



**NetClean**<sup>™</sup>

# WhiteBox<sup>™</sup>

Effectively blocks child sexual  
abusive websites on the Internet

No matter what,  
children will always  
need our protection

# Behind every abusive image there is a child who needs your help

- 3 Overview
- 6 Interface
- 10 Functional overview
- 11 System overview
- 12 Setup overview
- 14 FAQ

Router based solution for blocking URLs containing child sexual abuse images (CSAIs) in high performance networks, without affecting the ISP core and with the possibility to share one appliance among several ISPs.



## The WhiteBox



NetClean WhiteBox is a means of integrating social responsibility with successful business.

*NetClean WhiteBox is an extremely powerful tool for Internet Service Providers (ISPs) designed to block access to websites containing child sexual abuse material. NetClean WhiteBox is a hybrid solution using Border Gateway Protocol (BGP), URL inspection and a redirection mechanism that is robust. The solution is highly flexible and easily deployed and managed.*

Control access to illegal sites across multiple networks  
The NetClean WhiteBox system is designed for ISPs and Carriers who wish to block access to websites containing child sexual abuse images (CSAIs). The system can be used to block unwanted web access throughout networks or even groups of networks such as across multiple ISPs within a country or region.

is displayed instead of the requested page, otherwise the traffic is forwarded to the destination unaltered.

From a network point of view, the WhiteBox is installed as a router which announces suspected IP numbers through BGP to the core network.

### Technical description

The NetClean WhiteBox retrieves a block list and converts it into a list of IP addresses. These addresses are announced via BGP to the ISP routers with the intent of redirecting this traffic via the NetClean WhiteBox. A URL inspection device matches the requests in the traffic against the block list, and if there is a match, a block page

# Why NetClean WhiteBox?

## Quick and easy to implement

The system uses Border Gateway Protocol (BGP) to redirect the traffic. It is simply a matter of configuring a BGP session once the servers are in place.

## No effect on performance

There is no negative impact at all within the network using the NetClean WhiteBox, except adding a router hop for some destinations. The safety margins are set very high to allow peaks in the data passing through the NetClean WhiteBox.

## Flexibility with URL lists

The NetClean WhiteBox can use several block lists, and comes preconfigured with a list from the Internet Watch Foundation (IWF). It can also retrieve lists provided by customers or authorities within their region.

## Block exact URLs

The block lists can contain either sites or full URLs, which will be blocked as expected. If a site, e.g. [www.badsite.tld](http://www.badsite.tld) is in the list, everything on that site below that URL will be blocked. If the list contains an entry like [www.othersite.tld/path/to/content/pic.jpg](http://www.othersite.tld/path/to/content/pic.jpg) that particular picture will be blocked and nothing else.

## IP address checking

The IP addresses behind the URLs in the block lists are logged and kept track of to provide an effective means of filtering, since some sites often change IP addresses.

## Logging and reporting

Intercepts of requests for illegal material can be logged with different sets of detailed information, where the basic setup logs the intercepted URLs with timestamps. Depending of the legislation of the country, the IP addresses of the clients can be logged as well. A debug setting can also log all the requests that are not blocked.

## Fail-safe

A lot of safety mechanisms are built into the system to ensure that the traffic will not be disrupted if part of the system fails. In case of a total system failure the BGP will stop working, and the traffic will no longer be redirected via the NetClean WhiteBox. This ensures that the NetClean WhiteBox system can be installed on mission critical networks with full confidence.

... the availability of material depicting sexually abused children is both a social and a technological problem.



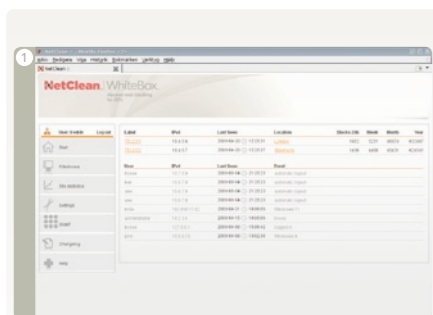
- > No effects on performance in the ISP core
- > No proxying
- > Easy to deploy and maintain
- > http responses are routed the normal way, since the WhiteBox needs only to see the http request
- > 100% accurate - can match whole URLs as required by IWF
- > No overblocking
- > One management centre can control several filter boxes if the network needs more than one filter box

## Technical details

1. Manage all the filter servers via one web GUI server.
2. Hardened Unix type operating system.
3. SNMP traps to your servers (and to the GUI).
4. RADIUS support for the web GUI (with several access levels in the GUI, read only, user, and admin).
5. Logging via Syslog to your servers (on request).
6. Appliance is rack mountable with multiple power supplies and raid disk arrays for high reliability.
7. Multiple filter-server solutions for redundancy.
8. No proxying.
9. All non-blocked traffic is passed unaltered.

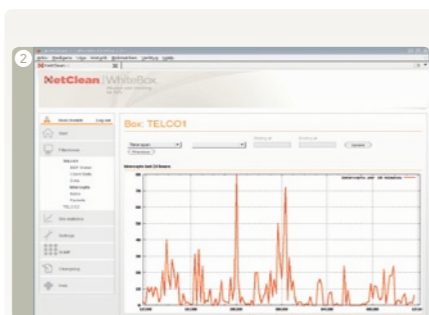
# The WhiteBox Interface

INTERFACE



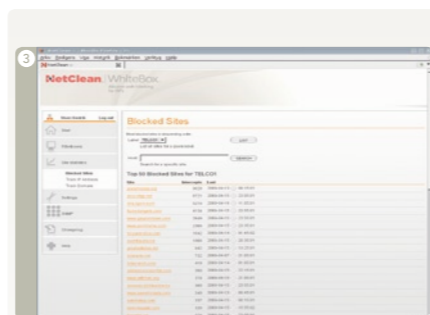
**1 Easy overview of the systems**  
You can view statistics for every connected filter server in an easy manner: blocks today, last week, month and year. The reachability of every connected system is displayed as well.

**1 Users of the GUI**  
The GUI is accessed via https, and can use radius or static accounts as authentication. You can see who is currently logged in to the GUI, and their last action, useful for NOCs.



**2 Live plots of intercepted URLs**  
For every filter server connected to the system, you are able to see raw data, plots of the number of intercepts, bytes and traffic, snapshots of the BGP status, and the amount of traffic that is allowed to bypass the filter (such as the authorities managing the blocklists).

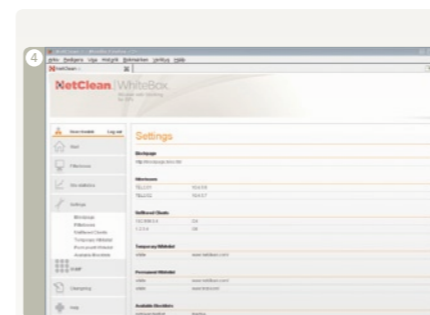
**2 URL lists**  
The block lists can use any type of URLs and will block the exact URLs and nothing else. The lists are usually provided by authorities within the ISP region. The IWF (Internet Watch Foundation) and a list from Interpol are supplied as an available default and are automatically updated daily.



**3 Site statistics in the block lists**  
For every filter server you can see a list of the most blocked sites. You can also keep track of the IP addresses the sites change between, and see all the other sites on the same IP address in an easy and searchable manner. The DNS/IP history is kept in a database.

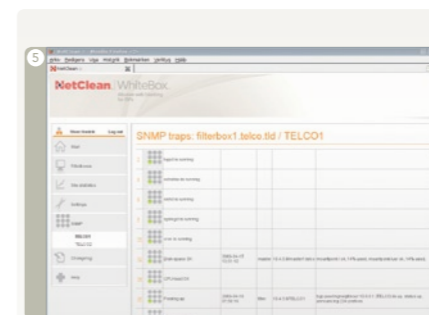
**3 Lists, IP addresses and DNS**  
The DNS lookups are performed against the NetClean resolver infrastructure spanning the continents. The resolvers are exchanged often and your system will always use the nearest resolvers first, and then apply a round robin approach.

**4 View and change settings easily**  
Overview of all the settings, such as which block page to use, the names/IP addresses of all connected filterboxes, clients allowed to bypass the filter, sites in the ISP white list, which block lists are available to use, which white lists are available to use (the white lists are URLs/domains that will never be blocked) etc.



**4 Control the filterboxes**  
The filterboxes can be controlled individually, the BGP sessions can be taken down separately, or the filterboxes can run in "test mode" to show the amount of would-be intercepts.

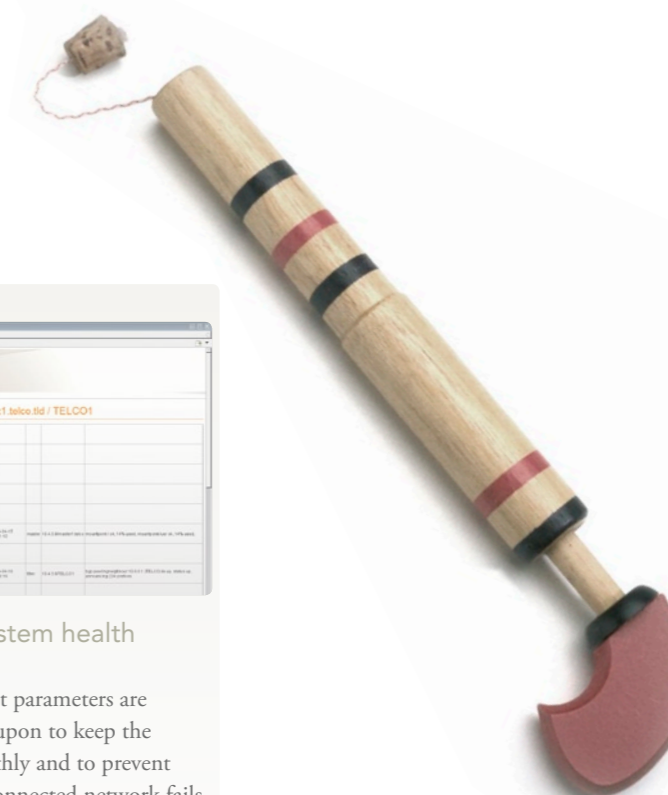
**4 A changelog of the settings**  
All changes in the configuration are kept in a browsable log which shows timestamps, users, actions and comments where available. Changes resulting in altered behaviour of the filter servers will send an alert via SNMP traps, such as changing the block server, enabling or disabling a block list, changes in BGP; changes to/from test mode etc.



**5 Overview of system health via SNMP Traps**  
More than 25 different parameters are monitored and acted upon to keep the system running smoothly and to prevent loss of quality if the connected network fails in any way. Parameters like daemons, system load, BGP peerings, reachability of servers and networks, temperatures, block lists, abusive IP addresses in the ISP etc.

**5 Ensure network quality**  
The system will monitor the reachability via the ISP, and will take down the BGP session to prevent blackholing. It uses several mechanisms to prevent disruption in the rerouted traffic in case of an overload attack. If the ISP itself is hosting content within the block lists the ISP will be alerted via SNMP traps.

... there are malicious groups of people that take advantage of the Internet and use it for criminal activities.



INTERFACE





# The WhiteBox system

## Technical overview

“In today’s business, being good is good business. As an ISP that always aims to be the business leader, launching a service that prevents access to child abuse image sites is an important step towards protecting children all over the world. Being a modern ISP includes social consciousness with services the public ask for.”

*Malin Frenning, CEO TeliaSonera International Carrier*

# Functional overview

Highlighting the accuracy of the NetClean WhiteBox

## Filter criterias

The WhiteBox has three criteria to make a block. The rerouted IP address, the fully qualified domain name and the path. All three must match for a site to be blocked. If one or more of the three criteria are not fulfilled, the traffic will reach the original destination unaltered.

## Rerouting traffic

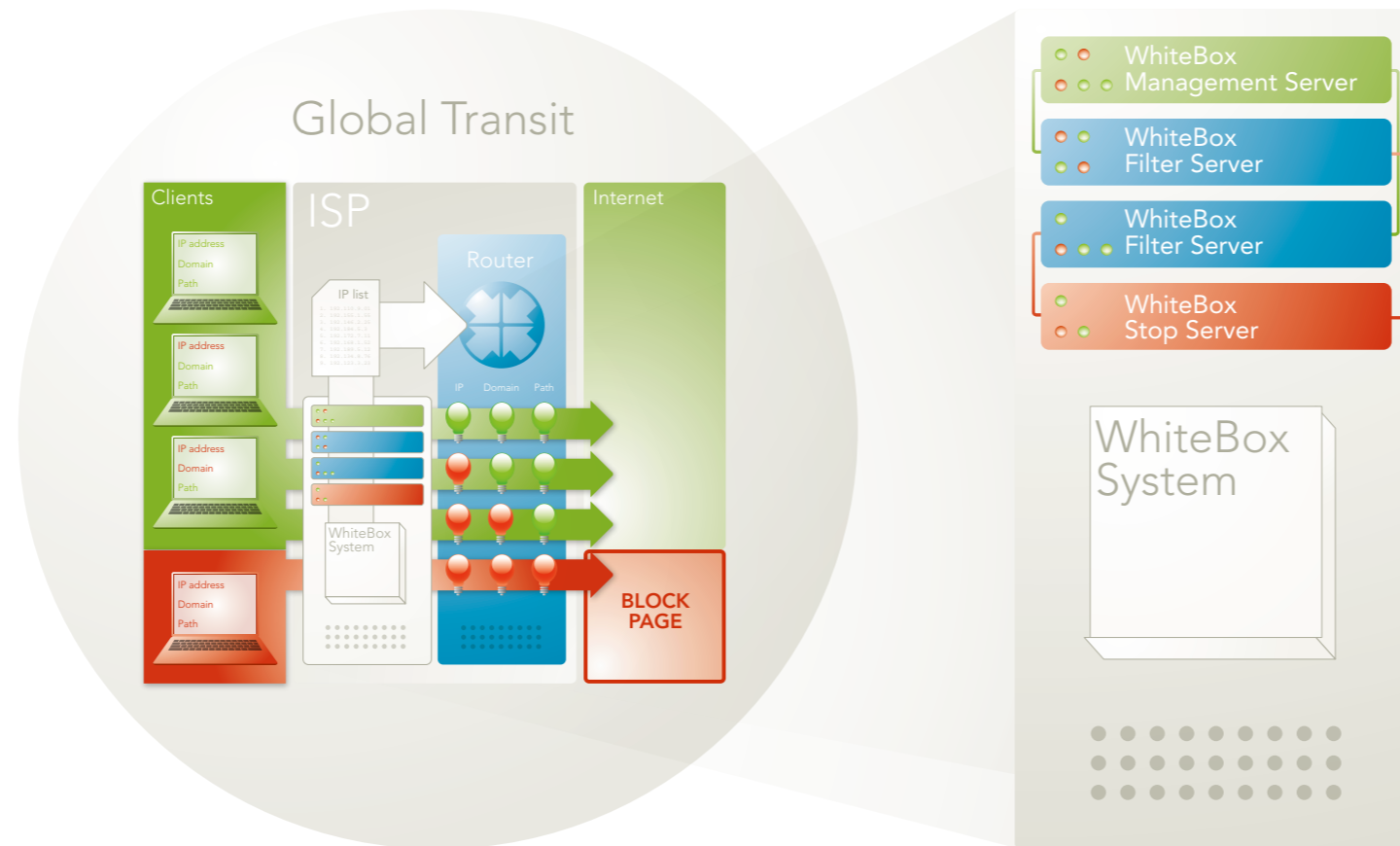
If an IP address is marked "red" via the WhiteBox it will be announced to the ISP and rerouted to the WhiteBox. An IP address is red if any of the fully qualified domains in the block lists resolves to that IP address.

## Blocking page

If the packets in the rerouted red IP address match the fully qualified domain name and the path to any of the entries in the block list, the WhiteBox will present a block page informing the client that the specified web page is blocked. This intercept will increase the counters in the WhiteBox GUI.

## Unaltered traffic

If the fully qualified domain part or the path in the URL does not match, the WhiteBox will allow the traffic to reach the destination unaltered.



FUNCTIONAL OVERVIEW

# System overview

Highlighting the simplicity of the NetClean WhiteBox system

## Filter servers

The filter servers do the actual filtering of the ISP network. This is done by rerouting selected host routes via a BGP peer between the filter server and an ISP router. Only the http traffic is inspected; for the rest of the rerouted traffic the filter server acts as a pure router and sends the traffic back to the Internet to reach the destination without inspection. The filter servers can be placed in central POPs in the ISP network - two per POP or region (country) is more than enough for redundancy and load sharing

## Management server

The management server is the web GUI used to manage the filter servers. It will also handle all the block lists and white lists, and all the DNS lookups for these. It receives updates from all the filter servers and presents these as statistics/plots, and it sends the block lists and IP lists to the filter servers regularly.

## The stop server

The stop server is an optional add-on with extra features. In the event a client gets intercepted this will show a stop page describing why the client was blocked. This can actually be any web page, but the NetClean stop server adds functionality

such as only allowing blocked clients to reach the stop page (and not the rest of the Internet). It can also display different stop pages depending on the client IP or client AS even. The stop server is usually placed separately from the rest of the WhiteBox servers.

There is **no negative impact** at all within the network using the NetClean WhiteBox.

Blocking access is a **vital step towards a safer world** for our children.



SYSTEM OVERVIEW

For a standard installation  
the WhiteBox servers will use 4 LANs

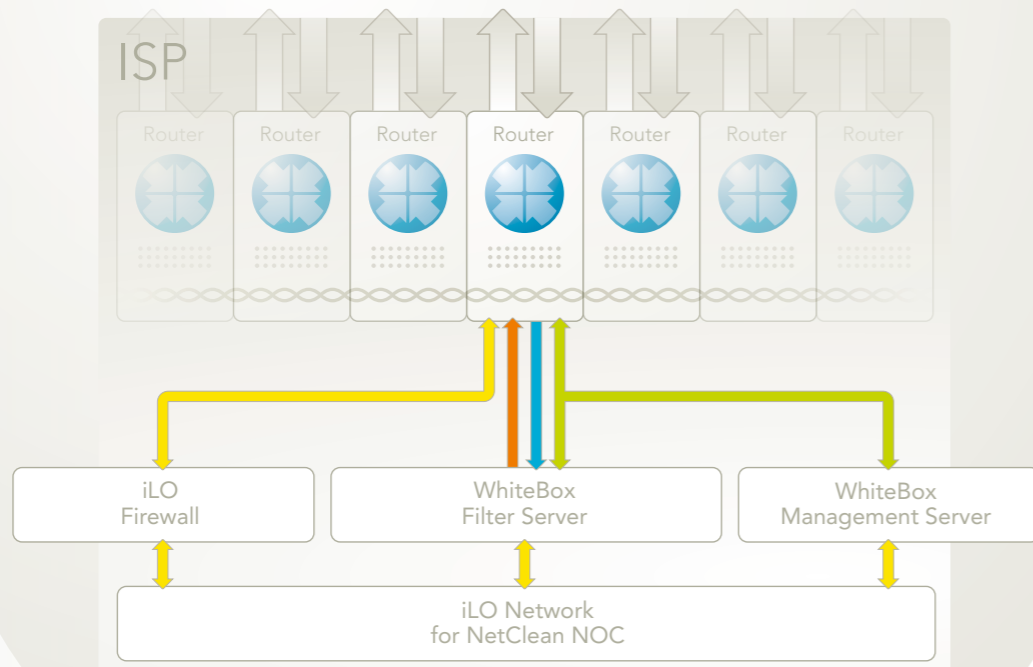
- iLO
- Ingress
- Egress
- Management



# Setup overview

Quick and easy implementation

## Global Transit



### iLO

The iLO (integrated Lights Out management) is used by NetClean NOC for remote management. It is connected to the network via a firewall, iLO-FW. The firewall can use a 10Base-T, 100Base-T or a 1000Base-T with a /29 mask (or larger depending on the amount of filter servers placed on the same LAN).

### Ingress

The ingress is used for the BGP peering between the filter server and the ISP; this is where we redirect selected network traffic to be inspected. This is a 1000Base-t with a /30 mask. These IP addresses need to be reachable via the ISP network, but do not need globally routed IP addresses, and can use RFC 1918 addresses for the purpose if needed. The WhiteBox filter server will use an AS (Autonomous System) that differs from the ISP network. NetClean can provide a unique AS for this if needed, or it can use any private AS since the announced host routes should never leave the ISP network.

### Egress

The egress is used for the outgoing traffic which is not blocked via the filter server. This is a 1000Base-T with a /30 mask. Since the WhiteBox setup uses BGP which announces

host routes to the ISP - this interface can not be connected to the same AS as the ISP; this would simply create a routing loop since the best way for the traffic to reach the rerouted host routes is via the WhiteBox. This is solved either by a default tunnel to the NetClean infrastructure residing within TeliaSonera International Carrier (AS1299), or via a tunnel to the ISP's global transit, or via a LAN to the global transit if available. If a tunnel setup is used, the IP addresses provided by the ISP need to be globally reachable and can not use RFC 1918. This is to enable termination of the tunnel towards the global transit used.

### Management

The management is used by the servers and the ISP and by NetClean in several ways. This is a 1000Base-T with a variable mask depending on the amount of servers placed there; several filter servers can be used simultaneously for load sharing or redundancy. These addresses need to be globally reachable. The filter server(s) need(s) to be able to send traffic to the web GUI server for statistics and list management, and they need to be able to send traffic to a client that is blocked. This is done via spoofed IP addresses, so the filter server(s) will never announce their IP address(es).

### Web GUI

The web GUI server needs to be able to send traffic to the filter server(s), and to the NOC at the ISP for the web GUI. The web GUI also handles all the DNS resolving of the lists via NetClean infrastructure resolvers residing with many ISPs around the world. NetClean will also use these addresses when upgrading or managing the systems.

### WhiteBox setup

WhiteBox-setup can not reside behind NAT or behind a firewall of any kind. It is a network element and can be viewed as a router within the ISP.

### Filter servers

The filter servers can actually be placed anywhere in the ISP network and do not have to reside on the same LAN as the web GUI master. The web GUI master can manage any amount of filter servers the ISP needs. Two is usually enough to cover any ISP, but this can be expanded to several more mainly to lower the RTT in networks covering several countries/continents.

# FAQ

FAQ

What happens if the website switches to a new IP address?

The system periodically refreshes the mappings between website and IP address (i.e. runs a new DNS lookup). This is done often, the system also “remembers” addresses with some delay to catch the sites that switch often between several sets of IP addresses.

How are the IP blacklist and the URL blacklist updated?

The blacklist can be from any source the ISP relies on, including law enforcement, NGOs or IWF, which we would recommend and include. The list of URLs will be converted to a list of IP addresses. This is done several times a day.

How many IP addresses are listed in the IP blacklist?

The blacklist consists of URLs, not IP addresses per se, so it varies. An example could be that a list of 3,000 URLs results in approximately 350 IP addresses that will be announced in BGP to the ISP using the WhiteBox. (This due to the fact that many of the URLs are on the same websites or simply are not reachable; some of the URLs exist only for a short time).

How are FTP, IRC, P2P and newsgroup flows etc. handled?

They are simply routed through the box if they are hosted on the same IP addresses as the websites that are to be blocked. Other protocols could be considered to be included in the WhiteBox later on, but the current version handles http only (which is the only type provided by IWF).

At what level is the filtering applied?

The filters can be applied at two levels: website, or parts of a website. It is possible to filter down to the level of folders or individual documents as images on a website. For instance you could filter <http://www.website.com/badcontent> but allow <http://www.website.com/goodcontent> on the same website.

Are there other routing protocols like OSPF that could be used?

No, just BGP in the current setup of the WhiteBox.

What happens when there are multiple websites on one IP address?

The requests for all of the websites are diverted to the filter server. The filter server receives the requests and looks at the URL to determine whether that site is banned or not.

If it is banned a “This website is banned” message is returned, otherwise the filter server forwards the request to the web server.

If a request is made for a non-banned website on an IP address that also has banned websites, does the request still go through the WhiteBox system? Yes. All traffic intended for the IP addresses are rerouted via the WhiteBox.

Does the filter server get both the request and the response from the website?

No. The WhiteBox will only see the SYN and ACKs of the flows. If the filter server passes the request to the website (i.e. it is to a non-banned website on a filtered Internet address), the response from the website goes straight to the user without passing through the filter server.

Will the filtering cause any performance issues?

Requests to blocked websites will, of course, not be available. Requests to websites that are not blocked but are at the same Internet addresses as blocked websites will not suffer any performance loss other than an extra router hop. Requests to websites that are not blocked and are not at the same Internet addresses will not be affected.



# We protect children on the Internet

The technological breakthroughs in recent decades have been almost inconceivable. They have made the development of tools, instruments and services possible that would otherwise have been utterly unimaginable. In the field of IT, the technological upsurge has taken on enormous proportions. The development of the Internet and the related infrastructure has fostered education, research and common knowledge. It has grown into a limitless network that supports amusement, recreation and professional activities, but nevertheless there are some inherent problems with this limitlessness.

Just like in society at large there exist malicious groups of people that take advantage of the system and use it for criminal activities. The existence of these activities must be narrowed down as much as possible. One of these activities is the distribution of child sexual abusive images. The spreading and consequently also the availability of material depicting sexually abused children is therefore both a social and a technological problem.

Each time this abusive material is shown, the children get abused once again. The images and videos will never disappear and will follow the victims throughout their lives due to the sustainability of Internet content. There are even commercial Internet sites that make a profit from distributing this kind of abusive material. These sites are not just illegal, they are also deeply hurtful for the abused children. Blocking access to these sites is a vital step in the fight against this harmful industry and towards a safer world for our children.

## NetClean™

[www.netclean.com](http://www.netclean.com)

Första Långgatan 30, SE-41327 Göteborg, Sweden

Phone: +46 (0) 31 719 08 00

Partners:



Summary:

## Why NetClean WhiteBox?



**A NetClean System for ISPs**  
Powerful tool for ISPs, designed to block access to websites containing abusive images.



**Exact blocking**  
Blocks only the portion of the site that needs to be blocked.



**Flexible**  
Configuration possible to use any URL blocking list containing child sexual abuse images.



**Quick and Easy**  
The system implementation requires minor or no changes in the ISP core due to the use of Border Gateway Protocol (BGP).



**Dynamic reporting**  
Dynamic, flexible traffic reports.



**No proxying**  
All non-blocked traffic is passed unaltered.

