

iPlanet proxy server

Robin 17may2001

Installation.....	1
Normal Proxy setup.....	1
Reverse Proxying setup.....	1
HTTPS reverse proxying setup	1
Proxy refuses to talk to remote site	1
Logging the requested full-qualified hostname in the logs/access file.....	2
Diagnosing reseller_proxy Big Brother alerts	2
Manually testing the proxy.....	2

Installation

NB. Use iPlanet proxy server v3.6 rather than v3.52 if you are going to do HTTPS proxying as it has a more up-to-date set of CA certs in it. For HTTP proxying v3.52 is fine.

Untar the tar file to a temporary location and run ns-setup as normal, install into /usr/netscape/iplanet or wherever. Connect to the admin server on the port you chose at install time.

Create a new proxy server with the following options:

```
run as nobody
no cacheing
never attempt to resolve IP addresses
no ftp or gopher proxying, only http and https
SSL tunneling enabled for https
extended log format
Cache HTTP:  remove tick
Cache FTP:  remove tick
Cache Gopher: remove tick
```

For a lightly-used proxy you can also reduce the number of server Processes from 32 to 8.

Normal Proxy setup

If you want to use the server as a normal proxy, you need do nothing else, you can configure your browser to use it and it will auto-configure your browser.

You can also use wget to test it from the command line:

```
export http_proxy=172.31.4.65
wget -Y on www.ibm.com
```

By default there is one mapping enabled in the URLs section of the admin server: this is the client-browser-autoconfigure mapping .

Reverse Proxying setup

If you want to use the server as a reverse proxy, you should NOT set up any reverse mappings. (!)

Delete the browser-autoconfig mapping, then go to the Virtual Multihosting option of the URL section and add entries for each site you want to reverse proxy:

```
Source hostname: www
Source domain name: ignite.com
Destination URL prefix: http://www.ignite.com
Template: NONE
```

If you run the reverse proxy server on port 80, you can then change the /etc/hosts file on each client to map the destination URLs you want to proxy, to the proxy's IP address:

```
172.31.4.65 www.ignite.com www.panties.com www.erdas.com www.mac.fr
```

HTTPS reverse proxying setup

This is the same as reverse proxying above, but you also need to enable encryption for the proxy server, i.e. get a Certificate for it as you would for a web server.

Then if you run the reverse proxy HTTPS server on port 443, the client will talk https to the proxy server, which will talk server-to-server https to the destination site.

Proxy refuses to talk to remote site

This can happen in two ways :

a) you get an error message in your browser like

“Proxy denies fulfilling the request

The proxy's access control configuration denies access to the requested object through this proxy.”

In this case you haven't added an entry for that site in the Virtual Multihosting page

b) If you cannot connect to an HTTPS site, check the logs/errors file

If you ever get the following message in the logs/errors file :

```
[24/May/2001:15:25:33] failure: for host 192.168.60.1 trying to GET /, retrieve-
exit-routine reports: proxy retrieve failed: The certificate issuer for this ser
ver is not recognized by Netscape. The security certificate may or may not be va
lid. Netscape refuses to connect to this server
```

this means that the site the proxy is trying to connect to has a Server Cert which is signed by a CA which is not recognised by Netscape Proxy (i.e. there is no Cert for that CA in the Netscape Proxy admin server's certificate database).

You will need to get that CA Cert. To do this, connect to the offending site with a browser and view the Server cert. It should show the Issuer, there should hopefully be an e-mail address or web site for that issuing CA: contact them and get their CA cert. You will need e.g. a server cert, Class 2 CA, and you will need it in PEM format so that Netscape Proxy can read it.

Install that cert in the Netscape Proxy admin server, and restart the admin and the proxy servers: connection to the offending site should now work! If not, you will have to blame it on someone else.. J

Logging the requested full-qualified hostname in the logs/access file

By default the Proxy will not log the name of the site that the client is requesting (which is contained in the Host: portion of the client's HTTP header).

To start logging it, select Custom format and add %Req->headers.host%

Diagnosing reseller_proxy Big Brother alerts

If you receive a Big Brother reseller_proxy alert, the alert should contain the name of a log file which will give you more details, e.g.

```
ERROR: priority:2 Yellow : McMillen not found from https://www.mac.de/po.asp : see
jupiter:/opt/bb/getw_logs/https://www.mac.de/po.asp/200105311012.log
```

You can look in the log file to see what errors may have occurred.

the .log file mentioned in the alert contains the HTTP headers received from the remote server :

```
HTTP/1.1 200 OK
Server: Microsoft-IIS/4.0
Date: Thu, 31 May 2001 09:59:37 GMT
Status: 401
Connection: Keep-Alive
Content-length: 309
Content-type: text/html
Expires: Mon, 01 Jan 2001 00:00:00 GMT
Cache-control: private
```

There should also be a file with the same name but without the .log extension: this is the HTML retrieved from the server :

```
bb@jupiter> more /opt/bb/getw_logs/https://www.mac-online.de/po.asp/200105311012
<html><head><title>Error 401</title><meta name="robots" content="noindex"></head><body><h2>HTTP Error
401</h2><p><strong>401 Unauthorised</strong></p><p>You are not authorised to access this
resource</p><p>Please contact <a href="mailto:mcmill@hse.com"> McMillen</a> for
assistance.</p></body></html>
```

Although this appears to be an Error it is a successful result ! (it contains Mr McMillen's name)

Manually testing the proxy

You can manually test the proxy by using wget or curl from the command line on any machine which has all had its /etc/hosts file modified to map www.mac.nl, www.warehouse.co.uk, etc. to use the proxy's IP address):

NB You should test the HTTP proxy separately from the HTTPS proxy (as there are two processes running on starsky) :

e.g. Testing the HTTP proxy using wget : here is a successful result :

```
bob@rowan > wget -O- www.mac.nl/po.asp
--11:23:15-- http://www.mac.nl:80/po.asp
=> `-'
Connecting to www.mac.nl:80... connected!
HTTP request sent, awaiting response... 200 OK
Length: 309 [text/html]
OK -> [100%]
```

```
<html><head><title>Error 401</title><meta name="robots" content="noindex"></head><body><h2>HTTP Error
401</h2><p><strong>401 Unauthorised</strong></p><p>You are not authorised to access this
resource</p><p>Please contact <a href="mailto:mcmill@hse.com">McMillen</a> for
assistance.</p></body></html>11:23:16 (4.79 KB/s) - '-' saved [309/309]
```

Testing the HTTPS proxy with curl (wget doesn't talk HTTPS. NB curl is only on jupyter) : here is a successful result :

```
bb @ jupyter > curl -i https://www.mac.nl/po.asp
HTTP/1.1 200 OK
Server: Microsoft-IIS/4.0
Date: Thu, 31 May 2001 11:17:52 GMT
Status: 401
Connection: Keep-Alive
Content-length: 309
Content-type: text/html
Expires: Mon, 01 Jan 2001 00:00:00 GMT
Cache-control: private
```

```
<html><head><title>Error 401</title><meta name="robots" content="noindex"></head><body><h2>HTTP Error
401</h2><p><strong>401 Unauthorised</strong></p><p>You are not authorised to access this
resource</p><p>Please contact <a href="mailto:mcmill@hse.com">McMillen</a> for
assistance.</p></body></html>
```

If the above tests fail you will need to log on to starsky and view the access/errors logs for the two proxy servers :
for the HTTPS proxy v3.6 : /usr/netscape/iplanet/proxy-rev-sec/logs
for the HTTP proxy v3.5 : /usr/netscape/suitespot/proxy-reverse/logs