2 of 2 DOCUMENTS

InfoWorld

June 23, 1997

SECTION: NETWORKING: Product Reviews; Pg. 64d

LENGTH: 1067 words

HEADLINE: Aventail delivers highly secure, flexible VPN solution

BYLINE: By Lai-Han Szeto

BODY:
For secure remote-access needs, Aventail's MobileVPN 2.0 and AutoSocks 2.1 comprise a virtual private network (VPN) software solution that lets you monitor and maintain access to your central site via application-level proxies.

Most VPN products, such as Microsoft's Steelhead technology, Digital's AltaVista Tunnel, and Data Fellow's F-Secure, do not address security issues beyond initial log-ins, tending to be server-centric. Aventail has engineered a solution that is user-centric, taking a more in-depth approach to VPN implementation.

Boasting nearly unmatched interoperability with other security protocols, MobileVPN and AutoSocks succeed as a VPN solution, but not without drawbacks: Unidirectional data flow prohibits broadcasting and remote administration, and the system requires third-party products for specific IP-layer features, such as IPX encapsulation.

High level of security

Aventail has developed its own connectivity protocol, Socks 5, which represents the next step in the evolution of the well-known Socks 4 protocol. The addition of security protocols makes Socks 5 a viable VPN tool and a contender to Microsoft's Point to Point Tunneling Protocol (PPTP). Aventail implements the Socks 5 protocol in the Aventail Server, the engine of its VPN package. Socks 5 is based on directed architecture, as opposed to the tunneled architecture one usually associates with VPN technology.

The server establishes a unidirectional connection with a remote client (AutoSocks) or second host site. A secured user can read, write, and execute to the host Server site according to the user's permission profile, but the host cannot likewise carry out transactions on the user's machine. This

setup prevents an intruder from accessing both sites.

Unlike IP-based protocols such as IP Security Architecture (IPSec), a tunneling protocol currently in the draft stage, Socks 5 compels a user to pass permission requirements once that user passes the system perimeter. Once users traverse firewalls, Socks 5 limits access to specific parts of your host system. The system locks out users from directories and applications according to their permission profile.

Socks 5 performs encryption and authentication at the session layer (Layer 5) of the IP packet, enabling an interoperability unmatched by most of Aventail's competitors.

Aventail products support Challenge Handshake Authentication Protocol, Secure Sockets Layer, and Remote Access Dial-In User Service authentication. In addition, Aventail deploys an open architecture to further enhance the flexibility of its products. Key management is compliant with Public Key Cryptography Standards. Encryption is DES and triple-DES enabled. Recently, Aventail announced Socks 5 capability with the IPSec, PPTP, and Layer 2 Tunneling Protocol security protocols.

Outside authority

MobileVPN represents an achievement in usability. I ran my VPN server on Windows NT 4.0 and used a Windows 95 client unit running AutoSocks.

MobileVPN carries handy administrative tools such as Proxy Chaining and Credential Caching, as well as myriad conventional utilities for alias tables, filtering, and session parameters.

AutoSocks acts as the remote-access agent that intercepts application requests between the client application itself and the WinSock interface. It offers logging and configuration GUIs that resemble a miniature version of MobileVPN, minus the high-level host controls.

I installed both pieces with minimal hassle, minus a certificate authority component. Aventail has no plans to become a certificate authority vendor, leaving the task to third parties, such as VeriSign. Unfortunately, this extra service can cost from $290 to as much as $2,000 per year per server.

Add this to Aventail's tiered licensing scheme, and the bottom line becomes a little steeper than that of most conventional VPN solutions. Whether it is worth the cost depends on the complexity of your security policies.

Fluctuating protocols

Implementing VPNs is not for the faint of heart or pocketbook. Tunneling protocols are maturing even as I write. The key to maintaining a foothold in the market is flexibility. In general, developers are building modular products in anticipation of the Internet Engineering Task Force's final draft of IPSec. It is hard to say what will become of Socks 5 (or Socks 6), but for now it has found a little-explored niche in secured connectivity.

Although MobileVPN and AutoSocks lack bidirectional communication and IP-layer features, their open architecture makes them compatible with multiple standards and provides a high level of security.

Lai-Han Szeto (laihan_szeto@infoworld.com) is a contract analyst at the InfoWorld Test Center.

THE BOTTOM LINE: EXCELLENT

MobileVPN 2.0 and AutoSocks 2.1

This virtual private network (VPN) software combination offers a secure and easy-to-manage remote-access solution.

Pros: Excellent proxy-level management; flexible architecture that complements other VPN and security products.

Cons: Third-party products required for specific IP-layer features such as IPX encapsulation; no broadcasting or remote administration.

Aventail Corp., Seattle; (888) 762-5785 (toll-free), (206) 777-5600; fax: (206) 777-5656; http://www.aventail.com.

Price: $4,999 per server for fewer than 25 connections; $66 per client seat for fewer than 25 seats. (Tiered pricing available.)

Platforms: MobileVPN: Unix, Windows NT; AutoSocks: Unix, Windows 3.x, Windows 95, Windows NT.

LOAD-DATE: June 23, 1997