



主要优势

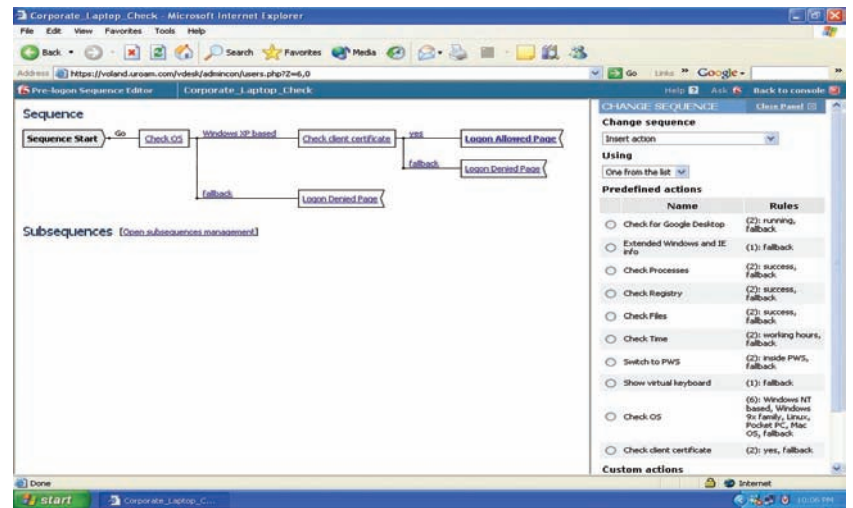
- **一流的策略管理**——独特的可视化策略编辑器能够提供直观、易用的“指向并点击”(point-and-click)界面，在降低管理成本的同时，轻松管理精细访问策略。
- **集成的端点安全性**——提供安全虚拟工作区、预先登录终端完整性检查，以及端点信任管理等功能，从而解除了您的后顾之忧，使您无需浪费精力于管理事务。
- **广泛的应用支持**——可实现从管理的及非管理的客户端设备从任何地方轻松、安全地访问电子邮件、Web门户、网络文件服务、终端服务、客户关系管理系统以及其它主要企业应用。
- **广泛的客户支持**——FirePass可提供广泛的多平台支持，允许用户从Windows(98、2000、ME、XP、Vista)、MAC、Linux和Pocket PC客户端安全访问网络。还支持全新的Vista客户端操作系统和IE7。
- **企业级可扩展性与性能**——在单一且易于管理的设备上可支持高达2,000个并发会话。通过与F5 BIG-IP本地流量管理器的集成，可支持几万个并发会话。借助任意IP应用流量的压缩和Web应用的服务器端高速缓存功能，可以优化最终用户的体验。
- **广泛的互操作性**——借助Active Directory、Radius、LDAP、PKI、RSA ACE及其它方式，为现有网络基础设施和身份管理系统提供支持。所提供的Web门户集成产品可支持Java applets、Javascript重写及其它技术(已通过VPNC认证)。
- **业内领先全球的高可用性**——与F5 BIG-IP广域流量管理器的独特集成，能够于发生站点灾难时在整个WAN上提供高度可用性。故障切换支持在站点内提供高度可用性。

一流的SSL VPN

F5的FirePass® SSL VPN设备通过采用标准Web浏览器为用户提供了一种安全访问企业应用和数据的方式。无论在家中还是在路上，FirePass出色的性能、可扩展性、易于使用特性以及安全特性，均有助于您提高工作效率，并保持企业数据的安全。

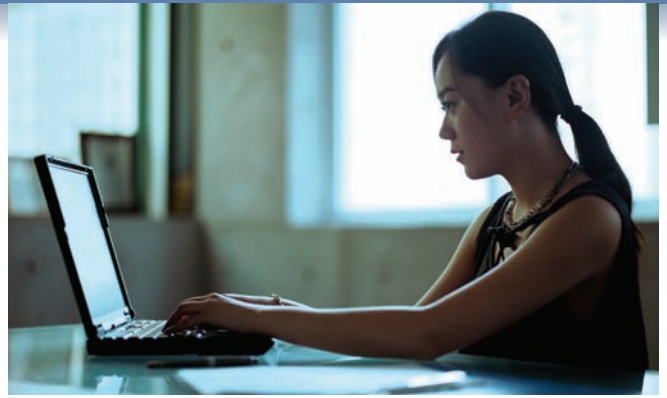
FirePass 可提供:

- 安全兼容系统自动侦测，防止病毒感染。
- 与业内数量最多的病毒扫描及个人防火墙解决方案(超过100种不同的防病毒(AV)和个人防火墙版本)自动集成。
- 自动拦截受感染的文件上传或电子邮件附件。
- 自动重新路由并隔离受感染或非兼容的系统，将其放入自我补救网络(self remediation network)中——以减少呼叫帮助中心的次数。
- 安全工作区可防止窃听及窃取敏感数据。
- 使用随机键输入系统进行安全登录，可防止按键记录器窃听。
- 由于能够与FirePass可视化策略编辑器完全集成，因此，可创建基于端点访问您的网络及您公司的安全配置文件的定制模板策略。



独特的可视化策略编辑器能够创建流程图样式的访问策略图形视图——通过“指向并点击”(point-and-click)方式，您能轻松配置并管理组、用户、设备或三者的任意组合。这一方式简化了端点策略的定义和管理，降低了管理成本，并提高了快速保护企业资源的能力。





网络访问



针对Windows (Vista, XP, 2000)、Mac、PocketPC和Linux系统的 FirePass 网络访问:

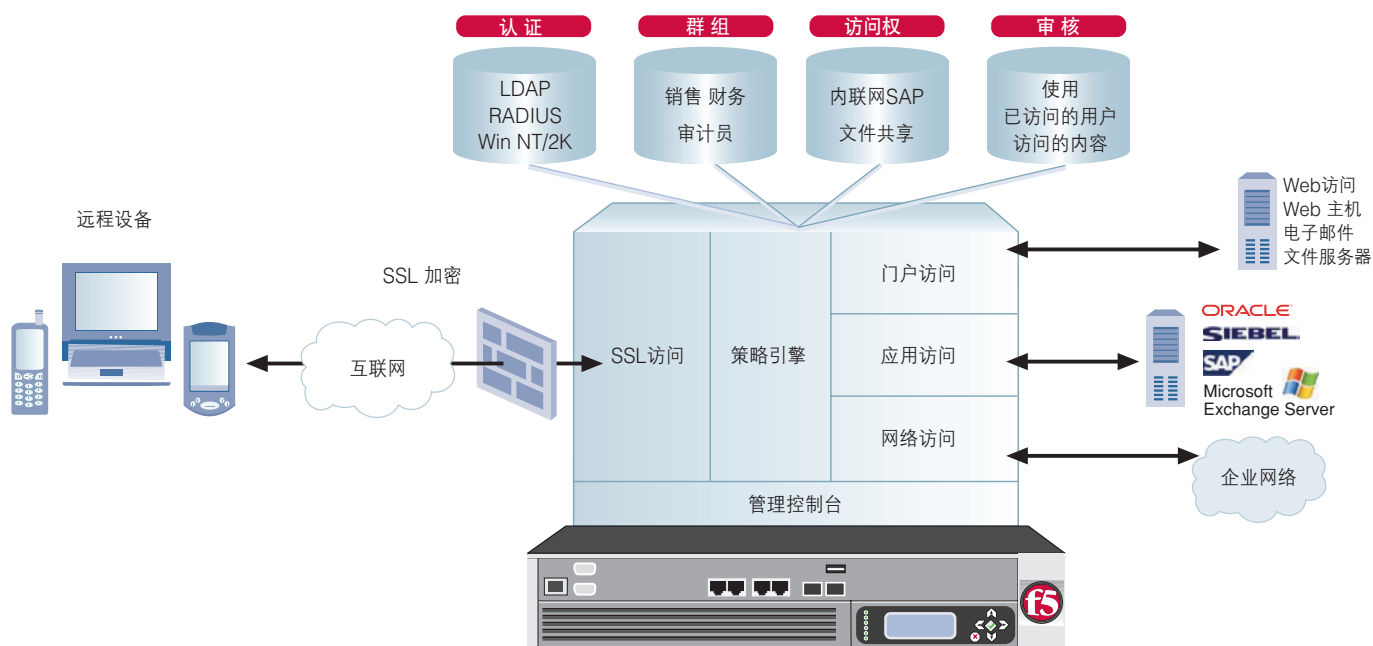
- Windows安装服务消除了FirePass客户端组件更新的特殊管理权限，从而降低了管理成本。
- 提供到面向所有基于IP (TCP, UDP) 应用的整个网络的安全远程访问。
- 具有所有台式机和笔记本电脑平台的标准特性，包括隧道分割、压缩、基于活动的时隙 (activity-based timeouts) 以及自动应用启动。
- 和传统IPSec VPN不同，无需在客户端进行软件预装以及远程设备配置，即可进行远程访问。同时也无需改变客户端或服务端应用。
- 允许管理员使用连接器，并通过制定网络或端口的访问限值规则来限制和保护资源的访问。
- 采用标准HTTPS协议，并以SSL作为传输协议，可支持所有HTTP代理，包括公共接入点、专用LAN以及任何不支持IPSec VPN的其它网络和ISP。
- 利用GZIP压缩。在对流量进行加密之前，首先进行压缩处理，从而减少互联网上传送的流量数量，进一步改善了性能。

客户端安全性

- **安全分割隧道**——当通过分割隧道进行网络访问时，为了防止后门 (backdoor) 攻击，FirePass提供了动态防火墙，以便在使用完全网络访问特性时保护 Win2k/XP 用户免受攻击。这一特性可阻止黑客通过客户机路由到企业网络上，或防止用户无意中流量发送到公共网络上。
- **客户机完整性检查**——FirePass通过在客户机进行完全网络访问之前检测是否存在所需进程 (如: 病毒扫描、个人防火墙、操作系统补丁级别、注册表设置等) 以及检测是否存在其它进程 (如: 键盘记录器)，来增强其安全性。

Windows网络访问特性

- **独立Windows客户端**——FirePass建立了一条完成用户认证之后的网络连接。软件使用微软的MSI installer技术，可自动被分配至客户端中。
- **Windows登录/GINA集成**——通过与GINA (“ctrl+alt+del”命令) 集成，支持用户简单、透明地登录至企业网络。
- **独立VPN客户端CLI** ——命令行界面支持通过与第三方应用 (如远程拨号软件) 相集成，提供单点登录支持。
- **Windows VPN拨号器**——简化最终用户体验，为用户提供更友好的拨号界面。
- **提供自动驱动器映射功能**——网络驱动器可被自动映射到用户的Windows电脑上。
- **提供静态IP支持**——当用户建立网络访问VPN连接时，可根据用户分配静态IP，这一方法大大降低了管理支持的成本。
- **透明网络访问**——消除网络访问浏览器Window弹出窗口，防止用户意外中断连接。



应用访问——对特定应用的安全访问

借助FirePass，管理员能够准许特定用户访问特定内容——例如，业务合作伙伴可使用并非由其本公司维护的设备，对特定的外联网应用和站点进行访问。FirePass只允许访问那些已经过系统管理员具体认可的应用，这一做法保护了网络资源。

特定客户端/服务器应用访问：

- 支持本地客户端应用通过浏览器与FirePass控制器之间的安全连接，与特定公司应用服务器进行通信。
- 无需用户预先安装或配置任何软件。
- 在网络端，被访问的应用服务器上无需使用额外软件。
- 采用标准HTTPS协议，并以SSL作为传输协议，因此可支持全部HTTP代理，包括公共接入点、专用LAN以及任何不支持传统IPSec VPN的其它网络和ISP。
- 所支持的应用包括Outlook、Exchange Cluster、被动式FTP、Citrix Nfuse和网络驱动映射。
- 管理员还能实现定制应用功能——包括客户关系管理 (CRM)，以及其它采用静态TCP端口的应用。
- 支持AppTunnels、Citrix、WTS应用的自动登录以简化最终用户的体验。
- 支持客户端应用的自动启动，以简化最终用户体验并降低支持成本。
- 通过提供独特的压缩支持功能，实现对WAN网络中客户机/服务器应用流量的压缩，从而获得更加优异的性能。

终端服务器访问

- 提供了一种基于Web的安全访问方式，可访问Microsoft终端服务器、Citrix MetaFrame应用、Windows XP远程桌面和VNC服务器等。
- 支持群组访问选项、用户认证、自动登录功能以及授权用户。
- 如果尚未在远程设备上安装，支持正确的终端服务或Citrix远程平台客户端组件的自动下载和安装，从而节省了时间。
- 支持远程访问XP桌面，以便使用RDP进行远端故障排除；使用内置VNC特性访问非XP桌面应用。

Dynamic AppTunnels

- 提供最大化支持，用于访问各种不同的客户端/服务器应用和基于Web的应用。
- 更好的选择，无需反向代理，即可从Windows客户端设备访问应用。
- 无需进行Web应用内容互操作行测试。
- 仅当安装时要求“高级用户”权限，执行时则不需任何特殊权限。
- 提供自动启动web应用渠道的附加支持，简化最终用户体验。

主机访问

- 能够对传统的VT100、VT320、Telnet、X-Term和IBM 3270/5250等应用进行基于Web的安全访问。
- 无需对应用或应用服务器进行修改。
- 无需使用第三方主机访问软件，降低了总体拥有成本 (TCO)。



门户访问——对web应用、文件及电子邮件的基于代理的访问

FirePass的门户访问能力支持任何装有浏览器 (Windows XP、Linux、Macintosh、Pocket PC、PDA等) 的操作系统。

在FirePass门户上可访问:

Web 应用

- 支持像在公司局域网里那样轻松访问内部Web服务器 (包括Microsoft Outlook Web Access、Lotus iNotes和MS SharePoint Portal)。
- 提供针对群组内联网资源的精细访问控制。例如, 员工可对整个内联网站访问, 而合作伙伴只能访问有限的特定Web主机。
- 访问资源时, FirePass可动态将内部URL映射到外部URL, 因此内部网络结构就不会泄露URL信息。
- 在 FirePass控制器上管理用户cookie, 以避免暴露敏感信息。
- 能够将用户证书发送给Web主机, 以支持自动登录以及其他用户对应用的特定访问。FirePass也可与现有身份管理服务器 (如Netegrity) 集成, 实现应用的单点登录。
- FirePass可代理Web主机上的登录请求, 以避免用户将密码高速缓存在客户端浏览器上。
- 精细访问控制 (ACL)——允许或限制对特定应用部分的访问, 从而增加安全性或降低业务风险。
- 为Web应用提供隧道分割支持, 可使最终用户访问公共网络站点时获得更快的性能。
- 对增加的Web应用 (反向代理) 提供动态的服务器端高速缓存功能, 缩短页面下载时间。
- 提供与设备无关的反向代理功能, 以重写Web页面中各种 Javascript内容, 从而节省了时间。

文件服务器访问

- 允许用户浏览、上传、下载、复制、移动或删除共享目录下的文件。
- 支持SMB共享、Windows 工作组; NT 4.0和Win2000域; 带有本地文件系统包的Novell 5.1/6.0, 以及NFS服务器。

电子邮件访问

- 提供基于安全Web、从标准和移动设备浏览器上对POP/IMAP/SMTP电子邮件服务器的访问。
- 允许用户发送和接收消息、下载附件以及将网络文件粘贴到电子邮件上。

移动设备支持

- 可通过PDA (如WAP和手机) 和iMode电话安全访问电子邮件和其它应用。
- 动态地对来自POP/IMAP/SMTP电子邮件服务器的电子邮件进行格式调整, 以便适应移动电话和PDA的较小屏幕。
 - 能够发送以网络文件作为附件的电子邮件, 并能查看文本或者Word文档。
 - ActiveSync支持——支持ActiveSync应用, 允许PDA从PDA设备的Exchange服务器上同步电子邮件和日历, 且无需预先安装VPN客户端组件。

门户访问——全方位的安全性

FirePass提供多层控制功能, 可确保从公共系统安全访问信息。

客户机安全性

- **受保护工作区**——Windows 2000/XP的用户可自动切换至受保护工作区, 来进行远程访问会话。在受保护工作区模式中, 用户无法将文件写入到受保护工作区和临时文件夹外的任何位置, 并且所有的内容都将在会话结束时被删除。
- **高速缓存清除**——高速缓存清除控件可删除在远程访问会话期间来自客户端电脑的下列数据: Cookies、浏览器历史记录、自动完成信息、浏览器高速缓存、临时文件、以及所有安装的ActiveX控件。同时它还可清空回收站数据。
- **安全虚拟键盘**——对于额外的密码安全方面的需求, FirePass提供了已申请专利的安全虚拟键盘功能, 它借助鼠标 (而不是键盘) 来实现安全的密码输入。
- **下载拦截**——对于无法安装“清除”控件的系统, 可配置FirePass以拦截所有文件的下载, 从而避免发生无意间遗留临时文件的情况, 同时还能对应用进行访问。

内容检测和Web应用安全

针对那些通过企业网络进行Web应用访问的用户, FirePass通过扫描Web应用访问以查找应用层攻击并在发现攻击时拦截访问的方式, 来增强应用的安全性, 并确保应用层免受攻击。

集成病毒防护功能

FirePass采用基于ICAP API的集成扫描仪或外部扫描仪对Web和文件上传进行扫描。这样, 受感染的文件在网关就会被阻断而无法访问网络中的电子邮件或文件服务器, 从而加强了防护。

动态策略引擎——整体管理控制

借助FirePass策略引擎，管理员可轻松管理用户认证和授权。

基于动态策略的访问

借助FirePass策略引擎，管理员可对网络资源进行快速而精细的控制。在这一策略支持下，管理员可根据用户和所用设备来授权应用访问。

用户认证

缺省模式下，系统将密码对照内部FirePass数据库进行认证。经配置后，FirePass还支持RADIUS、活动目录、RSA双因素、LDAP认证、基于表格的基本HTTP认证，以及身份管理服务器(如Netegrity)与Windows域名服务器认证等方式。

双因素认证

许多企业都采用“双因素”认证方式，这是一种使用用户ID与密码以外的信息进行认证的方式。FirePass完全支持领先的RSA SecurID®令牌式认证以及RSA纯粹ACE认证。

客户端证书/PKI 支持

FirePass支持管理员根据用来访问FirePass控制器的设备类型来限制或允许访问。FirePass可在用户登录期间检查客户端是否有电子证书。根据该电子证书的核查结果，FirePass可支持更广泛的应用访问。FirePass还将客户端证书作为双因素认证的一种方式，并禁止无有效客户端证书的用户访问所有网络。

群组管理

访问权限可分配给单个用户或用户群(如：“销售人员”、“合作伙伴”、“IT支持人员”)。这样，FirePass就可限制个人和用户群访问特定资源。

动态组映射

FirePass利用不同的动态组映射机制，如活动目录(Active Directory)、RADIUS、LDAP、客户端认证凭证、登录URI、虚拟主机名称，以及预先登录会话变量等，将用户映射至FirePass组。

会话超时及限制

管理员可对闲置及会话超时情况进行配置，以防止黑客控制用户(在信息遗忘注销的用户)发出的会话。

基于角色的管理

该管理方式通过向一些管理员用户提供注册新用户、终止会话、重设密码等管理功能，提高了组织机构的灵活性，但同时也保证了不向他们泄露所有功能(如关闭服务器及删除证书)

日志与报告

FirePass为日志用户、管理员、会话、应用及系统事件提供内置日志支持。此外，FirePass还提供系统日志格式，可用于与外部系统日志服务器相集成。管理控制台提供范围广泛的审核报告，以通过安全审核。汇总报告将根据日期、时间、访问操作系统、



使用特性、访问的Web站点、会话持续时间和会话终端类型及其它用户指定的时间间隔信息来汇总网络使用情况。

定制

最终用户图形界面(GUI)的本地化

FirePass支持将最终用户网页上包括特性名称(如Web应用)在内的所有字段进行本地化。借助此项功能，企业不仅可本地化用户收藏夹，还可本地化所有最终用户图形界面，从而使应用更加简化。

完成登录及WebTop定制

凭借FirePass，管理人员完全可以定制一套完整的登录流程，并使webtop网页与现有的企业网络站点门户实现最佳匹配；为了改善最终用户体验，FirePass允许使用WebDAV功能上传定制页面。

针对安全应用访问的 iControl SSL VPN 客户端API

由于只有SSL VPN产品具备开放式API和SDK，因此FirePass通过提供安全的系统到系统或应用到应用的通信，来实现对Win32客户端(98、2000、XP、VISTA)应用的自动、安全访问。现在，无需用户登录VPN，应用便可自动、透明地启动和关闭网络连接。这使最终用户能够更快速、更轻松地进行连接，同时降低了客户端应用安装成本。

集群

为支持大型部署，可将多个FirePass 4100或4300设备进行集群。对于高性能大容量集群，客户通过卸载SSL终端到BIG-IP上，可充分利用F5 BIG-IP的独特集成特性。能够在—个集群中处理儿万个并发会话，同时可实现SSL VPN集群的最大性能。

故障切换

FirePass控制器支持服务器对(在线服务器与备用服务器)间的故障切换，从而在主单元发生故障时，用户不必要重新登录到另一个FirePass。

订购信息

FirePass 4300系列

FirePass 4300控制器是专为大中型企业和运营商而精心设计的2U机架安装式服务器。它支持多达2000个并发用户采用四核CPU获得最佳性能。此外，FirePass 4300还支持内置的冗余电源和可选的千兆光纤端口。



FirePass 4300 系列



FirePass 4100 系列



FirePass 1200 系列

FirePass 4100系列

FirePass 4100控制器是专为大中型企业精心设计的2U机架安装式服务器。它可支持多达2000+并发用户，为基于Web方式安全远程访问企业应用和桌面提供了一套全面的解决方案。

FirePass 1200系列

FirePass 1200控制器是专为中小型企业精心设计的1U机架安装式服务器。它支持10-100个并发用户，为基于Web方式安全远程访问企业应用和桌面提供了一套全面的解决方案。

	4300 大中型企业、 服务提供商	4100 中型企业	1200 中小型企业 和分支办事处
面向的公司规模 (员工数量)*	2500 至几万	250 至 2500	50 至 250
建议并发用户的数量 (以性价比为依据)*	2000	500	100
每台设备的最大 并发用户数量	2000	2000	100
所包含的以太网端口	4 (10/100/100)	4 (10/100/1000)	2 (10/100)
CPU 速度	四核	双核	单核
基本内存	8GB	4GB (4110、4120及 4130) 和 8GB (4140、 4150)	512MB
冗余电源	有 (内置)	可选	无
可选光纤端口	有 (2个)	无	无
集群	有	有	无
故障切换	有	有	有

规格

FirePass 4300

电源: 冗余460W (内置)

重量: ~40磅

尺寸大小: 17.5英寸(宽)x 24.5英寸 (OAL)
/23.5英寸(深) (安装把手后面) x 3.5英寸(高)

认证:

美国/加拿大-ANSI/UL 60950和CAN/CSA
No.60950

欧盟-低电压指令-EN 60950

欧盟-EMC指令-EN 55022, EN 55024,

EN 61000-3-2以及EN 61000-3-3

CE

工作温度: 0-40°C

湿度: 40°C时为5-85% (无冷凝)

FirePass 4100

电源: 400 W (带有冗余选项)

重量: ~36 磅

规格尺寸: 17.5英寸(宽)x24.5英寸(OAL)
/23.5英寸(深) (安装把手后面) x3.5英寸(高)

认证:

美国/加拿大-ANSI/UL 60950和CAN/CSA
No.60950

欧盟-低电压指令-EN 60950

欧盟-EMC指令-EN55022, EN 55024,

EN 61000-3-2以及EN 61000-3-3

CE

工作温度: 0-40°C

湿度: 40°C时为5-85% (无冷凝)

FirePass 1200

电源: 180W (内置)

重量: ~10磅

尺寸大小: 16.7英寸x 1.7英寸/11英寸

认证:

美国/加拿大-UL-UL 1950

欧盟-低电压指令-EN 60950

欧盟-EMC指令-EN 50081-2 和 EN
61000-6-2

CE

工作温度: 0-40°C

湿度: 40°C时为5-85% (无冷凝)



<http://www.f5.com.cn>

F5公司北京代表处

地址: 北京市朝阳区建国路79号
华贸中心1号写字楼17层

邮编: 100025

电话: 010-59234000

传真: 010-59234100

F5公司上海代表处

地址: 上海市虹桥路3号
港汇中心2座2710室

邮编: 200030

电话: 021-61132588

传真: 021-61132599

F5公司广州代表处

地址: 广州市环市东路368号
花园酒店花园大厦1035室

邮编: 510064

电话: 020-83884169

传真: 020-83883897