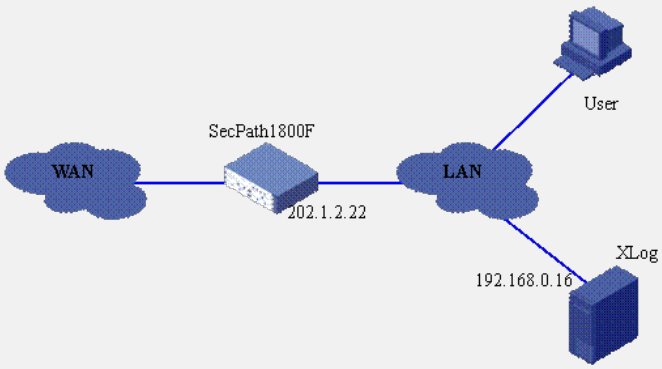
XLog F0204和SecPath1800F配合接收Flow日志的典型配置

陈斌A 2007-03-23 发表

XLog F0204和SecPath1800F配合接收Flow日志的典型配置

一　组网需求：
XLog V2.10-F0204，SecPath1800F
XLog和SecPath1800F路由可达，用户能和外网互通。

二　组网图：



SecPath1800F　Comware, V3.40-R0357.02(08)
XLog V2.10-F0204

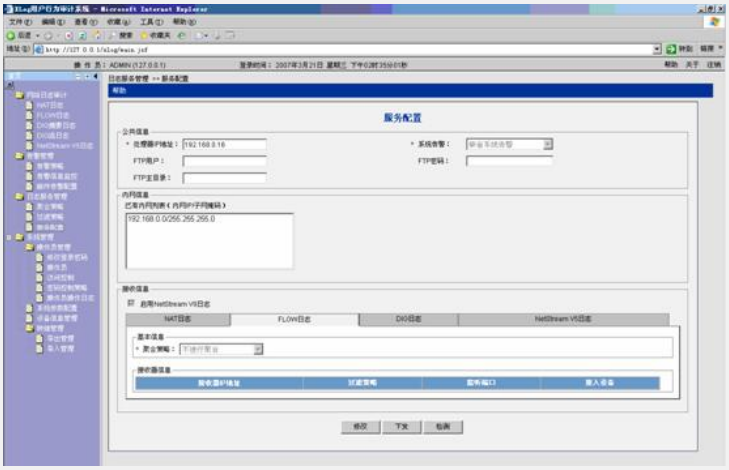
三　配置步骤：
3.1　配置设备
置防火墙域间记录Session的ACL
acl number 2000
rule 0 permit source 192.168.0.0 0.0.0.255
配置日志类型和XLog的地址、端口
firewall session log-type binary host 192.168.0.16 9020

将内网接口加入信任域，将外网接口加入不信任域
firewall zone trust
add interface Ethernet1/0/1
firewall zone untrust
add interface Ethernet1/0/0

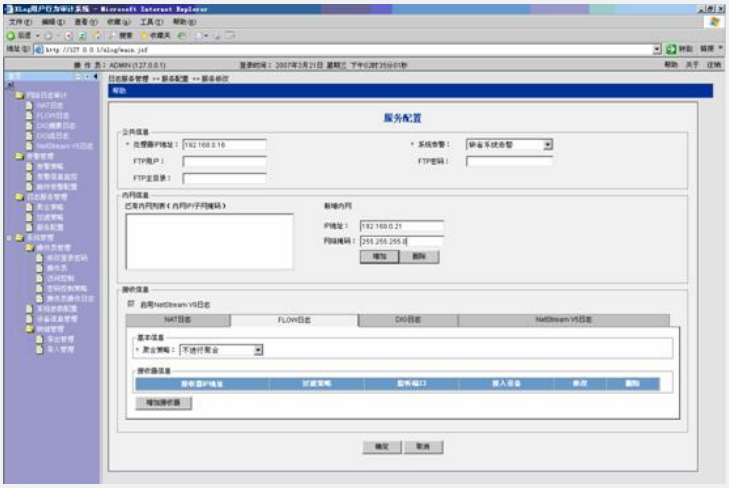
将域间的session进行日志记录
firewall interzone trust untrust
session log enable acl-number 2000 inbound
session log enable acl-number 2000 outbound

确认设备时间
dis clock　\\查看设备当前时间是否正确，若不正确请修改

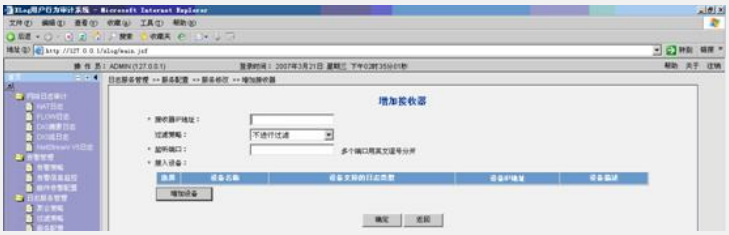
3.2　配置XLog
3.2.1　　请先确认Windows系统的时间和时区正确。
3.2.2　　在Windows的服务管理中停止XLog的两个服务：
H3C Xlog Server；H3C XLog Web Server
3.2.3　　用记事本打开配置文件：\H3C\XLog\conf**sysreceiver.xml**，修改该文件的如下参数由**0**改为**2**：
<BinaryLogProcessMode>**0**</BinaryLogProcessMode>
3.2.4　　启动XLog的两个服务。
3.2.5　　登陆到XLog配置管理平台：http://192.168.0.16/xlog
3.2.6　　点击左侧菜单中的<日志服务管理> <服务配置>，出现如下的配置界面：



3.2.7　　点击<修改>后配置相关参数，配置处理器地址（XLog 服务器的地址），添加内网网端，选择Flow日志菜单，增加接收器。

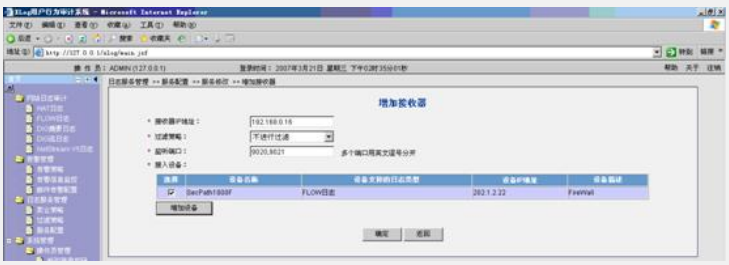


3.2.8　　进入增加接收器界面后点击增加设备：

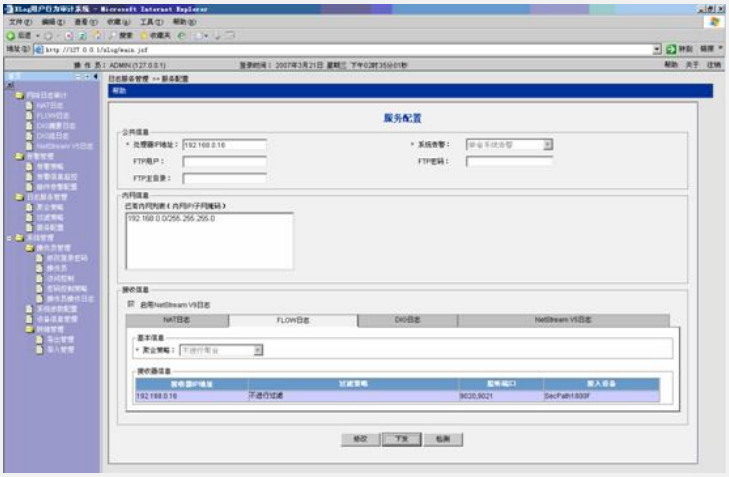


3.2.9　　输入设备名称，IP地址，选择设备时间处理方式。

3.2.10　　返回接收器界面，配置接收器IP，端口。



3.2.11　　返回服务配置窗口，点击<下发>

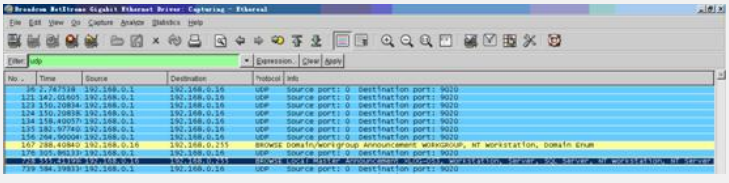


3.2.12　接下来会弹出下发的情况。

3.2.13　确定后再通过<检测>确认处理器和接收器的运行情况：

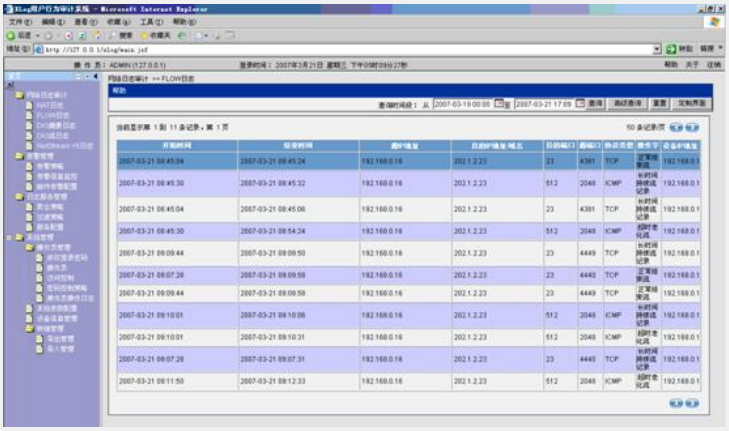
3.2.14　点击<详细信息>可以查看具体情况：

3.2.15　（此步不是必需）通过抓包确认设备已经正常发送UDP的日志报文到指定端口（9020）。



3.2.16　（此步不是必需）经过一段时间后，在\receiver_data文件夹下能发现Flow日志报文。

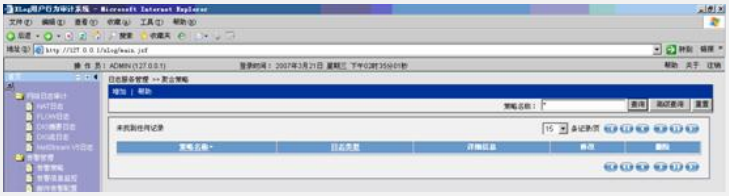
3.2.17　正常情况下再经过10分钟后就能在XLog的控制台上查询到Flow日志：
(请注意查询的结束时间需要比当前时间晚)：



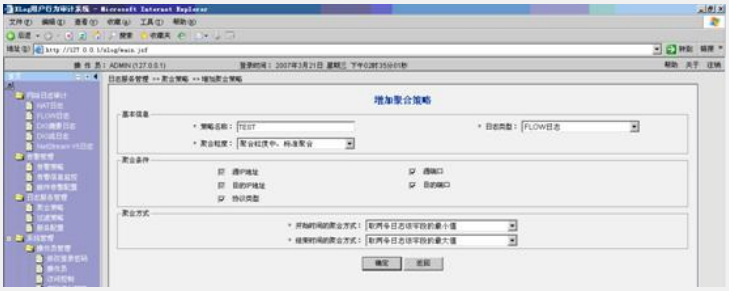
3.3 配置聚合和过滤策略

为了减少日志占用空间，需要配置聚合和过滤，具体步骤如下：

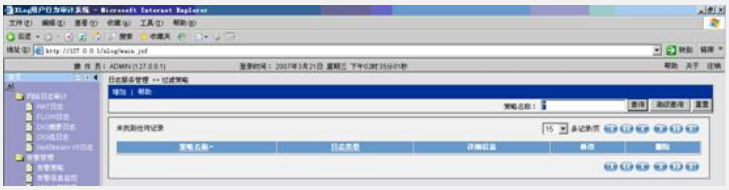
3.3.1 点击<日志服务管理> <聚合策略>，进入如下窗口，点击左上侧的<增加>创建聚合策略：



3.3.2 输入聚合策略名称、日志类型，聚合粒度等。



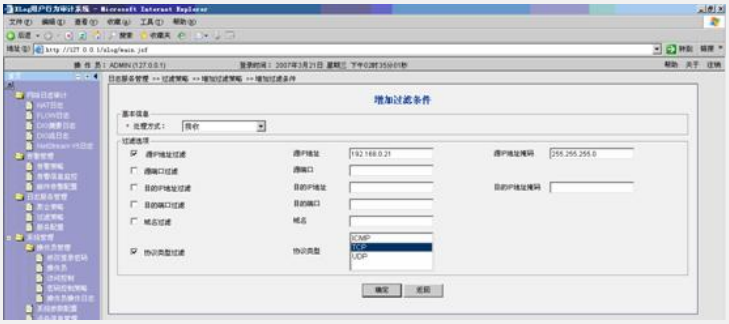
3.3.3 点击<日志服务管理> <过滤策略>，进入如下窗口，点击左上侧的<增加>创建过滤策略：



3.3.4 输入策略名称、日志类型、对不满足过滤条件的日志的处理方式，再点击<增加过滤条件>。

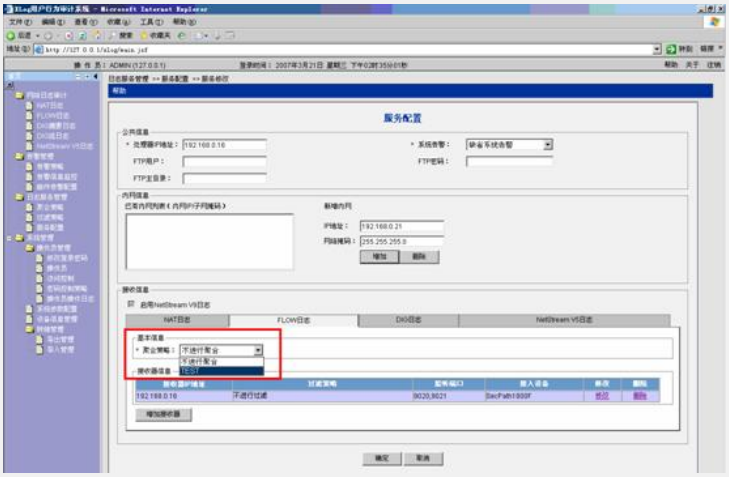
注意：这里的过滤策略必须慎重配置，不要丢弃了有用的日志。

3.3.5 配置相关参数：

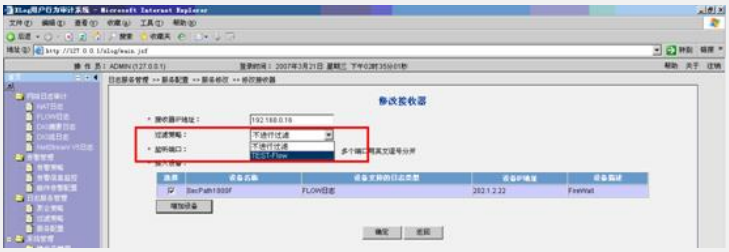


3.3.6 确定，返回。

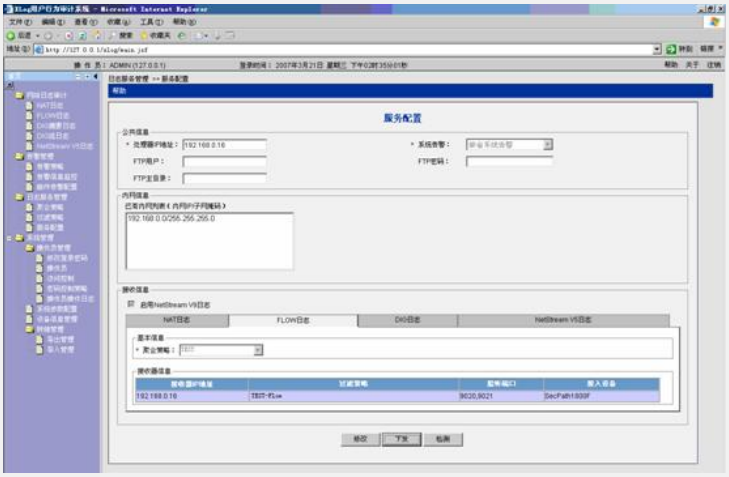
3.3.7 点击<日志服务管理>，<服务配置>，<修改>，在Flow日志的聚合策略中选择刚创建的策略。



3.3.8 在接收器选项中点击<修改>，<过滤策略>，选择刚建立的策略：



3.3.9 确定后返回服务配置页面，点击<下发>重新下发服务：



3.3.10　确认下发成功后，就大功告成了。

四　配置关键点：

1．正确配置设备和Windows系统的时间。

2．修改sysreceiver.xml文件

3．正确配置过滤条件。