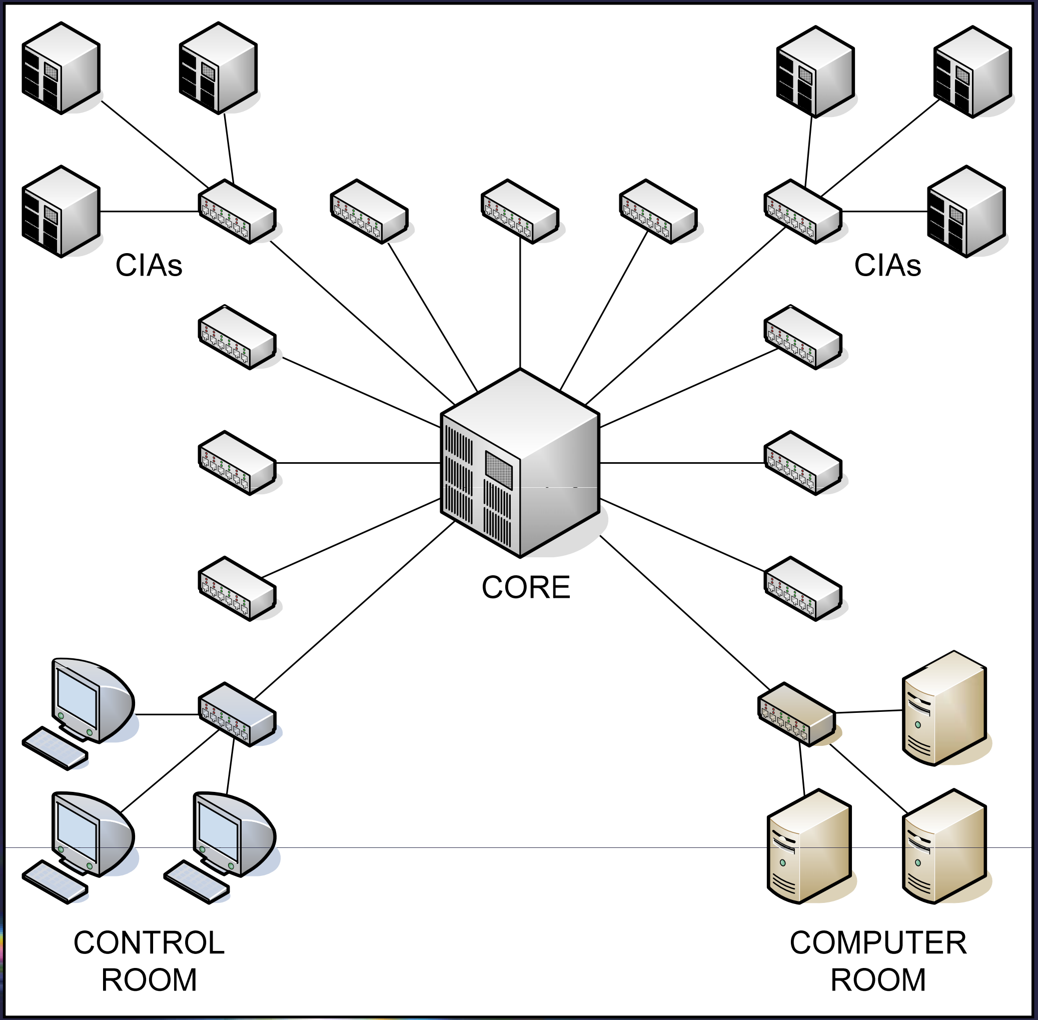
# Accelerator Control-System Network Security
# @
# Diamond Light Source

Mike Leech, Controls Group Computer Systems Manager

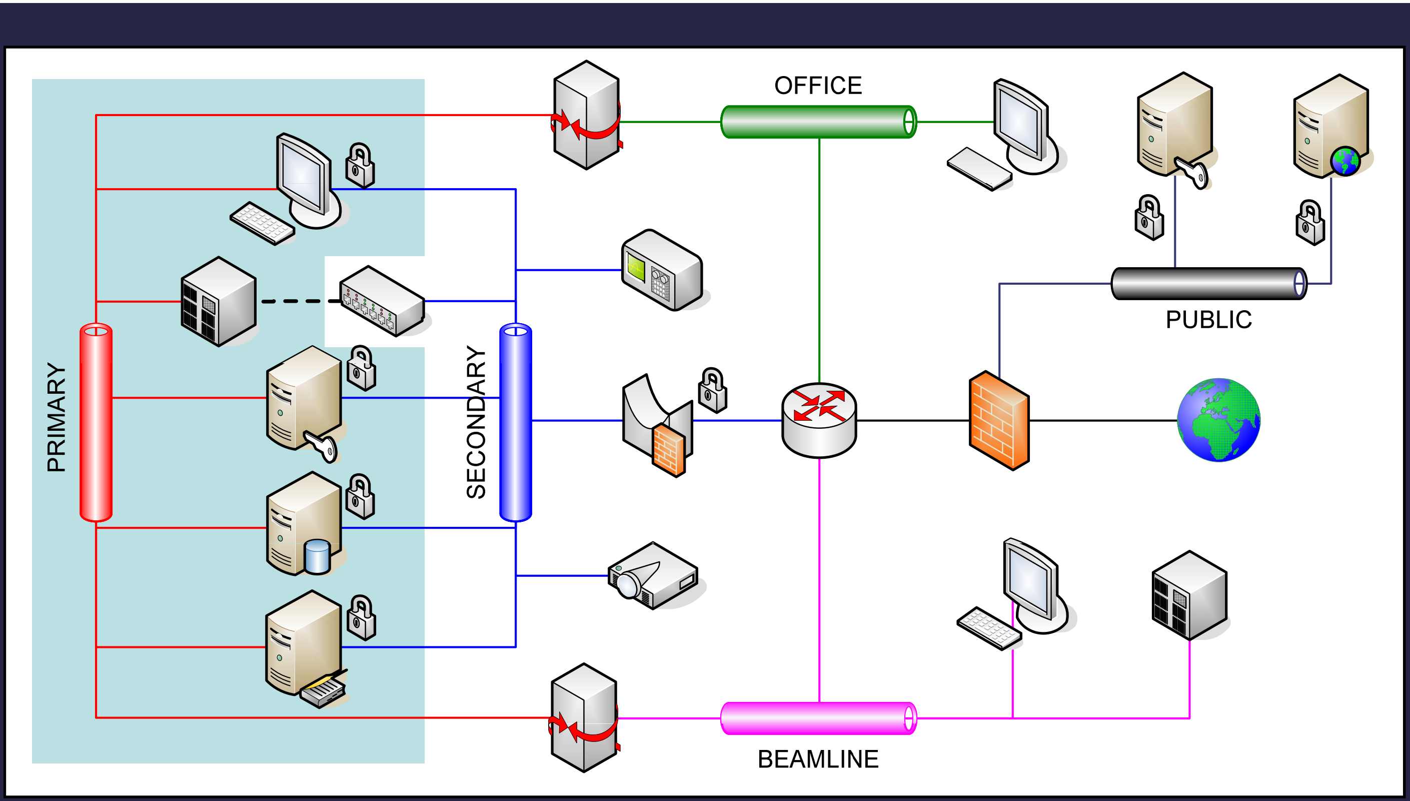
diamond

# “Dream Accelerator Controls Network?”



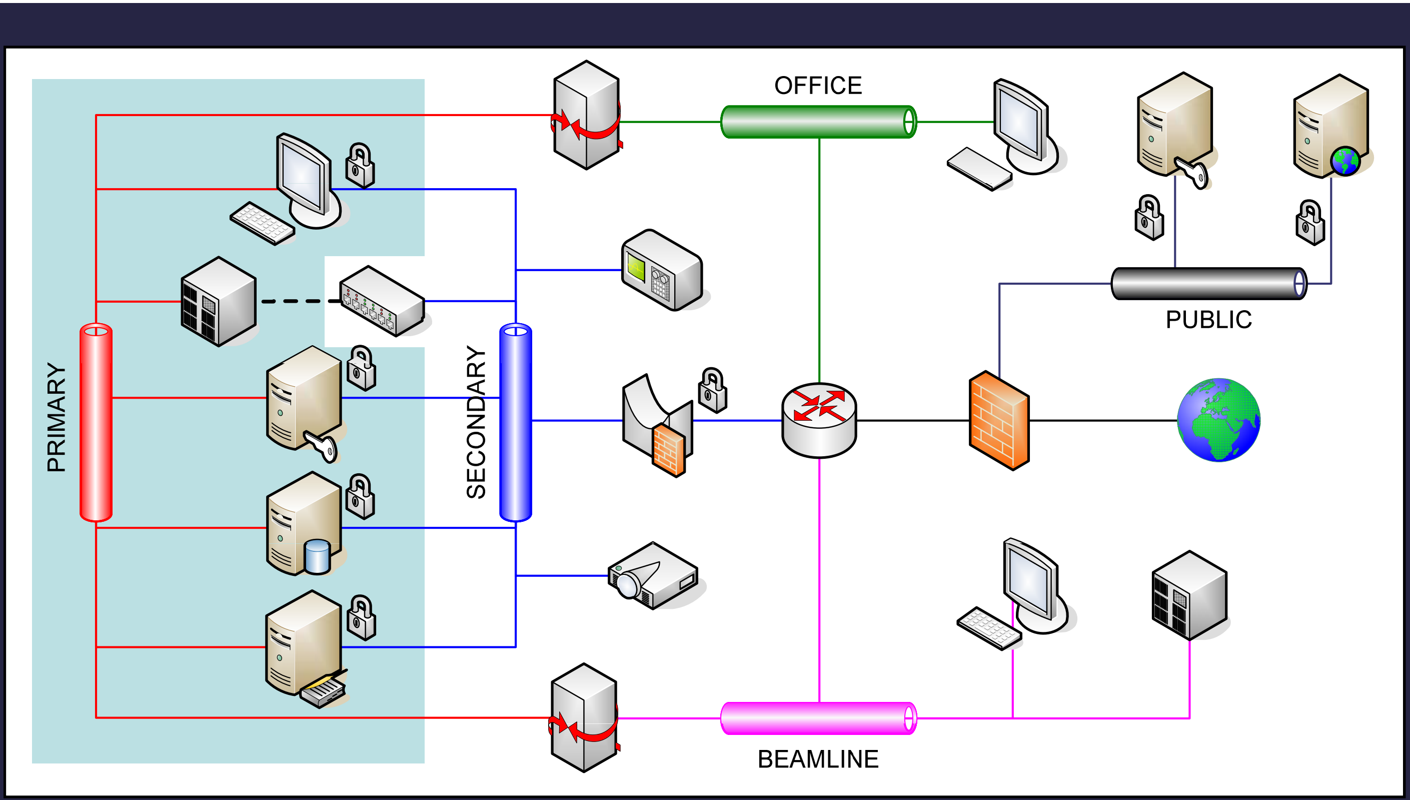
- ++ Isolated
- + No routing, Layer 2 only – Easy configuration and hardware replacement
- + Simple “Star” network – no daisy-chaining
- + Cheap

- - No diverse routes for fibres
- - No automatic hardware failover



## Primary Network:

- All EPICS control traffic
- Only primary network needed to run machine. All services contained within – DNS, NFS, NTP, IOC boot (FTP), Parameter archiving etc.

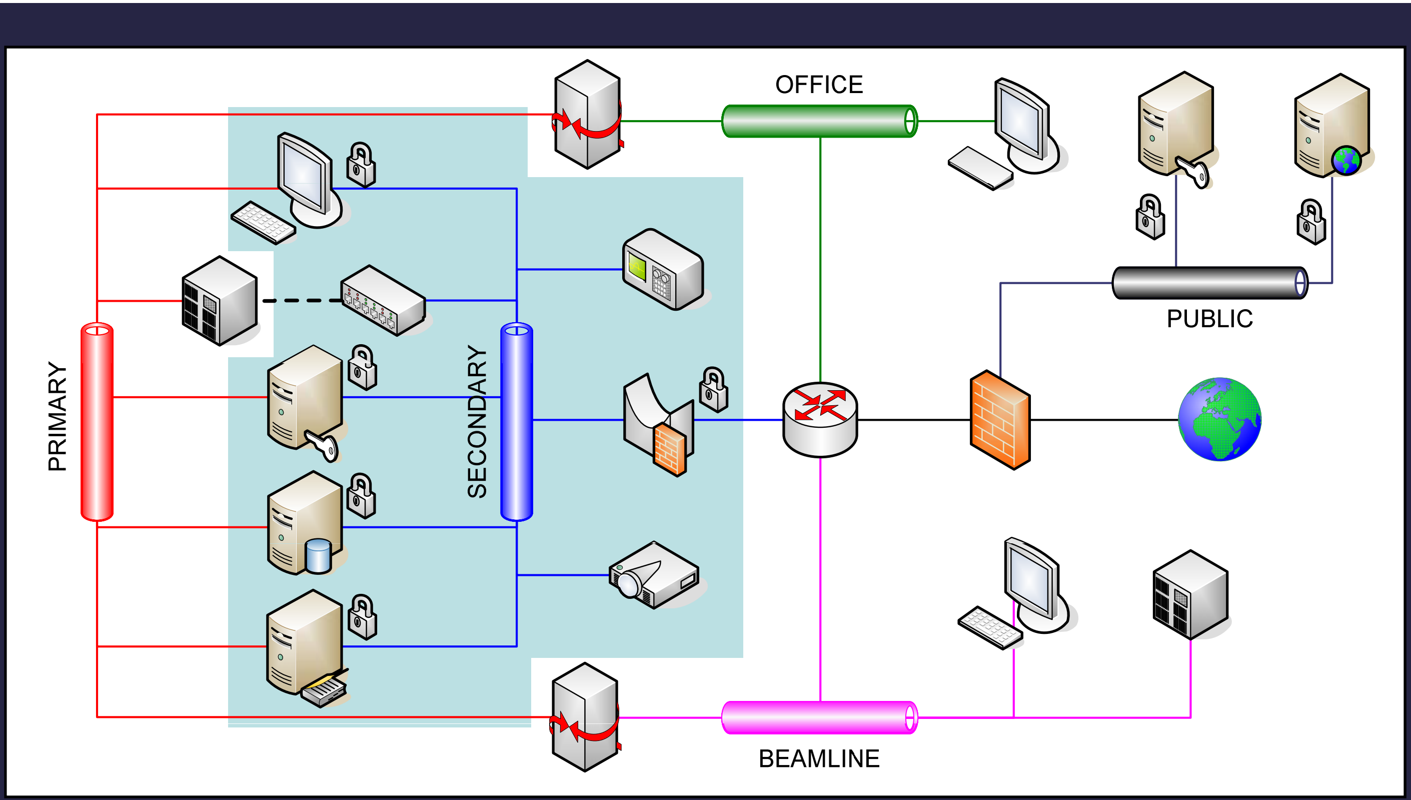


**Devices on the Primary Network:**

| | | |
|---|---|---|
| 16 Linux Servers | 11 Linux CA Gateways | 45 Linux Workstations |
| 298 VxWorks IOCs | 222 Linux BPMs | 4 Windows PCs |

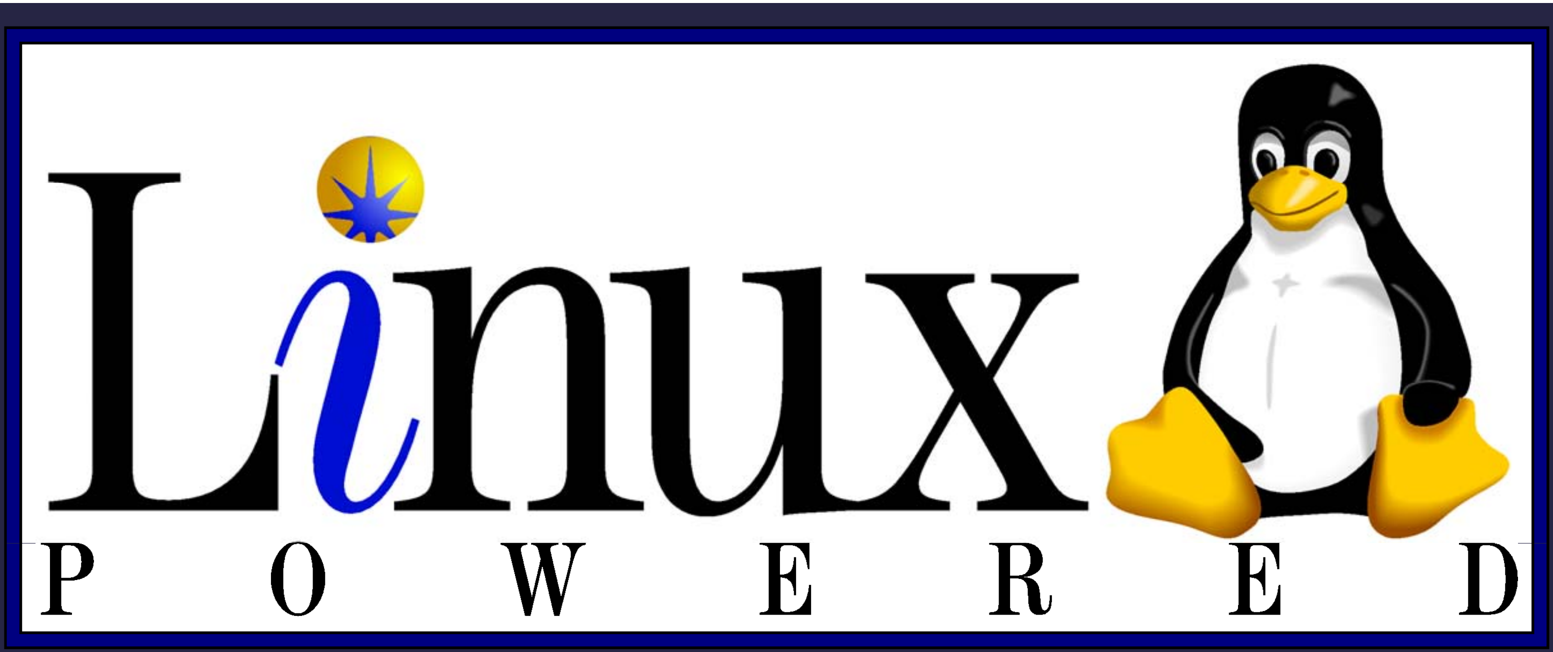
40 Linux/Windows Laptops 6 Other!!! (Atomic Clock, GPIB adapter, etc)

0 PLCs!!! (All PLCs hang off private networks on IOC second interface)

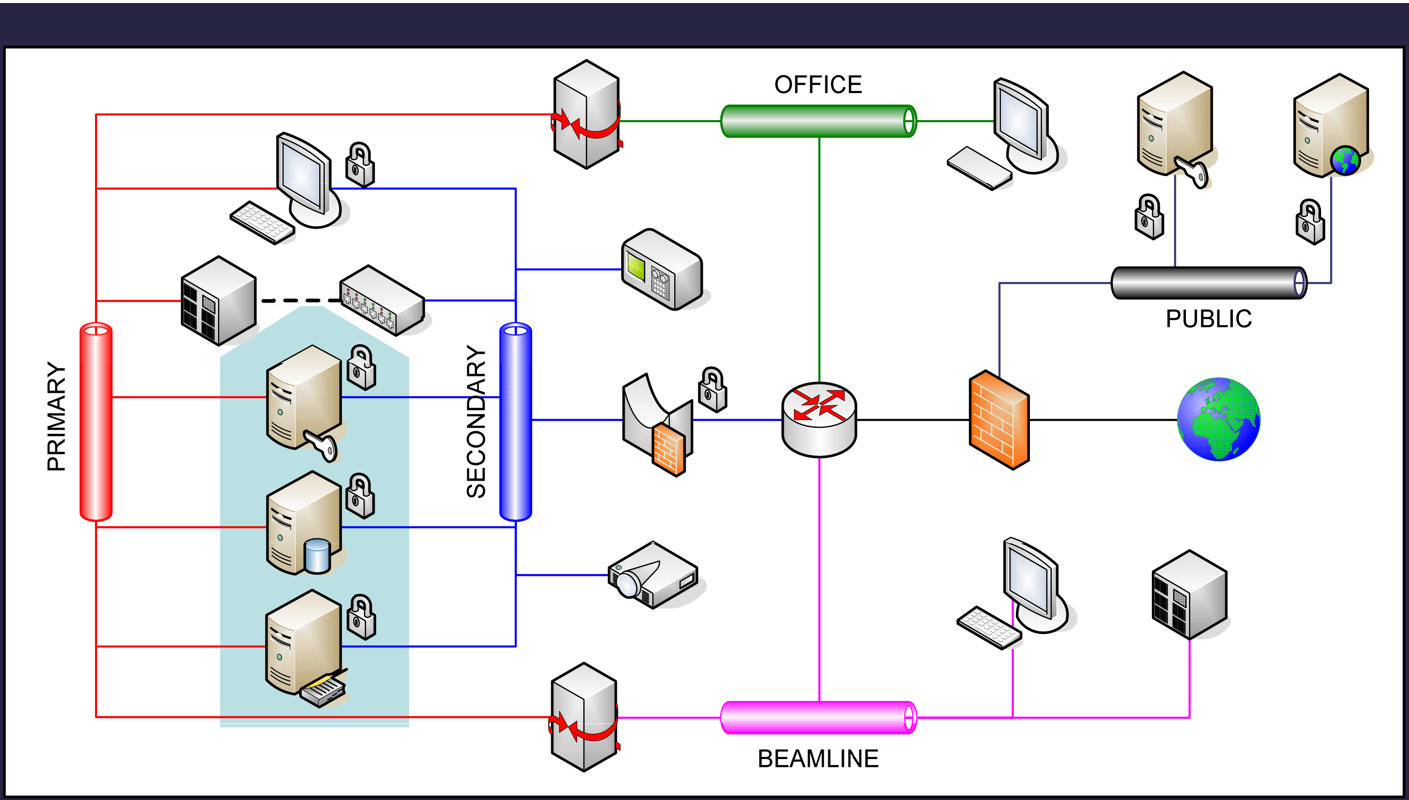


## Secondary Network:

- All non EPICS traffic and traffic not essential to machine operation
- Video cameras, scopes, terminal servers, IP phones, pump carts, residual gas analysers, printers etc.
- Nearly identical to primary network except, routed to allow access to dual homed servers and workstations.

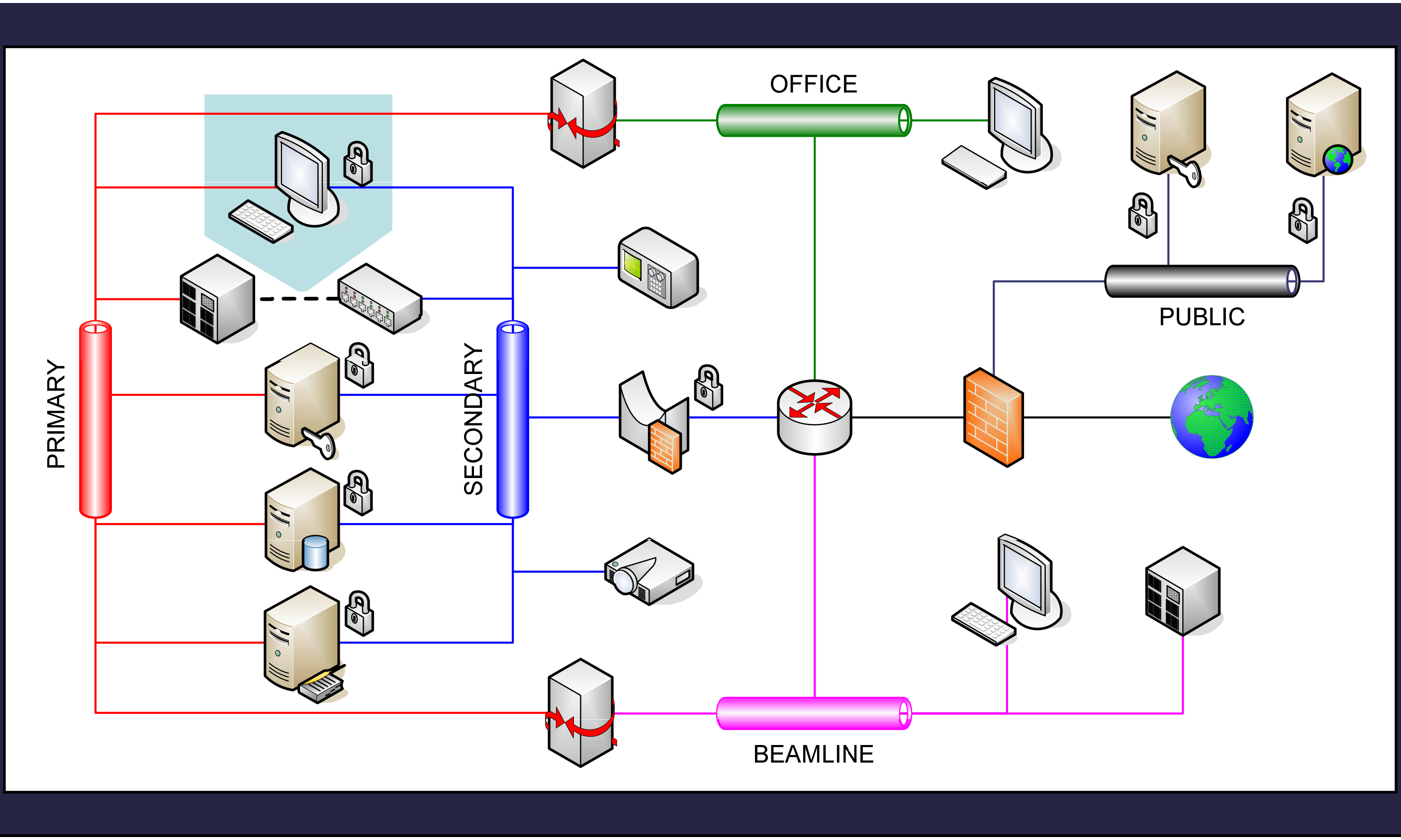


- Powerful security tools “out-of-the-box”: Iptables stateful firewall, tcpwrappers (hosts.allow), SSH encrypted login shell (copying, tunnelling and more).
- Open Source: Security flaws discovered and patched quickly.
- Secure services: VSFTP, Apache, SELinux Jail.
- Total control over system configuration – rebuild your own kernel.
- Security through obscurity: Less of a target for viruses and worms.
- No “Power Users” unless you configure elevated rights



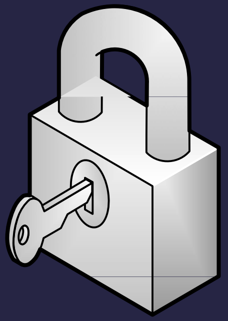
## Dual Homed Servers:

- SSH Bastion: Allows remote access during shutdown and emergency remote access during operation to fix faults
- EPICS Channel Access archiver: Allows office access to archived data.
- Bootserver: Allows office read-only access to software (3.14).
- Relational Database: Allows access to ELog, cable schedules etc



# Diamond Control Room

diamond



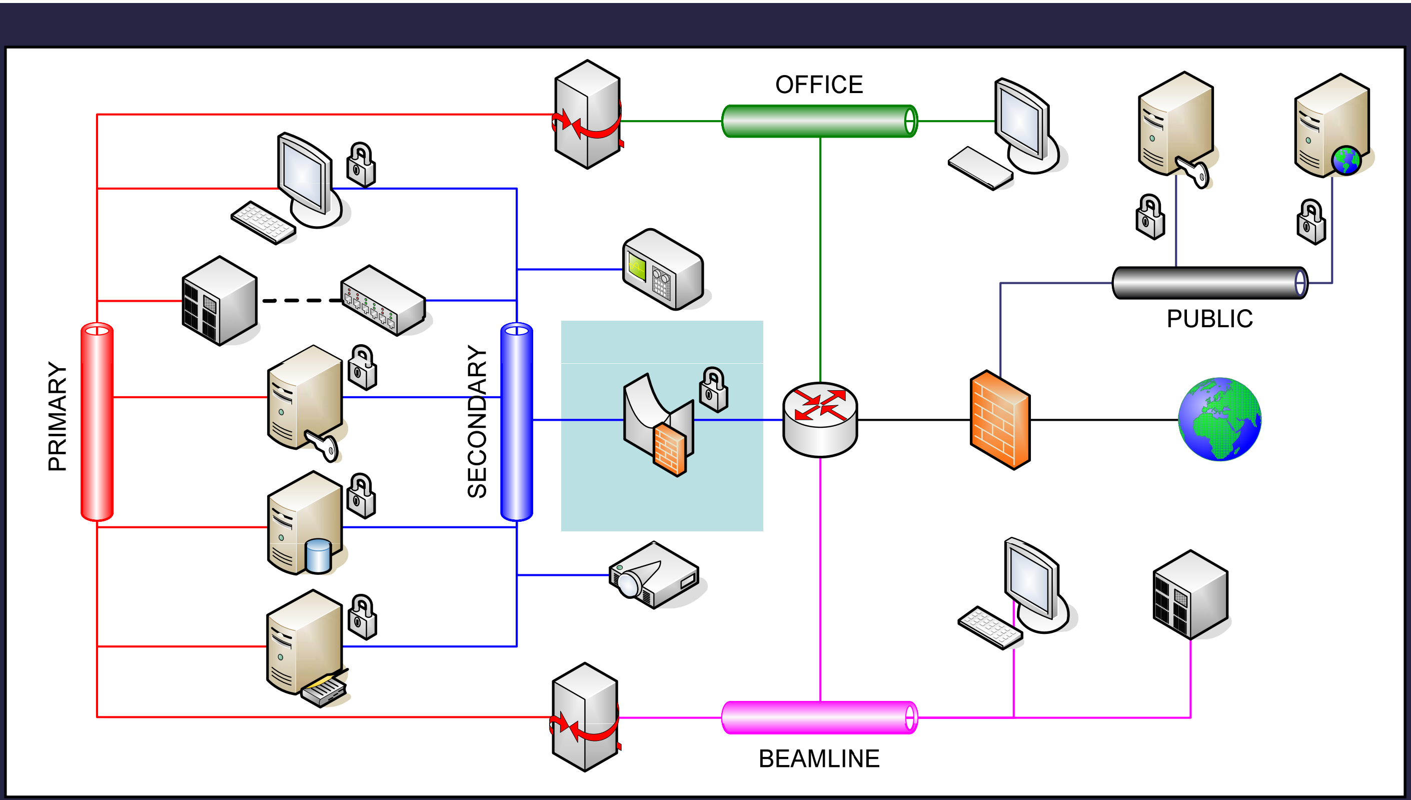
**Physical Access:**

Network access points are restricted to the following locations:

- Control and instrumentation areas (CIAs).
- Linac, booster and storage ring tunnels.
- Computer room.
- Control room.
- Comms rooms.
- NO labs or offices.
- NO wireless.

All these areas are under access control.

diamond



## Bridging (Stealth) firewall:

Close down both interfaces:

```
> ifdown eth0; ifdown eth1
> ifconfig eth0 0.0.0.0
> ifconfig eth1 0.0.0.0
```

Create a bridge:

```
> brctl addbr br0
```

Add both interfaces:

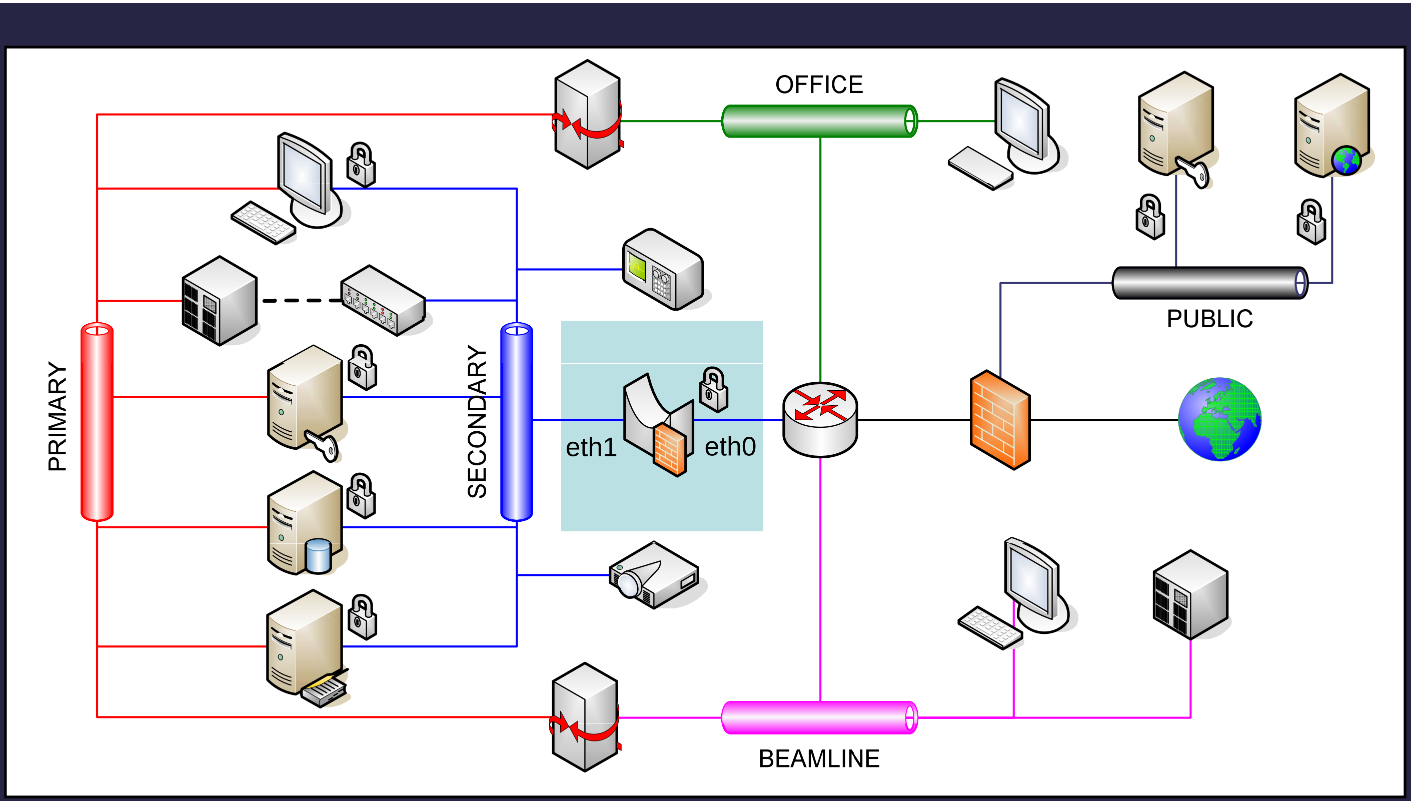
```
> brctl addif br0 eth0
> brctl addif br0 eth1
```

Turn on IP forwarding:

```
> echo 1 > /proc/sys/net/ipv4/ip_forward
```

Configure management interface:

```
> ifconfig br0 172.23.0.1 netmask 255.255.255.0 up
```



## Iptables firewall:

```
> iptables -F
> iptables -P FORWARD DROP
> iptables -P INPUT DROP; IPTABLES -P OUTPUT DROP
> iptables -A INPUT -i lo ACCEPT; iptables -A OUTPUT -o lo ACCEPT
```

Restrict by interface:

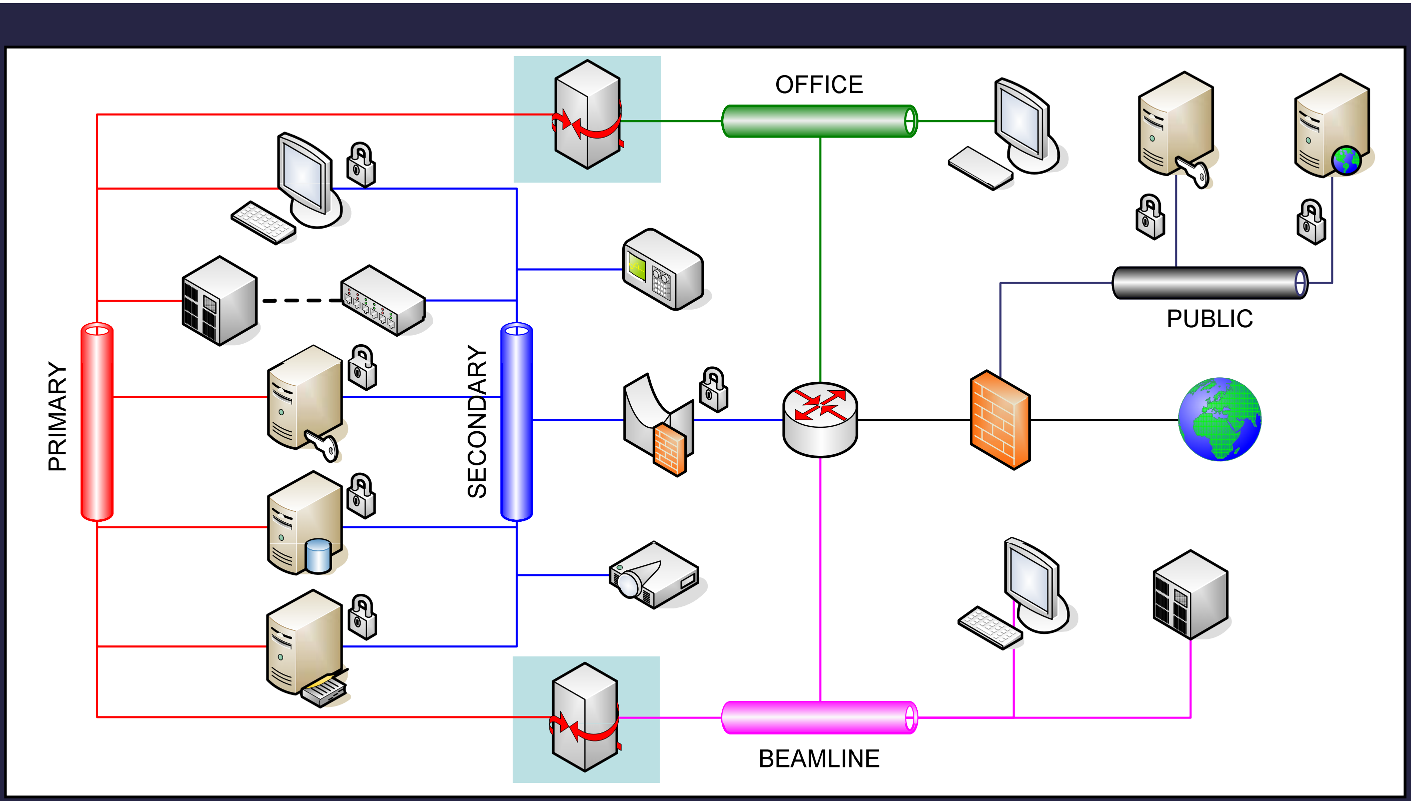
```
> iptables -A FORWARD -i eth1 -o eth0 -p tcp --dport 22 -j ACCEPT
```

Restrict by IP address range:

```
> iptables -A FORWARD --destination 172.23.0.0/16 -p udp --dport 53 -j ACCEPT
```

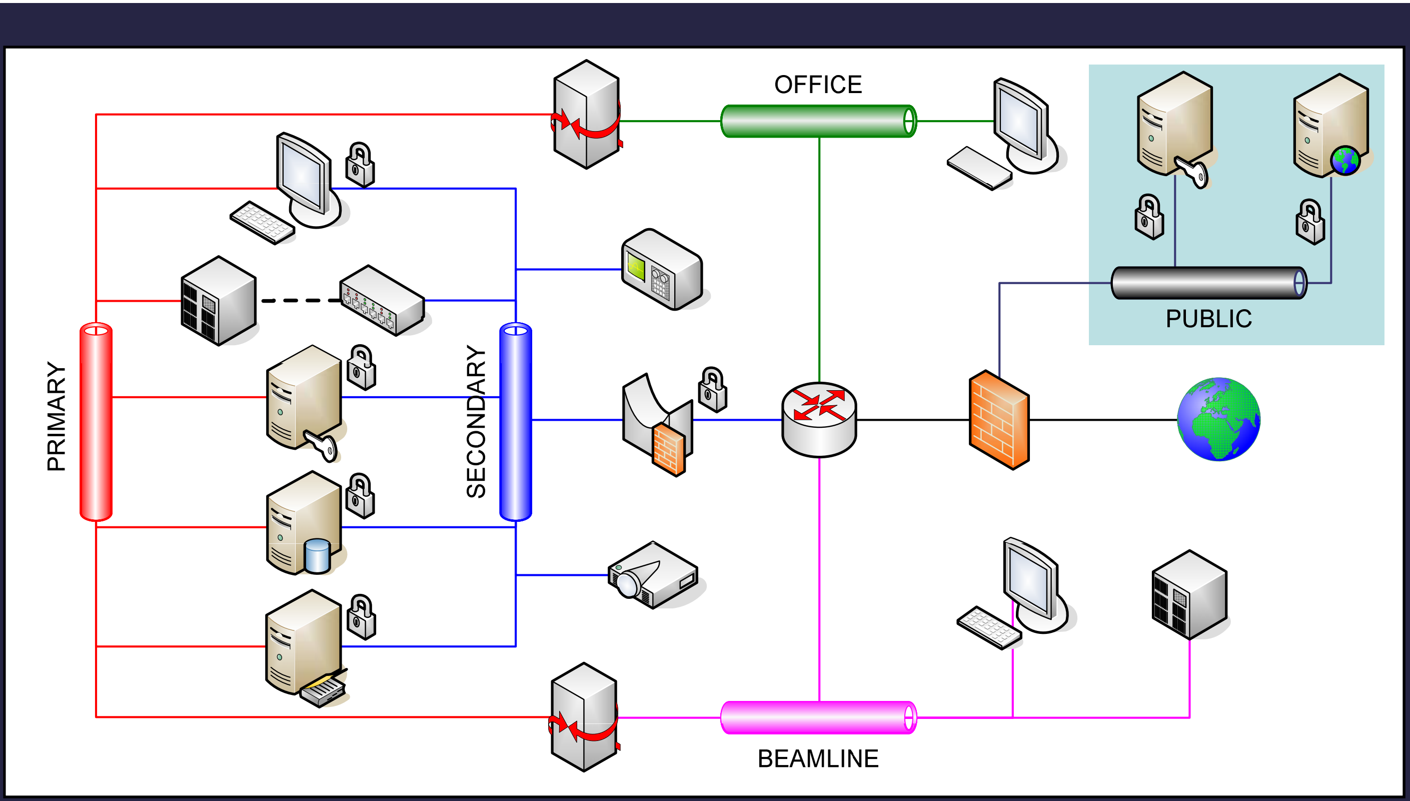
Stateful:

```
> iptables -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT
```



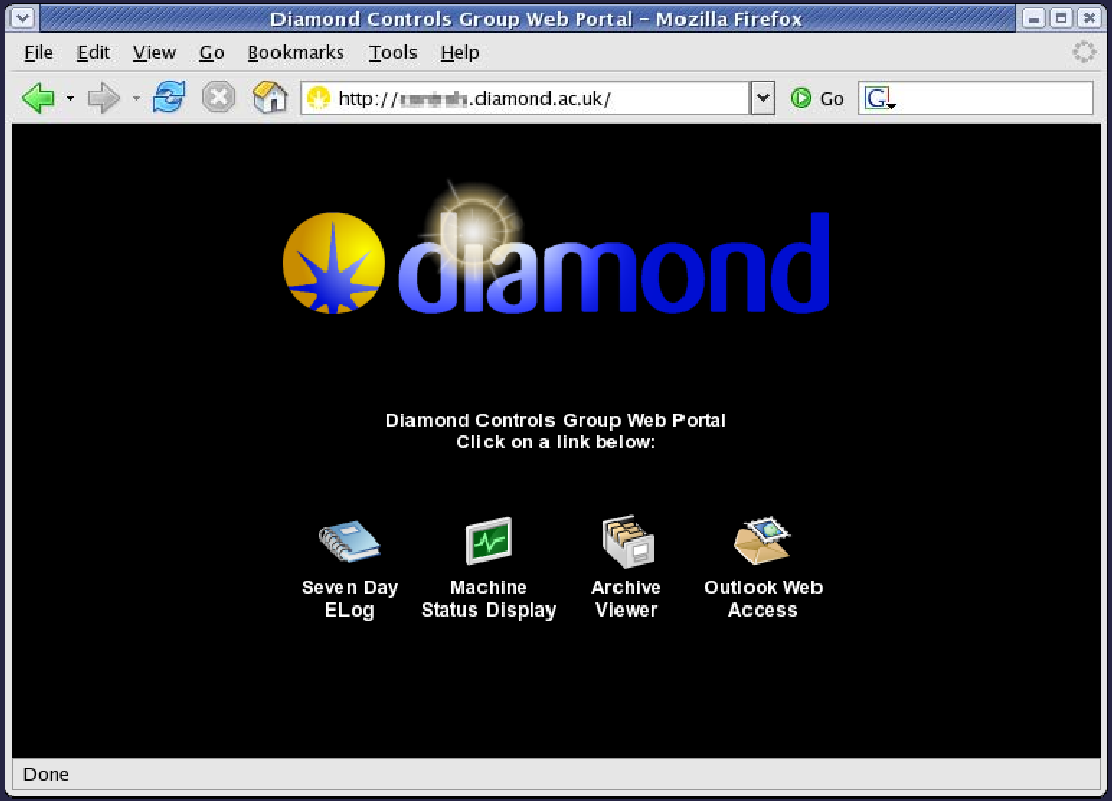
## Epics Channel Access Gateways:

- Enable machine parameters to be read from isolated primary network
- One for office networks and one for each beamline network
- Application layer gateways. No direct routing of IP packets
- Unidirectional read-only gateway for office
- Bidirectional read-only gateway per beamline – no default route
- CA monitor allows moving of ID gaps through read only gateway



## Diamonds Public and Private Networks:

- Diamonds control, office, science and beamline networks are all NAT’d private networks
- Some proxyed protocols eg. Real player, http, https
- A limited number of other protocols allowed out eg. ssh
- Diamond controls public network has a public address range and is directly routed to diamond private networks, but behind site firewall
- SSH bastion and reverse web proxy on public network
- No DMZ - yet!.


Diamond Controls Group Web Portal - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
http://[redacted].diamond.ac.uk/
Go
diamond

Diamond Controls Group Web Portal
Click on a link below:

Seven Day ELog
Machine Status Display
Archive Viewer
Outlook Web Access
Done

## Apache Reverse Web Proxy:

- Enables one web server to provide content from another transparently.
- Gives encrypted and authenticated access to certain internal web pages. Such as, Elog, archiver, Machine status.

http://internal.com -> https://external.com/internal

diamond

```
LoadModule proxy_module      modules/mod_proxy.so
LoadModule proxy_http_module modules/mod_proxy_http.so
LoadModule headers_module    modules/mod_headers.so
LoadFile   /usr/lib/libxml2.so
LoadModule proxy_html_module modules/mod_proxy_html.so

<VirtualHost 123.123.123.123:443>
    DocumentRoot /var/www/html/external
    ServerName external.com

    ProxyPass /internal/ http://www.internal.com/
    <Location /internal/>
        ProxyPassReverse /
        SetOutputFilter  proxy-html
        ProxyHTMLURLMap  /      /internal/
        ProxyHTMLURLMap  /internal  /internal
        RequestHeader    unset  Accept-Encoding
    </Location>

    SSLProxyEngine on
    <Proxy *>
        AuthType Basic
        AuthName “External Area"
        require valid-user
        Allow from all
    </Proxy>

    SSLEngine on
    SSLCertificateFile /etc/httpd/conf/ssl.crt/external.crt
    SSLCertificateKeyFile /etc/httpd/conf/ssl.key/external.key
</VirtualHost>
```

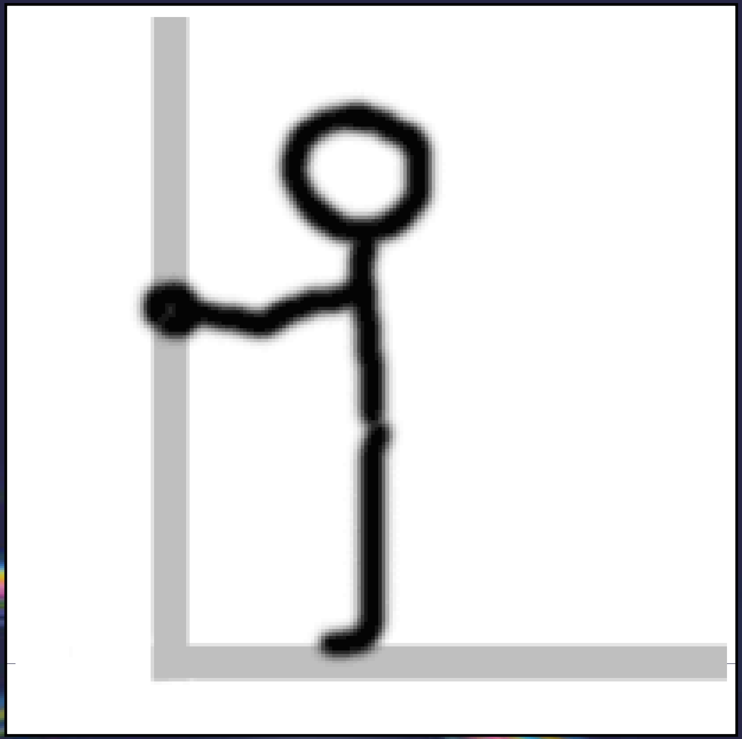
## Acknowledgements

I would like to thank the following for their help:

| | |
|---|---|
| Tim Hayton | Original Network Design and Tender |
| Mark Heron | Original Network Design / Contract Manager |
| Pete Leicester | Channel Access Gateways |
| Peter Denison, James Rowland | LINUX / EPICS Gurus |
| Frederik Ferner, Tina Friedrich | More LINUX Gurus |
| Paul Amos, Simon Lay | Original Cable Installation |
| Chris Colbourne, Nico Rotolo | Cabling Maintenance |

The LINUX and EPICS communities

Network security may seem like an impossible struggle!



But don't give up hope ;-)