

InterJak Application Notes Content Filtering

Filanet Corporation
931 Benecia Avenue
Sunnyvale, CA 94085 USA
(408) 331-2900

TABLE OF CONTENTS

InterJak Content Filtering

- Introduction**
- Benefits of Content Filtering**
- Content Filtering Database**
- InterJak Content Filtering**
 - Implementation**
 - Configuration**
 - Solutions**
 - Specifications**
 - Setup Check List**

InterJak Content Filtering Applications

Introduction

Content Filtering is a software technology that prevents or allows access to Internet sites. It is mainly used to block offensive sites, enhance productivity, reduce legal liability, optimize network bandwidth and enhance security.

The Internet connectivity creates a temptation to connect to unproductive, inappropriate and potentially dangerous sites. Studies show that majority of employees use the Internet on a regular basis for their personal use during the normal work hours. On an average, non-work related Internet surfing costs businesses in productivity losses every year. Popular activities by employees include e-mail to family and friends, visiting newsgroups, trading stocks, checking sports and searching jobs etc. All these activities add to the cumulative productivity loss of the company.

Benefits of Content Filtering

Enhance Productivity

The InterJak Content Filtering service uses content filters to block unproductive sites and increase the bandwidth availability on the WAN link by reducing the number of packets to be forwarded across the link.

Optimize Bandwidth

Non-work related activities consume valuable bandwidth and thus cost companies millions of dollars every year. By making better use of WAN resources, a network operation can save a substantial amount of money for the company.

Reduce Legal Liability

In addition to the productivity and bandwidth losses, objectionable and offensive materials in the office can cause major liabilities to the companies in embarrassing and expensive lawsuits.

Enhance Network Security

Excessive Internet surfing by the employees to unprotected sites may allow unauthorized hackers to create security holes, gain access to corporate information and perhaps download unauthorized applications.

Protect Students from Objectionable Sites

With more and more Internet usage in schools and libraries it has become increasingly important to protect students from the easily accessible objectionable content on the Internet.

InterJak Content Filtering is configured as an add-on keyed service that must be purchased before activating this service. Service Providers can choose to offer Content Filtering as part of their base service or a stand-alone value added service, depending on the individual needs of their customers.

Content Filtering Database

InterJak uses a professionally compiled proprietary set of CyberLists from SurfControl. The CyberLists are compiled by professional researchers, and then reviewed by the SurfControl oversight committee on a regular basis. The InterJak Content Filtering Service combines the following set of CyberLists into a single filter database:

- CyberNOT – depicting Nudity & other offensive sites
- CyberYES – considered appropriate for children
- Sports & Entertainment – Not appropriate to employees during work time
- HotNOT – Daily updates merged weekly into CyberNOT List

Sites included in the lists are organized into categories and subcategories, which then form the basis for defining flexible filtering rules. For example, the CyberNot list has the following twelve categories:

- Full Nudity
- Sex Education
- Sexual Acts / Text
- Violence / Profanity
- Intolerance
- Satanic or Cult
- Militant / Extremist
- Drugs / Drugs Culture
- Partial Nudity
- Illegal Gambling
- Alcohol & Tobacco
- Gross Depictions / Text

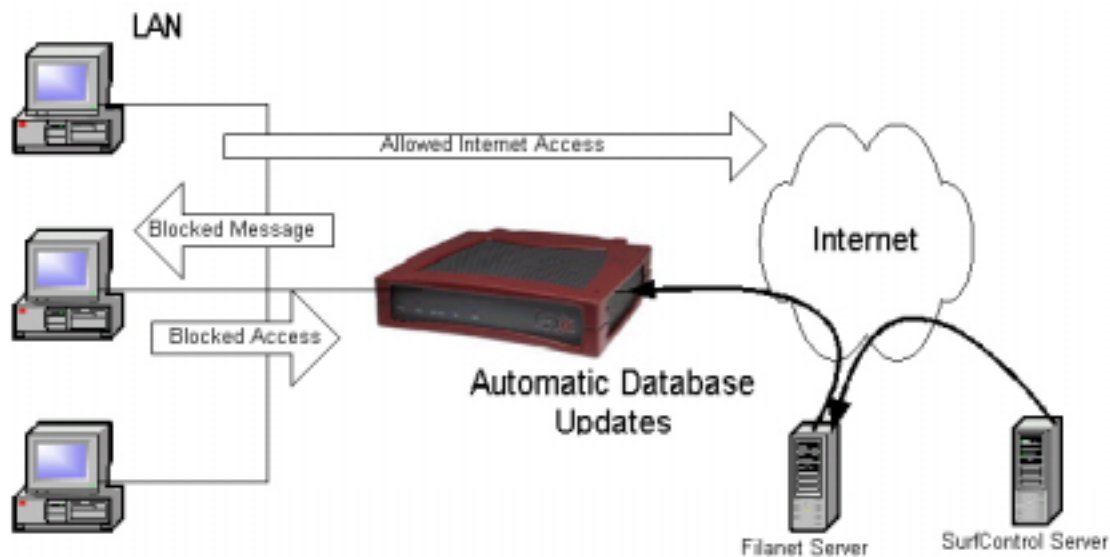
Since the Internet is changing continuously, the lists are updated regularly and are available for download to create specific filters for implementation on the InterJak. Separate categories of the CyberLIST may be combined in a Filter file and then automatically loaded on the InterJak according to the configuration.

InterJak Content Filtering Implementation

When the InterJak is powered, filter database is automatically downloaded from an external server. The default server address and filename for downloading the filter database are as follows:

Update Server: filters.filanet.com
 Update Filename: FILTER.V1 (All capital letters)

Access to the Internet is blocked during the database download. If the download fails, access will remain blocked until the download succeeds which is retried every 30 seconds. Once the filter database is loaded into the InterJak, Internet access is allowed according to the filter configuration.



InterJak Content Filtering Implementation

InterJak Content Filtering works as follows:

1. Content Filtering can only be applied to traffic on the Ethernet 1 interface of the InterJak. If the Content Filtering service is enabled then these settings will override the Web Site Filtering settings in the InterJak.

Filter Profiles

2. The InterJak Content Filtering uses the concept of Filter Profiles to be able to assign different access rights to different users on the local network. In addition, access restrictions can be applied based on the time of day, and day of week according to a Filter Schedule. It might be that all users accessing the Web through the InterJak will be filtered based on the default profiles according to the defined filter schedule. For example,

during normal working hours, access to the Sports and Entertainment pages are denied, but they may be allowed after hours and during the lunch break. A client (identified by its source IP address) can be assigned to a specific filter profile, e.g. allowing a dedicated PC to access pages related to, say, alcohol and tobacco. Once a client is assigned a Filter Profile, the profile is valid for the client regardless of the schedule. There are a total of 8 different profiles, each of which specify a number of Allowed Filtering Categories. These can be selected/ deselected as required.

3. When a request for a web address or newsgroup from a client computer is made, the InterJak looks up the source IP address to get the assigned Filter Profile. If no profile is specifically defined for that user then the default profile applies, according to the Filter Schedule.
4. The InterJak looks at the destination address and checks to see if the address is in the filter database of IP addresses.
5. If the address is not in the list, the default action of the profile (Allow or Deny) is applied.
6. If the address is in the list, the InterJak matches the categories given in the filter database for that address against the categories and their permissions defined in the profile. If the filter blocks any of the categories, access is denied to the client.
7. Sometimes the database will list a destination address as a “maybe” because some areas of a website do not contain listed category material but other areas do. In this case, the InterJak checks each URL as requested by the client, responding by proxy. This is therefore a partially blocked site.
8. Newsgroups are filtered similarly to web sites, using the same profile definition. In the filter database, individual newsgroup names are assigned to categories, just like web sites are. Then access to the newsgroup is blocked or allowed according to the category rules defined in the profile.

In addition, there is an additional control that can be imposed using the NNTP Server field in the InterJak Content Filtering configuration screen. If a News Server name is entered into this field, then users will only be able to access news groups from that news server. All client computers must be configured with the InterJak as their news server, and the InterJak will act as a proxy for all news requests. The category rules defined in the profile still apply.

If the NNTP Server field is left blank, then LAN clients can access any news server they want, but access to specific news groups will still be controlled by the profile definition.

InterJak Content Filtering Configuration

To enable the Content Filtering, enter the service key in the **Services** window of the InterJak Web Manager. Content Filtering can be easily configured through the **Services: Content Filter** window. The following window shows:

- *Filter Schedule* shows the active profiles at different times of the day.
- *Filter Profiles* is an overview of the profiles for content filtering.
- Local Content Filter Management allows associating a profile with specific clients (IP addresses).

Content Filtering Setup
 Status: Using profile: Profile 1
 Automatic update: Every 6 hours from filters.filanet.com
 Reject response: Default
 News server: Transparent
 Refresh Edit

Filter Schedule

Time Period	Mon	Tue	Wed	Thu	Fri	Sat	Sun
0:00 - 9:00	Profile 1	Profile 1	Profile 1	Profile 1	Profile 1	Profile 1	Profile 1
9:00 - 17:00	Profile 1	Profile 1	Profile 1	Profile 1	Profile 1	Profile 1	Profile 1
17:00 - 24:00	Profile 1	Profile 1	Profile 1	Profile 1	Profile 1	Profile 1	Profile 1

Edit Periods Edit Schedule

Filter Profiles

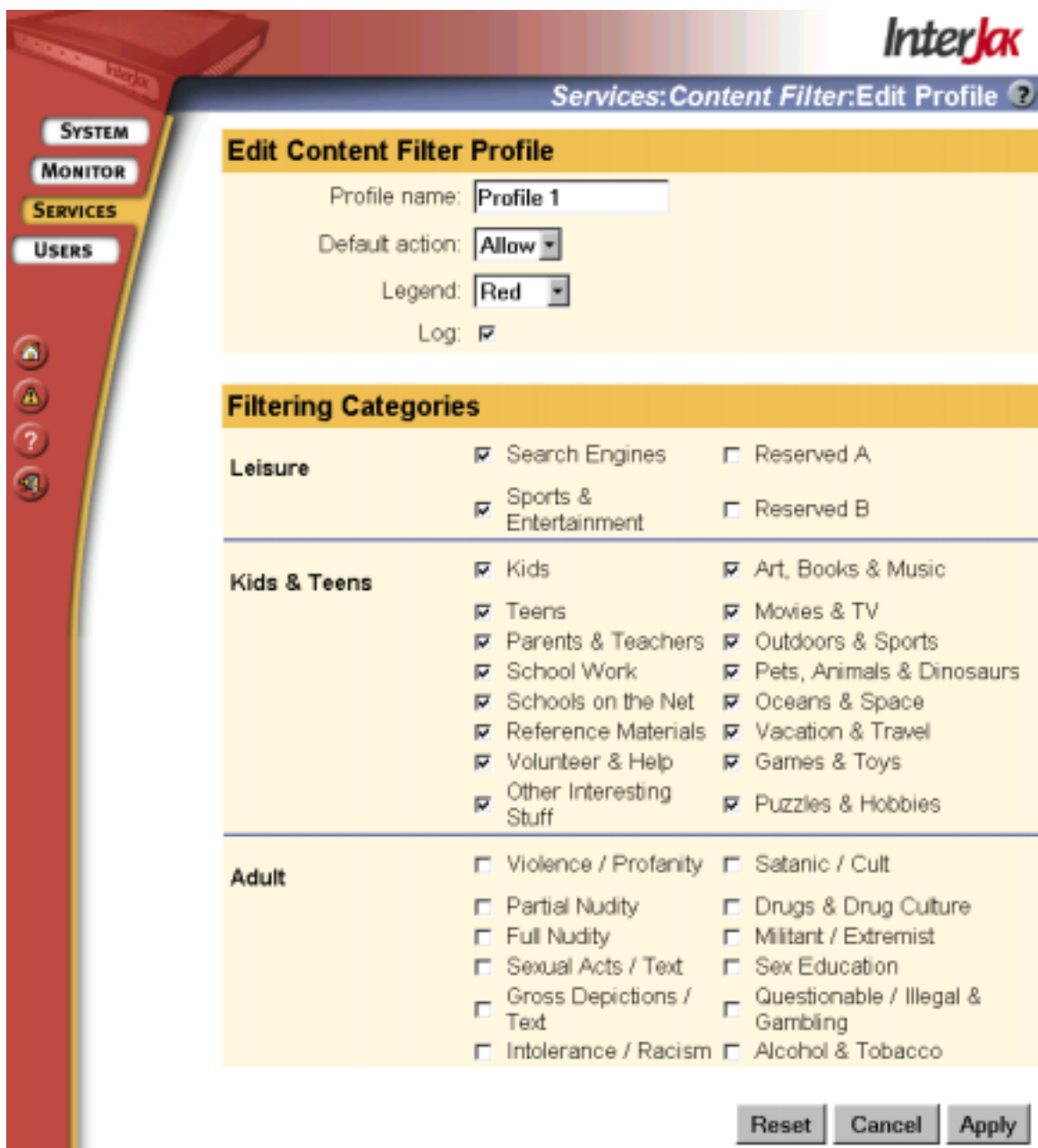
Profile	Default	Search	Leisure	Kids	Adult	Log
Profile 1	✓	✗	✗	✗	✓	Yes
Profile 2	✓	✓	✓	✓	✗	Yes
Profile 3	✗	✓	✗	✓	✗	Yes
Profile 4	✓	✓	✗	✓	✗	Yes
Profile 5	✓	✓	✗	✓	✗	Yes
Profile 6	✓	✓	✗	✓	✗	Yes
Profile 7	✓	✓	✗	✓	✗	Yes
Profile 8	✓	✓	✓	✓	✓	Yes

Local Content Filter Management
 Local Clients
 Back

Please refer to InterJak Internet Service Appliance Administrative Guide for detailed configuration details. However, the summary of the configuration features is listed below.

Configuring Filter Schedule – Configure time periods in 24-hour clock and Filter Profile association with the time periods.

Configuring Filter Profile – Edit Profile names, select categories to allow or block, default action for the sites not included in the filter database etc.



Local Content Filter Management - Link local clients by IP addresses to specific profiles. If a client is associated with a profile, the access restrictions of that profile always apply, regardless of the time of the day.

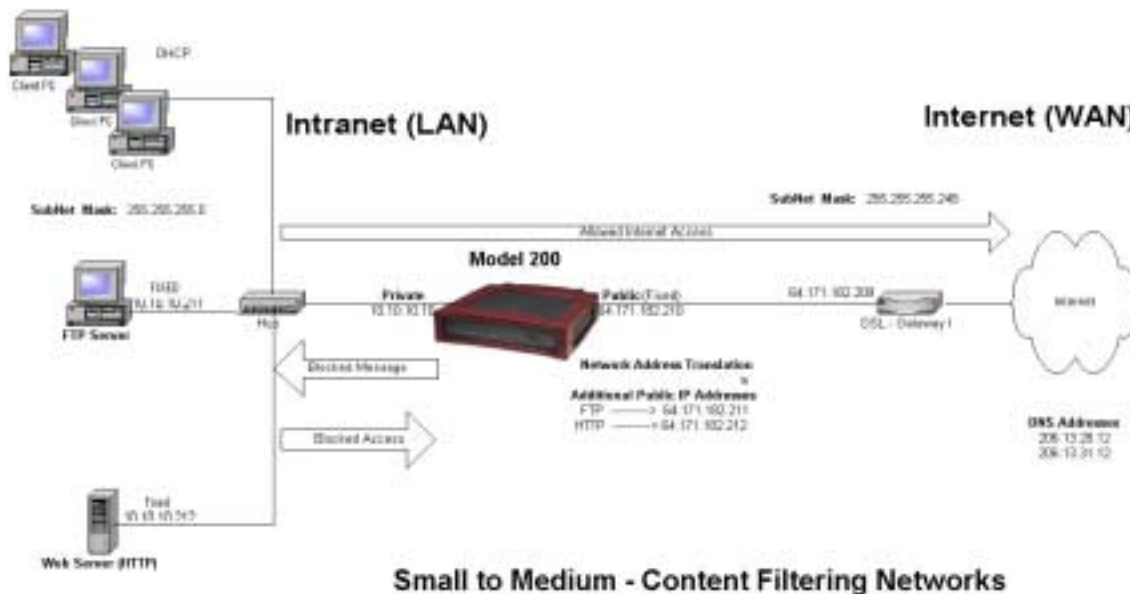
If the above IP address(s) is contained in more than one range, the union of all the access restrictions is applied. However, if one of the associations is checked exclusive, then this profile will apply.



InterJak Content Filtering Solutions

Small to Medium size networks

The following diagram shows a typical small to medium size office network setup. In addition to firewall, network Address Translation (NAT), Virtual Private Network (VPN) and number of other services, InterJak also provides Content Filtering service.

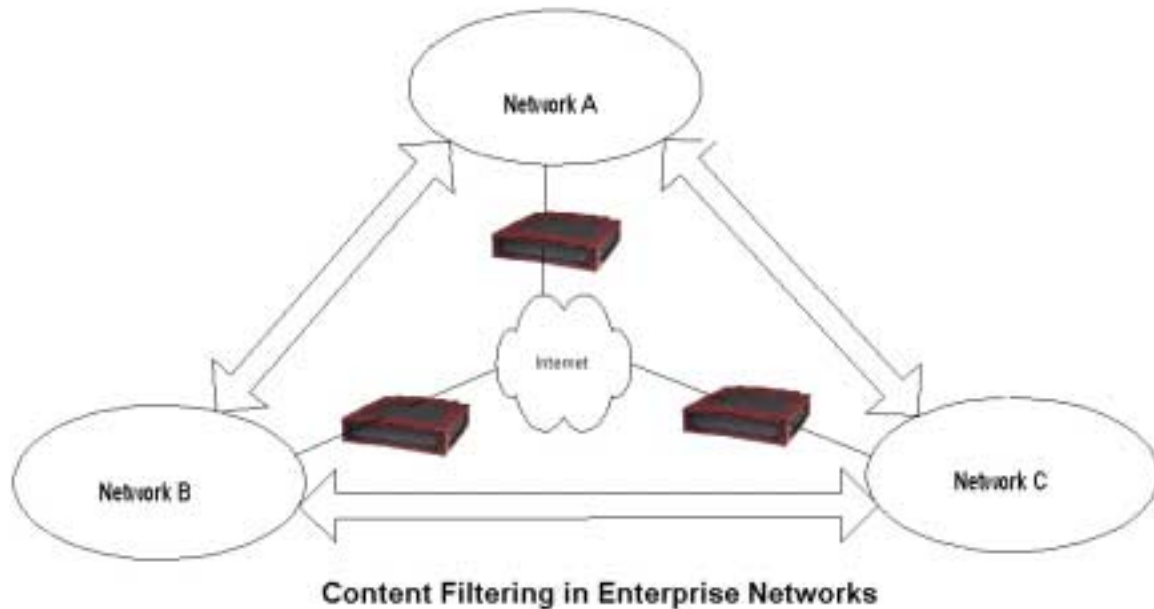


The above diagram shows:

- High speed DSL connection with fixed IP address obtained from the ISP.
- Ethernet 2 port configured as a WAN connection to the Internet.
- Ethernet 1 port configured as LAN connection for multiple PCs connected through the hub or switch. LAN port configured as DHCP or static IP addresses.
- Firewall and NAT/NAPT service activated for security.
- Exported or Public services such as HTTP and FTP are hosted on the LAN servers. These services are mapped to the public IP addresses through the NAT service.
- InterJak Content Filtering activated on the InterJak for filtering the traffic going through the InterJak to the Internet.

Large Enterprise Networks

The following diagram shows a large enterprise network where multiple networks interconnected with trust relationships. Since enterprise networks are made up of small networks similar to the small to medium size networks, InterJak can be implemented at different locations to perform important functions inside the networks.



The above diagram shows:

- Three networks are connected to each other with trust relationships to authenticate users, share resources etc.
- InterJak is used at different locations of the network to access Internet.
- Content Filtering and other important services can be implemented according to the security and network requirements.

InterJak Content Filtering Specifications

- Filanet Update Server: filters.filanet.com
- Filanet Update Filename: FILTER.V1 (All capital letters)
- Configurable Profiles (Filters): 8
- Filtering Configuration by: Time of Day, Profiles and LAN IP addresses
- Automatic Database download using: TFTP server
- Content Filtering Database: Generated from CyberLists provided by SurfControl, including

CyberNOT – depicting Nudity & other offensive sites

CyberYES – considered appropriate for children

Sports & Entertainment – Not appropriate during normal work time

HotNOT – Daily updates merged weekly into CyberNOT List

- Consolidated hardware and software solution
- Consolidated with Dynamic Stateful InterJak Firewall
- Blocks prohibited websites including sites with multiple IP addresses
- Lists are stored in the RAM of InterJak
- Lists automatically updates during InterJak power on
- Number of users accessing Internet: Unlimited, however limited by bandwidth & blocks
- Number of users using NNTP: 25

InterJak Setup Check List

- Make sure to activate the Content Filtering service by using the service Key
- Make sure the WAN IP address and Gateway are configured so that LAN PCs can access the Internet
- If InterJak is behind a firewall make sure the proper ports are open for InterJak to download the latest database using TFTP
- Make sure the Content Filtering service is enabled and the latest database is downloaded. It may take up to 5-10 minutes depending upon the WAN bandwidth. Refresh the screen to see the applicable Profile for that time period.
- Configure Filter Profiles, Filter schedules and PCs on the LAN for the required implementation.
- Every time the InterJak powers on it downloads the latest database.