XLog配合SecPath1000F接收NAT日志的典型配置

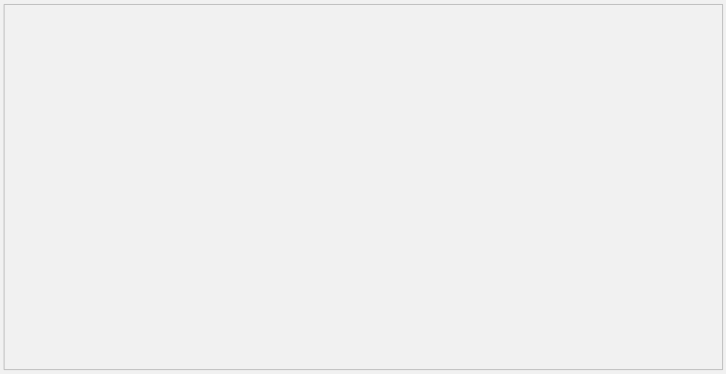
陈斌A 2006-11-06 发表

XLog配合SecPath1000F接收NAT日志的典型配置

一　组网需求：

1. 防火墙已经配置好安全过滤策略；
2. 防火墙和Xlog服务器能够互通；
3. XLog日志能正常通过防火墙内网接口。

二　组网图：



组网设备：防火墙：SecPath1000F VRP3.40, ESS 1605
XLog服务器：V1.2 R0315
IP规划：防火墙内网口： 172.16.200.2 255.255.255.0
防火墙外网口： 222.33.43.37 255.255.255.248
XLog服务器： 172.16.200.3 255.255.255.0

三　配置步骤：

1　配置防火墙

配置内网接口
[SecPath1000F] interface GigabitEthernet0/1
[SecPath1000F-interface-GigabitEthernet0/0] ip address 172.16.200.2 255.255.255.0

配置ACL
acl number 3000
rule 0 permit source 172.16.200.3 0.0.0.255 logging

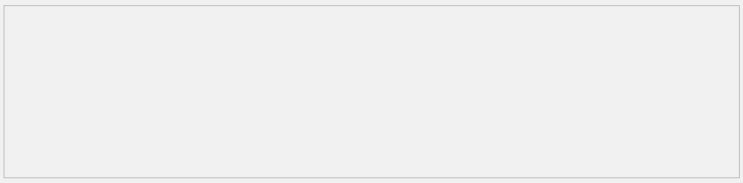
配置NAT
[SecPath1000F] nat address-group 0 222.33.43.33 222.33.43.37
[SecPath1000F] interface GigabitEthernet0/0
[SecPath1000F-interface-GigabitEthernet0/0] ip address 222.33.43.37 255.255.255.248
[SecPath1000F-interface-GigabitEthernet0/0] nat outbound 3000 address-group 0

配置XLog服务器地址及日志类型
[SecPath1000F] firewall binary-log host 172.16.200.3 9020
[SecPath1000F] firewall session log-type binary
[SecPath1000F] firewall nat log-type binary
[SecPath1000F] firewall session log-threshold time 1

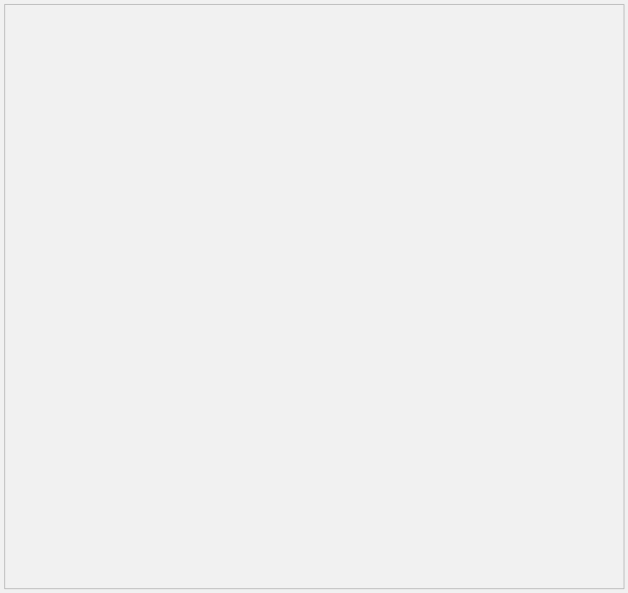
2　Xlog上的配置

2.1 停止XLog的两个服务：H3C Xlog Server ； H3C XLog Web Server
2.2 用记事本打开配置文件：\H3C\XLog\conf**sysreceiver.xml**，修改该文件的两个参数：
<BinaryLogProcessMode>**0**</BinaryLogProcessMode> 将0改为1
<TimeZone>**LOCAL**</TimeZone> LOCAL修改为GMT
2.3 启动XLog的两个服务。
2.4 登陆到XLog配置管理平台：http://172.16.200.3/xlog

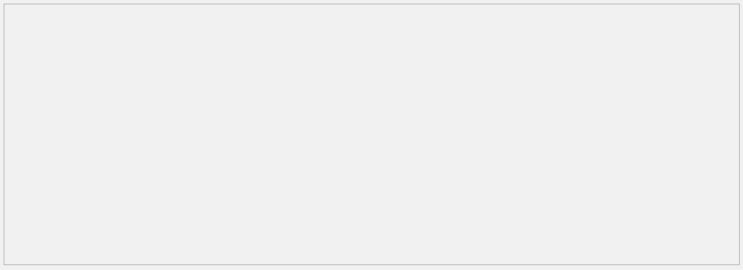
2.5. 配置过滤策略（可选）：日志服务配置>>过滤策略>>增加



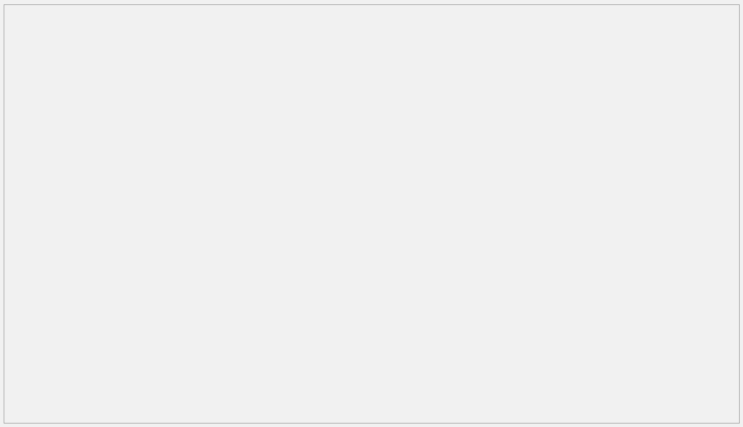
2.6 增加过滤条件：



2.7 配置聚合策略：日志服务配置>>聚合策略>>增加



2.8 配置服务：日志服务配置>>日志服务>>增加
这里处理器IP可以是实际IP也可以是127.0.0.1，推荐用后者。文件接受路径和文件保存路径需要手工添加，日志类型必须和设备上的日志类型一致。



日志接收器可以有多个，可以通过右下角的"添加接收器"按钮添加，若有多个接收器则必须架设FTP服务器且在服务中填上相关信息。在接收器的配置中选取过滤策略和聚合策略，保存。

2.9 下发配置：选择下发则会使配置立即生效。

3　　日志的接收

下发配置后大约15分钟后就可以在网络日志管理>>日志管理页面下看见生成的日志文件

再过10分钟左右就能够在网络日志管理>>NAT日志中查询到NAT日志

四　　配置关键点：

修改sysreceiver.xml以接收二进制日志中的NAT日志。