



Application Note

Cisco Router and Security Device Manager URL Filtering

Introduction

Cisco® Router and Security Device Manager (SDM) allows you to configure and maintain the local URL list and URL filter server list.

URL Filtering

URL filtering is a feature of Cisco IOS® Software. It prevents users from accessing Websites based on information contained in a URL list. You can maintain a local URL list on the router, and you can use URL lists stored on Websense or Secure Computing URL filter list servers. URL filtering provides solutions to Web access issues, including lost productivity, liability, and competitiveness; it is enabled by configuring an application security policy.

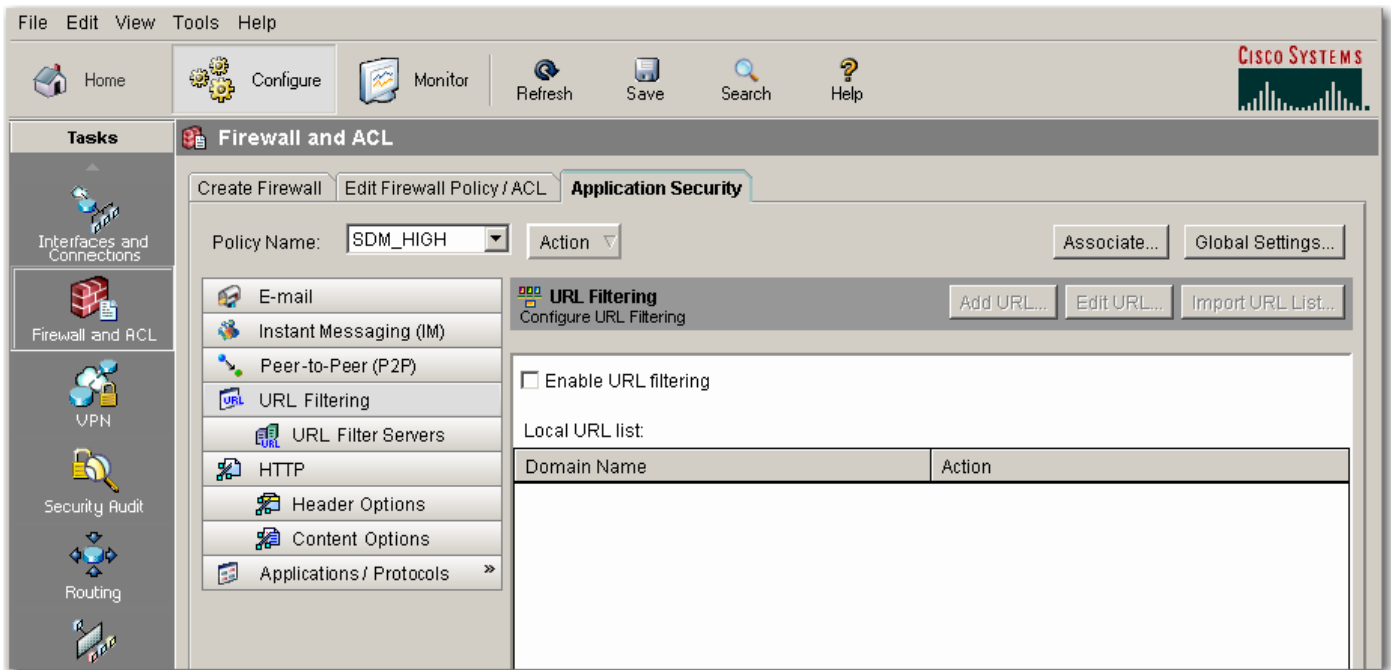
Even if no application security policy is configured on the router, you can still maintain a local URL list and a URL filter server list that can be used for URL filtering when a policy is created that enables it.

URL Filtering Precedence

From the Cisco SDM, URL filtering must be enabled by going to **Configure > Firewall and ACL > Application Security > URL Filtering** and clicking **Enable URL Filtering**. This can only be done when an application security policy is configured on the router. In Figure 1, the SDM_HIGH application security policy is configured.



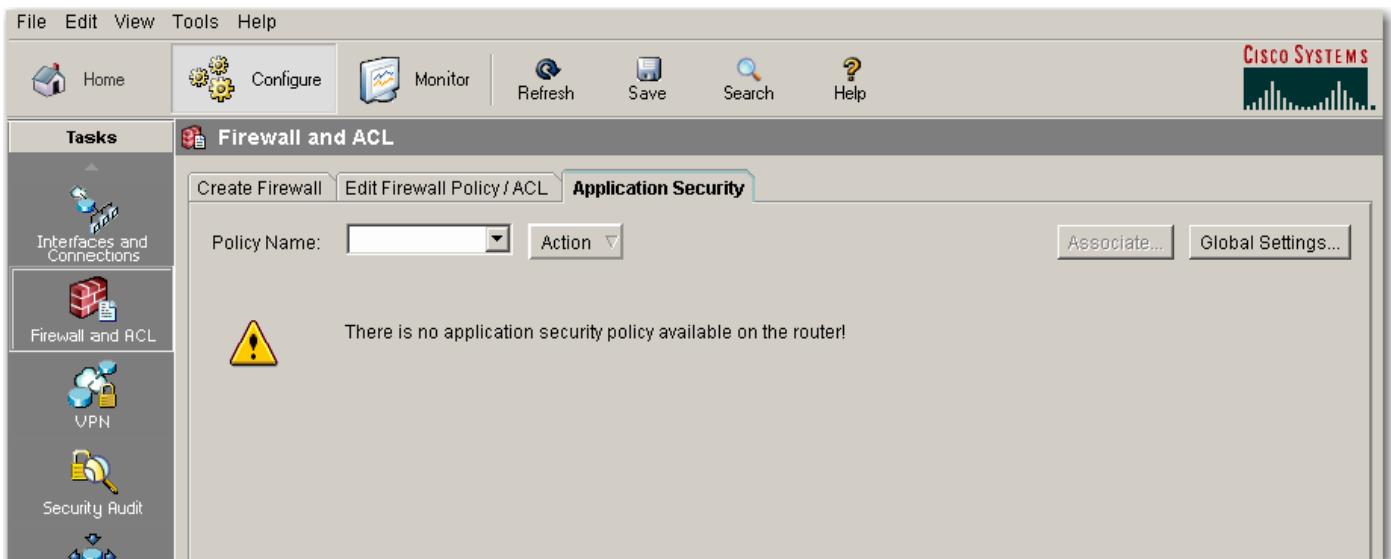
Figure 1. Application Security Policy Is Configured



After checking **Enable URL filtering**, the **Add URL...**, **Edit URL...**, and **Import URL List...** buttons are activated.

Figure 2 shows when an application security policy is not configured on the router.

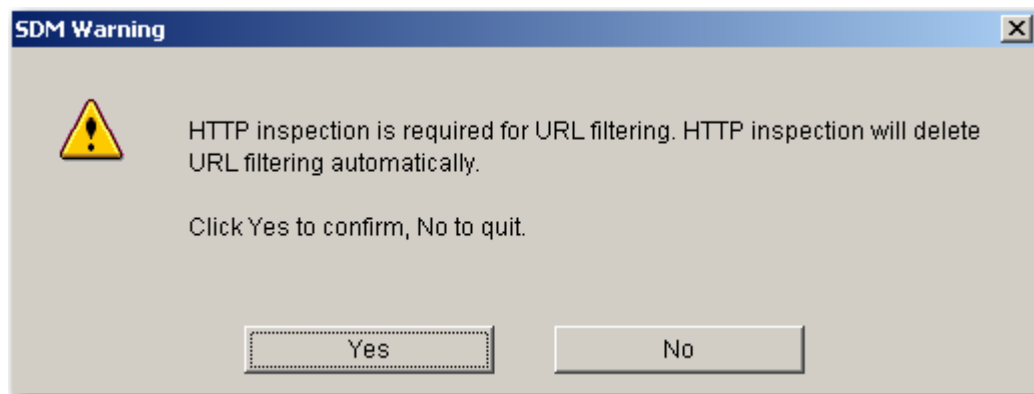
Figure 2. Application Security Is Not Configured



URL filtering requires HTTP inspection enabled; HTTP inspection will be enabled automatically when enabling URL filtering. When URL filtering is enabled, disabling HTTP inspection will disable URL filtering. Cisco SDM prompts user with a warning message (Figure 3) to confirm the disabling.



Figure 3. Disabling HTTP Inspection



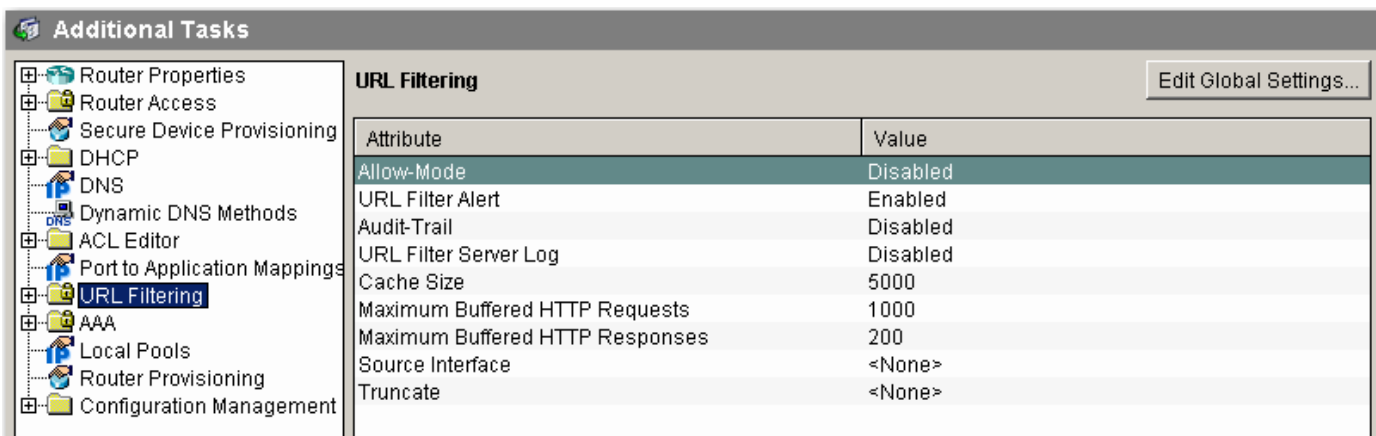
You can maintain the local URL list and the URL filter server list in the Additional Tasks screens or in the Application Security windows. The global settings for URL filtering can only be maintained from the Additional Tasks window.

URL Filtering – Additional Tasks

Maintaining the Local URL List

To create a URL entry, at **Configure Mode**, select the **Additional Tasks**, select **URL Filtering**. This window displays the global settings for URL filtering on the router (Figure 4).

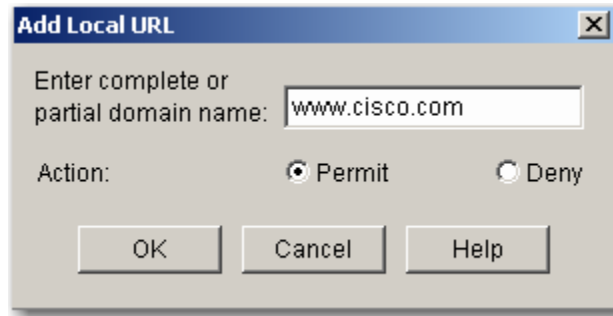
Figure 4. Global Settings for URL Filtering



Expand **URL Filtering** and select **Local URL Filtering**. Click the **Add...** button; the **Add Local URL** dialog appears. Enter a complete domain name, such as “www.cisco.com” (Figure 5), and select **Permit**. All HTTP traffic destined to this domain, such as “www.cisco.com/web/about/index.html” and “www.cisco.com/web/learning/index.html”, will be permitted.

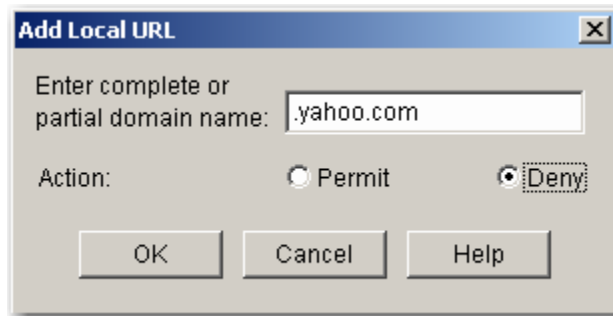


Figure 5. Complete Domain Name



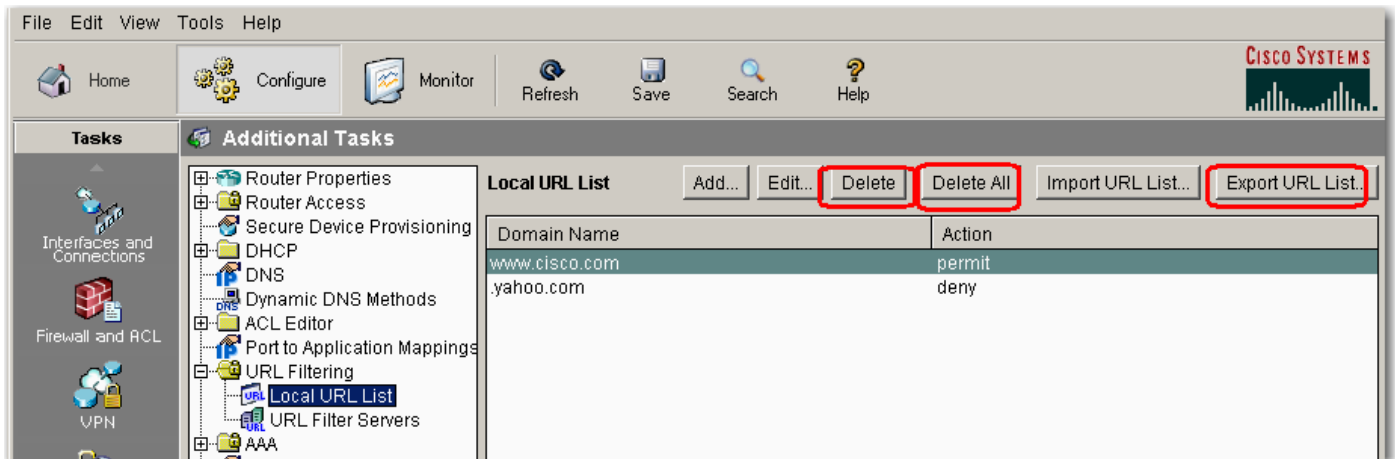
Enter a partial domain, such as “.yahoo.com” (Figure 6), and select **Deny**. All HTTP traffic destined to the URLs whose domain names end with this partial domain name, such as “mail.yahoo.com” and “smallbusiness.yahoo.com”, will be denied (blocked).

Figure 6. Partial Domain Name



Use the **Delete** or **Delete All** button to delete one selected entry or all entries on the router. Use the **Export URL List** button to save the local URL list to your PC (Figure 7). When you save a URL list to your PC, the list is given a .txt extension.

Figure 7. Local URL List



Use the **Import URL List** button to import a URL list from your PC to the router. The URL list that you select must have a .txt or .csv extension. After you select the list on your PC, Cisco SDM displays a dialog (Figure 8).



Figure 8. Import URL List



This dialog allows you to examine the URL list you are importing from your PC to the router and to specify what you want to do with each entry. If a URL entry in this dialog is not already present on the router, you can add it to the list on the router by clicking **Append**. If you attempt to add an entry that is already in the URL list, it will not be added even if the action specified for the domain in the entry is different from the action that is already in the list. If a URL entry is already present on the router but you want to replace it with the entry in this dialog, click **Replace**. If the entry checked is not already in the router's list, **Replace** has no effect.

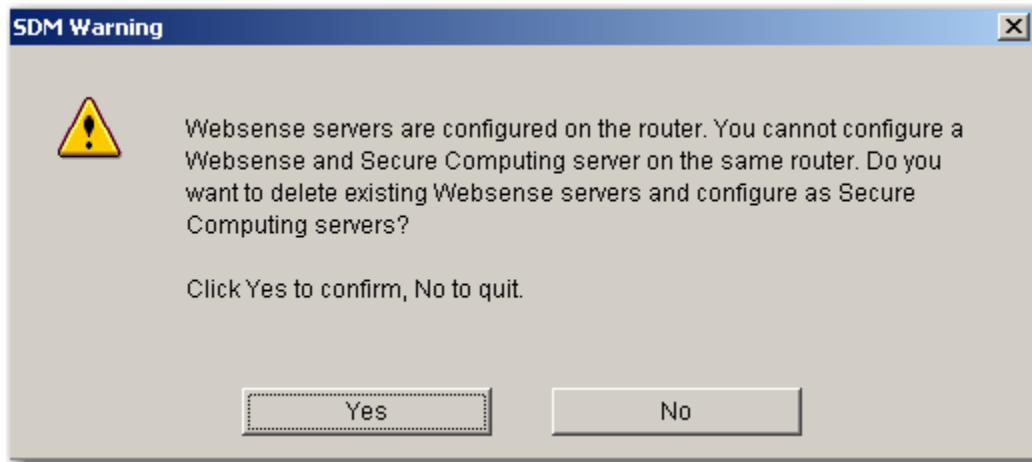
Configuring the URL Filter Server

The router can send HTTP requests to URL filtering servers that are capable of storing much larger URL lists than the router can store. If the router is configured with a URL filter server list, the router sends requests that do not match entries in the local list to the URL filter server it has a connection to, and permits or denies the request based on the response it receives from the server. When the server that the router is connected to fails, the router contacts the next server in the list until it establishes a connection.

Note: Cisco IOS Software can only use one type of URL filtering server, and does not allow you to add a server to the list if it is of a different type. When Websense servers are configured on the router, if a user configures a Secure Computing server on the same router, Cisco SDM prompts the user to delete existing Websense servers and configure as a Secure Computing server (Figure 9). The same is true in reverse.

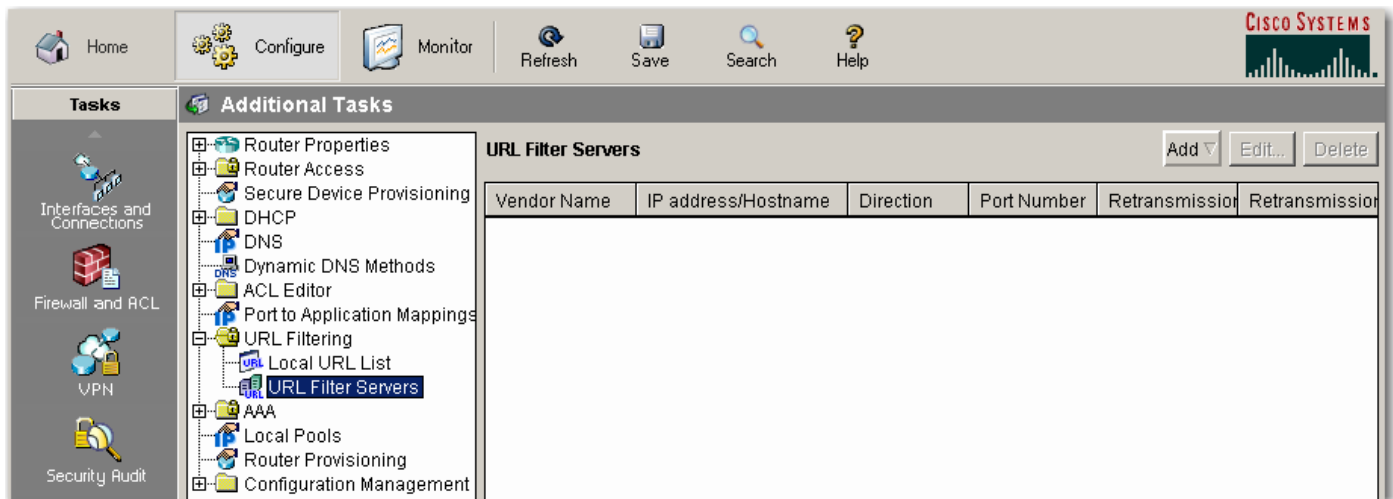


Figure 9. Cisco SDM Warning



To add a URL filtering server, at **Configure Mode**, select the **Additional Tasks**, expand **URL Filtering**, and select **URL Filter Servers** (Figure 10).

Figure 10. URL Filter Servers



Click **Add** and select **Add Websense** or **Add Secure Computing**. In our example, Websense is selected. The Add Websense Server dialog appears (Figure 11).



Figure 11. Add Websense Server Dialog

IP address/Hostname:	172.28.50.176
Direction:	inside
Port Number:	15868
Retransmission Count:	2
Retransmission Timeout:	5 Sec

OK Cancel Help

Enter the IP address or hostname for the server. If you enter a hostname, the router must have a connection to a DNS server to resolve the hostname to an IP address. In our example, IP address **172.28.50.176** is entered.

For Direction, choose **inside** if the URL filter server is part of the inside network. This is usually one of the networks that the router LAN interfaces connect to. Choose **outside** if the router is in the outside network. This is usually one of the networks that the router WAN interfaces connect to. In our example, **inside** is entered.

For Port Number, if you are adding a Websense server, the default value **15868** is listed. If you are adding a Secure Computing server, the default value 4005 is listed. Change this port number if the port that the server listens is different from the default. In our example, the default value for the Websense server is entered.

For the Retransmission Count, enter the number of times that you want the router to attempt to retransmit the request if no response arrives from the server. The default value is 2. This field accepts values from 1 to 10. In our example, **2** is entered

For Retransmission Timeout, enter the number of seconds that the router should wait for a response from the server before retransmitting the request. The default value is 5 seconds, which is entered in our example.

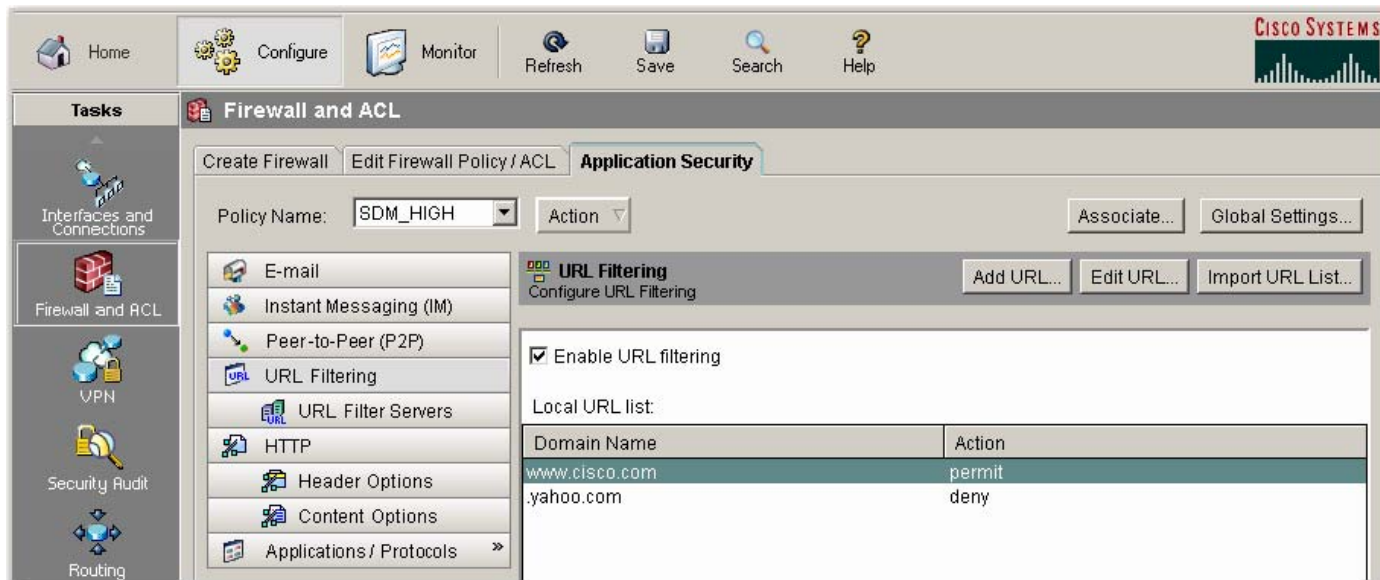
Adding URL Filtering to Application Security Policy

Maintaining the Local URL List

To create a URL entry, at **Configure Mode**, select the **Firewall and ACL** and click the **Application Security** tab. Click **URL Filtering** (Figure 12). You can include URL filtering capabilities in the application security policy by clicking **Enable URL filtering**.



Figure 12. Application Security – URL Filtering



The local URL list can be maintained in this window by using the **Add URL...**, **Edit URL...**, and **Import URL List...** buttons. Click **Apply Changes** to deliver the configuration to the router. Please refer to “URL Filtering – Additional Tasks” for more details.

Configuring the URL Filter Server

To configure the URL filter server, click **URL Filter Servers**. You can add and edit URL filter servers by clicking the **Add** and **Edit** buttons. Please refer to “URL Filtering – Additional Tasks” for more details.

URL Filtering Monitoring

URL filtering logs are displayed at **Monitor > Logging > Application Security Log**.

**Corporate Headquarters**

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters

Cisco Systems International
BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters

Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 317 7777
Fax: +65 317 7799

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

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland • Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Copyright © 2006 Cisco Systems, Inc. All rights reserved. CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, 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, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, Packet, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, 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. (0601R)

Printed in the USA