

NETSPECTIVE SOLUTIONS

Introduction

Access to the Internet has become a necessary business tool for many employees of today's companies. But that access is open to abuse by those users - abuse that may cost the company significant money in terms of lost productivity and the waste of expensive bandwidth resources. Worse yet, Internet abuse may leave the company exposed to adverse publicity or even legal liability as content from the dark side of the Internet - pornography, hate speech, or info-crimes such as stock manipulation - spread into the workplace.

The best defense against Internet abuse for your company is to set policies that control these activities, and enforce those policies with our NetSpective Internet Access Management (IAM) solution.

NetSpective provides fast, accurate and easy Internet access management for mid- to large-sized networks. It accurately and dependably blocks objectionable material from entering the workplace, and does it without introducing a potential point of failure that might affect the performance or reliability of the network.

NetSpective makes several important technological advances for IAM:

- NetSpective is implemented as a hardware appliance; easy to install, configure and operate. Its automated update services and easy, browser-based configuration and management were designed with ease of administration and maintenance in mind.
- NetSpective's SideScan™ filtering technology overcomes a major problem of IAM - the need for scalable, non-intrusive filtering - by implementing a transparent filtering approach that handles 100Base-T bandwidth. SideScan filtering listens to network traffic and intercepts requests for Internet addresses without becoming a bandwidth throughput bottleneck. By implementing advanced transparent filtering methods on a high-performance hardware platform, NetSpective is able to offer the performance and reliability benefits of transparent filtering even in busy networks.
- Adaptive Filtering™ is a new approach to analyzing the content of Web sites and classifying them for filtering and reporting. It directly addresses the categorization quality and relevance issues found in conventional keyword analysis or list-based filtering applications because it provides accurate content review for ALL sites surfed. Each NetSpective appliance comes pre-configured with millions of categorized sites in its embedded Adaptive Filtering Library. As users surf the Web, the NetSpective appliance logs all Web sites not found in the current Adaptive Filtering Library. The incremental site data is then forwarded to the centralized NetSpective Adaptive Filtering Lab where automated content recognition tools efficiently review each site for objectionable content. Many other types of content are classified into a total of 53 categories. The newly categorized sites are then automatically redistributed to all systems in the NetSpective subscriber community where they are immediately available for filtering and reporting purposes. This process provides users with an accurate and highly relevant database on which to base their Internet access policies.

- NetReporter™ is a reporting package optimized for the NetSpective appliance. The package offers a targeted solution for Internet access reporting and provides essential documentation for Internet access policy enforcement. NetSpective users with larger analysis needs may upgrade to NetReporter.

The sum of these parts is an IAM solution complete in itself - filtering and blocking, categorization and reporting - yet scalable as networks.

NetSpective Benefit Overview

NetSpective is an IAM solution that gives organizations fast, scalable protection from employee abuse of Internet access and the risks that abuse creates. In operation, NetSpective allows you to control the content that enters your workplace from the public Internet - from Web sites, news groups and file transfers. You can decide what types of sites, or even individual sites, will be blocked from your network, and you can administer access controls that give you very granular control over that access - by content category, by individual Internet address, or by individual employee.

This control can be as flexible as you choose to make it. You can control the action taken by NetSpective on a category-by-category basis - block employee access to some categories of sites, log access to others for later reporting, or take no action and let the requests pass. You can filter your network's Web traffic by time of day, so that access to some categories of content is permitted at some times but not at others.

To give you this level of control, NetSpective combines technology advances in many areas of computing into a hardware appliance that makes installation and maintenance simpler and easier than ever.

Our NetSpective solution provides:

Reliable Operation. The NetSpective appliance is a standalone device that cannot become a point of network failure. As a packaged appliance, it eliminates complexity and dependence on other devices such as firewalls and proxy servers. Its high performance design also ensures effective filtering at high traffic volumes.

Fast Performance. The NetSpective appliance is optimized for filtering and provides effective control with no network slowdowns. The appliance hardware platform and efficient SideScan transparent filtering technology provide ample IAM filtering power for even busy 100Base-T Ethernet networks.

Ease of use. NetSpective is designed for plug-and-play ease of installation - install two Ethernet cables and complete a brief configuration, and the appliance is ready to filter. This eliminates many common IAM configuration and interface hassles. Automated Adaptive Filtering Library and system updates and an intuitive Web-based interface further ensure easy administration.

Accurate Categorization. our unique Adaptive Filtering™ technology gives NetSpective fast, accurate categorization of actual corporate Web traffic and ensures that all the sites surfed by users are reviewed for content. Each NetSpective appliance starts out with a library of millions of sites assigned to 53 categories, and this library is continually expanded with Adaptive Filtering Lab reviews of newly surfed sites.

NetSpective's filtering process has three major components:



- The SideScan filtering technology. SideScan inspects all network traffic and identifies URL requests from users. In NetSpective, this “transparent” filtering technology conducts its inspections and blocks unacceptable requests without the necessity (and performance implications) of proxying user communications with the Internet. Also, its specialized high-performance design allows it to reliably handle fast 100Base-T bandwidth without missing traffic.
- The embedded Adaptive Filtering Library. The Adaptive Filtering Library is a large cache of information containing categorized Internet sites/top-level domains. It is the reference point for all NetSpective access management and monitoring policies.
- The Adaptive Filtering control mechanism. Based on the contents of the Adaptive Filtering Library and the rules defined by the user, the NetSpective filtering mechanism appliance will permit, block or simply log the Web site requests.

NetSpective Technology Review

There are four core technology components in the NetSpective Internet access management solution:

- The NetSpective Appliance
- SideScan filtering technology
- The Adaptive Filtering model
- NetReporter

The NetSpective Appliance

NetSpective Internet access filtering is a rack-mountable, hardware/software appliance that makes installing an IAM solution about as easy as it can be. Two Ethernet network interface cards are connected to the same network segment as the users to be monitored. One of these NICs listens to all traffic on the network. The other handles the appliance's filtering instructions, communication with the Adaptive Filtering Lab, and, optionally, a separate PC where the bundled NetReporter is installed. For more details and examples, see the section on “Installing and Configuring NetSpective” below.

During initial installation, a keyboard and monitor are required; from then on, administration is handled via the network through a browser-based interface: blocking rule definition, task scheduling, and so forth.

The implementation of NetSpective as plug-and-play hardware has great advantages:

Ease of use and low cost of ownership. Installing and setting up NetSpective is fast and easy, and the total cost of ownership is low, as compared to other approaches, because NetSpective is a standalone solution - it doesn't require specialized software installation or integration with an existing firewall or proxy server. Also, its filtering functions are self-contained: there's no need to provision or configure multiple additional machines for traffic scanning, filtering, or content categorization. This saves you time and hardware budget and eliminates hassles.

Performance. Packaging NetSpective 's IAM functionality with its own operating hardware guarantees that it will provide predictably high performance. This is a significant improvement over other solutions that rely on non-standard, user-supplied hardware platforms. In addition, the NetSpective appliance is dedicated to filtering - it doesn't have to devote processing cycles to categorizing URLs. Filtering receives the processing power it needs to handle even high-usage situations and large networks. The independent operation also ensures that the performance, reliability and security of caching servers and firewalls are not compromised.

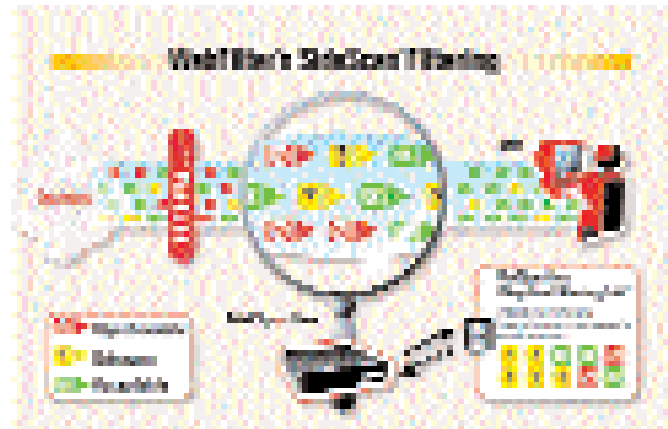
Reliability. NetSpective 's transparent SideScan filtering technology eliminates the inherent point of failure and bandwidth throttle of proxying pass-through filters. If a pass-through product malfunctions, it can halt network traffic and may bring down the server it runs on. With NetSpective, an appliance malfunction would not disrupt the Internet connection. The simplicity of NetSpective improves reliability as well. Other solutions depend on the synchronized operation of various software interface or redundant sensors. This complexity increases the number of interdependent components that could fail.

Accuracy. NetSpective 's high-performance design allows it to track and block objectionable content on even 100Base-T100Mb/sec. network segments. Under similar loads, other systems may miss and under block content, leading to a false sense of security.

SideScan™ Filtering

Among the most important requirements for an Internet access filtering solution is the ability to provide reliable, high-speed control without introducing a potential point of failure or performance degradation into the network.

Verso's unique SideScan filtering technology meets this challenge by providing a reliable, high-performance transparent filtering mechanism.



NetSpective's SideScan technology listens to all the network traffic on the segment it's connected to, searching for URL requests sent from users to servers on the Internet. It's designed to detect HTTP, FTP and NNTP traffic regardless of the port used. This eliminates a possible method of filter bypass. Also, as SideScan is independent of proxy servers, users can't evade filtering by simply modifying the proxy settings in their browser.

Scanned traffic destinations are checked against the Adaptive Filtering Library embedded in the NetSpective appliance. (The Adaptive Filtering Library data is maintained as an in-memory cache to give best performance.) The Adaptive Filtering Library may report that a request is objectionable, acceptable or unknown:

Objectionable. The Adaptive Filtering Library may report that a particular URL is objectionable - it should be blocked, because the site's content is in a category that is set by the administrator to be blocked. When a request is blocked, the NetSpective appliance simultaneously terminates the connection with the Web site and redirects the client browser to a dynamically generated message page hosted on NetSpective. The request is also logged for future reporting.

Acceptable. If the content of the site is not categorized as objectionable, the NetSpective takes no action to halt the delivery of the page to the user. Acceptable requests may be either monitored (logged) or ignored, again depending on the contents of the Adaptive Filtering Library and user-defined access rules.

Unknown. If a URL is not found in cache or permanent storage, it will be appended to a list of uncategorized sites. Once a day, each NetSpective unit transmits this log of unknown requests to the Adaptive Filtering Lab, a service operated by TeleMate.Net for all NetSpective subscribers.

SideScan filtering is very efficient for a couple of reasons:

- The actual process of listening to and sorting out the data is very fast. SideScan filtering detects the target TCP protocols and identifies URL requests without the need for tracking individual TCP sessions. The brunt of NetSpective's work is actually done by the time it decides it has found a packet it must process further. SideScan filtering has much less impact on CPU usage than traditional pass-through filtering applications.
- The NetSpective appliance itself is not tasked with the process of categorizing content on the fly, so it can be optimized to the filtering process. In contrast, a keyword-based filtering application must receive and process the requested content by comparing it to a list of objectionable keywords before it can determine whether to permit the user to access it. This imposes a computing overhead so high that many keyword-based products require a separate server dedicated to this.

SideScan Competitive Advantages

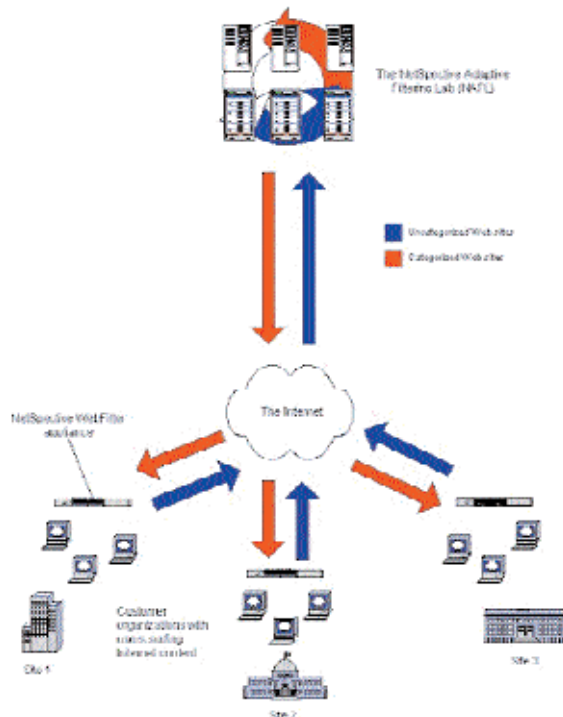
SideScan's efficiency, combined with other high-performance attributes of the NetSpective appliance, allow it to reliably scan and filter traffic on fast 100Base-T network segments. In contrast, many conventional passive scanning methods become quickly overloaded during periods of high traffic and miss large portions of site requests. Of course, if the filtering system never sees the traffic, it can't provide effective access control or documentation. This leads to a false sense of security and possibly a much higher TCO requirement if multiple traffic sensor machines are installed to compensate.

SideScan filtering technology is also superior to pass-through filtering approaches. An IAM product that uses pass-through filtering essentially operates as a proxy server: it requires all traffic to pass through the filter device and be inspected. The pass-through process makes two active TCP connections for each URL request - one with the user who requests the URL, and the other with the Web server that responds to the request. These products typically avoid deploying their own proxy device and instead run as an add-on process in an existing firewall or proxy server. While this leverages an installed component, it places an additional burden on the device that can impact its performance, reliability and security. It also introduces configuration complexities.

NetSpective, in contrast, doesn't impact the performance or reliability of other components on your network. SideScan filtering means that it doesn't have to proxy users in order to inspect URLs, so it doesn't carry the computing overhead of managing TCP connections. And because it doesn't have to stop network traffic in order to inspect it for URLs, it provides effective Internet access control without degrading network performance or posing a risk to network stability.

Adaptive Filtering

The effectiveness of any IAM solution is directly related to the quality and scope of its categorization method. The data about Web sites and their content must be accurate, or users will be inappropriately blocked from some sites, and inappropriately given access to others. It must also be relevant: there should not be large numbers of un-reviewed or uncategorized sites or else large amounts of objectionable content may slip by the filter. Either situation creates administrative hassles and a false sense of security.



- | | | |
|----------------------------|-----------------------|--------------------|
| advertising | hacking | reference |
| alcohol | hate speech | science |
| art | health | sex education |
| automotive | hobbies | sexual advice |
| consumer information | instant messaging | sexual orientation |
| criminal skills | job search | shopping |
| cult and occult | law | society |
| drugs | lingerie | sports |
| education | mature content | streaming media |
| entertainment file sharing | military | technology |
| Finance/Investing | news | tobacco |
| gambling | nudism and naturism | travel |
| games | personals/dating | violence |
| general business | politics and religion | weapons |
| glamour | pornography | web search |
| government | | |

Adaptive Filtering is NetSpective 's unique, proprietary process for analyzing ALL surfed Web sites for objectionable content and providing flexible access filtering.

The Adaptive Filtering process is based on automated content recognition engines located at the centralized NetSpective Adaptive Filtering Lab. The Adaptive Filtering Lab employs advanced neural net analysis, review of linked content, human review and other methods to accurately determine a category rating for an unknown site.

Adaptive Filtering directly addresses the categorization quality and relevance issues found in conventional keyword analysis or list-based filtering applications because it provides accurate content review for all sites surfed. Each NetSpective appliance comes pre-configured with millions of categorized sites in its embedded Adaptive Filtering Library. As users at NetSpective customer locations surf the Web, the NetSpective appliance logs sites not found in the current Adaptive Filtering Library. The incremental site data is then forwarded daily to the centralized Adaptive Filtering Lab where each site is reviewed for objectionable content - especially pornography, racist info and other types of high-risk data. Many other types of content are also classified into a total of 37 categories.

Within 24 to 72 hours, the newly categorized sites are then automatically redistributed to all NetSpective systems where they update the embedded Adaptive Filtering Library and become immediately available for filtering and reporting purposes. This process provides users with an accurate and highly relevant database to base their Internet access policies.

Adaptive Filtering Access Control

Content is categorized by site name and top-level domain. For example, www.bigsite.com/sex could be categorized as pornography, with everything below that level being tracked as pornography also. At the same time, www.bigsite.com/sports could be categorized as sports, with everything below that level being tracked as sports, too.

The Adaptive Filtering Lab categorizes all unknown sites within 24 to 72 hours. (In practice, objectionable sites are categorized most quickly - usually within 24 hours. Sites that remain uncategorized for longer periods are generally not objectionable, they just don't fit clearly into any particular category.)

NetSpective takes an "innocent until proven guilty" approach, and permits requests for unknown sites while they are under this review. Because Adaptive Filtering is driven by the actual surfing activity of its total user base, the number of un-reviewed sites should be very low - especially when compared to list-based products. It's also much more accurate than keyword scanning.

While users can request unknown sites during the review period, the category that is assigned will be used for reporting and the users can still be held accountable for their policy violations. (In contrast, conventional list or keyword-based products may never block or report on the site if it is not found and manually tagged as objectionable or picked up by a generic keyword scan. This creates a false sense of security.)

Adaptive Filtering Competitive Advantages

Adaptive Filtering offers many advantages over competing categorization approaches, including list-based, keyword analysis and on-site content analysis approaches. These advantages include:

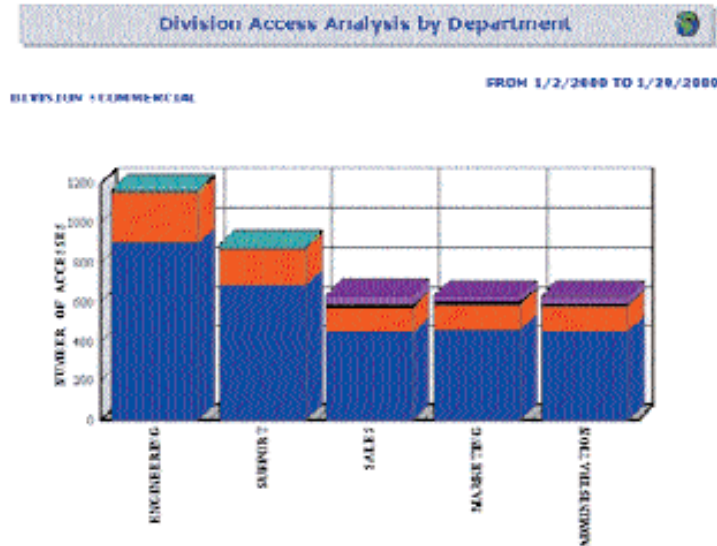
Relevance: Adaptive Filtering ensures positive categorization for Web content that is actually surfed, including obscure sites that wouldn't normally be identified in a scan of the Web. This avoids the major drawback of list-based filtering products, which provide a list of sites they think will be accessed. In real life, users of these products find that a significant portion of their Web traffic is never reviewed or made available for access management. As Adaptive Filtering is driven by real-world surf activity of thousands of users, it provides a highly focused and relevant access-control foundation.

Consistency: A person can only handle at most a few hundred sites per day, and no two reviewers will categorize the same list of sites with 100 percent consistency. Adaptive Filtering's automated content recognition categorizes content with a high degree of consistency and precision.

Accuracy: Adaptive Filtering provides full content review with a much higher degree of accuracy than the crude keyword filters offered by many products. Adaptive Filtering's sophisticated neural net analysis overcomes the problems with conventional keyword analysis, i.e. poor handling of words used in different contexts, inability to handle image-only or foreign language pages, etc. Adaptive Filtering's strength in accuracy allows it to control traffic without embarrassing over or under-blocking of content.

Scalability: Adaptive Filtering's centralized content analysis allows it to provide appropriate sophistication and processing power for accurate, high volume categorization. This allows it to efficiently categorize a much larger volume of traffic than is possible with content analysis solutions installed and maintained at a customer location. It also removes the added customer cost of supporting finicky remote analysis solutions.

NetSpective 's unique combination of full site review, automated content recognition and shared customer learning provides superior relevance, accuracy and control than conventional list-based or keyword.



NetSpective Reporter™

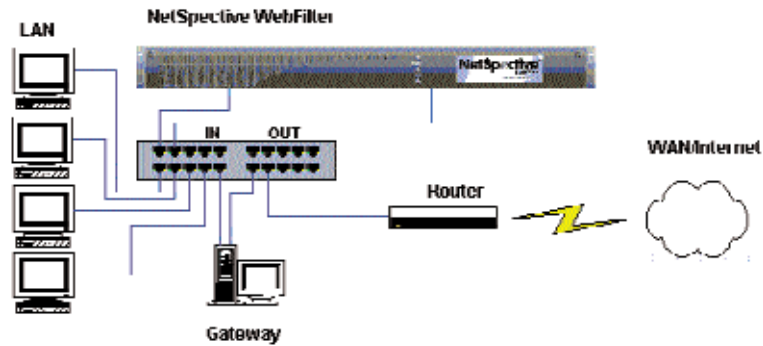
NetSpective includes a standard reporting package, NetSpective Reporter™, which provides specialized functionality optimized for the NetSpective appliance. NetSpective Reporter provides 23 standard reports for the analysis of NetSpective log file data (the NetSpective appliance logs date and time, NetSpective system name, client IP address, protocol, action (blocked or not blocked), category, and URL). The NetSpective Reporter system, installed on a separate PC, offers a targeted solution for Internet access reporting and provides essential documentation for Internet access policy enforcement. It makes it easy to produce reports on Internet access grouped by content categories, offers detail-on-demand reporting to help spot abuse and document Internet activity for problem resolution.

NetSpective users with demands for greater analysis capabilities may upgrade to NetReporter™. NetReporter provides robust Internet access and bandwidth usage reporting as part of an overall NetSpective Internet access management solution or as a standalone element. NetReporter provides a full SQL database for supporting log files of unlimited size. It allows the NetSpective user to produce reports on bandwidth usage and user-level information, and it supports aggregated reports on multiple NetSpective devices as well as third-party Internet access management solutions associated with firewalls or proxy servers.

Placement of NetSpective

In its simplest configuration, the NetSpective appliance is deployed in a network by connecting both of its Ethernet cards to a passive hub, and properly assigning a single IP address and a network mask that covers all or a subset of the network to be monitored.

A sample deployment strategy is shown in this diagram:



The NetSpective appliance is connected to the same network segment as the users it will monitor. This is the simplest possible network configuration - one Network Address Translation (NAT) point (at the router), and a single non-switched internal network segment.

This configuration requires a single NetSpective appliance. For scalability and redundancy, multiple appliances can be installed and operated on the same segment. Other configurations are possible depending on specific needs - network configuration, licensing requirements, and so forth. NetSpective can be deployed behind a firewall or Internet gateway, or in a DMZ with valid public addresses behind a packet filtering router. (If you deploy an appliance in a public DMZ, you must take care to allow administrative access while preventing unauthorized access from public addresses.)

Typically, you can optimize your NetSpective either for cost-effective filtering management, or the highest level of user control and detail reporting.

For more detail on implementing NetSpective in various network configurations, please consult the NetSpective Operational Overview.

Conclusion

NetSpective combines hardware and software into a single plug-and-play appliance - only one device to connect to the network, where other IAM products require multiple server machines to handle separate filtering and categorization tasks. SideScan filtering avoids the performance and reliability risks of pass-through filtering. Adaptive Filtering provides a superior alternative to keyword and list-based categorization schemes by aggregating and categorizing the actual Web surfing activity of all NetSpective users. And NetSpective's flexibility and scalability allow it to work efficiently and effectively in a wide variety of network configurations.

NetSpective takes advantage of major technological advances to implement Internet access management in a system that is far simpler than competing products with comparable functionality. NetSpective's fast performance, reliable operation, ease of use, and accurate categorization make it the solution of choice for Internet access.