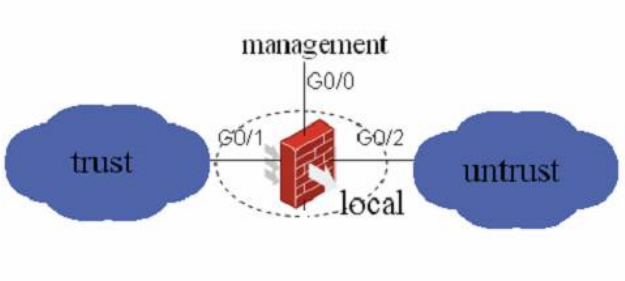
UTM开局预配置(三层)

万欣 2008-09-11 发表

（1）拓扑：

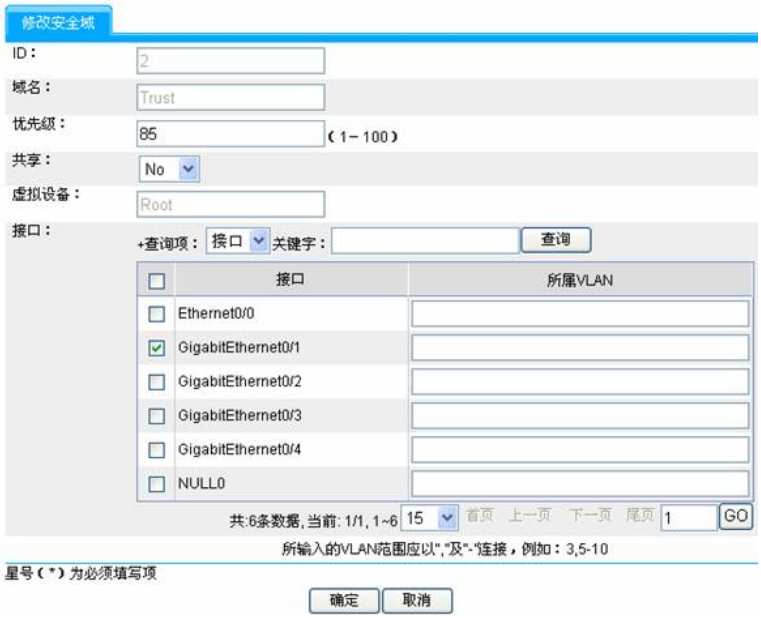


(2) U200-S运行于UTM模式
[H3C]startup utm
[H3C]
(3) 接口模式
G0/0、G0/1、G0/2、Eth0/0均为三层接口
Eth0/0的IP地址设置为10.254.254.1/24（必须设为该地址）。

系统管理 > 接口管理 > 指定接口操作栏中修改本接口按钮

（4）安全域
G0/0、Eth0/0置于Management域
G0/1置于root设备Trust域
G0/2置于root设备Untrust域

Web页面“系统管理 > 安全域管理 > 指定安全域操作栏中编辑安全域按钮 ”



(5) 配置ACL

创建三个ACL：

一个用于内网访问Internet时进行NAT（规则的源IP为内网IP网段）

一个用于i-ware的对外访问（规则的源IP为10.254.254.2/32）

一个用于深度安全策略（两条规则：源IP或目的IP为内网IP网段）

l “策略管理 > ACL > 新建 > 输入访问控制列表ID号（2000~3999） > 点击<确定>”

l 已创建ACL“操作”栏中“详细资料 > 新建 > 输入‘规则ID’”

l 选择“操作”；

l 对于基本ACL，输入“源IP地址”和“源地址通配符”(可选)，对于高级ACL选择协议、配置源IP地址/源地址通配符（可选）、配置目的IP地址/目的地址通配符（可选）、配置源操作/端口（可选，基于协议选择）、配置目的操作/端口（可选，基于协议选择）、点击<确定>；

(6) 配置NAT

包括：内网用户访问Internet时的NAT；i-ware更新特征库时的NAT；以及对i-ware进行配置管理时的NAT Server。

“策略管理 > 地址转换策略 > 地址转换 > 新建 > 选择接口（G0/2）”，输入acl号，地址转换方式选择Easy IP > 点击<确定>。

l “策略管理 > 地址转换策略 > 地址转换 > 新建 > 选择接口（G0/0）”，输入acl号，地址转换方式选择Easy IP > 点击<确定>。

l “策略管理 > 地址转换策略 > 内部服务器 > 新建 > 选择接口（G0/0）> 选择协议类型（TCP） > 输入外部IP地址（接口G0/0的IP地址） > 输入外部端口（8080） > 输入内部IP地址（10.254.254.2） > 输入内部端口（80） >点击<确定>”

(7) 保存配置

l “系统管理 > 配置维护 > 配置保存 > 点击<确定>”