

Proxies

Chapter 4

Network & Security

Gildas Avoine

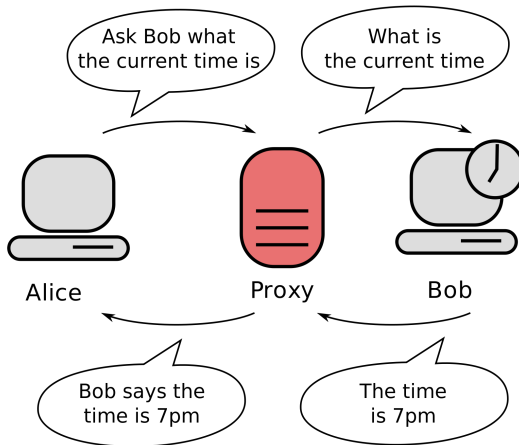
SUMMARY OF CHAPTER 4

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

GENERALITIES

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

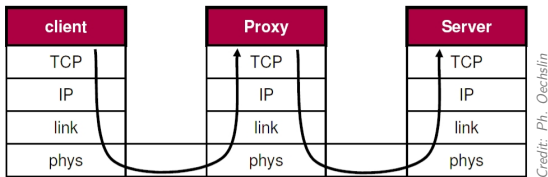
Introduction: A Proxy is a Relay



License: CC0 1.0 Universal

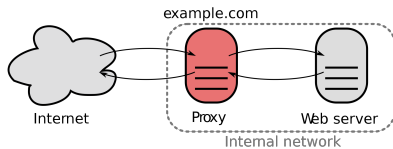
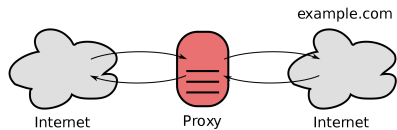
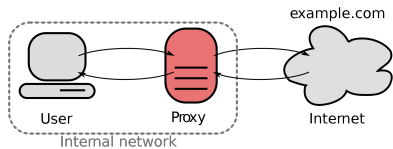
Proxies into the Layers

- A proxy are **application** relays.



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

Scenarios: Forward, Open, Reverse



License: CC0 1.0 Universal

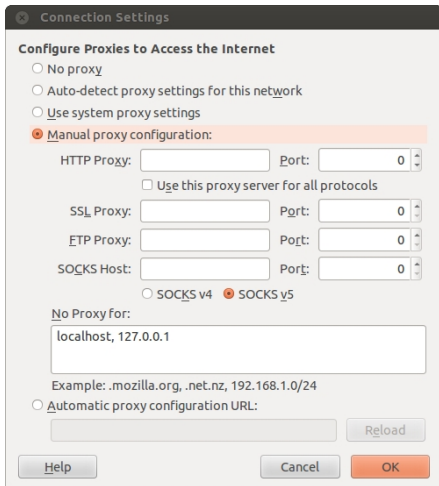
FORWARD PROXIES

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

- 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.

- **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-family: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>
</LI>
</UL>
<P>
```

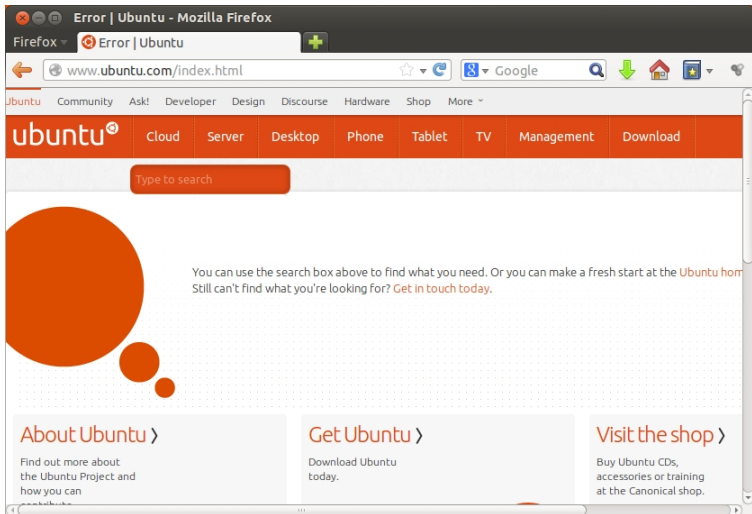
Telnet with Proxy

```
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

log2 [Wireshark 1.6.7]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.39	192.168.1.1	DNS	74	Standard query A www.ubuntu.com
2	0.000016	192.168.1.39	192.168.1.1	DNS	74	Standard query A www.ubuntu.com
3	0.000044	192.168.1.39	192.168.1.1	DNS	74	Standard query A www.ubuntu.com
4	0.068775	192.168.1.1	192.168.1.39	DNS	90	Standard query response A 91.189.90.59
5	0.069146	192.168.1.39	91.189.90.59	TCP	74	39794 > http [SYN] Seq=0 Win=14600 Len=0 MSS=1460
6	0.071846	192.168.1.1	192.168.1.39	DNS	90	Standard query response A 91.189.90.59
7	0.128416	91.189.90.59	192.168.1.39	TCP	74	http > 39794 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0
8	0.128466	192.168.1.39	91.189.90.59	TCP	66	39794 > http [ACK] Seq=1 Ack=1 Win=14720 Len=0 TSv
9	0.128568	192.168.1.39	91.189.90.59	HTTP	665	GET /index.html HTTP/1.1
10	0.196305	91.189.90.59	192.168.1.39	TCP	66	http > 39794 [ACK] Seq=1 Ack=600 Win=7040 Len=0 TS
11	0.457383	91.189.90.59	192.168.1.39	TCP	1506	[TCP segment of a reassembled PDU]
12	0.457420	192.168.1.39	91.189.90.59	TCP	66	39794 > http [ACK] Seq=600 Ack=1441 Win=17536 Len=
13	0.462061	91.189.90.59	192.168.1.39	TCP	1506	[TCP segment of a reassembled PDU]
14	0.462086	192.168.1.39	91.189.90.59	TCP	66	39794 > http [ACK] Seq=600 Ack=2881 Win=20480 Len=
15	0.466494	91.189.90.59	192.168.1.39	TCP	1506	[TCP segment of a reassembled PDU]
16	0.466514	192.168.1.39	91.189.90.59	TCP	66	39794 > http [ACK] Seq=600 Ack=4321 Win=23296 Len=
17	0.489729	192.168.1.39	192.168.1.1	DNS	80	Standard query A fonts.googleapis.com
18	0.489753	192.168.1.39	192.168.1.1	DNS	80	Standard query A fonts.googleapis.com
19	0.490226	192.168.1.39	91.189.90.59	TCP	74	39794 > http [SYN] Seq=0 Win=14600 Len=0 MSS=1460

▶ [SEQ/ACK analysis]

▼ Hypertext Transfer Protocol

▶ GET /index.html HTTP/1.1\r\n

▶ [Expert Info (Chat/Sequence): GET /index.html HTTP/1.1\r\n]

Request Method: GET

```
0000 40 5a 9b 70 7b 3d d4 be d9 5d b5 b5 08 00 45 00 @Z.p[...].E.
0010 02 8b 7d 6d 40 00 40 06 43 38 c0 a8 01 27 5b bd ..}m@.C8...'[.
0020 5a 3b 9b 72 00 58 a1 c2 33 02 bf b1 0b 80 18 Z;.r.PX..3.....
0030 00 73 7a 45 00 00 01 01 08 0a 00 7a bf 68 f2 82 .szE....z.h..
```

File: /home/avoine/poubelle/log... Packets: 125 Displayed: 125 Marked: 0 Load time: 0:00.003 Profile: Default

Wireshark Sniffing with Proxy

log3 [Wireshark 1.6.7]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	fe80::2842:e758:5ff02::1:2	ff02::1:2	DHCPv6	148	Solicit XID: 0xc87fa0 CID: 0001000118376e61a417310
2	1.000662	fe80::2842:e758:5ff02::1:2	ff02::1:2	DHCPv6	148	Solicit XID: 0xc87fa0 CID: 0001000118376e61a417310
3	1.124842	192.168.1.39	192.168.1.1	DNS	76	Standard query A daisy.ubuntu.com
4	1.124859	192.168.1.39	192.168.1.1	DNS	76	Standard query A daisy.ubuntu.com
5	1.152928	192.168.1.1	192.168.1.39	DNS	108	Standard query response A 91.189.95.54 A 91.189.95.54
6	2.584212	192.168.1.19	239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1
7	3.001255	fe80::2842:e758:5ff02::1:2	ff02::1:2	DHCPv6	148	Solicit XID: 0xc87fa0 CID: 0001000118376e61a417310
8	5.153783	192.168.1.39	111.8.55.73	TCP	74	49170 > http [SYN] Seq=0 Win=14600 Len=0 MSS=1460
9	5.404070	192.168.1.39	111.8.55.73	TCP	74	49171 > http [SYN] Seq=0 Win=14600 Len=0 MSS=1460
10	5.584488	192.168.1.19	239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1
11	5.592961	111.8.55.73	192.168.1.39	TCP	66	http > 49170 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0
12	5.593009	192.168.1.39	111.8.55.73	TCP	54	49170 > http [ACK] Seq=1 Ack=1 Win=14720 Len=0
13	5.593127	192.168.1.39	111.8.55.73	HTTP	674	GET http://www.ubuntu.com/index.html HTTP/1.1
14	5.832553	111.8.55.73	192.168.1.39	TCP	66	http > 49171 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0
15	5.832591	192.168.1.39	111.8.55.73	TCP	54	49171 > http [ACK] Seq=1 Ack=1 Win=14720 Len=0
16	6.035253	111.8.55.73	192.168.1.39	TCP	60	http > 49170 [ACK] Seq=1 Ack=621 Win=7168 Len=0
17	7.001775	fe80::2842:e758:5ff02::1:2	ff02::1:2	DHCPv6	148	Solicit XID: 0xc87fa0 CID: 0001000118376e61a417310
18	8.584451	192.168.1.19	239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1
19	10.024020	192.168.1.1	239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1

GET http://www.ubuntu.com/index.html HTTP/1.1\r\n

- [Expert Info (Chat/Sequence): GET http://www.ubuntu.com/index.html HTTP/1.1\r\n
- Request Method: GET
- Request URI: http://www.ubuntu.com/index.html
- Request Version: HTTP/1.1

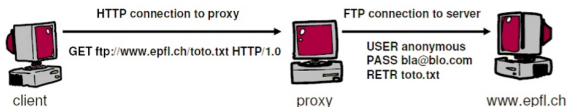
```
0000 40 5a 9b 70 7b 3d d4 be d9 5d b5 b5 08 00 45 00 @Z.p[.=. .]...E.
0010 02 94 2c 6c 40 00 40 06 a3 d7 c0 a8 01 27 6f 08 .,l@.@. ....'o.
0020 37 49 c0 12 00 50 a1 fc a1 13 ad bc 25 1d 50 18 7I...P... ..%.P
0030 00 73 6a a7 00 00 47 45 54 20 68 74 74 70 3a 2f .sj...GE T http/
```

File: "/home/avoine/poubelle/log... Packets: 82 Displayed: 82 Marked: 0 Load time: 0:00:00 Profile: Default

- 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**.

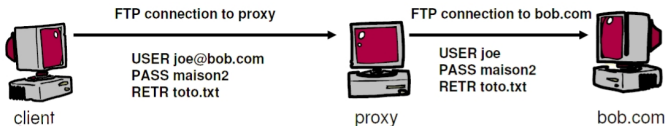


Credit: Ph. Oechslin

- 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 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.

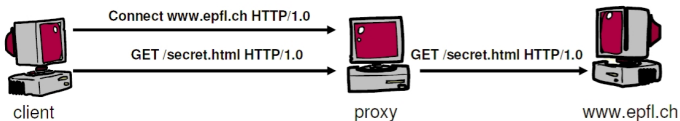
- Just like SMTP, the DNS protocol is used to re-transmit requests from server to server.
- DNS servers can work as proxies.
- DNS servers have a **cache to limit traffic** and **reduce response times**.
- It is a good idea to **configure a DNS proxy to direct all its request towards a bigger server**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

- SOCKS (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 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

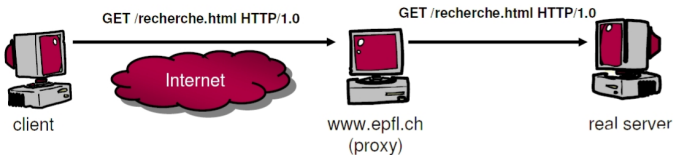
- The **HTTPS proxy** allows relaying any type of protocol (it is transparent, just like SOCKS).
- To limit abuses, the available ports are often limited to **443** (HTTPS) and **563** (SNEWS).
- To allow any protocol to cross a firewall, it is sufficient to run the server on port 443 and **pass through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



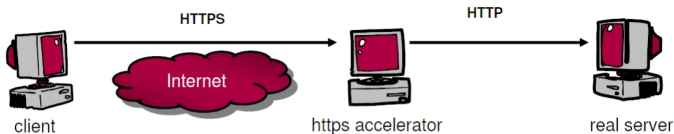
Credit: Ph. Oechslin

- 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 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**.

- 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

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

List of Open Proxies

Free Proxy List - Public Proxy Servers (IP PORT) - Hide My Ass! - Custom search #225390 - Mozilla Firefox

Firefox - Free Proxy List - Public Proxy S...

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**

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