Ultrasurf – Architecture Overview and Blocking Strategy

Author: Rich Sutton
8e6 Labs, 8e6 Technologies
rsutton [at] 8e6 [dot] com
Last Update: March 19, 2008

Table of Contents

Overview – Executive Summary

Ultrasurf is a proxy client, which is a program designed to allow end users to circumvent gateway security devices like web filters and secure web gateways in order to surf the Internet without restrictions.

Ultrasurf was developed by an organization called Ultrareach (http://www.ultrareach.com/), which was founded by a group of Chinese political dissidents. Ultrareach continues to actively maintain and update Ultrasurf. They designed Ultrasurf specifically to allow Chinese citizens to circumvent the Chinese government's efforts to restrict Internet use in China.

The Chinese government has constructed a large and formidable Internet filtering infrastructure in order to prevent Chinese citizens from accessing sites that it believes represent an ideological threat to the Chinese Communist Party. This filtering system is widely known as the "Golden Shield" or the "Great Firewall of China". Many large US-based technology companies have been complicit in its construction, as a contingency of doing business in China. It is a formidable adversary, likely one of the most sophisticated Internet filtering systems in the world.

http://www.forbes.com/forbes/2006/0227/090.html

http://www.businessweek.com/magazine/content/06_08/b3972061.htm

As a result, Ultrasurf is a very sophisticated piece of software. It uses a distributed network of proxy servers, installed and maintained by volunteers around the world much like a peer-to-peer network. It uses multiple schemes to locate the proxy servers in its network, spanning different protocols. It uses port and protocol tunneling in order to trick security devices into ignoring it or mishandling it. It also uses encryption and misdirection to thwart efforts to investigate how it works.

Ultrasurf is free and requires no registration, which makes it widely distributable. It requires no installation and can be run by a user that doesn't have administrative permissions to his computer, which makes it very portable. It can easily be carried around on a USB thumb drive and run from there.

Unfortunately, what makes Ultrasurf an incredibly powerful tool for allowing political dissidents around the world to evade oppression also provides end users on private, filtered networks with a way to access the Internet that violates acceptable use policies and introduces liability to an organization.

Up to and including version 8.1 of Ultrasurf, 8e6's Internet filter, the R3000, provided seamless blocking using packet signatures (aka "patterns"). However, Ultrareach made changes to the protocol used by Ultrasurf with version 8.2, introducing an end-to-end encryption scheme that renders packet signatures ineffective. Since then the R3000 has not been able to provide complete blocking of Ultrasurf like it can with almost every other proxy client. As of the end of 2007, the current release of Ultrasurf was version 8.8.

Since the release of Ultrasurf 8.2, we have done extensive research to determine how this program can be blocked using a combination of the R3000 and other gateway security devices, primarily a firewall. In this whitepaper, we will examine Ultrasurf's architecture and provide recommendations for firewall, network policy and R3000 filtering configurations that can effectively block Ultrasurf.

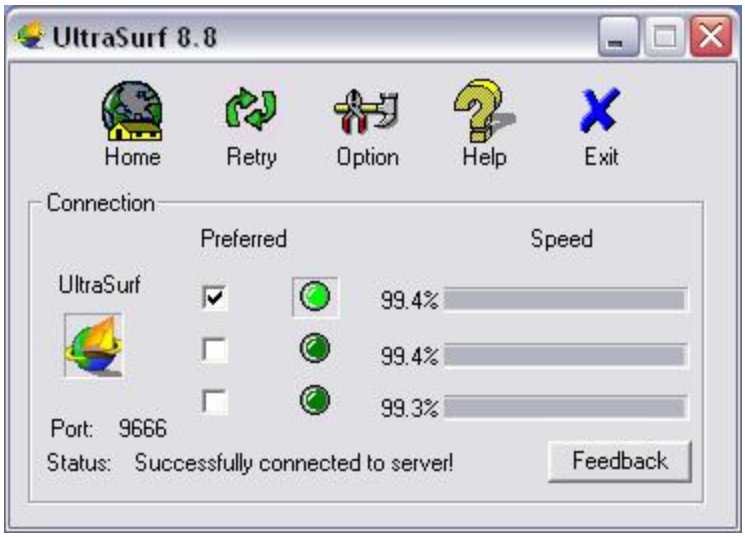
This research has been fed back into product development and 8e6 is planning a number of product enhancements to address the continuing evolution of sophisticated proxies like Ultrasurf.

How It Works

Local Proxy

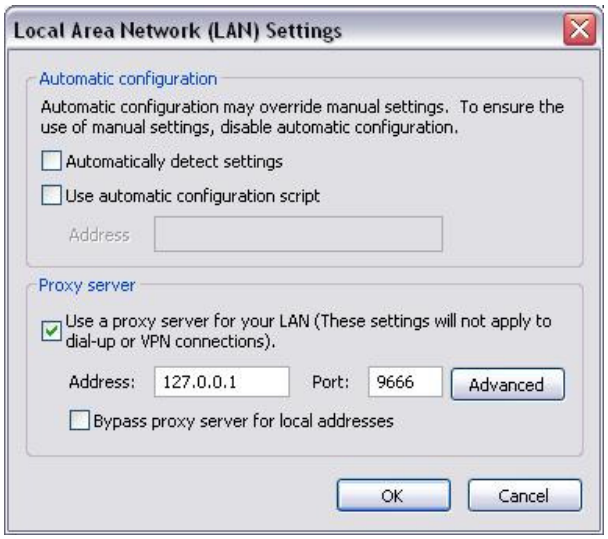
Ultrasurf is a proxy client, which means that it is a program that must be downloaded to and executed on the computer that the user uses for Internet access. For a more in-depth discussion of a proxy client, please refer to this article: http://8e6labs.com/2007/11/15/overview-of-the-different-types-of-proxies-that-exist-and-how-we-block-them/, which provides an overview of the different proxy types.

Ultrasurf requires Windows; there is no Mac or Linux version.



Ultrasurf screenshot

Ultrasurf sets up a local proxy on the user's computer, and then configures Internet Explorer's proxy settings to run all Internet requests through that local proxy. It works automatically with Internet Explorer; however, the user can also use Firefox or any other browser that supports a proxy configuration by manually changing the browser's proxy settings. The default port is 9666.

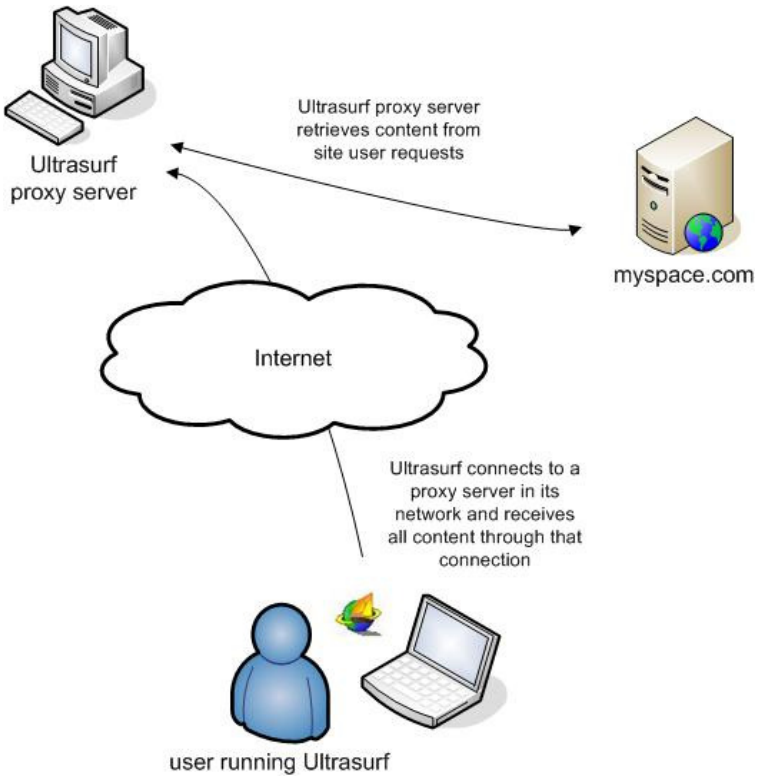


Internet Explorer's Proxy Settings

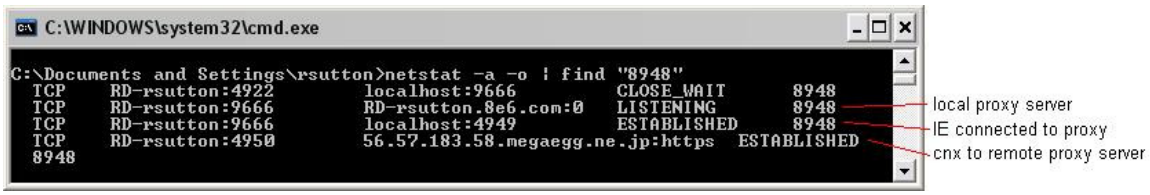
The user can then browse any Internet site normally using IE. All traffic funnels through the local Ultrasurf proxy. Since the traffic between Ultrasurf and IE is entirely on the localhost, it never goes to the network and can't be blocked by a network device.

Ultrasurf then sets up an encrypted connection with a remote server in its network of proxy servers. When the user browses a blocked site (for example, myspace.com), IE sends the request to Ultrasurf, which then forwards the request to its proxy server. The proxy server retrieves the content of myspace.com and returns it through the encrypted

tunnel to Ultrasurf, which sends it back to IE. All that you see at the gateway is the encrypted tunnel.



Ultrasurf basic architecture, which is typical of proxy clients



Netstat output showing Ultrasurf's TCP connections

This is a very typical setup for a proxy client, but Ultrasurf takes additional steps in order to make it difficult to defend at the gateway.

Non-Standard Use of SSL

The connection to the remote proxy server is made over port 443, which is the standard HTTPS port (that's why the netstat output above shows a connection as https). However, in Ultrasurf versions 6.6 and 6.7, the connection traveled port 443 but was not SSL. Starting in version 8.8, Ultrasurf began to use what appears to be an anonymous SSL connection, where the server side does not respond with a certificate. It is not known whether or not the subsequent communication continues to use SSL, or whether this is merely a diversion.

The use of port 443 is specifically to trick gateway devices into ignoring the traffic. The use of non-standard SSL or non-SSL transmissions over port 443 is designed to trick gateway devices into mishandling the traffic.

Proxy Server Discovery

Ultrasurf also has a very scalable and resilient design for discovering proxy servers in this network. It uses four methods; a few of these can be blocked at the firewall; others can be blocked by the R3000.

The methods are:

- A cache file of proxy server IPs stored in the user's local temp directory from a previous execution.
- DNS requests to external DNS servers, which return encoded IPs of proxy servers.
- A document on Google Docs containing a rapidly updated, signed and encrypted list of active proxy servers.
- A static list of proxy server IPs built into the program.

Once Ultrasurf discovers a proxy server in its network, it can retrieve IP addresses of other proxy servers directly from that server.

Cache File

Ultrasurf stores previously discovered nodes in a cache file that it writes to the user's temp directory. The name of the file appears to be based on some static element of the system, like a disk ID or other hardware token, because the name of the cache file will be different across systems but always the same on the same system.

If users in your network have already been using Ultrasurf, then they will already have created cache files. In order to eliminate the cache files and make the subsequent blocking advice in this document work effectively, you may have to manually remove the cache file. The best way to accomplish this is by deleting the contents of the user's temp directory when the user is not running Ultrasurf.

See the Proxy Server Locations section below for steps to take if this is not a feasible approach.

DNS

If no cache file is found, or the cache file doesn't contain a suitable number of proxy server nodes for fail-over, Ultrasurf attempts to locate proxy servers using a set of external DNS servers.

Ultrasurf makes multiple simultaneous requests to a set of DNS servers on the Internet. The list is compiled into Ultrasurf, so Ultrareach can only change the list with a new software release. The list contains 351 IP addresses. 8e6 maintains the full list, which is available to customers on request. The R3000 does not inspect UDP, so it can't block these DNS requests.

Like the cache file, the list appears to be indexed by some hardware token – Ultrasurf uses between 11 and 15 DNS servers depending on the version, and the list used is always the same on one computer but varies across different computers.

The DNS servers are public DNS servers, which are available for anyone to query, and are therefore not considered malicious in and of themselves. Reverse lookups on IPs in the list reveal that a majority of the servers are owned and operated by educational institutions.

The DNS requests are validly formed and are for a variety of hosts, some unregistered like www.chicagometallics.info, some well-known like www.torrentspy.com and others owned by Ultrareach itself:

http://whois.domaintools.com/fosterywheler.info

http://whois.domaintools.com/luce-here.info

It is most likely that the queries for well-known names are meant as misdirection. Since the DNS servers are clearly not owned by Ultrareach, they could have no control over the data returned from those queries.

The queries for hostnames owned by Ultrareach return three IP addresses each and that set of IPs changes every few minutes. The addresses appear to be encoded, because after receiving the DNS responses, Ultrasurf subsequently connects to different IP addresses.

Ultrareach uses public, external DNS servers to ensure correct name resolution for these hosts. Private DNS servers, especially those inside of China, could be configured to return an unreachable address (like localhost 127.0.0.1) for Ultrareach owned domains.

If the DNS requests are blocked, then Ultrasurf must move on to its next proxy server discovery method.

Blocking Advice: At the firewall, block DNS queries to external DNS servers or unauthorized DNS servers. Ensure that authorized DNS traffic is allowed, including outbound traffic from your internal DNS servers to upstream DNS servers. 8e6 will also maintain the full list of DNS servers used by Ultrasurf so that you may block only those, but that potentially leaves you one step behind when a new version of Ultrasurf comes out.

Google Docs

If Ultrasurf still needs to find proxy servers, it will request this document from Google Docs: https://docs.google.com/View?docid=dd4gbd38_6c8fpk2. The request is made in conjunction with a group of misdirection HTTPS requests that are meant to make it difficult to see what's going on in a packet sniffer.

This document is a signed, encrypted, base64 encoded list of IP addresses of active Ultrasurf proxy servers. It is updated relatively frequently – in our research we found that the list changed at least once an hour.

Blocking Advice: In the R3000, block docs.google.com by IP address (see below) and make sure that HTTPS filtering is on. This will prevent Ultrasurf from being able to request this document. Unfortunately, because we are not an SSL terminating proxy, we are not able to block only this specific document.

The important detail here is that in order to block docs.google.com, you must add its IP addresses to your list of blocked URLs.

The R3000's HTTPS filtering can only operate on data pulled from the HTTPS stream that's not encrypted, which includes the destination IP address and the certificate. The certificate used by docs.google.com is encoded with the hostname "*.google.com". As a result, the R3000 can't distinguish between google.com and docs.google.com by using the certificate. In order to allow the R3000 to tell the difference, you must also add the docs.google.com IP addresses to your blocked list.

As of March 19, 2008, docs.google.com was resolving to the following IPs:

209.85.167.100
209.85.167.101
209.85.167.102
209.85.167.113

Static List

If Ultrasurf still can't find a suitable proxy server, it falls back on a built-in list of proxy servers with static IPs. The list contains 196 IP addresses, 43 of which reside in network address ranges owned by Ultrareach itself. The rest appear to be computers connected to high-speed DSL or cable connections with static IPs. Like the cache file and DNS server list, this list appears to be indexed by a hardware token, as Ultrasurf will use the same subset of IPs from the list on one computer, but a different, unchanging subset on other computers.

8e6 places these IP addresses in the Proxy category of our Library. We monitor new releases of Ultrasurf and keep that list updated.

However, since the traffic Ultrasurf sends to these IPs is not HTTP, pattern detection must be enabled for blocking to occur. When proxy pattern detection is enabled, all TCP connections to an IP address in the Proxy category are terminated.

Blocking Advice: Make sure you are blocking the Proxy category and have pattern detection enabled.

Proxy Server Locations

This problem remains: Once Ultrasurf has found a proxy server and has stored that IP in its cache file in the temp directory, it will use that server until it can no longer connect to it or until it finds a faster one. Over the course of a month, we attempted to discover all of the nodes in the Ultrasurf network to block it by brute force. After harvesting over 1500 unique proxy server IPs, we saw a pattern that indicated that this approach is infeasible.

The majority of proxy "servers" are actually running on home computers attached to the Internet over DSL or some other high speed connection. These connections typically use DHCP addressing. Each time the home computer is powered on and off, the Internet connection is rebuilt and the computer is assigned a different IP by the ISP. Ultrasurf then appears to re-register to the proxy server network using its new IP.

The proxy "server" may very well simply be a promiscuous client or "master client node" in the form of a peer-to-peer network like Skype (we didn't verify that).

Luckily, almost all of this DHCP-based DSL addressing uses a fixed set of contiguous IP addresses known as a "netblock". This results in similar addresses being assigned to the same computer as long as it continues to connect from the same physical location. This assumption can be corroborated through reverse DNS lookups.

For example, here are a set of Ultrasurf proxy servers on the HiNet DSL network (which is an ISP in Taiwan), with their corresponding reverse DNS lookups

59.112.160.145	59-112-160-145.dynamic.hinet.net
59.112.167.127	59-112-167-127.dynamic.hinet.net
59.112.173.204	59-112-173-204.dynamic.hinet.net

These IPs are all in the HiNet netblock 59.112.0.0/14.

8e6 has built a comprehensive list of these "home computer netblocks", available on request. Not surprisingly, netblocks based in Taiwan and California communities with high concentrations of East Asian immigrants were most likely to be hosting large numbers of Ultrasurf servers.

Our research was corroborated by public dialup user lists (http://en.wikipedia.org/wiki/Dialup_Users_List) maintained by the spam blocking organizations SORBS and Spamhaus:

SORBS: http://www.au.sorbs.net/faq/dul.shtml

Spamhaus: http://www.spamhaus.org/pbl/index.lasso

Blocking these netblocks is low risk because the ISPs expressly don't allow those end users to run mail servers or web servers on those home computers. In fact they often publish data directly to organizations like Spamhaus in order to facilitate the blocking of spam.

Some would argue that *not* blocking those netblocks is a *high* risk. Home computers directly connected to the Internet are the computers least likely to be actively managed and kept up-to-date with patches, and are therefore the computers most often compromised by viruses and hijacked by bots. Most DDoS attacks emanate from hordes of infected home computers. Blocking these netblocks will have the dual effect of blocking Ultrasurf and protecting your end users from infection.

Blocking Advice: At the firewall, block IP ranges of problematic home computer netblocks. This list is available through 8e6's Tech Support.

Summary of Steps to Take to Block Ultrasurf

1. At the firewall, block all outbound DNS requests to unauthorized external DNS servers – or – request the list of known Ultrasurf DNS servers from 8e6 and block only those. Ensure that authorized DNS traffic is allowed, including outbound traffic from your internal DNS servers to upstream DNS servers.
2. At the web filter, block docs.google.com by IP address and make sure HTTPS filtering is on.
3. At the web filter, block the Proxy category and make sure that proxy pattern detection is enabled.

4. Remove Ultrasurf cache files in user temp directories – and/or – at the firewall, block the IP ranges of problematic home computer netblocks.

Appendix

Appendix A – Other Blocking Methods

8e6's Mobile Client

The next version of the mobile client (2.0.10) will block all applications from connecting to the network that are named "ultrasurf.exe" or have one of a number of variations on that name. This will provide some protection, but can obviously be circumvented by a determined attacker.

Antivirus – Sophos

Sophos has written a signature against Ultrasurf, calling it a "Potentially unwanted application". This allows Sophos anti-virus applications to detect Ultrasurf as the end user attempts to run it, just as if the end user had downloaded a virus:

http://www.sophos.com/virusinfo/analyses/ultrasurf.html

Sophos AV can be deployed on the endpoint and at the email gateway.

Antivirus – Symantec

Symantec (Norton) detects Ultrasurf version 8.7 as a Trojan horse. The detection is triggered by heuristics – Symantec has not written a signature against it.

Firewall – Symantec

Symantec Endpoint Security includes a host firewall. That firewall allows you to block executables from talking on the network by hash value. Using the firewall policy administrator, create hashes of Ultrasurf versions and add them to your firewall policy. Then push out that policy to all of your endpoints.

Active Directory Application Control

Microsoft's Active Directory can be used for application control. Via Group Policy, the administrator can restrict certain programs from being run by certain users.

Appendix B – Netblocks owned by Ultrareach

These netblocks are owned by Ultrareach. Many of the IPs in these ranges are used for proxy servers. 8e6 blocks all IPs in these ranges in the Proxy category.

Netblock	Start IP	End IP	Owner
67.15.183.0/25	67.15.183.0	67.15.183.127	Ultrareach - USA
67.15.100.192/26	67.15.100.192	67.15.100.255	Ultrareach - USA
67.15.151.64/26	67.15.151.64	67.15.151.127	Ultrareach - USA
64.62.138.0/25	64.62.138.0	64.62.138.127	Sound of Hope Radio Network - USA