

SECURITY

WWW.INFOSECURITYMAG.COM

Products

PRODUCTS & SERVICES TO SECURE YOUR ENTERPRISE



SSL VPN

FirePass 4100 Series

F5 Networks, www.f5.com

Price: Starts at \$24,990

The FirePass 4100 Series SSL VPN provides broad, browser-based application access across a variety of platforms.

F5 Networks' FirePass 4100 Series SSL VPN is a true integrated enterprise access solution, delivering the broad remote access capabilities of an IPSec VPN through a Web browser interface, plus robust endpoint security features.

IPSec VPNs offer full site connection, while SSL VPNs provide secure remote access to applications. However, SSL VPNs don't necessarily provide out-of-the-box support, requiring customization work upfront. FirePass goes a long way toward solving this dilemma.

FirePass covers most client platforms—Linux, Mac OS, Pocket PC and Windows—giving remote users a secure connection from outside the corporate firewall to inside enterprise applications using any Internet-connected device with most browsers, including WAP browsers and iMode phones. Once authenticated, users

have access to applications such as e-mail, intranet, internal Web servers, client-based applications and file servers. Users can securely access Windows WorkGroup shares, SMB, Novell and NFS services on Unix servers. Access to specific internal resources can be granted on an individual or group basis.

Exec Summary

↑	Extensive application/resource access
↑	Strong endpoint security
↑	Easy setup and management

FirePass eases access with Web site aggregation; instead of listing multiple secure Web sites, its portal page provides a single point of access. It acts as a proxy for internal FTP sites, providing an HTTP front end so users can log in without exposing credentials in the clear.

Through an innovative ActiveX control architecture, F5 designed FirePass with encryption capabilities using RC4, TripleDES and AES algorithms. It uses GZIP to compress traffic before encryption and SSL acceleration to improve performance.

F5 offers the strong endpoint security found in many stand-alone products. An ActiveX control can be enabled to inspect endpoint devices for policy compliance, such as enabled AV, an operational personal firewall, current OS patches and registry settings. Noncompliant devices can be quarantined until compliance issues have been addressed. FirePass uses a Java applet to provide browsers that don't support ActiveX with full functionality and protocol support.

Users log in through a portal page with an on-screen keyboard, effectively defeating key-stroke loggers with a click of the mouse. To further secure access from untrusted machines, the FirePass appliance caches cookies from internal sites, so no residual information remains on the computer if a user forgets to log out.

FirePass also includes a firewall that prevents application-layer attacks, such as cross-site scripting, SQL injection

and buffer overflows. It scans Web applications for attacks, then blocks user access when an attack is detected. The appliance can also scan Web and file uploads using either an integrated or external scanner.

This enterprise-caliber SSL VPN was easy to set up and manage; we had the device operational in 30 minutes. The intuitive interface lets security managers define policies, set up portal pages and determine authentication mechanisms.

FirePass can check for client digital certificates, and its compatibility with Active Directory, RADIUS and RSA SecurID (for two-factor authentication) provides secure turnkey access for up to 1,000 concurrent users.

FirePass provides reports from the activation and session logs. Summary reports aggregate usage by day, time, accessing OS, features used, Web sites accessed, session duration and session termination type.

The FirePass 4100 is the best remote access solution we've seen to date. It trumps other SSL VPN offerings with its ease of use, industrial strength hardware platform and advanced security features for unmanaged endpoint devices, one of the biggest risks emerging in this space. ▶

—GEORGE WRENN

