



How to Control Web Applications and Content

The nature of the network has changed. Applications and content are moving to the Web, making the Internet a vital component of enterprise infrastructure. This poses two challenges: how to manage application performance on a global network where no one is in charge, and how to distinguish valuable content from recreational or malicious content when all Web traffic looks the same. With the integration of WebPulse™, Blue Coat's real-time URL categorization service, Blue Coat PacketShaper is the only solution that controls today's Web-heavy network traffic by the applications that generate it and by the Web-based content it may contain. This allows network managers to speed the applications and content categories they prefer while suppressing undesirable applications and content.

The Goal

The goal of any network is to reliably deliver the applications and content that its administrators deem important. This is easy to say, but increasingly difficult to achieve. As more applications and content move to the Web, network managers need tools to ensure the performance of Web-based applications that they value, such as salesforce.com and WebEx. At the same time, the impact of permissible but less important traffic, such as streaming radio and sports, must never compromise more important traffic. Furthermore, undesirable applications such as malware and P2P, and Web content that presents legal risks or violates an organization's policies, should never be allowed to proliferate unchecked. And if that doesn't sound difficult enough, remember that tens of thousands of new Web pages are created and modified every hour, requiring real-time awareness rather than after-the-fact updates.

The Challenge

With Application Performance Management solutions like Blue Coat PacketShaper, network managers can assign bandwidth and priority on an application-by-application basis. In this way, it's simple to guarantee the performance of important applications, even during periods of network contention. The same should be true for Web content: with the migration of business-related applications and content to the Web, we know that people use the Web for both recreational and productive purposes. But with billions of Web pages online and more added every day, how can you make sure that your network knows the difference between good content and bad?

One approach to managing Web content is to add a security solution such as Blue Coat ProxySG, which you can use to set policies that allow, warn, or deny. This is the best way to block undesirable content categories like Violence/Hate or Illegal Drugs from your network, but what about categories like Entertainment, Social Networking, and News? There are legitimate reasons to allow access to this sort of content, but how do you contain its impact on bandwidth use and productivity? Consider the US Air Force. In September 2010, the Department of Defense ordered bases to permit access to social networking sites like Facebook, acknowledging that "Internet-based capabilities are integral to operations across the Department of Defense" (Directive-Type Memorandum 09-026). While not stating it formally like the military directive, organizations around the world have come to the conclusion that social networking should be allowed on their networks. Marketing uses social networking to reach customers; HR to research candidates; employees to keep connected with colleagues and families. The result: a substantial increase in Web traffic at networks around the world.

While many organizations permit access to social networking sites, most would rather not tempt their employees to spend hours playing Facebook games. What's needed is a method that permits reasonable access while containing the impact of bandwidth-heavy content like streaming media and Facebook games. Now that applications and content have merged on the Web, you need a traffic management solution that considers both.



Blue Coat Solution

Identifying and Measuring Web Traffic by Content Category

Blue Coat's latest innovation is the integration of the Web content awareness of WebPulse with the granular control capabilities of PacketShaper. Making its debut in Blue Coat PacketShaper 8.6 software, the Classify by URL Category feature sub-classifies Web traffic based on its content category. Every time a URL request passes through the PacketShaper, local cache is checked to see if that URL has already been categorized. If so, it classifies the Web traffic based on its content category and applies any configured policy. If the URL is new – for example, the next trendy Facebook game or coverage of breaking news – the PacketShaper queries the WebPulse service, leveraging its 70 million users who generate over 8 billion ratings per day. WebPulse responds with the content category (typically in less than a second), and PacketShaper controls the Web traffic accordingly.

Protecting Preferred Content

Since PacketShaper knows the content categories of Web traffic, you can configure PacketShaper to give preferential treatment to categories of traffic. Preferred categories might include content related to work, such as Online Meetings and Software Downloads, or content for which response time can be important, such as Auctions and Financial Services.

The screenshot shows the configuration for 'Online Meetings' (All Internet Protocol traffic). The 'Policy Type' is set to 'Priority'. The 'Priority' dropdown is open, showing options: 5 (High), 3 (Normal), 4, 5 (High) (selected), 6, and 7 (Highest). The 'DSCP' field is set to 4, and the 'Partition' is set to 6. There is an 'Assign Name' button and a 'Burstable Max' checkbox. 'Apply' and 'Revert' buttons are at the bottom.

Containing Permissible Content

Many categories of Web content are neither good nor bad: instead, they should be managed based on their impact on other network traffic and on behavioral factors such as productivity. Streaming media is a good example. While many organizations use streaming media sites for work-related purposes like product demonstrations and training, there's no question that most of this traffic

is generated by individuals sharing links to entertaining videos, or listening to music streams while at work. To contain the impact of streaming media, you can apply a policy that restricts it to a specified amount of bandwidth or to a percentage of the WAN link.

The screenshot shows the configuration for 'Video-Streams' (All Internet Protocol traffic). The 'Policy Type' is set to 'Rate'. The 'Guaranteed' field is set to 100k bps. The 'Burstable' checkbox is checked. The 'Priority' dropdown is set to 1 (Low), and the 'Limit' field is set to 500k bps.

Because PacketShaper gets Web content categories from WebPulse in real time, new Web content is managed by your existing policies. There's no need to make emergency plans for events like the Olympics or in response to breaking news; PacketShaper and WebPulse effectively manage tomorrow's Web content based on the Web category policies you have in place today.

Suppressing Undesirable Content

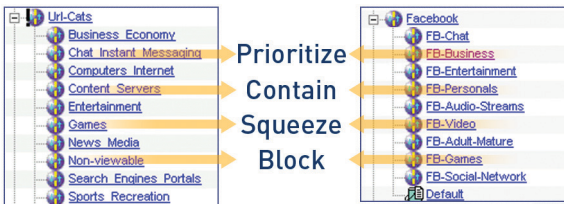
Unfortunately, the Web contains content that may be unsuitable for the workplace, such as gambling and pornography, or that poses threats with legal and financial consequences, such as spyware and phishing. PacketShaper is especially effective as a tool to audit existing security solutions. If your security appliance is configured to block content related to illegal drugs, and PacketShaper also detects and blocks this content category, you know that your current systems haven't kept up with cloud-based services such as WebPulse. You can configure PacketShaper to block undesirable content categories, but remember: since PacketShaper continues to pass traffic while determining its content, some forbidden traffic can still get through. Nevertheless, this is an effective method to suppress undesirable content and discourage users from attempting to access it.

In the case of Phishing threats, however, one request may be all that's needed to redirect a user to a malicious site. The only way to guarantee complete security is to add ProxySG, which checks all Web content for allowable categories before allowing it on the network. Because both PacketShaper and ProxySG use WebPulse to categorize URLs, you can use the two together; configure ProxySG to completely block undesirable content, and PacketShaper to control the performance and impact of allowed categories.



Managing Mixed Content

But what about sites like Facebook, where content such as status updates may be permissible but other content, such as games, should be contained? Unlike simpler URL filters that ascribe only one category to a Web page, WebPulse returns up to four categories for each URL. For example, a request for Farmville, a popular Facebook game, returns two categories: Social Networking and Games. You can configure PacketShaper to allow Social Networking traffic without restrictions, but squeeze Games to a 10kbps trickle. This sends a subtle message to users about playing games at work, without triggering complaints that “the Internet is down.”



Summary

Web traffic is diverse, and can't be effectively managed without considering both applications and content. PacketShaper leverages the real-time WebPulse service to classify the tens of millions of Websites and billions of URLs into 80 logical categories. This means that you can manage similar content collectively, rather than app-by-app or site-by-site. With PacketShaper's real-time content awareness, policies created today will apply to similar content created tomorrow, with no downloads or updates required. This makes PacketShaper an ideal tool for controlling the performance of Web-based applications and content.

About Blue Coat

Blue Coat is the technology leader in Application Delivery Networking (ADN). The ADN infrastructure provides the visibility, acceleration and security capabilities required to optimize and secure the flow of information to any user, on any network, anywhere. This application intelligence enables enterprises to tightly align network investments with business requirements, speed decision-making and secure business applications for long-term competitive advantage. To learn more, please visit us at www.bluecoat.com.