NetSpective Content Filter

Overview

NetSpective
Content Filter
A TeleMate.Net Software Monitoring Solution
NetSpective
Content Filter
A TeleMate.Net Software Monitoring Solution

TeleMate.Net® SOFTWARE

View a visual presentation of the product on our website

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.

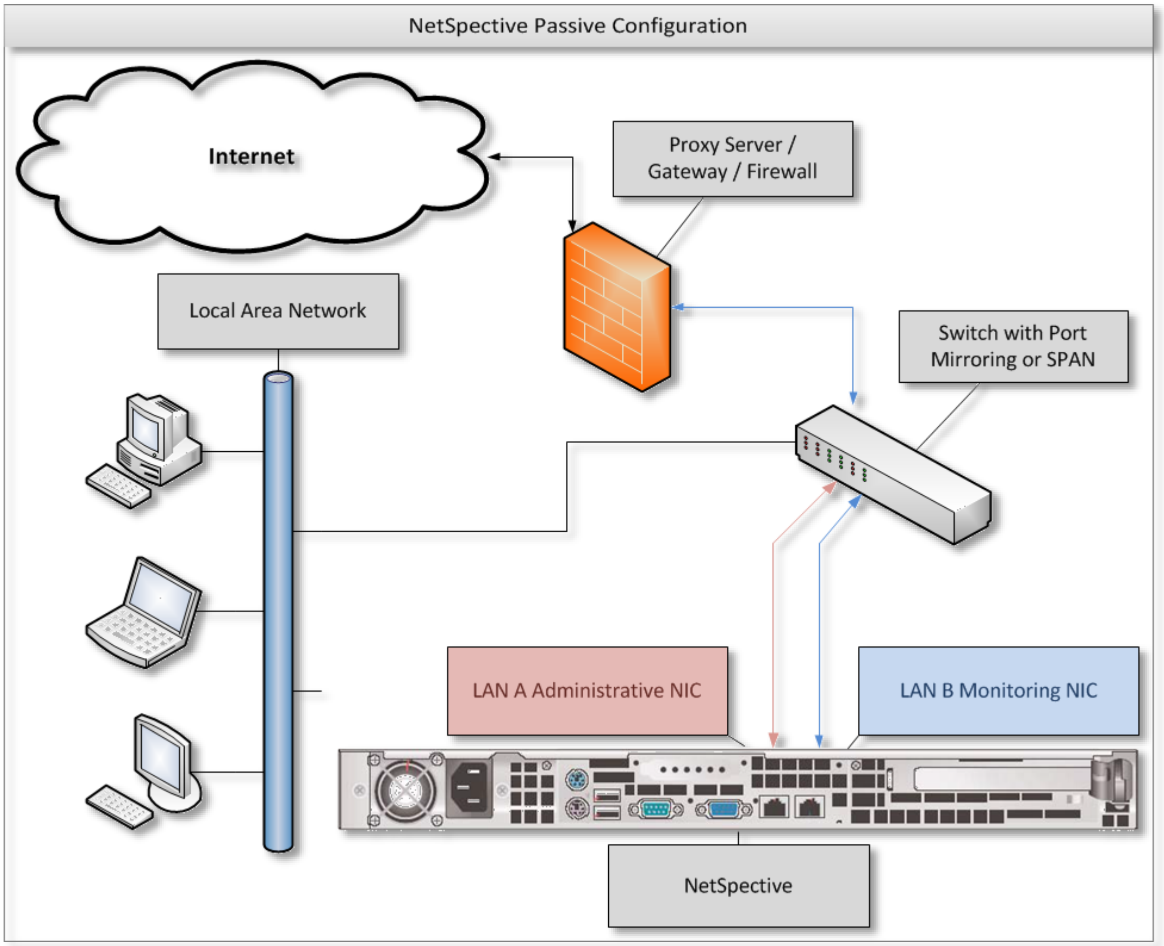
Our ability to listen and respond rapidly to customers' requirements and specifications has earned a credible and solid reputation amongst our customers. Our customers have told us the level of customer service they receive is second to none. Our 'top down' approach to the market is to make every customer 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.


NetSpective Passive Configuration
Internet
Proxy Server / Gateway / Firewall
Local Area Network
Switch with Port Mirroring or SPAN
LAN A Administrative NIC
LAN B Monitoring NIC
NetSpective

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.

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.

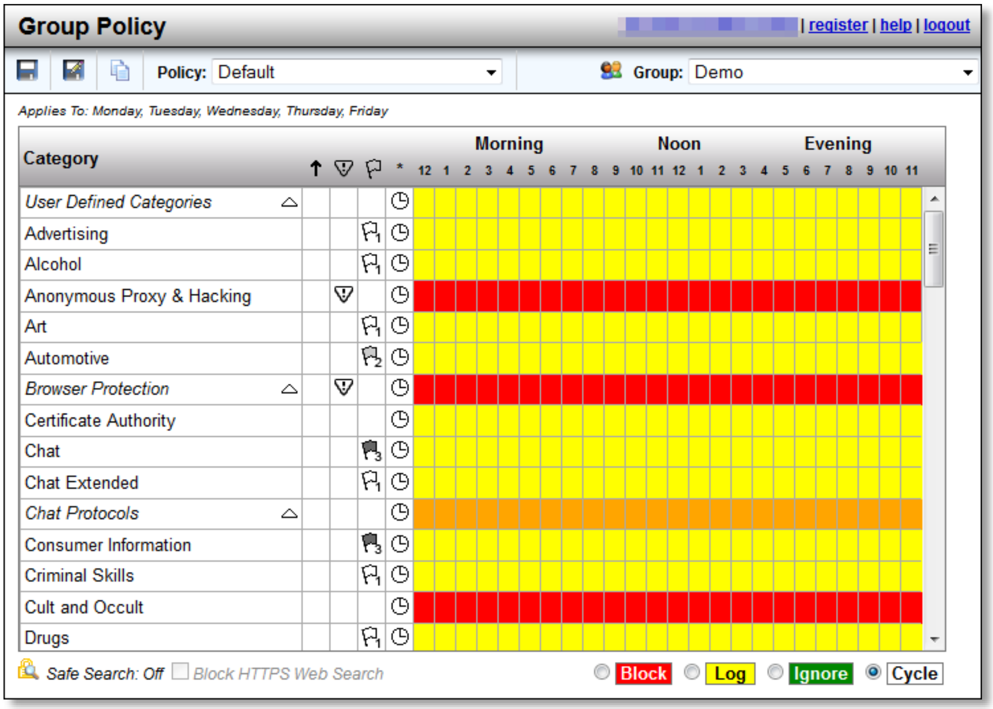
The NetSpective Solution allows schools and libraries to:

- 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.



Group Policy [redacted] | register | help | logout

Policy: Default ▾ Group: Demo ▾

Applies To: Monday, Tuesday, Wednesday, Thursday, Friday

Category	↑	▽	⚐	*	12	1	2	3	4	5	6	7	8	9	10	11	12	1	2	3	4	5	6	7	8	9	10	11
									Morning								Noon							Evening				
User Defined Categories △				🕒	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨
Advertising			⚐1	🕒	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨
Alcohol			⚐1	🕒	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨
Anonymous Proxy & Hacking		▽		🕒	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥
Art			⚐1	🕒	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨
Automotive			⚐2	🕒	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨
Browser Protection △		▽		🕒	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥
Certificate Authority				🕒	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨
Chat			⚑3	🕒	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨
Chat Extended			⚐1	🕒	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨
Chat Protocols △				🕒	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧
Consumer Information			⚑3	🕒	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨
Criminal Skills			⚐1	🕒	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨
Cult and Occult				🕒	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥
Drugs			⚐1	🕒	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨

Safe Search: Off □ *Block HTTPS Web Search* ○ Block ○ Log ○ Ignore ● Cycle

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, 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.

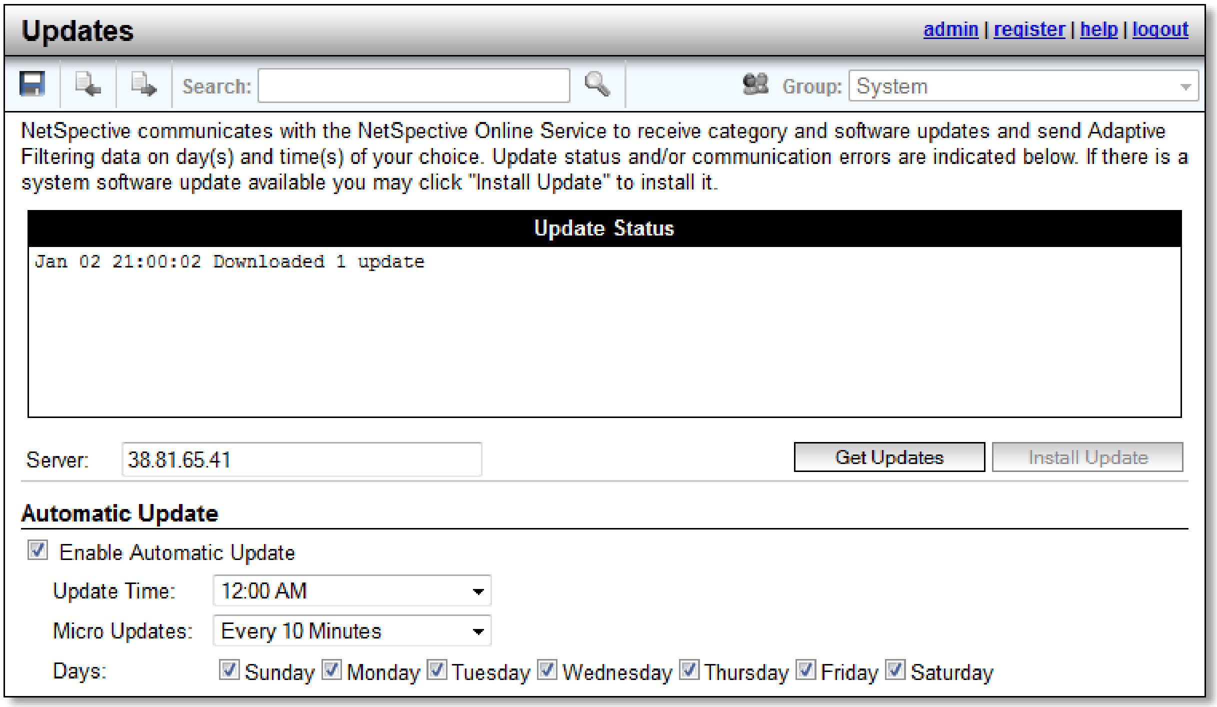
Web Log
(also known as blog) Site that serves as a publicly-accessible personal journal for an individual. Typically updated daily, blogs often reflect the personality of the author.

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.



Updates

Search:

Group: System

NetSpective communicates with the NetSpective Online Service to receive category and software updates and send Adaptive Filtering data on day(s) and time(s) of your choice. Update status and/or communication errors are indicated below. If there is a system software update available you may click "Install Update" to install it.

Update Status

```
Jan 02 21:00:02 Downloaded 1 update
```

Server: 38.81.65.41

Automatic Update

☑ Enable Automatic Update

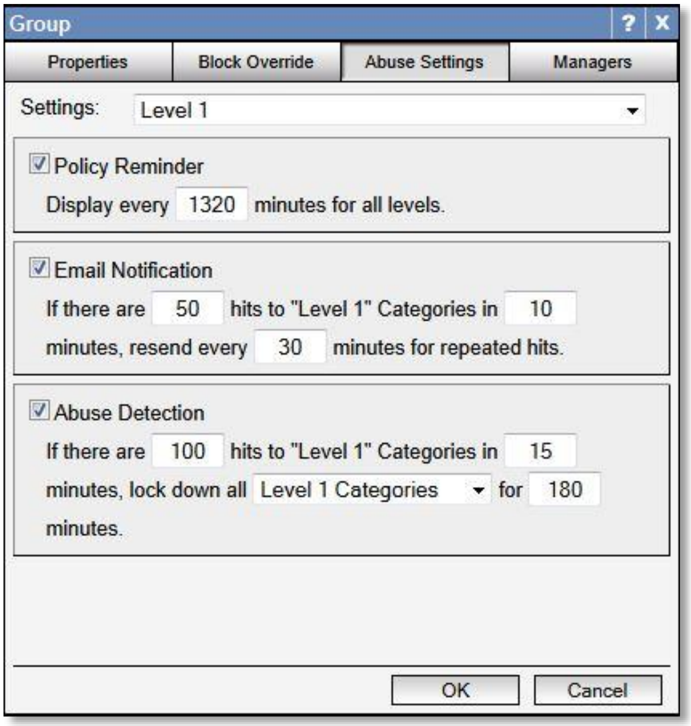
Update Time: 12:00 AM

Micro Updates: Every 10 Minutes

Days: ☑ Sunday ☑ Monday ☑ Tuesday ☑ Wednesday ☑ Thursday ☑ Friday ☑ Saturday

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.



Settings: Level 1

☑ Policy Reminder

Display every 1320 minutes for all levels.

☑ Email Notification

If there are 50 hits to "Level 1" Categories in 10 minutes, resend every 30 minutes for repeated hits.

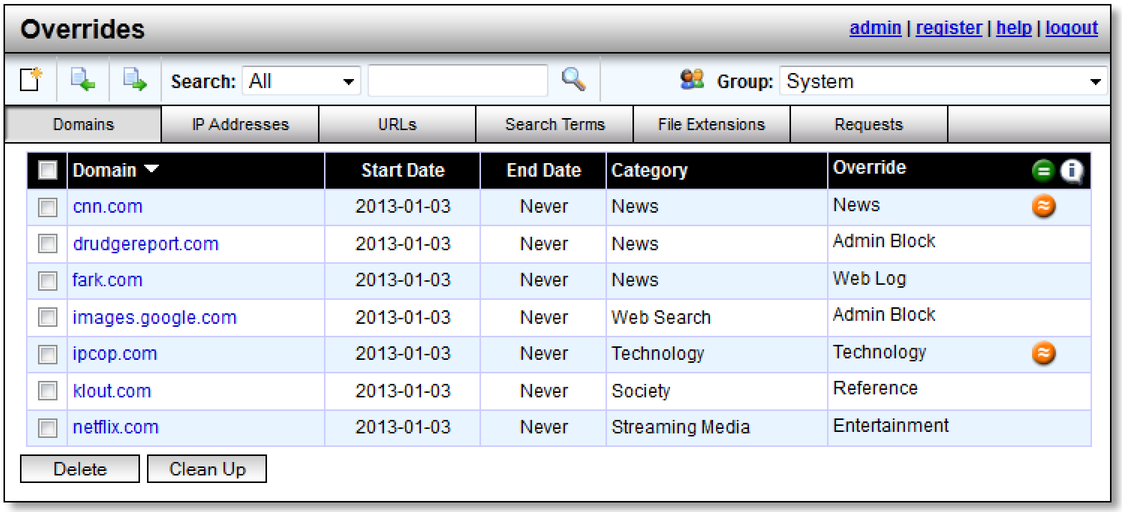
☑ Abuse Detection

If there are 100 hits to "Level 1" Categories in 15 minutes, lock down all Level 1 Categories for 180 minutes.

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.



☐	Domain	Start Date	End Date	Category	Override
☐	cnn.com	2013-01-03	Never	News	News
☐	drudgereport.com	2013-01-03	Never	News	Admin Block
☐	fark.com	2013-01-03	Never	News	Web Log
☐	images.google.com	2013-01-03	Never	Web Search	Admin Block
☐	ipcop.com	2013-01-03	Never	Technology	Technology
☐	klout.com	2013-01-03	Never	Society	Reference
☐	netflix.com	2013-01-03	Never	Streaming Media	Entertainment

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.

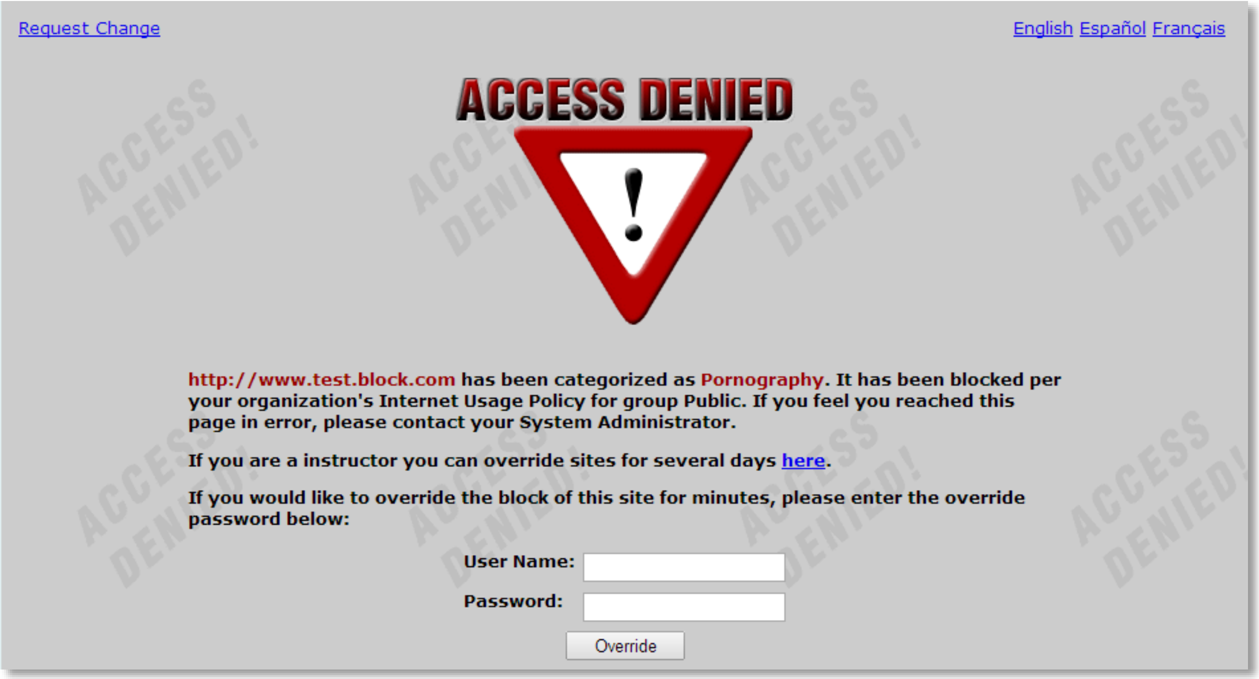
Override Request

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.



http://www.test.block.com has been categorized as Pornography. It has been blocked per your organization's Internet Usage Policy for group Public. If you feel you reached this page in error, please contact your System Administrator.

If you are a instructor you can override sites for several days here.

If you would like to override the block of this site for minutes, please enter the override password below:

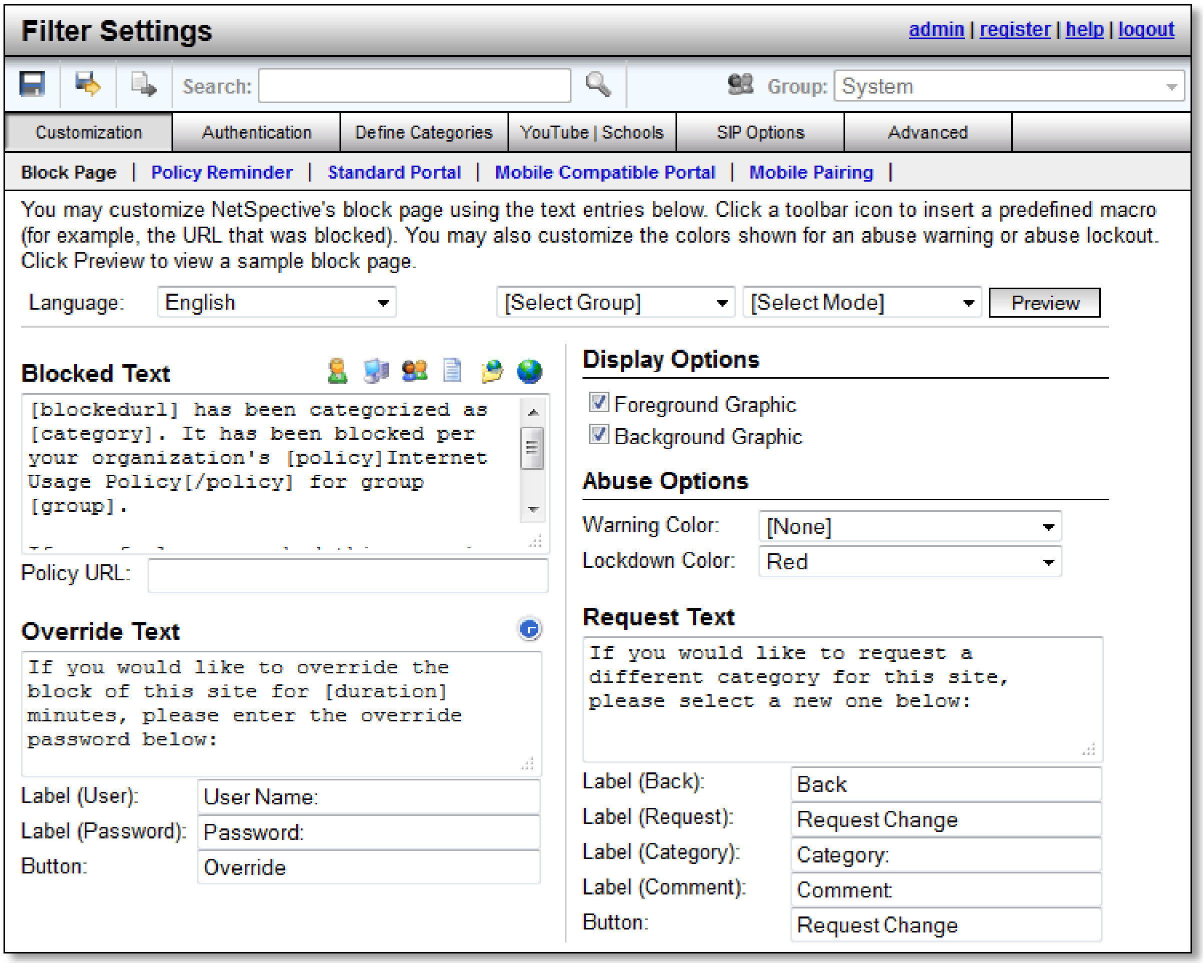
User Name:

Password:

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.


Filter Settings
admin | register | help | logout
Search:
Group: System
Customization
Authentication
Define Categories
YouTube | Schools
SIP Options
Advanced
Block Page | Policy Reminder | Standard Portal | Mobile Compatible Portal | Mobile Pairing |
Preview

You may customize NetSpective's block page using the text entries below. Click a toolbar icon to insert a predefined macro (for example, the URL that was blocked). You may also customize the colors shown for an abuse warning or abuse lockout. Click Preview to view a sample block page.

Language: English | [Select Group] | [Select Mode]

Blocked Text

```
[blockedurl] has been categorized as
[category]. It has been blocked per
your organization's [policy]Internet
Usage Policy[/policy] for group
[group].
```

Policy URL:

Override Text

```
If you would like to override the
block of this site for [duration]
minutes, please enter the override
password below:
```

Label (User):	User Name:
Label (Password):	Password:
Button:	Override

Display Options

☑ Foreground Graphic
☑ Background Graphic

Abuse Options

Warning Color:	[None]
Lockdown Color:	Red

Request Text

```
If you would like to request a
different category for this site,
please select a new one below:
```

Label (Back):	Back
Label (Request):	Request Change
Label (Category):	Category:
Label (Comment):	Comment
Button:	Request Change

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.

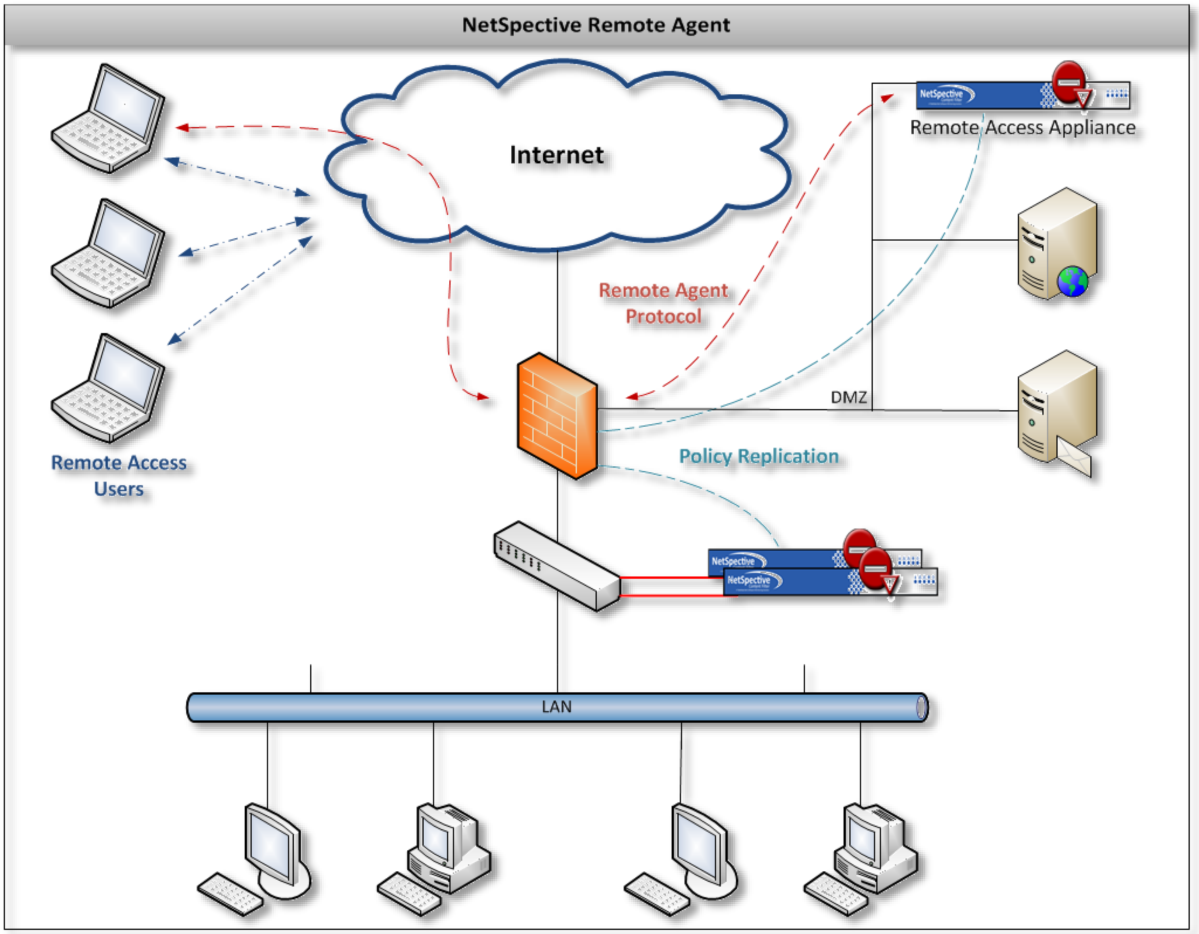
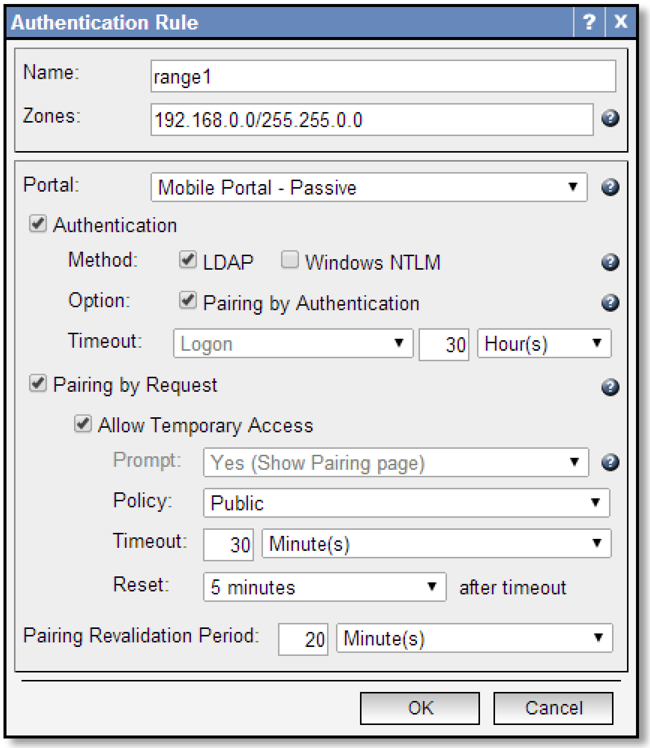


Image depicts an example of how the Remote Agent can operate. Remote Agent technology only requires one appliance so long as the appliance has an internal LAN IP address and an IP address outside of the network.

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.



Authentication Rule

Name: range1

Zones: 192.168.0.0/255.255.0.0

Portal: Mobile Portal - Passive

☑ Authentication

Method: ☑ LDAP ☐ Windows NTLM

Option: ☑ Pairing by Authentication

Timeout: Logon 30 Hour(s)

☑ Pairing by Request

☑ Allow Temporary Access

Prompt: Yes (Show Pairing page)

Policy: Public

Timeout: 30 Minute(s)

Reset: 5 minutes after timeout

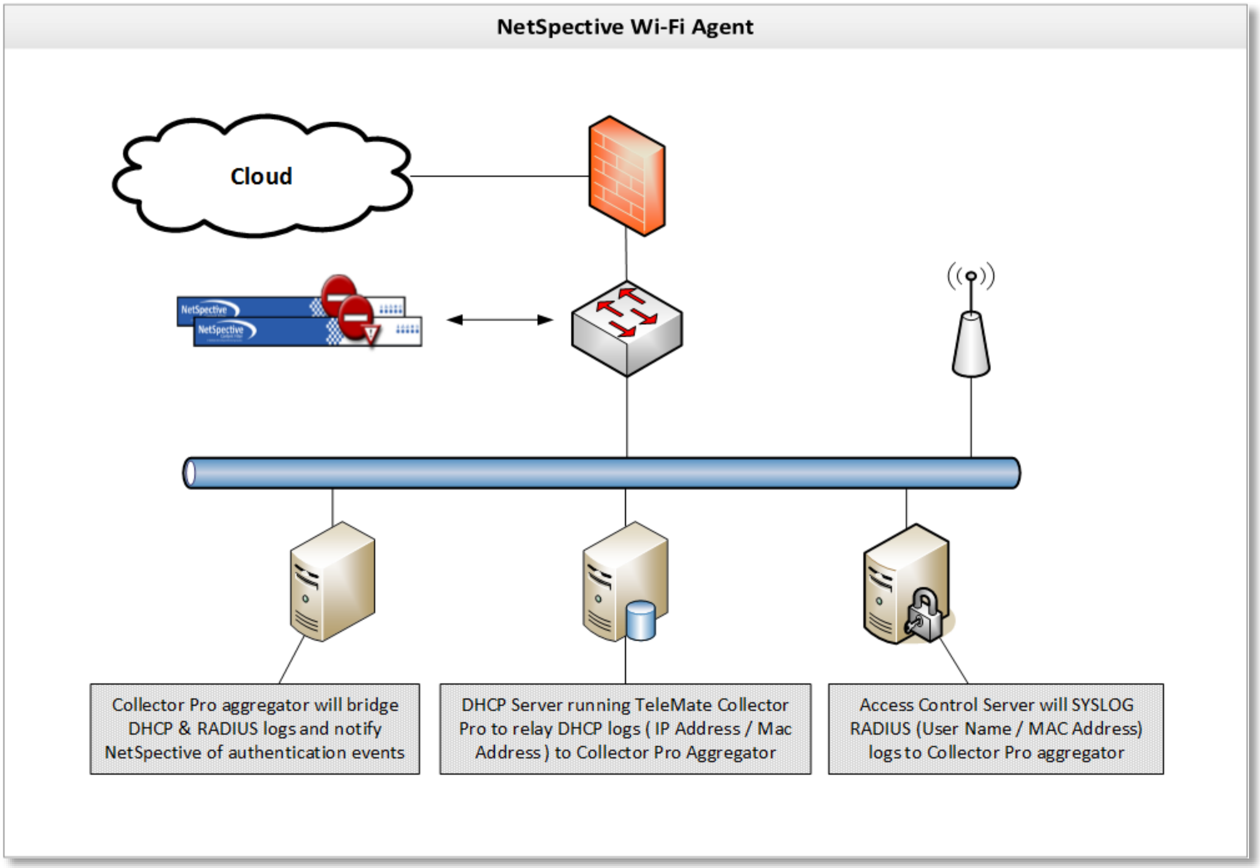
Pairing Revalidation Period: 20 Minute(s)

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).

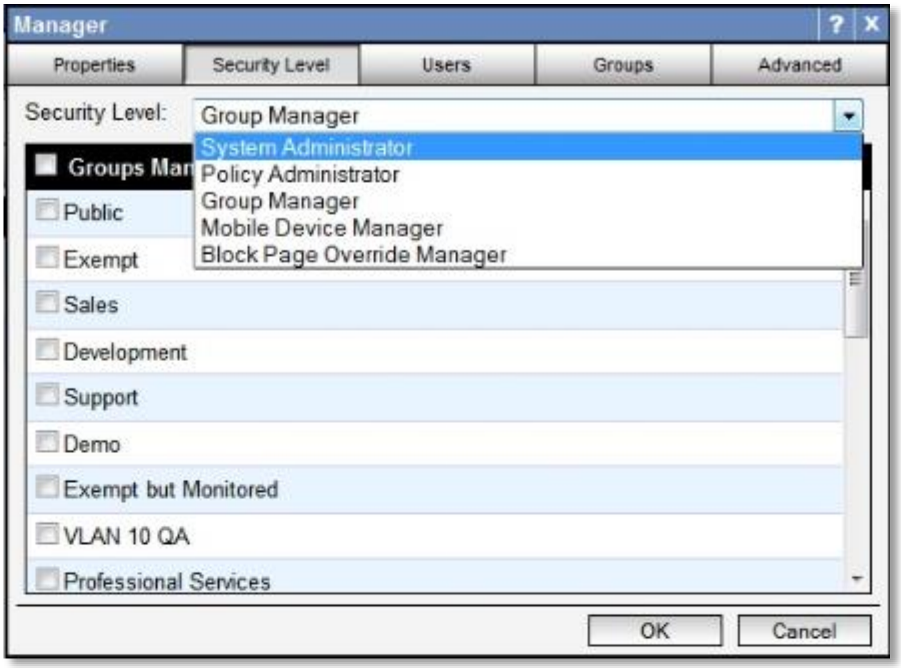

NetSpective Wi-Fi Agent
Cloud
NetSpective
NetSpective
Collector Pro aggregator will bridge DHCP & RADIUS logs and notify NetSpective of authentication events
DHCP Server running TeleMate Collector Pro to relay DHCP logs (IP Address / Mac Address) to Collector Pro Aggregator
Access Control Server will SYSLOG RADIUS (User Name / MAC Address) logs to Collector Pro aggregator

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: Group Manager

□ Groups Man

□ Public
□ Exempt
□ Sales
□ Development
□ Support
□ Demo
□ Exempt but Monitored
□ VLAN 10 QA
□ Professional Services

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.

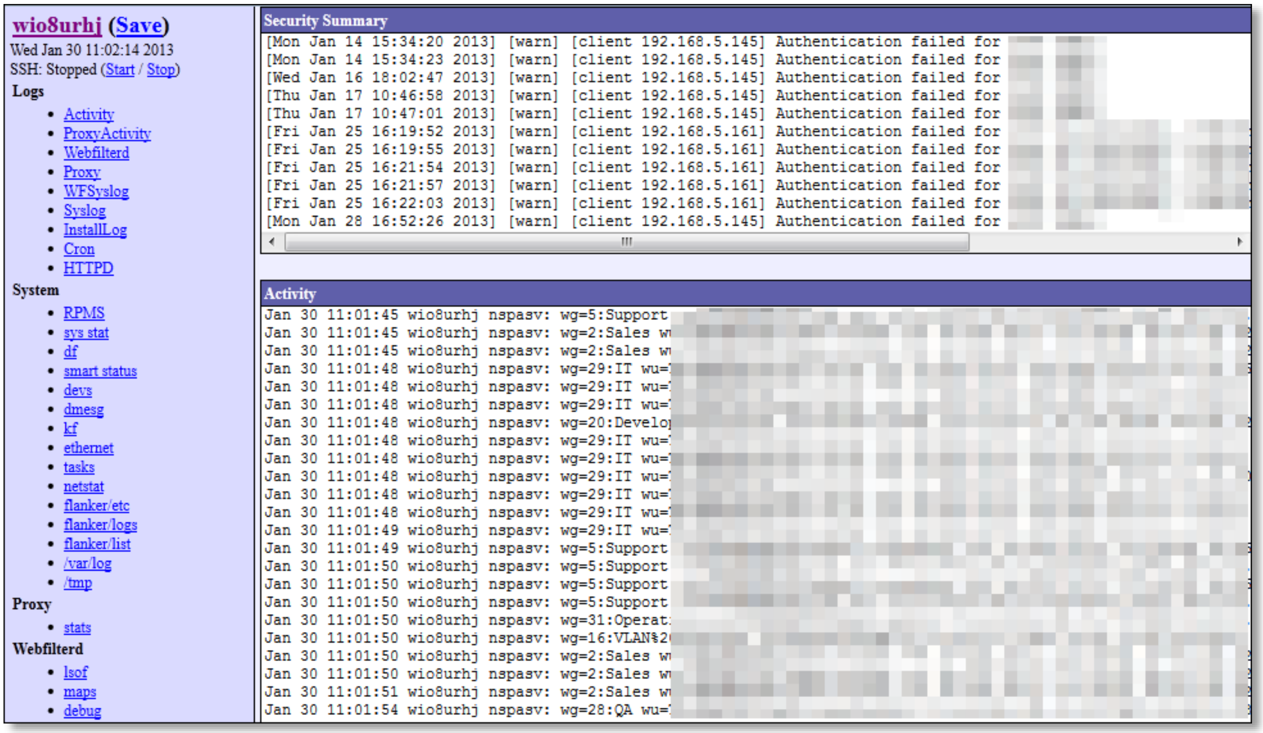
Managers can be configured to have emails sent to them automatically by the appliance. This feature can provide notifications for product updates, abuse detection, as well as block page overrides.

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.



wio8urhj (Save)
Wed Jan 30 11:02:14 2013
SSH: Stopped (Start / Stop)

Logs

- Activity
- ProxyActivity
- Webfilterd
- Proxy
- WFSyslog
- Syslog
- InstallLog
- Cron
- HTTPD

System

- RPMS
- sys stat
- df
- smart status
- devs
- dmesg
- kf
- ethernet
- tasks
- netstat
- flanker/etc
- flanker/logs
- flanker/list
- /var/log
- /tmp

Proxy

- stats

Webfilterd

- lsof
- maps
- debug

Security Summary

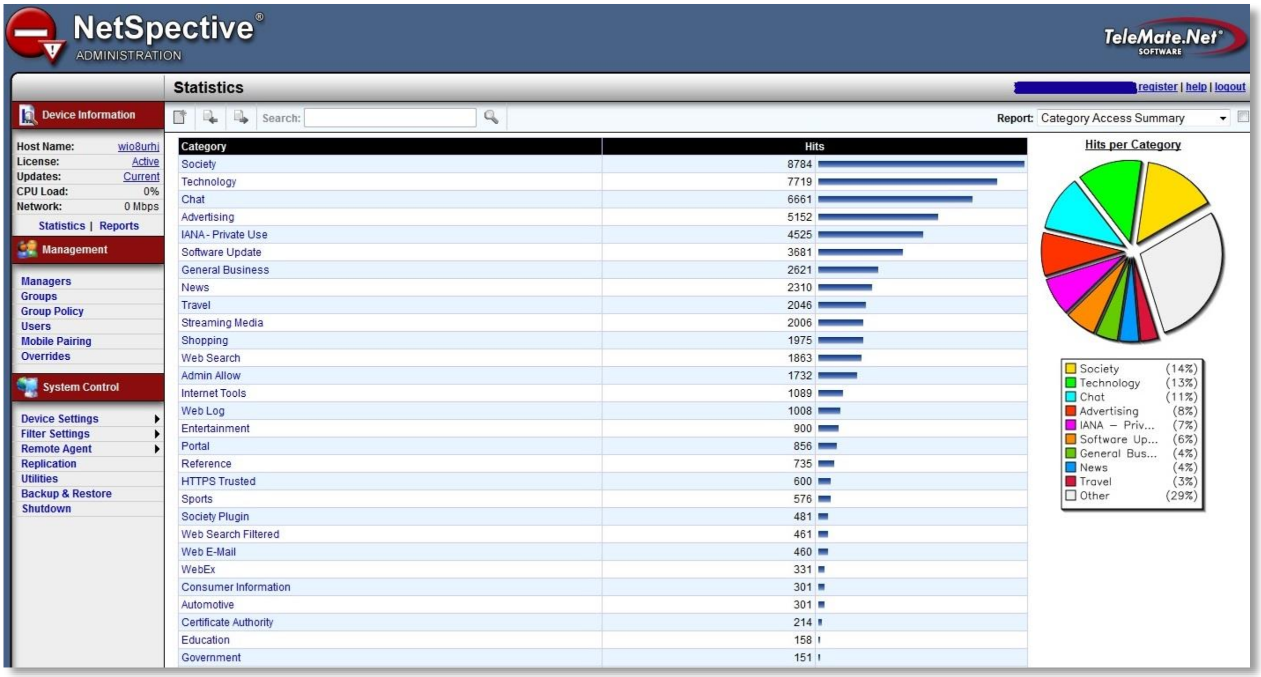
```
[Mon Jan 14 15:34:20 2013] [warn] [client 192.168.5.145] Authentication failed for [redacted]
[Mon Jan 14 15:34:23 2013] [warn] [client 192.168.5.145] Authentication failed for
[Wed Jan 16 18:02:47 2013] [warn] [client 192.168.5.145] Authentication failed for
[Thu Jan 17 10:46:58 2013] [warn] [client 192.168.5.145] Authentication failed for
[Thu Jan 17 10:47:01 2013] [warn] [client 192.168.5.145] Authentication failed for
[Fri Jan 25 16:19:52 2013] [warn] [client 192.168.5.161] Authentication failed for
[Fri Jan 25 16:19:55 2013] [warn] [client 192.168.5.161] Authentication failed for
[Fri Jan 25 16:21:54 2013] [warn] [client 192.168.5.161] Authentication failed for
[Fri Jan 25 16:21:57 2013] [warn] [client 192.168.5.161] Authentication failed for
[Fri Jan 25 16:22:03 2013] [warn] [client 192.168.5.161] Authentication failed for
[Mon Jan 28 16:52:26 2013] [warn] [client 192.168.5.145] Authentication failed for
```

Activity

```
Jan 30 11:01:45 wio8urhj nspasv: wg=5:Support [redacted]
Jan 30 11:01:45 wio8urhj nspasv: wg=2:Sales w
Jan 30 11:01:45 wio8urhj nspasv: wg=2:Sales w
Jan 30 11:01:48 wio8urhj nspasv: wg=29:IT wu=
Jan 30 11:01:48 wio8urhj nspasv: wg=29:IT wu=
Jan 30 11:01:48 wio8urhj nspasv: wg=29:IT wu=
Jan 30 11:01:48 wio8urhj nspasv: wg=20:Develo
Jan 30 11:01:48 wio8urhj nspasv: wg=29:IT wu=
Jan 30 11:01:48 wio8urhj nspasv: wg=29:IT wu=
Jan 30 11:01:48 wio8urhj nspasv: wg=29:IT wu=
Jan 30 11:01:48 wio8urhj nspasv: wg=29:IT wu=
Jan 30 11:01:48 wio8urhj nspasv: wg=29:IT wu=
Jan 30 11:01:49 wio8urhj nspasv: wg=29:IT wu=
Jan 30 11:01:49 wio8urhj nspasv: wg=5:Support
Jan 30 11:01:50 wio8urhj nspasv: wg=5:Support
Jan 30 11:01:50 wio8urhj nspasv: wg=5:Support
Jan 30 11:01:50 wio8urhj nspasv: wg=5:Support
Jan 30 11:01:50 wio8urhj nspasv: wg=31:Operat
Jan 30 11:01:50 wio8urhj nspasv: wg=16:VLAN%2
Jan 30 11:01:50 wio8urhj nspasv: wg=2:Sales w
Jan 30 11:01:50 wio8urhj nspasv: wg=2:Sales w
Jan 30 11:01:51 wio8urhj nspasv: wg=2:Sales w
Jan 30 11:01:54 wio8urhj nspasv: wg=28:QA wu=
```

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.



Host Name: wio8urhj
License: Active
Updates: Current
CPU Load: 0%
Network: 0 Mbps

Report: Category Access Summary

Category	Hits
Society	8784
Technology	7719
Chat	6661
Advertising	5152
IANA - Private Use	4525
Software Update	3681
General Business	2621
News	2310
Travel	2046
Streaming Media	2006
Shopping	1975
Web Search	1863
Admin Allow	1732
Internet Tools	1089
Web Log	1008
Entertainment	900
Portal	856
Reference	735
HTTPS Trusted	600
Sports	576
Society Plugin	481
Web Search Filtered	461
Web E-Mail	460
WebEx	331
Consumer Information	301
Automotive	301
Certificate Authority	214
Education	158
Government	151

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.

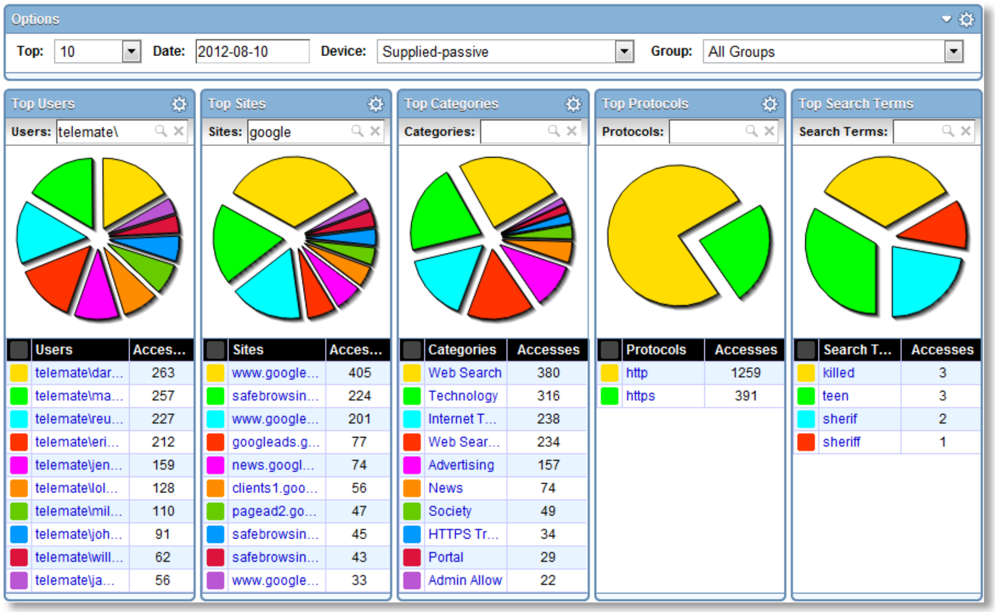
NetAuditor is provided for ‘off-the-box’ reporting. This can install any Windows based server, VM, or desktop. NetAuditor can also report on firewall logs from many popular manufacturers for various net flow statistics.

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.



Options

Top: 10 Date: 2012-08-10 Device: Supplied-passive Group: All Groups

Top Users — Users: telemate\

	Users	Acces...
🟨	telemate\dar...	263
🟩	telemate\ma...	257
🟦	telemate\reu...	227
🟥	telemate\eri...	212
🟪	telemate\jen...	159
🟧	telemate\lol...	128
🟩	telemate\mil...	110
🟦	telemate\joh...	91
🟥	telemate\will...	62
🟪	telemate\ja...	56

Top Sites — Sites: google

	Sites	Acces...
🟨	www.google...	405
🟩	safebrowsin...	224
🟦	www.google...	201
🟥	googleads.g...	77
🟪	news.googl...	74
🟧	clients1.goo...	56
🟩	pagead2.go...	47
🟦	safebrowsin...	45
🟥	safebrowsin...	43
🟪	www.google...	33

Top Categories — Categories:

	Categories	Accesses
🟨	Web Search	380
🟩	Technology	316
🟦	Internet T...	238
🟥	Web Sear...	234
🟪	Advertising	157
🟧	News	74
🟩	Society	49
🟦	HTTPS Tr...	34
🟥	Portal	29
🟪	Admin Allow	22

Top Protocols — Protocols:

	Protocols	Accesses
🟨	http	1259
🟩	https	391

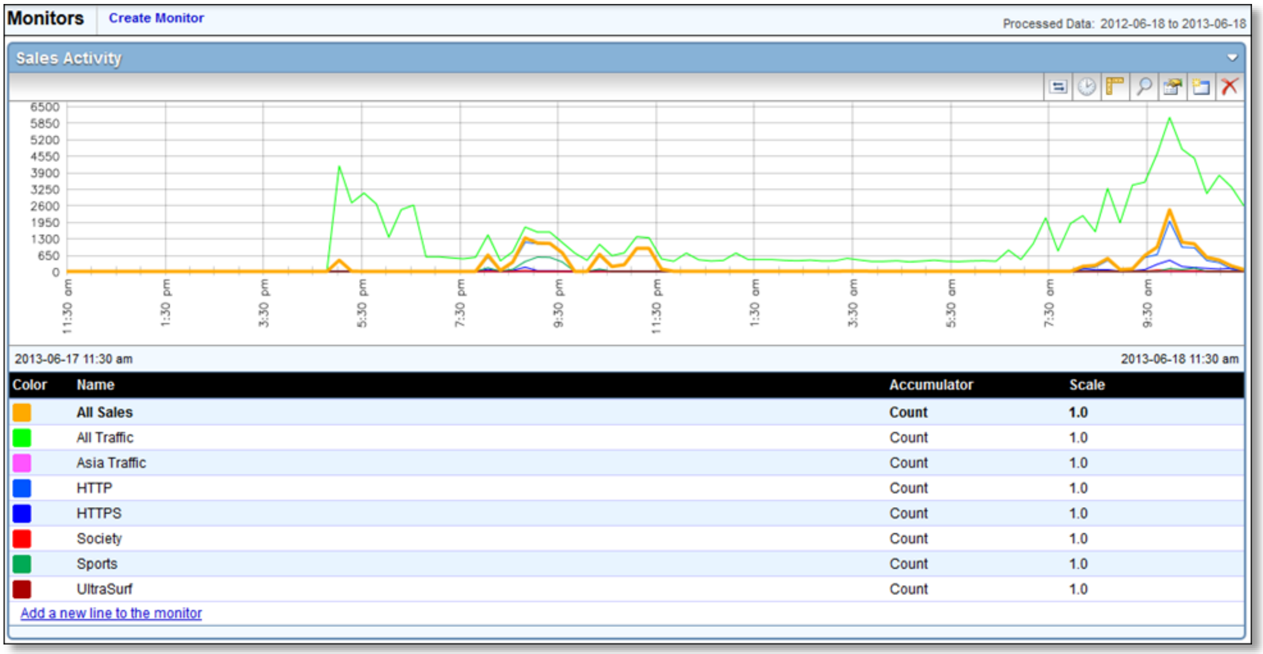
Top Search Terms — Search Terms:

	Search T...	Accesses
🟨	killed	3
🟩	teen	3
🟦	sherif	2
🟥	sheriff	1

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.



Processed Data: 2012-06-18 to 2013-06-18

2013-06-17 11:30 am

2013-06-18 11:30 am

Color	Name	Accumulator	Scale
🟧	**All Sales**	**Count**	**1.0**
🟩	All Traffic	Count	1.0
🟪	Asia Traffic	Count	1.0
🟦	HTTP	Count	1.0
🟦	HTTPS	Count	1.0
🟥	Society	Count	1.0
🟩	Sports	Count	1.0
🟫	UltraSurf	Count	1.0

Security Management

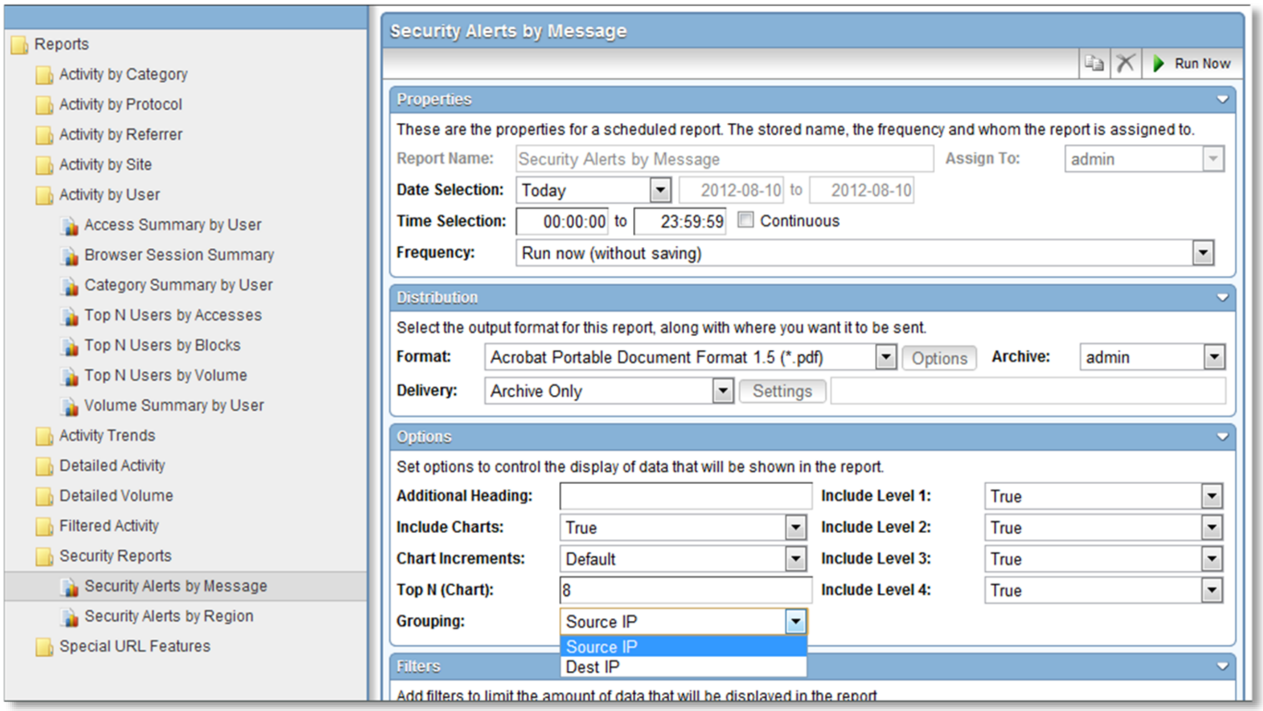
User groups are important in NetAuditor for a number of reasons. In addition to providing a cleaner way to group/filter/search your users when viewing your network traffic, it is also the primary means of providing access control to your manager accounts. For example, if you want a teacher to be able 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.



Security Alerts by Message

Properties

These are the properties for a scheduled report. The stored name, the frequency and whom the report is assigned to.

Report Name: Security Alerts by Message Assign To: admin
Date Selection: Today 2012-08-10 to 2012-08-10
Time Selection: 00:00:00 to 23:59:59 □ Continuous
Frequency: Run now (without saving)

Distribution

Select the output format for this report, along with where you want it to be sent.

Format: Acrobat Portable Document Format 1.5 (*.pdf) Options Archive: admin
Delivery: Archive Only Settings

Options

Set options to control the display of data that will be shown in the report.

Additional Heading: Include Level 1: True
Include Charts: True Include Level 2: True
Chart Increments: Default Include Level 3: True
Top N (Chart): 8 Include Level 4: True
Grouping: Source IP (Source IP, Dest IP)

Filters

Add filters to limit the amount of data that will be displayed in the report.

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.