



# Internet Filtering

*What it is – and isn't...*

Paul Brooks

Director – ISOC-AU

pbrooks@layer10.com.au

Problem... Or is it a problem?



10th March 2008



TCCM Cyber Savvy - March 2008  
- (c) ISOC-AU

2

## Agenda

- The Internet
- The InterWeb
- Not-the-InterWeb


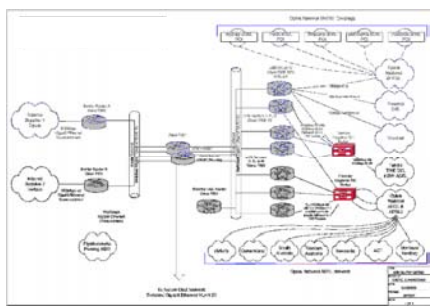
...in 15 minutes...



10th March 2008 TCCM Cyber Savvy - March 2008 - (c) ISOC-AU 3


## The Internet – filtering points

- Network (ISP) Filtering
- User-side Filtering
- User Filtering

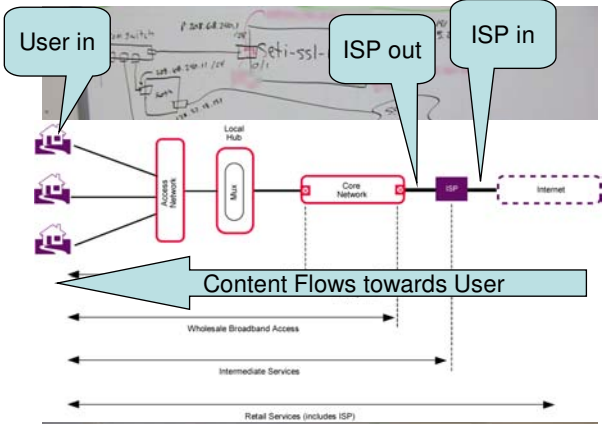


10th March 2008 TCCM Cyber Savvy - March 2008 - (c) ISOC-AU 4

## ISP Network Filtering




### Typical ISP Network Diagram for end-user connection...

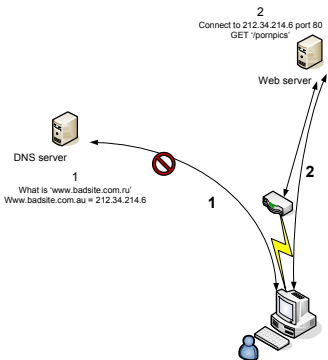


10th March 2008      TCCM Cyber Savvy - March 2008      5  
- (c) ISOC-AU


## The 'Interweb' – WWW requests



- User asks for [www.badsite.com.ru/pornpics](http://www.badsite.com.ru/pornpics)
- Block DNS request
  - ISP first has to know [www.badsite.com.ru](http://www.badsite.com.ru) is to be blocked – needs prior notification
  - Thousands of names can point to same address
  - User can bypass DNS request by just using the IP address in the browser
  - Blocks every website on that machine name – [www.bigpond.com](http://www.bigpond.com)? Massive collateral damage



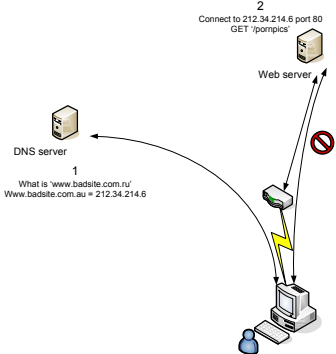
10th March 2008      TCCM Cyber Savvy - March 2008      6  
- (c) ISOC-AU



## The 'Interweb' – WWW requests


---

- User asks for 'www.badsite.com.ru/pornpics'
- Block IP address
  - ISP first has to know 212.34.214.6 is to be blocked – needs prior notification
  - Thousands of sites can be hosted on the same IP address – massive collateral damage
  - HTTP can use any port number, not just 'port 80' – under control of the site – so have to block all connectivity for all applications
  - Golden opportunity for Denial of Service – deliberately host inappropriate content on www.bigpond.com/user/fakename



---

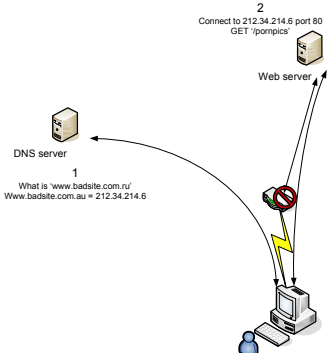
10th March 2008
TCCM Cyber Savvy - March 2008  
- (c) ISOC-AU
7



## The 'Interweb' – WWW requests

---


- User asks for 'www.badsite.com.ru/pornpics'
- Deep Packet Inspection
  - Attempts to look deep into packet contents to identify application, try to classify packets in 'real time' and identify signatures of 'bad stuff'
  - e.g. reconstruct images on the fly – look for excessive flesh tones
- However...
  - Doesn't scale – bandwidth required and number of images to be analysed increasing faster than Moore's Law
  - Still images being surpassed by streaming movies – impossible to analyse all movies/videos streaming in real time
  - Forces all content through a gatekeeper box – poor reliability
  - Indiscriminate Blocks medical sites, school swimming carnivals, baby photos.....
  - Defeated by Secure HTTP – encrypted webpages, identical to online banking



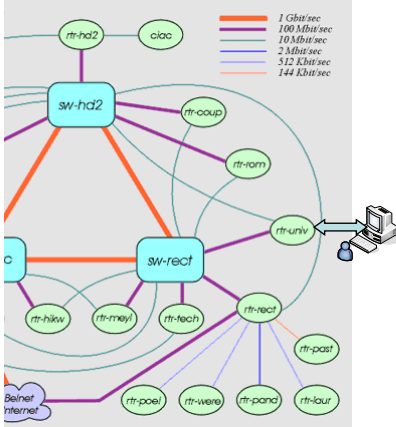
---

10th March 2008
TCCM Cyber Savvy - March 2008  
- (c) ISOC-AU
8

## Network Filter – where?




- Upstream Provider Link?
  - Most ISPs have 3 – 30 upstream providers
  - Peering Points – no 'provider'
- In the ISPs Core?
  - Single point of failure
  - Poor performance of 'trombone' traffic paths
  - Huge traffic increase – multiply cost of longhaul transmission
  - Misses content generated by other users of the same ISP
- At the PoP
  - Most ISPs will need 5 - 30 gatekeeper boxes!
- great idea if you sell gatekeeper boxes, not practical in real networks



---

10th March 2008
TCCM Cyber Savvy - March 2008  
- (c) ISOC-AU
9

## Fundamental Issues



- ISP-level filters can't tell if you are accessing photos of your own kids, or someone else's
- ISP-level filters can't tell the age of the user requesting the photo – can only be used for verified illegal content, not for 'inappropriate' content
- Easily circumvented using public anonymous proxy sites – the URL the ISP sees is completely different from the eventual URL being accessed
- Easily circumvented by encrypted webpages – HTTPS, SSL encryption

---

10th March 2008
TCCM Cyber Savvy - March 2008  
- (c) ISOC-AU
10

## User-side Filtering



- Software filter on a user's PC
  - Can be customised per user – Mum's level of filtering can be different from children
    - Mum must remember to log out, or the next person to the keyboard uses her permissions
  - Lists of inappropriate sites needs to be kept up to date
- Relatively easy to work around – public proxies, 'admin' user can disable
  - Generally complicated for an unsophisticated user to install and keep up to date

10th March 2008

TCCM Cyber Savvy - March 2008  
- (c) ISOC-AU

11

## Not-the-InterWeb



- The Internet, and inappropriate content, is not just exchanged using HTTP (WWW)
  - Email
  - USENET aka 'Network News'
  - Peer-to-peer – e.g. bittorrent
  - RSS - Podcasts
  - Instant Messenger – MSN, Yahoo, etc
  - Skype
  - .....and many others




10th March 2008


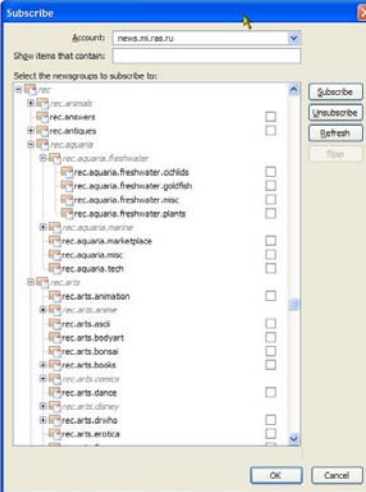
TCCM Cyber Savvy - March 2008  
- (c) ISOC-AU

12

## USENET News




- Message boards, Predates WWW
- >50,000 newsgroups active

10th March 2008      TCCM Cyber Savvy - March 2008      13  
- (c) ISOC-AU


## USENET news



- Messages are like Email – text encoded attachments
- Images split into dozens or hundreds of messages
- Messages can be distributed across multiple newsgroups
- Until all parts of a binary document (image, program, zip-file, movie) are received, the binary document cannot be reconstructed and analysed
- Even if it is inappropriate content, no way to block it until it has already been distributed

10th March 2008      TCCM Cyber Savvy - March 2008      7  
- (c) ISOC-AU

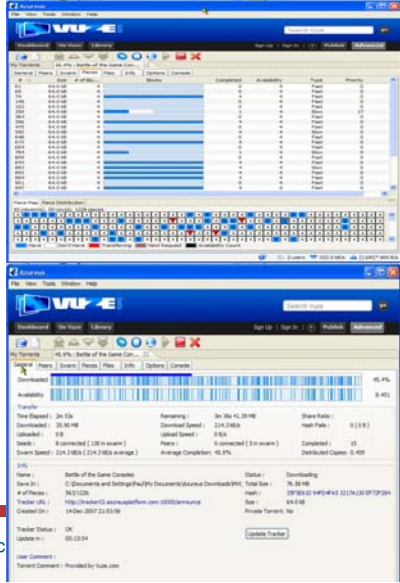
## Peer-to-peer transfers




- Files broken into hundreds of small pieces
- Central 'torrent servers' only have lists of 'peers' with pieces, no content themselves
- Collect pieces from hundreds of PCs while serving your pieces to hundreds that need them
- Looks to the ISP network like hundreds of random connections to other random IP addresses
- Can be encrypted - no way of knowing what is inside the files
- No way to analyse files until all pieces are downloaded
- **Cannot be blocked once started – the swarm of active sharers is self-sustaining**

10th March 2008

TCCM Cyber Savvy - Marc  
- (c) ISOC-AU



## What it isn't...



- ISP-level filtering is not very effective – too easy to go too far, and doesn't solve the problem
- The problem to be solved hasn't yet been articulated clearly
  - Are we blocking illegal content, blocking 'undesirable' content, and who does the classification?
- No substitute for **POS**  
**Parent Over the Shoulder**

10th March 2008

TCCM Cyber Savvy - March 2008  
- (c) ISOC-AU

16





Thank you

Paul Brooks  
Director, ISOC-AU  
[pbrooks@layer10.com.au](mailto:pbrooks@layer10.com.au)

[www.isoc-au.org.au](http://www.isoc-au.org.au)