



# EZproxy blocks





- Version 4.0h
- Responsibility shared with Library IT.
- We proxy all our traffic, on-campus & off.
- 2 ezproxy servers ( High Availability Solution)
- *Blocks not automatic on both servers*

Can monitor or block:

- illegal login attempts
- excessive downloads





# Illegal login attempts

2 options to monitor and suspend access:

- Both set up in the ezproxy.cfg, and work on the same principles -

Specify the number of times someone can attempt to login within a specified interval, after which ezproxy will evade further login attempts.

- If another interval passes without any further login attempts, the IP /Username will be cleared automatically.
- If the login attempts continue the IP/username will be blocked until manually cleared in the admin module.





## IntruderIPAttempts

- Monitors for repeated attempts to log into the EZproxy server from the same IP address, regardless of requested username, then blocks attempts to log in from that IP address.
- *Login attempts with bad details can block access to everyone at an institute, or ISP. TPG was blocked!*
- Can specify IPs which should be treated more leniently.
- *We don't because we don't have control of the way access is managed from the various research institutes.*
- reject.htm page





# IntruderUserAttempts

- Monitors for repeated attempts to log into the same username, regardless of source IP address, then blocks attempts to log into that username.
- *Names could be found in the uni phone-book....*
  - reject.htm page
  - *You have to work out which directive sent it.*





## Getting the parameters right

- A balancing act!
- If bona fide users are blocked, they will contact us. If bad guys get blocked, they won't.
- 3 changes to the settings, to try to prevent bad login attempts from blocking access at institutes.





## Current settings:

- **[Note: this slide deleted from published version]**





- **Deny**
- Lets you deny access to compromised user Ids
- *Used when notified by Auscert about IDs stolen using haxdoor.*
- *Used when an ID was posted on a website.*
  
- **RejectIP**
- Lets you deny access to specific IP(s)
- *Used to block IPs used with stolen ID or break-in attempts*





# Download monitoring & blocks

- **UsageLimit** can monitor and/or block transfers or Mbs downloaded
- *We monitor only.*
- Based on Username, or IP if on-campus
- Specify the amount and the interval when the downloading occurs.  
Suspension can be set to automatically expire after a specified period, or require the user to contact the Library so it can be manually cleared.





## View Usage Limits and Clear Suspensions

### Audit Events for 2008-01-23

No events matched.

### Audit Events for 2008-01-22

Date/Time	Event	IP	Username	Session	Other
15:47:15	UsageLimit	172.16.25.113	auto- 172.16.25.113	2RT3nNS6JMXr2xz	Global 400MB transfer exceeded





## Transfers or MB?

- Regular questions about this on the list
- **Transfers** counts the number of elements transferred in an ezproxy session – this would vary from product to product so haven't looked at this.
- **Megabytes** ...





## What should the limits be?

- Monitoring lots of “tripwire” limits put a big load on the server.

### **Sept-Dec 2005:**

- Most download sessions are small
- Top 1% of downloads – the average amount downloaded = 48.4 Mb. The largest amount was 8742 Mb.
- Vast majority of sessions are under 49 Mb
- Most are well under 5 Mb, even under 1 Mb





- Tried using `-enforce` if transfer > 200Mb  
Lasted 7 hours
- User blocked while downloading from  
Connect4 and FinAnalysis
- You can specify limits for particular databases.
- *But....need to know average file size and  
typical user behaviour for each resource*





## In-house scripts

- A script monitors the number of hits to each server each day.
- Output graphically and emailed the next day.
- Makes it easy to see if something uncharacteristic happened.





our	Hits	
0	1,339	*
1	1,322	*
2	910	*
3	674	*
4	621	*
5	418	
6	370	
7	603	*
8	627	*
9	1,142	*
0	22,563	*****
1	41,134	*****
2	2,298	**
3	3,048	***
4	2,995	***
5	3,133	***
6	2,712	***
7	3,101	***
8	2,108	**
9	1,978	**
0	1,525	**
1	2,545	***
2	1,989	**
3	966	*

*Initially I used to investigate but now have decided to wait until we are contacted by a publisher about possible abuse.*





## Email alert for intrusion attempts

- Another script checks the intrusion attempts recorded by ezproxy and emails Tony when an increase has been recorded.
- He then manually blocks that IP on the server firewall.
- The user doesn't get a message, their browser just times out. So far no-one has complained. A backup to the built in functionality in ezproxy.





- Still learning about user behaviour.
- Should we be blocking based on download amount?

