

The Barracuda SSL VPN Advantage

Comprehensive Secure Remote Access Solution

The Barracuda SSL VPN is an integrated hardware and software solution that enables secure, clientless, remote access to internal network resources. Accessible from any Web browser on any operating system, the Barracuda SSL VPN provides all the features needed to enable network resource access through a powerful policy-based permissions framework. The Barracuda SSL VPN also integrates with third-party authentication mechanisms to provide granular access control with single sign-on capabilities.

Value Proposition

Powerful Remote Access

- Intranet Web sites
- Network file shares
- Remote desktop, VNC, Citrix
- Other client/server applications

Secure

- SSL encryption-built into modern browsers
- Anti-virus scanning of uploaded files
- Granular access policy
- Client access controls
- Cache cleaning
- LDAP, RADIUS and multifactor authentication

Easy-to-Use

- Works with any Java-enabled Web browser
- End user portal to display available resources
- Single-sign-on to Web RDP and other applications
- Installable client for use with legacy applications

Affordable

- Single appliance will fully integrated functionality
- Appliance and subscriptions cost less than renewals of competing products
- No per user or per connection fees

Key Features

- Clientless remote access
- Integration with Active Directory, LDAP, NIS and built-in user databases
- Policy-based rights management
- Multifactor authentication schemes
- Built-in applications
- Virtual keyboard and cache cleaning
- Site-to-site connectivity
- Auditing and reporting
- Network access control

Feature Insights

Clientless Remote Access

Unlike traditional IPsec based VPNs that require client software installed on remote machines, the Barracuda SSL VPN provides secure remote access to network resources from any Web browser. This removes the overhead of installing and maintaining clients and permits secure access from any operating system that can support a standard Web browser.

SSL technology also eliminates some of the deployment issues around IPsec VPN technology like IP address conflicts, NAT traversal and DNS problems.

Policy-Based Resource Management

The Barracuda SSL VPN integrates a powerful policy engine that enables administrators to selectively authorize traffic to approved resources. The device integrates with Active Directory, LDAP or other user -databases permitting administrators to define granular policies allowing specific users and groups to access network resources without any changes to the resource itself.

Through the policy engine, administrators can configure access to resources such as Intranet Web sites, mapped network drives, applications like RDP, SSH/SFTP, CITRIX XenApp and others.

Multi-Factor Authentication

To increase network security remote users are required to properly identify themselves before obtaining access to the network. The Barracuda SSL VPN can be configured to enforce a combination of authentication schemes including Active Directory passwords, hardware tokens, client certificates, and PIN numbers. Moreover, The Barracuda SSL VPN supports RSA SecurID, VASCO, Safeword and CryptoCard authentication servers through RADIUS integration for access using a one-time password token. This security ensures that accessing the SSL VPN from any Web browser is backed by the protection of a strong authentication policy that allows only authorized users to enter the network.

Network Access Control

Remote users can access network resources from a variety of end-points or client machines including shared computers. The Barracuda SSL VPN provides extensive network access control methods that will ensure a computer requesting remote access adheres to established security policies based on the operating system, Web browser version and other connection parameters before permitting network access.

Secure Client Access

All files uploaded during a Barracuda SSL VPN session to the network file system or from a proxied Internet Web application are automatically scanned for viruses, spyware and other forms of malware.

The Barracuda SSL VPN also includes a cache cleaning utility that clears traces of a secure session from the Web browser cache, history and a virtual keyboard to protect users against keyloggers. This is especially useful when users access the Barracuda SSL VPN from shared computers.

Barracuda Network Connector

An additional resource that can be accessed over the SSL connection is the Barracuda Network Connector, which is an optional client that provides access to applications using UDP or other legacy client/server applications. The Barracuda Network connector provides enables a fully routed VPN connection to the network from a remote client and can be utilized by remote users that need complete network access.

For questions about the Barracuda SSL VPN, please visit <http://www.barracuda.com/sslvpn> or call Barracuda Networks for a free 30-day evaluation at 1-888-ANTI-SPAM or +1 408-342-5400. For more information on our other security and productivity solutions, please visit <http://www.barracuda.com/products>.

About Barracuda Networks Inc.

Barracuda Networks Inc. combines premises-based gateways and software, virtual appliances, cloud services, and sophisticated remote support to deliver comprehensive content security, data protection and application delivery solutions. The company's expansive product portfolio includes offerings for protection against email, Web and IM threats as well as products that improve application delivery and network access, message archiving, backup and data protection.

Coca-Cola, FedEx, Harvard University, IBM, L'Oreal, and Europcar are among the more than 100,000 organizations protecting their IT infrastructures with Barracuda Networks' range of affordable, easy-to-deploy and manage solutions. Barracuda Networks is privately held with its International headquarters in Campbell, Calif.