|  |
| --- |
| **Des Moines Public Schools** |
| NetSpective Content Filtering Proposal |
| **Riverside Technologies** |

|  |
| --- |
|  |

Contents

[Executive Summary](#_Toc384211975)

TeleMate Contact Information

TeleMate's Experience

References

[Deployment](#_Toc384211976)

Turnkey Deployment

Not a Point-of-Failure & Deployment

Scalability

[Filtering Solution](#_Toc384211318)

Pre-defined Categories & Granular Control

Exempt Groups

Automatic Updates

"Safe-search"

Allow, Monitor, or Block Traffic

Abuse Detection

User-defined Categories

Blocks Sub-URL Traffic

Wildcard URLs

Peer-to-peer Protocols

Chat Protocols

Streaming Video/Radio

Anonymous Proxies

Society(Facebook)

Blocking Subdomains

Overrides

Exempt Groups

Block Page Overrides

Email for Excessive Overrides

Mis-categorized Sites

Whitelists & Blacklists

List of Site Overrides

YouTube for Education

Categorization

Which Category?

Block Page Customization

CIPA Compliance

IPV6

HTTPS Filtering

HTTPS-Adaptive Filtering

Authentication

Directory Servers

Mobile Portal

Wifi Agent

Remote Agent

Global Proxy

Session Timeframe

Management Access

Concurrent Users

Automatic Daily Backups

Policy Replication

Reporting/NetAuditor

Popular Reports

Log Files

Log Transfer

Multi-tenancy Management

Sub-Administrator's View

Maintenace, Warranty, Service Level Agreement

Appendix A: [Category List](#_Toc384211320)

# EXECUTIVE SUMMARY

Riverside Technologies will provide Des Moines Public School District (DMPS) with the NetSpective Internet content filtering appliance which is consistent with the CIPA guidelines and compatible with the DMPS network. NetSpective is a sophisticated Internet content filtering appliance that maximizes the performance and security of your data network by eliminating undesirable web traffic including URL, HTTP, HTTPS, Anonymous Proxies, FTP, NNTP, Chat, Peer-to-Peer, Skype™, VoIP, and Streaming Media. Its rack-mount configuration easily connects to your network, and its filtering and operational controls are simple and flexible. The web hosted interface provides real-time status updates and control, including compliance with federal filtering mandates and communications tracking requirements. NetAuditor will provide comprehensive, real-time, and alarming reports for both the NetSpective and firewall logs.

The NetSpective appliance provided will not be a point-of-failure on DMPS’ network nor will it introduce any added latency. Its 10 Gbps interface will be capable of filtering up to 100,000,000 web connections daily.

An unlimited user license will be provided to allow for DMPS’ growing student population and device counts. Also, the pricing provided is all-inclusive: the hardware appliance, categorization subscription, NetAuditor Reporting (for both NetSpective logs and firewall logs), all methods of authentication, warranty, maintenance, and service.

**TeleMate Contact Information**

Shawn Harrington

678-589-3730

[Shawn.harrington@telemate.net](mailto:Shawn.harrington@telemate.net)

5555 Triangle Pkwy, Norcross, GA 30092

TeleMate.Net Software, Territory Manager 2000-2004 & 2013-present

MBA, BBA

Bill Babij

678-589-3630j

[William.babij@telemate.net](mailto:William.babij@telemate.net)

5555 Triangle Pkwy, Norcross, GA 30092

Sales Engineer, 2012-present

**TeleMate’s Experience**

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.

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

# REFERENCES

Keith Sandvall

**Sioux Falls Public Schools**

1101 North Western Ave

Sioux Falls, SD 57104

[Keith.Sandvall@k12.sd.us](mailto:Keith.Sandvall@k12.sd.us)

605-367-8432

Tim Smith

**ESC - Region 16**

5800 Bell Street

Amarillo, TX 79109

[Tim.Smith@ESC16.net](mailto:Tim.Smith@ESC16.net)

806-677-5254

Daniel Rebollar

**ESC – Region 1**

1900 W WSchunior

Edinburg, TX 78539

[drebollar@esc1.net](mailto:drebollar@esc1.net)

956-984-6076

# DEPLOYMENT

**Turnkey Deployment**

Riverside Technologies (RTI) will provide a total turnkey Internet filtering to Des Moines Public Schools. RTI will go onsite to Des Moines and fully implement the NetSpective solution. We will set-up customized settings to allow for multiple polices for user groups and device types. RTI also will set up any requested reports. Report recommendations also will be made based upon needs.

RTI will deploy a 10Gig NetSpective appliance. An optional failover appliance is available upon request. This appliance will be licensed for an unlimited amount of users. As the district’s network grows, no re-licensing will be necessary.

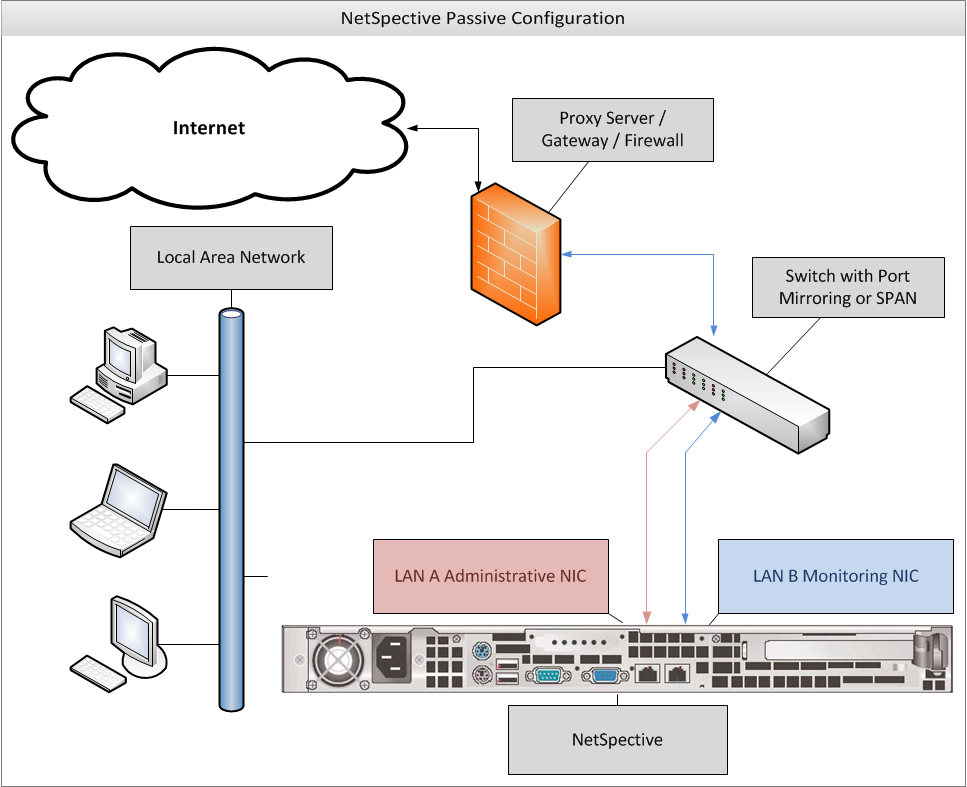
[](http://www.getnetspective.com/products/netspective/)

**Not a Point-of-Failure & 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**

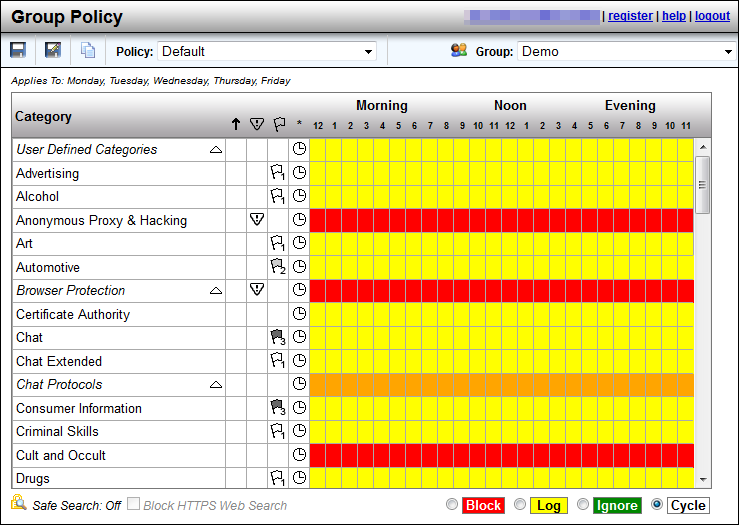
The use of 10 Gig appliances with an unlimited amount of users will allow Des Moines to scale to 10 Gigs of traffic on their network. No additional licensing will be required as the network grows.

# ****FILTERING SOLUTION****

**Pre-defined Categories & Granular 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.



**Exempt Group**

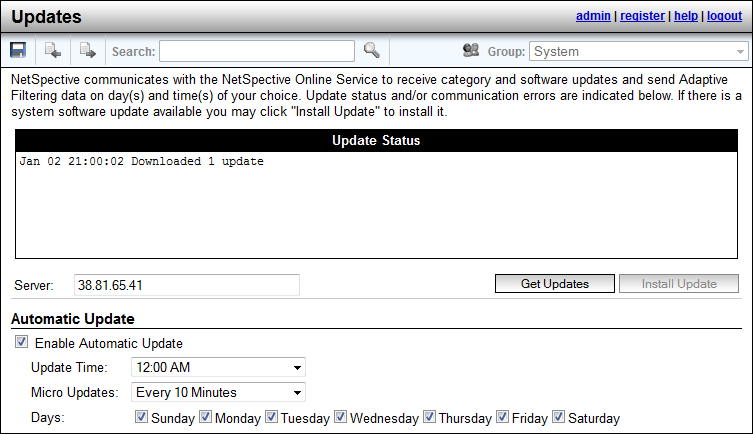
A group of users, specified user, or IP address can either be monitored, allowed or blocked by our predefined categories or a list of customized categories. Access can be defined by day-of-the-week and time-of-day.

The Exempt group is never blocked and is exempt from all overrides.

**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.



**“Safe-search”**

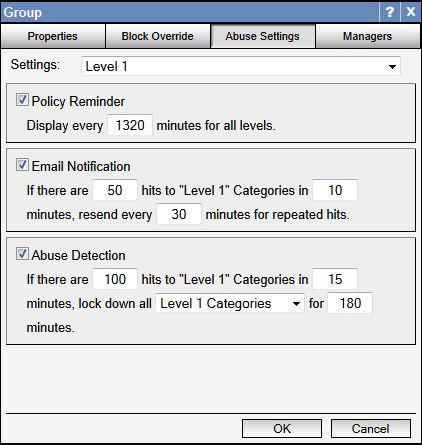
NetSpective supports Safe Search enforcement for sites that support searching the Web, news groups, or indices and directories thereof. These engines will not return objectionable content or explicit pictures. Safe search options are enforced via the Web Search Filtered category for Google, Bing, MSN,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

**Allow, Monitor, or Block Traffic**

NetSpective can be set to either monitor, allow, or block URL traffic from a predefined list as well as any sites manually entered. Each will be in effect for both HTTP and HTTPS sessions.

**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 users’ inappropriate surfing behavior, if he knows there are consequences to his action.



**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.

**Blocks Sub-URL Traffic**

Through the Overrides section, NetSpective can block or allow any domain, subdomain, URL, or sub- URL.

**Wildcard URLs**

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.

**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 Video/Radio**

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

**Anonymous Proxies**

NetSpective performs anonymous proxy filtering via our *Micro Updates* feature. New anonymous proxy sites are identified by the appliance and sent back to our labs where they are analyzed in real time. *Micro Updates* then pushes out category updates to all appliances in the field, stopping users from visiting these sites at a 10 minute interval.

**Society (Facebook)**

Facebook is categorized as ‘Society’ and is filtered differently than general web log sites which are defined as ‘Web Log’.

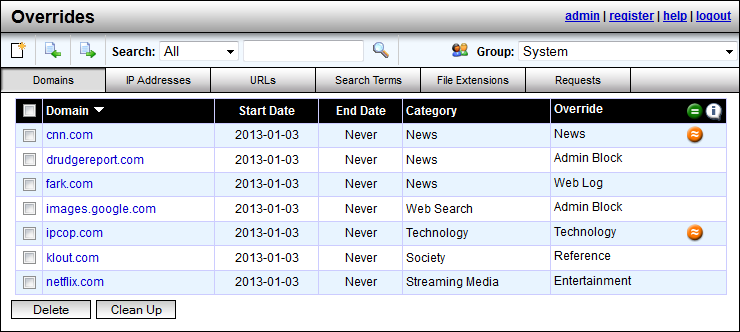
**Blocking Subdomains**

NetSpective can block access to specific URLs or subdomains while allowing access to the domain level site.

# ****OVERRIDES****

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.

****

**Exempt Group**

The Exempt group is never blocked and is exempt from all overrides. All other groups, including the Public group, have their own override lists. Additionally, system-wide overrides may be created. System level overrides are processed first and affect all groups except the Exempt group.

The web search term override feature is used to assign terms or combinations of terms used at search engines to a specific category. This feature in itself is a method of preventing a user from finding objectionable content. In addition, when a term is assigned to an abusive category that is blocked, it also triggers the abuse detection feature. Thus, a user searching for abusive content can also be given an abuse lockout.

**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.

**Email Notification for Excessive Overrides**

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.

**Mis-Categorized Site**

Administrators can easily override mis-categorized sites on the overrides page. No restarting of the system is required for overrides, and these changes are instantly applied and take effect for any profile.

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](http://www.telemate.net/services/support/url_review.php) 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.

**Whitelists & Blacklists**

The appliance supports up to 20 custom categories that can be populated with any domain, URL, IP address, search term, or file extension. The custom category can then be always blocked (black list) or always allowed (whitelist) by hour, on a group by group basis.

All custom whitelist and blacklist ‘overrides’ are communicated back to TeleMate.Net for human review.

Via the overrides page, NetSpective has the ability to block [www.goodsite.com/good-directory/badpage.html](http://www.goodsite.com/good-directory/badpage.html) while leaving the rest of [www.goodsite.com](http://www.goodsite.com) and its sub-pages unblocked.

Also via the overrides page, NetSpective can block [www.badsite.com/bad-directory](http://www.badsite.com/bad-directory), but unblocks www.badsite.com/bad-directlory/good-page.html.

Overrides are automatic and do not require rebooting of the system

**List of Site Overrides**

The overrides page displays an instant list of all site overrides. The overrides page also has an import and export feature. The entire list of overrides can be exported to a .csv file at any time.

**YouTube for EDUCATION**

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 [YouTubeEDU](http://www.youtube.com/education). 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.

# ****CATEGORIZATION****

Each site is put into only one category based upon its best ‘fit’. Specific sites can be always allowed or always blocked. A specific site being ‘white-listed’ or ‘black-listed’ takes precedence over the category it fits into.

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.

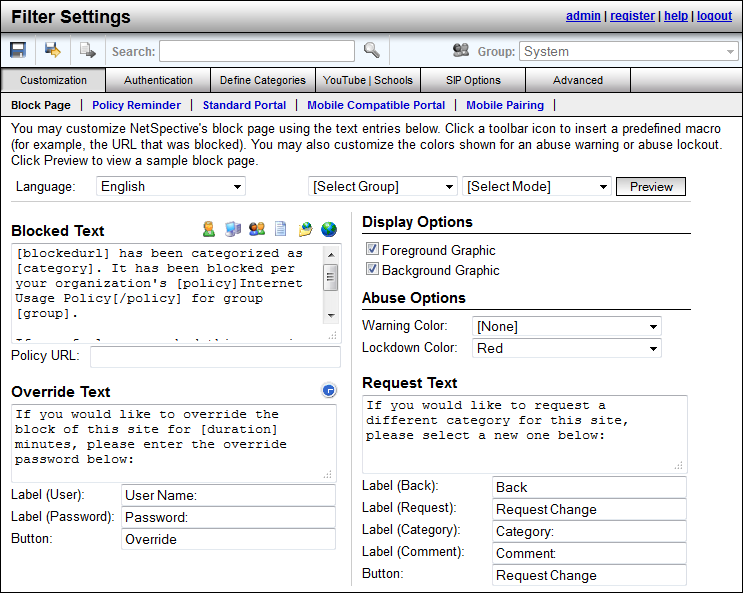
**Which Category?**

By utilizing our on-the-box reporting, an administrative user can easily look-up the category of a specific website.

# ****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.



**CIPA COMPLIANT**

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. NetSpective also provides a full CIPA compliant policy profile out of the box. Combined with our Save-To feature, you can apply our CIPA policy to all of our groups with one click, saving you time without having to set each category manually.

# ****IPV6 TRAFFIC****

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.

# ****HTTPS 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.

**HTTPS-Adaptive Filtering**

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 SSLcertificate 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

**AUTHENTICATION**

**Directory Server**

NetSpective can support Active Directory, eDirectory, or 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.

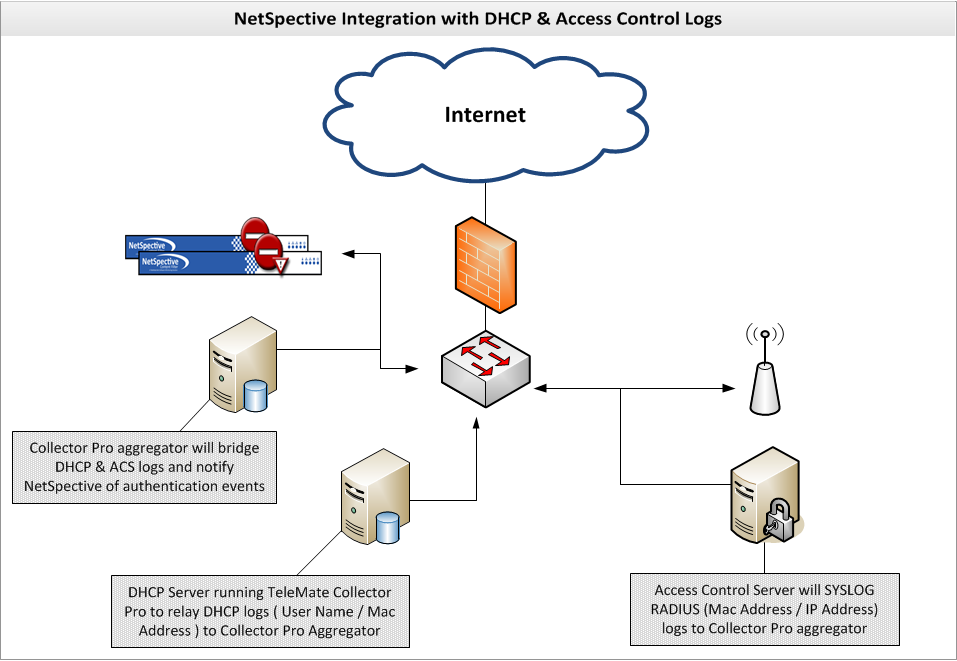
#### Mobile Portal and Mobile Portal with Pairing

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 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 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.

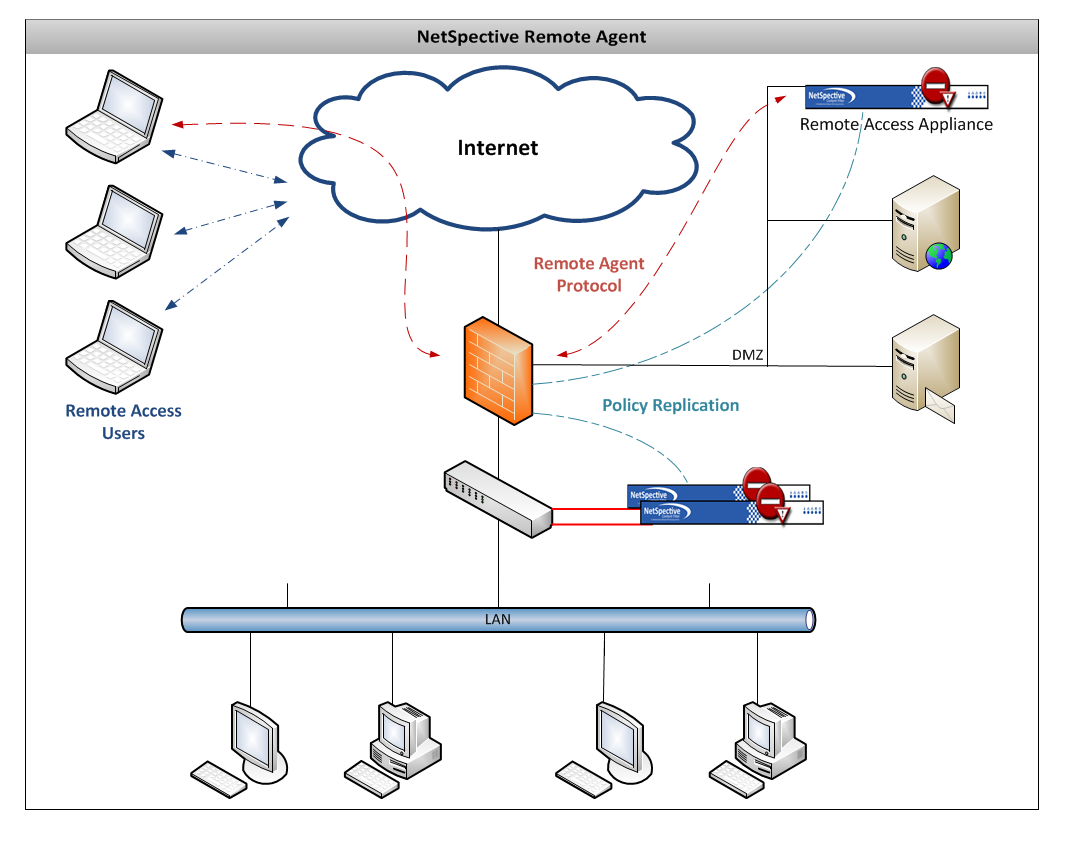


Image depicts an example of how the Remote Agent can operate. Remote Agent technology only requires one appliance so long as the appliance has an internal LAN IP address and an IP address outside of the network.

**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.

**Session Timeframe**

The administrative user has the ability to give a certain timeframe for authentication. Once a user authenticates, that user will stay logged into the filter until the session ends or the predetermined timeframe is met.

**MANAGEMENT ACCESS**

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.

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.

|  |  |
| --- | --- |
| 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. |

**Concurrent Users**

There is no defined limited to the number of concurrent and sub administrative users.

**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.

**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.

**REPORTING/NetAuditor**

NetSpective offers both on-the-box and off-the-box reporting. The NetAuditor runs on any Windows based server and comes free of charge with the NetSpective. Besides reporting off the log files of the NetSpective appliance, NetAuditor also can be set up to report off firewall logs.

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.

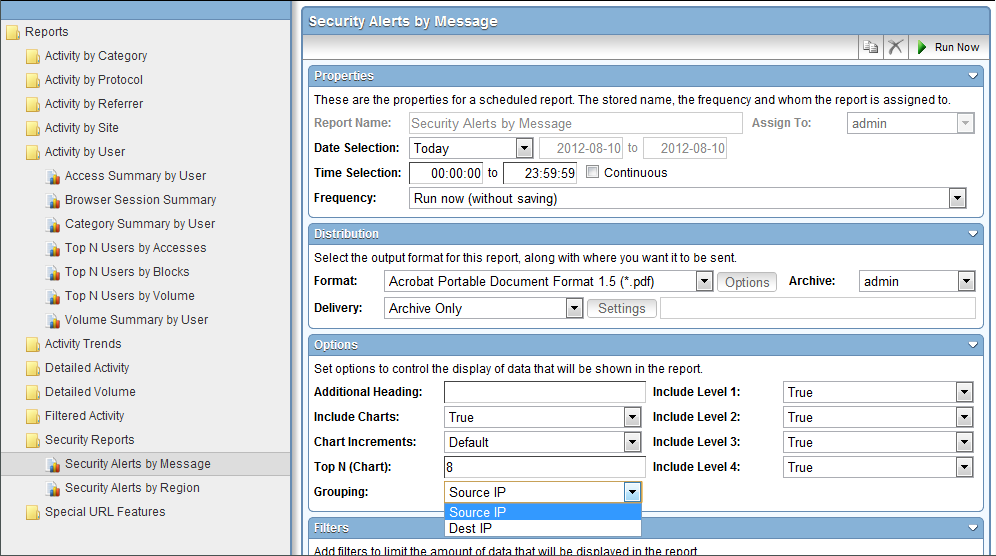
Along with our SNMP settings for alerting of box health, NetAuditor includes trend-based monitoring and notification to provide real-time awareness of traffic patterns. Where the dashboard allows you to perform "Top N" searches of your processed data, the monitors allow you to tell the NetAuditor processing 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.

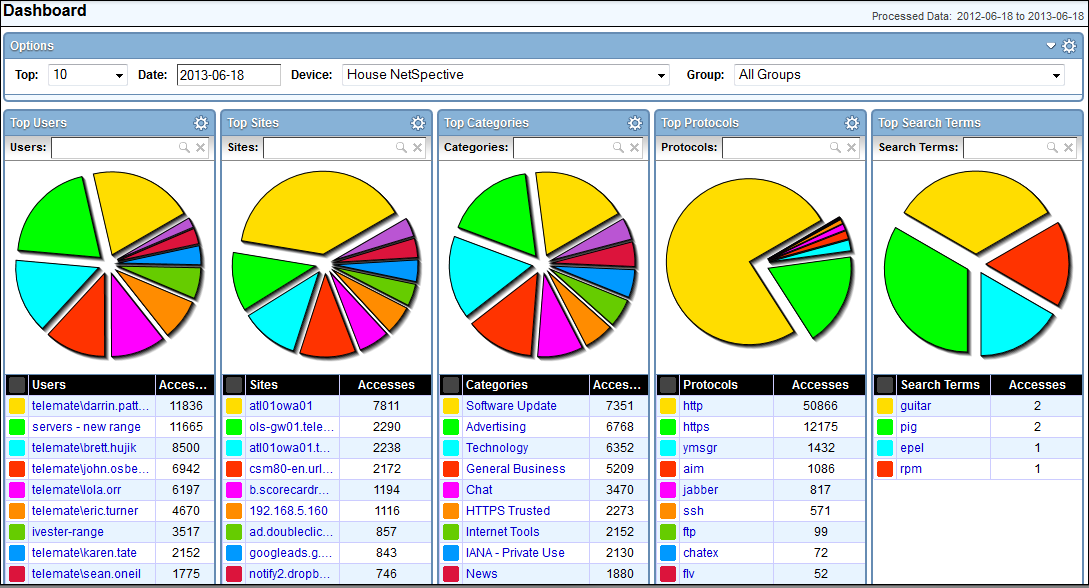
This feature is popular with our K12 customers for being used as a forensics tool. We recommend configuring monitors to track material such as search terms. A school may want to monitor sensitive search phrases such as Suicide, Bomb Making, Cyber Bullying, etc. These and any number of search terms can 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.

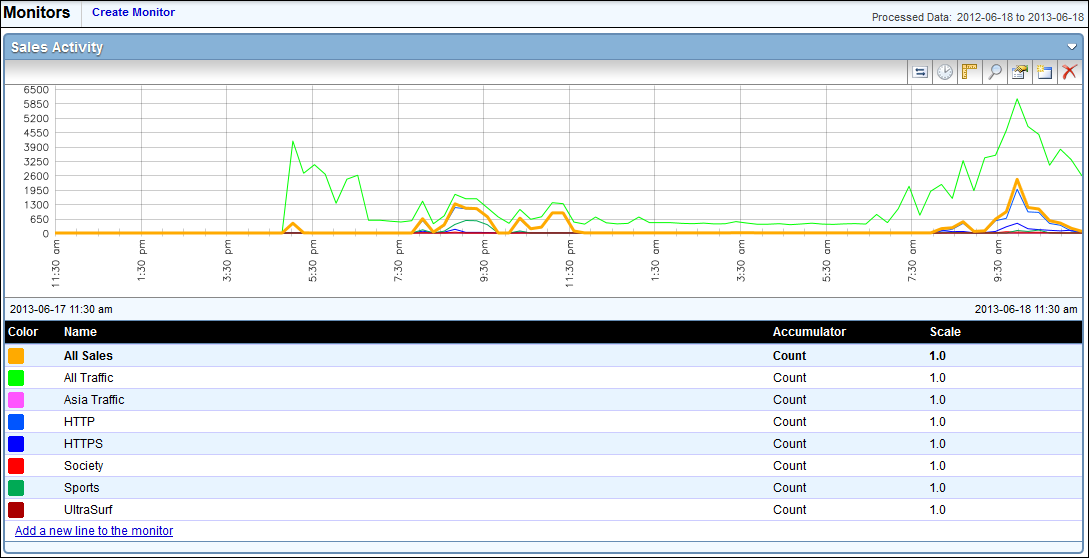
For more comprehensive information NetAuditor provides on-demand and automated reporting. Perhaps you found something in the dashboard you need more detailed information on. Perhaps you need more comprehensive summary/bandwidth reports, reports on firewall security alerts, traffic trends over time, or 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.







**Popular Reports**

Chronological Activity Detail Report

Summary Reports include:

Access Summary by Site

Category Summary by User

Volume Summary by Category

Access Reports include:

Top N Categories by Accesses

Top N Sites by Accesses

Top N Users by Accesses

Blocked Reports include:

Top N Sites by Blocks

Top N Protocols by Blocks

Top N Categories by Blocks

**Log Files**

The NetSpective appliance exports the log files in a compressed format via syslog or FTP. The NetAuditor then decompresses these log files to run reports. The following information is included: request date, time, originating client’s IP address, user id, requested URL, and the category applied to the request.

**Transfer Log Files (No Filter Interference)**

The administrator can choose to transfer log files:

* + 1. once a day
    2. every \_\_ hrs \_\_ mins
    3. on demand

The NetSpective appliance off-loads the logs and sends compressed log files to the NetAuditor which is on a separate server. Therefore, the transfer of log files does not interfere with normal filtering activity

**Multi-tenancy Management**

Sub-administrators may be assigned to run reports specific to them. The administrator will set-up which reports and filters the sub-administrator has access to. They will only have the ability to view these reports and filters.

**Sub-Administrator’s Views**

NetAuditor limits the sub-administrators log views to only their access level allowed. You can limit these managers to running reports only on certain groups of users, limiting features from the reporting product, or limiting the reports they are able to run. Depending on the level of access given, they will only be able to save and export the reports that the administrator allows them to.

**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.

**Service Level Agreement**

**APPENDIX ‘A’**

### 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, which can be seen in section [3.04](#_Overrides) of this proposal.

**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.