格尔安全认证网关产品白皮书

V5.5

上海格尔软件股份有限公司

2017 年 2 月

保密事宜：

本文档包含上海格尔软件股份有限公司的专有商业信息和保密信息。

接受方同意维护本文档所提供信息的保密性，承诺不对其进行复制，或向评估小组以外、非直接相关的人员公开此信息。对于以下三种信息，接受方不向格尔公司承担保密责任：

1） 接受方在接收该文档前，已经掌握的信息。

2） 可以通过与接受方无关的其它渠道公开获得的信息。

3） 可以从第三方，以无附加保密要求方式获得的信息。

上海格尔软件股份有限公司

上海市江场西路 299 弄 5 号（中铁中环时代广场 4 号楼）6 楼

http://www.koal.com/

目　录

上海格尔软件股份有限公司
上海市江场西路 299 弄 5 号（中铁中环时代广场 4 号楼）6 楼
http://www.koal.com/

1 概述

1.1 您的网络应用安全吗？

随着网络的快速发展，网络应用以其高效、便捷的特点得到广泛应用，如网上证券、网上银行、电子政务、电子商务、企业远程办公等。越来越多的重要业务在网上办理，越来越多的重要信息在网络中传输，如何保护这些重要资源的安全访问以及重要数据的安全流转是网络应用面临的重要问题，但通常的网络应用都存在以下安全隐患：

- 没有有效的身份认证机制：一般都采用用户名+口令的弱认证方式，这种认证用户的模式，存在极大的隐患，具体表现在：（a）口令易被猜测；（b）口令在公网中传输，容易被截获；（c）一旦口令泄密，所有安全机制即失效；（d）后台服务系统需要维护庞大的用户口令列表并负责口令保存的安全，管理非常困难。
- 数据传输不安全：当前大多网络应用所发放的数据包均是按照 TCP/IP 协议为明文方式传输，而 Internet 的开放性造成传输信息存在着被窃听、被篡改的安全问题。
- 操作抵赖：网络应用将现实世界的实体操作转化为虚拟世界的信息流，信息流的可复制性对操作的唯一性和可信性提出了挑战，操作可以被抵赖成为网络应用亟需解决的一个严重问题。

1.2 解决网络应用安全您要考虑

信任是安全的基础，在缺乏信任的环境下，实现信息系统的安全是不可想象的，因此解决网络应用安全的一个核心问题是解决信任问题，信任主要体现在以下几方面：

- 强身份认证。建立信任首先要确认参与者的身份，即身份认证。身份认证是安全保障的第一道门槛，也是后续安全措施的依据和基础，如果第

上海格尔软件股份有限公司
上海市江场西路 299 弄 5 号（中铁中环时代广场 4 号楼）6 楼
http://www.koal.com/

一道门槛被攻破，系统“认错人”，则后续的无论多么严密的安全措施基本实效，因此，身份认证机制强度的高低很大程度决定了安全系统的安全级别高低，对于一个直接面对互联网，如果身份认证机制的强度不够，根本无法起到屏障作用，无异于将网资源直接开放。因此，身份认证机制不在于多少，而在于够不够强。基于 PKI 数字证书的认证是目前被广泛接受的强身份认证机制之一。

- 数据秘密性和完整性。一方面，认证机制越强，效率越低。在网络应用中并不是每次交互都进行认证，而是根据第一次认证后的凭证来辨认用户，因此在真正用户在线认证通过后，窃取用户的认证凭证，冒充用户访问是一种有效的攻击手段。因此身份认证过程以及后续传输通讯都需全程保密。另一方面，网络应用中的重要信息被其他人特别是竞争对手得到造成的损失极大，因此要求信息传输时对信息进行高强度加密，保证传输安全性。总之，信息在网络上明文传输，被人轻易获取，无异于自己打开门把东西拿给别人，系统有再强的其他安全机制有何用呢？全程加密是对数据秘密性及完整性保障的优选方案之一。
- 不可抵赖性。不可抵赖是信任的一个关键因素也是一个关键约束，是对结果的认可和保障，如果可以事后赖账，无法追究责任，那么先前所作的一切都是前功尽弃。现实生活中已经形成一套不可抵赖性的方式方法，而在网络世界中，数字签名技术是公认的不可抵赖性实现的最优方案，《电子签名法》的颁布和实施也提供了相应的法律依据。

上海格尔软件股份有限公司
上海市江场西路 299 弄 5 号（中铁中环时代广场 4 号楼）6 楼
http://www.koal.com/

2 产品概述

图表 1 E 型网关外观

图表 2 G 型网关外观

（以上产品外观图仅做参考，具体外观及接口以实物为准）

格尔网关为网络应用提供基于数字证书的高强度身份认证服务、高强度数据链路加密服务及数字签名验证服务，可以有效保护网络资源的安全访问。支持 HTTP、HTTPS 的 B/S 应用以及 FTP、远程桌面等通用的 C/S 应用。

3 为什么选择格尔安全认证网关

格尔安全认证网关是：

- 上海格尔软件自主研发的网络安全应用产品，具备多项 PKI/SSL 相关的专利技术。
  - 01132344 具有 MIME 数据类型过滤技术的 SSL 代理方法
  - 200310109056 数字证书跨信任域互通方法
  - 201010618999 一种快速检索海量数字证书黑名单的方法
  - 201110447868 一种增强浏览器 SSL 算法强度的代理方法

上海格尔软件股份有限公司
上海市江场西路 299 弄 5 号（中铁中环时代广场 4 号楼）6 楼
http://www.koal.com/

- 201010619005 一种 SSL 服务端动态选择证书的实现方法

➢ 国内首批支持 SM1/2/3/4 算法及国密版 SSLVPN 协议的商用密码产品（SRJ1505）。

格尔安全认证网关的价值体现在以下几个方面：

3.1 PKI 数字证书及商用密码算法的全面支持

基于对 PKI 的深刻理解，格尔网关具备了对 PKI 的全面支持，包括以下几个方面：

- **RSA/SM2** 多种证书体系自适应（**专利技术《一种 SSL 服务端动态选择证书的实现方法》**）
- **TLS 1.0/1.1/1.2/国密 SSLVPN** 多种协议自适应。
- 多条证书链、多信任域支持：格尔网关支持多条证书链同时存在、同时生效，即同一个 SSL 服务可以同时认证多家 CA 中心的证书用户。（**专利技术《数字证书跨信任域互通方法》**）
- 超大黑名单动态支持：格尔网关可以支持千万级的黑名单动态更新（支持 LDAP、HTTP、手工上传等多种方式更新），不需要重新启动服务。（**专利技术《一种快速检索海量数字证书黑名单的方法》**）
- 客户端证书认证的多样化策略：格尔网关可以灵活配置建立认证用户证书的策略，包括强制认证，可选认证，仅信任本地证书链等。
- 多服务，多站点证书支持：格尔网关可以建立多个服务，保护不同的应用，每个服务可以使用不同的证书及策略。

3.2 对用户的一致性认证

通常的网关产品只是建立了一个加密连接，与应用完全无关，用户通过认证建立加密连接后必须经过再次认证（如用户名+口令、动态令牌等）登录应用系统，这种两次登录不仅没有加强安全性，而且在给用户带来不便的同时也带来安全隐患，由于加密连接和应用对用户认证的不一致，用户可以使用自己的证书建

立连接，使用别人的用户名登录，这种方式给应用的流程和日后审计、取证带来了混乱。

格尔网关可以将用户证书中的任意信息以 HTTP 注入（Cookie/Header）方式向后台服务器传送，应用系统无需额外接口就可以方便获取证书用户信息，即保证了用户的一次登录，又保证了应用对用户认证的一致性，安全性得到进一步保障。同时，使用网关保护的多个应用系统也实现了对用户的单点登录功能，即用户使用一张证书登录所有应用系统。

3.3 多应用类型支持

格尔网关除了可以对 B/S 应用进行安全防护外，对于 FTP、Telnet、SSH、远程桌面、SMTP、POP3 等多种非 B/S 应用也可以进行安全防护，具有广泛的适用性。

3.4 对应用的加速

格尔网关高端产品采用硬件加速，加解密运算全部由硬件完成，效率是同等硬件环境下软件实现的 10 倍以上，可以彻底将应用服务器的 CPU 资源从繁重的加解密中解放出来，起到了对应用加速的作用。

3.5 安全资质

格尔安全认证网关通过了国家保密局、国家密码管理局的严格鉴定，取得了相关安全资质，符合国家对于密码产品的使用规定。

上海格尔软件股份有限公司

上海市江场西路 299 弄 5 号（中铁中环时代广场 4 号楼）6 楼

http://www.koal.com/

商用密码产品型号证书

（证书编号：SXH2015189 号）

单位名称： 上海格尔软件股份有限公司

申报名称： 安全认证网关

批准型号： SRJ1505 安全认证网关

说明：1. 符合 GM/T 0024-2014《SSL VPN 技术规范》要求

2. 证书有效期五年

国家密码管理局

2015 年 11 月 06 日

涉密信息系统
产品检测证书

编号：国保测 2016C05096

兹证明：上海格尔软件股份有限公司
上海格尔安全科技有限公司

研制生产的 格尔安全网关 V5.2

经国家保密科技测评中心检测，符合国家保密标准《涉及国家秘密的信息系统网关安全技术要求》（暂行）的要求。

本证书有效期自 2016 年 11 月 21 日至 2019 年 11 月 20 日

批准人：

国家保密科技测评中心

产品检测专用章

使用证书复印件应由产品研制生产单位加盖公章　　证书信息核查：WWW.NSSTEC.ORG.CN

上海格尔软件股份有限公司
上海市江场西路 299 弄 5 号（中铁中环时代广场 4 号楼）6 楼
http://www.koal.com/

3.6 其他特性

- 安全性：系统设置专用网络接口管理系统，系统关闭所有不需要的服务和端口（如 FTP、SSH 等），只保留 SSL 服务端口，避免外界的攻击。
- 易用性：系统所有管理操作均采用 WEB 方式，操作简单方便。
- 适用性：系统支持串联、并联等多种部署方式，适用不同的网络环境和应用需求。
- 兼容性：支持 IE、Firefox、Chrome、Safari 等主流浏览器，支持 IIS、WebSphere、WebLogic、Apache、Tomcat 等主流 Web 服务器。
- 高可用性：系统支持双机热备。

4 产品主要功能

功能	说明	功能类型
证书认证		
RSA/SM2 证书自适应	系统可以在同一个服务实例中，配置 RSA 和 SM2 两张站点证书，并同时启用，根据客户端的算法能力进行自动适应。	基本功能
TLS 1.0/1.1/1.2 及国密 SSLVPN 协议自适应适应	系统可以在同一个服务实例中，同时支持国际标准协议（TLS 1.0/1.1/1.2）以及国家密码管理局制定的国密 SSLVPN 协议。根据客户端的支持情况自动适应。	基本功能
客户端证书认证策略	系统可以设置是否需要用户提交用户证书，包括不认证、可选认证、强制认证，仅信任本地证书链等。	基本功能

动态黑名单功能	系统可以自动更新黑名单、动态更新，不需要重新启动服务 支持 LDAP、HTTP、手工上传等多种方式更新 支持 B64、DER 等多种格式	基本功能
多站点证书功能	系统可以拥有多个站点证书，不同的服务可以拥有不同的站点证书	基本功能
多证书链功能	一个 SSL 服务中可同时配置多条证书链，验证不同 CA 的用户证书	基本功能
多种证书支持功能	支持格尔、CFCA 及多数省级 CA 中心数字证书	基本功能
证书信息传送功能	系统可以将用户证书信息包括扩展项信息传送给应用系统	基本功能
应用支持		
B/S 应用	支持 B/S 应用	基本功能
通用 C/S 应用	支持 FTP、Telnet、远程桌面以及通用的 C/S 应用	基本功能
网络应用	支持基于 IP 的所有应用	扩展功能
多服务功能	系统可以创建多个 SSL 服务，保护不同的应用服务，也可以采用同一个 SSL 服务保护多个应用服务（需客户端）	基本功能
地址隐藏功能	系统将真正应用服务的地址隐藏，用户仅知道网关地址	扩展功能
支持应用重定向功能	在有防火墙 NAT 映射的情况下正常访问有重定向的网站	基本功能

特色功能		
认证一致性	系统通过特有的 HTTP 注入（Cookie/Header）技术将用户的证书信息传送给后台应用，使应用无需证书接口开发就可以方便的获取用户证书信息	基本功能
自动登录功能	对于特定应用，系统采用用户映射技术，将证书映射为原有系统中的账户，并进行自动登录，在后台应用无需修改的情况下实现单点登录	扩展功能
策略统一下发	系统实现客户端策略的统一下发，用户无需对客户端进行任何配置	基本功能
信息统计	系统能够对用户连接数、应用访问情况，系统资源占用等信息进行详细统计，为更好了解应用及调节资源提供基础	基本功能
错误重定向	系统对于认证错误可以重定向到用户指定页面，增强友好性	基本功能
访问控制功能	实现 URL 级别的访问控制，对于不同用户、不同角色实现不同的控制	扩展功能
国密算法支持	系统支持国密 SM1/SM2/SM3/SM4 算法	基本功能
系统管理		
系统备份恢复功能	系统可以备份当前 SSL 的所有配置，保证系统瘫痪时的快速恢复	基本功能
恢复出厂设置功能	系统具有恢复默认设置功能，方便使用	基本功能

日志发送功能	系统将日志以 SYSLOG 的方式发送到指定服务器。	基本功能
系统在线升级	系统支持 Web 方式的系统升级	基本功能
性能检测功能	系统支持对 CPU、内存、磁盘容量、连接数、进程等资源情况的收集，便于系统的维护和问题定位	基本功能
可用性		
双机热备功能	高可靠性	扩展功能
负载均衡	系统支持被第三方的负载均衡器进行负载	基本功能
易用性		
管理员易于操作	系统所有管理操作都通过 web 方式进行，方便使用	基本功能
用户的良好体验	系统可以为终端用户提供良好的错误提示，如证书过期，证书未生效，证书已经作废等信息，不会显示“此页无法显示”令用户不知所措的页面	基本功能

注：扩展功能不包含在产品的基本版本中，是用户可选配功能。

5 产品部署

格尔网关可以部署为串联模式或者并联模式（单臂模式）。

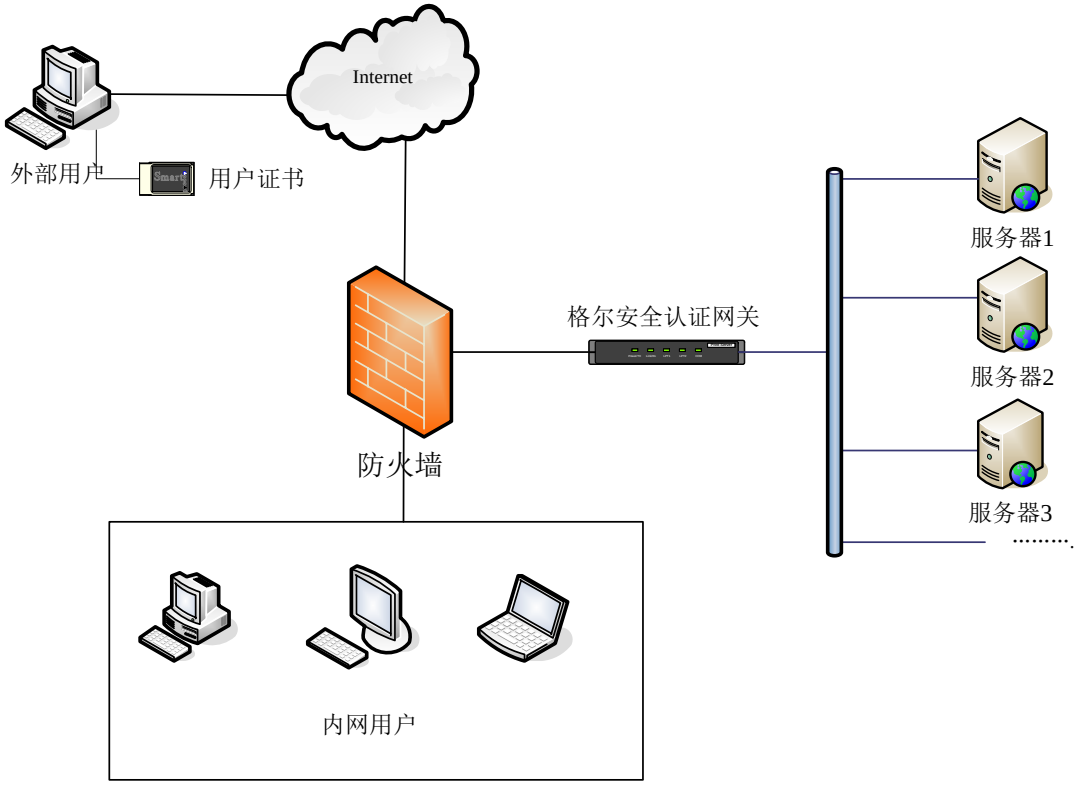
5.1 串联部署

串联模式指格尔网关物理部署在用户和被保护的服务器之间，即格尔网关的

上海格尔软件股份有限公司
上海市江场西路 299 弄 5 号（中铁中环时代广场 4 号楼）6 楼
http://www.koal.com/

外网口与用户网络连接，内网口与被保护服务器相连。由于被保护服务器通过内部网络与格尔网关连接，因此用户与服务器的连接被格尔网关隔离，用户只知道网关地址，无法直接访问被保护服务器，只有通过网关才能获得服务。

串联模式是格尔网关的标准部署模式，也是推荐部署模式，其部署示意图如下：



图表 3 串联部署示意图

串联模式的优点是：

- 安全性高：用户必须通过网关的认证加密后才能获取服务，同时网关将服务器与外界网络隔离，避免了对服务器的直接攻击。
- 结构清晰：串联模式在物理部署和逻辑结构上都非常简单，容易理解。
- 性能高：相对于并联模式，串联模式的效率及带宽利用率更高。

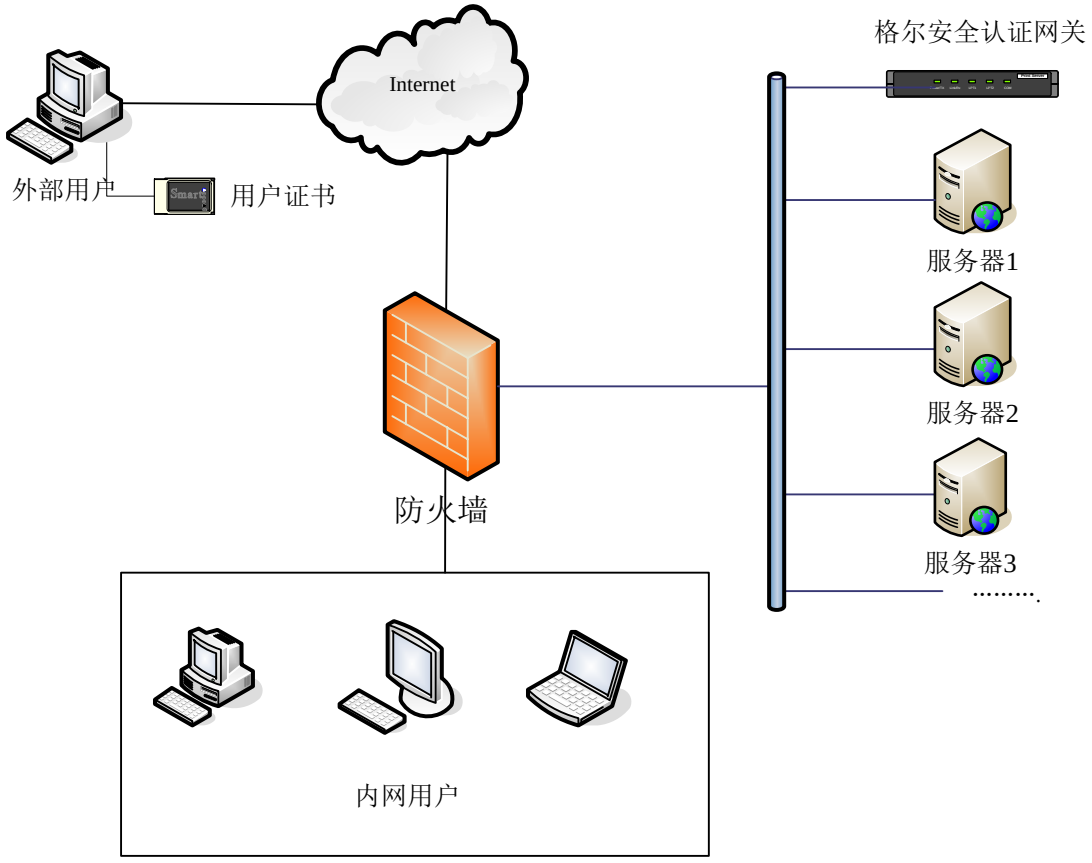
串联模式的缺点是：

- 需要对原有服务器进行网络改动及进行地址改变带来的必要的应用变更。

上海格尔软件股份有限公司
上海市江场西路 299 弄 5 号（中铁中环时代广场 4 号楼）6 楼
http://www.koal.com/

5.2 并联部署

并联模式（单臂模式）指格尔网关逻辑部署在用户和被保护的服务器之间，而物理连接是在同一网络中，即格尔网关的外网口接入原有用户与服务器的网络连接中。用户可以通过网关获取服务，也可以直接连接到服务器（在知道服务器地址情况下）获取服务。



图表 4 并联部署示意图

并联模式的优点是：

- 部署方便：应用无需作改动，用户只需变更一下访问地址即可。

并联模式的缺点是：

- 安全性低：由于服务器和外界网络连接，存在用户绕开网关直接连接服务器和使用其它方式攻击服务器的可能性；同时，网关到服务器的明文数据也在网络上传输，存在被窃听的安全隐患。
- 性能较低：相对于串联模式，并联模式中用户到网关和网关到服务器的

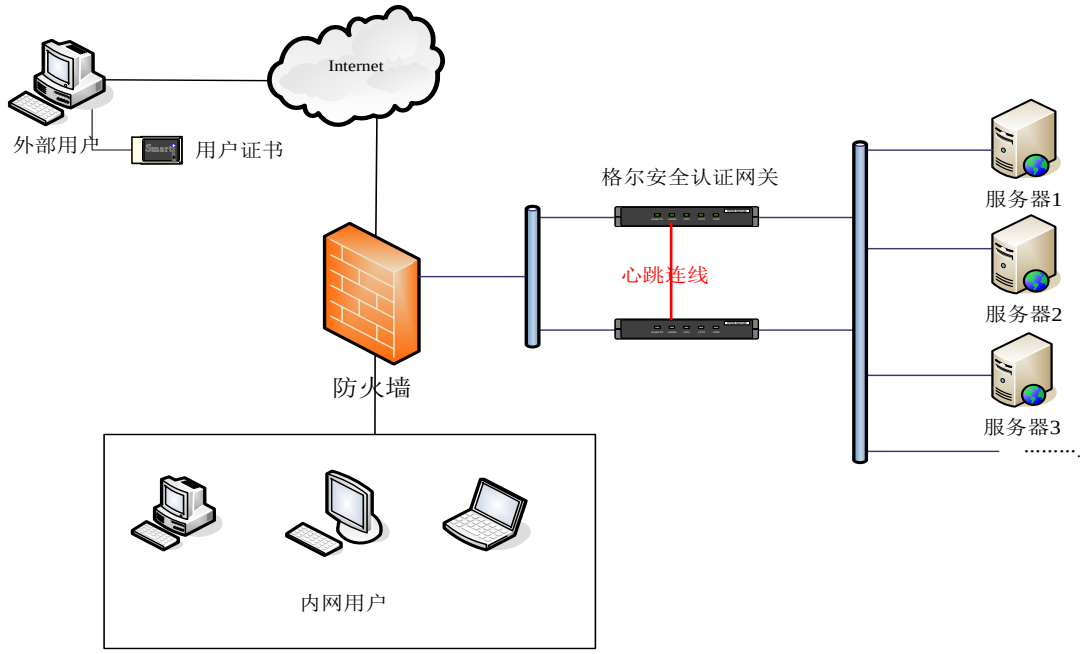
上海格尔软件股份有限公司
上海市江场西路 299 弄 5 号（中铁中环时代广场 4 号楼）6 楼
http://www.koal.com/

数据流量都通过一个网口进行，效率及带宽利用率相对较低。

并联模式部署时，为确保安全性，请务必在网络防火墙处进行限制——只允许网关访问应用服务器。

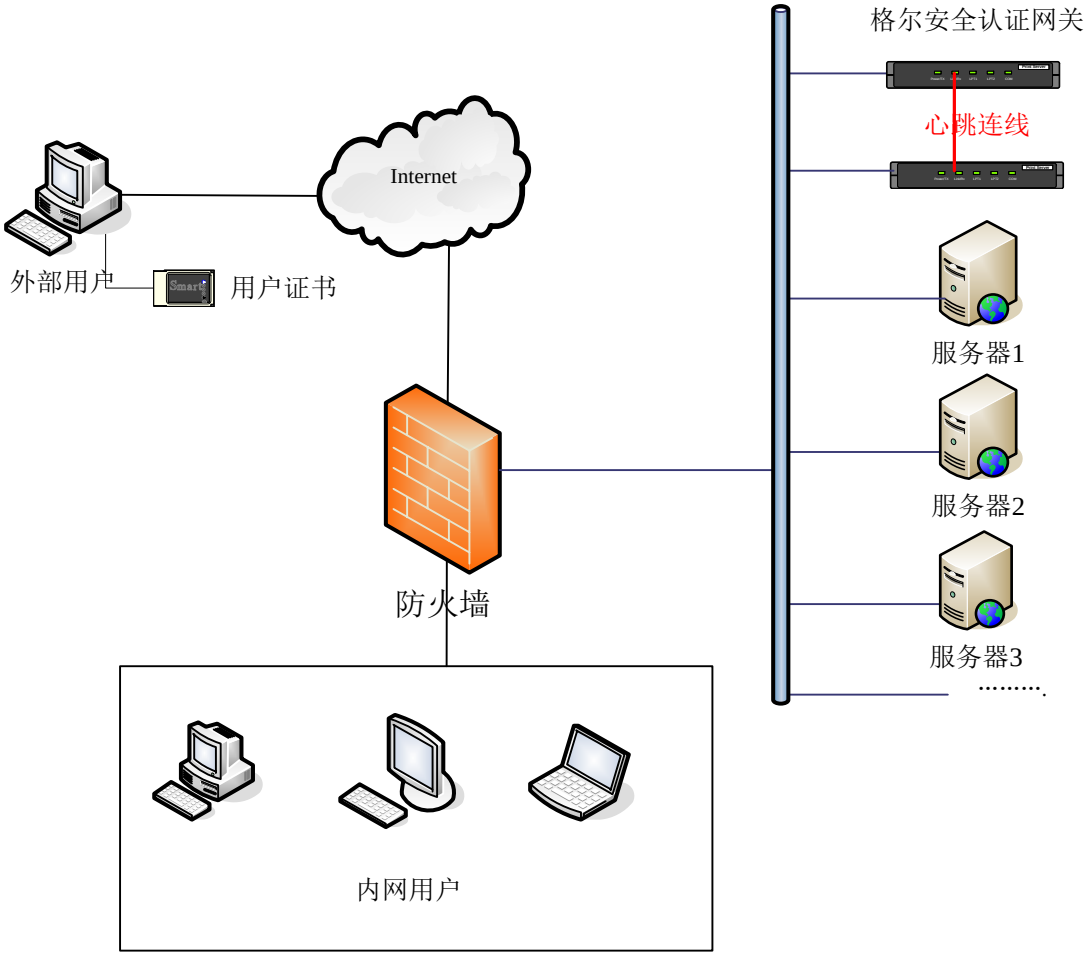
5.3 双机热备部署

系统支持双机热备功能，在需要高可靠性的环境下需要对网关进行双机热备部署。双机热备部署需要部署两台设备，一台作为主机，一台作为备机，两台机器都与网络连接，两台设备之间使用心跳线连接热备口进行状态检测，在正常情况下由主机提供服务，当主机发生异常时系统自动切换到备机进行服务。部署方式如图：



上海格尔软件股份有限公司
上海市江场西路 299 弄 5 号（中铁中环时代广场 4 号楼）6 楼
http://www.koal.com/

图表 5 串联模式下的双机热备部署

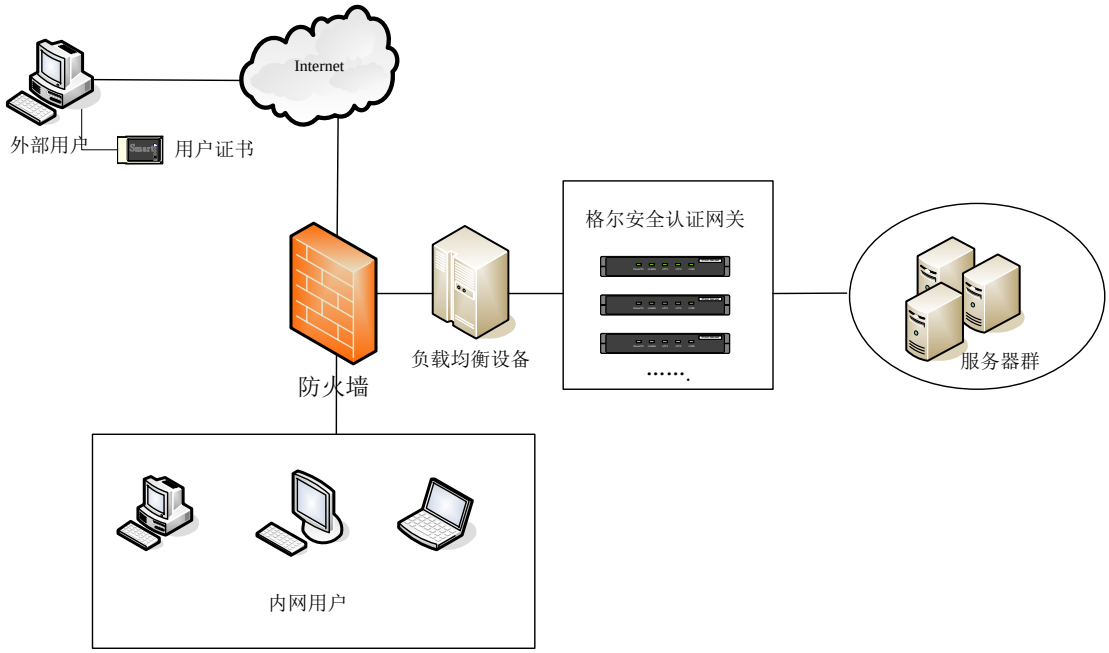


图表 6 并联模式下的双机热备部署

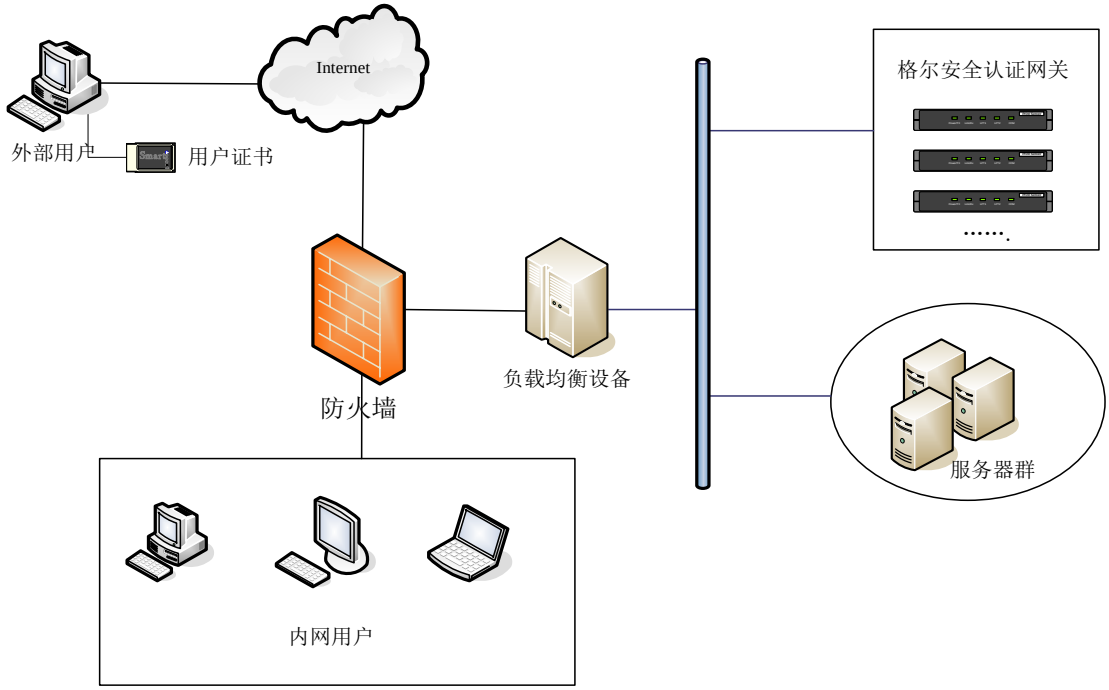
5.4 负载均衡部署

格尔网关可以和大多数负载均衡设备配合使用，格尔网关采用串联模式和并联模式都可以与负载均衡设备很好的配合使用。如下图：

上海格尔软件股份有限公司
上海市江场西路 299 弄 5 号（中铁中环时代广场 4 号楼）6 楼
http://www.koal.com/



图表 7 负载均衡环境下的串联模式部署



图表 8 负载均衡环境下的并联部署

注：负载均衡器将网络的 SSL 流量负载到可用的格尔网关上，格尔网关对后端的 Web 服务器并没有负载均衡的作用。

上海格尔软件股份有限公司
上海市江场西路 299 弄 5 号（中铁中环时代广场 4 号楼）6 楼
http://www.koal.com/

6 选购指南

格尔网关采用专用网络硬件设备，产品具有多个系列：

	E-2010	E-2020	E-2040	G-4020	G-4040
设备高度	1u	1u	1u	2u	2u
网络接口	6*1000M	6*1000M	6*1000M	6*1000M (可扩展光口或万兆口)	6*1000M (可扩展光口或万兆口)
电源指标 数量： 电压（V）： 电流（A）： 功率（W）：	 1 100~240 0.5~3 60	 1 100~240 3~6 60	 1 100~240 3~6 250	 1 90~264 4~8 250	 2 90~264 4~8 350
工作温度	0°C--40 °C	0°C--40 °C	0°C--40 °C	0°C--40 °C	0°C--40 °C
工作湿度	5%--95% RH，不凝结	5%--95% RH，不凝结	5%--95% RH，不凝结	5%--95% RH，不凝结	5%--95% RH，不凝结
最大新建连接数(RSA)	60 次/秒	160 次/秒	1000 次/秒	2500 次/秒	4000 次/秒
最大新建连接数(SM2)	60 次/秒	150 次/秒	1500 次/秒	2000 次/秒	4000 次/秒
每秒完成交易数	1000 次/秒	2000 次/秒	5000 次/秒	10000 次/秒	25000 次/秒

上海格尔软件股份有限公司
上海市江场西路 299 弄 5 号（中铁中环时代广场 4 号楼）6 楼
http://www.koal.com/

（TPS）					
最大并发连接数	400	800	1500	2500	5500
最大流量	100Mbps	200Mbps	500Mbps	1Gbps	2Gbps

注：上述所有规格及参数若有变动恕不另行通知，请以厂家提供的最终配置为准。

7 客户端运行环境

与格尔 SSL 安全网关连接的客户端推荐配置如下：

CPU：Intel i3 以上

内存：1G 以上

操作系统：Windows 7 以上版本

浏览器：IE8.0 以上

8 产品支持联系方式

上海格尔软件股份有限公司

地址：上海市江场西路 299 弄 5 号（中铁中环时代广场 4 号楼）6 楼

电话：（86-21）62327010

传真：（86-21）62327015

邮编： 200436

9 附录：名词解释

- SSL/TLS：安全套接层协议层，它是网景（Netscape）公司提出的基于 WEB 应用的安全协议，目前已发展到 TLS 1.2 版本。
- 证书认证机构（Certificate Authority）：一个产生和确定公开密钥证书的可靠和可信的第三方机构。它发行数字证书并确保证书的可信性，或证明一个用户和它们的公共密钥的身份。认证机构也可以为实体产生和确定密钥。习惯上又称作认证中心（CA）。
- 数字证书（Certificate）：数字证书中心签发的用于代表实体身份的一段电文。包括代表用户身份的用户证书和代表服务端身份的站点证书（服务器证书）。
- 数字签名（digital signature）：具有手写签名功能一如身份证明的一组电子数据。这些附加在数据单元上的一些数据，或是对数据单元所作的密码变换，允许数据单元的接收者用以确认数据单元的来源和完整性，并保护数据，防止被人（例如接收者）伪造。
- LDAP：(Lightweight Directory Access Protocol) 是一种轻量级的目录存取协定，提供客户从各个角落连接到目录服务器中。本手册中专指 CA 用于发布证书及黑名单的 LDAP 服务。
- 黑名单：通常所说的CRL（Certificate Revoke List ），因时间或者安全原因被废除的证书列表，一般发布在LDAP上。✧
- 国密 SSLVPN 协议：也即 GM/T 0024-2014《SSLVPN 技术规范》，是国家密码管理局制定的使用 SM1/2/3/4 算法的 SSL 协议。
- 反向代理：览器中访问HRP监听的地址，HRP将请求根据自身的配置代理到真实的后台应用。
- 正向代理：浏览器中访问应用的地址，客户端程序截获此数据包，经过SSL封装后传递给服务端的HRP，HRP解包后，根据原始访问信息，将请求传递给真实的应用。此模式又称为透明代理。