Surviving a DDoS Attack

Matt Johnson, Technical Director, Eduserv

Networkshop14, April 2014

eduserv

IT for public good

Agenda

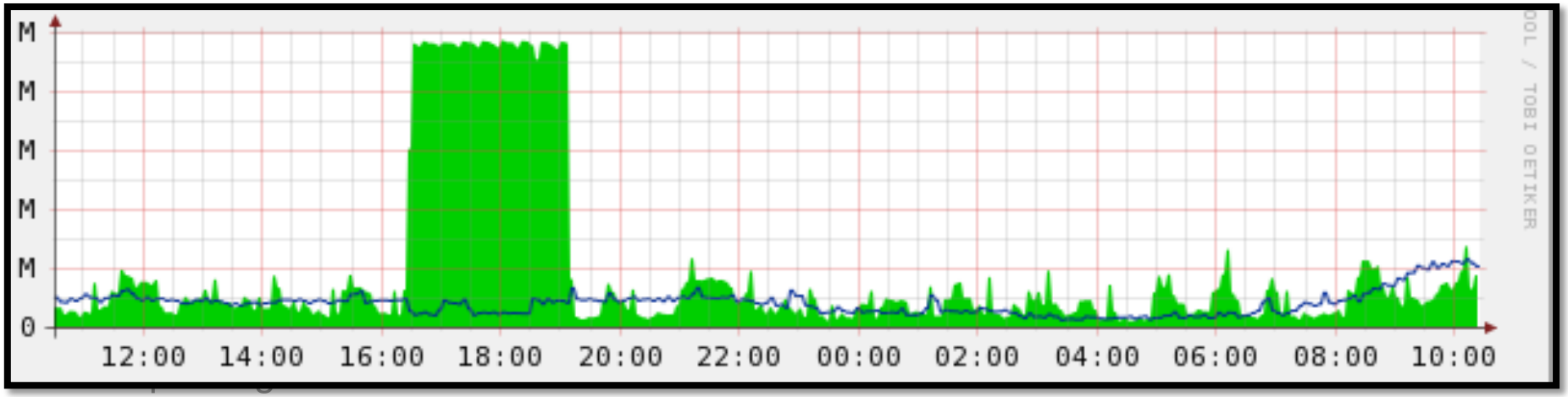
- Background
- Diary of the DDoS
- Attack profiles & social media
- Analysis and solution overview
- Costs
- Lessons learned
- Q&A

Background

- Eduserv is a registered charity providing IT services to public good organisations
  - Operates primary services from our Swindon datacentre, secondary and DR services from Slough / London
  - Providing hosting services since 1996
- IT services customer base
  - 20+ customers, across government, health, education and the charity sectors
  - Some of the government customers are high-profile targets

Day 1

- Initial attack was seen on the evening of Sunday 13th May
  - Lasted around 2 hours
- Attack was TCP-based, volumetric, probably HTTP-based
  - Primary sources in Brazil, Canada
  - Attack claimed by hacker via Twitter



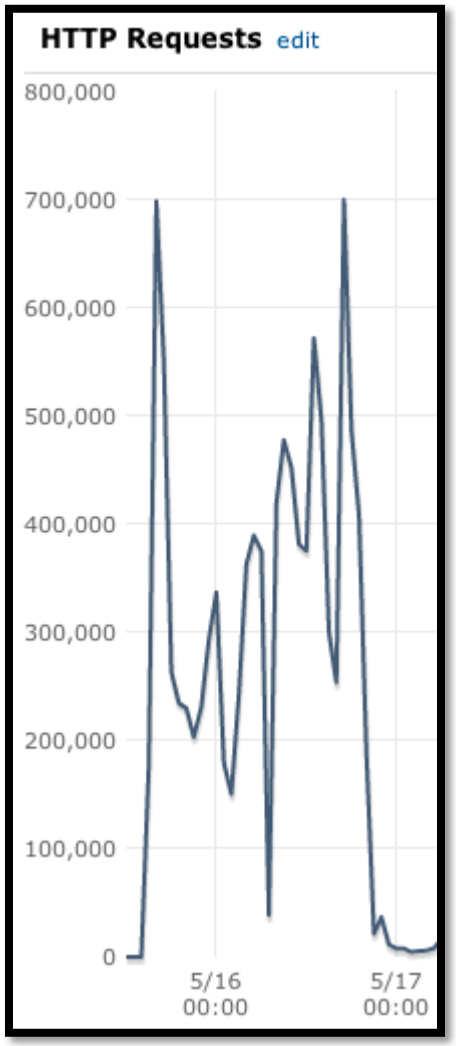
Day 2

- Second attack on afternoon of 14th May
  - Against a range of Govt. websites
- Attack was UDP-based
  - Probably DNS-amplification
  - Diverse source addresses
  - 1 hour DoS for a number of customers
- Damage limitation
  - Re-address and black-hole the address block of the targeted website services
  - “One sacrificed to save the many”

eduserv
IT for public good

Day 3

- Attacked website brought back online
  - Separate ISP link to mitigate impact to other services
- DDoS attacks resumed immediately
  - HTTP volumetric based attack overwhelmed web server cluster
  - Web service was a 3rd party legacy build, with poor caching



eduserv
IT for public good

Attack Methods

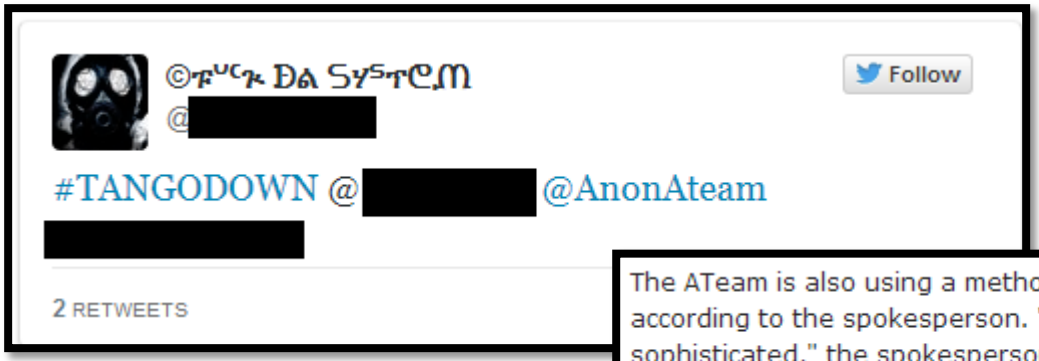
- Range of attack methods used
  - Low Orbit Ion Cannon (LOIC), High Orbit Ion Cannon (HOIC)
  - DNS Amplification, HTTP Idle Attacks,
- Scale of the attack
  - Bandwidth peak estimated >5 Gbps
  - 200+ malformed requests p/sec (normally 2-3 requests p/sec)
- Lack of support from upstream ISP for real-time blocking
  - Without this support, in a volumetric attack, hands are tied

Social Media

- Many attackers like to promote their “work” – can give an early insight into what’s happening (or about to happen)
- Don’t believe everything you read ☺

75,000 compromised or 'zombie' computers

The ATeam is using a network of around 75,000 compromised or 'zombie' computers called a 'botnet' to launch the DDoS attacks using automated attack methods only, an ATeam spokesperson told ZDNet UK via messages on Twitter. The botnet has been built using both volunteer machines and systems that have been infected by hackers, said the spokesperson.



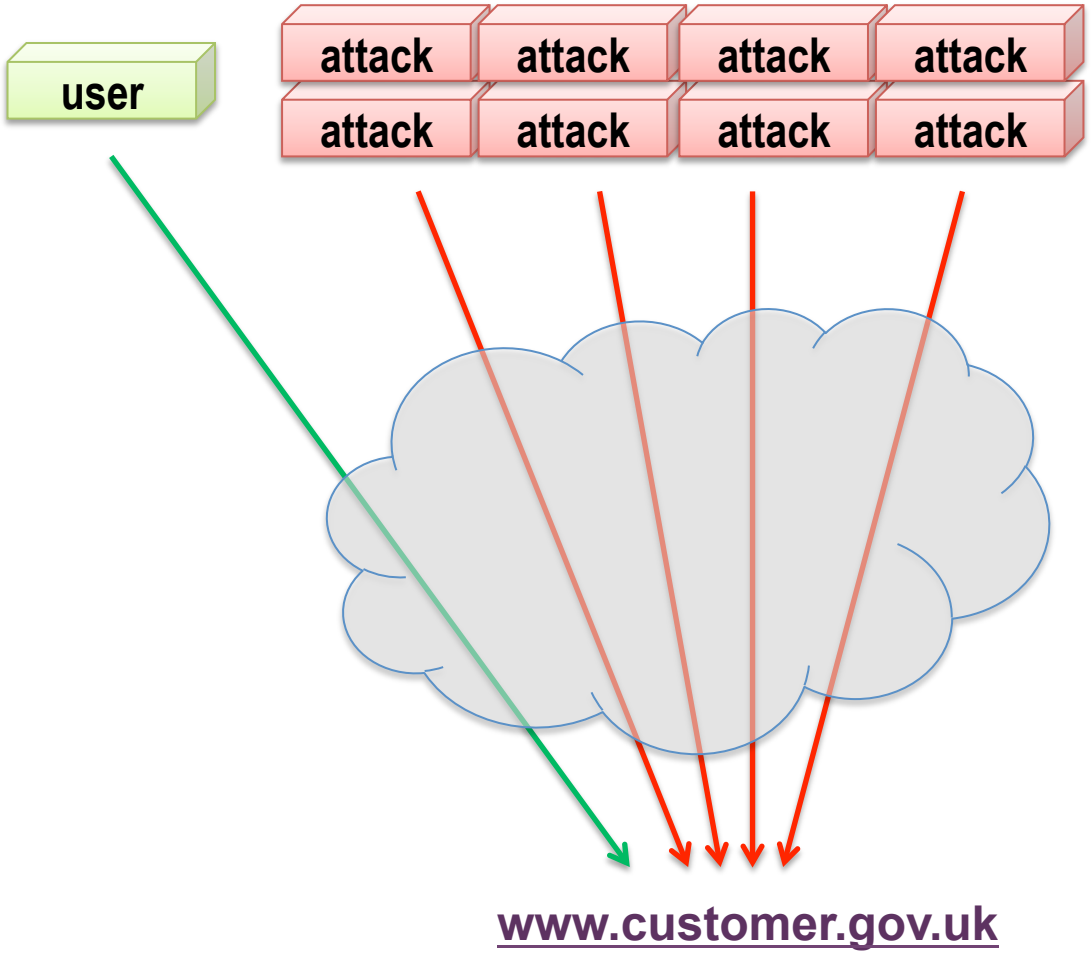
f 35 gigabits per second,

The ATeam is also using a method that can generate attack traffic of 35 gigabits per second, according to the spokesperson. "We also have another attack method which is very sophisticated," the spokesperson said. "We attack with 50 servers — we can blue-screen a server so that it needs to be reboot [sic]."

Incident Analysis

- Crisis Management Team formed
  - Multi-disciplinary teams – can bring new insight into solutions
  - Whiteboard-based evaluation of options
  - Continual comms with the impacted customer
- Possible solutions
  - Block or disable attacking platforms at source
  - Rebuild the web service to cope with the additional workloads
  - Filter the DDoS traffic whilst allowing legitimate requests

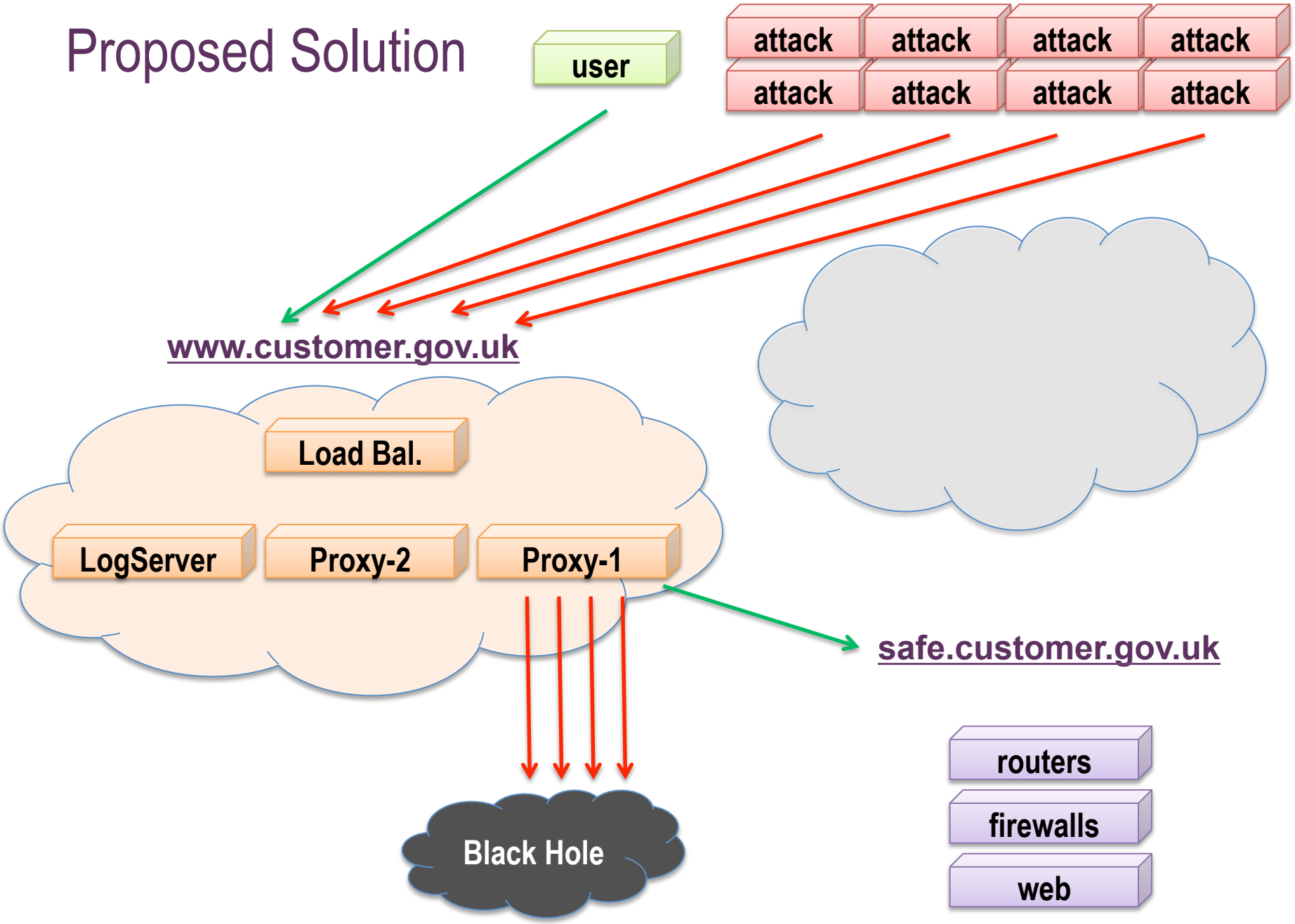
Starting Situation



eduserv

IT for public good

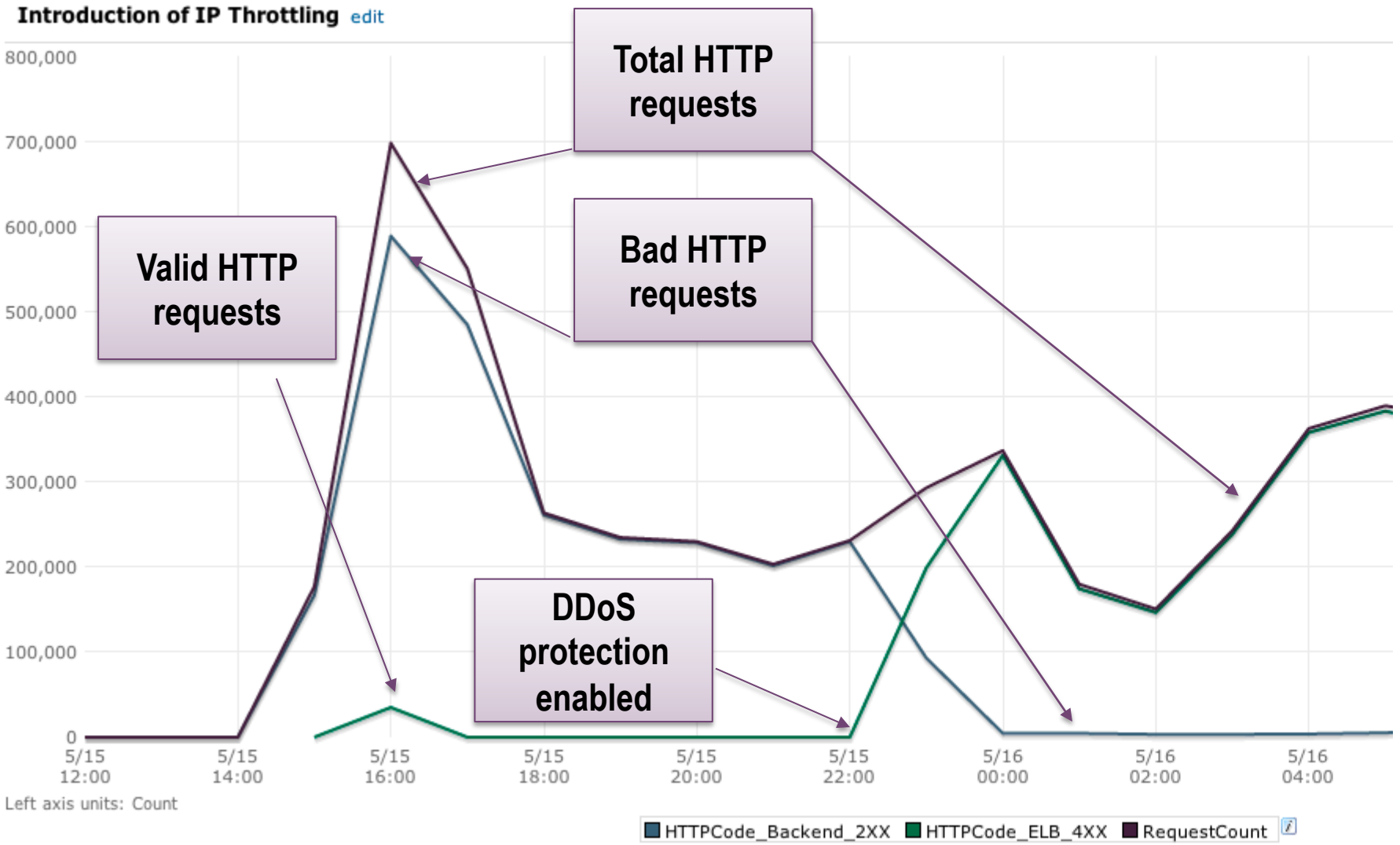
Proposed Solution



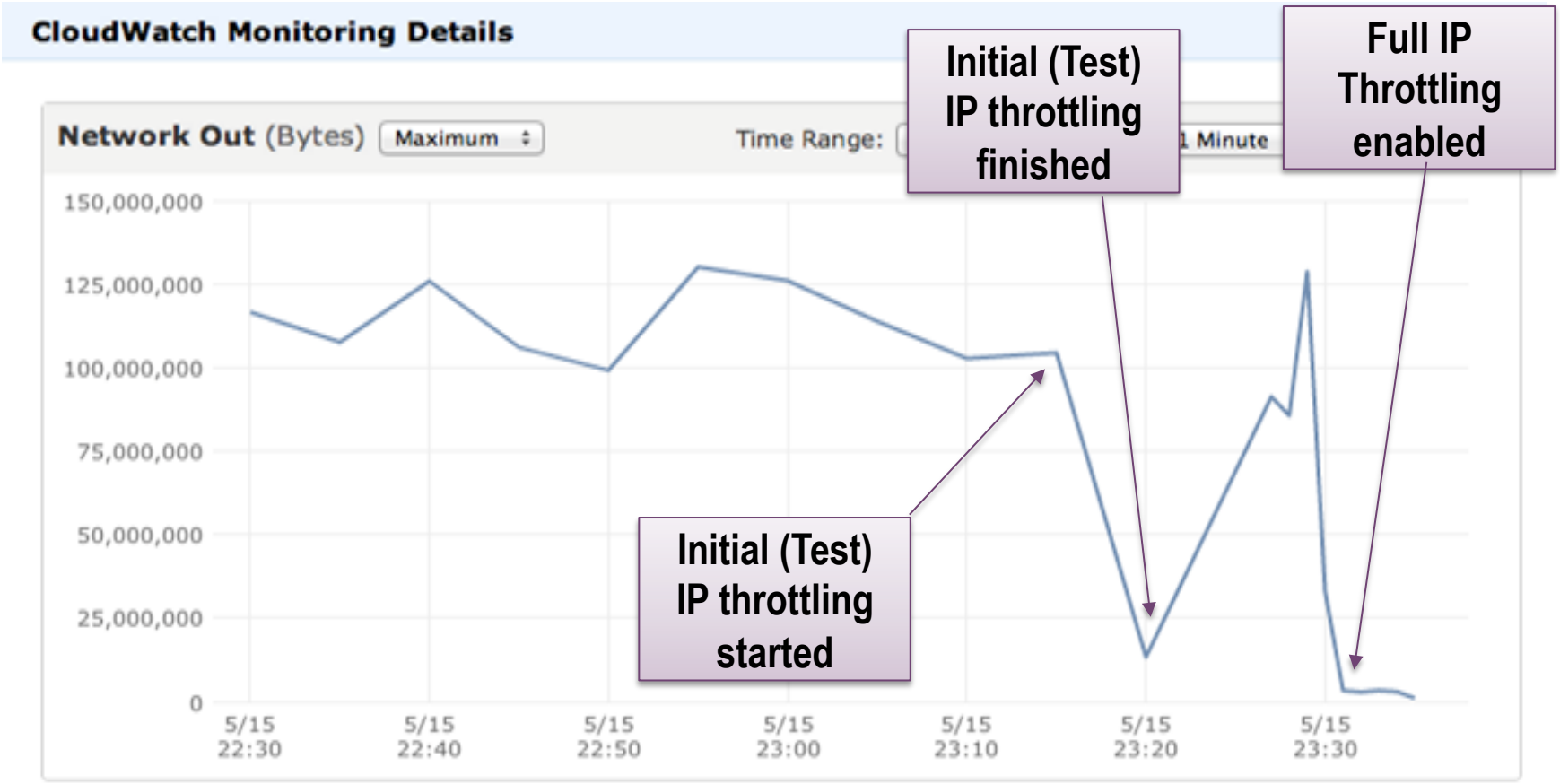
Web Proxy in the Cloud

- Cloud provider choice – Amazon Web Services
  - Already had expertise in deploying AWS services
  - Huge bandwidth capacity (estimated at 600 Gbps+)
  - AWS Marketplace offers quick deployment of application servers
- Proxy choice - AiCache
  - Searched the AWS Marketplace
  - AiCache seemed to deliver the functionality required
  - Available on a PAYG basis with no up-front licensing commitments
- Configured and implemented inside of 4 hours

Enabling DDoS protection



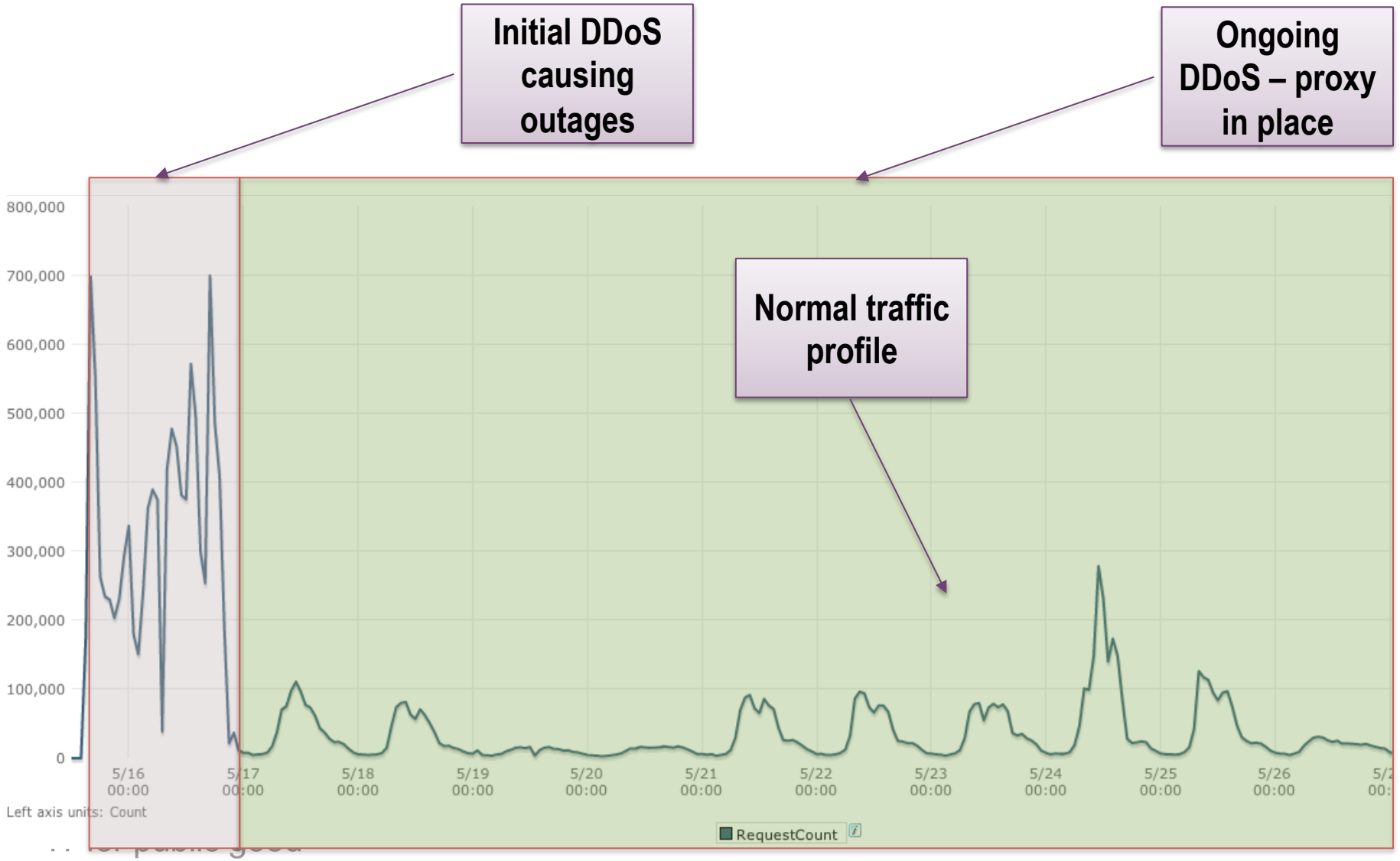
Enabling IP Throttling



eduserv

IT for public good

Traffic profile before and after proxy implementation



Costs

- IT costs: £350, comprising:
  - AWS: 150 GB of data transfer, load-balancing; 2 large VMs; 100 GB of data storage: ~$270 over 14 days
  - AiCache: 2 licences & support: $280, again over 14 days
- People costs: £25k, comprising
  - Incident response: ~£15k
  - Incident analysis: ~£10k
- Indirect costs: ~£20k
  - Impact on customer services, 3rd party effort, opportunity costs

Lessons Learned

- Bandwidth is king
  - In a sustained attack, whoever has the most, wins
  - Janet customers are in a pretty good place compared to commercial ISPs
- Build your relationship with upstream network providers
  - Janet have a great team – make sure you know who to contact
  - Don’t forget your non-Janet links

Lessons Learned

- DNS flexibility is vital
  - Having a well-architected DNS infrastructure allows you to change service endpoints quickly in response to targeted attacks
  - Make sure you have a diverse route into your DNS management
  - Keep at least one DNS server on a separate network
- Building your own works, but consider using specialist Cloud-based security providers
  - CloudFlare
  - Imperva

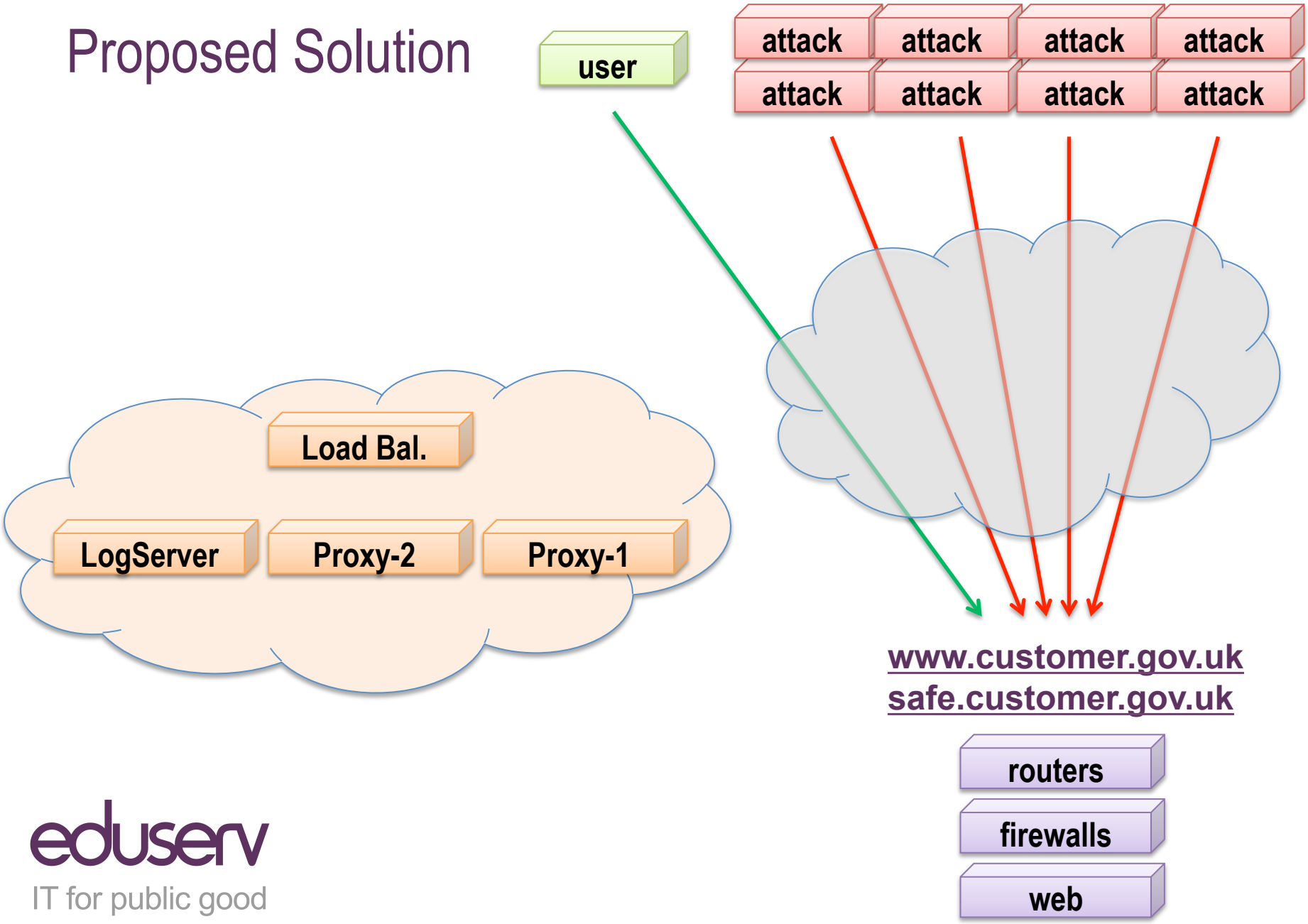
Thank you! Questions?

- Matt Johnson
  - Technical Director, Research
  - Matt.Johnson@eduserv.org.uk
  - @mhj_work
  - www.eduserv.org.uk
  - www.slideshare.net/eduserv

eduserv

IT for public good

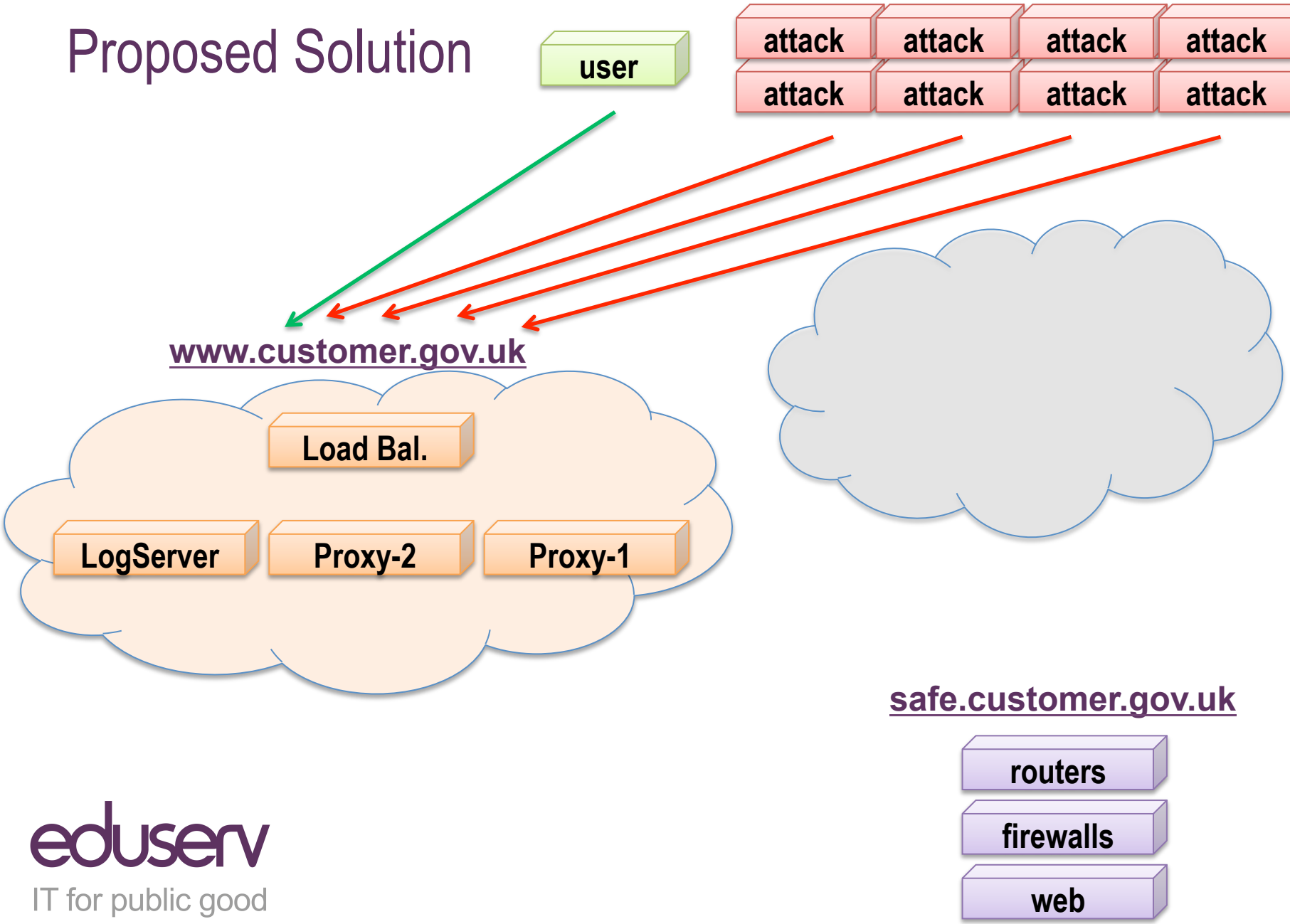
Proposed Solution



eduserv

IT for public good

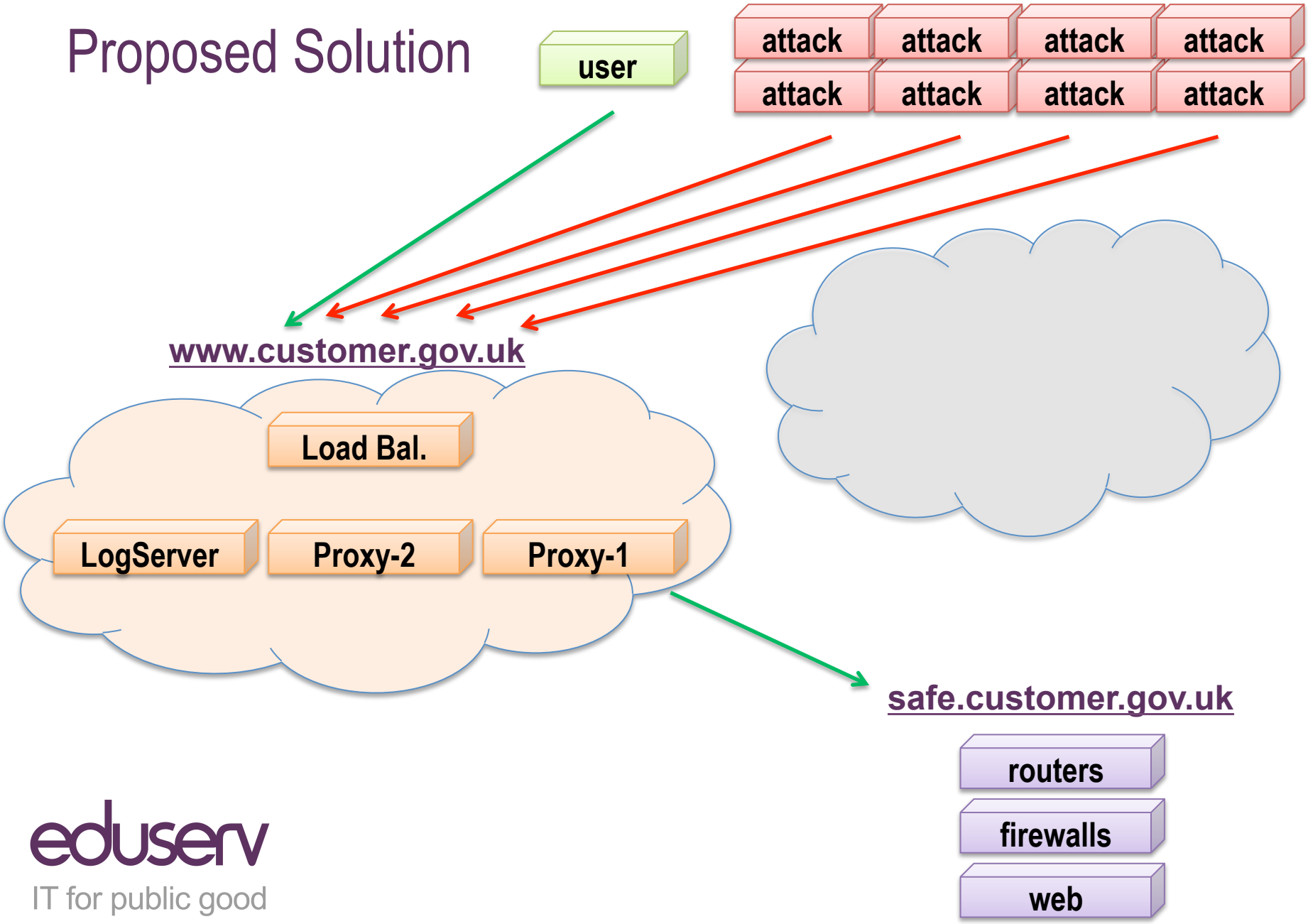
Proposed Solution



eduserv

IT for public good

Proposed Solution



eduserv

IT for public good

Issues we encountered

- Capturing log data from proxy/AWS infrastructure
  - Needed to enable x-forwarding headers on the AWS ELBs
- SSL website services
  - Where do you decrypt and inspect?
- Insight into what's happening
  - AWS has great tools, but only maintains 2 weeks of log files
  - AiCache can generate LOTS of log traffic

SSL services

- AiCache doesn't cache SSL by default
  - Luckily the DDoS target was the standard (non-HTTPS) website, so we had some breathing space
  - Made a decision to decrypt SSL in the Cloud (AiCache), and then re-encrypt for onward transit to the web service
  - This was done with the consent of the customer
  - Involved moving the SSL private key onto the AiCache VM
- Generated a new SSL certificate post-attack
  - Following best practice, rather than in response to any thought that the key might be compromised