


第十章 防火墙及配置

.1 防火墙介绍



防火墙的概念

简单的说，防火墙的作用是在保护一个网络免受“不信任”网络的攻击的同时，保证两个网络之间可以进行合法的通信。防火墙应该具有如下基本特征：

- 经过防火墙保护的网路之间的通信必须都经过防火墙。
- 只有经过各种配置的策略验证过的合法数据包才可以通过防火墙。
- 防火墙本身必须具有很强的抗攻击、渗透能力。


<http://www.kinth.com>

现代的防火墙体系不应该只是一个“入口的屏障”，防火墙应该是几个网络的接入控制点，所有经过被防火墙保护的网路的数据流都应该首先经过防火墙，形成一个信息进入的关口。

因此防火墙不但可以保护内部网路在 Internet 中的安全，同时还可以保护若干主机在一个内部网路中的安全。在每一个被防火墙分割的网路中，所有的计算机之间是被认为“可信任的”，它们之间的通信不受防火墙的干涉。而在各个被防火墙分割的网路之间，必须按照防火墙规定的“策略”进行互相的访问。

.2 网络安全技术

.2.1 网络安全技术介绍

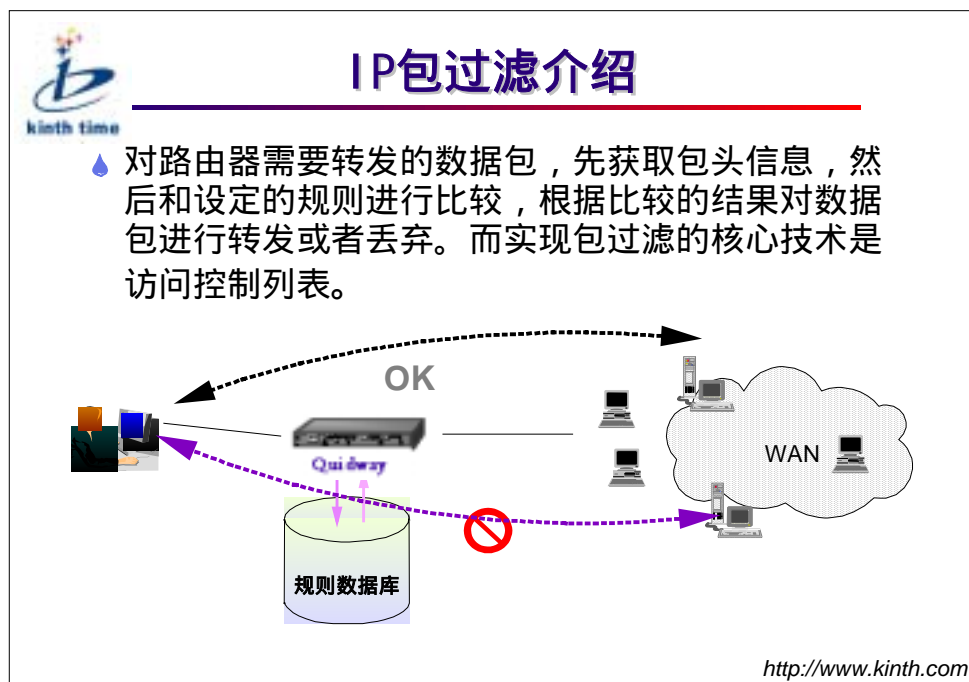


网络安全介绍

- ◆ Quidway 系列路由器提供一个全面的网络安全解决方案，包括用户验证、授权、数据保护等。
- ◆ Quidway系列路由器所采用的安全技术主要包括：
 - 包过滤技术 - 针对IP地址的一种访问控制
 - AAA验证 - 对用户进行验证、授权、计费的技术
 - 地址转换 - 屏蔽内部网络地址的一种技术
 - VPN技术 - 提供一种安全“私有连接”的技术
 - 智能防火墙 - 可以针对内容等进行访问控制的技术
 - 加密和密钥管理技术
- ◆ 在路由器中，包过滤技术是实现防火墙的最重要的手段。

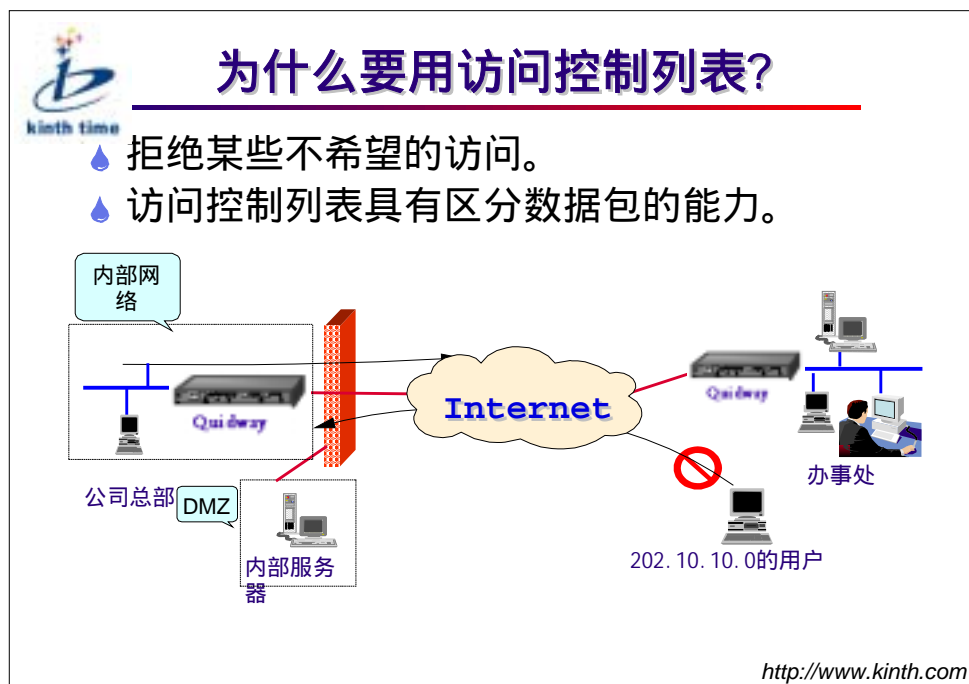
<http://www.kinth.com>

2.2 IP 包过滤技术介绍



包过滤技术主要是设定一定的规则，控制数据包。路由器会根据设定的规则和数据包的包头信息比较，来决定是否允许这个数据包通过。实现包过滤技术最核心内容就是访问控制列表。

.2.3 访问控制列表



用户可以通过 Internet 和外部网络进行联系，网络管理员都面临着一个问题，就是如何拒绝一些不希望的连接，同时又要保证合法用户进行的访问。

为了达到这样的效果，我们需要有一定的规则来定义哪些数据包是“合法”的（或者是可以允许访问），哪些是“非法”的（或者是禁止访问）。这些规则就是访问控制列表。

访问控制列表（续）



为什么要用访问控制列表？（续）

- 💧 访问控制列表按照数据包的特点，规定了一些规则。
 - 这些规则描述了具有一定特点的数据包，并且规定它们是被“允许”的还是“禁止”的。
 - 这些规则的定义是按照数据包包头的特点定义的，例如可以这样定义：
 - 允许202.38.0.0/16网段的主机可以使用协议
 - HTTP 访问129.10.10.1。
 - 禁止从202.110.0.0/16网段的所有访问。

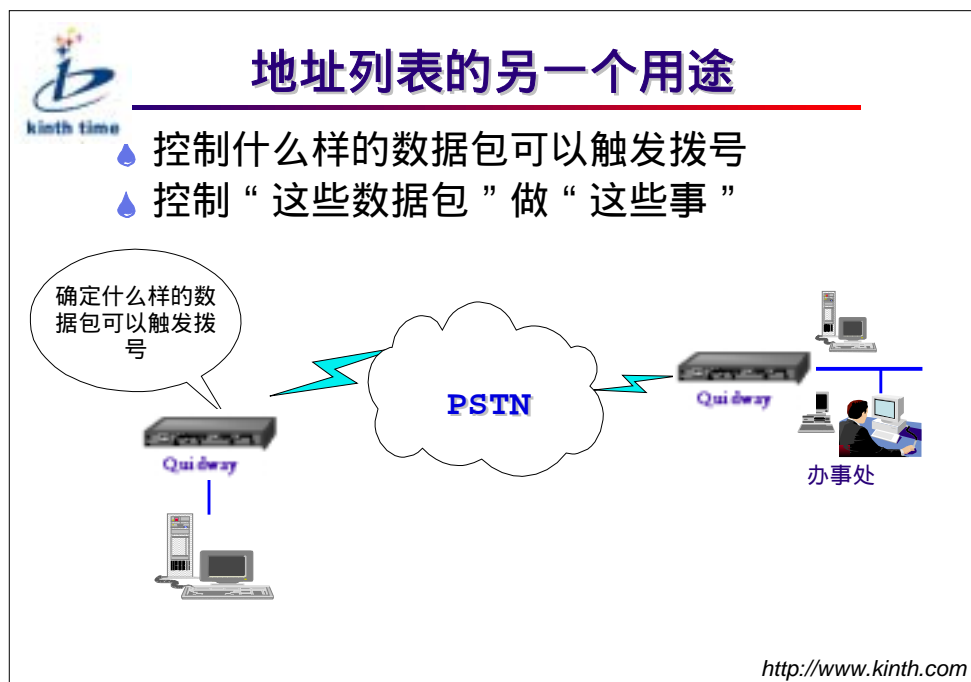
<http://www.kinth.com>

访问控制列表就可以提供这样的功能，它按照数据包的特点，规定了一些规则。

这些规则描述了具有一定特点的数据包，（例如所有源地址是202.10.10.0 地址段的数据包、所有使用 Telnet 访问的数据包等等）并且规定它们是被“允许”的还是“禁止”的。

这样可以将访问控制列表规则应用到路由器的接口，阻止一些非法的访问，同时并不影响合法用户的访问。访问控制列表提供了一种区分数据包种类的手段，它把各种数据包按照各自的特点区分成各种不同的种类，达到控制用户访问的目的。

.2.4 地址列表的其他用途

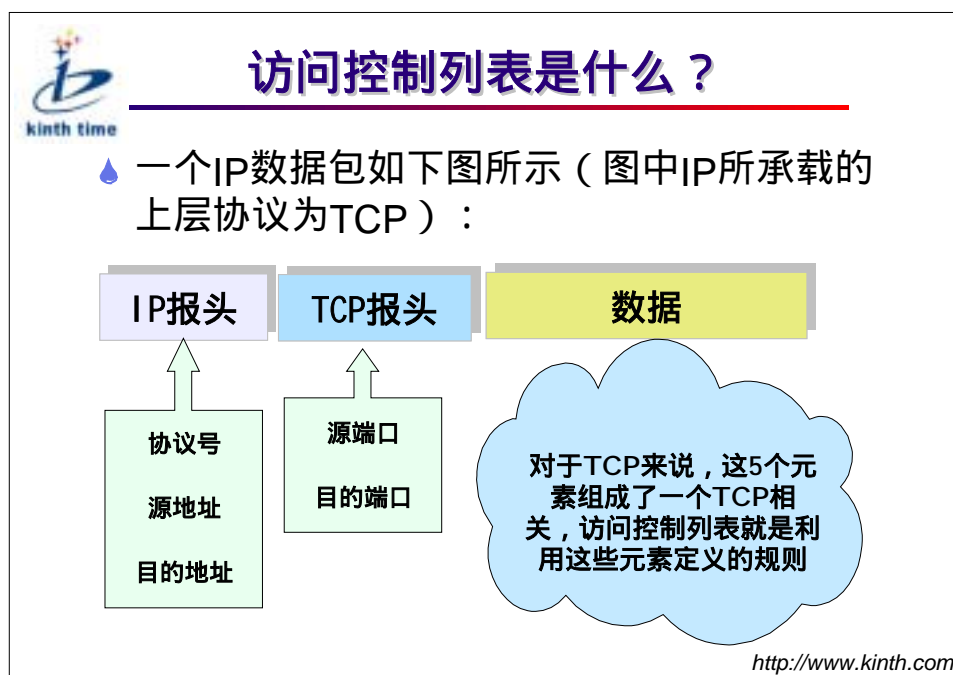


由于访问控制列表具有区分数据包的功能，因此，访问控制列表可以控制“什么样的数据包”，可以做什么样的事情。

例如，当企业内部网通过拨号方式访问 Internet，如果不希望所有的用户都可以拨号上网，就可以利用控制列表决定哪些主机可以触发拨号，以达到访问 Internet 的目的。

利用访问控制列表可以控制数据包的触发拨号，同样在 IPSec、地址转换等应用中，可以利用控制列表描述什么样的数据包可以加密，什么样的数据包可以地址转换等。

.2.5 访问控制列表原理



IP 数据包具有一定的特征，例如，对于每个 TCP 数据包，都包含有上图所示的 5 个元素，利用这 5 个元素就可以描述出一个数据包的特征。访问控制列表利用的就是这些包头的信息来定义规则的。

访问控制列表原理（续）

**访问控制列表是什么？（续）**

同时访问控制列表还表述出是“拒绝”或是“允许”这些数据包。例如你可以用访问表描述：

不让任何机器使用Telnet登录。

可以让每个机器经由SMTP向我们发送电子邮件。


那机器经由NNTP能把新闻发给我们，但是没有其他机器能这样做。然而，你不可以这样说：

这个用户能从外部远程登录，但是其它用户不能这样做。因为“用户”不是访问控制列表所能辨认的。

你能发送这些文件而不能发送那些文件。因为“文件”也不是包过滤系统所能辨认的。

<http://www.kinth.com>

访问控制列表原理（续）



如何使用通配比较位

- 通配比较位和子网掩码相似，但写法不同：
 - 0表示需要比较
 - 1表示忽略比较
- 通配比较和IP地址结合使用，可以描述一个地址范围

0	0	0	255	只比较前24位
0	0	255	255	只比较前16位
255	255	255	0	只比较后8位

<http://www.kinth.com>

通配比较位的意义和子网掩码很相似，但是用法上是不一样的。利用通配比较位可以定义一个范围内的地址。例如定义一个 10.110.0.0/16 网段的所有主机。

访问控制列表原理（续）




如何使用通配比较位（续）

💧 IP地址与地址通配位的关系语法规则如下：在通配位中相应位为1的地址中的位在比较中被忽略。IP地址与通配位都是32位的数。

- 如通配位是0x00ffffff (0. 255. 255. 255) ，则比较时，高8位需要比较，其他的都被忽略。
- 又如IP地址是129. 102. 1. 1，通配位是0. 0. 255. 255，则地址与通配位合在一起表示129. 102. 0. 0网段。
- 若要表示202. 38. 160. 0网段，地址位写成202. 38. 160. X (X是0-255之间的任意一个数字) ，通配位为0. 0. 0. 255。

<http://www.kinth.com>

访问控制列表原理（续）



如何标识访问控制列表？

- 利用数字标识访问控制列表
- 利用数字范围标识访问控制列表的种类。

列表的种类	数字标识的范围
IP 标准列表	1-99
IP 扩展列表	100 - 199

<http://www.kinth.com>

在配置访问控制列表时，有一个规则序列号，利用这个规则序列号来标识访问控制列表，同时提供了引用访问控制列表的方法。

规则序列号的范围表示了它属于什么样的访问控制列表。例如：

```
access-list 1 permit 202.110.10.0 0.0.0.255
```

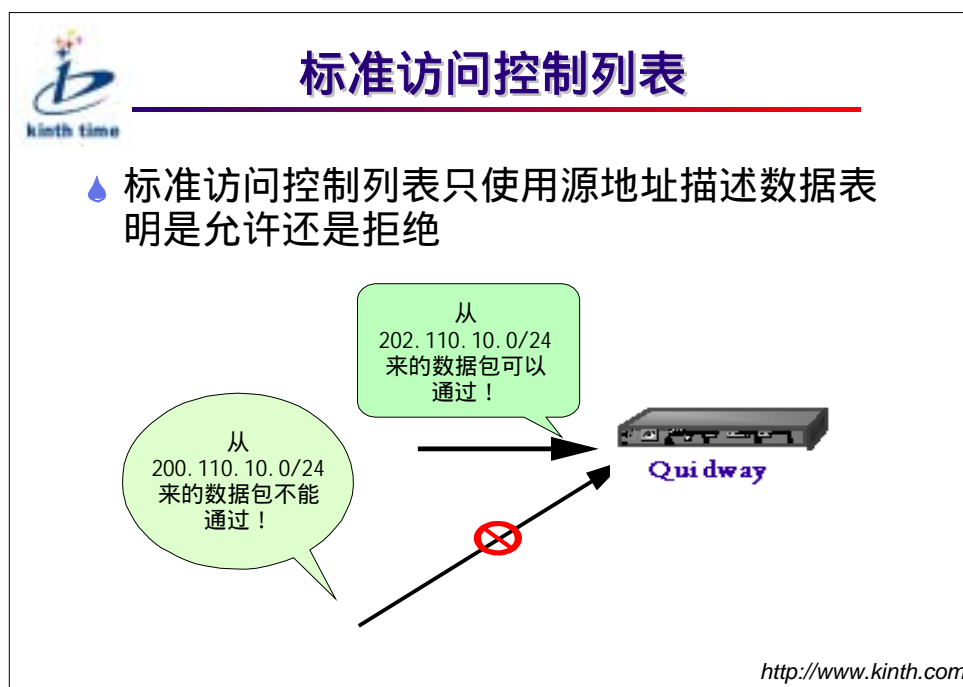
表示序号为 1 的访问控制列表，它是标准访问列表。

```
access-list 100 deny udp any any eq rip
```

表示序号为 100 的访问控制列表，它是扩展访问列表。

.3 标准访问控制列表

.3.1 标准访问控制列表概况



标准列表的规则序列号的范围为：1~99。

标准列表只使用 1 个条件判别数据包：数据包的源地址。

标准访问列表可以指定一个源地址段，这是由 IP 地址和地址通配符组合定义的一个地址段。

.3.2 标准访问控制列表的命令配置



标准访问控制列表

配置标准访问列表的格式如下：

```
access-list [normal|special] listnumber  
{ permit | deny } ip-address [ wildcard-mask ]
```

<http://www.kinth.com>

此格式表示：允许或拒绝来自指定网络的数据包，该网络由 IP 地址（ip-address）和地址通配掩码位（wildcard-mask）指定。其中：normal 和 special 表示该规则是在普通时间段中有效还是在特殊时间段中有效。

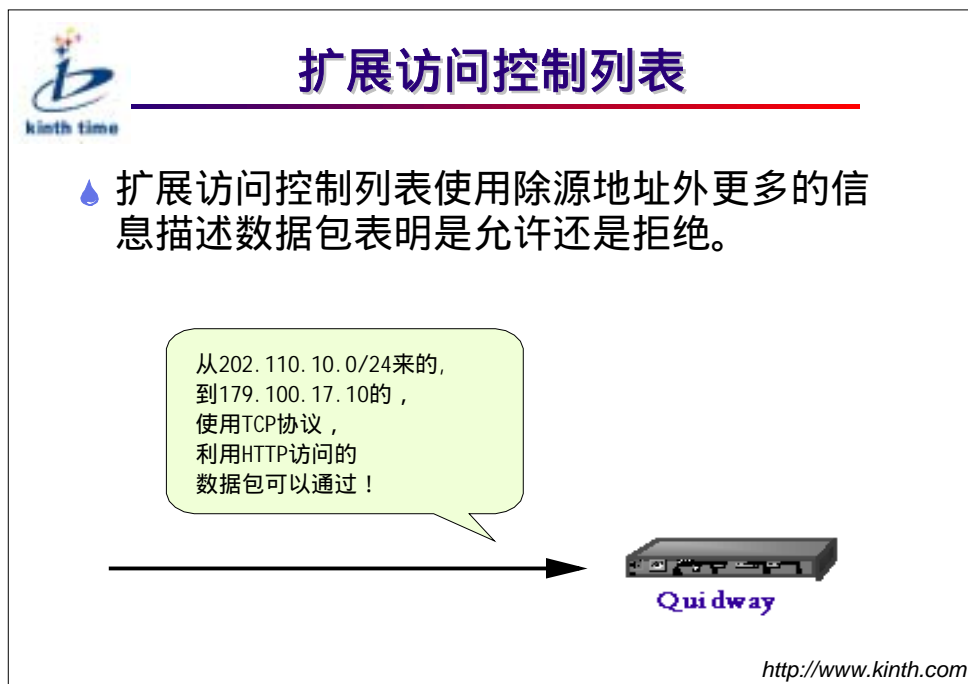
listnumber 为规则序号，标准访问列表的规则序号范围为 1-99。

permit 和 deny 表示允许或禁止满足该规则的数据包通过。

ip-address 和 wildcard-mask 分别为 IP 地址和通配比较位，用来指定某个网络。如果 IP 地址指定为 any，则表示所有 IP 地址，而且不需配置指定相应的通配位（通配位缺省为 0.0.0.0）。

.4 扩展访问控制列表

.4.1 扩展访问控制列表概况




扩展列表使用数据包的源地址的同时，还使用目的地址，和协议号（TCP、UDP 等）。

对于 TCP、UDP 协议可以同时使用目的端口号。

例如，利用扩展列表可以描述“从 202.110.10.0/24 的网段到 110.10.10.0/24 的网段的所有 IP 数据包是被拒绝的”，或者“从 202.110.10.0/24 网段到 110.10.10.0/24 网段的所有 Telnet（使用 TCP 协议的 23 端口）访问是被拒绝的”。它们到底如何表示？我们将从具体配置命令来入手来介绍。

4.2 扩展访问控制列表的配置命令



扩展访问控制列表的配置命令

- 配置TCP/UDP协议的扩展访问列表：
`access-list [normal | special] listnumber { permit | deny } { tcp | udp } source-addr [source-mask] dest-addr [dest-mask] [operator port1 [port2]] [log]`
- 配置ICMP协议的扩展访问列表：
`access-list [normal | special] listnumber { permit | deny } icmp source-addr [source-mask] dest-addr dest-mask [icmp-type [icmp-code]] [log]`
- 配置其它协议的扩展访问列表：
`access-list [normal | special] listnumber { permit | deny } protocol source-addr [source-mask] dest-addr [dest-mask] [log]`

<http://www.kinth.com>

Normal 和 special 表示该规则是在普通时间段生效还是在特殊时间段有效，缺省的情况是在普通时间段。

Listnumber 为规则序号，扩展访问列表的规则序号范围为 100-199。

Permit 和 deny 表示允许或禁止满足该规则的数据包通过。


Protocol 可以指定为 0-255 之间的任一协议号（如 1 表示 ICMP 协议），对于常见协议（如 TCP 和 UDP、ICMP），可以直观地指定协议名，若指定为 IP，则该规则对所有 IP 包均起作用。

source-addr 和 source-mask 分别为源地址和源地址的通配符。

Dest-addr 和 dest-mask 分别为目的地址和目的地址的通配符。如果 IP 地址指定为 any，则表示所有 IP 地址，而且不需配置指定相应的通配位（通配位缺省为 0.0.0.0）。

operator port1 - port2 用于指定端口范围，缺省为全部端口号 0-65535，只有 TCP 和 UDP 协议需要指定端口范围。operate 的意义如下页表所示。

扩展访问列表的操作符 operate 定义



扩展访问控制列表操作符的含义：

操作符及语法	意义
eg portnumber	等于端口号portnumber
gt portnumber	大于端口号portnumber
lt portnumber	小于端口号portnumber
neg portnumber	不等于端口号portnumber
range portnumber1 portnumber2	介于端口号portnumber1 和 portnumber2 之间

<http://www.kinth.com>

在指定 portnumber 时,对于常用的端口号可以使用“助记符”代替。如 FTP、Telnet 等。

下列表格所列为可能用到的各类端口号与助记符的对照表，供参照*。

协议	助记符	意义及实际值
TCP	Bgp	Border Gateway Protocol (179)
	Chargen	Character generator (19)
	Cmd	Remote commands (rcmd, 514)
	Daytime	Daytime (13)
	Discard	Discard (9)
	Domain	Domain Name Service (53)
	Echo	Echo (7)
	Exec	Exec (rsh, 512)
	Finger	Finger (79)
	Ftp	File Transfer Protocol (21)
	Ftp-data	FTP data connections (20)
	Gopher	Gopher (70)
	Hostname	NIC hostname server (101)
	Irc	Internet Relay Chat (194)
	Klogin	Kerberos login (543)
	Kshell	Kerberos shell (544)
	Login	Login (rlogin, 513)
	Lpd	Printer service (515)

	Nntp	Network News Transport Protocol (119)
	Pop2	Post Office Protocol v2 (109)
	Pop3	Post Office Protocol v3 (110)
	Sntp	Simple Mail Transport Protocol (25)
	Sunrpc	Sun Remote Procedure Call (111)
	Syslog	Syslog (514)
	Tacacs	TAC Access Control System (49)
	Talk	Talk (517)
	Telnet	Telnet (23)
	Time	Time (37)
	Uucp	Unix-to-Unix Copy Program (540)
	Whois	Nickname (43)
	Www	World Wide Web (HTTP, 80)
UDP	biff	Mail notify (512)
	bootpc	Bootstrap Protocol Client (68)
	bootps	Bootstrap Protocol Server (67)
	discard	Discard (9)
	dns	Mail notify (512)
	dnsix	DNSIX Securit Attribute Token Map (90)
	echo	Echo (7)
	mobileip-ag	MobileIP-Agent (434)
	mobileip-mn	MobilIP-MN (435)
	nameserver	Host Name Server (42)
	netbios-dgm	NETBIOS Datagram Service (138)
	netbios-ns	NETBIOS Name Service (137)
	netbios-ssn	NETBIOS Session Service (139)
	ntp	Network Time Protocol (123)
	rip	Routing Information Protocol (520)
	snmp	SNMP (161)
	snmptrap	SNMPTRAP (162)
	sunrpc	SUN Remote Procedure Call (111)
	syslog	Syslog (514)
	tacacs-ds	TACACS-Database Service (65)
	talk	Talk (517)
	tftp	Trivial File Transfer (69)
	time	Time (37)
	who	Who(513)
	xdmcp	X Display Manager Control Protocol (177)

对于 ICMP 协议可以指定 ICMP 报文类型，缺省为全部 ICMP 报文。指定 ICMP 报文类型时，可以用数字（0-255），也可以用助记符。助记符如下：

助记符	意义
echo	Type=8, Code=0
echo-reply	Type=0, Code=0
fragmentneed-DFset	Type=3, Code=4

host-redirect	Type=5, Code=1
host-tos-redirect	Type=5, Code=3
host-unreachable	Type=3, Code=1
information-reply	Type=16, Code=0
information-request	Type=15, Code=0
net-redirect	Type=5, Code=0
net-tos-redirect	Type=5, Code=2
net-unreachable	Type=3, Code=0
parameter-problem	Type=12, Code=0
port-unreachable	Type=3, Code=3
protocol-unreachable	Type=3, Code=2
reassembly-timeout	Type=11, Code=1
source-quench	Type=4, Code=0
source-route-failed	Type=3, Code=5
timestamp-reply	Type=14, Code=0
timestamp-request	Type=13, Code=0
ttl-exceeded	Type=11, Code=0

4.3 扩展访问控制列表的举例



扩展访问控制列表举例


100 deny icmp 10.1.0.0 0.0.255.255 any host-redirect
禁止从10.1.0.0网段发来的ICMP 主机不可达报文通过。

100 deny tcp 129.9.0.0 0.0.255.255 202.38.160.0
0.0.0.255 eq www log
该规则序号为100，禁止从129.9.0.0网段内的主机
建立与202.38.160.0网段内的主机的www端口（80）的
连接，并对违反此规则的事件作日志。

102 deny udp 129.9.8.0 0.0.0.255 202.38.160.0
0.0.0.255 gt 128
该规则序号为102，禁止从129.9.8.0网段内的主机
建立与202.38.160.0网段内的主机的端口号大于128的
UDP（用户数据报协议）连接。

<http://www.kinth.com>

.5 多条规则的组合



多条规则的组合

- 一条访问列表可以由多条规则组成
- 多条规则使用同样的序号
- 对冲突规则判断的依据是“深度”，也就是描述的地址范围越小的，将会优先考虑。
- 深度的判断要依靠通配比较位和IP地址结合比较

```
access-list 4 deny 202.38.0.0 0.0.255.255
access-list 4 permit 202.38.160.1 0.0.0.255
```

两条规则结合则表示禁止一个大网段
(202. 38. 0. 0) 上的主机但允许其中的一小部分主
机 (202. 38. 160. 0) 的访问。

<http://www.kinth.com>

可以使用相同的序号，建立多条规则，构成一个访问控制列表。

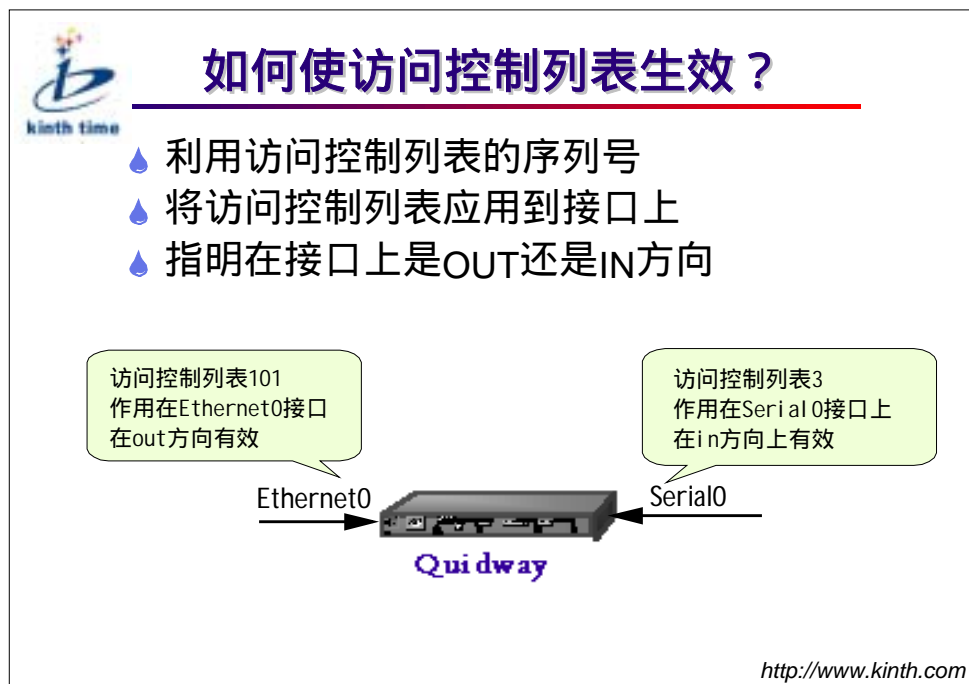
对于两条有冲突的规则或是有地址重叠的情况，判断的依据是“深度”，也就是描述的地址范围越小的，将会优先考虑。例如：

```
access-list 1 permit 202.38.160.0 0.0.255.255
access-list 1 deny 202.38.160.0 0.0.0.255
```

对于 202.38.160.23 这样的地址，访问列表是认为是拒绝的。因为第二条指定的地址范围小。

.6 访问列表的生效

.6.1 访问列表的生效



为了使访问控制列表生效，将访问控制列表定义在接口上。
具体命令配置如下页所示。

.6.2 访问列表在接口生效的命令配置




访问列表在接口生效命令配置

- 💧 基于接口配置访问列表，使访问列表生效
 - [no] ip access-group 命令
 - ➔ ip access-group *listnumber* { in|out }
 - ➔ no ip access-group *listnumber* { in|out }
- 💧 实例
 - ➔ 在Serial 0口配置模式下执行
 - ➔ ip access-group 1 in
将在Serial 0口上，对进入的数据包，使用访问控制列表1进行过滤。

<http://www.kinth.com>

.7 防火墙基本配置任务列表

.7.1 防火墙基本配置任务



防火墙配置任务列表

- 配置防火墙至少具有以下几个基本步骤：
 - 允许/禁止防火墙（Quidway系列路由器默认是禁止防火墙功能）
 - 定义访问控制列表（标准或扩展）
 - 在接口上应用访问控制列表
- 按照需求可以扩展以下应用：
 - 设置防火墙的缺省过滤模式
 - 允许或禁止时间段过滤
 - 设定特殊时间段
 - 指定日志主机
 - 显示配置状况

<http://www.kinth.com>

前面我们零星的介绍了 Quidway 系列路由器配置防火墙的相关内容，本页所示为完成防火墙配置的步骤。

在实际的使用中，还可能用到以下的扩展应用：

1. 设置防火墙的缺省过滤模式；
2. 允许或禁止时间段；
3. 设定时间段；
4. 允许日志主机；
5. 指定日志主机；
6. 显示配置状况。

其中，2 和 4 均在配置访问列表中设置，1、3、5 和 6 由专门的命令完成。

.7.2 防火墙的属性配置命令



防火墙的属性配置命令

- 💧 Firewall 命令
 - ➔ firewall { enable | disable }
- 💧 Firewall default 命令
 - ➔ firewall default { permit|deny }
- 💧 Show firewall 命令
 - ➔ show firewall

<http://www.kinth.com>

属性命令中，首先是打开防火墙的操作：

firewall {enable | disable} 允许/ 禁止防火墙过滤；

其次，是设置防火墙的缺省过滤模式的操作：

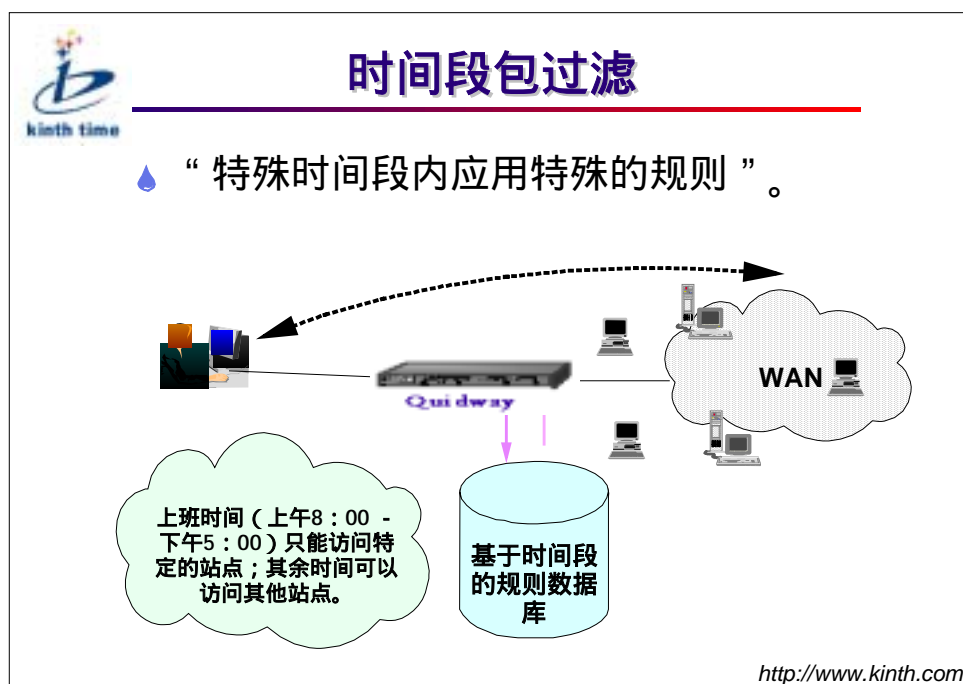
firewall default {permit | disable } 缺省方式是禁止还是允许；

缺省过滤模式用以定义对访问列表控制以外的 IP 或者 TCP 等数据包的处理，

Quidway 系列路由器防火墙的默认过滤模式是允许。

用 show firewall 命令可以 显示防火墙状态信息。

.7.3 时间段包过滤



基于时间段,用户可以指定一天 24 小时中的任意时间段为特殊时间段 (可以是多个),不在任何特殊时间段的其他时间称为普通时间段。用户在定义访问列表时,可以指定该规则是在特殊时间段还是在普通时间段生效。

时间段包过滤（续）



时间段的配置命令

- 💧 timerange 命令
 - ➡ timerange { enable|disable }
- 💧 [no] settr 命令
 - ➡ settr begin-time end-time [begin-time end-time]
 - ➡ no settr
- 💧 show isintr 命令
 - ➡ show isintr
- 💧 show timerange 命令
 - ➡ show timerange

http://www.kinth.com

timerange { enable|disable } 允许 | 禁止时间段

Quidway 防火墙默认为禁止时间段。

settr begin-time end-time [begin-time end-time] 设置特殊时间段

show isintr 显示当前时间是否在特殊时间段内

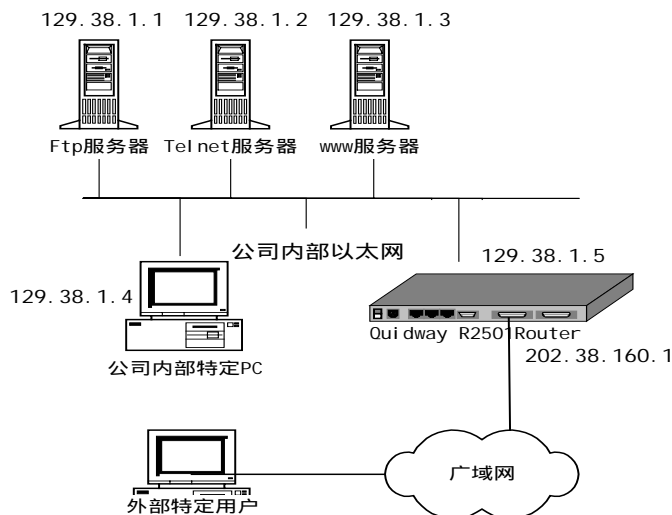
show timerange 显示配置的时间段

.8 防火墙配置举例

.8.1 组网图



典型防火墙配置案例 - 组网图



<http://www.kinth.com>

某公司通过一台 Quidway 2501 路由器的接口 Serial0 访问 Internet，公司内部对外提供 www、ftp 和 telnet 服务，公司内部子网为 129.38.1.0，其中，内部 ftp 服务器地址为 129.38.1.1，内部 telnet 服务器地址为 129.38.1.2，内部 www 服务器地址为 129.38.1.3，公司对外地址 202.38.160.1。在路由器上配置了地址转换，这样内部特定 PC 机（129.38.1.4）可以访问 Internet，外部 PC 可以访问内部服务器。通过配置防火墙，希望实现以下要求：

外部网络只有特定用户可以访问内部服务器。

内部网络只有特定主机可以访问外部网络。

假定外部特定用户的 IP 地址为 202.39.2.3。

.8.2 组网需求与配置



典型防火墙配置案例 - 组网需求

某公司通过一台Quidway 2501路由器的接口Serial0 访问Internet，公司内部对外提供www、ftp 和 telnet 服务，公司内部子网为129.38.1.0，其中，内部 ftp 服务器地址为129.38.1.1，内部telnet服务器地址为129.38.1.2，内部www服务器地址为129.38.1.3，公司对外地202.38.160.1。在路由器上配置了地址转换，这样内部PC机可以访问Internet，外部PC可以访问内部服务器。通过配置防火墙，希望实现以下要求：

- 外部网络只有特定用户可以访问内部服务器。
- 内部网络只有特定主机可以访问外部网络。
- 假定外部特定用户的IP地址为202.39.2.3。

<http://www.kinth.com>

参考配置如下：

允许防火墙：

```
Quidway(config)# firewall enable
```

设置防火墙缺省过滤方式为允许包通过：

```
Quidway(config)# firewall default permit
```

配置访问规则禁止所有包通过：

```
Quidway(config)# access-list 100 deny ip any any
```

配置规则允许特定主机（129.38.1.4）访问外部网，允许内部服务器访问外部网：

```
Quidway(config)# access-list 101 permit ip 129.38.1.4 0 any
```

```
Quidway(config)# access-list 101 permit ip 129.38.1.1 0 any
```

```
Quidway(config)# access-list 101 permit ip 129.38.1.2 0 any
```

```
Quidway(config)# access-list 101 permit ip 129.38.1.3 0 any
```

配置规则允许特定用户从外部网访问内部服务器：

```
Quidway(config)# access-list 102 permit tcp 202.39.2.3 0 202.38.160.1 0
```

配置规则允许特定用户从外部网取得数据（只允许端口号大于 1024 的包）：

```
Quidway(config) # access-list 102 permit tcp any 202.38.160.1 0 gt 1024
```

```
Quidway(config) # access-list normal 102 deny ip any any
```

将规则 100 作用于从接口 Ethernet0 进入的包：

```
Quidway(config)# interface ethernet 0
```

```
Quidway(config-if-Ethernet0)# ip access-group 100 in
```

将规则 101 作用于从接口 Ethernet0 进入的包：

```
Quidway(config-if-Ethernet0)#ip access-group 101 in
将规则 102 作用于从接口 Serial0 进入的包：
Quidway(config-if-Serial0)# ip access-group 102 in
在接口 Serial0 上作地址转换：
Quidway(config-if-Serial0)# nat enable
在全局模式下配置 Nat server  ：
natserver ftp host 129.38.1.1
natserver telnet host 129.38.1.2
natserver www host 129.38.1.3
其他内容如各端口 IP 地址，封装协议等这里不再赘述。
```

.9 本章重点



本章重点

- 💧 包过滤原理；
- 💧 标准访问列表的配置原则；
- 💧 扩展访问列表的配置原则；
- 💧 在端口上引用访问控制列表实现防火墙功能

<http://www.kinth.com>