

TEST CENTER

SECURITY

F5 Networks Makes SSL VPNs Easy

Updated FirePass 1000 box simplifies browser-based remote access to applications

EVERY YEAR MORE employees work from remote offices or from home. And every year, IT spends more time supporting remote access to corporate applications. One reason for the time drain is that IPsec, the standard VPN encryption standard, can be difficult to configure, even with the improvements made in Windows XP.

The new alternative are SSL VPNs, which use the SSL Web server standard



instead of IPsec. With SSL, a browser provides direct access to applications and the network, with no complex setup.

The F5 Networks FirePass family consists of the 1000 model, reviewed here, and the recently announced 4100 model, which has additional enterprise features such as hardware SSL acceleration. They both provide easy setup of enterprise applications — from e-mail and accounting applications to X-Windows applications and file and print services — for secure access through a browser.

Since we reviewed it last December (infoworld.com/674), the FirePass 1000 has boosted functionality, including better presentation of applications, more flexible policies, and more

granular management. In addition, it now provides PDA accessibility and has a Citrix MetaFrame portal.

Simple SSL Setup

Providing SSL access to a single application, especially if it's Web-enabled, is relatively simple. But providing SSL access to many apps that aren't Web enabled is another matter entirely. Presenting the application interface in a browser window is a challenge, one that the FirePass overcomes handily.

Running applications through the FirePass, using the ActiveX control, is no more difficult than running them from a Windows server. I was able to quickly and easily set up access to files, printers, and a wide variety of applications

though the Web portal. I could access those applications from browsers on a variety of Windows, Linux, Macintosh, and even Pocket PC systems, with little effort or configuration required on the client side.

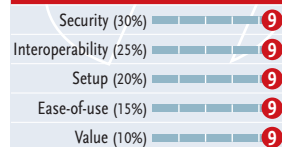
The FirePass can be configured to automatically download the required ActiveX or Java remote-access component to a user's browser, and to automatically clean up the browser and client system afterward, removing links, history, temp files, and more. For systems that have ActiveX disabled, the FirePass Java client puts a Java wrapper around ActiveX, so browsers with Java enabled will provide the same level of functionality as those with ActiveX.

Security is excellent throughout the system. You may enter passwords by clicking on a virtual keyboard with the mouse, making it impossible for keystroke loggers, screen-capture routines, or other spyware to collect charac-

FirePass 1000

F5 Networks f5networks.com

EXCELLENT 9.0



COST: Starts at \$9990 for 25 concurrent user license

PLATFORMS: Current Web browsers

BOTTOM LINE: The FirePass 1000 provides remote access to virtually any enterprise network application. It's easy to use and boasts excellent security, offering high levels of security, granular administration of users and groups, compatibility with a wide array of clients and browsers, and an easy setup and configuration.

ters. The Policy Engine will check to ensure that virus scanners or other security applications are installed before allowing access to your apps. It can ensure that necessary service packs have been installed, or look for spyware.

Policy Engine can also offer access to a restricted network to download any necessary patches or applications and can restrict access if the ActiveX client isn't loaded. The system protects apps, watching for buffer overflow attacks, SQL command injection, and other application-layer attacks, as well as stripping viruses and worms from e-mail attachments.

The FirePass itself gets user and group information directly from Active Directory or LDAP-compatible directories. Access to files stored on Windows Server or Unix/Linux servers is granted using the NFS standard. This access can be restricted by VLAN and group, such as limiting partner companies to a specific part of the network while giving employees unrestricted access.

Both administration and

user/group access is as granular as anyone could wish. One interesting new feature is the ability to create aliases for network resources, something not found in other SSL VPNs. For instance, if a drive mapping for an HR app is actually \\server1:home\hr, an alias of HR can be used to set up different groups with that mapping. Then, if the mapping is ever changed, the alias is changed in one spot rather than having to edit all the groups that use the HR mapping.

Solid App Support

Unlike other SSL VPNs, FirePass supports many applications directly, with no additional configuration required. These include Exchange, Citrix clients, Windows terminal services, virtual network computing apps, 3270 and 5250 terminal apps, SSH and telnet apps, and X-Windows apps. All are presented well in the browser window.

Setting up the initial portal Web page is easy. Each group can have separate login URLs that provide access to specific apps,

VLANs, file servers, or other network resources. Clicking on the initial URL on the user access Web site automatically downloads the browser plug-in, checks to ensure the proper software is installed on the client, and presents the login screen.

The FirePass offers browser-based access to client systems on the network through an application called Webifyer. Like GoToMyPC, the Webifyer adds great functionality for remote users. With this app, a remote user can login to their office PC, collaborate with users at the home office, and print to network printers, all with no remote access software required other than the standard FirePass browser plug-in on the client (the office PC must be running the Webifyer software).

The Webifyer has pre-configured access modes for standard browsers, WAP browsers, and PDA/mini-browsers. FirePass also supports IPSec, allowing IPSec tunneling through the SSL connection so that internal apps requiring IPSec can also be enabled through the gateway. The FirePass

acts as an IPSec host or gateway, so that IPSec tunnels are either terminated in the FirePass or passed through to the final destination as desired.

FirePass provides SSL-based access to virtually any network application, and does so with almost no effort on the part of the remote user — saving IT some time and effort, too. The added features — better presentation of applications, more flexible policies and more granular management, accessibility through PDAs and Citrix MetaFrame portal — make it worth the upgrade.

This is an excellent SSL VPN for companies with a dispersed workforce that still requires secure access to the enterprise network and applications. It sets a new standard for ease of use in setup and configuration, and for the wide array of client OSes and browsers supported.

Compared with IPSec or even other SSL VPN solutions, the FirePass will make both users and administrators happy with its ease of setup and administration.

— Logan G. Harbaugh

