



HuaTech-2000 型防火墙

北京中软华泰信息技术有限责任公司

目 录

1.	北京中软华泰信息技术有限责任公司公司简介	3
2.	HuaTech-2000 系列防火墙简介	4
3.	HuaTech-2000 系列防火墙的基本功能和特性	5
3.1.	基本功能	5
3.2.	HuaTech-2000 系列防火墙特性	6
4.	HuaTech-2000 系列防火墙型号规范说明	10
5.	接口设计说明	11
5.1.	型号	11
5.2.	系统组成	11
5.3.	接口配置	11
5.4.	电气性能	11
5.5.	参考的安全规范及标准	12
5.6.	抗干扰性	12
6.	HuaTech-2000 系列防火墙功能介绍	13
6.1.	多端口结构, 多协议支持	13
6.2.	状态检测技术	13
6.3.	深层过滤技术	14
6.4.	地址绑定技术	14
6.5.	双向网络地址转换技术	14
6.6.	动态路由	15
6.7.	多路由表、源地址选路	16
6.8.	组播路由	16
6.9.	内容过滤 (色情防堵)	17
6.10.	阻止P2P软件	17
6.11.	用户认证	17
6.12.	时间段访问控制	18
6.13.	入侵检测	18
6.14.	病毒扫描	18
6.15.	应用代理	19
6.16.	日志审计	19
6.17.	流量控制	20
6.18.	带宽控制	20
6.19.	VPN功能	20
6.20.	双机热备功能	20
6.21.	负载均衡功能	21
6.22.	支持VRRP	21
6.23.	较强的抗攻击能力	21
6.24.	采用内核性能优化和安全加固技术	22
7.	HuaTech-2000 型防火墙的典型应用	23
8.	HuaTech-2000 型防火墙功能、技术指标一览	24

1. 北京中软华泰信息技术有限责任公司 公司简介

公司成立背景

面对网络经济的挑战，全球经济一体化的发展态势，信息安全对一个国家和民族的战略重要性已成为不争的事实。为了迎接网络经济的挑战，维护国家的信息安全，加速我国信息安全技术及产品的研究、开发和产业化进程，北京中软华泰信息技术有限责任公司在新千年伊始即以高屋建瓴之势完成了组建并投入运行。

技术力量雄厚

享有国内安全界知名院士的指导，拥有以博士后、博士、硕士为骨干力量的高起点的团结奋进的研发队伍。

市场前景广阔

以强大的市场优势为依托，以互连网、局域网、ICP、ASP 等领域为行业开拓目标，以与 IT 业知名系统集成商捆绑为特点，完成自身的市场建设。

为您提供的服务

以安全操作系统和操作系统安全为产品研发和推广对象。竭诚为您提供以下服务：

- 各种网络安全整体解决方案。承接方案的设计及工程建设。
- 安全操作系统和操作系统的增强工具（Windows /Unix）。
- 操作系统及其网络安全保密平台。
- 防火墙、安全网关以及 IPSEC 系列产品。
- 系统漏洞扫描系统，入侵检测系统以及实时网络安全监控系统。
- 电子商务安全和信息对抗安全产品。
- 操作系统应用产品开发。
- 安全咨询和培训。

2. HuaTech-2000 系列防火墙简介

计算机和网上技术正以惊人的速度改变着整个世界，全世界的公司都面临着巨大的挑战和机会。借助网络，人们可以与异地的同事或是客户进行实时交流，快速地收取和发送信息；借助网络，人们可以提高工作效率、减少开支，同时做到了在尽可能短的时间内对市场形势的变化做出应急反应。

在这种环境下，局域网越来越多地被应用到公司的日常办公当中。公司的内部网上的信息有许多是属于商业机密，一旦被不怀好意的黑客窃取或被竞争对手得到，都将给公司带来难以预想的损失。但公司为了在 Internet 上发布信息，共享资源，就不得不将自己的内部网一定程度的对外开放，这就在无形当中增加了安全隐患，使有不良企图的人有机可乘。为了使信息系统在保障安全的基础上被正常访问，需要一定的设备来对系统实施保护，保证只有合法的用户才可以访问系统。就目前看，能够实现这种需求的性能价格比最优的设备就是防火墙。

HuaTech-2000 系列防火墙是由北京中软华泰信息技术有限责任公司自主开发研制，基于高速硬件平台和稳定的操作系统的复合型防火墙设备，具有操作简便、实用性强、高效、经济等特点。该产品已获得公安部认证以及计算机信息系统安全专用产品的销售许可，通过了中国信息安全测评认证中心的测评，安全可靠，是您保护内网安全不受侵害的首选产品。

HuaTech-2000 系列防火墙产品目前分为两种规格：百兆系列与千兆系列。

HuaTech-2000 防火墙产品已经取得：

公安部安全产品销售许可，销售许可证号：XKC33379（百兆）；

XKC33226（千兆）；

国家信息安全测评认证中心认证，注册号：CNISTEC2005TYP380；

国家认可注册号：A05-99；

军用信息安全产品认证证书：军密认字第 0062 号；

国家保密局科学技术成果鉴定证书：（2002）第 4 号。

HuaTech-2000 系列防火墙已经在中国人民银行、中国银行、中国民生银行、上海市公安局、中石化、新华社、河北省电子政务、北京市委党校等部门成功运行，获得用户的广泛好评。

3. HuaTech-2000 系列防火墙的基本功能和特性

3.1. 基本功能

- 支持状态检测功能
- 支持深层过滤技术
- 支持 DMZ 功能
- 支持长连接
- 支持地址绑定功能
- 支持双向地址转换功能
- 支持带宽管理功能
- 支持流量控制功能
- 支持透明桥连接
- 支持 VPN（虚拟专用网络）功能扩展
- 支持组播路由
- 支持基于 802.1Q 的 VLAN 扩展
- 支持 OSPF、RIP、BGP 等动态路由协议
- 支持 VoIP（H.323 协议）
- 支持双机热备功能
- 支持负载均衡功能
- 支持 VRRP
- 支持日志审计功能
- 支持用户认证功能
- 支持代理功能
- 支持内容过滤功能
- 支持 IDS 入侵检测功能
- 支持与第三方的 IDS 服务器联动
- 支持第三方的病毒扫描接口

- 支持阻止 P2P 软件
- 支持远程安全集中统一管理
- 可根据用户需求加载冗余电源模块

3.2. HuaTech-2000 系列防火墙特性

安全可靠

HuaTech-2000 系列防火墙建立在安全操作系统基础上。通过对操作系统内核的大规模裁减，剔除了原有的不安全模块，增加了自主开发的安全加固模块。通过对操作系统的改造，大大加强了系统内核的安全性和抗攻击能力。同其他同类防火墙相比，避免了因操作系统故障而导致的防火墙工作异常。

HuaTech-2000 系列防火墙功能全面，如果配置得当，可以保证您的网络系统坚如磐石。HuaTech-2000 系列防火墙的功能强大，具有状态检测功能、时间段控制访问功能、代理功能、地址绑定功能、双向地址转换功能、双机热备功能、日志审计功能等，同时 HuaTech-2000 系列防火墙系统较同类产品更加强壮、稳定，对其支撑平台而言更加安全。除了网络管理员，其他人员很难非法闯入防火墙系统。而且由于 HuaTech-2000 系列防火墙使用透明接入方式，使一般用户在正常操作时感觉不到防火墙的存在，这样既不影响网络的工作效率，又保证了更高的安全性。

高速稳定

HuaTech-2000 系列防火墙的操作系统内核采用的是经过适当裁减和安全加固的专用安全操作系统，从根本上保证了防火墙系统的稳定性。

HuaTech-2000 系列防火墙系统根据具体型号的不同采用了不同级别的中央处理器，这样既保证了不同级别的防火墙系统能够满负荷高速运转，又可为用户节约不必要的开支，做到物尽其用。

HuaTech-2000 系列防火墙采用了多种安全防护技术，对于不同的安全级别的网络服务采用不同的控制策略，保证了系统的高速性和通用性。安全防护机制的选择，完全根据用户对其具体业务系统的安全需求而定。不同的安全控制策略可以选择相应的安全防护机制。

对各种标准服务和用户自定义服务的高度兼容

HuaTech-2000 系列防火墙既支持 Internet 网络的主要服务（如 HTTP, SMTP, POP3, FTP, Telnet 等）的所有应用程序，又支持 UDP 一类非连接协议的应用程序。而且，还支持数据库访问这样的商务应用程序和象 Real Audio, VDOLive 和 Internet Phone 这样的多媒体应用程序。用户不必担心使用防火墙后，出现某些服务失效的副作用。另外，如果用户需要，HuaTech-2000 型防火墙可以支持用户的自定义服务。

HuaTech-2000 系列防火墙带有的透明代理服务器模块支持多种平台的多种网络应用程序，保证用户原有软件的普遍兼容。使普通用户在处理大多数日常业务时感觉不到防火墙的存在。

高扩展性

HuaTech-2000 百兆系列防火墙的标准配置为

标准 1U: 4 个 10/100 以太网控制器 (RJ45 接口), 1 个 Console 接口, 1 个双机热备接口。

可根据用户的具体需求可扩充 4 个接口。

HuaTech-2000 千兆系列防火墙的标准配置为

标准 2U: 4 个 10/100/1000 以太网控制器 (RJ45 接口), 4 个多模光纤接口, 1 个 Console 接口, 1 个双机热备接口。

可根据用户的具体需求适当扩充接口数量。

对外部的非法扫描和攻击的响应能力

HuaTech-2000 系列防火墙提供接口，支持与指定厂商的 IDS 系统联动，当系统检测到某些数据信息中包含入侵或误用的特征时，防火墙会认为该连接有入侵企图或误用倾向，并向一个预定的地址发送报警信息，根据管理员的配置，防火墙将自动切断与发起攻击的主机的连接，从而防止入侵或误用的进一步发生。

较强的抗攻击能力

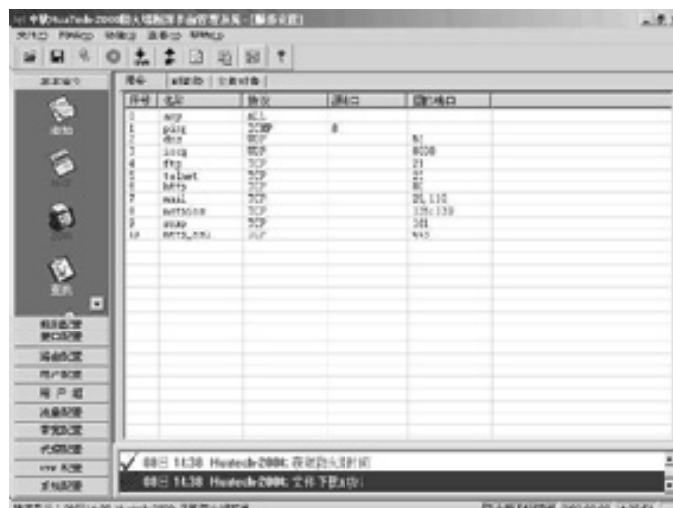
处于内网与外网通信唯一通路上的防火墙无形当中成为黑客攻击的首要目标，要保护内网的安全，首先要保证防火墙自身具有较强的抗攻击能力。HuaTech-2000 系列防火墙能够

抵御大多数常见的网络攻击，如 land-based attack、ping flood、teardrop attack、ping of death、ping sweep、smurf attack 和 syn flood 等等。

配置简单

HuaTech—2000 系列防火墙的配置非常简便。对它的操作及设置只需使用防火墙配置程序就可以实现。系统提供了三种配置管理程序：GUI 管理器、Web 管理器和 CLI 管理器。

配置程序（GUI）是本产品的专用配套程序。该管理器具有界面友好直观、功能齐全、通俗易懂等特点，可运行于 Microsoft Windows9X/Me/NT4.0/2000/XP 环境下。防火墙的所有功能都能够通过 GUI 管理器配置实现。管理器界面如下图所示：

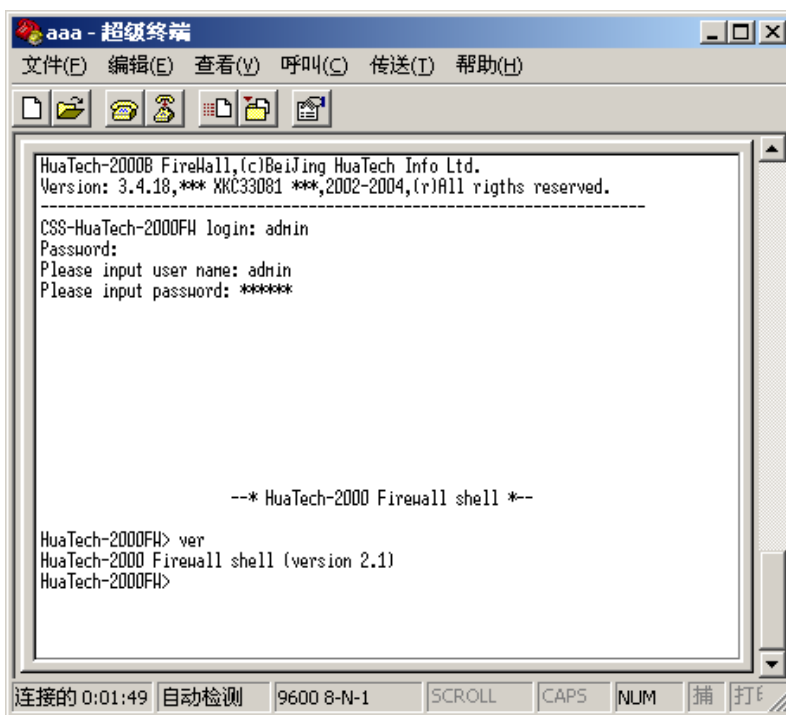


Web 配置方式为用户提供了简洁、友好的配置界面和详尽的提示说明，能够使用户在尽量短的时间内掌握防火墙的配置方法，但相对安全性较低。Web 管理器界面如下图所示：



CLI 命令行方式是指使用防火墙提供的 Console 接口进行本地管理。该管理器具有最高

的安全级别。管理器界面如下图所示：



真正支持透明接入

HuaTech—2000 系列防火墙系统做到了真正的透明，即无论使用任何功能，对正常使用网络的合法用户来说防火墙系统是不可感知的。很显然系统具有这样的功能有两个好处：

(1)防火墙系统的安装和卸载都不会影响网络的任何一部分，管理人员可以平滑地安装和卸下 HuaTech-2000 系列防火墙系统，而无需更改网络中其它设备的设置或参数，既可以节省网络管理员宝贵的工作时间，又不会影响到网络用户的正常工作。

(2)减少了用户的操作。一般情况下，用户为了使用代理服务器要在客户端的应用程序（如浏览器、FTP 程序）上设置代理的 IP 地址和端口，而且还要有一个前提，就是客户端应用程序必须支持代理（有很多种客户端应用程序是不支持代理的，如 TELNET 程序）。而使用 HuaTech-2000 系列防火墙系统的用户不必再做任何设置，就可以直接使用代理服务，极大的方便了网络用户。

支持集中统一管理

HuaTech—2000 系列防火墙支持安全管理中心的管理接口程序。通过安全管理中心，网络管理人员可以在一个工作站上远程管理多台防火墙设备，既节省了人力资源，又缩短了配置管理防火墙的时间。

4. HuaTech-2000 系列防火墙型号规范说明

HuaTech-2000 型防火墙（百兆系列）

产品规格	说明	适用模式
HT-FW-2000-BX	4*10/100M 低端硬件，基本功能	低端
	透明连接功能；路由连接功能；状态检测功能；支持 DMZ 功能；地址绑定功能；时间段控制访问功能；NAT 网络地址双向转换功能；支持防 DOS 攻击；日志审计功能--运行日志、管理日志（状态信息目前暂不提供）；PPPOE	
HT-FW-2000-EX	4*10/100M 高端硬件，包含多种功能模块	中高端
	在 BX 基础上增加：支持用户认证功能（OTP）；支持流量控制功能；应用代理；支持 VLAN；支持入侵检测功能（IDS）；支持与第三方 IDS 设备联动；支持与第三方病毒服务器联动；VPN 功能（网关到网关，不能做规则控制）；支持深层过滤；支持阻止 P2P 软件；支持组播路由；支持双机热备功能；支持 SNMP；完整的日志审计功能	
HT-FW-2000-TX	4*10/100/1000M 高端硬件，包含最新功能模块	高端
	在 EX 基础上增加：支持用户认证功能（RADIUS）；VPN 功能（客户端到网关，网关到网关可做规则控制）；支持负载均衡；支持路由策略；支持动态路由功能；VRRP(虚拟路由冗余协议)	

HuaTech-2000 型防火墙（千兆系列）

产品规格	说明	适用模式
HT-FW-2000-GX	标配千兆网卡 4 个,多模光纤口 4 个, 包含所有最新功能	高端

- 以上产品规格及功能仅供参考，防火墙系统本身可根据用户的实际需求定制。

5. 接口设计说明

5.1. 型号

HuaTech-2000 型防火墙（以 HT-FW-2000-TX 为例）

5.2. 系统组成

防火墙（硬件）：是一个高速稳定的硬件平台和经过安全加固的操作系统的完美结合体。

配置管理器（软件）：系统提供了三种管理程序，GUI、Web 和 CLI。用于防火墙进行配置及日常管理，其中 GUI 管理器支持远程集中统一管理；系统还提供了统一的日志管理系统。以上管理软件均可运行于 Microsoft Windows 9X/Me/NT4.0/2000/XP 环境下。

5.3. 接口配置

HuaTech-2000 百兆系列防火墙的标准配置为：

- 4 个 10/100 以太网控制器，RJ45 接口（内网、外网、DMZ、DMZ1）
- 2 个 CONSOLE（双机热备、Console）（RJ45）

HuaTech-2000 千兆系列防火墙的标准配置为：

- 4 个多模光口模块（内网、外网、DMZ、DMZ1），4 个 10/100/1000 以太网控制器，RJ45 接口（DMZ2、DMZ3、DMZ4、DMZ5）
- 2 个 CONSOLE（双机热备、Console）（RJ45）

5.4. 电气性能

电源

220V/50Hz 3.0A (最大) 260W (最大)

环境规范

运行温度: 0 - 45 摄氏度

非运行温度: -20 - 65 摄氏度

相对湿度: 10 - 90% @ 40 摄氏度, 非冷凝

5.5. 参考的安全规范及标准

UL 1950

EN 41003

AS/NZS 3260

AS/NZS 3548 Class A

CSA Class A

FCC Class A

EN 60555-2

VCCI (ClassII)

5.6. 抗干扰性

IEC - 1000 - 4 - 2 (ESD)

IEC - 1000 - 4 - 3 (辐射敏感性)

IEC - 1000 - 4 - 4 (电快速瞬变)

IEC - 1000 - 4 - 5 (电涌)

IEC - 1000 - 4 - 3 (谐波)

6. HuaTech-2000 系列防火墙功能介绍

6.1. 多端口结构，多协议支持

防火墙提供了两个或两个以上的独立的网络接口，将受保护网络从物理上分隔开来，不但提高了安全级别，更方便了防火墙与网络之间的连接；该防火墙除了支持标准的 TCP/IP 协议，还支持 802.1q 和 VOD 各种不同层次的协议标准。

6.2. 状态检测技术

状态检测技术：基于防火墙所维护的状态表的内容转发或拒绝数据包的传送，比普通的包过滤有着更好的网络性能和安全性。普通包过滤防火墙使用的过滤规则集是静态的。而采用状态检测技术的防火墙在运行过程中一直维护着一张状态表，这张表记录了从受保护网络发出的数据包的状态信息，然后防火墙根据该表内容对返回受保护网络的数据包进行分析判断，这样，只有响应受保护网络请求的数据包才被放行。对用户来说，状态检测不但能提高网络的性能，还能增强网络的安全性。

HuaTech-2000 系列防火墙的包过滤模块处于防火墙主机操作系统的网络结构中的数据链路层与 IP 层之间，数据链路层传送的数据格式与实际的网络有关，例如以太网、令牌环网、DEC net 等不同的网络拓扑，有着不同的数据格式，与网络协议有关的是 IP 层及以上的各层，所以 HuaTech-2000 系列防火墙拦在网络协议的最底层，能够看到完整的网络封包，包括 IP、TCP、UDP 及 ICMP 封包。即在网络层对数据报文进行检查和过滤。HuaTech-2000 系列防火墙对需要转发的数据包，先获取其包头信息，包括 IP 层所承载的上层协议的协议号、数据包的源地址、目的地址、源端口、目的端口等，然后与设定的规则进行比较，并根据比较的结果决定对数据包进行转发或者丢弃。也就是说，检测系统对用户数据不做任何操作，即不处理数据包中的用户数据。有了数据检测，可以允许别人经由某种特定协议向我们发送电子邮件，或者不让别人从外界使用某种特定的协议登录，等等。但是，这并不是说能控制某个用户能否从外部远程登录，而其它用户不能这样做。因为“用户”不是数据检测系

统所能辨认的。通过检测，我们可以根据数据包的协议、IP 地址、端口等做出判断，从而做出相应的处理。

6.3. 深层过滤技术

深度过滤技术深入检查通过防火墙的每个数据包及其应用载荷。虽然只检测包头部分是一种更加经济的方式，但是很多恶意行为可能隐藏在数据载荷中，通过防御边界在安全体系内部产生严重的危害。因为数据载荷中可能充斥着垃圾邮件、广告视频以及企业所不欣赏的 P2P 传输，而各种电子商务程序的 HTML 和 XML 格式数据中也可能夹带着后门和木马程序在网络节点之间交换。所以，在应用形式及其格式以爆炸速度增长的今天，仅仅依照数据包的第三层信息决定其是否准入，实在无法满足安全的要求。HuaTech-2000 系列防火墙支持数据包深层过滤技术，深度包检测引擎以基于指纹匹配、启发式技术、异常检测以及统计学分析等技术的规则集。可以有效的过滤 HTTP FTP SMTP POP3 协议中的非加密内容，HTTP FTP 命令并根据网络病毒和木马中的特征字符来阻止外网对内网进行网络病毒和木马攻击。更加有效保护内网用户的安全，使防火墙起到入侵保护的作用。

6.4. 地址绑定技术

每一块网卡都具有一个唯一的物理标识号码，也就是网卡的 MAC 地址，由于 MAC 地址的唯一性，决定了某一台主机的合法 IP 地址与其网卡的 MAC 地址绑定起来的对应关系是唯一的，HuaTech-2000 系列防火墙具有地址绑定功能，可以通过建立起来的合法 IP 地址与 MAC 地址的对应关系识破非法用户盗用合法 IP 地址的阴谋，并拒绝该连接请求。

6.5. 双向网络地址转换技术

NAT (Network Address Translation) 网络地址转换是一种将一个 IP 地址域映射到另一个 IP 地址域技术，从而为终端主机提供透明路由。NAT 包括静态网络地址转换、动态网络地址转换、网络地址及端口转换、动态网络地址及端口转换、端口映射等。NAT 常用于私有

地址域与公用地址域的转换以解决 IP 地址匮乏问题。

从内向外的地址转换技术（源地址转换）有一个非常大的缺点，就是外面的合法用户无法主动的访问防火墙所保护的内部网络。为了克服这个缺点，HuaTech—2000 系列防火墙实现了从外向内的地址转换（目的地址转换）。利用这种技术可以在防火墙的外网口上绑定多个公有 IP 地址与局域网上的相应服务器的对应关系，当外面的主机访问防火墙的外网口的某个 IP 地址时，防火墙将来自外部的服务请求转发到局域网内的真正的服务器上。这样就达到了既隐藏了网络内部信息，又可以让外部的合法用户访问内部的服务器。

6.6. 动态路由

动态路由是网络中的路由器之间相互通信，传递路由信息，利用收到的路由信息更新路由表的过程。它能实时地适应网络结构的变化。如果路由更新信息表明发生了网络变化，路由选择软件就会重新计算路由，并发出新的路由更新信息。这些信息通过各个网络，引起各路由器重新激活其路由算法，并更新各自的路由表以动态地反映网络拓扑变化。动态路由技术在当前网络规模不断扩大，拓扑结构不断复杂化的今天尤为重要。

HuaTech-2000 系列防火墙支持基于 RIP(Routing information Protocol)、OSPF(Open Shortest Path First)以及 BGP4 (Border Gateway protocol) 的高级动态路由。

RIP 协议最初是为 Xerox 网络系统的 Xerox parc 通用协议而设计的，是 Internet 中常用的路由协议。RIP 采用距离向量算法，即路由器根据距离选择路由，所以也称为距离向量协议。路由器收集所有可到达目的地的不同路径，并且保存有关到达每个目的地的最少站点数的路径信息，除到达目的地的最佳路径外，任何其它信息均予以丢弃。同时路由器也把所收集的路由信息用 RIP 协议通知相邻的其它路由器。这样，正确的路由信息逐渐扩散到了全网。RIP 使用非常广泛，它简单、可靠，便于配置。但是 RIP 只适用于小型的同构网络，因为它允许的最大站点数为 15，任何超过 15 个站点的目的地均被标记为不可达。而且 RIP 每隔 30s 一次的路由信息广播也是造成网络的广播风暴的重要原因之一。因此它并不适合复杂的大型网络。

OSPF 是一种基于链路状态的路由协议，需要每个路由器向其同一管理域的所有其它路由器发送链路状态广播信息。在 OSPF 的链路状态广播中包括所有接口信息、所有的量度和其它一些变量。利用 OSPF 的路由器首先必须收集有关的链路状态信息，并根据一定的算法

计算出到每个节点的最短路径。而基于距离向量的路由协议仅向其邻接路由器发送有关路由更新信息。与 RIP 不同，OSPF 将一个自治域再划分为区，相应地即有两种类型的路由选择方式：当源和目的地在同一区时，采用区内路由选择；当源和目的地在不同区时，则采用区间路由选择。这就大大减少了网络开销，并增加了网络的稳定性。当一个区内的路由器出了故障时并不影响自治域内其它区路由器的正常工作，这也给网络的管理、维护带来方便。

BGP 是为 TCP / IP 互联网设计的外部网关协议，用于多个自治域之间。它既不是基于纯粹的链路状态算法，也不是基于纯粹的距离向量算法。它的主要功能是与其它自治域的 BGP 交换网络可达信息。各个自治域可以运行不同的内部网关协议。BGP 更新信息包括网络号 / 自治域路径的成对信息。自治域路径包括到达某个特定网络须经过的自治域串，这些更新信息通过 TCP 传送出去，以保证传输的可靠性。在最新的 BGP4 中，还可以将相似路由合并为一条路由。

6.7. 多路由表、源地址选路

HuaTech-2000 系列防火墙系统采用了一种特殊的路由技术——源地址选路技术。一般的路由技术只根据目标地址来做出路由选择，而 HuaTech-2000 系列产品则根据通讯的源地址和目标地址来做出路由选择。防火墙系统会根据 IP 封包中的源地址判断数据包的路由走向，并在系统中已经建立起的多个路由列表中选择该数据包的路由。这种源地址路由技术可以很好的适应有多个网络出口或者根据用户身份分配带宽资源的网络环境。在这当前越来越复杂网络环境下，如果防火墙不支持源目的地址路由技术就很难实现受控、合理的利用网络资源（尤其是带宽资源），因为到互联网的目标地址都是一样的，只是来源不一样。

6.8. 组播路由

在现在的网络应用中，音频或视频流媒体服务越来越多的应用到组播技术。采用组播技术，单台服务器能够对几十万台主机同时发送连续数据流而无延时。组播发送方只要发送一个信息包而不是很多个，所有目的地同时收到同一信息包，更及时，更同步，可以把信息发送到任意不知名目的地，能减少网络上传输的信息包的总量。网络成本变得相当低廉，从而达到从未有过的传送能力。

传统的防火墙系统在收到网络中的广播或组播数据包时往往不予以转发,使得一部分对组播路由有特殊需求的应用受到限制, HuaTech-2000 系列防火墙支持组播路由技术, 防火墙系统可以判断区分网络中的广播或是组播, 并根据所配置的策略决定组播数据的通过与否, 以满足用户的特殊需求。

6.9. 内容过滤（色情防堵）

HuaTech-2000 系列防火墙支持内容过滤功能和色情防堵功能, 能够实现对应用层内容的检测, 提高网络的安全性, 内容过滤是在 http, ftp 和 smtp 等协议层根据过滤条件对信息流进行控制, 使得 URL、http 携带的 Java Applet, JavaScript, ActiveX, Servlet, CGI, PHP, img; 电子邮件的 subject, to, from 和 text 域; FTP 下载和上载文件的内容等可能包含危险信息, 如病毒, 色情或非法关键字, 非法操作命令等。因此对内容进行过滤能有效地提高网络的安全性。

6.10. 阻止P2P软件

P2P 软件直接将人们联系起来, 让人们通过互联网直接交互。 P2P 软件 使得网络上的沟通变得容易、更直接共享和交互, 真正地消除中间商。 P2P 软件 就是人可以直接连接到其他用户的计算机、交换文件, 而不是像过去那样连接到服务器去浏览与下载。由于 P2P 软件的这些特性导致正常网络带宽被大量 P2P 软件所占用。网络的正常的使用得不到保证。 HuaTech-2000 系列防火墙通过深层过滤技术阻止多种 P2P 协议, 如 eDonkey, eMule, KademiaKaZaA, FastTrack, Gnutella, Direct Connect, BitTorrent, extended BT 等, 使网络环境得以净化, 网络带宽合理分配。

6.11. 用户认证

为了降低内部网在管理和应用上的安全风险, 用户认证功能必不可少, HuaTech-2000 系列防火墙管理程序通过提供给用户专门客户端认证软件, 利用用户名, 用户口令和 IP 地

址等鉴别用户。

HuaTech-2000 型防火墙还支持基于 RADIUS 协议的用户认证，防火墙系统本身实现了 RADIUS 客户端的功能，它将用户的认证和网络访问服务信息发送给中央(第三方)RADIUS 服务器，并将返回的认证信息对用户进行授权，统计。防火墙系统管理员可以借此功能对不同属性的移动用户进行角色划分，从而实现基于用户的访问控制。

6.12. 时间段访问控制

HuaTech-2000 系列防火墙在访问规则中加入时间段访问控制，只有在规则设定的时间段内符合策略的数据报文才可能通过防火墙。此项工作极大地方便了系统管理员的管理，提高了访问控制的灵活性。

6.13. 入侵检测

所谓“入侵”(Intrusion)是个广义的概念，不仅包括发起攻击人(如恶意的黑客)取得超出合法范围的系统控制权，也包括收集漏洞信息，造成拒绝访问(Denial of Service)等对计算机系统造成危害的行为。入侵检测(Intrusion Detection)，顾名思义，便是对入侵行为的发觉。它通过对计算机网络或计算机系统中的若干关键点收集信息并对其进行分析，从中发现网络或系统中是否有违反安全策略的行为和被攻击的迹象。进行入侵检测的软件与硬件的组合便是入侵检测系统(Intrusion Detection System,简称IDS)。

为了尽可能的提高防火墙的运行效率，HuaTech-2000 系列防火墙本身集成了轻量级的入侵检测系统。可以检测部分常见的攻击及非法扫描。为了给用户提供更为全面的入侵检测服务，HuaTech-2000 系列防火墙还提供接口，支持与指定的第三方的IDS服务器联动。

6.14. 病毒扫描

在任何网络环境下，计算机病毒都有着不可估量的威胁性和破坏力，因此计算机病毒的防范是网络安全性建设中重要的一环。HuaTech-2000 系列防火墙提供接口支持与指定的第

三方的病毒扫描服务器联动。

6.15. 应用代理

应用代理（Application Proxy）作用在应用层，其特点是完全“阻隔”了网络通信流，通过对每种应用服务编制专门的代理程序，实现监视和控制应用层通信流的作用。实际中的应用代理功能通常由防火墙设备或专用工作站实现。

HuaTech—2000 系列防火墙的应用代理功能隐藏了内部网络结构，因为内部网的任意主机对外的最终请求都是由防火墙发出的，使外部不可信网络的主机并不知道与内部网络的哪个用户通信，而且还在一定程度上解决了 IP 地址紧缺的问题，因为服务器只需防火墙有一个公网的 IP 地址。

代理的功能是对来自局域网内的用户的会话请求进行会话请求转发。这样做有以下几个用处：

- 因为代理服务器在应用层，它完全阻断了网络报文的传输通道。因此比检测功能具有更高的安全性。
- 可以进行访问控制。
- 隐藏了内部网络结构，因为最终请求是由防火墙发出的，外面的主机并不知道与内部网络的哪个用户通信。
- 解决 IP 地址紧缺的问题。使用代理服务器只需防火墙有一个公网的 IP 地址。

目前 HuaTech—2000 系列防火墙支持的代理有：HTTP 代理、FTP 代理、SMTP 代理。

6.16. 日志审计

HuaTech-2000 系列防火墙系统的日志审计功能十分健全，不但包括了防火墙系统本身运行的日志纪录，而且还包含了运行日志，代理日志，入侵检测日志，流量统计日志，管理日志，双机热备日志，IDS 互动信息，状态信息共八大类日志，并可使用相关的配置程序进行日志浏览及管理。

6.17. 流量控制

流量不足是网络管理者遇到的最麻烦的问题之一，由于一些用户使用 FTP 之类大量消耗网络资源的应用，占用了大部分流量，影响了其他用户正常使用网络。对于专线用户，这个问题尤为严重。

HuaTech-2000 系列防火墙具有基于 IP 的流量控制功能，可以有效的管理网络资源。该功能通过控制每个网络接口的网络流量，防止某些应用占用过大的资源，从而保证关键接口以及重要用户的连接。

6.18. 带宽控制

HuaTech-2000 系列防火墙支持带宽控制，通过合理配置、分配带宽资源，使网络资源得到合理、充分的使用，使得网络中的关键用户在带宽资源紧张时也能够高效率的开展工作。

6.19. VPN功能

VPN 是指虚拟专用网络。实际上是在公众网上建立企业内部网络。在这一问题上，如何保证在公众网上的企业内部信息的安全传输成为关键。对于这一点 HuaTech-2000 系列防火墙是采用安全的加密算法和传输体制来做保证的。这样既减少了建立网络的物理成本，又保证了数据的安全。HuaTech-2000 防火墙 VPN 功能支持 ADSL 移动网关接入 透明接入 windows2000-xp 客户端和华泰 IPSEC 安全客户端等接入等各种接入方式。

6.20. 双机热备功能

HuaTech-2000 系列防火墙支持双机热备功能，从而提高系统的稳定性和可靠性。两台防火墙分为防火墙主机和防火墙从机，在防火墙主机工作的同时，防火墙从机处于实时监控防火墙主机的工作状态，这时所有对内部网络的保护工作由防火墙主机完成。当防火墙主机因不可抗力而工作异常时，防火墙从机能够及时发现问题并立即接替防火墙主机的工作，并

报警通知网络管理员。待防火墙主机故障排除并接入网络后，防火墙主机接管对内网的保护工作，防火墙从机则切换为监视状态，继续侦测防火墙主机的状态。

6.21. 负载均衡功能

HuaTech-2000 系列防火墙的负载均衡技术采用的是通过网络地址转换（Network Address Translation）将一组服务器构成一个高性能的、高可用的虚拟服务器，我们称之为 VS/NAT 技术（Virtual Server via Network Address Translation）。通过网络地址转换，调度器重写请求报文的目标地址，根据预设的调度算法，将请求分派给后端的真实服务器；真实服务器的响应报文通过调度器时，报文的源地址被重写，再返回给客户，完成整个负载调度过程。

6.22. 支持VRRP

VRRP（Virtual Router Redundancy Protocol），虚拟路由器冗余协议。该协议用于解决在静态设置默认路由策略的情况下的单点故障问题。VRRP 使用选举协议来动态的从 LAN 中的 VRRP 路由器中选举出一个作为虚拟路由器。在众多 VRRP 路由器中处理分配给虚拟路由器的地址的 VRRP 路由器叫做主路由器（Master），承担转发 IP 数据包的工作。选举虚拟路由器的过程规定了主路由器的失效条件。在主路由器失效的情况下，其他候选 VRRP 路由器可以动态协商选举出主路由器。这样虚拟路由器的 IP 地址就可以作为终端的默认下一跳路由器了。使用 VRRP 的好处是无需在每一个终端上配置动态路由或者路由发现协议，就可以得到高可靠性的默认路径。VRRP 提供的功能类似于 Cisco System, Inc. 私有协议—HSRP（Hot Standby Router Protocol）以及 Digital Equipment Corporation, Inc. 的私有协议—IP Standby Protocol。

6.23. 较强的抗攻击能力

作为一种网络安全防护设备，防火墙在网络中自然成为众多攻击者的首要目标，所以抗攻击能力也是防火墙的必备功能。HuaTech-2000 系列防火墙系统采取多种安全措施，可以

防范 Internet 环境中针对防火墙的攻击，如：抗 IP 假冒攻击，抗口令字探寻攻击，抗网络安全分析等。

6.24. 采用内核性能优化和安全加固技术

防火墙性能的优劣直接影响到它能够被广大客户所接受。对一些用户对响应时间非常敏感的服务必须做好充分的优化工作，否则用户会对防火墙的性能产生疑问。我们借鉴了许多国外的相关资料，针对防火墙中的服务模块，采用多种内核性能优化技术，大大提高了防火墙的工作效率以及系统本身的健壮性。

7. HuaTech-2000 型防火墙的典型应用

HuaTech-2000 系列防火墙可根据用户的具体要求，灵活配置各项功能，以满足不同用户的不同需求。下面描述了部分常见的应用情况：

- 应用在内部网与外部网（Internet）连接的唯一出入口，防止外部对内部网的非法访问。
- 对内部网的不安全区域或重点保护区域实施访问控制
- 保护公开服务器，如 Web 服务器、FTP 服务器、POP3 服务器等等。

8. HuaTech-2000 型防火墙功能、技术指标 一览

（百兆功能性能参数以 HT-FW-2000-TX 为标准）

通用指标体系		指标说明	
产品名称		HuaTech-2000 型防火墙	
防火墙类型		包过滤+状态检测+代理	
工作方式		兼容路由、网桥两种工作方式	
产品规格说明	HT-FW-2000-TX	适用模式 高端	
设备规格			
内部配置	操作系统	系统采用经过安全加固的专用操作系统	
	CPU	Intel Celeron M 420	
	内存	512M	
	硬盘	128M CF 卡	
电气性能	电源	220V/50Hz 3.0A（最大） 260W（最大）	
	环境规范	运行温度：0 — 45 摄氏度 非运行温度：-20 — 65 摄氏度 相对湿度：10—90%@4 摄氏度，非冷凝	
	参考的安全规范及标准	UL 1950、EN 41003、AS/NZS 3260、AS/NZS 3548 Class A、CSA Class A FCC Class A、EN 60555-2、VCCI (ClassII)	
	抗干扰性	IEC — 1000 — 4 — 2（ESD） IEC — 1000 — 4 — 3（辐射敏感性） IEC — 1000 — 4 — 4（电快速瞬变） IEC — 1000 — 4 — 5（电涌） IEC — 1000 — 4 — 3（谐波）	
系统组成	防火墙系统		是一个高速稳定的硬件平台和经过安全加固的操作系统的完美结合体
	配置管理系统	GUI 管理器	支持
		Web 管理器	支持
		CLI 管理器	支持
日志管理器	支持		
网络特性	支持网络适配器类型		10/100 以太网控制器 RJ45 接口
	支持最大接口数		4 个，可扩充至
	DNS 支持		支持
	VLAN 支持		支持 802.1Q 协议
	支持的非 IP 协议		IPX、NETBEUI
	支持 VoIP		H.323、SIP
性能指标	最大并发连接数		1, 200, 000
	网络吞吐率		≥98Mbps
	MTBF		≥80, 000 小时

集中管理	统一策略集中管理	支持
	提供基于时间的访问控制	支持
	SNMP	支持
	本地管理	GUI、WEB、CLI (Console)
	远程管理	GUI、WEB、CLI (SSH)
	集中管理中心支持环境	Microsoft Windows98/NT/2000/XP
访问控制	状态检测	支持
	用户权限级别设定	支持，可自定义权限
	支持的代理类型	支持正反向代理技术，支持 FTP、HTTP、SMTP 等多种协议
	支持双向网络地址转换	支持
	支持基于时间段的策略	支持
	双向 NAT、PAT	支持
	支持用户认证	支持 OTP、RADIUS 等
	MAC 地址绑定功能	支持
	带宽管理	支持
	流量控制功能	支持
	状态检测功能	支持
	深层过滤	支持
	抗 P2P	支持
VPN 支持	支持的 VPN 加密算法	3DES, DES, twofish, blowfla 等国家指定算法
	可以在 VPN 中使用的协议	TCP/IP
	建立 VPN 通道的协议	IPSec、IKE
	IPSEC 认证	手工密钥，基于 X.509 的 CA 证书，支持第三方证书导入
	L2TP, L2TP OVER IPSEC	支持 WIN2000/XP 虚拟专网接入
	客户端	Windows2000/XP 华泰 ipsec 安全客户端
	支持 SSL VPN	支持网关到网关
认证支持	支持的认证类型	OTP, RADIUS
	支持数字证书	X.509
分布日志	处理完整日志方法	专用日志管理系统
	日志报表生成方式	专用日志管理系统
	警告通知机制	支持
	提供审计报表	支持
	提供实时统计	日志、GUI、Web
	日志种类	8 种（防火墙的运行日志，代理日志，入侵检测日志，流量统计日志，管理日志，双机热备日志，IDS 互动信息，状态信息）
	日志备份	支持
	日志转发	支持
	日志删除	支持
	防御功能	防范攻击功能
与 IDS 服务器互动		支持
支持病毒扫描		支持
提供内容过滤		支持 URL、文件、邮件过滤

	能够防御的 DoS 攻击类型	PingofDeath, TCPSYNfloods 等 150 种
	防 IP 地址欺骗	支持
	阻止 ActiveX、Java、cookies、Javascript 侵入	支持
高可用性 (HA)	动态路由	支持
	VRRP	支持
	双机热备功能	支持
	负载均衡	支持
	失败恢复特性 (failover)	支持
	电源 (双/单)	支持双电源冗余模式
安全特性	提供入侵实时警告	支持
	提供实时入侵防范	支持
获得的许可证类别及号码	公安部销售许可证	证书编号: XKC33379
	国家信息安全测评认证中心认证证书	注册号: CNISTEC2005TYP380
	国家保密局科技成果鉴定	编号 (2002) 鉴字 04 号
	解放军信息安全测评认证中心认证证书	军密认字第 0062 号
	其它	软件著作权证书 0013262 号

(千兆功能性能参数以 HT-FW-2000-GX 为标准)

通用指标体系		指标说明
产品名称		中软 HuaTech-2000 型防火墙
产品型号		HT-FW-2000-GX
防火墙类型		包过滤+状态检测+代理
工作方式		支持透明模式、路由模式、混杂模式两种工作方式
型号规范	HT-FW-2000-GX	无用户限制
设备规格		2U
内部配置	操作系统	系统采用经过安全加固的专用操作系统
	CPU	Intel E 5120 双核
	内存	2G
	硬盘	128M CF 卡
电气性能	电源	220V/50Hz 3.0A (最大) 400W (最大)
	环境规范	运行温度: 0 — 45 摄氏度 非运行温度: -20 — 65 摄氏度 相对湿度: 10—90%@4 摄氏度, 非冷凝
	参考的安全规范及标准	UL 1950、EN 41003、AS/NZS 3260、AS/NZS 3548 Class A、CSA Class A FCC Class A、EN 60555-2、VCCI (ClassII) MTBF (平均故障间隔时间) ≥300,000 小时
	抗干扰性	IEC — 1000 — 4 — 2 (ESD) IEC — 1000 — 4 — 3 (辐射敏感性) IEC — 1000 — 4 — 4 (电快速瞬变) IEC — 1000 — 4 — 5 (电涌) IEC — 1000 — 4 — 3 (谐波)
系统组成	防火墙系统	是一个高速稳定的硬件平台和经过安全加固的操作系统的完美结合体

	配置管理系统	GUI 管理器	支持
		Web 管理器	支持
		CLI 管理器	支持
		日志管理器	支持
网络特性	支持网络适配器类型		10/100 以太网控制器 RJ45 千兆以太网控制器 1000Base-TX
	支持最大接口数		8 个接口, 其中 4 个光纤端口, 4 个 1000Base-TX 连接
	DNS 支持		支持
	支持网桥透明接入		网桥支持生成树计算协议 (包括 PVST 和 CST)
	VLAN 支持		支持 802.1Q 协议
	支持的非 IP 协议		IPX、NETBEUI
	支持 VoIP		基于 H.323
	最大并发连接数		2, 500, 000
	每秒最大会话数		25, 000
管理功能	通过统一策略集中管理多个防火墙		支持
	提供基于时间的访问控制		支持
	支持 SNMP 监视和配置		支持 SNMP 协议 V2、V3 版本
	本地管理		基于 SSL 连接的 GUI、WEB、CLI
	远程管理		GUI、WEB SSH
访问控制	用户权限级别设定		支持, 可自定义权限
	支持的代理类型		支持正反向代理技术, 支持 FTP、HTTP、SMTP 等多种协议
	支持双向网络地址转换		支持
	支持基于时间段的策略		支持
	支持用户认证		支持 OTP、RADIUS 等
	支持流量控制功能		支持
	支持带宽控制功能		支持
	MAC 地址绑定功能		支持
	状态检测功能		支持
	深层过滤		支持
抗 P2P		支持	
VPN 支持	支持的 VPN 加密算法		3DES, AES 等国家指定算法
	可以在 VPN 中使用的协议		TCP/IP
	建立 VPN 通道的协议		IPSec
	IPSEC 认证		手工密钥, 基于 X.509 的 CA 证书, 支持第三方证书导入
	L2TP, L2TP OVER IPSEC		支持 WIN2000/XP 虚拟专网接入
	客户端		Windows2000/XP
	支持 SSL VPN		支持网关到网关
日志	处理完整日志方法		HuaTech-2000 日志管理软件
	日志报表生成方式		HuaTech-2000 日志管理软件
	警告通知机制		支持
	提供审计报表		支持
	提供实时统计		支持

	日志种类	8 种（防火墙的运行日志，代理日志，入侵检测日志，流量统计日志，管理日志，双机热备日志，IDS 互动信息，状态信息）
	日志备份	支持
	日志转发	支持
	日志删除	支持
防御功能	防范攻击功能	常见 32 大类攻击行为（DoS,DDoS,系统溢出）
	与 IDS 服务器互动	支持
	支持病毒扫描	支持
	提供内容过滤	支持 URL、文件、邮件过滤
	能够防御的 DoS 攻击类型	PingofDeath, TCPSYNfloods 等 150 种
	防 IP 地址欺骗	支持
其它功能	阻止 ActiveX、Java、cookies、Javascript 侵入	支持
	支持带宽管理	支持多级带宽管理
	失败恢复特性（failover）	支持
	流量管理功能	支持
	支持负载均衡	支持
	VRRP(虚拟路由冗余协议)	支持
	支持路由策略	支持
	支持动态路由功能	支持
安全特性	支持组播路由	支持
	电源（双/单）	支持双电源冗余模式
	双机热备功能	支持
	提供入侵实时警告	支持
获得的许可证类别及号码	提供实时入侵防范	支持
	公安部销售许可证	证书编号：XKC33379
	国家信息安全测评认证中心认证证书	注册号：CNISTEC2005TYP380
	解放军信息安全测评认证中心认证证书	军密认字第 0062 号
	国家保密局科技成果鉴定	编号（2002）鉴字 04 号
	其它	软件著作权证书 0013262 号

（本功能列表截止到 2007 年 10 月为止，如果您需要了解最新增加功能请访问北京中软华泰信息技术有限责任公司网站：www.huatechsec.com.cn）