การใช้งาน Reverse Proxy โดย Squid Proxy เบื้องต้น

คมกริช คำสวัสดิ์
วิศวกรความมั่นคงปลอดภัยสารสนเทศอาวุโส
สำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน)

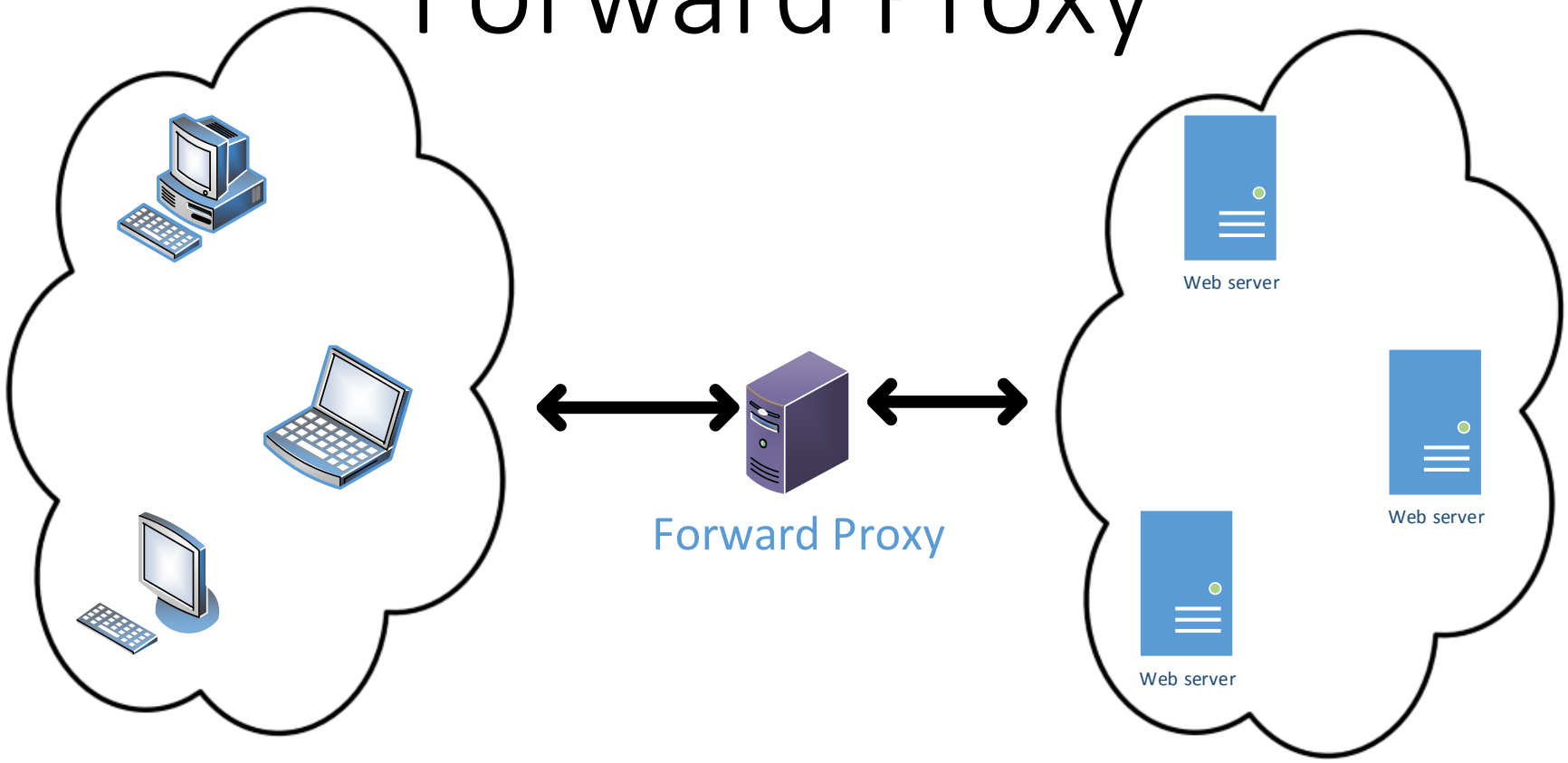
Proxy

http://en.wikipedia.org/wiki/Proxy_server

*In computer networks, a **proxy server** is a server (a computer system or an application) that acts as an intermediary for requests from clients seeking resources from other servers. A client connects to the proxy server, requesting some service, such as a file, connection, web page, or other resource available from a different server and the proxy server evaluates the request as a way to simplify and control its complexity. Proxies were invented to add structure and encapsulation to distributed systems.*

Forward Proxy
vs
Reverse Proxy

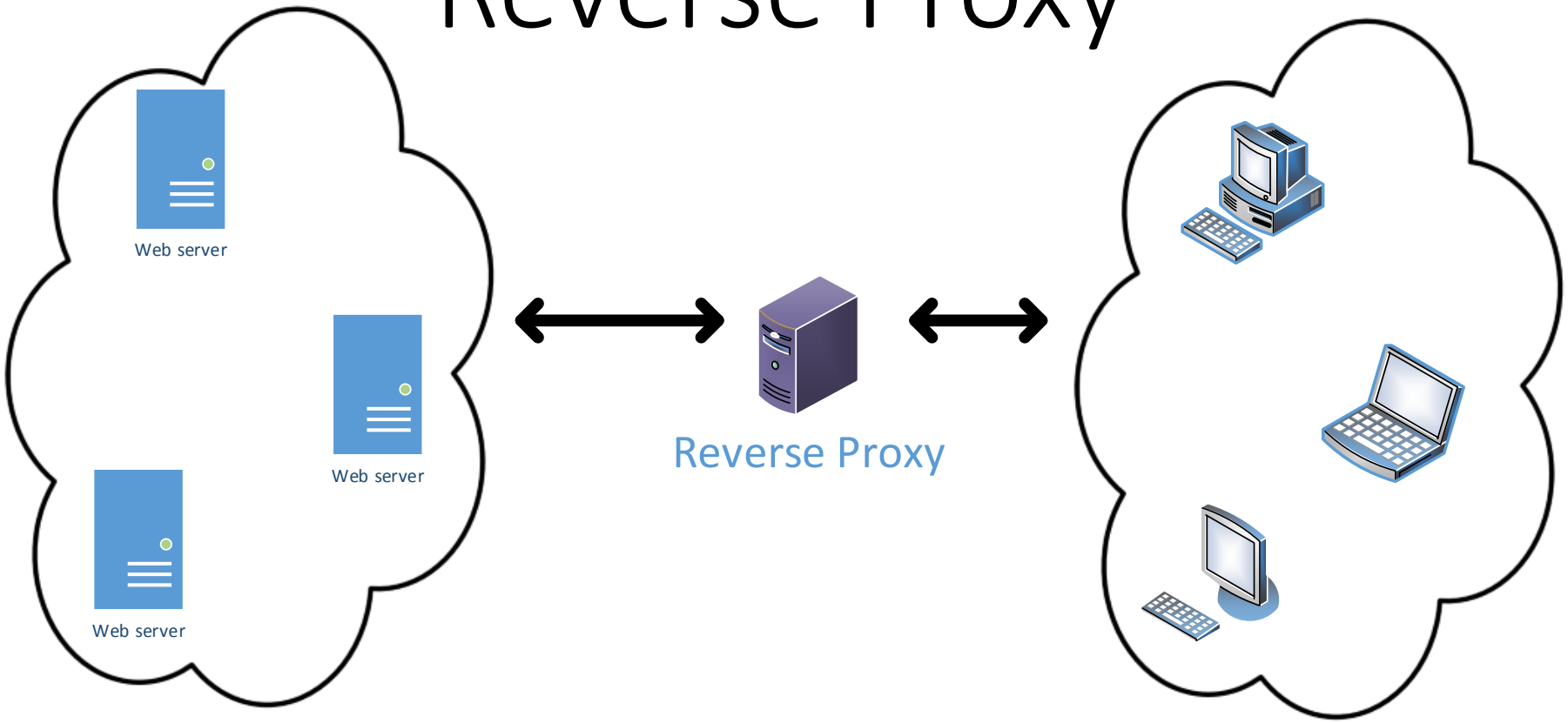
Forward Proxy



Internal users

Web servers

Reverse Proxy



Internal Web servers

External users

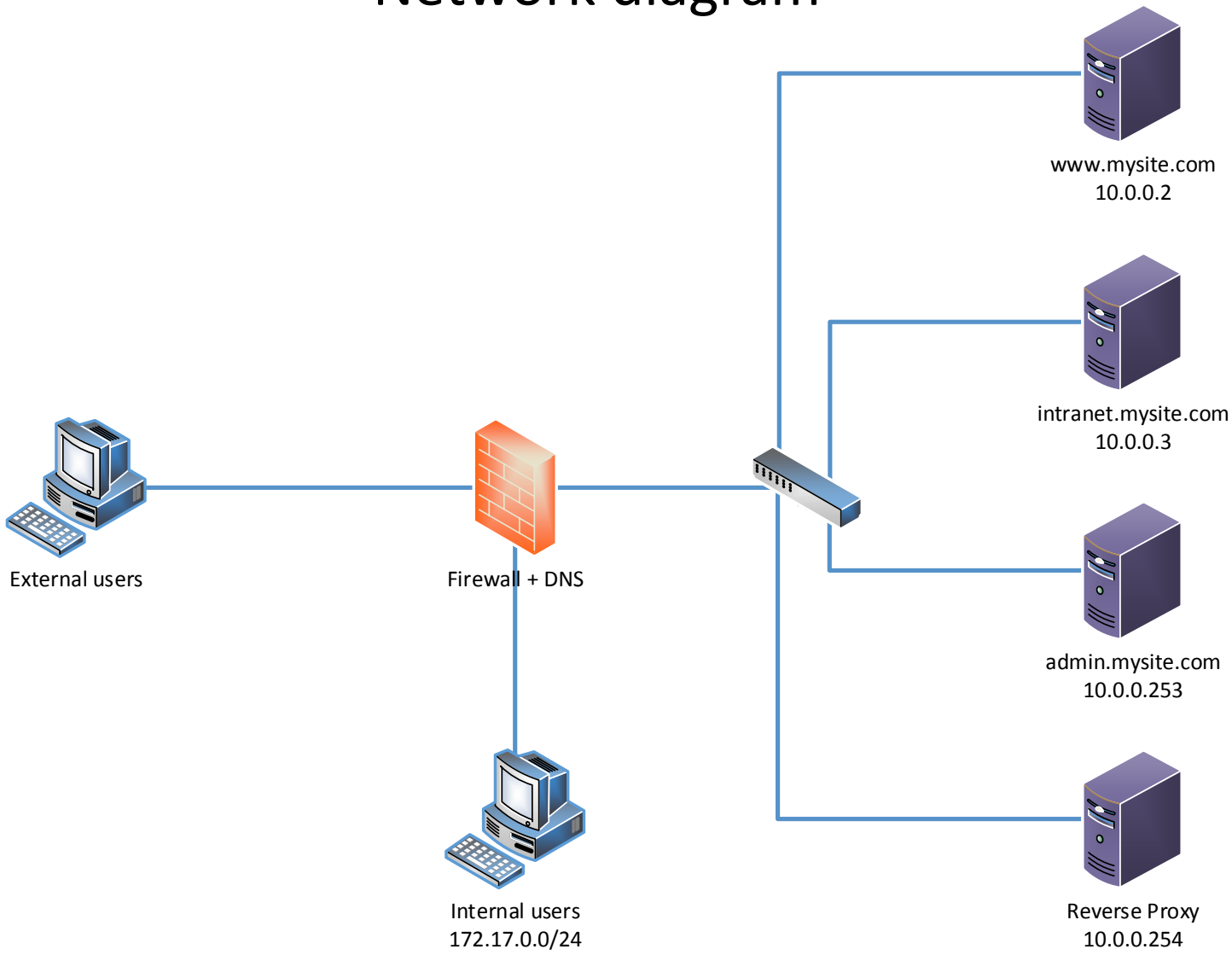
ประโยชน์ของ Reverse Proxy

1. Creates a single point of access to your file transfer servers
2. Simplifies access control tasks
3. Reduces risks to sensitive data
4. Helps achieve regulatory compliance
5. Allows transparent maintenance of backend servers
6. Enables load balancing and failover

ref. http://www.jscape.com/blog/bid/87841/Top-8-Benefits-of-a-Reverse-Proxy

การติดตั้ง Squid Proxy เพื่อเป็น Reverse Proxy

Network diagram



รายการ Software ที่ใช้ในการทำ Reverse proxy

Operating system:	**CentOS 6.6**
Website:	http://www.centos.org/
Proxy service:	**Squid proxy**
Website:	http://www.squid-cache.org/

การติดตั้ง การตรวจสอบ Version และการตรวจสอบการทำงานของ Squid

- การติดตั้ง Squid

```
[root@ReverseProxy ~]#  yum -y install squid
```

- การตรวจสอบ Version ของ Squid

```
[root@ReverseProxy ~]#  rpm -qa | grep squid
squid-3.1.10-29.el6.i686
```

- การกำหนดให้ Squid ทำงานเมื่อมีการ Reboot เครื่อง

```
[root@ReverseProxy ~]#  chkconfig squid on
```

การสั่ง Start, Stop, Restart และตรวจสอบสถานะการทำงานบริการ Proxy

```
[root@ReverseProxy ~]# service  squid  start
Starting squid: .                          [  OK  ]

[root@ReverseProxy ~]# service  squid  stop
Stopping squid: ......                     [  OK  ]

[root@ReverseProxy ~]# service  squid  restart
Stopping squid: ..                         [  OK  ]
Starting squid: .                          [  OK  ]

[root@ReverseProxy ~]# service  squid  status
squid (pid  1148) is running...
```

การ Configure ระบบ Reverse Proxy

- ตำแหน่งไฟล์ Configuration

/etc/squid/squid.conf

- ตำแหน่งในการจัดเก็บ Logs ของ Squid

/var/log/squid/access.log สำหรับ logs การเข้าใช้งาน

/var/log/squid/cache.log สำหรับ logs การทำงานของ Squid

- คำสั่งในการ Apply configuration

[root@ReverseProxy ~]# ***squid -k reconfigure***

การกำหนดค่าทั่วไปของ Squid

```
cache_mgr   admin@mysite.com
visible_hostname  ReverseProxy
http_port  80  vhost
forwarded_for  on
emulate_httpd_log  on
access_log  /var/log/squid/access.log
cache_log /var/log/squid/cache.log
cache_store_log  none
shutdown_lifetime  1  seconds
```

การสร้าง Network acl และการ Deny การใช้งาน HTTP method ที่ไม่จำเป็น

```
### Define network lists
acl localhost  src  127.0.0.1/32  ::1
acl  src_allow  src  172.17.0.0/24

### Deny some methods.
acl  mt_HEAD  method  HEAD
http_access  deny  mt_HEAD
acl  mt_OPTIONS  method  OPTIONS
http_access  deny  mt_OPTIONS
```

การป้องกันการเข้าถึง URL ที่ไม่อนุญาต หรือ URL ที่มีความเสี่ยง

```
### Deny bad URL.
acl  deny_url  url_regex  -i  "/etc/squid/deny_url.txt"
http_access  deny  !src_allow deny_url
```

"/etc/squid/deny_url.txt"

phpmyadmin

administrator

passwd

shadow

\/etc

\/var

\/bin

Windows

system32

.conf

.cfg

or\ 1\=1

\‘or\ 1\=1

การกำหนดค่า Reverse Proxy

Reverse proxy.

```
cache_peer 10.0.0.2 parent 80 0 no-query originserver name=mysite
acl reverse_mysite.com dstdomain mysite.com www.mysite.com 10.0.0.254

http_access allow reverse_mysite.com

cache_peer_access mysite allow reverse_mysite.com
cache_peer_access mysite deny all
```

การกำหนดค่า Reverse Proxy

```
### Reverse proxy.

## Intranet
cache_peer  10.0.0.3  parent  80  0  no-query  originserver  name=intranet
acl reverse_intranet  dstdomain  intranet.mysite.com

http_access  allow  reverse_intranet

cache_peer_access  intranet  allow  reverse_intranet
cache_peer_access  intranet  deny   all
```

การกำหนดค่า Reverse Proxy

```
### Reverse proxy.

## admin.mysite.com
cache_peer 10.0.0.253 parent 80 0 no-query originserver name=admin-mysite-com
acl reverse_admin-mysite-com dstdomain admin.mysite.com

http_access allow reverse_admin-mysite-com

cache_peer_access admin-mysite-com allow reverse_admin-mysite-com
cache_peer_access admin-mysite-com deny all
```

การกำหนดหน้าเพจสำหรับ URL ที่ถูก Deny

```
### Deny bad URL.
acl deny_url url_regex  -i  "/etc/squid/deny_url.txt"
http_access  deny  !src_allow deny_url

### Denied to page.
deny_info  http://admin.mysite.com/404.html  deny_url
```

การกำหนดหน้าเพจสำหรับ URL ที่ไม่ต้องการให้เข้าถึงได้

Landing page.

```
acl  restrict_url url_regex  -i  "/etc/squid/restrict_url.txt"
http_access  deny  restrict_url
deny_info  http://admin.mysite.com/underconstruction.html  restrict_url
```

/etc/squid/restrict_url.txt

http://intranet.mysite.com/hr

การกำหนดหน้าเพจสำหรับ URL ที่เกิด Error

redirect for TCP_404

```
acl  denied_status_404  http_status  404
deny_info  http://admin.mysite.com/404.html  denied_status_404
http_reply_access  deny  denied_status_404
```

การกำหนดค่าด้านความปลอดภัยอื่นๆ

Another security issues.

```
via  off
reply_header_access  X-Cache-Lookup  deny  all
reply_header_access  X-Squid-Error  deny  all
reply_header_access  X-Cache  deny  all
reply_header_access  Server  deny  all
```

Reverse Proxy + IPv6

```
cache_peer  10.0.0.2  parent  80  0  no-query  originserver  name=mysite
acl reverse_mysite.com dstdomain mysite.com www.mysite.com 10.0.0.254 2401:9d00::a:b

http_access  allow  reverse_mysite.com

cache_peer_access  mysite  allow  reverse_mysite.com
cache_peer_access  mysite  deny all
```

Squid logs: /var/log/squid/access.log

192.168.38.1 - - [13/Aug/2014:02:02:47 +0700] "GET http://www.mysite.com/ HTTP/1.1" 200 2647 TCP_MISS:FIRST_UP_PARENT

192.168.38.1 - - [13/Aug/2014:02:03:57 +0700] "GET http://www.mysite.com/administrator HTTP/1.1" 302 202 TCP_DENIED:NONE

192.168.38.1 - - [13/Aug/2014:02:03:57 +0700] "GET http://admin.mysite.com/404.html HTTP/1.1" 200 346 TCP_MISS:FIRST_UP_PARENT

172.17.0.200 - - [13/Aug/2014:02:16:11 +0700] "GET http://www.mysite.com/phpmyadmin/ HTTP/1.1" 200 3556 TCP_MISS:FIRST_UP_PARENT

172.17.0.200 - - [13/Aug/2014:02:16:11 +0700] "GET http://www.mysite.com/phpmyadmin/phpmyadmin.css.php? HTTP/1.1" 200 17545 TCP_MISS:FIRST_UP_PARENT

172.17.0.200 - - [13/Aug/2014:02:16:11 +0700] "GET http://www.mysite.com/phpmyadmin/js/get_image.js.php? HTTP/1.1" 200 6589 TCP_MISS:FIRST_UP_PARENT

Squid + IPv6 logs: /var/log/squid/access.log

2401:9d00:1:1::12:4305 - - [12/Aug/2014:13:18:22 +0700] "GET http://www.somewhere.go.th/personnel_04.png HTTP/1.1" 200 13335 TCP_MISS:FIRST_UP_PARENT

2401:9d00:1:1::12:4305 - - [12/Aug/2014:13:18:22 +0700] "GET http://www.somewhere.go.th/org/tmd_org.png HTTP/1.1" 200 14763 TCP_MISS:FIRST_UP_PARENT

2001::1:be30:5bff:feda:57ec - - [12/Aug/2014:14:34:22 +0700] "GET http://[**2401:9d00::67**]/ HTTP/1.1" 200 2694 TCP_MISS:FIRST_UP_PARENT

Squid logs: /var/log/squid/cache.log

2014/08/13 02:10:58| Starting Squid Cache version 3.1.10 for x86_64-redhat-linux-gnu...

2014/08/13 02:10:58| Process ID 1342

2014/08/13 02:10:58| With 1024000 file descriptors available

2014/08/13 02:10:58| Initializing IP Cache...

2014/08/13 02:10:58| DNS Socket created at [::], FD 7

2014/08/13 02:10:58| DNS Socket created at 0.0.0.0, FD 8

2014/08/13 02:10:58| Adding domain localdomain from /etc/resolv.conf

2014/08/13 02:10:58| Adding nameserver 10.0.0.1 from /etc/resolv.conf

2014/08/13 02:10:58| User-Agent logging is disabled.

2014/08/13 02:10:58| Referer logging is disabled.

2014/08/13 02:10:59| Unlinkd pipe opened on FD 13

2014/08/13 02:10:59| Local cache digest enabled; rebuild/rewrite every 3600/3600 sec

2014/08/13 02:10:59| Store logging disabled

Squid logs: /var/log/squid/cache.log

2014/08/13 02:10:59| Swap maxSize 0 + 262144 KB, estimated 20164 objects

2014/08/13 02:10:59| Target number of buckets: 1008

2014/08/13 02:10:59| Using 8192 Store buckets

2014/08/13 02:10:59| Max Mem size: 262144 KB

2014/08/13 02:10:59| Max Swap size: 0 KB

2014/08/13 02:10:59| Using Least Load store dir selection

2014/08/13 02:10:59| Current Directory is /

2014/08/13 02:10:59| Loaded Icons.

2014/08/13 02:10:59| Accepting accelerated HTTP connections at [::]:80, FD 14.

2014/08/13 02:10:59| HTCP Disabled.

2014/08/13 02:10:59| Configuring Parent 10.0.0.2/80/0

2014/08/13 02:10:59| Configuring Parent 10.0.0.3/80/0

2014/08/13 02:10:59| Configuring Parent 10.0.0.253/80/0

2014/08/13 02:10:59| Squid plugin modules loaded: 0

2014/08/13 02:10:59| Adaptation support is off.

2014/08/13 02:10:59| Ready to serve requests.


G-CERT
by EGA