SecPath1800F 日志服务器功能配置

王刚 2006-10-30 发表

SecPath1800F 日志服务器功能的配置

一、 组网需求：

日志功能是防火墙比不可少的功能之一，它防火墙的状态信息是。SecPath1800F可以通过外部的日志服务器记录防火墙的syslog信息、二进制流日志信息。

二、 组网图：

三、 配置步骤：

适用版本：SecPath1800F 所有防火墙版本

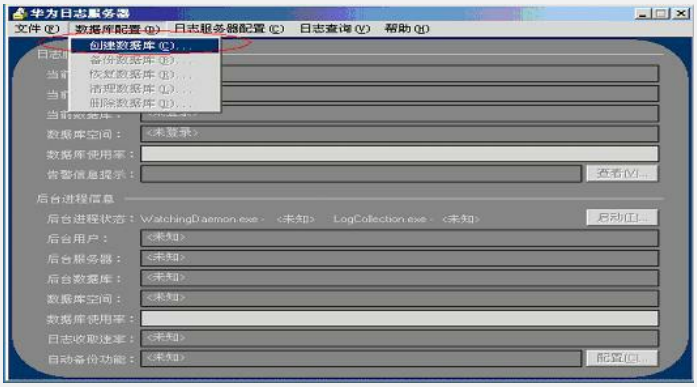
```
#
acl number 2000                          // 设置防火墙日志相关的acl
 rule 0 permit source 10.1.1.0 0.0.0.255
#
 sysname Eudemon
#
 info-center loghost 10.1.1.1            // 设置syslog日志主机
#
 firewall packet-filter default permit interzone local trust direction inbound
 firewall packet-filter default permit interzone local trust direction outbound
 firewall packet-filter default permit interzone local untrust direction inbound
 firewall packet-filter default permit interzone local untrust direction outbound
 firewall packet-filter default permit interzone local dmz direction inbound
 firewall packet-filter default permit interzone local dmz direction outbound
 firewall packet-filter default permit interzone trust untrust direction inbound
 firewall packet-filter default permit interzone trust untrust direction outbound
 firewall packet-filter default permit interzone trust dmz direction inbound
 firewall packet-filter default permit interzone trust dmz direction outbound
 firewall packet-filter default permit interzone dmz untrust direction inbound
 firewall packet-filter default permit interzone dmz untrust direction outbound
#
 firewall mode route
#
firewall session log-type binary host 10.1.1.1 9002  // 设置二进制日志主机及端口号
#
 firewall statistic system enable
#
interface Aux0
 async mode flow
 link-protocol ppp
#
interface Ethernet0/0/0
#
interface Ethernet0/0/1
#
interface Ethernet1/0/0
```

```
#
interface Ethernet1/0/1
 ip address 10.1.1.254 255.255.255.0
#
interface Ethernet1/0/2
#
interface Ethernet1/0/3
 ip address 202.106.86.254 255.255.255.0
#
interface Ethernet1/0/4
#
interface Ethernet1/0/5
#
interface Ethernet1/0/6
#
interface Ethernet1/0/7
#
interface NULL0
#
firewall zone local
 set priority 100
#
firewall zone trust                                    // 相应端口加入域
 set priority 85
 add interface Ethernet1/0/1
#
firewall zone untrust                                  // 相应端口加入域
 set priority 5
 add interface Ethernet1/0/3
#
firewall zone dmz
 set priority 50
#
firewall interzone local trust
#
firewall interzone local untrust
#
firewall interzone local dmz
#
firewall interzone trust untrust                       // 在域间启用日志功能
 session log enable acl-number 2000 inbound
 session log enable acl-number 2000 outbound
#
firewall interzone trust dmz
#
firewall interzone dmz untrust
#
aaa
 authentication-scheme default
#
 authorization-scheme default
#
 accounting-scheme default
#
 domain default
#
#
 ip route-static 0.0.0.0 0.0.0.0 202.106.86.253
#
user-interface con 0
user-interface aux 0
user-interface vty 0 4
#
return
```

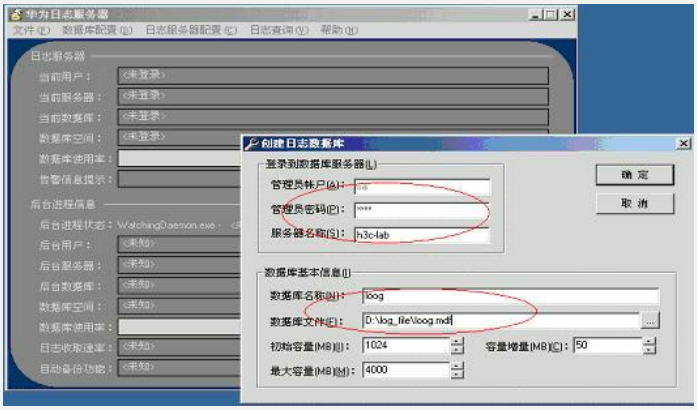
四、 日志服务器配置：

1、安装日志服务程序后，跳过设置界面

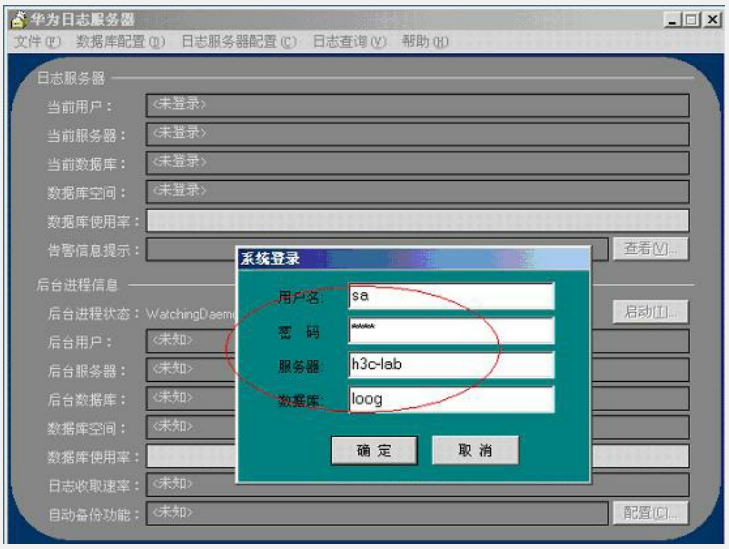
2、启动日志服务器程序设置相应的选项（创建数据库）



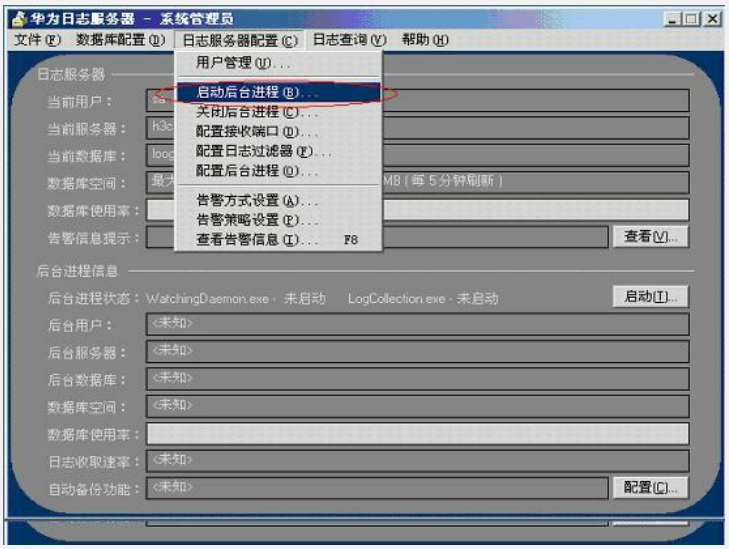
3、设置数据库相应的参数



4、配置后登陆数据库



5、启动后台进程（这一步很重要）



五、 配置关键点:

只有p2p限流版支持实时流量监控的功能，在防火墙上使用命令（全局模式）：

firewall log stream enable