



## Comprehensive Web Security with Blue Coat

Web traffic is increasingly becoming a popular vector for attacking networks as most organizations have addressed other well-known vulnerabilities by deploying email AV gateways and desktop AV clients. Now, attacks, such as drive-by installers of spyware and viruses tunneling over SSL, often go undetected by today's perimeter security, which is often merely a firewall with Web content filtering. Networks without comprehensive security at Internet access points, which analyst firm Gartner estimates is approximately 85% to 90% of corporate networks, organizations are unwittingly exposing themselves to serious, Web-based attacks.

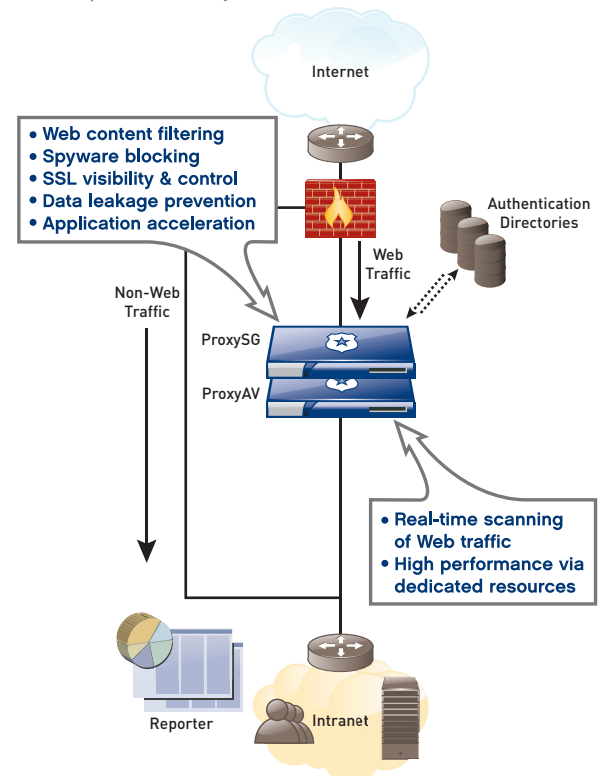
Adding to the problem, implementing more control – such as AV scanning of Web traffic and enforcing user-based policies – often corresponds to a noticeable decrease in Web application performance, frustrating users and undermining business benefits. Balancing the competing concerns of available Web access, proactive security, and high performance for end users, represents a significant challenge for IT departments.

To provide users with a safe and productive Web environment, organizations require a Web security infrastructure that will allow approved Web traffic – such as employees using Salesforce.com – and block unauthorized and unwanted Web traffic – such as unsanctioned URLs, malware hiding in SSL, or confidential information leaking over personal Webmail. In addition, the solution must not impede business by slowing down Web-based business applications. In fact, as users become more and more distributed, accelerating access to these applications becomes essential to keep businesses running. In short, organizations require a Web security solution that stops the bad and accelerates the good.

As Gartner's Magic Quadrant Leader for the Secure Web Gateway, Blue Coat provides a robust and flexible solution to control users and protect against Web-based threats – while actually improving Web performance. Blue Coat appliances are deployed at Internet access points across the distributed enterprise, providing an effective solution to control security for all Web applications and content – including encrypted SSL traffic.

- > Complements existing firewall and other perimeter security infrastructure.
- > Proxies all inbound and outbound Internet traffic – including SSL encrypted information – for comprehensive control.

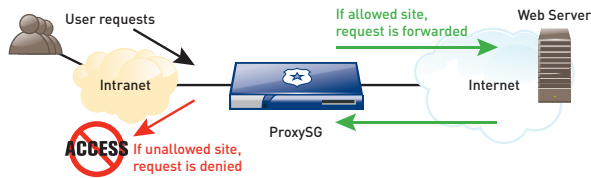
- > Enforces Internet Acceptable Use Policies for authorized Web surfing through on-box content filtering.
- > Protects against spyware and other malware by scanning all inbound and outbound Web traffic (including file attachments) for viruses and other malicious code.
- > Accelerates all or individual Web applications through integrated caching, content positioning, compression and bandwidth prioritization.
- > Controls access to instant messaging (IM), peer-to-peer (P2P) file sharing networks and streaming media applications.
- > Logs all Web traffic for comprehensive reporting by user for complete visibility.





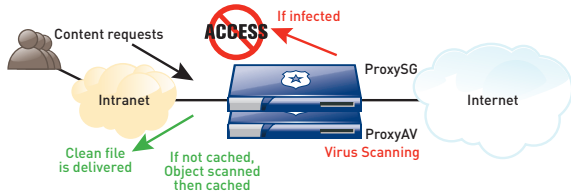
Blue Coat's ProxySG and ProxyAV appliances are the ideal choice for providing visibility and control of all Web communications, so organizations can both control Web traffic for maximum protection and accelerate Web applications for maximum productivity.

### URL/Content Filtering



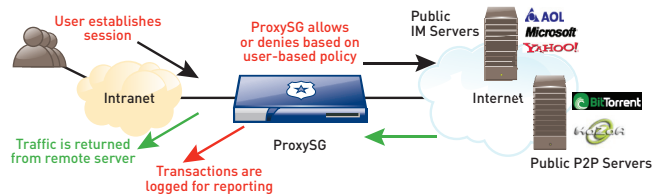
Integrated URL and content filtering allows organizations to prevent users from accessing or viewing inappropriate content, such as porn and gambling sites, on company machines. Additional protection is provided through content stripping and replacement, such as blocking inappropriate pictures from a Google image search.

### Web Virus & Spyware Protection



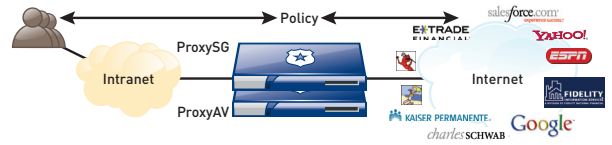
Scan once, serve many" approach provides the real-time performance and scalability required to effectively scan Web content. Further protection provided by controlling downloading executables and other potential malware from suspected spyware Web sites.

### IM & P2P Control



Protocol adapters for IM & P2P provide centralized management of leading Instant Messaging and P2P applications, including Skype.

### SSL Visibility & Control



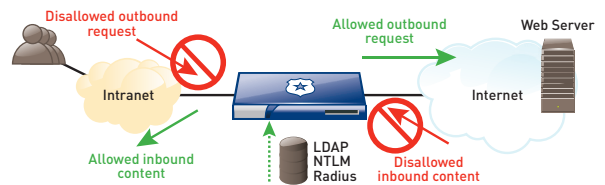
SSL proxy capabilities deliver granular control of SSL traffic, from blocking spyware and viruses tunneling over SSL to preventing the leakage of sensitive information over encrypted personal Webmail.

### Information Leakage Prevention



Visibility into all network traffic – including SSL-encrypted traffic, per policy – allows organizations to scan and block any confidential or sensitive information from crossing the network perimeter.

### Accelerated Web Applications



High-performance Web proxy with integrated caching, content positioning, compression and bandwidth management improves the performance of all or select Web applications.