

Protect your network against the risk and the cost of undesirable Internet and P2P traffic

Unauthorized or otherwise undesirable Internet traffic can degrade the performance of your network, expose it to web-based security threats, undermine employee productivity, and even leave your organization vulnerable to serious legal liabilities. NetSpective Internet content filtering solutions help secure your network and maximize its capacity by eliminating this traffic-without interfering with the legitimate Internet access required to run your business.

Eliminate Skype™, P2P and other "undesirable" traffic in your network

NetSpective is a sophisticated Internet content filtering device that maximizes the performance and security of your data network by eliminating undesirable web traffic. Its rack-mount configuration easily connects to your network, and its filtering and operational controls are simple and flexible. The web-based interface provides "at-a-glance" status updates, and NetSpective's suite of tools and applications addresses every practical aspect of Internet access control, including compliance with federal filtering mandates and communications tracking requirements.

The industry's most intelligent filtering solution

NetSpective's WebFilter function lets network administrators block any URL containing objectionable content. Its robust, continually updated categorization engine includes millions of potential problem sites in more than 60 URL categories including pornography, financial investing, file sharing, online chat, and more. Passive or transparent filtering prevents network performance degradation, and WebFilter's accuracy prevents user complaints of over-blocking.

Unprecedented Scalability

NetSpective integrates into complex networks to enforce filtering policies for local systems as well as mobile user or home offices, regardless of location. NetSpective's unprecedented reach combined with the ability to scale from a 50 employee organization to a worldwide corporation with unlimited users.

Comprehensive, accurate content review

NetSpective's Adaptive Filtering capability alerts the NetSpective Adaptive Filtering Lab when any site reached by your users is not already in our database. The site is subjected to both automatic and human review, categorized, and distributed to the entire NetSpective user community. Even the most obscure sites receive full content review.

Extra security through signature-blocking technology

NetSpective's built-in P2Pfilter prevents your network users from accessing P2P, IM, chat and Skype applications. Signature-based blocking technology analyzes the unique protocol signatures of all Internet traffic moving in and out of your network, guarding against circumvention by the rogue applications that render many competitive products ineffective.

Next generation P2P applications including Skype are designed as an invasive application that is undetectable and cannot be monitored. Additionally, being a true P2P application, Skype must leverage existing network resources to function, thus compromising an enterprise's network bandwidth to mission critical services. Skype's closed and proprietary implementation make it impossible to confirm the security of the software and enforce regulatory mandates. With this in mind vulnerabilities in the Skype protocol could be manipulated to make anti-virus and intrusion detection systems ineffective to attacks.

Packet-by-packet traffic inspection (SideScan™)

SideScan is a firewall-independent filtering technology designed into NetSpective that reviews every packet of information going out to the web-including HTTP, HTTPS, FTP, NNTP, chat, peer-to-peer, Skype, VoIP, and streaming media-and interrupts connections to websites or file sharing applications that have been blocked. SideScan accurately filters as much as twice the bandwidth possible with other Internet filters.

NetAuditor[®]: A complete view of your network traffic

NetSpective also includes the web-based NetAuditor, which monitors and reports on web traffic patterns. NetAuditor provides a detailed audit of such non-essential bandwidth usage as Skype, FTP, peer-to-peer, and instant messaging traffic, making it easy to identify wasteful, risky, or otherwise undesirable web activity.

An investment with instant returns

NetSpective can immediately boost your network's capacity and security by cutting out undesirable web traffic. And it will pay substantial long-term dividends in network and employee efficiency.

Contact us today to learn more.

Phone: 678.589.7100

Fax: 678.589.7110

E-mail: sales@telemate.net

www.telemate.net

NetSpective®

Key Features

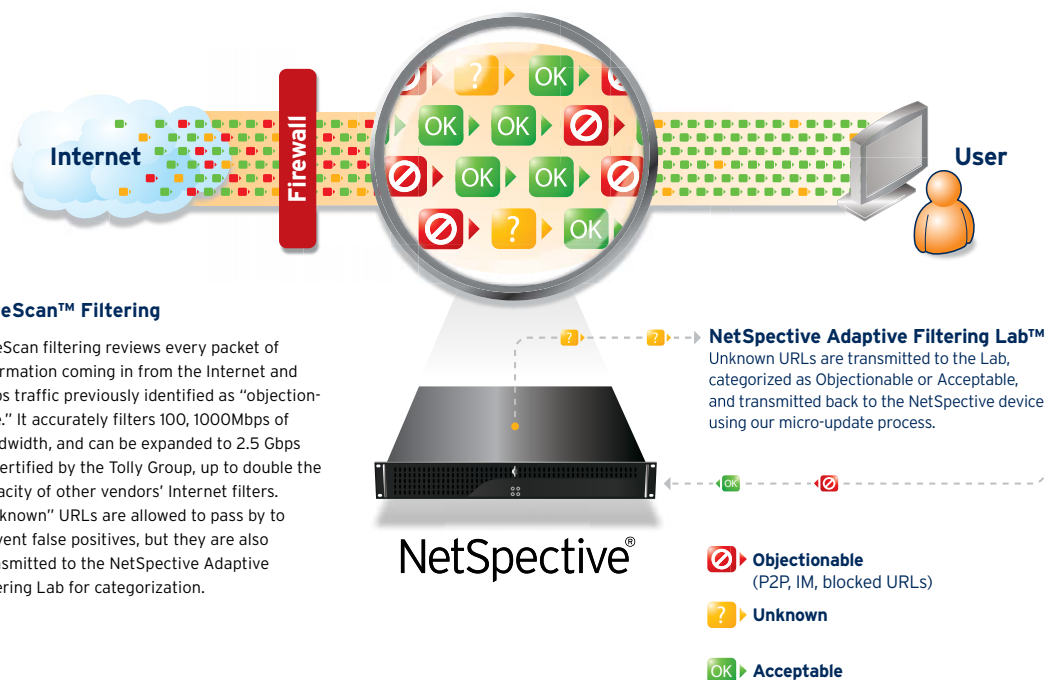
- SideScan filtering technology is not a point of network failure
- Monitor or block HTTP, HTTPS, NNTP, FTP, chat, peer-to-peer (P2P), Skype, VoIP (SIP, H.323), and streaming media protocols
- Signature-based blocking subscription with live updates
- Support for Citrix and Terminal Server
- Support for mobile users and home offices regardless of location
- Customized modes of operation by network IP address range(s) by time of day enabling pass through, monitor / report, or block / report traffic management
- Network Abuse Detection with session lockout
- Centralized policy management for distributed network environments
- Custom policies for special user group designations, supports 512 groups
- Support for usernames in DHCP environments via NetSpective Logon Agent
- Support Microsoft Active Directory and Novell eDirectory via LDAP
- Flexible policy exemption by IP Address, username or URL using wildcard overrides
- Google and Yahoo safe search enforcement
- Over 60 categories provided
- User defined categories
- Application and protocol level control of Peer-to-Peer traffic
- Comprehensive web-based reporting tool, NetAuditor
- NetAuditor documents all monitored and blocked activity
- Automated signature updates and product enhancements
- Automatic synchronization of URL overrides to TeleMate.Net Software's On-Line Service
- Available monitoring interfaces: 100 MB, 1000 MB, and Quad GigE

Optional Features

- Additional reporting on manufacturers firewalls using NetAuditor including:
 - Cisco
 - Microsoft
 - Checkpoint
 - Symantec
 - Juniper/NetScreen
 - Novell

Regulatory and Compliance

- Enables enterprise compliance with the statute for lawful interception (LI/CALEA)
- Enables compliance with E911 VoIP mandate, designed to aid first-responders
- Adheres to Sarbanes-Oxley Act for security and auditing requirements
- Compliant with Children's Internet Protection Act (CIPA)
- Enables compliance with the Health Insurance Portability and Accountability Act (HIPAA) for unlawful transmission of patient files



©Copyright TeleMate.Net Software 1997-2008. All rights reserved.

No part of this publication, including text, examples, diagrams, or icons, may be reproduced, transmitted, disclosed or translated in any form or by any means, electronic, mechanical, manual, optical or otherwise, for any purpose, without prior written permission of TeleMate.Net Software. Information in this publication is subject to change without prior notification. TeleMate.Net Software may have patents or pending patents applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this publication. The furnishing of this document does not give you license to these patents, trademarks, copyrights, or other intellectual property. Specifications are subject to change without prior notification.

Trademarks

NetAuditor and NetSpective are registered trademarks of TeleMate.Net Software in the United States and other jurisdictions. All other trademarks, registered trademarks and service marks are the property of their respective owners. NS_0608

TeleMate.Net®
SOFTWARE

5555 Triangle Parkway, NW
Suite 150
Atlanta, GA 30092
678.589.7100 Phone
678.589.7110 Fax
sales@telemate.net