Filtering by N2H2/Windows

INSTALLATION AND CONFIGURATION GUIDE

Copyright notice

Writers: Ailey Armstrong and Jessica Heinrich

Editor and proofreader: Jessica Heinrich

Filering by N2H2/Windows
© 2001 - 2004 Secure Computing Corporation. All rights reserved.
900 Fourth Avenue, Suite 3600
Seattle, WA 98164 U.S.A.

Filtering by N2H2 Installation and Configuration Guide
© 2001 - 2004 Secure Computing Corporation

Filtering by N2H2 Installation and Configuration Guide.0104.01

Contents

Chapter 1

Introducing Filtering by N2H2

What is Filtering by N2H2?

Filtering by N2H2 blocks inappropriate Web content, providing a safe, productive Internet environment for your organization.

Filtering by N2H2 gives users in your organization access to Internet resources while minimizing the legal, productivity, and bandwidth concerns that the Web often introduces.

Comprehensive, accurate Web content categorization

Filtering by N2H2 helps your organization harness the power of the Internet by giving you access to N2H2's comprehensive database of categorized Web sites, the largest database of URLs available. N2H2 adds thousands of new entries per day through a combination of techniques, including:

❖ Sophisticated artificial intelligence technology that harvests suspect URLs and analyzes their content.

❖ A team of expert human reviewers that analyzes Web site content and categorizes sites accordingly.

❖ Customer suggestions, which N2H2 evaluates and adds to its database as appropriate.

It's this unique blend of technology and human review that provides organizations with a superior filtering list.

Simple, secure, network-based administration

As a network-based filtering solution, Filtering by N2H2 operates at the server level on your Microsoft ISA Server, Microsoft Proxy Server, or other third-party network device (such as your firewall, proxy server, or cache server) to provide fast, secure Internet connectivity while simplifying filtering management.

Using Filtering by N2H2, you create filters based on predefined and custom categories of Web content, determining which categories are blocked, monitored, or allowed under each filter. (You can also create lists of specific sites, file types, and keywords to block or allow for all users in your organization.)

Then you apply the filters to your network by turning on global filtering and/or assigning filters to individual users, groups, and IP addresses. To provide more flexibility, you can give specific users the ability to bypass filtering for a set period of time.

By letting you apply filter settings to users on your network through a single administrative console, Filtering by N2H2 provides a Web filtering solution that is flexible and easy to maintain, and that gives you more precise control over how the Internet is used within your organization.

Filtering by N2H2 lets users on your network access useful Internet resources while preventing them from viewing inappropriate Web content.

Getting help

Use this guide, the Filtering by N2H2 Administrator's Guide, *and online help to learn more about Filtering by N2H2.*

Viewing the online guides

There are two online guides included with Filtering by N2H2:

- This *Filtering by N2H2 Installation and Configuration Guide* is geared toward system administrators and others responsible for installing Filtering by N2H2 and configuring it to run on a network. It includes step-by-step procedures and a troubleshooting section.
- The *Filtering by N2H2 Administrator's Guide* is geared toward filtering administrators and others responsible for implementing your organization's filtering policy. It includes overviews of product concepts and features, as well as step-by-step procedures.

Use Adobe Acrobat® to view the guides online or to print them. To view the Filtering by N2H2 guides, open the Program Files\N2H2Filtering folder, and then double-click n2h2ifp_sys.pdf (*Filtering by N2H2 Installation and Configuration Guide*) or n2h2ifp.pdf (*Filtering by N2H2 Administrator's Guide*).

✓ *For information on configuring your third-party network device (firewall, proxy server, or cache server) to work with Filtering by N2H2, go to the following site: www.n2h2.com/support/index.php. Click the link for your Filtering by N2H2 product, and then click the appropriate configuration guide.*

Looking at Filtering by N2H2 Help

Filtering by N2H2 Help provides instructions for using Filtering by N2H2. You can access help in several ways:

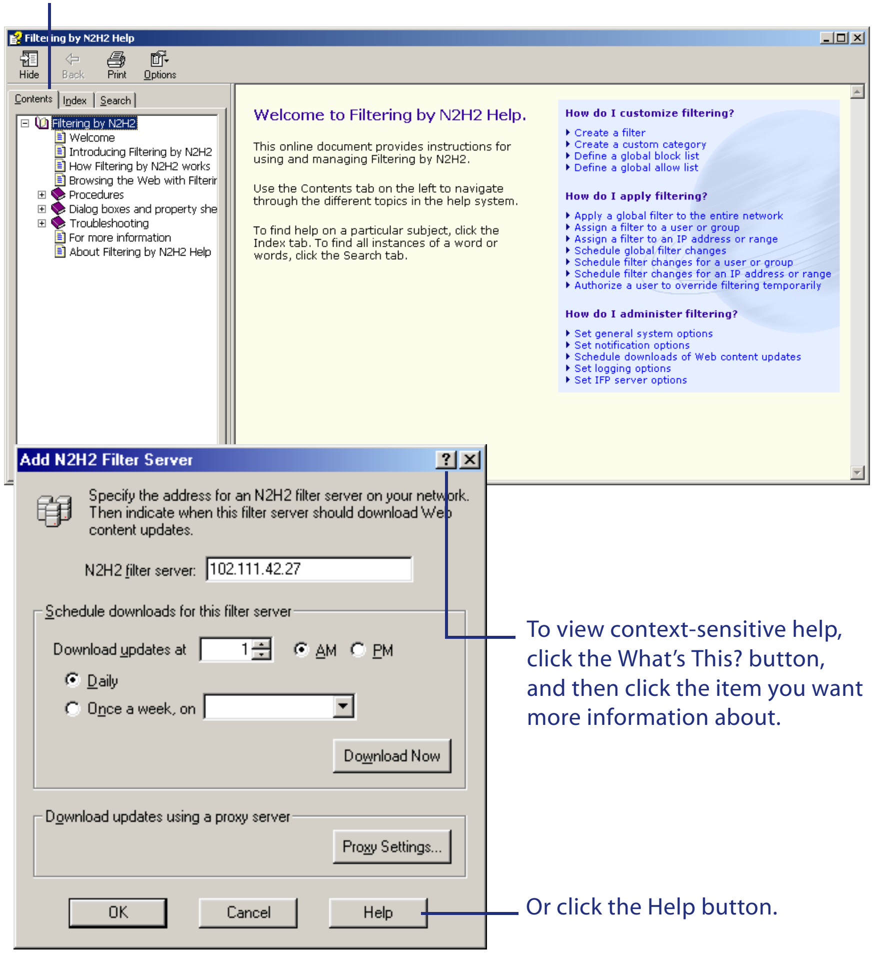
- **In the Filtering by N2H2 Manager.** Right-click Filtering by N2H2 in the left pane, and then click Help. Or click the Help button on the toolbar.
- **From a property sheet or dialog box.** To view context-sensitive help from within a dialog box or property sheet, click the Help button. Or click the What's This? button on the title bar.

Contacting technical support

Technical support for Filtering by N2H2 is available on the Web. You can access N2H2 support resources at the following Web address: www.n2h2.com/support/

If you're still unable to resolve a problem, call 800.246.1174 (in Seattle, call 206.336.1559).

Click an item on the Contents tab for overview information or help with a specific task. To locate information by keyword, use the Index or Search tabs.



Filtering by N2H2 Help
Hide
Back
Print
Options
Contents
Index
Search
Filtering by N2H2
Welcome
Introducing Filtering by N2H2
How Filtering by N2H2 works
Browsing the Web with Filterir
Procedures
Dialog boxes and property she
Troubleshooting
For more information
About Filtering by N2H2 Help

Welcome to Filtering by N2H2 Help.

This online document provides instructions for using and managing Filtering by N2H2.

Use the Contents tab on the left to navigate through the different topics in the help system.

To find help on a particular subject, click the Index tab. To find all instances of a word or words, click the Search tab.

How do I customize filtering?

- Create a filter
- Create a custom category
- Define a global block list
- Define a global allow list

How do I apply filtering?

- Apply a global filter to the entire network
- Assign a filter to a user or group
- Assign a filter to an IP address or range
- Schedule global filter changes
- Schedule filter changes for a user or group
- Schedule filter changes for an IP address or range
- Authorize a user to override filtering temporarily

How do I administer filtering?

- Set general system options
- Set notification options
- Schedule downloads of Web content updates
- Set logging options
- Set IFP server options

Add N2H2 Filter Server

Specify the address for an N2H2 filter server on your network. Then indicate when this filter server should download Web content updates.

N2H2 filter server: 102.111.42.27

Schedule downloads for this filter server

Download updates at 1 ● AM ○ PM

● Daily

○ Once a week, on

To view context-sensitive help, click the What's This? button, and then click the item you want more information about.

Or click the Help button.

Chapter 2

Installing Filtering by N2H2

How Filtering by N2H2 works

Filtering by N2H2 includes five main components: N2H2 administration, the N2H2 IFP server, the N2H2 filter server, the N2H2 authentication server, and the N2H2 log server.

Filtering by N2H2 operates at the server level to filter the Web content you choose. To implement Filtering by N2H2 on your network, you can install the following N2H2 components:

- **N2H2 administration** Provides the interface used to administer filtering.
- **N2H2 Internet Filtering Protocol (IFP) server** Stores the filter settings you assign to users, groups, and IP addresses, as well as your local block and allow lists. When the N2H2 IFP server receives an IFP request from your network device, it sends the request and the user's filter settings to the N2H2 filter server.
  - ✓ *The N2H2 Web server is installed with the N2H2 IFP server component. This server returns N2H2's HTML pages (such as the redirect page) to users' computers. In addition, if you're installing Filtering by N2H2 for Microsoft ISA Server or Filtering by N2H2 for Microsoft Proxy Server 2.0, a plug-in for these servers is automatically installed with the N2H2 IFP server component.*
- **N2H2 filter server** Downloads and stores site category information from the category database server located at N2H2. When the N2H2 filter server receives a request from the N2H2 IFP server, it checks the request against the stored category data to determine whether the request should be blocked or allowed.
  - ✓ *The N2H2 download service is installed with the N2H2 filter server component. This service downloads and processes the site information required for filtering.*
- **N2H2 authentication server (*optional*)** Facilitates transparent authentication of users on your network. This component only needs to be installed if you plan to implement transparent authentication on your Windows network.
- **N2H2 log server (*optional*)** Stores the Web activity data used for reporting.
  - ✓ *N2H2 Reporting is a subcomponent of the N2H2 log server. It lets you view, print, and export Web activity reports.*

You can install all of the N2H2 components on one computer, or install the components on individual computers.

How the components work together

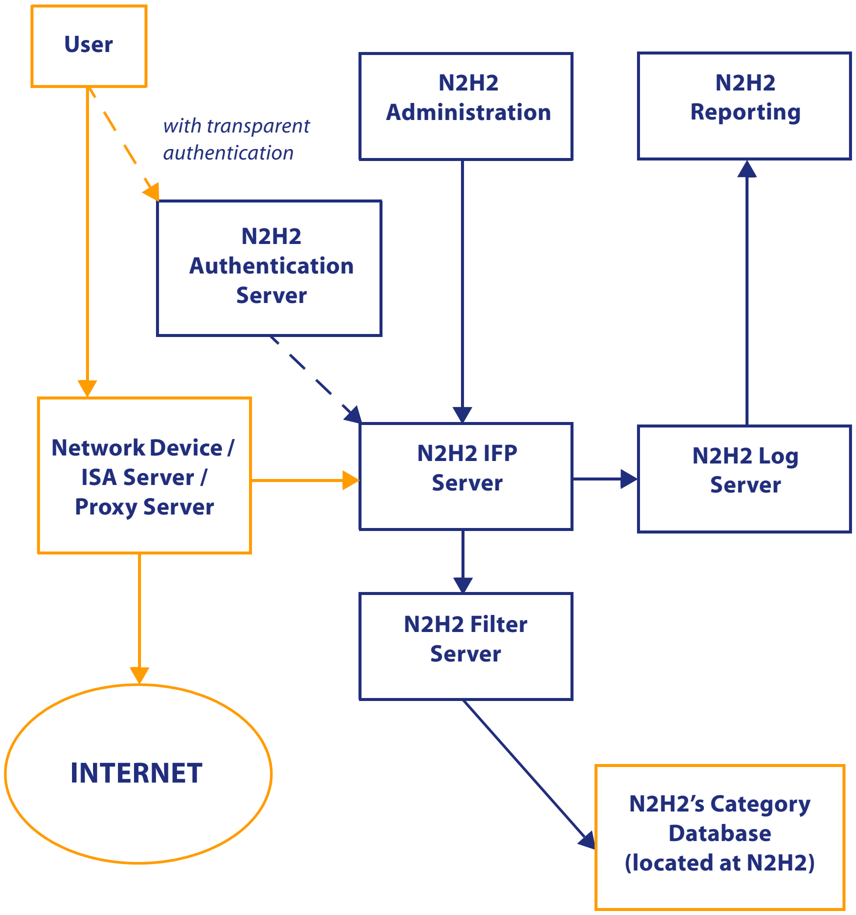
When a user requests a Web page, the request is sent to the N2H2 IFP server via your network device (or, if you're using transparent authentication, the N2H2 authentication server). The N2H2 IFP server combines the request with the filter settings specified for the user via the N2H2 administration component and sends this information to the N2H2 filter server. The N2H2 filter server then checks this information against its stored list of categorized Web sites.

How Filtering by N2H2 works

Filtering by N2H2 consists of N2H2 administration, the N2H2 IFP server, the N2H2 filter server, the N2H2 authentication server, and the N2H2 log server.

The N2H2 filter server regularly downloads Web content information from N2H2's category database, which is located at N2H2.

Note that the N2H2 authentication server is only necessary if you've implemented transparent authentication on your network.


User
with transparent authentication
N2H2 Administration
N2H2 Reporting
N2H2 Authentication Server
Network Device / ISA Server / Proxy Server
N2H2 IFP Server
N2H2 Log Server
N2H2 Filter Server
INTERNET
N2H2's Category Database (located at N2H2)

If the requested page is blocked under the user's filter settings, your network device denies the request. If the requested page is allowed under the user's filter settings, your network device displays the page in the user's browser.

Filtering by N2H2 requirements

Before you install Filtering by N2H2, make sure you have the necessary hardware, software, and server configuration.

Prior to installation, make sure that you have the hardware and software required to run Filtering by N2H2 on your network.

Installation requirements

Filtering by N2H2 includes five components: N2H2 administration, the N2H2 IFP server, the N2H2 filter server, the N2H2 authentication server, and the N2H2 log server (includes N2H2 Reporting). Each component has specific installation requirements.

✓ *In a low-volume network environment, you can install more than one component on a computer, as long as the computer meets the installation requirements for all components installed.*

The installation requirements for installing all components on a single computer are:

- 750 MHz processor (1 GHz or higher recommended)
- Microsoft Windows 2000 Server or Windows 2003 Server
- Microsoft Internet Information Services (IIS) installed prior to Microsoft .NET Framework and listening on port 80
- 512 MB RAM (1 GB recommended)
- 6 GB disk space free
- Network connection with Internet access
- Microsoft .NET Framework 1.1
- Microsoft SQL Server 2000 or Microsoft SQL Server 2000 Desktop Engine (MSDE 2000) *(can be installed on a separate computer)*

The requirements for installing components on separate computers are:

N2H2 administration

- Microsoft Windows 2000, Windows XP Professional, or Windows 2003 Server
- 5 MB disk space free

N2H2 IFP server

- Microsoft Windows 2000 Server or Windows 2003 Server
- 10 MB disk space free

✓ *If you're installing Filtering by N2H2 for Microsoft ISA Server or Filtering by N2H2 for Microsoft Proxy Server 2.0, be sure to install the N2H2 IFP server on your Microsoft ISA Server or Microsoft Proxy Server.*

N2H2 filter server

- 500 MHz processor (750 MHz or higher recommended)
- Microsoft Windows 2000, Windows XP Professional, or Windows 2003 Server
- 256 MB RAM (512 MB or higher recommended)
- 1.5 GB disk space free
- Network connection with Internet access (or connection to a proxy server with Internet access)

N2H2 authentication server

- Microsoft Windows 2000 Server or Windows 2003 Server
- Microsoft Internet Information Services (IIS) installed and listening on port 80
- Must be installed on same domain as network to be authenticated

N2H2 log server (includes N2H2 Reporting)

- 500 MHz processor (750 MHz or higher recommended)
- Microsoft Windows 2000 Server or Windows 2003 Server
- Microsoft Internet Information Services (IIS) installed prior to Microsoft .NET Framework and listening on port 80
- 256 MB RAM (512 MB or higher recommended)
- 4 GB disk space free
- Network connection to the N2H2 IFP server
- Microsoft .NET Framework 1.1
- Microsoft SQL Server 2000 or Microsoft SQL Server 2000 Desktop Engine (MSDE 2000) *(can be installed on a separate computer)*

Enabling filtering on your network

To assign filters to individual users and groups, you must configure your network service to authenticate access for users and groups defined on your network.

It's also recommended that you install Microsoft Internet Explorer 5.0 or later on all client workstations.

✓ *If you're installing Filtering by N2H2 for Microsoft ISA Server, set up your Microsoft ISA Server to allow HTTP and DNS traffic before using Filtering by N2H2. You can do this within ISA Server Management by creating and enabling HTTP Filter and DNS Filter. To filter Web content for specific users and groups on your network, create a global rule for the computer array that prompts unauthenticated users for identification. For more information on ISA Server Management, see Microsoft ISA Server Help.*

Installing Filtering by N2H2

Download Filtering by N2H2 and install its components.

To install Filtering by N2H2, download it from the N2H2 download Web site, and then run Setup.

Downloading and installing Filtering by N2H2

When you sign up for Filtering by N2H2, you select a personal identification number (PIN). N2H2 also provides an account ID and password for your organization. Use this information to download Filtering by N2H2.

Once you've downloaded Filtering by N2H2, you can install each of the N2H2 components. In a low-volume network environment, you can install two or more components on a single computer; in an environment with higher network volumes, it's better to install each component on a separate computer.

✓ *When installing components on separate computers, it's best to install them in the following order: N2H2 filter server, N2H2 log server, N2H2 IFP server, N2H2 administration, and N2H2 authentication server.*

To install Filtering by N2H2

1 Access the N2H2 download Web site.

2 Choose whether to run the installation program from its current location or save it to disk, and then click OK.

- ❖ If you chose to run the program from its current location, Filtering by N2H2 Setup opens.
- ❖ If you chose to save the program to disk, specify where you want to save the program. After the program file is saved, open the file from this location.

3 Follow the prompts in Setup.

Installing an N2H2 filter server

When you install an N2H2 filter server, you must enter your organization's account ID, password, and PIN. N2H2 uses this information to register the N2H2 filter server immediately after installation.

Note that Setup installs the N2H2 download service on the same computer as the N2H2 filter server. Once N2H2 registers the filter server, the N2H2 download service downloads and processes the Web content information required for filtering.

✓ *Initial download processing may take up to an hour to complete, depending on the speed of your connection. Subsequent downloads take less time. Filtering is unavailable on this filter server until download processing is finished.*

Installing N2H2 Reporting

Before installing N2H2 Reporting (a subcomponent of the N2H2 log server), you must install a reporting database: either Microsoft SQL Server 2000 or Microsoft SQL Server 2000 Desktop Engine (MSDE 2000). You can download MSDE 2000 from N2H2. (Microsoft SQL Server 2000 is available for purchase from Microsoft.)

To download MSDE 2000 from N2H2, go to http://download.n2h2.com/msde/n2h2msde2ksp3a.exe and download the program file. Unpack the program file, open a command prompt, and cd to the folder where MSDE was unpacked. MSDE 2000 Service Pack 3 requires a strong password account before it can be installed (see sp3readme.html in the MSDE folder for details). To create the strong password and start installation, type **setup.exe sapwd=*password***, where ***password*** is a combination of uppercase letters, lowercase letters, numbers, and symbols. After installation is complete, restart the computer. Then check the system tray to ensure that MSDE 2000 is running.

During installation, you're prompted for the location of the database. If the database computer has multiple DNS suffixes, enter the IP address or fully qualified domain name (FQDN) of the database computer (rather than just the host name).

Importing and exporting Filtering by N2H2 settings

After you install Filtering by N2H2 and specify filter settings, you can export these settings to a file. Then, if you need to re-install Filtering by N2H2 later, you can import this file to restore previous settings.

To export settings, open Filtering by N2H2. Right-click Filtering by N2H2 in the tree pane on the left, and then click Export Settings. Specify a name and location for the settings file, and then click Save.

To import settings, open Filtering by N2H2. Right-click Filtering by N2H2 in the tree pane on the left, and then click Import Settings. Locate the settings file, and then click Open.

Chapter 3

Setting system options

Overview of setting system options

Access Filtering by N2H2 settings and set general system options.

After you install Filtering by N2H2, you can access Filtering by N2H2 settings and modify system options.

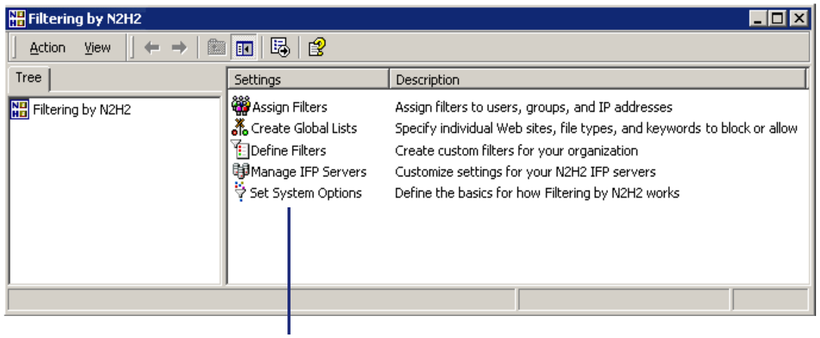
- Turn filtering on and off as necessary. For more information, see “Setting basic system options” on page 13.
- Choose whether to allow full Web access or no Web access if filtering is unavailable. For more information, see “Setting basic system options” on page 13.
- Specify a custom redirect page (also called a *block page*) that displays when users try to access blocked content. For more information, see “Setting basic system options” on page 13.
- Turn on Virtual Inspector™ and Virtual Reviewer.™ For more information, see “Setting basic system options” on page 13.
- Specify an e-mail address to receive site review requests, monitor with warning notifications, and override notifications. You can also choose under what circumstances monitor with warning notifications are sent to you. For more information, see “Setting notification options” on page 14.
- Change the settings for three N2H2 server components: the N2H2 filter server, N2H2 log server, and N2H2 Web server. For more information, see “Specifying N2H2 server settings” on page 15.
- Schedule the N2H2 filter server(s) on your network to download the latest Web information from N2H2. For more information, see “Getting updated Web information” on page 16.
- Specify advanced settings, such as turning off multiple warnings for a certain period of time after a user bypasses a warning page. For more information, see “Setting advanced options” on page 17.

Accessing Filtering by N2H2 settings

You can access Filtering by N2H2 settings through the Windows Start menu. In addition, because Filtering by N2H2 is distributed as a Microsoft Management Console (MMC) snap-in, you can combine it with other management tools to create a custom administrative console.

To access Filtering by N2H2 settings through the Start menu

1 On the Windows Start menu, point to Programs, and then point to the Filtering by N2H2 program group.



Settings	Description
Assign Filters	Assign filters to users, groups, and IP addresses
Create Global Lists	Specify individual Web sites, file types, and keywords to block or allow
Define Filters	Create custom filters for your organization
Manage IFP Servers	Customize settings for your N2H2 IFP servers
Set System Options	Define the basics for how Filtering by N2H2 works

Open Filtering by N2H2, and then double-click Set System Options.

2 Click Filtering by N2H2.

3 In the list pane, double-click the settings you want to view or modify.

Setting basic system options

Choose whether users can access the Web if filtering is unavailable. You can also specify your own redirect page.

Once you've opened Filtering by N2H2, you can set general system options.

To specify Filtering by N2H2 settings

1 Open Filtering by N2H2 and double-click Set System Options.

2 On the General tab, click On to turn on Filtering by N2H2.

Filtering by N2H2 is turned on by default. To turn off filtering, click Off.

3 Choose to block all Web access or allow unfiltered Web access if Filtering by N2H2 is unavailable.

This "safety net" feature lets you indicate what type of Web access is available to users on your network if filtering is temporarily unavailable. If you've chosen to block or allow specific sites under Create Global Lists, these sites are always blocked or allowed, regardless of whether filtering is available. (Users with override privileges can always access the Web, even if all Web access is blocked for other users.)

4 To specify a URL for a custom redirect page (also called the *block page*), in the Location of Redirect Page box, type the URL for the redirect page to display when users try to access inappropriate content.

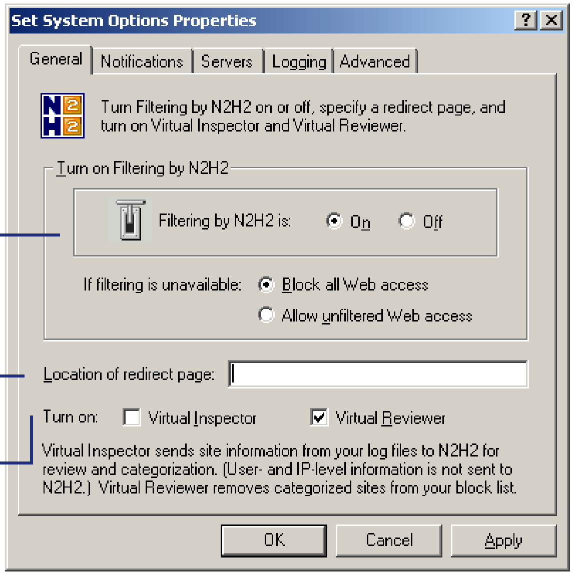
✓ *Leave the box empty to use the default redirect pages provided by N2H2. If you specify a URL for a custom redirect page, it must point to a page located on a Web server. For information on using CGI parameters to enhance a custom redirect page, see "Modifying the default redirect page" on page 28.*

5 To maximize Filtering by N2H2's effectiveness for your organization, turn on Virtual Inspector™ and Virtual Reviewer.™

- ❖ Virtual Inspector. Analyzes the data in your log files and forwards URLs that meet certain criteria to N2H2 for review and categorization. This lets you tailor N2H2's database to your organization's Web activity patterns.
- ❖ Virtual Reviewer. Reviews your global block list each night, removing URLs that have been categorized by N2H2. (You'll receive an e-mail notification each time a URL is removed.) This helps you keep your global block list as compact and efficient as possible.

✓ *For more information on Virtual Inspector and Virtual Reviewer, see "Using Virtual Inspector™ and Virtual Reviewer™" on page 30. For more information on the global block list, see the* Filtering by N2H2 Administrator's Guide.

6 Click OK.



Turn Filtering by N2H2 on or off, specify a redirect page, and turn on Virtual Inspector and Virtual Reviewer.

Turn on Filtering by N2H2

Filtering by N2H2 is: ● On ○ Off

If filtering is unavailable: ● Block all Web access ○ Allow unfiltered Web access

Location of redirect page:

Turn on: □ Virtual Inspector ☑ Virtual Reviewer

Virtual Inspector sends site information from your log files to N2H2 for review and categorization. (User- and IP-level information is not sent to N2H2.) Virtual Reviewer removes categorized sites from your block list.

Turn Filtering by N2H2 on and off as necessary and choose to block or allow Web access if filtering is unavailable.

Specify a custom redirect page if you don't want to use the default redirect page.

You can also turn on Virtual Inspector and Virtual Reviewer.

Tips on using Virtual Reviewer

- ❖ To prevent Filtering by N2H2 from removing an item from the block list, type **[lock]** before the item. For example, if you type **[lock] www.sports.com**, www.sports.com cannot be automatically deleted from your block list.
- ❖ Virtual Reviewer doesn't review or remove URLs that contain a wildcard (such as an asterisk) within the host name or path (for example, *.site.com). However, it may remove URLs that have a wildcard character at the end of the path (for example, www.site.com*).

✓ *It's recommended that you replace wildcard entries with the specific sites and domains you want to block. Minimizing wildcard usage in the block list also improves filtering performance.*

For more information on creating a global block list, see the *Filtering by N2H2 Administrator's Guide.*

Setting notification options

To receive notifications about Web activity on your network, enter your e-mail address.

You can specify preferences for receiving notifications about Web activity and Filtering by N2H2 system events on your network.

To set notification options

1 Open Filtering by N2H2 and double-click Set System Options.

2 Click the Notifications tab.

3 In the Administrator's E-mail Address box, type the e-mail address where site review requests, monitor with warning notifications, override notifications, and Virtual Reviewer™ notifications should be sent.

4 In the SMTP Server box, type the network address or IP address of the mail server.

5 Under Monitor with Warning Notifications, choose an option for receiving e-mail notifications when users bypass the warning page and access sites in categories you've chosen to "Monitor with Warning."

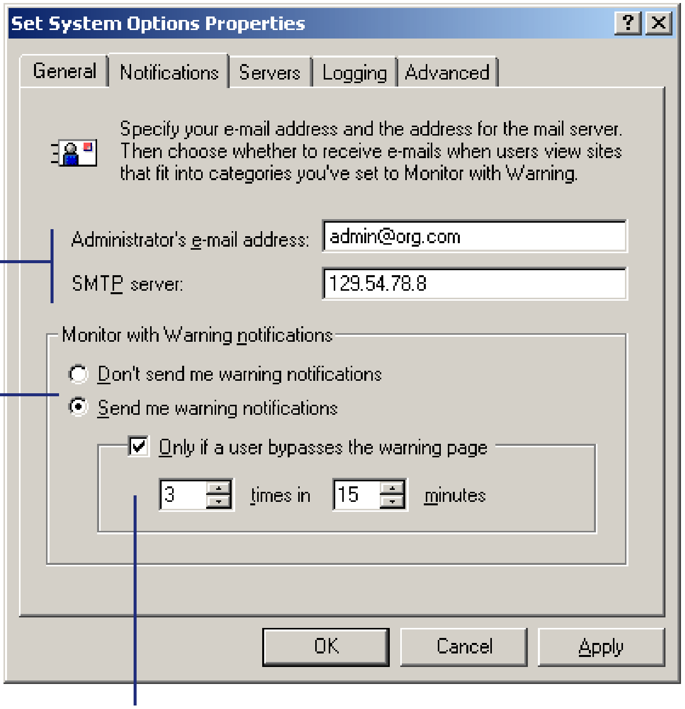
- ❖ Click Don't Send Me Warning Notifications if you don't want to receive e-mail notifications when users choose to bypass the warning page.
- ❖ Click Send Me Warning Notifications if you want to receive e-mail notifications when users choose to bypass the warning page.

6 If you chose to receive warning notifications, check Only If a User Bypasses the Warning Page to receive notifications only after a user bypasses the warning page a specific number of times within a certain period.

7 Type a number or click an arrow to specify the number of times that a user must bypass the warning page within a certain period in order to trigger the e-mail notification. Then type a number or click an arrow to specify the number of minutes in that period.

8 Click OK.

✓ *The SMTP client used by the N2H2 IFP server does not support authentication or encryption. Therefore, be sure your SMTP server does not require the machine you installed the IFP server on to authenticate or encrypt the SMTP session.*



Specify your e-mail address and the address for the mail server. Then choose whether to receive e-mails when users view sites that fit into categories you've set to Monitor with Warning.

Administrator's e-mail address: admin@org.com

SMTP server: 129.54.78.8

Monitor with Warning notifications

○ Don't send me warning notifications

● Send me warning notifications

☑ Only if a user bypasses the warning page

3 times in 15 minutes

To receive e-mail notifications, type your e-mail address and the address of the SMTP server.

Then choose whether to receive notifications when users bypass the warning page.

If you chose to receive warning notifications, specify under what circumstances the notifications are sent to you.

Specifying N2H2 server settings

Specify settings for your Filtering by N2H2 servers.

Specify settings for the N2H2 filter server (or servers), N2H2 Web server, and N2H2 log server installed on your network. To modify N2H2 IFP server settings, see chapter 4, "Managing N2H2 IFP servers."

Specifying N2H2 filter server settings

N2H2 filter servers download and store Web content information, as well as check user site requests.

✓ *You can install multiple N2H2 filter servers. When installed in an array (or cluster), multiple N2H2 filter servers ensure that Web filtering remains available when a server is down or processing an update; they also share the server load to improve network performance during heavy traffic periods.*

To add or change settings for an N2H2 filter server

1 Open Filtering by N2H2 and double-click Set System Options.

2 On the Servers tab, click Add to add a new N2H2 filter server. Or click Change to change settings for an existing N2H2 filter server.

3 In the N2H2 Filter Server box, type the address of the filter server.

The address can be the server's IP address, host name, or fully qualified domain name (FQDN). Be sure to specify a routable address, not a relative address (such as *localhost*).

4 Schedule this filter server to download Web content updates.

✓ *For more information on scheduling downloads, see "Getting updated Web information" on page 16.*

5 If this N2H2 filter server accesses the Internet through a proxy server, click Proxy Settings and specify the address and port of the proxy server.

✓ *This is only necessary if the filter server doesn't access the Internet directly.*

6 Click OK, and then click OK again.

To remove an N2H2 filter server

1 Open Filtering by N2H2 and double-click Set System Options.

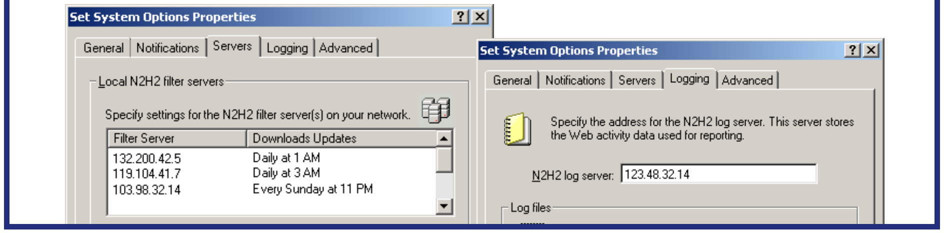
2 On the Servers tab, click the server you want to delete, and then click Remove.

3 Confirm that you want to remove the filter server, and then click OK.

Specifying N2H2 Web server settings

The N2H2 Web server returns N2H2's HTML pages (such as the redirect page) to users' computers.

To configure the N2H2 servers on your network, use the Servers and Logging tabs.



Specify settings for the N2H2 filter server(s) on your network.

Filter Server	Downloads Updates
132.200.42.5	Daily at 1 AM
119.104.41.7	Daily at 3 AM
103.98.32.14	Every Sunday at 11 PM

Specify the address for the N2H2 log server. This server stores the Web activity data used for reporting.

N2H2 log server: 123.48.32.14

To specify settings for the N2H2 Web server

1 Open Filtering by N2H2 and double-click Set System Options.

2 Click the Servers tab.

3 In the N2H2 Web Server Port box, type the number of the port you want the N2H2 Web server to use.

4 In the Domain Name box, type the domain of the network that your N2H2 Web server resides on.

✓ *It is only necessary to specify a domain if requesting clients are on a different network than the N2H2 Web server or cannot resolve the N2H2 Web server name.*

5 Click OK.

Specifying N2H2 log server settings

Specify the address for your N2H2 log server. This server stores the Web activity data used for reporting.

To set logging options

1 Open Filtering by N2H2 and double-click Set System Options.

2 Click the Logging tab.

3 In the N2H2 Log Server box, type the address of the server where Web activity data for your network should be stored.

The address can be the server's IP address, host name, or fully qualified domain name (FQDN). Be sure to specify a routable address, not a relative address (such as *localhost*).

4 Choose how many days to keep log files.

- Click Remove Log Files After [X] Days to delete log files after a certain period of time, and then specify the number of days to keep log files.
- Click Don't Remove Log Files to keep log files indefinitely.

5 Click OK.

Getting updated Web information

Configure Filtering by N2H2 to download the latest Web content updates to your N2H2 filter server(s) when you specify.

To provide the most up-to-date categorization of content on the Web, Filtering by N2H2 regularly downloads Web content updates from N2H2 to the N2H2 filter server (or servers) on your network. You choose when each N2H2 filter server downloads these updates.

Scheduling Web information downloads

For each N2H2 filter server on your network, choose when and how often to download Web content updates from N2H2.

For about three minutes during update processing, an N2H2 filter server cannot filter Web requests. If you have one N2H2 filter server on your network, schedule downloads to take place when users aren't browsing the Web. If you have multiple N2H2 filter servers, schedule each filter server to download Web content updates at a different time so that Web filtering is always available.

✓ *If Filtering by N2H2 is unable to download an update after repeated attempts, it continues to filter Web site requests using the most recent update received.*

To schedule Web content information downloads

1 Open Filtering by N2H2 and double-click Set System Options.

2 Click the Servers tab.

3 Choose the N2H2 filter server to schedule downloads for.

- To schedule downloads for a new N2H2 filter server, click Add, and then type the address of the filter server in the N2H2 Filter Server box.
- To schedule downloads for an existing N2H2 filter server, click the filter server in the list, and then click Change.

4 Specify the time for the download.

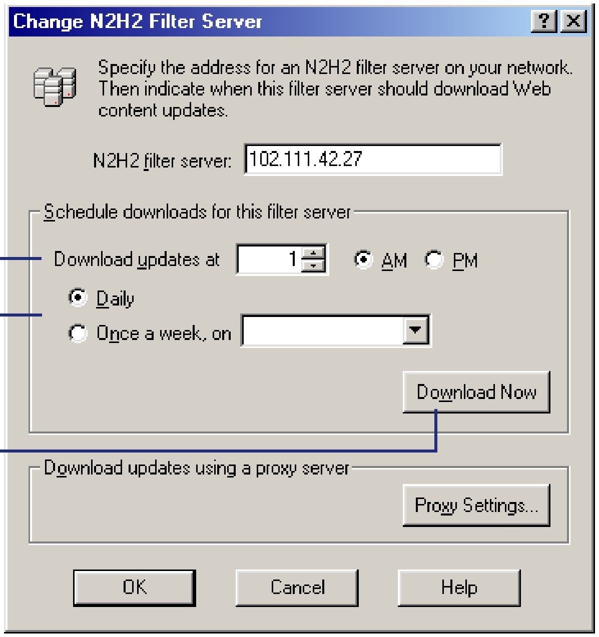
✓ *Downloads occur within an hour of the time you set. For example, if you choose 2 A.M., the server downloads the information between 2 A.M. and 3 A.M. according to the clock on your local N2H2 filter server.*

5 Click Daily or Once a Week to choose how often to download Web content updates from N2H2.

✓ *To provide the most accurate Web content filtering on your network, it's recommended that you download updates daily.*

6 If you chose to download updates once a week, choose the day of the week for the download.

7 Click OK, and then click OK again.



Change N2H2 Filter Server

Specify the address for an N2H2 filter server on your network. Then indicate when this filter server should download Web content updates.

N2H2 filter server: 102.111.42.27

Schedule downloads for this filter server

Download updates at 1 ● AM ○ PM

● Daily

○ Once a week, on

Download updates using a proxy server

Specify the time for the download. Downloads occur within an hour of the time you set.

You can download updates daily or once a week on a specific day.

To download the latest update immediately, click Download Now.

To get the latest Web content information immediately

1 Open Filtering by N2H2 and double-click Set System Options.

2 Click the Servers tab.

3 Click an N2H2 filter server in the list, and then click Change.

4 Click Download Now.

5 Click OK.

6 Repeat steps 3–5 for all other N2H2 filter servers on your network.

Setting advanced options

Specify advanced system options for Filtering by N2H2.

Use the Advanced tab to turn off multiple warnings for a certain period of time after a user bypasses the warning page.

Turning off multiple warnings

When you create a filter, you can set categories within that filter to Monitor with Warning. Then, when a user you've assigned that filter to attempts to access a site in a category set to Monitor with Warning, he or she sees a warning page. The user can then choose to bypass the warning page and view the site.

To prevent users from encountering additional warnings for sites in the *same category* as the site for which they bypassed an initial warning page, turn off multiple warnings. You can specify how long to turn off multiple warnings after the initial warning is bypassed.

For example, let's say that Mary, a user on your network, tries to access www.espn.com. Because the Sports category is set to Monitor with Warning under the filter you've assigned to her, Filtering by N2H2 displays a warning page. Mary decides to bypass the warning page and view the site.

If you've turned off multiple warnings, Mary can navigate to different areas within www.espn.com, as well as to other sites in the Sports category, without encountering additional warning pages for the amount of time you've specified. If you haven't turned off multiple warnings, Mary sees a warning page each time she tries to access a different page within www.espn.com, as well as when she tries to access other sports-related sites.

To turn off multiple warnings

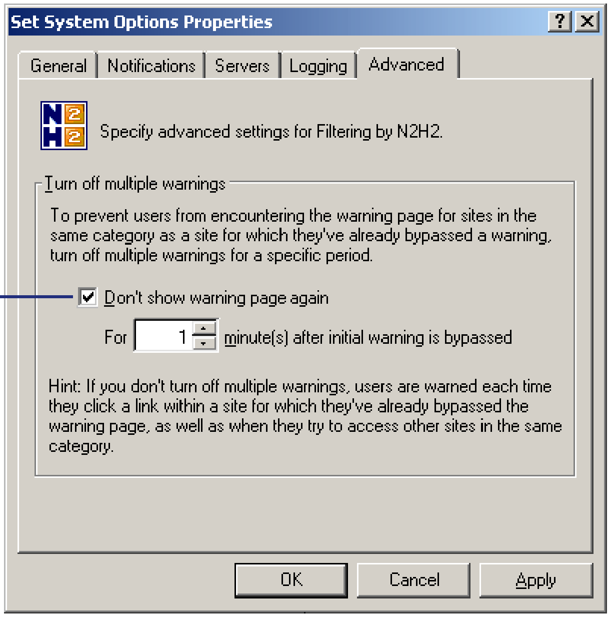
1 Open Filtering by N2H2 and double-click Set System Options.

2 Click the Advanced tab.

3 Check Don't Show Warning Page Again to turn off additional warnings for sites in the same category after a user bypasses the initial warning page.

4 Specify how long to turn off additional warnings after a user bypasses the initial warning page.

5 Click OK.



Specify advanced settings for Filtering by N2H2.

Turn off multiple warnings

To prevent users from encountering the warning page for sites in the same category as a site for which they've already bypassed a warning, turn off multiple warnings for a specific period.

☑ Don't show warning page again

For 1 minute(s) after initial warning is bypassed

Hint: If you don't turn off multiple warnings, users are warned each time they click a link within a site for which they've already bypassed the warning page, as well as when they try to access other sites in the same category.

To turn off multiple warnings, click Don't Show Warning Page Again, and then specify how long to turn off warnings after a user bypasses an initial warning page.

Chapter 4

Managing N2H2 IFP servers

Overview of N2H2 IFP servers

Specify IFP server settings for Filtering by N2H2.

The N2H2 Internet Filtering Protocol (IFP) server stores your filter settings, including user and group information and the global block and allow lists. When the N2H2 IFP server receives a Web request from your network device, it sends the request and the user's filter settings to the N2H2 filter server on your network. The N2H2 filter server checks the request against the most recent categorization information downloaded from N2H2, and then determines whether to block or allow the request.

You can install multiple N2H2 IFP servers on your network to support high network volumes. If you install multiple N2H2 IFP servers, create an array of N2H2 IFP servers. For information on arrays of N2H2 IFP servers, see "Creating arrays of N2H2 IFP servers" on page 21.

Specifying the address of the N2H2 IFP server

To administer Filtering by N2H2 remotely, install N2H2 administration and the N2H2 IFP server on separate computers, and then specify the address of the server where the N2H2 IFP server is installed.

✓ *You must be a member of the local administrator group on the computer that the N2H2 IFP server is installed on.*

To specify the address of the N2H2 IFP server

1 Open Filtering by N2H2.

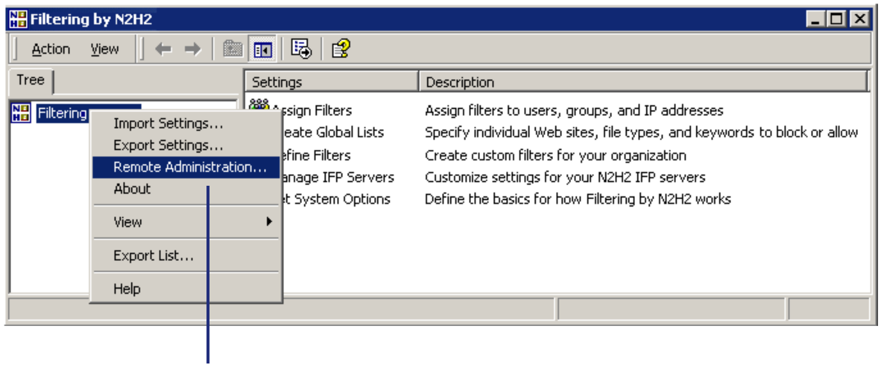
2 Right-click Filtering by N2H2 in the tree pane on the left, and then click Remote Administration.

3 Type the address of the server where the N2H2 IFP server is installed. If you installed multiple N2H2 IFP servers, type the address of any server where an N2H2 IFP server is installed.

The address can be the server's IP address, host name, or fully qualified domain name (FQDN). Be sure to specify a routable address, not a relative address (such as *localhost*).

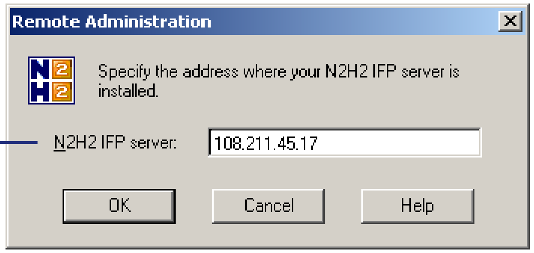
4 Click OK.

You can install N2H2 administration and the N2H2 IFP server on separate computers. If you move the N2H2 IFP server after installation, you must specify the new location.



Settings	Description
sign Filters	Assign filters to users, groups, and IP addresses
eate Global Lists	Specify individual Web sites, file types, and keywords to block or allow
fine Filters	Create custom filters for your organization
anage IFP Servers	Customize settings for your N2H2 IFP servers
t System Options	Define the basics for how Filtering by N2H2 works

Right-click Filtering by N2H2 in the tree pane, and then click Remote Administration.



Specify the address where your N2H2 IFP server is installed.

N2H2 IFP server: 108.211.45.17

Type the address of the server where the N2H2 IFP server is installed.

Specifying N2H2 IFP server settings

Change the port settings and IP address setting for your N2H2 IFP server(s) as necessary.

Specify settings for the N2H2 IFP server(s) on your network. If you have an array of N2H2 IFP servers, the port settings are propagated to all N2H2 IFP servers in the array. The IP address setting is not propagated.

To specify general IFP server options

1 Open Filtering by N2H2 and double-click Manage IFP Servers.

2 Change your port settings as necessary.

- ❖ To listen for IFP requests using TCP, in the TCP Port box, type the port number the N2H2 IFP server listens for IFP requests on.
- ❖ To listen for IFP requests using UDP, in the UDP Listen Port box, type the port number the N2H2 IFP server listens for IFP requests on.
- ❖ To reply using UDP, in the UDP Reply Port box, type the port number the N2H2 IFP server sends IFP responses to.

✓ *To reply to the port that the sender used to send the request, type 0 (zero) in the UDP Reply Port box.*

3 If you want the N2H2 IFP server to listen for IFP requests on one IP address only, type the IP address to listen on.

To listen for IFP requests on all of the N2H2 IFP server's IP addresses, leave this box empty.

4 Click OK.

✓ *Be sure to configure your network device to use the port number(s) you specified.*

Disabling TCP or UDP

By default, Filtering by N2H2 listens for IFP requests using two protocols, TCP and UDP. If you want, disable the protocol not in use on your network.

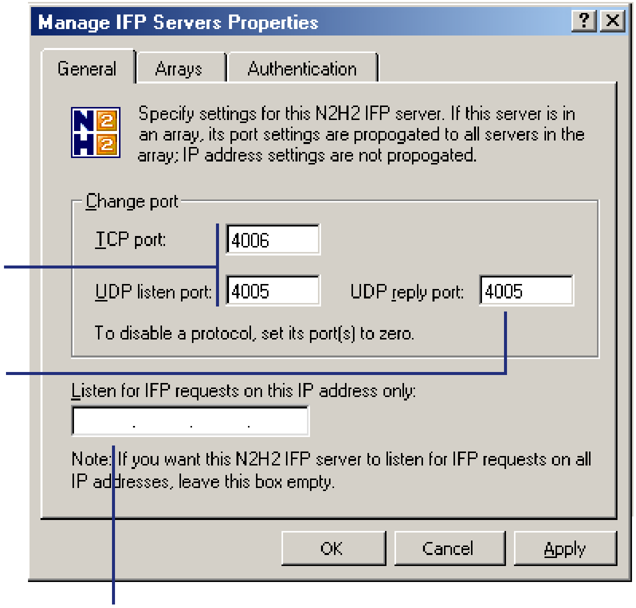
To disable TCP

❖ In the TCP Port box, type 0 (zero).

To disable UDP

❖ In the UDP Listen Port box, type 0 (zero).

Specify the TCP port and/or UDP ports to transfer IFP requests.



Manage IFP Servers Properties

Specify settings for this N2H2 IFP server. If this server is in an array, its port settings are propogated to all servers in the array; IP address settings are not propogated.

Change port

TCP port: 4006

UDP listen port: 4005 UDP reply port: 4005

To disable a protocol, set its port(s) to zero.

Listen for IFP requests on this IP address only:

Note: If you want this N2H2 IFP server to listen for IFP requests on all IP addresses, leave this box empty.

To disable TCP or UDP, type 0 (zero).

To reply to the port that the sender used to send the request, type 0 (zero).

To listen for IFP requests on one IP address only, type the IP address you want to listen on.

Creating arrays of N2H2 IFP servers

Create an array to easily update settings on multiple N2H2 IFP servers.

If you installed multiple N2H2 IFP servers to handle high network volumes, create an array of N2H2 IFP servers. An array of N2H2 IFP servers automatically propagates filter settings to each member in the array.

Special notes about arrays of N2H2 IFP servers:

- There are no master servers or client servers in arrays of N2H2 IFP servers.
- You must have administrative permissions to all servers in the array to join the array.
- New member servers take on the array's filter settings.

To create an array of IFP servers

1 Open Filtering by N2H2 and double-click Manage IFP Servers.

2 Click the Arrays tab.

3 Click Include This Server in Array.

"This Server" is the N2H2 IFP server specified under Remote Administration. For information on specifying an N2H2 IFP server under Remote Administration, see "Overview of N2H2 IFP servers" on page 19.

4 Choose whether to create a new array or join an existing array. To join an existing array, type the address of any N2H2 IFP server currently in the array.

The address can be the server's IP address, host name, or fully qualified domain name (FQDN). Be sure to specify a routable address, not a relative address, (such as *localhost*).

5 Click OK.

View the members in the array on the Arrays tab. To add an N2H2 IFP server to the array, click Add Another Server. Type the address of the N2H2 IFP server you want to add, and then click OK.

✓ *To change the array an N2H2 IFP server belongs to, first remove it from the current array. Then open Filtering by N2H2 from a computer in the new array, and add the N2H2 IFP server.*

To remove an IFP server from an array

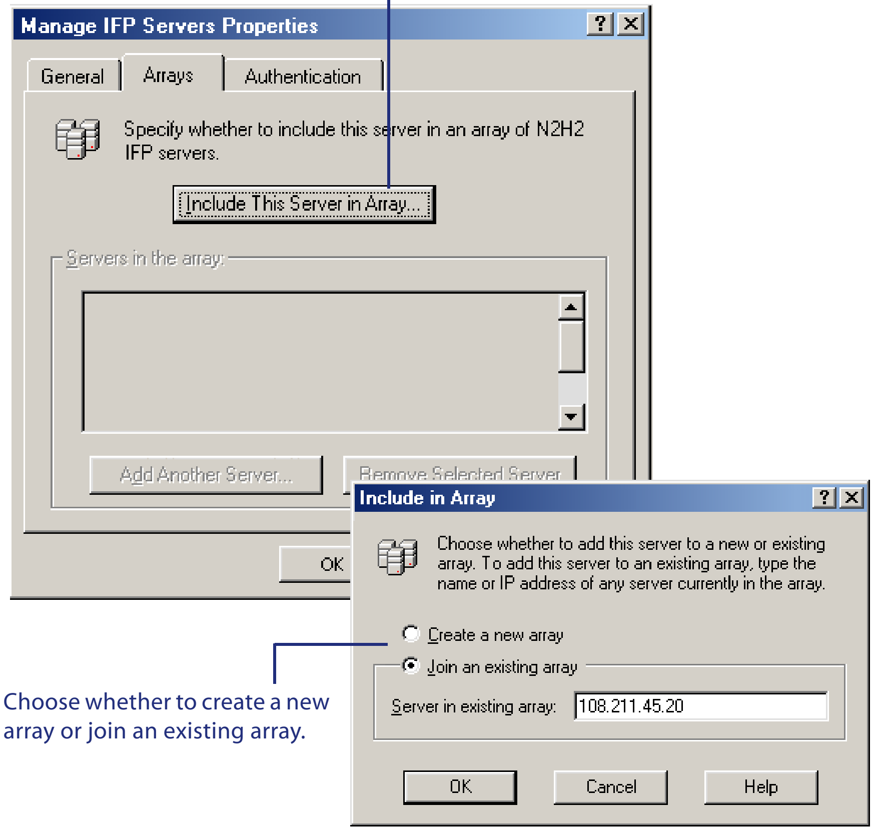
1 Open Filtering by N2H2 and double-click Manage IFP Servers.

2 Click the Arrays tab.

In the Servers in the Array list, click the N2H2 IFP server you want to remove from the array, and then click Remove Selected Server.

3 Confirm that you want to remove this N2H2 IFP server, and then click OK.

To create an array of N2H2 IFP servers, click Include This Server in Array.



Specify whether to include this server in an array of N2H2 IFP servers.

Choose whether to add this server to a new or existing array. To add this server to an existing array, type the name or IP address of any server currently in the array.

○ Create a new array

● Join an existing array

Server in existing array: 108.211.45.20

Choose whether to create a new array or join an existing array.

Using transparent authentication

Turn on transparent authentication on your Windows network.

Use the Authentication tab to allow transparent authentication on a Windows network. Transparent authentication lets you associate a user’s network logon with a particular IP address for a specific period of time; thus, users are not required to enter their logon information each time they open a Web browser.

✓ *The N2H2 authentication server must be installed and running before you configure transparent authentication.*

To use transparent authentication

1 Open Filtering by N2H2 and double-click Manage IFP Servers.

2 Click the Authentication tab.

3 Check Use Transparent Authentication.

4 Type the name of the server used for authentication.

✓ *The server name must be a Windows name; it cannot contain periods (.) and therefore cannot be an IP address or a FQDN. In addition, this server must be a member of the same domain, or of another trusted domain, where authentication is taking place.*

5 In the Authentication Duration list, click the length of time to associate a user’s Windows logon with a particular IP address.

✓ *When you specify a new duration setting, it takes effect the next time a user is authenticated. Any currently authenticated users still have the remainder of their original authentication time.*

6 To exclude certain IP addresses from transparent authentication, click Advanced.

✓ *For more information on excluding IP addresses from transparent authentication, see the procedure below.*

7 Click OK.

You can also exclude certain IP addresses and address ranges from transparent authentication as necessary.

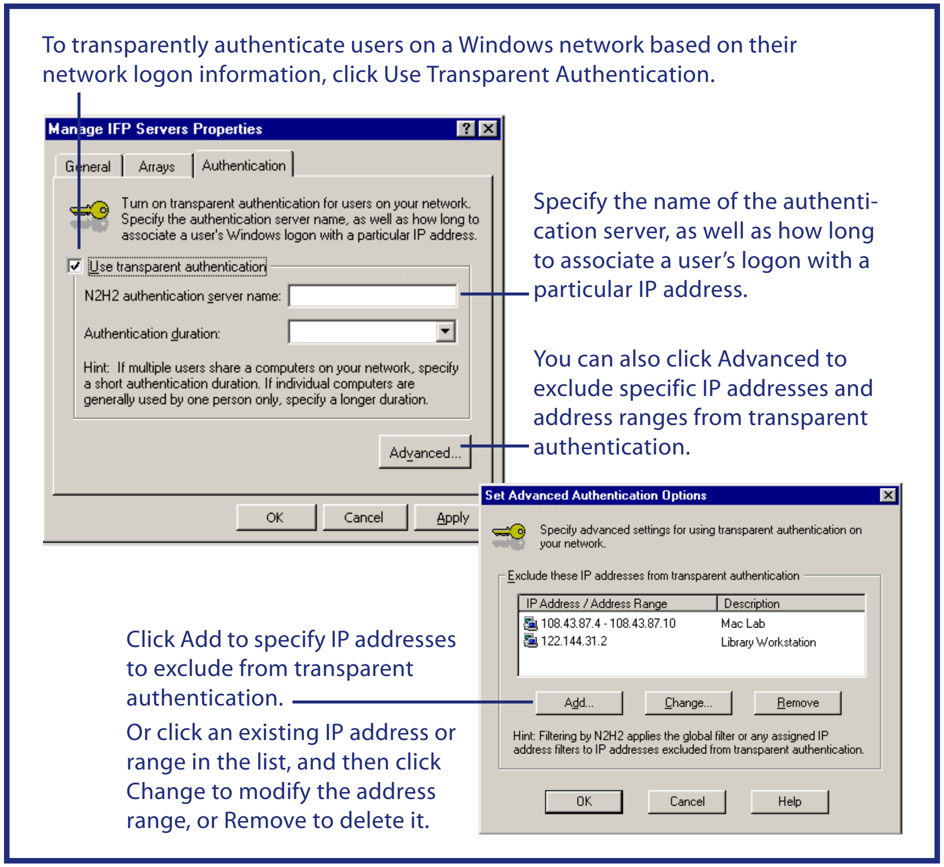
To exclude IP addresses from transparent authentication

1 On the Authentication tab, click Advanced.

2 Click Add to add a new IP address or address range to exclude. Or click an existing IP address or address range in the list, and then click Change.

3 In the From box, type the first IP address in the address range to exclude.

4 In the To box, type the last IP address in the address range to exclude.



To transparently authenticate users on a Windows network based on their network logon information, click Use Transparent Authentication.

Specify the name of the authentication server, as well as how long to associate a user’s logon with a particular IP address.

You can also click Advanced to exclude specific IP addresses and address ranges from transparent authentication.

Click Add to specify IP addresses to exclude from transparent authentication.

Or click an existing IP address or range in the list, and then click Change to modify the address range, or Remove to delete it.

Turn on transparent authentication for users on your network. Specify the authentication server name, as well as how long to associate a user's Windows logon with a particular IP address.

☑ Use transparent authentication

N2H2 authentication server name:

Authentication duration:

Hint: If multiple users share a computers on your network, specify a short authentication duration. If individual computers are generally used by one person only, specify a longer duration.

Specify advanced settings for using transparent authentication on your network.

Exclude these IP addresses from transparent authentication

IP Address / Address Range	Description
108.43.87.4 - 108.43.87.10	Mac Lab
122.144.31.2	Library Workstation

Hint: Filtering by N2H2 applies the global filter or any assigned IP address filters to IP addresses excluded from transparent authentication.

✓ *To exclude a single IP address from transparent authentication, just type the address in the From box and leave the To box empty.*

5 In the Description box, type a description of the IP address or address range.

6 Click OK, and then click OK again.

To allow transparent authentication of an IP address or address range that you’ve previously excluded from transparent authentication, remove the address or range from the list of IP addresses to exclude.

To allow transparent authentication of an excluded IP address or range

1 On the Authentication tab, click Advanced.

2 Click an existing IP address or address range in the list, and then click Remove.

3 Confirm that you want to allow transparent authentication of this IP address or range.

4 Click OK.

Chapter 5

Troubleshooting

Troubleshooting Filtering by N2H2

Resolve problems related to Filtering by N2H2.

This chapter provides suggestions for resolving problems related to Filtering by N2H2.

If you're unable to resolve a problem on your own, access online support resources at www.n2h2.com/support/ or call 800.246.1174 (in Seattle, call 206.336.1559).

Problems with installing Filtering by N2H2

I can't install the filter server component.

Make sure that the computer you want to install the N2H2 filter server on can connect to the Internet.

When you install the N2H2 filter server, you must register it by entering your Filtering by N2H2 account information, as well as an ID for the computer. Registration takes place automatically over the computer's Internet connection.

To run N2H2 Filter Server Setup again, open the Program Files folder on the computer where you installed the N2H2 filter server. Double-click the N2H2Filtering folder, and then double-click SignUpWin.exe.

I didn't register the filter server component when I first installed it, but I want to register it now.

To register the filter server component, run N2H2 Filter Server Setup: On the computer where you installed the filter server component, open the Program Files folder. Double-click the N2H2Filtering folder, and then double-click SignUpWin.exe.

Filtering by N2H2 Setup stalls when I try to add or remove Filtering by N2H2 components.

Use Windows Task Manager to close Filtering by N2H2 Setup, and then try again.

I've just installed Filtering by N2H2 for Microsoft ISA Server. How do I configure my ISA Server to work with Filtering by N2H2?

If you're using Filtering by N2H2 for Microsoft ISA Server, you must configure your ISA server to work with Filtering by N2H2. To do this, open ISA Server Management and do the following:

- Set your Microsoft ISA Server to allow HTTP and DNS traffic. To do this, create and enable HTTP Filter and DNS Filter.
- Create a site and content rule that forces authentication on the Microsoft ISA Server; or, create a global rule for the computer array that forces unauthenticated users to enter a user name and password. This lets you filter Web content for specific users and groups on your network.

For more information on configuring Microsoft ISA Server, see your Microsoft ISA Server Help.

Problems with downloading updates

Filtering isn't available immediately after I download an update.

Each time you download a Web content update, the N2H2 filter server restarts upon download completion. It takes about three minutes to process the update after the service restarts, and filtering is not available during processing. Use the Windows Event Log to view update processing status.

Because filtering is unavailable while the N2H2 filter server processes updates, it's recommended that you schedule downloads to occur when users aren't browsing the Web. Or, if you have multiple N2H2 filter servers, schedule each filter server to download Web content updates at a different time so that Web filtering is always available. For more information on scheduling downloads, see "Getting updated Web information" on page 16.

Web content updates aren't downloading.

There are a number of reasons why your N2H2 filter server may be unable to download Web content updates.

- The N2H2 database server, which resides on N2H2's network, is temporarily down.
- The account certificate you received from N2H2 was corrupted or deleted.
- Your Filtering by N2H2 trial period or contract has expired. Contact N2H2 sales support at 800.971.2622 (in Seattle, 206.336.1501).

In most cases, Filtering by N2H2 can continue to filter Web access on your network using the last update received. You can also try downloading the update manually. For more information on downloading updates manually, see "Getting updated Web information" on page 16.

Problems with filtering Web access

Users on my network can't access the Web.

View the default Web access option on the General tab under Set System Options. If your N2H2 filter server is down and you've chosen to block all Web access when

Filtering by N2H2 is unavailable, users on your network cannot access the Web. (Users with override privileges can always access the Web, even if all Web access is blocked for other users.)

To let users access the Web while filtering is unavailable, choose Allow Unfiltered Web Access. For more information on setting default Web access options, see "Setting basic system options" on page 13.

Users on my network can access any Web site regardless of the filter settings applied.

View the default Web access option on the General tab under Set System Options. If your N2H2 filter server is down and you've chosen to allow all Web access when Filtering by N2H2 is unavailable, users on your network can access any Web site allowed under your Microsoft ISA Server, Microsoft Proxy Server, or network device settings.

To prevent users from accessing the Web when filtering is unavailable, choose Block All Web Access. For more information on setting default Web access options, see "Setting basic system options" on page 13.

I added a site to my global block list, but it's still allowed.

Filtering by N2H2 uses a "longest path wins" rule to determine how sites that appear in both the global allow and block lists are handled.

For example, if you add www.cnn.com to your global block list and www.cnn.com/business to your global allow list, users can't view any pages at www.cnn.com *except* those with www.cnn.com/business in their URLs. (Thus, they can view www.cnn.com/business/stocks, but not www.cnn.com/sports.)

Check your global allow list to see if it contains the same site or domain, and then modify the global lists as necessary. For more information on blocking and allowing sites, see the *Filtering by N2H2 Administrator's Guide*.

I added a site to my global allow list, but it's still blocked.

Filtering by N2H2 uses a "longest path wins" rule to determine how sites that appear in both the global allow and block lists are handled. If a site appears in both global lists, and the site path is longer in the global block list, Filtering by N2H2 denies access to the site.

For example, if you add www.cnn.com to your global allow list and www.cnn.com/sports to your global block list, users can view all pages at www.cnn.com *except* those with www.cnn.com/sports in their URLs. (Thus, they can view www.cnn.com/business, but not www.cnn.com/sports/tennis.)

Check your global block list to see if it contains the same site or domain, and then modify the global lists as necessary. For more information on blocking and allowing sites, see the *Filtering by N2H2 Administrator's Guide*.

If you're using Filtering by N2H2 for Microsoft ISA Server, you can also view the access rules set up under ISA Server Management. If a site is allowed under Filtering by N2H2 but blocked under ISA Server Management site rules, users on your network can't view it.

For more information on setting ISA site and content rules, see Microsoft ISA Server Help.

I want to give users access to only a handful of Web sites.

To let users on your network access only a limited number of Web sites, you can create a "white list" filter and then apply it as the global filter for your network.

1 Open Filtering by N2H2 and double-click Define Filters.

2 Click the Custom Categories tab, and then click Add Category.

3 In the Name box, type a name for the custom category. The name should identify the category as a block category that prevents access to all Web sites except the few that you specify.

4 Click Block.

5 Type an asterisk (*), and then click OK.

6 Click Add Category again.

7 In the Name box, type a name for the second custom category. The name should identify this category as the exception category that includes the list of sites you want to allow.

8 Click Exception.

9 Type the Web sites, file types, and keywords to you want to allow.

✓ *For information on entering Web sites, file types, and keywords, see the* Filtering by N2H2 Administrator's Guide.

10 Click OK.

11 Click the Filters tab, and then click Add Filter.

12 In the Filter Name box, type a descriptive name for the filter.

13 Click the drop-down menu next to the block category you just created, and then click Block.

14 Click the drop-down menu next to the exception category you just created, and then click Allow.

15 Click OK, and then click OK again.

16 Double-click Assign Filters.

17 On the Global tab, check Global Filter, and then click the filter you just created.

18 Click OK.

I added a new user to an existing group on my network, but the filter settings I've assigned to that group aren't being applied to the user.

By default, Filtering by N2H2 applies group filter settings to new group members every morning at 4 A.M. To apply group filter settings to the new group member immediately, stop and restart the N2H2 IFP service.

I want to control how often user and group information is updated.

Filtering by N2H2 updates group and user information as follows: every morning at 4 A.M.; each time changes are applied in the Filtering by N2H2 interface; and each time the N2H2 IFP service is restarted.

To best suit your organization's needs, you can change how often Filtering by N2H2 updates user and group information.

1. Access the registry on the computer where the N2H2 IFP server is installed.
2. Select the N2H2 folder under HKLM\SOFTWARE.
3. To limit the conditions under which user and group information is updated, change the value of the DynamicGroupRefresh key to 1.

   When the value is set to 1, user and group information is updated only if these three conditions are met: 1) the N2H2 IFP server receives a request from a user that does not have an individual filter assignment; 2) one or more groups in your organization have filter assignments; and 3) the user's information is not cached. If all conditions are true, Filtering by N2H2 retrieves the user's group membership information from Active Directory. This information is then cached as described in step 4.
4. Choose how long Filtering by N2H2 caches information.
   - ❖ To flush the cache every X hours, change the value of the GroupRefreshFrequency key to **P:*number***, where ***number*** is an integer greater than 0. For example, to flush the cache every 12 hours, the GroupRefreshFrequency value would be **P:12**
   - ❖ To flush the cache every day at the same time, change the value of the GroupRefreshFrequency key to **D:*number***, where ***number*** is an integer between 0 and 23 that corresponds to the hour of day in military time. For example, to flush the cache every day at 7 PM, the GroupRefreshFrequency value would be **D:19**

   ✓ *By default, Filtering by N2H2 flushes the cache every morning at 4 A.M. (D:4).*
5. Restart the N2H2 IFP service.
6. Repeat steps 1 through 5 for all N2H2 IFP servers.

✓ *Filtering by N2H2 caches information using the GroupRefreshFrequency setting regardless of whether DynamicGroupRefresh is set to 0 or 1.*

Redirect pages aren't being displayed.

If requesting clients are on a different network than your N2H2 Web server, you must specify a domain name for the Web server. You can do this on the Servers tab under Set System Options. For more information on specifying N2H2 Web server settings, see "Specifying N2H2 server settings" on page 15.

I set up transparent authentication on my network, but users are still being prompted to enter a user name and password when they open their browsers.

Even if transparent authentication is turned on, users may be prompted to enter a user name and password when they open their Web browsers. This prompt generally appears if a user is browsing the Web using a computer that is running a non-Windows operating system, Windows XP, or a Web browser other than Microsoft Internet Explorer; if the user logged on to the computer as a local user; or if the authentication settings in the user's browser are more restrictive.

If a user is prompted to enter a user name and password when opening a Web browser, he or she must specify the name of the trusted domain server that his or her user name is being authenticated against.

- ❖ If prompted by Microsoft Internet Explorer, the user must type the name of the trusted domain server in the Domain box.
- ❖ If prompted by another Web browser (such as Netscape), the user must type <*domain name*>\<*user name*> (for example, mydomain\johnd) in the Name or User Name box.

Note that if the user does not specify a domain name when entering his or her user name and password, he or she may be authenticated against the N2H2 authentication server. (This occurs only if the user name entered exists on the authentication server.) This may cause the wrong filter to be applied to the user.

Chapter 6

Appendices

Appendix A:

Modifying the default redirect page

Customize N2H2's default redirect page for your organization.

N2H2 provides a default redirect page, as well as other default Web pages that may appear when a user attempts to access content that is blocked or monitored. These pages include functionality that let users submit site review requests, temporarily override filtering, and so on. You can customize these pages as necessary.

To customize the default redirect pages provided by N2H2

1 Using an HTML editor or text editor, access the Program Files\N2H2Filtering\html folder, and open the HTML file for the redirect page you want to customize.

2 Edit the file as necessary.

You can add and modify images, colors, fonts, spacing, tables, frames, and so on. However, to retain the functionality of the page, do not modify the existing formatting parameters (such as %url%, %clientip%, and other items formatted as %xxxx%) and certain tags (such as <a href=>, <form method=>, and <input type=>).

3 Save the file under the same name in the Program Files\N2H2Filtering\html folder. Do not change the file's name or location.

4 Restart the N2H2 IFP server to display the modified HTML file.

Notes on customizing the default redirect pages

- The default redirect pages available for modification include block, error, and warning pages, authorized override pages, review request pages, and restore filtering pages.
- If you have multiple IFP servers in an array, you must copy the customized page to the Program Files\N2H2Filtering\html folder on all IFP servers.
- To restore an original version of a redirect page, access the Program Files\N2H2Filtering folder and open the n2h2html.zip file. This file contains all original redirect page files.
- It is possible for resourceful users to access any file stored in the Program Files\N2H2Filtering\html folder via their Web browsers. Therefore, be sure that only those files that you want to return to users (such as redirect pages and any images you've included on these pages) are stored in this folder

Appendix B:

Creating redirect pages

To enhance your custom redirect page, you can incorporate CGI parameters to display details about redirected URLs.

! *You must have significant knowledge of Web page design and CGI scripting to successfully use the following parameters. Because there are numerous ways to create Web pages that use CGI parameters, you should consult your own Web design and scripting resources when creating these pages.*

To use a custom redirect page that is saved on your own Web server, you specify the page's location in the Location of Redirect Page box on the General tab (under Set System Options). You can also enter CGI parameters in the Location of Redirect Page box. For more information on specifying a custom redirect page, see “Setting basic system options” on page 13.

If you’re familiar with implementing CGI scripts on Web pages and want to include specific information about the redirected request on your custom redirect page, you can use the following CGI parameters. You must enter these parameters in the Location of Redirect Page box, as part of the custom redirect page URL.

- %url% The URL that was requested.
- %ip% The IP address of the URL that was requested.
- %clientip% The IP address of the client that made the request.
- %cats% The category (or categories) that the requested URL falls into. For predefined categories, the value is replaced with an abbreviated name. For custom categories, the value is replaced with a full names. (You can translate abbreviated names to display more meaningful information.)
- %username% The user name of the client that made the request. If the user name is unknown because authentication is not enforced, the value may be replaced with “anonymous,” or it may be an empty string.
- %replycode% The action taken. Depending on the filter settings, the value is replaced with “block,” “warn,” or “error.”

For example, let's say you want the redirect page to show the URL of the site that a user attempted to access, the category the site was blocked under, and the IP address of the computer used to access the site. You would type the following URL in the Location of Redirect Page box: **http://intranet.mycompany.com/block.html?url=%url%&category=%cats%&clientip=%clientip%**

Using these parameters, if you've chosen to block access to sites in the Search Engines category, and a user requests http://www.google.com, the result would be: http://intranet.mycompany.com/block.html?url=http%3A%2F%2Fwww.google.com&category=SE&clientip=192.168.0.1

Appendix C:

Using Virtual Inspector™ and Virtual Reviewer™

Use Filtering by N2H2's Virtual Inspector and Virtual Reviewer features to maximize the efficiency and effectiveness of your filtering implementation.

Virtual Inspector and Virtual Reviewer are powerful features that let you tailor N2H2's filtering database to your organization's filtering patterns, as well as improve the efficiency of your global block list.

✓ *Note that you can turn Virtual Inspector and Virtual Reviewer on and off whenever you choose. For step-by-step procedures on turning these features on and off, see "Setting basic system options" on page 13.*

Using Virtual Inspector

Through intelligent analysis of the URL data in your Web activity logs, Virtual Inspector gives you a secure, private, and efficient way to:

- Protect users from inadvertently accessing offensive Web material by ensuring that uncategorized sites are promptly reviewed and added to N2H2's filtering database.
- Stop Web abuse by preventing persistent users from repeatedly circumventing your organization's filtering policy.
- Allow the Web sites that are accessed most frequently by users in your organization to be reviewed regularly for changes that could affect categorization.

When analyzing your log files, Virtual Inspector doesn't just look for uncategorized Web sites. Instead, it uses a targeted criteria set to pinpoint only those specific URLs that might present potential problems, as well as to detect Web surfing patterns that are unique to your organization.

To gather only the most relevant URL information from your log files, Virtual Inspector evaluates log file information according to three types of criteria:

- **Keyword.** Virtual Inspector scans URLs for keywords that indicate that the sites might fall into certain key categories, such as Sex, Porn, Gambling, Hate, and Violence. Intelligent keyword matching helps Virtual Inspector distinguish safe sites from those that could pose potential problems.
- **Activity pattern.** By pinpointing unusual surfing patterns, Virtual Inspector can detect when problem sites that haven't yet been categorized may have been accessed. It captures these URLs for review and categorization. (Because Virtual Inspector captures only URL data, activity patterns can't be linked to specific users or IP addresses on your network.)
- **Frequency.** Virtual Inspector compiles a list of the most frequently accessed URLs on your network and returns this list to N2H2. This ensures that the sites accessed most frequently within your organization are regularly reviewed and re-categorized as necessary, thus promoting more accurate Web activity reporting for your network.

In addition, Virtual Inspector protects your organization's data and network resources by:

- **Ensuring anonymity.** Virtual Inspector gathers only pertinent URL information based on targeted reporting criteria. It doesn't report end-user data of any kind. Thus, the URL information reported by Virtual Inspector is completely anonymous and can't be linked to particular users or IP addresses on your network.
- **Encrypting data during transmission.** All data is SSL-encrypted as it's transferred to N2H2, thus ensuring that it can't be accessed by a third party.
- **Reporting only the most relevant URL data.** Because it targets only those URLs that meet its specific keyword, surf pattern, and frequency criteria, Virtual Inspector reports only a small amount of the data in your log files. It doesn't provide a "data dump," and it doesn't simply compile all of the uncategorized URLs that appear in your log files. Thus, the data transfer process can be performed quickly and without monopolizing network resources.

Using Virtual Reviewer

Virtual Reviewer improves the efficiency of your global block list by automatically looking for and removing any URLs that have already been categorized in N2H2's database. This ensures that your custom block list remains as compact as possible.

When Virtual Reviewer finds a URL that has been categorized by N2H2, it removes the URL and then sends you an e-mail notification. This notification specifies which URL was removed, as well as how that URL is categorized by N2H2.

Virtual Reviewer also forwards the URLs in your global lists to N2H2 for review. Forwarding these URLs to N2H2 lets the N2H2 review team analyze the URLs and categorize them as appropriate.

✓ *Note that you can prevent Filtering by N2H2 from removing specific URLs from the block list by typing* **[lock]** *before each URL you want to keep. For example, if you type* **[lock] www.sports.com***, www.sports.com cannot be automatically deleted from your block list.*

Index