Australian Government

Department of Broadband,
Communications and the Digital Economy

INTERNET SERVICE PROVIDER CONTENT FILTERING PILOT

TECHNICAL TESTING FRAMEWORK

November 2008

Contents

1. Introduction

The purpose of the live ISP level filtering Pilot is to explore a number of possible filtering implementation models in order to inform Government policy.

The documentation relating the live Pilot is non-prescriptive in recognition of the fact that the participation of particular ISPs in the live Pilot will be negotiated on a case by case basis.

ISPs are invited to participate in the Pilot through two streams:

1. Index filtering only of the Australian Communications and Media Authority (ACMA) blacklist of prohibited URLs; or
2. The ACMA blacklist plus additional filtering e.g. more extensive index filtering through to dynamic filtering of other unwanted internet content and non web based applications.

The Pilot is seeking to test a range of filtering solutions, using as a minimum filtering based on the ACMA blacklist. If a number of ISPs wish to participate in the Pilot to trial a number of different filtering solutions, their inclusion will be facilitated. We note that some ISPs already provide such filtering solutions and we would welcome participation by those ISPs, as well as ISPs who wish to trial the introduction of a filtering service.

Internet content filter providers can only participate via an operating ISP. The basis of participation of particular ISPs in the live Pilot will be negotiated on a case by case basis.

The Pilot test will be conducted on behalf of the Department by Enex TestLab.

Note that the ACMA blacklist is compiled on a URL basis. As part of the Pilot, the Department wants to consult with individual ISPs on the approach they would want to take. Ideally, we would like to test different approaches to filtering of the ACMA blacklist including IP based, URL based, or a combination of the two as has been adopted by British Telecom.

General Requirements

Wherever possible equipment will be configured to enable Enex test engineers to access the solutions remotely; this may obviate the need for physical access to an ISP's premises. Enex will need adequate information concerning the ISP's network and the configuration of their filtering solution within that network. Access to technical staff and additional information to enable the collection of robust data may be desirable but will be negotiated with ISPs on a case by case basis.

To undertake testing of an ISP's filtering solution it is proposed that Enex TestLab be provided with access to a sample filtered service and, ideally a sample unfiltered service.

For "unique" filtering solutions a face-to-face demonstration with the ISP and/or their chosen filter vendor partner may be required.

Access to technical staff and additional information to enable the collection of robust data may be desirable but will be negotiated with ISPs on a case by case basis.

Ideally, a participating ISP would provide a filtering solution to a sample of their customer base. Enex would then be provided with a sample filtered service and ideally a sample unfiltered service from the same participating ISP. If this is not feasible, a 'before filtering' and 'after filtering' approach may be used.

While customers may volunteer for the Pilot, during their participation they would not be aware at any particular point in time of whether or not they are receiving a filtered service, depending on the kind of filtering solution being tested.

2. The Pilot

The live Pilot will seek to obtain over time regular snapshots of filtered and unfiltered performance covering representative samples of each participating service.

To the extent possible, the aim is to test a range of different types of filtering including:

- ACMA blacklist filtering only (for a blacklist of up to 10,000 URLs); or
- ACMA blacklist filtering plus the filtering of other content using different approaches to filtering which would, for example, include:
    - Index filtering of different sized blacklists;
    - Dynamic analysis filtering;
    - IP versus URL filtering;
    - DNS poisoning.

The Pilot seeks to test a wide range of filtering solutions and is deliberately flexible.

It is acknowledged that the correlation and comparison of data between different filtering solutions would need to be carefully considered.

The specific filtering solutions proposed, and the size of the customer base to be filtered, is a matter for negotiation with the applicants. However, all participants in the Pilot must, at a minimum, filter the ACMA blacklist.

For each type of filtering solution, the Pilot will seek information on:

- Impact on network speed from the perspective of both the user and the ISP.
- Accuracy or over and under blocking.
- Relative ease of circumvention.
- Ease of use from a user perspective (and privacy/security from a user perspective).
- Costs associated with introducing ISP filtering.
- Scalability (i.e. scalability refers to the expectation that some ISPs will want to participate in the Pilot on a sample only basis. Moreover, there is also a question of whether the filtering solutions of some smaller ISPs could be scaled up for higher levels of traffic).
- Effectiveness of any additional functionalities of the filter product.

Note that access to a filtered service will enable Enex to evaluate the performance impact of a filtered service from the end user's perspective. Additional information from the ISP may be needed to evaluate the overall impact on the ISP – this will be discussed on a case by case basis.

A key component of the Pilot is scalability. The Pilot is, however, limited to the networks and filtering solutions of the participants and their willingness to provide relevant technical information.

Ideally the Pilot will involve a representative cross section of the industry, for example tier 1, 2 and 3 ISPs, metropolitan, regional and remote ISPs including mobile, wireless and satellite internet service providers and broadband and dial up customers. The basis of participation of particular ISPs in the live Pilot will be negotiated on a case by case basis.

3. Network Performance

Network performance can be affected by the introduction of content filtering technologies. This component of the Pilot will seek to ascertain the performance impact of the introduction of the range of ISP filtering approaches on the internet end-user experience, and seek to discover the impact on the service providers' overall network.

The availability of this information is obviously dependent on the level of engagement of participating ISPs.

To the extent possible the Pilot will seek to give consideration to emerging internet delivery technologies, for example IPv6. The ability of the Pilot to assess filtering within such environments is dependent on an ISP proposing to participate with such a delivery system.

The Pilot will seek to test this in a live environment.

Potential technologies/platforms to be considered for testing (scenarios)

The Pilot aims to assess delivery across a variety of internet delivery mediums (wireless and copper to HFC) ranging in speed from 56Kbps through to 12Mbps. Consideration (i.e. an assessment or examination) will also be given to future internet network performance above 12Mbps. To participate in the Pilot an ISP is not expected to deliver internet services across all mediums.

Testing Framework

The ACMA blacklist is compiled through a complaints-based system. The list is dynamic, and at the time of writing comprised approximately 1300 URLs. The majority of the blacklist consists of material that would likely be classified RC (Refused Classification) by the Classification Board.

This blacklist of child sexual abuse material may increase in size, initially through the addition of internationally available blacklists. It is estimated that the addition of these lists may take the total of URLs to up to around 10,000. It should also be noted that this is also expected to fluctuate over time.

Performance will be measured in Kbps/Mbps, latency tests will be included as well as data performance results.

Ideally a snapshot of simultaneous filtered and unfiltered performance on identical representative samples of the service providers' internet service will be captured at regular intervals over a period of time (e.g. six times a day over four weeks). This will be negotiated on a case by case basis with participating ISPs. The focus of the trial will be at the end user level, although ideally information would also be made available on upstream performance.

Note that:

- All participants in the Pilot must, at a minimum, filter the ACMA blacklist for all participating customers.
- Blacklist testing will be undertaken against the ACMA blacklist as well as an expanded blacklist to account for its future augmentation in relation to child pornography material.
- It is highly desirable that there are individual user and/or management controls (to switch filtering on/off) of the solution, for the purposes of the testing.
- Provision of both filtered and unfiltered sample service for comparative testing is highly desirable.

4. Accuracy

Accuracy relates to the end-user experience when attempting to access blocked content.

The Department is interested in evaluating mechanisms to address over-blocking, including through end user reporting, where a participating ISP is willing to trial such a mechanism. This includes the end-user's ability to report sites that they believe have been blocked incorrectly and vice-versa (reporting sites that they feel should be blocked).

Key considerations when evaluating accuracy will be to identify under blocking (i.e. content that should be blocked) and over blocking or false positives (i.e. blocking content that should be passed).

Note that ACMA would be responsible for maintaining the accuracy of the ACMA blacklist.

Testing Framework

Enex will be provided with a filtered internet connection from the participating ISP. Using this filtered connection URLs will be passed through Enex TestLab's *URL eTest Pro* Module. In addition the filtered connection will be assessed against ACMA's Black list, augmented black lists, additional category URL lists and false positive URL lists.

This testing framework can equally cover both the list and dynamic analysis filters.

Granularity of control over the filtering solution, individual user or management controls (on/off) of the solution are highly desirable. Provision of filtered/unfiltered sample services for testing is also important.

Note that the particular role of Enex TestLab will be determined on a case by case basis with the participating ISP. The level of cooperation of ISP and associated Internet Content Filter (ICF) vendors with the Pilot team is critical.

5. Circumvention

It is acknowledged that filtering can be circumvented by motivated people with a sufficient level of technical knowledge.

The Pilot will seek to test the ease with which different filtering solutions can be circumvented and the capacity of filters to detect and provide warnings on circumvention attempts.

Testing Framework

A number of techniques that could be used to bypass ISP based content filters will be selected and applied to each filter in the Pilot. Results will be recorded and alert/alarm/detection mechanisms reviewed. The time taken, and the level of skill/knowledge needed to achieve bypass, if successful, will also be recorded.

Circumvention testing will not involve intrusion into an ISP's network and will not involve tracking/logging of end users' internet use. This component of the Pilot will also not include destructive techniques such as compromising the ISP network infrastructure or Denial of Service (DoS or DDoS) attacks. Brute force attacks will also be excluded.

It is envisaged that this will involve common circumvention techniques (e.g. use of proxies) and the measures that a filtering solution has in place to address these.

6. User experience of filtering (including privacy/security issues)

The end-user should ultimately be the beneficiary of any technology solution. It is crucial that whenever introducing or evaluating a technology solution that the end-users' requirements are taken into consideration. User experience testing in this process leads to the end-user having a better experience and acceptance of the solution. This is applicable to content filtering technologies.

Testing Framework

A series of simple surveys (preferably electronic – e-mail or web) will be created around a range of criteria designed to ascertain and receive feedback from the end-users participating in the Pilot (considering key criteria such as performance, ease of use, perceptions of under and over blocking etc).

Ideally the surveys will be sent at regular intervals over a period of time during the Pilot, end-users will not know if their system is or is not being filtered and they will all be asked to respond to the same questions.

The surveys will be short, succinct and not too onerous for the participants to complete. Set tasks can also be incorporated into the surveys to see if the end-users can discern any differences between their experience in filtered and un-filtered environments.

The surveys will be compiled and undertaken in such a way as to minimize any impact on ISPs and their end users. Whether customers are surveyed, how they will be surveyed and whether an ISP participates in this component of the Pilot will be discussed on a case by case basis with the participating ISP.

Testing tools may be used to direct remote users to perform these tasks and to ask for their results/thoughts etc.

ISPs and their end-users confidentiality and privacy will be maintained. The minimum amount of end-user personal information as possible will be gathered.

7. Costs associated with introducing ISP filtering

Costs include capital expenditure (up-front) to acquire the technology and implement it, and operating expenditure (ongoing) costs to maintain the solution. These costs vary depending on the size and complexity of:

a) the size/scale of the organisation using the system (and their processes/procedures);

b) the type of solution chosen; and

c) the manner in which a solution is deployed.

Testing Framework.

Taking a representative sample of known environments, (small and large ISP infrastructure systems and varying technologies and geographies), hypothetical scenarios will be created. Enex TestLab will take these scenarios and request information from ICF vendors.

Enex TestLab will also request and/or research information on cost analysis research that has been undertaken previously by vendors and/or other parties.

Actual costs of filtering will be gathered as part of the Pilot and will be the result of the particular filtering solution deployed within the particular participating ISP's network. In particular, information will be gathered by participating ISPs and ICF vendors – this will show approximate operating expenditure when managing and maintaining ICF solutions. Results can be reported in cost per x number of users, for each scenario.

8. Scalability

It is understood that ISPs have a commercial imperative to ensure that their network is up and running (availability) consistently with the least amount of downtime (outages).

All responsible ISPs ensure that the technical architecture, planning and deployment of their service delivery network are robust and reliable. In most cases this is assisted with the deployment of telecommunications "carrier" grade technologies and equipment

specifically designed for continuous running, in-line maintenance, high availability, fault tolerance and redundancy in core systems.

Adding a content filter to this environment needs to be given the same level of planning. This is a key requirement when assessing the technologies/solutions/vendor selected by the ISP. Aspects to this are scalability, availability, fail over etc.

Additional considerations include ease-of-installation, configuration, administration and ongoing management. Some larger deployments will involve remote "nodes" that require centralised management systems.

Potential technologies/platforms to be considered for testing (scenarios)

A variety of internet delivery mediums (wireless and copper to HFC) ranging in speed from 56Kbps through to 12Mbps may be selected. Consideration will also be given to future internet network performance above 12Mbps.

Testing Framework

The vendor's product claims in relation to installation, configuration, ongoing management, administration, availability and scalability will be requested and analysed.

Consideration will be given, but not limited, to aspects such as:

- Maximum number of URLs supported by the solution as deployed at that individual ISP.
- Manner in which the solution has been configured.
- Redundancy in the systems and technologies.
- Upgrade paths available to handle higher speeds, increased traffic, alternate internet delivery technologies and increased list sizes.

External reports produced by third parties and / or vendors in relation to the capabilities of their products. Vendor / Analyst reports will be treated as marketing information and considered as an unverified / unsubstantiated claim.

Should any technical claim in the presented documents appear false / incorrect or beyond expectations then Enex TestLab may run a sub-test to examine and test those claims.

Tests will be conducted to take into account the ability for the products to maintain their benchmarked performance scaling up from the ACMA blacklist (approximately 1300 URLs), through to a predetermined number of sample services. Scalability to larger lists will be taken into consideration (this may require offline laboratory testing to determine maximum load before significant solution degradation is observed).

9. Effectiveness of additional filter functionalities

Where filtered services offer additional functionalities, these will also be considered in terms of the factors listed above.