



主要内容:

- 2 更优秀的用户体验
- 3 网络访问
- 5 应用访问—安全访问特定应用
- 6 门户访问—以基于代理的方式访问Web应用、文件和电子邮件
- 8 门户访问-全面安全性
- 9 动态策略引擎—全面管理控制
- 11 定制
- 12 针对安全应用访问的iControl SSL VPN客户端API
- 12 FirePass产品细节
- 14 FirePass规格
- 16 更多信息



通过灵活、安全的远程访问提高工作效率

随着越来越多的移动和远程员工采用日益增多的不同设备从任何地点访问企业应用和数据，企业将拥有更灵活、效率更高的用户。但是，防止应用、数据、网络和设备免遭未经授权访问和工具可能会迅速提高管理复杂度和成本。

FirePass[®] SSL VPN设备和虚拟版 (VE) 使用户能够通过任何设备或网络安全地远程访问企业应用和数据。FirePass通过提供卓越的性能、扩展能力、可用性、策略管理和终端安全，保证了对应用的轻松访问。这样实现了统一的安全策略执行和访问控制，从而提高了工作人员的敏捷性和工作效率。

主要优点:

提高员工的工作效率

实现从任何地点、任何设备以快速、安全、始终连接的方式进行远程访问。

实现最高的灵活性

快速且轻松地部署虚拟设备，为您现有的虚拟基础设施增加远程访问功能。

降低成本

通过轻松管理、简单部署以及安全的应用访问而降低部署和支持成本。

提高安全性

提供针对群组内联网资源的精细访问控制，以增强安全性。

通过终端安全而降低风险

借助终端安全功能快速且轻松地验证用户，以确认遵循企业政策。



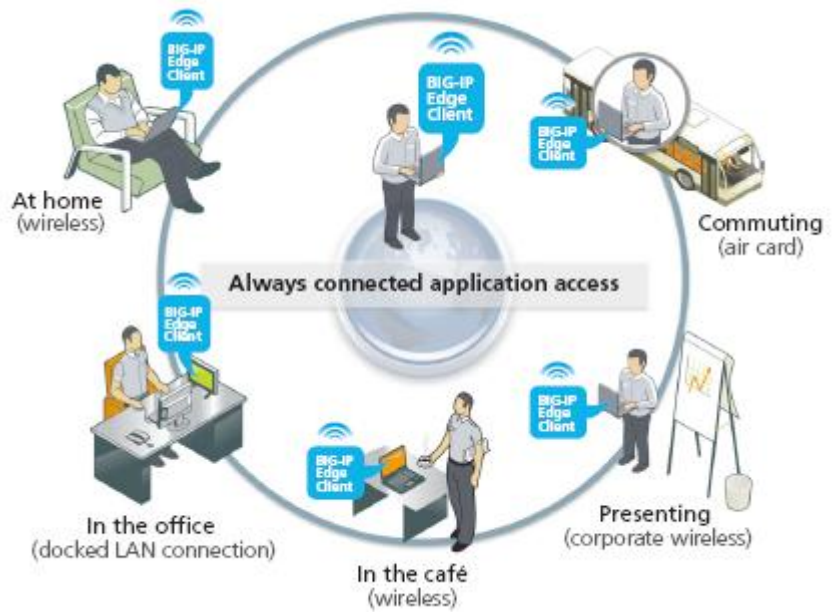
更优秀的用户体验

FirePass通过最大限度减少访问授权文件和应用所需的时间和工作量，从而有助于保证用户的工作效率。

“始终连接”的远程访问

某些接入客户端需要用户在不同地点移动或者重启应用时进行全天不间断地重新连接。**BIG-IP® Edge Client™**解决方案是一个先进的集成化客户端，提供了位置感知能力和区域确定能力，从而提供了与众不同的远程访问解决方案。当用户在不同地点间移动时，先进的漫游、地域检测和自动连接能力提供了无缝的切换。**BIG-IP Edge Client**有助于保证连续的高效率，无论用户是在家中使用无线网、在途中使用无线网卡连接、通过企业无线网发表演讲、在咖啡厅使用异地无线网，或者使用LAN连接。FirePass 6.1和7.0都支持**BIG-IP Edge Client**。

BIG-IP Edge Client采用领先的漫游、地域检测和自动连接技术，提供了地点间的无缝切换。



无缝的VPN接入

当用户在Windows过程中第一进入输入证书时，**BIG-IP Edge Client**缓存证书，然后在第一次尝试登录VPN时自动尝试。这优化了用户体验，从而有助于提高工作效率。

网络访问

FirePass通过支持现有的网络基础设施、身份管理系统和客户端/服务器操作系统，为所有应用提供了类似LAN的网络访问能力。

针对Microsoft Windows（Windows 7、Vista、XP）、Mac和Linux系统的FirePass网络访问

- 利用Windows Installer Service，消除了FirePass客户端组件升级时对特殊管理权限的需求，从而降低了管理成本。
- 提供了对整个网络中所有基于IP的（TCP、UDP）应用的安全远程访问。
- 包含所有桌面和笔记本电脑平台的标准特性，以及分割隧道、压缩、基于活动的超时时间和自动应用启动。
- 提供远程访问—与IPSec VPN不同—不需要预先安装客户端软件可配置远程设备。不需要更改客户端或服务器端的应用。
- 通过制订规则限制对特定网络或端口的访问，从而允许管理员限制和保护通过连接器访问的资源。
- 使用带有SSL作为传输机制的标准HTTPS协议，因此，设备通过所有HTTP代理工作，包括公共接入点、专用LAN，并通过不支持IPSec VPN的网络和ISP接入。
- 采用GZIP压缩算法，在加密之前对流量进行压缩，减少在互联网上传输的流量，并提高性能。
- 支持最新的操作系统和浏览器—FirePass 7.0支持32位版本的Windows 7、Vista和XP；Mac OS X Leopard和Snow Leopard；Internet Explorer 6、7和8；Firefox 3.x；以及Safari 4。它支持64位版本的Windows 7、Vista和XP；Linux（请向F5或分销人员索要完整列表）、Internet Explorer 7（Win 7除外）和8；以及Firefox 3.0。请咨询F5销售代表或分销人员，了解与您的环境的兼容性。

客户端安全

- 安全的分割隧道—为了防止在采用分离隧道访问网络时遭受后门攻击，FirePass提供了一个动态防火墙，以便在使用完全网络访问特性时保护Windows、Mac和Linux用户免受攻击。这一特性可阻止黑客通过客户端路由到企业网络上，或防止用户无意中将流量发送到公共网络上。
- 终端客户端检查—FirePass通过在客户端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、反恶意软件、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。
- 硬件终端检测器—FirePass检测客户端的特性，例如MAC地址、CPU ID和HDD ID，以识别远程识别。FirePass对机器授权时，不需要部署机器证书的复杂过程。

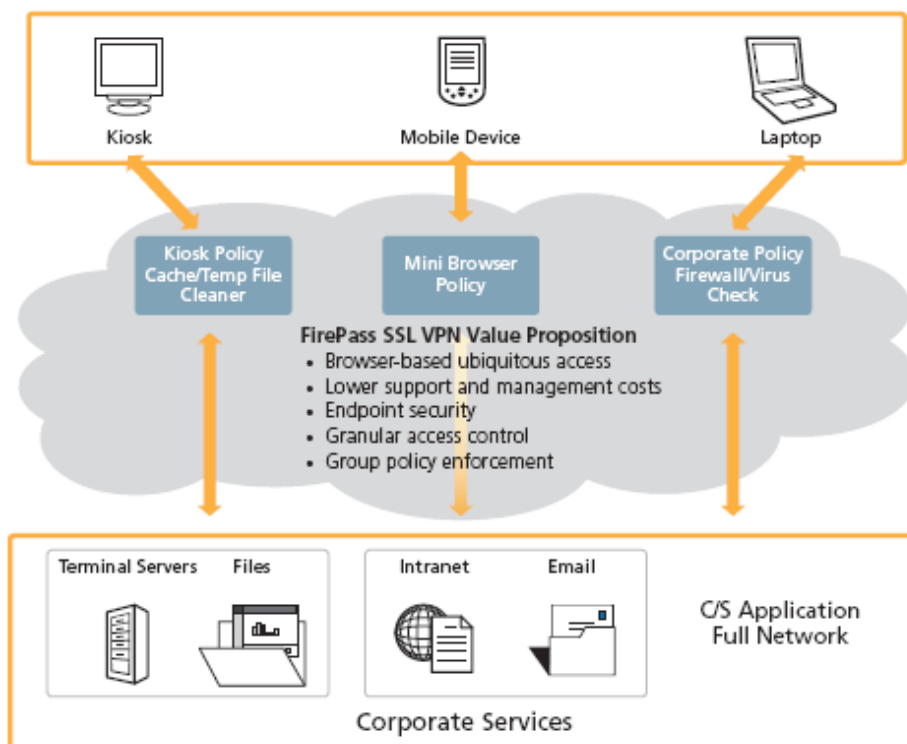
Windows网络访问特性

- 独立Windows客户端—FirePass在完成用户认证之后建立了一条网络连接。软件使用微软的MSI安装程序技术，可自动被分发到客户端中。
- Windows登录/GINA集成—通过与GINA ("Ctrl + Alt + Del"提示符)集成，支持用户简单、透明地登录到企业网络。
- 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，提供单一登录支持。
- 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。
- 自动驱动器映射—网络驱动器可被自动映射到用户的Windows电脑上。
- 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，从而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弹出窗口，防止用户意外中断连接。

移动设备支持

- 实现从Windows Mobile和智能电话安全地访问应用。
- 提供对客户端/服务器和基于Web的应用的访问。

FirePass策略应用安全地访问全部企业服务，包括信息台、移动设备或笔记本电脑。



应用访问—安全访问特定应用

FirePass允许管理员准许某些用户—例如，使用并非由本公司维护的设备的业务伙伴—访问特定的外部网络应用和站点。FirePass只允许访问那些已经过系统管理员认可的应用，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设备之间的安全连接，与特定公司应用服务器进行通信。
- 无需预先安装或配置任何软件。
- 在网络端不需要任何额外软件即可访问应用服务器。
- 采用标准协议访问应用，如HTTP和SSL/TLS。它支持所有HTTP代理、接入点和专用LAN，并可通过不支持传统IPSec VPN的网络和ISP进行访问。
- 包含支持的应用，例如Outlook、Exchange Clusters、被动式FTP、Citrix Nfuse和网络驱动器映射。
- 支持定制CRM应用和采用静态TCP端口的应用。
- 支持自动登录到AppTunnels、Citrix和WTS应用，以简化用户体验。
- 与Citrix SmartAccess集成，以向Citrix应用提供终端检测结果，并根据终端扫描结果向XenApp发送SmartAccess过滤器。
- 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。
- 允许对非Windows和Windows系统锁定基于Java的通道，以防止ActiveX控件的执行。
- 对进行网络访问的客户端提供完整的DHCP支持，自动进行IP地址分配和地址的动态DNS注册。DHCP支持能力提供了更轻松的多单位部署，而远程访问IP地址范围可与内部LAN重叠。
- 通过门户访问提供对Microsoft Communicator的支持，从而增强VoIP通信能力。
- 通过提供独特的压缩支持功能，实现对WAN网络中客户端/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。
- 为VMware View Web客户端提供终端服务，使用户能够从虚拟桌面进行访问。
- 支持群组访问选项、用户认证以及授权用户的自动登录功能。
- 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和带有内置VNC特性的非XP平台进行远程故障排除。
- 对Citrix和Microsoft提供基于Java的终端服务支持。

动态应用隧道

- 为访问各种不同的客户端/服务器应用和基于Web的应用提供最大化支持。
- 提供比反向代理更好的选择，用于从Windows客户端设备访问应用。
- 无需进行Web应用内容互操作性测试。
- 仅在安装时要求“高级用户”权限，执行时则不需任何特殊权限。
- 为自动启动web应用隧道提供额外的支持，简化最终用户体验。

主机访问

- 安全地基于Web方式访问旧有的VT100、VT320、Telnet、X-Term和IBM 3270/5250应用。
- 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—基于代理访问Web应用、文件和电子邮件

FirePass的门户访问能力支持任何装有浏览器的客户端操作系统：Windows、Linux、Mac、智能电话、PDA等。

Web应用

- 支持像在公司局域网中那样轻松访问内部Web服务器，包括Microsoft Outlook Web Access、Lotus iNotes和Microsoft SharePoint Server。
- 提供根据群组策略对内部网资源的精细访问控制。例如，员工可访问整个内部网站点，而合作伙伴只能访问有限的特定Web主机。
- 动态地将内部URL映射到外部URL，使内部网络结构不会泄露URL信息。
- 在FirePass设备级别管理用户cookie，以避免保留敏感信息。
- 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还与现有的身份管理服务器（如CA Netegrity）集成，实现应用的单一登录。
- 代理来自Web主机的登录请求，避免用户将密码缓存到客户端浏览器上。
- 通过精细访问控制列表 (ACL)，允许或限制访问应用的特定部分，从而提高安全性，并降低业务风险。

- 为Web应用提供分割隧道支持，使用户访问公共网站时获得更快的性能。
- 利用高速反向代理验证后端证书，以快速验证服务器的证书。
- 提供动态的服务器端和DNS缓存，以提高Web应用（反向代理）性能，并加快页面下载。
- 提供现成的反向代理支持，用于在网页中写入大量不同的JavaScript内容，从而节省时间。
- 提供Java补丁ACL支持，以使用门户接入能力通过FirePass限制客户端发起的连接。
- 为访问Web应用提供NTLMv2支持。
- 提供DNS中继代理服务，实现客户端名称解析，而不需要任何特殊的运行时权限（例如，主机的修改）。同时重定向端口，更全面地支持Outlook 和Windows驱动器映射等应用。

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

- 以安全的基于Web的方式从标准和移动设备浏览器访问POP/IMAP/SMTP电子邮件服务器。
- 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

- 通过Apple iPhone、Windows Mobile、PDA、智能电话、手机、WAP和iMode电话安全地访问电子邮件和其它基于Web的应用。
- 动态地对来自POP/IMAP/SMTP邮件服务器的电子邮件进行格式化处理，以适应手机和PDA的较小屏幕。
- 支持发送以网络文件作为附件的电子邮件，并支持查看文本或者Word文档。
- 支持ActiveSync应用，使PDA能够从PDA设备的Exchange服务器上同步电子邮件和日历，而无需预先安装VPN客户端组件。

门户访问—全方位的安全性

FirePass提供了多个控制层，以保证从公共系统访问的信息的安全。

客户端安全性

- 受保护工作区—Windows XP/Vista/7的32位版本或者Windows Vista/7的64位版本用户可自动切换至受保护的工作区，以进行远程访问会话。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外的任何位置，并且临时文件夹和其中所有的内容都将在会话结束时被删除。
- 缓存清理—缓存清理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、自动完成的信息、浏览器缓存、临时文件以及所有安装的**ActiveX**控件，同时清空回收站。
- 安全虚拟键盘—对于额外的密码安全需求，**FirePass**提供了已申请专利的安全虚拟键盘功能，借助鼠标（而不是键盘）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，**FirePass**可通过配置而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。
- 自动文件虚拟化—在受保护工作区模式下，临时文件和注册表设置被写入虚拟文件系统，而非本地机器。
- 已保存内容的加密—所有保存到远程系统上的临时内容都经过加密，以防受保护工作区未正常退出，例如断电、提交不可读的内容。
- 门户对常见移动客户的支持—**FirePass**支持通过**iPhone**、**BlackBerry**和**Opera Mini**浏览器访问门户。

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阻止访问的方式，以增强应用的安全性，并确保应用层免受攻击（例如跨站点脚本、无效字符、SQL注入、缓存溢出）。

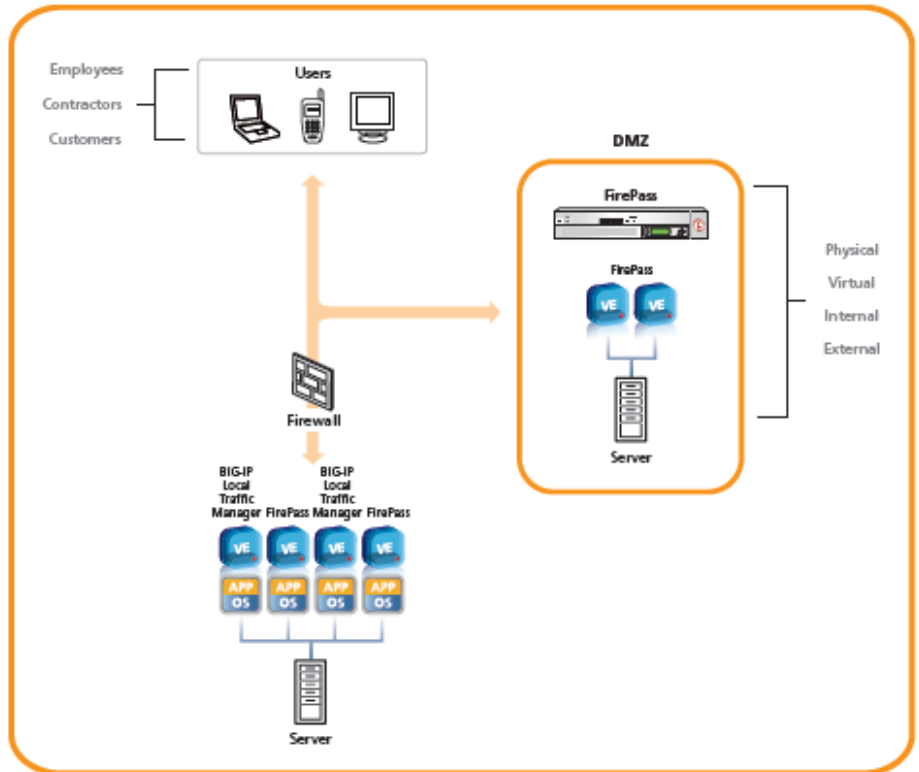
集成的病毒防护功能

FirePass可以使用集成式扫描仪或者外部扫描仪通过**ICAP API**对Web 和文件上传进行扫描。受感染的文件在网关就会被阻止，而不允许到达网络上的电子邮件或文件服务器，从而增强保护能力。

灵活的远程访问

FirePass虚拟版 (VE) 可以轻松地快速部署虚拟设备，为现有虚拟基础设施增加**SSL VPN**功能。这在灾难恢复场景中或者在远程访问需求激增时提供了更大的灵活性。**FirePass**虚拟版和**BIG-IP**本地流量管理器可以结合使用，在相同的环境中提供业界领先的应用交付和远程访问。

FirePass VE 可轻松地向您现有的虚拟环境添加灵活的远程访问能力。



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权限。

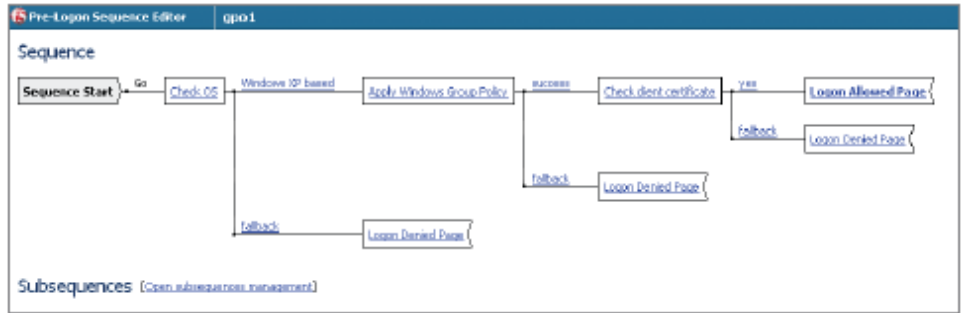
动态的基于策略的访问

管理员可对网络资源进行快速而精细的控制。提供对策略管理的支持，管理员可根据用户和所用设备来授权应用访问。管理员可以通过导入和导出预登录策略而轻松地实施现有策略。

可视化策略编辑器

可视化策略编辑器为您的访问策略创建了流程图样式的图形化视图。使您能够在确定和管理群组、用户、设备或这三个方面的任意组合时轻松地点击。这简化了终端策略的定义和管理，降低管理成本，并且提高快速确保企业资源受到保护的能力。

可视化策略编辑器可轻松地制订访问策略。



用户认证

系统通过将密码与内部FirePass数据库进行对比而认证用户。在经过简单配置后，FirePass也可以支持RADIUS、Active Directory、RSA双因子、LDAP认证方法、基础认证和基于表格的HTTP认证、身份管理服务器（例如Netegrity）和Windows域服务器。通过Active Directory，用户可以更改当前或过期的密码，并在密码即将过期时受到警告。对嵌套Active Directory配置的支持使用户能使用更复杂的分层目录结构。

双因子认证

许多企业都采用“双因子”认证方式（例如令牌或智能卡），这种方法不仅需要用户ID和密码。FirePass支持双因子认证，包括RSA SecurID® Native ACE认证。

问题回答测试

管理员可以实施CAPTCHA。这是一种简单的问题回答测试方法，适用于负责保护企业免遭DOS和基于脚本的暴力攻击的人员。



CAPTCHA可防止DoS和基于脚本的暴力攻击。

客户端和机器认证/PKI支持

FirePass与现有PKI基础设施无缝集成，允许管理员根据访问FirePass所用的设备而限制或允许访问。FirePass可以在用户登录过程中检查客户端数字证书或Windows机器证书的状态。根据有效证书的状态，FirePass可耿直访问更多的应用。FirePass还可以将客户端或机器证书作为双因子认证的一种方式，并禁止无有效证书的用户的所有网络访问请求。

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人员”）。这样，FirePass就可限制个人和用户群访问特定资源。

群组策略执行

群组策略提供了一种独有的机制，可对不是网络域一部分的客户端系统应用和执行策略。您可以使用可视化策略编辑器以模板形式设计群组策略，以限制用户权限和访问，同时满足PCI、HIPAA和GLBA法规。（注：群组策略对象仅适用于Active Directory。）

动态组映射

FirePass利用不同的动态组映射机制，如Active Directory、RADIUS、LDAP、客户端证书、登录URI和虚拟主机名以及预登录会话变量等，将用户动态映射至FirePass组。

单一登录 (SSO) 支持

SSO配置采用认证会话变量从证书中提取SSO信息，并从用户名和密码设置中提取认证信息。高级会话变量有助于系统管理员扩展并定制FirePass，使管理员能够处理和创建新的会话变量，以实现定制的部署。管理员还可以收集和获取RADIUS属性以及LDAP、Active Directory和证书字段值。

会话超时与限制

管理员可对不活动时间及会话超时时间进行配置，以防止黑客试图控制用户(在网吧忘记注销的用户)发出的会话。

基于角色的管理

提供能够灵活地向某些管理员用户提供一些管理功率(如注册新用户、终止会话、重新设置密码)，而不向他们泄露所有功能(例如，关闭服务器或者删除证书)。

日志与报告

FirePass为记录用户、管理员、会话、应用和系统事件提供了内置了日志支持能力。此外，FirePass以silo格式提供日志，以实现与外部syslog服务器的集成。管理控制台提供了大量审计报告，有助于遵循安全审计要求。汇总报告根据日期、时间、访问的操作系统、使用的特性、访问的网站、会话持续时间、会话终止类型和用户指定的时间间隔信息汇总网络使用情况。单个URL用于以HTML或电子表格格式检索汇总/群组报告。

定制

FirePass提供了先进的定制特性，使管理员能够设计独特的GUI，或者使现有的企业网站以最佳方式反映企业和用户的要求。

本地化用户GUI

FirePass对用户网页上的所有字段进行本地化处理，包括特性的名称(例如，Web应用)。这有助于企业本地化用户GUI，而不仅仅是用户收藏夹——从而提高业务价值，并降低总体拥有成本。

全面的登录和Webtop定制

凭借FirePass，管理员可以全面地定制整个登录过程和webtop网页，使其与现有的企业网站门户实现最佳匹配。管理员可以使用WebDAV能力上传定制网页，以增强用户体验。

针对安全应用访问的iControl SSL VPN客户端API

作为市场上唯一采用开放式客户端API和SDK的SSL VPN产品，FirePass通过提供安全的系统到系统或应用到应用的通信，实现了对Win32客户端操作系统（XP、Vista、7）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。

FirePass产品细节

FirePass设备和虚拟版产品可满足小型及大型企业的并行用户访问需求。

FirePass 1200

FirePass 1200设备针对中小型企业 and 分支机构而设计，可支持10至100个并行用户。

FirePass 4100

FirePass 4100控制器针对中型企业而设计，而且从性价比角度讲，建议拥有500个并行用户的企业使用。

FirePass 4300

FirePass 4300设备针对大中型企业和服务提供商而设计，可支持2000个并行用户。

FirePass虚拟版

FirePass虚拟版运行于VMware ESX 4.0虚拟环境中，是针对大中小企业和服务提供商而设计的，可支持多达2000个并行用户。

集群

FirePass 4100和4300设备与虚拟版都内置了集群支持功能。这些产品可以与F5 BIG-IP® 广域流量管理器™ 和BIG-IP® 本地流量管理器™ 结合使用，提供业界领先的扩展能力、性能和可用性。

故障切换

FirePass设备和虚拟版也可以经过配置，实现一对服务器（活动服务器和备用服务器）之间带状态信息的故障切换，以避免在可能出现主单元故障时必须重新登录另一个FirePass设备或虚拟版。

SSL加速器硬件选项

FirePass 4100提供了独特的硬件SSL加速选项，可减轻SSL密钥交换和SSL流量的加密与解密负荷。对于大企业环境中需要大量处理能力的加密，例如3DES和AES，这些选项可显著提高性能。

FIPS SSL加速器硬件选项

FirePass符合FIPS规范*，满足政府、金融机构、医疗机构和其它对安全要求较高的组织的安全需求。FirePass 4100和4300设备提供了对FIPS 140 2级防篡改型SSL密钥存储的支持，并采用经FIPS认证的加密支持能力对硬件的SSL流量进行加密和解密。FIPS SSL加速器是4100和4300基础平台的出厂安装选项。

* FIPS 140-2满足GESG（英国国家信息保障技术局）关于使用私有数据流量的安全标准。

FirePass规格

FirePass设备包含三种型号，并可提供虚拟版，满足各种规模的企业并行用户访问需求。



FirePass 虚拟版

虚拟版规格

建议连接的用户数量:	2000人*
集群支持:	支持 – 最多10个虚拟设备

*注：实际性能取决于硬件平台、可用资源和配置。客户负责FirePass虚拟版的性能测试和扩展。

主机系统要求 强烈建议主机系统包含基于AMD-V或Intel-VT技术的CPU。

系统管理程序:	VMware ESX 4.0或ESXi 4.0 VMware vSphere客户端 VMware虚拟硬件版本7
处理器:	1 CPU (建议使用4个或更多CPU，以支持超过500个并行用户)
内存:	2 GB RAM (建议配置8 GB或更高内存，以支持超过500个并行用户)
网络适配器:	3个网络接口
磁盘空间:	30 GB精简配置硬盘



4300和4100系列



1200系列

物理规格	4300	4100	1200
建议连接的用户数量:	2000	500	100
每个设备连接的最大用户数量:	2000	2000	100
接口:	4个 (10/100/1000) LAN端口	4个(10/100/1000) LAN端口	2和(10/100) LAN端口
尺寸:	3.5" H x 17.5" Wx 23.5" D 2U行业标准机架安装机箱	3.5" H x 17.5" Wx 23.5" D 2U行业标准机架安装机箱	1.7"Hx16.7"Wx11"D 1U 行业标准机架安装机箱
重量:	43磅	40磅	10磅
处理器:	两个Opteron 2.2 GHz – 双核	两个Opteron 2.0 GHz – 单核	Intel Celeron 2.0GHz – 单核
电源:	双475 W 90/240 +/- 10% VAC自动切换	425 W 90/240 +/- 10% VAC自动切换 可选冗余电源	单个全频250 W
典型功耗:	275 W	275 W	180 W
最大发热量:	939 BTU/小时	939 BTU/小时	785 BTU/小时
设备冗余:	看门狗定时器、故障安全电缆（主副）	看门狗定时器、故障安全电缆（主副）	看门狗定时器、故障安全电缆（主副）
集群支持:	支持 – 最多10个设备	支持 – 最多10个设备	不支持
FIPS SSL加速器卡选项:	支持-仅出厂配置	支持-仅出厂配置	不支持
硬盘容量:	160 GB	160 GB	40 GB
RAM:	标准8 GB	在4110、4120、4130上标准4 GB – 可在出厂前升级至8 GB（4140和4150标准8 GB）	512 MB
温度（运行）:	41°F至104°F（5°C至40°C）	41°F至104°F（5°C至40°C）	41°F至104°F（5°C至40°C）
非运行时的周围环境温度范围:	-40°F至149°F（-40°C至65°C） 相对湿度：40°C时为10%-95%，非冷凝	-40°F至149°F（-40°C至65°C） 相对湿度：40°C时为10%-95%，非冷凝	-40°F至149°F（-40°C至65°C） 相对湿度：40°C时为5%-85%，非冷凝
相对湿度:	40°C时为20%至90%	40°C时为20%至90%	40°C时为20%至90%
安全机构认证:	UL 60950 (UL 1950-3), CSA-C22.2 No 60950-00 (UL 60950双国家标准) IEC 950的CE测试认证, EN 60950	UL 60950 (UL 1950-3), CSA-C22.2 No 60950-00 (UL 60950双国家标准) IEC 950的CE测试认证, EN 60950	UL 60950 (UL 1950-3), CSA-C22.2 No 60950-00 (UL 60950双国家标准) IEC 950的CE测试认证, EN 60950
电磁辐射认证:	EN55022 1998 Class A EN55022 1998 Class A FCC Part 15B Class A VCCI Class A	EN55022 1998 Class A EN55022 1998 Class A FCC Part 15B Class A VCCI Class A	EN55022 1998 Class A EN55022 1998 Class A FCC Part 15B Class A VCCI Class A

更多信息

欲了解关于FirePass的更多信息，请在F5.com上访问以下资源。

白皮书

[F5 FirePass终端安全](#)

[了解GPO](#)

播客

[通过安全的远程访问实现灾难恢复](#)

案例研究

[Diamond Bar市部署FirePass](#)

部署指南

[带有BIG-IP LTM和GTM的F5 FirePass控制器（FirePass v6.x、LTM和GTM 9.4.2）部署指南](#)

[FirePass和VMware View部署指南](#)

