

F5 关键技术阐述

项目概况

X烟公司出差员工需要访问公司内部资源；

公司内部资源包括内部门户网站、办公协同系统、营销信息采集系统、K3财务系统等关键应用。营销信息和财务数据都要保证其安全性，避免被非法获取；

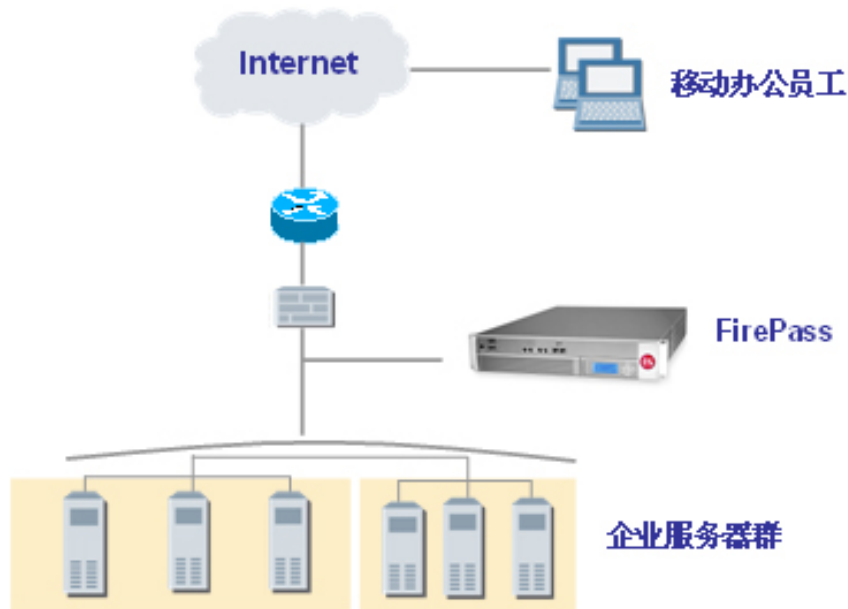
X烟公司内部由Active Directory统一规划和管理员工帐号和鉴权。

网络结构

Network Diagram



广东中烟工业公司远程安全访问—FirePass



客户需求

- ☆ 采用专用的SSL VPN设备实现安全远程接入；
- ☆ 通过SSL VPN设备可安全访问公司内部门户网站、办公协同系统、营销信息采集系统、K3财务系统等资源；

☆ 实现单点登陆，如在登陆内部门户网站时，只需点击VPN上的资源链接即可直接登陆的门户主页，不需再次输入帐号和口令；

☆ 按帐号所属Active Directory用户组的不同，定义不同的访问权限，用户只能访问自身帐号权限范围内的资源；

☆ VPN设备能与Active Directory无缝集成，用户只需使用Active Directory中的帐号和口令登陆VPN网关，即可访问该帐号权限所能访问的资源。

解决方案

广东X烟工业公司内部有门户网站、办公协同系统、营销信息采集系统、K3财务系统等核心应用系统，在加入FirePass以前，公司员工在外出差时无法访问公司内部资源，特别是营销人员，无法及时查询营销系统的信息，给工作带来极大不便。在加入了FirePass后，出差在外的公司员工可以通过 FirePass访问内部各应用系统，在家办公的IT管理人员也能在故障发生时及时通过远程接入公司内部网进行系统维护X中烟公司的每一位员工在 Active Directory上都有自己独立的帐号和密码，并根据部门的不同进行了分组。我们在FirePass用户组配置时使用Active Directory外部认证模式，使员工只要在FirePass的登陆界面输入自己AD帐户的用户名和密码就可以连入内部办公网络，使用内部网络资源。而 IT维护人员无需在为每一位员工特别建立FirePass登陆帐户，极大的节省了人力，可以认为是FirePass和现有资源的一次完美结合。

为什么选择F5

☆ 最广泛的应用支持：借助F5 FirePass，无论采用何种设备，均能实现对电子邮件、Web门户、网络文件服务、终端服务、CRM以及其它主要企业应用的访问；

☆ F5 FirePass和Active Directory无缝集成：F5 FirePass除了缺省的内部数据库认证，还能支持RADIUS、活动目录、RSA双因素、LDAP认证、基于表格的基本HTTP认证，以及身份管理服务与Windows域名服务器认证等方式；

☆ 支持中文配置界面，易于使用，且可设置的功能参数丰富，能最大程度实现用户个性化的需求；

☆ 对Citrix应用的集成度高，完全兼容用户的K3财务系统；

☆ 可自定义登陆界面；

☆ 众多的成功案例：信息产业部电信研究院成功的使用FirePass解决了员工从外部网络访问院内Notes系统的安全问题；天狮集团应用FirePass 安全网络访问，让员工从任何地点都可以轻松的通过浏览器从外部网络登陆到内部网络的Oracle ERP系统工作，同时使访问安全性和易用性的问题得到了十分成功的解决。

关键技术阐述

☆ 门户网站单点登陆
名称“企业门户通道”；

定义完整的URL `http://172.16.11.80/SYSParts/Login/VPNLogin.aspx`;

URL变量里将用户名和口令作为变量参数进行透传“`UserCode=%username%&PassWord=%password%`”，当用户点击“企业门户通道”链接即可以该用户的VPN登陆帐号密码直接登陆主页，不需重新输入帐号和口令；

通过FirePass 单点登陆设置后。外网用户一次输入FirePass的密码，就可以直接访问内网的多台应用了单点登陆的服务器而不需要重复输入密码。

资源组别:

App 通道 终端服务器

应用程序通道 web应用程序通道

web应用程序通道

[显示收藏夹允许列表](#)

企业门户通道 `http://172.16.11.80/SYSParts/Login/VPNLogin.aspx`

类型:

名称:

URL: [添加到允许列表](#)

Uri 变量:

使用 POST 作为 URL 变量:

被锁定的浏览器:

允许列表:

要求端点保护:

[添加新收藏夹](#)

默认:

☆ 动态组映射

与Active Directory联动，Firepass用户帐号定期与Active Directory的帐号建立信息同步；

用户: 组: 动态组映射 权限: 完全访问 帮助

组映射序列 组映射方式 主组映射表 资源组映射表

映射方式

活动目录 配置 删除

LDAP (用户对象) 新增映射方式

组映射序列 组映射方式 主组映射表 资源组映射表

映射方式

[返回到 组映射方法 页 >>](#)

域名: ZYGS.COM

Kerberos服务器名称(可选):

WINS 服务器 IP 地址(可选):

域管理员名称: administrator

域管理员密码:

使用一个次要的 AD 服务器

仅使用 Active Directory 首选组映射:

同步 FirePass 用户数据库和Active Directory

操作: 如果用户不在Active Directory, 则停用 FirePass 帐户 用电子邮件通知。

检查内部 (分钟) 1

更新来自 Active Directory 的用户信息:

映射名

在“资源组映射表”建立映射关系，如下图：

组映射序列

组映射方式

主组映射表

资源组映射表

资源组映射表

映射方式 活动目录 添加 删除

| | 源 | 外部组或值 | FirePass 资源组 |
|--------------------------|-------|----------------|----------------|
| <input type="checkbox"/> | 活动的目录 | 信息中心全体人员 | zygs_resource |
| <input type="checkbox"/> | 活动的目录 | 广东中烟工业公司全体人员 | zygs_webportal |
| <input type="checkbox"/> | 活动的目录 | 市场营销ForVPN组 | zygs_marketing |
| <input type="checkbox"/> | 活动的目录 | Citrix业务系统用户组 | zygs_citrix |
| <input type="checkbox"/> | 活动的目录 | Citrix财务系统用户组 | zygs_citrix |
| <input type="checkbox"/> | 活动的目录 | Citrix仓库系统用户组 | zygs_citrix |
| <input type="checkbox"/> | 活动的目录 | Citrix 管理测试用户组 | zygs_citrix |

删除

用户名称

密码（可选项）

测试

这样“信息中心全体人员”（映射到Firepass的用户组“poweruser_group”）的成员可访问资源组“zygs_resource”的资源。