

海蜘蛛路由代理服务器为例介绍代理服务器的配置。

1) 代理服务器软件安装。

按照安装手册进行安装海蜘蛛路由代理服务器。

2) 代理服务器的配置

(1) WEB 远程登录服务器进行管理。访问系统的 WEB 管理 URL 地址为：<http://<IP地址>:端口号 880>，输入用户 admin 和密码 admin，确定后登陆。

系统设置

网络设置

DNS 参数

动态域名解析

静态路由

多线负载均衡策略

透明网桥

网络接口配置

局域网 (LAN)

广域网 (WAN)

IP 隧道客户端

PPTP VPN 客户端

L2TP VPN 客户端

SSL VPN 客户端

防火墙

上网管理

服务应用

局域网接口

设置与本地(内部)网络相连的网卡的信息, 比如 IP 地址、子网掩码等; 您还可以在这个网卡上绑定多个 IP, 来扩充或隔离您的局域网。

LAN-1

LAN-2

LAN 间互访

网卡位置: 00:0b:0 | eth2 | Realtek Semiconductor RTL-8169 Gigabit Ethernet (rev 10) | LAN1* 绑定

流量统计:
共发送 0.0 byte, 发送包 0, 出错 0, 丢弃 0
共接收 0.0 byte, 接收包 0, 出错 0, 丢弃 0

物理连接状态: 网线被拔出或网卡未启动

参数设置...

MAC地址:

00-14-78-55-4b-ef

MAC地址克隆:

IP地址:

10.0.1.1

子网掩码:

255.255.255.0 (默认)

【此网段可容纳 254 台机器】

图 6-27 局域网接口设置界面

登陆上去后，就和硬路由一样进行设置。

如图 6-27 界面中，选择接入设置-局域网设置，设置内网网关。将网关地址和内网本地连接网关地址一样，内网本地连接网关地址为 10.0.1.1,所以网关也设置为 10.0.1.1。设置好内网后点下面点的保存设置。

(2) 再设置外网如图 6-28 所示。

系统设置

网络设置

DNS 参数

动态域名解析

静态路由

多线负载及策略

透明网桥

网络接口配置

局域网 (LAN)

广域网 (WAN)

IP 隧道客户端

PPTP VPN 客户端

L2TP VPN 客户端

SSL VPN 客户端

防火墙

上网管理

服务应用

流量控制

信息监测

产品中心

广域网接口

设置连接到 Internet 的网卡设备相关信息, 比如 IP 地址、子网掩码、网关等。

WAN-1

WAN-2

网卡位置: 00:09.0 | eth0 | Realtek Semiconductor RTL-8169 Gigabit Ethernet (re

Internet 接入方式: 以太网/静态IP (固定IP上网, 如光纤)

流量统计:
共发送 593.44 KB, 发送包 1.94K, 出错 0, 丢弃 0
共接收 252.08 KB, 接收包 2.14K, 出错 0, 丢弃 0

物理连接状态: 已连接, 速度: 100Mb/s (工作模式: 全双工)

参数设置...

带宽:	下行: 2 Mbit	上行: 130
MAC地址:	00-1d-0f-21-ff-82	
MAC地址克隆:		
IP地址:	192.168.12.12	
子网掩码:	255.255.255.0 (默认) [此网段可容	
网关:	192.168.12.1	
绑定网关MAC地址:		<div>绑定 获取</div>

图 6-28 广域网接口设置界面

图 6-28 中, 接入设置-广域网-WAN-1, 右边 IP 默认是静态 IP, IP 是静态就用默认 IP 地址。

IP 地址: 填写电信提供的外网 IP 地址和子网掩码。

海蜘蛛支持电信、联通双线策略路由, 内置电信和联通路由表, 可以针对电信或联通进行策略路由, 实现访问电信服务器通过电信线路进行访问, 访问联通服务器通过联通线路进行访问, 有效地解决电信联通互联瓶颈问题。

(3) 设置 DNS: 接入设置-DNS 参数-填写上本地的 DNS, 如图 6-29 所示。

系统设置

网络设置

DNS 参数

动态域名解析

静态路由

多线负载及策略

透明网桥

网络接口配置

局域网 (LAN)

DNS 参数

设置用于域名解析(将域名解析成 IP 地址)的服务器地址。

DNS 获取方式:

手动指定

首选 DNS:	202.103.224.68	运营商: 中国电信
辅助 DNS:	192.168.6.53	运营商: 其他运营商-1
可选 DNS-1:	208.67.222.222	运营商: 中国电信

图 6-29 DNS 参数设置界面

系统设置	DNS 域名解析服务	
网络设置	DNS 域名解析服务用于缓存 DNS 解析结果, 以加快客户机域名解析的速度。	
防火墙		
上网管理		
服务应用	DNS 解析服务状态: 运行中 (PID:2808,2809) 查询日志 (7.55Kb) 统计分析 (需开启查询日志)	
DHCP 服务	<div>运行参数DNS 重定向高级</div>	
DNS 代理解析		
NTP 时间服务	启用 DNS 域名解析服务: <input checked="" type="checkbox"/> 是	
Web 缓存加速	强制使用 DNS 代理: <input type="checkbox"/> 是 (DNS 即插即用, 启用后客户机可任意配置)	
PPPoE 拨号服务	DNS 查询记录缓存大小: 8192 (缓存 DNS 查询记录, 默认 8192, 最大)	
PPTP VPN 服务	DNS 缓存时间: 300 s (60~3600, 默认为 300)	
SSL VPN 服务	记录查询日志: <input checked="" type="checkbox"/> 是 (用于调试或分析网络)	
用户帐号管理	查询时严格遵循 DNS 服务器顺序: <input checked="" type="checkbox"/> 是 (一般开启)	
流量控制	一次查询所有 DNS 服务器: <input type="checkbox"/> 是 (一般不开启)	
信息监测	DNS 错误签名: <input type="text"/>	
产品中心		

图 6-30 DNS 代理解析设置界面

在服务应用-DNS 代理解析中启用 DNS 域名解析服务（缓存），如图 6-30 所示，需要的情况下可以勾选强制使用 DNS 代理。有个别地方，特别是偏远地方电信落后 DNS 差，经常出问题，有时候要换外省的 DNS，如果不开启强制使用 DNS 代理，机器上网开网站就会出现 DNS 错误。打勾选择后用外省 DNS 就不会出错了。

（4）防火墙管理

海蜘蛛抵御外部攻击的防火墙功能有三种模式，三种模式分别抵御不同的攻击行为，如图 6-31 所示，主要功能如包括：反端口扫描、攻击动态拦截、ARP 攻击检测、黑（白）名单、端口映射、端口镜像、IP&MAC 绑定（支持强制绑定）、DMZ 主机、DNS 重定向等实用功能。

➤ 控制 P2P 下载连接数

防火墙 TCP 和 UDP 的连接控制，对 P2P 类下载软件非常有效，一般情况下 1 台 PC 在进行 P2P 下载时连接数会达到 1000 以上，严重消耗路由器资源，造成网络环境急剧下降，而通过控制连接数后，一旦超过设定的值路由器将自动丢弃。



图 6-31 端口映射设置界面

➤ IP&MAC 地址强制绑定

在实际的网络使用过程中，用户随意更改 IP 地址的情况很普遍，这样就可能导致 IP 地址冲突，事先规划的 IP 地址被打乱，通过 IP 控制流量的策略也因此并不能有效控制，因此，需要对 IP 地址和网卡 MAC 地址进行强制绑定，用户更改 IP 地址后就不能上网，可以有效杜绝用户私自更改 IP 地址，能够有效的进行网络管理。

如图 6-33 所示，海蜘蛛的防火墙有 MAC 地址的“普通绑定”和“强制绑定”功能。启用强制绑定后当 IP 与绑定的 MAC 地址表不符时，路由器即不响应相应“非法”请求，管理员甚至还可以向“非法用户”推送“自定义内容”，以警告用户不要随意更改 IP。

16	192.168.1.252	00-0c-20-09-1d-df	AP-burgeon5	✓	✎	🗑
17	192.168.1.253	b8-ac-6f-8b-70-c0	Portal-DB	✓	✎	🗑
18	192.168.1.254	00-1d-0f-93-ca-88	AP-burgeon2	✓	✎	🗑

扫描导入 缓存导入 批量修改 导出为XLS

图 6-32 IP&MAC 地址绑定列表

☒ 启用IP与MAC地址绑定

绑定列表

强制绑定

强制进行 IP/MAC 地址绑定:	<input checked="" type="checkbox"/> 是 (只允许与绑定列表中 MAC 地址匹配的 IP 访问 Inte
启用未绑定网页提示:	<input checked="" type="checkbox"/> 是 (未绑定用户上网时将会看到此提示)
提示标题:	您更改了IP地址! (显示在浏览器标题栏)
提示内容:	请不要随意修改IP地址, 否则可能无法上网!

图 6-33 设置 IP&MAC 地址绑定界面

➤ IP\域名\URL 关键字过滤

工作人员可能在工作时间查看一些非工作相关的内容，例如：工作时间网上购物，玩游戏，甚至在线看电影等，不仅影响自身工作，还影响他们正常工作。

如图 6-34 所示海蜘蛛支持多种过滤方式，包括：DNS、IP、域名和 URL 关键字过滤规则，而且这些规划还支持“通配符”，有了这些规则管理员完全可以过滤任何形式的“非法”内容，对工作人员的上网行为进行必要的管理和约束。

系统设置

网络设置

防火墙

基本安全设置

黑白名单

IP-MAC 绑定

DNS/IP过滤

网址/关键字过滤

访问控制列表(ACL)

防火墙日志

网址/关键字过滤

过滤一些您不希望客户机看到或访问的站点，如广告、含有病毒、暴力或色情等内容的网址。关键字过滤可以针对网址（URL）中输入的关键字过滤，一般对搜索引擎或网站的特定目录比较有效；此外，还可以阻止用户下载指定扩展名的文件，只需将文件名后缀加入即可。

☒ 启用网址过滤
 ☐ 只允许访问以下网址
 ☐ 包含DNS过滤规则

☒ 启用URL关键字过滤

需要过滤的网址（每条记录占一行）： [清空列表](#) 3 条记录

.mp3.
 .music.
 .xiaonei.

需要过滤的关键字（每条记录占一行）： [清空列表](#) 8 条记录

.mp3
 game
 kugou
 mp3

图 6-34 网址/关键字过滤界面

➤ ACL 访问控制列表

在如图 6-35 的界面，ACL 可以根据协议、端口、源(目的)网络等，设定访问控制规则，这些规则还可以使用时间来约束。图中设置的规则为只有在 11:30 到 13:30 分之间可以使用 QQ 软件，QQ 软件使用的 TCP 端口号为 8000。

优先级:	1	(只能为数字, 数字越小优先级越高)
协议类型:	TCP+UDP	
数据流向:	进入	
源IP:	0.0.0.0	
源端口:	8000	
目的IP:	0.0.0.0	
目的端口:	8000	
匹配数据包大小:		
时间限制:	<input checked="" type="checkbox"/> 启用	
	起始日期	2011-04-08
	结束日期	2011-04-30
	起始时间	11:30
	结束时间	13:30
星期:	<input type="checkbox"/> 一 <input type="checkbox"/> 二 <input type="checkbox"/> 三 <input type="checkbox"/> 四 <input type="checkbox"/> 五 <input type="checkbox"/> 六 <input type="checkbox"/> 日 <input type="checkbox"/> 工作日 <input checked="" type="checkbox"/> 周末	

图 6-35 ACL 设置界面

➤ 自定义端口映射

传统的中低端路由器因其不能真正的做端口转发,因此不能很好的向外发布内部网络的多台相同的应用服务器(相同端口),如图 6-36 所示,而海蜘蛛则可以将外部访问端口号转换成内部端口号,实现多台相同服务器的对外发布如图 6-37 和 6-38 所示。

虚拟服务器

虚拟服务器定义了广域网服务端和局域网服务器之间的映射。有对该广域网服务端口的访问将会被重定位给通过IP地址指定的局服务器。

服务端口号:		(XX-XX or XX)
IP地址:		
协议:	ALL	
状态:	生效	

图 6-36 虚拟服务器设置界面

修改...

名称:	3389_OA	(只能由字母、数字、汉字、下
优先级:	1	(只能为数字, 数字越小优先级越高)
协议类型:	TCP+UDP	
对外端口:	3243	外部访问端口
对外 IP:	== 所有外网IP (默认) ==	
对内端口:	3389	转换成内部的端口号
对内 IP:	192.168.1.243	
忽略端口:	(您很可能需要将Web管理端口 8888 加入)	
备注:	-OA正式	

图 6-37 设置界面

名称	优先级	协议	对外IP:端口	对内IP:端口	备注
3389_OA	1	TCP+UDP	ALL:3243	192.168.1.243:3389	-OA正式
RTX-8009	1	TCP+UDP	ALL:8009	192.168.1.17:8009	客户端升级
3389_BI	1	TCP+UDP	ALL:3220	192.168.1.220:3389	

图 6-38 端口映射（内网多个相同端口对应不同 IP）

（5）流量控制

海蜘蛛的流量控制有“手动控制”和“智能 QOS 控制”2 种方式，手动控制可以根据网段、控制模式（共享或独立模式）、策略的优先级等方式控制流量，还可以对策略的应用时间进行控制，如图 6-39 所示。手动控制策略对 P2P、BT 等软件同样有效，如结合“连接数”控制对 P2P 类软件的控制效果更好。

智能 QOS 控制与手动控制的原理不尽相同，手动控制是直接控制所有或单个用户的宽带流量，而不管用户访问什么内容；而智能 QOS 则是控制用户访问内容为原则，它将访问内容按“VPN、视频、文字、未识别应用、P2P 下载、图片等”划分为优先级，按访问内容的优先级依次处理，实际上它并不对流量进行控制，如图 6-40 所示。

<input checked="" type="checkbox"/> 启用上传流量控制									
<input checked="" type="checkbox"/> 启用下载流量控制									
手动控制：网段，应用时间，模式，优先级等									
ID	名称	优先级	方向	限速对象	速度范围 (Kbyte/s)	带宽模式	时间	备注	生效
1	全局限速-下载	10	下载	192.168.1.20-192.168.1.239	1-30	独享	08:00-18:30		✓
2	全局限速-上传	20	上传	192.168.1.20-192.168.1.239	1-50	独享	08:00-17:30		✓

图 6-39 流量控制

运行参数

QoS 白名单

状态

当前所有WAN口总带宽为：上行 4MBit, 下行 4MBit, 如果和实际情况不符, 请在 [\[WAN口配置\]](#) 修改, 以免

☐ 启用智能 QoS 流量限速

QoS控制：根据访问内容的优先级做处理

总上行带宽最大使用率：

85%

(60~90%)

4000KBit => 425 KB/s

总下行带宽最大使用率：

95%

(75~95%)

4000KBit => 475 KB/s

启用下载智能识别限制：

☒ 是 (检测到IP在进行下载时自动将其放入下载限速)

P2P/大文件HTTP下载总带宽：

10%

(10~15%)

400KBit => 50 KB/s

未识别应用总带宽：

20%

(20~30%)

800KBit => 100 KB/s

单机初始分配的上传带宽：

20

KB/s

单机初始分配的下载带宽：

60

KB/s

图 6-40 QoS 控制