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. Pass-by-transparent filtering prevents network performance degradation, and WebFilter's accuracy prevents user complaints of over-blocking.

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.

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. The Verso 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.

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, 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.

Verso NetAuditor®: A complete view of your network traffic

NetSpective also includes the web-based Verso 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.

Toll-free: +1.866.829.8776 (U.S. and Canada only)
Outside the U.S. and Canada: +1.678.589.3500
E-mail: ns-sales@verso.com
www.verso.com

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

A global provider of Next Generation Network solutions
**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 and streaming media protocols
- Signature-based blocking subscription with live updates
- Customized modes of operation by network IP address range(s) by time of day enabling pass through, monitor / report, or block / report traffic management
- Centralized policy management for distributed network environments
- Custom policies for special user group designations, supports S12 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, Verso NetAuditor
- NetAuditor documents all monitored and blocked activity
- Automated signature updates and product enhancements
- Automatic synchronization of URL overrides to Verso's On-Line Service

**Optional Features**

- Gigabit monitoring interface
- Additional reporting on manufacturers firewalls using Verso 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

**SideScan™ Filtering**

SideScan filtering reviews every packet of information coming in from the Internet and stops traffic previously identified as “objectionable.” It accurately filters 100, 1000Mbps of bandwidth, and can be expanded to 2.5 Gbps as certified by the Tolly Group, up to double the capacity of other vendors’ Internet filters. “Unknown” URLs are allowed to pass by to prevent false positives, but they are also transmitted to the NetSpective Adaptive Filtering Lab for categorization.

**NetSpective Adaptive Filtering Lab™**

Unknown URLs are transmitted to the Lab, categorized as Objectionable or Acceptable, and transmitted back to the NetSpective device, usually within 24 to 72 hours.

**User**

Internet

Firewall

NetSpective®