Content Filtering

Feature Guide

Content Filtering

SSFG20160701-01

Global
Technology
Associates, Inc.

Global Technology Associates
3361 Rouse Rd, Suite 240
Orlando, FL 32817

Tel: +1.407.380.0220
Fax. +1.407.380.6080
Email: info@gta.com
Web: www.gta.com

Table of Contents

Introduction

About GTA’s Content Filtering

GTA’s Internet access management features basic content filtering and a web filtering subscription service for GTA Firewall UTM Appliances. Combined, they offer a complete and accurate solution that meets the requirements and demands of both users and technology providers.

GTA’s Content Filtering features one of the largest databases of categorized URLs, that combines blocking, monitoring and policy management in a centrally managed, out-sourced solution. When used in conjunction with GB-OS’ reporting features, real-time Internet usage reports are available from current and historical firewall log data.

GTA’s subscription service, Web Filtering, provides URL filtering via access to a database of over 100 million categorized URLs into over 65 categories. Categories are updated on a daily basis.

Content Filtering vs. Web Filtering

Content Filtering is the general feature as a whole. The Content Filtering feature includes the Content Filtering Proxy and basic Content Filtering Policies.

Web Filtering is a subscription-based service that may be purchased as an add-on to the entire Content Filtering feature. The Web Filtering subscription allows for specific URL filtering via categories.

Features

- Web Filtering with over 65 content categories for access control.
- Customizable local allow and local deny address objects.
- Over 100 million categorized URLs.
- Easy administration and enforcement of acceptable use policies.
- Economical deployment.
- No additional hardware required.
- Reports available through the GB-OS web interface

Requirements

- GB-OS version 5.0.6 and above.
- Web browser and Internet connection.
- GTA Firewall UTM Appliance or GB-Ware product registration.
- Subscription and feature activation code for Web Filtering.

Registration & Activation

If you have not yet registered your firewall products, go to the GTA Online Support Center (https://www.gta.com/support/center/login/). In the login screen, enter your user ID and password. Click the **Register Product** link and enter your product serial numbers and firewall activation (unlock) codes, then click **Submit**.

If you do not already have a GTA Online Support Center account, click the **Create an Account Now!** link on the GTA Online Support Center login screen.

Feature Activation Codes

Optional features for GB-OS require activation codes. Web Filtering activation can be automated or entered manually through the GB-OS Web interface.

The feature activation code can be found in **View Your Registered Products** on the GTA Online Support Center, by selecting the serial number of your GTA Firewall UTM Appliance. The activation code is also accessible through the GB-OS Web interface by navigating to **Configure>Configuration>Runtime> Update**. If no updates display, click on **Check Now**. All available feature codes and runtime updates will display.

Note

If the feature activation code does not appear in your GTA Online Support Center account, please contact GTA Support, including your serial number and Support Center User ID in the message subject.

About this Guide

This feature guide is a supplement to the *GB-OS User's Guide*. It illustrates the activation and use of the Content Filtering subscription service for GB-OS 5.0.6 and above.

Conventions

A few conventions are used in this guide to help you recognize specific elements of the text. If you are viewing this guide in PDF format, color variations may also be used to emphasize notes, warnings and new sections.

Bold Italics	Emphasis
Italics	Publications
Blue Underline	Clickable hyperlink (email address, Web site or in-PDF link)
Small Caps	On-screen field names
`Monospace Font`	On-screen text
Condensed Bold	On-screen menus, menu items
BOLD SMALL CAPS	On-screen buttons, links

Managing Internet Access

GTA's Internet access management solutions provide the ability to control Web access based on site content. GB-OS has three primary functions for access control: Content Filtering proxy settings, Content Filtering policies with URL categorization via Web Filtering, and local allow/deny lists. In addition, records of blocked sites can be created and sent to GTA firewall logs.

Content Filtering Proxy

When enabled, the Content Filtering proxy can either be configured to operate using a traditional or transparent proxy for HTTP (Web) requests.

The transparent proxy is the more common method for implementing a HTTP proxy. It is easy to implement, especially if the Content Filtering service is being configured to manage Internet access for a large network.

The traditional proxy is used primarily for systems which were put in place prior to the introduction of transparent proxy methods or for systems that require more control by directing Web request through a specific port.

Content Filtering Policies

Content Filtering policies provide a means to select Web access control facilities and specify how they will be applied to Web page requests. With every Web page request, GB-OS must choose to either accept or deny transmission. Content Filtering policies contain the criteria that cause a Web page to be accepted or denied and define any scripts or applets that should be blocked. Specific URL categorization is provided via the Web Filtering option.

By default, the Content Filtering service denies all Web page requests. This default will be enacted if a Web page request does not meet any listed policy. To ensure that all Web page requests are not rejected by default, at least one policy of type accept must be in place.

Local Allow and Local Deny Lists

Local allow and local deny lists, configured using address objects and used in conjunction with Content Filtering policies, allow the administrator to customize content filtering. Local allow and local deny lists take precedence over the Content Filtering category listings, so you can allow access to specific sites in categories that have been blocked or deny access to sites in categories that are otherwise allowed. This is particularly useful for companies whose policies allow access only to a few specific sites, or for those with policies which allow Web requests for a category, but deny specific sites within that category.

Remote Logging

Both Content Filtering proxy and policy entries are logged by GB-OS. Two examples, one of a accept (pass) and one of a deny (block) log message, are illustrated below.

Note

To learn more about log messages, see the *GB-OS User’s Guide*.

```
May 15 18:37:16 pri=5 msg=”Accept persistent outbound, NAT” cat _
action=pass cat _ site=”Sports” dstname=www.cmdarts.com proto=80/
tcp src=192.068.71.199 srcport=3817 nat=24.227.126.130 natport=3817
dst=64.34.176.47 dstport=80 rule=11 duration=6 sent=1205 rcvd=12709
pkts _ sent=11 pkts _ rcvd=12 op=GET arg=/images/newlogo.gif
```

Figure 1.1: *Content Filtering Persistent Connection Message*

```
May 15 18:39:03 pri=5 msg=”Accept outbound, NAT” cat _ action=pass
cat _ site=”News and Media” dstname=technology.timesonline.co.uk
proto=80/tcp src=192.068.71.199 srcport=2452 nat=24.227.126.130
natport=2452 dst=72.247.134.216 dstport=80 rule=11 duration=327 sent=260
rcvd=636 pkts _ sent=5 pkts _ rcvd=3 op=GET arg=/tol/img/global/chevron-
back-to-top.gif
```

Figure 1.2: *Content Filtering Proxy Accept Message*

```
May 15 18:39:27 pri=4 msg=”Block outbound, NAT” cat _ action=block
cat _ site=”Adult and Pornography” dstname=www.playboy.com proto=80/
tcp src=192.068.71.199 srcport=3827 nat=24.227.126.130 natport=3827
dst=216.163.137.3 dstport=80 rule=11 duration=22 sent=486 rcvd=48 pkts _
sent=3 pkts _ rcvd=1 op=GET arg=/favicon.ico
```

Figure 1.3: *Content Filtering Proxy Deny Message*

Table 1: Content Filtering Logging Fields

Field	Description
pri	Priority of log message.
msg	Message indication Accept or Block.
cat_action	Action taken.
cat_site	Content Filtering category, Local Accept or Local Deny.
dstname	Web site accepted or blocked by this action.
proto	Protocol (HTTP).
src	Source IP address of the Web request.
srcport	Port through which the Web request was made.
op	Operation requested.

Log messages are in WELF, the default log format.

Internet Access Policy

The Internet changes constantly and GTA's Content Filtering service can help you respond quickly to new and changing sites, restricting user access only to material that is consistent with your access policy.

Restricting Internet access can protect a company from bandwidth abuse, potential legal liability and lost productivity. For example, schools and libraries can set their Content Filtering policies to prevent access to Web sites that may not be appropriate for the workstation user's age.

When Content Filtering has been configured and the Web Filtering service is enabled, the content filtering engine compares a requested page to its database of categorized URLs at one of several GTA server sites, then allows or denies the request based on the policies created in accordance with your company's Internet access policy. This rating and review process includes not only the sites that a user explicitly requests by clicking on a link or typing a URL, but also protects users from material blocked as inappropriate on pages called up inadvertently (e.g., pop-up windows) when accessing sites. Blocked pop-up windows and graphics will display the firewall's content blocking message.

Steps to Implementation

Content filtering can be implemented as part of a complete Internet Access/Acceptable Use Policy. Prior to implementing the Content Filtering service, GTA suggests completing the following steps:

1. Develop an Internet Access Policy and create acceptable user guidelines.
2. Create address objects and/or user groups in GB-OS to define the various users and groups whose access you will be controlling using Content Filtering.
3. Create Content Filtering policies on your GTA firewall for the users and groups defined in the previous step, and choose which Web Filtering categories will be accepted and which will be denied.
4. Customize your content filtering further, if desired, by adding any specific pages or sites you wish to allow or deny to the local allow or local deny lists.
5. Turn on content filtering by selecting the Content Filtering proxy method.

Using GTA's Content Filtering & Web Filtering Option

This chapter describes configuration of Content Filtering and the activation and configuration of the Web Filtering subscription. Instructions in this chapter assume a prior working knowledge of common GB-OS configuration tasks and settings. For detailed instructions on the operation and configuration of GB-OS, see the *GB-OS User's Guide*.

Web Filtering Activation

Web Filtering is a subscription option providing additional URL filtering through defined categories. Web Filtering can only be activated after your GTA Firewall UTM Appliance or copy of GB-Ware has been registered through the GTA Online Support Center.

Note

Activating the Web Filtering service will require the firewall to reboot.

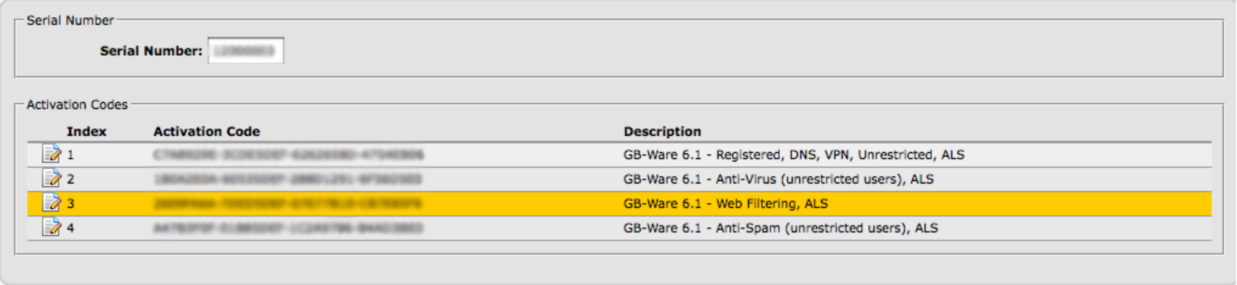
Automatic Activation

The Web Filtering service can be automatically activated through the GB-OS Web interface. Navigate to **Configure>Configuration>Runtime>Update**. If no updates display, click on **Check Now**. All available feature codes and runtime updates will display. Click on **Update** and the Web Filtering service will be automatically activated.

Manual Activation

To manually activate the Web Filtering service, retrieve the feature activation code by logging into the GTA Online Support Center and navigate to **View Your Registered Products.** Select the serial number of your GTA Firewall UTM Appliance to display the activation code.

Next, login to GB-OS and navigate to **Configure>System>Activation Codes**. Click the **New** icon to enter the feature activation code in the next available line. **Save** the section. When an activation code is entered correctly, the Description field will indicate "GB-*X*–Web Filtering", where *X* is your firewall product and version number.



Serial Number

Serial Number: [redacted]

Activation Codes

Index	Activation Code	Description
1	[redacted]	GB-Ware 6.1 - Registered, DNS, VPN, Unrestricted, ALS
2	[redacted]	GB-Ware 6.1 - Anti-Virus (unrestricted users), ALS
3	[redacted]	GB-Ware 6.1 - Web Filtering, ALS
4	[redacted]	GB-Ware 6.1 - Anti-Spam (unrestricted users), ALS

Figure 1: *Web Filtering - Activated*

Configuration

The steps for configuring Web Filtering must be done in order to ensure continuous Internet access for users. If Content Filtering is already in use, some of these steps will have already been completed.

To configure Web Filtering:

1. Define a DNS server (**Configure>Services>DNS**) to access your selected list server. (See the *GB-OS User's Guide* for more about defining a DNS server.)
2. Create and enable Content Filtering policies.
3. Add Local Allow and Deny lists (if desired).
4. Enable the Transparent Proxy.
5. And/or enable the Traditional Proxy.

Note

Before Web Filtering can be configured, a valid feature activation code must be entered.

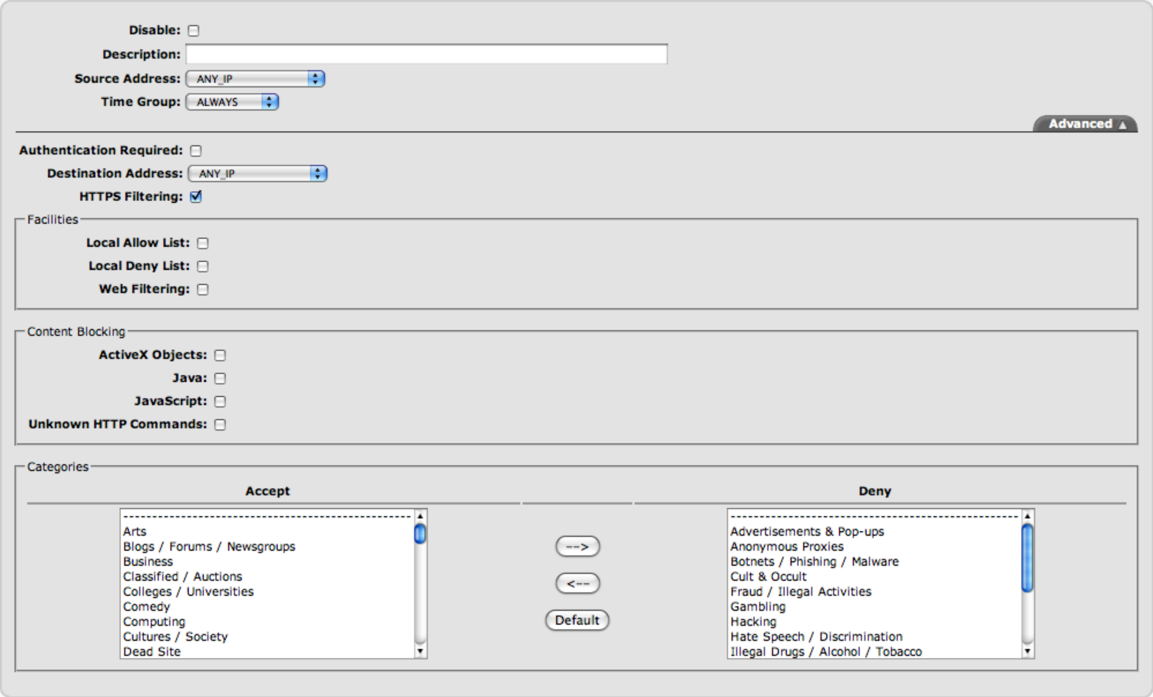
Configuring Content Filtering Policies

Content Filtering policies provide a means to select Web access control facilities and specify how they will be applied to Web requests. Each policy consists of a description, an address object representing the source of the Web request, the ability to specify content blocking preferences for the individual policy, and (with a valid subscription), content filtering category lists.

Like security policies, the order of Content Filtering policies is important. Each Web request is compared to the list, starting at Content Filtering policy index #1. The packet is compared sequentially against each policy until one of two events occur:

1. A Content Filtering policy is matched. The Web request is either allowed or blocked based on the policy's definition.
2. No Content Filtering policies are matched and the list is exhausted. In this case, the Web request is rejected.

To configure Content Filtering policies, navigate to **Configure>Threat Management>Content Filtering>Policies**. Click the **New** icon to define a new policy.



Disable: □
Description:
Source Address: ANY_IP
Time Group: ALWAYS

Authentication Required: □
Destination Address: ANY_IP
HTTPS Filtering: ☑

Facilities
Local Allow List: □
Local Deny List: □
Web Filtering: □

Content Blocking
ActiveX Objects: □
Java: □
JavaScript: □
Unknown HTTP Commands: □

Categories

Accept:
Arts
Blogs / Forums / Newsgroups
Business
Classified / Auctions
Colleges / Universities
Comedy
Computing
Cultures / Society
Dead Site

Deny:
Advertisements & Pop-ups
Anonymous Proxies
Botnets / Phishing / Malware
Cult & Occult
Fraud / Illegal Activities
Gambling
Hacking
Hate Speech / Discrimination
Illegal Drugs / Alcohol / Tobacco

Figure 2: *Configuring a Content Filtering Policy*

Table 2: Configuring a Content Filtering Policy

Field	Description
Disable	Disables the policy.
Description	A description for the policy.
Source Address	If a request matches an element of the specified address object of type Content Filtering, the packet will be compared to the policy.
Time Group	Select a user-defined time group in which the policy will be enabled. Time groups are defined at **Configure>System>Objects>Time Groups.**
Advanced	
Authentication Required	Enable to require users to authenticate with the GTA firewall using GBAuth. When enabled, a pull down will appear with configured user groups that will have the policy applied to them.
Destination Address	A selection of address objects that are of type All or Content Filtering. Select **<USER DEFINED>** to manually enter a destination address.
HTTPS Filtering	Enable to allow filtering of HTTPS protocols.
Content Filtering Facilities	
Local Allow List	Enable to use the firewall's local allow list by selecting its address object.
Local Deny List	Enable to use the firewall's local deny list by selecting its address object.
Web Filtering	Enable to use the Web Filtering Categories list.
Content Blocking	
ActiveX Objects	Enable to block ActiveX controls.
Java	Enable to block Java applets.
JavaScript	Enable to block JavaScript.
Unknown HTTP Commands	Enable to block unknown HTTP commands and unencrypted HTTP protocols.
Categories	
Accept / Deny	Specify allowed or blocked Web Filtering categories. Switch a category from one list to the other by selecting the item and clicking the left or right arrow button. Web Filtering must be activated and enabled to configure URL categories.

Content Filtering Facilities

The Content Filtering Facilities box contains selections for the local allow and local deny lists as well as the toggle to enable the use of Web Filtering subscription option.

Available selections from the Local Allow List and Local Deny List are all defined address objects defined in the Objects that are of type All or Content Filtering. See Local Allow/Deny Lists for more information.

Content Blocking

Portable code blocking for ActiveX objects, Java, JavaScript and unknown HTTP commands can protect your network from malicious programs such as viruses spread by Web pages (applets or scripts appear in inbound TCP ports 80, 8000 and 8080). In addition to blocking mobile programs embedded in Web pages, Content Blocking can also prevent tunneled, unencrypted non-HTTP connections over standard HTTP ports.

Web Filtering Categories

The Web Filtering service has a default set of Accept and Deny categories. Move these categories from one list to another to reflect your Internet access policy using the arrow buttons (**-->**, **<--**). For example, if you wish to deny access to Web sites that would fall under the `Sports` category, select that category in the Accept field (its default location) and click the **-->** button to move the `Sports` category to the Deny field. Categories can be reset to installation defaults at any time by selecting the **Default** button.

In order to make use of Web Filtering categories, the Web Filtering checkbox in the Content Filtering Facilities box must be enabled and Web Filtering must be activated.

Note

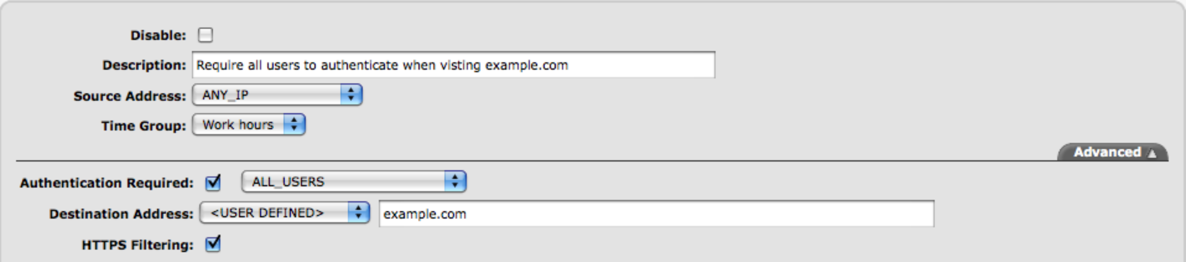
See Reference A: Categories for more information on Web Filtering default categories.

Local Allow/Deny Lists take precedence over the Web Filtering categories, and will ignore settings configured in this section of the Content Filtering policy.

Advanced Content Filtering Policy Settings

In addition to allowing or blocking by category via Web Filtering, Content Filtering policies can require user groups to authenticate with the firewall using GBAuth or Single Sign-On authentication as well as control Internet access based on the destination address. Restricting access by destination address is useful if the administrator wishes to block content on a certain Web site, such as ActiveX objects. Regular expression can also be used when defining the policy's Destination Address.

Advanced settings for Content Filtering policies are configured in **Configure>Threat Management>Content Filtering>Policies** under the **Advanced** tab.



Disable: ☐

Description: Require all users to authenticate when visting example.com

Source Address: ANY_IP

Time Group: Work hours

Authentication Required: ☑ ALL_USERS

Destination Address: <USER DEFINED> example.com

HTTPS Filtering: ☑

Figure 3: *Advanced Content Filtering Policies*

Table 3: Advanced Content Filtering Policies

Field	Description
Authentication Required	Enable to require users to authenticate with the GTA firewall using GBAuth or Single Sign-On authentication. When enabled, a pull down will appear with configured user groups that will have the policy applied to them.
Destination Address	A selection of address objects that are of type All or Content Filtering. Select **<USER DEFINED>** to manually enter a destination address.
HTTPS Filtering	Enable to allow filtering of HTTPS protocols.

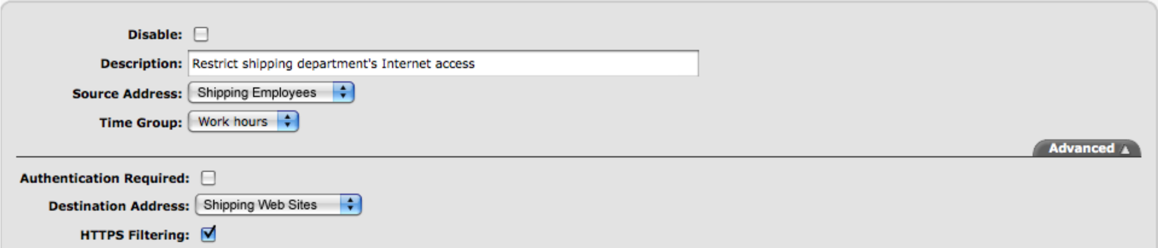
Example Policy Settings

Example Content Filtering policy configurations assume that the Content Filtering proxy has been enabled.

Example 1: Restricting Access to Specific Destinations

A company with a shipping department would like to restrict their shipping employees' Internet access to shipping related sites (FedEx, UPS, DHL, etc.) during work hours. To do so, two address objects of type All or Content Filtering and a time group must be defined:

1. An address object, named Shipping Employees, containing the IP addresses of all employees belonging to the shipping department.
2. The time group, Work hours, is selected for the time periods in which this policy is applied.
3. An address object, named Shipping Web Sites, containing all Web sites that the shipping employees will be granted access to. (In this example, fedex.com, ups.com and dhl.com.)
4. Once all necessary address objects have been defined, navigate to **Configure**>**Threat Management**>**Content Filtering**>**Policies** and click the **New** icon to define the policy that will be restricting the shipping department's Internet access.



Disable: □
Description: Restrict shipping department's Internet access
Source Address: Shipping Employees
Time Group: Work hours

Authentication Required: □
Destination Address: Shipping Web Sites
HTTPS Filtering: ☑

Figure 4: *Restricting Access to Specific Destinations*

5. When defining the Content Filtering policy, select the <**Shipping Employees**> address object for the policy's Source Address.
6. Select <**Work hours**> for the policy's Time Group.
7. Under the Advanced tab, select the <**Shipping Web Sites**> address object for the policy's Destination Address.
8. Click **Ok** and then **Save**. From now on, all IP addresses listed in the Shipping Employees address object will be restricted to Web sites listed in the Shipping Web Sites address object. All other Internet requests will be met with the Content Filtering proxy's configured Block Action.

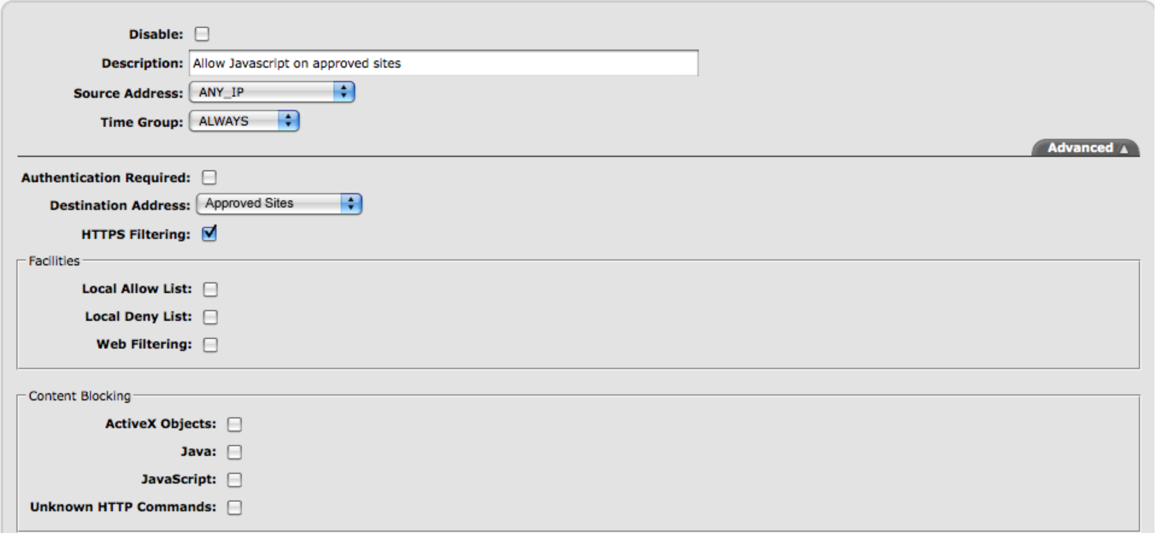
Example 2: Blocking Content from Specific Web sites

A company would like to disable JavaScript from running on all Web sites except for those they explicitly allow. By using Content Filtering, JavaScript and other potentially malicious content can be removed from Web sites, transparently to end users. To do so, two Content Filtering policies need to be defined:

1. A policy that allows JavaScript to run only on approved Web sites.
2. A policy that blocks JavaScript from running on all other Web sites.

Creating the First Content Filtering Policy

1. Before the first Content Filtering policy can be created, an address object of type All or Content Filtering named Approved Sites that contains all approved Web sites must be defined.
2. Once the address object has been defined, navigate to **Configure>Threat Management>Content Filtering>Policies** and click the **New** icon to define the policy that will allow JavaScript to be run on the desired Web sites.



Disable: □
Description: Allow Javascript on approved sites
Source Address: ANY_IP
Time Group: ALWAYS

Authentication Required: □
Destination Address: Approved Sites
HTTPS Filtering: ☑

Facilities
Local Allow List: □
Local Deny List: □
Web Filtering: □

Content Blocking
ActiveX Objects: □
Java: □
JavaScript: □
Unknown HTTP Commands: □

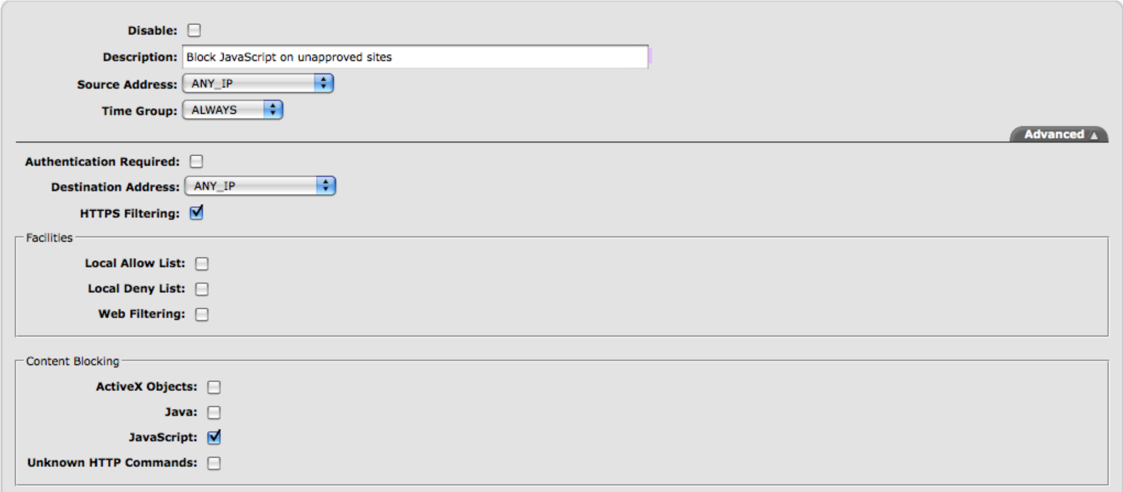
***Figure 5:** Allowing JavaScript to be Run on Specific Web sites*

3. When defining the Content Filtering policy, select **<ANY IP>** for the policy's Source Address.
4. Under the **Advanced** tab, select the **<Approved Sites>** address object for the policy's Destination Address.
5. In the Content Blocking box, ensure the JavaScript option is unchecked.
6. Click **OK** and then **Save**. You have now created the Content Filtering policy that will allow all IP addresses trying to access Web sites listed in the Approved Sites address object to view those Web sites with JavaScript intact.

Next, you must create a Content Filtering policy that will block all other Web sites from running JavaScript.

Creating the Second Content Filtering Policy

1. Click the **New** icon in the Content Filtering policy list to define the second policy.
2. Select <**ANY IP**> for the policy's Source Address.
3. Under the **Advanced** tab, ensure that <**ANY IP** > is selected for the policy's Destination Address.
4. Under the Content Blocking box, check the JavaScript option.



Disable:	□
Description:	Block JavaScript on unapproved sites
Source Address:	ANY_IP
Time Group:	ALWAYS

Authentication Required:	□
Destination Address:	ANY_IP
HTTPS Filtering:	☑

Facilities

Local Allow List:	□
Local Deny List:	□
Web Filtering:	□

Content Blocking

ActiveX Objects:	□
Java:	□
JavaScript:	☑
Unknown HTTP Commands:	□

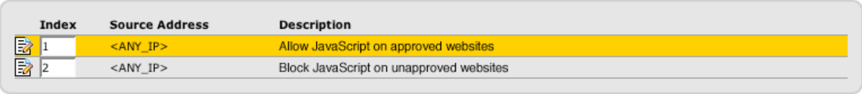
***Figure 6:** Blocking JavaScript on All Other Web sites*

5. Click **OK** and then **Save**. You have now created the Content Filtering policy that will block JavaScript from running on all other Web sites.

Next, you must configure the Content Filtering policy list's order so that the first policy will match before the policy you just created.

Sorting the Content Filtering Policy List

Once the policies have been configured and saved, verify that the first policy (which allows JavaScript on approved Web sites) is placed above the second policy (that blocks JavaScript on all other Web sites). If the order is reversed, the deny policy will match before the allow policy, resulting in JavaScript being stripped from all Web sites, regardless if they are in the Approved Sites address object or not.



Index	Source Address	Description
1	<ANY_IP>	Allow JavaScript on approved websites
2	<ANY_IP>	Block JavaScript on unapproved websites

***Figure 7:** Sorting the Content Filtering Policy List*

Local Allow/Deny Lists

Local allow and deny lists allow customization of content filtering using address objects. You can choose to execute all content filtering locally, allow access to sites that are disallowed by another content filtering facility or deny access to sites that are otherwise allowed.

To add domain names to the local allow and deny lists:

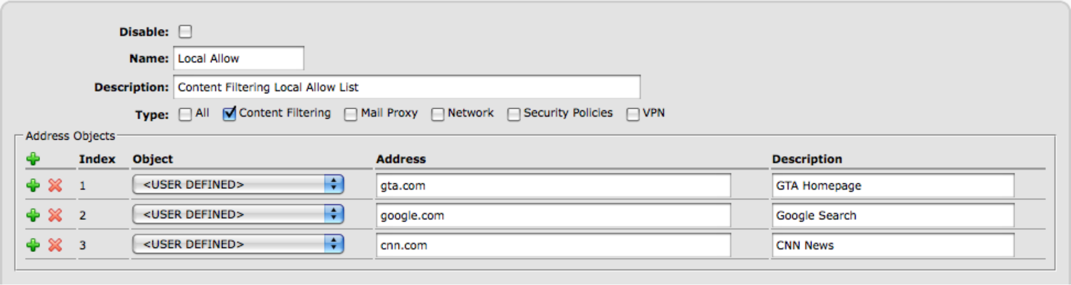
1. Navigate to **Configure>Objects>Address Objects**.
2. Select the local list you wish to edit.
3. In the Address field, enter the desired domain name and an optional description. For additional domain names, enter their value in the row below.
4. Click **OK** and then **Save**.

Enter domain names in the following format: `example.com.` WWW and other such subdomain prefixes (www2, www3) limit the effectiveness of the local allow or deny lists. For example, the value `www.example.com` only accepts or denies access for the specific site only, not to sites such as `www2.example.com` or `subdomain.example.com`. If you wish to block an entire domain and all of its subdomains, enter `example.com`.

Additionally, you may use regular expression to create more elaborate local allow and deny lists. See the *GB-OS User's Guide* for more information.

CAUTION

Using regular expression in Content Filtering policy definitions may result in an unexpected policy match.



Disable: □

Name: Local Allow

Description: Content Filtering Local Allow List

Type: □ All ☑ Content Filtering □ Mail Proxy □ Network □ Security Policies □ VPN

Address Objects

Index	Object	Address	Description
1	<USER DEFINED>	gta.com	GTA Homepage
2	<USER DEFINED>	google.com	Google Search
3	<USER DEFINED>	cnn.com	CNN News

Figure 8: *Defining Local Allow/Deny Lists*

Content Filtering Proxy

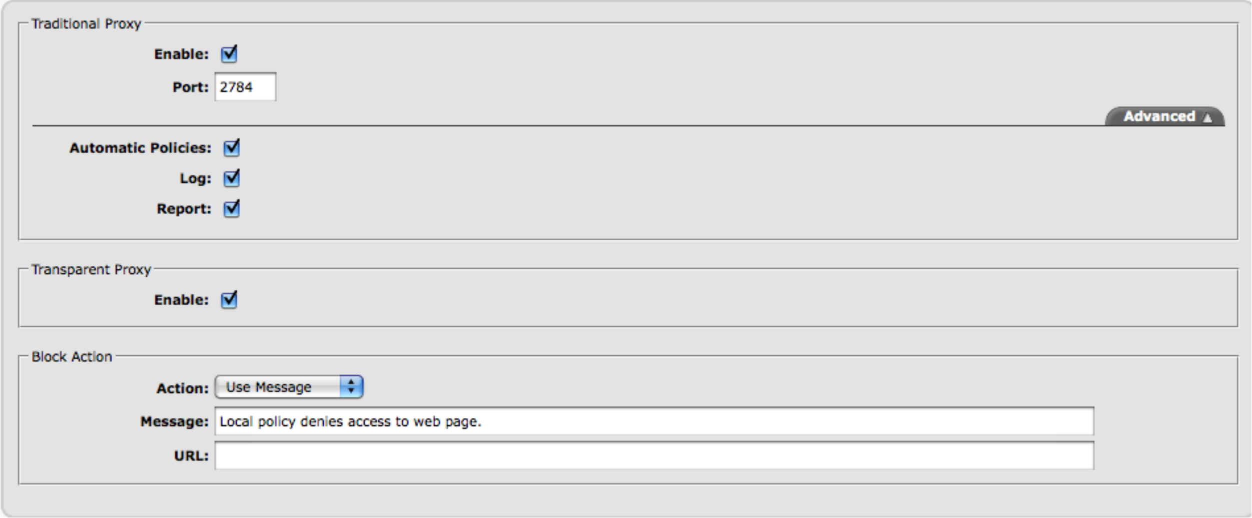
Content Filtering on a GTA firewall requires the configuration of the Content Filtering proxy. The Content Filtering proxy allows Internet requests to be managed by tunneling all requests through the proxy, where content can be filtered (as defined by Content Filtering policies).

CAUTION

Content Filtering policies must be created before enabling the Content Filtering proxy. Enabling the proxy before creating policies will block all HTTP Internet access.

Using the transparent proxy, IP addresses that are not explicitly allowed access in Content Filtering policies will be able to use TCP port 80 (the port used for Internet access). If only the traditional proxy is used, only users with browsers configured to use the traditional proxy will be affected, all other users will not have their Internet access filtered.

The Content Filtering proxy screen allows the firewall administrator to specify the use of the transparent proxy, the traditional proxy or both. Additional settings include the selection of a block message or URL redirect when an Internet request has been denied.



Traditional Proxy

Enable: ☑

Port: 2784

Automatic Policies: ☑

Log: ☑

Report: ☑

Transparent Proxy

Enable: ☑

Block Action

Action: Use Message

Message: Local policy denies access to web page.

URL:

***Figure 9:** Configuring the Content Filtering Proxy*

Table 4: Configuring the Content Filtering Proxy

Field	Description
Traditional Proxy	
Enable	Enables the traditional proxy.
Port	The port through which the proxy will run. Default is 2784.
Advanced	
Automatic Policies	A toggle for whether the firewall should automatically generate the required policies for the Content Filtering proxy to function. If unselected, it is necessary to define remote access policies. View at **Monitor>Activity>Security Policies.**
Log	Enables Content Filtering logging.
Report	Enables saving of Content Filtering data for Reports.
Transparent Proxy	
Enable	Enables the transparent proxy.

Block Action	
Action	A selection for the action to be performed when a request for blocked content is performed.
Message	If **<Use message>** is selected for the Action, the entered message will be displayed. Default is `Local policy denies access to Web page.`
URL	If **<Redirect to URL>** is selected for the Action, the user will be directed to the entered URL.

Enabling the Traditional Proxy

When the firewall is operating without the Content Filtering service enabled, it does not use a proxy. When the HTTP proxy is used in conjunction with a Web filtering facility, it runs on TCP port 2784 by default. To run the HTTP proxy on a different port, enter the desired port number in the Port field. The traditional proxy requires users located on protected networks to have browsers configured to use a proxy connection with the proxy IP address and port number. Only users specifying the traditional proxy port will use Web filtering for their traffic.

If the Automatic Policies toggle located under the **Advanced** tab has been disabled, a remote access policy that allows connection to the entered Port value from the protected network must be configured and enabled. Because of this, GTA recommends leaving the Automatic Policies toggle enabled to simplify configuration.

Transparent Proxy

The transparent proxy is the most common method of implementing an HTTP proxy because it is easier to implement than a traditional proxy, especially when a network is large and widespread. This method is invisible to users located on the protected network. No modification to their browsers settings is required, and there is no Port field. As the name implies, the transparent proxy allows the firewall to filter and mediate HTTP traffic transparently to end users.

Using Both Proxy Types

If some hosts are already using the traditional proxy and have a proxy port set, or the administrator wants to direct some users' Internet requests through a specific port in order to increase control, the traditional and transparent proxy may be enabled simultaneously.

With both types of proxy enabled, users without a proxy port set in their browser will use the transparent proxy while users with the proxy port defined will make use of the traditional proxy.

Block Actions

If a policy blocks a Web address (URL) and a user attempts to load a page from that address, the user will see a custom message, or be redirected to a URL (e.g., an internal Web site that defines the company's Internet policies and the administrative process to gain access to a blocked Web site).

Note

If your Content Filtering policies are configured to use local allow/deny lists, and your block action redirect is to a URL, make sure the URL is defined in your local allow list. Block actions on SSL will not display a block message.

Licensing

If the number of hosts using the Web Filtering service exceeds the number of licenses purchased, the next host attempting to access the Internet will be blocked. A message will be displayed in their Web browser and a “license exceeded” log message will be generated by the firewall.

User licenses are reserved for ten minutes. When a user has been inactive for ten minutes, the license will be released for use by another host. Contact the GTA sales staff or an authorized GTA channel partner for information on upgrading Web Filtering Service licenses for additional users.

Expired Licenses

If the Web Filtering service license has expired, a message will be displayed in the Web browser and a “License expired” log message will be generated by the firewall. A verification warning that the license has expired will also display in the GB-OS Web interface.

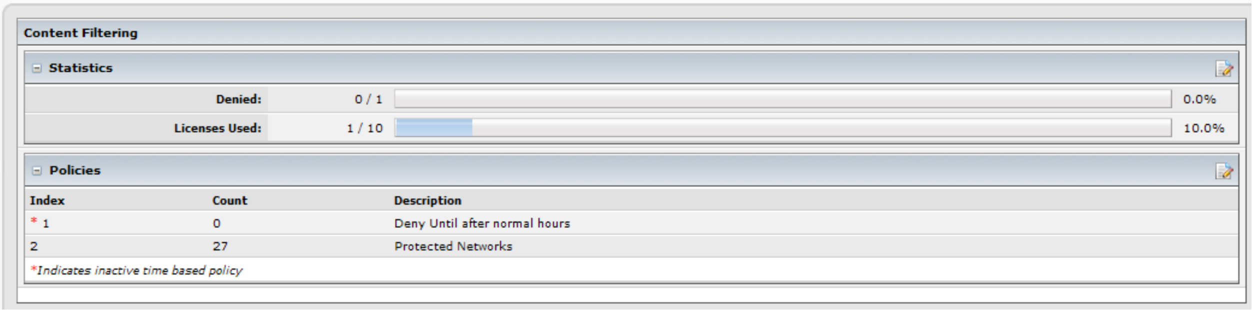
```
May 24 07:58:16 pri=4 msg=”Block outbound, NAT” cat _ action=block cat _
site=”License expired” dstname=l.yimg.com proto=80/tcp src=192.068.172.4
srcport=63652 nat=69.244.247.28 natport=63652 dst=209.73.188.78 dstport=80
rule=2 duration=22 sent=530 rcvd=44 pkts _ sent=3 pkts _ rcvd=1 op=GET
arg=/a/i/ww/thm/1/grd-1px _ 1.4.gif
```

Figure 10: *Web Filtering Service License Expired Log Message*

Viewing Activity

Content Filtering can be viewed by navigating to **Monitor>Activity>Threat Management>Content Filtering**. Information displayed includes:

- Statistics:
  - Count and percent denied
  - Licenses currently in use
- Policies:
  - Policy count and description



Content Filtering

⊟ Statistics

Denied:	0 / 1	0.0%
Licenses Used:	1 / 10	10.0%

⊟ Policies

Index	Count	Description
* 1	0	Deny Until after normal hours
2	27	Protected Networks

**Indicates inactive time based policy*

Figure 11: *Content Filtering Statistics*

Graphs and Reports

Graphical data is available for Web Filtering at **Monitor>Reporting>Graphs>Web Filtering**. Hourly, Daily, Weekly, Monthly and Yearly reports are available displaying web filtering, categorized and licenses used over time.

Web Filtering reports are available through the firewall at **Monitor>Reporting**. The number of Top reports is based upon the firewall product and available memory.

For more information on scheduling reports, running reports, and report preferences, see the *GB-OS User's Guide* section on Reporting in the Monitoring and Tools chapter.

The following reports are available:

- Web Filtering - Allowed - Domains
  - By Connection
  - By Traffic
  - By Duration
- Web Filtering - Allowed - Categories
  - By Connection
  - By Traffic
  - By Duration
- Web Filtering - Denied
  - Domains
  - Connections

Reference A: Categories

GTA's Web Filtering subscription contains over 65 categories for the administrator to use when customizing Content Filtering policies. A special category for Web sites that do not fit neatly into a category and for requests that do not return a rating is UNCATEGORIZED.

CAUTION

GTA recommends reviewing default category settings and modifying them to match your corporate Internet Access Policy.

Note

The Web Filtering categories have changed with the release of GB-OS 6.1.3. For complete category mapping from GB-OS 6.1.2 and below to GB-OS 6.1.3 and above, please see Reference B: Category Mapping.

Denied by Default

Categories denied by default are as follows:

Table A.1: Default Denied Categories

Category	Description
Advertisements & Pop-ups	Online advertisements or banners.
Alcohol	Alcohol manufacturer's commercial web sites and food/drink magazines and reviews or wine advisors.
Anonymous Proxies	Remote proxies or anonymous surfing. Sites for peer-to-peer sharing. Sites providing information on how to bypass proxy server features or gain access to URLs in any way that bypasses the URL filter or proxy server.
Botnets / Phishing / Malware	Phishing, pharming, and other sites that pose as a reputable site, usually to harvest personal information from a user. Sites that carry malicious content including executables, scripts, or viruses. Sites associated with Spyware or Adware.
Cult & Occult	Sites that promote or offer methods, means of instruction, or other resources to affect or influence real events through the use of spells, curses, magic powers, satanic or supernatural beings. Includes sites containing alternative religions such as Wicca or witchcraft.
Fraud / Illegal Activities	Sites that advocate, instruct, or give advice on performing illegal acts such as phone, service theft, evading law enforcement, lock picking, fraud, plagiarism/cheating, and burglary techniques.
Gambling	Online gambling or lottery web sites, virtual casinos, offshore gambling ventures and virtual sports leagues and betting pools.
Hacking	Sites providing information on hacking, or illegal, or questionable access to or the use of communications equipment/software.
Hate Speech / Discrimination	Sites that advocate or incite degradation or attacks on specified populations or institutions based on associations such as religion, race, nationality, gender, age, disability, or sexual orientation.
Illegal Drugs Tobacco	Sites that provide discussion or remedies for illegal, illicit, or abused drugs such as heroin, cocaine, or other street drugs. Information on "legal highs": glue sniffing, misuse of prescription drugs or abuse of other legal substances. Does not include sites which discuss medicinal drug use or education information on drug use.
Intimate Apparel / Swimsuits	Sites that contain images or offer the sale of swimsuits or intimate apparel or other types of suggestive clothing.

Table A.1: Default Denied Categories

Category	Description
Link Farms / Click Fraud	Link farming in which any group of web sites hyperlink to every other site in the group. Click fraud where a person, automated script or computer program imitates a legitimate user of a web browser clicking on an ad.
Malformed / Invalid URLs	URL's with improper or invalid structure or protocol.
Nudity	Sites containing nude or semi nude depictions of the human body.
Sexual / Pornography	Sites that contain sexually explicit material including explicit sexual acts and obscured or implied sexual acts. Adult products including sex toys, CD-ROMs, and videos. Erotic stories and textual descriptions of sexual acts. Adult services including video conferences, escort services, and strip clubs. Sexually explicit cartoons and animation.
Suicide Promotion	Sites that advocate suicide or self-mutilation.
Tobacco	Tobacco manufacturer's commercial web sites.
Violence	Sites that advocate violence, depictions, and methods, including game/comic violence and suicide.
Vulgar / Obscene Language	Sites that contain explicit sexual language, crude words, profanity and mild expletives.
Weapons	Sites that sell, review, or describe weapons such as guns, knives or martial arts devices, or provide information on their use, accessories, or other modifications.

Allowed by Default

Categories allowed by default are as follows:

Table A.2: Default Allowed Categories

Category	Description
Arts	Online museums, galleries and artist sites including photography, architecture and crafts. Sites with comic books and newspaper comics.
Blogs / Forums / Newsgroups	Newsgroups, forums and chat rooms. Social networking sites. Personal web sites posted by individuals or groups, as well as blogs
Business	Sites devoted to business firms, business information, economics, marketing, business management and entrepreneurship. Includes corporate Web sites.
Classified / Auctions	Internet malls, classifieds and online auction sites.
Colleges / Universities	Official sites for colleges and universities.
Comedy	Any site designed to be funny or satirical. Sites containing comedy, jokes, movie, video or sound clips. Sites belonging or promoting comedians.
Computing	Computer, software and internet companies including industry news and magazines. Reviews, information and buyer's guides for computers, computer parts and accessories, and software.
Cultures / Society	Web sites that cover a variety of topics relevant to the general populace, such as broad issues that impact a variety of people, safety, societal issues, adoption, etc Sites with information on foreign cultures.
Dead Site	Sites that do not respond to http queries.
Domain for Sale	Sites explicitly stating the domain is for sale.
Education	Educational institutions including pre-elementary, elementary, secondary and high schools. Distance education and trade schools. Educational sites for students.

Table A.2: Default Allowed Categories

Category	Description
Entertainment	Online magazines and reviews on the entertainment industry. Celebrity fan sites. Sites relating to the publishing industry including book reviews and promotions and publishing houses. Theater information and city guides. Horoscope sites.
Fashion / Style	Fashion or glamour magazines and clothing catalogues. Modeling information and agencies including model fan pages, and fitness/sport models. Sites containing tattoos and body paint of non-sexual nature.
Food & Eating	Web sites for recipes, cooking instructions and tips. Sites selling food products and accessories. Official sites for restaurants and bars serving food.
Game Media / Game Playing	Journals and magazines dedicated to game playing. Sites containing tips, advice or cheat codes. Sites for game playing, downloading, or hosting.
Gay / Lesbian	Homelife and family-related topics, including parenting tips, gay/lesbian/bisexual advocacy or support sites.
Government / Politics	Federal and local government sites. Sites for government services such as taxation, armed forces, customs bureaus, and emergency services. Local, national, and international political sites and news sites. Sites for political debate, canvassing and election information and results.
Health & Medical	Sites for medical information and research. Medical service related sites such as dentistry, optometry, and psychiatry. General health, fitness and well-being information including self-help books and organizations. Sites for medical and hospital insurance.
Home & Garden	Web sites for home improvement, gardening, home/garden maintenance, decorating or pets.
Hunting & Fishing	Articles and publications on hunting and fishing techniques or specific product reviews. Outdoor recreational activities such as hiking, camping, and rock climbing.
Image (Photo) & Video Search	Image and video sites with or without search engines. Image or video directories.
Instant Messaging	Web-based instant messaging services and software.
Internet / Net Services	Sites that design and/or maintain web pages including individual web designers. Online personal storage or backup sites and services. Pay-to-surf sites.
Investing / Stocks / Financial Services	General investing, stock, and financial services and advice. Online stock or equity trading and sites containing stock quotes, tickers, and fund rates. Money management investment services or firms. Accountants, actuaries, banks, mortgage and general insurance companies.
Job Search / Careers	Career and job search sites and networking groups. Sites for employment agencies, contractors, job listing and career information.
Kids & Teens	Child-centered sites and sites published by children. Organizations and institutions aimed at helping underprivileged children.
Libraries & Museums	Official sites for libraries and museums. Census, almanacs, and library catalogues.
Motor Vehicles	Car reviews, vehicle purchasing or sales tips, parts catalogs Auto trading, photos, discussion of vehicles including motorcycles, boats, cars, trucks and RVs. Journals and magazines on vehicle modification, repair, and customization Online automotive enthusiast clubs.
Music / Radio / TV / Movies / Film	Movie, film and television sites including programming guides, tv ratings, reviews, news, and discussion forums. Broadcasting firms and stations. Circuses, theatre and radio sites.
News	Sites that primarily report information or comments on current events or contemporary issues of the day. Includes online newspapers, headline news sites, news wire services, personalized news services, and weather sites.

Table A.2: Default Allowed Categories

Category	Description
No Content	Sites that are completely blank or may contain one line, such as “Test Page” or “Hello World.”
Personals / Dating / Romance	Dating web sites focused on establishing personal relationships. Sites with advice for dating or relationships including romance tips and suggestions.
Real Estate	Sites that provide information on renting, buying, or selling real estate or properties. Tips on buying or selling a home. Real estate agents, rental or relocation services, and home improvement.
Recreation	Sites dedicated to tips or trends focused on specific art, crafts or techniques. Online clubs, associations, or forums dedicated to a hobby.
Redirect	Sites which automatically redirect (open) to another URL than the one entered.
Reference	Online teacher resources. Topic-specific search engines. Personal, professional or educational reference. Online dictionaries, maps and language translation sites.
Religion	Churches, synagogues and other houses of worship. Sites that promote and provide information on conventional or unconventional religious or quasi-religious subjects, as well as churches, synagogues, or other houses of worship.
Retirement / Seniors	Associations, organizations, clubs and information on retirement or directed at senior citizens.
Science	Sites containing science information, research or discussion. Specific trade journals and news sites dedicated to science industries.
Search Engines	Web sites that enable the user to conduct searches, including by key words, images, or phrases such as Google, Bing or Yahoo.
Sex Education	Sites that provide information on reproduction, sexual development, safe sex practices, sexuality, birth control, and sexual development. Also includes sites that offer tips for sexual discussions. Sites that sell sexual paraphernalia without images of sexual content. Includes sites that inform about or discuss abortion.
Shopping	Department stores, retail stores, company catalogs and other sites that allow online consumer or business shopping. Sites that provide or advertise the means to obtain goods or services as their main purpose.
Sports	Team or conference web sites. International, national, college and professional scores and schedules. Sports-related online magazines or newsletters.
Streaming Media	Sites that contain video clips and sound clips for upload or download.
Travel	Airlines and flight booking agencies. Sites that promote or provide opportunity for travel planning, including finding and making travel reservations, vehicle rentals, descriptions of travel destinations, or promotions for hotels or casinos.
Uncategorized	Sites which do not fit into any specific category.
Under Construction	Sites displaying “Under Construction”. May contain parked domains.
Unsure	Sites that contain a login to access the site, thus content undetermined.
Web Email	Sites offering Web based email and email clients.
Web Hosting	Sites that provide Web hosting services to clients.

Reference B: Category Mapping

GB-OS 6.1.3 and above include modifications to the Web Filtering category listings. The Web Filtering categories will be modified when a GTA firewall running GB-OS 6.1.2 or below is updated to GB-OS 6.1.3 or above. Existing categories will be automatically mapped to the enhanced categories. This automatic mapping is detailed in the chart below.

Multiple categories may map to the same category. For example, `Abused Drugs` and `Marijuana` will both map to `Illegal Drugs`. The new category will be denied by default.

Other categories will map to multiple new categories. For example, `Entertainment & Arts` will now map to three new categories: `Arts`, `Comedy` and `Entertainment`.

Note

GTA strongly recommends reviewing the settings for all categories and making any necessary revisions to your Web Filtering settings and policies to ensure they meet your corporate Internet Access Policy.

Table B.1: Category Mapping

Category Name (6.1.2 and Below)	Category Name (6.1.3 and Above)
Abortion	Sex Education
Abused Drugs	Illegal Drugs
Adult and Pornography	Sexual / Pornography
Alcohol and Tobacco	Alcohol Tobacco
Auctions	Classified / Auctions
Botnets	Botnets / Phishing / Malware
Business and Economy	Business
Cheating	Fraud / Illegal Activities
Computer and Internet Information	Computing
Computer and Internet Security	Computing
Confirmed Spam Sources	Botnets / Phishing / Malware
Content Delivery Networks	Internet / Net Services
Cult and Occult	Cult & Occult
Dating	Personals / Dating / Romance
Dead Sites	Dead Sites
Dynamically Generated Content	No Content
Educational Institutions	Education Colleges / Universities Libraries & Museums
Entertainment & Arts	Arts Comedy Entertainment
Fashion and Beauty	Fashion / Style
Financial Services	Investing / Stocks / Financial Services
Games	Game Media / Game Playing
Government	Government / Politics
Gross	Violence
Hacking	Hacking
Hate and Racism	Hate Speech / Discrimination

Table B.1: Category Mapping

Category Name (6.1.2 and Below)	Category Name (6.1.3 and Above)
Health & Medicine	Health & Medical Retirement / Seniors
Home and Garden	Food & Eating Home & Garden
Hunting and Fishing	Hunting & Fishing
Illegal	Fraud / Illegal Activities
Image and Video Search	Image (Photo) & Video Search
Individual Stock Advice and Tools	Investing / Stocks / Financial Services
Internet Communications	Instant Messaging Internet / Net Services
Internet Portals	Anonymous Proxies
Job Search	Job Search / Careers
Keyloggers and Monitoring	Botnets / Phishing / Malware
Kids	Kids & Teens
Legal	Business
Malware Sites	Botnets / Phishing / Malware
Marijuana	Illegal Drugs
Military	Government / Politics
Motor Vehicles	Motor Vehicles
News and Media	News
Nudity	Nudity
Online Gambling	Gambling
Online Greeting Cards	No Conversion
Online Music Sales	Music / Radio / TV / Movies / Film
Online Personal Storage	Web Hosting
Open HTTP Proxies	Anonymous Proxies
Parked Domains	Domain for Sale Under Construction
Pay To Surf	Internet / Net Services
Peer to Peer	Anonymous Proxies
Personal Sites and Blogs	Blogs / Forums / Newsgroups
Philosophy and Political Advocacy	Government / Politics
Phishing and Other Frauds	Botnets / Phishing / Malware Fraud / Illegal Activities
Private IP Addresses	No Conversion
Proxy Avoidance and Anonymizers	Anonymous Proxies
Questionable	Botnets / Phishing / Malware
Real Estate	Real Estate
Recreation and Hobbies	Recreation / Hobbies
Reference and Research	Reference Science
Religion	Religion
Search Engines	Search Engines
Sex Education	Sex Education
Shareware and Freeware	Computing

Table B.1: Category Mapping	
Category Name (6.1.2 and Below)	**Category Name (6.1.3 and Above)**
Shopping	Shopping
Social Networking	Blogs / Forums / Newsgroups
Society	Gay / Lesbian Cultures / Society
Spam URLs	Link Farms / Click Fraud
Sports	Sports
Spyware and Adware	Botnets / Phishing / Malware
Streaming Media	Streaming Media
Swimsuits and Intimate Apparel	Intimate Apparel / Swimsuits
Tourist Information	Travel
Training and Tools	Reference
Translation Sites	Reference
Travel	Travel
Uncategorized	Malformed / Invalid URLs Redirect Uncategorized Unsure
Unconfirmed Spam Sources	Botnets / Phishing / Malware
Violence	Suicide Promotion Vulger or Obscene Language Violence
Weapons	Weapons
Web Advertisements	Advertisements & Popup-ups
Web Based Email	Web Mail
Web Hosting	Web Hosting

Copyright

Technical Support

GTA includes 30 days "up and running" installation support from the date of purchase. See GTA's Web site for more information. GTA's direct customers in the USA should call or email GTA using the telephone and email address below. International customers should contact a local Authorized GTA Channel Partner.

Tel: +1.407.380.0220 **Email:** support@gta.com

Disclaimer

Neither GTA, nor its distributors and dealers, make any warranties or representations, either expressed or implied, as to the software and documentation, including without limitation, the condition of software and implied warranties of its merchantability or fitness for a particular purpose. GTA shall not be liable for any lost profits or for any direct, indirect, incidental, consequential or other damages suffered by licensee or others resulting from the use of the program or arising out of any breach of warranty. GTA further reserves the right to make changes to the specifications of the program and contents of the manual without obligation to notify any person or organization of such changes.

Mention of third-party products is for informational purposes only and constitutes neither an endorsement nor a recommendation for their use. GTA assumes no responsibility with regard to the performance or use of these products.

Every effort has been made to ensure that the information in this manual is accurate. GTA is not responsible for printing or clerical errors.

Trademarks & Copyrights

Global Technology Associates, Inc.

3361 Rouse Rd, Suite 240 • Orlando, FL 32817 USA
Tel: +1.407.380.0220 • **Fax**: +1.407.380.6080 • **Web**: http://www.gta.com • **Email**: info@gta.com