



XROADS NETWORKS

---

Network Appliance How To Guide: Application Filtering

# How To Guide

EDGE NETWORK APPLIANCE

# How To Guide Filtering

---

© XRoads Networks  
17165 Von Karman • Suite 112  
888-9-XROADS

---

# Table of Contents

|                            |          |
|----------------------------|----------|
| <b>Filtering Overview</b>  | <b>3</b> |
| <br>                       |          |
| <b>C O M P O N E N T S</b> |          |
| <b>Filtering Control</b>   | <b>4</b> |
| <b>Database Management</b> | <b>5</b> |
| <b>Logging / Reporting</b> | <b>6</b> |
| <b>Bypass Rules</b>        | <b>7</b> |

# Edge Configuration Series

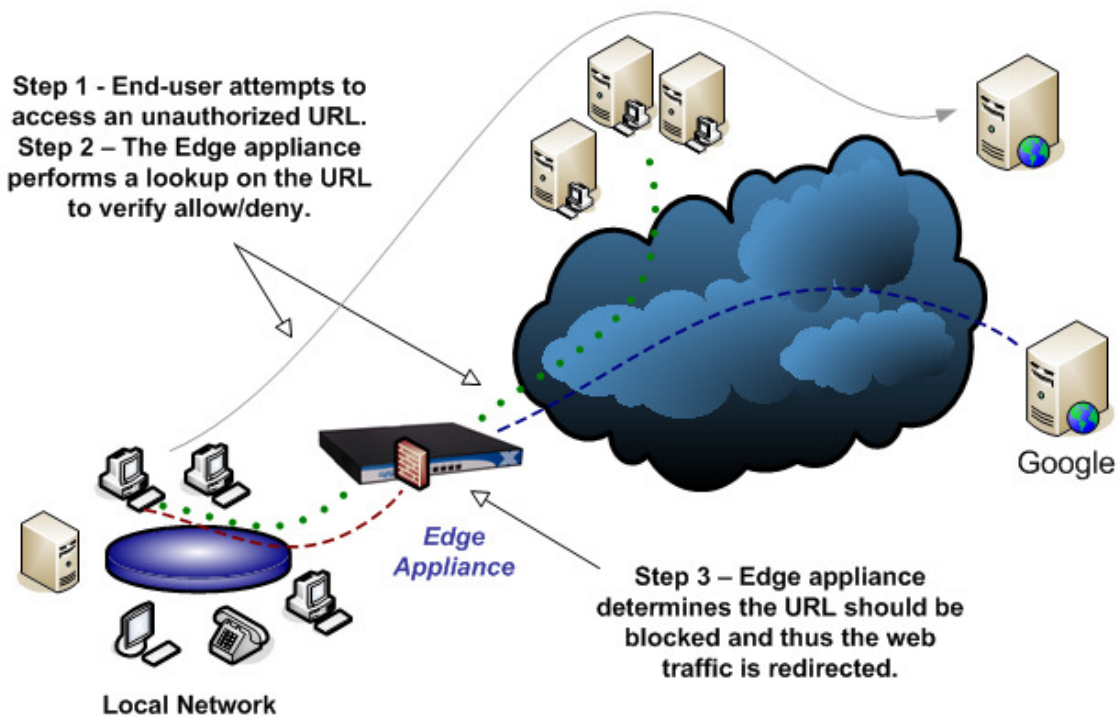
## Filtering Overview

The Edge application filtering module provides the ability to filter unauthorized web content in order to protect end-users and the organization as a whole.

The diagram below demonstrates how the Application Filtering works.

When a request is made by an end-user to access a web site, the Edge appliance captures that initial DNS request and performs a check against its filter database. If a match is made the site is validated, if the site is set to be blocked, then the end-user is redirected to a safe site and the request is logged for later reporting.

A site may initially be allowed but then blocked if certain keywords within the site are not allowed. Thus the first person to access the site may be permitted (and logged), however a future requests to that site will be blocked.

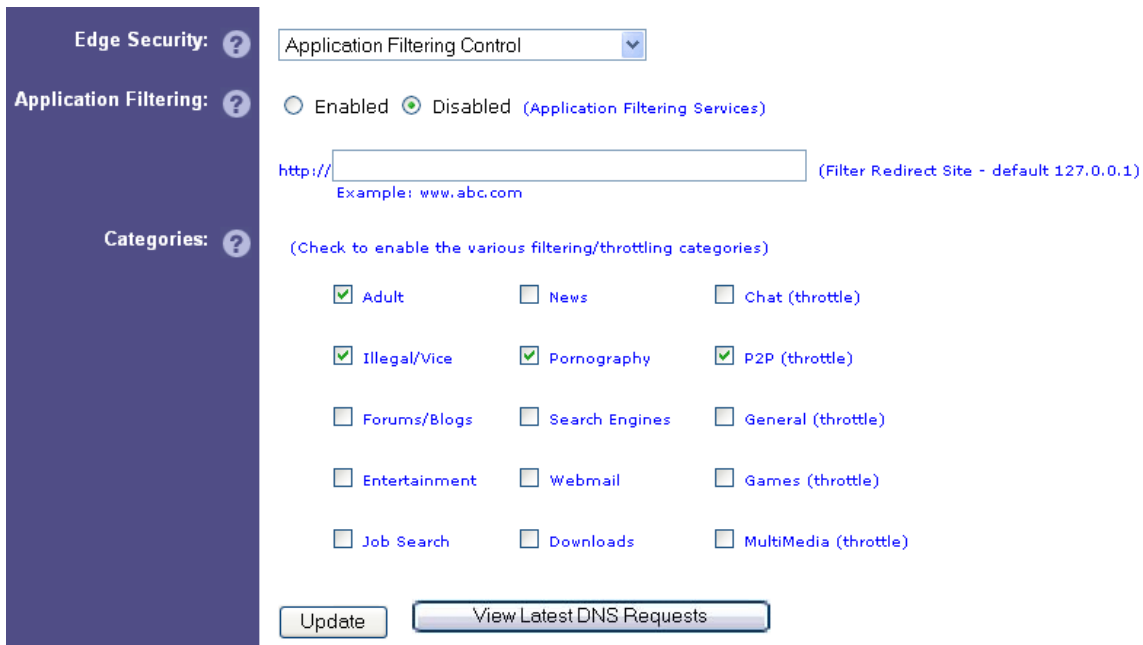


## Filtering Control

In order to enable the application filtering, the filtering engine must be enabled via the Application Filtering Control menu option.

Once enabled, all DNS requests will be filtered by the Edge appliance.

A redirect should also be entered so that end-users can be redirected to a “safe” site when they do attempt to access unauthorized content. If no redirect is entered, the default behavior is to send the end-user to a blank page.



The screenshot shows the configuration interface for Application Filtering Control. On the left is a dark blue sidebar with three sections: 'Edge Security: ?', 'Application Filtering: ?', and 'Categories: ?'. The main content area has a dropdown menu set to 'Application Filtering Control'. Below it, there are radio buttons for 'Enabled' and 'Disabled', with 'Disabled' selected and a link to '(Application Filtering Services)'. A text input field for a redirect URL is shown with 'http://' and an example 'www.abc.com'. Below this is a section for categories with a note '(Check to enable the various filtering/throttling categories)'. A grid of checkboxes is displayed, with 'Adult', 'Illegal/Vice', 'Pornography', and 'P2P (throttle)' checked. Other categories like 'News', 'Chat (throttle)', 'Forums/Blogs', 'Search Engines', 'General (throttle)', 'Entertainment', 'Webmail', 'Games (throttle)', 'Job Search', 'Downloads', and 'MultiMedia (throttle)' are unchecked. At the bottom are 'Update' and 'View Latest DNS Requests' buttons.

The next step is to select the appropriate categories from the list of checkboxes based on the organizations requirements. Each checkbox represents multiple sub-categories which are used by the database to allow/deny access to various sites matching those parameters.

Finally, the “View Latest DNS Requests” provides a real-time view of requests being made by end-users. This can be opened in a new window and used to monitor Internet access.

## Database Management

The filtering database is contained within the flash drive within the appliance. This database can be automatically updated on a daily basis using the Automated Updates subscription service provided by XRoads Networks.

**The database is able to block several million sites today.**

New sites are being added and categorized by XRoads Networks all the time. These sites are added from sources on the Internet and through our customers which add sites to block within their own network. Those updates are sent to XRoads Networks for testing and if they meet the general purpose of a specified category, are added to that category for a future update.

In addition to the pre-defined sites, the administrator may also add sites that they wish to be blocked. Using the Application Filtering Add Rules menu option, the administrator can instantly add sites that should be blocked, or allowed.

**Allowing Sites** – Sites that are blocked by the filter may be allowed by default by adding an allow rule. This will ensure that the site is allowed even if other rules are set to block the site.

**Block Sites** – Sites that are not being blocked properly or quickly enough (if based on site keyword search) it may be instantly blocked by adding the site to the database.

**Keyword Blocking** – The administrator may also add a keyword which will be used in conjunction with the database to block additional sites.

The screenshot shows a configuration interface for 'Edge Security' with a dark blue sidebar on the left containing 'Edge Security: ?' and 'Custom Rule: ?'. The main content area has a dropdown menu set to 'Application Filtering Add Rules'. Below this are two rows of radio buttons: the first row has 'Enabled' (selected) and 'Disabled' (with a note '(Determines whether the rule is active)'); the second row has 'Deny Rule' (selected) and 'Allow Rule' (with a note '(Determines how the rule below is applied)'). A text input field is present with the placeholder text 'Examples: limewire, aol.com, doubledclick, playboy.com' and a note '(Enter domain name, or single word which will match all URLs with that word)'. Below the input field is a dropdown menu set to 'All Categories' with a note '(Select a category for this rule)'. At the bottom are four buttons: 'Reset', 'Add / Update', 'View Report', and 'View Rules >>'.

To add a rule, simply select whether the rule is active, allowed or denied, the site or keyword, and the category to which the rule should be applied.

## Database Categories

These lists provide an overview of the types of content filtered performed by each level. Each level includes the items from the previous level.

- Adult
  - Promotion of weapon use
  - Dating Sites
  - Nudity
  - Male/Female genitals
  - Female breasts
- Illegal/Vice
  - Promotion of discrimination
  - Promotion of tobacco use
  - Promotion of alcohol use
  - Promotion of drug use
  - Killing of human beings, animals
  - Deliberate injury to human beings
  - Deliberate damage to objects
  - Gambling
- Entertainment
  - Sports
  - Shopping
  - Gaming
  - Travel
- News
  - Pop Culture
  - Religious Materials
  - General News
  - Magazines
  - Politics
- Pornography
  - Hardcore pornography
  - Erections or female genitals
  - Sexual violence/rape
  - Explicit sex

*NOTE: The content filtering is provided as a best effort service. XRoads Networks does not guarantee that all sites will be blocked, and can not be held liable in for content that is not blocked.*

## Database Search

To determine if a particular site is available in the database simply enter the site or keyword for the site in question into the Application Filtering Database Search menu option and any result will appear below.

Edge Security: ? Application Filtering Database Search

(Enter Search Criteria)

*NOTE: Use this search tool to check for existing entries in the rules database.*

Search

| Select | URL/Keyword | Description | Category | Status | Allow/Deny |
|--------|-------------|-------------|----------|--------|------------|
|--------|-------------|-------------|----------|--------|------------|

Update Selected *This will change the current Allow/Deny status of the rule.*

If a result is found, the administrator has the option of changing the status of the found rule set by selecting the rule and clicking the Update Selected button.

## Logging Reporting

As mentioned previously, all DNS requests are logged by the Edge appliance when Application Filtering is enabled. In order to perform a search, simply enter the search criteria, select which column to search and which type of rule should be found (allowed / denied).

This will return a list of matching requests. This list can be copied off for additional reporting and analysis. NOTE: To generate a quick report of all unauthorized access, simply select the Denied matching rule, and click the Search button with no other parameters given.

The screenshot shows the 'Edge Security' configuration page for logging reporting. On the left is a dark blue sidebar with 'Edge Security: ?' and 'Search Results: ?'. The main area has a dropdown menu set to 'Application Filtering Logging'. Below it is a search bar with a 'Search' button, followed by a text input field with '(Enter Search Criteria)' placeholder, a 'Username' dropdown, another text input field with '(Enter Search Field)' placeholder, a '10' input field with '(Limit Responses)' placeholder, and an 'Allowed' dropdown with '(Matching)' placeholder. At the bottom, there are five column selection buttons: 'Time', 'Username', 'Address', 'URL', and 'Allow/Deny', with 'Allow/Deny' currently selected.

This reporting feature can also be used in conjunction with the Application Filtering User Definition menu option in order to define the end-users information for quick reference based on their IP address. Additionally, the Edge appliance can tie an end-users IP address to their MAC address via the DHCP feature available via the LAN Interface configuration.

## Bypass Rules

In some cases, there are certain end-users or application servers which should have any filtering performed. In those cases a bypass rule may be created which allows those users/servers to pass through the Edge appliance with no filtering performed.

NOTE: The requests from the address of a bypass rule are still logged even through no action may have taken place to block or redirect the user/server.

The screenshot shows the 'Edge Security' configuration page for bypass rules. The sidebar has 'Edge Security: ?' and 'Bypass Policy: ?'. The main area has a dropdown menu set to 'Application Filtering Bypass'. Below it is a text input field for IP address with four segments and '(Define host/address)' placeholder. Underneath is a dropdown menu set to 'SINGLE HOST' with '(Define single host/subnet)' placeholder. At the bottom are two buttons: 'Add / Update' and 'View Bypass List >>'.