

STOP MALWARE AT THE WEB GATEWAY

Blue Coat® ProxyAV™ appliances offer advanced malware detection at the gateway as part of the Application Delivery Network (ADN), an infrastructure that provides complete application visibility, acceleration and security. By detecting and blocking malware, worms, trojans and spyware, including spyware that targets HTTP, FTP and HTTPS protocols, ProxyAV secures rogue channels that threaten the enterprise network. And ProxyAV integrates with ProxySG® to accelerate AV gateway performance with a scan-once-serve-many-times architecture.

FEATURES

Scalability and Performance

- > ProxySG analyzes Web objects with ProxyAV at wire speed with integrated caching (up to 240 Mbps, 7-9 msec latency).
- > Dual cache intelligence with timestamps optimizes performance for cacheable and non-cacheable objects and never requires an object cache flush.
- > ProxyAV provides four modes of analysis with traditional object analysis, trickle first or last stream analysis, or defer scan.
- > Defer scan is unique to Blue Coat, it keeps long load objects like web radio and other media out of vital processing threads to optimize web gateway performance to detect malware.
- > ProxyAV provides load balancing and clustering of multiple ProxyAV appliances for enterprise scalability resulting in less hardware than all-in-one solutions.
- > ProxyAV can be configured to analyze both inbound and outbound web traffic for malware and web threats.
- > ProxyAV supports malware detection with Kaspersky, McAfee, Panda or Sophos threat detection engines.
- > ProxyAV checks for threat updates every 30mins as a default and can be set as frequently as every 5mins providing the most current protection, often faster than desktop updates.

Ease of Deployment & Administration

- > Purpose-built appliance solutions from a single vendor; designed, tested and manufactured for compatibility.
- > Blue Coat's ProxySG and ProxyAV appliances communicate using an enhanced ICAP+ version enabling superior performance, reliability, and error/exception handling over software-based ICAP servers.
- > Administrators can define default or custom locations for malware detection updates, and configure behavior of ProxyAV upon license expiration.
- > Configurable options for malware analysis include: set time-out duration,

drop file if errors in detection occur, and define trusted sites.

- > Using an M:N ratio of ProxySG to ProxyAV appliances, malware detection load processing can be optimized, plus appliance utilization rates, resulting in a greener solution.
- > Administrators can apply policy for allow/deny lists with extensions along with file size and content type restrictions.
- > Customized alerts can notify administrators when malware is found, threat detection updates are successful, when updates fail, subscriptions expire, files are dropped, or files pass without malware analysis.
- > Log files can be customized using standard logging formats and sent off-box via TCP or UDP for processing.
- > Health checks from ProxySG to ProxyAV verify status and availability of appliances.
- > New firmware updates are sent to ProxyAV for administrator approval and installation.

Layered Security

- > ProxyAV provides malware detection for threat vectors that URL filtering cloud defenses cannot see, such as web mail, file downloads, social networking sites and SSL traffic, all popular ways to distribute malware.
- > ProxyAV is always current on threat defense updates whereas desktops are not, and ProxyAV can provide a malware defense that is different than the desktop defense, providing depth.
- > Combined with WebFilter that is continuously updated by the WebPulse community watch cloud service, these URL and AV layers work together to block malware downloads hidden in popular websites and hidden in file downloads, web mail and social networking.
- > Performance of ProxyAV is optimized with ProxySG using WebFilter to block hidden malware downloads in popular websites, blocking access to objectionable and unproductive sites often associated with malware, plus blocking downloads from unrated sites.

- > ProxyClient provides remote filtering via the WebPulse community watch cloud service to protect laptop users from hidden malware in popular sites, plus enforce acceptable web use policies with central management and reporting. Protection beyond the web gateway.
- > Reporter provides visibility into web threats detected by ProxyAV, WebFilter and the WebPulse community watch, plus ProxySG content controls with a customizable dashboard and detailed reports with drill down features.

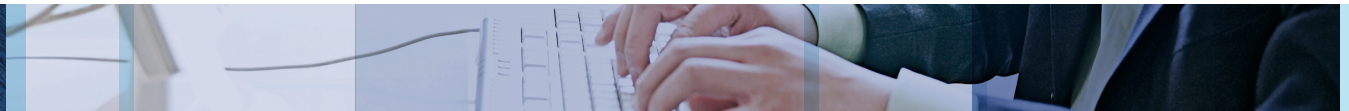
Control Beyond Inline Threat Analysis

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

- > ProxySG supports four simultaneous URL lists allowing customers to utilize WebFilter (and other leading URL lists), the Internet Watch Foundation (IWF) list, plus a custom allow/deny URL list
- > Define custom URL categories plus policy exceptions per user, group, source, destination, time, protocol, or user agent
- > Leverage URL categorization to determine SSL traffic analysis, plus source, destination or other variables
- > Block downloads from unrated sites reducing exposure to malware host downloads
- > Increase malware protection with 5min updates from WebFilter for security categories including phishing and reputation ratings
- > Participate in the WebPulse community watch cloud service by sending unrated requests, joining 54M+ other users in a united defense
- > Extend content filtering with WebFilter's real-time web content rating service plus filtering translation sites, search engine caches, image searches, and proxy avoidance.



Content Security

- > True File Type detection on masquerading files, plus hidden in compressed archives
- > Control MIME types and file extensions
- > Strip and replace active content (e.g. noscript policy)
- > User agent (e.g. browser type) 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 messenger support
- > Method-level control settings for file attachments, voice, and video, plus IM reflection for internal use
- > Keyword searches, plus in band/out-of-band alerts
- > Buddyname mapping to corporate identity

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

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

Layered Defense Solution

Blue Coat provides layered defenses with a community watch cloud service of WebFilter combined with inline threat detection of ProxyAV, plus the web content controls of ProxySG. The majority of malware comes from two vectors, hidden downloads in popular and trusted webs sites, and malware distribution through social networking, P2P and web mail. ProxySG and ProxyAV with WebFilter provide a layered malware defense.

Protection is also extended with ProxyClient to remote users to block hidden malware downloads and enforce web use policies. Visibility is provided by Reporter's dashboard and drill down reports, and multiple appliances are centrally managed by Director.



	210-A	AV510-A	AV810-A	AV810-B
System				
Processors	1 CPU	1 CPU	1 CPU	2 CPU
Disk drives	1x80GB IDE	1x80GB SATA	1x73GB SCSI Ultra 320	1x73GB SCSI Ultra 320
RAM	1GB	1GB	2GB	3GB
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		AC power 100-240V, 50-60Hz, 6.3-3.0A	
Maximum Power	45 Watts		150 Watts	
Thermal Rating	153.63 BTU/Hr		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	Desk/wall mount, rack mountable* (*specific rack mount kit required)		19" Rack-mountable	
Dimensions (L x W x H)	35.6cm x 19.1cm x 4.4cm (14in x 7.5in x 1.72in)		58 cm x 44 cm x 4.4 cm (22.8 in x 17.4 in x 1.7 in)	
Weight (maximum)	2.6kg (5.8lb)		12.3 kg (27 lb) 14.1 kg (31 lb) 14.7 kg (32.5 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				

Blue Coat Systems, Inc.
www.bluecoat.com

Corporate Headquarters
Sunnyvale, CA USA // +1.408.220.2200

EMEA Headquarters
Hampshire, UK // +44.1252.554600

APAC Headquarters
Hong Kong // +852.3476.1000

Copyright © 2008 Blue Coat Systems, Inc. All rights reserved worldwide. No part of this document may be reproduced by any means nor translated to any electronic medium without the written consent of Blue Coat Systems, Inc. Specifications are subject to change without notice. Information contained in this document is believed to be accurate and reliable, however, Blue Coat Systems, Inc. assumes no responsibility for its use. Blue Coat is a registered trademark of Blue Coat Systems, Inc. in the U.S. and worldwide. All other trademarks mentioned in this document are the property of their respective owners. v.DS-PROXYAV-v3-1208