practeo
ingénierie informatique

NetClean™ | WhiteBox™

Abusive web filtering for ISP's

swinog
swiss network operators group

October 22, 2008
Bern

IN A GLANCE

- a hybrid solution using BGP
- using IP tunnels
- doing packet inspection
- using a clever redirection mechanism

- based on several blacklists
- robust & flexible
- easily deployed and managed

NetClean | WhiteBox
Abusive web filtering
for ISP's

BACKGROUND AND PURPOSE

- **Social responsibility.**

  A stand against child pornography is proof that your organization adopts and lives up to commonly recognized values.

- **Common initiative**

  Reduce the occasions when innocent internet users might be exposed to traumatic and unlawful images.
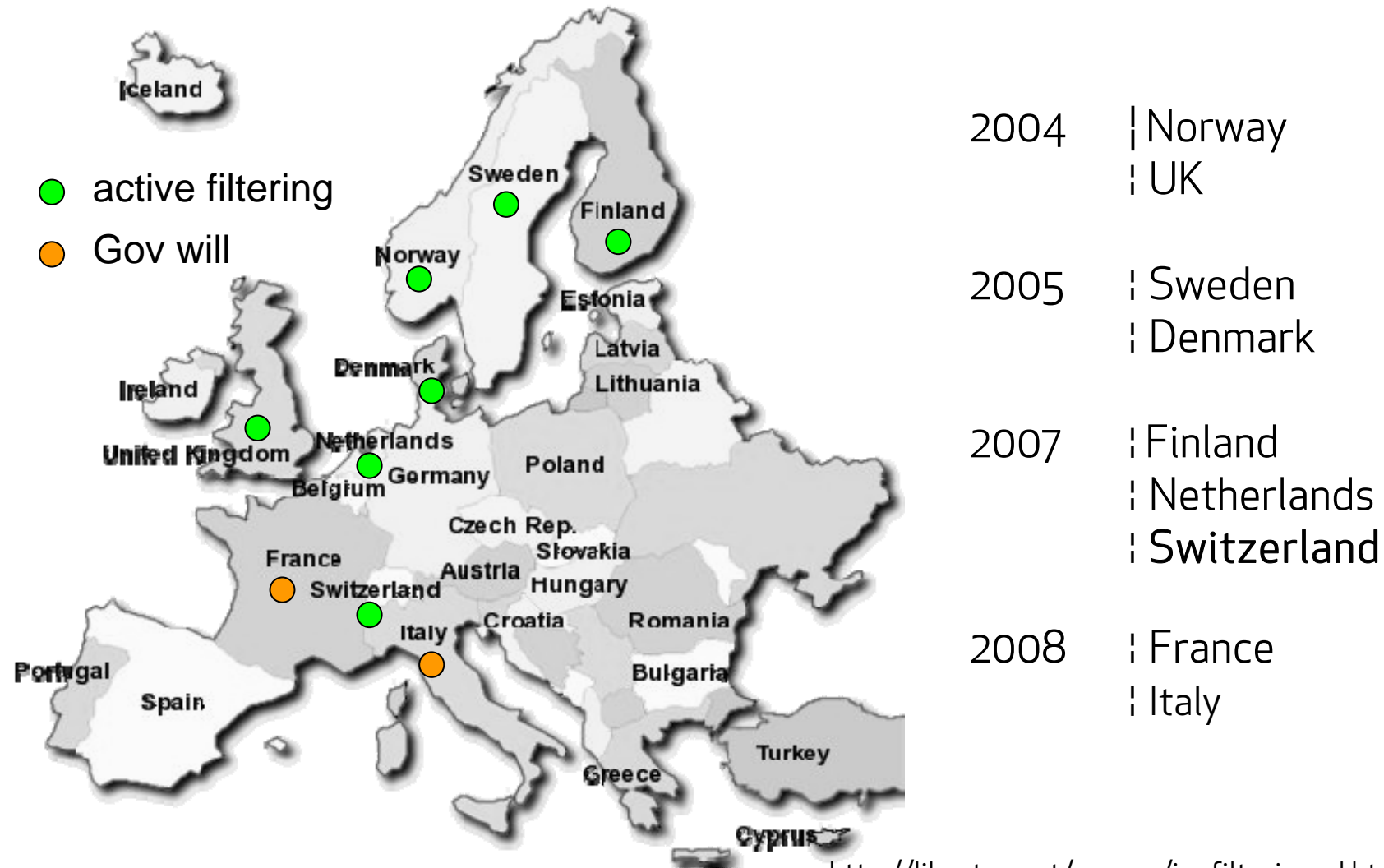
  Diminish the re-victimisation of children by restricting opportunities to view their sexual abuse.

  Disrupt the accessibility and supply of such content to those who may seek out such images.

NetClean. | WhiteBox.
Abusive web filtering
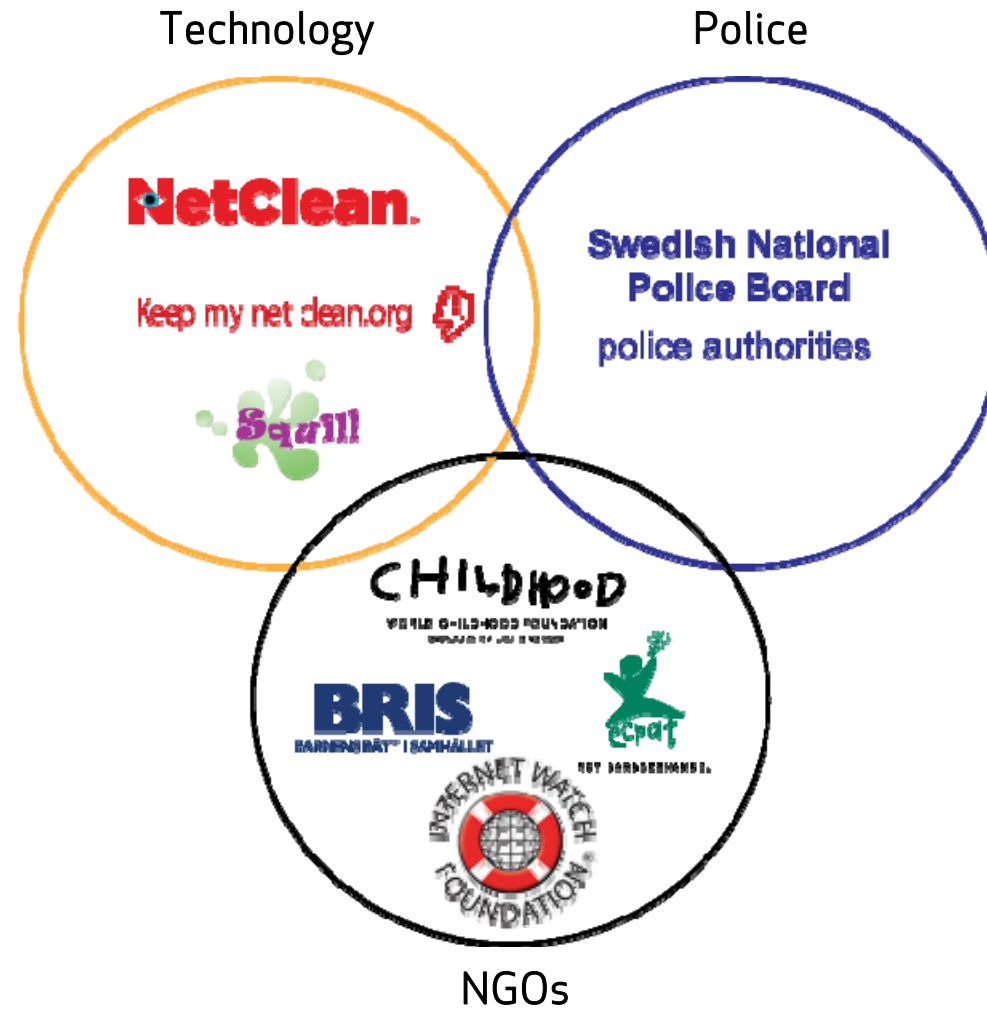for ISP's

LEGAL BACKGROUND

- Possession of child pornography is **against the law** (art. 197 CPS), exception for Internet temporary files (cache)

- In 2010, a law to punish surf on child porn websites should be edicted by the government (based on motion PRD Schweiger)

- Although it is illegal for an operator to track and store information about who makes the accesses, it is possible to **block the traffic accessing illegal content**.

- **Long run** before potential closing of child porn websites

NetClean | WhiteBox
Abusive web filtering
for ISP's

ONGOING TREND IN EUROPE

- 🟢 active filtering
- 🟠 Gov will

2004 ¦ Norway
     ¦ UK

2005 ¦ Sweden
     ¦ Denmark

2007 ¦ Finland
     ¦ Netherlands
     ¦ **Switzerland**

2008 ¦ France
     ¦ Italy

http://libertus.net/censor/ispfiltering-gl.html

PARTNER ORGANIZATIONS

NetClean | WhiteBox
Abusive web filtering
for ISP's

PARTNER BLACKLISTS

Polisen
- Provided by the Hotline
- Updated every month

Internet Watch Foundation
Since 2004
- Visual check of each URLs by 2 people
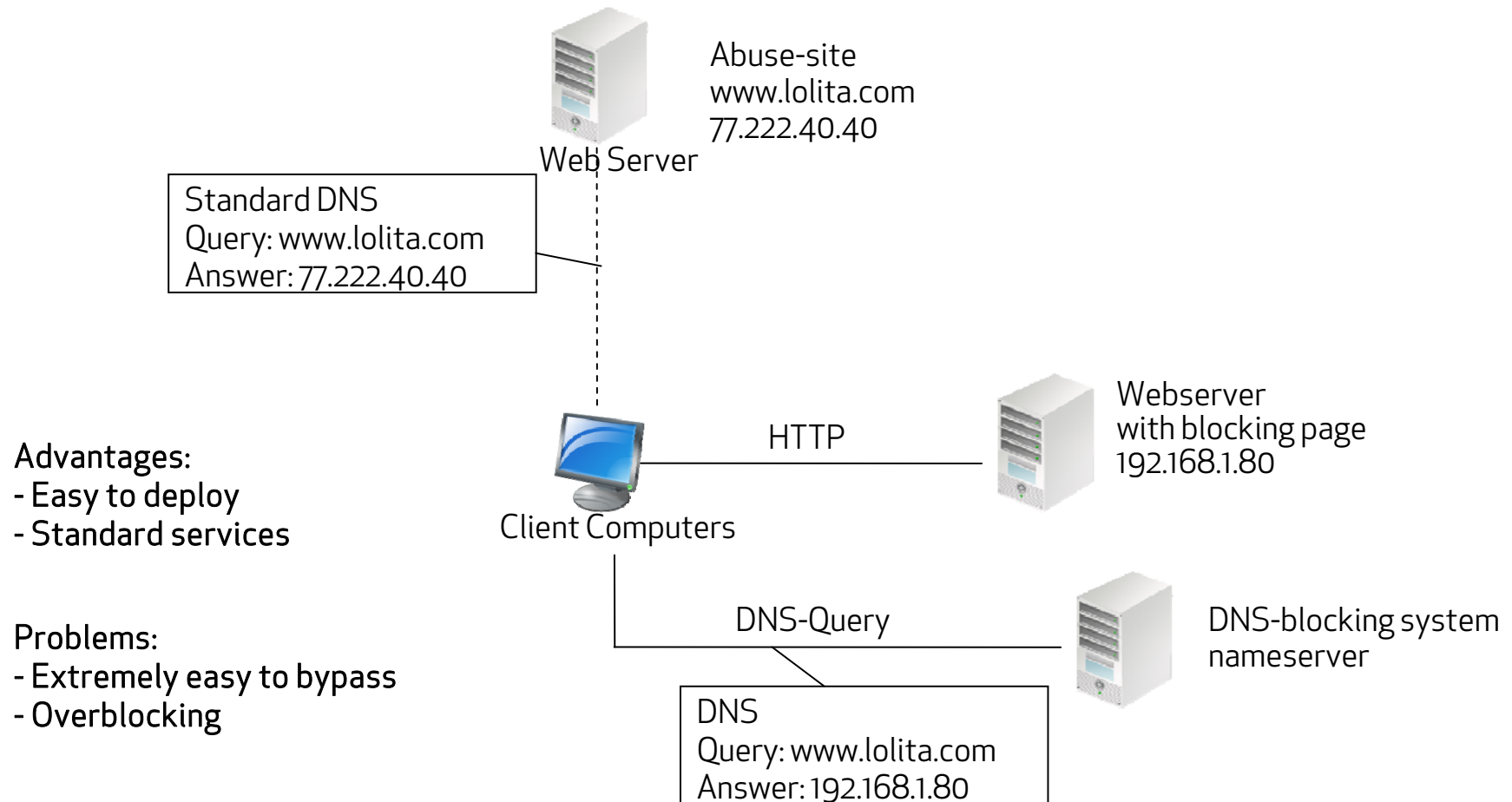- Full URLs up to the actual picture
- Updated twice a day
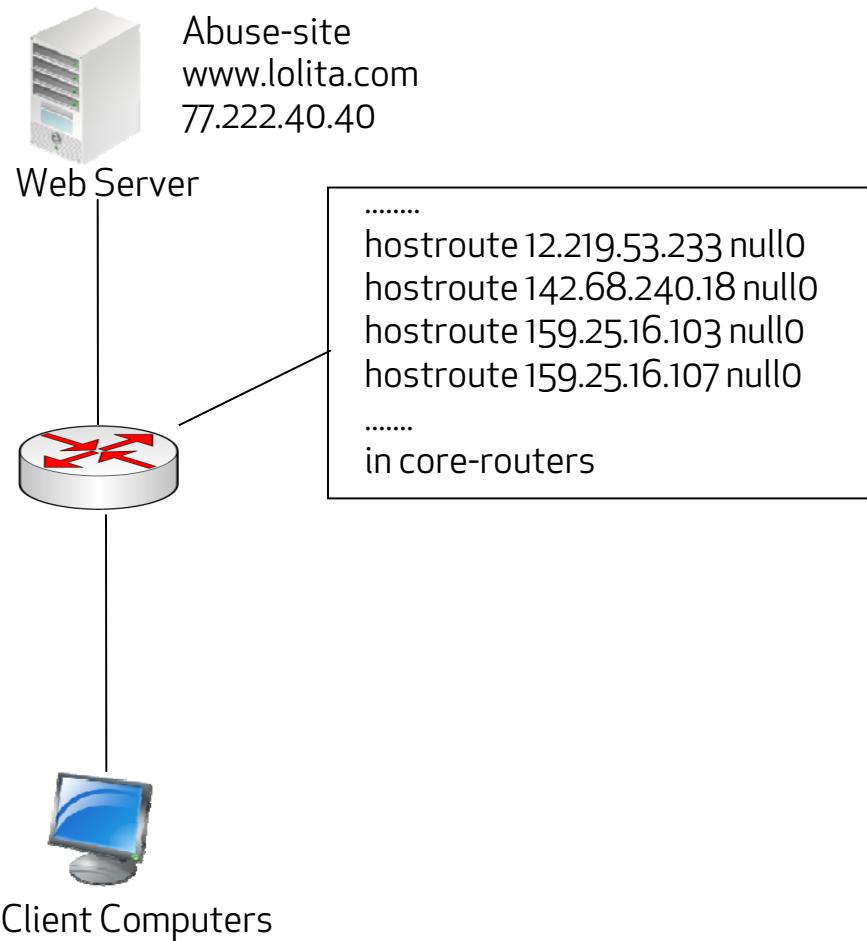
FAQs : www.iwf.org.uk/public/page.148.437.htm

KOBIK SCOCI CYCO
- Visual check of each URLs
- Domain name
- under discussions

NetClean | WhiteBox
Abusive web filtering
for ISP's

DNS BLOCKING (DNS POISONING)

Abuse-site
www.lolita.com
77.222.40.40

Web Server

Standard DNS
Query: www.lolita.com
Answer: 77.222.40.40

HTTP

Webserver
with blocking page
192.168.1.80

Client Computers

Advantages:
- Easy to deploy
- Standard services

DNS-Query

DNS-blocking system
nameserver

Problems:
- Extremely easy to bypass
- Overblocking

DNS
Query: www.lolita.com
Answer: 192.168.1.80

IP FILTER

practeo
ingénierie informatique

Abuse-site
www.lolita.com
77.222.40.40

Web Server

....
hostroute 12.219.53.233 null0
hostroute 142.68.240.18 null0
hostroute 159.25.16.103 null0
hostroute 159.25.16.107 null0
....
in core-routers

Advantages:
- Extremely easy to deploy

Problems:
- Extremely crude
- Massive overblocking

Client Computers

URL FILTERS

Web Server

....
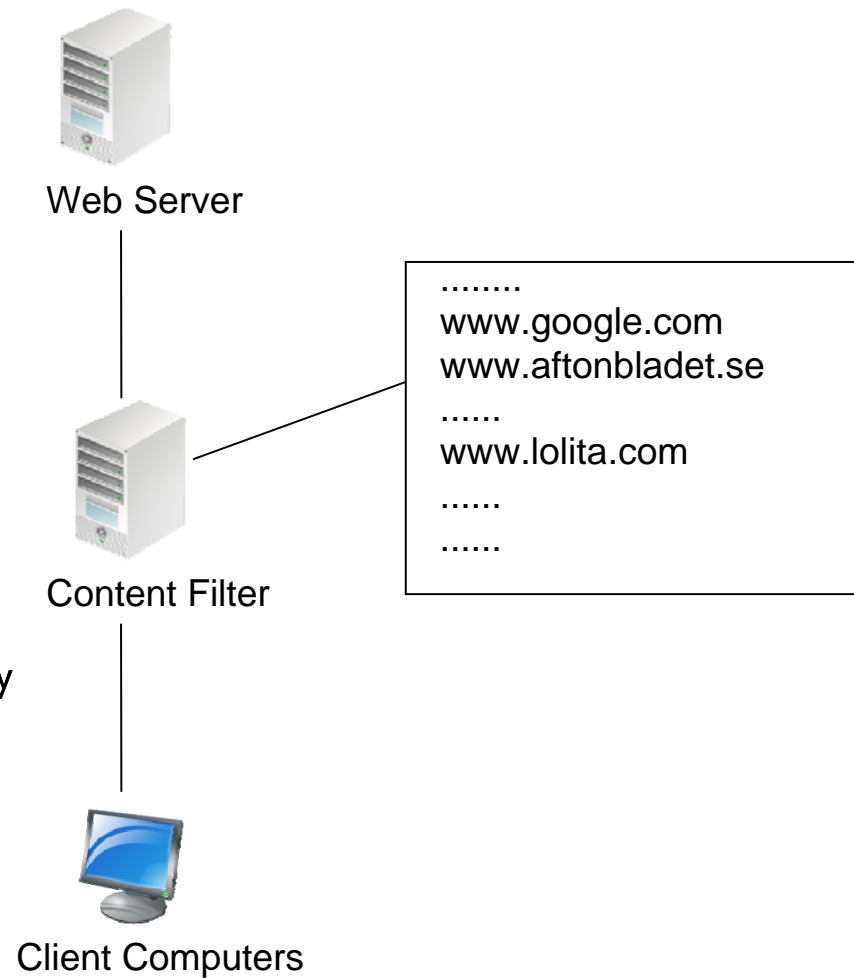www.google.com
www.aftonbladet.se
......
www.lolita.com
......
......

Content Filter

Advantages:
- Very accurate

Problems:
- Almost impossible to deploy in reality
- Requires deep packet inspection

Client Computers

HYBRID BLOCKING - OVERVIEW

http://abozar.tripod.com/adm/ad/toolbar.css
http://abutril.no.sapo.pt/adm/redirect/photo/photo/img/print_icon.gif
......
......
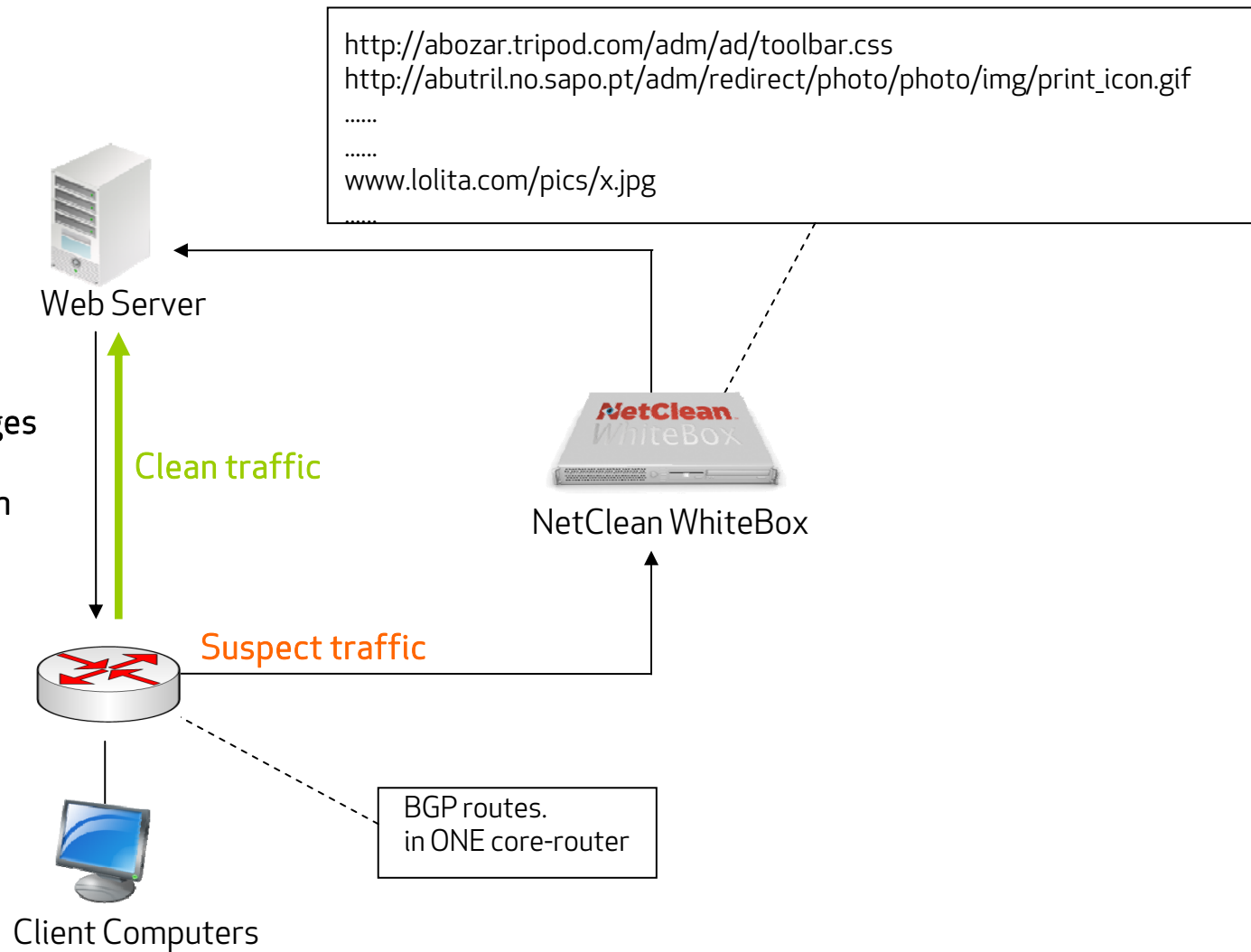www.lolita.com/pics/x.jpg
......

Web Server

Advantages:
- Combines the advantages of IP and URL-filter
- Very acurate, can match whole URL's
- Easy to deploy
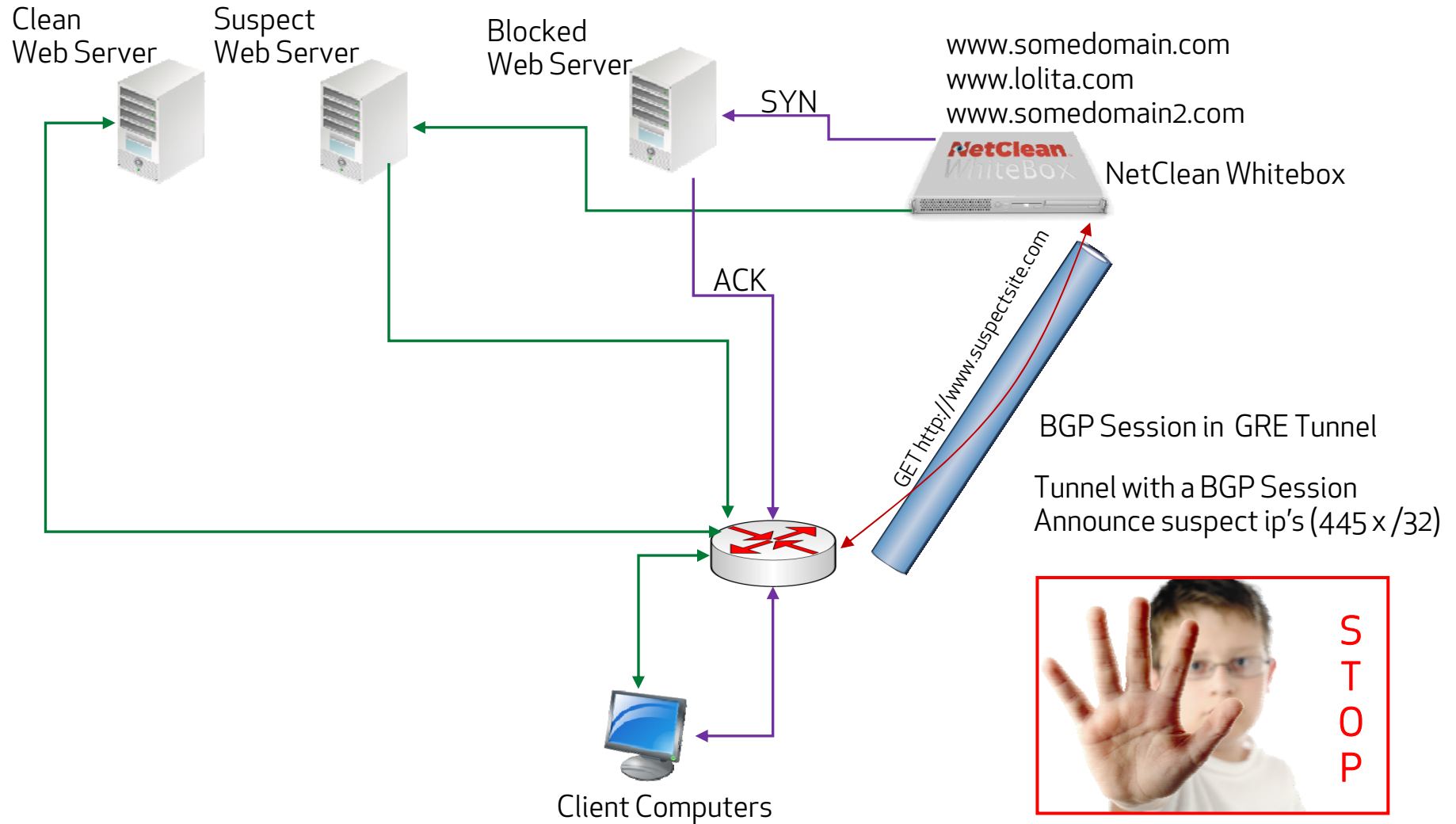- No overblocking at all
- No proxying

Clean traffic

Filtering proxy

Suspect traffic

....
hostroute 12.219.53.233 filtering_proxy
hostroute 142.68.240.18 filtering_proxy
hostroute 159.25.16.103 filtering_proxy
hostroute 159.25.16.107 filtering_proxy
....
in core-routers

Client Computers

WHITEBOX - ONSITE

http://abozar.tripod.com/adm/ad/toolbar.css
http://abutril.no.sapo.pt/adm/redirect/photo/photo/img/print_icon.gif
......
......
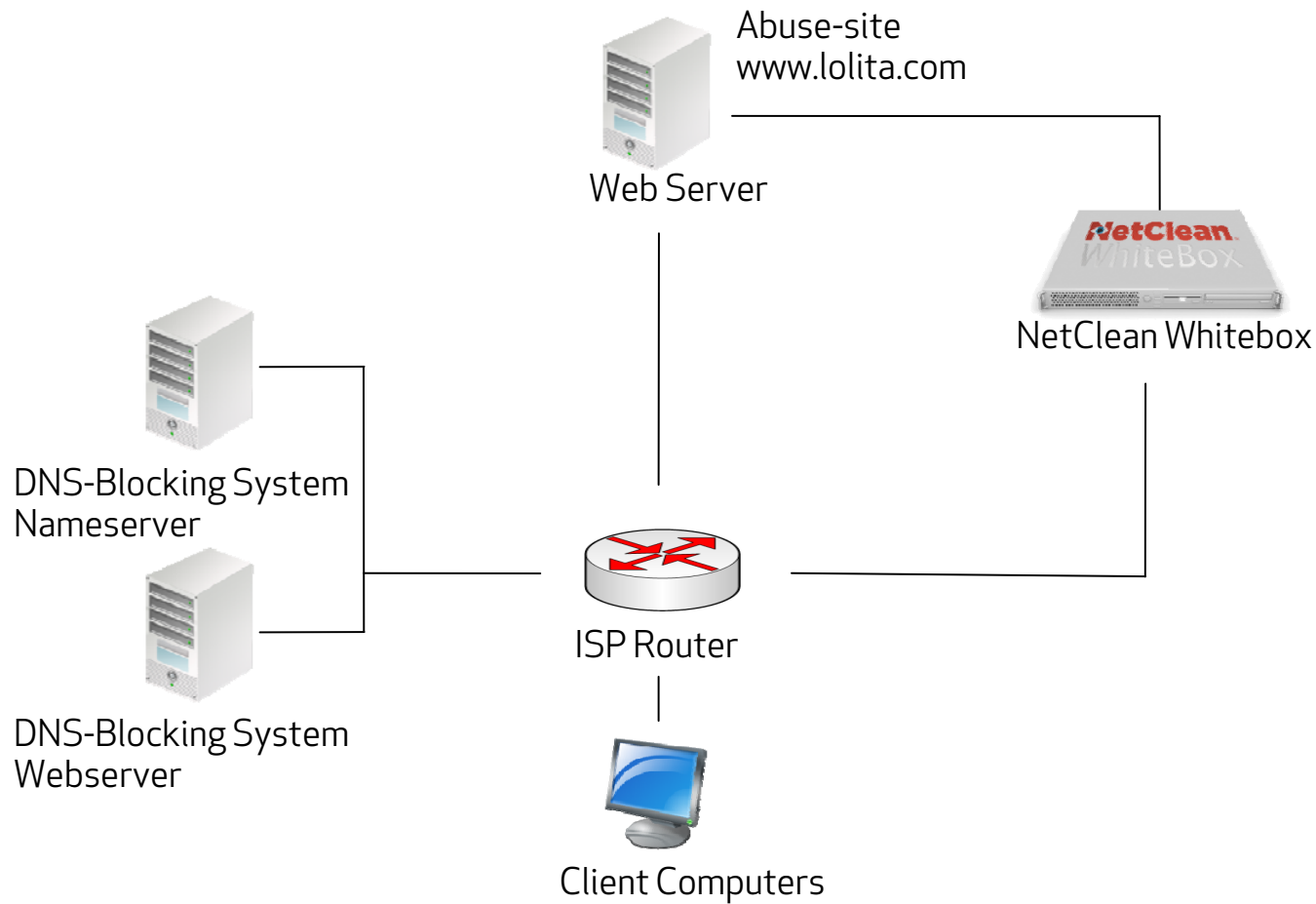www.lolita.com/pics/x.jpg
......

Web Server

Advantages:
- Combines the advantages of IP and URL-filter
- Very acurate, can match whole URL's
- Easy to deploy
- No overblocking at all
- No proxying

Clean traffic

NetClean WhiteBox

Suspect traffic

BGP routes.
in ONE core-router

Client Computers

NetClean | WhiteBox
Abusive web filtering
for ISP's

WHITEBOX – HOSTED

Clean
Web Server

Suspect
Web Server

Blocked
Web Server

www.somedomain.com
www.lolita.com
www.somedomain2.com

SYN

NetClean Whitebox

ACK

GET http://www.suspectsite.com

BGP Session in GRE Tunnel

Tunnel with a BGP Session
Announce suspect ip's (445 x /32)

S
T
O
P

Client Computers

NetClean | WhiteBox
Abusive web filtering
for ISP's

HYBRID BLOCKING
THRU NETCLEAN WHITEBOX

- Combines the advantages of IP and URL-filter

- Very accurate, can match whole URL's

- Easy to deploy

- No overblocking at all

- No proxying

- Hosted or Onsite Solution

NetClean | WhiteBox
Abusive web filtering
for ISP's

PROOF OF CONCEPT

Time frame

SUNET	(filtering between 12/2005 to 12/2007)
PORT80	(filtering between 08/2006 to 12/2007)
DGC	(filtering between 08/2006 to 12/2007)
CH_ISP	**(filtering between 08/2008 to 10/2008)**

Conclusions

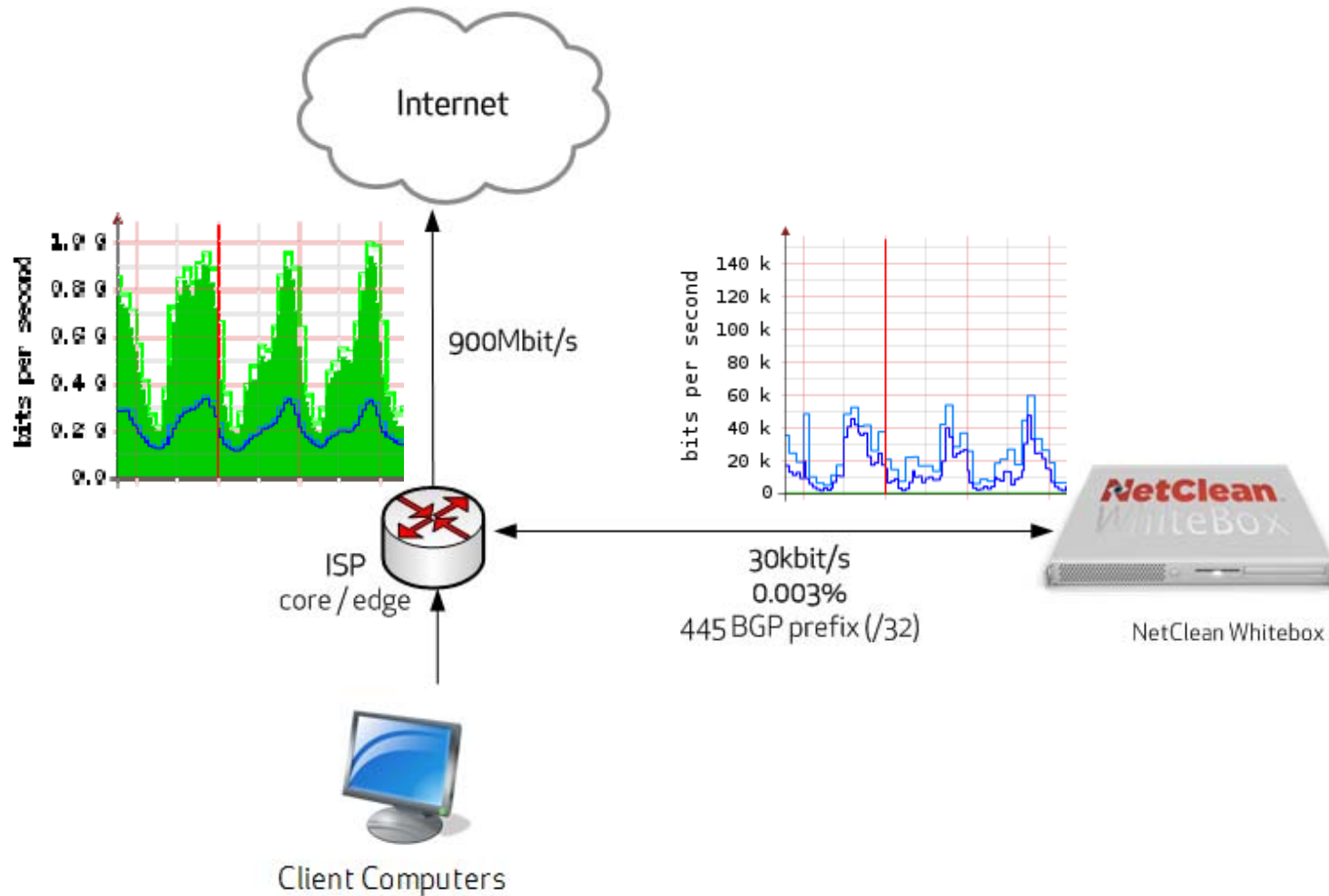|	
SUNET	approximately 2200 blocks per day occured,
PORT80	approximately 3300 blocks per day occurred
DGC	had 300 per day
CH_ISP	**had 2000 detections per day.**

PROOF OF CONCEPT

A deeper study of SUNET was made, where the filter was installed but not blocking anything for a month, and with the same setup the blocking was activated for a month, **800 out of 60.000 users accessed child pornography URLs,**

This means that around **1%** of the users were actively seeking for child pornography.
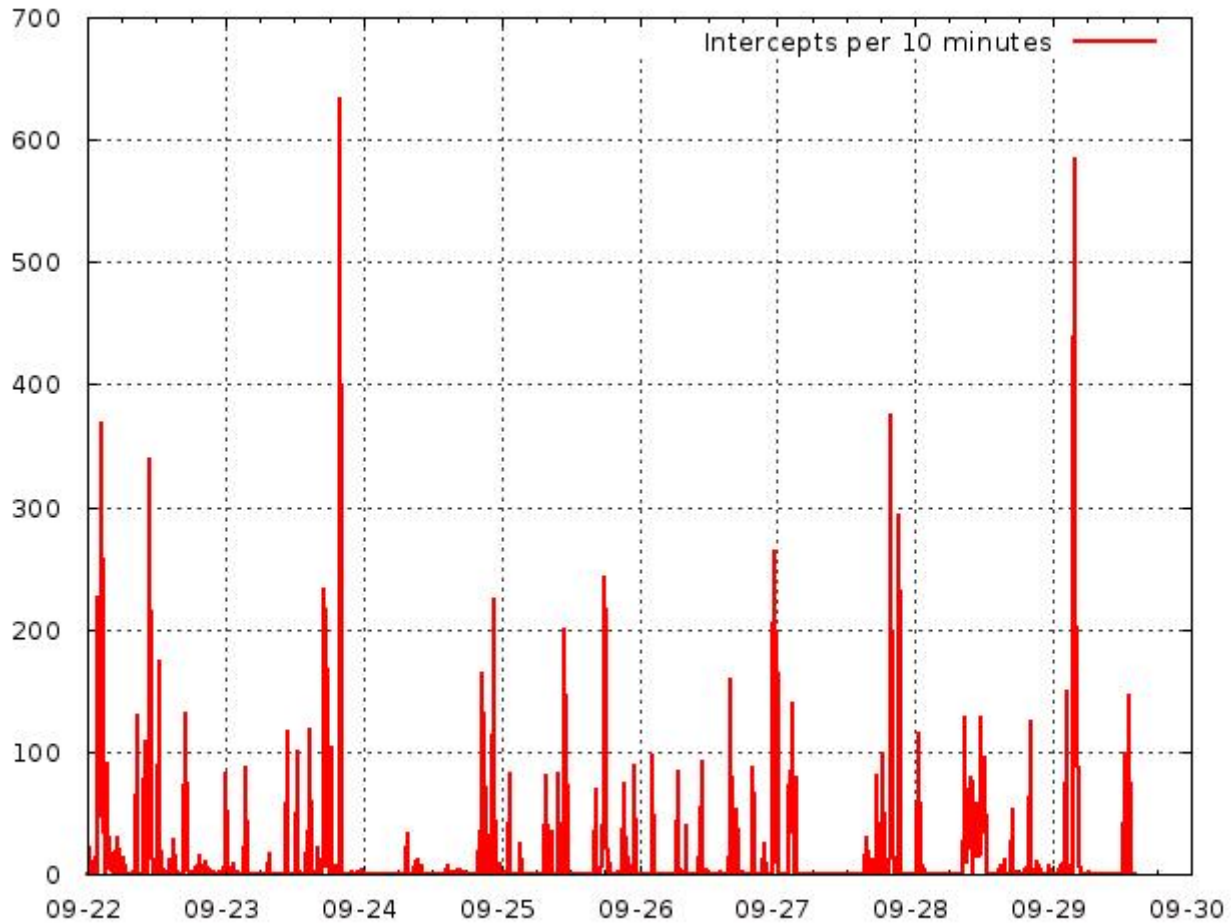
The number of people trying to **access black-listed URLs did not decrease even after the filter was installed.** The same number of users were seeking child pornography, but with less frequency due to active filtering.
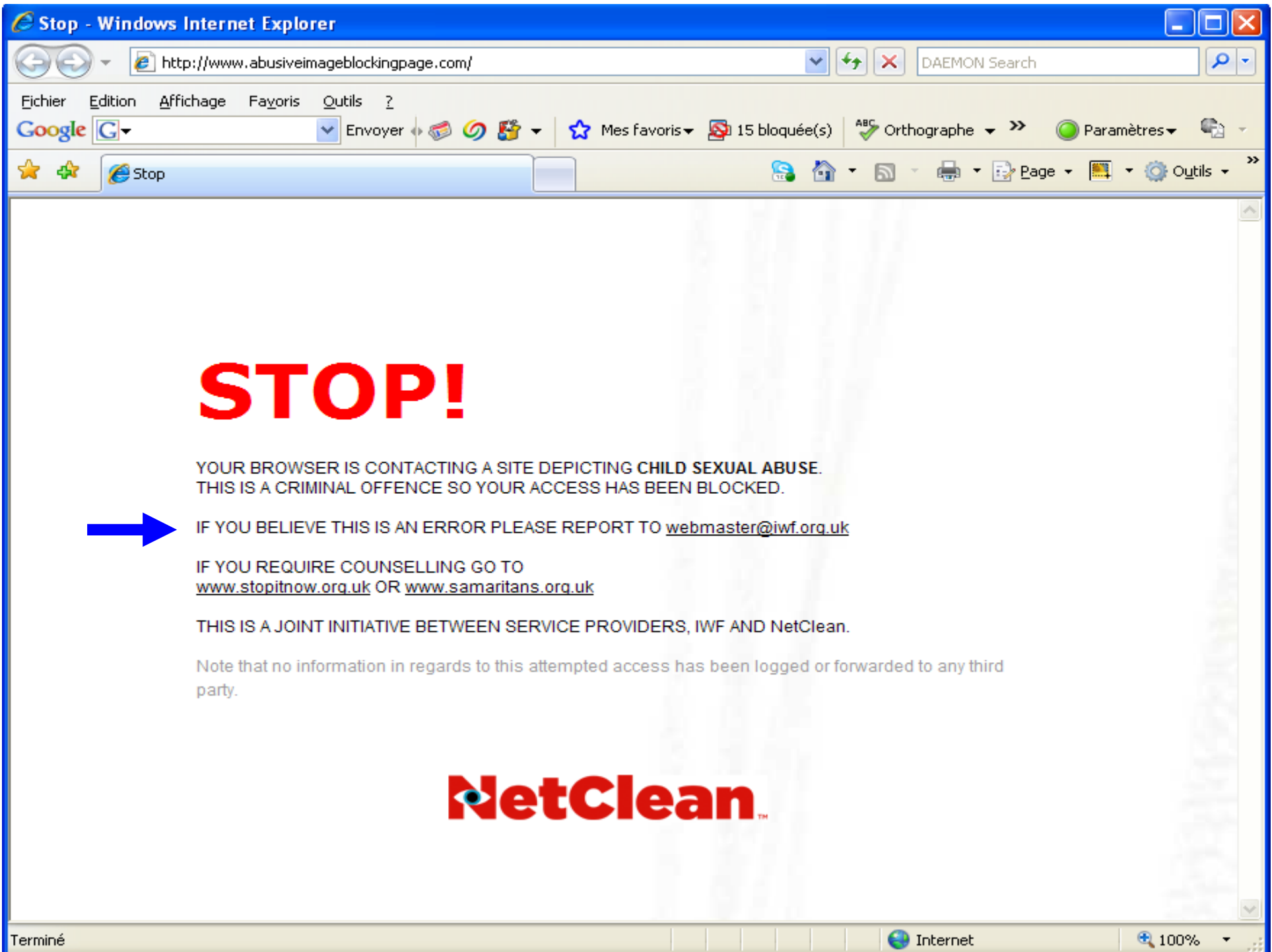
NetClean | **WhiteBox**™
Abusive web filtering
for ISP's

http://www.abusiveimageblockingpage.com/

DAEMON Search

Fichier   Edition   Affichage   Favoris   Outils   ?

Google [G▾]   ▾ Envoyer ◆ 🔴 🟢 🔲 ▾   ☆ Mes favoris▾   🚫 15 bloquée(s)   ABC Orthographe ▾ »   🟢 Paramètres▾ 🔵 ▾

☆ ☆   🟦 Stop   🔵 🏠 ▾ 🔷 ▾ 🖨 ▾ 📄 Page ▾ 🖼 ▾ 🔵 Outils ▾ »

STOP!

YOUR BROWSER IS CONTACTING A SITE DEPICTING **CHILD SEXUAL ABUSE**.
THIS IS A CRIMINAL OFFENCE SO YOUR ACCESS HAS BEEN BLOCKED.

IF YOU BELIEVE THIS IS AN ERROR PLEASE REPORT TO webmaster@iwf.org.uk

IF YOU REQUIRE COUNSELLING GO TO
www.stopitnow.org.uk OR www.samaritans.org.uk

THIS IS A JOINT INITIATIVE BETWEEN SERVICE PROVIDERS, IWF AND NetClean.

Note that no information in regards to this attempted access has been logged or forwarded to any third party.

NetClean.

Terminé   🌐 Internet   🔍 100% ▾

Whitebox: Settings - stop site - Mozilla Firefox

Arkiv   Redigera   Visa   Historik   Bokmärken   Verktyg   Hjälp

file:///tmp/whiteboxtunnel.netclean.com/sitelist.html

Google

WebMail   Calendar   Radio   People   Yellow Pages   Download   Customize...

Whitebox: Settings - stop...

NetClean.

user1

Start

tunnelserver3.netclean.com

Site statistics

Settings

Changelog

Site list

Most blocked sites in descending order.

Label SOME-ISP ▼   LIST

Host   SEARCH

Top 50 Blocked Sites for SOME-ISP (obfuscated for demo)

Site	Intercepts	Last
xxx.lolalists.xxx	14415	2008-09-22 02:45:02
xxx.sexypix.xxx	6420	2008-09-29 03:55:02
xxx.thaimisc.xxx	3923	2008-09-29 04:15:02
xxx.multiguestbook.xxx	3531	2008-09-29 19:25:02
xxx.greatestsites.xxx	3240	2008-09-29 03:55:02
xxx.allpornozona.xxx	2558	2008-09-29 17:35:02
xxx.homegirl-sex.xxx	2506	2008-09-30 07:15:02
xxx.virginbeach.xxx	2498	2008-09-28 21:25:02
xxx.plola.xxx	2468	2008-09-25 18:25:01
xxx.vestalgirls.xxx	2124	2008-09-29 13:25:02
xxx.sexypix.xxx	2002	2008-09-27 21:25:01
xxx.porntours.xxx	1746	2008-09-28 19:15:02

2008 PRICING – HOSTED

Estimated number of users	Yearly cost per user
0 to 50'000	CHF 0.30
50'001 to 100'000	CHF 0.28
101'000 to 200'000	CHF 0.26
201'000 to 400'000	CHF 0.23
401'000 to 800'000	CHF 0.19
801'000 to 1'000'000	CHF 0.15
more	Call us

Support is included in the price.

2008 PRICING – ONSITE

Estimated number of users	Installation cost	Update fee (year 2)
0 to 50'000	CHF 12'000	CHF 4'500
50'001 to 100'000	CHF 22'500	CHF 7'500
101'000 to 200'000	CHF 37'500	CHF 12'000
201'000 to 400'000	CHF 66'000	CHF 22'500
401'000 to 800'000	CHF 114'000	CHF 37'500
801'000 to 1'000'000	CHF 144'000	CHF 45'000
more	Call us	Call us

Hardware cost and support is not included in the price.

practeo
ingénierie informatique

NetClean | **WhiteBox**
Abusive web filtering
for ISP's

LAST WORDS

- Implementation of NetClean doesn't just mean your networks are protected from illegal material. It means your company is **contributing to protect innocent children.**

- **Free trial for two months** using the **hosted solution** given to **SWINOG** members

NetClean | **WhiteBox**
Abusive web filtering
for ISP's

Ethical debate…

Packet Transporter   vs   Social Responsability

CONTACT US

Pascal Seeger
Project Manager
pascal.seeger@practeo.ch

Grégoire Galland
Network Engineer
gregoire.galland@practeo.ch

PRACTEO SA
Rue de la Gare 2 - 1030 Bussigny
T +41 21 706.13.35
M +41 78 850.58.06
www.practeo.ch

NetClean | **WhiteBox**
Abusive web filtering
for ISP's