Configuring Cisco IOS Content Filtering Using Cisco Security Manager Version 3.3 in Cisco IOS Software Releases 12.4(15)XZ and Later

This document guides users through the easy steps involved in configuring Cisco IOS® Content Filtering using Cisco® Security Manager Version 3.3.

Cisco Security Manager is an enterprise-class management application designed to configure firewall, VPN, intrusion prevention (IPS), and IOS Content Filtering security services on Cisco network and security devices. Cisco Security Manager can be used in networks of all sizes—from small networks to large networks consisting of thousands of devices—by using policy-based management techniques. For a synopsis of Cisco Security Manager features and benefits, including new features in Version 3.3, refer to the Cisco Security Manager 3.3 data sheet at http://www.cisco.com/go/csmanager. Customer can download Cisco Security Manager 3.3 from Cisco.com at http://www.cisco.com/cgi-bin/tablebuild.pl/csm-app.

Prerequisites

Download and install Cisco Security Manager Version 3.3 from http://www.cisco.com/cgi-bin/tablebuild.pl/csm-app. A valid Cisco account is needed. Additional information on how to add a device to Cisco Security Manager can be found at http://www.cisco.com/go/csmanager.

Following are the tasks involved in configuring Cisco IOS Content Filtering using Cisco Security Manager Version 3.3:

Task 1: Create a parameter map to specify per-policy parameters when Content Filtering is used.

Task 2: Create a class map to configure categories and reputation of a URL that needs to be blocked or logged.

Task 3: Create a policy map to configure a URL filtering policy. Under this policy map, you can configure one parameter map and multiple class maps.

Task 4: Configure the Trend Global Settings.

Task 5: Create zone-based firewall rules to enable Content Filtering from the private interface to the Internet.

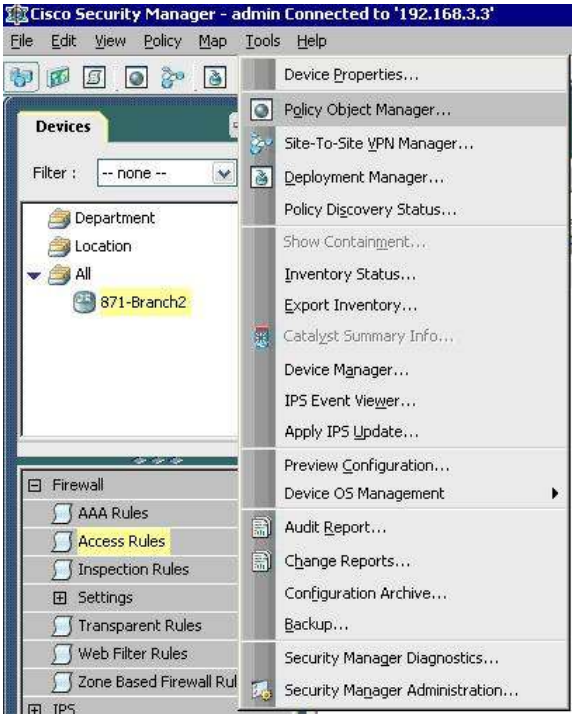
Task 6: Submit and deploy changes to the router.

Task 7: Test the Content Filtering configurations.

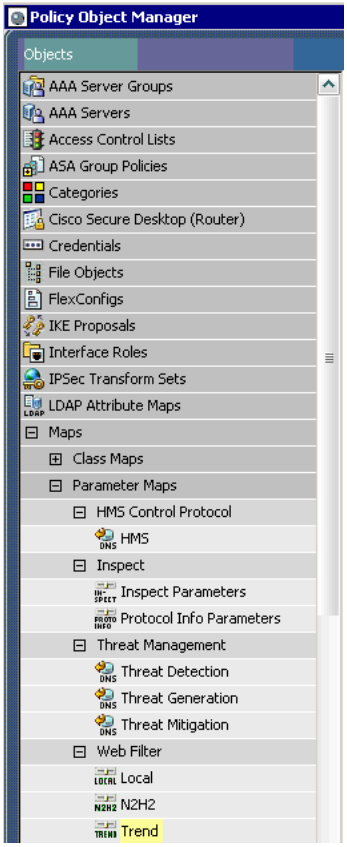
Task 1: Create a parameter map to specify per-policy parameters when Content Filtering is used.

Note: To create a parameter map, class map, and policy map, **Policy Object Manager** can be used. From the **Policy Object Manager**, re-usable objects can be created (for example, to represent network addresses, services, device settings, time ranges, or VPN parameters). Policies can be defined once and deployed on multiple devices to avoid manually entering values.

Step 1. From the Cisco Security Manager client GUI, choose **Tools → Policy Object Manager**.

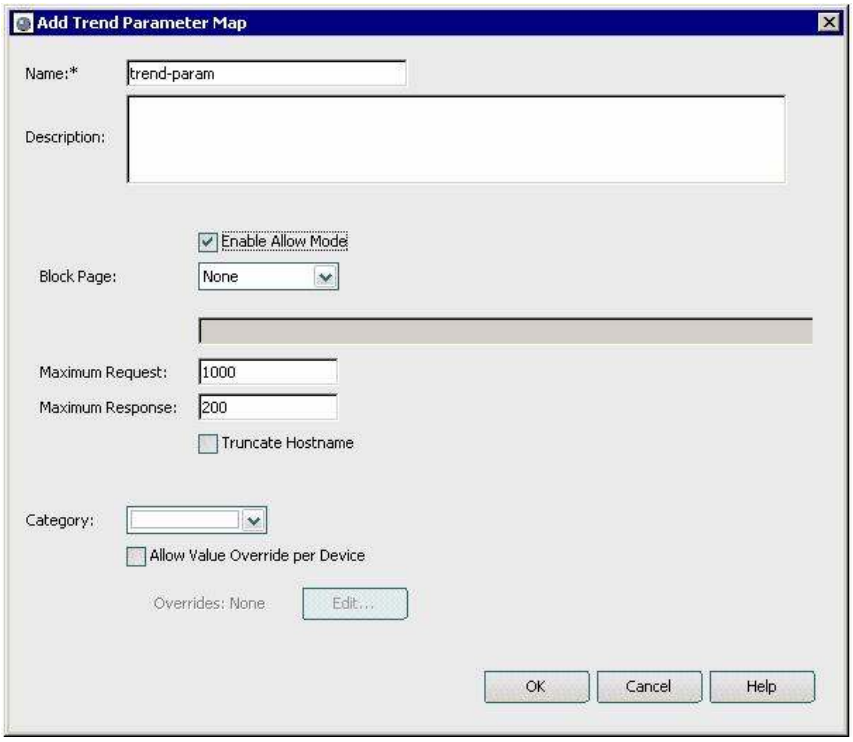


Step 2. From the Policy Object Manager, choose **Maps → Parameter Maps → Web Filter → Trend**.



Step 3. Create a new parameter map by clicking on the button.

Step 4. Enter the name of the parameter map. You can check **Enable Allow Mode** to allow web traffic when the Trend server is unreachable. **Maximum Request** and **Maximum Response** can also be configured. Click **OK**.

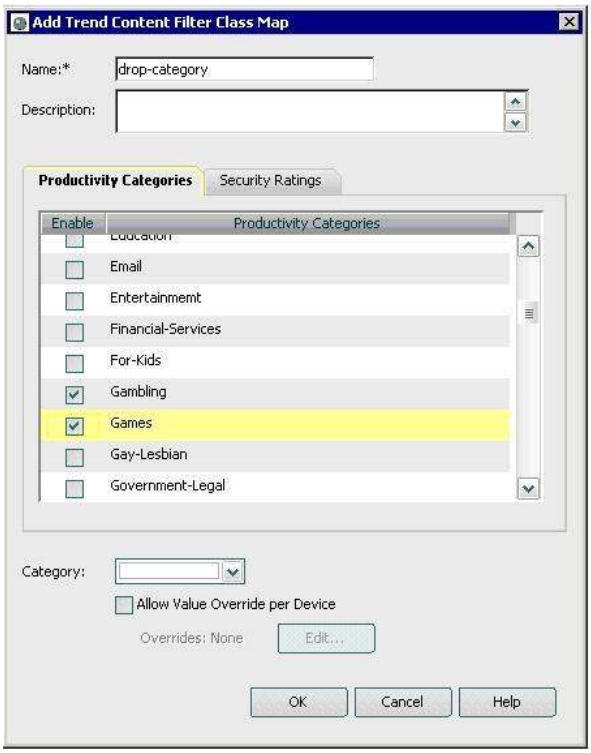


Step 5. You should see the following screen once you have configured the parameter map.

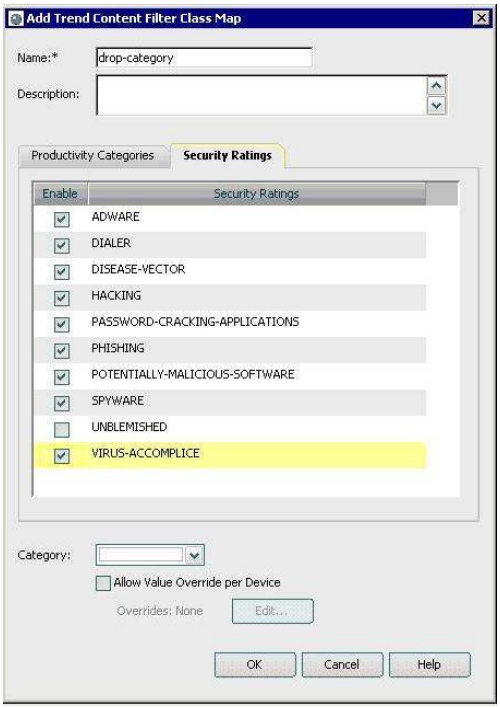
Task 2: Create a class map to configure categories and reputation of a URL that needs to be blocked or logged.

Step 6. Create a Trend class map by clicking on the button from **Maps → Class Maps → Web Filter → Trend**.

Step 7. Productivity categories contain websites that hinder employee productivity or house objectionable content. For example, the Gambling category contains “Poker.net.” If you don’t want employees visiting gambling websites, you can block the Gambling category. Cisco IOS Content Filtering supports more than 70 productivity categories. Choose the productivity categories you would like to block.

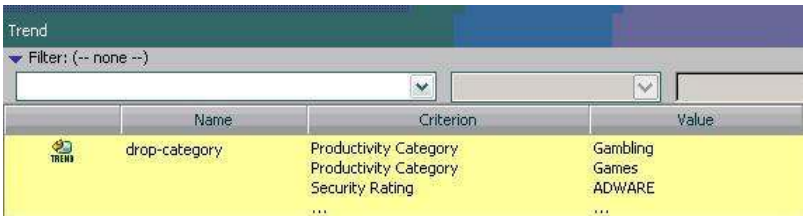


Step 8. Security ratings consist of categories that prevent malicious traffic from being downloaded into your environment. Cisco IOS Content Filtering supports 10 categories, including Adware, Phishing, Spyware, and Hacking. Security ratings are provided from the Trend Micro database that the router points to. The ratings of these websites are determined using various algorithms and industry research to avoid false positives. The URL database is regularly maintained and updated to reflect the latest threat information. Click the **Security Ratings** tab and select the security categories you want to block. **Cisco recommends turning on all the Security Categories except for the Unblemished category.**



Step 9. Click **OK**.

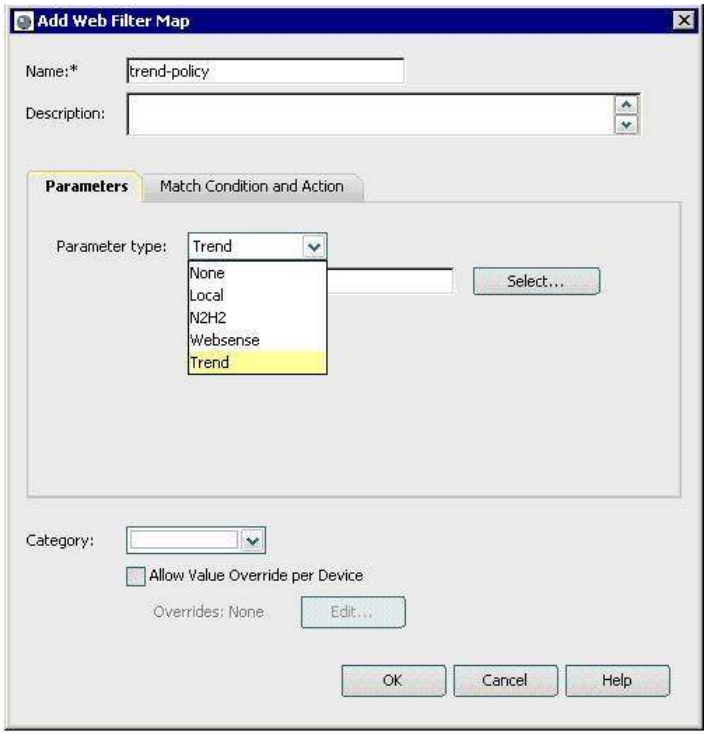
Step 10. Once the Trend class map is configured, you should see the following screen:



Task 3: Create a policy map to configure a URL filtering policy. Under this policy map, you can configure one parameter map and multiple class maps.

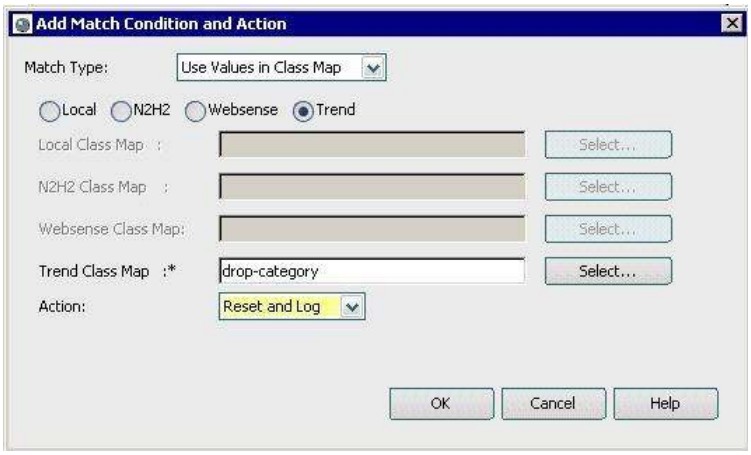
Step 11. Create a web filter policy map to incude the Trend parameter map and class map created in the previous steps. Select **Maps → Policy Map → Web Filter → Web Filter**.

Step 12. Click on  to create a policy map. Under the Parameter type pull-down menu, choose **Trend** and then click **Select** to choose the parameter map created in Step 4.

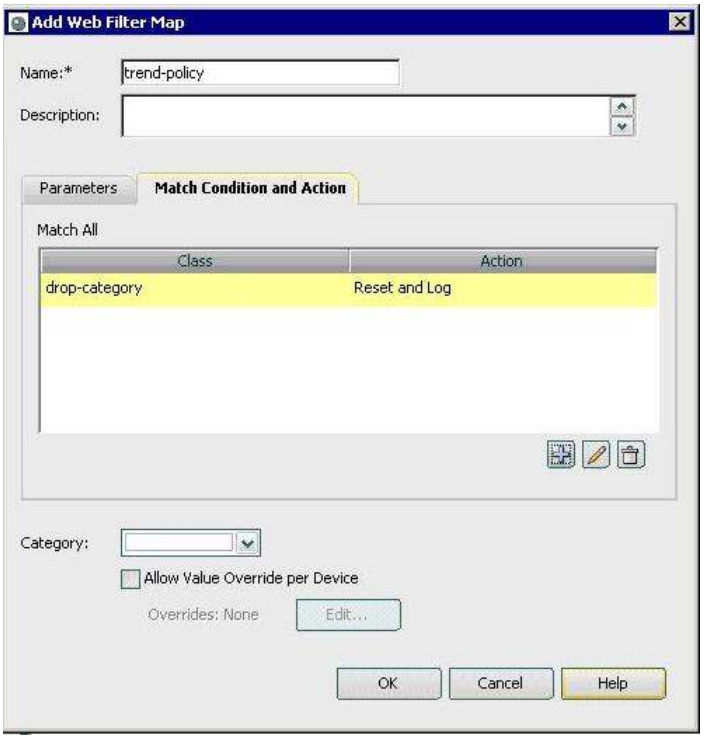


Step 13. Click the **Match Condition and Action** tab to select the class map. Click the  button to add a match condition and action.

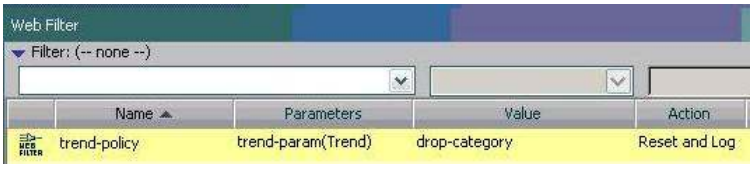
Step 14. **Trend** and click **Select** to choose the Trend class map created in Step 10. Set the desired **Action**. Click **OK**.



Step 15. Once the match condition and action is added, you should see the following screen. Click **OK**.



Step 16. A new web filter policy is created as shown below:



Step 17. Click **Close** to close the Policy Object Manager.

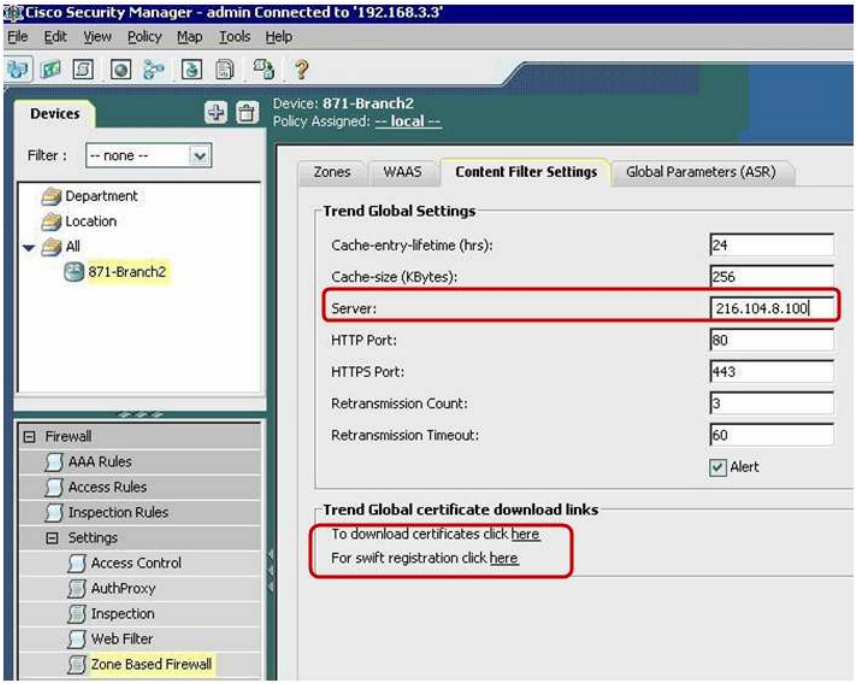
Note: Parameter maps and class maps can also be created from the policy map screen.

Task 4: Configure the Trend Global Settings.

Step 18. Click on the **Device** (871-Branch2 in this example) to configure Content Filtering. Choose **Firewall → Settings → Zone Based Firewall → Content Filter Settings**.

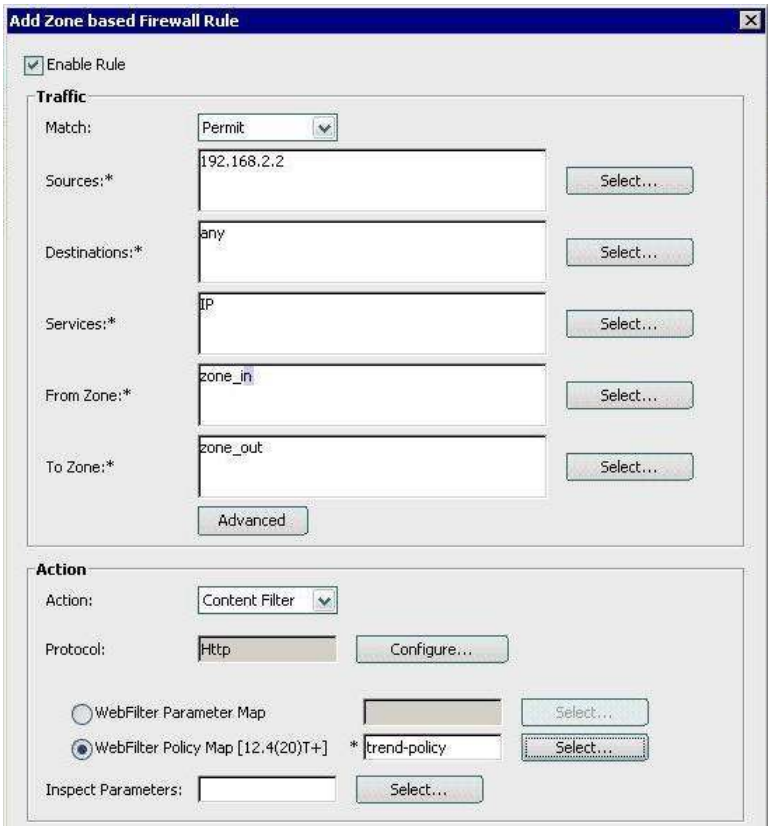
Step 19. Edit the Trend Global Settings.

- Specify the Trend server IP address and modify the other Trend settings.
- For secure communication between router and Content Filter vendor, you will need a digital certificate to be downloaded onto the router. Clicking on the **download certificate** link will open a webpage where you can enter the IP address of the router and download the certificate automatically to the router. Alternatively, this page can be accessed directly from the browser by visiting http://www.cisco.com/en/US/products/ps5854/products_configuration_example09186a0080816c23.shtml.
- To activate the license for Content Filtering, click on the **swift registration** link. You will be redirected to the Product License Registration page https://tools.cisco.com/SWIFT/Licensing/PrivateRegistrationServlet where you will have to enter the Product Authorization Key and register the router.



Task 5: Create zone-based firewall rules to enable Content Filtering from the private interface to the Internet.

Step 20. Click on **Firewall → Zone Based Firewall Rules**. Click  to add a new rule. Under **Action**, select **Content Filter**. Select **WebFilter Policy Map [12.4(20)T+]** and click **Select** to choose the policy map created in Step 15. Click **OK**.

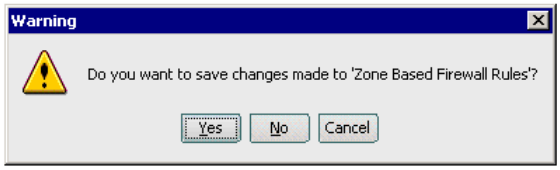


Step 21. You should see a new rule created as shown below:

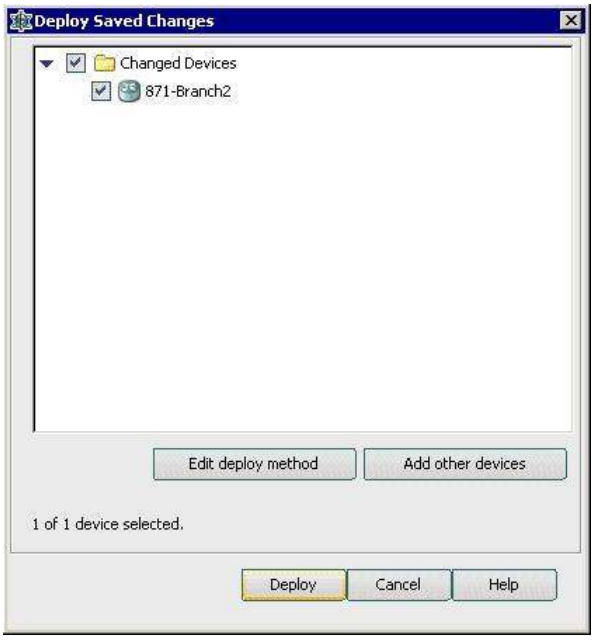
Task 6: Submit and deploy changes to the router.

Step 22. It is highly recommended to click the **Save** button to save the changes.

Step 23. From the File menu, click **Submit and Deploy** to deploy the changes to the router. In case you have not saved the changes, you will get a warning to save the changes. Click **Yes**.



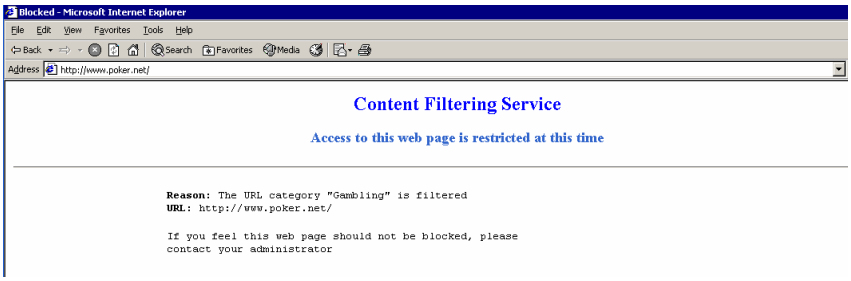
Step 24. You will get a **Deploy Saved Changes** screen displaying the changed devices. Click **Deploy**.



Step 25. You should get a successful deployment status. Click **Close** to exit.

Task 7: Test the Content Filtering configurations.

Step 26. Content Filtering is currently enabled on the router. From the web browser of the local PC connected to the router, surf for any websites belonging to productivity categories you have blocked. For example, if you have blocked the Gambling category, try to browse for any gambling sites. You should get a blocked page that states that the page is blocked because it belongs to the Gambling category. Here is a screen capture of the blocked page:



References

- Cisco IOS Content Filtering
  http://www.cisco.com/go/ioscontentfiltering
- Cisco IOS Content Filtering Deployment Guide
  http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6643/white_paper_c89-492776.html
- Cisco Security Manager
  http://www.cisco.com/go/csmanager

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 C27-552799-00 07/09