Anonymizing Proxies
What They Are and How they Work

Online fraud is a growing problem for retailers and other businesses. In 2011 alone, fraudsters stole over $3.4 billion. One way to make a dent in fraud: examine IP addresses and determine users' geolocation. This method, however, works only when it also identifies anonymizing proxies.

What They Are and How They Work
An anonymous Internet proxy server, a.k.a. “anonymizer” is a server on the Internet that acts as a conduit of communication between a user's computer and various Internet resources such as websites, e-commerce applications, newsgroups, chat rooms, and others. Proxies give users the ability to mask their public IP addresses in order to prevent their online identity from being detected.

When a user browses online using an anonymous proxy, the anonymizer appears in place of the user. Websites and e-commerce applications may not know that inbound traffic and requests are coming through a proxy server. All requests for data and all responses are exchanged with the anonymizer, which in turn exchanges this information privately with the actual user.

Some individuals use proxies in order to protect their identities, while others use proxies for the purposes of conducting fraudulent activities or to circumvent restrictions. In either case, anonymizers increase the risk of approving malicious users or blocking legitimate customers.

Legitimate Uses of Anonymous Proxies
Some anonymous proxy servers offer legitimate privacy services that help users protect themselves from pop-up ads, cookies, Internet censorship, or oppressive governments. Many websites employ techniques to read a visitor's browser information or to place cookies on the visitor's computer in order to track that person's browsing activities or serve them unwanted advertising.

Redirecting browser traffic through an anonymous proxy server prevents a website from effectively using this identification, tracking and targeting techniques and helps preserve user privacy. In some instances oppressive governments have put technology in place to prevent Internet users from accessing certain websites or to track individuals on the Internet. The use of anonymous proxy can circumvent these restrictions and protect a user's identity.
Illegitimate Uses of Anonymous Proxies

Criminal anonymizers have been set up covertly for the specific purpose of enabling and hiding malicious online activity. They are often difficult to find because they are advertised only within hacker and online criminal communities. Some fraudsters use anonymizers when conducting illegal activity on the Internet. When they visit a website in this way, it is as though they are walking through the front door of a brick-and-mortar operation wearing a ski mask. Alternatively, some people use anonymizing proxies to circumvent restrictions that limit online access to content or data to certain geographies. People who live outside of these locations may use a proxy in order to gain access to content that is denied by contract or by law.

Proxy Identification

Since 2005, Neustar IP Intelligence has developed a proprietary methodology for the identification and aging of Internet proxies. It is widely used in conjunction with other Neustar IP Intelligence geographic and technographic data to build varying business logic that are the cornerstone of many fraud, banking, and digital rights management platforms.

Neustar’s proxy detection and aging process is summarized in the following chart:

1. Obtain information about a suspected proxy
2. Suspected proxy is tested to validate if it is active
3. If test is negative then retest at a later time
4. If test is positive then proxy is added to the GeoPoint
5. Proxy is tested regularly to validate continued activity
6. Proxy remains in GeoPoint while active
7. Proxy is removed from GeoPoint after a period of inactivity

Proxy Intelligence

The ability to characterize the proxied connection of user’s reaching your site allows you to refine decision logic to meet the needs of your business. The following fields are available in GeoPoint for your IP based intelligent solutions.

Anonymizer Status

A status is assigned to IP addresses that have been detected as a proxy. The status is an indicator, at the highest level that an IP address may be associated with an anonymizing proxy. It is a relative indicator of how recent the proxy was found to be active and the proxy’s category.

Proxy Last Detected

Provides the most recent date on which Neustar IP Intelligence proxy detection technology confirmed the proxy was active or served as a private proxy. It provides a more granular indication that an IP address may be associated with an anonymizing proxy. Using the “last detected” date, allows you to decide how serious a threat the use of a proxy presents to your business.

Proxy Type

The type of network or protocol utilized by the server to proxy the user connection is identified. Proxy type classifications include the use of http, Tor, web and SOCKS.

Proxy Level

The level describes the degree of concealment provided by the use of the proxy. While all proxies act as an intermediary between the user and requested website, proxies provide differing levels of obfuscation to the user’s originating IP address. Levels of obfuscation include: transparent, anonymous, distorting and elite.

LEARN MORE

For more information Call +1.877.572.4581
Visit www.neustar.biz/enterprise/ip-intelligence
Email sales-IPIntel@neustar.biz