Ultrasurf – Architecture Overview and Blocking Strategy

Download page for testing

UltraSurf's use of custom protocols puts it beyond the scope of traditional web filtering solutions. This is especially true for out-of-band products, like the Web Filter. A full solution for UltraSurf at the network level requires an inline product, such as our Secure Web Gateway, coupled with a firewall that prevents most direct Internet connections from user PCs (thereby ensuring that web connections go through SWG), SWG is our in-line product(Secure Web Gateway).

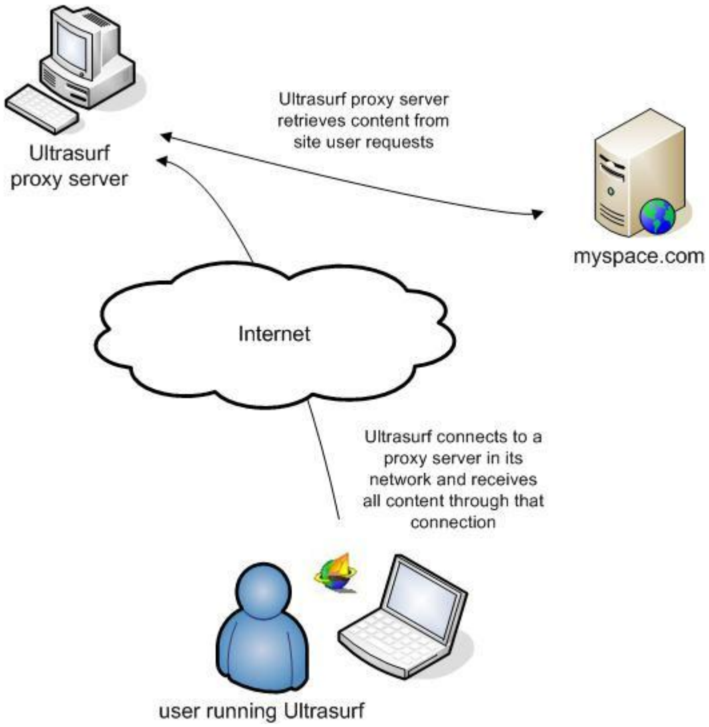
Best practice: If you have admin access over the PCs, the best way is a group policy restricting executable to only the ones you authorize.

How It Works

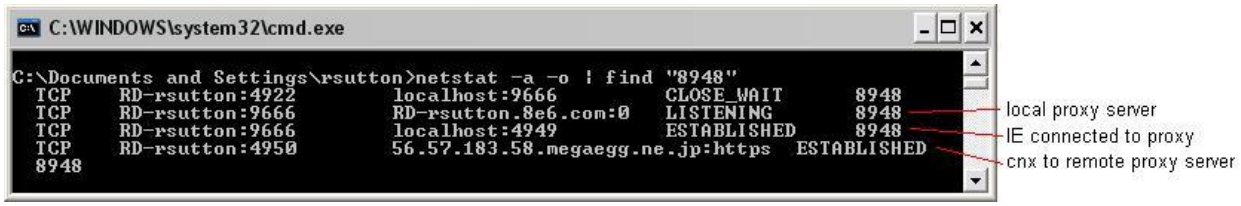
Blocking UltraSurf at the network level is a cat-and-mouse game. It always will be, given that UltraSurf's sole purpose is to defeat network filters. Consequently, it might be better to approach UltraSurf from a different angle – application controls on the desktop. At that point, it becomes a matter of preventing users from running untrusted code on desktop PCs.

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.

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 proxy server
Ultrasurf proxy server retrieves content from site user requests
myspace.com
Internet
Ultrasurf connects to a proxy server in its network and receives all content through that connection
user running Ultrasurf

Ultrasurf basic architecture, which is typical of proxy clients



```
C:\Documents and Settings\rsutton>netstat -a -o ¦ find "8948"
  TCP    RD-rsutton:4922        localhost:9666          CLOSE_WAIT      8948
  TCP    RD-rsutton:9666        RD-rsutton.8e6.com:0    LISTENING       8948
  TCP    RD-rsutton:9666        localhost:4949          ESTABLISHED     8948
  TCP    RD-rsutton:4950        56.57.183.58.megaegg.ne.jp:https  ESTABLISHED
  8948
```

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.

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).

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 thisnetwork. It uses four methods; a few of these can be blocked at the firewall; others can be blocked by the Filter.
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.

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 filter 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 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. but that potentially leaves you one step behind when a new version of Ultrasurf comes out.