



ProxyRA is an on demand SSL VPN that provides secure remote access for employees, partners and customers. With integrated endpoint security and information protection features and no VPN client software or local Admin rights required, ProxyRA 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. Proxy RA is the industry's only application-independent architecture and utilizes patent-pending on demand Connector technology.

FEATURES

On Demand Remote Access

Extensive application support

- > Provides out-of-the-box support for web and non-web TCP and UDP applications

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 on demand access to packaged and custom client-server and Web applications through unique on demand connectivity agent

Support for locked down environments

- > Never requires local Admin rights on end user machines (including Macs and PCs with Microsoft Vista's advanced security model)

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

- > Uses patent-pending technology to perform a pre-login behavioral scan for keyloggers and framgrabbers and continuously scans for spyware for duration of user's 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

Customizable host checking

- > Granular policy-based access—restricts access to internal resources based on endpoint security status

Client application validation

- > Provides application white lists and blacklists to control which applications, through checksum validation, are allowed

Application-specific acces

- > 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

Information Protection

Integrated with SSL VPN

- > Provides information protection for managed and unmanaged devices seamlessly integrated with remote access

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 framgrabbers to prevent spyware from stealing personal and corporate information

Scalability and Performance

Flexible user configuration

- > Support 25 to 5,000 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



RA510 SERIES		RA510-A	Physical Properties	
System				
Disk drives	1x80GB IDE		Dimensions and Weight	
RAM	512MB		Enclosure	19" Rack-mountable
Network Interfaces	(2) integrated (on board) 10/100Base-T NICs with passthrough		Dimensions (L x W x H)	58cm x 44cm x 4.4cm (22.8in x 17.4in x 2.7in)
Optional Cards	2x10/100/1000Base-T card 2x10/100/1000Base-SX (dual gigE Fibre) card		Weight (maximum)	14.1 kg (31 lb)
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 3048 M (10,000 ft)		

RA810 SERIES		RA810-A	RA810-B	Physical Properties	
System					
Disk drives	73GB SCSI	2x73GB SCSI RAID		Dimensions and Weight	
RAM	2GB	3GB		Enclosure	19" Rack-mountable
Network Interfaces	(2) integrated (on board) 10/100/1000 Base-T NICs			Dimensions (L x W x H)	58cm x 44cm x 4.4cm (22.8in x 17.4in x 1.7in)
Optional Cards	2x10/100/1000Base-T card 4x10/100/1000Base-T card 2x10/100/1000Base-SX card (dual GigE Fibre)			Weight (maximum)	14.1kg(31lb) 14.7kg(32.5lb)
Operating Environment					
Power		AC power 100-240V, 50-60Hz, 6.3-3.0A			
Maximum Power		375 Watts			
Thermal Rating		1280.25 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)			

RA8100 SERIES		RA8100-A	Physical Properties		
System					
Disk drives	2x73GB SCSI RAID		Dimensions and Weight		
RAM	4GB RAM		Enclosure	19" Rack-mountable	
Network Interfaces	(2) integrated (on board) 10/100/1000 Base-T NICs			Dimensions (L x W x H)	59.2cm X 44.2cm X 17.652cm (23.3in X 17.4in X 6.95in)
Optional Cards	2x10/100/1000Base-T card (dual GigE) 4x10/100/1000Base-T card (quad GigE) 4x10/100/1000Base-SX card (quad GigE Fibre)			Weight (maximum)	24.8kg(54.5lb)
Operating Environment					
Power		AC power 100-240V, 50-60Hz, 65 watts, 6.3-3.0A			
Maximum Power		525 Watts			
Thermal 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 3048m (10,000ft)			

FOR ALL RA SERIES	
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, C-tick, CCC, CE
Support Standard Warranty	90-day software & phone support with 1-year hardware support; extended and upgraded support plans available
End User Language	English, Traditional and Simplified Chinese, Japanese, and Korean
Protocols & 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®; ILOP; 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
Performance and Reliability	High Availability; Support for External Load Balancers; Single-, dual-, and quad-CPU models for high performance
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; 3DES with 168-bit key and SHA MAC
Authentication Mechanisms	Internal Username & Password (RFC1929); Microsoft Active Directory; LDAP/LDAPS; RADIUS; RSA SecurID®; TACACS+
Connector Support	Microsoft Windows 2000 SP4+, Microsoft Windows XP SP1+, Microsoft Windows Vista, Internet Explorer 6 & 7; Apple Mac OS X 10.4+, Safari 2.0.4+


 Your Blue Coat Reseller
www.altaware.com sales@altaware.com (866) 833-4070

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.DS-RA-v2- 1007