FirePass® *Series*

Datasheet
Best-In-Class SSL VPN

Key Benefits:

- **Broadest Application Support** – Access to email, web portals, network file services, terminal services, CRM and other key enterprise applications, from both managed and un-managed client devices.
- **Integrated Endpoint Security** – Delivers a Secure Virtual Workspace, pre-login endpoint integrity checks, and endpoint trust management for peace of mind with fewer administrative hassles.
- **Highest Scalability** – Supports up to 2,000 concurrent sessions on a single, easy-to-manage box. Built-in load balanced clustering can support up to 20,000 sessions. More than 20,000 sessions can be supported by integration with BIG-IP.
- **Low Cost of Ownership**
  Installs in 30 minutes or less. Visual Policy Editor delivers a point-and-click interface for managing access policies.
- **Market Leading Performance & Scalability** – Fast access using compression for file transfers and email; supports an unlimited number of users.
- **Broad Interoperability** – Supports existing network infrastructure and identity management systems via Radius, LDAP, and more. Delivers web portal integration with support for Java applets, Javascript rewrite, and more (VPNC certified).
- **High Availability and Reliability** – Fail-over support offers high availability for end-users. Integration with BIG-IP Global Traffic Manager offers high availability across WAN in case of site disaster.

Best-In-Class SSL VPN

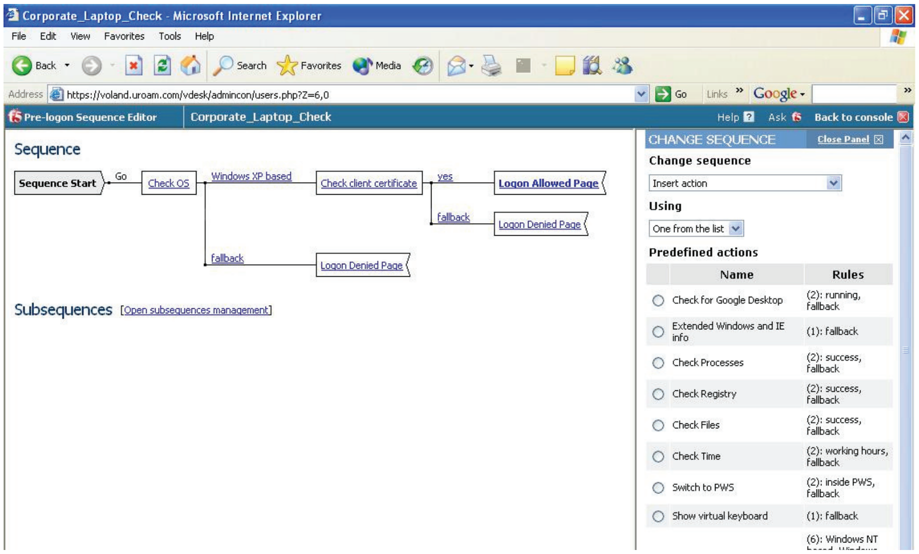
F5's FirePass® SSL VPN appliance provides secure access to corporate applications and data using a standard web browser. Delivering outstanding performance, scalability, ease-of-use, and end-point security, FirePass helps increase the productivity of those working from home or on the road while keeping corporate data secure.

Integrated Endpoint Security

FirePass prevents infected PCs, hosts, or users from connecting to your network. Automatic re-routing for infected PCs reduces help desk calls and prevents sensitive data from being snooped by keystroke loggers and malicious programs.

FirePass provides:

- Automatic detection of security compliant systems, preventing infection.
- Automatic integration with the largest number of virus scanning and personal firewall solutions in the industry (over 100 different AV & Personal Firewall versions).
- Automatic protection from infected file uploads or email attachments.
- Automatic re-routing and quarantine of infected or non-compliant systems to a self remediation network – reducing help desk calls.
- A secure workspace, preventing eavesdropping and theft of sensitive data.
- Secure Login with a randomized key entry system, preventing keystroke logger snooping.
- Full integration with the FirePass Visual Policy Editor. This enables the creation of custom template policies based on the endpoints accessing your network and your company's security profile.



Address https://voland.uroam.com/vdesk/admincon/users.php?Z=6,0

Change sequence: Insert action

Using: One from the list

Predefined actions

	Name	Rules
○	Check for Google Desktop	(2): running, fallback
○	Extended Windows and IE info	(1): fallback
○	Check Processes	(2): success, fallback
○	Check Registry	(2): success, fallback
○	Check Files	(2): success, fallback
○	Check Time	(2): working hours, fallback
○	Switch to PWS	(2): inside PWS, fallback
○	Show virtual keyboard	(1): fallback
		(6): Windows NT

The unique 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 end-point policies, lowers administrative costs, and increases the ability to quickly ensure the protection of company resources.

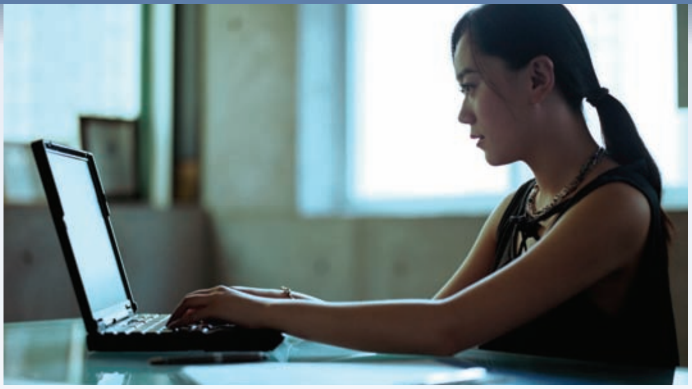
InfoWorld — *Rated Excellent*

INFORMATION SECURITY **Hot Pick!**

Network Access

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

- Provides secure remote access to the entire network for all IP-based (TCP, UDP) applications.
- Standard features across all desktop and laptop platforms include 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.

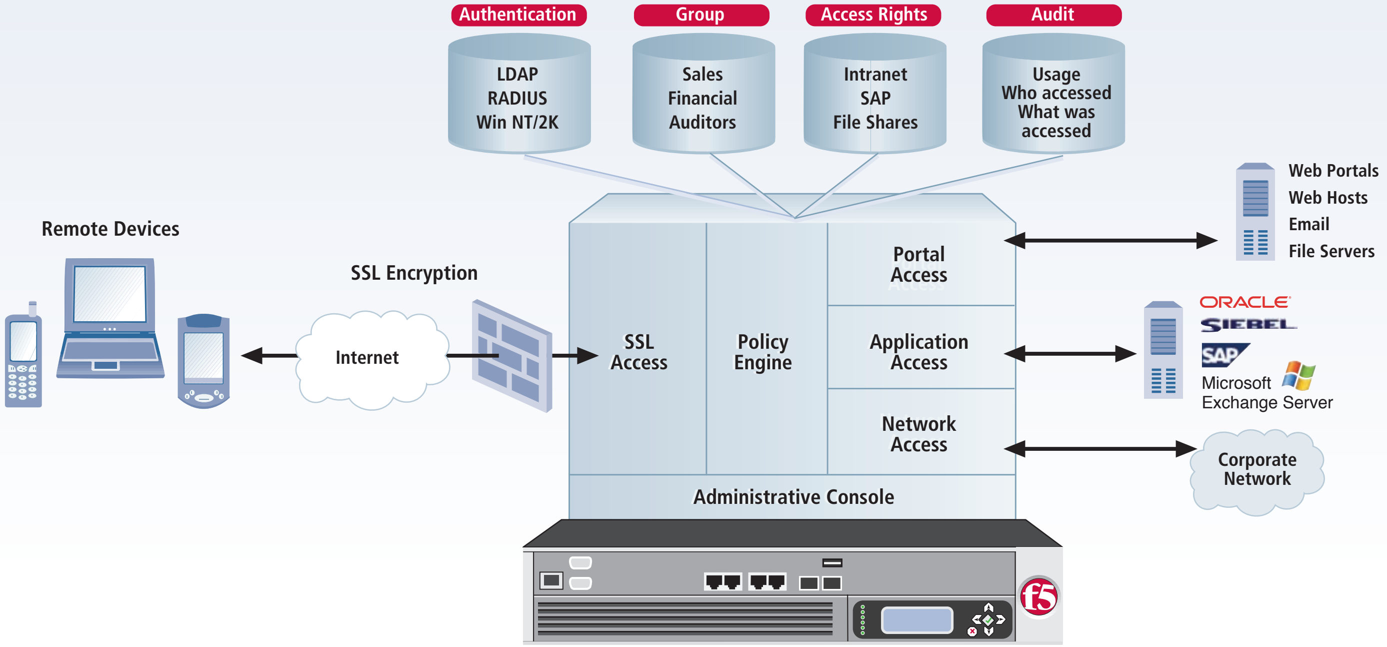


Client Security

- **Safe Split Tunneling** – To protect against backdoor attacks when accessing the network with split tunneling, FirePass provides a dynamic firewall that protects 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, 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 simplified, transparent user logon to the corporate network by integrating with the windows GINA ("ctrl + alt + del" prompt) logon process.
- **Standalone VPN Client CLI** – new 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.



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.
- 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.
- Supports auto-login to AppTunnels, Citrix, WTS applications to simplify end-user experience.
- Supports auto-launch of client side applications to simplify end-user experience and lower support costs.
- Unique support for compression of client/server application traffic over WAN to offer 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 built-in VNC feature.

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

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, Pocket PC's, PDAs and more.

Portal Access Available On FirePass:

Web Applications

- Provides access to internal web servers, including Microsoft Outlook Web Access, Lotus iNotes, 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 web sites.
- Dynamic server-side 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.

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.
  - **ActiveSync Support** – Support for ActiveSync application allows PDA synchronization of email and calendar on Exchange server from PDA device, without requiring 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 and the temporary folders and all of their contents are deleted at the end of the session.
- **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.
- **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

With FirePass, administrators have quick and granular control over their network resources. Through policy support, administrators can authorize access to applications based on the user and device being used.

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.

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 clientside 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.

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 syslog format for integration with 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, web sites accessed, session duration, session termination type, and other information for a user-specified time interval.

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 all end user's GUI, not just user favorites – improving ease of use.

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 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.

FirePass 1200 Series

FirePass 4100 Series

ICSA labs CERTIFIED www.ICSALabs.com SSL-TLS (VPN)

VPNC CERTIFIED
SSL Exchange
SSL File Access
SSL Portal

Ordering Information

FirePass 1200 Series

The FirePass 1200 Controller is a 1U rack-mount server designed for small to medium enterprise locations and branch offices. It supports 10 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 2000 concurrent users and offers a comprehensive solution for secure web-based remote access to corporate applications and desktops.

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 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 20,000 sessions on a single URL with built-in load balanced clustering option, without performance degradation. For high performance large scale clustering, customers can leverage unique integration with BIG-IP by off-loading SSL termination to BIG-IP, scale beyond the 20,000 concurrent sessions in a cluster, and maximize the SSL VPN cluster performance.

Failover

FirePass Controllers can be configured for failover between pairs of servers (an active server and a standby server) to avoid users from having to re-logon to another FirePass in case the primary unit fails.

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:** Full range 220W ATX PSU*

***Weight:** Net 11.45 lbs, Gross 21.59 lbs*

***Dimensions:** 16.87" (W) x 14.17" (D) x 1.73" (H)*

***Certifications:** CE/FCC/UL*

***Temperature (operating):** 5-40 Deg C*

***Humidity:** 20-90% RH*

FirePass 4100

***Power Supply:** 400W with redundant option*

***Weight:** ~36 lb*

Dimensions:
17.5" (W) x 24.5" (OAL)/23.5" (D) behind mounting ears x 3.5" (H)

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

F5 Networks
Japan K.K.
+81-3-5114-3200 Voice
+81-3-5114-3201 Fax
info@f5networks.co.jp