

Blue Coat RA8100



Blue Coat RA delivers an entirely on-demand SSL VPN that provides secure remote access for employees, partners and customers. With integrated endpoint security and information protection features and without ever requiring VPN client software or local Admin rights, Blue Coat RA provides an ideal remote access solution for extending applications and resources to users on unmanaged endpoints that are beyond the reach of IPSec VPNs and traditional SSL VPNs. Built on the industry's only application-independent architecture and utilizing patent-pending on-demand Connector technology, Blue Coat RA provides:

- On-demand access to virtually any TCP or UDP application – from Web to client-server – without the installation of VPN client software and without ever requiring URL rewriting for Web applications
- Extensive support for unmanaged endpoints (e.g. partner desktops and home PCs) without ever requiring local Admin rights and with comprehensive information protection features to prevent leakage and theft of corporate or personal data
- Endpoint security services, such as host integrity checking and automatic malware identification and suppression, to ensure the integrity of the connecting device

While traditional SSL VPNs often require port forwarding and network extender clients to support many Web and client server applications, Blue Coat RA never requires VPN client software or local Admin rights, allowing IT departments to extend secure, controlled access from unmanaged endpoints – such as partner PCs and employee home PCs – where installing client software is not an option. In addition to on demand connectivity, Blue Coat RA delivers the endpoint security services to ensure that access – even from unmanaged devices – and the information are protected.

Blue Coat RA represents the next generation of SSL VPNs that provides a single on demand mode of access for all Web and non-Web applications to extend rich connectivity beyond the managed user to the unmanaged endpoint. Unlike traditional SSL VPNs that are built on application-layer HTTPS reverse proxies, Blue Coat RA leverages a session-layer proxy architecture that never requires URL rewriting and never needs prior knowledge of the application or underlying protocol. Blue Coat RA also provides the comprehensive endpoint security and information protection features that enterprises require as they extend anytime anywhere access to sensitive and confidential corporate and personal information.

On Demand Remote Access

Patent-pending Connector technology delivers next generation SSL VPN that:

- Supports web and non-web applications
- Never requires VPN client software
- Never requires local admin rights

Integrated Endpoint Security

Adaptive Malware Protection technology provides pre-authentication spyware scan and suppresses all suspicious programs and customizable host integrity checking maintains security posture of connecting devices

Information Protection

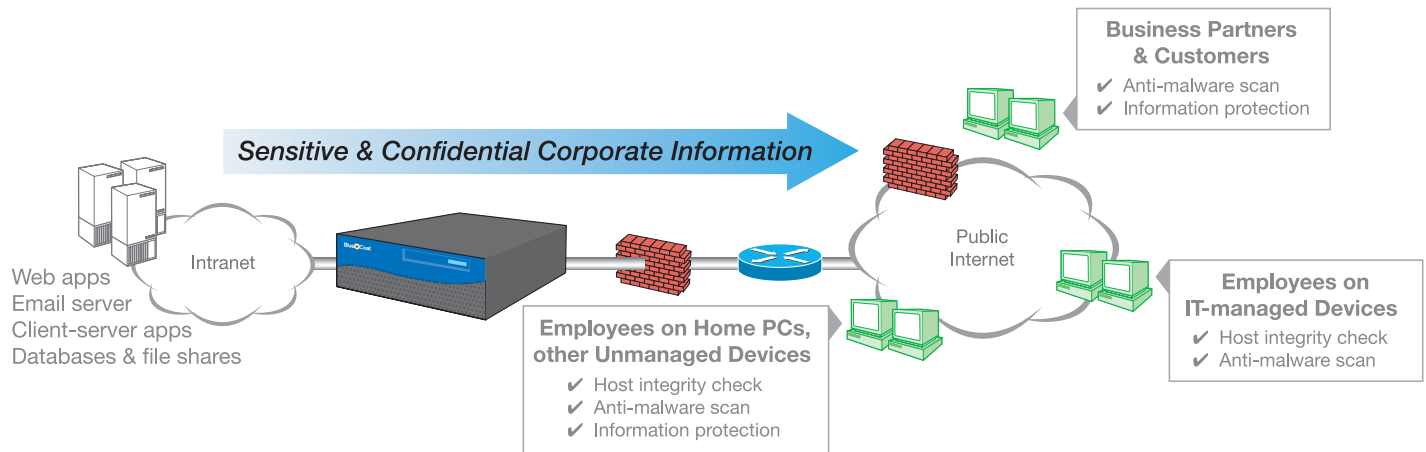
Rich series of endpoint controls and browser security features to prevent malicious data theft and inadvertent information leakage at the endpoint

Granular Application & User Management

Highly flexible and intuitive object-based management console for controlling targeted access to enterprise resources

Scalability and Performance

High performance architecture with automatic load balancing for uninterrupted connectivity



Never requiring local admin rights or leaving behind any client software, Blue Coat RA extends rich connectivity to corporate-owned and unmanaged endpoints with integrated endpoint security controls to prevent the leakage and theft of confidential corporate information.

On Demand Remote Access

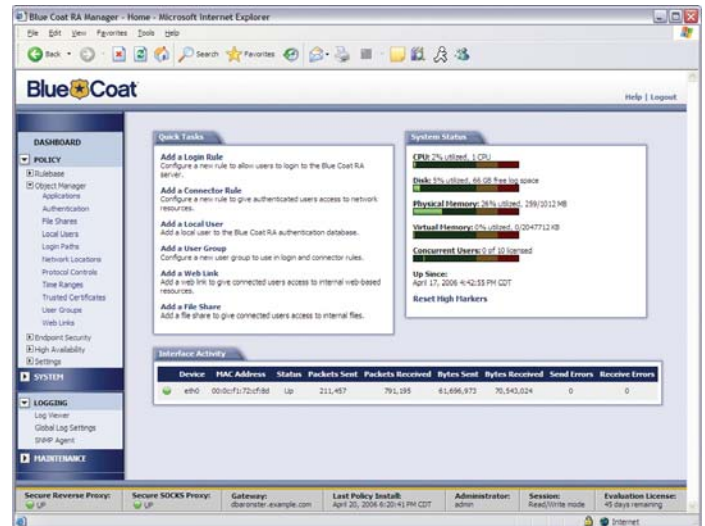
- **Extensive application support** – provides out-of-the-box support for web and non-web TCP and UDP applications without ever requiring VPN client software (see Application Support Guidelines)
- **Comprehensive web application support** – provides uninterrupted access to both simple and advanced and feature-rich web applications (XML, ActiveX, AJAX, Java, etc.) without relying on error-prone URL rewriting
- **Single access mode for all users** – provides access to all supported applications via patent-pending Blue Coat Connector, eliminating the headache of managing multiple access modes for different users
- **Support for locked down environments** – never requires local admin rights on end user devices for accessing web and non-web applications, extending access to both managed and unmanaged endpoints without exception
- **In office user experience** – provides IPSec-like user experience (e.g. launch native applications from desktop)
- **Application-layer access across all applications** – controls access by applications for all supported applications and never requires unrestricted network-layer connectivity
- **No changes to desktop** – leaves desktop as it found it when user session is over (no system alternations or modifications) and no software left behind

Endpoint Security

- **Integrated with SSL VPN** – provides endpoint security for managed and unmanaged devices seamlessly integrated with remote access deployment and management
- **Pre-authentication and continuous spyware scan** – leverages patent-pending AMP (Adaptive Malware Protection) technology to provide a pre-login scan for framgrabbers and keyloggers and continues to scan for duration of user session
- **Automatic spyware suppression** – identifies and temporarily suppresses processes and programs identified as potential threats, such as framgrabbers and keyloggers, for the duration of user session without any permanent system changes
- **On demand host integrity checks** – checks a variety of conditions (such as personal firewall settings, antivirus software updates and OS patches and service packs) on the endpoint to determine the security posture of the device
- **Customizable host checking** – provides tool for defining custom host checks (such as registry settings, processes running/not running and the existence of certain files)
- **Application blacklists and whitelists** – provides application white lists and blacklists to control which applications, through checksum validation, are allowed to be accessed / not accessed by the end user during the remote access session
- **Application-specific access** – allows administrators to limit which applications can reach specific resources to block unauthorized programs from contacting the internal assets
- **Configurable split tunneling** – blocks or enforces split tunneling

Granular Application & User Management

- **Intuitive object-based policy manager** – controls user access to targeted resources through easy-to-administer, object-based access rules
- **Granular user and access control** – defines access by user, target resource, source/location of user, time of day, and security profile of connecting device
- **Policy wizard** – creates access policies in minutes with user-friendly wizard
- **Extensive authentication support** – integrates with leading authentication schemes, such as Microsoft Active Directory, LDAP/LDAPS, RADIUS, RSA SecurID®, and TACACS+
- **Custom groups** – supports custom groups using existing directory groups or user attributes for targeted access to specific resources
- **Flexible tiered access controls** – allows minimum security thresholds, such as requisite OS patches, AV updates or personal firewalls settings, when accessing specific applications and other resources
- **Activity logs with flexible search tool** – logs all activity by user and application and provides intuitive search tool for locating specific records
- **System dashboard** – provides overview of system health (e.g. CPU usage and disk utilization), concurrent users logged on and overall system status
- **Customizable login page** – allows IT administrators to customize the user login page to integrate with corporate colors, branding and messaging



Blue Coat RA management console for intuitive object-based policy and user administration.

Information Protection

- **Integrated with SSL VPN** – provides information protection for managed and unmanaged devices seamlessly integrated with remote access deployment and management
- **Browser security** – encrypts all information stored by the browser, including cache, temp files and cookies, and clears all session information at the end of SSL VPN session using DoD 5220.22-spec file deletion
- **Information usage controls** – controls what users can do with the information accessed and downloaded by web applications, such as blocking or allowing file save, print, save to clipboard, cut-and-paste, and screen print operations
- **Framegrabber and keylogger protection** – scans for and suppresses keyloggers and framegrabbers to prevent spyware from stealing personal and corporate information

Scalability and Performance

- **Flexible user configuration** – support 500, 1000, 2500 or 5000 concurrent users
- **High availability** – transparent, automatic failover for uninterrupted connectivity
- **Load balancing** – supports external load balancers to satisfy performance-critical applications
- **High performance architecture** – easily supports LAN speeds

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 Blue Coat trainers enabling administrators to become fully proficient on all aspects of the Blue Coat 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 of the Blue Coat RA. 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 on Blue Coat appliances to provide field services. Our partners attend Instructor-led courses as well as monthly online training on the latest Blue Coat features and solutions. Look for and ask about Blue Coat certifications.

Configuration & Specification Chart

| | Model 8100-A |
|---------------------------------------|--|
| System | |
| Disk drives | 2x73GB SCSI Ultra 320 |
| RAM | 2GB RAM |
| Network Interfaces | Optional 2x10/100/1000 Base-T card or 4x10/100/1000 Base-T card or 4x10/100/1000 Base-SX (quad GigE fibre) card |
| Operating Environment | |
| Power | AC power 100-240V, 50-60Hz, 65 watts, 6.3-3.0A |
| Maximum Power | 525 Watts |
| WattsThermal Rating | 1792 BTU/Hr |
| Temperature | 5°C to 35°C (41°F to 95°F) |
| Humidity | Less than 90% relative humidity, non-condensing |
| Altitude | Up to 3048 M (10,000 ft) |
| Dimensions and Weight | |
| Enclosure | 19" Rack-mountable |
| Dimensions (L x W x H) | 23.3inch(L) X 17.4inch(W) X 6.95inch (H) or 592mm (L) X 442mm (W) X 176.52mm (H) |
| Weight (maximum) | 24.8 kg (54.5 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 | 90-day software & phone support with 1-year hardware support; extended and upgraded support plans available |
| Protocols and Applications | SSL VPN supports ICMP and virtually any TCP or UDP application. Partial list of tested applications and protocols include: HTTP; FTP; SMTP; RDP; VoIP; H.323; SIP; RTP/RTSP; Citrix ICA Client®; IIOIP; Microsoft Outlook (Exchange, IMAP, or POP); PCanywhere®; Yahoo Messenger®, AOL Instant Messenger®, MSN Messenger Service®, Open Bloomberg® |
| Connectivity and NAT | DNS Proxying ; Network Address Translation (NAT); Firewall and Proxy traversal; Multiple Server Chaining |
| Performance and Reliability | High Availability; Support for External Load Balancers; Symmetric Multiprocessor Support; Intel Hyperthreading Support |
| Administration Tools | Web-based Management Console; Real-time status and monitoring; Role-based administration |
| Auditing and Logging | Session, connection, failed connection logging; Administrative auditing; Endpoint Security event logging; Syslog support; Log file rotation and automated archiving; redundant logging; off-gateway audit trail |
| VPN Access Control Criteria | IP Address (Source and Destination); DNS Domain Name; Application/Port; User; Group; Time; Host Integrity Status |
| Encryption Standards | AES with 256-bit key and SHA MAC; RC4 with 128-bit key and MD5 MAC; DES with 56-bit key and SHA MAC; 3DES with 168-bit key and SHA MAC |
| Authentication Mechanisms | Internal Username & Password (RFC1929); Microsoft Active Directory; LDAP/LDAPS; RADIUS; RSA SecurID®; TACACS+ |
| Application Support Guidelines | RA supports any TCP or UDP application where (a) client initiates communication (b) application is running in user's environment (c) application uses standard Winsock API and (d) application does not access internal file shares. Also, application client must be launched after Connector has loaded. |
| Connector Support | Microsoft Windows 2000® SP4 Microsoft Windows XP® (SP1 & SP2) Internet Explorer 6 (ActiveX or Java enabled) |



Blue Coat Systems, Inc. 1.866.30.BCOAT • 408.220.2200 Direct • 408.220.2250 Fax • www.bluecoat.com

Copyright © 2007 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.DSRA8100v1.0407