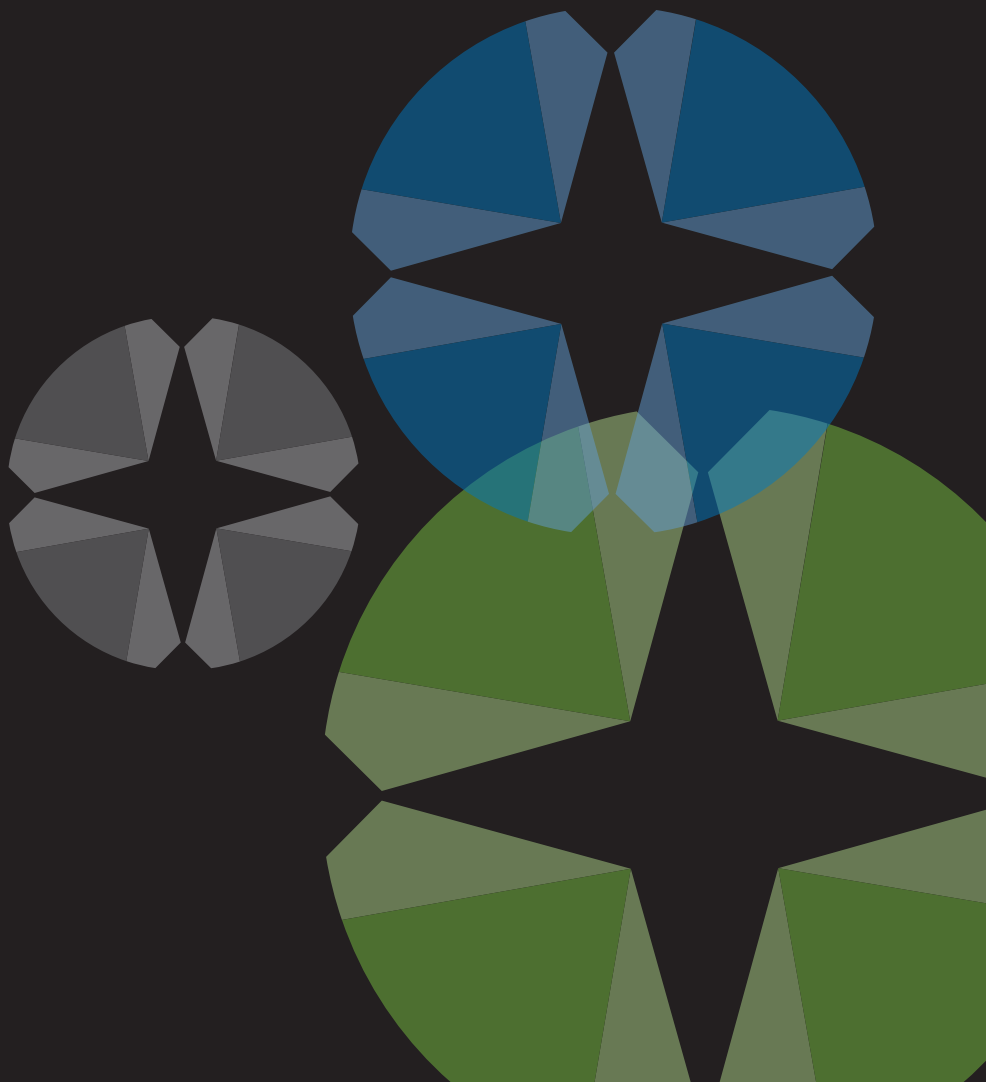
exinda

Anonymous Proxy Detection and Control

Enhance Network Security by Exposing Anonymous Proxy Traffic



Anonymous Proxy Detection and Control

Executive Summary

"On average, 37% of network capacity has been occupied by traffic that is not business-critical."

Aberdeen Group, "Application Performance Management: Getting IT on the C-Level Agenda", March 2009

Network managers and administrators face a steep uphill battle in effectively monitoring and managing network resources and controlling unwanted traffic. To keep their network safe, organizations have invested time and resources in developing appropriate network usage policies and implementing firewalls, URL filters and intrusion detection solutions. But just as organizations plug one network security gap, another opens up.

Anonymous proxy servers and applications pose one of the most pervasive threats to network security and performance. Anonymous proxies allow users to easily bypass an organization's network usage policies and to do so while going completely undetected by firewalls and filters. New anonymous proxies become available every day which makes it extremely difficult for an organization to block their access.

Anonymous proxies create the opportunity for users to access improper, banned or illegal sites, content and applications that may expose an organization to legal or regulatory consequences. Anonymous proxies also jeopardize the security and privacy of users and data by creating a security gap through which malicious traffic including malware and Trojans can gain access to the network.

Anonymous proxy traffic may also degrade network performance and slow the response times for critical applications. When unwanted applications are allowed to circumvent usage policies and consume bandwidth intended for legitimate business applications, productivity suffers and the entire organization may be put at risk.

This white paper will discuss the challenges of identifying and controlling anonymous proxy traffic on the network and how organizations can overcome these challenges by implementing the low-touch Exinda WAN optimization appliance.

Legitimate Uses of Proxy Servers

A proxy server is a server or application that acts as an intermediary for requests from clients seeking resources from other servers. A client connects to the proxy server, requesting a service such as a file, connection, web page or other resource that is available on a different server. The proxy server provides the service by connecting to the relevant server and requesting the service on behalf of the client.

Proxy servers have many legitimate uses. Most proxy programs provide the means to deny access to URLs specified in a predetermined blacklist, allowing organizations to filter content. As a result, proxy servers are routinely used in corporate, educational or library settings where it necessary or desirable to filter content.

Proxy servers may be used for many other legitimate purposes including:

- To cache web pages from a web server
- To speed up access to network resources
- To apply access policies to network services or content, e.g. to block unwanted sites
- To log and audit network usage, e.g. employee Internet usage reporting
- To scan transmitted content for malware or Trojans before delivery
- To scan outbound content for data leak protection
- To make internal systems anonymous to external parties on the Internet for security purposes

Unfortunately, the same proxy server technology that allows organizations to secure their networks and make them run more responsively can also be used to bypass network security policies and usage restrictions.

Anonymous Proxy Servers

Did You Know…
There are over 50,000 anonymous proxy sites in existence and many more are created every day.

An anonymous proxy server is intended to conceal a user's identity. One of the more common approaches is the open proxy. An open proxy is a proxy server that can be accessed by any Internet user. Anonymous open proxies allow any user of the Internet to conceal his or her IP address, identity and location from the service being accessed. The server receives requests from the "anonymizing" proxy server, and thus does not receive information about the "true" end user's IP address.

Many anonymous proxy servers are funded through advertising. For example, a site might allow users to evade organizational restrictions by providing encrypted HTTPS access to blocked Web sites such as MySpace, newsgroups, email or instant messaging. In exchange for providing this service, an ad is displayed to the user and cannot be removed unless the user pays to subscribe to the service.

Open proxies are very difficult to track which makes them especially useful to anyone seeking online anonymity – from political dissidents to grade school and university students to computer criminals.

While many users of anonymous proxies are motivated by a desire to protect their personal privacy online and mean no harm to an organization's network, others may have more sinister motives for wanting to hide their identities. Hackers often make anonymous proxies available to users in order to bypass firewalls and create a backdoor into the user's network. Once a backdoor has been created, hackers can exploit this security gap to collect personal information such as credit card numbers, passwords or sensitive organizational data.

In this scenario, the proxy acts like a Trojan horse, which appears to perform a desired function for the user but at the same time facilitates unauthorized access to the unwitting user's network and computer system. Once a proxy application or script is installed on the user's internal system, it can work in the background silently and undetected.

Given the very real threat of cybercrime and the loss of sensitive data, it is in the best interests of organizations to find a simple and effective means to detect and control anonymous proxy server traffic.

Anonymous Proxy Applications

There is also a wide array of anonymous proxy applications available online that are designed specifically to bypass an organization's firewall or filtering rules. The following anonymous proxy applications are just a few of the thousands of different applications and services that are available to users over the Internet:

Your Freedom

Your Freedom is a client application that turns any PC into an anonymous Web and SOCKS proxy that nearly any application can use. The Your Freedom website boasts that over 30,000 people in 160 countries use its client application every day. Your Freedom creates a huge security gap for organizations because it not only allows a user or employee to bypass security measures, but it also provides an open door into the network for others to exploit.

Vtunnel

Vtunnel is a tunneling proxy service. By browsing the Web through the Vtunnel service, many blocked websites can be accessed by users. Vtunnel provides the service completely free of charge due to advertiser support.

StealthNet

StealthNet is an application that allows anonymous file sharing. This can open up a backdoor into the network or allow an organization's intellectual property to be easily moved outside their network – credit card information, employee social security numbers, student information, industry trade secrets and other types of sensitive or confidential information.

VoipTunnel

VoipTunnel is a technology developed by VoipSwitch that enables users to make and receive VoIP calls from behind firewalls that block VoIP traffic. This can also expose an organization's users, network and machines to outside threats.

There are literally thousands of anonymous proxy applications available to savvy users with new applications appearing each day. The sheer number makes it difficult for network administrators – already under pressure to conserve bandwidth for critical applications – to keep up.

Perhaps even more alarming is the growing sophistication of anonymous proxy servers and applications which employ an arsenal of different evasive techniques. For example, proxy servers will constantly change their IP addresses – an anonymous proxy site may come online one hour and be gone the next.

Anonymous proxy servers and so-called “anonymizers” may use tunneling, encryption, encapsulation or other means to avoid detection and allow a user to access restricted sites or applications.

HTTP Tunneling

Tunneling through HTTP allows proxies to circumvent firewalls by hiding within legitimate-looking HTTP traffic. This is accomplished by using a protocol that a firewall would normally block such as FTP, but wrapping it inside the HTTP protocol which the firewall does not block.

HTTPS Tunneling

Tunneling HTTPS proxy servers leverage the Secure Sockets Layer (SSL) cryptographic protocol to create a secure, encrypted tunnel into the Internet. The proxy server sets up the SSL connection between itself and the web site the user is visiting and then back to the user’s computer. Because the traffic passing through the tunnel is SSL encrypted, traditional filtering solutions and access controls are unable to look inside packets to identify unwanted traffic. With some encrypted proxies, users can choose to use SSL for all connections they make or only for connections to those sites they wish to remain hidden from prying eyes. Tunneling HTTPS proxy servers enable users to easily defeat content blocking policies implemented by organizations.

Why Should Organizations Care?

Anonymous proxies place a constant burden on network administrators and IT staff, but they are not merely an IT problem. They may have serious and wide-ranging implications for an organization including:

- Compliance breaches that exposes an organization to regulatory or legal consequences
- Security holes that expose the network to malware, Trojans and other threats
- Loss, theft or exposure of sensitive or confidential information
- Increased costs through unwanted and unrestrained bandwidth usage
- Network performance issues that lead to unacceptable application response times and diminished employee productivity
- IT resources, time and effort diverted from more important strategic initiatives
- Potential damage to an organization’s reputation that can be difficult to repair

Given the risks, organizations simply cannot afford to allow users to bypass the security measures and policies they have put in place to restrict access to unwanted Web sites and applications.

To address the threat of anonymous proxies, organizations must be able to:

1. Detect anonymous proxy traffic on the network
2. Leverage application signatures to categorize network traffic
3. Implement network usage policies to shape traffic

In the next section, we'll look at how the Exinda WAN optimization appliance allows organizations to effectively detect and control anonymous proxies.

Anonymous Proxy Detection Made Easy

Exinda provides a full line of appliances that enable WAN optimization, traffic shaping and bandwidth management. The Exinda appliance provides network administrators with an easy-to-use, low-touch solution for exposing and controlling anonymous proxies.

Gain Visibility into internal Hosts Sending and Receiving Anonymous Proxy Traffic

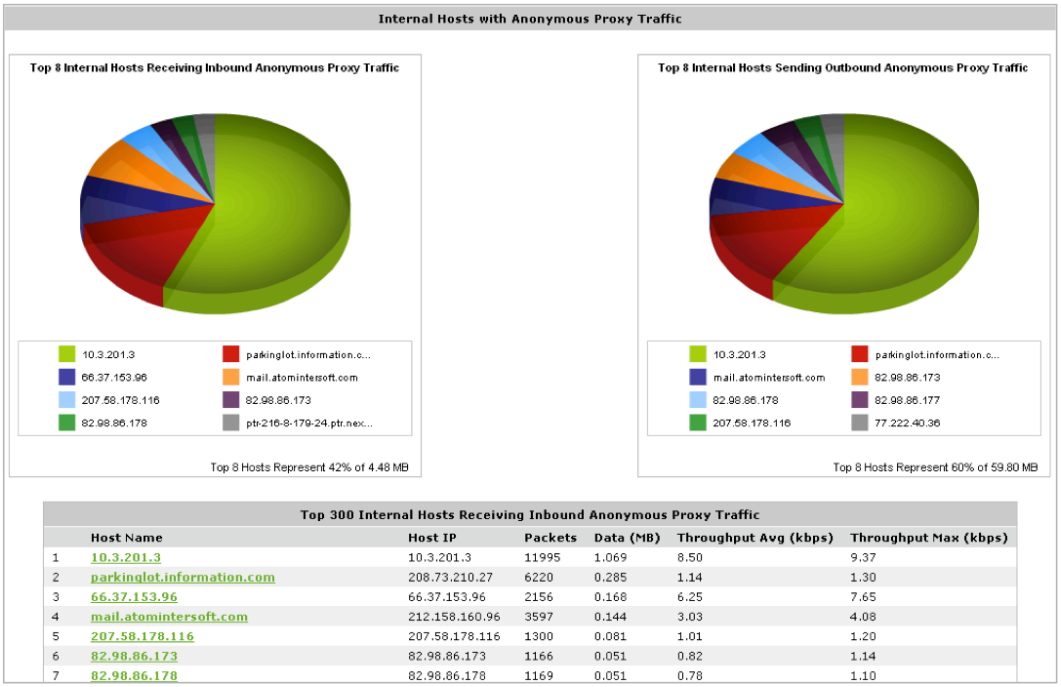


Figure 1 – The Exinda appliance allows network administrators to gain real-time visibility into anonymous proxy traffic in order to keep track of what users are doing. Graphical reports can be automatically emailed in PDF format to IT personnel, managers or human resources.

Real-time monitoring and reporting enables organizations to easily identify end users who are not complying with appropriate network usage policies.

Once the Exinda application classification engine has identified network traffic that is using anonymous proxies, it can then automatically respond by applying predetermined Quality of Service (QoS) policies to manage the anonymous proxy traffic – by limiting its bandwidth usage, for example, or blocking the traffic altogether.

Create Policies to Control Anonymous Proxy Traffic

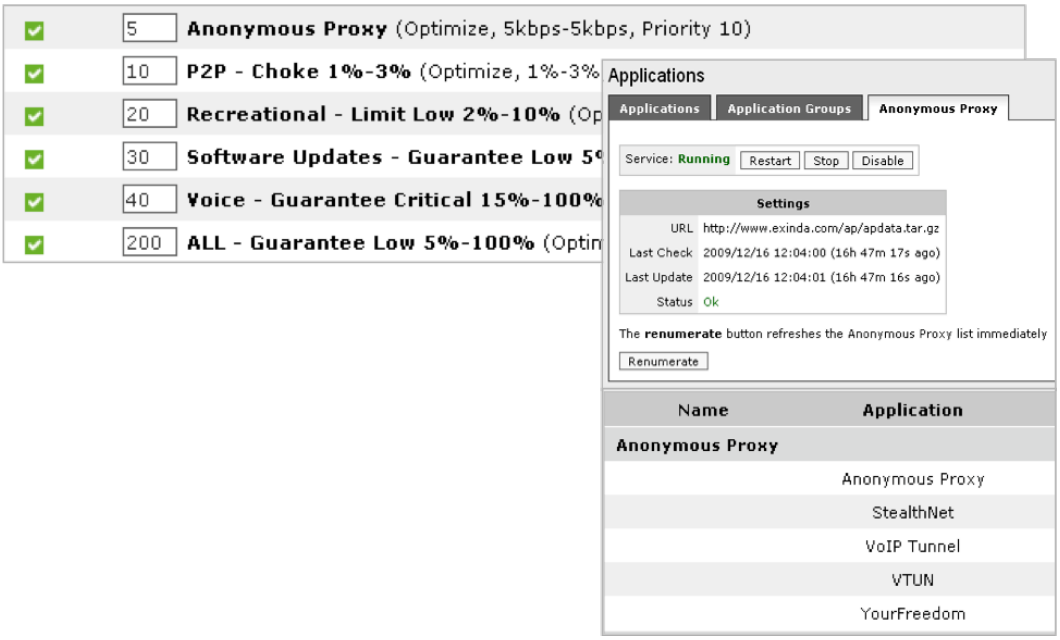


Figure 2 – The Exinda appliance enables network administrators to quickly and easily set policies to limit anonymous proxy traffic or block it altogether.

To stay on top of new anonymous proxy sites, the Exinda appliance's software maintains a up-to-date "living list" of URLs and sites to which access should be limited or blocked. Automated daily scheduled updates of new anonymous proxy information and application signatures ensure continuous detection of anonymous proxy sites. Exinda detects anonymous proxy traffic by URL, IP, domain, HTTPs and SSL application signatures, ensuring that encrypted proxy traffic is also exposed.

Combining an advanced anonymous proxy detection engine with policy-based traffic management and control, Exinda provides organizations with a simple and effective solution to prevent anonymous proxy traffic from interfering with application performance or compromising the security of the network.

Summing Up

Today's networks are under siege. Legitimate business applications now compete with Facebook, MySpace, YouTube and P2P applications like BitTorrent, Limewire and Kazaa for a limited amount of available bandwidth. Unwanted recreational traffic places a strain on networks that are already under pressure to deliver business applications.

When users deliberately circumvent network usage and security policies using anonymous proxies, it can create serious application delivery challenges for network administrators. More concerning are the potential security risks and dangers associated with anonymous proxies. Organizations have every right to ask why a user needs to be anonymous if he or she isn't doing anything wrong.

Every day, anonymous proxy servers and applications enable savvy users to access blocked sites – games, chat rooms, instant messaging, social networking and offensive content such as Internet pornography. Even if the user doesn't mean any harm to the organization, anonymous proxy server sites are often run by untrusted third parties that may have questionable intentions.

By providing visibility into all traffic on the network including anonymous proxy traffic, Exinda helps organizations maintain appropriate network usage policies and make the most of their available bandwidth. With the Exinda appliance, network administrators have a way to detect and control unwanted and potentially malicious traffic so that application performance and security are preserved.

About Exinda

Exinda is a global provider of WAN optimization and application acceleration products. Exinda has helped over 2,000 organizations worldwide reduce network operating costs and ensure consistent application performance over the WAN. The Exinda Unified Performance Management (UPM) solution encompasses application visibility, control, optimization and intelligent acceleration – all within a single network appliance that is affordable and easy to manage.

Founded in 2002, Exinda is headquartered in Boston, Massachusetts with regional offices in Canada and the United Kingdom. Research and Development is centralized in Melbourne, Australia.

To learn more about Exinda's award-winning solutions, contact your local reseller or visit: www.exinda.com.

exinda

North America
+1 877 439 4632

EMEA
+44 808 120 1996

Asia Pacific
+61 3 9415 8332

www.exinda.com

© 2010 Exinda Networks. All rights reserved. Exinda is a registered trademark of Exinda Networks PTY Ltd. All other product names, company names, trademarks, registered trademarks, logos and symbols are the property of their respective owners.