Anonymizer Enterprise Network
Privacy/Security Appliance

Technology Overview

Introduction

Anonymizer's **Enterprise Network Privacy Solution** protects everyone on a network by preventing others from tracking your usage and identifying who you are while accessing the Internet.

Every Web site on the Internet has the ability to track and identify all visitors that come to their site. This capability is almost universally exploited by major Web sites. Free and inexpensive tools exist to automate analysis of logs and other connection data, while other tools even allow Web sites to display different or misleading information based on who is connecting to them.

This **Enterprise Network Privacy Solution** uses our proprietary **Network Chameleon Technology**™ to hide or "mix" your Web activity with millions of other active users Internet traffic. Not only does this make it impossible for others to identify you, it also makes it extremely difficult to identify the traffic as coming from Anonymizer.

Vulnerabilities from this kind of tracking range from gathering false data, being denied access to certain Web pages, automated counter-hacking, exposure of confidential research or investigations, to the compromise of entire covert operations.

As the world leader in Internet privacy solutions, Anonymizer has protected billions of network connections since it was founded in 1995.

Anonymizer's core **Network Chameleon Technology**™ technology uses proxy servers armed with proprietary encryption technology to rewrite requested Web pages for it's end-users, filtering potential threats like cookies, Web bugs and mobile code while shielding the user from identification and on-line tracking. When surfing the Internet using the Anonymizer service, users are protected from Web site logging, tracking by on-line advertisers, hacker attacks and exploits, Web-borne viruses, network monitoring by ISPs or employers, and other threats.

Because Anonymizer's core technology is server-side and platform-independent, end users don't have to download client software or adjust their system configurations.

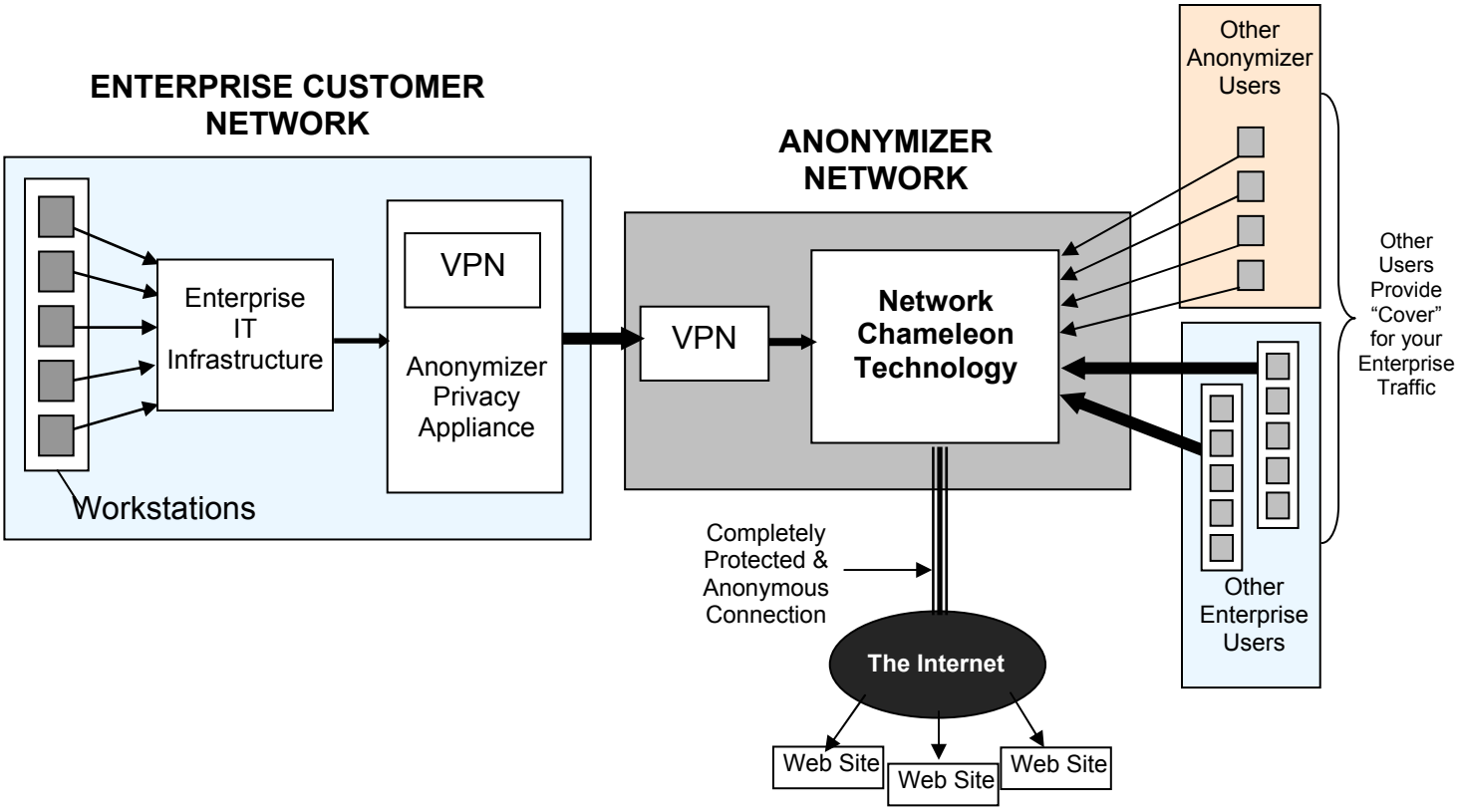
Technology overview

Anonymizer uses award winning **Network Chameleon Technology™** technology to "mix" the Internet Protocol (IP) address of more than one million users through our network mixing process. This process effectively masks or hides each and every users IP address in a substantial collection of electronic noise.

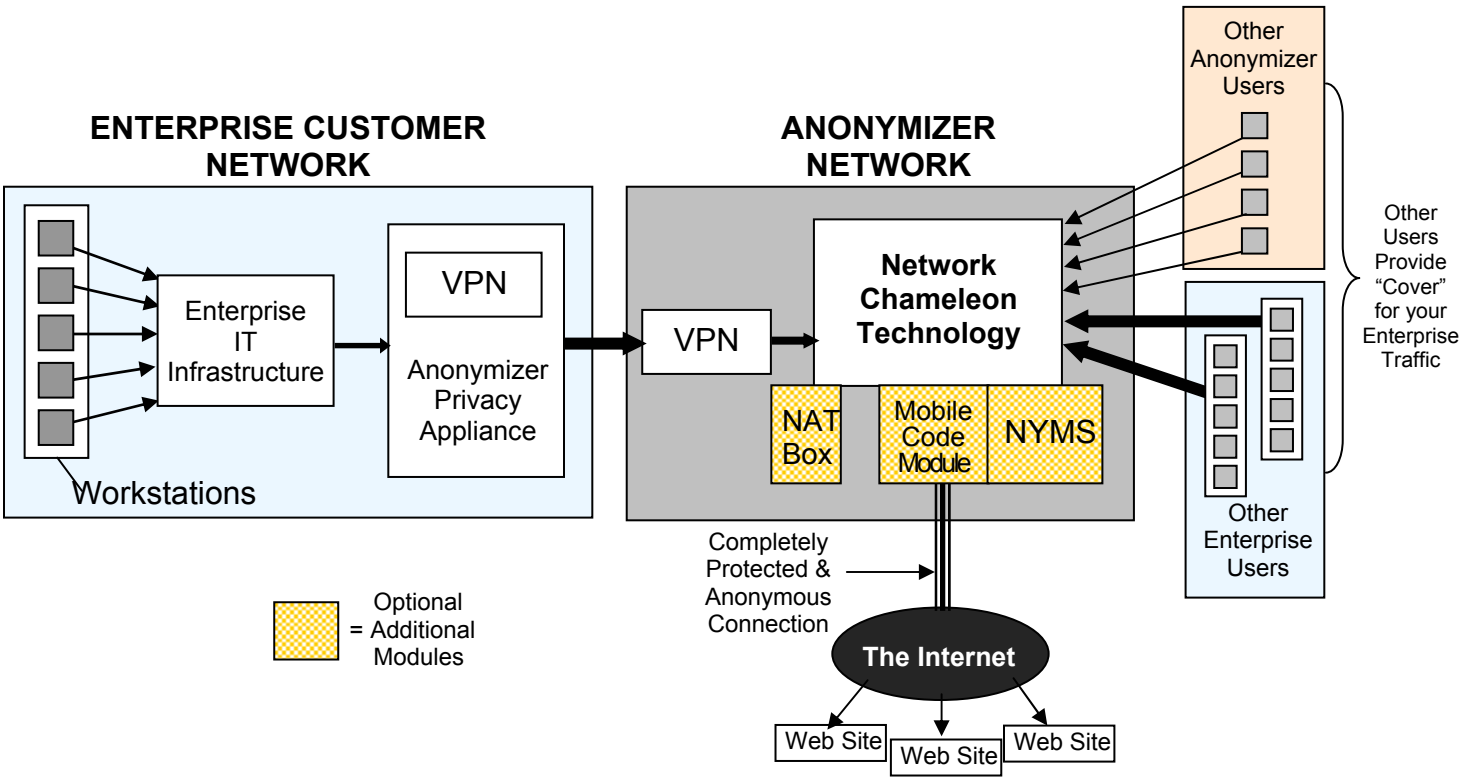
Anonymizer combines state-of-the-art hardware in the form of our **Network Address Translation (NAT)** box that routes traffic through our proxy servers and then back out to the worldwide Web. This technology, combined with liberal bandwidth, results in super fast performance with a network lag time that is recorded in the millisecond range, making any decrease insignificant.

The connection between your network and Anonymizer's facility is completely protected by high security VPN encryption.

Due to the high volume of cover traffic available to Anonymizer, any Web site you visit is likely to be visited by other Anonymizer users on a regular basis ensuring that your traffic does not stand out as significant in any way.



Optional Modules for Added Protection



NAT Box
This module helps dynamically control what IP address is presented to the outside world. With this module you have complete control to change the IP address anytime you need without having to contact Anonymizer, and can be configured for manual intervention or session enabled for each user or for each day.

Mobile Code Module
This module helps protect you against sites that are running hostile programs like Active X, Java, Java Script, VB Script, and a host of other threats. You have the flexibility to configure this on a site-by-site basis.

NYMS
The newest weapon in Anonymizers privacy arsenal, Nyms , are disposable email addresses that help prevent the propagation of Spam and help keep your real email address safe, secure, and private except to those that you choose to have it. A Nym is a disposable email address you give away with confidence because it can be quickly and easily disabled without effect on any other email address you may use. You can give a different Nym to every person, Web site, list, or organization you interact with. By eliminating any Nym you create, you have the ability to stop Spam in it's tracks. Nyms can be setup automatically in real time, uniquely for each Web site, whenever the Web site requests your email address.

ANONYMIZER®

Risks

- Tracing of an IP address back to the originating computer while performing on-line research
- Hacker attacks against networks / automated counter probes launched by Web sites
- Possible exposure and or advance warning to targets that confidential investigations or research being conducted
- Possible exposure of operations / operatives
- Receipt of planted or misleading information based on the source of queries
- Access to “specific” research prevented by outside sources blocking your IP address
- Your competition alerted to any research and development currently in progress
- Not being able to audit Web sites visited by employees **(optional robust security audit package)**
- Early warning to competitors of possible merger and/or acquisition being planned
- Early warning of investor information or specific stock targeting by the financial sector
- Spyware downloaded to corporate work stations **(optional Spy Ware Killer Application)**
- Possible Web site spoofing by hackers trying to obtain sensitive information
- Open to Spam **(optional NYMS module)**
- Possible exposure of sensitive client information

Risk Containment

Anonymizer Enterprise Network

Privacy/Security Appliance

- Complete privacy protection for an entire network, or sub-network.
- Protects against IP-based tracking
- Allows on-line investigations and data harvesting without giving away your identity or interests
- Centrally administered
- No client software required
- Platform independent
- Compatible with all automatic data harvesting, web scraping applications and analytics systems

ANONYMIZER®

Features

- All traffic mixed with the traffic from approximately 1 million other users of Anonymizer's privacy services
- Dedicated secure VPN connection to Anonymizer facility using Triple-DES or AES encryption
- Configurable log levels from zero logging, to very detailed logs of all activities
- Auditable security
- Automated "Network Chameleon" IP address hiding and changing technology to prevent association of traffic with Anonymizer
- Fully redundant VPN, traffic mixing systems, routers, load balancers, and backbone connections
- Secure facility:
  - 24/7 monitoring
  - Biometric access control to facility
  - Equipment in locked cabinets within the facility
- Support:
  - Basic business hours phone and email support included
  - 24/7 and “spare in the air” support programs available
- High security network firewalls
- Individual firewalls on all machines
- Intrusion detection systems
- Modified high security kernel configuration on servers
- All traffic proxied through high security servers, no direct network connections even through VPN
- All required hardware at customer facility provided pre-configured by Anonymizer
- On-site setup support
- 1 Year (extendable) hardware warrantee on hardware provided to customer
- Scaleable to billions of Web queries per month
- Proven security trusted by government and law enforcement agencies since 1997

Enterprise Add-ons
Added Value Software for your Enterprise Solution

- Spyware Killer – Protects against malicious spying and tracking
- Total System Sweeper- Wipes away potentially malicious files and tracking devices left on your Windows operating system
- Anti-Spam – Prevent unwanted email clutter
- VPN option – Secure connection between site-to-site
- Extra Redundancy – Additional safety feature in the event of system failure to ensure zero network downtime
- Support for protocols other than HTTP (FTP, IRC, ICQ, AIM, P2P, etc.)
- Geographic Distribution –Your traffic appear to come from different parts of the world, under your control

ANONYMIZER®

Solutions for Enterprise and Government

- **Competitive Intelligence Toolkit™**
  Allows corporations, law firms and government agencies to safely and privately perform research and harvest Web data. It combines Anonymizer's privacy technology with essential Web research tools such as Ping, DNS Lookup, Trace route, and spidering engines in a user-friendly interface to facilitate safe, anonymous on-line research by non-IT personnel.
- **Envoy Secure Intranet Access™**
  Enables employees, partners and clients to securely log on to company networks from any computer, anywhere, without requiring client software. Envoy rewrites Intranet content on special proxy servers, enabling employees, clients and partners to access vital information while preventing direct contact with data and eliminating the risk of intrusion and data tampering.
- **Ecommerce Fraud Prevention**
  Proprietary credit card fraud screening tools designed specifically for ecommerce merchants distributing digital goods on-line. By identifying high-risk Web behavior and traffic patterns, these Fraud Prevention systems provide more relevant scoring criteria and effectively reduce both fraud rates and “false positives”.
- **Anti-Censorship Systems**
  Provides the U.S. Government with anti-censorship technologies designed to enable unfettered, anonymous access to news and information for citizens living under oppressive regimes. Chameleon Proxies™ provides access censored Web sites while actively responding to and countering government attempts at blocking. Active outbound communications keep users informed of the changing addresses of the servers.
- **Enterprise Network Privacy Solution**
  Anonymizer provides organization-wide protection solutions via its VPN/Traffic Mixing systems. Anonymizer routes all traffic from the corporate LAN to the Internet through the Privacy Proxy network, effectively hiding the source of the traffic, and blending it with the traffic from over half a million other active users. Our Chameleon Proxies™ even prevents the destination site from knowing that a customer of Anonymizer is visiting it. The process is completely transparent, allows 100% functionality for all Web sites, and requires no software on the end user's computer. Only a single server needs to be installed at the client facility.

ANONYMIZER®

Management Team

Bill Unrue (CEO, Board Member) – Bill was recruited by Anonymizer in 2000 and has lead the Company to profitability and rapid growth in sales. Previously, he was brought in as president of Newpoint, Inc. which he turned around and made profitable in only nine months. As the director of Sunbeam's Healthcare Division, Bill grew annual sales from $60M to $170M. As an executive at Thermos, he led his group from a $12M loss to a $3M profit in only one year. Bill earned a BA in Economics from the University of Washington and holds an MBA from Northwestern.

Lance Cottrell (President, Founder, Chairman) – Lance is an internationally recognized expert in cryptography and on-line privacy and security issues. Since founding Anonymizer in 1995, he has gained wide media exposure for the Company and is regularly quoted by The Wall Street Journal and other national sources. He frequently addresses major conferences such as Comdex. Lance holds a BS degree from UCSD along with a Masters degree in Astrophysics.

James Reynolds (Director, Engineering) – James has 11 years of Web development management experience, primarily delivering financial service applications including credit-card fraud detection and numerous banking solutions. He has held engineering management positions at Digital Insight, HNC Software, Bexcom Research and Deutsche Bank. James holds a BA degree in Computer Information Systems from Weber State.

Patrick Moneymaker (Advisor)
President and COO, Ocean Systems Engineering Corporation. Retired Rear Admiral, US Navy. Former Commander, Blue Angels; former Navy Director of Space and Information Warfare.

For further information, please contact:

Bruce Krocza
888.270.0141 ext. 324
Bkrocza@anonymizer.com

Monday to Friday
7:00AM to 6:00PM PST