从协议说起（3）——Userlog

Flow日志 **胡伟** 2020-10-15 发表

组网及说明

无

配置步骤

Flow日志用来记录NAT会话信息，主要包括用户访问网络的流的5元组信息（源IP地址、目的IP地址、源端口、目的端口、协议号），以及发送和接收的报文统计信息。配置步骤如下：

```
# 开启NAT日志功能。
system-view
[Device] nat log enable
# 开启NAT新建、删除会话和活跃流的日志功能。
[Device] nat log flow-begin
[Device] nat log flow-end
[Device] nat log flow-active 10
# 将Flow日志报文版本号设为3.0。
[Device] userlog flow export version 3
# 将Flow日志信息发送给Flow日志主机（地址为1.2.3.6:2000）。
[Device] userlog flow export host 1.2.3.6 port 2000
# 将2.2.2.2配置为承载Flow日志的UDP报文的源IP地址。
[Device] userlog flow export source-ip 2.2.2.2
```

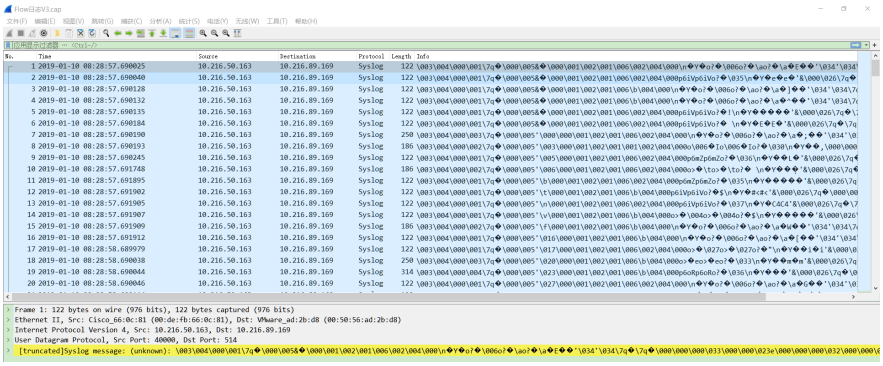
Flow日志有两种输出方式：

· 将Flow日志封装成UDP报文直接发送给网络中的日志主机。日志主机可以对Flow日志进行解析和分类显示，以达到远程监控的目的。

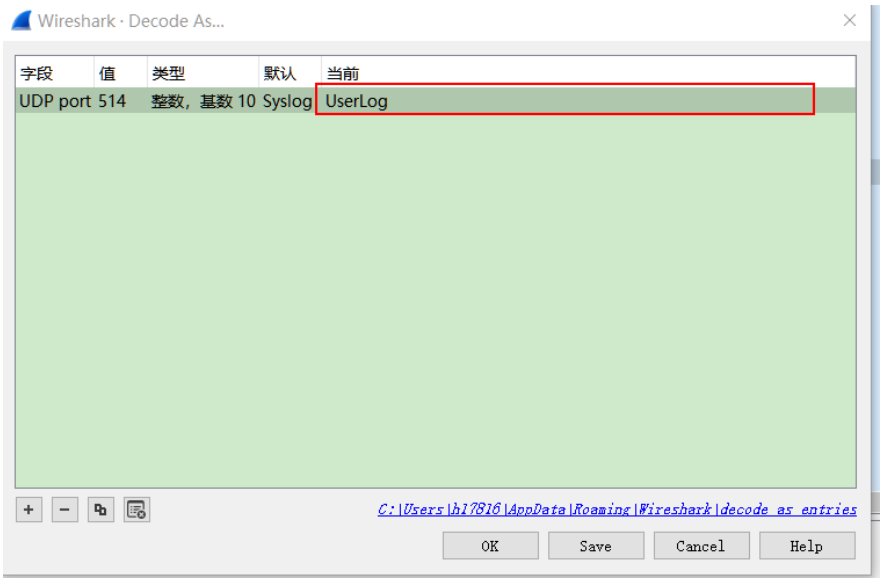
· 将Flow日志输出到本设备的信息中心模块（**userlog flow syslog**），再通过设置信息中心的输出参数，最终决定Flow日志的输出方向。

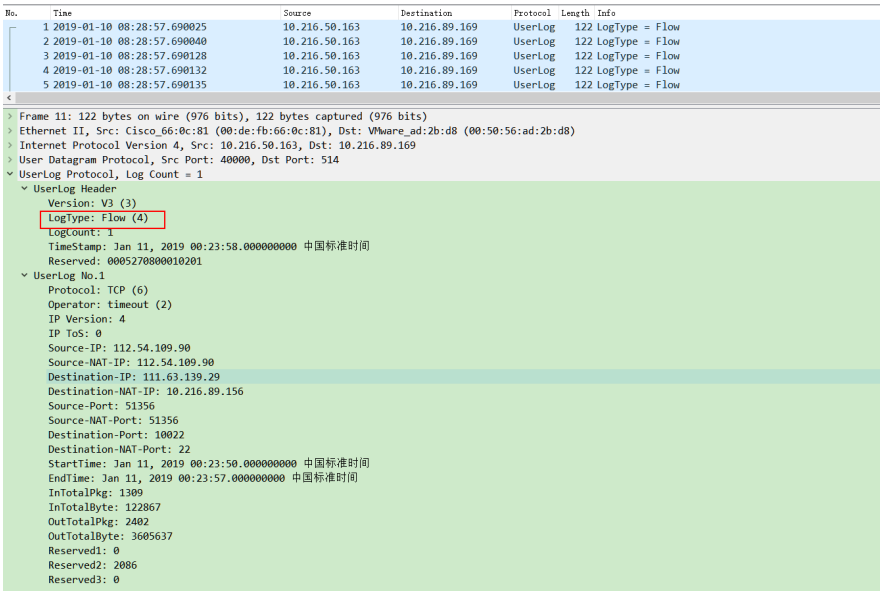
通常情况下，用户访问网络会在短时间内产生大量NAT会话日志。系统日志传输格式为ASCII码，相比Flow日志的二进制格式传输效率低。所以，建议在日志量较小的情况下，使用输出到信息中心的方式。

- 二进制格式的Flow日志Wireshark直接打开会显示乱码。



- 需要手工解码为Userlog格式才能正常显示，如下：点击日志报文，右键"decode as..."，下拉框中选择“userlog"并点击OK，便可正常显示。





Flow日志根据日志信息所包含字段多少分为Flow1.0、Flow3.0和Flow5.0三个版本。三种Flow日志的内容稍有不同，具体差别请参见表1-1、表1-2和表1-3。

下表中介绍的字段是设备向日志主机方向发送的原始信息所包含的字段，可能与用户最终看到的信息格式有差异，**最终显示格式与用户使用的日志解析工具有关，请以实际情况为准。**

表1-1 Flow1.0日志信息包含的字段

字段	描述
SrcIP	NAT转换前的源IP地址
DestIP	NAT转换前的目的IP地址
SrcPort	NAT转换前的TCP/UDP源端口号
DestPort	NAT转换前的TCP/UDP目的端口号
StartTime	流起始时间，以秒为单位，从1970/1/1 0:0开始计算
EndTime	流结束时间，以秒为单位，从1970/1/1 0:0开始计算 当Operator字段取值为6时，该字段为0
Protocol	IP承载的协议类型
Operator	操作字，记录生成Flow日志的原因： · 0：保留不用 · 1：正常流结束 · 2：定时器超时老化 · 3：清除配置/配置变动引起的流老化 · 4：资源不足带来的流老化 · 5：保留不用 · 6：活跃流定期记录其连接情况 · 7：新的流创建触发强制删除原有流 · 8：流创建 · FE：其他 · 10~FE-1：以后扩充用
Reserved	保留

表1-2 Flow3.0日志信息包含的字段

字段	描述
Protocol	IP承载的协议类型
Operator	操作字，记录生成Flow日志的原因： · 0：保留不用 · 1：正常流结束 · 2：定时器超时老化 · 3：清除配置/配置变动引起的流老化 · 4：资源不足带来的流老化 · 5：保留不用 · 6：活跃流定期记录其连接情况 · 7：新的流创建触发强制删除原有流 · 8：流创建 · FE：其他 · 10~FE-1：以后扩充用
IPVersion	IP报文版本
TosIPv4	IPv4报文的Tos字段
SourceIP	NAT转换前的源IP地址
SrcNatIP	NAT转换后的源IP地址
DestIP	NAT转换前的目的IP地址
DestNatIP	NAT转换后的目的IP地址
SrcPort	NAT转换前的TCP/UDP源端口号
SrcNatPort	NAT转换后的TCP/UDP源端口号
DestPort	NAT转换前的TCP/UDP目的端口号
DestNatPort	NAT转换后的TCP/UDP目的端口号
StartTime	流起始时间，以秒为单位，从1970/01/01 00:00开始计算
EndTime	流结束时间，以秒为单位，从1970/01/01 00:00开始计算 当Operator字段取值为6时，该字段为0
InTotalPkg	接收的报文包数
InTotalByte	接收的报文字节数
OutTotalPkg	发出的报文包数
OutTotalByte	发出的报文字节数
InVPNID	入VPN ID
OutVPNID	出VPN ID
Reserved1	保留
AppID	应用协议ID
Reserved3	保留

表1-3 Flow5.0日志信息包含的字段

字段	描述
Protocol	IP承载的协议类型
Operator	操作字，记录生成Flow日志的原因： · 0：保留不用 · 1：正常流结束 · 2：定时器超时老化 · 3：清除配置/配置变动引起的流老化 · 4：资源不足带来的流老化 · 5：保留不用 · 6：活跃流定期记录其连接情况 · 7：新的流创建触发强制删除原有流 · 8：流创建 · FE：其他 · 10~FE-1：以后扩充用
IPVersion	IP报文版本
TosIPv4	IPv4报文的Tos字段
SourceIP	NAT转换前的源IP地址
SrcNatIP	NAT转换后的源IP地址
DestIP	NAT转换前的目的IP地址
DestNatIP	NAT转换后的目的IP地址
SrcPort	NAT转换前的TCP/UDP源端口号
SrcNatPort	NAT转换后的TCP/UDP源端口号
DestPort	NAT转换前的TCP/UDP目的端口号
DestNatPort	NAT转换后的TCP/UDP目的端口号
StartTime	流起始时间，以秒为单位，从1970/01/01 00:00开始计算
EndTime	流结束时间，以秒为单位，从1970/01/01 00:00开始计算 当Operator字段取值为6时，该字段为0
InTotalPkg	接收的报文包数
InTotalByte	接收的报文字节数
OutTotalPkg	发出的报文包数
OutTotalByte	发出的报文字节数
InVPNID	入VPN ID

字段	描述
OutVPNID	出VPN ID
AppID	应用协议ID
UserName	用户名
Reserved1、2、3	保留字段

配置关键点

附件下载： Flow日志V3.rar