Proxies

Chapter 4

Network & Security

Gildas Avoine

INSA INSTITUT NATIONAL DES SCIENCES APPLIQUÉES RENNES

IUF

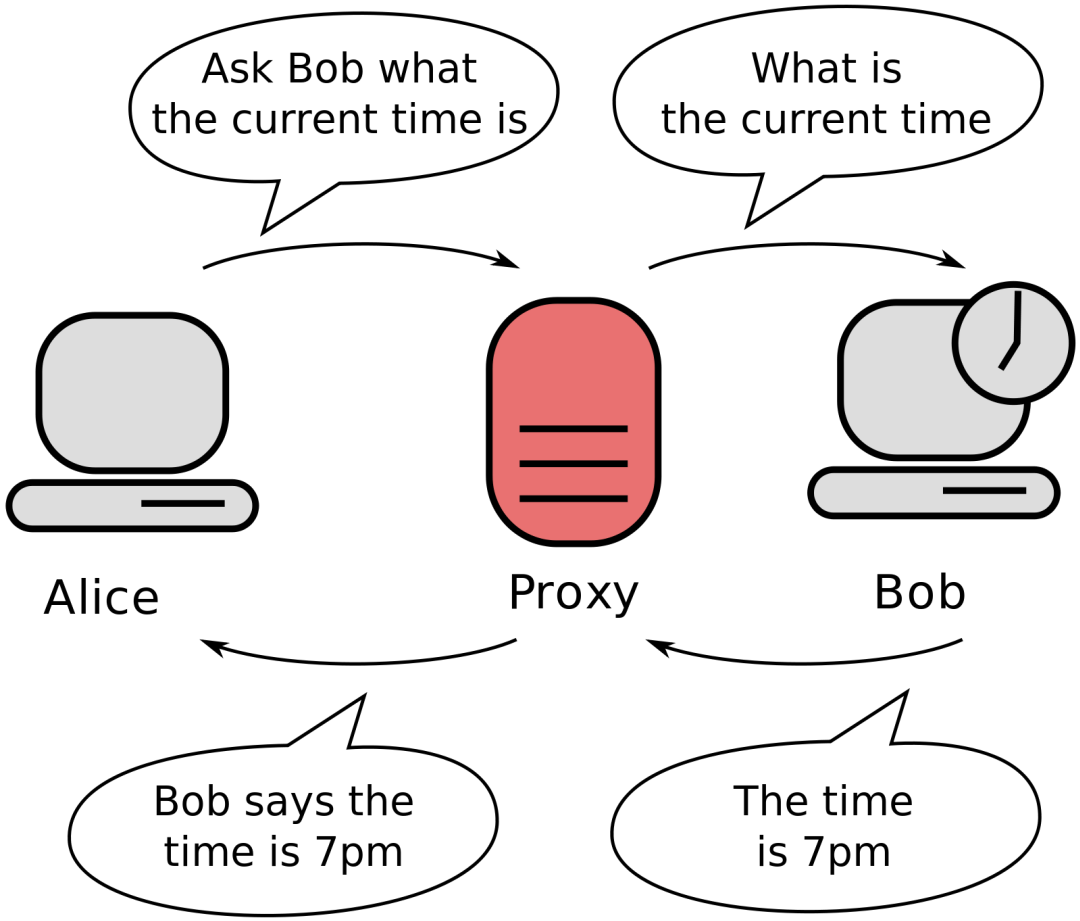
SUMMARY OF CHAPTER 4

- Generalities
- Forward Proxies
- Reverse Proxies
- Open Proxies
- Conclusion

GENERALITIES

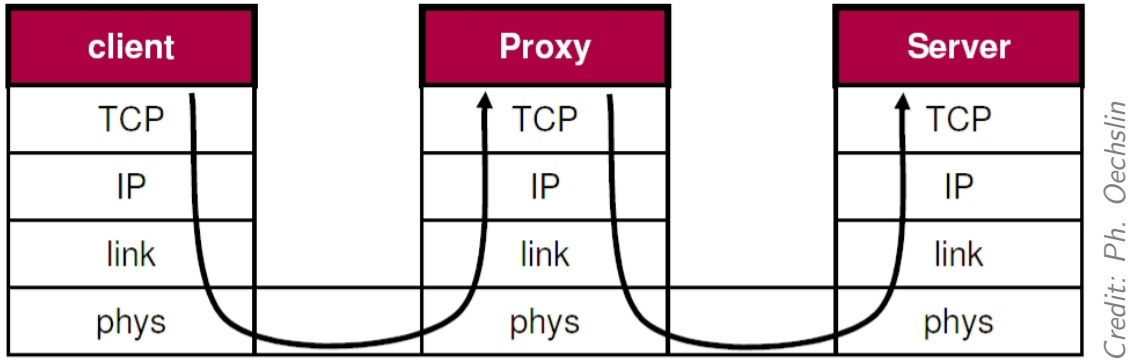
- Generalities
- Forward Proxies
- Reverse Proxies
- Open Proxies
- Conclusion

Introduction: A Proxy is a Relay



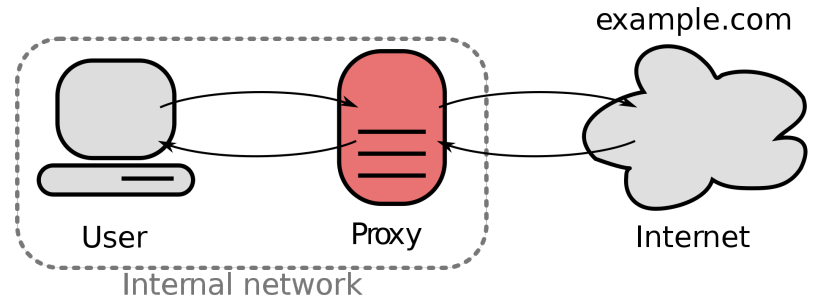
Proxies into the Layers

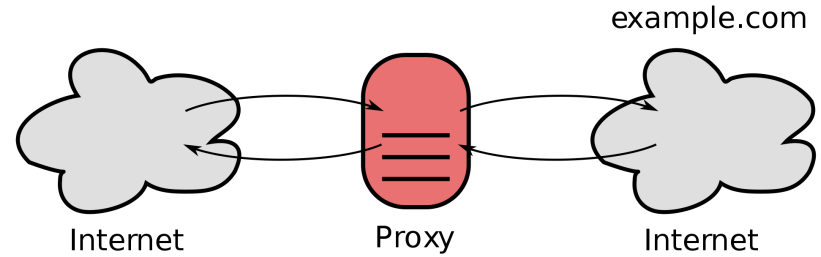
- A proxy are application relays.

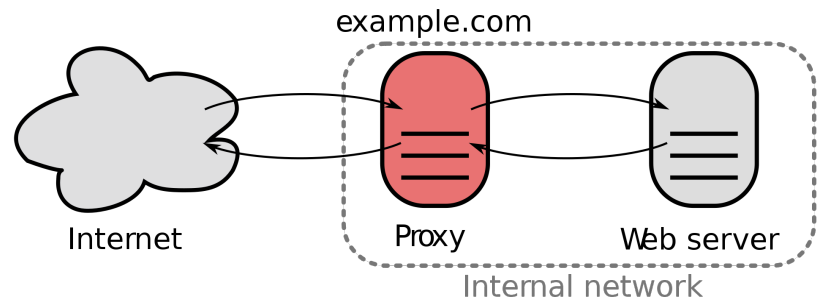


- A proxy plays the role of server for the client, and client for the server.

Scenarios: Forward, Open, Reverse







FORWARD PROXIES

- Generalities
- Forward Proxies
- Reverse Proxies
- Open Proxies
- Conclusion

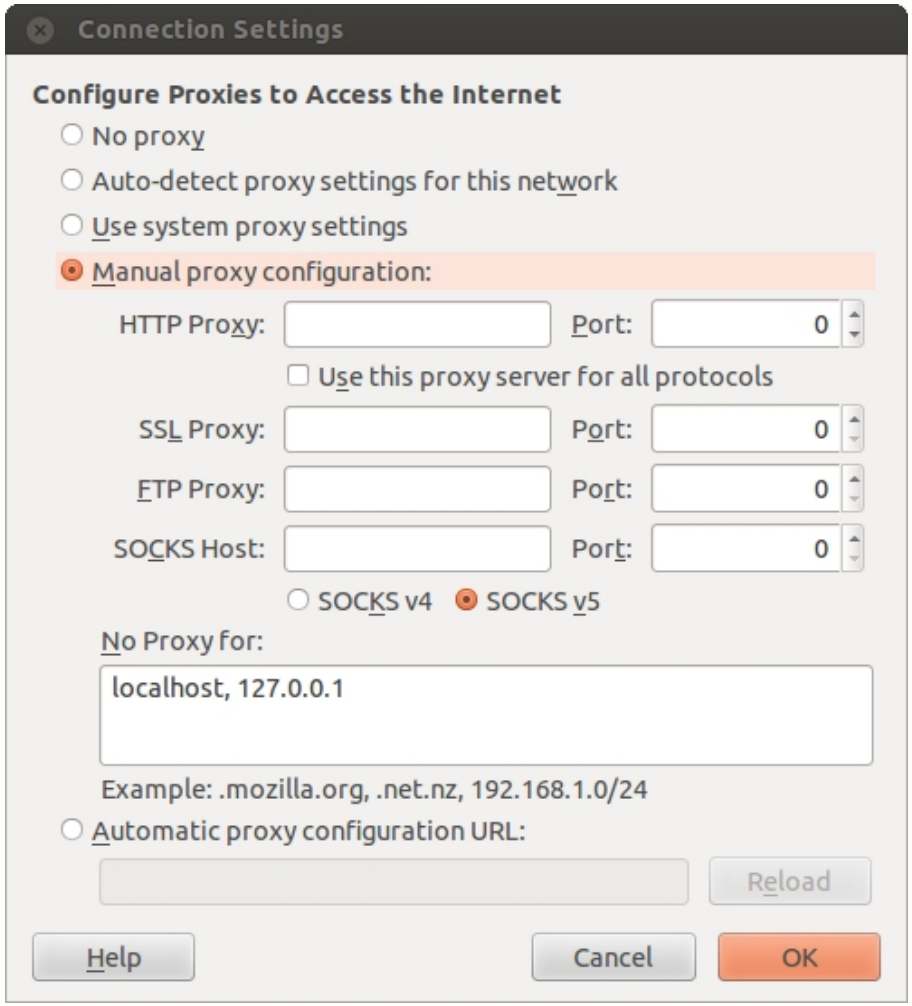
General Benefits

- A proxy prevents direct connections from an internal network towards the Internet.
  - Chokepoint.
  - Possibly authentication.
- A proxy can analyze data within the application's context and possibly filter.
  - URL or DNS blacklists, URL filtering, MIME filtering, keyword filtering, virus, exploit,...
- Proxies are a typical example of defense in depth and choke point principles.

HTTP Proxy

- Cache: the proxy keeps a local copy of all documents it fetched.
- When a second client asks for the same document, the proxy can provide the local copy.
- The transfer is much faster (increase in comfort).
- The proxy saves on bandwidth (indirectly cost).

Configure an HTTP Proxy with Firefox



Intercepting Proxy

- To avoid having to configure the browsers, intercepting proxies can be used.
- In this case, the traffic targeted at a certain port (80 for HTTP) is automatically re-directed towards the proxy by the firewall.
- Limitation: it does not work for Web servers that do not use the standard port.
- Typical use: to force the usage of a proxy.

Environment Variables without Proxy

```
[HTTP_HOST] => www.openskill.info
[HTTP_USER_AGENT] => Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:22.0) Gecko/20100101
[SERVER_SOFTWARE] => Apache/2.2.15 (CentOS)
[SERVER_NAME] => www.openskill.info
[SERVER_ADDR] => 10.42.20.81
[SERVER_PORT] => 80
[REMOTE_ADDR] =>  2.11.120.137
[DOCUMENT_ROOT] => /var/www/html/openskills.info/
[SERVER_ADMIN] => webmaster@openskills.info
[SCRIPT_FILENAME] => /var/www/html/openskills.info/pages/enviro.php
[REMOTE_PORT] => 52810
[GATEWAY_INTERFACE] => CGI/1.1
[SERVER_PROTOCOL] => HTTP/1.0
[REQUEST_METHOD] => GET
[QUERY_STRING] =>
[REQUEST_URI] => /pages/enviro.php
[SCRIPT_NAME] => /pages/enviro.php
[PHP_SELF] => /pages/enviro.php
[REQUEST_TIME] => 1394985213
```

Environment Variables with Proxy

```
[HTTP_HOST] => www.openskill.info
[HTTP_USER_AGENT] => Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:22.0) Gecko/20100101
[SERVER_SOFTWARE] => Apache/2.2.15 (CentOS)
[SERVER_NAME] => www.openskill.info
[SERVER_ADDR] => 10.42.20.81
[SERVER_PORT] => 80
[REMOTE_ADDR] =>  111.8.55.73
[DOCUMENT_ROOT] => /var/www/html/openskills.info/
[SERVER_ADMIN] => webmaster@openskills.info
[SCRIPT_FILENAME] => /var/www/html/openskills.info/pages/enviro.php
[REMOTE_PORT] => 52810
[GATEWAY_INTERFACE] => CGI/1.1
[SERVER_PROTOCOL] => HTTP/1.0
[REQUEST_METHOD] => GET
[QUERY_STRING] =>
[REQUEST_URI] => /pages/enviro.php
[SCRIPT_NAME] => /pages/enviro.php
[PHP_SELF] => /pages/enviro.php
[REQUEST_TIME] => 1394985213
```

Telnet without Proxy

avoine@asterix: ~

```
avoine@asterix:~$ telnet www.ubuntu.com 80
Trying 91.189.90.58...
Connected to www.ubuntu.com.
Escape character is '^]'.
GET /index.html
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
  "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en" dir="ltr">

<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
  <title>Error | Ubuntu</title>
  <meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<link rel="shortcut icon" href="/sites/all/themes/ubuntu10/favicon.ico" type="image/x-icon" />
  <link rel="alternate" type="application/rss+xml" title="Canonical RSS" href="http://www.canonical.
com/rss.xml" />
  <link href='http://fonts.googleapis.com/css?family=Ubuntu:300,400,700,300italic,400italic,700itali
c' rel='stylesheet' type='text/css' />

<style type="text/css" media="all">
  @import "/sites/www.ubuntu.com/files/active/ctools/css/6e2c426c2e7f34f61a85decd3aa0cdae_0.css?N";
  @import "/modules/node/node.css?N";
  @import "/modules/system/defaults.css?N";
  @import "/modules/system/system.css?N";
  @import "/modules/system/system-menus.css?N";
  @import "/modules/user/user.css?N";
  @import "/sites/all/modules/cck/theme/content-module.css?N";
```

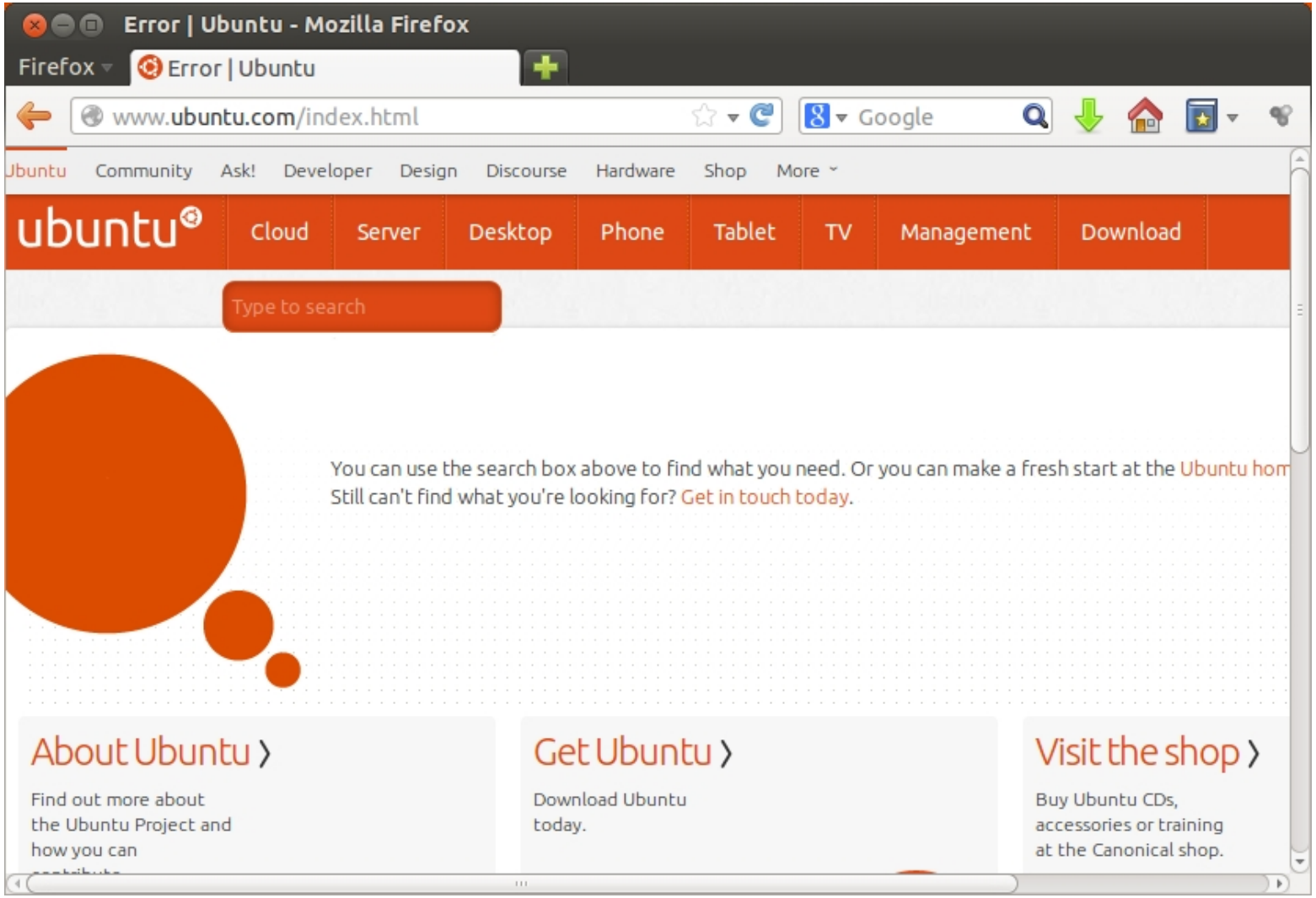
Telnet with Proxy

```
avoine@asterix: ~
avoine@asterix:~$ telnet 111.8.55.73 80
Trying 111.8.55.73...
Connected to 111.8.55.73.
Escape character is '^]'.
GET/index.html
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dtd
">
<HTML><HEAD><META HTTP-EQUIV="Content-Type" CONTENT="text/html; charset=iso-8859-1">
<TITLE>ERROR: The requested URL could not be retrieved</TITLE>
<STYLE type="text/css"><!--BODY{background-color:#ffffff;font-family:verdana,sans-serif}PRE{font-fam
ily:sans-serif}--></STYLE>
</HEAD><BODY>
<H1>ERROR</H1>
<H2>The requested URL could not be retrieved</H2>
<HR noshade size="1px">
<P>
While trying to retrieve the URL:
<A HREF="index.html">index.html</A>
<P>
The following error was encountered:
<UL>
<LI>
<STRONG>
Invalid URL
</STRONG>
</UL>

<P>
```

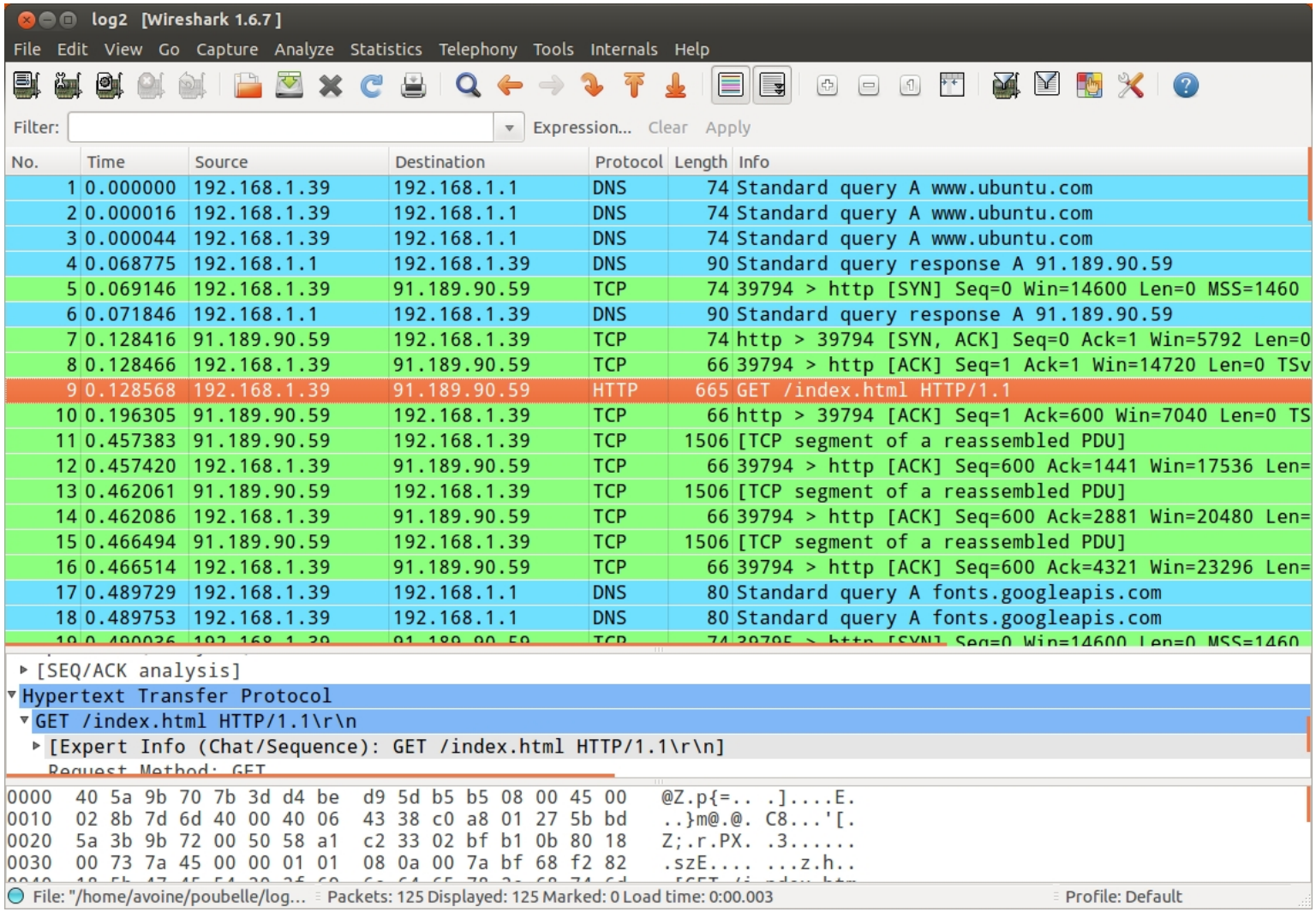
Telnet with Proxy

```
avoine@asterix: ~
avoine@asterix:~$ telnet 111.8.55.73 80
Trying 111.8.55.73...
Connected to 111.8.55.73.
Escape character is '^]'.
GET http://www.ubuntu.com/index.html
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
  "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en" dir="ltr">

<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
  <title>        Ubuntu</title>
  <meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<link rel="shortcut icon" href="/sites/all/themes/ubuntu10/favicon.ico" type="image/x-icon" />
  <link rel="alternate" type="application/rss+xml" title="Canonical RSS" href="http://www.canonical.
com/rss.xml" />
  <link href='http://fonts.googleapis.com/css?family=Ubuntu:300,400,700,300italic,400italic,700itali
c' rel='stylesheet' type='text/css' />

<style type="text/css" media="all">
  @import "/sites/www.ubuntu.com/files/active/ctools/css/6e2c426c2e7f34f61a85decd3aa0cdae_0.css?N";
  @import "/modules/node/node.css?N";
  @import "/modules/system/defaults.css?N";
  @import "/modules/system/system.css?N";
  @import "/modules/system/system-menus.css?N";
  @import "/modules/user/user.css?N";
  @import "/sites/all/modules/cck/theme/content-module.css?N";
  @import "/sites/www.ubuntu.com/files/active/css_injector_2.css?N";
```

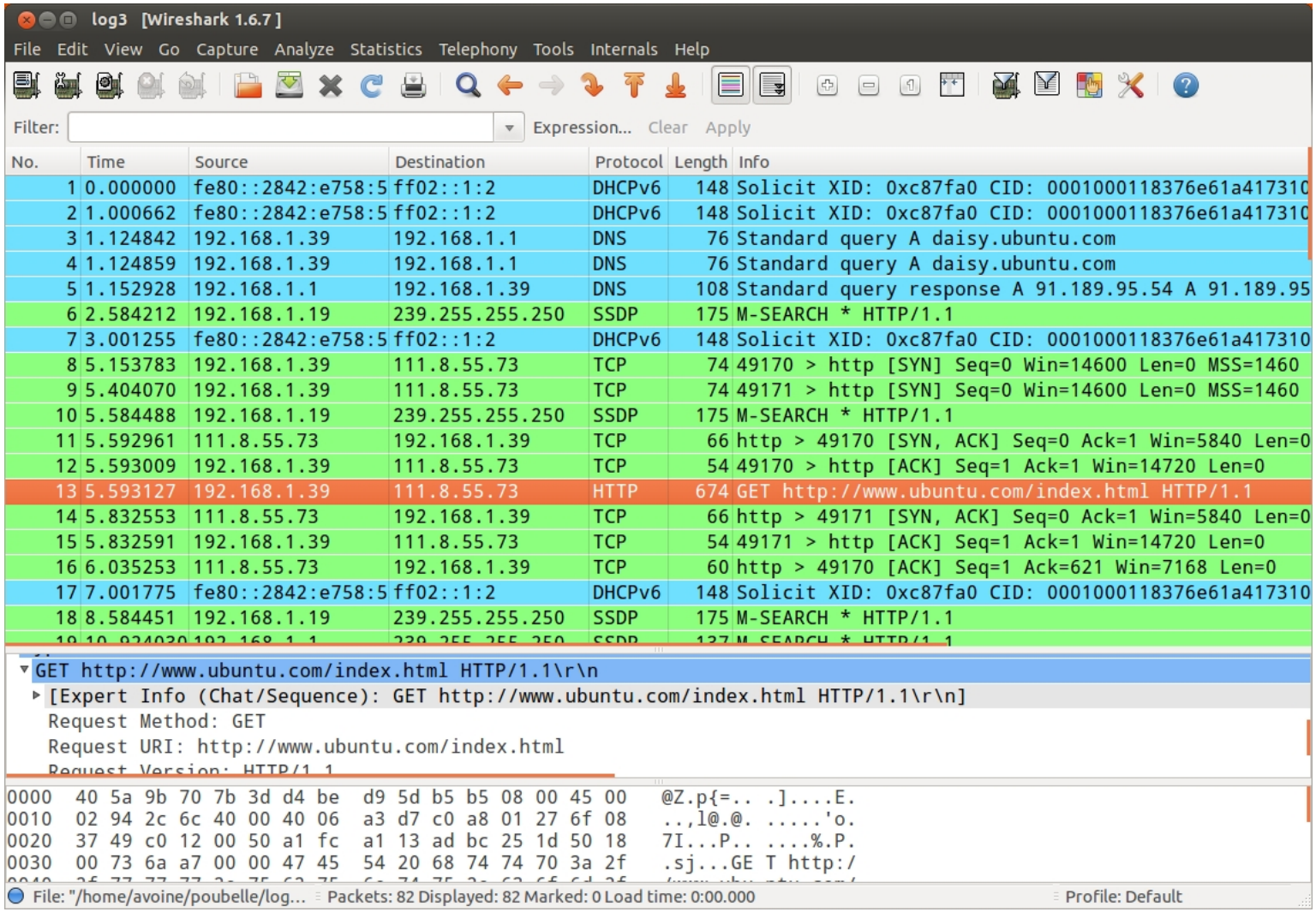
Connection With a Browser



Wireshark Sniffing without Proxy



Wireshark Sniffing with Proxy

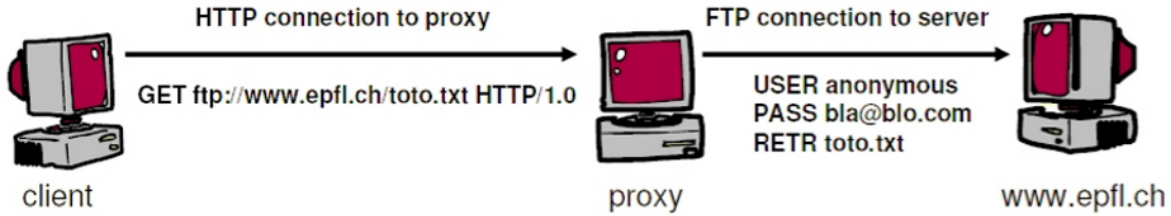


FTP Proxy

- FTP summary:
  - FTP uses a command connection and a data connection.
  - The data connection can be directed towards the client (active mode, default setting) or towards the server (passive mode).
- The FTP protocol was not designed to be used through a proxy.

FTP Proxy using HTTP

- Browsers allow specifying URLs such as FTP://my.server.com/file.txt.
- If the browser is configured to use a HTTP proxy, it will ask the proxy for the URL.
- The HTTP proxy carries out the FTP transfer and provides the document as part of the HTTP reply.

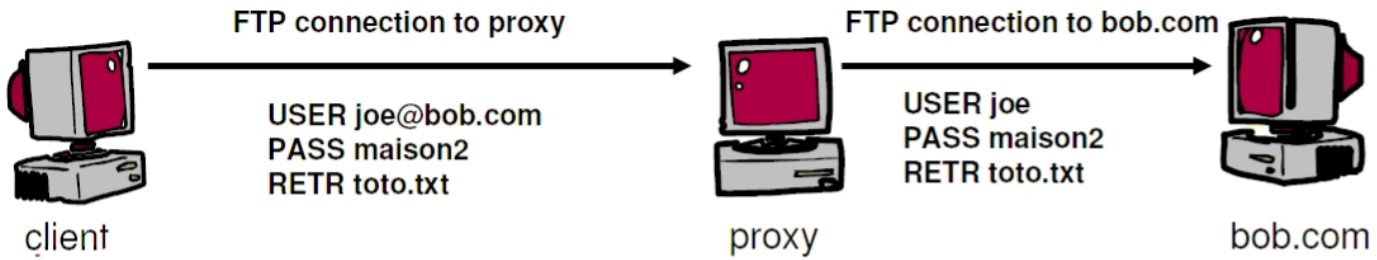


Credit: Ph. Oechslin

- Require to use a browser for the transfer.

User@ FTP Proxy

- The user@ server behaves like a standard FTP server.
- It can be used by any FTP client.
- To access the remote server BOB with username Joe, we provide Joe@BOB as username to the proxy.
- The latter connects to the server and relays the password, commands and the data.
- The 2 connections can use active or passive mode independently.



Credit: Ph. Oechslin

SMTP Proxy

- SMTP was conceived for relaying mail hop by hop.
- Hence, any SMTP server can work as a proxy.
- Outbound (forward path):
  - The proxy is simply specified as SMTP server for outgoing mail in the mail client.
- Inbound (reverse path):
  - The proxy has to be registered in the DNS as the official server for that domain.
  - The proxy has to be configured to forward all mails to the internal server that should receive the mail.

DNS Proxy

- Just like SMTP, the DNS protocol is used to re-transmit requests from server to server.
- DNS servers can work as proxies.
- DNS servers have a cache to limit traffic and reduce response times.
- It is a good idea to configure a DNS proxy to direct all its request towards a bigger server (for e.g. that of an ISP) just to take advantage of a bigger cache.

SOCKS Proxy

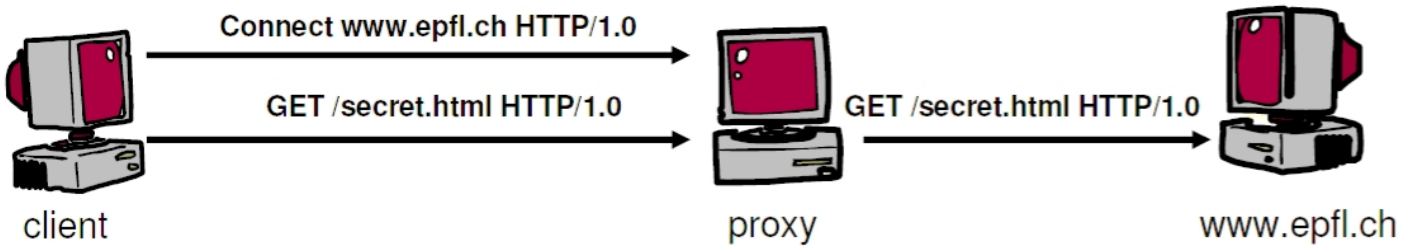
- SOCKS (Socket Server) proxy is a general proxy for TCP and UDP connections.
- It accepts a client's connection and opens another one towards the server.
- It then transfers the data between the two connections.
- Advantage: SOCKS allows any protocol to pass via a proxy.
- Limitation: SOCKS allows any protocol to pass via a proxy.

HTTPS Proxy

- HTTPS is the secure version of HTTP.
- HTTPS proxies are NOT a secure version of HTTP proxies!
- HTTPS encrypts and authenticates end-to-end. If the proxy were able to create the connection to the server, all the advantages of HTTPS would be lost.
- HTTPS proxy does no more than just transparently relay data between a client's connection and a server's connection (very much like SOCKS).

HTTPS Proxy: Implementation

- HTTPS proxy uses the HTTP command "connect" that indicates the server's address.
- It replies by a status and becomes transparent.



Credit: Ph. Oechslin

Security Issues

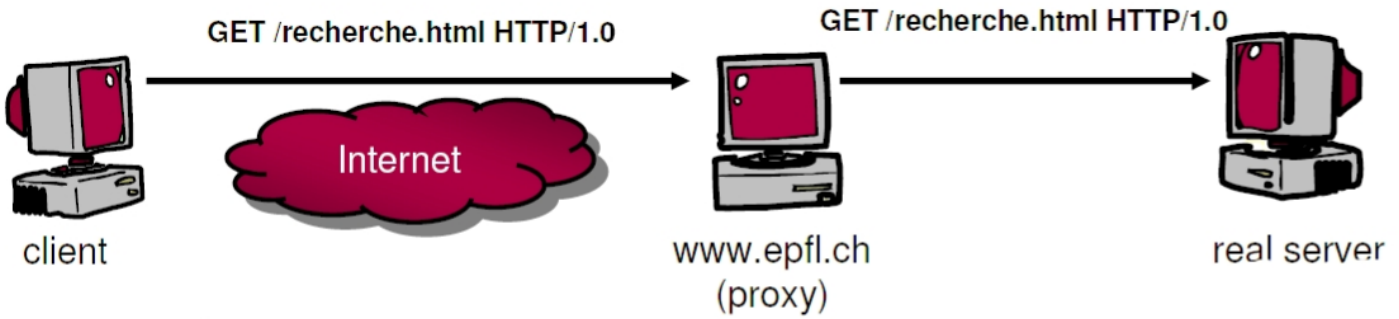
- The HTTPS proxy allows relaying any type of protocol (it is transparent, just like SOCKS).
- To limit abuses, the available ports are often limited to 443 (HTTPS) and 563 (SNEWS).
- To allow any protocol to cross a firewall, it is sufficient to run the server on port 443 and pass through a HTTPS proxy.

REVERSE PROXIES

- Generalities
- Forward Proxies
- Reverse Proxies
- Open Proxies
- Conclusion

Reverse (or Inverse) Proxy

- In the forward path, the client knows that he must pass through a proxy, thus he can adapt his requests accordingly.
- In the return path, the client does not know if he is talking to a server or to a proxy.



Credit: Ph. Oechslin

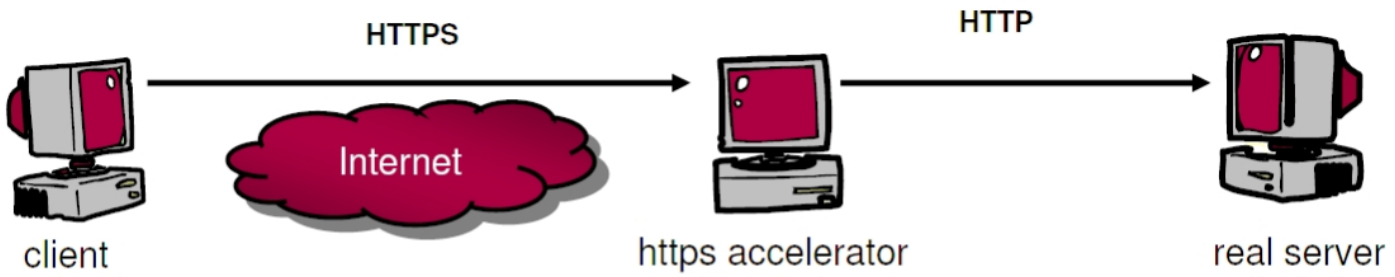
- The proxy must behave like a server.
- For protocols that do not support relaying (HTTP, FTP) the reverse proxy can relay to only one server.

Reverse HTTP Proxy

- Reverse HTTP proxies allow:
  - Filtering of requests (blocking exploits).
  - Authenticating clients even before they speak to the server (you cannot attack the server unless you are authenticated).
  - Accelerating servers.
  - Reformat pages (e.g. for cell phones or PDAs).
- Server accelerators:
  - Reverse proxies work just like caches.
  - The proxy provides static documents while the server only has to generate dynamic document.
  - Workload dispatcher.

Reverse HTTPS Proxy

- Reverse HTTPS proxies are used as encryption accelerators.
  - They can reduce the workload of servers by taking care of the encryption and the authentication.
  - The proxy can have a hardware accelerator for HTTPS.



Credit: Ph. Oechslin

- The connection between the proxy and the server consists of HTTP, not HTTPS.

Protocol Translation

- A proxy can use different protocols each side.
  - E.g. a Web mail application can accept HTTPS requests from the Internet and generate IMAP requests towards the mail server.
  - An e-commerce application can accept HTTPS requests from Internet and generate Corba or SQL requests towards the servers.
- The protocol diversity strongly limits the chances of exploiting a vulnerability across a proxy.

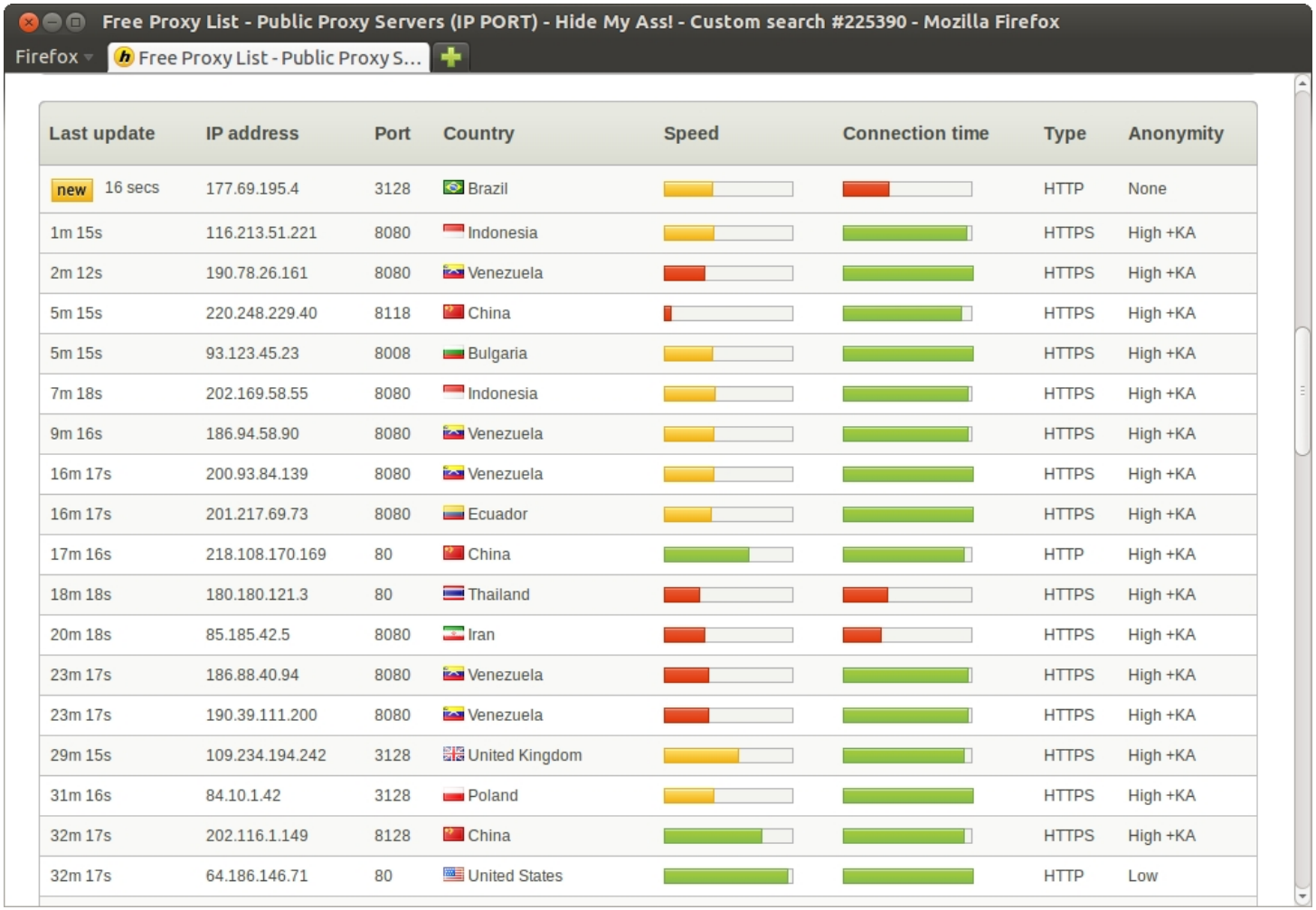
OPEN PROXIES

- Generalities
- Forward Proxies
- Reverse Proxies
- Open Proxies
- Conclusion

General Benefits

- Test a system from outside.
- Browse Internet (more or less) anonymously.

List of Open Proxies



Last update	IP address	Port	Country	Speed	Connection time	Type	Anonymity
new 16 secs	177.69.195.4	3128	Brazil			HTTP	None
1m 15s	116.213.51.221	8080	Indonesia			HTTPS	High +KA
2m 12s	190.78.26.161	8080	Venezuela			HTTPS	High +KA
5m 15s	220.248.229.40	8118	China			HTTPS	High +KA
5m 15s	93.123.45.23	8008	Bulgaria			HTTPS	High +KA
7m 18s	202.169.58.55	8080	Indonesia			HTTPS	High +KA
9m 16s	186.94.58.90	8080	Venezuela			HTTPS	High +KA
16m 17s	200.93.84.139	8080	Venezuela			HTTPS	High +KA
16m 17s	201.217.69.73	8080	Ecuador			HTTPS	High +KA
17m 16s	218.108.170.169	80	China			HTTP	High +KA
18m 18s	180.180.121.3	80	Thailand			HTTPS	High +KA
20m 18s	85.185.42.5	8080	Iran			HTTPS	High +KA
23m 17s	186.88.40.94	8080	Venezuela			HTTPS	High +KA
23m 17s	190.39.111.200	8080	Venezuela			HTTPS	High +KA
29m 15s	109.234.194.242	3128	United Kingdom			HTTPS	High +KA
31m 16s	84.10.1.42	3128	Poland			HTTPS	High +KA
32m 17s	202.116.1.149	8128	China			HTTPS	High +KA
32m 17s	64.186.146.71	80	United States			HTTP	Low

CONCLUSION

- Generalities
- Forward Proxies
- Reverse Proxies
- Open Proxies
- Conclusion

Conclusion

- A long time ago, caching was the main feature of proxies.
- Today's main purpose of proxies is security.
- Proxies are widely used in pratice, typically located in a DMZ.