Controlling Anonymous Proxies:

Why proxy-based and mirror-port filtering approaches fall short

A Cymphonix White Paper

CYMPHONIX

Controlling Anonymous Proxies:

Why proxy-based and mirror-port filtering approaches fall short

Filter avoidance technologies now utilize the latest security techniques to bypass content filters. Traditional proxy-based and mirror-port filtering approaches have become technologically unable to address the issue.

Proxy-based Filters Lack Visibility into Secure Anonymous Proxy Traffic

Because they do not sit in-line, by nature, proxy-based filters have no visibility into HTTPS and other secure web traffic. In fact, they are limited to accessing standard HTTP requests - leaving secure and non-browser traffic undetected

Issues:

- Secure traffic is encrypted, unreadable and is only certificate-verified by the proxy-based filter and therefore left uncontrolled
- Advanced, secure non-browser traffic using proprietary protocols (e.g., Torpark) is also unseen and uncontrolled by the filter
- Many anonymous proxies are dynamic - sometimes only up for a couple of hours and are therefore indetectable to database spiders

Proxy-based Filters Utilize Ineffective Attempts by Proxy Filters to Control Rogue Traffic

SSL Certificate Inspection: Recent marketing attempts tout certificate inspection as the solution for technologically-limited proxy filters to control secure anonymous proxy traffic. While this may sound compelling, several issues reveal its ineffectiveness

Issues:

- Certificates can be easily spoofed - making blocked content appear as content coming from approved sources
- Certificate issuing authorities do not limit certificates to appropriate sites…any site, serving appropriate content or not can purchase and utilize a certificate. Proxy filters may verify the certificate is valid, but cannot view the page content because it is encrypted - letting inappropriate content pass through - just because the certificate was valid.
- Certificates are easily attainable
- Certificates can be easily bypassed or ignored

URL Inspection: Like certificate-only inspection is limited in controlling anonymous proxy traffic.

Issues:

- Proxy site volume - no database update can keep up with the overwhelming number of proxy sites created every day. Additionally, users can create their own proxy server - something impossible for database updates to find and include
- Non-browser Traffic - proxies using prioprietary protocols or separate applications to serve up content pass traffic in ways traditional proxy filters don't even have access to

Effective Anonymous Proxy Control: a Four-Pronged Approach

In-line Packet Inspection:
Network ComposerTM by Cymphonix is an in-line device that delivers deep-packet scanning for complete traffic identification and control. Because of this unique feature among content filters, the device is able to identify and control traffic regardless of port or protocol - addressing the full spectrum of traffic, rather than just the HTTP requests traditional filters can address.

Certificate Inspection and Control:
As a first level of security, SSL certificate inspection can eliminate some anonymous proxy sites with low overhead performance costs. Network Composer includes SSL certificate inspection as a first line of defence against anonymous proxy sites. But, unlike other filters that only rely on certificate inspection, Network Composer delivers additional layers of protection - ensuring customers have the most robust anonymous proxy controls available.

Active Filter Avoidance Scanning Technology:
Cymphonix actively scans for and identifies anonymous proxy sites and pushes updates to connected devices daily whether the device's users attempt to access the sites or not. This active approach has created the industry's most aggressively updated and complete anonymous proxy database. For administrators, this elminates the need to update anonymous proxy blacklists manually and delivers a more comprehensive list than could be created manually - ensuring filter-bypass activity is blocked.

Full Decryption, Dynamic Scanning and Re-encryption:
Network Composer is the only mid-market solution capable of fully decrypting, scanning and controlling, then re-encrypting HTTPS traffic. Unlike proxy based or mirror port based filters, Network Composer is installed transparently in-line - allowing it to terminate SSL sessions and decrypt the traffic. Once decrypted, the device performs complete dynamic, database and hueristic scans to identify content that should be blocked. The device can then re-encrypt and pass legitimate traffic to the client or deliver a "content blocked" page to the client for inappropriate traffic.

To Learn More

This unique four-pronged approach delivers the only mid-market solution for effectively controlling secure anonymous proxies. Contact Cymphonix today to see how easy controlling anonymous proxies can be.

Contact your Authorized Cymphonix Reseller for an online demonstration or call or email Cymphonix at
866-511-1155 or
sales@cymphonix.com

CYMPHONIX