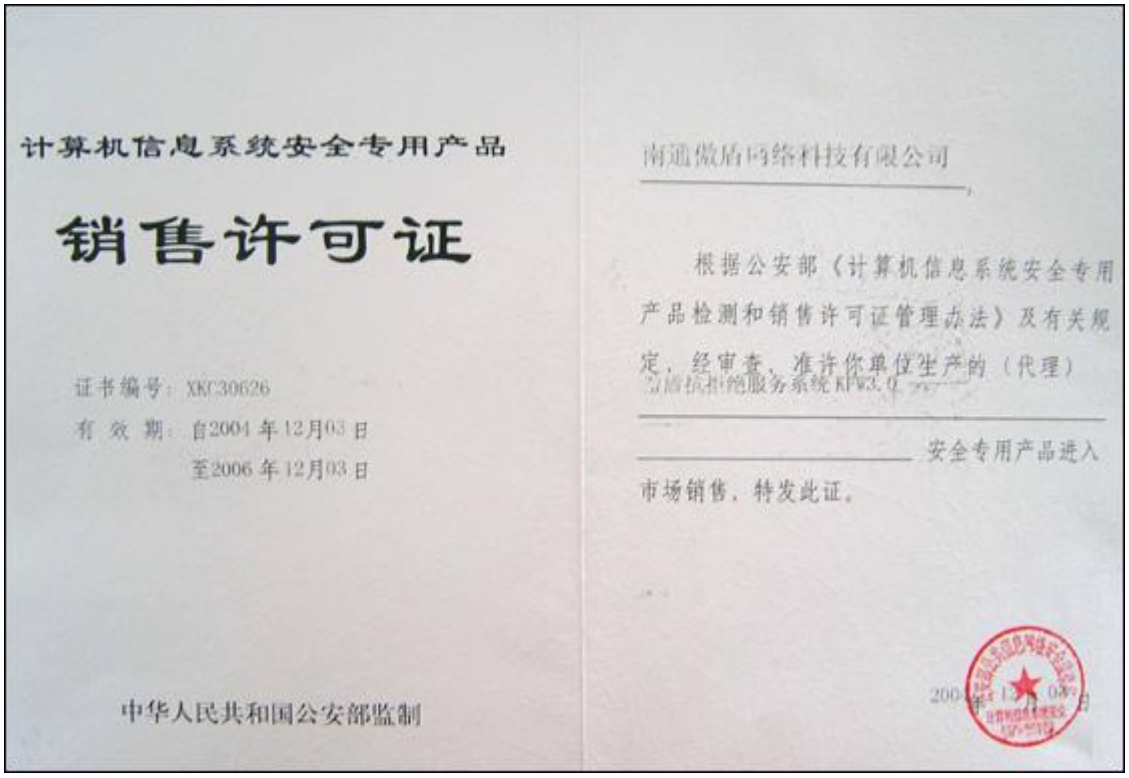
KFW 傲盾防火墙服务器版
(3.2)版
使用手册

地址：厦门软件园盛世大厦 1-4 楼（软件技术服务大楼裙楼） 邮编：361005 电话：0592-2577888 8607568

公安部计算机信息系统安全产品质量监督检验报告



计算机信息系统安全专用产品

销售许可证

证书编号：XKC30626

有 效 期：自2004 年 12月03 日

至2006 年 12月03 日

中华人民共和国公安部监制

南通微盾网络科技有限公司

根据公安部《计算机信息系统安全专用产品检测和销售许可证管理办法》及有关规定，经审查，准许你单位生产的（代理）

[illegible]安全专用产品进入市场销售，特发此证。

2004 年 12 月 03 日

公安部计算机信息系统安全专用产品检测和销售许可证

目录

一、功能简介

KFW 傲盾防火墙网站防护版是一款针对各种网站、信息平台、Internet 服务等，集成多种功能模块的安全平台。

本软件是具有完全知识版权的防火墙，使用了目前最先进的第三代防火墙技术《DataStream Fingerprint Inspection》数据流指纹检测技术，与企业级防火墙 Check Point 和 Cisco 相同，能够检测网络协议中所有层的状态，有效阻止 DoS、DDoS 等各种攻击，保护您的服务器免受来自 Internet 上的黑客和入侵者的攻击、破坏。通过最先进的企业级防火墙的技术，提供各种企业级功能，功能强大、齐全，价格低廉，是目前世界上性能价格比最高的网络防火墙产品。

功能列表

1. 数据包规则过滤
2. 数据流指纹检测过滤
3. 数据包内容定制过滤
4. 网关路由支持
5. NAT 功能(支持 FTP PASV 和 port,支持 irc 的 ddc 等动态端口模式，安装防火墙后不用设置 PASV 之类的端口)
6. 端口映射功能
7. 流量控制
8. 采用最先进的数据流指纹技术，提供强大的 DOS(拒绝服务)攻击防护，彻底防护各种已知和未知的 DOS 攻击。
9. 流量分析监测
10. 实时访问连接监控
11. 支持 dmz 区的建立
12. 账号，权限管理
13. 分布式管理

二、技术优势和特点

KFW 傲盾防火墙系统是一套全面、创新、高安全性、高性能的网络安全系统。它根据系统管理者设定的安全规则（Security Rules）把守企业网络，提供强大的访问控制、状态检测、网络地址转换（Network Address Translation）、信息过滤、流量控制等功能。提供完善的安全性设置，通过高性能的网络核心进行访问控制。

与国内外的防火墙产品所比较，傲盾防火墙有以下突出的技术优势和特点：

1.特有的 DdoS、Dos 攻击防御

DoS 攻击（Denial of Service 拒绝服务攻击）或着是 DDoS 攻击（Distribute Denial of

Service 分布式拒绝服务攻击）是近年来流行的一种危害极大的网络攻击方式。当 DoS 攻击发动的时候，有时甚至可以完全使网络服务器所提供的服务失效。

DoS 攻击的原理，简而言之，就是针对 TCP/IP 协议的薄弱环节，利用 IP 欺骗技术，对要攻击的节点疯狂地发出数据包；使得被攻击节点忙于处理这些虚假来源的数据包，从而使合法的使用者无法正常的连接到被攻击的节点。而且由于 DoS 攻击的发动者采用 IP 地址欺骗，使得很难对攻击来源进行定位。由于 DoS 攻击的这些特点，使它成为最有效，也最难防护的攻击手段之一。

针对 DoS 攻击的这些特点，KFW 傲盾防火墙专门设计了特有的 DoS 防御网关，可以有效的抵御各种 DoS、DDoS 攻击。

这里简要叙述 KFW 傲盾防火墙 DoS 防御网关的原理： KFW 傲盾防火墙所采用的特有专利技术，使得防火墙本身是不受 DoS 攻击的，这也是 KFW 傲盾防火墙能够有效防护需要保护的站点免受 DoS 攻击的先决条件。在这个条件的基础上，KFW 傲盾防火墙采用经过优化的 TCP 连接监控方式来保护防火墙内的脆弱机器。这种算法的特点是在处理 TCP 连接请求的时候，在确定连接请求是否合法以前，用户端与服务端是隔断的。这就令到 DoS 攻击者在发动攻击的时候并不能直接连接到防火墙内部的机器，所以攻击者所发出的所有 DoS 攻击包只能到达防火墙，从而保护了防火墙内部的机器不受到 DoS 攻击。 而且，KFW 傲盾防火墙通过高效的离散算法提供了超过 60 万以上的同时连接数的容量，为数据传输的高效和可靠提供了强有力地保障。

2.世界领先《DataStream Fingerprint Inspection》数据流指纹检测技术

传统的包过滤防火墙只是通过检测 IP 包头的相关信息来决定数据流的通过还是拒绝，KFW 傲盾防火墙独创的《DataStream Fingerprint Inspection》数据流指纹检测技术采用的是一种基于连接的状态检测机制，将属于同一连接的所有包作为一个整体的数据流看待，构成连接状态表，通过规则表与状态表的共同配合，对表中的各个连接状态因素加以识别。这里动态连接状态表中的记录可以是以前的通信信息，也可以是其他相关应用程序的信息，因此，与传统包过滤防火墙的静态过滤规则表相比，它具有更好的灵活性和安全性。

KFW 傲盾防火墙的核心数据流指纹检测技术，可以确保每个进入的数据包都是合法有效的，一旦确认连接的合法性防火墙就会信任这个连接，不在对后续包进行复杂的处理，从而大大提高了效率。

3.特有的 TCP 标志位检测功能：

在大多数的防火墙里，都缺少对连接是从哪方主动发起进行判断的选项，这将导致一个潜在的安全隐患是攻击者可能可以从一个外部主机的某个常用服务端口连入内部主机的高端口。例如，如果允许内部主机访问外部主机的 telnet 服务，这个方向连接的所有包应该是必须包含 ACK 位的，也就是说，不是主动发起的连接。但通常的防火墙的包过滤功能里并没有检查 ACK 位的设置，因此，攻击者就可以从外部主机的源 23 端口发起连接到内部主机的高端口(>1023)。KFW 傲盾防火墙系统通过在安全规则上的设置对数据包的 SYN/ACK 等标志位进行合法性检测和判断，防止不法攻击者利用常用服务的低端口与内部主机的高端口的连接，从而攻击内部主机。

国内包括国外的许多防火墙系统都无此防护功能。

4.强大的 NAT 地址转换功能

当 Internet 技术变成热门技术，获取有效 IP 地址的热潮即将耗尽有限的网络地址空间，因此有关地址扩展的建议如 IPng 已被确定为一个新 IP 编址标准--IPv6。所有的标准需要一定时间被广为接收和实现，在这之前，我们必须有一个代替的方法。另一方面，在网络安全问题上，能够隐蔽的私有地址会提供更为理想的安全性。由此，NAT 技术应运而生。 在 KFW 傲盾防火墙里，我们可以方便地应用 NAT 的方式使具备私有地址编址方式的机器能够安全的连上外部网络，并且应用 INTERNET 所提供的多姿多彩的生活；NAT 的重定向功能使得即便是私有地址空间的机器也能够在公有网络上提供 INTERNET 服务，这对那些想在网上安个"家"，而又只能用私有地址的用户来说再合适不过了，通过 NAT 功能可以方便的建立起 dmz 区，把服务器和 Interenet 隔离开。使服务器免受黑客的攻击(个人版，企业版 NAT 和路由网关功能只限于本机 ip 地址。门户版 NAT 和路由网关功能能够对一个内网进行地址转换，由此达到保护一个内网的目的)。

5.独立开发的高效率系统核心

KFW 傲盾防火墙采用专门设计、自行开发的独立操作系统的网络核心。使得它有着最贴近系统底层的高效率。并且，由于完全最贴近底层，使得它可以告别一切不稳定的因素。

三、网络部署极其安装

安装本软件，实际上是对网络的安全部署，关系到整个网络的安全和部署成败所以请您仔细阅读研究下面的说明。

安装注意事项

1. 防火墙不是越多越好，多个防火墙或者网络软件会造成系统紊乱大大降低网络效率尤其是一些个人版防火墙，由于技术和稳定性的原因，往往会造成蓝屏死机，网络缓慢，以及莫名的问题所以请彻底关闭，最好是卸载其它防火墙和网络产品(包括 KFW 个人版),以及系统本身的安全策略！
2. 如果您在用 win2000 的 路由和远程访问，或者 Interent 共享，以及 winroute,sygate 等类似软件请再服务里彻底禁止该服务，或者卸载。
3. kfw 企业版防火墙现在支持 windows2000,windows xp,windows2003 系列。
4. 内存最少要 128m（如果您的网络比较大推荐 512M，越大越好）,硬盘空间应该剩余 50M。(如果空间用尽，纪录文件将无法保存)

安装部署

KFW 傲盾防火墙服务器版安全非常简便，只要运行安装程序，安装完毕后重新启动就会默认保护所有的端口。如果需要一些定制的规则，可以通过防火墙规则或者接收包流量控制来设置。

安装的具体步骤：

1.在安装《KFW 傲盾防火墙服务器版》以前，请检查该机器以前是否安装了本产品，如有安装，请卸载。

2.打开产品安装目录，执行安装程序。

3.请用户认真阅读软件授权许可协议，如无异议，请选中“我接受以上许可协议中的条款”；按“下一步”以继续执行接下来的安装步骤。其间如出现“是否覆盖”的提示时，建议选择“全部覆盖”。

4.文件安装完成后，将需要重新启动计算机

5.重起完毕后，察看右下角托盘是否有 K 字样的图标，检查 KFW 是否在运行状态，如果没有运行请检查是否正确安装，请参见安装注意事项。

6.在[开始][程序]菜单中打开“KFW 傲盾防火墙服务器版”，选择 KFW 服务器版管理器,接着您将会进入本系统的“管理器”画面。

7.首先管理器菜单里的连接->连接到防火墙 如果是在 KFW 机器上运行的，连接地址请输入 127.0.0.1 如果不是请输入 KFW 机器的 Ip 地址，默认管理账号：root,默认密码：12345

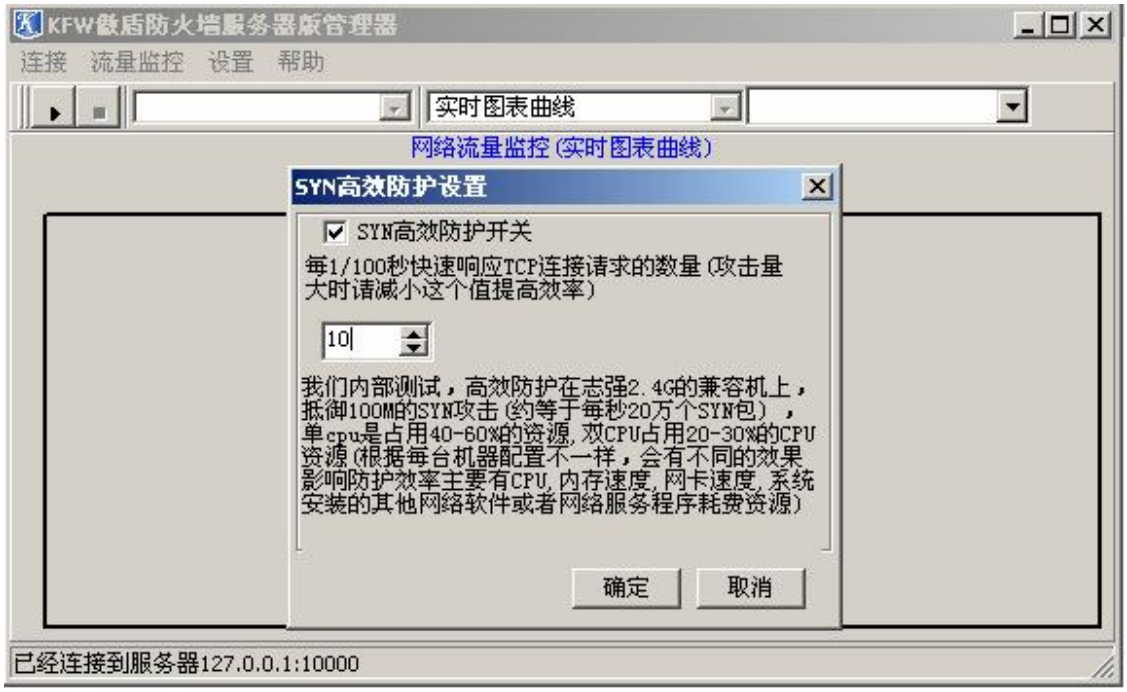
四、软件的配置和功能使用

安装文件包括：
主要执行文件
KFW 服务器版网络监控
网络连接的信息以及监控,
运行托盘
----监控 KFW 服务的运行情况
KFW 服务器版管理器
----管理配置防火墙
KFW 傲盾防火墙服务器版手册

KFW 服务器版管理器 主要功能的设置步奏

1. SYN 高效防护设置

选择菜单 设置->DOS 攻击防护->高效 syn 防护设置



syn 高效防护开关设置后，本机所有的端口都会被防护，不需要单独设置，防火墙安装后默认是打开的。

响应包数模式是 **10,**如果服务器的同时在线人数很大，可以加大这个设置。

2. SYN 拒绝服务攻击防护设置

选择菜单 设置->DOS 攻击防护->SYN 拒绝服务攻击防护

SYN 拒绝服务攻击防护，是本软件的一个重要功能，通过这里设置可以完全防护已知和未知

的 SYN DOS 拒绝服务攻击。

编号栏的选择框，可以选择让哪些规则有效。

设置说明:

1.[INTERENT IP 地址] 本机的 Interent Ip 地址，也就是遭受 syn dos 攻击的 Ip 地址,这个 Ip 必须已经注册购买。

2.[标准防护] 当受到大量单一的 SYN 包攻击时选择这个，这种攻击只是简单的发送大量 TCP 的 syn 数据包造成使用 TCP 协议的服务程序不能接收合法的访问请求。

3.[WEB SERVER 类保护] 最近流行的 "DDoS 攻击者" 是一种新的 syn 类攻击，这个攻击工具不但发送大量的 syn 数据包，而且还能完成 TCP 协议的三次握手形成正常的 TCP 连接，危害很大，大部分硬件防火墙都无法防护，选择这个设置可以防护，注意这个设置只适用于 WEB SERVER 类的服务。(详细资料请访问我们的网站)

4.[新建连接的合法检查] 针对 "DDoS 攻击者" 这类攻击 选择此项，如果你已经选择了[WEB SERVER 类保护]就不用选择本设置，本设置专门针对不是 WEB SERVER 类的服务，比如 FTP SERVER,选择[WEB SERVER 类保护]则不起作用，这是可以通过本设置来防护 "DDoS 攻击者" 这类的攻击。

5.[新建连接的合法检查-子项] 比如默认设置 [连接建立后 2 秒内] [客户端必须发送 3 个数据包] 表示 TCP 连接完成 3 次握手建立连接后 2 秒钟内系统将检查请求这个连接的客户端是否发送了 3 个数据包，如果客户端没有发送 3 个数据包，这个连接将被断开。通过这两个设置，可以防护未知的 syn 攻击。

3. 接收包流量限制

选择菜单 设置->DOS 攻击防护->接收包流量限制

接收包流量限制可以限制大量 **dos** 数据包攻击，通过这个设置可以防止所有 **ICMP,IGMP,UDP,TCP** 等之类的 **dos** 攻击

设置说明**:**

1.[协议类型] 可以选择各种协议，或者自定义协议。

2.[源地址] 要防止攻击包的源地址**,**默认是任何地址。

3.[目的地址] 要防止攻击包的目的地址**,** 默认是任何地址。

4.[协议属性] 选择不同的[协议类型] 这里为对应的协议属性,比如要限制 **TCP SYN** 的攻击包数，可以选择[协议类型]为 **TCP,**[协议属性] 把[**SYN**] [设置]分别选择上。

5.[**TCP** 协议属性] **TCP** 属性分别为 **SYN, ACK, FIN, RST, URG, PSH,**每个属性下面有一个[设置]选择 **,**选择需要检查的属性，选择这个属性的[设置] 表明这个属性必须设置为 **1,**例如，要检查 **syn** 和 **ack** 属性的 **tcp** 包，并且 **syn** 为 **1,ack** 为 **0** 则选择 **syn** 和 **ack,**然后在 **syn** 的[设置]属性打上对号，把 **ack**[设置]属性的对号去掉，再例如，需要检查 **syn rst fin** 标志，**syn =0,rst = 1,fin=0,**则分别选择 **syn rst fin,**然后把 **syn** 和 **fin** 的[设置]属性去掉对号，**rst** 的[设置]属性打上对号。

6.[时间单位] 分别是秒，分钟，小时，天，默认是秒，例如设置[时间单位]秒，[允许通过包] 为 **10,**[允许最大突发数为]**5** 表示，每秒允许通过 **10** 个包，最大突发包数是 **5,**，如果每秒超过 **10** 个包，超过的数据包将被拦截。

7.[拦截] 当上面的条件符合时拦截 这个数据包。

8.[智能拦截] 用在 **tcp** 协议，结合[**syn** 拒绝服务攻击防护]使用，例如当受到大量的 **syn** 包攻击，每秒超过 **5** 万个，如果你设置[拦截]的话 正常的请求也会被拦截，服务还是不能正常运转，这时可以设置 [智能拦截]**,**智能拦截并不会把超过流量限制的数据包给丢掉，而是通过智能判断来对正常的请求进行响应。

4. 网络设备设置

选择菜单 设置->网络设置->网络设备设置

请点击开关栏选择你需要保护的网络设备。(如果选择的设备的 IP 没有注册购买请不要选，否则会造成这个设备无法工作!)

点击属性可以设置通过 NAT 协议进行 DMZ 保护，DMZ 保护后在本机可以通过 NAT 协议访问 INTERNET，外面则无法直接访问本机的任何端口，这样这个网络设备所拥有的 IP 就会和 INTERNET 单向隔离开从而杜绝黑客攻击。设置 DMZ 保护后如果本机需要打开服务端口比如 IIS Web Server 的 80 端口，请在下一页的端口映射里进行设置，如果不设置将造成无法访问任何端口!

属性设置:

1.[对本级通过 NAT 进行 DMZ 保护] 打开 NAT DMZ 保护功能。

2.[自动分配端口] 选择 DMZ 保护后，本机访问 Interent 时通过 NAT 协议所用的端口，默认是 50000-55000，如果选择本选项则系统会自动根据原来的端口进行自动分配对外的端口。

3.[NAT 地址设置] 填上本计算机 Interent 的 IP 地址。

（关于 NAT 和 DMZ 区的详细介绍请访问我们的网站）

5. 端口映射

选择菜单 设置->网络设置->端口映射

如果你在上一页选择了 **NAT DMZ** 保护，需要在这里设置你需要打开的服务端口，比如 **IIS** 的 **WEB SERVER** 等服务端口，否则将无法访问本机的服务

设置说明**:**

1.[协议类型] 可以选择 **UDP** 或者 **TCP** 协议，根据服务使用的协议类型选择

2.[本机 **INTERNET** 地址] **INTERNET** 访问本机的 **IP** 地址

3.[映射到服务器地址] 服务的真实 **IP**，如果本机只有一个 **IP** 则[本机 **INTERNET** 地址]设置一样。

6. 防火墙规则设置

选择菜单 设置->防火墙设置->防火墙规则设置

可以通过防火墙规则，来确定实现对网络的安全设置，防火墙分为两个视图，[本机接收数据]设置本机所有接收的数据，[本机发送数据]设置本机所有发送的数据,点击这两个按钮可以切换视图

设置说明:

1.[协议类型] 可以选择各种协议，也可以自己定义协议

2.[发送端地址] 是数据包的源 IP 地址

3.[接收端地址] 是数据包的目的 IP 地址

4.[协议属性] 选择不同的[协议类型] 这里为对应的协议属性。

5.[TCP 协议属性] TCP 属性分别为 SYN, ACK, FIN, RST, URG, PSH,每个属性下面有一个[设置]选择 ,选择需要检查的属性，选择这个属性的[设置] 表明这个属性必须设置为 1,例如，要检查 syn 和 ack 属性的 tcp 包,并且 syn 为 1,ack 为 0 则选择 syn 和 ack,然后在 syn 的[设置]属性打上对号，把 ack[设置]属性的对号去掉，再例如，需要检查 syn rst fin 标志，syn =0,rst = 1,fin=0,则分别选择 syn rst fin,然后把 syn 和 fin 的[设置]属性去掉对号，rst 的[设置]属性打上对号。

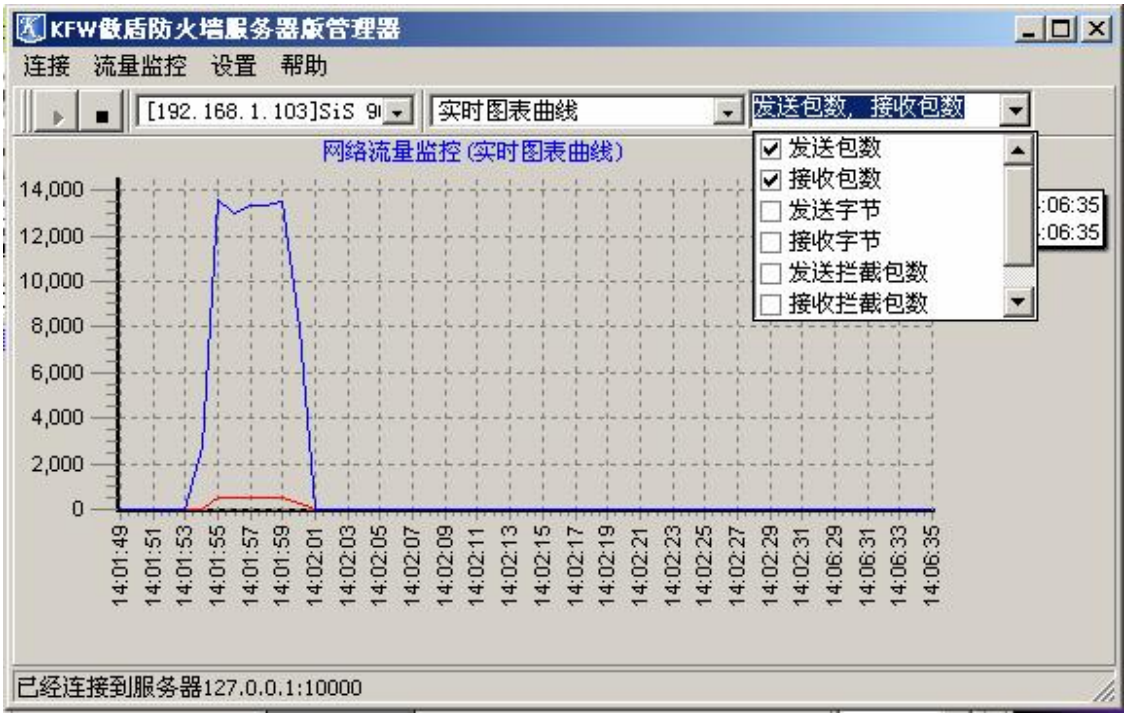
6.[高级设置] ->[ip 连接限制] 可以设置一个 ip 或者很多相邻 ip,能够和本机器建立多少个连接，例如要限制 202.102.224.0 - 202.102.224.255 这些 ip 地址，能够和本机建立 100 个 TCP 连接，首先在防火墙规则的[本机接收数据]->[发送端地址] 填写上 202.102.224.0 - 202.102.224.255 ip 段，在协议属性设置里选择[SYN]和[设置]，选择[条件符合时拦截] ,在[高级设置] ->[ip 连接限制] 里选择[进行 ip 限制],设置[允许连接数]为 100，[匹配掩码]设置 24,这样就表示 202.102.224.0 - 202.102.224.255 IP 段只能共享和本机建立 100 个 IP 连接(注意:如果 [匹配掩码] 设置 32,则表示 202.102.224.0 - 202.102.224.255 IP 段里的每个 ip 都能和本机建立 100 个连接)

7. 流量监控和统计

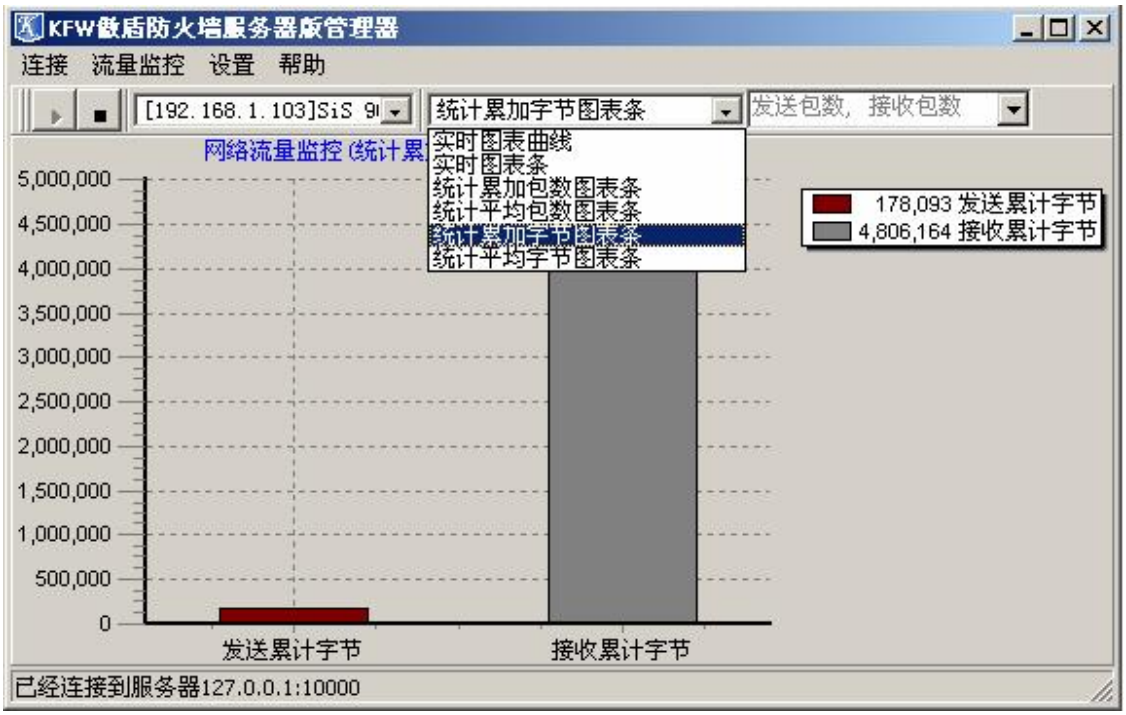
在 KFW 傲盾防火墙服务器版管理器里主界面里点击开始按钮。

选择工作的网卡，然后选择监控统计模式，选择监控统计的类别，就可以得到当前网络的实时监控统计信息了。

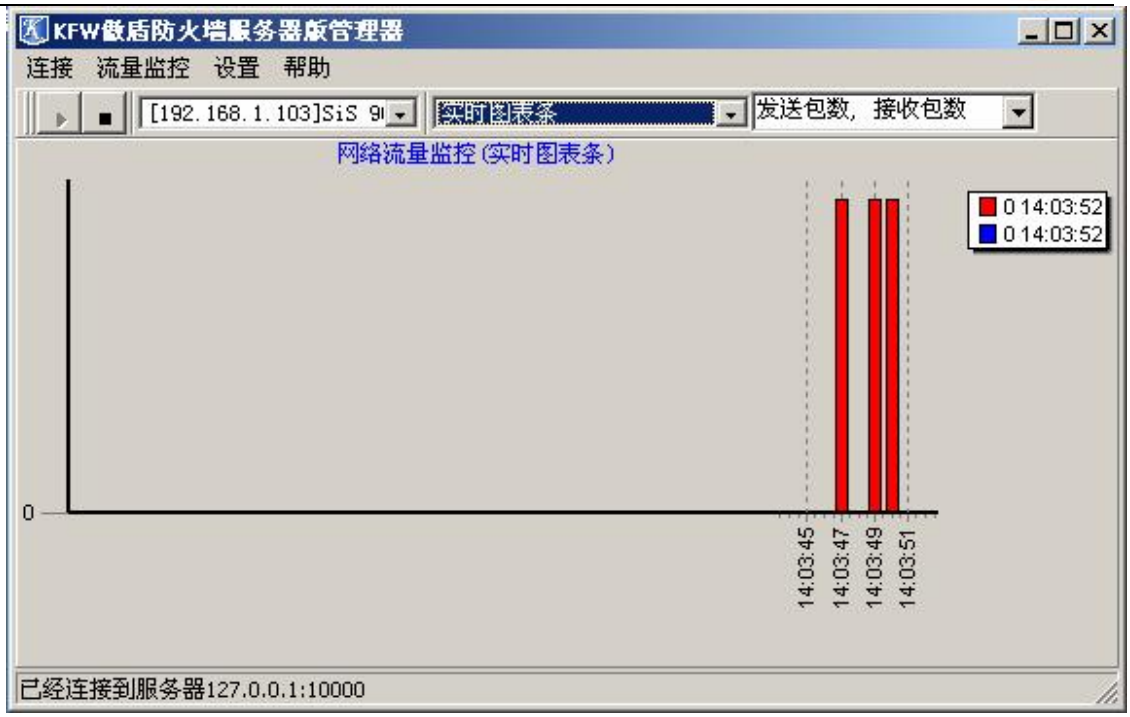
实时图表曲线->发送包数，接收包数



统计类教字节图标条



实时图表条->发送包数，接收包数



统计类教包数图标条

统计平均字节图标条

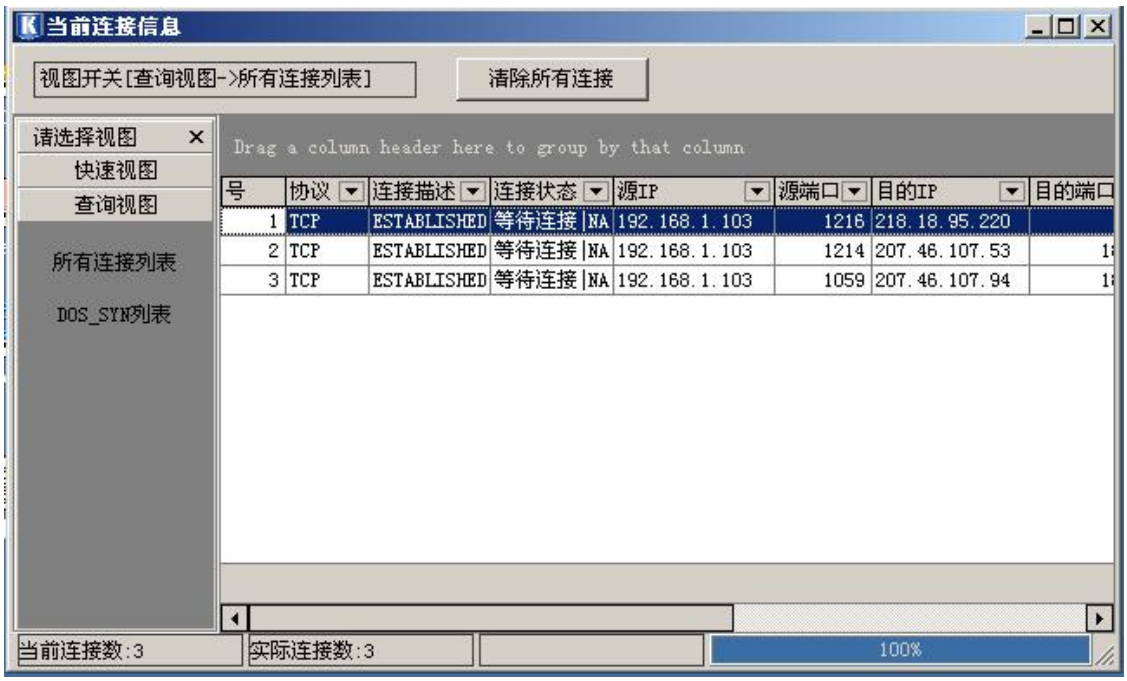
8. KFW 服务器版网络监控

通过网络监控可以方便的检测查询当前的连接详细信息，以及 **syn** 攻击的情况。

网络监控分为两大块，快速视图和查询视图，快速视图的信息比较简单，当有大量连接的时候可以很快列表出来，查询视图的信息很详尽，但是当连接数多的时候列表速度比较慢。

每个视图里都有所有连接列表和 **DOS_SYN** 列表 所有连接列表里显示当前正常连接到服务器的连接，**DOS_SYN** 列表里显示出当前 **SYN** 访问请求的所有列表，当有 **syn** 攻击的时候列表里会有几万几十万的数据。如果列表里有几百个连接应该是正常的。

查询视图所有连接列表



快速视图所有连接列表

快速视图 **DOS_SYN** 列表

查询视图 **DOS_SYN** 列表

9. 常用的一些设置步奏

1. dmz 区建立

a) 打开菜单**[**设置**->NAT** 网关设置**->**端口映射 添加。

b)选择适当的协议网关的 **IP** 是要访问这个服务的 **Interent IP,**端口是要访问这个服务的 对外端口比如 **80** 端口。

c)映射到服务器 **IP**，如果服务和防火墙装在一台机器上，这个 **Ip** 和网关的 **IP** 一样，端口是这个服务的实际端口。

2. 开放一个对外的服务比如 **web Server ftp server**

a)打开菜单**[**设置**->NAT** 网关设置**->**端口映射 添加。

b)选择适当的协议网关的 **IP** 是要访问这个服务的 **Interent IP,**端口是要访问这个服务的对外端口比如 **80** 端口。

c)映射到服务器 **IP**，如果服务和防火墙装在一台机器上，这个 **Ip** 和网关的 **IP** 一样，端口是这个服务的实际端口。

d)如果服务是单独装在局域网的另一台机器上，那么这个 **IP** 就是安装服务这台机器的局域网 **IP**。

e)把安装服务的这台机器的网关设置成防火墙的局域网 **IP** 地址。

五、常见问题

问：KFW 傲盾防火墙网站防护版支持哪些平台？
答：目前支持 windows 2000 系列,windows xp 系列,windows 2003 系列

问：安装防火墙后网络不通，无法远程连接服务器。
答：一般有几种情况：
(1)在防火墙里设置了一些规则把远程连接的端口给封掉了。
(2)攻击流量太大，把带宽堵塞了。
(3)服务器里安装了一些网络软件，或者是安全策略和防火墙有冲突。

问：安装时设置启动参数设置，我需要怎么选择？
答：一般如果远程安装第一次在服务器上安装，选择系统启动后暂停防火墙，防止一些规则设置错误，导致远程连接不上。等防火墙安装完毕，重新启动，设置完毕后如果没有什么问题，再设置随系统正常启动防火墙。

问：防火墙远程管理端口在哪里设置？
答：在桌面右下角的 kfw 图标托盘上点右键选择启动参数设置，可以设置管理端口，默认时 10000。

问：防火墙的连接数是怎么计算的，为什么有时候服务器的 ftp 在线人数有 100 人，在 KFW 服务器版网络监控里所有连接列表有 200 多个连接？
答：当前所有正常的连接，在 KFW 服务器版网络监控里所有连接列表里可以查看,这个连接不包括 syn 攻击所产生的伪造连接，是正常的 TCP 协议连接，因为一个客户端连接 ftp server 或者 web server 等服务器时，会产生好几个 TCP 连接，实现多线程下载。ftp 每次会建立两个连接一个是命令通道一个是数据传输通道，所以产生的 TCP 连接会比实际在线人数多。

问：安装上防火墙当有大流量攻击时 网络速度还是很慢，ping 老丢包？
答：服务器版防火墙，我们内部测试，在 p42.4 的机器上至少可以防护 260M 带宽流量的攻击，所以在百兆的网络里应该完全防护，登陆到服务器上看看 cpu 占用率有多少，如果 cpu 占用率没有 到 90%,造成这种现象应该是网络带宽不足造成的，可以从服务器上到别的网站下载一个文件，看看能达到多大的速度，以此确定是带宽问题还是防火墙问题。

问：在使用 kfw 服务器版网络监控提示防火墙连接数已经满了我该怎么办？
答：提示防火墙满了以后，防火墙可以继续使用，只是超过的连接不能建立，只能等不用的连接释放掉才能连接上，可以通过升级防火墙来增加连接。

问：100m 的独享带宽能够防护多少个 syn 攻击包？
答：我们在 100M 局域网上测试，100M 的带宽最多转发每秒 14.5 万个 syn 攻击包，到每秒 13 万个是就会出现丢包现象，这是 100M 带宽所限制的。

问：KFW 傲盾防火墙安装在 windows2003 系统上提示<打开设备驱动错误>应该怎么解决?
答：在本机搜索 KFW 防火墙驱动文件 kfwcorea.sys 将其复制到 system32/drivers 文件夹下面

重启机器。

六、名词解释

1> **Dos 攻击：Denial of Service** 的缩写，意为拒绝服务。**DoS** 攻击是网络上一种简单但很有效的破坏性攻击手段，是一种利用合理的服务请求占用过多的服务资源，从而使合法用户无法得到服务响应的网络攻击行为。其中 **SYN Flood** 攻击是最为常见的 **Dos** 攻击方式。

2> **SYN Flood 攻击：DoS** 攻击的典型种类—**SYN Flood**，就是攻击者利用伪造的 **IP** 地址，连续向被攻击的服务器发送大量的 **SYN** 包。被攻击的服务器收到这些 **SYN** 包后，连续向那些虚假的客户机（伪造的 **IP** 地址指向的客户机）发送 **ACK** 确认包。很显然，服务器是不会收到 **ACK** 确认包的，于是服务器就只能等待了。当服务器因超时而丢弃这个包后，攻击者虚假的 **SYN** 包又源源不断地补充过来。在这个过程中，由于服务器不停顿地处理攻击者的 **SYN** 包，从而正常用户发送的 **SYN** 包会被丢弃，得不到处理，从而造成了服务器的拒绝服务。

3> **Ddos 攻击：**英文全称为 **Distributed Denial of Service**，它是一种基于 **DoS** 的特殊形式的拒绝服务攻击，是一种分布、协作的大规模攻击方式，主要瞄准比较大的站点，象商业公司，搜索引擎和政府部门的站点。**DoS** 攻击只要一台单机和一个 **modem** 就可实现，与之不同的是 **DDoS** 攻击是利用一批受控制的机器向一台机器发起攻击，这样来势迅猛的攻击令人难以防备，因此具有较大的破坏性。

4> **NAT 功能：NAT**—**Network Address Translator** 的简称，**(**又叫网络地址转换**)**，实现内网 **IP** 地址与公网 **IP** 地址之间的相互转换，其作用是让服务器把指定端口的请求转发到指定的 **IP** 上，让其它的机器来响应这些请求，而内网向外网发送的时候不再是像其它网关服务那样随机分配端口，而是用上面指定的端口。也就是说，**NAT** 将多个内部地址映射为少数几个甚至一个公网地址，使整个局域网中的机器都能够连上 **Internet**，同时它还有隐藏内部网络结构的作用，具有一定的安全性。。

5> **IRC：IRC** 聊天是网上聊天的一种方式，它是 **INTERNET RELAY CHAT** 的缩写，意思是英特网继传聊天，通过特殊的协议**(IRC** 协议**)**，大家连到一台或者多台 **IRC** 服务器上进行聊天。它的特点是速度快**(**几秒钟内你就可以看到对方的**"**讲话**")**，功能多，所以通过 **IRC** 聊天是全世界网友的最佳选择。

6> **端口映射：**端口映射就是将主机的 **IP** 地址的一个端口映射到局域网中一台机器，当用户访问这个 **IP** 的这个端口时，服务器自动将请求映射到对应局域网分机。

7> **DMZ 区：**为了把局域网上的一台计算机设置成不设防区域（**Demilitarized Zone**，**DMZ**，也称非防护区，非军事区）。在一个路由器上有两个网络接口，你可以在私有网络里面设定一个隔离区接口增强安全。**DMZ** 接口是外部网络（公共互联网）和你的内部安全网络之间的一个缓冲的网络接口，**DMZ** 能提供外部网络和安全网络必要的服务。向公共互联网提供 **HTTP/FTP**（**Web**）服务，**HTTP/FTP** 代理服务，**SMTP** 和新闻（代理）服务。邮件服务器和新

闻服务器放在里面的安全网络，你可以禁止外部网络访问内部的安全网络，但可以在 DMZ 这隔离区中提供其它的服务。

8> IPv6：IPv6 是下一版本的互联网协议，也可以说是下一代互联网的协议，它的提出最初是因为随着互联网的迅速发展，IPv4 定义的有限地址空间将被耗尽，地址空间的不足必将妨碍互联网的进一步发展。为了扩大地址空间，拟通过 IPv6 重新定义地址空间。IPv4 采用 32 位地址长度，只有大约 43 亿个地址，估计在 2005-2010 年间将被分配完毕，而 IPv6 采用 128 位地址长度，几乎可以不受限制地提供地址。按保守方法估算 IPv6 实际可分配的地址，整个地球的每平方米面积上仍可分配 1000 多个地址。在 IPv6 的设计过程中除了一劳永逸地解决了地址短缺问题以外，还考虑了在 IPv4 中解决不好的其它问题，主要有端到端 IP 连接、服务质量（QoS）、安全性、多播、移动性、即插即用等。