The Problem:

As the internet continues to grow and expand and through the introduction of new technologies, there has been an explosion in websites offering child sexual abuse material to users. This material is offered in either subscription form ie via a payment scheme or via a streaming interface.

Whilst these sites are accessible to law enforcement they are quick to resurface upon discovering they have been taken down.

Over the last 10 years of talking to suspects the censorship compliance unit has discovered that the frontline sites offering this type of material is usually the first point in a suspects offending.

Additionally innocuous searching may also lead a user to these sites, exposing members of the public to harmful material. These innocuous search requests may also bring the material to the forefront, as it has been identified that the administrators of the sites will make every effort to put this material in your face in an attempt to normalize the subject material.

As there is a continued demand for this material, children will continue to be abused to fill it.

Due to this, a suitable method of restricting access to these frontline sites is being sought out.

Current Solutions:

Many security software providers offer a filtering service such as Norton Internet Security which enables the user to set rules on the type of information that is accessible via the internet to their household.

These systems sometimes referred to as content filters although simple to instigate rarely enforce the rules or are overly aggressive in there enforcement and prevent users from accessing legitimate content.

Internet service providers (ISP's) have reviewed the current technologies as they have become more apparent and found that although the technology is available to filter users internet habits, it is still too restrictive or unable to operate at the level required to make it a viable business offering.

An example of the current technology is the system known as clean feed. Clean feed is widely used in the United Kingdom and represents research completed by the provider BT. BT provides the outline for the system free of charge to approved entities. This system uses a process known as proxying whereby all customer requests are directed through a central system, if this request matches a predefined set of rules or blacklist the request is blocked and the user informed that the request is unsuccessful via a blocking page.

This system although very highly used in the United Kingdom is not very adaptive to needs and requires a lot of system resources such as hardware.

Other systems included the process DNS[1] poisoning[2]. This process redirects the users system based on a blacklist created by a government of private sector agency to a central blocking page containing text informing them the request was unsuccessful.

[1] The Domain Name System (DNS) is a hierarchical naming system for computers, services, or any resource participating in the Internet.

This process although much more efficient than proxying has many weaknesses and requires a lot of support from network providers such as APNIC, ARIN etc to ensure the system is available at the right level.

Solution Presented to the Unit:

The solution presented to the unit known as the Netclean Whitebox originates from Sweden.

The system designed by Netclean filters users requests via BGP [3] and a master list of known objectionable sites.

Due to this it is highly adaptable to websites changing their hosting provider which, is a common step taken by the hosts to avoid detection by law enforcement.

System Design:

The system designed for the trial used the following build specifications

Hardware

- 3 GHz CPU (minimum)
- 1 GB Memory
- 100 GB SATA/SCSI HDD
- Broadband Connection/Fibre (preferable)

Software

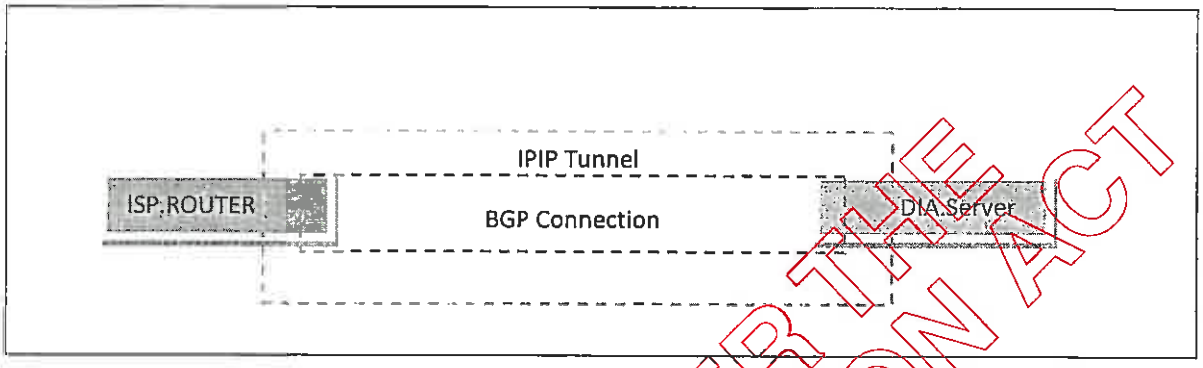
- FreeBsd[4] (a variant of Unix)
- Quagga[5] (a BGP routing daemon)

[2] DNS cache poisoning is a situation that provides data to a Domain Name Server that did not originate from authoritative DNS sources. This can happen through improper software design, misconfiguration of name servers, and maliciously designed scenarios exploiting the traditionally open-architecture of the DNS system.
[3] The Border Gateway Protocol (BGP) is the core routing protocol of the Internet. It maintains a table of IP networks or 'prefixes' which designate network reach ability among autonomous systems (AS)
[4] Freebsd : www.freebsd.org
[5] Quagga: www.quagga.net

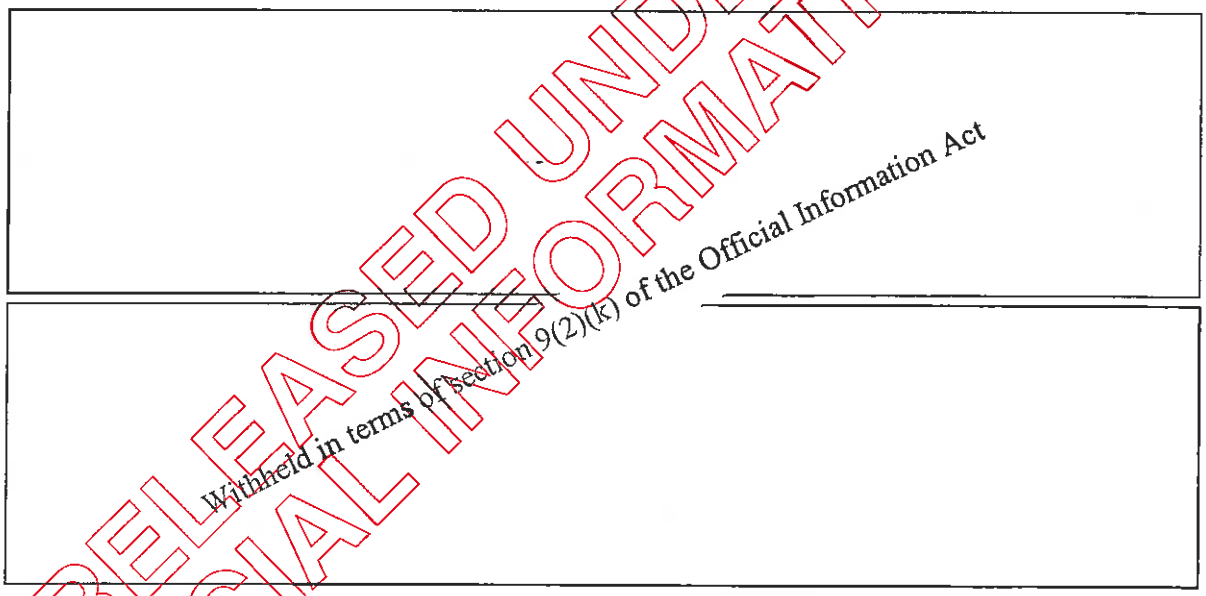
Client network design:

The connection to a service provider requires 2 steps

- A dedicated Tunnel is setup between the 2 locations
- A BGP session is then established.



All participant providers were provided with a common tunnel and BGP session design.



Investigation in to the lack of uptake of existing filtering services found that the resistance by providers to subscribe to a filter service was also related to the technician or engineer's time to configure the connection or network.

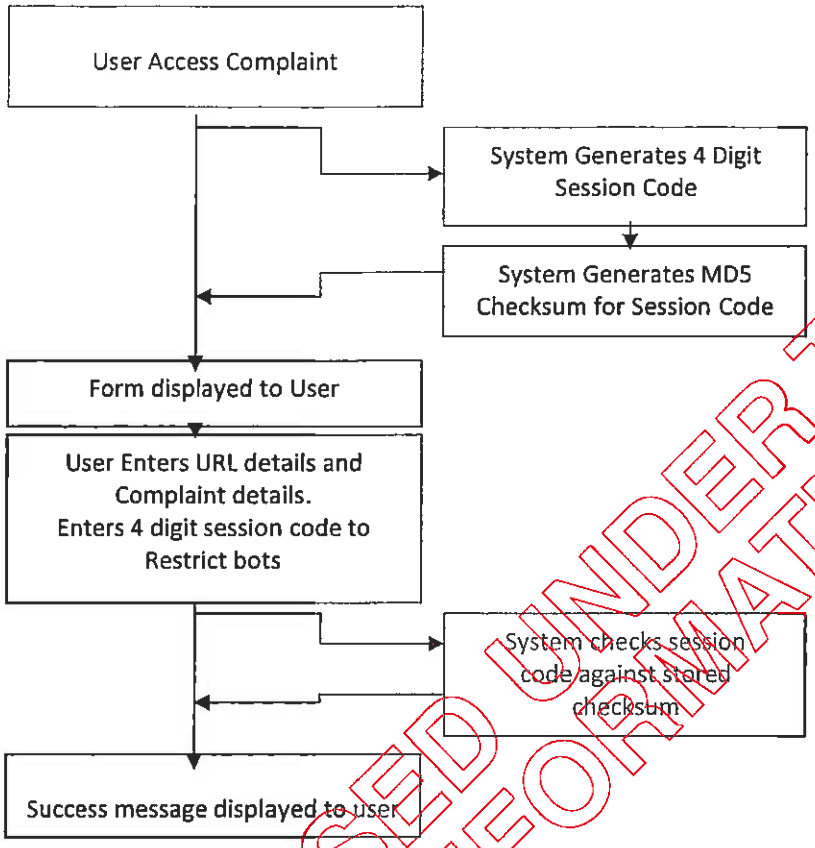
Landing Page Design:

Once the system detects a request for child sexual abuse material the user is redirect to the landing page.

The landing page was designed to achieve the following:

- Inform the user of the reason for the redirect
- Inform the user of the action taken
- Provide the user with a method to appeal the action.

The appeals process was designed to follow a set path to ensure privacy of the user making the appeal and also to protect the system from exploitation.



The appeals process does not ask for the users contact details and provides no method for follow up to the appeal.

Upon a successful signal being sent to the system the appeal is dispersed to nominated accounts within the censorship compliance unit for follow up.

Trialing of the solution proposed by Netclean:

To test the system the Censorship Compliance Unit performed a 2 year trial of the system

The trial was broken into follow 3 phases.

Phase 1:
To determine systems effectiveness against and in conjunction with commercial systems

Phase 2:
To determine effect on overall browsing speed and effectiveness of processing middle sized service provider

Phase 3:
To determine the scalability of the system and its effectiveness at processing large service providers

The unit chose 4 service providers to participate in the trial IHUG, Telstra Clear, Maxnet, Watchdog.

These ISPs were chosen due to their customer base and their current offerings such as content filtering.

Phase 1 Output:

Testing for phase 1 was focused on the operational effects of the system in conjunction with the provider's current filtering systems. This phase was limited to 1 service provider.

Providers network design incorporates a number of commercial systems aimed at restricting access to objectionable, adult, offensive websites via a commercially sourced list, filtering is at the proxying level.

Over the 4 month period for Phase 1 the system processed on average 3 million general requests at its peak the general requests[6] reached approximately 5 million.

Over the 4 month period for Phase 1 the system filtered access[7] to approximately 10,000 requests per month.

This Phase filtered access for 5,000 users.

Phase 2 Output:

Testing for phase 2 was focused on the effects the system could have on a users experience such as browsing speed when processing requests of a middle sized and small service provider.

This phase was limited to 2 service providers.

The middle sized provider was chosen due to the high uptake per customer of broadband.

Over the 6 month period for Phase 2 the system processed on average 8 million general requests, at its peak the general requests reached approximately 18 million.

This phase also incorporated the appeals system as a contained process. During the 6 months of Phase 2 the censorship compliance unit received 1 appeal. This appeal related to restriction of access.

Over the 6 month period of Phase 2 the system filtered access to on average 30,000 requests per month

[6] A general request is any request that parsed through the system or was handled by the system. This includes non objectionable websites.
[7] Filtered access relates to the system preventing the user from viewing the requested url

This phase filtered access for 25,000 users

This phase saw a 5 million unit increase in general requests per month and a 20,000 unit (peak 40,000) increase in filtered requests.

All tests surrounding general user experience were successful, no service interruptions occurred during the 6 month period.

Latency checks found that the network remained stable throughout the phase despite the increase in load.

Phase 3 Output:

Testing for phase 3 was focused on determining the scalability of the system and how effective it is at processing large service providers.

This phase was limited to 4 providers.

The large providers were chosen due to the size of the customer base and dispersion throughout the country.

Over the 3 month period for Phase 3 the system processed on average 40 million general requests at its peak the general requests reached approximately 100 million.

Over the 3 month period for Phase 3 the system filtered access to on average 100,000 requests per month at its peak it was processing 20,000 requests per week for 1 provider.

System tests performed during this period found that it was operating at approximately 80% capacity. This was decided the cut off point for reliable results for the scalability tests. The system did experience some stability issues processing this amount of requests and required maintenance on 2 occasions to replace hardware

This phase filtered access for approximately 600,000 users.

Database of Objectionable Sites:

Over the last 4 years the censorship compliance unit has developed a large database of sites offering child sexual abuse material.

In addition to this the unit has become affiliates of the CIRCAMP initiative which is initiated by the European Chief of Police Task Force and is solely aimed at combating organized criminal groups behind commercial sexual exploitation of children.

These partnerships together with the database already created by the unit have enabled the website filtering initiative to filter access to over 7000 sites.

The list is reviewed monthly, manually, to ensure that it is up to date and that the possibility of a false positive filter due to the list is removed.

Additional procedures have been built around the list to ensure that the security of it and the contents of it cannot change without the consent of at least 3 Censorship inspectors.

Additionally we also have access to the Chief Censor who is able to provide expert decision on any matter that require further clarification.

Overall Output:

The testing of this system showed it to be in its pure form a very simplistic but efficient mechanism for filtering this type of material. The system performed well in all tests and highlighted its ability to scale; the Censorship Compliance Unit will be seeking additional funding to move to a final production system in the first quarter of 2009.

Based on the test results the Censorship Compliance Unit would endorse any system based on the one trialed.

For the Netclean or any web filtering system to be successful the enforcement agencies need to be able to share intelligence on the sites identified hosting this material. This is something that the Censorship Compliance Unit is seeking to expand on and currently achieve with our relationship with CIRCAMP[8] and CSAADF[9].

Background on the Unit:

The Censorship Compliance Unit operates out of the Department of Internal Affairs. The unit is responsible for enforcing the Film, Videos and Publications Classification Act.

The unit is a dedicated team within New Zealand actively investigating internet offences against children. It has been active in this area since 1996.

It is both proactive in its own investigations and in supplying intelligence and acting on intelligence with overseas jurisdictions.

[8] European Chief of Police Task Force and is aimed at combating organized criminal groups behind commercial sexual exploitation of children

[9] The Child Sexual Abuse Anti Distribution Filter is an filtering initiative operated by Norway