Secure Remote Access

F5's FirePass® Controller provides secure remote access to corporate applications and data via standard Web browser technology. It enables companies to extend secure remote access to anyone connected to the Internet using desktops, laptops, PDAs, kiosks and more – while eliminating the need for complex IPSec VPNs.

FirePass is the first SSL VPN solution with complete cross-platform support. Extending its support for any IP application to Macintosh, PocketPC and Linux clients and expanding client and application security for Web, email and file application access, FirePass delivers the industry's most ubiquitous solution for secure application access.

It also offers the only open API (Application Programming Interface) and SDK (Software Developer's Kit) that enables 3rd party application vendors to build seamless, secure remote access into their client applications.

Key Benefits

Simple To Use -
Appliance installs quickly, offers an intuitive, familiar browser-based interface; uses standard SSL encryption and Web-browser technology to overcome access challenges – regardless of environment

Broadest Application Access –
FirePass supports access to Web hosts, terminal servers, client-server applications, legacy hosts, mobile devices and Windows desktops, without pre-installed client software or application updates

Reliable –
Web-based remote access works over all ISP connections; works behind other firewalls; operates entirely over HTTP - the secure application layer Internet protocol

Secure Communication –
Offers standard RC4, 3DES, AES bulk encryption for secure communication; delivers dynamic policy-based access for greater client security, control and enforcement

Comprehensive Security –
Provides more than just client security and application access -- delivers a unified security solution with client security, application access, virus scanning and application-level security

Reduced Costs –
Because it's a clientless solution, support overhead is dramatically reduced

Eliminates Ongoing Maintenance With Client Systems –
Requires no modifications to network resources, user remote devices, or network architecture, resulting in simplified deployment and fewer support calls

Business Policies –
Delivers granular control using groups, access rights and auditing

Dynamic Policy Engine - Total Administrative Control

The FirePass Policy Engine enables administrators to easily manage user authentication and authorization privileges.

Dynamic Policy Based Access

With FirePass, administrators have quick and granular control over their network resources. Through rules support, administrators can authorize access to applications based on the user and device being used. For example, administrators can configure a user's permission to allow email-only access from a public kiosk with active cache and temporary file cleanup, but provide them full network access from a corporate laptop with active firewall and virus detection software.

User Authentication

By default, users are authenticated against an internal FirePass database, using passwords. But FirePass can also be easily configured to work with RADIUS, Active Directory (Kerberos) and LDAP authentication methods, basic and form-based HTTP authentication, identity management servers (e.g. Netegrity), and Windows Domain Servers.

Two-Factor Authentication

Many organizations require "two-factor" authentication which uses something beyond knowledge of a user ID and password. FirePass fully supports RSA SecurID® token-based authentication. FirePass also offers a built-in implementation of VASCO Digipass®.

Client-Side Certificate Support

FirePass enables the administrator to restrict or permit access based on the device being used to access the FirePass Controller. FirePass can also check for the presence of a client-side digital certificate during user login. This certificate will only be present on the laptop. Based on the presence of this digital certificate, FirePass can support access to a broader range of applications. FirePass can also use the client-side certificate as a form of two-factor authentication and prohibit all network access for users without a valid client-side certificate. FirePass can act as a certificate authority and auto-generate and distribute client certificates. This drastically reduces the additional costs to purchase and manage certificates for each of the clients.

Group Management

Access privileges can be granted to individuals or to groups of users (for example: "Sales", "Partners", "IT"). This allows FirePass to restrict individuals and groups to particular resources. Partners may be allowed access only to an extranet server, while Sales staff can connect to email, the company Intranet, and the CRM system.

Scalable and Simplified Access Policy Management

Access Policies can be defined to a group of resources as opposed to individual resources. New resources can be simply added to a resource group without modifying individual access policies manually. In addition, resources can be defined as an alias so that any changes to resource definition are automatically updated in all resource aliases. These capabilities significantly reduce the policy management complexity in an enterprise environment that has a large number of user groups and resources.

Session Timeouts and Limits

Administrators can configure inactivity and session timeouts to protect against a hacker attempting to take over a session from a user who forgets to logoff at a kiosk.

Role-Based Administration

This gives organizations flexibility in providing some administrative functions (enrolling new users, terminating sessions, re-setting passwords) to some administrator-users, without exposing all functions to them (for example, shutting down the server, deleting a certificate). In addition, the authorities can be restricted to particular groups of end users: the Administrator in Finance, for example, won't be allowed to delete a user in Sales.

Audit Services

FirePass provides reports from the session and activation logs. Summary reports aggregate usage by day of the week, time of day, accessing OS, features used, Web sites accessed, session duration, session termination type, and other information for a user-specified time interval.

Customization

UI Customization

Administrators can adjust the appearance of the FirePass Web pages to match the more familiar look and feel of their company. For example, a company can present their corporate logo and corporate colors on the sign-in screen and user Web pages. FirePass also offers support for customized login and portal pages based on login IP/URI. This enables customers to present a customized end-user look and feel based on users such as partners or customers.

Localized End User GUI

FirePass allows all fields on the end user Web page to be localized, including the names of the feature (e.g. Web Applications). This enables companies to localize all end user's GUI, not just user favorites – improving ease of use.

Portal Access - Secure Access From Public Systems For Employees, Customers and Partners

The FirePass Portal Access capability works on any client OS with a browser – Windows, Linux, Macintosh, Pocket PC's, PDAs and more.

Portal Access Available On FirePass:

Web Applications

- Provides access to internal Web servers, including Microsoft Outlook Web Access and Lotus iNotes, as easily as from inside the corporate LAN.
- Delivers granular access control to intranet resources on a group basis. For example, employees can be provided access to all intranet sites; partners can be restricted to a specific Web host.
- While accessing resources, FirePass dynamically maps internal URLs to external URLs, so the internal network structure does not reveal them.
- Manages user cookies at the FirePass Controller to avoid exposing sensitive information. For applications that require access to cookies, FirePass can pass cookies to the remote browser.
- User credentials can be passed to Web hosts to support automatic login and other user specific access to applications. FirePass also integrates with existing identity management servers (e.g. Netegrity) to enable single signon to applications.
- FirePass proxies login requests from Web hosts to avoid having users cache their passwords on client browsers.
- FirePass proxies requests for FTP or network file Web links and downloads the files via the browser.

File Server Access

- Allows users to browse, upload, download, copy, move or delete files on shared directories.
- Supports SMB Shares, Windows Workgroups; NT 4.0 and Win2000 domains; Novell 5.1/6.0 with Native File System pack, and NFS servers.

Email Access

- Provides secure Web-based access to POP/IMAP/SMTP email servers from standard and mobile device browsers.
- Allows users to send and receive messages, download attachments and attach network files to emails.

Mobile Device Support

- Secure access from PDAs, e.g. Palm OS, cell phones, e.g. WAP and iMode phones to email and other applications.
- Dynamically formats email from POP/IMAP/SMTP email servers to fit the smaller screens of mobile phones and PDAs. Supports the sending of network files as email attachments and the viewing of text/Word documents.

Portal Access – Comprehensive Security

FirePass delivers multiple layers of control for securing information access from public systems.

Client Security

- **Protected Workspace** – Users of Windows 2000/XP can be automatically switched to a protected workspace for their remote access session. In a protected workspace mode, the user cannot write files to locations outside the protected workspace and the temporary folders and all of their contents are deleted at the end of the session.

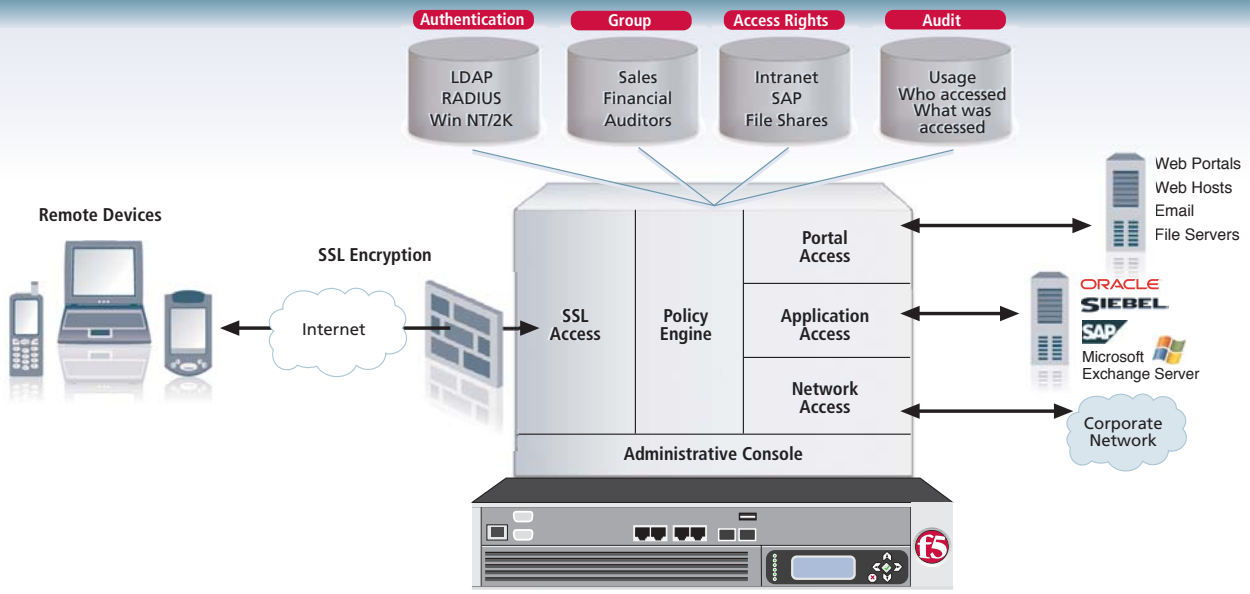
  Since the user session is in a separate desktop, users are protected from trojan horses and key loggers.
- **Cache Cleanup** – The cache cleanup control removes the following data from the client PC: Cookies, Browser history, Auto-Complete information, Browser cache, Temp files, all ActiveX controls installed during the remote access session, and empties the recycle bin.
- **Secure Virtual Keyboard** – For additional password security, FirePass offers the patent-pending Secure Virtual Keyboard which enables secure password entry from the mouse instead of the keyboard. When engaged, this feature enables users to securely enter a password on a system that has been compromised by a key logger.
- **Download Blocking** – For systems unable to install a "cleanup" control, FirePass can be configured to block all file downloads to avoid the issue of inadvertently leaving behind temporary files – yet still allow access to applications.

Content Inspection and Web Application Security

For users accessing Web applications on the corporate network, FirePass enhances application security and prevents application-layer attacks (e.g. cross-site scripting, invalid characters, SQL injection, buffer overflow) by scanning Web application access for application-layer attacks – then blocking user access when an attack is detected.

Integrated Virus Protection

FirePass can scan Web and file uploads using either an integrated scanner or external scanner via ICAP API. Infected files are blocked at the gateway and not allowed onto email or file servers on the network, heightening protection.



Application Access - Secure Access To Specific Applications

FirePass allows administrators to grant certain users – for example, business partners using equipment not maintained by the company – access to specific extranet applications and sites. FirePass protects network resources by only allowing access to applications that are specifically cleared by the system administrator. Supported applications include terminal servers, legacy hosts, Windows desktops, and X Windows systems. FirePass logs an audit trail of the specific applications accessed by each user to facilitate security audits.

Specific Client/Server Application Access:

- Enables a native client side application to communicate back to a specific corporate application server via a secure connection between the browser and the FirePass Controller.
- Does not require the user to preinstall or configure any software.
- On the network side, requires no additional enabling software on the application servers being accessed.
- Uses the standard HTTPS protocol, with SSL as the transport so it works through all HTTP proxies including public access points, private LANs, and over networks and ISPs that do not support traditional IPSec VPNs.
- Supported applications include Outlook to Exchange Clusters; Passive FTP, Citrix Nfuse, and network drive mapping.
- Administrators can also support custom applications including CRM as well as other applications that utilize static TCP ports.
- Compression is supported for better performance.

Terminal Server Access

- Provides secure Web-based access to Microsoft Terminal Servers, Citrix MetaFrame applications, Windows XP Remote Desktops, and VNC servers.
- Supports group access options, user authentication and automatic logon capabilities or authorized users.
- Supports automatic downloading and installation of the correct Terminal Services or Citrix remote-platform client component, if it is not currently installed on the remote device, saving time.

Desktop Access

- Allows secure remote control of Windows corporate desktops from Web browsers supporting Java or ActiveX downloads.
- Provides the ability to share the desktop with other users for Web-based collaboration or demonstrations; provides access to files, email and other applications.

Unix System Access

- Supports secure access to Unix/Linux systems from Web browsers supporting Java or ActiveX downloads.
- Utilizes X Windows to natively communicate with Unix systems
  – requires no modifications to the Unix system or application or preinstalled X Windows client software.

Host Access

- Enables secure Web-based access to legacy VT100, VT320, Telnet, X-Term, and IBM 3270/5250 applications.
- Requires no modifications to the applications or application servers.

Network Access

FirePass Network Access for Windows, Macintosh, PocketPC and Linux Systems:

- Standard features across all desktop and laptop platforms include split tunneling, compression, activity-based timeouts, and automatic application launching.
- Provides secure remote access to the entire network for all IP-based (TCP, UDP) applications.
- Unlike traditional IPSec VPNs, provides remote access without requiring pre-installed client software and configuration of the remote device. Client or server side application changes are not required.
- Allows administrators to restrict and protect resources accessible through the connector by instituting rules that limit access to a specific network or port.
- Uses the standard HTTPS protocol with SSL as the transport, so it works through all HTTP proxies including public access points, private LANs, and over networks and ISPs that don't support traditional IPSec VPNs.
- Utilizes GZIP compression to compress traffic before it is encrypted, reducing the amount of traffic that is sent across the Internet and improving performance.

Client Security

- Safe Split Tunneling – To protect against backdoor attacks when accessing the network with split tunneling, FirePass provides a dynamic firewall that protects Win2k/XP users when using the full network access feature. This eliminates the ability for a hacker to route through the client to the corporate network or for the user to inadvertently send traffic to the public network.
- Client Integrity Checking – FirePass increases security by detecting the presence of required processes (e.g. virus scan, personal firewalls, OS patch levels, registry settings and McAfee Antivirus levels) and the absence of other processes (e.g. key logger) on the client PC before allowing full network access. Users who fail these primary policies can be connected to a quarantine network where they update to current corporate security standards.

Other Network Access Features

- Standalone Windows Client - FirePass establishes a network connection after entering user credentials. Software can be automatically distributed to the client using Microsoft's MSI installer technology.
- Provides Automatic Drive Mapping - Network drives can be automatically mapped to a user's Windows PC.

iControl SSL VPN Client API for Secure Application Access

As the only SSL VPN product with an open API and SDK, FirePass Controller enables automated, secure access for rich Win32 client applications by providing secure system-to-system or application-to-application communication. Now, applications can automatically start and stop network connections transparently without requiring users to log into the VPN. This enables faster, easier connections for end users while reducing client application installation.

Organizations and developers interested in this API should visit F5's DevCentral (devcentral.f5.com) to learn more. DevCentral will provide developer guidance, sample code, documentation, technical tips, and collaboration via the DevCentral Forum.

FirePass 1000 Series

FirePass 4100 Series

Ordering Information

FirePass 1000 Series

The FirePass 1000 Controller is a 1U rack-mount server designed for small to medium enterprise locations. It supports up to 100 concurrent users and offers a comprehensive solution for secure Web-based remote access to corporate applications and desktops.

FirePass 4100 Series

The FirePass 4100 Controller is a 2U rack-mount server designed for large enterprise locations. It supports up to 1000 concurrent users and offers a comprehensive solution for secure Web-based remote access to corporate applications and desktops.

FIPS SSL Accelerator Hardware Option

FirePass offers FIPS support to meet the strong security needs of government, finance, healthcare and other security conscious organizations. FirePass 4100 offers unique support for FIPS 140 Level-2 enabled tamper proof storage of SSL keys, as well as FIPS certified cipher support for encrypting and decrypting SSL traffic in hardware. FIPS SSL Accelerator is available as a factory install option to the base 4100 platform.

SSL Accelerator Hardware Option

FirePass 4100 offers a unique Hardware SSL Acceleration option to offload the SSL key exchange as well as the encryption and decryption of SSL traffic. This enables significant performance gains in large enterprise environments for processor intensive ciphers such as 3DES and AES.

Clustering

FirePass 4100 Controllers can be clustered to support up to 10,000 concurrent connections on a single URL, without performance degradation. Advanced load balancing features distribute the sessions among available servers to maximize throughput.

Failover

FirePass Controllers can be configured for hot, stateful failover between yoked pairs of servers (an active server and a standby server), without session interruption or termination. This means that in the unlikely event of a server failure, all session data is preserved and the failover to a backup unit is invisible to the user.

Hardware Specifications

FirePass 1000

Power Supply:
180 Watt

Weight:
~10 lb

Dimensions:
16.7" x 1.7" x 11"

Certifications:
US/Canada - UL - UL 1950
European Union – Low Voltage directive - EN 60950
European Union – EMC directive EN50081-2 & EN 61000-6-2
CE

Temperature (operating):
0-40 Deg C

Humidity:
5-85% @ 40 Deg C (non-condensing)

FirePass 4100

Power Supply:
400W with redundant option

Weight:
~36 lb

Dimensions
17.5" x 24.5" (OAL)/23.5" behind mounting ears x 3.5"

Certifications:
US/Canada – UL – UL 1950
European Union – Low Voltage Directive – EN 60950
European Union – EMC Directive EN 50081-2 & EN 61000-6-2
CE

Temperature (operating):
5-40 Deg C

Humidity:
5 to 85% @ 40 Deg C (non-condensing)

F5 Networks, Inc.
Corporate Headquarters
401 Elliott Avenue West
Seattle, WA 98119
(206) 272-5555 Voice
(888) 88BIGIP Toll-free
(206) 272-5556 Fax
www.f5.com
info@f5.com

F5 Networks
Asia-Pacific
+65-6533-6103 Voice
+65-6533-6106 Fax
info.asia@f5.com

F5 Networks Ltd
Europe/Middle-East/Africa
+44 (0)1784 497210 Voice
+44 (0)1784 497211 Fax
emeainfo@f5.com

F5 Networks
Japan K.K.
+81-3-5766-5511 Voice
+81-3-5766-5512 Fax
info@f5networks.co.jp

Part No. DS-FP 0904