

# 中软 HuaTech-2000 型防火墙

## 成功案例

北京中软华泰信息技术有限责任公司

2002.6

# 目 录

1. 前言 .....	3
2. X省中国银行应用.....	3
3. 邯郸市信息中心.....	5
4. 河北省经贸委应用 .....	7
5. 河北省物价局.....	9
6. 北京市政管理委员会 .....	10

# 1. 前言

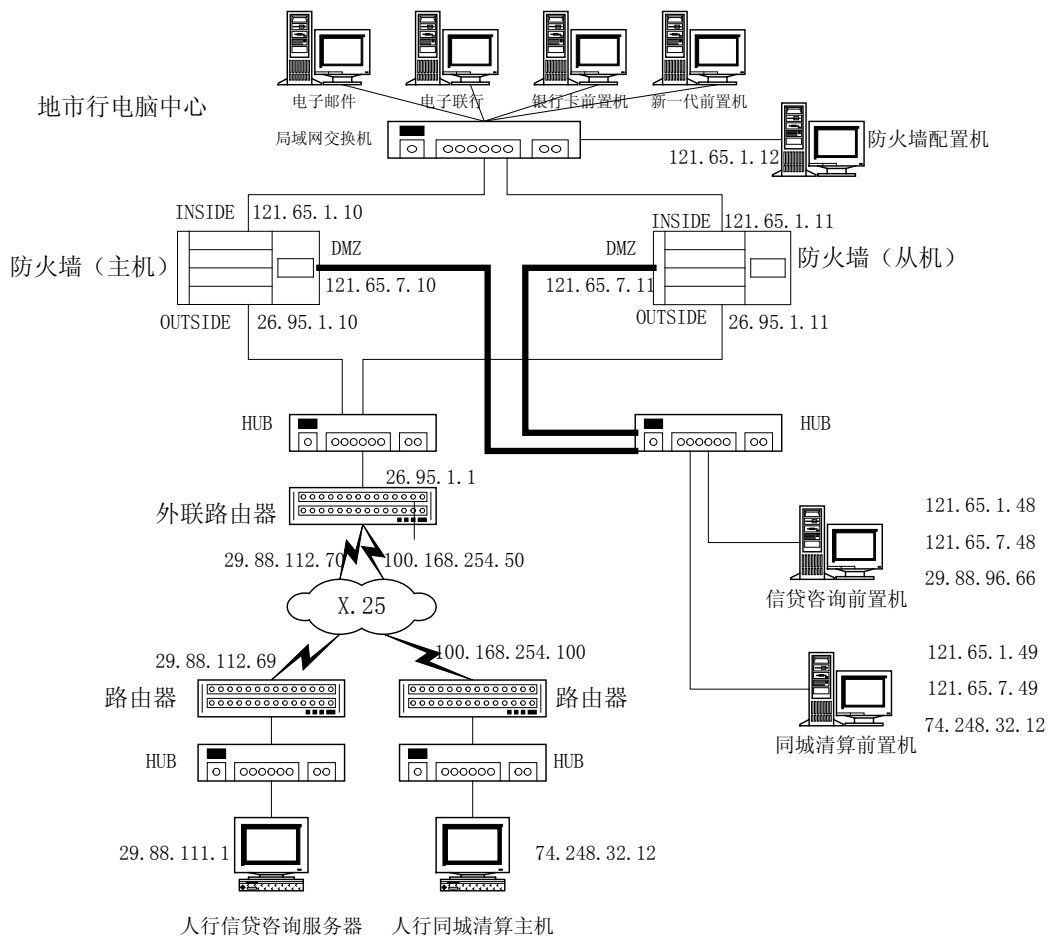
中软 HuaTech-2000 型高性能防火墙从出品至今，已经在许多行业得到广泛的应用。从目前反馈回来的信息看，产品性能良好，使用正常。产品面世一年多以来，使我们感到欣慰的是没有一台机器出现过故障，这是用户所希望的，也正是我们所追求的。我们的产品经得起时间的考验，也赢得了用户的信任。

## 2. X 省中国银行应用

硬件型号：中软 HuaTech-2000 增强型  
软件版本：V2.1

网络结构图如下：

XX分行地市行防火墙拓扑图



**用户要求:**

1、XX 市中行内部网机器可以主动访问信贷咨询前置机、同城清算前置机及其他前置机（主要是 HTTP, TELNET, FTP, 也即通过前置机访问人行服务器）。

2、X 省行某些 IP 机器可以访问 XX 市中行前置机。

3、中行前置机可以相对应地主动访问人行信贷咨询服务器、人行同城清算服务器及人行其他服务器（目前有些业务未开展，或即将开展）。

4、中行前置机可以主动访问中行内部网机器（限定访问内部的某些 IP 和 PORT），也可以访问中行省行和总行机器。

5、XX 市中行内部网机器可以通过防火墙使用 TELNET 访问控制外联路由器。

6、人行服务器主动访问中行前置机。向中行前置机发送业务回执，由前置机转发给中行内部网机器（各分理处业务机器）。

**启用服务及配置的规则:**

防火墙启用的服务主要有:

- 1、防火墙划分出 DMZ 区。将中行三台前置机联在 DMZ 区，如中行业务扩展，DMZ 区可以加入更多的前置机。
- 2、防火墙启用双机热备服务。因中行与人行外联业务重要且繁忙，不允许中断，因此防火墙设置双机保障中行与人行的外联通畅。
- 3、 防火墙加入对中行省行的静态路由。使设置在 DMZ 区的前置机对省中行某些 IP 的访问可以通过防火墙路由到省中行机器。
- 4、 防火墙加入缺省路由。使中行前置机对外联机器的所有访问通过防火墙外口路由出去。
- 5、 防火墙进行地址映射。使中行前置机通过防火墙访问人行服务器的数据包 IP 地址映射为行人行要求的 IP 地址。
- 6、 防火墙进行地址映射。使人行发往中行前置机的业务回执报文数据包 IP 地址映射为中行前置机的实际 IP 地址。
- 7、 防火墙加入包过滤规则。使符合业务流程的数据报文通过防火墙，并记录日志；其余数据包则给予拒绝并记录日志。

明细规则配置 略。。。

### 3. 邯郸市信息中心

邯郸市信息中心网络是大型的网络系统，此网络连接各市直机关、县、区各局、处等的局域网，由市信息中心作总出口接 Internet，信息中心服务器对外提供服务。

在建网初期由于资金等问题，没有考虑到安全防范措施。后由于安全性问题越来越受到重视，决定采用防火墙。由于网络规模较大，联网主机较多，防火墙接在主干网上，因此防火墙必须能高效、稳定、安全。经过综合考虑，市信息中心决定采用中软 HuaTech-2000 型高性能防火墙。

#### 目的要求

- ◆ 满足信息中心网络的正常运转
- ◆ 内部用户进入 Internet 的通讯要经过防火墙
- ◆ 内部用户访问中心的服务器需经过防火墙

- ◆ 从 Internet 外部访问中心的服务器要经过防火墙，外部用户不能访问内部主机

- ◆ 能实时统计内部用户的数据流量

### 防火墙安装

- ◆ 初始化防火墙的 IP 地址、路由等参数

- ◆ 防火墙的外网端口接路由器

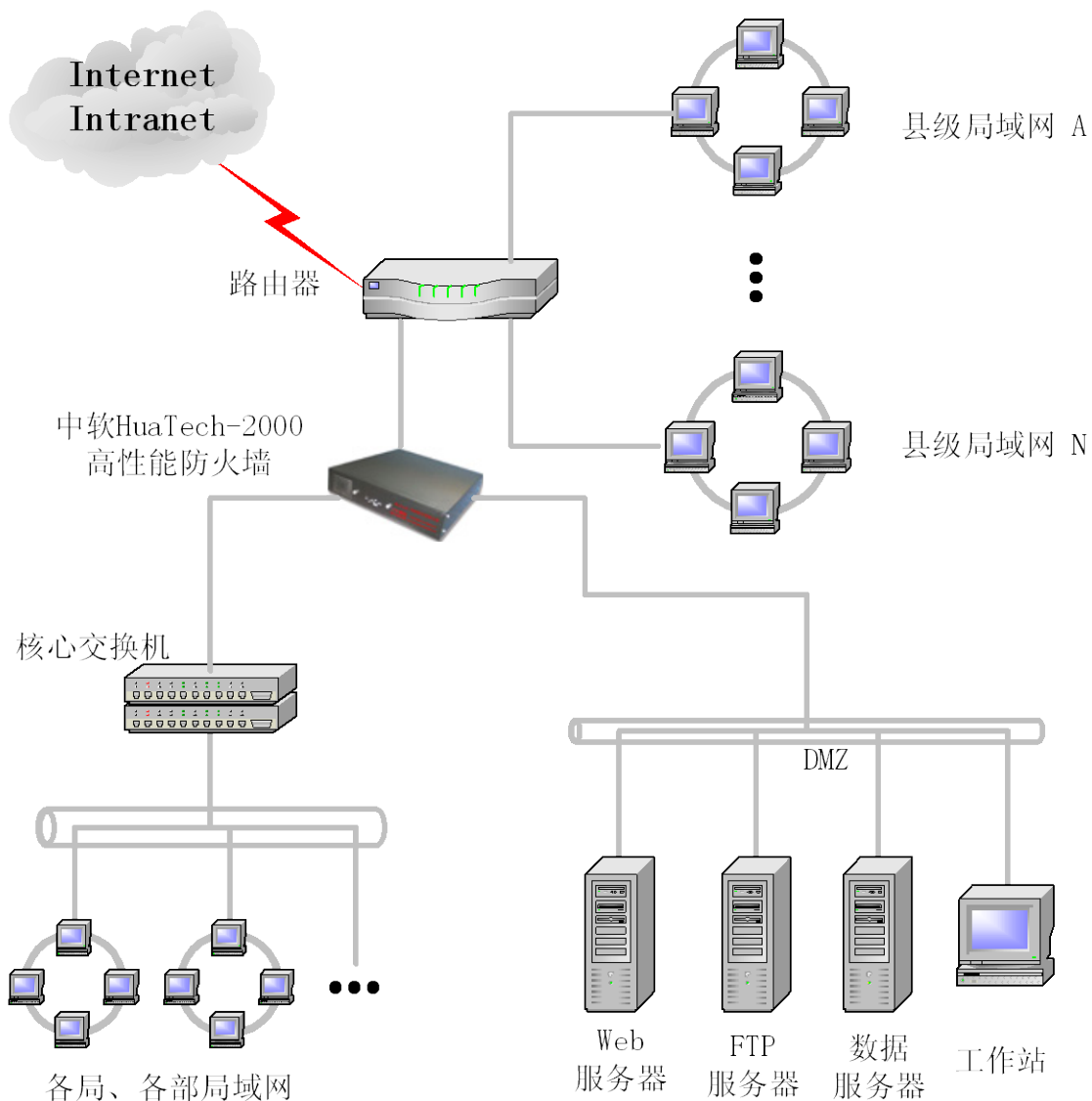
- ◆ 防火墙的内网端口接交换机

- ◆ 防火墙的 DMZ 网端口接与服务器连接的交换机

### 网络拓扑结构

我们选用中软 HuaTech-2000 型高性能防火墙，并把它接在路由器 NBII 之后，核心交换机之前，并把向外提供服务的服务器接入防火墙的 DMZ 网中。

连接如下图所示：



邯郸市信息中心网络示意图

## 4. 河北省经贸委应用

河北省政务网是一个政府办公网，它在物理上与互连网是完全隔离的。它的规模是相当大的。省信息中心是整个网的中心，连接各市直机关、局、委等部门的局域网。河北省经贸委是其中的一个分中心，配置有多台重要的服务器，包括 Web 服务器、域名服务器、数据服务器、邮件服务器、拨号服务器等，这些服务器向所有连网用户开放。需要防火墙来确保经贸委网络的安全。

## 目的与要求

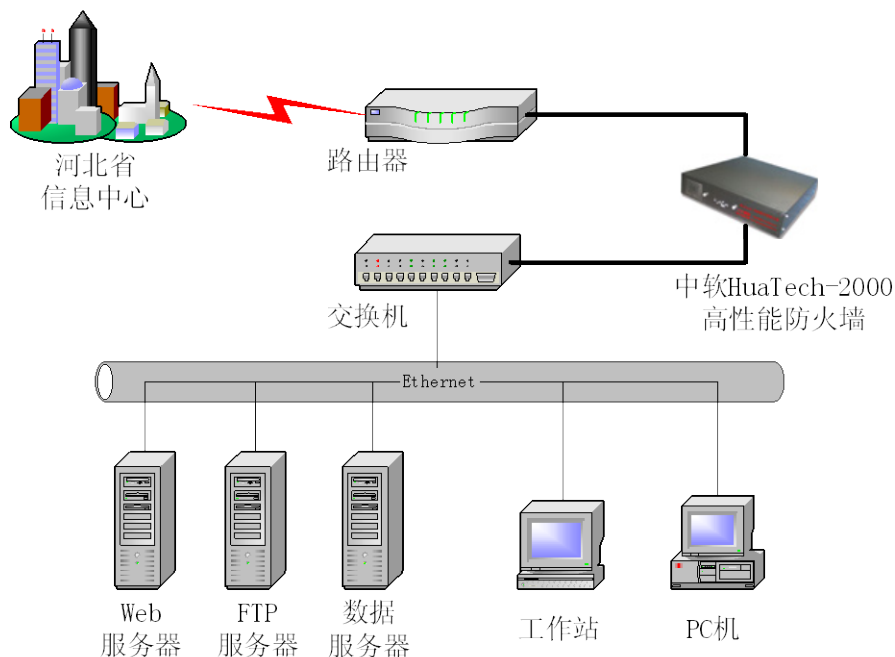
- ◆ 所有访问服务器的信息通讯都通过防火墙。
- ◆ 保证现有运行环境完整，不影响正常工作。
- ◆ 能够过滤指定的通讯协议。
- ◆ 外部用户不能访问除指定的服务器之外的主机。

## 防火墙安装

- ◆ 初始化防火墙的 IP 地址、指向路由器等参数
- ◆ 防火墙的外网端口接路由器
- ◆ 防火墙的内网端口接交换机
- ◆ 系统配置采用 GUI 图形管理器设置，简单易懂，用户自行配置

## 网络拓扑结构

根据用户的需求，我们选用中软 HuaTech-2000 型高性能防火墙，并把防火墙置于路由器和连接局域网的交换机之间，结构如下图所示：



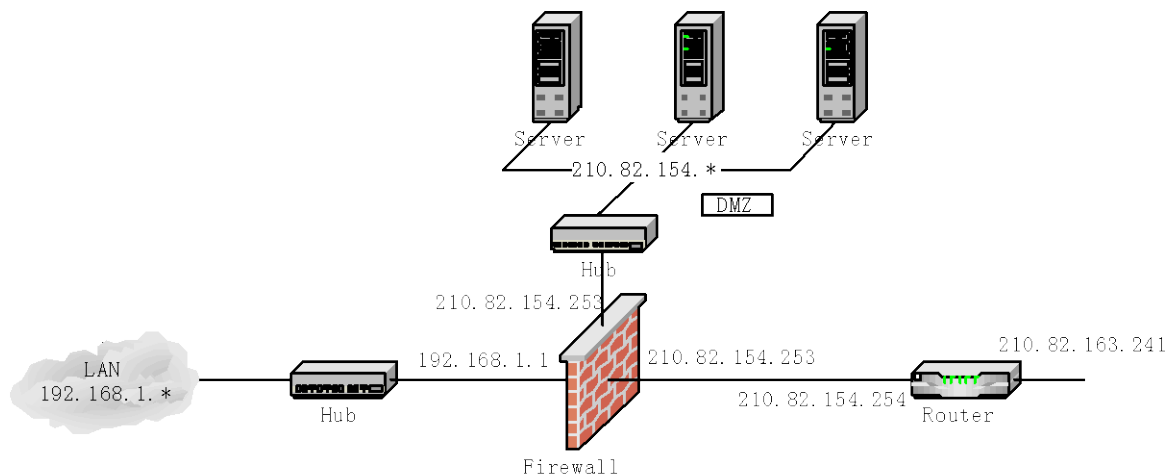
河北省经贸委网络结构示意图

在系统安装过程中进展非常顺利。防火墙经初始化之后，立即接入到网络中，网络断开时间很短，基本上对用户的使用没有造成影响。用户通过使用我们的 GUI 图形管理器，很快就学会了对防火墙进行配置、管理等工作。系统安装成功，安全性能充分满足了用户的需求，效果非常好，至今已正常运转多时，得到用户的好评。

## 5. 河北省物价局

硬件型号：中软 HuaTech-2000 增强型  
软件版本：V2.1

网络结构图



**客户要求：**

内网通过地址转换转换成合法的 IP 只允许 64 个地址（IP 192.168.1.0 掩码 255.255.255.192），192.168.1.45 以后绑定不存在的 DMZ 区用反线连一台服务器，另一台服务器放在内网通过地址映射允许外界访问。

**启用服务及配置的规则：**

透明方式

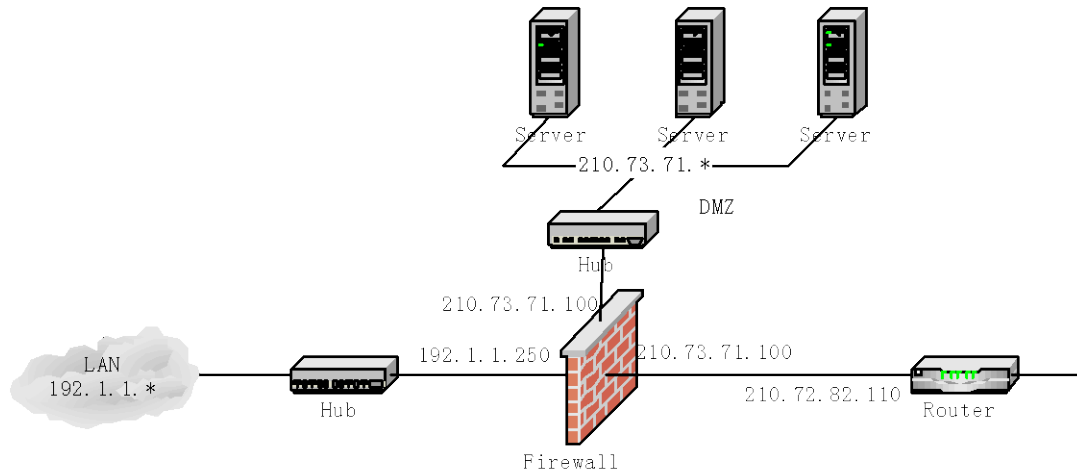
地址转换(192.168.1.0/255.255.255.192，全部协议)

DMZ、地址绑定

## 6. 北京市政管理委员会

硬件型号：中软 HuaTech-2000 增强型  
软件版本：V2.1

网络结构图



客户要求：

内网通过地址转换转换成合法的 IP，DMZ 区放置外网服务器。

启用服务及配置的规则：

透明方式

地址转换(全部协议)

DMZ