

# Technology @ a Glance

*This is NOT a complete list of all Patronus™ features.*

## Internet Filtering

### Dynamic URL Categorization

- Utilizes a filter with over 25 million sites grouped in 96 categories that can be permitted or blocked.

### Real Time Proxy Detection

- Offers dynamic blocking of proxy servers based on analysis of network traffic.

### SafeSearch Mode

- Enforces SafeSearch settings on a network-wide basis—regardless of the user’s browser settings.

### Filtering for Google™ and Bing® Images and Cached Searches

- Applies web content filtering policies to image searches by examining the destination of the image thumbnails, further protecting users from inappropriate content that is otherwise difficult to detect.

### File & Extension Blocking

- Filters web content by file types.

### Granular Website Control

- Permits overriding broad categories of sites while also providing the ability to allow or block specific sites—down to the page level. For more granular control, sites are categorized in multiple categories. If a site is blocked in one category, but allowed in another, a “trust” setting is available to always allow the site.

### Streaming Media Blocking

- Blocks streaming media while allowing focused media content.

### Instant Messenger Blocking

- Blocks most popular types of instant messenger clients on a profile basis.

### Flexible User Discretion

- Allows permission or discretion to be provided to profile managers to override sites within specific website categories.

### Kids Zone Web Library™

- Directs children to an online library of educator-selected sites.

### Instant Override

- Opens access for a specified time period.

## YouTube Filtering

### Supports YouTube for Schools\*

- Focuses students on the YouTube EDU videos found on youtube.com/education plus any videos added by your library.
- Enables librarians to add their own playlists of videos.
- Removes comments and suggested videos.

\* YouTube does not currently support the use of YouTube for Schools on iOS devices.

## Anywhere Filter™

### Mobile Filtering

- Enforces your policy on your mobile devices when used off-network. Works with iPad®, iPhone®, and iPod touch® devices using iOS (6 or later); OS X® (10.6 or later); Windows® 8.1/8/7/Vista/XP and Chromebook™ notebooks and Chromebox™ devices.
- Filters Chromebook notebooks and Chromebox devices using Patronus’s Anywhere Filter cloud deployment.

### Global Proxy Support

- Filters iOS devices using the Safari® browser.

### Protection from Public WiFi Signals and Personal Hotspots

- Prevents anyone using your mobile devices from dodging your filter through public WiFi or personal hotspots.

### Secures Staff Laptops

- Protects your network by securing your mobile devices from malware and phishing sites.

## Integrated Firewall

### Predefined Rules

- Allows the quick setup of firewall rules for many popular applications and protocols, all without understanding the details of each protocol.

### VPN Pass-Through

- Supports the definition of VPN pass-through rules for popular VPN protocols, such as IPSec, PPTP, and L2TP.

### Locked Down by Default

- Restricts all communication in or out of a network. Explicit definitions to selectively permit access helps to manage a network and bandwidth.

### Temporary Rules

- Enables and disables rules on demand, eliminating the need to constantly redefine infrequently-used rules.

### Port Forwarding

- Allows the definition of specific port forwards for applications that are not predefined.

### IP Translation/Outbound

- Supports network address translation (NAT), providing increased security and control of a network’s resources.

## Deep, Stateful Packet Inspection

- Tracks communication from end-to-end (instead of examining each packet without regard to its context) to increase network protection from common vulnerabilities.

## Authentication

### IP-Based

- Applies filter profiles to specific IP addresses or ranges within a network.

### Login-Based

- Assigns filter settings based on browser-based logins, restricting all access until the user is authenticated.

### Directory Services Integration (Novell, Microsoft Active Directory®, Open Directory)

- Provides filtering based on the user's or workstation's LDAP attributes, such as user name, group, or organizational membership.

## Reporting

### Workstation Reports

- Shows workstation usage by Profile Name, Access Zone, those set by Users, and those using the Profile Login method.

### Profile Reports

- Shows usage for profiles by Users or Access Zone.

### User Reports

- Lists users and their profiles or access zone privileges.

### Access Reports

- Shows usage based on requests such as most popular destinations and most active workstations and profiles.

## A 'Reports Only' User

- Provides the ability to create a User Account for a Reports Only User which is beneficial for an Administrator that needs access only to the Reporting function.

## Reporting-LDAP-based Directory Services

- Integrates with LDAP-based directory services—such as Novell eDirectory, Microsoft Active Directory, or Open Directory—to add Object Names to reports.

## Firewall Traffic Reports

- Logs specified network access requests.

## IP Multicast Support

- Supports PIM and IGMP to receive multicast streams.

## Flexible Setup

### Internet Gateway

- Supports WAN connections up to 1000MBps with configuration support for static IP, DHCP, or PPPoE.
- Supports 1 or 2 LAN connections, providing built-in routing and segregation for multiple physical local area networks.

### Proxy Only

- Works as a web proxy server without interfering with your existing LAN configuration.

### Transparent Bridge (with or without Firewall)

- Filters network traffic while leaving existing router and configuration in place.

### Virtual Appliance

- Delivers same powerful functionality on a virtual appliance.

## Patron Connect™

- Provides an additional Ethernet Interface for simply and inexpensively creating a separate, secure network for patrons without purchasing an additional Internet connection, router, and firewall.
- Use as a DMZ to serve web pages or provide Internet content.
- Can also be used for redundancy to provide failover protection.

## SMARTrecover Framework™ (High Availability Solution)

- Pairs two appliances to provide failover protection against network disruptions caused by critical hardware or software failures.

## Acceptable Use Policy Splash Screen

- Creates a WiFi hotspot for a portion of your network.

## Integrated Web Cache

- Provides network-wide web caching (including YouTube videos) to save bandwidth and increase performance.

## Peer-to-Peer Detection and Blocking

### Peer-to-Peer Blocking & Monitoring

- Provides dynamic monitoring and restriction of most popular peer-to-peer protocols by reviewing all network traffic.

## TorPark/XeroBank

- Incorporates TorPark control into the suite of detectable peer-to-peer protocols to fix the security issues these browsing proxies and anonymizers introduce.

