

## 知 V5平台防火墙Userlog日志包含哪些内容，部署时有哪些注意事项？

Syslog日志 彭旭 2019-10-29 发表

### 问题描述

V5平台防火墙Userlog日志包含哪些内容，部署时有哪些注意事项？

### 解决方法

V5平台防火墙支持Userlog日志功能。从名称看，Userlog日志与系统日志即Syslog相对，记录了除防火墙系统日志以外的其他信息，目前主要包含一种日志即会话日志，也称NAT日志。Userlog日志分V1、V3两种格式，如果希望记录某条会话在地址转换前和转换后的地址，必须使用V3格式进行输出。事实上无论防火墙上是否配置有NAT都可以输出Userlog日志。Userlog日志通常需要输出至一台日志主机查看，例如H3C SecCenter FW Manager，防火墙向SecCenter的UDP 30017端口以二进制流形式的输出日志，由SecCenter FWM接收后通过Web界面提供显示和查询功能；防火墙还支持通过信息中心以Syslog格式向日志主机输出，这样即使是普通的Syslog日志主机也能接收查看，但这种输出方式对防火墙CPU性能消耗较大，通常不建议采用这种部署方式。除了配置Userlog输出格式和具体的日志主机地址、端口等参数外，注意还要配置日志输出策略，必须配置需要输出日志的会话源安全区域、目的安全区域、其他输出参数等，防火墙才会真正产生Userlog日志并输出至日志主机。