

DELIVER ON-DEMAND APPLICATION SECURITY AND CONNECTIVITY

As part of the Application Delivery Network (ADN), Blue Coat® ProxyRA™ provides on-demand SSL VPN to secure remote access for employees, partners and customers. ProxyRA appliances offer the ADN an ideal remote access solution for extending applications and resources to users on unmanaged endpoints who are beyond the reach of IPSec and traditional SSL VPNs. ProxyRA offers an application-independent architecture to simplify and secure remote access from wherever users are located without the need of client software.

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

