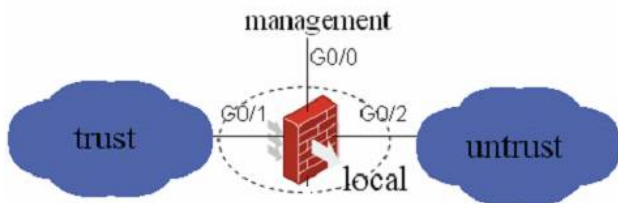


(1) 拓扑:



(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

接口编辑

接口名称: GigabitEthernet0/1

接口类型: 不设置

VID:

MTU: 1500 (46-1500, 缺省值=1500)

TCP MSS: 1460 (128-2048, 缺省值=1460)

工作模式:  二层模式  三层模式

IP配置:  无IP配置  静态地址  DHCP  BOOTP  PPP协商  借用地址

IP地址: 192.168.1.1

网络掩码: 24 (255.255.255.0)

其他接口: Ethernet0/0

确定 返回

(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”

修改安全域

ID: 2

域名: Trust

优先级: 85 (1-100)

共享: No

虚拟设备: Root

接口: +查询项: 接口 关键字:  查询

<input type="checkbox"/>	接口	所属VLAN
<input type="checkbox"/>	Ethernet0/0	<input type="text"/>
<input checked="" type="checkbox"/>	GigabitEthernet0/1	<input type="text"/>
<input type="checkbox"/>	GigabitEthernet0/2	<input type="text"/>
<input type="checkbox"/>	GigabitEthernet0/3	<input type="text"/>
<input type="checkbox"/>	GigabitEthernet0/4	<input type="text"/>
<input type="checkbox"/>	NULL0	<input type="text"/>

共6条数据, 当前: 1/1, 1~6 15 首页 上一页 下一页 尾页 1 GO

所输入的VLAN范围应以","及"-连接, 例如: 3,5-10

星号(\*)为必须填写项

确定 取消

## (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）

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

新建ACL

访问控制列表ID: 3999 \* 2000-2999 基本访问控制列表。  
3000-3999 高级访问控制列表。  
4000-4999 二层访问控制列表。

匹配规则: 用户配置

星号(\*)为必填填写项

确定 取消

1 已创建ACL“操作”栏中“详细资料 > 新建 > 输入‘规则ID’”

1 选择“操作”；

1 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>；

访问控制列表ID	类型	规则数量	匹配顺序	ACL加速管理	操作
3999	高级	0	用户配置		

新建 详细资料

ACL=3999 新建高级规则

规则ID: (0-65534。如果不输入规则ID，系统将会自动指定一个。)

操作: 允许 时间段: 无限制

分片报文  记录日志

IP地址过滤

源IP地址: 192.168.1.0 源地址通配符: 0.0.0.255

目的IP地址: 目的地址通配符:

协议 VPN实例: 无限制

协议: IP 选择ICMP: ---

ICMP类型: (0-255) ICMP码: (0-255)

TCP已连接

源操作: 无限制 端口: (0-65535)

目的操作: 无限制 端口: (0-65535)

优先级过滤

ToS: 无限制 Precedence: 无限制

DSCP: 无限制

确定 取消

## (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>。

新建地址转换

接口: GigabitEthernet0/2

ACL: 3999 \* (2000-3999)

地址转换方式: Easy IP

地址池索引: (0-31)

星号(\*)为必填填写项

确定 取消

1 “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>。

1 “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>”

**修改内部服务器**

接口：	<input type="text" value="GigabitEthernet0/0"/>
VPN实例：	<input type="text"/>
协议类型：	<input type="text" value="B(TCP)"/>
外部IP地址：	<input type="text" value="10.154.3.245"/> *
外部端口：	<input checked="" type="radio"/> <input type="text" value="8080"/> ( 0- 65535, 0表示任意端口 )
	<input type="radio"/> <input type="text"/> - <input type="text"/> ( 1- 65535 )
内部IP地址：	<input type="text" value="10.254.254.2"/> *
	<input type="text"/> - <input type="text"/>
内部端口：	<input type="text" value="80"/> ( 0- 65535, 0表示任意端口 )

星号(\*)为必须填写项

(7) 保存配置

1 “系统管理 > 配置维护 > 配置保存 > 点击<确定>”