



Intelligent Control with an Application Delivery Network >

BlueCoat ProxySG and PacketShaper Work Together For Secure and Reliable
Application Delivery Across the Enterprise WAN



Executive Summary

Enterprise IT organizations struggle to deliver applications quickly and securely across corporate networks, the Web and wireless connections. Users expect exceptional application performance and security no matter where they work, but IT often lacks high-level intelligence about business priorities, security policies and user identities to enable a headquarters work experience anywhere. Application performance and security tend to remain haphazard and unsatisfactory, especially across a distributed enterprise.

To manage these challenges now and in the future, enterprises need a new layer of intelligence and control in the network. This new layer – the Application Delivery Network (ADN) – combines real-time intelligence about users, applications, business rules, network status and security policies to deliver applications quickly and securely across the WAN and Internet.

Enterprises can create an Application Delivery Network by deploying two industry-leading network appliances: Blue Coat® PacketShaper® and ProxySG®, at the headquarters and in branch offices. PacketShaper provides comprehensive visibility into applications and granular controls for optimizing application performance. ProxySG, a WAN optimization and Secure Web gateway solution, provides state-of-the-art acceleration controls with essential branch office security. ProxySG is the only WAN optimization product that can make full use of PacketShaper's many network analysis and control capabilities in accelerating and securing applications.

Together, ProxySG and PacketShaper offer enterprises an immediate solution to implement an Application Delivery Network to meet the growing challenges for delivering applications faster and more securely across the distributed enterprise.

Introduction: Application Delivery Challenges on Today's WANs

Business is increasingly automated and Web-based, making network connectivity and application performance more important than ever before. But connectivity and high performance aren't the only challenges facing enterprise WANs. Business and logistical demands are forcing enterprise IT organizations to create exceptionally reliable, flexible and scalable networks.



Today's business networks are vast and diverse. They reach into customer and partner domains, span wired and wireless segments and increasingly encompass applications and storage networks. With this vast span of connections, specific applications might be provisioned for years of service, while others, focused on serving a tactical operation or team, might be put in place for only the length of a specific project. Application security and optimization must adapt to either scenario. Meanwhile, mobile computing has become the norm. Workers expect satisfactory application performance at any location – at headquarters or a branch office, at home or at a remote public site, such as a Wi-Fi hot spot.

While partners and customers are reaching into the network, key applications that were previously deployed inside the network perimeter are being replaced by software-as-a-service (SaaS) applications, such as Salesforce.com, WebEx and Workday, which are hosted and managed by third-party providers. Enterprises are switching to SaaS to benefit from rapid deployments, near-instant scalability and lower capital and operational expenses. A 2008 study of the SaaS market by the Sand Hill Group and McKinsey & Company found that SaaS applications already account for 11% of software budgets in large organizations, and will play an even larger role in enterprise IT in the coming years.¹

At the same time that network connectivity is reaching farther and application models are becoming more diverse, security threats are becoming more sophisticated and harmful. Hackers have discovered ways to inject malware into the Web pages of these sites, including major news portals and e-commerce sites, infecting users who visit. Meanwhile, data leakage remains a serious problem. Hackers routinely break into systems to steal confidential data, and employees continue to compromise confidential data and intellectual capital, either accidentally or with malicious intent.

Because branch office workers are increasingly turning to SaaS applications and other Web resources for their everyday work, it's tempting to offer branch offices direct access to the Internet. The line costs for direct Internet access are usually cheaper than the line costs for WAN connections, so a direct-to-net model for branch offices promises both cost savings and faster Internet access. However, for a direct-to-net model to be safe, Web filtering and security controls must be available at the branch, but today, most enterprises are centralizing these functions at the network core.

¹ "Enterprise Software Customer Survey 2008," Sand Hill Group and McKinsey & Company. In the survey of 857 IT executives, SaaS was rated more important than any other trend in IT, including Web services/SOA and off shoring.



Limitations of Functional Silos and the Connectivity Layer

To deliver applications quickly and reliably while protecting enterprise networks and data, IT organizations have relied on a variety of piecemeal approaches, each focused at a particular area of technology, such as network layer optimization or virus detection. This piecemeal approach has produced only middling results. Security breaches still occur, and users complain that they are not getting the application performance they need.

The limitation with this piecemeal approach is the heavy reliance on the capabilities of the connectivity layer – the lower layers in the OSI networking stack that constitute the basic infrastructure for connecting devices to one another. The connectivity layer knows a lot about devices and traffic routes, but little about users and applications. It cannot distinguish an employee from a visitor, a business application from a game or a safe Web site from a dangerous one. Blind to business priorities, user identities and usage patterns, the connectivity layer is simply an untenable option for implementing application acceleration and control.

The Blue Coat Solution: Enabling the Application Delivery Network

To provide comprehensive and reliable intelligence over applications across the WAN, enterprises need a new layer of visibility and control – one that works above the connectivity layer, and applies real-time intelligence about users, applications and network status to the job of accelerating and securing applications across all network locations, including headquarters, branch offices and remote sites such as Wi-Fi hotspots. Blue Coat defines this higher layer of control as the Application Delivery Network (ADN).

Drawing on real-time knowledge of applications and network activity, the ADN performs three essential functions:

- > **Application Performance Monitoring:** Identify and protect all types of applications running over any network segment in the WAN
- > **WAN Optimization:** Combine protocol optimization, caching and compression to dramatically accelerate application performance
- > **Secure Web Gateway:** Filter inbound and outbound traffic to block malware and access to dangerous sites, while ensuring that all network traffic complies with an organization's security policies

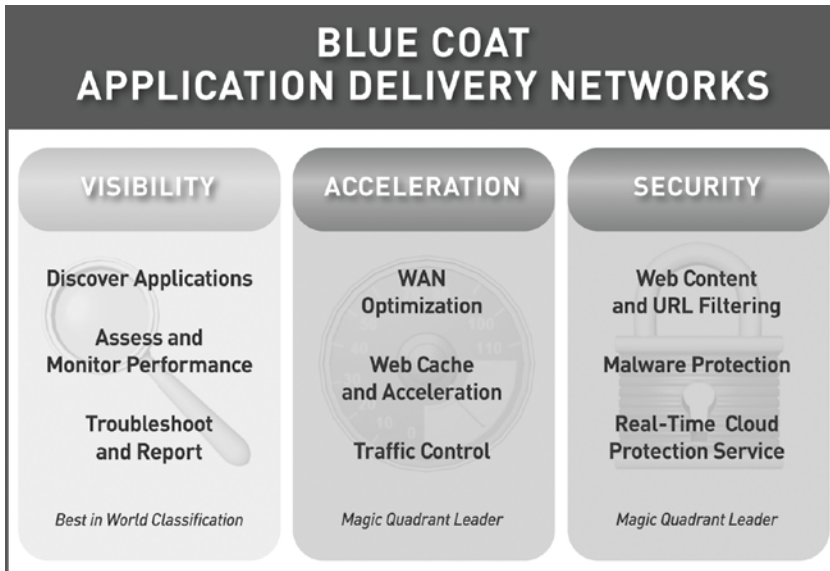


Figure 1: The Application Delivery Network (ADN) applies knowledge of users and applications to solve the problem of application performance and security.

Blue Coat appliance and software solutions intelligently secure and accelerate application delivery to all users connected over private WANs or the Internet. Whether an application is hosted internally or externally, Blue Coat can accelerate its performance up to 100 times, while protecting the application’s users from malware such as viruses and worms. Blue Coat also provides granular policy-based controls and enhances IT control over all distributed users – even those with unmanaged endpoint devices.

In June 2008, Blue Coat acquired Packeteer to combine the strengths of PacketShaper with ProxySG, creating a highly scalable solution for implementing Application Delivery Networks. The dual integrated solution of ProxySG and PacketShaper enables enterprises to see, secure, accelerate and control applications across their entire network, enabling IT to use in-depth network intelligence to deliver an exceptional user experience and help achieve business goals.

Blue Coat PacketShaper

Blue Coat PacketShaper is a best-of-breed, intelligent network appliance that classifies, monitors and controls network applications. PacketShaper offers granular visibility into your network traffic and applications, so you can quickly



identify and resolve application problems with more accuracy than any other network optimization solution on the market.

To accelerate or control application performance, you first need to identify what's on your network so you can prioritize traffic and enforce security policies. Products whose application analysis consists primarily of making inferences from port numbers are at a significant disadvantage compared to an application delivery solution featuring PacketShaper's precise, application signature-based classification technology.

PacketShaper performs other valuable services that give IT insight into network and application utilization and performance. It validates common protocols and monitors the state of every connection established by every application. It breaks traffic down by application and by site, reporting peak and average utilization rates, bytes transmitted, availability, utilization, top talkers/listeners, network efficiency and much more. It reports not just network-level metrics, but also application-level metrics, such as application response times (useful for monitoring applications like SAP), VoIP metrics (including MOS and R-Factor), and jitter, latency and loss for all VoIP and video applications.

In summary, PacketShaper enables enterprise IT organizations to:

- > Automatically analyze 650+ applications with Layer 7 Plus² network visibility.
- > Shape traffic in real-time with flexible policy-based quality-of-service (QoS) control.
- > Monitor end-to-end user application performance using 100+ metrics per network flow.
- > Accelerate and compress applications for maximum performance.
- > Deploy and control multiple units with centralized management and reporting.

Blue Coat ProxySG

Blue Coat ProxySG is a network appliance that serves both as a WAN optimization solution and as a Secure Web gateway.

As a WAN optimization solution, ProxySG applies byte and object caching, protocol optimization, compression, SSL acceleration and other techniques to dramatically accelerate application performance. For example, ProxySG can eliminate many back-and-forth communications that slow the performance of CIFS-based file access over the network. As a result, users in branch offices can access centrally stored files as quickly as files stored on the local LAN.

² PacketShaper's Layer 7 Plus technology uses specialized search algorithms to gain a more precise reading of application classification. The technology also uses historical and behavioral information to differentiate between business-critical traffic and some recreational applications, and supports the use of plug-ins to further customize application analysis.



Figure 2 summarizes the speedups that ProxySG achieves for common services and applications.

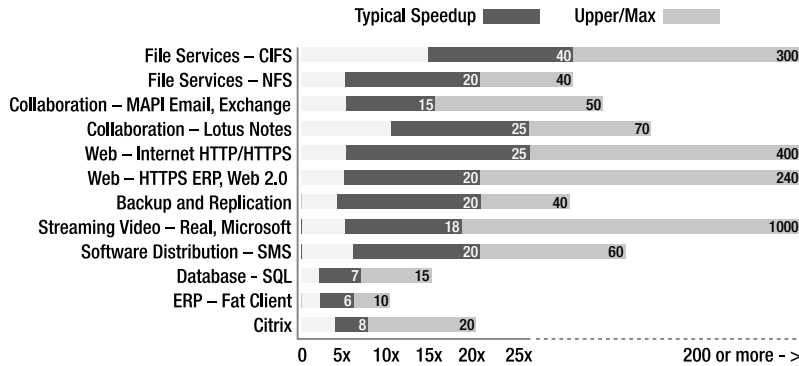


Figure 2: ProxySG dramatically accelerates common services and applications and on the WAN.

ProxySG also works as a Secure Web gateway. In this role, ProxySG performs a broad range of network security operations, including URL filtering, malicious-code detection and application controls for popular Web-based applications, such as instant messaging (IM) and Skype. ProxySG filters traffic in real time, ensuring that devices accessing public Web sites do not become infected. ProxySG also enforces company security and acceptable use policies, such as preventing users from accessing inappropriate Web content using company equipment.³

ProxySG gateway addresses these network needs:

- > **Performance** – Blue Coat’s patented acceleration technology optimizes application performance and helps IT ensure delivery of business-critical applications. Through an optimal use of application-level performance optimization, caching and parallelization, ProxySG improves the user experience no matter where the application is located, internally or externally on the Internet.
- > **Security** – The Blue Coat ProxySG security architecture addresses a wide range of requirements for network and data security, including filtering Web requests and content, preventing malware and other malicious mobile code, validating content and certificates, data leak prevention, inspecting encrypted SSL traffic and controlling IM, P2P and streaming traffic.
- > **Control** – Blue Coat’s patented Policy Processing Engine empowers IT to make intelligent decisions about network security, application delivery and data access. Using a wide range of attributes such as user, application, location, destination, content and others, organizations can effectively align security and performance policies with corporate priorities.

Both Gartner and Forrester recognize ProxySG as an industry-leading product for both Secure Web gateway and WAN optimization objectives.⁴

³ For more information about the characteristics of Secure Web gateways, see Gartner’s report, “Magic Quadrant for Secure Web Gateway, 2007,” GAS Core Research Note G00148895.

⁴ For example, see Gartner’s report, “Magic Quadrant for Secure Web Gateway, 2007,” cited earlier.

Deploying ProxySG and PacketShaper to Create an Application Delivery Network

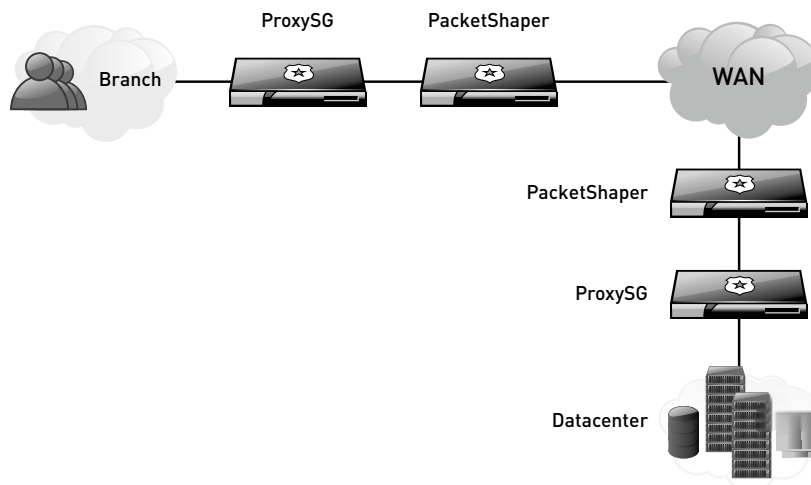


Figure 3: A Blue Coat solution comprising ProxySG and PacketShaper achieves the benefits of an Application Delivery Network.

Figure 3 shows how to deploy Blue Coat solutions to achieve the performance and control benefits of an Application Delivery Network. PacketShaper and ProxySG appliances are installed inline at the core and branch office sites, with the ProxySG deployed on the LAN side of the PacketShaper. The flow of outbound client-server WAN traffic passes first through ProxySG for acceleration, filtering and Web controls, then through PacketShaper for classification and QoS control and finally out to the WAN or Internet.

PacketShaper automatically detects and classifies inbound and outbound WAN traffic (which has either been optimized or bypassed by ProxySG). PacketShaper can then report the actual (optimized) volumes of traffic going across the WAN. In addition, with the ProxySG plug-in for PacketShaper available from Blue Coat, PacketShaper can discover, monitor and control network traffic from the ProxySG with granular sub-classification for each optimized protocol.

By deploying PacketShaper with ProxySG, enterprises can benefit from the sophisticated application analysis of PacketShaper, combined with the extensive security and performance capabilities of ProxySG. The two solutions complement and reinforce each other. PacketShaper is unparalleled at providing detailed traffic flow and user information by automatically identifying applications without port definition rules, thereby strengthening ProxySG's ability to secure and optimize traffic.



For example, working together, PacketShaper and ProxySG can ensure that an Oracle application receives priority over YouTube traffic. They can restrict YouTube traffic to certain hours of the day. ProxySG can also un-encrypt SSL traffic so specific protocol optimizations, such as optimizations for MAPI and HTTP can be applied to dramatically improve application performance.

PacketShaper and ProxySG: A Unique Partnership

This strategic use of PacketShaper is unique to Blue Coat. Combining PacketShaper with any other WAN optimization products sacrifices either PacketShaper's application performance monitoring or its QoS controls. If another WAN optimization product is configured inline before PacketShaper and the WAN, then PacketShaper's Layer 7 classification and monitoring will be unable to apply its signature-matching algorithms to native application traffic that has already been modified by the other device for optimization. If the PacketShaper appliance is configured inline before the WAN optimization product and WAN, it will be unable to control the application traffic it classifies, since the classified traffic that leaves PacketShaper must pass through the other device and then to the WAN. In this scenario, the PacketShaper appliance will not even be able to set the link size, because the appliance will have no idea how much optimization is taking place.

Blue Coat ProxySG is the only WAN optimization product that can operate jointly with PacketShaper in a way that enables both products to make full use of all their capabilities. The in-path placement of PacketShaper and the out-of-path placement of ProxySG ensure that all traffic flows are:

- > Analyzed, marked and controlled by PacketShaper
- > Fully optimized by ProxySG, which filters content, stops malware, accelerates applications and enforces security and usage policies

As the last device before the WAN, PacketShaper provides ultimate control over applications through QoS controls on marked traffic flows of optimized traffic.

In the Blue Coat solution, PacketShaper and ProxySG work together to accelerate and control applications across the WAN to create an Application Delivery Network.



Blue Coat Solutions for Application Delivery Networks

PacketShaper	ProxySG
Application Performance Monitoring	Malware Prevention
P2P Traffic Shaping	SSL Visibility and Control
Application Visibility	Web Content Filtering
MPLS Migration	Content Delivery Networks
Bandwidth Management	Application Acceleration
VoIP Optimization	Server Consolidation

Table 1: Summary of PacketShaper and ProxySG functions in the Application Delivery Network.

How Blue Coat Achieves an Application Delivery Network

Blue Coat solutions are essential to helping organizations establish an Application Delivery Network through comprehensive network security and application monitoring and performance capabilities.

Comprehensive Visibility into Application Traffic

The Blue Coat solution automatically identifies over 650 applications, including CIFS, MAPI and DOM, as well as complex applications such as SAP, Oracle and Citrix. It also identifies evasive P2P applications and recreational applications that can be configured to stream over different ports. This visibility is an essential foundation for effective network optimization and security and policy enforcement.

The visibility provided by the Blue Coat solution extends beyond application classification; it also enables IT to identify URLs and external sites within HTTP traffic. Legitimate sites can be distinguished from ones known to be dangerous, and traffic to recreational sites can be detected and assigned a lower priority than traffic to work-related sites.

Beyond applications and URLs, the Blue Coat solution offers visibility into application performance and the experience of end users, measuring end-user transaction times and issuing alarms when times exceed thresholds for acceptable performance. Blue Coat also measures MOS scores for both voice and video applications, so low-latency media applications can be monitored along with more traditional business applications. Blue Coat then monitors SLA metrics for applications and network links, tracking metrics such as utilization, delay, availability, jitter and loss, providing comprehensive application analysis for up to 100 statistics per application.



Pulling all this data together for engineers and managers, Blue Coat generates reports that can be integrated in an enterprise's existing performance monitoring infrastructure, such as network trace analyzer tools. IT engineers gain additional network visibility through the integrated reporting available from ProxySG and PacketShaper. Using these reports, engineers can monitor both pre- and post-optimization statistics (data reduction and response time improvements) for all applications and traffic types. No other WAN solution available today offers such comprehensive reporting.

Blue Coat's visibility and reporting capabilities help IT engineers troubleshoot performance problems, such as delays among servers, hosts and networks. Using Blue Coat solutions, administrators can isolate the source of delays between servers and networks, track connection states and identify problems affecting servers, networks and applications. They can also capture targeted packet streams for analysis with Sniffer.

Acceleration and Control of All Applications

Blue Coat enables enterprises to accelerate and control all types of applications, including desktop ,CRM, ERP, SaaS and VoIP.

Blue Coat achieves dramatic results in application acceleration through a combination of byte and object caching, protocol acceleration, compression, QoS controls and SSL acceleration. Typical results include:

- > Accelerating internal applications by 15-40X
- > Accelerating external applications, including SaaS applications and multi-media applications, by 5-25X
- > Reducing up to 60% of jitter and latency in real-time applications, such as voice and video

Real-time applications like VoIP benefit from Blue Coat's use of sub-application classification and application session QoS (ASQ).

Security for Applications and Business-Critical IT Resources

Blue Coat provides essential security controls for enterprise WANs by filtering incoming and outgoing Web, IM and P2P traffic in real time, detecting and blocking malware and integrating with any industry-leading AV solutions an enterprise already has in place.



By filtering Web content, Blue Coat dramatically reduces users' exposure to malware. Filtering also promotes employee productivity. Depending on company policies, traffic to recreational Web sites can be blocked or assigned a lower network priority. Enterprises can ensure that the content of Web postings, IM traffic and other online communications complies with HR and regulatory policies.

Blue Coat enforces identity-based access policies, preventing unauthorized access to networks and IT assets. To enforce authentication controls, Blue Coat supports any of 11 different authentication protocols such as Active Directory, RADIUS, TACACS and more. By providing capabilities to integrate with industry-leading data leak prevention (DLP) products, Blue Coat prevents the illicit transmission of confidential information and intellectual capital.

Blue Coat enforces security controls at branch offices, freeing enterprises to adopt direct-to-net architectures wherever feasible. As a result, branch office workers can access the Internet knowing that their activity is secure and compliant with all relevant policies and regulations.

Rapid Deployment

Deployment of the Blue Coat solution is quick and easy. Both the ProxySG and PacketShaper can be installed and configured within a few hours. Enterprises can begin benefitting from improved application performance and enhanced security right away.

Adherence to Best Practices for Managing Branch Office Traffic

Centralization is a major initiative for most IT organizations. Not surprisingly, when IT organizations implement a new infrastructure for network security and performance optimization, they tend to start at the center and work their way out to remote sites. They begin by tightening controls and improving visibility in core data centers. Then they assess the needs of branch offices, considering how to build out branch office networks to complement and extend the controls and optimizations put in place at the core. A fully realized network solution provides control and optimization both at the core and in branch offices, offering improved performance, cost savings and flexibility across the WAN.



As shown in the table below, best practices for WAN optimization and security follow a three-phase progression.

	Best Practice	Blue Coat Solution
Phase 1	Traffic filtering, security and optimization are installed at the network core.	Deploy ProxySG at the core
Phase 2	Application analysis and performance management is implemented at the core and branch offices.	Add PacketShaper at the core and in branch offices
Phase 3	Traffic filtering, security and optimization implemented in branch offices, including support for a direct-to-net model for Internet access.	Add ProxySG in branch offices

Most PacketShaper customers have reached Phase 2 in this progression and have the opportunity to move to Phase 3 by complementing PacketShaper with ProxySG.

The following diagrams describe these three phases in detail.

Best Practices Phase 1: Gateway Traffic Management

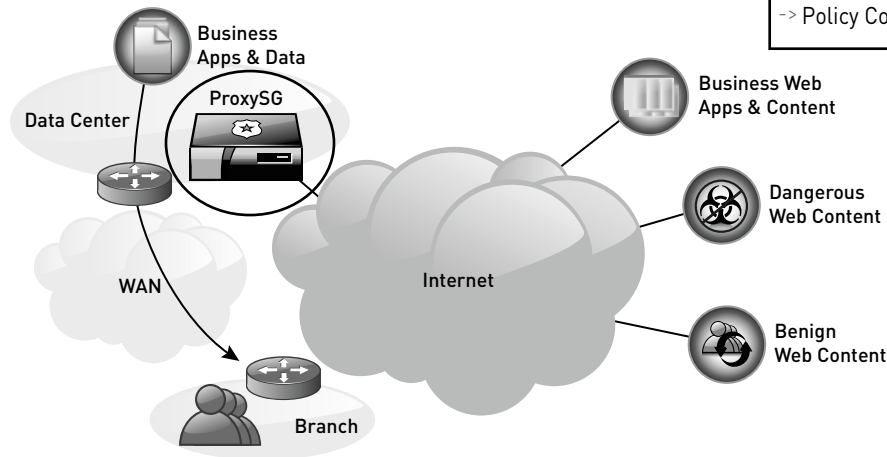
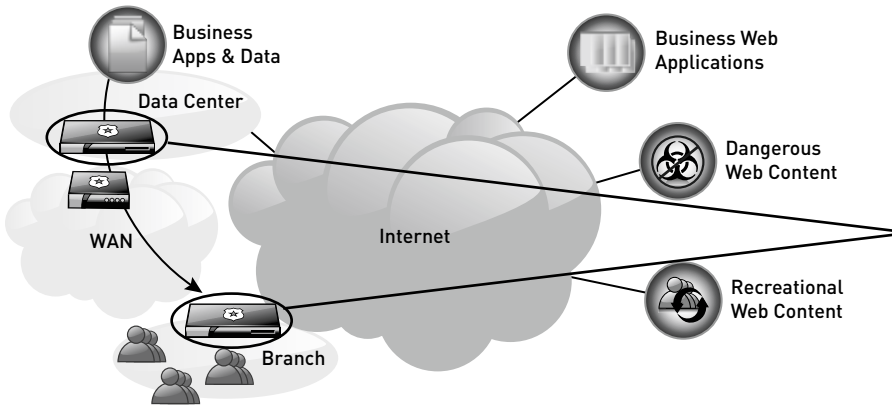


Figure 4: In Phase 1 of a best-practices implementation, ProxySG appliances at Internet access points filter Web traffic to block malware and enforce security and usage controls.



Best Practices Phase 2: Containing Recreational Traffic

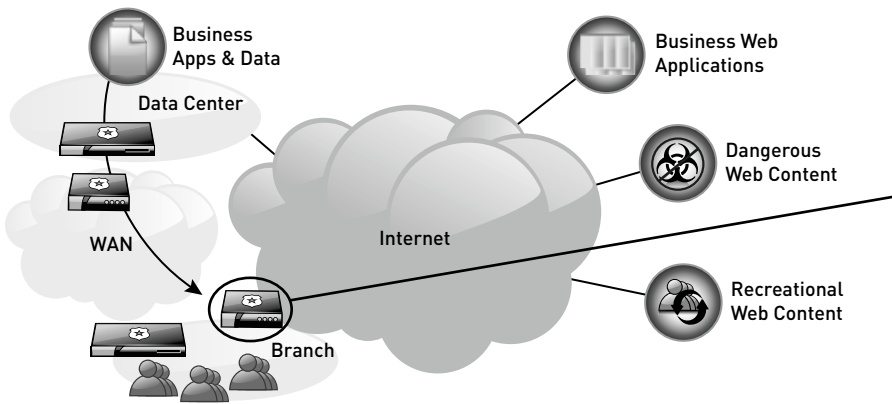


PacketShaper: Visibility & Control at WAN Core and at branches:

- > Discover all applications
- > Determine amount to backhaul Internet
- > Troubleshoot performance issues
- > Contain backhaul recreation to fix issues
- > Provides a single solution supporting Internet, meshed MPLS and hub-spoke WANS

Figure 5: In Phase 2 of a best-practices implementation, PacketShaper appliances at the WAN core and in branches discover applications, determine how much traffic needs to be backhauled and help troubleshoot performance issues for complex MPLS meshed networks or hub-spoke WAN topologies.

Best Practices Phase 3: Enabling Safe “Direct-to-Net” Access



Direct-to-the-Net: Add ProxySG at Branch Offices to Offload the WAN

- > Lower network OPEX, limit backhaul traffic
- > Deliver fast branch office to centralized applications
- > Secure access with policy/malware protection
- > Increases security ROI

Figure 6: In Phase 3, the addition of ProxySG in branch offices enables secure direct-to-net access.

By the time an organization implements Phase 3 of WAN best practices, it has tightened network security at all locations, accelerated application delivery to all users, and taken advantage of cost savings by providing branch offices with fast, secure and direct access to the Internet.

The Blue Coat solution supports all three phases of WAN best practices. Blue Coat enables IT organizations to get the most out of their WAN while supporting IT initiatives for centralization and user mobility.



Addressing Major Trends in Enterprise IT

The table below summarizes the benefits that Blue Coat solutions offer and why an Application Delivery Network should be a clear goal for enterprise IT as they address major business trends.

Trend	How Blue Coat Helps Establish an Application Delivery Network
Applications span multiple network technologies (wired and wireless) and network domains	Comprehensive security and acceleration
Enterprises adopt SaaS applications	5 to 25X acceleration of SaaS application delivery Secure Web access to external applications
P2P applications congest networks and create security threats	Detection, identification and control of P2P network traffic
All traffic through port 80 gets through firewalls	Classification and sub-classification of all the applications riding on port 80 for detailed monitoring and control
Network convergence: VoIP phones become the norm for new installations; there's an increasing amount of voice and video traffic on the WAN	More reliable performance of media applications Dramatic reduction of jitter and latency
Application integration relies on bloated XML communications, rather than terse messaging protocols	Acceleration of Web services through effective compression and caching
Data leaks brings risks of regulatory fines and loss of intellectual capital	Integration with lead data loss prevention (DLP) technologies protects data and stops data loss

Conclusion

Deployed jointly, Blue Coat ProxySG and PacketShaper offer a new level of control in the network stack to achieve an Application Delivery Network. PacketShaper provides industry-leading visibility into applications, as well as advanced controls for performance optimization. ProxySG provides state-of-the-art acceleration with essential branch office security. Together, ProxySG and PacketShaper provide improved visibility and reporting, more comprehensive security and faster application performance for all locations on the WAN.

By establishing an Application Delivery Network in your infrastructure, you can see, secure, accelerate and control applications and successfully meet business goals across your enterprise.



Blue Coat Systems, Inc. • 1.866.30.BCOAT • +1.408.220.2200 Direct
+1.408.220.2250 Fax • www.bluecoat.com



Copyright© 2008 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.