

403 Forbidden

本电子书由CyberArticle制作。点击[这里](#)下载CyberArticle。注册版本不会显示该信息。[删除广告](#)

防火墙日志输出到日志主机

目录

[1 配置需求或说明](#)

[1.1 适用的产品系列](#)

[1.2 配置需求及实现的效果](#)

[2 组网图](#)

[3 配置步骤](#)

[3.1 创建连接日志服务器的接口](#)

[3.2 创建安全策略](#)

[3.3 创建日志主机](#)

[3.4 保存配置](#)

[3.5 日志主机设置（举例）](#)

1 配置需求或说明

1.1 适用的产品系列

本案例适用于软件平台为Comware V7系列防火墙：F100-X-G2、F1000-X-G2、F100-WiNet、F1000-AK、F10X0等。

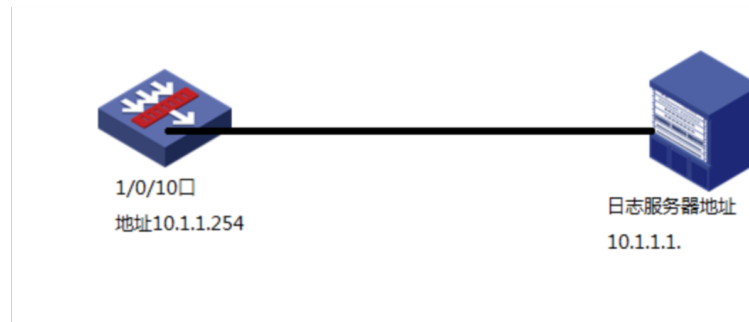
注：本案例是在F1000-C-G2的Version 7.1.064, Release 9345P2416版本上进行配置和验证的。

1.2 配置需求及实现的效果

将防火墙运行中产生的系统日志信息输出到日志主机，避免设备侧硬

件存储限制，即使防火墙发生故障无法启动也可以查看已经输出的日志信息。

2 组网图



3 配置步骤

3.1 创建连接日志服务器的接口

#在“网络”>“接口”选项中选择1/0/10接口并点击此接口最后面的”编辑”按钮。



“IP 地址” 填写和服务器同网段的地址 10.1.1.254，掩码 255.255.255.0，安全域选 Trust，也可以自行新建其他安全域并加入。

修改接口设置

① ×

名称

GE1/0/10

链路状态

Down

☐ 禁用

描述

GigabitEthernet1/0/10 Interface

工作模式

三层模式

安全域

Trust

基本配置

IPv4地址

IPv6地址

物理接口配置

保持上一跳

☒ 开启☐ 关闭

IP地址

☒ 指定IP地址☐ DHCP☐ PPPoE

IP地址/掩码长度

10.1.1.254 / 255.255.255.0

网关

+ 指定从IP地址

- 删除从IP地址

☐ 从IP地址

掩码

编辑

应用

确定

取消

3.2 创建安全策略

#在策略-安全策略中点击新建，选择新建策略

“源安全域”选择Local，“目的安全域”选择Trust，在“目的IP地址”中选择“添加IPv4地址对象组”，地址为日志服务器ip 10.1.1.1/32。

新建安全策略

名称 rizhi 自动命名

源安全域 Local [多选]

目的安全域 Trust [多选]

类型 IPv4 IPv6

所属策略组 请选择策略组

描述信息 (1-127字符)

动作 允许 拒绝

源IP/MAC地址

地址对象组 请选择或输入对象组 [多选]

IPv4地址

目的IP地址

地址对象组 请选择或输入对象组 [多选]

IPv4地址 + 新建IPv4地址对象组

Any

服务

确定 取消

新建IPv4地址对象组

对象组名称 * (1-31字符)

描述 (1-127字符)

安全域

类型	内容	排除地址	编辑
没有数据			

确定 取消

添加对象

对象 * (IPv4地址)

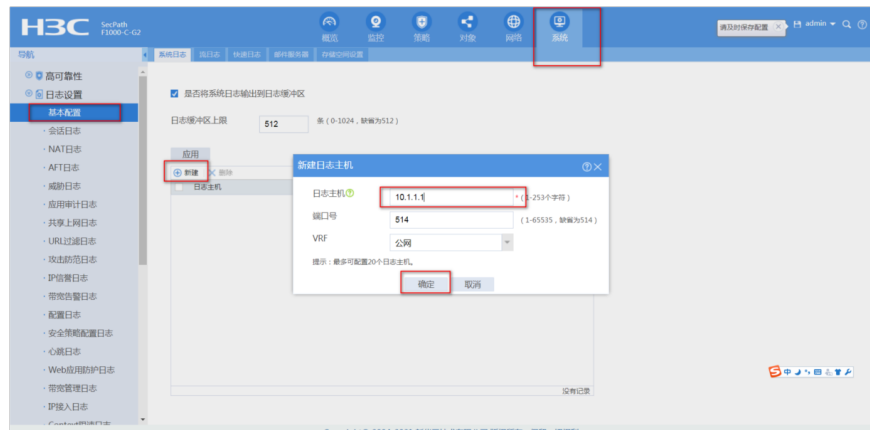
确定 取消

#完成后如下图所示

名称	源安全域	目的安全域	类型	ID	描述	源地址	目的地址	服务	用户	动作	内容...	命中...	流量	统计	应用	会话查看	编辑
riahi	Local	Trust	IPv4	0		Any	服务器	Any	Any	允许					<input checked="" type="checkbox"/>	查看	编辑

3.3 创建日志主机

#在“系统”-“日志设置”-“基本配置”-“系统日志”界面新建日志主机为10.1.1.1



3.4 保存配置

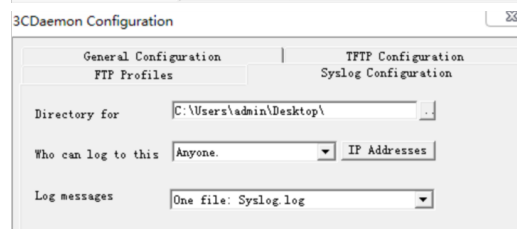
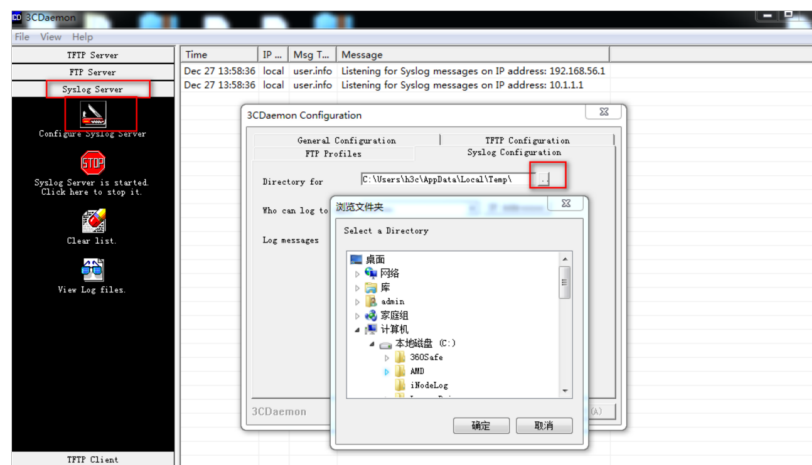
#在设备右上角选择“保存”选项，点击确定按钮完成配置。



3.5 日志主机设置（举例）

#案例中以3CDEmon举例参考，日志主机根据自己实际使用的日志软件或者专业日志主机进行设置。

如下图点击syslog server界面配置日志主机，指定存储日志文件的位置



#注意：创建好后需要点击左侧红色“STOP”禁用，然后变为绿色“GO”后再点击该按钮，让配置生效

测试可以收到日志信息：

