NEUSOFT 东软

软 件 创 造 客 户 价 值

NetEye防 火 墙

技　　术　　白　　皮　　书

沈 阳 东 软 软 件 股 份 有 限 公 司

一、概述

目前市场上存在着各种各样的网络安全工具，而技术最成熟、最早产品化的就是防火墙，由于防火墙技术的针对性很强，它已成为实现 Internet 网络安全的最重要的保障之一。

NetEye 防火墙 3.0 是东软集团 NetEye 防火墙系列中的最新版本，该系统在状态包过滤的基础上，采用了专门设计的 TCP 协议栈实现对应用协议信息流的过滤，能够实现在透明方式下的对应用层协议的控制能力。系统的整体结构严格按照国家应用级防火墙的最新标准设计，具备完善的身份鉴别、访问控制和审计能力。经国家权威部门检测，NetEye 防火墙 3.0 符合 GB/T 18019-1999（包过滤防火墙安全技术要求）和 GB/T 18020-1999（应用级防火墙安全技术要求）两个国家标准的技术要求。

系统提供了丰富的 GUI 方式的管理和监控工具，能够方便的对系统进行安全策略配置、用户管理、在线监控、审计查询、流量管理等操作。

系统实现了对攻击的识别模块，能够有效的防范多种 DoS 的攻击手段，并能够对攻击事件进行报警。同时为了保证用户网络的可靠运行，系统还实现了双机热备份的功能。

该系统的主要模块工作在操作系统的内核模式下，并对协议的处理进行了优化，其千兆版本能够利用多处理器的能力能够处理超过 20 万的并发连接，支持高速网络的应用。

二、体系结构 —— 基于状态包过滤的流过滤技术

防火墙最重要的作用就是在网络边界实现保护作用，保护能力与防火墙体系结构和运行机制有直接的关系，历史上每一次体系结构上的演变都会带来防火墙功能的质的飞跃。防火墙的基本结构可以分为包过滤和应用代理两种。包过滤技术关注的是网络层和传输层的保护，而应用代理则更关心应用层的保护。

包过滤是历史最久远的防火墙技术，从实现上分，有可以分为简单包过滤和状态检测的包过滤两种。

简单包过滤是对单个包的检查，目前绝大多数路由器产品都提供这样的功能。由于这类技术不能跟踪 TCP 的状态，所以对 TCP 层的控制是有漏洞的，比如当你在这样的产品上配置了仅允许从内到外的 TCP 访问时，一些以 TCP 应答包的形式进行的攻击仍然可以从外部透过防火墙对内部的系统进行攻击。简单包过滤的产品由于其保护的不完善，1999 年开始已经很少在主流产品中出现了。

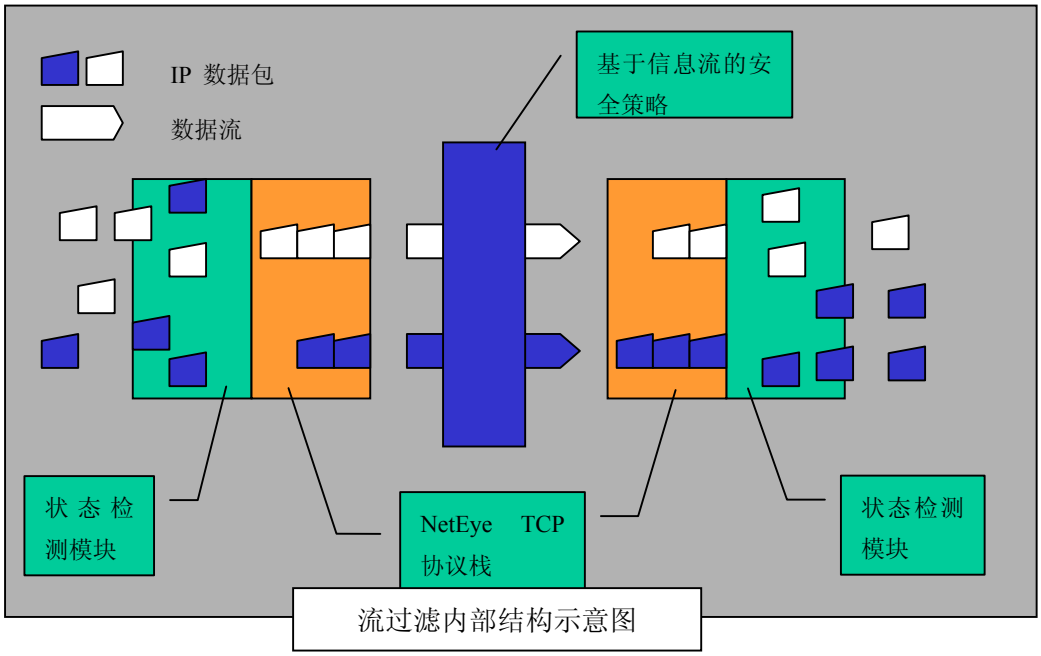
状态检测的包过滤利用状态表跟踪每一个网络会话的状态，对每一个包的检查不仅根据规则表，更考虑了数据包是否符合会话所处的状态。因而提供了更完整的对传输层的控制能力。同时由于一系列优化技术的采用，状态检测包过滤的性能也明显优于简单包过滤产品，尤其是在一些规则复杂的大型网络上。

应用代理防火墙可以说就是为防范应用层攻击而设计的。应用代理也算是一个历史比较长的技术，通常的表现形式是一组代理的集合。代理的原理是彻底隔断两端的直接通信，所有通信都必须经应用层的代理转发，访问者任何时候都不能与服务器建立直接的 TCP 连接，应用层的协议会话过程必须符合代理的安全策略的要求。针对各种应用协议的代理防火墙提供了丰富的应用层的控制能力。可以这样说，状态检测包过滤规范了网络层和传输层行为，而应用代理则是规范了特定的应用协议上的行为。

状态检测包过滤和应用代理这两种技术目前仍然是防火墙市场中普遍采用的主流技术，但两种技术正在形成一种融合的趋势。

我们在 NetEye 防火墙 3.0 中以状态检测包过滤为基础实现了一种称之为“流过滤”的结构，其基本的原理是以状态包过滤的形态实现应用层的保护能力。通过内嵌的专门实现的 TCP 协议栈，在状态检测包过滤的基础上实现了透明的应用信息过滤机制。在这种机制下，

从防火墙外部看，仍然是包过滤的形态，工作在链路层或 IP 层，在规则允许下，两端可以直接的访问，但是对于任何一个被规则允许的访问在防火墙内部都存在两个完全独立的 TCP 会话，数据是以“流”的方式从一个会话流向另一个会话，由于防火墙的应用层策略位于流的中间，因此可以在任何时候代替服务器或客户端参与应用层的会话，从而起到了与应用代理防火墙相同的控制能力。比如在 NetEye 防火墙对 SMTP 协议的处理中，系统可以在透明网桥的模式下实现完全的对邮件的存储转发，并实现丰富的对 SMTP 协议的各种攻击的防范功能。



流过滤内部结构示意图

流过滤的结构继承了包过滤防火墙的应用透明的特点，因而非常容易部署，而其安全保护能力则达到甚至超过了代理结构的产品。并且由于应用层安全策略与网络层安全策略是紧密衔接的，所以在任何一种部署方式下，都能够起到相同的保护作用。

流过滤的另一个优势在于性能，完全为过滤和转发目的而重新实现的 TCP 协议栈相对于以自身服务为目的的操作系统中的 TCP 协议栈来说，消耗资源更少而且更加高效，如果你需要一个能够支持几千个，甚至数万个并发访问，同时又有相当于代理的应用层防护能力的防火墙系统，流过滤结构几乎是唯一的选择。

流过滤与包过滤和代理技术对比

技术架构	综合安全性	网络层保护	应用层访问控制	应用透明性	性能
简单包过滤	低	有	无	有	较好
应用代理	高	很少	强，但缺少可扩展性	无	差
状态检测包过滤	中等	强	简单的内容过滤，具有局限性	有	好
流过滤	高	强	强，并易于扩展	有	好

三、功能介绍

3.1 核心安全保护能力：基于状态包过滤的流过滤架构

在状态包过滤基础上的流过滤机制是 NetEye3.0 的最突出的特点，这是通过一个内置的建立在状态包过滤基础上的专用 TCP 协议栈实现的。它可以提供透明方式下的完整的应用层协议的控制。基于这个机制，防火墙的应用协议处理模块可以根据需要重写应用会话的任何部分或全部。在 NetEye3.0 中支持的协议包括 HTTP，SMTP 和 FTP。

NetEye3.0 防火墙提供了两种工作模式：网桥模式和路由模式，在这两种模式下，防火墙都能提供同等的安全保护能力。

NetEye3.0 提供的 HTTP 过滤功能特性有：URL 关键字和小程序(Java Applet 和 ActiveX)两种类型的请求过滤、页面内容关键字过滤，并且提供了 HTTP 命令级控制，比较常用的命令有 GET(用于请求页面)、PUT(用于把本地页面上载到 HTTP 服务器)、POST(用来提交在页面中输入的信息)。

NetEye3.0 提供的 FTP 过滤功能特性有：命令级控制，其中比较常用的命令有 GET(用于下载文件)、PUT(用于把本地文件上载到 FTP 服务器)，以及基于命令级控制实现的对目录和文件的访问控制。

NetEye3.0 提供的 SMTP 过滤功能特性有：主题过滤、正文过滤、附带文件过滤、地址过滤、防止邮件炸弹、限制邮件大小、限制邮件 Relay 等功能。

对于上述所有的应用协议，都可以通过隐藏或替换服务器的标识信息达到防止服务器信息泄漏的目的，这个功能可以有效的阻止对服务器的应用级扫描。

3.2 动态规则

某些应用协议并不仅仅使用一个连接和一个端口，往往是通过一系列相关联的连接完成一个应用层的操作。比如 FTP 协议，用户命令是通过对 21 端口的连接传输，而数据则通过另外一个临时建立的连接（缺省的源端口是 20，在 PASSIVE 模式下则是临时分配的端口）。对于这样的应用，普通的防火墙很难设定一个安全的规则，往往不得不开放所有源端口为 20 的访问。

NetEye 防火墙 3.0 支持动态规则的机制，可以通过跟踪应用层会话的过程自动的允许合法的连接进入，而禁止其它的不符合会话状态的连接请求。对于 FTP 来说，只需要防火墙中设定一条对 21 端口的访问规则，就可以保证 FTP 传输的正常进行，包括 PASSIVE 方式的数据传输。这一功能不仅使规则更加简单，同时消除了必须开放 20 数据端口进入的危险。

3.3 身份认证

NetEye3.0 防火墙支持两种认证方式：本地认证和 Radius 认证。在本地认证方式中，防火墙根据系统本身的用户口令数据库检验用户口令，采用这种方式时，口令是普通的静态口令，保存在防火墙内的数据库中；在 Radius 认证方式中，防火墙通过工业标准的 Radius 协议访问第三方认证服务器，进行口令检验。采用 Radius 认证服务器的好处是可以与其他支持 Radius 协议的应用系统共享一个用户数据库，并且支持第三方的认证产品，如使用令牌（Token）的双因子认证产品。

NetEye3.0 的认证是在 TCP 连接建立过程中完成的，因此可以对任何基于 TCP 的应用协议提供完全一致的认证。如果用户要通过 NetEye3.0 防火墙访问外部网络，当用户所在主机发出的连接请求到达防火墙时，防火墙通过对用户所在主机发送专门的认证请求，激活客户端的认证程序。认证程序提示用户输入用户名和口令，并将用户名和口令以加密方式发送给防火墙。防火墙对用户名和口令进行验证，如果认证成功，则允许连接建立，否则拒绝或

禁止其通过。

认证用户可以被划分成不同的认证域，不同的认证域可以使用不同的认证方式和认证服务器。防火墙的管理员通过管理工具登录防火墙时，也需要进行身份认证，他们属于专门的认证域—管理域。

3.4 审计功能

一个安全防护体系中的审计系统的作用是记录安全系统发生的事件、状态的改变历史、通过该节点的符合安全策略的访问和不符合安全策略的企图，使管理员可以随时审核系统的安全效果、追踪危险事件、调整安全策略。所以安全审计是防火墙产品必须具备的 3 个基本要素之一（访问控制、身份认证、安全审计），也是国家应用级防火墙技术要求中重点强调的部分之一。

NetEye 防火墙 3.0 提供了完备的审计功能。

NetEye 防火墙 3.0 的审计日志包括两个部分：事件日志和访问日志。事件日志负责记录防火墙上曾经发生过的事件；访问日志负责记录经过防火墙的网络连接并记录相关信息，如：源 IP、目的 IP、目的端口、方向、流量等。

NetEye 防火墙 3.0 为审计日志提供了两种存储方式：本地和网络。本地方式将审计日志存储在防火墙上，网络方式将审计日志存储在专门的网络数据库上。

3.5 图形管理工具

从本质上讲，防火墙仅仅是实现网络安全的工具，是否能起到对网络的保护作用，以及起到多大的作用在很大程度上取决于管理防火墙的用户是否能够正确地使用防火墙管理工具。防火墙中的访问控制规则的编辑是管理防火墙的用户实施其安全策略的关键手段。早期防火墙的配置，特别是规则的制定和描述方法过于晦涩难懂，非专业人员很难配置。特别是当规则数目稍多时，规则的含义和结果，以及其正确性的判断将变得十分困难。从而经常使防火墙成为网络故障的发源地，更严重的是一些故障隐患长期存在，难以发觉，而对入侵者大开方便之门。

NetEye3.0 采用列表方式来制订访问控制规则，并且提供了规则制定的向导，引导用户一步一步制定出所需的访问控制规则。

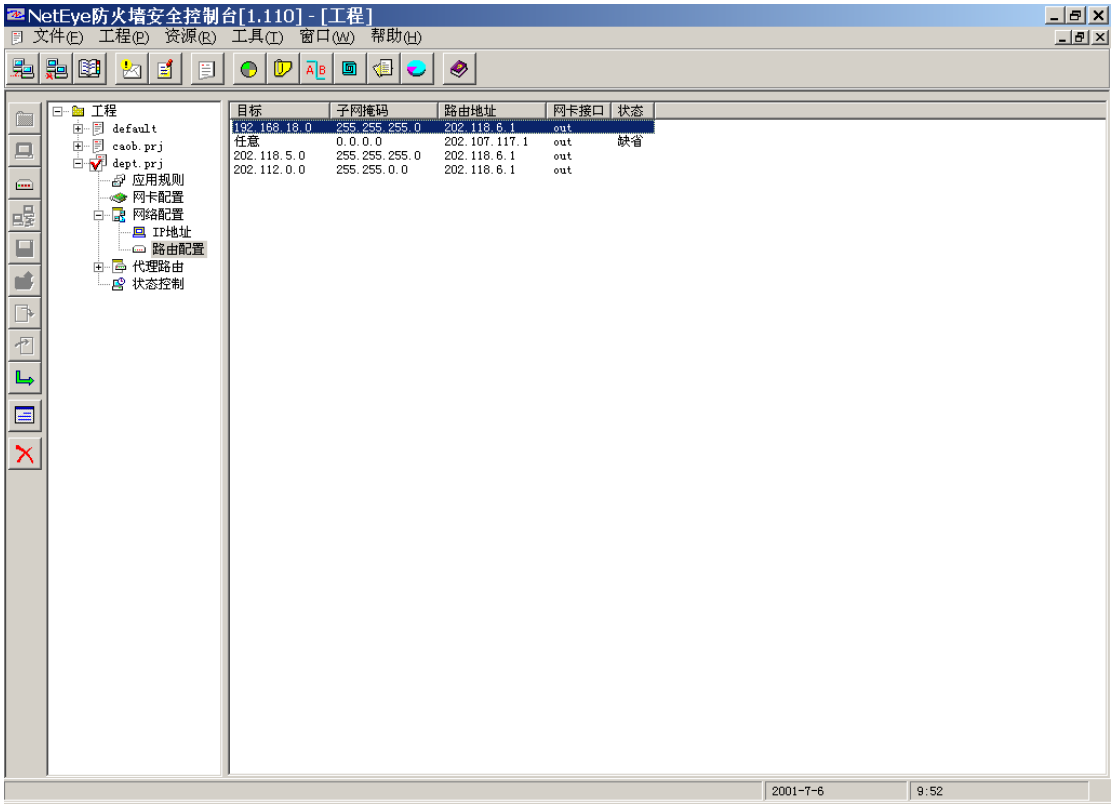
NetEye3.0 的图形管理界面(GUI)在使用上将更体贴用户，更具人性化，更为方便。

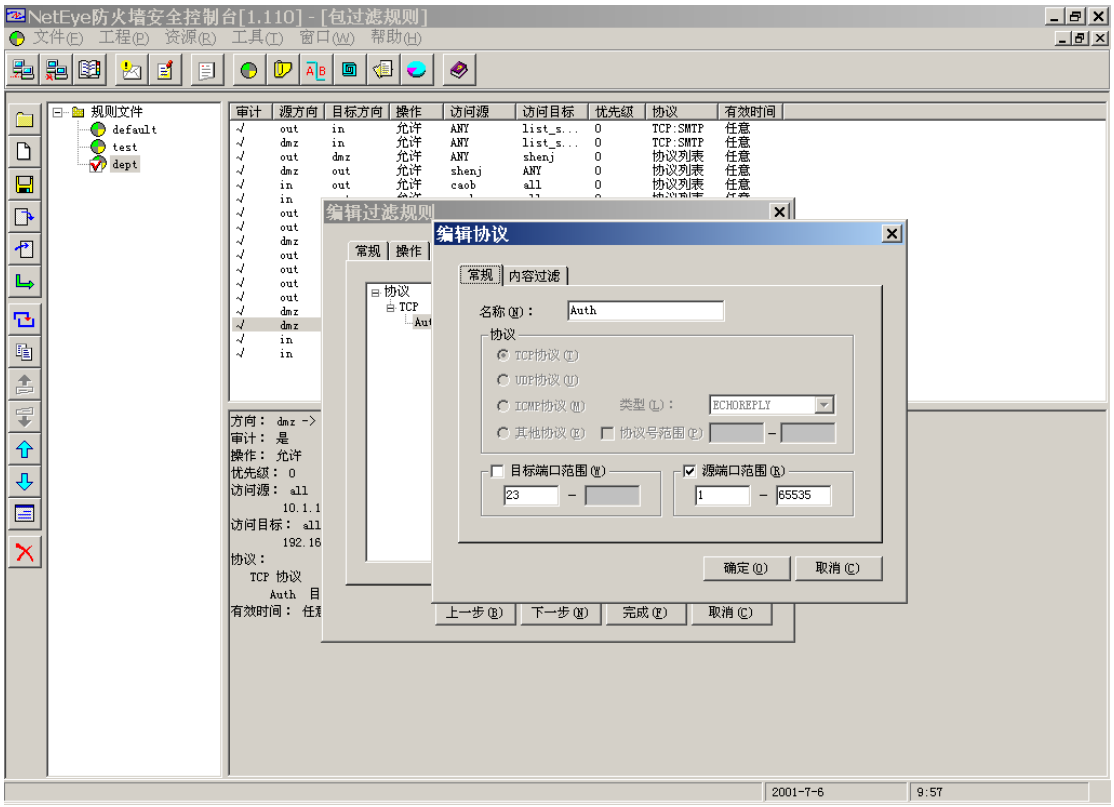
NetEye3.0 按照国家安全标准，把管理防火墙的用户分成三类：管理员、安全员、审计员。对应于这三类用户，NetEye3.0 为他们分别提供了三套管理工具。

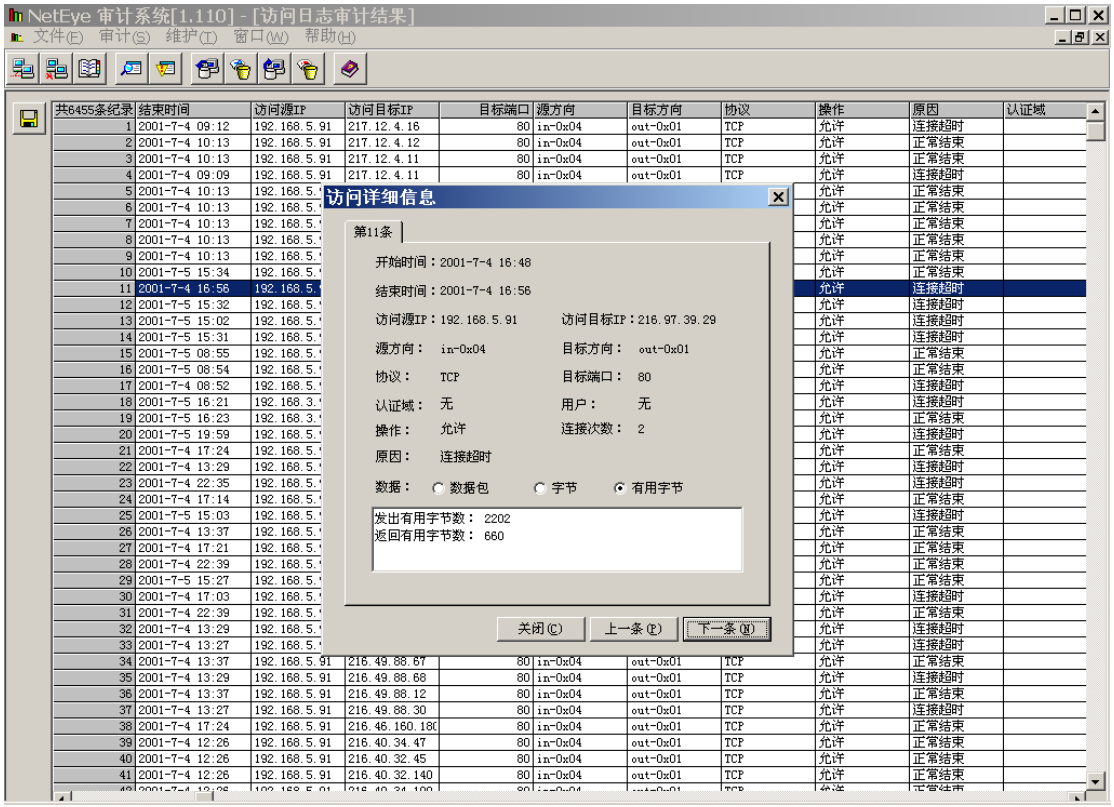
管理员使用“NetEye 用户管理器”来管理上述三类用户，他负责这三类用户的添加、修改和删除工作。

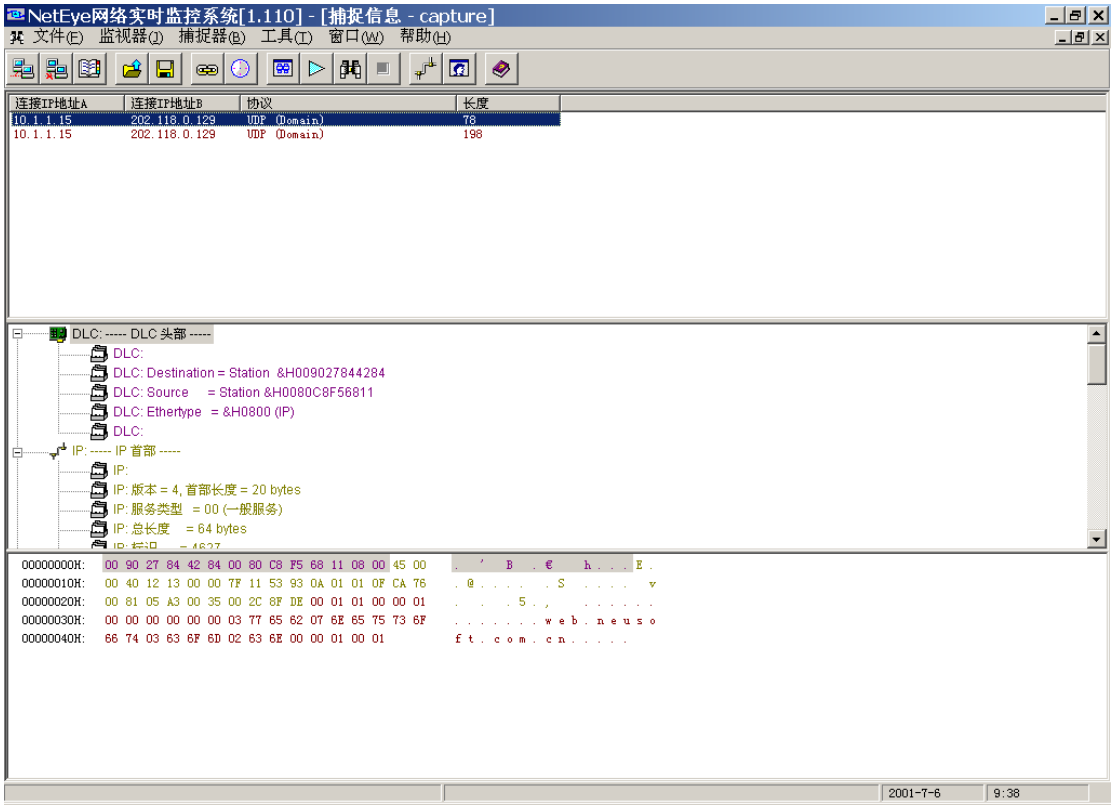
安全员使用“NetEye 安全控制台”来配置防火墙的各种信息，控制防火墙各种访问控制规则的制订和应用，以及普通用户及其所属认证域的添加、修改和删除等。并通过使用“NetEye 网络实时监控系统”实时的对网络运行状态进行监控。

审计员使用“NetEye 防火墙审计系统”对防火墙上的数据和防火墙上发生的事件进行统计分析，并对审计数据库进行维护。


NetEye防火墙安全控制台[1.110] - [工程]
文件(F) 工程(P) 资源(R) 工具(T) 窗口(W) 帮助(H)
工程
default
caob.prj
dept.prj
应用规则
网卡配置
网络配置
IP地址
路由配置
代理路由
状态控制
目标 子网掩码 路由地址 网卡接口 状态
192.168.18.0 255.255.255.0 202.118.6.1 out
任意 0.0.0.0 202.107.117.1 out 缺省
202.118.5.0 255.255.255.0 202.118.6.1 out
202.112.0.0 255.255.0.0 202.118.6.1 out
2001-7-6
9:52


NetEye防火墙安全控制台[1.110] - [包过滤规则]
文件(F) 工程(P) 资源(R) 工具(T) 窗口(W) 帮助(H)
规则文件
default
test
dept
审计 源方向 目标方向 操作 访问源 访问目标 优先级 协议 有效时间
编辑过滤规则
常规 操作
协议
TCP
编辑协议
常规 内容过滤
名称(N): Auth
协议
TCP协议(T)
UDP协议(U)
ICMP协议(M)
类型(L): ECHOREPLY
其他协议(E)
协议号范围(P)
目标端口范围(W)
源端口范围(R)
23
1
65535
确定(O) 取消(C)
上一步(B) 下一步(N) 完成(F) 取消(C)
方向: dmz ->
审计: 是
操作: 允许
优先级: 0
访问源: all
访问目标: all
协议:
TCP 协议
Auth
有效时间:
2001-7-6
9:57





3.6 其它重要特性：

- **加密支持**

为了保证数据传输的安全，NetEye3.0 防火墙在管理和认证的通信过程中采用了高强度

的加密算法和可靠的加密机制，可以有效的防止管理和认证信息被通过网络侦听所窃取。

- **双向地址转换（NAT）**

NetEye3.0 提供了完整的地址转换的功能，包括双向的静态转换和动态转换。

静态转换指的是单对单的转换，即转换前地址和转换后地址都是单个的 IP 地址，这种情况没有端口转换的概念，而是直接映射；动态转换其实是端口级 NAT 转换，包括多对一和多对多的转换，即转换前地址是一个地址集，而转换后地址分为两种情况，一种情况是转换为单个 IP 地址，一种情况是转换为一个地址集。

通过静态转换和动态转换，内部主机的 IP 地址可以通过 NAT 转换成外部有效 IP 地址，并且外部主机能够通过访问内部主机经 NAT 转换后得到的有效 IP 地址和端口来访问内部主机提供的服务。

NetEye3.0 还支持双向隐藏的 NAT，即可以对地址进行两次翻译，形成一种对称的结构，从而可以满足更高的安全保护要求。

- **事件报警**

当出现异常事件时，如遭到网络攻击，防火墙根据安全员的配置，可以进行事件报警。NetEye3.0 支持的报警方式有三种：邮件报警、SNMP 报警、蜂鸣报警。

- **支持 VLAN Trunk**

VLAN Trunk 是一个在一个或多个交换端口与另一个网络设备(例如一个路由器或一个交换机)之间的点到点连接(point-to-point link)。Trunk 通过一个单独的一个物理连结负载多个 VLAN 的数据通信，并允许你在整个网络内扩展多个 VLAN。

由于 Trunk 通常是各个 VLAN 的集中通道，在这个通道上安装防火墙可以有效的对各个 VLAN 进行专门的保护。在这个位置的防火墙必须支持专门的 Trunk 封装协议。

NetEye3.0 防火墙能够支持工业标准的 802.1Q 封装协议，因而可以把防火墙架设在交换机与交换机或交换机与路由器之间。并且防火墙还能够利用本身的路由模块代替路由器实现 VLAN 间的数据包转发，这样可以使系统具有更好的性能（因为包传输的路径更短了）和安全性（因为规则更加简洁和清晰）。

- **IP 与 MAC 地址绑定**

为了防止内部网地址盗用，NetEye3.0 提供了 IP 与 MAC 地址绑定的功能。IP 地址与 MAC 地址绑定规定某一 IP 只对应于某一特定的网卡(每个网卡具有唯一的 MAC 地址)，即限定一个 IP 地址只能在一台指定的机器上使用。当某台机器通过防火墙访问 Internet 时，防火墙要检查其发出的数据中的 IP 以及 MAC 是否与防火墙上的规定相符，如果相符就放行。否则不允许通过防火墙，同时给该机器返回一个警告信息。这样可大大方便了网络的 IP 地址管理。

- **流量管理**

NetEye 防火墙 3.0 提供了丰富的流量管理功能。

在 NetEye3.0 防火墙中，用账号来对 IP 主机和用户进行管理，一个账号中可以包括多(单)个 IP 地址/多(单)个用户。帐号根据各自的“组”的属性进行编组，NetEye3.0 的流量控制规则是通过组来制定的。

流量限制是通过规则来实现的，规则分为两类：周期性流量限制规则和一次性流量限制规则。周期性限制是指限制帐号所对应的用户在每个固定的时间段内（如一周或一个月）可

以使用的数据流量；而一次性限制则可以随时为帐户添加预存流量。

当某个帐号的流量超过预定的限制时，防火墙会自动取消帐号中的用户的访问权限。

- **网络实时监控**

除了执行安全策略进行保护以外，防火墙还应该是一个网络安全管理员了解网络状况的重要平台。NetEye 提供了类似专业网络分析仪（如 NAI 的 Sniffer Pro）的在线监控工具，可以对网络当前的负荷状况、连接状况进行详细的分析，并可以对特定的连接数据截获数据包进行数据包的协议结构分析，能够切断特定的 TCP 连接和 UDP 会话。

- **双机热备**

为了保证网络的高可用性，NetEye3.0 防火墙提供了双机热备份功能，即在同一个网络节点使用两个配置相同的防火墙。正常情况下一个处于工作状态，另一个处于备份状态，当工作状态的系统出现故障时，备份状态的防火墙自动切换到工作状态，并保证网络的正常使用。切换过程不需要人为操作和除两个防火墙以外的其他系统的参与。

- **支持 SNMP**

防火墙作为一种网络安全访问控制的基础网络设备，有必要为它提供一种标准的网络管理方式，使其支持网络集中管理，因此在 NetEye3.0 中，提供了对目前在计算机网络中应用最为广泛的网络管理手段，即简单网络管理协议(SNMP)的支持。

NetEye3.0 支持 SNMPv1、v2c 等不同版本，与当前通用的网络管理平台兼容，如 HP Openview、Cisco works 等，可以通过这些管理平台对防火墙的运行状况进行监控，并接收通过 SNMP TRAP 发送的报警信息。

为了避免由于 SNMP 本身的安全性上的缺陷而导致防火墙本身的安全性受到威胁，系统仅允许网管系统查询信息，而不允许改变防火墙的设置。所有可查询的信息都可以由安全管理员通过安全控制台进行限制。缺省状态下，系统的 SNMP 功能是关闭的。

沈 阳 东 软 软 件 股 份 有 限 公 司
地址：沈阳浑南高新技术产业开发区·东大软件园
传真：024-23784036　邮编：110179
网址：www.neusoft.com