

# 安全网关系统技术白皮书



北京电子科技学院

中安网脉（北京）技术股份有限公司

二零零七年十月

---

---

## 版权声明

---

安全网关系统技术白皮书

**首先，我们非常感谢您查看本文档：**

本文档介绍了安全网关系统的产品体系结构、功能、运行环境，为用户在选用本系统时提供参考。本手册仅提供电子文档。

Copyright © 2006 by SINOINFOSEC, 中安网脉（北京）技术股份有限公司版权所有。

未经书面许可，用户不得以任何形式或通过任何途径，包括使用影印、录制在内的电子或机械手段等对该书任何部分进行复制或传播。

**警告和承诺：**

本文档用于提供关于“安全网关系统”的产品信息。尽管我们尽最大的努力使本文档尽可能的完备和准确，但疏漏和缺陷之处在所难免。

任何人或实体由于本文档提供的信息造成的任何损失或损害，中安网脉（北京）技术股份有限公司不承担任何义务或责任。

本书中表达的观点权属于中安网脉（北京）技术股份有限公司。

**系统版权：**

中文名称：安全网关系统

开发单位：中安网脉（北京）技术股份有限公司

**本系统的版权单位：**

中安网脉（北京）技术股份有限公司

地址：北京市丰台区富丰路 7 号

邮政编码：100070

电话：(010) 63783209 或 83635361

邮箱：support@sinoinfosec.com

安全网关系统是中安网脉(北京)技术股份有限公司自主研发的受法律保护的商业软件。遵守法律是共同的责任，任何人未经授权人许可，不得以任何形式或方法以及出于任何目的复制或传播本软件，权利人将追究侵权者责任并保留要求赔偿的权利。

本软件系统及其文档中使用到其他公司的有关资源，其版权归相应公司所有，亦受到法律的严格保护。

**反馈信息：**

您的反馈意见将使我们受益非浅。如果您对本手册有任何疑问、意见或建议，请与我们联系：support@sinoinfosec.com，感谢您对我们的支持和帮助。

## 目 录

<b>第 1 章 产品研发单位简介</b> .....	<b>1</b>
<b>第 2 章 系统概述</b> .....	<b>2</b>
<b>第 3 章 系统需求</b> .....	<b>4</b>
3.1 专用服务器的密码安全防护需求.....	4
3.2 数据传输加密.....	4
3.3 数据本地加密存储需求.....	4
3.4 与内网PKI体系结合，建立安全认证机制.....	4
3.5 客户端软件易于安装、操作简便.....	5
<b>第 4 章 系统总体结构</b> .....	<b>6</b>
4.1 安全网关.....	6
4.1.1 设备功能.....	6
4.1.2 性能指标.....	7
4.2 安全管理中心.....	7
4.2.1 设备功能.....	7
4.2.2 性能指标.....	8
4.3 USB-KEY终端设备.....	8
4.4 客户端软件.....	8
<b>第 5 章 系统技术方案</b> .....	<b>10</b>
5.1 系统结构.....	10
5.2 安全机制.....	11
5.2.1 用户认证.....	11
5.2.2 用户授权.....	11
5.2.3 VPN隧道.....	11
5.2.4 数据安全.....	12
5.2.5 自身安全.....	12
5.2.6 数据备份.....	13

5.2.7 集群功能.....	13
5.2.8 日志审计.....	13
5.3 系统管理.....	14
<b>第 6 章 售后服务 .....</b>	<b>15</b>
6.1 系统配置建议.....	15
6.2 购买相关产品.....	15
6.3 系统实施服务.....	16
6.4 系统售后服务.....	17
6.5 软件培训服务.....	18
6.6 技术支持服务.....	18

## 第1章 产品研发单位简介

---

“中国商用密码与信息安全的中流砥柱”——是中安网脉（北京）技术股份有限公司肩负的国家使命，是中安网脉公司孜孜以求的奋斗目标，也是中安网脉公司自我评价的衡量标准。

“把握网络脉搏，引领安全方向”——中安网脉（北京）技术股份有限公司专注于商用密码与信息安全产品的开发与服务，致力于中国电子安全方案解决，正逐步成为中国信息安全领域的创新者和技术的领先者。

中安网脉（北京）技术股份有限公司由北京电子科技学院控股成立，北京电子科技学院隶属于中共中央办公厅，是我国唯一一所为全国各级党政机关培养信息安全专门人才的高等院校。学院有一支由教授、高工等专家为主导，由博士、硕士为成员的专业教学科研队伍。学院的建设和发展有着得天独厚的政治优势和各项保障，多年来一直得到党中央和中央办公厅领导的关怀和重视。温家宝、曾庆红、王刚等中央领导同志都为学院的发展和建设作过许多重要指示，并多次亲临学院视察工作。

中安网脉（北京）技术股份有限公司是集计算机网络信息安全服务、商密软、硬件产品、信息安全产品、提供网络安全整体解决方案的开发和研制为一体的高科技企业。公司拥有高素质专业员工 58 人，其中，80%以上为大学本科以上学历，他们具有丰富的科研开发、技术支持、生产及管理的专业知识和经验。公司技术力量雄厚，核心研发团队以经验丰富的信息安全专家为主导，由博士、硕士为成员组成，技术骨干均具有 5 年以上的网络通信、密码安全产品开发经验，已开发出了众多国内技术领先的产品，获得了较为广泛的应用。公司在数字电话密码机、传真加密机、内网安全、数据库加密、信息源加密、电子文档安全控制、安全审计等信息安全领域技术领先，研制成功的几十种密码与信息安全产品已广泛应用于各大部委、兵工系统和全国部分省市的党政机关。同时，公司在安全办公应用软件、信息安全等级保护、信息化密码保障服务的设计、开发、实施等方面也取得了一系列成绩和经验，很好地为我国的信息化建设起到了保驾护航的作用。

## 第2章 系统概述

---

随着网络信息安全问题的日益突出，网络上的各类应用系统面临着严重的安全威胁。各种安全问题层出不穷，影响着应用系统的自身安全，这些威胁包括：用户身份识别，用户访问权限控制，数据传输安全，对访问过程的完整记录等。具体包括：

### 1. 无法对用户身份进行识别

随着非授权入侵事件的增加，网络上的各种应用系统面临着严重的安全威胁。对于已经部署众多服务器的单位（包括 OA 服务器、电子邮件服务器、数据库服务器等），迫切需要建立严格的访问控制措施，依据用户身份和权限，对服务器的访问行为进行控制和授权，增强服务器的安全性，防止外来非法用户通过各种手段攻击或访问服务器。

### 2. 用户访问缺乏权限控制

一般来说，应用软件系统中，信息总是对特定用户开放，而对其他用户要求保密。用户被允许正常访问特定的信息，但同时又被禁止访问某些信息。用户在未授权情况下通过一些手段越权访问了别人不允许他访问的信息，可能造成他人的信息泄密。

尤其是一些重要的应用和业务系统，例如 OA 系统、电子邮件系统、数据库系统和文件服务器等，对于这些应用和业务系统，需特别关注合法用户的非授权侵犯问题，即合法用户在没有得到许可的情况下访问了他本不该访问的资源，尤其是一些存储有重要和敏感数据的服务器。

### 3. 数据传输缺乏安全保障

在数据传输的过程中，访问服务器的数据安全和完整性无法得到保障，非法用户可以通过各种手段窃取或篡改网络上传输的敏感数据。

### 4. 服务器访问缺乏记录

用户访问服务器，同时对其进行各种操作（如：私自拷贝、复制、删除、打印、刻录等），可能会造成文件丢失，内部重要数据被泄密。所以，缺乏对服务器访问的有效而真实的记录，使得安全事件发生后，无法对用户行为进行责任认

定。

为保证内部网络中业务系统数据访问、存储的安全性，实现对业务系统服务器、终端的密码安全保护，并使业务终端能够访问内网中的共享资源，需要提供基于服务器安全防护的整体解决方案。

## 第3章 系统需求

### 3.1 专用服务器的密码安全防护需求

为了增强服务器资源的访问控制和安全保护，可以在服务器资源前部署安全网关设备，安全网关可以用来在访问不信任的外网或内网上关键的服务资源时提供安全保护，对服务器的访问行为进行统一的认证授权和访问控制。同时，访问专用服务器的用户必须先与安全网关之间建立加密的 VPN 通信隧道，然后通过安全网关的授权后对服务器进行访问。

### 3.2 数据传输加密

客户端与服务器端进行数据交换时，通过客户端和安全网关之间的 VPN 隧道进行数据加密传输。客户端建立 VPN 隧道后，支持明通状态、密通状态、明通与密通共有的状态，缺省为密通状态。通过密通状态，业务终端只能与专用业务服务器双向传输加密数据；通过明通状态，业务终端可单向的访问其他子网的公共服务器，但不可访问专用业务服务器；通过明通与密通共有的状态可实现既与专用服务器双向传输加密数据，又可实现单向的访问其他子网的公共服务器。

### 3.3 数据本地加密存储需求

客户端用户使用个人私钥对本地文件进行加密存储。用户可应用本人的 USB-KEY 对自身或其他业务终端上的数据进行加密存储，当访问该数据时，只有使用本人的 USB-KEY 才能解密进行读取，其他用户是不能够通过其他方式进行访问的。

### 3.4 与内网PKI体系结合，建立安全认证机制

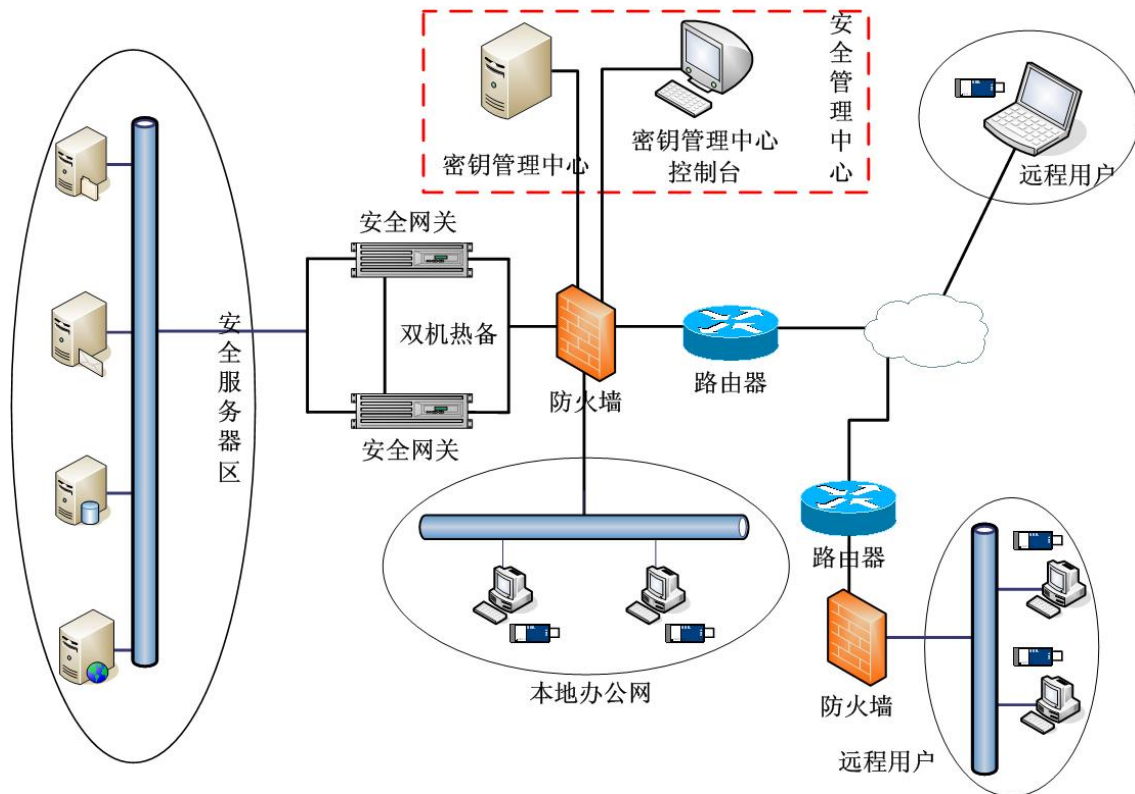
在建立 VPN 隧道以及访问授权控制均使用内网认证中心制发的数字证书实现。采用 PKI 数字证书和身份令牌在开机登录时强验证用户身份的合法性，各用

户独有的标识信息安全存放在 Key 中，由 USB 口读入，供终端计算机验证执行部件识别，在验证识别过程中不泄露身份特征信息，做到真正的不可假冒和伪造。如果用户无合法的 Key，就不能正常使用内网安全系统访问专用业务服务器。

### 3.5 客户端软件易于安装、操作简便

业务终端的客户端系统操作尽量简化，可以实现客户端驱动、代理软件的下载安装功能。

## 第4章 系统总体结构



基于安全网关的内网安全系统结构示意图

系统主要由安全管理中心、安全网关、安全客户端组成，其中安全管理中心由密钥管理中心、密钥管理中心控制台组成。通过与内网认证中心结合，为安全网关、USB-KEY 颁发数字证书，再由密钥管理中心为安全网关及 USB-KEY 下发数据加密密钥、安全规则及防护策略，使业务终端与安全网关建立 VPN 隧道以访问专网业务服务器。

### 4.1 安全网关

#### 4.1.1 设备功能

安全网关为新型网络安全设备，主要用于解决局域网之间的网络通信的安全保密问题，保护机密数据在局域网上进行安全传输的网络安全设备。通过对 IP 数据包的加密实现网络之间的加密通信；通过其网络访问控制功能在保护的网

和外部网络之间建立保护屏障，控制对内部网络的访问以保证内部网络的安全。它在网络层(IP层)采用IPSEC标准对数据报进行加密处理。利用IPSEC封装技术，可以组建VPN，并且对数据包提供鉴别服务、数据的机密性、抗重播及有限的抗流量分析等多项功能。具体功能如下：

- 安全通道：不同节点之间可建立各自独立的安全通道，提高网络安全性。
- 密钥管理：由安全管理中心统一产生、分发密钥，并定时自动刷新。
- 集中管理：安全管理中心对全网设备进行集中统一管理和监控；
- 身份鉴别：采用基于授权智能卡的身份鉴别管理，以控制对加密系统的使用，并提供网络密码机之间的相互鉴别；
- 日志审计：密码机自动记录运行状态，完整的日志信息自动向管理中心汇总。
- 防火墙：提供基于包过滤的防火墙功能，支持网络访问控制，防止外部用户攻击。

## 4.1.2 性能指标

- 物理接口：1000Base-T，1000Base-X，LC 接口、单/多模；SC 接口、单/多模等接口方式；
- 通信协议：以太网，IEEE802.3，IEEE802.1q，IEEE802.1p，10BASE-T，100BASE-Tx；
- 加密速率：双向处理 50~70Mbps；
- 电气指标：交流 220V (+10%~-15%)，50Hz (±3Hz)；
- 物理尺寸：2U 机架式结构。

## 4.2 安全管理中心

### 4.2.1 设备功能

安全管理中心是由密钥管理中心及密钥管理中心客户端组成，它是整个“基于VPN内网安全系统”的中心。密钥管理中心与安全网关、USB终端密码模块进行通信,实现对安全网关、USB终端密码模块的全面管理。密钥管理中心通过密钥管理协议统一管理整个密码机系统工作过程中的所有密钥,并且还提供对密

码机工作过程中的访问控制规则、网络参数、网络流量、状态查询、日志审计等管理。

密钥管理中心与管理中心客户机采用 C/S 结构，用户界面友好，操作简单，使用方便。

## 4.2.2 性能指标

- 设备参数：512M 内存、128M DOM 盘，1 个 RS232 串口，速率为 9600bps；2 个局域网接口，以太网卡的速率 10/100M 自适应。
- 密码强度：支持最大单独 300 个安全网关或单独 4096 USB 加密模块的密钥管理，终端用户并发接入能力为 200~300 个/分钟（在成功率为 100%的情况下，每分钟并发成功接入用户的个数。该数值与平台有关系）。
- 环境条件：工作温度为 0℃~40℃，存储温度为-20℃~55℃，相对湿度为 20%~80%。

## 4.3 USB-KEY 终端设备

终端设备采用 USB Key 或者 USB 密码盒设备，能支持客户端上本地数据存储加密和 VPN 通信的密钥协商加密算法。目前对本地存储加密和 VPN 通信密钥协商采用国家密码主管部门批准的商用密码算法。

USB Key 或者 USB 密码盒还存储用户的 RSA 私钥和用户证书，用来进行用户身份认证，认证流程请参考身份认证流程图。对于 VPN 的密钥协商则采用公钥列表方式来完成，用户的公钥列表集中存放在密钥管理中心。该用户的公钥列表，写入到用户设备中。

## 4.4 客户端软件

客户端软件包括 USB Key 或者密码盒的驱动，VPN 客户端的驱动和客户端软件。客户端首先需要安装密码设备的驱动，然后通过 WEB 方式下载安装客户端软件。客户端使用 USB Key 或者 USB 密码盒会有一个登录过程，需要用户输入密码。这个登录过程可以和 VPN 的登录合二为一，减少用户输入密码的次

数，增加易用性。用户一旦登录，首先启用密码设备，然后读取用户信息和证书，开始基于用户证书的身份认证过程。如果身份认证成功，则开始进行 VPN 密钥协商（IKE），IKE 采用公钥列表方式来建立 IKE 的会话密钥。

## 第5章 系统技术方案

### 5.1 系统结构

系统主要由安全管理中心、安全网关、安全客户端组成，其中安全管理中心由密钥管理中心、密钥管理中心控制台组成。

系统业务流程如下：

- 1 安装配置密钥管理中心和安全网关，为安全网关和密钥管理中心服务器发放数字证书，手工导入证书到安全网关和密钥管理中心服务器的密码卡中，导入并维护基础数据；
- 2 用户领取 UKey 或者 USB 密码盒，在 CA 申请数字证书，证书下载到 UKey 或 USB 密码盒中；
- 3 用户通过 WEB 方式安装客户端软件，用户使用 UKey 或 USB 密码盒进行注册；
- 4 密钥管理中心控制台为用户设置访问受保护服务器的策略；
- 5 用户输入密码登录安全网关，完成身份认证，获得访问授权，通过 VPN 隧道访问受保护服务器；
- 6 用户退出登录或者拔出 USB 密码设备，断开 VPN 隧道，禁止访问受保护服务器。

安全网关主要是完成 VPN 的建立和用户访问控制。安全管理中心负责基础数据的获取，访问权限和角色的定义，用户公钥列表的维护等，安全管理中心还是数据集中存储中心。安全网关配置密码卡，支持 SCB2 算法，用于 VPN 的 IKE 协商加密。安全网关第一次使用的时候需要通过命令手工导入它的证书和私钥到密码卡中，用密码卡来完成和客户端用户的双向身份验证。安全网关还需要下载它的公钥列表，用来进行 VPN 的 IKE 协商。

而客户端用户的证书是通过 CSP 接口获取的，用来进行用户身份验证。具体流程参考身份验证流程图。

用户客户端首先通过身份认证。身份认证通过后，客户端将与安全网关建立

安全隧道。至此安全网关已经为应用系统访问进行了用户的身份认证和建立了网络加密隧道。

当用户对应用系统发起访问请求，安全网关将通过访问控制来确定是否发送此请求给目标服务器。

## 5.2 安全机制

### 5.2.1 用户认证

当用户连接到安全网关时，用户必须确认是连接到正确的内网安全系统，而不是一些假冒的服务器；同时，安全网关也必须确认用户的真实身份，而不是一些假冒的恶意攻击者。因此，系统必须提供双向的认证机制。

安全网关通过 PKI/CA 机制来验证双方的身份，避免“中间人攻击”。当连接建立时，终端会验证服务器的证书，如果服务器证书不是所信任的 CA 中心所签发的，连接将被主动拒绝；同样，安全网关也会验证终端用户的证书，保证用户身份的真实性和合法性。而“中间人”无法提供这样的合法身份，也就杜绝了“中间人攻击”现象。

### 5.2.2 用户授权

安全网关通过授权机制来控制合法终端访问应用系统的请求，每个终端用户都在安全网关的控制下来访问各个应用系统。

安全网关对每个用户都可以设置详细的访问权限，包括两个层次：一是用户是否可以访问到应用系统；二是用户可以访问到哪个应用系统。经过这两个层次的授权，有效地控制用户的访问权限。

### 5.2.3 VPN隧道

完成身份校验后，终端和安全网关之间建立起 VPN 隧道，通过终端本地的虚拟网卡和安全网关之间形成一个密通通道。密通通道传输报文使用加密技术进行包重组。同时，可选择终端的明通连接将断开。使用这样的技术基于两个目的：

一是终端和应用系统之间的通讯将在密通通道中进行，没有合法用户身份不可能进入此密通通道，也就无法对应用系统进行攻击；二是杜绝了恶意攻击者通过木马作为跳板来攻击应用系统。

## 5.2.4 数据安全

终端连接到安全网关时，首先采用 IKE 和安全网关之间进行密钥的协商，并且在通讯过程中定期地进行密钥协商以更换会话密钥，增强数据报文的安全强度。（客户端下载动态算法，采用扩散算法的方式提高本地 U-KEY 的加密速度）

报文传输过程中，采用定期更新的会话密钥进行加密传输，中间拦截者无法对数据报文进行还原。

## 5.2.5 自身安全

### (1) 身份认证

当安全网关收到一个来自用户的连接请求时，通过挑战/响应方式完成基于证书的身份认证。如果认证成功，获取该用户的访问授权信息，根据授权信息决定是否运行该用户访问受保护服务器。

### (2) 拒绝服务攻击

内置 IP 黑洞功能，对于非以 KEY 为源头发出的网络连接不予响应，可以预防黑客漏洞扫描、DDOS 攻击等恶意破坏。只开放需要的服务必需的端口，其他端口一律屏蔽，预防漏洞攻击等攻击手段。

### (3) IP 过滤

当某个用户向安全网关发起连接请求，安全网关会检查该用户的 IP 地址是否在信任列表，如果该 IP 地址不在信任列表，则该次连接请求将被拒绝。

管理员可以将已知信任的 IP 地址或 IP 网段添加到安全网关的信任列表中。例如，管理员可以将内网的每个网段添加到信任列表之中。

### (4) 软件升级

客户端可以自动连接安全网关进行在线升级。客户端周期性的向安全网关查询新版本程序。如果有新版本程序存在，客户端会下载新版本的程序进行升级。

安全网关建立在裁剪定制的 LINUX 内核上,只运行必要的代理程序和守护进程。内置 IP 黑洞功能,对于非以 KEY 为源头发出的网络连接不予响应,可以预防黑客漏洞扫描、DDOS 攻击等恶意破坏。只开放需要的服务必需的端口,其他端口一律屏蔽,预防漏洞攻击等攻击手段。

受保护服务器放置于安全网关之后,在整个网络之中相当于被安全网关物理隔离,在没有 KEY 身份的情况下,无从获知应用系统的存在,即任何恶意攻击都无法攻击这个目标。

## 5.2.6 数据备份

将安全网关中的数据(用户信息、资源信息、安全策略等)备份到其他服务器,当安全网关发生故障时可以及时将备份数据导入安全网关,方便维护。

## 5.2.7 集群功能

采用集群功能可以将多台独立的安全网关整合起来提供高性能服务,减少每台安全网关的负载,提高整个安全网关集群的性能。

当网络规模扩大,原有安全网关超负荷时,可以简单的利用集群功能添加新的安全网关到整个集群中,提供高可用性以保证应用系统的正常工作。

## 5.2.8 日志审计

安全管理中心提供了非常丰富的日志功能,管理者可监视到异常流量、试图非法访问应用系统、异常登录等有效的分析信息,为综合分析提供依据。完整、精确的日志记录是成功进行审计的基础,是事后追查追踪的依据,同时也是预测安全发展态势的指南。本系统日志记录依据下列原则:

### ■ 日志数据准确性

无论在哪种情况下,都提供准确的日志数据不误报。

### ■ 日志的完整性

系统提供完整的日志数据。

### ■ 日志的不可抵赖性

## ■ 日志的实时性

日志内容有：

- 管理员操作日志
- 虚拟安全网络登录日志
- 应用服务访问日志
- 非授权访问日志

日志系统提供实时日志查看、告警日志查看、告警设置和历史日志审计。

## 5.3 系统管理

系统管理分为几个部分：基础数据维护管理，设备管理，用户管理，密钥管理，资源管理，角色权限管理。

设备管理包括网关设备和密钥管理中心服务器设备的注册和维护。控制台可以通过设备来查看相应的设备的状态，密码卡工作状态，VPN 隧道连接状态等信息，还可以设置网关设备的 VPN 隧道参数等信息。

用户管理主要是针对客户端注册用户的管理，用户使用的 USB 密码盒的管理。

密钥管理包括用户的公钥列表管理和密码设备的管理，涉及到整个密钥生成的生命周期的管理。

资源管理则是受保护的內网服务器的定义，包括受保护服务器的 IP 地址和服务端口等信息。

角色权限管理则是定义用户通过角色对服务器资源访问的权限。

其它管理功能还包括管理员帐号管理，日志审计，系统配置和数据备份恢复等。

## 第6章 售后服务

当客户部署安全网关时，为了使客户能够顺利部署实施，中安网脉（北京）技术股份有限公司会应客户的要求，成立专门的项目服务小组，该小组成员均具有丰富的实践经验，扎实的理论功底，热情周到的服务，从而形成技术支持、客户培训、资料支持、备件支持、工程服务等一体化的客户服务体系。我们以客户满意为一切工作的基本出发点，跟踪客户实际需求，建立完善的服务机制，向客户提供专业化、标准化和产品化的服务，在向客户提供优质产品的同时，又能保障为客户提供快速、高效、可持续的终身服务。

在客户采纳了安全网关后，我们将为客户提供下述专业技术服务。

- ◆ 系统配置建议
- ◆ 购买相关产品
- ◆ 系统实施服务
- ◆ 系统售后服务
- ◆ 软件培训服务

下面对上述各项服务加以详细说明：

### 6.1 系统配置建议

我们将客户单位目前的系统情况和切实要求做详细调研后，对系统的配置方案做出更加具体的建议。

若系统在将来需要升级和/或移植时，我们将对系统升级和/或移植方案提供参考建议。

### 6.2 购买相关产品

在双方签订了购买产品和服务的合同之后，我们将为客户订购所有相关的系统软件产品(包)和/或许可证，并办理所有相关事宜。

- 系统准备及检验

合同签订以后，整个系统所需全部硬件和系统软件将在 30 个工作日内（自合同签订之日起）到货。技术人员将在货物发给客户前对该系统的所有软件逐一进行清点及检验，以做到交给客户的产品是完好无误的。

- 开箱验机

本单位将在到货等工作完成后一周内（一般 2~3 天）派人员前往客户处开箱、验机和清点货物。在货物经检验没有任何问题的情况下，本单位将开始安排装机。

- 系统软件的安装

我们负责平台系统的安装工作，根据实际情况及协议，我们将派系统工程师实施系统软件安装。

- 保修期

在系统的软件安装完成并经买卖双方签字验收之日起开始计算保修期。产品的保修期按照厂商的保修条例执行，在保修期内，本单位负责免费的软件维护，保修期满，还可以根据需要购买一年以上的保修期。

## 6.3 系统实施服务

在系统实施服务期间，我们将与客户一起工作，保证该系统可满足客户最适合的功能需求，以及充分和完整地展示平台系统有关的技术和产品特性。

系统实施服务主要包括如下工作：

- 了解业务：对客户的业务流程进行了解和分析。
- 了解需求：对客户的业务需求进行了解和分析。
- 了解数据：对客户的相关信息数据进行了解和分析。
- 系统规划与部署：根据客户的应用系统需求，规划系统，包括网络规划、服务器规划、平台接口等，然后进行相应的部署。
- 综合测试：对系统进行综合的功能测试和系统测试。

我们在系统实施服务期间，也为客户提供顾问服务。我们将尽可能地将有关的理论、技术、知识、方法和经验与客户人员交流。客户人员通过和本单位人员

一起工作，可以逐渐掌握平台系统的使用与管理。

双方的工作场所可根据需要在本单位场所或客户场所、或两处同时进行，以客户场所为主。

## 6.4 系统售后服务

- 售后服务的时间

我们承诺对安全网关进行终身维护，其中在系统交付使用开始一年的时间为免费维护期，之后的维护按签订的后期维护合同进行收费。

- 售后服务的内容与方式

我们有专业的客户服务中心与技术支持部作为售后服务的坚强后盾。主要有：

- 按客户请求，对系统提供阶段性的检查和维护。
  - 对新的版本，补丁提供安装服务。
  - 日常使用的技术支持，客户可采用电话，邮件，EMAIL，网上等方式向技术支持部门寻求支持。
  - 若出现重大事故，由专业人员为客户提供指导性恢复。
  - 对软件的错误，24 小时内提供临时处理方法，2 周内提供新的版本或补丁。
  - 若对平台系统进行较大的功能的增加或变更，需由双方充分协商后再确定。
- 软件系统升级保证
  - 软件版本升级后，以电话和电子邮件的方式通知客户，客户可通过网上下载新的版本或补丁。
  - 客户文档更新后，客户可通过网上下载或电子邮件的方式获得最新的客户文档。

## 6.5 软件培训服务

人员培训是系统投产前一个很重要且不可忽略的环节，我们将会安全网关部署的期间按照客户的要求安排各种培训，以保证安全网关顺利为客户提供服务。

## 6.6 技术支持服务

如果客户在安装和使用安全网关时，遇到了问题请及时告诉我们，我们将尽全力和你们一起解决问题，最大限度地保护客户的权益。

通信地址：北京市丰台区富丰路7号

邮政编码：100070

联系人：吴科科

邮箱：support@sinoinfosec.com

技术支持电话：010-63783209、83635361、83635337

网址：www.sinoinfosec.com 或www.sinoinfosec.cn

客户还可以在互联网上随时和我们取得联系。假如你利用网络和我们联系，请在问题报告中安全网关的版本信息、许可证信息、主机使用平台名称和尽可能详细的问题描述，以便于我们能尽快解决您的问题。

中安网脉（北京）技术股份有限公司竭诚为客户提供热情周到的服务，为您解决难题，提供支持。保护您的安全网关系统能够安全使用是我们最大的心愿。