

第 10 章

IP 过滤/防火墙设定

11.1 介绍

IP 过滤/防火墙设定帮助您保护您的内部网络免受来自外部的攻击。同样它也可以限制内部网络的使用者对 Internet 的访问。另外，它还可以阻止内部某些数据包触发拨号。

11.2 IP 过滤/防火墙概述

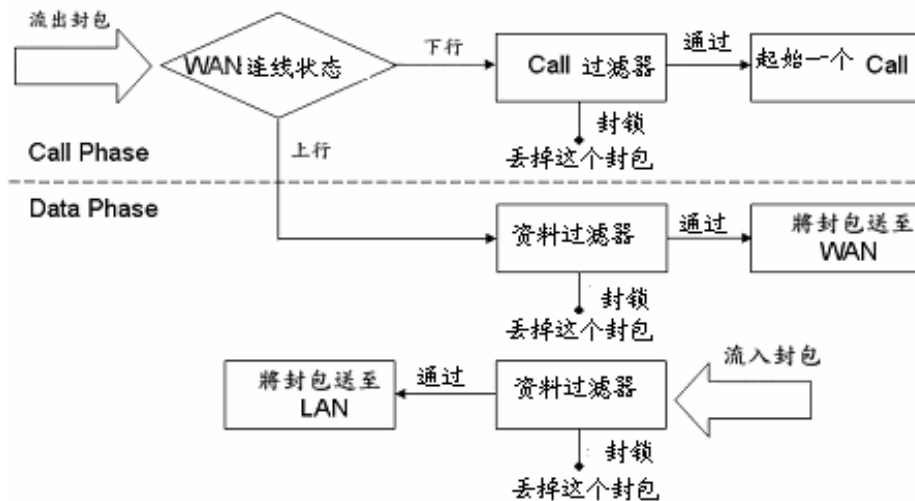
您路由器上的 IP 过滤/防火墙设定主要有以下几部分构成：信息包的过滤，DoS 攻击防御，URL 内容过滤，Web 内容过滤。在本章我们主要介绍信息包的过滤，随后的三章分别介绍 DoS 攻击防御，URL 内容过滤和 Web 内容过滤。

信息包的过滤包含两个部分：呼叫过滤器和数据过滤器。呼叫过滤器是用来阻止内部某些数据包触发拨号，数据过滤器是用来阻止某些内部网络对外部网络或者外部网络对内部网络的访问。

当一个往外的封包被送往 WAN 时，IP 过滤器会先决定这封包该送往呼叫过滤器还是数据过滤器。如果 WAN 是断线的，这个封包会被送往呼叫过滤器。若这个封包不合法，则会被丢弃；反之，呼叫过滤器会触发一个指令来建立 WAN 连线，然后让合法封包流出。如果 WAN 的连接本来就已经存在，这个封包会被送往数据过滤器。如果这个封包不合法，则直接被丢弃；反之送往 WAN 流出。

IP 过滤/防火墙设定

另外，如果有从 WAN 流入的封包，它会直接被送往数据过滤器。如果不是合法的封包，则被丢弃；反之它将被送往内部的 LAN。过滤器的结构图如下：



接下来的部分将对**IP过滤器/防火墙设定**中的一般设定和**过滤器设定**作详细的介绍。**Vigor**路由器提供 12 个过滤器组别，每个组别有 7 条过滤规则，所以在过滤器设定中一共可以设定 84 条过滤规则。

IP 过滤/防火墙设定



一般设定：关于呼叫过滤器和数据过滤器的一般性设定。

DoS 攻击防御功能设定：单击此项可以进入 DoS 攻击防御功能设定页面，来设置有关项以防范和减轻 Dos 攻击。更多细节请参见 13-A.

URL 内容过滤器：通过过滤 URL 地址，能够阻止对一些不适宜的网站的访问。
比如阻止儿童访问带有色情暴力内容的网站。

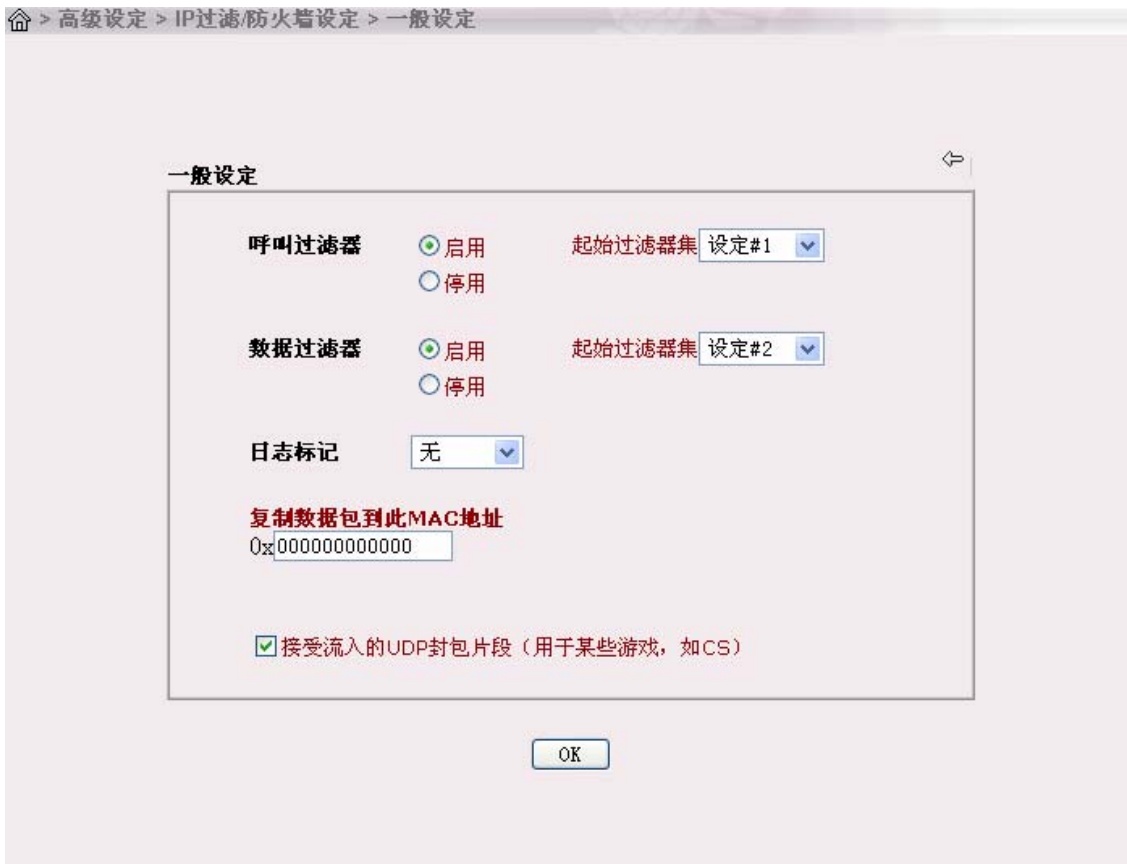
Web 内容过滤器：通过过滤 Web 站点的属性，能够阻止对一类网站的访问。
比如阻止员工访问新闻网站。

过滤器设定：IP过滤器设定中提供 12 个过滤器组别。

(Set to Factory Default): 选点回复出厂默认过滤器设置规则。

11.3 一般设定

在一般设定您可以启用/停用呼叫过滤器或数据过滤器，并指定起始过滤器组别，设定记录模式，并设定一个MAC地址供记录封包复制到该地址。



呼叫过滤器: 单击启用来激活呼叫过滤器，并指定起始过滤器组别。

数据过滤器: 单击启用来激活数据过滤器，并指定起始过滤器组别。

日志标记: 您可以设定过滤器记录档的储存内容以便排除疑难时参考。

None	停用记录功能。
------	---------

IP 过滤/防火墙设定

Block	记录所有被封锁的封包。
Pass	记录所有通行的封包。
No Match	记录所有不合法的封包。

注意：当您输入“log -f”指令后，过滤器的记录会显示在Telnet终端机上。

复制数据包到此MAC地址：记录的封包也可以通过以太网记录在一个网络位置。如果您想要从路由器复制一份记录档到网络上的另外一个位置，您必须填入改装之的MAC地址，输入 0 会停用此功能。

接受流入的UDP封包片段（用于某些有些，如CS）

有些在线游戏（例如：CS）使用长度很长的UDP封包传送资料，这些封包需要被切割。如果您没有启用“接收流入的UDP封包片段”Vigor路由器会拒绝这种封包，以避免受到黑客的攻击。如果您启用了此功能，就可以进行这类在线游戏。如果您比较在乎网络的安全性，建议您停用此功能。

11.4 编辑过滤器组别

🏠 > 高级设定 > IP过滤/防火墙设定 > 过滤器设定

过滤器设定 1 ↩️ ✎

注解:

过滤器规则	启用	注解
<input type="button" value="1"/>	<input checked="" type="checkbox"/>	Block NetBios
<input type="button" value="2"/>	<input type="checkbox"/>	
<input type="button" value="3"/>	<input type="checkbox"/>	
<input type="button" value="4"/>	<input type="checkbox"/>	
<input type="button" value="5"/>	<input type="checkbox"/>	
<input type="button" value="6"/>	<input type="checkbox"/>	
<input type="button" value="7"/>	<input type="checkbox"/>	

下一个过滤器集 ▼

注解：输入过滤器注解描述，最多输入 23 个字符。

过滤器规则：点选 **1~7** 的数字按钮编辑过滤器规则。

启用：启用或停用过滤器规则。

下一个过滤器组别：当封包通过目前的过滤器后，如果需要封包继续下一层过滤，请在这里设定。注意，请不要设定成循环的顺序！

下图显示了呼叫过滤器和数据过滤器的默认设定。

IP 过滤/防火墙设定

高级设定 > IP过滤/防火墙设定 > 过滤器设定

过滤器设定1



注解: Default Call Filter

过滤器规则	启用	注解
1	<input checked="" type="checkbox"/>	Block NetBios
2	<input type="checkbox"/>	
3	<input type="checkbox"/>	
4	<input type="checkbox"/>	
5	<input type="checkbox"/>	
6	<input type="checkbox"/>	
7	<input type="checkbox"/>	

下一个过滤器集 无

OK

IP 过滤/防火墙设定

高级设定 > IP过滤/防火墙设定 > 过滤器设定

过滤器设定2

注解: Default Data Filter

过滤器规则	启用	注解
1	<input checked="" type="checkbox"/>	xNetBios -> DNS
2	<input checked="" type="checkbox"/>	
3	<input checked="" type="checkbox"/>	
4	<input type="checkbox"/>	
5	<input type="checkbox"/>	
6	<input type="checkbox"/>	
7	<input type="checkbox"/>	

下一个过滤器集 无

OK

11.5 编辑过滤器规则

点选过滤器规则代号进入过滤器规则设定页面。

注解	输入过滤器组别注解描述，最多输入 14 字符。
启用	启用过滤启规则。

通过或封锁： 设定当封锁包符合条件时所采取的行动。

立刻封锁	当封锁包符合条件时立刻丢弃。
立刻通过	当封锁包符合条件时立刻放行。

IP 过滤/防火墙设定

封锁, 如果没有其它符合	当封锁包只符合此规则, 不符合其它规则时被丢弃。
通过, 如果没有其它符合	當当封锁包只符合此规则, 不符合其它规则时会放行。。

过滤器集2规则2
↔ ✎

注解:
☒ 选中以启用过滤器规则

通过或封锁
立即封锁

连接到其他过滤器设定
无

☐ 记录

方向 流出
通讯协议 任意

	IP地址	子网掩码	运算符	起始端口	终止端口
源地址	any	255.255.255.255 / 32	=		
目标地址	any	255.255.255.255 / 32	=		

☐ Keep State
片段 忽略

连接到其它过滤器设定	如果封包符合此规则, 则跳过失下的规则而直接用所选规则作为下一条规则。
记录	在此打勾启动记录功能。当您输入“log -f”指令后, 过滤器的记录会显示在Telnet终端机上。
方向	设定封包流向, 对于呼叫过滤器, 此项设定不重要。

对于数据过滤器:

流入: 设定规则只过滤流入的封包

流出: 设定规则只过滤流出的封包

通讯协定: 设定通讯规则适用的通讯协议

IP地址: 设定一组适用此过滤规则的来源和目标IP地址。如果在IP地址前面加上“!”符号则表示此过滤规则不适用于此IP地址。“!”相当于逻辑运算符NOT。

子网掩码: 配合上面的IP地址设定适用此过滤规则的子网掩码。通过这一设定可以使过滤规则适用于一个网段而不仅仅是一个IP。

运算符: 运算符的设定和通讯的端口有关。如果**起始端口**为空, 则**起始端口**和**终止端口**的栏位将被忽略, 过滤规则将适用于所有端口。

= : 如果**终止端口**不填, 过滤规则将只适用于**起始端口**所填的端口; 若有填入数值, 则过滤规则适用于从**起始端口**起到**终止端口**结束的所有端口。

!= : 如果**终止端口**不填, 过滤规则将只不适用于**起始端口**所填的端口; 若有填入数值, 则过滤规则不适用于从**起始端口**起到**终止端口**结束的所有端口。其它的端口都适用。

> : 过滤规则适用于所有端口大于等于**起始端口**的端口。

< : 过滤规则适用于所有端口小于等于**起始端口**的端口。

Keep State: 路由器会追踪封包并拒绝未经请求的流入封包。在通讯协定选项必须选择TCP, UDP, TCP/UDP或ICMP。

IP 过滤/防火墙设定

片段： 设定适用过滤规则的封包的切割形式。

<i>忽略</i>	过滤规则适用于所有的封包切割形式。
<i>完整无分片</i>	过滤规则适用于没有被切割的封包。
<i>片段</i>	过滤规则适用于被切割的封包。
<i>太短</i>	过滤规则适用于太短的封包。

11.6 拒绝未经许可的网络服务的设定范例

IP 过滤/防火墙设定

这里我们给出一个简单的范例：限制内网用户访问Web网页。我们家设备限制者的内网IP为 192.168.1.10，下面是数据过滤器组别中的过滤器规则。80 端口是访问网页所要用到的HTTP通讯端口。

过滤器集2规则2

注解：

☒ 选中以启用过滤器规则

通过或封锁

连接到其他过滤器设定

☐ 记录

方向

通讯协议

	IP地址	子网掩码	运算符	起始端口	终止端口
源地址	<input type="text" value="192.168.1.10"/>	<input type="text" value="255.255.255.255 / 32"/>	<input "="" type="text" value="="/>	<input type="text"/>	<input type="text"/>
目标地址	<input type="text" value="any"/>	<input type="text" value="255.255.255.255 / 32"/>	<input "="" type="text" value="="/>	<input type="text" value="80"/>	<input type="text"/>

☐ Keep State

片段

OK

第 11-A 章

预防DoS攻击

A.1 简介

DoS（Denial of Service）攻击防御功能帮助您侦测并缓和DoS攻击。这些攻击包括flooding-type攻击和vulnerability攻击。前者是一种企图耗尽您的系统资源的攻击方式，后者则是攻击通讯协议或作业系统的弱点从而使整个系统瘫痪。

A.2 DoS防御工具概述

DoS防御工具会对照攻击特征资料库检查每个流入的封包。任何可能使主机瘫痪的封包会被封锁，同时一个系统记录会马上被传送到客户端。DoS防御工具也会监视流量的变化，任何违反管理者设定的不正常情况都会被记录下来并采取适当的防御措施来缓和攻击。



A.3 设定

下面的部分将通过设定页面详细解释 DoS 攻击防御功能设定。这是 IP 过滤器/防火墙的子功能，总共有 15 种防御功能。DoS 攻击防御功能在路由器的默认设定中是停用的。一旦被启用后，在某些功能中预设的零界值和逾时分别设定为 300 封包/秒和 10 秒。下面将对 DoS 攻击防御功能中的每个项目做一个简要的介绍。

启用/拒绝服务（DoS） 攻击防御功能	勾选以启用 DoS 攻击防御功能。
启用 SYN flood 攻击防	勾选以启用 SYN flood 攻击防御功能。如果从互联网来

IP 过滤/防火墙设定

御功能	的 TCP SYN 数据包超过用户设置的临界值，Vigor 路由器将会在用户设置的超时时间内随机丢弃 TCP SYN 数据包。主要的目标是保护 Vigor 路由器不受企图耗尽路由器资源的 TCP SYN 数据包的威胁。
启用 UDP flood 攻击防御功能	勾选以启用 UDP flood 攻击防御功能。一旦从因特网来的 UDP 封包超过使用者设定的临界值，Vigor 路由器将会在使用者设定的逾时时间内丢弃所有随后的 UDP 封包。预设的临界值和逾时数值分别被预设为 300 封包/秒和 10 秒。
启用 ICMP flood 攻击防御功能	勾选以启用 ICMP flood 攻击防御功能。如同 UDP flood 攻击防御功能，一旦从因特网来的 ICMP 响应请求封包超过使用者设定的临界值(预设为 300 封包/秒)，Vigor 路由器将会在使用者定义的逾时时间(预设为 10 秒)内丢弃所有随后的 UDP 封包。
启用通讯端口扫描侦测功能	通讯端口扫描攻击是指传送很多不同通讯端口的封包，企图扫描有哪些通讯端口正在被使用，得知有哪些可用的服务。为了侦测通讯端口扫描行为，请勾选以启用 Vigor 路由器内的防御通讯端口扫描侦测功能。如果通讯端口扫描速率超过使用者设定的临界值，Vigor 路由器将会发现并且发出警告讯息。预设中，Vigor 路由器将临界值设定为 300 封包/秒。
封锁 IP 选项	勾选以启用封锁 IP Options。Vigor 路由器将会忽略任何在数据文件头中有 IP Option 字段的封包。IP Option 让主机可以传送一些重要讯息，例如 Security, Compartmentation, TCC (closed user group) 参数，一连串的网址，路由信息等。外人可能会加以分析，而清

IP 过滤/防火墙设定

	楚您的内部网络。
封锁 Land 攻击	勾选以启用 Vigor 路由器防御 Land 攻击。Land 攻击结合了 SYN 攻击技术和 IP 伪造。Land 攻击方式是攻击者传送伪造的 SYN 封包，封包内含相同的来源和目的地址 (和受害者地址相同)以及相同的通讯端口。
封锁 Smurf 攻击	勾选以启用封锁 Smurf 攻击功能。Vigor 路由器会拒绝任何指向广播地址的 ICMP 响应请求。
封锁路由追踪 (Trace Route)	勾选以启用此功能。Vigor 路由器将不会传送任何路由追踪封包。
封锁 SYN Fragment 攻击	勾选以启用封锁 SYN Fragment 封包功能。任何具有 SYN Flag 以及 More Fragment 位设为 1 的封包会被丢弃。
封锁 Fraggle 攻击	勾选以启用封锁 Fraggle 攻击功能。任何从因特网收到的广播 UDP 封包都会被封锁。 注意启用 DoS/DDoS 攻击防御功能可能会封锁一些合法的封包。例如当您启用封锁 Fraggle 攻击功能，所有从因特网上广播的 UDP 封包都会被封锁。所以，从因特网上来的 RIP 封包也会被丢弃。
封锁 TCP Flags 扫描	勾选以启用封锁 TCP Flags 扫描功能。任何具有不正常 Flag 设定的 TCP 封包会被丢弃。这些扫描的活动包含 no flag scan , FIN without ACK scan , SYN FINscan , Xmas scan , 以及 full Xmas scan 。
封锁 Tear Drop 攻击	勾选以启用封锁 Tear Drop 攻击功能。这种攻击是指攻击者传送部份重迭的封包到目标主机，当那些主机要重组

IP 过滤/防火墙设定

	封包时就会当机。Vigor 路由器会封锁这些封包。
封锁 Ping of Death 攻击	勾选以启用封锁 Ping of Death 攻击功能。许多机器在收到超过最大长度的 ICMP 封包可能会当机。为了避免这种攻击,路由器必须能丢弃任何长度超过 1024 字节的切割封包。
封锁 ICMP Fragment 攻击	勾选以启用封锁 ICMP Fragment 封包功能。任何 More Fragment 位设为 1 的 ICMP 封包会被丢弃。
封锁不明封包通讯协定	勾选以启用封锁不明通讯协议封包功能。每个 IP 封包在档头都会有一个通讯协议字段,用来指出在上层使用哪种通讯协议。然而,超过 100 的通讯协议代号目前仍然保留没有被定义,所以路由器要能侦测并拒绝这种封包。

IP 过滤/防火墙设定

高级设定 > IP过滤/防火墙设定 > DoS攻击防御功能设定

拒绝服务（DoS）攻击防御功能设定

☒ 启用拒绝服务（DoS）攻击防御功能

<input checked="" type="checkbox"/> 启用SYN flood攻击防御功能	临界值	300	封包 / 秒
	超时	10	秒
<input checked="" type="checkbox"/> 启用UDP flood攻击防御功能	临界值	300	封包 / 秒
	超时	10	秒
<input checked="" type="checkbox"/> 启用ICMP flood攻击防御功能	临界值	300	封包 / 秒
	超时	10	秒
<input checked="" type="checkbox"/> 启用通讯端口扫描侦测功能	临界值	300	封包 / 秒
<input checked="" type="checkbox"/> 封锁IP选项	<input checked="" type="checkbox"/> 封锁TCP flag扫描		
<input checked="" type="checkbox"/> 封锁Land攻击	<input checked="" type="checkbox"/> 封锁Tear Drop攻击		
<input checked="" type="checkbox"/> 封锁Smurf攻击	<input checked="" type="checkbox"/> 封锁Ping of Death攻击		
<input checked="" type="checkbox"/> 封锁路由追踪（Trace Route）	<input checked="" type="checkbox"/> 封锁ICMP fragment攻击		
<input checked="" type="checkbox"/> 封锁SYN fragment攻击	<input checked="" type="checkbox"/> 封锁不明封包通讯协议		
<input checked="" type="checkbox"/> 封锁Fraggle攻击			

Enable DoS defense function to prevent the attacks from hacker or crackers.

Cancel Clear All OK

A.4 警告讯息

在您启用系统纪录功能后，所有警告讯息会被送到系统纪录客户端。管理者可以使用设定网页在**系统日志(Syslog)/邮件警示设定**选单中设定系统纪录客户端。如此一来，管理者可以透过 DrayTek Syslog daemon 看到由 DoS 攻击防御功能发出的警告讯息。这种警告讯息的格式跟 **IP 过滤器/防火墙**的相似，除了在前头的关键词是“DoS 加上攻击型态的名称”。

IP 过滤/防火墙设定

SysLog访问设定

☒ 启用

服务器IP地址

192.168.1.10

目标端口

514

DrayTek Syslog

Controls

192.168.1.1

Vigor2900

LAN Status

TX Packets: 5850 RX Packets: 4517

WAN Status

Getway IP (Static)	TX Packets	RX Rate
172.16.2.5	1190	1
WAN IP (Static)	RX Packets	TX Rate
172.16.2.84	13115	1

Fire Wall Log | VPN Log | User Access Log | Call Log | WAN Log | Network Information | Net State

Time	Host	Message
Jan 1 03:46:27	Vigor	DoS fraggle Block 172.16.2.1,10752 -> 255.255.255.255,234 PR udp len 20 328
Jan 1 03:46:24	Vigor	DoS fraggle Block 172.16.2.83,10752 -> 172.16.2.255,234 PR udp len 20 233
Jan 1 03:46:23	Vigor	DoS trace_rt Block 192.168.3.1,10752 -> 224.0.0.9,234 PR udp len 20 52
Jan 1 03:46:19	Vigor	DoS fraggle Block 172.16.2.47,10752 -> 172.16.2.255,234 PR udp len 20 239
Jan 1 03:46:19	Vigor	DoS fin_wo_ack Block DoS synfin_scan Block 172.16.2.85,1024 -> 172.16.2.84,80
Jan 1 03:46:09	Vigor	DoS unknown_protocol Block 172.16.2.85 -> 172.16.2.84 PR 105 len 20 20
Jan 1 03:46:03	Vigor	DoS smurf Block 172.16.2.84 -> 172.16.2.255 PR icmp len 20 32 icmp 0/8
Jan 1 03:46:02	Vigor	DoS trace_rt Block 172.16.5.5,10752 -> 224.0.0.9,234 PR udp len 20 52
Jan 1 03:45:59	Vigor	DoS fraggle Block 172.16.2.9,10752 -> 172.16.2.255,234 PR udp len 20 233
Jan 1 03:45:59	Vigor	DoS land Block 172.16.2.84,80 -> 172.16.2.84,80 PR tcp len 20 40 -S 1 0
Jan 1 03:45:54	Vigor	DoS trace_rt Block 203.69.175.5,10752 -> 224.0.0.9,234 PR udp len 20 72
Jan 1 03:45:51	Vigor	DoS fraggle Block 172.16.2.25,10752 -> 172.16.2.255,234 PR udp len 20 78
Jan 1 03:45:52	Vigor	DoS fraggle Block 172.16.2.1,10752 -> 255.255.255.255,234 PR udp len 20 328

ADSL Status

Mode	State	Up Speed	Down Speed	SNR Margin	Loop Att
...

第 11-B 章

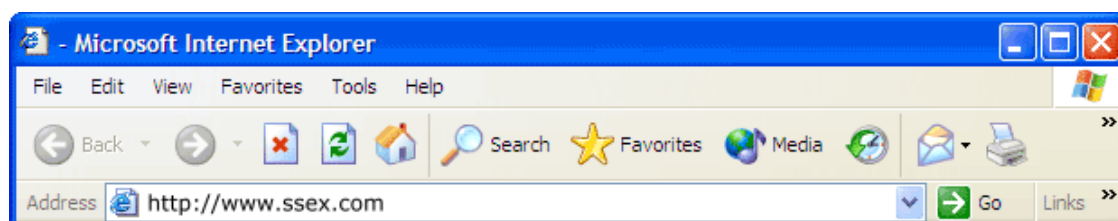
URL 内容过滤

B.1 介绍

因特网包含广泛的题材，但有些内容令人不适，甚至有些是违法的。URL 内容过滤器用来限制某些题材的存取，在互联网上对访问的题材进行区隔。URL 内容过滤器可评估哪些网站是不适宜的，应该被禁止访问，如此一来可以预防不适当的网页浏览。在预防存取网站的功能上，URL 内容过滤器可以帮助家长阻止未成年人对暴力色情网站的访问；也可以用在商业中，预防员工存取跟工作无关或不适当的网络服务。

传统的防火墙透过 TCP/IP 档头字段检查封包，而 URL 内容过滤器检查 URL 字符串或 TCP/IP 封包的数据负载。在 Vigor 路由器，URL 内容过滤器检查 URL 字符串以及一些隐藏在 TCP 封包中数据负载的 HTTP 数据。

B.2 URL 内容过滤概述



每当 HTTP 请求发出后，Vigor 路由器中的 URL 内容过滤器根据关键词列表检查每

个 URL 字符串。如果全部或部分的 URL 字符串(例如上图所示的 <http://www.ssex.com>)符合任何启用的关键词, Vigor路由器将会封锁相关的 HTTP请求, 而且自动送出系统纪录讯息给系统纪录客户端。此外, 任何包含恶意的程序的请求将会被Vigor路由器丢弃, 同样的, 系统纪录会被送到系统纪录客户端。

URL内容过滤器机制预防使用者存取到那些被URL字符串认定为禁止访问的网站。

注意您必须先清除浏览器的快取区, URL内容过滤器机制才能在您之前浏览过的网站上正常的运作。

B.3 设定

接下来的部份将叙述 URL 内容过滤器机制的网页设定, 包含特定的设定信息以及他们的限制。在主要选单中点选 **IP 过滤器/防火墙**之后即可找到这个设定的入口。

IP 过滤/防火墙设定



Vigor 路由器支持的 URL 内容过滤器机制包含：启用 URL 访问控制，防止使用 IP 地址对网站进行访问，启用限制网络功能，允许例外子网，以及时间表功能。

启用 URL 访问控制 比对 URL 字符串和使用者定义的关键词，控制网站的存取权限。

防止使用 IP 地址对网站进行访问 直接使用 URL 所在处的 IP 地址限制不当网站的存取，即使 URL 字符串符合使用者定义的关键词。

启用限制网络功能 封锁隐藏在网页中恶意的程序代码，例如 *Java Applet*, *Active X*, *Cookies*, *Proxy*, *compressed* 档案，以及 *executable* 档案。另外，此功能也可以限制从网站上多媒体的下载，以控制频宽的使用。

IP 过滤/防火墙设定

允许例外子网 允许管理者设定一群主机,这些主机不受*启用 URL 访问控制* 的限制。这群主机指定的方式可用一组 IP 地址或是子网掩码。最后, Vigor 路由器也提供 *时间表* 功能,可以控制何时采用 URL 内容过滤器机制。现在让我们更详细地介绍每项功能。

IP 过滤/防火墙设定

高级设定 > IP过滤/防火墙设定 > URL内容过滤器设定

URL内容屏蔽设定

☐ 启用URL访问控制

屏蔽关键字列表

编号	启用	关键字	编号	启用	关键字
1	<input type="checkbox"/>		5	<input type="checkbox"/>	
2	<input type="checkbox"/>		6	<input type="checkbox"/>	
3	<input type="checkbox"/>		7	<input type="checkbox"/>	
4	<input type="checkbox"/>		8	<input type="checkbox"/>	

空白处可同时指定数个关键字。例如: hotmail yahoo msn

☐ 防止使用IP地址对网站进行访问

☐ 启用限制网络功能

☐ Java ☐ ActiveX ☐ 压缩文件 ☐ 可执行程序 ☐ 多媒体文件
☐ Cookie ☐ 代理

☐ 允许例外子网

编号	启用	IP地址		子网掩码
1	<input type="checkbox"/>		~	
2	<input type="checkbox"/>		~	
3	<input type="checkbox"/>		~	
4	<input type="checkbox"/>		~	

时间表

☒ 一直封锁

☐ 封锁时段自 8 : 0 至 17 : 30

每周的:

☒ 每天

☐ 特定几天

☐ 周日 ☒ 周一 ☒ 周二 ☒ 周三 ☒ 周四 ☒ 周五 ☐ 周六

Cancel Clear All OK

Copyright (c) 2004, DrayTek Corp. All Rights Reserved.

启用URL访问控制: 在空白的方块点一下即可启用**启用URL访问控制**功能，而且(√)会出现。

屏蔽关键字列表: Vigor 路由器提供八个字段供使用者定义关键词，每个字段可以输入多个关键词。关键词可以是一个名词、部份的名词、或者是一个完整的 URL 字符串。若要在每个字段中指定多个关键词，请用空格键，逗号，或分号分开。此外每个字段最大输入的长度是 32 个字符。完成关键词设定后，如果网站中整个或部分的 URL 字符串符合使用者定义的关键词，Vigor 路由器将会拒绝存取。值得注意的是，如果封锁关键词清单的关键词越精简，反应速度会更快。

范例： 如果您想要过滤任何 URL 字符串包含“sex”，“fuck”，“gun”，或“drug”的网站，您应该在字段中加入这些字。如此一来，只要 URL 字符串包含任何一个清单中的关键词，Vigor 路由器会自动禁止浏览。例如当使用者想要连上 [www.backdoor.net/images/sex /p_386.html](http://www.backdoor.net/images/sex/p_386.html)，Vigor 路由器会停止该联机，因为这个网站是被禁止的。而使用者可以浏览 www.backdoor.net/firewall/forum/d_123.html。此外，URL 内容过滤器也允许您在封锁关键词清单中指定一个完整的 URL 字符串(例如“www.whitehouse.com”和“www.hotmail.com”)，或者部分的 URL 字符串(例如“yahoo.com”)。之后，Vigor 路由器将会辨别出这些被禁止的 URL 并且中断该联机。

防止使用 IP 地址对网站进行访问: 此功能启用后将会禁止直接输入 IP 地址连

IP 过滤/防火墙设定

上该网站。在空白的方块点一下即可启用，而且(√)会出现。

允许例外子网： 有四个编号可供您使用，来指定一个特定的 IP 地址或者网段，使其不受 *URL 访问控制* 的限制。在空白的方块点一下即可启用，而且(√)会出现。然后您就可以输入您想指定的 IP 地址和子网掩码。

启用限制网络功能： 防范从网站下载恶意的程序代码的保护机制是很重要的。恶意的程序代码可能会隐藏在某些执行档，例如 *ActiveX*，*Java Applet*，*compressed files*，或 *executable files*。如果这些档案从网站下载之后，将会对使用者的系统带来威胁。例如，*ActiveX* 档案可以从网站下载后执行，万一 *ActiveX* 档案内含恶意的程序代码，它可能会无限制的存取使用者的系统。

Java	勾选以启用封锁 Java 文件功能。Vigor 将会从因特网上丢弃 Java 文件。
ActiveX	勾选以启用封锁 ActiveX 文件。任何从因特网上来的 ActiveX 文件会被拒绝。
压缩文件	勾选以启用封锁压缩文件功能，可预防有人下载压缩文件。下面列出 Vigor 路由器会封锁的压缩文件类型。 .zip .rar .arj .ace .cab .sit 在空白的方块点一下即可启用，而且(√)会出现。
可执行程序	勾选以启用封锁执行文件功能，可预防有人下载可执行程序。下面列出 Vigor 路由器会封锁的可执行程序类型。 .exe .com .scr .pif .bas .bat .inf .reg

在空白的方块点一下即可启用，而且(√)会出现。

由 Netscape 采用的 *cookie* 功能帮助您持续监视网络的活动,例如 HTTP 的请求以及每个 Session 的回应。很多网站利用 *cookie* 制造状态 Session 以追踪因特网使用者,这样有可能会侵犯使用者的隐私。所以, Vigor 路由器提供 *Cookie* 过滤机制,帮助您过滤从内流出的 *cookie*。此外, Vigor 路由器也帮助您过滤所有 proxy 相关的传送,以加强您的安全性。

Cookie	勾选以启用封锁 Cookie 传送功能， Vigor 路由器将过滤从内流出的 cookie，以保护内部使用者的隐私。												
代理	<p>勾选以启用此功能，可拒绝所有代理传送。在空白的方块点一下即可启用，而且(√)会出现。</p> <p>为了有效控制有限频宽的使用，提供封锁多媒体档案下载的机制是很有帮助的。在空白的方块点一下即可启用，而且(√)会出现。下面列出 Vigor 路由器会封锁档案类型。</p> <table><tr><td>.mov</td><td>.mp3</td><td>.rm</td><td>.ra</td><td>.au</td><td>.wmv</td></tr><tr><td>.wav</td><td>.asf</td><td>.mpg</td><td>.mpeg</td><td>.avi</td><td>.ram</td></tr></table>	.mov	.mp3	.rm	.ra	.au	.wmv	.wav	.asf	.mpg	.mpeg	.avi	.ram
.mov	.mp3	.rm	.ra	.au	.wmv								
.wav	.asf	.mpg	.mpeg	.avi	.ram								

时间表: 设定何时该采用 URL 内容过滤器机制。

一直封锁: 点选使得URL内容过滤器机制一直执行。

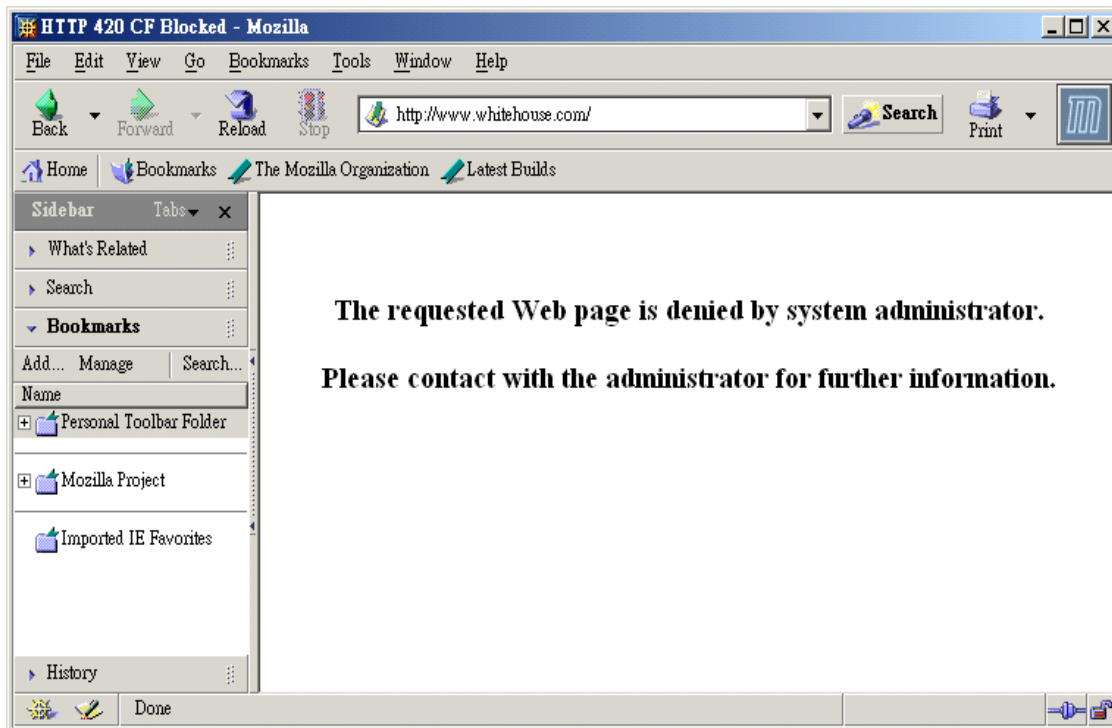
封锁时段自H1:M1 To H2:M2: 设定适当的时段, 从一天的H1:M1 到 H2:M2, 其中H1 和H2 表示小时, M1 和M2 表示分钟。

B.4 每周的: 设定一周中哪几天要使用URL内容过滤器机制。Vigor路由器支持两种选项, 每天或者一周中的某几天。如果您需要整周启用URL内容过滤器机制, 请点选“每天”, 否则您应该清楚指出在一周当中的哪几天。例如, 如果您希望URL

内容过滤器机制运作在周一到周三，那么请点选周一，周二，以及周三。在其它日子中，URL内容过滤器机制不会运作。

B.5 警告消息

当一个 HTTP 的请求被拒绝时，一个警告的画面将会出现在浏览器，如下图所示。



如果您有启用系统纪录功能，警告讯息将会自动送到系统纪录客户端。管理者可以在设定网页的**系统日志(Syslog)**/**邮件警示设定**设定系统纪录客户端。所以管理者可以透过 DrayTek Syslog daemon 中的 **URL 内容过滤器**看到警告讯息。这种警告讯息的格式跟 **IP 过滤器/防火墙**的相似，不同的地方在前头的关键词是“CF 加上被封锁的 HTTP 请求名称”。

IP 过滤/防火墙设定

> System Management > Syslog Access Setup

SysLog Access Setup

☒ Enable

Server IP Address: 192.168.1.10

Destination Port: 514

Cancel Clear OK

DrayTek Syslog

Controls: [Stop] [Pause] [Play] [Print] [Settings] 192.168.1.1

Vigor2900

LAN Status

TX Packets	RX Packets
1	2

WAN Status

Gateway IP (Static)	TX Packets	RX Rate
172.16.2.5	0	469
WAN IP (Static)	RX Packets	TX Rate
172.16.2.84	16	0

Fire Wall Log | VPN Log | User Access Log | Call Log | WAN Log | Network Information | Net State

Time	Host	Message
Jan 1 00:09:46	Vigor	CF java Block 192.168.1.11,1384 -> 210.59.230.160,80 PR tcp len 20 378 -PA -322980
Jan 1 00:09:45	Vigor	CF java Block 192.168.1.11,1381 -> 210.59.230.160,80 PR tcp len 20 381 -PA -325741
Jan 1 00:09:45	Vigor	CF java Block 192.168.1.11,1380 -> 210.59.230.160,80 PR tcp len 20 382 -PA -326241
Jan 1 00:09:45	Vigor	CF java Block 192.168.1.11,1379 -> 210.59.230.160,80 PR tcp len 20 382 -PA -326628
Jan 1 00:09:45	Vigor	CF java Block 192.168.1.11,1377 -> 210.59.230.160,80 PR tcp len 20 384 -PA -328021
Jan 1 00:09:45	Vigor	CF java Block 192.168.1.11,1378 -> 210.59.230.160,80 PR tcp len 20 381 -PA -327232
Jan 1 00:09:45	Vigor	CF java Block 192.168.1.11,1376 -> 210.59.230.160,80 PR tcp len 20 382 -PA -329186
Jan 1 00:09:29	Vigor	CF keyword Block 192.168.1.11,1372 -> www.google.com/search?q=fuck&ie=utf-8&o
Jan 1 00:09:09	Vigor	CF keyword Block 192.168.1.11,1374 -> www.yahoo.com/sex/index.php,80 PR tcp len
Jan 1 00:08:48	Vigor	CF keyword Block 192.168.1.11,1373 -> www.whitehouse.com/,80 PR tcp len 20 294 -

ADSL Status

Mode	State	Up Speed	Down Speed	SNR Margin	Loop Att
---	---	---	---	---	---

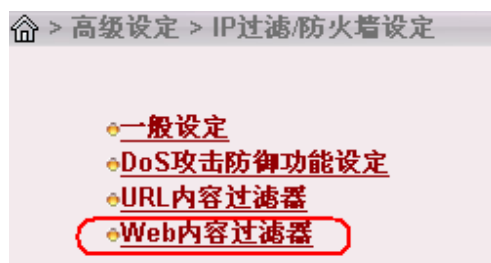
第 11-C 章

Web 内容过滤器

C.1 Web 内容过滤器概述

通过 CPA 服务器,可以对以归类的网站按类别来禁止对其的访问。

单击**Web 内容过滤器**进入配置页面:

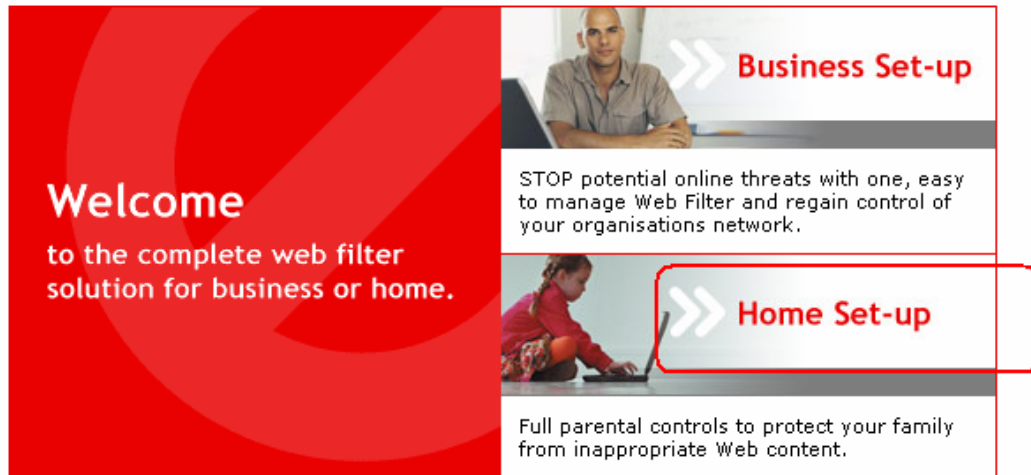


C.2 设定

选择一个 CPA 服务器,单击**激活免费使用 and 购买申请**



点选 Home Set-up



Welcome
to the complete web filter
solution for business or home.

Business Set-up
STOP potential online threats with one, easy to manage Web Filter and regain control of your organisations network.

Home Set-up
Full parental controls to protect your family from inappropriate Web content.



注册一个用户名:



Web Filter Set-up

Welcome to full parental controls for the HOME user.

» **Step 1**

» Step 2

» Step 3

By activating the easy to use software as part of your new router, you can easily control where your family surf on the Web, ensuring safe Internet access for all the family providing you with peace of mind, without restricting your childrens natural curiosity.

To enable your **30 day FREE TRIAL** or **Purchase a subscription now**, please enter your name and e-mail address below. On receipt, you will be sent a confirmation e-mail providing you with a link to activate your licence.

First Name *

Last Name

E-mail address *

Confirm E-mail address *

☒ I have read and accepted the [Terms & Conditions](#) below

» Purchase Subscription

» Activate Free Trial

Powered by



Terms & Conditions


Refund Policy

Contact Info

Hosted by
PowerNet
Internet Logistics Center

11-32

在用邮件认证后完成注册:



Web Filter Set-up

Thank you for activating your 30 day Web Filtering free trial

» Step 1

» Step 2

» Step 3

To complete the set-up, select the categories you wish to block in your routers configuration. Below are suggested categories that you might want to stop your family accessing.


Family categories to consider always restricting:
Adult/Sexually explicit, Criminal Skills, Drugs, Tobacco and Alcohol, Gambling, Hacking, Hate Speech, Violence, Weapons

Additional categories to consider restricting for younger children in the home:
Chat, Glamour & Intimate Apparel, Dating (Personals), Photo Searches, Usenet News, Sex Education

» If no categories are selected ALL Web content will be available to your family.

» Close

Powered by



[Terms & Conditions](#)[Refund Policy](#)[Contact Info](#)

Hosted by
PowerNet
Internet Logistics Center

IP 过滤/防火墙设定

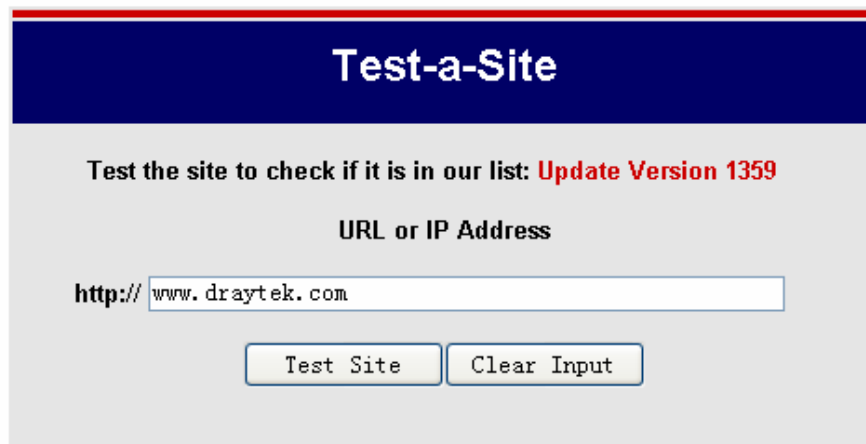
您可以点击**测试站点**以验证其是否已经归类
查看您想要block的网站类型：



输入“www.draytek.com”：

SurfControl Content Portal Authority Test-A-Site

Our Test-a-Site allows you to verify whether a site is categorized in our most recent filters.
After testing a site, you can choose to submit each site for review.



Test-a-Site

Test the site to check if it is in our list: **Update Version 1359**

URL or IP Address

http://

URLs and IP Addresses of the same site may be categorized differently.
For complete information, test both the URL and the IP of the site.

得到如下结果：计算机/网络

Test Results

www.draytek.com is in our list and categorized as **Computing & Internet**

If you would like to submit this URL for review, please click the button below.

Submit A Site

Test Another Site

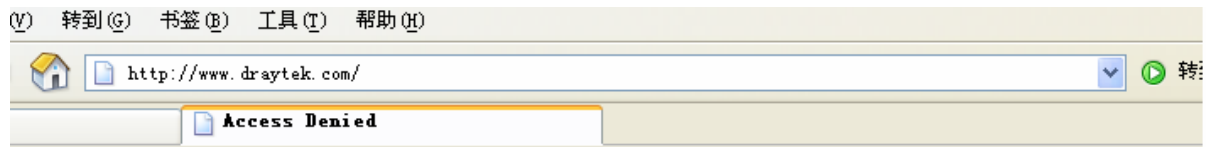
然后在计算机/网络前打勾：

☒ 启用Web内容过滤

组	分类(选中过滤。取消选中则不过滤)		
保护儿童	<input type="checkbox"/> 聊天	<input type="checkbox"/> 犯罪	<input type="checkbox"/> 烟酒
<div>全部选择</div>	<input type="checkbox"/> 赌博	<input type="checkbox"/> 黑客	<input type="checkbox"/> 粗口
<div>全部清除</div>	<input type="checkbox"/> 性	<input type="checkbox"/> 暴力	<input type="checkbox"/> 武器
休闲	<input type="checkbox"/> 广告	<input type="checkbox"/> 娱乐	<input type="checkbox"/> 食品
<div>全部选择</div>	<input type="checkbox"/> 游戏	<input type="checkbox"/> 时尚	<input type="checkbox"/> 健康
<div>全部清除</div>	<input type="checkbox"/> 业余爱好	<input type="checkbox"/> 生活方式	<input type="checkbox"/> 骑车
	<input type="checkbox"/> 婚介/约会	<input type="checkbox"/> 相片搜索	<input type="checkbox"/> 购物
	<input type="checkbox"/> 体育	<input type="checkbox"/> 流媒体	<input type="checkbox"/> 旅游
商业	<input checked="" type="checkbox"/> 计算机/网络	<input type="checkbox"/> 金融	<input type="checkbox"/> 求职
<div>全部选择</div>	<input type="checkbox"/> 政治	<input type="checkbox"/> 房地产	<input type="checkbox"/> 参考资料
<div>全部清除</div>	<input type="checkbox"/> 远程代理	<input type="checkbox"/> 搜索引擎	<input type="checkbox"/> Web邮件
其他	<input type="checkbox"/> 教育	<input type="checkbox"/> 主页托管站	<input type="checkbox"/> 儿童站点
<div>全部选择</div>	<input type="checkbox"/> 新闻	<input type="checkbox"/> 宗教	<input type="checkbox"/> 性教育
<div>全部清除</div>	<input type="checkbox"/> 新闻组	<input type="checkbox"/> Block all uncategorised sites	

此时对www.draytek.com的访问将被禁止：

IP 过滤/防火墙设定



The requested Web page is categorized as "computing"
and has been blocked by Web Content Filter.

Please contact your system administrator for further information.