Application Performance Brief: HTTPS Applications

Performance Summary

- Securely accelerate any HTTPS application on the Internet
- Realize 250 times or more improvement for HTTPS downloads
- Reduce bandwidth utilization by 95 percent or more for HTTP
- Improve user productivity, offload servers, create granular policy to control and protect users

Test Scenario

These tests were performed using a Windows XP client retrieving files from an Apache web server hosted on Windows 2003 server. The tests were run on a simulated WAN of 256Kbps with 40ms latency, and a T1 link with 100ms latency.

- For the cold test, the starting condition is no traffic has passed through the Blue Coat yet.
- For the warm test, the starting condition is same or similar traffic has already passed through the Blue Coat once.

Blue Coat Accelerates and Optimizes HTTPS

Enterprises face mounting challenges as the use of secure web based content and applications grow, many of them mission critical and confidential. These applications use an encrypted transport mechanism (commonly known as SSL or HTTPs) to secure applications ranging from database, ERP, and finance to collaboration software, such as Sharepoint and Webex. This traffic is generally not visible and therefore uncontrollable to network administrators, but requires significant WAN bandwidth and remain latency sensitive, leading to poor performance. In addition, harmful or malicious code can be masked by this encryption. Blue Coat appliances can intelligently detect, inspect, optimize and accelerate all secure web traffic – even for external servers you don't control – reducing latency, increasing WAN throughput, and returning control, visibility, and security to network administrators.

HTTPS over the WAN

Secure web traffic, commonly known as HTTPs, is based on HTTP but uses an authentication/encryption layer between HTTP and TCP. This additional layer is the Secure Sockets Layer (SSL) and Transport Layer Security (TLS), which is used to authenticate connection endpoints and provide an encrypted communications channel between the end user and secure web application server. SSL/HTTPs also secures against Man-In-The-Middle attacks. Endpoint authentication allows the server to be verified by the client, and if desired, the client to be verified by the server.

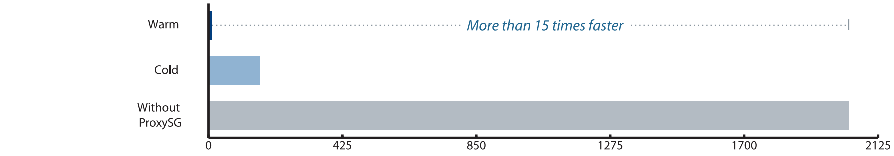
Server verification is accomplished by providing web servers with a digitally signed certificate from a trusted Certificate Authority (CA) and then presented to the end user. Similarly, user authentication is also provided by allocating digitally signed certificates to each user, and are presented only when mutual authentication is required.

Unlike other vendors introducing HTTPS optimization without a security background, Blue Coat has fielded SSL protocol optimization for years to major enterprises such as financial, defense, and government organizations. Detection and inspection capabilities are possible for all inbound and outbound HTTPs traffic, whether it is across the LAN, WAN, or destined for the Internet.

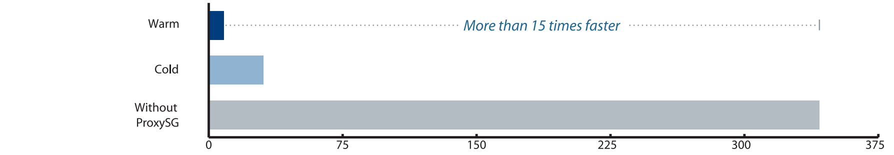
Performance Results

In a test of transferring a file via HTTPS, ProxySG appliances reduced the transfer time by over 99% to LAN wire speed, and decreased bandwidth usage by up to 100%. The test was transferring a 50MB file over a 256Kb WAN with 40 ms latency, and over a T1 with 100ms latency.

256K WAN with 40ms latency Transfer time: (no device=2076 sec, cold=145 sec, warm=7sec)



T1 WAN with 100ms latency Transfer time: (no device=343 sec, cold=31, warm=8 sec)



How Blue Coat Accelerates and Optimizes HTTPS

Blue Coat appliances use patented technology to detect, inspect, optimize and accelerate all HTTPs web traffic and SSL/TLS based applications. Unlike other solutions, administrators have the flexibility to choose the optimization and acceleration techniques for their enterprise depending on their security policies. Blue Coat appliances use patented software techniques and hardware acceleration to optimize encryption algorithms and reduce SSL/TLS handshakes over the WAN. This significantly improves user experience, improves overall productivity and increases performance of servers in the data center. In addition, administrators can reduce latency and improve bandwidth by securely reducing and limiting redundant patterns of traffic, anywhere from the byte/packet level up to the application level, or even both when configured. These acceleration and optimization techniques can be granularly applied (or not applied) based on users or departments, source or destination, application or content, or all of the above.

Blue Coat Benefits

Improve user productivity, reduce bandwidth usage

Objec t and Byte caching significantly improve HTTPS response times while conserving bandwidth.

Secure/Simple Deployment

- Avoid exposing sensitive private keys from HTTPS web servers unlike other simplistic solutions
- Easy to deploy, no need to explicitly gather and install/ import private keys for each and every HTTPS application.
- Securely accelerate Internet/ outsourced HTTPS applications.

Server Offload

Deploying Blue Coat for HTTPS acceleration can offload secure web servers, where key exchange and bulk encryption can be CPU intensive. Competing products which operate at the transport layer will generate server overload.

Remove Unwanted Traffic

Deploy Blue Coat to unclog your networks by removing business irrelevant and malicious web traffic hiding inside HTTPS.

Secure the Web

Blue Coat provides granular and flexible policy to enforce your company's security requirements and protect your users.

About Blue Coat MACH5 Acceleration Technology

Blue Coat MACH5 technology is a patent-pending combination of five separate application management and tuning technologies that provide unrivaled improvements in application performance and bandwidth utilization. Whether at the edge of your network, or right in the heart of it, MACH5 technology provides a powerful toolkit for meeting any application delivery challenge. These technologies include:

Bandwidth Management

Assign priority and network resources based not only on port or device, but on users, applications and content to more accurately reflect your corporate policies on the network. Works by itself, or integrates with your infrastructure QoS to provide application intelligence to the packet switching network.

Protocol Optimization

Improves the performance of protocols that are inefficient over the WAN through specific enhancements that make them more tolerant to the higher latencies typically found there. Blue Coat has been optimizing network protocols for over a decade, and offers multiple improvements for TCP, CIFS, HTTP, HTTPS, MAPI and most streaming video and IM protocols.

Byte Caching

Cache repetitive traffic found in the byte stream and serve it locally to reduce the amount of traffic that actually uses the WAN at all. Works like a customized compression algorithm for your network traffic, and leads to dramatic bandwidth savings.

Object Caching

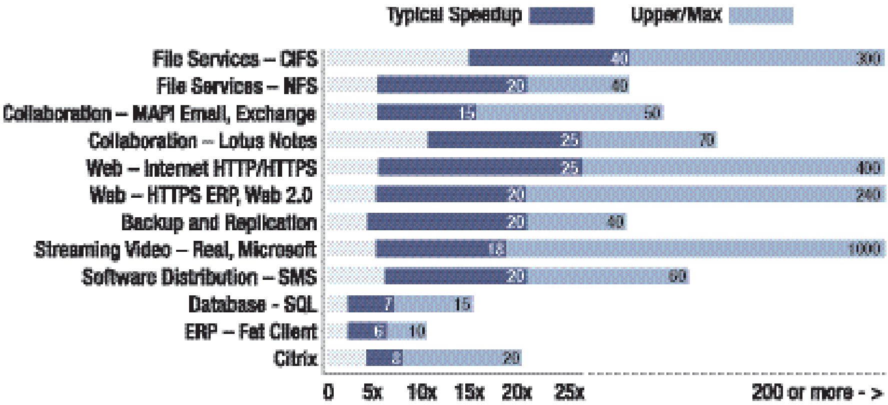
Store files, videos and web content locally, providing LAN-like performance for WAN users, without the overhead and risk of traditional wide area file services. For content delivery, no technology does more to reduce latency and bandwidth to improve the end user experience.

Compression

Inline compression can reduce predictable patterns even on the first pass, making it an ideal complement to byte caching technology.

About the Blue Coat ProxyClient

ProxyClient builds on Blue Coat's secure web gateway and acceleration technologies to extend application delivery to the desktop. Using MACH5 technology, including caching, compression and protocol optimization, ProxyClient accelerates web and office applications for roaming and small branch users. ProxyClient delivers LAN-like user experience and Blue Coat web filtering with a simple and easy footprint for installation, configuration, deployment and ongoing maintenance.


Typical Speedup
Upper/Max
File Services – CIFS 40 300
File Services – NFS 20 40
Collaboration – MAPI Email, Exchange 15 50
Collaboration – Lotus Notes 25 70
Web – Internet HTTP/HTTPS 25 400
Web – HTTPS ERP, Web 2.0 20 240
Backup and Replication 20 40
Streaming Video – Real, Microsoft 18 1000
Software Distribution – SMS 20 60
Database - SQL 7 15
ERP – Fat Client 6 10
Citrix 8 20
5x
10x
15x
20x
25x
200 or more - >