Content Filtering

Contents

Overview 7-2
- Risks Posed by Non-Work-Related Use of the Internet 7-2
- Web Content Filtering on the ProCurve Secure Router 7000dl Series 7-3
  - The Role of the Websense Enterprise Solution 7-3
  - The Role of the ProCurve Secure Router 7-4

Configuring Web Content Filtering 7-5
- Creating a Filter on the ProCurve Secure Router 7-5
- Specifying the Websense Server's IP Address 7-6
- Applying a Filter to a Router Interface 7-6
- Specifying Behavior When the Server Is Unreachable 7-8
- Defining Exclusive Domains—Domains the Router Automatically Allows or Blocks 7-8
- Specifying the Maximum Number of Outstanding Requests to the Websense Server 7-10
- Specifying the Maximum Number of Buffered Web Server Responses 7-10

Troubleshooting Web Content Filtering 7-11
- Troubleshooting Tools—show, debug, and clear Commands 7-11
- Troubleshooting Common Problems 7-14
  - Web Content Filtering Does Not Take Effect 7-14
  - Users Cannot Access the Web Sites They Need 7-17
  - The Router Cannot Connect to the Websense Server 7-18
  - Web Sites Do Not Load, Load Slowly, or Load Incompletely 7-20

Quick Start 7-21

Overview

For most companies, the Internet has become an invaluable work tool, providing new ways to do business and a high-level of contact with customers and suppliers. But with all its benefits, the Internet introduces costs. Almost everyone now realizes the risks posed by attacks launched through the Internet; however, not all costs associated with the Internet are as obvious as a virus, worm, or Denial of Service (DoS) attack. Some costs are introduced by the way your own employees, well-intentioned or otherwise, use the Internet. Web content filtering attempts to mitigate those risks by distinguishing traffic related to proper use of the Internet from traffic related to improper use—as determined by your company's policies.

Risks Posed by Non-Work-Related Use of the Internet

One obvious cost associated with Internet use is the decrease in productivity when employees take time from the work day to "surf" the Internet or make online purchases. Perhaps more serious than the lost time is the misuse of company assets for activities such as downloading and storing copyright-protected MP3 files or surfing pornography sites (sites, which if witnessed by other employees, present a potential hostile workplace situation). These non-work-related activities put businesses at risk for lawsuits resulting in potential large monetary settlements; more seriously, media coverage of such legal actions can seriously damage the company's reputation.

As employees download and store nonessential applications and data from the Internet, storage requirements on desktops and corporate servers escalate. Also, many users now routinely participate in bandwidth-intensive Internet activities, such as viewing streaming videos, downloading MP3 files, or playing Internet games. These activities can starve out business-related traffic on WAN and LAN links. Bandwidth consumption is of particular concern for WANs: personal Web surfing can congest connections that are already relatively slow.

Web Content Filtering on the ProCurve Secure Router 7000dl Series

Web content filtering is the best way to minimize the problems associated with misuse of the Internet at work. Web content filtering prevents undesirable Internet activity while allowing mission-critical traffic and applications.

Firewalls and access control lists (ACLs) are valuable security tools, but they are not designed to prevent legitimate users from accessing inappropriate content. For example, ACLs filter packets based on information in the IP header, which does not indicate whether a destination Web site is a legitimate research tool, an online retailer, a personal blog, or a pornography site.

Web content filtering solutions, on the other hand, look at information *inside* packets destined to the Internet—specifically, the URL of the Web site in question. The solution then determines whether the user sending the traffic is allowed to access that site, basing its decision on a database of URLs and a configurable set of policies.

Integrating with Websense® Enterprise, the ProCurve Secure Router 7000dl Series provides one piece of a Web content filtering solution. The ProCurve Secure Router collects requests for access to external Web sites and submits those requests to the Websense server, which makes the decision to allow or deny access to the site in question. The Websense server can be located on the same LAN as the ProCurve Secure Router or in another segment of the WAN (for example, at a central office), making this solution for companies with distributed offices.

The Role of the Websense Enterprise Solution

The ProCurve Secure Router's Web content filtering capabilities require your network to have a Websense Security Suite (version 6.1.1 or later) that includes Websense Enterprise. You actually create all filtering policies on the Websense server.

An enterprise-level content filtering solution such as Websense can draw on an extensive database of URLs that are classified according to content, making it easy for you to create comprehensive security policies. For example, you can configure the solution to prevent users from accessing gambling Web sites without personally tracking down every such Web site. Websense handles keeping the database up-to-date and accurate.

Your policies can be quite flexible, varying from user group to user group. You can also integrate the Websense policies with other security measures. For example, the Websense server can integrate with your authentication or directory service solution; the server automatically applies the correct filtering policies to a user who has logged in to the private network.

The Role of the ProCurve Secure Router

The Websense server needs to "see" traffic in order to control it. The ProCurve Secure Router, as the point of access to the Internet, collects HTTP traffic for the server and filters it according to the server's policy decisions.

For example, a user in the network attempts to navigate to an online auction Web site. His or her workstation sends a request to open a session with the external Web server. The router submits the request to the Websense server. The Websense server "reads" the request and matches the URL to an online retailer. Your company does not allow this employee to make purchases during work hours, so the server denies the request. The ProCurve Secure Router receives the server's decision and blocks the traffic.

The filtering exchange necessarily adds some latency. The ProCurve Secure Router minimizes delay by forwarding a copy of the workstation's request to the Web server at the same time that the router submits the request to the Websense server. While waiting for the Websense server's response, the router receives and buffers the traffic from the Web server, forwarding it on to the workstation only if the Websense server approves the user's request.

You can also configure the router to make some decisions on its own, automatically passing traffic destined to certain pre-approved domains and blocking traffic to known problem domains.

Note

Not all Internet traffic is HTTP traffic. Your Websense solution might filter non-HTTP traffic; however, the ProCurve Secure Router is responsible only for filtering HTTP traffic, which remains the bulk of Internet traffic.

Configuring Web Content Filtering

To configure Web content filtering on a ProCurve Secure Router 7000dl, you must complete these tasks:

- Install your Websense solution and configure filtering policies on the Websense server.
- On the ProCurve Secure Router:
  - Create a filter.
  - Specify the IP address of at least one Websense server to which the router should forward requests.
  - Apply the filter to one or more router interfaces.
  - Enable the firewall.

Optionally, you can customize these filtering settings:

- the router's behavior when the server is inaccessible (to block all Internet traffic or allow all Internet traffic)
- a list of domain names for which the router can allow or block traffic without querying the server
- the maximum number of outstanding requests to the Websense server
- the maximum number of buffered responses from Web servers

This guide instructs you how to configure web content filtering on the ProCurve Secure Router. For instructions on installing and configuring your Websense solution refer to *http://www.websense.com*.

Creating a Filter on the ProCurve Secure Router

To create a filter, enter this command from the ProCurve Secure Router's global configuration mode context:

Syntax: ip urlfilter <*name*> http

The ProCurve Secure Router filters HTTP traffic (traffic to port 80). If workstations send Web traffic to a non-standard port, the router will not filter it (although, depending on how you deploy Websense Network Agents, your Websense solution might).

You can create multiple named filters. Typically, however, you should create one filter, which you can apply to multiple interfaces. All filtering settings are created globally and apply to all filters.

Filtering settings include:

- Websense server IP address or addresses
- router's default behavior when the Websense server is unreachable
- list of domains about which the router can make its own decisions
- maximum number of outstanding requests to the Websense server
- number of buffered responses from Web servers on the Internet

Specifying the Websense Server's IP Address

You need to configure only one setting for the filter to function: the Websense server's IP address.

Enter this command from the global configuration mode context:

Syntax: ip urlfilter server <*A.B.C.D*>

Optionally, you can adjust these settings:

- port on which the server receives queries
- time before the router considers the server unreachable

To configure these optional settings, enter this command:

Syntax: ip urlfilter server <*A.B.C.D*> port <*value*> timeout <*seconds*>

The default port is 15868, which is the default port for the Websense server. The valid range is from 1 to 65,535. The default timeout is 5 seconds and can be set to between 1 and 300 seconds.

You can also specify multiple Websense servers. The router will query the server with the lowest IP address first. If the router cannot reach this server (that is, if the timeout value is exceeded), the router tries to contact the server with the next higher address. After establishing a connection with a server, the router maintains that relationship unless that server becomes unreachable.

Applying a Filter to a Router Interface

The ProCurve Secure Router does not begin filtering Web traffic until:

- you apply the filter to a router interface
- you enable the firewall

Filters control traffic on logical interfaces, which, on the ProCurve Secure Router, include:

- Ethernet interfaces
- Ethernet subinterfaces
- Point-to-Point Protocol (PPP) interfaces
- Frame Relay subinterfaces
- Asynchronous Transfer Mode (ATM) subinterfaces
- demand routing interfaces
- tunnel interfaces

You can apply the filter to inbound HTTP traffic that arrives on the interface or to outbound HTTP traffic that the interface transmits.

To filter all traffic from the private network, apply the filter to inbound traffic on the router's Ethernet interface or interfaces. You might choose this option if most traffic in your network is destined to the Internet.

If, on the other hand, your network also includes a WAN connection to a private network, you might want to filter only the traffic destined to the Internet. In this case, apply the filter to outbound traffic on the interface that connects to the Internet.

To apply the filter, complete the following steps:

1. Move to the interface configuration mode context.

   For example, enter:

   ProCurve(config)# interface ethernet 0/1

   Note that the interface must have an IP address before you can apply the filter.

2. Enter this command from the interface configuration mode context:

   Syntax: ip urlfilter <*name*> [in | out]

Be careful to enter the correct name (the case of the letters counts). A sign that you have entered the wrong name is this message:

```
Filter applied but not used until a port is defined and
IP firewall is enabled
```

The router applies the incorrectly named filter to the interface, but because this filter has not yet been configured, its port is not defined. Re-enter the command with the correct name.

Note

Remember to enable the firewall:

```
ProCurve(config)# ip firewall
```

For more information on the firewall, see *Chapter 4: ProCurve Secure Router OS Firewall—Protecting the Internal, Trusted Network*.

Specifying Behavior When the Server Is Unreachable

A failed network connection might prevent the ProCurve Secure Router from receiving instructions from the Websense server about how to filter HTTP traffic. You should consider this eventuality and decide which is more important to your company:

- that users do not access inappropriate content even at the cost of losing all (or most) connectivity to the Internet
- that users can access the Internet even if they might also access inappropriate content

If blocking inappropriate content is your company's priority, leave the router at its default configuration: Allow mode disabled. The router blocks all HTTP traffic (although you can use excluded domains, described in the next section, to set up some exceptions to this rule). If Internet access is your company's priority, enable Allow mode; when queries to the Websense server time out, the router allows all HTTP traffic.

Enter this command from the global configuration mode context to enable or disable Allow mode:

Syntax: [no] ip urlfilter allowmode

Defining Exclusive Domains—Domains the Router Automatically Allows or Blocks

Filtering Web traffic necessarily raises two potential concerns:

- Queries to the server consume bandwidth and time.
- The Websense server may become unavailable. As discussed above, this means either that users cannot reach the Internet at all, or that your filtering policies are no longer enforced.

To address these issues, you can create a list of frequently accessed domain names using the **ip urlfilter exclusive-domain** command. The router excludes Web sites with these names from the filtering policies set on the Websense server. Instead, you define whether the domain is permitted or

denied through the ProCurve Secure Router operating system (OS). The router then automatically passes traffic associated with the permitted domains and blocks traffic associated with the denied domains. (Note that you must still apply a filter to an interface in order for exclusive domains to take effect.)

Because the router allows or denies access to the exclusive domains without ever contacting the Websense server, the policy set by the **ip urlfilter exclusive-domain** command necessarily supersedes any policy set on the Websense server.

You might be tempted to use the **ip urlfilter exclusive-domain** command to override the way the Websense master database classifies a certain URL. Such a use is legitimate; however, it is often a better idea to use the Websense Manager for this function because the policy is then applied consistently throughout your network to the correct users and at the correct times. (To learn how to configure Custom URLs, download the "Websense Enterprise Administrator's Guide" from *http://www.websense.com/global/en/SupportAndKB/ProductDocumentation*.)

Instead of using the exclusive domain feature to override Websense decisions, you can use it to:

- speed processing for frequently accessed Web sites
- ensure that certain Web sites remain accessible even if the router loses contact with the Websense server and has *disabled* Allow mode
- ensure that certain Web sites remain blocked even if the router loses contact with the Websense server and has *enabled* Allow mode

All Web pages associated with the exclusive domain are permitted or denied as you specify in the command. However, some Web sites include sections that use different domain names; these will be unaffected by the command. Always be careful when setting up exclusive domains: you risk having policies that do not take effect as you anticipate. For example, many Web sites can be accessed through multiple domain names. You could deny one domain name only to have users access the site through another. On the other hand, you might attempt to permit a domain name, but users find that they cannot access portions of the Web Site because that domain name actually redirects clients to a different domain. Make sure to add both the domain names.

To specify a fully qualified domain name (FQDN) that users can *always* access, enter this command from the global configuration mode context:

Syntax: ip urlfilter exclusive-domain permit <*FQDN*>

For example, enter:

```
ProCurve(config)# ip urlfilter exclusive-domain permit www.procurve.com
```

To specify an FQDN that users can *never* access, enter this command from the global configuration mode context:

Syntax: ip urlfilter exclusive-domain deny <*FQDN*>

You can specify multiple domain names by entering multiple commands.

To view the exclusive domain names, as well as whether they are permitted or denied, enter this command:

```
ProCurve# show ip urlfilter exclusive-domain
```

Specifying the Maximum Number of Outstanding Requests to the Websense Server

In a busy network, the ProCurve Secure Router might receive many requests for sessions with Web servers. A request for which the Websense server has not yet returned a decision is called an outstanding request. When outstanding requests reach a certain level, the ProCurve Secure Router stops sending new requests to the Websense server.

Tailor the maximum number of outstanding requests according to the needs of your network with this global configuration mode command:

Syntax: ip urlfilter max-request <*value*>

You can specify a value between 1 and 500. By default, the router stops sending new requests when it has 500 outstanding requests to the Websense server. You might set this value lower if your network includes several devices sending queries to the Websense server to avoid overburdening that server. Setting the value too low, however, can add latency.

Specifying the Maximum Number of Buffered Web Server Responses

The ProCurve Secure Router begins forwarding requests to Internet Web servers as soon as it receives them from workstations in the private network—even before the router has received the Websense server's filtering decisions. However, the router does not pass the Web servers' responses back to the

workstations until it knows that access to them is allowed. While waiting for the Websense server's decisions, the router buffers the external Web servers' responses. At any one time, the ProCurve Secure Router can buffer up to 100 responses.

You can set the number of buffered responses using this global configuration mode command:

Syntax: ip urlfilter max-response <*value*>

Specify a value between 1 and 100. The default is 100.

Troubleshooting Web Content Filtering

Malfunctioning Web content filtering can have drastically different symptoms: users may continue browsing inappropriate materials, or users may lose access to the Internet entirely. Both problems are critical although the second is often the more immediate and noticeable.

You might also receive complaints about less extreme problems:

- When a user tries to navigate to a new Web site, the Web page does not load or loads very slowly.
- Users cannot access certain Web sites or portions of Web sites that they think that they should.

In this section, you will first learn about the **show** and **debug** commands that make up your troubleshooting tools. You will then learn about resolving the common problems discussed above.

Troubleshooting Tools—show, debug, and clear Commands

The ProCurve Secure Router OS provides several **show** commands related to Web content filtering. Table 7-1 displays the information returned when you enter each command.

Table 7-1. Web Content Filtering show Commands

Command Syntax	View
show ip urlfilter	Filtering configuration: • filter name or names • interface or interfaces to which each filter has been applied (including the traffic direction) • Websense servers' IP addresses, ports, and timeouts • permitted excluded domains • denied excluded domains • Allow mode on or off • maximum outstanding requests • maximum buffered responses
show ip urlfilter exclusive-domain	Domains to which the router does not apply Websense filtering policies: • permitted excluded domains • denied excluded domains
show ip urlfilter statistics	Filtering statistics: • current outstanding requests to the WebSense (filter) server • current responses buffered from Web servers • maximum outstanding requests to the WebSense server (the highest value at any one time) • maximum responses buffered from Web servers (the highest value at any one time) • total requests sent to the WebSense server • total responses received from the WebSense server • total number of requests allowed • total number of requests blocked • number of exclusive domains allowed • number of exclusive domains blocked • number of server bounces (a connected Websense server timed out) • time of the last server bounce

When troubleshooting, you often follow this standard practice:

1. Clear statistics.
2. Reproduce a problem.
3. View statistics.

To clear filtering statistics, enter this enable mode command:

```
ProCurve# clear ip urlfilter statistics
```

For more detailed troubleshooting, you can view all event messages related to Web content filtering. Enter this enable mode command:

```
ProCurve# debug ip urlfilter
```

The command line interface (CLI) then displays events such as:

- the ProCurve Secure Router connecting to a Websense server
- the router sending a request to check whether an HTTP request to a particular URL is allowed
- the router receiving responses from Web servers
- the router receiving a response from a Websense server and either allowing or blocking a URL
- a connection with a Websense server timing out
- the router applying an exclusive domain rule
- the router dropping traffic from a Web server because the maximum number of buffered responses has been reached

Table 7-2 shows some debug messages and the problems that they may indicate. The following section of this guide describes these problems in more detail.

Table 7-2. Web Content Filtering Debug Messages

Messages	Meaning	Possible Problems
• Could not connect to Websense Enterprise server A.B.C.D • Trying to connect to Websense Enterprise server A.B.C.D • Websense Enterprise server A.B.C.D refused connection	The router cannot connect to the Websense server.	• The link to the Websense server is down. • The server's IP address has been entered incorrectly. • The route to the server's network is incorrect. • The server is running a firewall. • The server has failed.
Reached maximum number of outstanding requests	The router cannot submit the request to access a Web site to the Websense server because the router is waiting for responses to previous requests.	• The ip urlfilter maximum-requests setting is too low. • The Websense server is overburdened.
Reached maximum number of buffered responses	The router is dropping responses from a Web server because its buffer is full.	• The ip urlfilter maximum-responses setting is too low. • The network is congested.
Allow mode set to allow all requests	The router cannot connect to the Websense server and will allow unlimited access to the Internet.	See Row 1.
Allow mode set to block all requests	The router cannot connect to the Websense server and will block all access to the Internet.	See Row 1.

Note Debug messages are processor-intensive and can seriously degrade network performance. Take care when using **debug** commands.

Troubleshooting Common Problems

This section will teach you how to look for and fix some common problems.

Web Content Filtering Does Not Take Effect

When your filtering policies do not seem to actually prevent users from reaching inappropriate Web sites, first determine the scope of the problem. Are any Web sites being prohibited or none at all?

No Filtering. If no Web sites at all are being prohibited, first verify that the firewall is enabled on the ProCurve Secure Router. The router cannot filter traffic unless the firewall is on.

Then, check these settings by entering **show ip urlfilter**:

- The filter is applied to the correct interface.
- The filter is applied to traffic in the correct direction (usually inbound on an Ethernet interface or outbound on a WAN interface).
- The Websense server's IP address is correct.
- The router has connected to a Websense server.

Figure 7-1 shows the output from the **show ip urlfilter** command.

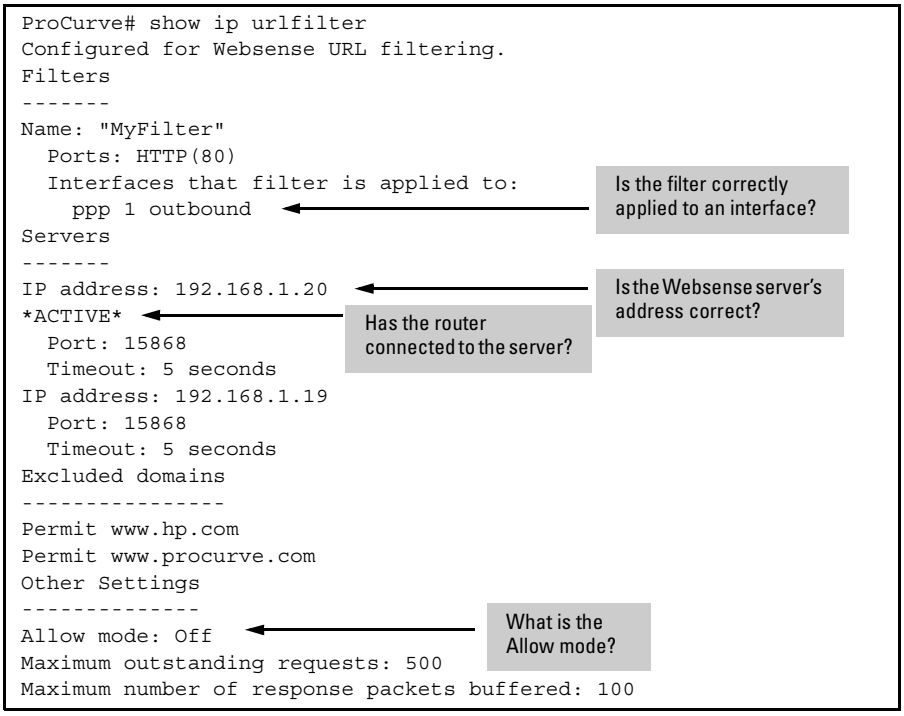

Figure 7-1. Viewing Web Content Filtering Settings

Fix any misconfigurations. For example, if you see that the filter has not been applied to any interfaces, move to the correct interface configuration mode context and apply the filter.

While viewing these settings, check the Allow mode. It is perfectly acceptable for Allow mode to be enabled. However, in this case, when the router cannot reach the Websense server, it will allow all traffic—a good description of your

current problem. If Allow mode is enabled, it may very well be that the router cannot contact the Websense server. See "The Router Cannot Connect to the Websense Server" on page 7-18 to diagnose and fix this problem.

Finally, it is possible that the filtering policy on the Websense server is misconfigured. By default, the Websense server does not prohibit any traffic. You must configure a filtering policy that blocks certain categories. Remember also to:

- add users, groups, workstations, or networks as monitored clients
- change the policy from monitoring only (the default) to active filtering

Detailed instructions for configuring policies and troubleshooting the Websense server are beyond the scope of this guide. For more instructions, use the Websense Manager's help tools or visit *http://www.websense.com/global/en/SupportAndKB/ProductDocumentation*.

Some, But Not All, Inappropriate Traffic Is Filtered. The most likely culprit for inconsistent filtering is a misconfigured Websense filtering policy. Again, refer to the Websense Manager's help and product documentation.

It is also possible that the router has lost contact with the Websense server and is applying its own policies, configured through the **ip urlfilter exclusive-domain** command. You can enter **show ip urlfilter exclusive-domain**, view permitted and denied URLs, and if necessary add to them. However, creating an entire filtering policy using exclusive domains is not feasible. The most important thing is to reestablish contact with the Websense server. (See "The Router Cannot Connect to the Websense Server" on page 7-18.)

An overburdened Websense server may filter traffic inconsistently. This is both because the router may drop requests until it receives responses to outstanding requests and because the router may time out the connection before the server has a chance to reply. Until the router can reconnect to the server, it will either allow or block all HTTP traffic (according to its Allow mode). You can attempt the following measures to deal with such a problem:

- increase the Websense server's timeout setting (**ip urlfilter server *<A.B.C.D>* timeout *<seconds>***)
- decrease the number of different policies that the Websense server enforces

Users Cannot Access the Web Sites They Need

Web content filtering should, of course, block some sites, but not all.

All Internet Access Is Blocked. No matter what site users try to visit, they see a screen telling them that they are prohibited from viewing that site. The most likely cause for such a problem is that the ProCurve Secure Router cannot connect to the Websense server and Allow mode is disabled.

Follow the tips given in "The Router Cannot Connect to the Websense Server" on page 7-18. If you need to grant users Internet access while you fix the problem, you can enable Allow mode. Alternatively, you can add limited access with this command:

```
ProCurve(config)# ip urlfilter exclusive-domain permit <FQDN>
```

Some Web Sites or Portions of Web Sites Are Blocked. Generally, when users complain about Web sites being blocked, your company might need to renegotiate policies, but the ProCurve Secure Router itself is behaving correctly. Prohibiting certain Web sites is the goal of content filtering, and prohibiting some portions of a Web site, but not others, is a perfectly ordinary and often desirable feature of Websense. While you should be prepared to adjust policies according to users' feedback, you do not need to reconfigure the router.

At times, however, users may be inappropriately blocked from certain sites. In this case, check for an exclusive domain set to **deny** instead of **permit** (**show ip urlfilter exclusive-domain**). You might also need to recheck the filtering policy set on the Websense server; perhaps an entire category of URLs is blocked when you meant to block only certain subcategories within that category.

A tip for determining whether the Websense policy or the router on its own is blocking access to the site: look at the screen that displays. If a *browser* screen informs you that you are not authorized to access the site, the router is blocking access. If the screen is a Websense screen, the Websense filtering policy is denying the site.

Unwanted behavior may only emerge when the Websense server is unreachable. Of course, without Allow mode, Internet access will always be severely limited in these circumstances, but incompletely configured exclusive domains can compound the problem.

For example, you have attempted to allow users to access the ProCurve Web site even if the router cannot reach the Websense server. You entered this command:

```
ProCurve(config)# ip urlfilter exclusive-domain permit www.procurve.com
```

One afternoon the Websense server fails; users try to access the ProCurve Web site, but they cannot open any pages within the site. The problem is that when users type *www.procurve.com* into their browsers, they are actually redirected to a site within this domain name: *www.hp.com*. The router allows the first name, but not the second. To fix this problem, you should allow both domain names.

You can anticipate such problems by checking exclusive domain names as you add them. View what domain name actually appears in your Web browser. If this name is different, add both names to the exclusive domains.

In most cases, you do not need to worry overly about configuring complicated exclusive domains. Remember that the problem described above would only occur in the relatively rare circumstance that the Websense server becomes unavailable.

The Router Cannot Connect to the Websense Server

Depending on whether Allow mode is enabled or not, the router's inability to connect to the Websense server can manifest as either giving users too much access or too little. You can determine whether the router and the Websense server are communicating at all by entering **show ip urlfilter statistics** and looking for requests sent and responses received. Figure 7-2 displays the output for this command.

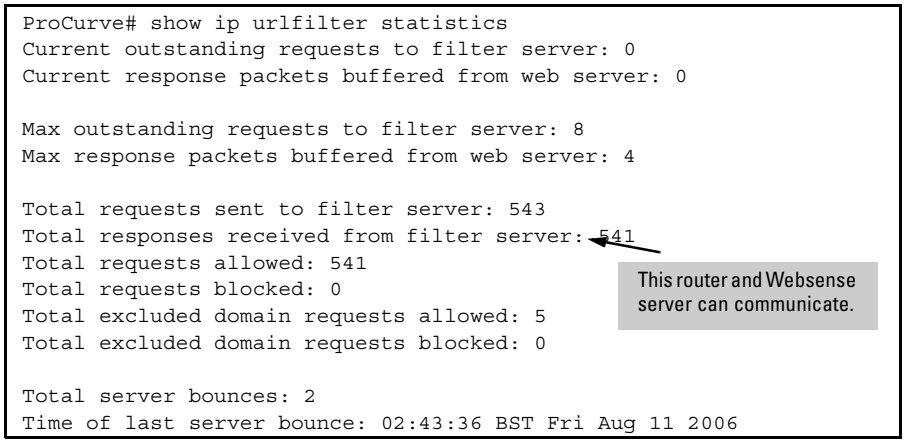

Figure 7-2. Viewing Web Content Filtering Statistics

When the router and server are not communicating, first attempt to ping the Websense server. If the ping fails, you have found the problem. Enter **traceroute <*A.B.C.D*>** to pinpoint the place at which the traffic is dropped; troubleshoot Physical and Data Link Layer connections or IP routing as necessary.

Simply being able to ping the server does not guarantee that the router can fully connect to the server and receive responses from it. If the router cannot connect to the Websense server, you will see messages such as the following when you enter **debug ip urlfilter**:

```
Trying to connect to Websense Enterprise server A.B.C.D
Websense Enterprise server A.B.C.D refused connection
All Websense Enterprise servers are down
```

Reasons that the router cannot connect to the Websense server include:

- The computer running the Websense server is using a firewall, and that firewall does not allow traffic from the router.

  Refer to the product's documentation for instructions on how to correctly deploy and install the Websense solution. (For example, often the server's computer should not use its own firewall at all.)

- The Websense server is listening for the router's requests on a different port.

  Enter this command to change the port to which the router sends the requests:

  ProCurve(config)# ip urlfilter server <A.B.C.D> port <1 to 65535>

No matter what you discover, remember to define the router's behavior while you fix the problem, enabling Allow mode if you want to grant users temporary, complete Internet access.

Web Sites Do Not Load, Load Slowly, or Load Incompletely

Filtering traffic adds a bit of latency while the router waits for the Websense server to issue policy decisions. Sometimes Web sites will load slowly. Sometimes a Web site may time out or load only partially. Tell users to refresh their browsers—a process that should fix the problem.

If this problem occurs frequently, the router might not be buffering enough responses from Web servers. Or, the router might be dropping HTTP requests because the maximum number of outstanding requests to the Websense server has been reached.

When you debug filtering, this message indicates that the maximum number of buffered responses may be too low:

```
Reached maximum number of buffered responses
```

This message indicates that the maximum number of outstanding requests may be too low:

```
Reached maximum number of outstanding requests
```

Check the thresholds with the **show ip urlfilter** command and, if necessary, raise them using these commands:

```
ProCurve(config)# ip urlfilter max-response <1 to 100>
ProCurve(config)# ip urlfilter max-request <1 to 500>
```

You might also check Websense servers' timeout settings. A very high setting would prevent the router from applying Allow mode in a timely manner should the Websense server fail. On the other hand, a setting that is too low can cause the router to time out the Websense server without adequate cause.

Finally, remember that latency increases:

- when the Websense server is located across a WAN connection
- when the Websense server must control many users

You might want to assign priority handling to traffic that is sent to and from the Websense server. (See *Chapter 8: Setting Up Quality of Service*). You should also evaluate the demands that your network places on the Websense solution and consider adding servers in more locations. (See the "Websense Enterprise Deployment Guide" available at *http://www.websense.com/global/en/SupportAndKB/ProductDocumentation*.)

Quick Start

This section provides the commands you must enter to quickly configure Web content filtering.

Only a minimal explanation is provided. If you need additional information about any of these options, see “Contents” on page 7-1 to locate the section and page number that contains the explanation you need.

Before performing these steps, you should have already deployed a Websense solution and configured all necessary filtering policies on that solution.

1. On the ProCurve Secure Router, move to the global configuration mode context and enable the firewall.

   Syntax: ip firewall

2. Create a named filter.

   Syntax: ip urlfilter <*name*> http

3. Specify your Websense server’s IP address. The default port for the server is 15868, and its timeout is 5 seconds. Optionally, you can change those settings.

   Syntax: ip urlfilter server <A.B.C.D> [port <1 to 65535>] [timeout <1 to 300 seconds>]

   You can enter the command multiple times if your WAN includes more than one Websense server.

4. Decide how you want the router to behave should the Websense server become unreachable. By default, the router drops all external HTTP traffic. To have the router allow all such traffic, enter this command:

   Syntax: ip urlfilter allowmode

5. For advanced configuration, complete this step. Otherwise, move directly to step 6.
   a. Add domain names that the router either permits or denies without contacting the Websense server:

      Syntax: ip urlfilter exclusive-domain <permit | deny> <*FQDN*>

   b. Specify the maximum number of outstanding requests the router allows to the Websense server (before dropping new requests):

      Syntax: ip urlfilter max-request <1 to 500>

   c. Specify the maximum number of Web server responses the router buffers:

      Syntax: ip urlfilter max-response <1 to 100>

6. Apply the filter to one or more logical interfaces. (The interface must have an IP address.)You can apply the filter to inbound traffic or to outbound traffic.

   Syntax: interface <*interface ID*>
   Syntax: ip address <*A.B.C.D*> <*subnet mask* | /*prefix length*>
   Syntax: ip urlfilter <*name*> [in | out]