BLUE COAT®

Security
Empowers
Business

# OPEN, MANAGE AND ACCELERATE SSL ENCRYPTED APPLICATIONS

## BALANCING SECURITY, PRIVACY AND PERFORMANCE FOR ENCRYPTED APPLICATIONS

Enterprise users and their data have never been further apart. Business pressures that keep employees out of headquarters and close to customers and partners have met head-on with other drivers that are bringing far flung servers back to the datacenter. Server consolidation for cost and compliance, along with outsourced business services over untrusted public networks, are compelling to business looking to simply operations and cut costs.

### Executive Summary

Often overlooked, however, is the technology that protects all that data and makes it safe to use untrusted networks, Secure Sockets Layer, or SSL. A form of encryption and potentially authentication, SSL ensures data remains private from eavesdroppers, and thwarts impersonation or man-in-the-middle attacks to establish a baseline level of trust between client and server. Because of these risks, everything from sales force automation to investor relations to ordering office supplies goes over SSL encrypted tunnels. This includes internally managed applications as well; the drive to 'webify' applications coupled with new compliance requirements is also generating large flows of encrypted traffic, making accelerating and prioritizing that traffic an IT imperative.

*The drive to 'webify' applications coupled with new compliance requirements is generating large flows of encrypted traffic, making accelerating and prioritizing that traffic an IT imperative.*

SSL may be a ubiquitous enabler of e-commerce and outsourcing, but it creates a special management headache for IT organizations, especially for network administrators and security professionals. SSL encryption thwarts normal acceleration and bandwidth management technologies. Worse, rogue application developers and unscrupulous employees know that SSL traffic is safe from oversight and interference. That traffic combines with the legitimate growth in SSL applications to make for a large and rapidly expanding percentage of WAN traffic opaque to network and security administrators alike.

To regain control over application delivery when almost anything business-related is encrypted, organizations need SSL-aware solutions that can inspect, understand, and accelerate. That solution needs to respect the unique privacy and security concerns inherent in SSL traffic management – the traffic may have been encrypted for good reason, and the network needs to make nuanced decisions about what to decrypt based on the user and application pairing.

### SSL Traffic is Growing in Volume and Importance

#### Organizations Becoming Dependant on SSL Tunneled Services

Real-time encryption has become a common practice for critical business processes. To ensure continued privacy, security and regulatory compliance, organizations are becoming more and more dependant on encryption to protect information on the move. Encryption, however, creates its own management challenges.

Though there are many technologies that can improve the security of data-in-motion, SSL has become the standard of choice for delivering secure applications. Originally a privacy and trust technology for business-to-consumer web sites, as more business-to-business applications 'web-ify' SSL becomes an obvious choice due to its simplicity and reliability. Indeed, owing to its ubiquity as a secure HTTP transport, SSL is being used to tunnel more and more network traffic, and even the entire network itself. However, this creates a special challenge, as the purpose of SSL is to make traffic secure from all inspection, snooping and tampering. Ironically, that makes it exceedingly difficult for organizations to manage their own SSL-tunneled applications. Worse, their own applications are not the only ones exploiting SSL's privacy; spyware, peer-to-peer file trading and other undesirable traffic has flocked to SSL, as IT departments are forced to allow all SSL traffic, or none, across their networks. As a result, though SSL traffic continues to grow, organizations struggle to understand how much of their bandwidth is going to which application, prioritize SSL-tunneled services and enforce corporate policy. To do that, they need an acceleration solution that can deconstruct an SSL tunnel, accelerate and inspect, then reconstruct the tunnel seamlessly.

Many organizations are adept at providing outbound services using SSL. However, as this paper explores, the growing use of SSL tunnels for business-critical data paths requires new management tools and methodologies. Although there are many, three of these drivers are explored below.

### Cost to encrypt data is falling rapidly

When SSL entered the mainstream during the Internet boom of the late 1990s, the computational cost was a significant burden for the server. Today, faster processors and SSL offloading hardware have significantly lowered the performance cost to encrypt.

To meet these requirements, most organizations employ some kind of encryption for data-in-motion. With the growing number of 'webified' applications subject to regulatory scrutiny, SSL has become a popular technology to ensure confidentiality and data integrity. Unfortunately, once the connection is started, it is difficult to manage, accelerate or audit activity owing to the private nature of the SSL tunnel.

### "Inside-Out" SSL tunnels from employees to external service providers

In the modern organization, essential services come from everywhere – from inside the organization, outsourced to tightly-coupled business partners and from opportunistic use of free or inexpensive services available on the Internet. Many such services, to encourage trust and lend a halo of security, use SSL to encapsulate their traffic. Yet that protection makes it difficult for IT departments to ensure delivery, improve responsiveness and triage the necessary traffic from the dangerous. For example, consider:

- **Salesforce.com, and other business critical software-as-a-service (SaaS) applications**. These popular websites have high executive visibility and yet offer IT little control over their reliability or performance. Moreover, since they transport sensitive financial and customer data, they are subject to all of the regulatory requirements of a managed, internally-housed application. Encrypted directly to the end desktop, normal acceleration and quality of service technologies have only limited impact over the end-user experience for this type of application.
- **Occasional service providers, such as financial services websites**. It's easy to overlook just how many different services come from outside the organization. From ADP payroll automation, to investor relations webcasts, to employees checking their 401k plans, down to shopping at approved merchants online, the number of touch points are impressive. Moreover, many of these services, when used, are tapped en-masse and can overwhelm the network; consider employees rushing to the company broker at earnings announcement, or jamming access to the online broker during the approved stock trading window. Though the content is highly repetitive and could greatly benefit from traditional caching and acceleration technologies, encryption requires each packet be served directly from the original source.
- **Partner-hosted secure web applications**. The web has become the mechanism for interfacing with partners. Be it a channel partner entering an order or a streaming web services provider feeding foreign exchange trades into the CFOs office, odds are very good that data travels over HTTPS. Some of these services are trivial or time-insensitive, and should be de-prioritized. Others require a speedy end user experience, even if the application is not hosted internally. Providing and demonstrating that quality of service can be frustrating.
- **Document management systems and inter/intra company collaboration tools**. Easing collaboration between disparate divisions, subsidiaries and partners is a new breed of 'webified' files services, such as Microsoft's SharePoint. Though easy to deploy and very effective in reducing email traffic, these tools consume immense bandwidth. With the redundancy inherent in file transfer, however, they could be dramatically accelerated if security and compliance didn't require the traffic be encrypted.
- **Hosted Email**. For many organizations, outsourcing email to a service provider is a cost-effective and reliable way to provision a vital tool. For others, it is a bandwidth-intensive, opaque way for employees to circumvent controls, leak inappropriate information and conduct personal business on company time. Very often, however, this traffic is SSL-tunneled for end user privacy. As a result, most organizations would like to take a nuanced posture towards web email – accelerating appropriate providers while throttling or outright denying access to others – but struggle to do so.

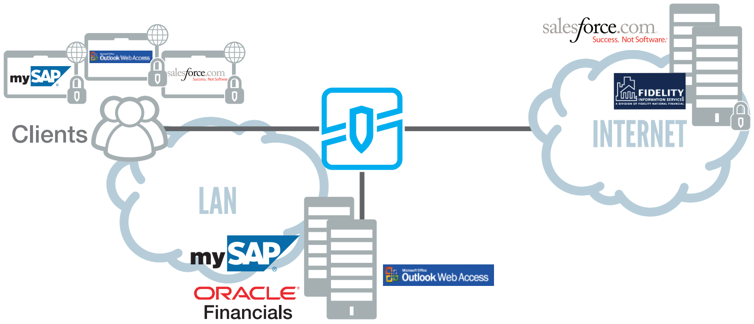

Figure 1: Blue Coat ProxySG appliances provide control and acceleration for all your SSL applications, whether internal or externally hosted.

As more and more of the organization becomes 'virtual,' and best of breed suppliers vie for previously internal processes, the number and diversity of external – and encrypted – services will continue to grow. Though not the original provisioners of the service, the IT department remains "on the hook" to ensure the responsiveness of the network and the security and privacy of the end user.

## Forced To Choose Between Privacy and Performance

Conflicting business drivers are confusing and blurring the boundaries of the modern IT enterprise. On the one hand, organizations of all type are under pressure to get closer to their customers and partners, physically and logically. Simultaneously, other forces push to centralize IT services at the datacenter. Cost is a driver , as is compliance resulting in servers and equipment coming out of remote offices and back to headquarters.

As people move away from the network core, and IT resources move back towards it, the result is a lengthened IT supply line, distancing users from their information and potentially slowing critical business processes. The WAN connections that tie these systems together are increasingly overcommitted, and many of the protocols found there were not written with WAN traffic in mind. Worse, history shows that adding more bandwidth isn't a cost-effective solution, if it's a solution at all. There are too many users, with too many chatty, bandwidth-hungry applications contending for the same network. And, more and more, those applications are using SSL to create tunnels that thwart the caching, compression, and bandwidth management technologies traditionally used to accelerate WAN traffic.

### Regulatory requirements that data be encrypted in transit

Although the precise requirements of regulatory compliance are continually interpreted, it is fair to generalize that many share similar themes: control who has access to what information, and verify the chain of control remains unbroken and fully accounted for at all times. The sidebar contains some examples.

- Sarbanes-Oxley, which requires senior management testify to the accuracy and confidentiality of corporate financials.
- Gramm-Leach-Bliley Act, mandating privacy protections for any non-governmental organization that handles the personal financial data of US citizens.
- Health Information Protection and Portability Act that sets potentially conflicting requirements over health care records – that they be transferable yet punishes unauthorized disclosure severely.
- Safe Harbor has privacy implications for all US firms that have access to the personally identifiable information of European citizens.
- The European Union's Directive on Data Protection goes further, with complicated guidelines for Euro-zone companies that mandate significant data security.
- Payment Card Industry Data Security Standard is a trade-group policy that mandates controls for any organization collecting, processing or verifying payment card holder information.

Ironically, in some ways, complying with regulatory requirements may force organizations to adopt practices that actually hinder best-of-breed security and degrade customer satisfaction. To accommodate the large number of business-critical applications using SSL, most IT departments are compelled to leave the HTTPS port (443 TCP), totally open to outbound traffic; some organizations are obliged to leave it open inbound as well. Developers of rogue applications have quickly seized on this opportunity. Skype, IM, and many peer-to-peer file sharing technologies attempt egress on port 443, and some now use SSL to encrypt their content. Even if the firewall is able to sort true SSL traffic from other applications using port 443, it is unable to answer the more nuanced questions IT is asking. These include:

- What traffic is desirable, and should be allowed (and accelerated, if possible)
- What is benign and can pass but with lower priority
- What should be denied altogether?

The answers likely vary by user, application, location and time of day - far beyond the routing decisions of a typical firewall.

## Most Technologies Don't Solve the Problem

There are several ways to address the spiraling growth of SSL and the resulting loss of control and performance. Each has its own benefits and drawbacks.

### Use SSL offloading hardware

The initial handshake and key exchange for SSL can be computationally intensive, and chatty protocols that open and close connections repeatedly in a single user session only add to the problem. However, offloading that processing to add-on cards helps only the original server and does nothing to address network bottlenecks. If the performance of a single web application is the problem, SSL offloading may be useful tool to consider. By itself, however, SSL offloading will not improve overall network latency, control, or bandwidth availability.

### Decrypt the Tunnel, use Client Web Accelerators

One straightforward option is just to break the SSL connection at the perimeter, and apply browser-based web accelerating technology to the traffic. From a security perspective, this improves visibility and manageability, while also improving performance characteristics of some web applications. Web accelerators rely on two techniques – pre-fetching and object caching – to improve the apparent responsiveness of the web.

However, web accelerators are not designed to improve most of the types of applications that are business critical and bandwidth intensive in today's enterprise. Indeed, over bandwidth and latency stretched WAN links pre-fetching is likely to lead to significantly more traffic. The extra burden web accelerators put on servers and the network causes software-as-a-service websites to block accelerators to keep them from pre-fetching data-intensive dynamic content, such as the entire customer list. On collaboration websites like SharePoint, the default behavior of accelerators often results in large files being pulled down needlessly, while their local caching creates data integrity and security issues as well.

Also, from a security perspective, breaking the tunnel and then passing on the request in the clear may improve security, but impair compliance. Breaking but not restoring the tunnel makes the assumption that the outside network is bad, and the internal unconditionally good – not an assumption auditors frequently share when measuring regulatory compliance. Most requirements clearly mandate sensitive data remain protected for the entirety of transmission over shared media, and the integrity of the source be constant and verified.

### Decrypt the Tunnel, use Server Web Acceleration

For application services directly under IT's control, several vendors including Blue Coat offer application front-ending solutions to optimize content presentation. Many of these devices are effective in improving web application performance on the LAN, across the WAN and through the Internet cloud and should be considered as part of a comprehensive application provisioning plan.

However, though an effective solution for internal applications, they fail to address many of the pain points of SSL tunnels through WAN links. First and foremost, they can only accelerate applications IT owns and manages, and therefore leave outsourced, managed and software-as-a-service applications untouched. Additionally, these devices are specialized for web applications, and are generally blind to file services, streaming content and email that make up the bulk of WAN traffic. Finally, though individual connections to the server are optimized, the overall traffic is not. Redundancies such as graphics, sounds and other repeated content will still cross the WAN and cannot be cached or otherwise accelerated. The cost and latency introduced by backhauling traffic remains.

### Content Delivery Networks

Another possible solution is to buy or build a content delivery network. These services host content in multiple places around the network (or the world) and intelligently route the user to the closest source. Originally designed for truly massive one-to-many consumer websites, the growing scale of web-ified business applications has led some organizations to use them internally. They can be outsourced, or built in-house with commodity clustering and routing technology. Techniques such as dynamic DNS and network location awareness are used to properly match up the user with content. Although an expensive option usually outsourced to global hosting companies, a delivery network can significantly improve the end user experience by localizing the content closer to the point of consumption.

A content delivery network is so successful because it does what IT already knows will work: put servers in the field, close to users. Unfortunately, this assumes that you own the servers and provision the service yourself, and are not sensitive to the cost or compliance concerns that are driving server consolidation. Nor will outsourcing to a third party like Akamai necessarily help, as most branch offices will still have to traverse the WAN to reach the content hosted on the Internet. Unopened and unmanaged SSL will remain a problem on those WAN links.

### MACH5 with Outsourced Applications

More and more critical services are being provided by partners, often over the Internet and secured by SSL. Be it order entry, fulfillment, HR or sales management, organizations are dependent on fast and reliable access to these outsourced applications. Until recently, however, that critical traffic was opaque to IT management because it was tunneled through SSL.

Blue Coat ProxySG appliances at the branch can provide performance relief for backhauled Internet applications, even if they are SSL encrypted. With caching, compression and protocol optimizations, Blue Coat's MACH5 technology dramatically reduces user wait times caused by long round trips to and from the organizations secure web gateway while cutting bandwidth use by 80% or more. Using bandwidth management, the organization can prioritize their SSL outbound traffic to optimize certain critical sites and guarantee a minimum quality of service. Reducing rogue applications alone can result in significant bandwidth gains, but more granular controls allow for sophisticated management techniques – for example changing application priorities at month's end, or making room for backups on crowded MPLS links at night.

Putting ProxySG appliances out in the field has additional benefits; by the time outsourced application data reaches the secured Internet gateway, it is already optimized and compressed to minimize network load on that pipe as well. Combining MACH5 from the branch with ProxySG appliances at the gateway enables IT to have complete, policy-based control over application delivery and security.

## Basic Requirements of an SSL Acceleration Solution

In the absence of an SSL tunnel complicating the solution, the traditional approach is use proxy technology to optimize the WAN link. The addition of SSL creates a special problem for proxies, however, as by definition a proxy silently decrypts and terminates a connection between client and server – exactly what SSL is designed to prevent. To successfully inspect the session, therefore, one side (server or client) must cooperate by extending trust to the acceleration proxy, enabling it to create tunnels on behalf of the endpoint after it has optimized and controlled the underlying traffic.

An SSL proxy, similar to a regular proxy, works as follows:

- The client makes a request for a service, which is discovered somewhere on the network by the proxy.
- If the request is allowed according the proxy's policy, the proxy re-issues the request to the source server on the user's behalf.
- Once the decision to encrypt is made and the SSL handshake begins, the proxy completes the handshake on the client side using the server's encrypted key, and replies to the server as the client.
- There are then two separate tunnels, one on each end of the proxy, with the proxy in the middle bridging the connection. Ideally, this is transparent to both parties.
- WAN Optimization technologies that involve symmetric, or paired, proxies forming compression and optimization tunnels work similarly, with the addition of a secured tunnel between them.

The impact of such impersonation within a protocol designed to ensure both privacy and trust can be significant, however, and potentially troublesome. Though privacy can be maintained with end-to-end encryption, services that rely on SSL certificates for trust-based authentication or authorization – such as HTTPS-based web services or single sign on mechanisms – can be undermined. When one endpoint cedes trust to the proxy to allow its optimization and control, the other endpoint thinks it is communicating directly to a known, trusted party when in fact it is connected through an intermediary. Therefore, ironically the trust and security of the endpoint that doesn't acknowledge the inspection is the most likely to be compromised.

For these reasons, there are certain features of an SSL-aware proxy that can make or break the user and management experience, facilitating or hindering organizational imperatives. Therefore, here are some important considerations when deciding if an SSL proxy is appropriate for your organization.

**A proxy must be able open SSL tunnels transparently to the user**. Unsophisticated users will be confused by certificate warning pop-ups in their browser, resulting in additional unnecessary calls to the help desk. Worse, over time users will simply come to ignore such warnings, increasing the risk of phishing and other online scams.

**The proxy must be able to decrypt at the server side**. This deployment allows servers to be front-ended and offloaded even if they extend services through SSL. Useful for delivering applications outside of the organization to client endpoints not under IT control, server-side decryption generally requires placing the server's private keys on the proxy.

**The proxy must be able to decrypt at the client side**. Client-side decryption is preferable to server-side decryption for two critical deployment types. The first is for decrypting and accelerating client communication with servers you don't control – which is the majority of services by both number and bandwidth in most organizations. This allows control and acceleration of applications in the cloud or out on the Internet. The second is WAN Optimization using two proxies forming a tunnel, where backhaul of SSL encrypted data thwarts caching, protocol optimization and compression. Client-side decryption enables full, end-to-end acceleration for all applications regardless of destination.

**The proxy must participate in the AAA and PKI infrastructures of the organization**. In order to maintain the SSL trust model, the proxy must be able to authenticate both the device and the user it impersonates, regardless of where in the network the inspection occurs. Ideally, it should do so transparently to all parties and integrate into the existing authentication, authorization and audit infrastructure without becoming another database to manage.

**Users should be notified of the inspection, and acknowledge an acceptable use policy**. For legal protection, this is a requirement in many industries and geographies. User notification and consent becomes particularly important in full SSL control and acceleration deployments.

### MACH5 with Internal Applications

Internal applications are SSL tunneled as well, either as part of a VPN solution or due to regulatory mandates. Now IT staff needn't worry about compromising speed and security in the name of privacy and compliance. By selectively opening SSL tunnels, user's expectation of privacy can be maintained while known-good or known-bad applications can be silently accelerated or dropped, respectively. All without requiring that server certificates leave the safety of the datacenter or sending insecure session requests to downstream appliances. The flexibility of MACH5 technology allows for unmatched sophistication in meeting quality of service mandates for internal applications. Natively supporting not only HTTPS but also CIFS, MAPI and most streaming media, the ProxySG is well equipped for the protocols that clog intra-company WANs.

Understanding the interaction between user, content and application, the SG is able to make nuanced prioritization and security decisions, even with encrypted content. Is this allowed content, from an allowed application, from an allowed source, with a valid certificate, going to the right person at the right time? Translating corporate policy to network imperatives, Blue Coat's MACH5 means you don't have to choose between security and performance.

**The proxy must selectively inspect user sessions to allow privacy for appropriate personal use while accelerating company data**. Inspecting all traffic may not be feasible, or desirable. Moreover, those requirements are constantly evolving and could change at any time. Therefore user, application and destination based controls over inspection are a must.

**Routing and prioritization based on user and application, not just IP address**. Business imperatives are more granular than simple host-based matching. Specific combinations of user, application and network situation should all be factored into acceleration and security decisions to align with real-world expectations.

**A proxy must provide significant improvements in speed (latency).** Technologies such as dictionary or byte caching, object caching and protocol optimization can significantly improve the user experience. These begin service delivery almost immediately upon request, removing the inherent delay of data traveling back and forth across a long-haul link.

**The proxy solution must be enterprise scalable and manageable**. Even small organizations consume surprisingly large amounts of bandwidth, and acceleration logic quickly becomes taxing for any device. Further, putting appliances in lights-out networking closets around the globe requires confidence in the remote management and automation capabilities of the solution. And finally, to achieve service and compliance objectives, the proxy must be able to integrate with your existing reporting solutions to seamlessly aggregate data collected from the datacenter, and in the field.

## Choosing to Use an SSL Proxy

Once the proxy has bridged the SSL tunnel – hopefully in a secure fashion – it now has a window into the traffic. At this point, a suite of acceleration techniques can be applied to maximize bandwidth over the WAN link and to minimize latency by serving the client out of a local cache. Critical applications can be prioritized above less important ones, and rogue traffic can be dropped entirely. By blending all traffic bandwidth allocation decisions, the presence of SSL encryption no longer effects the performance of applications across a WAN link. Like with all proxy technology, however, there are privacy and authentication concerns that need to be addressed.

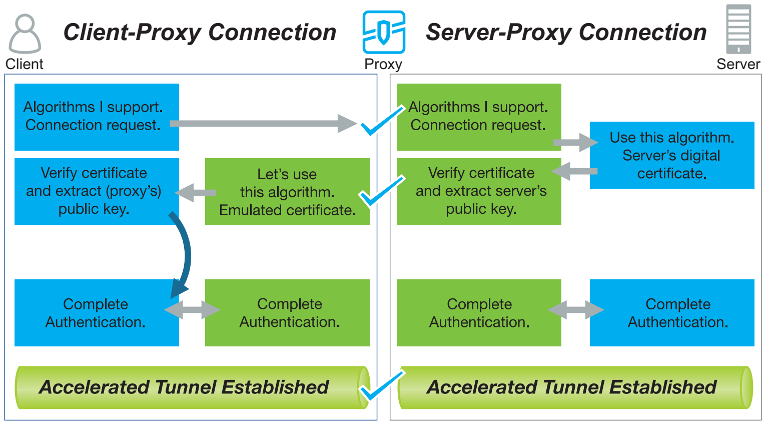
Client-Proxy Connection
Server-Proxy Connection
Client
Proxy
Server
Algorithms I support. Connection request.
Verify certificate and extract (proxy's) public key.
Let's use this algorithm. Emulated certificate.
Algorithms I support. Connection request.
Use this algorithm. Server's digital certificate.
Verify certificate and extract server's public key.
Complete Authentication.
Complete Authentication.
Complete Authentication.
Complete Authentication.
Accelerated Tunnel Established
Accelerated Tunnel Established

Figure 2: Using Blue Coat SSL proxy technology, secure applications are transparently decrypted and optimized

### Balancing User Performance and User Privacy

Using an SSL proxy to manage encrypted traffic can remove a significant network blind spot. Yet by inspecting the traffic, the explicit trust model of SSL comes into question; SSL is, after all, deployed to ensure that the traffic is private during transit. Certain situations require more care and consideration. Employees, for example, may be allowed to connect to secure web brokerages to manage their corporate compensation plans, or to health insurance sites to schedule confidential doctors visits. Partners and other invited guests connecting back to their own offices may access confidential materials under the expectation of secrecy. Depending on your jurisdiction, respecting the privacy of such communication may be more than a policy – it may be the law. When deploying an SSL proxy, therefore, organizations have to consider three different balances of optimization and privacy.

1. Inspect and proxy none of the SSL-tunneled traffic. This is a short term solution that bypasses any regulatory or perception issues associated with decrypting SSL connections. Generally, however, this is only an option when SSL traffic is minimal or can be otherwise restricted, optimization of other protocols frees up sufficient bandwidth on the WAN, and latency of existing SSL applications is not a concern.

2. Proxy selected SSL connections, respecting user confidentiality where appropriate. The choice to inspect could be based either on a white list of known business applications that require acceleration, or an exclude list of known private sites that users are allowed to browse without the proxy opening their communication. For highly regulated organizations that need to testify to the flow of information for compliance purposes, this type of partial proxy deployment allows them the flexibility to inspect and audit traffic selectively.

3. Open, inspect and accelerate all SSL traffic. Clearly, this would allow the proxy maximum control over bandwidth and unauthorized communication. Implicitly, it also facilitates and encourages additional use of SSL by removing network performance considerations, aiding compliance objectives. Though ideal from an application performance and bandwidth management perspective, any full SSL proxy must be able to notify users and log their consent to a use policy. That requires the use of a pop-up or splash screen to collect the consent, logging functions to aggregate it and a reporting mechanism to produce audit-proof documentation.

## Blue Coat MACH5 – An Intelligent, SSL-Aware Acceleration Framework

Blue Coat's SG Operating System offers a best-of-breed framework for application acceleration and management called MACH5. A five-part Multiprotocol Acceleration Caching Framework, MACH5 brings to bear the complete range of Blue Coat's content security and management solutions while offering unparalleled bandwidth savings and application acceleration. SSL stands at the intersection of application performance and security, and the Blue Coat ProxySG appliance with MACH5 technology is the only full SSL proxy capable of decrypting, accelerating and managing SSL content regardless of the application's location around the network.

**SSL Session Management**. The first step towards regaining control of tunneled traffic requires understanding who is connecting to what. Only an application layer, SSL-aware proxy with integration into the enterprise authentication system can make quality of service decisions based on user and application pairs. Blue Coat MACH5 SSL proxy technology goes further, allowing acceleration, accept/deny and routing decisions dictated by SSL characteristics, including facts about the source certificate that include who signed it, when it expires and the organization that issued it. Combining SSL session awareness with AAA and PKI integration uniquely allows the Blue Coat solution to fully accelerate and control SSL traffic without breaking the SSL trust model.

Based on all that information – user, certificate credentials, application, port, destination, etc – the Blue Coat ProxySG can make decisions about how to handle SSL connections. It can choose to proxy all SSL traffic silently, without the user being aware, or can offer notification and even user-responsive acceptance pages to let the user know a proxy is actively inspecting their communication.

**Accelerate SSL Encrypted Content**. Whether the organization chooses to inspect all SSL traffic, or only selected streams, Blue Coat ProxySG proxies can accelerate all SSL traffic you allow them to see regardless of whether or not you control the source server. Using native HTTP and TCP protocol enhancements for HTTPS traffic, in addition to byte caching, object caching and compression, results in industry-leading performance enhancements even over encrypted content.

**Choose Where To Inspect**. Blue Coat supports both server-side and client-side SSL decryption to provide the broadest array of deployment options to accelerate SSL applications both internally and externally in a manner consistent with your certificate management practices.

**A Reliable and Manageable Solution**. Blue Coat is the premier supplier of content delivery appliances, with over 30,000 devices in deployment, thousands of customers and dozens of installations exceeding 500 ProxySG appliances each. The requirements of our customers, including some of the largest organizations in the world, for an enterprise-class solution means that we have already met some of the most stringent scalability and manageability requirements in the industry. These include transparent tunnels that do not interfere with network management suites, full "n-way" native clustering for scale and availability, and automatic auto-discovery with encrypted tunnels that maintain private connectivity between appliances should the network suddenly change.

To deliver this level of high performance while retaining flexibility, Blue Coat relies on a custom OS. The Secure Gateway Operating System has been organically developed internally for over a decade, and is designed for nothing but accelerating and securing content. As a result, Blue Coat is uniquely positioned to provide policy-based, granular control over all types of traffic at wire speed for a reasonable cost.

Combined, these characteristics make the Blue Coat ProxySG appliances with MACH5 technology an enterprise-class solution for a variety of application performance and security challenges.

## Conclusion

Delivering applications over long, skinny WAN pipelines is no easy feat, and the presence of impenetrable SSL tunnels made it impossible to accelerate a growing part of that traffic. Now, with the help of Blue Coat MACH5 technology, IT can once again gain control over their WAN links, accelerating the good and denying the bad, regardless of SSL encryption. No matter how your users reach their critical applications, Blue Coat's MACH5 can help: inbound to your own server farm, outbound to third-party service providers, SSL tunneled or in the clear, MACH5 accelerates and secures your business data. Blue Coat's appliances do all of this in a way that acknowledges that the balance of performance, security and privacy will be different for each organization, and empowers IT to translate written business policy into a deliverable quality of service pledge.

Security
Empowers
Business

This document is for informational purposes only. Blue Coat makes no warranties, express, implied, or statutory, as to the information in this document. Blue Coat products, technical services, and any other technical data referenced in this document are subject to U.S. export control and sanctions laws, regulations and requirements, and may be subject to export or import regulations in other countries. You agree to comply strictly with these laws, regulations and requirements, and acknowledge that you have the responsibility to obtain any licenses, permits or other approvals that may be required in order to export, re-export, transfer in country or import after delivery to you.

v.WP-ACCELERATE-SSL-ENCRYPTED-APPLICATIONS-EN-v5b-1013

Blue Coat Systems Inc.
www.bluecoat.com

Corporate Headquarters
Sunnyvale, CA
+1.408.220.2200

EMEA Headquarters
Hampshire, UK
+44.1252.554600

APAC Headquarters
Singapore
+65.6826.7000