

Ensure a Safer Internet Experience with Allot WebSafe



Solution Brief



Table of Contents

Introduction	2
Allot WebSafe	2
WebSafe benefits & advantages	3
Allot WebSafe solution	3
How it Works	4
The URL filtering process.....	4
The blacklist updating process.....	5
Conclusion	6

Introduction

The Internet has changed our behavior in many ways. By bringing a wealth of information, ways to shop, bank, plan holidays, and opportunities to share our lives with friends and communities, the Internet has become an indispensable tool in our daily lives. Yet, the Internet also has a darker side as it opens our doors to content that we do not want. With its vast and fast distribution capabilities the Internet provides an ideal platform for delivering all kinds of content, including illegal content, such as incitement to hatred and child pornography. Moreover, it allows illegal content providers to remain anonymous and to change their venue at a moment's notice, making them harder to stop. Most people want to avoid exposing themselves and their families to this kind of content. In

response to growing consumer concerns, mobile and fixed broadband service providers can take a pro-active role in delivering a safer Internet experience to their subscribers while protecting their networks from being exploited and used as vehicles for illegal content.

Local and international organizations invest tremendous effort into fighting the creation and distribution of child pornography and other forms of illegal content. Some countries already have legislation in place to fight online illegal content. Others are in the process of setting up Internet specific regulations to fight it. In the future, it may be incumbent upon the ISP to enforce any such regulations that result. Why wait? ISPs can take steps now to provide the protection that subscribers want, through preemptive self-regulation that polices the network and blocks the way for illegal content.

Allot WebSafe

Allot WebSafe is a URL filtering service that empowers ISPs to block online access to illegal content in order to provide a safer Internet environment for their subscribers. Allot has become a member of the Internet Watch Foundation* (IWF) and is working with similar organizations and customers worldwide to enhance WebSafe's coverage and fulfill local requirements. This membership guarantees that Allot's ISP customers operate an up-to-date URL filtering service at all times.

IWF reports:

- 310% growth of child abuse sites from 2004 to 2006
- 54% of the known child abuse domains are hosted in the US
- Nearly 1 in 20 UK adult Internet users (or 1.5 million people) say they have been exposed to child sexual abuse images
- 69% of victims exploited in images or videos appear to be between the ages of 0 and 10; 24% are between 6 years old and younger; 4% are 2 years old or younger
- 81% child abuse sites have a life-cycle of under 100 days

WebSafe benefits & advantages

Protect subscribers from illegal content

- Provide a safe Internet experience while strengthening your brand image and customer loyalty
- Comply with regulations and arising regulatory bodies

Cost-effective integrated solution

- **Highly accurate filtering** using a URL blacklist
- **Real-time updates** ensure that URL blacklists are current. Any change to the blacklist is propagated immediately to all WebSafe installations.
- **Centralized management and control** by Allot NetXplorer management system. WebSafe deployment requires no additional hardware.
- **Minimal impact on subscriber experience**– WebSafe’s high-performance blacklist check introduces almost no delay in processing Internet requests.

Allot WebSafe solution

WebSafe is a network service deployed on the Allot Service Gateway Sigma, NetEnforcer AC-5000 Series, NetEnforcer AC-10000 Series devices and future platforms. WebSafe filters specific content using a blacklist of URLs, compiled by IWF or local organizations.

WebSafe supports a secure URL blacklist with a capacity of up to 100,000 entries. Unlike other solutions such as DNS filtering, which block entire domains, WebSafe filters only the URLs specified in the blacklist.

The solution also supports a white list, allowing accessibility to specific URLs that may be mistakenly blacklisted. The white list overrides the blacklist allowing operators to take remedial measure right away, without having to wait for blacklist update.

In a typical deployment, WebSafe is integrated within the existing Allot Service Gateway or NetEnforcer devices installed on peering links connecting the operator’s network to the Internet. This configuration allows full investigation of all outgoing Internet traffic managed by Allot solutions.

Alternatively, WebSafe is deployed on Allot devices installed on links connecting the access network to the core network. In this configuration Allot devices must be distributed across the operator’s network to ensure that WebSafe filters all outgoing traffic.

How it Works

WebSafe is centrally controlled and managed by Allot NetXplorer Management Suite. The NetXplorer server distributes the blacklist through a user-friendly GUI and guarantees that all Allot devices deployed in the network are running its latest version. Moreover, NetXplorer provides advanced monitoring and reporting tools to track WebSafe's performance and status.

URL filtering process

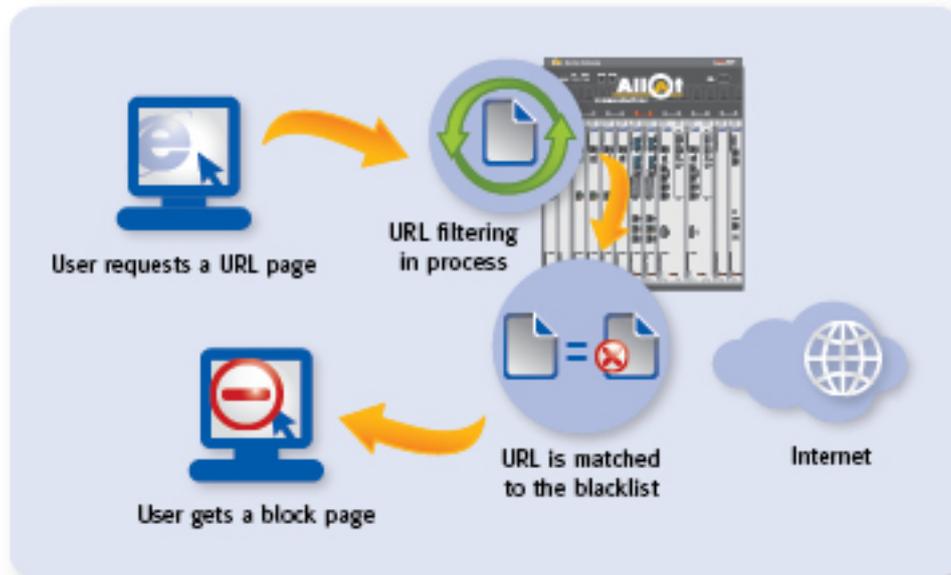


Figure 1: How WebSafe works

Typically, when a user requests a URL, the request is processed and the URL is displayed in the user's browser. When deploying WebSafe, an additional layer is added to the process. The scenario below describes how URL requests are handled and the measures that are taken when access to illegal content is requested.

1. Subscriber requests a URL in his browser.
2. This HTTP request travels via Allot Service Gateway/NetEnforcer to the Internet.
3. Allot WebSafe service filters the URL and check is against the blacklist
4. If the URL is blacklisted Allot Service Gateway/NetEnforcer drops the HTTP request.
5. After dropping the request, WebSafe notifies the subscriber by:
6. Sending a block-page notification (a user-configurable HTML file preloaded in the Service Gateway/NetEnforcer platform)
7. Redirecting the subscriber to a warning webpage (using HTTP redirect)
8. In both cases the subscriber receives an error message and is not able to access the illegal content.

Updating the Blacklist

Turn-around of new or recycled illegal content is exceptionally fast. Therefore an efficient URL filtering solution requires frequent updates of the URL blacklist. WebSafe is designed with the flexibility to get real-time updates using either manual or automatic methods.

WebSafe manual updates

WebSafe's manual update functionality allows operators to upload an external text file and update the URL blacklist upon request. The blacklist file is uploaded to the NetXplorer server which securely distributes it to Allot Service Gateway and NetEnforcer units deployed in the operator's network.

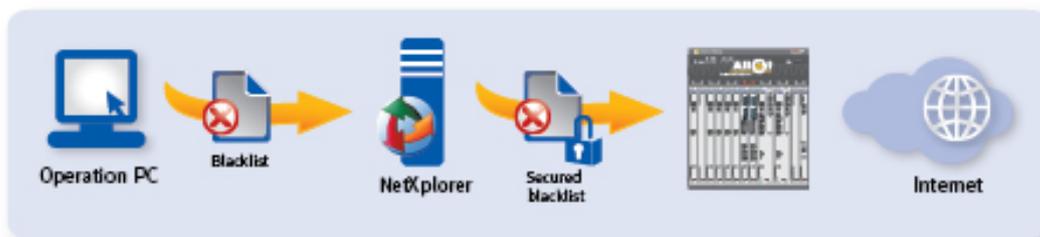


Figure 2: WebSafe manual update process

WebSafe automatic updates

Since each country has a self-regulatory body that manages URL filtering blacklists, WebSafe allows ISPs to receive real-time updates from their regulatory bodies over a secure Internet connection. In most cases, updates occur on a daily basis and through an automatic interface. WebSafe offers a convenient functionality that allows a smooth integration with any external blacklist resource. Allot has become a member of the IWF as part of our efforts to make sure our ISP customers receive real-time, automatic updates.

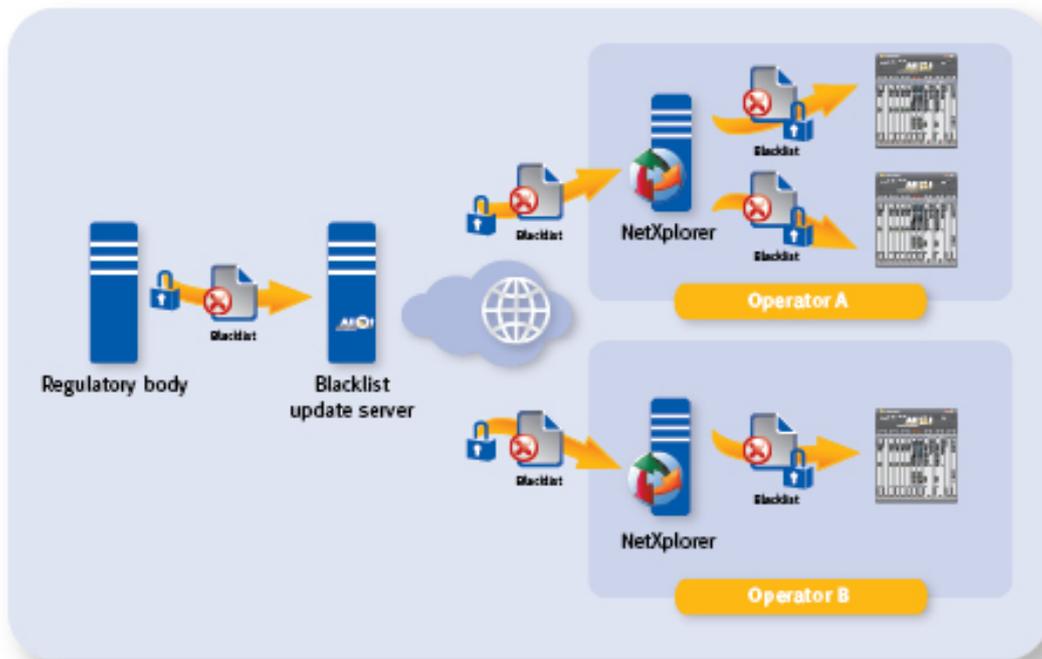


Figure 3: WebSafe automatic update process

Conclusion

Allot WebSafe enables mobile and fixed broadband service providers to respond to their subscribers' expectations for safer and cleaner Internet networks. Safer networks promote confidence in the service provider and improve customer loyalty.

Deploying a URL filtering service such as WebSafe involves service providers in the overall efforts to prevent the proliferation and distribution of online illegal content. By taking a proactive approach to URL filtering, service providers set up an infrastructure to comply with existing and future regulations.

WebSafe is a highly accurate filtering service. Its blacklist allows service providers to filter specific web pages that publish illegal content and prevent the inconveniences of DNS filtering that unreasonably filters entire domains. Allot's URL filtering service also provides a very user friendly updating process; ISPs can either manually update their blacklist or rely on ongoing automatic updates from their local regulatory bodies.

Allot's URL filtering service has a negligible impact on the subscriber quality of experience (QoE). It is easily integrated within the providers' existing Allot infrastructure. WebSafe is a scalable network service that can be seamlessly deployed within any service provider environment.

www.allot.com info@allot.com

Americas: 300 TradeCenter, Suite 4680, Woburn, MA 01801 USA - Tel: 781-939-9300; Toll free: 877-255-6826; Fax: 781-939-9393

Europe: NCI—Les Centres d’Affaires Village d’Entreprises, ‘Green Side’ 400 Avenue Roumanille, BP309 06906 Sophia Antipolis, Cedex France - Tel: 33 (0) 4-93-001160; Fax: 33 (0) 4-93-001165

Asia Pacific: 6 New Industrial Road, #08-01, Hoe Huat Industrial Building, Singapore 536199; Tel: +65-6283 8990; Fax: +65-6282 7280

Japan: 4-2-3-301 Kanda Surugadai, Chiyoda-ku, Tokyo 101-0062 - Tel: 81 (3) 5297 7668; Fax: 81 (3) 5297 7669

Middle East & Africa: 22 Hanagar Street, Industrial Zone B, Hod Hasharon, 45240 Israel - Tel: 972 (9) 761-9200; Fax: 972 (9) 744-3626

