

KEEPING PROGRAMS AND PEOPLE FROM BEHAVING BADLY WITH TOTAL TRAFFIC CONTROL FROM LIGHTSPEED SYSTEMS, INC.

Introduction

Public school systems faces unique network security, operating, and regulatory issues.

In many communities, the public school network is the largest and most complex – hosting an incredible variety of applications and users. While traditional firewall and related security measures are necessary – to prevent confidential data from being compromised – the biggest security threat to these networks is from the inside. Students and/or staff may attempt to hack the system, surf inappropriate web content, download illegal, dangerous or copyrighted material, or unwittingly compromise the system by connecting an unprotected “home” laptop.

Lightspeed Systems has developed comprehensive, integrated network security software specifically to meet the needs of K-12 school network administrators. This system – Total Traffic Control – has been deployed in over 600 school districts nationwide – including over one 20% of the school districts in California, Texas, Alabama, South Carolina, and Utah (as measured by enrollment). We expect TTC to be the most common K-12 school solution in the nation within several years.

The unique power of TTC rests in its ease of use, flexibility, and comprehensive feature set.

Easy to Use. Standard TTC is installed on a standard Windows server. It is inserted behind the firewall (on smaller networks it may function as the firewall as well) and can be configured in minutes to report on all network traffic, filter content, block spam, prioritize traffic, and block malware (such as spyware and viruses). All functions are easily configured with simple “check box” wizards and managed from a single central admin console that is accessible as a familiar Microsoft Management Console (MMC) snap-in or web browser.

For high volume networks, a FreeBSD-based TTC+ server is placed in line behind the firewall – and via UDP – communicates with a standard TTC windows server. This deployment provides the routing speed/stability of UNIX with the easy to use, familiar Windows policy/reporting interface.

Flexible. TTC is designed to maximize local flexibility. All databases (content filter, spam, malware) are open, and local administrators can easily add or delete entries to any of them. Databases are automatically updated nightly, but local decisions always override the master database. Local administrators can easily turn off or on any of the features.

The software is also designed and priced to provide maximum flexibility for network placement and growth.

Comprehensive. The gateway server software, coupled with Security Agents on each desktop, provides the district with detailed network traffic reports and the ability to easily adjust network traffic to

- enforce acceptable use policies,
- prioritize critical network traffic,
- prevent inappropriate or illegal Internet surfing and spam.

The desktop Security Agents protect your network from your biggest threat--your users:

- prevent malware from being launched from within the network,
- provide network administrators with a comprehensive audit of all applications installed on the network,
- give the network administrators the ability to enforce security policies.

In sum, TTC is an excellent network management solution for large K-12 school districts. It is powerful – yet easy to use. It is comprehensive – yet maximizes local flexibility. A substantial and growing customer base strongly endorses the product. Reference accounts are available.

Detailed information is enclosed which highlights TTC's unparalleled functionality.

How Total Traffic Control Keeps Programs and People from Behaving Badly

1. Extensive monitoring and detailed forensic reporting
2. Internet access management (content filtering)
3. Spam blocking & E-Mail Filtering
4. Desktop Security
5. Gateway Security
6. Traffic Prioritization
7. Message Journaling

1 - Extensive Monitoring & Detailed Forensic Reporting: Know who's doing what on your network

Monitor and report your entire network's activity or a user's activity so you know exactly what you need to be concerned with. Total Traffic Control's exhaustive reports include everything you'd expect, plus file names and sizes of uploads/downloads, search-engine keywords used, suspicious search-engine queries that indicate a persistent user seeking inappropriate content (e.g., pornography, drugs), instant messaging sessions, applications inventory and usage, email sent and received, virus activity, and busiest traffic types (http, https, SMTP, Kazaa, etc.).

These detailed and easy-to-interpret traffic reports can be viewed and configured locally or remotely, printed to a PDF file, and exported for use with Excel, Word, etc.

2 - Internet Access Management (content filtering): Control what people can do and see on the Internet

Rely on a comprehensive, accurate, and accessible data base.

Lightspeed Systems provides our customers unparalleled access to the data base. Customers can see how any site is categorized, why it is categorized that way, who categorized it and when. Every detail about the site, links to the site, and other relevant information is available for review. Not only can you check our accuracy easily – you can make much more informed decisions when internal customers request sites be unblocked or re-categorized. Go to www.TTCCompare.com for details.

Remote Content Filtering for your laptop computers

(See white paper titled “SA White Paper” for more detail)

Desktop content filtering allows you to control which websites are acceptable for browsing at the desktop level. When users take their company laptops off the premises, the content filtering goes along. External servers are setup so that the district laptops can apply policies and block undesired websites from anywhere. (i.e.: If Playboy.com is blocked while the laptop is connected to your network, Playboy.com will be blocked no matter where that laptop logs onto the internet.)

The Desktop Security Agent also provides the following:

- User name authentication for forensic reporting
- Desktop antivirus (known viruses, malware, worms, spyware, etc. It also will block any “unknown” programs from launching and accessing your network)
- Hardware/Software inventory on the desktop or laptop computer
- Remote Content Filtering

Create different rule sets as needed

With a variety of users, you have a variety of needs. Configure TTC to meet the needs of each of your user groups.

User types. Filtering policies can be set for various groups inside your organization including IP address, IP address range, user, group of users, organizational units, sites, or entire domains.

Time. Another way to ensure productivity during regular business hours is to limit non-work related web access to after hours and weekends. For example, you can set shopping and finance sites to only be accessible after 5pm and before 8am, Monday through Friday, and anytime Saturday and Sunday.

Authentication & Soft Blocking. You can also create an exceptions list made up of users who should be allowed to bypass the content filter. When a blocked access screen is encountered, users on the exceptions list simply authenticate using their network login credentials.

Block or limit all types of web traffic

With Total Traffic Control, it’s easy to block or limit (to a specified number of kilobytes or megabytes per second) each of the following:

Categories of web traffic. Filter web traffic by content category so that inappropriate or bandwidth-sapping sites are either blocked entirely or their bandwidth is limited. Total Traffic Control comes with 50+ content categories, but you may add and modify categories as needed.

Peer-to-peer (P2P) traffic on any port. Block or limit all the bandwidth-sapping peer-to-peer applications like Gnutella, Kazaa, or whatever the fad may be on any given day--even if it's coming from somewhere other than port 80.

Instant messaging. Block or limit instant messaging sessions that often become major distractions and attract risky attachments.

Dangerous web activities. Block dangerous web applications, hacking tools, and file types by extension.

Minimize over- and under-blocking

With full control over the content database and a variety of tools, you can minimize over- and under-blocking concerns.

Add, re-categorize, unblock sites in seconds. A couple of mouse clicks is all it takes to add or modify a site's categorization--because you own the database.

Easily create categories. Define a new category using a short list of sites the category should include. Total Traffic Control will use the list to create a statistical model. All the current web sites, plus any future web sites, can then be re-categorized to reflect the newly defined criteria. There is no limit to the number of categories you can add.

Share database updates with like-minded peers. To best serve your region or industry's needs, you may want to share database entries and category definitions. Database criteria and updates may be shared between school districts, libraries, government agencies, sister organizations, or any trusted sources, any way you want.

Allow or disallow unknown sites. If someone on your network visits a web site not in the database, the site will be uploaded to Lightspeed Systems for automatic categorization and/or review. You have the option whether to allow or block sites not in the database.

Force Google or Yahoo! SafeSearch. You can optionally force Google and Yahoo! SafeSearch. When SafeSearch is turned on, sites and web pages containing pornography and explicit sexual content are blocked from search results.

3 - Spam Blocking & E-Mail Filtering: Control what people are exposed to through email

Total Traffic Control's Spam Mail Blocker provides multiple lines of defense against spam and offensive emails including integration with your blocked-content specifications, virus scanning, dangerous-attachment scanning, black lists, white lists

(individual and organization wide), adult subject-line screening, database lookups of known spammers (spam content category and real-time blackhole lists like Spamhaus), local learning of what's considered spam at your site, Bayesian statistical comparison to keep up with the newest spammer techniques. You can also create your own spam-pattern definitions.

In addition, to lift the burden from administrators, individuals may manage their own spam through daily emailed summary reports that help fine tune the software.

4 - Desktop Security: Stop "Unknowns" along with known viruses, spyware, malware, worms...

See additional information titled, "Network Security Beyond The Firewall"

"Eighty to 90 percent of computers have some form of spyware on them."
Rich Mogull, research director for analyst firm Gartner Inc.

Spyware, adware and other forms of malware are easy to get and difficult to remove. They slip in without the user's knowledge, monitor computer activity, and bury software components so they can resurrect themselves when deleted.

Most anti-spyware solutions available today were not developed for the network. Centralized deployment and management are limited if available at all. Further, they do not address both the desktop and the network.

Using "program permissions" on desktops that are similar to "user permissions" on a network, the Security Agent can be remotely managed to prevent known bad programs as well as previously unknown programs from behaving badly.
(See white paper titled "SA White Paper" for more detail)

Desktop content filtering allows you to control which websites are acceptable for browsing at the desktop level. When users take their company laptops off the premises, the content filtering goes along. External servers are setup so that the district laptops can apply policies and block undesired websites from anywhere. (i.e.: If Playboy.com is blocked while the laptop is connected to your network, Playboy.com will be blocked no matter where that laptop logs onto the internet.)

The Desktop Security Agent also provides the following:

- User name authentication for forensic reporting
- Desktop antivirus (known viruses, malware, worms, spyware, etc. It also will block any "unknown" programs from launching and accessing your network)
- Hardware/Software inventory on the desktop or laptop computer
- Remote Content Filtering

5 – Gateway Security

See additional information titled, “Network Security Beyond The Firewall”

Lightspeed Firewall protects your valuable network resources from unwanted access and dangerous traffic with its well-integrated, multiple levels of security.

Traditional firewall security:

- [Advanced, stateful packet inspection](#)
 - Allow or deny traffic according to security policies
 - Thwart denial-of-service attacks
- [Mask internal network structure \(NAT\)](#)

PLUS these integrated layers of security

- [Control applications on the network](#)
 - inventory applications and usage
 - block spyware
 - block instant messaging
 - block peer-to-peer traffic
 - allow/deny HTTP, FTP, SMTP commands
- [Monitor/report network and user activity](#)
- [Resolve usernames for policy enforcement](#)
- [Access network virtually with Microsoft PPTP \(VPN\)](#)
- [Fault-Tolerant Capable](#)

Advanced, Stateful Packet Inspection. Generally considered "state of the art" firewall technology, stateful packet inspection is a technology similar to that used by the industry-leading products. In addition to protecting resources on the network, this inspection protects against Denial of Service (DoS) attacks where the intent is to end user access to network resources.

Using configured security policies, Lightspeed Firewall actively inspects both inbound and outbound network traffic to determine whether or not the traffic is allowed. The Lightspeed Firewall security policies can be created to manage traffic by:

- user
- group
- IP address
- application
- DiffServ marking
- time of day
- URL
- more

Network Address Translation (NAT). Lightspeed Firewall can perform network address translation to mask the internal network structure from the outside world. All the LAN's PCs appear on the Internet with one public IP address. This way the address of a PC on your network is never transmitted on the Internet. This functionality also allows

Lightspeed Firewall to be used with DSL and cable modems where the ISP has provided just one IP address.

Application-Layer Inspection. For granular access-control policies, Lightspeed Firewall inspects traffic at the application layer.

* *All applications may be inventoried* and usage recorded so that you know exactly what's running on your network. Any unwanted application may be stopped and banned network wide.

* *Spyware, adware, and malware may be blocked* using application permissions. All "good" applications on your network are given an appropriate set of permissions so that they may not be modified to behave in inappropriate or "virus-like" ways. Known "bad" applications have no permissions. Unknown applications are quarantined until reviewed by an administrator.

* *Peer to peer (P2P) and instant messaging sessions may be categorically blocked* since these are often accompanied by dangerous or illegal file attachments.

* *Application-level proxies* are included for many protocols including HTTP, FTP and SMTP so that specific commands within these protocols may be allowed or denied at the gateway level. For example, the FTP delete 'DELE' command can be blocked for all inbound connections from the Internet, quickly securing your files from deletion by unknown users.

Real-time and Recorded Statistics. Lightspeed Firewall includes detailed real-time and recorded stats that tell the network administrator the status of their network at any moment, or trends over days or weeks. Reports may be viewed from anywhere with a web browser and include the following:

- Firewall events
- Intrusion log
- Network activity by individual or group
- Network activity by IP address or range of addresses
- Network activity by type of traffic
- and much more

Username Resolution. Through username authentication and IP address resolution, reports display who is doing what on your network. This documented activity allows real-time enforcement of security and acceptable use policies.

VPN Support. Microsoft VPN point-to-point tunneling protocol (PPTP) is supported by a built-in proxy for both inbound and outbound PPTP connections.

Fault-Tolerant for Mission-Critical Networks. A pair of Lightspeed Firewall appliances installed on a network eliminates a single point of failure. The backup

appliance constantly monitors the health of the active appliance and takes over all processing responsibilities if problems arise - transparent to the end user.

6 - Traffic Prioritization: Prioritize mission-critical traffic

Traffic prioritization allows you to prioritize mission-critical applications like document management, accounting, Citrix applications, and voice over IP while limiting or blocking risky instant messaging and bandwidth-sapping file-sharing applications like Kazaa, eDonkey, and BitTorrent.

7 – Message Journaling

Easily archive and retrieve email and instant messages

With federal rules requiring organizations to keep tabs on all employee email, instant messages (IM), and other digital communications, clear policies and methods for archiving and retrieving these records are paramount.

Total Traffic Control includes Message Journaling at no additional cost. You can search, retrieve, and report on inbound, outbound, internal and external email-including attachments-as well as instant messaging.

TTC Message Journaling meets all the common criteria set by network administrators for complying with federal regulations:

- Easy to implement and to use.
- Comprehensive capturing and indexing of message attachments as well as full message details.
- Time-stamped and unalterable file-integrity for the archived data.
- Flexible data search, reporting and message retrieval.

- [Read about Frenchtown School District's use of Message Journaling](#)

Wondering if it's feature rich? Go ahead; compare this list to any competing product.

ARCHIVE

- Inbound and/or outbound SMTP traffic
- Inbound and/or outbound AOL Instant Messaging (AIM) and MSN Messenger
- Email message file with indexing parameters for: From, To, Subject, Date, Keywords, and Body Text
- Attachments: Document, program, and multimedia files
 - To conserve storage space, message attachments with multiple senders or receivers are stored only once

- Internal email processed by Microsoft Exchange Server 2003 (GroupWise and Exchange 2007 support now in development)

SEARCH & RETRIEVE

- Basic end-user searches on sender, recipient, subject, and date range
- Extended administrator searches on keywords, attachments, meta info, body text, and "suspicious phrases"
- "Retrieve Mail" link on every report allows quick, easy forwarding

TAILOR TO YOUR NEEDS

- Customize and generate reports on "suspicious phrases."
- Configure data redundancy of archived email (backup servers).
- Avoid limitations-journaling and archiving capacity is limited only by available disk space.

Low Total Cost of Ownership

Because Total Traffic Control can replace multiple existing products with a single admin console and a low cost per seat, Total Traffic Control saves both hard and soft costs.

Independent test lab, The Tolly Group, recently released its study pitting security "best-of-breed" combinations against integrated solutions to determine the "effort and complexity required to deploy and to manage a comprehensive perimeter security solution for a typical medium-sized business for a period of 12 months." This security included firewall/packet filtering, VPN connectivity, Internet content filtering, spam blocking, and antivirus.

Key findings:

- "Best-of-breed" combinations took 2.9x to 4x more time to configure and deploy than the integrated solution.
- "Best-of-breed" combinations consumed 1.8X to 2.4X more time to manage on an ongoing basis compared to the integrated solution.
- There is clear value to pre-integrated solutions including benefits of a single user interface, one integrated update mechanism, and one set of management tools.

Further, a quick return on investment is realized through network resource savings, employee productivity gains, and legal liability reduction.

Network Resource Savings

- **Avoid Spam**
--\$86 per mailbox in 2004
(Radicati Group)
- **Avoid Viruses & Worms**
--MyDoom damage in U.S.: \$12.2B
(Web Host Industry Review)
help desk, overtime, loss of business, bandwidth clogging, productivity erosion, management time, and cost of recovery
- **Avoid Bandwidth Upgrades**
--prioritize mission-critical traffic and avoid costs associated with bandwidth upgrades

Employee Productivity Gains

- **Avoid Spam**
--3.1 percent of employee productivity, or \$1,934 per employee in 2004
(Nucleus Research)

- **Avoid Web Distractions**
--1 hour per week per employee costs \$1,000 (\$20/hour x 50 weeks)

Legal Liability Reduction

Detect and block

1. Child pornography, estimated to be on every large network (Internet News)
2. File uploads/downloads of copyrighted material
3. Offensive spam mail, which can lead to serious penalties (up to \$300,000) if you require staff to use email, but take no action to block offensive spam messages. (Cornell Law School)

Total Traffic Control v6

Cost Comparison Checklist



Functionality	TTCv6	Other	Cost
Content Filtering			
Filter all web traffic	Yes	Yes/No	\$ _____
Filter all web traffic on laptops inside the network	Yes	Yes/No	\$ _____
Filter all web traffic on laptops outside the network	Yes	Yes/No	\$ _____
Access and modify the complete content database	Yes	Yes/No	\$ _____
Spam Management			
Block spam mail like "Get Viagra Cheap Now"	Yes	Yes/No	\$ _____
Allow users to review messages categorized as spam	Yes	Yes/No	\$ _____
Individual user spam management	Yes	Yes/No	\$ _____
Message Journaling			
Search and retrieve email	Yes	Yes/No	\$ _____
Search and retrieve instant messages	Yes	Yes/No	\$ _____
Network Security			
Block/Limit P2P file trading like Kazaa, Morpheus	Yes	Yes/No	\$ _____
Block/Limit instant messaging like AIM, MSN, Yahoo	Yes	Yes/No	\$ _____
Block viruses, worms and spyware @ the gateway	Yes	Yes/No	\$ _____
Block adware, malware	Yes	Yes/No	\$ _____
Block phishing and pharming	Yes	Yes/No	\$ _____
Block hacking tools	Yes	Yes/No	\$ _____
Desktop Security			
Block viruses, worms and spyware @ the desktop	Yes	Yes/No	\$ _____
Inventory applications and usage	Yes	Yes/No	\$ _____
Inventory hardware on all network machines	Yes	Yes/No	\$ _____
Restrict unknown programs from "virus-like" actions	Yes	Yes/No	\$ _____
Restrict known, unwanted programs on all network machines	Yes	Yes/No	\$ _____
Removeable media control	Yes	Yes/No	\$ _____
Reporting			
Monitor users (sites visited, protocols, up/downloads, IM)	Yes	Yes/No	\$ _____
Monitor all emails going in and out of the network	Yes	Yes/No	\$ _____
Monitor all files going in and out of the network	Yes	Yes/No	\$ _____
Monitor instant messages going in and out of the network	Yes	Yes/No	\$ _____
Monitor all processes running on the network	Yes	Yes/No	\$ _____
Report on all aspects of network traffic	Yes	Yes/No	\$ _____
Bandwidth Management			
Prioritize traffic with class-based queuing	Yes	Yes/No	\$ _____
Prioritize traffic with user min/max	Yes	Yes/No	\$ _____
Easy Administration			
Manage on the web	Yes	Yes/No	\$ _____
Free training, 24/7 support, daily updates	Yes	Yes/No	\$ _____
Delegate administrative tasks	Yes	Yes/No	\$ _____
Total cost per workstation:	\$ _____	compared to	\$ _____

Reference Accounts: Available upon request

More on Lightspeed Systems

Lightspeed Systems specializes in network traffic management and security software for the modern Microsoft network in K-12 school districts. The company directs its software development around these principles: 1) software architecture should be modular, 2) a community of network administrators can solve common pain points, and 3) firewalls and antivirus software have failed to protect networks.

Founded:

The company has been addressing network traffic issues between disparate systems since 1984 to provide leading-edge connectivity software for a worldwide customer base of Fortune 500/1000 companies, educational institutions, and government agencies. For four years Lightspeed Systems operated a regional Internet Service Provider business which peaked at 20,000 customers and was sold to a national ISP. Since the dawn of the commercial Internet, Lightspeed Systems has been focused on helping schools safely and securely manage their networks.

Management:

Robert E. McCarthy III	Founder/CTO
Joel Heinrichs	CEO
Scott Garrison	VP of Sales & Marketing
John Genter	VP of Operations
Brock Meadows	VP of Product Development
Phil Scrivano	VP of Customer Services

Products:

Lightspeed Systems has the only full-featured, network traffic management and security product built for the business standard networking environment, Microsoft Windows. Delivering a one-two punch with both extensive traffic monitoring and reporting and the tools to resolve detected issues, Lightspeed Systems rises above all other network traffic products.

The software has several unique and advantageous characteristics. First, the suite of tools employs "IP Objects" which may be turned on or off as needed (e.g., traffic reporting, spam mail blocking, content filtering, intrusion prevention, virus scanning). Second, the virus, malware, spam, and content filtering databases are open and built out by the community of network administrators using the software and choosing to share their best practices. Third, the content filter automatically categorizes web sites using statistical analysis to compare unknown sites to those in editable category lists of matches and near matches. Fourth, security for Windows is extended to restrict program actions either network wide or at the client running Security Agent software.

To unify the configuration and maintenance of its various functions, Total Traffic Control's user interface works as a familiar Microsoft Management Console (MMC) snap-in with a strikingly similar web-based interface.

Located:

1800 19th Street

Bakersfield, CA 93301

Tel: (661) 324-4291

Toll free: (877) 447-6244

Fax: (661) 324-1437

Internet: <http://www.lightspeedsystems.com>