Key Benefits:

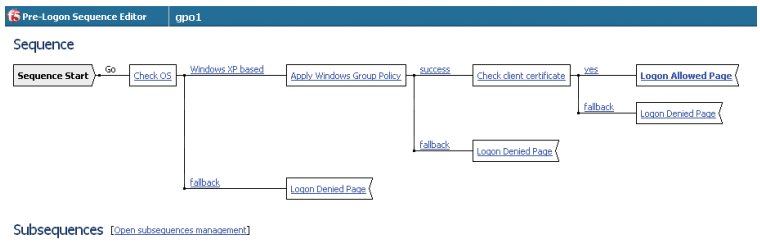
- Increased worker productivity—ability to work from any location
- Streamlined business processes with partners, suppliers and customers
- Lower deployment and support costs
- Increased security with granular access control
- Risk reduction with strong endpoint security
- Continuous business and worker continuity

Best-In-Class SSL VPN

The F5 FirePass® SSL VPN appliance provides secure remote access to corporate applications and data using a standard web browser as well as a standalone client. FirePass delivers outstanding performance, scalability, availability, policy management, ease-of-use, and end-point security, to ensure high productivity for those working from home or on the road while keeping corporate data secure.

Key Features:

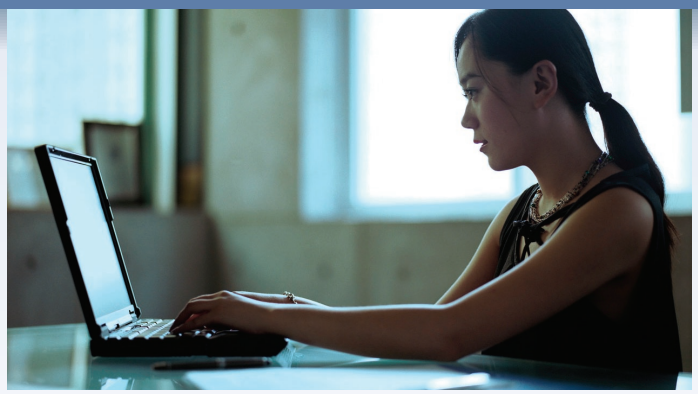
- **Best-in-Class Policy Management** – Unique Visual Policy Editor delivers an easy to use, intuitive, point-and-click interface for managing granular access policies while lowering management costs. Administrators can easily implement existing policies with import/export of pre-logon policies.
- **Group Policy Enforcement** – Provides an exclusive mechanism to apply and enforce group policies on client systems, not part of the network domain. Policies, in the form of templates, restrict user authority and access on the client while enforcing compliance with PCI, HIPAA, and GLBA.
- **Integrated Endpoint Security** – Delivers a secure virtual workspace, pre-logon endpoint integrity checks, and endpoint trust management for simplified administration.
- **Broadest Application Support** – Provides secure and easy access to email, web portals, network file services, Terminal Services, CRM and other key enterprise applications, from both managed and un-managed client devices, from any location.
- **Broad Client Support** – FirePass offers broad multi-platform support for secure network access from Windows (2000, XP, Vista), Linux, Mac, Apple iPhone, Windows Mobile, and other smart phones.
- **Enterprise Class Scalability and Performance** – Supports up to 2,000 concurrent sessions on a single, easy-to manage device. Easily scales to support a worldwide rollout through integration with F5 BIG-IP Local Traffic Manager and clustering capabilities. Optimizes the end-user experience using capabilities such as compression for any IP application traffic and server-side caching for web applications.
- **Broad Interoperability** – Supports existing network infrastructure and identity management systems via Active Directory, Radius, LDAP, PKI, RSA ACE, and more. Delivers web portal integration with support for Java applets, JavaScript rewrite, and more (VPNC certified).
- **Industry-Leading Global High Availability** – Unique integration with F5 BIG-IP Global Traffic Manager provides high availability across the WAN in case of site disaster. Failover support offers high availability within a site.



The Visual Policy Editor creates a flow-chart style graphical view of your access policies, giving you point-and-click ease in profiling and managing groups, users, devices or any combination of the three. This enables a simplified definition and management of endpoint policies, lowers administrative costs, and increases the ability to quickly ensure the protection of company resources.

InfoWorld — Rated Excellent

INFORMATION SECURITY Hot Pick!



Network Access

FirePass Network Access for Windows (Vista, XP, 2000), Mac, and Linux Systems:

- Windows Installer Service eliminates the need for special administrative privileges for FirePass client component updates, lowering management costs.
- Provides secure remote access to the entire network for all IP-based (TCP, UDP) applications.
- Standard features across all desktop and laptop platformsinclude split tunneling, compression, activity-based timeouts, and automatic application launching.
- Unlike 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 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

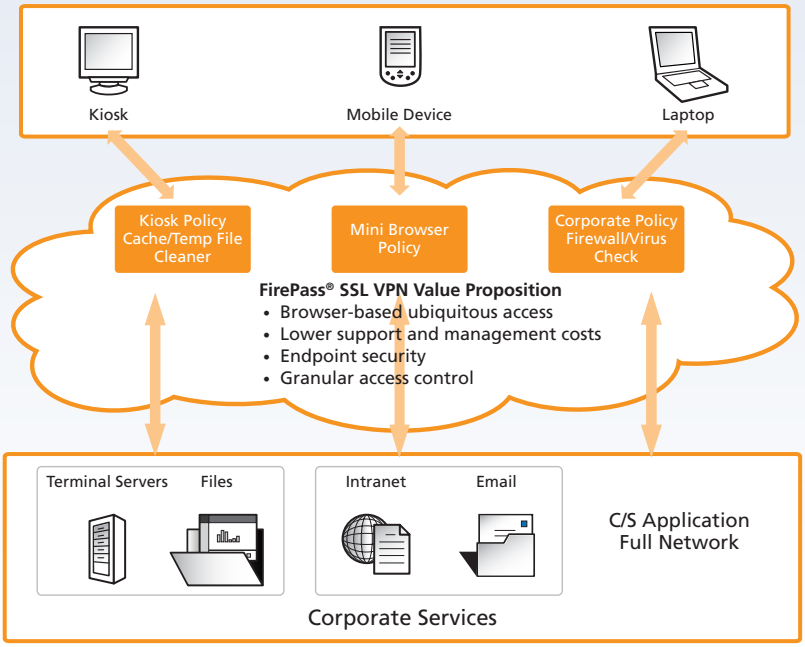
- Safe Split Tunneling – To protect against backdoor attacks when accessing the network with split tunneling, FirePass provides a dynamic firewall that protects Windows 2000/XP/Vista, Mac, and Linux users when using the full network access feature. This eliminates the ability for a hacker to route through 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, etc.) and the absence of other processes (e.g. key logger) on the client PC before allowing full network access.

Windows 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.
- Windows Logon/GINA Integration – Enables implied, transparent user logon to the corporate network by integrating with the GINA ("ctrl + alt + del" prompt) logon process.
- Standalone VPN Client CLI – Command line interface support offers single sign-on support through integration with 3rd party applications (such as remote dialer software).
- Windows VPN Dialer – Provides a simplified end user experience for users more comfortable with the dialup interface.
- Provides Automatic Drive Mapping – Network drives can be automatically mapped to a user's Windows PC.
- Provides Static IP Support – Assigns static IP based on the user, when the user establishes a network access VPN connection – lowering administrative support costs.
- Transparent Network Access – Eliminates network access browser window pop-ups; prevents users from accidentally terminating the connection.

Mobile Device Support

- Secure application access from Windows Mobile and Smart Phones.
- Access to both client/server and web based applications.



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.

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 pre-install or configure any software.
- On the network side, requires no additional enabling software on the application servers being accessed.
- As with network access, application access is via standard protocols: HTTP and SSL/TLS. It works with all HTTP proxies, access points, and 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.
- Supports auto-login to AppTunnels, Citrix, and WTS applications to simplify the end-user experience.
- Supports auto-launch of client side applications to simplify the end user experience and lower support costs.
- Enables Java-based application tunnels for non-Windows systems and Windows systems locked down to prevent execution of ActiveX controls.
- Offers complete DHCP support for clients using network access, automating IP address assignment, and dynamic DNS registration of addresses. DHCP support provides easier multi-unit deployments while remote access IP address range can overlap with internal LAN.
- Delivers support for MS Communicator via Portal Access, enhancing VoIP communications.
- Unique support for compression of client/server application traffic over the WAN for better performance.

Terminal Server Access

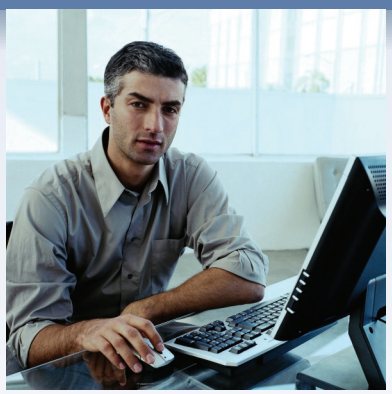
- Provides secure web based access to Microsoft Terminal Servers, Citrix MetaFrame applications, Windows XP Remote Desktops, and VNC servers.
- Supports group access options, user authentication, and automatic logon capabilities or authorized users.
- Supports automatic downloading and installation of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

Dynamic AppTunnels

- Maximum support for accessing a wide variety of client/server applications and web based applications.
- A better alternative than reverse proxies for accessing applications from Windows client devices.
- Eliminates the need for web application content interoperability testing.
- Requires only 'power user' privileges for installation and no special privileges for execution.
- Provides added support for auto launching web application tunnels, simplifying the end user experience.

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.
- Eliminates the need for 3rd party host access software, reducing TCO.



Portal Access – Proxy-Based Access to Web Applications, Files, and Email

The FirePass Portal Access capability works on any client OS with a browser: Windows, Linux, Macintosh, Smart Phones, PDAs and more.

Web Applications

- Provides access to internal web servers, including Microsoft Outlook Web Access, Lotus iNotes, and MS SharePoint Portal 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.
- 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 sign on to applications.
- FirePass proxies login requests from web hosts to avoid having users cache their passwords on client browsers.
- Granular Access Control List (ACL) – Allows or restricts access to specific parts of an application for increased security and lower business risks.
- Provides split-tunneling support for web applications, resulting in faster end user performance when accessing public websites.
- Rapid reverse-proxy backend certificate validation quickly validates the server's certificate.
- Dynamic server-side and DNS caching for increased web application (reverse proxy) performance and faster page download times.
- Delivers out-of-the-box reverse proxy support for rewriting a wide variety of JavaScript content in web pages, saving time.
- Provides Java patch ACL support to limit client-initiated connections through FirePass using Portal Access.
- Enables NTLMv2 support for access to web applications.
- Delivers DNS relay proxy service, enabling client-side name resolution without requiring any special runtime rights (for example, modification of hosts). Also enables redirection of ports to more fully support applications such as Outlook and Windows drive mapping.

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 Apple iPhone, Windows Mobile, PDAs, Smart Phones, cell phones, WAP, and iMode phones to email and other web-based 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.
- ActiveSync Support – Support for ActiveSync application allows PDA synchronization of email and calendar on Exchange server from a PDA device, without requiring the pre-installed VPN client component.

Portal Access – Comprehensive Security

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

Client Security

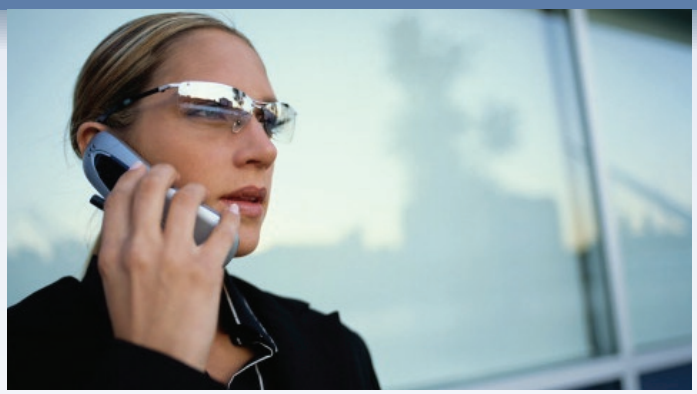
- **Protected Workspace** – Users of Windows 2000/XP can be automatically switched to a protected workspace for their remote access session. In a protected workspace mode, the user cannot write files to locations outside the protected workspace; the temporary folders and all of their contents are deleted at the end of the session.
- **Cache Cleanup** – The cache cleanup control removes—and empties from the recycle bin—the following data from the client PC: cookies, browser history, auto-complete information, browser cache, temp files, and all ActiveX controls installed during the remote access session.
- **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.
- **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.



Dynamic Policy Engine – Total Administrative Control

The FirePass policy engine enables administrators to easily manage user authentication and authorization privileges.

Dynamic Policy-Based Access
Administrators have quick and granular control over their network resources. Through policy support, they can authorize access to applications based on the user and device being used. Administrators can easily implement existing policies with import and export of pre-logon policies.

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, RSA 2-Factor, LDAP authentication methods, basic and form-based HTTP authentication, identity management servers (e.g. Netegrity), and Windows domain servers. With Active Directory, users can change current or expired passwords and receive warnings when passwords are set to expire. Support for nested Active Directory configurations enables the use of a more complex, hierarchical directory structure.

Two-Factor Authentication
Many organizations require "two-factor" authentication which uses something beyond knowledge of a user ID and password. FirePass supports two-factor authentication including RSA SecurID® Native ACE authentication.

Client-Side Certificate/PKI Support
FirePass enables the administrator to restrict or permit access based on the device being used to access the FirePass Controller. FirePass can check for the presence of a client side digital certificate during user login. 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.

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.

Dynamic Group Mapping
FirePass dynamically maps users to FirePass groups using various dynamic group mapping mechanisms such as Active Directory, RADIUS, LDAP, Client Certificates, Landing URI, Virtual Host name as well as pre-logon Session Variables.

Single Sign On (SSO) Support
SSO configuration uses authentication session variables to extract SSO information from certificates and authentication information from username and password settings. Advanced session variables allow system administrators to extend and customize FirePass, enabling them to manipulate and create new session variables for custom deployments. They also can collect and capture RADIUS attributes plus LDAP, AD, and certificate field values.

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).

Logging & Reporting
FirePass delivers built-in logging support for logging user, administrator, session, application, and system events. Additionally, FirePass provides logs in silo format for integration with an external syslog server. The administration console offers a wide range of audit reports to help comply with security audits. Summary reports aggregate usage by day of the week, time of day, accessing OS, features used, websites accessed, session duration, session termination type, and other information for a user-specified time interval. A single URL is used to retrieve summary/group reports in either HTML or spreadsheet format.

Customization

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 the end user's GUI, not just user favorites—increasing business value and lowering TCO.

Complete Login and WebTop Customization
With FirePass, administrators can completely customize an entire login and webtop web page to best suit their existing corporate web site portals. FirePass allows the uploading of custom pages using WebDAV capabilities for an enhanced end user experience.

iControl SSL VPN Client API for Secure Application Access

As the only SSL VPN product with an open client API and SDK, FirePass enables automated, secure access from the Win32 client OS (2000, XP, Vista) 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 costs.

FirePass 1200 Series

FirePass 4100 & 4300 Series

Product details

The FirePass series of appliances are offered in three models to address the concurrent user access needs for small to very large enterprises.

FirePass 1200 Series
The FirePass 1200 appliance is designed for small to medium enterprises and Branch Offices and supports from 10 to 100 concurrent users.

FirePass 4100 Series
The FirePass 4100 controller is designed for medium-size enterprises and, from a price/performance standpoint, is recommended for up to 500 concurrent users.

FirePass 4300 Series
The FirePass 4300 appliance is designed for medium to large enterprises and service providers and supports up to 2000 concurrent users.

Clustering
Both the FirePass 4100 and 4300 appliances have built-in clustering support. They can be combined with BIG-IP Global Traffic Manager and BIG-IP Local Traffic Manager to provide industry-leading scalability, performance, and availability.

Failover
FirePass appliances can also be configured for failover between pairs of servers (an active server and a standby server) to avoid users having to re-logon to another FirePass in the unlikely event of a primary unit failure.

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.

FIPS SSL Accelerator Hardware Option*
FirePass is FIPS compliant* to meet the strong security needs of government, finance, healthcare and other security conscious organizations. FirePass 4100 and 4300 offers 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 and 4300 platform.

**FIPS 140-2 meets the security criteria of CESG (UK's National Technical Authority For Information Assurance) for use in private data traffic.*

Hardware Specifications

FirePass 1200
Power Supply:
Single full-range 250W

Weight: *10 lbs*

Dimensions: *1.7"H x 16.7" W x 11" D*
1U industry standard rack mount chassis

Safety Agency Approval:
UL 60950 (UL 1950-3), CSA-C22.2
No 60950-00 (Bi-national standard with UL 60950)
CB test certification to IEC 950,
EN 60950

Temperature (operating):
41° F to 104° F (5° C to 40° C)

Humidity (relative): *20% to 90% at 40° C*

FirePass 4100
Power Supply: *425W 90/240 +/- 10% VAC*
auto switching
Optional redundant power supply

Weight: *40 lbs*

Dimensions: *3.5" H x 17.5" W x 23.5" D*
2U industry standard rack mount chassis

Safety Agency Approval:
UL 60950 (UL 1950-3), CSA-C22.2
No 60950-00 (Bi-national standard with UL 60950)
CB test certification to IEC 950,
EN 60950

Temperature (operating):
41° F to 104° F(5° C to 40° C)

Humidity (relative): *20% to 90% at 40° C*

FirePass 4300
Power Supply:
Dual 475W 90/240 +/- 10% VAC
auto switching

Weight: *43 lbs*

Dimensions: *3.5" H x 17.5" W x 23.5" D*
2U industry standard rack mount chassis

Safety Agency Approval:
UL 60950 (UL 1950-3), CSA-C22.2
No 60950-00 (Bi-national standard with UL 60950
CB test certification to IEC 950,
EN 60950

Temperature (operating):
41° F to 104° F(5° C to 40° C)

Humidity (relative): *20% to 90% at 40° C*

F5 Networks, Inc.
Corporate Headquarters

401 Elliott Avenue West
Seattle, WA 98119
206-272-5555 Phone
888-88BIGIP Toll-free
206-272-5556 Fax
www.f5.com
info@f5.com

F5 Networks
Asia-Pacific

+65-6533-6103 Phone
+65-6533-6106 Fax
info.asia@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa

+44 (0) 1932-582-000 Phone
+44 (0) 1932-582-001 Fax
emeainfo@f5.com

F5 Networks
Japan K.K.

+81-3-5114-3200 Phone
+81-3-5114-3201 Fax
info@f5networks.co.jp

Part No. DS-FirePass 1007