# The scope of qualified product features and deliverables are as follow

## a) Product must support a global proxy to filter devices when they are not on the West Bend

## School District Network. Must work with iPads, Chromebooks. OSX, Windows Tablets,

## Windows Laptops, Android Devices, IOS.

**Yes. As a separate appliance that scales independently, the NetSpective Global Proxy is capable of filtering any device on or off the network. Devices such as iPads and Chromebooks that suspend applications or revert their image when restarted cannot be filtered with traditional agents. The Global Proxy can direct all traffic these devices generate back onto the network to ensure that school owned devices are filtered at home. The Global Proxy solution is compatible with iPads, Chromebooks. OSX, Windows Tablets,**

**Windows Laptops, Android Devices, IOS.**

b) Product must be able to support 10G connectivity and be able to scale up to multiple Gigabit or larger external connections.

**Yes. The NetSpective 12H is equipped with a 10 Gigabit NIC, Ethernet or Fiber Optic, and can scale to a fully saturated 10 Gbps with a single appliance.**

c)Product must be able to meet the requirements of federal and state laws including CIPA.

**Yes. NetSpective is the only CIPA-compliant URL filtering appliance that prevents access to both P2P sites and P2P applications, effectively ensuring the safety and security of a school or library's network.**

d) Product must have a fail over ability in the event of a hardware failure.

**Yes. All NetSpective solutions have the capability to be configured with failover redundancy.**

e) The solution should provide a means of redundancy or fail-over. Filtering services must not be degraded while the solution is in a redundant or failed-over-state.

**Yes. Solutions can be paired up to provide failover redundancy. Filtering services will not be degraded in any way when in a failover state.**

f) Inline solutions must provide fail-over capability such that the filtering device does not block network traffic in the event of loss of power, crash, or other failure.

**Yes. Our Passive solution fails open without blocking network traffic. Our Proxy solution is capable of deploying with failover capabilities so that network traffic is not blocked.**

g) A bypass/transparent mode filtering solution is preferred, but inline solutions will be considered.

**Yes. Our Passive appliance acts in a bypass mode, monitoring all requests to the internet. Our Proxy solution is deployed transparent to user workstations.**

h) Product should be able to load balance multiple external internet connections or a recommendation made on how externally load balance multiple (more than 3) ISP’s.

**Yes. With our passive solution, we do not impact the performance of network traffic, so load balancing isn’t necessary. Our proxy solution can be configured for load balancing as well.**

i) Product installation and integration will take place no later than August 26 th.

**Yes. The solution can be installed and configured in about 30 minutes. Our entire solution can be easily deployed by August 26th.**

j) Product must be able to support filtering by groups in Active Directory and/or SSID’s WLAN connections in the school.

**Yes. NetSpective has full AD integration, identifying users by their AD credentials. We can also identify any user on your Wi-Fi network (SSID) in various ways. Wi-Fi integration can also identify users by AD credentials.**

k) Product must be able to complete the internet/content filtering without having any effect on the speed, reliability or performance of the network and internet connection.

**Yes. Our Passive and Proxy configurations do not affect the speed, reliability, or performance of the network.**

l) Product must be able to integrate with both Aerohive and Cisco Wireless Systems

**Yes. We can integrate with both Aerohive and Cisco Wireless Systems. The NetSpective Wi-Fi agent is capable of binding DHCP and Access Control Server log files to inject user identification directly into NetSpective. This is done in real time without any authentication presented to the end user.**

m) Product must be able to allow for historical reporting/tracking of internet traffic by user up to one year.

**Yes. Our NetAuditor Security Event Manager is Windows based software that can be installed on any server, VM, or desktop. Any amount of hard disk space can be allocated, allowing you to keep logs for one year or more.**

n) Allow access to YouTube for EDU even if access to the overall YouTube site is blocked. Ability to allow staff full access to YouTube while filtering content and comments.

**Yes. NetSpective’s YouTube for Schools features can limit YouTube content to only educational content specified by YouTube for EDU or the account holder. NetSpective will also allow full YouTube access to staff while filtering content and comments.**

o) Allow for definition of specific blocked or allowed URLs. These can be specified down to the individual page level.

**Yes. Overrides can recategorize domains, IPs, URLs, search terms, , newsgroups, and file extensions. URL overrides can be used to specify an individual web page level.**

p) Allow for the unblocking of specific web ports (not 80 or 443).

**Yes. NetSpective’s passive based solution works independently from all ports and can meet this requirement.**

q) Allow for the ability to not cache specific websites.

**Yes. NetSpective will not cache websites specified by the administration.**

r) Allow override entries to be added on the fly without requiring restart of the system. If a library, list, or group must be recompiled or reloaded for the added override to take effect, filtering must continue while the reload is occurring.

**Yes. Overrides do not require a restart of the appliance system and are in effect immediately.**

s) The page used to display block information should be customizable. It must be capable of displaying the URL that was blocked, time, date, the IP and username it was coming from and the reason that it was blocked.

**Yes. The block page is fully customizable. You can specify URL that was blocked, time, date, the IP, username, and add custom script to the block page.**

t) Allow specified users or IP addresses to bypass any or all predefined categories and any custom entries.

**Yes. There are multiple ways of exempting users from any and all traffic. The Exempt group will allow the users or IP addresses to go unfiltered. Any group can have their policy customized to do the same.**

## u) The system must allow the configuration settings, including custom override lists, to be backed up both manually and on a scheduled basis. It must be possible for the backup set to be copied automatically to a remote server via FTP or SSL. It should also be possible for the backup to be downloaded to the administrator’s PC.

**Yes. Full system settings can be backed up, both manually or periodically over FTP.**

## v) The product must be able to be managed remotely from a browser-based interface.

**Yes. The administration web interface can be accessed anywhere on network or off network, and can be secured through HTTPS.**

w) The management solution should allow the settings made on one unit to be easily replicated to the other unit(s), preferably automatically.

**Yes. All appliances that are deployed can be paired through Replication. Replication will mirror all settings except for network settings. All management can be done through one interface without having to make changes on each appliance.**

x) Provide automatic updates to predefined categories on at least a daily basis.

**Yes. NetSpective categorization updates occur nightly and automatically. However, due to sensitive sites such as Anonymous Proxy and Hacking or Pornography changing on a day to day basis, we utilize a feature referred to as our Micro Updates. With this, unknown websites that are detected by the NetSpective appliance are sent back to TeleMate.Net for evaluation. TeleMate.Net’s web crawler will then categorize the URL and send it back out to all NetSpective Appliances in distribution every 10 minutes. This gives each customer the benefit of learning from our entire customer base.**

y) Force non-SSL safe search and translate for students.

**Yes. NetSpective can enforce non-SSL safe search and translate for popular search engines such as Google and Bing.**

## z) Monitor and provide capability to block URLs in the predefined lists and those specified manually by the administrator. These should be acted upon whether HTTP or HTTPS protocol is used.

## Peer-to-peer traffic, including voice services such as Skype

## Instant messaging traffic

## Streaming video

## Access to anonymous proxy servers, such access should be detectable based on traffic patterns as well as by URL list.

## Access to weblog/chat sites frequented by students, such as Facebook. It is preferred that such sites be categorized separately from general weblog sites maintained by journalists, celebrities, political commentators, etc.

## VPN and RDC

**Yes. NetSpective can detect and block Peer to Peer traffic, Skype, IM, Streaming Media, Anonymous Proxies, Chat, Society sites such as Facebook, Web Log, and Remote Login protocols such as VPN. Anonymous Proxies are updated every 10 minutes, both signature based and from our proprietary web crawlers that analyze website traffic patterns.**

# 2)System Feature Questions

If the proposed solution includes multiple active units (appliances/servers), the Contractor must specify how these units are to be deployed, load balanced, etc.

**TeleMate.Net Software proposes one 12H 10Gbps Passive appliance and one 12H 10Gbps Global Proxy appliance. Appliances will be configured in Replication mode to mirror all settings and provide one management interface. Any requested failover appliances can be purchased and deployed at a later time.**

The District might want to be able to decrypt HTTPS traffic. Such decoding should be category-based so that the administrator can exempt categories such as banking sites from decoding. The Contractor should note if this feature is available. If it is an extra-cost option, it should be proposed as an addendum to the contract and not in the main body of the response.

**Yes, our HTTPS traffic decryption methods allow for exempting certain types of traffic. Finance and Banking sites will be exempt from all SSL traffic decryption.**

How often is the URL Content filtering, list updated?

**The URL content filtering list is updated once a night, as well as “micro updates” every 10 minutes.**

Is the proposed solution CIPA complaint? **Yes**

Specify software and/or firmware Update interval **Quarterly**

Specify filter list update interval **Nightly and every 10 minutes**

Number of categories/classes/groups classified **Over 120**

Are all categories included in basic price? **Yes**

Attach category list **Check ( See Page 38 )**

Approximate size of URL database **302 Million, expandable to 2 Billion from our providers**

Describe (separate documents) methods and supporting hardware for:

URL filtering **Check, Page 15**

SSL filtering **Check, Page 16**

Describe file type blocking **Check, Page 21**

Image search or image site blocking **Check, Page 16**

Is a proxy necessary for solution operation **No**

Does the product have a Global Proxy that allows for filtering of devices of the district’s network? Please explain how it works with iPads, Chromebooks, Android, OSX, Windows Tablets, Windows laptops, IOS.

**Yes, Page 28**

Are other protocols filtered and if so attach list. **Yes, Page 17 and 18**

Can streaming protocols be blocked separately in different categories? **Yes**

Are file downloads in instant messaging blocked separately from messaging services? **Yes**

Is malware/grayware/adware blocked and if so attach a list **Yes, Malware and Phishing**

Describe URL redirect page options. **Yes, Page 22 and 23**

Describe browser, end user workstation hardware/software and configuration requirements, and platforms supported. **NetSpective supports all web browsers. Special end user software/hardware is not necessary for filtering. Supports Windows, Mac OS X, Terminal Servers, iOS, Android, and Chrome.**

Does your product require a client or App to achieve filtering? **No**

Does the product support filtering based on IP address range and user authentication? **Yes, IP and LDAP Authentication**

Specify user authentication methods such as (AD, LDAP) supported. **Active Directory, eDirectory, Open Directory, or Local Machine Name/Local User Name.**

Describe override options of the filtering. **See attached overview**

Does the product support custom site block/allow lists by IP address range and/or group policy. **Yes. By Domain, IP, URL. Can be applied based on date, system, group, or user.**

Number of custom categories supported **20 by default, expandable on request.**

Is distributed administration supported? **Yes**

Describe Hardware Features (complete as necessary) **See Page 47**

Describe hardware redundancy options **See Page 13 Policy Replication**

List support hours and methods included in solution price (24x7 support required) **Support phone line hours 8am – 6pm EST, email 24/7**

Describe product warranty, equipment replacement in the event of a failure and cost packages for support. **Page 37**

Explain options for technical contacts for customer support. **Customers can contact our support line via phone or email. Phone or email contact with sales engineer and sales manager will also be provided.**

Can you copy or migrate current filtering criteria into the proposed product? If yes, please explain. **Yes. Category Overrides, Groups, and Users can be imported via .txt or .csv file.**

Does the proposed solution support the following reporting options:

Is distributed reporting supported? **Yes**

Can you schedule reports that are e-mailed to specific staff members? **Yes**

List standard reports **See Page 50**

Describe custom report options available. **See Page 32**

How far back can historical data be reported within the proposed solution? **Historical reporting software is provided. Data can be reported on as far back as the amount of logs you store and the hard disk space you provide the software.**

Can you go back further into historical data by accessing information from a Syslog? **Yes**

# NetSpective Content Filter

**Overview**



[](http://www.telemate.net/)

[**View a visual presentation of the product on our website**](http://www.telemate.net/products/netspective/training_videos.php)

**Company Background**

TeleMate.Net Software is a global leader in providing scalable network monitoring and security solutions. Our product families including, TeleMate™ Unified Call Management, NetSpective™ Content Filter, and NetAuditor™ Event Manager are considered products of choice for many Federal, State, Local, Educational, and Fortune 1000 institutions.

TeleMate.Net Software is proud to highlight our accomplishments as delivering easy to use, fully automated, highly reliable and lowest total cost of ownership solutions in the industry. TeleMate.Net Software accomplishes this by listening to customers and delivering scalable solutions to the IT professional that is being stretched. These tools increase productivity, allowing the IT professional do more with less, enabling ROI measured in months in many cases. Organizations of all sizes use TeleMate.Net Software products to help control and recover network costs, improve employee productivity and enhance network security. Every customer is a reference customer.

Since 1986, TeleMate.Net Software has evolved its core reporting technology, incorporating the latest advances in database, reporting, user-interface, and categorization technologies, to become the dominate force in addressing telecommunications administrators core requirements for Unified Call Management. In 1996, TeleMate.Net Software extended the company's market presence by introducing the world's first patented integrated voice and data reporting platform for monitoring PBXs, voice managers, firewalls, intrusion detection sensors, web servers, and mail servers. Continuing our leadership position TeleMate.Net Software introduced NetSpective™ Content Filter in 2001 as the need for real-time enforcement of network usage policies became evident. Today, innovation continues with complete integration into directory services and real-time notification and reporting.

Since the original inception of TeleMate.Net Software the company has over 18,000 installations worldwide. The success of the technology TeleMate.Net Software develops and services has been driven by recognizing trends and providing solutions that seamlessly integrate with technology from leading manufacturers including but not limited to Cisco Systems, AVAYA, Nortel, NEC, Siemens, ShoreTel, Asterisk, Microsoft, Symantec, Juniper Networks, Check Point Software, and Novell.

Our ability to listen and respond rapidly to customers' requirements and specifications has earned a credible and solid reputation amongst our customers. Our customers have told us the level of customer service they receive is second to none. Our 'top down' approach to the market is to make every customer a reference account by listening and then delivering scalable, feature rich solutions that are easy to use.

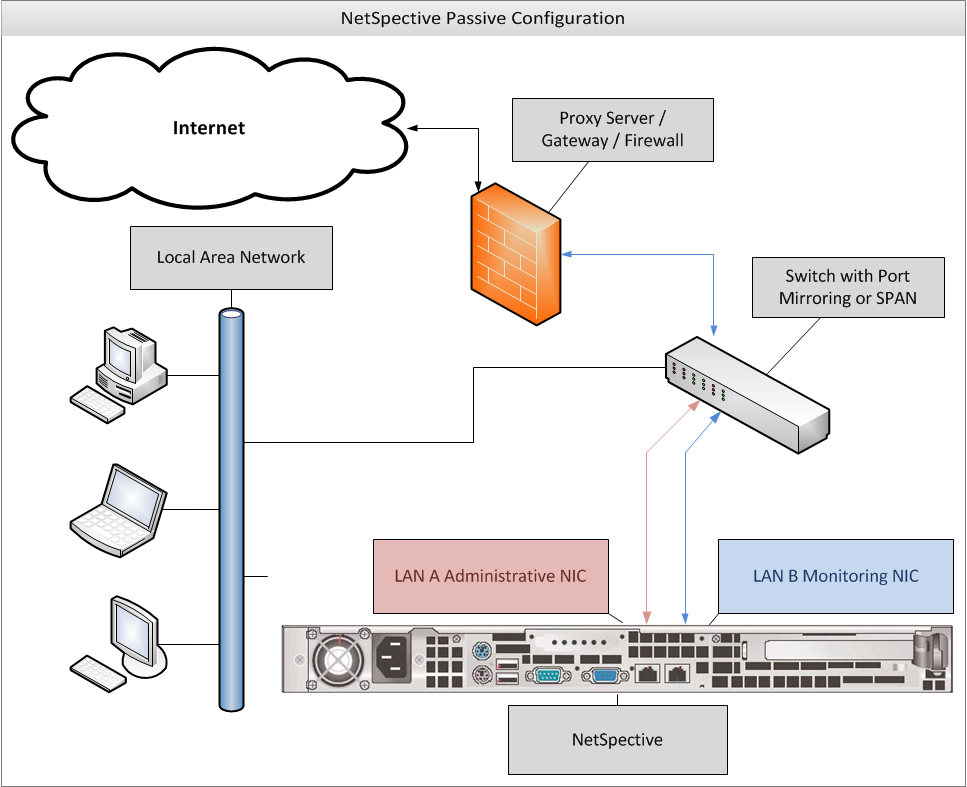
TeleMate’s product families include: TeleMate™ Unified Call Management, NetSpective™ Content Filter, and NetAuditor™ Event Manager.

**Deployment**

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.

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.



**Scalability**

NetSpective’s 12Q chassis is equipped with a quad core Intel processor and can scale to an unlimited number of users. We can provide further scalability through our 12H chassis, which can scale to 10 Gbps. The 12H is equipped with a hex core processor and a redundant power supply.

|  |  |  |  |
| --- | --- | --- | --- |
| Solutions | Number of Concurrent Users Supported | Bandwidth Capacity | Network Interface Types Supported |
| NetSpective Passive 12D Appliance | 250 users up to 5000 concurrent users | 1Gig Bandwidth | Ethernet |
| NetSpective Passive 12Q Appliance | Unlimited Users | 1Gig Bandwidth | Ethernet |
| NetSpective Passive 10 Gig 12H Appliance | Unlimited Users | 10Gig Bandwidth | Ethernet or Fiber Optic Interface |

**Policy Replication**

If more than one appliance is needed, Policy Replication mirrors all policy settings from one appliance to the rest, automatically. One appliance is set to ‘Parent’ and the others are all set to ‘Child’. Policy changes are then replicated across all ‘Child’ appliances. With this feature, you only have to manage one web interface. Settings never need to be changed on the ‘Child’ appliances. Passive appliances can be deployed as a hot spare for failover. Proxy appliances can be deployed in failover or load balancing modes.

**CIPA Compliance**

CIPA requires schools and libraries with computer Internet access to certify that they have Internet safety policies and technology protection measures, e.g., software filtering technology, both on and off network, to receive discounts for Internet access and internal connections under the schools and libraries universal service support mechanism.

NetSpective® is the only CIPA-compliant URL filtering appliance that prevents access to both P2P sites and P2P applications, effectively ensuring the safety and security of a school or library's network.

The NetSpective Solution is highly flexible and easily customizable; with a database that includes over a million URLs grouped into over 120 categories that is dynamically updated to provide the most accurate and current information available. It easily lets you monitor, block or report on:

• URL visits

• Use of streaming media and audio files, and their Web sites

• Use of Peer-to-Peer File sharing

• Use of Instant Messaging and other online chat applications

NetSpective also allows users to apply Internet access policy by class, section, grade, school, or individual workstation, both On network and Off network; allowing access to a children's reading room different than the adult reading room for example.

NetSpective's centralized management console offers several options to disable filtering, including exempting specific workstations, modifying filtering rules by time of day, etc.

The NetSpective Solution allows schools and libraries to:

• Facilitate CIPA compliance

• Control Web site access by images and text content

• Tailor access policies from group to individual workstations

• Easily modify policies to meet patron's needs

• Centrally manage polices from a single console

• Block Peer-to-Peer File sharing and Instant Messaging applications

• Prevent access to streaming media that can put a drag on bandwidth resources

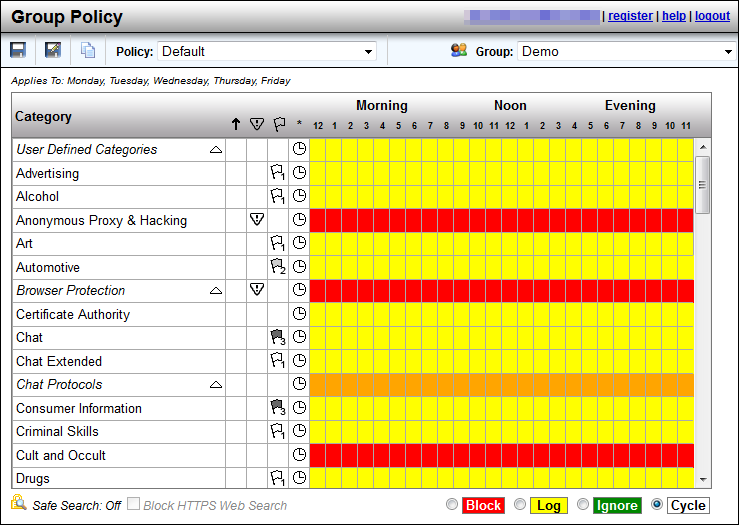
• Filter users both On network and Off network

• Manage One to One, as well as BYOD initiatives

**Categories & Granular Policy Control**

NetSpective was designed for the K12 market. The appliance contains over 120 different categories, including education specific ones. Some of our most popular K12 categories include: Alcohol, Anonymous Proxies & Hacking, Chat, Criminal Skills, Cults & Occult, Drugs, Hosting Site, Lingerie, Mature Content, Pornography, Sexual Advice, Society (Facebook), Society Plug-ins, Streaming Media, Tobacco, Violence, Weapons, Web Log (Blog)….and many more. (Appendix A contains a full list and definitions)

Each user group and/or IP subnet has the ability to block traffic utilizing our pre-defined or customized categories and specific sites by day-of-the-week and time-of-day. A full CIPA group policy profile comes pre-defined out of the box for easy implementation.



**Categorization**

NetSpective handles categorization in several ways. We use category lists from a number of different vendors. We realize that each vendor has its strengths and weaknesses from one category to the next, thus we pick and choose which lists we use from each vendor.

For more sensitive and ever changing sites, we have proprietary web crawlers constantly searching the internet and evaluating each website. Due to sensitive sites such as Anonymous Proxy and Hacking or Pornography changing on a day to day basis, we utilize a feature referred to as our Micro Updates. With this, unknown websites that are detected by the NetSpective appliance are sent back to TeleMate.Net for evaluation. TeleMate.Net’s web crawler will then categorize the URL and send it back out to all NetSpective Appliances in distribution every 10 minutes. This gives each customer the benefit of learning from our entire customer base.

Lastly, any category overrides a customer makes on their appliance is communicated back to TeleMate.Net. TeleMate frequently has human eyes combing over these customer overrides and evaluating their category listing. If we make any changes to these websites, those changes will be reflected in the Overrides section of the product so you may see what we agreed upon or disagreed with. Any URLs that we changed to match your overrides can be cleared out easily with the ‘clean up’ button so the administrator does not have to review them.

**HTTPS-Adaptive Filtering**

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.

The NetSpective Adaptive Filtering Lab will categorize the site based on the following criteria:

* If the site's SSL certificate is invalid, self-signed, or signed by an untrusted certificate authority, then the site will be categorized as "HTTPS Untrusted".
* If the site's SSL certificate is valid, signed by a trusted certificate authority, and the site cannot be categorized, then the site will be categorized as "HTTPS Trusted".
* If the site's SSL certificate is valid, signed by a trusted certificate authority, and the site can be categorized, then the site will be categorized as a specific category (for example, "Mature Content"). Thus, blocking "Mature Content" would block HTTP and HTTPS traffic to the site.

This method of filtering is global on every appliance. However if you choose, you can enable or disable the following categories on a group by group basis.

* HTTPS Trusted
* HTTPS Untrusted
* HTTPS Unrated

**Safe Search**

NetSpective supports Safe Search enforcement for sites that support searching the Web, Images, 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.

**User Defined Categories**

The admin can also set up ‘User Defined Categories’. These are categories which you can create yourself and populate with anything you wish through the use of the ‘Overrides’ section of the product. By default, a maximum of 20 categories may be created.

**IPv6**

NetSpective supports all major protocols over IPv6. The appliance runs on a dual stack, supporting both IPv4 and IPv6 simultaneously. Only protocols that do not support IPv6, such as Skype, are not supported on our dual stack platform.

**Peer-to-Peer Protocols**

Peer to Peer protocols, such as Ultra Surf and TOR are included in our protocol filtering. *Skype* is filtered as a streaming media protocol and can be allowed or block per the users policy.

**Peer-to-Peer Protocols**

Ares

BitTorrent

Direct Connect

EDonkey

Freegate

Gnutella

Kazaa

Napster

Pando

Piolet

The Onion Router

Ultra Surf

WinMX

**Chat Protocols**

All Instant Messaging and Chat are blocked or allowed underneath our ‘Chat’ protocol.

**Chat Protocols**

AOL

ICQ

IRC

Jabber

MSN

MySpace

Yahoo

**Streaming Media**

Streaming Video is categorized under our ‘Streaming Media’ category. NetSpective categories both ‘Streaming Media’ and ‘Streaming Internet Radio’ separately, allowing for more granular control.

**Streaming Internet Radio**

Sites that transmit audio in real-time (i.e., as the information is received).

<http://www.pandora.com/>

<http://www.shoutcast.com/>

**Streaming Media**

Sites that stream audio and video on demand.

<http://www.youtube.com/>

<http://www.hulu.com/>

**Streaming Media Protocols**

Flash

QuickTime

Real

Skype

Slingbox

Winamp Shoutcast

Windows Media

**Society vs Blogs**

Sites like Facebook and Twitter are categorized separately from sites like Blogger. You will find social media websites like Facebook in the Society category. Blogging websites are then categorized as Web Log. We have also gone a step further to place Society Plugins in their own separate category. This allows you to prevent users from “liking” every page they visit, or omitting the useless data from your reports.

**Society**

Sites that provide information on matters of daily life including sites that contain material relative to an individual's personal life, whether straight, gay, lesbian, or otherwise; any site pertaining to any particular culture, behavior, organization, society, club, etc.

https://www.facebook.com/

<https://twitter.com/>

**Society Plugin**

Examples such as ‘Like’ buttons, Google+ ‘+1” buttons, and ‘Share on Twitter’ buttons.

**Web Log**

(also known as blog) Site that serves as a publicly-accessible personal journal for an individual. Typically updated daily, blogs often reflect the personality of the author.

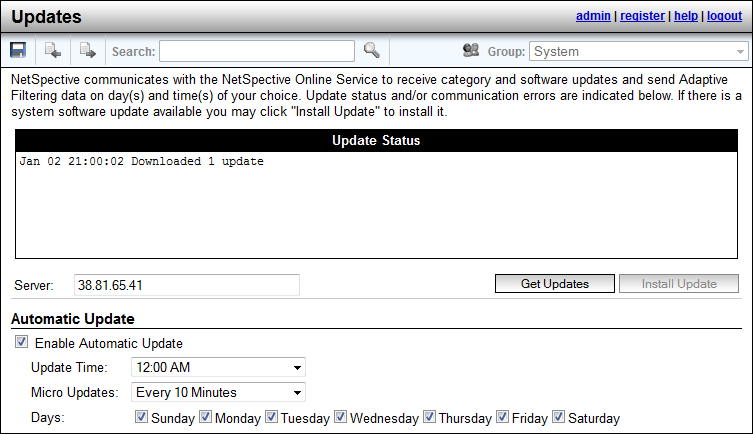
<HTTP://www.blogger.com/>

<http://googleblog.blogspot.com/>

**Automatic Updates**

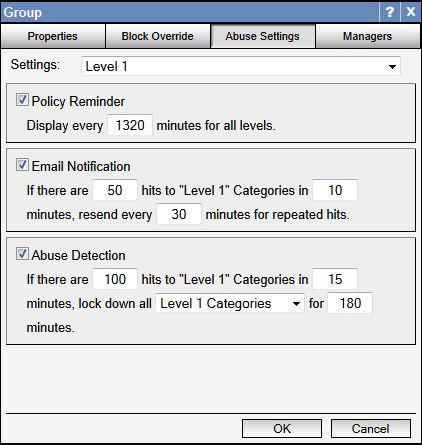
NetSpective categorization updates occur nightly and automatically. However, due to sensitive sites such as Anonymous Proxy and Hacking or Pornography changing on a day to day basis, we utilize a feature referred to as our Micro Updates. With this, unknown websites that are detected by the NetSpective appliance are sent back to TeleMate.Net for evaluation. TeleMate.Net’s web crawler will then categorize the URL and send it back out to all NetSpective Appliances in distribution every 10 minutes. This gives each customer the benefit of learning from our entire customer base.

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 also will be blocked; halting the function of any malware on a client workstation.



**Abuse Detection**

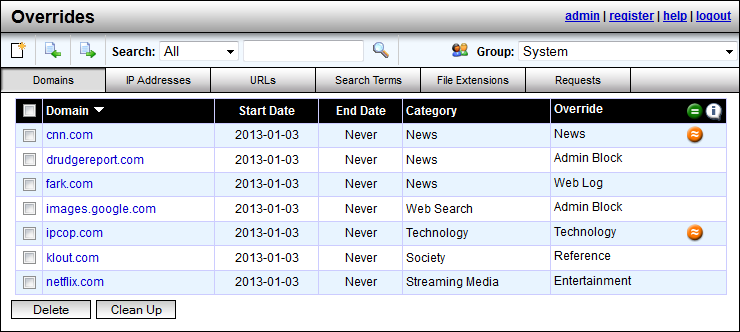
NetSpective’s abuse detection feature will send email notification to the network administrator or lock down a specific user’s traffic (whichever is preferred) when a user attempts too many hits at a Level 1 category for a specific amount of time. The number of hits and the timeframe are customizable. This feature curbs a user’s inappropriate surfing behavior, if the user knows there are consequences to their actions.



**Recategorization**

The Overrides function allows for both domain and URL blocking. URL blocking is granular down to the page you wish to filter. General category filtering also provides non-exclusive category filtering. With this functionality, a website can be allowed through, but an objectionable page on the site can still be blocked.

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. Overrides can be imported from a simple text file as well.NetSpective can block or allow any domain, subdomain, URL, or sub- URL.

****

Our overrides inherently filter with an implied star at the beginning of each domain, and an implied star at the end of all URLs. Thus, the wildcard would include any subdomain. Thus if you overwrote \*.xyx.com to entertainment, all subdomains like games.xyx.com would also be classified as entertainment.

Any category overrides a customer makes on their appliance are communicated back to TeleMate.Net. TeleMate frequently has human eyes combing over these customer overrides and evaluating their category listing. If we make any changes to these websites, those changes will be reflected in the Overrides section of the product so you may see what we agreed upon or disagreed with. Any URLs that we changed to match your overrides can be cleared out easily with the ‘clean up’ button so the administrator does not have to review them.

There is also a link on the TeleMate.Net Website where customers can manually request a website’s category be reviewed and changed. Any changes made to these categories will be updated with our ‘Category Master List’ which typically happens daily at midnight or when the customer chooses to set their automatic updates within the appliance’s administration interface.

**Referrer Depth**

Within the Overrides section is our Referrer Depth feature. With this, when an administrator whitelists a website, we have the ability to also allow any content linked to that site. With this anything linked to the website we are overriding will also be allowed, such as images linked from different web pages.

Many of our K12 customers found another use for this feature by poking pinhole access into YouTube. An administrator would whitelist a teacher’s personal webpage. The teacher would then add links to YouTube or another educational streaming media service. We would add this referrer depth feature to that teacher’s website, so that when a student would click on that link, they would go to YouTube and watch that video. If the student tried to access the same video through another means, like going directly through YouTube they would still be blocked.

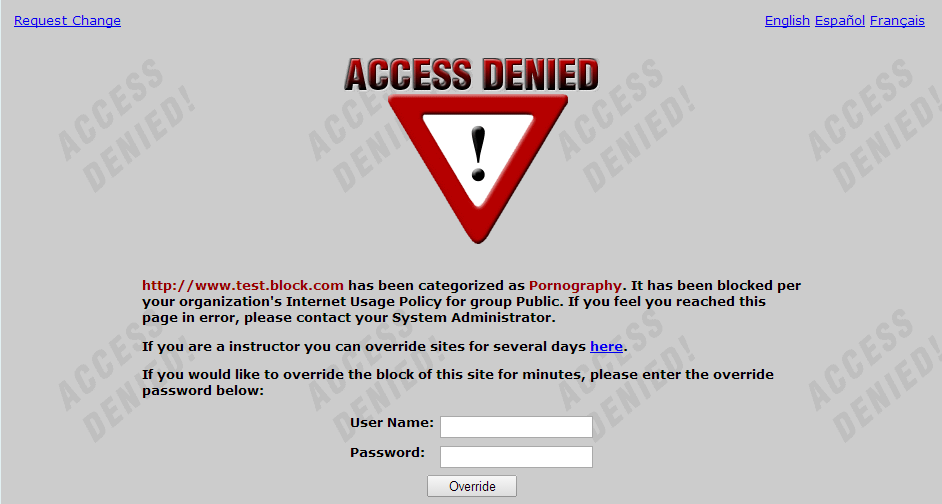
**Override Request**

If an administrator enables this feature, user will have the ability to request the category for a website be changed. A user will encounter a block page, view the category and website as reasons for why they were blocked, and can then click on the ‘request category change’ link. Once they make those requests, they can be seen in the Overrides section of the product. The administrator can then go in and view those requests, then decide if they want to re-categorize those websites or not.

**Block Page Overrides**

Permissible users can override sites on the block page by entering in their password to gain access into a blocked site. The network administrator controls the amount of time this block-page override can occur and also monitors who and how many overrides they allow. This monitoring helps to curb inappropriate behavior.

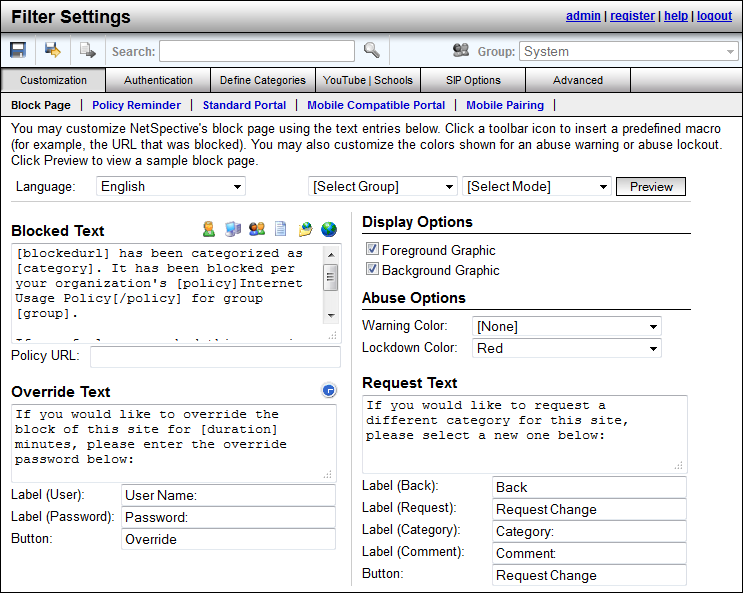
An email will be sent to the network administrator if a manager has issued an excessive amount of block page overrides. The amount deemed ‘excessive’ will be determined by the administrator.



**Block Page Customization**

NetSpective supports customization of block pages, policy reminder pages, standard portal, mobile compatible portal, and the mobile pairing pages. Each page can be customized with different color, text, images, even HTML code. NetSpective also supports redirecting users to a custom redirect page on the customer’s network by IP address. These customization settings are a global feature, not on a per group basis.

The Policy Reminder Page will also display the policy every ‘X’ minutes for all users. This amount of time also is customizable.



**YouTube for Schools**

NetSpective can limit YouTube access to only educational videos on YouTube EDU by assigning a YouTube for Schools code to a NetSpective group. This code is acquired by signing up for an account on YouTube EDU. Members of the group will only be able to view videos YouTube has flagged as educational or videos found in the assigned account’s playlist. This allows NetSpective to limit YouTube content on a group by group basis based on educational needs. For example, you may want Elementary School students to have one account, and High School students to have a different account, since their needs for education would be different.

**LDAP Integration**

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.

**Authentication**

**NetSpective Logon Agent**

Designed as a domain based technology, our logon agents are used to filter desktops and notebooks on the LAN. Our logon agents support Windows, Citrix Terminal Servers, as well as Max OS X desktops and notebooks. Logon Agents typically sit on the domain controller and execute through a Group Policy Object (GPO) or Network Logon Script. They can be run with a number of parameters.

In persistent mode, logon agents would stay up and running on the user’s workstation, sending NetSpective username and IP address association periodically. This is helpful for notebooks which may be on a wireless connection and their IP address may change over time.

In non-persistent mode, the logon agent would run and terminate in about a millisecond, just sending the username and IP address association once.

In the silent mode, the logon agent can be completely hidden as a service. This is for preventing students from being aware of its existence, and thus being unable to remove or terminate the agent.

**NetSpective Remote Agent**

Our Remote Agents are designed for filtering and reporting on Windows and Mac OS X notebooks both on and off network. When installed on the user’s notebook, the remote agent will communicate back to the NetSpective appliance asking for a ‘Go’ or ‘No-Go’ on the user’s web traffic using a proprietary UDP packet. The appliance then checks against the user’s policy and sends that packet back to the remote agent to either allow the traffic or redirect to a block page. The user’s surfing history logs are sent back to the appliance periodically. Even if communication to the appliance is interrupted, the remote agent will hold log files until connection is restored. Our remote agents work intelligently alongside our logon agents and will deactivate themselves when the presence of the logon agent is detected so users on the LAN do not send logon information multiple times.

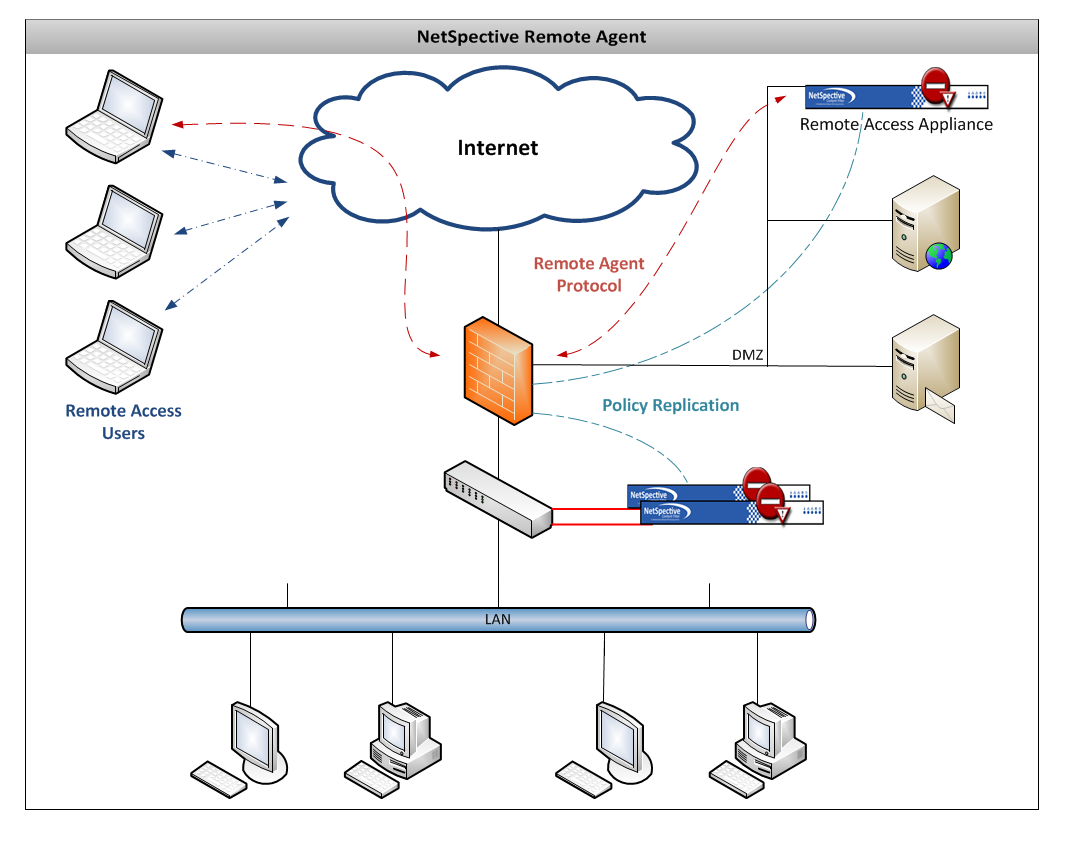
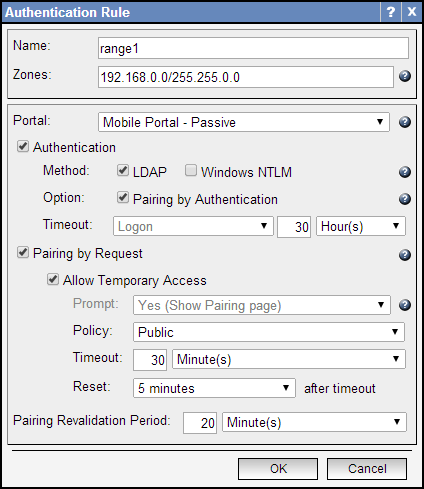


Image depicts an example of how the Remote Agent can operate. Remote Agent technology only requires one appliance so long as the appliance has an internal LAN IP address and an IP address outside of the network.

**Mobile Portal and Mobile Portal with Pairing**

The Mobile Portal was designed under HTML5 to be web browser and operating system independent. This is primarily used to filter mobile devices on the LAN such as iPhones, iPads, Android Phones, and various tablets. With the mobile portal we can authenticate users with LDAP or transparently with Windows NTLM.

Through Mobile Portal with Pairing, we can pair a device to a user either temporarily or permanently if you choose. This is popular in school libraries where iPads are being issued out much like checking out a book. This feature also supports Pairing by Request. Guest users can encounter the same portal page, but request a temporary pairing. Through this you can specify a policy to put guest users under as well as the length of time you wish to give them access. Mobile Portal with Pairing users can be further managed through the Mobile Pairing menu.

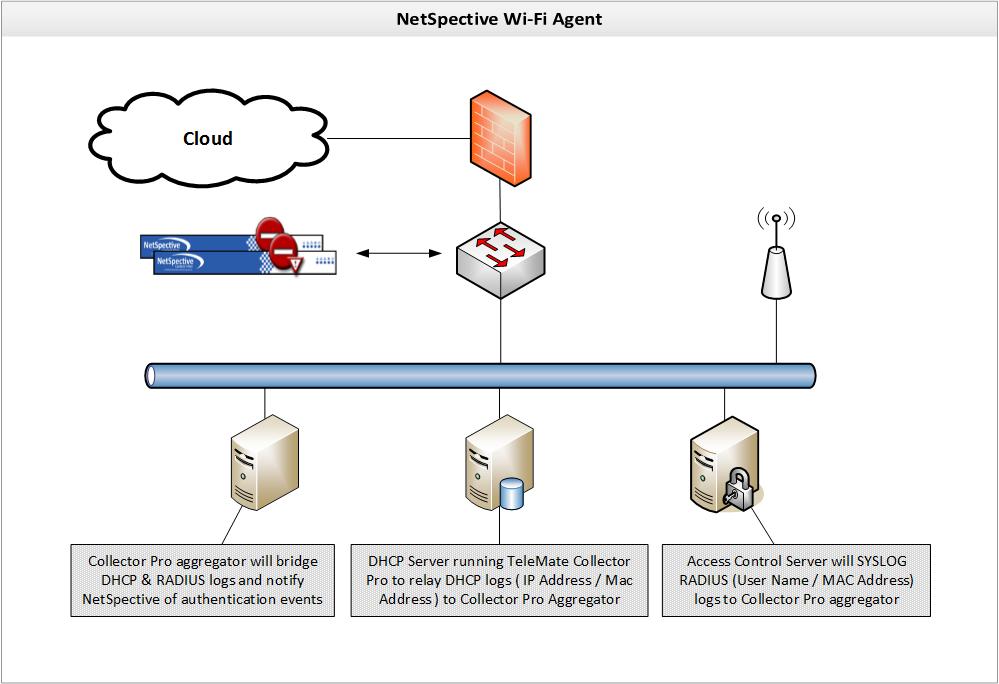


**NetSpective Mobile Browser**

Found on the Apple Store, our NetSpective Mobile Browser was designed as a mirror of Safari in layout and feel. This mobile browser is used to filter iPads both on and off network. Built into the mobile browser is our same remote agent technology. iPads can be identified either by LDAP authentication or by device name. The mobile browser also supports the ability to identify filename extensions that you may wish to open as attachments.

**NetSpective Wi-Fi Agent**

Alternate methods of binding User ID to IP Addresses have been developed and are available based on customer requirements. For environments that utilize authentication at the wireless access point, NetSpective deployments can be customized to dynamically bind DHCP log and Access Control Server logs (RADIUS logs).

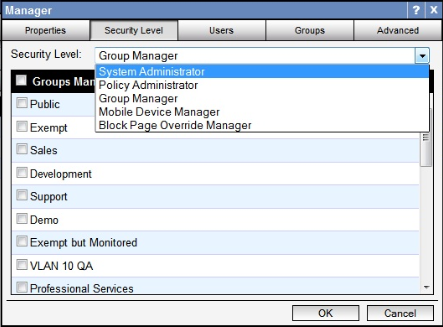


**NetSpective Global Proxy**

As a separate appliance that scales independently, the NetSpective Global Proxy is capable of filtering any device on or off the network. Devices such as iPads and Chromebooks that suspend applications or revert their image when restarted cannot be filtered with traditional agents. The Global Proxy can direct all traffic these devices generate back onto the network to ensure that school owned devices are filtered at home.

**Management**

NetSpective’s administration interface is entirely web based and has no operating system or web browser limitations. In addition to the built-in admin manager, you may create other managers to delegate authority of your NetSpective. You may create manager accounts manually or you may use an LDAP source (such as Active Directory) to authenticate users and passwords. Managers may have different levels of authority, which are summarized by the table below.



|  |  |
| --- | --- |
| Security Level | Permissions |
| System Administrator | * Can create/edit/delete other managers (except admin). * Can create/edit/delete Groups and Users. * Can edit all of NetSpective's configuration options. * Can authorize a temporary override of the block page for any group. |
| Policy Administrator | * Can create/edit/delete other managers (except admin). * Can create/edit/delete Groups and Users. * Can authorize a temporary override of the block page for any group. * Can edit all of NetSpective's filtering options. |
| Group Manager | * Can edit the group policy for assigned groups and categories allowed by security options. * Can edit the group options for assigned groups. * Can edit site overrides for assigned groups, if allowed by security options. * Can move users between managed groups, but cannot add or remove users or groups. * Can authorize a temporary override of the block page for assigned groups. |
| Mobile Device Manager | * Can edit mobile pairings for assigned groups. |
| Block Page Override Manager | * Can authorize a temporary override of the block page for assigned groups. |

Group Managers have additional configurable security options. The options include the ability to change the available permissions for managing Users and Groups. Group Managers also have security options to block access to the Overrides section, specific categories on the Group Policy page, and can be limited to managing only specific IP ranges. These options are only available for Group managers configured to authenticate manually (Local) or authenticate individual users using an LDAP source (LDAP Users). IP Partitions are used to limit access to specific IP Ranges. The managers will only be able to add and/or modify Users within the configured IP Ranges.

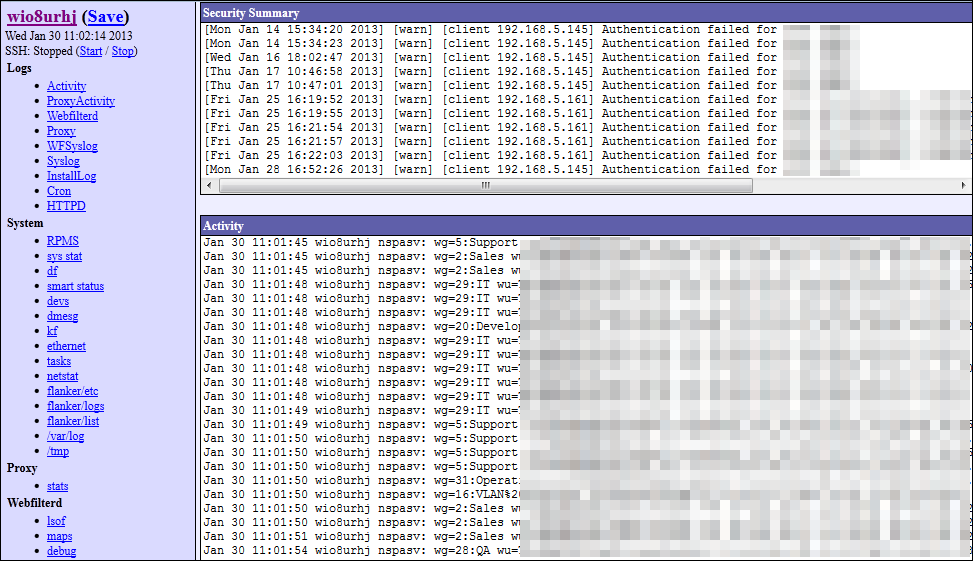
Managers can be configured to have emails sent to them automatically by the appliance. This feature can provide notifications for product updates, abuse detection, as well as block page overrides.

**Automatic Daily Backups**

NetSpective Automatic Daily Backups are sent via FTP and will save all settings on the appliance with the exception of the Network settings (IP address). Backups can also be triggered manually. This makes it easy to apply these settings to a new appliance or restore the current appliance’s settings.

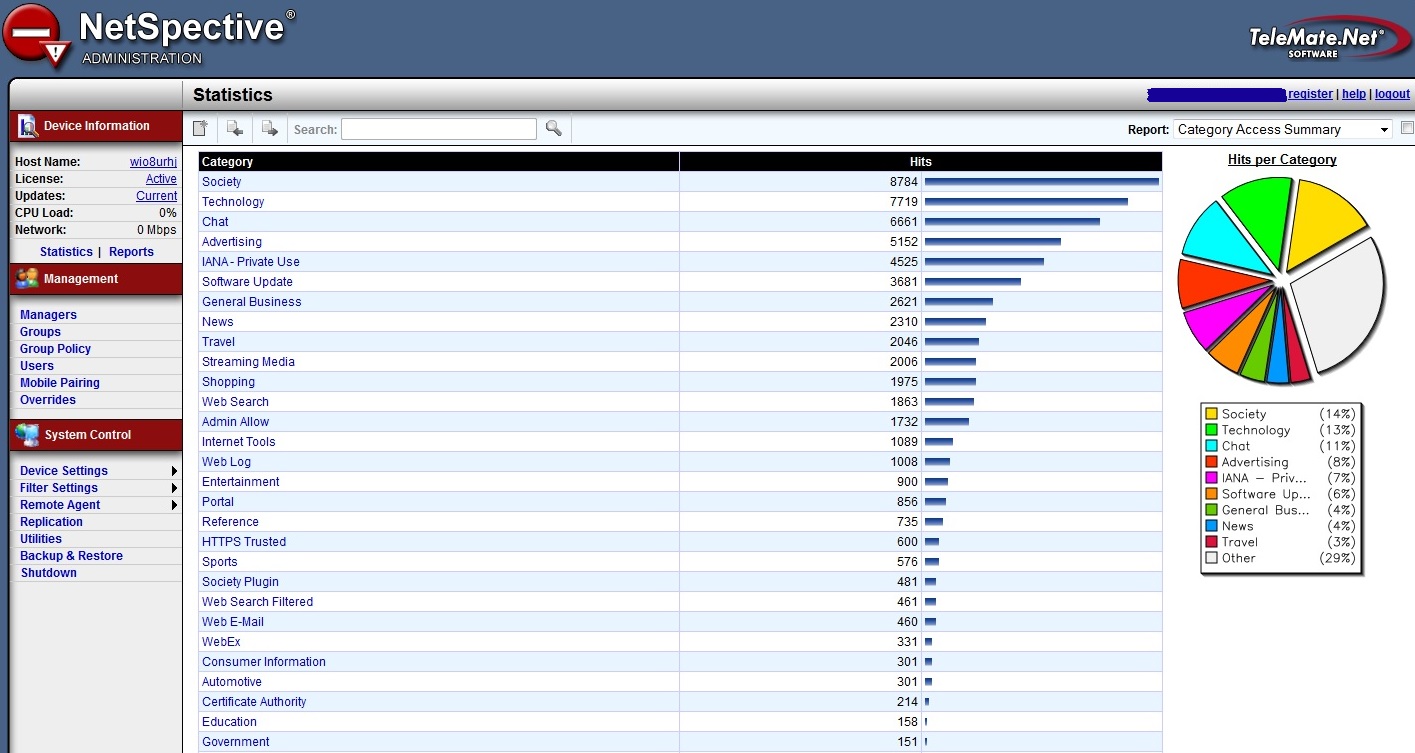
**Diagnostic Tool**

Within NetSpective is our diagnostic tool designed primarily for support and development use. Contained within this tool is a number of reports for seeing how NetSpective is handling and processing web traffic.



**On the Box Statistics**

NetSpective provides several built in, real time, 'gas gauge' type reports as well as the ability to view or search a recent portion of the traffic activity log for troubleshooting.



**NetAuditor Security Event Manager**

Provided for free with our NetSpective Content Filtering is our NetAuditor Security Event Manager. 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.

NetAuditor is provided for ‘off-the-box’ reporting. This can install any Windows based server, VM, or desktop. NetAuditor can also report on firewall logs from many popular manufacturers for various net flow statistics.

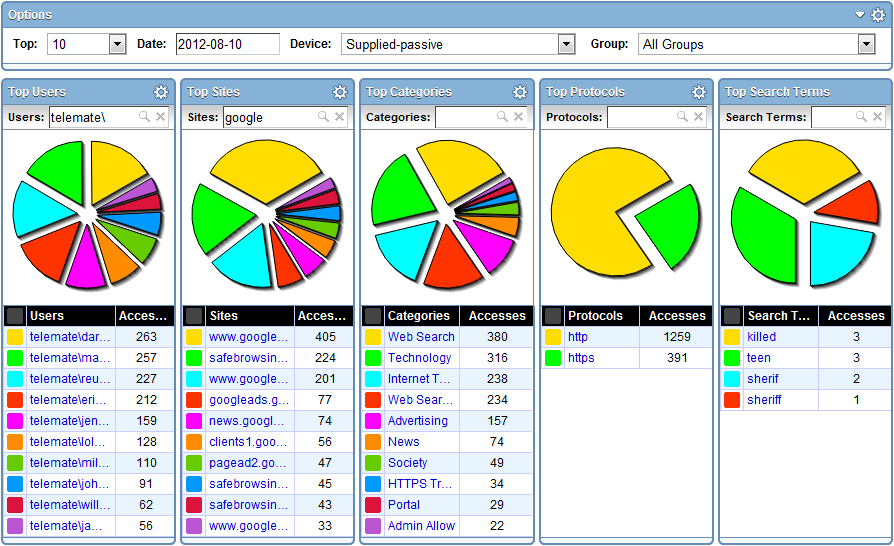
All reports within NetAuditor can be customized and saved for later use. Each report can be tailored by Time, Date, Frequency, Output format, Delivery or Archive method, Object level control, and filtered. Filters vary by report but content filter reports can typically include Source Device, User Group, User Name, User Host, User IP, User Interface, Site Interface, Site Name, Site IP, Protocol, Category, Various Status Flags, and Country.

**Interactive Real-time Dashboards**

NetAuditor provides a dashboard component for a fast and convenient way to search through all of your processed event data. You can select any date that you have processed data for and then start searching for traffic of interest. If you choose "today", the dashboard listings will auto-refresh as new data is processed in for the current day.

The dashboard provides a number of options for quickly finding data you are interested in:

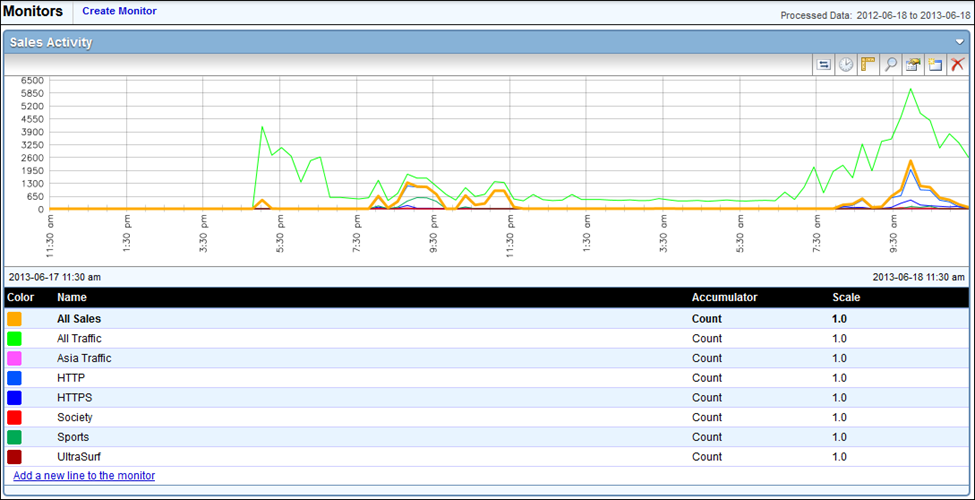
* Filtering options include device, date, and group membership using LDAP; IPv4; IPv6; Host; and User Name.
* Options exist to enable viewing per dashboard by volume and accesses. Additionally, each dashboard has interactive search fields with expression based syntax to quickly find data.



**Trend-based Real-time Monitoring**

NetAuditor includes trend-based monitoring and notification to provide real-time awareness of traffic patterns. Where the dashboard allows you to perform "Top N" searches of your processed data, the monitors allow you to tell the NetAuditor processing engine to watch for something specific as data is processed in real-time. You can check the monitor component at any time and instantly see all monitored traffic for the past 24 hours (down to 1-minute increments). You can set up alerts or event triggers to have the processing engine alert you immediately if the monitored traffic exceeds certain thresholds.

This feature is popular with our K12 customers for being used as a forensics tool. We recommend configuring monitors to track material such as search terms. A school may want to monitor sensitive search phrases such as Suicide, Bomb Making, Cyber Bullying, etc. These and any number of search terms can be monitored and then alerted on. Alerts can be tied to any monitor line and configured by day of week, number of accesses, threshold timeframe, and lead time. NetAuditor can then alert a manager through a number of ways such as email, text, HTTPS Get, or have a custom report sent.



**Security Management**

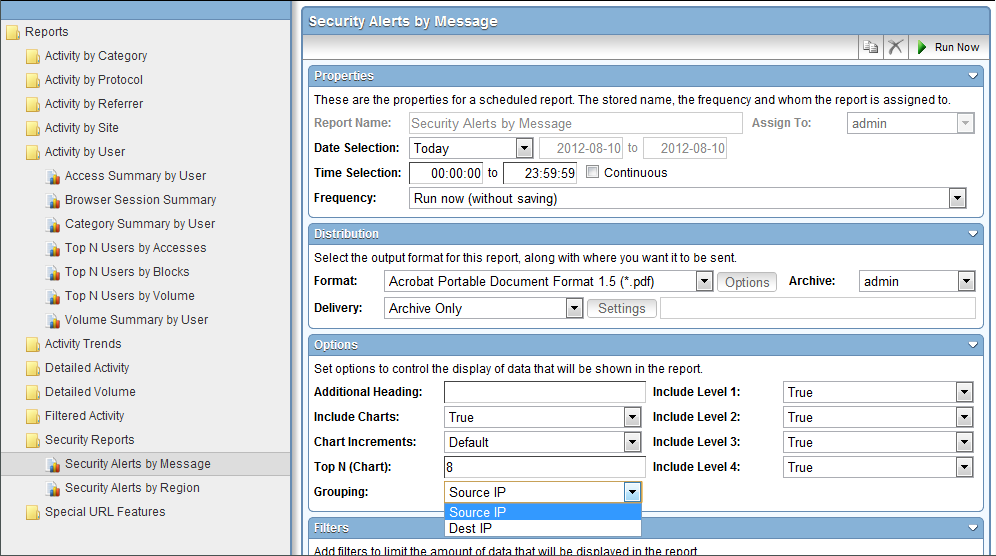
User groups are important in NetAuditor for a number of reasons. In addition to providing a cleaner way to group/filter/search your users when viewing your network traffic, it is also the primary means of providing access control to your manager accounts. For example, if you want a teacher to be able to log into NetAuditor and set up reports and/or monitors on his students (without letting him see traffic generated by other classrooms, grades, or schools), you can set up a user group that exists for his class and then you can provide him with a manager account that only has access to that user group.

**Automated Reporting**

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.



**Support**

TeleMate.Net Software offers a broad range of support, training, and consulting services designed to help you speed deployment and increase your efficiency, productivity and return on your technology investment.

Tier 2 and 3 support will be provided 24/7/365 and all hardware replacements are shipped overnight. On-site training as well as remote training can both be provided as needed.

**MAINTENANCE, WARRANTY, & SERVICE**

**Maintenance**

Maintenance is fully included with the license contract. Any hardware will be replaced if failure occurs. Maintenance also includes all updates, which are automatically sent to the appliance nightly.

Maintenance releases and patches are automatically sent to the box. The administrator will receive an email when one is sent. They are usually automatic.

Major and minor upgrades occur a few times per year depending on how the technology is developing in the marketplace.

When a major software upgrade occurs, the appliance may have to reboot. Rebooting will happen automatically when the update is installed. This process usually takes about 2 minutes. For this reason, major updates will download automatically, but must be manually applied.

Minor software updates will download and apply automatically. Major updates only require the click of one button and approximately 2 minutes for the system to reboot.

Customization and configurations are always maintained during upgrades. Your policies and settings will remain the same after applying a major update. If any field in the product should change, the administrator will be notified in the release notes before ever applying the major update.

**Warranty**

The hardware and software are fully warranted during the contract period. If a box fails, a replacement appliance will be sent for no additional charge.

### Category List

**User Defined Categories**

These are categories you can create yourself and populate with anything you with through the use of the ‘Overrides’ section of the product.

**Advertising**

Sites that provide banner advertising servers.

<HTTP://googleadservices.com/>

<HTTP://ad.doubleclick.net/>

**Alcohol**

Sites promoting alcohol use, including drink recipes, home brewing methods, advertisements, etc.

<HTTP://www.captainmorgan.com/>

<HTTP://www.greygoose.com/>

**Anonymous Proxy & Hacking**

Sites specifically designed to bypass content filters and security. Promotion, instruction, or advice on the questionable or illegal use of computer equipment and software.

<http://unblocksites.com/js/>

<http://myyoutubeunblocker.com/>

**Art**

Sites providing online galleries, museums and artist sites.

<HTTP://www.vangoghgallery.com/>

<HTTP://www.leonardoda-vinci.org/>

**Automotive**

Sites of automobile manufacturers, dealers, sales and clubs.

<HTTP://www.hyundaiusa.com/>

<HTTP://www.nissanusa.com/>

***Browser Protection***

**Malware**

Sites that attempt to interfere with normal computer functions and/or send personal data about you to unauthorized parties over the Internet. Only Admin Allow can override this category.

**Phishing**

Sites that impersonate another site in an attempt to mislead you into providing personal information. Only Admin Allow can override this category.

**Certificate Authority**

<HTTP://ocsp.godaddy.com/>

<HTTP://ocsp.verisign.com/>

**Chat**

Sites and protocols related to Instant Messaging and Chat applications.

<HTTP://www.aim.com/>

<HTTP://www.google.com/talk/>

**Chat Extended**

Sites and protocols related to additional Instant Messaging features such as, File Sharing, Voice over IP, Streaming Internet Radio Video Messaging, etc.

74.125.137.113

173.194.37.33

***Chat Protocols***

AOL

ICQ

IRC

Jabber

MSN

MySpace

Yahoo

**Consumer Information**

Sites with consumer-generated reviews, buying tips, ratings and pricing.

<HTTP://www.kbb.com>

<HTTP://www.consumerreports.org>

**Criminal Skills**

Sites advocating, instructing, or giving advice on performing illegal acts.

<HTTP://www.gregmiller.net/locks/>

<HTTP://www.lockpickguide.com/>

**Cult and Occult**

Sites promoting cult or occult matters and other types of psychological control or manipulation.

<HTTP://tsl.org/>

<http://krishna.org/>

**Drugs**

Sites promoting the use or purchase of illegal drugs and narcotics, including techniques and products.

<http://www.rollitup.org>

<HTTP://greenpartypills.com/>

**Dynamic Hosting**

Sites for third party content provider networks that service a wide range of frequently changing content using a distributed network of servers.

<http://www.godaddy.com/>

<HTTP://us.bc.yahoo.com/b>

**Education**

Sites sponsored by schools or other educational facilities, faculty or alumni groups that promote educational events or activities.

<HTTP://mathtag.com/>

<HTTP://educationbug.org/>

**Entertainment**

Sites containing movies, theater times, comic strips, television, music, hobbies, rock bands, etc.

<HTTP://www.imdb.com/>

<HTTP://www.rottentomatoes.com/>

**Finance/Investing**

Sites of financial trade, financial news, online banking services, trading exchanges.

<HTTPS://us.etrade.com:443>

<HTTP://www.tdameritrade.com/home.page>

**Gambling**

Sites which encourage gambling such as betting sites, bookmaker odds, lottery, bingo, online sport betting, and online casinos.

<HTTP://www.onlinegambling.com/>

<HTTP://www.netbet.org/>

**Games**

Sites related to computer or other games, game download and online game sites.

<HTTP://battle.net/wow>

<https://www.guildwars2.com/en/>

**General Business**

Sites sponsored by or devoted to individual business firms.

<http://listingbook.com/home/>

<http://www.insperity.com/>

**Glamour**

Sites related to fashion and modeling.

<http://www.fashion.net/>

<http://www.elle.com/fashion/>

**Government**

Sites sponsored by government branches or agencies.

<http://www.fbi.gov/>

<http://www.irs.gov/>

**Hate Speech**

Sites containing material related to the discrimination of any group of people based on race, religion, gender, nationality, sexual orientation, etc.

<HTTP://www.kkk.com/>

<http://kkk.bz/>

**Health**

Sites that provide information or advice on personal health or medical services, health insurance, procedures, or devices. This includes information such as diet, nutritional facts, therapies and counseling services.

<http://www.redcross.org/>

[http:/www.gwinnettmedicalcenter.org/](http://www.gwinnettmedicalcenter.org/)

**Hobbies**

Sites that provide information on private and largely sedentary pastimes.

<http://www.modelairplanenews.com/>

<http://www.modelaircraft.org/>

**Hosting Site**

Sites for third party content provider networks that service a wide range of frequently changing content using a distributed network of servers.

<HTTP://www.hostgator.com/>

<HTTP://www.namecheap.com/>

***HTTPS / Direct Connections***

**HTTPS Trusted**

HTTPS sites with verified certificates signed by a trusted Certificate Authority that don’t fall within a current category.

**HTTPS Untrusted**

HTTPS sites with self-signed, invalid, or expired certificates.

**HTTPS Unrated**

HTTPS sites not seen before that will be processed within 24 hours and moved to an appropriate category. (Passive / Remote Agent only)

**Internet Tools**

Sites or services that give users the ability to store personal information or remotely access Web-Conferencing.

<HTTPS://spreadsheets.google.com:443>

<HTTP://docs.google.com/>

**Job Search**

Sites that offer information on or support seeking employment.

<HTTP://www.monster.com>

<http://www.dice.com/>

**Law**

Sites with legal content to include laws, legal topics and lawyers.

<http://www.splcenter.org/get-informed/intelligence-files/ideology/ku-klux-klan>

<http://www.laws.com/>

**Lingerie**

Sites selling or modeling undergarments or lingerie.

<http://www.victoriassecret.com/>

<http://www.fredericks.com/>

**Mature Content**

Sites with mature content that may not be considered explicitly pornographic- like lingerie, swimsuits and revealing pictures.

<http://www.maxim.com/>

<http://www.fhm.com/>

**Military**

Sites sponsored by military branches or agencies.

<http://www.military.com/>

<http://www.militarytimes.com>

**News**

Sites relating to mainstream online news publications or media format such as print, radio, or television.

<http://www.cnn.com/>

<http://www.foxnews.com/>

**Not Rated**

Sites that don't fall into a specific category.

**Nudism and Naturism**

Sites related to nudists and naturists.

<HTTP://www.truenudists.com/>

<HTTP://www.aanr.com/world-of-nude-recreation>

**Peer-to-Peer**

Sites and protocols related to file sharing applications. example: KaZaa and Gnutella.

<HTTP://www.kazaa.com/>

<http://www.bittorrent.com/>

***Peer-to-Peer Protocols***

Ares

BitTorrent

Direct Connect

EDonkey

Freegate

Gnutella

Kazaa

Napster

Pando

Piolet

The Onion Router

Ultra Surf

WinMx

**Personals/Dating**

Sites related to personal ads, dating sites and services, relationships, introductions.

<HTTP://www.eharmony.com/>

<HTTP://www.pof.com/>

**Politics & Religion**

Sites that pertain to politicians, election campaigns, political organizations and publications, churches and related publications, discussion forums, religions.

<HTTP://www.scientology.org/>

<http://www.buckheadchurch.org/>

**Pornography**

Sites with nudity of any sort, vulgarity, including the likes of Playboy, Hustler, Penthouse, etc.

<http://www.playboy.com/>

<http://penthouse.com/>

**Portal**

Site or service that offers a broad array of resources and services, such as e-mail, forums, search engines, and on-line shopping malls.

<HTTP://www.yahoo.com/>

<HTTP://aol.com/>

**Reference**

Personal, professional, or educational references to include online dictionaries, maps, and language translation sites.

<HTTP://dictionary.com/>

<HTTP://mapquest.com/>

**Remote Login**

Sites hosting Remote Login tools.

<HTTPS://secure.logmein.com:443>

<https://secure.logmein.com/products/hamachi/download.aspx>

***Remote Login Protocols***

OpenVPN

SSH

VNC

Citrix

Remote Desktop

PCAnywhere

**Science**

Sites whose primary function is to provide scientific/research pages or materials.

<HTTP://www.billnye.com/>

<HTTP://www.scires.com/>

**Sex Education**

Sites offering information on sexuality and sexual content.

<HTTP://www.advocatesforyouth.org/>

<HTTP://www.plannedparenthood.org/>

**Sexual Advice**

Information related to sexual relationships and sexual issue.

<HTTP://www.thefrisky.com/>

<http://www.yourtango.com/>

**Sexual Orientation**

Sites related to the discussion of homosexuality or other sexual orientation issues.

<HTTP://www.glaad.org/>

<http://www.gaycenter.org/>

**Shopping**

Sites which contain consumer oriented online shopping, online malls, real estate, automobiles, classifieds and online trading services.

<http://www.amazon.com/>

<http://www.hottopic.com>

**Shopping Auction**

Shopping sites that specifically conduct their shopping business as auctions.

<HTTP://ebay.com/>

<HTTP://www.shopgoodwill.com/>

**Society**

Sites that provide information on matters of daily life including sites that contain material relative to an individual's personal life, whether straight, gay, lesbian, or otherwise; any site pertaining to any particular culture, behavior, organization, society, club, etc.

<https://www.facebook.com/>

<https://twitter.com/>

**Society Plugin**

Examples such as ‘Like’ buttons, Google+ ‘+1” buttons, and ‘Share on Twitter’ buttons.

**Sports**

Sites that provide information on or promote sports, active games, and recreation.

<http://www.nfl.com/>

<http://www.nhl.com/>

**Streaming Internet Radio**

Sites that transmit audio in real-time (i.e., as the information is received).

<http://www.pandora.com/>

<http://www.shoutcast.com/>

**Streaming Media**

Sites that stream audio and video on demand.

<http://www.youtube.com/>

<http://www.hulu.com/>

***Streaming Media Protocols***

Flash

QuickTime

Real

Slingbox

Winamp Shoutcast

Windows Media

**Technology**

Sites dedicated to general computer/internet related information pertaining to both hardware and software.

<http://www.dell.com/>

<http://www.asus.com/>

**Tobacco**

Sites that provide information on, promote, or support the sale of tobacco products, and any associated paraphernalia.

<https://camel.tobaccopleasure.com>

<https://www.marlboro.com>

**Travel**

Sites that offer travel tickets and reservations, travel clubs, travelogues, visitor information bureaus, travel promotions, etc.

<http://www.travelocity.com/>

<http://www.priceline.com/>

**Violence**

Sites that provide information on or promote violent activity.

<http://www.facesofdeath.com/>

***Voice Over IP***

SIP

NetMeeting H.323

Skype

**Weapons**

Sites that provide information on, promote, or support the sale of weapons and related items.

<http://www.weapons-universe.com/>

<HTTP://www.gunsmagazine.com/>

**Web E-Mail**

Site that allow users to send e-mail via a web browsing application including sites such as hotmail.com and Yahoo! mail.

<HTTPS://gmail.com>

<https://login.secureserver.net/>

**Web Log**

(also known as blog) Site that serves as a publicly-accessible personal journal for an individual. Typically updated daily, blogs often reflect the personality of the author.

<HTTP://www.blogger.com/>

<http://googleblog.blogspot.com/>

**Web Search**

Sites that support searching the Web, news groups, or indices and directories thereof.

[www.google.com](http://www.google.com)

[www.bing.com](file:///\\tm-wss01\Users\shawn.harrington\My%20Documents\www.bing.com)

**Web Search Filtered**

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 this category for Google, Bing, MSN, Yahoo, Hotbot, Lycos, Ask, and Dogpile.

# Hardware Specifications

## NetSpective 12D

Box – S-1200R3, 1U Chassis w/Single Blower

CPU – Core I3-2120 Dual Core 3.3GHZ, 3MB Cache

The 2nd generation Intel Core i3 processor offers a fast, responsive, and visually immersive experience available to everyone. With the 2nd generation Intel Core i3 processor, you get built-in visuals that offer a rich and exciting set of capabilities for a stunning and seamless visual experience with no additional hardware required. Also featured is Intel Hyper-Threading Technology, which enables each processor core to work on two tasks at the same time, giving you smart multitasking performance to move between applications quickly and without hesitation. This is where to start for visibly smart performance.

The Intel microarchitecture codename Sandy Bridge is an incredible leap in processor integration and manufacturing introduced in the 2nd generation Intel Core processor family. Manufactured entirely on Intel 32nm process technology, Sandy Bridge unifies processor cores, memory controller, last-level cache (LLC), and graphics and media processing. Such tight integration enables a host of performance and efficiency improvements, including fast access by cores and graphics to shared data in the last-level cache to accelerate graphics processing, fewer buses over which data and signaling must travel for faster processing, and more memory bandwidth for the cores to boost system performance.

Memory – 4GB DDR3-1333, Unbuffered, ECC, 240-PIN

Hard Disk – Intel S3500 Series 80GB MLC Solid State Drive, 20NM NAND, 2.5” SATA III

Network Adapter – Two Gigabit Ethernet Controllers

## NetSpective 12Q

Box – S-1200R3, 1U Chassis w/Single Blower

CPU – Xeon E3-1225 Quad Core, 3.1GHZ, 6MB Cache

Servers based on the Intel Xeon processor E3-1200 product family give you smarter control of the things that matter to your business—increased sales, improved margins, and reduced risk. Based on 32nm Intel Microarchitecture, the Intel Xeon processor E3-1200 is designed with innovative features that allow you to enjoy faster application response time with reduced energy consumption.

Packed with Intel Turbo Boost Technology 2.0, the Intel Xeon processor E3-1200 product family features intelligent performance that adapts to your needs, allowing you to get more done in less time. With built-in 24/7 dependability and advanced security features like ECC memory support, Intel Trusted Execution Technology and Intel AES New Instructions (Intel AES-NI) accelerating data encryption and decryption, you can avoid costly business interruptions and potentially catastrophic security breaches.

The Intel Xeon processor E3-1200 product family is ideal for small business stepping up to their first server, companies requiring a dedicated server for a workgroup, and organizations that need a server to support multiple clients. With Intel Xeon processor E3-1200 family-based servers, you'll spend less time frustrated with outdated desktop systems and more time responding to customers, opportunities, and trends. It's more than a server upgrade; it's a smart investment in your business' future.

Memory – 4GB DDR3-1333 Unbuffered, ECC, 240-PIN

Hard Disk - Intel S3500 Series 80GB MLC Solid State Drive, 20NM NAND, 2.5” SATA III

Network Adapter - Two Gigabit Ethernet Controllers

## NetSpective 10 Gbps 12H

Box – S-1900 R2, 1U, Dual PSU

CPU – Hex Core 2.40GHZ Intel Xeon E5645, 12MB Cache, 5.86GT/S, LGA1366

Defy the limits when it comes to workstation or server computing with the Intel BX80614E5645 Xeon E5645 Processor. This processor owns 6 cores as it runs at 2.40GHz for super-fast processing performance to quench your cravings for a fast system. The Intel Xeon E5645 Processor uses 80W of power for that efficient performance along with its 12MB L2 cache for a huge boost on its quick responses.

Memory – 4GB DDR3-1333 REGISTERED, ECC, 240-PIN

Hard Disk - Intel S3500 Series 80GB MLC Solid State Drive, 20NM NAND, 2.5” SATA III

Network Adapter - INTEL X520-SR2, 10G ETHERNET DUAL PORT FIBER LC, PCI-E 2.0 X8

Network Adapter - 10G INTEL X520-T2, DUAL PORT, 10GBASE-T, PCIE, LOW PROFILE

# NetAuditor List of Reports

## NetAuditor Report Type: Activity by Category

## Reports

There are five types of Activity by Category reports. They are:

* Access Summary by Category
* Top N Categories by Accesses
* Top N Categories by Blocks
* Top N Categories by Volume
* Volume Summary by Category

**Report Sections**

**Header**

In the header of this report you will see the date range of the report.

**Protocol Activity for Categories**

This is a graphical representation of the total accesses by protocol.

**Access Summary by Category**

This shows the categories and all associated accesses during the date range of the report. You can see the entire listing of categories that we currently support, along with complete definitions of what belongs in each category [here](http://www.telemate.net/products/netspective/category_listing.php).

* Unique Users: The number of users that accessed sites in each category.
* Unique Sites: The number of web sites that were accessed in each category.
* Percent of Accesses: Percentage of the total number of accesses.
* Accesses: An access is defined as one Get Request for HTTP, one Connection for HTTPS, one file for FTP, one login or group change for NNTP. For CHAT/P2P/VOIP/Streaming Media it depends on our individual signature for that protocol which maybe the login, connection, or file. Total accesses are the sum of all accesses for all supported protocols.
* Percent Blocked: Percentage of accesses that were blocked.

**Top N Protocols**

This shows the top N protocols for all accesses during the date range of the report.

* Unique Sites: The number of websites that were accessed in each category.
* Percent of Accesses: Percentage of the total number of accesses.
* Accesses: See above definition for accesses.
* Percent Blocked: Percentage of accesses that were blocked.

**Top N Users**

This shows the top N users for all accesses during the date range of the report.

* User Group: The user group that the user belongs to.
* Unique Sites: The number of websites that were accessed in each category.
* Percent of Accesses: Percentage of the total number of accesses.
* Accesses: See above definition for accesses.
* Percent Blocked: Percentage of accesses that were blocked.

**Top N Sites**

This shows the top N websites for all accesses during the date range of the report.

* Percent of Accesses: Percentage of the total number of accesses.
* Accesses: See above definition for accesses.
* Percent Blocked: Percentage of accesses that were blocked.

**NetAuditor Report Type: Activity by Protocol**

**Reports**

There are five types of Activity by Protocol reports. They are:

* Access Summary by Protocol
* Top N Protocols by Accesses
* Top N Protocols by Blocks
* Top N Protocols by Volume
* Volume Summary by Protocol

**Report Sections**

**Header**

In the header of this report you will see the date range of the report.

**Top N Protocols by Accesses**

This shows the top protocols and all associated accesses during the date range of the report.

* Unique Users: The number of users that accessed data in each protocol.
* Unique Sites: The number of web sites that were accessed in each protocol.
* Percent Blocked: Percentage of accesses that were blocked.
* Accesses: An access is defined as one Get Request for HTTP, one Connection for HTTPS, one file for FTP, one login or group change for NNTP. For CHAT/P2P/VOIP/Streaming Media it depends on our individual signature for that protocol which maybe the login, connection, or file. Total accesses are the sum of all accesses for all supported protocols.
* Percent of Accesses: Percentage of the total number of accesses.

**Protocol Header**

In the header for each protocol, you will see:

* Unique Users: The number of users that accessed data in each protocol.
* Unique Sites: The number of web sites that were accessed in each protocol.
* Accesses: See above definition for accesses.
* Percent Blocked: Percentage of accesses that were blocked.

**Category Activity for Protocol**

This is a graphical representation of the total accesses by protocol for each hour within the time frame specified for the report.

**Top N Categories for a Protocol**

This shows the top N categories for all accesses during the date range of the report.

* Unique Sites: The number of web sites that were accessed in each protocol.
* Percent of Accesses: Percentage of the total number of accesses.
* Accesses: See above definition for accesses.
* Percent Blocked: Percentage of accesses that were blocked.

**Top N Users for a Protocol**

This shows the top N users for all accesses during the date range of the report.

* User Group: The user group that the user belongs to.
* Unique Sites: The number of web sites that were accessed in each protocol.
* Percent of Accesses: Percentage of the total number of accesses.
* Accesses: See above definition for accesses.
* Percent Blocked: Percentage of accesses that were blocked.

**Top N Sites for a Protocol**

This shows the top N sites for all accesses during the date range of the report.

* Category: The category that the website belongs to.
* Percent of Accesses: Percentage of the total number of accesses.
* Accesses: See above definition for accesses.
* Percent Blocked: Percentage of accesses that were blocked.

**NetAuditor Report Type: Activity by Referrer**

**Reports**

There are five types of Activity by Referrer reports. They are:

* Chronological Activity Detail with Referrer
* Chronological Detail by User with Referrer
* Referrer Analysis by User
* Search Terms by Referred Category
* Top N Referrers by Accesses

**Report Sections**

**Header**

In the header of this report you will see the date range of the report. The report is then separated by each user and grouped by group.

**Referrer Analysis by User**

This shows each website hit a user has generated, the website they were referred by, as well as the time frame of each Referrer Chain within the overall time frame specified for the report.

* Referring Site: The website that referred the user to the Referred Site.
* Referred Site: The website that the user was referred to by the Referring Site.
* Start Time: The time the user began viewing the Referred Site.
* End Time: The time the user stopped viewing the Referred Site.
* Accesses: An access is defined as one Get Request for HTTP, one Connection for HTTPS, one file for FTP, one login or group change for NNTP. For CHAT/P2P/VOIP/Streaming Media it depends on our individual signature for that protocol which maybe the login, connection, or file. Total accesses are the sum of all accesses for all supported protocols.
* Percent Blocked: Percentage of accesses that were blocked.

**NetAuditor Report Type: Activity by Site**

**Reports**

There are five types of Activity by Site reports. They are:

* Access Summary by Site
* Top N Sites by Accesses
* Top N Sites by Blocks
* Top N Sites by Volume
* Volume Summary by Site

**Report Sections**

**Header**

In the header of this report you will see the date range of the report.

**Top N Sites by Accesses**

This shows the top N sites for all accesses during the date range of the report.

* Category: The category that the website belongs to.
* Unique Users: The number of users that accessed data in each site.
* Percent Blocked: Percentage of accesses that were blocked.
* Accesses: An access is defined as one Get Request for HTTP, one Connection for HTTPS, one file for FTP, one login or group change for NNTP. For CHAT/P2P/VOIP/Streaming Media it depends on our individual signature for that protocol which maybe the login, connection, or file. Total accesses are the sum of all accesses for all supported protocols.
* Percent of Accesses: Percentage of the total number of accesses.

**Protocol Activity for Sites**

This is a graphical representation of the total accesses by site. The heading displays the total number of unique users, the total number of accesses, and the percentage of sites that were blocked.

**Top N Protocols for Sites**

* Unique Users: The number of users that accessed data in each site.
* Percent of Accesses: Percentage of the total number of accesses.
* Accesses: Accesses: See above definition for accesses.
* Percent Blocked: Percentage of accesses that were blocked.

**Top N Users for Sites**

* User Group: The user group that the user belongs to.
* Percent of Accesses: Percentage of the total number of accesses.
* Accesses: See above definition for accesses.
* Percent Blocked: Percentage of accesses that were blocked.

**Top N Categories for Sites**

* Unique Users: The number of users that accessed data in each site.
* Percent of Accesses: Percentage of the total number of accesses.
* Accesses: See above definition for accesses.
* Percent Blocked: Percentage of accesses that were blocked.

**NetAuditor Report Type: Activity by User**

**Reports**

There are seven types of Activity by User reports. They are:

* Access Summary by User
* Browser Session Summary
* Category Summary by User
* Top N Users by Accesses
* Top N Users by Blocks
* Top N Users by Volume
* Volume Summary by User

**Report Sections**

**Header**

In the header of this report you will see the date range of the report.

**Top N Users by Accesses**

This shows the top N users for all accesses during the date range of the report.

* User Group: The user group that the user belongs to.
* Unique Sites: The number of web sites that were accessed by each user.
* Percent Blocked: Percentage of accesses that were blocked.
* Accesses: An access is defined as one Get Request for HTTP, one Connection for HTTPS, one file for FTP, one login or group change for NNTP. For CHAT/P2P/VOIP/Streaming Media it depends on our individual signature for that protocol which maybe the login, connection, or file. Total accesses are the sum of all accesses for all supported protocols.
* Percent of Accesses: Percentage of the total number of accesses.

**Protocol Activity for User**

This is a graphical representation of the total accesses by protocol. The heading displays the total number of unique sites, the total number of accesses, and the percentage of sites that were blocked.

**Top N Protocols for User**

* Unique Sites: The number of web sites that were accessed by each user.
* Percent of Accesses: Percentage of the total number of accesses.
* Accesses: See above definition for accesses.
* Percent Blocked: Percentage of accesses that were blocked.

**Top N Categories for User**

* Unique Sites: The number of web sites that were accessed by each user.
* Percent of Accesses: Percentage of the total number of accesses.
* Accesses: See above definition for accesses.
* Percent Blocked: Percentage of accesses that were blocked.

**Top N Sites for User**

* Category: The category that the website belongs to.
* Percent of Accesses: Percentage of the total number of accesses.
* Accesses See above definition for accesses.
* Percent Blocked: Percentage of accesses that were blocked.

**NetAuditor Report Type: Activity Trends**

**Reports**

There are two types of Activity Trend reports. They are:

* Trend Analysis by Day of Week
* Trend Analysis by Hour

**Report Sections**

**Header**

In the header of this report you will see the date range of the report.

**Trend Analysis by Hour**

This is a graphical representation of the total number of accesses by hour, for each week of the past 4 weeks including the week the report begins on. The header of each section also shows the week you are looking at.

* Prior Max Accesses: The maximum number of accesses for the prior week.
* Prior Min Accesses: The minimum number of accesses for the prior week.
* Prior Average Accesses: The average number of accesses for the prior week.
* Current Accesses: The number of accesses for the week shown in the header.
* Percent Change: The percentage of access changes from the prior week to the week shown in the header.

**Trend Analysis by Day of Week**

This is a graphical representation of the total number of accesses by day, for each week of the past 4 weeks including the week the report begins on. The header of each section also shows the week you are looking at.

* Prior Max Accesses: The maximum number of accesses for the prior week.
* Prior Min Accesses: The minimum number of accesses for the prior week.
* Prior Average Accesses: The average number of accesses for the prior week.
* Current Accesses: The number of accesses for the week shown in the header.
* Percent Change: The percentage of access changes from the prior week to the week shown in the header.

**NetAuditor Report Type: Detailed Activity**

**Reports**

There are three types of Detailed Activity reports. They are:

* Chronological Activity Detail
* Chronological Detail by User
* Chronological Summary by User

**Report Sections**

**Header**

In the header of this report you will see the date range of the report, the group you are reporting on, the user you are reporting on, as well as the time frame of the report.

**Chronological Detail by User**

This shows the all accesses for the user during the date and time range of the report.

* Date: The date of the access or block
* User IP: The IP address of the user.
* Protocol: The protocol the user was using.
* Site: The website the user accessed.
* Category: The category that the website is associated with.
* Action: Actions such as AdminPass and Blocks are in this column.
* Flags: Status flags such as Abuse Flags, Remote Agents, and Redirects are in this column.

**Chronological Activity Detail**

This shows the all accesses for the group and containing users during the date and time range of the report.

* Date: The date of the access or block
* User IP: The IP address of the user.
* User Group: The group the user is a member of
* User: The user represented
* Protocol: The protocol the user was using.
* Site: The website the user accessed.
* Category: The category that the website is associated with.
* Action: Actions such as AdminPass and Blocks are in this column.
* Flags: Status flags such as Abuse Flags, Remote Agents, and Redirects are in this column.

**Chronological Summary by User**

This shows the all accesses for the user during the date and time range of the report in a summarized format.

* Date: The date of the access or block
* User IP: The IP address of the user.
* Start Time: The time in which the initial access was seen.
* End Time: The time in which the last access was seen for the site.
* Protocol: The protocol the user was using.
* Site: The website the user accessed.
* Category: The category that the website is associated with.
* Accesses: The number of accesses seen for the site.
* Action: Actions such as AdminPass and Blocks are in this column.
* Flags: Status flags such as Abuse Flags, Remote Agents, and Redirects are in this column.

**NetAuditor Report Type: Detailed Volume**

**Reports**

There are two types of Detailed Volume reports. They are:

* Volume Summary by Country
* Volume Summary by Interface

**Report Sections**

**Header**

In the header of this report you will see the date range of the report, as well as the interface represented in the graph and chart on the given page.

**Volume Summary by User Interface and IP**

This is a graphical representation of the total volume of traffic by interface.

* Country: The country the traffic was sent to or received by. (Volume Summary by Country report)
* Volume: The volume of traffic for the given interface.
* Percent Up / Down: The percentage of traffic that was uploaded and downloaded.
* Percent of Total: The percentage of your overall traffic that the current interface represents.

**Volume by User Address for Interface**

This is a graphical representation of the total volume of traffic by user IP address.

* User Address: The IP address of the user.
* User Name: The username of the user or associated IP address.
* Volume: The total volume of traffic for the user.
* Percent Up / Down: The percentage of traffic uploaded and percentage of traffic downloaded.
* Percent of Total: The percentage of the total traffic that the user represents.

**Volume by Site for Interface**

This is a graphical representation of the total volume of traffic by site.

* Site: The website that traffic was received by or sent to.
* Category: The category the website is associated with.
* Volume: The total volume of traffic for the site.
* Percent Up / Down: The percentage of traffic uploaded and percentage of traffic downloaded.
* Percent of Total: The percentage of the total traffic that the site represents.

**Volume by Port for Interface**

This is a graphical representation of the total volume of traffic by port.

* Port: The port that the traffic was sent out of or received through.
* Protocol: The protocol used to send traffic through the associate port.
* Volume: The total volume of traffic for the port.
* Percent Up / Down: The percentage of traffic uploaded and percentage of traffic downloaded.
* Percent of Total: The percentage of the total traffic that the port represents.

**NetAuditor Report Type: Filtered Activity**

**Reports**

There are two types of Filtered Activity reports. They are:

* Block Page Override Audit
* Remote Agent Summary by User

**Report Sections**

**Header**

In the header of this report you will see the date range of the report.

**Block Page Override Audit**

* Date: The date that the override was made.
* Time: The time that the override was made.
* User: The user who encountered the blocked webpage and was given an override to access the related webpage temporarily.
* User Group: The group the user belongs to.
* Site: The website the user was trying to visit when they were blocked and given override access.
* Category: The category the website belongs to.
* Manager: The manager who issued the block page override for the associated user.
* Type: The type of override issued, group or individual. Group overrides allow the associated website to be viewed by all users in the same group for a specified time. Individual overrides allow the associated website to be viewed by only the user who requested the override.

**NetAuditor Report Type: Security Reports**

**Reports**

There are two types of security reports. They are:

* Security Alerts by Message
* Security Alerts by Region

**Report Sections**

**Header**

In the header of this report you will see the date range of the report.

**Security Alerts by Message**

This is a graphical representation of the number of security alerts by interface for the time and date range of the report.

* Interface: The interfaces you are reporting on.
* Message Count: Number of alerts for the specified interface.
* Percent of Total: The percent of the total number of alerts the specified interface represents.

**Alert Messages by Category for Interface**

This is a graphical representation of the number of security alerts by category for the interface selected.

* Category: The classification of the alert, typically either consumed or dropped.
* Message Count: The number of messages for the selected category.
* Percent of Total: The percentage of the total number of alerts.

**Alert Messages by Source IP for Message Type**

This is a graphical representation of the number of security messages by source IP address.

* IP Address: The source IP address that the alert originated from.
* Message Count: The number of messages for the specified source IP address.
* Percent of Total: The percentage of the total number of alerts.

**NetAuditor Report Type: Special URL Features**

**Reports**

There are Three types of security reports. They are:

* Search Phrases by User
* Top N Extensions by Accesses
* Top N Search Terms by Accesses

**Report Sections**

**Header**

In the header of this report you will see the date range of the report.

**Search Phrases by User**

This is list of all the search phrases a user has searched for during the specified time.

* Time: The Time the search was made.
* User IP: The IP address of the user
* Type: The Search Engine that was used
* Phrase: The search phrase that was entered.

**Top N Extensions by Accesses**

This is a list of all the file extensions that were accessed during the specified time.

* Extension: The file extension that was accessed.
* Content Type: The type of content the file extension typically represents.
* Unique Users: The number of unique users that accessed the file type.
* Unique Sites: The number of unique sites the file extension was accessed from.
* Percent blocked: The percentage of blocked accesses.
* Accesses: The number of files that were accessed.
* Percent of accesses: The overall percent of accesses for all file types.