



Blue Coat WebFilter™ Technology

White Paper

ABSTRACT

Content filtering faces new challenges and opportunities. As the evolving Web makes managing appropriate surfing and bandwidth use more difficult, it also introduces new security threats that filtering may be uniquely well suited to address. However, the Web content security role makes inaccurate site rating, poor coverage, and delayed rating of new URLs even more costly. Millions of new URLs are created monthly, compounding the challenges. This document examines the requirements for a dynamic content filtering solution to perform an effective policy enforcement and gateway security role, and details Blue Coat WebFilter's approach.

Table of Contents

Introduction: New Challenges, New Opportunities3
Blue Coat WebFilter™4
Database Coverage4
Classification Accuracy7
Performance8
A Closer Look – Dynamic Rating8
Implications for New Security Opportunities12
Spyware12
Phishing13
IM Control14
P2P Control14
Bot Networks14
Streaming Control14
Conclusion15

INTRODUCTION: NEW CHALLENGES, NEW OPPORTUNITIES

The Web filtering challenge is changing. In the early days of URL filtering, the challenge was getting a large enough population of URLs rated to make it unlikely a student or employee could view objectionable Web pages. Back then, the primary drivers were legal liability and productivity. Early-generation filtering technology covered both bases with varying degrees of adequacy. Vendors chose Web crawlers and site mining as the fastest and easiest means of developing large URL databases, but a high percentage of the sites chosen for rating were so obscure as to be irrelevant to users. This made direct comparisons of “number of URLs rated” difficult. As vendors sought ways to extend their value and differentiation, issues such as reducing bandwidth abuse on media-rich, non-business sites received some attention as well.

New content threats provide new opportunities and new challenges for Web filtering. As firewalls and desktop antivirus became ubiquitous, hackers and unethical entrepreneurs found the only remaining open door to be the Web browser. Web content threats are the fastest growing computer danger because most organizations leave ports 80 and 443 open through their firewalls. The browser has become the soft underbelly of network security. According to Symantec, 40% of malicious attacks now target the browser.

The character of these new security threats has also changed. Traditional viruses could be detected with pattern matching and algorithms because, once released, the virus could only change in predictable ways. Spyware, on the other hand, is almost always downloaded directly from a server. To evade traditional code scanning, spyware vendors automatically recompile the spyware code (for example inserting random lines of camouflage code) between downloads. We call this evasion technique, “server-side polymorphism.” Each downloaded spyware binary can be unique, severely limiting the usefulness of traditional malware scanning.

Conversely, URL filtering is relatively efficient at blocking new and unknown spyware. The spyware binaries may change frequently, but the sites installing the spyware are more consistent. This creates new opportunities for URL filtering, but also raises the stakes if URL filtering is incomplete in its coverage or inaccurate in its site rating. Coverage and accuracy have become ever more crucial metrics of Web filtering effectiveness.

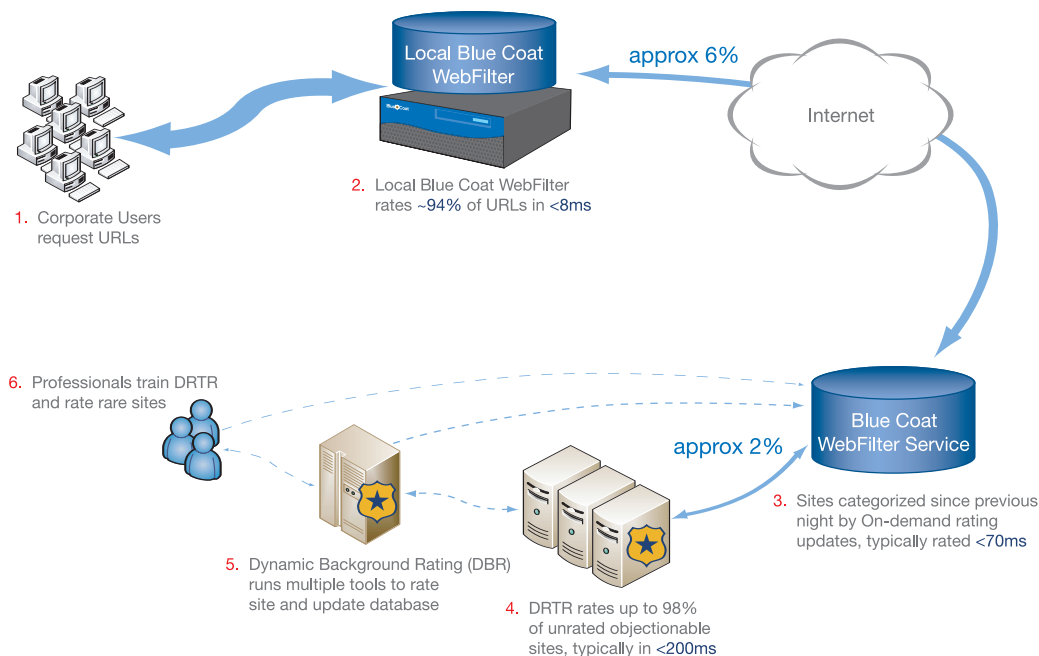
Simultaneously, traditional URL filtering is seeing its effectiveness at blocking access to inappropriate content eroded by new dynamics. As the first generation of URL filtering technologies have become pervasive, techniques to circumvent them have become widely known. Social networking makes rank-and-file workers expert enough to bypass early-generation or static URL filtering. Translation sites, archive sites, image searches, and personal proxies are frequently mentioned on message boards as means of bypassing traditional URL filtering.

Database “coverage” and classification “accuracy” are the most important factors to effectively enforce appropriate use policy and secure Web content. Without either, policies simply won’t work and users will be vulnerable. To be viable, a Web filtering architecture must be as “future proof” as possible to ensure coverage is optimized for both known and new Web pages. The architecture must also provide a means of accurately reflecting the complexity inherent in contemporary Web pages. Overly simplified rating structures are quickly overwhelmed by millions of unique, and often multi-disciplinary, Web sites. These are just a few of the many elements that must be addressed to deliver a high database coverage rate with highly accurate classification. A more in-depth look is provided later in this document.

BLUE COAT WEBFILTER™

Blue Coat WebFilter is an “on-proxy” web filtering solution that enables enterprises and service providers to protect their users and networks from Internet threats and abuse, including spyware; phishing attacks; P2P, IM and streaming traffic; adult content; and others.

WebFilter includes over fifteen million ratings, representing billions of Web pages, organized into the most useful categories. To ensure accuracy, each site can be classified into multiple categories, which also allows customers to define an unlimited number of “cross-categories” to fit specific requirements (for example block a site that is categorized as both SPORTS and GAMBLING or block a site that is in ADULT CONTENT except if it is also in HEALTH). To address sites not classified, each license includes Dynamic Real-Time Rating (DRTR™), a technology that categorizes web sites on-the-fly as a user attempts access. Blue Coat WebFilter runs on Blue Coat SG appliances, which provide the world’s fastest proxy caching platform and most flexible policy enforcement. As various aspects of filtering are discussed, Blue Coat WebFilter’s approach will be noted as a reference. Later, we will provide a more detailed look at key Blue Coat WebFilter technologies, including Dynamic Real-Time Rating.



Database Coverage

Coverage is the ability of a filtering product to identify all websites which should be placed in a given category. Coverage answers the question, “Of 100 websites that were actually category ‘X’ (Pornography, Spyware, Gambling, etc.), how many did the filter actually categorize as ‘X’?” The higher the percentage is, then the greater the filter’s coverage.

To have the best coverage, a web filtering product must be able to:

- **Rate domains (rather than URL or IP address) where appropriate**

An individual domain may have thousands of unique URLs underneath it. New URLs may be added under these domains daily, or in some cases, by the minute. For homogenous domains, there are coverage and performance advantages to rating the domain instead of

the URL or IP. By rating the domain, all new URLs added under that domain are instantly covered. This also requires less space in the database, which improves overall performance. Blue Coat WebFilter rates approximately 9 million domains and directories and several million IP addresses to cover billions of unique Web pages.

- **Categorize websites by IP address, as well as by URL as appropriate**

Websites are accessed not only via URL, but also via IP address. Although this sounds simplistic, not all filtering products are able to categorize both. Some early-generation filtering products attempt to infer ratings for requested IP addresses from known URLs by using reverse-DNS lookups, but this is slow and unreliable. Blue Coat WebFilter categorizes millions of IP addresses to ensure a rating regardless of how a site is accessed. Blue Coat also takes into account when a common IP address is used to host several sites with varying content (as reflected in their URL ratings). Blue Coat harvests IP addresses from around the world to have more than just the North-American host-to-IP mappings (as the same domain has several sites around the world). Blue Coat's approach maximizes coverage.

- **Rate sites harvested primarily from user requests**

Another measure of coverage quality is the relevance of a filtering database. No vendor can rate all 16 billion+ web pages on the Web, and it's not necessary to do so. A large percentage of those pages are defunct or so obscure that including a rating adds no value. They are not relevant for policy enforcement, yet do add a performance cost and hence should be avoided. This raises the question, "What techniques ensure that the sites a user is most likely to visit are most likely to be rated?" The answer is simple, although uncommon in the URL filtering industry. Blue Coat WebFilter prioritizes sites users actually visit into the filtering database. This is made feasible by Blue Coat's Dynamic Real-Time Rating (DRTR™) technology (see below). The only types of sites that are not selected for rating based on user traffic are classes of malware sites that can be proactively found via "honey pots" and other data mining.

- **Transparently Pull Updates On Demand**

Being able to pull new ratings on demand as needed provides better real-time coverage than frequently pushing batches of recent URL ratings to the local copy of the filtering database. Automated pulling checks for up-to-the-second ratings of the specific Web page being accessed. In contrast, pushing updates at intervals is more likely to result in missing a relevant web site. Frequent pushes use more bandwidth for thousands of sub-optimal refreshes per month, most of which are pages users in your organization will not see on a given day. Conversely, pulling ratings for sites categorized since the previous night's update focuses bandwidth only on relevant sites and uses much less total bandwidth each day. Blue Coat WebFilter includes as a standard feature On-Demand Rating Updates, which means if a user encounters a new Web page that was rated since the previous night's update, Blue Coat WebFilter pulls the rating immediately (typically in about 70 milliseconds), and enforces your policy the first time the user encounters the site.

- **Categorize new or unrated Web sites on the fly**

Tens of millions of new pages are created each month, and approximately 30,000 new pornographic pages a day. Web crawlers and data mining are prone to finding irrelevant pages, and such a “boil the ocean” approach finds new pages too slowly. High coverage requires the ability to rate new pages in real time, at the moment a user accesses the page. This is a compliment to the strategy of rating only sites users actually visit (to increase the relevance and performance of the database). Blue Coat WebFilter includes as a standard feature - our Dynamic Real-Time Rating (DRTR™) service; when users encounter a new Web page, DRTR can use extremely accurate artificial intelligence to confidently rate the page (typically in about 200 milliseconds) so that appropriate use and security policy can be enforced the first time the Web page is encountered. DRTR is particularly accurate at rating potentially objectionable sites (rating up to 98% automatically). See further details on DRTR in the “closer look” section below.

- **Include relevant categories from a policy enforcement standpoint**

Early-generation filtering products often inflated their reported coverage rates by creating meaningless catch-all or miscellaneous categories. This also inflated their number of categories, but added no value for policy enforcement. Blue Coat’s design philosophy requires that all categories be highly useful for policy enforcement. Blue Coat offers 61 robust categories. When combined with Blue Coat WebFilter’s ability to have up to four ratings per site (see below), the usefulness of Blue Coat’s categorization is very broad and deep.

For example, a growing number of websites are sources of spyware. Because these sites may have legitimate business content, blocking access to them altogether is impractical. At the same time, in almost all cases, access to “phone home” spyware destination sites should be blocked, in order to protect confidential information. The ideal balance is to prevent the download of any possible spyware installers, but allow users to safely view the HTML content (assuming their other ratings are acceptable), and always block existing spyware “phone home” attempts. Blue Coat has two categories for spyware (sources and effects) so administrators can define different policies to optimize inbound protection (block the downloader without blocking the clean objects on the page) and preventing outbound traffic (Spyware “phoning home”).

- **Recognize and categorize websites in a wide range of languages**

The Internet is a global tool, and used by enterprises and organizations with offices worldwide. Therefore, the ability to categorize web pages and sites across a broad set of languages is critical for web filtering solutions. Blue Coat WebFilter categorizes websites in over fifty languages, for the broadest language coverage.

Classification Accuracy

Accuracy is the ability of a filtering product to precisely and consistently categorize sites. Accuracy answers the question, “Of the 100 websites the filter categorized as ‘X’ (Pornography, Spyware, Gambling, etc.), how many actually were ‘X’?” The higher the percentage, the greater the filter’s accuracy.

To achieve the highest accuracy, a web filtering product must be able to:

- **Accurately categorize the sites users are ultimately attempting to access.**

Users can bypass early generation URL filtering through several widely-known techniques. All of these techniques use an intermediary Web page which pulls content that a user selects from an entirely different kind or category of Web page. Early generation filtering only “sees” (and hence only rates) the intermediary page, rather than the true destination content. Examples include;

- **Translation sites** - online translation from one language to another
- **Archive sites** - which cache selectable content from the past
- **Image searches** - delivered by a search engine
- **Proxy anonymizers** - which relay requests via an intermediary, often obscure site

Early generation filtering technology often only has a superficial rating (e.g., “translation site”, “image search” or “archive site”), but this is not helpful for a policy. Customers do not want to block all image searches, all translation and archive requests. In contrast, Blue Coat is able to see the destination webpage embedded in the intermediary page to make an accurate and useful rating. For example, Blue Coat WebFilter accurately categorizes an archive of penthousemag.com as pornography/adult content, and an archive of cnn.com as news. Blue Coat WebFilter can allow Google Image Search images that meet the local policy (by seeing the source site’s rating) but deny those that do not. This is unique in the industry. When no source information is available, Blue Coat SG’s proxy policy can enforce Google Image “Safe Search” mode at the gateway, even if the user attempts to manually disable it.

- **Place websites in multiple categories, as necessary**

Web pages do not always fit easily into a single category. An example of this is www.covers.com/sportsbetting, which is both a sports/recreation site, as well as a gambling site. An accurate web filter would recognize this and classify the site into both of these categories, as many enterprises will allow (perhaps limited) access to sports sites, but block access to gambling sites altogether. Blue Coat WebFilter can have up to four categories per Web page, which much more accurately reflects the content on Web pages, and allows for thousands of granular sub-category combinations for very flexible and powerful policy enforcement.

- **Categorize subdirectories, as well as top-level domains**

For example, an accurate web filtering product should recognize sites that host home pages for users (e.g., GeoCities), and categorize the actual content on each specific URL. Blue Coat WebFilter can accurately categorize subdirectories to provide flexible and useful filtering.

Performance

- **Process rating requests “on proxy”**

To minimize impact on user productivity, and scale to the needs of large enterprises, a content filtering solution must be efficiently architected to deliver very high performance. Some commodity operating systems are inherently slower at processing rating requests. Common configurations, such as hosting the filtering intelligence in pass-by mode off-box, are inherently slow. Blue Coat WebFilter is optimized to run “on-proxy,” on Blue Coat’s world’s fastest proxy OS and optimized appliances, such that rating requests are processed in RAM, usually an order of magnitude faster than when they are run “off-box.” Blue Coat WebFilter rates 94% of the Web pages a typical corporate or educational user requests on-proxy, in less than 8 milliseconds. Of the other 6% of pages, a rating can be instantly and transparently requested from Blue Coat’s On-Demand Rating Update service (typically in less than 70 ms) or from Blue Coat’s DRTR (typically in about 200 ms, although there are some dependencies on the performance of the site in question). Processing rating requests on-proxy is the fastest possible architecture for high performance and scalability.

- **Include IP ratings locally**

Some early generation filtering systems attempt to provide ratings for the IP version of URLs in the database by performing a reverse-DNS lookup whenever just the IP is requested. However, this adds considerable latency to processing the rating request. Frequently, requests are handled so slowly an error message is returned instead of a rating. Such short-cuts only benefit the filtering vendor, not the user. Blue Coat WebFilter has specific ratings for millions of the most common IP addresses to ensure secure control and reliable, high-performance ratings.

DYNAMIC RATING –A CLOSER LOOK

Blue Coat offers three complementary services to provide ratings for new Web pages (or pages not yet rated on the local copy of the WebFilter database). All of these services come standard with every Blue Coat WebFilter subscription.

1. **On-Demand Rating Updates**

Blue Coat’s On-Demand Rating Update service ensures that every rating Blue Coat has produced is available to users transparently, even if it is only seconds old. Blue Coat rates new sites around the clock, and pushes a batch update each night to licensed SG appliances for efficient distribution. If a user encounters a recently rated site prior to the nightly update, the Blue Coat SG appliance can automatically check one of Blue Coat’s distributed datacenters, via the Internet, for a rating. The typical response time is approximately 70 milliseconds, and since this happens automatically, it is seamless to the user.

This architecture is the most precise, efficient and effective means of keeping a content filtering database up to date. Ratings are still applied the first time a user requests access to a webpage – even if was rated just seconds earlier. Since 94% of the sites a typical enterprise user visits will already be rated on the local copy of Blue Coat WebFilter, bandwidth usage is nominal and response times are extremely fast.

2. **Dynamic Real-Time Rating**

When a user encounters a webpage that has never been seen before (about 2 million such pages are created daily), Blue Coat's DRTR technology uses learning machines to categorize the site on the fly and return a rating for immediate enforcement of your acceptable use and security policy. DRTR is particularly tuned to rate objectionable sites, since these are statistically most likely to present security issues and have policy implications.

DRTR queries the actual target Web site and retrieves key pieces of the page's content and context. DRTR parses the webpage into atomic components and in real-time, makes a determination of what category the URL/domain belongs (see Figure 1 for a DRTR graphical overview).

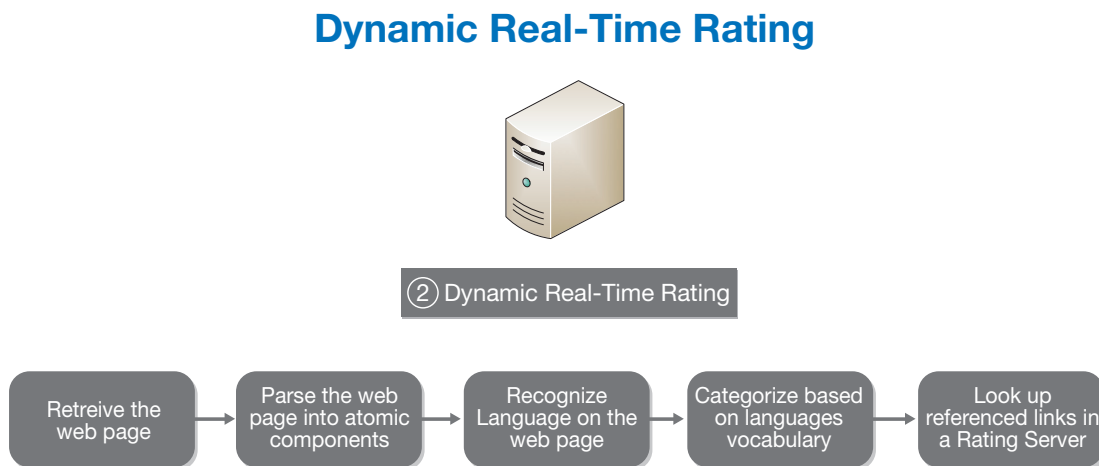


Figure 1: DRTR

One of the items that DRTR looks at is the language used on the webpage. DRTR currently recognizes 40 different languages and is adding new languages on a regular basis. Blue Coat adds new language support through its customers: As Blue Coat's customers request domain ratings for Web sites in these new languages, Blue Coat quickly learns to recognize that language and is able to rate sites in that language (see Figure 4).

DRTR then analyzes each word on a website and assigns a probability rating for each of the 60 categories. For example, the English word "casino," which may appear most frequently in the "gambling" category—receives the highest probability rating—will also have a statistic rating in all of the other 59 categories. This implies that just because "casino" is associated with gambling does not mean that every page containing the word is a gambling page.

The context of a Web site is also crucial to accurately determining its category. Web sites usually contain links to other Web sites. Typically, the linked Web sites have already been categorized and this information can help more definitively rule in or rule out the proper category of the site in question. Health sites tend to link to other health sites, pornography sites tend to link to other pornography sites, and so forth. Context is generally very valuable for rating a site.

Blue Coat DRTR compares all of these component factors to what is known. Blue Coat's learning machines have been trained with tens of thousands of sites that it knows are in certain categories, and tens of thousands of sites that it knows are not in given categories. This allows DRTR to determine both a likely category and a confidence factor that the provisional rating is correct. Blue Coat then makes a quality cut-off decision to determine whether or not to categorize the site based on DRTR's recommendation. This allows Blue Coat to maintain a very low percentage of sites that are miscategorized by DRTR.

As described previously, DRTR is particularly successful at rating potentially objectionable sites. Blue Coat has focused on potentially objectionable categories for DRTR because of the exposure, liability and risk that organizations face when users access such material. For example, presently DRTR accurately rates approximately 98% of new pornography sites on first review. DRTR is continuously being trained and refined to increase its accuracy and confidence in all categories.

Like all aspects of the Blue Coat WebFilter Ecosystem, DRTR is designed with redundancy. All systems are fully load-balanced. For each On Demand Rating Update server, there are multiple DRTR servers available for real-time URL categorization. DRTR servers are true peers with native load-balancing. This redundancy is transparent to the end user—when a URL request is not found in the cache database, there is no noticeable performance degradation.

DRTR is able to provide ratings for many of the sites that are sent to it. In the event the confidence level given a site by DRTR is not high enough to assign the site to a particular category, it will return an “unknown” rating for that page, and Blue Coat implements the next layer of its Web filtering process.

3. Dynamic Background Rating

The patent-pending Blue Coat Dynamic Background Rating (DBR) service is the next layer in the Blue Coat URL ratings hierarchy. There are situations where a URL is not found in the cached database and where DRTR cannot categorize a URL with enough confidence to produce an acceptable rating. When this happens, the URL is logged and forwarded to Blue Coat's centralized processing center. On a regular basis—multiple times each day—DBR runs the list of uncategorized URLs against a series of URL analysis tools (see Figure 2 for a DBR graphical overview). DRTR is extremely accurate at rating Web sites and thus increases WebFilter's overall coverage. DBR's Web site rating classifications are used to update the Internet-based databases frequently and the Blue Coat SG databases each day.

DBR uses a number of proprietary rating techniques or modules to individually rate and categorize a page, in addition to the output from DRTR. Some of these techniques include local link classification, outbound link classification, and same-domain pages (both rated and unrated URLs). Each technique or module is given a categorization vote with an assigned statistical level of confidence. If the combined total votes reach a predetermined level of confidence, that rating is accepted and placed in the database and made available to all Blue Coat Service Points.

Once a URL/domain has been categorized by DRTR and has been run through Blue Coat's DBR service, the URL/domain is placed in the local cached database. On a regular basis, all databases throughout Blue Coat's Service Points are updated and synchronized allowing all users to benefit from the aggregate surfing habits of Blue Coat's global customer base. Blue Coat provides ratings for approximately 50 million requests per day.

Dynamic Background Rating

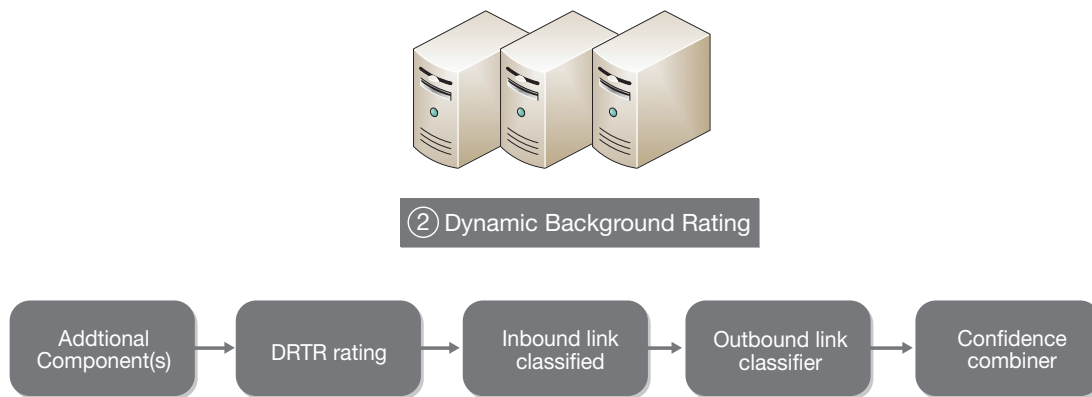


Figure 2: DBR

The key to DBR's ability to correctly categorize web content is in the training data which has been provided to it for each category. Training data is the population of domains and URLs which have been analyzed by Blue Coat's professional staff to be highly indicative of belonging to a specific category. DBR, and more importantly DRTR, has a large population of domains and URLs belonging to a specific category, so new URLs are easier to rate because they have a tried and tested profile to compare against. For example, if the system has classified 50,000 pornography domains, the 50,001st is easy to categorize as pornography.

DBR also includes proprietary tools to proactively seek out and analyze pages for potential security threats. Spyware, phishing, Botnets, and such are sought through similar learning machine training of known threat sites, for rapid inclusion in the Blue Coat WebFilter database.

Human Raters

Human involvement in the rating process provides three purposes to Blue Coat WebFilter: rating sites that cannot be rated by a machine, providing training data to DRTR and DBR, and responding to site submissions. In order for DRTR to rate less-popular sites in real-time, it needs to have high-confidence in the statistical profile for each category. Humans help ensure that the trained data is accurate — that is, that the rated domains truly belong to the stated category. Professional raters also investigate disputed ratings and typically provide replies in less than one business day.

Individual submissions from users

Site submissions can be made by anyone worldwide, either by accessing Blue Coat's webpage or via the link provided on the K9 application. These requests are to rate a site previously unrated or, in rare occasions, when they believe the URL categorization is in error.

When Blue Coat receives one of these site submissions, a human reviewer reviews the site in question in order to make a determination of whether the site is categorized correctly or in error. Blue Coat then sends that end user an email directly stating either the URL was categorized correctly or that it was re-categorized. This helps Blue Coat fine-tune its database and training data, provides the end user some recourse should they need it, and eliminates the need to bother the local administrator with these mundane tasks.

IMPLICATIONS FOR NEW SECURITY OPPORTUNITIES

URL filtering can be very powerful for preventing unknown malicious code from known untrustworthy sites. As discussed above, coverage and accuracy are even more important when employing content filtering for Web security than for simply enforcing appropriate Web browsing. Blue Coat's use of up to 4 categories per Web page and ability to rate based on true destination page (embedded content) dramatically improves accuracy. Blue Coat's unique On-Demand Updates, DRTR and DBR provide the most complete, most up-to-date coverage. This combination helps Blue Coat deliver the strongest filtering security solution available.

However, there are limitations to using even optimized filtering for Web security. Every technology has strengths and weaknesses. Given the high stakes of Web security, these limitations can be significant.

- **Overblocking creates new problems.** For example, hundreds of thousands of sites use commercial spyware (adware) downloads to create revenue. A certain percentage of these sites will have information of business value. Blocking access to the entire page denies users the business value of these sites (or possible legitimate personal use), and tends to generate new help desk tickets.
- **Filtering technology has difficulty dealing with previously-rated sites that later become threat sites.** Given the financial incentives behind spyware, this is statistically significant. It is not possible to re-rate 16 billion Web pages daily or hourly to keep up with this dynamic challenge.
- **Rating technology has limits in its ability to recognize threat sites.** Threats evolve rapidly. Hackers and unethical entrepreneurs continuously seek to circumvent security technology, and that makes it harder to recognize and accurately rate threats on an ongoing basis.

Blue Coat addresses these inherent limitations in using filtering for security by leveraging the attributes of Blue Coat's unique proxy appliances. Blue Coat's policy engine has more than 500 trigger-action combinations enabling the most granular and powerful proxy policy. By combining information from Blue Coat WebFilter with optimized proxy policy, Blue Coat synergistically delivers a much stronger level of Web security than any competing technology.

Spyware

Blue Coat SG appliances prevent new and unknown spyware at the gateway more effectively than any other offering. Case studies of Blue Coat users consistently show that Blue Coat simply stops spyware related help desk tickets.

(See http://www.bluecoat.com/downloads/datasheets/CaseStudy_Mustang.pdf
http://www.bluecoat.com/downloads/datasheets/CaseStudy_DenverHealth.pdf

http://www.bluecoat.com/downloads/datasheets/CaseStudy_StateofDE.pdf as examples). Given the inherently evasive nature of spyware, this is the most revealing metric of a security solution's effectiveness.

Blue Coat prevents known and unknown spyware via any or all of the following techniques.

- Blocks all unauthorized (non-white-listed) drive-by downloaders regardless of whether their source URL is known or rated. Drive-by downloaders are the most dangerous and common vector for spyware installs.
- Block many common exploits (Windows, IE, etc.) used to install spyware and Botnet Trojans, independently of their source URL.
- Block downloads with spoofed file extensions (e.g., declares itself a JPEG but is actually an EXE), regardless of source.
- Strip all executable downloads from sites in Blue Coat WebFilter's "Spyware Sources" category (tens of thousands of known spyware sites). This blocks all potential spyware, but allows page views (pending what other category the Web page is in) to maximize business value of the Web.
- Strip all potential spyware downloads from sites at high risk of becoming spyware sites. Blue Coat statistical analysis found most known spyware emanates from 15 high-risk categories. Also preserves page views to maximize business value of Web.
- Optionally, heuristic virus and Trojan scanning (by Blue Coat AV appliances) of remaining downloads. This additional layer of defense can prevent known and unknown spyware Trojans and rootkits from getting to PCs regardless of their source.
- Detects previously installed spyware attempting to "phone home" to "Spyware Effects" sites, blocks the communication and alerts the administrator which desktops need cleansing.
- Apply all of the above to fully proxied HTTPS/SSL traffic.

Importantly, Blue Coat's solution installs at the network gateway, and has proven high performance, so deployment costs are minimal, and business is not impeded.

Phishing

Phishing introduces other unique challenges. By its very nature, phishing is a sneak attack. The phisher creates a counterfeit Web page, sends the bait email to tens or hundreds of thousands of email addresses, and within moments begins harvesting users' or corporations' financial credentials. Attempting to rate phishing pages reactively is extremely challenging and reliance upon human raters is simply too slow.

Blue Coat prevents known and unknown phishing via the following techniques.

- Block known phishing sites (to protect users who are slow to open the bait email). On-Demand Updating transparently ensures users have fastest access to these new ratings.
- Prevent users from posting (entering data) to sites at high risk of being phishing sites. Risk criteria include fraudulent or expired SSL certificates, deceptive characters in URL (e.g, an Ö in WWW.WELLSFARGÖ.COM) etc.

- Coach users in context via pop-up alerts to minimize vulnerability. For example, if a user is being asked to post to an uncategorized site, they can be warned that this is probably not a well-known financial institution and inputting personal information is risky.
- Block or warn users of sites that have an invalid SSL certificate.

IM Control

Many organizations want to allow reasonable use of IM technology but are concerned about introducing possible security issues. They may also have regulatory compliance concerns about tracking and logging IM communications. Traditional URL filtering lacks logging, can partially harass some IM technology and is powerless to inhibit others. Blue Coat provides the following capabilities.

- Monitor and log session content by proxying the leading IM protocols (AOL, Yahoo!, MSN), to meet regulatory compliance.
- Monitor and block key words and sensitive information from being transmitted via IM
- Deny IM attachments to prevent loss of proprietary information, and prevent potential virus transmissions
- Block all other IM clients

P2P Control

Many P2P technologies are bandwidth intensive, introduce security vulnerabilities, or simply do not adhere to acceptable use policy. Blue Coat allows administrators to throttle or simply block P2P communications across the network gateway. Skype is an especially interesting case. Skype uses a proprietary, encrypted protocol and is port agile, making Skype very difficult to see on the network, let alone control. Skype includes video and file attachments, so it's potential for abuse is considerable. Blue Coat can selectively allow some users to use Skype and disallow others by locking down ports and then allowing only legitimate SSL traffic on port 443. Blue Coat's ability to proxy HTTPS makes this very secure approach possible.

Bot Networks

Hackers surreptitiously hijack control of PCs to amass distributed armies of robot (also known as "zombie" or "Bot") PCs to perpetrate crimes on the Internet. While a properly configured firewall gives most organizations the greatest degree of protection, Blue Coat provides the following additional layers of protection.

- Block downloads from sites in malware category
- Block common exploits and vulnerabilities via policy to prevent new and unknown Bot hacks.
- Optional Blue Coat AV heuristically detects and blocks Bot Trojans regardless of source.

Streaming Control

While streaming is seldom seen as a security threat, in aggregate, uncontrolled streaming can "take down" a network. Popular sporting events, such as U.S. college basketball playoffs and the FIFA World Cup are common instigators. However, the Web is becoming more media rich all the time. Podcasts are showing up in 50 different categories of Web sites. Even appropriate business content can hobble a network. Blue Coat provides the following application-aware bandwidth management capabilities:

- Block or throttle bandwidth usage based on protocol, category, user, group, time of day, etc. Movie trailers may be denied, business news streaming limited to 128 Kbps, internal e-learning accelerated, and the CEO allowed to do whatever she chooses.
- Cap bandwidth usage by protocol, category, user, group, time of day, etc. During core business hours, streaming might be limited to no more than 20% of available bandwidth.
- Stream splitting and multi-casting allow a single stream from the Internet to be split in real-time to multiple internal viewers, dramatically reducing bandwidth usage.
- Proxy caching eliminates redundant downloads, dramatically reducing latency and bandwidth usage.

CONCLUSION

The nature of Web traffic and browsing habits has evolved far beyond early-generation URL filtering architectures. Enforcing appropriate use policy and providing robust Web content security requires a truly dynamic filtering solution. Blue Coat WebFilter uses a combination of leading edge, dynamic techniques in its architecture and ecosystem to provide the most accurate, highest coverage and most effective content filtering available.

In conjunction with the powerful proxy policy control of Blue Coat SG appliances, WebFilter successfully mitigates a variety of content security threats. Case studies show that Blue Coat can eliminate the most difficult problems, such as spyware, by the most exacting metrics, such as eliminating related help desk tickets. With more than 500 trigger-action combinations, Blue Coat's policy engine provides the flexibility and power needed to deal with new and emerging threats as well. All of this is delivered on a proxy caching platform that substantially accelerates "good" Internet traffic. Further, IT receives the visibility and control necessary to keep up with future challenges and opportunities.



420 North Mary Ave.
Sunnyvale, CA 94085
www.bluecoat.com

1.866.30.BCOAT
408.220.2200 Direct
408.220.2250 Fax

Copyright ©2006 Blue Coat Systems, Inc. All rights reserved worldwide. No part of this document may be reproduced by any means nor translated to any electronic medium without the written consent of Blue Coat Systems, Inc. Specifications are subject to change without notice. Information contained in this document is believed to be accurate and reliable, however, Blue Coat Systems, Inc. assumes no responsibility for its use. Blue Coat is a registered trademark of Blue Coat Systems, Inc. in the U.S. and worldwide. All other trademarks mentioned in this document are the property of their respective owners. Version 1.0

Blue Coat secures Web communications and accelerates business applications across the distributed enterprise. Blue Coat's family of appliances and client-based solutions – deployed in branch offices, Internet gateways, end points, and data centers – provide intelligent points of policy-based control enabling IT organizations to optimize security and accelerate performance for all users and applications. Blue Coat is headquartered in Sunnyvale, California, and can be reached at 408.220.2200 or www.bluecoat.com.