

1. Barracuda Web Filter - Overview	3
1.1 What's New in the Barracuda Web Filter	3
1.1.1 Release Notes	7
1.2 Deployment Options	8
1.2.1 Inline Pass-Through (Transparent) Mode Deployment	8
1.2.2 Forward Proxy Deployment of the Barracuda Web Filter	10
1.2.3 High Availability - Clustering the Barracuda Web Filter	11
1.2.4 Inline Pass-through With Pre-existing Proxy Deployment	13
1.2.5 Connecting Inline to your Network with a Pre-existing Proxy Server	14
1.2.6 Policy-Based Routing	15
1.2.7 Source-Based Routing	20
1.2.8 VLAN Deployments	21
1.2.9 Virtual Deployment	23
1.2.9.1 Hypervisor Compatibility and Deployment - OVF Package	24
1.2.9.2 Hypervisor Compatibility and Deployment - VMX Package	25
1.2.9.3 Hypervisor Compatibility and Deployment - XVA Package	26
1.2.9.4 Barracuda Web Filter Vx Quick Start Guide	26
1.2.9.5 Backing Up Your Virtual Machine System State	27
1.2.9.6 Directing Traffic to the Barracuda Web Filter Vx	27
1.2.9.7 Sizing Disk, Drives and RAM for Your Barracuda Web Filter Vx	28
1.2.10 WCCP Deployment 6.x	29
1.3 Getting Started	32
1.3.1 Step 1: Network Considerations	32
1.3.1.1 Using Static Routes	34
1.3.2 Step 2: Installation	35
1.3.3 Step 3: Configure the Barracuda Web Filter	37
1.3.4 Step 4: Configure and Secure the Web Interface	39
1.3.5 Step 5: Connect the Barracuda Web Filter to Your Network	40
1.3.6 Barracuda Web Filter 30 Day Evaluation Guide	42
1.4 Managing Policies	43
1.4.1 Best Practices in Configuring Policy	44
1.4.2 BLOCK/ACCEPT Order of Precedence - Barracuda Web Filter	45
1.4.3 Block Messages	46
1.4.4 Creating Block and Accept Policies	48
1.4.4.1 Application Filtering for Non Web Based Applications	51
1.4.5 Using Custom Categories	51
1.4.6 Exception Policies 6.x	52
1.4.7 Exception Policies 7.x	54
1.4.8 Barracuda Web Filter for Education	58
1.4.9 How to Set Up YouTube for Schools	60
1.4.10 How to Enable Safe Search for Students	62
1.4.11 Suspicious Keyword Tracking	63
1.4.12 Temporary Access for Education	64
1.4.13 How to Use Temporary Access for Students - Teacher's Guide	71
1.4.14 How to Configure Web Application Monitoring	77
1.4.15 Using SSL Inspection With the Barracuda Web Filter	79
1.4.15.1 How to Configure SSL Inspection 7.x	81
1.4.15.2 How to Configure SSL Inspection for Google Chrome Browser	81
1.4.15.3 How to Configure SSL Inspection 6.x	82
1.4.16 Google Apps Control Over HTTPS	83
1.4.17 Facebook Control Over HTTPS	86
1.5 Managing Users and Groups	89
1.5.1 Creating Users and Groups	89
1.5.2 Integrating the Barracuda Web Filter With a User Authentication Service	91
1.5.3 How to Choose Your Authentication Mechanisms	92
1.5.3.1 How to Configure Kerberos Authentication	93
1.5.3.2 How to Enable LDAP Domain User Authentication	95
1.5.3.3 How to Enable NTLM Domain User Authentication	95
1.5.4 Role-based Administration 6.x	96
1.5.5 Role-based Administration 7.x	97
1.6 Advanced Configuration	98

1.7 Remote Filtering for Offsite and Mobile Users	99
1.7.1 Barracuda Web Security Agent (WSA) - How it Works	99
1.7.1.1 How to Configure and Manage the Barracuda WSA	101
1.7.1.2 How to Install the Barracuda WSA With the Barracuda Web Filter	102
1.7.1.2.1 Installation on a Macintosh	104
1.7.1.2.2 Installation using a Windows GPO from the Command Line	104
1.7.1.2.3 Installation using a Windows GPO from the Windows Interface	106
1.7.1.2.4 Manual local Installation from the Command Line	109
1.7.1.2.5 Uninstalling the Barracuda Web Security Agent for Win2K3 Server	112
1.7.1.2.6 Uninstalling the Barracuda Web Security Agent for Win2K8 Server	113
1.7.2 How to Configure Global HTTP Proxy with Barracuda Web Security Solutions	113
1.7.3 Barracuda Safe Browser Setup Guide - With Barracuda Web Filter	117
1.8 Monitoring the System	119
1.8.1 Basic Monitoring Tools	119
1.8.1.1 Audit Log of Configuration Changes	122
1.8.2 Reporting 6.x	123
1.8.3 Reporting 7.x	123
1.8.4 How to Set Up Alerts and SNMP Monitoring	125
1.8.4.1 Barracuda Reference MIB	126
1.8.4.2 Barracuda Web Filter SNMP MIB	126
1.8.5 How to Set Up Barracuda Cloud Control	134
1.8.6 Troubleshooting	134
1.8.7 Syslog and the Barracuda Web Filter	136
1.9 Maintenance	141
1.9.1 How to Back Up and Restore Your System Configuration	142
1.10 Web Use Categories	142
1.11 About the Barracuda Web Filter Hardware	147
1.11.1 Hardware Compliance	154
1.12 Limited Warranty and License	154
1.13 About the Barracuda DC Agent	164
1.14 How to Get and Configure the Barracuda DC Agent	165
2. How to Use the Barracuda Malware Removal Tool	169

Barracuda Web Filter - Overview

Searching Barracuda Web Filter

The Barracuda Web Filter is an integrated content filtering, application blocking and malware protection solution that is powerful, easy to use and affordable for businesses and educational institutions of all sizes. It enforces Internet usage policies on and off network by blocking access to websites and Internet applications that are not related to business or education, and it easily and completely eliminates spyware and other forms of malware from your organization.

Where to Start

If you have the Barracuda Web Filter Vx virtual machine, start here:

- [Barracuda Web Filter Vx Virtual Deployment](#)
- [The 30 Day Evaluation Process](#) – A roadmap for your product evaluation (optional)
- [Managing Policies](#) – Best practices, precedence of block/accept policies, authentication schemes

If you have the Barracuda Web Filter appliance, start here:

- [Getting Started](#)
- [The 30 Day Evaluation Process](#) – A roadmap for your product evaluation (optional).
- [Managing Policies](#) – Best practices, precedence of block/accept policies, authentication schemes.

Key Features

- Content filtering, with HTTP/HTTPS support and URL filtering by category for various types of users and groups.
- Comprehensive network threat protection.
- LDAP integration, Single Sign-on user authentication – See [How to Choose Your Authentication Mechanisms](#).

Safe Browsing for Schools and Remote Users

- [Barracuda Web Filter for Education](#) – A suite of features to regulate use of social media applications, alert on cyberbullying and provide safe browsing and content delivery for the classroom
- [Remote Filtering for Offsite and Mobile Users](#) – A policy enforcement solution for BYOD, campus-issued laptops and iOS devices

Granular Policy Control

- HTTPS-based Policy – Create policy exceptions specific to HTTP traffic, HTTPS, or another legitimate URI scheme
- Social Media monitoring – Control and [archiving](#) of web-based application traffic and/or content, regulating use of Google Apps, Facebook, YouTube and other web 2.0 applications.

What's New in the Barracuda Web Filter

For the changelog, please read the [Release Notes](#).

What's New in Version 7.0

Web Interface

- **New look and feel** - The new Barracuda Web Filter web interface is cleaner with a new color scheme, but is functionally the same with no changes to navigation.
- **Enhanced Dashboard** - View live feed of current TCP connections and graphs of blocked requests, user browse times and bandwidth usage for a quick picture of web traffic on your network. See the **BASIC > Status** page.
- **New controls** for viewing logs and switching graph content type on-screen.
- **Recent Flagged Terms** - (Available on 610 and higher) This new section of the dashboard on the **BASIC > Status** page displays a list of the most used *suspicious keyword terms* in social media and search engine activities per settings on the **BLOCK/ACCEPT > Web Application Monitor** page. These terms are categorized in a suspicious keywords lexicon provided by Barracuda Networks and can be added to by creating a custom list on the **BLOCK/ACCEPT > Web Application Monitor** page.
- **Improved reporting** presentation tools as described below.
- **Limited support for Barracuda Appliance Control (BAC)**. The new web interface includes several key enhancements, especially

around the dashboard (**BASIC > Status** page). Future versions of the Barracuda Web Filter firmware will fully support the new web interface. You can still join your Barracuda Web Filter running version 7.0 to Barracuda Appliance Control, with limited feature support.

Temporary Access for Teachers, Students

- This feature replaces the Temporary Whitelist role. For research projects and other classroom needs, the Temporary Access Portal enables teachers to obtain student access, for a specified time period, to websites that are typically regulated by administrators. Administrators either create credentials for teachers, or teachers simply log into the portal via LDAP. From the portal teachers can request domains and/or categories of domains for temporary student access. The Temporary Access Portal issues a token for each request that the teacher can then give to students for bypassing block pages. See [Temporary Access for Students](#) for details and workflow. To configure, see **ADVANCED > Temporary Access**. The **BASIC > Temporary Access Requests** log tracks activity by teachers who have been given credentials to request temporary access for their students to typically blocked domains. The log displays the status of tokens teachers create by username and date, including expiration date and time of tokens.

Web Application Monitoring (Available on 610 and higher)

- **Suspicious Keyword Alerts** - Applies to terms categorized as related to cyberbullying, profanity, adult or terrorism in social media interactions. Barracuda Networks provides a lexicon of keywords you want the Barracuda Web Filter to flag for generating email alerts when they appear in user social media interactions or search engine activities. You can add your own categories and lists of keywords as well. See the **BLOCK/ACCEPT > Web App Monitor** page for details and to configure. The **BASIC > Status** page includes a listing of the top flagged suspicious keywords identified in filtered traffic.
- **New Web App Monitor Log page** - This new page on the **BASIC** tab displays a log of all archived chat, email, user registrations and social media interaction traffic processed by the Barracuda Web Filter. Configure which kinds of activities you want to capture on the **BLOCK/ACCEPT > Web App Monitor** page. Use the **BASIC > Web App Monitor Log** page to view these captured application interactions by date, source IP address, username and associated details.

Enhanced HTTPS Filtering

- **SSL Inspection** - Now available for inline deployments with some models. See [Using SSL Inspection With the Barracuda Web Filter](#) or the **ADVANCED > SSL Inspection** page. Provides for granular control of web 2.0 applications over HTTPS as described above within Facebook, Google Apps, YouTube and more.
- **HTTPS Block Page** - A block page is presented when users attempt to visit a website over HTTPS that either poses a security risk, violates policy, or that falls under the *Warn* policy action. Using the HTTP block page template on the **BLOCK/ACCEPT > Block Messages** page, you can customize the text on the web page displayed by the Barracuda Web Filter.

Reporting

- **New reporting engine** with enhanced performance for fast response times.
New report set – Organized for Productivity, Safety & Liability, Web Activity, Infection Activity and Administrative (Temporary Access Requests), including:
 - Top Facebook Users by Browse Time
 - Top Users by Bandwidth on Streaming Media Sites
 - Top Gaming Domains by Requests
 - Top Users by Requests to Spyware Sites
 - ...and many more

Enhanced PDF and HTML presentation with informative header, footer and easy-to-read layout.

See [Reporting](#) for an overview. For a complete list of reports & descriptions of output, click the **Help** button on the **BASIC > Reports** page in the Barracuda Web Filter web interface.

New Audit Log

- The Barracuda Web Filter maintains a log of events including logins/logouts and changes to configuration settings in conjunction with role-based administration. The new **BASIC > Audit Log** page lists these events including date, source IP address, username, role and associated details.

Policy Rule Checking

- From the **ADVANCED > Troubleshooting** page you can test policy rules applied to traffic on specified servers. You can verify access restrictions and exceptions that you define in the pages on the **BLOCK/ACCEPT** tab. The Policy Rule Check returns a list of all of the rules that would apply to traffic and actions (**Allow**, **Monitor**, **Warn**, or **Deny**) that would be taken based on the rule.

Support for External ICAP servers

- Ability to redirect traffic from the Barracuda Web Filter to a 3rd party server. Select *DLP*, *Antivirus*, or other dedicated ICAP server on the **ADVANCED > External Servers** page. The Barracuda Web Filter will first apply all configured policies to inbound or outbound traffic, and then forward the traffic to the specified ICAP server for DLP scanning, antivirus scanning or other processing

What's New in Version 6.0.1

Safe Browsing and Remote User Access

- **Barracuda Safe Browser Support** - The Barracuda Safe Browser is a full-featured web browser, currently available for the iOS platform that is integrated with the Barracuda Web Filter (as well as the Barracuda Web Security Service). Great for students and BYOD work environments, web requests made through the browser on a mobile device will automatically be filtered to block access to malicious web sites and to enforce compliance policies that you configure in the BLOCK/ACCEPT pages, just as you configure policies for any other traffic source.
- **Web Security Agent** - Version 4.2.3 of the Barracuda Web Security Agent supports Windows 8.
- **Remote Device Tracking** - The Barracuda Web Filter maintains a log of remote user and mobile device locations via the Barracuda Web Security Agent (WSA) and the Barracuda Safe Browser. Logged data includes the Username, Domain, Device Name, Device Type, IP Address, Location (link to Google Maps), and Last Seen date and time. This data is logged each time a remote user logs into the Barracuda WSA or the Barracuda Safe Browser, and when the mobile device synchronizes with Barracuda Web Filter settings. See the **ADVANCED > Remote Devices** page to view.
- Bypassing YouTube for Schools - see Exceptions to Policy below.

LDAP Authentication - New DC Agent

- The new DC Agent 6.0 provides the same integration as before of your domain controller with the Barracuda Web Filter to enable use of single sign-on for your users. Except for remote installations (see below), the DC Agent requires Microsoft Windows Server 2003 with Service Pack 2 (SP2) or higher. See the **USERS/GROUPS > Authentication** page to configure. For deployment, see [How to Get and Configure the Barracuda DC Agent](#).
 - Windows Server 2012 support.
 - New easy-to-use graphical interface.
 - Improved stability and performance.
 - Requires Microsoft .Net Framework 4.0 Client Profile.
 - Remote installation requires Microsoft Windows 7 or higher. Also note that, for the remote installation of DC Agent, you **MUST** be a domain member to query the server

System Status

- **Status page enhancement** - The new Link Status section provides icons for LAN, WAN and AUX port connections where applicable. Hover the mouse over one of the port icons for a tool tip showing: eth1/eth2, IP Address, MAC Address, throughput, link Speed, duplex. Note that, for the Barracuda Web Filter FX, only the LAN connection will be present.
- Creating Exceptions to Policy From the **BLOCK/ACCEPT > Exceptions** page.

HTTPS Filtering and Policy

- **HTTPS-based Policy** - You can now create policy exceptions specific to HTTP traffic, HTTPS, or another legitimate URI scheme (e.g. SMB:\\) using the Protocol field. Note that Enable HTTPS Filtering must be enabled on the **BLOCK/ACCEPT > Configuration** page if HTTPS is selected.

Exceptions to Policy

- **List of Exceptions table** - New multiple-select capability allows for selecting and moving multiple items at one time to change order of precedence of exceptions.
- **YouTube for Schools Bypass** - You can create an exception for a specific set of users to bypass the YouTube for Schools feature if it is enabled. This feature enables creation of a school account for access to YouTube EDU content as well as a customizable playlist of videos that will be viewable only within your own school network. You can learn more about what YouTube for Schools offers by visiting the YouTube for Schools website. For information about configuring this feature, see the Barracuda TechLibrary article [How to Set Up YouTube for Schools](#).

What's New in Version 6.0

Web Interface

- Improved applications filtering interface. The **BLOCK/ACCEPT > Applications** page now provides block and allow actions for specific application traffic that is not browser-based. For example: Skype, Pandora, Adobe Acrobat, FTP. You can select from a pre-defined list of non-HTTP Web applications as well as submit a suggestion of an application that the Barracuda Web Filter should block.
- Revised layout for **ADVANCED > Remote Filtering** page Barracuda Web Security Agent settings. Includes new support for Mac OS-X with the Barracuda Web Security Agent.

Web Application Control

- Provides block and allow actions for web-based applications such as Facebook, MySpace, Twitter and others. You can, for example, allow users in the organization to log into Facebook to view and make status updates and use chat, while blocking games, shares and other Facebook apps to protect your network from viruses and malware. Couple this functionality with the powerful Web Application Monitoring feature, which allows you to capture these social media interactions for archiving. Configure from the new **BLOCK/ACCEPT > Web App Control** page.

Web Application Monitoring (Available on the Barracuda Web Filter 610 and higher)

- Enables the capture of chat, email, user registrations and social media interactions on social media portals for the purpose of archiving and searching by source or content. The archiving repository can be your Barracuda Message Archiver, your Microsoft Exchange Server journaling tool or, for example, a system administrator email address. Configure from the **BLOCK/ACCEPT > Web App. Monitor** page.
- Specify a Notification Email Address for archiving selected actions and associated content. The Barracuda Web Filter will package each interaction as an SMTP message and email it to this address, which can then be marked for archiving. Use the Barracuda Message Archiver or other archiving solution to index messages for searching by source or content. Alerts can then be generated per policy you set in your archiving solution.

Networking

- Dual Bridge Mode, providing dual LAN/WAN bridges for Barracuda Web Filter 1010.

Enhanced HTTPS Filtering

- Support for HTTPS with WCCP deployment. HTTPS traffic will be filtered in WCCP deployment mode if Enable HTTPS Filtering is enabled from the **BLOCK/ACCEPT > Configuration** page.
- SSL Inspection. The Barracuda Web Filter can decrypt HTTPS traffic at the URL level and apply policy accordingly. For Forward Proxy deployments only, this feature is configurable from the **BLOCK/ACCEPT > Configuration** page. To use SSL Inspection, you must also either upload a trusted or create a self-signed root certificate to install on all client browsers and other Barracuda Web Filters (when using linked management). Configure SSL Inspection certs from the **ADVANCED > SSL Inspection** page. Available on the Barracuda Web Filter 610 and higher.

What's New in Version 5.0

Role Based Administration

- Configurable from the **ADVANCED > Delegated Admin** page
- Ability to grant specific LDAP users access to the Barracuda Web Filter Web interface
- Temporary whitelisting feature enabling an authorized user to temporarily allow content blocked by policy

Policy

- Safe Browsing YouTube for Schools support. See [How to Set Up YouTube for Schools](#).
- LDAP OU (organizational unit) based policy and reporting
- Pre-population of Applications to Filter on the **ADVANCED > Remote Filtering** page
- New email alerts summarizing policy violations

Web Security Agent

- Support for Policy Lookup Only Mode
- Ability to synchronize configuration via a non-default HTTPS port

Reporting and Logs

- Enhanced performance
- Support for scheduling reports in non-English languages

- Some reports renamed for consistency and readability
- The Calendar picker on BASIC > Reports page is compatible with Chrome browsers
- Improved alignment for text based reports
- Support of PDF report format for the IE7 browser
- Ability to use a non-standard SMB port for External Servers
- Use of the HH:MM:SS time format for logs exported to CSV file
- Support for export of filtered Web Logs to CSV format for IE8 and Firefox browsers
- Support for the IE9 browser for web interface log pages

Authentication

- Ability to configure Open Directory specifically
- Block page now supports more than 10 Existing Authentication Services
- Support for NTLM Authentication with Windows 2008 R2 Server

Miscellaneous

- Backward Compatibility Support for OSX 10.5
- Improved DNS resolution

Release Notes

Please Read Before Upgrading

CAUTION: Do NOT upgrade to this version of the 7.0 release if any of the following apply to your Barracuda Web Filter installation:

- You use one of your Barracuda Web Filters as a reporting unit that receives syslog output from other Barracuda Web Filters.



Important: Make a Backup First

Before installing any firmware version, back up your configuration and read all release notes that apply to versions more recent than the one currently running on your system. **Important:** A configuration backup made in version 4.4 and lower *cannot* be restored to version 4.5 and higher.

Do not manually reboot your system at any time during an upgrade, unless otherwise instructed by Barracuda Networks Technical Support. The upgrade process typically takes only a few minutes after the upgrade is applied. If the process takes longer, please contact Technical Support for further assistance.

Upgrading to Version 6.x and 7.x

- After upgrading to version 6.0, reverting back to the previous firmware version or to the factory installed version is not possible.
- Note that the **BASIC > WebLog** and **BASIC > Application Log** pages get cleared on updating from 6.0.0 to 6.0.1, but the log data is still intact and will still appear in reports.

Firmware Version 7.0

For a list of new features, please see **What's New in the Barracuda Web Filter** at <http://techlib.barracuda.com/x/J4K-AQ>.

Version 6.0.1

Version 6.0.1.012

- Enhancement: Improved memory usage on the Barracuda Web Filter 210.
- Enhancement: Improved block page delivery when the number of blocked URLs is high.
- Fix: Upgrades to the Barracuda Web Filter 1010 no longer require additional patches.

Version 6.0.1.011

- Fix: Application Control using the Packet Inspection method works as expected.

Version 6.0.1.010:

- Fix: Performance enhancements for traffic filtering and management interfaces.

Version 6.0.1.009:

- Enhancement: DC Agent version 6.0.0.32 now installs, if necessary, the Microsoft .Net Framework 4.0 Client Profile.
- Enhancement: Download links for Web Security Agent are upgraded for better usability on the ADVANCED > Remote Filtering page.
- Fix: Barracuda Cloud Control no longer displays links from within the Barracuda Web Filter view to download the Barracuda Web Security Agent or the Barracuda DC Agent. These agents must be downloaded via the local web interface of each Barracuda Web Filter. [BNYF-6272]
- Fix: Improved policy engine stability. [BNYF-6257]
- Fix: The Barracuda Web Filter properly re-categorizes domains when many custom categories are present, resulting in proper policy enforcement. [BNYF-6239]
- Fix: Web Log updates and filters as expected. [BNYF-6244], [BNYF-6282], [BNYF-6256]
- Fix: Web Application Monitor notifications are sent out as expected. [BNYF-6294]
- Fix: HTTPS access to the web interface (ADVANCED > Secure Administration page) works as expected. [BNYF-6233]
- Fix: Configuration Backup while using the primary IP address as the local service address works as expected. [BNYF-6291].

Version 6.0

Version 6.0.0.012:

- Enhancement: Improved performance of serving block pages.

Version 5.0.0

Version 5.0.0.016:

- Enhancement: Improved reporting performance.
- Fix: Improved web interface performance at high system loads.

Deployment Options

You can deploy your Barracuda Web Filter so it is inline with your core network components or you can deploy the system as a forward proxy. The following sections provide a brief overview of inline and forward proxy deployment types, including virtual machine deployment. Barracuda Networks recommends reviewing and determining the best deployment option for your network before continuing with installation. As you determine the best deployment for your organization, please also see [Step 1: Network Considerations](#).

In this Section

- [Inline Pass-Through \(Transparent\) Mode Deployment](#)
- [Forward Proxy Deployment of the Barracuda Web Filter](#)
- [High Availability - Clustering the Barracuda Web Filter](#)
- [Inline Pass-through With Pre-existing Proxy Deployment](#)
- [Connecting Inline to your Network with a Pre-existing Proxy Server](#)
- [Policy-Based Routing](#)
- [Source-Based Routing](#)
- [VLAN Deployments](#)
- [Virtual Deployment](#)
- [WCCP Deployment 6.x](#)

Inline Pass-Through (Transparent) Mode Deployment

Inline pass-through is the recommended type of deployment for the Barracuda Web Filter appliance (not supported by the Barracuda Web Filter Vx virtual machine) because it provides the strongest level of protection against spyware. In this deployment, the Barracuda Web Filter is directly inline with your core Internet network components, and all network traffic to the Internet passes through the Barracuda Web Filter. In this mode, your Barracuda Web Filter is able to:

- Filter and scan all Internet traffic requests
- Perform content filtering and scan downloads for spyware and viruses
- Detect and block outbound spyware protocol requests
- Scan all outbound traffic for spyware activity on all ports to detect infected clients
- Perform [SSL Inspection](#) - i.e. scanning of HTTPS traffic at the URL level- **on the Barracuda Web Filter 910 and higher** (the 610 and 810 require proxy deployment for this feature)

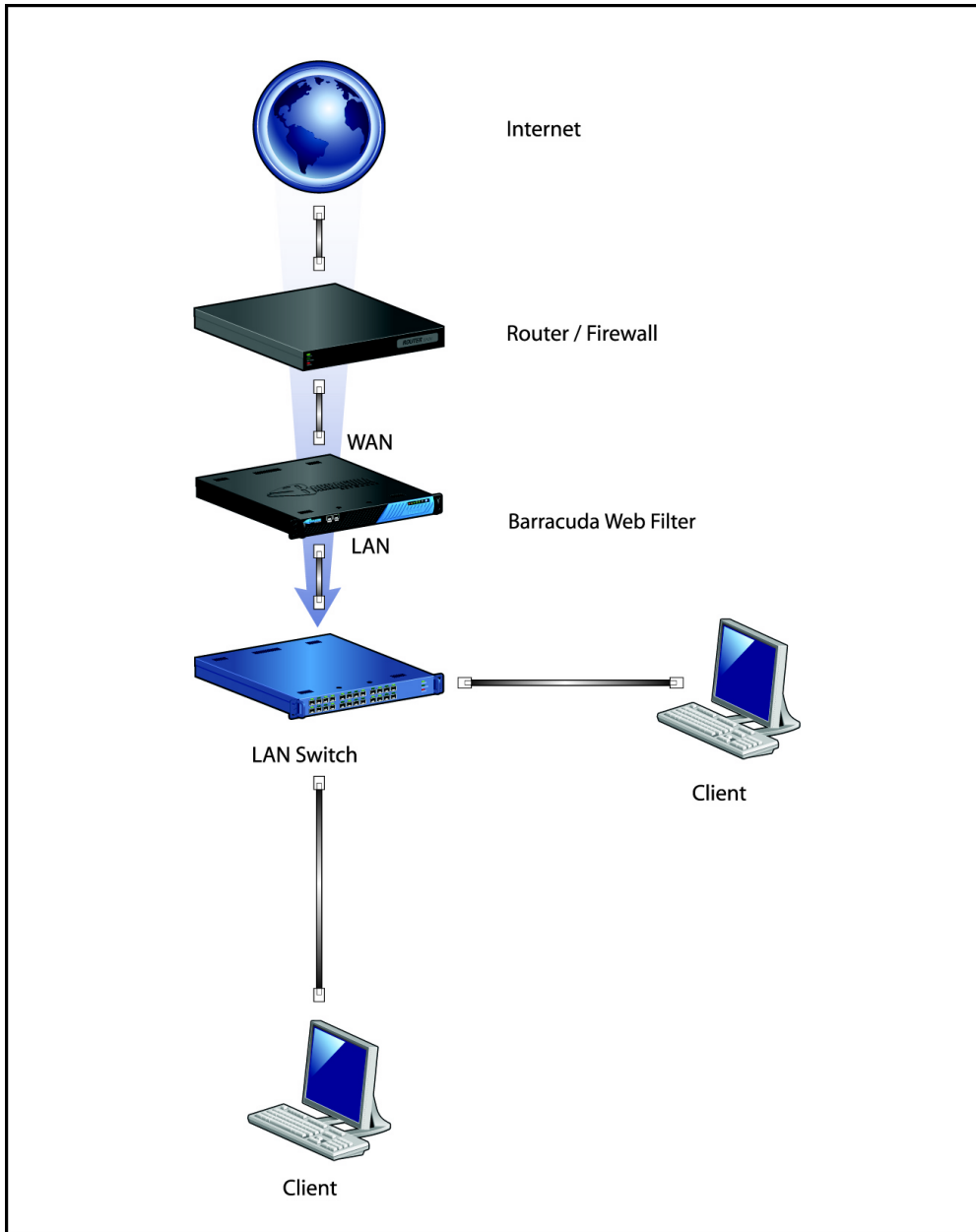
Inline pass-through deployment requires you to have an understanding of your network topology because even though the Barracuda Web Filter acts as a proxy, it does not participate in routing protocols. As a result, you may need to set up [static routes](#) in your Barracuda Web Filter so it knows how to properly route traffic.

Per Figure 1 below, you'll typically route traffic from your switch or router, via the Barracuda Web Filter, to the internal IP address of your firewall or another device used for routing on the WAN side of the Barracuda Web Filter.

The following table describes the advantages and disadvantages of deploying your Barracuda Web Filter in inline pass-through mode.

Advantages	Disadvantages
Supports application blocking.	May require setting up static routes in your Barracuda Web Filter.
Supports automatic pass-through mode in the event of a system failure (model 310 and above).	Initial setup requires an interruption to network traffic while you make necessary cabling changes.
Does not require users to configure proxy server settings in their Web browser.	
Uses perimeter transparency mode that exposes client IP addresses (supports corporate firewall rules).	

Figure 1: Inline Pass-through Deployment.



Forward Proxy Deployment of the Barracuda Web Filter

A key advantage of this deployment is that initial setup does not require any interruptions to your network traffic. However, be aware that, in a forward proxy deployment, only HTTP/HTTPS Internet traffic passes through the Barracuda Web Filter. As such, in this mode the Barracuda Web Filter does not scan non-HTTP traffic for viruses and spyware, nor does it block applications. Please see [Limitations of This Deployment Type](#) below for more details. **Note that you must use either this deployment or WCCP Deployment for the Barracuda Web Filter Vx.**

How This Deployment Works

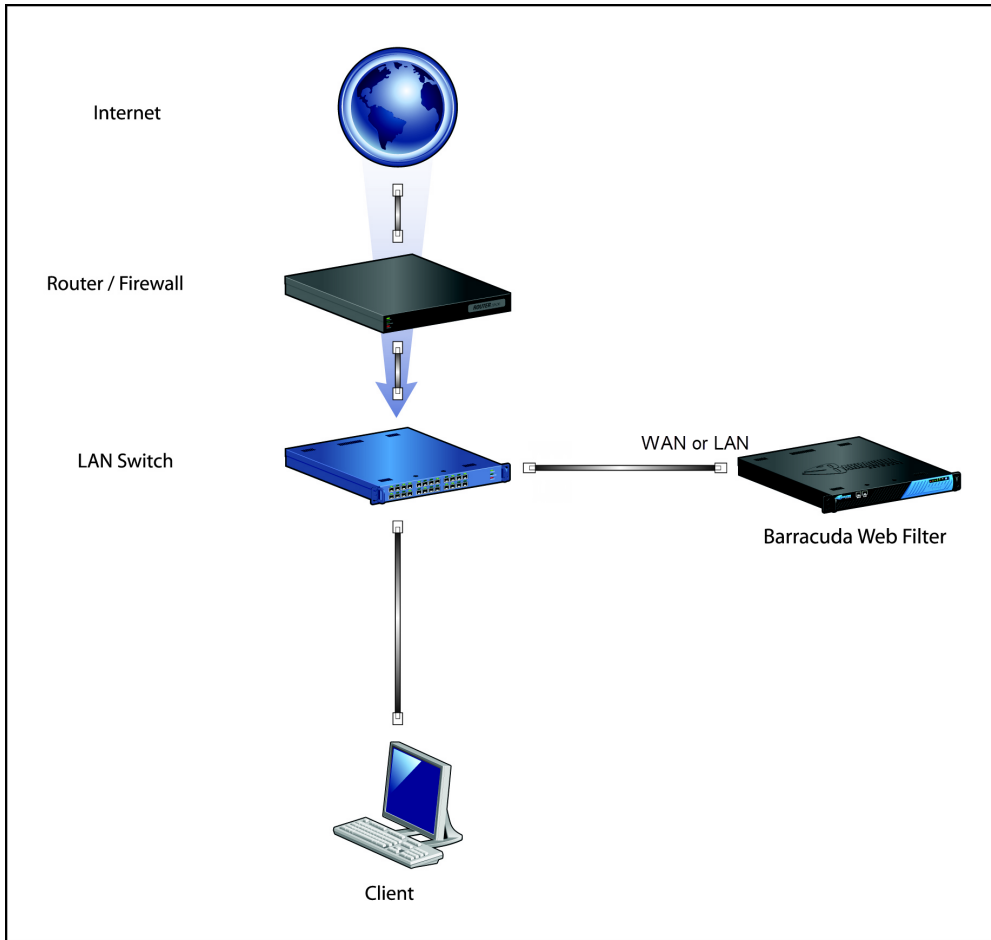
The Forward Proxy deployment uses a proxy, the Barracuda Web Filter, as an intermediary between a client and the Internet to protect the client from being visible from the Internet. After the Barracuda Web Filter processes clients' HTTP/HTTPS requests, it sends the requests out directly to the Internet. When deployed as a forward proxy, the Barracuda Web Filter shows all HTTP/HTTPS traffic as coming from its own IP address instead of from the individual client IP addresses as is done in the inline pass-through deployment.

Barracuda Networks recommends deploying the Barracuda Web Filter in forward proxy mode in the following situations:

- You need to replace an existing forward proxy (such as Microsoft ISA Server) with the Barracuda Web Filter.

- You do not want the Barracuda Web Filter to reside inline with all your network traffic and are satisfied with the system **only scanning HTTP/HTTPS traffic** for viruses and spyware.

The figure below illustrates a basic installation using the Forward Proxy Deployment.



Configuring Forward Proxy Mode

To set up the Barracuda Web Filter as a forward proxy without placing it inline, you must manually direct all outgoing web traffic through the Barracuda Web Filter.

1. Connect either the WAN or LAN port of the Barracuda Web Filter to the same switch as the network gateway (just one network hop away).
2. Configure the browsers of all users with the IP address of the Barracuda Web Filter as their forward proxy server on port 3128. If you wish to use a different port, you can change the **Proxy Port** setting on the **ADVANCED > Proxy** page.
3. From the **BASIC > IP Configuration** page of the web interface, set the **Operating Mode** to **Active**. Note that **Audit mode does not apply to this deployment**; in either **Audit** or **Active** modes, traffic will be logged and policy will be applied.

Limitations of This Deployment Type

Because the Barracuda Web Filter only scans outbound HTTP/HTTPS traffic in this deployment, the system *cannot* perform the following functions in Forward Proxy mode:

- Block access to applications listed on the **BLOCK/ACCEPT > Applications** pages.
- Block access to applications that use the destination IP address specified on the **BLOCK/ACCEPT > IP Block/Exempt** page.
- Block access to applications that use the destination port specified on the **BLOCK/ACCEPT > IP Block/Exempt** page.
- Inspect outbound traffic for spyware infection activity.
- Scan non-HTTP traffic for viruses and spyware.

High Availability - Clustering the Barracuda Web Filter

If you are not using a WCCP deployment, you can cluster, or link two or more

Barracuda Web Filters together to provide high availability. Using the Linked Management feature, clustering multiple Barracuda Web Filters automatically synchronizes most configuration settings and policy among the systems.

Related Articles
Forward Proxy Deployment

Clustered systems can be geographically dispersed and do not need to be co-located on the same network. Note that Linked Management does not provide load-balancing functionality. The Barracuda Web Filter uses ports 8001 and 8002 to synchronize configuration between linked systems.

Use the **ADVANCED > Linked Management** page to link multiple Barracuda Web Filters. This feature is available on the Barracuda Web Filter 410 and above.

Some network environments may not be suitable to linking multiple Barracuda Web Filter systems together. For example, if you have multiple network segments that each require different policies, it may be better to provide a dedicated, unlinked Barracuda Web Filter for each segment. This way you can configure each Barracuda Web Filter without the configuration settings propagating to the other systems.

High Availability Deployment Options

Consider the following methods for deploying clustered Barracuda Web Filters for failover and, in some cases, load balancing, depending on your OS and network configuration:

Method 1: Use a PAC file with a GPO. Create a PAC file on your network and use Windows GPO to tell client browsers where to locate the PAC file. The PAC file indicates the proxy server URL (Barracuda Web Filter) to which the browsers are to proxy user requests. In the PAC file you can also specify URL exceptions that won't accept proxied requests. The advantages of this method are:

In the PAC file you can specify a primary and secondary Barracuda Web Filter IP address so that if one is unavailable, the browser will proxy to the other.

You can specify URL exceptions in the PAC file for which you want user requests to bypass the Barracuda Web Filter. These exceptions might include intranet sites or other sites that accept connections from particular 'allowed' IP addresses.

Method 2: Use a PAC file with autodetection via DHCP or DNS. This is an alternative to using a Windows GPO to propagate PAC file information to client browsers. With DHCP, updates to your clients can include PAC file location information along with dynamically assigned IP addresses and other attributes. Configure this in your DHCP server settings. With DNS, you can add a hostname wpad (web proxy auto discovery) to your domain name in the DNS server. The wpad contains the IP address where the PAC file is hosted on the network.

Method 3: Use a Barracuda Load Balancer. This deployment makes sense if your network requires dynamic traffic load balancing. In this case, your client browsers will proxy traffic to a virtual IP address - the load balancing device - which then load balances traffic to the Barracuda Web Filters. The Barracuda Load Balancer provides failover and dynamic traffic load balancing.

Method 4: Use Multiple A Records. For each Barracuda Web Filter in the cluster, make an A record in your DNS server with the same hostname. Depending on what IP address to which the user's machine resolved the hostname, they may get a proxy error.

Data Propagated to the Linked Systems

Linking systems together not only makes it easier to manage multiple Barracuda Web Filters, but it also provides 100 percent redundant coverage of the propagated configuration and policy (Block/Accept) data. Table 2.2 identifies the data that is propagated to the other clustered systems when a new system joins.

Propagated Data	Data Not Propagated
------------------------	----------------------------

System settings (global and domain) configured through the web interface. This includes the block/accept filters.

- System IP configuration (IP address, subnet mask, default gateway, and DNS server) configured on the **BASIC > IP Configuration** page.
- System password and time zone as configured on the **BASIC > Administration** page.
- Cluster hostname and cluster local host map configured on the **ADVANCED > Linked Management** page.
- Static route settings as configured on the **BASIC > IP Configuration** page.
- Branding image and image URL as configured on the **ADVANCED > Appearance** page.
- VLAN configuration settings as configured on the **ADVANCED > Advanced Networking** page.
- Source-based routes as defined using the **IP Routing** feature. See the **ADVANCED > Advanced Networking** page.
- SSL Inspection Certificates as configured on the **ADVANCED > SSL Inspection** page.
- Kerberos and NTLM settings on the **USERS/GROUPS > Authentication** page.

Switching a System to Standby Mode

You can also use the **ADVANCED > Linked Management** page to switch a clustered system from **Active** to **Standby** mode. When a system is in **Standby** mode, it does not synchronize its configuration with the other active systems in the cluster.

Barracuda recommends switching a system to **Standby** mode when you need to:

- Upgrade the firmware of all systems in a cluster. If a system is part of a cluster, Barracuda recommends changing the system's mode to **Standby** before you upgrade its firmware, and then repeat this process on each system in the cluster. After the firmware on each system has been upgraded, you can then change the mode on each system back to **Active**. Changing a linked system to **Standby** mode before upgrading prevents a system on a more recent firmware version from trying to synchronize its configuration with a system on an earlier firmware version.
- Perform maintenance that requires a system to be powered down or disconnected from your network. For example, if you need to physically move a Barracuda Web Filter, you should change its mode to **Standby** so the other systems in the cluster do not try to synchronize their configuration while the system is down.

Inline Pass-through With Pre-existing Proxy Deployment

This deployment type is much less common than either Inline mode or Forward Proxy mode, and involves deploying the Barracuda Web Filter as an inline device that uses a pre-existing proxy server on your network. This type of deployment is not recommended because it breaks the following features of the Barracuda Web Filter:

- Infection reports do not display the IP addresses of infected clients.
- Infected clients cannot be automatically redirected to the [Barracuda Malware Removal Tool](#).

To resolve these issues, Barracuda Networks recommends that you remove your pre-existing proxy server and deploy the Barracuda Web Filter inline as described in [Inline Pass-Through \(Transparent\) Mode Deployment](#).

The Barracuda Web Filter can be placed on the client or the server side of the existing proxy server. If the existing proxy server is performing user authentication, then the Barracuda Web Filter must be placed on the server side of the proxy. In this deployment, the Barracuda Web Filter detects all network traffic. The proxy server connects directly to the Barracuda Web Filter LAN port. This connection may require a crossover cable. No special port or IP address is required.

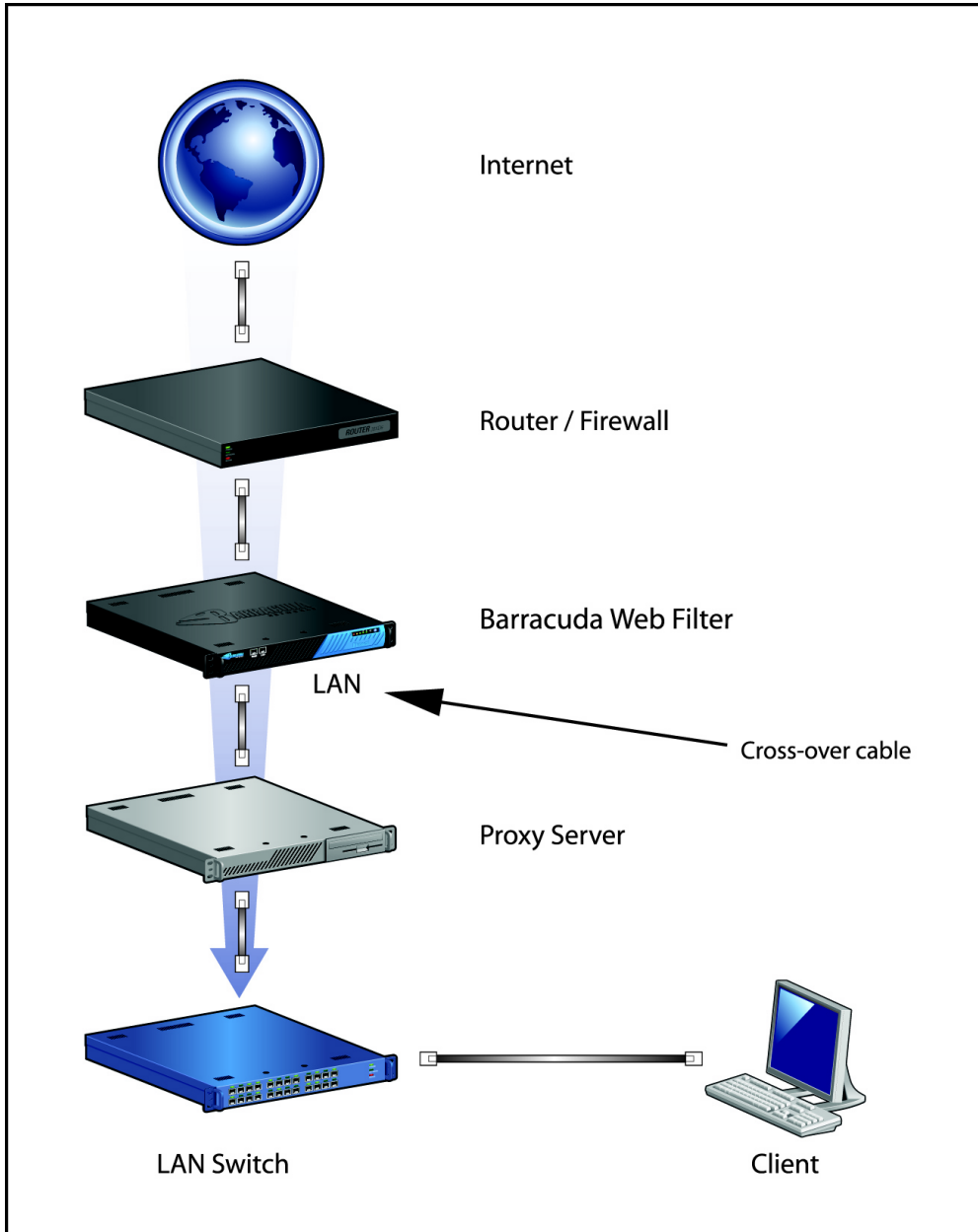
The Barracuda Web Filter scans for all inbound and outbound HTTP traffic from the proxy server. All outbound traffic on other ports is scanned for normal spyware communication. However, since the proxy server will most likely hide user identity, the Barracuda Web Filter cannot apply any user, group or IP based policies. Figure 1 below illustrates this deployment type.

Alternatively, the Barracuda Web Filter can be placed inline on the client side of the existing proxy server. The LAN Switch can be connected to the LAN port of the Barracuda Web Filter and the WAN port of the Barracuda Web Filter can be connected to the Proxy Server. This will ensure

that the Barracuda Web Filter can identify users before the requests are proxied. In this configuration, you may have to ensure that the Barracuda Web Filter passes client IP addresses through to the proxy server or that the proxy server can handle requests coming from the Barracuda Web Filter's IP address. However, this configuration may not work when the proxy server is performing strong user authentication.

The placement of your pre-existing proxy server and its functionality will have an impact on the Barracuda Web Filter deployment. Some configurations may require technical assistance from Barracuda Networks Technical support. Please see [Contacting Barracuda Networks Technical Support](#). To connect your Barracuda Web Filter with this deployment mode, see [Connecting Inline to your Network with a Pre-existing Proxy Server](#).

Figure 1: Inline Passthrough with Pre-existing Proxy Server Deployment.



Connecting Inline to your Network with a Pre-existing Proxy Server

This article follows [Inline Pass-through With Pre-existing Proxy Deployment](#).

To set up the Barracuda Web Filter inline with your existing proxy server, place the proxy server between the Barracuda Web Filter and your internal network switch.

If you have a proxy server, most HTTP requests are routed from your internal network through the proxy server to the Barracuda Web Filter.

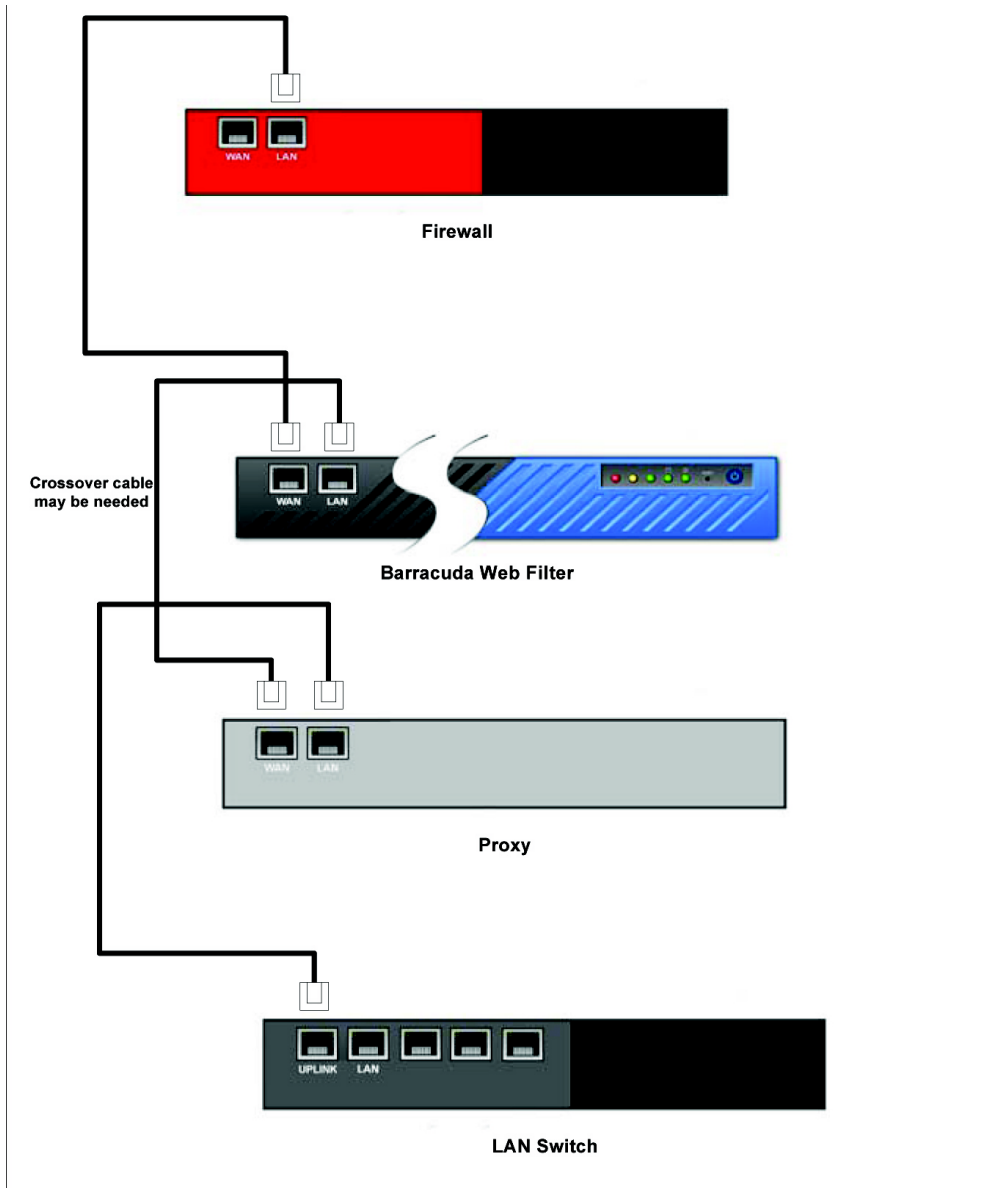
When a website responds, the responding traffic goes through the Barracuda Web Filter, which filters any spyware and viruses before allowing the traffic to go through the proxy server and back to the clients.

The Barracuda Web Filter has been tested with Microsoft ISA and Squid proxy servers.

To connect your Barracuda Web Filter and existing proxy server to your network:

1. Connect your LAN port from your proxy server to the **Uplink** port of your internal network switch.

Figure 1: Proxy Behind the Barracuda Web Filter.



2. Connect the Ethernet cable from your WAN port of your proxy server to the LAN port on the Barracuda Web Filter. Note that you do not need to configure the WAN port. The Barracuda Web Filter creates an Ethernet bridge between the WAN and LAN ports.

i A crossover cable may be needed if your corporate firewall does not have a switchable port and therefore cannot switch between RX and TX. Another solution is to place a switch between the corporate firewall and the Barracuda Web Filter.

3. Connect an Ethernet cable from the WAN port on the Barracuda Web Filter to the LAN port on your firewall.
4. Go to the **BASIC > IP Configuration** page in the web interface, and set the **Operating Mode** to **Active**.

Policy-Based Routing

Transparently Routing Web Traffic to the Barracuda Web Filter

This article demonstrates how to route traffic to the Barracuda Web Filter as a proxy without requiring proxy rules to be pushed out to all clients on the network. This method allows the Barracuda Web Filter to forward HTTPS (443) traffic in addition to standard HTTP traffic, which cannot be done using other methods of transparent proxy routing.

The example shown in this article assumes a configuration with a Cisco Router with built-in Firewall Security Module (FWSM), but it should work with any routing equipment supporting Policy-Based Routing (PBR).



Run this command on the router

Text in yellow boxes shows commands that need to be run on the router.

Related Articles

- [Deployment Options](#)
- [WCCP Deployment 6.x](#)
- [Source-Based Routing](#)

Installation of the Barracuda Web Filter

For this configuration, you will need to connect the Barracuda Web Filter LAN interface to its own dedicated port on the router. Give the Barracuda Web Filter an IP address in its own dedicated IP subnet, and assign a gateway IP to the router interface that it is connected to. An example network is shown here:

Barracuda IP Address:

10.100.3.2/30 gateway 10.100.3.1

Internal Ranges:

10.100.1.0/24 (VLAN_1)

10.100.2.0/24 (VLAN_2)

Router Configuration

Step 1. Define 2 access lists

You must define two access lists because you need to create a route-map for both the internal and external interfaces of the router. These rules describe which clients will be routed to the Barracuda Web Filter. Your routing rules will be different based on whether this is outbound or inbound traffic.



Run these commands on the router

[Inbound]

```
ip access-list extended HTTP(S)_Proxy_Inbound
permit udp any eq domain 10.100.0.0 0.0.255.255
permit tcp any eq 443 10.100.0.0 0.0.255.255
```

[Outbound]

```
ip access-list extended HTTP(S)_Proxy_Outbound
permit tcp 10.100.0.0 0.0.255.255 any eq www
permit tcp 10.100.0.0 0.0.255.255 any eq 443
```

Note that this is routing inbound DNS traffic back through the Barracuda Web Filter. This is the key to making policy-based routing work for HTTPS traffic.

Step 2. Create route maps

Match these route-maps to the access lists you just created. Any traffic matching those lists will have the “match” rule applied to it. In this case, you are modifying the next-hop for the packet to the Barracuda Web Filter’s IP address. Note that you need two route-maps—one for inbound traffic, and one for outbound traffic.

**Run these commands on the router****[Inbound]**

```
route-map HTTP(S)_Proxy_Inbound permit 10
match ip address HTTP(S)_Proxy_Inbound
set ip next-hop 10.100.3.2
```

[Outbound]

```
route-map HTTP(S)_Proxy_Outbound permit 20
match ip address HTTP(S)_Proxy_Inbound
set ip next-hop 10.100.3.2
```

Step 3. Apply route-maps to the interfaces on your router

The inbound route-map you created is applied to the outside (WAN-side) interface on your router/firewall. The outbound route-maps are applied to any internal interfaces on your router/firewall. This includes any sub-interfaces that are connected to client networks that need filtering.

[Inbound]

```
interface FastEthernet0/1
description Test WAN
ip address 1.1.1.2 255.255.255.0
ip access-group Inbound_Rules in
no ip redirects
no ip unreachable
ip nat outside
```

**Run this command on the router**

```
ip policy route-map HTTP(S)_Proxy_Inbound
```

```
duplex auto
speed auto
```

[Outbound]

Note that there are *two* interfaces listed here—one for each VLAN on the test network. The outbound route-map rule needs to be enabled for each internal interface or sub-interface to be filtered. Start with one and test.

```
interface FastEthernet0/0.1
description VLAN_1
encapsulation dot1Q 1
ip address 10.100.1.1 255.255.255.0
ip nat inside
```

**Run this command on the router**

```
ip policy route-map HTTP(S)_Proxy_Outbound
```

```
interface FastEthernet0/0.2
description VLAN_2
encapsulation dot1Q 2
ip address 10.100.2.1 255.255.255.0
ip nat inside
```

**Run this command on the router**

```
ip policy route-map HTTP(S)_Proxy_Outbound
```

Sample Cisco IOS Configuration

```
!
version 12.2
service timestamps debug uptime
```

```
service timestamps log uptime
service password-encryption
!
hostname cisco
!
boot system flash slot1:c3660-ik9o3s-mz.122-32.bin
no logging monitor
enable secret 5 *****
!
username seadmin privilege 15 password 7 *****
ip subnet-zero
ip wccp web-cache redirect-list WCCP
!!
ip ftp username *****
ip ftp password 7 *****
ip domain-name *****
!
ip audit notify log
ip audit po max-events 100
!!
call rsvp-sync
!
!!
!!
fax interface-type fax-mail
mta receive maximum-recipients 0
!!
!
interface FastEthernet0/0
description Test LAN
no ip address
ip nat inside
duplex auto
speed auto
!
interface FastEthernet0/0.1
description Barracuda Systems
encapsulation dot1Q 1
ip address 10.100.1.1 255.255.255.0
ip nat inside
ip policy route-map HTTP(S)_Proxy_Outbound
!
interface FastEthernet0/0.2
description Other OS (Windows, Mac, Linux...)
encapsulation dot1Q 2
ip address 10.100.2.1 255.255.255.0
ip nat inside
!
interface FastEthernet0/0.100
encapsulation dot1Q 100 native
!
interface FastEthernet0/1
description CudaSE.net WAN
ip address 1.1.1.3 255.255.255.0 secondary
ip address 1.1.1.2 255.255.255.0
ip access-group Inbound_Rules in
no ip redirects
```

```
no ip unreachable
ip nat outside
ip policy route-map HTTP(S)_Proxy_Inbound
duplex auto
speed auto
!
interface FastEthernet2/0
description HTTP(S) Proxy
ip address 10.100.3.1 255.255.255.0
duplex auto
speed auto
!
ip nat inside source list Outbound_NAT interface FastEthernet0/1 overload
ip classless
ip route 0.0.0.0 0.0.0.0 1.1.1.1
no ip http server
!
!
ip access-list extended HTTP(S)_Proxy_Inbound
permit udp any eq domain 10.100.0.0 0.0.255.255
permit tcp any eq 443 10.100.0.0 0.0.255.255
ip access-list extended HTTP(S)_Proxy_Outbound
permit tcp 10.100.0.0 0.0.255.255 any eq www
permit tcp 10.100.0.0 0.0.255.255 any eq 443
ip access-list extended Inbound_Rules
permit icmp any any echo
permit icmp any any echo-reply
permit icmp any any source-quench
permit icmp any any packet-too-big
permit icmp any any time-exceeded
permit udp any any gt 1023
permit tcp any any ack
deny ip any any
ip access-list extended Outbound_NAT
permit ip 10.100.1.0 0.0.0.255 any
permit ip 10.100.2.0 0.0.0.255 any
permit ip 10.100.3.0 0.0.0.255 any
deny ip any any
route-map HTTP(S)_Proxy_Inbound permit 10
match ip address HTTP(S)_Proxy_Inbound
set ip next-hop 10.100.3.2
!
route-map HTTP(S)_Proxy_Outbound permit 20
match ip address HTTP(S)_Proxy_Outbound
set ip next-hop 10.100.3.2
!!
dial-peer cor custom
!
!!
!!
line con 0
line aux 0
line vty 0 4
privilege level 15
login local
transport input telnet ssh
line vty 5 15
```

```
privilege level 15
login local
transport input telnet ssh
!
end
```

Source-Based Routing

This configuration is available with any type of Barracuda Web Filter deployment.

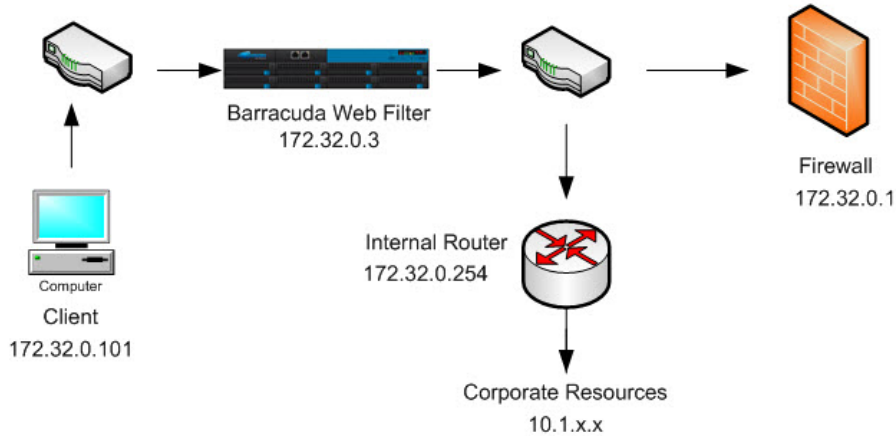
If you have clients or networks that you want to route to the Internet via a different gateway than the default set for the Barracuda Web Filter, you can configure routing by specifying the source and destination IP addresses and gateways using the **IP Routing** feature. See the **ADVANCED > Advanced Networking** page to set up source based routing.

For example, assume your organization has multiple physical locations. The server dedicated to Sales services and resources is located in Los Angeles, and a user in the Sales department at the Atlanta office needs to access those resources on the corporate intranet. Rather than use the default route to the cloud, the user has a secondary exit point (172.32.0.254) that handles all intranet activity across a dedicated connection to the 10.1.0.0/16 (Corporate Resources) network.

Related Articles
<ul style="list-style-type: none"> • Forward Proxy Deployment of the Barracuda Web Filter • Inline Pass-Through (Transparent) Mode Deployment • Directing Traffic to the Barracuda Web Filter Vx • WCCP Deployment 6.x • Policy-Based Routing

The Barracuda Web Filter can look at traffic from the user's machine (client) and direct the traffic to the appropriate gateway based on the source / destination of the traffic. If the packet is bound for a corporate resource, in this instance the Barracuda Web Filter will route it out via the internal router, and all other traffic will proceed to the Internet via the Firewall.

Figure 1: Source Based Routing Provided by the Barracuda Web Filter.



To set up the Barracuda Web Filter per the above example, go to the **IP Routing** section of the **ADVANCED > Advanced Networking** page and configure the following settings. This example configures the Barracuda Web Filter so that all client traffic from the 172.32.0.0 subnet routes to the specified Destination IP Address via the Gateway Address.



The IP addresses used in this example are just that - example addresses for demonstration purposes. Make sure to obtain the correct IP address and netmask values for your network for the actual configuration.

Setting	Meaning and example value
Source IP Address	IP address of client or network to be routed to the alternate gateway. Enter 172.32.0.0 for the subnet the client is coming from.
Source Netmask	Netmask of client or network to route to the alternate gateway; enter 255.255.0.0.
Destination IP Address	Alternate gateway (the corporate intranet, in this case) to which you want to route the client(s) or network. Enter 10.1.0.0.
Destination Netmask	Netmask of alternate gateway. Enter 255.255.0.0.
Gateway Address	Gateway address through which you're routing these clients/networks to the Internet - this would be the address of the Internal Router as shown above. Enter 172.32.0.254.

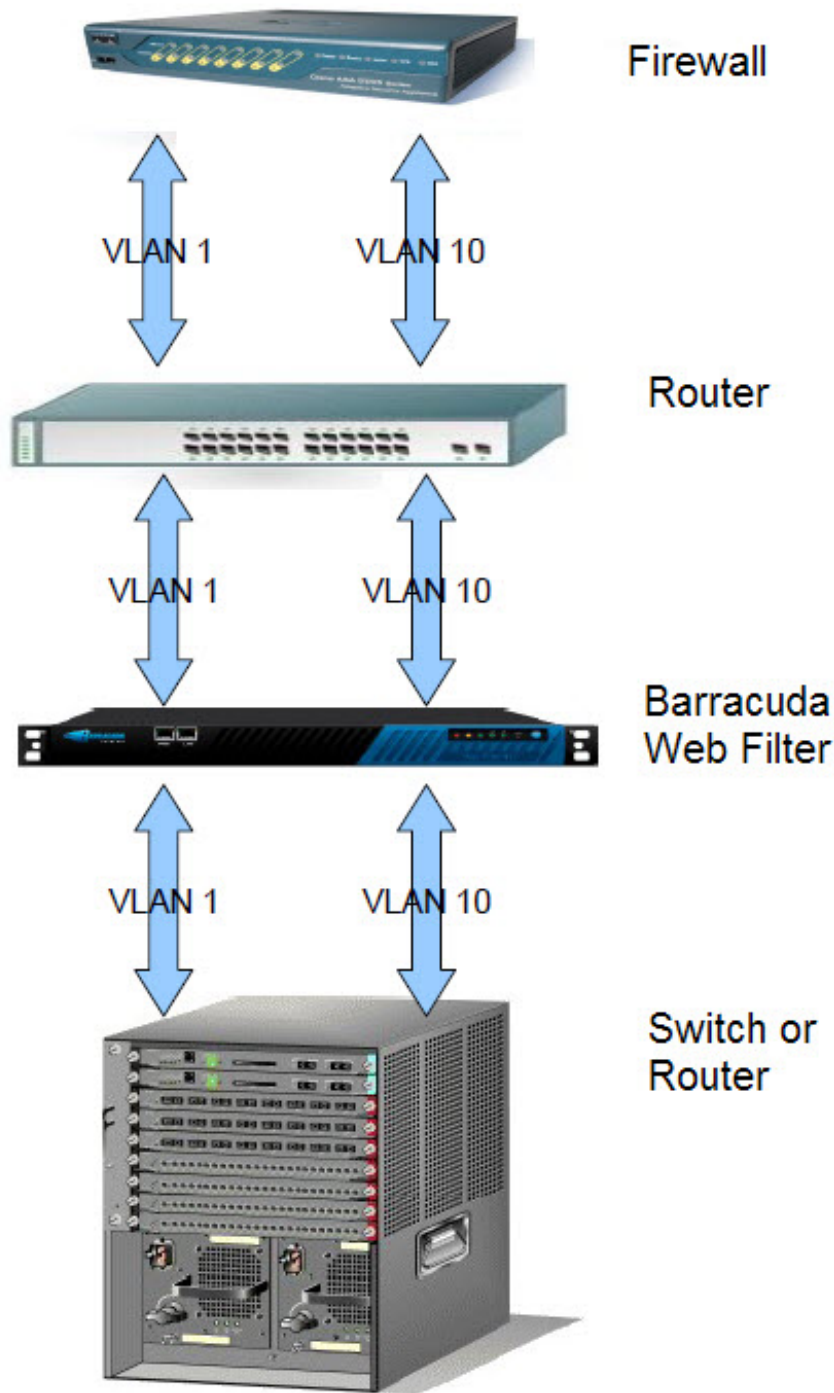
VLAN Deployments

VLAN - Bridge Configuration

The Barracuda Web Filter can filter and route tagged traffic for multiple VLANs to the Internet, preserving the segregation of the VLANs on the WAN port (to the Firewall). In a VLAN deployment, the LAN and WAN ports behave like trunk ports much like a switch or router. For cases in which multiple VLANs need to send traffic through the Barracuda Web Filter to the Internet, and you want to preserve the segregation of these VLANs, use the **Bridge** VLAN deployment, connecting multiple VLANs to the LAN side of the Barracuda Web Filter.

You can also use this deployment configuration to route multiple networks (not VLANs, but untagged traffic) sending outbound traffic through the Barracuda Web Filter.

Figure 1: Bridge VLAN Deployment.



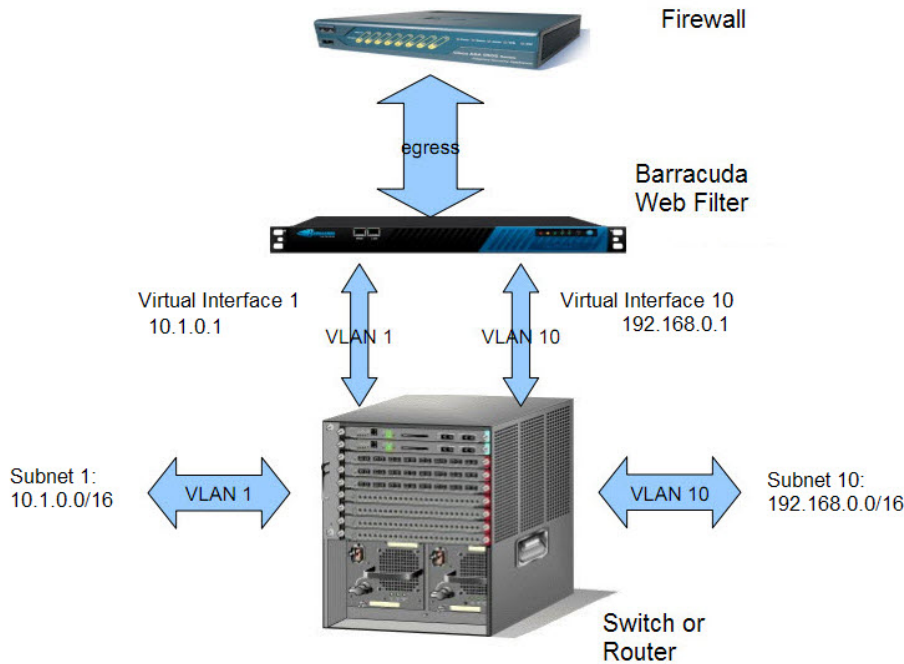
To configure, from the web interface, navigate to the **ADVANCED > Advanced Networking** page. In the VLAN Configuration section, first select Bridge for VLAN Interface. You will need to create a name and ID for each VLAN. For example, if the marketing department is on one VLAN and the finance department is on another, call them MRK_VLAN and FIN_VLAN. Each ID should be unique, in the range specified on the **ADVANCED > Advanced Networking** page.

Every VLAN or subnet that you are routing to the Barracuda Web Filter needs to be associated with a valid IP address, and you make that association by creating a virtual interface. In the Virtual Interfaces section of the **ADVANCED > Advanced Networking** page, you will need to enter the IP address and associated information for each VLAN or subnet. Please see the online help for details on VLAN configuration.

VLAN Deployment - LAN Configuration

If you have multiple VLANs or subnets and you want to filter the traffic but not expose the traffic outside of your network, use the LAN configuration of a VLAN deployment. In this case, all VLAN or subnet traffic is NAT'ed by the Barracuda Web Filter and requests are proxied via the WAN port to the Internet.

Figure 2: LAN-VLAN Deployment.



To configure, from the web interface, navigate to the **ADVANCED > Advanced Networking** page. In the **VLAN Configuration** section, first select *LAN* for **VLAN Interface**. You will need to create a name and ID for each VLAN. Then, using the **Virtual Interfaces** section of the page, associate each VLAN with a Virtual Interface which is defined with an IP address, a Netmask and a Gateway address.

For example, if the marketing department is on one VLAN and the finance department is on another, you might name your VLANs "MRK_VLAN" and "FIN_VLAN". Each ID should be unique, in the range specified on the **ADVANCED > Advanced Networking** page. See the online help for more details on VLAN configuration.

Virtual Deployment

Before setting up your Barracuda Web Filter Vx, you might want to consider the best deployment option for your network configuration:

- Forward Proxy deployment.
- WCCP cache engine on a network with a WCCP capable core routing platform.

Since the Barracuda Web Filter Vx does not support inline deployments, application filtering is not supported. All other features and functions of the Barracuda Web Filter appliance are supported by the Vx. Note that this virtual appliance requires a 64-bit capable host.

In this Section

- **Step 1: Select Your Hypervisor Package:**

Download Package Type	Hypervisor Compatibility
OVF Package	<ul style="list-style-type: none">• VMware ESX and ESXi ("vSphere Hypervisor") versions 4.0, 4.1, 5.0, 5.1• VMware ESX and ESXi version 3.5
VMX Package Deployment	<ul style="list-style-type: none">• VMware Server 2.0+• Workstation 6.0+, Player 3.0+• Fusion 3.0
XVA Package Deployment	<ul style="list-style-type: none">• Citrix XenServer 5.5+

- **Step 2: Getting Your Virtual Machine Up and Running:**

- [Quick Start Guide](#).

- **Step 3: Get Traffic Flowing:**

- [Directing Traffic to the Barracuda Web Filter Vx](#)

- **Managing Your Virtual Machine:**

- [Adding Disk Space, Drives and RAM for Your Virtual Appliance](#)
- [Backing Up Your Virtual Machine System State](#)

Hypervisor Compatibility and Deployment - OVF Package

Hypervisor Compatibility

This package's virtual appliance runs under the following hypervisors:

- VMware ESX and ESXi ("vSphere Hypervisor") versions 4.0 and 4.1
- VMware ESX and ESXi version 3.5
- Sun/Oracle VirtualBox and VirtualBox OSE version 3.2

Deploying the Virtual Appliance With Your Hypervisor

ESX(i) 3.5:

Use the OVF file ending in:

-35.ovf

for this environment.

1. From the **File** menu in the VMware Infrastructure client, choose **Virtual Appliance -> Import**
2. Select **Import from file:** and navigate to the file BarracudaWebFilter-vm3.1.0-fw__FIRMWARE__-20120327-35.ovf.
3. Clicking **Next**, review the appliance information, End User License Agreement, and set the name of the virtual appliance to something useful to your environment. Click **Finish**.
4. Once your appliance has finished importing, right-click it and choose **Open Console** and then click the green arrow to power on the virtual appliance.
5. Follow the [Quickstart Guide - Vx](#) instructions to provision your virtual appliance.

ESX(i) 4.x:

Use the OVF file ending in:

-4x.ovf

for this environment.

1. From the **File** menu in the vSphere client, choose **Deploy OVF Template...**
2. Select **Import from file:** and navigate to the file BarracudaWebFilter-vm3.1.0-fw__FIRMWARE__-20120327-4x.ovf.
3. Clicking **Next**, review the appliance information, End User License Agreement, and set the name of the virtual appliance to something useful to your environment. Set the network to point to the target network for this virtual appliance.
4. Once your appliance has finished importing, right-click it and choose **Open Console** and then click the green arrow to power on the virtual appliance.
5. Follow the [Quickstart Guide - Vx](#) instructions to provision your virtual appliance.

VirtualBox:

Use the OVF file ending in:

-4x.ovf

for this environment.

1. From the **File** menu in the VirtualBox client, choose **Import Appliance**.
2. Navigate to the file BarracudaWebFilter-vm3.1.0-fw__FIRMWARE__-20120327-4x.ovf
3. Use the default settings for the import and click **Finish**.
4. Start the appliance.
5. Follow the [Quickstart Guide - Vx](#) instructions to provision your virtual appliance.

Hypervisor Compatibility and Deployment - VMX Package

Hypervisor Compatibility

This package's virtual appliance runs under the following hypervisors:

- VMware Server 2.0+
- Workstation 6.0+, Player 3.0+
- Fusion 3.0+

Deploying the Virtual Appliance With Your Hypervisor

Server 2.x:

1. Put the files ending in **.vmx** and **.vmdk** into a folder in your datastore (which you can locate from the **Datastores** list on your server's summary page).
2. From the VMware Infrastructure Web Access client's **Virtual Machine** menu, choose **Add Virtual Machine to Inventory**.
3. Navigate to the folder used in step 1 and click the file **BarracudaWebFilter.vmx** from the list under **Contents**. Click **OK**.
4. Start the appliance.
5. Follow the [Quickstart Guide - Vx](#) instructions to provision your virtual appliance.

Player 3.x:

1. From the **File** menu, choose **Open a Virtual Machine**.
2. Navigate to the file BarracudaWebFilter.vmx
3. Use the default settings and click **Finish**.
4. Start the appliance.
5. Follow the [Quickstart Guide - Vx](#) instructions to provision your virtual appliance.

Workstation 6.x:

1. From the **File** menu, choose **Open a Virtual Machine**.
2. Navigate to the file BarracudaWebFilter.vmx
3. Use the default settings and click **Finish**.
4. Start the appliance.
5. Follow the [Quickstart Guide - Vx](#) instructions to provision your virtual appliance.

Fusion 3.x:

1. From the **File** menu, choose **Open a Virtual Machine**.
2. Navigate to the file BarracudaWebFilter.vmx
3. Use the default settings and click **Finish**.
4. Start the appliance.

5. Follow the [Quickstart Guide - Vx](#) instructions to provision your virtual appliance.

Hypervisor Compatibility and Deployment - XVA Package

Hypervisor Compatibility

This package's virtual appliance runs under the following hypervisors:

- Citrix XenServer 5.5+

Deploying the Virtual Appliance With Your Hypervisor

1. From the **File** menu in the XenCenter client, choose **Import VM...**
2. Browse to the file `BarracudaWebFilter-<version#>-fw__FIRMWARE__-<version#>.xva` and choose the **Exported template** radio button.
3. Clicking **Next >**, review the template information and click **Finish** to import the template.
4. Right-click the resulting template and choose **New VM...**
5. Follow the [Quick Start Guide - Vx](#) instructions to provision your virtual appliance.

Barracuda Web Filter Vx Quick Start Guide

Make sure you have completed deployment of your hypervisor before continuing with the steps below. You will need only a single virtual NIC on your virtual appliance.

Once your virtual appliance has been deployed, it's time to provision it. You will need your Barracuda Vx license token. You should have received this via email or from the website when you downloaded the Barracuda Web Filter Vx package. If not, you can request an evaluation on the Barracuda Networks website at <http://www.barracuda.com>. The license token looks similar to the following: "01234-56789-ACEFG" (without the double quotes).

Related Articles

- [Directing Traffic to the Barracuda Web Filter Vx](#)
- [Adding Disk Space, Drives and RAM](#)
- [Backing Up Your Virtual Machine System State](#)

1. In your hypervisor client, start your virtual appliance, and then open the Console.
2. When the login prompt appears, log in as **admin** with a password of **admin**.
3. Arrow down to **TCP/IP Configuration**. Set the IP address, Netmask Default Gateway, Primary DNS Server and Secondary DNS Server for your virtual appliance. These fields can later be edited if needed from the **BASIC > IP Configuration** page in the product web interface.
4. Arrow down to **Licensing** and enter your Barracuda License Token and default domain to complete provisioning.
5. Arrow down to **Save Changes** and press Enter.
6. The virtual appliance will reboot.
7. Once the virtual appliance has finished rebooting, go to `http://<your ip>:8000` to access the web interface and finalize configuration.

Log Into the Web Interface and Configure Domain Information

Once the virtual appliance has finished rebooting, go to `http://<your ip address>:8000` to access the Barracuda Web Filter Vx web interface and finalize configuration of the product:

1. Log into the Barracuda Web Filter Vx web interface as the administrator:

Use Username: `admin` Password: `admin`

2. Go to the **BASIC > IP Configuration** page and enter values for **Default Hostname** and **Default Domain**. For example, enter `barracuda` as the **Default Hostname** and `<yourcompanydomain.com>` as the **Default Domain**. These names will be associated with anti-spyware email notification messages from the virtual appliance.
Note that, unlike the Barracuda Web Filter appliance, there is no need or facility to set **Operating Mode** for the Barracuda Web Filter Vx. This is because, in Forward Proxy deployment, *Audit* mode works just like *Active* mode; traffic is logged and policies are applied.
3. Click the **Save Changes** button to save all of the information.

Configure Your Firewall

You will need to configure your network firewall to allow ICMP traffic to outside servers as well as opening port 443 to updates.barracudacentral.com. You also need to make sure that your DNS servers can resolve updates.barracudacentral.com.

Update the Firmware

Click on the **Advanced > Firmware Update** page. If there is a new *Latest General Release* available, perform the following steps to update the system firmware:

1. Click on the **Download Now** button located next to the firmware version that you wish to install. To view download progress, click on the **Refresh** button. When the download is complete, the **Refresh** button will be replaced by an **Apply Now** button.
2. Click on the **Apply Now** button to install the firmware. This will take a few minutes to complete.
3. After the firmware has been applied, the Barracuda Web Filter Vx will automatically reboot, displaying the login page when the system has come back up.
4. Log back into the Web interface again and read the Release Notes to learn about enhancements and new features. It is also good practice to verify settings you may have already entered, as new features may have been included with the firmware update.

Change the Administrator Password

To avoid unauthorized use, we recommend you change the default administrator password to a more secure password. You can only change the administrator password for the Web interface. Go to the **BASIC > Administration** page and enter your old and new passwords, then click on **Save Password**.

Continue with [Directing Traffic to the Barracuda Web Filter Vx](#). See also [Adding Disk Space, Drives and RAM for Your Virtual Appliance](#).

Backing Up Your Virtual Machine System State

Virtual machine environments generally provide a "snapshot" capability, which captures the state of a system as it's running. Once a snapshot is created, you can perform additional operations on the system and "revert" to the snapshot in the case of disaster recovery (or for any other reason). Because this feature is so powerful, Barracuda Networks very strongly recommends performing a snapshot at certain points in time:

- Before upgrading the Barracuda Networks product firmware.
- Before making major changes to your configuration (this makes snapshotting a convenient "undo" mechanism).
- After completing and confirming a large set of changes, such as initial configuration.
- As a periodic backup mechanism.

Barracuda Networks also strongly recommends that you review your virtual environment documentation regarding snapshotting capabilities and be familiar with their features and limitations.

Directing Traffic to the Barracuda Web Filter Vx

There is no need to shut down your virtual machine when making changes to network connections. On your hypervisor, go to Networks and choose from available networks on your switches. If adding a network adaptor to the virtual machine, you must first shut it down.

Related Articles

- [Forward Proxy Deployment](#)
- [WCCP Deployment](#)
- [Policy-Based Routing](#)
- [Barracuda Web Security Agent - How it Works](#)

Determine Your Deployment Scenario

The Barracuda Web Filter Vx can be deployed in any configuration *except* for inline. Deploy your Vx:

1. Using a Forward Proxy Deployment. You can deploy the Barracuda Web Filter Vx in forward proxy mode via PAC file or GPO. This is the most common deployment scenario. See [Forward Proxy Deployment of the Barracuda Web Filter](#).
2. As a WCCP cache engine on a network with a WCCP capable core routing platform.
3. Using the Barracuda Web Security Agent. Please see [Barracuda Web Security Agent - How it Works](#).
4. Using [Policy-Based Routing](#). This deployment involves redirecting all port 80 traffic from your firewall through a policy-based route to your

Barracuda Web Filter Vx.

Since the Barracuda Web Filter Vx does not support inline deployment, note that the only feature *not* available to the Vx is application filtering (as noted on the **BLOCK/ACCEPT > Applications** page in the Barracuda Web Filter web interface).

Once you have installed your Barracuda Web Filter Vx and configured your firewall, you can test the configuration using the **ADVANCED > Troubleshooting** page in the web interface to ping updates.barracudacentral.com.

Sizing Disk, Drives and RAM for Your Barracuda Web Filter Vx

Barracuda Networks recommends the following sizing for initial deployment of your virtual appliance, or upgrading existing installations.

RAM

Model	#Cores	RAM
310	2	2G
410	3 or more	4G
610	4	8G
higher	limited only by license	2G per extra core

CPUs/Cores

You need to provision the number of cores in your hypervisor before the Barracuda Web Filter Vx can make use of them. Each model can only make use of a certain number of cores. If you assign 6 cores, for example, to a model 300 Barracuda Web Filter Vx, which can only make use of 2 cores, the virtual machine will turn off the extra cores that cannot be used. To add cores:


1. Shut down your hypervisor.
2. Go into Hypervisor settings.
3. Add CPUs. Note: The number of CPUs shown that you can add will vary with your hypervisor licensing and version. In some cases, the number of CPUs you can add must be a multiple of 2.

Hard Drives

Barracuda Networks *requires* a minimum of 50G hard disk space to run your Barracuda Web Filter Vx:

Model	Hard Disk Space
310	50G
410	50-200G
610	200-500G
higher	

From your hypervisor, you can edit the provisioned size of the hard drives, or you can add a hard drive.

 If you are using VMware, note that VMware tools support and thin provisioning are not currently available in the virtual product lines. As such, Barracuda Networks recommends using the **THICK** Provisioning format when allocating disk storage for your Barracuda Networks virtual machine.

To add a hard drive:

1. Shut down your Barracuda Web Filter Vx.
2. Take a snapshot of your virtual machine.
3. Edit the settings in your virtual machine and either increase the size of the hard drive or add a new hard drive.
4. Restart the virtual machine. As it's booting up, a blue screen will pop up and ask if you want to use the new additional space. Answer 'Yes'. Note that the popup will time out in 30 seconds if you don't respond, and the answer will default to 'No'. Resizing may take several

minutes, depending on the amount of provisioned hard drive space.

Related Articles

- [Virtual Deployment](#)
- [Backing Up Your Virtual Machine System State](#)

WCCP Deployment 6.x

The Barracuda Web Filter 410 and above can be deployed as a WCCP cache engine on a network with a WCCP capable core routing platform. Because the WCCP control router or switch transparently redirects content requests, you don't need to configure end users' browsers to use the Barracuda Web Filter as an HTTP proxy. Note the two different deployment diagrams for filtering HTTP traffic only versus filtering *both* HTTP and HTTPS traffic. **Note: HTTPS support requires running version 6.0.1 or higher.**

Check your Cisco Systems documentation for the recommended router/switch/firewall interface configurations.

High Availability and Load Balancing

In addition to compatibility with other WCCP capable routers, the Barracuda Web Filter supports Cisco v1 routers. Enabling WCCP on your Barracuda Web Filter allows you to take full advantage of your WCCP capable Cisco router's ability to provide for failover and load balancing for multiple Barracuda Web Filters connected to the router in a proxy configuration. For large installations requiring high availability and fault tolerance, this is an attractive deployment option. Other ways to achieve high availability without using WCCP are discussed in [High Availability - Clustering the Barracuda Web Filter](#).

Considerations when using the WCCP deployment

WCCP allows Cisco routers/switches to forward non-http traffic to web cache servers, but the Barracuda Web Filter only accepts HTTP/HTTPS traffic (port 80/443) in this configuration. WCCP also allows multiple Cisco routers to be connected to the same web cache server. The Barracuda Web Filter does not support this feature and can only be connected to one WCCP router/switch. However, as always, multiple Barracuda Web Filters can be connected to a single router/switch.

Also note the following:

- NTLM and Kerberos authentication mechanisms will not work because they both require that the Barracuda Web Filter be a trusted host in the Windows Domain and that it receive traffic directly from users (as a proxy). In WCCP deployments, the Barracuda Web Filter receives outgoing traffic via the Cisco Router.
- Application blocking will not work.
- Outbound spyware will not be blocked.

HTTPS traffic will be also be filtered if (if you are running version 6.0.1 or higher) if **Enable HTTPS Filtering** is enabled from the **BLOCK/ACCEPT > Configuration** page. To filter HTTPS traffic in this mode, make sure to configure the Cisco WCCP services as follows:

- Enable Service ID 80 for HTTPS
- Enable Service ID 90 for DNS UDP traffic
- Enable Service ID 91 for DNS TCP traffic

Figure 1 shows deployment with a WCCP router for filtering HTTP traffic only. For filtering HTTP and HTTPS traffic, see Figure 2. See the **BASIC > IP Configuration** page to select and configure WCCP deployment.

Figure 1: WCCP Deployment for filtering HTTP traffic only

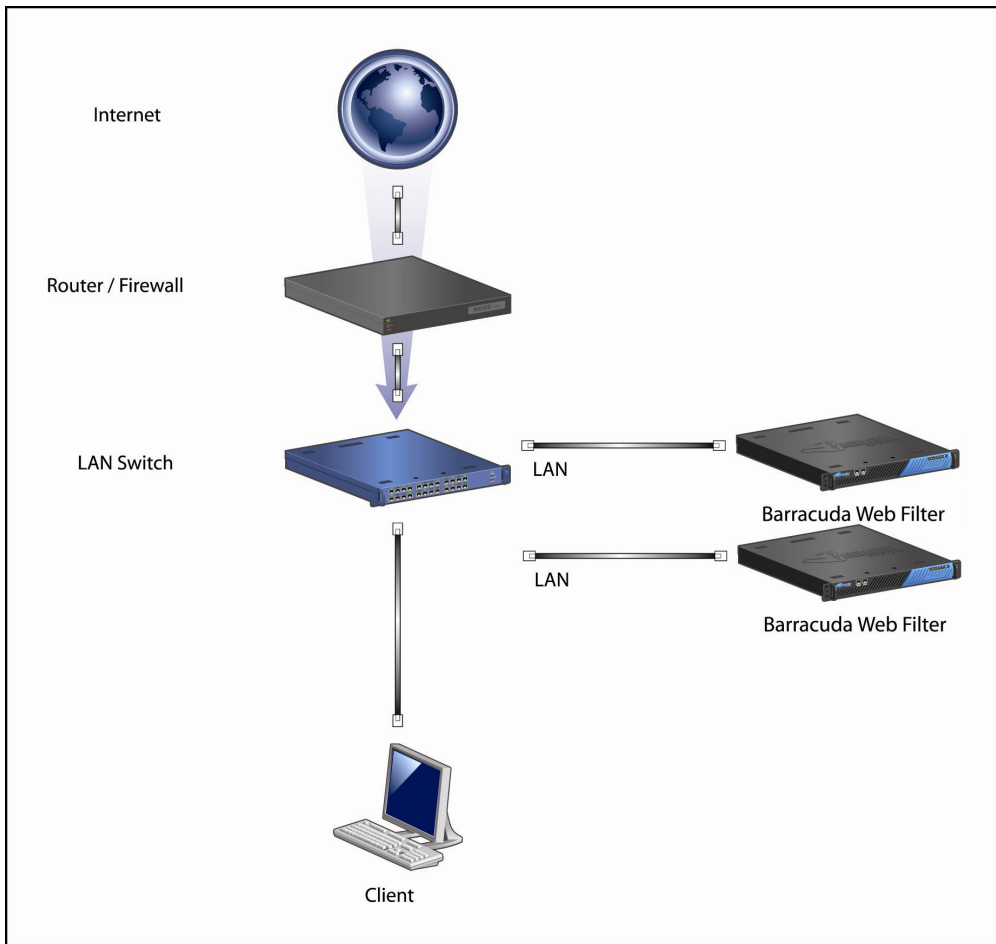


Figure 2 below shows deployment with a WCCP router for filtering both HTTP and HTTPS traffic. In this deployment, the Barracuda Web Filter uses a physically separate gateway to the internet relative to the WCCP router. This configuration is appropriate if your switch does not support VLANs and you want to filter both HTTP and HTTPS traffic with your WCCP router. See the **BASIC > IP Configuration** page to select and configure WCCP deployment.

Figure 2: WCCP Deployment for filtering HTTP and HTTPS traffic with a separate gateway for the Barracuda Web Filter.

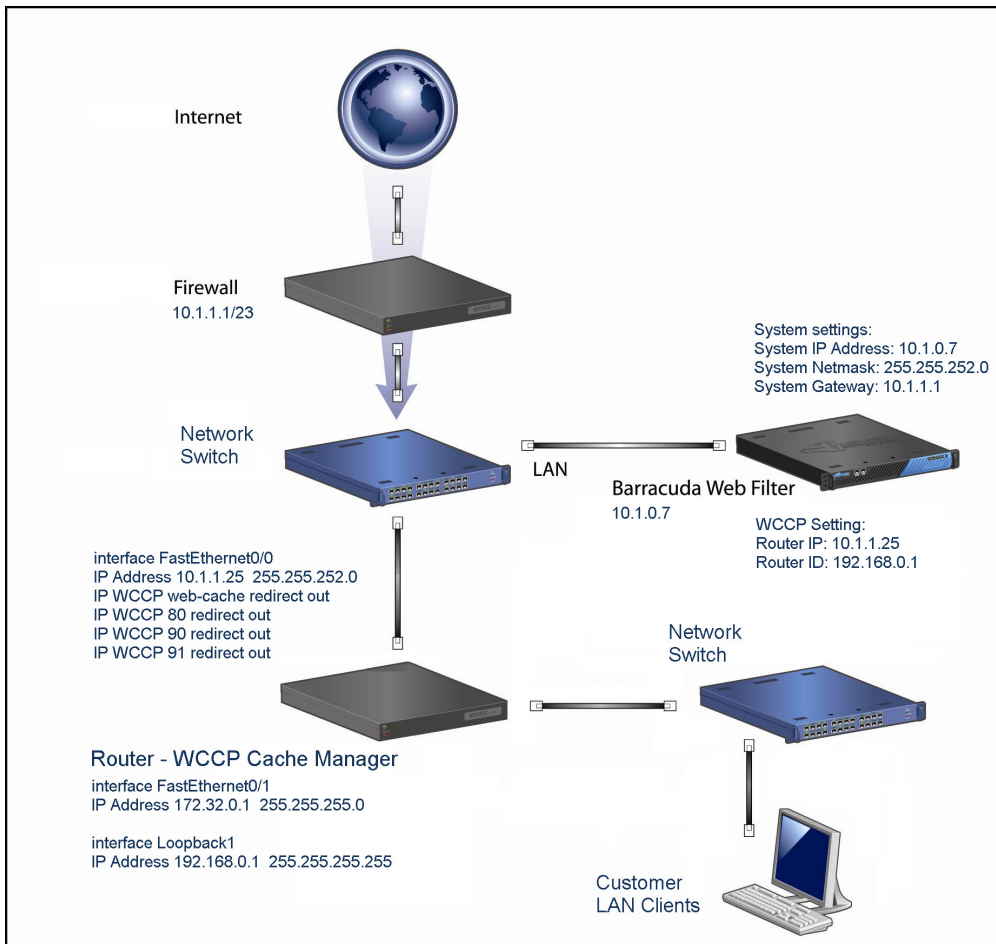
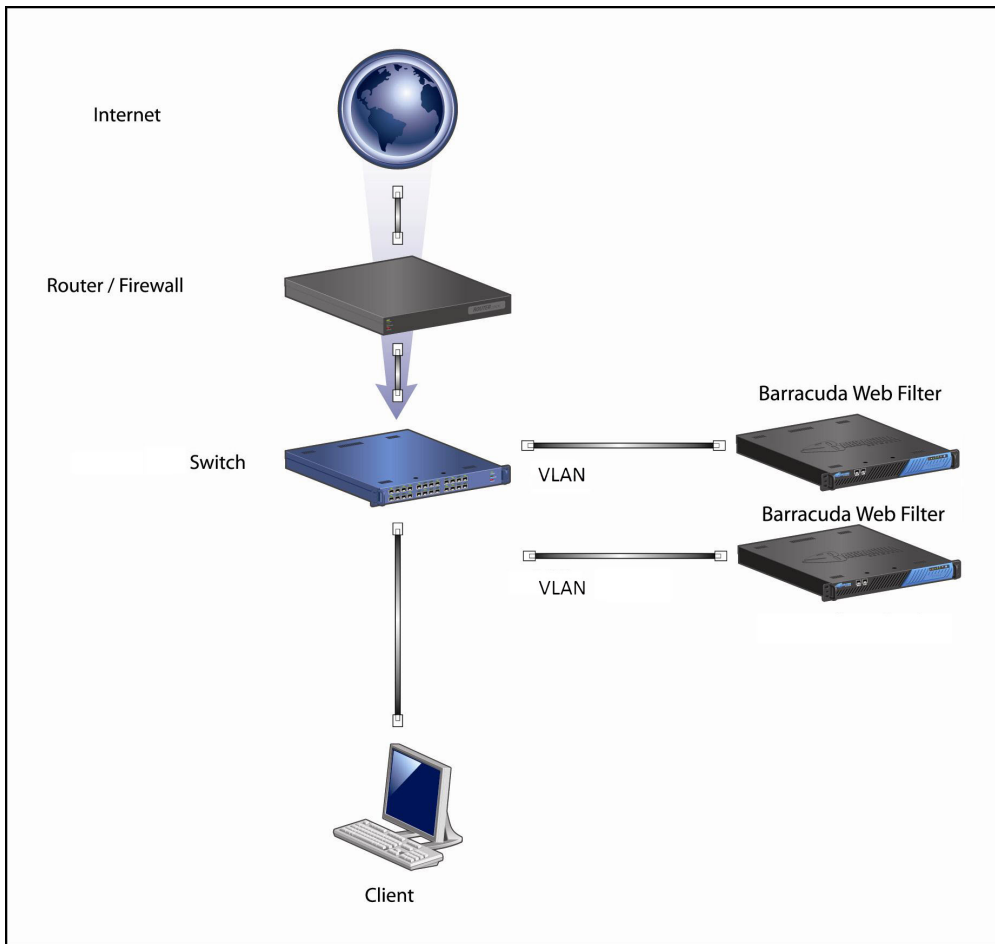


Figure 3 below shows deployment with a WCCP router for filtering both HTTP and HTTPS traffic, and a high availability (HA) deployment of two Barracuda Web Filters. In this deployment, each Barracuda Web Filter connects to your enterprise-class switch via a separate VLAN. This configuration is appropriate if your switch supports VLANs and you want to filter both HTTP and HTTPS traffic with your WCCP router. See the **ASIC > IP Configuration** page to select and configure WCCP deployment. Note that you can filter both HTTP and HTTPS traffic with just one Barracuda Web Filter or with multiple, as shown in this example.

Figure 3: WCCP Deployment for filtering HTTP and HTTPS traffic with the Barracuda Web Filter on a separate VLAN.



Getting Started

Barracuda Networks recommends first reviewing [Deployment Options](#). When you've determined the right deployment, you're ready to install and configure the Barracuda Web Filter.

Recommended Steps

If you already installed your Barracuda Web Filter using the [Barracuda Web Filter Quick Start Guide](#) which is shipped with your appliance, start with [Step 3: Configure the Barracuda Web Filter](#). If you are using the Barracuda Web Filter Vx, start with [Virtual Deployment](#).

- [Step 1: Network Considerations](#)
- [Step 2: Installation](#)
- [Step 3: Configure the Barracuda Web Filter](#)
- [Step 4: Configure and Secure the Web Interface](#)
- [Step 5: Connect the Barracuda Web Filter to Your Network](#)
- [Barracuda Web Filter 30 Day Evaluation Guide](#)

Step 1: Network Considerations

The Barracuda Web Filter appliance is designed for low-risk deployment because it is intended to be a bridge within your network. The Barracuda Web Filter can view Internet traffic that passes through the network but does not affect its routing. To reduce the risk of interfering with important network traffic, initially set the Barracuda Web Filter to monitor and log the spyware activity only. Determine which internal servers and clients to exclude from spyware and virus scans.

Related Articles

- [Using Static Routes](#)
- [VLAN Deployments](#)

The following pre-installation considerations may help you understand some of the issues that may occur, and Barracuda Networks recommends reading and understanding the [Deployment Options](#) for the Barracuda Web Filter before proceeding.

In this article:

- [Routers](#)
- [External DNS](#)
- [Internal DNS](#)
- [Enterprise class Layer 3 switch, VLANS, VPN concentrators](#)
- [Firewall DMZ](#)
- [Caching and the Current Time Setting](#)
- [QoS/Packet Reconfiguration \(Quality of Service, Packet Shapers\)](#)
- [Mounting and cabling considerations](#)

Routers

Make sure the default gateway is properly set to reach the Internet. Also, if you are testing the Barracuda Web Filter in one portion of your network and move to another portion of the network for deployment, make sure that you check the default gateway and make changes as necessary.

External DNS

Some of the considerations regarding DNS include the following issues:

Optimal DNS query response time: When the Barracuda Web Filter is in Active mode, it proxies all Internet requests for the clients. As a result, the Barracuda Web Filter needs to resolve website hostnames to IP addresses while proxying the HTTP requests made by the users. The response for web server DNS queries needs to be optimal to allow the Barracuda Web Filter to look up and quickly process these requests. A slow DNS server will cause the Barracuda Web Filter to respond slowly to clients, which adds latency to their Internet access.

Requests for fully qualified Web application server names: If a user attempts to browse to a website by specifying a web server name which is not a fully qualified name that includes the domain name, the Barracuda Web Filter automatically appends the string `barracuda.com` to the unqualified name in order to resolve the request. For example, if the user enters the server name `myserver` instead of `myserver.mydomain.com`, the Barracuda Web Filter resolves the request using the hostname `myserver.barracuda.com`.

Internal DNS

If you have an internal server that is only resolvable via an internal DNS, make sure that this DNS server is used by the Barracuda Web Filter as a secondary DNS.

Enterprise class Layer 3 switch, VLANS, VPN concentrators

These device types are normally capable of handling multiple subnets and providing default routes to clients. However, they may affect the Barracuda Web Filter deployment in the following ways:

- A Layer 3 switch can also be set up to have multiple VLANs (Virtual Local Networks) using port assignments. There is no side effect by having VLAN tags in the traffic that is visible to the Barracuda Web Filter (see also [VLAN Deployments](#)). However, when the Barracuda Web Filter is set up to a single subnet, it needs to have routes to process requests for other subnets. Although all VLAN operations are in Layer 2, most of the Layer 3 switches have better control since they offer a management user interface. Layer 2 "Smart" switches offer VLAN support as well. Layer 3 switches primarily differ from their capabilities of routing in IPv4 and IPv6, so it acts more like a router which is beyond normal switching hardware can do.
- A standard solution is to add [static routes](#) to these foreign subnets. All Layer 3 switch subnets should use its IP address as the gateway. In the case of a VPN concentrator, use the IP of the concentrator as the default gateway for all the networks aggregated by that VPN concentrator.

Firewall DMZ

Servers in the demilitarized zone (DMZ) are accessible from the internet. Servers inside this zone, such as mail servers, for example, may be configured to access certain servers within an internal network with their own security rules set up. The Barracuda Web Filter should not be

deployed to protect these machines. **The Barracuda Web Filter is not designed to protect servers but, rather, to protect end user machines.**



Internal Servers

In most organizations, internal servers are protected by corporate firewalls that use port forwarding rules to limit access to the servers. Port forwarding rules define the ports that can be used to access the servers (such as HTTP, FTP, and mail servers). These servers should have optimal response time.

As a result, the server traffic must not be interrupted. Barracuda Networks recommends that you exempt or bypass these servers from the Barracuda Web Filter. To reduce Layer 2 bridging overhead, place a switch between the firewall and the Barracuda Web Filter and connect your server farm on a different port on the switch. In this case, set up the servers parallel to the Barracuda Web Filter instead of behind it, and then configure the **IP and Port Exemptions** feature on the **BLOCK/ACCEPT > IP Block/Exempt** page to exclude these IP addresses from filtering

Caching and the Current Time Setting

Caching provides faster access to repeatedly requested content by storing content locally on the Barracuda Web Filter. Data is handled using an LRU (Least Recently Used) algorithm. You can enable or disable content caching, and specify domains to exempt from content caching, on the **ADVANCED > Caching** page. Note that the time value entered in the Current Time field on the **BASIC > Administration** page must be accurate since the Barracuda Web Filter uses the current time to ensure accurate cache updates.

QoS/Packet Reconfiguration (Quality of Service, Packet Shapers)

There are many products available that can control traffic in a LAN environment, specify priorities, and size these different traffic types. Normally, this is done using a Layer 7 device on different types of applications. The Barracuda Web Filter deployment is affected when the Barracuda Web Filter is placed in front of these devices to benefit from the shaped data. Place the Barracuda Web Filter close to the Internet to help reduce noise and overhead on both the Layer 2 bridging and HTTP proxy.

Mounting and cabling considerations

To install the Barracuda Web Filter you need to:

- Mount it on a rack or shelf, unless you have a desktop model and don't need to rack it.
- Cable it to other network devices

The Barracuda Web Filter is designed to be installed in a data center with other networking devices and servers. Depending on the model, its dimensions are suitable for a 19-inch rack, or can be adapted to a rack with the mounting kit. You must position it within cabling distance of any switches or other devices that access the network segments that you want to protect. The appliance can be mounted facing either direction in your rack, so consider which side will have access to the ports. You may need access to the ports during installation, and you may need to use the back panel during initial configuration.

Continue with [Step 2: Installation](#).

Using Static Routes

For an inline deployment, static routes are necessary to enable the Barracuda Web Filter to protect any client machines that are at IP addresses outside of the native subnet of the Barracuda Web Filter.

For example, suppose your Barracuda Web Filter is assigned the IP address **172.20.0.6** and a subnet mask of **255.255.255.0** and uses the default gateway at **172.20.0.9**.

- If you needed to create a static route to reach client machines in the **192.168.2.x** range, the **Netmask** value would need to be **255.255.255.0**.
- If you needed to create a static route to reach client machines in the **192.x.x.x** range, the **Netmask** value would need to be **255.0.0.0**.

In both cases, the **IP/Network Address** would need to be *outside* the **172.20.0.x** network of the Barracuda Web Filter, and the **Gateway Address** would need to be *inside* **172.20.0.x**.

To use static routing, from the **BASIC > IP Configuration** page, you would set up the following:

- **IP/Network Address** - IP address of a host or network located outside of the native subnet of the Barracuda Web Filter.
- **Netmask** - Subnet mask for the destination host or network.

- **Gateway Address** - IP address of the next hop that can be used to reach the destination host or network. When the Barracuda Web Filter receives ingress Web traffic for client machines in the specified IP range, it forwards the packets to the router at the IP address you specify in this field. Therefore, this IP address must be on the same subnet as the Barracuda Web Filter.

Note:The core switch or router typically contains routing statements for the entire network.

Step 2: Installation

Checklist for Unpacking

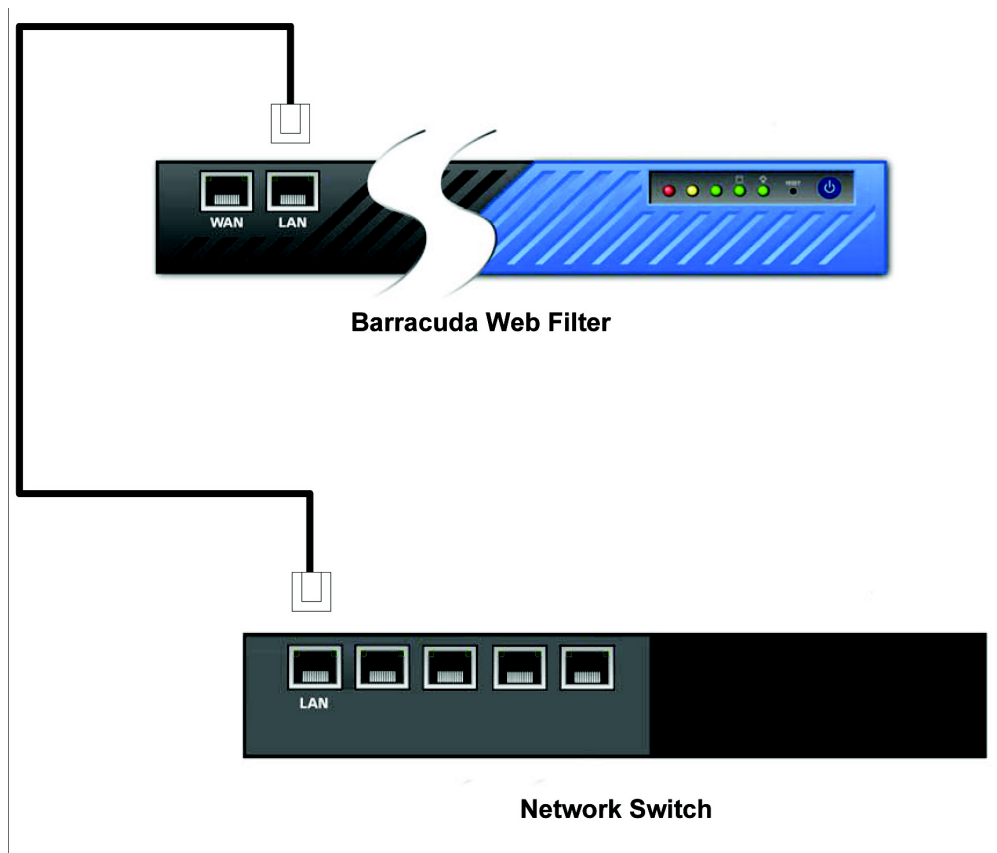
Before installing your Barracuda Web Filter, make sure you have the following equipment:

- Barracuda Web Filter (check that you have received the correct model)
- AC power cord
- Ethernet cables
- Mounting rails and screws (available for the Barracuda Web Filter 610, 810, and 910 only)
- VGA monitor (recommended)
- PS2 keyboard (recommended)

Install the Barracuda Web Filter

1. If you have a desktop Barracuda Web Filter, you do not need to install it in a rack, but if you wish to do so, use the rack-mount kit (sold separately) for [Rack Installation](#).
2. Fasten the Barracuda Web Filter to a standard 19-inch rack or other stable location. Do not block the cooling vents located on the front and rear of the unit or, for the Barracuda Web Filter 210, the top of the unit.
3. Connect a CAT5 Ethernet cable from your network switch to the LAN port on the back of your Barracuda Web Filter 210, or to the front of your Barracuda Web Filter 310 and higher, as shown in the following figure.

Figure 1: Connecting the Barracuda Web Filter 310 and higher to your network.



The Barracuda Web Filter supports 10BaseT, 100BaseT and, on the 610 and higher, 1xGigabit Ethernet.

i If your switch records the MAC address of an external device, make sure you delete all pre-existing MAC address records from your switch.

Do not connect any other cables to the unit. The connectors on the back panel are for diagnostic purposes.

3. Connect the following hardware to your Barracuda Web Filter:

- Power cord
- VGA monitor
- PS2 or USB keyboard

After you connect the AC power cord, the Barracuda Web Filter may power on for a few seconds and then power off. This is standard behavior

4. Press the Power button located on the front of the unit. The login prompt for the administrative console displays on the monitor and the power light on the front of the Barracuda Web Filter turns on.

Configure the IP Address and Network Settings

The Barracuda Web Filter is assigned a default IP address of 192.168.200.200. You can change the address using the administrative console or by pressing and holding the RESET button on the front panel. Choose an IP address that is on the same subnet as the devices connected to the WAN and LAN ports of the appliance.

Holding RESET for eight seconds changes the IP address to 192.168.1.200. Holding the button for 12 seconds changes the IP address to 10.1.1.200.

To set a new IP address from the administrative console:

1. With your keyboard and monitor connected directly to the Barracuda Web Filter, at the barracuda login prompt, enter admin for the login and admin for the password. The User Confirmation Requested window displays the current IP configuration of the Barracuda Web Filter.
2. Using your Tab key, select Change and click Enter to change the IP configuration.
3. Enter the new IP address, subnet mask, and default gateway IP address for your Barracuda Web Filter. Select Save to enter your changes. The Primary DNS and Secondary DNS files are optional. Select Exit.

The new IP address and network settings are applied to your Barracuda Web Filter.

Configure Your Corporate Firewall

If your Barracuda Web Filter is located behind a corporate firewall, refer to the table below for the ports that need to be opened on your corporate firewall to allow communication between the Barracuda Web Filter and remote servers.

Port	Direction	Protocol	Description
22	In/Out	TCP	Remote diagnostics and technical support services
25	Out	TCP	Email and email bounces
53	Out	TCP/UDP	DNS (Domain Name Server0
80	Out	TCP	Virus, spyware, category definition updates, and firmware updates
123	In/Out	UDP	NTP (Network Time Protocol)
8000	In/Out	TCP	See Initial Configuration of the System .

8001, 8002	In/Out	TCP	Synchronization between linked systems. For more information, see High Availability - Clustering the Barracuda Web Filter
------------	--------	-----	--

In addition to the ports listed above, you may have to configure your corporate firewall to allow the Barracuda Web Filter to email system alerts and reports. Some organizations create firewall rules that only allow emails to be sent from the IP address of their email server. In this case, you should configure your corporate firewall to allow emails to be sent from the Barracuda Web Filter as well.

If your Barracuda Web Filter is located in a DMZ, you may need to configure your corporate firewall to allow the Barracuda Web Filter to send notifications to your internal email server.

Continue with [Step 3: Configure the Barracuda Web Filter](#).

Step 3: Configure the Barracuda Web Filter

After choosing the IP address of the Barracuda Web Filter and opening the necessary ports on your corporate firewall, configure the Barracuda Web Filter from the web interface per the instructions below. Make sure the computer from which you are configuring the Barracuda Web Filter is connected to the same network and that the appropriate routing is in place to allow connection to the Barracuda Web Filter's IP address via a web browser.

In this article:

- [Understanding Operating Modes](#)
- [Configure the Barracuda Web Filter](#)
- [Activate Your Subscriptions](#)
- [Product Activation](#)
- [Update the Barracuda Web Filter Firmware](#)
- [Update Definitions](#)

Understanding Operating Modes

Before you configure the Barracuda Web Filter to filter traffic, it is recommended to become familiar with the possible operating modes and how they affect which traffic can be filtered and blocked. For initial configuration with an inline deployment, you should set the **Operating Mode** to *Audit* from the **BASIC > IP Configuration** page, and note how traffic is logged.

Operating modes include:

- *Active* - The Barracuda Web Filter actively protects your network by detecting spyware-infected machines on your network, using transparent HTTP proxy scanning to block and log non-HTTP spyware traffic, and using filters to block and log web traffic that conflicts with your organization's Internet usage policy. Note: In this mode, the system operates in Active Bridging Mode to manage connections between network devices and the Barracuda Web Filter.
- *Audit* - In this mode, for an inline deployment, HTTP traffic is logged but not blocked, and **downloads over HTTP will NOT be scanned for viruses or spyware**. Use this mode to preview how your currently configured Internet policies would be applied, but without disturbing production traffic. For forward proxy deployments, traffic is logged and policies are applied, just as in *Active* mode.

For non-HTTP traffic, the following configured policies DO apply:

- Application blocking
- IP Block/Exempt rules (Exempt traffic is logged)
- Outbound spyware activity is blocked

For non-HTTP traffic, the following does NOT apply:

- Content Filter settings
- MIME-type blocking
- Domains - blocked and allowed rules
- URL Patterns - logged only
- Categories - logged only
- Exceptions

In *Audit* mode, access to spyware sites and spyware downloads is not blocked but is logged.

Note: If the Barracuda Web Filter is deployed as a web traffic monitoring device (as opposed to a web traffic filtering device), the system

monitors traffic sent through any mirrored (spanned) port on your switches.

- **Safe** - This mode can only be entered automatically by the Barracuda Web Filter and is **not** configurable via the web interface. When the **System Load** exceeds normal thresholds for an extended period, as indicated on the **BASIC > Status** screen, the device shifts to **Safe** mode until the **System Load** returns to normal levels. **Note: In this mode, traffic is neither filtered nor logged.** **Safe** mode does not apply if the Barracuda Web Filter is deployed in a WCCP configuration.

Configure the Barracuda Web Filter

1. From a web browser, enter the IP address of the Barracuda Web Filter followed by port.
For example: **http://192.168.200.200:8000**
2. To log into the web interface, enter *admin* for the username and *admin* for the password. Select the **BASIC > IP Configuration** page and perform the following steps. Click the **Help** button on the right side of each section title for additional online help.
 - a. Enter the **IP address** of your Barracuda Web Filter that you chose in the steps above. Enter the **Subnet Mask** that is used to define this area of your network, and the **Default Gateway**, which is the IP address of the next outbound hop from the Barracuda Web Filter. The Barracuda Web Filter sends all egress traffic to the default gateway via the WAN port on the front of the appliance.
 - b. Enter the IP address of your primary and secondary DNS servers (if these have not yet been set up).
 - c. Set **Operating Mode** to *Audit*.
 - d. Set **Enable Proxy on WAN** to *No* to protect against WAN-side proxy requests if the Barracuda Web Filter is deployed outside of the corporate firewall.
 - e. Enter the **Default Hostname** which will be displayed in alerts, notifications, and messages sent by the Barracuda Web Filter.
 - f. Enter the **Default Domain** which will be displayed in alerts, notifications, and messages sent by the Barracuda Web Filter.
 - g. Click **Save Changes**.



If the IP address of your Barracuda Web Filter on the **BASIC > IP Configuration** page is changed, you are disconnected from the web interface. If this occurs, log in again using the new IP address.

Activate Your Subscriptions

After installation, your Energize Updates and other optional subscriptions must be activated for the Barracuda Web Filter to be fully enabled and to continue to receive the latest updates to all spyware, virus and category definitions from Barracuda Central. The Energize Updates service is responsible for downloading these updates to your Barracuda Web Filter.

Product Activation

1. At the top of every page, you may see the following warning:

Error: Activation has not been completed. Please activate your Barracuda Web Filter to enable functionality. [\(Click here for activation code\)](#)

2. Click on the designated link to open up the **Product Activation** page in a new browser window.
3. On the **Product Activation** page, fill in the required fields and click **Activate**. A confirmation page opens to display the terms of your subscription.
4. Return to the Barracuda Web Filter web interface and navigate to the **BASIC > Status** page. In the **Subscription Status** section, verify that the word *Current* appears next to **Energize Updates**, **Instant Replacement Service** (if purchased) and **Premium Support** (if purchased):

The screenshot displays the Barracuda Web Filter web interface. At the top, there's a user profile 'admin' and a language dropdown set to 'English'. Below the navigation tabs, the 'Status' section is active, showing various logs and reports. The 'MOST RECENTLY BLOCKED REQUESTS' table lists several blocked requests from the IP 10.4.129.145. The 'SUBSCRIPTION STATUS' section shows that all services (Energize Updates, Instant Replacement, Premium Support) are 'Current'. The 'LINK STATUS' section shows the LAN connection.

There may be a slight delay of a few minutes for the display to reflect your updated subscription status. If the status is still showing as not activated, click **Refresh** in the **Subscription Status** section.

i If your subscription status does not change to *Current* within an hour, or if you have trouble filling out the **Product Activation** page, please call your Barracuda Networks sales representative.

Update the Barracuda Web Filter Firmware

Prior to upgrading the firmware on your Barracuda Web Filter, it is always recommended that you read the release notes. To update the firmware on the Barracuda Web Filter:

1. From the web interface, select **ADVANCED > Firmware Update**.
2. Read the release notes to learn about the latest features and fixes provided in the new firmware version.
3. Click **Download Now** next to Latest General Release. **Download Now** is disabled if the Barracuda Web Filter is already up-to-date with the latest firmware version.

The Barracuda Web Filter begins downloading the latest firmware version. You can view the download status by clicking **Refresh**. A message displays once the download is complete. **It is important to not power-cycle the unit during the download.**

Updating the firmware may take several minutes. Do not turn off the unit during this process.

4. Click **Apply Now** when the download completes. The Barracuda Web Filter will apply the firmware and automatically reboot. **It is important to not power-cycle the unit during this process.** A Status page displays the progress of the reboot. Once the reboot is complete, the login page appears.

Update Definitions

To apply the newest definitions provided by Energize Updates:

1. Select **ADVANCED > Energize Updates**.
2. Select *On* for **Automatically Update**. The recommended setting is *On* for all available definitions.
3. Check to see if the current version is the same as the latest general release. If the rules are up-to-date, proceed to the next section. If the rules are not up-to-date, continue to the next step.
4. Click **Update** to download and install the latest available definitions onto the Barracuda Web Filter.

Continue with [Step 4: Configure and Secure the Web Interface](#).

Step 4: Configure and Secure the Web Interface

In this article:

- [Controlling Access to the Web Interface](#)
- [Customizing the Appearance of the Web interface](#)
- [Enabling SSL for Administrators and Users](#)

Controlling Access to the Web Interface

Use the **BASIC > Administration** page to perform the following tasks for initial setup:

1. Assign a new administration password to the Barracuda Web Filter (optional). This step is highly recommended.
2. Make sure the local time zone is set correctly. Time on the Barracuda Web Filter is automatically updated via NTP (Network Time Protocol). It requires that port 123 is opened for inbound and outbound UDP (User Datagram Protocol) traffic on your firewall (if the Barracuda Web Filter is located behind one).

It is important that the time zone is set correctly because this information is used to determine the delivery times for messages and is displayed in certain mail reading programs. The current time is also used to deliver accurate cache updates if caching is enabled (see the **ADVANCED > Caching** page).

3. If desired, change the port number used to access the Barracuda Web Filter Web interface. The default port is 8000.
4. Enter the amount of time for the **Session Expiration Length** (in minutes) of your Web interface session. If the session expires, you are required to log back into the web interface.
5. Specify your local SMTP server information. Enter the email address for your Administrator to receive system and threat email alerts and notifications.
6. Click **Save Changes**.

Customizing the Appearance of the Web interface

The **ADVANCED > Appearance** page allows you to customize the default images used on the web interface. You can also give the Barracuda Web Filter a name (e.g. "Science Library Web Filter") that will appear in the login page above the login panel that contains the Language selector and the Username and Password prompts. The **ADVANCED > Appearance** page is only displayed on the Barracuda Web Filter 410 and above.

Changing the Language of the Web Interface

You can change the language of the web interface by selecting a language from the drop-down menu in the upper right corner of the page near the **Log Off** link and the breadcrumbs. Supported languages include Chinese, Japanese, Spanish, French, and others. The language you select is only applied to your individual web interface. No other user's web interface is affected.

Enabling SSL for Administrators and Users

SSL (Secure Socket Layer) ensures that your passwords are encrypted and that all data transmitted to and received from the web interface is encrypted as well. All Barracuda Web Filters support SSL access without any additional configuration. However, some sites may wish to enforce using a secured connection to access the web interface, or prefer to use their own trusted certificates.

To enforce SSL-only access:

1. On the **ADVANCED > Secure Administration** page, select **Yes** to enable **HTTPS/SSL Access Only** to the web interface. Setting this to **No** will still allow the Barracuda Web Filter to accept non-SSL connections.
2. Enter your desired **Web Interface HTTPS/SSL port** for the web interface. The default is 443.
3. Click **Save Changes**.

If you wish to change the certificate that is used, you must first create and upload it to the Barracuda Web Filter before changing the **Certificate Type** in the **SSL Certificate Configuration** section of the **ADVANCED > Secure Administration** page. See the online help for instructions. The Barracuda Web Filter supports the following types of certificates:

- **Default (Barracuda Networks)** certificates are signed by Barracuda Networks. On some browsers, these may generate some benign warnings which can be safely ignored. No additional configuration is required to use these certificates, and are provided free of charge as the default type of certificate.
- **Private (self-signed)** certificates provide strong encryption without the cost of purchasing a certificate from a trusted Certificate Authority (CA). These certificates are created by providing the information requested in the **Private (self-signed)** section of the page. You may also want to download the Private Root Certificate and import it into your browser, to allow it to verify the authenticity of the certificate and prevent any warnings that may come up when accessing the web interface.
- **Trusted (signed by a trusted CA)** certificates are issued by trusted Certificate Authorities (CA), and must be purchased from them separately with a Certificate Signing Request (CSR). This can be downloaded after providing the information requested in the **Trusted (Signed by a trusted CA)** section of the page. Once you have received the certificate and key from the CA, you must upload both items to the Barracuda Web Filter from this section of the page. The certificate will be in effect as soon as the upload is complete.

Continue with [Step 5: Connect the Barracuda Web Filter to Your Network](#).

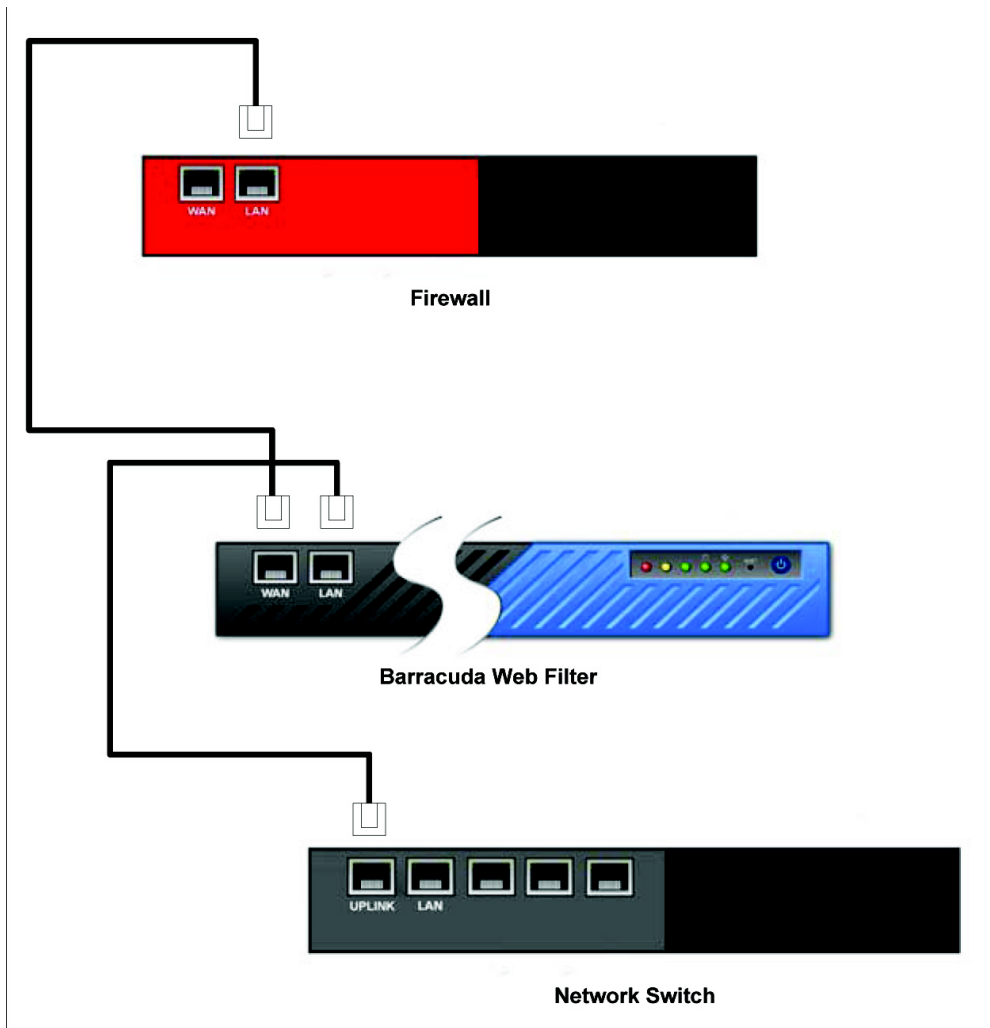
Step 5: Connect the Barracuda Web Filter to Your Network

To connect the Barracuda Web Filter to your network:

1. Connect the Ethernet cable from your corporate firewall to the WAN port on the front panel of the Barracuda Web Filter. This step may

require disconnecting your internal network switch from the corporate firewall.

A crossover cable may be needed if your corporate firewall does not have a switchable port and therefore cannot switch between RX and TX. Another solution is to place a switch between the corporate firewall and the Barracuda Web Filter. You do not need to configure the WAN port. The Barracuda Web Filter creates an Ethernet bridge between the WAN and LAN ports.



2. Select the **BASIC > IP Configuration** page in the web interface, and set the **Operating Mode** to *Active*.
3. For a forward proxy deployment, configure your clients' HTTP proxy settings from their browser to access the Internet. See [Forward Proxy Deployment of the Barracuda Web Filter](#) for more information.
4. If necessary, set up static routes on the **BASIC > IP Configuration** page. Setting up static routes is often necessary in complex networks so that the Barracuda Web Filter knows the proper way to route traffic on your network.

Static routes are generally necessary to enable the Barracuda Web Filters to protect any client machines that are at IP addresses outside of the native subnet of the Barracuda Web Filter.

For example, if the Barracuda Web Filter is assigned an IP address of 172.20.0.6 and a subnet mask of 255.255.255.0 and uses the default gateway at 172.20.0.9, you will need to create a static route to reach client machines in the 192.168.2.x range with a Netmask value of 255.255.255.0. The **Gateway Address** should be inside 172.20.0.x.

Test and adjust the Barracuda Web Filter

After connecting your Barracuda Web Filter to the network, verify connectivity. Open your web browser from a machine on your network. If you cannot browse the web, review the installation steps to make sure your Barracuda Web Filter is properly configured and connected to your corporate firewall and network switch.


If you can browse the web without any issues, you are ready to adjust the settings on the Barracuda Web Filter. The most common adjustment to make is to create filters that determine what traffic and applications the Barracuda Web Filter blocks and accepts. For more information about the available filters, refer to [Monitoring the Barracuda Web Filter](#).

Go to the **BLOCK/ACCEPT > IP Block/Exempt** page and use the **IP and Port Exemption** section to bypass scanning or filtering for clients or targeted servers. To avoid accidentally specifying a broader than intended exemption range, be sure to apply the proper subnet mask.

Barracuda Web Filter 30 Day Evaluation Guide

Where to start

Please begin with the [Barracuda Web Filter Quick Start Guide](#) . This guide is included as a 2-sided 8.5 x 11" card included with your Barracuda Web Filter and will guide you in safe installation and initial configuration of your Barracuda Web Filter. If you have the Barracuda Web Filter Vx virtual appliance, start with [Virtual Deployment](#), then return to this page for hints and guidelines for your 30 day evaluation process.

 If you have a model 610 or higher, you automatically have a Barracuda sales engineer assigned to help you make the most of your 30 evaluation of the Barracuda Web Filter. Simply call your reseller or sales representative if you have not yet been contacted by a sales engineer.

Common Use Cases

You are encouraged to work with your sales representative if you have questions about your initial setup, or feel free to call [Barracuda Networks Technical Support](#) to discuss how to best deploy and test the Barracuda Web Filter in your network. Here are a few common use cases and guidelines to prepare you for success.

Use Case: Reporting

1. If possible, deploy the Barracuda Web Filter inline as described in [Inline Pass-Through \(Transparent\) Mode Deployment](#). This deployment does not require setting a proxy in client browsers. You can either set up the Barracuda Web Filter inline with your computer for initial testing, or follow steps 3 and 4 to configure users and authentication for testing policies.
2. Set the Barracuda Web Filter **Operating Mode** on the **BASIC > Administration** page to *Audit*. This mode logs traffic but doesn't warn or block users from accessing any URL. In *Audit* mode, for inline deployments, HTTP traffic is logged but not blocked, and downloads over HTTP are NOT scanned for viruses or spyware. Use this mode to preview how your currently configured Internet policies would be applied, but without disturbing production traffic. In [Forward Proxy](#) deployment, *Audit* mode works just like *Active* mode; traffic is logged and policies are applied.
3. Configure authentication as needed using your LDAP server, Kerberos or NTLM. See [How to Choose Your Authentication Mechanisms](#) for more information and to get started.
4. Create a set of [Users and Groups](#) if you want to assign block and allow policies to *Authenticated* users.
5. Use the filters on the **BLOCK/ACCEPT** pages to set policies for what you want to block, monitor, warn users about, or allow in web traffic for *Authenticated* or *Unauthenticated* users. See [Best Practices in Configuring Policy](#) for guidelines in setting up your traffic filtering policies.
6. After you have had the Barracuda Web Filter running for awhile, run reports on user activity, bandwidth usage, most visited domains, and other metrics from the **BASIC > Reports** page.
7. After reviewing reports, you'll have a good idea of what browsing activities or web 2.0 applications you want to warn, monitor, block or allow. Use the **BLOCK/ACCEPT** pages to adjust policies according to your organization's needs.
8. When you are ready to begin blocking specific web traffic, set the Barracuda Web Filter Operating Mode on the **BASIC > Administration** page to *Active*.

Use Case: Social Media Regulation and Monitoring

The Barracuda Web Filter 610 and higher enables granular control over Web 2.0 applications running over HTTPS. For example you can allow access to Facebook messages but block games, chat, posts etc. You can provide safe access to YouTube videos that provide rich educational content using your [YouTube for Schools](#) account. Since many social media applications such as Facebook and Google Apps typically run over HTTPS, you must configure the **SSL Inspection** feature on the Barracuda Web Filter, which is available on the 610 and higher. It is recommended to work with your sales engineer to configure SSL Inspection.

With the **Web Application Monitoring** feature and **SSL Inspection**, you can capture and archive the content of social media interactions.

1. For the Barracuda Web Filter 610 and 810, use the [Forward Proxy Deployment](#) if you are using SSL Inspection to regulate/monitor applications over HTTPS. With the Barracuda Web Filter 910 and above, you can also use SSL Inspection with [Inline Deployment](#) and [WCCP Deployment](#).
2. Follow steps 2-5 above.
3. See the **BLOCK/ACCEPT > Web App Monitor** page in the Barracuda Web Filter web interface to configure. See [How to Configure Web Application Monitoring](#) for more information and examples.

For schools, using SSL Inspection and Web Application Monitoring provides powerful benefits with common use cases such as these:

- [Google Apps Control Over HTTPS](#) - Granular regulation of Google Apps tools over HTTPS (Business Gmail as opposed to personal Gmail, and more)
- [Facebook Control Over HTTPS](#) - Granular regulation of Facebook applications (chat, posting, games, etc.)
- Alert authorities of emerging cases of cyberbullying, harassment, or loss of confidential data using the [Suspicious Keyword Tracking](#) feature. Monitor social messaging in real time, with keyword alert emails to teachers or administrators. This feature does *not* require the use of SSL Inspection unless you want to monitor HTTPS traffic content, and is available on the Barracuda Web Filter 610 and higher.

With the Barracuda 210, 310 and 410, you can block or allow websites and subdomains as well as some applications, but you cannot capture the content of social media interactions as described above. To simply block or allow applications like Facebook Games, Flickr upload, LinkedIn Email and many more, see the **BLOCK/ACCEPT > Web App Control** page in the web interface.

Use Case: Remote Filtering for Students and Offsite Users

Remote Filtering with the Barracuda Web Filter enables your IT department to provide and control content security beyond the perimeter of the IT infrastructure. To learn about options for managing and applying filtering policies to remote laptops, iOS devices and other computers, see [Remote Filtering for Offsite and Mobile Users](#).

1. Begin by deploying the Barracuda Web Filter in your network, selecting your authentication mechanism, and testing out policies as described above.
2. After you have configured and tested block and allow policies and authentication, you're ready to test extending this protection to your remote laptop or iPad, for example. If your use case is:
 - Remote laptops, PC and Macintosh computers – Install the Barracuda Web Security Agent on one of these devices, which synchronizes them with the Barracuda Web Filter policies. See [Barracuda Web Security Agent - How it Works](#) and [How to Install the Barracuda WSA With the Barracuda Web Filter](#) to get started.
 - Students with school issued iPads – You can either install the [Barracuda Safe Browser](#) or use the [Global HTTP Proxy](#) tool from Apple Inc. to direct traffic from the iOS device to the Barracuda Web Filter.
3. Test your block and allow policies with one remote device before extending to all remote devices.

For use case examples specific to students, see:

- [Facebook Control Over HTTPS](#)
- [Google Apps Control Over HTTPS](#)
- [Barracuda Web Filter for Education](#)

Creating Exceptions to Policies

If you want to exempt certain users from block and allow policies, such as HR, Finance, Students, Teachers, etc.:

1. Create users and assign them to groups of users on the **USERS > Users and Groups** pages.
2. Set up your authentication mechanism as described above for users and groups.
3. Use the **BLOCK/ACCEPT** pages as described above to create policies.
4. Use the **BLOCK/ACCEPT > Exceptions** page to create exceptions to policies. See [Exception Policies](#) for more information and examples.

Social media application such as Facebook and Google Apps typically run over HTTPS

Managing Policies

Begin creating filtering policies which you can assign to specific users and/or groups by following recommended [Best Practices in Configuring Policy](#). The BLOCK/ACCEPT pages in the web interface provide a wide range of filters that enhance the default spyware and virus detection capabilities of the Barracuda Web Filter. Note that application filtering is supported by the Barracuda Web Filter appliance, but not by the Barracuda Web Filter Vx virtual machine.

In this Section

- [Best Practices in Configuring Policy](#)
- [BLOCK/ACCEPT Order of Precedence - Barracuda Web Filter](#)
- [Block Messages](#)
- [Creating Block and Accept Policies](#)
- [Using Custom Categories](#)
- [Exception Policies 6.x](#)

- [Exception Policies 7.x](#)
- [Barracuda Web Filter for Education](#)
- [How to Set Up YouTube for Schools](#)
- [How to Enable Safe Search for Students](#)
- [Suspicious Keyword Tracking](#)
- [Temporary Access for Education](#)
- [How to Use Temporary Access for Students - Teacher's Guide](#)
- [How to Configure Web Application Monitoring](#)
- [Using SSL Inspection With the Barracuda Web Filter](#)
- [Google Apps Control Over HTTPS](#)
- [Facebook Control Over HTTPS](#)

Best Practices in Configuring Policy

Begin creating filtering policies which you can assign to specific users and/or groups by following the best practices listed below. The BLOCK/ACCEPT pages in the web interface provide a wide range of filters that enhance the default spyware and virus detection capabilities of the Barracuda Web Filter. **Note that application filtering is supported by the Barracuda Web Filter appliance, but not by the Barracuda Web Filter Vx virtual machine.**

Users and Groups for Authentication

You can apply domain, IP address, pattern, content, application, and MIME type blocking filters to *authenticated* and/or *unauthenticated* users. The first step in creating your policy should be deciding which categories your users will **not** be allowed to visit (*Adult Content, Game Playing & Game Media, Streaming Media, etc.*). You can later override this policy using exception policies to grant either additional or more restrictive access for individual users or groups. Before you create or modify a filter, make sure to use the drop-down menu on the right side of the web interface page to select which type of user you want the filter applied to (authenticated or unauthenticated).

Use the **USERS/GROUPS** pages to manage users and authentication.

Related Articles
<ul style="list-style-type: none"> • Creating Block and Accept Policies • Managing Policies • Exception Policies 7.x

Exception Policies for Specific Access

Exceptions are useful for creating policies that allow a subset of your users to access content that is blocked for other users. On the **BLOCK/ACCEPT > Exceptions** page, you can create policies to override filters you have created on a per-user or group basis. For example, if you configure your content filters to block access to auction sites for both *authenticated* and *unauthenticated* users, but a member of your purchasing department requires access to these sites, you can create an exception policy that allows access to only this user. Or you could create an exception for the entire purchasing department (a 'Group') using the LDAP organizational unit in your Active Directory server.

Exception policies are applied in the order in which they are listed in the table on the **BLOCK/ACCEPT > Exceptions** page of the web interface. You can drag and drop exceptions to re-order them in the table. See [Exception Policies 7.x](#) for details.

Block Pages and Authorized Logins

When a user tries to access content that is blocked by one of the assigned filters, the user receives a block message (see Figure 1 below) that may contain login fields, depending on how you configure authentication on your Barracuda Web Filter. If you want to hide the login fields because you have not created any exception policies that allow users to bypass the block filter, go to the **BLOCK/ACCEPT > Configuration** page and change the **Enable Login Override of Block Pages** setting to *No*. Note that remote users who access the Barracuda Web Filter via the Remote Filtering (WSA) feature or via the Barracuda Safe Browser on their mobile devices will *not* see login fields on block pages.

Figure 1: Block Message with Login Fields



Access Denied

Cancel/Go back

The link you are accessing has been blocked by the Barracuda Web Filter because it contains content belonging to the category of: Travel

If you believe this is an error or need to access this link please contact your administrator.

URL: <http://www.expedia.com>

Login

Apply

The Barracuda Web Filter will recognize specific types of block and accept rules in the order they are listed (from top to bottom). If conflicting rules are created, the rule listed first will be honored. Whitelist or "allow" rules take precedence over block rules of the same type. The different rules, configured under the **BLOCK/ACCEPT** tab, are applied in this order:

1. IP Block/Exempt
2. Exceptions
3. Applications
4. MIME Type Blocking
5. Domains
6. URL Patterns
7. Content Filter

Policy Alerts: You can specify email alerts to be sent to an administrator or other roles when one or more users violate content filtering policies (Block, Warn or Monitor Actions) more than a specified number of times. See [Policy Alerts](#) for more information.

BLOCK/ACCEPT Order of Precedence - Barracuda Web Filter


The **BLOCK/ACCEPT** pages in the Barracuda Web Filter web interface provide a wide range of filters that enhance the default spyware and virus detection capabilities of the Barracuda Web Filter. **Note that application filtering is supported by the Barracuda Web Filter appliance but *not* by the Barracuda Web Filter Vx virtual machine.** See also [Best Practices in Configuring Policy](#) for guidelines on planning and creating your Block/Accept rules, and [Creating Block and Accept Policies](#) for details on filters available.

Related Articles
<ul style="list-style-type: none">• Best Practices in Configuring Policy Exception Policies 6.x• Exception Policies 6.x• Creating Block and Accept Policies• Web Use Categories

Order of Precedence of Block/Accept Rules

The Barracuda Web Filter will recognize specific types of block and accept rules in the order they are listed below (from top to bottom). If conflicting rules are created, the rule listed first will be honored. Whitelist or Allow rules take precedence over Block rules of the same type.

1. **BLOCK/ACCEPT > IP Block/Exempt** - Use this section to exempt traffic from all filtering - including spyware filtering - based on IP address criteria. You can exempt certain ports, portions of your network, or external application servers.
2. **BLOCK/ACCEPT > Exceptions** - Use the **Exceptions** page to manage policy exceptions for specific users or groups. An exception rule grants selected users - local users or groups, domain users or groups, or all users (authenticated or unauthenticated) - exceptions to a Barracuda Web Filter policy for a specific period of time.
3. **BLOCK/ACCEPT > Applications** - Available for Inline deployments only. Use this feature to block or allow specific application traffic. You can select from a pre-defined list of non-HTTP web applications including IM clients, media programs, common PC tools, software updates, and peer-to-peer software.
4. **BLOCK/ACCEPT > MIME Type Blocking** - Use the **MIME Type Blocking** page to blacklist standard MIME types. You can create a MIME type blacklist for either unauthenticated or authenticated users. These rules are useful when content is not easily blocked by other methods.
5. **BLOCK/ACCEPT > Domains** - Use this section to specify a domain that should be blocked, warned, or monitored. This blocking filter will operate in addition to those defined in other filtering categories.
6. **BLOCK/ACCEPT > URL Patterns** - Use this section to specify a pattern or keyword to match parts of a URL that should be blocked, warned, or monitored.
7. **BLOCK/ACCEPT > Content Filter** - Use the **Content Filter** page to manage your users' Internet access based on the web site content being requested. You can apply content category filters to either unauthenticated or authenticated users.

 Barracuda does not recommend using IP block/exempt rules for blocking traffic to websites or for specific applications. IP block/exempt rules are generally used to control access to and from particular client computers or external web servers (such as email servers or update servers). However, you can use this feature to control access by specifying destination IP/port combinations. Keep in mind that these rules have precedence over all other block/accept rules.

Block Messages

When the Barracuda Web Filter blocks access to a website, it presents a block page with a message that informs the user why that site is being blocked as shown in Figure 1. The Barracuda Web Filter blocks a website if it contains spyware, a virus, content that has been blocked due to policies you set, or a blacklisted URL. You can optionally choose to have the Barracuda Web Filter redirect blocked users to any other URL, such as a custom block page, search engine page, etc. See [External Block Page](#), page 86 for details. If you are using the Barracuda Web Filter built-in block page, use the **BLOCK/ACCEPT > Block Messages** page to perform the following tasks:

- Select the language that the block message is displayed in for all users.
- Customize the message in case the default text is insufficient.

Figure 1: Block Message with Login Fields.



Access Denied

Cancel/Go back

The link you are accessing has been blocked by the Barracuda Web Filter because it contains content belonging to the category of: Travel

If you believe this is an error or need to access this link please contact your administrator.

URL: <http://www.expedia.com>

Login

Apply

With the Barracuda Web Filter 610 and higher: If you enable the **Temporary Access** feature for teachers and students to gain access to specific websites for classroom research, students can enter a token given by the teacher to bypass block pages to those sites for a limited time. See [Temporary Access for Education](#) for details about this feature, which offloads temporary access management from the system administrator to the teacher.



Remote users logged in with the Barracuda Web Security Agent (WSA) will not have the option to bypass block pages with a login.

External Block Page

You can choose to redirect the user to a custom block page which you provide/design (or any URL) instead using the Barracuda Web Filter block page when a policy prevents the user from accessing a requested website or application. To use this option you must enable the **Use External Block Page** feature and specify an **External Block Page URL** on the **BLOCK/ACCEPT > Configuration page**.

The **Barracuda Web Filter** will redirect the blocked user to the URL you specify, which can be your own page/site, a search engine, etc.

Terms and Conditions Page (Captive Portal)

For hotels, internet cafés or other entities that wish to present a customized 'terms and conditions' page to which the user must agree before proceeding to browse the web, the **Captive Portal** feature can be enabled on the **BLOCK/ACCEPT > Configuration** page. This feature **ONLY** applies to unauthenticated users and is not an authentication mechanism.

With **Captive Portal** enabled, the first request from every user will be served a splash page displaying customized terms and conditions, which you enter on the **BLOCK/ACCEPT > Block Message** page, to which they must agree before beginning to browse the web via the Barracuda Web Filter. Once the user agrees, the page is not presented again for the duration of the browsing session and the user can view content that is not blocked for the accepted local user - a special user that is created from the **USERS/GROUPS > New Users** page. Please see the **BLOCK/ACCEPT > Configuration** page for easy instructions. All traffic for the user is logged.

Creating Block and Accept Policies

This article covers creating block and accept filtering policy. To create exceptions by user, group, time, etc. to the policies you set, see [Exception Policies 6.x](#).

In this article:

- [Content filtering](#)
- [Safe Search](#)
- [Safe Browsing for Schools](#)
- [Application Filtering](#)
 - [Non Web-Based Applications](#)
 - [Social Media and Other Web-Based Applications](#)
 - [Web Application Monitoring](#)
- [Domain filtering](#)
- [URL pattern filtering](#)
- [Custom categories filtering](#)
- [MIME type blocking](#)
- [IP-based exemption](#)
- [IP-based blocking](#)

Content filtering

Barracuda web security products employ a comprehensive database of frequently updated categories of website content types. Use the **BLOCK/ACCEPT > Content Filter** page to control user access to categories of websites that should be blocked, warned, monitored, or allowed based on content. When you block a category, you block all HTTP and HTTPS traffic to the associated URLs in that category.

For example, <http://mail.yahoo.com> is categorized as a web-based email site. If you want to block users from accessing their web-based email accounts, block the Web-based Email category.

See [Web Use Categories](#) for a listing and definition of content classification.

Safe Search

Safe Search mode prevents a web search engine from displaying objectionable thumbnail images in search results; only filtered thumbnails are displayed in the search results. To limit Safe Search to specific users, create an exception using the **BLOCK/ACCEPT > Exceptions** page. For details, see [Safe Browsing / Safe Search - Limiting to Specific Users](#). The entries in this category include search engines which allow users to enable or disable Safe Search mode for image searches. If you enable Safe Search through the Barracuda Web Filter, users cannot use the search engine settings to override this mode. If you only want to enable Safe Search for certain users, select **Disable** for each search engine listed in the table, or click the **All** link. On the **BLOCK/ACCEPT > Exceptions** page, create an **Enable** exception for the user or group of users for whom you want to enable Safe Search.

Safe Browsing for Schools


- For educational institutions wishing to use **YouTube For Schools** filtering, the procedure to configure the Barracuda Web Filter to work with this tool is detailed in [How to Set Up YouTube for Schools](#).
- See [Temporary Access for Education](#) to give teachers and students temporary access to websites, for classroom research, that are typically blocked.

Application Filtering

Non Web-Based Applications

Use the **BLOCK/ACCEPT > Applications** page to block or allow specific application traffic over the HTTP (and HTTPS) protocol that is not browser-based. For example: Skype, Pandora, Adobe Acrobat, FTP. This type of filtering does NOT scan for content. If you need to scan and filter content, you must enable [SSL Inspection](#). Note, however, that the SSL Inspection feature is only available on the Barracuda Web Filter 610 and higher, and requires more system resources and installation of SSL certificates to configure. To block/allow specific functions that run within web applications, such as Facebook games or Skype chat, configure on the **BLOCK/ACCEPT > Web App Control** page.

For a user to download or use an application, the user's application needs to communicate with an external server. When you select to block an application, the Barracuda Web Filter searches for traffic that contains data associated with an application server and then blocks that traffic.

	The Barracuda Web Filter Vx virtual machine does not support application filtering because it cannot be deployed inline, and application filtering is ONLY supported by inline deployments.
---	---

Exceptions to policies can be created for a specific user or group based on bandwidth quotas, time of day and/or days of the week. For example, you might want to allow employees to access certain applications such as Skype, for example, ONLY during lunch hours. See [Limiting Access by Time frames, Time Quotas and Bandwidth Quotas](#). You can use the applications filter as a pre-emptive measure to protect your network against malware.

Social Media and Other Web-Based Applications

From the **BLOCK/ACCEPT > Web App Control** page you can block or allow specific web-based application traffic. For example: Facebook, LinkedIn, MySpace, Twitter, and others. You can allow or block the entire application or only specific functions that run within these web applications. For example, you might allow Facebook, but want to block Facebook games and Facebook apps to protect against viruses and malware.

As another example, you may want to block the IRC application because this type of application can present a security risk to the network. An infected PC may communicate with the "hacker" through an IRC channel, and the hacker can send commands to the channel instructing bots to launch an attack. IRC could also be used by a disgruntled employee to launch attacks on other networks or to communicate sensitive information outside of the network.

You can also use the application blocking feature when you hear about a virus spreading over a specific IM service or tool. In this case, you can proactively protect your network from the infection by blocking that particular service until the threat has been resolved.

Web Application Monitoring

Use this feature to capture and archive chat, email, user registrations and other social media interactions. The archiving repository can be your Barracuda Message Archiver, your Microsoft Exchange Server journaling tool or, for example, a system administrator email address.

For example, you might want to allow users in the organization to use Facebook to view and make status updates and use chat, but you want to capture the content. You might also want to block games, shares and other Facebook apps to protect your network from viruses and malware.

To configure Web Application Monitoring, you'll want to first set up your block/accept policies for web-based applications. Here's the process for this example:

1. From the **BLOCK/ACCEPT > Web App. Control** page, in the Application Navigator, check Facebook to allow some or all Facebook applications.
2. Select the *Facebook* actions to block and allow and save your changes. In this example, you'd leave chat and status update in the **Allowed Applications** list, moving other applications you want to block, such as shares, games and other apps, to the **Blocked Applications** list. Save your changes.
3. From the **BLOCK/ACCEPT > Web App. Monitor** page, enable the application actions whose content you want to archive. In this example, you would enable *Facebook Wall Posts*, *Chat Message* and *Private Message*. Once you enable any actions on the page, the Barracuda Web Filter will capture the content from each action, package it as an SMTP message and email it to the **Notification Email Address** you specify.

Domain filtering

Use the **BLOCK/ACCEPT > Domains** page to blocklist (block), warn, monitor or whitelist (allow) traffic to specific domains and subdomains. Use domain whitelists to allow access to domains that belong to categories that are generally blocked. Note that domains that are whitelisted ARE

subject to the MIME type blocking rules you create (see below). Use domain blocklists to restrict access to domains in addition to those specified in other filtering categories.

i Tip

To control access to a domain and all its associated URLs, make sure you enter the domain identifier. For example, **www.example.com** will control access only to the specific URL but **example.com** will control access to all URLs under the domain.

URL pattern filtering

Use the **BLOCK/ACCEPT > URL Patterns** page to enter regular expressions or keywords that, if matched to a URL, will block (blocklist), warn, monitor, or allow (whitelist) that URL. For more information about using regular expressions, refer to [Regular Expressions](#). Note that URLs that are whitelisted ARE subject to the MIME type blocking rules you create (see below).

Examples:

1. You want to block all websites that contain porn in the URL - enter *porn* as a blocked pattern. Sometimes spyware applications use different hostnames but the same domain name, so the URLs appear to be from different hosts. In this case you can enter the domain name as a pattern to block all URLs on that domain.
2. You want to allow access to **example.com** but want to block **maps.example.com**. In this case, specify **example.com** as an *allowed* pattern and specify **maps.example.com** as a *blocked* URL.

i Tip

Run a test on your regular expressions with special characters before you encode them in a pattern filter.

Custom categories filtering

Use the **BLOCK/ACCEPT > Custom Categories** page to create a custom filter, which can consist of the domain names or built-in web content categories you select. Custom categories are used in the same way as the built-in filters:

- You can apply a custom category to either authenticated or unauthenticated users.
- You can define a user- or group- specific exception rule to a custom category policy.

After you define a custom category, allow between five and ten minutes for the Barracuda Web Filter to compile and then fully activate the new category. To verify that a newly created custom category is active, you can use the **Content Filter Lookup** facility in the **BLOCK/ACCEPT > Content Filter** page, as described in the online help for the **BLOCK/ACCEPT > Custom Categories** page.

MIME type blocking

Use the **BLOCK/ACCEPT > MIME Blocking** page to specify standard MIME types that you want to block. Note that websites that are whitelisted ARE subject to the MIME type blocking rules you create. Many organizations choose to block Internet radio and streaming media because they add load to the internal network, as well as executable files because they can install viruses and various other malware. To block Internet radio, which uses MPEG (.mpg, mpeg, or .abs) or Microsoft audio (.wav) files, enter audio/x-mpeg or audio/x-wav as blocked MIME types. To block streaming media, which uses MPEG video, enter video/mpeg or video/x-msvideo as blocked MIME types. To block access to executables (.exe), enter application/octet-stream as a blocked MIME type.

IP-based exemption

If you want to exempt certain clients or sub-networks from all filtering (including spyware filtering), you can use the **BLOCK/ACCEPT > IP Block/Exempt** page and specify the source IP address for those clients under IP and Port Exemptions. For example, if you want to exempt an executive's client machine from all filtering, you can do so using the IP address of the client. Similarly, if you want to exempt certain external devices (such as trusted servers outside the protected network), from all filtering, you can specify the destination IP address and specific port under **IP and Port Exemptions**.

Exempted IP addresses will bypass the following block filters:

- Content filtering
- IM blocking
- All types of download blocking

Exempted IP Addresses will bypass ALL filters including spyware and virus filters.

IP-based blocking

To block ALL IP-based URLs, set **Block IP Based URLs** to Yes on the **BLOCK/ACCEPT > URL Patterns** page. The default and recommended value for this setting is *No*.

If you want to block certain clients or sub-networks from all access, you can use the **BLOCK/ACCEPT > IP Block/Exempt** page and specify the source IP address for those clients under **IP and Port Exemptions**. For example, if you want to block traffic from a suspicious client machine or email servers or internal web servers, you can do so using the IP address of the client. Similarly, if you want to block certain external devices, you can specify the destination IP address and specific port under **IP and Port Exemptions**. Note that when the Barracuda Web Filter is deployed as a forward proxy, IP block/exempt rules based on request destination are not applied.

Application Filtering for Non Web Based Applications

The Barracuda Web Filter supports application filtering for *inline* deployments and not for proxy deployments. Since the Barracuda Web Filter Vx virtual machine only supports proxy deployments, it does not support application filtering.

Use the **BLOCK/ACCEPT > Applications** page to block or allow specific application traffic over the HTTP (and HTTPS) protocol that is not browser-based. For example: iTunes (Music Store, update), BitTorrent, various games, Skype, Pandora, Adobe Acrobat, FTP.

For a user to download or use an application, the user's application needs to communicate with an external server. When you select to block an application, the Barracuda Web Filter searches for traffic that contains data associated with an application server and then blocks that traffic.

Related Articles

- [Using SSL Inspection With the Barracuda Web Filter](#)
- [How to Configure SSL Inspection 7.x](#)
- [How to Configure SSL Inspection 6.x](#)

Exceptions to policies can be created for a specific user or group based on bandwidth quotas, time of day and/or days of the week. For example, you might want to allow employees to access certain applications such as Skype, for example, ONLY during lunch hours. See [Limiting Access by Time frames](#), [Time Quotas and Bandwidth Quotas](#). You can use the applications filter as a pre-emptive measure to protect your network against malware.



Most common web applications are accessed over HTTPS. Note that application filtering configured on the **BLOCK/ACCEPT > Applications** page does NOT scan for content. If you need to scan and filter content over HTTPS, you must enable [SSL Inspection](#). Note, however, that the SSL Inspection feature is only available on the Barracuda Web Filter 610 and higher, and requires more system resources and installation of SSL certificates to configure. For background on SSL Inspection, see [Using SSL Inspection With the Barracuda Web Filter](#).

To simply block/allow specific functions that run within web applications, such as Facebook games or comments, or Skype chat, configure on the **BLOCK/ACCEPT > Web App Control** page.

Using Custom Categories

If you navigate to the **Block/Accept > Custom Categories** page, you can build your own custom categories using any specific domains you would like to include, any existing categories you would like to include, or both. All you need to do is:

1. Name your category at the top using the **Category Name** field.
2. Enter the names of the domains you would like to include in the **Domains** field.
3. Select the existing categories you would like to include in this category and click the **< Add** button.
4. When you've finished and are ready to create this new custom category, click the **Add** button at the bottom of the page.

Custom categories can be used in the same ways as existing categories. You can apply any rules or exceptions to custom categories in the same way as you would using existing categories.

Exception Policies 6.x

This article applies to the Barracuda Web Filter running firmware versions up to 6.x. For version 7.0 and higher, see [Exception Policies 7.x](#).

Once you have created desired block and accept policies, use the **BLOCK/ACCEPT > Exceptions** page to create exception policies for specific users or groups so they can override the filters that block, warn or monitor access to applications and websites. You can create temporary exceptions, called Temporary Whitelisting, using the **ADVANCED > Delegated Admin** page. You can create exception policies for the following types of filters:

- Domains
- URL Patterns
- Content, including Safe Search
- Applications
- Search Terms
- Web Applications
- All web traffic

You may want to create an exception policy that allows a subset of your users to access content that is blocked for other users. For example, some organizations configure their content filters to block access to Job Search and Career Development sites like Monster.com. However, your Human Resources department may require access to such sites. In this case, you can create an allow exception for the Job Search and Career Development Subcategory and assign the policy to your Human Resources group.

In this article:

- [How Exceptions Work](#)
- [Policy Alerts](#)
- [Temporary Whitelist Exceptions](#)
- [Limiting Access by Time frames, Time Quotas and Bandwidth Quotas](#)
- [Safe Browsing / Safe Search - Limiting to Specific Users](#)
- [Filtering on Search Terms](#)

How Exceptions Work

When a user tries to access content that is blocked by one of the Barracuda Web Filter policies, the user receives a block message. If the user is not authenticated with NTLM and is not using the Barracuda WSA agent, the block page will contain login fields as shown below:

Figure 1. Block page with login fields

[Cancel/Go back](#)

Access Denied

The link you are accessing has been blocked by the Barracuda Web Filter because it contains content belonging to the category of: Pornography

If you believe this is an error or need to access this link please contact your administrator.

URL: English ▾

Login

Username:

Password:

[Temporary Whitelist >>](#)

If an exception policy exists for the blocked content, the user can enter the username and password for the account that was assigned to the exception policy. After the user enters the correct account information, the Barracuda Web Filter applies the effective policy for that authenticated user.

Policy Alerts

You can configure the Barracuda Web Filter to send an email alert to one or more email addresses when a content filter rule is triggered more than a specified number of times. For example, if you block shopping and adult content categories from the **BLOCK/ACCEPT > Content Filter** page and one or more authenticated users browses sites under those categories, a Policy Alert email can be sent at a predefined interval (hourly, etc.), summarizing the top number of users violating policy and the actions taken (block, warn, etc.).

You can set a policy alert frequency for sending the summary, a format (HTML, PDF, etc.) and a count of the top number of violators per content category to include in the summary.

See the **BASIC > Administration** page to enable/disable and configure policy alerts, and then use the **BLOCK/ACCEPT > Exceptions** page to specify the action, user(s) or group(s) to include as well as the content category and threshold for when to send alerts. You can also specify email addresses to which policy alerts should be sent by role using the **ADVANCED > Delegated Admin** page.

Temporary Whitelist Exceptions

You can create temporary exceptions to ongoing policies if you need a user or set of users to be able to override a policy for a limited time (under 24 hours). This applies in particular to a user to whom you don't want to give login credentials for the Barracuda Web filter. To enable temporary exceptions, you must create a Temporary Whitelist role, login and password on the **ADVANCED > Delegated Admin** page. See [Role-based Administration 6.x](#) for information about how to create the Temporary Whitelist role and assign/limit permissions to specific users or groups. See Figure 1 above with the **Temporary Whitelist** button at the lower left of the block page.

An example of this role would be a group of students needing to access websites relative to a science class on reproduction, but those sites are typically blocked by policy. The teacher can be given the *Temporary Whitelist* role login and password or use their LDAP credentials to log in when a block page comes up. This enables the teacher to allow the blocked site (or the category of sites to which that URL belongs) for a limited time while the students do research.

Limiting Access by Time frames, Time Quotas and Bandwidth Quotas

Use the Time Quota and Bandwidth Quota exception types on the **BLOCK/ACCEPT > Exceptions** page to assign browsing limits by domain, URL, content category and/or application to specific users. A time quota specifies a quantity of time allowed for a user/group to browse certain domains, URLs content categories and/or applications, while the bandwidth quota specifies a limited amount of bandwidth allowed per user or group for the same. Bandwidth quotas include both download and upload traffic. The allow and monitor actions are available for time or bandwidth quotas.

Quotas can be configured to be in effect during the Time Frame you specify.

Example 1: Suppose you want to limit access to chat sites to 30 minutes per day during business hours.

1. First create a block policy for this content category on the **BLOCK/ACCEPT > Content Filter** page.
2. Next, on the **BLOCK/ACCEPT > Exceptions** page, create an *Allow* action for a time quota of 30 minutes for a particular user or group between the hours of 6:00 (6am) and 18:00 (6pm) for the Content Filter category and the Gaming sub category, and check each box for Monday - Friday.

Note: Exceptions are applied in the order in which they are listed in the table on the **BLOCK/ACCEPT > Exceptions** page. For example, if you want to block access to all web traffic for unauthenticated users but allow access to selected websites, first create the *block* exception and then create the *allow* exception. You can re-order exception rules once they are created by dragging and dropping exceptions in the table.

Example 2: You might want to allow limited access to gaming sites during lunch time.

1. Create a block policy on the **BLOCK/ACCEPT > Content Filter** page for the Game Playing category.
2. On the **BLOCK/ACCEPT > Exceptions** page, create an *Allow* action for a particular user or group between the hours of 12:00 (12pm) and 1:00 (1pm) for the Content Filter category and the Gaming sub category. To prevent excessive bandwidth usage (uploading or downloading), begin by creating a *Block* policy on the **BLOCK/ACCEPT > Content Filter** page for the Streaming Media category.
3. On the **BLOCK/ACCEPT > Exceptions** page, create an *Allow* action for a particular user or group for the Content Filter category and the Streaming Media sub category, which includes the following:

- Audio or video streaming services
- Internet TV and radio
- Webcam services
- VoIP (Voice over IP) or telephone services via your computer

Specify the bandwidth limit to allow for these types of traffic in kb and select Daily, Weekly or Monthly from the drop-down. Use the **ASIC > Reports** page to create reports on time and/or bandwidth usage by user, group, application, content type, domain or URL.

Safe Browsing / Safe Search - Limiting to Specific Users

If you have disabled the Safe Browsing feature on the **BLOCK/ACCEPT > Content Filter** page, all users will be able to browse freely with the listed search engines. If you enabled Safe Browsing, users will not see search engine content that contains objectionable thumbnail images in the search results; only filtered thumbnails are displayed in the search results. To limit Safe Browsing only to specific users or groups of users, create an exception using the *Enable* action, like this:

1. Select the Content Filter category.
2. Select the Safe Browsing sub category.
3. Select the *Enable Action*.
4. Click the Add button to see the exception added to the List of Exceptions table on the page.

Filtering on Search Terms

You can set an exception to *Block*, *Warn*, *Monitor* or *Allow* traffic one or more **Search Terms** you specify are found in any part of a URL. To configure:

1. Select the **Action**.
2. In **Applies To**, select what type of user or group this rule applies to.
3. Select **Search Terms** as the **Exception Type**.
4. Select how to match:
 - Match Any - match any of the words you enter in the **Sub Category** text box in any order within the URL
 - Match All - match all of the words you enter in the **Sub Category** text box in any order within the URL
 - All In Order
5. Enter one or more alphanumeric strings in the **Sub Category** text box you want to filter in entire URLs. Separate multiple search terms by single spaces.
6. Set other options such as HTTP Methods, Protocol, Time Frame or Days of Week as needed.
7. Use **Policy Alerts** (described above) if you want to be notified when your search terms are found. This is a useful feature to help detect cyberbullying, adult content or other suspicious activities.

Exception Policies 7.x

This article applies to the Barracuda Web Filter running firmware version 7.0 and higher.

Related Articles

- [How to Set Up YouTube for Schools](#)
- [How to Enable Safe Search for Students](#)

Once you have created desired block and accept policies, use the **BLOCK/ACCEPT > Exceptions** page to create exception policies for specific users or groups so they can override the filters that block, warn or monitor access to applications and websites. You can create exception policies for the following types of filters:

- Domains
- URL Patterns
- Content, including Safe Search
- Applications
- Web 2.0 applications
- Search terms (found anywhere in the URL)
- All web traffic

Exceptions are useful for creating exception policies that allow a subset of your users to access content that is blocked for other users. See [Examples](#) below.

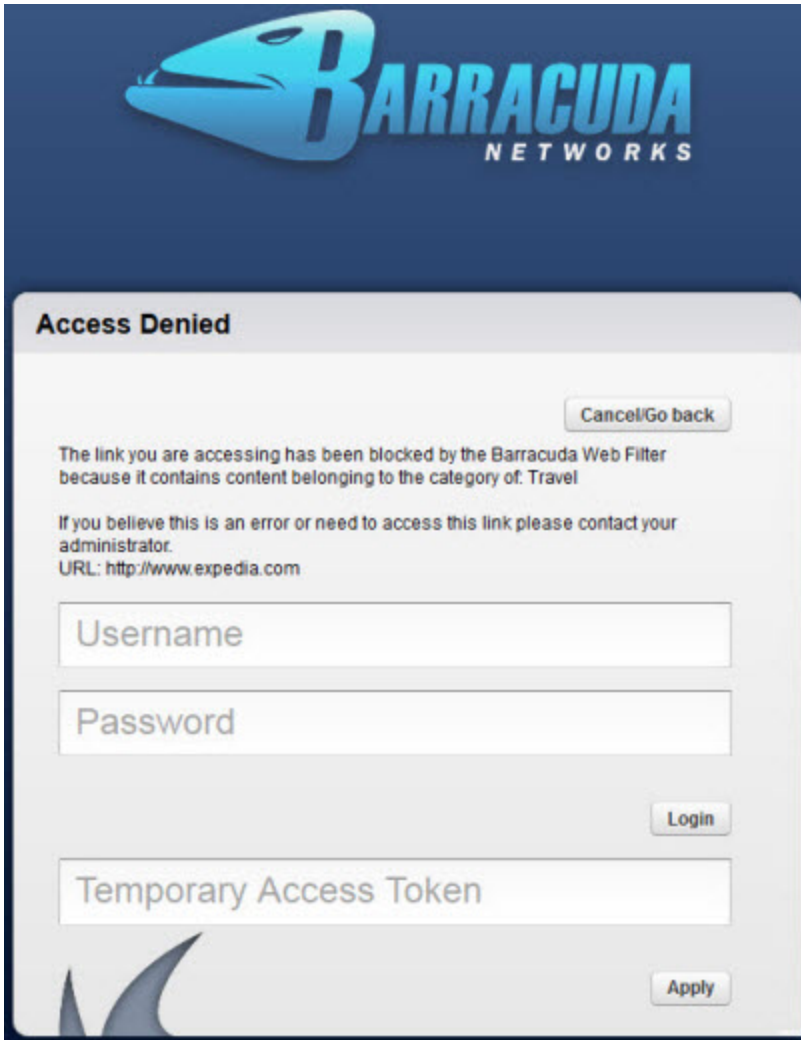
In this article:

- [How Exceptions Work](#)
- [Examples of Using Exceptions](#)
 - [Example 1 – Limiting access to job search websites](#)
 - [Example 2 – Restricting use of Google mail during business hours](#)
- [Policy Alerts](#)
- [Limiting Access by Time frames, Time Quotas and Bandwidth Quotas](#)
- [Safe Browsing / Safe Search - Limiting to Specific Users](#)

How Exceptions Work

When a user tries to access content that is blocked by one of the Barracuda Web Filter policies, the user receives a block message. If the user is not authenticated with NTLM and is not using the Barracuda WSA agent, the block page will contain login fields as shown below:

Figure 1. Block page with login fields



If an exception policy exists for the blocked content, the user can enter their username and password (LDAP credentials, if configured) for the account that was assigned to the exception policy. The block page also includes a **Temporary Access Token** field where a student can enter a code they've been given by a teacher to allow temporary access to a particular website or category of websites for classroom research. See [Temporary Access for Education](#) for details. After the user enters the correct account information, the Barracuda Web Filter applies the effective policy for that authenticated user.

Examples of Using Exceptions

Example 1 – Limiting access to job search websites

Your organization configures their content filters to block access to Job Search and Career Development sites like Monster.com. However, your Human Resources department requires access to such sites. In this case, you would do the following to create the policy:

1. Create a group called *HR* on the **USERS > USERS/GROUPS** page. Assign appropriate users to this group.
2. Create a *Block* policy for *Authenticated* users on the **BLOCK/ACCEPT > Content Filter** page.
3. On the **BLOCK/ACCEPT > Exceptions** page, create an *Allow* exception for the Group *HR*.
4. Select the *Job Search and Career Development* **Content Type** for the *Content Filter* **Exception Type**.

Example 2 – Restricting use of Google mail during business hours

You want to allow managers access to Google Apps business mail, but block personal gmail during business hours. Here are the basic steps. For detailed steps and other examples using Google Apps, see [Google Apps Control Over HTTPS](#). This example requires configuration of [SSL Inspection](#), which is available on the Barracuda Web Filter 610 and higher.

1. Create a group called *Managers* on the **USERS > USERS/GROUPS** page. Assign appropriate users to this group.
2. On the **BLOCK/ACCEPT > Exceptions** page, create a *Block* policy (exception) for <https://mail.google.com/mail> using **URL Patterns**.
3. Select a **Time Frame** of Monday - Friday, 8am - 5pm (business hours).

4. Select *HTTPS* as the **Protocol**.
5. Next, create an *Allow* exception for business Gmail use: On the **BLOCK/ACCEPT > Exceptions** page, select the *Allow Action* for *Authenticated* users.
6. Enter your business email domain name (ex: a1business.com) as the **URL pattern**.

Policy Alerts

You can configure the Barracuda Web Filter to send an email alert to one or more email addresses when a content filter rule is triggered more than a specified number of times. For example, say you block the *Propriety* and *Commerce* categories on the **BLOCK/ACCEPT > Content Filter** page and one or more authenticated users browses sites under those categories (such as *Adult Content* and *Shopping* content types respectively). A Policy Alert email can be sent at a predefined interval (hourly, etc.), summarizing the top number of users violating the *block* policy for these categories.

Where to configure Policy Alerts

- See the **BLOCK/ACCEPT > Exceptions** page to enable/disable and configure policy alerts, and to specify the action, user(s) or group(s) to include as well as the content category and threshold for when to send alerts.
- You can alternatively specify the email addresses to which policy alerts should be sent by *role* using the **ADVANCED > Delegated Admin** page.
- Configure policy alerts format (HTML, PDF, etc.) and frequency of notification emails from the **BLOCK/ACCEPT > Configuration** page.

Limiting Access by Time frames, Time Quotas and Bandwidth Quotas

Use the Time Quota and Bandwidth Quota exception types on the **BLOCK/ACCEPT > Exceptions** page to assign browsing limits by domain, URL, content category and/or application to specific users. A time quota specifies a quantity of time allowed for a user/group to browse certain domains, URLs content categories and/or applications, while the bandwidth quota specifies a limited amount of bandwidth allowed per user or group for the same. Bandwidth quotas include both download and upload traffic. The allow and monitor actions are available for time or bandwidth quotas.

Quotas can be configured to be in effect during the Time Frame you specify.

Example 1: Suppose you want to limit access to chat sites to 30 minutes per day during business hours.

1. First create a block policy for this content category on the **BLOCK/ACCEPT > Content Filter** page.
2. Next, on the **BLOCK/ACCEPT > Exceptions** page, create an *Allow* action for a time quota of 30 minutes for a particular user or group between the hours of 6:00 (6am) and 18:00 (6pm) for the *Content Filter Exception Type* and the *Gaming Content Type*, and check each box for Monday - Friday.

Note: Exceptions are applied in the order in which they are listed in the table on the **BLOCK/ACCEPT > Exceptions** page. For example, if you want to block access to all web traffic for unauthenticated users but allow access to selected websites, first create the *block* exception and then create the *allow* exception. You can re-order exception rules once they are created by dragging and dropping exceptions in the table.

Example 2: You might want to allow limited access to gaming sites during lunch time.

1. Create a block policy on the **BLOCK/ACCEPT > Content Filter** page for the Game Playing category.
2. On the **BLOCK/ACCEPT > Exceptions** page, create an *Allow* action for a particular user or group between the hours of 12:00 (12pm) and 1:00 (1pm) for the *Content Filter Exception Type* and the *Gaming Content Type*. To prevent excessive bandwidth usage (uploading or downloading), begin by creating a *Block* policy on the **BLOCK/ACCEPT > Content Filter** page for the Streaming Media category.
3. On the **BLOCK/ACCEPT > Exceptions** page, create an *Allow* action for a particular user or group for the *Content Filter Exception Type* and the *Streaming Media Content Type*, which includes the following:

- Audio or video streaming services
- Internet TV and radio
- Webcam services
- VoIP (Voice over IP) or telephone services via your computer

Specify the bandwidth limit to allow for these types of traffic in kb and select Daily, Weekly or Monthly from the drop-down. Use the **ASIC > Reports** page to create reports on time and/or bandwidth usage by user, group, application, content type, domain or URL.

Safe Browsing / Safe Search - Limiting to Specific Users

If you have disabled the Safe Browsing feature on the **BLOCK/ACCEPT > Content Filter** page, all users will be able to browse freely with the listed search engines. If you enabled Safe Browsing, users will *not* see search engine content that contains objectionable thumbnail images in the search results; only filtered thumbnails are displayed in the search results. For instructions on limiting safe browsing to a group such as, for

example, students, see [How to Enable Safe Search for Students](#).

Barracuda Web Filter for Education

The Barracuda Web Filter provides powerful tools for K-12 and beyond to easily address the complex challenges of content and mobile security facing today's school-based network administrators. Features described in this article include:

- Management of remote users off-campus and off-network
- Safe browser for iOS devices issued to students, with location tracking
- Safely providing YouTube for Schools content to classrooms
- Portal for teachers to log in and allow students temporary access to specific websites for school research projects
- Tracking of social media interactions, including detection of cyberbullying, for administrators and teachers
- Regulating use of social media and Web 2.0 applications such as Facebook games, chat and posting, Google Apps, and more

Related Articles
<ul style="list-style-type: none">• Using SSL Inspection With the Barracuda Web Filter• How to Configure Web Application Monitoring• How to Enable Safe Search for Students• Barracuda Safe Browser - FAQ• Barracuda Safe Browser Setup Guide

Tools for Administrators

Remote Filtering

With iPad Initiatives (school issued iPads) and campus-issued laptops emerging as a standard throughout the U.S. educational system, school network administrators need to track devices on and off network as well as ensure safe browsing and enforcement of school policies regarding content. For remote users with laptops, desktops and iOS devices, the Barracuda Web Filter provides location detection and the same application of policies as local users with the following tools, both of which provide:

- Location detection
- Tamper proof use
- Safe browsing

Web Security Agent (WSA)

Deployed on each remote desktop or laptop, the Barracuda Web Security Agent proxies all web traffic over the Internet to a specified Barracuda Web Filter, which has been configured to recognize each remote client by traffic signed by the Barracuda Web Filter. The same security policies are applied to remote users as those applied to other users in the rest of your network. See [Barracuda Web Security Agent - How it Works](#).

Barracuda Safe Browser (BSB)

Deploy and use the Barracuda Safe Browser on iOS mobile devices in place of the native browser, applying the same security policies as those applied by the Barracuda Web Filter to other users in the rest of your network. See [Barracuda Safe Browser Setup Guide - With Barracuda Web Filter](#).

Educational Tools, Educational Content

- [YouTube for Schools](#) - Access thousands of free high quality educational videos on YouTube in a controlled environment for your students. You can create your own school account for access to *YouTube EDU* content.
- [Temporary Access](#) to websites for student research - A portal to the Barracuda Web Filter where teachers can request and manage temporary access for students to specified domains or categories of domains that are typically blocked by school policy.

Social Networking and Web 2.0 - Regulating Use of Applications

The Barracuda Web Filter enables granular control over Web 2.0 applications. For example you can allow access to Facebook messages but block games, chat, posts etc. You can provide safe access to YouTube videos that provide rich educational content using your [YouTube for Schools](#) account. With Web Application Monitoring, you can capture and archive the content of social media interactions. See [How to Configure Web Application Monitoring](#).

The Barracuda Web Filter also provides SSL inspection if users access these applications over HTTPS. For schools this provides powerful benefits with common use cases such as these:

- [Google Apps Control Over HTTPS](#) - Granular regulation of Google Apps tools over HTTPS (Business Gmail as opposed to personal Gmail, and more)
- [YouTube Control Over HTTPS](#) - Granular regulation of YouTube over HTTPS
- [Facebook Control Over HTTPS](#) - Granular regulation of Facebook applications (chat, posting, games, etc.)
- [Suspicious Keyword Tracking](#) - Monitor social messaging in real time, with keyword alert emails to teachers or administrators to trigger immediate responses to emerging cases of bullying, harassment, or loss of confidential data. This feature does *not* require the use of SSL Inspection unless you want to monitor HTTPS traffic content, and is available on the Barracuda Web Filter 610 and higher.

Note that SSL inspection is an opt-in feature available in forward proxy deployments with the Barracuda Web Filter 610 and above. Also available for inline deployments with the Barracuda Web Filter 910 and 1010.

Delegated Administration

The administrator of the Barracuda Web Filter can choose to delegate certain administrative tasks such as scheduling or running reports, viewing system status, load and log pages, or creating exceptions to policy. For example, school districts can maintain system level control while providing restricted access to individual schools to manage policies or generate reports for teachers. See [Role-based Administration](#) for details.

General Web Filtering on the Campus Network

- Blocking access to proxy servers students might try to use to circumvent web filtering policies. IT administrators must know the IP addresses of any proxies to block as part of school policy. Ability to add new URLs daily as reported by teachers or other trusted sources.
- Ability to create custom categories of domains for specific filtering.
- Ability to report bad URLs to Barracuda Networks. Newly reported URLs to block and improved content filtering rules are updated to your Barracuda Web Filter on a daily basis.
- Sophisticated application control - block, monitor, warn, allow on Skype, Spotify, gaming software, communications, etc. See [How to Configure Web Application Monitoring](#).

Safe Browsing / Safe Search - Limiting to Students

You can enable the **Safe Browsing** feature on the **BLOCK/ACCEPT > Content Filter** page so that the group of users you specify will *not* see search engine content that contains objectionable thumbnail images in the search results; only filtered thumbnails are displayed in the search results. To limit **Safe Browsing** only to students, but allow appearance of all thumbnail images in search results for teachers and staff, see [How to Enable Safe Search for Students](#).

Tools for Teachers

- Temporary Access for Students (see above) - For school research projects or other classroom needs, with an easy to use web interface. See [How to Use Temporary Access for Students - Teacher's Guide](#)
- [Suspicious Keyword Tracking](#) and Cyberbullying Alerts (teachers can submit new keywords, keyword categories to their system administrator)
- YouTube for Schools access (see above)



How to Set Up YouTube for Schools

This feature applies to the Barracuda Web Filter 5.0 and higher.

In this article:

- [About YouTube for Schools](#)
- [Configuring YouTube for Schools](#)
- [Blocking HTTPS Access to YouTube.com](#)
- [How to Bypass the YouTube for Schools Feature for Specific Users](#)

Related Articles

- [Creating Block and Accept Policies](#)
- [Best Practices in Configuring Policy](#)

About YouTube for Schools

Access thousands of free high quality educational videos on YouTube in a controlled environment for your students. You can create your own school account for access to [YouTube EDU](#) content as well as a customizable playlist of videos that will be viewable only within your own school network. To learn more about what **YouTube for Schools** offers, visit the [YouTube for Schools](#) website. Please read through this article carefully to understand how to best provide access for your users to YouTube for Schools content.

Configuring YouTube for Schools

For educational institutions wishing to use YouTube For Schools filtering, the procedure to configure the Barracuda Web Filter follows:

1. Log into your YouTube.com account and sign up for YouTube for Schools here:
http://www.youtube.com/education_signup.
2. You can find instructions for setting up your YouTube for Schools account here: [Signing up and Getting Started](#).
 - a. During the sign up process, YouTube.com will provide you with a security token, or 'unique ID', which is a string of characters.
 - b. Save this string and enter it into the **YouTube for Schools Token** field in the **Safe Browsing Configuration** section on the **BLOCK/ACCEPT > Configuration** page on the Barracuda Web Filter. This string will be appended by the Barracuda Web Filter to a custom HTTP Header that will be used to identify all web traffic from computers on your school network.

For example, the ID string you receive from YouTube for Schools might look something like this: ABCD1234567890abcdef. The Barracuda Web Filter will append this string to a field named

X-YouTube-Edu-Filter

to create a customer HTTP header, like this:

X-YouTube-Edu-Filter:ABCD1234567890abcdef

All outgoing traffic to YouTube.com from the Barracuda Web Filter will include this custom HTTP header to identify your school's network. If you are not blocking Streaming Media (on the **BLOCK/ACCEPT > Content Filter** page) on your Barracuda Web Filter, go to step 5.

3. If you are blocking Streaming Media, you will need to create a new Custom Category on the **BLOCK/ACCEPT > Custom Categories** page. **Caution:** When naming your Custom Category, use something unique that is not already included on the **BLOCK/ACCEPT > Content Filter** page. For example, in this case, you might name the new category *Youtube Edu*.
4. Ensure that the following top-level domains are not blocked, so add them to the **Domains to be Included** box:
youtube.com
yting.com

You must also check the **Recategorize Domains** box. This ensures that these two domains will be removed from the *Streaming Media* category. If you don't recategorize them, YouTube media will be blocked.

5. From the **BLOCK/ACCEPT > Content Filter** page, scroll down to **Saved Custom Categories** and click **Allow** for your new category for both Authenticated and Unauthenticated users (selected at the top of the page).
6. In the **Safe Browsing** section, enable **YouTube For Schools** for both Authenticated and Unauthenticated users.

Blocking HTTPS Access to YouTube.com



If you are running version 6.0.1 or higher and want to block HTTPS access to YouTube.com and variants and subdomains of YouTube.com, you can create an exception for HTTPS traffic by doing the following (see Figure 1 below):

1. On the **BLOCK/ACCEPT > Exceptions** page, select the *Block Action*.
2. For **Applies To**, select the types of users to include in your exception. In this example, the users who will be blocked are *Authenticated*.
3. Select *Content Filter* for **Exception Type**.
4. In the **Content Type** drop-down, select the custom category you created in step #3 above.
For example, if you created a new custom category for YouTube for Schools called *Youtube Edu*, select that Content Type.
5. If desired, select a Time Frame and/or Days of Week to apply the exception. In this example, the policy is enforced weekdays.
6. Select *HTTPS* in the **Protocol** drop-down.
7. Click the **Add** button to see the exception added to the **List of Exceptions** table below (see Figure 3). Now the Barracuda Web Filter will allow all YouTube for Schools via HTTP, but will block HTTPS traffic from YouTube.com and its subdomains and variants.

Important: A prerequisite to this configuration is that, in your Google account, you must **not** enforce 'HTTPS Only' for YouTube. HTTP traffic must be allowed. Also note that, if the user types HTTPS into the YouTube.com URL, access will be blocked and, if the Barracuda Web Filter is deployed inline, no block page will be presented. The user must then type HTTP for the YouTube.com URL to have access to YouTube.com content.

Figure 1: Creating an exception to block HTTPS traffic from YouTube.com, while allowing HTTP traffic.

How to Bypass the YouTube for Schools Feature for Specific Users

(Version 6.0.1 and higher)

If the YouTube for Schools feature is enabled under **Safe Browsing** on the **BLOCK/ACCEPT > Content Filter** page, you can create an exception for a specific user or group of users to bypass this feature by doing the following:

1. On the **BLOCK/ACCEPT > Exceptions** page, select the *Content Filter Exception Type*.
2. Select the *YouTube for Schools Content Type* (in the **Safe Browsing** section of the drop-down list).
3. Select the *Disable* Action to allow the specified user or group to bypass the YouTube for Schools feature.
4. In the **Applies To** drop-down, select the user(s) or group to allow to bypass YouTube for Schools. In this example, the *Finance* group is selected.
5. If desired, select a Time Frame and/or Days of Week to apply the exception. In this example, the policy is enforced weekdays.
6. Click the **Add** button to see the exception added to the **List of Exceptions** table below (see Figure 3).

Figure 2: Creating an exception to allow the Finance group to bypass YouTube.com.

Figure 3: List of exceptions created above.

ID	Action	Applies To	Proto...	Match Type	Schedule	Quota	Exception ...	Sub Category/Expres...	Message	Alert	HTTP Meth...	Disa...	Edit
11	Disable	Finance	All				Content Fi...	YouTube for Schools		No			Edit
12	Block	Authenticated	HTTPS		Weekdays		Content Fi...	Youtube Edu		No			Edit
2	Allow	All Users	All		01:00 - 24:...	1000 KB/...	Content Fi...	Streaming Media		No			Edit

How to Enable Safe Search for Students

You can enable the **Safe Browsing** feature on the **BLOCK/ACCEPT > Content Filter** page so that the group of users you specify will *not* see search engine content that contains objectionable thumbnail images in the search results; only filtered thumbnails are displayed in the search results. To limit **Safe Browsing** only to students, but allow appearance of all thumbnail images in search results for teachers and staff, create an exception using the *Enable* action, like this:

1. On the **USERS/GROUPS > Local Groups** page, create a new group called *Students*.
2. On the **USERS/GROUPS > New Users** page, add the students' usernames on the Barracuda Web Filter to the *Students* group, following instructions in the online help for that page.
3. On the **BLOCK/ACCEPT > Content Filter** page, in the table under **Safe Browsing**, select *Disable* for each search engine listed in the table, or click the [All](#) link.
4. On the **BLOCK/ACCEPT > Exceptions** page, create the policy:
 - a. For **Applies To**, select *Local Group*, and then in the next drop-down, select *Students*.
 - b. Select the **Exception Type** as *Content Filter*.
 - c. For **Content Type**, scroll down and select *Safe Browsing*.
 - d. Select the **Enable Action** (it may be automatically selected) above.
 - e. Click the **Add** button to see the exception added to the **List of Exceptions** table on the page.

Related Articles

- [Temporary Access for Education](#)
- [Temporary Access for Students - Teacher's Guide](#)
- [Barracuda Web Filter for Education](#)
- [Barracuda Safe Browser Setup Guide](#)
- [Barracuda Safe Browser - FAQ](#)



Suspicious Keyword Tracking

This feature is available with the Barracuda Web Filter 610 and higher running version 7.0 and higher.

The Barracuda Web Filter can identify, track and report on suspicious keywords in filtered social media traffic for notification and reporting purposes. For identifying cyberbullying, profanity, terrorism, adult content and other suspicious social media communications, Barracuda Networks employs a *suspicious keywords* lexicon to which you can add custom keywords you want the Barracuda Web Filter to scan for and flag in captured social media traffic.

Related Articles

- [How to Configure Web Application Monitoring](#)
- [How to Configure SSL Inspection](#)
- [Using SSL Inspection With the Barracuda Web Filter](#)

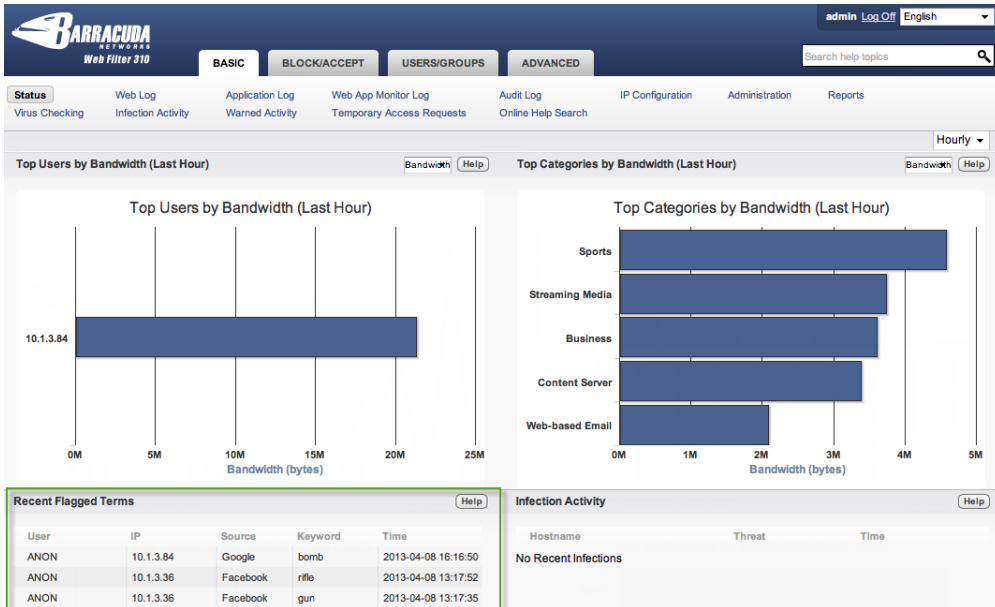
You can configure alerts to be sent when these keywords are detected in captured traffic. The **SSL Inspection** feature must be enabled on the **ADVANCED > SSL Inspection** page to use this feature. Using SSL inspection involves creating and/or installing SSL certificates in the Barracuda Web Filter and, for self-signed certificates, in all client browsers. For details, see [Using SSL Inspection With the Barracuda Web Filter](#) and [How to Configure SSL Inspection](#).

To configure Suspicious Keyword Tracking, do the following:

1. From the **BLOCK/ACCEPT > Web App Monitor** page, enable web application monitoring for specific actions you select in Facebook, Twitter, Google and other popular social media portals. Granularity of actions includes chat, login, wall post, user registration, sending email and more.
2. Optionally specify a **Web Activity Archiving Email Address** on the page, and the Barracuda Web Filter will package each interaction as an SMTP message and email it to that address. Archived messages can then be indexed and searched by source or content, and alerts can be generated per policy you set in your archiving solution. For information about searching archived messages and using policy alerts with the Barracuda Message Archiver, see [Understanding Basic and Advanced Search](#) and [Policy Alerts](#).
3. Enable tracking and flagging of suspicious keywords by selecting the keyword categories you want to scan for in the web applications and actions enabled on the page. Click **Save** after making your selections to update the configuration. A report summarizing content policy violations based on the selected Suspicious Keyword Categories will be emailed to the **Suspicious Keywords Alert Email Address** you define in this section.
4. Optionally create your own custom keyword categories and associated words to scan for in searches and social media activities. For each custom keyword category, enter your own words, each on a new line, that you wish to include in the keyword group. Click **Add**. The new keyword category is added to the table.
5. Enable **SSL Inspection** on the **ADVANCED > SSL Inspection** page and create or upload an SSL certificate. Follow instructions in [How to Configure SSL Inspection](#) to choose the best way to set up your SSL certificate.

The **BASIC > Status** page includes a section showing **Recent Flagged Terms** from the suspicious keywords lexicon that were identified in captured social media interactions, as shown in Figure 1 below.

Figure 1: Recent Flagged Terms (suspicious keywords) in captured social media interactions



slang, pornography, terrorism, cyberbullying, cyber, bullying

Temporary Access for Education

This article applies to the Barracuda Web Filter running firmware version 7.0 and higher.

The Temporary Access feature provides a portal where teachers can request and manage temporary access for students to specified domains or categories of domains that are typically blocked by school policy. In this way, students can access web content that may be useful for research projects or other classroom needs on a temporary basis.

Related Articles

- [How to Use Temporary Access for Students - Teacher's Guide](#)
- [Exception Policies - for administrators](#)
- [Role-based Administration 7.x](#)

If the teacher's requested domains are approved, the Barracuda Web Filter issues a security token to the teacher to give to students to bypass block pages when browsing specific websites. The teacher can specify a time frame during which security tokens are valid, and can disable tokens at will. The administrator can revoke access for any security token, and can grant or revoke access to the Temporary Access portal to teachers. Certain domains or categories of domains can be prohibited by the administrator from ever being granted temporary access.



Administrators have full visibility into teacher and student browsing activity via the **BASIC > Temporary Access Requests** log page in the Barracuda Web Filter web interface. The teacher has a log of requests they've made and tokens assigned for accessing approved websites as shown in Figure 8.

Workflow for Administrators

1. Begin by enabling the Temporary Access portal for teachers from the **ADVANCED > Temporary Access** page in the Barracuda Web Filter web interface. From this page you can also:
 - a. Create a list of teachers and configure whether the teacher logs in using their LDAP credentials, or with credentials you create on this page
 - b. Specify maximum time frame the teacher can use for student access tokens to remain valid
 - c. List domains and or categories that will always be prohibited from temporary access
 - d. Specify maximum number of domains or categories that can be requested by a teacher
 - e. Use the **Limited To** field control to limit who can use the Temporary Access feature based on Local users, Groups or IP

addresses.

See the **ADVANCED > Temporary Access** page for details about the configuration.

2. Make sure that the email address contact you want attached to the [ContactIT](#) link on the Temporary Access portal (see Figure 1 below) is entered in the **System Alerts Email Address** in the **Email Notifications** section of the **BASIC > Administration** page.
3. Copy and paste the URL for the Temporary Access Portal from the **ADVANCED > Temporary Access** page into an email to the teacher. The URL is defined as <https://YourWebFilterIPAddress/portal>. Include in the email the credentials you created on the page for the teacher, or instruct them to use their LDAP credentials if you checked the **Use LDAP Authentication** checkbox. Also include a link to the article [How to Use Temporary Access for Students - Teacher's Guide](#), which has step-by-step instructions for the teacher to request domains and get tokens to give their students. This article is also linked from within the help file that appears upon clicking the **Help** button on the Temporary Access Portal pages.
4. Use the **BASIC > Temporary Access Requests** page to monitor activity of tokens by teacher username and date/time. You can also revoke tokens on that page.

Prohibited Categories and Domains

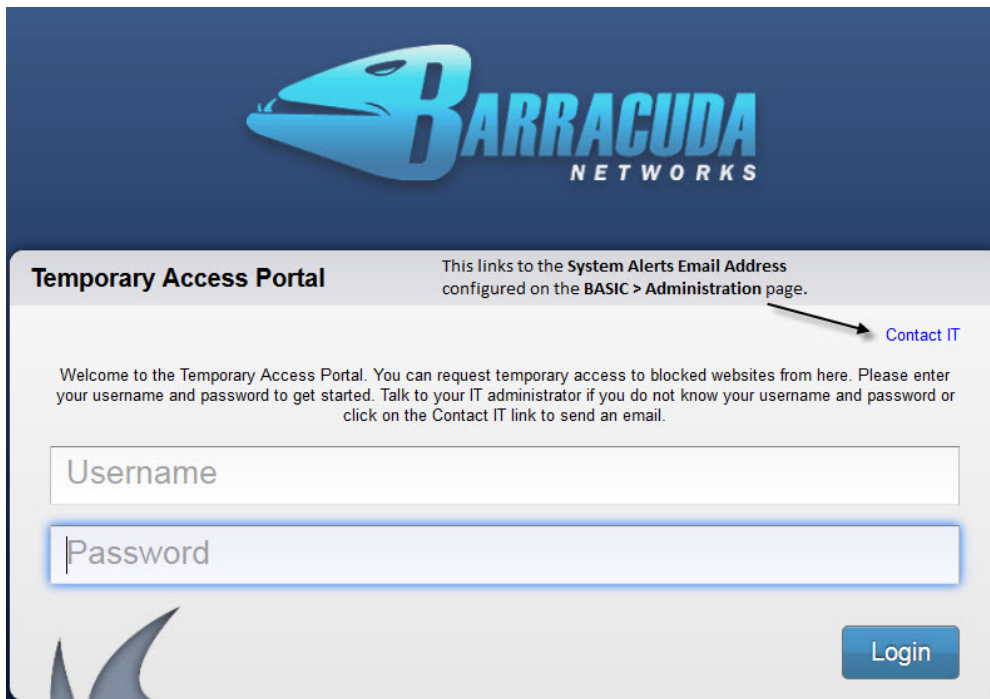
If you have specified, from the **ADVANCED > Temporary Access** page, any categories or domains that are *prohibited* from temporary student access, be sure to let the teacher know which ones are prohibited; otherwise, if the teacher requests those domains or categories, he/she will receive an error message in the Temporary Access Portal.

Workflow for the Teacher

The workflow documented here helps the administrator to understand how to use the **ADVANCED > Temporary Access** page to configure this feature, and answers some questions the teachers might have about getting and managing security tokens to give students to access specific websites. For a set of instructions to give to teachers, see [How to Use Temporary Access for Students](#), which can also be printed out as a PDF.

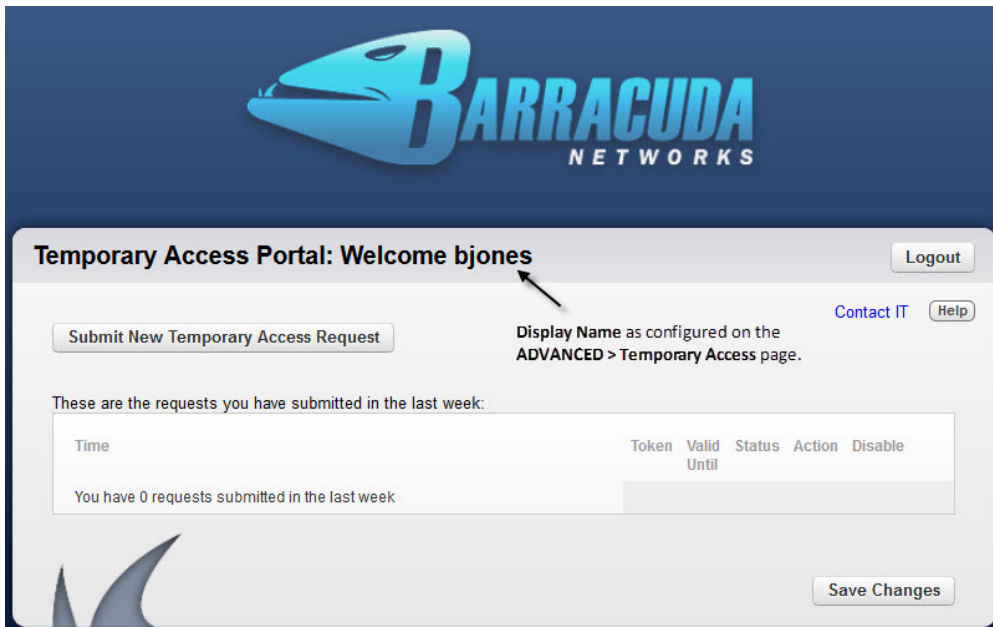
1. The teacher receives an email from the system administrator containing:
 - URL for the Temporary Access Portal
 - Either credentials for logging into the portal, or instructions to use their LDAP credentials
2. The teacher sees this login page upon browsing the URL and logs in as instructed.

Figure 1: Temporary Access Portal Login page



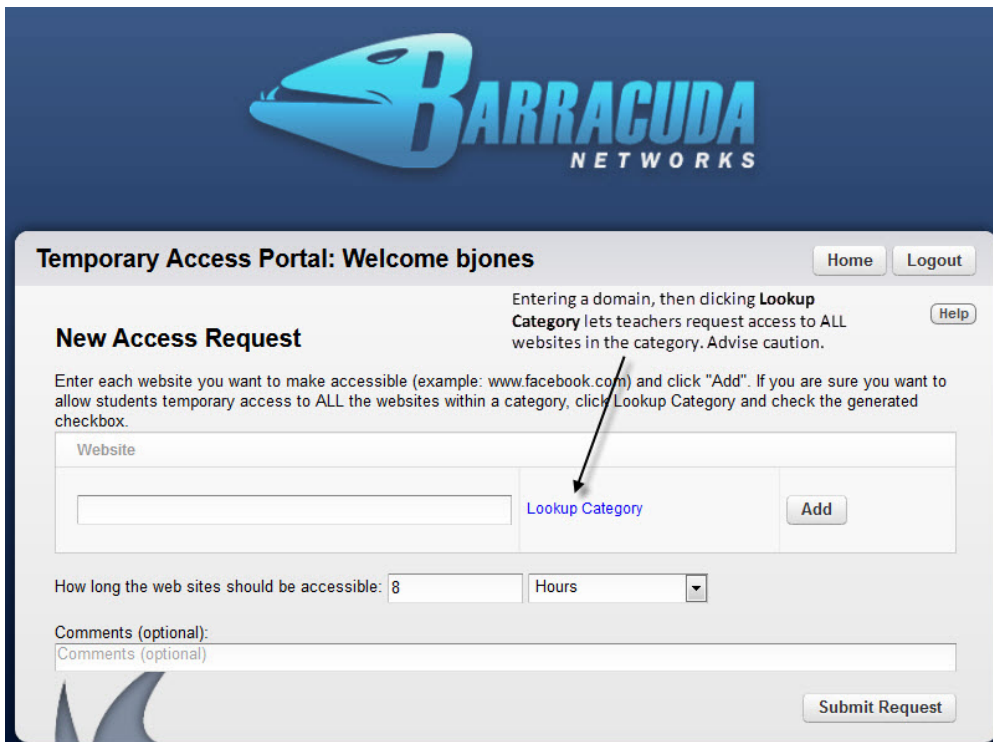
3. Once the teacher logs in, the Temporary Access Portal home page appears. In this case, the **Display Name** entered on the **ADVANCED > Temporary Access** page for the teacher who is logged in is *BJones*.

Figure 2: Temporary Access Portal Welcome page



- The teacher clicks **Submit New Temporary Access Request** to begin requesting domains for temporary student access from the Temporary Access Portal Home page.

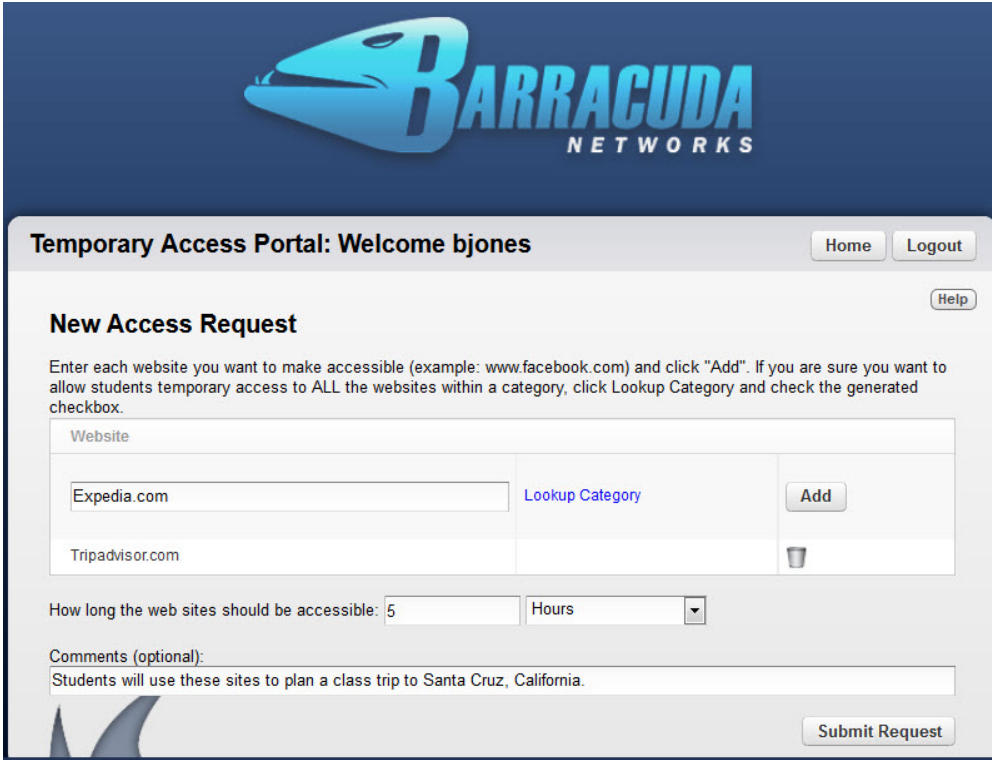
Figure 3: Temporary Access Portal Home page



Via the portal, the teacher can enter domains and/or select from a list of *sub-categories* (not *categories*) as defined on the **BLOCK/ACCE PT > Content Filter** page, including any custom categories you have defined. In the example shown in Figure 4, the teacher has requested the Tripadvisor.com domain and is about to request Expedia.com. If the teacher had selected the *Travel* sub-category (where the category is *Leisure*), those domains would have been included along with lots of other domains categorized as 'travel'. But if the teacher only wants the students to be able to access these two travel domains, then only the explicit domains should be requested.

Discussing the **Lookup Category** option with teachers and educating them about categorization of domains may better prepare them to use it safely.

Figure 4: In this example, the teacher has selected *Tripadvisor.com* and is about to select *Expedia.com* for temporary student access.



The teacher cannot actually select an entire category; only sub-categories, as shown below. However, to simplify instructions for teachers, the documentation will refer to selection of *categories* for an entire set of websites. After selecting the requested domains and/or sub-categories for temporary student access, the teacher selects the time frame for access and optionally enters a comment, such as the reason for access to these domains. All of this data is logged by date and username for the administrator to monitor on the **BASIC > Temporary Access Requests** page. The domains, sub-categories and comments (if any) entered by the teacher will appear in the *Details* popup linked to that page.

Figure 5: The teacher has clicked **Lookup Category** for the domain *Expedia.com*. *Travel* is a sub-category of the *Leisure* category.



Temporary Access Portal: Welcome bjones Home Logout

Help

New Access Request

Enter each website you want to make accessible (example: www.facebook.com) and click "Add". If you are sure you want to allow students temporary access to ALL the websites within a category, click Lookup Category and check the generated checkbox.

Website	
Expedia.com	<input type="checkbox"/> Travel Lookup Category
Tripadvisor.com	<input type="checkbox"/>

How long the web sites should be accessible: Hours

Comments (optional):
Students will use these sites to plan a class trip to Santa Cruz, California.

5. After the teacher makes a request for access to one or more sub-categories and/or domains and clicks **Submit Request**, the Barracuda Web Filter returns a token (as shown in Figure 6), and the teacher can click the [Make Another Request](#) link at the bottom of the page for more additions. The teacher gives the domain names and token to the students, who input the token to block pages when accessing those domains.

Figure 6: Getting a token that is associated with access to all domains and/or sub-categories in a request.



Temporary Access Portal: Welcome bjones Home Logout Help

Request Granted
Thank you - your request has been approved. Please provide the Token on this page to students for use in accessing the websites you have requested. The Token will expire in the time specified below.

Token: nmtaad

Website
Tripadvisor.com

How long the web sites should be accessible: 5 Hours

Comments (optional):
Comments (optional)

[Make Another Request](#)

When the student tries to access a typically blocked website, he or she can enter the token as shown below to bypass the block page and browse the site for the temporary time frame requested by the teacher:

Figure 7: The student enters the token to bypass the block page for sites the teacher has requested



Access Denied

Cancel/Go back

The link you are accessing has been blocked by the Barracuda Web Filter because it contains content belonging to the category of: Travel

If you believe this is an error or need to access this link please contact your administrator.

URL: <http://www.expedia.com>

Student types in token here

Login

Apply

Managing Temporary Access Requests and Tokens

When the teacher logs into the Temporary Access Portal, they can view a list of their temporary access requests on the home page. To view this list from another page, the teacher clicks **Home** in upper right of the portal. For each request, the status and expiration dates are displayed for the associated tokens.

From this page the teacher can disable a token before it expires, if necessary, by selecting the **Disable** check box, or can click the [Copy](#) link to make a copy of the original request to renew it. Clicking [Details](#) for a request displays associated domains, categories, and comments.

The administrator can view the same detail about tokens and revoke tokens from the **BASIC > Temporary Access Requests** page.

Figure 8: List of temporary access requests made by *bjones* in the last week



Temporary Access Portal: Welcome bjones Logout

[Submit New Temporary Access Request](#) Contact IT Help

These are the requests you have submitted in the last week:

Time	Token	Valid Until	Status	Action	Disable	
2013-03-28 13:36:45	G5NcNC	2013-03-28 18:36:45	Active	Copy	<input type="checkbox"/>	Details
2013-03-28 13:31:30	n8bywA	2013-03-28 18:31:30	Active	Copy	<input type="checkbox"/>	Details
2013-03-26 09:30:24	lirkTb	2013-03-26 14:30:24	Expired	Copy	<input type="checkbox"/>	Details
2013-03-21 08:38:20	J433vt	2013-03-21 13:38:20	Expired	Copy	<input type="checkbox"/>	Details
2013-03-21 08:37:58	zzOPLJ	2013-03-21 13:37:58	Expired	Copy	<input checked="" type="checkbox"/>	Details

Save Changes

How to Use Temporary Access for Students - Teacher's Guide

This article applies to the Barracuda Web Filter running firmware version 7.0 and higher.

With the Temporary Access feature of the Barracuda Web Filter, you can let your students temporarily access websites that are blocked by school policy. You can create a list of domains (websites) that you want students to access and specify how long this access should be granted. The maximum allowed time frame is determined by your system administrator.

To get temporary access for your students, use the Temporary Access Portal. In the portal, you can request temporary access to certain domains for a specific period of time. When you submit your list of domains (or category of domains), you will receive a temporary access token for your

students. When your students browse any of the domains in your list, they can use this token to bypass block pages. The token has an expiration time and date, after which the domains in your list be blocked again per school policy.

In the Temporary Access Portal, you can view the status and expiration dates of the tokens for your temporary access requests. You can also choose to disable tokens before they expire.

In this article:

- [Choosing Domains and Categories of Domains](#)
- [Steps to Request Temporary Access for Students](#)
- [How Students Use the Temporary Access Token](#)
- [Managing Temporary Access Requests and Tokens](#)

Choosing Domains and Categories of Domains

You can request temporary access for specific domains, as well as entire categories of domains. Domains, or websites, are commonly categorized into groups so that schools and other organizations can create safe browsing policies for their users. For example, travel websites would be in the **Travel** category. To let students access travel websites when planning a school trip, you can request that they be granted temporary access to this category. However, use caution when allowing an entire category. Verify with your system administrator that the category does not have objectionable content.

Prohibited Categories and Domains

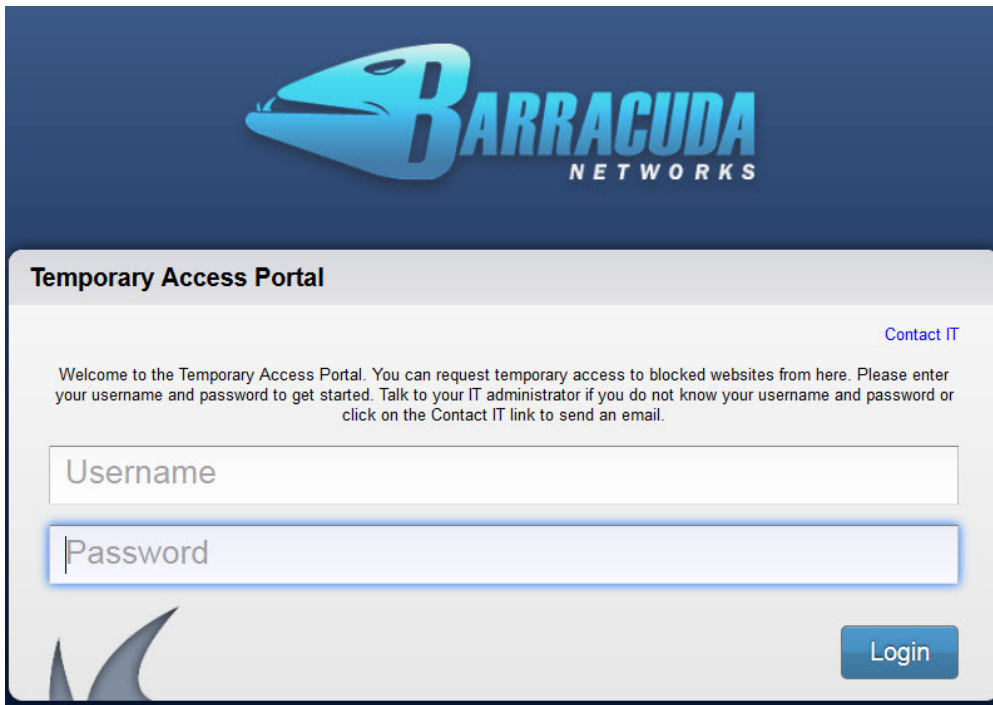
If your system administrator has prohibited any categories or domains from temporary student access, you will receive an error message if you request access to them. Before submitting your list of domains for temporary access, it is recommended that you let your system administrator review your list for any prohibited categories or domains.

Steps to Request Temporary Access for Students

When you have a list of domains or categories of domains that you want students to temporarily access, log into the Temporary Access Portal to submit your request and get an access token for your students.

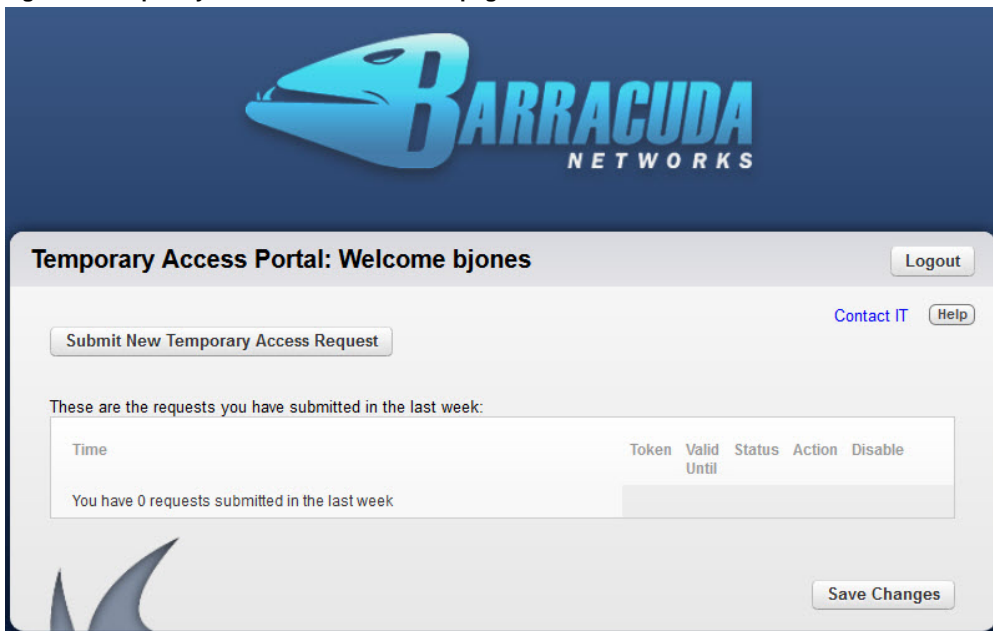
1. If you do not have a URL or a login and password for the Temporary Access Portal, request this information from your system administrator.
 - If you did not receive a login and password, you might have been instructed to use your regular network (LDAP) login and password.
 - The URL for the Temporary Access Portal will look something like this:
https://10.1.1.1/portal
2. Go to the URL for the Temporary Access Portal, enter the credentials that you received from your administrator, and click **Login**.

Figure 1. Temporary Access Portal Login page.



3. On the **Welcome** page, click **Submit New Temporary Access Request**.

Figure 2. Temporary Access Portal Welcome page.



4. In the **Website** section of the **New Access Request** form, you can add domains and categories for domains.
 - To add a domain, enter the domain name in the text field and click **Add**.
 - To add a category for a domain, enter the domain name in the text field and then click [Lookup Category](#) to see what category the domain belongs to. When the category displays, select it and then click **Add**.



When allowing an entire category, verify with your system administrator that the category does not include domains that have objectionable content.

In the example shown in Figure 3, the teacher has requested the *Tripadvisor.com* domain and is about to request *Expedia.com*.

Figure 3. In this example, the teacher has selected *Tripadvisor.com* and is about to select *Expedia.com* for temporary student access.

BARRACUDA NETWORKS

Temporary Access Portal: Welcome bjones Home Logout Help

New Access Request

Enter each website you want to make accessible (example: www.facebook.com) and click "Add". If you are sure you want to allow students temporary access to ALL the websites within a category, click Lookup Category and check the generated checkbox.

Website		
<input type="text" value="Expedia.com"/>	Lookup Category	<input type="button" value="Add"/>
<input type="text" value="Tripadvisor.com"/>		<input type="button" value=""/>

How long the web sites should be accessible:

Comments (optional):

In the example shown in Figure 4, the category has been looked up for *Expedia.com*.

Figure 4. After clicking **Lookup Category** for the domain *Expedia.com*, the *Travel* category is displayed.

BARRACUDA NETWORKS

Temporary Access Portal: Welcome bjones Home Logout Help

New Access Request

Enter each website you want to make accessible (example: www.facebook.com) and click "Add". If you are sure you want to allow students temporary access to ALL the websites within a category, click Lookup Category and check the generated checkbox.


Website		
<input type="text" value="Expedia.com"/>	<input type="checkbox"/> Travel Lookup Category	<input type="button" value="Add"/>
<input type="text" value="Tripadvisor.com"/>		<input type="button" value=""/>

How long the web sites should be accessible:

Comments (optional):

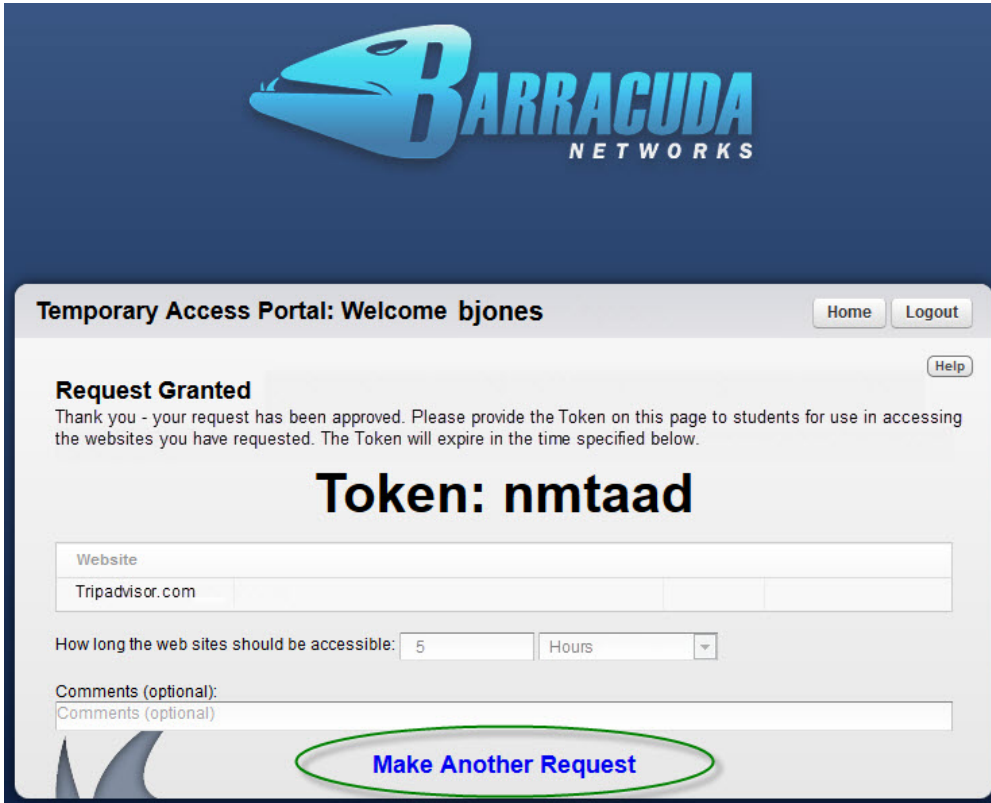
If the teacher had selected the *Travel* category, both the *Tripadvisor.com* and *Expedia.com* domains would have been included along with lots of other domains categorized as **Travel**. But if the teacher only wants the students to be able to access these two travel domains, then only those domains must be added.

5. After you enter all of the domains and categories for temporary student access, specify how long this access should be granted and optionally enter a comment that describes why access to these domains is being granted.

 Enter as much time as students will need from the moment you submit the request until you want the temporary access to expire. When you submit the request and receive a token, the time for the token immediately begins running down.

6. Click **Submit Request**. The Barracuda Web Filter returns a token (as shown in Figure 5). Give the token and list of allowed domain names to your students.

Figure 5. Getting a token that is associated with access to all domains and/or categories in a request.



7. To make another temporary access request, click [Make Another Request](#) at the bottom of the page.
8. To see a list of any other temporary access requests that you made over the past week, click **Home** in the upper right of the page.

How Students Use the Temporary Access Token

When your students try to access a blocked website, an **Access Denied** page displays. On this page, your students can enter the token to bypass the block page and browse the site for the time frame that you specified when you submitted your temporary access request.

Figure 6. The student enters the token to bypass the block page.



Access Denied

[Cancel/Go back](#)

The link you are accessing has been blocked by the Barracuda Web Filter because it contains content belonging to the category of: Travel

If you believe this is an error or need to access this link please contact your administrator.
URL: <http://www.expedia.com>

Username

Password

Student types in token here

Temporary Access Token

[Login](#)

[Apply](#)

Managing Temporary Access Requests and Tokens

When you log into the Temporary Access Portal, you can view a list of your temporary access requests on the home page. To view this list from another page, you can return to the home page by clicking **Home** in upper right of the portal. For each request, you can view the status and expiration dates of the associated tokens.

From the list of temporary access requests, you can manage tokens or view more information about the request:

- To disable a token before it expires, select the **Disable** check box.
- To extend the access time frame, click [Copy](#) to make a copy of the original request.
- To view more details for a request, click [Details](#) to view domains, categories, and comments.

Figure 7. List of temporary access requests made by bjones in the last week.



Temporary Access Portal: Welcome bjones Logout

[Contact IT](#) Help

[Submit New Temporary Access Request](#)

These are the requests you have submitted in the last week:

Time	Token	Valid Until	Status	Action	Disable	
2013-03-28 13:36:45	G5NcNC	2013-03-28 18:36:45	Active	Copy	<input type="checkbox"/>	Details
2013-03-28 13:31:30	n8bywA	2013-03-28 18:31:30	Active	Copy	<input type="checkbox"/>	Details
2013-03-26 09:30:24	lirkTb	2013-03-26 14:30:24	Expired	Copy	<input type="checkbox"/>	Details
2013-03-21 08:38:20	J433vt	2013-03-21 13:38:20	Expired	Copy	<input type="checkbox"/>	Details
2013-03-21 08:37:58	zzOPLJ	2013-03-21 13:37:58	Expired	Copy	<input checked="" type="checkbox"/>	Details

[Save Changes](#)

How to Configure Web Application Monitoring

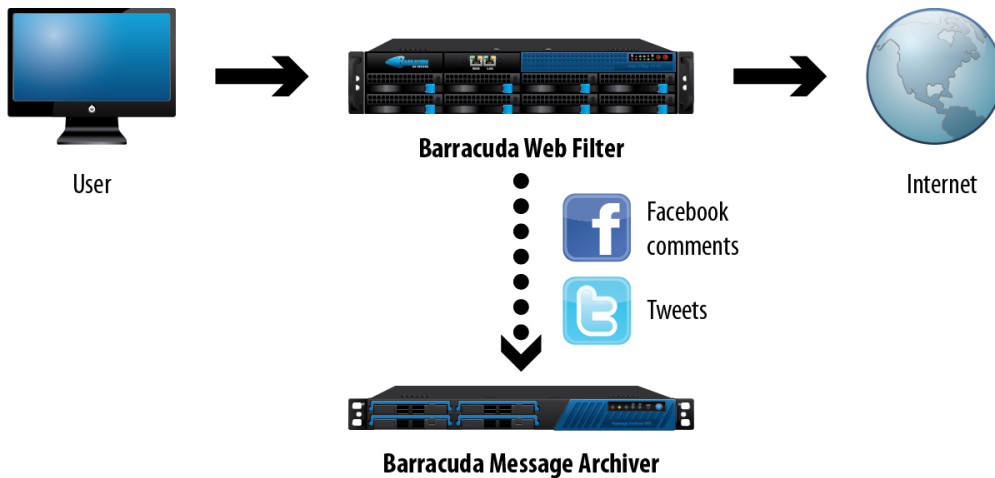
This feature applies to the Barracuda Web Filter 610 and higher running firmware version 6.0 and higher.

Capture and Archive Chat, Email, and Other Social Media Communications

The Barracuda Web Filter can inspect and catalog outbound content and forward it to an email address or external message archiver, like the [Barracuda Message Archiver](#). These messages can be tied to the users' Active Directory credentials and fully indexed, making them as easy to search as MS Exchange emails. This ensures that social media communications from corporate networks are always available for access and retrieval for eDiscovery and audits as well as to create alerts for proactive monitoring.

Use this feature to capture and archive chat, email, user registrations and other social media communications on social media portals.

Figure 1: Web Activity Monitoring



How Archiving and Searching Monitored Web Activity Works

From the **BASIC > Administration** page, you can specify a **Web App Monitor Email Address** for archiving selected actions such as logins, chat, posts, comments and associated content. The Barracuda Web Filter will package each interaction as an SMTP message and email it to this address, which can then be marked for archiving. Archived messages can then be indexed and searched by source or content, and alerts can be generated per policy you set in your archiving solution. For information about searching archived messages and using policy alerts with the Barracuda Message Archiver, see [Understanding Basic and Advanced Search](#) and [Policy Alerts](#).

NOTE: SSL Inspection must be enabled for actions shown with an asterisk (*) on the **BLOCK/ACCEPT > Web App Monitor** page to be archived. Examples include:

- Facebook *user registration and login*
- Google *chat message*
- Twitter *send tweet, login, direct message, user registration*

For a complete list of actions for which SSL Inspection must be enabled for capture, see the **BLOCK/ACCEPT > Web App Monitor** page.

For more information about SSL Inspection, see [Using SSL Inspection With the Barracuda Web Filter](#) and [How to Configure SSL Inspection 6.x](#).

Example of Social Media Archiving

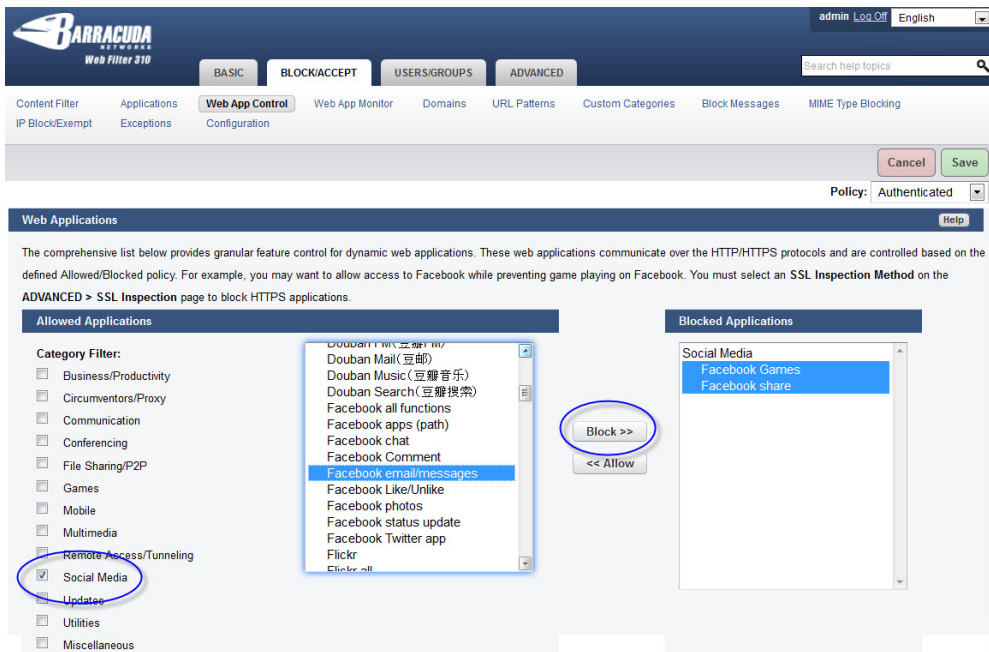
You might want to allow users in the organization to use Facebook to view and make status updates and comments, but you want to capture the content. You might also want to block games, shares and email/messages or other Facebook apps to protect your network from viruses and malware.



If you want to regulate web 2.0 applications over HTTPS, then you must configure SSL Inspection from the **ADVANCED > SSL Inspection** page and set up SSL certificates. See [How to Configure SSL Inspection 7.x](#).

To configure Web Application Monitoring, you'll want to first set up your block/accept policies for social media. Here's the process for the example mentioned above:

1. From the **BLOCK/ACCEPT > Web App Control** page, in the **Application Navigator**, make sure that *Social Media* is checked. In the **Allowed Applications** list box, hold the CTRL key and click *Facebook games*, *Facebook share* and/or any other Facebook applications you want to block. Click **Block**. Those applications will move to the **Blocked Applications** list box.

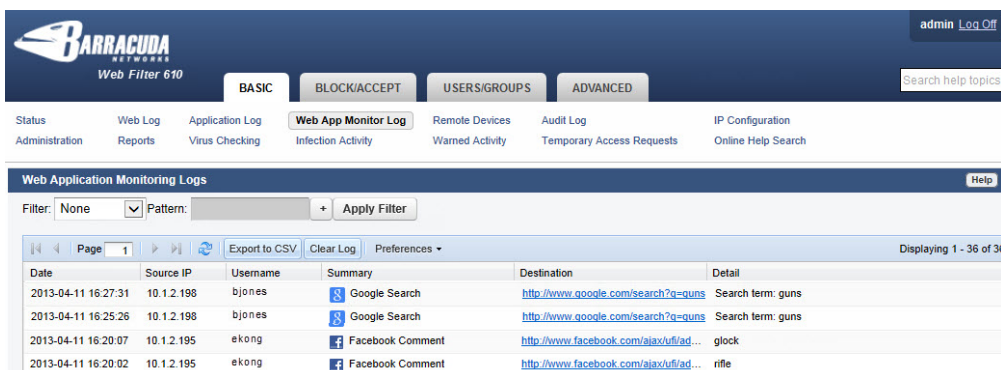


2. Save your changes. In this example, you have left *Comment* and *status update* and other Facebook apps in the **Allowed Applications** list, moving the applications you want to block, such as shares and games to the **Blocked Applications** list.
3. From the **BLOCK/ACCEPT > Web App Monitor** page, enable the application actions whose content you want to archive. In this example, you would enable Facebook Comments and Status Update. Once you enable any actions on the page, the Barracuda Web Filter will capture the content from each action, package it as an SMTP message and email it to the **Web App Monitor Email Address** you specify on the **BASIC > Administration** page.

Web App Monitor Log

The **BASIC > Web App Monitor Log** lists all chat, email, user registrations and other social media interaction traffic it processes per settings you configure on the **BLOCK/ACCEPT Web App Monitor** page. Fields logged are:

- **Date** - Date and time of the request.
- **Source IP** - IP address of the client that originated the request.
- **Username** - The name of the user that sent the request.
- **Summary** - The action represented in the request. For example, *Facebook Comment*.
- **Destination** - URL visited in the request.
- **Details** - Detailed information about the actions: search engine keywords, word from a *Facebook Comment*, etc.



Using SSL Inspection With the Barracuda Web Filter

SSL Inspection applies to the Barracuda Web Filter 610 and higher, running firmware version 6.0 and higher in Forward Proxy deployments. SSL Inspection with inline and WCCP deployments is available on some models running version 7.0 and higher.

Related Articles

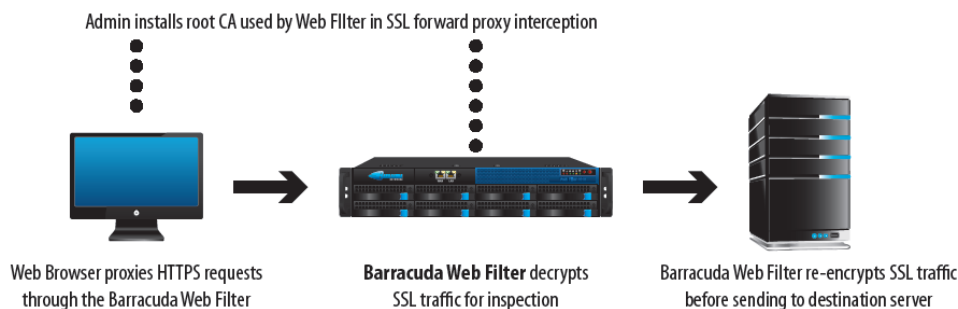
- [How to Configure SSL Inspection 6.x \(Barracuda Web Filter\)](#)
- [How to Configure SSL Inspection 7.x \(Barracuda Web Filter\)](#)
- [Using SSL Inspection with the Barracuda Web Security Service](#)

How SSL Inspection Works

With SSL Inspection, the content of a URL over HTTPS can be scanned. This allows the Barracuda Web Filter to apply policies and detect malware and viruses at the URL level.

The Barracuda Web Filter acts as a secure intermediary between user HTTPS web requests and the destination web server (i.e. Facebook.com, YouTube.com, yourdomain.com, etc.). HTTPS content in user web requests is decrypted and scanned by the Barracuda Web Filter, which then detects malware and enforces web policies configured on the **BLOCK/ACCEPT** pages. After processing, this HTTPS traffic will be re-encrypted on the fly by the Barracuda Web Filter and routed to the destination web server as shown in Figure 1.

Figure 1: SSL Inspection



To use this feature, the administrator installs a root certificate from the Barracuda Web Filter. The Barracuda Web Filter can then intercept and inspect the HTTPS connections by presenting the client a CA derived from this root CA. If you have a high availability deployment, you must install the same root certificate on each Barracuda Web Filter.

Popular Use Cases of SSL Inspection

Social media sites like Facebook and YouTube are now typically accessed over HTTPS, the encryption protocol used to protect online banking sessions and user logins for services of all kinds on the web.

- [Suspicious Keyword Tracking](#) – (Version 7.0 and higher) Monitor social messaging over HTTP/HTTPS in real time, with keyword alert emails to teachers or administrators to trigger immediate responses to emerging cases of bullying, harassment, or loss of confidential data. This feature only requires the use of SSL Inspection if traffic is over HTTPS (which is typical for Facebook, Google Apps, etc.) and is available on the Barracuda Web Filter 610 and higher. Database of keywords is embedded in the Barracuda Web Filter, is frequently updated, and can be customized. See the **BLOCK/ACCEPT > Web App Monitor** page to configure.
- [Google Apps Control Over HTTPS](#) – Granular regulation of Google Apps tools over HTTPS; for example, allow business Gmail account access, but block personal Gmail account access.
- [Facebook Control Over HTTPS](#) – Regulation and archiving of Facebook application interactions (chat, posting, games, etc.)

For configuration steps, see [How to Configure SSL Inspection](#).



If you enable SSL Inspection, *only* the domains (maximum of 5) and/or URL categories that you specify on the **ADVANCED > SSL Inspection** page will be filtered at the URL level.

How to Configure SSL Inspection 7.x

SSL Inspection applies to the Barracuda Web Filter 610 and higher, running firmware version up to 6.x (see [How to Configure SSL Inspection 6.x](#)) and version 7.0 and higher (as described in this article). **Note that if you enable SSL Inspection, only domains and/or URL categories that you specify on the ADVANCED > SSL Inspection page will be inspected and filtered at the URL level.**

For background information about this feature, see [Using SSL Inspection With the Barracuda Web Filter](#). If you are using Google Chrome browser, after reading this article, see [How to Configure SSL Inspection for Google Chrome Browser](#).

Enable SSL Inspection

1. On the **ADVANCED > SSL Inspection** page, set **SSL Inspection Method** to one of the following:
 - *Transparent* – Available on some models. This inspection method is more resource intensive than *Proxy* inspection and may have significant impact on system performance. This method works with inline deployments.



CAUTION: This is a resource intensive feature, and *Transparent* inspection can, under certain configurations, result in a large impact on performance. Note that you cannot inspect categories with this method.

- *Proxy* – Available for the Barracuda Web Filter 610 and higher. This method works with Forward Proxy deployments only and is less resource intensive than the *Transparent* inspection method. Configure all client web browsers with the IP address of the Barracuda Web Filter as their forward proxy server. If you are using the Chrome browser, also see [How to Configure SSL Inspection for Google Chrome Browser](#).
 - *No SSL Inspection* – Disable SSL Inspection of HTTPS traffic. This means that the Barracuda Web Filter will not decrypt HTTPS traffic at the URL level. You will be able to block/allow HTTPS domains, but you will not be able to archive actions users take on social media sites such as, for example, Facebook chat content, logins on Twitter or Yahoo!, etc. as defined on the **BLOCK/ACC EPT > Web App Monitor** page.
2. Select **Create** to generate and download an SSL certificate to install in each client browser. Alternatively you can use an enterprise certificate authority (CA) and **upload** the certificate, however, creating the certificate on the Barracuda Web Filter is recommended because the private key never leaves the device. If you have a high availability deployment, you must install the same root certificate on each Barracuda Web Filter. See instructions in the online help on the **ADVANCED > SSL Inspection** page to create and install the certificate(s). **Note:** If you use the **Upload** option, make sure to upload both the private and public key files. Formats supported include .pem, der, pkcs12, pkcs7, and pfx. The .jks (java key store) format is not supported.



Immediately after you enable HTTPS Filtering, any client machines that had previously established an HTTPS session are communicating with an IP address and will not be blocked. In this situation, the HTTPS website IP address remains in the DNS client resolver cache (as well as in the DNS table on the core router or domain controller) until the DNS request time-to-live (TTL) expires. This can take up to a day or two, depending upon how the HTTPS sites configure TTL.

Specify Domains and URL Categories for SSL Inspection



Note that enabling SSL Inspection increases the load on system resources, so you should only specify the domains and/or categories of URLs to inspect that are not trusted with HTTPS traffic.

On the **ADVANCED > SSL Inspection** page you must specify one or both of the following settings for applying SSL Inspection.

- **Domains to Be Inspected** – Enter up to 5 domain names that you want to be inspected and filtered at the URL level.
- **URL Categories** – Using the **Add** and **Remove** buttons, from the **Categories List**, you can add or remove URL categories to/from the list of categories that you want to be inspected. You must use the *Proxy* inspection method if you want to inspect categories.

Any domains or URL categories that are NOT specified on the page will NOT be subject to SSL Inspection.

How to Configure SSL Inspection for Google Chrome Browser

Because the Google Chrome browser adheres to stringent security checks for client protection, the user gets certificate errors when SSL inspection is enabled on the Barracuda Web Filter. These errors cause browser activity to stop without an opportunity to bypass or override the

error, and the session is disconnected.

To avoid these certificate errors, you can download a root CA (SSL certificate) from the Barracuda Web Filter and install it on each Chrome client browser. To do so, follow these steps:

1. Log into the Barracuda Web Filter as **admin**.
2. Go to the **ADVANCED > SSL Inspection** page.
3. Select your **SSL Inspection Method** at the top of the page.
4. Scroll down to the **Certificate Creation** section of the page and select **Create Certificate**.
5. In the **Certificate Generation** section below, fill in your organization information, following the instructions on the page, or in the Help file, and then click **Create Certificate**.
6. In the **Available Certificates** section below, click **Download** for the **Root Certificate for Browsers**.
7. If Chrome presents a notification popup, click **Keep**.
8. Go to your Downloads folder, or wherever you saved the `.der` file, right click on it, and select **Install**.
9. Follow prompts on certificate install wizard.
10. Successful installation is indicated by an **Import Successful** message.

How to Configure SSL Inspection 6.x

SSL Inspection applies to the Barracuda Web Filter 610 and higher. This article applies to the Barracuda Web Filter running up to firmware version 6.0, and only in Forward Proxy deployments. For firmware version 7.0 and higher, see [How to Configure SSL Inspection 7.x](#). **Note that if you enable SSL Inspection, only domains and/or URL categories you specify on the ADVANCED > SSL Inspection page will be inspected and filtered at the URL level.**

Related Articles

- [Using SSL Inspection With the Barracuda Web Filter](#)

Enable SSL Inspection

1. On the **ADVANCED > SSL Inspection** page:
 - a. Set **Enable SSL Inspection** to Yes.
 - b. Select **Create** to generate and download an SSL certificate to install in each client browser. Alternatively you can use an enterprise certificate authority (CA) and **upload** the certificate, however, creating the certificate on the Barracuda Web Filter is recommended because the private key never leaves the device. If you have a high availability deployment, you must install the same root certificate on each Barracuda Web Filter. See instructions in the online help to create and install the certificate(s). **Note:** If you use the **Upload** option, make sure to upload both the private and public key files. Formats supported include `.pem`, `der`, `pkcs12`, `pkcs7`, and `pxf`. The `.jks` (java key store) format is not supported.
2. If you haven't already done so, configure all client web browsers with the IP address of the Barracuda Web Filter as their forward proxy server, on port 3128.



Immediately after you enable HTTPS Filtering, any client machines that had previously established an HTTPS session are communicating with an IP address and will not be blocked. In this situation, the HTTPS website IP address remains in the DNS client resolver cache (as well as in the DNS table on the core router or domain controller) until the DNS request time-to-live (TTL) expires. This can take up to a day or two, depending upon how the HTTPS sites configure TTL.

Specify Domains and URL Categories for SSL Inspection



Note that enabling SSL Inspection increases the load on system resources, so you should only specify the domains and/or categories of URLs to inspect that are not trusted with HTTPS traffic.

On the **ADVANCED > SSL Inspection** page you must specify one or both of the following settings for applying SSL Inspection.

- **Domains to Be Inspected** – Enter up to 5 domain names that you want to be inspected and filtered at the URL level.
- **URL Categories** – Using the **Add** and **Remove** buttons, from the **Categories List**, you can add or remove URL categories to/from the list of categories that you want to be inspected.

Any domains or URL categories that are NOT specified on the page will NOT be subject to SSL Inspection.

Google Apps Control Over HTTPS

SSL Inspection of HTTPS traffic for this use case is available:

- With either WCCP or Forward Proxy deployments on the Barracuda Web Filter 610 and higher, running version 6.x and higher.
- With either inline, WCCP, or Forward Proxy deployments on the Barracuda Web Filter 910 and 1010 running version 7.0 and higher.

The Barracuda Web Filter can be configured for scanning of HTTPS traffic at the URL level when the **SSL Inspection** feature is enabled. This means that the administrator has granular control over what applications are blocked or allowed on websites like Google.com. The administrator can control Google Apps traffic, for example, by specifying domain/sub-domain patterns associated with Google Apps to be inspected over HTTPS. With SSL Inspection, the Barracuda Web Filter can apply policies granularly to HTTPS traffic at the URL level as well as detect malware and viruses. For more information about this feature, see [Using SSL Inspection With the Barracuda Web Filter](#). This article provides several use cases as examples.

In this article:

- [Enable and Configure SSL Inspection](#)
- [Use Case #1 – Allow Most Google Apps, While Blocking Google Wallet and Google Notebook for Students](#)
- [Use Case #2 – Blocking Personal Gmail](#)
- [Use Case #3 – Blocking Personal Gmail, While Allowing Business Gmail Access](#)

Related Articles

- [Facebook control over HTTPS](#)
- [Using SSL Inspection With the Barracuda Web Filter](#)
- [How to Configure SSL Inspection 7.x](#)
- [How to Configure SSL Inspection 6.x](#)

Enable and Configure SSL Inspection

This is the first step for performing granular control of HTTPS applications with the Barracuda Web Filter. The examples in this article use SSL inspection of the domain `Google.com`.

1. Log into the Barracuda Web Filter web interface as an administrator.
2. On the **ADVANCED > SSL Inspection** page, set **Enable SSL Inspection** to **Yes**.
3. In the Inspected Domains field, enter `Google.com` and click **Add**.
4. Install an SSL certificate. There are two options:
 - a. Select **Upload** to upload a *trusted* certificate signed by a CA or from your organization's CA server. Once you install the trusted certificate on the Barracuda Web Filter, your users can browse HTTPS sites without any warnings when **SSL Inspection** is enabled. If you have a high availability deployment, you will need to install the same root certificate on each Barracuda Web Filter. **Note:** If you use this option, make sure to upload both the private and public key files. Formats supported include .pem, der, pkcs12, pkcs7, pfx, but not .jks (java key store).
 - b. Select **Create** to generate your own SSL certificate and download it to install in or push out to each client browser. If you don't, users will see a warning each time they browse an HTTPS site when **SSL Inspection** is enabled. On the other hand, if you

create the certificate on the Barracuda Web Filter, the private key is more secure as it never leaves the device. If you have a high availability deployment, you will need to install the same root certificate on each Barracuda Web Filter. Follow instructions in the online help to create and install the certificate(s).

Use Case #1 – Allow Most Google Apps, While Blocking Google Wallet and Google Notebook for Students

This scenario allows access to Google Gmail and most other Google Apps, which tend to be accessed via HTTPS. Exceptions to this policy are blocking Google Notebook and Google Wallet over HTTPS. Since no time frame is specified on the **BLOCK/ACCEPT > Exceptions** page in this example, these policies would be enforced by the Barracuda Web Filter 24/7 if configured as shown here.

Step 1. Configure SSL Inspection as described above under [Enable and Configure SSL Inspection](#).

Step 2. Create the *Block* policy for Google Notebook.

1. Set up users and groups as needed as well as authentication mechanisms. See [Managing Users and Groups](#) and [How to Choose Your Authentication Mechanisms](#).
2. On the **BLOCK/ACCEPT > Exceptions** page, in the **Add Exceptions** section, select the **Block Action**. See **Figure 1**.
3. Select the type of users you want to block (*Authenticated*, *Local Group*, etc.) in the **Applies To** field. In this case we've chosen the *Students* group.
4. Select *Web App Control* as the **Exception Type**.

Figure 1: Blocking the *Students* group of users from using Google Notebook

The screenshot shows the Barracuda Web Filter 310 configuration interface. The 'BLOCK/ACCEPT' tab is active, and the 'Exceptions' page is displayed. The configuration is as follows:

- Action:** Block
- Applies To:** Local Group (Students selected)
- Exception Type:** Web App Control (Google Notebook selected)
- Web App Name:** - Google Notebook
- Create Policy Alert:** No
- Alert Threshold (requests):** (empty)
- Time Frame:** 00:00 - 24:00
- Days of Week:** All days (Su, M, T, W, Th, F, S) are checked.
- Time Quota (min):** Daily
- Bandwidth Quota (kB):** Daily
- HTTP Methods:** (empty)
- Protocol:** HTTPS
- Message:** Block Google Notebook for students

5. From the **Web App Name** drop-down, select *Google Notebook*.
6. From the **Protocol** drop-down, select *HTTPS*.
7. Click **Add**.

Step 3. Create the *Block* policy for Google Wallet.

1. On the **BLOCK/ACCEPT > Exceptions** page, in the **Add Exceptions** section, select the **Block Action**. See **Figure 2**.
2. Select the type of users you want to block (*Authenticated*, *Local Group*, etc.) in the **Applies To** field. In this case we've chosen the *Students* group.
3. Select *URL Patterns* as the **Exception Type**.

Figure 2: Blocking Google Wallet for the *Students* group

4. In the **URL Pattern** text box, enter `wallet.google.com`
5. From the **Protocol** drop-down, select *HTTPS*.
6. Click **Add**.

Use Case #2 – Blocking Personal Gmail

Suppose you want block access to personal Google Gmail for users in your organization during working hours Monday through Friday, but allow it before 8am and after 5pm and all day on weekends. Using the URL pattern for non-business Google Gmail accounts (`https://mail.google.com/mail`), you will create a policy on the **BLOCK/ACCEPT > Exceptions** page.

Step 1. Configure SSL Inspection as described above under [Enable and Configure SSL Inspection](#).

Step 2. Create the policy.

1. On the **BLOCK/ACCEPT > Exceptions** page, in the **Add Exceptions** section, select the *Block Action*. See **Figure 3**.
2. Select the type of users you want to block (*Authenticated*, *Local Group*, etc.) in the **Applies To** field. In this case we've chosen *Authenticated* users.
3. Select *URL Pattern* as the **Exception Type**.
4. Enter `https://mail.google.com/mail` as the **URL pattern**.
5. Set the **Time Frame** from 8:00 - 17:00 Mon. - Fri. , or whatever constitutes 'working hours'.

Figure 3: Creating a *Block* policy for personal Gmail during working hours

6. Select the **Protocol** as *HTTPS*. Enter a message if you like to describe what the policy is about.
7. Configure policy alerts as needed. With **Enable Policy Alerts** set to *On*, the Barracuda Web Filter will send an email summarizing

content policy violations to the email address(es) entered in the **Policy Alerts Email Address** field.

8. Click **Add**.

Use Case #3 – Blocking Personal Gmail, While Allowing Business Gmail Access

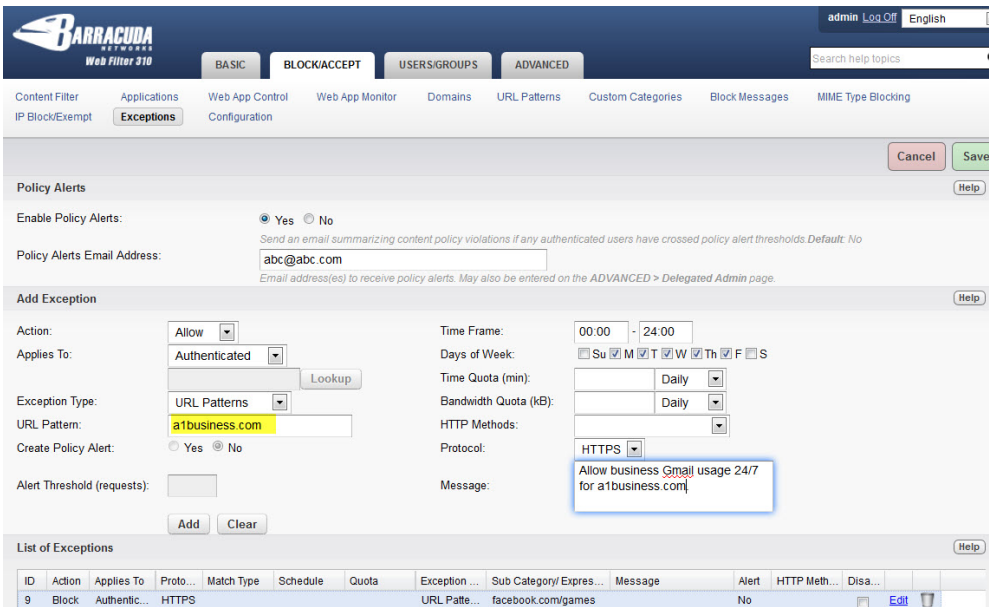
Step 1. Configure SSL Inspection as described above under [Enable and Configure SSL Inspection](#).

Step 2. Follow the instructions above to create a *Block* policy for personal gmail accounts. You don't need to fill in the **Time Frame** fields unless you want to only apply the *Block* during certain hours.

Step 3. Create the *Allow* policy for business Gmail use.

1. On the **BLOCK/ACCEPT > Exceptions** page, in the **Add Exceptions** section, select the *Allow* Action. See **Figure 4**.
2. Select the type of users you want to allow (*Authenticated*, *Local Group*, etc.) in the **Applies To** field. In this case we've chosen *Authenticated* users.

Figure 4: Creating an *Allow* policy for business Gmail access 24/7



3. Select *URL Pattern* as the **Exception Type**.
4. Enter your business email domain name (ex: a1business.com) as the **URL pattern**.
5. Leave the **Time Frame** setting as 00:00 - 24:00 to allow business Gmail access 24/7.
6. Click **Add**.

Facebook Control Over HTTPS

The Barracuda Web Filter can be configured for scanning of HTTPS traffic at the URL level when the **SSL Inspection** feature is enabled. This means that the administrator has granular control over what applications are blocked or allowed on websites like Facebook.com. The administrator can control Facebook traffic, for example, by specifying domain/sub-domain patterns associated with Facebook applications to be inspected over HTTPS. With SSL Inspection, the Barracuda Web Filter can apply policies granularly to HTTPs traffic at the URL level as well as detect malware and

viruses. For more information about this feature, see [Using SSL Inspection With the Barracuda Web Filter](#). This article provides several use cases as examples.

Related Articles
<ul style="list-style-type: none">• Exception Policies 7.x• Exception Policies 6.x• Google Apps Control Over HTTPS• Using SSL Inspection With the Barracuda Web Filter• How to Configure SSL Inspection 7.x• How to Configure SSL Inspection 6.x

SSL Inspection of HTTPS traffic for this use case is available:

- With either WCCP or Forward Proxy deployments on the Barracuda Web Filter 610 and higher, running version 6.x and higher.
- With either inline, WCCP, or Forward Proxy deployments on the Barracuda Web Filter 910 and 1010 running version 7.0 and higher.

Use Case #1 – Blocking Facebook Apps

Suppose you want allow access to Facebook.com for students, but want to ONLY allow Facebook *Applications (Apps)* during school lunch time. Using the URL pattern for Facebook *Apps* (<https://apps.facebook.com>, <https://www.facebook.com/appcenter/>), you would first configure **SSL Inspection**, then create a policy on the **BLOCK/ACCEPT > Exceptions** page.

Step 1. Enable and configure SSL Inspection:

1. Log into the Barracuda Web Filter web interface as an administrator.
2. On the **ADVANCED > SSL Inspection** page, set **Enable SSL Inspection** to Yes.
3. In the Inspected Domains field, enter Facebook.com and click Add.
4. Install an SSL certificate. There are two options:
 - a. Select **Upload** to upload a *trusted* certificate signed by a CA or from your organization's CA server. Once you install the trusted certificate on the Barracuda Web Filter, your users can browse HTTPS sites without any warnings when **SSL Inspection** is enabled. If you have a high availability deployment, you will need to install the same root certificate on each Barracuda Web Filter. **Note:** If you use this option, make sure to upload both the private and public key files. Formats supported include .pem, der, pkcs12, pkcs7, pfx, but not .jks (java key store).
 - b. Select **Create** to generate your own SSL certificate and download it to install in or push out to each client browser. If you don't, users will see a warning each time they browse an HTTPS site when **SSL Inspection** is enabled. On the other hand, if you create the certificate on the Barracuda Web Filter, the private key is more secure as it never leaves the device. If you have a high availability deployment, you will need to install the same root certificate on each Barracuda Web Filter. Follow instructions in the online help to create and install the certificate(s).

Step 2. Create the policy:

1. On the **BLOCK/ACCEPT > Exceptions** page, in the **Add Exceptions** section, select the *Allow Action*. See **Figure 1** below.
2. Select the type of users you want to allow (*Authenticated, Local Group, etc.*) in the **Applies To** field. In this case we've chosen *Authenticated* users. If your set of authenticated users includes teachers, you might want to create a group for students using the **USERS/ GROUPS** pages and then select the student group for **Applies To**.
3. Select *URL Pattern* as the **Exception Type**.
4. Enter <https://apps.facebook.com>, <https://www.facebook.com/appcenter/> as the **URL pattern** (make sure to include a comma between URLs).
5. Set the **Time Frame** from 12:00 - 13:00 Mon. - Fri. , or whatever constitutes 'lunch hour'.

Figure 1: Creating a limited Allow policy for Facebook applications during school lunch hours

The screenshot shows the Barracuda Web Filter administration interface. At the top, there's a navigation bar with tabs for 'BASIC', 'BLOCK/ACCEPT', 'USERS/GROUPS', and 'ADVANCED'. The 'ADVANCED' tab is selected, and the 'Exceptions' sub-tab is active. The main content area is divided into two sections: 'Policy Alerts' and 'Add Exception'. In the 'Policy Alerts' section, 'Enable Policy Alerts' is set to 'Yes', and the 'Policy Alerts Email Address' is 'abc@abc.com'. The 'Add Exception' section is where a new policy is being configured. The 'Action' is set to 'Allow', 'Applies To' is 'Authenticated', and 'Exception Type' is 'URL Patterns'. The 'URL Pattern' field contains 'https://apps.facebook.com, https://a...'. The 'Create Policy Alert' option is set to 'No'. The 'Alert Threshold (requests)' is set to 0. The 'Time Frame' is '12:00 - 13:00', and 'Days of Week' are 'M', 'T', 'W', 'T', 'F'. The 'Time Quota' and 'Bandwidth Quota' are both set to 'Daily'. The 'Protocol' is 'HTTPS', and the 'Message' field contains the text: 'ONLY allow access to ALL Facebook Apps during lunch hour, Mon-Fri.'.

6. Select the **Protocol** as *HTTPS*. Enter a message if you like to describe what the policy is about.
7. Configure policy alerts as needed. With **Enable Policy Alerts** set to *On*, the Barracuda Web Filter will send an email summarizing content policy violations to the email address(es) entered in the **Policy Alerts Email Address** field.
8. Click **Add**. You have now created your policy.

Use Case #2 – Blocking Facebook Chat for students

Suppose you want allow access to all Facebook activities *except* chat for students. Using the URL pattern for Facebook Messages (<https://www.facebook.com/messages>), you would first configure SSL Inspection, then create a policy on the **BLOCK/ACCEPT > Exceptions** page.

Step 1. Enable and configure SSL Inspection (if not already done):

1. Log into the Barracuda Web Filter web interface as an administrator.
2. On the **ADVANCED > SSL Inspection** page, set **Enable SSL Inspection** to *Yes*.
3. In the **Inspected Domains** field, enter Facebook.com and click **Add**.
4. Select **Create** to generate and download an SSL certificate to install in each client browser. Alternatively you can use an enterprise CA (certificate authority) and **upload** the certificate, but creating the certificate on the Barracuda Web Filter is recommended such that the private key never leaves the device. If you have a high availability deployment, you will need to install the same root certificate on each Barracuda Web Filter. Follow instructions in the online help to create and install the certificate(s). **Note:** If you use the **Upload** option, make sure to upload both the private and public key files. Formats supported include .pem, der, pkcs12, pkcs7, pfx, but not .jks (java key store).

Step 2. Create the policy:

1. On the **BLOCK/ACCEPT > Exceptions** page, in the **Add Exceptions** section, select the *Block Action*. See **Figure 2** below. Select the type of users you want to allow (*Authenticated*, *Local Group*, etc.) in the **Applies To** field. In this example we've created a group called *Students* from the **USERS/ GROUPS > Local Groups** page, and here, we have selected that group for **Applies To**.
2. Select *URL Pattern* as the **Exception Type**.
3. Enter `https://www.facebook.com/messages` as the **URL pattern**.
4. There is no need to set a time frame unless you want to allow access to Facebook chat *OUTSIDE* the hours you're blocking.

Figure 2: Creating a *Block* policy for Facebook chat

The screenshot shows the Barracuda Web Filter Administration console. The top navigation bar includes 'admin', 'Log Off', and 'English'. The main menu has tabs for 'BASIC', 'BLOCK/ACCEPT', 'USERS/GROUPS', and 'ADVANCED'. The 'ADVANCED' tab is selected, and the 'Exceptions' sub-tab is active. The 'Policy Alerts' section is visible, with 'Enable Policy Alerts' set to 'Yes'. Below this is the 'Add Exception' section, which is currently empty. The form fields for 'Add Exception' are as follows:

- Action: Block
- Applies To: Local Group (Students)
- Exception Type: URL Patterns
- URL Pattern: https://www.facebook.com/messages
- Create Policy Alert: No
- Alert Threshold (requests):
- Time Frame: 00:00 - 24:00
- Days of Week: Su, M, Tu, W, Th, F, S (all checked)
- Time Quota (min): Daily
- Bandwidth Quota (KB): Daily
- HTTP Methods:
- Protocol: HTTPS
- Message: Block students from using Facebook chat (messaging). No Policy Alerts are necessary.

5. Select the **Protocol** as *HTTPS*. Enter a message if you like to describe what the policy is about.
6. Configure policy alerts as needed. In this example, the **Message** field explains that **Policy Alerts** were purposely not enabled.
7. Click **Add**. You have now created your policy.

Managing Users and Groups

In this Section

- [Creating Users and Groups](#)
- [Integrating the Barracuda Web Filter With a User Authentication Service](#)
- [How to Choose Your Authentication Mechanisms](#)
- [Role-based Administration 6.x](#)
- [Role-based Administration 7.x](#)

Creating Users and Groups

In this article:

- [Local Users](#)
- [Domain Users](#)
- [Creating Local User Accounts](#)
- [Viewing and Managing Accounts](#)
- [Creating Local Groups](#)
- [Creating IP Address Groups](#)
- [Assigning Policy to LDAP Organizational Units](#)

Related Articles

- [Integrating the Barracuda Web Filter With a User Authentication Service](#)
- [How to Configure Kerberos Authentication](#)

The Barracuda Web Filter distinguishes between two basic classes of the users who access websites and web applications from client machines that it has been configured to protect: *local users* and *domain users*.

You can apply filtering and blocking policies as well as exception rules to both classes of users, and, with several user authentication methods to choose from in the Barracuda Web Filter, you can apply such rules and policies to specific users, groups, LDAP organizational units (OUs) or machines. Authentication options are addressed below.

You can also view the following information about both local users and domain users:

- Account details
- Traffic Log
- Applications Log
- Warned Activity
- Reports output

Local users are shown as anonymous until they authenticate in the Barracuda Web Filter system by providing login information in order to proceed to a blocked or warned web page or application.

Domain users are shown as anonymous until they become authenticated in the Barracuda Web Filter system by providing credentials to their respective authentication service that has been integrated with the Barracuda Web Filter. Authenticated domain users are shown by username, client IP address, and group membership.

In some cases, you may need to create local accounts as well as enable your Barracuda Web Filter to look up domain accounts. For example, if your regular employees have LDAP accounts but contract employees do not, then you might need to create local accounts for the contractor employees.

Local Users

You can define Local users by listing their existing usernames in the **USERS/GROUPS > New Users** page. The Barracuda Web Filter authenticates these users from its local database. To apply Web filtering policies (and exception rules to your filtering policies) to multiple local users, you can assign local users to local groups that you define in the **USERS/GROUPS > Local Groups** page.

You can also create IP subnet-based groups - i.e. groups of users who access websites and web applications from client machines within specific ranges of IP addresses. Define IP subnet-based groups of local users in the **USERS/GROUPS > IP Groups** page.

Domain Users

The Barracuda Web Filter can authenticate domain users using your existing authentication service. You can integrate the Barracuda Web Filter with any of the following types authentication servers:

- LDAP
- NTLM
- Kerberos

Doing so enables you to apply web filtering policies and policy exceptions to your domain users without having to re-create local accounts for these users.

Creating Local User Accounts

Use the **USERS/GROUPS > New Users** page to create a local database of users that the Barracuda Web Filter will authenticate. If you want users to be authenticated using your existing user authentication service instead, go to the **USERS/GROUPS > Authentication** page and enter the information for your authentication server.

Local user accounts cannot be used to log into the web interface. You can only use the default admin account to log into the web interface.

If you want a new user account to be a member of a group, be sure the group already exists on the **USERS/GROUPS > Local Groups** page.

Viewing and Managing Accounts

The **USERS/GROUPS > Account View** page displays all the user accounts that have either been created locally on your Barracuda Web Filter or which reside in your LDAP database. This page lets you view details about each account and make the following changes to any locally created accounts:


- Edit a local account by assigning it to a group or enabling/disabling the account
- Change the password of a local account
- Delete a local account

To quickly locate a specific account, use the filter feature at the top of the page to search for specific patterns in the account details.

Creating Local Groups

Use the **USERS/GROUPS > Local Groups** page to create groups for your local users. The most common reason to create a group is so you can apply an exception policy to multiple users at the same time instead of to individual users. For example, you can create a Finance group and create a policy that allows members of that group to browse financial sites, while blocking those sites from other users on the network.

To create a group, enter the group name in the provided field and click **Add**. To assign an existing user to this group, go to the **USERS/GROUPS > Accounts View** page and click **Edit** next to the account that you want to join the group. A user can belong to multiple groups.

 When you navigate to the **USERS/GROUPS > Local Groups** page, the Barracuda Web Filter will only display groups for which you have created an exception. For this reason, it is possible that you won't always see all groups associated with users. To refresh the Groups list, click the **Sync Now** button in the **Group Membership Synchronization** section of the **USERS/GROUPS > Authentication** page.

Note that the **Sync Now** button will only be displayed on that page if you have configured an LDAP, NTLM or Kerberos server..

Creating IP Address Groups

The **USERS/GROUPS > IP Subnets/Groups** page lets you create a group for a single or range of IP addresses. The most common reasons to create an IP group is to apply an exception policy to:

- Multiple users on the same subnet. In this case, enter the subnet mask for the subnet in the provided field.
- A static IP address. In this case, enter the static IP address in the provided field.

After you enter the IP address or subnet mask and click Add, you can assign an exception policy to the IP group on the **BLOCK/ACCEPT > Exceptions** page.

Assigning Policy to LDAP Organizational Units

If you are using an Active Directory or other LDAP server, you can create policy exceptions for individual members of an organizational unit or for the entire unit. The Barracuda Web Filter can lookup the organizational units defined on your server after you have configured the server(s) on the **USERS/GROUPS > Authentication** page. See the **Applies To** field on that page in the **Add Exception** section. You can select the server, then click the **Lookup** button to view OUs in your server.

Integrating the Barracuda Web Filter With a User Authentication Service

In this article:

- [Granular Policies By Users, Groups or Machines](#)
- [Applying Web Access Policy by Groups](#)
- [Terminal Environments and Authentication](#)
- [LDAP Authentication](#)

Related Articles

- [How to Configure Kerberos Authentication](#)
- [Creating Users and Groups](#)

Granular Policies By Users, Groups or Machines

By integrating the Barracuda Web Filter with your existing authentication server, you can configure usage policies at several levels of granularity; policies can apply to the whole organization or to specific users, machines, or groups. Using LDAP, NTLM, or [Kerberos](#) authentication or a combination of them, you can apply policies and generate reports directly on users, LDAP organizational units (defined on your LDAP server) or groups you define without the need to create local user accounts on the Barracuda Web Filter.

Applying Web Access Policy by Groups

Typically, computer users in a network are grouped along organizational, departmental, physical or functional boundaries. As the administrator, you can create secure accounts for network users and also group them as appropriate. Users then supply their login credentials from their workstations to activate their network privileges. This allows the administrator to control Internet access privileges separately for each user or group of users. For example, a school can apply a more restrictive browsing policy for students than for teachers and staff, or an organization can allow access to job sites only to the Human Resources department (which you may have defined as an organizational unit on your LDAP server).

If you do not integrate with your LDAP, NTLM or Kerberos authentication server, you can apply filtering policy exceptions only to local users and groups that you create in the **USERS/GROUPS** tab.

Terminal Environments and Authentication

Kerberos and NTLM authentication schemes work well with Citrix terminal environments and Windows terminal services environments. The Barracuda Web Filter can also support various user groups using different authentication schemes to provide different types of user access and policy control. For example, if your organization has a group of Windows desktop users who authenticate against an LDAP server and another group using a Citrix terminal environment or Windows terminal services environment, you can configure both groups with one Barracuda Web Filter.

Using **Hybrid Mode**, Windows desktop users can authenticate via your LDAP server while the terminal users can authenticate via NTLM or Kerberos in a forward proxy configuration. In the latter setup, each user's browser will forward their credentials to the Barracuda Web Filter.

To use Hybrid Mode, simply add your LDAP and NTLM or Kerberos services as described below and detailed in the online help in the web interface.

LDAP Authentication

LDAP users are authenticated when credentials are provided in order to proceed to a blocked or warned web page or application. NTLM and Kerberos users are authenticated by single sign-on access against the NTLM or Kerberos authentication service, so they are transparently authenticated in the Barracuda Web Filter using their Microsoft Windows credentials. Authenticated domain users are known by username, client IP address, and group membership:

- Usernames and client IP addresses of authenticated LDAP domain users are visible in the **USERS/GROUPS > Account View** page, the **Web Log** page, the **Application Log** page and in reporting output.
- Group membership information about authenticated domain users is available by opening the Lookup facility (accessed by clicking Lookup button in the **BLOCK/ACCEPT > Exceptions** page) and using the **Active Directory User/Group** section of that window.

Note: Domain users that are *unauthenticated* in the Barracuda Web Filter appear as anonymous users.

How to Choose Your Authentication Mechanisms

In this section:

- [How to Configure Kerberos Authentication](#)
- [How to Enable LDAP Domain User Authentication](#)
- [How to Enable NTLM Domain User Authentication](#)

Below are some use case scenarios to help you decide which authentication scheme(s) to configure on your Barracuda Web Filter. Each example addresses a particular type of environment:

Related Articles
<ul style="list-style-type: none">• How to Configure Kerberos Authentication• How to Enable NTLM Domain User Authentication

Example 1: Fat clients (standard desktops) using Active Directory

Step 1: Configure **LDAP authentication**, as described in [How to Enable LDAP Domain User Authentication](#), on the Barracuda Web Filter and synchronize group membership information with your domain controllers (Active Directory servers). This provides a manual way for users to authenticate on the Barracuda Web Filter so you can track user browsing activity.

Step 2: If you want to use single sign-on, install and configure the DC Agent on every domain controller as described in [How to Get and Configure the Barracuda DC Agent](#). For an overview, see [About the Barracuda DC Agent](#).

Example 2: Using only Citrix or other terminal environments

Step 1: Configure NTLM or Kerberos so that the Barracuda Web Filter can join the domain. Reasons for choosing NTLM versus Kerberos are discussed below.

Step 2. Force users to use the Barracuda Web Filter as a proxy server that provides authentication and single sign-on. See [Forward Proxy Deployment of the Barracuda Web Filter](#) for details on proxy deployment.

Example 3: Mix of fat clients and Citrix or other terminal environments

Configure per examples 1 and 2. The articles in this section, linked above, further explain reasons and requirements for employing these various authentication schemes.

Exempting selected LDAP domain users from filtering

To exempt LDAP domain users from policy engine processing, on the **USERS/GROUPS > Authentication LDAP** tab, navigate to the **DC Agent Configuration** section where exempt user names can be entered. An example use case for this feature is to prevent traffic caused by script logic or other background users from appearing in the traffic log.

NTLM Versus Kerberos

Kerberos is an authentication protocol that provides mutual authentication; i.e. both the user and the server verify each other's identity. For this reason, Kerberos is considered a more secure authentication protocol than NTLM. Implementing Kerberos-based authentication within your network will allow the Barracuda Web Filter to associate outgoing web requests with Active Directory users, log user activity, and apply user-specific or group-specific policies to outgoing connections without requiring users to log into the Barracuda Web Filter.

Kerberos is useful when a Microsoft domain controller is running in native mode. It is a Forward Proxy authentication scheme and the Barracuda Web Filter need not verify each authentication request against a domain controller. See [How to Configure Kerberos Authentication](#) for more information about Kerberos.

If your network uses an NT LAN Manager (**NTLM**) authentication server, your NTLM domain users transparently become authenticated in the Barracuda Web Filter using their Microsoft Windows credentials. This single sign-on (SSO) method of access control is provided by transparent proxy authentication against the your NTLM server.

To enable transparent proxy authentication against your NTLM server, you must join the Barracuda Web Filter to the NTLM domain as an authorized host. The process of joining the domain also synchronizes NTLM group information from your domain controller to the Barracuda Web Filter. Configure NTLM authentication on the **USERS/GROUPS > Authentication** page **NTLM** tab. See [How to Enable NTLM Domain User Authentication](#) for more information about NTLM.

How to Configure Kerberos Authentication

This solution applies to all Barracuda Web Filters running firmware version 4.2 and higher. Windows 2000 and later platforms use Kerberos as the native authentication method.

Related Articles

- [Integrating the Barracuda Web Filter With a User Authentication Service](#)

When to use Kerberos Authentication

Use Kerberos with the Barracuda Web Filter in any of the following scenarios:

- **Clients are behind a NAT-enabled router** - Requests from users on client machines behind a NAT-enabled router would appear to the

Barracuda Web Filter to be sent from the same reusable NAT Router IP address.

- **Windows Terminal Services** — Requests from users using Windows Terminal Services to access remote data and applications on another client machine would appear to the Barracuda Web Filter to be sent from the Windows terminal IP address.
- **Citrix Presentation Services** — Requests from users accessing remote data and applications on a Citrix Presentation Server would appear to the Barracuda Web Filter to be sent from the Citrix Presentation Server.

Requirements for using a Kerberos authentication server

Before you integrate with a Kerberos authentication server, please verify the following requirements:

- The Barracuda Web Filter must be deployed as a forward proxy. For more information on deploying your Barracuda Web Filter as a forward proxy, please refer to [Forward Proxy Deployment of the Barracuda Web Filter](#).
- The only other authentication service you may configure, in addition to Kerberos, is LDAP. This is called **Hybrid Authentication Mode**.
- No Barracuda DC Agents may be in use on any of your domain controllers. Domain controllers must be running in native mode.
- Web browsers must support Kerberos (Internet Explorer version 7 or Firefox version 3) and must be configured to use the Barracuda Web Filter as an HTTP proxy.
- Client workstations and the Barracuda Web Filter must have properly configured DNS resolution mechanisms. DNS servers must be able to resolve IP addresses in both forward and reverse.
- All host machine clocks must be synchronized within 5 minutes of the Kerberos server clock.
- All users must have domain logon credentials, generally speaking; however, non-domain machines can use Kerberos authentication provided that Kerberos is configured correctly on those machines.

Implementing Kerberos

Follow these steps to create your Kerberos service on the Barracuda Web Filter:

1. Set your **Default Domain** and **Default Hostname** on the **BASIC > IP configuration** page. On your DNS server(s), add an entry (both forward and reverse mappings) for your Barracuda Web Filter.
2. On the **Kerberos** tab of the **USERS/GROUPS > Authentication** page, enter the **Realm**, or Windows administrative domain name.
3. On that page, in the **KDC** field, enter the fully qualified domain name (FQDN) of the Key Distribution Center server for the realm you specified. This is typically the FQDN of your domain controller.
4. Enter the **Username** and **Password** of an account that has administrative privileges on your Active Directory server.
5. Click the **Add** button to create the new Kerberos service. Once you do this, the service should appear as type **Kerberos** in the **Existing Authentication Services** table on the **USERS/GROUPS > Authentication** page on the **Kerberos** tab.
6. Ensure that the Barracuda Web Filter's FQDN (not the IP) and port 8080 are configured as an HTTP proxy on all users' browsers.

Note that implementing Kerberos Authentication will restrict some configuration options, as follows:

- **No login override of blocked pages:** When a policy on the Barracuda Web Filter blocks Internet access for a user, that user will not be offered login fields at the bottom of the block message page, even if **Allow Login Override of Blocked Pages** is enabled on the **BLOCK /ACCEPT > Configuration** page.
- **No logout option:** Users cannot log out when proceeding to a blocked page in order to surf anonymously. More precisely, when a policy on the Barracuda Web Filter blocks Internet access for user, that user will not be offered a logout option at the bottom of the block message page, even if the **Offer Logout** option on the **BLOCK/ACCEPT > Configuration** page is enabled.
- Users are not displayed in the **USERS/GROUPS > Account View** page when authenticated via Kerberos.

Hybrid Authentication Mode

Hybrid mode means using EITHER Kerberos or NTLM authentication along with LDAP, but not both. This enables you to deploy the Barracuda Web Filter both in inline mode for one group of users and in forward proxy mode for another group of users. This is useful if you want to apply different browsing policies to two different user groups.

For example, if you configure LDAP with **Single Sign-On** for one group of users and Kerberos authentication for another group of users, each group will receive a pop-up window indicating access denied to blocked sites, but the LDAP group will be able to bypass the block page by logging in with their LDAP credentials. The Kerberos group will not be able to bypass the block page.

For Hybrid Mode, configure LDAP and either NTLM or Kerberos authentication services as usual. When configured in this manner, the default proxy server port is 3128. You do not need to do anything else to enable Hybrid Mode.

Background

Kerberos is an authentication protocol that provides mutual authentication; i.e. both the user and the server verify each other's identity. For this reason, Kerberos is considered a more secure authentication protocol than NTLM. Implementing Kerberos-based authentication within your network will allow the Barracuda Web Filter to associate outgoing web requests with Active Directory users, log user activity, and apply

user-specific or group-specific policies to outgoing connections without requiring users to log into the Barracuda Web Filter.

Kerberos is useful when a Microsoft domain controller is running in native mode. It is a Forward Proxy authentication scheme and the Barracuda Web Filter need not verify each authentication request against a domain controller.

How to Enable LDAP Domain User Authentication

If your network uses a Lightweight Directory Access Protocol (LDAP) or Active Directory authentication (AD) server, your LDAP domain users can use the LDAP or AD authentication service to be authenticated in the Barracuda Web Filter system. The Barracuda Web Filter can also enable you to look up users by organizational units you have defined on your LDAP server when creating exceptions to block/accept policy.

To enable LDAP user authentication, from the **USERS/GROUPS > Authentication** page, in the LDAP tab, provide information about connecting to the LDAP server, binding to the LDAP server, encryption type and LDAP attributes. See the online help for detailed steps.

How to Enable NTLM Domain User Authentication

If your network uses an NT LAN Manager (NTLM) authentication server, your NTLM domain users transparently become authenticated in the Barracuda Web Filter using their Microsoft Windows credentials. This single sign-on (SSO) method of access control is provided by transparent proxy authentication against the your NTLM server.

To enable transparent proxy authentication against your NTLM server, you must join the Barracuda Web Filter to the NTLM domain as an authorized host. The process of joining the domain also synchronizes NTLM group information from your domain controller to the Barracuda Web Filter. Configure NTLM authentication on the **USERS/GROUPS > Authentication** page **NTLM** tab.

Related Articles
<ul style="list-style-type: none">• Integrating the Barracuda Web Filter With a User Authentication Service• How to Choose Your Authentication Mechanisms• How to Configure Kerberos Authentication

Windows Support for NTLM authentication

Windows Server 2000 and Windows 2003 with Active Directory (in mixed mode) run the NTLM authentication protocol by default. In a native mode Active Directory domain, Windows Server 2003 runs the Kerberos authentication protocol.

Starting with Windows Vista, and also with Windows Server 2008 and Windows 7, both LM and NTLM are de-activated by default. Microsoft adopted Kerberos as the preferred authentication protocol for Windows 2003 and Windows Server 2008 Active Directory domains. Kerberos is typically used when a client belongs to a Windows Server domain, or if a trust relationship with a Windows Server Domain is established in some other way. For more on Kerberos, see [How to Configure Kerberos Authentication](#). However, NTLM can still be used in the following situations:

- The client is authenticating to a server using an IP address
- The client is authenticating to a server that belongs to a different Active Directory forest, or doesn't belong to a domain at all
- No Active Directory domain exists

For detailed descriptions of these scenarios, see the online help for the **USERS/GROUPS > Authentication** page.

Requirements for using an NTLM Authentication Server

Before you integrate with an NTLM authentication server, verify the following requirements:

- The Barracuda Web Filter must be deployed as a forward proxy.
- No other authentication services (LDAP, Kerberos, etc.) may be configured.
- No Barracuda DC Agents may be in use on any of your domain controllers.
- Web browsers must be configured to use the Barracuda Web Filter as the HTTP proxy.

For detailed descriptions of these requirements, see the online help for the **USERS/GROUPS > Authentication** page.

Limitations when using an NTLM Authentication Server

The following limitations apply when using an NTLM authentication server with the Barracuda Web Filter:

- No login override of blocked pages for NTLM domain users who encounter a block message.
- No logout option for NTLM domain users who proceed to a blocked web page.
- NTLM domain users are not listed in the Account View page.
- NTLM realm is not listed for users listed in the syslog output.

For detailed descriptions of these restrictions, see the online help for the **USERS/GROUPS > Authentication** page.

Role-based Administration 6.x

This article applies to the Barracuda Web Filter running firmware version 6.x. For information that applies to version 7.0 and higher, see [Role-based Administration 7.x](#).

The administrator of the Barracuda Web Filter might choose to delegate certain administrative tasks such as scheduling and/or running reports, viewing status and log pages, or creating exceptions to policy.

From the **ADVANCED > Delegated Admin** page, you can create and manage account roles for existing users. You can use the **Limit Access To** setting to further restrict access for an account to data associated with local users, local groups and/or IP groups. The roles are enumerated below. To enable users with these roles (except the Temporary Whitelist role, which does not log into the system) to log into the Barracuda Web Filter using their LDAP credentials, check the **Use LDAP Authentication** box on the page.

The **Policy Alerts** feature enables you to have the Barracuda Web Filter send an email alert to the Policy Alert Email Address you specify with a summary of authenticated violators of policy (Warn, Block or Monitor actions taken) based on content filters. The message will summarize actions by the top violators based on settings on the **BASIC > Administration** page. From the **ADVANCED > Delegated Admin** page you can specify any role(s) to receive alerts by clicking **Receive Policy Alerts** and filling in an email address. You can alternatively configure the recipient on the **BASIC > Administration** page. See [Policy Alerts](#) for more information.

Roles and Permissions

Administrator

The administrator role has all permissions and is the only role that can create policies. The **Limit Access To** setting does not apply.

Read Only

This is the most restricted role, including access to all tabs in read-only mode and viewing (running, but not scheduling) reports. The **Limit Access To** setting does not apply. This role does not enable changing any settings.

Manage

The Manage role can view Status and Log pages, view and schedule reports and create exceptions on the **BLOCK/ACCEPT > Exceptions** page. All other **BLOCK/ACCEPT** tabs are read-only. The following pages are disabled:

- USERS/GROUPS
- ADVANCED
- BASIC > IP Configuration
- BASIC > Administration

The **Limit Access To** setting applies.

Monitor

This role can view Status and Log pages and can view and schedule reports. All **BLOCK/ACCEPT** pages are read-only. The following pages are disabled:

- USERS/GROUPS
- ADVANCED
- BASIC > IP Configuration
- BASIC > Administration

The **Limit Access To** setting applies.

Support

For users in a helpdesk type of position, the Support role enables viewing Status and Log pages as well as reports, but this role cannot schedule reports. The Support role can create exceptions on the BLOCK/ACCEPT > Exceptions page, but all other BLOCK/ACCEPT tabs are read-only. The following pages are disabled:

- USERS/GROUPS
- ADVANCED
- BASIC > IP Configuration
- BASIC > Administration

Temporary Whitelist

This role has the unique purpose of providing authority to one or more specified users, groups or (LDAP) organizational units for temporary override of block policy for certain websites. This is helpful in situations in which you don't want to give the user a login to the Barracuda Web Filter, but you want them to be able to *temporarily* override block policies, perhaps for other users such as students or coworkers. When you create this role, you must choose one of these authentication methods:

- Enter a **Username** and **Password** on the **ADVANCED > Delegated Admin** page that the selected user(s) must use to override block pages. The user must then keep these credentials secure for their own use.
- Check **Use LDAP Authentication** to require a user to enter their LDAP credentials for overriding block pages. If using this authentication option, it's best to also use the **Limit Access To** drop-down to select the user(s), group(s) or LDAP organizational unit(s) who can override block pages.

If you create this role, then the next time a user is blocked, the block page will include a **Request Override** button. Clicking this button launches a form below the block page with Username and Password fields as well as radio buttons to specify either allowing the specific site or the entire category of sites to which the URL belongs. The authorized user would then enter either the Username and Password you create on the **ADVANCED > Delegated Admin** page or their LDAP credentials, depending on how you configured the role. You can also specify the **Access Duration**, allowing access the site or category of sites for a specific time frame.

Note that you **MUST** create a *Temporary Whitelist* role before you'll see the **Request Override** button on the block page that allows for the login and block override for this role.

Use Cases for Various Roles

- **Monitoring and Reporting:** Use the *Read Only* role for the user who will be monitoring status and running (but not scheduling) reports on the Barracuda Web Filter. This role cannot change any settings.
- **Temporary Whitelist:** A group of students needs to access websites relative to a science class on reproduction, but those sites are typically blocked by policy. The teacher can be given the *Temporary Whitelist* role login and password or use their LDAP credentials to log in when a block page comes up. This enables the teacher to allow the blocked site (or the category of sites to which that URL belongs) for a limited time while the students do research.
- **Monitoring, Reporting and Creating Exceptions:** The *Support* role is designed for the Helpdesk person in the organization who provides daily reporting and monitoring of set policies for the administrator who has delegated these tasks. Unlike the *Read Only* role, this role can also create exceptions to policies as directed by the administrator.

Role-based Administration 7.x

This article applies to the Barracuda Web Filter running firmware version 7.0 and higher. For information that applies to version 6.x, see [Role-based Administration 6.x](#).

The administrator of the Barracuda Web Filter might choose to delegate certain administrative tasks such as scheduling and/or running reports, viewing status and log pages, or creating exceptions to policy.

On the **ADVANCED > Delegated Admin** page, you can create and manage account roles for existing users. You can use the **Limit Access To** setting to further restrict access for an account to data associated with local users, local groups and/or IP groups. The roles are enumerated below. To enable users with these roles to log into the Barracuda Web Filter using their LDAP credentials, check the **Use LDAP Authentication** box on the page. Alternatively, you can assign a username and password to the role when you create it on the **ADVANCED > Delegated Admin** page.

The **Policy Alerts** feature enables you to have the Barracuda Web Filter send an email alert to any role you specify, summarizing authenticated users who violate policy. The message will summarize actions (Warn, Block or Monitor) by the top violators of policies configured on the **BLOCK/ACCEPT > Content Filter** page and on the **BLOCK/ACCEPT > Exceptions** page. For details on configuration, see [Policy Alerts](#).

Roles and Permissions

Administrator

The administrator role has all permissions and is the only role that can create policies. The **Limit Access To** setting does not apply.

Read Only

This is the most restricted role, including access to all tabs in read-only mode and viewing (running, but not scheduling) reports. The **Limit Access To** setting does not apply. This role does not enable changing any settings.

Manage

The Manage role can view Status and Log pages, view and schedule reports and create exceptions on the **BLOCK/ACCEPT > Exceptions** page. All other **BLOCK/ACCEPT** tabs are read-only. The following pages are disabled:

- USERS/GROUPS
- ADVANCED
- BASIC > IP Configuration
- BASIC > Administration

The **Limit Access To** setting applies.

Monitor

This role can view Status and Log pages and can view and schedule reports. All **BLOCK/ACCEPT** pages are read-only. The following pages are disabled:

- USERS/GROUPS
- ADVANCED
- BASIC > IP Configuration
- BASIC > Administration

The **Limit Access To** setting applies.

Support

For users in a helpdesk type of position, the Support role enables viewing Status and Log pages as well as reports, but this role cannot schedule reports. The Support role can create exceptions on the **BLOCK/ACCEPT > Exceptions** page, but all other **BLOCK/ACCEPT** tabs are read-only. The following pages are disabled:

- USERS/GROUPS
- ADVANCED
- BASIC > IP Configuration
- BASIC > Administration

Use Cases for Various Roles

- **Monitoring and Reporting:** Use the *Read Only* role for the user who will be monitoring status and running (but not scheduling) reports on the Barracuda Web Filter. This role cannot change any settings.
- **Monitoring, Reporting and Creating Exceptions:** The *Support* role is designed for the Helpdesk person in the organization who provides daily reporting and monitoring of set policies for the administrator who has delegated these tasks. Unlike the *Read Only* role, this role can also create exceptions to policies as directed by the administrator.
- **Users are blocked from websites they need to access:** The *Manage* role can create exceptions to policy for block, warn, monitor or allow actions that have been set for various domains or categories of domains. For example, job search websites may be blocked for most employees, but certain members of the HR department need to access them. This role can make an *Allow* exception for a Local Group such as *HR Managers* (see **USERS/GROUPS > New Users** and **USERS/GROUPS > Local Groups** to assign users to groups) to access the *Job Search & Career Development* sub category of domains .
- **Support for performance or connectivity issues:** The *Support* role can view the **BASIC > Status** page to check performance statistics and note if there are any red indicators on throughput, system load or report/log storage.

Related Articles

- [Audit Log](#)

Advanced Configuration

For details about configuration of these features, please see the online help in the Barracuda Web Filter web interface.

Enabling and Disabling Virus Protection

By default, virus scanning is automatically enabled on the Barracuda Web Filter, and the virus definitions are updated on a regular basis (hourly by default) using Energize Updates.

When virus scanning is enabled, all traffic processed by the Barracuda Web Filter is scanned for viruses and any traffic that contains a virus is blocked. If you already have anti-virus software protecting your web traffic, you can turn off virus scanning on the Barracuda Web Filter using the **BASIC > Virus Checking** page. Otherwise, it is recommended to leave this feature turned on.

Proxy Settings

Use the **ADVANCED > Proxy** page to configure proxy settings for peer proxies, headers, HTTP and HTTPS ports as well as exceptions to proxy authentication by source IP address, domain name, header pattern or destination IP address. Note that peer proxy only works with inline deployments.

Web Caching

Web caching on the Barracuda Web Filter can accelerate web page downloads and also reduce traffic on the external network connections. For these reasons, it is recommended to keep web caching enabled. Use the **ADVANCED > Caching** page to enable or disable web caching, to clear the cache or to create exceptions for domains you don't want the Barracuda Web Filter to cache.

Remote Filtering for Offsite and Mobile Users

Remote Filtering enables your IT department to provide and control content security beyond the perimeter of the IT infrastructure. For satellite offices, remote and mobile workers, and students, the Remote Filtering feature allows secure web browsing access, from any computer or iOS device and any location, that complies with the web access and security policies of the organization. The Remote Filtering feature is available for use with the Barracuda Web Filter model 410 and higher and the [Barracuda Web Security Service](#).

Three options give you flexibility in how you protect your remote and mobile users online:

- [Barracuda Web Security Agent](#) - The Barracuda Web Security Agent (WSA) is deployed on each remote desktop or laptop and proxies all web traffic over the Internet to a specified Barracuda Web Filter, which can monitor web traffic and apply web security policies. Also available with the [Barracuda Web Security Service](#).
- [Barracuda Safe Browser](#) - You can deploy and use the Barracuda Safe Browser on mobile devices in place of the native browser, applying the same security policies as those applied by the Barracuda Web Filter to other users in the rest of your network. If you have a Barracuda Web Filter running version 6.0.1 or higher, you can deploy and use the Barracuda Safe Browser on mobile devices running on and off of the network. Also available with the [Barracuda Web Security Service](#).
- [Global HTTP Proxy](#) - Global HTTP Proxy, an offering of Apple, Inc., is a feature embedded in the client for proxying traffic from iOS 6.0 devices over cellular or WiFi networks to a web security solution. Global HTTP Proxy is particularly useful for schools issuing iPads to students who take them off network.

Barracuda Web Security Agent (WSA) - How it Works

Remote Filtering With the Barracuda Web Filter

To take advantage of Remote Filtering, the Barracuda Web Security Agent (WSA) is deployed on each remote desktop or laptop and proxies all web traffic over the Internet to a specified Barracuda Web Filter, which has been configured to recognize each remote client by traffic signed by the Barracuda WSA.

Related Articles

- [How to Install the Barracuda WSA](#)
- [How to Configure and Manage the Barracuda WSA](#)

You can download the files required to install the Barracuda WSA for Windows or Macintosh and configure how it filters traffic for your remote users via the **ADVANCED > Remote Filtering** page in the Barracuda Web Filter web interface.


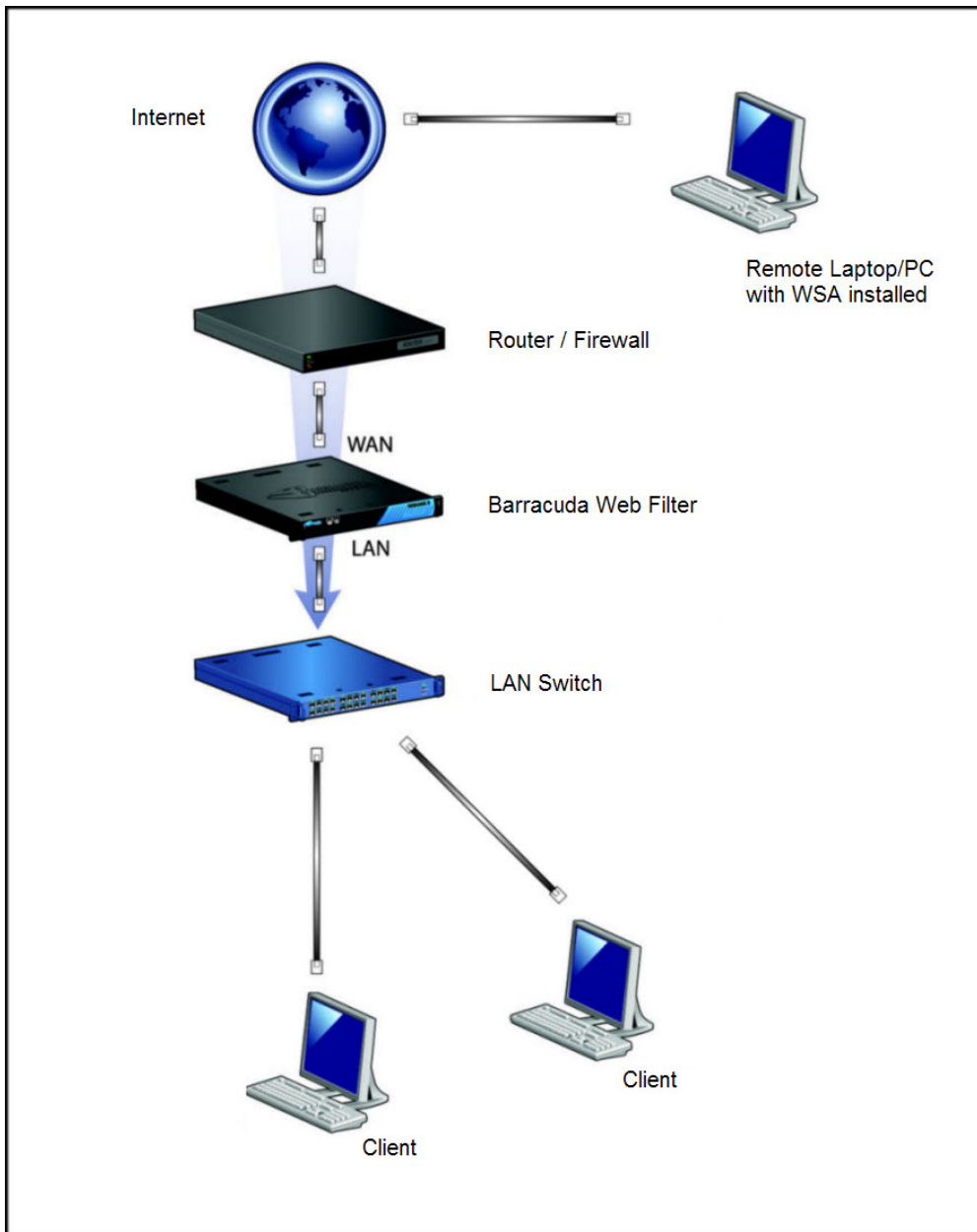
 The Barracuda WSA works with LDAP authenticated users.

Figure 1: The Barracuda WSA proxies remote users' web traffic to the Barracuda Web Filter.



When remote users browse the web, all filtering policies configured on the Barracuda Web Filter associated with their Barracuda WSA are applied to their browsing sessions. The Barracuda WSA intercepts all HTTP/S and FTP traffic through any connection on the remote computer without regard to the type of web browser. This includes Ethernet, wireless, or dial-up connections. The Barracuda WSA works with the Barracuda Web Filter to prevent malware from reaching remote computers, and only safe traffic is passed down to their web browsers.

Exceptions to Filtering with the Barracuda WSA

From the **ADVANCED > Remote Filtering** page, you can specify domains or subnets that should bypass filtering by the Barracuda Web Filter as well as any existing proxies on the client's LAN for which traffic should bypass filtering.

Begin initial configuration of your Barracuda WSA installation by identifying all of your internal IP addresses and proxies, then entering those in the Bypass Filter and Proxy Exception text boxes on the **ADVANCED > Remote Filtering** page. This will exempt these IP addresses from traffic

redirection. If you have a PAC or WPAD driven proxy setup, ensure that the proxy hosts are also listed as Proxy Exceptions. Also make sure to identify the external IP address of your Barracuda Web Filter in the External Hostname/IP field so that the Barracuda WSA can direct user web traffic to that IP address.

Policy Lookup-Only Mode

In this mode, the Barracuda WSA on the remote user's machine looks up policies configured on the Barracuda Web Filter for that user/client, applies the policies, then routes allowed web traffic from the user's machine via its usual path to the Internet. Traffic is not routed through the Barracuda Web Filter.

The advantage of using Policy Lookup Only mode is that it saves corporate bandwidth and reduces traffic through your Barracuda Web Filter. The disadvantage is that, since the remote client's traffic does not pass through the Barracuda Web Filter, virus and malware scanning is not applied to this traffic. This is an important consideration when deciding whether or not to enable Policy Lookup Only mode.

To enable this mode, simply set **Policy Lookup Only Mode** to Yes on the **ADVANCED > Remote Filtering** page of the Barracuda Web Filter web interface.

Application Filtering with the Barracuda WSA

The Barracuda WSA automatically forwards web browser traffic on all ports, and forwards traffic from all other applications on ports 80 and 443. On the **ADVANCED > Remote Filtering** page you can specify how the Barracuda WSA filters application traffic by default (Default Filter Settings):

- Filter ports 80 and 443 for all applications,
- Filter specified applications and allow all others, or
- Filter specified applications and block all others.

If you have specific applications that use other ports, you can add them to the **Applications to Filter** (All Ports) list on the **ADVANCED > Remote Filtering** page. You can also list specific applications to always block, or specific applications to filter.



The Barracuda Web Filter Vx virtual appliance does not support application blocking.

How to Configure and Manage the Barracuda WSA

Initial Configuration

Begin initial configuration of your Barracuda WSA installation by doing the following using the **ADVANCED > Remote Filtering** page on the Barracuda Web Filter Web interface:

1. Identify the external IP address of your Barracuda Web Filter in the **External Hostname/IP** field so that the Barracuda WSA can direct user web traffic to that IP address. **Note:** It is recommended that you enter the *hostname* of your Barracuda Web Filter in case the IP address of the appliance changes, which would interrupt service for your current Barracuda WSA installations in the field. If you do enter the IP address and must change it at some point, the following procedure is required to ensure minimal service interruptions:
 - 1a. Create the new IP address forward on your network firewall while the existing/old Barracuda Web Filter IP address is still accessible to Barracuda WSA installations.
 - 1b. Enter the new IP address in this field so that the Barracuda WSA in the field can be updated with the new IP address of the Barracuda Web Filter.
 - 1c. Once all of your Barracuda WSA installations are updated with the new IP address, you can expire the old IP address.
2. Identify all of your internal IP addresses and proxies, then entering those in the **Bypass Filter** and **Proxy Exception** text boxes. This will exempt these IP addresses from traffic redirection. If you have a PAC or WPAD driven proxy setup, ensure that the proxy hosts are also listed as **Proxy Exceptions**.
3. Create a port forward on your network firewall on port 8280 to the external IP address of your Barracuda Web Filter (**External Hostname/IP**).
4. Read the online help for the **ADVANCED > Remote Filtering** page on the Barracuda Web Filter web interface for details on the above and other configuration options.

Web Connectivity Issues and the Barracuda WSA

Once the Barracuda WSA is deployed for end users, the administrator can do any of the following to address any web connectivity issues users might have when using the Barracuda WSA on their remote laptops and PCs:

- Temporarily disable the Barracuda WSA if the user is experiencing any problems when they are logging into the network from a hotel or other captive portal. Check to see if the **Captive Portal** feature is enabled on the **BLOCK/ACCEPT > Configuration** page of your Barracuda Web Filter.
- Stop the Barracuda WSA service on the user's laptop or PC. Uninstall the Barracuda WSA from the user's laptop or PC through

How to Install the Barracuda WSA With the Barracuda Web Filter

Barracuda Networks recommends reading this entire article before installing the Barracuda Web Security Agent (WSA). After the Barracuda WSA is installed and configured, your web traffic is protected by the Barracuda Web Filter automatically. The Barracuda WSA directs all traffic from web browsers, and other application traffic on ports 80 and 443, to the Barracuda Web Filter.

Operating Systems Supported

- Windows XP SP3 32 bit & 64 bit
- Windows Vista 32 bit & 64 bit
- Windows 7 32 bit & 64 bit
- Windows 8 32 bit & 64 bit
- OS X 10.7 and 10.8 (for the iWSA)

Related Articles

- [Barracuda Web Security Agent - How it Works](#)
- [Download and Install Barracuda WSA \(Barracuda Web Security Service\)](#)
- [Remote Filtering for Offsite and Mobile Users](#)

Notes on Installing and Configuring the Barracuda Web Security Agent (WSA)

The methods for installing the Barracuda WSA include:

- [Installation Using a Windows GPO From the Windows Interface](#) - push the Barracuda WSA to a group of remote computers using a Windows tool to create a template for the GPO.
- [Installation Using a Windows GPO From the Command Line](#) - push the Barracuda WSA to a group of remote computers from a batch (.bat) file on the server.
- [Manual local Installation from the Command Line](#)
- [Installation on a Macintosh](#) - using the Macintosh installation program.

To uninstall, see [Uninstalling the Barracuda Web Security Agent for Win2K8 Server](#) or [Uninstalling the Barracuda Web Security Agent for Win2K3 Server](#), depending on your Windows server version.

You can download the installation files for MS Windows or the Macintosh from the **ADVANCED > Remote Filtering** page in the Barracuda Web Filter Web interface.

System Requirements for Windows

You can install Barracuda WSA on Windows systems that meet the following requirements:

- Latest released Service Packs of 32-bit version of Windows XP, and 32-bit or 64-bit versions of Windows Vista, Windows Server 2003 or Windows 7
- 1 GB ram
- 2 Ghz processor
- 30 MB free disk space
- Microsoft .NET Framework 4.0 Client Profile

System Requirements for Macintosh

You can install the Barracuda WSA on Macintosh systems that meet the following requirements:

- Version 10.5 (Leopard) or later operating system
- 50MB memory (10.5 requires 512MB, 10.6 requires 1.0GB)
- 3.5 GB RAM
- Intel or Power PC G4 or G5 processor
- 30 MB free disk space

Prerequisites for Installation or Upgrade

Consider the following prerequisites before installing the Barracuda WSA on one or more remote computers:

- The client PC must have Windows installed on the C:\ drive for successful installation of the Barracuda WSA. The Barracuda WSA will not install successfully when Windows is installed on the D:\ drive.
- The remote user must have an LDAP record in the domain.
- Because the Barracuda Web Filter will listen on port 8280 (by default) for Barracuda WSA requests, you must make this port be available for incoming and outgoing traffic to the Barracuda Web Filter. The Barracuda WSA cannot forward traffic properly if personal firewalls or other devices block non-standard ports. Create a port forward on your network firewall on port 8280 to the external IP address of your Barracuda Web Filter (as specified in the External Hostname/IP Address field on the **ADVANCED > Remote Filtering** page).
- The Barracuda WSA operates on network traffic at a low level within the operating systems, so some anti-virus applications may flag the Barracuda WSA as suspicious during installation or operation. Ensure that your anti-virus client does not block or has an exception for any Barracuda WSA files that the anti-virus client flags as suspicious.
- You must have Microsoft .NET framework installed before you install the Barracuda WSA using the MSI installation method. The MSI file does not install the .NET framework for you. If you do not install the .NET framework before you begin installation with the .MSI file, a message appears prompting you to download and install the .NET framework and then install the Barracuda WSA.
- The Barracuda WSA is now localized for the following languages:
 - German
 - Japanese
 - Dutch
 - Chinese
 - Chinese Traditional
 - Portuguese
 - Spanish

Password Protection and User Privileges

During installation, you have an option to specify a password to protect configuration options and control user privileges. If you specify a password during installation, that password is required for any user to:

- Change configuration settings
- Temporarily disable the Barracuda WSA (to allow a user to connect to a public network, such as at a captive portal in a hotel or coffee shop, before the Barracuda WSA starts again automatically after two minutes)
- Stop or start the Barracuda WSA service
- Uninstall Barracuda WSA on the client

There is no password reset; if the password is lost, the administrator must reinstall the Barracuda WSA.

Allow Uninstall Option

You can choose the **Allow Uninstall Through Add/Remove Programs** option during installation to allow the user to remove the Barracuda WSA from a computer using the Microsoft Windows Add or Remove Programs window. Use the password protection feature to ensure that unauthorized users cannot uninstall the Barracuda WSA. Note that the Barracuda WSA does not, by default, appear in the Windows Add or Remove Programs list.

Stop/Start Service Option

You can choose an option during installation that lets users stop and start the Barracuda WSA from the task tray. This is sometimes helpful with troubleshooting network or performance issues, or when the user needs to connect with their VPN (see below). You can use the password protection feature to ensure that only authorized users can stop or start the Barracuda WSA.

VPN Interoperability

The Barracuda WSA will forward all web traffic to the Barracuda Web Filter, so virtual private network (VPN) clients that rely on web browser settings to forward traffic to private networks may interfere with the Barracuda WSA's operation.

In order to use a VPN client on a PC that is running the Barracuda WSA, the end user may either have to:

- Stop the Barracuda WSA when connecting with the VPN,

- Use the VPN in split tunnel mode, or
- Have the Barracuda Web Filter enter bypasses for the VPN server IP address in the Bypass Filter text box on the **ADVANCED > Remote Filtering** page of the Barracuda Web Filter web interface. You can also specify bypass exception network addresses in the Bypass field during manual local installation or by using the BYPASS option in a GPO installation.

If you install and configure the Barracuda WSA so that end users may not stop and restart it, then only bypasses or split tunnel mode will work simultaneously with the Barracuda WSA. You can use the password protection feature, available during installation, to ensure that only authorized users can stop or start the Barracuda WSA.

Automatic Software Updates

The Barracuda WSA periodically checks the Barracuda Web Filter for available software updates. When an upgrade is available, the Barracuda WSA automatically and silently downloads and installs it, preserving any configuration information you have in place. The automatic updater works whether the Barracuda WSA is installed in regular mode or silent operating mode. Automatic updates may be disabled at installation for those network environments that prefer to manage upgrade deployments manually.

Installation on a Macintosh

Macintosh System Requirements for the Barracuda Web Security Agent

You can install the Barracuda WSA on Macintosh systems that meet the following requirements:

- Version 10.5 (Leopard) or later operating system
- 50MB memory (10.5 requires 512MB, 10.6 requires 1.0GB)
- 3.5 GB RAM
- Intel or Power PC G4 or G5 processor
- 30 MB free disk space

Installation

Navigate to the **ADVANCED > Remote Filtering** page of the Barracuda Web Filter web interface. In the **Download Web Security Agent** section of the page, click the **Download/Install** link for the Macintosh OS-X. Launch the installer on the Macintosh and follow on-screen instructions.

Installation using a Windows GPO from the Command Line

The Barracuda WSA can be pushed to a group of remote computers using a GPO from the command line with a batch file. The batch file simply needs to contain one line, indicating the name of the msiexec file that executes the .msi file used to install the application, and any options you specify per the table below. The .msi installer file is downloadable from the **ADVANCED > Remote Filtering** page on the Barracuda Web Filter.

Step 1: Download the MSI Windows Installer Package and create an MST file

1. Log on to the server computer as an administrator.
2. Create a shared folder on the network where you will put the installer package (.msi file) that you want to distribute. Clients to which you want to push the Barracuda WSA in the Windows domain must have access to this shared folder.
3. Log in to the Barracuda Web Filter interface with the administrator credentials. Navigate to the **ADVANCED > Remote Filtering** page.
4. Click on the **Download/Install** link to download the Barracuda WSA MSI installer from the **Download Web Security Agent** section of the page.
5. Save the MSI installer file in the shared folder on the network.
6. Create a one-line batch file (per the syntax in the example below) and save the file on a network shared folder that is accessible to all remote computers to which you want to push the Barracuda WSA. Include the options and arguments per the table below.
7. Create a GPO container for all users / machines to which you want to push the application.
8. Create a GPO with the Windows GPO editor.
9. In the GPO editor, select either 'startup' or 'shutdown' to trigger when the GPO installs the application on the remote machine.
10. Add the batch file (script) you saved in the shared folder. The application should then install silently on the remote machine when the user either logs in or shuts down the machine.

Example of the command line to put into the batch file:

```
BarracudaWSASetup.exe /s /v"/lvemo \setup.log /qn ALLOW_REMOVE=1
```

```
EXCEPTIONS=chrome.exe|safari.exe APPLICATIONS=explorer.exe|firefox.exe
```

```
BYPASS=11.11.11.0;*.myWebfilter.com;192.168.* PASSWORD=pass"
```

This example also writes a log file to the setup directory called **setup.log**.

Command Line Arguments and Options

Use the following arguments and options to control the configuration of Barracuda WSA.

Arguments:

- **s** runs Setup.exe in silent mode (no dialog boxes).
- **v** passes the **/qn** (no UI) parameter to the installer, which runs the executable in silent mode.

The following table describes additional options:

Option	Description	
ALLOW_REMOVE	<p>1 indicates that users are allowed to remove the Barracuda WSA.</p> <p>0 indicates that users are NOT allowed to remove the Barracuda WSA.</p>	
EXCEPTIONS	If there are specific applications from which you don't want to capture any traffic, type them in as a pipe-delimited list.	
APPLICATIONS	Type a pipe-delimited list of applications that will forward all ports to the Barracuda Web Filter.	
BLOCKS	Type a pipe-delimited list of applications to block. Example: BLOCKS=block1.exe block2.exe	
BYPASS	Type a semi-colon-delimited list of network addresses that you want to bypass the Barracuda Web Filter, such as trusted internal networks. Guidelines: Use a * in any octet (except the first) to indicate "any". Bypass entries that begin with a dot (.) will include any URL that matches the dot and subsequent string(s). For example, if you use *.example.com as a bypass entry, any URL that ends with .example.com will bypass the proxy. URL names that begin with a string (and not a dot) must match the string exactly.	
PASSWORD	Type the password users must know to configure, stop or start the Barracuda WSA.	
USER_MODE	<p>0 indicates ordinary operation.</p> <p>1 indicates silent operation.</p>	
SERVICE_URL	Type the IP address or hostname of the Barracuda Web Filter, followed by SERVICE_PORT and the port number.	

SERVICE_PORT	Type the port number of the Barracuda Web Filter, which is 8280 by default. This parameter follows the SERVICE_URL. Example: SERVICE_URL=myWebFilter.com SERVICE_PORT=8280	
SERVICE_MODE	2 indicates that you are using the Barracuda Web Filter. Example: SERVICE_MODE=2	
DISABLE_AUTOMATIC_UPDATES	1 indicates that updates are DISABLED. 0 indicates that updates are ENABLED.	
DEFAULT_BEHAVIOR	1 indicates that all application traffic is forwarded to ports 80 and 443 by default. 2 indicates that no application traffic is forwarded by default and you specify only the applications to filter. 3 indicates all applications are blocked by default and only applications you specify for filtering are forwarded.	
PROXY_EXCEPTIONS	Type a semi-colon-delimited list of network addresses to specify proxy exceptions for internal proxies that should be reachable by Barracuda WSA clients for internal proxying and filtering. Guidelines: Use a * in any octet (except the first) to indicate "any". Entries that begin with a dot (.) will include any URL that matches the dot and subsequent string(s). For example, if you use *.example.com as a proxy exception entry, any URL that ends with .example.com will bypass the proxy. URL names that begin with a string (and not a dot) must match the string exactly.	

Installation using a Windows GPO from the Windows Interface

This article covers installation using a Windows GPO from the Windows interface on Win2K8 server and Win2k3 server.

Install the Barracuda WSA application on Win2K8 Server

Step 1: Download the MSI Windows Installer Package and create an MST file

Related Articles
<ul style="list-style-type: none"> • Uninstalling the WSA - Win2K8 Server • Uninstalling the WSA - Win2K3 Server

1. Log on to the server computer as an administrator.
2. Create a shared folder on the network where you will put the installer package (.msi file) that you want to distribute. Clients to which you want to

push the Barracuda WSA must have access to this shared folder.

3. Log in to the Barracuda Web Filter Web interface with the administrator credentials. Navigate to the **ADVANCED > Remote Filtering** page.
4. Click on the **Download/Install** link to download the Barracuda WSA **MSI** installer from the **Download Web Security Agent** section of the page.
5. Save the MSI installer file in the shared folder on the network.
6. Download the open source ORCA tool, a Windows installer package editor which you can use to create a Windows transform file (.mst file). You can download the ORCA tool from: <http://www.softpedia.com/progDownload/Orca-Download-79861.html>
7. Launch the ORCA tool after download. Click on File -> Open in the dialog window. Select the installer package *BarracudaWSASetupshared folder* from the shared folder. Click on Open. Once all the database tables are loaded, select New Transform from the Transform menu item. Select the Property table from the left list. Scroll to the bottom of the table, right click and select "Add Row". Add the following Properties with corresponding values to specify the use of Barracuda Web Filter as a service.

Property:SERVICE_MODEValue:2

Property:USER_MODEValue:0

Property:SERVICE_URLValue:<Barracuda Web Filter IP Address>

Property:SERVICE_PORTValue:8280

8. After adding all the properties, select "Generate Transform" from the Transform menu item. Save this .mst file in the same shared folder which contains the .msi file. Close the ORCA tool window.

Step 2: Deploy the Barracuda WSA through the Active Directory by creating a GPO

1. Create a Container or Organizational Unit. Open the Active Directory **Users and Computers** window. In the console tree, right-click your domain, and then select New -> Organizational Unit. Provide a name for the container and uncheck the checkbox "Protect container from accidental deletion" so as to be able to delete this container later. If checkbox is marked, it is not possible to delete this container.

In the same Active Directory Users and Computers window, to the Container, add the users and machines for which the policy needs to be applied. OR you can move the users from the USERS account to the container and machine accounts from COMPUTERS account to the container. Moving the users or machines prompts a warning. New domain users and computers can be created in this container.

2. Create a GPO. Click Start, point to Administrative Tools, and then click Group Policy Management. Expand the tree for your domain, select the newly created Container or OU, right-click and select the item "Create a GPO in this domain, and Link it here...". Provide a name for the GPO and click the OK button to close the window. This GPO will be added to your container and also to the Group Policy Objects list.
3. Now, select this GPO which is present in your container and right-click. Click on Edit to open the Group Policy Management Editor. If you assign this application to a user, it is installed when the user logs on to the computer. If you assign this application to a computer, it is installed when the computer starts.

To assign an application to a computer:

In the Group Policy Management Editor, expand "Computer Configuration", then expand "Policies" and "Software Settings". Select "Software Installation", right-click and select New -> Package...

In the open dialog box, make sure to type the full Universal Naming Convention (UNC) path of the shared installer package that you want. For example:

```
\\QAWIN2K8DC\msi files\BarracudaWSASetup.msi
```

Click Open. Select the Deployment Method as *Advanced* and click OK. In the Barracuda Web Security Agent Properties window, Click on the Modifications tab and click the Add button. In the Open dialog box, type the full Universal Naming Convention (UNC) path of the .mst Transform file. For example, \\QAWIN2K8DC\msi files\mysetup.mst and click Open. Click the OK button in the Barracuda Web Security Agent Properties window. Close all the open windows.

4. From the command-line window, run the command to force an update of group policy:

```
C:\Users\Administrator>gpupdate /Force
```

You should see the following output:

```
Updating Policy...
```

User Policy update has completed successfully.

Computer Policy update has completed successfully.

To assign an application to a user:

Expand "User Configuration", and then expand "Policies" and "Software Settings". Select "Software installation", right-click and select New -> Package. The rest of the setup for User Configuration is similar to the Computer Configuration as described above, concluding with a forced group policy update.

Step 3: Application Install (both Win2K3 and Win2K8 servers)

1. Start a computer that is joined to the domain for applying the computer-based policy.
2. Log in as the domain user to apply the user-based policy.
3. You should see the Barracuda WSA Monitor icon in the system tray. This indicates that the Barracuda WSA application has been installed. You can also verify this in Add/Remove Programs from the Windows Control Panel.

Install the Barracuda WSA application on Win2K3 Server

Step 1: Download the MSI Windows Installer Package and create an MST

1. Log on to the server computer as an administrator.
2. Create a shared folder on the network where you will put the installer package (.msi file) that you want to distribute.
3. Log in to the Barracuda Web Filter interface using the administrator credentials. Navigate to the **ADVANCED > Remote Filtering** page.
4. Click on the **Download/Install** link to download the Barracuda WSA **MSI** installer from the **Download Web Security Agent** section of the page.
5. Save the MSI Installer file in the shared folder.
6. Download the open source ORCA tool, a Windows installer package editor which you can use to create a Windows transform file (.mst file). You can download the ORCA tool from:

<http://www.softpedia.com/progDownload/Orca-Download-79861.html>.

7. Launch the ORCA tool after download. Click on File -> Open in the dialog window. Select the installer package *BarracudaWSASetupshared folder* from the shared folder. Click on Open. Once all the database tables are loaded, select New Transform from the Transform menu item. Select the Property table from the left list. Scroll to the bottom of the table, right click and select "Add Row". Add the following Properties with corresponding values to specify the use of Barracuda Web Filter as a service.

Property:SERVICE_MODE Value:2

Property:USER_MODE Value:0

Property:SERVICE_URL Value:<Barracuda Web Filter IP Address>

Property:SERVICE_PORT Value:8280

8. After adding all the properties, select "Generate Transform" from the Transform menu item. Save this .mst file in the same shared folder which contains the .msi file. Close the ORCA tool window.

Step 2: Deploy the Barracuda WSA application through the Active Directory by creating a GPO

1. Create a Container or Organizational Unit. Open the Active Directory **Users and Computers** window. In the console tree, right-click your domain, and then select New -> Organizational Unit. Provide a name for the container and Click OK. In the same Active Directory Users and Computers window, to the Container, add the users and machines for which the policy needs to be applied. OR you can move the users from the USERS account to the container and machine accounts from COMPUTERS to the container. Moving the users or machines prompts a warning. New domain users and computers can be created in this container.
2. Create a GPO. Open the Active Directory Users and Computers window, select your domain, right-click and select Properties. In the Properties window, click on the Group Policy tab. Click on New button. Provide a name for this new Policy object. Close the Properties window by clicking on Close button.
3. Link this GPO to the new Container. In the same Active Directory Users and Computers window, select the new container, right-click and

choose Properties. In the Properties window, click on the Group Policy tab. Click the Add button. In the window "Add a Group Policy Object Link", click the All tab. Select the new GPO and Click OK to close the window. Click on Apply and OK to close the Container Properties window. If you assign this application to a user, it is installed when the user logs on to the computer. If you assign this application to a computer, it is installed when the computer starts.

4. Deploy the application. **To assign the application to a computer:**

4a. Right-click your domain in Active Directory Users and Computers window and select Properties. In the domain Properties window, click on the Group Policy tab. Select the new GPO and click on the Edit button. This opens the Group Policy Object Editor.

4b. Expand "Computer Configuration", and then "Software Settings". Select "Software installation", right-click and select New -> Package...

4c. In the Open dialog box, make sure you type the full Universal Naming Convention (UNC) path of the shared installer package that you want. For example, \\WFDEVDC01\msi files\BarracudaWSASetup.msi Click Open. Select the Deployment Method as Advanced and click OK.

4d. In the Barracuda Web Security Agent Properties window, Click on the Modifications tab and click the Add button. In the Open dialog box, type the full Universal Naming Convention (UNC) path of the .mst Transform file. For example, \\WFDEVDC01\msi files\mysetup.mst and click Open. Click the OK button in the Barracuda Web Security Agent Properties window. Close all the open windows.

4e. From the command-line window, run the command to force update of group policy.

```
C:\Documents and Settings\Administrator.WFDEVDC01>gpupdate/Force
```

```
Refreshing Policy...
```

```
User Policy Refresh has completed.
```

```
Computer Policy Refresh has completed.
```

To check for errors in policy processing, review the event log. Certain user policies are enabled that can only run during login. Certain computer policies are enabled that can only run during startup.

```
OK to Reboot? (Y/N)
```

If the server computer is rebooted, it installs the Barracuda WSA on the server machine also.

To assign the application to a user:

Expand "User Configuration", then expand "Policies" and "Software Settings". Select "Software installation", right-click and select New -> Package... The rest of the setup for User Configuration is similar to Computer Configuration as described above, concluding with a forced group policy update.

Step 3: Application Install (both Win2K3 and Win2K8 servers)

1. Start a computer that is joined to the domain for applying the computer-based policy.
2. Log in as the domain user to apply the user-based policy.
3. You should see the Barracuda WSA Monitor icon in the system tray. This indicates that the Barracuda WSA application has been installed. You can also verify this in Add/Remove Programs from the Windows Control Panel.

Troubleshooting

- A common cause of failure is the user and/or the user's computer does not have adequate access to the share location. Verify that all access and network privileges have been configured appropriately.
- Additional error messages may be found in the Event Log on the domain computer.
- If the Event Log has no useful information, consider enabling verbose logging and restarting the computer.
- Additional information on fixing Group Policy issues can be found on the Microsoft technet: <http://technet.microsoft.com/en-us/library/cc775423.aspx>

Manual local Installation from the Command Line

Local installation from the command line on the remote PC follows the same procedure as above without using a GPO. You can simply execute a one line command with options and arguments as shown below to immediately install the Barracuda WSA on the remote computer. Use the following command to install on a Windows PC or laptop:

```
BarracudaWSASetup.exe /s /v" /qb SERVICE_MODE=2 SERVICE_URL=10.1.0.51
```

SERVICE_PORT=8280 WD=1

Arguments and Options

Use the following arguments and options to control the configuration of the Barracuda WSA.

Arguments:

- **s** runs Setup.exe in silent mode (no dialog boxes).
- **v** passes the **/qn** (no UI) parameter to the installer, which runs the executable in silent mode.

You can set the **USER_MODE** switch to **1** for silent operation (the end user will not see the Barracuda WSA icon in the System Tray or Start Menu).

The following table describes additional options:

Option	Description
ADS	<p>1 indicates that users are allowed to disable the Barracuda Web Filter.</p> <p>0 indicates that users are NOT allowed to disable the Barracuda Web Filter.</p>
ALLOW_REMOVE	<p>1 indicates that users are allowed to remove the Barracuda WSA.</p> <p>0 indicates that users are NOT allowed to remove the Barracuda WSA.</p>
ALLOW_UPDATE	<p>1 allows seamless updates to the Barracuda WSA. The Check for Update menu option does not appear in the Configuration Tool (default).</p> <p>0 disables seamless updates. The Check for Update menu option appears in the Configuration Tool.</p>
APPLICATIONS	<p>Type a pipe-delimited list of applications to be filtered on all ports to the Barracuda Web Filter.</p> <p>Example:</p> <p>APPLICATIONS= iexplore.exe firefox.exe</p>
AUTH_KEY	<p>Paste or type the Barracuda Web Filter authentication key (generated by the Barracuda Web Filter).</p>
BLOCKS	<p>Type a pipe-delimited list of applications to block. Example:</p> <p>BLOCKS=block1.exe block2.exe</p>
BYPASS	<p>Type a semi-colon-delimited list of network addresses that you want to bypass the Barracuda Web Filter, such as trusted internal networks. Guidelines:</p> <p>Use a * in any octet (except the first) to indicate "any".</p> <p>Bypass entries that begin with a dot (.) will include any URL that matches the dot and subsequent string(s). For example, if you use *.example.com as a bypass entry, any URL that ends with .example.com will bypass the proxy.</p> <p>URL names that begin with a string (and not a dot) must match the string exactly.</p>

DEBUG	<p>1 indicates that the Debug mode is ENABLED.</p> <p>0 indicates that the Debug mode is DISABLED (default).</p>
DEFAULT_BEHAVIOR	<p>1 indicates that all application traffic is forwarded to ports 80 and 443 by default.</p> <p>2 indicates that no application traffic is forwarded by default and you specify only the applications to filter.</p> <p>3 indicates all applications are blocked by default and only applications you specify for filtering are forwarded.</p>
DISABLE_AUTOMATIC_UPDATES	<p>1 indicates that updates are DISABLED.</p> <p>0 indicates that updates are ENABLED.</p>
EXCEPTIONS	<p>If there are specific applications from which you don't want to capture any traffic, type them in as a pipe-delimited list.</p>
LANG	<p>Specifies the language that the Barracuda WSA uses on English operating systems.</p> <p>German: de-DE</p> <p>Japanese: ja-JP</p> <p>Dutch: nl-NL</p> <p>Chinese: zh-CN</p> <p>Chinese Traditional: zh-TW</p> <p>Portuguese: pt-BR</p> <p>Spanish: es-ES</p>
PASSWORD	<p>Type the password users must know to configure, stop or start the Barracuda WSA.</p>
PROXY_EXCEPTIONS	<p>Type a semi-colon-delimited list of network addresses to specify proxy exceptions for internal proxies that should be reachable by Barracuda WSA clients for internal proxying and filtering. Guidelines:</p> <p>Use a * in any octet (except the first) to indicate "any". Entries that begin with a dot (.) will include any URL that matches the dot and subsequent string(s). For example, if you use *.example.com as a proxy exception entry, any URL that ends with .example.com will bypass the proxy. URL names that begin with a string (and not a dot) must match the string exactly.</p>
SERVICE_MODE	<p>2 indicates that you are using the Barracuda Web Filter.</p> <p>Example: SERVICE_MODE=2</p>
SERVICE_PORT	<p>Type the port number of the Barracuda Web Filter, which is 8280 by default. This parameter follows the SERVICE_URL.</p> <p>Example: SERVICE_URL=myWebFilter.com SERVICE_PORT=8280</p>
SERVICE_URL	<p>Type the IP address or hostname of the Barracuda Web Filter, followed by SERVICE_PORT and the port number.</p>
USER_MODE	<p>0 indicates ordinary operation.</p> <p>1 indicates silent operation.</p>

Related Articles

- [Uninstalling the Barracuda WSA - Win2K8 Server](#)
- [Installation using a Windows GPO - Windows Interface](#)
- [Installation using a Windows GPO - Command Line](#)

Uninstalling the Barracuda Web Security Agent for Win2K8 Server

1. Log on to the server computer as an administrator.
2. Click **Start**, point to Administrative Tools, and then click **Group Policy Management**. Expand the tree for your domain, select the newly created Container or OU, expand the Container, select the new GPO, right-click and click **Edit...**
3. Expand the Configuration based on the assignment of a new GPO as follows:
 - a. Computer Configuration | Policies | Software Settings | Software installation.
User Configuration | Policies | Software Settings | Software installation.
 - b. Select "Software installation" and then select the Software "Barracuda Web Security Agent" from the right side list. Do a right-click and select All Tasks > Remove... This prompts the Removal method option. Choose the option "Immediately uninstall the software from users and computers" and click **OK**.
4. Close all the open windows. Run the command to force update of group policy.

```
C:\.Users\Administrator>gpupdate /Force
```

```
Updating Policy...
```

```
User Policy update has completed successfully.
```

```
Computer Policy update has completed successfully.
```

- a. Start the same computer on which Barracuda WSA application is installed (computer-based policy).
- b. Log in as the domain user to a machine on which Barracuda WSA application is installed (user-based policy).
- c. Look at the system tray - the Barracuda WSA Monitor icon should not be present. This indicates that Barracuda WSA application has been uninstalled. You can also verify this in the Add/Remove Programs section of the Control Panel.

Related Articles

- [Uninstalling the Barracuda WSA for Win2K3 Server](#)
- [Installation using a Windows GPO - Windows Interface](#)
- [Installation using a Windows GPO - Command Line](#)

How to Configure Global HTTP Proxy with Barracuda Web Security Solutions

Apple Inc. provides Global HTTP Proxy as a feature embedded in the client for proxying traffic from iOS 6.0 devices over cellular or WiFi networks to a web security solution. Global HTTP Proxy is particularly useful for schools issuing iPads to students who take them off network. Using the Global HTTP Proxy, you can be assured that ALL traffic to/from the iOS device is directed to and filtered by the service you configure – either the Barracuda Web Filter, or the Barracuda Web Security Service. You can use Global HTTP Proxy *instead of* the Barracuda Safe Browser to apply browsing policies and detect malware on iOS devices, and achieve the same results.

In this article:

- [System Requirements](#)
- [Global HTTP Proxy Configuration](#)
- [Sample Global HTTP Proxy Configuration Profiles](#)
 - [Using Global HTTP Proxy and the Barracuda Web Security Service](#)
 - [Using the HTTPS Global Proxy and the Barracuda Web Filter](#)

System Requirements

To use the Apple Global HTTP Proxy, you must have Apple Configurator v1.2 (requires OS X 10.6.6 or higher). You can use the Apple Configurator user interface to configure proxy settings in the Global HTTP Proxy, much like you would configure proxy settings in a client browser.

To use the Global HTTP Proxy you will need:

- iPad, iPhone or iPod touch running iOS 6.0. The most common use case is iPads.
- Mac with OS X 10.6.6 or higher;
- [Apple Configurator v1.2](#).

Global HTTP Proxy Configuration

To set up Global HTTP Proxy with either the Barracuda Web Filter or the Barracuda Web Security Service, you will need to prepare and supervise the iOS devices using the Apple Configurator.



The Apple Configurator will **erase** all the content and settings from a device when configuring the Global HTTP Proxy.

1. Use the USB cable to connect the iOS device to a Mac running Apple Configurator v1.2.
2. In the Apple Configurator, click **Prepare**.
3. Click Settings and set **Supervision** to *On*.
4. Click the **New Configuration Profile** button below the **Profiles** list and choose *Create New Profile*.
 - a. Enter a name for the profile in the General Settings payload that appears.
 - b. Select the Global Proxy payload from the list of payloads on the left, click Configure.
 - c. In the Global HTTP Proxy payload use the following configuration:
 - **Proxy Type** – *manual*
 - **Proxy Server** – Hostname of the Barracuda web security solution you're using:
 - External Hostname/IP Address of your Barracuda Web Filter, or
 - Service Hostname of the Barracuda Web Security Service.
 - **Port** – *8080*
 - d. Click the **Save** button to save the configuration profile.
5. Select the created profile in the **Profiles** list.
6. Click the **Prepare** button at the bottom of the Apple Configurator window.
7. Apply the changes.

Initial setup (preparation and supervision) may take up to 10-15 minutes.

Sample Global HTTP Proxy Configuration Profiles

Using Global HTTP Proxy and the Barracuda Web Security Service

The following is a sample configuration profile containing a Global HTTP Proxy payload using the Barracuda Web Security Service.

```
<?xml version="1.0" encoding="UTF-8"?>
```

```
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
  <key>PayloadContent</key>
  <array>
    <dict>
      <key>PayloadDescription</key>
      <string>Global HTTP Proxy</string>
      <key>PayloadDisplayName</key>
      <string>Global HTTP Proxy</string>
      <key>PayloadIdentifier</key>
      <string>mountains-mac-mini.local.CCA628EA-2206-4B7B-AEC3-6273781F0E6B.com.apple.proxy.http.global.EE0FFBA6-9307-4D98-9DD7-B7F5B5906523</string>
      <key>PayloadType</key>
      <string>com.apple.proxy.http.global</string>
      <key>PayloadUUID</key>
      <string>69A150DA-7935-47A0-A0E7-31D8A8C3E2C1</string>
      <key>PayloadVersion</key>
      <integer>1</integer>
      <key>ProxyServer</key>
      <string>ple7.flex.purewire.com</string>
      <key>ProxyServerPort</key>
      <integer>8080</integer>
      <key>ProxyType</key>
      <string>Manual</string>
    </dict>
  </array>
  <key>PayloadDisplayName</key>
  <string>Global HTTP Proxy with Flex</string>
  <key>PayloadIdentifier</key>
  <string>mountains-mac-mini.local.CCA628EA-2206-4B7B-AEC3-6273781F0E6B</string>
  <key>PayloadRemovalDisallowed</key>
  <false/>
  <key>PayloadType</key>
  <string>Configuration</string>
  <key>PayloadUUID</key>
```

```
<string>A5548496-F15B-4517-A965-6A4C336D480F</string>
<key>PayloadVersion</key>
<integer>1</integer>
</dict>
</plist>
```

Using the HTTPS Global Proxy and the Barracuda Web Filter

The following is a sample configuration profile containing a Global HTTP Proxy payload using the Barracuda Web Filter.

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
  <key>PayloadContent</key>
  <array>
    <dict>
      <key>PayloadDescription</key>
      <string>Global HTTP Proxy</string>
      <key>PayloadDisplayName</key>
      <string>Global HTTP Proxy</string>
      <key>PayloadIdentifier</key>
      <string>mountains-mac-mini.local.3804FE57-A0BD-44F7-B041-D2F2BE2D3C4D.com.apple.proxy.http.global.1FB665D8-D7A3-4177-A233-CC15EA8328A</string>
      <key>PayloadType</key>
      <string>com.apple.proxy.http.global</string>
      <key>PayloadUUID</key>
      <string>C132CE1D-5D49-42B6-A4F3-1E093C9D0D36</string>
      <key>PayloadVersion</key>
      <integer>1</integer>
      <key>ProxyServer</key>
      <string>10.1.0.235</string>
      <key>ProxyServerPort</key>
      <integer>8080</integer>
      <key>ProxyType</key>
      <string>Manual</string>
    </dict>
  </array>
  <key>PayloadDisplayName</key>
```

```
<string>Global HTTP Proxy with WF</string>
<key>PayloadIdentifier</key>
<string>mountains-mac-mini.local.3804FE57-A0BD-44F7-B041-D2F2BE2D3C4D</string>
<key>PayloadRemovalDisallowed</key>
<false/>
<key>PayloadType</key>
<string>Configuration</string>
<key>PayloadUUID</key>
<string>0494C196-BD6E-4DA8-A526-19FAD778B941</string>
<key>PayloadVersion</key>
<integer>1</integer>
</dict>
</plist>
```

Barracuda Safe Browser Setup Guide - With Barracuda Web Filter

In this article:

- [Basic Setup on the Barracuda Web Filter](#)
- [Basic Setup of the iOS Mobile Device](#)
- [Managing the Application in iOS](#)
- [Advanced Setup](#)

Related Articles

- [Barracuda Safe Browser - FAQ](#)
- [Barracuda Safe Browser User Guide](#)

i If you have a Barracuda Web Filter running version 6.0.1 or higher, you can deploy and use the Barracuda Safe Browser on mobile devices running on and off of the network. The Barracuda Safe Browser supports iOS 4.3 and higher.

You can deploy and use the Barracuda Safe Browser on mobile devices in place of the native browser, applying the same security policies as those applied by the Barracuda Web Filter to other users in the rest of your network. The Barracuda Safe Browser communicates with the Barracuda Web Filter to provide web security to mobile users, per settings configured on the **ADVANCED > Remote Filtering** page and per policies you configure on the **BLOCK/ACCEPT** pages.

Figure 1: iOS devices with the Barracuda Safe Browser installed are protected by the Barracuda Web Filter



Basic Setup on the Barracuda Web Filter

To configure and install the Barracuda Safe Browser:

1. Log into your Barracuda Web Filter as *admin* and navigate to the **ADVANCED > Remote Filtering** page. Under the **Remote Filtering Configuration** section, enter the **External IP Address/Hostname** (the external IP address or hostname of the Barracuda Web Filter that

will handle web traffic proxied from remote iOS devices running the Barracuda Safe Browser), and the **Destination Port** to which you want the Barracuda Safe Browser to direct web traffic from mobile devices. You will need to create a port forward rule on your firewall to this port and the **External IP Address/Hostname**.

2. On the **Safe Browser** tab, select an authentication option and other other settings specific to the Barracuda Safe Browser from the **Safe Browser** tab on the bottom portion of the page. Click on **Help** for additional information about the available settings.

Basic Setup of the iOS Mobile Device

1. From within your Wi-Fi network, launch the Safari browser on your iOS device and visit the [Apps Store](#) to fetch the Barracuda Safe Browser application.
2. Select the application for iPad or the iPhone and touch **Install**. Enter your Apple ID Password if prompted. When the application has downloaded, you'll see the Barracuda Safe Browser icon on the display. There are two options for the initial launch and provisioning of the Barracuda Safe Browser:
 - a. The administrator can send an email to the email address configured on the device with a link to provision the Barracuda Safe Browser. The link format is: `bsb://provision?mode=appliance&wanip=xx.xx.xx.xx:xxxx` , where `xx.xx.xx.xx:xxxx` represents the **External IP Address/Hostname** of your Barracuda Web Filter and `:xxxx` represents the **Destination Port** as entered on the **ADVANCED > Remote Filtering** page. Then the user can simply open the email message on the mobile device and touch the link in the email. The Barracuda Safe Browser will automatically be provisioned and will launch.
 - b. If the administrator has not sent the email, then under the orange **Provision** button, select the **Web Filter** option, then **Done**. In the *Host* textbox, the enter the IP address and port that was entered by the administrator on the Barracuda Web Filter **ADVANCED > Remote Filtering** page as mentioned above. Use the format per this example: `111.222.333.444:8280`
3. If the **Session Authentication** field on the **ADVANCED > Remote Filtering** page is set to *Forced Authentication*, the user will be prompted to provide LDAP credentials to log in. Alternatively one can tap the **Continue as Guest** button. **Note:** If you want to use the device with a different Barracuda Web Filter account, you must unprovision the device. When you connect to the other account, the device will be re-provisioned.
4. To enable the **BASIC > Remote Devices** page to report the physical location of the mobile device, touch **OK** when prompted to "Use Your Current Location".
5. **Enable Restrictions for the Safari browser locally on the device** through Settings > Restrictions, or using an MDM or Apple Configurator.
6. Once the local browser is restricted, the icon for that browser will disappear from the UI on the mobile device, and the user is ready to run Barracuda Safe Browser with policies you've configured in Barracuda Web Filter. Your Barracuda Web Filter policy will now be applied to all traffic from the Barracuda Safe Browser and will be reflected in reports.

Managing the Application in iOS

View Bookmarks: From the **Bookmarks** button at the bottom of the iOS display, you can view bookmarks provisioned to the device by Barracuda Web Filter as well as the bookmarks added by the user.

Log Out, Unprovision and Clear History: From the **Settings** button at the bottom of the iOS display you can view the Username, Hostname, Auth Key, Device ID and Version. If you need to log out the current user if the device will be shared, you can **Log Out, Unprovision** the device and **Clear History**. When the next user runs the Barracuda Safe Browser, the device will be re-provisioned and the user will be prompted to log in per the configuration by Barracuda Web Filter.

Advanced Setup

1. On the **ADVANCED > Remote Filtering** page, in the **WSA / Safe Browser Configuration** section, configure the following settings on the **Safe Browser** tab:
 - **Session Authentication:** If you want to require users to log in with LDAP credentials before browsing, select *Forced Authentication*. Selecting *Optional Authentication* will give the user the choice of either logging in and browsing with assigned policies, or browsing as a guest under a different set of policies. Select *None* if you don't want the user to be presented with a log in option – the user will only browse as a guest.
- Note:** If you configure LDAP authentication in Barracuda Web Filter for your Barracuda Safe Browser users, you can apply user-specific policies for each mobile user. Otherwise you can only apply global policies to all mobile users. To configure LDAP authentication, you'll need to expose your LDAP server to the Internet by port forwarding from your Barracuda Web Filter external IP address to port 389 (non-secure) or port 636 (secure) for your LDAP server. Currently Barracuda Web Filter supports Microsoft Active Directory.
- **Session Timeout:** If you have configured LDAP authentication for your mobile users, use this setting to specify the amount of time, in minutes, that is allowed to elapse before a user's login expires and re-authentication is required. To disable session expiration (so that a session does not expire until the user logs off), set this value to **0** hours or minutes. The recommended setting is **24 hours**.
 - **Idle Timeout** - If you have configured LDAP authentication for your mobile users, use this setting to specify the amount of time, in

minutes, that a user's session is allowed to remain idle before that login session automatically expires. To disable session expiration based on idle time, set this value to **0** hours or minutes. The recommended setting is *8 hours*.

- **Password:** Creating a password means that the user (or the administrator of the mobile device) can enter it to bypass all filtering by pressing the **Bypass** action button on their mobile device.
- **Bypass Filter:** Enter any IP addresses that you want to bypass filtering by Barracuda Web Filter.
- **Fail Open:** Set to *Yes* if you want the Barracuda Safe Browser to allow all web requests if the mobile device cannot reach Barracuda Web Filter for some reason. Setting to *No* means that all requests would be blocked in that case.
- **Enable Geolocation:** Setting to *Yes* means that the last location from which the user of the device logged in, or that the settings were synchronized, will be displayed in Barracuda Web Filter. If this feature is enabled, then on the **Remote Filtering > Safe Browser > Last Seen Devices** page, you'll see the username, the domain, the Device ID, the IP address, the last-seen location and time/date that the user last made a web request. This feature is useful for locating lost or stolen devices.
- **Allow Temporary Bypass Filtering:** Enabling this feature allows the administrator or user to temporarily bypass filtering by Barracuda Web Filter for up to 5 minutes, at which point filtering automatically resumes. If the user is connecting from an Internet cafe or hotel portal, for example, and needs to temporarily disable the Barracuda Safe Browser so that they can connect to their network, they can do so for the 5 minute period. Only 3 temporary disables are allowed once the Barracuda Safe Browser is installed. The **Password**, configured per above, is *not* required.
- **Allow Bypass Filtering:** Users who have administrative rights on their mobile devices will be able to bypass filtering indefinitely in their Barracuda Safe Browser. The **Password**, configured per above, is required.

Monitoring the System

The Barracuda Web Filter incorporates hardware and software fail-safe mechanisms that are indicated via system alerts and logs. The powerful reporting engine provides a broad spectrum of web traffic statistics and user-level activity reports which can be created ad-hoc, emailed to administrators or sent to an FTP or SMB server. You can monitor multiple Barracuda Web Filters using Barracuda Cloud Control (BCC), a centralized management web interface for managing, configuring and reporting on multiple devices from one central web console. These articles describe the tools and monitoring tasks you can use via the web interface and the front panel of the Barracuda Web Filter to track system performance and configure system alerts.

In this Section

- [Basic Monitoring Tools](#)
- [Reporting 6.x](#)
- [Reporting 7.x](#)
- [How to Set Up Alerts and SNMP Monitoring](#)
- [How to Set Up Barracuda Cloud Control](#)
- [Troubleshooting](#)
- [Syslog and the Barracuda Web Filter](#)

Basic Monitoring Tools

Performance statistics for the Barracuda Web Filter are presented on the **BASIC > Status** page for IT administrators to monitor the health of the system and to make sure traffic is flowing as expected. Web requests by users on the network is tracked and presented as raw data in the web logs as described below, but that data is also packaged and presented in an easy-to-read format in the reports module. In general the reports listed on the **BASIC > Reports** page should serve the needs of both managers and IT administrators regarding user productivity, bandwidth usage, infection/malware detection and more. For more about the Barracuda Web Filter reporting engine, see the [Reporting](#) article. For details about configuring and scheduling reports, see the online help in the **BASIC > Reports** page.

Related Articles

- [Reporting 6.x](#)
- [Audit Log of Configuration Changes](#)
- [Barracuda Cloud Control - Overview](#)
- [Syslog and the Barracuda Web Filter](#)

In this article:

- [Viewing performance statistics](#)
- [Logs for Web Traffic and Syslog](#)
 - [Web Traffic Log](#)
 - [Application log](#)
 - [Using a Syslog Server to Centrally Monitor System Logs](#)
 - [Warned Activity List](#)
 - [List of Infected Clients](#)
- [Remote Devices Tracking by Time and Location](#)
- [Task Manager](#)

Viewing performance statistics

The **BASIC > Status** page provides an overview of the health and performance of your Barracuda Web Filter, including the following:

- Filtering statistics (such as threats blocked by the filtering rules, blocked visits to known spyware websites, blocked downloads of spyware or viruses) for the past day and hour, as well as total statistics since installation (or last reset) of the Barracuda Web Filter.
- Performance statistics, such as CPU temperature, throughput, system load and TCP connections. Statistics displayed in red signify that the value exceeds the normal threshold.
- **Protection Status** -The current **Operating Mode** of the Barracuda Web Filter. With the exception of *Safe* mode, **Operating Mode** is configured on the **BASIC > IP Configuration** page. Possible modes are:
 - *Active*: Traffic is logged and policies are applied.
 - *Audit*: In inline mode, traffic is logged only. Policies are not applied. In forward proxy deployment, traffic is logged and policies are applied, just like they are in *Active* mode.
 - *Safe*: Note that this mode is systematically set if the system load on your Barracuda Web Filter is excessive because either the maximum number of TCP connections allowed on your model is exceeded, or the reporting engine is processing a large volume of data. **Safe mode cannot be triggered over the web interface and is not applicable if the Barracuda Web Filter is deployed in WCCP configuration.** In *Safe* mode the device will pass web traffic through without filtering and logging. The Barracuda Web Filter will send a notification email to the **System Alerts Email Address** that is specified on the **BASIC > Administration** page indicating the reason the device is experiencing a load issue. If the number of current TCP connections and/or the load on the reporting engine returns to normal range, the Barracuda Web Filter will resume *Active* mode; otherwise the device will remain in *Safe* mode and traffic will not be filtered or logged. At this point it is recommended that you place the Barracuda Web Filter in *Audit* mode and troubleshoot the problem. For further assistance, please contact [Barracuda Networks Technical Support](#).
- **Throughput** gauges the total volume of traffic that is passing through the Barracuda Web Filter and is measured in Mb/s.
- **TCP Connections** indicates number of concurrent TCP connections used by the Barracuda Web Filter to service Internet traffic, reported as a percentage of the maximum number of connections that can be handled by the system. TCP Connection usage can be monitored while in Audit mode as well as in Active mode without affecting production traffic. A single user typically requires 1 to 1.5 active TCP connections; however, the peak number of TCP connections can significantly increase with heavy Web browsing or with bandwidth-intensive Internet applications such as voice, instant messaging (IM) or other streaming media applications.
- **Cloud Control** indicates whether or not this Barracuda Web Filter is connected to the Barracuda Cloud Control (BCC) management tool. For general information about Barracuda Cloud Control, see [Barracuda Cloud Control - Overview](#). For details about connecting the Barracuda Web Filter to the BCC, see [How to Set Up Barracuda Cloud Control](#).
- **System Load** represents an estimate of CPU and disk load on the system. It is not unusual for the load to reach 100%, especially when the incoming queue is large. 100% load for long periods of time indicates trouble in the system, especially if the incoming queue continues to increase in size. If the System Load exceeds 50% for more than 5 minutes, the Operating Mode will automatically shift to Safe mode (unless the Barracuda Web Filter is deployed in WCCP configuration) and will pass traffic without filtering or logging until normal operation can be resumed. See the online help for the **BASIC > Status** page for more information.
- **Cache Hit Ratio** indicates the percentage of requests handled by the cache.
- **Subscription** status for Energize Updates, Instant Replacement, and Premium Support.
- Lists of infected clients and blocked web requests.

- A set of bar graphs that illustrate an hourly breakdown of requests made by your users in the last 24 hours, and a set of bar graphs that illustrate a daily breakdown of requests made by your users in the last 30 days. Both sets of graphs illustrate the following data:
 - Number of requests blocked
 - Number of requests received
 - Number of kilobytes per second used by the requests allowed

Each bar graph is accompanied by two Top Ten lists: domains represented in the graph and web content categories represented in the graph.

- LAN, WAN and AUX port connection details are associated with icons in the Link Status section, displaying connectivity where applicable (version 6.0.1 and higher). Hover the mouse over the LAN icon, for example, to see LAN connection details (MAC address, IP address, throughput). If the AUX port is configured, the icon will be displayed with details for that port in addition to icons for either or both the WAN and LAN. On the Barracuda Web Filter Vx, only the LAN port icon and details are displayed.

Logs for Web Traffic and Syslog

Web Traffic Log

The **BASIC > Web Log** page displays a list of system logs for your Barracuda Web Filter. On a regular basis you should view the Web Log page to monitor the web and spyware traffic (both HTTP and non-HTTP) passing through your Barracuda Web Filter. The page also has a button used to clear all traffic logs as needed. Use this page to view the following information about each entry in this log:

- Date and time the Barracuda Web Filter processed the request.
- IP address of the client that originated the request.
- IP address of the requested website or application
- For search engine requests, the search keyword(s) entered by the user
- Type of file contained in the request, as designated by the HTTP header. For a list of common MIME types, see the help page for the MIME Type Blocking feature.
- The user name or group that sent the request.
- The action taken by the Barracuda Web Filter (Allowed, Detected, Warned, Monitored, Blocked).
- The reason the Barracuda Web Filter performed the action.
- Detailed information about the actions.
- Number of bytes of data processed for this request.

You can perform the following operations on the **Web Log** page:

- Apply filters to locate specific log entries
- Refresh to update the log. The most recent entry is at the top of the list.
- Clear the log to purge all the current entries.
- Export the displayed entries to a CSV file.

Application log

The **BASIC > Application Log** page displays the log of web application traffic blocked by the Barracuda Web Filter. Note that the Barracuda Web Filter Vx virtual machine does not block applications. Use this page to view the following information about each entry in this log:

- Date and time the Barracuda Web Filter blocked the request.
- IP address of the client that initiated the request.
- Name of the application that was blocked.

You can perform the following operations in the **Application Log** page:

- Customize the appearance of the display
- Update the contents displayed in this page
- Clear the contents of the traffic log itself
- Filter the entries displayed
- Export the displayed entries to a CSV file

Using a Syslog Server to Centrally Monitor System Logs

Syslog is a standard UNIX/Linux tool for sending remote system logs and is available on all UNIX/Linux systems. The Barracuda Web Filter provides syslog data for both web traffic and system events. Use the **ADVANCED > Syslog** page to specify servers to which the Barracuda Web Filter sends each type of syslog data.

Syslog servers are also available for Windows platforms from a number of free and premium vendors. Barracuda Networks has tested with a Windows freeware syslog server from Kiwi Enterprises (www.kiwisyslog.com). Barracuda Networks makes no guarantees that your Barracuda

Web Filter will be completely compatible with this syslog server. **Note that syslog support is not available on the Barracuda Web Filter 210.**

For details about syslog output from the Barracuda Web Filter, see [Syslog and the Barracuda Web Filter](#).

Warned Activity List

The **BASIC > Warned Activity** page displays the list of all warned activity that is in effect for the client machines protected by the Barracuda Web Filter system. Use this page to view the following information about each entry in this log:

Date and time that the warned activity was triggered.

- IP address of the client machine that triggered the warned activity.
- Username that triggered the warned activity. This field indicates whether the user account is from the local, LDAP or NTLM realm.
- The URL that the user was attempting to access when the warned activity triggered.
- The domain names that triggered the warned activity.
- The Web content category that triggered the warned activity.

You can perform the following operations in the **Warned Activity** page:

- View details about a warned activity
- Clear all warned activity

A warned activity remains in effect until it times out (as configured in the **BLOCK/ACCEPT > Configuration** page) or until it is explicitly removed by the Administrator (using the **BASIC > Warned Activity** page). If the user attempts to access the same website after a warned activity times out or is deleted, the user must click the **Proceed** button to re-acknowledge the warning and then access the website again.

List of Infected Clients

The **BASIC > Infection Activity** page displays outbound activity monitored by the Barracuda Web Filter to sites/IP addresses that are known to be malicious, and displays a list of clients in the network that are infected with a virus or with spyware. Check this page for activity by client hostname or IP address to determine if further investigation should be performed on the client. The data in the log includes:

- **Spyware** - Names of the threats blocked by the Barracuda Web Filter.
- **Count** - Number of times that the Barracuda Web Filter blocked this threat.
- **Last Seen** - Date and time this threat type was last detected on this client.
- **Port** - The port over which the infection was detected.

You can use this list to determine if any of your clients have been prompted to use the [Barracuda Malware Removal Tool](#).

Remote Devices Tracking by Time and Location

(version 6.0.1. and higher)

The Barracuda Web Filter maintains a log of remote user and mobile devices seen by the Barracuda Web Security Agent (WSA) and the Barracuda Safe Browser. Logged data includes the date, time and location from which a remote user logged in or a mobile device was synchronized with Barracuda Web Filter settings. See the **ADVANCED > Remote Devices** page to view and configure. Logged fields include:

- **Username** - Username created for the device user login.
- **Domain** - Domain the user is logged into
- **Device Name** - Name given to the mobile device for identification
- **Device Type** - Mobile device type, for example: iPad, iPhone, etc.
- **IP Address** - IP address of the mobile device
- **Location** - GPS coordinates of the mobile device
- **Last Seen** - Date and time of the last user login or device synchronization with the Barracuda Web Filter

Task Manager

The **ADVANCED > Task Manager** page provides a list of system tasks that are in the process of being performed and also displays any errors encountered when performing these tasks.

Some of the tasks that the Barracuda Web Filter tracks include:

- Linked management setup
- Configuration restoration

If a task takes a long time to complete, you can click **Cancel** next to the task name and then run the task at a later time when the system is less busy. The **Task Errors** section will list an error until you manually remove it from the list. Note that the errors are not phased out over time.

Audit Log of Configuration Changes

The **BASIC > Audit Log** page displays updates to the configuration settings of the Barracuda Web Filter in conjunction with [Role-based Administration](#). This log provides the following information:

- Date and time the Barracuda Web Filter processed the operation.
- The name of the user that did the operation.
- The role assigned to the user that did the operation.
- The action performed by the user that did the operation:
 - *add* - Added a value for a field in the configuration.
 - *set* - Set a value for a field in the configuration.
 - *del* - Deleted a value for a field in the configuration.
- The scope, or area of the Barracuda Web Filter affected by the operation:
 - *global* - Applies to global level variables in the configuration.
 - *domain* - Applies to a variable associated with a particular domain.
 - *user* - Applies to a particular Barracuda Web Filter user account.
 - *policy* - Operation was done to a variable for which you can select a **Policy** of either *Authenticated* or *Unauthenticated* users. For example, **BLOCK/ACCEPT > Content Filters**, or **BLOCK/ACCEPT > Applications**.
- Detailed information about the operation.
- Which configuration variable affected by the operation, if any.
- Original value before the operation
- Changed value after the operation.

Log data can be exported to CSV file, and the rate of data streaming to the log can be adjusted.

Reporting 6.x

Use the **BASIC > Reports** page to choose from more than 40 different system reports that can help you keep track of activity performed by the Barracuda Web Filter. You can either generate a system report on-demand or configure the Barracuda Web Filter to automatically generate the system reports on an hourly, daily, weekly or monthly basis and email the reports to specific email addresses or send them to an FTP or SMB server. Reports can be anchored on user activity, content or actions.

Accurately Reporting User Browsing Times

Embedded web content is intelligently detected by the Barracuda Web Filter to maximize reporting accuracy. For example, a site such as **cnn.com** embeds requests to Facebook, twitter, and other social networks. While a user visiting the news site might not explicitly click on any of the embedded links, the embedded content still makes periodic web requests. On a report, this could appear as if the user visited cnn, facebook and twitter and spent 15 minutes browsing each site.

While this is accurate, it can misrepresent the user's actions on reports that are reviewed by the Human Resources department, for example. The Barracuda Web Filter can make the distinction between such embedded requests – also known as “referred requests” – and actual user visits and distinguish them accordingly in the reports. Consequently, reports more accurately reflect user actions.

Session Time Versus Browse Time

Session time is the time calculated for each browsing session generated, with an idle timeout value of about 3 minutes. So if, for example, a user visits cnn.com, but doesn't click anything else for more than 3 minutes, that's one session of 3 minutes for that user on cnn.com. If the user did click around cnn.com within the 3 minute time frame, the session would continue to increase in length until there was a 3 minute idle time.

Browse time as shown in reports is the sum of all session times in a particular grouping (domain, category, user, etc).

For detailed descriptions of the system reports, see the online help for the **BASIC > Reports** page.

To clear traffic logs, see the **BASIC > Web Log** page.

Reporting 7.x

Some of the reports and features noted in this article are specific to the Barracuda Web Filter version 7.0 and higher.

In this article:

- [Report Set Grouped by Use Cases](#)
- [Accurately Reporting User Browsing Times](#)
 - [Session Time Versus Browse Time](#)
- [Clearing Traffic Logs](#)

Report Set Grouped by Use Cases

Use the **BASIC > Reports** page to choose from more than 50 different system reports that can help you keep track of activity performed by the Barracuda Web Filter. You can either generate a system report on-demand or configure the Barracuda Web Filter to automatically generate the system reports on an hourly, daily, weekly or monthly basis and email the reports to specific email addresses or send them to an FTP or SMB server.

Reports can be anchored on user activity, content or bandwidth usage and, in version 7.0 and higher, are grouped as follows:

For Human Resources, Teachers and Managers

These reports are user friendly, easy to read and provide the following critical information:

- **Productivity** reports reflecting user activity with social networking and other applications; for example:
 - Top Users by Browse Time on Gaming Sites
 - Top Social Networking Domains by Requests - may determine which domains you want to block, warn or monitor
 - Top YouTube Users by Bandwidth
 - Top Facebook Users by Browse Time
 - Top Users by Browse Time on Social Networking Sites
 - ... and many more
- **Safety and Liability** reports; for example:
 - Top Users by Requests to Intolerance and Hate Sites
 - Top Users by Requests to Anonymizer Sites - An anonymizer is a tool that attempts to make activity on the Internet untraceable. It is a proxy server computer that acts as an intermediary and privacy shield between a client computer and the rest of the Internet, hiding the client computer's identity (IP address).
 - Suspicious Keywords by Users - for detection of possible cyberbullying, mention of weapons,terrorism. See the **BLOCK/ACCEPT > Web App Monitor** page for details.

For IT, system administrators

These report types show infection activity, blocked virus downloads, bandwidth usage by time frame and many other system performance-related reports, such as:

- **Infection Activity** reports:
 - Malware Blocks – IP addresses from which requests were made to known spyware sites.
 - Virus Blocks – A list of blocked virus downloads during the specified time frame.
- **Web Activity** reports:
 - Session time, browse time by hour or time of day.
 - Popular IP addresses to which requests were made.
 - Categories (i.e. adult, gaming, leisure, etc.) by bandwidth, number of requests, browse time.
 - Users by session time, browse time.
- **Administrative** reports:
 - Audit Log for tracking logins and logouts to the web interface, as well as changes to the configuration by role.
 - Temporary Access Request Log – Log of activity by *Temporary Access Administrators* (teachers) who have been given credentials to request temporary access for their students to domains that are typically regulated by system administrators. See [Temporary Access for Education](#).
 - Temporary Access Requests by Domains, Users or Categories.
- **Network Activity**
 - TCP Connection Usage
 - Daily Bandwidth
 - Web Requests Log

For a complete list and detailed descriptions of the system reports, see the online help for the **BASIC > Reports** page.

Accurately Reporting User Browsing Times

Embedded web content is intelligently detected by the Barracuda Web Filter to maximize reporting accuracy. For example, a site such as **cnn.com** embeds requests to Facebook, Twitter, and other social networks. While a user visiting the news site might not explicitly click on any of the embedded links, the embedded content still makes periodic web requests. On a report, this could appear as if the user visited CNN, Facebook and Twitter and spent 15 minutes on each site.

While this is technically accurate, it can misrepresent the user's actions on reports that are reviewed by the Human Resources department, for example. The Barracuda Web Filter can make the distinction between such embedded requests – also known as “referred requests” – and actual user visits in most cases, but there are some limitations due to the behavior of some client applications. Consequently, reports reflect estimates of

actual user browse and session times.



Important

In calculating browse times, the Barracuda Web Filter uses the HTTP referer (sic) header to make the distinction between embedded requests and user visits. However, it is important to note that there are various client applications that limit the accuracy of calculating browse times. Here are several examples:

- Javascript that downloads assets from another site and may not set referal;
- iOS apps that request web assets and do not set the referal;
- Android apps that request web assets place the app package name in the referal.

Session Time Versus Browse Time

Session time is the time calculated for each browsing session generated, with an idle timeout value of about 3 minutes. So if, for example, a user visits cnn.com, but doesn't click anything else for more than 3 minutes, that's one session of 3 minutes for that user on cnn.com. If the user did click around cnn.com within the 3 minute time frame, the session would continue to increase in length until there was a 3 minute idle time.

Browse time as shown in reports is the sum of all estimated session times in a particular grouping (domain, category, user, etc).

Clearing Traffic Logs

To clear traffic logs, see the **BASIC > Web Log** page.

How to Set Up Alerts and SNMP Monitoring

Alerts and Notifications

Emailed System Alerts

Use the **BASIC > Administration** page to configure the Barracuda Web Filter to automatically email system alerts to the email addresses you specify. System alerts notify you when:

- Your Energize Update subscription is about to expire
- New virus definitions are available
- New firmware updates are available
- Your system is low on disk space
- The Barracuda Web Filter **Operating Mode** changes to *Safe Mode*.
- Threat Alerts

When any virus downloads or spyware downloads are detected in the HTTP data path, threat alerts can be sent to the email address(es) you specify in the **Email Notifications** section of the **BASIC > Administration** page.

Setting up SNMP Query, Alerts and Traps

While the Barracuda Web Filter will send email alerts to the **System Alerts Email Address** as specified on the **BASIC > Administration** page, these alerts are limited and do not include latency, inqueue sizes, and other system health information. To monitor more specific information on a Barracuda Web Filter, Barracuda Networks recommends using SNMP monitoring with an SNMP server. The Barracuda Web Filter 410 and higher offers the ability to monitor various settings via SNMP alerts or traps, including system statistics such as:

- System Load Averages (1m/5m/15m)
- Memory Utilization
- System Uptime
- Raid Status
- CPU idle times

To query the Barracuda Web Filter for these statistics via SNMP, you must do the following in the **SNMP Manager** section of the **BASIC > Administration** page:

1. Set **Enable SNMP** to Yes.
2. Enter the **SNMP Community String**.
3. Select the **SNMP Version**. The Barracuda Web Filter supports both SNMP version v2c and v3. Select version v3 for more secure transmission. Version v3 provides the following options for additional security (make sure that the settings you select are supported by your SNMP monitor):
 - Authentication methods MD5 or SHA, where SHA is the more secure method.
 - Encryption methods DES or AES, where AES is the more secure method.
4. Enter the IP address of the server that will be making the SNMP connection in the **Allowed SNMP and API IP/Range** section of the page. IP addresses entered in this field are allowed to access the Barracuda Web Filter via SNMP queries to retrieve error information, or via the API to configure the device.

You can configure SNMP traps by listing one or more IP addresses to which the Barracuda Web Filter has access for sending SNMP traps as configured by a client.

SNMP MIBs

Click to download the [Barracuda Web Filter SNMP MIB](#) and the [Barracuda Reference MIB](#). You can monitor objects included in these MIBs either from custom scripts or from your SNMP monitor.

Barracuda Reference MIB

Using SNMP monitoring with an SNMP server, you can monitor objects included in this MIB from your SNMP monitor. You can also use custom scripts. This MIB applies to all Barracuda products that support SNMP monitoring. See also your product-specific SNMP MIB.

```
Barracuda-REF DEFINITIONS ::= BEGIN

IMPORTS
    MODULE-IDENTITY, enterprises
        FROM SNMPv2-SMI;

barracuda MODULE-IDENTITY
    LAST-UPDATED "200906100000Z" -- June 10, 2009
    ORGANIZATION "Barracuda Networks, Inc."
    CONTACT-INFO
        "
        Barracuda Networks Inc.
        3175 S. Winchester Blvd.
        Campbell, CA 95008
        "
    DESCRIPTION
        "
        Main Barracuda MIB
        "
    ::= { enterprises 20632 } -- assigned by IANA

END
```

Barracuda Web Filter SNMP MIB

You can monitor objects included in this MIB either from custom scripts or from your SNMP monitor. See also [Barracuda Reference MIB](#).

Barracuda-SPYWARE DEFINITIONS ::=BEGIN

IMPORTS

MODULE-IDENTITY, OBJECT-TYPE, INTEGER

FROM SNMPv2-SMI

barracuda

FROM Barracuda-REF;

bspyware MODULE-IDENTITY

LAST-UPDATED "201011040000Z"

ORGANIZATION "Barracuda Networks, Inc."

CONTACT-INFO

"

Barracuda Networks Inc.

3175 S. Winchester Blvd.

Campbell, CA 95008

"

DESCRIPTION

"

Barracuda Web Filter MIB.

Provides:

Objects:

- * 1.3.6.1.4.1.20632.3.1.2 -- ActiveTCPConnections
- * 1.3.6.1.4.1.20632.3.1.3 -- Throughput
- * 1.3.6.1.4.1.20632.3.1.4 -- PolicyBlocks
- * 1.3.6.1.4.1.20632.3.1.5 -- SpywareWebHitBlocks
- * 1.3.6.1.4.1.20632.3.1.6 -- SpywareDownloadBlock
- * 1.3.6.1.4.1.20632.3.1.7 -- VirusDownloadBlock
- * 1.3.6.1.4.1.20632.3.1.8 -- SpywareProtocolBlocks
- * 1.3.6.1.4.1.20632.3.1.9 -- HTTPTrafficAllowed
- * 1.3.6.1.4.1.20632.3.1.10 -- system
 - * 1.3.6.1.4.1.20632.3.1.10.1 -- cpuFanSpeed
 - * 1.3.6.1.4.1.20632.3.1.10.2 -- systemFanSpeed
 - * 1.3.6.1.4.1.20632.3.1.10.3 -- cpuTemperature
 - * 1.3.6.1.4.1.20632.3.1.10.4 -- systemTemperature
 - * 1.3.6.1.4.1.20632.3.1.10.5 -- firmwareStorage
 - * 1.3.6.1.4.1.20632.3.1.10.6 -- logStorage
- * 1.3.6.1.4.1.20632.3.1.11 -- SystemUpTime

Traps:

- * 1.3.6.1.4.1.20632.3.2 -- traps
- * 1.3.6.1.4.1.20632.3.2.2 -- ActiveTCPConnectionsHigh
- * 1.3.6.1.4.1.20632.3.2.3 -- ThroughputHigh
- * 1.3.6.1.4.1.20632.3.2.4 -- cpuTempHigh
- * 1.3.6.1.4.1.20632.3.2.5 -- sysTempHigh
- * 1.3.6.1.4.1.20632.3.2.6 -- cpuFanDead
- * 1.3.6.1.4.1.20632.3.2.7 -- sysFanDead
- * 1.3.6.1.4.1.20632.3.2.8 -- firmwareStorageHigh
- * 1.3.6.1.4.1.20632.3.2.9 -- logStorageHigh
- * 1.3.6.1.4.1.20632.3.2.10 -- lanStatus
- * 1.3.6.1.4.1.20632.3.2.11 -- wanStatus

"

::= { barracuda 3 }

--

-- Objects

--

ActiveTCPConnections OBJECT-TYPE

SYNTAX INTEGER

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"Web Filter active tcp connections."

::= { bspyware 2 }

Throughput OBJECT-TYPE

SYNTAX INTEGER

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"Web Filter throughput."

::= { bspyware 3 }

PolicyBlocks OBJECT-TYPE

SYNTAX INTEGER

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"Web Filter policy blocks"

::= { bspyware 4 }

SpywareWebHitBlocks OBJECT-TYPE

SYNTAX INTEGER

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"Web Filter spyware web hit blocks"

::= { bspyware 5 }

SpywareDownloadBlock OBJECT-TYPE

SYNTAX INTEGER

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"Web Filter spyware download block"

::= { bspyware 6 }

VirusDownloadBlock OBJECT-TYPE

SYNTAX INTEGER

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"Web Filter virus download block"

::= { bspyware 7 }

SpywareProtocolBlock OBJECT-TYPE

SYNTAX INTEGER

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"Web Filter spyware protocol block"

::= { bspyware 8 }

HTTPTrafficAllowed OBJECT-TYPE

SYNTAX INTEGER

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"Web Filter HTTP traffic allowed"

::= { bspyware 9 }

system OBJECT-GROUP

OBJECTS {

cpuFanSpeed,

systemFanSpeed,

cpuTemperature,

systemTemperature,

logStorage,

firmwareStorage

}

STATUS current

DESCRIPTION

"System parameters."

::= { bspyware 10 }

cpuFanSpeed OBJECT-TYPE

SYNTAX Integer32

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"CPU fan speed in RPM."

::= { system 1 }

systemFanSpeed OBJECT-TYPE

SYNTAX Integer32

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"System fan speed in RPM."

::= { system 2 }

cpuTemperature OBJECT-TYPE

SYNTAX Integer32

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"CPU temperature in degrees Celsius."

::= { system 3 }

systemTemperature OBJECT-TYPE

SYNTAX Integer32

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"CPU temperature in degrees Celsius."

::= { system 4 }

firmwareStorage OBJECT-TYPE

SYNTAX Integer32

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"Firmware storage utilization in percentage."

::= { system 5 }

logStorage OBJECT-TYPE

SYNTAX Integer32

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"Log storage utilization in percentage."

::= { system 6 }

SystemUpTime OBJECT-TYPE

SYNTAX INTEGER

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"Web Filter system uptime."

::= { bspyware 11 }

--

-- Traps

--

bspywaretraps OBJECT IDENTIFIER ::= { bspyware 2 }

ActiveTCPConnectionsHigh NOTIFICATION-TYPE

STATUS current

DESCRIPTION

"Number of active tcp connections are high than threshold."

::= { bspywaretraps 2 }

ThroughputHigh NOTIFICATION-TYPE

STATUS current

DESCRIPTION

"Throughput is high."

::= { bspywaretraps 3 }

cpuTempHigh NOTIFICATION-TYPE

STATUS current

DESCRIPTION

"CPU temperature exceeded its threshold."

::= { bspywaretraps 4 }

sysTempHigh NOTIFICATION-TYPE

STATUS current

DESCRIPTION

"System temperature exceeded its threshold."

::= { bspywaretraps 5 }

cpuFanDead NOTIFICATION-TYPE

STATUS current

DESCRIPTION

"CPU fan is dead."

::= { bspywaretraps 6 }

sysFanDead NOTIFICATION-TYPE

STATUS current

DESCRIPTION

"System fan is dead."

::= { bspywaretraps 7 }

firmwareStorageHigh NOTIFICATION-TYPE

STATUS current

DESCRIPTION

"Firmware storage exceeded its threshold."

::= { bspywaretraps 8 }

logStorageHigh NOTIFICATION-TYPE

STATUS current

DESCRIPTION

"Log storage utilization exceeded its threshold."

::= { bspywaretraps 9 }

lanStatus NOTIFICATION-TYPE

STATUS current

DESCRIPTION

"Current LAN Status for web filter."

::= { bspywaretraps 10 }

wanStatus NOTIFICATION-TYPE

STATUS current

DESCRIPTION

"Current WAN Status for web filter."

::= { bspywaretraps 11 }

END

How to Set Up Barracuda Cloud Control

Barracuda Cloud Control enables administrators to manage, monitor and configure multiple Barracuda Web Filters (firmware version 4.3 and higher) at one time from one console. The same tabbed pages are available on Barracuda Cloud Control for managing all aspects of your Barracuda Web Filter configuration that you see in each individual web interface, and you can create aggregated reports for multiple devices from the Barracuda Cloud Control console. You can connect one or more Barracuda Web Filters to Barracuda Cloud Control by doing the following:

1. If you don't already have an account with Barracuda Networks, see [Create a Barracuda Cloud Control Account](#).
2. Make a note of your username (email address) and password.
3. Log into your Barracuda Web Filter as the administrator. From the **ADVANCED > Firmware Upgrade** page, check to make sure you have the latest firmware installed. If not, download and install it now.
4. From the **ADVANCED > Cloud Control** page, enter the Barracuda Networks username and password you created and click **Yes** to connect to Barracuda Cloud Control. Note that your Barracuda Web Filter can connect with only one Barracuda Cloud Control account at a time.
5. Log into Barracuda Cloud Control with your username and password and you will see your Barracuda Web Filter statistics displayed on the **BASIC > Status** page. To access the web interface of your Barracuda Web Filter, click on the link in the Products column in the **Appliance Control** Centerpane on the left side of the page. Or you can click on the product name in the Product column of the Unit Health pane on the right side of the page.
6. Follow steps 3 and 4 to connect every subsequent Barracuda Web Filter to Barracuda Cloud Control.

To disconnect your Barracuda Web Filter from Barracuda Cloud Control, from the **ADVANCED > Cloud Control** page, enter the Barracuda Cloud Control username and password and click **No** for **Connect to Barracuda Cloud Control**.

For details on using Barracuda Cloud Control, please see [Barracuda Cloud Control - Overview](#).

Troubleshooting

In this article:

- [Basic Troubleshooting Tools](#)
- [Connect to Barracuda Support Servers](#)
- [Rebooting the System in Recovery Mode](#)
- [Reboot options](#)
- [Replacing a failed system](#)
 - [Barracuda Instant Replacement Service](#)

Basic Troubleshooting Tools

The **ADVANCED > Troubleshooting** page provides various tools that help troubleshoot network connectivity issues that may be impacting the performance of your Barracuda Web Filter.

For example, you can test the connection between the Barracuda Web Filter to Barracuda Central to make sure it can successfully download the latest virus and spyware definitions. You can also ping or telnet to devices from the Barracuda system, perform a traceroute from the Barracuda system to a destination server, run a packet capture, and other tasks.

Connect to Barracuda Support Servers

In the Support Diagnostics section of the **ADVANCED > Troubleshooting** page, you can initiate a connection between your Barracuda Spam & Virus Firewall and the [Barracuda Networks Technical Support Center](#) which will allow technical support engineers to troubleshoot any issues you may be experiencing.

Rebooting the System in Recovery Mode

If your Barracuda Web Filter experiences a serious issue that impacts its core functionality, you can use diagnostic and recovery tools that are available at the reboot menu to return your system to an operational state.

Before you use the diagnostic and recovery tools, do the following:

- Use the built-in troubleshooting tools on the **ADVANCED > Troubleshooting** page to help diagnose the problem.
- Perform a system restore from the last known good backup file.
- Contact Barracuda Networks Technical Support for additional troubleshooting tips.

As a last resort, you can reboot your Barracuda Web Filter and run a memory test or perform a complete system recovery, as described in this

section.

To perform a system recovery or hardware test:

1. Connect a monitor and keyboard directly to your Barracuda Web Filter.
2. Reboot the system by doing one of the following:
 - In the web interface: Go to the **BASIC > Administration** page, navigate to the **System Reload/Shutdown** section, and click **Restart**.
 - At the front panel of the Barracuda Web Filter: Press the **Power** button on the front panel to turn off the system, and then press the **Power** button again to turn the system on.

The splash screen displays with the following three boot options:

Barracuda
Recovery
Hardware_Test

3. Use your keyboard to select the desired boot option, and press the **Enter** key.
You must select the boot option within three seconds after the splash screen appears. If you do not select an option within three seconds, the Barracuda Web Filter starts up in *Normal* mode (first option).
For a description of each boot option, refer to **Reboot Options** below.



To stop a hardware test, reboot your Barracuda Web Filter by pressing the Ctrl-Alt-Del keys.

Reboot options

The table below describes the options available at the reboot menu.

Reboot Options	Description
Barracuda	Starts the Barracuda Web Filter in the normal (default) mode. This option is automatically selected if no other option is specified within the first three seconds of the splash screen appearing.
Recovery	Displays the Recovery Console, where you can select the following options: <ul style="list-style-type: none">• Perform file system repair—Repairs the file system on XFS-based Barracuda Web Filter. Select this option only if the serial number on your Barracuda Web Filter is below 24364; otherwise select the Perform Full System Re-image option.• Perform full system re-image—Restores the factory settings on your Barracuda Web Filter and clears out the configuration information. Select this option if the serial number on your Barracuda Web Filter is 24364 or above.• Enable remote administration—Turns on reverse tunnel that allows Barracuda Networks Technical Support to access the system. Another method for enabling remote administration is to click Establish Connection to Barracuda Support Center on the ADVANCED > Troubleshooting page.• Run diagnostic memory test—Runs a diagnostic memory test from the operating system. If problems are reported when running this option, we recommend running the Hardware_Test option next.
Hardware_Test	Performs a thorough memory test that shows most memory related errors within a two-hour time period. The memory test is performed outside of the operating system and can take a long time to complete. Reboot your Barracuda Web Filter to stop the hardware test.

Replacing a failed system

Before you replace your Barracuda Web Filter, use the tools provided on the **ADVANCED > Troubleshooting** page to try to resolve the problem.

Barracuda Instant Replacement Service

In the event that a Barracuda Web Filter system fails and you cannot resolve the issue, customers that have purchased the Instant Replacement service can call t and receive a new unit within 24 hours.

After receiving the new system, ship the failed Barracuda Web Filter back to Barracuda Networks at the address below with an RMA number marked clearly on the package. Barracuda Networks can provide details on the best way to return the unit.

Barracuda Networks

3175 S. Winchester Blvd

Campbell, CA 95008

attn: RMA # <your RMA number>



To set up the new Barracuda Web Filter so it has the same configuration as your old failed system, restore the backup file from the old system onto the new system, and then manually configure the new system's IP information on the **BASIC > IP Configuration** page. For information on restoring data, refer to [How to Back Up and Restore Your System Configuration](#).

Syslog and the Barracuda Web Filter

In this article:

- [What is the Barracuda Syslog?](#)
- [Enabling Syslog](#)
- [Barracuda Syslog Format - New for Version 7.0 and Higher](#)
- [Syslog Examples](#)
- [Detailed Description](#)

What is the Barracuda Syslog?

The Barracuda Web Filter generates syslog messages as a means of logging both changes to the web interface configuration and what happens to each traffic request performed by your users. The syslog messages are stored in text file format on the Barracuda Web Filter and can be sent to a remote server configurable by the administrator. There are two syslog outputs you can monitor: the *Web Interface* syslog and the *Web Traffic* syslog.

This article describes each element of a syslog message so you can better analyze why your Barracuda Web Filter performs a particular action for each traffic request.

Enabling Syslog

To enable syslog reporting on your Barracuda Web Filter, log into the web interface and navigate to the **Advanced > Syslog** page. For both the Web Traffic Syslog and Web Interface Syslog, enter the IP address of the syslog server that you want to direct messages to. If you are running syslog on a UNIX machine, be sure to start the syslog daemon process with the “-r” option so that it can receive messages from sources other than itself. Windows users will have to install a separate program to use syslog because the Windows OS does not include syslog capabilities. **Kiwi Syslog** is a popular solution, but many others are available that are both free and commercial.

Syslog messages are, by default, sent to the standard syslog UDP port 514. However, if your syslog server blocks UDP and/or communicates via TCP protocol, the Barracuda Web Filter will transmit syslog data via TCP. If there are any firewalls between the Barracuda Web Filter and the server receiving the syslog messages, be sure that port 514 is open on the firewalls. The syslog messages arrive on the mail facility at the *debug* priority level. As the Barracuda Web Filter uses the syslog messages internally for its own message logging, it is not possible to change the facility or the priority level. For more information about where the syslog messages will be placed, refer to the documentation of your syslog server.

Barracuda Syslog Format - New for Version 7.0 and Higher

Each syslog message contains three types of information:

- Section 1: Basic Information
- Section 2: Transparent Proxy Information
- Section 3: Policy Engine Information

This section identifies each element of the syslog based on the following example:

```
Sep 19 17:07:07 Barracuda httpscan[3365]: 1158710827 1 10.1.1.8 172.27.72.27 text/html 10.1.1.8 http://www.sex.com/ 2704
3767734cc16059e52447ee498d31f822 ALLOWED CLEAN 2 1 0 1 3 - 1 adult 0 - 0 sex.com adult,porn ANON
```

? Unknown Attachment

The following table describe each element of a syslog message.

Field Name	Example	Description
Epoch Time	1158710827	Seconds since 1970, unix timestamp.
Src IP	10.1.1.8	IP address of the client.
Dest IP	172.27.72.27(72.32.54.242)	IP address for the page that was blocked by the Barracuda Web Filter.
Content Type	text/html	HTTP header designated content type.
Src IP	10.1.1.8	IP address of the client.
Destination URL	http://www.sex.com	The URL the client tried to visit.
Data Size	2704	The size of the content.
MD5 anchor	37...22	The anchor used for parsing. This information is not usually important.
Action	ALLOWED	<p>Action performed by the transparent proxy. The type of actions include:</p> <ul style="list-style-type: none"> • ALLOWED: Traffic was processed by the transparent proxy and no virus or spyware was detected. • BLOCKED: Traffic was blocked by the transparent proxy most likely because the proxy detected virus or spyware. • DETECTED: Another process detected outbound spyware activity.
Reason	CLEAN	<p>Reason for the action:</p> <ul style="list-style-type: none"> • CLEAN: Traffic does not contain any virus or spyware. • VIRUS: Traffic was blocked because it contains a virus. • SPYWARE: Traffic was blocked because it contained spyware.
Details (only for blocked traffic)	Stream=>Eicar-Test-Signature FOUND	The name of the virus or spyware that was detected in the blocked traffic.

Syslog Examples

Example 1. Clean, policy-allowed traffic

The following example shows a syslog message for clean traffic going to an allowed website (CNN.com). The term “clean” represents traffic that does not contain viruses or spyware.

```
Sep 19 17:06:59 Barracuda httpscan[3365]: 1158710819 1 10.1.1.8 64.236.16.139 image/gif 10.1.1.8 http://i.cnn.net/cnn/element/img/1.3/video/ab.middle.on.gif 1744 3767734cc16059e52447ee498d31f822 ALLOWED CLEAN 2 0 0 0 0 - 0 - 0 - 0 cnn.net news ANON
```

Example 2: Clean, policy-denied traffic

The following example shows “clean” traffic going to a website that is blocked by one of the Barracuda Web Filter policies. In this example, the website sex.com is blocked by the...

```
Sep 19 17:07:07 Barracuda httpscan[3365]: 1158710827 1 10.1.1.8 172.27.72.27 text/html 10.1.1.8 http://www.sex.com/ 2704 3767734cc16059e52447ee498d31f822 ALLOWED CLEAN 2 1 0 1 3 - 1 adult 0 - 0 sex.com adult,porn ANON
```

Example 3: Virus-infected traffic blocked by the Barracuda Web Filter

The following example shows traffic that has been blocked by the Barracuda Web Filter because the traffic contains a known virus.

```
Sep 19 17:08:00 Barracuda httpscan[3365]: 1158710880 1 10.1.1.8 127.0.0.1 - 10.1.1.8 http://www.eicar.org/download/eicar.com.txt 0 3767734cc16059e52447ee498d31f822 BLOCKED VIRUS stream=>Eicar-Test-Signature FOUND 2 0 0 0 0 - 0 - 0 - 0 eicar.org computing-technology ANON
```

Detailed Description

The following table describes each element of a syslog message.

Field Name	Example	Description
Epoch Time	1158710827	Seconds since 1970, unix timestamp.
Src IP	10.1.1.8	IP address of the client.
Dest IP	172.27.72.27(72.32.54.242)	IP address for the page that was blocked by the Barracuda Web Filter.
Content Type	text/html	HTTP header designated content type.
Src IP	10.1.1.8	IP address of the client.
Destination URL	http://www.sex.com	The URL the client tried to visit.
Data Size	2704	The size of the content.
MD5 anchor	37...22	The anchor used for parsing. This information is not usually important.
Action	ALLOWED	Action performed by the transparent proxy. The type of actions include: <ul style="list-style-type: none">• ALLOWED: Traffic was processed by the transparent proxy and no virus or spyware was detected.• BLOCKED: Traffic was blocked by the transparent proxy most likely because the proxy detected virus or spyware.• DETECTED: Another process detected outbound spyware activity.

Reason	CLEAN	Reason for the action: <ul style="list-style-type: none"> • CLEAN: Traffic does not contain any virus or spyware. • VIRUS: Traffic was blocked because it contains a virus. • SPYWARE: Traffic was blocked because it contained spyware.
Details (only for blocked traffic)	Stream=>Eicar-Test-Signature FOUND	The name of the virus or spyware that was detected in the blocked traffic.
Format Ver	2	The version of the policy engine output. The most current 3.0 firmware uses policy engine version 2.
Match flag	1	Whether an existing policy matched the traffic. 1=Yes and 0=No.
TQ flag	0	Whether the rule is time-qualified. For Example, during work hours 9am - 5pm. 1=Yes and 0=No.
Action Type	1	The action performed by the policy engine on this request: <ul style="list-style-type: none"> 0 : allowed 1 : denied 2 : redirected 3 : rewrote by add/set a new parameter in query 4 : rewrote by delete an existing parameter in query 5 : matched a rule and allowed but marked as monitored 6 : branched to another rule set.
Src Type	3	If matched by source, what is its type: <ul style="list-style-type: none"> 0 : always, matches any source 1 : group, matched by group id 2 : ipv4addr, matched by an Ipv4 address 3 : login, matched by login 4 : login any, matched any authenticated user 5 : min_score, matched due to minimum infection threshold breached.
Src Detail	-	Any detail related to the matched source.

Dst Type	1	<p>If matched by destination, what is its type?</p> <p>0 : always, matched any destination</p> <p>1 : category, matched a particular category</p> <p>2 : category any, matched any category</p> <p>3 : domain, matched due to domain or subdomain</p> <p>4 : mimetype, matched due to mime-type</p> <p>5 : spyware hit, matched due to spyware hit</p> <p>6 : uri path regex, matched URI path</p> <p>7 : uri regex, matched any part of the URI</p> <p>8 : application, matches an application characteristics</p>
Dst Detail	adult	Detail of the matched destination. In this case it is the first matched category, which is adult.
Spy Type	0	<p>If it is a spyware hit, what is its type:</p> <p>0: allow</p> <p>1: block</p> <p>2: infection</p>
Spy ID	-	The name of the spyware if matched due to spyware hit.
Infection Score	0	Weight of the infection. Currently, mostly 0.
Matched Part	sex.com	The part of the rule that matched.
Matched Category	adult,porn	The policy category that matched the traffic.
User Info	ANON	<p>User information:</p> <ul style="list-style-type: none"> • ANON: Anonymous, unauthenticated users • ldap: Username: LDAP user info • username: Non-LDAP user info (users created create in the admin interface).
Referer Domain	http://www.cnn.com/ www.cnn.com	(Version 7.0 and higher) If enabled, displays domain of referer. If disabled, displays a dash '-'. (Applies to version 7.0 and higher).
Referer Category	news	(Version 7.0 and higher) If enabled, displays the <i>category</i> to which the referer domain belongs. If disabled, displays a dash '-'. (Applies to version 7.0 and higher).

WSA Remote User Type	1	(Version 7.0 and higher) If traffic comes from a remote device, indicates whether it came from a Windows WSA client (wsa), a Macintosh WSA client (iwsa) or the Barracuda Safe Browser (an iOS device). (Applies to version 7.0 and higher). 0 : local traffic (not from a remote device) 1 : remote agent (wsa or iwsa) 2 : Barracuda Safe Browser
----------------------	---	--

Maintenance

In this article:

- [Release Notes and Updating the Barracuda Web Filter Firmware](#)
 - [Updating the Firmware of Linked Systems](#)
- [Updating the Spyware, Virus, Category, Application and Security Definitions](#)
- [Reloading, Restarting, and Shutting Down the System](#)

Release Notes and Updating the Barracuda Web Filter Firmware



Important

Before updating the firmware on your Barracuda Web Filter, Barracuda recommends reading the [Release Notes](#). For a description of new features in a release, see [What's New in the Barracuda Web Filter](#).

Use the **ADVANCED > Firmware Update** page to manually update the firmware version of the system or revert to a previous version. The only time you should revert back to an old firmware version is if you recently downloaded a new version that is causing unexpected problems. In this case, call [Barracuda Networks Technical Support](#) before reverting back to a previous firmware version.

Updating the Firmware of Linked Systems

If a system is part of a cluster, we recommend changing the system's **Mode** in the **Clustered Systems** section of the **ADVANCED > Linked Management** page to *Standby* before you upgrade its firmware, and then repeat this process on each system in the cluster. Once the firmware on each system has been upgraded, you can then change the mode on each system back to *Active*.

Changing a linked system to *Standby* mode before upgrading prevents a system on a more recent firmware version from trying to synchronize its configuration with a system on an earlier firmware version. If you have the latest firmware version already installed, the **Download Now** button on the **ADVANCED > Firmware Update** page is disabled.

Applying a new firmware version results in a temporary loss of service. For this reason, you should apply new firmware versions during non-business hours.

Updating the Spyware, Virus, Category, Application and Security Definitions

Use the **ADVANCED > Energize Updates** page to manually or automatically update your Barracuda Web Filter with the most current spyware, virus, category, application and security definitions. Barracuda Networks recommends that the **Automatic Updates** setting for your spyware and virus definitions be set to *On* so your Barracuda Web Filter receives the latest definitions as soon as new threats are identified by [Barracuda Central](#).

This should be one of settings the administrator configures in the initial installation of the Barracuda Web Filter.

Reloading, Restarting, and Shutting Down the System

Use the **System Reset/Shutdown** section on the **BASIC > Administration** page to shutdown, reset, and reload the Barracuda Web Filter. Shutting down the system powers off the unit. Restarting the system reboots the unit. Reloading the system re-applies the system configuration.

You can also reset the system by pressing the **RESET** button on the front panel of the system. The following actions occur:

- Reboots the system
- Resets the IP address if held down for 5 seconds or more. Do not press and hold the **RESET** button for longer than a few seconds – doing so changes the IP address of the system. Pushing and holding the **RESET** button for:
 - 5 seconds changes the IP address to the default of 192.168.200.200
 - 8 seconds changes the IP address to 192.168.1.200
 - 12 seconds changes the IP address to 10.1.1.200

How to Back Up and Restore Your System Configuration

Backing Up and Restoring Your System Configuration

The **ADVANCED > Backup** page lets you back up and restore the configuration of your Barracuda Web Filter. You should back up your system on a regular basis in case you need to restore this information on a replacement Barracuda Web Filter or in the event your current system data becomes corrupted.

If you are restoring a backup file on a new Barracuda Web Filter that is not yet configured, you first need to assign your new system an IP address and DNS information on the **BASIC > IP Configuration** page. Note the following about the backup file:

- **Do not edit backup files.** Any configuration changes you want to make need to be done via the web interface. The configuration backup file contains a checksum that prevents the file from being uploaded to the system if any changes are made.
- You can safely view a backup file in Windows WordPad or Microsoft Word. You should avoid viewing backup files in Windows Notepad because the file can become corrupted if you save the file from this application.
- The following information is not included in the backup file:
 - System password
 - System IP information
 - DNS information

Restoring a Backup

Restoring a backup simply requires browsing your local system with the click of a button on the **ADVANCED > Backup** page and selecting a backup file. Please see the online help on that page for details about restoring backups. Please note that restoring a backup will overwrite the current configuration.



Caution

Do not restore a configuration file onto a machine that is currently part of a cluster. All cluster information will be lost and the units will need to be re-clustered if this happens.

Web Use Categories

The Barracuda Web Filter URL filtering engine uses one of the most extensive content definition databases, covering some of the highest risk websites on the Internet.

The websites in the Barracuda Networks database are organized into 96 content categories (subcategories) which are grouped below by supercategories.

When you create rules that block categories of websites, you can choose a supercategory to block, or you can drill down and block websites at the subcategory level. See **Related Articles** listed at the end of this article for details.

Bandwidth

Websites delivering content that can use large amounts of network resources.

Category	Criteria
Streaming Media	Websites that provide streaming audio and video, or software and tools for streaming media.
Streaming Radio/TV	Websites that provide streaming radio or TV.

Advertisements & Popups	Websites that host or serve advertisements or provide software that serves advertisements.
Media Downloads	Websites that provide downloads of music and video content in any format.
Media Sharing	Websites that allow posting and sharing of music and video content in any format.

Commerce

Websites that contain business information or facilitate commercial transactions.

Category	Criteria
Auctions & Classifieds	Websites that allow bidding and selling of items and services. Does not include non-selling related advertising.
Business	Websites that provide business-related overview, planning and strategy information.
Finance & Investment	Websites that provide financial information or access to online banking.
Real Estate	Websites that provide residential and commercial property sales and rental information, listings and services.
Shopping	Websites that sell goods and services, but not marketing or ordering websites for single products.
Stock Trading	Websites that allow monitoring, purchase, or sale of stocks.

Communications

Websites that let users communicate through web browsers.

Category	Criteria
Chat	Websites that provide Web-based messaging and chat rooms, including IRC and social networking chat functions.
Peer-to-Peer	Websites that distribute file sharing software or allow the exchange of files between users.
Web-based Email	Websites that enable sending, reading and archiving of email.
Instant Messaging	Websites that provide instant messaging software such as instant messaging clients or chat clients that are not Web-based.
Messaging	Websites that allow users to send and receive messages, e.g. SMS, MMS, voice mail, or FAX.
Mobile Communications	Websites that provide support information for mobile communication devices.
Online Meetings	Websites that enable multiple users to interact transparently with each other through messaging, audio or video connections.
Web-based Telephony	Websites that enable voice communication over the Web.

Information

Websites that provide searching, general news and information, including business content.

Category	Criteria
Education & Reference	Websites that provide academic information about schools or education related topics.
Forums & Newsgroups	Websites containing user-generated Web logs, discussion forums or wikis.
Government & Legal	Websites maintained by domestic and foreign government and military agencies.
Health & Medicine	Websites that provide health and wellness material or information about health products and service providers.
Job Search & Career Development	Websites that enable users to search for job openings and career opportunities, either with specific companies or job boards.
Motor Vehicles	Websites containing information and marketing for cars, auto parts and services.
News	Websites that contain general news information on a local, national and international level.
Advocacy/NGO	Websites for groups that promote or defend specific causes.
Religion	Websites that include content related to spirituality, religion, and philosophy.

History

Websites providing historical content.

Category	Criteria
Moderated Forums	Websites monitored by an authority who can prevent posting of inappropriate material.
Political Issues	Websites that contain opinion and political information, groups and discussions.
Professional Networking	The subset of social networking websites which includes content intended exclusively for businesses or professionals.
Public Information	Websites allowing search and access of the public records of people or organizations.
Technical/Business Forums	Websites which allow discussions or posting of user-generated content related to business or technical development.
Usenet News	Websites providing access to Usenet news groups or other bulletin boards.

Leisure

Entertainment and personal websites that are normally not business-related.

Category	Criteria
Marketing & Merchandising	Websites that provide information about products and services not available on the Web.
Blogs & Wikis	Websites allowing users to post content, edit and re-post frequently.

Arts & Society & Culture	Websites that display art galleries, information about artists and ethnic and cultural heritage.
Comics & Humor & Jokes	Websites containing comical or funny content.
Entertainment	Websites providing information on theater arts, movies, concerts, tv, radio and other amusements, or about celebrities of those venues.
Food & Dining	Websites with information, reviews, and online ordering for restaurants, bars, and catering.
Game Playing & Game Media	Websites that provide video game information or enable the online playing of games.
Hobbies & Recreation	Websites dedicated to recreational activities and hobbies, or organizations and businesses dedicated to recreation, such as amusement parks.
Kids Sites	Websites that are family-oriented and geared toward children.
Personals & Dating	Websites that enable users to meet and interact with each other for the purposes of dating or making friends.
Social Networking	Websites that enable friends to interact and share information, but not for the purposes of dating.
Sports	Websites with information and news about amateur and professional sports.
Travel	Websites that provide information about travel destinations or allow online booking of travel plans.
Digital Cards	Websites that enable the sending and receiving of digital postcards and greeting cards.
Fashion & Beauty	Websites that provide information or products related to fashion and beauty.
Hosted Personal Pages	Websites which allow users to design and post personal websites.

Liability

Users may be committing crimes or exposing the organization to legal liability with these sites.

Category	Criteria
Criminal Activity	Websites that provide information on how to commit illegal activities, perpetrate scams or commit fraud.
Illegal Drugs	Websites that provide information on the manufacturing or selling of illegal drugs or prescription drugs obtained illegally.
Illegal Software	Websites that provide information about or downloads of pirated software.
Academic Cheating	Websites that advocate or assist plagiarism or provide or sell questionable educational material.

Propriety

Websites that are intended for mature or adult users only.

Category	Criteria
----------	----------

Text/Audio Only	Websites that contain text or audio only, but no pictures.
Adult Content	These websites include content intended for legitimate reproductive science and sexual development educational material.
Alcohol & Tobacco	Websites that promote or sell alcoholic beverages or tobacco products.
Gambling	Websites that provide gambling odds and information or allow online betting.
Intimate Apparel & Swimwear	Websites containing revealing images such as swimsuits and modeling, but not nudity.
Intolerance & Hate	Websites encouraging bigotry or discrimination.
Pornography	Any website that contains sexually suggestive, explicit or erotic content.
Tasteless & Offensive	Websites portraying horror or perverse content.
Violence & Terrorism	Websites encouraging, instructing, or portraying extreme violence to people or property.
Weapons	Websites that contain information about making, buying, or obtaining any sort of weapons.
Extremely Offensive	Websites containing content that is shocking, gory, perverse, or horrific in nature.
Gambling Related	Websites providing information or promoting services, techniques or accessories related to gambling.
Game/Cartoon Violence	Websites containing graphically violent animated content.
Historical Opinion	Websites dedicated to subjective analysis of historical events, especially partisan or agenda-driven analysis.
Incidental Nudity	Websites which include nude images because they are part of a broader category of art or education.
Nudity	Websites containing bare images of the human body which are not suggestive or explicit.
Profanity	Websites which contain excessive use of profanity or obscenities.

Security

Websites that are security risks or sources of malware, or that allow users to circumvent policies.

Category	Criteria
Hacking	Websites that contain instructions and information for how to commit fraud or steal information through computer security vulnerabilities.
Phishing & Fraud	Websites that are known to be distributed as links in phishing emails.
Proxies	Websites that enable users to hide their browsing destinations, IP address, or username to avoid detection and bypass Web filters.
Spam	Websites delivering unwanted or unsolicited electronic messages.
Spyware	Websites that are accessed from spam message clicks, which distribute programs to gather user information, or covertly send information to third party websites.

Proxy Utilities	Websites providing users with resources to help them avoid detection or bypass Web filters.
Information Security	Websites that provide information about protecting personal or business data.
Malicious Sites	Websites that provide or display content which intends harm to users or their computer systems.
Suspicious Sites	Suspect websites whose malicious intent cannot be confirmed.

Technology

Websites that allow users to access search engines, portals and various technologies.

Category	Criteria
Computing & Technology	Websites that provide technical support information, but not of a security nature.
Content Server	Includes domains that host websites of other types and are often sources of security threats.
Downloads	Websites that distribute copies of free and shared software.
Parked Sites	For sale or expired websites that display links or advertisements.
Visual Search	Websites that provide image searching and matching technology.
Search Engines & Portals	Websites that aggregate disparate information or allow users to search across large amounts of data.
Software/Hardware	Websites that provide access to software or hardware technology.
Interactive Web Applications	Websites that provide access to groupware or interactive conference rooms.
Online Services	Websites that provide access to Web-based services.
Online Storage	Websites that allow the uploading of files and backups for remote data storage.
Remote Access	Websites that provide access to resources from a remote locations.
Resource Sharing	Websites that allow posting and sharing of resources and downloads to a network of people.
Technical Information	Websites that provide information on technical details of technologies.
Translators	Websites that provide translation services.
URL Redirectors	Websites that automatically forward the user from the requested URL to another URL.

Related Articles

- [Creating Block and Accept Policies](#)
- [BLOCK/ACCEPT Order of Precedence - Barracuda Web Filter](#)

About the Barracuda Web Filter Hardware

In this article:

- Front Panel of the Barracuda Web Filter
 - Barracuda Web Filter 210
 - Barracuda Web Filter 310 and 410
 - Barracuda Web Filter 610
 - Barracuda Web Filter 810 and 910
- Back Panel of the Barracuda Web Filter
 - Barracuda Web Filter 210
 - Barracuda Web Filter 310 and 410
 - Barracuda Web Filter 610
 - Barracuda Web Filter 810 and 910
 - Barracuda Web Filter 1010

Front Panel of the Barracuda Web Filter

Figures 1-4 illustrate the front panels for each model.

Barracuda Web Filter 210

Figure 1: Barracuda Web Filter 210 Front Panel.

Note that the WAN and LAN ports are located on the back of the unit.



Barracuda Web Filter 310 and 410

Figure 2: Barracuda Web Filter 310 and 410 Front Panel as described in Table 1.

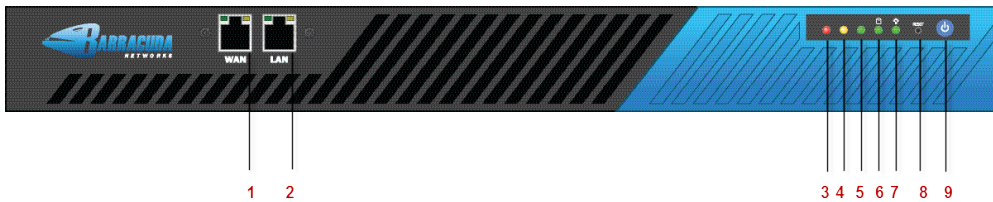


Table 1: Front Panel Descriptions for the Barracuda Web Filter models 210, 310 and 410.

Diagram Location	Component Name	Description
1	WAN port	Port for WAN Connection
2	LAN port	Port for LAN Connection
3	Spyware Activity	Blinks when the Barracuda Web Filter blocks installed spyware from accessing external sites
4	Spyware or Virus Downloads	Blinks when the Barracuda Web Filter blocks a virus or spyware application from being downloaded

5	Web Activity	Blinks when the Barracuda Web Filter processes traffic
6	Hard Disk	Blinks during disk activity
7	System Power	Displays a solid green light when the system is powered on
8	Reset Button	Resets the Barracuda Web Filter
9	Power Button	Powers the Barracuda Web Filter on or off

Barracuda Web Filter 610

Figure 3: Barracuda Web Filter 610 Front Panel as described in Table 2.

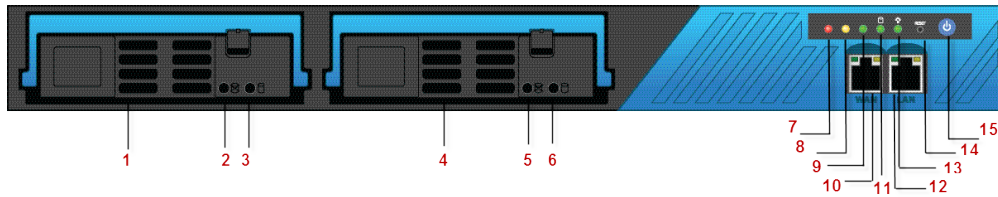


Table 2: Barracuda Web Filter 610 Front Panel Descriptions.

Diagram Location	Component Name	Description
1	Hard Disk Drive #1	Location of #1 disk drive
2	Hard Disk Drive Inactivity	Displays the hard disk is inactive
3	Hard Disk Drive Activity	Displays the hard disk drive is active
4	Hard Disk Drive #2	Location of #2 hard disk drive
5	Hard Disk Drive Inactivity	Displays the hard disk is inactive
6	Hard Disk Drive Activity	Displays the hard disk drive is active
7	Spyware Activity	Displays spyware activity
8	Spyware or Virus Downloads	Displays spyware or virus download activity
9	Internet Activity	Displays normal Internet activity
10	WAN port	Port for WAN connection
11	Hard Disk	Displays hard disk activity
12	System Power	Displays system power
12	LAN port	Port for LAN connection
14	Reset button	Resets the Barracuda Web Filter
15	Power button	Powers the Barracuda Web Filter on or off

Barracuda Web Filter 810 and 910

Figure 4: Barracuda Web Filter 810 and 910 Front Panel as described in Table 3.

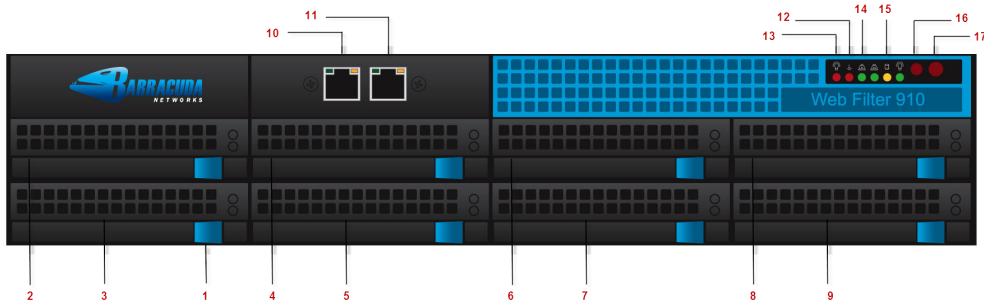


Table 3: Barracuda Web Filter 810 and 910 Front Panel Descriptions.

Diagram Location	Component Name	Description
1	Hard disk drive locks	Location of #1 disk drive
2	Hard Disk Drive #2	Location of #2 disk drive
3	Hard Disk Drive #3	Location of #3 disk drive
4	Hard Disk Drive #4	Location of #4 disk drive
5	Hard Disk Drive #5	Location of #5 disk drive
6	Hard Disk Drive #6	Location of #6 disk drive
7	Hard Disk Drive #7	Location of #7 disk drive
8	Hard Disk Drive #8	Location of #8 disk drive
9	Reset button	Resets the Barracuda Web Filter
10	WAN port	Port for WAN connection
11	LAN port	Port for LAN connection
12	Spyware Activity	Displays spyware activity
13	Spyware or Virus Downloads	Displays spyware or virus download activity
14	Web activity	Displays normal web traffic
15	Hard Disk	Displays hard disk activity
16	System Power	Displays system power
17	Power button	Powers the Barracuda Web Filter on or off

Back Panel of the Barracuda Web Filter

Figure 5, Figure 6, Figure 7 and and Figure 8 illustrate the back panels for each model.

Barracuda Web Filter 210

Figure 5: Barracuda Web Filter 210 Back Panel as described in Table 4.

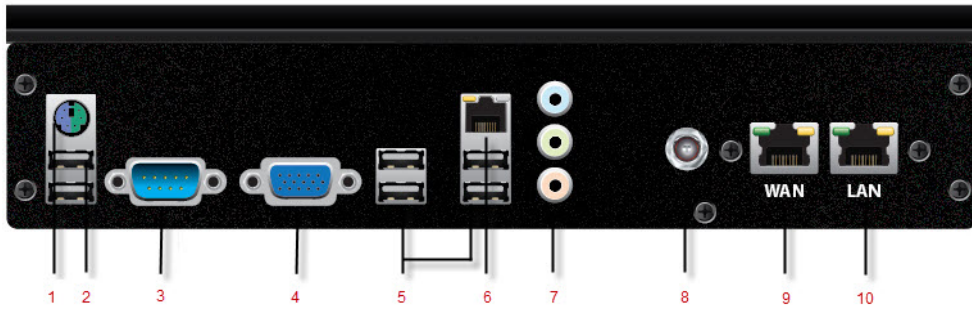


Table 4: Barracuda Web Filter 210 Back Component Descriptions.

Diagram Location	Component Name	Description
1	Keyboard port	Connection for the keyboard
2	USB ports (2)	Connection for USB devices
3	Serial port	Connection for the serial console cable
4	Monitor port	Connection for the monitor
5	USB ports (4)	Connection for USB devices
6	Auxiliary port	Connection for various deployments, Energize Update traffic
7	Not Used	Not used
8	Power	Connection for the AC power cord, standard power supply
9	WAN port	Port for WAN connection
10	LAN port	Port for LAN connection

Barracuda Web Filter 310 and 410

Figure 6: Barracuda Web Filter 310 and 410 Back Panel as described in Table 5.

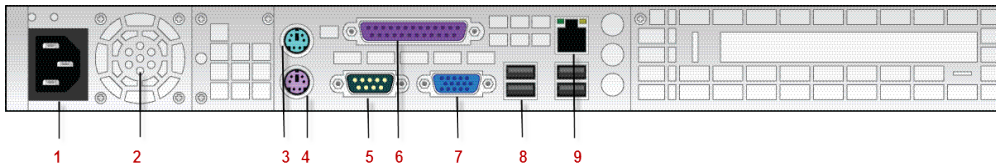


Table 5: Barracuda Web Filter 310 and 410 Back Component Descriptions.

Diagram Location	Component Name	Description
1	Power Supply	Connection for the AC power cord, standard
2	Fan	Location of the fan
3	Mouse port	Connection for the mouse
4	Keyboard port	Connection for the keyboard

5	Serial port	Connection for the serial console cable
6	Parallel Port	Connection for the parallel cable
7	Monitor Port	Connection for the monitor
8	USB ports (4)	Connection for USB devices
9	Auxiliary Port	Connection for various deployments, Energize Update traffic

Barracuda Web Filter 610

Figure 7: Barracuda Web Filter back panel as described in Table 6.

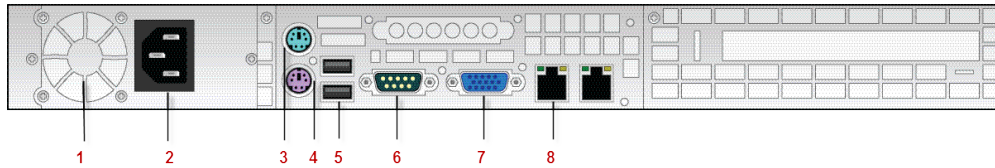


Table 6: Barracuda Web Filter 610 Back Component Descriptions.

Diagram Location	Component Name	Description
1	Fan	Location of the fan
2	Power Supply	Connection for the AC power cord, standard power supply
3	Mouse port	Connection for the mouse
4	Keyboard port	Connection for the keyboard
5	USB ports (2)	Connection for USB devices
6	Serial port	Connection for the serial console cable
6	Parallel Port	Connection for the parallel cable
7	Monitor Port	Connection for the monitor
8	Auxiliary Port	Connection for various deployments, Energize Update traffic

Barracuda Web Filter 810 and 910

Figure 8: Barracuda Web Filter 810 and 910 Back Panel as described in Table 7.

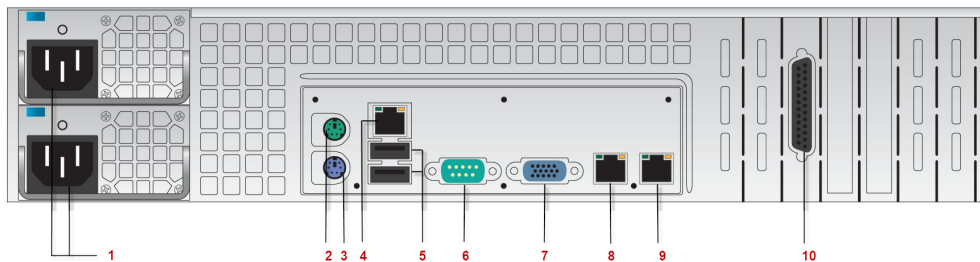


Table 7: Barracuda Web Filter 810 and 910 Back Component Descriptions.

Diagram Location	Component Name	Description
------------------	----------------	-------------

1	Power Supplies (2)	Connection for the AC power cord, standard power supply
2	Mouse port	Connection for the mouse
3	Keyboard port	Connection for the keyboard
4	Not used	Not used
5	USB ports (2)	Connection for USB devices
6	Serial port	Connection for the serial console cable
7	Monitor Port	Connection for the monitor
8	Auxiliary Port	Connection for various deployments, Energize Update traffic
9	Not used	Not used
10	Not used	Not used

Barracuda Web Filter 1010

Figure 9: Barracuda Web Filter 1010 Back Panel as described in Table 8.

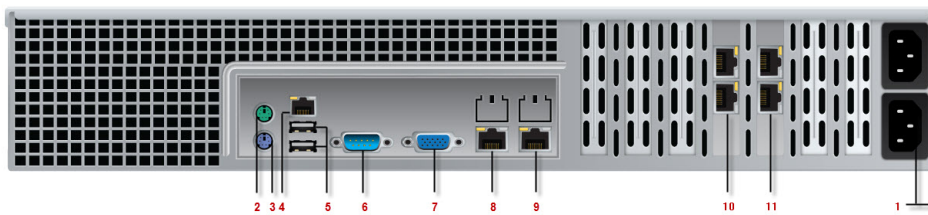


Table 8: Barracuda Web Filter 1010 Back Component Descriptions.

Diagram Location	Component Name	Description
1	Power Supplies (2)	Connection for the AC power cord, standard power supply
2	Mouse port	Connection for the mouse
3	Keyboard port	Connection for the keyboard
4	Not used	Not used
5	USB ports (2)	Connection for USB devices
6	Serial port	Connection for the serial console cable
7	Monitor Port	Connection for the monitor
8	Auxiliary Port	Connection for various deployments, Energize Update traffic
9	Not Used	Not Used
10	LAN2 / WAN2 Ports	Ports for LAN2, WAN2 connections
11	LAN1 / WAN1 Ports	Ports for LAN1, WAN1 connections

Related Articles

- [Hardware Compliance](#)

Hardware Compliance

This section contains compliance information for the appliance.



Notice for the USA

Compliance Information Statement (Declaration of Conformity Procedure) DoC FCC Part 15: This device complies with part 15 of the FCC Rules.

Operation is subject to the following conditions:

1. This device may not cause harmful interference, and
2. This device must accept any interference received including interference that may cause undesired operation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try one or more of the following measures:
 - Reorient or relocate the receiving antenna.
 - Increase the separation between the equipment and the receiver.
 - Plug the equipment into an outlet on a circuit different from that of the receiver.
 - Consult the dealer on an experienced radio/ television technician for help.

Notice for Canada

This apparatus complies with the Class B limits for radio interference as specified in the Canadian Department of Communication Radio Interference Regulations.



Notice for Europe (CE Mark)

This product is in conformity with the Council Directive 89/336/EEC, 92/31/EEC (EMC).

Power Requirements

AC input voltage 100-240 volts; frequency 50/60 Hz.

Limited Warranty and License

Limited Warranty

Barracuda Networks, Inc., or the Barracuda Networks, Inc. subsidiary or authorized Distributor selling the Barracuda Networks product, if sale is not directly by Barracuda Networks, Inc., ("Barracuda Networks") warrants that commencing from the date of delivery to Customer (but in case of resale by a Barracuda Networks reseller, commencing not more than sixty (60) days after original shipment by Barracuda Networks, Inc.), and continuing for a period of one (1) year: (a) its products (excluding any software) will be free from material defects in materials and workmanship under normal use; and (b) the software provided in connection with its products, including any software contained or embedded in such products will substantially conform to Barracuda Networks published specifications in effect as of the date of manufacture. Except for the foregoing, the software is provided as is. In no event does Barracuda Networks warrant that the software is error free or that Customer will be able to operate the software without problems or interruptions. In addition, due to the continual development of new techniques for intruding upon and attacking

networks, Barracuda Networks does not warrant that the software or any equipment, system or network on which the software is used will be free of vulnerability to intrusion or attack. The limited warranty extends only to you the original buyer of the Barracuda Networks product and is non-transferable.

Exclusive Remedy

Your sole and exclusive remedy and the entire liability of Barracuda Networks under this limited warranty shall be, at Barracuda Networks or its service centers option and expense, the repair, replacement or refund of the purchase price of any products sold which do not comply with this warranty. Hardware replaced under the terms of this limited warranty may be refurbished or new equipment substituted at Barracuda Networks option. Barracuda Networks obligations hereunder are conditioned upon the return of affected articles in accordance with Barracuda Networks then-current Return Material Authorization ("RMA") procedures. All parts will be new or refurbished, at Barracuda Networks discretion, and shall be furnished on an exchange basis. All parts removed for replacement will become the property of the Barracuda Networks. In connection with warranty services hereunder, Barracuda Networks may at its discretion modify the hardware of the product at no cost to you to improve its reliability or performance. The warranty period is not extended if Barracuda Networks repairs or replaces a warranted product or any parts. Barracuda Networks may change the availability of limited warranties, at its discretion, but any changes will not be retroactive. IN NO EVENT SHALL BARRACUDA NETWORKS LIABILITY EXCEED THE PRICE PAID FOR THE PRODUCT FROM DIRECT, INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES RESULTING FROM THE USE OF THE PRODUCT, ITS ACCOMPANYING SOFTWARE, OR ITS DOCUMENTATION.

Exclusions and Restrictions

This limited warranty does not apply to Barracuda Networks products that are or have been (a) marked or identified as "sample" or "beta," (b) loaned or provided to you at no cost, (c) sold "as is," (d) repaired, altered or modified except by Barracuda Networks, (e) not installed, operated or maintained in accordance with instructions supplied by Barracuda Networks, or (f) subjected to abnormal physical or electrical stress, misuse, negligence or to an accident.

EXCEPT FOR THE ABOVE WARRANTY, BARRACUDA NETWORKS MAKES NO OTHER WARRANTY, EXPRESS, IMPLIED OR STATUTORY, WITH RESPECT TO BARRACUDA NETWORKS PRODUCTS, INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTY OF TITLE, AVAILABILITY, RELIABILITY, USEFULNESS, MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NONINFRINGEMENT, OR ARISING FROM COURSE OF PERFORMANCE, DEALING, USAGE OR TRADE. EXCEPT FOR THE ABOVE WARRANTY, BARRACUDA NETWORKS PRODUCTS AND THE SOFTWARE IS PROVIDED "AS IS" AND BARRACUDA NETWORKS DOES NOT WARRANT THAT ITS PRODUCTS WILL MEET YOUR REQUIREMENTS OR BE UNINTERRUPTED, TIMELY, AVAILABLE, SECURE OR ERROR-FREE, OR THAT ANY ERRORS IN ITS PRODUCTS OR THE SOFTWARE WILL BE CORRECTED. FURTHERMORE, BARRACUDA NETWORKS DOES NOT WARRANT THAT BARRACUDA NETWORKS PRODUCTS, THE SOFTWARE OR ANY EQUIPMENT, SYSTEM OR NETWORK ON WHICH BARRACUDA NETWORKS PRODUCTS WILL BE USED WILL BE FREE OF VULNERABILITY TO INTRUSION OR ATTACK.

Software License

PLEASE READ THIS SOFTWARE LICENSE AGREEMENT ("AGREEMENT") CAREFULLY BEFORE USING THE BARRACUDA SOFTWARE. BY USING THE BARRACUDA SOFTWARE YOU ARE AGREEING TO BE BOUND BY THE TERMS OF THIS LICENSE. IF YOU DO NOT AGREE TO THE TERMS OF THIS LICENSE DO NOT USE THE SOFTWARE. IF YOU DO NOT AGREE TO THE TERMS OF THIS LICENSE YOU MAY RETURN THE SOFTWARE OR HARDWARE CONTAINING THE SOFTWARE FOR A FULL REFUND TO YOUR PLACE OF PURCHASE.

1. The software, documentation, whether on disk, in read only memory, or on any other media or in any other form (collectively "Barracuda Software") is licensed, not sold, to you by Barracuda Networks, Inc. ("Barracuda") for use only under the terms of this License and Barracuda reserves all rights not expressly granted to you. The rights granted are limited to Barracuda's intellectual property rights in the Barracuda Software and do not include any other patent or intellectual property rights. You own the media on which the Barracuda Software is recorded but Barracuda retains ownership of the Barracuda Software itself.
2. Permitted License Uses and Restrictions. This License allows you to use the Software only on the single Barracuda labeled hardware device on which the software was delivered. You may not make copies of the Software and you may not make the Software available over a network where it could be utilized by multiple devices or copied. You may not make a backup copy of the Software. You may not modify or create derivative works of the Software except as provided by the Open Source Licenses included below. The BARRACUDA SOFTWARE IS NOT INTENDED FOR USE IN THE OPERATION OF NUCLEAR FACILITIES, AIRCRAFT NAVIGATION OR COMMUNICATION SYSTEMS, LIFE SUPPORT MACHINES, OR OTHER EQUIPEMENT IN WHICH FAILURE COULD LEAD TO DEATH, PERSONAL INJURY, OR ENVIRONMENTAL DAMAGE.
3. You may not transfer, rent, lease, lend, or sublicense the Barracuda Software.
4. This License is effective until terminated. This License is automatically terminated without notice if you fail to comply with any term of the License. Upon termination you must destroy or return all copies of the Barracuda Software.

5. YOU EXPRESSLY ACKNOWLEDGE AND AGREE THAT THE USE OF THE BARRACUDA SOFTWARE IS AT YOUR OWN RISK AND THAT THE ENTIRE RISK AS TO SATISFACTION, QUALITY, PERFORMANCE, AND ACCURACY IS WITH YOU. THE BARRACUDA SOFTWARE IS PROVIDED "AS IS" WITH ALL FAULTS AND WITHOUT WARRANTY OF ANY KIND, AND BARRACUDA HEREBY DISCLAIMS ALL WARRANTIES AND CONDITIONS WITH RESPECT TO THE BARRACUDA SOFTWARE, EITHER EXPRESSED OR IMPLIED OR STATUTORY, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES AND/OR CONDITIONS OF MERCHANTABILITY, OF SATISFACTORY QUALITY, OF FITNESS FOR ANY APPLICATION, OF ACCURACY, AND OF NON-INFRINGEMENT OF THIRD PARTY RIGHTS. BARRACUDA DOES NOT WARRANT THE CONTINUED OPERATION OF THE SOFTWARE, THAT THE PERFORMANCE WILL MEET YOUR EXPECTATIONS, THAT THE FUNCTIONS WILL MEET YOUR REQUIREMENTS, THAT THE OPERATION WILL BE ERROR FREE OR CONTINUOUS, OR THAT DEFECTS WILL BE CORRECTED. NO ORAL OR WRITTEN INFORMATION GIVEN BY BARRACUDA OR AUTHORIZED BARRACUDA REPRESENTATIVE SHALL CREATE A WARRANTY. SHOULD THE BARRACUDA SOFTWARE PROVE DEFECTIVE, YOU ASSUME THE ENTIRE COST OF ALL NECESSARY SERVICING, REPAIR, OR CORRECTION.

6. License. YOU EXPRESSLY ACKNOWLEDGE AND AGREE THAT YOU WILL PROVIDE AN UNLIMITED ZERO COST LICENSE TO BARRACUDA FOR ANY PATENTS OR OTHER INTELLECTUAL PROPERTY RIGHTS UTILIZED IN THE BARRACUDA SOFTWARE WHICH YOU EITHER OWN OR CONTROL.

7. Limitation of Liability. TO THE EXTENT NOT PROHIBITED BY LAW, IN NO EVENT SHALL BARRACUDA BE LIABLE FOR PERSONAL INJURY OR ANY INCIDENTAL SPECIAL, INDIRECT, OR CONSEQUENTIAL DAMAGES WHATSOEVER, INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, LOSS OF DATA, BUSINESS INTERRUPTION, OR ANY OTHER COMMERCIAL DAMAGES OR LOSSES, ARISING OUT OF OR RELATED TO YOUR ABILITY TO USE OR INABILITY TO USE THE BARRACUDA SOFTWARE HOWEVER CAUSED, REGARDLESS OF THE THEORY OF LIABILITY AND EVEN IF BARRACUDA HAS BEEN ADVISED OF THE POSSIBILITY OF DAMAGES. In no event shall Barracuda's total liability to you for all damages exceed the amount of one hundred dollars.

8. Export Control. You may not use or otherwise export or re-export Barracuda Software except as authorized by the United States law and the laws of the jurisdiction where the Barracuda Software was obtained.

Energize Update Software License

PLEASE READ THIS ENERGIZE UPDATE SOFTWARE LICENSE CAREFULLY BEFORE DOWNLOADING, INSTALLING OR USING BARRACUDA NETWORKS OR BARRACUDA NETWORKS-SUPPLIED ENERGIZE UPDATE SOFTWARE.

BY DOWNLOADING OR INSTALLING THE ENERGIZE UPDATE SOFTWARE, OR USING THE EQUIPMENT THAT CONTAINS THIS SOFTWARE, YOU ARE CONSENTING TO BE BOUND BY THIS LICENSE. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THIS LICENSE, THEN (A) DO NOT DOWNLOAD, INSTALL OR USE THE SOFTWARE, AND (B) YOU MAY RETURN THE SOFTWARE FOR A FULL REFUND, OR, IF THE SOFTWARE IS SUPPLIED AS PART OF ANOTHER PRODUCT, YOU MAY RETURN THE ENTIRE PRODUCT FOR A FULL REFUND. YOUR RIGHT TO RETURN AND REFUND EXPIRES 30 DAYS AFTER PURCHASE FROM BARRACUDA NETWORKS OR AN AUTHORIZED BARRACUDA NETWORKS RESELLER, AND APPLIES ONLY IF YOU ARE THE ORIGINAL PURCHASER.

The following terms govern your use of the Energize Update Software except to the extent a particular program (a) is the subject of a separate written agreement with Barracuda Networks or (b) includes a separate "click-on" license agreement as part of the installation and/or download process. To the extent of a conflict between the provisions of the foregoing documents, the order of precedence shall be (1) the written agreement, (2) the click-on agreement, and (3) this Energize Update Software License.

License. Subject to the terms and conditions of and except as otherwise provided in this Agreement, Barracuda Networks, Inc., or a Barracuda Networks, Inc. subsidiary (collectively "Barracuda Networks"), grants to the end-user ("Customer") a nonexclusive and nontransferable license to use the Barracuda Networks Energize Update program modules and data files for which Customer has paid the required license fees (the "Energize Update Software"). In addition, the foregoing license shall also be subject to the following limitations, as applicable:

Unless otherwise expressly provided in the documentation, Customer shall use the Energize Update Software solely as embedded in, for execution on, or (where the applicable documentation permits installation on non-Barracuda Networks equipment) for communication with Barracuda Networks equipment owned or leased by Customer; Customer's use of the Energize Update Software shall be limited to use on a single hardware chassis, on a single central processing unit, as applicable, or use on such greater number of chassis or central processing units as Customer may have paid Barracuda Networks the required license fee; and Customer's use of the Energize Update Software shall also be limited, as applicable and set forth in Customer's purchase order or in Barracuda Networks' product catalog, user documentation, or web site, to a maximum number of (a) seats (i.e. users with access to the installed Energize Update Software), (b) concurrent users, sessions, ports, and/or issued and outstanding IP addresses, and/or (c) central processing unit cycles or instructions per second. Customer's use of the Energize Update Software shall also be limited by any other restrictions set forth in Customer's purchase order or in Barracuda Networks' product catalog, user documentation or web site for the Energize Update Software.

General Limitations. Except as otherwise expressly provided under this Agreement, Customer shall have no right, and Customer specifically agrees not to:

- i. transfer, assign or sublicense its license rights to any other person, or use the Energize Update Software on unauthorized or secondhand Barracuda Networks equipment, and any such attempted transfer, assignment or

- sublicense shall be void;
- ii. make error corrections to or otherwise modify or adapt the Energize Update Software or create derivative works based upon the Energize Update Software, or to permit third parties to do the same; or
 - iii. decompile, decrypt, reverse engineer, disassemble or otherwise reduce the Energize Update Software to human-readable form to gain access to trade secrets or confidential information in the Energize Update Software.

Upgrades and Additional Copies. For purposes of this Agreement, "Energize Update Software" shall include (and the terms and conditions of this Agreement shall apply to) any Energize Update upgrades, updates, bug fixes or modified versions (collectively, "Upgrades") or backup copies of the Energize Update Software licensed or provided to Customer by Barracuda Networks or an authorized distributor/reseller for which Customer has paid the applicable license fees. NOTWITHSTANDING ANY OTHER PROVISION OF THIS AGREEMENT: (1) CUSTOMER HAS NO LICENSE OR RIGHT TO USE ANY SUCH ADDITIONAL COPIES OR UPGRADES UNLESS CUSTOMER, AT THE TIME OF ACQUIRING SUCH COPY OR UPGRADE, ALREADY HOLDS A VALID LICENSE TO THE ORIGINAL ENERGIZE UPDATE SOFTWARE AND HAS PAID THE APPLICABLE FEE FOR THE UPGRADE; (2) USE OF UPGRADES IS LIMITED TO BARRACUDA NETWORKS EQUIPMENT FOR WHICH CUSTOMER IS THE ORIGINAL END USER PURCHASER OR LESSEE OR WHO OTHERWISE HOLDS A VALID LICENSE TO USE THE ENERGIZE UPDATE SOFTWARE WHICH IS BEING UPGRADED; AND (3) USE OF ADDITIONAL COPIES IS LIMITED TO BACKUP PURPOSES ONLY.

Energize Update Changes. Barracuda Networks reserves the right at any time not to release or to discontinue release of any Energize Update Software and to alter prices, features, specifications, capabilities, functions, licensing terms, release dates, general availability or other characteristics of any future releases of the Energize Update Software.

Proprietary Notices. Customer agrees to maintain and reproduce all copyright and other proprietary notices on all copies, in any form, of the Energize Update Software in the same form and manner that such copyright and other proprietary notices are included on the Energize Update Software. Except as expressly authorized in this Agreement, Customer shall not make any copies or duplicates of any Energize Update Software without the prior written permission of Barracuda Networks. Customer may make such backup copies of the Energize Update Software as may be necessary for Customer's lawful use, provided Customer affixes to such copies all copyright, confidentiality, and proprietary notices that appear on the original.

Protection of Information. Customer agrees that aspects of the Energize Update Software and associated documentation, including the specific design and structure of individual programs, constitute trade secrets and/or copyrighted material of Barracuda Networks. Customer shall not disclose, provide, or otherwise make available such trade secrets or copyrighted material in any form to any third party without the prior written consent of Barracuda Networks. Customer shall implement reasonable security measures to protect and maintain the confidentiality of such trade secrets and copyrighted material. Title to Energize Update Software and documentation shall remain solely with Barracuda Networks.

Indemnity. Customer agrees to indemnify, hold harmless and defend Barracuda Networks and its affiliates, subsidiaries, officers, directors, employees and agents at Customer's expense, against any and all third-party claims, actions, proceedings, and suits and all related liabilities, damages, settlements, penalties, fines, costs and expenses (including, without limitation, reasonable attorneys fees and other dispute resolution expenses) incurred by Barracuda Networks arising out of or relating to Customer's (a) violation or breach of any term of this Agreement or any policy or guidelines referenced herein, or (b) use or misuse of the Barracuda Networks Energize Update Software.

Term and Termination. This License is effective upon date of delivery to Customer of the initial Energize Update Software (but in case of resale by a Barracuda Networks distributor or reseller, commencing not more than sixty (60) days after original Energize Update Software purchase from Barracuda Networks) and continues for the period for which Customer has paid the required license fees. Customer may terminate this License at any time by notifying Barracuda Networks and ceasing all use of the Energize Update Software. By terminating this License, Customer forfeits any refund of license fees paid and is responsible for paying any and all outstanding invoices. Customer's rights under this License will terminate immediately without notice from Barracuda Networks if Customer fails to comply with any provision of this License. Upon termination, Customer must cease use of all copies of Energize Update Software in its possession or control.

Export. Software, including technical data, may be subject to U.S. export control laws, including the U.S. Export Administration Act and its associated regulations, and may be subject to export or import regulations in other countries. Customer agrees to comply strictly with all such regulations and acknowledges that it has the responsibility to obtain licenses to export, re-export, or import Energize Update Software.

Restricted Rights. Barracuda Networks' commercial software and commercial computer software documentation is provided to United States Government agencies in accordance with the terms of this Agreement, and per subparagraph "(c)" of the "Commercial Computer Software - Restricted Rights" clause at FAR 52.227-19 (June 1987). For DOD agencies, the restrictions set forth in the "Technical Data-Commercial Items" clause at DFARS 252.227-7015 (Nov 1995) shall also apply.

No Warranty. The Energize Update Software is provided AS IS. Customer's sole and exclusive remedy and the entire liability of Barracuda Networks under this Energize Update Software License Agreement will be, at Barracuda Networks option, repair, replacement, or refund of the Energize Update Software.

Renewal. At the end of the Energize Update Service Period, Customer may have the option to renew the Energize Update Service at the current list price, provided such Energize Update Service is available. All initial subscriptions commence at the time of sale of the unit and all renewals commence at the expiration of the previous valid subscription.

In no event does Barracuda Networks warrant that the Energize Update Software is error free or that Customer will be able to operate the Energize Update Software without problems or interruptions. In addition, due to the continual development of new techniques for intruding upon and attacking networks, Barracuda Networks does not warrant that the Energize Update Software or any equipment, system or network on which the Energize Update Software is used will be free of vulnerability to intrusion or attack.

DISCLAIMER OF WARRANTY. ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS, AND WARRANTIES INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTY OR CONDITION OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NONINFRINGEMENT, SATISFACTORY QUALITY OR ARISING FROM A COURSE OF DEALING, LAW, USAGE, OR TRADE PRACTICE, ARE HEREBY EXCLUDED TO THE EXTENT ALLOWED BY APPLICABLE LAW. TO THE EXTENT AN IMPLIED WARRANTY CANNOT BE EXCLUDED, SUCH WARRANTY IS LIMITED IN DURATION TO THE WARRANTY PERIOD. BECAUSE SOME STATES OR JURISDICTIONS DO NOT ALLOW LIMITATIONS ON HOW LONG AN IMPLIED WARRANTY LASTS, THE ABOVE LIMITATION MAY NOT APPLY TO YOU. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS, AND YOU MAY ALSO HAVE OTHER RIGHTS WHICH VARY FROM JURISDICTION TO JURISDICTION.

General Terms Applicable to the Energize Update Software License Disclaimer of Liabilities. IN NO EVENT WILL BARRACUDA NETWORKS BE LIABLE FOR ANY LOST REVENUE, PROFIT, OR DATA, OR FOR SPECIAL, INDIRECT, CONSEQUENTIAL, INCIDENTAL, OR PUNITIVE DAMAGES HOWEVER CAUSED AND REGARDLESS OF THE THEORY OF LIABILITY ARISING OUT OF THE USE OF OR INABILITY TO USE THE ENERGIZE UPDATE SOFTWARE EVEN IF BARRACUDA NETWORKS OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. In no event shall Barracuda Networks' liability to Customer, whether in contract, tort (including negligence), or otherwise, exceed the price paid by Customer. BECAUSE SOME STATES OR JURISDICTIONS DO NOT ALLOW LIMITATION OR EXCLUSION OF CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE ABOVE LIMITATION MAY NOT APPLY TO YOU.

This Energize Update Software License shall be governed by and construed in accordance with the laws of the State of California, without reference to principles of conflict of laws, provided that for Customers located in a member state of the European Union, Norway or Switzerland, English law shall apply. The United Nations Convention on the International Sale of Goods shall not apply. If any portion hereof is found to be void or unenforceable, the remaining provisions of the Energize Update Software License shall remain in full force and effect. Except as expressly provided herein, the Energize Update Software License constitutes the entire agreement between the parties with respect to the license of the Energize Update Software and supersedes any conflicting or additional terms contained in the purchase order.

Open Source Licensing

Barracuda products may include programs that are covered by the GNU General Public License (GPL) or other "open source" license agreements. The GNU license is re-printed below for your reference. These programs are copyrighted by their authors or other parties, and the authors and copyright holders disclaim any warranty for such programs. Other programs are copyright by Barracuda Networks.

GNU GENERAL PUBLIC LICENSE, (GPL) Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc. 51 Franklin St, Fifth Floor, Boston, MA 02110-1301 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public

License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

- a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.
- b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.
- c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

- a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
- b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
- c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed

(in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

one line to give the program's name and an idea of what it does.

Copyright (C) yyyy name of author

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 59 Temple Place - Suite 330, Boston, MA 02111-1307, USA.

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

Gnomovision version 69, Copyright (C) 19yy name of author Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type `show w'. This is free software, and you are welcome to redistribute it under certain conditions; type `show c' for details.

The hypothetical commands `show w' and `show c' should show the appropriate parts of the General Public License. Of course, the commands you use may be called something other than `show w' and `show c'; they could even be mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the program, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the program `Gnomovision' (which makes passes at compilers) written by James Hacker.

signature of Ty Coon, 1 April 1989

Ty Coon, President of Vice

This General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Library General Public License instead of this License.

Barracuda Products may contain programs that are copyright (c)1995-2005 International Business Machines Corporation and others. All rights reserved. These programs are covered by the following License:

"Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, provided that the above copyright notice(s) and this permission notice appear in all copies of the Software and that both the above copyright notice(s) and this permission notice appear in supporting documentation."

Barracuda Products may include programs that are covered by the BSD License: "Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation

and/or other materials provided with the distribution.

The names of the authors may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED ``AS IS'' AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE."

Barracuda Products may include the libspf library which is Copyright (c) 2004 James Couzens & Sean Comeau All rights reserved. It is covered by the following agreement: Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met: 1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer. 2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution. THIS SOFTWARE IS PROVIDED ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHORS MAKING USE OF THIS LICENSE OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Barracuda Products may contain programs that are Copyright (c) 1998-2003 Carnegie Mellon University. All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met: 1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer. 2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution. The name "Carnegie Mellon University" must not be used to endorse or promote products derived from this software without prior written permission. For permission or any other legal details, please contact Office of Technology Transfer Carnegie Mellon University 5000 Forbes Avenue Pittsburgh, PA 15213-3890 (412) 268-4387, fax: (412) 268-7395 tech-transfer@andrew.cmu.edu .Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes software developed by Computing Services at Carnegie Mellon University (<http://www.cmu.edu/computing/>)." CARNEGIE MELLON UNIVERSITY DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS, IN NO EVENT SHALL CARNEGIE MELLON UNIVERSITY BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Barracuda products may include programs that are covered by the Apache License or other Open Source license agreements. The Apache license is re-printed below for you reference. These programs are copyrighted by their authors or other parties, and the authors and copyright holders disclaim any warranty for such programs. Other programs are copyright by Barracuda Networks.

Apache License
Version 2.0, January 2004
<http://www.apache.org/licenses/>

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

(a) You must give any other recipients of the Work or Derivative Works a copy of this License; and

(b) You must cause any modified files to carry prominent notices stating that You changed the files; and

(c) You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

(d) If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License.

You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by

applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

APPENDIX: How to apply the Apache License to your work.

To apply the Apache License to your work, attach the following boilerplate notice, with the fields enclosed by brackets "[]" replaced with your own identifying information. (Don't include the brackets!) The text should be enclosed in the appropriate comment syntax for the file format. We also recommend that a file or class name and description of purpose be included on the same "printed page" as the copyright notice for easier identification within third-party archives.

Copyright [yyyy] [name of copyright owner]

Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License. You may obtain a copy of the License at

<http://www.apache.org/licenses/LICENSE-2.0>

Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.

Source Code Availability

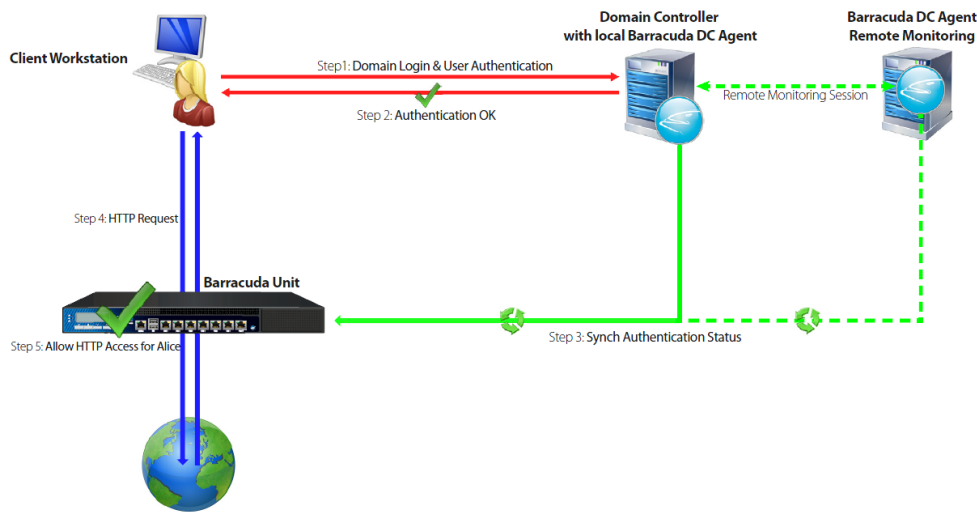
Per the GPL and other "open source" license agreements the complete machine readable source code for programs covered by the GPL or other "open source" license agreements is available from Barracuda Networks at no charge. If you would like a copy of the source code or the changes to a particular program we will gladly provide them, on a CD, for a fee of \$100.00. This fee is to pay for the time for a Barracuda Networks engineer to assemble the changes and source code, create the media, package the media, and mail the media. Please send a check payable in USA funds and include the program name. We mail the packaged source code for any program covered under the GPL or other "open source" license.

About the Barracuda DC Agent

For system requirements and information on how to get the latest version of the Barracuda DC Agent, see [How to Get and Configure the Barracuda DC Agent](#).

You can install the Barracuda DC Agent either on the domain controller or on a dedicated Windows PC on the office network. The Barracuda DC Agent periodically checks the domain controller for login events and to obtain a record of authenticated users. The IP addresses of authenticated users are mapped to their username and group context. The list of authenticated users is provided to the Barracuda Session Manager on your Barracuda Networks product, allowing true single sign-on capabilities.

A typical use case scenario: Alice comes into her office in the morning and logs into her workstation. She enters her user credentials and is authenticated by the domain controller. The Barracuda DC Agent recognizes that Alice has authenticated herself within the corporate network domain and forwards this information to all connected Barracuda Networks products. These systems now give Alice access to services or network areas for which a valid user or Microsoft Active Directory group context is required. Alice does not need to re-enter any credentials because her initial authentication by Active Directory is reused.



Exclusions

The Barracuda DC Agent lets you manually exclude IP addresses of user client PCs or known multi-user computer systems and provides a "learning mode" that proposes the exclusion of suspicious systems. Due to the complexity of today's network environments and multi-user computer systems, a user-to-IP association is not always possible or required. For example, you can exclude the HTTP Proxy and Terminal Server because they allow multiple users and use a single IP address for authentication against domain controllers.

Remote Monitoring

If you install the Barracuda DC Agent on a dedicated computer system instead of the Active Directory server, you can also remotely monitor Active Directory.

Logs

The Barracuda DC Agent logs activity to a file named *DCAgent.log* in the system temp directory, i.e.

%tmp%DcAgent.log

How to Get and Configure the Barracuda DC Agent

In this article:

- System Requirements
- Get and Install the Barracuda DC Agent Version 7.x
- Configure the Barracuda DC Agent
- How to Create a User with WMI Query Permission (optional)
 - Step 1. MS Windows 7 and Windows Server 2008 Configuration
 - Step 2. Windows Firewall Configuration
 - Step 3. Configure DCOM Access
- DC Agent Logging
- Configure your Barracuda Networks Product

Related Articles

- Using the Barracuda DC Agent with Microsoft Network Policy Server
- About the Barracuda DC Agent

System Requirements

Before configuring the Barracuda DC Agent, make sure that your system meets the following requirements:

- Local Installation - Microsoft Windows Server 2008, 2008R2 or 2012. Windows Server Core is not supported for local installation and monitoring. The DC Agent can, however, communicate with a domain controller that is running Windows Server Core.
- Remote Installation - Microsoft Windows 2008 and higher. Also note that, for the remote installation of DC Agent, you MUST be a domain member to query the server.

Get and Install the Barracuda DC Agent Version 7.x

You can install the Barracuda DC Agent directly on the domain controller or on a dedicated Windows PC within your network environment. To monitor wireless device logins using Windows Network Policy Server (NPS) log events, see [Using the Barracuda DC Agent with Microsoft Network Policy Server](#).

For the Barracuda Web Filter:

1. Log into the web interface as *admin* and download the Barracuda DC Agent from the **USERS > Authentication** page using the **Barracuda DC Agent (Download/Install)** link at the bottom of the screen.
2. Launch the installation file (DCAgent.exe) and follow the instructions in the wizard.

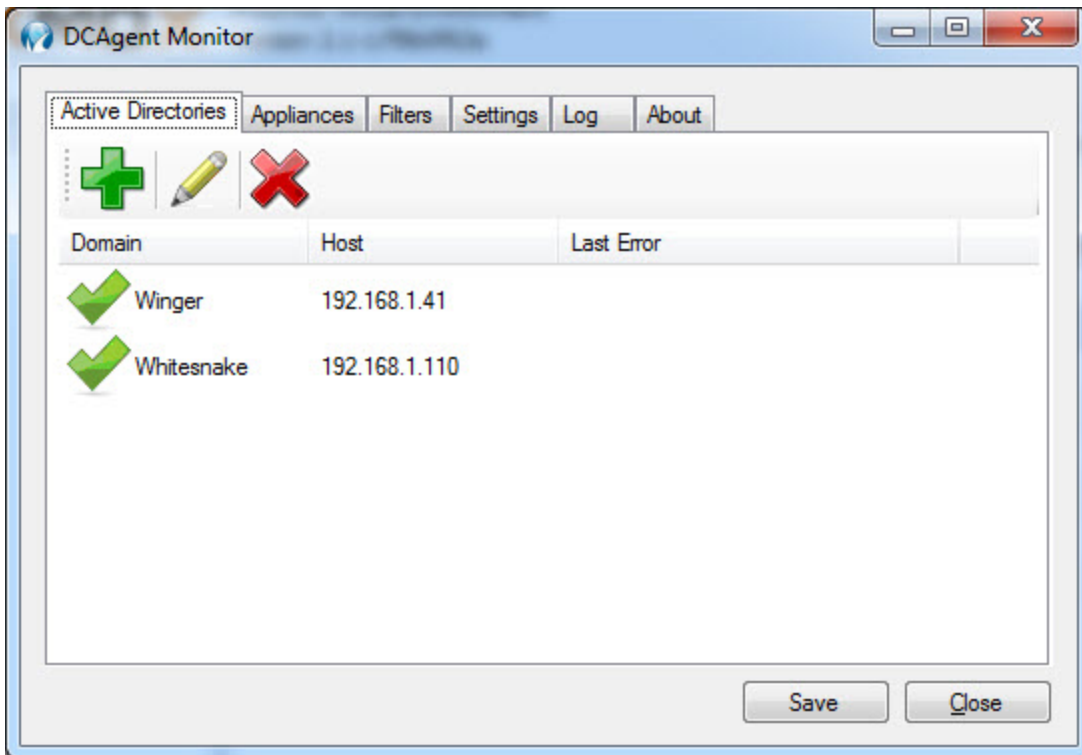
For the Barracuda NG Firewall:

1. Get the Barracuda DC Agent from your [Barracuda Cloud Control Account](#).
2. While logged into your account, go to the **Support > Downloads** page.
3. From the **Product** list, select **Barracuda NG Firewall**.
4. Select **Fulltext**, enter **Barracuda DC Agent**, and then click **Search**.
5. Download the latest Barracuda DC Agent version that is compatible with your system.
6. Launch the installation file and follow the instructions in the wizard.
7. Confirm that **Logon Events** are monitored by your domain controller:
 - a. Open **Domain Controller Security Policy (Start > Programs > Administrative Tools)**.
 - b. Click **Local Policies**.
 - c. For **Audit account logon events** and **Audit logon events**, make sure that the **Policy Settings** column displays **Success**.

Configure the Barracuda DC Agent

After the Barracuda DC Agent is installed and running correctly, launch the application and complete the following steps. **Note:** Your entries in the DC Agent interface will NOT be saved until you click the **Save** button.

1. Define location and login credentials for your Active Directory. Click the **Active Directories** tab and click the green + sign to add a domain.
 - a. Select **Local** if you installed the DC Agent on the Domain Controller; select **Remote** if you installed on another machine on the network.
 - b. If you selected **Remote**, enter the Fully Qualified Domain Name (FQDN) in the **Host** field.
 - c. Enter a name for referring to the domain, e.g. 'Finance', 'Salesnet', etc.
 - d. The **Username** should be associated with permissions to run WMI queries on the domain controller. Enter that user's **Password** and click **OK**.
 - e. Click **Test** to verify connectivity with the domain controller.



2. Add the **internal IP Address** and a **Description** for each Barracuda Networks appliance (Barracuda Web Filter, NG Firewall, etc. - hardware or virtual) with which you want to use the DC Agent.
3. On the **Filters** tab, specify the **IP Address** for any client PCs or networks for which you don't want the DC Agent to capture and send login information to your Barracuda Networks products. These are exceptions and associated login events will be ignored by the DC Agent.
4. On the **Settings** tab, configure the following:
 - **Appliance Listening Port** - If required, you can change the TCP listening port. Make sure that you also specify the same port on all configured Barracuda Networks products. Default is port 5049.
 - **Debug Log Level:**
 - 0 = log errors only
 - 1 = informational
 - 2 = verbose (most information logged)
 - **Group Options** (Barracuda NG Firewall only) - select which option best fits your logging requirements. If group information is required for authenticated users, select one of these group name types.
 - **Cache groups for:** Amount of time, in minutes, to allow the DC Agent to rely on cached login information. Since users will most likely log in once/workday, the default time is 480 minutes, or 8 hours. The shorter this time is, the more often the DC Agent will retrieve login event information from the domain controller and pass it to the Barracuda Networks product, which requires more processing overhead.

How to Create a User with WMI Query Permission (optional)

The Barracuda DC Agent must have certain permissions if you want it to perform WMI queries to identify user logon events. You can also install the DC Agent on a different Windows machine to provide remote monitoring of WMI events.

A normal account can be used for remote WMI access. This account can be restricted with no-login access but needs certain read-only rights to access the WMI repository remotely. The following attributes need to be configured:

- The user needs to have DCOM access. This is used to execute the WMI queries.
- The user needs access to the WMI tree (or at least the "root/CIMV2" portion of the tree).
- For performance monitoring, the user needs to be in the group "Performance Monitor Users".

The easiest configuration method is to create a user and add the user to the groups **Distributed COM Users** and **Performance Monitor Users**. By default, the group **Distributed COM Users** has remote access rights to the DCOM. The group **Performance Monitor Users** has rights to read the performance counts by default as well.

Step 1. MS Windows 7 and Windows Server 2008 Configuration

1. Create a normal user via the **Active Directory Users and Computers** tool.
2. Add the created user to the groups **Performance Monitor Users** and **Distributed COM Users** under **Builtin**.
3. Open a command prompt window and execute the `wmicmgmt.msc` command.
4. Select the **Properties** of **WMI Control (local)**.
5. Select the **Security** tab.
6. Select **Root** and click the **Security** button.
7. Add the group **Performance Monitor Users**.
8. Enable all **Remote Enable**, **Execute Methods**, **Enable Account** and all read rights.
9. Close the add dialog and select the group **Performance Monitor Users** in the list.
10. Select **Advanced** in the **Security for Root** dialog and then select the group and press **Edit**.
11. Select **This namespace and subnamespaces** to grant read-only access to the whole WMI tree to this account.

Step 2. Windows Firewall Configuration

If the MS Windows Firewall blocks remote WMI access, perform the following steps:

1. Start the Windows Firewall using the Control Panel. It is not necessary to use the Windows Firewall with Advanced Security control.
2. Select **Allow a program or feature** through Windows Firewall.
3. Open **Component Services > Computers > My Computer** and then **Properties** of My Computer.
4. Enable **Windows Management Instrumentation (WMI) for Domain and/or Home/Work Networks**.

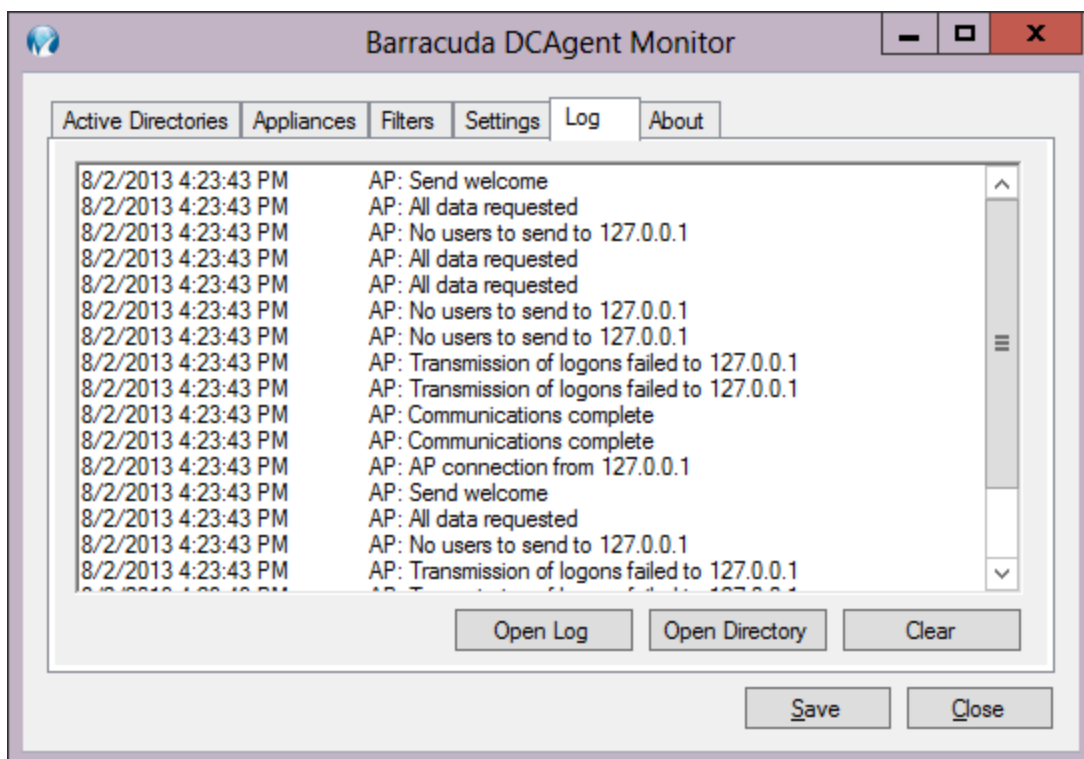
Step 3. Configure DCOM Access

Optional if the predefined group **Distributed COM Users** is not used.

1. Start `dcomcnfg.exe`
2. Open **Component Services > Computers > My Computer** and then **Properties of My Computer**.
3. Select **COM Security**.
4. Click on **Edit Limits on Launch and Activation Permissions**.
5. Check the rights of the group **Distributed COM Users** (should have full rights) .

DC Agent Logging

Typically you'll only need the Log upon first install of the DC Agent to make sure everything is working as expected. Note that, if you were previously running another version of the DC Agent, that data logged while the old agent was running will no longer show in the user interface log window. That data is still, however, in the database and will appear in reports as usual. To monitor wireless device logins using Windows Network Policy Server (NPS) log events, see [Using the Barracuda DC Agent with Microsoft Network Policy Server](#).



Configure your Barracuda Networks Product

To ensure that your Barracuda Web Filter or Barracuda NG Firewall can communicate with the Barracuda DC Agent, you must configure the product as well.

- For the Barracuda Web Filter, see the online help on the **USERS > Authentication** page in the web interface.
- For the Barracuda NG Firewall, see [How to Configure the MSAD DC Client](#).

How to Use the Barracuda Malware Removal Tool

The Barracuda Malware Removal Tool performs a comprehensive scan of your computer for any traces of spyware or other malware. This scan is very thorough and takes several minutes to complete. After the analysis is complete, you can remove all the malware and traces of malware that have been found.

The Barracuda Malware Removal Tool detects and removes many small traces, cookies, potential spyware files, and temporary files from your computer. Although these files are normally harmless, removing them can cause some websites to malfunction, and it is generally not appropriate that the Barracuda Web Filter block them at the network level. As such, the Barracuda Malware Removal Tool may identify potential files for removal from your computer that are not blocked at the network level by the Barracuda Web Filter.

For maximum security, complete removal of these files from your computer is recommended.

Use the **Infection Warning Threshold** field to configure whether your users are prompted to run the Barracuda Malware Removal Tool when spyware is detected on their system. By default, the Barracuda Malware Removal Tool is enabled.

Barracuda recommends that you keep the **Infection Warning Threshold** field set to **0** in Network Address Translation (NAT) environments because the Barracuda Web Filter uses the IP address to identify an infected system. As a result, if one system becomes infected with spyware, then all systems in the NAT environment are prompted to use the Barracuda Malware Removal Tool regardless of their infection status. This issue can occur when you deploy the Barracuda Web Filter with a pre-existing proxy server.

Enabling the Barracuda Malware Removal Tool

To enable users to run the Barracuda Malware Removal Tool:

1. From the **BLOCK/ACCEPT > Configuration** page, click **Yes** for the **Enable Removal Tool** setting in the **Infected Client Warning** section.

2. Clear the Infection Activity log so users are not prompted to run the Barracuda Malware Removal Tool based on old infection activity data or false positives. To clear the log, go to the **BASIC > Infection Activity** page and click Clear All.
3. On the **BLOCK/ACCEPT > Configuration** page, enter a value greater than **0** in the **Infection Warning Threshold** field. When the number of infection activities on a user's system exceeds the value of this field, the user is prompted to run the Barracuda Malware Removal Tool. The user can then select to run the tool immediately or postpone running the tool until the following day.
4. (Optional) Create a dedicated fully qualified hostname for the Barracuda Malware Removal Tool:
 - a. In the **Dedicated Removal Tool Hostname** field, enter a custom fully qualified hostname for the tool.
 - b. Add the custom hostname to your DNS server with the following resolving IP address: 172.27.72.27.
5. Click **Save Changes**.