Blue Coat AV™ 510 Series

Blue Coat AV prevents viruses, trojans, worms, and spyware from entering your organization via the Web. Gateway anti-virus scanning secures rogue channels such as personal Web email and Web downloads. Blue Coat AV uniquely provides:

- Enterprise-level manageability with ICAP+ level of integration for enhanced deployability and automated event management

- Wire-speed, enterprise-grade scanning performance

- Choice of best-of-breed AV engines to facilitate a multi-layered defense-in-depth strategy of different AV engines at the gateway and the desktop

Traditional Web anti-virus gateways scan frequently downloaded objects over and over, wasting processing power, compounding latency, and compromising performance. Blue Coat AV, integrated with Blue Coat SG™'s world's fastest caching, accelerates AV gateway performance with a scan-once-serve-many-times architecture.

The Blue Coat AV510 Series is a purpose-built solution designed for simple integration with Blue Coat SG810 and SG510 series solutions for medium enterprise or distributed environments providing scalable performance with a choice of antivirus engines.

"Given the widespread use of web-based email systems by employees for their personal email – which often bypasses a company's email servers – and their antivirus protection, network deployment of antivirus technology is an important complement to host-based antivirus software."

– ICSA Labs

Blue Coat AV Highlights:

Web Virus Scanning
Real-time, scalable virus scanning using a proven antivirus engine to protect against:

- Infected Web Email
- Spyware & SPAM Trojans
- Internet Worms
- Malicious HTTP & FTP Content
- Optionally scan HTTPS traffic to remove viruses from encrypted browser session downloads

Scalability & Performance
Integrated system allows scanning of web-objects at wire speed. Heuristics improve scanning response while the Blue Coat SG caches clean content for almost zero latency distribution.

Layered Security
Choice of proven antivirus engines with automated updates allows enterprises to leverage "Vendor A" for gateway scanning and "Vendor B" for desktop and server scanning. Choose from:

- Kaspersky
- McAfee
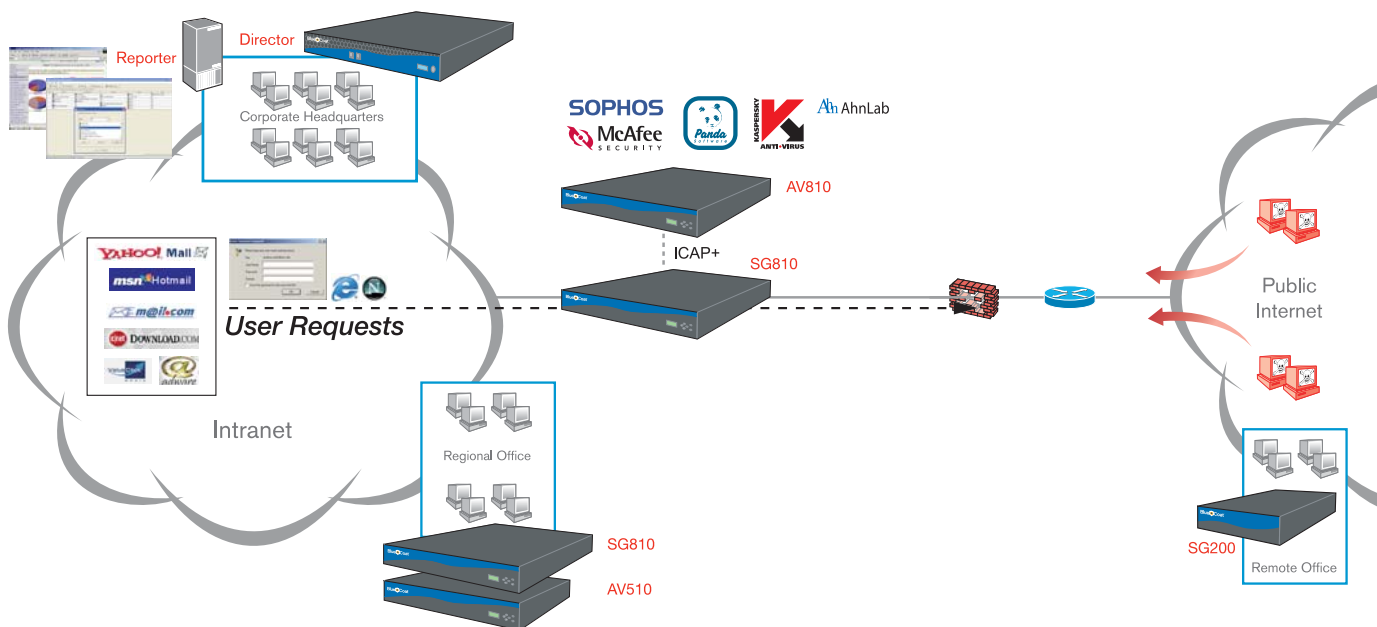- Panda
- Sophos
- Ahn Lab

Ease of Deployment
Integration between the Blue Coat AV and the Blue Coat SG is seamless with default configurations optimized for performance. One vendor, one solution, with purpose-built appliances.

And More...
See Blue Coat TechBriefs for additional Blue Coat SG & Blue Coat AV application & control solutions:

www.bluecoat.com/resources

The Blue Coat AV510 integrated with the Blue Coat SG provides the scalability and performance to scan Web communications and file downloads for viruses, worms, trojans and spyware

Scalability and Performance

Pairing the Blue Coat AV with the Blue Coat SG provides significant advantages for high-speed Web virus scanning that standalone systems cannot match, such as:

- Blue Coat SG processes Web objects at wire speed with integrated caching (up to 400 Mbps, 7 msec latency)
- Blue Coat AV only scans Web objects forwarded from the Blue Coat SG for improved performance
- Blue Coat AV focuses CPU processing on virus scanning using heuristics to maximize throughput
- Blue Coat AV provides load balancing and clustering of multiple Blue Coat AV appliances for enterprise scalability

- Granular policies and method-level controls in the Blue Coat SG stop worm outbreaks where virus signatures fall short (e.g., spIM buddylink)
- Active/active bridging provides failover support on the Blue Coat SG and allows the addition of multiple Blue Coat AV appliances for future growth
- Enhanced processing architecture

The Blue Coat solution means less hardware, high performance virus scanning, and granular control of Web communications. The Blue Coat AV with Blue Coat SG provides unmatched visibility, control, and scalability in an integrated system.

Ease of Deployment & Administration

The Blue Coat AV is optimized for integration with the Blue Coat SG as a complete system, through the following:

- Purpose-built appliance solutions from a single vendor; designed, tested and manufactured for compatibility
- Blue Coat's Blue Coat SG and Blue Coat AV appliances communicate using an enhanced and optimized version of ICAP, enabling superior performance, reliability, and error/exception handling over software-based ICAP servers.
- Virus updates to the Blue Coat AV are automated with definable time frequency settings, and cached content is automatically cleared with each update
- Administrators can define default or custom locations for signatures and virus engine updates, and configure behavior of Blue Coat AV upon license expiration
- Configurable options for scanning files include: set time-out duration, drop file if errors in scanning occur, and define trusted sites

- Heuristics fingerprint recurring files as infected or clean for non-cacheable content to improve efficiency
- Administrators can apply allow/deny lists with extensions along with file size and content type restrictions
- Customized alerts can notify administrators when a virus is found, AV updates are successful, AV updates fail, subscriptions expire, files are dropped, or files pass without scanning
- Log files can be customized using standard logging formats and sent off-box via TCP or UDP for processing
- Health checks from Blue Coat SG to Blue Coat AV verify status and availability of appliances
- New firmware updates and release notes are sent to Blue Coat AV for administrator approval and installation

Layered Security

Recent virus and worm outbreaks, spyware, and the increase in browser-based attacks show the importance of a layered security strategy provided by:

- Choice of proven antivirus engines with automated updates allows enterprises to leverage "Vendor A" for gateway scanning and "Vendor B" for desktop and server scanning.

- Utilizing Blue Coat SG for control over Web communications for both outbound requests and content replies to provide added protection beyond virus signatures and patterns

- Implementing three key methods to control Web communications - the Blue Coat SG controls "transport" and "content", while the Blue Coat AV provides "signatures"

- Enforcing Blue Coat SG policies to control Web communications upon outbreaks and before virus signatures are available

Control Beyond Signatures

The patent-pending Policy Processing Engine within Blue Coat SG enables enforcement of sophisticated security policy based on individual users, groups of users, time of day, location, protocol, user agent, content type and other attributes. These comprehensive capabilities include:

Proxy support for multiple protocols

- HTTP, HTTPS, FTP, Telnet, SOCKS, P2P, AOL IM, Yahoo IM, Microsoft IM, MMS, RTSP, QuickTime, TCP-Tunnel, DNS, CIFS, MAPI

- Apply policy to all

Content Filtering

- On-proxy support of leading URL lists, popular regional lists, plus custom lists

- Performance gains through integrated caching

- Define additional custom categories

Optionally scan inside SSL Traffic

- Enforce all policies in HTTPS as well as HTTP and FTP

- Remove viruses in SSL-based Webmail attachments

- Prevent Trojans, worms, spyware and viruses from entering via encrypted browser sessions

Content Security

- Control MIME types and file extensions

- Strip and replace active content

- User agent and version control

- Header inspection, rewrite, and suppression

- Method-level controls per protocol

- Policy flexibility beyond typical "regex"

- URL parsing

IM Logging and Controls

- MSN, Yahoo!, AIM

- Method-level control settings for file attachments, voice, and video, plus IM reflection for internal use

- Keyword searches
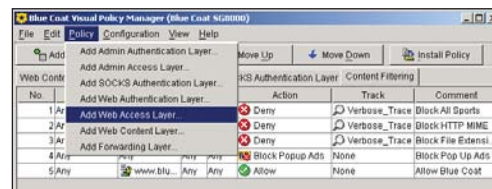
The Blue Coat Visual Policy Manager enables a breadth of solutions addressing general to specific customer requirements for Web content control and Web virus scanning.

- In band/out-of-band alerts

Block or control Streaming Media

- MS, Real, QuickTime

- Bandwidth optimization with stream splitting and caching

P2P file sharing controls

- Log and block P2P traffic by user agent and version, plus numeric host file transfers

- Control BitTorrent, eDonkey, Gnutella, and FastTrack

- Bandwidth optimization

Pop-up Control and Anti-Phishing

- Policy-based

- Deny/allow per application

Comprehensive port services

- Enable/disable needed ports

- Modify port attributes

Authentication

- Utilize a company's existing authentication including local password files, NTLM, LDAP (Active Directory, eDirectory, SunOne), Oracle Access Manager, RADIUS, CA eTrust SiteMinder, and certificates

- Multi-realm authentication sequencing

- Secure credential acquisition via SSL

Integrated System Solution

The combination of Blue Coat SG + Blue Coat AV provides scalable performance with control over transport and Web content with integrated virus scanning. Virus engines and signatures are only one part of Web content control. New worms and trojans are using IM and Web spam to propagate with new techniques always on the horizon. For the first time, Web communication controls and Web virus scanning work together using Blue Coat solutions.

Blue Coat Support Services

Blue Coat supports its products with an outstanding customer support program. All Blue Coat products come with a 90-day software and one-year hardware warranty. Support services include a WebPower password enabling access to the following:

- Online access to open technical support cases, review open cases, and add comments to existing cases
- Exclusive support documentation, installation notes, and FAQs
- Blue Coat Instant Support provides an online self-service portal for your technical needs, and our online TechBriefs review popular protocol and application solutions for a quick start on common configurations.

Platinum Service: 24X7 Technical phone support, Advance hardware replacement*, software updates

* Hardware will be shipped same day when RMA Requests are received during regular business hours and deemed necessary by Technical Support before the RMA cut off time.

Blue Coat Training

Blue Coat provides educational services and technical training (basic to advanced) by certified and experienced trainers enabling administrators to become fully proficient on all aspects of Blue Coat SG and Blue Coat AV appliances. All courses are replete with real world examples and feature extensive hands-on lab exercises.

Each student will learn to install, configure and troubleshoot all features and functions. Please refer to the following Web link for training times, locations and cost:

www.bluecoat.com/resources/training

Blue Coat channel sales partners are also certified to provide field services. Our partners attend Instructor-led courses as well as monthly online training on the latest product features and solutions. Look for and ask about Blue Coat certifications.

Configuration & Specification Chart

	Model AV510-A
System	
Disk drives	1x80GB SATA
RAM	1GB RAM
Network Interface	(2) integrated (on board) 10/100/1000 Base-T NICs
Operating Environment	
Power	AC power 100-240V, 50-60Hz, 6.3-3.0A
Maximum Power	150 Watts
Thermal Rating	512 BTU/Hr
Temperature	5°C to 35°C (41°F to 95°F)
Humidity	Less than 90% relative humidity, non-condensing
Altitude	Up to 3048m (10,000ft)
Dimensions and Weight	
Enclosure	19" Rack-mountable
Dimensions (L x W x H)	58 cm x 44 cm x 4.4 cm (22.8 in x 17.4 in x 1.7 in)
Weight (maximum)	12.3 kg (27 lb)
Regulations	
Emissions	FCC Class A, EN55022 Class A, VCCI Class A No.1706609, BSMI, CCC, C-tick
Safety	CSA C22.2 No. 950 M95, UL 60950 3rd Edition, EN60950, TUV-GS, TUV-S, CCC, BSMI
Standards	UL/CSA, TUV-S, BSMI, Ctick, CCC, CE
Support Standard warranty	90-day software & phone support with 1-year hardware support; extended and upgraded support plans available