AccessPoint SSL VPN Toolkit

SSL VPN Source Code Solution for OEMs

The AccessPoint SSL VPN Toolkit provides the source code software you need to build an advanced SSL VPN appliance or add SSL VPN capabilities to your current security or networking devices. The AccessPoint SSL VPN Toolkit offers:

- Accelerated time to market and reduced development costs
- A turnkey, comprehensive SSL VPN implementation
- Support and integration assistance from SSL VPN experts

Custom Designed for OEM Vendors

The AccessPoint SSL VPN Toolkit is the industry's first SSL VPN solution developed expressly for equipment vendors and system integrators. It is designed to streamline the development time and meet the performance and memory footprint constraints of today's leading network equipment manufacturers. AccessPoint provides the best SSL VPN solution to meet OEM customers' development requirements.

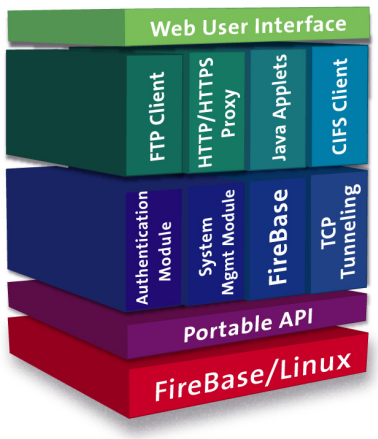
The AccessPoint SSL VPN Toolkit provides an end-to-end software solution for dedicated, high-performance SSL VPN appliances or low-cost, embedded networking devices. In addition, AccessPoint SSL VPN software can be added to firewalls, IPSec VPN devices, web application gateways, load balancers, and access routers.

Product Features

The AccessPoint SSL VPN Toolkit consists of different packages customized to our customers' unique requirements. The four primary packages that provide web and Java-based SSL VPN access are bundled together to form the AccessPoint SSL VPN Standard Package. The AccessPoint software is written in pure ANSI C, Java and Perl and is POSIX complaint.

The AccessPoint SSL VPN Toolkit provides:

- **Remote Desktop Access –** AccessPoint provides access to remote desktops and applications. AccessPoint supports Terminal Services for Windows XP Professional, 2000 Server and 2003 Server and Virtual Network Computing (VNC) for remote desktop access. Terminal Services allow users to access the entire desktop or individual desktop applications.
- **HTTP and HTTPS Proxy** – AccessPoint SSL VPN portal includes an HTTP and HTTPS reverse-map URL proxy. With AccessPoint, end users can remotely access Intranet web servers and HTTPS servers located on the corporate network through a standard web browser. The proxy supports HTML, complex JavaScript, VBScript, and HTTP basic and digest authentication.
- **FTP and Windows Network File Sharing –** FTP and network file sharing enable end users to upload and download files located on corporate FTP servers and file servers. The SSL VPN portal provides clientless DHTML access to FTP and CIFS (Common Internet File System), allowing files to be transferred from a standard web browser.



AccessPoint Architecture Diagram

Features at a Glance

- **Security –** x.509 Digital certificate and up to 128-bit encryption (1024-bit public key encryption)*, encrypted session-based cookies, non-cached web pages, ActiveX web cache control, granular SSL VPN access policies and SSL VPN logging and auditing support.
- **Full Application Support -** AccessPoint offers a full range of SSL VPN clientless and thin client packages for network, application and desktop access.

* Encryption key length will vary due to export regulations

Benefits for OEM Vendors

- **Portability –** Platform-independent design is portable to embedded and proprietary operating systems
- **High Performance –** Compact design ensures high performance and low memory requirements
- **Manageability –** AccessPoint includes an intuitive and customizable web user interface and online help that accelerate OEM vendors' time to market.

- **Terminal Access** – The AccessPoint SSL VPN Toolkit provides Java thin client access to Telnet and SSH servers, allowing remote users to access network computers from the SSL VPN portal.
- **AAA Authentication** – AccessPoint supports Radius, LDAP, Microsoft Active Directory and NT Domain authentication. Thoroughly tested with the most popular authentication server vendors.
- **TCP Tunneling** - TCP Tunneling enables mobile users with client software such as Microsoft Outlook, Outlook Express, Lotus Notes, and Netscape Mail to securely access corporate servers. Native client access is transparent, regardless of whether users are on the local LAN or outside of the network.

  Virtual Passage SSL VPN Client – Regardless of the number of applications that are supported by the SSL VPN portal, some users will always require complete network access. Virtual Passage allows Windows and Apple Mac users to connect to a remote network by launching an ActiveX control from the SSL VPN portal.

Specifications and Features

- **Secure Socket Layer (SSL) encryption**
- **Logging and monitoring –** Syslog logging of SSL VPN events by user, service and type of event.
- **Single sign-on (SSO) –** The AccessPoint device caches the user credentials and applies these credentials when accessing private network resources. Single sign-on information is stored on the AccessPoint SSL VPN gateway, not the client machine.
- **Web cache cleaner –** ActiveX program that transparently deletes web files, cookies and history.
- **Encrypted cookies –** both session-based and persistent cookies encrypted.
- **Role based management**
- **Authentication –** Radius, LDAP, Active Directory, NT Domain, and internal user database authentication.
- **Fine Grained Access Policy Management –** Permit and deny policies by SSL VPN service type, user, and IP/IP address range of internal servers.
- **Group and Global Bookmark Support –** Enables users to access desktops or servers without needing to remember hostnames or IP addresses.

SSL VPN Application Support

- **Remote Desktop Management Protocols:** Windows Terminal Services and Virtual Network Computing
- **Web Protocols:** HTML, Java, HTTP/HTTPS
- **File Sharing Protocols:** Windows CIFS
- **File Transfer Protocols:** FTP
- **Native Client Applications:** Microsoft Outlook, Outlook Express, Netscape Mail, IBM Lotus Notes (supports standard SSL clients for any protocols, including SMTP, POP3 and IMAP)
- **Terminal Emulation Protocols:** Telnet and SSH
- **All IP protocols via the Virtual Passage SSL VPN Client**

Protocols Implemented

- HTTP Over TLS – RFC 2818
- The TLS Protocol Version 1.0 – RFC 2246
- Transport Layer Security (TLS) Extensions – RFC 3546
- Lightweight Directory Access Protocol v3 – RFC 3377
- Remote Access Dial In User Service (RADIUS) – RFC 2865
- Kerberos Network Authentication Service – RFC 1510
- File Transfer Protocol – RFC 959
- Telnet Protocol Specification – RFC 854
- SSH Protocol Architecture – IETF Internet-Draft
- ISO Transport Protocol ISO 8073 – RFC 905
- ISO Transport Service on top of TCP – RFC 2126
- Simple Authentication & Security Layer - RFC 2222
- SASL GSSAPI Mechanisms – IETF Internet Draft
- Using TLS with IMAP, POP3 and ACAP - RFC 2595
- SMTP Service Extension for Secure SMTP over TLS – RFC 2487
- The BSD Syslog Protocol - RFC 3164
- CIFS - Microsoft Common Internet File Sharing standard for Microsoft Windows; extension to SMBv2.0

System Requirements

- Operating System – Linux, Solaris, BSD
- Web Server – Apache
- SSL Encryption Library – OpenSSL version 0.96
- Compiler - GCC with GLibc or uClibc tool chain
- Memory – Requirement varies depending upon compiler used; 3MB footprint if compiled with uClibc library.

Menlo Logic

Menlo Logic LLC
488 University Ave Suite 212
Palo Alto, CA 94301
Phone: 650-922-6500 Fax: 650-649-1953