

ZyWALL 2 Plus

网络安全设备

用户手册

版本 4.00

2006年5月

Edition 1



目录

第 1 章 了解您的ZyWALL	1
1.1 ZyWALL互联网安全设施概述	1
1.2 物理特性	1
1.3 ZyWALL应用范例.....	5
第 2 章Web设置介绍	8
2.1 Web设置界面概述	8
2.2 接入ZyWALL的Web配置界面	8
2.3 重置ZyWALL	9
2.4 ZyWALL Web配置界面向导	10
第 3 章 向导设置.....	24
3.1 向导设置概述.....	24
3.2 Internet接入	24
3.3 VPN向导网关设置	33
3.4 VPN向导网络设置	35
3.5 VPN向导IKE隧道设置（IKE 阶段 1）	37
3.6 VPN向导IPSec隧道设置（IKE 阶段 2）	38
3.7 VPN向导状态汇总	40
3.8 VPN向导设置完成	43
第 4 章 注册	44
4.1 myZyXEL.com概览	44
4.2 注册	44
4.3 服务	46
第 5 章 局域网界面	48
5.1 LAN、WAN 和ZyWALL	48
5.2 IP地址和子网掩码.....	48
5.3 DHCP	49
5.4 RIP 设置.....	50
5.5 组播	50
5.6 WINS	51
5.7 LAN	51
5.8 LAN 静态 DHCP	54

5.9 局域网IP别名	55
第 6 章 网桥界面.....	58
6.1 网桥	58
6.2 生成树协议	59
6.3 网桥	60
第 7 章 广域网界面	63
7.1 广域网概述	63
7.2 TCP/IP优先权（跃点数）	63
7.3 广域网路由	63
7.4 广域网IP地址分配.....	65
7.5 DNS服务器地址分配.....	65
7.6 WAN MAC地址.....	65
7.7 广域网	66
7.8 流量重定向	77
7.9 配置流量重定向	78
7.10 配置备用拨号	79
7.11 高级模式设置	83
7.12 配置高级调制解调器的参数	84
第 8 章 防火墙界面	86
8.1 防火墙概述	86
8.2 防火墙连接方向	87
8.3 安全性事项	87
8.4 防火墙规则示例	88
8.5 防火墙缺省规则（路由模式）	90
8.6 防火墙缺省规则（网桥模式）	91
8.7 防火墙规则汇总	93
8.8 反探测.....	98
8.9 拒绝服务（DoS）攻击	99
8.10 防火墙门限	100
8.11 Threshold界面.....	101
8.12 服务	103
8.13 解决非对称路由问题示例.....	105
8.14 我的服务防火墙规则示例	106

第 9 章 内容过滤界面	111
9.1 内容过滤概述	111
9.2 内容过滤常规信息的配置	111
9.3 基于分类的内容过滤（Category Based 内容过滤ing）	114
9.4 内容过滤分类	114
9.5 用户自定义	120
9.6 自定义关键字的检索	122
9.7 内容过滤缓存	123
第 10 章 内容过滤报告	125
10.1 查看内容过滤激活情况	125
10.2 查看内容过滤报告	125
10.3 网站递交	130
第 11 章 IPSec VPN	132
11.1 IPSec VPN概述	132
11.2 基于因特网密钥交换（IKE）的虚拟专用网（VPN）规则	144
11.3 编辑因特网密钥交换（IKE）方式下的VPN 网关策略	146
11.4 VPN规则（IKE）：编辑网络策略	153
11.5 VPN规则（IKE）：网络策略移动	158
11.6 VPN规则（手动）	159
11.7 VPN规则（手动）：编辑	161
11.8 VPN SA监控	164
11.9 VPN通用设定	165
11.10 远程办公VPN/IPSec的范例	167
第 12 章 证书	171
12.1 证书的优点	172
12.2 自签名证书	172
12.3 配置汇总	172
12.4 我的证书	173
12.5 导入一个证书	175
12.6 创建一个证书	176
12.7 证书详细内容	179
12.8 可信任的CA	183
12.9 导入一个可信的CA证书	184

12.10	可信任CA证书的详细内容	185
12.11	可信任的远程主机	188
12.12	验证一个可信任远程主机的证书	190
12.13	导入一个可信任远程主机的证书	191
12.14	可信任远程主机证书的详细内容	192
12.15	目录服务器	195
12.16	添加或编辑目录服务器	196
第 13 章	认证服务器	199
13.1	认证服务器概述	199
13.2	本地用户数据库	199
13.3	RADIUS（远程认证拨号用户服务）	199
13.4	本地用户数据库	200
13.5	RADIUS	202
第 14 章	网络地址转换（NAT）	204
14.1	NAT 简介	204
14.2	使用 NAT	209
14.3	NAT 概述	210
14.4	NAT地址映射（NAT Address Mapping）	211
14.5	端口转发	214
14.6	配置端口转发	217
14.7	端口转发示例—WAN 到 LAN的HTTP转发规则	218
14.8	端口触发（Port Triggering）	219
第 15 章	静态路由	223
15.1	IP静态路由	223
15.2	静态路由界面	223
第 16 章	带宽管理	227
16.1	带宽管理概述	227
16.2	带宽分类与过滤	227
16.3	按比例分配带宽	228
16.4	基于应用的带宽管理	228
16.5	基于子网的带宽管理	228
16.6	基于应用和子网的带宽管理范例	228
16.7	调度	229

16.8	带宽借用	231
16.9	同时启用带宽借用和最大带宽利用	232
16.10	配置汇总	233
16.11	设置类别	234
第 17 章	DNS.....	242
17.1	DNS概述.....	242
17.2	DNS服务器地址分配	242
17.3	DNS服务器	242
17.4	地址记录	243
17.5	名称服务器记录	243
17.6	系统界面	244
17.7	DNS缓存.....	248
17.8	配置DNS缓存	249
17.9	配置DNS DHCP	250
17.10	动态DNS.....	251
17.11	配置动态DNS.....	252
第 18 章	远程管理.....	255
18.1	远程管理概述	255
18.2	介绍HTTPS	256
18.3	WWW	257
18.4	HTTPS范例.....	258
18.5	SSH	264
18.6	如何工作	264
18.7	ZyWALL上的SSH应用	265
18.8	配置SSH	266
18.9	使用SSH执行Telnet的范例	267
18.10	使用SSH的安全FTP范例	269
18.11	Telnet	269
18.12	配置TELNET	270
18.13	配置FTP	271
18.14	配置SNMP	272
18.15	配置DNS.....	275
18.16	介绍Vantage CNM	275

18.17 配置CNM	276
第 19 章 UPnP	279
19.1 通用即插即用功能介绍	279
19.2 配置UPnP	280
19.3 浏览UPnP端口映射	281
19.4 在Windows中安装UPnP范例	282
19.5 在Windows XP中使用UPnP范例	284
第 20 章 ALG界面	288
20.1 ALG概述	288
20.2 FTP	288
20.3 H.323	289
20.4 RTP	289
20.5 SIP	290
20.6 ALG界面	291
第 21 章 日志界面	293
21.1 配置View 日志	293
21.2 日志描述范例	294
21.3 配置日志参数	296
21.4 配置报告信息	300
第 22 章 维护	306
22.1 维护介绍	306
22.2 常规设置	306
22.3 配置密码	307
22.4 时间和日期	308
22.5 预定义NTP时间服务器列表	310
22.6 透明网桥介绍	312
22.7 透明防火墙	313
22.8 配置设备模式（路由模式）	314
22.9 配置设备模式（网桥模式）	315
22.10 韧体升级界面	316
22.11 备份和恢复	318
22.12 重启动界面	320
第 23 章 SMT介绍	322

23.1 SMT介绍	322
23.2 通过控制口访问SMT	322
23.3 SMT界面导航	323
23.4 更改系统密码	328
23.5 重置 ZyWALL	329
第 24 章 SMT菜单 1-常规设置	329
24.1 常规设置的介绍	329
24.2 配置常规设置	329
第 25 章 广域网和拨号备份设置	336
25.1 介绍广域网和拨号备份配置	336
25.2 广域网配置	336
25.3 拨号备份	337
25.4 在菜单 2 中配置拨号备份	337
25.5 高级WAN设置	338
25.6 远程节点说明（备份ISP）	340
25.7 编辑PPP选择	342
25.8 编辑 TCP/IP 选项	343
25.9 编辑登录脚本	345
25.10 远程节点过滤器	347
第 26 章 LAN设置	349
26.1 LAN设置介绍	349
26.2 访问LAN菜单	349
26.3 LAN口过滤设置	349
26.4 TCP/IP和DHCP以太网设置菜单	350
第 27 章 Internet接入	355
27.1 Internet接入设置介绍	355
27.2 以太网封装	355
27.3 配置PPTP客户端	357
27.4 配置PPPOE客户端	358
27.5 基本设置完成	359
第 28 章 远程节点设置	360
28.1 远程节点设置基础	360

28.2	远程节点设置	360
28.3	远程节点参数组设置	360
28.4	编辑IP	366
28.5	远程节点过滤器	368
28.6	流量重定向	369
第 29 章	IP静态路由设置	371
29.1	IP静态路由设置	371
第 30 章	网络地址转换 (NAT)	373
30.1	应用NAT	373
30.2	NAT设置	375
30.3	配置一个NAT之后的服务器	381
30.4	普通NAT范例	383
30.5	触发端口转发	390
第 31 章	ZyWALL防火墙介绍	392
31.1	进入防火墙设置	392
31.2	防火墙 SMT 菜单	392
第 32 章	过滤器配置	394
32.1	过滤器介绍	394
32.2	包过滤与防火墙比较	396
32.3	配置一个过滤器	398
32.4	过滤器实例	406
32.5	过滤器类型和NAT	409
32.6	防火墙与过滤器	410
32.7	应用一个过滤器	410
第 33 章	SNMP配置	412
33.1	SNMP配置	412
33.2	SNMP 陷阱	413
第 34 章	系统信息和诊断	414
34.1	系统状况介绍	414
34.2	系统状况	414
34.3	系统信息和控制口速度	416
34.4	日志记录和追踪	418

34.5 Diagnostic	423
第 35 章 韧体和配置文件维护	426
35.1 介绍	426
35.2 文件名协定	426
35.3 备份配置	427
35.4 恢复配置	432
35.5 上传韧体和配置文件	434
第 36 章 系统维护菜单 8 到 10	441
36.1 命令解释程序模式	441
36.2 呼叫控制支持	443
36.3 设置时间和日期	445
第 37 章 远程管理	449
37.1 Remote Management	449
第 38 章 访问时间表	452
38.1 访问时间表介绍	452
第 39 章 排障	456
39.1 ZyWALL启动问题	456
39.2 LAN端口的问题	456
39.3 WAN接口上的问题	457
39.4 访问ZyWALL时的问题	457
39.5 数据包流	465

第 1 章 了解您的 ZyWALL

本章将会向您介绍 ZyWALL 的主要特点和应用方式。

1.1 ZyWALL 互联网安全设施概述

加载 ZyWALL 时伴随的安全特性包括 VPN、防火墙、内容过滤和证书。您还可以用最小的配置将 ZyWALL 配置为现有网络中透明的防火墙。ZyWALL 提供了带宽管理、NAT、端口转发、DHCP 服务器和许多其他强大的功能。

1.2 物理特性

4 端口局域网交换机

交换机和路由器的组合令 ZyWALL 成为经济有效的可行网络解决方案。您无需再另行支付集线器的费用就可以将最多四台计算机连接到 ZyWALL。使用集线器将四个以上的计算机添加到您的局域网中。

广域网

以太网 WAN 端口通过宽带调制解调器或路由器连接到互联网。

自适应 10/100 Mbps 以太网端口

所有 ZyWALL 的以太网端口均是 10/100 Mbps 自动协商的。这允许 ZyWALL 检测传入传输的速度并在无需手动干预的情况下适当调节。它们允许以半双工或全双工的模式按 10 Mbps 或 100 Mbps 的速度传输数据，具体模式取决于您的以太网网络。这些端口还可以自动交叉 (MDI/MDI-X)，意味着这些端口可以通过以太网端口按交叉网线或直接网线进行连接。

备用拨号广域网

如果广域网和流量重定向连接失败，备用拨号端口可逆向用作传统拨号连接。

时间和日期

当您开启 ZyWALL 时，ZyWALL 允许您从外部服务器中获取当前时间和日期。您还可以手动设置时间。

重置按钮

使用重置按钮将工厂默认密码复原为 1234；将 IP 地址复原为 192.168.1.1，将子网掩码复原为 255.255.255.0，且复原为用 192.168.1.33 开头的 32 个 IP 地址启用的 DHCP 服务器。

1.2.1 非物理特性

透明防火墙

ZyWALL 通过在两个 WAN 端口之间分担数据的传输来提高服务质量，并实现带宽的最大利用率。

SIP 穿越

ZyWALL 内置了一个 SIP 应用层网关 (ALG)。通过检查和转换数据流中内置的 IP 地址，ZyWALL 可以允许 VoIP 呼叫通过 NAT。您可以在 ALG 界面中启用或者禁用 SIP ALG 功能。

STP (生成树协议) /RSTP (快速 STP)

当 ZyWALL 设置为网桥模式的时候，(R)STP 可以检测并消除网络环路，并可以提供交换机，网桥或路由器之间的备份链路。它允许您网络中的一个网桥可以和其它支持(R)STP 的网桥交换相关信息，确保网络中的两个站点之间只存在一条路径。带宽管理带宽管理允许您按照自定义规则来分配网络资源。这种功能可以更好地帮助您实现一些实时性要求较高的应用，例如 VoIP 的应用。

带宽管理

带宽管理允许您按照自定义规则来分配网络资源。这种功能可以更好地帮助您实现一些实时性要求较高的应用，例如 VoIP 的应用。

IPSec VPN 的支持

您可以和商业伙伴，分支机构建立一条虚拟私有网络 (VPN) 的连接，在互联网上传输经过加密的数据，VPN 可以为用户提供安全的连接而不需要租用昂贵的专线服务。ZyWALL 的 VPN 是基于 IPSec 标准的，完全兼容于其它基于 IPSec 标准的 VPN 产品。

X-Auth (扩展认证)

X-Auth 为 VPN 提供了附加的安全保证，每个 VPN 的客户端在接入的时候都要输入用户名和密码。

证书

ZyWALL 可以采用证书 (又称数字 ID) 对用户进行认证，证书基于公私密钥机制。证书提供了一种在认证过程中安全交换公钥的方法。

SSH

ZyWALL 可以采用 SSH (安全壳) 安全通信协议来保证加密的数据在非安全网络中的两台主机之间安全传输。

HTTPS

安全套接层超文本传输协议或 SSL HTTP 是一种负责对 web 会话进行加密或解密的协议。HTTPS 方式可以保证用户以安全的方式登陆 ZyWALL 的 web 设置界面。

防火墙

ZyWALL 是一款全状态检测型的防火墙，可以防止 DoS 攻击。默认方式下，防火墙为激活状态，非 LAN 要求的 WAN 到 LAN 的数据流量将被丢弃。ZyWALL 可以支持 TCP/UDP 检查，DoS 侦测及防护，实时的警告，报告，日志等功能。

内容过滤

ZyWALL 可以阻止一些 web 特征，例如启用 X 控件，Java 小程序和 cookies，也可以禁止网内用户使用 web 代理服务器。ZyWALL 可以禁止或者允许网内用户访问您所指定的网站。ZyWALL 还可以禁止网内用户访问您指定的有某些关键字（如色情或暴力等）的网站。您可以按照时间段来启用或者禁用内容过滤功能，也可以指定需要经过内容过滤器检测的用户范围。

您也可以购买内容过滤目录库，ZyWALL 将会检索内容过滤数据目录库来过滤含有色情，暴力等内容的网站，目录库会定期升级，它会维护成千上万条站点信息。

通用即插即用(UPnP)

使用标准 TCP/IP 协议，ZyWALL 和其他启用通用即插即用的设备可以动态假如网络，获得 IP 地址，并将其功能转换到网络上的其他设备。

RADIUS (RFC2138, 2139)

远程验证拨入用户服务（RADIUS）服务器允许用户验证、授权和计费。

IEEE 802.1x 网络安全

ZyWALL 支持 IEEE 802.1x 标准，它配合 IEEE 802.11 的无线应用可以增强用户认证机制。内置的认证服务器可以允许您设置和对 32 个用户进行认证，您也可以外接认证服务器，为用户提供接入认证服务。

数据包过滤

数据包过滤机制阻止不想要的流量进入/离开您的网络。

呼叫排程

配置所有时间周期以限制和允许用户在远程节点上的访问。

PPPoE

ZyWALL 内置的 PPPoE 功能可以让用户采用熟悉的拨号网络登陆的方式接入到宽带网络。

PPTP 封装

点对点隧道协议(PPTP)是允许将数据从远程客户端传输到专用服务器的网络协议，使用基于 TCP/IP 的网络来创建虚拟专用网络(VPN)。PPTP 支持诸如互联网等公共网络的按需、多协议和

虚拟专用网络连接。ZyWALL 支持在任何给定时间的一个 PPTP 服务器连接。

动态 DNS 支持

采用动态 DNS（域名系统）支持时，您可以具有动态 IP 地址的静态主机名的别名，使得更易于从互联网的各个位置访问主机。您必须在动态 DNS 服务提供商处登记此项服务。

IP 组播

使用 IP 组播将 IP 数据包传送到主机的特定组。互联网组管理协议（IGMP）是用于支持组播组的协议。最新的版本是版本 2（参见 RFC 2236）；ZyWALL 同时支持版本 1 和版本 2。

IP 别名

IP 别名允许通过相同的以太网接口将物理网络划分为逻辑网络。ZyWALL 支持三个逻辑局域网，通过其单个物理以太网 LAN 接口与 ZyWALL 作为每个网络的网关进行接口。

集中网络管理

集中网络管理(CNM)允许企业或服务提供商网络管理员管理您的 ZyWALL。企业或服务提供商网络管理员可以配置您的 ZyWALL、执行固件升级和为您进行故障诊断。

SNMP

SNMP（简单网络管理协议）是用于在网络设备间交换管理信息的协议。SNMP 是 TCP/IP 协议族的一员。ZyWALL 支持 SNMP 协议，允许用户采用 SNMP 协议管理 ZyWALL 网络。ZyWALL 支持的版本为（SNMP v1）。

网络地址转换（NAT）

网络地址转换（NAT）允许将网络内部的 IP 地址（如局域网私有地址）转换为合法的公网 IP 地址。

数据流量重定向

当 ZyWALL 不能连通互联网的时候，您可以将 WAN 口的数据重新定向发送给局域网上面的一个备份网关，这样您可以在正常的 WAN 口连接失效的时候，采用一种灵活的备份方式，保证数据的持续传输。

端口转发

利用该功能您可以将某些基于端口接入的服务请求重新定向到局域网内某一台服务器上。您需要输入准备转发的一个或一组端口号，和指定为服务器的本地 IP 地址。

DHCP(动态主机配置协议)

DHCP(动态主机配置协议)允许单个客户端计算机在启动时从集中的 DHCP 服务器中获得 TCP/IP 配置。ZyWALL 具有内置的 DHCP 服务器功能，默认情况下是启用的，这意味着它可以

将 IP 地址、IP 默认网关和 DNS 服务器分配到支持 DHCP 客户端的所有系统。ZyWALL 还可以用作代理 DHCP 服务器，该服务器将 IP 地址赋值从另一个 DHCP 服务器中继到客户端。

完全网络管理

内嵌的 web 配置程序是可在所有平台上运行且基于 web 的实用程序，使您易于管理和配置 ZyWALL。ZyWALL 的大多数功能还是通过 SMT(系统管理终端)接口进行软件配置的。SMT 是菜单驱动的接口，可通过控制台连接端口或 telnet 连接访问终端模拟器。

支持 RoadRunner

除了标准的有线调制解调器服务之外，ZyWALL 还支持时代华纳的 RoadRunner 服务。

日志和追踪

内置的日志信息和封包追踪功能。

支持 sys 日志工具。

可升级的固件

ZyWALL 的固件可升级。

内置 FTP 和 TFTP 服务器

ZyWALL 内置 FTP 和 TFTP 服务器，用于升级固件和恢复配置。

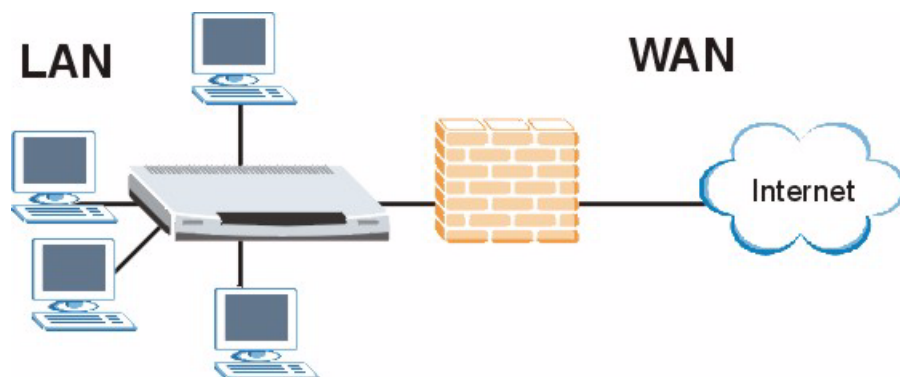
1.3 ZyWALL 应用范例

以下是几个 ZyWALL 的实际应用范例。

1.3.1 通过有线调制解调器或 DSL 调制解调器的安全宽带互联网接入

您可以以太网端口将有线调制解调器、DSL 或无线调制解调器连接到 ZyWALL 用于宽带互联网接入。ZyWALL 不但确保高速互联网接入，还能确保安全的内部网络保护和流量管理。

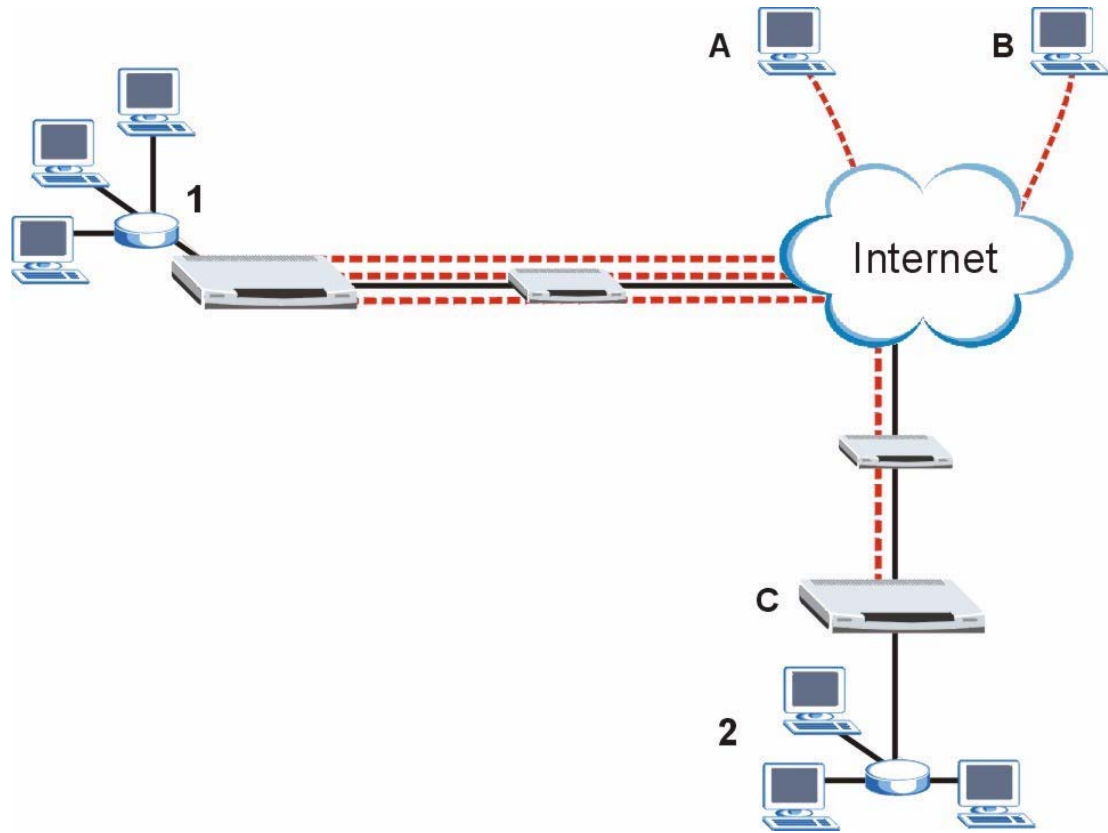
图 1 通过有线调制解调器、DSL 调制解调器或无线调制解调器的安全互联网接入



1.3.2 VPN 应用

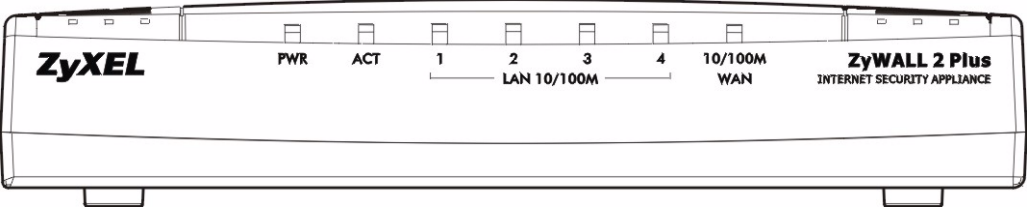
ZyWALL VPN 是通过互联网连接分公司和商业合作伙伴的理想的经济有效方式，无需站点间的租用线路（和费用）。在下图中，A 是安全远程管理的 VPN 客户端，B 是用于远程接入的 VPN 客户端，而 C 是远程 IPSec 路由器。LAN 标记为 1 而远程网络标记为 2。点划线显示了 VPN 隧道。

图 2 VPN 应用



1.3.3 前侧面板指示灯

图 3 前侧面板



下表描述了指示灯。

表 1 前侧面板指示灯

LED	颜色	状态	说明
PWR		熄灭	ZyWALL 被关闭。
	绿色	点亮	ZyWALL 被开启。
	红色	闪烁	ZyWALL 正执行系统测试。
		点亮	ZyWALL 的功率过低。
ACT	绿色	熄灭	备用端口未连接。
		点亮	备用端口已连接。
		闪烁	备用端口正发送或接收数据包。
LAN 10/100M 1-4		熄灭	LAN 未连接。
	绿色	点亮	ZyWALL 具有成功的 10Mbps 以太网连接。
		闪烁	10M LAN 正发送或接收数据包。
	橙色	点亮	ZyWALL 具有成功的 100Mbps 以太网连接。
		闪烁	100M LAN 正发送或接收数据包。
WAN 10/100M		熄灭	广域网连接未就绪，或已经失败。
	绿色	点亮	ZyWALL 具有连接成功的 10Mbps 广域网连接。
		闪烁	10M WAN 正发送或接收数据包。
	橙色	点亮	ZyWALL 具有成功的 100Mbps 广域网连接。
		闪烁	100M WAN 正发送或接收数据包。

第 2 章 Web 设置介绍

本章说明了如何访问 ZyWALL web 配置程序并提供该界面的概述。

2.1 Web 设置界面概述

内置的 web 设置菜单可以让您通过浏览器（如 IE 或 Netscape Navigator）来方便地管理 ZyWALL。您需要采用 IE 6.0 及以上版本或 Netscape Navigator 7.0 及以上版本，浏览器需要支持 Java 脚本功能。请您注意不同的固件版本在设置界面上可能会有所不同。建议您将计算机界面分辨率设置成 1024*768，这样可以获得一个好的视觉效果。

为了使用 web 配置程序，您需要允许：

- 来自设备的 Web 浏览器弹出窗口。默认情况下，在 Windows XP SP（服务包）2 中 Web 弹出阻止是启用的。
- JavaScripts（默认情况下是启用的）。
- Java 权限（默认情况下是启用的）。

如果您要确保在 Internet Explorer 或 Netscape Navigator 中可以使用这些功能，则请参见故障诊断章节。

2.2 接入 ZyWALL 的 Web 配置界面

1. 确保您的 ZyWALL 已经和电脑正确地连接起来（请参考快速安装指南）。
2. 开启 web 浏览器。
3. 在浏览器地址栏中输入“192.168.1.1”。
4. 在密码栏中输入“1234”（默认密码），然后点击替换。在某些版本中，默认密码会自动填入密码栏中，您只需要点击替换即可。
5. 您会看到一个提示您修改密码的界面，我们强烈建议您修改 ZyWALL 的初始密码。输入新的密码，然后在确认栏中重新输入一遍新密码，点击应用后点击替换，或者点击忽略。

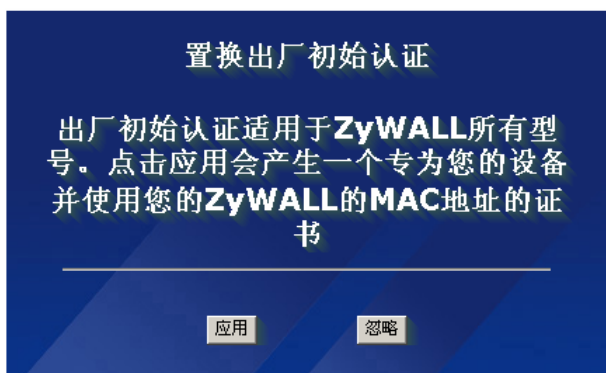
图 4 修改密码界面



6. 在替换认证画面中点击应用，可以创建一个使用 ZyWALL 的 MAC 地址来标识设备的证书。

注意：如果不在此或者在证书界面中替换该缺省证书，您每次登陆的时候都会见到此提示界面。

图 5 替换证书界面



7. 您现在可以看到首页（请参考图 7）。

注意：如果系统管理员在管理员闲置时间中设置了管理任务自动时间溢出的时间段（缺省为 5 分钟），那么您在该画面不作任何操作的话，一定的时间之后，系统将会断开和管理者的连接，您必须重新登陆 ZyWALL。

2.3 重置 ZyWALL

如果您忘记了 ZyWALL 的密码或者不能接入到 web 浏览器，您可以重置 ZyWALL 使它恢复出厂默认配置，利用 ZyWALL 后面的重置按钮即可恢复出厂默认配置。您也可以将出厂默认配置文件上传到 ZyWALL 上替代原有的配置文件。进行了重置操作意味着您以前的所有配置将会全部清除，控制口速率恢复为 9600 bps，8 个数据位，无奇偶校验位，1 个停止位，没有数据流控，密码恢复为 1234。

2.3.1 如何使用重置按钮

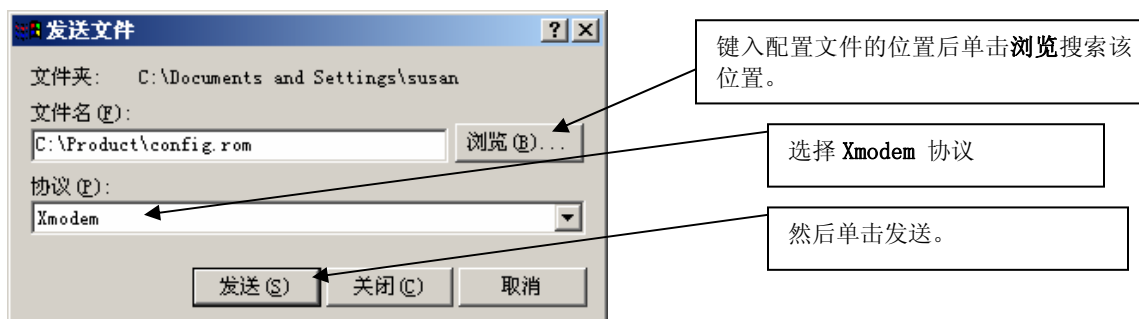
您在开始操作之前请先确认 **SYS LED** 指示灯是常亮的（不是闪烁的）。

- 1 按下重置按钮 10 秒钟，然后松开。ZyWALL 采用复原的默认设置重新启动。否则转到步骤 2。
- 2 关闭 ZyWALL。
- 3 按住重置按钮，然后打开 ZyWALL 的电源。
- 4 持续按住重置按钮。ZyWALL 采用复原的默认设置重新启动。
- 5 松开重置按钮，等待 ZyWALL 重新启动完毕。

2.3.2 通过控制口上传配置文件

1. 从 ftp.zyxel.com 上下载缺省配置文件，解压缩到一个文件夹中。
2. 关闭 ZyWALL，建立一个超级终端连接并打开 ZyWALL 电源。当出现“Press Any key to enter Debug 模式 within 3 秒”的时候，按下任何键进入 debug 模式。
3. 在“Enter Debug 模式”提示符下输入“atlc”。
4. 等待出现“Starting Xmodem upload”信息提示，采用超级终端方式下的 Xmodem 协议传输文件。
5. 点击传送，然后点击发送文件，随后会出现如下界面。

图 6 Xmodem 上传范例



6. 上传韧体成功后，输入“atgo”重新启动设备。

2.4 ZyWALL Web 配置界面向导

下面将从首页界面开始为您介绍 ZyWALL 的配置界面。

注意：您可以参考以下对首页页面的说明或者点击  图标（位于界面的右上角）寻

求在线帮助。

该界面会根据您在设备维护的设备模式界面中的选项有所不同。

2.4.1 路由模式

当 ZyWALL 设置为路由模式的时候，您会见到以下界面。ZyWALL 的缺省设置为路由模式。

图 7 Web 主配置界面（路由模式）



以下为界面相关的描述。

表 2 Web 主配置界面（路由模式）

标签	描述
快速设置向导	
接入互联网	单击接入互联网以使用初始配置向导。这会配置连接到互联网的广域网端口。
VPN	单击 VPN 以配置虚拟专用网络 (VPN) 策略，用于站点之间的安全通讯。
设备信息	
系统名称	这是您在设备维护常规界面中输入的系统名称。该名字用于识别。
固件版本	这是已创建的 ZyNOS 固件版本和日期。ZyNOS 是 ZyXEL 的自有网络操作系统。

路由协议	这显示了配置 ZyWALL 的 IP 路由协议。该字段是不可配置的。
设备模式	这显示了 ZyWALL 用作路由器还是网桥。
防火墙	这显示了 ZyWALL 的防火墙是否被激活。
系统时间	该字段显示了您的 ZyWALL 的当前日期和时间以及与格林威治时区 (GMT) 的时差。与 GMT 的时差值基于时区。如果您设置 ZyWALL 采用夏令时，还可以调节夏令时的时差。
内存	第一个数字表示了 ZyWALL 正使用多少个千字节的缓存。缓存指得是 ZyNOS (ZyXEL 网络操作系统) 未使用的存储器，且可用于运行 NAT、VPN 和防火墙等进程。 第二个数字表示了 ZyWALL 的总缓存（以千字节为单位）。 这一栏显示了多少百分比的 ZyWALL 缓存正被使用。当达到最大值时，该栏颜色从绿色变为红色。
会话进程	第一个数字显示 ZyWALL 当前正在处理的会话数量。其中包括当前的所有会话：穿过 ZyWALL 的 终结于 ZyWALL 的 初始于 ZyWALL 的 第二个数字显示的是 ZyWALL 可以同时处理的最大会话数量。进度条显示现在处理的会话数量占可处理最大会话数量的百分比例。当数值接近最大的时候，进度条会由绿色变成红色。
网络状态	

表 2 Web 主配置界面（路由模式）（续）

标签	描述
网络界面	这是端口类型。单击“+”展开或单击“-”折叠局域网下拉列表。
状态	对于局域网端口，这显示了端口速度和双工设置。以太网端口可以是半双工或全双工模式。全双工指的是设备同时发送和接收数据的能力，半双工指的是数据流每次只可以在一个方向流动。以太网端口必须使用与同层连接的以太网端口相同的速度或双工模式设置来连接。 对于广域网和备用拨号端口，如果您正使用以太网封装则它显示端口速度和双工设置，而如果您正使用 PPPoE 封装，则会出现未连接（线路停用或未连接）、空闲（线路(ppp)空闲）、呼叫（开始触发呼叫）或丢弃（丢弃一个

	呼叫)。
IP 地址	这显示了端口的 IP 地址。
子网掩码	这显示了端口的子网掩码。
DHCP	对于广域网，DHCP client 显示 ZyWALL 是否自动获取其 IP 地址。静态显示 ZyWALL 是否手动输入静态（固定）IP 地址。 对于局域网，DHCP 服务器显示了何时将 ZyWALL 设置为自动将 IP 地址信息送给连接到局域网的计算机。DHCP relay 显示了何时将 ZyWALL 设置为将 IP 地址分配请求转发到另一台 DHCP 服务器。静态显示了局域网端口正使用静态的（固定的）IP 地址。这种情况下，您必须在您的局域网上具有另一台 DHCP 服务器，否则这些计算机必须被手动配置。 对于备用拨号端口，这显示为 N/A。
更新	如果您正使用以太网封装，且广域网端口配置为自动从 ISP 中获取 IP 地址，单击更新以释放广域网端口动态分配的 IP 地址并再次获取 IP 地址。单击呼叫以拨号接入 PPTP、PPPoE 或备用拨号连接。
显示统计资料	单击显示统计资料以查看性能统计信息，例如每个端口发送的数据包数和接收的数据包数。
显示 DHCP 表单	单击显示 DHCP 表单以显示 ZyWALL 已经将 IP 地址信息分配到的计算机的列表。
VPN 状态	单击 VPN 状态以显示活动的 VPN（安去的）连接。

2.4.2 网桥模式

当 ZyWALL 设置成网桥模式的时候，您会见到以下界面。在网桥模式下，ZyWALL 不能从一个 DHCP 服务器获得一个 IP 地址。LAN，WAN，DMZ 和 WLAN 端口都具有相同的（静态的）IP 地址和子网掩码。您可以配置 ZyWALL 的 IP 地址用于访问管理。如果您想通过计算机直接连接到 ZyWALL，您需要给该计算机配置一个和 ZyWALL 在同一个子网下的 IP 地址。

ZyWALL 会以网桥的方式传送各端口之间的数据。您可以使用网桥模式（请参考防火墙一章了解防火墙的详细配置）下的防火墙。

图 8 Web 主配置界面（网桥模式）



以下为界面相关的描述。

表 3 Web 主配置界面（网桥模式）

标签	描述
VPN	单击 VPN 以配置虚拟专用网络(VPN) 策略，用于站点之间的安全通信。
设备信息	
系统名称	这是您在设备维护 常规界面中输入的系统名称。用于标识。
固件版本	这是已创建的 ZyNOS 固件版本和日期。ZyNOS 是 ZyXEL 的自有网络操作系统。
设备模式	这显示了 ZyWALL 的作用是路由器还是网桥。
防火墙	这显示了 ZyWALL 的防火墙是否被激活。

系统时间	该字段显示了您的 ZyWALL 的当前日期和时间，以及与格林威治时区(GMT)的时差。与 GMT 的时差取决于时区。如果您设置 ZyWALL 使用夏令时，这还要按照夏令时进行调节。
内存	第一个数字表示了 ZyWALL 正使用多少个千字节的缓存。缓存指得是 ZyNOS (ZyXEL 网络操作系统) 未使用的存储器，且可用于运行 NAT、VPN 和防火墙等进程。 第二个数字表示了 ZyWALL 的总缓存（以千字节为单位）。 这一栏显示了多少百分比的 ZyWALL 缓存正被使用。当达到最大值时，该栏颜色从绿色变为红色。
会话进程	第一个数字显示 ZyWALL 当前正在处理的会话数量。其中包括当前的所有会话： 穿过 ZyWALL 的 终结于 ZyWALL 的 初始于 ZyWALL 的 第二个数字显示的是 ZyWALL 可以同时处理的最大会话数量。进度条显示现在处理的会话数量占可处理最大会话数量的百分比比例。当数值接近最大的时候，进度条会由绿色变成红色。
网络状态	
IP 地址	这是 ZyWALL 的 IP 地址，是用句点分隔的十进制数字。
子网掩码	这是 ZyWALL 的 IP 子网掩码。
网关 IP 地址	这是网关 IP 地址。该网关通常是将 ZyWALL 连接到互联网的设备。
网关 IP 地址	这是网关 IP 地址。该网关通常是将 ZyWALL 连接到互联网的设备。
RSTP	这显示了快速跨接树协议（RSTP）是否激活。当 RSTP 被禁用时，以下与 RSTP 相关的标签或值不会应用。
网桥优先级	这是 ZyWALL 的网桥优先权。
网桥问候时间	这是从根网桥中网桥协议数据单元（BPDU）的时间间隔。
网桥最大保留时间	这是预先定义的时间间隔，网桥在此时间间隔后从根网桥中获取欢迎消息（BPDU）。
传送延迟	这是转发延迟时间间隔。
网桥端口	这是端口类型。端口类型为 WAN 或 LAN。

通信端口状态	这显示了端口速度和双工设置。以太网端口连接可以是半双工或全双工模式。全双工模式指的是同时发送和接收数据的设备能力，而半双工模式指的是每次流量只可以从一个方向流动。以太网端口必须使用与同层连接的以太网端口相同的速度或双工模式设置来连接。 对于广域网连接，当链路还未就绪或连接失败时，它显示未连接。
RSTP 状态	这是相应端口的 RSTP 状态。
启用 RSTP	这显示了相应端口上的 RSTP 是否激活。
RSTP 优先级	这是相应端口的 RSTP 优先权。
RSTP 路径权值	这是将帧从根网桥传送到相应端口的开销。
显示统计资料	单击显示统计资料以查看网桥性能统计信息，例如每个端口发送的数据包数和每个端口接收的数据包数。
VPN 状态	单击 VPN 状态以显示活动的 VPN（安全的）连接。

2.4.3 导航栏

当您输入密码后，可以采用导航栏来设置 ZyWALL 的各种特征。下表描述了每种模式下的特征列表。

表 4 特征比较

特征	网桥模式	路由模式
互联网接入向导		○
VPN 向导	○	○
DHCP 表		○
系统统计	○	○
注册	○	○
局域网		○
广域网		○
网桥	○	
防火墙	○	○
内容过滤器	○	○
VPN	○	○
证书	○	○
验证服务器	○	○
NAT		○
静态路由		○
带宽管理	○	○

DNS		O
远程管理	O	O
通用即插即用		O
ALG	O	O
日志	O	O
维护	O	O

注意：模式列表中的“O”说明在此模式下 ZyWALL 具有此项功能。列表中的相关信息目前都正确，但是以后可能会有所改动。

以下为子菜单的相关描述。

表 5 界面汇总

链接	项目	功能
首页		该界面显示了 ZyWALL 的设备信息和网络状态。在该界面下您可以访问向导，统计和 DHCP 表。
注册	注册	您可以在该界面注册您的 ZyWALL，并激活您定制的试用服务。
	服务	您可以在该处管理和更新服务状态，及许可证信息。
网络		
LAN	LAN	您可在该界面中设置 LAN DHCP 和 TCP/IP 参数。
	静态 DHCP	您可在该界面中为 LAN 用户分配固定的 IP 地址。
	IP 别名	您可在该界面中为 LAN 口设置多个子网接口。
网桥	网桥	您可在该界面中修改 ZyWALL 的网桥参数。
WAN	路由	该界面允许您配置广域网流量重定向和备用拨号路由优先权。
	WAN	使用该界面以配置 the WAN 端口 for 互联网接入。
	流量重定向	使用该界面以配置您的流量重定向属性和参数。
	拨号备份	使用该界面以配置备用广域网拨号连接。
安全		
防火墙	默认规则	您可在该界面中激活或禁用防火墙功能，并根据网络数据流向应用到防火墙规则中。
	规则概述	该界面中显示了防火墙规则的汇总信息，允许您编辑/删除防火墙的规则。
	反探测	您可在该界面中修改反探测的设置。
	临界值	您可在该界面中设置 DoS 攻击的门限值。
内容过滤	常规	该界面允许您启用过滤和阻止某些 web 功能。

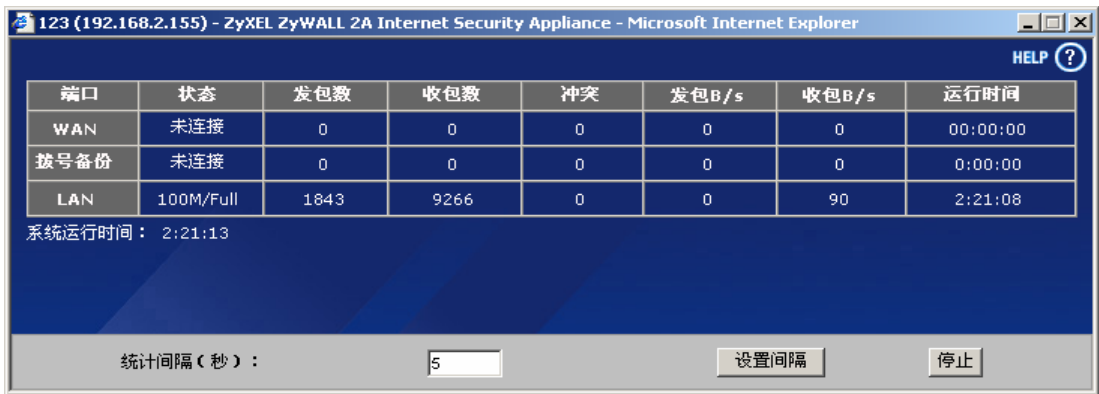
	类别	使用该界面以选择要过滤哪些类别的网页，以及要注册哪些类别的外部数据库内容过滤和查看报告。
	定制	使用该界面以定制内容过滤器清单。
	缓存	使用该界面以查看和配置 ZyWALL 的 URL 缓存。
VPN	VPN 规则 (IKE)	使用该界面以配置使用 IKE 密钥管理的 VPN 连接，并查看规则摘要信息。
	VPN 规则 (手动)	使用该界面以配置使用手动密钥管理的 VPN 连接并查看规则摘要信息。
	SA 监控	使用该界面以显示和管理活动的 VPN 连接。
	通用设定	使用该界面以配置 IPSec 定时器设置。
证书	我的证书	使用该界面以查看证书的摘要列表并管理证书和凭证请求。
	可信的 CAs	使用该界面以查看和管理信任的凭证管理中心清单。
	可信的远程主机	使用该界面以查看和管理属于信任的远程主机的证书。
	目录服务器	使用该界面以查看和管理目录服务器的清单。
认证服务器	本地用户数据库	使用该界面以配置 ZyWALL 上的本地用户帐户。
	RADIUS	配置该界面以使用外部服务器以验证 VPN 用户。
高级		
NAT	NAT 概述	使用该界面以启用 NAT。
	地址映射	使用该界面以配置网络地址转换映射规则。
	端口转发	使用该界面以配置 ZyWALL 后的服务器。
	触发端口	使用该界面以更改您的 ZyWALL 的端口触发设置。
静态路由	静态路由	使用该界面以配置 IP 静态路由。
带宽管理	概要	使用该界面以启用接口上的带宽管理。
	类别设置	使用该界面以设置带宽类别。
	监控	使用该界面以查看 ZyWALL 的带宽用法和分配。
DNS	系统	使用该界面以配置地址和名称服务器记录。
	缓存	使用该界面以配置 DNS 解析缓存。
	DHCP	使用该界面以配置 ZyWALL 分配到 DHCP 客户端的 DNS 信息。
	DDNS	使用该界面以设置动态 DNS。

远程管理	WWW	使用该界面以配置通过哪些接口和从哪些 IP 地址中用户可以使用 HTTPS 或 HTTP 来管理 ZyWALL。
	SSH	使用该界面以配置通过哪些接口和从哪些 IP 地址,用于可以使用安全壳来管理 ZyWALL。
	TELNET	使用该界面以配置通过哪些接口和从哪些 IP 地址中用户可以使用 Telnet 来管理 ZyWALL。
	FTP	使用该界面以配置通过哪些接口和从哪些 IP 地址中用户可以使用 FTP 来接入 ZyWALL。
	SNMP	使用该界面以配置用于简单网络管理协议管理的 ZyWALL 设置。
	DNS	使用该界面以配置通过哪些接口和从哪些 IP 地址中用户可以将 DNS 查询发送到 ZyWALL。
	CNM	使用该界面以配置并允许您的 ZyWALL 被 Vantage CNM 服务器管理。
UPnP	UPnP	使用该界面以启用 ZyWALL 上的通用即插即用。
	端口 s	使用该界面以查看通用即插即用在 ZyWALL 上创建的 NAT 端口映射规则。
ALG	ALG	使用该界面以允许某些应用程序传输 ZyWALL。
日志	观察日志	使用该界面以查看您选择的类别日志。
	日志设置	使用该界面以更改您的 ZyWALL 的日志设置。
	Re 端口 s	使用该界面以拥有 ZyWALL 记录并显示网络使用报告。
设备维护	常规 I	该界面中包含有管理和系统相关信息。
	密码	您可在该界面中修改您登录系统的密码。
	时间与日期	您可在该界面中修改您系统的日期和时间。
	设备模式	您可以在该界面中配置 ZyWALL 是作为路由器还是作为网桥来使用。
	韧体上传	您可在该界面中上传 ZyWALL 的韧体。
	设置	您可在该界面中备份和恢复 ZyWALL 的设置参数。
	重新启动	在该界面中您无需开关电源即可重新启动 ZyWALL。
注销		点击该按钮可以退出 web 设置界面。

2.4.4 系统统计

在首页界面中点击显示 系统统计。这里会显示一些只读信息，包括端口状态和某些特定类型数据包的统计。这里还提供“运行时间”和“统计间隔”信息。您可以设置统计间隔区域。不是所有的区域在所有的设备上都有效。

图 9 主页：统计显示



以下为界面相关的描述。

表 6 主页：统计显示

标签	描述
端口	这些是 ZyWALL 的接口。
状态	对于 LAN 和 DMZ 端口，此处会显示端口速率和双工模式。 对于 WAN 和拨号备份端口，如果您使用以太网封装方式，这里显示端口的速率和双工模式；您如果采用 PPPoE 封装方式，您会见到以下各种状态：掉线（掉线），空闲（线路空闲），拨号（开始触发拨号）和 Drop（断开呼叫）。
发包数	这里会显示该端口发送数据包的数量。
收包数	这里会显示该端口接收数据包的数量。
冲突	
发包 B/s	这里会显示该端口每秒钟发送数据包的数量（byte）。
收包 B/s	这里会显示该端口每秒钟接收数据包的数量（byte）。
运行时间	这里会显示线路工作的总时间。
系统运行时间	这里会显示 ZyWALL 通电启动的总时间。
统计间隔	在这里输入刷新统计列表的更新时间。
设置间隔	点击这个按钮，您可以使用在统计间隔中设置的时间。

停止	点击停止可以停止刷新统计表。

2.4.5 DHCP 表单界面

DHCP(动态主机配置协议、RFC 2131 和 RFC 2132)允许计算机在启动时从服务器中获取 TCP/IP 配置（包括 IP 地址、子网掩码、网关和某些网络细细，例如 DNS 服务器的 IP 地址）。您可以将 ZyWALL 配置为 DHCP 服务器或禁用它。当配置为服务器时，ZyWALL 向客户端提供了 TCP/IP 配置。如果 ZyWALL 的 DHCP 服务被禁用，这您必须在局域网上有另一台 DHCP 服务器，否则计算机必须手动配置。

当 ZyWALL 设置为路由模式的时候，在首页画面中点击显示 DHCP 表单，您可以看到当前 DHCP 客户端信息（包括 IP 地址，主机名称和 MAC 地址），这些信息是只读的。

图 10 主页：DHCP 表单



以下为界面相关的描述。

表 7 主页：DHCP 表

标签	描述
接口	选择 LAN，DMZ 或 WLAN 可以显示相应端口当前 DHCP 客户端的信息。
#	这里显示主机的索引号。
IP 地址	这里显示主机的 IP 地址。
主机名称	这里显示主机名。
MAC 地址	这里显示以太网卡的 MAC 地址，它对于每台计算机都是唯一的。网卡的 MAC 地址均为出厂设定的，这个地址遵循工业标准，以确保不会有两个 MAC 地址相同的网卡。
保留	选择标题行中的复选框以自动选择所有复选框或选择每个条目中的复选框，令 ZyWALL 始终将所选项的 IP 地址分配到相应的 MAC 地址（和主机名）中。在

	您单击应用后，MAC 地址和 IP 地址还显示在 LAN 静态 DHCP 界面中（在此界面中可以编辑这些地址）。
更新	点击 Refresh 可以重新加载 DHCP 表。

2.4.6 VPN 状态

当 ZyWALL 设置为路由模式的时候，您可以在首页页面中点击 VPN 状态。一些只读的封装模式和安全协议的信息将会显示出来。您可以设置统计间隔区域。

图 11 主页：VPN 状态



以下为界面相关的描述。

表 8 主页：VPN 状态

标识	描述
#	此处显示安全关联的索引号。
名称	此处显示 VPN 策略的标识名字。
本地网络	该区域显示能够使用您的 ZyWALL 提供的 VPN IPSec 特征的计算机的 IP 地址。
远程网络	该区域显示处于远程 IPSec 路由器的远端网络中的计算机的 IP 地址（一定范围当中的）。
封装	此处显示隧道或传输模式。
IPSec 运算法则	此处显示安全关联采用的安全协议。 AH 和 ESP 均会提高 ZyWALL 的处理需求和通信时延。

统计间隔	在这里输入刷新统计列表的时间间隔。
设置间隔	点击这个按钮可以使用您在统计间隔中设置的时间。
停止	点击停止可以停止刷新统计表。

第 3 章 向导设置

本章将会向您介绍 **Wizard** 设置界面。本章只有您在将 **ZyWALL** 设置为路由模式的时候才会有效。

3.1 向导设置概述

web 配置程序的设置向导帮助您配置广域网端口访问互联网，编辑 VPN 策略，并配置 IKE 设置以建立 VPN 隧道。

3.2 Internet 接入

第一次进入 **Internet** 连接向导界面时根据您采用的封装方式不同会有 3 种变化。请您根据 ISP 提供的信息在每个区域中输入相应内容。如果您不知道这些信息，您可以将这些栏目留空。

3.2.1 ISP 参数

ZyWALL 可以提供三种封装模式的选择。它们是 **Ethernet**、**PPTP** 或 **PPPoE**。

3.2.1.1 Ethernet

如果某些 ISP 通过 **UDP heartbeat** 数据包来确认用户是否一直在线，请您为这些封包创建一条 **WAN-to-WAN/ZyWALL** 的防火墙规则。您可联系 ISP 得到正确的端口号。

当 WAN 端口连接一个正常的以太网络的时候，请选择 **Ethernet**。

图 12 ISP 参数：以太网封装

向导 — 使用互联网

互联网接入ISP参数

您可以依据您所在的网络来选择以太网、PPPoE 或 PPTP。如果您不知道，请咨询您的网络管理员。最常使用的网络类型是以太网。

封装

Ethernet

WAN IP地址分配

IP地址设置

使用固定IP地址

我的WAN IP地址

0 . 0 . 0 . 0

我的WAN IP子网掩码

0 . 0 . 0 . 0

网关 IP 地址

0 . 0 . 0 . 0

第一 DNS 服务器

0 . 0 . 0 . 0

第二 DNS 服务器

0 . 0 . 0 . 0

应用

以下为界面相关的描述。

表 9 ISP 参数：以太网封装

标识	描述
互联网接入 ISP 参数	
封装	当 WAN 口连接以太网的时候，您需要选择 Ethernet 选项。否则，请选择 PPPoE 或 PPTP 来创建拨号连接。
WAN IP 地址分配	
IP 地址设置	如果您的 ISP 没有给您提供固定的 IP 地址，请选择自动从 ISP 取得。这是缺省选项。 如果 ISP 给您分配了固定的 IP 地址，请选择静态。 只有在您选择静态的时候，以下区域才会有效。
我的 WAN IP 地址	输入您的 WAN 口 IP 地址。
我的 WAN IP 子网掩码	当 WAN 口连接以太网的时候，您需要选择 Ethernet 选项。否则，请选择 PPPoE 或 PPTP 来创建拨号连接。
网关 IP 地址	输入 IP 子网掩码。
第一 DNS 服务器 第二 DNS 服务器	输入网关的 IP 地址。

应用	在右边区域输入 DNS 服务器的 IP 地址。如果您不想配置 DNS 服务器，请留空此处。如果您没有配置 DNS 服务器的 IP 地址，您需要确切知道您想访问的机器的 IP 地址。

3.2.1.2 PPPoE 封装

以太网点对点协议(PPPoE)用作拨号连接。PPPoE 是互联网工程任务组（IETF）标准，指定个人计算机如何与宽带调制解调器（例如 DSL、有线、无线等）交互以获得对高速数据网络的接入。

图 13 ISP 参数：PPPoE 封装

向导 — 使用互联网

互联网接入ISP参数

您可以依据您所在的网络来选择以太网、PPPoE 或 PPTP。如果您不知道，请咨询您的网络管理员。最常使用的网络类型是以太网。

封装

PPP over Ethernet

服务名称

(选项)

用户名

密码

再输入一次以便确认

☐ 固定联机

闲置超时

100

(秒)

WAN IP地址分配

IP地址设置

使用固定IP地址

第一 DNS 服务器

0 . 0 . 0 . 0

第二 DNS 服务器

0 . 0 . 0 . 0

应用

以下为界面相关的描述。

表 10 ISP 参数：PPPoE 封装

标签	描述
互联网接入 ISP 参数	
封装	在下拉菜单中选择封装方式。采用 PPP over Ethernet 建立一个拨号连接。
服务名称	输入服务提供者的名称。

用户名	输入 ISP 提供的用户名。
密码	输入密码。
再输入一次以便确认	重新输入一次密码。
固定联机	选择固定联机可以使您永远在线。
闲置逾时	输入一个以秒为单位的时间值，网络无流量情况超过这个时间值的时候，ZyWALL 会自动与 PPPoE 服务器断开连接。默认值为 100 秒。
WAN IP 地址 分配	
IP 地址设置	如果您的 ISP 未分配固定的 IP 地址，则选择自动从 ISP 取得。这是默认的选项。 如果 ISP 分配了固定的 IP 地址，则选择静态。 只有选择静态时，才可以使用以下字段。
我的 WAN IP 地址	输入您的 WAN IP 地址下面的区域中。
第一 DNS 服务器	在右侧字段中输入 DNS 服务器的 IP 地址。
第二 DNS 服务器	如果您不想要配置 DNS 服务器，将该字段保留为 0.0.0.0。如果不配置 DNS 服务器，则必须知道机器的 IP 地址以访问它。
应用	单击应用以保存更改并转到下一个界面。

3.2.1.3 PPTP 封装

PPTP（点到点通道协议）是一种网络协议，它允许从一个远程客户端向一台私有服务器发送数据。它可以在基于 TCP/IP 的网络上创建一条虚拟私有网络（VPN）的连接。PPTP 支持按需，多协议和在公网（Internet）上创建虚拟的私有网络等多种特征。

注意：ZyWALL 同时仅支持一条 PPTP 服务器的连接。

图 14 ISP 参数：PPTP 封装

向导 — 使用互联网

互联网接入ISP参数

您可以依据您所在的网络来选择以太网、PPPoE 或 PPTP。如果您不知道，请咨询您的网络管理员。最常使用的网络类型是以太网。

封装

PPTP

用户名

密码

再输入一次以便确认

☐ 固定联机

闲置超时

100

(秒)

PPTP 设置

我的 IP地址

0 . 0 . 0 . 0

我的 IP子网掩码

0 . 0 . 0 . 0

服务器 IP地址

0 . 0 . 0 . 0

联机 ID/名称

WAN IP地址分配

IP地址设置

自动从ISP取得

应用

以下为界面相关的描述。

表 11 ISP 参数：PPTP 封装

标签	描述
互联网接入 ISP 参数	
封装	在下拉菜单中选择 PPTP 封装。
用户名	输入 ISP 提供的用户名。
密码	输入密码。
再输入一次以便确认	重新输入一次密码。
固定联机	选择固定联机可以使您永远在线。
闲置超时	输入一个以秒为单位的时间值，网络无流量情况超过这个时间值的时候，ZyWALL 会自动与 PPTP 服务器断开连接。
PPTP 设置	

我的 IP 地址	输入由 ISP 分配的静态 IP 地址。
我的 IP 子网掩码	输入子网掩码。
服务器 IP 地址	输入 PPTP 服务器的 IP 地址。
联机 ID/名称	输入连接 ID 或连接名称。格式要符合“c:id”和“n:名称”。例如，C:12 或 N:我的 ISP。 根据您的 Xdsl 模式的要求，此项为可选项。
WAN IP 地址分配	如果您的 ISP 没有给您提供固定的 IP 地址，请选择自动从 ISP 取得。这是缺省选项。 如果 ISP 给您分配了固定的 IP 地址，请选择静态。
IP 地址设置	点击应用保存您的修改，进入下一个界面。
我的 WAN IP 地址	输入由 ISP 分配的静态 IP 地址。
第一 DNS 服务器 第二 DNS 服务器	输入子网掩码。
应用	输入 PPTP 服务器的 IP 地址。

3.2.2 互联网接入向导：第二个界面

单击下一步以转到您可以注册 ZyWALL 的界面并激活免费内容过滤试用应用程序。否则，单击跳过以显示恭喜界面并单击关闭以完成互联网接入设置。

图 15 互联网接入向导：第二个界面



图 16 互联网接入设置完成

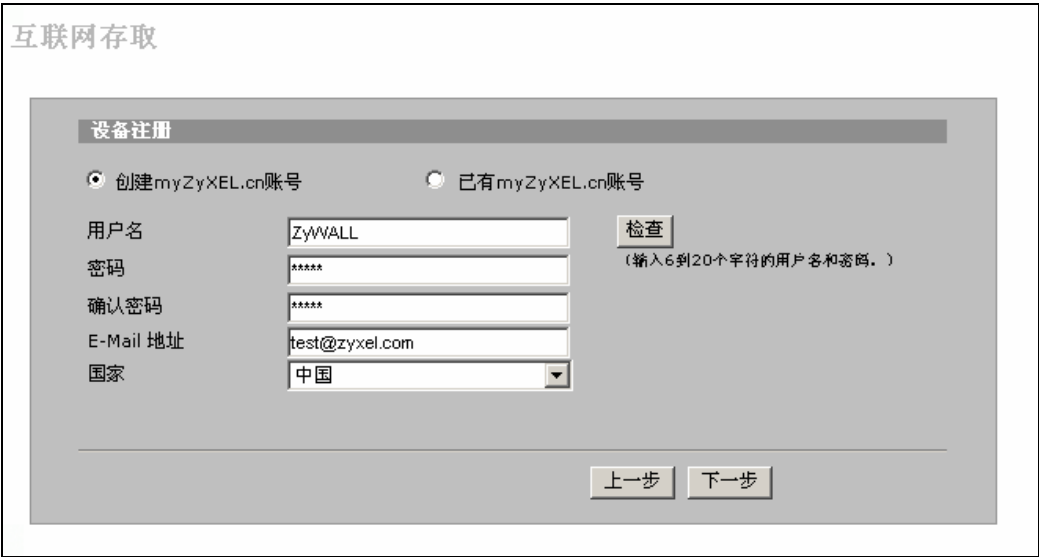


3.2.3 Internet 访问配置向导：注册

如果您在上以界面（参见图 15）中点击下一步，会出现以下界面。

注意：如果您想利用您的 iCard 的 PIN 码（许可证密码）激活一个标准的服务，可以使用注册服务界面。

图 17 Internet 访问配置向导：注册



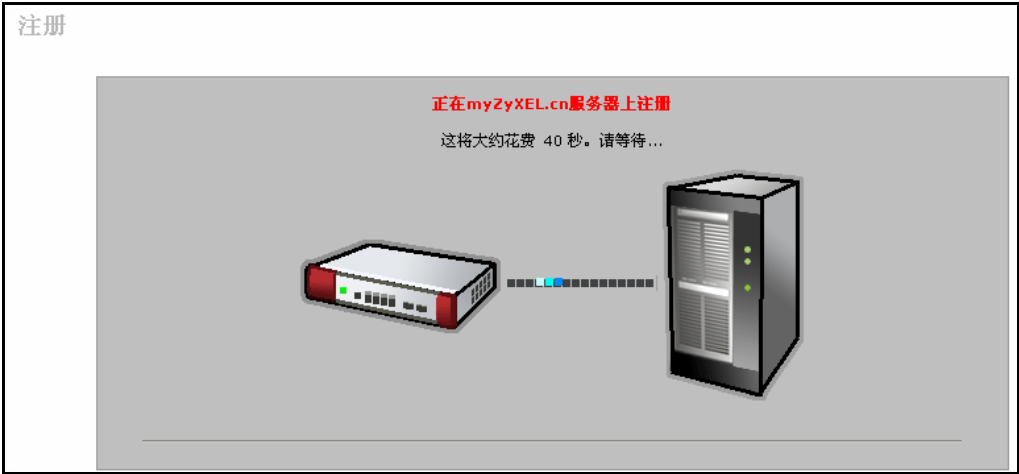
以下为界面相关的描述。

表 12 互联网接入向导：注册

标签	描述
设备注册	如果您选择已有 myZyXEL.com 帐号，只有用户名和密码区域有效。
创建 myZyXEL.com 帐号	如果您还没有在 myZyXEL.com 中创建一个账号，请选择该项，配置以下区域来创建一个账号，注册您的 ZyWALL。
已有 myZyXEL.com 帐号	如果您已经在 myZyXEL.com 中拥有了一个账号，请选择该项，然后输入您的用户名和密码来注册您的 ZyWALL。
用户名	输入您在 myZyXEL.com 中注册的用户名。用户名需要为 6 到 20 位的包括数字和字母的字符（包括下划线）。不允许使用空格。
检查	点击该按钮可以在 myZyXEL.com 的数据库中查询确认您的用户名是否已经被使用过了。
密码	输入一个 6 到 20 位的包括数字和字母的密码（包括下划线）。不允许使用空格。
确认密码	再次输入一遍密码以确认。
E-Mail 地址	输入您的 e-mail 地址。
国家	从下拉菜单中选择您所处的国家。
上一步	点击上一步可以回到前面的界面。
下一步	点击下一步可以继续。

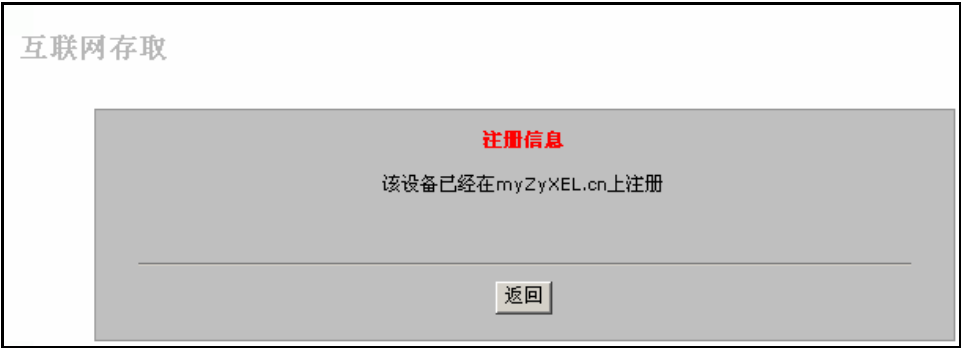
如果您在以上各区域输入完相关内容，然后点击下一步，可以见到以下的注册过程界面。
请等待一段时间，直到注册完成。

图 18 Internet 访问配置向导：注册过程



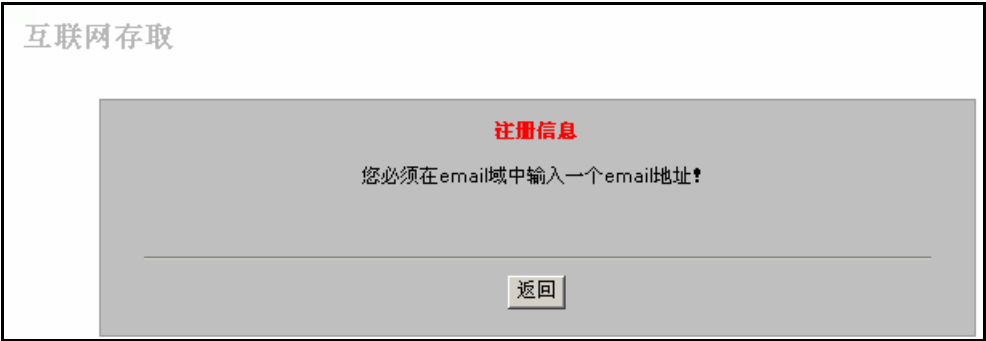
如果您在以上各区域输入完相关内容，然后点击下一步，可以见到以下的注册过程界面。
请等待一段时间，直到注册完成。

图 19 Internet 访问配置向导：状态



如果注册没有成功，您会见到以下界面。点击 **Return**，回到设备注册界面，您可以重新检查相关的设置参数。

图 20 Internet 访问配置向导：注册失败



如果 ZyWALL 已经注册成功，设备 注册界面只会显示只读信息。如果继续点击下一步，您会在服务激活界面中见到有哪些应用已经激活了。

图 21 Internet 访问配置向导：设备已注册

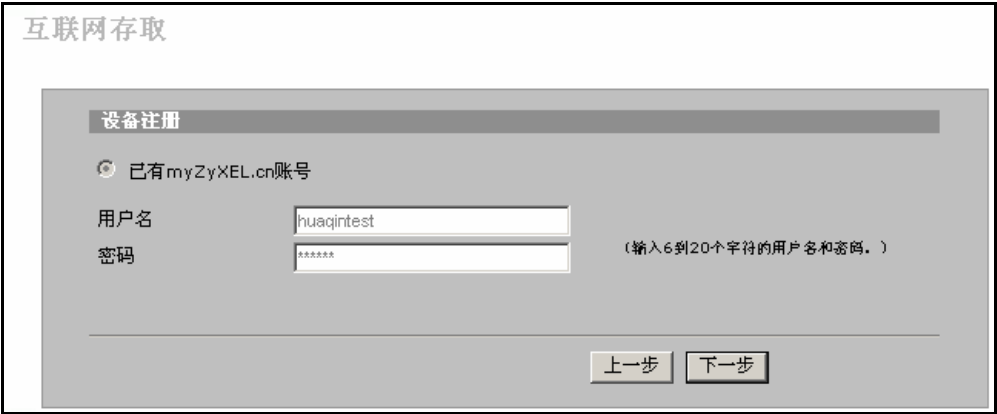
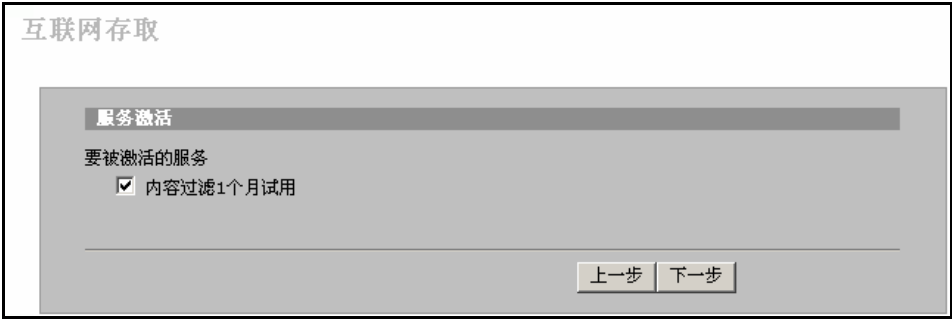


图 22 互联网接入向导：激活服务



3.3 VPN 向导网关设置

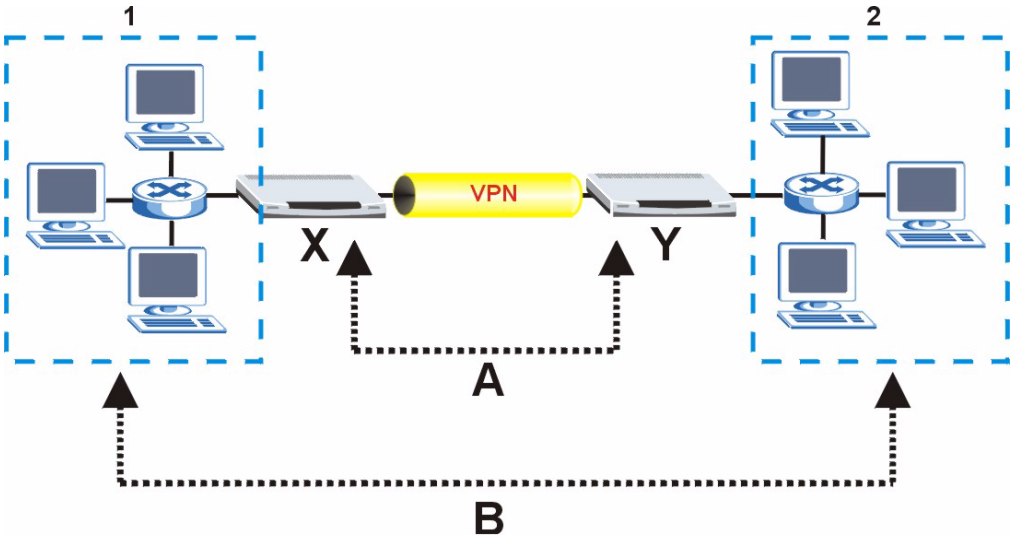
虚拟专用网络（VPN）隧道给出了与另一台计算机或网络的安全连接。

网关策略标识了 VPN 隧道任一端的 IPSec 路由器。

网络策略指定了哪些设备（在 IPSec 路由器后）可以使用 VPN 隧道。

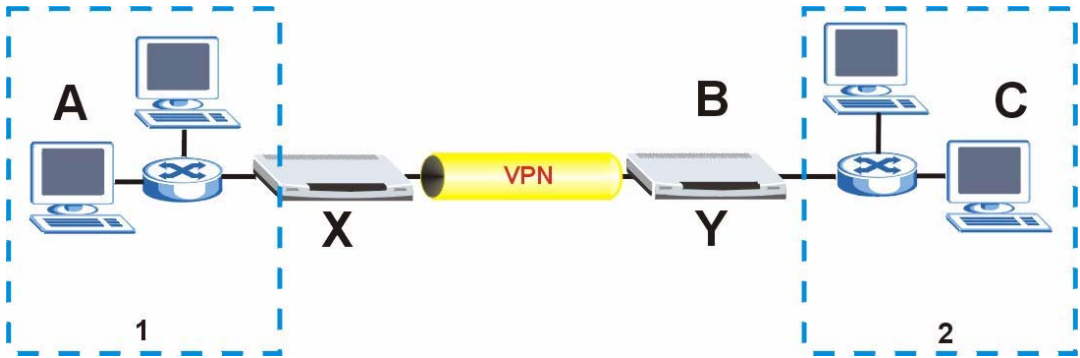
在下图中，X 是您的 ZyWALL，Y 是远程 IPSec 路由器，A 箭头表示网关策略，而 B 箭头表示网络策略。本地网络标为 1，而远程网络标为 2。

图 23 网关和网络策略



该图帮助解释向导界面中的主要字段。在该图中，X 是您的 ZyWALL，Y 是远程 IPSec 路由器，A 表示本地网络 IP 地址，B 表示远程网关地址，而 C 表示远程网络地址。本地网络标为 1，而远程网络标为 2。

图 24 IPSec 字段摘要



使用 VPN 向导界面来配置使用预先共享的密钥的 VPN 规则。如果您要设置使用证书的规则，请转到配置用的 VPN 界面。

单击首页界面中的 VPN Wizard 以打开 VPN 配置向导。第一个屏幕如下所示。

注：当您单击上一步时，您的设置不会被保存。

图 25 VPN 向导：网关设置

向导 — VPN

网关策略内容

名称

网关策略设置

我的ZyWALL

远程网关地址

下一步

下表描述了此界面中的标签。

表 13 VPN 向导：网关设置

标签	描述
网关策略内容	
名称	键入最多 32 个字符以标识此 VPN 网关策略。您可以使用任何字符，包括空格，但是 ZyWALL 丢弃尾部的空格。

我的 ZyWALL	当 ZyWALL 处于路由器模式时，输入 ZyWALL 的广域网 IP 地址或域名或将字段保留设置为 0.0.0.0。 如果您将该字段设置为 0.0.0.0，ZyWALL 在设置 VPN 隧道时使用其当前的广域网 IP 地址（静态或动态）。如果广域网连接断开，当使用拨号备用时 ZyWALL 使用 VPN 隧道的备用拨号 IP 地址，当使用流量重定向时使用局域网 IP 地址。 如果该 IP 地址更改，则 VPN 隧道必须构建。 当 ZyWALL 处于网桥模式时，该字段为只读且显示 ZyWALL 的 IP 地址。
远程网关地址	在以下字段中输入广域网 IP 地址或远程 IPSec 路由器（安全网关）的域名，用以通过其 IP 地址或域名来标识远程 IPSec 路由器。如果远程 IPSec 路由器具有动态广域网 IP 地址，则将此字段设置为 0.0.0.0。
下一步	单击下一步以继续。

3.4 VPN 向导网络设置

两条激活的 SA 不能同时拥有相同的本地和远端 IP 地址。两条激活的 SA 可以有相同的本地和远端 IP 地址，但是不能同时使用。您可以配置具有相同本地和远端 IP 地址的多条 SA，但是只能同时激活一条。

图 26 VPN 向导：网络设置

向导 — VPN

网络策略内容

☒ 启用

名称

Test

网络设置

本地网络

☐ 单一IP地址 ☐ 指定IP 段 ☒ IP子网

IP 地址区段起点

192 , 168 , 1 , 0

IP 地址区段终点 / 子网掩码

255 , 255 , 255 , 0

远程网络

☐ 单一IP地址 ☐ 指定IP 段 ☒ IP子网

IP 地址区段起点

10 , 0 , 0 , 0

IP 地址区段终点 / 子网掩码

255 , 0 , 0 , 0

上一步

下一步

以下为界面相关的描述。

35

表 14 VPN 向导：网络设置

标签	描述
网络策略内容	
启用	如果启用复选框被选中，则隧道的数据包触发 ZyWALL 来构建隧道。 清除启用复选框以关闭网络策略。ZyWALL 不会应用策略。隧道的数据包不会触发隧道。
名称	输入一串最多 32 位的字符来标识该 VPN 网关策略。您可以使用任何字符，包括空格，但是 ZyWALL 会不计末尾空格。
网络设置	
本地网络	本地网络 IP 地址必须是固定的而且必须与远端网关设定的远端网络 IP 地址是一致的。 选择单一 IP 地址，可以填入单一的 IP 地址，选择指定 IP 段可以指定一段 IP 地址，选择 IP 子网可以指定一个子网段。
IP 地址区段起点	当本地网络处设置为单一 IP 地址时，这里是您的 ZyWALL 后面局域网内的一个固定 IP 地址。当本地网络处设置为指定 IP 段时，这里是您的 ZyWALL 后面局域网一个范围内的起始 IP 地址。当本地网络处设置为 IP 子网时，这里是您的 ZyWALL 后面局域网内的一个固定 IP 地址。
IP 地址区段终点/ 子网掩码	当本地网络处设置为单一 IP 地址时，此处为 N/A。当本地网络处设置为指定 IP 段时，这里是您的 ZyWALL 后面局域网一个范围内的末尾 IP 地址。当本地网络处设置为 IP 子网时，这里是您的 ZyWALL 后面局域网的子网掩码。
远程网络	远端 IP 地址必须是固定的而且必须与远端网关设定的本地网络 IP 地址 是一致的。选择单一 IP 地址指定单一 IP 地址，选择指定 IP 段指定一段 IP 地址，选择 IP 子网指定一个子网段。
Starting IP 地址	当 远程 网络设置为单一 IP 地址时，这里是远端的 ZyWALL 后面局域网内的一个固定 IP。当远程 网络设置为指定 IP 段时，这里是远端的 ZyWALL 后面局域网一个范围内的起始 IP 地址。当远程网络设置为 IP 子网时，这里是远端的 ZyWALL 后面局域网内的一个固定 IP 地址。
Ending IP 地址/ 子网掩码	当远程 网络设置为单一 IP 地址时，此处为 N/A。当远程 网络设置为指定 IP 段时，这里是远端的 ZyWALL 后面局域网一个范围内的末尾 IP 地址。当远程 网络设置为 IP 子网时，这里是远端的 ZyWALL 后面局域网的子网掩码。
上一步	点击上一步回到上一界面。

下一步	点击下一步继续进行设置。

3.5 VPN 向导 IKE 隧道设置 (IKE 阶段 1)

图 27 VPN 向导：IKE 隧道设置



以下为界面相关的描述。

表 15 VPN 向导：IKE 隧道设置

标签	描述
协商模式	您可在此点选主模式或主动模式。主模式对身份保持方面起到了重要的作用（您的身份在协商过程中不被泄露）。主动模式在协商速度上面要快一些，但是付出的代价是较快的速度限制了它的协商能力且不能提供身份保护。注意：通过同一个安全网关建立的多条 SA（安全关联）必须具有相同的协商模式。
加密算法	当 DES 用于数据通信时，无论是发送者还是接收者都必须知道同一个密钥，该密钥要用来对信息进行加密、解密或产生和校验信息的验证码。DES 加密算法使用 56 位的密钥。三倍 DES（3DES）是在 DES 基础上的一种改进，它使用 168 位密码。这样 3DES 比 DES 更加安全。但同时它也要求有更高的处理能力，结果是造成了轻微的延迟和吞吐量的降低。AES 采用 128 位加密，速率要优于 3DES。

认证算法	MD5（信息摘要 5）和 SHA1（安全哈希算法）都是用来对数据包做认证的哈希算法。SHA1 算法比 MD5 算法更安全，但相应的速度有所降低。
密钥群组	您需要为阶段 1 阶段的 IKE 设置提供一个密钥组。DH1（缺省）是指一个 768 位随机数的 Diffie-Hellman 组 1。DH2 是指一个 1024 位随机数的 Diffie-Hellman 组 2。
SA 生命周期(秒)	在该栏目中可定义 IKE 安全关联在自动重新协商前存在的时间长度。最小值为 180 秒。 一个较短的 SA 生存时间可以通过更换加密和验证密钥的方法来增强 SA 的安全性，然而每次 VPN 隧道重新协商建立时，所有访问远端资源的用户都会临时被断掉。
预分配密钥	您在此处输入预共享密钥。预共享密钥在阶段 1 的 IKE 协商中用于标识通信双方。它之所以被称为“预共享密钥”是因为您在 与其它方通过安全连接进行通信之前首先要共享此密钥。 您可输入一个 8 到 31 位的 ASCII 字符（区分大小写）或 16 到 62 个 十六进制字符（“0-9”，“A-F”）。 您需要在十六进制字符前输入“0x” （零 x）的前缀，它们不包括在 16 到 62 位的密钥之内。例如，在“0x0123456789ABCDEF”中“0x”代表这是十六进制的密钥，
上一步	点击上一步返回上一界面。
下一步	点击下一步继续进行设置。

3.6 VPN 向导 IPsec 隧道设置（IKE 阶段 2）

图 28 VPN 向导：IPsec 设置



以下为界面相关的描述。

表 16 VPN 向导:IPSec 设置

标签	描述
封装模式	选择隧道模式或传输模式。隧道模式封装了整个 IP 数据包来进行安全传输。网关服务往往需要隧道模式来提供内部系统的接入。隧道模式是一种包括认证和加密的基本的 IP 隧道。这是最普通的工作模式，在网关到网关和主机到网关的通信中经常会用到。传输模式用于保护上层协议安全性的，只作用于 IP 数据包中的数据。在此模式中，安全协议（AH 或 ESP）位于 IP 数据包中的原始 IP 包头和其它项后面，而在高层协议（如 TCP 和 UDP）的前面。
IPSec 协议	选择一个建立 SA 的安全协议。 AH 和 ESP 都会增加 ZyWALL 的处理负荷，造成通信上的微小时延。
加密算法	当 DES 用于数据通信时，无论是发送者还是接收者都必须知道同一个密钥，该密钥要用来对信息进行加密、解密或产生和校验信息的验证码。DES 加密算法使用 56 位的密钥。三倍 DES 样 3DES 比 DES 更加安全。但同时它也要求有更高的处理能力，结果是造成了轻微的延迟和吞吐量的降低。AES 采用 128 位加密，速率要优于 3DES。
认证算法	MD5（信息摘要 5）和 SHA1（安全哈斯算法）都是用来对数据包做认证的哈斯算法。SHA1 算法比 MD5 算法更安全，但相应的速度有所降低。

SA 生命周期(秒)	在该栏目中可定义 IKE 安全关联在自动重新协商前存在的时间 长度。最小值为 180 秒。 一个较短的 SA 生存时间可以通过更换加密和验证密钥的方法 来增强 SA 的安全性，然而每次 VPN 隧道重新协商建立时，所 有访问远端资源的用户都会临时被断掉。
Perfect Forward Secret (PFS)	完美向前保密(PFS)在 阶段 2 阶段 IPSec SA 设置中被设置为无(缺省)。这提供了更快速的 IPSec 建立，而不是最安全的。 用空格键选择 DH1 或 DH2 以应用 PFS。DH1 是指 Diffie-Hellman 组 1，有 768 位的随机数。DH2 是指 Diffie-Hellman 组 2，有 1024 位的随机数（更安全，但会较慢）。
上一步	点击上一步返回上一界面。
下一步	点击下一步继续进行设置。

3.7 VPN 向导状态汇总

这个界面将以只读信息显示当前 VPN 的设置状态。您可在该使用该汇总表格来检查您的设置是否正确。

图 29 VPN 向导：VPN 状态



以下为界面相关的描述。

表 17 VPN 向导：VPN 状态

标识	描述
网关策略内容	
名称	这是该 VPN 网关策略的名称。
网关策略设置	
我的 ZyWALL	这是路由模式下 ZyWALL 的 WAN 口 IP 地址或域名，或者网桥模式下 ZyWALL 的 IP 地址。
远程网关地址	这是用于标识远端 IPSec 路由器的 IP 地址或域名。
网络策略内容	
启用	可以显示该 VPN 网络策略是否已经激活。
名称	这是该 VPN 网络策略的名称。
网络策略设置	
本地网络	
IP 地址段起点	这是 ZyWALL 后面本地网络的起始 IP 地址（固定地址）。

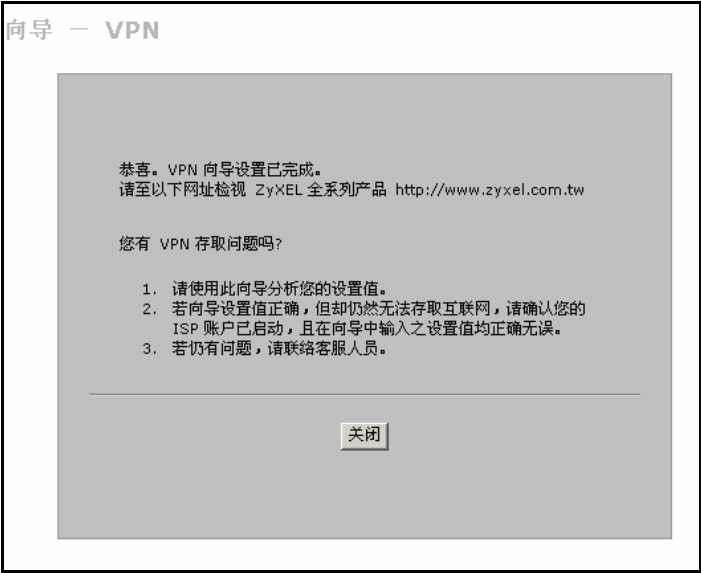
IP 地址段终点/子网掩码	当本地网络设置为单一 IP 地址的时候这一栏目显示为 N/A。当本地网络设置为一段 IP 地址的时候，这里显示末尾的 IP 地址。 当本地网络设置为一段子网的时候，这里显示子网掩码。
远程网络	
IP 地址段起点	这是远端 IPSec 路由器后面内部网络的起始 IP 地址（固定地址）。
IP 地址段终点/IP 子网 Mask	当远端网络设置为单一 IP 地址的时候这一栏目显示为 N/A。当远端网络设置为一段 IP 地址的时候，这里显示末尾 IP 地址。当远端网络设置为一段子网的时候，这里显示子网掩码。
IKE 通道设置 (IKE 阶段 1)	
协商模式	这里显示主模式或主动模式。和一个安全网关建立的多条 SA 必须具有相同的协商方式。
加密算法	这是数据的加密方法。选项有 DES, 3DES 和 AES 三种。
认证算法	MD5（信息摘要 5）和 SHA1（安全哈希算法）是用于对数据包做认证的哈希算法。
密钥群组	这是在阶段 1 阶段 IKE 设置中采用的密钥组。
SA 生命周期 (秒)	这里是一个 IKE SA 重新协商建立之前的存活时间。
预分配密钥	这是一个用于在阶段 1 阶段 IKE 协商中对通信双方做认证的预共享密钥。
IPSec 设置 (IKE 阶段 2)	
封装模式	这里显示隧道模式或传输模式。
IPSec 协议	ESP 或 AH 都是用于建立 SA 的安全协议。
加密算法	这里是数据加密的方法。选项有 DES, 3DES, AES 或 NULL。
认证算法	MD5（信息摘要 5）和 SHA1（安全哈希算法）都是用于对数据包做认证的哈希算法。
SA 生命周期 (秒)	这里是一个 IKE SA 自动重新协商建立之前的存活时间。
完全保密 (PFS)	完美向前加密 (PFS) 在阶段 2 阶段 IPSec SA 设置中缺省是禁用的 (None)。除非选择 DH1 或 DH2, 该功能才可以启用。

上一步	点击上一步返回上一界面。
完成	点击完成，完成并保存设置。

3.8 VPN 向导设置完成

恭喜您！您已经成功完成了 ZyWALL 的 VPN 规则设置。

图 30 VPN 向导设置完成



第 4 章 注册

4.1 myZyXEL.com 概览

myZyXEL.com 是 ZyXEL 的在线服务中心。您可以在这里注册您的 ZyWALL，管理 ZyWALL 支持的多种服务。

注意：您在注册您的设备之前需要创建一个账号，并在 myZyXEL.com 上激活相关的服务。

您可以直接创建一个 myZyXEL.com 账号，注册您的 ZyWALL，使用注册界面激活一个服务。要不然，您可以到 <http://www.myZyXEL.com> 上，利用 ZyWALL 的序列号和 LAN 口 MAC 地址进行注册。您可以参考 web 站点的在线帮助寻求详细信息。

注意：如果想要激活一台 ZyWALL 的服务，您需要通过该 ZyWALL 来访问 myZyXEL.com。

4.1.1 内容过滤订购服务

ZyWALL 可以使用内容过滤订购服务。内容过滤允许或阻止访问网站。订购基于类别的内容过滤阻止访问基于内容的网站类别。您的 ZyWALL 访问具有数百万按照类别分类的数百万外部数据库。您可以用 ZyWALL 阻止、阻止和/或根据这些类别访问网站。有关更多信息，请参见有关内容过滤的章节。

4.2 注册

若要用 myXEL.com 注册 ZyWALL 并激活内容过滤服务，请单击导航面板中的注册以打开以下显示的界面。

图 31 注册

注册

注册

服务

设备注册

☒ 创建myZyXEL.cn账号

☐ 已有myZyXEL.cn账号

用户名

密码

确认密码

E-Mail 地址

国家

检查

(输入6到20个字符的用户名和密码。)

服务激活

☐ 内容过滤1个月试用

注意：关于更多的服务管理，请点击[myZyXEL.cn](#)

应用

重置

以下为界面相关的描述。

表 18 注册

标识	描述
设备注册	如果您选择已有 myZyXEL.com 帐号，只有用户名称和密码区域有效。
创建 myZyXEL.com 帐号	如果您还没有在 myZyXEL.com 中创建一个账号，请选择该项，配置以下区域来创建一个账号，注册您的 ZyWALL。
已有 myZyXEL.com 帐号	如果您已经在 myZyXEL.com 中拥有了一个账号，请选择该项，然后输入您的用户名和密码来注册您的 ZyWALL。
用户名	输入您在 myZyXEL.com 中注册的用户名。用户名需要为 6 到 20 位的包括数字和字母的字符（包括下划线）。不允许使用空格。
检查	点击该按钮可以在 myZyXEL.com 的数据库中查询确认您的用户名是否已经被使用过了。
密码	输入一个 6 到 20 位的包括数字和字母的密码（包括下划线）。不允许使用空格。
确认密码	再次输入一遍密码以确认。
E-Mail 地址	输入您的 e-mail 地址。
国家	从下拉菜单中选择您所处的国家。
服务激活	您可以试用以下的这些服务。当试用期结束以后，您可以购买一个 iCard，然后在注册 服务界面中输入许可证密码以便能够延长该服务的使用期。

内容过滤 1 个月试用 I	勾选该选框可以激活内容过滤的试用服务。试用期从您激活该项功能当天开始的一个月之内有效。
应用	点击应用可以保存设置，并退回主界面。
重置	点击重置可以重新开始设置该界面。

注意：如果 ZyWALL 已经注册完了，该界面只会显示只读信息，说明试用服务是否已经激活。
您可以在服务界面中更新您的服务状态。

图 32 注册：已注册设备



4.3 服务

当激活了一项试用服务以后，您也可以使用服务界面来进行注册，输入您的 iCard 的 PIN 码（许可证密码）。依次点击 注册，服务 来打开下面的界面。注意：如果您在注册以后将 ZyWALL 恢复到出厂缺省配置，或者加载了一个不同的配置文件，请点击更新服务注册信息按钮来更新注册信息。

图 33 注册：服务



以下为界面相关的描述。

表 19 服务

标签	描述
服务管理	
服务	该区域显示 ZyWALL 上的有效服务名称。
状态	该区域显示服务是否已经激活。
注册类型	该区域显示该项应用是试用(Trial)，还是已经利用您的 iCard 的 PIN 码注册了该项服务（标准）。
失效日期	这里显示到期日期。
注册升级	
注册码	输入您的 iCard 的 PIN 码，然后点击升级来激活或者延长 使用一个标准的服务。 如果一个标准的服务已经过期，您需要购买一个新的 iCard，然后输入新的 PIN 码来延长服务期。
更新服务注册日期	点击该按钮来更新服务注册信息。

第 5 章 局域网界面

本章说明了如何配置局域网设置。本章仅适用于当 ZyWALL 处于路由器模式时。

5.1 LAN、WAN 和 ZyWALL

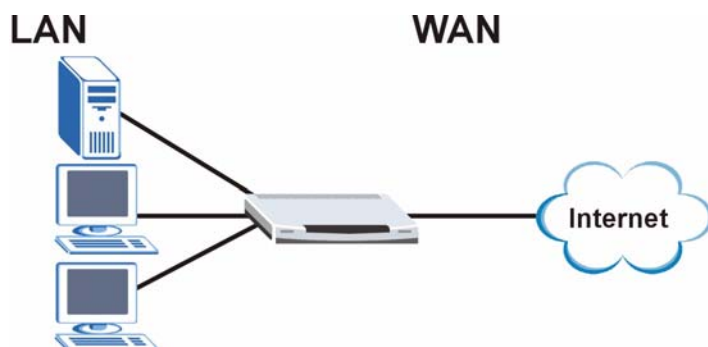
网络是连接有许多计算机的共享通讯系统。

本地局域网（LAN）包含您家中或办公室里连接到 ZyWALL 上 LAN 端口的计算机和网络设备。

广域网（WAN）是您连接到 ZyWALL LAN 端口另一种网络（多数为 Internet）。有关如何使用 WAN 界面设置您的 WAN 连接的信息，请参见第 7 章。

LAN 和 WAN 是两个独立的网络。ZyWALL 对这两者之间的流量进行控制。下图为一示例。

图 34 LAN 和 WAN



5.2 IP 地址和子网掩码

类似于街道中的房屋共享一个公共的街道名，局域网中的计算机也共享一个公共的网络号。

获取网络号的位置取决于特定的情况。如果 ISP 或您的网络管理员向您分配了一组注册的 IP 地址，则按照说明选择 IP 地址和子网掩码。

如果 ISP 没有明确向您给出 IP 网络号，则最可能您具有一个单一的用户帐户，且当连接建立时 ISP 将向您分配动态的 IP 地址。如果是这种情况，则建议您选择从 192.168.0.0 到 192.168.255.0 的网络号，且必须启用 ZyWALL 的网络地址转换 (NAT) 功能。互联网编号分配机构(IANA)保留这组专用地址；请不要使用任何其他号码，除非您被告知采用其他号码。如果

您选择 192.168.1.0 用作网络号；它包含 254 个单个地址，从 192.168.1.1 到 192.168.1.254（零和 255 保留）。也就是说，前面的三个数字指定网络号，而后面的数字标识网络上的单个计算机。

一旦您已经决定了网络号，则为您的 ZyWALL 选择一个易于记忆的 IP 地址，例如 192.168.1.1，但是要确保网络上没有其他设备正使用该 IP 地址。

子网掩码指定了 IP 地址的网络号部分。您的 ZyWALL 将自动根据您输入的 IP 地址来计算子网掩码。您不必通过 ZyWALL 来更改计算的子网掩码，除非您被指示要这样做。

5.2.1 专用 IP 地址

Internet 上的每台机器必须具有一个唯一的地址。如果您的网络与互联网隔离，例如只有两个分公司办公室，则您可以将任何 IP 地址分配给主机，不会出现任何问题。然而，国际因特网地址分配委员会（IANA）已将下列三个 IP 地址区段特别保留给私有网络使用：

- 10.0.0.0 — 10.255.255.255
- 172.16.0.0 — 172.31.255.255
- 192.168.0.0 — 192.168.255.255

您的 IP 地址可以从 IANA 或 ISP 获得，或者也可由私有网络分配给您。如果您属于一个小型组织，并且通过 ISP 访问互联网的，则 ISP 会向您提供互联网地址供您的局域网使用。另一方面，如果您是某个大型组织的一部分，则应询问您的网络管理员，以获得合适的 IP 地址。

注意：无论您属于哪种情况，请勿随意创建 IP 地址；请务必遵循上述准则。有关地址分配的详细信息，请参考 RFC 1597（私有网络地址分配）以及 RFC 1466（IP 地址空间管理准则）。

5.3 DHCP

ZyWALL 可以使用 DHCP（动态主机配置协议、RFC 2131 和 RFC 2132）来自动将 IP 地址子网掩码、网关和某些网络信息（例如 DNS 服务器的 IP 地址）分配到局域网中的计算机。您还可以从另一台 DHCP 服务器中选择用 ZyWALL 中继 DHCP 信息。如果您禁用 ZyWALL 的 DHCP 服务，则您必须将另一台 DHCP 服务器装在您的局域网上，否则计算机必须手动配置。

5.3.1 IP 池设置

ZyWALL 已为您的局域网上的计算机 IP 地址预置了一个 IP 池。有关缺省 IP 池范围，请参见附录 A。请不要将您局域网上计算机的静态 IP 地址指定为 DHCP 池中地址。

5.4 RIP 设置

RIP（路由信息协议、RFC 1058 和 RFC 1389）允许路由器与其他路由器交换路由信息。RIP 方向 控制 RIP 数据包的发送和接收。当设置为 **Both** 或 **Out Only** 时，ZyWALL 将定期广播其路由表。当设置为 **Both** 或 **In Only**，它将合并接收的 RIP 信息；当设置为 **None** 时，它不会发送任何 RIP 数据包且将忽略接收的任何 RIP 数据包。

RIP 版本控制 ZyWALL 发送的 RIP 数据包的格式和广播方法（在接收时两种格式均可识别）。RIP-1 可普遍支持，但 RIP-2 能携带更多信息。RIP-1 基本上适用于大多数网络，除非您的网络拓扑比较特殊。

RIP-2B 和 RIP-2M 都以 RIP-2 格式发送路由数据；其不同之处在于 RIP-2B 使用子网广播，而 RIP-2M 则使用组播。组播可降低非路由机器的负荷，这是因为这些机器通常不会侦听 RIP 组播地址，也就不会接收 RIP 数据包。但是，如果您网络上的一个路由器使用组播，则所有的路由器都必须使用组播。

缺省情况下，RIP 方向设置为 **Both**，并且 RIP 版本设置为 RIP-1。

5.5 组播

传统情况下，IP 数据包按照两种方式进行传输，单播（1 个发送方，1 个 接收方）或广播（1 个发送方，网络上的每个人）。组播将 IP 数据包传送到网络上的一组主机，不是每个人，也不是只有 1 个。

IGMP（互联网组群管理协议，Internet Group 组播协议）是一种网络层协议，用于在组播组中创建成员资格。它不用于携带用户数据。IGMP 第 2 版（RFC 2236）是第 1 版（RFC 1112）的改良，但 IGMP 第 1 版仍然广泛使用。如果您要阅读有关 IGMP 第 1 版和第 2 版间互用性的详细信息，请参见 RFC 2236 的第 3 和 4 节。地址 224.0.0.0 未分配到任何组，且由 IP 组播计算机使用。地址 224.0.0.1 用于查询消息，且分配到所有 IP 主机（包括网关）的永久组。所有主机必须加入 224.0.0.1 组，以便参与 IGMP。地址 224.0.0.2 被分配到组播路由器组。

ZyWALL 支持 IGMP 版本 1 (IGMP-v1) 和 IGMP 版本 2 (IGMP-v2)。启动时，ZyWALL 查询所有直接连接的网络以收集组成员关系。从此之后，ZyWALL 定期更新该信息。IP 组播可以在 web 配置程序(LAN; WAN)中的 ZyWALL 局域网和/或广域网接口上被启用/禁用。选择 **None** 以禁用这些接口上的 IP 组播。

5.6 WINS

WINS（Windows Internet 命名服务）是 Windows 平台上 NetBIOS 名称服务器（NBNS）的 Windows 实现。它记录 NetBIOS 计算机名称，并且存储您的网络中计算名称与 IP 地址的映射表。由 DHCP 分配的 IP 地址会在该表中自动更新。计算机可查询服务器而不必发出广播请求计算机名称对应的 IP 地址，因而有助于降低网络的广播流量。WINS 在这方面类似于 DNS。但是和 DNS 不同的是，它不使用层次结构。一个网络可以拥有一个以上 WINS 服务器。Samba 也可用作 WINS 服务器。

5.7 LAN

依次点击 安全 > VPN, 打开 LAN 界面。使用此界面配置 ZyWALL 的 IP 和其他 LAN TCP/IP 设置，包括内置的 DHCP 服务器功能。DHCP 服务器功能将 IP 地址和 DNS 服务器分配给支持 DHCP 客户端功能的系统。

图 35 局域网

LAN

LAN

静态DHCP

IP别名

LAN TCP/IP

IP地址

192 . 168 . 1 . 1

RIP方向

Both

IP子网掩码

255 . 255 . 255 . 0

RIP版本

RIP-1

组播

None

DHCP 设置

DHCP服务器

Server

IP地址池起始地址

192 . 168 . 1 . 33

地址池大小

128

DHCP服务器地址

0 . 0 . 0 . 0

DHCP WINS服务器1

0 . 0 . 0 . 0

DHCP WINS服务器2

0 . 0 . 0 . 0

DNS设置请点击[这里](#)

Windows网络（NetBIOS over TCP/IP）

☐ 允许LAN与WAN之间通讯

（您可能还需要建立相关防火墙规则！）

应用

重置

下表说明了此屏幕中的各个标签。

表 20 局域网

标签	描述

LAN TCP/IP	
IP 地址	键入您的 ZyWALL 的 IP 地址，格式为十进制数字（用句点分隔）。 192.168.1.1 是工厂默认值。另外，也可点击鼠标右键复制和/或粘贴 IP 地址。
IP 子网掩码	子网掩码指定了 IP 地址的网络号部分。您的 ZyWALL 将自动根据分配的 IP 地址来计算子网掩码。除非您正实现子网，否则使用 ZyWALL 计算的子网掩码。
RIP 方向	RIP（路由信息协议、RFC 1058 和 RFC 1389）允许路由器与其他路由器交换路由信息。RIP 方向 字段控制 RIP 数据包的发送和接收。从 Both/In Only/Out Only/None 中选择 RIP 方向。当设置为 Both 或 Out Only 时，ZyWALL 将定期广播其路由表。当设置为 Both 或 In Only，它将合并接收的 RIP 信息；当设置为 None 时，它不会发送任何 RIP 数据包且将忽略接收的任何 RIP 数据包。Both 是默认值。
RIP 版本	RIP 版本栏位控制 ZyWALL 发送的 RIP 数据包的格式和广播方法（在接收时两种格式均可识别）。RIP-1 可普遍支持，但 RIP-2 能携带更多信息。 RIP-1 基本上适用于大多数网络，除非您的网络拓扑比较特殊。RIP-2B 和 RIP-2M 都以 RIP-2 格式发送路由数据；其不同之处在于 RIP-2B 使用子网广播，而 RIP-2M 则使用组播。 组播可降低非路由机器的负荷，这是因为这些机器通常不会侦听 RIP 组播地址，也就不会接收 RIP 数据包。 但是，如果您网络上的一个路由器使用组播，则所有的路由器都必须使用组播。缺省情况下，RIP 方向设置为 Both，并且版本设置为 RIP-1。
组播	选择 IGMP V-1、IGMP V-2 或 None。IGMP（互联网组群管理协议，Internet Group 组播协议）是一种网络层协议，用于在组播组中创建成员资格。它不用于携带用户数据。IGMP 第 2 版（RFC 2236）是第 1 版（RFC 1112）的改良，但 IGMP 第 1 版仍然广泛使用。如果您要阅读有关 IGMP 第 1 版和第 2 版间互用性的详细信息，请参见 RFC 2236 的第 3 和 4 节。
DHCP 设置	

DHCP	DHCP（动态主机配置协议、RFC 2131 和 RFC 2132）允许客户端（工作站）在启动时从服务器获得 TCP/IP 设置参数。除非经由您的 ISP 指导，请将此栏位设置为服务器。如果配置为为服务器，ZyWALL 会为客户端提供 TCP/IP 设置参数。如果设为服务器，请填入 IP 地址池起始地址和地址池大小栏位。 选择 Relay 使 ZyWALL 将 DHCP 请求转发至其他 DHCP 服务器。如果设为 Relay，请填入 DHCP 服务器地址栏位。 选择 None 停止 ZyWALL 的 DHCP 服务器角色。如果选择 None，您必须在您的局域网上有其他的 DHCP 服务器，或者计算机必须进行手动配置。
IP 地址池起始地址	此栏位指定 IP 地址池中连续地址的第一个。
地址池大小	此栏位指定 IP 地址池大小或计数。
DHCP 服务器地址	输入您要 ZyWALL 将 DHCP 请求中继到的 DHCP 服务器的 IP 地址。请使用句点分隔的十进制数字。另外，也可点击鼠标右键复制和/或粘贴 IP 地址。
DHCP WINS 服务器 1, 2	输入您要发送到 DHCP 客户端的 WINS（Windows Internet 命名服务）服务器的 IP 地址。WINS 服务器保存您网络上的计算机名称和其正使用的 IP 地址的一个映射表。
DNS 设置 请点击这里	单击该链接以转到 DNS DHCP 界面以配置 DNS 服务器信息，ZyWALL 将该信息发送到局域网上的 DHCP 客户端设备。
Windows 网络 (NetBIOS over TCP/IP)	NetBIOS（网络基本输入/输出系统）为可使计算机连接到 LAN 并进行通讯的 TCP 或 UDP 数据包。对于某些拨号接入服务，如 PPPoE 或 PPTP 等，NetBIOS 数据包会产生不需要的呼叫。 但是某些时候，有必要允许 NetBIOS 数据包通过 WAN，以便能找到 WAN 上的计算机。
允许 LAN 和 WAN 之间通讯	选择此复选框，可将 NetBIOS 数据包从局域网到广域网和从广域网到局域网进行转发。如果您的防火墙启用了阻止所有从广域网到局域网的流量的缺省策略，您还需要启用广域网到局域网的防火墙规则以转发 NetBIOS 流量。 清除此复选框，可阻止局域网和广域网之间的所有 NetBIOS 流量。

应用	单击应用以将更改保存回 ZyWALL。
重置	单击重置以开始重新配置此界面。

5.8 LAN 静态 DHCP

此表允许您根据 MAC 地址将局域网上的 IP 地址分配到特定的单个计算机。

每个以太网设备具有唯一的 MAC（媒体访问控制）地址。MAC 地址在工厂进行分配，且由六对十六进制字符组成，例如 00:A0:C5:00:00:02。

若要更改您的 ZyWALL 的静态 DHCP 设置，请单击网络 > LAN > 静态 DHCP。该界面如下图所示。

图 36 LAN 静态 DHCP

LAN

LAN

静态DHCP

IP别名

静态DHCP表单

#	MAC地址	IP地址
1		0 . 0 . 0 . 0
2		0 . 0 . 0 . 0
3		0 . 0 . 0 . 0
4		0 . 0 . 0 . 0
5		0 . 0 . 0 . 0
6		0 . 0 . 0 . 0
7		0 . 0 . 0 . 0
8		0 . 0 . 0 . 0
9		0 . 0 . 0 . 0
10		0 . 0 . 0 . 0
123		0 . 0 . 0 . 0
124		0 . 0 . 0 . 0
125		0 . 0 . 0 . 0
126		0 . 0 . 0 . 0
127		0 . 0 . 0 . 0
128		0 . 0 . 0 . 0

应用

重置

下表说明了此屏幕中的各个标签。

表 21 LAN 静态 DHCP

标签	描述
#	这是静态 IP 表单（行）的索引号。
MAC 地址	键入局域网上的计算机 MAC 地址。

IP 地址	键入您要在局域网上分配到计算机的 IP 地址。另外，也可点击鼠标右键复制和/或粘贴 IP 地址。
应用	单击应用以将更改保存回 ZyWALL。
重置	单击重置以开始重新配置此界面。

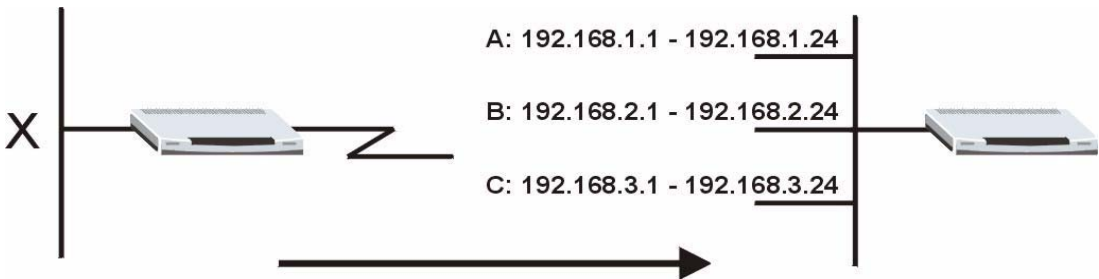
5.9 局域网 IP 别名

您可以通过 IP 别名功能将您的物理网络分隔成相同以太网接口上的不同逻辑网络。ZyWALL 支持与 ZyWALL 本身的单个物理以太网接口三个逻辑局域网接口，作为每个局域网网络的网关。

当您使用 IP 别名时，您还可以配置防火墙规则来控制局域网逻辑网络（子网）之间的访问。
注：确保逻辑网络的子网不重叠。

下图显示了划分为子网 A、B 和 C 子网的局域网。以太网接口标为 X。

图 37 物理网络与分区的逻辑网络



若要更改您的 ZyWALL 的 IP 别名设置，请单击网络 > LAN > IP 别名。该界面如下图所示。

图 38 局域网 IP 别名

LAN

LAN

静态DHCP

IP 别名

IP别名1

☒ 启用IP别名1

IP地址

192 . 168 . 2 . 1

IP子网掩码

255 . 255 . 255 . 0

RIP方向

None

RIP版本

RIP-1

IP别名2

☒ 启用IP别名2

IP地址

192 . 168 . 3 . 1

IP子网掩码

255 . 255 . 255 . 0

RIP方向

None

RIP版本

RIP-1

应用

重置

下表说明了此界面中的各个标签。

表 22 局域网 IP 别名

标签	描述
启用 IP 别名 1,2	选择该复选框以配置 ZyWALL 的另一个局域网网络。
IP 地址	键入您的 ZyWALL 的 IP 地址，格式为十进制数字（用句点分隔）。另外，也可点击鼠标右键复制和/或粘贴 IP 地址。
IP 子网掩码	您的 ZyWALL 将自动根据分配的 IP 地址来计算子网掩码。除非您正实现子网，否则使用 ZyWALL 计算的子网掩码。
RIP 方向	RIP（路由信息协议、RFC 1058 和 RFC 1389）允许路由器与其他路由器交换路由信息。RIP 方向 字段控制 RIP 数据包的发送和接收。从 Both/In Only/Out Only/None 中选择 RIP 方向。当设置为 Both 或 Out Only 时，ZyWALL 将定期广播其路由表。当设置为 Both 或 In Only，它将合并接收的 RIP 信息；当设置为 None 时，它不会发送任何 RIP 数据包且将忽略接收的任何 RIP 数据包。
RIP 版本	RIP 版本栏位控制 ZyWALL 发送的 RIP 数据包的格式和广播方法（在接收时两种格式均可识别）。RIP-1 可普遍支持，但 RIP-2 能携带更多信息。RIP-1 基本上适用于大多数网络，除非您的网络拓扑比较特殊。RIP-2B 和 RIP-2M 都以 RIP-2 格式发送路由数据；其不同之处在于 RIP-2B 使用

	子网广播，而 RIP-2M 则使用组播。 组播可降低非路由机器的负荷，这是因为这些机器通常不会侦听 RIP 组播地址，也就不会接收 RIP 数据包。 但是，如果您网络上的一个路由器使用组播，则所有的路由器都必须使用组播。缺省情况下，RIP 方向设置为 Both，并且 Version 设置为 RIP-1。
应用	单击应用以将更改保存回 ZyWALL 。
重置	单击重置以开始重新配置此界面。

第 6 章 网桥界面

本章说明了如何配置网桥设置。本章仅适用于当 ZyWALL 处于网桥模式时。

6.1 网桥

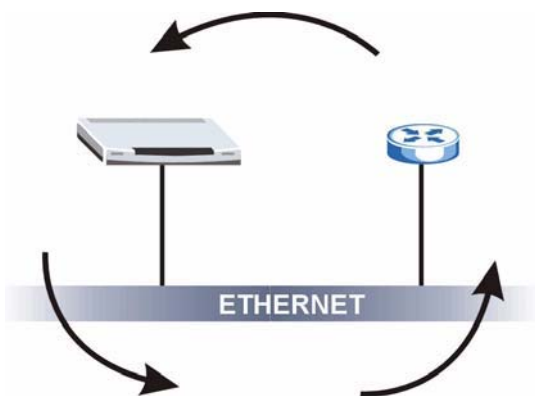
ZyWALL 可以用作透明的防火墙（也称为网桥防火墙），以便提供防火墙保护，避免拒绝服务攻击。您不必将现有网络配置更改为将 ZyWALL 用作网桥防火墙。ZyWALL 用作交换机和有线局域网或两个路由器和过滤器之间的网桥，并检测数据包。

6.1.1 网桥回路

当在 ZyWALL 中启用网桥时当心避免网桥回路。网桥回路使得广播流量在网络中无限循环，可能造成通信的性能降低和中断。以下示例显示了可以造成这种问题的网络拓扑。

ZyWALL（处于网桥模式）在与另一个网桥通信时被连接到有线局域网，或连接到相同有线局域网的交换机。因此通讯流量将在网络中循环

图 39 网桥回路：连接到有线局域网的网桥



通过确保您的 ZyWALL 在连接到相同局域网的两个有线片段时未设置为网桥模式，您可以避免网桥回路。如果您的网络使用 RSTP，则可以在 ZyWALL 连接到相同局域网的两个有线片段时将其设置为网桥模式，前提是要在 ZyWALL 上启用 RSTP 和局域网的其他联网设备。

6.2 生成树协议

生成树协议（STP）可以检测并消除网络环路，并且可以在两台交换机，网桥或路由器之间提供备份的连接。这样可以允许一个网桥和其它支持 STP 的网桥通信，以确保在网络上的任意两个终端之间只会存在一条路径。

6.2.1 快速生成树协议

ZyWALL 使用 IEEE 802.1w 中定义的快速生成树协议（RSTP）可以实现生成树的快速（相比较只支持 STP 的网桥来说）融合。使用 RSTP 的时候，拓扑更改信息也可以不用传播到根网桥，同时无用的已学地址会从过滤数据库中删除掉。RSTP 定义了 3 种端口状态：丢弃、学习和转发。

6.2.2 STP 术语

6.2.2 STP 术语根网桥是生成树的基础；它是具有最低标识值（MAC 地址）的网桥。

路径开销是从根网桥向某一个端口发送数据帧的开销。它是根据该端口所接链路的速率而定的。链路速率越低，开销值越大（请参考下表）。

表 23 STP 路径开销

	链路速率	建议数值	建议范围	允许的范围
Path Cost	4Mbps	250	100 到 1000	1 到 65535
Path Cost	10Mbps	100	50 到 600	1 到 65535
Path Cost	16Mbps	62	40 到 400	1 到 65535
Path Cost	100Mbps	19	10 到 60	1 到 65535
Path Cost	1Gbps	4	3 到 10	1 到 65535
Path Cost	10Gbps	2	1 到 5	1 到 65535

在每一个网桥里，根端口是其它网桥和根网桥通信的端口。它是交换机到根网桥的路径开销最小的端口。如果没有根端口，那么这台交换机就会作为生成树网络的根网桥。为了确定哪一个端口应该关闭，必须知道指定端口（指定网桥）。指定端口（网桥）取决于物理网段，在所有的物理网段上都存在指定端口（网桥）。它是该网段中到根网桥 开销最低的网桥。

6.2.3 STP 怎样工作

当利用 STP 生成树协议决定了开销最低的生成树之后，它将允许根端口和指定端口处于激活状态，其它的端口处于阻塞状态。这样网络数据包将只能通过这些激活端口，从而消除网络环路。

支持 STP 生成树协议的交换机将会周期性地交换 BPDU（网桥协议数据单元）但是当交换网络结构改变的时候，一个新的生成树将会重新构架。

一旦网络拓扑稳定下来，所有的网桥都会侦听从根网桥发送的 BPDU 数据。如果一个网桥在一段间隔时间之后还没有收到 BPDU 信息，就会认为到根网桥的链路断掉了。这样网桥就会和其它网桥重新协商建立一个有效的网络拓扑。

6.2.4 STP 端口状态

STP 会采用 5 种端口状态（见下表）来消除网络环路。

表 24 STP 端口状态

端口状态	描述
Disabled	STP 未激活（缺省）。
Blocking	只有管理和配置 BPDU 信息可以接收并被处理。
Listening	所有的 BPDU 都可以接收并被处理。
Learning	所有的 BPDU 都可以接收并被处理。信息帧发送到学习过程，但是不再进行转发。
Forwarding	所有的 BPDU 都可以接收并被处理。所有的信息帧都可以接收并转发。

6.3 网桥

在设备维护 设备模式界面中先点击网桥,然后点击应用可以启用 ZyWALL 的网桥功能。如果您想修改 ZyWALL 的网桥参数，可以先后点击网络，网桥。您会见到以下界面。

图 40 网桥

网桥

桥接

桥接设置

IP地址

192 , 168 , 1 , 1

IP子网掩码

255 , 255 , 255 , 0

网关IP地址

0 , 0 , 0 , 0

第一DNS服务器

0 , 0 , 0 , 0

第二DNS服务器

0 , 0 , 0 , 0

第三DNS服务器

0 , 0 , 0 , 0

Rapid Spanning Tree通信协议设置

☐ 启用RSTP

网桥优先级:

32768

0 (最高) ~ 61440 (最低)

网桥问候时间:

2

1 (秒) ~ 10 (秒)

网桥最大保留时间:

20

6 (秒) ~ 40 (秒)

转送延迟:

15

4 (秒) ~ 30 (秒)

网桥端口	启用RSTP	RSTP优先级 0 (最高) ~ 240 (最低)	RSTP路径权值 1 (最低) ~ 65535 (最高)
WAN	☐	128	250
LAN	☐	128	250

应用

重置

以下为界面相关的描述。

表 25 网桥

标签	描述
桥接设置	
IP 地址	输入 ZyWALL 的 IP 地址。
IP 子网掩码	输入相应的子网掩码。
网关 IP 地址	输入网关的 IP 地址。
第一/第二/第三 DNS 服务器	DNS 可以将域名映射为相应的 IP 地址。DNS 相当重要，因为如果没有它，我们在连接某台机器的时候需要知道它的 IP 地址才可以。ZyWALL 可以使用一个系统 DNS 服务器（您 在这里规定的）来解析内容过滤和时间服务器等的域名。 如果您知道 DNS 服务器的 IP 地址，可以在此处输入该地址。
Rapid Spanning Tree 通信协议设置	

启用 RSTP	点选此框可以激活 ZyWALL 的 RSTP 功能。
桥接优先级	输入一个范围在 0 到 61440 之间的数值作为 ZyWALL 的优先级。0 是最高的优先级。
网桥问候时间	以秒为单位输入一个时间数值（范围在 6 到 40 之间），这是网桥生成两个 BPDU(网桥协议数据单元)配置信息的时间间隔。
网桥最大保留时间	以秒为单位输入一个时间数值（范围在 6 到 40 之间），这是网桥等待从根网桥获得一个 Hello BPDU 信息的最大时间。
传送延迟	以秒为单位输入一个时间数值（范围在 6 到 40 之间），这是网桥在改变状态之前的最大时间。在这段时间中网桥会一直保持侦听和学习端口的状态。缺省时间为 15 秒。
网桥端口	这是网桥端口的类型。端口类型有：WAN，LAN，WLAN 和 DMZ。
启用 RSTP	点选此框可以激活相应端口的 RSTP。
RSTP 优先级 0(最高)~240(最低)	输入一个范围在 0 到 240 之间的数值，代表相应端口的 RSTP 优先级。0 代表最高优先级。
RSTP 路径权值 1(最低)~65535(最高)	输入一个范围在 1 到 65535 之间的数值，代表相应端口的 RSTP 路径开销。65535 是最大开销值。
应用	点击应用可以保存设置。
重置	点击重置可以重新配置该界面。

第 7 章 广域网界面

本章说明了如何配置广域网设置。

7.1 广域网概述

- 使用 WAN 路由界面来配置路由优先权。
- 使用 WAN 界面来配置互联网介入的广域网端口。
- 使用流量重定向 界面来配置您的流量重定向属性和参数。
- 使用拨号备份 界面来配置备用广域网拨号连接。

7.2 TCP/IP 优先权（跃点数）

跃点数代表了“传输的成本”。路由器通过选择具有最低“成本”的路径决定了传输的最佳路由。RIP 路由使用跳跃计数来作为成本测量方法，最小为 1 表示直接连接到网络。数字必须介于“1”和“15”之间；数字大于“15”表示链接断开。数值越小，开销越低。

- 1 跃进点将 ZyWALL 的路由优先权设置为互联网。每个路由必须具有一个唯一的跃进点。
- 2 广域网端口路由的优先权必须始终大于备用拨号和流量重定向路由优先权。

如果广域网端口具有跃进点“1”，而流量重定向路由具有跃进点“2”，且备用拨号路由具有跃进点“3”，则广域网端口路由用作主要默认路由。如果广域网端口路由不能连接到互联网，则 ZyWALL 尝试接下来将流量重定向路由。按照相同的方式，如果流量重定向路由也失败，则 ZyWALL 使用备用拨号路由。

备用拨号或流量重定向路由无法具有比广域网路由更高的优先权。

7.3 广域网路由

依次单击网络 > WAN 以打开路由界面。使用该界面以配置路由优先权。

图 41 广域网路由

WAN

路由

WAN

流量重定向

拨号备份

路由优先级

WAN

流量重定向

拨号备份

优先级 (权值)

1

1 (最高) ~ 15 (最低)

优先级 (权值)

14

1 (最高) ~ 15 (最低)

优先级 (权值)

15

1 (最高) ~ 15 (最低)

Windows 网络 (NetBIOS over TCP/IP)

☐ 允许WAN与LAN之间通讯

☐ 允许触发拨号

(您可能还需要建立相关防火墙规则!)

应用

重置

下表说明了此界面中的各个标签。

表 26 广域网路由

标签	描述
路由优先级	
WAN 流量重定向 拨号备份	默认广域网连接是"1", 因为通过广域网端口您的宽带连接应始终是访问广域网的首选方法。 路由的默认优先权是 WAN 、流量重定向和拨号备份: 如果您的常规广域网连接断开, 则您有两个辅助连接选择 (流量重定向和拨号备份)。 如果拨号备份 首选为流量重定向, 则在拨号备份优先级 (权值)字段中键入"14" (在默认值为 15 时保留流量重定向优先级 (权值)。 只有您在拨号备份界面中启用相应的备用拨号功能时, 拨号备份 字段才可用。
Windows 网络 (NetBIOS over TCP/IP):	NetBIOS (网络基本输入/输出系统) 为可使计算机连接到 LAN 并进行通讯的 TCP 或 UDP 数据包。对于某些拨号接入服务, 如 PPPoE 或 PPTP 等, NetBIOS 数据包会产生不需要的呼叫。
允许 WAN 和 LAN 之间通讯	选择此复选框, 可将 NetBIOS 数据包从局域网到广域网和从广域网到局域网进行转发。如果您的防火墙启用了阻止所有从广域网到局域网的流量的缺省策略, 您还需要启用广域网到局域网的防火墙规则以转发 NetBIOS 流量。 清除此复选框, 可阻止局域网和广域网之间的所有 NetBIOS 流量。
允许触发拨号	选择该选项允许 NetBIOS 数据包初始化呼叫。
应用	单击应用以将更改保存回 ZyWALL。

重置	单击重置以开始重新配置此界面。

7.4 广域网 IP 地址分配

互联网上的每台机器必须具有一个唯一的 IP 地址。如果您的网络与互联网隔离，例如只有两个分公司办公室，则您可以将任何 IP 地址分配给主机，不会出现任何问题。然而，国际因特网地址分配委员会（IANA）已将下列三个 IP 地址区段特别保留给私有网络使用。

表 27 专用 IP 地址范围

10.0.0.0	-	10.255.255.255
172.16.0.0	-	172.31.255.255
192.168.0.	-	192.168.255.255

您的 IP 地址可以从 IANA 或 ISP 获得，或者也可由专用网络分配给您。如果您属于一个小型组织，并且通过 ISP 访问互联网的，则 ISP 会向您提供互联网地址供您的局域网使用。另一方面，如果您是某个大型组织的一部分，则应询问您的网络管理员，以获得合适的 IP 地址。

注意：无论您属于哪种情况，请勿随意创建 IP 地址；请务必遵循上述准则。有关地址分配的详细信息，请参考 RFC 1597（私有网络地址分配）以及 RFC 1466（IP 地址空间管理准则）。

7.5 DNS 服务器地址分配

使用 DNS（域名系统）将域名映射到相应的 IP 地址，或者将相应的 IP 地址映射到域名，例如 **www.zyxel.com** 的 IP 地址是 **204.217.0.2**。DNS 服务器极其重要，因为没有 DNS 服务器，您必须在访问该服务器之前知道计算机的 IP 地址。

ZyWALL 可以按照以下方式获取 DNS 服务器地址。

- 1 ISP 在您登入时告知您 DNS 服务器地址，通常是信息页面的表格。如果您的 ISP 向您给出 DNS 服务器地址，则在 DNS 服务器字段中手动输入这些地址。
- 2 如果您的 ISP 动态分配 DNS 服务器 IP 地址（以及 ZyWALL 的广域网 IP 地址），则将 DNS 服务器字段设置为从 ISP 中获取 DNS 服务器地址。
- 3 您可以手动输入另一个 DNS 服务器的 IP 地址。这些服务器可以是 公共的或专有的。DNS 服务器甚至可以位于远程 IPSec 路由器之后（参见第 17.5.1 节）。

7.6 WAN MAC 地址

每一台以太网设备都必须有一个唯一的 MAC 地址。每台设备出厂的时候都被指定一个

12 位的 MAC 地址，如 00:A0:C5:00:00:02。您可以使出厂设置的 MAC 地址作为 WAN 口的 MAC 地址，也可以将局域网内的一台计算机的 MAC 地址映射到 WAN 口上作为它的 MAC 地址。注意：即使 ISP 不需要对 ZyWALL 的 MAC 地址做认证，ZyXEL 建议您最好也采用克隆内部计算机 MAC 地址的方式。

表 28 有固定 IP 地址的 LAN 服务器的网络属性

选择一个 IP 地址	192.168.1.2-192.168.1.32;
子网掩码	255.255.255.0
网关（或缺省路由）	192.168.1.1(ZyWALL 的 LAN 口 IP 地址)

7.7 广域网

若要更改您的 ZyWALL 的广域网 ISP、IP 和 MAC 设置，请单击网络 > WAN > WAN。该界面的封装方式不同。

7.7.1 广域网以太网封装

对于发送 UDP 心跳数据包以验证客户仍然在线的 ISP（例如 Telstra），请创建用于这些数据包的 WAN-to-WAN/ZyWALL 防火墙。联系您的 ISP 以查找正确的端口号。

以下显示的界面用于 Ethernet 封装。

图 42 WAN：以太网封装

WAN

路由

WAN

流量重定向

拨号备份

互联网接入ISP参数

封装

Ethernet

服务类型

RR-Toshiba

用户名

密码

再输入一次以便确认

登入服务器的IP地址

0 . 1 . 0 . 0

WAN IP地址分配

☒ 自动从ISP取得

☐ 使用固定IP地址

我的WAN IP地址

0 . 0 . 0 . 0

我的WAN IP子网掩码

0 . 0 . 0 . 0

网关IP地址

0 . 0 . 0 . 0

高级设置

☒ 启用NAT（网络地址转换）

RIP方向

None

RIP版本

RIP-1

☐ 启用组播

组播版本

IGMP v1

☐ 变更WAN端口MAC

复制电脑的MAC— IP地址

192 . 168 . 1 . 90

应用

重置

以下为界面相关的描述。

表 29 WAN：以太网封装

标识	描述
ISP	
封装	当您 WAN 口连接普通的以太网的时候一定要选择 Ethernet 选项。
服务类型	您从下拉菜单中选择 Standard, Telstra（RoadRunner Telstra 认证模式 ），RR-Manager （ Roadrunner Manage 认证模式 ），RR-Toshiba （RoadRunner Toshiba 认证模式）或 Telia 登入。 下面的选项在选择 Standard 服务类型时不会出现。
用户名	输入 ISP 给您的用户名。
密码	输入与以上用户名相关的密码。

再输入一次以便确认	重新输入密码以保证密码输入正确。
登入服务器的 IP 地址	如果 ISP 给了您认证服务器的 IP 地址，请在此处输入该值。如果是 Telia 登入的模式，则不需要设置该项。
登入服务器（仅适用于 Telia 登入）	输入 Telia 登入服务器的域名，例如“登入 1.telia.com”。
Relongin Every (min)（仅适用于 Telia 登入）	如果 ZyWALL 没有定期登录服务器的话，Telia 登入服务器会断开此连接。以分钟为单位输入从 1 到 59（缺省为 30）的数值来作为 ZyWALL 两次登录的时间间隔。
WAN IP 地址分配	
自动从 ISP 取得	如果您的 ISP 没有给您固定 IP 地址的话，请选择此项。设备缺省选择此项。
使用固定的 IP 地址	如果您的 ISP 给了固定的 IP 地址，请选此项。
我的 WAN IP 地址	如果您在前面选择了 使用固定 IP 地址，可以在此输入 ISP 给您的 IP 地址。
我的 WAN IP 子网掩码	如果您在前面选择了使用固定 IP 地址，可以在此输入您的子网掩码（如果 ISP 给您的话）。
网关 IP 地址	如果您在前面选择了使用固定 IP 地址，可以在此输入您的网关地址（如果 ISP 给您的话）。
高级设置	
启用 NAT(网络地址转换)	NAT 技术一般用来作内、外网的地址转换，以实现节省 IP 地址的目的。点选此框可以启用 NAT 功能。 如果您想了解 NAT 更多的知识，请参考网络地址转换（NAT）一章。
RIP 方向	RIP（路由信息协议）允许路由器与其它路由器交换路由信息。RIP 方向 控制发送和接收 RIP 数据包。 选项包括 Both, None, In only 或 Out only。 当您选择 Both 或 Out only 时，路由器会周期性地广播路由表。 当您选择 Both 或 In only 时，路由器会合并其接收到的 RIP 信息。 当选择 None 时，路由器既不会发送也不会接收任何 RIP 信息。 缺省选择是 Both。

RIP 版本	RIP 版本项控制 ZyWALL 发送 RIP 数据包的格式和广播方式。选项有 RIP-1, RIP-2B 或 RIP-2M。 RIP-1 是广泛被支持的, 但 RIP-2 可携带更多的信息。RIP-1 对大多数网络来说已经足够了, 除非您使用不常用的网络拓扑。RIP-2M 和 RIP-2B 都支持 RIP-2 的路由数据发送格式, 区别是 RIP-2B 使用子网广播方式而 RIP-2M 使用组播方式。由于非路由设备不会侦听 RIP 组播的地址, 这样就不会接收到 RIP 数据包, 所以可以减少这些设备上的负荷。然而, 如果一台路由器使用组播, 那么您网络上所有的路由器都必须使用组播。缺省设置是 RIP-1。
启用组播	点选此框可以打开 IGMP 功能。IGMP 是一种网络层协议, 用于在同一个组播组内建立组播组成员, IGMP 不用于传输用户数据。
组播版本	选择有 None (缺省), IGMP-V1 和 IGMP-V2。IGMP 用来在同一个组播组内建立组播组成员, 不用来传输用户数据。IGMP V2 (RFC2236) 是 IGMP V1 (RFC1112) 的增强版本, 但 IGMP V1 还在广泛应用。如果您想了解 IGMP V1 和 V2 的相关信息及关系请参考 RFC2236 的第 4 节和第 5 节。
变更 WAN 端口 MAC 地址	您可以使用出厂默认的 MAC 地址, 也可以从您接在 LAN 口上的内网中的一台机器上克隆过来一个 MAC 地址。 选择 S 地址池 WAN MAC 地址, 并输入您内网那台被克隆 MAC 地址的计算机的 IP 地址。一旦成功, 该 MAC 地址会被存入 ROM 配置文件中, 除非您更改此项设置或重新刷新 ROM 文件, 否则该项设置不会改变。
复制电脑的 MAC 地址—IP 地址	输入您内网那台被克隆 MAC 地址的计算机的 IP 地址。建议您在把设备接到外网之前先做此项工作。
应用	点击应用可以保存设置。
重置	点此重置可以重新设置该界面。

7.7.2 PPPoE 封装

ZyWALL 支持 PPPoE (以太网点对点协议)。PPPoE 是 IETF 标准 (RFC 2516), 指定了个人计算机(PC)如何与宽带调制解调器 (DSL、有线、无线等) 连接进行交互。PPPoE 选项使用 PPPoE 用于拨号连接。通过直接在 ZyWALL 上实现 PPPoE (而不是单个计算机), 局域网上的计算机不需要已安装的 PPPoE 软件, 因为 ZyWALL 是任务的一部分。而且, 使用 NAT,

所有局域网的计算机将可以访问。

PPPoE 的其中一个优点是能够允许访问多个网络服务的某个。 功能称为动态服务选项。这使得服务提供商已于创建和提供新的个人 IP 服务。

实际上，PPPoE 为您和 ISP 或运营商节省了重要的努力，因为它在客户侧不需要宽带调制解调器的特定配置。以下显示的界面用于 PPPoE 封装。

图 43 WAN: PPPoE 封装

WAN

路由

WAN

流量重定向

拨号备份

互联网接入ISP参数

封装

PPP over Ethernet

服务名称

(选项)

用户名

密码

再输入一次以便确认

验证类型

CHAP/PAP

☐ 固定联机

闲置超时

100

(秒)

WAN IP地址分配

☒ 自动从ISP取得

☐ 使用固定IP地址

我的WAN IP地址

0 . 0 . 0 . 0

高级设置

☒ 启用NAT(网络地址转换)

RIP方向

None

RIP版本

RIP-1

☐ 启用组播

组播版本

IGMP v1

☐ 变更WAN端口MAC

复制电脑的MAC- IP地址

192 . 168 . 1 . 90

应用

重置

The 下表描述了界面的标签。

表 30 WAN: PPPoE 封装

标签	描述
互联网接入 ISP 参数	

封装	PPPoE 选项使用 PPPoE 用于拨号连接。路由器支持 PPPoE（以太网点对点协议）。PPPoE 是 IETF 标准（RFC 2516），指定了个人计算机(PC)如何与宽带调制解调器（DSL、有线、无线等）连接进行交互。实际上，PPPoE 为最终用户和 ISP 或运营商节省了重要的努力，因为它在客户侧不需要宽带调制解调器的特定配置。通过直接在路由器上实现 PPPoE（而不是单个计算机），局域网上的计算机不需要已安装的 PPPoE 软件，因为路由器是任务的一部分。而且，使用 NAT，所有局域网的计算机将可以访问。
服务名称	键入提供给您 PPPoE 服务名称。PPPoE 使用服务名称来标识和达到 PPPoE 服务器。
用户名	键入 ISP 向您给出的用户名称。
密码	键入与以上用户名关联的密码。
再输入一次以便确认	再次键入您的密码以确保您输入的密码是正确的。
验证类型	使用下拉列表框以选择传出呼叫的验证协议。选项为： CHAP/PAP – 当该远程节点请求时，您的 ZyWALL 接受 CHAP 或 PAP。 CHAP - 您的 ZyWALL 只接受 CHAP。 PAP - 您的 ZyWALL 只接受 PAP。
固定联机	如果您不想要连接超时，则选择固定联机。
闲置超时	该值指定了 ZyWALL 自动与 PPPoE 服务器断开连接之前用掉的时间（以秒为单位）。
WAN IP 地址 分配	
自动从 ISP 取得	如果您的 ISP 不向您分配固定的 IP 地址，则选择该选项。这是默认的选项。
使用固定 IP 地址	如果 ISP 不向您分配固定的 IP 地址，则选择该选项。
我的 WAN IP 地址	如果您选择使用固定 IP 地址，则在该字段中输入广域网 IP 地址。
高级设置	

启用 NAT (网络地址转换)	网络地址转换(NAT) 允许将一个网络内使用的互联网协议地址（例如本地网络网络中使用的专用 IP 地址）转换为另一个网络中已知的不同 IP 地址（例如互联网上使用的公共 IP 地址）。 选择此复选框启用 NAT。 有关 NAT 的更多信息，请参见第 4 章。
RIP 方向	RIP（路由信息协议）允许路由器与其他路由器交换路由信息。RIP 方向 字段控制 RIP 数据包的发送和接收。 选择 Both、None、In Only 或 Out Only。 当设置为 Both 或 Out Only 时，ZyWALL 将定期广播其路由表。 当设置为 Both 或 In Only 时，ZyWALL 将合并接收的 RIP 信息。 当设置为 None 时，ZyWALL 不会发送任何 RIP 数据包且将忽略任何已接收的 RIP 数据包。 默认情况下，RIP 方向 被设置为 Both。
RIP 版本	RIP 版本栏位控制 ZyWALL 发送的 RIP 数据包的格式和广播方法（在接收时两种格式均可识别）。 选择 RIP-1、RIP-2B 或 RIP-2M。 RIP-1 可普遍支持，但 RIP-2 能携带更多信息。RIP-1 基本上适用于大多数网络，除非您的网络拓扑比较特殊。RIP-2B 和 RIP-2M 都以 RIP-2 格式发送路由数据；其不同之处在于 RIP-2B 使用子网广播，而 RIP-2M 则使用组播。组播可降低非路由机器的负荷，这是因为这些机器通常不会侦听 RIP 组播地址，也就不会接收 RIP 数据包。但是，如果您网络上的一个路由器使用组播，则所有的路由器都必须使用组播。默认情况下，RIP 版本字段被设置为 RIP-1。
启用组播	选中此复选框，以开启 IGMP（互联网组组播协议）。IGMP（互联网组群管理协议）是一种网络层协议，用于在组播组中创建成员资格。它不用于携带用户数据。
组播版本	选择 None（默认值）、IGMP-V1 或 IGMP-V2。IGMP（互联网组群管理协议，Internet Group 组播协议）是一种会话层协议，用于在组播组中创建成员资格。它不用于携带用户数据。IGMP 第 2 版（RFC 2236）是第 1 版（RFC 1112）的改良，但 IGMP 第 1 版仍然广泛使用。如果您要阅读有关 IGMP 第 1 版和第 2 版间互用性的详细信息，请参见 RFC 2236 的第 3 和 4 节。

变更 WAN 端口 MAC 地址	您可以使用工厂分配的默认 MAC 地址或从局域网的计算机中来克隆的 MAC 地址。 否则，选择变更 WAN 端口 MAC 地址旁边的复选框并输入您正克隆 MAC 的局域网中计算机的 IP 地址。一旦它成功配置，地址将被复制到 rom 文件（ZyNOS 配置文件）。除非您更改设置或上传一个不同的 ROM 文件，否则它不会更改。
复制电脑的 MAC 地址 – IP 地址	输入您正克隆 MAC 的局域网中的计算机的 IP 地址。 推荐您在挂起广域网端口之前克隆 MAC 地址。
应用	单击应用以将更改保存回 ZyWALL。
重置	单击重置以开始重新配置此界面。

7.7.3 PPTP 封装

点对点隧道协议(PPTP) 是一种网络协议，允许将数据从远程客户端传输到专用服务器，使用基于 TCP/IP 的网络来创建虚拟专用网络(VPN)。

PPTP 支持按需、多协议和公共网络上的虚拟专用网络，例如互联网。以下显示的界面用于 PPTP 封装。

图 44 WAN: PPTP 封装

WAN

路由

WAN

流量重定向

拨号备份

互联网接入ISP参数

封装

PPTP

用户名

密码

再输入一次以便确认

验证类型

CHAP/PAP

☐ 固定联机

闲置超时

100

(秒)

PPTP 设置

我的 IP地址

0 . 0 . 0 . 0

我的 IP子网掩码

0 . 0 . 0 . 0

服务器 IP地址

0 . 0 . 0 . 0

联机 ID/名称

WAN IP地址分配

☒ 自动从ISP取得

☐ 使用固定IP地址

我的WAN IP地址

0 . 0 . 0 . 0

高级设置

☒ 启用NAT(网络地址转换)

RIP方向

None

RIP版本

RIP-1

☐ 启用组播

组播版本

IGMP v1

☐ 变更WAN端口MAC

复制电脑的MAC- IP地址

192 . 168 . 1 . 90

应用

重置

下表说明了此界面中的各个标签。

表 31 WAN: PPTP 封装

标签	描述
互联网接入 ISP 参数	

封装	点对点隧道协议(PPTP) 是一种网络协议，允许将数据从远程客户端传输到专用服务器，使用基于 TCP/IP 的网络来创建虚拟专用网络(VPN)。PPTP 支持按需、多协议和公共网络上的虚拟专用网络，例如互联网。ZyWALL 在任何给定时间内仅支持一个 PPTP 服务器连接。若要配置 PPTP 客户端，您必须为 PPP 连接配置用户名 和密码 字段，并为 PPTP 连接创建 PPTP 参数。
用户名	键入 ISP 向您给出的用户名称。
密码	键入与以上用户名关联的密码。
再输入一次以便确认	再次键入您的密码以确保您输入的密码是正确的。
认证 类型	使用下拉列表框以选择传出呼叫的验证协议。选项为： CHAP/PAP – 当该远程节点请求时，您的 ZyWALL 接受 CHAP 或 PAP。 CHAP - 您的 ZyWALL 只接受 CHAP。 PAP - 您的 ZyWALL 只接受 PAP 。
固定联机	如果您不想要连接超时，则选择固定联机。
闲置超时	该值指定了 ZyWALL 自动与 PPTP 服务器断开连接之前用掉的时间（以秒为单位）。
PPTP 设置	
我的 IP 地址	键入 ISP 向您给出的静态 IP 地址。
我的 IP 子网掩码	您的 ZyWALL 将自动根据分配的 IP 地址来计算子网掩码。除非您正实现子网，否则使用 ZyWALL 计算的子网掩码。
服务器 IP 地址	输入 PPTP 服务器的 IP 地址。
联机 ID/名称	键入 PPTP 服务器的标识名称。
WAN IP 地址分配	
自动从 ISP 取得	如果 ISP 未向您分配 IP 地址，则选择该选项。这是默认选项。
使用固定 IP 地址	如果 ISP 向您分配 IP 地址，则选择该选项。
我的 WAN IP 地址	如果您选择使用固定 IP 地址，则在此字段中输入广域网 IP 地址。
高级设置	

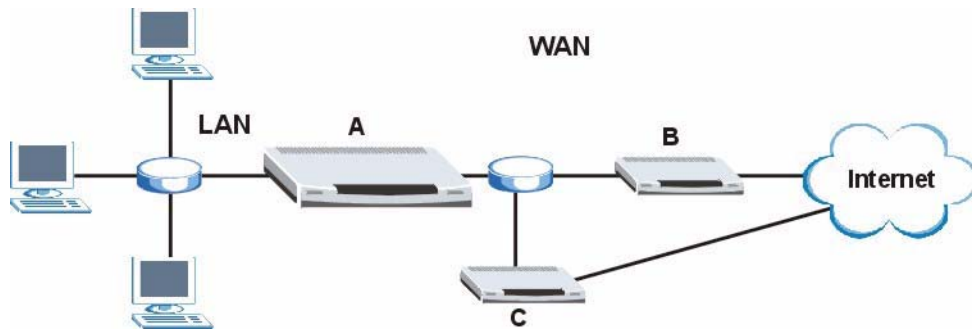
启用 NAT (网络地址 转换)	网络地址转换(NAT) 允许将一个网络（例如本地网络中使用的专用 IP 地址）内使用的互联网协议地址转换到另一个网络中已知的不同 IP 地址（例如互联网上使用的公共 IP 地址）。 选择此复选框启用 NAT。 有关 NAT 的更多信息，请参见第 4 章。
RIP 方向	RIP（路由信息协议）允许路由器与其他路由器交换路由信息。RIP 方向字段控制 RIP 数据包的发送和接收。 选择 Both、None、In Only 或 Out Only。 当设置为 Both 或 Out Only 时，ZyWALL 将定期广播其路由表。 当设置为 Both 或 in Only 时，ZyWALL 将合并接收的 RIP 信息。 当设置为 None 时，ZyWALL 将不会发送任何 RIP 数据包且将忽略任何已接收的 RIP 数据包。 默认情况下，RIP 方向 被设置为 Both。
RIP 版本	RIP 版本栏位控制 ZyWALL 发送的 RIP 数据包的格式和广播方法（在接收时两种格式均可识别）。 选择 RIP-1、RIP-2B 或 RIP-2M。 RIP-1 可普遍支持，但 RIP-2 能携带更多信息。RIP-1 基本上适用于大多数网络，除非您的网络拓扑比较特殊。RIP-2B 和 RIP-2M 都以 RIP-2 格式发送路由数据；其不同之处在于 RIP-2B 使用子网广播，而 RIP-2M 则使用组播。组播可降低非路由机器的负荷，这是因为这些机器通常不会侦听 RIP 组播地址，也就不会接收 RIP 数据包。但是，如果您网络上的一个路由器使用组播，则所有的路由器都必须使用组播。默认情况下，RIP 版本 字段被设置为 RIP-1。
启用组播	选中此复选框，以开启 IGMP（互联网小组组播协议）。IGMP（互联网网络层协议）是一种网络层协议，用于在组播组中创建成员资格。它不用于携带用户数据。
组播版本	选择 None（默认值）、IGMP-V1 或 IGMP-V2。IGMP（互联网组群管理协议）是一种会话层协议，用于在组播组中创建成员资格。它不用于携带用户数据。IGMP 第 2 版（RFC 2236）是第 1 版（RFC 1112）的改良，但 IGMP 第 1 版仍然广泛使用。如果您要阅读有关 IGMP 第 1 版和第 2 版间互用性的详细信息，请参见 RFC 2236 的第 3 和 4 节。

变更 WAN 端口 MAC 地址	您可以使用工厂分配的默认 MAC 地址或克隆局域网上计算机中的 MAC 地址。 否则,选择变更 WAN 端口 MAC 地址旁边的复选框,并输入您正克隆 MAC 的局域网中的计算机的 IP 地址。一旦它成功配置,地址将被复制到 rom 文件 (ZyNOS 配置文件)。除非您更改设置或上传一个不同的 ROM 文件,否则它不会更改。
复制电脑的 MAC 地址 – IP 地址	输入您正克隆 MAC 的局域网中的计算机的 IP 地址。 推荐您在挂起广域网端口之前克隆 MAC 地址。.
应用	单击应用以将更改保存回 ZyWALL。
重置	单击重置以开始重新配置此界面。

7.8 流量重定向

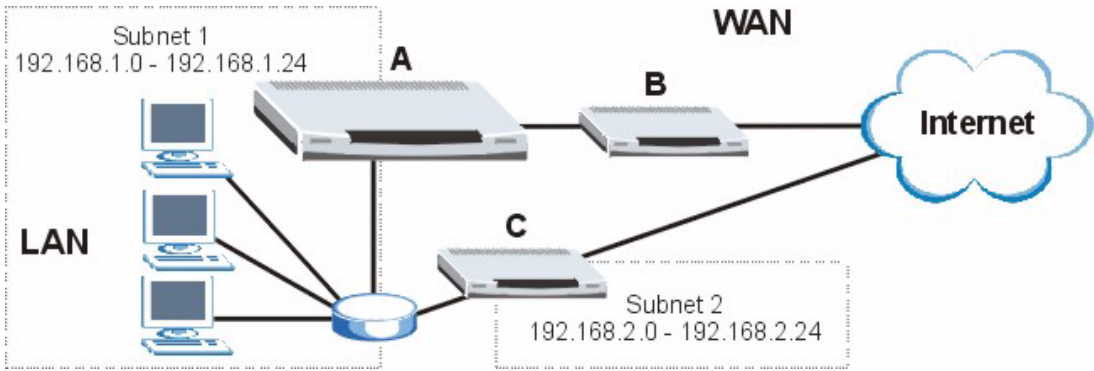
当 ZyWALL 无法通过正常网关连接到互联网时,流量重定向将广域网流量转发到备用网关。连接广域网上的备用网关,因此 ZyWALL 仍然提供了防火墙保护。在下图中,您的 ZyWALL 标为 A,网关标为 B,而备用网关标为 C。

图 45 流量重定向广域网设置



以下网络拓扑允许您避免备用网关连接到局域网时的三角路由安全问题 (参见第 8.13 节)。使用 IP 别名将局域网配置成两个或三个逻辑网络,同时 ZyWALL 本身用作每个局域网网络的网关。将受保护的局域网放在一个子网 (下图中的子网 1) 中,而将备用网关放在另一个子网 (子网 2) 中。将局域网配置为 LAN/ZyWALL 防火墙规则,此规则将数据包从受保护的局域网 (子网 1) 转发到备用网关 (子网 2)。在下图中,您的 ZyWALL 标为 A,网关标为 B,而备用网关标为 C。

图 46 流量重定向局域网设置



7.9 配置流量重定向

若要更改您的 ZyWALL 的流量重定向设置，请单击网络 > WAN > 流量重定向。该界面如下图所示。

图 47：流量重定向

WAN

路由

WAN

流量重定向

拨号备份

流量重定向

☐ 启用

备份网关 IP地址

检查WAN IP地址

容错

周期

闲置时间

0

.

0

.

0

.

0

0

.

0

.

0

.

0

2

5

(秒)

3

(秒)

应用

重置

下表说明了此界面中的各个标签。

表 32 流量重定向

标签	描述
启用	如果正常广域网连接断开，则选择该复选框令 ZyWALL 使用流量重定向。
备份网关 IP地址	键入您的备用网关的 IP 地址，格式为十进制数字（用句点分隔）。如果 ZyWALL 的互联网连接终止，则 ZyWALL 自动将流量转发到该地址。
检查 WAN IP地址	该字段的配置为可选的。如果您未在此处输入 IP 地址，则 ZyWALL 将使用默认网关 IP 地址。配置该字段以测试 ZyWALL 的广域网可访问性。键入计算机附近可靠的地址（例如您的 ISP 的 DNS 服务器地址）。

容错	键入连接被视为“断开”（未连接）之前要有多少个广域网连接检查失败（1 到 10）。ZyWALL 仍然检查“断开”连接以检测是否重新连接。
周期	ZyWALL 通过定期向默认网关或检查 WAN IP 地址字段中的地址发送 PING 来测试广域网连接。 键入秒数（5 到 300）来设置检查之间的时间间隔。如果您的目标 IP 地址处理大量流量，则允许更多时间。
闲置时间	键入 ZyWALL 的秒数（1 到 10）来等待考虑检查已经失败之前 ping 的响应。该设置必须小于周期。如果您的网络繁忙或阻塞，请使用较高的值。
应用	单击应用以将更改保存回 ZyWALL。
重置	单击重置以开始重新配置此界面。

7.10 配置备用拨号

如果广域网和流量重定向连接失败，对于通过外部模拟调制解调器实施的传统拨号连接，可以反向使用备用拨号端口。

依次单击网络 > WAN > 拨号备份 以打开拨号备份 界面。使用该界面来配置备用广域网拨号连接。

图 48 拨号备份

WAN

路由

WAN

流量重定向

拨号备份

拨号备份设置

☐ 启用拨号备份

基础设置

登录名称

ChangeMe

密码

再输入一次以便确认

验证类型

CHAP/PAP

主要电话号码

0

次要电话号码

(选项)

拨号端口速率

115200

AT 指令初始字符串

at&fs0=0

Modem高级设置

编辑

TCP/IP选项

☒ 从ISP自动获取

☐ 使用固定IP地址

我的WAN IP地址

0 . 0 . 0 . 0

远程IP子网掩码

0 . 0 . 0 . 0

远程节点IP子网掩码

0 . 0 . 0 . 0

☒ 启用NAT (网络地址转换)

☐ 启用RIP

RIP版本

RIP-1

RIP方向

Both

☐ 广播拨号备份路由

☐ 启用组播

组播版本

IGMP-v1

PPP选项

PPP封装

Standard PPP

☐ 启动压缩

上网预算

☐ 保持开启

☒ 配置预算

分配预算

0

(分钟)

周期

0

(小时)

闲置时间

100

(秒)

应用

重置

下表描述了该界面中的标签。

表 33 拨号备份

标识	描述
拨号备份设置	
启用拨号备份	点选此框可以启用拨号备份的功能。
基础设置	

登录名称	输入由 ISP 分配的登录名称。
密码	输入由 ISP 分配的登录密码。
再输入一次以便确认	再输入一次密码，确保输入的正确性。
验证类型	使用下拉菜单选择一种输出呼叫的认证协议。选项有： CHAP/PAP: ZyWALL 既会接受远程节点的 CHAP 请求，也会接受 PAP 请求。 CHAP: ZyWALL 只会接受 CHAP 请求。 PAP: ZyWALL 只会接受 PAP 请求。
主要/次要电话号码	输入由 ISP 分配的头一个（主要的）电话号码。如果这个主要的 电话号码忙线或不应答，您的 ZyWALL 会拨叫第二个号码（如果 这个电话存在）。在一些区域进行本地呼叫的时候，您还需要在电话号码前面添加一个符号“#”。
拨号端口速率	从下拉菜单中选择一个拨号备份端口和外接设备的连接速率。有效速率有：9600，19200，38400，57600，115200 或 230400bps。
AT 指令初始字符串	输入所连 WAN 设备的初始化 AT 指令。您可参考 WAN 设备的说明书来进行 AT 指令的设置。
高级设置模式	点击 编辑可以显示 高级设置界面，您可在此编辑您拨号备份的设置项。
TCP/IP 选项	
从 ISP 自动获取	如果 WAN 口 IP 地址是由 ISP 动态分配的，那么请选择此项。
使用固定 IP 地址	如果 ISP 给您分配了固定的 IP 地址，您可以选择此项，然后在下面的区域输入 IP 地址。
我的 WAN IP 地址	如果您不知道 WAN 口的 IP 地址，您可以将此处设置为 0.0.0.0（缺省设置），让 ISP 或其它远程路由器动态（自动）给您分配 IP 地址。如果您知道这个地址（静态的），您可以在此处输入 WAN 口的 IP 地址。这个地址是分配给您本地 ZyWALL 的，而不是分配给远程路由器的。
远程 IP 子网掩码	如果您不知道 WAN 口 IP 的子网掩码，您可以将此处设置为 0.0.0.0（缺省设置），让 ISP 或其它远程路由器动态给您发送子网掩码的信息。如果您知道这个子网掩码，您可以在此处输入此值。
远程节点 IP 地址	如果您不知道远程节点的 IP 地址，您可以将此处设置为 0.0.0.0（缺省设置），让 ISP 或其它远程路由器动态给您发送这个 IP 地址。如果您知道这个地址（静态的），您可以在此处输入该值。

启用 NAT (网络地址转换)	NAT 技术一般用来作内、外网的地址转换, 以实现节省 IP 地址 的目的。 点选此框可以激活 NAT 的功能。
启用 RIP	点选此框可以启用 RIP (路由信息协议) 的功能, 它可以允许一台路由器和 其它路由器交换路由信息。
RIP 版本	RIP 版本 项控制 ZyWALL 发送 RIP 数据包的格式和广播方式。 选项有 RIP-1, RIP-2B 或 RIP-2M。 RIP-1 是广泛被支持的, 但 RIP-2 可携带更多的信息。RIP-1 对 大多数 网络来说已经足够了, 除非您使用不常用的网络拓扑。RIP-2M 和 RIP-2B 都支持 RIP-2 的路由数据发送格式, 区别是 RIP-2B 使用子网广播方式 而 RIP-2M 使用组播方式。组播会减轻 非路由器设备的负担, 因为它们 一般不会侦听 RIP 组播地址, 因而也不会收到 RIP 数据包。然而一旦有 一台路由器使用组播, 那么网内所有的路由器都要使用组播。
RIP 方向	RIP (路由信息协议) 允许路由器与其它路由器交换路由信息。
	RIP 方向 控制发送和接收 RIP 数据包。 选项包括 Both, None, In only 或 Out only。 当您选择 Both 或 Out only 时, 路由器会周期性地广播路由表。当您选 择 Both 或 In only 时, 路由器会合并其接收到的 RIP 信息。 当选择 None 时, 路由器既不会发送也不会接收任何 RIP 信息。
广播拨号备份路由	点选此框可以将备份路由广播发送到 WAN 上。
启用组播	点选此框可以启用 IGMP 组播协议。
组播版本	您可从下拉菜单中选择 IGMP-v1 或 IGMP-v2。IGMP v2 (RFC2236) 是 在 IGMP v1 (RFC 1112) 基础之上的改进, 但是 IGMPv1 仍然在广泛使 用。如果想要了解关于 IGMP v2 和 IGMP v1 之间互操作性的更详细信 息, 请参考 RFC 2236 的第 4 和第 5 节。
PPP 选项	
PPP 封装	如果您拨号备份的 WAN 设备使用 Cisco PPP 的封装方式, 您可以从下 拉菜单中选择 CISCO PPP。否则请选择 Standard PPP。
启用压缩	点选此框可以使用数据压缩功能。
上网预算	
保持开启	选择此项可以让拨号备份的连接一直保持不断。
配置预算	选择此项可以让拨号备份的连接在您设置的时间段内保持不断。

分配预算 t	输入一个时间数量（以分钟计算），规定在周期区域中配置的时间段内拨号备份的连接可以使用的时间。设置的时间要小于您在周期中设置的值。
周期	输入一个时间段（以小时计算），规定上网预算多久刷新一次。例如，只允许在一小时内对一个远程节点的呼叫最多 10 分钟，那么就需要将 Allocated Budget 设置为 10（分钟）， Period 设置为 1（小时）。
闲置时间	输入一个空闲时间值（如果没有从 ZyWALL 到远程节点的数据），
	规定 ZyWALL 自动断开这个拨号备份连接的等待时间值。如果该处设置为“0”，那么这个拨号备份的连接将不会时间溢出（类似于选择 Always On ）。
应用	点击应用可以保存设置。
重置	点击重置可以重新配置该界面。

7.11 高级模式设置

7.11.1 AT 命令字符串

对于常规电话线路，缺省情况下会使用“Dial”字符串来告诉调制解调器线路使用音频进行拨号，“ATDT”是交换机需要使用音频拨号的命令。如果交换机需要脉冲拨号，将改命令行改为“ATDP”。

ISDN 线路会有更多的协议和操作模式，请参考您 TA 的有关文档。您也许会需要更多的“dial”和“Init”指令字符串。

7.11.2 DTR 信号

多数广域网设备在 DTE 断开 DTR（数据终端准备好）信号时，可挂断当前呼叫。如果您选上“Drop DTR When Hang Up”的时候，**ZyWALL** 会使用这个硬件信号强制广域网设备挂起，而不是使用断开命令“ATH”。

7.11.3 响应字符串

响应字符串在从广域网设备传送不同的呼叫参数之前，通知 **ZyWALL** 标志或标签。响应字符串尚未标准化，请参考广域网设备的有关文档查找到正确的标志。

7.12 配置高级调制解调器的参数

在拨号备份界面中点击编辑按钮，您可以见到高级设置界面。注意：请参考您的拨号备份端口所连 WAN 设备的用户手册来配置 AT 命令。

图 49 高级设置

WAN — 高级Modem设置

AT 指令字符串

拨号

atdt

结束

~++++~ath

应答

ata

☒ 挂断时结束DTR

AT响应字符串

CLID

NMBER =

来话号码

速率

CONNECT

通话控制

拨号闲置时间（秒）

60

重试次数

0

重试区隔（秒）

10

结束闲置时间（秒）

20

回拨延迟（秒）

15

应用

取消

以下为界面相关的描述。

表 34 高级设置

标识	描述
AT 指令字符串	
拨号	输入发起呼叫的 AT 指令字符串。
结束	输入断开呼叫的 AT 指令字符串。“~”代表一个一秒钟的等待，例如，如果模式响应时间较慢，您可以使用“~~~++++~ath”指令。
应答	输入呼叫应答指令。

挂断时结束 DTR	点选此框可以让 ZyWALL 在发出 AT 指令字符串“Drop”的时候断开 DTR 信号。
AT 相应字符串	
CLID	在 AT 响应字符串中的 CLID 之前输入一个关键字。它可以让 ZyWALL 从 WAN 设备发送的 AT 响应字符串中捕获 CLID 值。CLID 用于 CLID 认证。
来话号码	输入呼叫号码之前的关键字。
速率	输入连接速度之前的关键字。
通话控制	
拨号闲置时间 (秒)	输入一个时间值 (以秒为单位), 代表 ZyWALL 在时间溢出之前 (停止呼叫) 尝试向外呼叫的时间。
重试次数	输入一个数值, 规定 ZyWALL 尝试呼叫一个忙线或无应答号码的次数。
重试间隔 (秒)	输入一个时间值 (以秒为单位), 规定了 ZyWALL 在一次呼叫失败后尝试另一次呼叫的等待时间。
结束闲置时间(秒)	输入一个时间值 (以秒为单位), 规定了 ZyWALL 如果没有收到一个肯定的连接断开确认, 在断开 DTR 信号之前的等待时间。
回拨延迟 (sec)	输入一个时间值 (以秒为单位), 规定了 ZyWALL 断开一个回拨请求和呼叫一个回拨电话之间的等待时间。
应用	点击应用可以保存设置。
取消	点击取消可以退出该界面, 不保存设置。

第 8 章 防火墙界面

本章说明如何配置您的 ZyWALL 防火墙。

8.1 防火墙概述

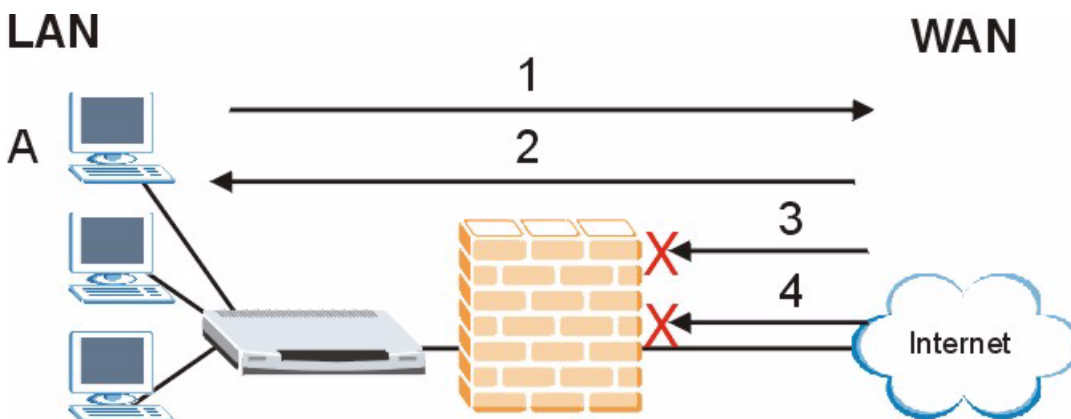
防火墙这个网络术语是指两个网络之间强制执行访问控制策略的一个系统或系统组。它通常是隔离受信任网络和不受信任网络的一种机制。

ZyWALL 从物理上将您私有的本地局域网（LAN）计算机和到互联网的广域网（WAN）连接隔离开，并且充当这两个网络之间通过的数据的一个安全性网关。ZyWALL 可保护网络免受拒绝服务（DoS）攻击，预防盗窃、破坏和修改数据以及日志事件。

- 启用防火墙可保护您的局域网计算机免受互联网上黑客的攻击，并且能够控制 LAN 和 WAN 之间的访问。
- 缺省情况下，防火墙允许始发于您 LAN 计算机的流量，并阻止来自于 WAN 上的流量。
- 您应当仅在您需要限制 LAN 计算机可访问的内容或许可来自 WAN 的访问的时候，对防火墙规则进行配置。

下图说明缺省的防火墙操作。用户 A 可以从 LAN 向 WAN 发起一个 IM（即时消息）会话 (1)。此会话的返回流量也被允许 (2)。但是，其他发起自 WAN 的流量会被阻止 (3 和 4)。

图 50 缺省防火墙操作



您自定义的规则将会超越于 ZyWALL 的缺省设置，具有优先权。ZyWALL 将网络流量的来源 IP 地址、目标 IP 地址以及 IP 协议类型与防火墙规则相比较（按照您列举的顺序）。当流量符合一条规则时，ZyWALL 执行该规则指定的操作。

8.2 防火墙连接方向

防火墙规则按照它们所应用到的数据包的传输方向来分组。缺省情况下，ZyWALL 允许以下列方向传输的数据包：

- **LAN 到 LAN/ZyWALL**

这些规则指定 LAN 上的哪些计算机可以管理 ZyWALL，以及在连接到 LAN 接口的网络或子网之间进行通讯。

注意：您也可以将远程管理设定配置为仅允许某一特定的计算机对 ZyWALL 进行管理。

- **LAN 到 WAN**

这些规则指定 LAN 上的哪些计算机可以访问 WAN 上的哪些计算机和服务。有关示例，请参见第 8.4 节。

缺省情况下，ZyWALL 丢弃以下列方向传输的数据包：

- **WAN 到 LAN**

这些规则指定 WAN 上的哪些计算机可以访问 LAN 上的哪些计算机和服务。例如，您可创建规则以允许：

- 从互联网上特定主机到 LAN 上特定主机的某些类型的流量，如 Lotus Notes 数据库同步。
- 对您的受保护网络上的 WEB 服务器的公共访问。您也可阻止某些 IP 地址对它进行访问。

注意：您也需要配置 NAT 端口转发（或全面的 NAT 地址映射规则）以允许 WAN 上的计算机访问 LAN 上的设备。有关示例，请参见第 14.5.3 节。

- **WAN 到 WAN/ZyWALL**

缺省情况下，ZyWALL 会停止 WAN 计算机管理 ZyWALL，或将 ZyWALL 用作与 WAN 上其他计算机进行通讯的网关。您可配置这些规则之一，以允许 WAN 计算机管理 ZyWALL。

注意：您也需要将远程管理设定配置为仅允许 WAN 计算机对 ZyWALL 进行管理。

8.3 安全性事项

注意：防火墙配置不当可能会阻止有效的访问，或给 ZyWALL 及您的受保护网络带来安全隐患。请在创建或删除防火墙规则时务必小心谨慎，并在创建后对您的防火墙进行测试。

在创建规则前，请先考虑如下安全性分支：

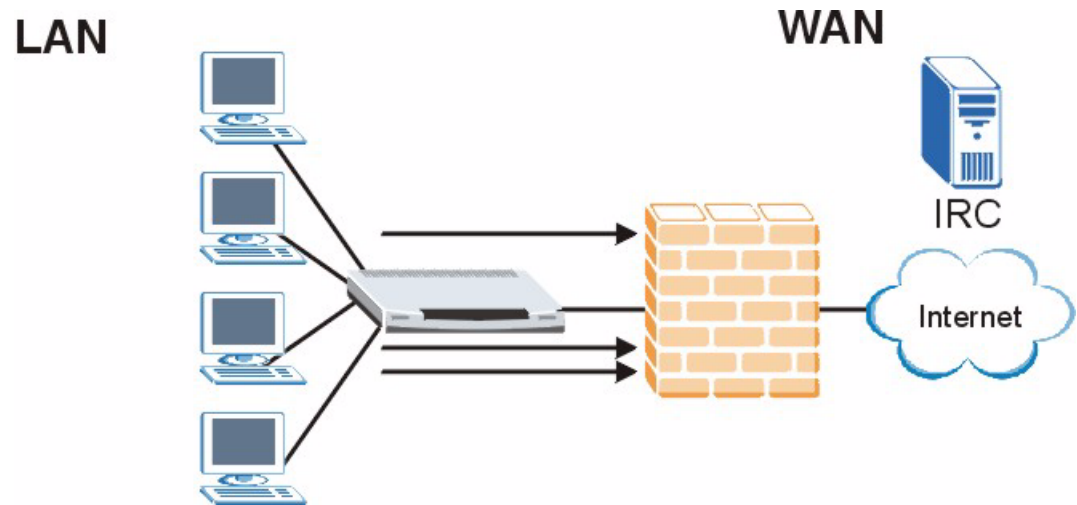
- 1 这条规则会阻止 LAN 用户访问互联网上的重要资源吗？例如，如果要阻止 IRC，是不是有用户需要这项服务？
- 2 有没有可能修改规则，以将规则变得更加具体？例如，如果要阻止所有用户的 IRC，是不是一条仅阻止某些用户的规则更为有效？
- 3 允许互联网用户访问 LAN 上的资源的规则是否会存在受到攻击的弱点？例如，如果允许允许互联网通过 FTP 端口（TCP 20、21）访问 LAN，互联网用户可能会可以连接到 LAN 内部运行着 FTP 服务器的计算机。
- 4 这条规则是否和现有的规则相冲突？

一旦这些问题都解决了，添加规则就变得轻而易举，仅仅是在 web 设置界面上正确的栏位中输入信息而已。

8.4 防火墙规则示例

假设您的公司决定阻止所有 LAN 用户通过互联网使用 IRC（互联网在线聊天）服务。为了进行此操作，您可能会配置一条 LAN 到 WAN 防火墙规则，阻止从任何来源 IP 地址到任何目标地址的 IRC 流量。您不需要指定时间表，因为您需要这条防火墙规则总是有效。下图显示这条规则的结果。

图 51 缺省阻止所有 LAN to WAN IRC 流量示例



您的防火墙具有以下配置。

表 35 缺省阻止所有 LAN to WAN IRC 流量示例

#	来源	目的地	时间表	服务	操作
1	任意	任意	任意	IRC	丢弃
缺省	任意	任意	任意	任意	允许

- 第一行阻止 LAN 访问 WAN 上的 IRC 服务。
- 第二行为防火墙缺省策略，允许来自于 LAN 的所有流量传输到 WAN。

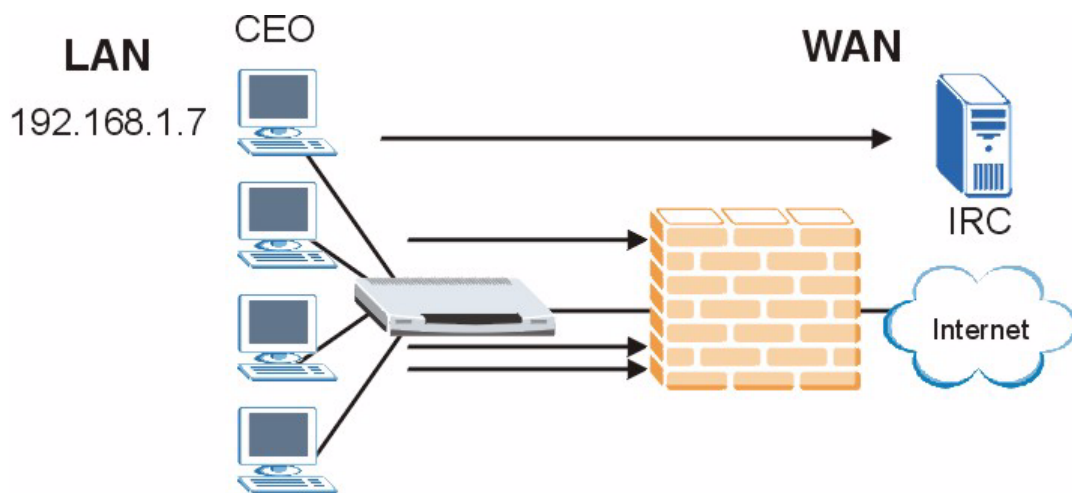
ZyWALL 按照次序应用防火墙规则。因此在本例中，当 ZyWALL 从 LAN 上接收到流量，它先检查第一条规则。如果流量符合（若它是 IRC 流量）该规则，防火墙执行规则中的操作（丢弃），并且停止检查防火墙规则。所有不符合第一条防火墙规则的流量，均符合该缺省规则，ZyWALL 将转发该流量。

现在假设您的公司想要让 CEO 使用 IRC。您可配置一条 LAN to WAN 防火墙规则，允许来自于 CEO 计算机的 IP 地址的 IRC 流量。为了确保 CEO 的计算机总是使用相同的 IP 地址，请务必确保：

- 使用静态 IP 地址，
- 或者，您配置一个静态 DHCP 条目以便 ZyWALL 总会将相同的 IP 地址分配给该计算机（有关静态 DHCP 的信息，请参见第 5.8 节）。

现在您配置一条 LAN to WAN 防火墙规则，允许来自于 CEO 计算机的 IP 地址（例如 192.168.1.7）的 IRC 流量可传输到任何目标地址。您不需要指定时间表，因为您需要这条防火墙规则总是有效。下图显示这两条自定义规则的结果。

图 52 受限的 LAN 到 WAN IRC 流量示例



您的防火墙具有以下配置。

表 36 受限的 LAN to WAN IRC 流量示例

#	来源	目的地	时间表	服务	操作
1	192.16	任意	任意	IRC	允许

2	任意	任意	任意	IRC	丢弃
缺省	任意	任意	任意	任意	允许

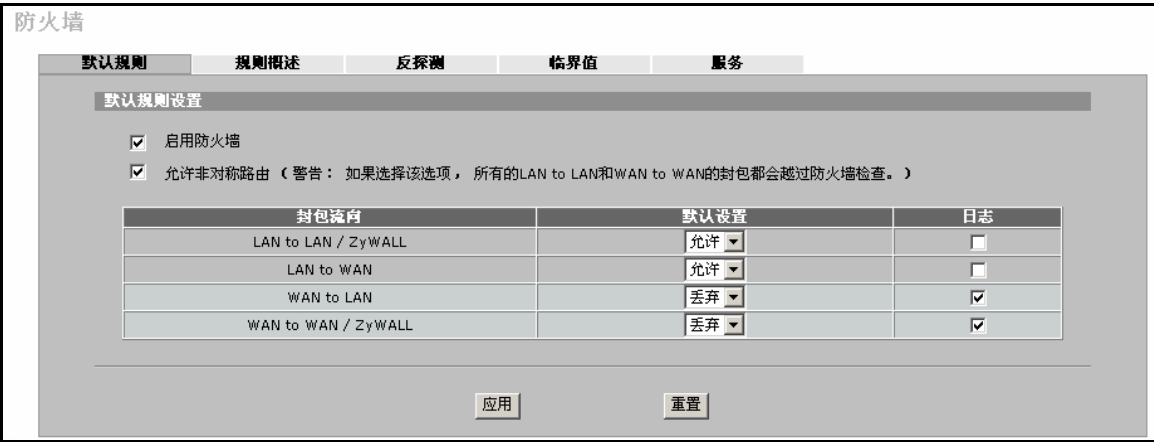
- 第一行允许 IP 地址为 192.168.1.7 的 LAN 计算机访问 WAN 上的 IRC 服务。
- 第二行阻止 LAN 访问 WAN 上的 IRC 服务。
- 第三行为防火墙缺省策略，允许来自于 LAN 的所有流量传输到 WAN。

为 CEO 设定的规则必须放在阻止所有 LAN to WAN IRC 流量的规则的前面。如果将阻止所有 LAN to WAN IRC 流量的规则放在前面，CEO 的 IRC 会符合该规则，ZyWALL 就会丢弃该流量，并且不再检查任何其他防火墙规则。

8.5 防火墙缺省规则（路由模式）

依次点击 安全 > 防火墙，打开默认规则界面。在 ZyWALL 设为路由模式时，使用此界面配置常规防火墙规则。

图 53 防火墙缺省规则（路由模式）



下表说明了此界面中的各个标签。

表 37 防火墙缺省规则（路由模式）

标签	描述
启用防火墙	选中此复选框，激活防火墙功能。当防火墙激活时，ZyWALL 会执行访问控制，防范拒绝服务（DoS）攻击。

允许非对称路由	如果 LAN 上的另一个网关的 IP 地址与 ZyWALL LAN 的 IP 地址在相同的子网中，返回流量可能无法通过 ZyWALL。这称为非对称或者“三角”路由。这会导致 ZyWALL 重新设置连接，因为连接还未被认可。 选中此复选框，允许 ZyWALL 在网络上使用非对称路由拓扑（而不是重设连接）。 注意：允许非对称路由可能会使来自 WAN 的流量不经过 ZyWALL，直接传入 LAN。更好的解决方案是使用 IP 别名，以便将 ZyWALL 和备用网关置于不同的子网内。有关示例，请参见第 8.13 节。
封包流向	该栏位数据包传输方向。 防火墙规则按照它们所应用到的数据包的传输方向来分组。从 LAN 到 LAN 表示数据包从一个 LAN 子网上的一台电脑或一个子网传送到 ZyWALL 的 LAN 接口上的另一台电脑或另一个 LAN 子网或，者 ZyWALL 本身。
默认设置	选择对以指定方向传输并且不符合任意一条防火墙规则的数据包所执行的缺省操作。 选中丢弃可无消息丢弃数据包，而不发送 TCP 重置数据包或“ICMP 目标无法到达”消息给发送者。 选中拒绝，可拒绝数据包，并且发送 TCP 重置数据包（对于 TCP 数据包）或 ICMP 目标无法到达”消息（对于 UDP 数据包）给发送者。 选中允许，可允许数据包通过。
日志	选中此复选框，将所执行的上述操作记录在日志内。
应用	单击应用将所做的更改保存到 ZyWALL。
重置	点击重置开始重新配置此界面。

8.6 防火墙缺省规则（网桥模式）

依次点击 安全 > 防火墙，打开默认规则界面。在 ZyWALL 设为网桥模式时，使用此界面配置常规防火墙规则。

图 54 防火墙缺省规则（网桥模式）

防火墙

默认规则

规则概述

反探测

临界值

服务

默认规则设置

☒ 启用防火墙

封包流向	默认设置	日志	记录广播帧
LAN to LAN / ZyWALL	允许	☐	☒
LAN to WAN	允许	☐	☒
WAN to LAN	丢弃	☒	☒
WAN to WAN / ZyWALL	丢弃	☒	☒

应用

重置

下表说明了此界面中的各个标签。

表 38 防火墙缺省规则（网桥模式）

标签	描述
启用防火墙	选中此复选框，激活防火墙功能。当防火墙激活时，ZyWALL 会执行访问控制，防范拒绝服务（DoS）攻击。
封包方向	该栏位数据包传输方向。 防火墙规则按照它们所应用到的数据包的传输方向来分组。From LAN To LAN 表示数据包从一个 LAN 子网上的一台电脑或一个子网传送到 ZyWALL 的 LAN 接口上的另一台电脑或另一个 LAN 子网或，者 ZyWALL 本身。
默认设置	选择对以指定方向传输并且不符合任意一条防火墙规则的数据包所执行的缺省操作。 选中丢弃可无消息丢弃数据包，而不发送 TCP 重置数据包或“ICMP 目标无法到达”消息给发送者。 选中拒绝，可拒绝数据包，并且发送 TCP 重置数据包（对于 TCP 数据包）或“ICMP 目标无法到达”消息（对于 UDP 数据包）给发送者。 选中允许，可允许数据包通过。
日志	选中此复选框，将所执行的上述操作记录在日志内。

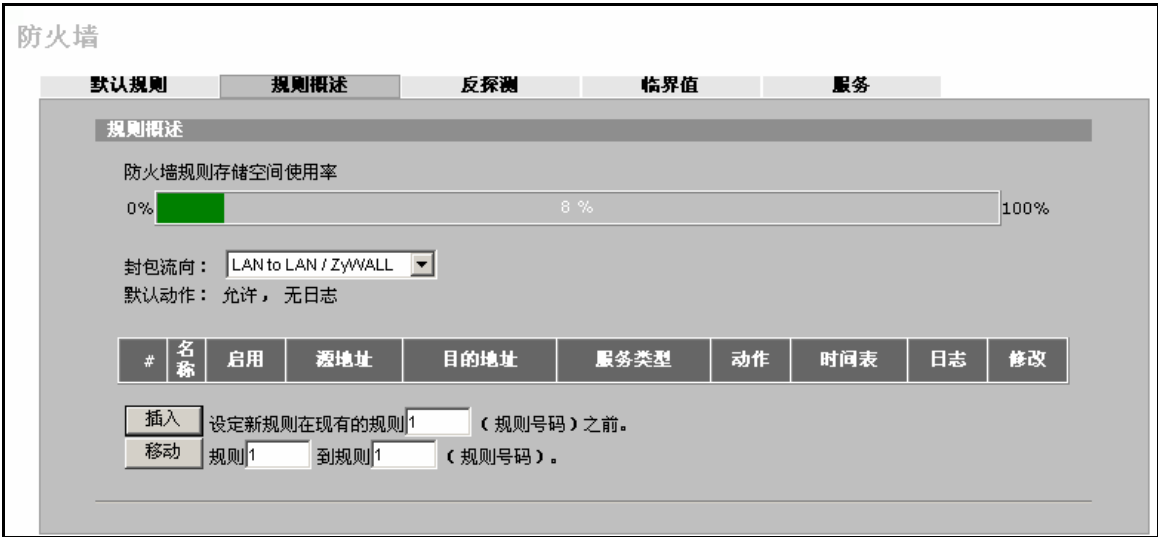
记录广播帧	选中此复选框，为任何以选定方向传输的广播数据帧记录日志。 较短时间内的大量此类日志，可能表示广播风暴。广播风暴在数据包引发一个网络内所有主机的多个响应时发生，或者在计算机尝试响应到永远不可能回应的主机时发生。其结果就是，重复的数据包不断地被创建并且在网络中循环，造成网络性能的降低或者甚至使网络无法运行。广播风暴可由对网络的攻击、网络拓扑设置不正确（例如网桥环路）或网络设备故障引起。
应用	单击应用将所做的更改保存到 ZyWALL。
重置	点击重置开始重新配置此界面。

8.7 防火墙规则汇总

依次点击安全 > 防火墙 >规则概述，打开该界面。本界面显示您所配置的防火墙规则的一个列表。

注意：由于规则的应用是根据所列顺序的，所以您的规则排序非常重要。

图 55 规则概述界面



下表说明了此界面中的各个标签。

表 39 规则概述

标签	描述

防火墙规则存储 空间使用率	此进度条显示 ZyWALL 防火墙规则存储量当前使用的百分比。当数值接近最大时，进度条会由绿色变成红色。当进度条变为红色时，您应当先考虑删除不必要的防火墙规则，再添加新的规则。
封包流向	使用下拉列表选择您要配置防火墙规则的数据包传输方向。
默认策略	此栏位显示您在默认规则为上面的栏位所对应的数据包方向所选定的缺省操作以及日志策略。
下列只读栏位汇总了您创建的应用到选定数据包方向传输的流量的规则。您所配置的防火墙规则（下方汇总的规则）要优先于上面所列常规防火墙操作设置。	
#	这是防火墙规则号。由于规则是按照次序应用的，因而您的规则排序也非常重要。点击“+”展开，或者“-”折叠源地址、目标地址和服务类型下拉列表。
名称	该栏位显示防火墙规则名称。
启用	此栏位显示防火墙处于开启（Y）或关闭（N）状态。
源地址	此下拉列表显示该防火墙规则所应用的来源地址或来源地址范围。请注意来源地址或目标地址栏空白等同于“任何”。
目标地址	此下拉列表显示该防火墙规则所应用的目标地址或目标地址范围。请注意来源地址或目标地址栏空白等同于“任何”。
服务类型	此下拉列表显示该防火墙规则所应用的服务。有关常用服务，请参见附录 E。
动作	此栏位显示防火墙是无消息丢弃数据包（丢弃）、丢弃数据包并且发送 TCP 重置数据包或“ICMP 目标无法到达”消息给发送者（拒绝），还是允许数据包通过（允许）。
时间表	此栏位显示时间表是开启（Y）或关闭（N）状态。
日志	此栏位显示当数据包符合此规则时是否记录在日志里：“是”或“否”。
修改	点击编辑图标，进入您可对该规则进行编辑的界面。 点击删除图标，删除一条现有的防火墙规则。将会显示一个窗口，询问您是否确定要删除该防火墙规则。请注意您执行该操作后，所有后续防火墙规则将顺序上移。
插入	输入您要将防火墙规则放入的序列号。例如，如果您输入 6，新规则将是第 6 条规则，而原先的第 6 条规则（若有的话）将变为第 7 条。 点击插入，显示此界面，并参照以下表格，获取有关栏位的信息。

移动	输入您规则的序列号，以及您要将该规则放入的位置的号码。点击 Move ，将该规则移动到您刚输入的号码位置。由于规则是按照次序应用的，因而您的规则排序也非常重要。

8.7.1 编辑防火墙规则

按照下列指导，创建新的规则。

- 1 在规则概述界面中，输入您要将规则放入位置的序列号。例如，如果您输入 **6**，新规则将是第 **6** 条规则，而原先的第 **6** 条规则（若有的话）将变为第 **7** 条。
- 2. 点击插入，显示防火墙编辑规则界面，并参照以下表格，获取有关栏位的信息。

表 56 编辑防火墙规则

防火墙—编辑规则

规则名称

编辑源地址

地址编辑

地址类型

起始 IP 地址

结束 IP 地址

子网掩码

源地址

编辑目的地址

地址编辑

地址类型

起始 IP 地址

结束 IP 地址

子网掩码

目的地址

编辑服务

现有服务 (参见 [服务](#))

Any(All)
Any(TCP)
Any(UDP)
Any(ICMP)
AIMNEW_ICQ(TCP:5190)
AUTH(TCP:113)
BGP(TCP:179)
BOOTP_CLIENT(UDP:68)
BOOTP_SERVER(UDP:67)
CU-SEEME(TCP/UDP:7648,24032)
DNS(TCP/UDP:53)
FINGER(TCP:79)
FTP(TCP:20,21)
H.323(TCP:1720)
HTTP(TCP:80)

<< >>

已选服务

编辑日程

应用日期：

☒ 周日 ☒ 周一 ☒ 周二 ☒ 周三 ☒ 周四 ☒ 周五 ☒ 周六

当日应用时刻：（24 小时制）

☒ 全天

开始： (小时) (分钟) 结束： (小时) (分钟)

当匹配时的动作

☐ 比对符合时将封包信息记入日志

☐ 符合时将警示邮寄给管理人

封包比对符合时之动作

下表说明了此界面中的各个标签。

表 40 编辑防火墙规则

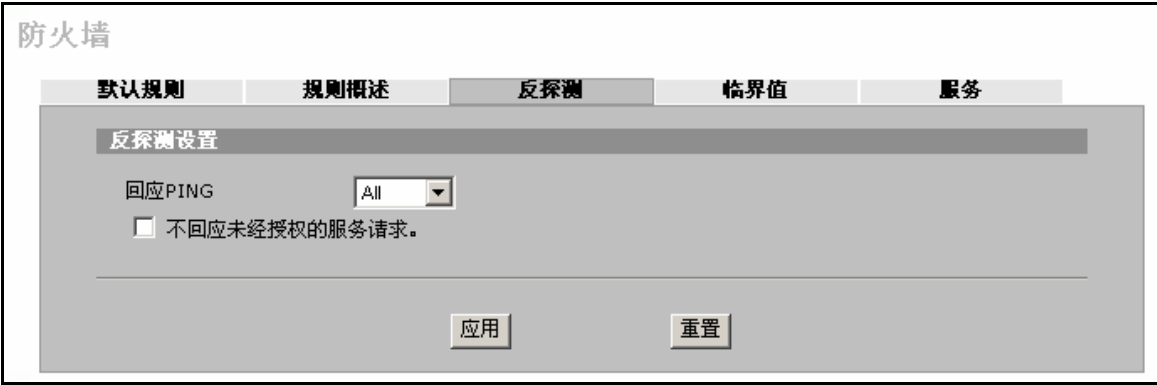
标签	描述
规则名称	输入一个防火墙规则的描述性名称（最多 31 个可打印 ASCII 字符，除扩展 ASCII 字符外），允许空格。
编辑源/目的地址	
地址类型	您是否希望将您的规则应用到某个（单个）IP 地址、一个网段的 IP 地址（例如 192.168.1.10 到 192.169.1.50）、一个子网或任何 IP 地址？可从下拉列表中选择一个该规则适用的范围：单一 IP 地址、指定 IP 段地址、IP 子网 地址和任何地址。
起始 IP 地址	输入单个 IP 地址，或一个 IP 网段的起始 IP 地址。
结束 IP 地址	输入一个 IP 网段的末尾 IP 地址。
子网掩码	输入子网掩码地址（若适用）。
添加	点击 Add 在源或目的地址栏中添加一个新地址。您可以添加多个 IP 地址、一段 IP 地址和/或一个子网段。
修改	若要编辑一个现有的来源或目标 IP 地址，从列表中将它选中，再点击修改。
删除	在源或目的地址(es)框中高亮显示一个现有的来源或目标 IP 地址，然后点击删除即可将它删除。
编辑服务	
现有/已选服务	从左侧的现有服务 s 框中高亮显示您需要的服务，再点击 >> 将它添加到右侧的已选服务框中。若要移除服务，则从右侧的已选服务(s)框中高亮显示您需要的服务，再点击 << 即可。 在服务名称的旁边的括号内会显示两个字段。第一个字段表示 IP 协议类型（TCP、UDP 或 ICMP）。第二个字段表示定义该服务的 IP 端口号。（请注意，可能会有一个以上 IP 协议类型。）例如，请看一下 DNS 条目，(UDP/TCP:53) 表示 UDP 端口 53 和 TCP 端口 53。点击服务链接进入服务界面，在该界面中您可配置自定义服务端口。有关常用服务和端口号，请参见附录 E。
编辑日程	
应用日期	选择该规则每周应用的日期：每日或星期几。

当日应用时刻 (24-小时制)	设置应用该规则的时间：选择全天，或输入开始和截至的时刻（以小时一分钟为格式）。
当匹配时动作	
比对符合时将封包信息记入日志	此栏位显示当数据包符合此规则时是否记录在日志里：是（Yes）或否（No）。可进入日志设置页面，选择存取控制日志类别，将 ZyWALL 设定为记录这些日志。
符合时将警讯邮寄给管理人	选中此复选框，可将 ZyWALL 设为在数据包符合防火墙规则时生成一个报警信息。
封包对比符合时动作	使用下拉列表选择在数据包符合此规则时防火墙应执行的操作。 选中丢弃可无消息丢弃数据包，而不发送 TCP 重置数据包或“ICMP 目标无法到达”消息给发送者。 选中拒绝，可拒绝数据包，并且发送 TCP 重置数据包（对于 TCP 数据包）或“ICMP 目标无法到达”消息（对于 UDP 数据包）给发送者。 选中允许，可允许数据包通过。 注意：您也需要配置 NAT 端口转发（或全面的 NAT 地址映射规则）以允许 WAN 上的计算机访问 LAN 上的设备。 注意：您也需要将远程管理设定配置为仅允许 WAN 计算机对 ZyWALL 进行管理。
应用	单击应用保存您的自定义设置并退出该界面。
取消	单击取消以退出此界面，不保存任何更改。

8.8 反探测

依次点击安全 > 防火墙 > 反探测，打开下图所示界面。配置此界面，将有助于 ZyWALL 将自身隐藏而不被探测到。您可指定 ZyWALL 的哪个接口对 Ping 请求作出响应，以及 ZyWALL 是否响应对其未被使用端口的探测。

图 57 反探测



下表说明了此界面中的各个标签。

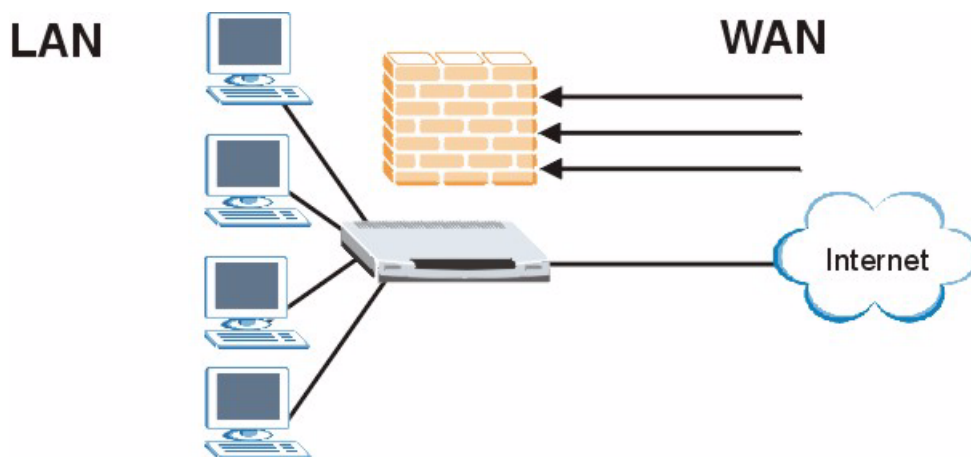
表 41 反探测

标签	描述
回应 PING	选择您要回应进入 Ping 请求的接口。 选择 Disable 使 ZyWALL 不回应任何进入的 Ping 请求。
不回应未经授权的服务请求.	选中此选项可防止黑客通过探测未使用端口来查找 ZyWALL。如果您选中此选项，ZyWALL 将不会响应对未知端口的请求，因而可让这些未使用端口和 ZyWALL 保持不可见状态。如果不选中此选项，对于未使用的 UDP 端口，ZyWALL 将会对此端口的探测回应一个 ICMP 端口不可到达的数据包，而对于未使用的 TCP 端口，ZyWALL 将会对此端口的探测回应一个 TCP 重置数据包。 请注意，这种探测数据包首先会经过 ZyWALL 的防火墙机制，然后才到达反探测机制。因此，如果防火墙机制中会阻挡一个探测数据包，那 ZyWALL 就会按照防火墙的规则做出反应：对于拦截的 TCP 数据包，发送一个 TCP 重置数据包（对于拦截的 UDP 数据包则发送一个 ICMP 不可到达数据包），或仅丢弃该数据包而不发出响应数据包。
应用	单击应用将所做的更改保存到 ZyWALL。
重置	点击重置开始重新配置此界面。

8.9 拒绝服务（DoS）攻击

拒绝服务（DoS）攻击针对的是连接到互联网的设备和网络。它们的目标不是为了窃取信息，而是为了禁用设备或网络，使得用户无法再访问网络资源。ZyWALL 预置为自动探测和防御目前所知的 DoS 攻击。

图 58 ZyWALL 防火墙应用

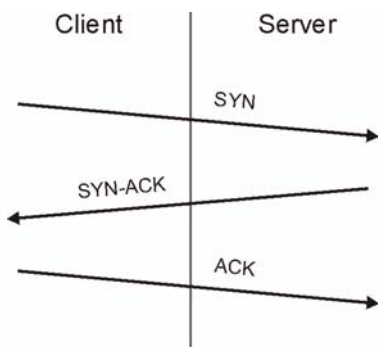


8.10 防火墙门限

对于拒绝服务（DoS）攻击，ZyWALL 使用门限值来决定何时开始丢弃尚未处于“完全建立”状态的会话（半开放会话）。这些门限值对所有会话全局有效。

对于 TCP，半开放表示会话还未达到已建立的状态 —TCP 三方握手还未完成。通常情况下，发起会话的应用程序会发送一个 SYN（同步）数据包到接收服务器。接收服务器发回一个 ACK（认可）数据包以及它自身的 SYN 数据包，然后发起者再回应一个 ACK 数据包。此握手完成后，一个连接就建立了。

图 59 三方握手



对于 UDP，半开放表示防火墙没有探测到返回流量。半开放会话的数量（或到达率）高于正常值，可能表示存在 DOS 攻击。

8.10.1 门限值

如果一切都运行正常，您可能不需要更改门限值设置，因为缺省门限值可以满足大多数的小型企业的需求了。如果您觉得 ZyWALL 正接收到 DoS 攻击但未能记录在日志里，或者日志

显示 ZyWALL 正将正常的流量识别为 DoS 攻击，那就需要调整这些参数。影响门限值选择的因素有：

- 1 开放会话的最大数量。
- 2 LAN 中服务器任务积压的最小能力。
- 3 LAN 中服务器 CPU 的能力。
- 4 网络带宽。
- 5 某些服务器的流量类型。

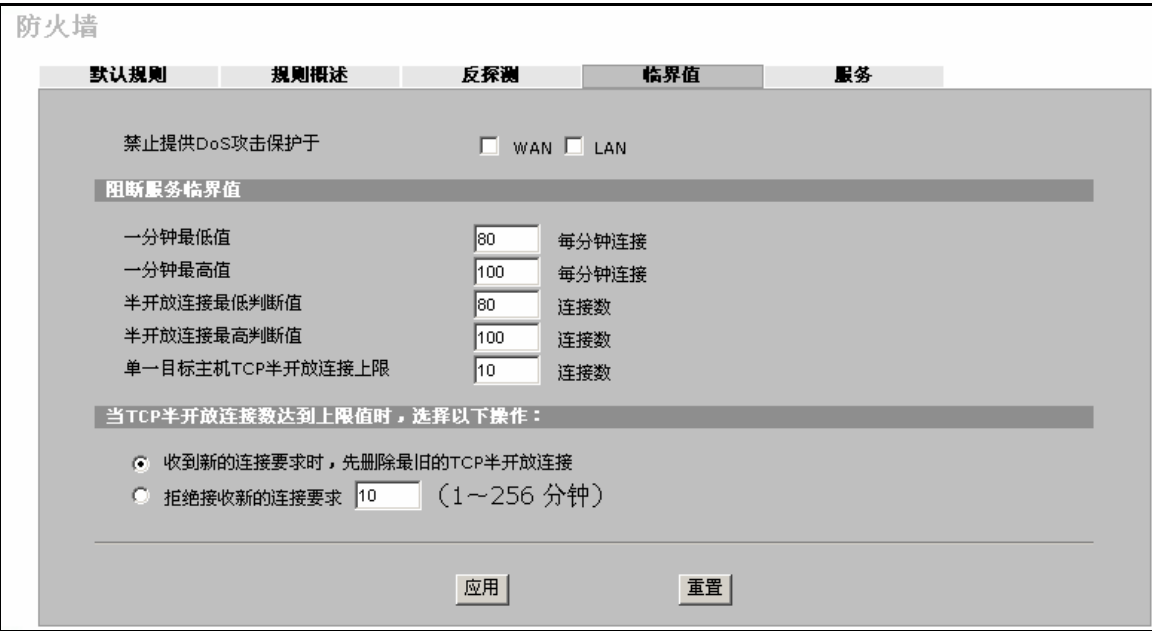
如果您的网络由于这些因素（特别是有一些服务器速度慢或处理太多任务，工作繁忙）比通常情况下要慢，则需要降低门限值。

如果您经常使用 P2P 应用程序，例如使用 eMule 或 eDonkey 共享文件，建议您提供门限值。这是因为这些应用程序会在短时间内建立许多个会话，ZyWALL 可能会将它们识别为 DoS 攻击。

8.11 Threshold 界面

依次点击安全 > 防火墙 > 临界值，打开下图所示界面。在该界面指定门限的全局值，以及应用到所有 TCP 连接的超时值。

图 60 防火墙门限



下表说明了此界面中的各个标签。

表 42 防火墙门限

标签	描述
禁止提供 Dos 攻击保护于	选中接口的复选框，ZyWALL 不将门限值应用到此接口。这将对选定的接口禁用 Dos 攻击保护。
阻断服务临界值	ZyWALL 会同时测量现有半开放会话的总数以及会话建立尝试的速率。在总数和比例的测量中，TCP 和 UDP 半开放会话均会计算在内。测量每分钟进行一次。
一分钟最低值	这是新半开放会话的建立速率，它会触发防火墙停止删除半开放会话。除非新建连接的速率降到此值以下，否则 ZyWALL 会持续删除半开放会话。
一分钟最高值	这是新半开放会话的建立速率，它会触发防火墙开始删除半开放会话。当新建连接的速率高于此值时，ZyWALL 会开始删除半开放会话，以便接收新建连接请求。例如，如果您将一分钟最高值设为 100，当 ZyWALL 在上一分钟内探测到的会话建立尝试超过 100 时，即开始删除半开放会话。而当所测到的会话建立尝试的数量低于在一分钟最低值中设的值时，ZyWALL 则停止删除半开放会话。
半开放连接最低判断值	这是现有半开放会话数量，它会触发防火墙停止删除半开放会话。除非现有半开放会话数量降到此值以下，否则 ZyWALL 会持续删除半开放会话。
半开放连接最高判断值	这是现有半开放会话数量，它会触发防火墙开始删除半开放会话。当现有半开放会话数量高于此值时，ZyWALL 会开始删除半开放会话，以便接收新建连接请求。请勿将半开放连接最高判断值设为低于半开放连接最低判断值中的值。例如，如果您将半开放连接最高判断值设为 100，当现有半开放会话数量超过 100 时，ZyWALL 开始删除半开放会话；而当现有数量低于半开放连接最低判断值中设的值时，ZyWALL 停止删除半开放会话。
当 TCP 半开放连接数达到上限值时，选择以下操作	具有相同目标主机地址的半开放会话数量超过寻常值时，可能表示该主机已被发起拒绝服务攻击。 指定具有相同目标主机 IP 地址的现有半开放 TCP 会话数量，它会触发防火墙开始丢弃具有该目标主机 IP 地址的半开放会话。输入 1 到 256 之间的一个数字。一般规则为，对较小的网络、较慢的系统或有限的带宽，应选择较小的数字。当超过 TCP 半开放连接上限时，ZyWALL 会发出报警。 您也需要选择当达到 TCP 半开放连接上限门限值时，ZyWALL 应执行的操作。您可以将 ZyWALL 设为： 在新连接请求进入时删除最旧的半开放会话。 或者在您指定的分钟数（1 到 256 分钟）内拒绝新连接请求。

应用	单击应用将所做的更改保存到 ZyWALL。
重置	点击重置开始重新配置此界面。

8.12 服务

次点击 安全 > 防火墙，然后点击服务，打开如下图所示界面。使用此界面配置在防火墙规则中使用的自定义服务，或者查看在 ZyWALL 中预定义的服务。

图 61 防火墙服务

防火墙

默认规则

规则概述

反探测

临界值

服务

自定义服务

#	服务名称	协议	属性*	修改
*属性：TCP/UDP的端口号，ICMP的类型/代码。				
添加				

预定义服务

#	服务名称	协议	属性
1	Any_All	ALL	-
2	Any_TCP	TCP	1~65535
3	Any_UDP	UDP	1~65535
4	Any_ICMP	ICMP	-
5	AIM/NEW_ICQ	TCP	5190
6	AUTH	TCP	113
7	BGP	TCP	179
8	BOOTP_CLIENT	UDP	68
9	BOOTP_SERVER	UDP	67
41	RTELNET	TCP	107
42	RTSP	TCP/UDP	554
43	SFTP	TCP	115
44	SIP-V2	UDP	5060
45	SMTP	TCP	25
46	SNMP	TCP/UDP	161
47	SNMP-TRAPS	TCP/UDP	162
48	SQL-NET	TCP	1521
49	SSDP	UDP	1900
50	SSH	TCP/UDP	22
51	STRMWORKS	UDP	1558
52	SYSLOG	UDP	514
53	TACACS	UDP	49
54	TELNET	TCP	23
55	TFTP	UDP	69
56	VDOLIVE	TCP	7000
57	Microsoft RDP	TCP	3389
58	VNC	TCP	5900
59	NTP	TCP/UDP	123

下表说明了此界面中的各个标签。

表 43 防火墙服务

标签	描述
自定义服务	此表格显示所配置的自定义服务。
#	此为自定义服务的索引号。
服务名称	此为服务的名称。
协议	此处显示 IP 协议类型。 如果您选择了自定义，则此栏为您所输入的 IP 协议值。
属性	此处为定义该服务的 IP 端口号或 ICMP 类型和代码。
修改	点击编辑图标，进入您可对该服务进行编辑的界面。 点击删除图标，删除一个现有的服务。将会显示一个窗口，询问您是否确定要删除该服务。请注意您执行该操作后，所有后续服务将会顺序上移动。
添加	点击该按钮，打开一个界面，在该界面配置一个不在预定义服务列表中的新自定义服务。
预定义服务	该表格显示所有已在防火墙规则配置的服务。有关常用服务，请参见附录 E。
#	此为预定义服务的索引号。
服务名称	此为服务的名称。
协议	此处显示 IP 协议类型。可能会有一个以上 IP 协议类型
属性	此处为定义该服务的 IP 端口号或 ICMP 类型和代码。

8.12.1 编辑防火墙自定义服务

点击自定义服务下的添加按钮，打开如下图所示界面。使用此界面配置未在 ZyWALL 中预定义的自定义服务条目。有关常用服务和端口号，请参见附录 E。

图 62 编辑防火墙自定义服务

防火墙 — 编辑规则 — 编辑自订服务

自定义服务

服务名称

IP协议

TCP/UDP

端口范围

从 0 到 0

应用

取消

下表说明了此界面中的各个标签。

表 44 编辑防火墙自定义服务

标签	描述
服务名称	为自定义服务输入一个描述性名称（最多 31 个可打印 ASII 字符，除扩展 ASCII 字符外），不可使用“(”字符，但可使用空格。
IP 协议	从下拉列表中选择定义您的自定义服务的 IP 协议（TCP、UDP、TCP/UDP、ICMP 或 Custom。
端口范围	输入定义自定义服务的端口号（自 1 到 255）。 若要仅指定一个端口，请在从栏输入端口号，然后在到栏内再次输入该号码。 若要指定一个端口范围，请在从栏输入起始端口号，然后在到栏内输入终止端口号。
类型/代码	只有您在 IP 协议栏内选择 ICMP 时，此栏位才可用。 ICMP 信息通过它们的类型，以及某些情况下它们的代码进行标识。在类型栏内输入类型号码，并且点击代码按钮，再输入代码（若有）。
应用	单击应用保存您的自定义设置并退出该界面。
取消	单击取消以退出此界面，不保存任何更改。

8.13 解决非对称路由问题示例

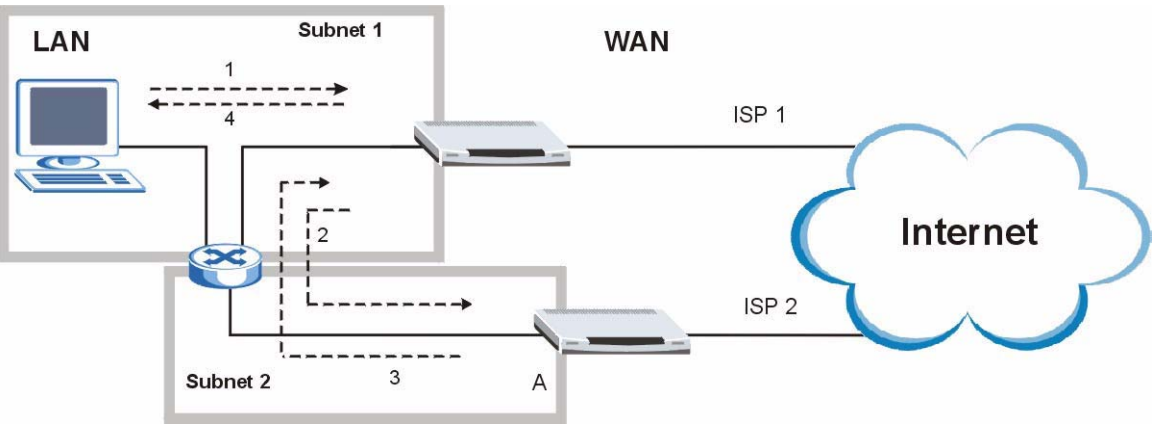
如果您将 ZyWALL 设为允许非对称路由会话，来自 WAN 上的流量将能够不经过 ZyWALL 及其防火墙保护，而直接进入 LAN 计算机。

另一个解决方案是使用 IP 别名。您可以通过 IP 别名功能将您的网络分隔成以太网接口上的多个逻辑区段。您的 ZyWALL 支持最多 3 个逻辑 LAN 接口，并且 ZyWALL 可用作每个罗机网络的网关。

这实际上使您在相同的物理网线和端口上拥有多个 LAN 网络。通过将您的 LAN 和网关 A 放在不同的子网内，所有返回网络流量就必须通过 ZyWALL 才能进入您的 LAN。以下步骤说明了这一方案。

- 1 LAN 上的一台计算机通过发送 SYN 数据包到 LAN 上的接收服务器，发起一个连接。
- 2 ZyWALL 将数据包重定路由至网关 A，网关 A 在 IP 子网 2 中。
- 3 来自 WAN 上的响应传送到 ZyWALL。
- 4 ZyWALL 再将它发送到 LAN 上的计算机（IP 子网 1 中）。

图 63 IP 别名

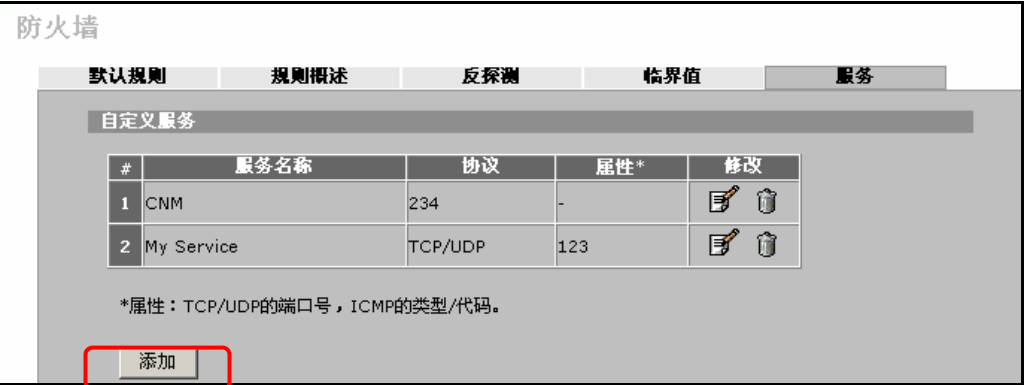


8.14 我的服务防火墙规则示例

下面是一个互联网防火墙规则示例，它允许互联网上的用户连入一个假想的“我的服务”。

- 1 在服务界面中，点击添加打开编辑自定义服务界面。

图 64 我的服务防火墙规则示例：服务



- 2 按如下所示进行配置，再点击应用。

图 65 我的服务防火墙规则示例：编辑自定义服务



- 3 点击规则概述。从数据包方向下拉列表选择 WAN 到 LAN。
- 4 在规则概述界面中，输入您要将规则放入位置的序列号。例如，如果您输入 6，新规则将是第 6 条规则，而原先的第 6 条规则（若有的话）将变为第 7 条。
- 5 点击插入，打开防火墙规则配置界面。

图 66 我的服务防火墙规则示例：规则概述



- 6 输入防火墙规则的名称。
- 7 在目的地址框中选择 Any，再点击删除。
- 8 按如下所示配置目标地址栏位，再点击添加。

图 67 我的服务防火墙规则示例：编辑规则

防火墙 - 编辑规则

规则名称Ex1

编辑源地址

地址编辑

地址类型Any Address

起始 IP 地址0 . 0 . 0 . 0

结束 IP 地址0 . 0 . 0 . 0

子网掩码0 . 0 . 0 . 0

添加修改

源地址Any

删除

编辑目的地址

地址编辑

地址类型Any Address

起始 IP 地址0 . 0 . 0 . 0

结束 IP 地址0 . 0 . 0 . 0

子网掩码0 . 0 . 0 . 0

添加修改

目的地址Any

删除

9 在编辑规则界面中，使用可用服务和已选服务之间的箭头进行配置，如下图所示。完成后，点击应用。

注意：在服务 s 列表和规则概述列表中，自定义的服务名称之前会显示“*”号。

图 68 我的服务防火墙规则示例：规则配置。

防火墙—编辑规则

规则名称

Ex1

编辑源地址

地址编辑

地址类型

Any Address

起始 IP 地址

0 . 0 . 0 . 0

结束 IP 地址

0 . 0 . 0 . 0

子网掩码

0 . 0 . 0 . 0

添加

修改

源地址

Any

删除

编辑目的地址

地址编辑

地址类型

Any Address

起始 IP 地址

0 . 0 . 0 . 0

结束 IP 地址

0 . 0 . 0 . 0

子网掩码

0 . 0 . 0 . 0

添加

修改

目的地址

10.10.0.10 - 10.10.0.15

删除

编辑服务

现有服务 (参见 服务)

^CNM(IP:234)

Any(All)

Any(TCP)

Any(UDP)

Any(ICMP)

AIM/NEW_ICQ(TCP:5190)

AUTH(TCP:113)

BGP(TCP:179)

BOOTP_CLIENT(UDP:68)

BOOTP_SERVER(UDP:67)

CU-SEEME(TCP/UDP:7648,24032)

DNS(TCP/UDP:53)

FINGER(TCP:79)

FTP(TCP:20,21)

H.323(TCP:1720)

已选服务

*My Service(TCP/UDP:123)

<

>

编辑日程

应用日期：

☒周日☒周一☒周二☒周三☒周四☒周五☒周六

当日应用时刻：（24 小时制）

☒全天

开始：0（小时）0（分钟）

结束：0（小时）0（分钟）

当匹配时的动作

☐ 比对符合时将封包信息记入日志

☐ 符合时将资讯邮寄给管理人

封包比对符合时之动作

允许

应用

取消

规则 1 将允许从 WAN 到 LAN 上的 10.0.0.10 至 10.0.0.15 的 IP 地址的我的服务连接。

图 69 我的服务防火墙规则示例：规则概述

防火墙

默认规则

规则概述

反探测

临界值

服务

规则概述

防火墙规则存储空间使用率

0%12 %100%

封包流向：WAN to LAN

默认动作：丢弃 日志

#	名称	启用	源地址	目的地址	服务类型	动作	时间表	日志	修改
1	Ex1	Y	Any	10.10.0.10 - 10.10.0.15	*My Service(TCP/UDP:123)	允许	No	No	 
2	W2L_Rule_1	N	Any	Any	BOOTP_CLIENT(UDP:68)	允许	No	No	 
3	W2L_Rule_2	N	Any	Any	NetBIOS(TCP/UDP:137~139,445)	允许	No	No	 

插入

移动

设定新规则在现有的规则1 (规则号码) 之前。

规则1 到规则1 (规则号码)。

第 9 章 内容过滤界面

本章对内容过滤作了概述。

9.1 内容过滤概述

内容过滤允许你阻止某些网络特征，例如启用X 控件，Java applets，cookies，以及屏蔽代理服务器等。ZyWALL可以阻止或允许对指定网站访问，还可以阻止包含你指定关键字的网站。你可以指定内容过滤的时间及日期，以及在局域网中使用或不使用内容过滤的用户范围。

你也能制订基于分类的内容过滤，来允许ZyWALL对照一个具有百万网站动态更新率的外部数据库检查网站。

9.1.1 限制 web 特征

ZyWALL 可以阻止的 web 特征包括，启用X 控制，Java applets，cookies 和禁用web 代理。

9.1.2 创建一个过滤列表

您可以在一个预定义列表中选择需要阻止浏览的类别，例如色情或种族歧视。

9.1.3 过滤规定的 web 站点

您的 ZyWALL 可以根据在 web 站点内容中规定的 URL 地址或一些关键字来阻止或允许接入到某些 web 站点。

9.2 内容过滤常规信息的配置

依次点击**安全, 内容过滤**, 您可以打开**内容过滤 常规**界面。您可在该界面中启用内容过滤的功能，配置一个时间策略和创建一个拒绝信息。您也可以选择规定的计算机使用内容策略或选择规定的计算机不使用内容策略。

图 70 内容过滤：基本

内容过滤

常规

类别

定制

缓存

常规设置

☒ 启用内容过滤

限定Web功能

拦截

☐ ActiveX

☐ Java Applet

☐ Cookies

☐ Web Proxy

时间表设定

☒ 永远阻挡

☐ 阻挡从 : 到 : (24 小时制)

Web被阻挡时的显示信息

阻挡服务信息

URL重定向

不受限的电脑

☒ 对所有电脑实施内容过滤策略

☐ 对指定地址范围的电脑应用内容过滤

☐ 在使用内容过滤时排除指定地址范围

新增地址范围

从

到

添加范围

地址清单

排除范围

应用

重置

以下为界面相关的描述。

表 45 内容过滤：基本

标识	描述
常规设置	
启用内容过滤	点选此框可以、激活内容过滤的功能。
限定Web功能	点选某一个选框可以限制相应的特征。当您下载的页面中包含了一个被限制的特征的时候,web页面的区域会显示空白或输出灰色。
拦截 ActiveX	ActiveX是一种可以创建动态和活动的 web 页面和分布式目标应用的工具。当您浏览一个支持ActiveX的web站点的时候,ActiveX控件就会下载到您的浏览器中,一旦您再次浏览该页面,它们还会保留。
Java	Java是一种编程语言,用于建立各种可下载的web内容或Internet和Intranet的商业应用。

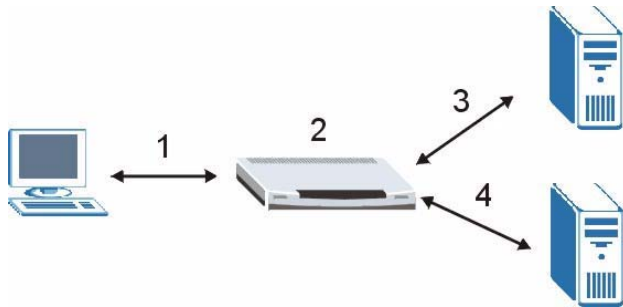
Cookies	Cookies 就是存储在计算机硬盘上的文件。一些 web 服务器会使用它们来做使用跟踪和提供基于 ID 的服务。
Web Proxy	处于一个用户和 Internet 之间的一台服务器可以提供安全保障，管理控制和缓存等服务。当一台代理服务器位于 WAN 上的时候，LAN 上的用户可以通过指向这台代理服务器来访问一些被 ISP 禁止访问的 web 站点。
时间表设定	规定内容过滤列表有效的时间段。
永远阻挡	选择此项可以让内容过滤全天有效。这是缺省选项。
阻挡从/到	选择此项可以规定一个内容过滤有效的时间段。在阻挡从和到区域中，您可以输入这个时间段信息。
Web被阻挡时的显示信息	
阻挡服务信息	输入一条信息，当用户尝试接入一个被禁止的 web 站点的时候，此信息会显示给用户。缺省信息是“Please contact your 网络 administrator！”。
不受限的电脑	
对所有电脑实施内容过滤策略	选择此项可以让LAN上所有的用户都遵守此内容过滤策略（缺省）。
对指定地址范围的电脑应用内容过滤	选择此项可以让LAN上规定范围中的用户都遵守此内容过滤策略。
在使用内容过滤时排除指定地址范围	选择此项可以让 LAN上规定范围以外的用户都遵守此内容过滤策略。
新增地址范围	
从	输入 LAN 上规定用户范围的起始 IP 地址。
到	输入 LAN 上规定用户范围的最后一个 IP地址，然后点击添加范围按钮。
地址清单	此文本框可以显示您所规定的地址范围。
添加范围	当您配置好上面的从和到域后，点击添加范围按钮。
排除范围	当您选择好准备删除的地址范围之后，点击排除范围按钮。
应用	点击应用可以保存设置。

重置	点击 重置 可以重新配置该界面。

9.3 基于分类的内容过滤（Category Based 内容过滤 ing）

具有一个外部数据库的内容过滤您的 ZyWALL 可以使用一个应用服务提供商提供的外部内容过滤服务。如果您应用了此过滤服务功能，您的 ZyWALL 会接入到一个外部的数据库，它可以动态更新数以百万的 web 站点。内容过滤的查询流程请见下图。

图 71 内容过滤查询流程



1. ZyWALL 后面的计算机准备访问一个 web 站点。
2. ZyWALL 在本地数据库中查询 web 站点的信息。如果过去曾经尝试访问过某些 web 站点，那么这些站点的种类情况就会记录在 ZyWALL 的缓存当中。ZyWALL 会根据您配置的策略来阻止或允许这些请求信息的发送。
3. 您可以在**内容过滤 缓存**界面中配置一个曾经被访问过的web站点地址可以在内容过滤缓存当中保存多长的时间。当内容过滤缓存时间溢出的时候ZyWALL会将此web站点的记录从内容过滤缓存中删除。当ZyWALL 重新启动的时候，所有的 web 站点地址记录会从本地缓存中清除掉。
4. 如果 ZyWALL 没有此 web 站点的信息，它就会查询内容过滤外部数据库，并同 时向 web 服务器发送请求信息。
5. 外部的内容过滤数据库会向 ZyWALL 发送种类信息,提示是发送还是阻止此 web内容。随后此 web 站点的地址也同时会储存在 ZyWALL 的内容过滤缓存当中。

9.4 内容过滤分类

先点击 **安全, 内容过滤**, 然后 点 击**类别** 标 签 可 以 显 示**内容过滤 类别**界面。您可以在该界面中根据类别来配置内容过滤服务。您也可以设置ZyWALL使用外部数据库内

容过滤服务，并且可以选择对哪些类别的网站进行拦截和/或记录。在您使用外部内容过滤服务之前，首先需要进行注册。您可以利用注册界面创建一个myZyXEL.com帐户，注册设备并激活外部内容过滤服务。

请根据下列步骤来查看内容过滤报告。

- 1. 登录myZyXEL.com 并点击设备链接打开它的Service Management界面。
- 2. 点击Service Name区中的Content Filter可以打开Blue Coat登录界面。
- 3. 在Name区域中输入ZyXEL设备的MAC地址（小写字母）。您可以在Service Management界面中发现这个MAC地址。您可以在Password区域中输入您的myZyXEL.com帐户密码。然后点击Submit。

图 72 内容过滤：类别

内容过滤

常规

类别

定制

缓存

启用内容过滤

☒ 启动外部数据库内容过滤

☒ 拦截☒ 日志

☐ 拦截☐ 日志

☒ 拦截☐ 日志

符合的网页

未分级网页

无法使用内容过滤服务器时

内容过滤服务器无回应超时10 (1~30 秒)

选择类别

☐ 选择所有类别☐ 清除所有类别

☐ 成人/性爱相关内容☐ 色情图片☐ 性教育

☐ 内衣/泳装☐ 裸体☐ 酒类/烟草

☐ 非法的/内容可疑的☐ 赌博☐ 暴力/仇恨/种族歧视

☐ 武器☐ 堕胎☐ 艺术/娱乐

☐ 商业/经济☐ 迷信/神秘☐ 违禁药物

高级>>

测试网站属性

测试网站是否被拦截

(域名或IP地址)

用本地缓存测试

用互联网服务器测试

内容过滤服务状态

内容过滤服务：试用版已激活

失效日期：2006-10-01

应用

重置

以下为界面相关的描述。

表 46 内容过滤：分类

标识	描述
类别设置	
启用外部数据库内容过滤	点选此框可以启用外部内容过滤数据库，这样 ZyWALL 可以在这个外部数据库中查找一个 web 页面的请求是属于哪一个分类项。然后 ZyWALL 会根据您在此界面中的配置项来允许或阻止用户对该 web 页的访问。
符合的网页	选择拦截，可以禁止用户访问符合下列所选列表项的 web 页。 当外部内容过滤数据库阻止用户访问一个 web 页面的时候，您会看到一条在 内容过滤 常规 界面中设置的阻止访问提示信息。 选择 日志 您可以记录下尝试访问被禁止的 web 页面的动作。
未分级的网页	选择拦截，可以禁止用户访问不符合下面列表中所列各项的 web 页。当外部内容过滤数据库阻止用户访问一个 web 页面的时候，您会看到一条在 内容过滤 常规 界面中设置的阻止访问提示信息。 选择 日志 ，您可以记录下尝试访问在列表各项中没有涉及到的 web 页面的动作。
当无法使用内容过滤服务器时	选择拦截，可以在外部内容过滤数据库无效的时候禁止用户发送任何 web 页面的请求信息。 您在 内容过滤服务器无响应超时 区域中设置的时间段内没有收到任何从外置的内容过滤数据库发送的响应信息。 ZyWALL 不能正常解析外置的内容过滤数据库的域名。收到了一个从外部内容过滤数据库中发送的错误响应（这可能是由于一个已过期的内容过滤注册信息所导致的） 选择 日志 ，您可以在外部内容过滤数据库无效的时候记录下尝试访问 web 页面的动作。
内容过滤服务器无响应超时	以秒为单位设置一个时间段 1 到 30 规定了 ZyWALL 等待外部内容过滤器的响应时间。如果在时间溢出之后 还没有收到响应，ZyWALL 会根据您在拦截 当无法使用内容过滤服务器时 区域中的设置来阻止或允许您访问的请求 web 页面。
选择类别	

选择所有类别	点选此框可以选中下面所有的列表项。
清除类别	点选此框可以清除下面所有的列表选项。
成人/性爱内容	点选此框可以禁止访问包含过多的与性内容、暴力以及裸体相关的页面。这些页面包括了许多不适合儿童浏览的亵渎和粗俗的内容。
色情图片	点选此框可以禁止访问一些描写色情的色情文学网站。
性教育	点选此框可以禁止访问与性教育相关的页面。
内衣/泳装	点选此框可以禁止访问一些与性感服饰或女性泳衣相关的页面内容。
裸体	点选此框可以禁止访问一些有裸体或半裸相关描述的页面。
酒类/烟草	点选此框可以禁止访问一些与酒精或烟草相关的页面。
非法的/内容可疑的	点选此框可以禁止访问一些与违法犯罪相关的页面。 注意： 这些站点可能是怀有恶意的（例如含有病毒，间谍软件等等）
赌博	点选此框可以禁止访问一些与赌博相关的页面。
暴力/仇恨/种族歧视	点选此框可以禁止访问一些与暴力，仇恨或种族歧视相关的页面。
武器	点选此框可以禁止访问一些与武器相关的页面。
堕胎	点选此框可以禁止访问一些与堕胎相关的页面。
艺术/娱乐	点选此框可以禁止访问一些与文娱，娱乐相关的页面。
商业/经济	点选此框可以禁止访问一些与商业，经济相关的页面。
迷信/神秘	点选此框可以禁止访问一些与祭祀，神秘事件相关的页面。
违禁药物	点选此框可以禁止访问一些与违法药品相关的页面。
教育	点选此框可以禁止访问一些与教育相关的页面。
文化团体	点选此框可以禁止访问一些与娱乐场所相关的页面。
金融服务s	点选此框可以禁止访问一些与金融服务相关的页面。
经济/贸易	点选此框可以禁止访问一些与经济业务以及贸易相关的页面。
游戏	点选此框可以禁止访问一些与游戏相关的页面。

政府/法律	点选此框可以禁止访问一些与政府，法律相关的页面。
军事	点选此框可以禁止访问一些与军事相关的页面。
政治/激进团体	点选此框可以禁止访问一些与政治或激进团体相关的页面。
健康	点选此框可以禁止访问一些与健康相关的页面。
电脑/互联网	点选此框可以禁止访问一些与计算机或互联网相关的页面。
黑客/逃避代理	点选此框可以禁止访问一些与怎样超越代理服务器访问一些受屏蔽网站相关的页面。
搜寻引擎/入口网站	点选此框可以禁止访问一些网站查询网站。
网页通信	点选此框可以禁止访问一些与网络通讯相关的页面。
求职/职业	点选此框可以禁止访问一些与找作，职业相关的页面。
新闻媒体	点选此框可以禁止访问一些与新闻，媒体相关的页面。
私人/约会	点选此框可以禁止访问一些与文娱，娱乐相关的页面。
参考	点选此框可以禁止访问一些与公共关系相关的页面。
聊天/实时传讯	点选此框可以禁止访问一些与聊天，及时信息相关的页面。
电子邮件	点选此框可以禁止访问一些收发电子邮件的页面。
新闻群组	点选此框可以禁止访问一些新闻组。
宗教	点选此框可以禁止访问一些宗教网站。
购物	点选此框可以禁止访问一些购物网站。
拍卖	点选此框可以禁止访问一些拍卖网站。
不动产	点选此框可以禁止访问一些与不动产交易相关的网站。
社会/生活方式	点选此框可以禁止访问一些与社会，生活相关的页面。
同性恋	点选此框可以禁止访问一些与同性恋相关的页面。
餐厅/用餐/食物	点选此框可以禁止访问一些与餐饮，食品相关的页面。
运动/健身/爱好	点选此框可以禁止访问一些与体育，娱乐或业余爱好相关的页面。
旅游	点选此框可以禁止访问一些旅游网站。
车辆	点选此框可以禁止访问一些与交通工具相关的页面。
幽默/笑话	点选此框可以禁止访问一些与笑话，幽默相关的页面。
流通媒体/MP3	点选此框可以禁止访问一些与流媒体或 MP3 相关的页面。

软件下载	点选此框可以禁止访问一些提供软件下载的页面。
付费上网	点选此框可以禁止访问一些与点击网页挣钱的相关的页面。
儿童专用	点选此框可以禁止访问一些具有欺骗性质的网站。
网页广告	点选此框可以禁止访问一些互联网广告。
网页管理	点选此框可以禁止访问一些可以提供最高级别域名服务的网站。
高级/基本	点击 高级 可以查看一个扩展的列表信息，点击 基本 可以查看很少的几个列表信息。
测试网站属性	
测试网站是否被拦截	您可在文本框中输入一个域名，然后点击相关按钮就可以了解这个域名是否已经被屏蔽掉了。
用本地缓存测试	您可在文本框中输入一个域名，然后点击此按钮就可以了解这个域名是否已经储存在 ZyWALL 的已屏蔽网站的数据库中了。
用互联网服务器测试	您可在文本框中输入一个域名，然后点击此按钮就可以了解这个域名是否已经储存在外部内容过滤服务器的已屏蔽网站数据库中。
内容过滤服务状态	该只读区域显示了基于类别的内容过滤（利用一个外部 数据库）服务订购的状况。 服务未激活显示您是否没有注册和激活这个基 于类别的内容过滤服务。 服务激活和 订购有效期显示您是否已经注册ZyWALL并激活了基于类别的内容过滤服务。 试用激活 和 试用 有效期 显示 您 是否 已经 注册 ZyWALL 并激活基于类别的内容过滤服务。 服务未激活和 订购有效期显示您所订购的基于类别的内容过滤服务是否期满。 注意：在您注册完内容过滤之后，您需要等待最多 5 分钟，就可激活内容过滤。
应用	点击 应用 可以保存设置。
重置	点击 重置 可以重新配置该界面。

9.5 用户自定义

先点击 **安全**，**内容过滤**，然后点击**定制** 标签可以显示 **内容过滤** 自定义界面。

您可以创建一系列的有益（允许访问）网站地址和一系列的有害（拦截）网站地址。

您也可以根据网站的地址所包含的关键字来拦截某些网站地址。您可以在该界面的过滤列表中添加或删除指定的站点或关键字

图 73 内容过滤：用户自定义

内容过滤

常规

类别

定制

缓存

网站清单定制

☒ 启用网站定制功能

☐ 除了受信任网站外，关闭所有网页通信

☐ 不要拦截受信任网站的Java/ActiveX/Cookies/Web Proxy

新增受信任网站

添加受信任网站

新增

受信任网站

www.zyxel.com.tw

删除

禁用网站清单

添加禁用网站

新增

禁用网站

www.playboy.com

删除

关键字拦截

☒ 拦截包含以下关键字的网站

新增关键字

新增

关键字清单

bed
sex

删除

应用

重置

以下为界面相关的描述。

表91 内容过滤：用户自定义

标识	描述
网站清单定制功能	
启用网站定制功能	点选此框可以允许访问 受信任网站 中输入的网站，禁止访问 禁用网站 中输入的网站。
除了受信任网站外，关闭所有网页通信	当此项选中后，ZyWALL 只会允许访问在 受信任网站 列表中出现的网站。
不要拦截受信任网站的 Java/ActiveX/Cookies/Web Proxy	当此项选中后，ZyWALL 会允许在 受信任网站 列表中出现的网站向 LAN 上的用户发送 Java, ActiveX 和 Cookies 信息。
新增受信任网站	您可以在这里设置可信任站点。最多可以输入 32 个可信任站点。
添加受信任网站	在文本框中输入类似于“www.good-site.com”的域名。注意 不要包括“http: //”。所有的子域名都会被信任。例如，您输入“zyxel.com”，那么您也同时信任了“www.zyxel.com”，“partner.zyxel.com”和“press.zyxel.com”这样的站点。
受信任网站	列表中会显示已经添加了的 web 站点。
新增	点击此按钮可以将您在文本框中输入的域名添加到可信任站点列表中。
删除	在 受信任网站清单 中选中的一个站点名称，然后点击此按钮可以删除这个站点。
禁用网站清单	您可以在这里设置禁止访问的站点。最多可以输入 32个禁止访问的站点。
添加禁用网站	在文本框中输入类似于“www.bad-site.com”的域名。注意 不要包括“http: //”。所有的子域名都会被信任。例如，您输入“bad-site.com”，那么您也同时禁止访问“www.bad-site.com”，“partner.bad-site.com”和“press.bad-site.com”这样的站点。
禁用网站	列表中会显示已经添加了的 web 站点。

新增	点击此按钮可以将您在文本框中输入的域名添加到禁止访问的站点列表中。
删除	在 禁用网站清单 中选中一个站点名称，然后点击此按钮可以删除这个站点。
关键字拦截	您可以通过设置关键字来禁止访问某些网站。
拦截包含以下关键字的网站	点选此框可以启用此项功能。
新增关键字	输入一个用于禁止访问的关键字。
关键字清单	这里会显示一个关键字列表。
新增	点击此按钮可以将您在文本框中输入的关键字添加到关键字列表中。
删除	在关键字清单中选中一个关键字，然后点击此按钮可以删除这个关键字。
应用	点击 应用 可以保存设置。
重置	点击 重置 可以重新配置该界面。

9.6 自定义关键字的检索

您可以使用指令来设置内容过滤如何检索 URL 中的关键字您可以参考附录来了解如何访问和使用命令提示符。

9.6.1 检索 URL 中的域名或 IP 地址

缺省情况下，ZyWALL 在执行关键字屏蔽的时候只会检索 URL 中的域名或 IP 地址。这就意味着 ZyWALL 只会检索 URL 中头一个斜线之前的字符。

例如，URL如果是 www.zyxel.com.tw/news/pressroom.php，内容过滤只会检索 www.zyxel.com.tw中的关键字。

9.6.2 检索 URL 中的全路径

如果采用全路径检索方式，ZyWALL 会检查最后一个斜线之前的字符。例如，URL如果是 www.zyxel.com.tw/news/pressroom.php，URL全路径检索方式会检查 www.zyxel.com.tw/news中的关键字。

您需要使用指令 `ip urlfilter customize actionFlags 6 [disable | enable]`来启用或关闭URL 的全路径检索方式。

9.6.3 File 名称 URL Checking

如果采用文件名 URL 检索方式，ZyWALL 会检查 URL 中所有的字符。例如，文件名URL检索方式会检查www.zyxel.com.tw/news/pressroom.php中的关键字。

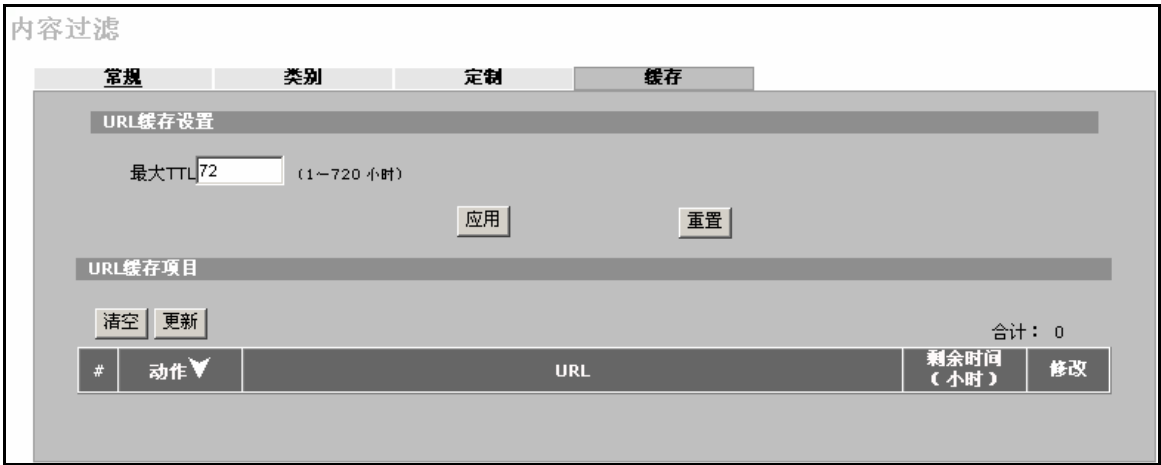
您需要使用指令 `ip urlfilter customize actionFlags 8 [disable | enable]`来启用或关闭文件名 URL 检索方式。

9.7 内容过滤缓存

先点击**安全，内容过滤**，然后点击**缓存**标签可以显示**内容过滤 缓存**界面。您可以利用该界面来查看和配置ZyWALL的URL缓存。您也不但可以配置某一类网址在缓存中保留多久，还可以查看那些被外部内容过滤服务器允许和拦截的网址。ZyWALL仅为缓存中没有发现的站点询问外部内容过滤数据库。

您也可以删除缓存中的个别条目。当您做完这个动作的时候，如果下次再有人访问该站点，ZyWALL会再次查询外部数据库。这就可以允许您检查一个站点种类是否已经改变了。请参阅章节**10.3**来了解更多关于如何递交不正确种类的网站。

图74 内容过滤：缓存



以下为界面相关的描述。

表48 内容过滤：缓存

标识	描述

URL缓存设置	
最大TTL	输入最大活动时间（1到720小时）。这个设置是ZyWALL允许一个条目在抛弃前能在URL缓存中保存多久。
应用	点击 应用 可以保存设置。
重置	点击 重置 开始重新配置该界面。
URL 缓存项目	
清空	点击该按钮可以手动清除缓存中的网址。
更新	点击该按钮可以重新加载缓存。
#	这是一类网址记录的索引号。
动作	该区域显示是否能够访问被拦截和允许的网站的URL。点击列首可以排列条目。如果三角向下，被拦截的URL会先于允许接入的URL显示出来。如果三角向上，则反之。
URL	这是ZyWALL以前与外部内容过滤数据库相符的网址。
剩余时间 (小时)	这是在URL条目被丢弃前的剩余时间。
修改	点击删除按钮把相应的URL条目从缓存中清除。

第 10 章 内容过滤报告

本章将会向您介绍在您激活根据分类的内容过滤订购服务之后，如何查看内容过滤报告。参阅第4章了解如何在myZyXEL.com上创建一个账号，然后注册您的设备并在注册界面中激活订购服务。

10.1 查看内容过滤激活情况

激活了内容过滤功能以后，您需要等待大约5分钟的时间来让其生效。如果没有内容过滤的已激活提示，如果内容过滤没有激活，您也可以按照以下的方法来查看。

1. 进入设备的**内容过滤 类别**配置界面。
2. 至少选择一个分类项，然后点击**应用**。
3. 在**测试网站是否被拦截**区域中输入一个有效的web页URL或IP地址，然后点击**用互联网服务器测试**按钮。如果内容过滤已经激活了，您应该可以看到一个禁止或允许通过的信息。如果内容过滤没有激活，您会看到一条错误信息。

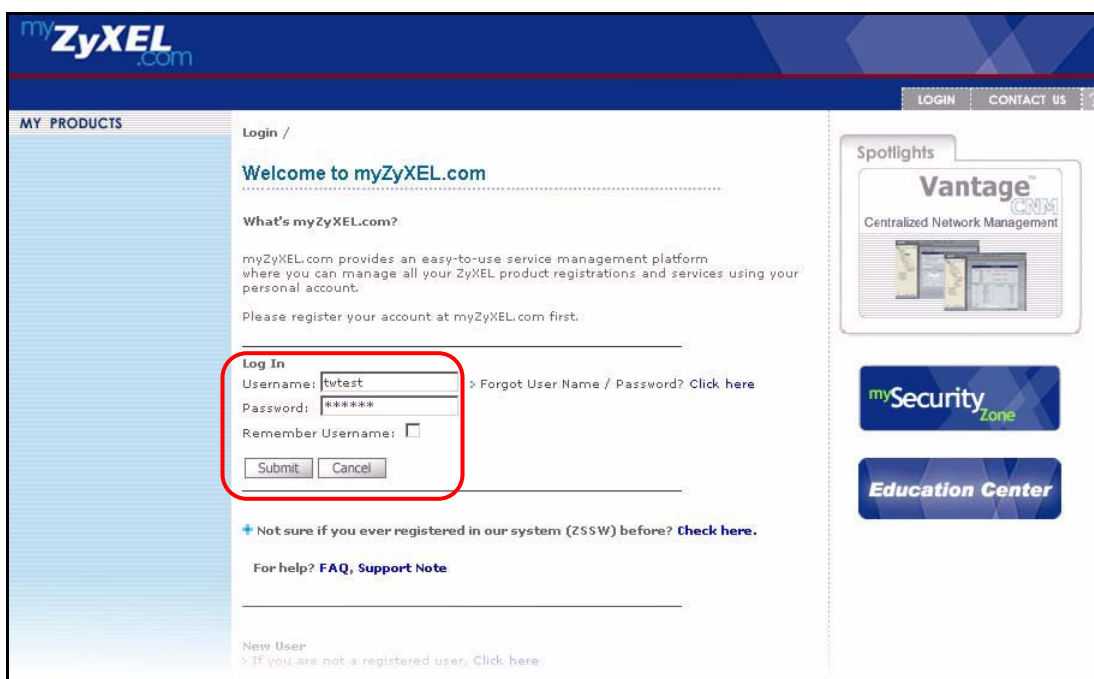
10.2 查看内容过滤报告

内容过滤报告会生成统计数据 and 图表，可以反馈用户访问您在内容过滤界面中选择的 受限制网站的相关信息。

您在查看内容过滤报告之前需要注册您的iCard。另外，您在试用期（最多30天）内也可以查看内容过滤报告。

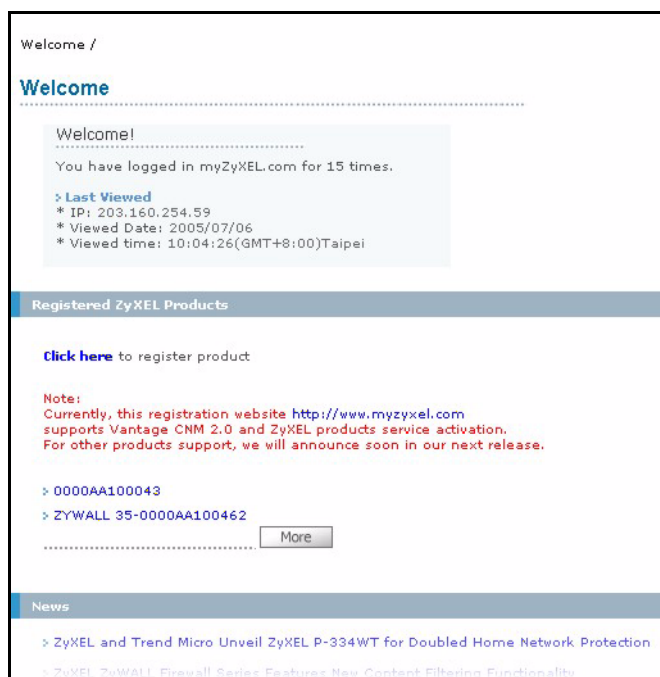
1. 进入<http://www.myZyXEL.com>。
2. 填写您的myZyXEL.com帐户信息并点击**Submit**。

图75 myZyXEL.com: 登录



3. 随后出现一个欢迎界面。在**Registered ZyXEL Products**的下面点击您的ZyWALL的型号名称和MAC地址。在**Service Management**界面中点击**Rename**按钮，您可以为您的ZyWALL修改名称。

图76 myZyXEL.com: 欢迎



4 在**Service Management**界面中点击**Service Name**区域中的**Content Filter**,

您可以打开Blue Coat登录界面。

图77 myZyXEL.com: 服务管理

My Products / Service Activation

Service Management

Product Information

0000AA100043

Serial Number: AAAA100043
 Products: ZYWALL 35
 Authentication Code / MAC Address: 0000AA100043
 Activation Key: N/A

Manage Product

Manage this product's registration by clicking on the appropriate buttons below:

> 0000AA100043

Applicable Service List

To enable your service(s), please click "Activate" shown below to enter your license key(s).
 To login the Content Filter admin site, please click and input the mac address(lower case) & password.

	Service Name	Service Activation	Status	Expiry Date	Remark
1	Anti Spam	Upgrade	Trial	2005-10-06	-
2	Content Filter	Upgrade	Installed	2006-07-13	-
3	IDP AV	Upgrade	Trial	2005-11-09	-

5 在Name中输入ZyXEL设备的MAC地址（小写）。您可以在Service Management界面中找到该MAC地址（图77）。在Password中输入您在myZyXEL.com中注册的账号密码。

6 点击Submit。

图78 Blue Coat: 登录

ZyXEL Powered By **Blue Coat** Technical Support

System Login

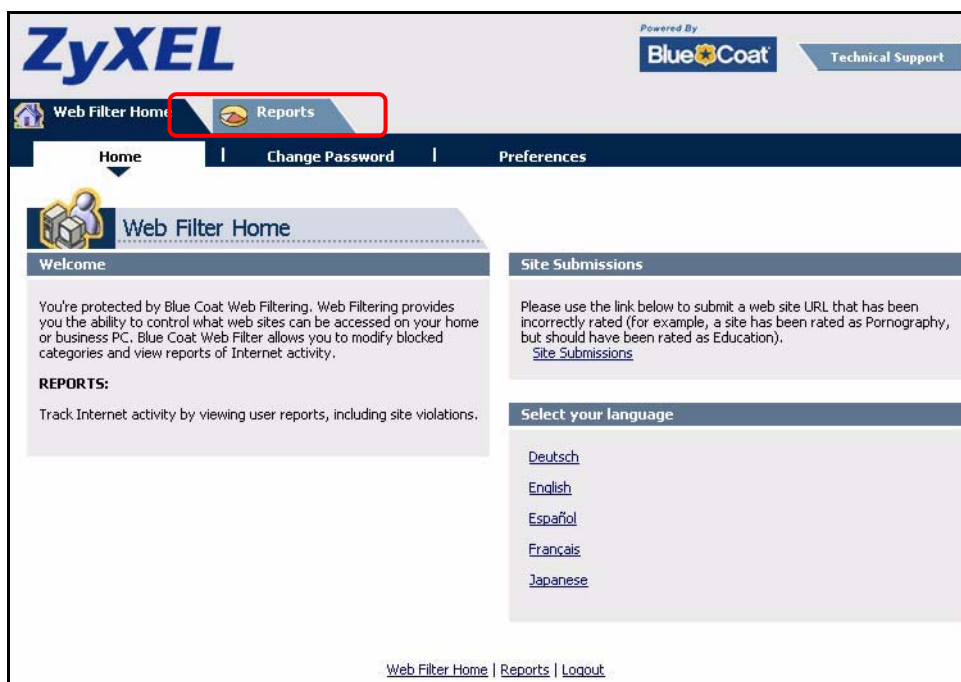
Welcome to your Blue Coat Web Filter Administration site. Please login using your Username and Password.

Name:

Password:

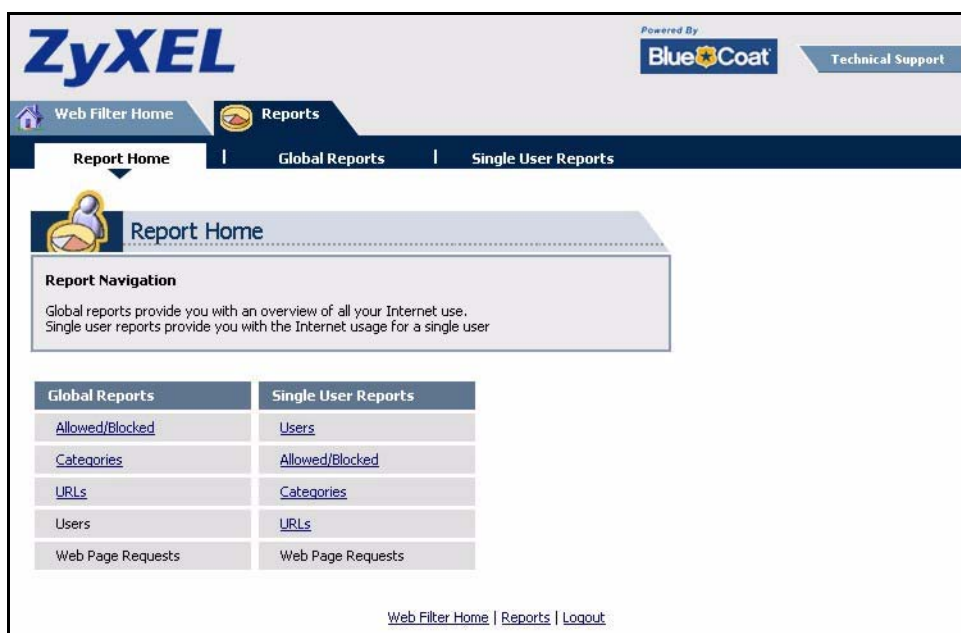
7 在Web Filter Home界面中，点击Reports标签。

图79 内容过滤报告主界面



8 您可以选择**Global Reports**或**Single—IP Address User Reports**下面的条目来查看相应的报告。

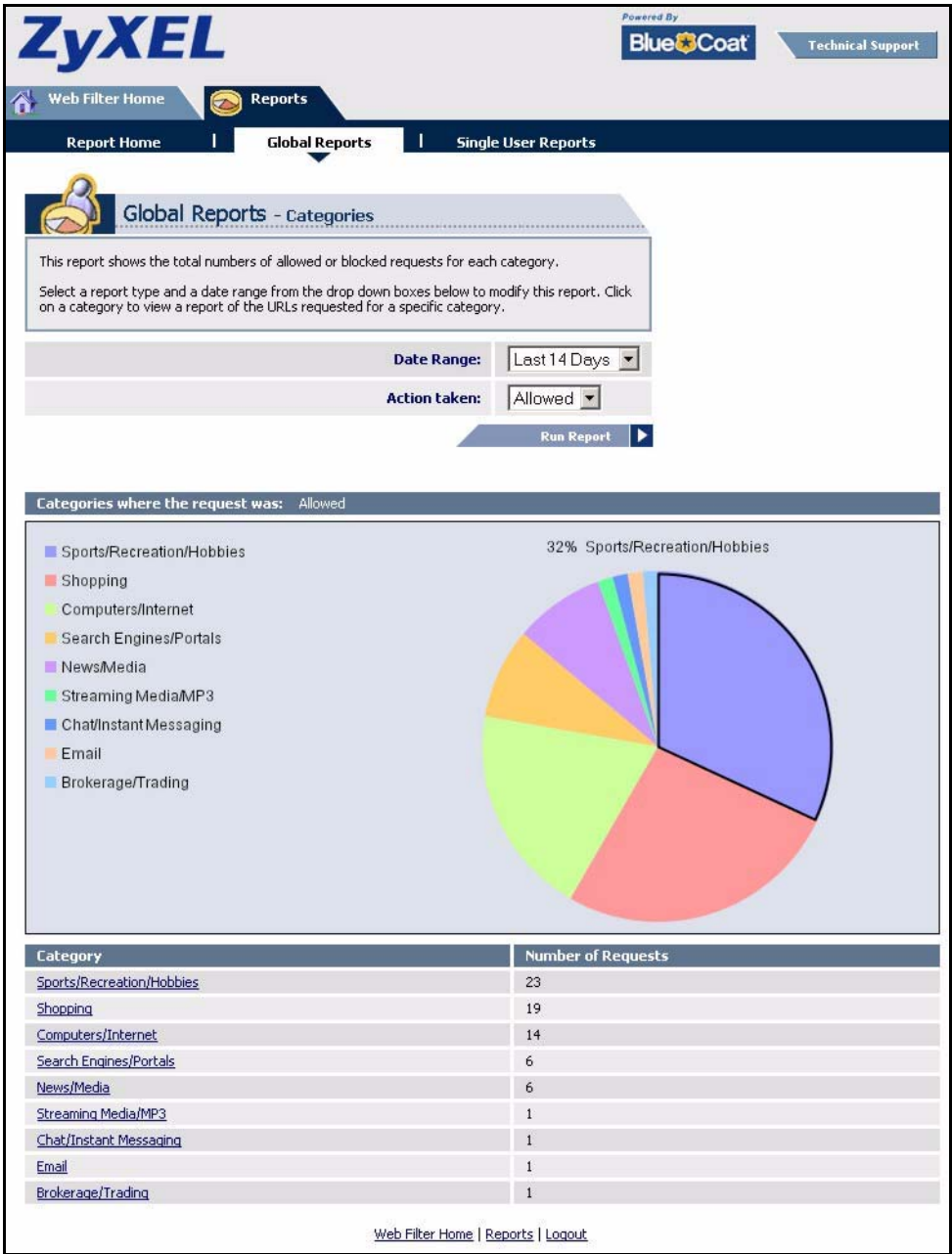
图80Blue Coat: 报告主页



9 在**Data Range**区域中选择一个时间段，您可以选择查看**Action Taken**区域中的**Allow**或者**Block**报告和一个分类（或者输入用户名，您可以查看单用户报告），然后点击**Run Report**。该界面会根据您在**Report Home**界面中所选择的报告类型而有所不同。

10 这样该界面的下方就会出现请求访问网站种类的图形列表信息。

图81 全局报告界面范例



11 您可以点击**Categories**报告中的一个类别或点击**Report Home**界面中的**URLs**来查看所需要的URL信息。

图82 请求访问URL的范例

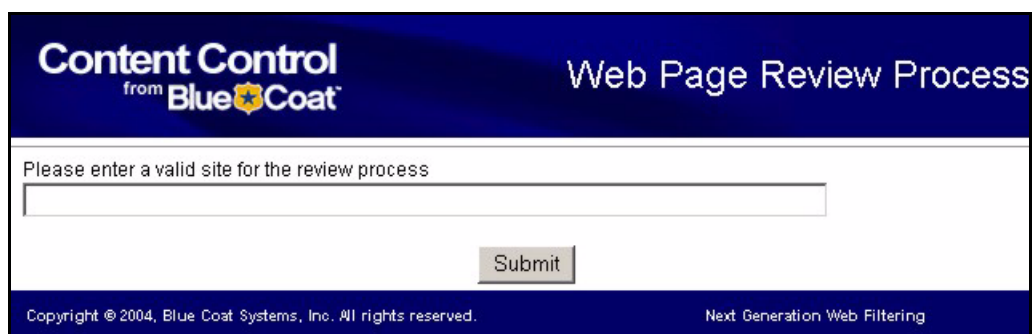


10.3 网站递交

有时您会发现某些站点没有被正确分类，或者网站内容已经变更，这样内容过滤的分 类就需要更新。请根据下列步骤递交网站以便查看。

- 1. 登录到内容过滤报告的网站（请参考章节10.2）
- 2. 进入 **Web Filter Home**界面（请参考图79）然后点击 **Site Submissions** 以打 开 **Web Page Review** 界面。

图83 web页面查验处理界面



The image shows a web interface titled "Content Control from Blue Coat" and "Web Page Review Process". It features a text input field with the placeholder text "Please enter a valid site for the review process" and a "Submit" button. The footer contains the copyright notice "Copyright © 2004, Blue Coat Systems, Inc. All rights reserved." and the text "Next Generation Web Filtering".

Content Control
from Blue Coat

Web Page Review Process

Please enter a valid site for the review process

Submit

Copyright © 2004, Blue Coat Systems, Inc. All rights reserved. Next Generation Web Filtering

3 在空白处输入web站点的URL地址，然后点击**Submit**以提交查验。

第 11 章 IPSec VPN

本章介绍如何进行 ZyWALL 的 IPSec VPN 的安装和维护。

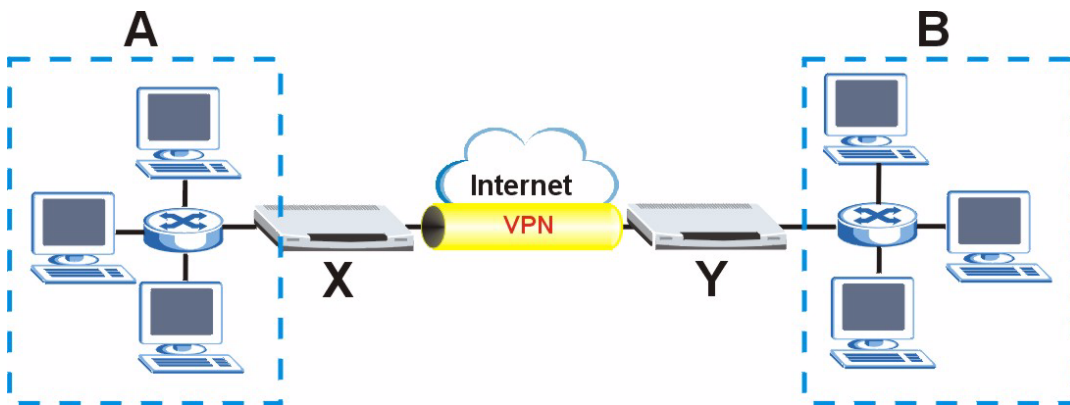
11.1 IPSec VPN 概述

VPN（虚拟专用网）可以提供网络站点之间的安全通信，而不需要花费租用站点到站点路由器线路的昂贵费用。一条安全的 VPN 包括隧道、加密、认证、接入控制和审核等技术。它适合在 Internet 上或在任何采用 TCP/IP 协议进行网络通信的不安全网络中传输数据。

互联网协议安全（IPSec）是一种基于网络标准建立的虚拟专用网（VPN），它为能够在类似于 Internet 的公共网络上进行安全的数据通信提供了灵活的解决方案。IPSec 通过采用多种标准化的密码技术在 IP 层保证了数据的私密性、完整性和认证的准确性。

下图是一个 VPN 通道的示意图

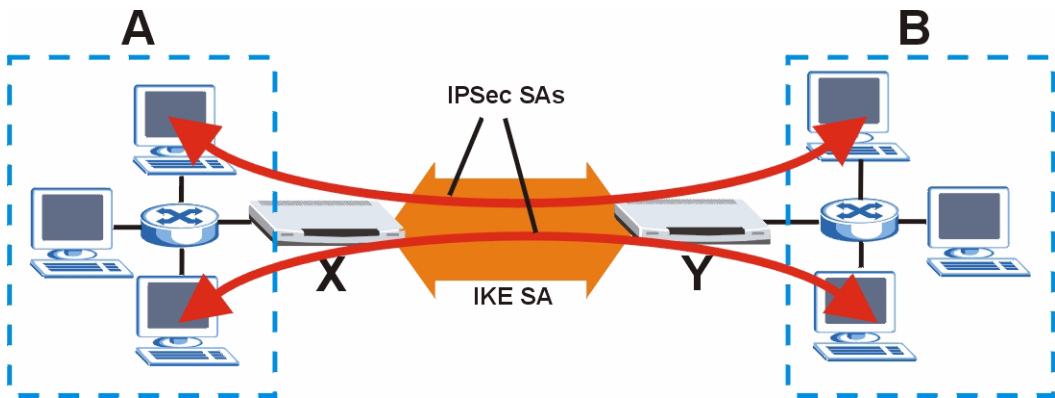
图 84 VPN（虚拟专用网）：高级实例



VPN 通道将 ZyWALL（X）和远程 IPSec 路由器（Y）连接在一起。然后这些路由器将本地网络（A）和远程网络（B）连接起来。

VPN（虚拟专用网）通道的建立一般包括两个阶段。每个阶段之间建立一个安全关联（SA），这种安全关联实际是一种约定，规定了 ZyWALL 和远程 IPSec 路由器将采用哪一种安全参数。第一个阶段（阶段 1），是在 ZyWALL 和远程 IPSec 路由器之间建立因特网密钥交换（IKE）安全关联；第二个阶段（阶段 2），是通过已经建立的 IKE 安全关联实现可靠的 IPSec 安全关联，通过这一关联，ZyWALL 和远程 IPSec 路由器之间可以为本地网络与远程网络之间的计算机传输数据。下图对此做了说明。

图 85 VPN（虚拟专用网）：IKE 安全关联和 IPSec 安全关联



在某些情形，你也可能想要快速临时建立一个 VPN。此时，你可以用 Manual 手动密钥创建一个 IPSec SA。在这种类型的 VPN 隧道，没有 IKE SA，而你可以的手工指定加密及认证的密钥。

在本节的其余章节，将讨论使用 Manual 手动密钥时 IKE SA、IPSec SA 以及 IPSec SA 的更多细节，然后，会详细阐述更具体主题，如加密和认证。

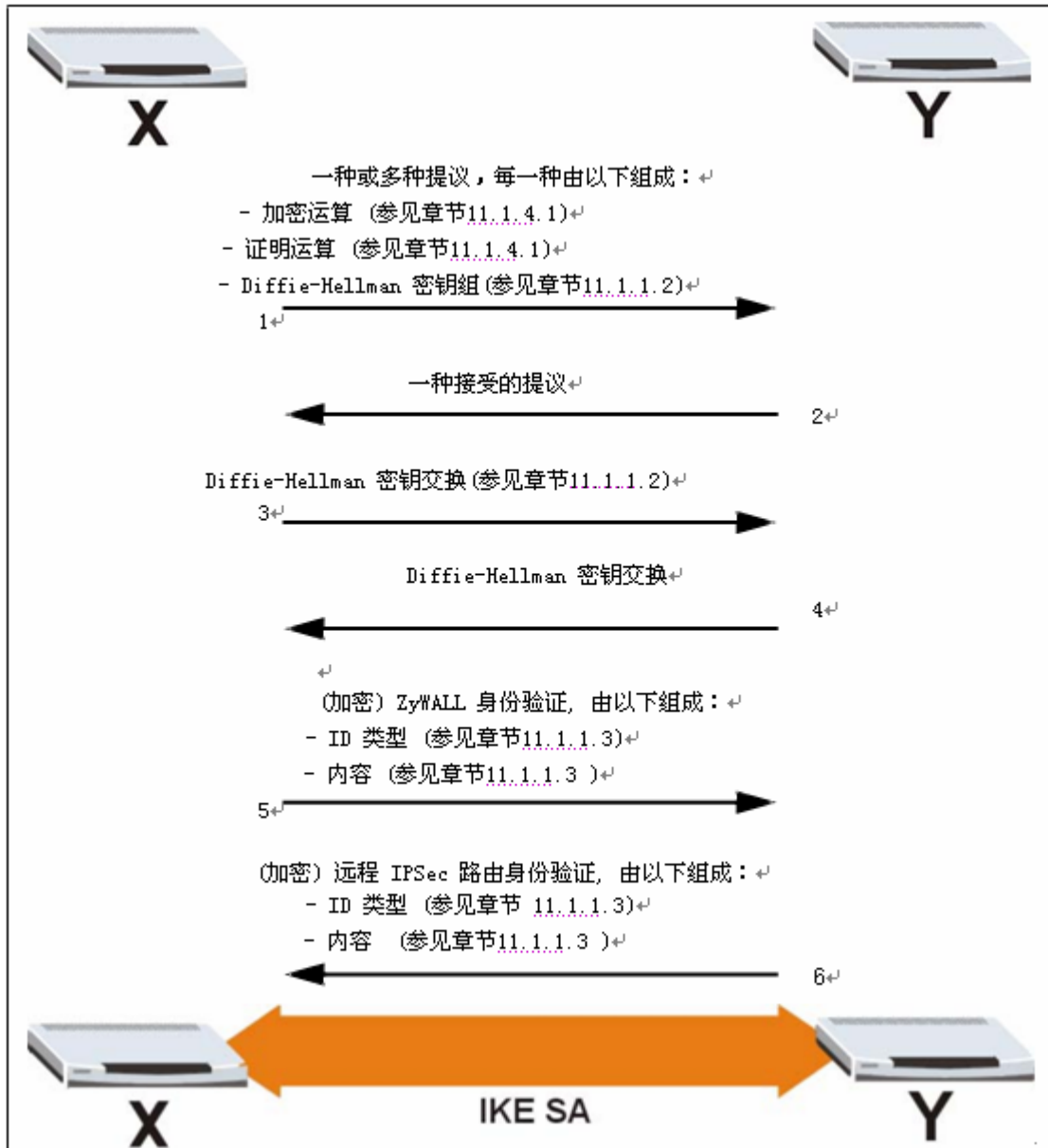
注意：如果要 VPN 隧道支持远程管理（例如 Telnet、http 等），你不能在此配置它，你应该在远程管理界面配置它。

11.1.1 IKE SA

协商模式（协商模式）确定在 ZyWALL 与远程路由器之间如何建立一个 IKE SA，有两种协商模式-- 主模式（主模式）与主动模式（野蛮模式），两个路由器必须都使用同样的协商模式。

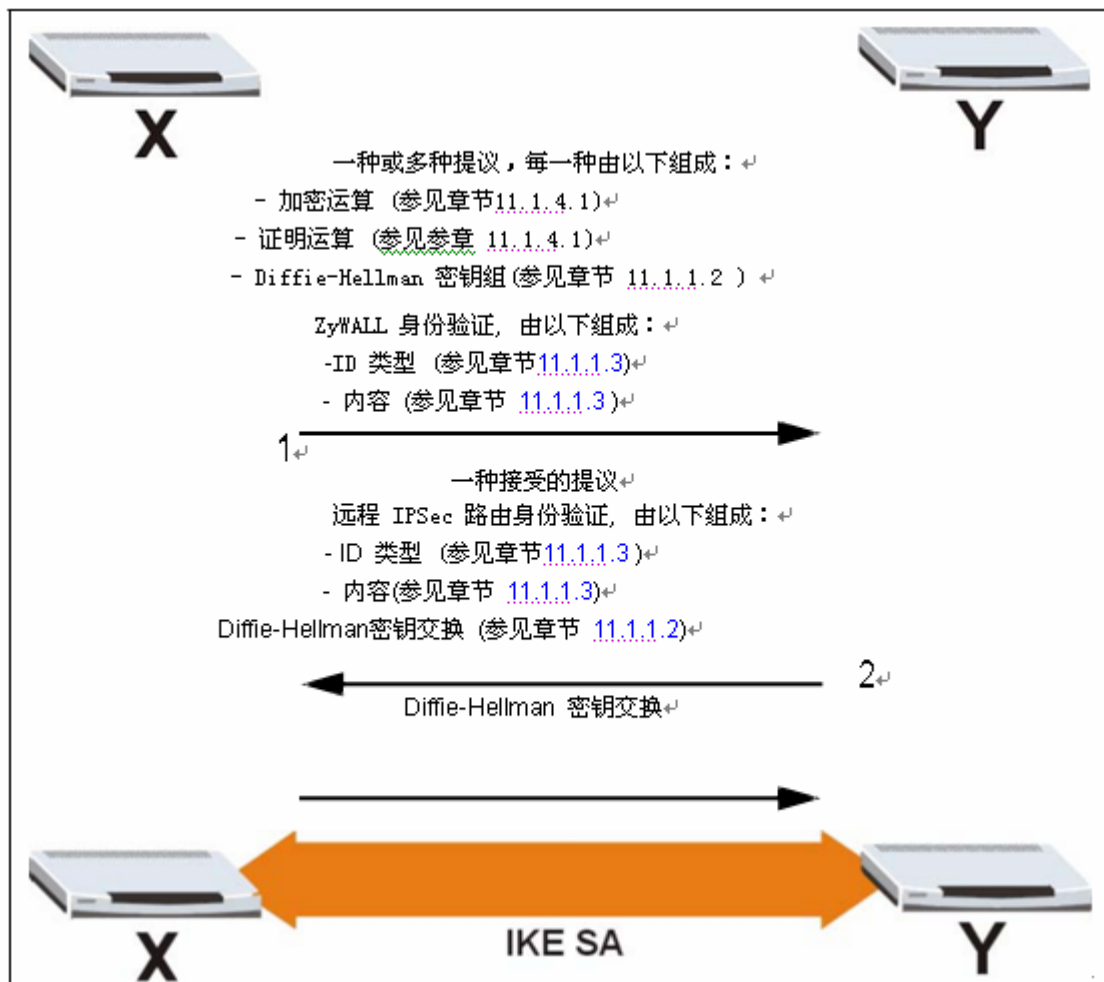
主模式（主模式）用下例进行了说明，在此，ZyWALL（X）初始一个 IKE SA。

图 86 IKE SA：主模式协商模式



ZyWALL 发送提案 (proposal) 到远端 IPSec 路由器，远端 IPSec 路由器选择一个可接受的提案，并向 ZyWALL 回送其接受的提案；然后 ZyWALL 和远程的 IPSec 路由器将参与一个 Diffie-Hellman 密钥交换；最后，ZyWALL 和远程的 IPSec 路由器创建一个用作加密的密钥，加密它们的内容，并交换它们加密的内容进行认证。

主模式（主模式）提供了更高的安全性，因为在第 5 和第 6 步，对你的 ID 也进行了加密。这里有一个折衷 (trade-off)，就是建立 IKE SA 的步骤数。反之，主动模式则更快，但没有足够高的安全性，主动模式显示如下：



主动模式仅用了 3 个步骤来建立 IKE SA，对你的 ID 不再加密。它在远程接入状态很有用，此时发起者（initiator）的地址对于回复者（responder）而言是未知的，双方要以预共享密钥进行认证。例如，IPSec 远程路由器有可能是一个没有固定 IP 地址的远程用户。

协商模式是 IKE SA 的一个特征，包含的其余的特征如下：

- ZyWALL 和远程 IPSec 路由器：此特征说明了在网络中如何标识 ZyWALL 和远程 IPSec 路由器。
- IKE SA 提案（以及哪个提案是可接受的：一项提案包括加密算法、认证算法以及密钥组 DHx。
- 认证方法（以及扩展认证）：这些特征控制了 ZyWALL 和远程 IPSec 路由器如何认证对方。
- 额外的属性：：这些特征包括 IKE SA 的生命期、NAT 穿透等等，SA 的生命期参见 11.1.2.3，NAT 穿透参见 11.1.4.3，以及在相应界面中可查看到其它的属性。

以下对前面三组特性进行讨论。

11.1.1.1 ZyWALL 和远程 IPSec 路由器

在 IKE SA 中，ZyWALL 能通过一个静态 IP 地址、域名或动态域名来标识，静态远程 IPSec 路由器也可以用一个静态 IP 地址、域名或动态域名来标识。

11.1.1.2 IKE SA 提案

IKE SA 包括一个加密算法、认证算法以及 Diffie-Hellman (DHx) 密钥组。在 ZyWALL 中，你只能对一个 VPN 网关指定一个 DHx 密钥组，但你可以指定多对加密和认证算法。这种做法增加了 ZyWALL 和远程 IPSec 路由器在可接受的 IKE SA 方面达成协议的可能性。

11.1.4.1 节对加密和认证算法的更多细节进行了讨论。

一旦 IKE SA 建立，ZyWALL 和远程 IPSec 路由器将使用 Diffie-Hellman 公共密钥加密协议 (public-key cryptography protocol) 建立起共享的秘密。此共享的秘密然后用来生成 IKE SA 密钥和 IPSec SA 加密。Diffie-Hellman 公共密钥加密协议 (public-key cryptography protocol) 基于了 DHx 密钥组。每个密钥组具有固定的位长度，长度越长，加密越安全，但同时加密和解密的时间越长。例如，DH2 密钥 (1024 bits) 就比 DH1 密钥 (768 bits) 更安全，但在加密和解密方面花费的时间更长。

注意： ZyWALL 和远程 IPSec 路由器须使用同样的 DHx 密钥组。

完美向前保密 (PFS)，采用 DHx 密钥组增强了加密信息的机密性，在 185 页 11.1.2.1 进行了讨论。

11.1.1.3 认证密钥与扩展认证 (X-Auth)

如果 ZyWALL 和远程 IPSec 路由器能用证书认证对方，则此证书提供了所以用作认证的信息；否则，你需要手工地提供认证信息。

你需要创建 (并发布) 一个用作认证的预共享密钥。

注意： ZyWALL 和远程 IPSec 路由器 必须使用同样的预共享密钥。

ZyWALL 和远程 IPSec 路由器使用 ID 类型及内容进行互相认证，ID 类型可以是域名、IP 地址、或是电子邮件地址；内容是有正确格式的具体域名、IP 地址、或是电子邮件地址，内容仅用作认证，这样的域名或电子邮件地址不必真正存在，此域名或 IP 地址也无须对应于 ZyWALL 或远程 IPSec 路由器相应的属性。

ZyWALL 和远程 IPSec 路由器分别有着 ID 类型和内容值，所以它们需存储两组信息，一组是它自己，另一组是对方。本地 ID 类型 (本地 ID 类型) 指对应于自己的 ID 类型和内容，

对方 ID 类型（对端 ID 类型）指应用于对方的 ID 类型和内容。

为建立起 IKE SA，ZyWALL 的必须匹配在远程 IPSec 路由器中的对方及本地 ID 类型和内容。例如，在表 49 中，ZyWALL 和远程 IPSec 路由器成功的认证了对方；相反，在表 50 中，ZyWALL 和远程 IPSec 路由器不能认证对方，不能建立 IKE SA。

表 49 VPN 示例：匹配的 ID 类型和内容

ZYWALL	远程 IPSEC 路由器
本地 ID 类型： E-mail	本地 ID 类型： IP
本地 ID 内容： tom@yourcompany.com	本地 ID 内容： 1.1.1.2
对方 ID 类型： IP	对方 ID 类型： E-mail
对方 ID 内容： 1.1.1.2	对方 ID 内容： tom@yourcompany.com

表 50 VPN 示例：不匹配的 ID 类型和内容

ZYWALL	远程 IPSEC 路由器
本地 ID 类型： IP	本地 ID 类型： IP
本地 ID 内容： 1.1.1.10	本地 ID 内容： 1.1.1.10
对方 ID 类型： E-mail	对方 ID 类型： IP
对方 ID 内容： aa@yahoo.com	对方 ID 内容： N/A

如果 ZyWALL 与远程 IPSec 路由器使用证书，你也可以指定对方的主题名称（Subject 名称）的 ID 类型。在此情形，ID 的内容来至于证书的主题名称。

如果你想 ZyWALL 在认证时忽略远程 IPSec 路由器的 ID 类型和内容，你可以对此 VPN 网关的对端 ID 类型任意选择。

注意：不管如何设置 ID 类型和内容，对于重叠的本地与远程 IP 地址，ZyWALL 不允许保存多个活动的 IPSec SA。

扩展认证有助于多个 IPSec 路由器使用一个 VPN 规则来连接到一个 IPSec 路由器。在扩展认证中，一个路由器（ZyWALL 或远程 IPSec 路由器）使用本地用户数据库或外部 RADIUS 服务器不验证用户姓名及密码。因此，没有有效的用户名及密码，进攻者不能建立起 IPSec SA。在扩展认证中，ZyWALL 支持两种角色：在服务器模式，它接收来自远程 IPSec 路由器的用户名及密码，并使用本地用户数据库或者一个特定服务器进行验证；在客户模式，它提供用户名和密码到远程 IPSec 路由器进行认证。

11.1.2 基于因特网密钥交换（IKE）的虚拟专用网（VPN）规则

在一个使用 IKE SA 的 IPSec 安全关联（IPSec SA）中，在 ZyWALL 和远程 IPSec 路由器建立起 IKE SA 后，IPSec SA 也建立了。一个 IPSec 安全关联分成以下一些特征集。

- IPSec SA 提案：IPSec 安全关联提案，此特征控制 ZyWALL 与远程 IPSec 路由器如

何协商并建立 IPSec SA。

- 本地和远程网络：本地及远程网络，这些特征说明本地与远程网络如何标识。
- IPSec SA 内容：IPSec 安全关联的属性，这些特征控制在 IPSec 安全关联建立后的决策。

以下对各个特征集进行讨论。

11.1.2.1 IPSec SA 提案（IPSec 安全关联提案）

一旦 ZyWALL 和远程 IPSec 路由器建立起 IKE SA，它们就能协商一个 IPSec 安全关联（IPSec SA）。激活的协议（ESP 或 AH）提供进行 IPSec SA 的认证，你也可以指定数据包应有的封装类型（隧道或传输）。两个路由器必须使用同样的协议和封装。关于 ESP 与 AH 的协议与封装的更多信息，分别参见 11.1.4.1 节与 11.1.4.2 节。

同 IKE SA 提案类似，ZyWALL 与远程 IPSec 路由器协商采用的加密与认证的算法。在 IPSec SA 建立以前，每对加密—认证算法称为一个提案，在此情形下，如果远程 IPSec 路由器不接受第一个提案，它可以接受另一个。关于加密与认证算法的更多信息，参见 11.1.4.1 节。

ZyWALL 与远程 IPSec 路由器也能许可完美向前保密（PFS）。每次一个 IPSec SA 建立，PFS 就使用一个新的 Diffie-Hellman 交换来改变用于生成加密密钥的根密钥，因此，在一个加密密钥协商好后，先前的以及其后续的密钥因从不同的根密钥继承，也是安全的。Diffie-Hellman 交换很费时，如无需如此安全的数据，它也许是不必要的。

11.1.2.2 本地和远程网络（本地与远程网络）

如果 IPSec SA 有重叠的本地网络与重叠的远程网络，在一个时刻这些 IPSec SA 中只有一个能设置成活动的。如果一个数据包要经一个重叠（不活动）的连接转发，它会被丢弃。

注意：对于重叠的本地与远程 IP 地址，ZyWALL 不允许保存多个活动的 IPSec SA。

11.1.2.3 IPSec SA 内容（IPSec 安全关联属性）

一个 IPSec 安全关联也可以以下属性：

- **Replay detection:** 重放检测，ZyWALL 检测并拒绝老的或者重复的数据包来防范拒绝服务（DoS）攻击。
- **NetBIOS traffic**，NetBIOS 数据流，你可以设置 ZyWALL 许可某些 TCP/UDP 包通过

IPSec SA，这样本地计算机能找到远程网络中的计算机，反之亦然。

11.1.3 IPSec SA 使用手动密钥

在使用手动密钥 IPSec SA 时，ZyWALL 和 远程 IPSec 路由器只建立一个 IPSec SA。它们不建立一个 IKE SA。另外，你要明确提供加密密钥和认证密钥。因此，这类 IPSec SA 比通常的 IPSec SA 更简单，但也更不安全。通常，这只是一种临时的解决方案。

使用手动密钥的 IPSec SA 有以下特征：

- ZyWALL 和远程 IPSec 路由器：ZyWALL 和远程 IPSec 路由器 可仅由其 IP 地址标识。反之，IKE SA 更灵活。（参见 11.1.1.1 节）
- 手动密钥：手动密钥，这些特征指定手工密钥、活动协座以及封装。以下进行了更多的讨论。
- 本地和远程网络：本地和远程网络，这是同其它 IPSec SA 是一样的。（参见 11.1.2.2 节）
- IPSec SA 内容：IPSec SA 属性，在 IPSec SA 使用手动密钥时，一些可用的使用 IKE SA 的 IPSec SA 的属性。（参见 11.1.2.3 节）

在 IKE SA 以及其它类型的 IPSec SA，你可以这提案指定多对加密—认证算法；在使用手动密钥的 IPSec SA，你只能指定一个加密算法及一个认证算法，同时，你须提供对应的加密密钥与认证密钥。

认证也简化了，你可以指定 SPI（安全参数索引）来取代 ID 的类型及内容。SPI 用来明确区分在同一目的地并使用同一 IPSec 协议的不同 SA。这允许你在一个网关使用多路 IPSec SA。在使用手动密钥的 IPSec SA，SPI 和目标 IP 地址唯一标识一个特定的安全关联。

当使用手动密钥的 IPSec SA 建立后，SPI 参数将从远程 IPSec 路由器传送到 ZyWALL，然后 ZyWALL 可使用管理员同 SPI 关联的网络、加密及密钥值，建立 IPSec SA。

注意：当前 ZyXEL 采用相同的输入和输出 SPI 值。

你也可以指定封装和活动的协议，其具有其它 IPSec SA 所需的同样特性。这些特性分别在 11.1.4.2 节 11.1.4.1 节进行了讨论。

使用手动密钥的 IPSec SA 不需要 DHx 密钥组或 PFS。另外，使用手动密钥的 IPSec SA 不支持 NAT 穿透或许多的其它 IPSec SA 属性，这些 IPSec SA 也没有 SA 生命期。

11.1.4 其它的 IPSec VPN 主题

本节讨论 IPSec VPN 其它的适用于 IKE SA、IPSec SA 或是两者都适用的主题，也着重了这些主题之间的关系。

11.1.4.1 活动协议、加密算法及认证算法

要创建一个 IPSec SA，你必须指定一个活动的协议来描述数据包的格式以及缺省的数据包结构（包括执行算法）。ZyWALL 提供了 AH（认证包头）协议和 ESP（封装安全负载）协议（RFC 2406）两种。

AH 协议（RFC 2402）被设计为进行完整性、认证性、序列完整性（防止重放攻击）校验的算法，是一种认证性校验，而不是象 ESP 一样为保密性而设计的。反之，ESP 协议（RFC2406）提供加密的措施以及负载填充特性，能隐藏数据包中的信息，但因为在其进行认证的过程中 IP 包头信息并不包括在内，所以只有有限的认证属性。

在活动协议与可用的加密、认证算法之间有一定的关系。此关系显示在表 51 中，对于每种类型的加密与认证算法也提供了更多的信息。

表 51 VPN： 在 ESP 和 AH 中加密与认证的类型

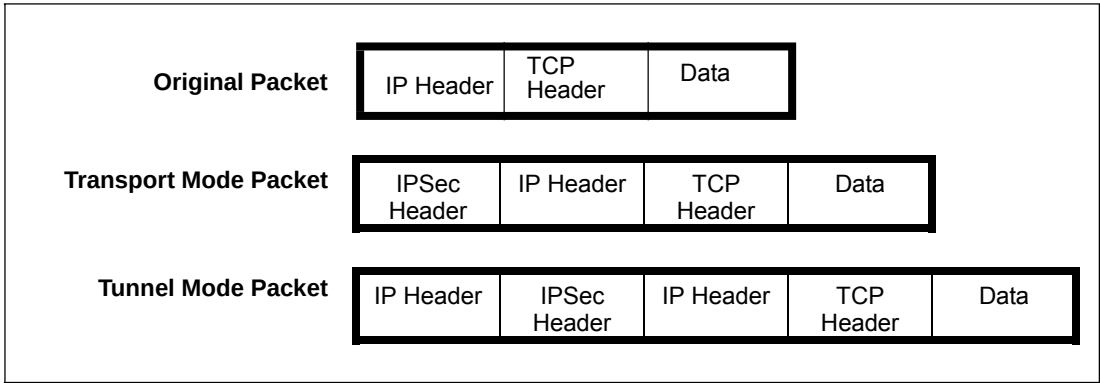
	ESP	AH
加密	DES 数据加密标准（DES）是一种广泛应用的采用私钥进行数据加密的方法。DES 对每一个 64 位的数据用 56 位的密钥进行加密。	
	3DES Triple DES（3DES）是一组 DES 的变量，使用三组单独的 DES 密码重复加密三遍（3*56=168 bits），有效地加强了 DES 加密的强度。	
	AES 高级加密标准是一种新的数据加密方法，它也使用一个密钥。AES 使用一个 128 位的密钥对 128 位的数据进行加密。AES 的速度要高于 3DES。	

	如果您选择 NULL，则会建立一不加密的 IPSec SA。	
认证	MD5（信息摘要 5）会产生一个 128 位的摘要来对数据包进行验证。	MD5（信息摘要 5）会产生一个 128 位的摘要来对数据包进行验证。
	SHA1（安全哈斯算法）产生出 160 位的摘要来对数据包进行认证。	SHA1（安全哈斯算法）产生出 160 位的摘要来对数据包进行认证。
	MD5 提供较低的安全保障，SHA-1 提供较高的安全保障。	

11.1.4.2 封装

IPSec VPN 使用传输模式（传输模式）和 隧道模式（隧道模式）来封装数据包，这些模式讨论如下。

表 52 VPN：传输端口模式和 隧道模式封装



隧道模式是最普通的工作模式，在提供内部系统的接入时需要隧道式，在网关到网关和主机到网关的通信中也需要隧道模式。隧道模式是基本的带认证与加密 IPSec SA，它封装了整个 IP 包进行安全传输。

隧道模式通信包括两组 IP 包头：

- 外部包头：外部 IP 包头包括 VPN 网关的目的 IP 地址。
- 内部包头：内部 IP 包头包括 VPN 网关后面的最终系统的目的 IP 地址。安全协议就位于外部 IP 包头和内部 IP 头之间。

传输模式是用于保护上层协议安全性的，只作用于 IP 数据包中的数据。在此模式中，安全协议（AH 或 ESP）位于 IP 数据包中的原始 IP 包头和其它项后面，而在高层协议（如 TCP 和 UDP）的前面。

通过 ESP，只是数据包中的上层协议得到保护。IP 包头信息和其它项在认证过程中

不会被用到。因此，源 IP 地址不能用于校验数据的完整性。

而安全协议采用 AH 的话，被保护的部分扩展到 IP 包头，从而采用将部分源 IP 包头进行哈斯运算的方法来对整个数据包进行安全性校验。

11.1.4.3 VPN、 NAT 和 NAT 穿透

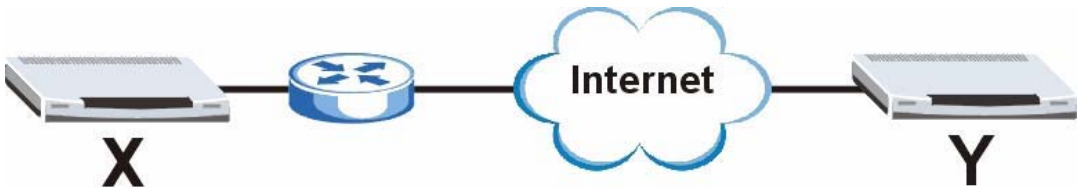
NAT 与 AH 协议是不兼容的，无论它是传输模式还是隧道模式。一个 IPSec SA 用 AH 协议来对发出的数据包进行数字签名，包括数据载荷和包头，数据包上会添加一个哈斯值。

一个位于 IPSec 两端点之间的 NAT 设备将会改变数据包中的源或目的地址。接收端的 VPN 设备在发现收到的数据包后的哈斯值与实际情况无法对应就假设数据被恶意地更改了。

隧道模式下支持认证的 ESP 是与 NAT 兼容的，因为完整性的检查是在初始包头及初始数据载荷上进行的，而这些是不会被 NAT 设备所改变的。传输方式下 NAT 与 ESP 通常是不兼容的，这是因为 NAT 路由器改变了 IPSec 包的包头，但 ZyWALL 的 NAT 穿透特性提供了处理它的方法。

而 NAT 穿透通过在 IPSec 数据包上添加一个 UDP 端口 500 的包头，就可以解决此问题。NAT 路由器在转发数据的时候不修改 UDP 端口 500 的 IPSec 数据包头。例如，在下图中，当路由器 X 尝试建立一 IKE SA，路由器 Y 检查 UDP 端口 500 的包头，IPSec 路由器 A 和 B 建立起 IKE SA。

图 88 VPN 示例： NAT 穿透



要 NAT 穿透工作，您需要：

- 使用 ESP 安全协议（传输或隧道模式）。
- 使用 IKE 密钥模式。
- 在两端的 IPSec 网关上启用 NAT 穿透功能。
- 在 NAT 路由器上设置 UDP 端口 500 到 IPSec 路由 A 上的映射。

在隧道模式和传输模式，AH、 ESP 与 NAT 的兼容性总结如下：

表 53 VPN： NAT 同活动协议与封装的兼容性

活动协议	封装	NAT 兼容

AH	传输	No
AH	隧道	No
ESP	传输	Yes*
ESP	隧道	Yes

* - 如果激活了 NAT 穿透，则此项在 ZyWALL 中支持。

11.1.4.4 SA 生存时间

SA 的特征之一是 SA 的生存时间，SA 的生存时间指定了 SA 在其到期前可存在多长时间，当 SA 到期后，ZyWALL 在以下情况会自动重新协商 SA：

- SA 生存时间到期后仍有数据流。
- 在 ZyWALL 中设置了 IPsec SA 为 保持连接 （见下）

反之，则在下次需要发送数据流时 ZyWALL 必须重新协商 SA。

注意：如果 IPsec SA 在连接中，IKE SA 到期，IPsec SA 保持连接。

一个 IPsec SA 也能设置为保持连接。正常时，在生存时间到期或只有发送的数据而没有接收数据 2 分钟后，ZyWALL 会丢弃此 IPsec SA。如果设置了 IPsec SA 为 保持连接，ZyWALL 会在 SA 到期后自动重协商 IPsec SA，而即使没有接收的数据流，也不会丢弃 IPsec SA。

注意：SA 生存时间及保持连接设置仅适用于规则以静态远程 IP 地址或域名标识了 IPsec 路由器时，如果远程网关地址项设置成了 0.0.0.0，ZyWALL 将不能初始隧道（也不能协商 SA）。

11.1.4.5 IPsec 高可用性

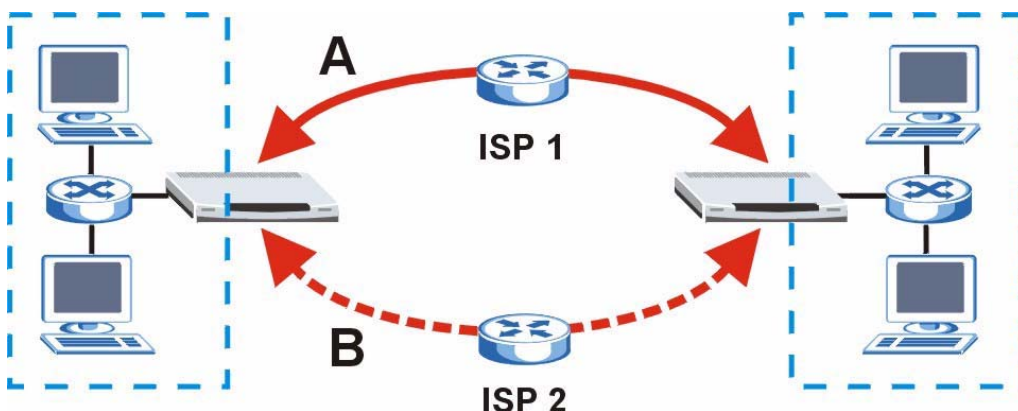
IPsec 高可用性（IPsec HA 或 VPN HA）允许您在主用的 VPN 连接断掉的时候，使用一个冗余（备份）的 VPN 连接，连接到远程 IPsec 路由器的其它 WAN 接口。

配置一个 IPsec 高可用性 VPN 通道，远程 IPsec 路由器需：

- 必须有多于一个 WAN 连接
- 仅需要配置一个对应的 IPsec 规则
- 在对应的 IPsec 规则里，应没有 IPsec 高可用性设置。
- 应以域名标识自己（或动态域名）。
- 必须没有把我的 IP 地址项设置到特定 IP 地址（使用域名、动态域名或 0.0.0.0）。
- 对此 ZyWALL 的 WAN IP 地址，应使用一个 WAN 连接检查。

如果远程 IPSec 路由器不是一个 ZyWALL，你也可能想避免设置 IPSec 规则为保持连接。在下图中，如果主用的 VPN 通道 A 断掉，ZyWALL 将使用冗余的 VPN 通道（B）。

图 89 IPSec 高可用性



11.2 基于因特网密钥交换（IKE）的虚拟专用网（VPN）规则

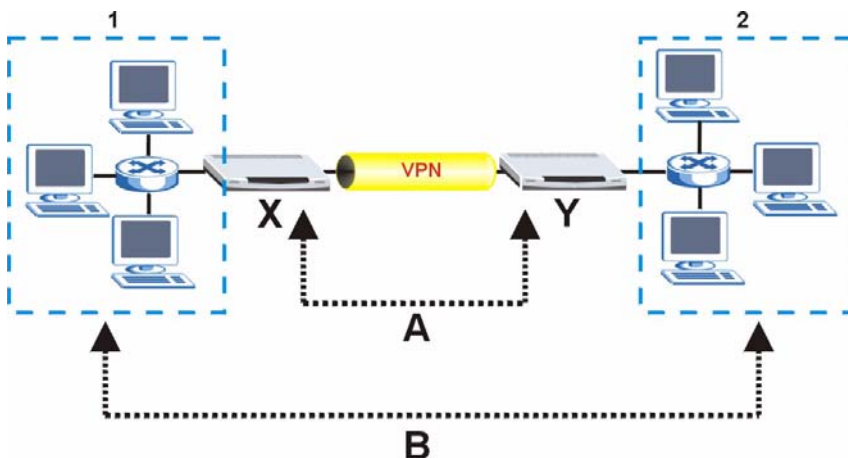
VPN（虚拟专用网）通道可以让您安全地连接到另外一台计算机或另一个网络。

一个网关策略用于识别任意一条 VPN 通道末端的 IPSec 路由器，在 IKE SA 协商（阶段 1）的配置中被使用到。

一个网络策略指定了 IPSec 路由器后面哪个设备能使用 VPN 通道，在 IPSec SA 协商（阶段 2）的配置中被使用到。

在下图中，X 是你的 ZyWALL，Y 是一个远程 IPSec 路由器，箭头 A 表示网关策略，箭头 B 表示网络策略，本地网络标记为 1，远程网络标记为 2。

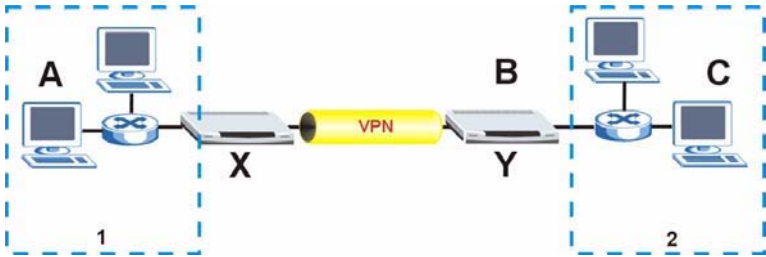
图 90 网关和网络策略



下图说明了 VPN 配置中的主要项，在此图中，X 是你的 ZyWALL，Y 是一个远程 IPSec 路由器，A 表示一个本地网络 IP 地址，B 表示一个远程网关地址，C 表示一个远程

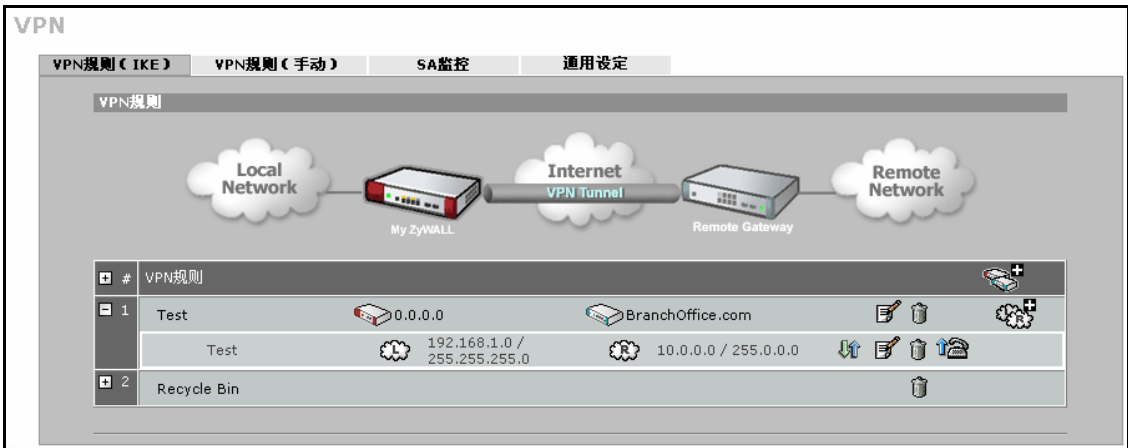
网络地址。本地网络标记为 1，远程网络标记为 2。

图 91 IPSec 配置项汇总



点击 VPN 显示 VPN 规则 s (IKE) 界面。使用此界面来管理 ZyWALL 使用 IKE S 的 VPN 通道列表。

图 92 VPN 规则 (IKE)



下表是对界面中标签的说明。

表 54 VPN 规则 (IKE)

标签	描述
VPN Rules	这些规则对建立 VPN 通道从而安全连接其他计算机或网络所需的设置做出了定义。
	按此图标增加网关策略或 (IPSec 规则)
Gateway Policies	每项 VPN 规则的第一列显示的是网关策略。网关策略对一条 VPN 通道中两端的计算机加以识别 (My ZyWALL 和远程网关)，并规定了在计算机之间协商请求第一阶段 IKE 安全关联时所必须的设置，如身份认证、加密和其他的相关设置 (点击“edit”图标显示其他设置)。

表 54 VPN 规则 (IKE) (继续)

标签	说明
 我的地址	代表您所使用的 ZyWALL。 以路由器模式显示出您的 ZyWALL 所使用的 WANIP 地址、域名、或动态域名。 以桥接模式显示 ZyWALL 的 IP 地址。
 主要远程网关	这里代表的是远程网关。 如果被指定，远程 IPSec 路由器的 IP 地址、域名或动态域名就会被显示出来。否则，会以动态方式进行显示。
	点击该图标可以添加一个 VPN 网络策略。
网络策略	每一项 VPN 规则中随后各列的内容是网络策略。网络策略指定了一条 VPN 通道两端位于 IPSec 路由器后面的设备，并规定了计算机之间第二阶段协商请求 IPSec 安全关联时所必须的设置，如身份认证、加密和其他的相关设置。
 本地网络	这是位于 ZyWALL 后面的网络。网络策略指定了（位于 IPSec 路由器后面的）哪些设备可以使用该 VPN 通道。
 远程网络	这是位于 IPSec 路由器后面的远程网络
	点击该图标可以显示一个界面，在该界面中您可以将一个网络策略联结到一个网关策略。
	点击该图标可以显示一个界面，在该界面中您可以修改网关或网络策略的设置。
	点击该图标可以删除一个网关或网络策略。 如果您删除了一个网关策略，ZyWALL 会自动删除相关的网关策略到回收站。
	点击该图标可以建立一条连接到远端网络的 VPN。
	表示网关或网络策略未激活。
回收站	没有任何网关策略与之相关联的网络策略都将被放在回收站里。

11.3 编辑因特网密钥交换（IKE）方式下的 VPN 网关策略

在 VPN 规则（IKE）屏幕界面，点击“添加网关策略”图标（）或“编辑”图标（），打开“VPN—网关策略—编辑”（VPN 网关策略编辑）界面。

在该界面中对 VPN 网关策略进行配置。网关策略对 VPN 通道中两端连接的 IPSec 路由器（我的地址和远程网关）加以识别，并规定了在计算机之间协商请求第一阶段 IKE 安全关联时所必须的设置—身份认证、加密和其他的相关设置。

图 93 VPN 规则（IKE）：网关策略编辑

VPN—网关策略—编辑

内容

名称FTP_Tunnel

☐ NAT穿透

网关策略信息

我的ZyWALL

☒ 我的地址10.1.1.1 (域名或IP地址)

☐ 我的域名None (参阅[DDNS](#))

主要远程网关10.9.9.9 (域名或IP地址)

☐ 启用IPSec高可靠性

冗余远程网关 (域名或IP地址)

☐ 如果可能，转回到主要远程网关

转回检查间隔*28800 (180~86400秒)

*转回检查间隔：检查主要远程网关可用性的间隔。当IPSec生命周期时间设置大于该值的时候，其将会被取代。

验证密钥

☒ 预共享密钥12345678

☐ 认证auto_generated_self_signed_cert (参阅[我的证书](#))

本地ID类型IP

内容10.1.1.1

对方ID类型IP

内容10.9.9.9

扩展认证

☐ 启动扩展认证

☐ 服务器模式(先搜索[本地用户数据库](#) 再找[RADIUS](#))

☒ 客户端模式

用户名

密码

IKE提案

协商模式Main

加密算法DES

验证算法MD5

SA使用期限(秒)28800

密钥群组DH1

☐ 使用多个提案

相关网络原则

#	名称	本地网络	远程网络
应用 取消			

以下为界面相关的描述。

表 55VPN 规则（IKE）：网关策略：编辑

标识	描述
内容	
名称	此处是 VPN 策略的标识名称，最多 32 个字符。您可以使用任意字符，包括空格，但是 ZyWALL 会忽略末尾的空格。
NAT 穿透	点选此框可以启用 NAT 穿透的功能。NAT 穿透可以允许您在中间有一台 NAT 路由设备的两个 IPSec 网关之间建立一条 VPN 的连接。 注意：远端的 IPSec 网关也必须支持 NAT 穿透功能。 您可以在采用传输或隧道模式的 ESP 协议中采用 NAT 穿透的功能。但是 AH 协议或手工密钥管理则不支持 NAT 穿透。如果希望 NAT 设备后面的 IPSec 网关设备能够接收一个初始化 IPSec 数据包，您需要在 NAT 设备上设置一个 UDP 端口 500 到 IPSec 网关的映射。
网关策略信息	
我的地址	当 ZyWALL 处于路由模式的时候，此字段为 WAN IP 地址或 ZyWALL 的域名。你可以选择我的地址，并输入 ZyWALL 的静态 WAN IP 地址（如果有的话），或者设置为 0.0.0.0。 如果您将此处设置为 0.0.0.0，ZyWALL 会使用 WAN 口当前使用的 IP 地址（静态或动态）。如果 WAN 连接断开的话，当使用拨号备份时，对于 VPN 隧道 ZyWALL 使用拨号备份 IP 地址，或者当用流量重定向时 ZyWALL 使用 LAN IP 地址。 否则您可以选择我的域名，然后设置一个已经配置的动态域名(在 DDNS 界面中)，让 ZyWALL 使用动态域名的 IP 地址。 当 ZyWALL 为网桥模式时，此处为只读并显示 ZyWALL 的 IP 地址。 如果在 VPN 建立后我的地址的 IP 地址被更改，则 VPN 隧道将会重新建立。

主要远程网关	输入您准备建立 VPN 的 IPSec 网关的 WAN 口 IP 地址或域名（最多 31 个字符串）。如果远端 IPSec 路由器有一个动态 WAN IP 地址，那么将此处设为 0.0.0.0。 为了使多条远程网关地址的地方设置为 0.0.0.0 的规则同时激活，本地 IP 地址的范围不能相互重叠。 如果您已经配置了一条远程 网关 地址设置为 0.0.0.0 的规则，本地 IP 地址的范围是整个网段，那么您就不能再配置 远程网关地址设置为 0.0.0.0 的规则。
启用 IPSec 高可靠性	打开高可用性特性，如果主用（正常）VPN 断掉，则使用冗余（备份）的 VPN 连接，连接到远程 IPSec 路由器的其它 WAN 接口。为使用此特性，远程 IPSec 路由器必须有第二个 WAN 连接。 要使用此特性，你必须用 WAN IP 地址或域名来标识主用的和冗余的远程 IPSec 路由器（不能都设置为 0.0.0.0）。
冗余远程网关	输入在 ZyWALL 不能连接主用远程网关时使用的备用 IPSec 网关的 WAN IP 地址或域名（最多 31 个字符串）。
如果可能，转回到主要远程网关	选择此项，在断开的连接恢复正常后，使 ZyWALL 返回到使用主用远程网关状态。
转回检查间隔	设置连接到备用远程网关时， ZyWALL 应间隔多长时间检查一下到主用远程网关的连接。 每个网关策略使用一个或多个网络策略，如果此间隔时间比网络策略的 SA 生存时间短，则此间隔用作检查的间隔时间及网络策略的 SA 生存时间。如果此间隔时间比网络策略的 SA 生存时间长，则 SA 的生存时间用作检查的间隔时间及网络策略的 SA 生存时间。
验证密钥	
预共享密钥	选择与共享密钥选项，然后在该区域中输入一个预共享密码。 预分配密钥用于在 IKE 协商的步骤一阶段标识通信双方。由于在您 的 ZyWALL 和其它 IPSec 网关通过一条安全连接通信之前，需要分享这个密钥，所以我们将其称作预共享。 请输入一个 8 到 31 位的 ASCII 字符（区分大小写）或 16 到 62 位的十六 进制字符（“0-9”，“A-F”）。您还需要在十六进制字符前面预置一个“0x”标志，而这个字符串不属于密码本身。例如，“0x123456789ABCDEF”，“0x”代表此字符串是一个十六进制的密码，

	“123456789ABCDEF”是真正的密码。 VPN 通道两端需要使用相同的预共享密码。如果通信双方的预共享密码不同的时候，您会收到一个“PYLD_MALFORMED”数据包。
认证	选择认证选项，您可以使用一个证书来标识 ZyWALL。 从下拉菜单中选择一个证书用于这条 VPN 的创建。您需要在我的证书界面中提前配置好证书。点击我的证书，进入我的证书界面，您可以查看 ZyWALL 的证书列表。
本地 ID 类型	选择 IP，ZyWALL 可以通过 IP 地址来标识。 选择 DNS，ZyWALL 可以通过一个域名来标识。 选择 E-mail，ZyWALL 可以通过一个电子邮箱地址来标识。 如果您在认证模式中选择认证，就不用配置本地 ID 类型和内容。ZyWALL 会从您所选择的证书中获得这些信息。
内容	如果您在本地 ID 类型中选择了 IP，请在本地的内容区域中输入 IP 地址。如果您将内容配置为 0.0.0.0 或留空，ZyWALL 会自动在此应用您在我的地址（请参考我的地址区域的描述）中配置的 IP 地址。 在下面几种情况下，我们建议您在本地内容区域中输入一个 IP 地址或者使用 DNS 或 E-mail 地址的方式，而不输入 0.0.0.0 或留空： - 当两个 IPSec 路由器中有一个 NAT 路由器的时候。 - 如果您想让远端 IPSec 路由器能够区分具有动态 WAN 口 IP 地址的 IPSec 路由器发出的 VPN 连接需求的时候。 如果您在本地 ID 类型中选择了 DNS 或 E-mail，请输入一个域名或电子邮箱地址来标识本地 ZyWALL。您可以使用最多 31 个 ASCII 字符，包括空格，但是 ZyWALL 会忽略末尾的空格。此域名或电子邮箱地址只用于标识，可以是任何字符串。
对方 ID 类型	如果您在认证模式选择了预分配密钥，请从以下选项中选择： 选择 IP，可以通过 IP 地址来标识远端 IPSec 网关。 选择 DNS，可以通过一个域名来标识远端 IPSec 网关。 选择 E-mail，可以通过一个电子邮箱地址来标识远端 IPSec 网关。如果您在认证模式选择了 Certificate，请从以下选项中选择： 选择 IP，可以通过 IP 地址来标识远端 IPSec 网关。出现于 VPN 连接时使用证书的主题可选名称中。

内容	选择名称，可以通过 VPN 连接时使用证书的主题可选名称来标识 IPSec 网关。选择 DNS，可以通过一个域名来标识远端 IPSec 网关。出现于 VPN 连接时使用证书的主题可选名称中。 选择 E-mail，可以通过一个 E-mail 地址来标识远端 IPSec 网关。出现于 VPN 连接时使用证书的主题可选名称中。 选择 Any，可以让 ZyWALL 不检查远端 IPSec 网关的 ID。 对端内容的配置依赖于对端 ID 类型的选择。 如果您在认证模式中选择了预分配密钥，请从以下选项中选择： 如果您选择了 IP，请输入对端的 IP 地址。如果您将内容配置为 0.0.0.0 或留空，ZyWALL 会自动在此应用您在远程网关地址（请参考远程网关地址区域的描述）中配置的 IP 地址。 如果您选择了 DNS 或 E-mail，请输入一个域名或电子邮箱地址来标识远端 IPSec 网关。您可以使用最多 31 个 ASCII 字符，包括空格，但是 ZyWALL 会忽略末尾的空格。此域名或电子邮箱地址只用于标识，可以是任何字符串。 在下面几种情况下，我们建议您在本地内容区域中输入一个 IP 地址或者使用 DNS 或 E-mail 地址的方式，而不输入 0.0.0.0 或留空： 当两个 IPSec 路由器中有一个 NAT 路由器的时候。 如果您想让远端 IPSec 路由器能够区分具有动态 WAN 口 IP 地址的 IPSec 路由器发出的 VPN 连接需求的时候。 如果您在认证模式中选择了 Certificate，请从以下选项中选择： 如果您选择 IP，在 VPN 连接时，远端 IPSec 网关使用证书的主题可选名称中输入 IP 地址。如果您将此处配置为 0.0.0.0 或留空，ZyWALL 会使用远程网关地址中（请参考远程对端内容的配置依赖于对端 ID 类型的选择。 如果您在认证模式中选择了预分配密钥，请从以下选项中选择： 如果您选择了 IP，请输入对端的 IP 地址。如果您将内容配置为 0.0.0.0 或留空，ZyWALL 会自动在此应用您在远程网关地址（请参考远程网关地址区域的描述）中配置的 IP 地址。
扩展认证	
启用扩展认证	点选此框，可以激活扩展认证功能。

服务器模式	选择服务器 模式，可以让本台 ZyWALL 对其它的扩展认证客户端的 VPN 连接请求做认证。 您需要同时在认证服务器的本地用户数据库或 RADIUS 服务器（请参考认证服务器一节）中配置扩展认证客户端的用户名和密码。点击本地用户，您可以回到本地用户 数据库界面，您在此可以浏览和/或编辑用户的账号列表。点击 RADIUS，可以进入 RADIUS 界面，您可以在这里配置 ZyWALL 查询一个外置的 RADIUS 服务器。 在认证期间，如果扩展认证服务器在内部的用户数据库当中没有找到 扩展认证客户端的用户名，它就会继续在外置的 RADIUS 服务器中查询，尝试通过 RADIUS 服务器对用户做认证。
客户端模式	选择客户端模式，当 ZyWALL 与支持扩展认证服务器的 ZyWALL 建立 VPN 连接的时候，它需要使用一个用户名和密码。只需要一个 VPN 扩展认证客户端就可以初始化这条 VPN 的连接。
用户名	输入用户名，最多 31 个 ASCII 字符（区分大小写），不允许出现空格。当您选择客户端模式的时候，需要输入一个用户名。
密码	输入一个和用户名相对应的密码。最多 31 个 ASCII 字符（区分大小写），不允许出现空格。
IKE 提案	
协商模式	从下拉菜单中选择主或主动。通过同一个安全网关建立的多条 SA 必须具有同一种协商模式。
加密算法	从下拉菜单中选择 DES, 3DES 或 AES。数据通信的收发双方需要使用相同的加密密钥，由此可以用于加密和 解密信息，或生成，并标识一个信息认证码。DES 加密算法使用 56bit 的密钥，3DES 使用 168bit 的密钥。这样 3DES 会比 DES 更安全，但需要更多的处理时间，这样会导致时延加大和吞吐量降低。AES 使用 128bit 的密钥，AES 处理速度要快于 3DES。
验证算法	从下拉菜单中选择 SHA-1 或 MD5。MD5 和 SHA-1 都是哈希算法，用于 认证数据包。SHA-1 算法比 MD5 更强健，但是效率更低。MD5 具有低 的安全性，而 SHA-1 具有高的安全性。

SA 使用期限 (秒)	在该栏目中可定义 IKE SA 在自动重新协商前存在的时间。它的设置范围从 180 到 3, 000, 000 秒（约 35 天）。 一个较短的 SA 生存时间可以通过更换加密和验证密钥的方法来增强 SA 的安全性，然而每次 VPN 隧道重新协商建立时，所有访问远端资源 的用户都会临时被断掉。
密钥群组	您需要给 阶段 1 IKE 设置选择 一个密钥组 。 DH1 （缺省）是指 Diffie-Hellman 组 1，有 768 位的随机数。DH2 是指 Diffie-Hellman 组 2，有 1024 位的随机数（更安全一些，但会较慢）。
使用多个提案	选择该选框，当协商 IPSec SA 的时候，允许 ZyWALL 使用阶段 1 或阶段 2 加密和证明法则的任何一个。 当您使用多个提案时，ZyWALL 允许远端 IPSec 路由器选择加密和运算法则用于 VPN 隧道，即使他们比您为 VPN 规则配置的安全程度要低。 不选该选框表示当协商 IPSec SA 的时候，ZyWALL 只使用阶段 1 或阶段 2 加密和运算法则配置下列项目。
相关网络原则	下表显示您为该规则配置的策略。要添加一个 VPN 策略，点击 VPN 规则（IKE）界面中的添加网络策略图标  （参考图 92）。参阅章节 11.4 可以了解更多信息。
#	这是策略索引号。
名称	这是策略名称。
本地网络	这里显示 ZyWALL 后面的一个或一定范围的 IP 地址。
远程网络	这里显示一个远程 IPSec 路由器后面的一个或一定范围的 IP 地址。
应用	点击应用可以保存设置。
取消	点击取消可以不保存设置并退出界面。

11.4 VPN 规则（IKE）：编辑网络策略

首先进入 VPN 规则（IKE）界面，然后点击添加网络策略图标（），您可以见到 VPN-网络策略 -Edit 界面。一个网络策略用于识别任意一条 VPN 通道末端的 IPSec 路由器后面的设备，规定在阶段 2 IPSec SA 协商的时候需要用到的认证、封装和其它参数。

图 94VPN 策略（IKE）：编辑网络策略

VPN－网络原则－编辑

内容

☒ 启用

名称

FTP_Server

协议

0

☐ 保持连接

☐ 允许通过 IPsec 通道进行 NetBIOS 传输

☐ 检查IPSec通道连接 ☐ 日志

Ping这个地址

0 . 0 . 0 . 0

网关策略信息

 网关策略

FTP_Tunnel

本地网络

 地址类型

Single Address

开始IP地址

192 . 168 . 1 . 4

结束IP地址/子网掩码

0 . 0 . 0 . 0

本地通信端口

开始 0 结束 0

远程网络

 地址类型

Range Address

开始IP地址

192 . 168 . 2 . 1

结束IP地址/子网掩码

192 . 168 . 2 . 25

远程通信端口

开始 0 结束 0

IPSec提案

封装模式

Tunnel

启动的协议

ESP

加密算法

DES

验证算法

SHA1

SA使用期限（秒）

28800

完美保密（PFS）

NONE

☐ 启动重复侦测

☐ 使用多个提案

应用

取消

以下为界面相关的描述。

表 56 VPN 策略（IKE）编辑网络策略

标识	描述

启用	点选启用，使用该通道的数据包可以触发 ZyWALL 建立 VPN 隧道。不选该框，表示关闭该网络策略。ZyWALL 不使用该策略。使用该通道的数据包不能触发 ZyWALL 建立 VPN 隧道。 当隧道建立起来的时候，如果您去掉了该框的勾选，那么您就关闭了这个网络策略和并断开了该隧道。
名称	输入一个名称代表该 VPN 网络策略。您可以使用任意字符，包括空格，但是 ZyWALL 会忽略末尾的空格。
协议	输入 1 代表 ICMP，6 代表 TCP，17 代表 UDP 等等。0 是缺省值，代表任何协议。
保持连接	选择该选框可以为该 SA 打开 Nailed-Up 功能。 打开保持连接，在生命周期终止之后，即便没有数据流，ZyWALL 也会自动发起建立 SA。当 ZyWALL 重新启动的，ZyWALL 也会重新建立 SA。 如果它因为流入流出闲置定时器而断开连接，那么 ZyWALL 也会重建隧道。
允许通过 IPSec 通道进行 NetBIOS 传输	当 ZyWALL 为网桥模式时此处不可用。 NetBIOS（网络基本输入输出系统）是 TCP 或 UDP 数据包，它可以让局域网内的计算机互相通信。对于一些拨号服务如 PPPoE 或 PPTP，NetBIOS 封包经常导致建立一些不是需要的拨号。然而在某些时候必须通过 NETBIOS 与 WAN 上的计算机进行通信。有时候为了允许本地计算机查找到远端网络，允许 NetBIOS 通过 VPN 隧道也是很重要的，反之亦然。 选择该选框可以通过 VPN 连接来发送 NetBIOS。
检查 IPSec 通道进行 NetBIOS 传输	选择 Ping this 地址选框，然后配置一个 IP 地址，ZyWALL 会定时测试到远端 IPSec 路由器的 VPN 通道。 ZyWALL 每分钟会 ping 一次这个 IP 地址。当发送 ping 数据包时，ZyWALL 会开启 IPSec 连接闲置时间定时器。如果闲置时间周期终止，IPSec 路由器也没有流量，ZyWALL 会断开 VPN 隧道的连接。
日志	点选此框可以让 ZyWALL 在没有 ping 通这个远端设备的时候创建日志记录。

Ping 这个地址	如果您选择检查 IPSec 通道连通性，可以输入一个远端 IPSec 网络中计算机的 IP 地址。这个计算机的 IP 地址必须在 IP 策略中的远程 IP 地址范围之内才可以（请参考远程网络区域）。
网关策略信息	
网关策略	为您希望使用的 VPN 策略选择网关策略。
本地网络	本地 IP 地址必须是静态的，它相对应于在远端 IPSec 路由器配置的远端 IP 地址。两条激活的 SA 中可以配置相同的本地或远端 IP 地址，但是不能同时一样。您可以使多条 SA 使用相同的本地和远端 IP 地址，但是随时只会有一条处于激活状态。
地址类型	从下拉菜单中选择单一 IP 地址，指定 IP 段地址，或 IP 子网地址。Single 代表单一的 IP 地址，指定 IP 段地址代表一个地址范围，IP 子网地址代表一个子网段。
开始 IP 地址	当地址类型中配置为单一 IP 地址的时候，输入 ZyWALL 的一个（静态）IP 地址。当地址类型中配置为指定 IP 段地址的时候，输入一个 IP 地址范围的起始（静态）IP 地址。当地址类型中配置为 IP 子网地址的时候，输入您 ZyWALL 本地子网的其中一个（静态）IP 地址。
结束 IP 地址/子网掩码	当地址类型中配置为单一 IP 地址的时候，此处为 N/A。当地址类型中配置为指定 IP 段地址的时候，输入一个 IP 地址范围的末尾（静态）IP 地址。当地址类型中配置为 IP 子网地址的时候，输入您 ZyWALL 本地子网的子网掩码。
本地通信端口	0 是缺省值，意味着任何端口。在开始和结束区域中输入一个从 0 到 65535 的端口号。一些最普通的 IP 端口：21，FTP；53，DNS；23，Telnet；80，HTTP；25，SMTP；110，POP3。
远程网络	远端 IP 地址必须是静态的，它对应着远端 IPSec 路由器的本地 IP 地址。两条激活的 SA 中可以配置相同的本地或远端 IP 地址，但是不能同时一样。您可以使多条 SA 使用相同的本地和远端 IP 地址，但是随时只会有一条处于激活状态。
地址类型	从下拉菜单中选择单一 IP 地址，指定 IP 段地址，或 IP 子网地址。Single 代表单一的 IP 地址，指定 IP 段地址代表一个地址范围，IP 子网地址代表一个子网段。

开始 P 地址	当地址 类型中配置为单一 IP 地址的时候，输入远端 IPSec 路由器的一个（静态）IP 地址。当地址 类型中 配置为 指定 IP 段地址的时候，输入一个 IP 地址范围的起始（静态）IP 地址。当地址类型中配置为 IP 子网地址的时候，输入远端 IPSec 路由器后面子网内的其中一个（静态）IP 地址。
结束 IP 地址/子网掩码	当地址 类型中配置为单一 IP 地址的时候，此处为 N/A。当地址类型中配置为指定 IP 段 地址的时候，输入一个 IP 地址范 围的末尾（静态）IP 地址。当地址类型中配置为 IP 子网 地址 的时候，输入远端 IPSec 路由器后面子网内的子网掩码。
远程通信端口	0 是缺省值，意味着任何端口。在 Start 和 End 区域中输入一个从 0 到 65535 的端口号。一些最普通的 IP 端口：21，FTP；53，DNS；23，Telnet；80，HTTP；25，SMTP；110，POP3。
IPSec 提案	
封装模式	选择隧道封装模式或传输封装模式。
启用的协议	选择一个建立 SA 的安全协议。AH 和 ESP 都会增加 ZyWALL 的处理负荷，造成通信上的微小延时。
加密算法	当 DES 用于数据通信时，无论是发送者还是接收者都必须知道同一个密钥，该密钥要用来对信息进行加密、解密或产生和校验信息的验证码。DES 加密算法使用 56 位的密钥。Triple DES（3DES）是在 DES 基础上的一种改进，它使用 168 位密码。这样 3DES 比 DES 更加安全。但同时它也要求有更高的处理能力，结果是造成了轻微的延迟和吞吐量的降低。AES 采用 128 位加密，速率要优于 3DES。 如果您选择 NULL，则会建立一条不加密的隧道。
验证算法	MD5（信息摘要 5）和 SHA1（安全哈斯算法）都是用来对数据包做认证的哈斯算法。SHA1 算法比 MD5 算法更安全，但相应的速度有所降低。
SA 使用期限 (秒)	在该栏目中可定义 IKE 安全关联在自动重新协商前存在的时间长度。最小值为 180 秒。 一个较短的 SA 生存时间可以通过更换加密和验证密钥的方法来增强 SA 的安全性，然而每次 VPN 隧道重新协商建立时，所有访问远端资源的用户都会临时被断掉。

完美保密（PFS）	完美向前保密(PFS)在阶段 2 IPsec SA 设置中被设置为 None(缺省)。这提供了更快速的 IPsec 建立，而不是最安全的。 选择 DH1 或 DH2 以应用 PFS。DH1 是指 Diffie-Hellman 组 1，有 768 位的随机数。DH2 是指 Diffie-Hellman 组 2，有 1024 位的随机数（更安全，但会较慢）。
启用重复侦测	当 VPN 设置逐步加强时，整个系统容易受到 DoS 攻击。IPsec 接收方可以检测并拒绝老的或者重复的数据包来防范重放攻击。选择该框可以启用重放攻击检测功能。
使用多个提案	选择该选框，当协商 IPsec SA 的时候，允许 ZyWALL 使用阶段 1 或阶段 2 加密和证明法则的任何一个。 当您使用多个提案时，ZyWALL 允许远端 IPsec 路由器选择加密和运算法则用于 VPN 隧道，即使他们比您为 VPN 规则配置的安全程度要低。 不选该选框表示当协商 IPsec SA 的时候，ZyWALL 只使用阶段 1 或阶段 2 加密和运算法则配置下列项目。
应用	点击应用可以保存设置。
取消	点击取消，退回到 VPN 界面，但不保存设置。

11.5 VPN 规则（IKE）：网络策略移动

首先进入 VPN 规则（IKE）界面，然后点击移动图标（），您可以见到网络策略移动界面。

图 95 VPN 策略（IKE）：网络策略移动



以下为界面相关的描述。

表 57 VPN 策略（IKE）：网络策略移动

标识	描述
网络策略信息	以下区域显示该 VPN 策略的基本网络参数。
名称	该区域显示策略名称。
本地网络	该区域显示位于 ZyWALL 后面 的一个或者一定范围内的计算机 IP 地址。
远程网络	该区域显示处于远端 IPSec 路由器后面的远程网络中的一个或者一定范围的 IP 地址。
网关策略信息	
网关策略	选择一个需要和该 VPN 网络政策相结合的 VPN 规则的名称（或网关策略）。 如果您不想给该网络策略结合任意一个网关策略，请从下拉列表框中选择资源回收桶。对任 何没有 相关 网关策 略的 网络策略来说，资源回收桶网关策略只是一个虚拟占位符。当资源回收桶中有一个网络策略的时候，在 VPN 规则（IKE）界面中的资源回收桶网关策略会自动显示出来。
应用	点击应用可以保存设置。
取消	点击取消可以退回到 VPN 界面，但不保存设置。

11.6 VPN 规则（手动）

请参考图 91 来了解在 web 配置界面中的图示说明。

点击 **VPN** 和 **VPN 规则（手动）** 标签可以打开 **VPN 规则（手动）** 界面。

使用此界面可管理 ZyWALL 使用手工密钥的 VPN 规则（通道）列表。

当使用 IKE 密钥管理有问题的时候，您也可以使用手工密钥管理。

图 96 VPN 规则（手动）



以下为界面相关的描述。

表 58VPN 规则（手动）

标识	描述
#	这是 VPN 策略的索引号。
名称	此处显示该 VPN 策略的标识名称。
启用	此处显示该 VPN 策略是否激活。Yes 表示规则激活，No 表示未激活。
本地网络	这是在 ZyWALL 后面的本地网络中的计算机 IP 地址。 当 VPN – 手动密钥-编辑界面中的本地网络地址类型区域配置为单一 IP 地址地址的时候，相同的（静态的）IP 地址会显示两次。当 VPN – 手动密钥-编辑界面中的本地网络地址类型区域配置为指定 IP 段地址的时候，此处会显示在一定范围的计算机内的开始和结尾的 IP 地址。 当 VPN – 手动 密钥-编辑界面中的本地网络地址类型区域配置为 IP 子网地址的时候，此处会显示一个（静态的）IP 地址和一个子网掩码。
远程网络	这是远程网络后面远程 IPSec 路由器上所接计算机的 IP 地址。 当远程网关地址区域显示 0.0.0.0 时，此处显示 N/A。 当 VPN -手动密钥-编辑界面上的本地网络 地址类型区 域配置为单一 IP 地址的时候，相同的（静态的）IP 地址会显示两次。 当 VPN-手动密钥-编辑 t 界面中的本地网络地址类型区域配置为指定 IP 段地址的时候，此处会显示在一定范围的计算机内 的开始和结尾的 IP 地址。 当 VPN -手动密钥-编辑界面中的本地网络地址类型区域配置为 IP 子网地址的时候，此处会显示一个（静态的）IP 地址和 一个子网掩码。
封装	此处会显示隧道模式或传输模式（Tunnel 为缺省选项）。
IPSec 算法	此处会显示 SA 使用的安全协议。 AH 和 ESP 都会增加 ZyWALL 的处理负荷，造成通信上的微小延时。
远程网关地址	这是远端 IPSec 路由器的静态 WAN 口 IP 地址或域名。
修改	点击编辑图标可以编辑该 VPN 策略。 点击删除图标可以删除该 VPN 策略。随后会弹出一个窗口询问您是否确定删除该 VPN 规则。当一条 VPN 策略被删除时，列表中后面的策略会上移一位。 点击拨号图标可以进行手工拨号连接。如果一条 VPN 隧道已经被建立了并且拨号成功，这样当您再次点击这个图标的时候，在界面底部的状态 栏中会出现一条警告消息。
添加	点击添加可以添加一条新的 VPN 策略。

11.7 VPN 规则（手动）：编辑

点击 VPN 规则（手动）界面中的编辑图标可以编辑 VPN 规则。在此界面可配置使用手工密钥的 VPN 规则，手工密钥管理在 IKE 密钥管理有问题的时候非常有用。

图 97 VPN 策略（手动）：编辑

VPN — 手动密钥 — 编辑

内容

☐ 启用

名称

☐ 允许通过IPsec通道进行NetBIOS传输

本地网络

地址类型

Single Address

开始IP地址

0 . 0 . 0 . 0

结束IP地址/子网掩码

0 . 0 . 0 . 0

远程网络

地址类型

Single Address

开始IP地址

0 . 0 . 0 . 0

结束IP地址/子网掩码

0 . 0 . 0 . 0

网关策略信息

我的ZyWALL

0 . 0 . 0 . 0

主要远程网关

0 . 0 . 0 . 0

手工设定

SPI

0

封装模式

Tunnel

启动的协议

ESP

加密算法

DES

验证算法

SHA1

加密密钥

验证密钥

应用

取消

以下为界面相关的描述。

表 59 VPN 策略（手动）：编辑

标识	描述
内容	
启用	选择该选框可以激活 VPN 策略。

161

名称	此处为 VPN 策略的标识名称，最多 32 个字符。您可以使用任意字符，包括空格，但是 ZyWALL 会忽略末尾的空格。
允许通过 IPSec 通道进行 NetBIOS 传输	当 ZyWALL 为网桥模式时此处不可用。 NetBIOS（网络基本输入输出系统）是 TCP 或 UDP 数据包，它可以让局域网内的计算机互相通信。对于一些拨号服务如 PPPoE 或 PPTP，NetBIOS 封包经常导致建立一些不是需要的拨号。然而在某些时候必须通过 NETBIOS 与 WAN 上的计算机进行通信。有时候为了允许本地计算机查找到远端网络，允许 NetBIOS 通过 VPN 隧道也是很重要的，反之亦然。 选择该选框通过 VPN 连接发送 NetBIOS。
本地网络	本地 IP 地址必须是静态的，它相对应于在远端 IPSec 路由器配置的远端 IP 地址。 两条激活的 SA 中可以配置相同的本地或远端 IP 地址，但是不能同时一样。您可以使多条 SA 使用相同的本地和远端 IP 地址，但是随时只会有 一条处于激活状态。
地址类型	从下拉菜单中选择单一 IP 地址，指定 IP 段地址，或 IP 子网地址。Singel 代表单一的 IP 地址，指定 IP 段 地址代表一个地址范围，IP 子网 地址代表一个子网段。
开始 IP 地址	当地址 类型中配置为单一 IP 地址的时候，输入 ZyWALL 的一个（静态）IP 地址。当地址类型中配置为指定 IP 段地址的时候，输入一个 IP 地址范围的起始（静态）IP 地址。当地址类型 中配置为 IP 子网地址的时候，输入您 ZyWALL 本地子网的其中 一个（静态）IP 地址。
结束 IP 地址/子网掩码	当地址 类型中配置为单一 IP 地址的时候，此处为 N/A。当地址类型中配置为指定 IP 段 地址的时候，输入一个 IP 地址范 围的末尾（静态）IP 地址。当地址类型中配置为 IP 子网地址的时候，输入您 ZyWALL 本地子网的子网掩码。
远程网络	远端 IP 地址必须是静态的，它对应着远端 IPSec 路由器的本地 IP 地址。 两条激活的 SA 中可以配置相同的本地或远端 IP 地址，但是不能同时一样。您可以使多条 SA 使用相同的本地和远端 IP 地址，但是随时只会有 一条处于激活状态。
地址类型	从下拉菜单中选择单一 IP 地址，指定 IP 段地址，或 IP 子网地址。Singel 代表单一的 IP 地址，指定 IP 段地址代表一个地址范围，IP 子网地址代表一个子网段。

开始 IP 地址	当地址类型中配置为单一 IP 地址的时候,输入远端 IPSec 路由器的一个(静态) IP 地址。 当地址类型中 配置为指定 IP 段 地址的时候,输入一个 IP 地址范围的起始(静态) IP 地址。当 地址类型中配置为 IP 子网地址的时候,输入远端 IPSec 路由器后面子网内的其中一个(静态) IP 地址。
结束 IP 地址/子网掩码	当地址 类型中配置为单一 IP 地址的时候,此处为 N/A。当地址类型中配置为指定 IP 段 地址的时候,输入一个 IP 地址范 围的末尾(静态) IP 地址。当地址类型中配置为 IP 子网 地址 的时候,输入远端 IPSec 路由器后面子网内的子网掩码。
网关策略信息	
我的 ZyWALL	当 ZyWALL 处于路由模式的时候,输入 ZyWALL 的 WAN 口 IP 地址,或者域名,或者设置为 0.0.0.0。 如果您将此处设为 0.0.0.0,那么 ZyWALL 在设立的 VPN 隧道中使用它的当前的 WAN 口 IP 地址(静态或动态)。如果两个 WAN 口连接断开的话,当使用拨号备份时,对于 VPN 隧道 ZyWALL 使用拨号备份 IP 地址,或者当用流量重定向时 ZyWALL 使用 LAN IP 地址时。 否则您可以选择我的域名称,然后设置一个已经配置的动态域名(在 DDNS 界面中),让 ZyWALL 使用动态域名的 IP 地址。当 ZyWALL 为网桥模式时,此处为只读并显示 ZyWALL 的 IP 地址。如果在 VPN 建立后我的 ZyWALL 的 IP 地址被更改,则 VPN 隧道将会重新建立。
主要远程网关	输入您准备建立 VPN 的 IPSec 网关的 WAN 口 IP 地址或域名(最多 31 个 字符串)。
手工设定	
SPI	输入一个唯一的 1 到 4 个字符长度的 SPI(安全参数索引)值。有效的字符为“0, 1, 2, 3, 4, 5, 6, 7, 8 和 9”。
封装模式	从下拉菜单中选择隧道模式或传输模式。

启用的协议	如果您想使用 ESP （封装安全负载），您可以选择 ESP 。 ESP 协议比 AH 协议多提供了加密的服务。如果您在这里选择了 ESP ，您必须选择加密算法和认证算法区域的选项（在下面进行描述）。如果您使用 AH （认证包头协议）可以选择 AH 。 AH 协议（RFC 2402）被设计用来提供完整性、认证性、序列完整性（防重放攻击），而不能像 ESP 那样提供保密功能。在对保密性无要求的应用中， AH 协议可以用来保证数据的完整性。这种方案不能保护信息不被传播，但是能校验信息的完整性并对信息发起者进行认证。如果您选择了 AH ，还必须选择认证算法区域的选项（在下面描述）。
加密算法	从下拉菜单中选择 DES ， 3DES 或 NULL 。 当使用 DES 的时候，收发双方需要知道加密密钥，由此可以用于加密和解密信息，或生成，并标识一个信息认证码。 DES 加密算法使用 56bit 的密钥， 3DES 使用 168bit 的密钥。这样 3DES 会比 DES 更安全，但需要更多的处理时间，这样会导致时延加大和吞吐量降低的结果。如果您不想使用加密，可以选择 NULL 。当您选择 NULL 的时候，您不必输入一个密钥。
认证算法	从下拉菜单中选择 SHA-1 或 MD5 。 MD5 和 SHA-1 都是哈希算法，用于认证数据包。 SHA-1 算法比 MD5 更强健，但是效率更低。 MD5 具有低的安全性，而 SHA-1 具有高的安全性。
加密密钥	如果采用 DES ，请输入一个 8 字符长度的密钥。如果采用 3DES ，请输入一个 24 字符长度的密钥。任何字符串都可以使用，包括空格，但是末尾的空格会被忽略。
验证密钥	请输入一个唯一的认证密钥。如果采用 MD5 ，请输入一个 16 字符长度的密钥。如果采用 SHA-1 ，请输入一个 20 字符长度的密钥。任何字符串都可以使用，包括空格，但是末尾的空格会被忽略。
应用	点击应用，可以保存设置。
取消	点击取消，可以不保存设置并退出界面。

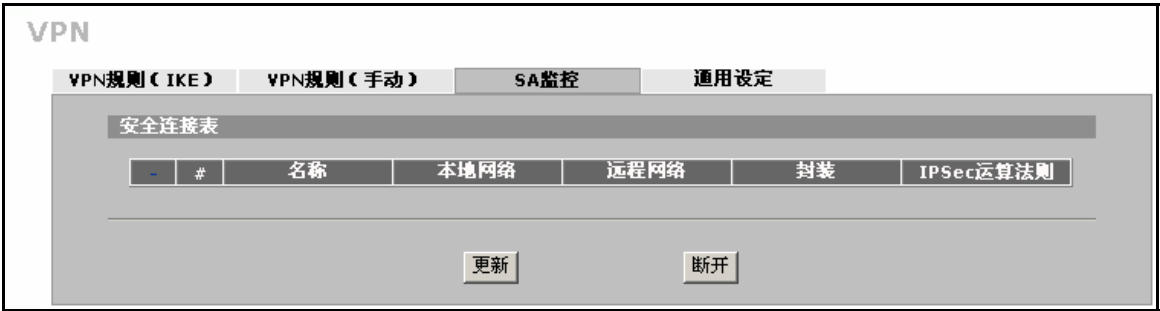
11.8 VPN SA 监控

在 web 设置界面里，先点击 **VPN**，然后点击 **SA Monitor** 标签。使用该界面，您可以查看和管理已激活的 **VPN** 连接。

安全关联 **SA**（**Secure Association**）是单向的，在安全网关之间定义了如何使用安全服务进行通信。它由下列元素组成：安全参数索引 **SPI**、**IP** 目的地址、安全协议（**AH** 或 **ESP**）。

这个界面显示了激活的 VPN 连接。您使用 Refresh 就可以显示激活的 VPN 连接。该界面为只读界面。

图 98VPN：SA 监控



以下为界面相关的描述。

表 60 VPN：SA 监控

标识	描述
#	这是 SA 的索引号。
名称	此处为 VPN 策略的标识名称。
本地网络	此处显示正在使用 ZyWALL 的 VPN IPSec 功能的计算机 IP 地址。
远程网络	此处显示位于远端 IPSec 路由器后面的远端网络中的计算机 IP 地址。
封装	此处会显示隧道或传输模式。
IPSec 运算法则	此处会显示 SA 所使用的安全协议。 AH 和 ESP 都会增加 ZyWALL 的处理负荷，造成通信上的微小延时。
更新	点击 Refresh 可以显示当前激活的 VPN 连接。
断开	选择一个 SA 的索引号，然后点击 Disconnect，可以断开此连接。

11.9 VPN 通用设定

点击 VPN，然后点击通用设定标签可以打开 VPN 通用设定界面。利用该界面您可以修改 ZyWALL 的通用设定。

图 99 VPN：通用设定

VPN

VPN规则（IKE）

VPN规则（手动）

SA监控

通用设定

IPSec 计时器设置

输出闲置计时器

120

(30~3600秒, 0表示计时器无效)

输入闲置计时器

0

(30~3600秒, 0表示计时器无效)

网关域名更新计时器

5

(2~60分, 0表示计时器无效)

调整TCP最大段的大小

Auto

0

☐ VPN规则跳过应用于本地和远程重复地址范围的VPN规则。

(警告: 当不勾选时, 由于VPN被触发您可能无法访问设备。)

应用

重置

以下为界面相关的描述。

表 61 VPN：通用设定

标识	描述
输出闲置计时器	如果在规定的时段内 ZyWALL 没有收到发送到远端 IPSec 路由器的数据包的回复,它就会检查VPN的连接情况。如果远端的IPSec 路由器没有回复, ZyWALL 就会自动断开该 VPN 的连接。 输入一个时 间段 (30 到 3600 秒), 规定了 ZyWALL 在检查到远端 IPSec 路由器的 VPN 连接之前的等待时间。 输入 0 可以取消该特征。
输入闲置计时器	如果在规定的时段内 ZyWALL 没有收到来自远端 IPSec 路由器的数据包, 它就会检查 VPN 的连接情况。如果远端的IPSec 路由器没有回复, ZyWALL 就会自动断开该 VPN 的连接。 输入一个时 间段 (30 到 3600 秒), 规定了 ZyWALL 在检查到远端 IPSec 路由器的 VPN 连接之前的等待时间。 输入 0 可以取消该特征。

网关域名更新计时器	当您输入一个域名来标识 ZyWALL 和/或远端安全网关的时候，该区域才会有用。 输入一个时间段（2 到 60 分钟），规定了 ZyWALL 通过一个 DNS 服务器更新域名到 IP 地址的映射之前的等待时间。 如果 ZyWALL 发现该域名使用了一个不同的 IP 地址（使用该 VPN 通道的任何用户都将会暂时断开连接），它就会重新建立该 VPN 通道。 输入 0 可以取消该特征。
调整 TCP 最大段的大小	因在 ZyWALL 针对 VPN 加密数据包后，TCP 包变大，ZyWALL 的数据包会比连接的 MTU（Maximum Transmit Unit，最大传输单位）大。 在大多数情况下，你应保留此项设置为 Auto。ZyWALL 自动设置基于封装类型的 VPN 加密的 TCP 包最大分段尺寸。 选择 Off 则对加密 TCP 包不调整 MSS。 如果你的网络环境引起分片问题，影响到吞吐性能，你可以手工设置 VPN 加密的 TCP 数据包一个较小 MSS。选择用户定义，并指定大小，可从 0~1460 byte 选取。0 时 ZyWALL 使用自动设置。
VPN 规则跳过应用于本地和远程重复地址范围的 VPN 规则	当你配置一个 VPN 规则时，ZyWALL 会检查确认在本地及远程网络中的 IP 地址没有重叠。如果你需要配置一个本地和远程 IP 地址重叠的 VPN 规则，选中此选框禁用此项检查。 注意：如果一个 VPN 策略的本地及远程 IP 地址重叠，由于 ZyWALL 将自动触发一个 VPN 通道到具有同样 IP 地址的远程设备，你或许不能访问你局域网中的设备。
应用	点击应用可以保存设置。
重置	点击重置可以重新配置该界面。

11.10 远程办公 VPN/IPSec 的范例

以下范例向您介绍多个远程办公用户如何创建连接到一个总部 ZyWALL 的 VPN 连接。远程办公用户采用动态获得 WANIP 的 IPSec 网关。ZyWALL 在总部具有一个静态的公网 IP 地址。

11.10.1 远程办公用户分享一个 VPN 规则范例

参照下图和下表，范例中说明多个远程办公用户（图中的 A，B 和 C）使用相同的 VPN 规则同时接入到总部（图中的 HQ）的 ZyWALL 上。远程办公用户不需要做域名到他们各自 IPSec 网关 WAN 口 IP 地址的映射。但是这些用户必须使用相同的 IPSec 参数，但是他们各自的本地 IP 地址（或地址范围）不能重叠。

图 100 远程办公用户使用相同的 VPN 规则范例

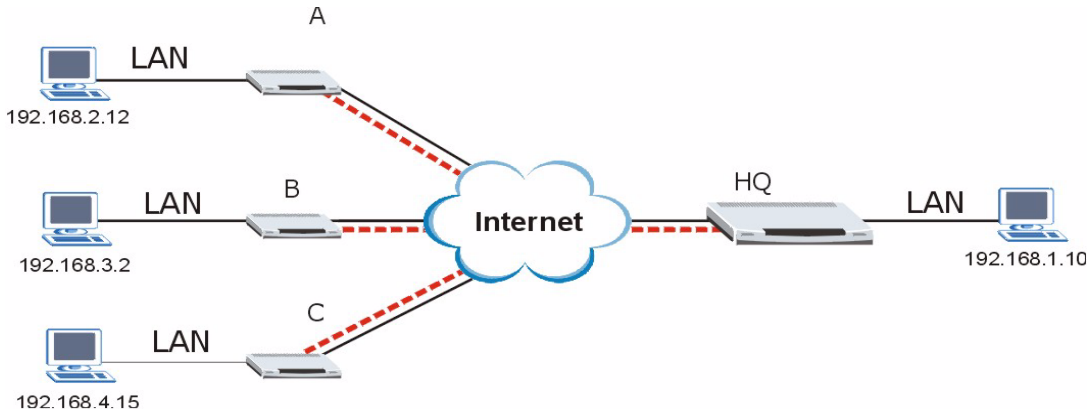


表 62 远程办公用户使用相同的 VPN 规则范例

设置区域	远程办公用户	总部
我的地址:	0.0.0.0 (获得由 ISP 分配的动态地址)	公网静态 IP 地址
远程网关地址:	公网静态 IP 地址	0.0.0.0 (只有远程办公用户才可以初始化 IPSec 通道)
本地网络 - 单一 IP 地址:	远程办公用户 A: 192.168.2.12 远程办公用户 B: 192.168.3.2 远程办公用户 C: 192.168.4.15	192.168.1.10
远程网络 - 单一 IP 地址:	192.168.1.10	0.0.0.0 (N/A)

11.10.2 远程办公用户使用各自的 VPN 规则范例

在此范例中，远程办公用户（图中的 A，B 和 C）在 IPSec 网关中设置域名到他们各自动态 WAN 口 IP 地址的映射（使用动态 DNS 去做）。

利用主动协商模式（参考章节 19.8.1 一节），ZyWALL 可以使用 ID 类型和内容来区

分 VPN 规则。远程办公用户可以使用不同的 VPN 规则同时接入到总部的 ZyWALL 上。他们可以使用不同的 IPSec 参数。总部 ZyWALL 上设置的本地 IP 地址（或地址范围）可以重叠。但是远程办公用户的 IPSec 网关上设置的本地 IP 地址不能重叠。

下图范例中，3 个远程办公用户使用不同的 VPN 规则创建到总部 ZyWALL 的 VPN 连接。总部的 ZyWALL（图中的 HQ）使用 ID 类型和内容来区分进入的 SA。

由于总部的 ZyWALL 可以通过解析它们的域名来找到远程办公用户，所以它也能初始化到远程办公用户的 VPN 连接。

图 101 远程办公用户使用不同的 VPN 规则范例

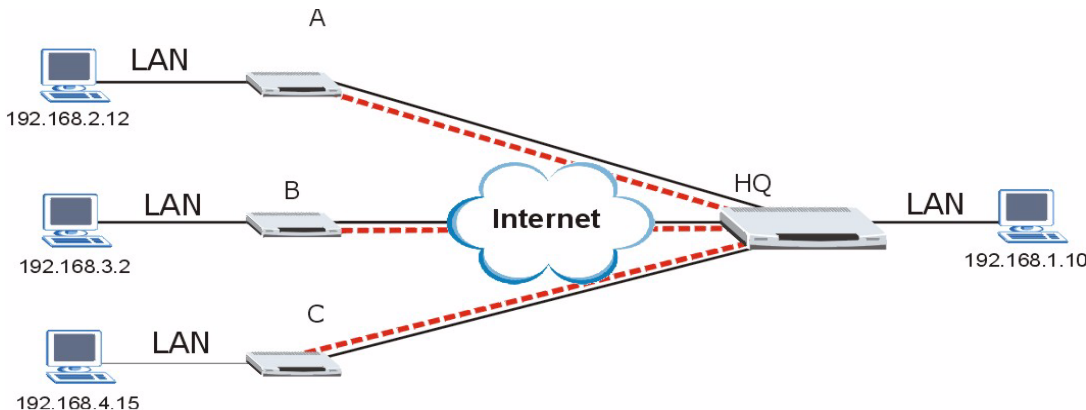


表 63 远程办公用户使用不同的 VPN 规则范例

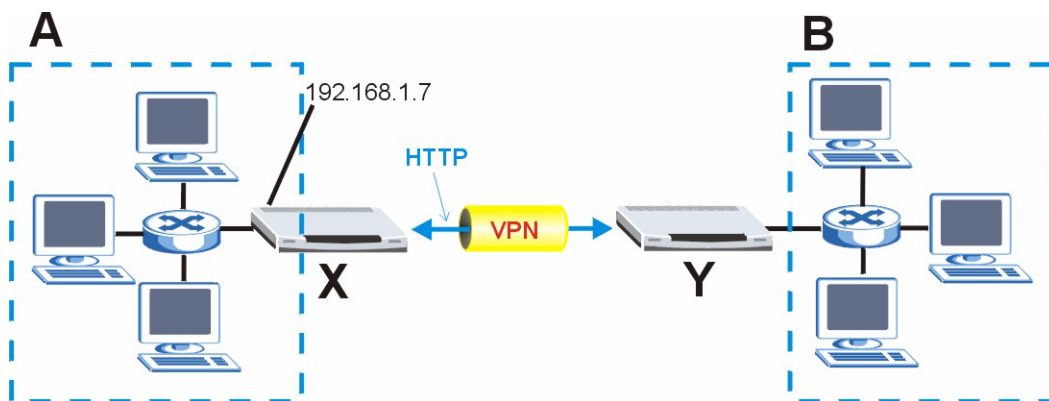
远程办公用户	总部
所有远程办公用户都支持的规则:	所有规则都支持的设置:
我的地址 0.0.0.0	我的地址: bigcompanyhq.com
远程网关地址: bigcompanyhq.com	本地网络 - 单一 IP 地址: 192.168.1.10
远程网络 - 单一 IP 地址: 192.168.1.10	本地 ID 类型: E-mail
对方 ID 类型: E-mail	本地 ID 内容: bob@bigcompanyhq.com
对方 ID 内容: bob@bigcompanyhq.com	
远 程 用 户 A (telecommutera.dydns.org) (telecommutera.dydns.org) (telecommutera.dydns.org)	总部 ZyWALL 规则 1:
本地 ID 类型: IP	对方 ID 类型: IP
本地 ID 内容: 192.168.2.12	对方 ID 内容: 192.168.2.12
本地 IP 地址: 192.168.2.12	远程网关地址: telecommutera.dydns.org

	远程 地址 192.168.2.12
远程用户 B (telecommutera.dydns.org)	总部 ZyWALL 规则 2:
本地 ID 类型: DNS	对方 ID 类型: DNS
本地 ID 内容: telecommuterb.com	对方 ID 内容: telecommuterb.com
本地 IP 地址: 192.168.3.2	远程网关地址: telecommuterb.dydns.org
	远程地址 192.168.3.2
远程用户 C (telecommutera.dydns.org)	总部 ZyWALL 规则 3:
本地 ID 类型: E-mail	对方 ID 类型: E-mail
本地 ID 内容: myVPN@myplace.com	对方 ID 内容: myVPN@myplace.com
本地 IP 地址: 192.168.4.15	远程网关地址: telecommuterc.dydns.org
	远程地址 192.168.4.15

你可以许可他人使用服务（例如 Telnet 或 HTTP）经过 VPN 通道来管理 ZyWALL。ZyWALL 的一个端口必须 VPN 规则的本地网络的一部分，如果你想不允许 WAN 端口的远程管理，这能是 ZyWALL 的 LAN 端口。你还必须配置远程管理（远程 MGMT）许可从特定端口来的服务的管理接入。

在下面示例中,VPN 规则的本地网络(A)包括了 ZyWALL 的 LAN IP 地址 192.168.1.7, 在远程网络的某人能使用服务（例如 HTTP）经 VPN 通道访问 ZyWALL 的 LAN 接口。远程网络必须配置允许 HTTP 访问 ZyWALL 的 LAN 接口。

图 102 VPN 远程管理示例



第 12 章 证书

本章将会向您介绍公匙密钥证书的背景信息和使用方法。

ZyWALL 可以使用证书（也叫做数字 ID）来认证用户。证书是基于公私密钥对。数字证书采用公钥体制，即利用一对互相匹配的密钥进行加密和解密。每个用户自己设定一特定的仅为本人所知的私有密钥私钥)用它进行解密和签名;同时设定一把公共密钥（公钥）并由本人公开，为一组用户所共享，用于加密和验证签名。当发送一份保密文件时，发送方使用接收方的公钥对数据加密，而接收方则使用自己的私钥解密，这样信息就可以安全无误地到达目的地了。通过数字的手段保证加密过程是一个不可逆过程，即只有用私有密钥才能解密。用户也可以采用自己的私钥对信息加以处理，由于密钥仅为本人所有，这样就产生了别人无法生成的文件，也就形成了数字签名。

CA 机构，又称为证书授权（Certificate Authority）中心，CA 中心为每个使用公开密钥的用户发放一个数字证书，数字证书的作用是证明证书中列出的用户合法拥有证书中列出的公开密钥。CA 机构的数字签名使得攻击者不能伪造和篡改证书。您可采用一些商业或政府等部门提供的 CA 服务，也可以使用 ZyWALL 自身提供的证书服务。

在公钥加密盒解密中，每个主机都有两个密钥。一个是公共的，能够公开可用的；另一个是私有的，必须保证安全的。公钥加密的常规操作如下：

1. Tim想要发送一个私密的信息给Jenny。Tim生成了一个公钥对。
2. Tim保有私钥并使公钥公开可用。
3. Tim用他的密钥对信息进行加密并发送给Jenny。
4. Jenny受到该信息并用Tim的公钥解密。
5. 除此之外，Jenny用她自己的私钥对一条信息进行加密并且Tim用Jenny的公钥对该信息解密。

ZyWALL 可以使用基于公钥体制的证书来认证尝试建立连接的用户在建立连接以后发送的数据不会被加密。而连接建立以后的数据保护方法是基于连接的类型。例如，一个VPN 通道可以使用 3DES 加密算法。证书的认证可以使用它的私钥来做证书签名。任何人都可以使用 CA 提供的公钥来确认证书。

证书路径就是 CA 发放一个有效证书的层次。证书路径可以定义为完整信任链（包含来自可信 CA 的证书），该链的起点为特定的证书，终点为证书层次结构中的根 CA。如果该

路径上的任何证书已经过期或作废，ZyWALL 将不会再信任该证书。

在时间溢出之前就被作废的证书目录叫做 **CRL**（作废证书目录）。ZyWALL 可以在服务器上的作废证书列表中比对查询对端的证书是否已经作废。管制或操纵证书与公钥及私钥的策略、标准和软件的结构叫做 **PKI**（公钥基本结构）。PKI 是指由数字证书、证书颁发机构（CA）以及其它注册机构组成的一套系统。

12.1. 证书的优点

证书具有以下优势：

不管您需要对多少台设备做认证，ZyWALL 只需要保存它信任的 CA 的证书即可。

密钥的分发很简单，并且很安全。您可以将公钥随便发送出去，而不用将私钥发送出去。

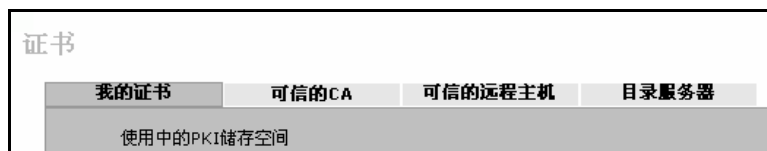
12.2 自签名证书

虽然公钥体制变得很成熟了，但是它还不能应用在某些地方。您可以让 ZyWALL 充当 CA 来签名自己的证书。

12.3 配置汇总

下图说明如何配置 ZyWALL 上的证书

图 103 证书配置说明



使用我的证书界面，您可以生成和输出自签名证书或证书请求和引入ZyWALL的CA签名证书。

使用可信的CA界面，您可以将CA证书保存到ZyWALL。

使用可信的远程主机界面，您可以引入自签名证书。

使用目录服务器界面，您可以配置一个目录服务器的地址列表（包括有效的和已经废除的目录列表）。

12.4 我的证书

依次点击**安全，证书，我的证书**可以打开 ZyWALL 的证书和证书申请的汇总表。证书用黑色表示，证书申请用灰色表示。请参看下图。

图 104 我的证书



以下为界面相关的描述。

表 64 我的证书

标签	描述
使用 PKI 存储空间	本栏显示的是 ZyWALL 中当前的 PKI 存储空间的使用率。当存储百分比在 80% 以下的时候，状态条是绿色的，当超过了 80%，状态条就变成红色的了，您需要将已经过期的，或没用的证书删除掉，然后再添加新的证书。
取代	当 ZyWALL 有出厂缺省证书的时候，会出现此按钮。所有 ZyWALL 新出厂时，一般都采用出厂缺省证书。ZyWALL 会建议您用 ZyWALL 的 MAC 地址来替换出厂缺省证书。
#	此处为证书索引号。
名称	此处显示证书的标识名称。建议您给每一个证书分配一个不同的名称。

类型	此处显示证书的类型。 REQ 代表一个证书申请，不是一个有效的证书。ZyWALL 会给 CA 发送一个证书申请随后返回一个证书。您可使用我的证书 导入界面来注入该证书，然后替换掉相应的证书申请。 SELF代表一个自签名的证书。 *SELF代表缺省的自签名证书 ZyWALL 用它来对进入 ZyWALL 的可信任远程主机证书做签名。 CERT代表一个由 CA 发放的证书。
主题	此处显示证书所有者的标识信息，例如 CN（一般名称）OU（组织单位或部门）O（组织或公司）和 C（国家）建议您给每一个证书提供一个唯一的标识。
发行者	此处显示证书的发行 CA 描述信息，例如一个一般名称，组织单位或部门，组织或公司和国家。对于自签名证书来说，此处的信息和主题处显示的一样。
有效期自	此处显示证书开始应用的日期。如果证书还不能使用，此处会显示一个红色的信息“Not Yet Valid！”。
到期日	此处显示证书失效的日期。如果证书将要到期或已经到期，此处会显示一个红色的信息“Expiring！”或“Expired”。
修改	点击细节图标可以打开一个界面，显示证书的纵深列表信息。 点击删除图标可以删除证书。如果证书正在进行配置，您不能删除该证书。请按照以下步骤来删除在类型中显示为*SELF的证书。 1. 确保没有其它的特征，例如 HTTPS, VPN, SSH...正在配置使用*SELF证书。 2. 点击细节图标，切换到其它的自签名证书。 3. 选择为导入的远程主机签发证书的预设自动签发证书选框。 4. 点击应用保存设置，回到我的证书界面。 5. 原来显示为*SELF的证书现在显示为SELF，随后您可以进行删除。 注意，执行完此操作后，后面的证书会前移一位。
导入	点击导入，您可以打开一个界面，在此处，您可以将您从 CA 注册申请的证书从计算机保存到 ZyWALL 上。

创建	点击 创建 ，您可以切换到 ZyWALL 生成一个证书或一个证书申请的界面里面。
更新	点击 更新 ，可以显示当前有效的证书状态。

12.5 导入一个证书

依次点击**安全**，**证书**，**我的证书**和**导入**，可以打开**我的证书 导入**界面。您在此可以将一个现存的证书保存到**ZyWALL** 中。

注意：您只能导入一个和 **ZyWALL** 生成证书申请的响应相匹配的证书。

您导入的证书将替换掉在**我的证书**界面中响应的请求。

在您导入证书之前，您需要将证书文件名中的任何空格都去掉。

12.5.1 证书文件格式

您想要导入的 **CA** 证书需要是下面的其中一种文件格式。

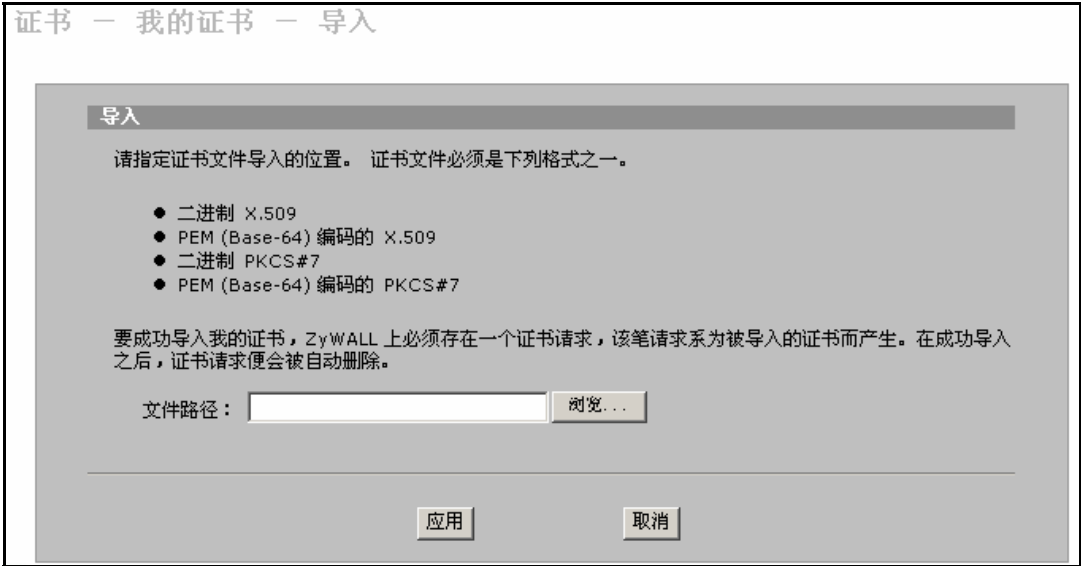
二进制 X.509：这是 ITU-T 中定义的 **X.509** 证书的格式。

PEM(Base-64)编码的 X.509：这是保密加强邮件格式**PEM**，它使用 **Base-64**编码方式将一个二进制的 **X.509** 证书转化为一个可输出形式。

二进制 PKCS#7：这是一种通用句法数据(包括数字符号)加密的标准。**ZyWALL** 目前允许包括一个单独证书的 **PKS#7** 文件的输入。

PEMBase-64编码的 PKCS#7这是保密加强邮件格式**PEM**，它使用 **Base-64**编码方式将一个二进制的 **PKCS#7** 证书转化为一个可输出模式。

图 105 导入证书



以下为界面相关的描述。

表 65 导入证书

标识	描述
文件路径	输入您准备上传的证书路径，或点击浏览来找到该证书。
浏览	点击浏览，找到该证书。
应用	点击应用，在 ZyWALL 上保存证书。
取消	点击取消，退回到我的证书界面。

12.6 创建一个证书

依次点击 安全，证书，我的证书和创建可以打开我的证书 创建界面。在该界面中，您可以创建一个自签名的证书，在 CA 上注册一个证书或生成一个证书申请，请参考下图。

图 106 创建证书

证书 — 我的证书 — 创建

证书名称

主体信息

公用名称

主机 IP 地址

0 . 0 . 0 . 0

主机域名

电子邮件

组织单位

组织

国家

密钥长度

1024 位数

注册选项

产生一个自行签发的证书

产生一个证书请求，并在本地保存一份副本以备稍后手动登记

产生一个证书请求，并立即在线登记证书

登记协议

Simple Certificate Enrollment Protocol (SCEP)

CA 服务器地址

CA 证书

VeriSign.cer (参阅 [可信的CA](#))

请求识别

密钥

应用

取消

以下为界面相关的描述。

表 66 创建证书

标识	描述
证书名称	输入一个最多 31 个 ASCII 字符的证书标识名称。
主体信息	您在此处可以记录证书拥有者的标识信息。您不用每个选项都输入，但是公用名称处需要输入相关信息。CA 在发放证书的时候有时会在主体信息处添加一些信息例如一个序列号，所以希望每一个证书都能有一个唯一的标题信息。
公用名称	选择一个选项，您可以通过 IP地址，域名或 e-mail 地址来标识证书的所有者。其中域名和 e-mai 地址最多 31 个 ASCII 字符，域名和 e-mail 地址仅供标识使用，可以是任何字符串。
组织单位	输入一个最多 127 位 ASCII 字符来标识证书拥有者所属的政府部门或单位。您可以使用任何字符串，包括空格，但是末尾空格会被忽略。

组织	输入一个最多 127 位 ASCII 字符来标识证书拥有者所属的公司或团队。您可以使用任何字符串,包括空格,但是末尾空格会被或略。
国家	输入一个最多 127 位 ASCII 字符来标识证书拥有者所属的国家。您可以使用任何字符串,包括空格,但是末尾空格会被或略。
密钥长度	从下拉菜单中选择一组密钥长度 (512 或 2048) 密钥长度越大就越安全。但是长密钥需要占用更多的 PKI 存储空间。
注册选项	以下的选项用来决定证书生成的方法和时间。
产生一个自行签发的证书	点选 产生一个自行签发的证书 , 可以让 ZyWALL 生成证书, 自己作为 CA。这样您就不需要给证书提供一个 CA 了。
产生一个证书请求, 并在本地保存一份副本以备稍后手动登记	点选 产生一个证书请求, 并在本地保存一份副本以备稍后手动登记 , 可以让 ZyWALL 生成并存储一个证书申请。 您可以使用 我的证书 细节 界面 (查看章节 20.7) 来查看证书申请和复制发送到 CA。
产生一个证书请求, 并立即在线登记证书	点选 产生一个证书请求, 并立即在线登记证书 , 可以让 ZyWALL 生成一个证书申请, 然后将一个 CA 应用到证书中。 您需要在 可信的CA 界面中预先输入一个 CA 的证书。 当您选择此选项的时候, 您需要选择 CA 的注册协议, 从下拉菜单中选择 CA 的证书, 然后输入 CA 的服务器地址。如果 CA 需要, 您同时还需要在 参阅和密钥 中输入相关信息。
登记协议	从下拉菜单中选择 CA 的注册协议。 Simple Certificate Enrollment Protocol (SCEP) 是由 VeriSign 和 Cisco 开发的基于 TCP 的注册协议。 Certificate Management Protocol (CMP) 是由 IETF 的公钥体制 X.509 工作组开发的基于 TCP 的注册协议, 在 RFC 2510 中做了规定。
CA证书	从 CA证书 下拉菜单中选择 CA 的证书。 您需要在 可信的CA 界面里已经输入了 CA 的证书。点击 可信的CA , 回到 可信的CA 界面中, 在此您可以查看 (和管理) ZyWALL 的可信任 CA 的证书列表。

请求识别	当您选择了 产生一个证书请求，并立即在线登记证书 ，那么 CA 会在您发送证书申请的 时候，要求您提供一个参考号和密钥来识别您。如果您的 CA 使用 CMP 注册协议，请在 参阅 和 密钥 的区域中输入 相关信息。如果您的 CA 使用的是 SECP 注册协议，只要输入 密钥 区域的相关信息即可。
密钥	输入 CA 给您的密钥。
应用	点击 应用 可以开始生成证书或证书申请。
取消	点击 取消 ，可以退回到 我的证书 界面。

当您在 **我的证书 创建**界面中点击了**应用**，您可以看到一个界面，会提示您 ZyWALL 正在生成自签名证书或证书申请。

当 ZyWALL 成功注册了一个证书或者生成了一个证书申请或一个自签名证书，您会见到一个界面，带有一个**返回**按钮，点击此按钮可以回到**我的证书**界面。

如果您配置 **我的证书 创建**界面，让 ZyWALL 注册一个证书，但是证书注册 没有成功，您会见到一个界面，带有一个**返回**按钮，点击此按钮可以回到**我的证书 创建**界面。您可以在 **我的证书 创建**界面中检查您的信息。如果 您想在线注册一个证书，请确保 CA 信息正确，网络连接正常工作。

12.7 证书详细内容

依次点击 **安全，证书，我的证书** 可以打开**我的证书**界面（参考图 104）点击细节图标，您可以打开 **我的证书 细节**界面。您可以使用该界面来查看更多的证书相关信息，修改证书名称。对于自签名证书来说，您可以设置它来让 ZyWALL 能够对输入到 ZyWALL 上的可信任的远程主机证书做签名。

图 107 证书详细内容

证书 — 我的证书 — 细节

名称

auto_generated_self_signed_cert

属性

☒ 为导入的远程主机签发证书的预设自动签发证书。

证书路径

Searching...

更新

证书信息

Type	Self-signed X.509 Certificate
Version	V3
Serial Number	946684930
Subject	CN=ZyWALL 2 Plus Factory Default Certificate
Issuer	CN=ZyWALL 2 Plus Factory Default Certificate
Signature Algorithm	rsa-pkcs1-sha1
Valid From	2000 Jan 1st, 00:00:00 GMT
Valid To	2030 Jan 1st, 00:00:00 GMT
Key Algorithm	rsaEncryption (512 bits)
Subject Alternative Name	EMAIL=factory@auto.gen.cert
Key Usage	DigitalSignature, KeyEncipherment, KeyCertSign
Basic Constraint	Subject Type=CA, Path Length Constraint=1
MD5 Fingerprint	27:6d:5a:28:73:34:58:70:06:a3:e7:03:e8:ad:f9:67
SHA1 Fingerprint	4e:f9:9d:cb:05:53:e0:05:92:6c:a4:3d:e1:41:52:d9:09:98:71:7d

PEM (Base-64) 编码格式的证书

```

-----BEGIN CERTIFICATE-----
MIIBPDCCAU6gAwIBAgIBOg1EAjANBgkqhkiG9w0BAQUFADAOMTIwMAYDVQQDEyla
eVdBTEwgMiBQbHVzIEZyY3RvcnkRGVnYXVsdCBDZXJ0aWZpY2FOZTAEFw0wMDAx
MDEwMDAwMDBaFw0zMDAxMDEwMDAwMDAmdQxmMjAwBgNVBAMTKVp5V0FMTCAyIFBs
dXNMcG9yZSBEZWZhdWx0IENlcnRpZmljYXR1MFwwDQYJKoZIhvcNAQEBBQAD
SwAwSAJBAP51yIiHWK0WeiR4c9gGVNZgHbtncIB3HiyBN367YJXBB9fUFL7eaVjg
613EJ1k/NBLAKTyact464EDA5U3dq0sCawEAAAaNIMEYwDgYDVR0PAQEBAQDAgKk
MCAGAUUdEQQZMBEwBFWZlY3Rvcn1AYXV0by5nZW4uY2Y2YyDASBgNVHRMBAQAECDAG
AQH/AgEBMA0GCsQGS1b3DQEBBQUAA0EAAANKtrzt18DJysHufUfJbKQ3Bg9X39vWky
aahQdWVLxjzMvw/zmfTUUE2pM1skwipz0ZJnlmKjt0iHXWdypG9PJQ==

```

导出

应用

取消

以下为界面相关的描述。

表 67 证书详细内容

标识	描述
名称	此处为证书的标识名称。如果您想修改名称，可以输入最多 31 个字符来标识此证书。您可以使用任何字符（不包括空格）。
为导入的远程主机签发证书的预设自动签发证书	点选此框可以让 ZyWALL 使用该证书来对输入到 ZyWALL 上的可信任远程主机证书做签名。该选框只对自签名证书有效。如果该选项已经选上了，您就不能在此界面中清除它。除非您在其它自签名证书的详细内容界面中选中此选项，那么在以前设置用来对输入的可信任远程主机证书做签名的证书详细内容界面中的选项就会自动清除。
导入远程主机证书	对输入的可信任远程主机证书做签名的证书详细内容界面中的选项就会自动清除。
证书路径	点击 更新 按钮，可以在只读文本框中显示 CA 有效证书的层次。如果该 CA 是您已经输入的可信任 CA 中的一个，那么它可能是列表中唯一的 CA 。如果证书是自签名证书，那么证书本身在列表中就是唯一的。如果在路径上的任何证书已经过期或无效了，那么 ZyWALL 将不会信任该证书，在此处会显示“ Not 可信的”。
更新	点击 更新 可以显示证书路径。
证书信息	此处为只读信息，都是关于证书的详细信息。
类型	此处显示证书的一般信息。“ CA-signed ”说明一个 CA 对证书做签名。 “ Self-signed ”说明证书的拥有者签名该证书不是一个 CA 。 “ X.509 ”说明该证书是根据 ITU-T X.509 建议使用的公钥体制证书定义的格式来创建和签名的。
Version	此处显示 X.509 的版本号。
Serial Number	此处显示由 CA 或由 ZyWALL 生成的证书的标识号码。
Subject	此处显示证书拥有者的标识信息，例如普通名称（ CN ）组织单位（ OU ）组织机构（ O ）和国家（ C ）。
Issuer	此处显示发放证书的 CA 标识信息，例如普通名称，组织单位，组织机构和国家。对于自签名证书，此处和 主题 一样。

Signature Algorithm	此处会显示用于对证书进行签名的算法。ZyWALL 使用rsa-pkcs1-sha1 (RSA 公私密钥加密算法和 SHA-1 哈斯算法)算法。一些 CA 可能使用 rsa-pkcs1-md5 (RSA 公私密钥加密算法和 MD5 哈斯算法)算法。
Valid From	此处显示证书开始应用的日期。如果该证书还没有应用，那么会出现一条红色的“Not Yet Valid!”的信息。
Key Algorithm	此处会显示用于生成证书密钥对 (ZyWALL 使用 RSA 加密方法)的算法类型和密钥长度 (例如 1024bits)
Subject Alternative Name	此处显示证书拥有者的 IP 地址(IP)域名(DNS)或 e-mail 地址(EMAIL)
Key Usage	此处显示证书的密钥可被使用的功能。例如，“DigitalSignature”说明该密钥用于签名证书，“KeyEncipherment”说明该密钥用于加密文本。
Basic Constraint	此处显示证书的基本信息。例如，“Subject Type=CA”说明这是一个CA 的证书，“Path Length Constraint=1”说明在证书的路径上只存在一个 CA。
MD5 Fingerprint	这是 ZyWALL 使用 MD5 算法进行计算的证书信息摘要。
SHA1 Fingerprint	这是 ZyWALL 使用 SHA1 算法进行计算的证书信息摘要。
Certificate in PEM (Base-64) Encoded Format	这些只读信息是以保密加强邮件 (PEM) 格式显示的证书或证书申请。PEM 使用 Base-64 编码方式将二进制的证书转化为一个可输出形式。 您可以将一个证书申请复制，粘贴到一个 CA 的web 页上，或通过e-mail 发送到 CA,或粘贴到一个文本编辑器上，然后保存到一台管理计算机上，以备以后手工注册。 您可以将一个证书复制，粘贴到一封 e-mail 里面，然后发送给朋友，同事或者复制，粘贴到一个文本编辑器上，然后保存到一台管理计算机上，以备以后分发 (例如通过磁盘进行)
导出	点击此按钮，然后在文件下载界面里面点击保存。随后打开一个另存为界面，您可通过浏览找到您想保存的位置，最后点击保存即可。
应用	点击应用保存设置。您在此界面中只能修改名称，除非是在自签名证书方式下，您还可以设置缺省的自签名证书用来对输入的可信任远程主机证书做签名。
取消	点击取消回到我的证书界面。

12.8 可信任的 CA

依次点击 **安全，证书，可信的CA** 可以打开**可信的CA**界面。 在该界面中，您可以见到您在 **ZyWALL** 中设置的可信任 **CA** 所提供证书的一个汇总列表。 **ZyWALL** 将会接受任何列表中出现的可信任 **CA** 签名的有效证书；这样您就不必再输入这些 **CA** 签名的证书了。请参考下图。

图 108 可信的CA



以下为界面相关的描述。

表 68 可信的CA

标识	描述
使用中的PKI存储空间	本栏显示的是 ZyWALL 中当前的 PKI 存储空间的使用率。当存储百分比在 80% 以下的时候，状态条是绿色的，当超过了 80% ，状态条就变成红色的了，您需要将已经过期的，或没用的证书删除掉，然后再添加新的证书。
#	此处显示的是证书的索引号。
名称	此处显示的是用于标识该证书的名称。
主题	此处显示证书拥有者的标识信息,例如普通名称 CN ,组织单位 OU ,组织机构 (O) 和国家 (C) 。建议您为每一个证书使用不同的主题信息。
发行者	此处显示发放证书的 CA 标识信息，例如普通名称，组织单位，组织机构和国家。对于自签名证书，此处和 主题 一样。

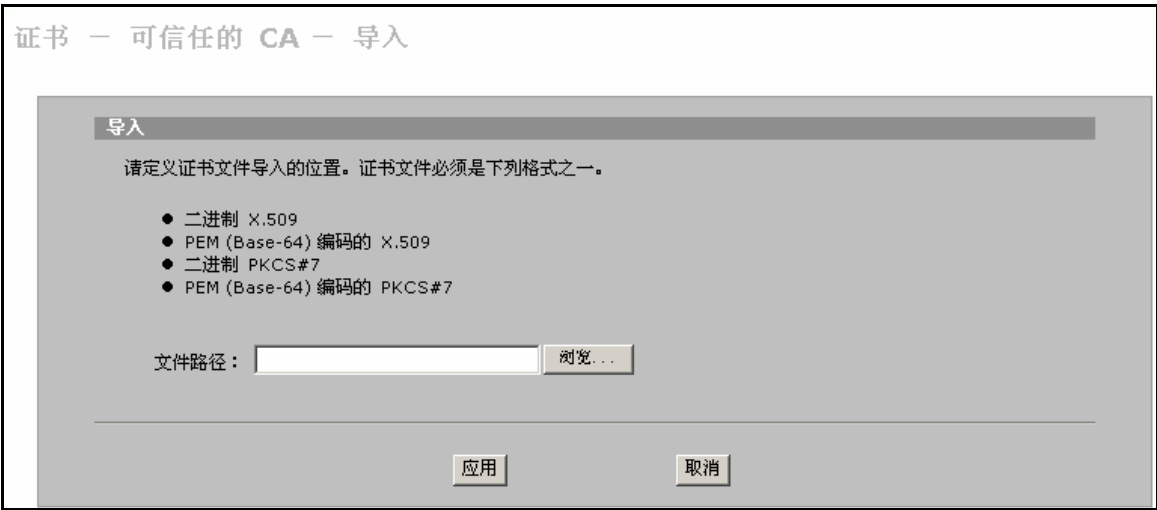
Valid From	此处显示证书开始应用的日期。如果证书还没有应用，此处会显示一个红色的信息“Not Yet Valid！”。
Valid To	此处显示证书失效的日期。如果证书将要到期或已经到期，此处会显示一个红色的信息“Expiring！”或“Expired”。
CRL发行者	如果 CA 想要发送证书已经发送出去的证书撤销列表，并且您在证书详细信息界面里面点选了 Issues certificate revocation lists（CRL） 选项，让ZyWALL 在信任由 CA 发送的任何证书之前检查 CRL，此处会显示“Yes”。否则显示“No”。
修改	点击细节图标可以打开一个界面，显示证书的纵深列表信息。 点击删除图标可以删除证书。会出现一个会话窗口提示您确认删除动作。随后后面的证书会上移过来。
导入	点击 导入 可以打开一个界面，您在此处可以将您可信任 CA 提供的证书从计算机上保存到 ZyWALL 里面。
更新	点击此按钮可以显示证书当前的有效状态。

12.9 导入一个可信的 CA 证书

依次点击 **安全，证书，可信的CA**，可以打开**可信的CA**界面，然后点击**导入**，可以打开**可信的CA 导入**界面。您可按照以下说明来将一个可信任 CA 的证书保存到 ZyWALL 里面。

注意：请在您输入证书之前删除证书文件名里面的任何空格。

图 109 可信任 CA 的导入



以下为界面相关的描述。

表 69 可信任CA的导入

标识	描述
文件路径	您在此处输入您要上载的文件所在的位置，或点击 浏览 找到它。
浏览	点击 浏览 来找到您要上载的证书文件。
应用	点击 应用 ，可以在 ZyWALL 上保存证书。
取消	点击 取消 ，退回到 可信的CA 界面。

12.10 可信任 CA 证书的详细内容

依次点击 **安全, 证书, 可信的CA**可以打开 **可信的CAs**界面。再点击细节图标，就可打开 **可信的CA 细节**界面。使用该界面，您可深入了解 CA 证书的详细信息，修改证书的名称，设置是否让 ZyWALL 在相信由 CA 发送的证书之前检查 CA 的撤销证书列表。

图 110 可信任 CA 的详细内容

证书 — 受信任的 CA — 细节

名称VeriSign.cer

属性

☐ 检查由此CA根据CRL所发来的证书

证书路径

Searching...

更新

证书信息

TypeSelf-signed X.509 Certificate

VersionV1

Serial Number3558802160848854062232407011527417280

SubjectOU=Secure Server Certification Authority, O=RSA Data Security\, Inc., C=US

IssuerOU=Secure Server Certification Authority, O=RSA Data Security\, Inc., C=US

Signature Algorithmrsa-pkcs1-md2

Valid From1994 Nov 9th, 00:00:00 GMT

Valid To2010 Jan 7th, 23:59:59 GMT

Key AlgorithmrsaEncryption (1000 bits)

MD5 Fingerprint74:7b:82:03:43:f0:00:9e:6b:b3:ec:47:bf:85:a5:93

SHA1 Fingerprint44:63:c5:31:d7:cc:c1:00:67:94:61:2b:b6:56:d3:bf:82:57:84:6f

PEM (Base-64) 编码格式的证书

-----BEGIN CERTIFICATE-----

MIICNDCCAaECEAKtZn5ORf5eV288mBle3cAwDQYJKoZIhvcNAQECBQAwXzELMAkG

A1UEBhMCVVMxIDAeBgNVBAAoTF1JTQSBFYXRhIFN1Y3VyaXR5L0JmMuMS4wLAYD

VQQLLEyVTZWV1cmUgU2VydmluYyIEN1cnRpb24gQXV0aG9yaXR5MB4XDk0

MTEwOTAwMDAwMFoXDTEwMDEwNzIzNTk1OVowXzELMAkGA1UEBhMCVVMxIDAeBgNV

BAAoTF1JTQSBFYXRhIFN1Y3VyaXR5L0JmMuMS4wLAYDVQQLLEyVTZWV1cmUgU2Vy

dmVydmluYyIEN1cnRpb24gQXV0aG9yaXR5MIGbMA0GCSCqGSIb3DQEBAQUAA4GJ

ADCBhQJ+AJLOesGugz5aqomDV6w1AXYMr60LDf06zV4ZFQD5YRAUcm/jwjiioII

0haGN1XpsSECrXZogZoFokvJSyVmIlZsiAeP94FZbYQHZAATcXY+m3dM41CJVphI

uR2nKR0TLkoRWZweFdVJVCxzOmmCsZc5nG1wZ0j1S3WYB57AgMBAAEwDQYJKoZI

导出

应用

取消

以下为界面相关的描述。

表 70 可信任 CA 的详细内容

标识	描述
名称	此处为证书的标识名称。如果您想修改名称，可以输入最多31个字符来标识此证书。您可以使用任何字符（不包括空格）
检查由此CA根据CRL所发来的证书	点选此框可以让 ZyWALL 检查输入的证书是否是从 CRL 中的CA发送出来的。不选此框，ZyWALL 不会检查证书是否是从 CRL 中的 CA发送出来的。

186

证书路径	点击 更新 按钮,可以在只读文本框中显示终端实体的证书和一个CA证书的列表,我们可以看到有效的终端实体证书的 CA 层次。如果该CA是您已经输入的可信任 CA 中的一个,那么它可能是列表中唯一的 CA(连同终端实体自身的证书)如果在路径上的任何证书已经过期或无效了,那么ZyWALL将不会信任该终端实体证书,在此处会显示“不可信的”。
更新	点击 更新 可以显示证书路径。
证书路径	此处为只读信息,都是关于证书的详细信息。
类型	此处显示证书的一般信息。“CA-signed”说明一个 CA 对证书做签名。“Self-signed”说明证书的拥有者签名该证书(不是一个CA)“X.509”说明该证书是根据 ITU-T X.509 建议使用的公钥体制证书定义的格式来创建和签名的。
Version	此处显示 X.509 的版本号。
Serial Number	此处显示由 CA 生成的证书的标识号码。
Subject	此处显示证书拥有者的标识信息,例如普通名称(CN) 组织单位(OU) 组织机构(O) 和国家(C)
Issuer	此处显示发放证书的 CA 标识信息,例如普通名称,组织单位, 组织机构和国家。 对于自签名证书,此处和 主题 一样。
Signature Algorithm	此处会显示用于对证书进行签名的算法。ZyWALL使用 rsa-pkcs1-sha1(RSA 公私密钥加密算法和 SHA-1 哈斯算法) 算法。一些 CA 可能使用 rsa-pkcs1-md5(RSA 公私密钥加密算法和 MD5 哈斯算法) 算法。
Valid From	此处显示证书开始应用的日期。如果该证书还没有应用,那么会出现一条红色的“Not Yet Valid!”的信息。
Valid To	此处会显示证书失效的日期。如果证书将要失效或已经失效,此处会出现一条红色的“Expiring!”或“Expired!”信息。
Key Algorithm	此处会显示用于生成证书密钥对(ZyWALL 使用 RSA 加密方法)的算法类和密钥长度(例如 1024bits)。
Subject Alternative Name	此处显示证书拥有者的 IP 地址(IP) 域名(DNS) 或 e-mail地址(EMAIL)

Key Usage	此处显示证书的密钥可被使用的功能。例如，“DigitalSignature”，说明该密钥用于签名证书，“KeyEncipherment”说明该密钥用于加密文本。
Basic Constraint	此处显示证书的基本信息。例如，“Subject Type=CA”说明这是一个 CA 的证书，“Path Length Constraint=1”说明在证书的路径上只存在一个 CA。
CRL Distribution Points	这里显示有多少带有证书撤销列表的目录服务器,该证书由权威机构证明是可用的。这里也显示服务器的域名或 IP 地址。
MD5 Fingerprint	这是 ZyWALL 使用 MD5 算法进行计算的证书信息摘要。您可以使用此值来向 CA（例如通过电话）确认这个证书是他们的证书。
SHA1 Fingerprint	这是 ZyWALL 使用 SHA1 算法进行计算的证书信息摘要。您可以使用此值来向 CA（例如通过电话）确认这个证书是他们的证书。
Certificate in PEM (Base-64) Encoded Format	这些只读信息是以保密加强邮件(PEM)格式显示的证书或证书申请。PEM 使用 Base-64 编码方式将二进制的证书转化为一个可输出形式。 您可以将一个证书复制，粘贴到一封e-mail里面，然后发送给朋友，同事或者复制，粘贴到一个文本编辑器上，然后保存到一台管理计算机上，以备以后分发（例如通过磁盘进行）
导出	点击此按钮，然后在 文件下载 界面里面点击 保存 。随后打开一个 另存为 界面，您可通过浏览找到您想保存的位置，最后点击 保存 即可。
应用	点击 应用 保存设置。您在此界面中只能修改名称和/或设置是否您想让 ZyWALL 在相信一个 CA 发送的证书之前检查 CA 发送的 CRL。
取消	点击 取消 回到 可信的CA 界面。

12.11 可信任的远程主机

依次点击 **安全，证书，可信的远程主机** 可以打开 **可信的远程主机** 界面。该界面显示了您信任但是还没有被**可信的CA**界面里的任意一个证书签名的远端证书的列表。

因为 ZyWALL 会自动将任何一个已经被可信任的 CA 签名的有效证书作为可信任的证书，所以您不必添加任何已经被在**可信的CA**界面里的 CA 签名的证书。

图 111 可信任远程主机



以下为界面相关的描述。

表 71 可信任远程主机

标识	描述
使用中的PKI存储空间	本栏显示的是 ZyWALL 中当前的 PKI 存储空间的使用率。当存储使用中的PKI存储百分比在 80%以下的时候，状态条是绿色的，当超过了80%，状态条就变成红色的了,您需要将已经过期的,或没用的证书删除掉，然后再添加新的证书。
发证者(我的默认自行签发证书)	此处显示 ZyWALL 上缺省的自签名证书的标识信息ZyWALL 用于对可信任的远程主机证书做签名。
#	次出显示的是证书的索引号。
名称	此处显示的是用于标识该证书的名称。
主题	此处显示证书拥有者的标识信息，例如普通名称(CN)组织单位(OU)组织机构(O)和国家(C)建议您为每一个证书使用不 同的主题信息。
有效期起自	此处显示证书开始应用的日期。如果证书还不能使用，此处会显示一个红色的信息“Not Yet Valid! ”。
到期	此处显示证书失效的日期。如果证书将要到期或已经到期，此处会显示一个红色的信息“Expiring! ”或“Expired”。
修改	点击细节图标可以打开一个界面，显示证书的纵深列表信息。 点击删除图标可以删除证书。会出现一个会话窗口提示您确认删除动作。随后后面的证书会上移过来。

导入	点击 导入 可以打开一个界面，您在此处可以将您可信任 CA 提供的证书从计算机上保存到 ZyWALL 里面。
更新	点击此按钮可以显示证书当前的有效状态。

12.12 验证一个可信任远程主机的证书

由 CA 发送的证书有用于让您验证的 CA 的签名。自签名证书只有主机自己的签名。这就意味着，当您决定输入（从而信任）一个远程主机的自签名证书的时候需要非常小心。

12.12.1 相信远程主机证书的指纹

证书的指纹也就是使用 MD5 或 SHA1 算法的消息摘要。以下步骤描述了如何使用一个证书的指纹来验证您所拥有的远程主机当前的证书。

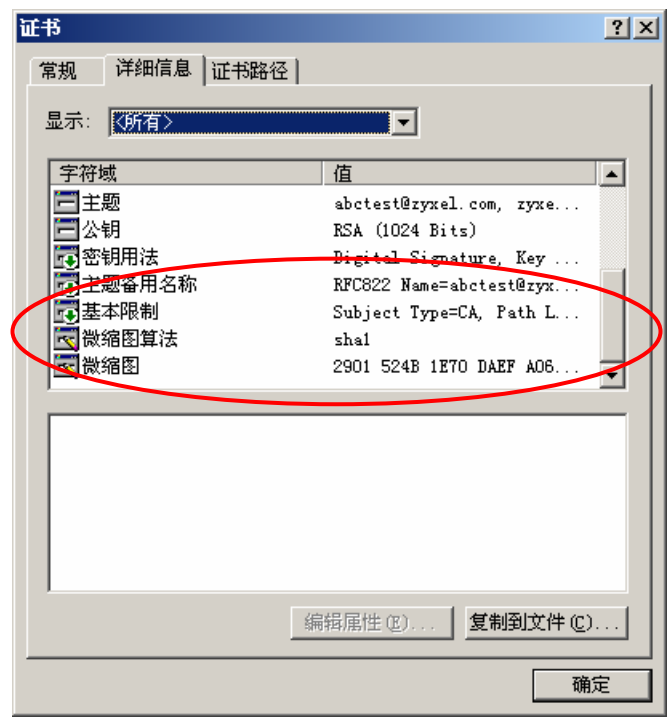
- 1. 通过浏览找到远程主机的证书在您计算机上的位置。
- 2. 确保该证书有一个“.cer”或“.crt”的扩展名。

图112 远程主机证书



- 3. 双击证书的图标，可以打开**证书**窗口。点击**细节**标签，然后下拉到**微缩图算法**和 **微缩图**的位置上。

表 113 证书详细内容



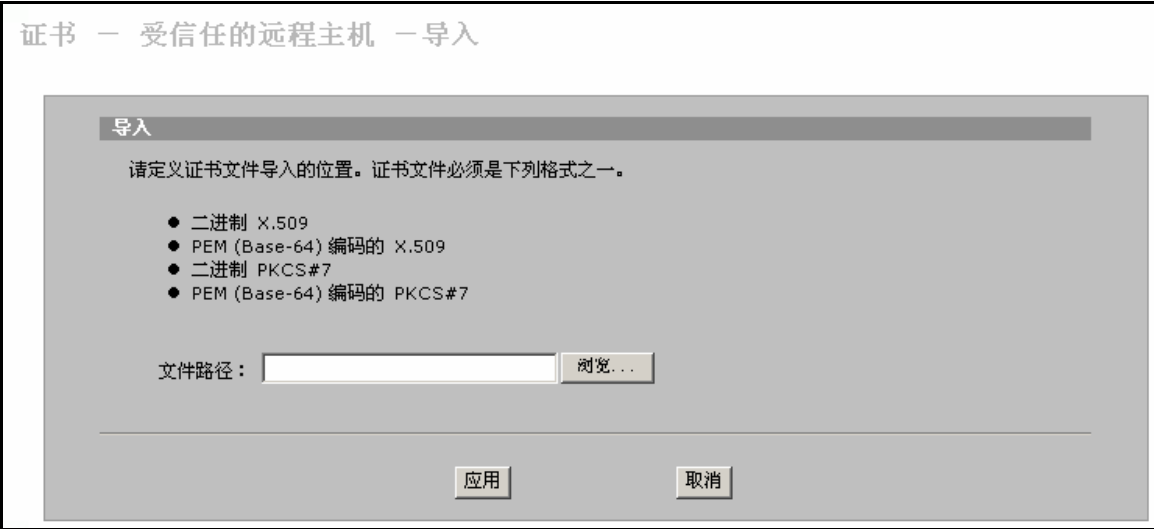
确认（例如通过电话）远程主机在微缩图算法和微缩图区域中具有相同的信息。

12.13 导入一个可信任远程主机的证书

依次点击安全，证书，可信的远程主机可以打开可信的远程主机界面，然后点击导入打开可信的远程主机 导入界面。

注意：可信任的远程主机证书必须是一个自签名的证书；您在输入该证书之前，需要删除文件名中的任何空格。

图 72 可信任远程主机的导入



以下为界面相关的描述。

表 72 可信任远程主机的输入

标识	描述
文件路径	您在此处输入您要导入的文件所处的具体路径，或点击 浏览 找到它。
浏览	点击 浏览 来找到您要导入的证书文件。
应用	点击 应用 ，您可以在 ZyWALL 上保存证书。
取消	点击 取消 ，退回到 可信的远程主机 界面。

12.14 可信任远程主机证书的详细内容

依次点击**安全，证书，可信的远程主机**可以打开**可信的远程主机**界面，然后点击 **detail** 图标打开**可信的远程主机 细节**界面。您可 以使用该界面来查看可信任远程主机证书的详细信息和/或修改证书的名称。

图 115 可信任远程主机的详细信息

证书 — 受信任远程主机 — 细节

名称

test

证书路径

Searching...

更新

证书信息

Type	CA-signed X.509 Certificate
Version	V3
Serial Number	946686627
Subject	CN=abctest@zyxel.com, OU=zyxel, O=zyxel, C=China
Issuer	CN=ZyWALL 2 Plus Factory Default Certificate
Signature Algorithm	rsa-pkcs1-sha1
Valid From	1999 Dec 31st, 00:30:27 GMT
Valid To	2002 Dec 31st, 00:30:27 GMT
Key Algorithm	rsaEncryption (1024 bits)
Subject Alternative Name	EMAIL=abctest@zyxel.com
Key Usage	DigitalSignature, KeyEncipherment
Basic Constraint	Path Length Constraint=10
MD5 Fingerprint	00:e1:00:d4:34:21:39:a1:41:27:3d:31:75:b5:82:91
SHA1 Fingerprint	31:fb:8f:05:64:d3:85:ea:cb:4c:d5:2f:4c:c2:21:f5:10:cc:93:d1

PEM (Base-64) 编码格式的证书

```

-----BEGIN CERTIFICATE-----
MIIB9jCCAAcGawIBAgIEOgIKozANBgkqhkiG9w0BAQUFADAOMTIwMAYDVQQDEYl
eVdBTEwgMIBQbHVzIEZhY3RvcnkRGVmYXVsdCBDZXJ0aWZpY2F0ZTAeFw050TEy
MzEwMDMwMjdaFw0wMjEzYmZlbnMjdaMEwxDjAMBGNVBAITBUNoaW5hMq4wDAYD
VQKKEwV6eXhlbDEOMAwGA1UECxFEnl4ZWxzGjAYBgNVBAMMEWFyY3Rlc3RAen14
ZWVwY29tMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCX5sBkwS3iE0D1g7p
8seFDKQjInxcH5IyBn3U1/H0x+pWx+jHC/9bftFFRES0m4YJDbdbN5XK49Ff864b
aDwE30KbGiorCkjcFKPGxba+zWODpR5ZrbzKYdqCSz8rbfjEAIqi/AEUpCoprFt
07kZoiB31yyr5YPWyJEUFWIVqWIDAQABoz4wPDALBgNVHQ8EBAMCAqQwHAYDVR0R
BBUwE4ERYWJjGvZdEB6eXhlbC5jb20wDwYDVR0TBAgwBgEBAAIIBCjANBgkqhkiG

```

导出

应用

取消

以下为界面相关的描述。

表 73 可信任远程主机的详细信息

标识	描述
名称	此处为证书的标识名称。如果您想修改名称，可以输入最多 31 个字符来标识此证书。您可以使用任何字符（不包括空格）
证书路径	点击 更新 按钮，可以在只读文本框中显示终端实体的证书 和一个 CA 证书的列表，我们可以看到有效的终端实体证书的 CA 层次。对于一个可信任主机来说，列表包括终端实体的证书和 ZyWALL 用于对远程主机证书签名的缺省的自签名证书。

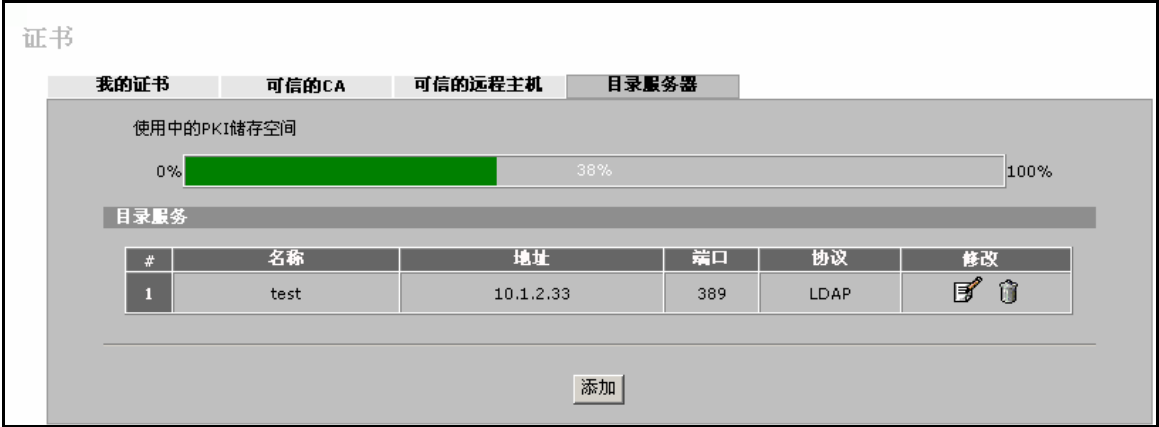
更新	点击 更新 可以显示证书路径。
证书信息	此处为只读信息，都是关于证书的详细信息。
类型	此处显示证书的一般信息。“CA-signed”说明一个 CA 对证书做签名。“Self-signed”说明证书的拥有者签名该证书（不是一个 CA）。X.509”说明该证书是根据 ITU-T X.509 建议使用的公钥体制证书定义的格式来创建和签名的。
Version	此处显示 X.509 的版本号。
Serial Number	此处显示由生成证书的设备提供的证书标识号码。
Subject	此处显示证书拥有者的标识信息，例如普通名称（CN）组织单位（OU）组织机构（O）和国家（C）
Issuer	此处显示发放证书的 CA 标识信息，例如普通名称，组织单位，组织机构和国家。对于自签名证书，此处和 主题 一样。
Signature Algorithm	此处会显示用于对证书进行签名的算法。ZyWALL 使用 rsa-pkcs1-sha1（RSA 公私密钥加密算法和 SHA-1 哈希算法）算法。一些 CA 可能使用 rsa-pkcs1-md5（RSA 公私密钥加密算法和 MD5 哈希算法）算法。
Valid From	此处显示证书开始应用的日期。如果该证书还没有应用，那么会出现一条红色的“Not Yet Valid！”的信息。
Valid To	此处会显示证书失效的日期。如果证书将要失效或已经失效，此处会出现一条红色的“Expiring!”或“Expired！”信息。
Key Algorithm	此处会显示用于生成证书密钥对 ZyWALL 使用 RSA 加密方法的算法类型和密钥长度（例如 1024bits）
Subject Alternative Name	此处显示证书拥有者的 IP 地址（IP）域名（DNS）或 e-mail 地址（EMAIL）
Key Usage	此处显示证书的密钥可被使用的功能。例如，“DigitalSignature”说明该密钥用于签名证书，“Key Encipherment”说明该密钥用加密文本。
Basic Constraint	此处显示证书的基本信息。例如，“Subject Type=CA”说明这是一个 CA 的证书，“Path Length Constraint=1”说明在证书的路径上只存在一个 CA。

MD5 Fingerprint	这是 ZyWALL 使用 MD5 算法进行计算的证书信息摘要。您不能使用此值来检查确保这是远程主机的实际证书，因为ZyWALL 已经对证书做了签名；这样就导致了此值和远程主机的实际证书不一样。请参考确认一个可信任远程主机的证书一节，了解如何查验一个远程主机的证书。
SHA1 Fingerprint	这是 ZyWALL 使用 SHA1 算法进行计算的证书信息摘要。您不能使用此值来检查确保这是远程主机的实际证书，因为ZyWALL 已经对证书做了签名；这样就导致了此值和远程主机的实际证书不一样。请参考确认一个可信任远程主机的证书一节，了解如何查验一个远程主机的证书。
Certificate in PEM (Base-64) Encoded Format	这些只读信息是以保密加强邮件(PEM)格式显示的证书或证书申请。PEM 使用 Base-64 编码方式将二进制的证书转化为一个可输出形式。 您可以将一个证书复制，粘贴到一封e-mail 里面，然后发送给朋友，同事或者复制，粘贴到一个文本编辑器上，然后保存到一台管理计算机上，以备以后分发（例如通过磁盘进行）
导出	点击此按钮，然后在 文件下载 界面里面点击 保存 。随后打开一个 另存为 界面，您可通过浏览找到您想保存的位置，最后点击 保存 即可。
应用	点击 应用 保存设置。您在此界面中只能修改名称。
取消	点击 取消 回到 可信的远程主机 界面。

12.15 目录服务器

依次点击 **安全，证书，目录服务器** 可以打开**目录服务器**界面。界面中显示了一个已经保存到 ZyWALL 中的目录服务器（包括有效的和已 废除的证书列表）的汇总表。如果您想让 ZyWALL 查验输入的证书是否在 CA 的已废除证书的列表中出现，ZyWALL 会首先查验输入证书的 **CRL Distribution Points** 区域中的服务器列表。如果证书没有列出服务器或者已列出的服务器无效，ZyWALL 会查验此处的服务器列表。

图 173 目录服务器



以下为界面相关的描述.

表 74 目录服务器

标识	描 述
使用中的PKI存储空间	本栏显示的是 ZyWALL 中当前的 PKI 存储空间的使用率.当存储百分比在 80%以下的时候, 状态条是绿色的, 当超过了80%, 状态条就变成红色的了, 您需要将已经过期的, 或没用的证书删除掉, 然后再添加新的证书。
#	这是目录服务器的索引号。
名称	此处显示用于标识这个目录服务器的名称。
地址	此处显示这个目录服务器的 IP 地址或域名。
端口	此处显示目录服务器使用的端口号。
协议	此处显示目录服务器使用的协议。
修改	点击细节图标可以打开一个界面, 您可以修改该目录服务器的信息。 点击删除图标可以删除该目录服务器.随后会出现一个会话窗口提示您确认删除动作。随后后面的证书会上移过来。
添加	点击 添加 可以打开一个界面, 您可以配置一个目录服务器的相关信息, 以便能够让 ZyWALL 接入进来。

12.16 添加或编辑目录服务器

依次点击 **安全, 证书, 目录服务器**可以打开**目录服务器** 界面.然后点击**添加**(或 细节图标)可以打开以下界面.您在该界面中可以配置目录服务器的相关信息, 以便让 ZyWALL 可以访问进来.

图 117 目录服务器的添加

证书 — 目录服务器 — 添加

目录服务器设置

名称

存取协议

LDAP ▾

服务器地址

(主机名称或IP地址)

服务器端口

389

登录设置

登录

密码

应用

取消

以下为界面相关的描述。

表 75 目录服务器的添加

标识	描述
Directory 服务设置	
名称	输入最多 31 个 ASCII 字符（不包括空格）来标识这个目录服务器。
存取协议	使用下拉菜单来选择目录服务器使用的访问协议。 LDAP （轻量级目录访问协议）是一种基于 TCP 的协议，规定了客户端如何访问目录证书和已废除证书的列表。
服务器地址	输入目录服务器的 IP 地址或域名。
服务器端口	此处显示您在 存取协议 处选择的协议所使用的缺省服务端口号。 如果需要，您可以修改服务端口号，但是目录服务器也必须要使用相同的服务端口号。 389 是 LDAP 缺省的服务端口号。
登陆设置	
登陆	ZyWALL 为了接入到目录服务器，需要认证自身。输入一个从实体维护目录服务器（一般是一个 CA)的登录名称(最多 31 个 ASCII 字符)
密码	输入一个从实体维护目录服务器（一般是一个 CA)的密码（最多 31个 ASCII 字符)
应用	点击 应用 可以保存设置。
取消	点击 取消 可以退回到 目录服务器 界面。

目前，LDAP 是目录服务器访问协议唯一的选项。

第 13 章 认证服务器

本章将会向您介绍如何配置 ZyWALL 的证明服务器

13.1 认证服务器概述

ZyWALL 可以设置 VPN 扩展认证服务器，它既可以使用 ZyWALL 内置的本地认证服务器，也可以外挂一个不限制用户数量的 RADIUS 服务器。ZyWALL为VPN 扩展认证服务。

13.2 本地用户数据库

通过在 ZyWALL 上储存本地用户的信息，ZyWALL 就可以不使用网络 RADIUS 服务器对用户做认证。然而，通过这种方式来认证的用户数量是有限的。

13.3 RADIUS（远程认证拨号用户服务）

ZyWALL能使用RADIUS服务器进行无数量限制的用户认证。RADIUS基于一种客户/服务器的模式，支持认证、授权和计费。接入点是客户，服务器则是RADIUS服务器，服务器处理以下任务：

- 认证（Authentication）
确定用户身份
- 授权（Authorization）
在通过认证的用户接入到网络后，确定可使用的网络服务。
- 计费（Accounting）
对客户网络行为保持跟踪

RADIUS是一个简单的包交换，在这里，ZyWALL作为客户与RADIUS服务器之间的消息中继。

13.3.1 RADIUS 消息类型

以下是AP和RADIUS服务器之间交换的几种用于用户认证的RADIUS消息的类型：

- **Access-Request**

由AP发送的认证请求消息。

- **Access-Reject**

由RADIUS服务器发送的拒绝接入消息。

- **Access-Accept**

由RADIUS服务器发送的允许接入的消息。

- **Access-Challenge**

由RADIUS服务器发送的要求接入用户提供更多信息的请求。AP会发送一个适当的用户响应，然后再发送另一个Access-Request消息。

以下是AP和RADIUS服务器之间交换的几种用于用户计费的RADIUS消息的类型：

- **Accounting -Request**

由AP发送的计费请求消息。

- **Accounting -Response**

由RADIUS服务器发送的开始或者停止计费的消息。

为了确保网络的安全，AP和RADIUS服务器采用一个共享的安全密钥来作为双方使用的密码。该密钥将不会在网络上传输。为了共享该密钥，密码信息的交换也进行了加密，这样可以有效防止非认证用户的接入。

13.4 本地用户数据库

先点击**安全**，然后点击**认证服务器** 打开**本地用户数据库**界面。利用该界面您可以修改ZyWALL 的本地用户列表。

图118 本地用户数据库

认证服务器

本地用户数据库

RADIUS

用户数据库

#	启用	用户名	密码
1	☐		
2	☐		
3	☐		
4	☐		
5	☐		
6	☐		
7	☐		
8	☐		
9	☐		
10	☐		
11	☐		
12	☐		
13	☐		
14	☐		
15	☐		
16	☐		
17	☐		
18	☐		
19	☐		
20	☐		
21	☐		
22	☐		
23	☐		
24	☐		
25	☐		
26	☐		
27	☐		
28	☐		
29	☐		
30	☐		
31	☐		
32	☐		

应用

重置

以下为界面相关的描述。

表76 本地用户数据库e

标识	描述
启用	点选此框可以启用该条用户账号。
用户名	输入用户名。
密码	输入密码，最多31个字符。
应用	点击 应用 可以保存设置。

重置	点击 重置 可以重新配置该界面。

13.5 RADIUS

您可以采用外置的RADIUS服务器对用户做认证。

先点击**安全**，**认证服务器**，然后点击**RADIUS**标签打开**RADIUS**界面。 利用该界面您可以设置 ZyWALL 的 RADIUS 服务器参数。

图 119 RADIUS

认证服务器

本地用户数据库

RADIUS

认证服务器

☐ 启用

服务器IP

端口号

密钥

0.0.0.0

1812

计费服务器

☐ 启用

服务器IP

端口号

密钥

0.0.0.0

1813

应用

重置

以下为界面相关的描述。

表77 RADIUS

标识	描述
认证服务器	
启用	点选此框可以采用外置的认证服务器对用户做认证。 不选此框可以使用ZyWALL内置的本地用户数据库对用户做认证。
服务器IP	输入外置认证服务器的IP地址。
端口号	RADIUS服务器默认的认证端口号为 1812 。您不需要改变此值。
密钥	输入一个ZyWALL和外置认证服务器共享的密钥（最多 31 个字符）。 这个密钥不会在网上发送。该密钥在外部认证服务器和ZyWALL上必须是相同的。
计费服务器	

启用	点选此框可以采用外置的计费服务器对用户做计费。
服务器IP	输入外置计费服务器的IP地址。
端口号	RADIUS 服务器默认的计费端口号为 1813 。您不需要改变此值。
密钥	输入一个 ZyWALL 和外置计费服务器共享的密钥（最多 31 个字符）。这个密钥不会在网上发送。该密钥在外部认证服务器和 ZyWALL 上必须是相同的。
应用	点击 应用 可以保存设置。
重置	点击 重置 可以重新设置该界面。

第 14 章 网络地址转换（NAT）

本章将会向您介绍如何在 ZyWALL 中配置 NAT。

14.1 NAT 简介

NAT（网络地址转换，RFC 1631）就是对封包中主机的 IP 地址进行转换。例如，在某个网络中被使用的数据包的源地址，被送达另外一个网络时会被转换为另一个不同的 IP 地址。

14.1.1 NAT 的一些定义

“内部” / “外部”用于表示一台主机相对于 ZyWALL 的位置。例如，用户的计算机是内部主机，而在 Internet 上的 web 服务器属于外部的宿主。

“全球” / “本地”用于表示封包在穿越路由器时主机的 IP 地址，例如，本地地址是指当封包位于本地网络内部时主机的 IP 地址，而全球地址则是封包在广域网传输时主机的 IP 地址。

注意“内部” / “外部”是指主机的位置而“全球” / “本地”是指封包中主机使用的 IP 地址。因此，ILA（Inside Local Address）表示当封包仍在本地网时，内部主机的 IP 地址；IGA（Inside Global Address）表示封包在广域网时，相同主机的 IP 地址。请参考下面的表格。

表78 NAT 的一些定义

术语	描述
Inside	指位于局域网的主机。
Outside	指位于广域网的主机。
本地	指封包在局域网内传输时的 IP 地址（包括源地址与目的地址）
全局	指封包在广域网上传输时的 IP 地址（包括源地址与目的地址）

注意：NAT 不会改变外部主机的 IP 地址（包括本地与外地的 IP 地址）

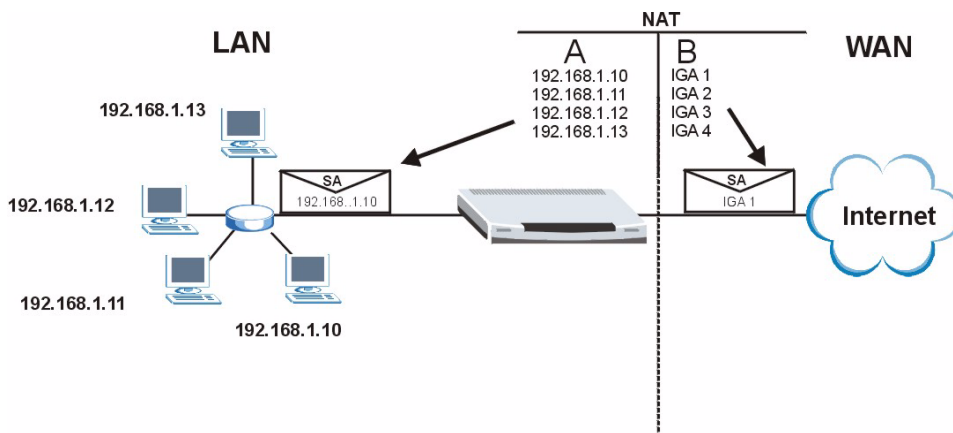
14.1.2 NAT 的作用

内部主机的全IP地址可以是静态的也可以由ISP动态分配。另外，您能在您的本地网络选定服务器(例如网络服务器和远端服务器)并使他们容易接近对外部世界。另外，您也可以在本机网络中指定一些服务器(例如 web 服务器和 telnet 服务器)可以被外网访问。如果您不指定任何服务器，NAT 会起到防火墙的功能。如果没有指定服务器，您的 ZyWALL 会将源自外网的连接请求全部过滤掉这样可以防止入侵者探查您的网络对于更多关于 IP 地址转换的信息，您可以参考 RFC 1631，IP 网址转换(NAT)。

14.1.3 NAT 的工作机制

每一个数据包都有两个地址，一个源地址和一个目的地址。对于发出去的数据包，在局域网 ILA（内部本地地址）就是源地址，而在广域网上 IGA（内部全球地址）则是源地址。对于接收到的数据包，在局域网 ILA 是目标地址，而在广域网上 IGA 则是目标地址。当本地主机要求与其它网络上的主机进行通信时，NAT 将本地主机的私有（本地）IP 地址映射为全球唯一的 IP 地址。它将每个数据包中的原始 IP 源地址（包括用于多对一和多对多加载 NAT 映射的 TCP 或 UDP 源端口替换然后再传送到 Internet 上此时 ZyWALL 持续跟踪原始地址和端口号，以使返回的数据包能够恢复到原始值。请参考下面的图示。图中 NAT 表 A 栏显示 ILAs，B 栏显示 IGAs

图 120 NAT 如何工作

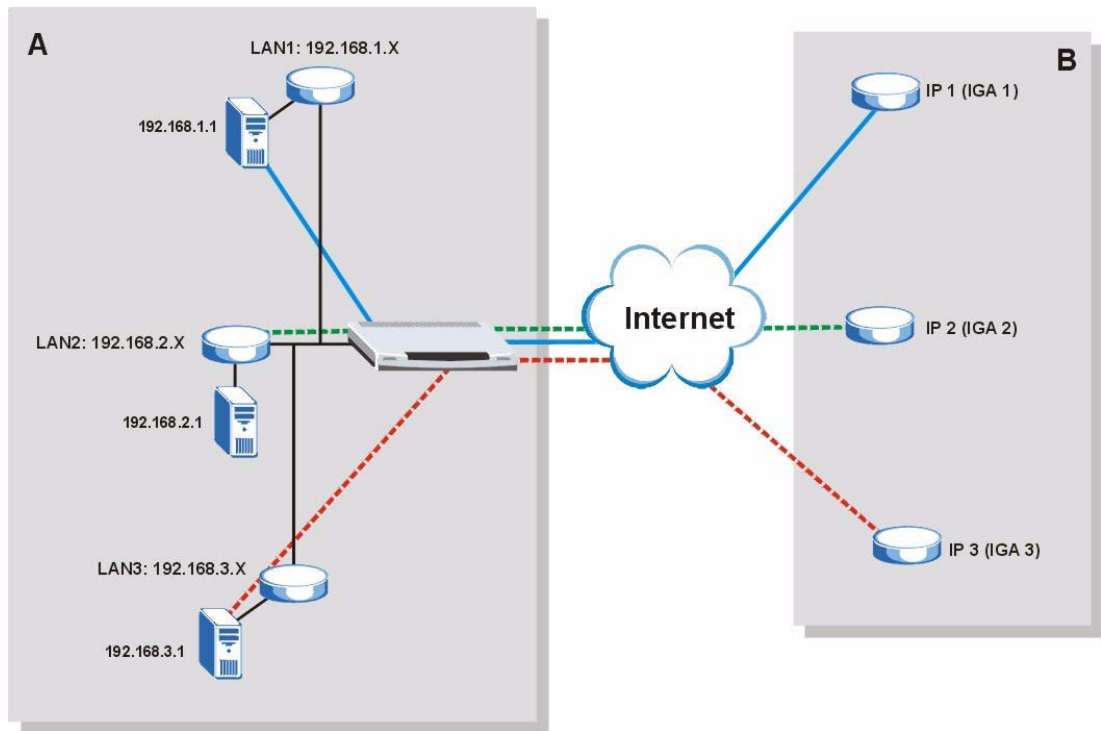


14.1.4 NAT 应用

下图描述了一个 NAT 的应用，隐藏在 ZyWALL 后面的三个内部局域网（用 IP 别

名区分的逻辑局域网) 能够和广域网上另外三个不同的网络进行通信。更多的范例请参考这一章的结束部分。在本例中, 公司A的网络标识为A, 公司B的网络标识为B。

图 121 支持 IP 别名的 NAT 应用



下表对本例中的路由作了描述。

图 79 支持 IP 别名的 NAT 应用

WAN地址	LAN 地址 (默认的IPS)
IGA1	192.168.1.1
IGA2	192.168.2.1
IGA3	192.168.3.1

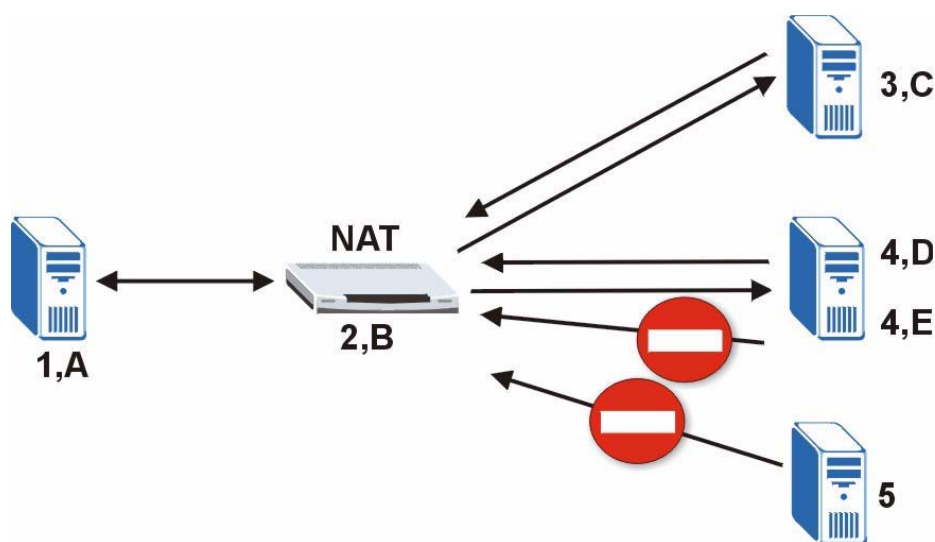
14.1.5 端口受限锥形 NAT

目前 ZyNOS 版本为 4.0 的ZyWALL 采用的是端口受限锥体 NAT 方式。端口受限锥形 NAT 会把所有来自同一个内部私网地址/端口的请求, 都映射到同一个外部公网地址/端口上。如下面的范例所示, ZyWALL 会把所有来自内部私网 IP 地址为 1, 端口为 A 的请求,

都映射到外部公网 IP 地址为 **2**，端口为 **B** 上。这样一个外部公网上的主机（例如 IP 地址为 **3**，端口为 **C**）只能将数据包发送到已经给这个外部主机和端口发送过数据的内部主机上。

如果 IP 地址为 **1** 端口为 **A** 的服务器给 IP 地址为 **3** 端口为 **C** 以及 IP 地址为 **4** 端口为 **D** 的主机发送数据包，ZyWALL 会将服务器的 IP 地址该为 **2**，端口该为 **B**。这样既然 **1, A** 已经给 **3, C** 和 **4, D** 发送过了数据包，那么它们就可以反过来给 **2, B** 发送数据包，接着 ZyWALL 再通过 NAT 将这些数据包发送到 IP 地址为 **1**，端口为 **A** 的服务器上。而 **1, A** 没有给 **4, E** 和 **5** 发送过数据包，所以他们就不能给 **1, A** 发送数据包。

图 122 端口受限锥形 NAT



14.1.6 NAT 的映射类型

NAT 支持五种不同类型的 IP / 端口映射。它们是：

One to One: 在一对一的模式中，ZyWALL 会将一个本地 IP 地址映射到一个全球 IP 地址上。

Many to One: 在多对一的模式中，ZyWALL 将多个本地 IP 地址映射到一个全球 IP 地址上。这等同于 SUA（例如：PAT，端口地址转换）就是 ZyXEL 路由器支持的单用户帐号功能（SUA 仅作为可选项）

Many to many Overload: 在多对多加载的模式中，ZyWALL 将多个本地 IP 地址映射到多个共享的全球地址上。

Many one to one: 在多个一对一的模式中，ZyWALL 将每一个本地 IP 地址映射到单独对应的全球地址上。也就是一个本地地址对应一个全球地址。

服务器：这种模式允许指定隐藏于 NAT 后面的提供不同服务的内部服务器，并为全球提供接入服务。

注意：在 **One to One** 和 **Many One to One** 的 NAT 映射中，端口号不会改变。下表是这些类型的总结。

表 80 NAT 映射类型

类型	IP 映射		SMT 缩写
One-to-One	ILA1	IGA1	1-1
Many-to-One (SUA/PAT)	ILA1	IGA1	M-1
	ILA2	IGA1	
Many-to-Many Overload	ILA1	IGA1	M-M Ov
	ILA2	IGA2	
	ILA3	IGA1	
Many-One-to-One	ILA1	IGA1	M-1-1
	ILA2	IGA2	
	ILA3	IGA3	
服务器	服务器 1 IP	IGA1	服务器
	服务器 2 IP	IGA1	

14.2 使用 NAT

注意：除配置SUA/NAT外，你必须创建一个防火墙规则，允许来至WAN的数据流需经ZyWALL转发。

14.2.1 SUA（单用户账号）和 NAT

SUA 是 Zynos 所执行的 NAT 子集支持两种映射**Many-to-One** 和**Server**ZyWALL 也支持**全部功能**的 NAT功能，可以将多个全球 IP 地址映射到客户机或服务器的多个私有局域网 IP 地址。您可在 **NAT概述**选择 **SUA**或**全部功能**。

选择 **SUA**意味着多重 WAN-to-LAN地址转换。这意味着如果您使用 **SUA** NAT 映射，在带有公网 IP 地址的LAN上的计算机将依旧不得不要受到 NAT 映射。如果这不是您的目的那么请为那些带有公网 IP 地址的LAN上的计算机选择**全部功能**NAT 或不配置 NAT 映射规则。

14.3 NAT 概述

点击**高级**，**NAT**可以打开**NAT概述**界面。

图 123 NAT 概述



以下为界面相关的描述。

表 81 NAT 概述

标识	描述
设置	
NAT设置	该只读区域显示的是 ZyWALL 同时允许通过的最大 NAT 会话数量。
最大并发会话进程数	您可以在该区域设置 ZyWALL 同时允许每台主机通过的最大 NAT 会话数量。
启用NAT	点选此框可以启用 WAN 口的 NAT 功能。
地址映射规则	选择SUA，ZyWALL 可以使用永久的，预先确定的 NAT 地址映射规则。 选择全部功能，ZyWALL 可以使用您所配置的地址映射规则。这也称之为全特征 NAT 方式。 条形显示 ZyWALL 已配置的地址映射规则的数量。头一个数字显示的是已经配置的规则数量,后面的数字显示的是 ZyWALL 可以配置的地址映射规则的最大数量。

端口映射规则	条形显示 ZyWALL 已配置的端口转发规则的数量。头一个数字显示的是已经配置的规则数量,后面的数字显示的是 ZyWALL 可以配置的端口转发规则的最大数量。
端口触发规则	条形显示 ZyWALL 已配置的触发端口规则的数量。头一个数字显示的是已经配置的规则数量,后面的数字显示的是 ZyWALL 可以配置的触发端口规则的最大数量。
应用	点击 应用 可以保存设置。
重置	点击 重置 可以重新设置该界面。

14.4 NAT 地址映射（NAT Address Mapping）

对规则进行分类很重要,因为 ZyWALL 会按照您所规定的顺序来应用规则。当数据包和一个规则相符的时候,ZyWALL 会采取相应的动作,而不用理会其它的规则。如果在您新配置的规则之前有一个空项,您配置的规则会前移到空项规则的序列号位置。例如,如果您已经在当前的配置界面里配置了规则 1 到 6,随后您又配置了规则 9。在设置汇总界面里面,新的规则将会是规则 7,而不是 9。如果此时您再删除规则 4,那么规则 5 到 7 将会各自前移一位,这样老的规则 5,6 和 7 将会变成新的规则 4,5 和 6。

如果您想修改 ZyWALL 的地址映射表,可以先点击 **高级, NAT**,然后点击**地址映射**标签。您可以见到以下界面。

图 124 地址映射



以下为界面相关的描述。

表 82 地址映射

标识	描述
SUA 地址映射规则	该只读表显示的是缺省的地址映射规则。
全功能地址映射规则	
#	此处为规则索引号。
本地起始IP	这里是指内部本地地址（ILA）的起始 IP 地址。如果规则针对于所有的本地 IP 地址，此处会显示 0.0.0.0。对于Server的端口映射，本地 IP 地址会显示 N/A。
本地结束IP	这里是指内部本地地址（ILA）的最后一个 IP 地址。如果规则针对于所有的本地 IP 地址,此处会显示 255.255.255.255。对于 One-to-One 和Server的端口映射，本地 IP 地址会显示 N/A。

全局起始IP	这里是指内部全球 IP 地址(IGA)的起始 IP 地址。对于 Many-to-One 和 Server 的端口映射，如果 WAN 口 IP 地址是由 ISP 动态分配的，此处会显示 0.0.0.0。
全局结束IP	这里是指内部全球 IP 地址（IGA）的最后一个 IP 地址。对于 One-to-One,Many-to-One 和 Server 的端口映射,此处会显示 N/A。
类型	1. One-to-One 模式。 2. Many-to-One 模式。 3. Many-to-Many Overload 模式。 4. Many One-to-One 模式。 5. Server 模式。
修改	点击编辑按钮，可以进入您希望进行编辑的地址映射规则界面。 点击删除按钮，可以删除一个现存的地址映射规则。随后会出现一个提示窗口，确认您的删除动作。您删除完该规则以后，后续的地址映射规则会上移一位。
插入	点击 插入 可以在一个现存的规则之前插入一个新映射规则项。

14.4.1 编辑 NAT 地址映射规则

如果您想编辑一个映射规则，可以点击**编辑**按钮，见到以下界面。.

图 125 NAT 地址映射的编辑

NAT — 地址映射

地址映射规范

类型

One-to-One

本地起始IP

0 . 0 . 0 . 0

本地结束IP

N/A

全局起始IP

0 . 0 . 0 . 0

全局结束IP

N/A

应用

取消

以下为界面相关的描述。

表 83 NAT 地址映射的编辑

标识	描述

类型	从下拉菜单中选择一组映射规则。 1. One to One: 在一对一的模式中, ZyWALL 会将一个本地IP地址映射到一个全球IP 地址上。 2. Many to One: 在多对一的模式中, ZyWALL 将多个本地IP 地址映射到一个全球IP 地址上。这等同于SUA(例如: PAT, 端口地址转换), 就是ZyXEL 路由器支持的单用户帐号功能 (SUA 仅作为可选项)。 3. Many to many Overload: 在多对多加载的模式中, ZyWALL 将多个本地IP 地址映射到多个共享的全球地址上。 4. Many one to one: 在多个一对一的模式中, ZyWALL 将每一个本地IP 地址映射到单独对应的全球地址上。也就是一个本地地址对应一个全球地址。 5. Server: 这种模式允许指定隐藏于NAT 后面的提供不同服务的内部服务器, 并为全球提供接入服务。
本地起始IP	这里是指内部本地地址 (ILA) 的起始 IP 地址。如果规则针对于 Server 的端口映射, 本地 IP 地址会显示 N/A 。
本地结束IP	这里是指内部本地地址 (ILA) 的最后一个 IP 地址。如果规则针对于所有的本地 IP 地址, 此处会显示 255.255.255.255 。对于 One-to-One 和 Server 的端口映射, 本地 IP 地址会显示 N/A 。
全局起始IP	这里是指内部全球 IP 地址(IGA)的起始 IP 地址。如果 WAN 口 IP 地址是由 ISP 动态分配的, 此处会显示 0.0.0.0 。
全局结束IP	这里是指内部全球 IP 地址 (IGA) 的最后一个 IP 地址。对于 One-to-One, Many-to-One 和 Server 的端口映射, 此处会显示 N/A 。
应用	点击 应用 可以将修改的设置保存到 ZyWALL 中。
取消	点击 取消 可以不保存设置, 并退出该界面。

14.5 端口转发

端口转发设置是一系列的内部服务器(隐藏在 NAT 后面的局域网中), 例如, web 或 FTP 服务器。通过这样的设置, 即使对于外部网络来说, 整个内部网络相当于是一个具有单一IP地址的计算机, 外部的用户也可以穿透 NAT 来访问内部的服务器。

您可以设置一个端口或者一个范围的端口对应着本地网络中确定为服务器的IP地

址。

相应的端口号指定了对应的服务，例如，**web** 服务的端口是 **80**，**FTP** 的端口是 **21**。在某些情况中，如果存在一些不知名的服务或一个同时提供多种服务(**web** 和 **FTP**)的服务器，建议最好指定端口的范围。您可以规定一个服务器的 **IP** 地址对应着一个或一个范围的端口。

很多小区的宽带 **ISP** 帐号不允许用户在小区里运行任何的服务器进程（比如 **Web** 或 **FTP**）他们会定期检测服务器的存在并可能在当发现用户在小区里运行服务器时将用户的帐号挂起（暂停）如果不确定会出现这种情况，请咨询您的 **ISP**。

14.5.1 缺省服务器的 IP 地址

除了规定的服务之外，**NAT** 还可以支持一个缺省的服务器 **IP** 地址。这样即使在设置界面中没有规定某些端口，但是一台缺省的服务器也可以收到相应的数据包。

注意：如果您没有设置**默认服务器IP**地址，并且在设置界面中或在远程管理设置界面里没有规定某些端口，那么 **ZyWALL** 将会丢弃所有在该端口接收到的数据包。

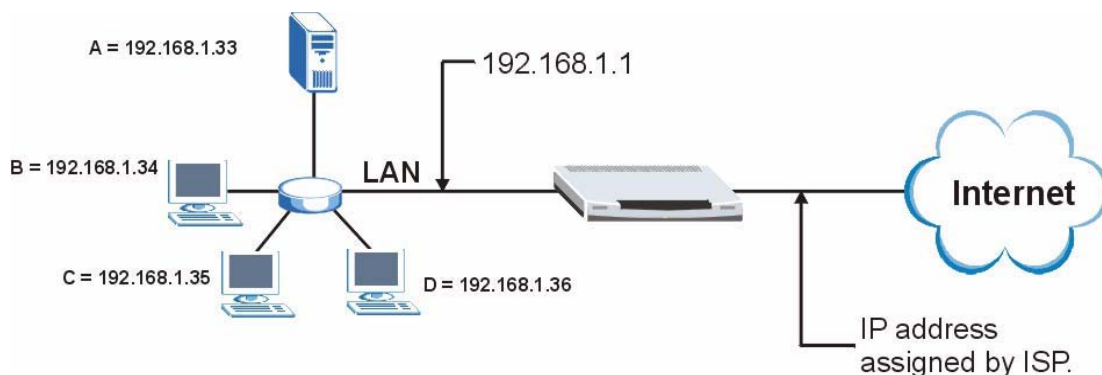
14.5.2 端口转发：服务和端口号

使用端口转发（**Port Forwarding**）界面可配置将来访的服务请求转发到你本地网络的服务器。通常使用的服务以及端口号参见录E。

14.5.3 配置端口转发到后面的服务器（范例）

例如您想设置端口 **21~25** 对应着一个 **FTP**，**Telnet** 和 **SMTP** 服务器（范例中的 **A**）端口 **80** 对应着一台 **web** 服务器（范例中的 **B**）给 **192.168.1.35**（范例中的 **C**）分配一个缺省服务器。您设置 **LAN IP** 地址，**ISP** 设置 **WAN IP** 地址。**NAT** 网络可以看成是 **Internet** 上的一台单一主机。

图 126 NAT 后面多台服务器的范例



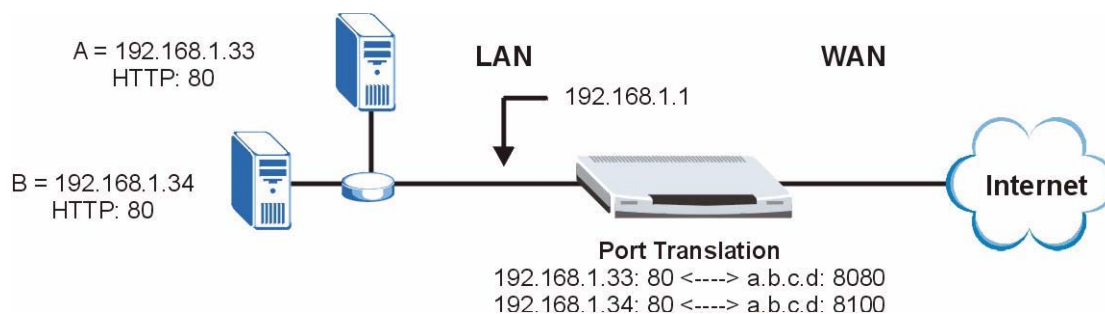
14.5.4 端口转译 (Port Translation)

ZyWALL 可以将从 WAN 口的不同端口或一个端口范围上发送的数据包转换到 LAN 上主机的其它端口或一个端口范围内。当您使用无端口转换的端口转发时，LAN 上的一个服务器可以使用一个规定的端口号，通过一个单一的 WAN 口 IP 地址来对外提供服务。当您使用支持端口转换的端口转发时，LAN 上的多个服务器使用相同的端口号，通过一个单一的 WAN 口 IP 地址来对外提供服务。

下面的范例说明在 LAN 上会有两个 web 服务器服务器 A 使用 IP 地址 192.168.1.33，服务器 B 使用 IP 地址 192.168.1.34。这两台服务器都使用端口号 80。小写的 a.b.c.d 代表 WAN 口的 IP 地址。ZyWALL 会将 WAN 口 (IP 地址为 a.b.c.d) 8080 端口上收到的数据发送到服务器 A (IP 地址为 192.168.1.33) 上。同时 ZyWALL 会将 WAN 口 (IP 地址为 a.b.c.d) 8100 端口上收到的数据送到服务器 B (IP 地址为 192.168.1.34) 上。

注意：在这个范例中，任何人如果想访问服务器 A，必须使用端口号 8080。任何人如果想访问服务器 B，必须使用端口号 8100。

图 127 端口转译范例



14.6 配置端口转发

注意: 如果您没有设置**默认服务器**的 IP 地址, 并且在设置界面中或在远程管理设置界面里没有规定某些端口, 那么 ZyWALL 将会丢弃所有在该端口接收到的数据包。

点击 **高级, NAT**, 然后点击**端口转发**可以打开**端口转发**界面。

请参考附录E来了解不同服务通常使用的端口。

注意:最后的端口转发规则是专供Roadrunner服务来使用的。这个规则仅在您将**WAN封装**设置为**Ethernet**, 并且将**服务类型**设置为除了**标准**以外的其它选项时才可用

图 128 端口转发

NAT

NAT概述地址映射端口转发触发端口

端口转发规则

默认服务器192 . 168 . 1 . 5

#	启用	名称	连入端口	端口转译	服务器IP地址
1	☒	Webser	80 - 80	0 - 0	192 . 168 . 1 . 12
2	☐		0 - 0	0 - 0	0 . 0 . 0 . 0
3	☐		0 - 0	0 - 0	0 . 0 . 0 . 0
4	☐		0 - 0	0 - 0	0 . 0 . 0 . 0
5	☐		0 - 0	0 - 0	0 . 0 . 0 . 0
6	☐		0 - 0	0 - 0	0 . 0 . 0 . 0
7	☐		0 - 0	0 - 0	0 . 0 . 0 . 0
8	☐		0 - 0	0 - 0	0 . 0 . 0 . 0
9	☐		0 - 0	0 - 0	0 . 0 . 0 . 0
10	☐		0 - 0	0 - 0	0 . 0 . 0 . 0
11	☐		0 - 0	0 - 0	0 . 0 . 0 . 0
#	☐	RR-Reserved	1026 - 1026	0 - 0	192 . 168 . 1 . 1

注意1：您可能还需要建立相关[防火墙](#)规则。
注意2：端口转译为可选项。

应用重置

以下为界面相关的描述。

表 84 端口转发

标识	描述
默认服务器	除了您所规定服务的服务器，NAT 还支持一个缺省的服务器。一个缺省的服务器可以接收该界面中没有规定的端口收到的数据。如果您没有设置 默认服务器 的 IP 地址，并且在设置界面中或在远程管理设置界面里没有规定某些端口,那么 ZyWALL 将会丢弃所有在该端口接收到的数据包。
#	这是各端口转发服务器项的索引号码。
启用	点选此项可以激活相应的端口转发服务器项。
名称	输入一个端口转发规则的标识名称。
连入端口	该处为端口号。如果转发到一个端口，您可以在前后两个区域输入相同的端口号。如果您想规定一个端口范围，您可在前后两个区域输入这个范围的始末端口号。
端口转译	您可在此输入 ZyWALL 会将连入端口转换到的端口号。对于一个端口范围，您只需要输入该范围的起始端口号即可，ZyWALL 可以自动计算转换端口范围的末尾端口号。
服务器 IP 地址	输入服务器的内网 IP 地址。
应用	点击 应用 ，可以保存设置。
重置	点击 重置 ，可以重新配置该界面。

14.7 端口转发示例—WAN 到 LAN 的 HTTP 转发规则

下面的示例说明了如何配置一个端口转发规则，来允许从WAN访问局域网IP地址为192.168.1.12的公共HTTP(Web)服务器。

注意:您还需要配置相应的防火墙规则，以便能够从WAN访问服务器。

- 1 选择启用选框，激活规则使用。
- 2 指定规则的名称。
- 3 输入端口80作为来访端口（输入两次）
- 4 指定在局域网上HTTP服务器的IP地址（本例中是192.168.1.12）。

图129 端口转发

NAT

NAT概述地址映射端口转发触发端口

端口转发规则

默认服务器192 . 168 . 1 . 5

#	启用	名称	连入端口	端口转译	服务器IP地址
1	☒	Webser	80 - 80	0 - 0	192 . 168 . 1 . 12
2	☐		0 - 0	0 - 0	0 . 0 . 0 . 0
3	☐		0 - 0	0 - 0	0 . 0 . 0 . 0
4	☐		0 - 0	0 - 0	0 . 0 . 0 . 0
5	☐		0 - 0	0 - 0	0 . 0 . 0 . 0
6	☐		0 - 0	0 - 0	0 . 0 . 0 . 0
7	☐		0 - 0	0 - 0	0 . 0 . 0 . 0
8	☐		0 - 0	0 - 0	0 . 0 . 0 . 0
9	☐		0 - 0	0 - 0	0 . 0 . 0 . 0
10	☐		0 - 0	0 - 0	0 . 0 . 0 . 0
11	☐		0 - 0	0 - 0	0 . 0 . 0 . 0
*	☐	RR-Reserved	1026 - 1026	0 - 0	192 . 168 . 1 . 1

注意1：您可能还需要建立相关[防火墙](#)规则。

注意2：端口转译为可选项。

应用

重置

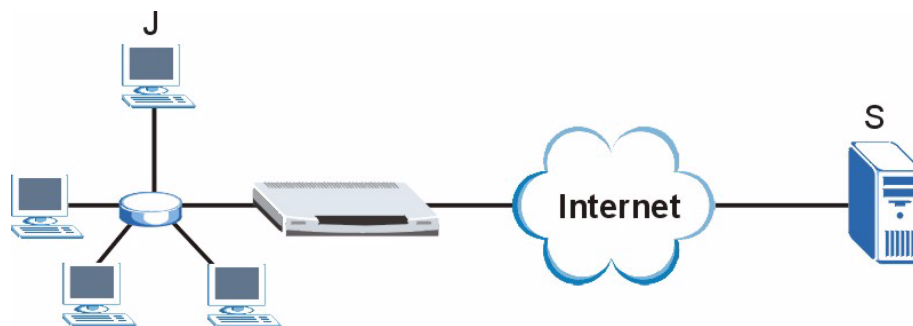
14.8 端口触发（Port Triggering）

一些应用服务会在客户端使用专门的一组端口，服务器端也使用专门的一组端口。对于一般的端口转发，您需要在 NAT 上设置一个转发端口规则，可以将某种服务（从 WAN 上的服务器发送过来）转发到客户端侧（LAN）的一个 IP 地址的计算机上。但问题是只能对单独的一个 LAN IP 地址提供该服务的端口转发。如果想让 LAN 上的其它计算机也可以使用此种服务，您需要手动修改端口转发所对应的 LAN 计算机的 IP 地址才可以实现。

触发端口转发的功能就可以解决这个问题，它可以允许内网的计算机动态获得此项服务的机会。当内网的计算机向外网发送数据包，请求获得一个专门端口号和协议（一个“触发”端口）的服务的时候，ZyWALL 会记录下该计算机的 IP 地址。当 ZyWALL 利用规定的 端口号和协议（“入”端口）接收到一个回应，它会将此数据包转发到发送请求的内网计算机上如果这台计算机的服务连接关闭了那么 LAN 上其它的计算机也可以使用该项服务。这样您就不用在配置界面里面修改 LAN 上能够应用这项服务的机算计的 IP 地址了。

范例如下：

图 130 触发端口转发流程：范例



1. 图中标识为J的为Jane的计算机，向图中标识为S的Real Audio服务器（端口号7070）请一个文件。
2. 端口“7070”就是一个“触发”端口可以让 ZyWALL 记录下 Jane 的计算机 IP 地址。随后 ZyWALL 会将 Jane 的计算机 IP 地址和“入”端口（范围在6970-7170）联系起来。
3. Real Audio 服务器会使用一个范围在 6970 到 7170 的端口号来进行回应。
4. ZyWALL 再将该数据包发送到 Jane 的计算机上。
5. 如果 Jane 的应用服务连接没有断开或者没有时间溢出，只有她可以使用该项服务。ZyWALL 对于 UDP 的应用存在 3 分钟的溢出时间，对于 TCP/IP 的应用存在2小时的溢出时间。

如果想修改 ZyWALL 的触发端口参数，您可先点击 **高级NAT** 然后点击 **端口触发** 标签。以下为设置界面。

图 131 端口触发

NAT

NAT概述地址映射端口转发触发端口

端口触发原则

#	名称	进入		触发	
		起始端口	结束端口	起始端口	结束端口
1		0	0	0	0
2		0	0	0	0
3		0	0	0	0
4		0	0	0	0
5		0	0	0	0
6		0	0	0	0
7		0	0	0	0
8		0	0	0	0
9		0	0	0	0
10		0	0	0	0
11		0	0	0	0
12		0	0	0	0

注意：您可能还需要建立相关[防火墙](#)规则。

应用重置

以下为界面相关的描述。

表 85 触发端口

标签	描述
#	这是规则索引号（只读）
名称	输入一个标识名称(最多 15 个字符)所有的字符都可以支持—包括空格。
进入	入端口就是 WAN 上的服务器用来发送一种特殊服务的端口。ZyWALL 会 将该端口（或端口范围）上的数据转发到 LAN 上的与这种服务相联系的客户计算机上。
起始端口	输入一个端口范围的起始端口号。
结束端口	输入一个端口范围的最后一个端口号。
触发	触发端口就是能够让 ZyWALL 记录下 LAN 内向 WAN 上的服务器发送数据包的计算机 IP 地址的端口号。
起始端口	输入一个端口范围的起始端口号。
结束端口	输入一个端口范围的最后一个端口号。

应用	点击 应用 可以将设置保存到 ZyWALL 中。
重置	点击 重置 可以重新配置该界面。

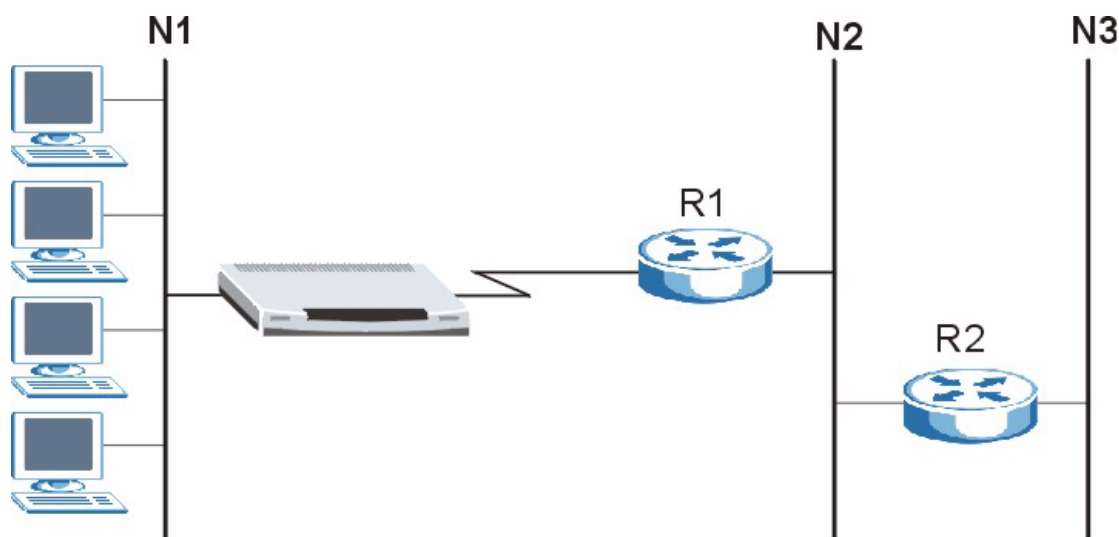
第 15 章 静态路由

本章向您介绍如何设置 ZyWALL 的静态路由。

15.1 IP 静态路由

每个远程节点仅规定了和网关直连的网络，ZyWALL 并不了解远端网络的情况。例如在下图中，ZyWALL 通过远程节点路由器 1 而得到关于网络 N2 的情况。然而，ZyWALL 不能发送数据包到 N3，因为它不知道通过同样的远程节点路由器 1（经由网关路由器 2）存在一条通路。静态路由是要把远程节点的网络情况通知给 ZyWALL。

图 132 静态路由拓扑范例



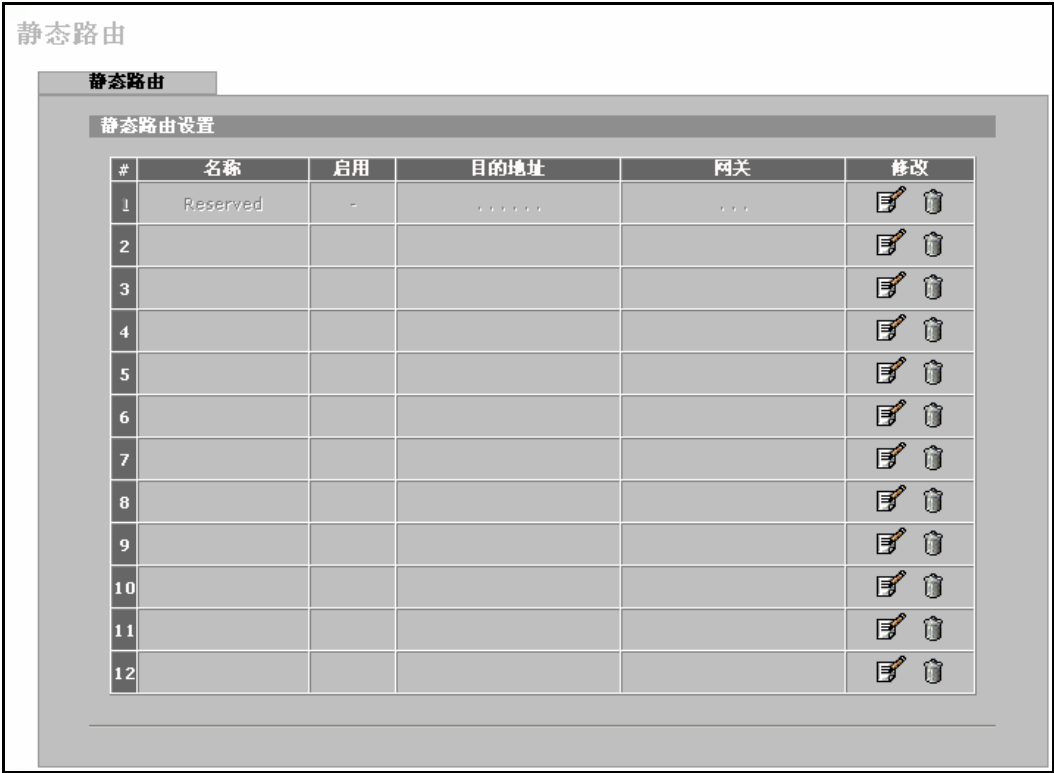
15.2 静态路由界面

点击 **高级 > 静态路由** 打开静态路由界面（界面上的一些空白行没有显示出来）。

注意： 第一个静态路由项用作缺省WAN 路由，你不能修改或删除它。保留名称为空，除非你已配置了一个静态WAN IP地址。

注意： 在你改变静态 WAN IP 地址为一个动态 WAN IP 地址后，缺省路由不再可用。

图 133 IP 静态路由



以下为界面相关的描述。

表 86 IP 静态路由

标识	描述
#	这是静态路由规则序列号。
名称	这是该条静态路由的描述名称。
启用	此处显示该规则是激活（Yes）还是未激活（No）
目的地址	该参数规定了最终目标的 IP 网络地址。路由永远基于网络号。
网关	这是网关的 IP 地址。网关是 ZyWALL 将数据发送到目的地的最近的邻居。在 LAN 上，网关是相同网段上的一台路由器，例如 ZyWALL；在 WAN 上，网关是其中一个远端节点的 IP 地址。
修改	点击编辑图标可以打开ZyWALL上一条静态路由的配置界面。 点击删除图标可以删除 ZyWALL 上的一条静态路由。随后会出现一个窗口，询问您是否确定要删除该路由。

15.2.1 配置 IP 静态路由

选择一条静态路由的索引号，然后点击编辑，可以显示该条静态路由的配置界面。

图 134 编辑 IP 静态路由

静态路由 — 编辑

静态路由设置

路由名称

☐ 启用

目的 IP 地址

0 . 0 . 0 . 0

IP 子网掩码

0 . 0 . 0 . 0

网关 IP 地址

0 . 0 . 0 . 0

跳数

2

☐ 私有

应用

取消

以下为界面相关的描述。

表 87 编辑 IP 静态路由

标识	描述
路由名称	输入该条 IP 静态路由的名称。此处留空可以删除该条静态路由。
启用	点选此框可以激活该条静态路由。
目的IP地址	该参数规定了最终目标的 IP 网络地址。路由永远基于网络号。如果您规定了一条到一台主机的路由，您需要在子网掩码处使用 255.255.255.255 的子网掩码来标识该主机。
IP子网掩码	输入 IP 子网掩码。
网关IP地址	这是网关的 IP 地址网关是 ZyWALL 将数据发送到目的地的最近的邻居。在LAN 上，网关是相同网段上的一台路由器，例如 ZyWALL；在WAN 上，网关是其中一个远端节点的 IP 地址。

跳数	Metric 代表路由的传输“成本”。IP 路由使用跳数来作为开销量度，最小值1代表直接连接的网络。您可输入一个数字来代表近似的链路开销值。数字不必精确，但是它必须在 1 到 15 之间。一般采用 2 或 3较好。
私有	这个参数决定 ZyWALL 是否在 RIP 广播的时候将该路由器的信息发送给远端节点。 点选此框可以保持这台路由器的私密性，不包括在 RIP 广播之内。 不选此框可以通过 RIP 广播将这台路由器信息传播给其它主机。
应用	点击 应用 ，可以将设置保存到 ZyWALL 中。
取消	点击 取消 ，可以不保存设置并退出该界面。

第 16 章 带宽管理

本章将会向您介绍带宽管理的功能与配置。

16.1 带宽管理概述

您可利用带宽管理功能在各通信端口上根据规定的通信类型来分配带宽。这样可以确保您的ZyWALL可以正常转发那些需要最小时延的通信应用（实时性要求很高的应用）。随着Voice-over-IP（VoIP）等实时应用的不断增加，人们对带宽分配的需求也日益增长。

关于带宽管理提出以下几点问题：

您可能会遇到多少种特殊应用的接入？

对于每一种通信类型需要设置什么样的优先级？

哪种通信类型的传输需要得到保证？

对于需要得到保证的传输类型应分配多大的带宽？

您可以利用带宽管理功能在接口上根据网络所承载的应用来分配带宽。这样可以减少在下一个路由设备上的时延和丢包现象。例如，如果连接到WAN口的宽带设备上行速率为1000kbps，则可将WAN口速率设置为1000kbps。设置页面的所有设置单位都是kbps（千比特/秒），而本用户手册都以简便起见，使用Mbps（兆比特/秒）为单位。

16.2 带宽分类与过滤

您可使用带宽分类与子类来分配带宽。您也可以根据特殊的应用和/或子网设置一个带宽过滤器来定义带宽类别或子类。您可以在**类别设置**标签（详情请参考章节16.11.1）中设置带宽类别的名称、带宽分配和带宽过滤器。您可为每一个带宽类别配置一个带宽过滤器。也可以只设置带宽类别，而不设置带宽过滤器。我们推荐您为所有不带过滤器的类别设置一个带过滤器的子类。ZyWALL可采用带宽预留分配机制为本身不带过滤器的类别或带过滤器的子类别提供不用的带宽。在**类别设置**标签下可以查看您设置的带宽类别与子类别（详情请参考章节16.11）。

为子类设置的带宽总量不能超过母类的预设带宽。

16.3 按比例分配带宽

您可以通过带宽管理来定义每个类别可获得多少带宽；实际上，分配给每个类别的带宽 会与实际可用带宽按一定的比例增加或减少。

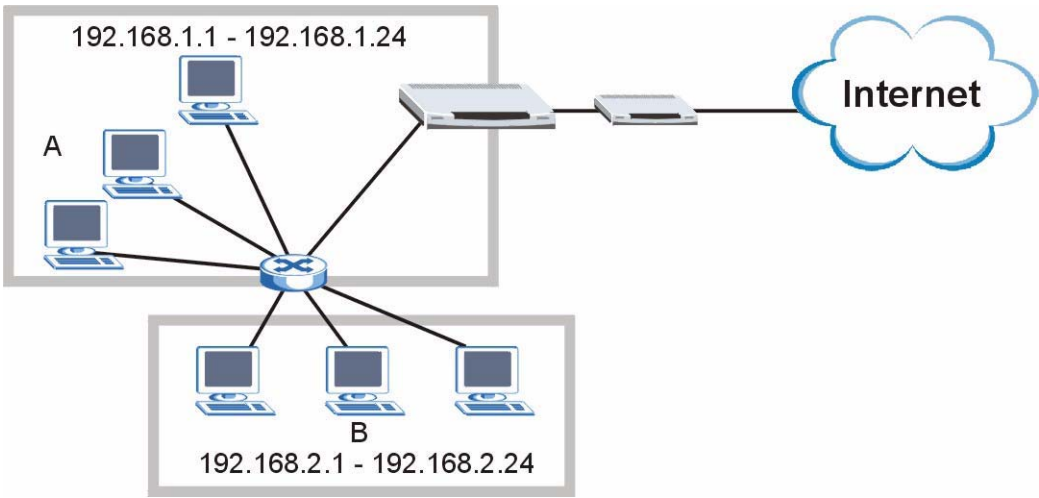
16.4 基于应用的带宽管理

您可以根据不同的应用（例如 VoIP、Web、FTP、E-mail 和 Video 等）来分配带宽。

16.5 基于子网的带宽管理

您可以根据子网来分配带宽。 下图显示了LAN上的各子网，您可以分别为子网A和子网B分别分配一个带宽类别。

图 135 基于子网的带宽管理范例



16.6 基于应用和子网的带宽管理范例

下例使用了基于LAN子网和应用的带宽类别（每个子网中按指定应用分配带宽）。

表88 基于应用和子网的带宽管理范例。

流量类型	来自子网A	来自子网B
VoIP	64 Kbps	64 Kbps
Web	64 Kbps	64 Kbps

FTP	64 Kbps	64 Kbps
E-mail	64 Kbps	64 Kbps
Video	64 Kbps	64 Kbps

16.7 调度

调度功能可在带宽级别中划分端口带宽。ZyWALL提供两种调度：基于公平的调度和 基于优先级的调度。

16.7.1 基于优先级的调度

启用基于优先级的调度后，ZyWALL根据您为带宽级别设定的优先级来转发流量。带宽级别的优先级越大，转发越快。为实时性应用（例如视频或音频）分配更高优先级可保证数据稳定传输。

16.7.2 基于公平的调度

启用基于公平的调度后，ZyWALL为所有带宽级别提供相同的带宽，以防止某个带宽级别使用端口所有的带宽。

16.7.3 最大带宽利用

使用最大带宽利用功能(参见276页图136)，ZyWALL可为需要更多带宽的类别划分端口上所有可用的带宽（包括分配的但其它类别没有使用的带宽和未分配的带宽）。启用最大带宽利用功能后，ZyWALL首先确认每个带宽类实际使用的带宽。

其次，ZyWALL根据需要更多带宽的类别数量和它们的优先级，进行端口的可用带宽（未划分的带宽或其它类未使用的带宽）的划分。如果只有一个类需要更多带宽，ZyWALL会将多余带宽分给该类。

如果有多个类需要更多带宽，ZyWALL先为最高优先级类别提供可用带宽（如果有足够带宽，则将按需分配）；如果还有可用带宽，则为低一级的类别提供带宽。如果优先级相同，ZyWALL会在同级类别之间平均分配可用带宽。

16.7.4 为不属于任何带宽类的流量预留带宽

请按照以下步骤设置ZyWALL，为不属于任何带宽类的流量提供带宽。

1. 预留一些带宽。
2. 不要启用端口的**最大带宽使用量**选项。
3. 如果是由根类作为父类的子类，则不要启用它的带宽借用功能（参见章节16.8）。

16.7.5 最大带宽使用量范例

以下是在ZyWALL上的一个端口启用最大带宽利用率的范例。下图是每个带宽类的带宽预留和优先级。这些类别是基于子网设置的。端口速率是10Mbps，每个子网分配2Mbps。在没有选择最大带宽利用率选项时，剩余的2Mbps用于不属于任何一个类别的流量。

表 89 最大带宽使用量范例

带宽类别和分配	
Root Class: 10240 kbps	Administration: 2048 kbps
	Sales: 2048 kbps
	Marketing: 2048 kbps
	Research: 2048 kbps

ZyWALL将预留的2Mbps划分给需要更多带宽的类别。如果Administration类只使用了分配给它的2Mbps中的1Mbps，ZyWALL会将剩余的1Mbps分配给需要更多带宽的类别。因此，ZyWALL将未分配和未使用的共3Mbps分配给需要更多带宽的类别。在本例中，假设除Administration类之外的所有类别都需要更多带宽。

16.7.5.1 基于优先级分配没有使用和没有预留的带宽

下表表示每个类别的优先级和每个类别获得带宽的数量。

表 90 基于优先级的分配没有使用和没有预留的带宽范例

带宽类别，优先权和分配	
Root Class: 10240 kbps	Administration: 优先级 4, 1024 kbps
	Sales: 优先级 6, 3584 kbps
	Marketing: 优先级 6, 3584 kbps
	Research: 优先级 5, 2048 kbps

假设除Administration类之外的所有类别都需要更多带宽。

administration类只使用了分配给它的2048kbps中的1024kbps，其它类别使用的 带宽都已经达到了它们的门限制。

由于Sales类和Marketing类具有最高优先级（6）而最先获得额外的带宽。如果 它们每个需要1536 kbps或更多的额外带宽，ZyWALL则会把共3072 kbps的未分 配和未使用的带宽在Sales类和Marketing类之间进行平均分配 为这2个类分别划 分1536 kbps的额外带宽，带宽共计3584 kbps）这样分配是因为它们具有最高优先级。

Research类也需要更多的带宽，但是只能获得设定的2Mbps，因为所有未分配和 未使用的带宽都已被分配给具有更高优先级的sales和marketing类。

16.7.5.2 基于公平的分配没有使用而没有预留的带宽

下表表示每个类别获得的带宽数量。

表 91 基于公平的分配没有使用而没有预留的带宽范例

带宽类别和分配	
Root Class: 10240 kbps	Administration: 1024 kbps
	Sales: 3072 kbps
	Marketing: 3072 kbps
	Research: 3072 kbps

假设除Administration类之外的所有类别都需要更多带宽。

administration类只使用了分配给它的2048 kbps中的1024kbps，其它类别使用的 带宽都已经达到了它们的门限制。

ZyWALL将未分配和未使用的共3072 kbps进行平均分配给其他带宽的类别。这样额外的1024 kbps使得其它类别每一个获得共计3072 kbps的带宽。

16.8 带宽借用

带宽借用是指子类从父类借用未使用的带宽，然而最大带宽利用允许类别借用端口上所有未分配或未使用的带宽。

启用子类的带宽借用后，子类则可从父类借用其未使用的带宽。父类未使用的带宽首先分配给最高优先级的子类。如果子类的父类也可从其父类借用未使用的带宽，这个子类则可向更高一级的父类（祖父类）借用带宽。以此类推，只要设置了带宽借用，就可以向多级类别的父类借用带宽（参见章节26.8.1）。

对子类分配的带宽不能超过对其父类的。ZyWALL使用这种规则在子类之间划分父类未使用的带宽。

16.8.1 带宽借用范例

以下是一个设置类别带宽借用的带宽管理范例。根据部门划分类别并且各部门之间是独立的。

关于在ZyWALL 中有多少类别等级可以配置，请参考附录中的产品规范。

表 92 带宽借用范例

带宽类别和带宽借用设定			
Root Class:	Administration: 可借用		
	Sales: Borrowing不能借用	Sales USA: 可借用	Bill: 可借用
			Amy: 不能借用
		Sales Asia: 不能借用	Tina: 可借用
			Fred: 不能借用
	Marketing: 可借用		
	Research: 不能借用	Software: 可借用	
		Hardware: 可借用	

Bill类启用带宽借用，Bill类则可从Sales USA类借用未使用的带宽。

Sales USA类启用带宽借用，Bill类则可从Sales类借用未使用的带宽。

Sales类未启用带宽借用，Bill类则不能从Root类借用未使用的带宽。

Amy类未启用带宽借用，Amy类则不能从Sales USA类借用未使用的带宽。

Research的Software类和Hardware类都启用带宽借用，Software类和Hardware类都可从Research类借用未使用的带宽。

Research类启用带宽借用，Software类和Hardware类都可从Root类借用未使用的带宽。

16.9 同时启用带宽借用和最大带宽利用

如果同时启用端口的最大带宽利用和独立子类的带宽借用，ZyWALL将按以下原理工作：

1. ZyWALL根据每个类别预定的带宽发送流量。

- 2. ZyWALL向启用带宽借用并且需要比设定值更多带宽的子类分配其父类的未使用带宽。ZyWALL先对最高优先级的子类进行带宽分配，若优先级相同的则平均分配。
- 3. ZyWALL将端口上未使用或未分配的带宽分配给任何需要带宽的类别。ZyWALL先从最高优先级开始分配，同优先级的平均分配。
- 4. ZyWALL将剩余的未分配带宽提供给不属于任何类别的流量。

16.10 配置汇总

点击高级>带宽管理可以打开概要界面。

打开端口的带宽管理，为端口设置带宽使用上限。

图 136 带宽管理：概要

带宽管理设置

概要

类别设置

监控

带宽管理设置

带宽管理功能可以管理从路由器指定界面流出的通信流量。每一个界面的带宽管理功能均可独立开启或关闭。

类别	启用	速度（ kbps ）	规则	最大带宽使用量
WAN	☐	100000	Fairness-Based	☐
LAN	☐	100000	Fairness-Based	☐

应用

重置

以下为界面相关的描述。

表 93 带宽管理：概要

标识	描述
类别	这些是表示物理接口的只读标识。点选端口选项可以启用端口的带宽管理。带宽管理将被应用于从该端口流出的所有流量，而与流量的来源无关。 流量重定向或IP别名可能导致LAN-to-LAN的流量通过ZyWALL时也要去匹配带宽管理的规则。
启用	点选该框可以启用端口的带宽管理。

速度 (kbps)	输入该端口上使用带宽管理的带宽总量。 此处为该端口的根类分配带宽(参见277页章节16.11)。推荐填入一个与该端口连接设备处理能力相匹配的速率。例如，如果WAN端口连接一台上行速率为1000kbps宽带设备，则将WAN口速率设为1000kbps。
规则	在下拉列表框中选择 Priority-Based 或 Fairness-Based 来控制流量。 若选择 Priority-Based ，则根据优先级顺序进行调度。 若选择 Fairness-Based ，则平等对待所有带宽类别。参见章节16.7。
最大带宽使用量	点选该框，ZyWALL会将端口上所有未分配和未使用的带宽分配给需要更多带宽的类别。如果需要为不属于任何类别的流量预留带宽，或者需要进行端口限速（参见速度字段的说明）则请不要选择该选项。（参见章节16.7.4。）
应用	点击 应用 ，可以保存设置。
重置	在下拉列表框中选择 Priority-Based 或 Fairness-Based 来控制流量。 若选择 Priority-Based ，则根据优先级顺序进行调度。 若选择 Fairness-Based ，则平等对待所有带宽类别。参见章节25.7。

16.11 设置类别

您可在类别设置页面中为每个端口设置带宽类别。选择一个端口，然后按以下讲解进行设置。点击“+”展开类别的树形结构或点击“-”合并树。每个端口都有一个永久根。根的预留带宽即为设置的端口带宽（请参考章节16.10来设置端口速率），然后为根设置子类。

选择**高级 > 带宽管理**中**类别设置**标签，即可添加或删除端口的子类，页面显示如下。

图 137 带宽管理：类别设置



以下为界面相关的描述。

表 94 带宽管理：类别设置

标签	描述
接口	在下拉列表中选择一个端口进行设置。 带宽管理控制了某一个界面上的输出流量，而不是输入流量。所以为了限制局域网用户的下载带宽，请设置局域网上的带宽管理级别。为了限制上传带宽，请设置相应的广域网接口的带宽管理级别。
带宽管理	该区域显示所选接口的带宽管理是否激活，激活（启用）或没激活（未启用）。
添加子类	点击 添加子类 增加一个子类。
编辑	点击 编辑 设置选择的类别，根类是不能编辑的。
删除	点击 删除 删除类别和其所有的子类，根类是不能删除的。
统计资料	点击 统计资料 显示选择类别的状态。
过滤清单	该列表显示在选择的界面被配置为类别的带宽管理过滤规则。为了使它们出现在这里，ZyWALL 要应用带宽管理过滤规则。一旦一个连接与一个带宽管理过滤规则相匹配，ZyWALL 将运用对应的带宽管理类的规则，并且不检查连接其它的带宽管理过滤规则。
#	这是单独的带宽管理过滤规则的索引号。

过滤名称	这是识别带宽管理过滤规则的名称。
服务	这是配置为需要管理的带宽管理规则。
目的IP地址	这是该带宽管理过滤规则应用的目标IP地址。
目的端口	这是该带宽管理过滤规则应用的目标端口号。
来源IP地址	这是该带宽管理过滤规则应用的源IP地址。
源端口	这是该带宽管理过滤规则应用的源端口号。
协议ID	这是该带宽管理过滤规则应用的连接协议ID（服务类型）号。举例来说：1代表ICMP，6代表TCP或17代表UDP。
移动	输入过滤规则的索引号和您想放置过滤规则的号码。点击 移动 ，移动过滤规则到您输入的位置。您过滤规则的排序非常重要，因为他们会按编号的顺序来应用。

16.11.1 带宽管理类别设置

可在**类别设置**页面中配置一个带宽管理类。在设置端口的类别之前，您需要在**概要**界面中启用该端口的带宽管理。

要添加一个子类，请先点击**高级>带宽管理**，然后点击**类别设置**标签，最后点击**添加子类**按钮可以打开以下页面。

图 138 带宽管理：编辑类别

带宽管理 — 编辑类别

类别设置

类别名称

admin

带宽预算容量

15000

(Kbps)

优先级

3

(0-7)

☐

从上层类别借用带宽

过滤设置

☒

启动带宽过滤

服务

FTP

目的IP地址

0

.

0

.

0

.

0

目的子网掩码

0

.

0

.

0

.

0

目的端口

0

来源IP地址

192

.

168

.

1

.

0

来源子网掩码

255

.

255

.

255

.

0

来源端口

0

协议ID

0

应用

取消

以下为界面相关的描述。

表 95 带宽管理：编辑类别

标签	描述
类别设置	
类别名称	使用自动生成的名称或输入一个描述性的名称，最多20个字符，包括空格。
带宽预算容量	以kbps为单位指定最大允许的带宽。推荐设置在20kbps到20000 kbps之间。
优先级	输入0到7之间的数字设置类的优先级。数字越大，优先级越高。默认值是3。

从上层类别借用带宽	选择此选项后，如果父类实际使用的带宽没有达到预设值，子类可向其父类借用带宽。 带宽借用通过子类的优先级进行管理。即最高优先级（7）的子类先获得从父类借用带宽的权力。 如果需要预留出其它流量的带宽（参见272页16.7.4节）或将端口速率设置为与相连网络设备的处理能力相匹配的值(参见表93)，请不要对根类的子类进行此项设置。
过滤设置	
启用带宽过滤	选择启用带宽过滤 ZyWALL则在执行带宽管理时进行带宽过滤。 至少填写以下字段中的一个（除了子网掩码字段，只有在输入源或目的IP地址后才需要输入）。
服务	该区域可以简化带宽类别配置，您只需要选择一个预定义的应用即可。当您选择了一个预定义的应用，您就不用再配置带宽过滤区域中的其它项（除了启用或不启用该规则）。 FTP（文件传输程序）是一种能够使文件快速传递的程序，包括那些不能由电子邮件传递的大文件。从下拉列表中选择FTP，然后为FTP流量配置带宽过滤规则。 H.323是一种用于通过网络进行多媒体通信的协议，例如 NetMeeting。从下拉列表中选择H.323，然后为H.323流量配置带宽过滤规则。 注意：如果您选择了H.323，请确定您也利用ALG界面来启用ALG。 SIP（会话启动协议）是应用层控制（发信号）协议，用于操作建立，警告和声音拆卸以及通过互联网进行多点会话。ZyWALL 支持SIP穿越。从下拉列表框中选择SIP，然后为SIP流量配置带宽过滤规则。这个选项使它更加容易为SIP流量处理带宽，如果当您的LAN上有一个VoIP设备，该选项会很有用。 注意：如果您选择了SIP，请确保您在ALG界面中也启用了SIP ALG功能。 如果您不想为带宽类别使用一个预定义的应用，请从下拉列表框中选择Custom。当选中Custom的时候，您需要至少配置后面区域中的一个。
目的IP地址	输入目的IP地址。

目的IP子网掩码	输入目的子网掩码。如果您不填 目的IP地址 字段，该字段也可以不用填。更多详细信息请参见附录D。
目的端口	输入目的端口号。请参考附录E。.
来源IP地址	输入源IP地址。
来源子网掩码	输入源的子网掩码。如果您不填 来源IP地址 字段，该字段也可以不用填。更多详细信息请参见附录D。
来源端口	输入源端口号。
协议ID	输入协议ID（服务类型）号，例如：1对应ICMP，6对应TCP或17对应UDP。
应用	点击 应用 可以保存设置。
取消	点击 取消 可以退出该界面，不保存设置。

表 96 服务与端口号

服务	端口号
ECHO	7
FTP（文件传输协议）	2
SMTP（简单邮件传输协议）	2
DNS（域名服务系统）	5
Finger	7
HTTP（超文本传输协议或WWW, Web）	8
POP3（电子邮件协议）	11
NNTP（网络新闻传输协议）	11
SNMP（简单网络管理协议）	16
SNMP 陷阱	16
PPTP（点对点隧道协议）	172

16.11.2 带宽管理统计

您可以使用**带宽管理统计**页面查看网络性能。点击**类别设置**页面中的**统计资料**按钮可以打开**统计资料**页面。

图 139 带宽管理统计



以下为界面相关的描述。

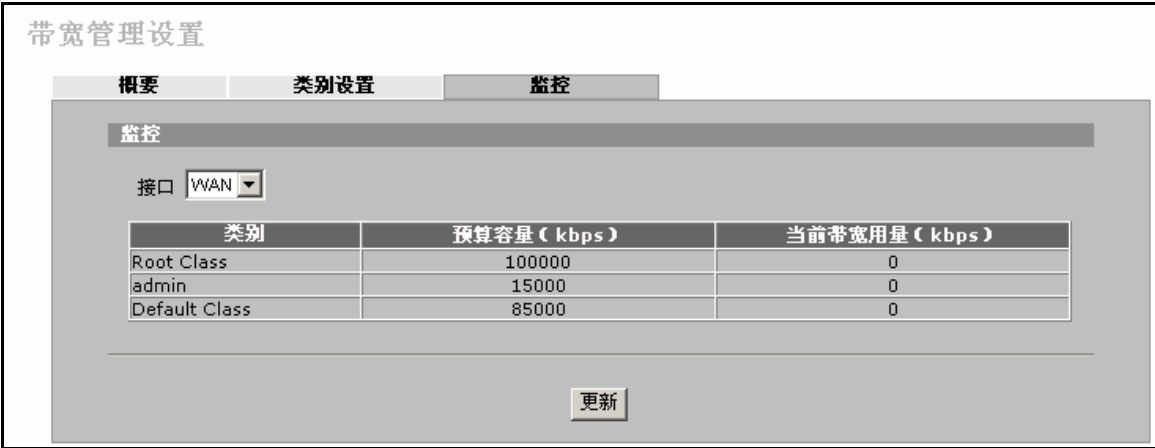
表 97 带宽管理统计

标识	描述
类别名称	本字段表示本统计页显示的类别名称。
预 算 容 量 (kbps)	本字段表示分配给本类别的总带宽量。
发包数	本字段表示传输数据包的总量。
发包量	本字段表示传输的总字节量。
丢包数	本字段表示丢弃数据包的总量。
丢包量Bytes	本字段表示丢弃数据包的总字节量。
过去8秒内的带宽统计	
本区域表示过去1-8秒的带宽统计（以bps为单位）。例如，t-1表示刚过去的1秒。	
更新周期(秒)	输入以秒为单位的时间间隔，定义多久进行信息刷新。
设置区隔	点击 设置区隔 ,启用在上面 更新周期 字段中输入的新时间间隔。
停止更新	点击 停止更新 ，停止浏览器刷新带宽管理统计表。
清除计数器	点击 清除计数器 ，清空所有的带宽管理统计表。

16.12 配置监控

点击 **高级 > 带宽管理>监控**打开以下界面，使用此界面来可看设备的带宽使用以及分配情况。

图 140 带宽管理：监控



以下为界面显示。

表 98 带宽管理：监控

标识	描述
接口	从下拉列表中选择一个端口，以浏览其带宽使用与带宽类别情况。
类别	本字段显示类别的名称。 在 Root Class 中会自动出现一个 Defaule Class ，将所有的带宽分配给没有分配带宽的类别。如果您没有在该界面启用最大带宽利用功能，ZyWALL会用这个默认类别来发送不匹配任何带宽类别的流量。
预算容量 (kbps)	该区域显示分配给该类的带宽总量。
当前带宽用量 (kbps)	该区域显示该类实际使用的带宽总量。
更新	点击 更新 可以刷新该页面。

a.如果您将所有的根类别的带宽都分配给各带宽类别,那么在默认 class处仍然会显示一个2kbps中的一个门限制（能够给一个带宽类别分派的为最小带宽）

第 17 章 DNS

本章将会向您介绍 DNS 的配置界面。

17.1 DNS 概述

DNS（域名系统）可以将一个域名映射为相应的 IP 地址，让后在网上传输。DNS 相当重要，因为如果没有它，您需要知道设备的 IP 地址才可以进行访问。ZyWALL 使用一个系统 DNS 服务器（您在 **DNS 系统** 界面中规定的）来解析域名，例如，VPN，DDNS 和时间服务器。

17.2 DNS 服务器地址分配

ZyWALL 可以用以下几种方法来获得 DNS 服务器的地址。

1. ISP 会告诉您 DNS 服务器的 IP 地址，一般在您申请的时候，DNS 服务器的 IP 地址会填在一个表格里面。如果您的 ISP 给您分配了 DNS 服务器的 IP 地址，您可以手工填写在 DNS 服务器的区域中。
2. 如果 ISP 动态给您分配 DNS 服务器的 IP 地址（同时还有 ZyWALL 的 WAN 口 IP 地址），您需要在 DNS 服务器区域中设置从 ISP 获得 DNS 服务器的 IP 地址。
3. 您可以手工输入其它 DNS 服务器的 IP 地址。这个服务器可以在公网，也可以在私网。DNS 服务器甚至可以在一个远程 IPSec 路由器的后面（请参考章节 17.5.1）。

17.3 DNS 服务器

您可以在 ZyWALL 上的 3 个地方可以配置 DNS。

1. 在 **DNS 系统** 界面中配置 DNS 服务器的 IP 地址，它可以为 VPN，DDNS 和时间服务器提供地址解析。
2. 在 **DNS DHCP** 界面中配置 DNS 服务器的 IP 地址，它可以将 DNS 服务器

的 IP 地址发送到 LAN, DMZ 或 WLAN 里的 DHCP 客户端上。

3. 您可以在**远程管理 DNS**界面中配置 ZyWALL 路由模式是接收还是丢弃 DNS 查询信息。

17.4 地址记录

地址记录包括完全合格的域名 (FQDN) 到一个 IP 地址的映射。一个 FQDN 由一个主机名和域名以及高层域名组成。例如, **www.zyxel.com.tw** 就是一个 FQDN, 其中 **www** 就是主机名 **zyxel** 就是二级域名 **com.tw** 就是高层域名。
mail.myZyXEL.com.tw 也是一个 FQDN, 其中 **mail** 就是主机名, **myZyXEL** 就是二级域名, **com.tw** 就是高层域名。

ZyXELL 允许您配置有关 ZyXEL 自身或其它设备的地址记录信息。通过这种方法, 您可以在您的网络上保留一个人们经常使用的 DNS 名称和地址的记录。如果 ZyWALL 收到了一个 FQDN 的 DNS 查询, 而 ZyWALL 的地址记录信息中就有这样的记录。ZyWALL 就不再向 DNS 名称服务器进行查询而直接回送相应的 IP 地址。

17.4.1 DNS 通配符

通配符功能可以使 ***.yourhost.com** 与 **yourhost.com** 使用相同的 IP 地址。例如, **www.yourhost.com** 仍然可以访问您的主机。

17.5 名称服务器记录

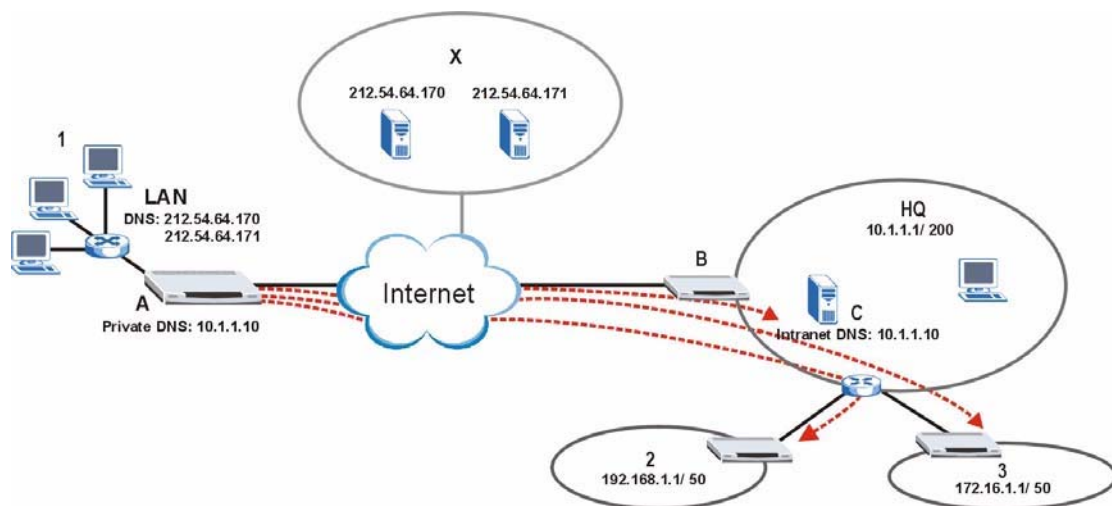
名称服务器的记录包括了一个 DNS 服务器的 IP 地址。ZyWALL 可以查询 DNS 服务器, 用于为 VPN, DDNS 和时间服务器提供地址解析服务。其中也包括域名区。域名区就是没有主机名的 FQDN。例如, **zyxel.com.tw** 就是域名区, 而 **www.zyxel.com.tw** 就是 FQDN。

17.5.1 私有 DNS 服务器

如果您想使用域名来访问远程私有网络里的服务器, 您就需要指定一台 DNS 服务器。您不能使用您 LAN 网中或 ISP 提供的 DNS 服务器, 它不能进行域名到远程私有网络服务器 IP 地址的解析。

下图描述了一个应用范例：由 ZyWALL 建立了 3 条 VPN 隧道，一条连到分支办事处 2，一条连到分支办事处 3，另外一条连到总部（HQ）。为了使用域名来访问 HQ 网络中的计算机，分支办事处 1 中的 ZyWALL 需要使用总部里的内部 DNS 服务器。

图 141 私有 DNS 服务器范例



注意：如果您没有规定远程网络中的 DNS 服务器，那么 VPN 主机就需要使用 IP 地址 来访问远程私有网络中的计算机。

17.6 系统界面

如果您想配置 ZyWALL 的 DNS 地址和名称服务器记录,点击 **高级,DNS** 即可。随后会出现以下界面。

图 142 系统 DNS

DNS

系统缓存DHCPDDNS

地址记录

#	FQDN	通配符	IP地址	修改
1	www.zyxel.com.tw	No	172.23.23.41	 

添加

名称服务器记录

#	网域区域	来自	DNS服务器	修改
-	*	Default	None	N/A

插入新的记录于1（记录号）之前。

以下为界面相关的描述。

表 99 系统DNS

标签	描述
地址记录	地址 record 项指定一个完全合格域名（fully qualified domain name, FQDN）到一个IP 地址的映射。一个FQDN 由一个主机及域名组成，包含一个顶级域名。例如， www.zyxel.com.tw 就是一个完全合格域名，这里“www” 是主机，“zyxel”是二级域名，“com.tw”是顶级域名。
#	此处为地址记录项的索引号。
FQDN	这是主机的完全合格域名。
通配符	此处显示该域名是否启用了DNS通配符的功能。
IP地址	这是主机的 IP 地址。
修改	点击 编辑图标，您可以进入记录项的编辑页面。 点击删除图标，您可以删除一个现存的记录。随后会出现一个窗口提示您的删除动作。当您删除完该记录以后，后续的记录会前移一位。
添加	点击 添加 ，您可以填加一条记录。请参考表100了解相关信息。

名称服务器记录	当 ZyWALL 需要解析一个域名的时候，它会按顺序查询该列表中的域名服务器记录项。 “*”代表无域名区的名称服务器记录。缺省的记录是灰色的。如果需要解析的域名和任何其它名称服务器记录都不相符的时候,ZyWALL 会使用这个缺省的记录。
#	这是名称服务器记录的索引号。
网络区域	域名区就是一个无主机名的 FQDN。例如，zyxel.com.tw 就是 www.zyxel.com.tw（FQDN）的域名区。
来自	此处显示 DNS 服务器的 IP 地址是来自于 WAN 口还是用户规定的。
DNS服务器	此处显示 DNS 服务器的 IP 地址。
修改	点击三角图标可以将记录项在列表中移动。 点击编辑图标，您可以编辑该记录项。 点击 删除 图标,您可以删除一个现存的记录项。随后会出现一个窗口提示您的删除动作。当您删除完该记录以后，后续的记录会前移一位。
插入	您可以点击 插入 插入一条新的名称服务器记录项。请参考表 1011 了解相关信息。

17.6.1 添加一条地址记录

在 系统 界面中点击 添加可以添加一条地址记录。

图 143 系统 DNS: 添加地址记录

DNS - 编辑地址记录

地址记录

FQDN

IP地址

WAN接口

0.0.0.0

自订

0 . 0 . 0 . 0

☐ 启用通配符

应用

取消

以下为界面相关的描述。

表 100 系统 DNS: 添加地址记录

标签	描述

FQDN	输入一台服务器的完全合格的域名（FQDN）。一个FQDN 由一个主机名和域名以及高层域名组成。例如，www.zyxel.com.tw 就是一个FQDN，其中www 就是主机名，zyxel 就是二级域名，com.tw 就是高层域名。
IP地址	如果该项对应着WAN口，您可以选择WAN接口，然后从下拉菜单中选择一个WAN口。 如果该项没有对着WAN口，您可以选择自定，然后输入主机的IP地址。
启用通配符	选择该选框可以激活DNS通配符的功能。
应用	点击应用，可以保存设置。
取消	点击取消，可以不保存设置并退出该界面。

17.6.2 插入一条名称服务器记录

在系统界面中点击插入可以插入一条名称服务器记录项。

图 144 插入一条名称服务器记录

DNS - 编辑名称服务器记录

名称服务器记录

网域区域*

* 可选项。如果所有网域区域都是由指定的DNS服务器提供服务，请保留这个栏位的空白。

DNS服务器

来自ISP的DNS服务器

第一DNS服务器

第二DNS服务器

第三DNS服务器

N/A

N/A

N/A

公用DNS服务器

私有DNS服务器

0 . 0 . 0 . 0

0 . 0 . 0 . 0

应用

取消

以下为界面相关的描述。

表 101 系统 DNS：插入名称服务器记录

标识	描述
网域区域	该项可选。
	如果所有的域名区都由规定的 DNS 服务器提供，此处可以留空。

DNS服务器	如果 ISP 动态分配 DNS 服务器的信息, 请选择 来自ISP的DNS服务器按钮。下面会显示只读的 DNS (由 ISP 分配的) 服务器的 IP 地址。如果 ISP 没有分配 DNS 服务器的 IP 地址, 此处会显示 N/A。如果 ZyWALL 有一个固定的 WAN 口 IP 地址, 此处会显示 N/A。 如果您有一个 DNS 服务器的 IP 地址, 请选择公用DNS服务器。这个IP地址必须是一个公网或您 LAN 内的私网地址。在右边输入该地址。 如果您选择了公用DNS服务器, 您就不能输入 0.0.0.0。 如果 DNS 服务器有一个私有的 IP 地址, 并且在一个远端 VPN 路由器的后面, 请选择私有DNS服务器。在右边输入该地址。 如果您想使用一台 私有DNS 服务器, 您需要同时在 DNS LAN 界面中配置头一个 DNS 服务器项使用 DNS Relay。 如果 ZyWALL 使用 VPN 通道向那一台 Private DNS 服务器 转发 DNS 查询信息的时候您需要同时配置一条 VPN 规则。该规则需要将 ZyWALL 的 LAN 口 IP 地址作为本地 IP 地址DNS 服务器的 IP 地址作为一个远端 IP 地址。 如果您选择了私有DNS服务器, 您就不能输入 0.0.0.0。
应用	点击 应用 , 可以保存设置。
取消	点击 取消 , 可以不保存设置并退出该界面。

17.7 DNS 缓存

DNS 缓存就是路由器里面的一个临时存储从 DNS 服务器返回的响应信息的区域。当 ZyWALL 收到 DNS 服务器发送的响应信息的时候, 它会将此响应记录在 DNS 缓存里面。该响应信息有可能是肯定的, 也可能是否定的。肯定的响应就是 ZyWALL 收到了一个域名所对应的 IP 地址。否定的响应就是 ZyWALL 在 5 秒钟的 DNS 溢出时间内没有收到一个域名所对应的 IP 地址。

当 ZyWALL 收到了一个 DNS 查询信息的时候它会在将此查询信息发送到 DNS 服务器之前先在 DNS 缓存里面进行比较。如果该 DNS 查询信息符合肯定响应区域中的某一项, ZyWALL 就会直接响应肯定项中所对应的 IP 地址。如果该 DNS 查询信息符合否定响应区域中的某一项, ZyWALL 就会直接回送 DNS 查询失败的信息。

17.8 配置 DNS 缓存

如果想配置 ZyWALL 的 DNS 缓存,先点击 **高级,DNS**,然后点击**缓存**标签。随后会出现以下界面。

图 145 DNS 缓存

DNS

系统缓存DHCPDDNS

DNS缓存设置

☒缓存正确的DNS解析

最大的TTL

3600

(60~3600 秒)

☐缓存不正确的DNS解析

不正确的缓存周期

60

(60~3600 秒)

应用

重置

DNS缓存项目

清除更新

#	缓存类型▲	域名	IP 地址	剩余时间 (秒)	修改

以下为界面相关的描述。

表 102 DNS缓存

标识	描述
DNS缓存设置	
缓存正确的DNS解析	点选此框可以在缓存中存储肯定的 DNS 解析信息。这样可以提高 ZyWALL 处理 DNS 查询的速度,减少 ZyWALL 通过 WAN 口发送的大量查询信息。
最大的TTL	输入最大的生存时间 (TTL) (60 到 3600 秒)。该时间可以决定 ZyWALL 在丢弃肯定查询信息之前的最大保留时间。
缓存不正确的DNS解析	点选此框可以在缓存中存储否定的 DNS 解析信息。这样可以提高 ZyWALL 处理 DNS 查询的速度,减少 ZyWALL 通过 WAN 口发送的大量查询信息。
不正确的缓存周期	输入最大的生存时间 (TTL) (60 到 3600 秒)。该时间可以决定 ZyWALL 在丢弃否定查询信息之前的最大保留时间。
应用	点击 应用 ,可以保存设置。

重置	点击 重置 ，可以重新设置该界面。
DNS缓存项目	
清除	点击该按钮可以手工清除缓存区域。
更新	点击该按钮可以重新加载缓存。
#	此处为记录项的索引号。
缓存类型	此处显示 DNS 请求响应信息是肯定的还是否定的。
域名	此处为主机域名。
IP地址	此处为主机相应的 IP 地址。对于否定的 DNS 解析项此处为 0.0.0.0。
剩余时间(秒)	这里显示该缓存项在被丢弃之前的保留剩余时间。
修改	点击删除图标可以删除该缓存项。

17.9 配置 DNS DHCP

先点击 **高级**，**DNS**，然后点击 **DHCP** 标签可以打开 **DNS DHCP** 界面。
您可以 在该界面中配置 **DNS** 服务器信息，ZyWALL 会将该信息发送到 **LAN**，**DMZ** 或 **WLAN** 上的 **DHCP** 客户端处。

图 146 DNS DHCP

DNS

系统

缓存

DHCP

DDNS

由DHCP服务器分派的DNS服务器

选择接口

LAN

#	DNS		IP
1	第一DNS服务器	From ISP	N/A
2	第二DNS服务器	From ISP	N/A
3	第三DNS服务器	From ISP	N/A

应用

重置

以下为界面相关的描述。

表 103 DNS DHCP

标识	描述

由DHCP服务器分配的DNS服务器	ZyWALL可以给DHCP客户端提供DNS服务器的IP地址。
选择接口	从下拉列表中选择一个界面，为指定的界面配置DNS服务器。
DNS	这个是只读标识，表示DNS服务器。
IP	如果您的ISP动态给您分配的信息（和ZyWALL的WAN口IP地址），请选择From ISP。在右边的区域中您可以从下拉菜单中选择一个由ISP分配的DNS服务器的IP地址。 如果您知道DNS服务器的IP地址，您可以选择User-Defined。在右边的区域中您输入DNS服务器的IP地址。 如果您选择了User-Defined，但是地址处您输入的是0.0.0.0，在您点击应用以后，User-Defined会变成None。如果您在第二个选项处选择了User-Defined，并设置了相同的IP地址，在您点击应用以后，第二个选项处的User-Defined会变成None。ZyWALL如果作为一个DNS Proxy，请选择DNS Proxy。这样ZyWALL的LAN口IP地址就会出现在右边的区域中（只读）。ZyWALL会告诉LAN内的DHCP客户端，它就是DNS服务器。 当LAN内的计算机向ZyWALL发送一个DNS查询的时候，ZyWALL就会将这个查询信息发送到ZyWALL的系统DNS服务器（您在DNS 系统界面中配置的），并将响应信息发送给这台计算机。您只能选择一个DNS Relay，如果您将第二个或者第三个DNS服务器配制成DNS Relay，在您点击应用以后，该选项会变成None。如果您不想配置DNS服务器，请选择None。如果您不配置DNS服务器的IP的地址，您就需要知道您要访问计算机的IP地址。
应用	点击 应用 ，可以保存设置。
重置	点击 重置 ，可以重新设置该界面。

17.10 动态 DNS

如果 ZyWALL 的 WAN 口 IP 地址是动态获得的，此时您也希望别人能够通过 Internet 来访问您提供的一种或多种服务（例如 web, IPsec VPN 等服务），您就可以采用动态 DNS 的技术来实现。例如您做了一个网站 myweb.vicp.net，如果别人想访问您的网站，就需要知道您当前的 IP 地址。如果采用了动态 DNS 的技术，大家不用知道您当前的临时 IP 地址，只要直接访问 myweb.vicp.net 就可以了。

但是首先您需要在动态 DNS 服务提供商处注册一个动态 DNS 的账号和域名。ZyWALL 内置的动态 DNS 提供者是 www.dyndns.org，国内的用户可以直接采用国内的动态 DNS 服务提供商提供的动态 DNS 的域名解析服务。您在注册完账号和域名以后，需要下载一个动态 DNS 的客户端软件，安装在 ZyWALL 内网的计算机上，并输入您注册的账号和域名，使之运行起来。

注意：您在正常使用动态 DNS 服务之前，需要到动态 DNS 服务提供商的 web 站点上注册一个用户账号和一个域名。

17.10.1 DYNDNS 通配符

通配符功能可以使 *. yourhost. dyndns.org 与 yourhost. dyndns.org 使用相同的 IP 地址。例如，www.yourhost.dyndns.org 仍然可以访问您的主机。

注意：如果你具有私有 WAN IP，那么你不能使用动态 DNS。

17.10.2 高有效性

DNS 服务器 可以将域名映射到一个 WAN 口的 IP 地址上。如果该 WAN 口的连接断开，高有效性可以允许 ZyWALL 将域名解析到另外的一个 WAN 口的 IP 地址上。

17.11 配置动态 DNS

要更改 ZyWALL 的 DDNS，点击 **高级 > DNS > DDNS**，界面显示如下：

图147 DDNS

DNS

系统

缓存

DHCP

DDNS

帐户设置

☒ 启用

服务供货商

使用者名称

密码

WWW.DynDNS.ORG

我的域名

#	域名	DDNS类型	离线	通配符	IP地址更新原则
1	ZyWALL	Dynamic	☐	☒	Use WAN IP Address
2		Dynamic	☐	☐	Use WAN IP Address
3		Dynamic	☐	☐	Use WAN IP Address
4		Dynamic	☐	☐	Use WAN IP Address
5		Dynamic	☐	☐	Use WAN IP Address

应用

重置

以下为界面相关的描述。

表 104 DDNS

标识	描述
帐户设置	
启用	点选此框可以使用动态 DNS 服务只限于下面的动态 DNS 服务提供商提供的服务）。
服务供货商	这是一个动态服务提供商的名称（只读）。
使用者名称	输入您的用户名。最多 31 个区分大小写的字符（包括下划线），不包括空格。
密码	输入密码最多 31 个区分大小写的字符包括下划线不包括空 格。
我的域名	
域名1~5	输入主机名。
DDNS类型	选择您从该动态 DNS 服务提供商处注册的服务类型。如果您有动态 DNS 服务，请选择 Dynamic 。如果您有静态 DNS 服务，请选择 Static 。 如果您有自定义的 DNS 服务，请选择 Custom 。

离线	当您在 DDNS类型 区域中选择 Custom 的时候, 该项有效。当您离线的时候, 动态域名服务提供商会将访问数据发送到一个指定的URL (您可以规定) 处。
通配符	点选此框可以启用 DYNDNS 的通配符。
WAN Interface	选择一个 WAN 口用于更新域名解析得到的 IP 地址。
IP 地址更新原则	选择 Use WAN IP Address, ZyWALL 会使用 WAN 口 IP 地址来更新域名。 选择 User-Defined, 如果您有静态的 IP 地址, 请输入该地址。 只当 ZyWALL 和 DDNS 服务器 之间存在一个或多个 NAT 路由器的候, 您才可以选择 Let DDNS Server Auto Detect。该特征可以 DDNS 服务器 自动检测, 并使用 NAT 路由器的 IP 地址作为一个网 的 IP 地址。 注意: 如果在 ZyWALL 和 DDNS 服务器 之间有一个 HTTP proxy 服务器 的时候, DDNS 服务器 可能不能检测到正确的 IP 地址。
应用	点击 应用 , 可以保存设置。
重置	点击 重置 , 可以重新配置该界面。

第 18 章 远程管理

本章将会向您介绍远程管理界面。

18.1 远程管理概述

远程管理可以决定您从哪些电脑以何种方式通过什么样的界面可以接入到 ZyWALL 里面来。

注意：当您从 WAN 口进行远程管理的时候，必须设置一条允许接入的防火墙规则。防火墙规则的详细配置请参第8章。

您可以通过以下的各种方式来远程管理您的 ZyWALL：

Internet (WAN only)	—仅广域网
ALL (LAN&WAN&DMZ&WLAN)	—所有均可
LAN only	—仅局域网
Neither (Disable)	—均不采用，屏蔽此功能。

注意：当选择 **DMZ only**，**WAN only**，**WLAN only** 或者 **ALL**

(**LAN&WAN&DMZ&WLAN**) 的时候，您需要设置防火墙规则以便允许接入。如果您不想开放远程管理的功能可以在 **服务器访问接口**的相应区域内选择 **Disable**。您每次只能同时使用一种远程管理的功能。当高权限的远程管理接入的时候，ZyWALL 会自动断开低权限的远程管理。以下是不同远程管理的权限定义：

1. 本地控制口
2. SSH
3. Telnet
4. HTTPS 和 HTTP

18.1.1 远程管理局限性

出现以下各种情况的时候，您将不能通过 LAN 或者 WAN 来进行远程管理：

1. 在 SMT 界面中的 menu 3.1 (LAN) 或者在 menu 11.5 (WAN) 中应用一条过滤规则，阻止了 Telnet、FTP 或者 Web 服务。

2. 您在远程管理的界面中关闭了相关的服务。
3. 客户端的 IP 地址和在 **Secure Client IP Address** 中设置的 IP 地址不相符。如果不一致的话，ZyWALL 会立即断开该任务。
4. 如果目前已经存在一个具有相同优先级或更高优先级的远程管理。并且您同时只能使用一种远程管理方式。
5. 存在一条防火墙规则，阻止进行远程管理。

18.1.2 系统超时

缺省的系统管理空闲时间为 5 分钟（300 秒）如果您在 5 分钟之内没有执行任何管理操作的话，ZyWALL 会自动结束您的管理任务。当一个统计界面正在输出的时候，管理任务不会超时。您可以在**系统**界面中修改您的时间值。

18.2 介绍 HTTPS

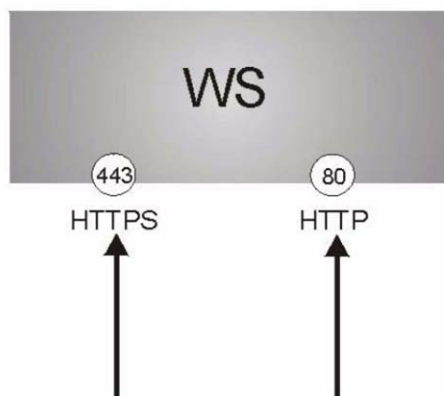
HTTPS (HyperText Transfer协议 over Secure Socket Layer或 HTTP over SSL 安全套接层上的超文本传输协议) 是一种可以加密和解密 web 页的 web 协议。安全套接层 (SSL) 是一种应用层协议，它能够确保数据传输中的机密性（未经授权的人不能读取传输的数据）、认证性（一方能够鉴别另一方）、完整性（您可知道数据是否已经被更改过了）。

它依靠证书、公匙和私匙（详细资料请参见217页12章）。ZyWALL 上使用 HTTPS 是为了保证您在进行 web 配置的时候能够安全接入到 ZyWALL 里面来。SSL 协议中规定 SSL 服务器（ZyWALL）总是为 SSL 客户端（请求到 ZyWALL 进行 HTTPS 连接的计算机）鉴别自己，但是当 SSL 服务器请求它这样做的时候，SSL 客户端只鉴别自己（在**远程管理**，**WWW** 界面中选择 **验证客户端的认证**）即可。**验证客户端的认证**可选，如果选择它的话，说明 SSL 客户端需要给 ZyWALL 发送一个证书。您需要从 ZyWALL 可信任的 CA 上为浏览器申请一个证书。

请参考下图说明：

1. HTTPS 连接是从一个支持 SSL 的 web 浏览器发送请求到 ZyWALL WS (web 服务器) 的 443 端口（缺省）。
2. HTTP 连接是从一个 web 浏览器发送请求到 ZyWALL WS (web服务器) 的80 端口（缺省）。

图 148 HTTPS 的建立



注意：如果您在 **远程管理 WWW** 界面中禁用 **HTTP** 服务器访问接口 (**Disable**) 的话，ZyWALL 会阻止所有 HTTP 的尝试连接。

18.3 WWW

如果想更改 ZyWALL 的 web 设置，您可点击 **高级，远程管理** 来打 开 **WWW** 界面。

图 149 WWW

远程管理

WWW	SSH	TELNET	FTP	SNMP	DNS	CNM
HTTPS						
服务器认证		auto_generated_self_signed_cert (参阅 我的证书)				
☐ 验证客户端的认证 (参阅 可信的CA)						
服务器端口		443				
服务器访问接口		All				
可靠客户端的IP地址		☒ 全部 ☐ 已选取的 0.0.0.0				
HTTP						
服务器端口		80				
服务器访问接口		All				
可靠客户端的IP地址		☒ 全部 ☐ 已选取的 0.0.0.0				
注意 1：若要让 UPnP 正常运作，必须先有 HTTP 服务，让使用 UPnP 的局域网电脑可以使用。 注意 2：若要正常作用，您可能还需要建立相关 防火墙 规则。						
应用		重置				

以下为界面相关的描述。

表 105 WWW

标识	描述
HTTPS	
服务器认证	选择 服务器认证 。ZyWALL可以鉴别自身。ZyWALL是一个SSL服务器，总是需要为SSL客户端请求到ZyWALL进行HTTPS连接的（计算机）鉴别自己。
验证客户端的认证	选择 验证客户端的认证 （可选项），可以要求SSL客户端通过向ZyWALL发送一个证书来认证自己。首先SSL客户端需要从ZyWALL的可信任CA上获得一个证书。
服务器端口	缺省的情况下，HTTPS代理服务侦听端口 443 。如果您想修改ZyWALL的HTTPS端口，例如改为 8443 ，您需要通知人们用以下方式来接入到ZyWALL的web配置页面来：“https://ZyWALL IP 地址: 8443”。
服务器访问接口	您可以从 服务器访问接口 的下拉菜单中选择一个ZyWALL的接口，用于建立HTTPS的连接。您可以在 HTTPS 服务器访问接口 中选择 Disable ，在 HTTPS 服务器访问接口 区域中选择一个接口来只允许安全的web配置的接入。
可靠客户端的IP地址	一个安全的客户端就是一个可以信任的电脑，可以允许接入到ZyWALL中来。选择 ALL ，可以允许任何电脑接入ZyWALL。 选择 已选取的 ，可以允许指定IP的电脑接入ZyWALL。
HTTP	
服务器端口	如果需要，您可以改变某个服务的服务器端口号，但是为了远程管理，必须使用相同的端口。
服务器访问接口	您可以从 服务器访问接口 的下拉菜单中选择一个ZyWALL的接口，用于建立HTTP的连接。
可靠客户端的IP地址	一个安全的客户端就是一个可以信任的电脑，可以允许接入到ZyWALL中来。选择 ALL ，可以允许任何电脑接入ZyWALL。 选择 已选取的 ，可以允许指定IP的电脑接入ZyWALL。
应用	点击 应用 ，保存设置并退出界面。
重置	点击 重置 ，重新开始配置界面。

18.4 HTTPS 范例

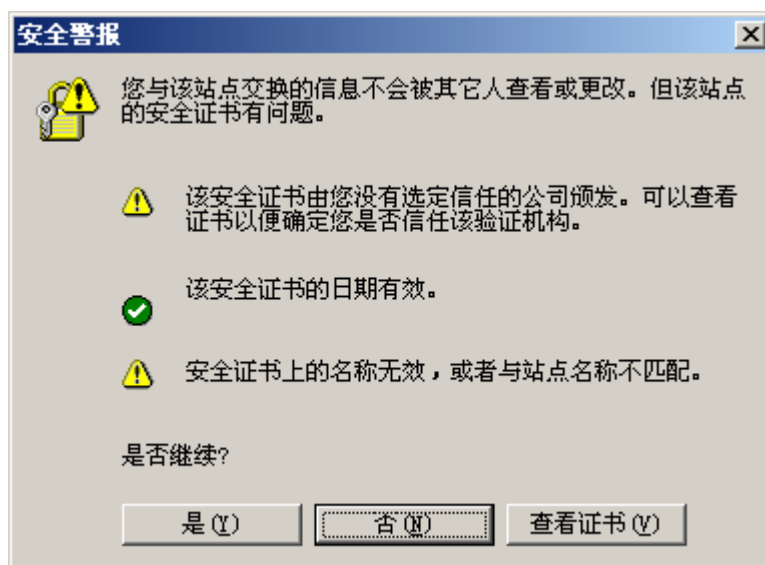
如果不改变ZyWALL缺省的HTTPS端口，您可直接在浏览器中输入“https://ZyWALL IP 地址”。

址/”，其中“ZyWALL IP 地址”就是ZyWALL的IP地址或域名。

18.4.1 IE 报警信息

当试图连接到ZyWALL的HTTPS服务器时，一个视窗对话框会弹出来询问是否信任该服务器证书。如果您想确认该证书是否来自于ZyWALL，可以击**查看证书**。随后您会在IE中看到**安全报警**界面。选择**是**，可以进入配置登录的WEB页；如果选择**否**，WEB配置接入会被关闭。

图150 安全警报对话框（Internet Explorer）



18.4.2 Netscape Navigator 警告信息

当您试图接入ZyWALL的HTTPS服务器时，一个**Website Certified by an Unknown Authority**界面会弹出来向您询问是否信任该服务器证书。如果您想确认该证书来自于ZyWALL，可以击**Examine Certificate**。

如果您选择**Accept this certificate temporarily for this session**，点击**OK**可以继续。

如果您选择**Accept this certificate permanently**，就会将ZyWALL的证书注入到SSL客户端中。

图 151 安全证书 1 (Netscape)

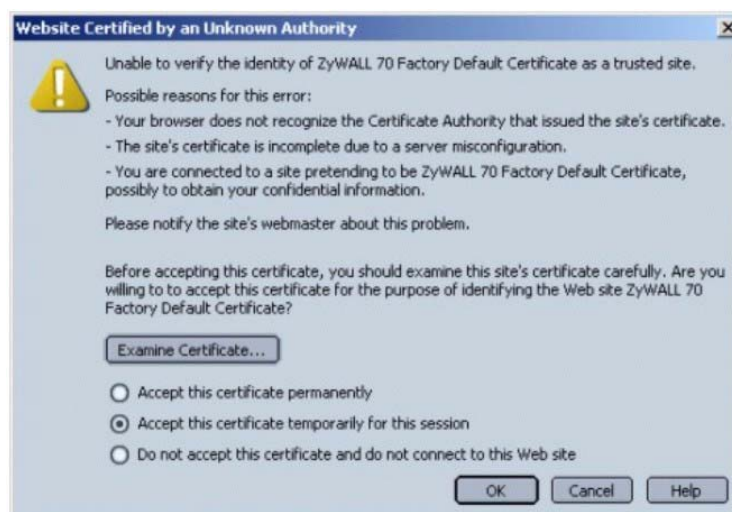


图 152 安全证书 2 (Netscape)



18.4.3 避免出现浏览器报警信息

以下描述是您的浏览器出现有关ZyWALL的HTTPS服务器证书报警信息的主要原因，以及您可以采取那些措施来避免此类报警信息的出现。

ZyWALL的HTTPS服务器所发放的证书不是浏览器信任的证书机构发放的证书。而ZyWALL发放的证书是ZyWALL出厂缺省的证书，也就是ZyWALL自签名的证书。

- 如果浏览器相信这个自签名的证书，可以将这个证书存放到您的操作系统上，作为一个可信任证书。
- 如果想让浏览器相信一个认证中心所发放的证书，可以将该认证中心发放的证书存放到您的操作系统里作为一个可以信任的证书来使用。

HTTPS服务器上真实的IP地址（您试图连接的ZyWALL相应端口的IP地址）和您 浏览器接收到的ZyWALL的HTTPS服务器证书的通用名称不相符。请按照以下步骤来检查ZyWALL发送给HTTPS客户端的证书上所规定的通用名称。

A) 点击**远程管理**。记住在**服务器认证**里显示的证书的名称。

B) 点击**证书**。找到证书，检查一下它的**主题**栏。**CN**代表证书的通用名称。

利用下面这个步骤您可以让ZyWALL使用一个和ZyWALL的真实IP地址相符的通用名称。如果您需要接入到一个使用动态分配IP地址的WAN口上，您就不能使用这个步骤了。

A) 给ZyWALL创建一个新的证书，使用IP地址作为证书的通用名称。例如，如果想使用HTTPS接入到一个IP地址是192.168.1.1的LAN口,您需要创建一个使用192.168.1.1做为通用名称的证书。

B) 进入远程管理**WWW**界面，然后在**服务器认证**中选择一个新创建的证书。点击**应用**。

18. 4.4 登录界面

当您接受了这个证书,随即会出现 ZyWALL 的登录界面。在浏览器的右下方出现了一个锁头的标志，说明这是一个安全的连接。

图 153 登录界面 (Internet Explorer)

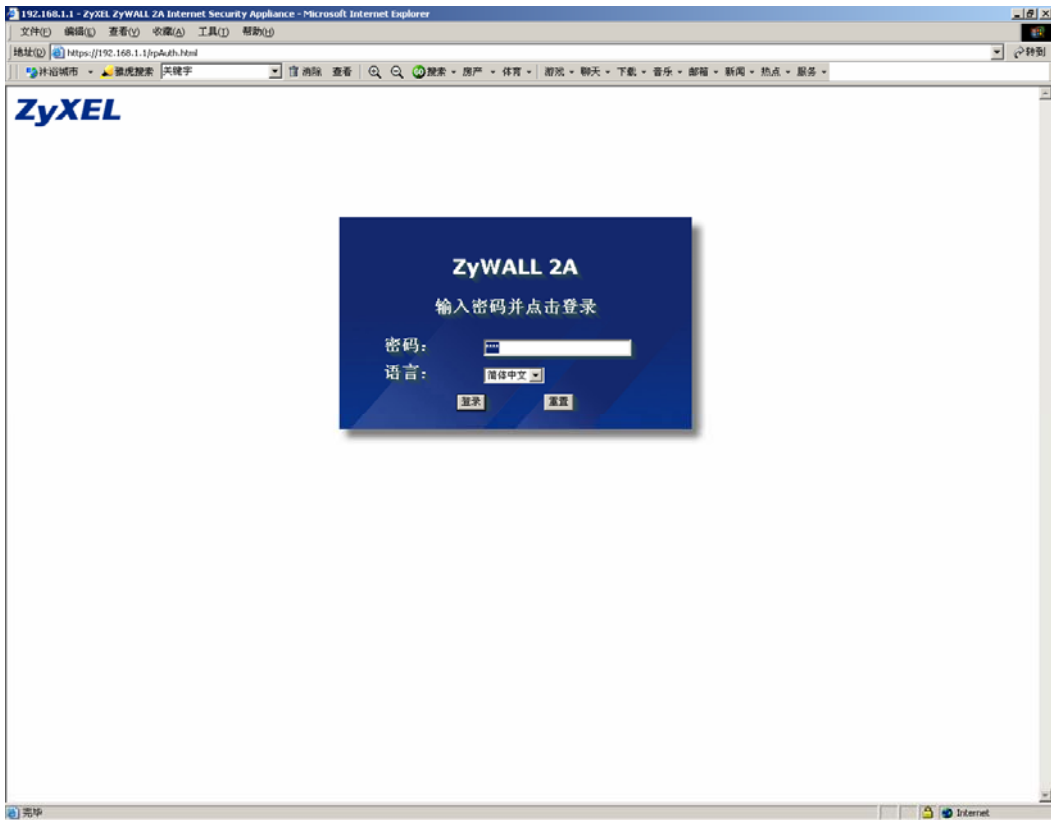
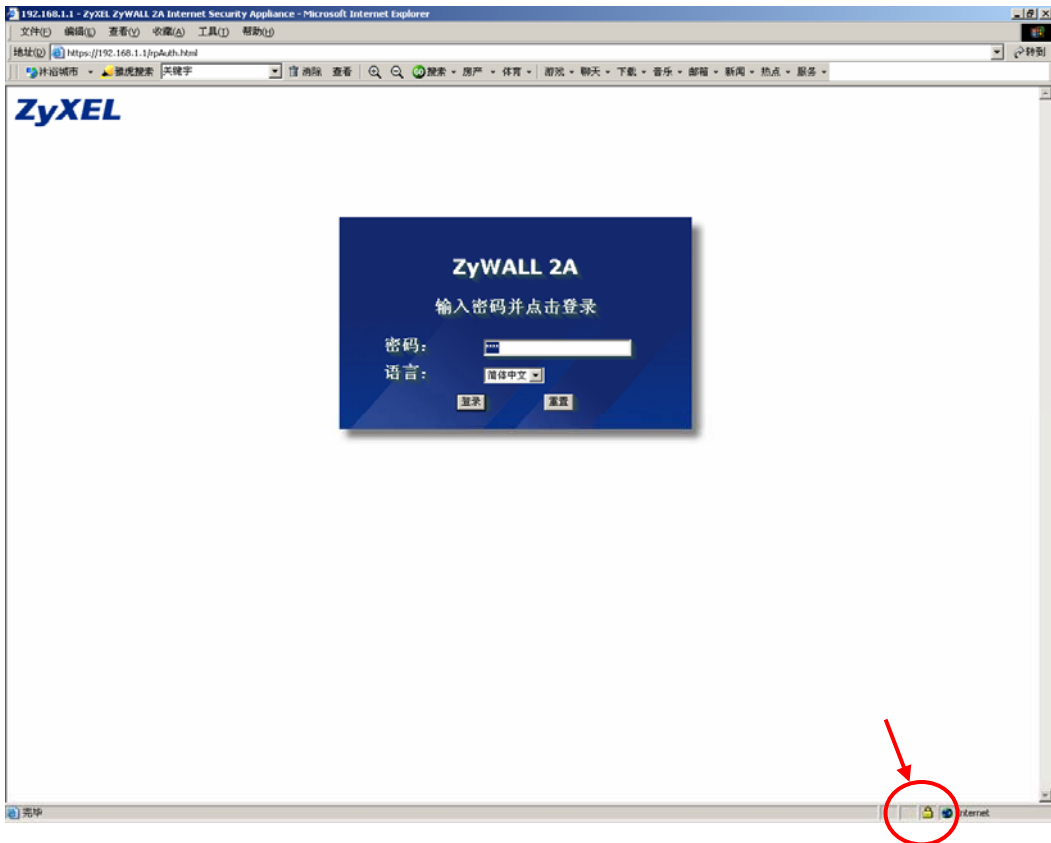
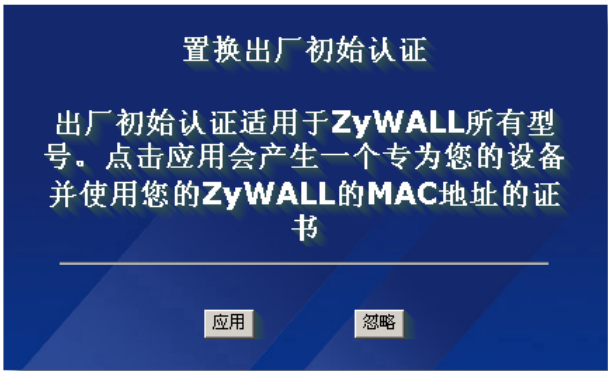


图154 登录界面（IE浏览器）



直接点击**登陆**，您会见到以下界面。出厂缺省的证书是一个适用于所有ZyWALL产品的通用缺省证书

图 155 置换出厂初始认证



您在**置换出厂初始认证**界面里点击**应用**，可以利用ZyWALL的MAC地址来创建 一个证书。点击**证书**，打开**我的证书**界面。您会见到类似于下图中显示的信息。

图 156 设备规定的证书



您如果在**置换出厂初始认证**界面中点击**忽略**，就会使用这个通用的ZyWALL证书。您在**我的证书**界面中就会见到这个信息。

图 157 通用ZyWALL证书



18.5 SSH

不同于Telnet 或FTP对文本透明的传输，SSH (Secure Shell)则是一个安全的通信协议，同时支持认证和加密功能。利用它，您可以实现通信双方在不安全的网络上进行安全的通信。

下图中，A是SSH服务器，B是SSH客户。

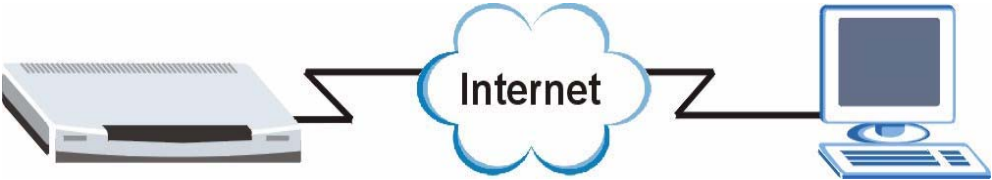
图 158 SSH 通信示例

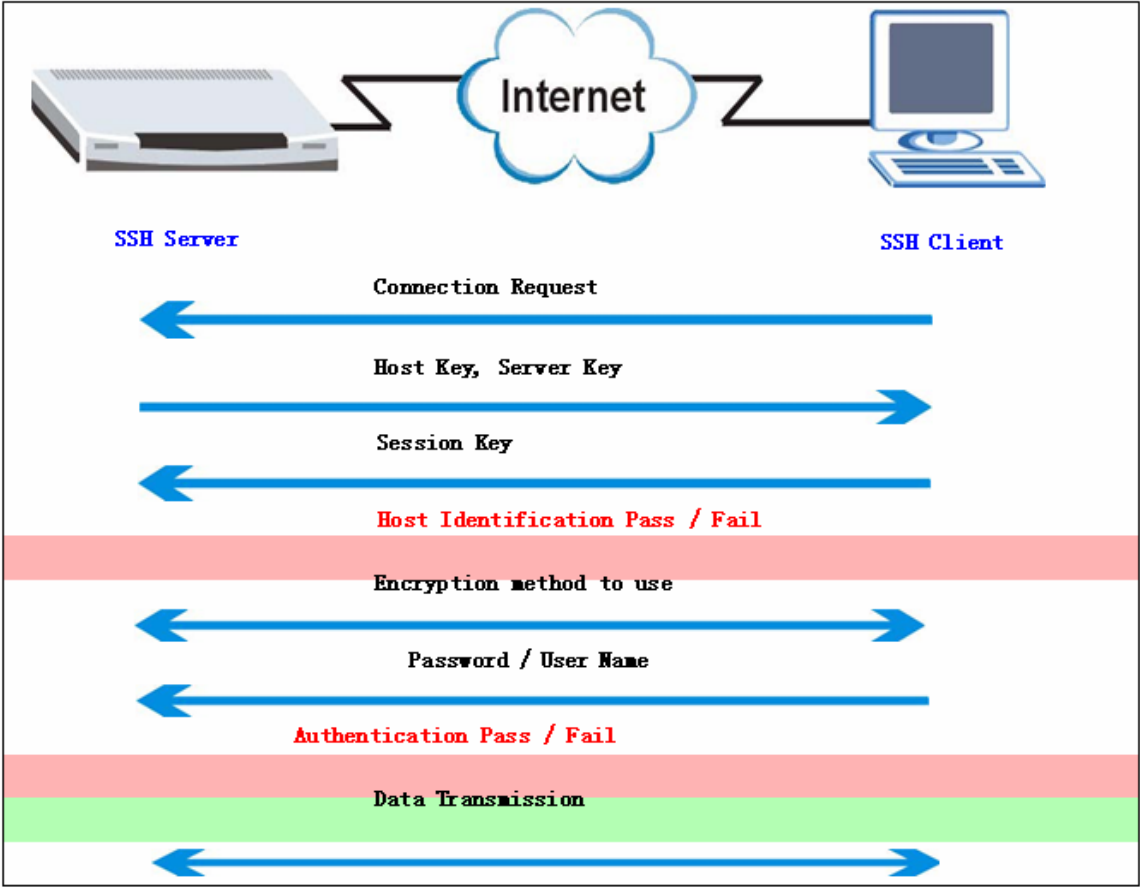


18.6 如何工作

下图向您介绍了如何在通信双方建立一条安全的连接。

表 106 SSH如何工作





1 主机确认

SSH客户端首先向SSH服务器发送一个连接请求。服务器向客户端发送一个包，内容包括自己的主机密钥（Host Key）的公钥部分、服务密钥（服务器 Key）的公钥部分和一个 64位的随机数（cookie）等信息。这个包没有加密，是明文发送的。

客户端接收包后，依据这两把密钥和被称为cookie的64位随机数计算出会话号(session id)和用于加密的会话密钥（session key）随后客户端回送一个包给服务器，内容包括这个经过加密的会话 密钥。

2. 加密方式一旦经过了确认，客户端和服务端就需要协商数据加密的方法。

3. 认证和数据传输 经过主机确认和数据加密启用以后，客户端和服务端之间就建立起了一条安全的通道。然后客户端再将认证信息（用户名和密码）发送给服务器，以便能够登录到服务器。

18.7 ZyWALL 上的 SSH 应用

您的ZyWALL支持版本为1.5的SSH采用RSA的认证方式和3种加密方式DES3DES 和

Blowfish) ZyWALL上的SSH服务器可用于进行远程SMT管理和在端口22上的文件传输。
需要注意同时只能存在一条SSH的连接。

18.7.1 使用 SSH 的需求

您需要在通过SSH连接到ZyWALL的客户计算机上安装一个SSH客户端程序。

18.8 配置 SSH

如果您想修改ZyWALL安全壳的设置，可以先点击**远程管理**，然后打开**SSH**一栏。
界面如下所示。 注意：特别提示您，如果采用SSH方式进行安全连接的话，您需要关闭Telnet和FTP的连接。

图 159 SSH



以下为界面相关的描述。

表154 SSH

标识	描述
服务器主机密码	选择一个证书，相应的私钥用于在SSH连接中标识ZyWALL。您需要在 我的证书 界面中提前配置好证书（点击 我的证书 ，查看第12章，以寻求更多信息）
服务器端口	如果需要的话，您可以修改相应的服务端口号，但是您也需要使用相同的端口号的服务来进行远程管理。
服务器访问端口	选择一个接口，计算机可以通过该接口使用此服务访问ZyWALL。
可靠客户端的IP地址	安全的客户端就是可信任的计算机，可以允许使用此服务接入到 ZyWALL中来。选择 All ，表示所有的计算机都可以使用此服务接入到ZyWALL中来。选择 已选取的 ，只允许规定IP地址的计算机使用此服务接入到ZyWALL中来。

应用	点击 应用 ，可以保存设置，并退出该界面。
重置	点击 重置 ，可以重新配置该界面。

18.9 使用 SSH 执行 Telnet 的范例

本章向您介绍如何使用一个命令界面和一个图形化的SSH客户端程序来远程接入到ZyWALL中。配置和连接步骤类似于大多数的SSH客户端程序。请参考SSH客户端程序用户手册。

18.9.1 范例 1: Microsoft Windows

本节介绍如何使用安全壳客户端程序来接入到ZyWALL中。

1. 安装SSH客户端程序，设置到ZyWALL的连接信息(IP地址，端口号或设备名称)
2. 配置SSH客户端以接受使用SSH（版本v1）的连接。
3. 一个视窗会出现，提醒您将主机密钥保存到电脑上。点击**Yes**可以继续。

160 SSH范例1: 保存主机密钥



输入密码登录到ZyWALL中，随后会出现一个SMT主界面。

18.9.2 范例 2: Linux

本节为您介绍如何使用大多数Linux采用的OpenSSH客户端程序来登录到ZyWALL中。

1. 测试是否ZyWALL上已经启用了SSH服务。

在一个终端提示符下输入“telnet 192.168.1.1 22”，然后点击**[ENTER]**。计算机尝试连接到ZyWALL的端口22上（使用缺省的IP地址：192.168.1.1）随后会出现

一个ZyWALL的SSH的当前版本。

图161 SSH范例2: Test

```
$ telnet 192.168.1.1 22
Trying 192.168.1.1... Connected
to 192.168.1.1. Escape character
is '^]'. SSH-1.5-1.0.0
```

2. 输入“ssh -l 192.168.1.1”。这个命令会让您的计算机使用SSH（版本为v1）连接到ZyWALL中。如果这是您首次使用SSH连接ZyWALL的话，会出现一条信息，提醒您将ZyWALL的主机信息保存起来。输入“yes”，然后点击[ENTER]。输入密码即可登录到ZyWALL中。

图162 SSH范例2：登录

```
$ ssh -l 192.168.1.1
The authenticity of host '192.168.1.1 (192.168.1.1)' can't be established.
RSA1 key fingerprint is
21: 6c: 07: 25: 7e: f4: 75: 80: ec: af: bd: d4: 3d: 80: 53: d1.
Are you sure you want to continue connecting (yes/no)? yes Warning: Permanently
added '192.168.1.1' (RSA1) to the list of known hosts.
Administrator@192.168.1.1's password:
```

3. 随后会出现SMT的主界面。

18.10 使用 SSH 的安全 FTP 范例

本节向您介绍如何使用OpenSSH客户端程序来传输文件配置和连接步骤都类似于其它的SSH客户端程序。请参考SSH客户端程序的用户手册。

1 输入“`sftp -l 192.168.1.1`”。这个命令会让您的计算机使用SSH（版本为v1）连接到ZyWALL中。如果这是您首次使用SSH连接ZyWALL的话，会出现一条信息，提醒您将ZyWALL的主机信息保存起来。输入“yes”，然后点击[ENTER]。

2.输入密码即可登录到ZyWALL中。

3.使用“put”命令可以将新的固件上传到ZyWALL中。

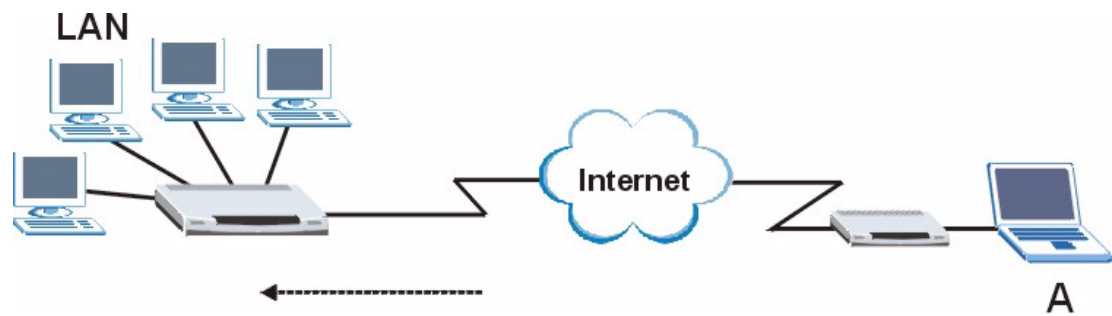
图 163 安全FTP：固件升级范例

```
$ sftp -l 192.168.1.1
Connecting to 192.168.1.1...
The authenticity of host '192.168.1.1 (192.168.1.1)' can't be established.
RSA1 key fingerprint is
21: 6c: 07: 25: 7e: f4: 75: 80: ec: af: bd: d4: 3d: 80: 53: d1.
Are you sure you want to continue connecting (yes/no)? yes Warning: Permanently
added '192.168.1.1' (RSA1) to the list of known hosts.
Administrator@192.168.1.1's password:
sftp> put firmware.bin ras
Uploading firmware.bin to /ras
Read from remote host 192.168.1.1: Connection reset by peer
Connection closed
$
```

18.11 Telnet

您可以将ZyWALL配制成如下图所示的Telnet管理方式。

图 164 在 TCP/IP 网络上 Telnet 的配置



18.12 配置 TELNET

先点击**高级，远程管理**，然后点击**TELNET**标签。可以显示以下界面。

注意：在你为安全连接配置SSH时，建议你屏蔽Telnet 和 FTP。

图 165 Telnet

The screenshot shows the ZyWall configuration interface for TELNET. The interface has tabs for WWW, SSH, TELNET, FTP, SNMP, DNS, and CNM. The TELNET tab is selected. The configuration fields include: 服务器端口 (Server Port) set to 23, 服务器访问接口 (Server Access Interface) set to All, and 可靠客户端的IP地址 (Trusted Client IP Address) with radio buttons for 全部 (All) and 已选取的 (Selected), and a text box for the IP address (0.0.0.0). A note at the bottom says: 注意：您可能还需要建立相关[防火墙](#)规则。 (Note: You may also need to establish related [firewall](#) rules.) There are buttons for 应用 (Apply) and 重置 (Reset).

以下为界面相关的描述。

表 108 Telnet

标识	描述
服务器端口	如果需要的话，您可以修改相应的服务端口号，但是您也需要使用相同的端口号的服务来进行远程管理。
服务器访问端口	选择一个接口，通过该口，计算机可以使用此服务接入到ZyWALL中来。
可靠客户端的IP地址	安全的客户端就是可信任的计算机，可以允许使用此服务接入到ZyWALL中来。 选择 全部 ，表示所有的计算机都可以使用此服务接入到ZyWALL中来。 选择 已选取的 ，只允许规定IP地址的计算机使用此服务接入到ZyWALL中来。
应用	点击 应用 ，可以保存设置并退出该界面。

重置	点击 重置 ，可以重新配置该界面。

18.13 配置 FTP

您可以使用FTP来上传和下载ZyWALL的韧体和配置文件，请参考韧体和配置文件维护一章寻求更多信息。如果想使用这个特征，您的计算机需要有一个FTP客户端。

如果想修改ZyWALL的FTP设置，先点击**高级 > 远程管理**，然后点击**FTP**标签。您会见到以下界面。

注意：在你为安全连接配置SSH时，建议你屏蔽Telnet 和 FTP。

图 166 FTP

远程管理

WWW

SSH

TELNET

FTP

SNMP

DNS

CNM

FTP

服务器端口

21

服务器访问接口

All

可靠客户端的IP地址

☒ 全部

☐ 已选取的

0

.

0

.

0

.

0

注意：您可能还需要建立相关[防火墙](#)规则。

应用

重置

以下为界面相关的描述。

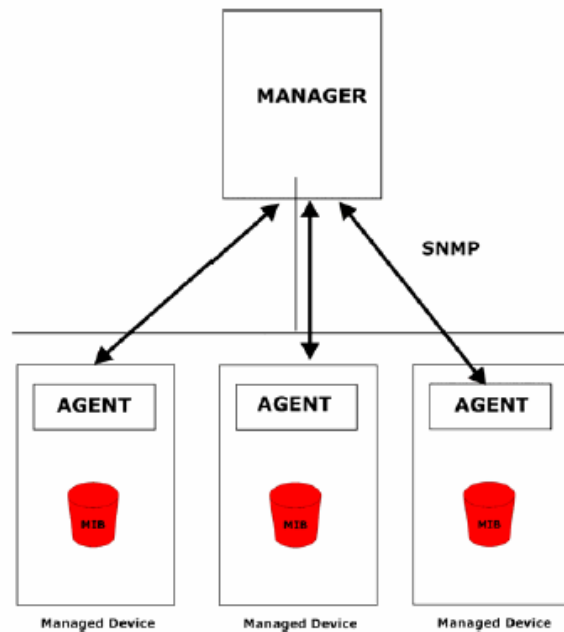
表 109 FTP

标识	描述
服务器端口	如果需要的话，您可以修改相应的服务端口号，但是您也需要使用相同的端口号的服务来进行远程管理。
服务器访问端口	选择一个接口，通过该口，计算机可以使用此服务接入到ZyWALL中来。
可靠客户端的IP地址	安全的客户端就是可信任的计算机，可以允许使用此服务接入到ZyWALL中来。 选择 全部 ，表示所有的计算机都可以使用此服务接入到ZyWALL中来。 选择 以选取的 ，只允许规定IP地址的计算机使用此服务接入到ZyWALL中来。
应用	点击 应用 ，可以保存设置，并退出该界面。
重置	点击 重置 ，可以重新配置该界面。

18.14 配置 SNMP

SNMP简单网络管理协议是一个应用层协议，用于管理和监控基于TCP/IP的设备。它经常用于在网络管理系统和被管理设备之间交换管理信息。ZyWALL 70支持SNMP的两个版本，SNMPv1和SNMPv2。下图举例描述一个SNMP的管理操作。假如TCP/IP被设定，SNMP就可以使用了。

图226 SNMP管理模型



一个 SNMP 网管系统是由 Agents 代理和 Manager 管理器两个主要部分组成的。

一个 Agent 是位于被管理设备（ZyWALL）中的管理软件模块。一个 agent 把当前的管理信息从被管理设备翻译成易于 SNMP 辨认并与之兼容的信息。管理器是网管执行网络管理功能的控制平台。它执行控制和监控管理系统的各项应用。

被管理设备包括目标变量和被管理对象，此二者定义了被收集的每一条关于系统的信息。例如变量包括被收到的数据包的数量，节点端口状态等。管理系统库（MIB）是一个管理对象的集合。SNMP 允许管理器和代理为了实现访问目标而进行通信。

SNMP 是一个基于管理/代理模块的简单请求/响应的协议。用以下协议操作管理器发出一个请求，代理反馈响应：

Get: 管理站读取代理者处对象的值。

Get下一步: 管理站用于扫描 MIB 树和检索数据。

Set: 管理站设置代理者处对象的值。

Trap: 代理者向管理站通报重要事件。

18.14.1 支持的 MIB

ZyWALL支持MIBII，在RFC-1213和RFC-1215中都有定义。MIB的重点在于让管理员收集统计数据，监控状态和性能。

18.14.2 SNMP陷阱

ZyWALL 在当一个事件发生的时候会发送陷阱信息给 SNMP 网管。所支持的 SNMP陷阱将在下面的表中做一略述。

表 110 SNMP 陷阱 (Trap)

陷阱#	陷阱名称	描述
0	coldStart (在 RFC-1215 中定义)	当 ZyWALL 重新加电的时候此 trap 送出。
1	WarmStart (在 RFC-1215 中定义)	当 ZyWALL 软件重启的时候此 trap 送出。
4	AuthenticationFailure (在 RFC-1215 中定义)	当接收到任何 community (密码) 设置错误的 SNMP get 或 set 信息的时候,此trap 送给管理员。
6	whyReboot (在 ZYXEL-MIB 中定义)	当系统准备重新启动(热启动)之前会发送重新启动原因的 trap 包。
6a	For intentional reboot	如果人为重新启动设备以后,一个带有“系统 reboot by 用户”信息的 trap 包发送出去。
6b	For fatal error	如果系统因为重大错误重新启动,一个带有重大错误码的信息就会发送出去。

18.14.3 远程管理: SNMP

如果想修改ZyWALL的SNMP设置,先点击**高级>远程管理**,然后点 击**SNMP**标签。您会见到以下界面。

图168 SNMP

远程管理

WWW

SSH

TELNET

FTP

SNMP

DNS

CNM

SNMP配置

执行Get的字串

public

执行Set的字串

public

Trap

群组

public

目的

0 . 0 . 0 . 0

SNMP

服务端口

161

存取服务

All

可靠客户端的IP地址

☒ 全部 ☐ 已选取的

0 . 0 . 0 . 0

注意：您可能还需要建立相关[防火墙](#)规则。

应用

重置

以下为界面相关的描述。

表111 SNMP

标识	描述
SNMP配置	
执行Get的字串	输入 执行Get的字串 值，它是进入管理工作站的 Get 和 Get 下一步 requests 的密码。缺省为 public ，允许所有的请求。
执行Set的字串	输入 执行Set的字串 值，它是由管理工作站输入的 Set requests 的密码。缺省为 public ，允许所有的请求。
Trap	
群组	输入 trap 群组的参数，它是随着发送到 SNMP 管理者的每一个 trap 信息的密码。缺省是 public ，允许所有的请求。
目的	输入可以将 SNMP trap 信息发送到的站点 IP 地址。
SNMP	
服务端口	如果需要的话，您可以修改相应的服务端口号，但是您也需要使用相同的端口号的服务来进行远程管理。
存取服务	选择一个接口，通过该口，计算机可以使用此服务接入到 ZyWALL 中来。
可靠客户端的IP地址	安全的客户端就是可信任的计算机，可以允许使用此服务接入到 ZyWALL 中来。 选择 全部 ，表示所有的计算机都可以使用此服务接入到 ZyWALL 中来。 选择 已选取的 ，只允许规定 IP 地址的计算机使用此服务接入到 ZyWALL 中来。

应用	点击 应用 ，可以保存设置，并退出该界面。
重置	点击 重置 ，可以重新配置该界面。

18.15 配置 DNS

您可以使用**DNS**进行域名到IP地址的解析。请参考109页第7章了解更多信息。 如果想修改ZyWALL的DNS设置，先点击**高级，远程管理**，然后点击**DNS**标签。您会见到以下界面。

图169 DNS

远程管理

WWWSSHTELNETFTPSNMP**DNS**CNM

DNS

服务端口53

存取服务All

可靠客户端的IP地址全部已选取的0.0.0.0

注意：您可能还需要建立相关[防火墙](#)规则。

应用重置

以下为界面相关的描述。

表112 DNS

标识	描述
服务端口	DNS的端口是53，您不能修改这里。
存取服务	选择一个接口，通过该口，计算机可以将DNS请求发送到ZyWALL中来。
可靠客户端的IP地址	安全的客户端就是可信任的计算机,可以允许向ZyWALL发送DNS请求。 择 全部 ，表示所有的计算机都可以向ZyWALL发送DNS请求。 选择已选取的，只允许规定IP地址的计算机向ZyWALL发送DNS请求。
应用	点击 应用 ，可以保存设置，并退出该界面。
重置	点击 重置 ，可以重新配置该界面。

18.16 介绍 Vantage CNM

Vantage CNM(集中网络管理)2.0可提供基于浏览器的全局管理解决方案，它可以 允许管理员从任何地方对处于各地的ZyXEL设备进行配置，管理，监控和排障。请查看 *Vantage CNM*用户手册了解更多信息。

如果您想让ZyWALL可以被Vantage CNM服务器管理，您就不能不通知Vantage CNM管理员而直接管理ZyWALL（通过web配置界面，SMT菜单或命令行模式）

18.17 配置 CNM

缺省情况下，ZyWALL不能通过Vantage CNM来管理。您可以在导航栏中先点击高级，远程管理，然后点击CNM标签。

图170 CNM

远程管理

WWWSSHTELNETFTPSNMPDNSCNM

注册信息

注册状态

未注册

上次注册时间

0000 - 00 - 00, 00 : 00 : 00

重新整理

Vantage CNM设置

☐ 启用

Vantage CNM服务器地址

0 . 0 . 0 . 0

加密法则

3DES

加密密钥

应用

重置

以下为界面相关的描述。

表113 CNM

标识	描述
注册信息	

注册状态	如果启用没有选择的时候，该只读区域显示未注册。 当ZyWALL首次连接Vantage CNM服务器的时候，这里会显示正在注册当ZyWALL在Vantage CNM服务器上注册成功的时候，这里会显示已注册。如果出现以下情况时，ZyWALL不会和Vantage CNM服务器成功注册： Vantage CNM服务器关闭。 Vantage CNM服务器的IP地址不正确。 Vantage CNM服务器在一台NAT路由器或防火墙后面，没有能够将数据发送到Vantage CNM服务器上。 ZyWALL和Vantage CNM服务器的加密算法和/或加密密钥不相符。
上次注册时间	此处显示ZyWALL上一次在Vantage CNM服务器上的注册时间。如果ZyWALL还没有和Vantage CNM服务器成功注册过，
	此处会显示全部时区。
重新整理	点击 重新整理 可以更新注册状态和上次注册时间。
Vantage CNM 设置	
启用	點選此框可以允许Vantage CNM管理ZyWALL。
Vantage CNM 服务器地址	如果Vantage CNM服务器和ZyXEL设备在同一个网段上，请输入Vantage CNM服务器的公网或私网IP地址。 如果Vantage CNM服务器和ZyXEL设备不在同一个网段上，请输入Vantage CNM服务器的公网IP地址。 如果Vantage CNM服务器和ZyXEL设备不在同一个网段上，并且在NAT路由器的后面，请输入NAT路由器的WAN口IP地址，并在NAT路由器上配置一个UDP 1864的端口映射到Vantage CNM服务器上。如果ZyWALL在一台防火墙的后面，您需要在防火墙上创建一条规则，允许UDP端口为1864的数据发送到Vantage CNM服务器（大部分（新的）的ZyXEL防火墙会自动允许这样做）
加密法则	请在 加密法则 区域中选择一个ZyWALL和Vantage CNM服务器之间传输的数据进行加密的加密算法。选项有 DES ， 3DES 或 None 。

加密密钥	当您选择 DES 加密算法的时候，请输入8个区分大小写的字符（“0”到“9”，“a”到“z”或“A”到“Z”），当您选择 3DES 加密算法的时候，请输入24个区分大小写的字符（“0”到“9”，“a”到“z”或“A”到“Z”）。ZyWALL需要和Vantage CNM服务器使用相同的加密密钥。
应用	点击 应用 ，可以将设置保存到ZyWALL中。
重置	点击 重置 ，可以重新修改该界面。

第 19 章 UPnP

本章将会向您介绍UPnP的特征。本章只有当ZyWALL处于路由模式的时候才有效。

19.1 通用即插即用功能介绍

UPnP是一种分布式的开放网络标准,它使用TCP/IP建立起设备之间的点到点的连接。借助UPnP技术,设备可以动态加入到网络中并获得IP地址、传达功能以及了解其它设备的存在和性能。此后,设备之间可以直接通讯,这又进一步地实现了对等网络功能。

19.1.1 我们如何知道正在使用 UPnP 功能呢？

UPnP硬件可以在网络连接文件夹（Windows XP）中以图标方式表示出来。您网络上的每一台支持UPnP的设备都会作为一个单独的图标。选择一个UPnP设备的图标,可以使您了解那台设备的接入信息和特性。

19.1.2 NAT 穿透

UPnP的NAT 穿透功能可以动态地允许一些应用穿过NAT。UPnP网络设备可以动态地配置网络地址,向其它UPnP设备宣告它们在网络上的存在,以及能够进行简单的产品和服务描述信息的交换。NAT 穿透允许以下操作:

- 动态端口映射
- 学习公网IP地址
- 给映射表分配租借时间

Windows Messenger就是支持NAT 穿透和UPnP的应用范例。请参考14章,了解NAT的更多信息。

19.1.3 使用 UPnP 的警告

利用NAT 穿透应用动态地建立它们自己的服务和操作防火墙端口的时候会留下 网络

安全的隐患。在一些网络环境下，网络信息和配置有可能会被用户获得并修改。

所有支持UPnP的设备可以不用额外的配置就可以自由地彼此通信。如果您不想这么做的话，就可以关闭UPnP的功能。

19.1.4 UPnP 和 ZyXEL

ZyXEL已经从UPnP Implementers Corporation获得了UPnP证书。ZyXEL采用的 UPnP支持IGD 1.0（Internet 网关 设备）的标准。ZyXEL的UPnP目前支持Windows Messenger 4.6和4.7，还会支持Windows Messenger 5.0和Xbox等应用。

UPnP广播只允许在LAN上实现。

19.2 配置 UPnP

点击UPnP可以见到以下界面。

图171 配置UPnP



以下为界面相关的描述。

表 114 UPnP

标识	描述
UpnP设置	
设备名称	在UPnP应用中用于标识ZyXEL设备。
启用UPnP功能（UPnP）	点选此框可以激活UPnP功能。您需要注意，启用该功能后，任何人不用输入ZyWALL的IP地址（但是您还需要输入密码才可以登录进来）就可以登录到web配置界面。

允许用户透过UPnp来更改设定	点选此框可以允许支持UPnP的应用自动配置ZyWALL，以便能够通过ZyWALL进行通信。例如，通过NAT 穿透 功能，UPnP应用能够自动保留一个NAT转发端口，用于和其它支持UPnP的设备通信，这样就可以不用人工配置干预。
允许UPnP通过防火墙	点选此框可以允许支持UPnP应用的数据传过防火墙。 不选此框，可以让防火墙阻止所有的UPnP应用数据包（例如：MSN数据包）。
应用	点击 应用 ，保存设置并退出。
重置	点击 重置 ，重新配置该界面。

19.3 浏览 UPnP 端口映射

先点击**UPnP**，然后点击**端口**就可以见到以下界面。您在此界面中可以浏览UPnP在ZyWALL中创建的NAT端口映射规则。

图172 UPnP端口



以下为界面相关的描述。

表115 UPnP端口

标识	描述
系统启动后，将UPnp的NAT规则保存在内存中	点选此框可以让ZyWALL在重新启动的时候保留UPnP创建的这些 NAT规则。如果您使用UPnP，并且在您的计算机上为一种特殊的服务（例如FTP文件发送）设置了一个端口。那么这个功能可以当 您的计算机使用UPnP为这个服务创建一个 NAT转发规则的时候，在ZyWALL上保留一个记录。
以下为只读信息，包括在ZyWALL的NAT路由表里面UPnP创建的NAT映射规则信息。	
#	这是UPnP创建的NAT映射规则表的目录索引号。
远程主机	此处为进入ZyWALL的IP数据包的源地址（WAN上）

外部端口	此处为ZyWALL侦听目标为NAT规则中 内部端口 和 内部客户端 的连接请求的端口号。
协议	此处为NAT映射规则（TCP或UDP）的协议。
内部端口	此处为ZyWALL将入站连接请求发送到 内部客户端 的端口号。
内部用户端	此处为LAN上的DNS主机名或IP地址。如果内部客户端中设置为255.255.255.255的UDP映射，那么多个NAT客户端就可以同时使用一个端口。
启用	此处显示UPnP创建的NAT映射规则是否激活。
描述	此处显示一个NAT映射规则的文本描述。
租用期间	此处显示一个动态的端口映射规则存活时间（以秒为单位）如果该端口映射是静态的，那么此处会显示“0”。
应用	点击 应用 ，保存设置并退出ZyWALL。
更新	点击 更新 ，可以刷新界面表项。

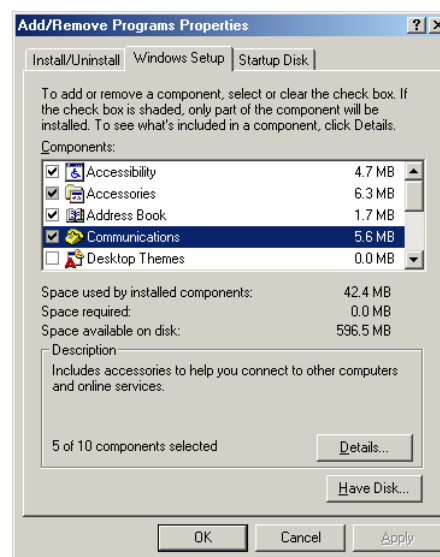
19.4 在 Windows 中安装 UPnP 范例

本节向您介绍如何在Windows Me和Windows XP中安装UPnP。

19.4.1 在 Windows Me 中安装

以下为是在Windows Me中安装UPnP的步骤。

1. 依次点击开始、设置和控制面板。双击添加/删除程序。
2. 点击**Windows设置**标签，在组件中选择通讯。点击详细信息。

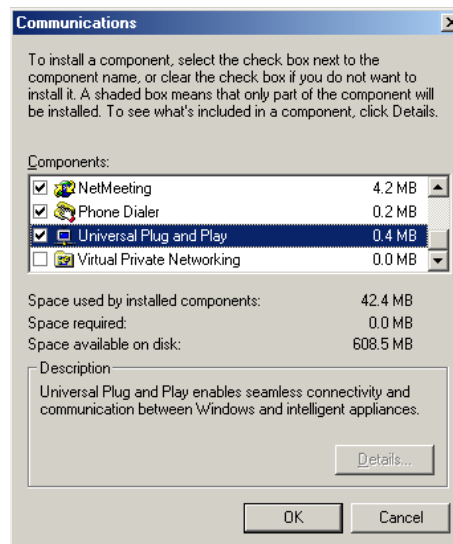


3 在 Communications

界面, 在**Components**选择框
中选择 **Universal Plug and
Play**。

4 点击**OK**回到添加/删
除程序窗口, 然后点击下一
步。

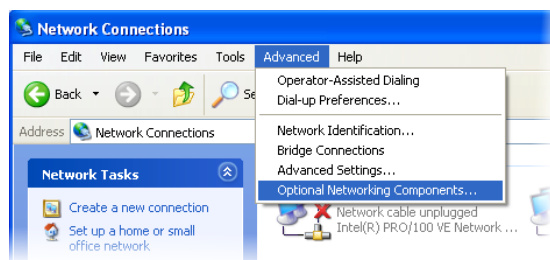
5当操作完毕, 重新启动计算机。



19.4.2 在 Windows XP 中安装 UPnP

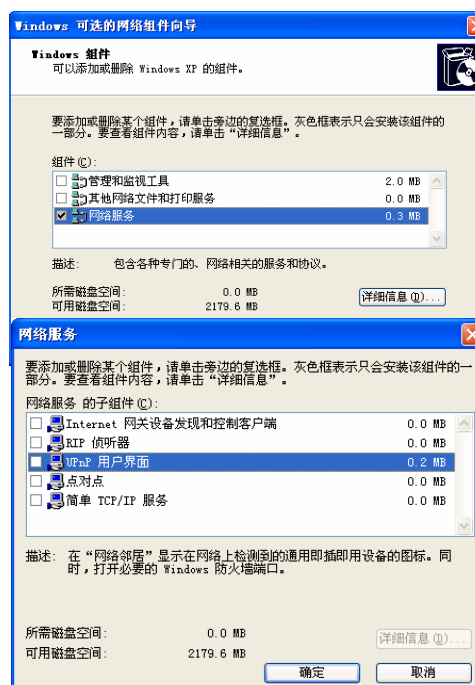
以下是在Windows XP中安装UPnP的步骤。

- 1 依次点击开始、设置和控制面板。
- 2 双击网络连接。
- 3 在网络连接窗口中点击高级按钮,
然后选择下拉出来的可选网络组件...。
随后**Windows**可选网络组件向导窗
口会出现。
- 4在组件中选择网络服务, 然后点击详
细信息。



- 5 在网络服务窗口中, 选择即插即用。

- 6 点击**OK**回到**Windows**可选网络组件
窗口, 然后点击**Next**。



19.5 在 Windows XP 中使用 UPnP 范例

本节将会向您介绍如何在Windows XP中使用UPnP的功能。您需要在Windows XP中已经安装了UPnP，并且在ZyXEL的设备上激活了UPnP的功能。

确保您的计算机能够连接到ZyXEL设备LAN口上。打开计算机和ZyXEL设备。

19.5.1 支持 UPnP 网络设备的自动发现

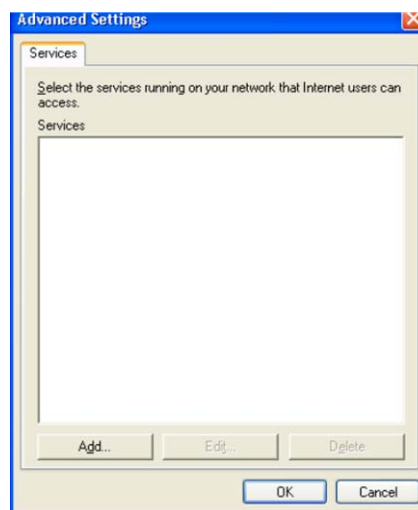
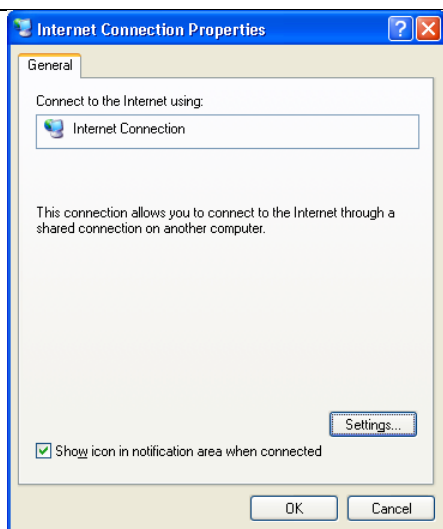
1 点击开始，设置和控制面板。双击网络连接。在Internet网关中会出现一个图标。用鼠标右键点击图标，选择属性。

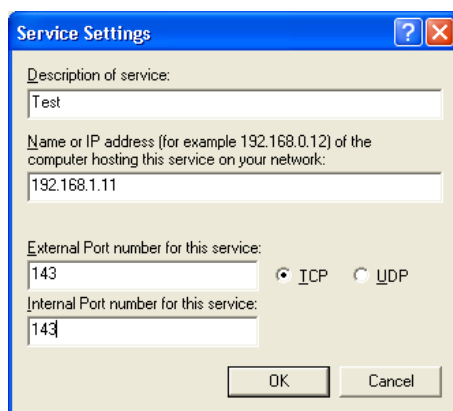
2 在Internet连接属性窗口，点击Setting，可以见到自动创建的端口映射项。

3 在 Internet Connection Properties窗口，点击Settings 查看自动创建的端口映射。



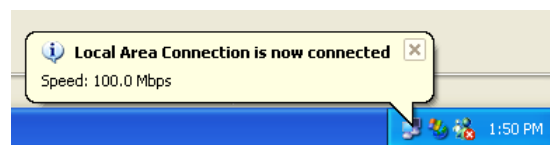
你可以编辑或删除端口映射，点击Add，手工加入端口映射。





注意：如果支持UPnP的设备从您的计算机上断开连接，所有的端口映射都会自动删除。

4 选择当连接的时候在提示区显示图标选框，然后点击**OK**。一个图标会在系统栏中显示出来。



5 双击此图标会出现Internet连接的当前状态。。

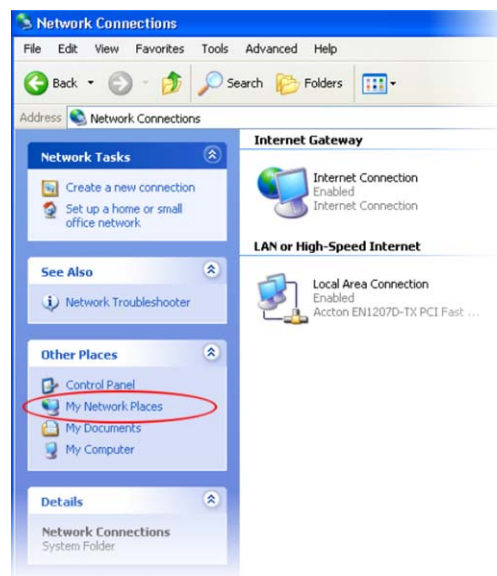


19.5.2 接入 web 配置界面

使用UPnP,您可以不用先找到ZyXEL设备的IP地址就可以接入到web浏览器当中。当您不知道ZyXEL设备IP地址的时候,这一点很有用。

下面介绍接入web配置界面的步骤。

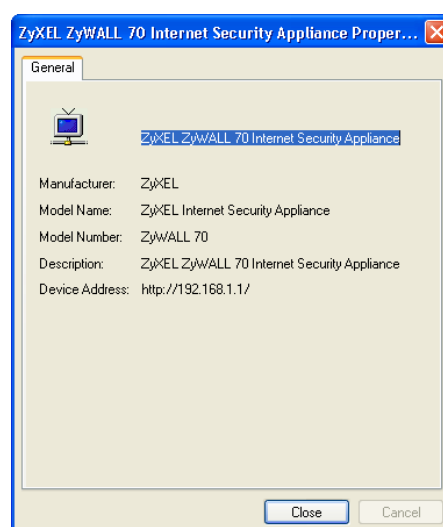
- 1 点击开始, 设置和控制面板。
- 2 双击网络连接。
- 3 在其它位置中选择我的网络位置。。



- 4在本地连接中会出现每一个支持UPnP的网络设备图标。
- 5 用鼠标右键点击ZyXEL设备, 然后选择调用。随后会出现登录界面。



6 用鼠标右键点击ZyXEL设备, 然后选择属性。随后会出现属性信息界面。



第 20 章 ALG 界面

本章将会向您介绍如何配置ZyWALL的ALG功能以允许某些应用能够穿越ZyWALL。

20.1 ALG 概述

ZyWALL可以作为一种应用层网关（ALG）以允许某些和NAT配合有问题的应用（例如SIP）顺利穿越NAT。

一些应用不能顺利穿越NAT，因为它们会将IP地址和端口号嵌入到这些数据包的数据载荷里。ZyWALL会检查数据流中的IP地址和端口信息。当ZyWALL后面的一台设备使用ZyWALL中启用ALG服务的一种应用的时候，ZyWALL会将该设备所传数据流中的私有IP地址转换为公网的IP地址。它也会同时记录下会话端口号，并动态创建隐含的NAT端口转发和防火墙规则以便可以让该应用可以从WAN再回到LAN。

20.1.1 ALG 和 NAT

ZyWALL会动态创建一条隐含的NAT会话，以便让该应用的数据可以从WAN再回到LAN。

ZyWALL上的ALG支持所有的NAT映射类型，包括**One to One**，**Many to One**，**Many to Many Overload**和**Many One to One**。

20.1.2 ALG 和防火墙

ZyWALL在创建一条临时的防火墙规则用于数据传输的时候，会让会话使用动态的端口来发送数据。ZyWALL会通过查验该应用数据包的数据负载来决定传输方向，并且防火墙只会允许该方向上的会话流通过。应用数据流穿越防火墙之后，防火墙规则会自动删除。

20.2 FTP

文件传输协议（FTP）是一种互联网文件传输服务，可以通过TCP/IP协议在互联网上

操作。一个运行FTP服务器的系统会接受从一个运行FTP客户端的系统发出的指令。该服务会允许用户向服务器发送指令来上传或下载文件。FTP ALG会允许目标端口为21的TCP数据包穿过去。如果FTP服务器在LAN上,并且允许客户可以从WAN上访问该服务器,您 还需要配置NAT端口转发和防火墙规则。

20.3 H.323

H.323是一种标准的电信会议协议集,可以提供音频,数据和视频会议服务。它允许客户端计算机之间通过一个包交换的网络来实现点对点和多点间的通信,但是它不提供可以保证的服务品质。

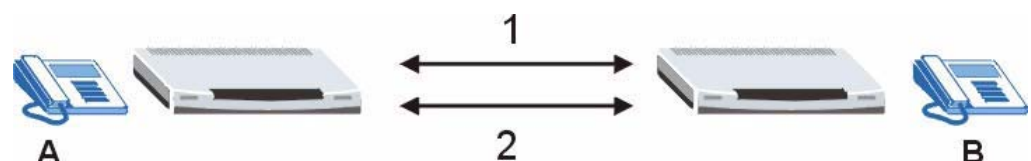
20.4 RTP

当您使用基于 H.323 或 SIP 的 VoIP 呼叫的时候, RTP (实时传输协议) 会处理语音数据传输。

20.4.1 H.323 ALG 细节

- H.323 ALG 支持点对点 (Peer-to-Peer) 的 H.323 呼叫。
- H.323 ALG 让 H.323 呼叫经过NAT或ZyWALL路由, 你也可以让其它H.323 呼叫不经过NAT或路由。例如在同一子网LAN IP地址间的呼叫。
- H.323 ALG 允许呼叫经NAT 出去, 例如, 你可以让呼叫从LAN中私有IP地址到一个WAN上的点设备。
- 你必须配置防火墙及端口转发, 允许从WAN进入的 (peer-to-peer) 呼叫到一个在LAN 的私有IP地址。 以下示例显示了在H.323设备间的 H.323信令及语音会话。图中, 标记1的箭头显示了一个TCP端口1720的会话, 标记2的箭头显示了一个使用RTP的语音会话。

图173 H.323 ALG示例



- H.323 ALG 在目的地址TCP端口1720上工作。
- ZyWALL 允许 H.323 语音连接。
- 对于经H.323 ALG 的数据流，ZyWALL也能进行带宽管理。

20.5 SIP

会话初始协议（SIP）是一种应用层控制（信令）协议，可以处理互联网上语音和多媒体会话的创建，报警和拆卸。SIP用于VoIP（Voice over IP）当中，可以实现在互联网上传送语音信号。

SIP信令和处理会话的媒体分离开来。媒体的会话交换过程中使用一条与信令不同的信道。SIP在处理语音呼叫的时候可以和传统的电路交换的电话网络结合在一起。

20.5.1 STUN

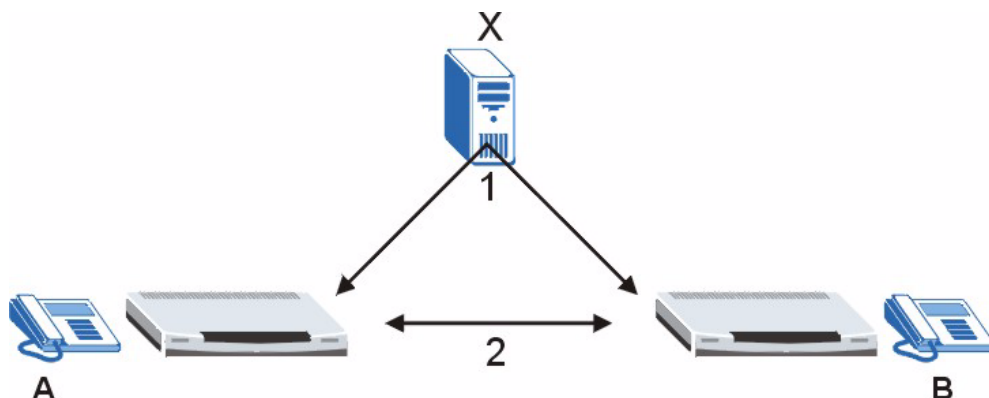
STUN（通过网络地址转换的用户数据报协议（UDP）简单穿越协议）允许VoIP设备发现在它和互联网之间的NAT路由器和/或防火墙的存在和类型。STUN也可以允许VoIP设备找到NAT分配的公网IP地址，所以VoIP设备可以将它嵌入到SIP数据流当中。如果您启用了SIP ALG，ZyWALL后面的设备就不需要使用STUN了。

20.5.2 SIP ALG 细节

- SIP 客户能连接到LAN，SIP 服务器必须在WAN上。
- 你可以在LAN 与WAN之间接受呼叫，但你不能在 LAN 与LAN 间接受呼叫。
- SIP ALG(会话初始协议应用层网关)允许目标端口为5060的 UDP数据包通过。
- ZyWALL 允许SIP 语音流连接。

下面的示例显示了SIP客户A与B、SIP服务器（X）之间的SIP信令及语音会话。在UDP端口5060的信令会话用标记1的箭头显示出，使用RTP的语音会话用标记2的箭头显示出。

图174 SIP ALG 示例



20.5.3 SIP 信令会话溢出时间

大多数SIP客户端都有一个代表信令会话寿命的“过期”机制SIP用户会向SIP服务器定期发送注册数据包，以保持ZyWALL里的会话活动。

如果SIP客户端没有这种机制，并且在ZyWALL的SIP时间溢出（缺省为60分）期间没有进行呼叫，ZyWALL SIP ALG就会在时间溢出以后断掉所有的进入呼叫。

20.5.4 SIP 语音会话溢出时间

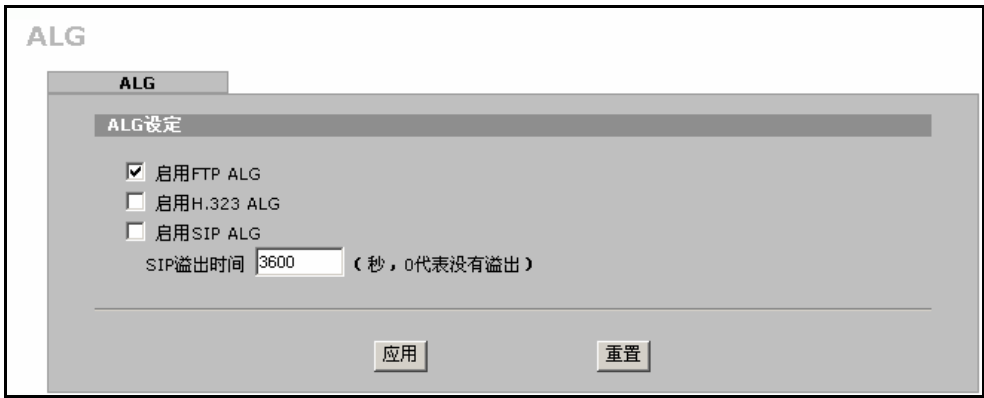
在溢出时间缺省为5分钟到期之后如果没有任何语音数据包穿越SIP ALG,SIP ALG不会阻挡呼叫信息，但是会阻挡所有语音数据包，并删除音频会话。您就不能听到任何声音，所以您需要再通过一个新的呼叫来延续您的会话。

20.6 ALG 界面

依次点击**高级**，**ALG**可以打开**ALG**界面。您可以在**ALG**界面中单独启用或关闭某个ALG组件，并设置SIP的溢出时间。

注意：如果ZyWALL为某种服务提供一个ALG，您必须要启用相应的ALG，以便能够对该服务的数据流执行带宽管理。

图 175 ALG



以下为界面相关的描述。

表116 ALG

标识	描述
启用FTP LG	选择次框可以允许FTP会话穿越ZyWALL。
启用H.323 ALG	选择次框可以允许H.323会话穿越ZyWALL。
启用SIP ALG	选择次框可以允许SIP会话穿越ZyWALL。
SIP溢出时间	以秒为单位输入一个SIP溢出时间值,缺省为60分钟。0代表没有溢出时间。
应用	点击 应用 可以保存设置。
重置	点击 重置 可以重新设置该界面。

第 21 章 日志界面

本章向您介绍如何配置通用的日志设置和查看ZyWALL的日志信息。

21.1 配置 View 日志

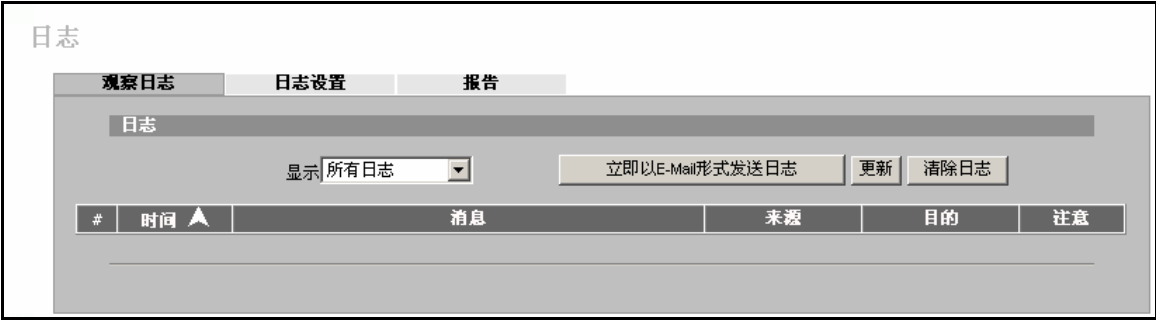
在web浏览器中，您可以在一个地方查看所有有关ZyWALL的日志信息。

点击**日志**，您可以打开**观察日志**界面。使用**观察日志**界面，您可以看到您在**日志设置**（查看章节21.3）界面中选定的日志信息相应类别的日志信息。这些选项包括关于系统维护，系统错误，接入控制，允许或阻止web页，阻止web特征（例如启用X控制，java 和cookie）攻击（例如DoS）和IPSec。

用红色标注出来的日志信息是系统错误日志。当日志满的时候，老的日志信息会被删除。

您点击一个列表头部可以对相应的条目进行排序。一个三角标志代表条目顺序的向上排列 或向下排列。

图 176 浏览日志信息



以下为界面相关的描述。

表 117 浏览日志信息

标识	描述
显示	从下拉菜单中您可以见到您在 日志设置 界面（参见章节21.3）中所选的条目。 您可以选择一个条目来查看相关的日志信息；您也可以选择 所有日志 来查看您在 日志设置 界面里选择的所有相关日志信息。
#	此处显示日志信息序号。

时间	此处显示日志信息记录的时间。请参考ZyWALL时间和日期的设置和配置一节。
消息	此处显示日志记录的原因。
来源	此处显示输入数据包的源IP地址和端口号列表。
目的	此处显示输入数据包的目的IP地址和端口号。
注意	此处显示有关日志输入的附加信息。
立即以E-Mail形式发送日志	点击 立即以E-Mail形式发送日志 ，您可以将此日志界面发送到您在 日志设置 界面中所设置的e-mail地址中。
更新	点击 更新 ，您可以刷新该日志界面。
清除日志	点击 清除日志 ，您可以删除所有的日志信息。

21.2 日志描述范例

下面是一条日志记录范例的描述。

```
#      .time                source                destination notes↵
      message↵
5|06/08/2004 05: 58: 20 |172.21.4.187: 137          |172.21.255.255: 137↵
|ACCESS BLOCK↵
      Firewall default policy:  UDP (W to W/ZW)↵
```

表 118 日志描述范例

标识	描述
#	这是第五条日志记录。
Time	生成时间为 2004 年 6 月 8 日，上午 5 点 58 分 20 秒。
Source	记录的是一条从 172.21.4.187 端口为 137 发出的 NetBIOS 数据包。
destination	该 NetBIOS 数据包会发送到 172.21.255.255 网络的 137 口上。这是一个 NetBIOS UDP 广播数据包，用于探测网络上的设备。
Notes	ZyWALL 阻挡住了该数据包。
Message	ZyWALL 根据防火墙的缺省规则（阻挡源自 WAN 上的会话）阻挡住了 该数据包。 “UDP”说明这是一个用户数据包协议。“W to W/ZW”代表该数据包从 WAN 发送到 WAN 或 ZyWALL。

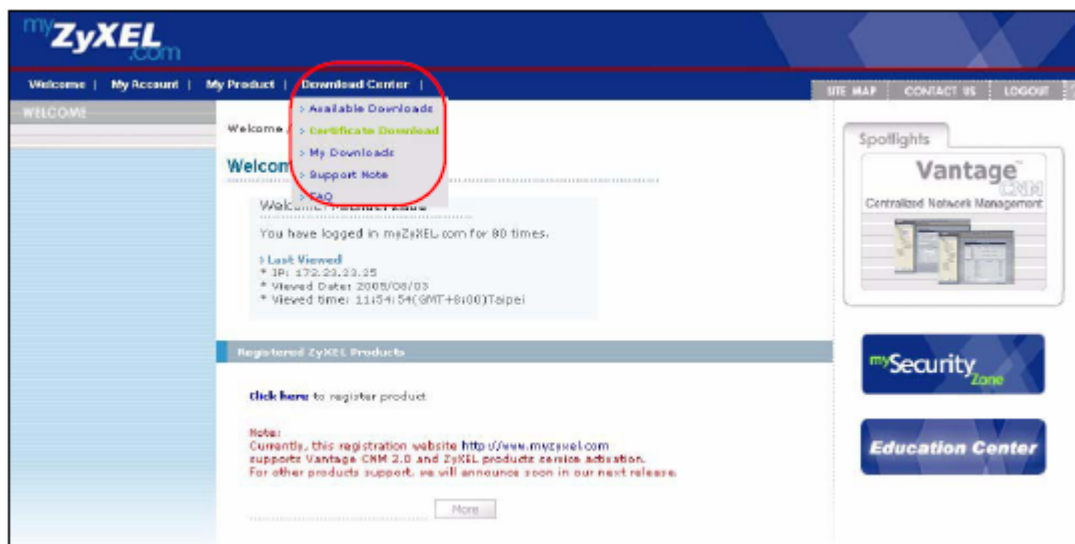
21.2.1 不可信证书记录

myZyXEL.com和更新服务器都使用 VeriSign 签署的证书来确认它们自己。如果 ZyWALL 没有一个通过可信任的CA VeriSign 签署的CA证书,那么ZyWALL就不会相信来自 myZyXEL.com和更新服务器的证书。ZyWALL每次与myZyXEL.com和更新服务器长时建立连接(HTTPS)的时候将产生一个日志,如"Due to error code(11), cert not 可信的: SSL/TLS peer certif...". 4.0版本缺省配置文件包含了一个由VeriSign签署的可信任的CA 证书。如果您升级ZyNOS4.0版的固件时,没有升级4.0版本的缺省配置文件,您可以通过 VeriSign从myZyXEL.com下载一个CA证书,并将其导入到ZyWALL 作为一个可信任的CA。这将使ZyWALL在试图与myZyXEL.com和更新服务器建立连接时不再产生该日志。

根据下列步骤从myZyXEL.com下载证书。

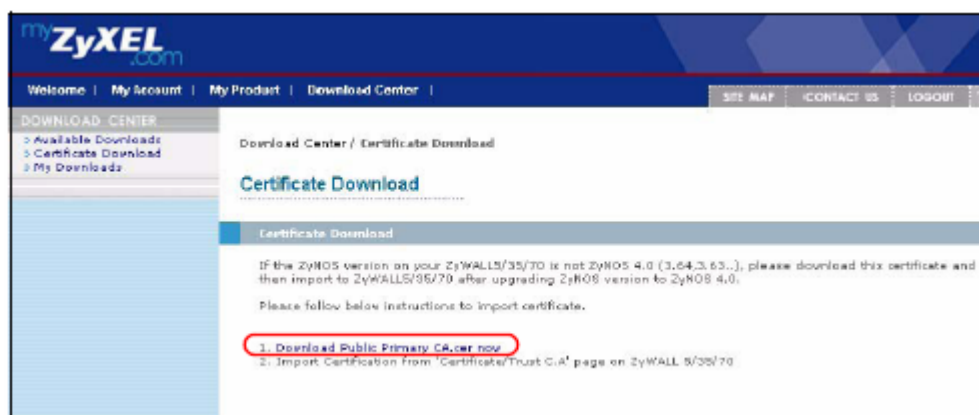
1. 用您自己的账户进入<http://www.myZyXEL.com>
2. 先点击**Download Center**, 然后点击**Certificate Download**。

图177 myZyXEL.com: 下载中心



3. 在 **Certificate Download** 界面中点击该链接。

图 178 myZyXEL.com: 证书下载



21.3 配置日志参数

如果您想修改日志设置的参数，可以点击**日志**，然后点击**日志设置**标签。随后会出现一个界面。

您可以使用**日志设置**界面来配置ZyWALL将日志信息发送到的地方；ZyWALL何时发送信息；发送哪些信息；以及是否直接发送该信息。

报警信息就是那些提请严重关注的日志信息类型。它们包括系统错误，攻击（接入控制）和尝试接入被阻止的web站点或具有被组织web特征（例如cookie，启用 X等）的web站点。有些条目，例如**System Errors**包括日志和报警。您可以在**观察日志**界面中通过颜色来区分它们。报警信息会以红色标识出来，而日志信息会以黑色来表示。

注意：当出现报警的时候，信息会及时通过e-mail发送出去。当日志信息满的时候（请参考日志调度一节），该信息也会通过e-mail发送出去。选择许多报警和/或日志条目（特别是接入控制）的结果是会发送出很多的e-mail信件。

图179 日志设置

日志

观察日志	日志设置	报告
电子邮件日志设定		
邮件服务器		(发送SMTP服务器名称或IP地址)
邮件主题		
邮件发送者		(E-Mail地址)
发送日志到		(电子邮件地址)
发送警告到		(电子邮件地址)
日志进度表	None v	
日志发送日	Sunday v	
日志发送时间	0 (小时) 0 (分钟)	
☐ SMTP认证 用户名 密码		
Syslog日志		
☐ 启用 Syslog服务器 0.0.0.0 (服务器名称或IP地址) 日志工具 Local 1 v		
启用日志和警示		
日志 ☒ 系统维护 ☒ 系统错误 ☒ 存取控制 ☐ 非对称路由 ☐ 组播/广播 ☐ TCP重置 ☐ 封包过滤器 ☒ ICMP ☒ 远程管理 ☒ 呼叫记录 ☒ PPP ☐ UPnP ☐ 已转发网站 ☒ 遭拦截网站 ☒ 遭拦截的Java等 ☒ 攻击 ☒ IPSec ☒ IKE ☒ PKI ☒ SSL/TLS		发送紧急警示 ☐ 系统错误 ☐ 存取控制 ☐ 遭拦截网站 ☐ 遭拦截的Java等 ☐ 攻击 ☐ IPSec ☐ IKE ☐ PKI
日志合并		
☒ 启用 日志合并周期 10 1 ~ 600 (秒)		
应用		重置

以下为界面相关的描述。

表119 日志设置

标识	描述
电子邮件日志设定	
邮件服务器	输入mail 服务器的服务器名称和IP地址。如果此处留空，日志信息和报警信息将不会通过e-mail送出。
邮件主题	给ZyWALL发送的e-mail添加一个标题。
邮件发送者	输入一个e-mail地址， 它会出现在ZyWALL发送的日志e-mail信息中的发送者一栏。如果您想激活SMTP认证的功能， 该e-mail地址也必须能够被mail服务器认证。
发送日志到	规定一个日志信息发送到的e-mail地址。如果此处留空，日志信息将不会通过e-mail送出。
日志告警到	规定一个报警信息发送到的e-mail地址。如果此处留空，报警信息将不会通过e-mail送出。
日志进度表	从下拉菜单中选择一个E-mail发送的时间频率： Daily Weekly Hourly When log is Full ⌘ None 如果您选择Weekly或Daily，需要规定一个E-mail发送出去的时间。如果您选择Weekly，需要规定一个E-mail发送出去的日期。 如果您选择When log is Full，日志记录满的时候报警信息就会发送出去。如果您选择None，不会发出任何信息。
日志发送日	使用下拉菜单选择日志信息发送的日期。
日志发送时间	输入日志信息发送的时间（24小时制，例如 23：00 代表晚上 11：00 点）
SMTP认证	SMTP(简单邮件传输协议)是一种在Internet上进行信息交换的标准。SMTP可以允许您将电子邮件从一个电子邮件服务器发送到其它的电子邮件服务器。 点选此框可以激活SMTP认证的功能如果邮件服务器需要认证，但是该功能被禁用了，您就不能接收到电子邮件日志记录。

用户名	输入用户名（最多 31 个字符）（一般是电子邮件账号的用户名）。
密码	输入相应的密码。
Syslog日志	Sys 日志 日志信息会发送到一个外部的 sys 日志 服务器中，用于存储该日志信息。
启用	点击 启用 可以启用该功能。
Syslog服务器	输入 syslog 服务器的服务器名称和 IP 地址。
日志工具	从下拉菜单列表中选择一个位置此功能可以允许您将日志信息存放在 syslog 服务器里面不同的文件中。请参考您的 sys 日志程序相关文档以了解更多信息。
启用日志和警示	
日志	选择您准备记录的日志类别项，也包括报警信息。
发送紧急警示	选择您准备让ZyWALL立即通过 e-mail 发送的报警信息类别项。 E-mail 地址信息就是您在 发送告警到 中定义的。
日志合并	
启用	一些日志（比如攻击日志）可能如此之多以致它会变得容易忽略其它的重要日志信息。选择该复选框将一些同样的日志合并成一个信息。您可以使用命令 syslog consolidate msglist 来查看有哪些日志记录会被合并。
日志合并周期	设置一个时间，规定ZyWALL将同类信息合并成一个信息的时间间隔。
应用	点击 应用 可以保存设置，并退出该界面。
重置	点击 重置 可以重新设置该界面。

21.4 配置报告信息

您可以在**报告**界面中看到**LAN**上的哪些计算机在收发大量的数据。局域网上的用户经常访问哪些网站或者哪些数据类型。使用**报告**界面，您可以让ZyWALL记录和展示以下的一些网络使用情况：

- 经常访问的**Web**站点
- 最常访问站点的访问次数
- 最常用的协议或服务端口
- 最常使用的协议和服务端口的数据量
- 哪些**LAN IP**地址在发送和接收大量的数据

在收发大量数据的LAN IP具有多大的吞吐量

注意：Web站点的点击数量也许不能100%准确，因为有时某些单独的web页在加载的时候，它可能会包括一些其它的站点的指向信息，而这些站点也会增加点击的数量。

ZyWALL是通过计算HTTP GET数据包来记录web站点的点击数量，许多web站点中包括指向其它站点的HTTP GET信息，那么ZyWALL也会记录这些数量，这样这些web站点的点击数量也许就不能100%准确了。

如果您想更改ZyWALL的报告记录，先点击**日志**，然后点击**报告**标签即可在里面 修改。界面如下图所示：

图 180 报告



注意：启用ZyWALL的报告功能会降低约1Mbps的吞吐量。

以下为界面相关的描述。

表 120 报告

标识	描述
收集统计资料	点选此框，然后点击 应用 可以让ZyWALL记录报告数据。
将未经处理的通信统计资料传送到 Syslog 服务器进行分析	点选此框，然后点击 应用 可以让ZyWALL将未处理的原始数据发送到一台syslog服务器进行分析。 您需要已经在 日志设置 界面中配置了syslog服务器。
应用	点击 应用 可以将参数保存到ZyWALL上。
重置	点击 重置 可以重新配置该界面。

报告类别	使用下拉菜单，您可以选择显示的报告类型。 Web Site Hits ，可以显示LAN用户最常访问的站点和访问次数。 Protocol/Port ，可以显示最常使用的协议和服务端口，以及相应的吞吐量。 Host IP Address ，可以显示具有最大吞吐量的IP地址，以及相应的吞吐量。
更新	点击 更新 可以更新记录。当您关闭并再次打开该界面的时候，报告信息会同样进行更新。
清空	点击 清空 可以丢弃老的报告数据，更新报告显示。

注意：当您关闭ZyWALL的时候，所有的报告信息会删除。

21.4.1 查看 Web 站点点击情况

在**报告**界面的**报告类别**下拉菜单中选择**Web Site Hits**，您可以了解LAN用户最常访问的站点和访问次数等信息。

图 181 Web站点点击报告范例



以下为界面相关的描述。

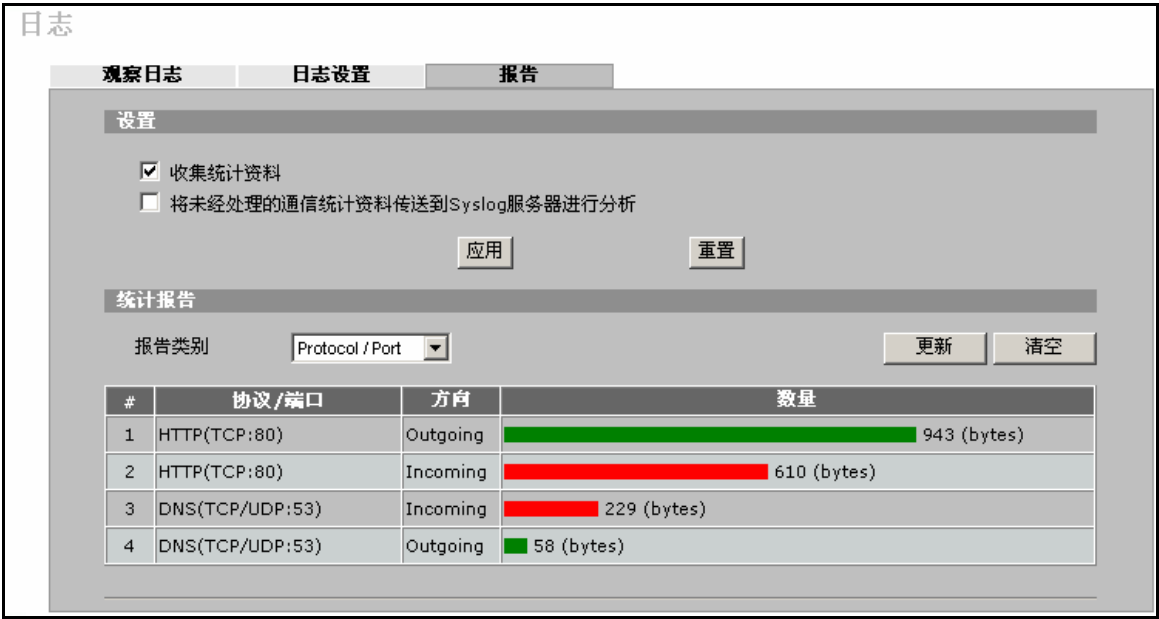
表 121 Web站点点击报告

标识	描述
网站站点	这些列表就是LAN用户访问量最多的Web站点。
命中	这些柱状列表是站点被访问的次数（请参考表124。

21.4.2 查看协议/端口

在报告界面中的报告类别下拉菜单中选择Protocol/Port，您可以了解最常使用的协议和服务端口，以及相应的吞吐量。

图 182 协议/端口报告范例



以下为界面相关的描述。

表 122 协议/端口报告范例

标识	描述
协议/端口	此列表出了在ZyWALL上具有最多应用的协议和服务端口。协议和服务端口以降序排列，使用最多的协议和服务端口最先列出。
方向	Incoming代表数据流是从WAN到LAN，WLAN或DMZ。 Outgoing代表数据流是从LAN，WLAN或DMZ到WAN。
数量	此列显示相应协议和服务端口的发送或接收的数据吞吐量。显示测量结果（bytes，Kbytes，Mbytes或Gbytes）随协议和服务端口的吞吐量变化。如果协议和服务端口通过的字节数在所设置计数限制内，显示为0 (参见349页表 124)。

21.4.3 查看 Host IP Address

在报告界面的报告类别下拉菜单中选择Host IP Address，您可以了解具有最大吞吐量的

IP地址，以及相应的吞吐量。

注意：如果计算机使用动态分配的IP地址，那么即使一个IP地址分配给了不同的计算机，ZyWALL也将继续记录从这个LAN IP地址上收发的数据包。

图 183 Host IP 地址报告示例



以下为界面相关的描述。

表 123 Host IP Address报告

标识	描述
IP地址	该列表显示已经有大量数据发送的LAN，DMZ或WLAN上的IP地址。LAN，DMZ或WLAN上的IP地址会根据相应接口上的数据流量而降序排列。
方向	Incoming代表数据流是从WAN到LAN，WLAN或DMZ。 Outgoing代表数据流是从LAN，WLAN或DMZ到WAN。
数量	此列显示相应协议和服务端口的发送或接收的数据吞吐量。显示测量结果（bytes，Kbytes，Mbytes或Gbytes）随协议和服务端口的吞吐量变化。如果协议和服务端口通过的字节数在所设置计数限制内，显示为0（参见349页表 124）。

21.4.4 报告规格

下表为报告特征的详细规格。

表124 报告规格

标识	描述

Number of web sites/protocols or Ports/IP Addresses listed:	20
Hit count limit:	每个Web站点最多计算次数为2的32次方次。如果超过40亿次，归零重新计算。
Bytes count limit:	每一个协议/端口或LAN IP地址的吞吐量最大为2的64次方bytes。如果超过2的64次方bytes，归零，重新计算。

第 22 章 维护

本章将会向您介绍维护界面上的相关信息。

22.1 维护介绍

您可在维护界面上查看系统信息，升级固件，管理配置文件和重启您的ZyWALL。

22.2 常规设置

22.2.1 常规设置和系统名称

常规设置包括管理存活时间和系统相关信息。**系统名称**只用于标识。但是，由于一些ISP需要检查您的名称，所以您需要输入计算机的计算机名称。

在Windows 95/98中，依次点击开始，设置，控制面板，网络。点击标识标签，注意在计算机名称中输入一个名称来作为系统名称。

在Windows 2000中，依次点击开始，设置，控制面板，然后双击系统。点击网络标识标签，然后点击属性按钮。注意在计算机名称中输入一个名称来作为系统名称。

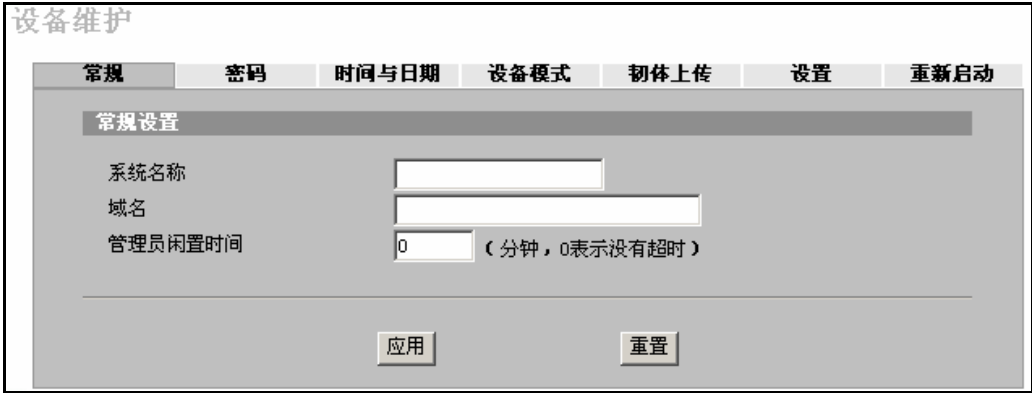
在Windows XP中，依次点击开始，我的电脑，浏览系统信息，然后点击计算机名称标签。注意在计算机名称中输入一个名称来作为系统名称。

22.2.2 常规设置

您在**域名**中输入的信息将会发送到LAN上的DHCP客户端处。如果您此处留空，域名会由DHCP从ISP处获得。但是您需要在每一台计算机上都输入主机名称（系统名称），域名可经由DHCP从ZyWALL获得。

点击**设备维护**，可以打开常规界面。

图 184 常规设置



以下为界面相关的描述。

表 125 常规设置

标识	描述
常规设置	
系统名称	输入一个标识名称。最多允许输入30个区分大小写的字符，不支持空格，但是支持连字符“-”和下划线“_”。
域名	输入一个域名（如果知道的话）
管理员闲置时间	输入一个时间值（以分钟为单位）。当您已经登录到管理界面中，但是在这个规定的时间之内没有任何操作的话，系统会终止您此次的管理任务。如果您想继续管理设备，可以重新通过登录界面，输入密码登录进去。数值“0”代表管理任务不会自动终止，即使您很长时间没有对设备进行操作也如此（不建议这样设置）
应用	点击 应用 ，可以保存设置。
重置	点击 重置 ，可以重新配置该界面。

22.3 配置密码

如果想修改ZyWALL的密码（强烈建议）您可以先点击**设备维护**，然后点击**密码**标签，可以见到以下界面。在该界面中，您可以修改ZyWALL的密码。

图 185 密码设置



以下为界面相关的描述。

表 126 密码设置

标识	描述
旧密码	输入缺省密码或现在您能使用的密码。
新密码	输入新密码（最多30个字符）密码会以（*）号显示出来。
重新输入以便确认密码	再次输入新密码，进行确认。
应用	点击 应用 ，保存设置。
重置	点击 重置 ，重新设置该界面。

22.4 时间和日期

在您开启ZyWALL时，有相应的软件机制，可以从外部服务器取得当前的日期和时间，手工设置当前的时间。

如果您想修改ZyWALL的时间和日期，请点击设备维护，然后点击Time andDate标签。以下为设置界面。请使用您当地的时区来配置ZyWALL的时间。

图 186 时间和日期

设备维护

常规

密码

时间和日期

设备模式

固件上传

设置

重新启动

当前时间和日期

当前时间

06:35 GMT

当前日期

2000-01-01

时间和日期设置

☐ 手动设置

新时间（时：分：秒）

6

:

35

:

35

新日期（年-月-日）

2000

-

1

-

1

☒ 从时间服务器取得

时间协议

NTP (RFC-1305)

时间服务器地址

a.ntp.alphazed.net

立即同步

*可选项。预先确定的NTP时间服务器列表

时区设置

时区

(GMT) 格林威治标准时间：都柏林，爱丁堡，伦敦，里斯本

☐ 启动夏时制时间

开始日期

第一

:

周日

:

的

:

一月

:

(2000-01-02)

:

在

:

0

:

点

结束日期

第一

:

周日

:

的

:

一月

:

(2000-01-02)

:

在

:

0

:

点

应用

重置

以下为界面相关的描述。

表 127 时间和日期

标识	描述
当前时间和日期	
当前时间	此处显示ZyWALL的当前时间。
当前日期	此处显示ZyWALL的当前日期。
	每次加载该页面的时候，ZyWALL都会和时间服务器同步日期。
时间和日期设置	
手动设置	点选此按钮，您可以手工输入时间和日期。
新时间（时：分：秒）	当您在时间和日期设置中选择手动设置的时候,您可在此处输入新的时间，然后点击应用。
新日期（年-月-日）	当您在时间和日期设置中选择手动设置的时候,您可在此处输入新的日期，然后点击应用。

从时间服务器取得	点选此按钮，ZyWALL可以从您规定的时间服务器上得到时间和日期。
时间协议	请选择时间服务器所采用的时间服务协议。并不是所有的时间服务器支持所有的时间服务协议，所以您需要设置与时间服务器相匹配的时间服务协议。 它们之间的主要区别是： Daytime（RFC 867） 时间形式为day/month/year/time。 Time（RFC 868） 格式为4字节整数，提供从1970/1/1 0: 0: 0开始的全部秒数。 缺省为NTP（RFC 1305）类似于Time（RFC 868）
时间服务器地址	输入时间服务器的URL和IP地址。
立即同步	点击此按钮，ZyWALL可以从前面所规定的时间服务器（查看 时间服务器地址 区域）上得到时间和日期。这样也同时会保存您的设置（包括时间服务器的地址）
时区设置	
时区	选择您当地的时区。
启用夏时制时间	夏时制时间是一个时间阶段，从晚春到早秋。许多国家会在这一阶段将时间提早一小时，以便让人们在傍晚得到更多的日光。 如果您使用这种功能，请选择该项。
开始日期	如果您选择 启用夏时制时间 ，输入一个起始日期。
结束日期	如果您选择 启用夏时制时间 ，输入一个终止日期。
应用	点击 应用 ，保存设置。
重置	点击 重置 ，可以重新配置该界面。

22.5 预定义 NTP 时间服务器列表

当您首次启动 ZyWALL 的时候，日期和时间从 2000-01-01 00: 00: 00 开始。如果您不想规定一个时间服务器，或者不能和您规定的时间服务器同步的时候，ZyWALL 可以使用预定义的 NTP 时间服务器。

注意：ZyWALL 可以不管您在**时间协议**中的设置而采用这个预定义的时间服务器列表。

当ZyWALL 使用这个预定义的 NTP 时间服务器列表的时候，它会随机选择一个服

务器来进行时间同步。如果同步失败，ZyWALL 会继续尝试使用其它的服务器来进行时间同步。ZyWALL 会一直进行尝试连接同步，直到所有的服务器都试过来为止。

表 128 缺省的时间服务器

ntp1.cs.wisc.edu
ntp1.gbg.netnod.se
ntp2.cs.wisc.edu
tock.usno.navy.mil
ntp3.cs.wisc.edu
ntp.cs.strath.ac.uk
ntp1.sp.se
time1.stupi.se
tick.stdtime.gov.tw
tock.stdtime.gov.tw
time.stdtime.gov.tw

22.5.1 复位时间

在以下情况下，ZyWALL 的时间会复位：

当您点击**立即同步**的时候。

在您保存配置的时候。

当 ZyWALL 启动的时候。

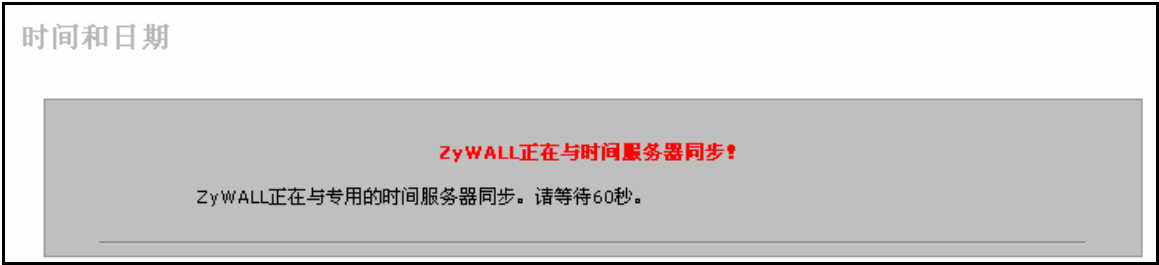
启动后的 24 间隔。

22.5.2 时间服务器同步

点击**立即同步**按钮，ZyWALL 可以从预定义的时间服务器或您在**时间服务器地址**区域中规定的时间服务器获得时间。

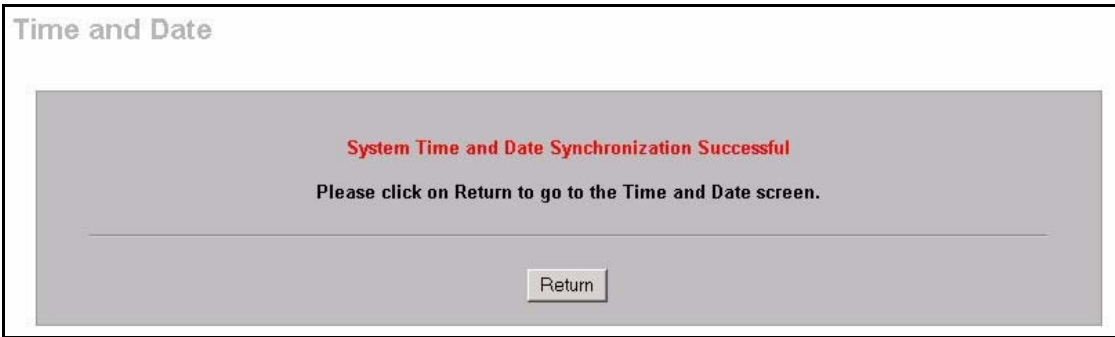
如果出现 **ZyWALL正在与时间服务器同步**界面的时候，请等待一分钟左右的时间。

图 187 同步进程



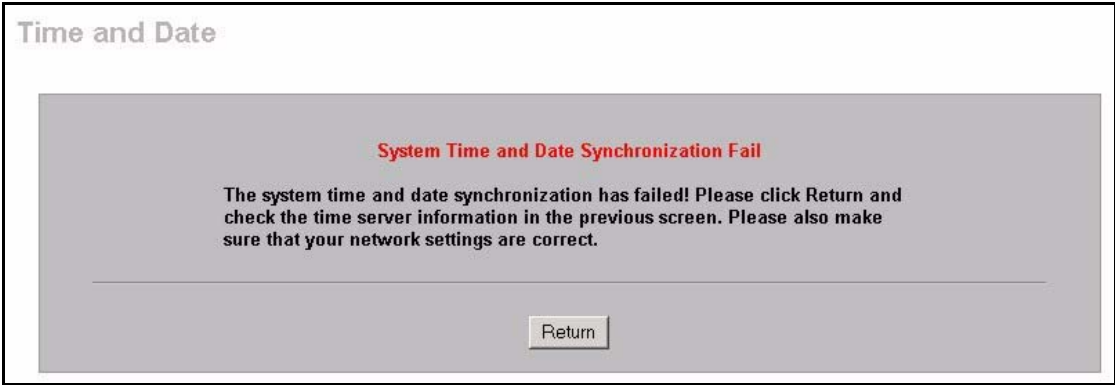
当时间和日期成功更新以后，您可以点击**返回**按钮回到**时间和日期**界面。

图 188 同步成功



如果更新没有成功，您会见到以下界面。点击**返回**可以回到**时间和日期**界面。

图 189 同步失败



22.6 透明网桥介绍

透明网桥对网络的操作来说是无形的，因为它不会修改所转发的数据帧。网桥会检查 在某端口导入数据帧的源地址，以学习和该端口相关的**MAC**地址。到该 **MAC**地址的所有未 来通信将只被发送到那个端口。

网桥将逐渐建立一个主机**MAC**地址到端口的映射表，例如以下的范

例。.

表 129 MAC地址到端口的映射表

主机MAC	端口
00a0c5123456	3
00a0c5123478	1
00a0c512349a	3
00a0c51234bc	2
00a0c51234de	4

例如，如果网桥通过端口1收到来自主机A（MAC地址为00a0c5123478）的一个数据帧，网桥会把主机A和端口1结合起来。如果网桥从某一个端口上再收到目的地址为00a0c5123478的数据帧的时候，它会通过检查内部表直接将数据帧发送到端口1。当网桥通过内部数据表检查一个导入数据帧的目的地址以后，它会采取以下动作中的一个：.

- 如果该表包含了一条目的地址和网桥中任意一个除了接收该数据帧的端口以外的端口的联系，那么该数据帧就会通过与之相联系的端口转发出去。
- 如果不存在相关的联系，该数据帧会泛洪到除了入端口以外的其它所有端口。广播和组播均是这种形式的泛洪方式。
- 如果相联系的端口就是入端口本身，那么该数据帧就会被丢弃掉（过滤）

22.7 透明防火墙

透明防火墙（也被称为透明，内置，隐蔽，秘密的或网桥式的防火墙）有如下的优点：

1. 因为不需要更改您现有的网络配置（主机，邻接路由器和防火墙自身），所以网桥式防火墙会减少您的配置和部署时间。
2. 由于它处理较少的负载，所以性能会有所提升。
3. 透明网桥不修改它转发的数据帧，对攻击者来说是无形的，但它可以提供一种有效的“秘密行动”。

如果需要在复杂的环境中快速配置一台新的防火墙，网桥设备是最有用的。透明的网桥防火墙也是具有多家分支机构型公司的首选，因为一般在这些机构里网络的设置常常是类似的。您可以在总部配置这些网桥防火墙，然后再将它们分发到各分支机构直接安装，而不需要其它的配置。

22.8 配置设备模式（路由模式）

如果您想将 ZyWALL 配制成路由或网桥模式，可以先点击**维护**，然后点击**设备模式**标签。当 ZyWALL 处于路由模式的时候，您会见到以下界面。

图 190 设备模式（路由模式）

系统维护

常规

密码

时间与日期

设备模式

固件上传

设置

重新启动

使用中设备模式

设备模式

路由模式

设备模式设置

ZyWALL将在您变更设备模式并按下应用后自动重新启动。

☒ 路由模式

IP地址

(请参阅 [LAN](#)和[WAN](#))

☐ 透明模式

IP地址

IP子网掩码

网关IP地址：

0

0

0

0

.

0

0

0

0

.

0

0

0

0

.

0

0

0

0

0

0

0

0

.

0

0

0

0

.

0

0

0

0

.

0

0

0

0

0

0

0

0

.

0

0

0

0

.

0

0

0

0

.

0

0

0

0

应用

重置

以下为界面相关的描述。.

表 130 设备模式（路由模式）

标识	描述
使用中设备模式	
设备模式	此处显示 ZyWALL 处于路由模式，还是出于网桥模式。
设备模式设置	
路由模式	如果您选择此按钮，可以将 ZyWALL 设置为路由模式。
IP地址	点击 LAN 、 WAN 或 DMZ ，您可以进入 LAN 、 WAN 、 WLAN 或 DMZ 界面查看和/或修改相关的设置。
透明模式	如果您选择此按钮，然后点击 应用 可以将 ZyWALL设置为网桥模式。
IP地址	输入 ZyWALL 的管理 IP 地址。
IP子网掩码	输入 ZyWALL 的 IP 子网掩码。
网关IP地址	输入网关的 IP 地址。

314

应用	点击 应用 ，可以保存设置。如果您修改了 ZyWALL 的管理 IP 地址，点击 应用 以后，请等待一会儿，然后再使用您修改的IP地址访问 ZyWALL。
重置	点击 重置 ，可以重新设置该界面。

22.9 配置设备模式（网桥模式）

如果您想将 ZyWALL 配制成路由或网桥模式，可以先点击**维护**，然后点击**设备模式**标签。当 ZyWALL 处于网桥模式的时候，您会见到以下界面。.

表 191 设备模式（网桥模式）

系统维护

常规

密码

时间与日期

设备模式

固件上传

设置

重新启动

使用中设备模式

设备模式透明模式

设备模式设置

ZyWALL将在您变更设备模式并按下应用后自动重新启动。

☐ 路由模式

LAN接口IP地址192 . 168 . 1 . 1

LAN界面子网掩码255 . 255 . 255 . 0

☒ DHCP服务器

IP地址池起始地址192 . 168 . 1 . 33

地址池大小128

☒ 透明模式

IP地址（请参阅 [网桥](#)）

应用

重置

以下为界面相关的描述。

表 131 设备模式（网桥模式）

标识	描述
使用中设备模式	
设备模式	此处显示 ZyWALL 处于路由模式，还是处于网桥模式。
设备模式设置	
路由模式	如果您选择此按钮，然后点击 应用 可以将 ZyWALL 设置为路由模式。
LAN接口IP地址	输入 ZyWALL LAN 口的 IP 地址，缺省值为 192.168.1.1。
LAN界面子网掩码	输入 ZyWALL LAN 口的 IP子网掩码。

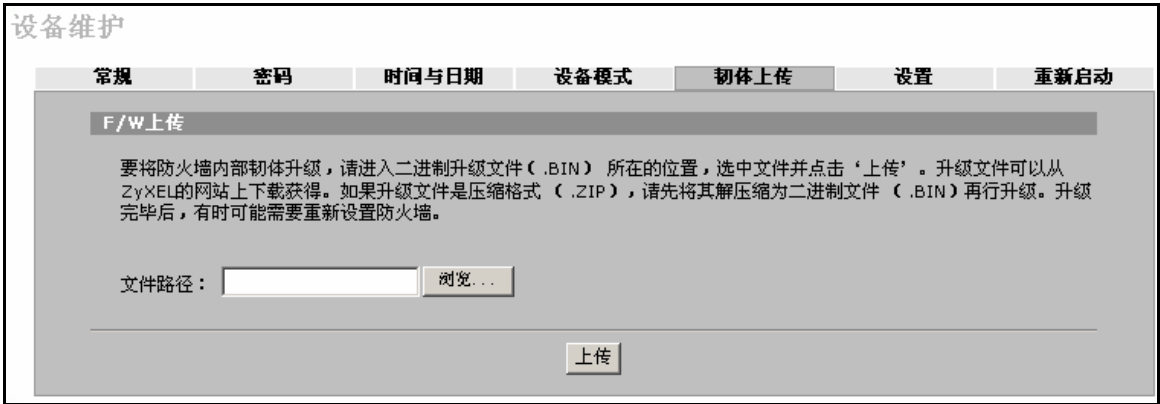
DHCP服务器	点选此框，您可以将 ZyWALL 设置成 DHCP 服务器，给DHCP客户端分配 TCP/IP 配置信息。如果您不选此框，需要在网络上 再提供一台 DHCP 服务器或者手工设置客户端计算机的TCP/IP信息。
IP地址池起始地址	规定一个 IP 地址池的起始 IP 地址。
地址池大小	设置一个 IP 地址池的 IP 地址数量。
透明模式	如果您选择此按钮，可以将 ZyWALL 设置为网桥模式。
IP地址	点击 网桥 ，进入 网桥 界面，然后您可以查看或者修改ZyWALL的管理 IP 地址。
应用	点击 应用 ，可以保存设置。如果您修改了 ZyWALL 的管理 IP 地址，点击 应用 以后，请等待一会儿，然后再使用您修改的IP地址访问 ZyWALL。
重置	点击 重置 ，可以重新设置该界面。

22.10 韧体升级界面

您可从www.zyxel.com上获得最新的韧体(又称“韧体”)，一般会以“.bin”作为扩展名，例如“zywall.bin”。使用HTTP（超文本传输协议）来升级韧体，大约需要2分钟。成功 升级之后，系统会重新启动。请参考升级韧体和配置文件一节，了解怎样使用FTP/TFTP 指令来升级韧体。

先点击**设备维护**，然后点击**韧体上传**标签。您可按照以下步骤来升级ZyWALL的韧体。

图 192 韧体上传



以下为界面相关的描述。

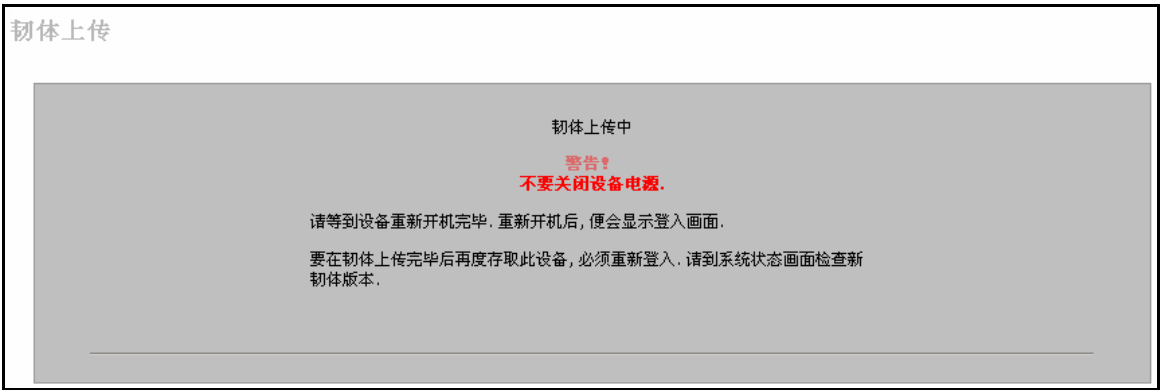
表 132 韧体升级

标识	描述
文件路径	您可在此输入文件存放的路径，或点击 浏览 来找到文件。
浏览	点击 浏览 ，您可以找到需要升级的文件。需要注意的是，升级文件必须是解压缩文件。
上传	点击 上传 ，您可以开始升级过程。这个过程需要近2分钟。

注意：在升级的时候不要关闭电源！

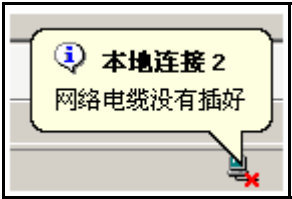
当您见到**韧体上传**中界面的时候，您需要等待2分钟再登录设备。

图 193 韧体升级过程



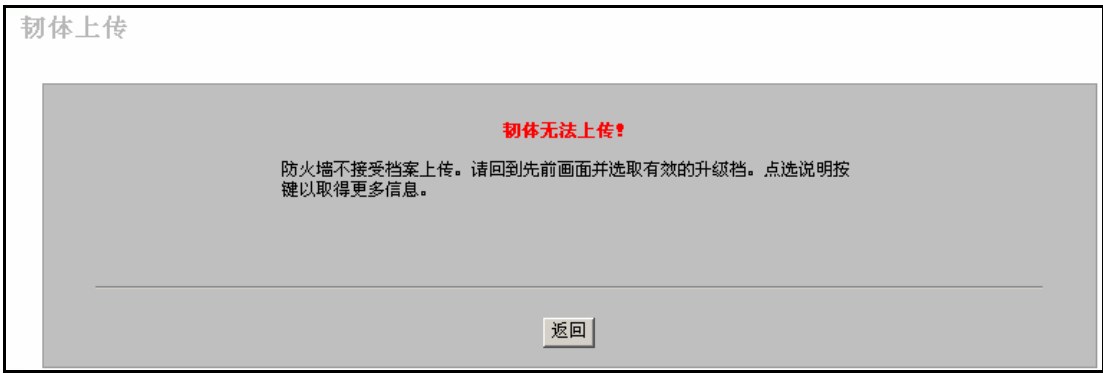
设备重新启动的时候会有一段时间的网络断开现象。在一些操作系统中，您会见到以下提示信息。

图 194 网络的暂时中断



2分钟之后，您又可以登录进去。您可以在**首页**界面中查看新韧体的版本。如果没有升级成功，会出现以下界面。点击**返回**，可以回到**韧体上传**界面。

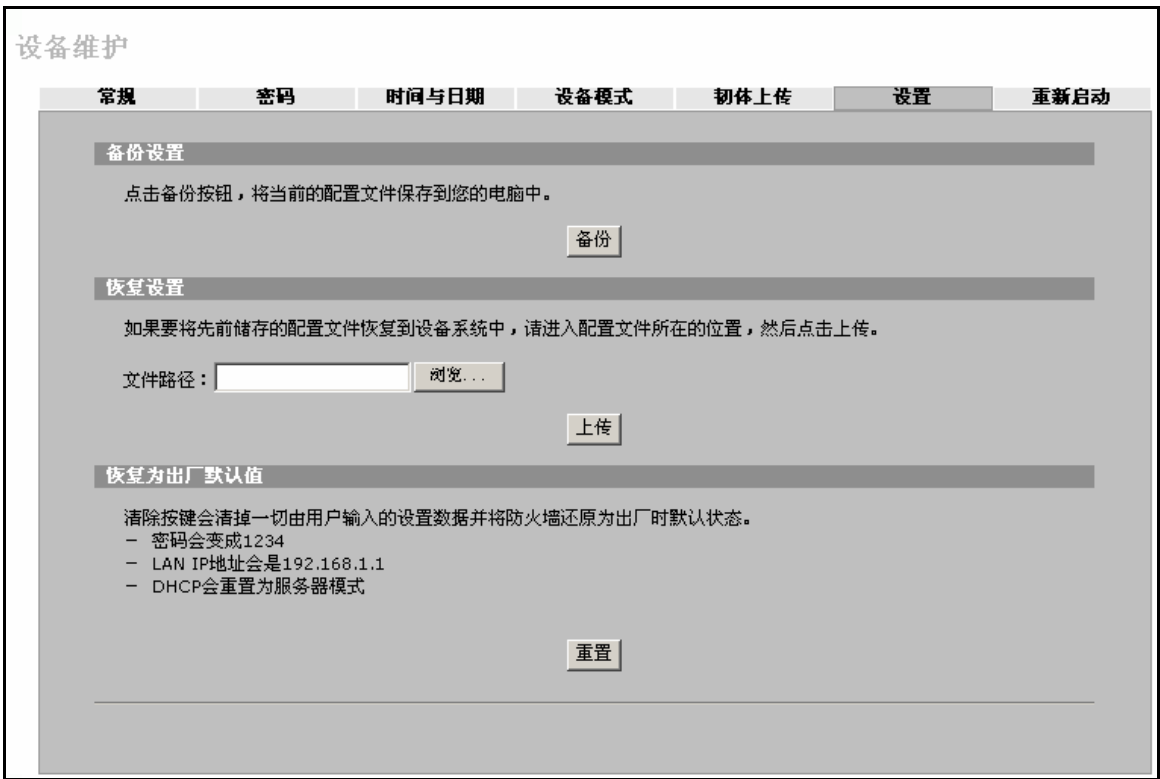
图195 韧体升级失败



22.11 备份和恢复

请参考章节35.5，您可以使用FTP/TFTP指令来传送配置文件。先点击**设备维护**，然后点击设置标签。您会见到以下界面。

图 196 备份和恢复



22.11.1 备份配置文件

备份配置文件的功能可以让您将ZyWALL当前的配置信息备份到计算机上。一旦您的ZyWALL经过配置后工作正常了，希望您能备份一下它的配置。一旦您需要将ZyWALL恢复到

以前的设置，那么这个配置文件就非常有用。

点击**备份**，可以将ZyWALL当前的配置文件保存到您的计算机上。

22.11.2 配置文件的恢复

您可利用此功能将以前保存到计算机里的配置文件重新加载到ZyWALL中，使其恢复到以前的配置。

表 133 配置文件的恢复

标识	描述
文件路径	您可在此输入文件存放的路径，或点击 浏览 来找到文件。
浏览...	点击 浏览... ，您可以找到需要恢复的配置文件。需要注意的是，配置文件必须是解压缩文件。
上传	点击 上传 ，您可以开始配置文件的恢复工作。

注意：在配置文件上传的时候不要关闭电源！

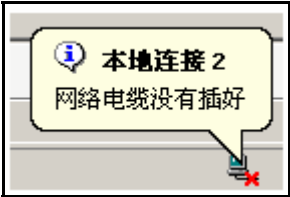
当您见到**设备还原完毕**界面的时候，您需要等待1分钟再登录设备。。

图197 配置文件恢复成功



设备重新启动的时候会有一段时间的网络断开现象。在一些操作系统中，您会见到以下提示信息。

图 198 网络的暂时中断

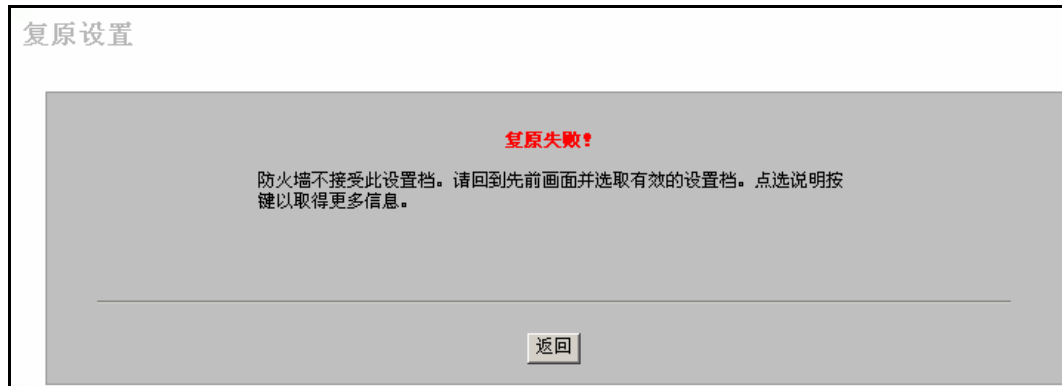


如果您恢复的是出厂缺省设置，那么ZyWALL当前的LAN口IP地址是

192.168.1.1。如果您以前设置的时候修改过此值，就需要将计算机的IP地址设置成和ZyWALL LAN口同一网段的IP地址才可以互通。请参考快速安装手册，您可以知道如何设置计算机的IP地址。

如果配置文件没有成功恢复，您就会见到以下界面。点击**返回**，您可以回到**设置**界面。

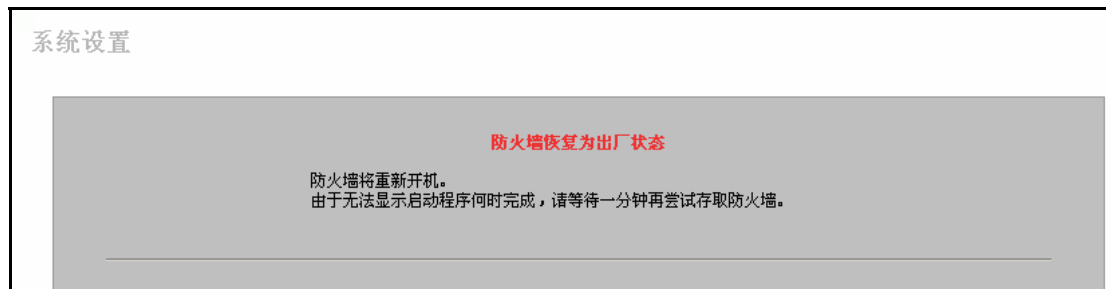
图 199 配置文件恢复失败



22.11.3 恢复设备的出厂缺省参数

点击**重置**按钮，您可以将ZyWALL恢复到出厂缺省设置，并见到以下界面。

图 200 重置警告信息

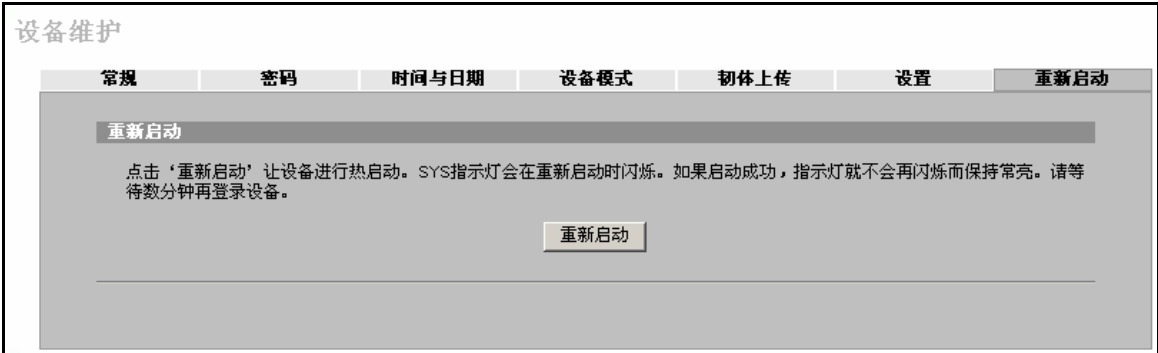


您也可以通过按动ZyWALL后面板上的**重置**键来将ZyWALL恢复到出厂缺省设置。

22.12 重新启动界面

系统重启动功能可以允许您在不关掉ZyWALL电源的情况下也可以重新启动该设备。您先点击**设备维护**，然后点击**Restart**。然后您再点击**Restart**按钮来重新启动ZyWALL。这样做不会影响ZyWALL的配置。

图201 重启动界面



第 23 章 SMT 介绍

本章将向您介绍如何进入系统管理终端（SMT），并了解其菜单的相关内容。

23.1 SMT 介绍

ZyWALL的SMT（系统管理终端）是一个菜单控制界面，您能通过控制口或远程连接从终端仿真器来访问。本章将会向您介绍如何通过控制口来访问SMT（系统管理终端）菜单，如何操纵SMT和如何配置SMT菜单。

23.2 通过控制口访问 SMT

请确信您已经按照快速设置手册上的描述正确地建立了物理连接。当利用控制口来配置时，您需要有一台装有通信软件的计算机，配置参数如下：

VT100终端仿真程序软件

速率9600

无奇偶校验位，8个数据位，1个停止位，流控制设置为无

23.2.1 初始界面

当您启动ZyWALL的时候，它会执行几个内部的测试以完成线路初始化。测试完毕后，ZyWALL会要求您按回车键继续，如下所示：

图 202 初始化界面

```
Copyright (c) 1994 - 2006 ZyXEL Communications Corp.↵

initialize ch =0, ethernet address: 00: A0: C5: 01: 23: 45↵
initialize ch =1, ethernet address: 00: A0: C5: 01: 23: 46↵
AUX port init . done↵
Modem init . inactive↵

Press ENTER to continue...↵
```

23.2.2 输入密码

在您按回车键之后会出现登录界面，提示您输入密码，如下所示。

如果您首次登录，请输入默认密码“1234”。当您输入密码时，界面对您输入的每个字符都会显示一个“X”。

请注意如果在您登录后超过5分钟没有任何动作 ZyWALL会自动退出并显示一个空白的界面。如果您看到空白界面，请按回车键重新登录。

图 203 密码界面

```
Enter Password : XXXX↵
```

23.3 SMT 界面导航

SMT是一个您用来配置ZyWALL的界面。您在试图修改配置之前应该熟悉几个操作，如下表。

表134 主菜单命令

操作	按键	描述
进入其它菜单	[ENTER]	转到子菜单，输入需要的子菜单的数值，然后按[ENTER].
返回上一级菜单	[ESC]	按[ESC]键返回上一级菜单
进入隐藏的“菜单”	按 [SPACE BAR] 将No改变为Yes，然后按[ENTER]	该处默认设置为No，菜单被隐藏了。按空格键使其变为Yes，然后按回车键进入“隐藏”的菜单。

移动指针	[ENTER]或[UP]/ [DOWN]箭头键	在一个菜单里，按[ENTER]键移动到下一处。您也能分别利用向上或向下的箭头键，移动到上一区域或下一区域。当您看到已经在菜单的最上区域时，按向上箭头会移到菜单的最下端。
输入信息	填写或者按 [SPACE BAR] ， 然后 按 [ENTER]从选项中进行选择	在该处您需要通过两种方式填写。第一种是直接输入适当的信息。第二种允许您通过按空格键来循环选择可用的项目。
必需的区域	<? >	为了保存新的配置，所有带有符号<?>的地方必须填写。
N/A区域	<N/A>	在SMT的一些地方会显示一个<N/A>。这个符号表示这里引用了一个不被应用的选项。
保存您的配置	[ENTER]	当看到提示信息“Press ENTER to confirm or ESC to cancel”时按回车键来保存您的配置。请确保您在每个界面里都保存了设置。
退出SMT	输入 99 ， 然后 按 [ENTER]	在主菜单的提示下输入99，然后按回车键，即可退出SMT界面。

23.3.1 主菜单

您输入密码后，SMT会显示**ZyWALL Main Menu**，如下所示。

图 204 主菜单（路由模式）

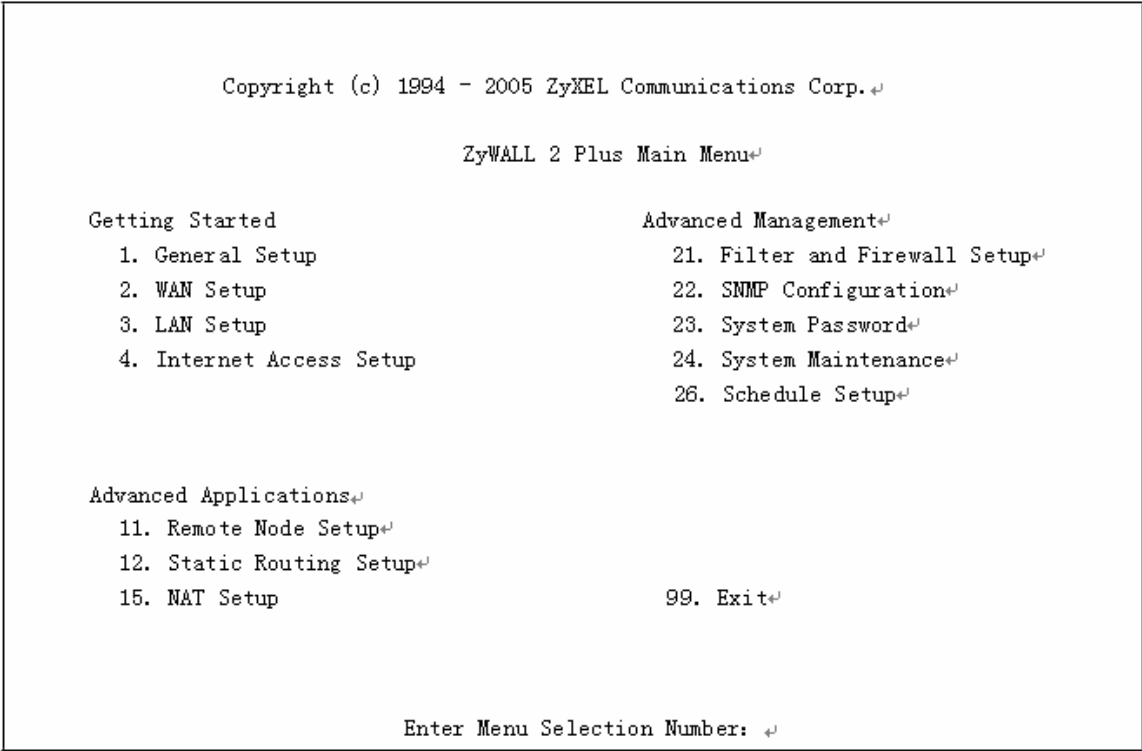
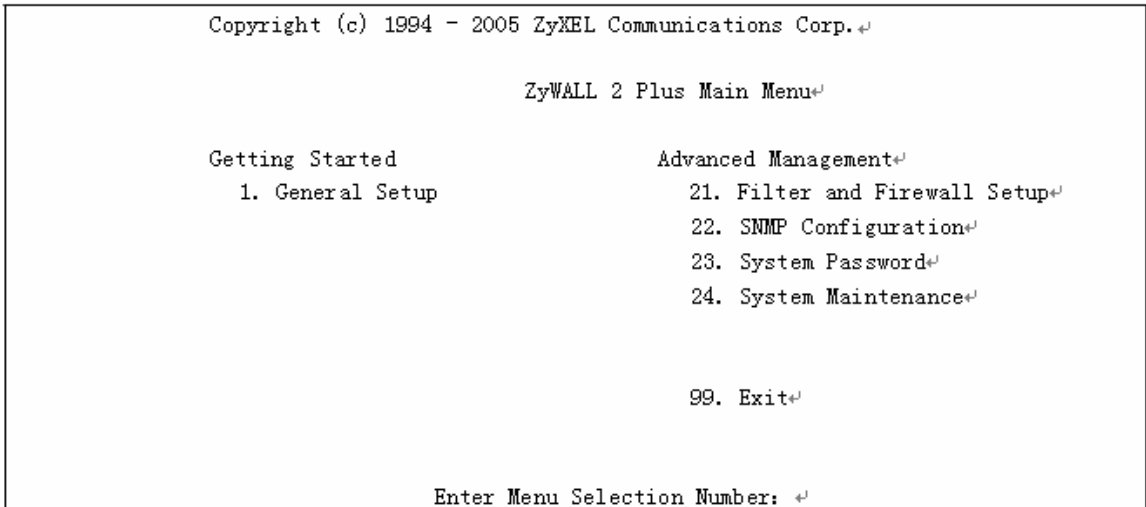


图 205 主菜单（网桥模式）



下表为界面相关的描述。

表 135 主菜单概述

号码	菜单名称	功能
1	General Setup	用该菜单设置设备模式，动态DNS和管理信息。

2	WAN Setup	用该菜单从您局域网的一台计算机复制一个MAC地址,还可以设置一个WAN口备份拨号连接。
3	LAN Setup	利用这个菜单应用LAN过滤规则, 配置LAN口的DHCP和TCP/IP参数。
4	Internet Access Setup	用该菜单配置您的网络访问设置(互联网地址, 网关, 登录参数等等)
11	Remote Node Setup	利用该菜单配置详细的远程节点设置(您的ISP也是一个远程节点) 还可以应用WAN口过滤规则。
12	Static Routing Setup	该菜单配置IP静态路由。
15	NAT Setup	利用该菜单配置网络地址转换。
21	Filter and Firewall Setup	配置过滤规则, 启用或不启用防火墙。
22	SNMP Configuration	利用该菜单配置SNMP相关的参数。
23	System Password	在该菜单中修改ZyWALL的密码(推荐)
24	System Maintenance	从显示系统状况到上传固件, 该菜单提供了全面的系统维护功能。
26	Schedule Setup	利用该菜单来确定向外呼叫的时间计划。
99	Exit	利用该菜单退出(远程设置所必需的)

23.3.2 SMT 菜单总览

下表是ZyWALL各类菜单的总览。

表 136 SMT菜单总览

菜单	子菜单		
1 General Setup	1.1 Configure Dynamic DNS	1.1.1 DDNS Host Summary	1.1.1 DDNS Edit Host
2 WAN Setup	2.1 Advanced WAN Setup		
3 LAN Setup	3.1 LAN Port Filter Setup		
	3.2 TCP/IP and DHCP Ethernet Setup	3.2.1 IP Alias Setup	

4 Internet Access Setup			
11 Remote Node Setup	11.1 Remote Node Profile	11.1.2 Remote Node Network Layer Options	
		11.1.4 Remote Node Filter	
		11.1.5 Traffic Redirect Setup	
	11.2 Remote Node Profile (Backup ISP)	11.2.1 Remote Node PPP Options	
		11.2.2 Remote Node Network Layer Options	
		11.2.3 Remote Node Script	
		11.2.4 Remote Node Filter	
12 Static Routing Setup	12.1 Edit Static Route Setup		
15 NAT Setup	15.1 Address Mapping Sets	15.1.x Address Mapping Rules	15.1.x.x Address Mapping Rule
	15.2 NAT Server Sets	15.2.x NAT Server Setup	15.2.x.x - NAT Server Configuration
	15.3 Trigger Ports	15.3.x Trigger Port Setup	
21 Filter and Firewall Setup	21.1 Filter Configuration	21.1.x Filter Rules Summary	21.1.x.x Generic Filter Rule
			21.1.x.x TCP/IP Filter Rule
	21.2 Firewall Setup		
23 System Password			
24 System Maintenance	24.1 System Status		
	24.2 System Information	24.2.1 System Information	

	and Console Port Speed	24.2.2 Console Port Speed	
	24.3 Log and Trace	24.3.1 View Error Log	
		24.3.2 Syslog Logging	
		24.3.4 Call-Triggering Packet	
	24.4 Diagnostic		
	24.5 Backup Configuration		
	24.6 Restore Configuration		
	24.7 Upload Firmware	24.7.1 Upload System Firmware	
		24.7.2 Upload System Configuration File	
	24.8 Command Interpreter Mode		
	24.9 Call Control	24.9.1 Budget Management	
		24.9.2 Call History	
	24.10 Time and Date Setting		
	24.11 Remote Management Setup		
26 Schedule Setup	26.1 Schedule Set Setup		

23.4 更改系统密码

您可以通过以下的步骤来改变系统密码。

1. 在主菜单中输入23，进入Menu23 – System Password。

图 206 Menu 23: 系统密码

```
Menu 23 - System Password␣  
  
Old Password= ? New  
Password= ?␣  
Retype to confirm= ?␣  
  
Enter here to CONFIRM or ESC to CANCEL: ␣
```

2. 输入您现有的密码，然后按回车键。
3. 输入新的系统密码，然后按回车键。
4. 再输入一遍新的系统密码以确认，然后按回车键。 注意当您输入密码时，界面会对您输入的每个字符都显示“x”。

23.5 重置 ZyWALL

关于重新设置ZyWALL,请参见2.3章节。

第 24 章 SMT 菜单 1-常规设置

Menu 1 – General Setup包含管理和系统相关信息。

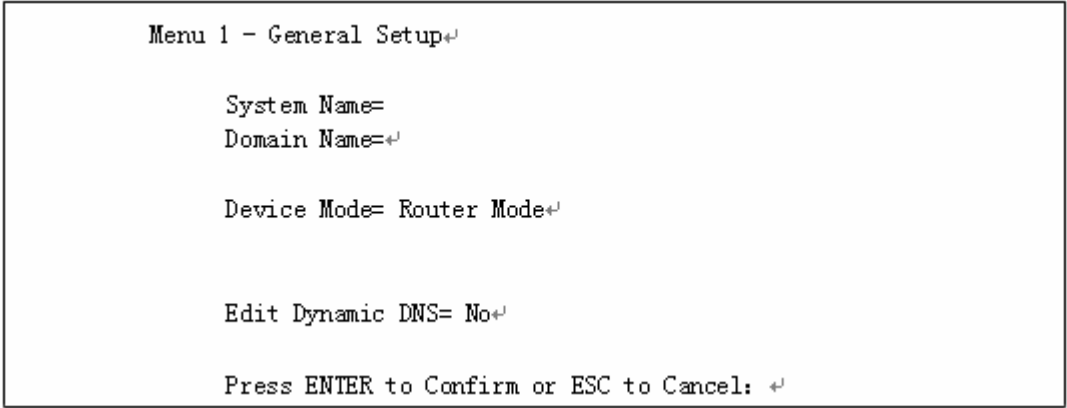
24.1 常规设置的介绍

Menu 1 – General Setup包含管理和系统相关信息。

24.2 配置常规设置

1. 在主菜单输入1，进入**Menu 1 – General Setup**。
2. 显示**Menu 1 – General Setup**界面，如下图所示。填写必需的区域。

图 207 Menu 1: 常规设置（路由模式）

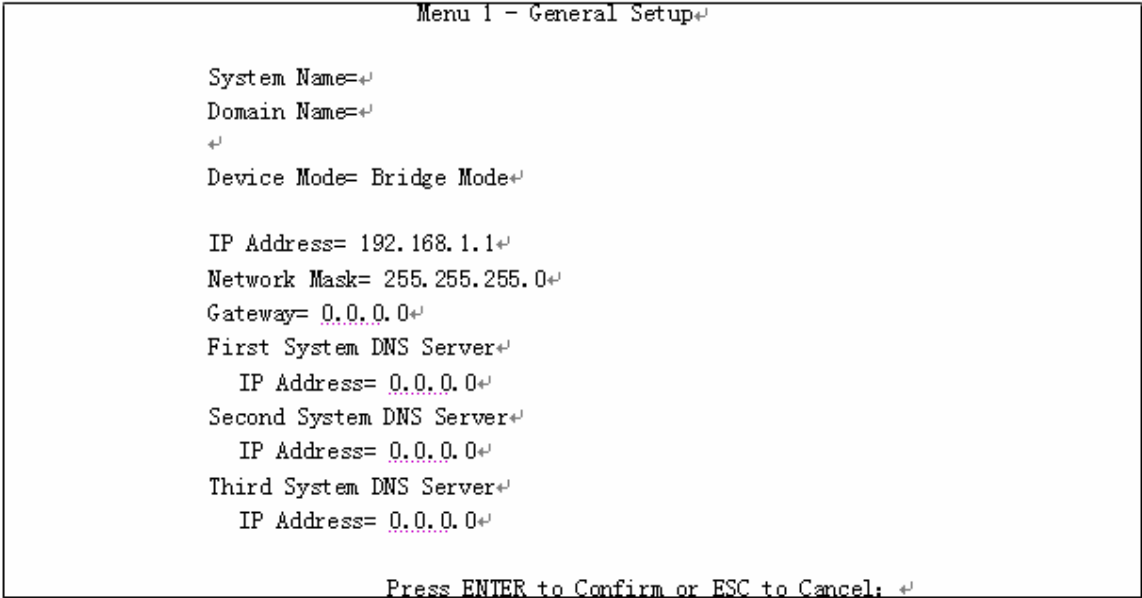


以下为界面相关的描述。

表 137 Menu1：常规设置（路由模式）

区域	描述
System Name	设置一个名称，仅用于标识。推荐输入您的计算机名。该名称最多可以输入30个数字或文字的字符，不能有空格，允许有下划线和虚线。
Domain Name	在这里输入域名（如果您知道的话）如果您留空的话，ISP可以通过DHCP为您指派一个域名。您可以进入菜单24.8，并输入“sys domain name”通过路由器来查看当前域名。优先输入ISP分配的域名，如果您想清除该处，只要按一下空格键，然后再按回车键即可。
Device Mode	按一下空格键，然后再按回车键选择Route Mode。
Edit Dynamic DNS	按一下空格键，然后再按回车键选择Yes或No（默认值）选择Yes来配置Menu 1.1: Configure Dynamic DNS。
当您已经完成了这个菜单，看到“Press ENTER to Confirm...”的提示后按回车键，保存您的配置，或者按“ESC”键在任何时候都可以取消。	

图 208 菜单 1： 常规设置（网桥模式）



以下为界面相关的描述。（参见表137）.

表138 菜单 1： 常规设置（网桥模式）

区域	描述
Device Mode	按一下空格键，然后再按回车键选择网桥模式。
IP Address	输入IP地址。
Network Mask	输入子网掩码。
Gateway	输入网关IP地址。
First System DNS Server Second System DNS Server Third System DNS Server	如果您有DNS服务器的IP地址，请在 IP Address 处输入该地址。

24.2.1 配置动态 DNS

如果想要配置动态DNS，请首先在Menu 1或者在**MAINTENANCE Device Mode**界面 中将ZyWALL设置为路由模式。选择**Menu 1-General Setup**，然后在**Edit Dynamic DNS** 处按下空格键选择**Yes**。按回车键显示**Menu 1.1-Configure Dynamic DNS**（显示如下）.

图 209 菜单 1.1： 配置动态DNS

Menu 1.1 - Configure Dynamic DNS↵

Service Provider= WWW.DynDNS.ORG Active=

No↵

Username=↵

Password= ***** Edit Host=

No↵

Press ENTER to Confirm or ESC to Cancel: ↵

请

按照下表中的介绍来配置动态DNS参数。

表 139 菜单 1.1： 配置动态DNS

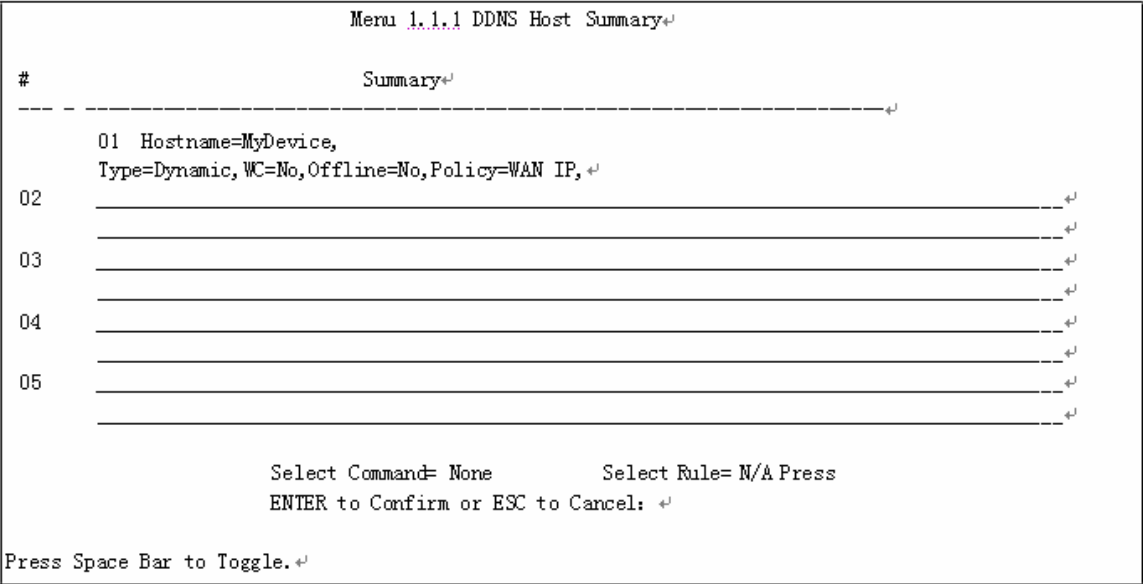
区域	描述
Service Provider	这是您的动态DNS服务供应商的名称。
Active	按空格键选择 Yes ，然后按回车启用DNS。
Username	输入您的用户名。
Password	输入分配给您的密码
Edit Host	如果您要配置一台DDNS主机，请先按空格键，然后回车选择 Yes 。
当您已经完成了这个菜单，看到“Press ENTER to Confirm...”的提示后按回车键，保存您的配置，或者随时按“ESC”键以取消。	

24.2.1.1 编辑 DDNS 主机

请按照以下程序来配置一台DDNS主机。

- 在菜单1或**MAINTENANCE Device Mode**界面将您的ZyWALL配置为一台路由器。
- 在主菜单中输入1，进入**Menu 1-General Setup**。
- 在 **Edit Dynamic DNS** 界面中按空格键选择 **Yes**，然后按回车键显示 **Menu 1.1-Configure Dynamic DNS**。
- 在 **Edit Host**区域按空格键选择 **Yes**，然后回车显示 **Menu 1.1.1-DDNS Host Summary**。

图 210 菜单 1.1.1: DDNS Host 汇总



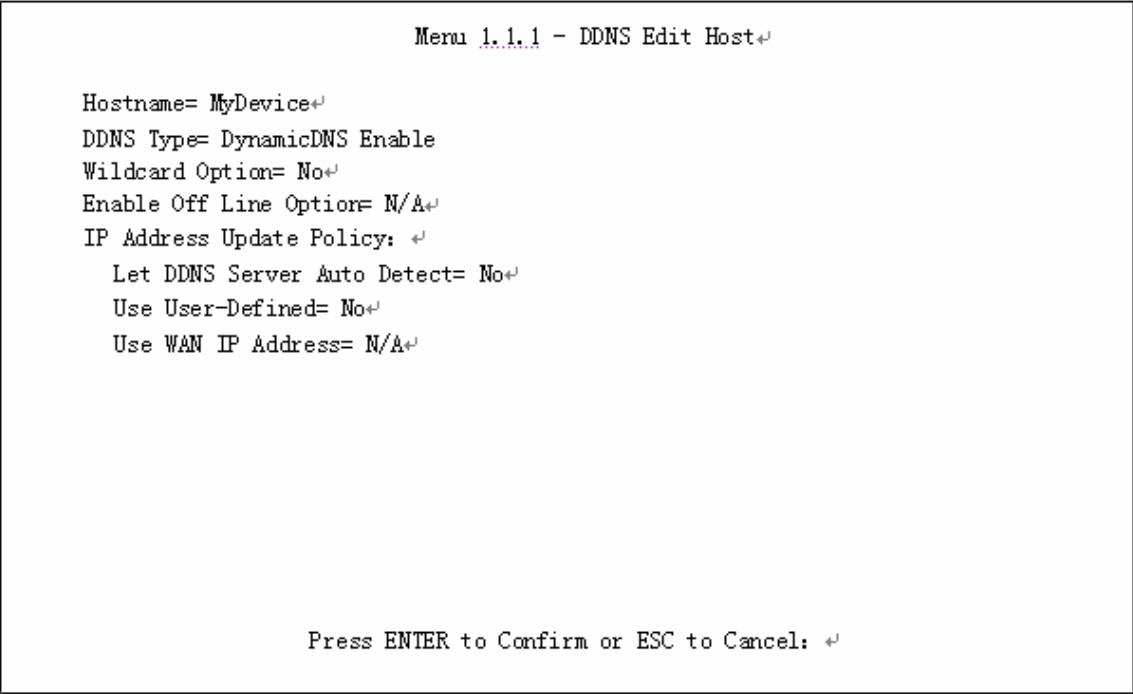
下表为界面相关的描述。

表 140 菜单 1.1.1: DDNS主机摘要

区域	描述
#	这里显示DDNS主机的索引号。
Summary	这里显示关于DDNS主机的详细情况。
Select Command	按空格键选择 None . Edit . Delete . Next Page 或者 Previous Page , 然后回车。选择 Edit 或 Delete 命令时,您必须在接下来的一个域选择一个DDNS主机。 选择 None 然后回车, 出现提示“Press ENTER to Confirm...”。 利用 Edit 可以创建或编辑一条规则。利用 Delete 可以删除一条规则。编辑或者删除一个DDNS主机, 首要的是确定您是在一个正确的页 面。当一条规则被删除后, 后来的规则不能被提前。 选择 Next Page 或 Previous Page 来查看下一页或上一页。
Select Rule	输入您想要编辑或删除的DDNS主机索引号, 然后回车。
当您已经完成了这个菜单, 看到“Press ENTER to Confirm...”的提示后按回车键, 保存您的配置, 或者在任何时候都可以按“ESC”键取消。	

5 在**Select Command**处选择**Edit**; 在**Select Rule**处输入您想要配置的DDNS主机索引号, 然后回车打开**Menu 1.1.1-DDNS Edit Host** (参阅下图)

图211 菜单1.1.1: DDNS编辑主机



以下为界面相关的描述。

表 141 菜单 1.1.1： DDNS编辑主机

区域	描述
Host Name	在此处输入您的主机名。
DDNS Type	如果您有动态的DNS服务，按空格键然后回车选择 Dynamic DNS 。 如果您有静态的DNS服务，请选择 Static DNS 。 如果您有自定义的DNS服务，请选择 Custom DNS 。
Enable Wildcard Option	ZyWALL支持DYNDNS通配符。按空格键然后回车选择 Yes 或 No 。 当您选择DDNS客户端时，该区会显示 N/A 。
Enable Off Line Option	只有当 DDNS Type 区域中选择 Custom DNS 时，该选项才会有效。 按空格键然后回车选择 Yes 。当选择 Yes 的时候， http: //www.dyndns.org/ 流量会被重定向到一个您先前指定的URL上。
Bind WAN	输入用于更新域名IP地址的WAN端口。
IP Address Update Policy:	您可以在 Let DDNS Server Auto Detect 区域(推荐)或 Use User-Defined 区域选择 Yes ，但是不能同时选择。 当 Let DDNS Server Auto Detect 区域和 Use User-Defined 区域

	域 都设置为 No 的时候,DDNS服务器会自动利用WAN口的IP地址来更新主机名的IP地址。 DDNS不能配合私有IP地址工作。当两个区都设置为 No 的时候,为了能使DDNS工作ZyWALL必须有一个公网的WAN IP地址。
Let DDNS Server Auto Detect	当在ZyWALL和DDNS服务器之间有一个或更多的 NAT 路由器的时 候, 只能选择该选项。按空格键并且选择 Yes , 然后回车让 DDNS 服务器自动侦测并使用NAT路由器的公网IP地址。 注意: 如果在ZyWALL和DDNS服务器之间有一个HTTP代理服务器, DDNS服务器就可能不能侦测正确的IP地址。
Use User-Defined	按空格键选择 Yes , 然后回车来以新带有WAN IP地址的主机名的IP 地址。 如果ZyWALL使用或者隐藏在静态公网IP地址的后面, 您只能选择 Yes 。
Use WAN IP ADDRESS	如果在 Use User-Defined 区域您选择 Yes 请输入静态公网IP地址。
当您已经完成了这个菜单, 看到“Press ENTER to Confirm...”的提示后按回车键, 保存 您的配置, 或者在任何时候都可以按“ESC”键取消。	

当您重新配置菜单1或执行DHCP客户端更新时, IP地址会更新。

第 25 章 广域网和拨号备份设置

本章主要描述了如何在菜单2中配置广域网，在菜单2.1和11.1中配置拨号备份。

25.1 介绍广域网和拨号备份配置

本章介绍了如何配置您的广域网端口和如何配置ZyWALL来使用拨号备份。

25.2 广域网配置

在主菜单中输入2，打开Menu 2。

图 212 WAN Setup中的MAC地址克隆

Menu 2 - WAN Setup↵

MAC Address: ↵
Assigned By= Factory default↵
IP Address= N/A↵

Dial-Backup:
Active= No↵

Port Speed= 115200↵
AT Command String:
Init= at&fs0=0↵
Edit Advanced Setup= No↵

Press ENTER to Confirm or ESC to Cancel: ↵

以下为界面相关的描述。

表142 在WAN Setup中设置MAC地址克隆

区域	描述
(WAN 1/2) MAC Address	

Assigned By	点击空格键然后回车选择其中的一种方法来分配一个MAC地址。选择 Factory Default 可以选择分配出厂缺省的MAC地址。选择 IP address attached on LAN 可以使用您在下一区指定计算机的MAC地址。
IP Address	只有您在 Assigned By 区域选择 IP address attached on LAN 的时候才有效。输入局域网上您需要克隆MAC地址的计算机的IP地址。
当您已经完成了这个菜单，看到“Press ENTER to Confirm...”的提示后按回车键，保存您的配置，或者在任何时候都可以按“ESC”键取消。	

25.3 拨号备份

当WAN口的宽带连接失败的情况下，您也可以设置启用拨号备份的连接。请首先确认您已经建立好了端口连接（参阅快速安装指南），然后配置。

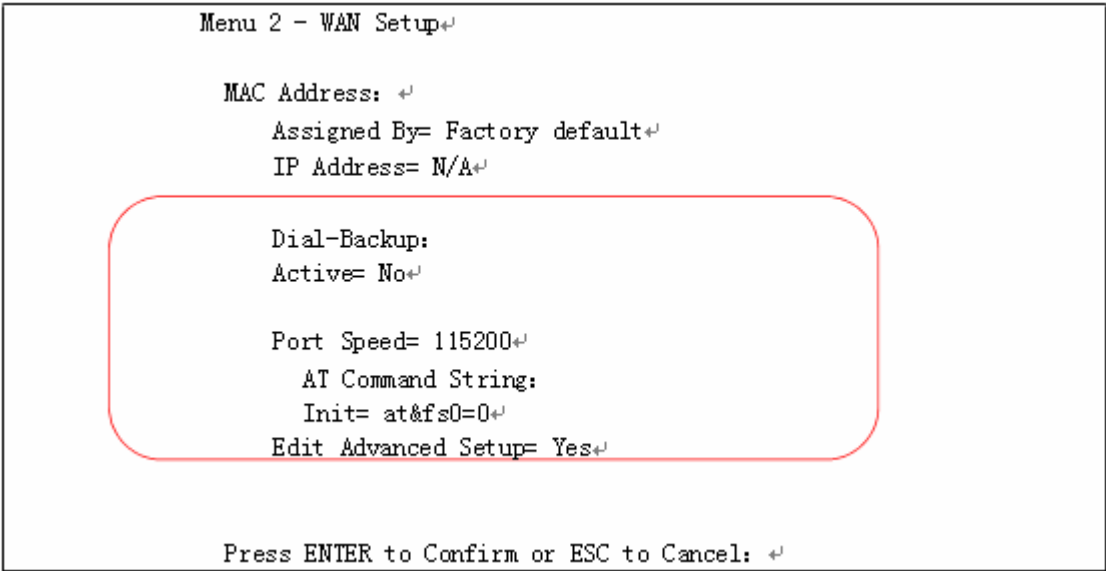
1. Menu 2-WAN Setup,

2. Menu 2.1-Advanced WAN Setup

3. Menu 11.1 – Remote Node Profile (Backup ISP) 您也可以参考流量重定向的章节来了解关于备份广域网连接的信息。

25.4 在菜单 2 中配置拨号备份

在菜单中输入2，打开菜单2。



以下为界面相关的描述。

表 143 菜单 2：拨号备份设置

区域	描述
Dial-Backup:	
Active	使用该区可以启用（Yes）或者关闭（No）拨号备份功能。
Port Speed	使用空格键然后按回车键来选择拨号备份端口和外部设备之间的连接速率。有效速率有：9600, 19200, 38400, 57600, 115200或230400 bps。
AT Command String:	
Init	输入AT指令来初始化广域网设备,请参考广域网设备的说明书来设置相关的AT指令。
Edit Advanced Setup	如果需要编辑拨号备份端口的高级选项，请先将指针移动到该区域，按空格键选择Yes，然后回车进入Menu 2.1-Advanced Setup。
当您已经完成了这个菜单，看到“Press ENTER to Confirm...”的提示后按回车键，保存您的配置，或者在任何时候都可以按“ESC”键取消。	

25.5 高级 WAN 设置

注意：请参考您的拨号备份端口所连广域网设备的用户手册来明确AT命令。

如果想要编辑拨号备份端口的高级设置项，可以在**Menu 2-WAN Setup**中将指针移动到**Edit Advanced Setup**处，按空格键选择**Yes**然后回车即可。

AT Command Strings:

Dial= atdt

Drop= ~~~+++~~~ath

Drop DTR When Hang Up= Yes

AT Response Strings:

CLID= NMBER =

Called Id= Speed=

CONNECT

Press ENTER to Confirm or ESC to Cancel:

Call Control:

Dial Timeout(sec)= 60

Retry Count= 0

Answer= ataRetry

Interval(sec)= N/A Drop

Timeout(sec)= 20

Call Back Delay(sec)= 15

以下为界面相关的描述。.

表144 高级广域网端口设置：AT指令区域

区域	描述
AT Command Strings:	
Dial	输入AT指令，建立一个呼叫。
Drop	输入AT指令来断开一个呼叫，“~”代表一个一秒钟的等待。如果 modem响应时间较慢，您可以使用指令“~~~+++~~~ath”。
Answer	输入一个AT指令来应答一个呼叫。
Drop DTR When Hang Up	按空格键然后选择 Yes 或 No 。当选择 Yes （默认）ZyWALL在发出AT指令字符串“Drop”的时候断开DTR信号。
AT Response Strings:	
CLID (Calling Line Identification)	在AT响应字符串中的CLID（呼叫线路标识）之前输入一个关键字。它可以让 ZyWALL 从 WAN 设备发送的 AT 响应字符串中捕获 CLID值。CLID用于CLID认证。
Called Id	在被拨叫的电话号码之前输入关键字。
Speed	在连接速率之前输入关键字。
Call Control	

Dial Timeout (sec)	以秒为单位输入一个时间值，用来代表ZyWALL在时间溢出（停止）之前尝试向外呼叫的时间。如果ZyWALL在规定的时间内不能建立一个向外的呼叫，它就会由于时间溢出而停止呼叫。
Retry Count	输入一个数值，规定了ZyWALL在将该号码置于黑名单之前尝试呼叫一个忙线或无应答号码的次数。
Retry Interval (sec)	以秒为单位输入一个时间值，规定了ZyWALL从一次呼叫失败后到开始另外一次呼叫的等待时间。此项会在将该号码置于黑名单之前应用。
Drop Timeout (sec)	以秒为单位输入一个时间值，用来规定ZyWALL如果没有收到一个肯定的连接断开确认而断开DTR信号之前的等待时间。
Call Back Delay (sec)	以秒为单位输入一个时间值，规定了ZyWALL断开一个回拨请求和呼叫一个回拨电话之间的等待时间。

25.6 远程节点说明（备份 ISP）

在**Menu 11** 进入 **2 - Remote Node Setup**，打开 **Menu 11.2 - Remote Node Profile**

(Backup ISP)，配置您的拨号备份端口的连接。

图 215 菜单 11.2： 远程节点介绍（备份ISP）

Menu 11.2 - Remote Node Profile (Backup ISP)

Rem Node Name=

Active= No

Outgoing:

My Login= ChangeMe

My Password= *****

Retype to Confirm= *****

Authen= CHAP/PAP

Pri Phone #= 0

Sec Phone #=

Edit PPP Options= No

Edit IP= No

Edit Script Options= No

Telco Option:

Allocated Budget (min)= 0

Period(hr)= 0

Schedules=

Always On= No

Session Options:

Edit Filter Sets= No

Idle Timeout (sec)= 100

Press ENTER to Confirm or ESC to Cancel:

以下为界面相关的描述。

表146 菜单 11.2: 远程节点介绍（备份ISP）

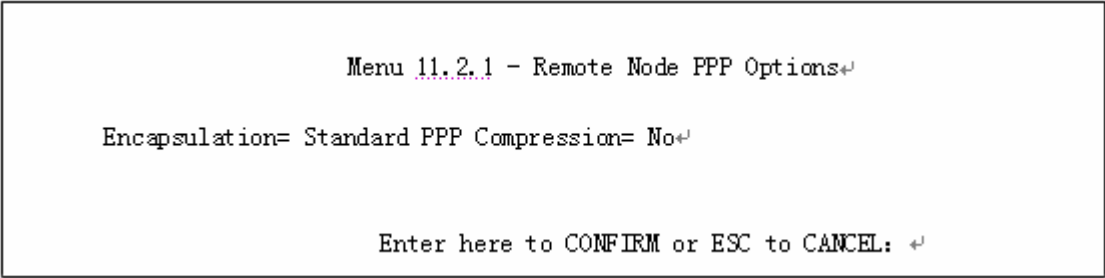
区域	描述
Rem Node Name	为远程节点输入一个描述性的名称。该区域最多可以输入8个字符。
Active	按空格键然后按回车键选择 Yes 启用该远程节点，或者选择 No 来取消远程节点。
Outgoing	
My Login	输入ISP分配给您的远程节点的登录名称。
My Password	输入ISP分配给您的远程节点的登录密码。
Retype to Confirm	再次输入您的密码以确认。
Authen	该区设置用于向外呼叫时所用的认证协议。 选项如下： CHAP/PAP - ZyWALL会同时接受远程节点的 CHAP 或 PAP 请求。 CHAP - 仅接受CHAP。 PAP - 仅接受PAP。
Pri Phone # Sec Phone #	为这个远程节点输入一个ISP的首个（主要的）电话号码。如果主电话号码忙线或无应答，您的ZyWALL会尝试拨打第二个电话号码（如果存在第二个号码）如果一些区域要求在市内电话号码前拨符号#，那么就请按照要求在电话号码前加#。

Edit PPP Options	先将指针移动到该区域，按空格键选择 Yes ，然后按回车键为该远程节点编辑PPP项。您会见到菜单显示 Menu 11.3.1 - Remote Node PPP Options （参阅章节25.7）。
Edit IP	按空格键选择 Yes 然后按回车键，进入 Menu 11.3.2 - Remote Node Network Layer Options 。请参考章节25.8了解更多信息。
Edit Script Options	按空格键选择 Yes 然后按回车键，为该拨号备份远程节点编辑AT指令脚本（ Menu 11.3.3 - Remote Node Script ）请参考章节34.9了解更多信息。
Telco Option	
Allocated Budget	以分钟为单位输入一个数值，代表该远程节点在 Period 区域内设置的时间周期内被呼叫的最长时间。默认值为0，意思是访问该远程节点没有门限和时间限制。
Period(hr)	输入一个时间周期（以小时为单位）代表该门限多久会被复位。例如，允许对该远程节点的呼叫为每个小时最多10分钟，设置 Allocated Budget 为10（分钟）， Period 为1（小时）。
Schedules	您能在这里应用四个时间计划。详情参见第51章。
Always On	按空格键选择 Yes 设置该连接不管是否有流量总是为开启。选择 No 将该连接作为一个拨接连接。
Session	

25.7 编辑 PPP 选择

ZyWALL在实现拨号备份的时候会使用PPP。如果需要编辑远程节点的PPP选项，请将光标移动到**Menu 11.2 - Remote Node Profile (Backup ISP)**区域中的**Edit PPP Options**项，按空格键选择**Yes**，然后按回车键进入**Menu 11.2.1 - Remote Node PPP Options**，如下所示。

图 216 Menu 11.2.1: 远程节点PPP选择



该表格描述了远程节点PPP选择菜单，也介绍了如果配置PPP选择域

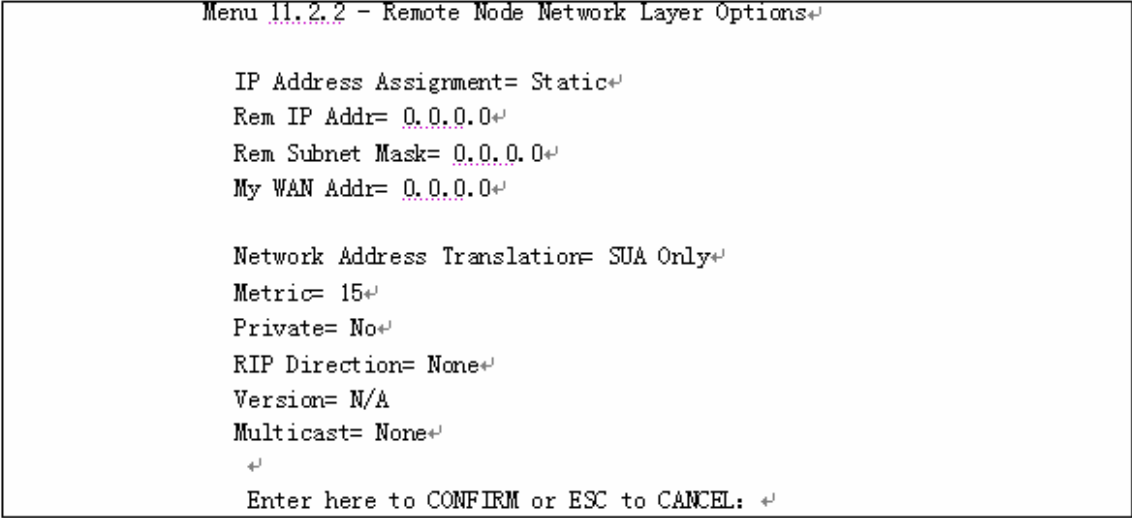
Table 147 Menu 11.2.1: 远程节点PPP选择

区域	描述
Encapsulation	如果您的WAN设备使用Cisco PPP封装方式，请按空格键，然后按回车键来选择 CISCO PPP 项，否则选择 Standard PPP 即可。
Compression	按空格键然后按回车键选择 Yes 可以启用压缩功能，或者选择 No ，不使用压缩功能。
当您已经完成了这个菜单，看到“Press ENTER to Confirm...”的提示后按回车键，保存您的配置，或者在任何时候都可以按“ESC”键取消。	

25.8 编辑 TCP/IP 选项

将光标移动到menu 11.2中的Edit IP区域，按空格键选择Yes，再按回车键进入Menu 11.2.2 - Remote Node Network Layer Options。

图 217 菜单 11.2.2: 远程节点网络层选项



以下为界面相关的描述。

表148 菜单 11.2.2: 远程节点网络层选项

区域	描述
IP Address Assignment	如果ISP没有给您分配一个固定的IP地址，请按空格键然后回车来选择 Dynamic ，或选择 Static ，并输入IP地址和子网掩码。
Re IP Address	输入ISP分配给您的固定的IP地址，（在上个菜单中选择静态地址分配）
Rem Subnet Mask	输入您的静态IP地址所对应的子网掩码。
My WAN Addr	如果您不知道ISP或其它远程路由器动态地（自动地）分配给您的 WAN 口的IP地址，请留空此处为0.0.0.0。如果您知道，请在这里输入分配给您的静态的WAN口IP地址。 这是分配给您本地ZyWALL的地址，而不是分配给远程路由器的。

Network Address Translation	网络地址转换（NAT）允许互联网协议地址从一个网络（例如一个用于本地网络的私有IP地址）转化为其它网络的一个已知的不同的IP地址（例如一个用于互联网的公网IP地址）。 先按空格键，然后回车选择Full Feature，None或SUA Only其中的任意一个。 选择None会禁用NAT。 如果您只有一个公网IP地址，请选择SUA Only。SUA（单用户帐号，Single User Account）是NAT的一个子集，支持两种类型的映射：Many-to-One和Server。 查看249页14节关于此特性的全面讨论。
Metric	为ZyWALL输入一个1到15之间的数字，来表示路由的优先级，越小的数字优先级别越高。
Private	该参数决定在ZyWALL的RIP广播中是否会包括到这个远程节点的路由。如果设定为 Yes ，该路由会为私有状态，不包含在RIP广播中。如果设定为 No ，到这个远程节点的路由就会通过RIP广播传播到其它主机。
RIP Direction	按空格然后按回车键来从 Both ， None ， In Only ， Out Only 和 None 中选择 RIP Direction 。
Version	按空格键，然后按回车键来从 RIP-1 ， RIP-2B 和 RIP-2M 中选择一个RIP的版本。
Multicast	IGMP（互联网组播协议）是一种会话层协议，用于在组播组中创建成员。ZyWALL支持IGMP版本1（IGMP-v1）和版本2（IGMP-v2）。 按空格键可以激活IP组播或者选择None禁用该功能。参见第5章可了解更多信息。
当您已经完成了Menu 11.2.2 Remote Node Network Layer Options这个菜单，看到“Press ENTER to Confirm...”的提示后按回车键，保存您的配置，返回菜单；或者在任何时候都可以按“ESC”键取消。	

25.9 编辑登录脚本

对于一些远程网关来说，在PPP协商开始之前文本登录是必需的。ZyWALL为此提供

了一种脚本工具。该脚本有六个可编程的设定，每个设定由一个“Expect”和一个“Send”字符串组成。在从服务器传回的信息与“Expect”相匹配之后，ZyWALL返回该组的“Send”字符串给服务器。

例如，一个典型的注册顺序从服务器发送一段标语开始，注册提示输入用户名，密码：

Welcome to Acme, Inc.

Login: my Login

Password:

根据第一个提示，在set 1里您指定“ogin: ”作为“Expect”字符串和“myLogin”作为“Send”字符串。忽略第一个字母“L”是为了避免要严格区分是否需要区分大小写字母。同样的，按照第二个提示，指定“word: ”作为“Expect”字符串，并且您的密码作为 “Send”字符串。

您可以用两个变量\$USERNAME和\$PASSWORD（所有大写），代表真实的用户名和密码，这样它们就不会显示出来。它们在远程节点用对外的用户名和密码代替，当ZyWALL看到它们在‘Send’串中的时候，请注意必须正确地输入两个变量。前后不能出现其它字符，也就是说它们必须被单独用于登录和密码提示。

需要注意的是这些组的顺序是非常重要的，例如，ZyWALL从第一组开始，等到所期望的（Expect）字符串，然后才会继续处理第二组，再这样往下处理其它的脚本。如果当前设定的“Expect”和“Send”栏为空时，ZyWALL将终止脚本进程并开始PPP的协商。这意味着两件事：第一，这些组必须为连续的；所有在空的组后面的都将被忽略。第二，最后一组应该和服务器发送的最后的消息相匹配。比如，当您输入密码后服务器端发出信息：

Login

successfu

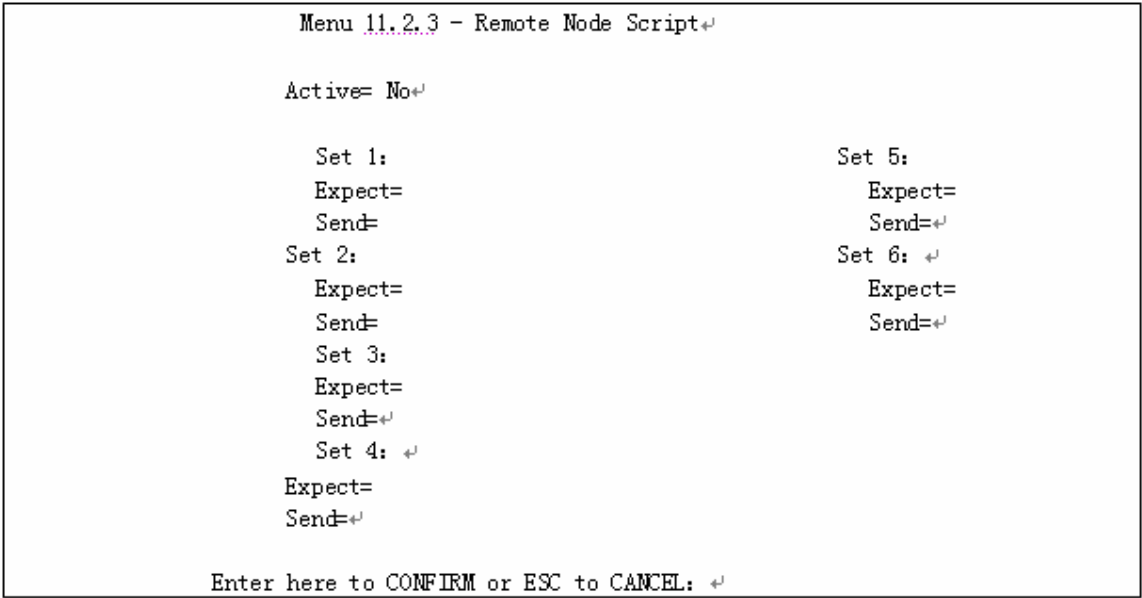
I. Starting

PPP...

在您输入密码后，则您应该再创建第三个组来匹配“PPP...”，但是这个组里面的send字段需要为空。否则ZyWALL会在向服务器发送密码之后立刻开始PPP协商。

如果脚本中有一些错误，并且它卡在一组，而且时间比菜单2中“Dial Timeout”（默认60秒）还长，ZyWALL会超时并断线。如果服务器信息和提示的顺序不是您所希望的，可以到菜单24.4发动一个手动呼叫，并查看捕获的信息进行脚本的调试。

图 218 菜单 11.2.3: 远程节点脚本



以下为界面相关的描述。

表 149 菜单 11.2.3： 远程节点脚本

区域	描述
Active	按空格键，然后按回车键来选择 Yes 以激活该 AT 指令字符串，或者选择 No 来禁用它们。
Set 1-6: Expect	输入一个期望匹配的字符串。匹配之后，ZyWALL 会在 Send 区域返回这个字符串。
Set 1-6: Send	输入一个字符串，它会在期望的字符串匹配之后发送出去。

25.10 远程节点过滤器

将光标移动到菜单11.2的**Edit Filter Sets**处，然后按空格键设置为**Yes**。
按回车键进入**Menu 11.2.4 - Remote Node Filter**。

您可在菜单11.2.4中将规定的过滤规则应用于该远程节点和ZyWALL之间输入和输出 的流量上，用于防止某些封包触发呼叫。您可以在每个过滤区指定四个过滤组，用逗号隔 开，例如，1, 5, 9, 12。注意在这里空格也是可用的。请参阅第437页32章了解更多关于过滤器 的信息。

图 219 菜单 11.2.4： 远程节点过滤

Menu 11.2.4 - Remote Node Filter↵

```
Input Filter Sets: ↵
protocol filters= device
filters= Output Filter
Sets: protocol filters=
device filters=↵
Call Filter Sets: ↵
  protocol filters=↵
    device filters=↵
```

Enter here to CONFIRM or ESC to CANCEL: ↵

第 26 章 LAN 设置

本章描述了如何在**Menu 3 - LAN Setup**中配置LAN参数。

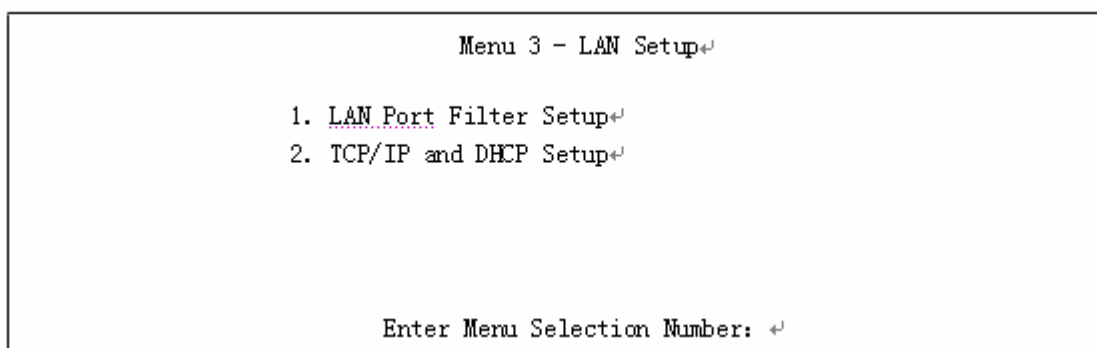
26.1 LAN 设置介绍

本章介绍了如何为局域网和无限局域网配置ZyWALL。

26.2 访问 LAN 菜单

在主菜单中输入3，进入**Menu 3 - LAN Setup**。

图 220 菜单 3： LAN 设置



26.3 LAN 口过滤设置

您可以在这个菜单里将规定的过滤规则应用于LAN流量。您很少需要过滤LAN流量，但是，过滤规则可以对于拦截某些封包，减少流量和阻止安全被攻破是有益的。

图 221 菜单 3.1： LAN端口过滤规则设置

Menu 3.1 - LAN Port Filter Setup

Input Filter Sets:

protocol filters= device

filters= Output Filter

Sets: protocol filters=

device filters=

Press ENTER to Confirm or ESC to Cancel:

26.4 TCP/IP 和 DHCP 以太网设置菜单

在主菜单中输入3，进入**Menu3-LAN Setup**。您可以在这里配置TCP/IP（RFC 1155）和DHCP以太网参数。

图222 菜单 3: TCP/IP和DHCP设置

Menu 3 - LAN Setup

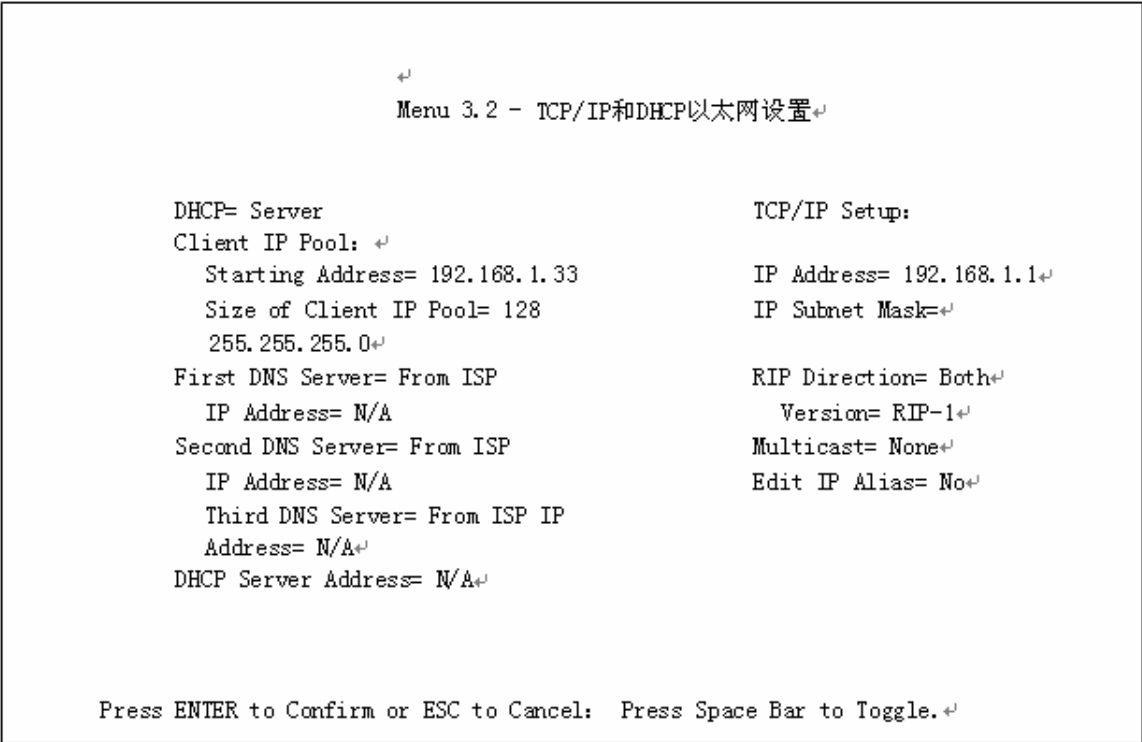
1. LAN Port Filter Setup

2. **TCP/IP and DHCP Setup**

Enter Menu Selection Number:

从菜单3中选择子菜单选项**TCP/IP and DHCP Setup**，然后回车。随后会出现**Menu 3.2 - TCP/IP and DHCP Ethernet Setup**，如下所示。

图 223 菜单 3.2: TCP/IP和DHCP以太网设置



以下为界面相关的描述。

表 150 菜单 3.2: DHCP以太网设置区域

区域	描述
DHCP	通过该处可以激活或禁用DHCP服务器的功能。 如果设为 Server ，您的ZyWALL将会成为一个DHCP服务器。 如果设为 None ，DHCP服务器的功能会被禁用掉。 如果设为 Relay ，ZyWALL将作为一个DHCP代理服务器并且在远程 服务器和客户端转发请求和响应信息。 当设为 Server 时，下列各项需要设定。
Client IP Pool:	
Starting Address	指定IP地址池中的连续的地址的第一个。
Size of Client IP Pool	指定IP地址池的大小或数量。

First DNS Server Second DNS Server Third DNS Server	如果您的ISP分配了DNS服务器信息（以及ZyWALL的广域网IP地址）请选择From ISP。下面的IP Address处显示了ISP分配的DNS 服务器（只读）IP地址。 如果您有一个DNS服务器的IP地址，就选择User-Defined。在下面的IP Address 中输入 DNS 服务器的 IP 地址。如果选择了 User-Defined，而 IP 地址设为 0.0.0.0，在您保存了更改后，User-Defined变为None。 如果您设置了第二选择User-Defined，并设置IP地址为0.0.0.0，在您保存了更改后，第二个User-Defined 变为 None。选择 DNS Relay，则 ZyWALL 作为一个 DNS 代理。ZyWALL的局域网IP地址在下面的IP Address栏（只读）中显示，ZyWALL告诉局域网上的用户ZyWALL本身就是DNS服务器。局域网上的计算机向ZyWALL发送DNS请求，ZyWALL将请求转给ZyWALL系统的DNS服务器（在menu 1中配置），并将响应发回计算机。您可以仅为三个服务器中的一个选择DNS Relay； 如果为第二或第三DNS服务器选择DNS Relay，在保存更改后，选择变为 None。如果不想配置DNS服务器，选择None，如果这样，您必须知道设备的IP地址，才可以接入。
DHCP Server Address	如果上面 DHCP 处选择了 Relay ，那么在这里输入实际的远程DHCP服务器的IP地址。

使用下面表格中的说明为LAN端口配置TCP/IP参数。

表 151 菜单 3.2: LAN TCP/IP设置区域

区域	描述
TCP/IP Setup:	
IP Address	输入ZyWALL的IP地址。
IP Subnet Mask	您的ZyWALL会自动地根据上面的IP地址来计算子网掩码。除非您使用子网，否则请使用ZyWALL提供的子网掩码。
RIP Direction	先按空格键，然后按回车键选择RIP方向。选项有： Both ， In Only ， Out Only 或者 None 。
Version	先按空格键，然后按回车键选择RIP版本。选项有： RIP-1 ， RIP-2B 或 RIP-2M 。

Multicast	IGMP(互联网组群管理协议, Internet Group Multicast Protocol)是一种会话层协议,用于在组播组中创建成员。ZyWALL可以同时支持 版本1 (IGMP-v1) 和版本2 (IGMP-v2)。 先按空格键, 然后按回车键可以激活IP组播或者选择None不启用。
Edit IP Alias	ZyWALL在它的单一的物理以太网接口上可以支持3个逻辑LAN网段。ZyWALL自身作为每个LAN网络的网关。先按空格键选择Yes, 然后按回车键即可显示菜单3.2.1。
当您已经完成了这个菜单, 看到“Press ENTER to Confirm...”的提示后按回车键, 保存您的配置, 或者在任何时候都可以按“ESC”键取消。	

26.4.1 IP 别名设置

您可以使用IP别名的功能将一个物理网络划分为多个不同的逻辑网段。通过一个单独的物理以太网端口, ZyWALL自身作为网关, ZyWALL最多可以支持3个逻辑网段。

您必须使用菜单3.2来配置第一个网络 移动光标到Edit IP Alias处 按空格键选择Yes, 并按回车键即可配置第二个和第三个网络。

按回车键可以打开Menu 3.2.1 - IP Alias Setup, 如下所示。

图 224 菜单 3.2.1: IP 别名设置

```
Menu 3.2.1 - IP Alias Setup↵

IP Alias 1= Yes↵
  IP Address= 192.168.2.1↵
  IP Subnet Mask= 255.255.255.0↵
  RIP Direction= None↵
    Version= RIP-1↵
  Incoming protocol filters=
  Outgoing protocol filters=↵
IP Alias 2= No↵
  IP Address= N/A↵
  IP Subnet Mask= N/A RIP
  Direction= N/A↵
    Version= N/A↵
  Incoming protocol filters= N/A Outgoing
  protocol filters= N/A↵

Enter here to CONFIRM or ESC to CANCEL: ↵
```

以下为界面相关的描述。

表 152 菜单 3.2.1: IP 别名设置

区域	描述
IP Alias 1, 2	选择Yes可以给ZyWALL配置其它的LAN网段。
IP Address	输入ZyWALL的IP地址。
IP Subnet Mask	ZyWALL会根据您设置的IP地址自动计算子网掩码。除非您划分子网段，否则请使用ZyWALL计算的子网掩码。
RIP Direction	按[空格键]并回车选择RIP direction。选项是Both, In Only, Out Only 或 None。
Version	先按空格键，然后按回车键选择RIP版本。选项为：RIP-1, RIP-2B 或RIP-2M。
Incoming Protocol Filters	输入您想给该节点和ZyWALL之间的入站数据流所应用的规律规则。
Outgoing Protocol Filters	输入您想给该节点和ZyWALL之间的出站数据流所应用的规律规则。
当您已经完成了这个菜单，看到“Press ENTER to Confirm...”的提示后按回车键，保存您的配置，或者在任何时候都可以按“ESC”键取消。	

第 27 章 Internet 接入

本章将会向您介绍如何配置 ZyWALL，实现 Internet 接入。

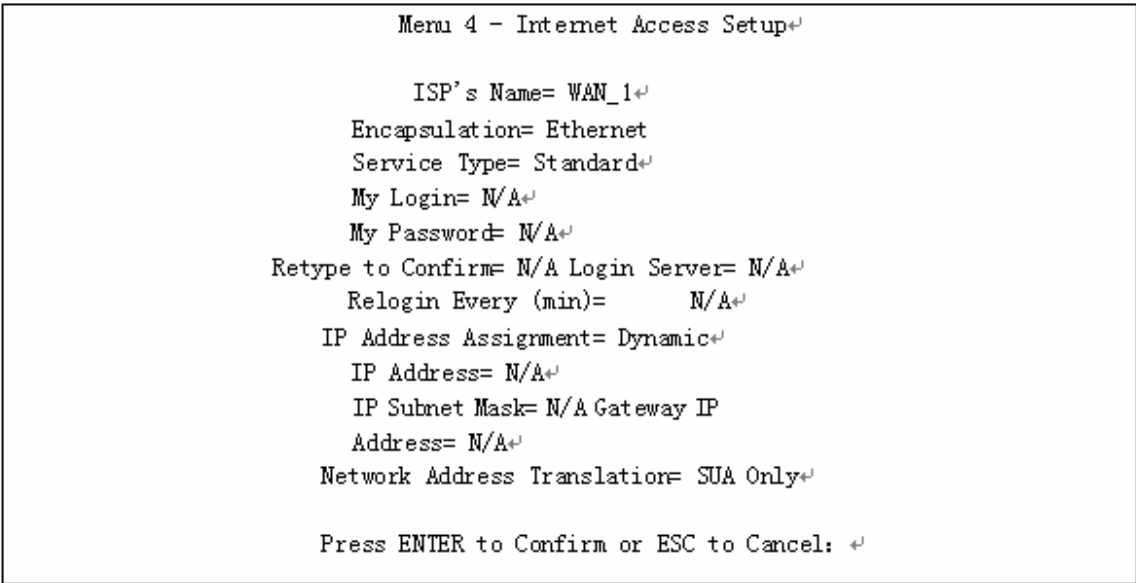
27.1 Internet 接入设置介绍

请使用您从ISP处获得的信息和本章的介绍来配置ZyWALL，使其能够接入Internet。根据您所选择的是**Ethernet**，**PPTP**还是**PPPoE**的封装方式，这里会有3个不同的菜单界面。请先和您的ISP取得联系，了解您应该采用那种封装方式。

27.2 以太网封装

如果在菜单4中选择**Ethernet**，您将会看到下面的菜单。

图 225 菜单 4： Internet访问设置（Ethernet）



以下为界面相关的描述。

表 153 菜单 4： Internet 连接设置 (Ethernet)

区域	描述

ISP's Name	这是ISP的标识名称。
Encapsulation	请按空格键然后按回车键来选择 Ethernet 。
Service Type	先按空格键，然后按回车键选择 Standard ， RR-Toshiba （RoadRunner Toshiba 鉴定方法）， RR-Manager （RoadRunner Toshiba 鉴定方法）， RR-Telstra 或者 Telia Login 。如果您的ISP 是Time Warner's RoadRunner，就选择其中的一种服务类型，否则选择 Standard 。
注意:DSL用户必须只能选择 Standard 。此时 My Login 、 My Password 和 Login Server 都是无效的。	
My Login	输入 ISP 分配给您的登录名称。
My Password	输入一个确定的密码。
Retype to Confirm	再次输入密码，以确认密码正确。
Login Server	如果此处留空ZyWALL将找到RoadRunner服务器的IP地址否则，您必须输入认证服务器的IP地址。
Relogin Every (min)	该区域只有当您选择 Service Type 中的 Telia Login 时才会有效。如果ZyWALL没有定时登录，Telia服务器会将ZyWALL登出。ZyWALL提供一个从1到59的登录之间的最大等待时间（建议使用30分钟）
IP Address Assignment	如果您的ISP没有分配给您一个固定的IP地址，按空格键并回车选择 Dynamic ，否则选择 Static ，并在下列区域输入IP地址和子网掩码。
IP Address	输入一个 ISP 分配给您的固定的 IP 地址。
IP Subnet Mask	输入和您的静态 IP 地址相应的子网掩码。
Gateway IP Address	输入和您的静态 IP 地址相应的网关地址。
Network Address Translation	选择 None 不启用NAT。如果您有一个单独的公网IP地址，请选择 SUA Only 。SUA（单用户帐号，Single User Account）是NAT的一个子集，支持两种映射： Many-to-One 和 Server 。如果您有多个公网IP地址，请选择 Full Feature 的映射类型。 Full Feature 映射类型包括： One-to-One ， Many-to-One （SUA/PAT）， Many-to-Many

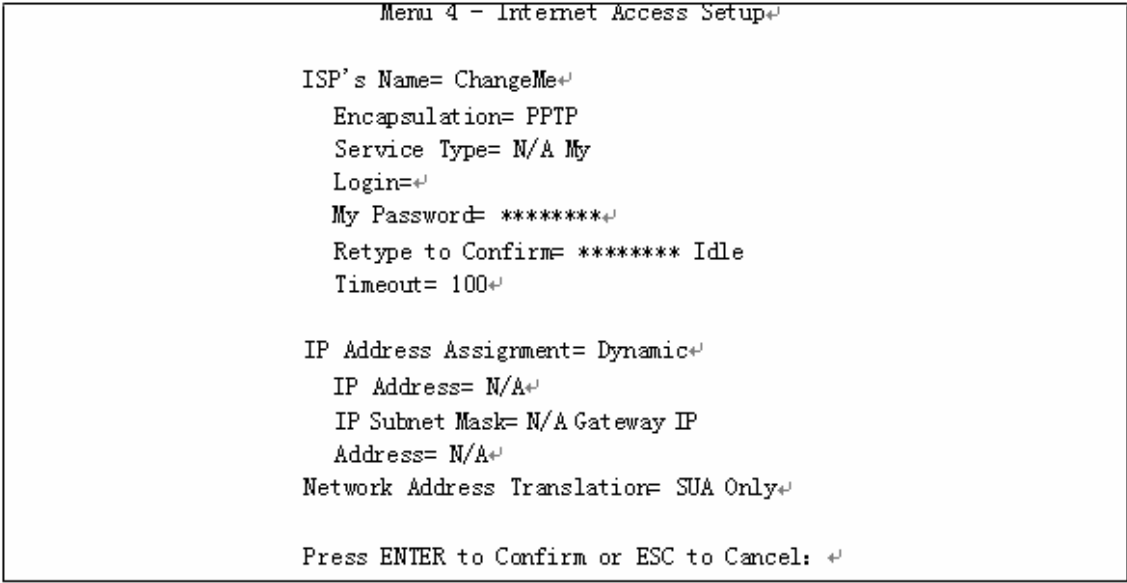
	Overload, Many- One-to-One 和 Server。 如果您 选择了 Full Feature ，您必须配置至少一个地址映射设置。 请参阅第14章了解更多关于网络地址转换功能的信息。
当您已经完成了这个菜单，看到“Press ENTER to Confirm...”的提示后按回车键，保存您的配置，或者在任何时候都可以按“ESC”键取消。	

27.3 配置 PPTP 客户端

注意：在任何特定时间里ZyWALL仅支持一条到PPTP服务器的连接。 如果您想配置PPTP客户端，您必须为PPP连接配置**My Login**和**Password**区域以及为PPTP连接配置PPTP参数。

为PPP连接配置完**My Login**和**Password**之后，在**Menu 4 -Internet Access Setup**中的**Encapsulation**区域按空格键并回车选择**PPTP**。将显示如下界面。

图 226 互联网接入配置（PPTP）



如果您在菜单4中选择**Encapsulation**区域中的**PPTP**。下表包含了关于新区域的介绍。

Table 154 菜单4（PPTP）中新区域的介绍

区域	描述
Encapsulation	先按空格键，然后按回车键来选择 PPTP 。封装方法将影响您 IP Address 项的选择。

Idle Timeout	这是一个特定的时间值，网络无流量情况超过这个时间值的时候，ZyWALL会自动与PPTP服务器断开连接。

27.4 配置 PPPOE 客户端

如果在菜单4中启用了PPPoE的封装方式，您会看到下面的界面。

图 227 互联网接入配置（PPPoE）

Menu 4 - Internet Access Setup↵

ISP's Name= WAN_1↵

Encapsulation= PPPoE

Service Type= N/A My

Login=↵

My Password= *****↵

Retype to Confirm= ***** Idle Timeout= 100↵

IP Address Assigrment= Dynamic↵

IP Address= N/A↵

IP Subnet Mask= N/A Gateway IP

Address= N/A↵

Network Address Translation= SUA Only↵

Press ENTER to Confirm or ESC to Cancel: ↵

如果您在菜单4中选择**Encapsulation**区域中的**PPPoE**。下表包含了关于新区域的介绍。

表 155 菜单4（PPPoE）中新区域的介绍

区域	描述
Encapsulation	先按空格键，然后按回车键来选择 PPPoE 。
Idle Timeout	这是一个特定的时间值，网络无流量情况超过这个时间值的时候，ZyWALL会自动与PPPoE服务器断开连接。

如果需要一个PPPoE服务名称来标识并到达PPPoE服务器，请打开菜单11并在 **Service Name**处输入提供给您的PPPoE服务名称。否则请输入any。

27.5 基本设置完成

您现在已经可以接入互联网了。

注意：当防火墙被激活的时候，默认的策略会允许所有从局域网到互联网的通信，并且阻挡所有从互联网到局域网的流量。

您可以在菜单**21.2**中或者通过**ZyWALL**内置的网页配置器解除防火墙的设定。您也可以定义附加的防火墙规则或者修改现有的一个规则，但是在做这些的时候请务必要非常注意。请参阅防火墙一章获取更多信息。

第 28 章 远程节点设置

本章将会向您介绍如何配置一个远程节点。

28.1 远程节点设置基础

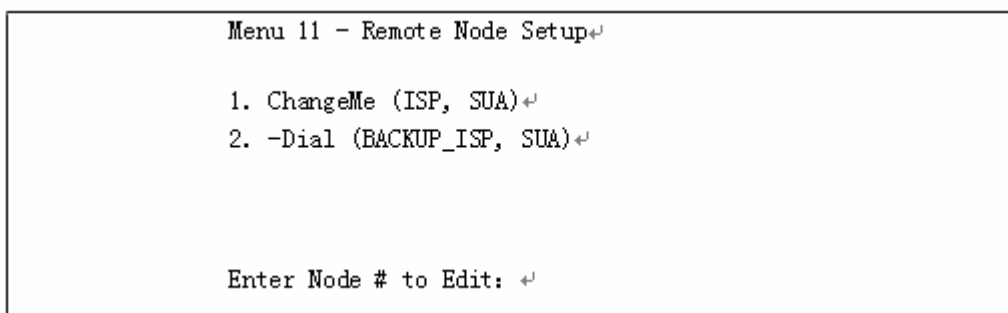
对于一个远程网关来说为了设置呼叫，一个远程节点是必须的。远程节点象征远程网关和互联网。注意当您使用菜单 4 设置互联网接入时，事实上您正在配置一个远程节点。下面会介绍如何配置 **Menu 11.x** (这里 **x** 代表 **1** 或者 **2**) - **Remote Node Profile**, **Menu 11.x.2 - Remote Node Network Layer Options** 和 **Menu 11.x.4-Remote Node Filter**。

28.2 远程节点设置

在主菜单中选择 11 进入菜单 **Menu 11 - Remote Node Setup**。

输入 **1** 进入 **Menu 11.1 - Remote Node Profile** 配置WAN端口设置，输入 **2**进入 **Menu 11.2 Remote Node Profile (Backup ISP)** 配置拨号备份端口连接（见25章381页）。

图228 菜单 11： 远程节点设置



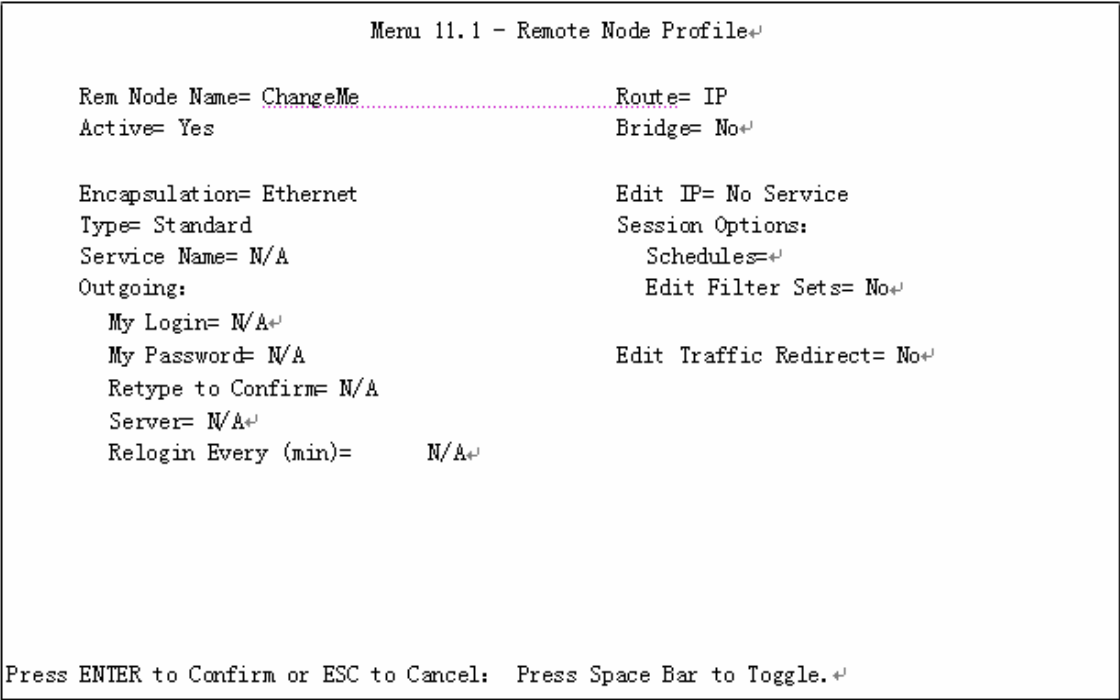
28.3 远程节点参数组设置

下面介绍如何配置远程节点参数组菜单。

28.3.1 以太网封装

根据您是选择 **Ethernet Encapsulation** , **PPPoE Encapsulation** 或者 **PPTP Encapsulation**，这里会有三种菜单。当 WAN 口作为一个常规以太网使用时，您必须选择 **Ethernet** 选项。第一个菜单 11.x 的以太网封装界面会显示如下。.

图 229 菜单 11.1：以太网封装的远程节点参数组



以下为界面相关的描述。

表 156 菜单 11.1： 以太网封装的远程节点参数组

区域	描述
Rem Node Name	输入一个描述远程节点的名称，最多 8 个字符。
Active	按空格键，然后按回车键来选择 Yes （激活远程节点）或者 No （关闭远程节点）。
Encapsulation	Ethernet 是默认的封装方式，请按空格键再按回车键来选择 PPPoE 或 PPTP 的封装方式。

Service Type	先按空格键，然后按回车键选择 Standard ， RR-Toshiba RR-Manager ， RR-Telstr 或 Telia Login 。如果您ISP为TimeWarner's RoadRunner 请选择其中一种RoadRunner 方式，否则选择 Standard 。
Service Name	在使用 PPPoE 封装，在此输入PPPoE 服务的名称。
Outgoing	
My Login	该区域只适用于 PPPoE 的封装方式。当 ZyWALL 呼叫该远程节点时，请输入 ISP 分配给您的登录名。一些 ISP 会将该区域添加到 Service Name 区域的前面(例如, jim@poellc)来接入 PPPoE 服务器。
My Password	当ZyWALL 呼叫该远程节点时，输入ISP 分配给您的密码。仅对 PPPoE 封装有效。
Retype to Confirm	再次输入密码以便确认您所输入的是正确的。
Server	只有当您在 Service Type 区域中选择了 RoadRunner 的时候，该区域才会有效。如果此处留空，ZyWALL 将会自动寻找RoadRunner服务器的IP 地址。如果不留空，那么您就必须在这里输入认证服务器的IP 地址。
Relogin Every (min)	只有当您在 Service Type 区域中选择了 Telia Login 的时候，该区域才会有效。如果ZyWALL 不定时登录，Telia 服务器会与ZyWALL断开。请输入1 到59 的分钟数（建议时间为30 分钟）作为ZyWALL两次登录之间的等待时间。
Route	该区域是会被ZyWALL 路由的协议，对ZyWALL 来说IP 是唯一的选项。
Bridge	在bridging 激活时，ZyWALL 将转发所有的数据包，不路由到远程节点；反之，数据包被丢弃。选择 Yes 激活， No 禁用。
Edit IP	该区域是一个“隐藏的”菜单。按空格键选择 Yes ，然后按回车键进入菜单 Menu 11.x.2 - Remote Node Network Layer Options 。
Session Options	
Schedules	您可以在该区域设置4 个时间计划表。请参考第38章495页来了解更多的信息。

Edit Filter Sets	该区域是一个“隐藏的”菜单。按空格键选择 Yes ，然后按回车键进入菜单 Menu 11.x.4 – 编辑过滤器设置 ，请参考第28.5节410页来了解更多的信息。
Edit Traffic Redirect	按空格键，来选择 Yes 或者 No 。 如果您不想配置该功能，请选择 No （默认设置）。选择 Yes ，然后按回车键可以进入菜单 Menu 11.1.5 - Traffic Redirect Setup
当您已经完成了这个菜单，看到“Press ENTER to Confirm...”的提示后按回车键，保存您的配置，或者在任何时候都可以按“ESC”键取消。	

28.3.2 PPPoE 封装

ZyWALL 支持 PPPoE(基与以太网的点对点协议)。当您使用 DSL 调制解调器作为 WAN 设备的时候，您可能会使用 PPPoE 的封装方式。如果改变封装为 PPPoE，您将看到如下的界面。

图 230 菜单 11.1： PPPoE 封装的远程节点参数组

```
Menu 11.1 - Remote Node Profile↵

Rem Node Name= ChangeMe..... Route= IP
Active= Yes                               Bridge= No↵

Encapsulation= PPPoE                      Edit IP= No↵
Service Type= Standard                    Telco Option: ↵
Service Name=                             Allocated Budget (min)= 0↵
Outgoing:                                Period(hr)= 0↵
  My Login=                               Schedules=↵
  My Password= *****                   Nailed-Up Connection= No↵
  Retype to Confirm= ***** Authen=
  CHAP/PAP↵

Session Options: ↵
  Edit Filter Sets= No↵
  Idle Timeout (sec)= 100↵

Edit Traffic Redirect= No↵

Press ENTER to Confirm or ESC to Cancel: Press Space Bar to Toggle.↵
```

28.3.2.1 导出认证协议

一般来说，您应该使用强有力的验证。然而，在一些用户简介中一些供应商的应用包括了一个特定的验证协议。如果协商协议与用户简介中的特殊协议不同，甚至当协商协议比特殊协议强的时候，它就会断开连接。如果您碰到这样的问题，在成功地验证之后，远端就断开了连接，当正在连接到这样一个应用的时候，请确保您指定了一个正确的验证协议。

28.3.2.2 Nailed-Up 连接

一个nailed-up连接是一条拨号线，但不管流量的需要它总是处于连线状态。当您指定了一个nailed-up连接的时候，ZyWALL要做两件事。一是使闲置时间不起作用,二是,无论何时是打开还是断开的时候,ZyWALL 都会设法连接。显而易见nailed-up连接是非常昂贵的。

除非您的电话公司提供的服务费用是包月的，或者您需要一个固定连接并且费用对您来说是无关紧要的，请不要设置 nailed-up 连接。

28.3.2.3 Metric

请参考章节 7.2 了解详情。

表 157 菜单 11.1 区域中的参数（PPPoE 封装详解）

区域	描述
Service Name	如果您使用 PPPoE 封装，那么请在这里输入 PPPoE 的服务名称。仅为 PPPoE 封装有效。
Authen	该区域设置用于对外呼叫的认证协议。 选项有： CHAP/PAP — 您的 ZyWALL 会接受远程节点的 CHAP 或 PAP 请求。 CHAP — 仅接受 CHAP 请求。 PAP —仅接受 PAP 请求。
Telco Option	
Allocated Budget	此处为远程节点设置对外呼叫的时间上限。默认值为 0 表示没有预算控制。
Period (hr)	这里表示预估重置的时间期限。例如，如果呼叫远程节点每小时最多10分钟，那么 Allocated Budget 是（10 分钟）而 Period (hr) 是 1 小时。

Schedules	您可以在这里设置 4 个时间计划表。请参考495页第 38 章来了解详情。
Nailed-Up	如果您想要和该节点创建一个 nailed-up 的连接，请设置该区域。
Connection	
Session Options	
Idle Timeout	以秒为单位创建一个时间，规定 ZyWALL 在自动断开 PPPoE 连接之前的空闲时间（当从 ZyWALL 没有流量流向远程节点的时候）该选项只有在 ZyWALL 触发呼叫时可用。

28.3.3 PPTP 封装

如果您在菜单11.1 中选择了 PPTP 的封装方式,您将看到下面的界面.请参考 3.2.1.3来了解有关PPTP的信息。.

图 231 菜单 11.1： PPTP 封装的远程节点参数组

Menu 11.1 - Remote Node Profile↵

Rem Node Name= ChangeMe↵

Route= IP

Active= Yes

Bridge= No↵

Encapsulation= PPTP

Edit IP= No↵

Service Type= Standard

Telco Option: ↵

Service Name= N/A

Allocated Budget (min)= 0↵

Outgoing:

Period(hr)= 0↵

My Login=

Schedules=↵

My Password= *****

Nailed-Up Connection= No↵

Retype to Confirm= ***** Authen=

CHAP/PAP↵

PPTP:

Session Options: ↵

My IP Addr=

Edit Filter Sets= No↵

My IP Mask=

Idle Timeout(sec)= 100↵

Server IP Addr=↵

Edit Traffic Redirect= No↵

Connection ID/Name=

Press ENTER to Confirm or ESC to Cancel: Press Space Bar to Toggle.↵

下表描述了如何配置菜单 11.1 的区域，并非之前所讨论的。

表 158 菜单 11.1： PPTP 封装的远程节点参数组

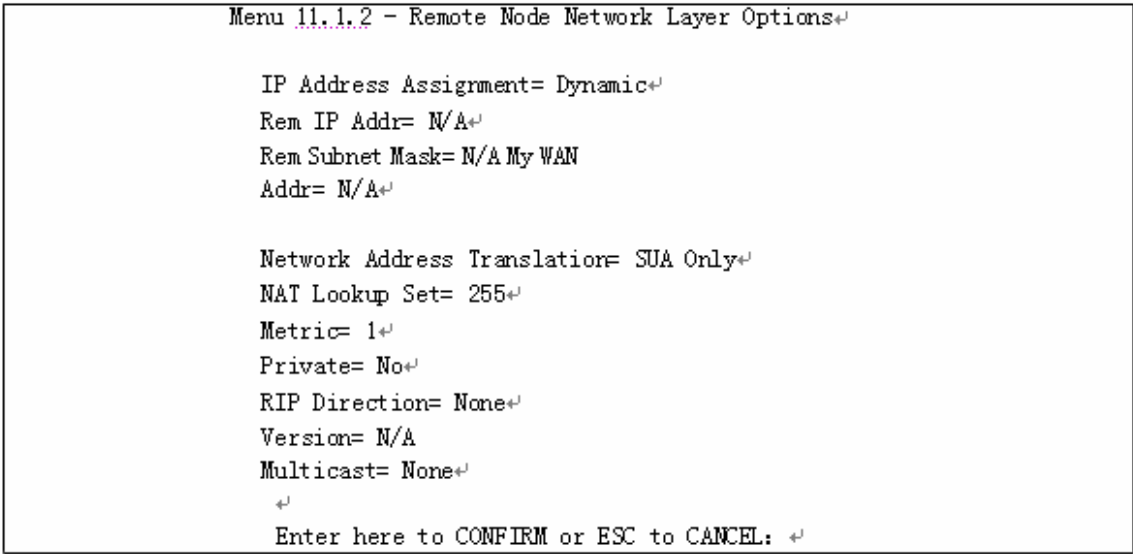
区域	描述

Encapsulation	按空格键然后按回车键来选则 PPTP 。一旦您选择了该封装方式，您必须到菜单 11.3 检查 IP 地址设定。
My IP Addr	为以太网WAN口输入IP地址。
My IP Mask	输入WAN口以太网的子网掩码。
Server IP Addr	输入ANT调制解调器的IP地址。
Connection ID/Name	输入ANT的连接ID或者连接名称。名称必须依据“c: id”和“n: name”的格式。此处可以根据您的 DSLmodem 的需求进行选择。
Schedules	您可以在这里设置 4 个时间计划表。更多信息请参考395页第 38章。
Nailed-Up Connections	如果您想要和该节点创建一个nailed-up的连接，请先按空格键，然后按回车键选择 Yes 。

28.4 编辑 IP

移动光标到菜单11.1的**Edit IP**处,然后按空格键选择**Yes**。按回车键进入 **Menu11.1.2 - Remote Node Network Layer Options**。

图 232 菜单 11.1.2:以太网封装的远程节点网络层选项



该菜单显示了PPPoE和PPTP封装的My WAN Addr 区域，以及 Ethernet 封装的Gateway IP Addr 区域。下表为相关的描述。

表 159 以太网封装的远程节点网络层选项

区域	描述
IP Address Assignment	如果您的 ISP 没有给您分配一个静态的 IP 地址, 请按空格键, 然后按 回车键来选择 Dynamic 。否则选择 Static , 然后输入您的 IP 地址和子网掩码。
(Rem) IP Address	如果您有一个静态的 IP 地址, 那么请输入该 IP 地址。
(Rem) IP Subnet Mask	如果您有一个静态的 IP 地址, 那么请输入 IP 的子网掩码。
Gateway IP Addr	此处仅对 Ethernet 封装可用。如果您正在使用一个静态的 IP 地址, 那么请输入分配给您的网关 IP 地址。
My WAN Addr	该区域只有 PPPoE 和 PPTP 两种封装方式可以使用。在 UNIX 系统中, 如果是这样的情况, 请为您的 ZyWALL 的 WAN 端口设置一个 IP 地址。注意这是分配给您本地 ZyWALL 的地址, 不是远程路由器的 IP 地址。
Network Address Translation	网络地址转换 (NAT) 允许您将网络内部的互联网协议地址 (如局域网私有地址) 转换为其它网络内部的一个不同的 IP 地址 (如公网 IP 地址) 选择 None 使 NAT 不起作用。 如果您有一个单独的公共 IP 地址, 请选择 SUA Only。SUA (单用户帐号, Single User Account) 是 NAT 的子集, 支持两种类型的映射: Many-to-One 和 Server。 如果您有多个公网 IP 地址, 请选择 Full Feature。Full Feature 映射包括 One-to-One, Many-to-One (SUA/PAT), Many-to-Many Overload, Many-to-One 和 Server。当您选择了 Full Feature, 您必须配置至少一个地址映射。 请参考第14 章了解更多信息。
NAT Lookup Set	如果您在 Network Address Translation 处选择了 SUA Only, 它会在菜单 15.1 中显示 255 和指出 SMT 将利用预配置的 Set 255 (只读) 如果您在 Network Address Translation 处选择了 Full Feature, 或者 None, 它会显示 1, 2 或者 3, 并且指出在菜单 15.1 中 SMT 将使用为第一个 WAN 口的预配置 Set 1, 第二个 WAN 口的 Set 2, 备份端口的 Set 3。 请参考章节 30.2 来了解更多信息。

Metric	输入一个从1到15的数字，设定该路由的优先级。较小的数字优先级较高。
Private	该区域只在 PPTP 或 PPPoE 封装中有效该参数会确定在到该远程节点的RIP广播中ZyWALL 是否会包括该路由。如果设定为 Yes ，该路由会保留为私有，不会包含在 RIP 广播中。如果设定为 No ，那么这个到远程节点的路由就会通过 RIP 广播传播给其它主机。
RIP Direction	先按空格键，然后按回车键 Both, None, In Only 和 Out Only 中进行选择 RIP 方向。详情请参考第 5 章。RIP 的默认设置是 None 。
Version	先按空格键，然后按回车键从 RIP-1, RIP-2B 和 RIP-2M 中选择 RIP 版本。
Multicast	IGMP（互联网组群管理协议，Internet Group Multicast Protocol）是会话层协议，用于在组播组中创建成员。ZyWALL 支持版本 1（IGMP-v1）和版本 2（IGMP-v2）按空格键可以选择激活 IP 组播或者选择 None 来禁用该功能。请参考第 5 章了解更多信息。
当您已经完成了这个菜单，看到“Press ENTER to Confirm...”的提示后按回车键，保存您的配置，或者在任何时候都可以按“ESC”键取消。	

28.5 远程节点过滤器

移动光标到菜单11.1的**Edit Filter Sets** 处，然后按空格键，设置该值为 **Yes**。按回车键进入菜单**Menu 11.1.4 - Remote Node Filter**。

您可以在菜单 11.1.4 中将过滤规则应用于在该远程节点和 ZyWALL 之间导入和导出的流量上，用于防止某些封包触发呼叫。您可以在每个过滤区指定四个过滤组，用逗号隔开，例如，1, 5, 9, 12。注意在这里空格也是可用的。请参阅第32章了解更多关于过滤器的信息。对于 PPPoE 封装或 PPTP 封装，您还会见到附加的对远程节点呼叫的过滤项设置。

图 233 菜单 11.1.4: 远程节点过滤器（以太网封装）

```

Menu 11.1.4 - Remote Node Filter↵

Input Filter Sets: ↵
protocol filters= device
filters= Output Filter
Sets: protocol filters=
device filters=↵

Enter here to CONFIRM or ESC to CANCEL: ↵

```

图 234 远程节点过滤器（PPPoE 或 PPTP 封装）

```

Menu 11.1.4 - Remote Node Filter↵

Input Filter Sets: ↵
protocol filters= device
filters= Output Filter
Sets: protocol filters=
device filters=↵
Call Filter Sets: ↵
    protocol filters=↵
    device filters=↵

Enter here to CONFIRM or ESC to CANCEL: ↵

```

28.6 流量重定向

配置相关的参数来决定 ZyWALL 何时会将发送到广域网的数据转发到您在 **Menu 11.1.5 - Traffic Redirect Setup** 中规定的备份网关上。.

```

Menu 11.1.5 - Traffic Redirect Setup↵

Active= Yes↵
Configuration: ↵
Backup Gateway IP Address= 0.0.0.0↵
Metric= 14↵
Check WAN IP Address= 0.0.0.0↵
Fail Tolerance= 10↵
Period(sec)= 300↵
Timeout(sec)= 8↵

Press ENTER to Confirm or ESC to Cancel: ↵

```

以下为界面相关的描述。

表 160 菜单 11.1.5: 流量重定向设置

区域	描述
Active	按空格键选择 Yes （启用）或者 No （禁用）流量重定向的设置。默认的是 No 。
Configuration	
Backup Gateway IP Address	输入您的备份网关IP地址。 如果ZyWALL的互联网连接中断,它会自动将流量转发到该 IP地址。
Metric	输入从1到15的数字，设定该路由的优先级。较小的数字优先级较高。
Check WAN IP Address	输入一个附近可靠的计算机的IP地址（例如您的ISP 的DSN 服务器的IP地址），用于测试 ZyWALL 广域网的连通性。如果您不输入以上内容，则使用默认网关的 IP 地址。 如果您使用 PPTP或者PPPoE的封装方式，输入“0.0.0.0”以便让 ZyWALL 可以检查 PVC（永久虚拟电路）或者 PPTP 隧道。
Fail Tolerance	输入一个数值,规定 ZyWALL 在将流量发送到备份网关之前尝试连接互联网的次数。一般设置成 2 到 5 即可。
Period(sec)	以秒为单位输入一个数字，规定ZyWALL每次检查广域网连接之间的等待时间。一般设置成5到60即可。
Timeout(sec) field.	以秒为单位输入一个数字，规定了ZyWALL对您在 Check WAN IP Address 区域中设置的IP地址进行ping时的等待响应超时时间。 该区域中的数值要小于您在 Period 区域中规定的数值。一般设置成3到50即可。 在经过了您在 Fail Tolerance 区域中规定次数的超时以后，该WAN连接会被认为是“断开”。
当您已经完成了这个菜单，看到“Press ENTER to Confirm...”的提示后按回车键，保存您的配置，或者在任何时候都可以按“ESC”键取消。	

第 29 章 IP 静态路由设置

本章介绍了如何配置ZyWALL的静态路由。

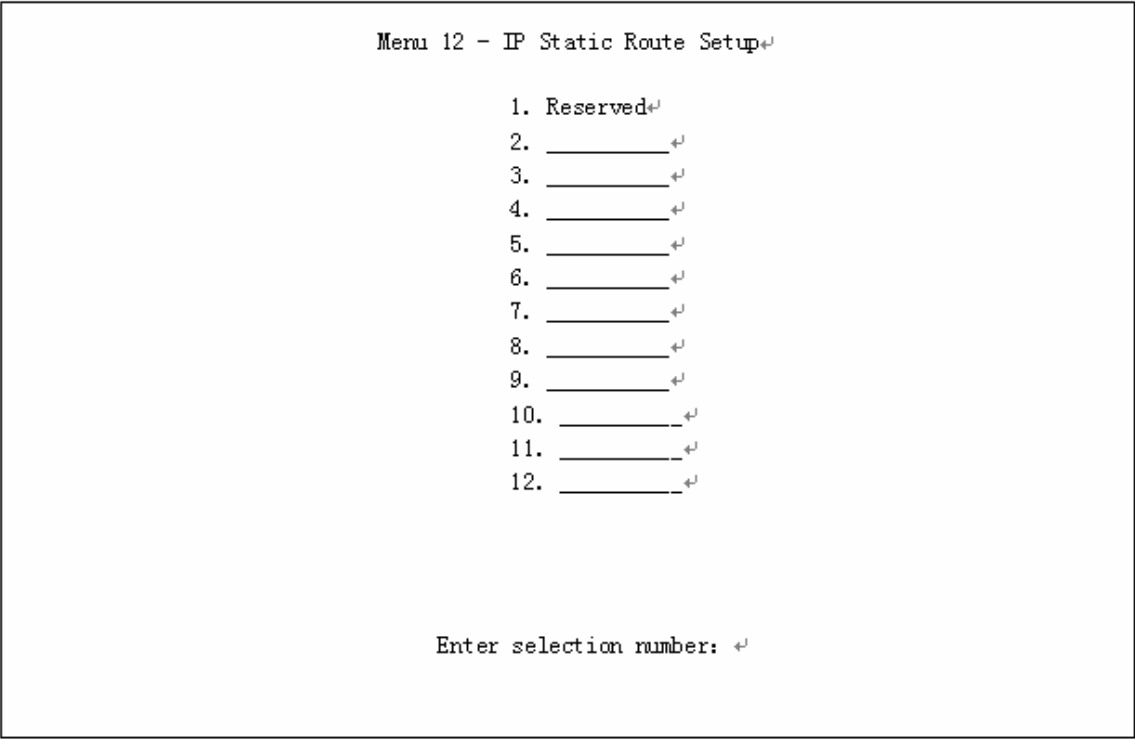
29.1 IP 静态路由设置

在主菜单中输入12。然后在Menu 12.1中选择一个IP静态路由来配置IP静态路由。

注意：第一个静态路由项用作缺省WAN 路由，你不能修改或删除它。
保留名称为空，除非你已配置了一个静态WAN IP地址。

将静态WAN IP地址改为动态WAN IP之后，路由名称会由
“default”变为“-default”，表示该静态路由不启用。

图 236 菜单 12:IP静态路由设置



现在，输入您所配置的静态路由的索引号。

图 237 菜单 12.2: 编辑IP静态路由

Menu 12.1 - Edit IP Static Route↵

Route #: 3↵

Route Name= ?

Active= No↵

Destination IP Address= ?↵

IP Subnet Mask= ? Gateway IP

Address= ? Metric= 2↵

Private= No↵

Press ENTER to CONFIRM or ESC to CANCEL: ↵

以下为界面相关的描述。

表161菜单 12. 2：编辑IP静态路由

区域	描述
Route #	这是您在菜单12中选择的索引号。
Route Name	为该路由输入一个标识名称。
Active	您可以在该区域激活或禁用该路由。
Destination IP Address	这个参数会指定最后的目的地IP地址。路由总是基于网络数值。如果您需要指定一条路由到一个独立的主机，可以利用子网掩码255.255.255.255来配合实现。
IP Subnet Mask	输入目的地的IP子网掩码。
Gateway IP Address	输入网关的IP地址。该网关与ZyWALL直接相连，它可以将封包发送到目的地。在局域网上，网关必须是一个与您的ZyWALL在一个网段上的路由器；在广域网上，网关必须是远程节点的一个IP地址。
Metric	输入从1到15的数值，设置该路由在ZyWALL的路由中的优先级，数字越小，优先级越高。
Private	该参数决定在ZyWALL的RIP广播中是否会包括到这个远程节点的路由。如果设定为 Yes ，该路由会为私有状态，不包含在RIP广播中。如果设定为 No ，到这个远程节点的路由就会通过RIP广播传播到其它主机。
当您已经完成了这个菜单，看到“Press ENTER to Confirm...”的提示后按回车键，保存您的配置，或者在任何时候都可以按“ESC”键取消。	

第 30 章 网络地址转换（NAT）

本章主要描述了怎样在ZyWALL上配置NAT。

30.1 应用 NAT

注意：除了设置SUA/NAT之外，您还必须创建一条防火墙规则来允许通过ZyWALL传送来自WAN的流量。

30.1.1 SUA（单用户账号）对 NAT

SUA（单用户帐号，Single User Account）是一个ZyNOS所执行的NAT子集，它包括两种映射：**Many-to-One**和**Server**。ZyWALL也支持**Full Feature**的NAT功能，它可以将多个全球IP地址映射到客户机或服务器的多个私有局域网的IP地址上。

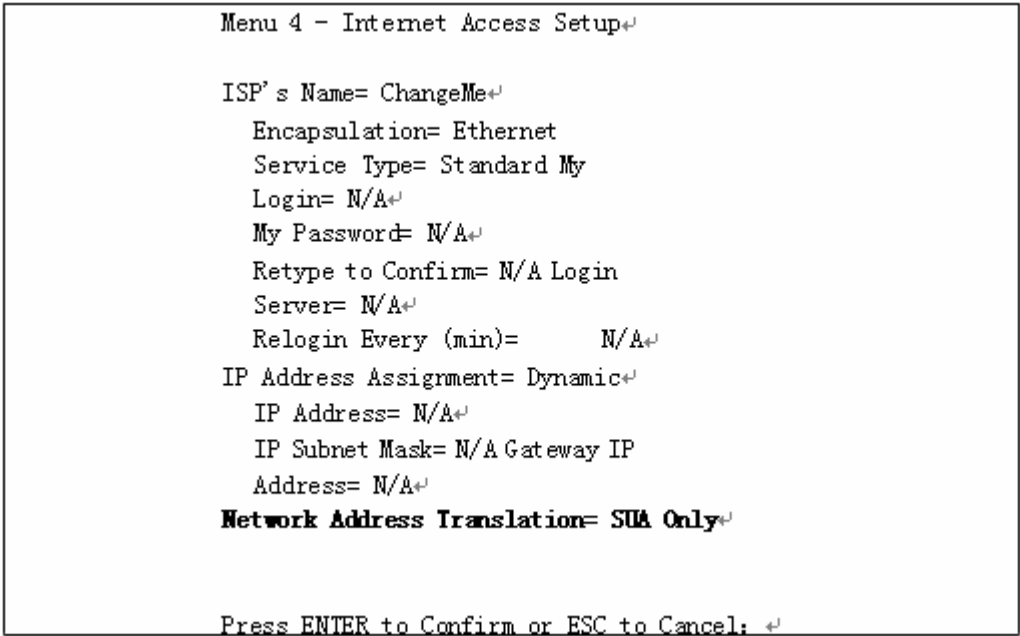
注意：如果您的ZyWALL只有一个广域网的IP地址，请选择**SUA Only**。

如果您的ZyWALL有多个广域网的IP地址，请选择**Full Feature**。

30.1.2 应用 NAT

您可以在菜单4或者菜单11.1.2来应用NAT。下图显示如何在菜单4中使用NAT来接入互联网。在主菜单中输入4进入**Menu 4 -Internet Access Setup**。

图 238 Menu 4： 应用NAT实现互联网访问

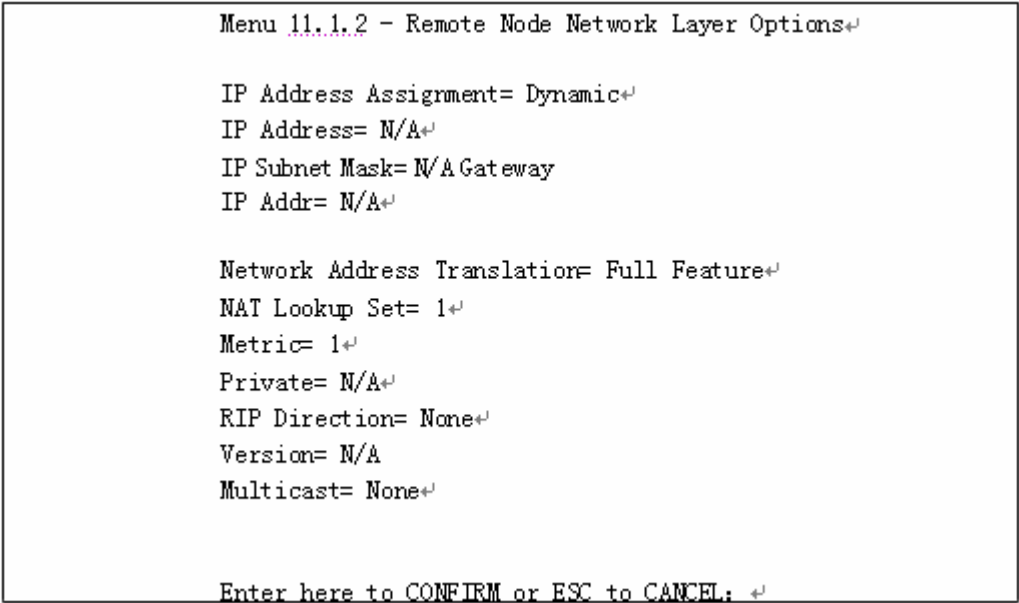


下图说明了如何通过菜单 11.1 在远程节点上来应用 NAT。

- 1. 在主菜单中输入 11。
- 2. 输入 1 进入菜单 **Menu 11.1- Remote Node Profile**。
- 3. 移动光标到 **Edit IP** 处，按空格键选择 **Yes**，然后按回车键进入菜单 **Menu**

11.1.2-Remote Node Network Layer Options。

图 239 菜单 11.1.2： 在远程节点上应用 NAT



以下为界面相关的描述。。

表 162 在菜单 4和菜单 11.1.1中应用NAT.

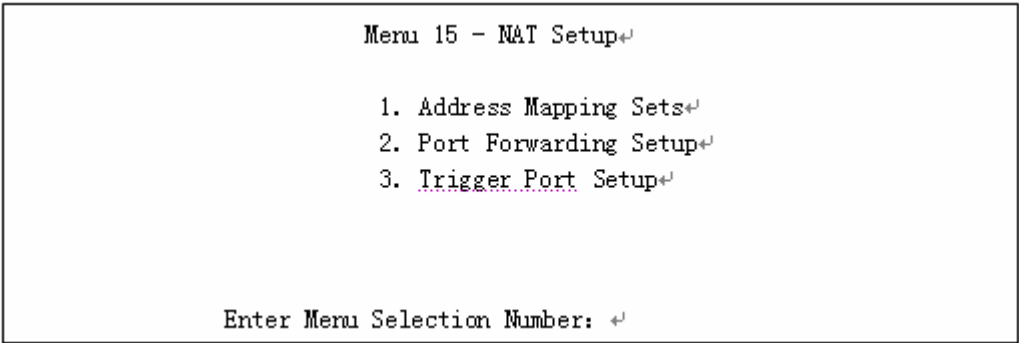
区域	描述	选项
Network Address Translation	如果您选择了该项，SMT会利用地址映射组1（Menu 15.1-查看章节30.2.1）。您可以配置任意一个映射类型，类型描述参考第22章。如果您的ZyWALL有多个共网IP地址，请选择 Full Feature 。 如果选择了 Full Feature ，您必须配置至少一个地址映射组。	Full Feature
	当您选择该选项时，NAT是不起作用的。	None
	当您选择该选项时，SMT会利用地址映射组255（Menu 15.1-查看章节42.2.1）。如果您的ZyWALL只有一个公网IP地址，请选择 SUA Only 。	SUA Only

30.2 NAT 设置

利用地址映射设置菜单和子菜单来创建映射表，用于分配全球地址给LAN上的计算机。**Set 255**用于SUA。当您在菜单4，菜单11.1.2或者11.2.2中选择了**Full Feature**，SMT将分配**set 1**给第一个WAN口，**set 2**给第二个WAN口。当您选择了**SUA Only**，SMT 会使用预选设置**Set 255**（只读）

服务器设置是一个LAN服务器映射到外部端口的列表。使用该设定，一个服务器规则必须是建立在NAT地址映射规定之内。请参考第22章来了解更详细的信息。在主菜单中输入15可以配置NAT。

图 240 菜单 15: NAT设置

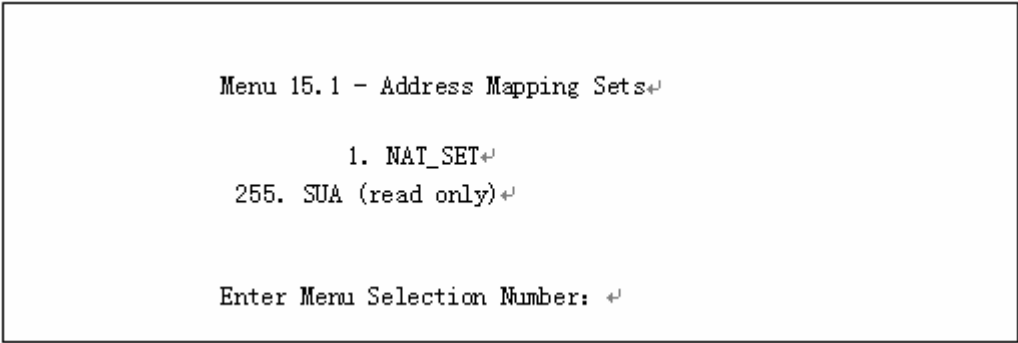


注意：在NAT 菜单 15.1 与 15.2配置LAN IP 地址。

30.2.1 地址映射设置

输入1进入菜单**Menu 15.1 - Address Mapping Sets**。

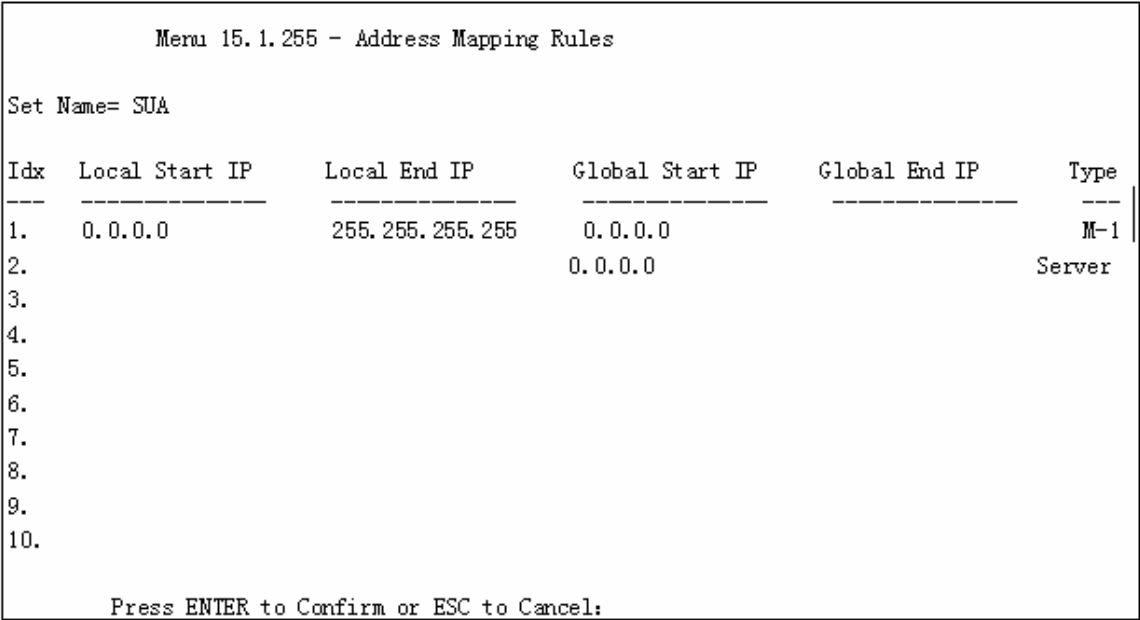
图 241 菜单 15.1： 地址映射设置



30.2.1.1 SUA 地址映射设置

输入255显示以下界面（也可参考415页章节30.1.1）此处不能被修改。

图 242 菜单 15.1.255： 以下为界面相关的描述。



以下为界面相关的描述。

注意：菜单15.1.255为只读。

表 163 SUA地址映射设置

区域	描述

Set Name	这是您在菜单15.1中选择的规则名称，或者为一个新的规则输入您想创建的名称。
Idx	
Local Start IP	Local Start IP 是指内部本地地址（ILA）的起始IP地址。
Local End IP	Local End IP 是指内部本地地址（ILA）的最后一个IP地址。如果规则针对所有的本地IP地址，那么起始IP地址为0.0.0.0，末尾IP地址为255.255.255.255。
Global Start IP	这里是指内部全球IP地址（IGA）的起始IP地址。对于一个动态的IP地址，在 Global Start IP 处输入0.0.0.0。
Global End IP	这里是指内部全球IP地址（IGA）的最后一个IP地址。
Type	这些是以上描述的映射类型。 Server 允许我们为这台NAT后面的设备指定为多个具有不同类型的服务器。参阅后面的一些范例。
当您已经完成了这个菜单，看到“Press ENTER to Confirm...”的提示后按回车键，保存您的配置，或者在任何时候都可以按“ESC”键取消。	

30.2.1.2 用户自定义地址映射设置

现在请看菜单15.1中的选项1。输入1打开该菜单。对比上一个菜单，您可以看到差异。 在该界面中，注意额外的**Action**和**Select Rule**，意味着您能够配置规则。同时注意在**Set Name**区域中的[?]，意味着这是一个必需的地方并且您必须为这个设定输入一个名字。.

注意：如果您在**Set Name**处留空并且一直回车到底，那么该设定将会被删除。.

图 243 菜单 15.1.1 地址映射规则.

Menu 15.1.1 - Address Mapping Rules

Set Name= NAT_SET

Idx	Local Start IP	Local End IP	Global Start IP	Global End IP	Type
1.	0.0.0.0	255.255.255.255	0.0.0.0		M-1
2.			0.0.0.0		Server
3.					
4.					
5.					
6.					
7.					
8.					
9.					
10.					

Action= None Select Rule= N/A Press
ENTER to Confirm or ESC to Cancel:

注意：您在菜单15.1.1.1中配置的Type，Local和Global Start/End IP也会在这里显示出来。

30.2.1.3 定制您的规则

定制规则是很必要的，因为ZyWALL会按顺序使用您定义的规则。当一条规则与当前封包匹配，ZyWALL会执行相应动作并且剩余的规则会被忽略。如果有任何空的规则在您的新配置的规则之前，您配置的规则将被那个空的规则的数字推前。举例来说，如果在当前的设定您已经配置了规则1到6并且现在您配置规则9。在汇总界面上，新规则将会是7而不是9。

如果您现在删除规则4，那么规则5到7将会前移，这样的老规则5会变为规则4，老规则6会变为规则5，老规则7会变为规则6。

表 164 菜单15.1.1中的区域

区域	描述
Set Name	为该规则输入一个名字。这是一个必要的区域。如果该处留空，那么该规则将会被删除。

Action	缺省为 Edit Edit 的意思是您想编辑一个已选择的规则(参考下面的区域)。 Insert Before 的意思是在已选择的规则前插入一条规则。在已选择的规则后面的这些规则将会后移一位。 Delete 的意思是删除已经选择的规则，并且在已选择的规则后面的这些规则将会前移一位。选择 None 会使 Select Rule 项失去作用。
Select Rule	当您在上一级菜单选择了 Edit , Insert Before 或 Delete ，光标会跳到该处，允许您选择一个规则来应用上面的动作。

注意：您必须按回车键到底来保存该设置。如果您修改了任何的设置，包括删除了一条规则，您必须再次回车到底进行保存。否则该规则不会生效。

在 **Action** 区域中选择 **Edit**，然后选择一条规则进入下一个菜单 **Menu 15.1.1.1 - Address Mapping Rule**。这里您可以编辑一个单独的规则并配置**Type**, **Local**和**Global Start/End IPs**。

注意：一个末尾的IP地址一定要比它相应的起始IP地址大。

图 244 Menu 15.1.1.1: 编辑或配置一条单独的规则

Menu 15.1.1.1 Address Mapping Rule

Type= One-to-One

Local

IP:

Start=

End= N/A

Global IP:

Start=

End = N/A

Server Mapping Set= N/A

Press ENTER to Confirm or ESC to Cancel:

以下为界面相关的描述。

表165 Menu 15.1.1.1: 编辑或配置一条单独的规则

区域	描述
Type	按空格键然后按回车键来选择一个类型。有关映射类型的介绍在249页第14章。 Server 允许您将NAT后面的某台计算机指定为提供多种服务的服务器。请参考426页章节30.4.3的范例。
Local IP	对于服务器仅本地IP区域是 N/A ；全球IP区必须要为 Server 设定。
Start	输入本地IP（ILA）的起始地址。
End	输入本地IP（ILA）最后一个IP地址。如果规则针对于所有的本地IP地址，Start IP要设置为0.0.0.0，End IP为255.255.255.255。对于One-to-One和Server类型该处是 N/A 。
Global IP	
Start	输入本地全球IP地址（IGA）的起始IP。如果您有一个动态IP，在Global IP Start中输入0.0.0.0注意只有类型为 Many-to-One 或 Server 时，Global IP Start才能设为0.0.0.0。
End	输入本地全球IP地址（IGA）的末尾IP。对于 One-to-One 和 Server Type ，该处是 N/A 。

Server Mapping Set	在 Type 处仅当您选择了 Server 时，该处才是可用的。
当您已经完成了这个菜单，看到“Press ENTER to Confirm...”的提示后按回车键，保存您的配置，或者在任何时候都可以按“ESC”键取消。	

30.3 配置一个 NAT 之后的服务器

注意：如果您不给**Default Server**分配一个IP地址，ZyWALL会将没有在这里或者在 远
程管理中设置的端口上收到的数据丢弃掉。

请按照下列步骤来配置NAT之后的一台服务器：

- 1在主菜单中输入15进入菜单**Menu 15 - NAT Setup**。
- 2 输入2 打开 **Menu 15.2 - NAT Server Setup** (并配置WAN端口的地址映射规则)。

图 245 菜单 15.2.1： NAT服务器设置

Menu 15.2 - NAT Server Setup				
Default Server: 0.0.0.0				
Rule	Act.	Start Port	End Port	IP Address
001	No	0	0	0.0.0.0
002	No	0	0	0.0.0.0
003	No	0	0	0.0.0.0
004	No	0	0	0.0.0.0
005	No	0	0	0.0.0.0
006	No	0	0	0.0.0.0
007	No	0	0	0.0.0.0
008	No	0	0	0.0.0.0
009	No	0	0	0.0.0.0
010	No	0	0	0.0.0.0
Select Command= None			Select Rule= N/A	
Press ENTER to Confirm or ESC to Cancel:				

3. 在**Select Command**区域中选择**Edit Rule**；在**Select Rule**区域中输入您要配置的
NAT 服务器的索引号， 然后按回车键进入菜单**Menu 15.2.x - NAT Server Configuration**
(参看下图)。

15.2.3 - NAT Server Configuration

Index= 2

----- Name=

1

Active= Yes

Start port= 21

End port= 25

IP Address= 192.168.1.33

Press ENTER to Confirm or ESC to Cancel:

下表对该界面的项进行了描述。

表166 15.2.x: NAT服务器配置

区域	描述
Index	这是一个单独的端口转发服务器项的索引号。
Name	输入一个该端口转发规则的标识名称。
Active	先按空格键然后按回车键选择 Yes ，可以激活该NAT服务器项。
Start Port	在 Start Port 处输入一个端口号。如果仅转发一个端口，在 End Port 处重新输入一遍端口号。对于一定范围的端口，在 End Port 处输入被转发端口范围的最后一个端口号。
End Port	
IP Address	输入内部服务器的IP地址。
当您已经完成了这个菜单，看到“Press ENTER to Confirm...”的提示后按回车键，保存您的配置，或者在任何时候都可以按“ESC”键取消。	

4 在**Start Port**处输入一个端口号。如果仅转发一个端口，在**End Port**处重新输入一遍端口号。对于一定范围的端口，在**End Port**处输入被转发端口范围的最后一个端口号。

5 在 **IP Address** 处输入内部服务器的IP地址 。在下图中 您有一台计算机在192.168.1.33处作为一台FTP，Telnet和SMTP服务器（端口分别为21,23和25）。

6 如果您已经配置好了所有的服务器，可以回车到底保存您的配置，或者随时按ESC键取消设置。

图 247 Menu 15.2: NAT服务器设置

Menu 15.2 - NAT Server Setup

Default Server: 0.0.0.0

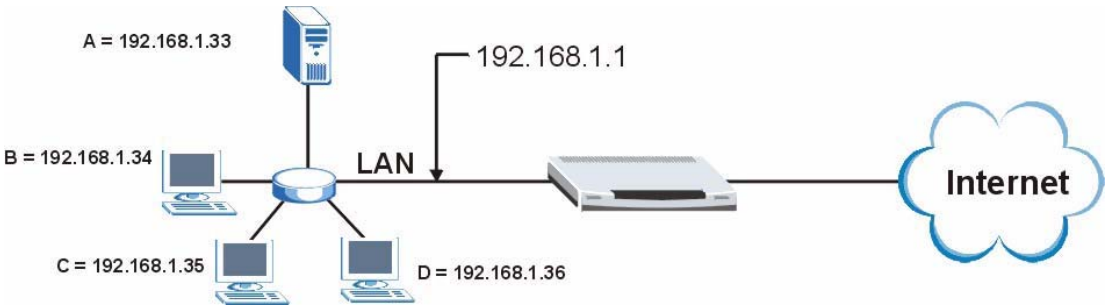
Rule	Act.	Start Port	End Port	IP Address
001	No	0	0	0.0.0.0
002	Yes	21	25	192.168.1.33
003	No	0	0	0.0.0.0
004	No	0	0	0.0.0.0
005	No	0	0	0.0.0.0
006	No	0	0	0.0.0.0
007	No	0	0	0.0.0.0
008	No	0	0	0.0.0.0
009	No	0	0	0.0.0.0
010	No	0	0	0.0.0.0

Select Command= None Select Rule= N/A

Press ENTER to Confirm or ESC to Cancel:

如果启用了 NAT 功能，那么整个 NAT 网络在互联网上就相当于是一台主机。图中 A 代表 FTP/Telnet/SMTP 服务器。

图 248 后面的服务器范例



30.4 普通 NAT 范例

以下为一些NAT配置的范例。

30.4.1 仅接入互联网

下面是一个互联网访问的范例。当所有的ILAs（内部本地地址）都影射到一个动态的由ISP分配的IGA上（内部全球地址）的时候，您只需要配置一条规则.

图 249 NAT范例1

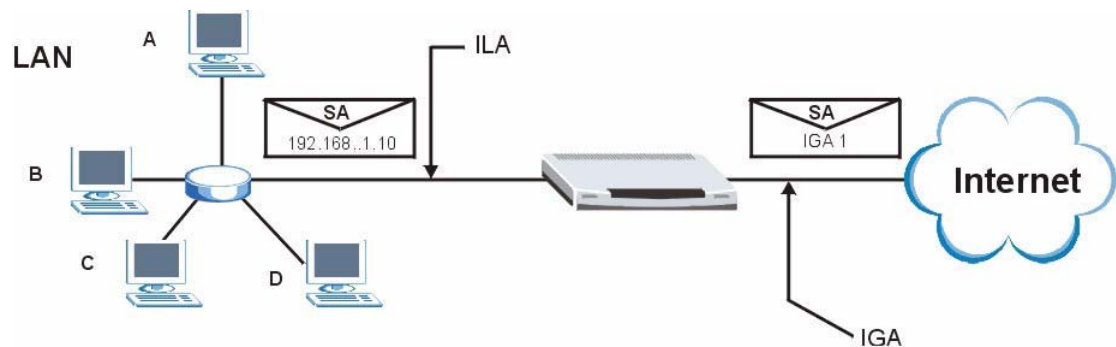


图 250 菜单 4： 互联网访问和NAT范例

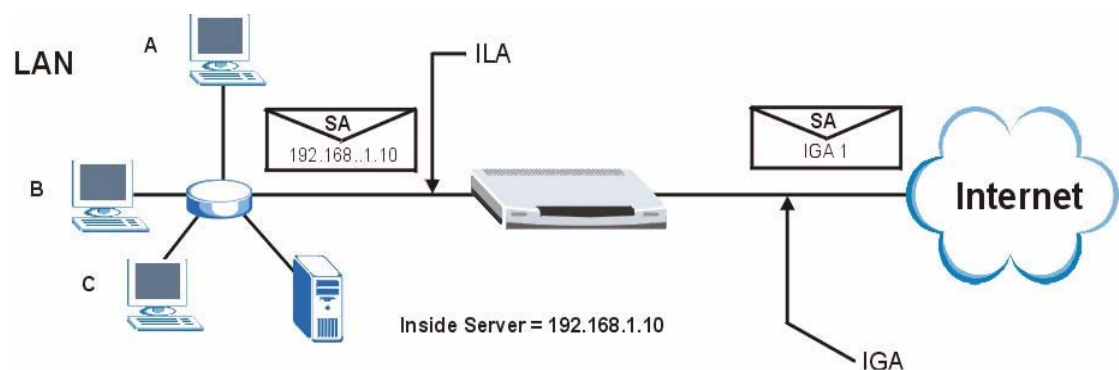
```
Menu 4 - Internet Access Setup
ISP's Name= ChangeMe
Encapsulation= Ethernet
Service Type= Standard My
Login= N/A
My Password= N/A
Retype to Confirm= N/A Login
Server= N/A
Relogin Every (min)= N/A
IP Address Assignment= Dynamic
IP Address= N/A
IP Subnet Mask= N/A Gateway IP
Address= N/A
Network Address Translation= SUA Only

Press ENTER to Confirm or ESC to Cancel:
```

从前面的菜单4来看，从**Network Address Translation**中仅需选择**SUA Only**项。它属于Many-to-One映射类型，详情请参阅424页章节30.4。

30.4.2 范例 2： 带有缺省服务器的互联网访问

图 251 NAT范例2



在这个案例中您首先按照上面的说明（使用预配置的**SUA Only**参数）进行配置，然后按照下图的说明在菜单15.2中配置NAT后面的**Default Server**。

图 252 菜单 15.2： 指定一个内部服务器

Menu 15.2 - NAT Server Setup				
Default Server: 192.168.1.10				
Rule	Act.	Start Port	End Port	IP Address
001	No	0	0	0.0.0.0
002	Yes	21	25	192.168.1.33
003	No	0	0	0.0.0.0
004	No	0	0	0.0.0.0
005	No	0	0	0.0.0.0
006	No	0	0	0.0.0.0
007	No	0	0	0.0.0.0
008	No	0	0	0.0.0.0
009	No	0	0	0.0.0.0
010	No	0	0	0.0.0.0
Select Command= None Select Rule= N/A				
Press ENTER to Confirm or ESC to Cancel:				

30.4.3 范例 3： 使用多个公网 IP 地址的内部服务器

在这个范例中，有3个从ISP获得的IGA。有很多部门，但其中两个有自己的FTP服务器。所有的部门都共享一个路由器。该范例将为每个带有FTP服务器的部门保留一个IGA，并且所有部门使用其它的IGA。将FTP服务器映射到头两个IGA，其它的LAN流量都映射到剩余的IGA上。将第三个IGA映射到一个内部的web服务器和邮件服务器。这里需要配置四条规则，两条双向的，两条单向的。

- 1. 将第一个IGA映射到第一个内部的FTP服务器上，提供双向的（1：1映射，提供本地和全球的IP地址）FTP通数据传输。

- 2. 将第二个IGA映射到第二个内部的FTP服务器上，提供双向的（1：1映射，提供本地和全球的IP地址）FTP通数据传输。
 - 3. 将LAN上其它的数据流映射到IGA3（Many：1映射）上。
 - 4. 您也可以将第三个IGA映射到LAN上的web服务器和邮件服务器。您可以利用Server将多个不同类型的服务器指定到NAT后面LAN内的其它计算机上。
- 该案例的情形有点像下图，其中A是web服务器，B是mail服务器，C 是FTP 服务器1， D 是 FTP服务器2。

图253 NAT范例3

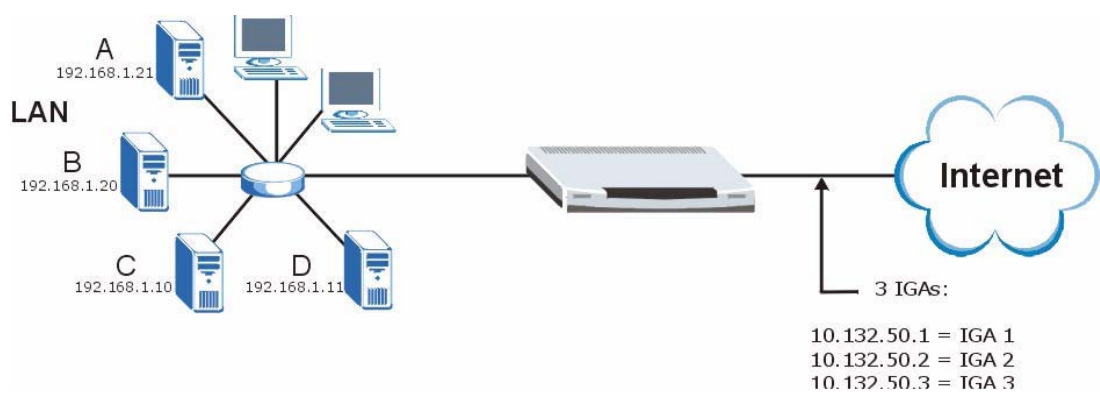


表 167 NAT范例3

MAPPING RULES

FTP1	IGA 1 Type 1: 1
FTP2	IGA 2 Type 1: 1
Other LAN traffic	IGA 3 Type M-1 (outgoing traffic)
IGA 3	Inside web server and mail server(incoming traffic)

- 1. 这个案例中您需要在Menu 15.1 – Address Mapping Sets中配置地址映射组 1 。因此您必须从Network Address Translation （在菜单4或者11.3中）选择Full Feature选项。
- 2. 在主菜单中输入15。
- 3. 输入1来配置地址映射组。
- 4 输入1开始配置这个新组 输入一个标识名称 选择Edit Action然后在Select Rule区域中输入1。按回车键确认。
- 5 .择Type为One-to-One,输入本地Start IP为192.168.1.10（FTP服务器1的IP地址） 输入全球Start IP为10.132.50.1（第一个IGA）(查看第329章)
- 6. 规则2到4的设置重复以上步骤即可。
- 7. 完成设置以后，菜单15.1.1会像如下显示。

图 254 范例3: 菜单11.1.2.

```
Menu 11.1.2 - Remote Node Network Layer Options

      IP Address Assignment= Dynamic
      IP Address= N/A
      IP Subnet Mask= N/A
      Gateway IP Addr= N/A

      Network Address Translation= SUA Only
      Metric= 2
      Private=
      RIP Direction= None
      Version= N/A
      Multicast= None

      Enter here to CONFIRM or ESC to CANCEL:
```

下图显示如何配置第一个规则。

图 255 范例3: 菜单15.1.1.1

```
Menu 15.1.1.1 Address Mapping Rule

      Type= One-to-One

      Local IP:
      Start= 192.168.1.10
      End   = N/A

      Global IP:
      Start= 10.132.50.1
      End   = N/A

      Server Mapping Set= N/A
      Press ENTER to Confirm or ESC to Cancel:
```

图 256 范例3：最后的菜单15.1.1

Menu 15.1.1 - Address Mapping Rules

Set Name= Example3

Idx	Local Start IP	Local End IP	Global Start IP	Global End IP	Type
1.	192.168.1.10		10.132.50.1		1-1
2	192.168.1.11		10.132.50.2		1-1
3.	0.0.0.0	255.255.255.255	10.132.50.3		M-1
4.			10.132.50.3		Server
5.					
6.					
7.					
8.					
9.					
10.					

Action= Edit Select Rule=

Press ENTER to Confirm or ESC to Cancel:

现在配置将IGA 3映射到LAN内的web服务器和邮件服务器上。

- 1. 在主菜单中键入15。
- 2. 键入2进入菜单15.2，按430页图257进行配置。

图257 Example 3： Menu 15.2

Menu 15.2 - NAT Server Setup

Default Server: 0.0.0.0

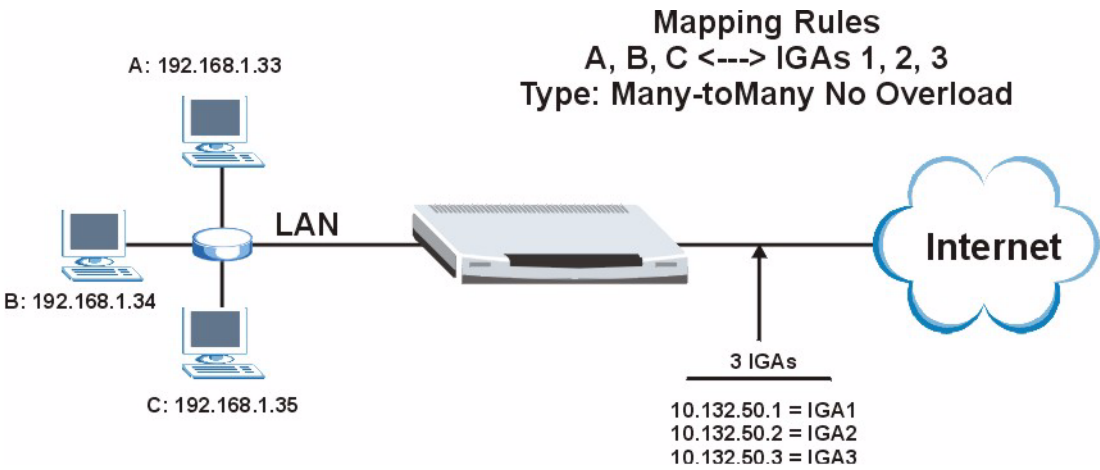
Rule	Act.	Start Port	End Port	IP Address
001	Yes	80	80	192.168.1.21
002	Yes	25	25	192.168.1.20
003	No	0	0	0.0.0.0
004	No	0	0	0.0.0.0
005	No	0	0	0.0.0.0
006	No	0	0	0.0.0.0
007	No	0	0	0.0.0.0
008	No	0	0	0.0.0.0
009	No	0	0	0.0.0.0
010	No	0	0	0.0.0.0

Select Command= None Select Rule= N/A

30.4.4 范例 4：不利于使用 NAT 的应用程序

一些应用程序不支持使用 TCP 或 UDP 端口转换的 NAT 映射。在该案例中，最好使用 **Many- to-Many No Overload** 的映射方式。下图说明了该范例。

图 258 NAT范例 4



注意：例如一些游戏软件是不利于使用NAT的应用程序，因为它们在数据流中插入了地址信息。甚至当使用**One-to-One**和**Many-One-to-One**映射类型时，这些应用软件能不通过NAT工作。

请根据案例3中的步骤来配置下面的两个菜单。

```
Menu 15.1.1.1 Address Mapping Rule

Type= Many-One-to-One

Local IP:
  Start= 192.168.1.10
  End   = 192.168.1.12

Global IP:
  Start= 10.132.50.1
  End   = 10.132.50.3

Press ENTER to Confirm or ESC to Cancel:
```

设置完该规则以后，您应该检查菜单15.1.1中的配置信息。如下图所示。

图 260 范例4： Menu 15.1.1: Address Mapping Rules

Menu 15.1.1 - Address Mapping Rules					
Set Name= Example4					
Idx	Local Start IP	Local End IP	Global Start IP	Global End IP	Type
1.	192.168.1.10	192.168.1.12	10.132.50.1	10.132.50.3	M-1-1
2.					
3.					
4.					
5.					
6.					
7.					
8.					
9.					
10.					
Action= Edit Select Rule=					
Press ENTER to Confirm or ESC to Cancel:					

30.5 触发端口转发

一些服务从客户端到服务器端都使用一个专门的端口范围。通常都是利用您在NAT中设置的端口将某种服务(来自于WAN上)转发到客户端的某台电脑的IP上。可问题是只能 将该服务转发给一个单独的LAN IP地址。为了让LAN上的不同计算机能够利用同一种服务，您必须手动将转发端口修改对应到LAN内其它计算机的IP地址上。

触发端口的方式通过允许LAN上的计算机动态轮流使用该服务可以解决该问题。如果LAN上的某台计算机通过一个指定的端口号和协议(Trigger端口)向WAN上发送服务请求的时候，ZyWALL会记录下该计算机的IP地址。当ZyWALL收到了一个从WAN上的指定端口号和协议(Incoming端口)发送的回应的时候，ZyWALL会将该信息转发给发送了请求的计算机的IP地址。如果该计算机的服务连接关闭了，那么LAN上的其它计算机就可以使用相同方式的服务了。这样当您要让LAN上一个不同的计算机来使用该应用程序的时候就不需要重新配置新的IP地址了。

触发端口

- 1. 只有源自ZyWALL内网到外网的数据才有可能引起触发事件。
- 2. 如果某个应用软件需要一个连续的数据流，该端口（范围）将被占用，以致LAN上的其它计算机不能触发它。注意：每次LAN上只有一台计算机能够使用触发端口。

注意：每次LAN上只有一台计算机能够使用触发端口。

在菜单15中输入3可以显示菜单**Menu 15.3 - Trigger Ports**。

图261 菜单 15.3： 触发端口设置

Menu 15.3 - Trigger Port Setup						
Rule	Name	Incoming		Trigger		
		Start Port	End Port	Start Port	End Port	
1.	Real Audio	6970	7170	7070	7070	
2.		0	0	0	0	
3.		0	0	0	0	
4.		0	0	0	0	
5.		0	0	0	0	
6.		0	0	0	0	
7.		0	0	0	0	
8.		0	0	0	0	
9.		0	0	0	0	
10.		0	0	0	0	
11.		0	0	0	0	
12.		0	0	0	0	

Press ENTER to Confirm or ESC to Cancel:

HTTP: 80 FTP: 21 Telnet: 23 SMTP: 25 POP3: 110 PPTP: 1723

以下为界面相关的描述。

表 168 菜单 15.3： 触发端口设置

区域	描述
Rule	这是规则的索引号。
Name	输入一个标识名称。您可以输入最多15个字符，包含空格。
Incoming	Incoming端口是WAN上的服务器使用的一个（或一定范围）的端口。
Start Port	输入一个端口号或起始端口号。
End Port	输入一个端口号或末尾端口号。
Trigger	触发端口是引起ZyWALL记录LAN计算机的IP地址的端口(或端口范围),该地址的计算机将会向WAN上的服务器发送数据
Start Port	输入一个端口号或起始端口号。
End Port	输入一个端口号或末尾端口号。

当您已经完成了这个菜单，看到“Press ENTER to Confirm...”的提示后按回车键，保存您的配置，或者在任何时候都可以按“ESC”键取消。

第 31 章 ZyWALL 防火墙介绍

本章将会向您介绍如何使用ZyWALL防火墙。

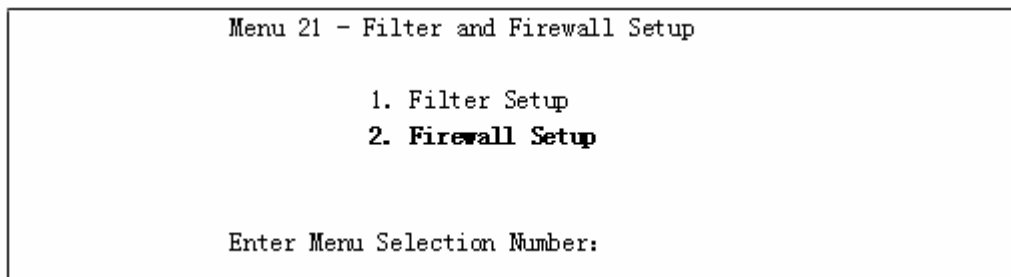
31.1 进入防火墙设置

Web界面配置可以说是ZyWALL提供的最完善的防火墙配置工具，因此，那建议您使用Web界面配置进行防火墙配置。SMT界面允许您激活防火墙，命令提供有限的防火墙配置选项，不建议使用。

31.2 防火墙 SMT 菜单

在主菜单中输入21进入菜单**Menu 21 - Filter Set and Firewall Configuration**，界面显示如下：

图262菜单 21：过滤器和防火墙设置



```
Menu 21 - Filter and Firewall Setup

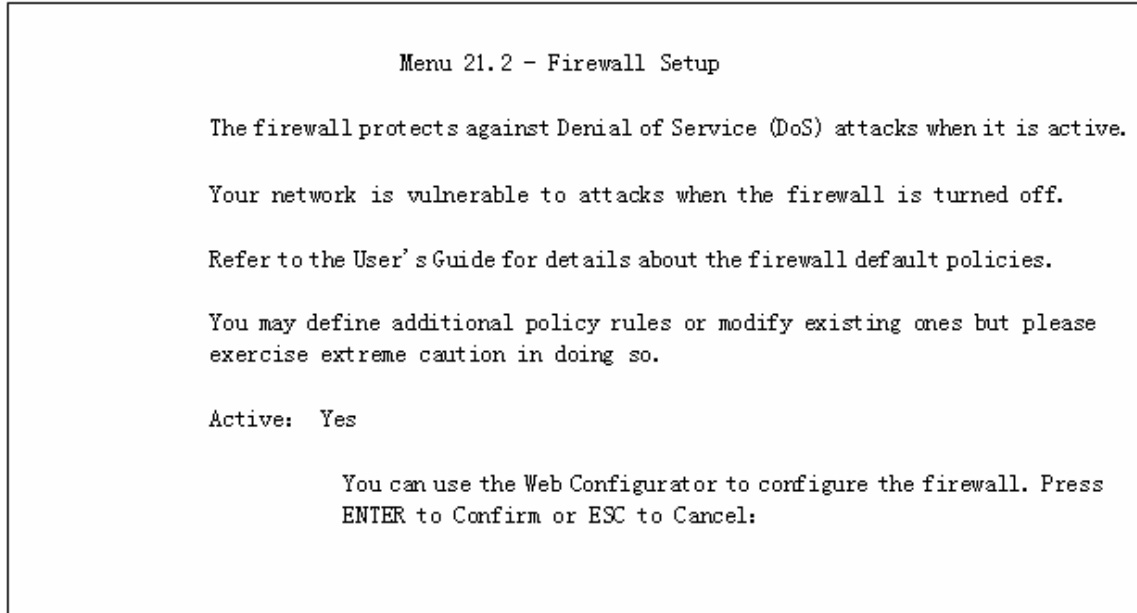
1. Filter Setup
2. Firewall Setup

Enter Menu Selection Number:
```

31.2.1 激活防火墙

在主菜单中输入2，进入以下界面。先按空格键，然后按回车键在**Active**处选择**Yes**，激活防火墙。防火墙必须被激活以防范拒绝服务（DoS）攻击。您需要配合使用Web界面来配置防火墙规则。

图 263 Menu 21.2: 防火墙设置



注意：您需要利用Web设置界面或CLI命令来配置防火墙规则。

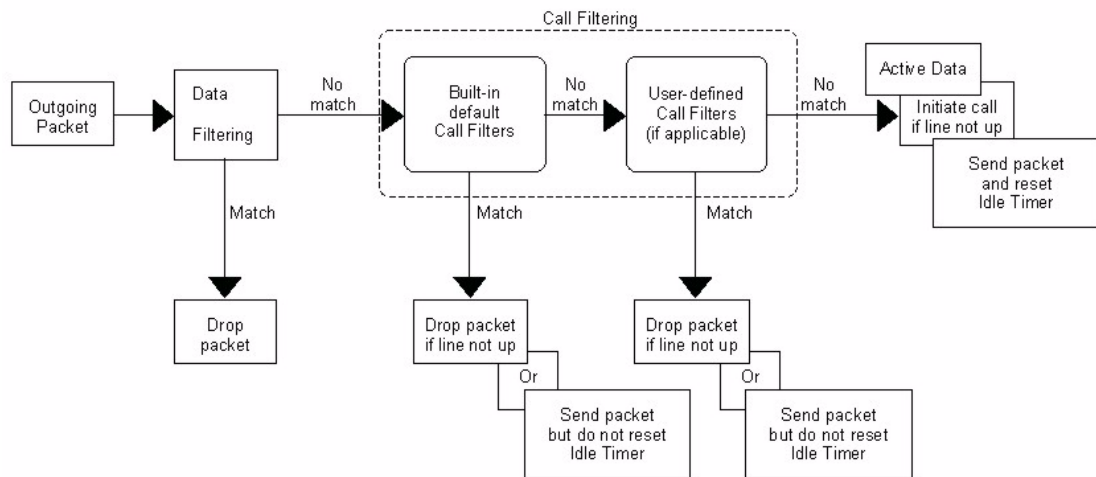
第 32 章 过滤器配置

本章将会向您介绍如何配置过滤器。

32.1 过滤器介绍

ZyWALL使用过滤器来决定是否允许一个数据包的通过和/或建立呼叫。过滤器有两种应用类型：数据过滤和呼叫过滤。过滤器又细分为设备和协议过滤器，这些将在以后介绍。数据过滤界面数据决定封包是否被允许通过。根据相对于端口的数据包传输方向，数据过滤器分成进入和流出过滤器。数据过滤器既能够应用于WAN侧，也可以应用于LAN侧。呼叫过滤用于决定一个封包是否可以触发一个呼叫。只有当使用PPPoE封装的时候，远程节点呼叫过滤器才会有效。流出数据包在它们到达呼叫过滤器之前必须经过数据过滤器，如下图所示。

图264 流出数据包过滤器流程



对于进入的数据包，您的 ZyWALL 只会使用数据过滤器。对于数据包的处理要根据它是否和一个规则相匹配。下面的章节将会描述了如何配置过滤器。

32.1.1 ZyWALL 的过滤器结构

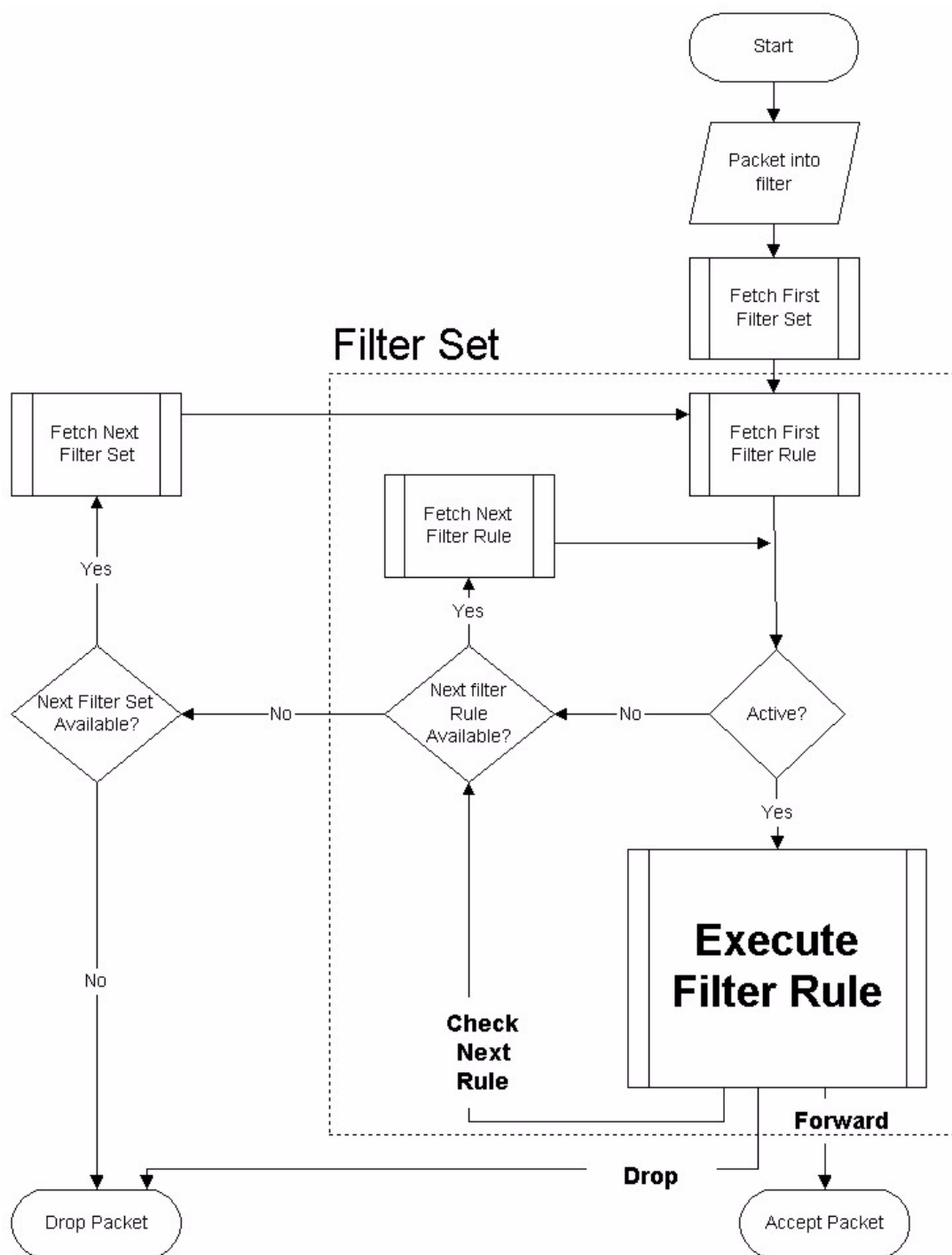
一个过滤器组由一个或多个过滤器规则组成。通常您将组合相关的规则，比如，为 NetBIOS的所有规则，在一个单独的组内并给予一个描述的名称。ZyWALL允许您配置最多

12个过滤器组，每组有6条规则，一个系统中总共有72个过滤器规则。在同一组中您不能混淆设备过滤器和协议过滤器规则。

菜单21中的出厂默认过滤器规则被配置用来阻止NetBIOS流量触发呼叫并且阻止进入的telnet会话。下面为这些过滤器规则的概述。

下图描述了执行一个过滤器规则时的逻辑流程。参见图 269

图 265 过滤规则流程



您可以给一个特定的端口最多应用四个过滤器组来阻止多种类型的封包。由于每个过滤器组有最多六条规则，所以在一个单独的端口上您可以最多启用**24**条规则。

32.2 包过滤与防火墙比较

以下是一些对ZyWALL的包过滤与防火墙功能的比较。

32.2.1 包过滤 (Packet Filtering)

包过滤限制访问机制是基于数据包和应用的源/目的网络地址。

- 当数据包通过路由器接口的时候，路由器会根据您制定的规则来过滤数据包。
- 包过滤是一个功能强大的工具，但是设置和维护都比较复杂，尤其是当您需要一系列的规则来过滤一种服务的时候。
- 包过滤只检查IP 包的包头。

32.2.1.1 何时使用包过滤

1. 根据MAC 地址来拒绝/允许LAN 网的数据包。
2. 拒绝/允许特殊的非TCP、UDP 或ICMP 的IP 数据包。
3. 拒绝/允许在两个特定的内部主机/网络“A”和外部主机/网络“B”之间由外网向内网（WAN 到LAN）和由内网向外网（LAN 到WAN）的通信。如果过滤器拒绝了A 到B 的通信，它也会拒绝B 到A 的通信。过滤器无法通过IP 地址来判断通信是源自内部主机还是外部主机。
4. 拒绝/允许IP 跟踪路由。

32.2.2 防火墙 Firewall

ZyWALL 防火墙限制机制是通过对比预先定义的规则检查数据包，基于IP 地址和协议作接入控制决定，它们也“检查”会话数据确保连接的完整以及适应动态协议。

- 防火墙会监测数据包的内容和它的源/目的地址。这类防火墙提供了一个适用于所有协议的监测模块，可以理解供其它协议层使用的，从网络层（IP 包头）到应用层的数据。
- 防火墙提供了状态监测的功能。它考虑了它所处理的连接的状态。例如，一个合法的输入数据包会与该数据包的外部请求比较来决定是否进入。相反，一个输入数据包伪装成一个不存在的外部请求的回应，就会被拒绝。
- 防火墙利用的是会话过滤，例如，聪明的规则能够加强过滤过程和控制网络会话，而不是控制会话中的每个数据包。

- 当报警发生时，防火墙会通过e-mail 来给您提供日常报告。

32.2.2.1 何时使用防火墙

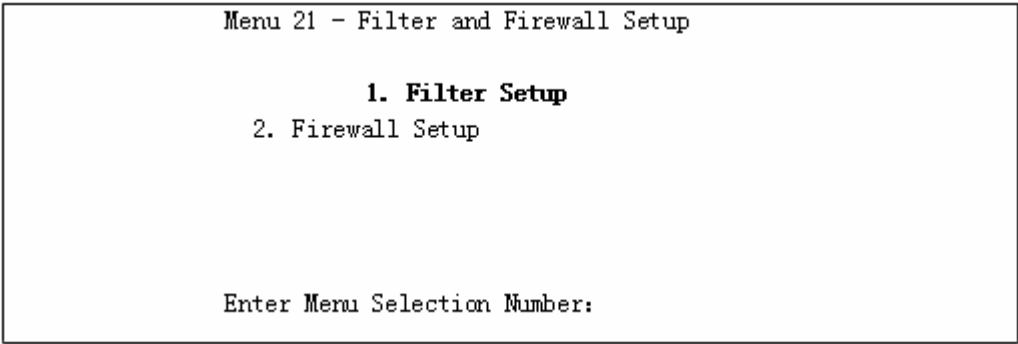
1. 阻止DoS 攻击和黑客入侵您的网络。
2. 当需要设置复杂的规则的时候，较好的选择就是在一条防火墙规则中规定出一组源和目的IP 地址和端口号。
3. 有选择地允许/拒绝在内部主机/网络与外部主机/网络之间的由外网向内网或由内网向外网的通信。记住，过滤器无法从IP 地址来区分通信是源自内部主机还是外部主机。
4. 如果您需要检查很多规则，防火墙比过滤器更好。
5. 如果您需要关于您的系统日常e-mail 报告或需要被攻击时报警，您应该使用防火墙。
6. 防火墙可以阻止某些特定的URL 的数据通信。URL 可以记录在一个访问控制列表（ACL）数据库里面。

32.3 配置一个过滤器

缺省情况下,ZyWALL配置了一个NetBIOS over TCP/IP的过滤规则。要配置其它的过滤器组，请按照下面的程序进行。

- 1 在主菜单中键入21，进入菜单21。

图 266 菜单 21： 过滤器和防火墙设置



- 2 键入1，进入如下菜单。

图 267 菜单 21.1： 过滤器设置

Menu 21.1 - Filter Set Configuration

Filter Set #	Comments	Filter Set #	Comments
1		7	
2		8	
3		9	
4		10	
5		11	
6		12	

Enter Filter Set Number to Configure= 0

Edit Comments= N/A

Press ENTER to Confirm or ESC to Cancel:

3. 选择一个您希望配置的过滤组（1-12）然后按回车键。
4. 在**Edit Comments**处输入一个描述名称或注释，然后按回车键。
5. 根据信息提示[Press ENTER to confirm]按回车键进入菜单**Menu 21.1.1 - Filte Rules Summary**。

该界面显示了过滤组中现有规则的概述下表包含了菜单的中一些缩写词的简短描述。

表169 在过滤器规则汇总界面中使用的缩写词

区域	描述
A	Active: “Y”表示规则被启用。“N”表示规则没有启用。
Type	过滤器规则类型: “GEN”是Generic（普通的）, “IP”是指TCP/IP。
Filter Rules	这些参数在这里是不被显示的。
M	More（更多）。 “Y”表示有更多的规则要检查, 这些规则由当前规则形成一个规则链。直到规则链的完成才能使动作产生作用。 “N”表示没有规则要被检查。您能指定一个动作, 比如, 发送封包, 丢弃封包或者检查下一个规则。对于后者, 下一个规则是不依赖刚被检查过的规则的。

m	Action Matched（行为不匹配）。 “F”表示立即转发该封包并跳过检查剩余规则。 “D”表示丢弃该封包。 “N”表示检查下一个规则。
n	Action Matched（行为不匹配）。 “F”表示立即转发该封包并跳过检查剩余规则。 “D”表示丢弃该封包。 “N”表示检查下一个规则。

协议依据过滤器规则而定，缩写词如下列表。

表 170 规则缩写词用法

缩写	描述
IP Pr SA SP DA DP	协议 源地址 源端口号 目的地址 目的端口号
GEN Off Len	Offset Length

请参考以下章节来了解更多关于配置过滤器规则的信息。

32.3.1 配置一条过滤器规则

如果需要配置一条过滤器规则，在菜单**Menu 21.1.1 - Filter Rules Summary**中输入相应的数值，然后按回车键，进入菜单**21.1.1.1**。

为了加快过滤速度，一个过滤器组中的所有的规则必须为同一级别，例如，协议过滤器或一般过滤器。一个过滤器组的级别是取决于您创建的第一条规则。当在一个端口应用 过滤器组的时候，请为协议和设备过滤器组提供分开的菜单区域。如果在设备过滤器区域 包含了一个协议过滤器，反之亦然，ZyWALL会提出警告并不允许您保存。

32.3.2 配置一个 TCP/IP 过滤器规则

该章节说明如何配置一条TCP/IP过滤器规则。TCP/IP规则允许您根据IP层以及上层协议进行配置，例如，UDP和TCP头。

想要配置TCP/IP规则，您可以从**Filter Type**区域中选择**TCP/IP Filter Rule**，然后按回车键，进入菜单**Menu 21.1.1.1 - TCP/IP Filter Rule**，如下图所示。

图 268 菜单 21.1.1.1： TCP/IP过滤规则

Menu 21.1.1.1 - TCP/IP Filter Rule

Filter #: 1,1

Filter Type= TCP/IP Filter Rule

Active= Yes

IP Protocol= 0

IP Source Route= No

Destination: IP Addr=

IP Mask=

Port #=

Port # Comp= None

Source: IP Addr=

IP Mask=

Port #=

Port # Comp= None

TCP Estab= N/A

More= No

Log= None

Action Matched= Check Next Rule

Action Not Matched= Check Next Rule

Press ENTER to Confirm or ESC to Cancel:

下表描述了如何配置您的TCP/IP过滤规则。

表 171 菜单 21.1.1.1： TCP/IP过滤器规则

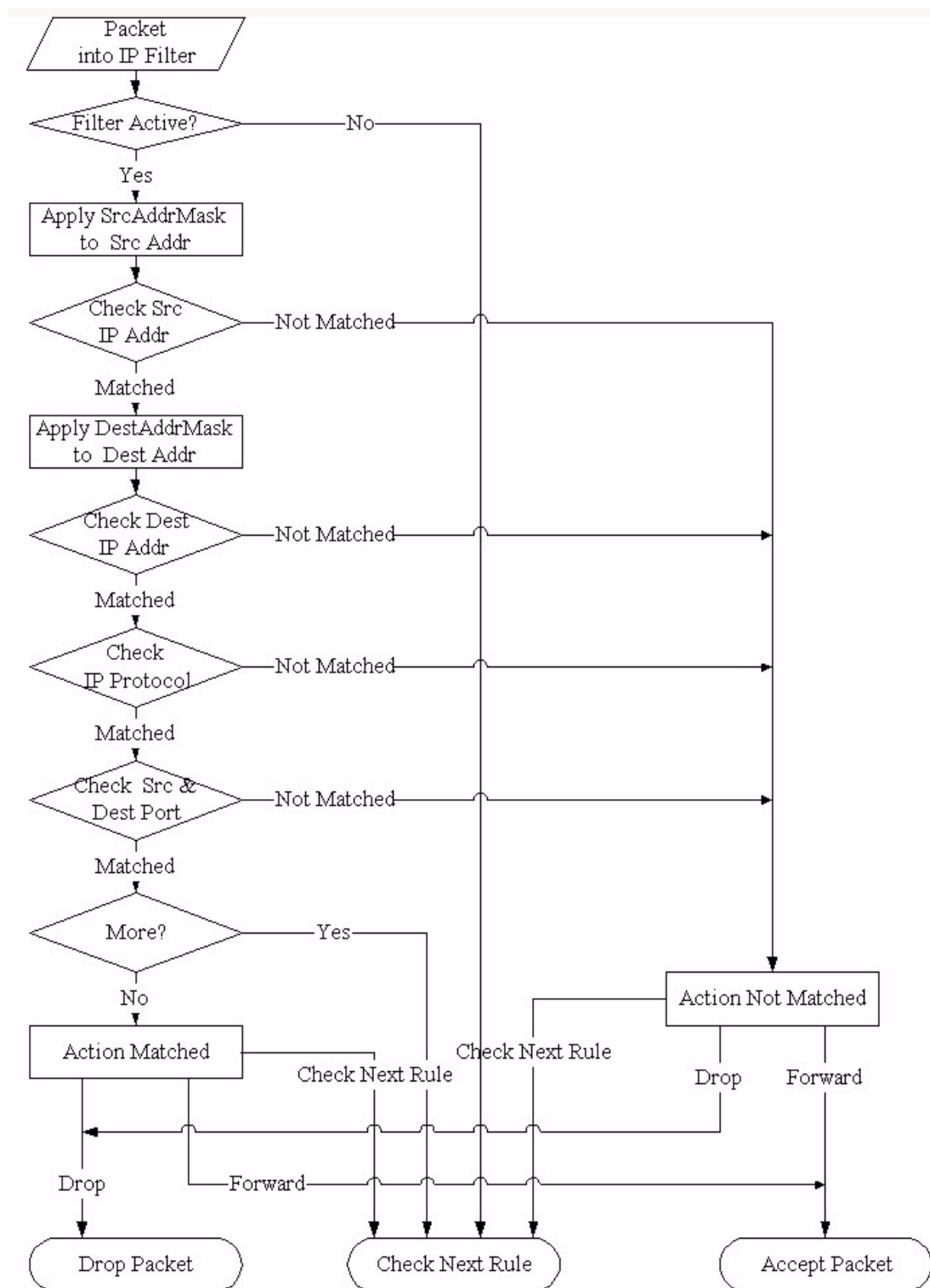
FIELD	DESCRIPTION
Active	先按空格键，然后按回车键选择 Yes 来激活该过滤器规则或选择 No 不启用该规则。
IP Protocol	协议请参考上层协议，例如，TCP是6，UDP是17，ICMP是1。在0和255之间输入一个值。0值可以匹配任何协议。

IP Source Route	先按空格键，然后按回车键选择 Yes ，给带有一个IP源路由选项的封包应用该规则。否则，该封包没有必要有一个源路由选项。多数IP封包是没有源路由的。
Destination	
IP Addr	该规则应用于的目的IP地址。如果地址是0.0.0.0，该处被忽略。
IP Mask	输入相应的子网掩码。
Port #	输入封包的目的端口号。该处的范围是从0到65535，如果是0的话将被忽略。
Port # Comp	先按空格键，然后按回车键来选择和 Destination: Port # 处的端口数值进行对比的方法。选项有 None ， Equal ， Not Equal ， Less 和 Greater 。
Source	
IP Addr	该规则应用于的源的IP地址。如果地址是0.0.0.0，该处被忽略。
IP Mask	输入相应的子网掩码。
Port #	输入封包的目的端口号。该处的范围是从0到65535，如果是0的话将被忽略。
Port # Comp	先按空格键，然后按回车键来选择和 Destination: Port # 处的端口数值进行对比的方法。选项有 None ， Equal ， Not Equal ， Less 和达式 Greater 。
TCP Estab	只有当IP协议为6（TCP）的时候该区域才会有效。先按空格键，然后按回车键选择 Yes ，这样该规则就会和想要建立一个TCP连接的封包相匹配（SYN=1和ACK=0）；如果选择 No ，则该处被忽略。
More	先按空格键，然后按回车键选择 Yes 或者 No 。如果选择 Yes ，在一个动作产生前，一个匹配的封包会被传到下一个过滤器规则。如果选择 No ，依照行为区域的设置来处理封包。 如果 More 是 Yes ， Action Matched 和 Action Not Matched 将会是 N/A 。

Log	先按空格键，然后按回车键从以下选择中选择一个日志记录选项： None - 没有封包将被记录。 Action Matched - 只有与规则参数相匹配的封包才会被记录。 Action Not Matched - 只有与规则参数不匹配的封包才会被记录。 Both - 所有封包都会被记录。
Action Matched	先按空格键，然后按回车键为一个匹配的封包选择一个行为。选项有 Check Next Rule, Forward和Drop。
Action Not Matched	先按空格键，然后按回车键为一个不匹配的封包选择一个行为。选项 Check Next Rule, Forward和Drop。
当您配置Menu 21.1.1.1 - TCP/IP Filter Rule的时候，看到提示信息“Press ENTER to Confirm”，您就可以按回车键保存您的配置，或按ESC键取消配置。这个数据就会显示在Menu 21.1.1 - Filter Rules Summary上。	

下图描述了一个IP过滤器的逻辑流程。

图 269 执行一个IP过滤器



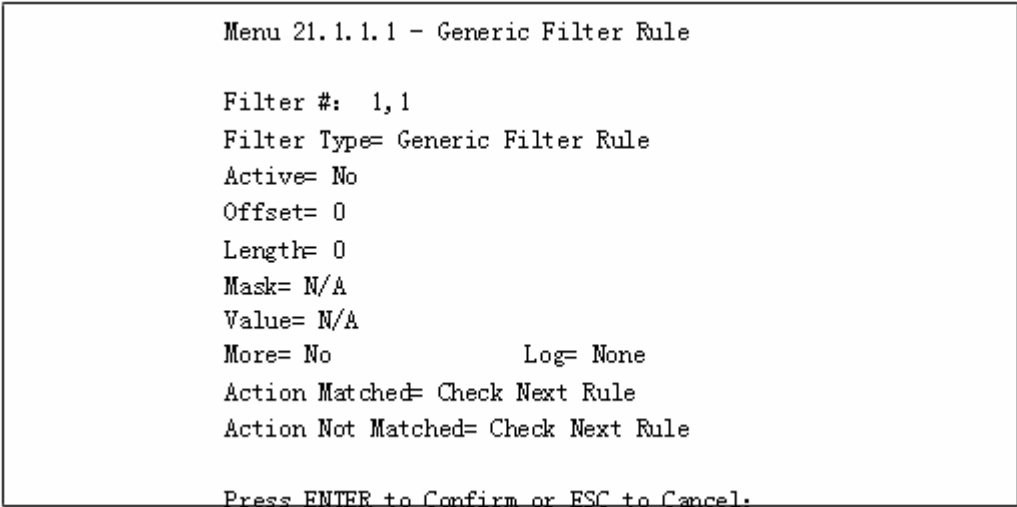
32.3.3 配置一个一般过滤器规则

本章描述了如何配置一个一般过滤器规则。一般规则的目的在于允许您过滤非IP封包。
对于IP封包，一般直接使用IP规则比较简单。

对于一般规则，当ZyWALL处理非IP或者IPX数据包时，会将一个数据包当作一个字节流来处理。您要规定数据包中的部分信息和与**Offset**（从0开始）和**Length**相匹配。在将 结果与确定一个匹配的数值进行比较之前 **ZyWALL**会给数据部份应用掩码**Mask**和**Value** 被指定采用十六进制数。注意它采取两个十六进制数字来表示一个字节，因此如果长度是**4**，任意一个区域中的值将采取**8**个数字，例如，FFFFFFF。

配置一个一般规则，请在菜单**21.1.1.1**里的**Filter Type**区域选择**Generic Filter Rule**，然后按回车键进入一般过滤器规则，如下图所示。

图 270 菜单 21.1.1.1： 一般过滤规则



下表是对**Generic Filter Rule**菜单的描述。

表 172 一般过滤器规则菜单区域

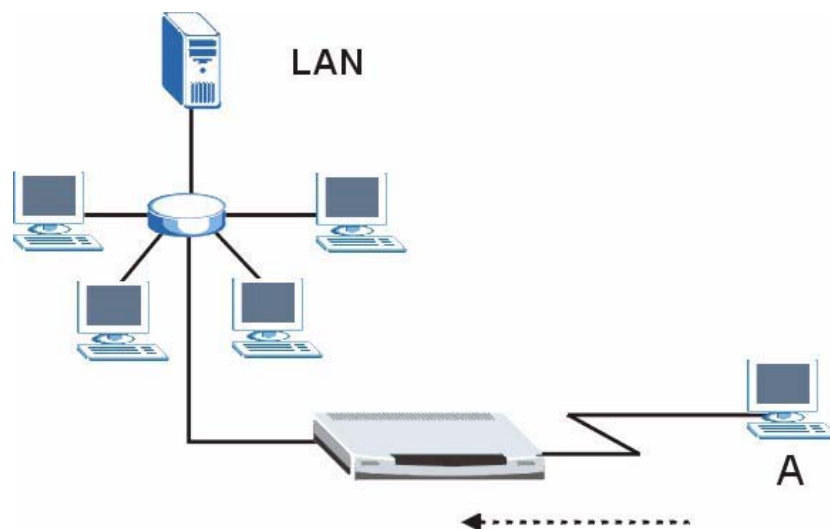
区域	描述
Filter #	这是过滤器组，如2, 3是指第二个过滤器组中的第三个过滤器规则。
Filter Type	先按空格键，然后按回车键选择一个规则类型。下面显示的参数对于每种类型都将会不同。一般过滤器规则允许过滤非IP封包，而TCP/IP过滤规则用于过滤器IP封包。 选项有 Generic Filter Rule 和 TCP/IP Filter Rule 。

Active	选择 Yes 启用过滤规则，选择 No 则是关闭该规则。
Offset	输入一个封包中您想要比较的数据的起始字节。范围从0到255。
Length	输入一个封包中您想要比较的数据字节长度。范围从0到8。
Mask	输入一个掩码（以十六进制形式），应用于比较的数据。
Value	输入一个用于比较的数值（以十六进制形式）。
More	如果选择 Yes ，在一个动作产生前，一个匹配的封包会被传到下一个过滤器规则。如果选择 No ，依照行为区域的设置来处理封包。 如果 More 是 Yes , Action Matched 和 Action Not Matched 将会是 No
Log	先按空格键，然后按回车键从以下选择中选择一个日志记录选项： None - 没有封包将被记录。 Action Matched - 只有与规则参数相匹配的封包才会被记录。 Action Not Matched - 只有与规则参数不匹配的封包才会被记录。 Both - 所有的封包都会被记录。
Action Matched	先按空格键，然后按回车键为一个匹配的封包选择一个行为。选项有 Check Next Rule , Forward 和 Drop 。
Action Not Matched	先按空格键，然后按回车键为一个不匹配的封包选择一个行为。选项 Check Next Rule , Forward 和 Drop 。
当您配置 Menu 21.1.1.1 - Generic Filter Rule 的时候，看到提示信息“Press ENTER to Confirm”，您就可以按回车键保存您的配置，或按ESC键取消配置。这个数据就会显示在 Menu 21.1.1 - Filter Rules Summary 上。	

32.4 过滤器实例

让我们来看一个如何阻止外网用户通过telnet访问ZyWALL的范例，更多的示例参见随机赠送的光盘。在下图中，A是使用telnet进入LAN的用户，箭头标出了进来的数据流。

图 271 Telnet 过滤器范例



1. 在主菜单中输入21，进入菜单**Menu 21 - Filter and Firewall Setup**。
2. 输入1，进入菜单**Menu 21.1- Filter Set Configuration**。
3. 输入一个您想要配置的过滤器的索引号（比如3）然后按回车键。
4. 在**Edit Comments**中输入一个描述性名称或注释然后按回车键。

5. 看到提示信息“Press ENTER to confirm”的时候按回车键，进入菜单**Menu 21.1.3 - Filter Rules Summary**。

6. 输入1，配置第一个过滤器规则（该组只有一个过滤器规则）如下图所示。

图 272 过滤器范例：菜单21.1.3.1

```
Menu 21.1.3.1 - TCP/IP Filter Rule

Filter #: 3,1
Filter Type= TCP/IP Filter Rule
Active= Yes
IP Protocol= 6          IP Source Route= No
Destination: IP Addr= 0.0.0.0
                IP Mask= 0.0.0.0
                Port #= 23
                Port # Comp= Equal
                Source: IP Addr= 0.0.0.0
                IP Mask= 0.0.0.0
                Port #= 0
                Port # Comp= None
TCP Estab= No
More= No                Log= None
Action Matched= Drop
Action Not Matched= Forward

Press ENTER to Confirm or ESC to Cancel:  Press Space Bar to Toggle.
```

telnet服务（TCP 协议）的端口号是23。请参阅RFC1060了解通用的端口号。

当您按回车键进行确认时，您将看到以下界面。注意在该组中只有一个过滤器规则。

图 273 过滤器规则汇总范例：Menu 21.1.13

```
Menu 21.1.3 - Filter Rules Summary

# A Type                Filter Rules                M m n
-----
1 Y IP      Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP=23      N D F
2 N
3 N
4 N
5 N
6 N

Enter Filter Rule Number (1-6) to Configure: 1
```

这里显示您为目标telnet端口（**DP = 23**）配置并激活了（**A = Y**）一个TCP/IP过滤器 规则（**Type =IP, Pr = 6**）

M = N表示一个行为能立即发生。如果行为被匹配那么该行为是丢弃封包（**m = D**）如

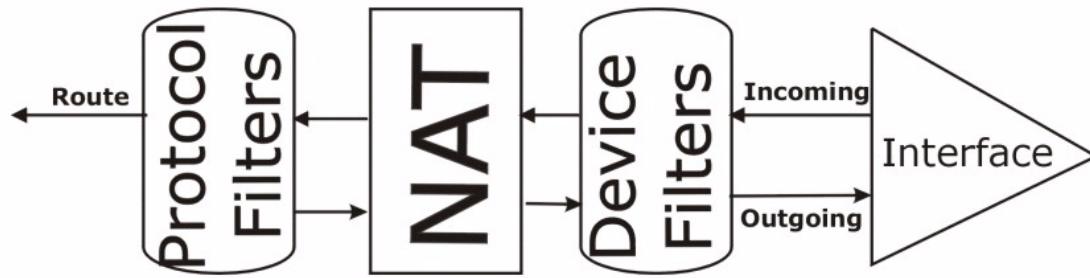
果行为不匹配无论是否有更多的规则被检查，那么行为就是立即转发封包（该例子中没有）。在您已经创建了过滤器组之后，您必须应用它。

1. 在主菜单中输入11，进入菜单11。
2. 输入1或2进入菜单**Menu 11.x - Remote Node Profile**。
3. 切换到**Edit Filter Sets**处，按空格键选择**Yes**，并按回车键。
4. 随后进入菜单**11.1.4**。按下图所示应用一个过滤器组（我们的范例为过滤器组3）
5. 在您输入组值后，按回车键进行确认并离开菜单**11.1.4**。

32.5 过滤器类型和 NAT

过滤器规则有两个级别，**Generic Filter**（设备）规则和**Protocol Filter**（TCP/IP）规则。一般过滤器规则对来往于LAN和WAN内的最原始数据起作用。而协议过滤器规则对IP封包起作用。一般过滤器和TCP/IP过滤器规则将会在下一章中有更详细的讨论。当NAT（网络地址转换，**Network Address Translation**）被启用的时候，在连接基础上的内部的IP地址和端口号会被取代这使得它在线路上不可能确切地知道该地址和端口因此，ZyWALL会对流出数据包在NAT之前和进入数据包在NAT之后对“本地的”IP地址和端口号应用协议过滤器。另一方面，一般或设备过滤器都可以应用于线路上的原始封包。当ZyWALL接收和发送封包时，它们就应用在该点上，例如，接口。接口可以是一个以太网或其它任何硬件端口。下列图表对此进行了描述。

图 274 协议和设备过滤器组



32.6 防火墙与过滤器

防火墙的配置在131页第8章进行讨论。我们随后对过滤器，NAT和防火墙进行比较。

32.7 应用一个过滤器

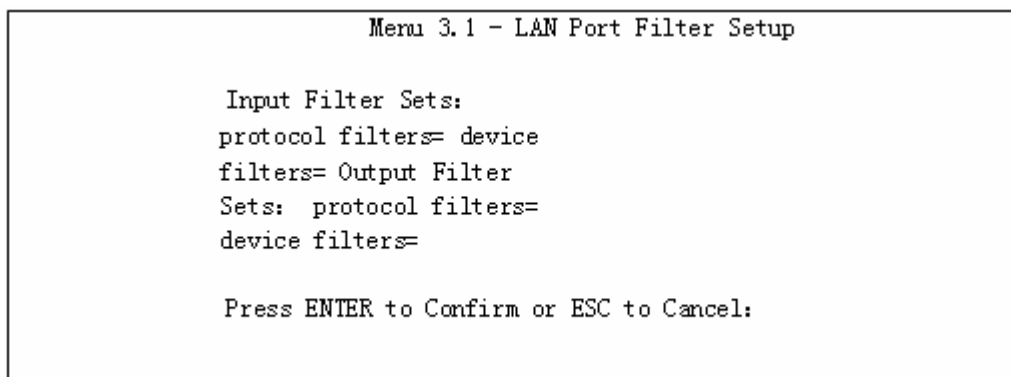
本章将会说明在哪里应用您设计的过滤器。ZyWALL已经预设了几个过滤器来阻止NetBIOS流量触发呼叫，以及进入的telnet，FTP和HTTP连接。

注意：如果您不激活防火墙，最好启用您的过滤器功能。

32.7.1 应用 LAN 过滤器

LAN流量过滤器非常便于阻止一些封包，以减少流量并预防安全漏洞。进入菜单3.1（如下图所示），然后输入您想要应用的适当的过滤器组的数值。通过利用逗号分离，您可以选择使用最多4个过滤器组（从12个中），例如，3，4，6，11。输入过滤器组可以对流入到ZyWALL的数据流进行过滤，输出过滤器组可以对来自ZyWALL的数据流进行过滤。对于PPPoE或PPTP的封装，您还有额外的选项来对远程节点的呼叫进行过滤。

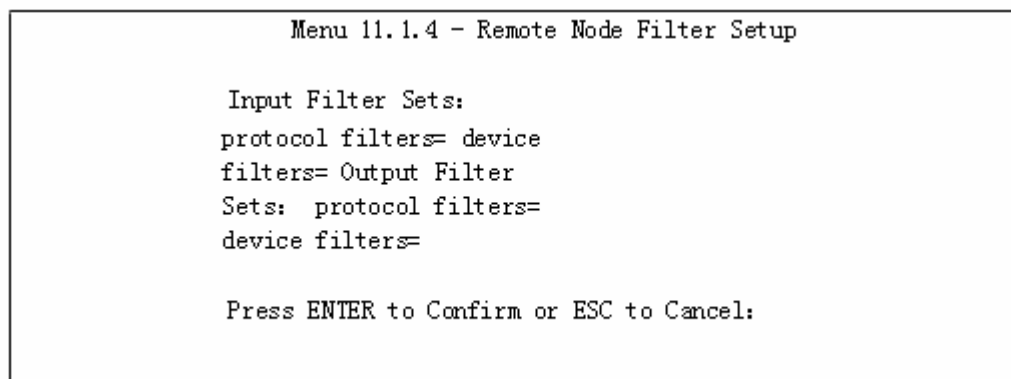
图 275 过滤LAN流量



32.7.2 应用远程节点过滤器

应用远程节点过滤器 进入菜单11.1.4（显示如下，注意目前只有PPPoE封装才有呼叫过滤器的设置）并且输入适当的过滤器组的数值。通过利用逗号分离，您可以选择使用最多4个过滤器组。输入过滤器组可以对流入到ZyWALL的数据流进行过滤，输出过滤器组可以对来自ZyWALL的数据流进行过滤。ZyWALL已经预置了过滤器来防止NetBIOS流量触发呼叫，并阻止进来的telnet，FTP和HTTP连接。

图 276 过滤器远程节点流量



第 33 章 SNMP 配置

本章将会向您介绍如何在菜单22中配置SNMP。

33.1 SNMP 配置

在主菜单中输入22，进入菜单**Menu 22 – SNMP Configuration**，如下所示。**Get**，**Set**和**Trap**处的“community”是SNMP的密码术语。

图277 菜单22：SNMP配置

Menu 22 - SNMP Configuration

SNMP:

Get Community= public Set

Community= public Trusted

Host= 0.0.0.0

Trap:

Community= public

Destination= 0.0.0.0

Press ENTER to Confirm or ESC to Cancel:

下表介绍了SNMP的配置参数。

表 173 SNMP配置菜单区域

区域	描述
Get Community	输入Get community，这是从管理端发送Get及GetNext请求的密码。
Set Community	输入Set community，这是从管理端发送Set请求的密码。
Trusted Host	如果您输入一个可信的主机，您的ZyWALL将仅对来自该地址的SNMP信息作出回应。一个空白区（默认）表示您的ZyWALL不管来源，将对它收到的所有的SNMP信息作出回应。
Trap	
Community	输入Trap community，这是随着每一个陷阱发送给SNMP管理员的密码。

Destination	输入您希望将SNMP陷阱发送到的站点的IP地址。
当您配置完该菜单的时候，如果看到提示信息“Press ENTER to Confirm”，您就可以按回车键保存您的配置，或按ESC键取消配置。	

33.2 SNMP 陷阱

当任何一个以下事件发生的时候，ZyWALL会将陷阱信息发送给SNMP管理者。

表174 SNMP陷阱

陷阱 #	陷阱名称	描述
0	coldStart (defined in RFC-1215)	当ZyWALL重新启动（开机）的时候会送出一个陷阱信息。
1	warmStart (defined in RFC-1215)	当ZyWALL软件重新启动的时候会送出一个陷阱信息。
4	authenticationFailure (defined in RFC-1215)	当接收到任何 community（密码）设置错误的 SNMP get或set信息的时候，会给管理员送出一个陷阱信息。
6	whyReboot (defined in ZYXEL- MIB)	当系统准备重新启动（热启动）的时候，在重启前，一个带有重启原因的陷阱信息会发送出去。
6a	For intentional reboot:	如果人为重新启动设备以后，一个带有 System reboot by user”信息的陷阱信息会发送出去，（例如，下载新的文件，CLI命令“sys reboot”等等）
6b	For fatal error:	如果系统由于致命的错误而重启，一个带有致命编码的信息的陷阱信息会被送出。

第 34 章 系统信息和诊断

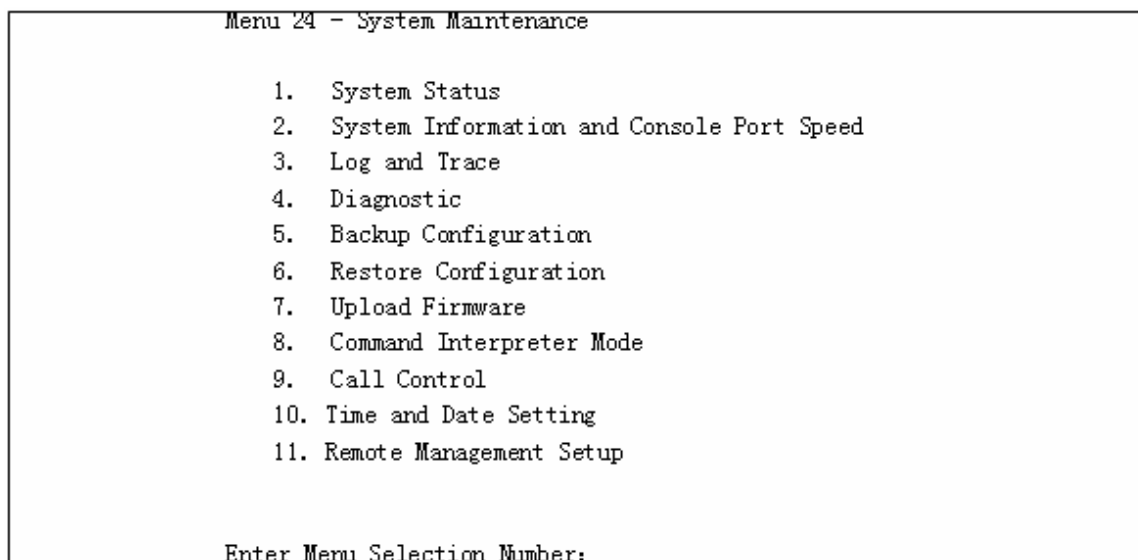
本章包括SMT菜单24.1到24.4

34.1 系统状况介绍

本章包括可以帮助您维护ZyWALL的诊断工具。这些工具包括系统状况，端口状况，日志和追踪能力的更新材料。

在主菜单中选择24，进入菜单**Menu 24 - System Maintenance, as shown below**。

图278 菜单 24： 系统维护



34.2 系统状况

第一个选项是系统状态，提供给您关于系统韧体的版本和端口统计的信息，如下图所示。系统状态是可用于监测 ZyWALL 的工具。具体地说，它提供给您关于系统韧体版本的信息、封包发送和收到的数量。

如果想获得系统状况的信息：

1. 输入数字24，进入菜单24- System Maintenance。
2. 在该菜单中输入1，进入菜单System Maintenance – Status。

3在Menu 24.1 - System Maintenance - Status中有三个命令 输入1可以断开WAN的连接，输入9可以重置计数器，按ESC键可以回到上一级菜单。

图 279 菜单 24.1： 系统维护： 状态

Menu 24.1 - System Maintenance - Status							07: 15: 51
							Fri. Mar. 31, 2006
Port	Status	TxPkts	RxPkts	Cols	Tx B/s	Rx B/s	Up Time
WAN	100M/Full	9521	105390	0	0	760	7: 25: 33
LAN	100M/Full	13438	10927	0	0	0	7: 25: 34
Port	Ethernet Address		IP Address		IP Mask		DHCP
WAN	00: 13: 49: 00: 00: 02		172.23.23.60		255.255.255.0		Client
LAN	00: 13: 49: 00: 00: 01		192.168.1.1		255.255.255.0		Server
System up Time:		7: 25: 39					
Name: test.domainname							
Routing: IP							
ZyNOS F/W Version: V4.00(XU.0)b2-2006.3.29 03/29/2006							
Press Command:							
COMMANDS: 1-Drop WAN 9-Reset Counters				ESC-Exit			

下表描述的是菜单Menu 24.1 - System Maintenance –Status的区域。这些区域是只读的并且用于诊断的目的。界面右上角显示时间和日期是按照您在菜单24.10中的设定显示的。

表 175 系统维护： 状态菜单区

区域	描述
Port	该处可以标识ZyWALL上的一个端口。
Status	对于LAN，DMZ和WLAN接口，该处会显示端口速率和双工模式。 对于WAN端口，如果您正在使用以太网的封装方式，该处会显示端口速率和双工模式。如果您正在使用PPPoE的封装方式，该处会显示Down（线路断开或没有连接），Idle（线路（ppp）空闲），Dial（开始触发一个呼叫）或Drop（断开呼叫）。
TxPkts	这是该端口上传数据包的数量。
RxPkts	这是该端口上收到数据包的数量。

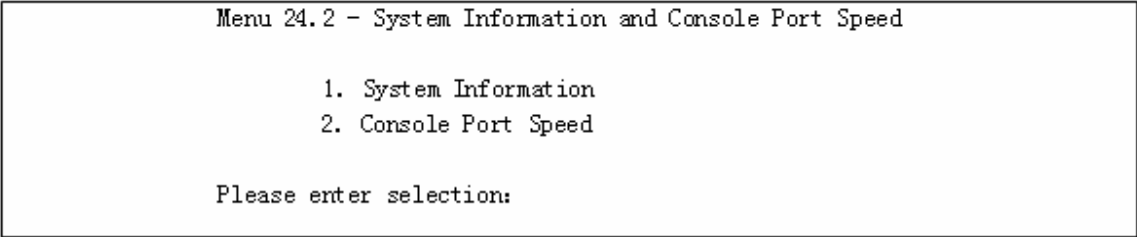
Cols	这是该端口上冲突的数量。
Tx B/s	这里显示端口上每秒的传输速度。
Rx B/s	这里显示端口上每秒的接收速度。
Up Time	这里显示线路激活的时间总和。
Ethernet Address	左边列出的是端口的以太网地址。
IP Address	左边列出的是端口的IP地址。
IP Mask	这是端口IP掩码。
DHCP	这是端口的DHCP设置。
System up Time	ZyWALL开启的时间总和。
Name	这处会显示在菜单1中分配的系统名和域名。例如，System Name=xxx; Domain Name= baboo.mickey.com。
Routing	显示使用的路由协议。对于ZyWALL配置本项为IP，不可配置。
ZyNOS F/W Version	显示ZyNOS版本的版本及相关数据，ZyNOS是 ZyXEL的网络操作系统软件。
输入1可以断开WAN的连接，输入9可以重置计数器，按ESC键可以回到上一级菜单。	

34.3 系统信息和控制口速度

本节介绍您的系统，并允许您选择不同的控制口速度。如何获得系统信息和控制口速度：

1. 输入24，进入菜单**Menu 24 - System Maintenance**。
2. 输入2，进入**Menu 24.2 - System Information and Console Port Speed**。
3. 如下图所示在该菜单中您有两个选择。

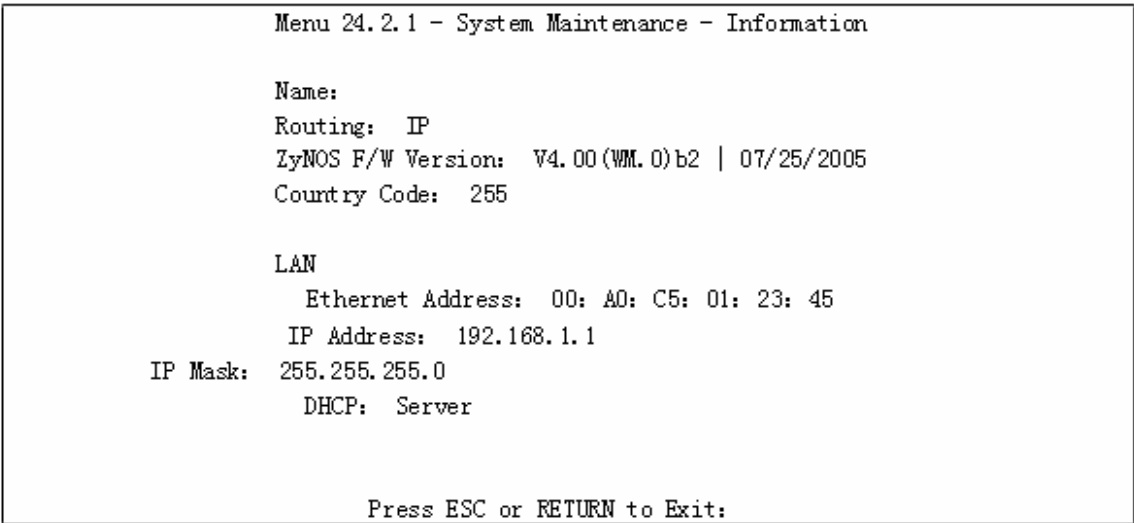
图280 菜单 24.2： 系统信息和控制口速度



34.3.1 系统信息

如下图所示,您可以获得关于系统的一些信息。并且您将获得更确切的关于路由协议,以太网地址, IP地址等等的信息。

图 281 菜单 24.2.1: 系统维护: 信息



以下为界面相关的描述。

表176 系统维护区域: 信息

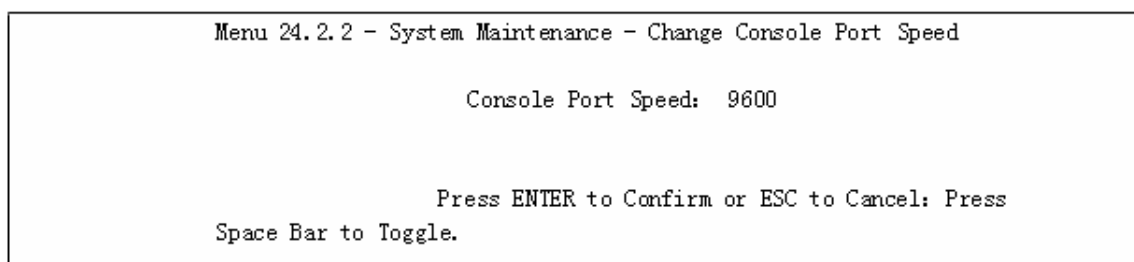
区域	描述
Name	这处会显示在菜单1中分配的系统名和域名。例如, System Name=xxx; Domain Name= baboo.mickey.com。
Routing	显示使用的路由协议。对于ZyWALL配置本项为IP, 不可配置。
ZyNOS F/W Version	显示ZyNOS韧本的版本及相关数据, ZyNOS是 ZyXEL的网络操作系统软件。
Country Code	显示韧体的国家代码。
LAN	

Ethernet Address	显示您的ZyWALL的以太网MAC（媒体访问控制）地址。
IP Address	这是ZyWALL的IP地址。
IP Mask	这是ZyWALL的IP掩码。
DHCP	这是ZyWALL的DHCP设置。
查看完毕，按ESC键或按回车键退出	

34.3.2 控制台端口速度

您可以在菜单**Menu 24.2.2 - Console Port Speed** 中修改控制口的速度。您的ZyWALL支持9600（默认）、19200、8400、57600和115200bps的速度。先按空格键，然后按回车键可以选择菜单24.2.2中预置的速度，如下所示。

图 282 菜单 24.2.2： 系统维护：更改控制口速度



34.4 日志记录和追踪

ZyWALL中有两个日志工具。第一个是错误日志和追踪记录。第二个是为信息记录的UNIX系统日志工具。

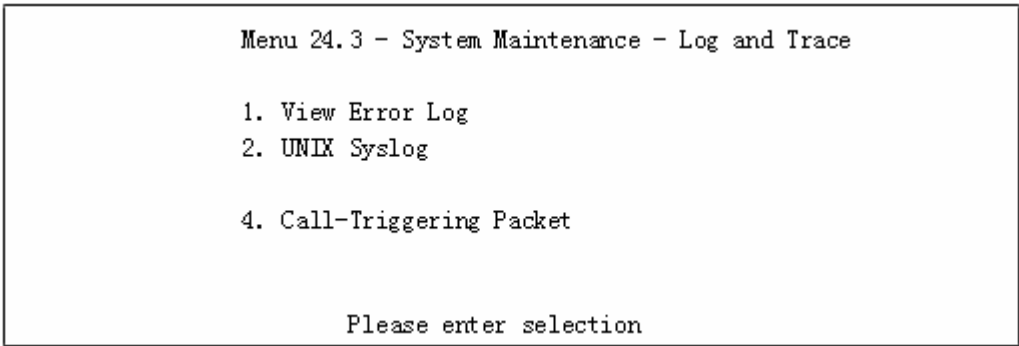
34.4.1 检查错误日志

当某事有问题的时候，您应该寻找线索来了解错误和追踪日志。您可以按照以下步骤来检查本地错误和追踪日志。

1. 在主菜单中选择24，进入菜单**Menu 24 - System Maintenance**。
2. 在菜单24中选择3，进入菜单**Menu 24.3 - System Maintenance - Log and Trace**。
3. 在菜单**Menu 24.3 - System Maintenance - Log and Trace**中选择第一个选项，可以显示系统中的错误日志。

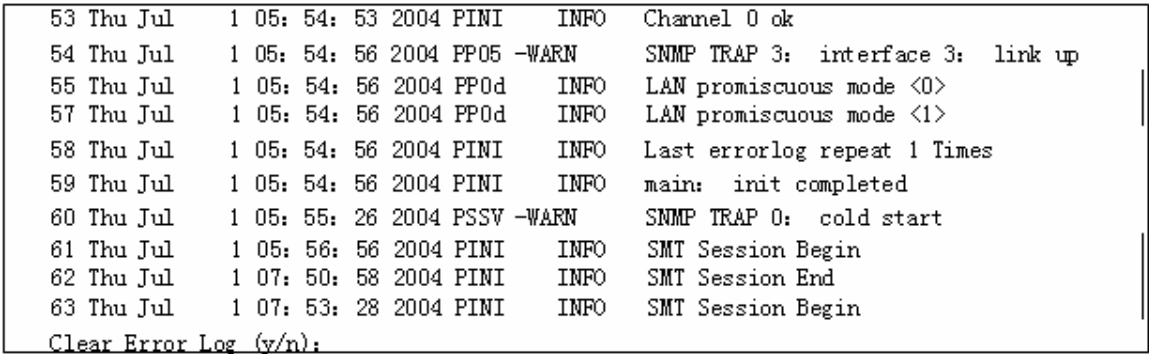
在ZyWALL完成显示后，还会有选项清除错误日志信息。

图283 菜单 24.3: 系统维护: 日志和跟踪



下图中是一些典型的错误例子和信息。

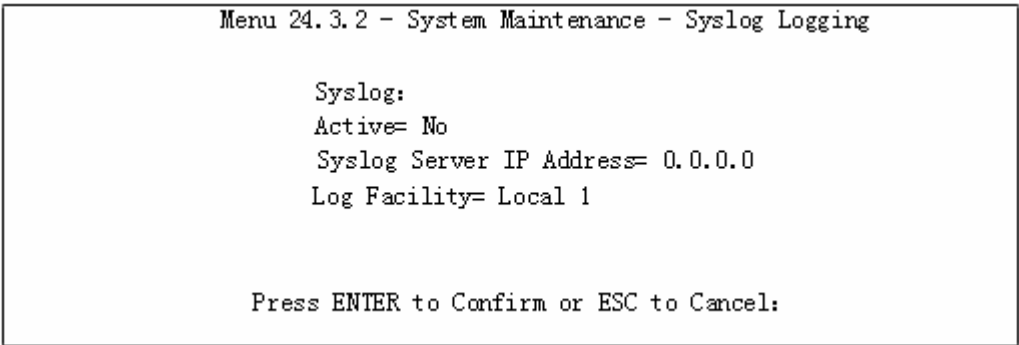
图 284 错误通知和信息的范例



34.4.2 系统日志

ZyWALL可以使用系统日志工具来记录发送到一个系统日志服务器的CDR（呼叫细节记录）和系统信息。系统日志和账目记录可以在**Menu 24.3.2 -System Maintenance - Syslog Logging**中配置，如下图所示。

图285 菜单 24.3.2: 系统维护 : 系统日志记录



您需要配置系统日志参数，在下表中将会有描述，激活系统日志功能后选择您想要记 录

的日志。

表 177 系统维护菜单：系统日志参数

区域	描述
Syslog:	
Active	先按空格键，然后按回车键打开或关闭系统日志功能。
Syslog Server IP Address	输入系统日志服务器的名称或IP地址，它会对您选择的日志种类作记录。
Log Facility	先按空格键，然后按回车键选择一个位置。日志工具允许您在系统日志服务器中将记录的信息保存到不同的文件里面请参考您的系统日志程序的文件来了解更多信息。
完成该界面的配置后，按回车键确认或按ESC键取消。	

您的ZyWALL会发送5种类型的系统日志信息。如下是一些带有它们的信息格式的系统日志信息的范例。

1 CDR

CDR Message Format
<pre> SdcmSyslogSend(SYSLOG_CDR, SYSLOG_INFO, String); String = board xx line xx channel xx, call xx, str board = the hardware board ID line = the WAN ID in a board Channel = channel ID within the WAN call = the call reference number which starts from 1 and increments by 1 for each new call str = C01 Outgoing Call dev xx ch xx (dev: device No. ch: channel No.) L02 Tunnel Connected(L2TP) C02 OutCall Connected xxxx (means connected speed) xxxxx (means Remote Call Number) L02 Call Terminated C02 Call Terminated Jul 19 11: 19: 27 192.168.102.2 ZyXEL: board 0 line 0 channel 0, call 1, C01 Outgoing Call dev=2 ch=0 40002 Jul 19 11: 19: 32 192.168.102.2 ZyXEL: board 0 line 0 channel 0, call 1, C02 OutCall Connected 64000 40002 Jul 19 11: 20: 06 192.168.102.2 ZyXEL: board 0 line 0 channel 0, call 1, C02 Call Terminated </pre>

2触发数据包

Packet triggered Message Format

```
SdcmSyslogSend( SYSLOG_PKTTRI, SYSLOG_NOTICE, String );
    String = Packet trigger: Protocol=xx Data=xxxxxxxxx...x
    Protocol: (1: IP 2: IPX 3: IPXHC 4: BPDU 5: ATALK 6: IPNG)
    Data: We will send forty-eight Hex characters to the server
Jul 19 11: 28: 39 192.168.102.2 ZyKEL: Packet Trigger: Protocol=1,
Data=4500003c100100001f010004c0a86614ca849a7b08004a5c020001006162636465666768696a
6b6c6d6e6f7071727374
Jul 19 11: 28: 56 192.168.102.2 ZyKEL: Packet Trigger: Protocol=1,
Data=4500002c1b0140001f06b50ec0a86614ca849a7b0427001700195b3e0000000600220008cd4
0000020405b4
Jul 19 11: 29: 06 192.168.102.2 ZyKEL: Packet Trigger: Protocol=1,
Data=45000028240140001f06ac12c0a86614ca849a7b0427001700195b451d143013500400007760
0000
```

3 过滤日志

```
SdcmSyslogSend(SYSLOG_FILTERLOG, SYSLOG_NOTICE, String );
String = IP[Src=xx.xx.xx.xx Dst=xx.xx.xx.xx prot=xxxx spo=xxxx dpo=xxxx] S04>R01mD IP[...] is the packet header and
S04>R01mD means filter set 4 (S) and rule 1 (R)...
match (m) drop (D)...
    Src: Source Address..
    Dst: Destination Address..
    prot: Protocol ("TCP", "UDP", "ICMP")..
spo: Source port..
dpo: Destination port
Mar 03 10: 39: 43 202.132.155.97 ZyKEL:
GEN[fffffffff0080] }S05>R01mF..
Mar 03 10: 41: 29 202.132.155.97 ZyKEL:
GEN[00a0c5f502f0080] }S05>R01mF Mar 03 10:
41: 34 202.132.155.97 ZyKEL: ..
IP[Src=192.168.2.33 Dst=202.132.155.93 ICMP] }S04>R01mF..
Mar 03 11: 59: 20 202.132.155.97 ZyKEL:
GEN[00a0c5f502f0080] }S05>R01mF Mar 03 12:
00: 52 202.132.155.97 ZyKEL:
GEN[fffffffff0080] }S05>R01mF..
Mar 03 12: 00: 57 202.132.155.97 ZyKEL:
GEN[00a0c5f502010080] }S05>R01mF..
Mar 03 12: 01: 06 202.132.155.97 ZyKEL: ..
IP[Src=192.168.2.33 Dst=202.132.155.93 TCP spo=01170 dpo=00021] }S04>R01mF..
```

4 PPP记录

PPP Log Message Format↵
<pre> SdcmSyslogSend(SYSLOG_PPLOG, SYSLOG_NOTICE, String);↵ String = ppp: Proto Starting / ppp: Proto Opening / ppp: Proto Closing / ppp: Proto↵ Shutdown↵ Proto = LCP / ATCP / BACP / BCP / CBCP / CCP / CHAP/ PAP / IPCP / IPXCP↵ Jul 19 11: 42: 44 192.168.102.2 ZyXEL: ppp: LCP Closing Jul 19 11: 42: 49 192.168.102.2 ZyXEL: ppp: IPCP Closing Jul 19 11: 42: 54 192.168.102.2 ZyXEL: ppp: CCP Closing↵ </pre>

5 防火墙记录

Firewall Log Message Format↵
<pre> SdcmSyslogSend(SYSLOG_FIREWALL, SYSLOG_NOTICE, buf);↵ buf = IP[Src=xx.xx.xx.xx : spo=xxxx Dst=xx.xx.xx.xx : dpo=xxxx prot rule ↵ action]↵ Src: Source Address↵ spo: Source port (empty means no source port information) Dst: Destination Address↵ dpo: Destination port (empty means no destination port information)↵ prot: Protocol ("TCP", "UDP", "ICMP", "IGMP", "GRE", "ESP")↵ rule: <a,b> where a means "set" number; b means "rule" number. Action: nothing(N) block (B) forward (F)↵ 08-01-200011: 48: 41Local1.Notice192.168.10.10RAS: FW 172.21.1.80 : 137 -↵ >172.21.1.80 : 137 UDP default permit: <2,0> B↵ 08-01-200011: 48: 41Local1.Notice192.168.10.10RAS: FW 192.168.77.88 : 520 -↵ >192.168.77.88 : 520 UDP default permit: <2,0> B↵ 08-01-200011: 48: 39Local1.Notice192.168.10.10RAS: FW 172.21.1.50 ->172.21.1.50↵ IGMP<2> default permit: <2,0> B↵ 08-01-200011: 48: 39Local1.Notice192.168.10.10RAS: FW 172.21.1.25 ->172.21.1.25↵ IGMP<2> default permit: <2,0> B↵ </pre>

34.4.3 呼叫触发封包

呼叫触发封包会以一种简单易读的格式来显示关于触发拨出呼叫的封包的信息。下图为一个范例。

图286 呼叫-触发封包范例


```

IP Frame: ENET0-RCV Size:      44/  44   Time:  17: 02: 44.262
Frame Type:

  IP Header:
    IP Version                = 4
    Header Length              = 20
    Type of Service            = 0x00 (0) Total
    Length                     = 0x002C (44)
    Identification             = 0x0002 (2) Flags
                                = 0x00
    Fragment Offset            = 0x00
    Time to Live                = 0xFE (254) Protocol
                                = 0x06 (TCP) Header
    Checksum                   = 0xFB20 (64288)
    Source IP                  = 0xC0A80101 (192.168.1.1)
    Destination IP             = 0x00000000 (0.0.0.0)

  TCP Header:
    Source Port                = 0x0401 (1025)
    Destination Port           = 0x000D (13)
    Sequence Number            = 0x05B8D000 (95997952) Ack
    Number                     = 0x00000000 (0)
    Header Length               = 24
    Flags                      = 0x02 (...S.)
    Window Size                 = 0x2000 (8192)
    Checksum                   = 0xE06A (57450)
    Urgent Ptr                  = 0x0000 (0)
    Options                    =
      0000:  02 04 02 00

  RAW DATA:
    0000:  45 00 00 2C 00 02 00 00-FE 06 FB 20 C0 A8 01 01  E.....
    0010:  00 00 00 00 04 01 00 0D-05 B8 D0 00 00 00 00 00
    .....
    0020:  60 02 20 00 E0 6A 00 00-02 04 02 00
Press any key to continue...

```

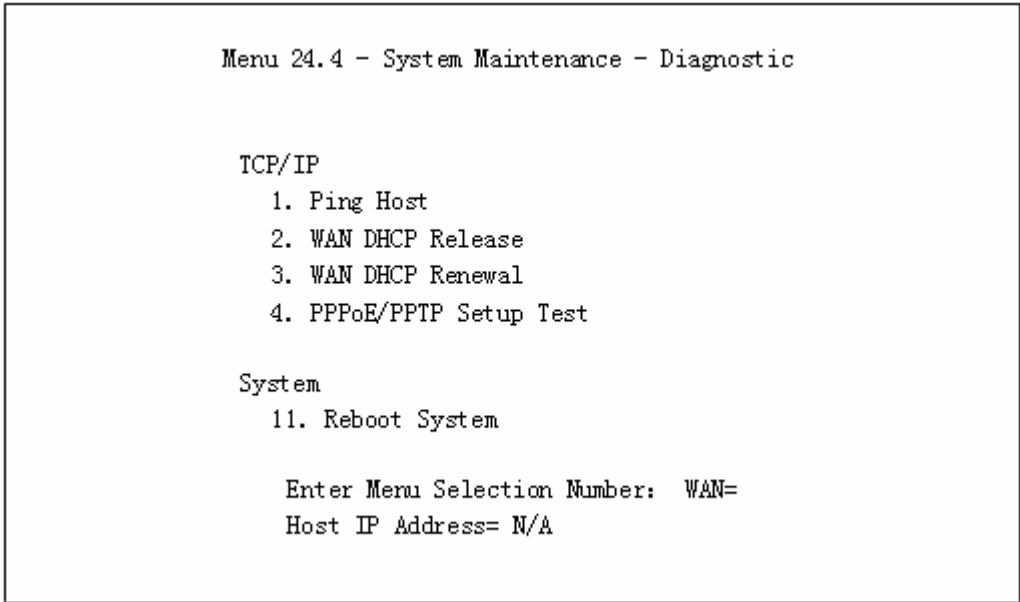
34.5 Diagnostic

诊断工具允许您测试ZyWALL 的不同方面来确定它是否工作正常。菜单24.4 允许您选择不同类型的诊断测试来评价系统，如下所示。

根据以下步骤进入菜单**Menu 24.4 - System Maintenance – Diagnostic**。

- 1. 在主菜单中输入24，进入菜单**Menu 24 - System Maintenance**。
- 2. 在该菜单中选择4，进入菜单**Menu 24.4 – System Maintenance – Diagnostic**。

图 287 菜单 24.4： 系统维护：诊断



34.5.1 WAN DHCP

在LAN或WAN上DHCP功能可以被激活，如图315所示。LAN DHCP已经讨论过了。ZyWALL能够作为WAN DHCP客户端（菜单4中的**IP Address Assignment** 或菜单11.x.2中选择**Dynamic**，菜单4中的**Encapsulation**或菜单11选择**Ethernet**）或者**None**（当您有一个静态IP）。菜单24.4的**WAN Release**和**Renewal**允许您发布和/或更新分配的WAN 口IP地址，子网掩码和默认网关。

下表描述了通过菜单24中的诊断来测试ZyWALL和相关连接可用的诊断测试。

表 178 系统维护菜单诊断

区域	描述
Ping Host	在LAN或WAN上输入1，可以ping任何一台机器（带有一个IP地址）在 Host IP Address 中输入它的IP地址。
WAN DHCP Release	输入2以释放WAN口的DHCP参数。
WAN DHCP Renewal	输入3来更新WAN口的DHCP参数。

PPPoE/PPTP Setup Test	输入4来测试互联网的设置。您也可以在菜单 Menu 4 – Internet Access 中测试互联网的设置。请参考339页27章，此特性仅对使用PPPoE or PPTP封装的拨号连接有效。
Reboot System	输入11重启ZyWALL。
WAN	如果您在 Enter Menu Selection Number 中输入2或3,那么在该处则要输入WAN口的数字。
Host IP Address	如果您在 Enter Menu Selection Number 中输入1，那么然后要输入您想Ping的计算机的IP地址。
输入您想要执行的选项的数字，或按ESC键取消。	

第 35 章 韧体和配置文件维护

本章将会介绍如何上传新的韧体和配置文件，如何备份和恢复配置文件。

35.1 介绍

您可以利用本章的介绍来修改ZyWALL的配置文件或升级韧体。配置ZyWALL后，可以备份配置文件到一台计算机上。如果不配置ZyWALL，可以上传备份文件以恢复以前的 设定。如果想返回ZyWALL到最初默认设置，可以上传出厂默认设置文件。韧体决定了 ZyWALL的可用的功能和特性。您可以从最近的ZyXEL FTP站点上下载新的韧体来提升 ZyWALL的性能。

35.2 文件名协定

配置文件（通常被称为romfile 或rom-0）包含出厂默认设置，例如密码，DHCP设置，TCP/IP设置等等。它是一个带有“rom”的扩展文件名，一旦您已经定制了ZyWALL的设置，它们可以用您所选择的文件名来保存到您的计算机上。

ZyNOS（ZyXEL网络操作系统有时称为“ras”文件）是系统韧体并且有一个“bin”的扩展名，对于FTP和TFTP客户端程序来讲，文件名如下类似：

```
ftp> put firmware.bin ras
```

这个FTP会话表示将计算机中的 “firmware.bin” 文件传输到ZyWALL中。

```
ftp> get rom-0 config.cfg
```

这个FTP会话表示将目前的配置存储到计算机的文件“config.cfg”中。

因为ZyWALL只认可“rom-0”及“ras”，如果FTP客户端不允许您的目的文件名与源文件名不同，则必须重新命名。一定保留两个文件的原副本。

下表为简单概述。请注意内部文件名引用了ZyWALL上的文件名，并且外部文件名引用的文件名不是ZyWALL上的，换句话说，在您的计算机，本地网络或FTP站点上，该文件名（但不是扩展名）是可以变化的。上传新的韧体后，查看菜单**Menu 24.2.1 - System Maintenance - Information**中的**ZyNOS F/W Version**项,确认您已经上传了正确的韧体。AT命令是当SMT菜单提示进入调试方式时，在您按“Y”后您输入的命令。

表179 文件名协定

文件类型	内部名	外部名	描述
配置文件	Rom-0	这是ZyWALL上的配置文件名。上传rom-0文件取代整个ROM文件系统，包括ZyWALL的配置，系统相关的数据（包含默认密码），	*.rom
韧体	Ras	这是ZyWALL上的ZyNOS韧体的称谓。	*.bin

35.3 备份配置

注意:ZyWALL显示不同的信息说明不同的备份方式。在菜单24.5,24.6,24.7和24.7.2中恢复和上传文件取决于您是使用串口还是采用telnet方式。

菜单**Menu 24 - System Maintenance**中的选项5允许您备份ZyWALL当前的配置到计算机上。一旦您的ZyWALL工作正常，强烈建议您备份一下当前的配置文件。由于FTP的速度较快，所以它是备份您当前配置的首选方式。您也可以在菜单24中用串口进行备份和恢复。任何串口通信程序都能够运行良好，然而，您必须使用Xmodem协议来进行下载或上传，并且您不必重新命名文件。

请注意术语“download（下载）”和“upload（上传）”。下载的意思是从ZyWALL传递到计算机，而上传的意思是将文件从您的计算机上传递到ZyWALL。

35.3.1 备份设置

请参考下图的介绍。

图288 telnet到菜单24.5

Menu 24.5 - Backup Configuration

To transfer the configuration file to your workstation, follow the procedure below:

1. Launch the FTP client on your workstation.
2. Type "open" and the IP address of your router. Then type "root" and SMT password as requested.
3. Locate the 'rom-0' file.
4. Type 'get rom-0' to back up the current router configuration to your workstation.

For details on FTP commands, please consult the documentation of your FTP client program.

For details on backup using TFTP

(note that you must remain in this menu to back up using TFTP), please see your router manual.

Press ENTER to Exit:

35.3.2 使用命令行来执行 FTP 命令

1. 在您的计算机上启动FTP客户端程序。
2. 输入“open”，接着按一下空格键，随后输入您的ZyWALL的IP地址。
3. 输入用户名，按回车键。
4. 依照请求输入密码（默认值为“1234”）
5. 输入“bin”设置转换模式为二进位的。
6. 利用“get”将文件从ZyWALL传递到计算机，例如，“get rom-0 config.rom”是指将配置文件从ZyWALL传递到您的计算机上并将文件重命名为“config.rom”。
7. 输入“quit”退出从提示符中退出。

35.3.3 来自命令行的 FTP 命令范例

图 289 FTP会话范例

```
331 Enter PASS command
Password:
230 Logged in
ftp> bin
200 Type I OK
ftp> get rom-0 zyxel.rom
200 Port command okay
150 Opening data connection for STOR ras
226 File received OK
ftp: 16384 bytes sent in 1.10Seconds
297.89Kbytes/sec.
ftp> quit
```

35.3.4 基于 GUI 的 FTP 客户端程序

下表描述了一些您在基于 GUI 的 FTP 客户端程序所能看到的命令。

表180 基于 GUI 的 FTP 客户端程序的一般命令

命令	描述
Host Address	输入主机服务器的地址。
Login Type	匿名的。采用匿名登录时,用户名和密码会自动地提供给服务器。 只有当您的ISP或网络管理员已经开启此项时,匿名登录才有效。 正常服务器登录需要一个独特的用户名和密码。
Transfer Type	既可以用ASCII（纯文本格式）码,也可以用二进制码来传递文件。
Initial Remote	指定默认的远程目录（路径）。
Initial Local Directory	指定默认的本地目录（路径）。

35.3.5 通过广域网进行文件维护

通过广域网进行的TFTP, FTP和telnet在以下一些情况下是不能实现的:

- 1.防火墙是激活的在菜单21.2中关闭防火墙或者创建一条防火墙规则来允许从WAN来访问)
- 2. 在菜单24.11中您已经禁用了远程管理的功能。
- 3. 在菜单3.1（LAN）或11.5（WAN）中您已经应用了一个过滤器来阻止远程管理。
- 4. 您在菜单24.11的Secured Client IP中输入的IP与客户端IP不匹配。如果不匹配的话, ZyWALL会立即断开远程管理会话。
- 5. 您正在进行一个SMT的管理。

35.3.6 使用 TFTP 备份配置文件

利用LAN上的TFTP（Trivial File Transfer Protocol，小文件传输协议），ZyWALL支持 韧体和配置文件的上传或下载。虽然TFTP需要通过广域网工作，但是不推荐使用。

如果想使用TFTP，您的计算机必须有telnet和TFTP客户端程序。请依照以下步骤来备份配置文件。

1. 首先从您的计算机telnet到ZyWALL并登录。由于TFTP没有任何安全机制，所以ZyWALL只会记录下该telnet客户端的IP地址，并接受来自该地址的TFTP请求。
2. 在菜单**Menu 24 – System Maintenance**中输入8，进入命令行模式。
3. 输入命令“**sys stdio 0**”使SMT闲置时间失效，这样TFTP传输将不会被打断。
文件传输完毕后，输入命令“**sys stdio 5**”恢复SMT5分钟闲置时间（默认）。
4. 启动您计算机上的TFTP客户端程序并连接到ZyWALL。在开始数据传输前设置传输模式为二进制。
5. 使用TFTP客户端程序（查看下面的范例）将文件从ZyWALL传到计算机。配置文件名为“rom-0”（rom-zero，并非大写字母O）。

注意：对于UNIX来讲，利用“get”将文件从ZyWALL传输到计算机，并且将“binary”设置为二进制的传输模式。

35.3.7 TFTP 命令范例

以下为TFTP命令范例。

```
tftp [-i] host get rom-0 config.rom
```

这里“i”是指二进制传输模式（当传输二进制文件时使用该模式），“host”是ZyWALL 的IP地址，“get”是将ZyWALL上的原始资料（rom-0，ZyWALL上的配置文件名）传送给计算机上的目标文件，并将其重命名为config.rom。

35.3.8 基于 GUI 的 TFTP 客户端程序

下表描述了您能够看到的基于GUI的TFTP客户端程序中的一些区域。

表181 基于GUI的TFTP客户端程序的一般命令

命令	描述
Host	输入ZyWALL的IP地址。192.168.1.1是ZyWALL的默认IP地址。

Send/Fetch	利用“Send”将文件上传到ZyWALL，利用“Fetch”将文件备份到您的计算机上。
Local File	输入韧体（.bin的扩展名）或配置文件（.rom的扩展名）在您的计算机上的路径和名称。
Remote File	这是 ZyWALL 上的文件名。韧体的文件名为“ras”，配置的文件名为“rom-0”。
Binary	以二进制模式传输文件。
Abort	停止文件的传输。

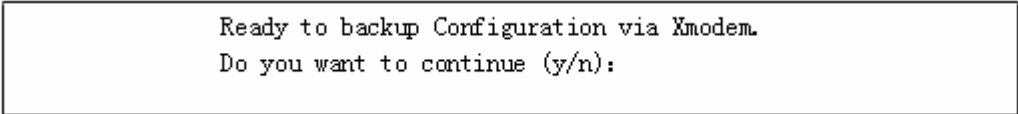
请参考章节35.3.5了解如何禁止通过广域网来实现TFTP和FTP的应用。

35.3.9 通过控制口进行备份

按如下超级终端程序所示通过控制口备份配置文件。

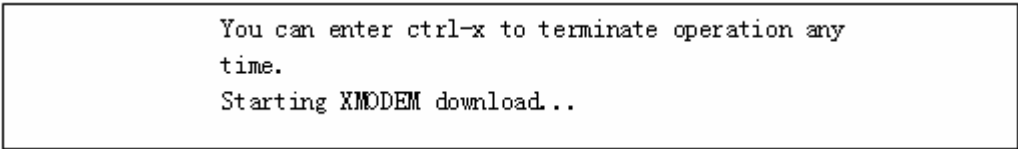
- 1 进入菜单24.5，并在如下界面输入“y”

图 290 系统维护：备份配置文件



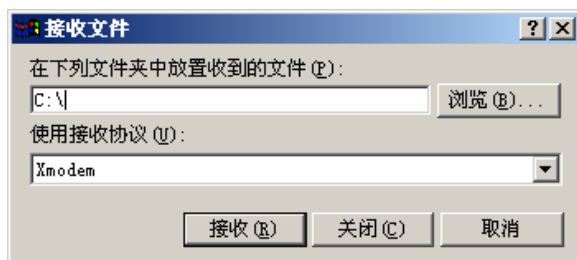
- 2 以下界面显示Xmodem下载已经开始。

图 291 系统维护：开始进行Xmodem下载界面



3. 按如下界面所示先点击呼叫，然后点击接收文件来运行超级终端程序。

图 292 备份配置文件范例



输入一个位置来存储配置文件或者点击**浏览**查找一个位置。

选择**Xmodem**协议。

然后点击**接收**。

4. 在成功地进行备份之后您将看到以下界面。按任意键返回到**SMT**菜单。

图 293 成功完成备份确认界面

```
** Backup Configuration completed. OK.  
### Hit any key to continue. ###
```

35.4 恢复配置

本节将告诉您如何恢复一个先前保存的配置。该动作会擦除当前的配置，请不要试图恢复配置，除非您在硬盘上已经有了一个备份的配置文件。

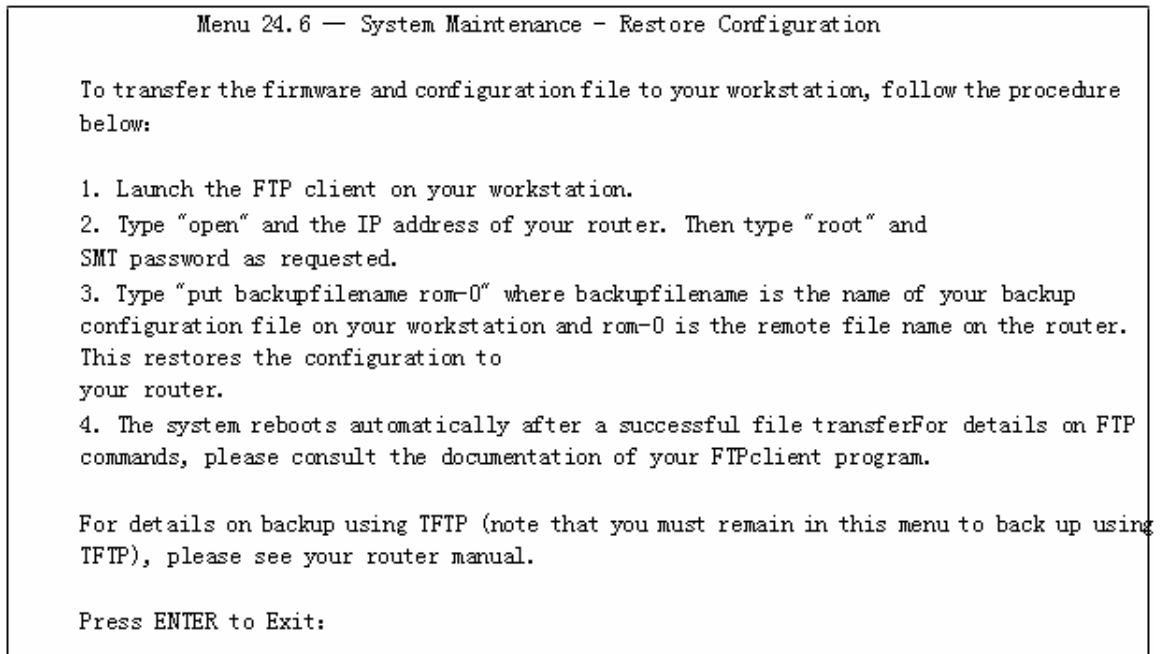
采用**FTP**的方式将您计算机中的配置文件发送给**ZyWALL**的速度较快，所以它是恢复配置的首选方式。请注意文件传输完成后您必须等待系统的自动重启。

注意：警告！不要终止文件的传输进程，这样会导致永久伤害您的**ZyWALL**。恢复配置进程完成后，**ZyWALL**将会自动重启。

35.4.1 利用 FTP 恢复

关于如何使用（T）**FTP**进行备份的详细信息，请参考本章中的**FTP**和**TFTP**文件上传内容。

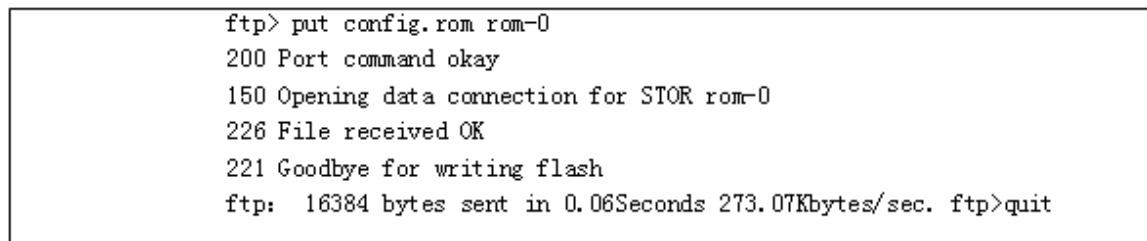
图 294 telnet到菜单24.6



1. 启动您计算机上的FTP客户端程序。
2. 输入“open”，接着按一下空格，然后输入您的ZyWALL的IP地址。
3. 输入用户名，按回车键。
4. 依照请求输入密码（默认值为“1234”）。
5. 输入“bin”设置传输模式为二进制的。
6. 在您计算机上找到您想要恢复到ZyWALL中的“rom”文件。
7. 利用“put”将文件从ZyWALL传递到计算机，例如，“put config.rom rom-0”是指将配置文件“config.rom”从ZyWALL传递到您的计算机上。
8. 输入“quit”退出ftp提示。当恢复工作完成后ZyWALL将自动重启。

35.4.2 利用 FTP 会话进行恢复的范例

图 295 利用FTP会话进行恢复的范例



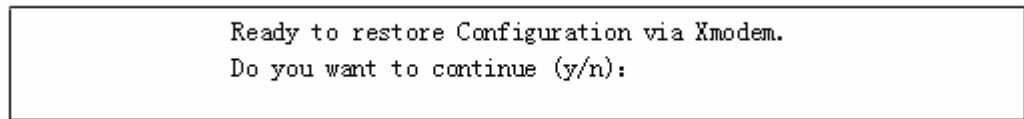
参考35.3.5 节阅读关于不允可WAN的TFTP 及 FTP。

35.4.3 通过串口恢复配置

通过串口恢复配置，请按照如下步骤来实现。

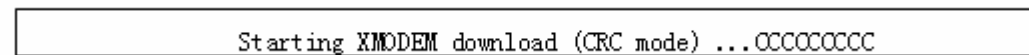
- 1 显示菜单24.6，并在如下界面中输入“y”。

图 296 系统维护：恢复配置



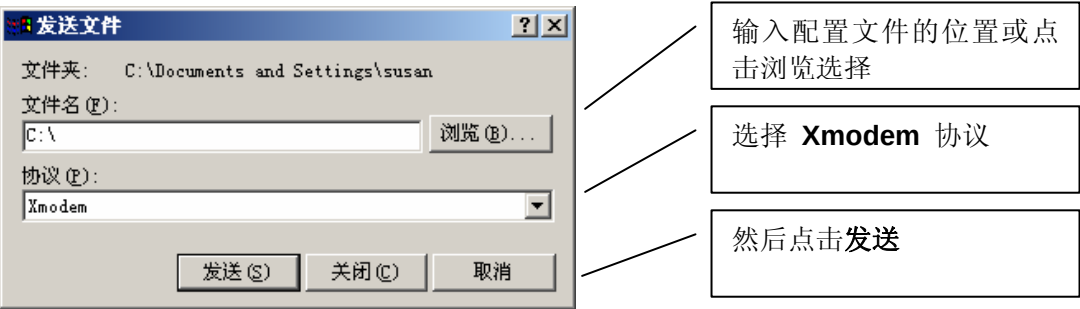
- 2 以下界面表示Xmodem下载已经开始。

图 297 系统维护：开始进行Xmodem下载界面



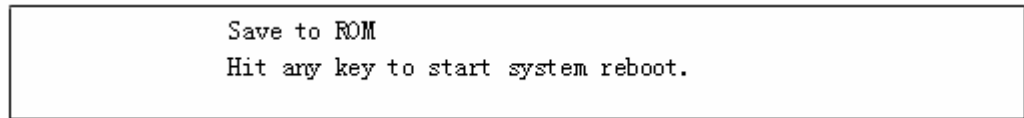
- 3 按照如下界面所示先点击**呼叫**，然后点击**发送**。

图 298 恢复配置范例



4. 恢复成功后您将会看到如下界面。按任意键重启ZyWALL并返回SMT菜单。

图 299 成功恢复配置界面



35.5 上传固件和配置文件

本节向您介绍如何上传固件和配置文件。您可以按照473页章节35.4的介绍或者是菜单**Menu 24.7.2 - System Maintenance - Upload System Configuration File**的介绍（通过 串口）来上传配置文件

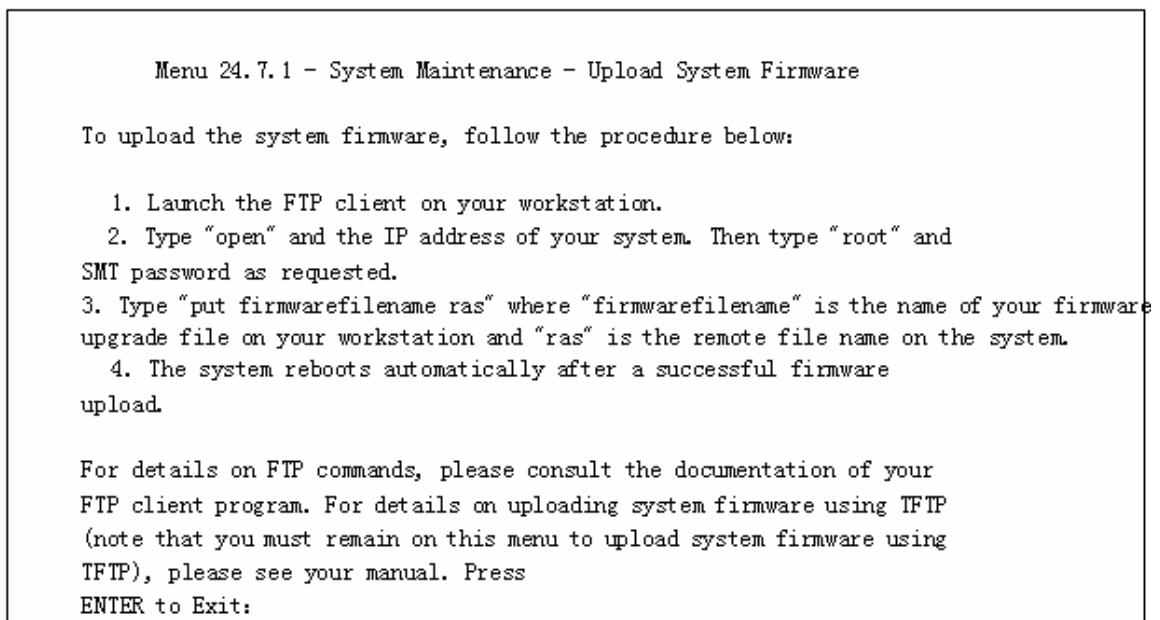
注意：警告！不要中断文件传输进程，因为这有可能会永久地损害您的ZyWALL。

35.5.1 韧体文件上传

FTP是上传韧体和配置的首选方法。要使用该功能，您的计算机必须有一个FTP客户端程序。

当您telnet到ZyWALL的时候，您会看到如下界面，介绍如何利用FTP来上传韧体和配置文件。

图 300 telnet到菜单24.7.1：上传系统韧体



35.5.2 配置文件上传

当您telnet到菜单24.7.2的时候，界面如下所示。

图 301 telnet到菜单24.7.2：系统维护

Menu 24.7.2 - System Maintenance - Upload System Configuration File

To upload the system configuration file, follow the procedure below:

1. Launch the FTP client on your workstation.
2. Type "open" and the IP address of your system. Then type "root" and SMT password as requested.
3. Type "put configurationfilename rom-0" where "configurationfilename" is the name of your system configuration file on your workstation, which will be transferred to the "rom-0" file on the system.
4. The system reboots automatically after the upload system configuration file process is complete.

For details on FTP commands, please consult the documentation of your FTP client program. For details on uploading configuration file using TFTP (note that you must remain on this menu to upload configuration file using TFTP), please see your manual.

Press ENTER to Exit:

上传固件和配置文件，以下为相关范例。

35.5.3 在 DOS 提示符下执行 FTP 文件上传命令的范例

1. 开启您计算机上的 FTP 客户端程序。
2. 输入"open"，按一下空格，随后输入 ZyWALL 的 IP 地址。
3. 出现提示要求输入一个用户名的时候按回车键。
4. 根据要求输入密码（默认值为"1234"）
5. 输入"bin"设置转换模式为二进制。

6. 利用"put"将文件从计算机传送到 ZyWALL，例如，"put firmware.bin ras"将计算机上的固件传到 ZyWALL，重命名为"ras"。同样，"put config.rom rom-0"将计算机上的配置文件传到 ZyWALL，重命名为"rom-0"。同样，"get rom-0 config.rom"命令把 ZyWALL上的配置文件传送到计算机上，重命名为"config.rom"。文件名规定详见本章前面的部分。

7. 输入"quit"退出 FTP。

35.5.4 固件文件上传的 FTP 会话范例

图 302 固件文件上传的FTP会话范例

```
331 Enter PASS command
Password:
230 Logged in ftp>
bin
200 Type I OK
ftp> put firmware.bin ras
200 Port command okay
150 Opening data connection for STOR ras
226 File received OK
ftp: 1103936 bytes sent in 1.10Seconds
297.89Kbytes/sec.
ftp> quit
```

本章前面列出了更多命令（在配置界面的FTP客户端）

请参考章节35.3.5来了解如何禁止从广域网上对ZyWALL进行TFTP和FTP的配置。

35.5.5 TFTP 文件上传

ZyWALL也支持在LAN上用TFTP上传韧体文件，虽然并不推荐使用这种方法。

用TFTP，您的计算机必须有telnet功能和TFTP客户端程序。根据下列步骤来传输韧体和配置文件。

1. 首先从您的计算机telnet到ZyWALL并登录。由于TFTP没有安全检查机制，所以ZyWALL会记录下telnet客户端的IP地址，并只接受从该地址发送的TFTP请求。
2. 在菜单Menu24 – System Maintenance中输入8进入命令行模式。
3. 输入命令“sys stdio 0”禁用控制口的空闲溢出，这样TFTP文件传输将不会被中断。当文件传输完成后，输入命令“sys stdio 5”恢复5分钟的控制口空闲溢出时间（默认）
4. 在您的计算机上开启TFTP客户端程序并连接到ZyWALL上。开始数据传输之前，把传输模式设为二进制。
5. 利用TFTP客户端程序（参阅以下范例）在ZyWALL和计算机之间传输文件。
韧体 文件名为“ras”。

注意在TFTP传输文件之前和传输期间，telnet连接必须是激活的并且ZyWALL处于命令行模式。详细的TFTP命令请参考您的TFTP客户端程序的文件。对于UNIX，用“get”可以将文件从ZyWALL传送到计算机，反之使用“put”，设置二进制的传输模式。

35.5.6 TFTP 上传命令范例

以下是一个TFTP命令的范例：

```
tftp [-i] host put firmware.bin ras
```

此处“i”代表二进制的传输模式，“host”是ZyWALL的IP地址，“put”是将计算机上的源文件（**firmware.bin** – 韧体在计算机上的名称）传输到远程主机上的目标文件（**ras** – 韧体在 ZyWALL上的名称）

在基于GUI的TFTP客户端程序上所能看到命令在本章早已列出来了。

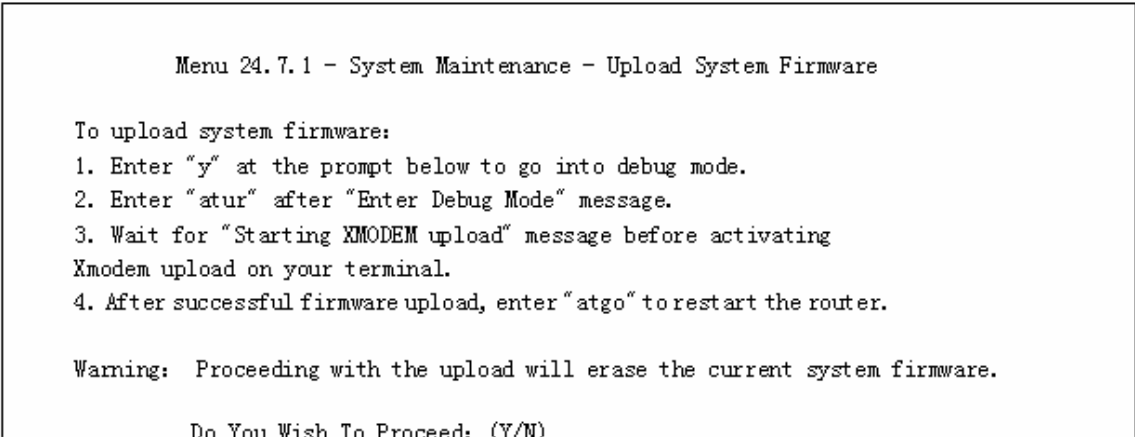
35.5.7 通过串口上传

对于将韧体上传到ZyWALL中，FTP或者TFTP是首选方法。然而，如果发生网络断线的话，上传文件只能通过串口直接传输到ZyWALL上。由于FTP或TFTP传输速度比较快，所以在通常的条件下并不推荐使用通过串口上传文件任何串行通信程序都可以正常使用；但是，您必须使用Xmodem协议来执行下载或上传。

35.5.8 通过串口上传韧体文件

1. 在菜单**Menu 24.7 – System Maintenance - Upload Firmware**中选择1，进入菜单**Menu 24.7.1 – System Maintenance – Upload System Firmware**，然后按照下图所示的流程进行上传。

图 303 菜单24.7.1 As Seen Using the Console Port

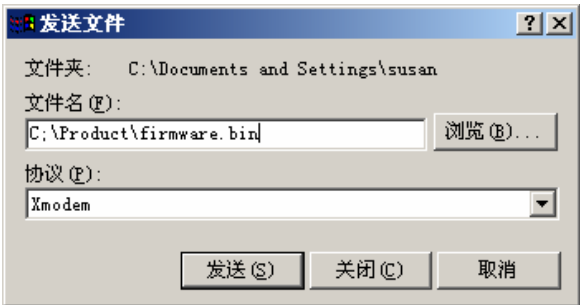


2. 在出现“Starting Xmodem upload”的提示后，选择Xmodem协议即可。

35.5.9 利用超级终端上传韧体范例

先点击呼叫，然后点击发送显示以下界面。

图 304 Xmodem上传范例



韧体上传完成后，输入“atgo”重启ZyWALL。

35.5.10 通过串口上传配置文件

1. 从菜单Menu 24.7 – System Maintenance – Upload Firmware中选择2，进入菜单Menu 24.7.2 - System Maintenance - Upload System Configuration File。根据以下界面的介绍操作。

图 305 菜单24.7.2 As Seen Using the Console Port

Menu 24.7.2 - System Maintenance - Upload System Configuration File

To upload system configuration file:

1. Enter "y" at the prompt below to go into debug mode.
2. Enter "atlc" after "Enter Debug Mode" message.
3. Wait for "Starting XMODEM upload" message before activating Xmodem upload on your terminal.
4. After successful firmware upload, enter "atgo" to restart the system.

Warning:

1. Proceeding with the upload will erase the current configuration file.
2. The system's console port speed (Menu 24.2.2) may change when it is restarted; please adjust your terminal's speed accordingly. The password may change (menu 23), also.
3. When uploading the DEFAULT configuration file, the console port speed will be reset to 9600 bps and the password to "1234". Do You Wish To Proceed: (Y/N)

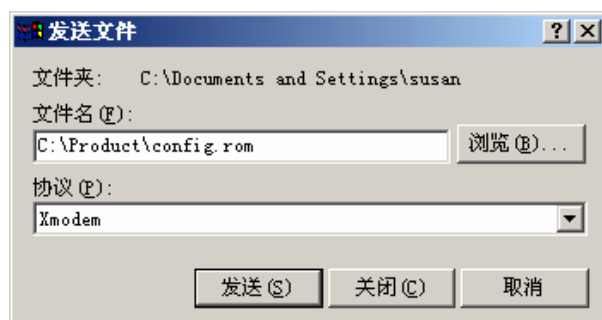
2 在出现“Starting Xmodem upload”的提示后，在您计算机中激活 Xmodem协议。按在前面超级终端程序中显示的过程，对于其它串口，此过程应是类似的。

3 输入“atgo”重启 ZyWALL。

35.5.11 利用超级终端上传配置范例

先点击**呼叫**，然后点击**发送**，显示以下界面。

图 306 Xmodem上传范例



配置上传完成后，输入“atgo”重启ZyWALL。

第 36 章 系统维护菜单 8 到 10

本章将会向您介绍SMT菜单24.8到24.10。

36.1 命令解释程序模式

命令解释程序（CI）是路由本体的一部分。CI提供了与SMT相同的功能，如添加一些低级的设置和诊断功能。您可以进入菜单24.8来执行CI命令。虽然有一些命令只会在串口连接的时候有效，但是您通过串口或telnet都可以进入CI模式。更多关于CI的信息请参考附赠的光盘或zyxel.com。

注意：使用非事实证明的命令或错误的配置会损坏部分系统并可能致使它不能使用。

图 307 在菜单 24 中的命令模式

```
Menu 24 - System Maintenance
  1. System Status
  2. System Information and Console Port Speed
  3. Log and Trace
  4. Diagnostic
  5. Backup Configuration
  6. Restore Configuration
  7. Upload Firmware
  8. Command Interpreter Mode
  9. Call Control
 10. Time and Date Setting
 11. Remote Management Setup

Enter Menu Selection Number:
```

36.1.1 命令语法

命令关键字的字体为courier new字体。

输入如下所示的确切的命令关键字，不要缩写。

命令中的必需区域在<>中。

命令中的可选区域在[]中。

| 符号表示或者。

例如，

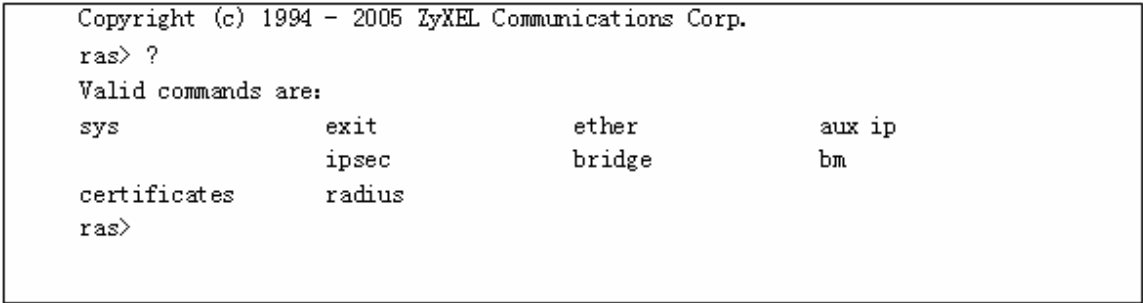
```
sys filter netbios config <type> <on|off>
```

表示您必须指定netbios过滤器的类型和是否关闭或开启。

36.1.2 命令用法

通过输入命令help或者?来查找命令列表。命令必须是完整的。需要结束时，输入exit即可返回SMT主菜单。

图 308 有效的命令



下表为该界面中一些命令的描述。

表182 有效的命令

命令	描述
sys	系统命令，显示设备的信息和配置情况。
exit	返回SMT主菜单。
ether	显示以太网信息及其配置情况。
aux	显示拨接备份情况和控制拨接备份连接。
ip	显示IP信息和IP配置。
ipsec	显示IPSec信息及其配置情况。
bridge	显示网桥信息。
bm	显示带宽管理设置及其配置情况。
certificates	显示验证信息及其配置情况。
radius	显示RADIUS及其配置信息。

36.2 呼叫控制支持

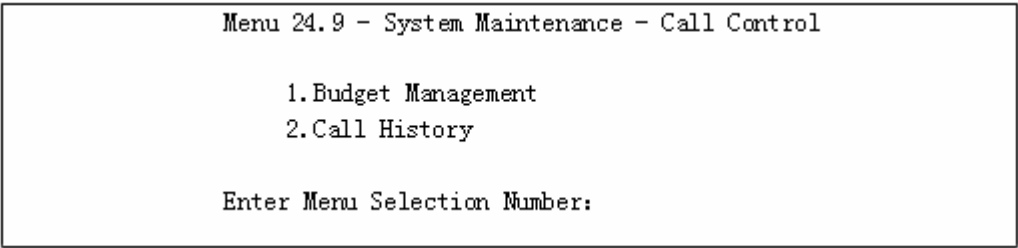
yWALL提供两个呼叫控制功能：预算管理 and 呼叫历史记录。请注意只有当菜单4或菜单11.1中的Encapsulation被设定为PPPoE或PPTP的时候才可用。

预算管理功能允许您对一定时间内ZyWALL呼出时间总额设定一个界限。当所有呼出时间超过了这个限制，那么当前呼叫会断开并中断所有即将发出的呼叫。

呼叫历史记录会记录之前收到和发出的呼叫。

进入呼叫控制菜单，选择菜单24中的选项9，进入菜单 **Menu 24.9 - System Maintenance - Call Control**，如下图所示。

图309 呼叫控制



36.2.1 预算管理

菜单24.9.1 显示了预算管理对发出的呼叫的统计。在**Menu 24.9 - SystemMaintenance - Call Control**中输入1，显示如下菜单。

图310 预算管理

Menu 24.9.1 - Budget Management		
Remote Node Period	Connection Time/Total Budget	Elapsed Time/Total
1.ChangeMe	No Budget	No Budget
2.Dial	No Budget	No Budget
Reset Node (0 to update screen):		

全部的预算是发送到远程节点的呼叫的时间界限。当到达该界限时，呼叫将会断开并且更多的发送到远程节点的呼叫将被中断。每个周期后，全部预算将会重置。默认预算是0 分钟，周期是0 小时，表示没有预算控制。您可以在该菜单中通过输入一个远程节点的索引号来重新设定累积的连接时间。输入0 来更新界面。预算和重置周期可以在菜单11.1中为远程节点配置。

表 183 预算管理

区域	描述	范例
Remote Node	输入远程节点的索引号	1
Connection Time/ Total Budget	这是已经用完的全部连接时间（在菜单11.1分配的预算内）。	5/10表示已经用完了5分钟,而10分钟表示全部的预算。
Elapsed Time/Total Period	这个周期是指在一段时间（以小时为单位）内分配的预算被重置的循环时间。 Elapsed Time是指在这个周期内所用完的时间。	0.5/1表示 30分钟已经用完,而1小时表示一个循环周期。
输入“0”可以更新界面或按ESC键返回上一个界面。		

36.2.2 呼叫历史记录

这是菜单Menu 24.9 - System Maintenance - Call Control的第二个选项。显示了关

于过去收到和发出的呼叫。在菜单**Menu 24.9 – System Maintenance - Call Control**中输入**2**进入以下的菜单。

图 311 呼叫记录

Menu 24.9.2 - Call History

Phone Number	Dir	Rate	#call	Max	Min	Total
1.						
2.						
3.						
4.						
5.						
6.						
7.						
8.						
9.						
10.						

Enter Entry to Delete (0 to Exit):

以下为界面相关的描述

表 184 呼叫记录

区域	描述
Phone Number	显示PPPoE服务名。
Dir	显示呼叫是收到的还是发出的。
Rate	呼叫的传输速度。
#call	这是从电话号码上收到的或者发出的呼叫号。
Max	这是最长的打电话的时间的长度。
Min	这是最短的打电话的时间的长度。
Total	这是所有拨出电话或收到的呼叫的全部长度。
您可以输入一个编号来删除它或者输入“0”退出。	

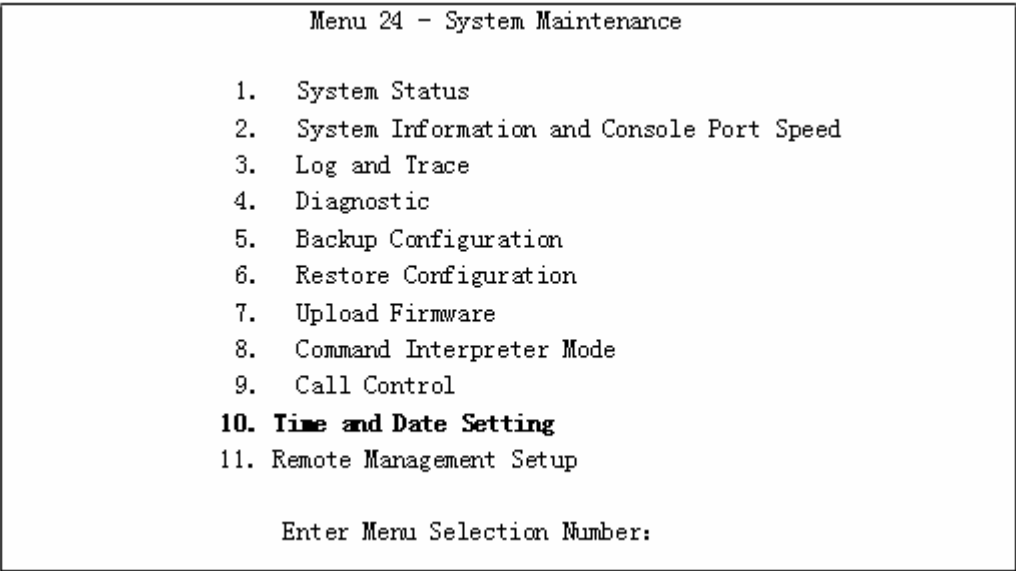
36.3 设置时间和日期

有一个软件机制在您开启ZyWALL时人工地设定时间或者从一个外部服务器获取当前时间和日期。菜单**24.10**允许您更新ZyWALL的时间和日期设定，实时时间在日志

中显示。

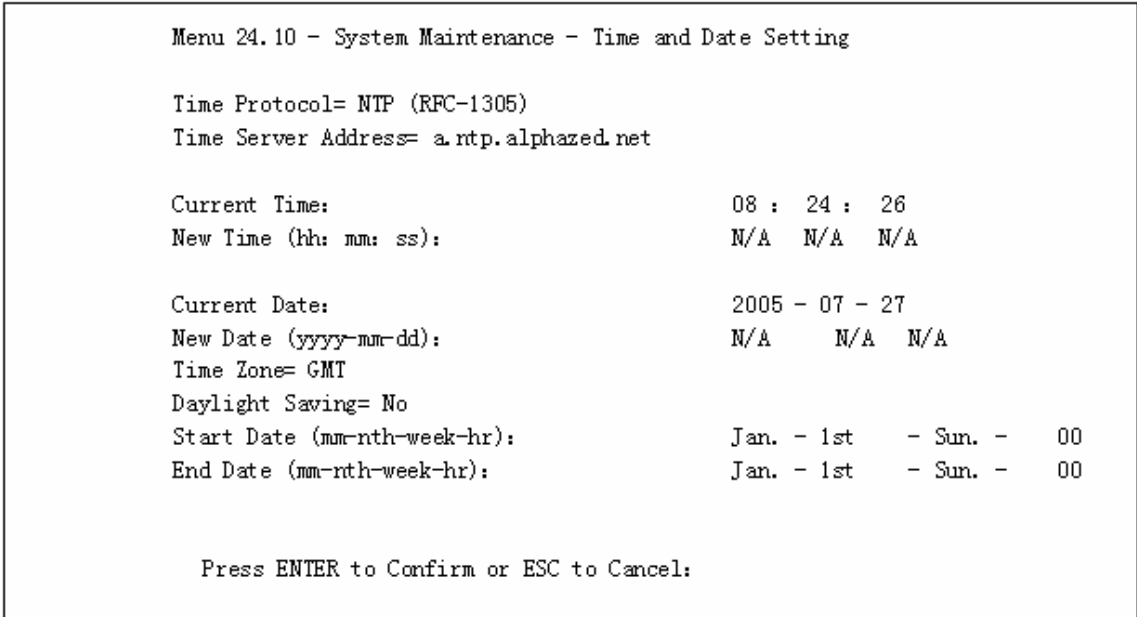
在主菜单中，选择24进入菜单**Menu 24 - System Maintenance**，如下所示。

图312 菜单24：系统维护



输入10进入菜单**Menu 24.10 - System Maintenance - Time and Date Setting**来更新 ZyWALL的时间和日期设定，如以下界面所示。

图313 菜单24.10 系统维护：时间和日期的设置



下表为界面相关的描述。

表 185 菜单24.10 系统维护：时间和日期的设置

区域	描述
Time Protocol	输入您的时间服务器使用的时间服务协议。不是所有的时间服务器支持所有的协议，您可能需要咨询您的ISP或网络管理员或者反复试验来找到一个合适的协议。它们之间主要的不同在于格式。 Daytime (RFC 867) 格式是day/month/year/time zone。 Time (RFC-868) 格式有一个4个字节的整数并且完整到秒数，如1970/1/1 at 0: 0: 0。 缺省情况下NTP (RFC-1305)与Time (RFC-868)类似。选择Manual可以手动输入新的时间和日期。
Time Server Address	输入时间服务器的IP地址或域名。假如您对该信息不确定，请与您的ISP或网络管理员。默认值为 tick.stdtime.gov.tw 。
Current Time	只有在您重新进入该菜单时才会显示一个更新过的时间。
New Time	以小时，分钟，秒的格式输入新的时间。只有您在 Time Protocol 处选择了 Manual 的时候才可用。
Current Date	只有在您重新进入该菜单时才会显示一个更新过的日期。
New Date	以年，月，日的格式输入新的日期。只有您在 Time Protocol 处选择了 Manual 的时候才可用。
Time Zone	先按空格键，然后按回车键设置您当地的时间区域和格林威治时间的时差。
Daylight Saving	Daylight saving是一个时间阶段，从晚春到早秋。许多国家会在这一阶段将时间提早一小时，以便让人们在傍晚得到更多的日光。 如果您使用这种功能，请选择该项。

Start Date (mm-nth-week-hr)	如果您在Daylight Saving处选择Yes。在hr区使用24小时格式。这里有几个例子： 美国的大部分地区开始夏时制是在4月的第一个星期天。在美国的 每个时区开始使用夏时制都在当地时间上午2点。所以在美国的话， 您要选择Apr.,1st,Sun。然后在hr处输入02。在欧共体夏时制是在3月的最后一个星期天开始。欧共体所有时区同时（凌晨1点GMT或UTC）开始使用夏时制。所以您如果在欧共体的话要选择Mar.,Last, Sun。您在hr区输入的时间取决于您的时区。例如在德国，您应该输入02，因为德国的时区是在GMT或UTC（GMT+1）的前一个小时。
End Date (mm-nth-week-hr)	如果您在Daylight Saving处选择Yes。在hr区使用24小时格式。这里有几个例子： 美国的大部分地区开始夏时制是在4月的第一个星期天。在美国的 每个时区开始使用夏时制都在当地时间上午2点。所以在美国的话， 您要选择Apr.,1st,Sun。然后在hr处输入02。在欧共体夏时制是在3月的最后一个星期天开始。欧共体所有时区同时（凌晨1点GMT或UTC）开始使用夏时制。所以您如果在欧共体的话要选择Mar.,Last, Sun。您在hr区输入的时间取决于您的时区。例如在德国，您应该输入02，因为德国的时区是在GMT或UTC（GMT+1）的前一个小时。
当您看到提示信息“Press ENTER to Confirm”的时候，您就可以按回车键保存您的配置，或按ESC键取消配置。	

第 37 章 远程管理

本章将会向您介绍菜单24.11的远端管理。

37.1 Remote Management

远程管理可以决定您从哪些电脑以何种方式通过什么样的协议可以接入到ZyWALL里面来。您可以通过以下的方式来远程管理您的ZyWALL。

您可以通过以下的方式来远程管理您的ZyWALL：

- Internet (WAN only) • ALL (LAN&WAN)
- LAN only • Neither (Disable).

注意：当您选择DMZ only，WAN only，WLAN only或者ALL（LAN & WAN&DMZ&WLAN）的时候，需要设置防火墙规则以便允许接入。

如果不想开放远程管理的功能，可以在**Server Access**的相应选项内选择**Disable**。

在菜单24中输入11进入菜单**Menu 24.11 - Remote Management Control**。

图 314 菜单 24.11 -远程管理控制

TELNET Server:

Port = 23

Access = ALL

Secure Client IP = 0.0.0.0

FTP Server:

Port = 21

Access = ALL

Secure Client IP = 0.0.0.0

SSH Server:

Certificate = auto_generated_self_signed_cert

Port = 22

Access = ALL

Secure Client IP = 0.0.0.0

HTTPS Server:

Certificate = auto_generated_self_signed_cert

Authenticate Client Certificates = No

Port = 443

Access = ALL

Secure Client IP = 0.0.0.0

HTTP Server:

Port = 80

Access = ALL

Secure Client IP = 0.0.0.0

SNMP Service:

Port = 161

Access = ALL

Secure Client IP = 0.0.0.0

DNS Service:

Port = 53

Access = ALL

Secure Client IP = 0.0.0.0

Press ENTER to Confirm or ESC to Cancel:

下表为界面相关的描述。

表 186 菜单24.11 – 远程管理控制

区域	描述
Telnet Server FTP Server SSH Server HTTPS Server HTTP Server SNMP Service DNS Service	这里每一个只读标签表示一个您可以用来进行远程管理 ZyWALL 的服务。
Port	该区域表示该服务或协议的端口号。如果需要的话您可以改变端口号，但是您必须使用相同的端口号来访问ZyWALL。
Access	按空格键选择访问界面，然后按回车键从 LAN only ， WAN only ， DMZ only ， WLAN only ， ALL 或 Disable 中选择。
Secure Client IP	默认值为0.0.0.0，允许任何客户端程序使用该服务来远程管理 ZyWALL。输入一个IP地址可以限制一个具有匹配的IP地址的客户端可以访问ZyWALL。

Certificate	先按空格键，然后按回车键选择ZyWALL将用来证明自身的证书。ZyWALL是SSL服务器并且必须始终鉴别连接到SSL客户端的自身（该计算机请求到ZyWALL的HTTPS连接）。
Authenticate Client Certificates	按空格键选择 Yes ，然后按回车键请求SSL客户端程序通过给ZyWALL发送一个证书来认证自身。SSL客户端必须有一个来自CA的CA签名证书，并且该CA已经作为一个可信任的CA被导入到了ZyWALL中。（更多细节参见557页附录G）。
当您看到提示信息“Press ENTER to Confirm”的时候，您就可以按回车键保存您的配置，或按ESC键取消配置。	

37.1.1 远程管理限制

下列情况不能在LAN或WAN上进行远程管理：

1. 在菜单3.1（LAN）或者菜单11.5（WAN）中应用过滤规则，阻止了Telnet、FTP或者Web服务。
2. 在菜单24.11中的服务已经被禁用了。
3. 客户端的IP地址和在**Secure Client IP**（菜单24.11）中设置的IP地址不相符。如果不一致的话，ZyWALL会立即断开该任务。
4. 有一个控制口会话正在运行。
5. 已经有另外一个相等或更高的权限的远程管理对话在运行。同一时间里您只能有一个远程管理的会话存在。
6. 有一条防火墙规则阻止进行远程管理。

第 38 章 访问时间表

访问时间表允许设定远程节点何时访问及访问的时长。

38.1 访问时间表介绍

访问时间表功能允许ZyWALL管理一个远程节点，并作出规定何时访问及访问的时长。

该功能与磁带录像机的日程安排程序相似（您可以为VCR指定一个时间周期进行记录）。您可以在菜单**Menu 11.1 - Remote Node Profile**中申请最多4个时间表。在主菜单中输入26进入菜单**Menu 26 - Schedule Setup**，如下所示。

图 315 时间表设置

Menu 26 - Schedule Setup

Schedule Set #	Name	Schedule Set #	Name
1		7	
2		8	
3		9	
4		10	
5		11	
6		12	

Enter Schedule Set Number to Configure= 0
Edit Name= N/A
Press ENTER to Confirm or ESC to Cancel:

较小数值的设置要优先于较大数值的设置，因此可以避免日程的冲突。例如，远程节点中的设定1，2，3，4那么1会优先于2，3和4。默认的先应用较小数值。同样，2优先于3和4，以此类推。

您可以设计最多12个时间表，但是对于一个远程节点来说您最多只可以应用4个时间表。

注意：如果想要删除一个时间表项，您可以在Edit Name区域中输入相应的数值，然后按空格键选择DEL，随后按回车键即可。

如果想要设置一个时间表，从菜单26（1-12）中选择您想要设定的时间表项，并按

回车键即可进入菜单**Menu 26.1 - Schedule Set Setup**，如下所示。

图 316 时间表设置

Menu 26.1 - Schedule Set Setup

Active= Yes

How Often= Once

Start Date (yyyy-mm-dd) = N/A Once:

Date (yyyy-mm-dd)= 2000 - 01 - 01

Weekdays:

Sunday= N/A

Monday= N/A

Tuesday= N/A

Wednesday= N/A

Thursday= N/A

Friday= N/A

Saturday= N/A

Start Time (hh: mm)= 00 : 00

Duration (hh: mm)= 00 : 00

Action= Forced On

Press ENTER to Confirm or ESC to Cancel: Press Space Bar to Toggle

如果一个连接已经建立，则ZyWALL不会断开。一旦连接被手动断开或超时，那么直 到 **Duration**的结束才能再次触发该远程节点。

表 187 时间表设置

区域	描述
Active	按空格键选择 Yes 或 No 。选择 Yes ，并按回车键可以激活该时间表设置项。
How Often	时间表是每周出现还是只使用一次？先按空格键，然后按回车键选择 Once 或 Weekly 。这两个选项是互相排斥的。如果选中 Once ，那么所有的 周日设置为 N/A ，当 Once 被选中时，经过预定义的时间之后，该时 间表项会自动地删除。
Start Date	当您希望以年-月-日格式来设置开始生效日期，输入一个开始日期。有 效日期是从当前日期到2036- February-5。
Once:	
Date	如果您在上面的 How Often 处选择了 Once ，那么在这里输入日期。
Weekdays:	

Day	如果您在上面的 How Often 处选择了 Weekly ，那么请通过按空格键选择 Yes 来使相应的日期能应用该时间计划。
Start Time	当您希望以小时-分钟的格式设置开始生效的时间，请输入一个开始时间。
Duration	在该区域以小时-分钟的格式设置一个时间，规定ZyWALL持续应用您在 Action 处设置的动作的时间。
Action	Forced On 表示无论是否有一个在线需求呼叫，都一直保持连接，并且将保持 Duration 中指定的时间周期。 Forced Down 表示无论是否有在线需求呼叫，连接都会断开。 Enable Dial-On-Demand 表示时间表允许一个在线的请求呼叫。 Disable Dial-On-Demand 表示时间表拒绝一个在线的请求呼叫。
当您看到提示信息“Press ENTER to Confirm”的时候，您就可以按回车键保存您的配置，或按ESC键取消配置。	

一旦将时间表配置好，就必须将其应用到所要的远程节点上。在主菜单输入**11**，然后输入远程节点的索引号。先按空格键，然后按回车键选择**Encapsulation**项中的**PPPoE**。显示如下时间表设置界面。

图 317 给一个远程节点（PPPoP）应用一个时间表

Menu 11.1 - Remote Node Profile

Rem Node Name= ChangeMe
Active= Yes

Route= IP

Encapsulation= PPPoE
Service Type= Standard
Service Name=
Outgoing=
My Login=
My Password= *****
Authen= CHAP/PAP

Edit IP= No
Telco Option:
Allocated Budget (min)= 0
Period(hr)= 0
Schedules= 1,2,3,4
Nailed-Up Connection= No

Session Options:
Edit Filter Sets= No
Idle Timeout(sec)= 100

Press ENTER to Confirm or ESC to Cancel:

您可以为该远程节点应用最多**4**个时间表，并用逗号分隔开。您可以根据您的选择来修改时间表的设定编号。

图 318 给一个远程节点 (PPPTP) 应用一个时间表

Menu 11.1 - Remote Node Profile

Rem Node Name= ChangeMe	Route= IP
Active= Yes	
Encapsulation= PPTP	Edit IP= No
Service Type= Standard	Telco Option:
	Allocated Budget (min)= 0
Outgoing=	Period(hr)= 0
My Login=	Schedules= 1,2,3,4
My Password= *****	Nailed-up Connections= No
Retype to Confirm= ***** Authen=	
CHAP/PAP	
PPTP:	Session Options:
My IP Addr=	Edit Filter Sets= No
My IP Mask=	Idle Timeout (sec)= 100
Server IP Addr=	
Connection ID/Name=	
Press ENTER to Confirm or ESC to Cancel:	

第 39 章 排障

本章主要介绍了一些潜在的问题以及可能的补救措施。在每一个问题描述之后，都会有相应的指导来帮助您诊断并解决问题。更多信息请参考随机附赠的光盘。

39.1 ZyWALL 启动问题

表243 ZyWALL启动时的排障

问题	更正动作	
当您给ZyWALL加电的时候没有一个LED灯亮。	请检查并确保随机附带的电源线正确连接到电源上。	
	如果问题仍然存在，则可能存在硬件问题，请联系您的供货商。	
不能通过控制口来访问ZyWALL。	请检查ZyWALL是否已经和您PC上的串口连接好。	
	请检查通信程序是否已正确配置，正确的配置如下：	VT100终端仿真。
		默认出厂设置的波特率为9600bps，如果速度被修改过，则请尝试其它的速率。
		无奇偶校验，8个数据位，1个停止位，没有数据流控制。

39.2 LAN 端口的问题

表189 LAN口故障修复

问题	更正动作
不能从LAN口访问yWALL	请检查网线的类型，以及是否接触良好。请参阅快速安装手册了解关于LAN连接的说明。
	请确保您的PC的以太网卡已安装，并工作正常。

不能ping通 LAN上的计算 机。	检查前面板上的10M/100M LAN LED灯。其中应该有一个LED是亮着的。如果所有的灯都熄灭了，请检查ZyWALL与hub或工作站之间的连线。
	请检查ZyWALL和电脑的IP地址与子网掩码，确保它们在相同的子网内。

39.3 WAN 接口上的问题

表190 WAN接口上的排障

问题	更正动作
无法从ISP获取 WAN口IP地址	通过验证后ISP会提供WAN的IP地址。认证时会使用用户名和密码，MAC地址或者主机名。用下列动作来确认ISP能否验证您的连接。
	如果您用PPPoE或者PPTP封装模式，那么您需要一个用户名和密码。请确认您已经输入了一个正确的Service Type，User Name和Password（用户名和密码区分大小写）。请参阅109页第7章或399页27章。
	如果ISP检查MAC地址，您应该从LAN上的电脑来克隆MAC地址。请参阅109页第7章或381页25章。即便您的ISP目前不检查MAC地址，我们也建议您克隆您的计算机的MAC地址。
	如果您的ISP需要检查主机名，请配置和计算机名一样的ZyWALL系统名。请参阅69页第3章或375页24章。

39.4 访问 ZyWALL 时的问题

表 191 访问ZyWALL时的排障

问题	更正动作
无法访问 ZyWALL	默认密码为“1234”。密码区分大小写。
	利用 Reset 按钮恢复出厂设置，包括密码。

无法通过串口访问ZyWALL	1. 查看ZyWALL是否正确连接到计算机的串口。 2. 查看连接程序是否已经正确配置。连接软件应该按照如下配置： • VT100终端机仿真模式。 • 9600bps的出厂默认连接速度。如果该速度被改变请尝试其它的速度。 • 无奇偶校验、8个数据位、1个停止位、无流量控制。
无法接入web设置界面	确保没有一个控制口会话在进行。当配置来自WAN的时候,请使用ZyWALL的WAN口IP地址。当配置来自LAN的时候,请使用ZyWALL的LAN口IP地址。检查您已经启用了web服务访问功能。如果您已经配置了一个安全的客户端IP地址,那么您的计算机的IP地址必须与其相匹配。对于局域网接入,您的计算机和ZyWALL的IP地址必须是在相同的子网上。如果您改变了ZyWALL的LAN口IP地址,那么请输入新的地址信息。在SMT菜单3.1 (LAN) 或菜单11.5 (WAN) 中删除所有用来拦截网络服务的过滤器。 在下列章节查看弹出窗口, JavaScripts和Java许可。
	您也许要清除您的网络浏览器的缓冲。在IE中,先点击Tools,然后点击Internet Options打开该界面。在General标签页中,点击Delete Files。在弹出窗口中,选择Delete all offline content复选框,并点击OK。然后在Internet Options界面中点击OK关闭窗口。
	如果您的计算机与一个设备断开然后连接到另一个有着相同IP地址的设备上,该计算机的ARP表可能会有一条管理IP地址到上一台设备MAC地址的映射项。 在MS-Dos中,可以使用命令arp -d来删除计算机ARP表中的所有条目。

39.4.1 允许弹出窗口, Java 脚本和 Java 权限

为了能够使用web设置界面,请参考以下进行:

- 网页浏览器弹出窗口来自您的设备。
- Java脚本 (默认激活)。
- Java权限 (默认激活)。

注意：这里使用的网页浏览器版本6的界面。可能和其它版本的界面有所不同。

39.4.1.1 网页浏览器弹出窗口阻止

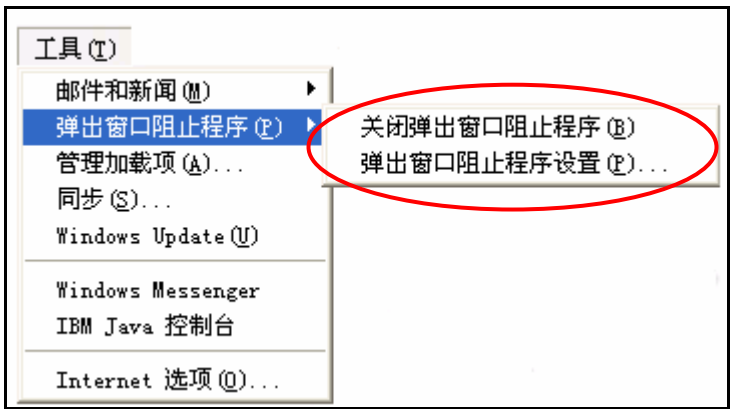
您也许需要禁用弹出阻止窗口功能来登录到您的设备。

或者禁用窗口阻止功能（在 Windows XP（SP2）中缺省设置为启用），或者为您的设备的IP地址单独创建一条允许项。

39.4.1.1.1 禁用弹出窗口阻止

- 1. 在IE浏览器中依次选择**工具（T）**，**弹出窗口阻止程序（P）**，然后选择**关闭弹出窗口阻止程序（B）**。

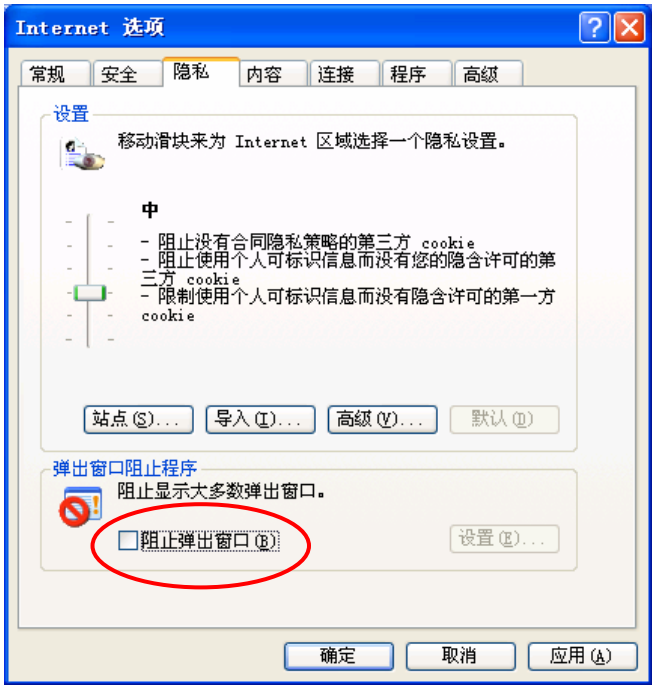
Figure 319 弹出窗口阻止



您也可以查看**隐私**标签页中的**弹出窗口阻止程序**项的弹开窗口阻止功能是否被关闭。

- 1. 在IE浏览器中依次选择**工具（T）**，**Internet 选项（O）**，**隐私**。
- 2. 清除**弹出窗口阻止程序**项中的**阻止弹出窗口（B）**复选框。这样就会使那些已经激活的弹开窗口阻止功能全部失效。

Figure 320 Internet选项：隐私



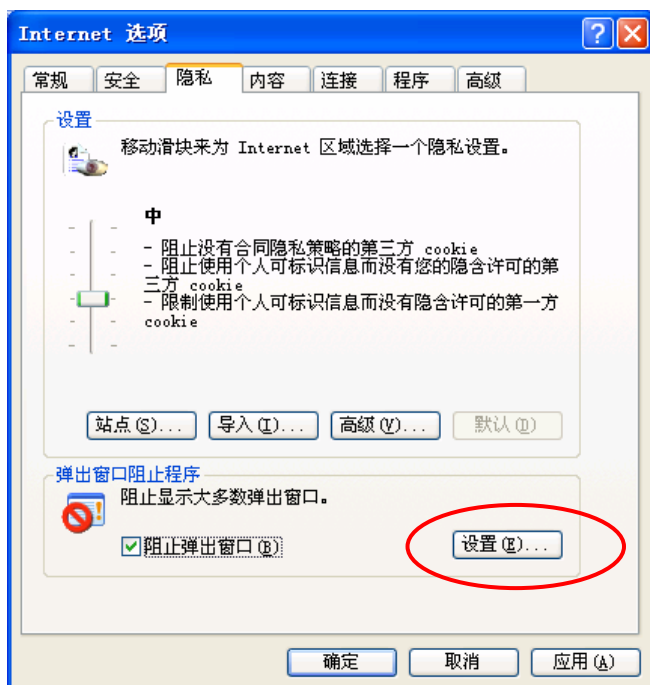
3. 点击应用保存该设置。

39.4.1.1.2 启用带有例外的弹出窗口阻止功能

或者，如果您只允许来自您设备的弹出窗口，请按照以下步骤来操作。

- 1 在IE浏览器，选择工具(T) > Internet 选项(O) > 隐私。
- 2 选择 设置(E) ...，打开 弹出窗口阻止程序设置界面。

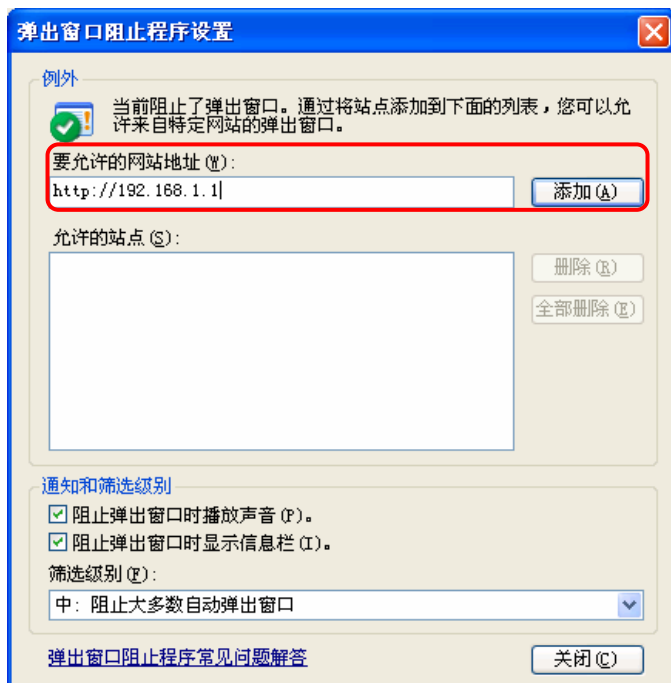
图 321 Internet 选项：隐私



3 输入您设备的 IP 地址（您不想有被阻止的网页），加上前缀“http://”。如 <http://192.168.1.1>。

4 点击 **添加(A)** 将该 IP 地址加入到 **允许的站点** 列表

图322 弹出窗口阻止设置



5 点击 **关闭(C)** 返回到 **隐私** 界面。

6 点击 **应用** 保存该页面。

39.4.1.2 Java 脚本

如果web配置界面在IE中无法正常显示，请检查Java脚本是否被允许了。

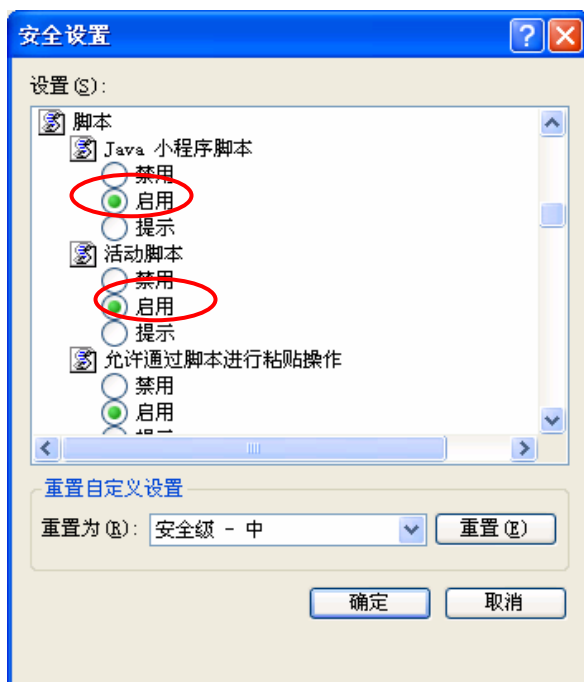
- 1 在 IE浏览器，点击工具 (T) > Internet 选项 (O) > 安全。

图 323 Internet 选项



- 2 点击 自定义级别 (C) ... 按钮。
- 3 通过下拉菜单找到 脚本。
- 4 确定 活动脚本 下面的 启用 已被选中 (默认值)
- 5 确定 Java小程序脚本 下面的 启用 已被选中 (默认值)
- 6 点击 确定 关闭该窗口。

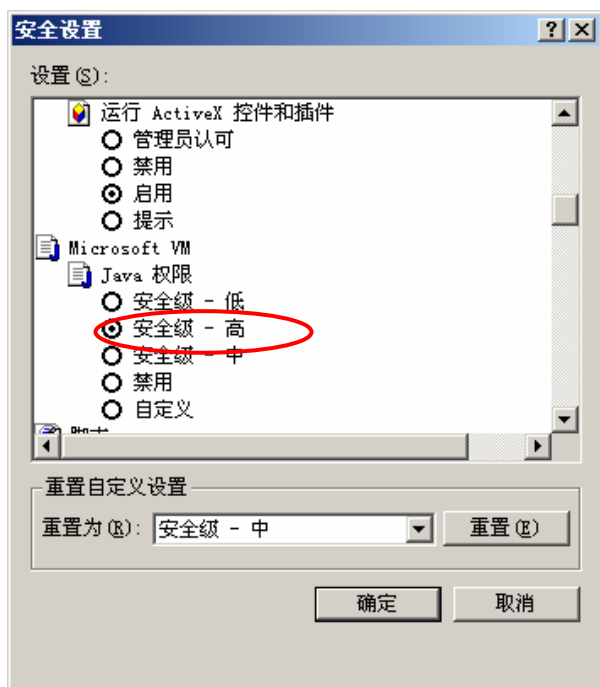
图 324 安全设置-Java 脚本



39.4.1.3 Java 权限

- 1 从 IE浏览器，点击 工具 (T) >Internet 选项 (O) > 安全。
- 2 点击自定义级别 (C) ...按钮。
- 3 通过下拉菜单找到 **Microsoft VM**。
- 4 确定**Java**权限下面的安全类型已被选中。
- 5 点击 **确定** 关闭该窗口。

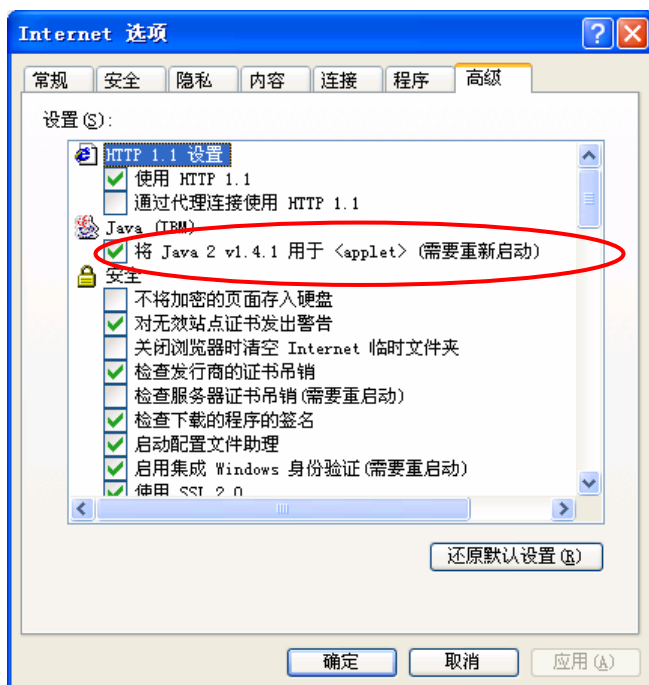
图 325 安全设置-Java



39.4.1.3.1 JAVA (Sun)

- 1 从IE浏览器，点击 工具 (T) > Internet 选项 (O) > 高级。
- 2 确定 Java (Sun) 面的 将Java 2 v1.4.1用于<applet>(需要重新启动)已被选中。
- 3 点击 确定 关闭该窗口。

图 326 Java (Sun)



39.5 数据包流

下面是ZyWALL上的数据检测流程。

LAN to WAN: 数据和呼叫过滤器（在SMT 菜单21 中）-> Firewall ->远程节点数据过滤（在SMT 菜单21 中）->内容过滤-> NAT

WAN to LAN: 远程节点数据过滤（在 SMT 菜单 21 中）-> NAT -> Firewall -> LAN 数据过滤器（在 SMT 菜单 21 中）->内容过滤