

Menlo Logic AccessPoint SSL VPN





An Introduction to SSL VPN

The Secure Sockets Layer (SSL) protocol provides flexible and secure remote access over the Internet, enabling mobile users, business partners and customers to easily access network resources from anywhere in the world. So it is not surprising that SSL-based VPNs (Virtual Private Networks) are expected to be "the dominant method for remote access, with 80% of users utilizing SSL," according to the advisory firm, META Group. San Jose research firm Infonetix predicts that the SSL VPN market will grow to almost \$1 billion USD by 2005.

What is fueling this extraordinary growth? This growth is driven by the limitations of traditional remote access products and by the evolving demands of employees and customers. Because SSL operates on top of TCP/IP, SSL VPN supports many different types of connections, including web, Java or ActiveX thin client, and full client connectivity to private network resources. So it provides remote access to PCs running Windows, MacOS, Linux, and Solaris. Even PDAs and Smart phones can securely connect to the corporate network through a web browser.

In addition, SSL VPN offers simplified deployment; users connecting to desktop machines, intranet web sites, email, and FTP do not need to download, install and configure complicated VPN client software. By logging into a secure web portal, users can click on personal bookmarks that open frequently accessed files and applications, such as their home directory on a file server, their desktop

machine, or an Intranet web site. Users do not need to remember hostnames or IP addresses or install pcAnywhere client software to access machines through a VPN tunnel.

SSL VPN Benefits

- **End-to-End Encryption** – Sensitive data is encrypted from the SSL VPN gateway to the client machine; if the back end server supports SSL, then data can be encrypted from the client machine all the way to the server. Traditional site-to-site VPN tunnels only encrypt data sent over the Internet; communications from network PCs to the VPN gateway are not encrypted.
- **Single Sign On Authentication** – Most SSL VPN products support Single Sign On authentication, meaning that once a user has logged into the SSL VPN portal, his user information will be cached and he will not need to re-authenticate to access his computer, shared files, or other resources. SSL VPN gateways can authenticate users via Radius, Active Directory, LDAP and NT Domain and other standard types of authentication.
- **Unfiltered VPN Access** – Occasionally, Internet access provided at locations such as hotels, airports and wireless hot spots will block all traffic except for standard TCP and UDP services. IPsec VPN uses its own transmission protocol for communications, not a standard TCP or UDP service. So business travelers may not be able to connect to their corporate network using IPsec VPN if this type of traffic is filtered.



SSL VPN uses standard TCP port 443 for communications, ensuring full remote access from any location.

- **Fine Grain Access Control and Logging** – SSL VPN gateways can not only deny and permit access based on port number, IP address or user, they can also control access to individual files, applications and web URLs. SSL VPN gateways can also log all transactions, enabling administrators to monitor unusual or suspicious activity.
- **Easier Deployment and Use** – SSL VPN gateways avoid the need to install and configure client software because services are provided through a standard web browser. SSL VPN also enables users to securely access their corporate network from a shared machine, such as a friend's home PC, without needing to install and then uninstall VPN software. Users that require full, unrestricted access to the network, similar to an IPSec VPN tunnel, can download an SSL VPN client from the SSL VPN portal. The SSL VPN client will usually include the configuration settings required to access the corporate network, avoiding manual VPN configuration. The SSL VPN portal provides a secure, streamlined way to deploy VPN client software.
- **Wider Interoperability** – Because almost all Internet-enabled devices include a web browser, SSL VPN is broadly supported on most platforms and devices.¹ Administrators no longer need to contend

with buggy VPN software to enable Linux, Mac, or other clients to access network resources.

- **Protected Extranet Sites** – Increasingly, enterprises need a secure way to allow business partners and customers to access CRM applications, accounting information or shared resources. For these requirements, SSL VPN provides the ideal solution, enabling customers or business partners to log into an extranet portal that shares the same look and feel as the external web site. The SSL VPN portal not only encrypts data over the Internet, it also supports authentication to an existing authentication server, logging of user activity, and fine grain control of network access by user.

The AccessPoint Solution

Menlo Logic has developed the AccessPoint SSL VPN product line to meet the needs of both enterprises and security appliance vendors. The AccessPoint Enterprise Suite provides a comprehensive SSL VPN solution at an affordable price—making SSL VPN technology available to small and medium size businesses. The AccessPoint Enterprise Suite is a software package that includes a hardened operating system, firewall, and intrusion detection in addition to SSL VPN remote access. It also includes an intuitive web management interface for easy configuration and management.

AccessPoint Features

- **SSL VPN Portal** – Web based access to FTP, network file sharing, Intranet web

¹ Note that full network access provided by SSL VPN client software will have operating system limitations similar to IPSec VPN software.



and HTTPS sites, desktop and desktop applications, and Telnet and SSH terminal access.

- **TCP Tunneling for Email** – Client software such as Microsoft Outlook, Outlook Express, Netscape Mail, Eudora and Lotus Notes can securely connect to mail and directory servers using TCP tunneling.
- **SSL VPN Client** – For complete network access, the AccessPoint solution includes SSL VPN client software for Windows 2000/XP. The SSL VPN client may be downloaded from the SSL VPN portal and requires no end user configuration.
- **Logging and Reporting** – The AccessPoint Enterprise Suite includes detailed logging, monitoring and reporting utilities.
- **Authentication** – In addition to internal database authentication, AccessPoint supports Radius, XAUTH, NT Domain, Active Directory and LDAP authentication.
- **Powerful Access Control Policies** – Administrators can define access control policies for SSL VPN users and groups based on the SSL VPN service and the name, IP address or address range of the system being accessed.

- **Integrated Firewall and Intrusion Detection** – The AccessPoint Enterprise Suite includes an enterprise-class firewall with flexible rule policies and DoS attack protection. In addition, it includes an Intrusion Detection System (IDS), providing intelligent detection and reporting of irregular SSL and network activity.
- **Intuitive Web Management Interface** – AccessPoint's clear, simple management interface helps ensure greater security because administrators can comfortably use and configure network access policies and understand log events.

Menlo Logic also provides source code and binary software for OEM vendors. The AccessPoint Source Code Toolkit provides security vendors with everything they need to bring a comprehensive SSL VPN product to market. Security vendors can customize and extend the AccessPoint SSL VPN software or they can simply add the SSL VPN application as is to their hardware platform. The AccessPoint SSL VPN solution has been architected to provide maximum performance using a small memory footprint.



Menlo Logic, LLC
488 University Ave., Suite 212
Palo Alto, CA 94301
Phone: (650) 922-6500
www.menlologic.com

© 2004 Menlo Logic, LLC. All rights reserved.
All trademarks and tradenames mentioned are
the property of their respective owners.

Part No. MLB-042-0010