



Monitor · Manage · Control

ContentKeeper – Bypassing Microsoft ISA Server

Overview

A ContentKeeper server must access the ContentKeeper DataCenter in order to retrieve its hourly updates. A ContentKeeper server connects to the DataCenter via the HTTP protocol, in the same way that a browser connects to the Internet. It is common to use a proxy server when connecting the ContentKeeper Management to the Internet.

In cases where a proxy server requires authentication, a bypass must be configured for the ContentKeeper Management port. This document describes how a bypass may be configured on a dual homed Microsoft ISA server.

Document Revision B

Date: 5th May 2003

Copyright © 2000, 2001,2002, 2003 ContentKeeper Technologies

ContentKeeper® Closed Loop Collaborative Filtering™ and *TrickleFeed™* are trademarks of ContentKeeper Technologies. Copyright © 2000 - 2003, ContentKeeper Technologies, Canberra, Australia. All Rights Reserved.

Linux is a registered trademark of Linus Torvalds, Red Hat Linux is a registered trademark of Red Hat Inc.

All other product names mentioned herein are trademarks or registered trademarks of their respective owners.

The products and specifications, configurations, and other technical information regarding the products contained in this manual are subject to change without notice. All statements, technical information, and recommendations contained in this manual are believed to be accurate and reliable but are presented without warranty of any kind, express or implied, and users must take full responsibility for their application of any products specified in this manual.

Document Author & Designer: Matthew R Richards

ContentKeeper Technologies
218 Northbourne Avenue
Braddon ACT 2612
Australia
PH +61-2-62614950
Fax +61-2-62579801
info@ContentKeeper.com
www.ContentKeeper.com

ContentKeeper and Proxy Servers

Accessing the DataCenter

A central component of the ContentKeeper Internet content filtering solution is the ContentKeeper URL database. The URL database is a growing entity that changes in real time to reflect the current state of the Internet.

The ContentKeeper URL Database is housed within the ContentKeeper DataCenter. All ContentKeeper servers connect to the DataCenter on an hourly basis to retrieve updates to their local copy of the URL database as well as contribute new and reclassified URLs.

This document is designed to assist those administrators whose networks make use of a Microsoft ISA Server, dual homed and configured to require authentication, in allowing ContentKeeper to access the DataCenter.

Integrating ContentKeeper

Version 117.9 of ContentKeeper cannot negotiate authentication on outgoing HTTP requests. An example of this is an HTTP proxy server that requires authentication.

This means that if you configure ContentKeeper to use an HTTP proxy server that requires authentication, ContentKeeper will not be able to authenticate, and therefore fail to register with the DataCenter for its hourly updates.

The solution is to enable a bypass for the ContentKeeper Management Port within the proxy server, or to bypass the proxy server all together. Bypassing an ISA server all together is only possible when the ISA server is not the gateway device.

Planning Considerations

When planning to enable a bypass for the ContentKeeper Management Port within an ISA server, there are a number items to consider. Each item and the repercussions of changing its configuration should be examined.

The following items will be affected by enabling a bypass for the ContentKeeper Management Port within the ISA server:

- **This document has been designed for use with an ISA Server configured with two or more network interface cards.**
- **Protocol Rules** (The Protocol Rules must be updated to enable the management port to access the DataCenter.)
- **Site and Content Rules** (The Site and Content Rules must be updated to enable the management port to access the DataCenter.)

- **HTTP Redirector Filter** (The HTTP Redirector Filter must be reconfigured to forward HTTP requests to the requested server.)
- **Existing Rules or Filters** (Ensure that any existing rules or filters do not prevent ContentKeeper from accessing the DataCenter.)

Technical Support

ContentKeeper Technologies recognise the need to provide world-class support to our global customers and have put in place a technical support infrastructure to ensure that technical support calls are recorded and responded to in a timely manner.

Our helpdesk technicians are ContentKeeper product specialists with extensive background in networking at both infrastructure and systems level. This allows most support calls to be resolved quickly, usually on the first call. Should additional assistance be required, our technicians also have access to network specialists as well as to the ContentKeeper development team and are willing to work with you to resolve any problems.

ContentKeeper Technical Support Contact Details

ContentKeeper Technologies
218 Northbourne Avenue
Braddon ACT 2612
Australia
PH +61-2-62614950
Fax +61-2-62579801
support@ContentKeeper.com
www.ContentKeeper.com

Procedure Overview

The following is an overview of the procedure involved in enabling a bypass for the ContentKeeper Management Port within the ISA Server:

1. Create a new Client Address Set

The new Client Address Set will allow the ISA Server to uniquely identify ContentKeeper by the Management Port IP address.

2. Create a new Protocol Rule

The new Protocol rule will allow TCP/IP traffic of a specified type that originates at the ContentKeeper server to traverse the ISA Server.

3. Create a new Site and Content rule

The new Site and Content rule will allow ContentKeeper to retrieve updates from the DataCenter uninhibited.

4. Reconfigure the HTTP Redirector Filter

The HTTP Redirector Filter will be reconfigured to redirect HTTP requests directly to the Internet instead of to the ISA Proxy service.

5. Examine existing rules and filters

Configure exclusions for any existing rules or filters do not prevent ContentKeeper from accessing the DataCenter

6. Restart

7. Configure ContentKeeper

The ContentKeeper server will be configured to connect straight to the Internet, not via a proxy server.

The full procedure for enabling a bypass within a Microsoft ISA Server is outlined in the following pages.

This document has been designed for use with an ISA Server configured with two or more network interface cards.

For more Information regarding ContentKeeper and the DataCenter refer to the ContentKeeper Administration Guide.

Create a new Client Address Set

To open ISA Management, click **Start**, point to **Programs**, point to **Microsoft ISA Server**, and then click **ISA Management**.

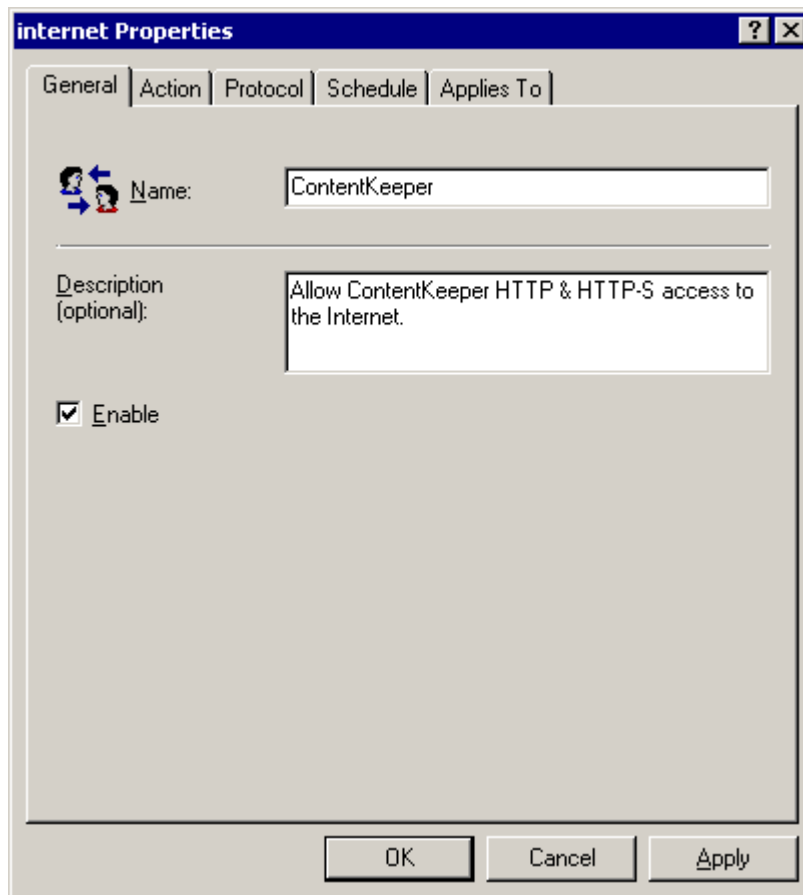
1. In the console tree of **ISA Management**, locate **Client Address Sets**.
 - o Internet Security and Acceleration Server
 - o Servers and Arrays
 - o *Name*
 - o Policy Elements
 - o Client Address Sets

From	To
192.9.200.67	192.9.200.67

2. Right-click **Client Address Sets**, point to **New**, and then click **Set**.
3. In **Name**, type **ContentKeeper**.
4. (Optional) In **Description**, type a description for the set.
5. Click **Add**.
6. In **From**, type the IP address of the ContentKeeper Management port.
7. In **To**, type the IP address of the ContentKeeper Management port then click **Ok**.
8. Click **Ok** to finish.

Create a new Protocol Rule

1. In the console tree of **ISA Management** locate **Protocol Rules**.
 - o Internet Security and Acceleration Server
 - o Servers and Arrays
 - o *Name*
 - o Access Policy
 - o Protocol Rules



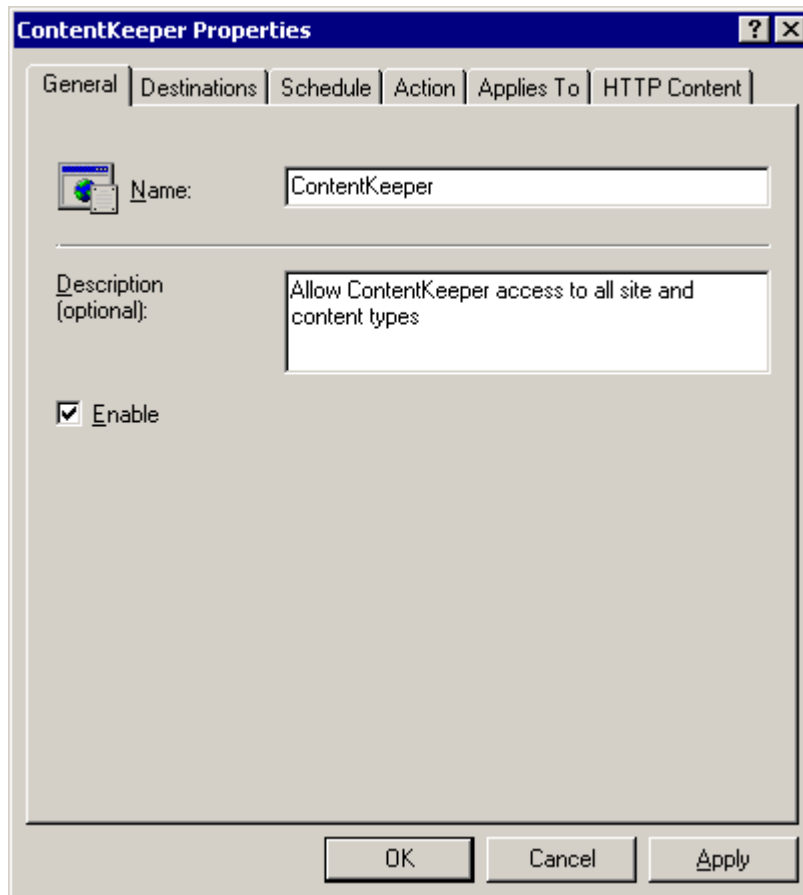
2. Right-click **Protocol Rules**, point to **New**, and then click **Rule**.
3. In the New Protocol Rule Wizard, type a name for the new rule.
4. In **Name**, type **ContentKeeper**.
5. (Optional) In **Description**, type a description for the set.
6. Choose **Selected Protocols** from the **Apply this rule to:** drop down box.
7. In the **Protocols** field, select the following:
 - o **HTTP**
 - o **HTTPS**

Note: If you use a DNS server that is not on your local network, then you will also need to select **DNS Query**.

8. Specify the **Always** Schedule.
9. Choose **Specific computers (client address sets)**.
10. Click **Add** and highlight the **ContentKeeper** address set, then click **Add** followed by **Ok**. Click **Ok** to finish.

Create a new Site and Content Rule

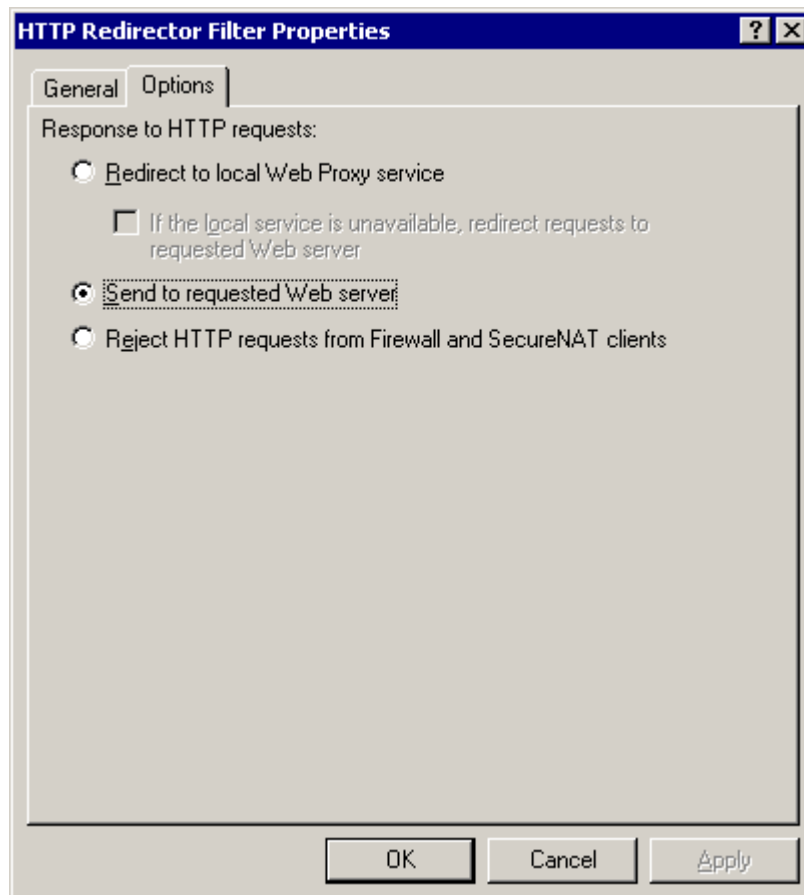
1. In the console tree of **ISA Management**, locate **Site and Content Rules**.
 - o Internet Security and Acceleration Server
 - o Servers and Arrays
 - o *Name*
 - o Access Policy
 - o Site and Content Rules



2. Right-click **Site and Content Rules**, point to **New**, and then click **Rule**.
3. In the New Site and Content Rule Wizard, type a name for the new rule.
4. In **Name**, type **ContentKeeper**.
5. Select a **Custom** rule configuration.
6. Select **All Destinations**.
7. Choose a schedule of **Always**.
8. Choose **Specific computers (client address sets)**.
9. Click **Add** and highlight the **ContentKeeper** address set, then click **Add** followed by **Ok**.
10. Specify **Any Content Type**.
11. Click **Finish**.

Reconfigure the HTTP Redirector Filter

1. In the console tree of **ISA Management**, locate and click **Application Filters**.
 - o Internet Security and Acceleration Server
 - o Servers and Arrays
 - o *Name*
 - o Extensions
 - o Application Filters



2. In the details pane, right-click **HTTP redirector filter** and select **Properties**.
3. On the **Options** tab, click **Send to requested web server**.
4. Click **Ok** to finish.

Examine Existing Rules and Filters

If the ContentKeeper Management Port has been assigned an IP address from a network to which the Microsoft ISA Server is attached it is possible that one or more of the existing Protocol Rules or Site and Content Filters may prevent the Management Port from accessing the DataCenter.

Rules or Filters that either apply to a **Client Set** whose scope includes the Management Port IP address, or apply to **Any Request** or **All Destinations**, will affect the Management Port.

Ensure that any existing Protocol Rules or Site and Content Filters do not prevent ContentKeeper from accessing the DataCenter.

1. In the console tree of **ISA Management**, locate **Protocol Rules** and **Site and Content Filters**.
 - Internet Security and Acceleration Server
 - Servers and Arrays
 - *Name*
 - Network Configuration
 - Protocol Rules
 - Site and Content Rules
2. Determine whether or not the existing **Protocol Rules** and **Site and Content Filters** affect the Management Port IP address.
3. Exclude the ContentKeeper Management Port from any of the existing **Protocol Rules** and **Site and Content Filters** that affect the Management Port using the following method:
 - a. View the Properties of each of the existing **Protocol Rules** and **Site and Content Filters**.
 - b. Under each Rule or Filter, select the **Applies To** tab.
 - c. Click the **Add** button next to the **Exceptions** field.
 - d. Add the ContentKeeper **Client Address Set**.
 - e. Apply any changes.

Restart

Restart the Microsoft ISA Server Proxy and Firewall services or restart the server if possible.

View the Microsoft ISA Server Proxy and Firewall services in the following location:

- Internet Security and Acceleration Server
 - Servers and Arrays
 - *Name*
 - Monitoring
 - Services

Stop and then start the by right clicking on each service and selecting **Stop** and then **Start**.

Configure ContentKeeper

As the Microsoft ISA Server has been configured to send requests directly to the requested web server, ContentKeeper will not be connecting to the proxy server. Use the following method to ensure that ContentKeeper is not configured to use a proxy server.

To access the **ContentKeeper Web Interface**, use an Internet browser to browse to the IP address of the **Management Port**.

Management Port Proxy Settings

Use a Proxy Server	No
Proxy IP Address	<input type="text"/>
Proxy Port	<input type="text"/>

(**Caution:** This will restart ContentKeeper!)

1. Under the **Operational Settings** menu click on **Management Port Proxy Settings**.
2. Ensure that **Use a Proxy Server** is set to **No**.
3. Click **Save** to apply any changes.

For more Information regarding ContentKeeper and the DataCenter refer to the ContentKeeper Administration Guide.