SecPath防火墙Netflow日志功能的典型配置

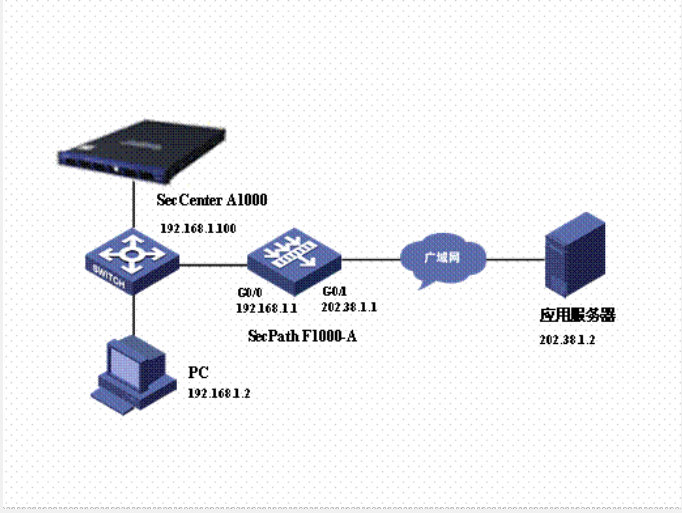
赵彪 2007-11-02 发表

SecPath防火墙Netflow日志功能的典型配置

一、 组网需求：

对所有经过防火墙的会话以及攻击防火墙的实时连接进行采集，通过发送Netflow日志给SecCenter A1000进行安全审计。

二、 组网图



目前防火墙只有V1R6及以后的版本支持。

三、 配置步骤

1. SecPath F1000-A的主要配置

```
#
 sysname SecPath F1000-A
#
 firewall packet-filter enable
 firewall packet-filter default permit
#
 firewall binary-log host 192.168.1.100 9002  //配置二进制日志主机IP及端口
 firewall session log-type binary                 //指定防火墙会话日志类型
 firewall session log-threshold time 5                 //指定日志发送阀值
#
acl number 3000
 rule 0 permit ip source 192.168.1.0 0.0.0.255
#
interface GigabitEthernet0/0
 ip address 192.168.1.1 255.255.255.0
#
interface GigabitEthernet0/1
 ip address 202.38.1.1 255.255.255.0
 nat outbound 3000
#
firewall zone trust
 add interface GigabitEthernet0/0
 set priority 85
#
firewall zone untrust
 add interface GigabitEthernet0/1
 set priority 5
#
firewall interzone trust untrust
 session log enable                          //在域间开启会话日志功能
#
```

四、 配置关键点

1. 防火墙会话是二进制日志，可以通过display firewall session table查看，不会保存到logbuffer中；
2. 支持Netflow日志的软件有Xlog和SecCenter等。