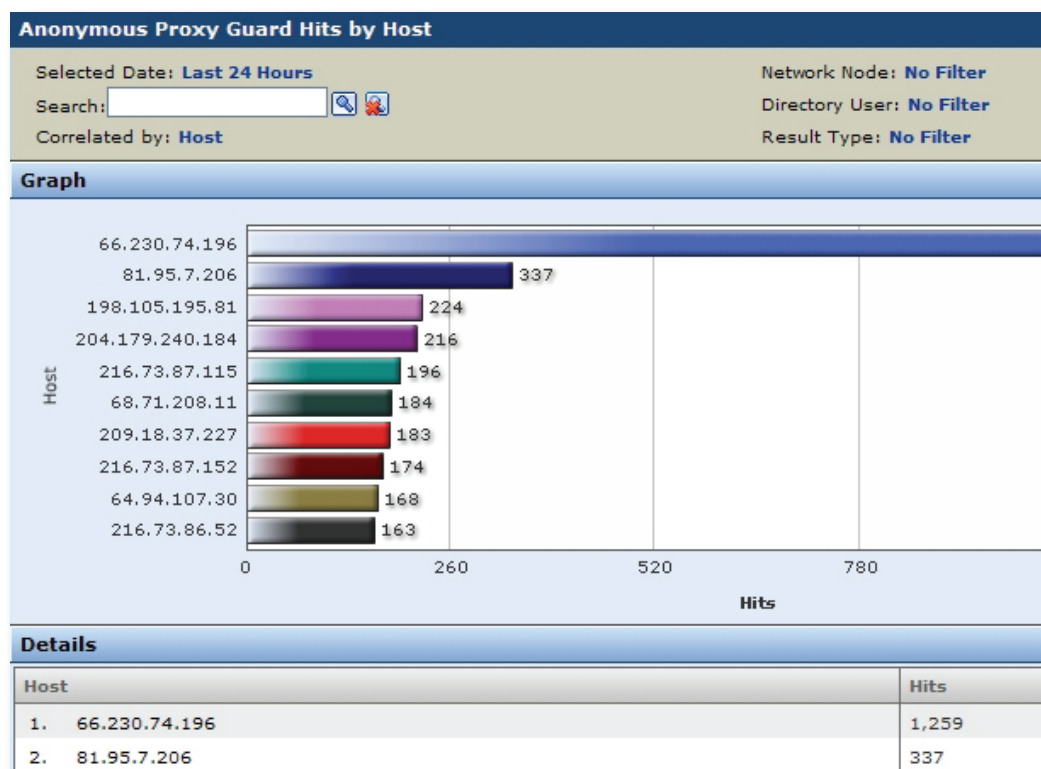
How Cymphonix Solves the Problem

The key to the Cymphonix success in identifying and controlling the different types of proxies is how Cymphonix identifies all the traffic in moving into and out of the network. Cymphonix is an inline device and is able to look across multiple ports and protocols. The first type of proxy known as a web proxy is fundamentally a website. Cymphonix accurately identifies websites using 3 methods, a database, url keywords and real time content analysis. For the second type of proxy services also know as hardware proxies Cymphonix uses Anonymous Proxy Guard™. From its inline position, Network Composer actively scans across all ports and protocols and uses application recognition signatures to detect suspicious HTTP traffic.

Using Cymphonix Anonymous Proxy Guard technology enables organizations to stop or manage employee use of rogue applications or anonymous Web surfing encrypted in an SSL session. It can also stop encrypted malware, including viruses and spyware, from infiltrating enterprise networks through encrypted tunnels. The SSL proxy can deny threats from secured phishing attempts that now utilize SSL explicitly as a cloaking mechanism. Cymphonix Network Composer can also receive updates on an hourly basis ensuring that the best possible technology to fight the use of proxy systems is always in place.

To find out more about Cymphonix Network Composer and how it can help you control anonymous proxies call us at 866-511-1155 or visit us online at www.cymphonix.com.

Report Example



Reinvent Your Relationship with the Internet.

Network Composer is ready to offer your organization new levels of Internet safety, performance, and control, so you can maximize the value and productivity of your Internet connection. Visit www.cymphonix.com to learn more and schedule a live demo.

Call us at: 866.511.1155

Visit our website at: www.cymphonix.com

