Service Control EasyApp - A Safe Internet Experience

Abstract

This Cisco® Service Control Engine (SCE) EasyApp guide explains how service providers can use the Cisco SCE Family to help their customers experience the Internet safely. It explains the different services that the Cisco SCE can facilitate and outlines the technical approach to their implementation.

| EasyApp Category	Service Creation	SCE equipment and software version	Hardware: Cisco SCE 2000 and 8000 Series Service Control Engine
			Software: Release 3.5 or later
Type of Effort	Depending on the approach taken, may require as little as several hours to set up or a more comprehensive effort requiring new service definition and policy integration.		

A Safe Internet Experience

As the Internet becomes increasingly integrated into people's lives, concerns about Internet safety are mounting. Whether it is to protect computers from harmful agents and viruses or to block inappropriate content and activity, the challenges grow in parallel with the web itself. With the Cisco SCE platform, service providers can offer a number of different safety-enhancing services and features to help protect their subscribers and enable a more productive and enjoyable online experience. This improves customer satisfaction, reduces turnover, and contributes to increase in average revenue per user (ARPU). This guide highlights the different safety-enhancing services that an ISP can offer (either individually or combined) to gain customer loyalty and a competitive advantage.

Further reading: Read a case study of how an ISP implemented Cisco SCE-based security services: http://www.cisco.com/en/US/prod/collateral/ps7045/ps6129/ps6133/ps9591/siminn_cs.pdf.

Cisco SCE-Based Safe Internet Offerings

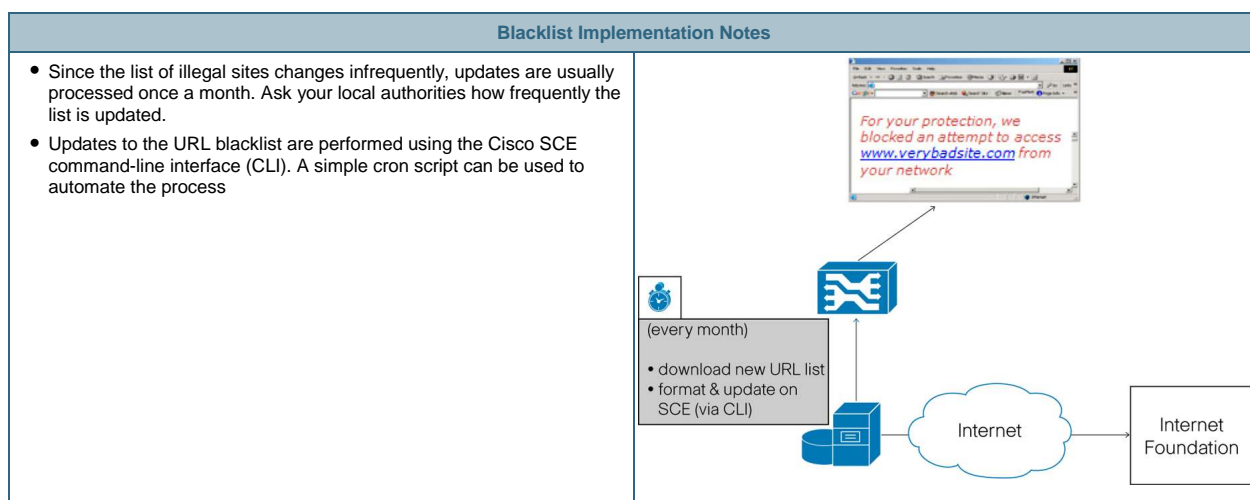**Figure 1.**   SCE-based Safe Internet Offering
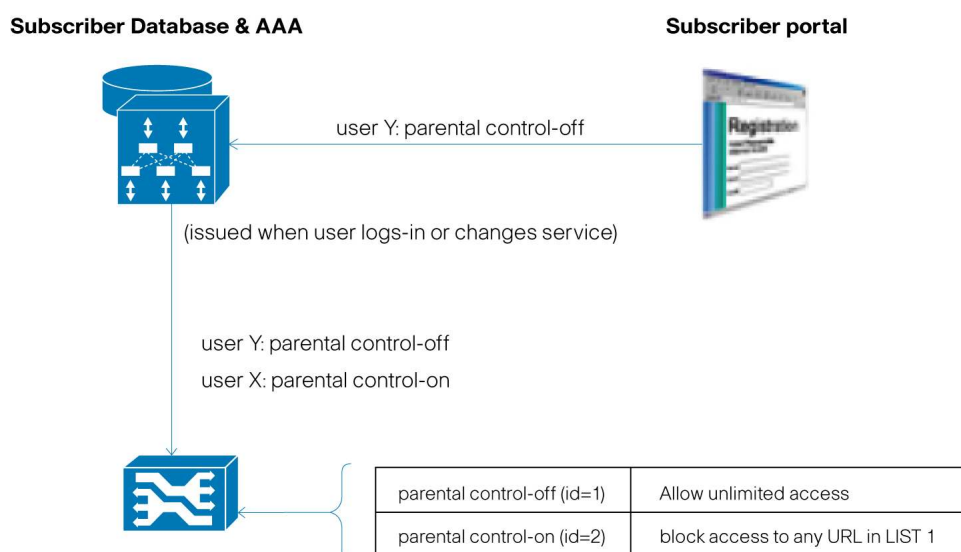
The figure1 shows the main components of the Cisco SCE solution used to create Safe Internet offerings. The core features of the Cisco SCE used in creating Safe Internet services are the HTTP-based URL classification and the capability to assign different subscribers different packages, which are stored in the subscriber-management system and introduced to the SCE whenever the subscriber's Internet connection is granted an IP address. A self-service portal is typically used to allow customers to change their subscription plan (for example, to upgrade to a premium service or purchase a "Safe Internet" service add-on).

There are many variations to the type of services that can be created. The following sections highlight some options for service providers to consider in their customer offerings.

Blacklists - Automatic Blocking of Illegal Sites

A blacklist service is one in which the Cisco SCE is instructed to block access to a set of defined URLs, using its built-in URL Lists feature. This is typically done to block access to illegal sites (such as child pornography, racism and hate sites, etc.), a list of which is provided by a local government office or non-profit organization, such as the Internet Watch Foundation. (There are different organizations that support different countries and regions and the appropriate one should be used by each ISP.)

While in some countries there are laws requiring ISPs to provide this service, the universal purpose of such a service is to provide subscribers with the peace of mind that accidental access to illegal sites will automatically be blocked by the ISP. Many ISPs choose to provide this as a default feature of any Internet service plan, and in many cases do not provide an "opt-out" mechanism.

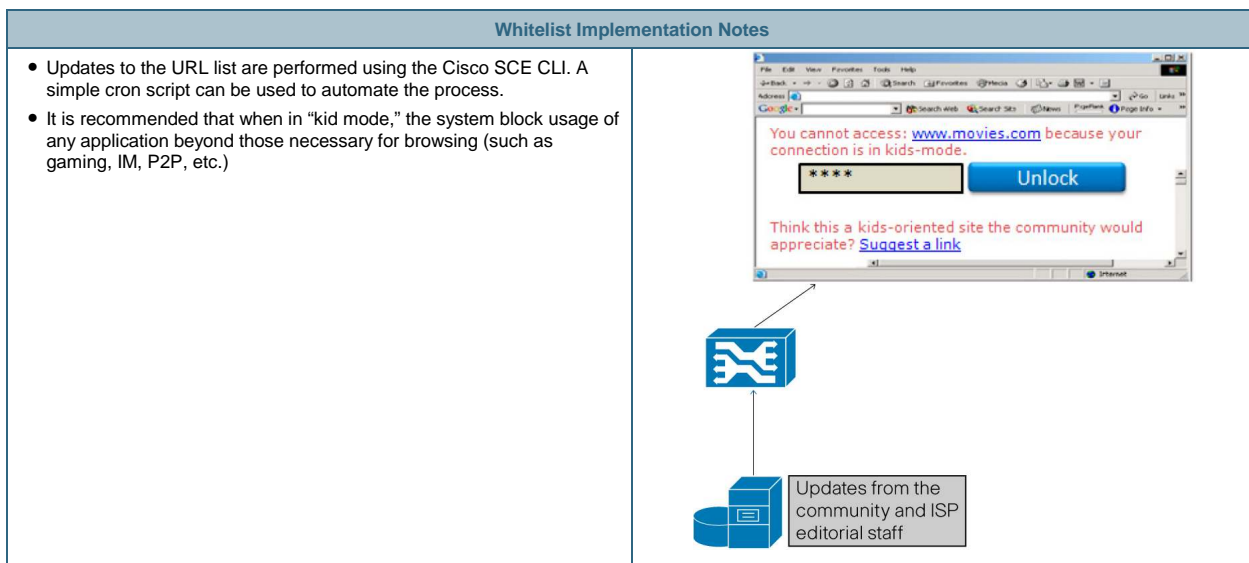| Blacklist Implementation Notes |
|---|
| Since the list of illegal sites changes infrequently, updates are usually processed once a month. Ask your local authorities how frequently the list is updated. Updates to the URL blacklist are performed using the Cisco SCE command-line interface (CLI). A simple cron script can be used to automate the process |

Whitelist - Kid-Friendly Internet

A whitelist service operates in the opposite fashion as the blacklist service. The Cisco SCE only permits browsing requests to go through if the web address they are accessing is on a permitted sites list, which the ISP curates and maintains. The purpose of this service is to create a restricted "safe for kids" service that ensures all Internet activity is with safe, kid-friendly (often educational) sites.

Because it is rare (with the possible exception of Internet connections to schools and other children facilities) that an Internet connection is used exclusively by children, the service needs to offer an "unlock" page through which a parent can provide a password for unrestricted browsing. In addition, a "Recommend a Site" option should be available for subscribers to suggest sites that are presently not on the whitelist.
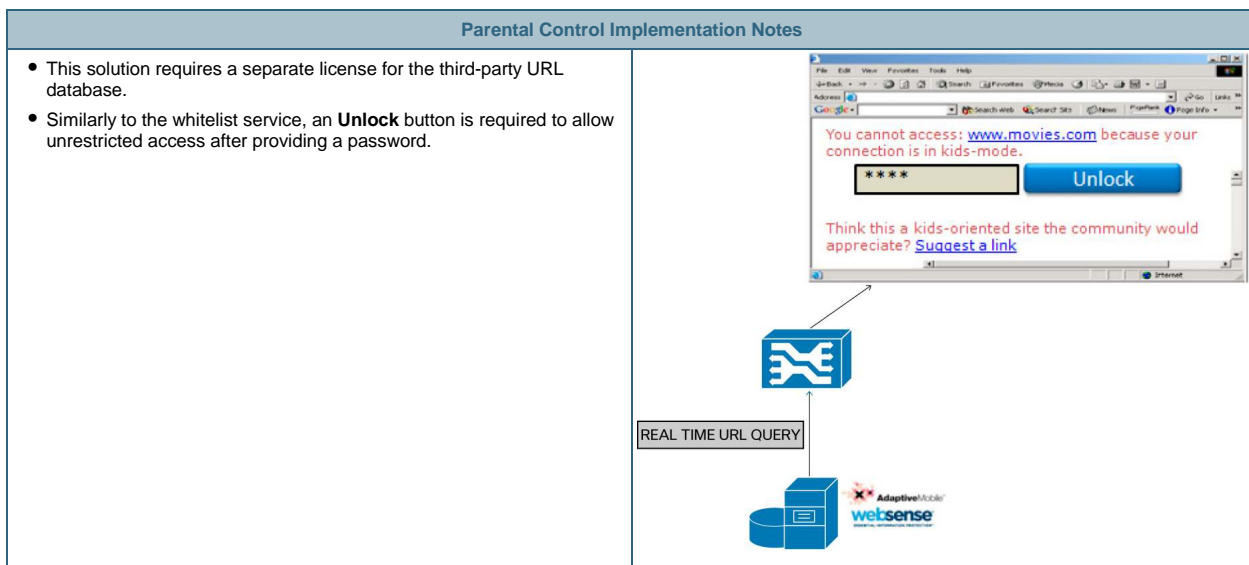
A whitelist service is an effective way to alleviate the safety concerns of parents without a lot of effort on their part. And while it does require the ISP to invest some time in ensuring the whitelist is up to date, it helps the ISP build a strong sense of community, which increases customer satisfaction and reduces turnover.

Whitelist Implementation Notes	
• Updates to the URL list are performed using the Cisco SCE CLI. A simple cron script can be used to automate the process. • It is recommended that when in "kid mode," the system block usage of any application beyond those necessary for browsing (such as gaming, IM, P2P, etc.)	

Real-Time, Third-Party URL Filtering - Parental Controls

While the blacklist service provides wide coverage and regulatory compliance, and the whitelist service an option to create a simple, highly restrictive "for kids" service, a more robust filtering engine is required for a full-fledged parental control offering. The Cisco SCE integrates with leading web-filtering technology from Websense and AdaptiveMobile to offer a complete URL-filtering solution. With this approach the SCE manages a connection to the third-party server and tests each URL request, in real time, to check if the subscriber is allowed access. Caching on the SCE is used to help ensure that the solution can cope with the high bandwidth requirements on broadband networks.

Using this approach, the ISP can offer a fully hosted, parental control solution for its subscribers, saving them the time and money of purchasing a client-side solution as well the ongoing maintenance of all IP-enabled devices at the home.

Parental Control Implementation Notes	
• This solution requires a separate license for the third-party URL database. • Similarly to the whitelist service, an **Unlock** button is required to allow unrestricted access after providing a password.	

For More Information

The short, easy-to-follow **Cisco Service Control EasyApp guides** provide new and experienced Cisco SCE customers with information on how to best utilize the platform in their network. The guides contain practical, actionable advice on the SCE platform that will help you learn more about network usage patterns and how to reduce costs and optimize the network's behavior to provide a superior experience for its users. Browse the full selection of **Cisco Service Control EasyApp guides** on http://www.cisco.com/go/servicecontrol to improve your network today.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Printed in USA

C11-606444-00   06/10