Why are there network errors when the ESA communicates with the syslog server?

Document ID: 119199

Contributed by Enrico Werner, Cisco TAC Engineer.
Jul 27, 2015

Contents

Introduction

This document describes why the Email Security Appliance (ESA) is unable to send data to a syslog server.

Why are there network errors when the ESA communicates with the syslog server?

The ESA has been configured to push log subscriptions to a syslog server. ***The files might or might not be successfully pushed to the syslog server.*** In any case, there can be network errors in the mail log file similar to this:

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

A packet capture between the ESA and the syslog server shows connection drops initiated by the syslog server, which in this example is 10.44.167.30.

o.	Time	Source	Destination	Protocol	Info
278	2015-06-25 08:50:04.111689	10.229.24.230	10.44.167.30	TCP	26040 > shell [SYN] Seq=0 Win=16384 Len=0 MSS=1460 WS=8 SACK_P
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

If you follow the TCP stream in the packet capture you will see this:

```
<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...".
```

The errors indicate that there is either a firewall or Intrusion Prevention System (IPS) that blocks access to the syslog server at the IP Address. If all devices in−between have been examined and confirmed in order to allow the traffic, then this could also mean that the syslog server is too busy and refused the connections. When the ESA is configured to send a log file to a syslog server, then by default it will use the UDP syslog port 514 unless configured to use TCP. Once the appliance is configured, the only thing that causes the connection to be listed as refused is if it receives packets that close the connection when it is opened.