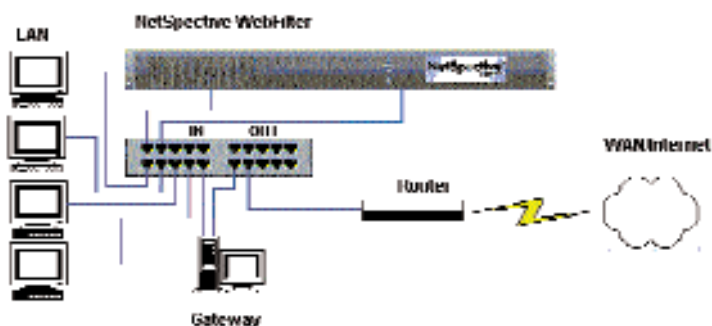


NETSPECTIVE OPERATIONAL OVERVIEW WHITE PAPER

NetSpective® is a network appliance that monitors a LAN for HTTP, FTP, and NNTP resource requests using the SideScan™ filtering technology. It can be configured to enforce the management of established Internet usage policies or to simply log requests made on these services, appending category flags to them. For additional flexibility, NetSpective can also be configured to take no action with regard to any of the above-listed resource requests. At the user interface level, these three discrete actions or policies are referred to as blocking, monitoring, and ignoring, respectively.

A sample deployment strategy is shown in Figure 1. For implementation purposes, it should be noted that NetSpective should be assigned to the address space of the clients to be monitored.

Figure 1: Typical Installation Scenario



With one interface configured as a conventional network activity analyzer, the SideScan filtering technology reviews every raw network packet on the wire. As such, SideScan is highly redundant, and does not pose the risk of interrupting Internet access in the event of a shutdown or failure. The efficiency of the SideScan packet analysis process relies on highly accurate methods for detecting the target TCP protocols without the need for tracking individual TCP sessions. The Category Management process returns codes to the network analyzer indicating whether a specific request is either approved (monitored or ignored) or disapproved (blocked), based on the policies configured via the Web interface. If a request is disapproved, a TCP-terminate message is sent to both the client and the server, and the client is subsequently redirected to a dynamically generated "block" page hosted on NetSpective.

Adaptive Filtering™ and System Updates

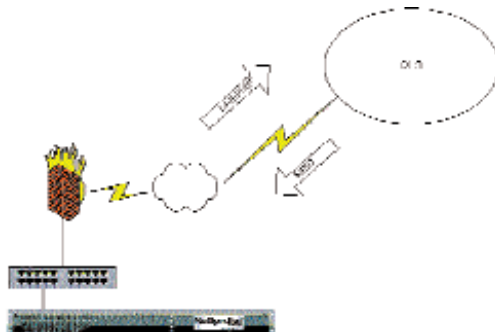
On startup, the Category Management process loads a cached list of sites, and their respective categories, from permanent storage in the Adaptive Filtering™ Library. The cache itself is generated using simple most-recently-used logic, where the cache list contains the most recently requested URLs. When the process cannot find a URL in its cache or permanent Adaptive Filtering Library storage lists, it sets the unknown URL aside for future processing.

Every day, a NetSpective unit will send the list of unknown URLs to the NetSpective Adaptive Filtering Lab™ servers for analysis. The results of the categorization analysis will then be published on a daily basis on an FTP server, accessible by the NetSpective unit for download. Once downloaded, the Category Management process will update its permanent and cache lists with the newly available information.

There are several advantages of this approach. First, the Adaptive Filtering Lab processes are based on well-trained neural network engines that are routinely retrained to classify Web pages through linguistic pattern recognition. Even if a page contains no text, the Adaptive Filtering Lab processes will attempt to identify links in and out of the page, so that it can come up with an intelligent decision as to the contents of a page. Another advantage is that NetSpective itself is not tasked with the process of classifying Web page content, focusing exclusively on the blocking process. Finally, since the Adaptive Filtering Lab receives, in an anonymous fashion, the requests of many NetSpective units on the field, every single customer receives the collective benefit of a high-quality categorization list, without the concern of excessive data due to invalid or non-existent URLs. In this way, the contents of the list are not based on arbitrary Web crawls, but on what each and every customer is surfing on the field.

The process is illustrated in Figure 2. There are two general update elements available from the Adaptive Filtering Lab on-line service (OLS). The first is the categorization update, which can be downloaded on a schedule configured via the administrative Web interface. The second is a general software update for the appliance, which will also be downloaded automatically as it becomes available. The software update is generally installed via the administrative Web interface, while the categorization updates are performed silently in the background.

Figure 2: NetSpective Adaptive Filtering Lab Online Service (OLS)



Logging

NetSpective generates log files that can be analyzed with the NetSpective Reporter™ software included with the NetSpective package (i). The log files contain the date and time, NetSpective system name, client IP address, protocol, action [blocked (1) or not-blocked (0)], category, and URL. NetSpective Reporter provides 23 reports for the analysis of access trends and Internet usage policy compliance. Specific configuration details are available on the NetSpective Reporter software.

Installation

In its simplest configuration, the NetSpective 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. Depending on the network configuration and licensing requirements, NetSpective can be connected in different segments of a network. For example, NetSpective can be deployed either behind a firewall or Internet gateway, or in a DMZ with valid public addresses behind a packet filtering router (ii).

- (i) A separate PC is required to install NetSpective™ Reporter.
- (ii) When deployed in a public DMZ, care must be taken to allow administrative access while preventing unauthorized access from public addresses.

Licensing

NetSpective is sold based on number of human users being filtered by the system or based on bandwidth (i.e. throughput on 100Base-T networks). One component of user-based licensing is a variable monitoring NIC speed, depending on the user license level. Table 1 shows the different options.

Table 1: Licensing Levels

Number of Users	Monitoring NIC speed
> 1000	100 Mbps

For licensing, the user will receive a licensing key, the name or IP address of the on-line licensing server, and a password. The host name of the appliance and the licensing password are used as the user name and password for the FTP downloads from the Online Service.

NetSpective access control functions and Adaptive Filtering Lab updates are licensed on an annual subscription basis. If the NetSpective subscription expires, the NetSpective will cease filtering and logging operations, though Web traffic will be unimpeded.

Licensing

While there are certain technical considerations in the installation of NetSpective, a number of scenarios will fall on the general categories depicted in Table 2. This chart can help determine where to place the NetSpective appliance to address various access control or solution cost constraints. Notice that, since NetSpective sets one of its network cards in promiscuous mode; certain considerations will exist in switched environments. In such cases, the traffic destined to a specific gateway should be replicated or mirrored on the port on which the Monitoring NIC of NetSpective is connected. (refer to Figure 3, Figure 4, and Figure 5)

Table 2: NetSpective Network Location Reference Chart:

Network Layout/Operational Priority	User Control / Maximum User Log Detail	Minimum Cost /Global Control
NetSpective Network Location		
Single NAT point, Single DMZ (Figure 3)	NetSpective appliance behind NAT	Single NetSpective appliance in DMZ
2+ NAT points, Single DMZ (Figure 4)	Multiple NetSpective appliances behind NAT	NetSpective appliance in DMZ
2+NAT points, 2+ DMZ (Figure 5)	Multiple NetSpective appliances behind NAT	Multiple NetSpective appliances in all access DMZs

Network Configuration vs. Deployment

In each case, a tradeoff exists between the network configuration/hardware and the desired policy goal. In general, when user-based policies are employed, an installation in the same subnet as the client machines is called for, whereas global policies are better served when the appliance is deployed in the network upstream of the users.

Special considerations should be kept in mind when caching proxies are used as Internet access gateways. The issue in question is described in Figure 6. The network depicted uses a caching proxy server with Network Address Translation across its network interfaces. If NetSpective is placed in the network upstream of the NAT point (e.g., common to the external interface of the proxy), the caching proxy will be in a position to fulfill a client request before NetSpective can analyze it. In this case, the cache should be emptied. Even in cases where NetSpective is deployed behind the proxy/NAT point, it will be useful to clean up the proxy cache before installing NetSpective for maximum benefit.

Additionally, a situation may arise in that one gateway does not serve all of the basic protocols that are filtered by NetSpective. For example, a proxy server could be configured to handle HTTP requests, and a firewall handles FTP and NNTP. Through careful mirroring of both the proxy and firewall ports on a switch, [NetSpective can be configured to properly work in this case with either a minimal number of appliances \(when licensing does not call for more than one NetSpective, for example\), or in a redundant fashion.](#)

Figure 3: Single Internal Net/Single Access Point

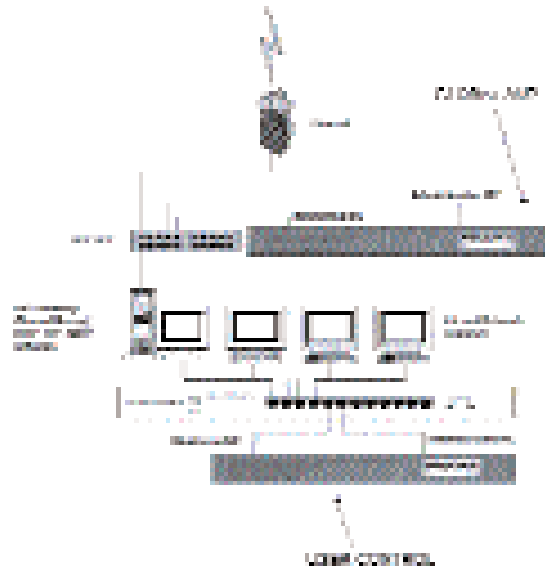


Figure 4: Multiple Internal Networks, Single Access Point

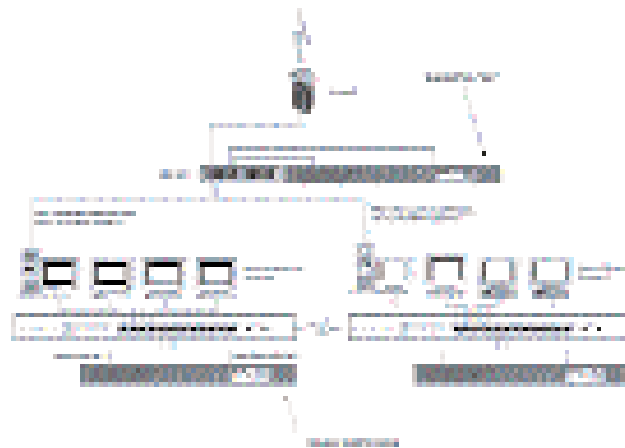


Figure 5: Multiple Internal Networks/Multiple Access Points

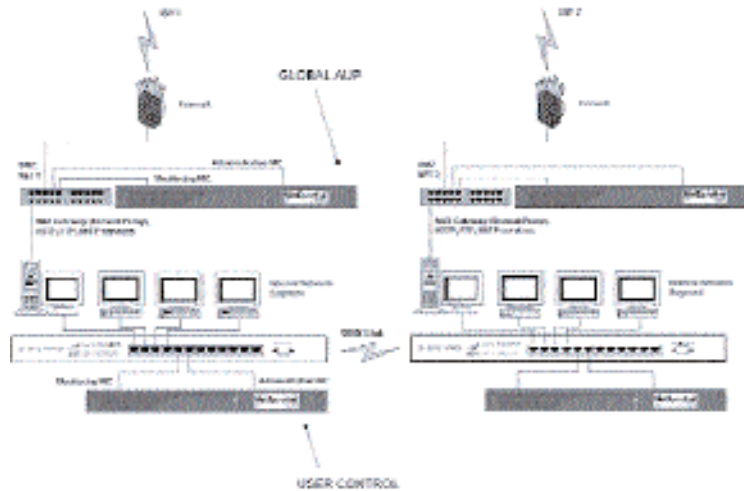
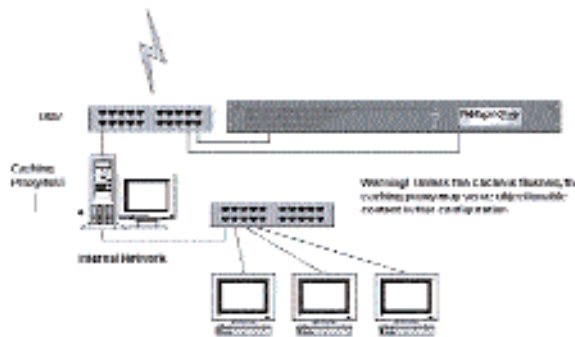


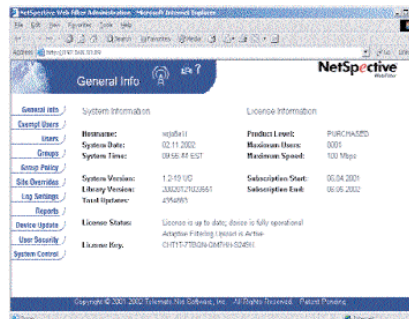
Figure 6: Caching Proxy Interaction



NetSpective Appliance Administration & User Interface

Most of the configuration and administration of a NetSpective system is done through a Web browser-based interface that you access by entering the IP address of the appliance. The "home page" for this interface (Figure 7) shows general status information about the system and the license for the appliance:

Figure 7: Main Page



(The license information on the right-hand side of the screen is important because the NetSpective system is licensed on a per-user basis -- that is, to filter a specified number of human users, not a number of machine names or IP addresses, on an annual service basis. This license includes access to the Adaptive Filtering Lab and system updates. If you allow the license to expire, NetSpective will cease filtering and logging operations, though Web traffic will be unimpeded.)

The other major administrative functions are indicated by the links on the left side of the screen. Many of these are the controls for configuring the functionality of the Adaptive Filtering process. Their values are stored in the Adaptive Filtering Library cache and read whenever a requested URL is reviewed.

Users, Groups, and Group Policy

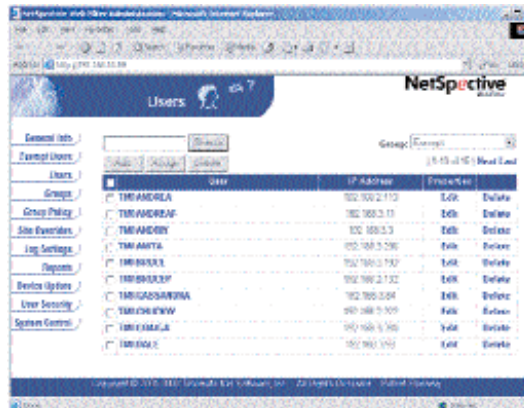
NetSpective allows the administrator to create and manage filtering policies by logical user groups, where each user group has an associated policy defined by the periods in the day where certain content is blocked, monitored or ignored. This feature has several key pieces to consider:

- a) NetSpective defines two default user groups - Public and Exempt (these names cannot be changed). The filtering policy associated with the Public group applies to all users/client systems that are not members of any other group, including those who have not been explicitly added to the Public group itself. This feature allows the administrator to create a baseline policy for the majority of users (without typing or entering user names and IP addresses by hand) and then adding other groups and associated policies for exceptional Internet usage. The Exempt group includes all users/IP addresses that will be exempt from NetSpective's Adaptive Filtering policies. This is analogous to the Exempt Clients functionality provided in v1.1. If Exempt Clients were defined in v1.1, they will be listed as members of the Exempt group upon upgrading to NetSpective v1.2.
- b) The administrator may define additional groups (up to 256) for policies that fall outside the scope of Public/Exempt policies. Additional groups may be created from the Groups page.

Thus, depending on particular needs, the administrator need not setup additional groups beyond Public and Exempt.

Users can be entered into the system through the new Users page on the NetSpective interface by clicking on the Add button (see Figure 8). Users can be assigned into different groups by selecting the appropriate checkboxes adjacent to the user names and clicking on the Assign button.

Figure 8: Users Page



It should be noted that the Static IP option (visible in the User Add/Edit dialog, Figure 9) should be selected for users that are entered in by hand at the interface, since NetSpective does not automatically assume user ID/IP address pairs. However, the NetSpective™ Logon Agent for Microsoft Networks automatically adds users to the NetSpective system without administrator intervention. See below for more information.

Figure 9: Add User Dialog - Use Static IP option unless using the NetSpective Logon Agent

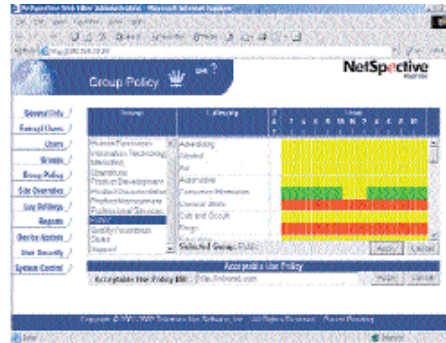


Group Policy Functionality

The improved policy functionality provides flexible daily scheduling (at the hour level) and immediate visual feedback on the policy periods for blocking, monitoring, and ignoring traffic for each group (see Figure 10).

On a category-by-category basis per user group, you can instruct Adaptive Filtering to take one of three actions to be taken on requests for URLs included in the category: “block” prohibits access (red); “monitor” allows access and logs the request (yellow); “ignore” allows access and takes no further action (green). Also on this screen you can schedule start and stop times for these actions: you can, for example, schedule the “Consumer Information” category for the Public group to be ignored from midnight through 10 a.m., monitor from 10 a.m. through 2 p.m., and ignored again from 2 p.m. until midnight. The “DAY” column is used to configure single filtering settings for the entire 24-hour period.

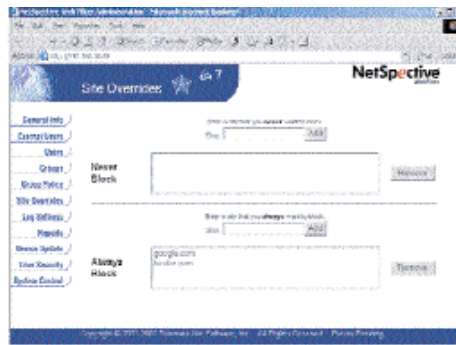
Figure 10: Group Policy Page



Site Overrides

Regardless of the Adaptive Filtering data for a site, you can elect to always block it or never block it (Figure 11).

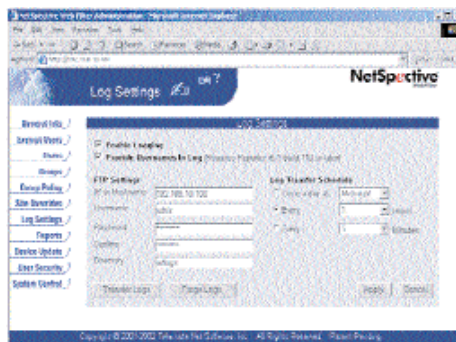
Figure 11: Site Overrides



Log Settings

Regardless of the Adaptive Filtering data for a site, you can elect to always block it or never block it (Figure 11).

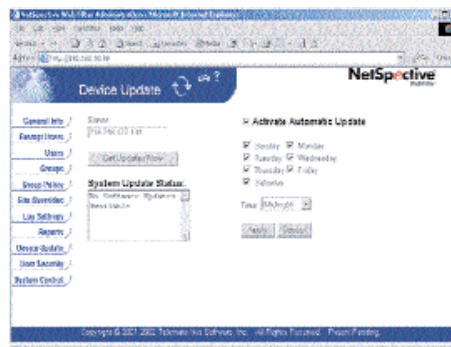
Figure 12: Log Settings



Device Update

Both site categorization data and the appliance's operating software can be updated by downloads from the Adaptive Filtering Lab. These downloads can either be initiated manually or scheduled to take place automatically on this screen (Figure 13).

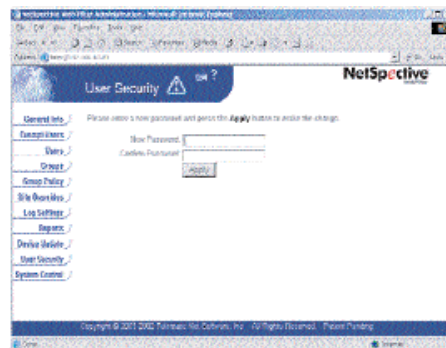
Figure 13: Device Update



User Security

NetSpective administration settings are password protected to help eliminate tampering (Figure 14).

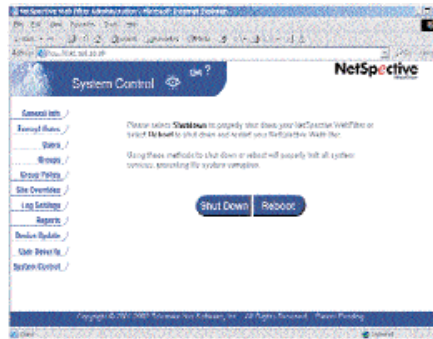
Figure 14: User Security



System Control

The off switch for NetSpective: The “Shut down” button initiates an orderly shutdown, important because it prevents corruption of important files. The “Reboot” button restarts the NetSpective to read in new categorization data or system updates (Figure 15).

Figure 15: System Control



NetSpective Block Screen

When a user attempts to access blocked content, their browser is redirected to a special HTML block page that includes a link to a user-defined Internet access policy statement. This link is configured in the Group Policy page. The page is provided in English, French and Spanish (Figure 16).

Figure 16: Block Screen

