

当ESA与系统日志服务器时，联络为什么有网络错误？

目录

[简介](#)

[当ESA与系统日志服务器时，联络为什么有网络错误？](#)

简介

本文描述电子邮件安全工具(ESA)为什么无法发送数据到系统日志服务器。

当ESA与系统日志服务器时，联络为什么有网络错误？

ESA配置推送日志订阅到系统日志服务器。文件可能或也许不顺利地推送到系统日志服务器。无论如何，可以有在邮件日志文件的网络错误类似于此：

```
Log Error: Subscription Mail_Log: Network error while sending log data to syslog server
```

在ESA和系统日志服务器之间的一数据包捕获显示系统日志服务器启动的连接丢包，在本例中是10.44.167.30。

o.	Time	Source	Destination	Protocol	Info
278	2015-06-25 08:50:04.111889	10.229.24.230	10.44.167.30	TCP	26040 > shell [SYN] Seq=0 Win=16384 Len=0 MSS=1460 WS=0 SACK_F
279	2015-06-25 08:50:04.114360	10.44.167.30	10.229.24.230	TCP	shell > 26040 [SYN, ACK] Seq=0 Ack=1 Win=32120 Len=0 MSS=1350
280	2015-06-25 08:50:04.114375	10.229.24.230	10.44.167.30	TCP	26040 > shell [ACK] Seq=1 Ack=1 Win=17550 Len=0
281	2015-06-25 08:50:04.114518	10.229.24.230	10.44.167.30	RSH	Client -> Server data
282	2015-06-25 08:50:04.114877	10.44.167.30	10.229.24.230	TCP	shell > 26040 [ACK] Seq=1 Ack=48 Win=32073 Len=0
283	2015-06-25 08:50:04.114883	10.229.24.230	10.44.167.30	RSH	Client -> Server data
284	2015-06-25 08:50:04.115362	10.44.167.30	10.229.24.230	TCP	shell > 26040 [ACK] Seq=1 Ack=413 Win=31755 Len=0
285	2015-06-25 08:50:04.116192	10.44.167.30	10.229.24.230	TCP	shell > 26040 [RST, ACK] Seq=1 Ack=413 Win=32120 Len=0

如果跟随在数据包捕获的TCP数据流您将看到此：

```
<22>Jun 25 08:50:03 example.com: Info: Begin Logfile
<22>Jun 25 08:50:03 example.com: Info: Version: 8.0.1-023 SN: A4BADB4712A9-511AA1E
<22>Jun 25 08:50:03 example.com: Info: Time offset from UTC: 7200 seconds
<22>Jun 25 08:50:03 example.com: Info: A System/Critical alert was sent to
alerts@ironport.com with subject "Critical <System> mail.example.com: Log Error:
Subscription Mail_Log: Network error while sending l..."
```

错误表明有阻止对系统日志服务器的访问在IP地址的防火墙或入侵防御系统(IPS)。如果所有设备中间被检查并且被确认为了允许流量，则这可能也意味着系统日志服务器太忙碌并且拒绝连接。当ESA配置发送日志文件到系统日志服务器，默认情况下然后将使用UDP系统日志端口514，除非配置使用TCP。一旦设备配置，造成连接列出作为拒绝的唯一的是一件事，如果收到断开连接的数据包，当打开时。