

Application Rule Set and Lists

<https://campus.barracuda.com/doc/43846925/>

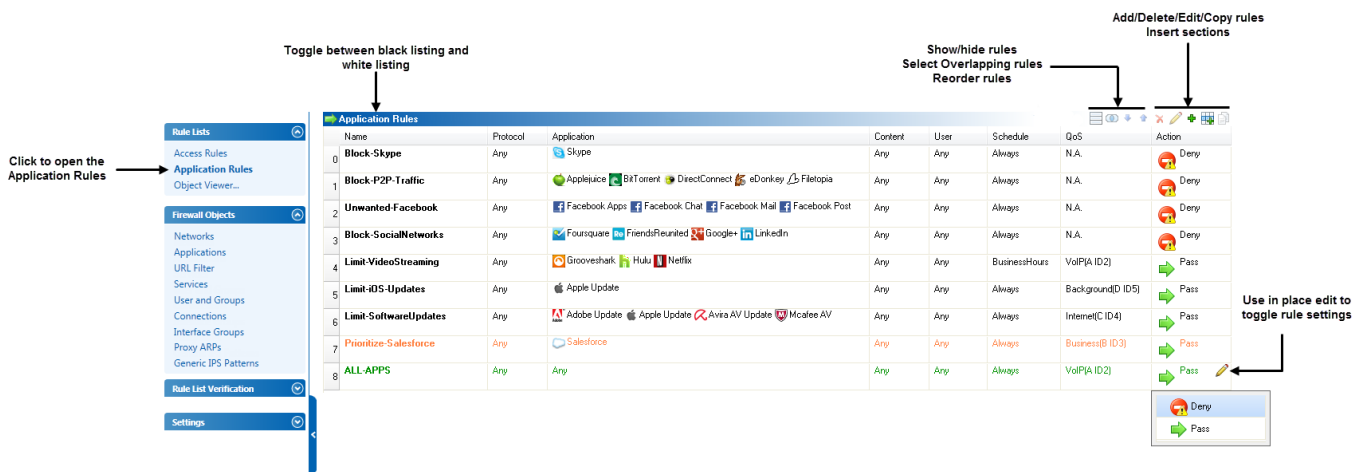
On the **Forwarding Firewall - Rules** page, you can view and configure the application rule set. You can also view the list of application and URL filter objects that can be used in application rules.

In this article:

Application Rule Set

In the **Application Rules** section of the **Forwarding Firewall - Rules** page, you can view and edit the application rule set. It lists all of the application rules that have been created. After adding a new application rule, you can directly edit specific rules. For more information, see [Firewall Access Rules](#)

The following figure displays the application rule set.



In the rule set, information and settings for each rule is organized into the following columns:

Column	Description
Name	The name of the application rule.
Application	The applications and sub-applications that are affected by the rule. You can either statically assign specific applications or use an application object. Barracuda Networks recommends that you use Application Object or Application Filter instead of linking static applications to access rules.

Content	The types of multimedia content that are affected by the rule. You can choose to globally block Flash, AVI, MPEG, QuickTime, and RealMedia content in websites.
URL Filter Match	The URL Filter Match policy that are affected by the rule. You can either statically assign specific URL filters or use an existing URL filter match object. Barracuda Networks recommends that you use URL Filter Match Objects instead of linking static URL Filter Match policies to access rules.
URL Filter Policy	The URL Filter Policy that are affected by the rule. You can either statically assign specific URL Policies or use an existing URL Filter Policy object. Barracuda Networks recommends that you use URL Filter Policy Object instead of linking static URL Filter policies to access rules.
Protocol	The protocols that are affected by the rule. With protocols, traffic can be controlled without having to match criteria like source or destination network. For example, you can select protocols to globally detect IPsec or SMTP network traffic and apply QoS policies to prioritize business critical network communications without needing to know the origin or target.
User	The users and user groups who are affected by the rule.
Schedule	The time or date during which the rule can be applied.
QoS	The traffic shaping settings that are used by the rule. For more information, see Traffic Shaping and How to Create and Apply QoS Bands .
Action	The action that is performed when the application is accessed by the user (<i>Deny or Pass</i>).
Source	The source network address of the traffic that is affected by the rule. Because the source network is already evaluated in the Access Rule set, you can either use <i>Any</i> or enter specific IP addresses.
Destination	The destination network address of the traffic that is affected by the rule. Because the destination network is already evaluated in the Access Rule set, you can either use <i>Any</i> or enter specific IP addresses.
Comment	Optional. Additional information about the application rule.
IPS Policy	The Intrusion Prevention System (IPS) policy that is enforced by the rule. For more information on IPS, see Intrusion Prevention System (IPS) .
Usage	Optional. Additional information about the application rule.
TI-Settings	The Traffic Intelligence (TI) settings. For more information, see Traffic Intelligence .

Application Objects List

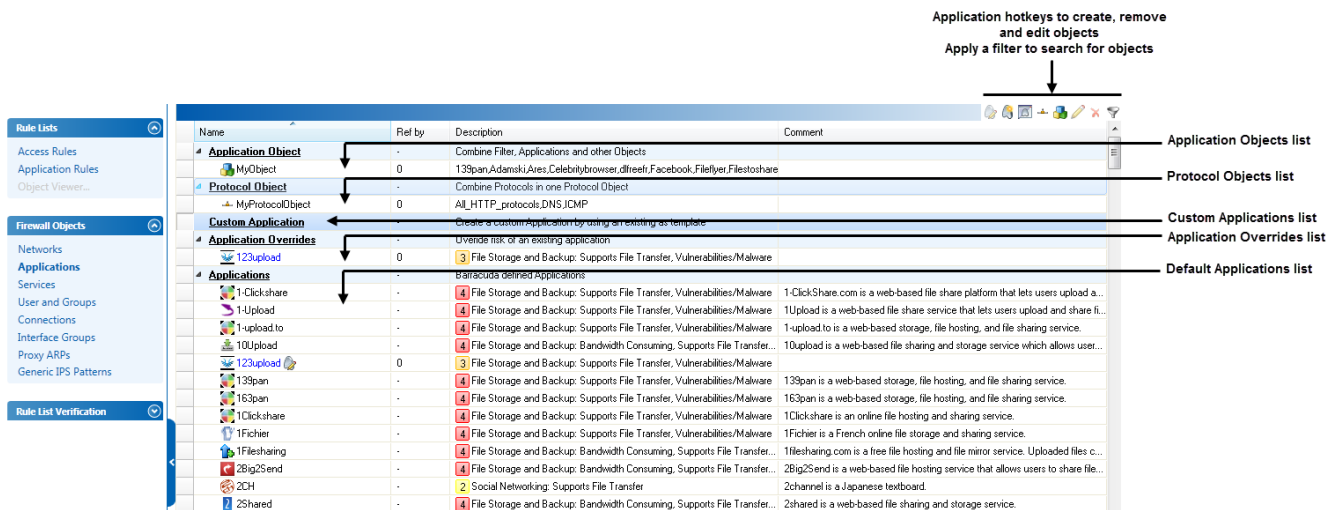
In the **Applications** section of the **Forwarding Firewall - Rules** page, you can view, create, and edit the applications and application objects that are used in application rules. Applications are organized into the following categories:

- **Application Object** – Lists any application objects that you have created. An application object

is a reusable combination of predefined applications, custom applications, and other applications objects. Application objects help simplify the configuration of application rules. For more information, see [How to Create an Application Object](#).

- **Protocol Object** - Lists any protocol objects that you have created. A protocol object is a reusable combination of predefined protocols. For more information, see [How to Create a Protocol Object](#).
- **Custom Application** - Lists any custom applications that you have created. If the default Application Control 2.0 pattern database does not cover an application that you want to use in your application rules, you can customize an application. For more information, see [How to Create a Custom Application Object](#).
- **Application Overrides** - Lists any applications whose risk levels you have changed. For more information, see [How to Override the Risk Classification of an Application](#).
- **Applications** - Lists predefined applications from the Application Control 2.0 database.

The following figure displays the **Applications** section.



Name	Ref by	Description	Comment
Application Objects list			
Application Object	-	Combine Filter, Applications and other Objects	
MyObject	0	133pan,Adamski,Ares,Celebrity,browser,direct,Facebook,Fileflyer,Filestoshare	
Protocol Objects list			
Protocol Object	-	Combine Protocols in one Protocol Object	
MyProtocolObject	0	All_HTTP_protocols,DNS,ICMP	
Custom Applications list			
Custom Application	-	Create a custom Application by using an existing as template	
Application Overrides list			
Application Overrides	-	Override risk of an existing application	
123upload	0	File Storage and Backup; Supports File Transfer, Vulnerabilities/Malware	
Default Applications list			
Barracuda defined Applications			
1-Clickshare	-	File Storage and Backup; Supports File Transfer, Vulnerabilities/Malware	1-ClickShare.com is a web-based file share platform that lets users upload a...
1-Upload	-	File Storage and Backup; Supports File Transfer, Vulnerabilities/Malware	1Upload is a web-based file share service that lets users upload and share fi...
1-upload.to	-	File Storage and Backup; Supports File Transfer, Vulnerabilities/Malware	1upload.to is a web-based storage, file hosting, and file sharing service.
10Upload	-	File Storage and Backup; Bandwidth Consuming; Supports File Transfer...	10upload is a web-based file sharing and storage service which allows user...
123upload	0	File Storage and Backup; Supports File Transfer, Vulnerabilities/Malware	
133pan	-	File Storage and Backup; Supports File Transfer, Vulnerabilities/Malware	133pan is a web-based storage, file hosting, and file sharing service.
163pan	-	File Storage and Backup; Supports File Transfer, Vulnerabilities/Malware	163pan is a web-based storage, file hosting, and file sharing service.
1Clickshare	-	File Storage and Backup; Supports File Transfer, Vulnerabilities/Malware	1Clickshare is an online file hosting and sharing service.
1Fichier	-	File Storage and Backup; Supports File Transfer, Vulnerabilities/Malware	1Fichier is a French online file storage and sharing service.
1Filesharing	-	File Storage and Backup; Bandwidth Consuming; Supports File Transfer...	1filesharing.com is a free file hosting and file mirror service. Uploaded files c...
2Big2Send	-	File Storage and Backup; Bandwidth Consuming; Supports File Transfer...	2Big2Send is a web-based file hosting service that allows users to share file...
2CH	-	Social Networking; Supports File Transfer	2channel is a Japanese textboard.
2Shared	-	File Storage and Backup; Bandwidth Consuming; Supports File Transfer...	2shared is a web-based file sharing and storage service.

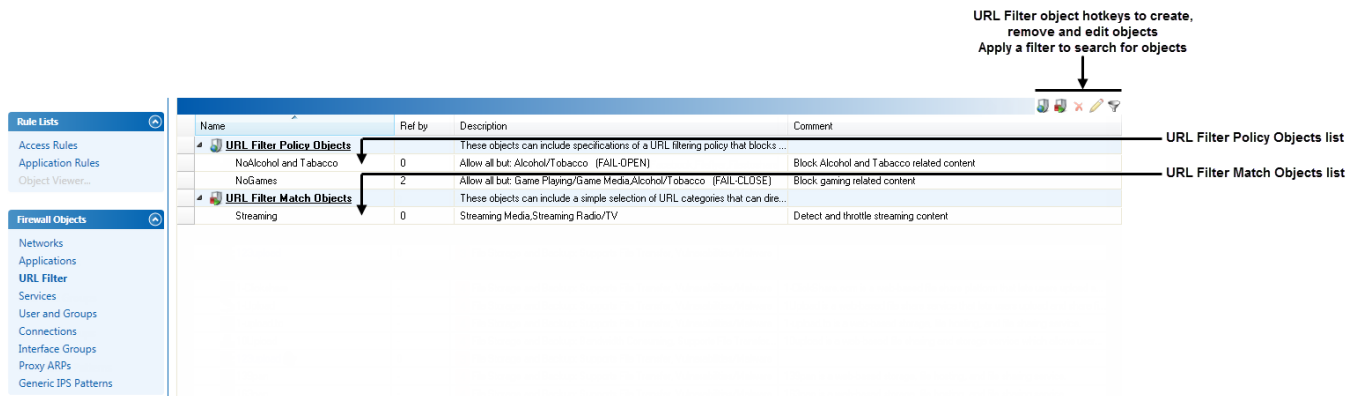
The following information is provided for each application and application object:

- **Name** - The name of the application including the icon of the service/application.
- **Ref by** - The reference to which application object the selection points. This is applied when an application filter is created. Note that referenced objects cannot be deleted.
- **Description** - A description of the application including type and features.
- **Comment** - General information about the application.

URL Filter Objects List

In the **URL Filter** section of the **Forwarding Firewall - Rules** page, you can view, create, and edit URL filter objects that are used in application rules.

URL Filter object hotkeys to create, remove and edit objects
Apply a filter to search for objects



Name	Ref by	Description	Comment
URL Filter Policy Objects			
NoAlcohol and Tobacco	0	Allow all but: Alcohol/Tobacco (FAIL-OPEN)	Block Alcohol and Tobacco related content
NoGames	2	Allow all but: Game Playing/Game Media/Alcohol/Tobacco (FAIL-CLOSE)	Block gaming related content
URL Filter Match Objects			
Streaming	0	Streaming Media, Streaming Radio/TV	Detect and throttle streaming content

The following information is provided for each URL filter object:

- **Name** – The name of the URL filter object.
- **Ref by** – The reference to which URL filter object the selection points. Note that referenced objects cannot be deleted.
- **Description** – A description of the URL filter object, including type and features.
- **Comment** – General information about the URL filter object.

Figures

1. Application Rules.png
2. Application Browser.png
3. URL Filter Object Browser.png

© Barracuda Networks Inc., 2019 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.