FirePass SSL VPN

PRODUCT OVERVIEW

"One of the biggest impacts of FirePass SSL VPN is that it's a solid, reliable, stable platform."

Ken Desforges, IS Director,
City of Diamond Bar, California

Increase Productivity with Flexible, Secure Remote Access

Key benefits:

- Improve user experience and productivity
- Ensure security with granular access control
- Gain ultimate flexibility using both virtual and physical appliances
- Reduce risk with strong endpoint security
- Decrease deployment, management, and support costs

As more mobile and remote workers use an increasing number of devices to access corporate applications and data from many different locations—whether it's from home, an internal wireless connection, airport, hotel, or coffee shop—your business benefits from more flexible and productive users. But securing applications, data, the network, and client devices from unauthorized access and attacks can quickly add management complexity and cost as new threats evolve.

The FirePass® SSL VPN appliance and Virtual Edition (VE) provide secure remote access to enterprise applications and data for users over any device or network. FirePass ensures easy access to applications by delivering outstanding performance, scalability, availability, policy management, and endpoint security. The result is unified security enforcement and access control that increases the agility and productivity of your workforce.

ICSA labs CERTIFIED SSL VPN

Increase worker productivity

With FirePass SSL VPN, you can ensure workers have secure remote access across a wide variety of applications and devices, including Apple iPhone and Windows Mobile devices. Connecting through a simple and seamless process, users anywhere can easily access the resources they need. FirePass includes a state-of-the-art, integrated client that offers advanced roaming, domain detection, and automatic connection. The BIG-IP® Edge Client™ solution gives users fast application access to ensure continued productivity.

Improve security and PCI compliance

FirePass gives you granular access control on a group basis to ensure security for intranet resources. Using group policy enforcement, you can require client systems to comply with company policies. For example, employees can gain access to all intranet sites while partners are restricted to a specific web host. Non-compliant clients can be quarantined and passed to DMZ management processes for compliance updating. Group policy enforcement can help you achieve PCI compliance.

Gain ultimate flexibility

Available in both physical and virtual editions, FirePass gives you the flexibility to deploy according to your business needs. You can support up to 2,000* concurrent sessions on a single, easy-to manage device or virtual appliance. FirePass easily scales to support a worldwide rollout through integration with F5 BIG-IP® Local Traffic Manager.™

Reduce risk with endpoint security

Protecting your organization from unauthorized client device access is just as important as protecting against unauthorized users. FirePass provides endpoint security that quickly and easily verifies the user and ensures that connected devices are fully patched and protected in compliance with corporate policy. With FirePass, you can determine which resources the client can access, whether it's all, some, or none at all.

Decrease costs

Unlike IPSec VPN systems, FirePass SSL VPN does not require preinstalled client software and configuration. No client- or server-side application changes are necessary, so setup and management is fast and cost-effective. FirePass simplifies management and integrates with many third-party products to reduce your ongoing costs.

*Actual performance varies depending on hardware platform, resources available, and configuration. Customer is responsible for performance testing and scaling of FirePass Virtual Edition.

FirePass Features

- Network access for Windows, Mac, and Linux
- Virtual and physical editions
- Client integrity checking, including Mac and Linux
- Standalone Windows and VPN client
- BIG-IP Edge Client
  - Smart connection: location awareness and auto-connect
  - Windows logon credential reuse
- VMware View, Windows Terminal Services, and Citrix SmartAccess integrations
- Mobile device support
- Client/server application access
- Terminal server access
- Dynamic application tunnels
- Portal access to proxy-based web applications, files, and email
- User and two-factor authentication
- Content inspection and web application security
- Endpoint security and virus protection
- Protected workspace with encryption, file virtualization, and 64-bit OS support
- Visual Policy Editor
- Group policy enforcement and management
- CAPTCHA support
- Single sign-on support
- Inspection and validation of authorized hardware
- Role-based administration
- Logging and reporting
- GUI localization and customization
- iControl® SSL VPN client API

Learn more about FirePass

For more information about FirePass, use the search function on F5.com to find these resources.

Datasheet

FirePass SSL VPN

White papers

F5 FirePass Endpoint Security

Get to Know Group Policy Objects

Podcast

Secure Remote Access for Disaster Recovery

Case study

City of Diamond Bar Gives Its Vendors Secure, Reliable Access to Applications

F5 Networks, Inc. 401 Elliott Avenue West, Seattle, WA 98119 888-882-4447 www.f5.com

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com

IT agility. Your way.

CS04-00006 0710