|  |
| --- |
| Garland ISD |
| NetSpective Proposal |
| Garland ISD |

|  |
| --- |
|  |

Contents

[Executive Summary 3](#_Toc359322903)

[Deployment 4](#_Toc359322904)

[Filtering Solution 6](#_Toc359322905)

[Identifies and Blocks access to Web sites based on domain, URL pattern, key word, and content category. 6](#_Toc359322906)

[Identifies and Blocks downloads based on file type. 6](#_Toc359322907)

[Identifies and Blocks applications that access the Internet, including (but not limited to) IM, music services, and software update utilities. 7](#_Toc359322908)

[Integrates with "safe search" filters built into popular images search engines. 7](#_Toc359322909)

[Provides integrated spyware/malware protection. 7](#_Toc359322910)

[Provides Internet filtering capability for Windows PC’s, Macs, Linux devices, IOS devices, and Android devices to enforce GISD Internet policies when remote to the GISD network. 7](#_Toc359322911)

[Provides granular Internet filtering controls based on user login in directory services (eDirectory and/or AD), time-of-day, traffic volume (quotas), and IP subnet. 8](#_Toc359322912)

[Provides for policy enforcement on sites with dynamic content. 8](#_Toc359322913)

[Provides SSL decryption for SSL site evaluation. 8](#_Toc359322914)

[Provides for application blocking. 8](#_Toc359322915)

[Provides for Malware and botnet protection by blocking malicious software at the gateway. 8](#_Toc359322916)

[Provides for Web-based reporting and administration. 9](#_Toc359322917)

[Provides for the Master Database to be locally installed with support to update the Database via network/Internet. 9](#_Toc359322918)

[The database should be flexible, providing the ability to be locally modified in the form of allowed and blocked overrides to meet GISD needs. 9](#_Toc359322919)

[The database should support bulk loading of URLs/overrides. 9](#_Toc359322920)

[The database should be flexible to add/remove filters or categories. 9](#_Toc359322921)

[Should be redundant and fault tolerant. 10](#_Toc359322922)

[Should be capable of passing up to 20 gigabits of throughput. 10](#_Toc359322923)

[Should be capable of filtering as a pass-through devices and/or capable of sitting "off-to-the-side" via a spanned port. 10](#_Toc359322924)

[Should be manageable via web-based HTTP or HTTPS browser client. 10](#_Toc359322925)

[Should be capable of scanning outbound and inbound traffic. 10](#_Toc359322926)

[Should support L4 traffic monitoring & malware detection. 10](#_Toc359322927)

[Should have built-in URL filtering functionality via categories, as well as the capability to allow or block specific URLs as override. 10](#_Toc359322928)

[Should support pre-defined, undefined, and custom categories. 11](#_Toc359322929)

[Should have the capability to catch malware that attempts to bypass port 80. 11](#_Toc359322930)

[Should provide easy auto-updating of any system patches and URL categories. 11](#_Toc359322931)

[Should integrate with Novell eDirectory and Windows Active Directory and be LDAP compliant for filtering based on users, OUs, or groups. 11](#_Toc359322932)

[Should provide reporting by category, workstation, username, group membership or other criteria. 11](#_Toc359322933)

[Should provide general reports such as past activity and top users. 13](#_Toc359322934)

[Should provide reports on overall bandwidth consumed vs. bandwidth saved or other like reports. 14](#_Toc359322935)

[Pricing Options 15](#_Toc359322936)

# Executive Summary

NetSpective is a sophisticated Internet content filtering appliance 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 hosted interface provides real-time status updates and control, including compliance with federal filtering mandates and communications tracking requirements.

As a **Passive or Transparent** filter NetSpective prevents network performance degradation. 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

The signature based inspection incorporated into SideScan enables a single NetSpective appliance to scale to support unlimited users in large networks as well as distributed networks leveraging NetSpective's ability to selectively replicate policy and device settings.

Security concerns and legal liability of threats caused by remote users increase sharply as computers leave your network's border security. Malware, spyware, phishing sites, closed P2P applications like Skype and proxy avoidance tools like Ultra Surf are the typical culprits. NetSpective's Remote Agent technology enforces internet policies regardless of physical location.

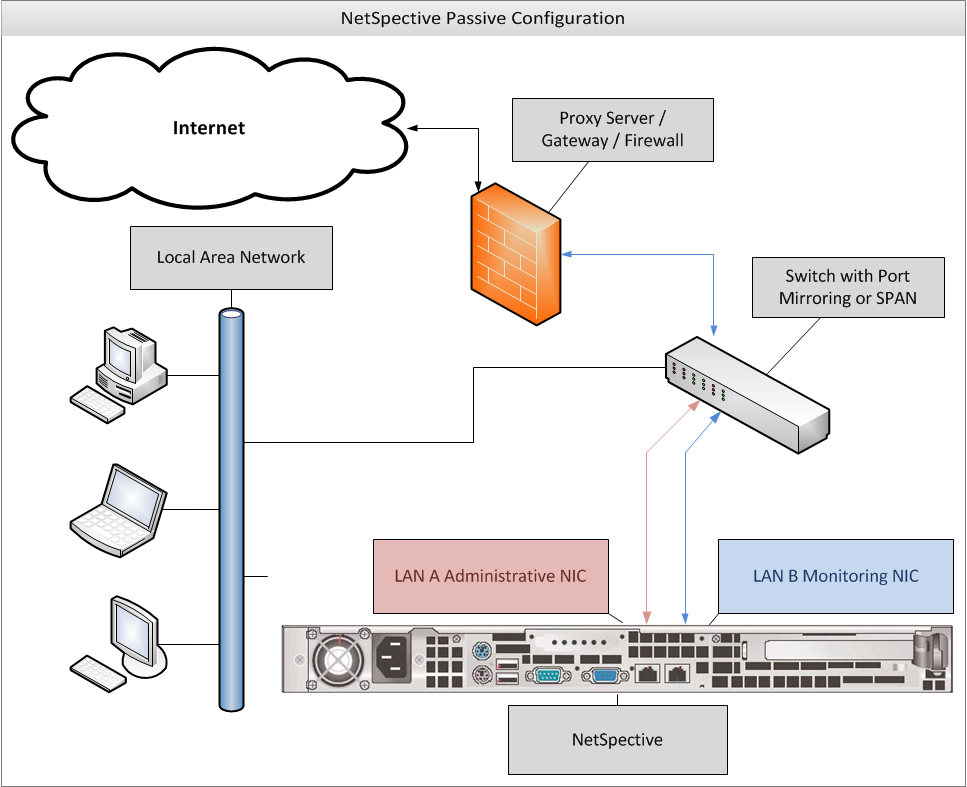
Installed at the socket level in Windows and Mac operating systems, agents protect and log all remote user Internet activity, are password protected, and provide a complete audit trail of all internet activity.

NetAuditor expands network security event management (SEM) strategies beyond basic end-point protection by accelerating the detection and automated response that leading firewall manufacturers omit in their border security offerings. NetAuditor includes automatic end-user identity association, geographic location identification by region; country; and service provider, Internet content categorization, real-time monitoring, and network event triggers.

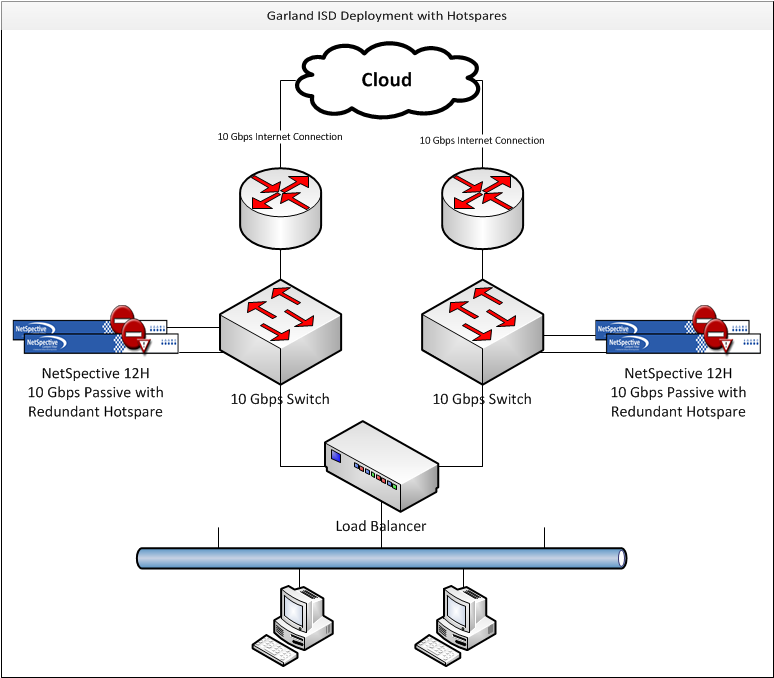
[](http://www.getnetspective.com/products/netspective/)

# Deployment

With our Passive approach, we hang off the SPAN or Mirror port of a switch monitoring all requests the internet. With this we are not a point of failure on the network and do not introduce any added latency. We do support multi-appliance load balancing and hot spare failover scenarios for redundancy.



**A typical ISD deployment consists of one NetSpective 12H 10Gbps appliance at each egress point. A second appliance at each point is usually requested as a hot-spare for redundancy.**

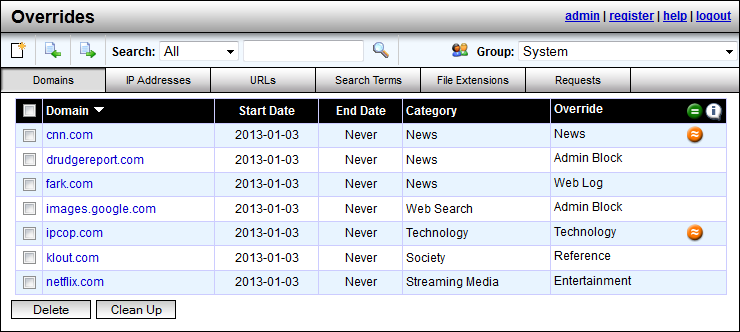
****

**The NetSpective 12H can monitor up to 10 Gbps currently. Therefore, we recommend placement of the appliance upstream to your load balancer, so that the appliance only monitors 10 Gbps of traffic at a time.**

# ****Filtering Solution****

## Identifies and Blocks access to Web sites based on domain, URL pattern, key word, and content category.

* NetSpective contains over 120 different categories that can be blocked and logged on an hourly basis.
* Overrides may be created to allow, block, or categorize specific web sites, news groups, IP addresses, URLs, web search terms, or file types. The different types of overrides are grouped together on different pages. Overrides can be imported from a simple text file as well.

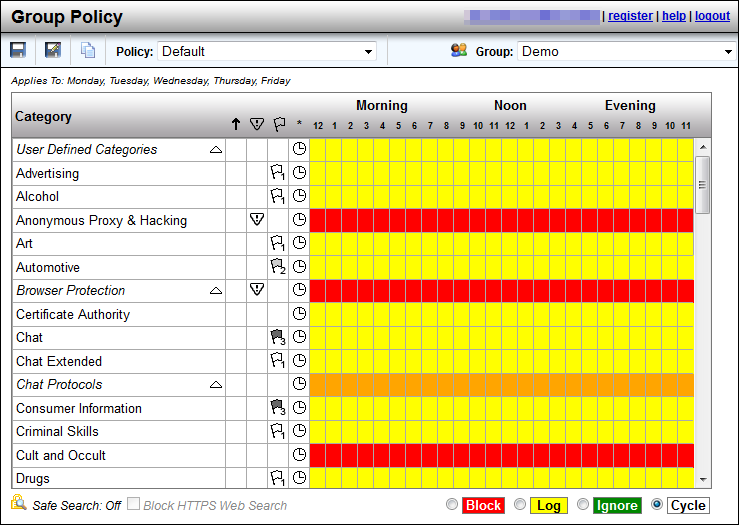


## Identifies and Blocks downloads based on file type.

* Overrides can be created to block file extensions and placed in categories for blocking.

## Identifies and Blocks applications that access the Internet, including (but not limited to) IM, music services, and software update utilities.

* NetSpective blocks applications by protocol under categories such as Chat, Peer-to-Peer, Remote Login, Streaming Media, and VoIP, and Software Updates.



## Integrates with "safe search" filters built into popular images search engines.

* NetSpective supports Safe Search enforcement for sites that support searching the Web, news groups, or indices and directories thereof. These engines will not return objectionable content or explicit pictures. Safe search options are enforced via the Web Search Filtered category for Google, Bing, MSN, Yahoo, Hotbot, Lycos, Ask, and Dogpile.

## Provides integrated spyware/malware protection.

* NetSpective Browser Protection checks for web sites attempting to interfere with normal computer functions or mislead users into providing personal information to unauthorized parties. NetSpective will enable the 'Malware' and 'Phishing' categories and configure all group policies to block these categories by default.

## Provides Internet filtering capability for Windows PC’s, Macs, Linux devices, IOS devices, and Android devices to enforce GISD Internet policies when remote to the GISD network.

* NetSpective Remote Agent technology can filter Windows, Mac, and iOS devices both on and off network. With our Global Proxy solution, we can filter any device capable of directing traffic to a proxy solution. This includes the above devices including Linux and Android devices.

## Provides granular Internet filtering controls based on user login in directory services (eDirectory and/or AD), time-of-day, traffic volume (quotas), and IP subnet.

* NetSpective can support Active Directory, eDirectory, and Open Directory. Users can be blocked by time-of-day right from the Group Policy page. Users can also be created by static IP address, or a range of addresses, which can then be placed under a filtering policy.

## Provides for policy enforcement on sites with dynamic content.

* Any website we categorized can be blocked regardless of dynamic content. Sites may contain sub domains with different categorization than the domain.

## Provides SSL decryption for SSL site evaluation.

* As a passive appliance, NetSpective does not decrypt SSL traffic. In Passive mode, NetSpective monitors the network for particular signatures much like an intrusion detection product. Since HTTPS tunnels HTTP sessions over SSL, NetSpective detects the SSL connection and takes actions based on the categorization of the HTTPS/SSL server.
* If the IP address of an HTTPS/SSL server is categorized and the policy is set to block, then all HTTPS and other SSL connections to it are blocked. Therefore, an objectionable site cannot be accessed via HTTPS (port 443 or otherwise), SSH, or any other protocol based on SSL.
* NetSpective also utilizes the adaptive filtering process for public SSL sites. When the appliance detects uncategorized SSL accesses on port 443, the site is temporarily categorized as "HTTPS Unrated" and then uploaded to the Adaptive Filtering Lab for categorization.

## Provides for application blocking.

* NetSpective monitors the protocols used by many applications that may be of concern for an educational institution. By filtering and blocking these protocols, we can effectively disable the function of applications such as: anonymous proxies, chat programs, peer-to-peer programs, remote login tools, streaming media applications, and voice over IP tools. Malware and Phishing sites are list based on our appliance. Any communication to those sites and addresses will also be blocked, halting the function of any malware on a client workstation.

## Provides for Malware and botnet protection by blocking malicious software at the gateway.

* NetSpective blocks sites that attempt to interfere with normal computer functions and/or send personal data about you to unauthorized parties over the Internet. We also block sites that impersonate another site in an attempt to mislead you into providing personal information. These sites are located in our Browser Protection category which contains the sub categories Malware and Phishing.

## Provides for Web-based reporting and administration.

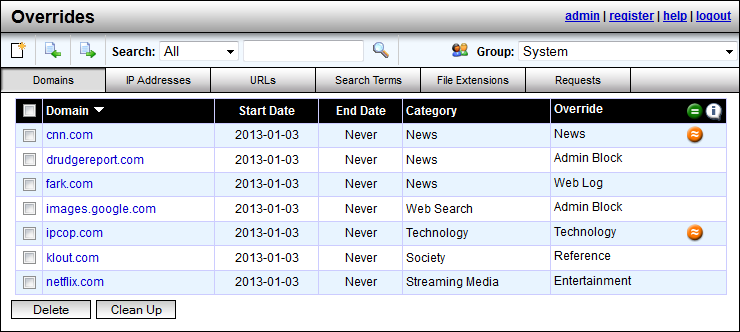
* The NetSpective administration is fully web based. Also, provided for free with our NetSpective Content Filtering is our [NetAuditor Security Event Manager](http://www.telemate.net/products/netauditor/). NetAuditor expands network security event management (SEM) strategies beyond basic end-point protection by accelerating the detection and automated response that leading firewall manufacturers omit in their border security offerings. NetAuditor includes automatic end-user identity association, geographic location identification by region; country; and service provider, Internet content categorization, real-time monitoring, and network event triggers.

## Provides for the Master Database to be locally installed with support to update the Database via network/Internet.

* Database is contained on the appliance which is locally installed. Updates are downloaded nightly at midnight, which can be changed by the administrator.

## The database should be flexible, providing the ability to be locally modified in the form of allowed and blocked overrides to meet GISD needs.

* Overrides may be created to allow, block, or categorize specific web sites, news groups, IP addresses, web search terms, or file types. The different types of overrides are grouped together on different pages.



## The database should support bulk loading of URLs/overrides.

* Overrides can be imported from a simple text file.

## The database should be flexible to add/remove filters or categories.

* NetSpective has over 120 Categories that can be enabled or disabled, including the creation of custom categories.

## Should be redundant and fault tolerant.

* There are three replication roles that NetSpective supports. They are Stand-Alone, Parent and Child. Devices that are not part of a replication group should have a role of "Stand-Alone" and are managed individually. Otherwise, devices that are part of a replication group should have a role of "Parent" or "Child". Users, groups, policies, and other configuration settings are managed centrally on a parent device and are automatically pushed to all of its child devices. A child device should have only one parent device. A NetSpective device in Child mode does not let you edit any settings that are replicated to it by its parent. These replicated settings are hidden from the administration web interface. These clustering modes give the customer a range of ‘hot spare’ modes for failover or load balancing.

## Should be capable of passing up to 20 gigabits of throughput.

* As shown in the Deployment topic, we would deploy two 10 Gbps appliances at the core, one for each 10 Gbps egress point.

## Should be capable of filtering as a pass-through devices and/or capable of sitting "off-to-the-side" via a spanned port.

* With our Passive approach, we hang off the SPAN or Mirror port of a switch monitoring all requests the internet.

## Should be manageable via web-based HTTP or HTTPS browser client.

* The Web Administration can be accessed from any web browser via HTTP or HTTPS.

## Should be capable of scanning outbound and inbound traffic.

* NetSpective scans both outbound and inbound traffic. Any traffic passing by the mirror port on the switch will be seen by NetSpective.

## Should support L4 traffic monitoring & malware detection.

* NetSpective supports protocol level filtering of traffic and inspects all packets across all ports. NetSpective blocks sites that attempt to interfere with normal computer functions and/or send personal data about you to unauthorized parties over the Internet. We also block sites that impersonate another site in an attempt to mislead you into providing personal information. These sites are located in our Browser Protection category which contains the sub categories Malware and Phishing.

## Should have built-in URL filtering functionality via categories, as well as the capability to allow or block specific URLs as override.

* Overrides may be created to allow, block, or categorize specific web sites, news groups, IP addresses, web search terms, or file types. URLs can also be placed in user defined categories.

## Should support pre-defined, undefined, and custom categories.

* Our list of 120 categories includes pre-defined, “Not Rated” or undefined, as well as 20 or more user defined “custom” categories.

## Should have the capability to catch malware that attempts to bypass port 80.

* NetSpective blocks sites that attempt to interfere with normal computer functions and/or send personal data about you to unauthorized parties over the Internet. We also block sites that impersonate another site in an attempt to mislead you into providing personal information. These sites are located in our Browser Protection category which contains the sub categories Malware and Phishing. NetSpective will detect this traffic across all ports.

## Should provide easy auto-updating of any system patches and URL categories.

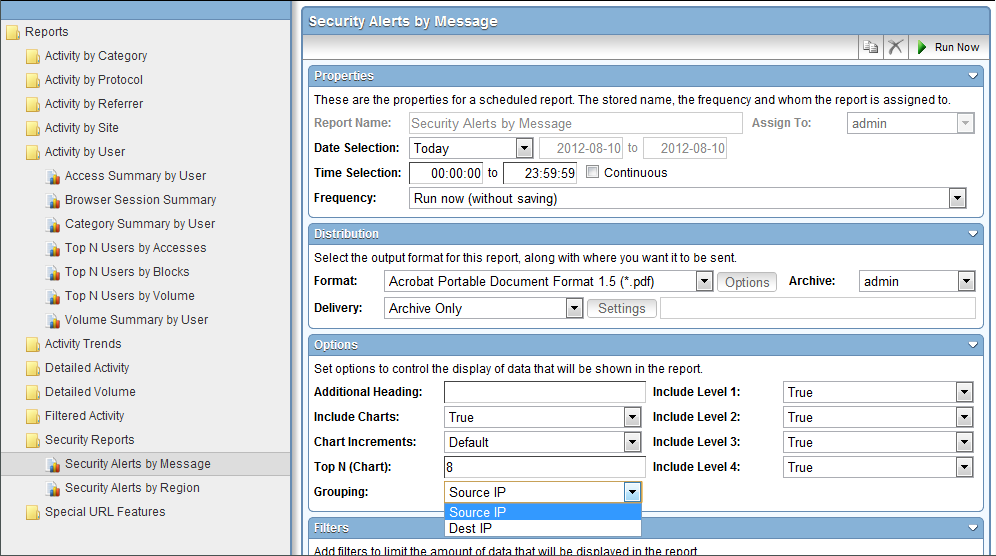
* NetSpective patches and category updates are automatically downloaded each night. Any major software updates are downloaded, but must be applied manually. This is due to the time for an appliance to install the update and reboot, which is expected to take approximately 2 minutes.

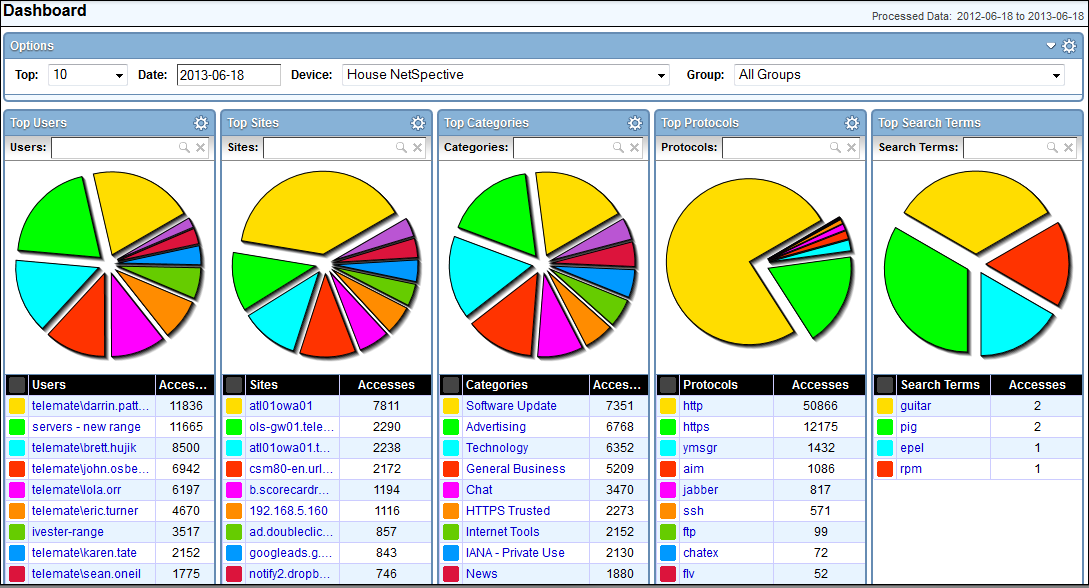
## Should integrate with Novell eDirectory and Windows Active Directory and be LDAP compliant for filtering based on users, OUs, or groups.

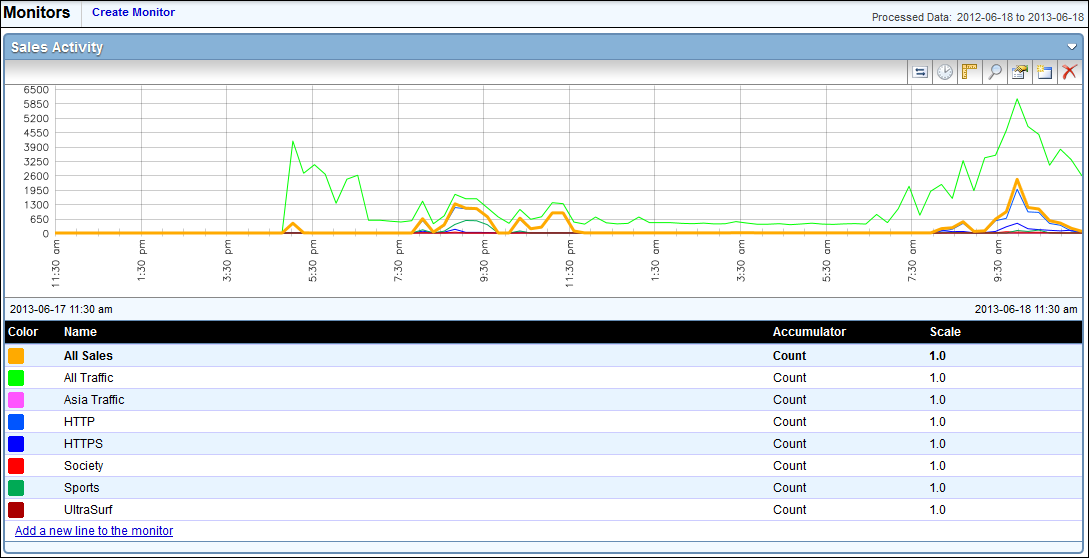
* NetSpective can support Active Directory, eDirectory, and Open Directory. We typically only require user access to the directory, not admin rights. The appliance can support any number of LDAP sources as well as any combination you wish to use together.

## Should provide reporting by category, workstation, username, group membership or other criteria.

* For more comprehensive information NetAuditor provides on-demand and automated reporting. Perhaps you found something in the dashboard you need more detailed information on. Perhaps you need more comprehensive summary/bandwidth reports, reports on firewall security alerts, traffic trends over time, or you want a PDF automatically generated every night/week/month for you to review. NetAuditor reporting provides several views to assist in managing reports and provides secured access.
* Configuring reports enables an end-user to run, save, or schedule a new report. It will show you a list of all available report templates, which will be grouped by report categories. Properties exist for distributing via Email and FTP, and export formats include PDF, XLS, and HTML.
* Filters are important to consider when configuring a report. If you have multiple groups or classrooms and you only want to see the data logged by one of them, specifying a filter on that group will make the report run faster and will make the resulting report smaller. When running detail reports, you could end up with a report that is too large to open. Omitting data from categories you aren’t interested in such as advertisements or society plugins will make your reports cleaner, only showing you the information you’re interested in seeing. This makes it easier to narrow down what a student has been surfing without having to waste time sifting through useless data. With over 40 reports and countless combinations of filters, you’ll always be able to narrow down your search to find the information you need.







## Should provide general reports such as past activity and top users.

* NetAuditor Security Event Manager contains over 40 reports ranging from Top N users/categories/sites/protocols, Chronological Detail, Security Alerts, Browser Session, Trend Analysis, Search Phrases, and Volume reports.

## Should provide reports on overall bandwidth consumed vs. bandwidth saved or other like reports.

* NetAuditor can report on firewall logs to view Netflow statistics, various bandwidth reports, GoIP data, and Security Alert Messages.

# Pricing Options

With NetSpective any user count over 10,000 is considered an unlimited license subscription. You will see the pricing broken down into Licensing, Hardware and Annual Renewals. The total price includes:

* Licensing for an unlimited number of users.
* A quantity of 4 10 GIG Appliances- the warranty and maintenance is included for each appliance.
* NetAuditor, our Reporting tool that offers a variety of reports including real-time dashboards and monitors with alarming notifications is included in the price.
* Remote Agents that can be installed on any laptops allowing you to filter them off the network.
* Support- you will have access to our support team from the day you purchase. A member of our team will walk you through the deployment and make sure that it is set up and running the way you want it to. Through out the duration of your contract you will have access to our support team 24x7. They have the ability escalate issues to our Engineer team if needed.

**Below you will see Option 1. This is to purchase one year at a time. I have outlined the price for year one and then each additional year if purchased at the end of the contract year.**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Option 1: Year to Year | | | | |
| SKU | **Product** | **Price** | **Quantity** | **Year 1 Price** |
| NWHWNPULM | NetSpective Content Filter | $ 40,000.00 | 1 | **$ 40,000.00** |
|  | Unlimited Licenses |  |  |  |
| NWH1BHTSP10G | NetSpective 10 GIG Appliance | $ 7,500.00 | 4 | **$ 30,000.00** |
|  | Includes Hardware Maintenance and Warranty |  |  |  |
|  |  | **Year One Price** | | **$ 70,000.00** |
|  | | | | |
| NWHWNPULMRNWL | NetSpective Content Filter Renewal | $ 25,500.00 | 1 | **$ 25,500.00** |
|  | Unlimited Licenses |  |  |  |
| NWH1BHTSP10GRNWL | NetSpective 10 GIG Appliance Annual Renewal | $ 3,500.00 | 4 | **$ 14,000.00** |
|  | Includes Hardware Maintenance and Warranty |  |  |  |
|  |  | **Annual Renewal** | | **$ 39,500.00** |

**Below you will see Option 2. This is to purchase 3 years upfront. By choosing the multi-year contract you will save a total of $16,000.**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Option 2: 3 Year Contract | | | | |
| SKU | **Product** | **Price** | **Quantity** | **Year 1 Price** |
| NWHWNPULM | NetSpective Content Filter | $ 30,000.00 | 1 | **$ 30,000.00** |
|  | Unlimited Licences |  |  |  |
| NWH1BHTSP10G | NetSpective 10 GIG Appliance | $ 7,500.00 | 4 | **$ 30,000.00** |
|  | Includes Hardware Maintenance and Warranty |  |  |  |
|  |  | **Year One Price** | | **$ 60,000.00** |
|  | | | | |
| NWHWNPULMRNWL | NetSpective Content Filter Renewal | $ 22,500.00 | 1 | **$ 22,500.00** |
|  | Unlimited Licences |  |  |  |
| NWH1BHTSP10GRNWL | NetSpective 10 GIG Appliance Annual Renewal | $ 3,500.00 | 4 | **$ 14,000.00** |
|  | Includes Hardware Maintenance and Warranty |  |  |  |
|  |  | **Year 2 Renewal** | | **$ 36,500.00** |
|  | | | | |
| NWHWNPULMRNWL | NetSpective Content Filter Renewal | $ 22,500.00 | 1 | **$ 22,500.00** |
|  | Unlimited Licences |  |  |  |
| NWH1BHTSP10GRNWL | NetSpective 10 GIG Appliance Annual Renewal | $ 3,500.00 | 4 | **$ 14,000.00** |
|  | Includes Hardware Maintenance and Warranty |  |  |  |
|  |  | **Year 3 Renewal** | | **$ 36,500.00** |
|  | | | | |
|  |  | **Total Price for 3 Years** | | **$ 133,000.00** |
|  |  | **Savings with Option 2** | | **$ 16,000.00** |