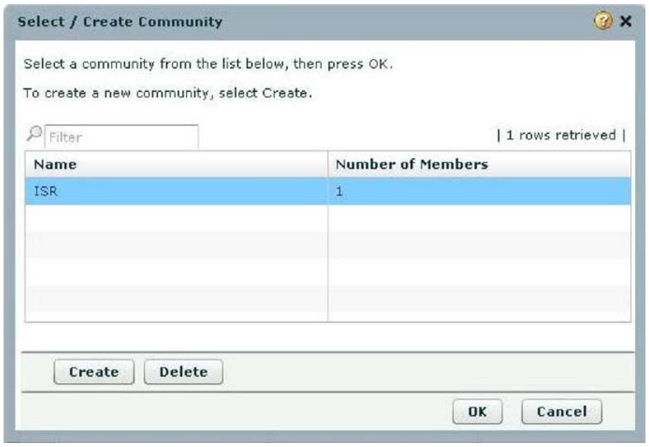
Configuring Cisco IOS Content Filtering using Cisco Configuration Professional V1.1 in 12.4(15)XZ and Later Releases

This document guides users through the several steps involved in configuring Cisco IOS Content Filtering using the Cisco Configuration Professional V1.1 (CCP).

Following are the tasks involved in configuring Cisco IOS Content Filtering:

Step 1. Download **CCP V1.1** from the URL http://tools.cisco.com/support/downloads/pub/Redirect.x?mdfid=281795035 and install it on the local PC. A valid Cisco account is needed to download CCP. Additional information on how to add a device to CCP can be found at the CCP website http://www.cisco.com/go/ccp

Step 2. Launch CCP from the local PC and choose the **community** which has the router you want to configure IOS Content Filtering

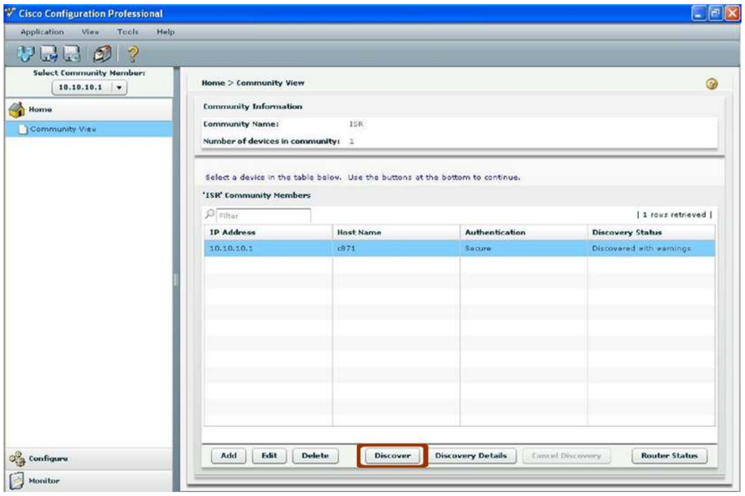


Select a community from the list below, then press OK.

To create a new community, select Create.

Name	Number of Members
ISR	1

Step 3. Discover the device where you want to configure IOS Content Filtering by highlighting the router and clicking on the **Discover** button.



Community Information

Community Name: ISR

Number of devices in community: 1

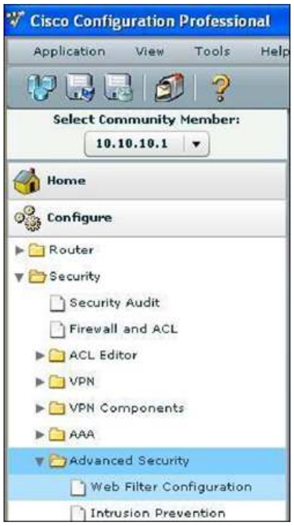
Select a device in the table below. Use the buttons at the bottom to continue.

'ISR' Community Members

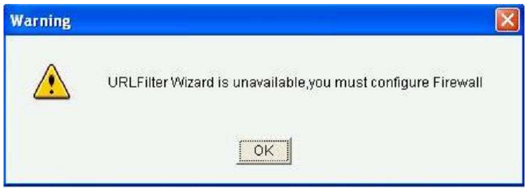
Filter | 1 rows retrieved |

IP Address	Host Name	Authentication	Discovery Status
10.10.10.1	c871	Secure	Discovered with warnings

Step 4. To setup Content Filtering Select **Configure -> Security -> Advanced Security -> Web Filter Configuration** on the left panel of CCP

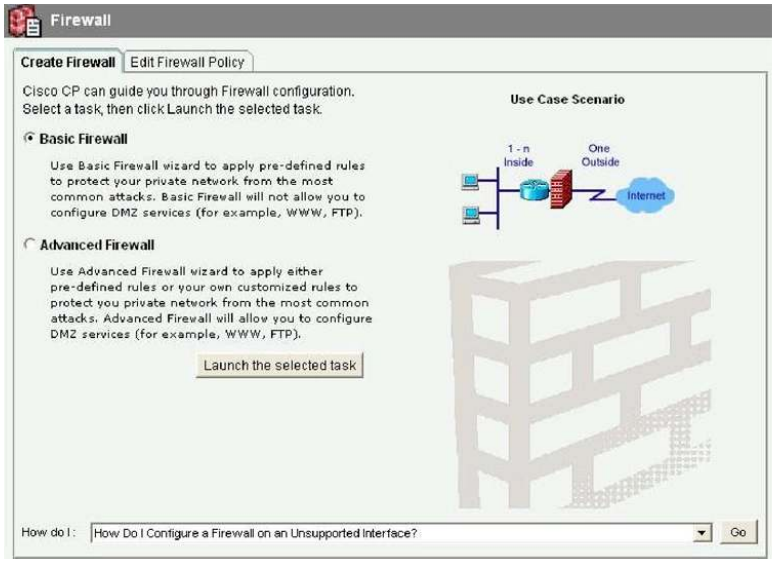


Step 5. The pre-requisite for enabling Content Filtering is that Zone-based Firewall has to enabled on the interfaces. If Zone-based Firewall is not configured, you will get a warning that the “URLFilter wizard is unavailable. You must configure Firewall”. Click **OK**



URLFilter Wizard is unavailable,you must configure Firewall

Step 6. You will be redirected to the Firewall Configuration page where Zone-based Firewall has to be configured.



Cisco CP can guide you through Firewall configuration.
Select a task, then click Launch the selected task.

● Basic Firewall

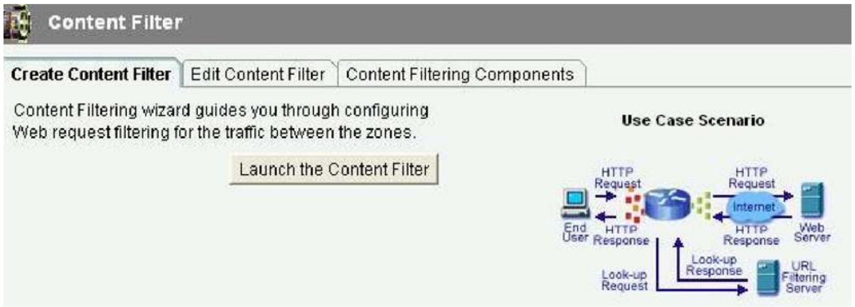
Use Basic Firewall wizard to apply pre-defined rules to protect your private network from the most common attacks. Basic Firewall will not allow you to configure DMZ services (for example, WWW, FTP).

○ Advanced Firewall

Use Advanced Firewall wizard to apply either pre-defined rules or your own customized rules to protect you private network from the most common attacks. Advanced Firewall will allow you to configure DMZ services (for example, WWW, FTP).

How do I : How Do I Configure a Firewall on an Unsupported Interface?

Step 7. Once the Firewall is configured, you will be allowed to configure Content Filtering. Click on **Launch the Content Filter** to get started with the configuration wizard for setting up Content Filtering

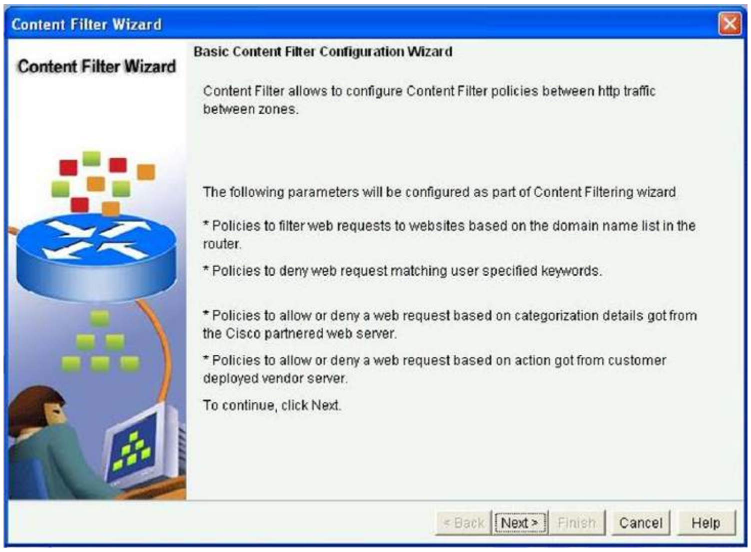


Content Filter

Create Content Filter | Edit Content Filter | Content Filtering Components

Content Filtering wizard guides you through configuring Web request filtering for the traffic between the zones.

Step 8. The wizard appears with the summary of the tasks that it performs to setup Content Filtering. Click **Next**.



Content Filter Wizard

Content Filter Wizard

Basic Content Filter Configuration Wizard

Content Filter allows to configure Content Filter policies between http traffic between zones.

The following parameters will be configured as part of Content Filtering wizard

* Policies to filter web requests to websites based on the domain name list in the router.

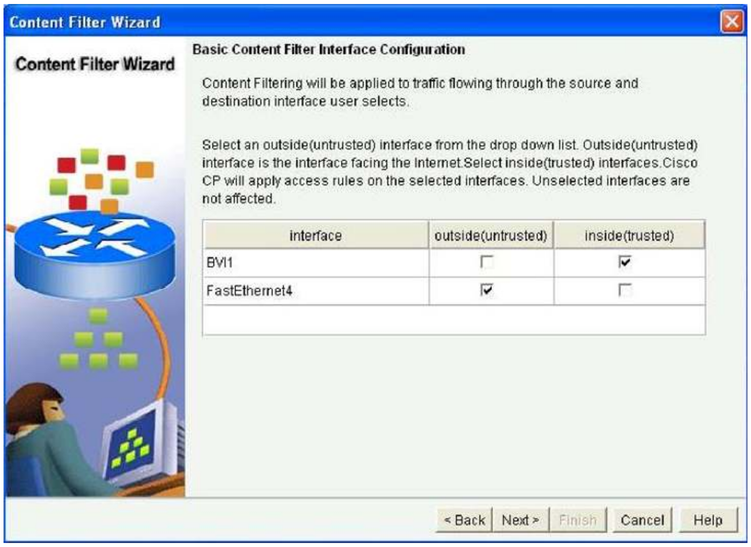
* Policies to deny web request matching user specified keywords.

* Policies to allow or deny a web request based on categorization details got from the Cisco partnered web server.

* Policies to allow or deny a web request based on action got from customer deployed vendor server.

To continue, click Next.

Step 9. Select the interfaces on which the Content Filtering will be applied. Choose the inside and outside interfaces. Click **Next.**



Content Filter Wizard

Content Filter Wizard

Basic Content Filter Interface Configuration

Content Filtering will be applied to traffic flowing through the source and destination interface user selects.

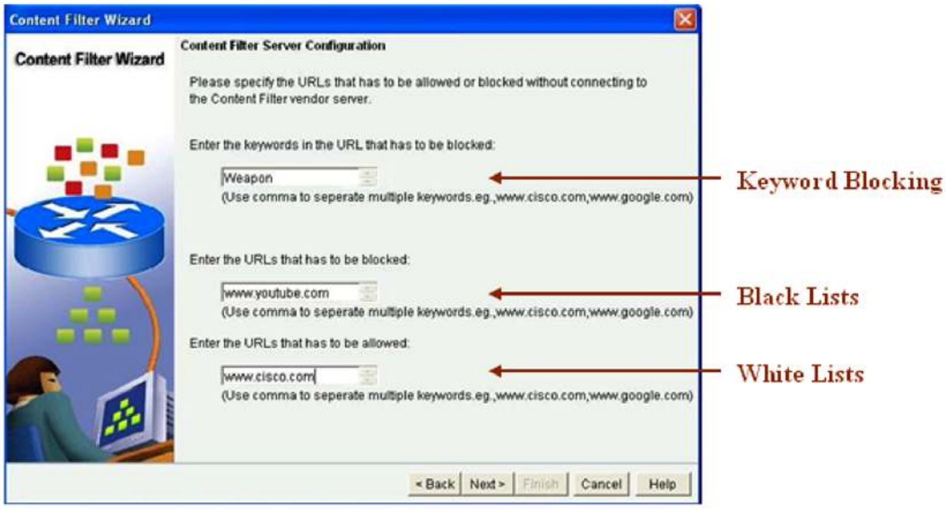
Select an outside(untrusted) interface from the drop down list. Outside(untrusted) interface is the interface facing the Internet.Select inside(trusted) interfaces.Cisco CP will apply access rules on the selected interfaces. Unselected interfaces are not affected.

interface	outside(untrusted)	inside(trusted)
BVI1	☐	☑
FastEthernet4	☑	☐

Step 10. Local filtering on Cisco® router allows blocking of Websites based on keywords. Only **keywords** that are not part of the domain are blocked. Specify the keywords in the URL which you want to block.

Step 11. Next we have the black lists. Cisco IOS content filtering supports 100 black lists. This is also part of the local policy in IOS. These are static lists that can be configured in IOS to allow or disallow URLs. Enter the **URLs** which you want to block.

Step 12. Next we have the white lists. Cisco IOS content filtering supports 100 white lists. White lists are useful when you want users to access only certain websites and not anything else. Enter the **URLs** which you want to allow. Click **Next**.



Content Filter Server Configuration

Please specify the URLs that has to be allowed or blocked without connecting to the Content Filter vendor server.

Enter the keywords in the URL that has to be blocked:

Weapon

(Use comma to seperate multiple keywords.eg.,www.cisco.com,www.google.com)

Enter the URLs that has to be blocked:

www.youtube.com

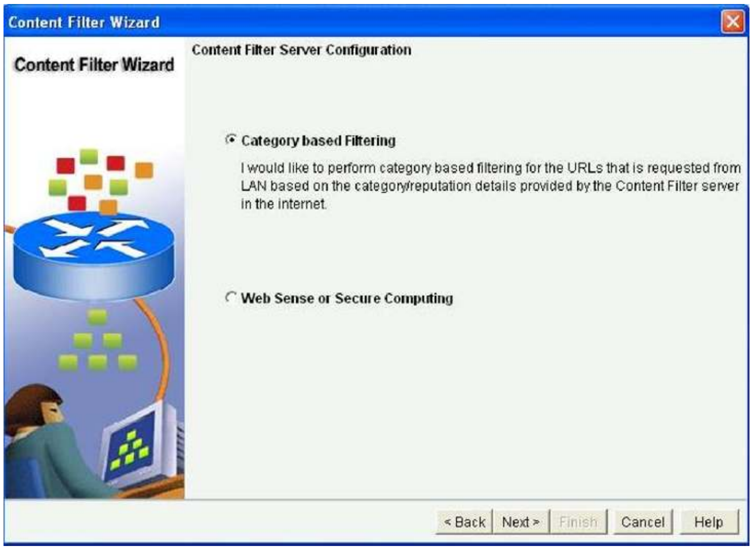
(Use comma to seperate multiple keywords.eg.,www.cisco.com,www.google.com)

Enter the URLs that has to be allowed:

www.cisco.com

(Use comma to seperate multiple keywords.eg.,www.cisco.com,www.google.com)

Step 13. In this screen you get to choose if you want to use Subscription based category filtering or use Websense or Secure Computing for third party filtering. To choose Subscription based category filtering, select **Category Based Filtering**. Cisco has partnered with TrendMicro for Category based Filtering. You will need to have active subscriptions services from TrendMicro to use this option. Click **Next.**



Content Filter Server Configuration

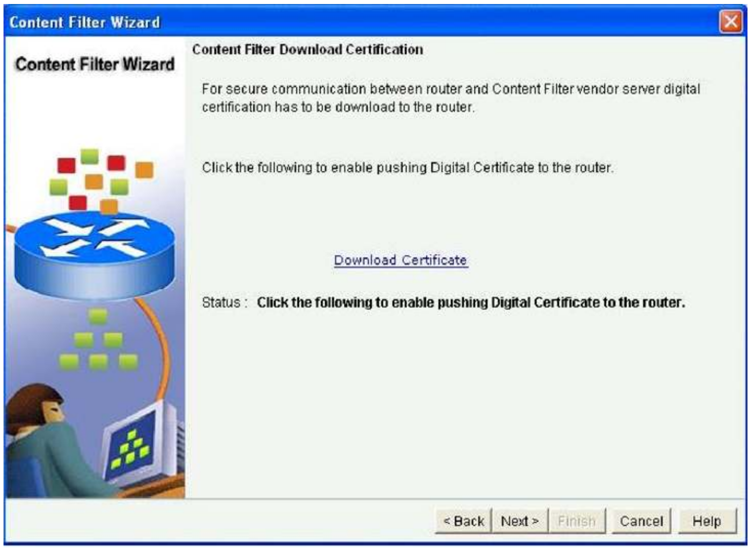
● Category based Filtering

I would like to perform category based filtering for the URLs that is requested from LAN based on the category/reputation details provided by the Content Filter server in the internet.

○ Web Sense or Secure Computing

Step 14. Enter the **DNS Server IP address** and Click **Next.**

Step 15. For Secure Communication between router and Content Filter vendor you will need a digital certificate to be downloaded on to the router. Click on Download Certificate.



Content Filter Download Certification

For secure communication between router and Content Filter vendor server digital certification has to be download to the router.

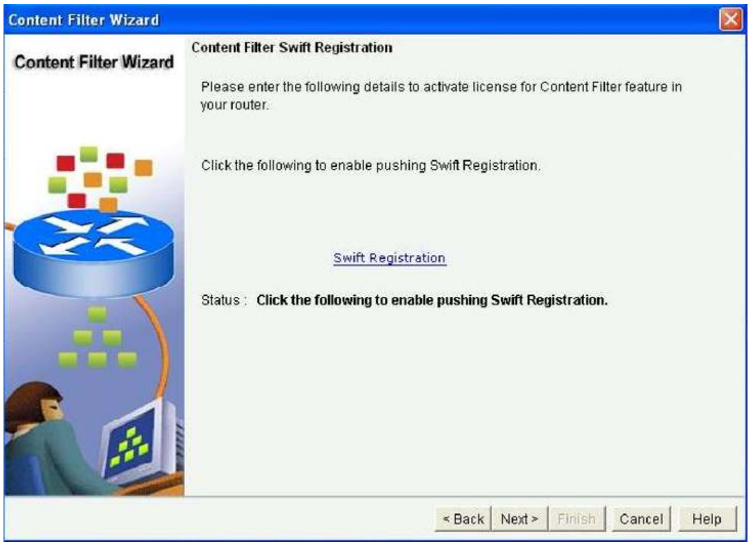
Click the following to enable pushing Digital Certificate to the router.

Download Certificate

Status : **Click the following to enable pushing Digital Certificate to the router.**

Step 16. You will get a webpage where you can enter the IP address of the router and download the certificate automatically on the router. Alternatively, this page can be accessed directly from the browser with the URL http://www.cisco.com/en/US/products/ps5854/products_configuration_example09186a0080816c23.shtml. Click **Next**.

Step 17. To activate the license for Content Filtering click on **Swift Registration**. 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.



Content Filter Swift Registration

Please enter the following details to activate license for Content Filter feature in your router.

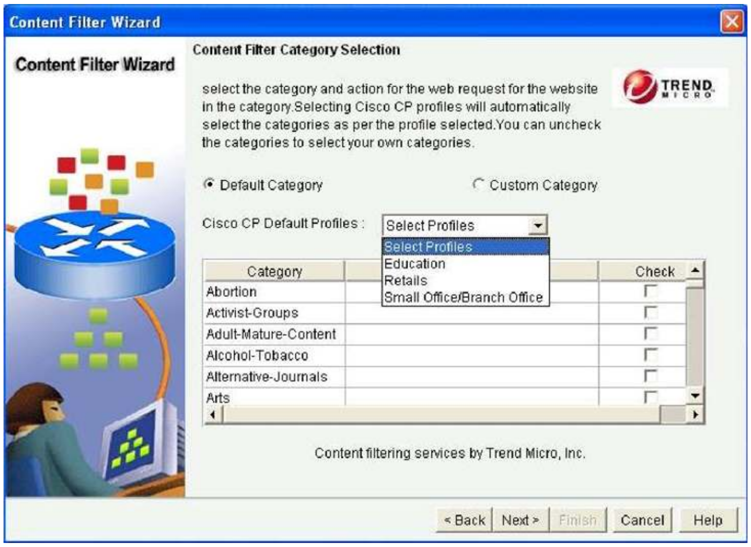
Click the following to enable pushing Swift Registration.

Swift Registration

Status : **Click the following to enable pushing Swift Registration.**

Step 18. Click **Next**.

Step 19. In this screen you get to choose the Productivity Categories. Productivity categories contain web sites 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. There are three pre-selected categories for you to block based on common deployment in the **retail, education** or **small office/branch office verticals**. Choose **Default Category** to start with one of these profiles.



Content Filter Wizard

Content Filter Category Selection

select the category and action for the web request for the website in the category.Selecting Cisco CP profiles will automatically select the categories as per the profile selected.You can uncheck the categories to select your own categories.

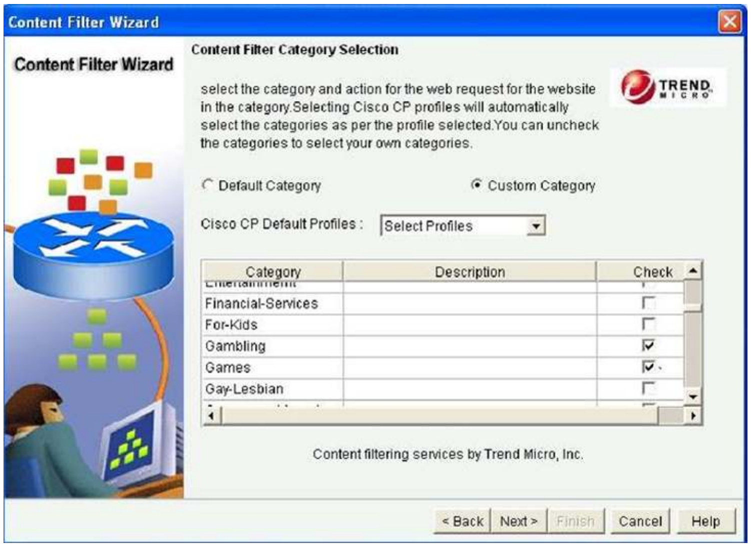
● Default Category ○ Custom Category

Cisco CP Default Profiles : Select Profiles

Category		Check
Abortion		□
Activist-Groups		□
Adult-Mature-Content		□
Alcohol-Tobacco		□
Alternative-Journals		□
Arts		□

Content filtering services by Trend Micro, Inc.

Step 20. If you want to choose your own categories select **Custom Category**. Check all the Categories you want to block on.



Content Filter Wizard

Content Filter Category Selection

select the category and action for the web request for the website in the category.Selecting Cisco CP profiles will automatically select the categories as per the profile selected.You can uncheck the categories to select your own categories.

○ Default Category ● Custom Category

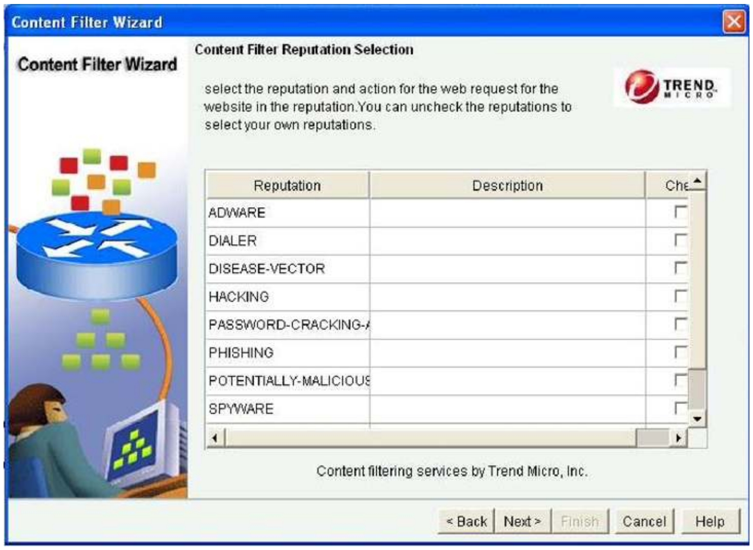
Cisco CP Default Profiles : Select Profiles

Category	Description	Check
Entertainment		□
Financial-Services		□
For-Kids		□
Gambling		☑
Games		☑
Gay-Lesbian		□

Content filtering services by Trend Micro, Inc.

Step 21. Click **Next**.

Step 22. In this screen you get to choose the **Security Ratings**. Security Ratings consist of categories that prevent malicious traffic from being downloaded into your environment. IOS content filtering supports 10 categories such as **Adware, Phishing, Spyware** and **Hacking**. Security ratings are provided from the Trend Micro database that the ISR 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. Select the security categories you want to block on. **Cisco recommends turning on all the Security Categories except for UNBLEMISHED category**.



Content Filter Reputation Selection

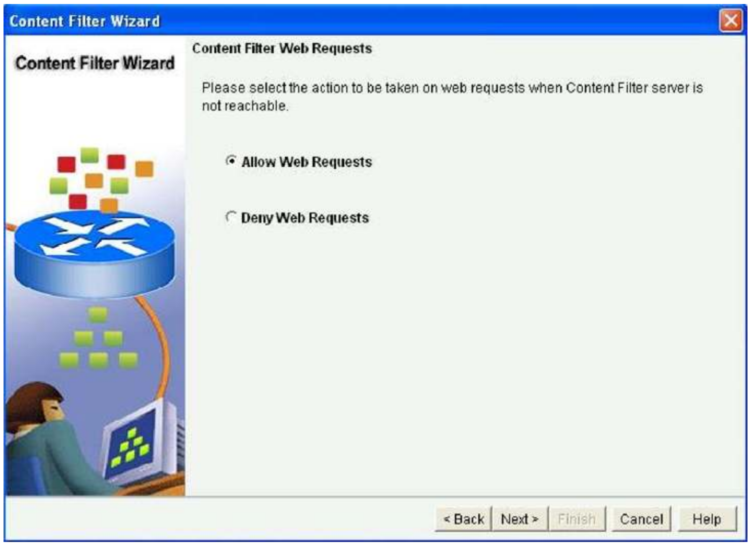
select the reputation and action for the web request for the website in the reputation.You can uncheck the reputations to select your own reputations.

Reputation	Description	Che
ADWARE		☐
DIALER		☐
DISEASE-VECTOR		☐
HACKING		☐
PASSWORD-CRACKING-/		☐
PHISHING		☐
POTENTIALLY-MALICIOUS		☐
SPYWARE		☐

Content filtering services by Trend Micro, Inc.

Step 23. Click **Next**.

Step 24. In case the content filtering database is not reachable, you have the following options—allow or disallow all web requests. You can choose to **Allow Web Requests** to allow all the web traffic. If you want to block all the web traffic then, choose **Disallow Web Requests**.



Content Filter Web Requests

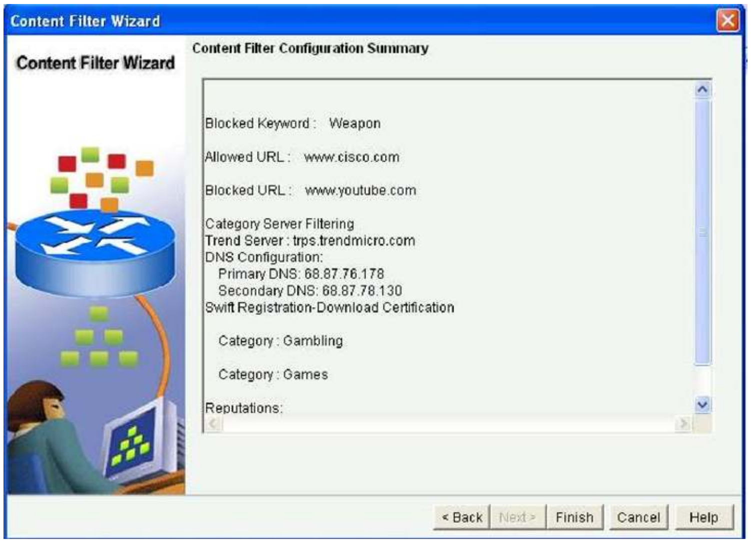
Please select the action to be taken on web requests when Content Filter server is not reachable.

● Allow Web Requests

○ Deny Web Requests

Step 25. Click **Next.**

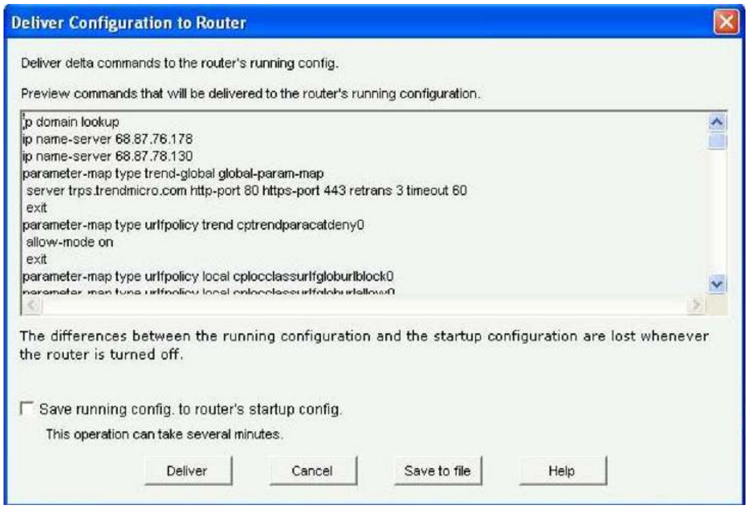
Step 26. Verify the Content Filter configuration and Click on **Finish** to deliver the configurations to the router.



Content Filter Configuration Summary

```
Blocked Keyword :   Weapon

Allowed URL :   www.cisco.com

Blocked URL :   www.youtube.com

Category Server Filtering
Trend Server : trps.trendmicro.com
DNS Configuration:
   Primary DNS: 68.87.76.178
   Secondary DNS: 68.87.78.130
Swift Registration-Download Certification

   Category : Gambling

   Category : Games

Reputations:
```

Step 27. You will get a preview of the commands to be delivered on the router. Click **Deliver**.



Deliver Configuration to Router

Deliver delta commands to the router's running config.

Preview commands that will be delivered to the router's running configuration.

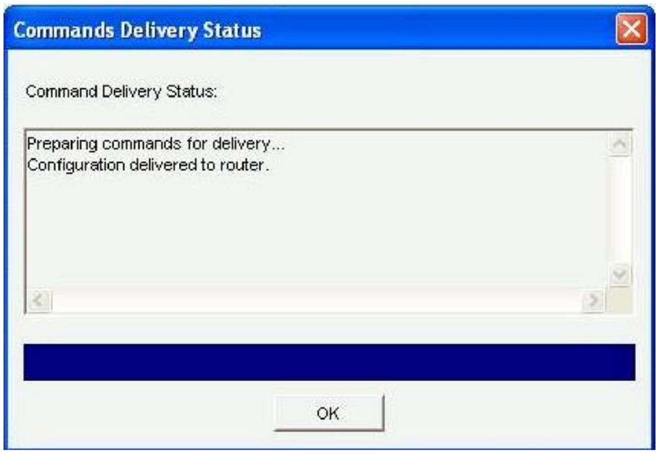
```
ip domain lookup
ip name-server 68.87.76.178
ip name-server 68.87.78.130
parameter-map type trend-global global-param-map
 server trps.trendmicro.com http-port 80 https-port 443 retrans 3 timeout 60
 exit
parameter-map type urlfpolicy trend cptrendparacatdeny0
 allow-mode on
 exit
parameter-map type urlfpolicy local cplocclassurlfgloburlblock0
parameter-map type urlfpolicy local cplocclassurlfgloburlallow0
```

The differences between the running configuration and the startup configuration are lost whenever the router is turned off.

☐ Save running config. to router's startup config.

This operation can take several minutes.

Step 28. You will get a **Command Delivery Status** screen displaying that the Configuration is delivered on to the router. Click **OK**.



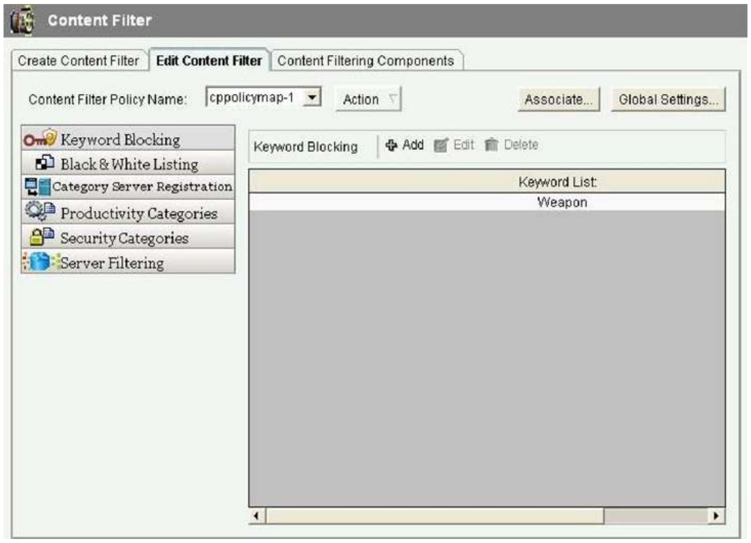
Commands Delivery Status

Command Delivery Status:

```
Preparing commands for delivery...
Configuration delivered to router.
```

Step 29. Congratulations!! You have finished the initial provisioning of Content Filtering using CCP 1.1. Now you can explore the other configuration changes that can be performed on Content Filtering using CCP. To edit any of the existing configurations, Click on **Edit Content Filter** tab.

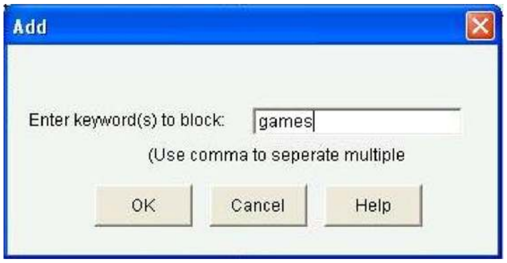
Step 30. To add, delete or modify the keywords, Click on **Keyword Blocking**.



Content Filter Policy Name: cppolicymap-1

Keyword List:
Weapon

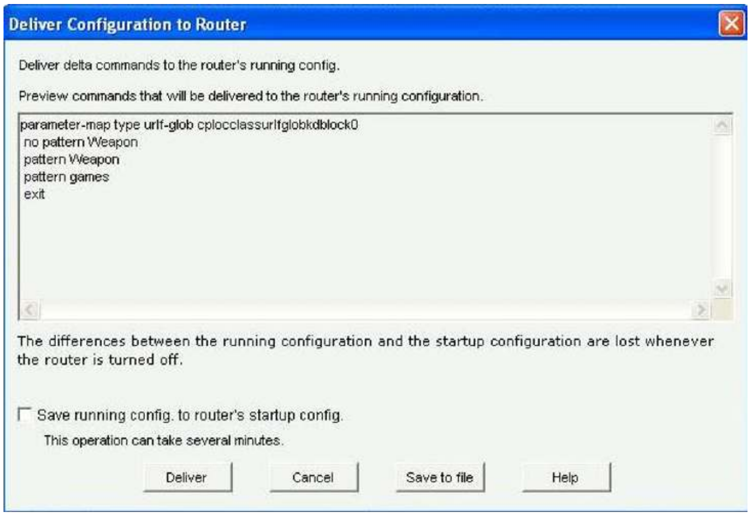
Step 31. To add a new keyword, Click **Add**. Enter the **keyword** you want to block. Click **OK**.



Enter keyword(s) to block: games

(Use comma to seperate multiple

Step 32. You will get a **Preview** of the commands to be delivered to the router. Click **Deliver** to deploy the changes onto the router.



Deliver delta commands to the router's running config.

Preview commands that will be delivered to the router's running configuration.

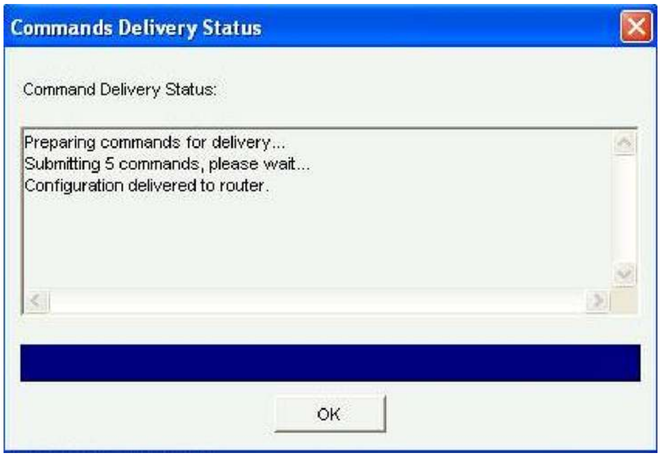
```
parameter-map type urlf-glob cplocclassurlfglobkdblock0
 no pattern Weapon
 pattern Weapon
 pattern games
 exit
```

The differences between the running configuration and the startup configuration are lost whenever the router is turned off.

☐ Save running config. to router's startup config.

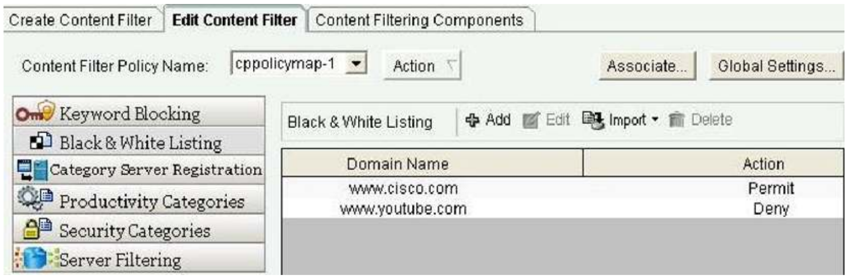
This operation can take several minutes.

Step 33. You will get a **Commands Delivery Status** screen displaying that the commands are delivered to the router. Click **OK**.



```
Preparing commands for delivery...
Submitting 5 commands, please wait...
Configuration delivered to router.
```

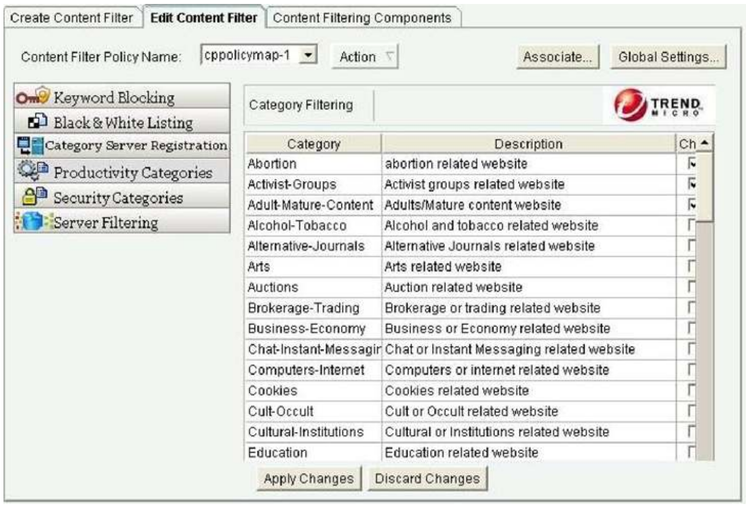
Step 34. Similarly you can make changes to the Black and White lists by clicking on **Black & White Listing**.



Content Filter Policy Name: cppolicymap-1

Domain Name	Action
www.cisco.com	Permit
www.youtube.com	Deny

Step 35. You can modify the productivity category selected by clicking on **Productivity Categories**. Choose all the categories you want to block and click on **Apply Changes** to deploy the changes onto the router.



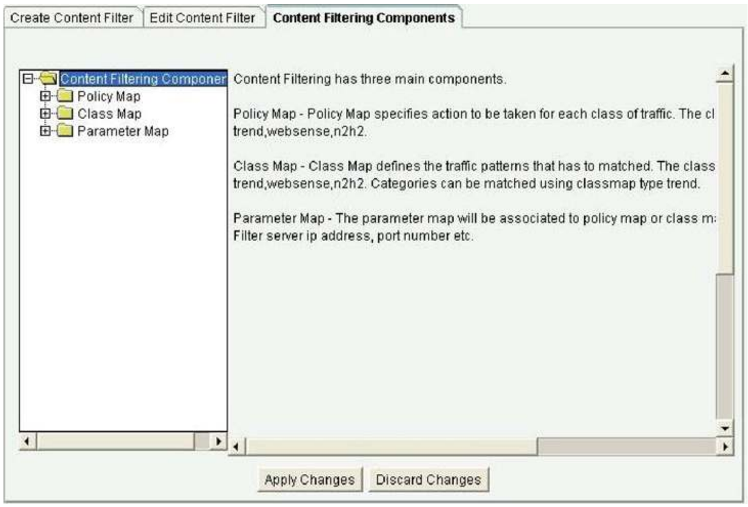
Content Filter Policy Name: cppolicymap-1

Category	Description	Ch
Abortion	abortion related website	☑
Activist-Groups	Activist groups related website	☑
Adult-Mature-Content	Adults/Mature content website	☑
Alcohol-Tobacco	Alcohol and tobacco related website	□
Alternative-Journals	Alternative Journals related website	□
Arts	Arts related website	□
Auctions	Auction related website	□
Brokerage-Trading	Brokerage or trading related website	□
Business-Economy	Business or Economy related website	□
Chat-Instant-Messagir	Chat or Instant Messaging related website	□
Computers-Internet	Computers or internet related website	□
Cookies	Cookies related website	□
Cult-Occult	Cult or Occult related website	□
Cultural-Institutions	Cultural or Institutions related website	□
Education	Education related website	□

Step 36. Similarly the Security Categories can be modified by clicking on Security Categories.

Step 37. To view and edit the Content Filtering components click on **Content Filtering Components**. Content Filtering has 3 main components Policy Map, Class Map and Parameter Map.

Step 38. Expand the **Content Filtering Components** to view the **Policy Map, Class Map and Parameter Map.** You can make changes to each of these components.



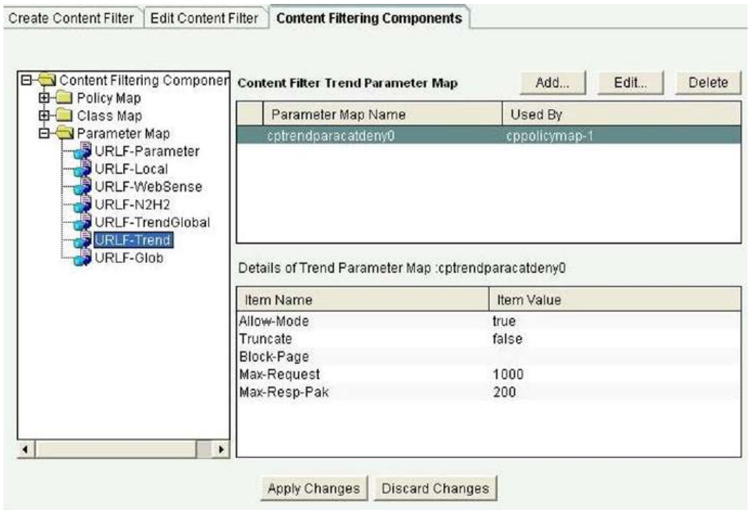
Content Filtering has three main components.

Policy Map - Policy Map specifies action to be taken for each class of traffic. The cl
trend,websense,n2h2.

Class Map - Class Map defines the traffic patterns that has to matched. The class
trend,websense,n2h2. Categories can be matched using classmap type trend.

Parameter Map - The parameter map will be associated to policy map or class m
Filter server ip address, port number etc.

Step 39. To edit the message that is displayed on the blocked page for TrendMicro based categories, expand Parameter Map and select **URLF-Trend**.



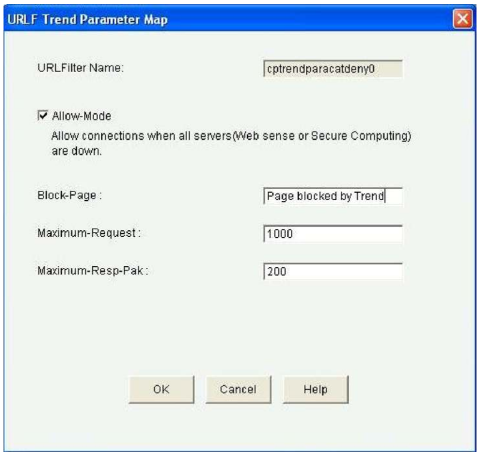
Content Filter Trend Parameter Map

Parameter Map Name	Used By
cptrendparacatdeny0	cppolicymap-1

Details of Trend Parameter Map :cptrendparacatdeny0

Item Name	Item Value
Allow-Mode	true
Truncate	false
Block-Page	
Max-Request	1000
Max-Resp-Pak	200

Step 40. Click on **Edit** and enter the message you want to be displayed on the blocked page. Click **OK**.



URLFilter Name: cptrendparacatdeny0

☑ Allow-Mode

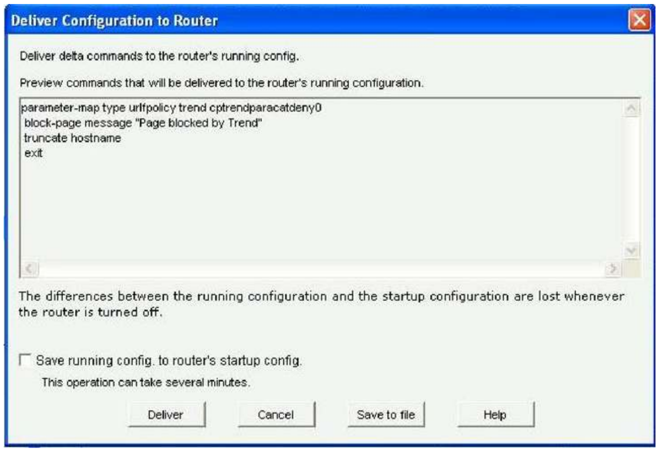
Allow connections when all servers(Web sense or Secure Computing) are down.

Block-Page : Page blocked by Trend

Maximum-Request : 1000

Maximum-Resp-Pak : 200

Step 41. Click **Deliver** to deploy the changes onto the router.



Deliver Configuration to Router

Deliver delta commands to the router's running config.

Preview commands that will be delivered to the router's running configuration.

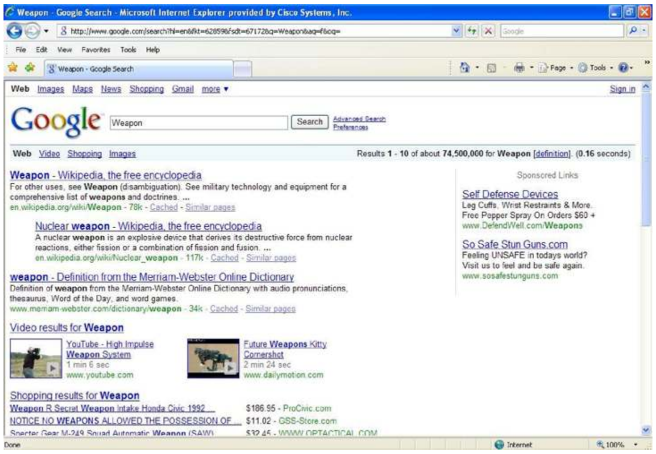
```
parameter-map type urlfpolicy trend cptrendparacatdeny0
 block-page message "Page blocked by Trend"
 truncate hostname
 exit
```

The differences between the running configuration and the startup configuration are lost whenever the router is turned off.

☐ Save running config. to router's startup config.
This operation can take several minutes.

Step 42. You will get the **Commands Delivery Status** screen. Click **OK.**

Step 43. Content Filtering is now enabled on the Router. From the web browser of the local PC connected to the router, search for the keyword you had chosen to block.



Weapon - Google Search - Microsoft Internet Explorer provided by Cisco Systems, Inc.

http://www.google.com/search?hl=en&rlz=...&q=Weapon&aq=f&oq=

Results **1** - **10** of about **74,500,000** for **Weapon** [definition]. (**0.16** seconds)

Weapon - Wikipedia, the free encyclopedia
For other uses, see **Weapon** (disambiguation). See military technology and equipment for a comprehensive list of **weapons** and doctrines. ...
en.wikipedia.org/wiki/**Weapon** - 78k - Cached - Similar pages

Nuclear **weapon** - Wikipedia, the free encyclopedia
A nuclear **weapon** is an explosive device that derives its destructive force from nuclear reactions, either fission or a combination of fission and fusion. ...
en.wikipedia.org/wiki/Nuclear_**weapon** - 117k - Cached - Similar pages

weapon - Definition from the Merriam-Webster Online Dictionary
Definition of **weapon** from the Merriam-Webster Online Dictionary with audio pronunciations, thesaurus, Word of the Day, and word games.
www.merriam-webster.com/dictionary/**weapon** - 34k - Cached - Similar pages

Video results for **Weapon**

YouTube - High Impulse **Weapon** System
1 min 6 sec
www.youtube.com

Future **Weapons** Kitty Cornershot
2 min 24 sec
www.dailymotion.com

Shopping results for **Weapon**

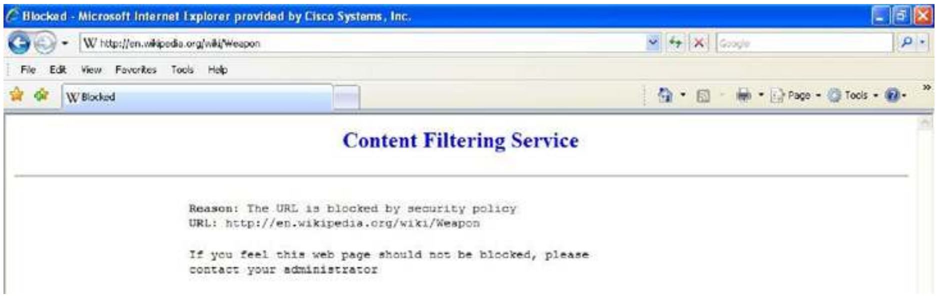
Weapon R Secret **Weapon** Intake Honda Civic 1992 ... $186.95 - ProCivic.com
NOTICE NO **WEAPONS** ALLOWED THE POSSESSION OF ... $11.02 - GSS-Store.com
Specter Gear M-249 Squad Automatic **Weapon** (SAW) $32.45 - WWW.OPTACTICAL.COM

Sponsored Links

Self Defense Devices
Leg Cuffs, Wrist Restraints & More. Free Pepper Spray On Orders $60 +
www.DefendWell.com/**Weapons**

So Safe Stun Guns.com
Feeling UNSAFE in todays world? Visit us to feel and be safe again.
www.sosafestunguns.com

Step 44. You should get a blocked page illustrating that the website is blocked due to a security policy.



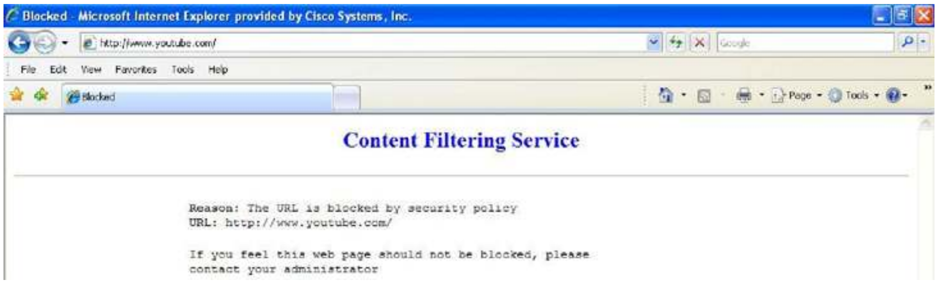
Blocked - Microsoft Internet Explorer provided by Cisco Systems, Inc.

http://en.wikipedia.org/wiki/Weapon

Content Filtering Service

```
Reason: The URL is blocked by security policy
URL: http://en.wikipedia.org/wiki/Weapon

If you feel this web page should not be blocked, please
contact your administrator
```

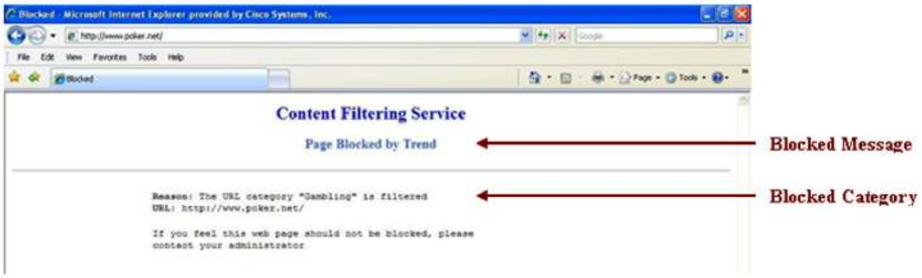
Step 45. From the browser search for one of the websites in your black list. You should get a blocked page.


Blocked - Microsoft Internet Explorer provided by Cisco Systems, Inc.
http://www.youtube.com/
Google
File Edit View Favorites Tools Help
Blocked
Page
Tools

Content Filtering Service

```
Reason: The URL is blocked by security policy
URL: http://www.youtube.com/

If you feel this web page should not be blocked, please
contact your administrator
```

Step 46. Browse for any of the websites you have chosen to block in the Productivity Category. For example, if you have chosen to block Gambling category. Try to browse for any of the websites which belong to Gambling Category. You should get a blocked page illustrating that the page is blocked as it belongs to the Gambling category. You should also see the blocked message added in the blocked page which we added in Task 39.

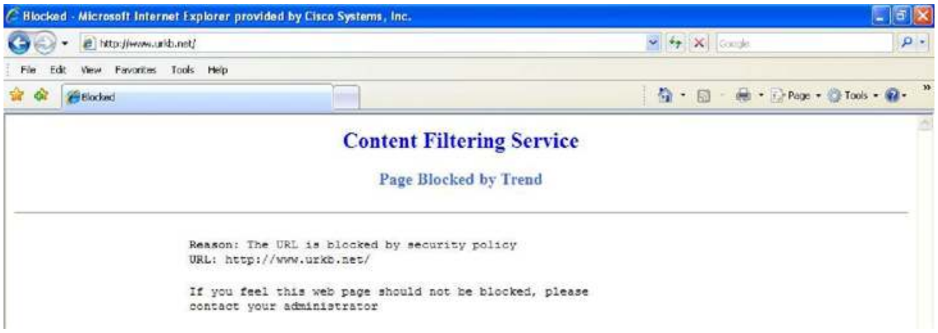

Blocked - Microsoft Internet Explorer provided by Cisco Systems, Inc.
http://www.poker.net/
Google
File Edit View Favorites Tools Help
Blocked
Page
Tools
Blocked Message
Blocked Category

Content Filtering Service

Page Blocked by Trend

```
Reason: The URL category "Gambling" is filtered
URL: http://www.poker.net/

If you feel this web page should not be blocked, please
contact your administrator
```

Step 47. Browse for any of the Phishing sites and you will see that access is blocked.


Blocked - Microsoft Internet Explorer provided by Cisco Systems, Inc.
http://www.urkb.net/
Google
File Edit View Favorites Tools Help
Blocked
Page
Tools

Content Filtering Service

Page Blocked by Trend

```
Reason: The URL is blocked by security policy
URL: http://www.urkb.net/

If you feel this web page should not be blocked, please
contact your administrator
```

References

- Cisco IOS Content Filtering at Cisco.com

  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 Configuration Professional at Cisco.com

  http://www.cisco.com/go/ccp

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

C89-492776-00 01/09