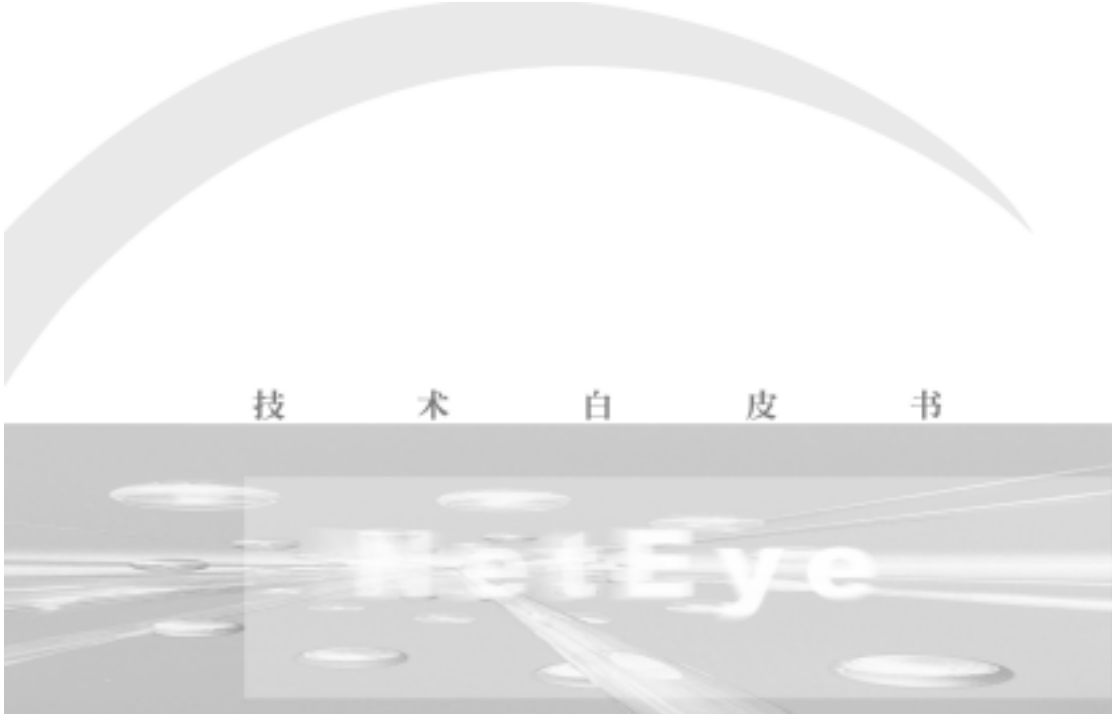
NEUSOFT 东软 软件创造客户价值

SNMP 补充说明

技 术 白 皮 书



SNMP ODDITIONAL EXPLICATION

东 软 集 团 有 限 公 司

SNMP 设置

本系统中支持版本 1、版本 2c、版本 3 的 SNMP，如需要对 SNMP 进行设置，请参考本补充说明。另外，请不要参考 Neteye 防火墙使用指南手册中的事件配置里的 SNMP 的连接，如要配置请选择“ 工具 ”菜单项下的 SNMP 设置。

术语：

- SNMP 用户 SNMPv1 和 SNMPv2c 中提供了基于共用体(community)的安全模型,SNMPv3 中提供了基于用户 （user） 的安全模型，在 Neteye 防火墙系统中，将共用体和用户统称为 SNMP 用户。
- SNMP 视图：MIB（管理信息数据库）的一个子集。定义了包含在这个视图之中以及被排除在这个视图之外的管理信息。
- 访问控制模型：访问控制是指控制用户可以访问的管理信息。SNMPv3 提供了基于视图的访问控制模型，通过将用户和 SNMP 视图关联起来来完成这个工作。
- Trap：SNMP 代理可以查找特定的事件并检测它们，并且发送 Trap 消息给预先配置好的管理工作站。
- 系统信息：包括 SNMP 服务端口、系统物理位置、系统信息、Trap 团体名等信息。

单击“ SNMP 设置 ”菜单项，弹出“ SNMP 设置 ”窗口，如图 1-1 所示：

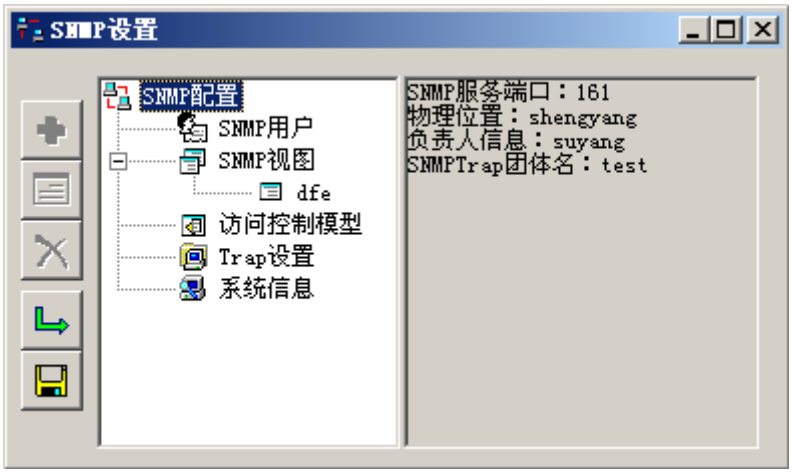


图 1-1 “ SNMP 设置 ”窗口

此窗口由两个部分组成：左边是工具栏，右边是两个列表，一个是 SNMP 配置项列表，另一个是 SNMP 配置信息列表，默认是系统信息。

按钮功能说明：

- 添加：添加 SNMP 用户、SNMP 视图、访问控制模型、Trap 地址等。
- 编辑：编辑 SNMP 用户、SNMP 视图、访问控制模型、Trap 地址、系统信息等。
- 删除：删除 SNMP 用户、SNMP 视图、访问控制模型、Trap 地址等。

- 刷新：重新从防火墙服务端读取配置信息。
- 保存：将配置信息保存到防火墙服务端。

SNMP 配置项：

- SNMP 用户

点击“ SNMP 用户 ”配置项，将显示用户信息列表，如图 1-2 所示：

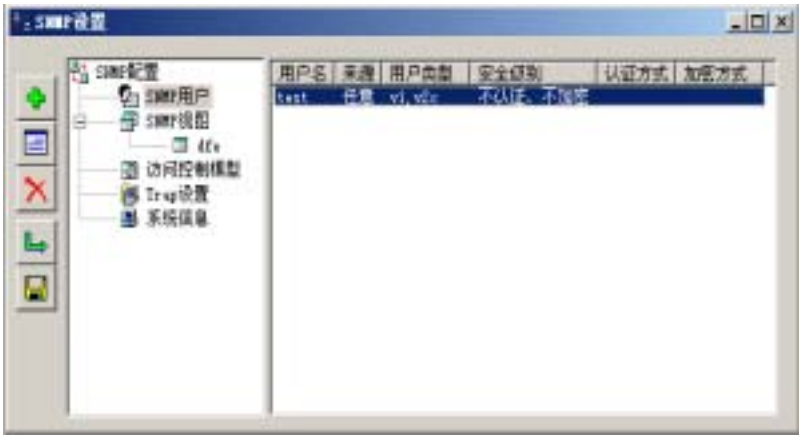


图 1-2 用户信息列表

SNMP 用户配置包括用户名、来源、用户类型、安全级别，如果是 SNMP v3 用户，还包括认证方式（HMAC-MD5-96 和 HMAC-SHA1-96）、加密方式（DES）。

点击“ 添加 ”按钮，将显示“ 添加用户 ”窗口，如图 1-3 所示：

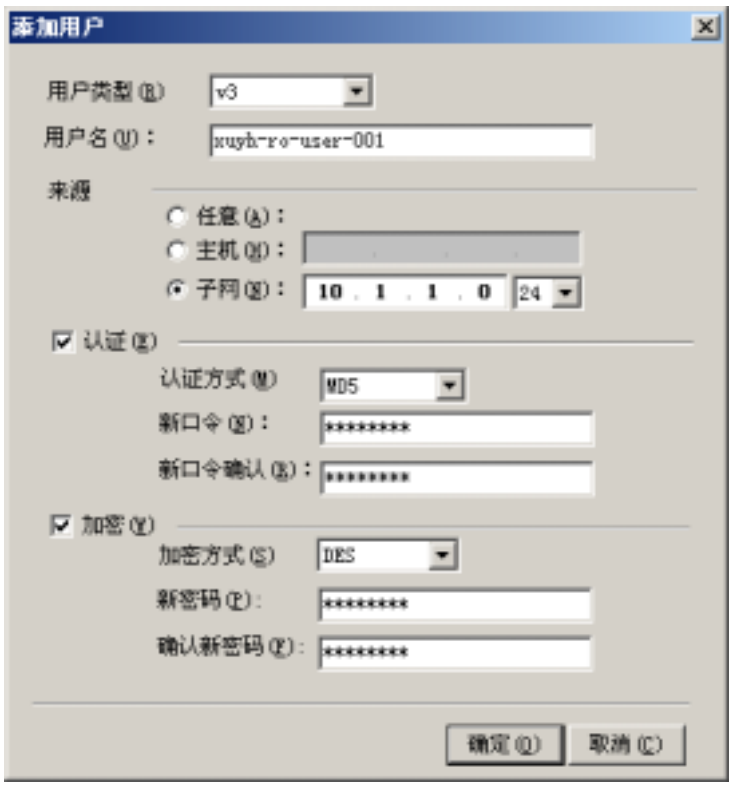


图 1-3 添加 SNMP 用户

“ 用户类型 ”包括版本 1、版本 2c、版本 3 的用户。

“ 用户名 ”的长度不能超过 32 个字节，并且必须是“ a-z ”、“ A-Z ”、“ 0-9 ”、“ - ”、“ _ ”等字符。

“ 来源 ”表示对用户来源的限制。“ 任意 ”表示不限制用户来源，“ 主机 ”表示用户只能从指定主机进行 SNMP 访问，“ 子网 ”表示用户只能从指定子网进行 SNMP 访问。如果用户类型选择版本 3，可以选择认证与加密。认证方式和加密方式可以有以下几

种组合：不加密＋不认证、认证＋不加密、认证＋加密。

在图 1-2 中选中某个用户，点击“ 编辑 ”按钮，将显示“ 编辑用户 ”窗口，如图 1-4 所示：

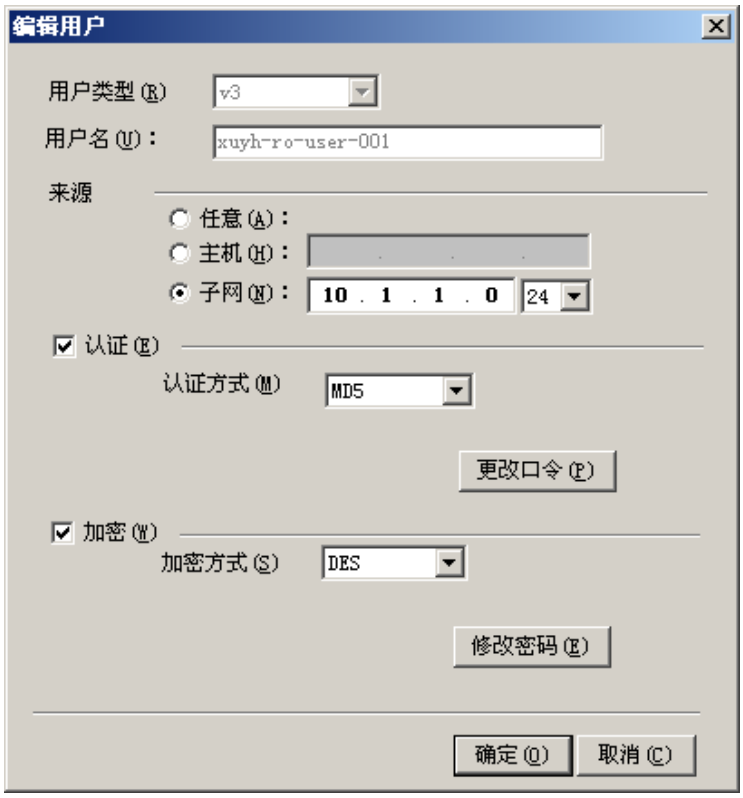


图 1-4 编辑用户

在此窗口中，可以对用户来源、SNMP v3 用户的认证方式、认证口令、加密方式、加密密码进行编辑。

点击〈更改口令〉按钮，显示“ 更改口令 ”窗口，如图 1-5 所示：

图 1-5 更改口令

点击〈修改密码〉按钮，将显示和更改口令相似的“ 修改密码 ”窗口，修改口令和修改密码的时候，首先输入用户旧口令（密码），之后输入新口令（密码），并对新口令（密码）确认。

选中某个用户，点击“ 删除 ”按钮，将删除该用户。如果该用户在访问控制模型中被使用，必须在访问控制模型中删除对应的访问控制规则之后才可以删除该用户。

- SNMP 视图

点击“ SNMP 视图 ”配置项，将显示 SNMP 视图列表，如图 1-6 所示：

图 1-6 SNMP 视图列表

选中某个视图，将显示该视图的信息，如图 1-7 所示：

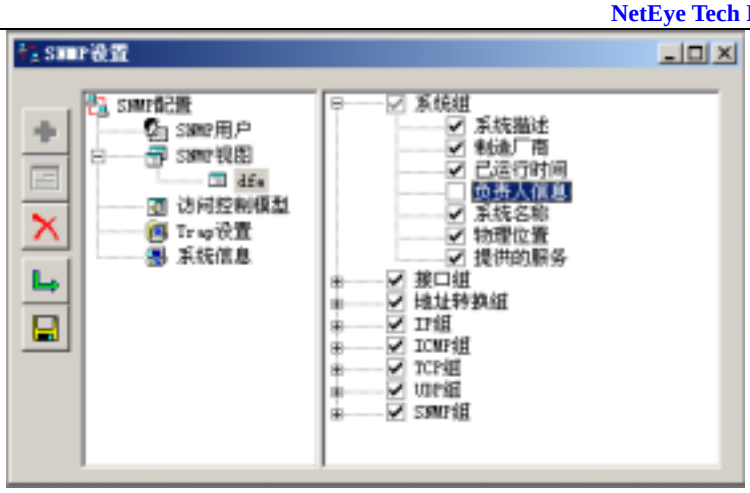


图 1-7 SNMP 视图

在此窗口中，右侧为管理信息列表，可以在管理信息列表中选择 MIB 信息。

选中某个视图，点击“ 删除 ”按钮，将删除该视图。如果该视图在访问控制模型中被使用，则必须首先删除对应的访问控制规则才能够删除该视图。

- 访问控制模型

点击“ 访问控制模型 ”配置项，将显示访问控制列表，如图 1-8 所示：

图 1-8 访问控制模型列表

点击“ 添加 ”按钮，将显示添加访问控制模型界面，如图 1-9 所示：

图 1-9 添加访问控制模型

用户名：显示的是用户信息中的用户列表。

安全模型：包括 v1、v2c 以及 usm（基于用户的安全模型）三种安全模型。

安全级别：当安全模型选择为 usm 时，可以选择安全级别：不认证＋不加密、认证＋不加密、认证＋加密三种安全级别。

视图：在 SNMP 视图中配置的视图列表。

图 1-9 所示的含义为：SNMP 的用户 xuyh-ro-user-001，如果想要访问防火墙上 ro-view-001 视图指定的管理对象，必须满足以下三个条件：使用 usm 安全模型，安全等级设置为认证＋加密，用户的源地址必须在 10.1.1.0 网段中（添加用户时候指定）。

选中某一访问控制模型，点击“ 编辑 ”按钮，将出现“ 编辑访问控制模型 ”窗口，如图 1-10 所示：

图 1-10 编辑访问控制模型

选中某一访问控制模型，点击“ 删除 ”按钮，将删除该条访问控制模型。

- Trap 设置

点击“ Trap 设置 ”配置项，将显示 Trap 设置信息，如图 1-11 所示：

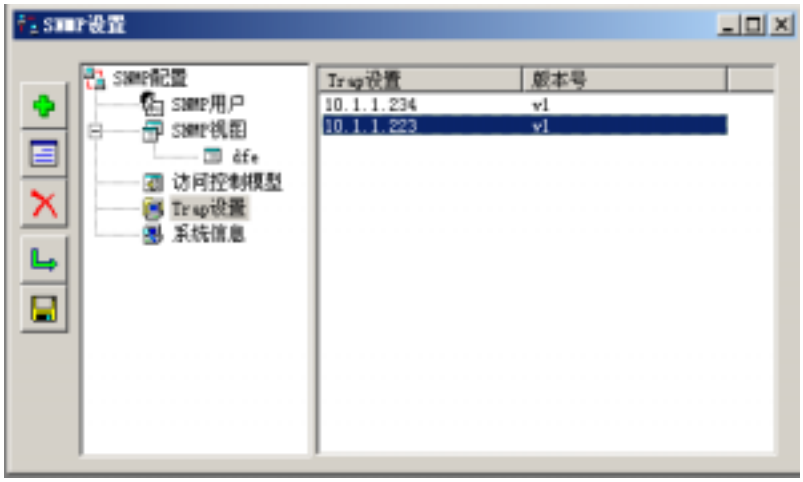


图 1-11 Trap 信息列表

点击“添加”按钮，将显示添加 Trap 地址窗口，如图 1-12 所示：

图 1-12 添加 Trap 地址

选中某一 Trap 地址，点击“编辑”按钮，将显示编辑 Trap 地址窗口，如图 1-13 所示：

图 1-13 编辑 Trap 地址

在 1-13 和 1-14 两个窗口中，可以添加或编辑接受 Trap 信息的主机的 IP 地址，这样，如果安全员在事件设置中，把某些事件的报警方式设置为“向 SNMP 报警”，则防火

墙发生这些事件时，SNMP 代理将发送 Trap 信息给这些 IP 地址的主机上。

选中某一 Trap 地址，点击“ 删除 ”按钮，将删除该条 Trap 设置。

- 系统信息

点击“ 系统信息 ”配置项，将显示系统信息配置，如图 1-14 所示：

图 1-14 系统信息

点击“ 编辑 ”按钮，将显示系统信息配置窗口，如图 1-15 所示：

图 1-15 系统信息设置

在此窗口中，可以设置防火墙的物理位置、系统负责人信息（如 mail 等）、SNMP 服务端口、SNMP Trap 团体名。

点击“ 刷新 ”按钮，管理器将从防火墙服务器端重新获取所有配置信息，该信息为上一次保存的结果。

点击“ 保存 ”按钮，将管理器中设置的所有配置信息保存到防火墙服务器上。