

## Mobile Content Filtering and Control: Why it is Needed, How it Works

As mobile operators begin offering more and different types of content to their subscribers, they need the ability to filter and control the content that individual subscribers can access. Reasons include satisfying customer preferences, providing parental controls, and complying with various social, cultural, legal, and corporate requirements.

Cisco® offers a flexible, scalable mobile content filtering and control solution as part of the Cisco mobile Service Exchange Framework (mSEF) for Cisco on the move.

### Executive Summary

Mobile operators have begun offering content services to their subscribers, a proven strategy to attract and retain customers and increase average revenue per user (ARPU). With this opportunity there arises a new business and technical challenge: how to control the content that each subscriber can access. Not all content is appropriate for all subscribers. Therefore, mobile operators need to give their subscribers choice and control of the content they access, while also complying with a variety of potential constraints: legal, religious, cultural, parental control, corporate policy, or social responsibility.

Cisco offers a comprehensive solution for mobile content filtering and control. When users request content, the request is intercepted and compared against a filtering database for that particular user, based on the preferences of the user or his or her parents or employer. Requests for allowed content are fulfilled as usual, and requests for disallowed content are blocked or redirected to a server that indicates the request cannot be fulfilled. The solution provides great flexibility, allowing parents to prevent their children from accessing adult content at any time or employers to block access to non-business-related content during business hours.

The Cisco Mobile Content Filtering and Control solution is part of mSEF, an open platform providing value-added services through intelligence and control at the mobile Internet edge, independent of the network or radio access technology. Mobile operators can install and deploy Cisco mSEF without disrupting any services. Providing an intelligent enforcement layer within the operator's network, Cisco mSEF is enhanced and complemented by Cisco unrivaled partnerships. Cisco has already proven the platform's interoperability with major Radio Access Network (RAN), authentication, authorization, and accounting (AAA), content billing, content filtering, and compression solutions, relieving mobile operators of the need to dedicate resources to ensure a smooth deployment. More than 40 mobile operators worldwide have deployed and validated the superiority of the Cisco mSEF platform.

This white paper describes the market factors creating a need for content filtering, technical requirements, the Cisco Mobile Content Filtering and Control solution, and its business benefits for mobile operators.

## Market Factors and Challenges

With the advent of next-generation mobile networks, mobile subscribers can access the same content available to traditional fixed-line and WiFi Internet users. Additionally, the sheer nature of mobility and its convenience encourage users to access more types of “recreational” content. While this enables new applications and revenue streams, it also creates new concerns relating to the appropriateness of content for different types of users. Groups that want to control access to content in mobile environments include:

- *Subscribers* themselves, who want some control over the content delivered to their phones, for cultural, religious, ethical, or other personal or social reasons
- *Parents and caregivers*, who want to filter inappropriate content for minors
- *Businesses* with corporate-liable mobile phone service to their employees that want to provide access to work-related content only during work hours, to protect against liability or increase productivity

Beyond meeting these requirements, mobile operators have additional motives for controlling content delivery, including:

- Disassociating their brand from certain types of content.
- Offering different levels of filtering services with tiered pricing.
- Complying with government regulations. For example, the European Union is considering regulating mobile-market content as part of its ongoing Internet Safer program, and operators in the United Kingdom have agreed to assume responsibility for protecting underage subscribers from viewing inappropriate content.

To gain the flexibility to meet these requirements, mobile operators need the following capabilities:

- Content categorization and control with a deep level of granularity and nuances, or associating content with categories that customers might choose to filter, such as gambling or pornography
- Subscriber identification
- Flexibility to filter different categories of content for different subscribers, at different times of the day or week if needed
- Scalability and robustness

## Service Description

Mobile operators can offer content filtering to all customers, to differentiate their service, or else offer it as a value-added service for increased service revenue. For example, mobile operators might offer a basic filtering service to shield underage users from inappropriate content, and bill for value-added filtering services such as applying different policies at different times of day or allowing for a more granular and nuanced choice of filtering categories.

When a mobile subscriber requests data content, the Cisco Content Services Gateway (CSG) intercepts the traffic and forwards the requested URL to the filtering application and database to determine if the request complies with or violates policy for the specific subscriber. The filtering application and database return the applicable policy to the Cisco CSG for enforcement. If the content is allowed, subscribers view it as they would ordinarily. If not, the session is either blocked or redirected to a notification server that indicates the reason the request was not fulfilled.

### Use Scenario

Using a 2.5G or 3G phone, a prepaid subscriber enters a sports Website address to check the final score for a football game that has just ended. Pleased by the results, the subscriber clicks a link to a gambling site, intending to place a bet on next week's game. The network operator's policy is to restrict access to gambling sites to subscribers over the age of 21. Because this subscriber is a prepaid user, the network operator is unaware of his profile or age. Therefore, the network redirects the subscriber's request to a site that sends a message to the phone explaining the over-21 policy and inviting the user to subscribe to a service package that includes access to gambling sites. To subscribe, the user will need to prove that he is over 21.

### Behind the Scenes

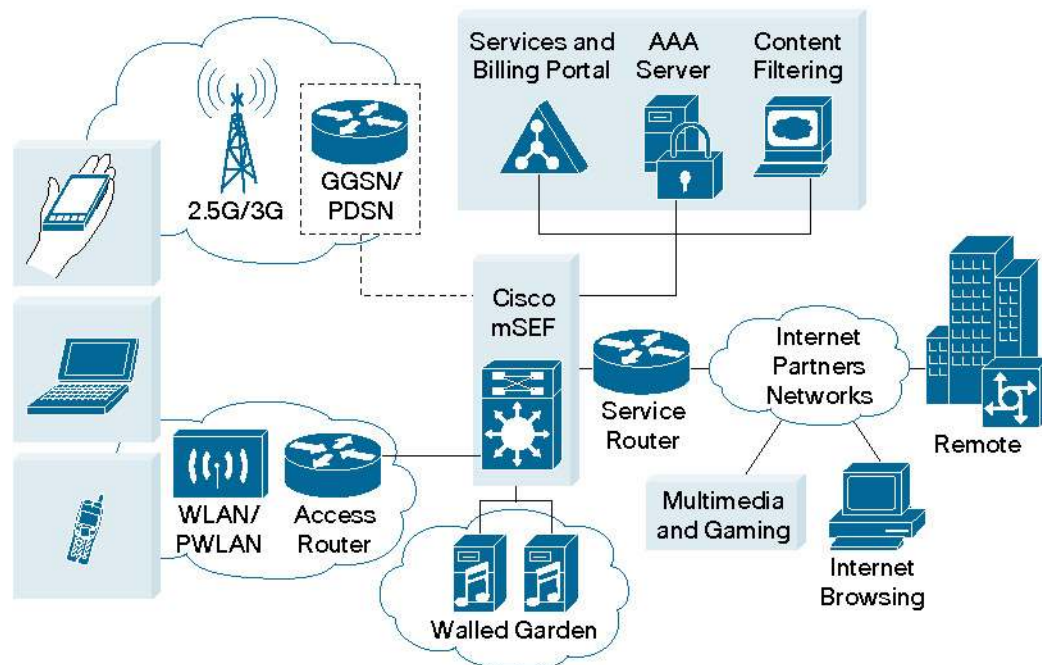
The following actions occur behind the scenes when a subscriber requests content from a mobile device.

1. *Identify user* – The Cisco CSG acts as a RADIUS proxy in General Packet Radio Service (GPRS) and Code Division Multiple Access (CDMA) networks. Using the RADIUS information, the Cisco CSG maps the user's IP address to either a username or Mobile Subscriber ISDN (MSISDN). Based on this information, the Cisco CSG populates an internal user database.
2. *Request the user's profile* – After identifying the user, the Cisco CSG requests the user's profile from the filtering application. The filtering application queries the real-time subscriber database to retrieve the user or group profile and then returns this information to the Cisco CSG.
3. *Determine appropriate filtering policy* – If the profile indicates that content filtering is not required, no further involvement is needed from the content-control application. If the profile indicates content filtering is required for this subscriber, the Cisco CSG queries the filtering application on a per-event basis, such as per HTTP, Wireless Application Protocol (WAP), Real-Time Streaming Protocol (RTSP), or Simple Mail Transfer Protocol (SMTP) requests.
4. *Enforce policy* – When the subscriber attempts to access content, the Cisco CSG sends a content-authorization request to the filtering application. This request contains specific information related to the protocol. The filtering application queries its database to determine if the content belongs to one of the categories that should be filtered. If so, it instructs the Cisco CSG to either redirect to a notification server or block the session.

### Solution Description

The Cisco Mobile Content Filtering and Control solution uses proven hardware and software to meet the content-filtering requirements of mobile operators and their subscribers. The Cisco Mobile Content Filtering and Control solution is part of the Cisco mSEF of solutions, which empowers mobile operators to offer value-added data services to mobile subscribers (Figure 1).

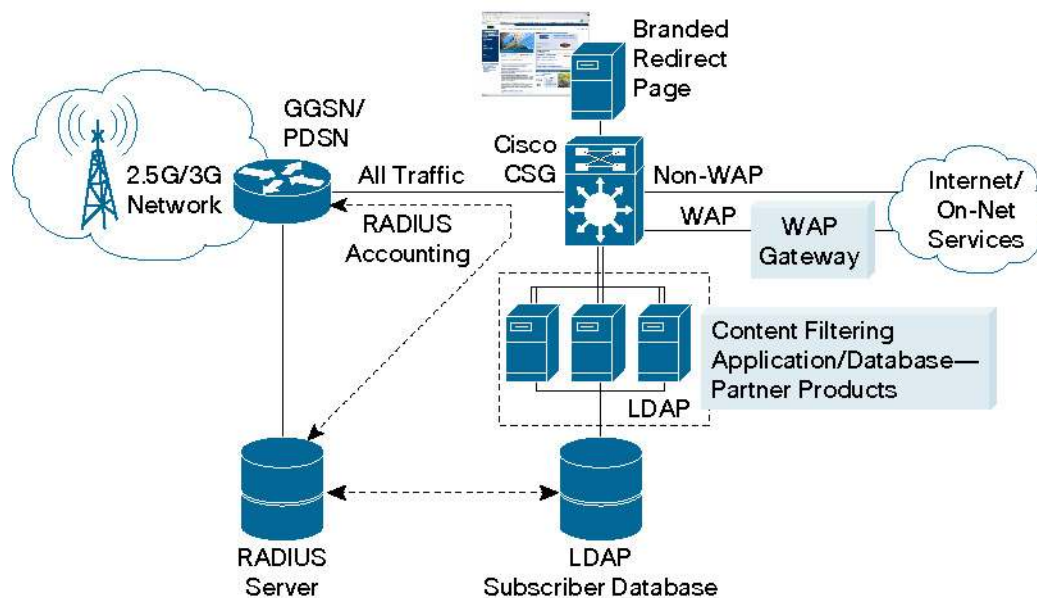
**Figure 1.** Cisco mSEF



**Solution Components**

Figure 2 illustrates the solution components.

**Figure 2.** Cisco Mobile Content Filtering and Control Solution Architecture Overview



**Cisco Content Services Gateway**

The Cisco CSG is a high-speed processing module designed for Cisco Catalyst® 6500 Series switches and Cisco 7600 Series routers. The role of the Cisco CSG is to examine the data stream beyond the IP and TCP/UDP headers. Used in the Cisco Mobile Content Filtering and Control solution, the Cisco CSG allows mobile operators to control subscriber access to varied content types, including specific HTTP and WAP pages and multimedia content.

Important advantages of the Cisco CSG for content filtering and control include:

- *Scalability* – The Cisco CSG can support thousands of subscribers per module. As the number of subscribers or volume increases, the mobile operator can sustain content-filtering performance by adding Cisco CSG modules to the Cisco Catalyst 6500 Series or Cisco 7600 Series platform. Load-balancing techniques distribute the traffic between Cisco CSGs for optimal performance.
- *Availability* – Two Cisco CSGs can be deployed in a redundant configuration, either within a single chassis or distributed over two separate chassis. Stateful failover prevents the transaction from being interrupted in the event of a chassis failure.
- *Wide protocol support* – Helps enable mobile operators to filter a variety of content types other than Web pages:
  - HTTP 1.0/1.1
  - WAP 1.x/2.0
  - FTP
  - RTSP
  - SMTP

### **Filtering Application and Database**

Cisco has partnered with leaders in content filtering and control software to provide the filtering application and database portion of the Cisco Mobile Content Filtering and Control solution. Mobile operators use the filtering application and database to define, monitor, and maintain clear Internet usage policies for individual users, groups of users, and organizations. The filtering application and database provide a comprehensive list of URLs and IP addresses, each associated with predefined or user-defined categories. The mobile operator can create exceptions to the predefined categories by adding or deleting URLs. Mobile operators can establish policies for category filtering based on the user's credentials, IP address, or group membership, and restrict different categories based on time of day. For example, a parent or caregiver might want to limit access during the hours that a child has a mobile handset at school, but provide unrestricted access during evenings and weekends.

### **Why Cisco**

Mobile operators that use the Cisco Mobile Content Filtering and Control solution gain two unique advantages: flexibility and the confidence that comes from working with the industry leader.

#### **Flexibility**

The Cisco Mobile Content Filtering and Control solution offers mobile operators unparalleled flexibility to categorize content and offer different types of content control for different subscribers.

#### **Market Leadership**

As part of the Cisco mSEF, the Cisco Mobile Content Filtering and Control solution complements an integrated set of solutions that mobile operators around the world are using to maximize the profitability of their second- and third-generation mobile packet infrastructures, 802.11 public WLAN hotspots, and dial-up networks. Mobile operators gain the confidence that comes from using a mature platform, such as the Cisco Catalyst 6500 Series Switch and Cisco 7600 Series Router, as well as from Cisco expertise with IP in general and the service provider market in particular. Choosing a tested solution from a financially stable company minimizes the risk of new service introduction.

## Comprehensive Programs

Through Cisco Advanced Services, mobile operators gain access to in-depth technical knowledge from certified experts, specialized tools and methodologies, industry-leading research labs, and a network of certified partners to help ensure the delivery of high-quality mobile wireless services. Cisco consultants and engineers help minimize the risk to valuable business assets by working with the mobile operator to plan, design, implement, operate, and optimize mobile wireless networking solutions. Contact your Cisco representative to find out more about how Cisco Advanced Services experts can help improve staff productivity, and help reduce the total cost of ownership for your network.

## Conclusion

Content filtering and control is an essential part of the mobile operator's content-delivery strategy. More than a point solution, the Cisco Mobile Content Filtering and Control solution is part of a wider framework allowing mobile operators to build a comprehensive, intelligent mobile Internet edge. The Cisco mSEF provides a wide range of service capabilities, including content-based billing, mobility management, single Access Point Name (APN) provisioning, and subscriber authentication and authorization.

For more information on the Cisco Mobile Content Filtering and Control solution, contact your Cisco account manager or visit: [www.cisco.com/go/mobile](http://www.cisco.com/go/mobile).



**Americas Headquarters**  
Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
[www.cisco.com](http://www.cisco.com)  
Tel: 408 526-4000  
800 553-NETS (6387)  
Fax: 408 527-0883

**Asia Pacific Headquarters**  
Cisco Systems, Inc.  
168 Robinson Road  
#29-01 Capital Tower  
Singapore 068912  
[www.cisco.com](http://www.cisco.com)  
Tel: +65 6317 7777  
Fax: +65 6317 7799

**Europe Headquarters**  
Cisco Systems International BV  
Haarlerbergpark  
Haarlerbergweg 13-19  
1101 CH Amsterdam  
The Netherlands  
[www-europe.cisco.com](http://www-europe.cisco.com)  
Tel: +31 0 800 020 0791  
Fax: +31 0 20 357 1100

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](http://www.cisco.com/go/offices).

©2007 Cisco Systems, Inc. All rights reserved. CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc., and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, IQ Expertise, the IQ logo, IQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, Packet, PIX, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0701R)