HT-2000 VPN 服务器配置指南

北京合力万通科技有限公司

2011-01-12

目录

一．VPN 服务概述

VPN 属于远程访问技术，简单地说就是利用公网链路架设私有网络。例如公司员工出差到外地，他想访问企业内网的服务器资源，这种访问就属于远程访问。怎么才能让外地员工访问到内网资源呢?VPN 的解决方法是在内网中架设一台 VPN 服务器，VPN 服务器有两块网卡，一块连接内网，一块连接公网。外地员工在当地连上互联网后，通过互联网找到 VPN 服务器，然后利用 VPN 服务器作为跳板进入企业内网。为了保证数据安全，VPN 服务器和客户机之间的通讯数据都进行了加密处理。有了数据加密，就可以认为数据是在一条专用的数据链路上进行安全传输，就如同专门架设了一个专用网络一样。但实际上 VPN 使用的是互联网上的公用链路，因此只能称为虚拟专用网。即：VPN 实质上就是利用加密技术在公网上封装出一个数据通讯隧道。有了 VPN 技术，用户无论是在外地出差还是在家中办公，只要能上互联网就能利用 VPN 非常方便地访问内网资源，这就是为什么 VPN 在企业中应用得如此广泛。

二．进行 VPN 认证的特点

（1）安全保障

VPN 通过建立一个隧道，利用加密技术对传输数据进行加密，以保证数据的私有和安全性。

（2）服务质量保证（QoS）

VPN 可以不同要求提供不同等级的服务质量保证。

（3）可扩充性和灵活性

VPN 支持通过 ***Interne***t 和 ***Extrane***t 的任何类型的数据流。

（4）可管理性

VPN 可以从用户和运营商角度方便进行管理。

三．HT2000 VPN 服务器基本功能

VPN 使用的标准：

- 2 层隧道协议(L2TP)。
- 点到点隧道协议(PPTP)。
- IP 安全性(IPsec)。

四．HT-2000 VPN 服务器功能特点

主要体现在数据的加密方面：

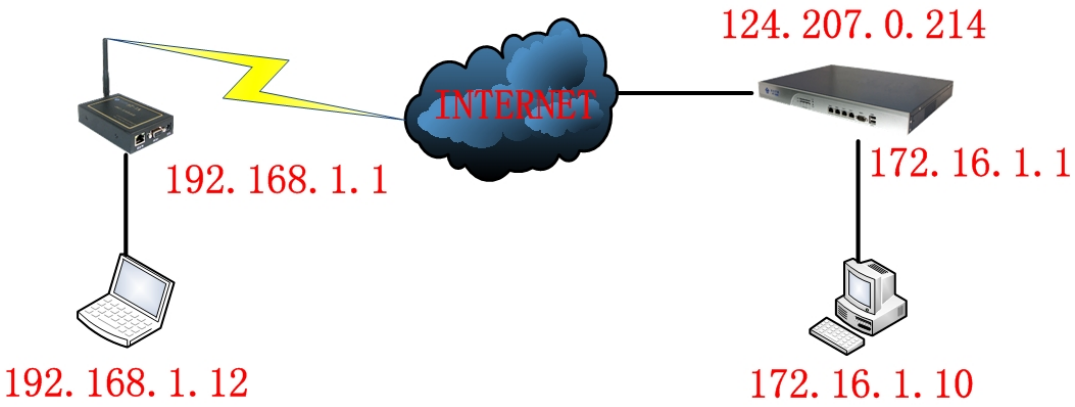
- 机密性—这表示发送到Ｉｎｔｅｒｎｅｔ上的信息可以用一种可靠的方法来保密。
- 验证—这表示当数据由目的地的实体接收时，存在一个方法检验数据是否来自正确的实体并且是否在传输过程中被篡改。

为了实现这些概念，ＩＰｓｅｃ使用两组协议，称为传输安全协议：

- 验证报头（ＡＨ）。
- 封装安全有效负载（ＥＳＰ）。

五．HT-2000 VPN 服务器应用方案及网络拓扑说明

拓扑图：



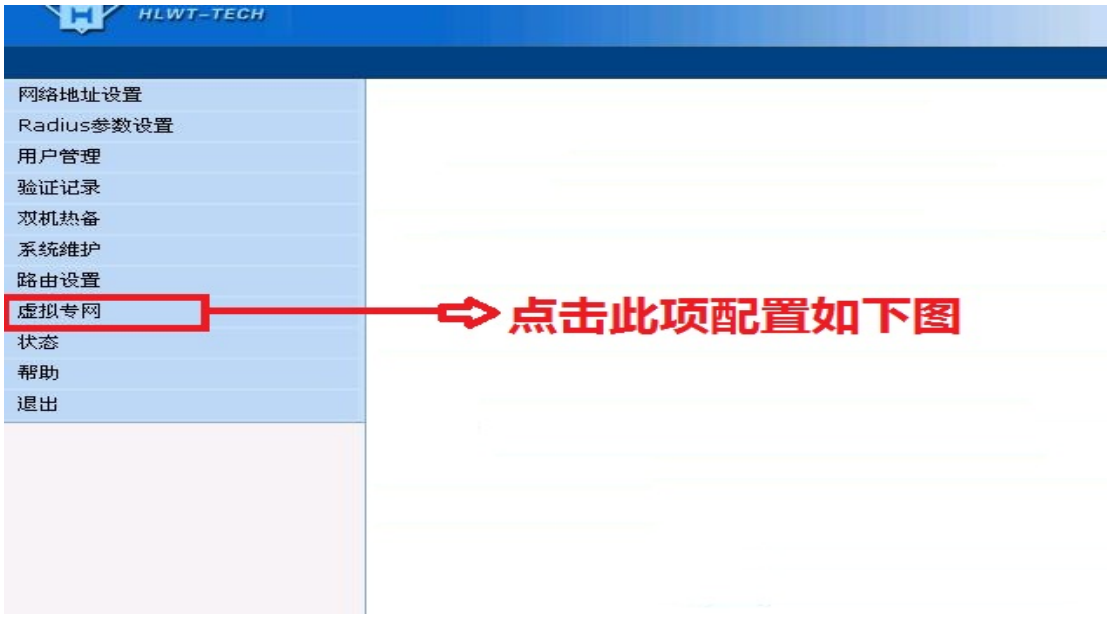
左边：本公司产品 HT-3GW 与下挂终端（外部设备）

中间 internet 网云：互联网

右边：本公司产品 HT-2000（即中心、总部）

通过建立 IPsec VPN，使下挂终端（192.168.1.12）与中心内网机器（172.16.1.10）进行加密通讯。

配置 VPN：



PHASE 1

哈希算法:	md5
加密算法:	des
协商群:	group 2
生存周期:	3600 秒
本地标识类型:	IP Address
本地标识:	124.207.0.214
对端标识类型:	USER_FQDN
对端标识:	test@123.com
预共享密钥:	●●●●●

PHASE 2

加密算法:	des
哈希算法:	hmac_md5
完全向前保密:	关闭
生存周期:	7200 秒

提交

PHASE 1

哈希算法: md5
加密算法: des
协商群: group 2
生存周期: 3600 秒
启动模式: 主动
本地标识类型: USER_FQDN
本地标识: test@123.com
对端标识类型: IP Address
对端标识: 124.207.0.214
预共享密钥: •••••

PHASE 2

加密算法: des
哈希算法: hmac_md5
完全向前保密: 关闭
生存周期: 7200 秒

提交

IPSec VPN 开启

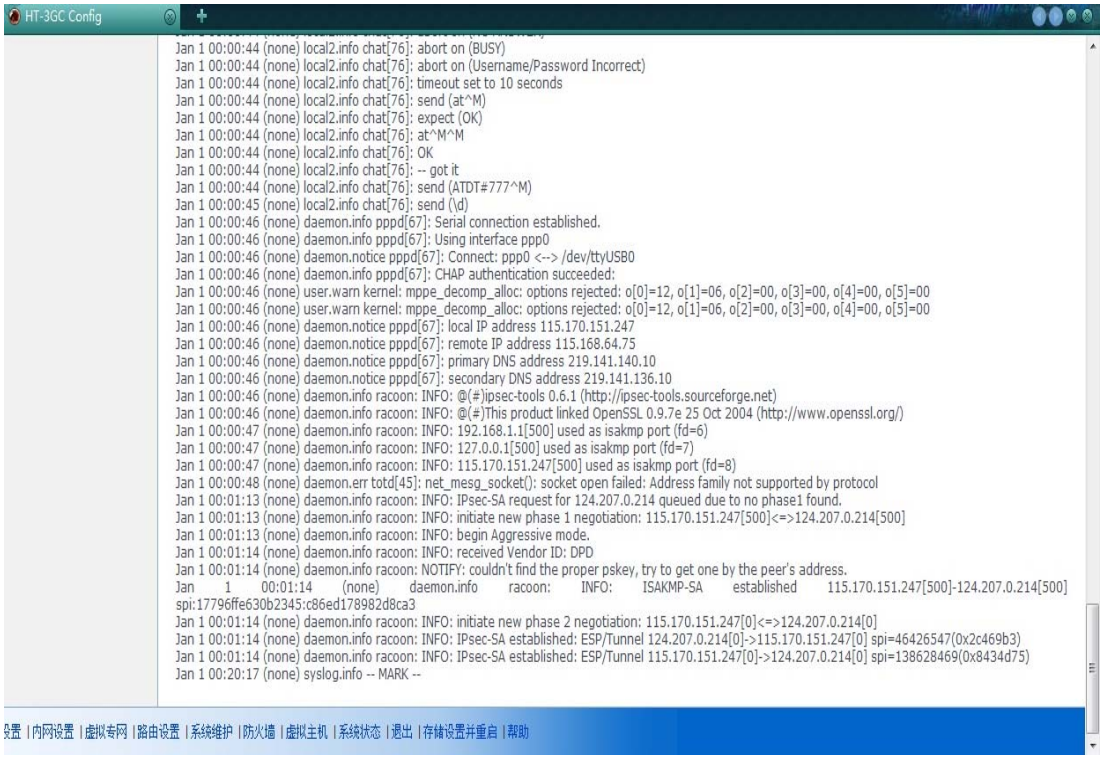
IPSec服务器地址: 124.207.0.214
选择IPSec协议: ESP
交换模式: 野蛮模式
选择IPSec模式: Tunnel

对端网络地址: 172.16.1.10
对端网络掩码: 255.255.255.0
对端网络地址2:
对端网络掩码2:
⋮
对端网络掩码8:
本地网络地址: 192.168.1.12
本地网络掩码: 255.255.255.0

VPN自动建立: 开启

目标IP地址: 172.16.1.10

HT-3GW 产品连接成功日志图：



下挂终端（192.168.1.12） Ping 中心内网机（172.16.1.10）：

六．HT-2000 硬件参数

处理器：Intel
电 源：220V/2.0A
RJ45 网口 ： 4 个
USB 接口： 2 个
RS232 接口： 1 个
尺 寸： 4.5 X 31 X 43 CM

七．配置说明

1.访问与登陆
如图 1，打开网页浏览器，将电脑与HT2000 内网口相连,输入地址http://192.168.1.1/访问HT-2000，页面将会出现登录界面，如图 4-1：
当前用户名为:admin 口令:admin

图 4-1.登录界面

2.主界面
登录成功后，将出现主界面，如图 4-2，主要包括“网络地址设置”、“Radius参数设置”、“用户管理”、“系统维护”、“状态”、“退出”、“帮助”等页面入口。

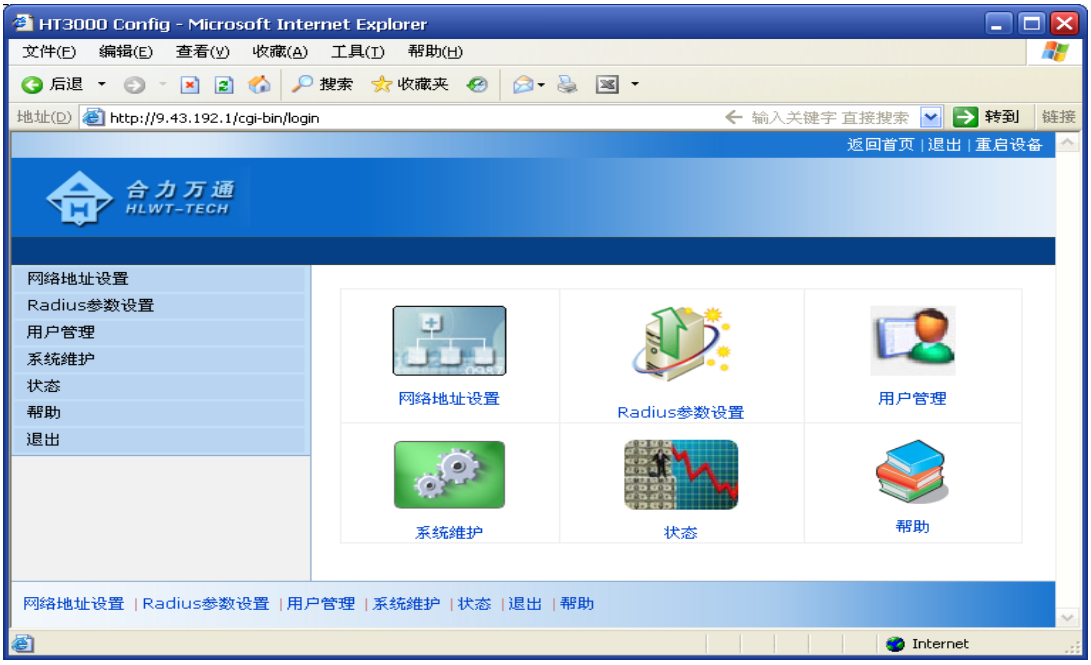


图 4-2 主界面

3. 网络地址设置

“网络地址设置”用于配置HT-2000 的各以太网端口的IP地址，网络掩码，网关等信息。如图 4-3：

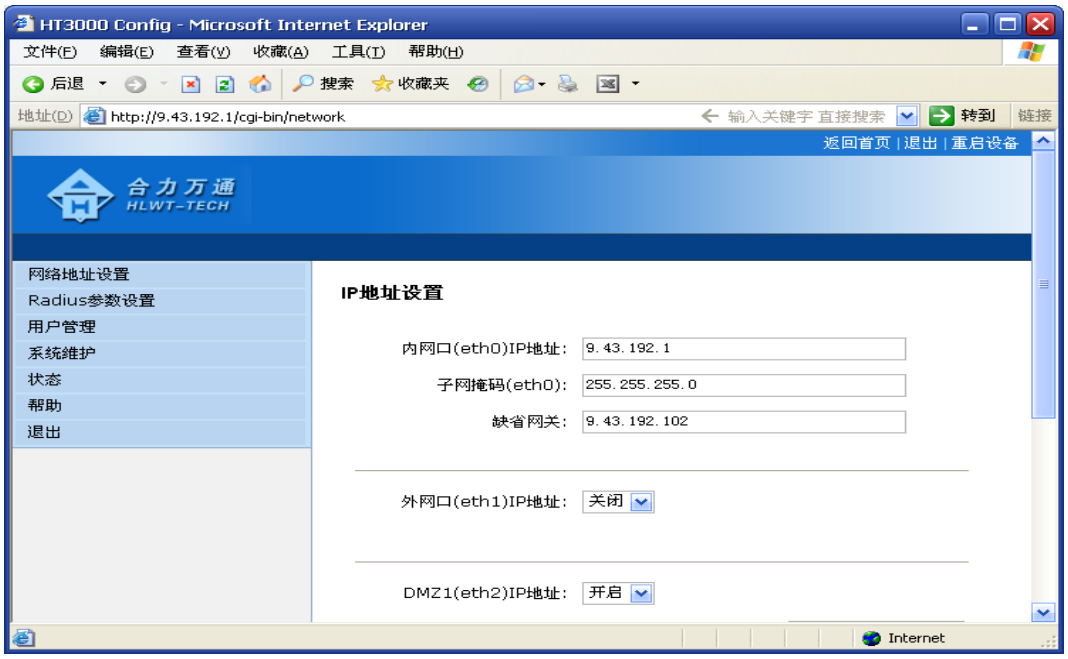


图 4-3 网络地址设置

4. 系统维护

“系统维护”用来备份和还原网络地址设置/Radius 参数设置和用户列表的配置信息。如图 4-4：

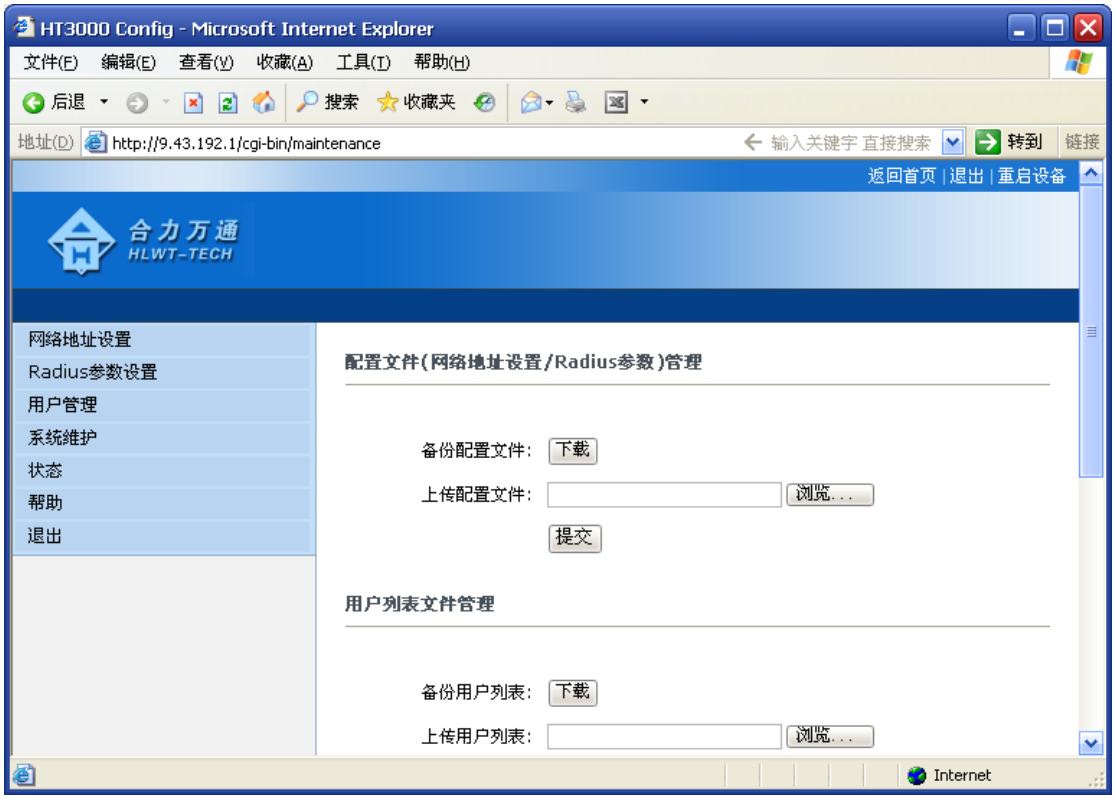


图 4-4 系统维护

5. 状态

“状态”用来主机网络状态、进程信息、和系统日志等信息。如图 4-7：

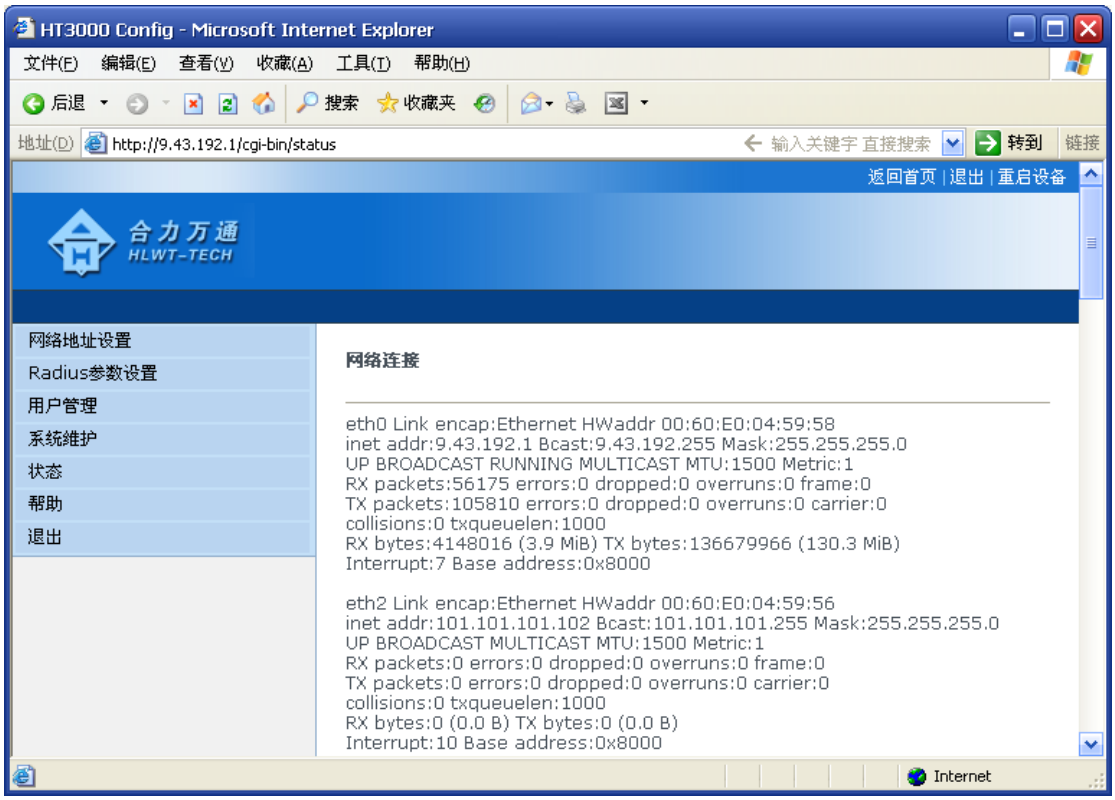


图 4-5 状态

6. 帮助

“帮助”用来显示主机默认参数等帮助信息。如图 4-8：

图 4-8

7. 退出

“退出”用来安全退出登录状态，退出后再次访问 HT-2000 时将要求管理员输入用户名、口令登录。（默认情况下，客户登录 HT-2000 设备后，如果 20 分钟内没有再次访问，将自动退出登录状态）

八．HT-2000 出厂参数及口令恢复方法

默认情况下 HT-2000 DMZ2 端口 IP 地址固定配置为 192.168.1.1 掩码 255.255.255.0，当用户忘记了其它端口的 IP 地址设置时，可使用此端口登录 HT3000 管理界面。

如果用户忘记了用户名、口令设置，则可以通过 DMZ2 端口访问 HT-2000，只需将 PC 机配置为 192.168.1.2 即可无需用户名、口令直接访问 HT-2000。

结束