

# Blue Coat SG™ with Web Virus Scanning

## High performance, Real-time Virus Scanning of Web Content

New viruses, spyware, Trojans, 'bots, worms, and other malware increasingly use the Web browser to invade organizations' PCs. Profit-motivated hackers exploit HTTP and HTTPS because these are essentially allowed protocols for most organizations, and permitted by firewalls. This is the weak spot in most security plans. To make matters worse, newer malware often uses root kits so difficult to remove that administrators are forced to erase the hard drive and start over. To prevent these increasing costs and headaches, malware must never get to the PCs where it could execute.

Virus Scanning at the Internet access point plays a critical role in network security by removing harmful content at the security perimeter—before it enters and infects the network. Just as organizations deployed virus scanning on corporate email systems to secure SMTP-based services, there is a need to deploy virus and malware scanning solutions to protect against new HTTP and HTTPS threats that utilize Web-based services.

## Why Use Blue Coat SG to Virus Scan Web Objects?

**Integrated Web Anti-virus (AV) System** – Blue Coat SG supports gateway AV Scanning by integrating with Blue Coat AV™ appliances, or ICAP-Compliant AV servers. Blue Coat SG with content caching provides a scan-once-serve-many-times solution, to increase performance of HTTP, HTTPS, and FTP virus scanning. When AV updates are applied, Blue Coat SG intelligently rescans cached content based on user demand, maximizing bandwidth gains and improving the user experience. Blue Coat AV™ provides additional performance gains by tracking checksum “fingerprints” of many non-cachable objects, and avoiding unnecessary scanning if the identical object is downloaded again. Additionally, Blue Coat AV's integration with Blue Coat SG leverages an extended ICAP+ protocol with the improved error and exception handling required to efficiently and effectively deal with enterprise Web traffic.

**Scalable Performance** – The Blue Coat SG runs on a purpose-built, secure operating system specifically designed to provide fault tolerance, scalability and performance required for the largest Web AV installations. Latency remains flat with Blue Coat SG and one or more Blue Coat AV (or ICAP compliant AV) servers allow the integrated system to scale performance.

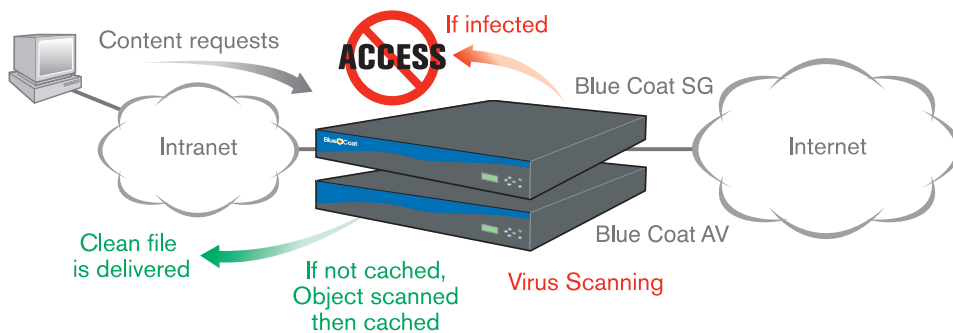
**Layered Security** – Web AV with Blue Coat SG provides a choice of AV engines allowing enterprises to leverage “Vendor A” for their network virus scanning and “Vendor B” for their desktops, servers and gateways. Comprehensive Blue Coat policies and method-level controls in the Blue Coat SG stop worm outbreaks where virus signatures fall short.

Blue Coat SG with Web virus scanning enables organizations to:

- Improve corporate security by scanning for viruses, trojans and worms that utilize Web-based backdoors
- Synchronize AV updates with Blue Coat SG cached content to avoid re-infecting users while maintaining bandwidth gains
- Perform health checks of virus scanning servers, plus load balance multiple servers for scalability
- Control Web content and Web virus scanning in one integrated system with centralized policy management
- Interoperate with Blue Coat AV appliances or ICAP-compliant AV servers with a choice of AV engines
- Blue Coat AV utilizes engines from:
  - Kaspersky
  - McAfee
  - Panda
  - Sophos
  - Ahn Lab
- Blue Coat SG integration with ICAP-compliant AV solutions (e.g. Symantec)

Reference our TechBriefs for details about Web AV integration with Blue Coat SG

[www.bluecoat.com/resources](http://www.bluecoat.com/resources)



Blue Coat allows organizations a choice of leading virus-scanning products to provide a scalable, low latency virus scanning solution for Web content.

Web virus scanning with Blue Coat SG enables organizations to scan for viruses, worms and trojans entering through Web-based backdoors including:

- Personal Web email accounts where a majority of viruses and worms propagate
- Web spam or email spam which unknowingly may activate trojan downloads
- Browser-based file downloads that bypass existing virus scanning defenses

Blue Coat Systems has developed strategic partnerships to complete its Web virus scanning solution. Blue Coat AV provides an appliance-ready solution with support for anti-virus engines from Kaspersky, McAfee, Panda, Sophos, and Ahn Lab.

Leveraging the Internet Content Adaptation Protocol (ICAP), the Blue Coat SG easily integrates with ICAP-based solutions from Symantec, and others.

Blue Coat's Web virus scanning solution is fully optimized within the Blue Coat SG family of proxy appliances. The Blue Coat SG provides comprehensive control, logging and reporting of all scanned traffic while delivering a single point of management for additional services. With the power and flexibility of the Blue Coat SG and AV appliances, organizations can leverage their existing security infrastructure to stop Web-based threats in their tracks.

## Key Features:

### Blue Coat AV Integration

Pre-defined settings in Blue Coat AV for optimal performance and reliability with Blue Coat SG, plus simple appliance deployment

### Visual Policy Manager

Web-based policy management application with an intuitive, graphical user interface for defining and managing content scanning and filtering policies

### Policy Processing Engine

Patent-pending system enables sophisticated, granular policies based on individual users, groups of users, time of day, location, protocol, user agent, content type and other attributes

### Custom Splash Pages

"Coach" users through custom splash pages that communicate the organization's Internet access and download policies

### Content Stripping

Define policy for uploaded and downloaded content based on file or MIME type

### ICAP Server Integration

Blue Coat SG integrates with ICAP compliant AV servers for a standard solution

### Auto Sense Settings

Quickly obtain settings from existing ICAP servers to avoid tedious configuration steps